

CA Service Desk Manager

管理ガイド

リリース 12.9.00



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、

(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとでの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2013 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

このドキュメントは、以下の CA Technologies 製品を参照しています。

- CA APM (CA Asset Portfolio Management)
- CA CMDB
- CA Business Intelligence
- CA Business Service Insight (CA BSI)
- CA Configuration Automation (以前の CA Cohesion ACM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Workload Automation (CA EWA)
- CA Process Automation (以前の CA IT PAM)
- CA 管理データベース (CA MDB)
- CA Management Portal
- CA NSM (CA Network and Systems Management)
- CA Portal
- CA Remote Control Manager (CA RCM)
- CA Service Desk Manager (CA SDM)
- CA Service Management
- CA Siteminder
- CA Software Delivery
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Wily
- CA Workflow

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

目次

第 1 章: はじめに	27
対象読者.....	27
必要な知識.....	27
サービス管理プロセスおよびベスト プラクティス	28
 第 2 章: サーバの管理	 29
サーバ数.....	29
サーバ設定を変更する方法	30
CA SDM サーバを起動する方法	31
標準設定での CA SDM サーバの起動	33
高可用性設定での CA SDM サーバの起動	34
CA SDM サーバのローリング メンテナンスを実行する方法	35
考慮事項の確認.....	37
スタンバイ サーバとバックグラウンド サーバ間でのバージョン管理の抑制.....	38
新しいバックグラウンドサーバとしてのスタンバイ サーバの昇格.....	38
アプリケーション サーバのローリング メンテナンスの実行	40
SSL 認証を設定する方法.....	43
前提条件を確認します。	44
WebDirector パラメータでの Web エンジンの機能の設定	44
SSL ログイン環境の選択.....	45
SSL ログイン環境のセットアップ	48
TCP/IP を設定する方法	55
CMDBf Web サービスを展開する方法	56
CA SDM サーバを再起動する方法	57
標準設定での CA SDM サーバの再起動	57
高可用性設定での CA SDM サーバの再起動	57
CA SDM サーバを停止する方法	61
標準設定での CA SDM サーバの停止	61
高可用性設定での CA SDM サーバの停止	62
タブレットのサポート	65
Tomcat ログイン	68
サーブレットのデフォルト値.....	69
PDA インターフェース	70
REST ログイン	71

CXF ログインの有効化.....	72
CA SDM サーバのプロセスを設定する方法	80
サーバの追加.....	81
プロセス設定の作成.....	83
CA SDM サーバプロセスの追加.....	84
設定の確認.....	100

第 3 章: REST サンプル モバイル ユーザ インターフェース 101

REST モバイル サンプル ユーザ インターフェースを展開する方法	103
REST Web サービスの設定	104
REST モバイル サンプル ユーザ インターフェースの有効化.....	105
REST モバイル サンプル インターフェースからのインシデントの管理.....	106
例: アナリスト インターフェース ホーム ページ.....	107
例: 従業員インターフェース ホーム ページ	108
例: 従業員によるインシデントの作成	109

第 4 章: CA SDM Mobile Enabler の設定 111

CA SDM Mobile Enabler	111
アナリスト キュー.....	112
承認	113
Open Space	116
前提条件の確認.....	118
認定モバイル オペレーティング システム	118
Open Space へのパッチ適用	118
CORS 設定の有効化.....	119
(オプション) フォーム フィールドを非必須として設定する.....	121
(オプション) アップグレード後の承認互換性の適用	122
CA SDM Mobile Enabler へのアクセス	122

第 5 章: 業務構造の定義 123

ビジネス ストラクチャの作成	124
ビジネス ストラクチャを作成する方法	127
業務インフラストラクチャの定義.....	137
オブジェクト定義の要求.....	138
ファミリーおよびクラス.....	138
製造者とモデル.....	139
サービス ステータス.....	139
ベンダー タイプとベンダー	139

設定項目.....	140
外部のアセット管理ツール.....	140
マルチ テナンシー.....	141
サービス プロバイダ.....	142
マルチテナンシーの仕組み.....	143
ユーザ インターフェースの影響.....	151
サポート オートメーションの影響度.....	155
ナレッジ マネジメントの影響.....	156
Multi-Tenancy の使い方.....	158

第 6 章: 統合検索による複数の検索エンジンの統合 171

統合検索の設定.....	172
前提条件の完了.....	174
統合検索の有効化.....	175
統合検索用の設定 XML ファイルの生成.....	176
CA SDM での統合検索ソースの作成.....	183
検索アダプタのアンインストール.....	184
Crawler Surface の設定.....	186
前提条件の完了.....	187
CA SDM ユーザの Crawler Surface の作成.....	187
Tomcat リモート IP アドレス フィルタの設定.....	188
Crawler Surface ユーザ ID の設定.....	190
SharePoint クローラの設定.....	199
SharePoint でのコンテンツ ソースの作成.....	200
クローラ ルールの作成.....	201
SharePoint でのクローラの開始.....	202
SharePoint でのメタデータの設定.....	203
SharePoint でのクローラ データの確認.....	204
トラブルシューティング.....	205
SDK インターフェースによる新しいカスタム アダプタの作成.....	207
新しいカスタム アダプタ Jar ファイルのコンパイル.....	209
CAFedSearch コンポーネントによる新しいカスタム検索アダプタの設定.....	212
新しいカスタム検索アダプタの確認.....	214
CORS (Cross-Origin Resource Sharing) フィルタの追加.....	215
REST による CAFedSearch サブプレットの呼び出し.....	216

第 7 章: ポリシーの実装 219

ポリシーの実装.....	219

通知	219
CA SDM インテグレーション	349

第 8 章: ユーザ アカウントの設定 373

連絡先	373
連絡先の定義	373
グループ	375
連絡先タイプ	376
連絡先タイプに基づく動作の決定	376
連絡先タイプに基づく通知のセットアップ	376
連絡先タイプに基づく連絡先の選択	377
特殊処理タイプ	377
特殊処理連絡先を設定する方法	378
特殊処理タイプに対する連絡先の関連付け	379
LDAP ディレクトリ データ	380

第 9 章: 役割の管理 409

役割	409
事前定義役割	410
役割ベースのセキュリティ	412
アクセス タイプについて	413
役割レコード	416
機能アクセス領域	417
データ パーティション	423
役割ベースのナビゲーション	423
Tabs	423
事前定義タブ	425
Web フォーム	427
フォーム グループ	428
メニュー ツリー	428
メニュー ツリー リソース	430
メニュー バー	430
ツールバー	432
実行リソース	432
ヘルプ セット	433
カスタム役割の実装方法	433
カスタム メニュー ツリーの实装方法	435
役割レコードの作成	437

タブ レコードの作成	438
メニュー バー レコードの作成	439
Web フォーム レコードの作成	440
メニュー ツリーのコピー	442
メニュー ツリーの作成およびカスタマイズ	443
ヘルプ セットの作成および発行	445
役割の切り替え	446

第 10 章: サポート ストラクチャの確立 449

モデル	450
内部モデル	450
外部モデル	451
結合モデル	452
CA Workflow	453
実行時の Workflow	454
Workflow プロセス定義の選択	455
ワークフロー タスク	456
CA Process Automation Workflow の統合	457
CA Process Automation コンポーネント	458
実行時の CA Process Automation の CA SDM との統合	459
プロセス定義を作成する方法	460
開始リクエスト フォームの作成	461
CA Process Automation プロセス定義の添付	463
共有コード	465
優先度コード	466
重大度コード	466
影響コード	467
緊急度コード	467
ステータス コード	468
リクエスト ステータス コード	469
変更要求ステータス コード	470
案件ステータス コード	471
タスク ステータス コード	472
タスク タイプ	473
インシデント トラッキングのインストール	475
リクエスト/インシデント/問題領域	476
[リクエスト/インシデント/問題領域] プロパティ	478
セルフ サービスのリクエスト/インシデント/問題領域の定義	480
変更要求と案件カテゴリ	481

事前定義済み変更カテゴリ	482
事前定義済み案件カテゴリ	482
チケットのカテゴリを変更する場合のルール	483
カテゴリのプロパティ	484
セルフ サービスに変更および案件カテゴリを定義する	487
チケットの自動クローズ	488
自動クローズ チケット設定を定義する方法	489
自動クローズ アクティビティ通知を定義する方法	490
関連チケット アクティビティ	490
関連チケットにアクティビティ通知を定義する方法	492
関連チケット アクティビティ通知を定義する方法	493
優先順位計算	493
優先順位計算でチケットの値を管理する方法	495
セルフサービス チケットの保存後に優先順位計算によって生成される緊急度値	498
優先順位計算の設定方法	500
ステータス遷移および従属属性のコントロール	513
ステータス移行および従属属性コントロールでの作業	514
ステータス移行の設定	514
従属属性コントロールの設定	516
Web サービス メソッド	517
事前定義済み移行フロー	518
ベスト プラクティス：事前定義済みステータス移行	522
セルフ サービスのためのステータス遷移	524
セルフ サービスの移行のしくみ	525
移行の移行タイプを作成または更新する方法	526
移行タイプを移行にリンクする方法	527
事前定義済み移行タイプのアクティブ化	527
タイマ	529
タイムゾーン	530
サービス タイプ イベント トリガ	531
タイムゾーン イベント トリガ	531
タイムゾーンのルール	532
添付ファイル ライブラリをセットアップする方法	533
CA SDM Web UI の表示	535
ファイル タイプの作成	535
リポジトリの選択	536
フォルダの作成	545
アナウンスメント	546
内部アナウンスメントの表示設定	547
アナウンスメントの緊急度の指定	548

ストアドクエリのセットアップ	548
シーケンス番号	550
監査ログの使用	551
CA ネットワークとシステム管理の統合	551
CA SDM Web ページの印刷	552
Web インターフェイスでのレコード ロック 動作	553
サポート 構造	554
CAPA ヘルプの有効化	554

第 11 章: システムの動作の制御 557

オプション マネージャの使用	557
システム環境を変更する方法	558

第 12 章: 自動割り当ての設定 565

自動割り当て	565
自動割り当ての関係	566
自動割り当てメソッド	566
自動割り当てを実装し始める方法	567
領域とカテゴリ	568
アナリスト グループ	568
アナリスト	569
グループ内の連絡先ではなく、グループに対してチケットの自動割り当てを行う方法	570
ロケーションに基づく自動割り当て	571
ワークシフト別の自動割り当て	572
デフォルトのグループと担当者	574
自動割り当てを有効にする	575
自動割り当て設定	576
割り当て制御	577
手動割り当て	577
Assignee_set オプション	578
lss assignee_set	578
Area_Defaults	578
必須担当者/グループのオプション	578
テンプレート	580
CA Network and Systems Management インターフェイス	580
アクティビティのログ記録	580
追加の属性に対するアクティビティ ログの有効化	581
自動割り当てのトレース	582

ストアドクエリ	582
自動割り当てでのチケット割り当て方法	583
自動割り当てでのワークフロー タスクの割り当て方法	590
構成アイテムベースの自動割り当て	594
構成アイテムに基づいた自動割り当てのしくみ	594
構成アイテムに基づいた自動割り当ての有効化	598

第 13 章: データベースの管理 601

データベース管理ユーティリティ	601
データベースの選択と設定	601
データベース ローダ	602
入力ファイルを作成および使用する方法	603
制約の削除と復元	604
データベースのバックアップ	605
データベースのリストア	606
データベース テーブル置換	606
データ抽出	607
データの修飾参照	609
pdm_deref の使用方法の例	609
dbadmin モードの使用	612
ブラウザ キャッシュを使用したパフォーマンスの向上	626
Microsoft Internet Information Server の設定	626
Apache の設定	627
キャッシュのクリア	628
環境設定ファイルの変更	629
SchedExpMaximum	640
SelListCacheExclude	640
SelListCacheMax	640

第 14 章: Text API の使用 647

Text API	647
コマンドライン インターフェース	648
CA Network and Systems Management インターフェース	648
入力フォーマット	649
キーワード	650
キーワードの入力規則	653
チケットを更新するための電子メールのフォーマット	654
電子メール メッセージの開始および終了区切り文字	655

Text API におけるアーチファクトの使用	655
チケットを更新する通知応答のセットアップ方法	656
変換メソッド	660
環境設定ファイル	663

第 15 章: CA SDM サーバにわたるシステム カスタマイズのバージョン管理方法 669

前提条件の確認	671
サーババージョン管理ファイルの変更	671
バージョン管理コンポーネント	672
バージョン管理のパラメータ	673
クライアントでの CA SDM の再起動	679
アクティビティの少ないアプリケーション サーバの選択	680
ほかのアプリケーション サーバの停止	680
クライアントでのカスタマイズの確認	681

第 16 章: 構成アイテムの管理 683

Web インターフェースの使用	683
構成アイテムの表示	684
構成アイテムの作成	685
構成アイテムの更新	686
CI と保守ウィンドウの関連付け	687
関連付けられた変更ウィンドウの表示	687
構成アイテムの履歴表示	688
構成アイテムの非アクティブ化	688
構成アイテムの再アクティブ化	689
連絡先、ロケーション、組織 CI	689
ベース オブジェクトからの CI の作成	690
CI のベース オブジェクトの選択	691
ベース オブジェクトの CI の詳細の編集	691
ベース オブジェクトの CI 属性の編集	692
GRLoader を使用したベース オブジェクト CI の作成	693
CI 関係	694
構成アイテム関係タイプ	695
関係タイプの作成	695
構成アイテム関係の管理	696
構成アイテム関係の作成	697
CI 間の関係の表示	697

CI 関係の非アクティブ化.....	698
CI 関係の再アクティブ化.....	698
CI 関係の非アクティブ化（リスト内で編集）	699
GRLoader を使用した CI 関係の非アクティブ化	700
GRLoader を使用した CI 関係の復活	701
データベースからの CI 関係の削除.....	702
CI 関係履歴および比較.....	702
バージョン指定.....	703
バージョン指定の用途.....	705
共有アセットと CI 監査証拠レコード	706
バージョン指定の用語.....	706
バージョン指定データのソース	710
CA SDM 変更管理統合.....	711
CA APM 統合.....	713
CI バージョン指定管理.....	714
CA SDM 変更管理.....	734
他の CA 製品での CI 属性の表示.....	735
CMDBf ドライバの使用.....	736
CMDB Visualizer	736
根本原因の分析.....	739
Visualizer 管理	739
検出されたアセットの追加	740
アセット フラグと CI フラグ	741
CI 調整.....	743
MDR-Based 調整.....	744
あいまいな CI を識別して解決する方法	746
トランザクションワーク エリア（TWA）を使用した着信データの確認と変更.....	761
ステージング済みトランザクションの管理	767
トランザクションワーク エリア	768
TWA へのデータ入力.....	770
TWA 内のデータの更新に Web インターフェースを使用する方法	783
関係トランザクションの管理.....	787
CMDB にトランザクションをロードする方法	789
TWA の管理.....	791
CA CMDB データ保守	795
CA CMDB のファミリ クラス構造.....	796
単一の CI のファミリ/クラスの変更	797
CI のリストのファミリ/クラスの変更	797
GRLoader を使用したファミリ/クラスの変更.....	798
CA CMDB の拡張	799

構成監査および制御機能 (CACF)	811
CACF の管理およびポリシー定義.....	813
管理対象属性.....	830
管理対象変更状態.....	830
変更仕様.....	833
変更検証の実行方法.....	838
監査データのアーカイブおよびパージ方法.....	844
変更検証戦略の実装.....	845
変更検証の計画および実装.....	850
変更検証のベストプラクティス.....	858
CI 属性値の更新の手動検証.....	862
例：特定のロケーションからのみ非承認の更新を許可する	868
例：組織内のラップトップのアップグレード	869
例：検証されていない変更要求の除外	871
例：一致する変更要求が存在しない場合に CI 更新を許可する	871
例：すべての更新を CA Configuration Automation から TWA に延期する	872
例：ポリシー結果をテストとしてのみログに記録する	873
例：CI 更新を拒否する	873
例：仕様なしで作成された変更要求を許可する	874
例：仕様なしで作成された変更要求を許可しない	874
例：選択されたソースからの非承認の挿入を許可する	875
例：実稼働以外の CI の非承認の更新を許可する	875

第 17 章: <MDR> の管理 877

MDR とは.....	877
MDR のクラスおよび MDR 名	878
MDR に CA SDM を実装する方法	878
CA SDM への MDR の定義.....	879
MDR Launcher.....	879
MDR を起動するための URL を定義する	880
CA APM の MDR プロバイダをセットアップする	882
CA CMDB から CA APM のコンテキストでの起動.....	883
MDR Federation をサポートする CI 優先度.....	883
統一アセット ID	883
MDR 名.....	884
MDR クラス.....	884
CA Cohesion ACM のインストールによる MDR 定義	885
CA Cohesion ACM MDR.....	886
MDR を手動で CI に関連付ける方法	887

CA Cohesion の自動インポート	888
MDR への CI のマッピング	888
MDR 定義の管理	890
CA Cohesion ACM のレポート	890
GRLoader の使用	891
CI の命名規則および命名制限	891
system_name の命名規則	893
CMDBf ドライバの使用	895
CMDBf マッピングのメタデータ ファイルの更新方法	895
MDR 属性値を CA CMDB 属性名で表示する方法	897
MDR プロバイダ属性を非表示にする方法	898
CA CMDB が対応していない MDR 属性を定義する方法	899
CMDBf データ プロバイダ メタデータの定義	899

第 18 章: 変更の管理 901

CA SDM での変更管理	901
変更管理コンポーネント	902
変更カレンダーの表示	904
CAB の役割	904
CAB プロセスの仕組み	905
CAB グループへのメンバーの割り当て	905
変更マネージャの役割	906
変更マネージャの役割の仕組み	907
変更マネージャの役割に割り当てるタスクの定義	908
変更カテゴリ、ステータス、およびリスク レベル	909
変更要求スコアボードの表示	910
変更要求のストアドクエリの定義	911
変更マネージャ オプションの設定	912
変更カレンダー	913
変更要求へのスケジュール情報の追加	913
iCalendar イベント テンプレート	914
iCalendar へのスケジュールのエクスポート	915
スケジュール ビュー	916
スケジュール ビューの環境設定	918
変更要求のスケジュール方法	928
変更スケジューラの使用例	929
変更ウィンドウのスケジュール方法	933
変更ウィンドウの表示	934
CI と保守ウィンドウの関連付け	935

関連付けられた CI の表示.....	935
中断ウィンドウの作成例.....	936
グローバル保守ウィンドウの作成.....	937
競合分析と衝突検出.....	937
CA Workflow の視覚化.....	938
ワークフローの視覚化方法.....	938
CA Workflow 用の変更管理プロセス定義.....	940
変更管理プロセス定義のコンポーネント.....	941
変更管理プロセス定義の設定方法.....	942
変更管理プロセス定義の動作のしくみ.....	948
ActivityNode Actor が見つかりませんでした：オブジェクトの更新 - Service Desk r12.....	963
変更要求が閉じない.....	964
CAB コンソールとレポートの作成.....	964
CAB グループの管理.....	966
CAB グループの割り当て.....	968
CAB 承認.....	968
CAB コンソールのプロパティの変更.....	969
変更管理のレポート.....	970
リスク評価.....	971
リスク調査の実装方法.....	972
URL からリスク調査に直接アクセスする方法.....	974
影響度エクスプローラ.....	975
影響度エクスプローラの起動.....	976
添付された構成アイテムの調査.....	976
影響度エクスプローラでの構成アイテムの表示.....	977
変更要求への関連する構成アイテムの追加.....	978
構成アイテム子孫リストの表示.....	978
影響度エクスプローラからの CMDB Visualizer の起動.....	979
影響度エクスプローラの設定.....	979

第 19 章: レポートの管理 981

第 20 章: CA Business Intelligence レポート 983

レポート シナリオ.....	984
レポート コンポーネント.....	984
レポート データ フロー図.....	988
InfoView での Web ベースのレポートの表示.....	989
セキュリティと認証.....	990
グループとユーザ.....	991

Infoview 内の CA SDM データ パーティション	992
ユニバースとユニバース接続	992
レポート フォルダ	993
アクセス レベル	995
既存の CA Business Intelligence サーバ が CA SDM サーバを指す方法	997
ODBC データ ソースを作成する	997
ユニバースの設定	998
ユニバースのエクスポート	999
レポートへのデータ パーティション セキュリティのセットアップ方法	999
CMC への CA SDM 特権ユーザの追加	1000
ユニバース データベースのクレデンシャルの定義	1000
データ パーティションの設定	1002
オフライン レポート用の複製されたデータベース	1002
ロールベースのレポート	1002
役割への役割ベース レポートの定義	1002
[レポート] タブへの新規レポートの表示	1005
Web ベースのレポート	1013
BusinessObjects InfoView インターフェース	1013
レポートへの移動	1014
InfoView の環境設定	1014
レポートのスケジュール	1015
データ分析のセットアップ	1016
レポートの発行と配布	1016
重要業績評価指標 (KPI)	1016
KPI タイプ	1017
事前定義済み KPI	1018
KPI デーモン	1018
システム KPI	1019
ストアドクエリ KPI	1021
SQL KPIs	1022
KPI フィールド	1023
チケットデータの取得	1025
トラブルシューティング	1028
一時的なレポート	1030
Web Intelligence インターフェース	1030
一時的なレポートの作成機能の仕組み	1031
一時的なレポートの例	1032
例：優先度 1 および 2 のすべてのオープン リクエストをすべてのユーザに表示	1032
例：[作業中] ステータスが含まれていないすべてのオープン リクエストの表示	1034
例：姓が「C」で始まるユーザの過去 30 日間のすべてのクローズ リクエストの表示	1035

ダッシュボード レポート	1038
InfoView でのダッシュボードおよびレポートの表示	1039
CA Business Intelligence レポートの作成	1039
CA SDM ODBC ドライバ	1040
BusinessObjects レポート用の SQL の作成	1041
PDM 関数	1042
属性の別名	1045
pdm_isql による対話的な SQL	1045

第 21 章: CA SDM でのレポートの生成 1047

レポートの生成	1047
データベース ビュー	1047
基本ビュー	1048
高度なビュー	1050
レポート方法のセットアップ	1051
レポート形式	1052
列の並べ替え順の変更	1053
概要レポートと詳細レポート	1053
分析レポート	1054
リクエスト レポートまたは案件レポートの生成	1054
リクエスト領域レポートまたは案件カテゴリ レポートの生成	1055
優先度別のリクエスト領域レポートまたは優先度別の案件カテゴリ レポートの生成	1055

第 22 章: ナレッジの管理 1057

ナレッジ マネジメント	1057
ナレッジ マネジメントの手順の検索	1058
ナレッジとマルチテナンシー	1059
ナレッジ ベースのセットアップ方法	1059
サンプル ナレッジ データのインポート	1060
ナレッジ ベースの監視	1060
ナレッジ ベースのインデックスの再作成	1061
バッチ処理とインスタント処理用のインデックス作成およびインデックス解除のキュー設定	1061
ナレッジ ベースのドキュメントの使用方法	1062
CA SDM からのナレッジのサブミット	1064
セルフサービスからのナレッジのサブミット	1065
ドキュメント属性	1065
ドキュメント権限	1065
解決方法の編集	1066

ドキュメントの発行準備.....	1067
ドキュメントの発行.....	1067
ドキュメントのバージョン管理.....	1068
ドキュメントの有効期限.....	1069
ドキュメントのアーカイブとパージ.....	1069
ナレッジ検索.....	1070
REST Web サービスを介して CAFedSearch サブレットを呼び出す方法.....	1071
フォーラム.....	1072
ナレッジ ツリー ドキュメント.....	1072
ナレッジ ドキュメント スケジュール.....	1073
ナレッジ スケジュール フィルタ.....	1073
[ナレッジ スケジュール] ビュー.....	1076
スケジュール ビューの環境設定.....	1077
エクスポート/インポートへのアクセス.....	1084
ナレッジのエクスポート/インポート方法.....	1085
ドキュメントのエクスポート/インポート.....	1089
パッケージのエクスポート/インポート.....	1089
エクスポート/インポートテンプレートの表示.....	1091
pdm_ket ユーティリティ - ナレッジ エクスポート ツール.....	1100
pdm_kit ユーティリティ - ナレッジ インポート ツール.....	1101
ナレッジのエクスポートまたはインポートをユーザに許可.....	1103
Web サービス.....	1104

第 23 章: ナレッジ マネジメント の管理 1105

ナレッジ管理.....	1105
ナレッジ管理の手順の検索.....	1105
ナレッジ マネジメント の役割と機能.....	1106
ナレッジ マネジメント のユーザ インターフェース.....	1107
ナレッジ マネジメント の設定機能と管理機能.....	1108
セルフサービス ナレッジ オプション.....	1109
ドキュメントとユーザ.....	1115
役割権限とドキュメントの表示/非表示の管理方法.....	1119
アクション コンテンツ.....	1120
アクション コンテンツの表示.....	1121
アクション コンテンツ (アクション URL) の作成.....	1122
アクション コンテンツ (内部 HTML) の作成.....	1123
アクション コンテンツの編集.....	1124
アクション コンテンツの検索.....	1124
ドキュメント承認プロセス.....	1126

承認プロセス マネージャ	1127
ドキュメント編集のための承認プロセスの定義	1127
承認プロセス テンプレートの作成	1129
ドキュメント ステータスの定義	1132
自動ポリシー	1134
自動ポリシーの表示	1134
自動ポリシーをセットアップする方法	1136
自動ポリシーの作成	1136
自動ポリシーの編集	1137
自動ポリシーのスケジュール	1138
ドキュメント ライフサイクル ポリシー レポートの表示	1139
ナレッジ ドキュメントの制御	1140
コメント タイプ	1141
ドキュメント テンプレート	1148
ナレッジ ドキュメント リンクを作成する方法	1157
ナレッジ カテゴリ	1159
レポートおよびメトリック	1171
検索	1173
解決策に関する調査	1203
ナレッジ マネジメント システムの設定	1206
一般設定の構成	1207

第 24 章: サポート オートメーション の管理 1213

環境でのサポートの自動化	1213
ライブ アシスタンス	1214
サポート オートメーション アナリスト 管理	1217
はじめに	1217
アナリスト向けにライブ アシスタンスを設定する方法	1218
アナリストによるライブ アシスタンスの起動方法	1228
アナリスト向けにライブ アシスタンスを設定する方法	1229
エンドユーザがアシスタンス セッションに参加する方法	1230
アナリストがエンドユーザへのサポートを自動化する方法	1232
アナリストによるライブ アシスタンスの提供方法	1233
サポート オートメーション のユーザ 管理	1234
サポート オートメーション 役割権限を設定する方法	1234
サポート オートメーション 匿名ユーザと登録ユーザ	1235
ゲスト ユーザ向けにサポート オートメーションを設定する方法	1236
サポート オートメーション のアクセス レベル 管理	1239
サポート オートメーション のアクティビティ 通知 管理	1241

サポート オートメーション ページの適応化	1242
ブランディング管理.....	1243
ローカライゼーション管理.....	1244
ページレイアウト設定.....	1245
サポート オートメーション のシステム プロパティ.....	1246
サポート オートメーション のキュー管理	1246
キュー管理.....	1247
キューの概要の管理方法.....	1248
キュー時間を管理する方法.....	1249
チケット テンプレート管理.....	1249
管理設定.....	1250
サポート オートメーション の設定を構成する方法	1250
サポート オートメーション ツールをカスタマイズする方法.....	1252
自動タスク	1253
チャット プリセット管理.....	1259
デフォルト認証情報.....	1260
免責条項.....	1261
セッション ログ管理.....	1261
セッション ログの表示.....	1262
サポート オートメーション レポート	1262
チケット リクエストの受信.....	1265
エンド ユーザをアシスタンス セッションに招待	1266
チャット セッションを使用したチケットの解決.....	1267
ライブ アシスタンスの提供.....	1268
アシスタンス セッションを終了し、チケットをクローズします。	1269

第 25 章: CA SDM のパフォーマンスの問題を識別する方法 1271

パフォーマンスの問題の定義.....	1273
前提条件を確認します。	1274
Windows への Ps ツールのインストール	1274
CA 診断レポート ツールからの情報の収集.....	1275
CA 診断ツールの実行	1276
Windows レポートの検証.....	1277
UNIX レポートの検証.....	1279
収集された診断レポートの検証.....	1280
データベース サーバ環境の詳細の収集	1281
CA SDM のパフォーマンス データを収集します。	1282
期間ログを使用した使用率データの収集.....	1283
一般的なチューニングの推奨事項の確認	1286

付録 A: 参照コマンド

1289

bop_sinfo -- システム情報の表示.....	1290
dbmonitor_nxd -- データベース監視デーモン.....	1291
pdm_backup—ASCII ファイルへのデータベースの書き込み.....	1293
pdm_cache_refresh—データベースの更新.....	1294
pdm_configure—環境設定ウィンドウを開く.....	1296
pdm_d_refresh—失敗したデーモンの起動.....	1297
pdm_deref—ASCII データの修飾参照.....	1297
pdm_discimp -- 検出されたアセットのインポート.....	1301
pdm_discupd -- 検出されたアセットの更新.....	1303
pdm_extract—データベースからのデータの抽出.....	1304
pdm_halt—デーモンまたはサービスの終了.....	1308
pdm_init—デーモンの起動.....	1309
pdm_key_refresh—キャッシュされたキー情報の更新.....	1309
pdm_lexutil--CA SDM 語彙集の変更.....	1310
pdm_k_reindex-- Knowledge Re-Index Utility.....	1311
pdm_k_reindex を使用するタイミング.....	1313
インデックス再作成のトラッキング.....	1313
インポートとインデックス再作成.....	1314
バッチ処理とインスタント処理用のインデックス作成およびインデックス解除のキュー設定.....	1314
pdm_listconn—アクティブな接続のリスト.....	1315
pdm_load—データベース レコードの追加、更新、および削除.....	1318
pdm_logfile—stdlog のカットオーバー サイズの変更.....	1320
pdm_log4j_config ユーティリティ - log4j プロパティ ファイルの変更.....	1321
ユーティリティの使用例.....	1323
ログ ファイル更新間隔の手動変更.....	1325
jsrvr.log アペンダの変更.....	1326
jstd.log アペンダの変更.....	1326
pdm_proctor_init—セカンダリ サーバでの proctor の開始.....	1327
pdm_replace—データベース テーブルの置換.....	1327
pdm_rest_util - CA SDM RESTful Web サービス アプリケーションの管理.....	1329
REST Web サービス アプリケーションの展開解除.....	1330
pdm_restore—データベースの復元.....	1330
pdm_status—デーモンまたはプロセスのステータスの表示.....	1332
pdm_task—環境変数の設定.....	1333
pdm_text_cmd—Text API コマンドライン インターフェース.....	1333
入力例.....	1336
pdm_uconv--ローカルの文字セットから UTF-8 への変換.....	1337
pdm_userload—データベース レコードの追加、更新、および削除.....	1340

pdm_webstat—Web 使用状況の統計の表示	1343
report—レポートの生成.....	1348
rpt_srv—レポートの生成	1349
uniconv--UNIX CA NSM Event Converter デーモンの起動.....	1351
pdm_mail ユーティリティ -- 電子メール情報の送信	1352
pdm_server_control ユーティリティ -- サーバの識別	1355

付録 B: ビューのフィールドの説明 1357

ビューのフィールドの説明	1358
View_Act_Log.....	1358
View_Audit_Assignee.....	1360
View_Audit_Group.....	1360
View_Audit_Priority	1361
View_Audit_Status	1362
View_Change_Act_Log.....	1362
View_Change.....	1364
View_Change_to_Assets.....	1369
View_Change_to_Change_Act_Log	1370
View_Change_to_Change_WF.....	1371
View_Change_to_Properties	1374
View_Contact_Full	1375
View_Contact_to_Environment.....	1378
View_Group	1379
View_Group_to_Contact.....	1380
View_Issue	1380
View_Issue_Act_Log.....	1385
View_Issue_to_Assets.....	1387
View_Issue_to_Issue_Act_Log	1387
View_Change_to_Request	1389
View_Issue_to_Issue_WF.....	1392
View_Issue_to_Properties	1395
View_Request	1396
View_Request_to_Act_Log	1401
View_Request_to_Properties	1402

付録 C: フォーム グループ 1405

顧客フォーム グループ	1406
従業員フォーム グループ	1407
アナリスト フォーム グループ	1409

付録 D: RFC 2251 LDAP 結果コード	1435
LDAP のリターン コード.....	1435
LDAP サーバの戻り値	1435
LDAP クライアントの戻り値	1442
LDAP 関連の RFC 標準	1444

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

[対象読者](#) (P. 27)

[必要な知識](#) (P. 27)

[サービス管理プロセスおよびベスト プラクティス](#) (P. 28)

対象読者

本書は、製品の管理に関して全面的な責任を負う **CA Service Desk Manager (CA SDM)** 管理者を対象としています。管理者が実行するタスクの一部を以下に示します。

- CA SDM サーバに対して必要なサービスの起動と停止
- さまざまなシステム コンポーネントのセットアップ
- ユーザが利用可能なオプションの決定
- サービス デスク データに基づくレポートの生成

本書の目的は、**CA SDM** によって、サービス デリバリーを実装、管理、および適用できるように支援することです。本書は、問題発生からその解決まで、サービス デリバリーの完全自動化と管理という課題を本製品でどのように解決するかを理解するのに役立ちます。

必要な知識

CA SDM を正しく管理するには、以下について理解している必要があります。

- **CA SDM** がインストールされている動作環境
- Web サーバの操作
- 基本的な管理タスク

本書は、「実装ガイド」の情報に基づいて、製品が正しくインストールされていることを前提としています。

サービス管理プロセスおよびベスト プラクティス

標準化されたプロセスおよびベスト プラクティスの導入は、サービス サポート環境の効率性、生産性、およびコストに直接影響を及ぼします。CA では、業界標準に準拠したサービス管理を実現するための推奨プロセスとベスト プラクティス、および ITIL、CobIT、BS15000 などの定評あるベスト プラクティス フレームワークで構成するライブラリを用意しています。記載されている CA SDM のプロセスは、以下のとおりです。

- インシデント管理
- 問題管理
- 変更管理
- リクエスト管理
- 環境設定管理
- リリース管理
- ナレッジマネジメント
- サポート オートメーション

注: ベスト プラクティス ライブラリに関する情報はオンラインで入手できます。CA のサービス管理のベスト プラクティスについては、<http://www.ca.com/sm/bp> <http://www.ca.com/sm/bp> にアクセスし、ホワイト ペーパーやその他の記事を参照してください。また、ベスト プラクティスをそれぞれの組織に合わせて採用できるように、CA パートナーの戦略 プロセス専門家が支援いたします。

第 2 章：サーバの管理

このセクションには、以下のトピックが含まれています。

- [サーバ数 \(P. 29\)](#)
- [サーバ設定を変更する方法 \(P. 30\)](#)
- [CA SDM サーバを起動する方法 \(P. 31\)](#)
- [CA SDM サーバのローリング メンテナンスを実行する方法 \(P. 35\)](#)
- [SSL 認証を設定する方法 \(P. 43\)](#)
- [TCP/IP を設定する方法 \(P. 55\)](#)
- [CMDBf Web サービスを展開する方法 \(P. 56\)](#)
- [CA SDM サーバを再起動する方法 \(P. 57\)](#)
- [CA SDM サーバを停止する方法 \(P. 61\)](#)
- [タブレットのサポート \(P. 65\)](#)
- [Tomcat ログイン \(P. 68\)](#)
- [PDA インターフェース \(P. 70\)](#)
- [REST ログイン \(P. 71\)](#)
- [CA SDM サーバのプロセスを設定する方法 \(P. 80\)](#)

サーバ数

CA SDM インストールには、管理者が管理するサーバ コンポーネントが 1 つ以上あります。サーバの数は CA SDM の設定に依存します。

- 標準：1 つのプライマリ サーバおよび 1 つ以上のセカンダリ サーバ。
- 高可用性：1 つのバックグラウンドサーバ、1 つ以上のスタンバイサーバ、および 1 つ以上のアプリケーション サーバ。

CA SDM をインストールした後、製品コンポーネントを実行する各コンピュータを環境設定します。サーバ設定は、インストールプロセスの一部としてを実行することも、後で実行することもできます。サーバ設定を変更した後、CA SDM サービスを再起動する必要があります。

サーバの計画および設定方法の詳細については、「[実装ガイド](#)」を参照してください。

サーバ設定を変更する方法

管理者は、CA SDM インストールのすべてのサーバを設定します。サーバの数とタイプはCA SDM の設定に依存します。最初の環境設定は、CA SDM インストールプロセスの一部として実行されます。

注: システム環境の変更に伴い、サーバの設定の変更が必要になることがあります。たとえば、データベース管理システムの変更、Tomcat などの Web サーバとの統合、または CA EEM との統合などがあります。

構成ユーティリティを使用して、サーバ構成を変更することができます。サーバの設定の詳細については、「実装ガイド」を参照してください。

次の手順に従ってください:

1. 設定するサーバに再度ログインします。
2. Windows の [スタート] メニューから、[すべてのプログラム] - [CA] - [CA SDM] - [環境設定] を選択します。

CA SDM 環境設定ユーティリティが表示されます。

3. ユーティリティ フィールドの変更を完了し、[次へ] をクリックします。

左のナビゲーションペインでハイライトされているリンクのフィールドが、右のパネルに表示されます。

4. 引き続き画面の指示に従ってインストールを完了し、[完了] をクリックします。

サーバ構成が変更されます。

CA SDM サーバを起動する方法

CA SDM の設定に応じて、以下のアクションを実行します。

- [標準設定で CA SDM サーバを起動します](#) (P. 33)
- [高可用性設定で CA SDM サーバを起動します](#) (P. 34)。

以下の表では、CA SDM サーバを起動すると自動的に開始されるプロセスについて説明します。

プロセス	説明
Daemon Agent (pdm_proctor_nxd)	管理対象デーモンを開始するデーモン エージェントです。
Daemon Monitor (pdm_d_mgr)	デーモン プロセスを監視します。
BOP Virtual DB (bpvirtb_svr)	BOP Virtual Database サーバです。
Data Dictionary (ddictbuild)	システムを起動するたびに、データ辞書が再構築されます。これは実行後に消去されます。
KPI Daemon (kpi_daemon)	KPI データの収集、編成、および格納を管理します。
Oracle エージェント (orcl_agent)	Oracle データベースのエージェントです。インスタンス数は負荷に応じて異なります。
Oracle DB (orcl_prov_nxd)	Oracle データベース プロバイダです。
SQL エージェント (sql_agent) (MS SQL を使用している場合のみ 実行します)	SQL Server データベースのエージェントです。インスタンス数は負荷に応じて異なります。
SQL DB (sql_prov_nxd) (MS SQL を使用している場合のみ 実行します)	Microsoft SQL Server データベース プロバイダです。
Event Manager (ehm_nxd)	イベント マネージャです。
Message Dispatcher (sslump_nxd)	メッセージをディスパッチします。
Notification Manager (bpnotify_nxd)	通知を管理します。
Object Engine (domsrvr)	CA SDM オブジェクト マネージャです。
Report Manager (pcrpt_nxd)	PC のレポート機能です。

プロセス	説明
Software Version Control (pdm_ver_nxd)	特定のシステム コンポーネントのバージョンを管理します。
Method Engine (spel_srvr)	spell コードインタプリタです。
Text API (pdm_text_nxd)	電子メールや CA NSM インターフェースに使用するテキスト API デーモンです。
Timed Events/Notifications (animator_nxd)	時間関連のイベントおよび通知です。
User Validation (boplogin)	ユーザ アカウントの検証
User Authentication (bopauth)	ユーザ アカウントの認証
Web Engine (webengine)	Web クライアント用のエンジンを実行します。
Archive Purge Daemon (arcpur_srvr)	バックグラウンドのアーカイブおよびパージ処理を管理します。
BU Daemon (bu_daemon)	ナレッジ ドキュメントのために、 FAQ 評価計算を制御します。
DB Monitor (dbmonitor_nxd)	変更がないかどうか、 CA の共通テーブルを監視します。
EBR Daemon (bpebr_nxd)	ナレッジ検索リクエストを制御します。
EBR Idx Daemon (bpeid_nxd)	EBR のキーワード インデックス作成/インデックス再作成を制御します。
KRC Daemon (krc_daemon)	ナレッジ レポート カードのために、統計の計算や通知を管理します。
KT Daemon (kt_daemon)	ナレッジ ドキュメント (KD 承認プロセス、許可、通知など) を管理します。
LDAP virtldb (ldap_virtldb)	LDAP サーバに対する通信エージェントです。
Mail Daemon (pdm_mail_nxd)	送信電子メール通知を制御します。
Mail Eater (pdm_maileater_nxd)	受信電子メール通知を制御します。
MDB Registration Server (mdb_registration_nxd)	MDB 登録リクエストを制御するエージェントです。
PDM RPC (PDM_RPC)	Web サービス リクエストを管理します。
Repository Daemon (rep_daemon)	添付ファイル リポジトリを制御します。
Spell checker (lexagent_nxd)	スペル チェック リクエストを制御します。

プロセス	説明
Time-to-Violation (ttv_nxd)	サービス レベル アグリーメント違反を予測する機能です。
tomcat controller (pdm_tomcat_nxd)	Tomcat サービスを管理します。

注: この表で、Notification Manager プロセスは Windows 環境のみに適用され、Default DB プロセスは UNIX 環境のみに適用されます。

標準設定での CA SDM サーバの起動

以下の順序でサーバを起動します。

1. [セカンダリ サーバを起動します](#) (P. 33)。
2. [プライマリ サーバを起動します](#) (P. 34)。

セカンダリ サーバの起動

使用中のインストール環境に 1 つ以上のセカンダリ サーバが含まれる場合は、セカンダリ サーバをすべて起動してからプライマリ サーバを起動する必要があります。

次の手順に従ってください:

- (Windows) [コントロール パネル] から [サービス] を選択し、[CA SDM Remote Proctor] サービスを選択して、[開始] をクリックします。
- (UNIX) コマンドラインから `pdm_init` を使用します。

関連項目:

[pdm_proctor_init—セカンダリ サーバでの proctor の開始](#) (P. 1327)

プライマリ サーバの起動

各 CA SDM インストールには、基本的な製品機能进行处理する 1 つのプライマリ サーバがあります。

重要: インストールに 1 つ以上のセカンダリ サーバが含まれる場合、プライマリ サーバを起動する前に[セカンダリ サーバを起動 \(P. 33\)](#)しておく必要があります。

次の手順に従ってください:

- (Windows) [コントロール パネル] から [CA SDM Server] サービスを選択し、[開始] をクリックします。必要なときにいつでも手動でこのサービスを開始できます。また、ほかの Windows サービスと同様に自動的に開始されるように設定できます。
- (UNIX) コマンドラインから `pdm_init` を使用します。

高可用性設定での CA SDM サーバの起動

以下の順序でサーバを起動します。

注: (Windows) [コントロール パネル] から [CA SDM Server] サービスを選択し、[開始] をクリックします。必要なときにいつでも手動でこのサービスを開始できます。また、ほかの Windows サービスと同様に自動的に開始されるように設定できます。(UNIX) コマンドラインから `pdm_init` を使用します。

1. バックグラウンドサーバを起動します。
2. スタンバイサーバとアプリケーションサーバを(任意の順序で)起動します。

CA SDM サーバのローリング メンテナンスを実行する方法

システム管理者は、CA SDM サーバのローリング メンテナンスを実行します。このメンテナンスは、サーバに対してパッチを適用する場合、または一般的なメンテナンスを実施する場合に実行できます。すべてのサーバに対して、特定の順序でメンテナンスを実行することをお勧めします。このプロセスにより、すべてのサーバが同様の変更で更新され、エンドユーザに対する中断が最小限になるか、または発生しません。サーバに固有の変更については、ほかのすべてのサーバを更新する必要はありません。

重要: 共通の MDB パッチ、または OS またはセキュリティ パッチを適用する前に、すべての CA SDM サーバをシャットダウンする必要があります。このような場合、ユーザ タスクが中断され、すべてのサーバが起動して稼働するまで、CA SDM にアクセスできません。システム管理者には、状況に応じてパッチの適用を計画することをお勧めします。

以下の図は、CA SDM サーバのローリング メンテナンスを実行する推奨プロセスを示しています。

注: 組織の標準に応じて、組織内のローリング メンテナンス プロセスが推奨プロセスとは異なる場合があります。



次の手順に従ってください:

1. [考慮事項を確認します](#) (P. 37)。
2. (新しいバックグラウンドとして昇格させる) スタンバイ サーバを停止します。
3. スタンバイ サーバのローリング メンテナンスを実行します。
4. [スタンバイ サーバとバックグラウンド サーバ間でバージョン管理を抑制します](#) (P. 38)。
5. スタンバイ サーバを起動します。
6. [スタンバイ サーバを新しいバックグラウンドサーバとして昇格させます](#) (P. 38)。
7. 古いバックグラウンドサーバのローリング メンテナンスを実行します。
8. 古いバックグラウンドサーバを起動します。
バックグラウンドサーバを起動すると、スタンバイ サーバになります。
9. その他すべてのスタンバイ サーバのローリング メンテナンスを実行します。
注: スタンバイ サーバを停止し、ローリング メンテナンスを実行して、そのサーバを起動します。
10. [アプリケーション サーバのローリング メンテナンスを実行します](#) (P. 40)。

考慮事項の確認

バックグラウンドサーバからスタンバイサーバへのフェールオーバー時には、以下の点を考慮します。

- 新しいユーザはログインできません。
- すでに接続されているユーザの場合、フェールオーバー中には以下の操作を実行できないため、フェールオーバー後に再試行する必要があります。
 - 添付ファイルを使用したチケットの作成。
 - 添付ファイルのダウンロード。

- ナレッジ ドキュメントの検索。
- 新しいナレッジ ドキュメントのインデックス作成。
- 受信電子メール。
- フェールオーバーが完了するまでトリガされない SLA イベント。

重要: サードパーティ ツールを設定して **CA SDM** サーバの自動フェールオーバーを有効にした場合、定常保守を開始する前にそれを無効にする必要があります。

スタンバイ サーバとバックグラウンド サーバ間でのバージョン管理の抑制

CA SDM のバージョン管理は、すべての CA SDM サーバにわたるシステムのカスタマイズを管理するのに役立ちます。スタンバイ サーバを起動する前に、スタンバイ サーバに対するバージョン管理を抑制したことを確認します。このプロセスにより、スタンバイ サーバはバックグラウンドサーバのシステムのカスタマイズに対してアップグレードされません。バージョン管理を抑制するには、アップグレードしたスタンバイ サーバに対して以下のコマンドを実行します。

```
pdm_server_control -v
```

新しいバックグラウンド サーバとしてのスタンバイ サーバの昇格

バックグラウンドサーバを停止する前に、（アップグレードした）スタンバイ サーバを新しいバックグラウンドサーバとして昇格させます。サポート オートメーション が **CA SDM** でインストールされている場合、バックグラウンドサーバのシャットダウンをアクティブな サポート オートメーション ユーザに通知します。

次の手順に従ってください:

1. バックグラウンドサーバ上で以下のコマンドを実行して、サポート オートメーション を使用しているすべてのアクティブなユーザに作業を保存するよう通知します。

```
sa_server_notifier [-h] | [-q seconds] | [-c]
```

```
-h
```

ヘルプ ページを表示します。

-q seconds

このオプションは、ローカル サーバ（バックグラウンド）に指定された時間間隔内に休止するよう通知します。この間隔は、サーバがオフラインになるまでの秒数です。このオプションは、スタンバイ サーバまたはアプリケーション サーバには使用できません。

-c

このオプションは、以前に送信された休止リクエストをキャンセルします。

サポート オートメーション を使用しているすべてのアクティブなユーザにポップアップ メッセージが表示されます。このメッセージは、ユーザにサーバのシャットダウンと、シャットダウンまでに残された時間について通知します。ユーザは自分の作業を保存し、そのスケジュールされた時間内にログアウトする必要があります。

2. 新しいバックグラウンドサーバとして昇格させるスタンバイ サーバ上で、以下のコマンドを実行します。

```
pdm_server_control - b
```

-b

ローカルのスタンバイ サーバにバックグラウンドサーバになるよう通知します。スタンバイ サーバがすでに実行されている必要があります。このサーバが実行されていない場合は起動されますが、フェールオーバは実行されません。フェールオーバを開始するには、コマンドを再度実行します。

バックグラウンドサーバは自動的にシャットダウンし、スタンバイサーバが新しいバックグラウンドサーバとして昇格されます。この変更は、エンドユーザセッションには影響を与えません。進行中の更新（存在する場合）は保存され、新しいバックグラウンドサーバがオンラインになるまで遅延されます。

アプリケーション サーバのローリング メンテナンスの実行

ベスト プラクティスとして、まず最小限のユーザが接続しているか、ユーザが接続していないアプリケーション サーバのローリング メンテナンスを実行できます。次に、更新されたサーバにログインするために、ほかのアプリケーション サーバ上でアクティブなすべてのユーザに通知します。最後に、ほかのアプリケーション サーバのメンテナンスを実行できます。このプロセスにより、ユーザがアプリケーション サーバ間で複数回移動されないことが保証されます。

次の手順に従ってください:

1. [アクティビティの少ないアプリケーション サーバを選択します](#) (P. 40)。
アプリケーション サーバが、すべての変更で更新されます。
2. アクティビティの少ないアプリケーション サーバを停止し、ローリング メンテナンスを実行して起動します。
アプリケーション サーバが、すべての変更で更新されます。
3. [ほかのアプリケーション サーバを停止します](#) (P. 41)。
アプリケーション サーバのローリング メンテナンスを実行して起動します。
アプリケーション サーバが、すべての変更で更新されます。
4. [ほかのアプリケーション サーバに対して手順 3 および 4 を実行します](#)。
すべてのアプリケーション サーバが、すべての変更で更新されます。

アクティビティの少ないアプリケーション サーバの選択

ユーザ アクティビティが最も少ないアプリケーション サーバを選択します。各アプリケーション サーバに対して以下のコマンドを実行し、アクティブなセッションが最少または存在しないサーバを選択します。

```
pdm_webstat
```

注: このコマンドは、SOAP または REST Web サービス セッションをキャプチャしません。

ほかのアプリケーション サーバの停止

アプリケーション サーバを停止する前に、アプリケーション サーバ上のすべてのアクティブなユーザに対して、アクティビティの少ないアプリケーション サーバに移動するように通知します。アクティビティの少ないアプリケーション サーバにすべてのユーザを移動する前に、そのサーバを再起動したことを確認します。

次の手順に従ってください:

1. (推奨) 停止するアプリケーション サーバ上のすべてのアクティブなサポート オートメーションアナリストに対して、そのセッション情報を持つ CA SDM でチケットを作成するように通知します。このプロセスにより、セッション情報が失われないようになります。たとえば、サポート オートメーションアナリストが、ハードウェアの問題を解決するために顧客とセッション中だとします。このような場合、アプリケーション サーバがシャット ダウンする前に、サポート オートメーションアナリストは、そのセッション情報を使用して CA SDM で問題を作成できます。
2. アプリケーション サーバ上のすべてのアクティブなユーザに対して、再起動したアクティビティの少ないアプリケーション サーバに移動するように、通知（電子メール通知など）を送信します。この通知には、更新されたアプリケーション サーバの詳細を含めることができます。
3. アプリケーション サーバ上で、以下のコマンドを実行します。

```
pdm_server_control [-h] -q interval -s server_name
```

-h

ヘルプ ページを表示します。

-q interval -s server_name

ローカルまたはリモート アプリケーション サーバに指定された時間間隔内に休止するよう通知します。この間隔は、サーバがオフラインになるまでの秒数です。**server_name** なしでこのオプションを使用した場合は、ローカル サーバが休止するよう通知されます。このオプションは、バックグラウンドまたはスタンバイ サーバには使用できません。

アプリケーション サーバ上のすべてのアクティブなユーザにポップアップ メッセージが表示され、サーバのシャットダウンとシャットダウンまでに残された時間が通知されます。ユーザは自分の作業を保存し、その時間内にログアウトする必要があります。アプリケーションサーバは指定された時間の後に停止します。ユーザが自分の作業を再開するには、ほかのアプリケーションサーバにログオンします。サポート オートメーションアナリストはチケットを参照して、それらのユーザの作業を再開できます。

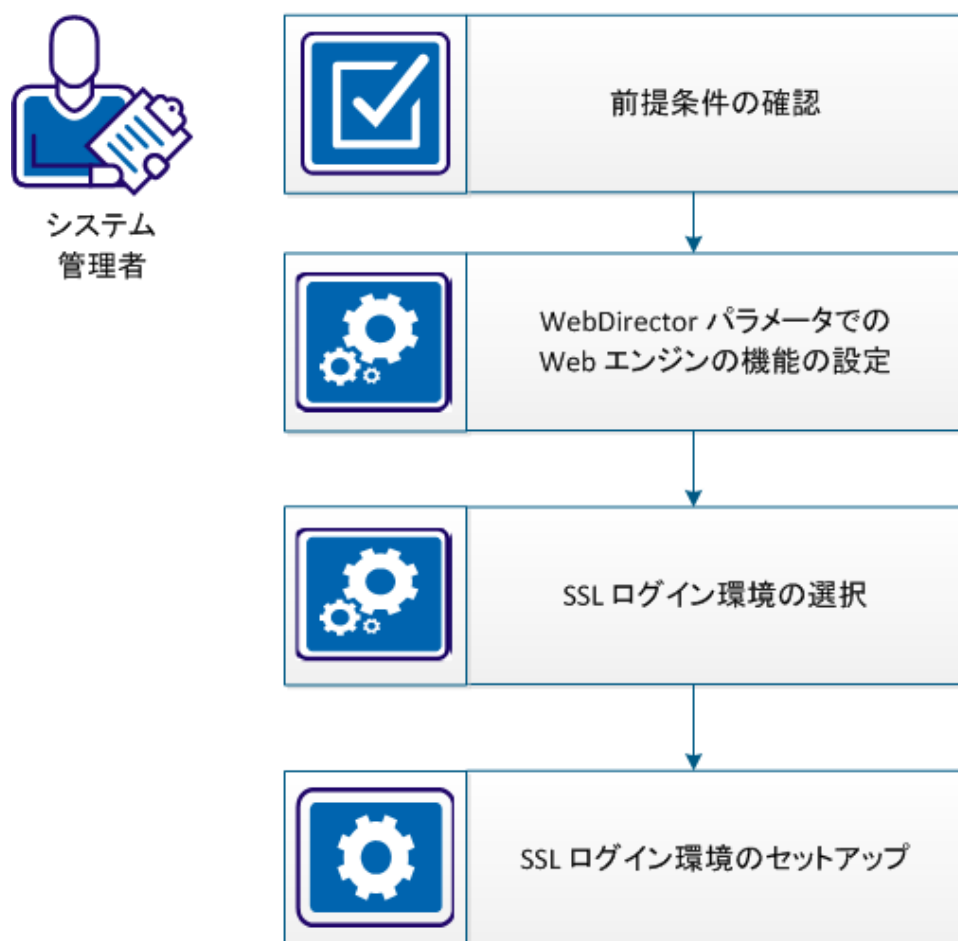
アプリケーション サーバが正常に停止されます。

SSL 認証を設定する方法

システム管理者は、SSL（Secure Socket Layer）プロトコルを使用して、特定の Web エンジンにログインリクエストを送るように WebDirector を設定できます。SSL 認証を設定すると、ログインのセキュリティが強化され、接続のパフォーマンスが向上します。

Equation 1: CA SDM 用の SSL 認証を設定する方法

SSL 認証を設定する方法



関連項目:

[WebDirector パラメータでの Web エンジンの機能の設定](#) (P. 44)

[SSL ログイン環境のセットアップ](#) (P. 48)

[SSL ログイン環境の選択](#) (P. 45)

[前提条件を確認します。](#) (P. 44)

前提条件を確認します。

SSL 設定を行う前に、以下の前提条件を確認します。

- SSL を実装するサーバに CA SDM がインストールおよび設定されている。
- 少なくとも 2 つの Web エンジンが設定および割り当てられており、それらが WebDirector に対して設定および割り当てられている。Web エンジンおよび WebDirector の設定方法の詳細については、CA SDM にサーバプロセスを設定してパフォーマンスを向上させる方法のシナリオを参照してください。

WebDirector パラメータでの Web エンジンの機能の設定

WebDirector を使用するよう Web エンジンを設定した後、Web エンジンは Web クライアント リクエストを処理できます。Web エンジンは、ログイン リクエスト（ログイン以外をいずれかの場所にリダイレクト）、またはログイン以外のリクエスト（ログインをいずれかの場所にリダイレクト）、またはその両方（汎用 Web エンジン）を処理できます。

<Host_Name>-web[#].cfg ファイル内の WebDirector パラメータにより、Web エンジンがどのようにログイン リクエストを処理できるかが決まります。

以下の表に、Web エンジンの役割と WebDirector パラメータ設定の関係を示します。

Web エンジンの機能	'<Host_Name>-web[#].cfg' 'WebDirector' パラメータ設定
ログイン リクエストのサービス	'UseDirector AfterLogin'; 'Willingness 0'
ログイン以外のアクティビティのサービス	'UseDirector BeforeLogin'; 'Willingness [1～10]'
汎用目的	'UseDirector Yes'; 'Willingness [1～10]'

SSL ログイン環境の選択

SSL/非 SSL 混在 Web 環境でターゲットの SSL ログインに対して WebDirector を使用して、特定の SSL Web エンジンへのすべての Web ログイン リクエストをリダイレクトできます。その他のすべてのリクエストは、非 SSL Web エンジンにリダイレクトして処理できます。

以下の SSL ログイン環境から選択します。

- 基本的な負荷分散が行われる非 SSL 環境
- 基本的な負荷分散が行われるグローバル SSL 環境
- オプションの負荷分散が行われる、ログイン ターゲットが定められた非 SSL 環境
- オプションの負荷分散が行われる、SSL ログイン ターゲットが定められた混在環境

基本的な負荷分散が行われる非 SSL 環境

基本的な負荷分散が行われる非 SSL 環境で WebDirector を使用することができます。WebDirector は、各 Web エンジンの willingness 値に従って、すべての Web エンジン間で負荷を分散します。各 Web エンジンには、ログイン リクエストとログイン以外のリクエストを処理することができます。Web クライアントと Web サーバ間の通信には、HTTP プロトコルが使用されます。

WebDirector の制御下にある各 Web エンジンで、Web エンジンの `<Host_Name>-web[#].cfg` ファイル内の WebDirector パラメータを以下のよう
に設定します。

- UseDirector : Yes
- WebDirectorSlumpName : (この値は変更しないでください)
- WillingnessValue : [1~10]
- RedirectingURL : (先頭のプロトコル値は指定しなくてもかまいません。
または、http を指定します)

基本的な負荷分散が行われるグローバル SSL 環境

基本的な負荷分散が行われるグローバル SSL 環境で WebDirector を使用
することができます。WebDirector は、各 Web エンジンの willingness 値に
従って、すべての Web エンジン間で負荷を分散します。各 Web エンジン
は、ログイン リクエストとログイン以外のリクエストを処理することが
できます。Web クライアントと Web サーバ間のすべての通信に HTTPS プ
ロトコルを使用する必要があります。

WebDirector の制御下にある各 Web エンジンで、Web エンジンの
`<Host_Name>-web[#].cfg` ファイル内の WebDirector パラメータを以下のよ
うに設定します。

- UseDirector : Yes
- WebDirectorSlumpName : (この値は変更しないでください)
- WillingnessValue : [1~10]
- RedirectingURL : (先頭のプロトコル値は「https」にする必要がありま
す)

オプションの負荷分散が行われる、ログイン ターゲットが定められた非 SSL 環境

オプションの負荷分散が行われる、ログイン ターゲットが定められた非
SSL 環境で WebDirector を使用することができます。ログイン専用の Web
エンジンは、ログイン リクエストだけを処理します。WebDirector の制御
下にある残りの Web エンジンが、その他のすべてのリクエストを処理し
ます。この設定の場合、ログイン リクエストの処理に伴うすべての負荷
が、指定したログイン専用の Web エンジンに課せられます。Web クライ
アントと Web サーバ間の通信には、HTTP プロトコルが使用されます。

ログイン専用の Web エンジンで、Web エンジンの `<Host_Name>-web[#].cfg` ファイル内の WebDirector パラメータを以下のように設定します。

- UseDirector : AfterLogin
- WebDirectorSlumpName : (この値は変更しないでください)
- WillingnessValue : 0
- RedirectingURL : (先頭のプロトコル値は指定しなくてもかまいません。または、http を指定します)

ログイン以外の Web エンジンで、Web エンジンの `<Host_Name>-web[#].cfg` ファイル内の WebDirector パラメータを以下のように設定します。

- UseDirector : Before Login
- WebDirectorSlumpName : (この値は変更しないでください)
- WillingnessValue : [1~10]
- RedirectingURL : (先頭のプロトコル値は指定しなくてもかまいません。または、http を指定します)

オプションの負荷分散が行われる、SSL ログイン ターゲットが定められた混合環境

オプションの負荷分散が行われる、SSL ログイン ターゲットが定められた SSL/非 SSL 混在 Web 環境で WebDirector を使用することができます。すべての Web ログイン リクエストが SSL Web エンジンにリダイレクトされて処理され、その他のリクエストが非 SSL Web エンジンによって処理されます。Web クライアントと SSL Web エンジン間のすべての通信で HTTPS プロトコルを使用する必要があります。

SSL ログイン環境のセットアップ

SSL をセットアップすることで、Web トランザクションを暗号化して、パスワードなどの重要なデータのセキュリティ保護を最大限に高めることができます。設定タイプに応じて、設定された CA SDM サーバ上で SSL ログイン環境を実装できます。

次の手順に従ってください: :

1. CA SDM の設定に応じて、以下のサーバにログインします。
 - 高可用性: アプリケーション サーバ
 - 標準: プライマリまたはセカンダリ サーバ
2. サーバが SSL 証明書を正常にインポートできたことを確認します。
3. `$NX_ROOT/bopcfg/www/wwwroot` ディレクトリ (サブディレクトリを含む) のコピーを作成し、以下の名前を付けます。

`$NX_ROOT/bopcfg/www/wwwrootsec`

4. Web サーバ用の新しい仮想ディレクトリ `CAisdsec` を追加します。
5. この仮想ディレクトリが以下の物理ディレクトリをポイントするようにします。

`$NX_ROOT/bopcfg/www/wwwrootsec`

6. スクリプトを実行するための `CAisdsec` 仮想ディレクトリの許可が、`CAisd` 仮想ディレクトリの許可と一致していることを確認します。
`CAisdsec` 仮想ディレクトリに SSL を適用します。

注: この例では、`CAisdsec` という名前はユーザが定義したもので、変更が可能です。

7. 変更を保存します。

注: WebDirector は `<Host_Name>-web[#].cfg` ファイルを使用しません。ただし、Web エンジンは一意的な `<Host_Name>-web[#].cfg` ファイルを必要とします。サンプル `web.cfg` ファイルは、設定を実行する間に自動的に生成されます。元の `web.cfg` を、使用するテンプレートファイルとして指定することで、元の `web.cfg` のカスタマイズを新しい Web 環境設定ファイルにインポートすることができます。

8. 以下のファイルをコピーおよび保存します。これらのファイルのバックアップは、元の環境を復元する必要があるときに役立ちます。
 - `$NX_ROOT/pdmconf/pdm_startup.tpl`
 - `$NX_ROOT/pdmconf/pdm_startup`

- `$NX_ROOT/bopcfg/www/web.cfg` ファイル
 - 既存のあらゆる `primary-web[#].cfg` ファイル
 - `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml` および `web.xml.tpl`
 - セカンダリ サーバ設定では、既存のすべての `$NX_ROOT/bopcfg/www/web.cfg` ファイルまたは `<Secondary_Server_Host_Name>-web[#].cfg` ファイルおよび `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*` のバックアップコピーを保存します
9. WebDirector に割り当てられている各 Web エンジンで、ファイルをテキストエディタで表示し、Web エンジンのパラメータ (`<Host_Name>-web[#].cfg 'webdirector'`) が正しく設定されていることを確認します。必要に応じて、Web エンジンのロールを反映するように WebDirector パラメータの値を変更します。次に、`$NX_ROOT/bopcfg/www` ディレクトリにそれらをコピーします。
10. すべての `$NX_ROOT/samples/pdmconf/primary-web[#].cfg` ファイルを `$NX_ROOT/bopcfg/www` ディレクトリに移動します。
- セカンダリ サーバ設定では、すべての `$NX_ROOT/samples/pdmconf/secondary_server_name-web[#].cfg` をプライマリ サーバからセカンダリ サーバの `$NX_ROOT/bopcfg/www` ディレクトリに移動します。
11. Tomcat などのサーブレット サーバについては、CA SDM は、Web エンジンホストする各サーバ上の `web.xml` ファイルを置き換えることが可能な `web.xml` ファイルを作成します。これらのファイルの名前は、`primary-web.xml` です。ファイルの名前を変更し、それらを `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF` ディレクトリにコピーします。
- IIS または Apache などの HTTP サーバの場合は、`pdmweb.exe` ファイルのコピーを `$NX_ROOT/bopcfg/www/wwwroot` ディレクトリに作成し、`pdmweb[#].exe` ファイルを各 Web エンジンに作成し、`pdmweb_d[#].exe` ファイルを設定した各 WebDirector に作成します。`pdmweb[#].exe` と `pdmweb_d[#].exe` の名前が、正しい CGI I/F 値に従っていることを確認します（例：`pdmweb1.exe`、`pdmweb2.exe`、`pdmweb_d1.exe` など）。
12. IIS を使用していて、各 CGI インターフェースのサーバ拡張機能を追加する必要がある場合は、`primary-site.dat` ファイルを `$NX_ROOT/bopcfg/www` ディレクトリに `site.dat` としてコピーします。システムが再設定されたときに、これらのサイトが IIS に追加されます。システムが再構成されると、これらのサイトが IIS に追加されます。

13. データベースを再初期化せずにプライマリ サーバを再設定し、サービスを開始します。
14. 再構成後、現在の設定が有効であることを確認します。CA SDM デーモンを起動します。stdlog ファイルにエラーがないことを確認します。デーモンとそのステータスを表示するには、pdm_status を使用します。
`http://localhost:8080/CAisd/pdmweb.exe` を使用してシステムにアクセスします。
15. ナレッジマネジメント から CA SDM へのインテグレーションで、CA SDM に SSL を適用した場合は、CA SDM の URL プロトコル値を変更する必要があります。
 - a. Knowledge Tools で、[設定マネージャ] - [全般] - [インテグレーション]を選択し、CA SDM の URL プロトコル値を http から https に変更します。
 - b. 保存して終了します。
16. Web ブラウザを開いて CA SDM のログイン ページを表示し、ユーザがログインすることができることと、リダイレクト/ログイン動作が预期したとおりであることを確認します。

SSL ログイン環境の実装

セットアップした SSL ログインを実装するには、WebDirector パラメータ値を変更します。

次の手順に従ってください:

1. セキュリティ保護されたログイン Web エンジンの場合は、<Host_Name>-web[#].cfg を以下のように編集します。
 - a. CAisd パラメータ値を /CAisd から /CAisdsec に変更します。
 - b. WebDirector がパススルー認証を使用する場合は、UseDirector パラメータ値を Yes から AfterLogin に変更します。
 - c. Willingness パラメータ値を 5 から 0 に変更します。
 - d. RedirectingURL 値のプロトコルが https になっていることを確認します。
 - e. RedirectingURL <cgi ディレクトリ> 値を CAisd から CAisdsec に変更します。
 - f. 変更を保存します。
2. その他のすべてのアクティビティを処理するセキュリティ保護されていない Web エンジンについては、<Host_Name>-web[#].cfg ファイルを以下のように編集します。
 - a. CAisd パラメータ値が /CAisd になっていることを確認します。
 - b. UseDirector パラメータ値を Yes から BeforeLogin に変更します。
 - c. Willingness 値を 5 のままにしておくか、必要な負荷重み付けに応じて 1~10 の整数を設定します。
 - d. RedirectingURL 値のプロトコルが http になっていることを確認します。
 - e. RedirectingURL <cgi ディレクトリ> 値が CAisd になっていることを確認します。
 - f. 変更を保存します。

設定の後、Service Desk を再起動します。サービスの再起動後、HTTP を使用して 非 SSL Web エンジンにアクセスすることにより、ログインをテストします。ログインのために、HTTPS でセキュリティ保護された Web エンジンに自動的にリダイレクトされることを確認します。ログインすると、通常の Service Desk アクティビティでは、非 SSL HTTP Web エンジンに自動的にリダイレクトされます。

SSL ログイン環境の確認

Web エンジンの SSL ログイン環境を確認できます。

次の手順に従ってください：

- セキュリティ保護されたログイン Web エンジンは、SSL が適用された仮想ディレクトリにマップされている物理ディレクトリ内にある必要があります（この例では CAisdsec）。

セキュリティ保護されたログイン Web エンジンの場合、
pdmweb.exe のインスタンスを \$NX_ROOT/bopcfg/www/wwwrootsec
ディレクトリに pdmweb[#].exe という名前で作成します。実行可能
ファイルの名前は、各セキュリティ保護されたログイン Web エンジン
の CGI I/F 値に一致する必要があります。

例：セキュリティ保護されたログイン Web エンジンに CGI I/F 値
pdmweb2 を割り当てた場合は、pdmweb.exe の物理コピーを作成し、
名前を pdmweb2.exe に変更します。

- セキュリティ保護されていない Web エンジンと WebDirector は、SSL が適用されていない仮想ディレクトリ CAisd にマップされている物理ディレクトリ内にある必要があります。

セキュリティ保護されていない Web エンジンと WebDirector の場合は、
pdmweb.exe の新しいインスタンスを
\$NX_ROOT/bopcfg/www/wwwroot ディレクトリに作成します。設定さ
れたセキュリティ保護されていない Web エンジンと WebDirector ご
とに pdmweb.exe のコピーが存在している必要があります。実行可能
ファイルの新しい名前が、Web エンジンと WebDirector 用に定義され
ている CGI I/F 値に一致するようにコピーの名前を変更します。

例：セキュリティ保護されていない Web エンジンに CGI I/F 値
pdmweb3 を割り当てていて、WebDirector に値 pdmweb_d1 を割り当て
ている場合は、pdmweb.exe のコピーを 2 つ作成します。最初のコピー
の名前を pdmweb3.exe に変更し、2 番目のコピーの名前を
pdmweb_d1.exe に変更します。

Tomcat サーバ用の SSL ログインのセットアップ

CA SDM 環境の Tomcat サーバで SSL を設定します。

次の手順に従ってください:

1. SSL 証明書を必要とする各 CA SDM サーバでキー ストアを作成するには、以下の手順に従います。

注: キーストアは、証明書用のストアまたはストレージであり、証明書がインポートされた後、Tomcat はそのキーストアおよび SSL 用の証明書を指定して使用します。

- a. C: ドライブ（またはローカル ドライブ）に、`certificates` という名前のディレクトリを作成します。
- b. コマンドラインを使用して、JRE bin ディレクトリ（Service Desk でインストールされた JRE では通常 `/SC/JRE`）に移動します
- c. コマンド「`keytool -genkey -alias tomcat -keyalg RSA -keystore c:/certificates/keystore.jks`」を実行します。
- d. 必要に応じて、フィールドに入力します（後でこの情報が必要になる場合があるため、各フィールドに入力した内容を確実に記録してください）。

C:¥certificates¥ ディレクトリに `keystore.jks` ファイルが作成されます。

2. 各サーバの証明書リクエストを生成します。証明書リクエストを生成するには、以下の手順に従います。
 - a. コマンドラインを使用して、JRE bin ディレクトリ（Service Desk でインストールされた JRE では通常 `/SC/JRE`）に移動します
 - b. コマンド「`keytool -certreq -alias tomcat -keystore c:/certificates/keystore.jks -file servername-certreq.csr`」を実行します
証明書リクエストを生成した各サーバ上の `c:/certificates` ディレクトリに、`.csr` ファイルが作成されます。
 - c. 各サーバに関して、選択したベンダーに `.csr` ファイルを送信します。その後、そのベンダーが、証明書リクエストに基づいて必要とする適切な証明書を生成します。

注: 受信する証明書はそれぞれ異なります。一部のベンダーは、ルート証明書、中間証明書、および認証局証明書などを含む複数の証明書を送信します。ベンダーによって、提供された証明書をキーストアにインポートするための手順は異なります。したがって、証明書の生成に使用した特定のベンダーに対して、Tomcat キーストアへの証明書のインポート方法に関する特定の手順を問い合わせることが重要です。

ベンダーから特定の手順を受け取ったら、それに従って、各サーバ上のキーストアに適切な証明書をインポートすることができます。その手順が完了したら、証明書がインポートされたキーストアを指すように、Service Desk 側の事柄に対して Tomcat を設定できます。

3. テキスト エディタを使用して

¥bopcfg¥www¥CATALINA_BASE¥conf¥server.xml ファイルを開き、以下を見つめます。

```
<!-- <Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="keystoreFile="C:¥Documents and Settings¥user¥.keystore"
keystorePass="password"/> -->
```

4. これらのコードを以下のように変更します。

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="keystoreFile="C:¥certs¥keystore.jks"
keystorePass="password"/>
```

注: 現在 Tomcat の HTTPS/SSL コネクタをコメント化している <!-- タグと --> タグを必ず削除し、最初に生成したキーストアに対して適切なパスおよびパスワードを設定したことを確認してください。

5. server.xml ファイルを保存します。

6. 以下のコマンドを使用して Tomcat を再起動します。

```
pdm_tomcat_nxd - c stop
pdm_tomcat_nxd - c start
```

注: すべての CA SDM サーバを再起動して、Tomcat が再起動されることを確認するようお勧めします。

7. HTTPS プロトコルおよび Tomcat ポートを使用して、ブラウザを開いて Service Desk の URL に移動することにより、Tomcat の SSL 接続をテストします。たとえば、以下の URL を使用します。

`https://servername:8080/CAisd/pdmweb.exe`

Service Desk ログイン画面が開きます。Tomcat で SSL が正常に設定されています。

TCP/IP を設定する方法

1 つ以上のサーバ上で、デフォルトの TCP/IP (TCP Internet Protocol) 設定を変更できます。この設定は、サーバ上でサポートされていない場合、クライアントで強制できません。

TCP/IP 設定は、`$NX_Root` ディレクトリにある `NX.env` ファイルを使用して制御します。このファイルを編集するには、ワードパッドなどのテキストエディタを使用します。以下のオプションによって TCP/IP 設定を制御します。

`NX_PROTOCOL_ONLY=mode`

ここで、*mode* は以下の値のうちの 1 つになります。

IPv4

IPv4 モードでは、システムは IPv4 トラフィックをリッスンする slump プロセスのソケットを開きます。

IPv6

IPv6 モードでは、システムは IPv6 トラフィックをリッスンする slump プロセスのソケットを開きます。

混在

混合モードでは、システムは IPv4 トラフィックと IPv6 トラフィックの両方をリッスンする slump プロセスのソケットを開きます。CA SDM の設定に応じて、以下の状況で混在モードを設定できます。

- 標準：プライマリ サーバとは異なるインターネット プロトコル、または互いに異なるインターネット プロトコルを使用するセカンダリ サーバ。
- 高可用性：バックグラウンドサーバとは異なるインターネット プロトコル、または互いに異なるインターネット プロトコルを使用するアプリケーションサーバ。

注: IPv4 と IPv6 のホストがネットワーク上で共存する場合は、サーバ設定を変更する前に、これらの技術をサポートする適切な移行戦略、ツール、およびメカニズムが整っていることを確認します。

例

```
NX_PROTOCOL_ONLY=ipv4
```

CMDBf Web サービスを展開する方法

CA SDM のインストール後、CMDBf Web サービスを展開できます。

次の手順に従ってください:

1. Web サーバが起動し、実行中であることを確認します。
2. CMDBHOME¥sdk¥websvc¥CMDBF ディレクトリに移動します。
3. deploy_cmdbws.bat を実行します。

CMDBf Web サービスが展開され、起動されます。

注: CMDBf Web サービスの展開の詳細については、「CA CMDB テクニカルリファレンス ガイド」を参照してください。

CA SDM サーバを再起動する方法

CA SDM の設定に応じて、以下を実行します。

- [標準設定で CA SDM サーバを再起動します](#) (P. 57)。
- [高可用性設定で CA SDM サーバを再起動します](#) (P. 57)。

標準設定での CA SDM サーバの再起動

標準設定では、以下の順序でサーバを再起動します。

注: サーバを再起動するには、[スタート] - [設定] - [コントロールパネル] - [管理ツール] - [サービス] をクリックします。[CA SDM Server] を右クリックし、[開始] を選択します。

1. セカンダリ サーバを再起動します。
2. プライマリ サーバを再起動します。

高可用性設定での CA SDM サーバの再起動

高可用性設定では、以下の順序で CA SDM サーバを再起動することを推奨します。

注: サーバを再起動するには、[スタート] - [設定] - [コントロールパネル] - [管理ツール] - [サービス] をクリックします。[CA SDM Server] を右クリックし、[開始] を選択します。

1. すべてのスタンバイ サーバを再起動します。
2. [スタンバイ サーバを新しいバックグラウンドサーバとして昇格させます](#) (P. 38)。
3. 古いバックグラウンドサーバを起動します。
バックグラウンドサーバを起動すると、スタンバイ サーバになります。
4. [アクティビティの少ないアプリケーション サーバを選択します](#) (P. 40)。
5. アクティビティの少ないアプリケーション サーバを再起動します。

6. [ほかのアプリケーション サーバを停止します](#) (P. 41)。
7. アプリケーション サーバを起動します。
- 8.ほかのアプリケーション サーバに対して手順 6 および 7 を実行します。

新しいバックグラウンド サーバとしてのスタンバイ サーバの昇格

バックグラウンド サーバを停止する前に、(アップグレードした) スタンバイ サーバを新しいバックグラウンド サーバとして昇格させます。サポート オートメーション が CA SDM でインストールされている場合、バックグラウンド サーバのシャットダウンをアクティブな サポート オートメーション ユーザに通知します。

次の手順に従ってください:

1. バックグラウンド サーバ上で以下のコマンドを実行して、サポート オートメーション を使用しているすべてのアクティブなユーザに作業を保存するよう通知します。

```
sa_server_notifier [-h] | [-q seconds] | [-c]
```

-h

ヘルプ ページを表示します。

-q seconds

このオプションは、ローカル サーバ (バックグラウンド) に指定された時間間隔内に休止するよう通知します。この間隔は、サーバがオフラインになるまでの秒数です。このオプションは、スタンバイ サーバまたはアプリケーション サーバには使用できません。

-c

このオプションは、以前に送信された休止リクエストをキャンセルします。

サポート オートメーション を使用しているすべてのアクティブなユーザにポップアップ メッセージが表示されます。このメッセージは、ユーザにサーバのシャットダウンと、シャットダウンまでに残された時間について通知します。ユーザは自分の作業を保存し、そのスケジュールされた時間内にログアウトする必要があります。

2. 新しいバックグラウンドサーバとして昇格させるスタンバイ サーバ上で、以下のコマンドを実行します。

```
pdm_server_control -b
```

```
-b
```

ローカルのスタンバイ サーバにバックグラウンドサーバになるよう通知します。スタンバイ サーバがすでに実行されている必要があります。このサーバが実行されていない場合は起動されますが、フェールオーバーは実行されません。フェールオーバーを開始するには、コマンドを再度実行します。

バックグラウンドサーバは自動的にシャットダウンし、スタンバイサーバが新しいバックグラウンドサーバとして昇格されます。この変更は、エンドユーザセッションには影響を与えません。進行中の更新（存在する場合）は保存され、新しいバックグラウンドサーバがオンラインになるまで遅延されます。

アクティビティの少ないアプリケーション サーバの選択

ユーザ アクティビティが最も少ないアプリケーション サーバを選択します。各アプリケーション サーバに対して以下のコマンドを実行し、アクティブなセッションが最少または存在しないサーバを選択します。

```
pdm_webstat
```

注: このコマンドは、SOAP または REST Web サービス セッションをキャプチャしません。

ほかのアプリケーション サーバの停止

アプリケーション サーバを停止する前に、アプリケーション サーバ上のすべてのアクティブなユーザに対して、アクティビティの少ないアプリケーション サーバに移動するように通知します。アクティビティの少ないアプリケーション サーバにすべてのユーザを移動する前に、そのサーバを再起動したことを確認します。

次の手順に従ってください:

1. (推奨) 停止するアプリケーション サーバ上のすべてのアクティブなサポート オートメーション アナリストに対して、そのセッション情報を持つ **CA SDM** でチケットを作成するように通知します。このプロセスにより、セッション情報が失われないようになります。たとえば、サポート オートメーション アナリストが、ハードウェアの問題を解決するために顧客とセッション中だとします。このような場合、アプリケーション サーバがシャット ダウンする前に、サポート オートメーション アナリストは、そのセッション情報を使用して **CA SDM** で問題を作成できます。
2. アプリケーション サーバ上のすべてのアクティブなユーザに対して、再起動したアクティビティの少ないアプリケーション サーバに移動するように、通知（電子メール通知など）を送信します。この通知には、更新されたアプリケーション サーバの詳細を含めることができます。
3. アプリケーション サーバ上で、以下のコマンドを実行します。

```
pdm_server_control [-h] -q interval -s server_name
```

-h

ヘルプ ページを表示します。

-q interval -s server_name

ローカルまたはリモート アプリケーション サーバに指定された時間間隔内に休止するよう通知します。この間隔は、サーバがオフラインになるまでの秒数です。**server_name** なしでこのオプションを使用した場合は、ローカル サーバが休止するよう通知されます。このオプションは、バックグラウンドまたはスタンバイ サーバには使用できません。

アプリケーション サーバ上のすべてのアクティブなユーザにポップアップメッセージが表示され、サーバのシャットダウンとシャットダウンまでに残された時間が通知されます。ユーザは自分の作業を保存し、その時間内にログアウトする必要があります。アプリケーション サーバは指定された時間の後に停止します。ユーザが自分の作業を再開するには、ほかのアプリケーション サーバにログオンします。サポート オートメーション アナリストはチケットを参照して、それらのユーザの作業を再開できます。

アプリケーション サーバが正常に停止されます。

CA SDM サーバを停止する方法

CA SDM の設定に応じて、以下のいずれかのアクションを実行します。

- [標準設定で CA SDM サーバを停止します](#) (P. 61)。
- [高可用性設定で CA SDM サーバを停止します](#) (P. 62)。

標準設定での CA SDM サーバの停止

以下のサーバを停止します。

- [プライマリ サーバを停止します](#) (P. 61)。
- [セカンダリ サーバを停止します](#) (P. 62)。

(標準設定)プライマリ サーバの停止

Windows または UNIX 環境でプライマリ サーバを停止できます。

(Windows) 以下の手順に従います。

1. [コントロール パネル] から [サービス] を選択します。
[サービス] ウィンドウが開きます。
2. [CA Service Desk Manager Server] サービスを選択し、[停止] をクリックします。

プライマリ サーバが停止します。セカンダリ サーバ上のプロセスまたはデーモンも停止されます。

(UNIX) 以下の手順に従います。

- コマンド プロンプトで以下のコマンドを入力します。

```
pdm_halt
```

プライマリ サーバが停止します。セカンダリ サーバ上のプロセスまたはデーモンも停止されます。

(標準設定)セカンダリ サーバの停止

Windows または UNIX 環境でセカンダリ サーバを停止できます。

(Windows) 以下の手順に従います。

1. [コントロール パネル] から [サービス] を選択します。
[サービス] ウィンドウが開きます。
2. [CA Service Desk Manager Remote Proctor] サービスを選択し、[停止] をクリックします。
セカンダリ サーバが停止します。

(UNIX) 以下の手順に従います。

- コマンド プロンプトで以下のコマンドを入力します。
`pdm_halt`
セカンダリ サーバが停止します。

高可用性設定での CA SDM サーバの停止

以下のサーバを停止します。

- [スタンバイ サーバを停止します](#) (P. 62)。
- [バックグラウンド サーバを停止します](#) (P. 63)。
- [アプリケーション サーバを再起動します](#) (P. 64)。

(高可用性設定)スタンバイ サーバの停止

Windows または UNIX 環境でスタンバイ サーバを停止できます。

(Windows) 以下の手順に従います。

1. [コントロール パネル] から [サービス] を選択します。
[サービス] ウィンドウが開きます。

2. [CA Service Desk Manager Server] サービスを選択し、[停止] をクリックします。

スタンバイ サーバが停止します。

(UNIX) 以下の手順に従います。

- コマンドプロンプトで以下のコマンドを入力します。

```
pdm_halt
```

スタンバイ サーバが停止します。

(高可用性設定)バックグラウンド サーバの停止

バックグラウンド サーバを停止する前に、(アップグレードした) スタンバイ サーバを新しいバックグラウンド サーバとして昇格させます。サポート オートメーション が CA SDM でインストールされている場合、バックグラウンドサーバのシャットダウンをアクティブな サポート オートメーション ユーザに通知します。

次の手順に従ってください:

1. バックグラウンド サーバ上で以下のコマンドを実行して、サポート オートメーション を使用しているすべてのアクティブなユーザに作業を保存するよう通知します。

```
sa_server_notifier [-h] | [-q seconds] | [-c]
```

-h

ヘルプ ページを表示します。

-q seconds

このオプションは、ローカル サーバ (バックグラウンド) に指定された時間間隔内に休止するよう通知します。この間隔は、サーバがオフラインになるまでの秒数です。このオプションは、スタンバイ サーバまたはアプリケーション サーバには使用できません。

-c

このオプションは、以前に送信された休止リクエストをキャンセルします。

サポート オートメーション を使用しているすべてのアクティブなユーザにポップアップメッセージが表示されます。このメッセージは、ユーザにサーバのシャットダウンと、シャットダウンまでに残された時間について通知します。ユーザは自分の作業を保存し、そのスケジュールされた時間内にログアウトする必要があります。

2. 新しいバックグラウンドサーバとして昇格させるスタンバイ サーバ上で、以下のコマンドを実行します。

```
pdm_server_control -b
```

-b

ローカルのスタンバイ サーバにバックグラウンドサーバになるよう通知します。スタンバイ サーバがすでに実行されている必要があります。このサーバが実行されていない場合は起動されますが、フェールオーバーは実行されません。フェールオーバーを開始するには、コマンドを再度実行します。

バックグラウンドサーバは自動的にシャットダウンし、スタンバイサーバが新しいバックグラウンドサーバとして昇格されます。この変更は、エンドユーザセッションには影響を与えません。進行中の更新（存在する場合）は保存され、新しいバックグラウンドサーバがオンラインになるまで遅延されます。

（高可用性設定）アプリケーション サーバの停止

アプリケーション サーバを停止する前に、すべてのアクティブなユーザに対して、別のアプリケーション サーバに移動するよう通知する必要があります。

次の手順に従ってください：

1. 停止するアプリケーション サーバ上のすべてのアクティブなユーザに対して、別のアプリケーション サーバに移動するよう通知を送信します。この通知には、ほかのアプリケーション サーバの詳細を含めることができます。たとえば、電子メール通知を送信できます。

2. 停止するアプリケーション サーバ上で以下のコマンドを実行します。

```
pdm_server_control -q interval -s server_name
```

-q interval -s server_name

ローカルまたはリモート アプリケーション サーバに指定された時間間隔内に休止するよう通知します。この間隔は、サーバがオフラインになるまでの秒数です。**server_name** を指定せずにこのオプションを使用すると、ローカル サーバに休止するよう通知されます。このオプションは、バックグラウンドまたはスタンバイサーバには使用できません。

アプリケーション サーバ上のすべてのアクティブなユーザにポップアップメッセージが表示されます。このメッセージは、ユーザにサーバのシャットダウンと、シャットダウンまでに残された時間について通知します。ユーザは自分の作業を保存し、その時間内にログアウトする必要があります。アプリケーション サーバは指定された時間の後に停止します。ユーザが自分の作業を再開するには、ほかのアプリケーション サーバにログオンします。

(推奨) アクティブなサポート オートメーション アナリストは、自分のセッションに関連するチケットを作成して、その作業を保存できます。ほかのアプリケーション サーバにログインし、このチケットを参照して作業を再開できます。

タブレットのサポート

Apple iPad でデフォルトのブラウザを使用した場合、アナリスト インターフェイス、従業員セルフサービス、顧客セルフサービス、およびベンダーセルフサービスの限られた機能のみが表示されます。CA SDM は、タブレットでの添付ファイルの使用をサポートしていません。

注: PDA アナリスト インターフェイスは、他のすべてのタブレットで表示されます。iPad の場合、Safari ブラウザを使用すると CA SDM のすべてのユーザ インターフェイスがサポートされます。iPad で他のブラウザを使用した場合に、すべてのユーザ インターフェイスが表示される場合がありますが、それらの機能はサポートされていません。

Tomcat ロギング

CA SDM は、サーブレットや PDM_RPC などの Web コンポーネント用に個別の `log4j.properties` ファイルを使用します。サポートオートメーション、CMDB Visualizer および REST にも個別の `log4j.properties` ファイルがあります。Tomcat ロギングを開始または停止するために、Tomcat デーモンをリサイクルする必要はありません。

以下のリストでは、CA SDM コンポーネントの `log4j.properties` ファイルの相違点について説明します。

- CA SDM は、`NX_ROOT¥site¥cfg` および `NX_ROOT¥bopcfg¥www¥CATALINA_BASE¥webapps¥CAisd¥WEB-INF` 内にある `log4j.properties` の変更を監視します。
- サポートオートメーションは、`NX_ROOT¥bopcfg¥www¥CATALINA_BASE_SA¥webapps¥SupportAutomation¥WEB-INF` 内にある `log4j.properties` を監視します。
- CMDB Visualizer は、`NX_ROOT¥bopcfg¥www¥CATALINA_BASE_VIZ¥webapps¥CMDBVisualizer¥WEB-INF¥classes` 内にある `cmdbvisualizerlogging.properties` を監視します。
- REST は、`NX_ROOT¥site¥cfg` 内にある `rest.log4j.properties` を監視します。

`pdm_log4j_config` ユーティリティは、`log4j.properties`、`cmdbvisualizerlogging.properties` および `rest.log4j.properties` ファイル内の変数を変更する場合にのみ使用してください。`pdm_log4j_config` ユーティリティを使用して、ポーリング間隔を変更することはできません。

CA SDM は、`log4j` プロパティ ファイルの変更を定期的にチェックします。時間間隔は、`NX.env` ファイル内の `NX_LOG4J_REFRESH_INTERVAL` 変数を変更して設定します。

サーブレットのデフォルト値

以下のサーブレットは、デフォルトでは **INFO** レベルのメッセージを `jsrvr.log` ファイルにログ記録します。

- **PDMContextListener** -- サービスのスタートアップおよびシャットダウン中にログ エントリを生成します。
- **PDMweb** -- ユーザ インターフェースの操作を元にログ エントリを生成します。
- **UploadServlet** -- チケットにファイルを添付すると、ログ エントリを生成します。
- **pdmExport** -- リスト フォーム上で [エクスポート] をクリックすると、ログ エントリを生成します。
- **pdm_report** -- リスト フォーム上で [レポート] メニューをクリックすると、ログ エントリを生成します。
- **page_cache** -- ユーザ インターフェースの操作を元にログ エントリを生成します。
- **ProcessServlet** -- **CA Workflow** をインストールし、**CA Workflow** タスクにアクセスすると、ログ エントリを生成します。

注: これらのアクションにより、**pdm_rpc** デーモンもログ エントリを生成します。
- **BOServlet** -- **CA Business Intelligence** を設定し、[レポート] タブをクリックすると、ログ エントリを生成します。

PDA インターフェース

CA SDM では、PDA (Personal Digital Assistant) インターフェース用に ITIL 用語がサポートされます。エンドユーザはこのインターフェースを使用して、リクエスト、インシデント、および問題を作成できます。また、以下のチケットタイプを検索できます。

- インシデント
- 問題
- リクエスト
- 変更要求
- 案件

アナリストは PDA インターフェースを使用できます。このインターフェースは、連絡先のアクセスタイプの [PDA 役割] フィールドに存在する役割を遵守します。

PDA インターフェースは、サポート対象外のすべてのデバイスおよびブラウザで表示されます。

連絡先検索用のルックアップ サービスは、複数のタブおよび複数のブラウザ ウィンドウをサポートする PDA ブラウザ上でのみ動作します。マルチテナンシーはブラウザ インターフェースと同様に動作しますが、マルチテナンシー選択用のドロップダウン リストは提供されません。チケットを作成する場合、テナンシーは依頼者、影響を受けるエンドユーザ、およびアナリストに基づきます。

Automatic Priority Calculator (APC) は、属性、緊急度、影響、リクエスト領域、および影響を受けるエンドユーザに基づいて、インシデント/問題の作成時に優先度を決定するのに役立ちます。

注: アスタリスクは必須フィールドを示します。たとえば、リクエストを作成する場合、[影響を受けるエンドユーザ] と [優先度] を指定します。チケットを作成する際、PDA インターフェースでは添付ファイルはサポートされていません。

REST ロギング

REST は `pdm_rest_util.jar` および `rest-core.jar` パッケージを使用します。これには、`log4j` ロギング サポートが含まれています。これらのコンポーネントは、標準ログ (`stdlog.*`) にはメッセージを書き込みませんが、`log4j` コンポーネントを介して書き込みが行われます。デフォルトでは、これらのパッケージは、**INFO**、**ERROR** および **WARN** メッセージをログ記録します。Java パッケージは同じ `log4j` 設定プロパティ ファイルを使用するため、各々は同じ出力ファイルにメッセージをログ記録します。
`$NX_ROOT¥site¥cfg¥` ディレクトリ内の `rest.log4j.properties` ファイルを表示します。

トレースまたはデバッグ用にログ レベルを増加させるには、`rest.log4j.properties` ファイル内の以下のセクションを更新します。

```
log4j.rootCategory=debug, jrestlog
```

以下のディレクトリの設定プロパティ ファイルに定義されている出力ファイルを見つけます。

```
$NX_ROOT¥log¥jrest.log
```

CXF ロギングの有効化

実稼働環境でのパフォーマンスに影響するため、CA SDM のデフォルト設定では、CXF ロギングは無効化されています。ユーザの環境でデバッグ用にロギングが必要な場合、管理者は `beans.xml` ファイルを変更して、CXF ロギングを有効化できます。

次の手順に従ってください:

1. 以下のディレクトリで `beans.xml` ファイルを見つけます。

```
NX_ROOT¥bopcfg¥www¥CATALINA_BASE_REST¥webapps¥caisd-rest¥WEB-INF
```

2. XML ファイル内の以下のセクションを見つけます。

```
<cxf:bus>
  <cxf:features>
  </cxf:features>
</cxf:bus>
```

3. 以下の例のようにセクションに `<cxf:logging/>` を追加します。

```
<cxf:bus>
  <cxf:features>
    <cxf:logging/>
  </cxf:features>
</cxf:bus>
```

4. XML ファイルを保存します。

ITIL 設定

IT インフラストラクチャ ライブラリ (ITIL) は、コンピュータ データ センター管理のベスト プラクティスを集めたものです。ITIL フレームワークの主な利点は、推奨プロセスを規定するだけでなく、通常使用されているデータ センター技術を正確に定義する点です。IT 業界では、同じ語が別のことを意味するのに使用されたり、人によってそれぞれに特別な意味合いを持たせた独特の語が用いられる場合がしばしばあります。ITIL は、この問題を回避するのに役立ちます。

以下のチケットタイプが使用可能です。

- リクエスト
- 変更要求
- 案件
- インシデント
- 問題

重要: CA SDM でサポートされるのは、ITIL インターフェースのみです。ITIL インターフェースでは、製品の以前の非 ITIL バージョンでは使用されていなかったデータ オブジェクト（問題チケットやインシデント チケットなど）がサポートされます。

ITIL は以下の作業を実行します。

- CA SDM インストールの ITIL インターフェースの生成
- CA SDM のデータベース、フォーム、およびフィールドの、標準的なインストールとは異なる ITIL の規則への準拠

重要: 既存のシステムをアップグレードする場合、データベース テーブルおよびデータを保持するために "デフォルト データのロード" チェック ボックスをオフにしてください。オフにしない場合、既存のデータがすべて失われます。非 ITIL 環境からのマイグレーションの詳細については、「実装ガイド」を参照してください。

ITIL サービス基準

ITIL では、複数の基準のベスト プラクティス が示されます。サービス サポート 基準とサービス デリバリー 基準を組み合わせることで、組織のサービス 管理能力が確立されます。サービス 管理の 10 の基準の間にある複雑な相互関係が相互に作用して、IT インフラストラクチャによって高レベルのサービスがビジネスに提供されることが保証されます。

サービス サポートには、以下の基準があります。

- インシデント管理
- 問題管理
- 変更管理
- リリース管理
- 環境設定管理

CA SDM は、特にインシデント管理、問題管理、変更管理、および環境設定管理に対応しています。

サービス デリバリーには、以下の基準があります。

- サービス管理
- 可用性管理
- キャパシティ管理
- IT サービス財務管理
- IT サービス継続性管理

CA SDM は、特にサービス管理に対応しています。

従業員用インターフェース オプションとゲスト用インターフェース オプション

CA SDM を使用すると、従業員とゲストに別々のインターフェースを設定できます。これらの別々のインターフェースは、[管理] タブの [オプション マネージャ] で設定します。これらのインターフェースは、以下の値によって制御されます。

employee_intf_incident_support

以下の値が表示されます。

- リクエストのみ
- インシデントのみ
- インシデントとリクエストの両方

guest_intf_incident_support

以下の値が表示されます。

- リクエストのみ
- インシデントのみ
- インシデントとリクエストの両方

重要: これが新規インストールである場合、ITIL はデフォルトで [インシデントのみ] に設定された値で設定されています。以前の非 ITIL の設定からマイグレートしている場合、オプションはインストールされますが、値は [リクエストのみ] に設定されます。

従業員用インターフェースの構成

インシデント、リクエスト、またはその両方を表示する従業員用インターフェースを構成できます。

従業員用インターフェースを構成するには

1. [管理] タブをクリックします。
[管理] コンソールが表示されます。
2. [オプション マネージャ] - [リクエスト マネージャ] をクリックします。
[オプション リスト] が表示されます。

3. [employee_intf_incident_support] をクリックします。
[オプションの詳細] ページが表示されます。
4. [オプション値] フィールドを以下のいずれかの値に変更します。

インシデントのみ

(ITIL のデフォルト) 従業員用インターフェースにインシデント チケット タイプのみを表示します。

リクエストのみ

従業員用インターフェースにリクエスト チケット タイプのみを表示します。

インシデントとリクエストの両方

従業員用インターフェースにインシデント チケット タイプとリクエスト チケット タイプの両方を表示します。

[保存] をクリックします。

5. [更新] をクリックして選択内容を確認します。
[オプションの詳細] が更新されます。
6. [オプションの詳細] を閉じます。
[オプション リスト] が表示されます。

ゲスト用インターフェースの構成

インシデント、リクエスト、またはその両方を表示するゲスト用インターフェースを構成できます。

ゲスト用インターフェースを構成するには

1. [管理] タブをクリックします。
[管理] コンソールが表示されます。
2. [オプション マネージャ] - [リクエスト マネージャ] をクリックします。
[オプション リスト] が表示されます。
3. [guest_intf_incident_support] をクリックします。
[オプションの詳細] ページが表示されます。

4. [オプション値] フィールドを以下のいずれかの値に変更します。

インシデントのみ

(デフォルト) ゲスト用インターフェースにインシデント チケット タイプのみを表示します。

リクエストのみ

ゲスト用インターフェースにリクエスト チケット タイプのみを表示します。

インシデントとリクエストの両方

ゲスト用インターフェースにインシデント チケット タイプとリクエスト チケット タイプの両方を表示します。

[保存] をクリックします。

5. [更新] をクリックして選択内容を確認します。

[オプションの詳細] が更新されます。

6. [オプションの詳細] を閉じます。

[オプション リスト] が表示されます。

アクティビティ ログのセキュリティ

[アクティビティ ログ] セキュリティ オプションを使用すると、エンドユーザがアクティビティ ログでフィールドを更新できないようにすることができます。内部オプションを選択して、カスタマがログを表示できないようにすることができます。

アクティビティ ログのセキュリティは、以下のチケット タイプのアクティビティ ログに影響を与えます。

- リクエスト
- 変更要求
- 案件
- インシデント
- 問題

アクティビティ ログのセキュリティの有効化

アクティビティ ログのセキュリティは、[管理] タブのオプション マネージャから有効にすることができます。

アクティビティ ログのセキュリティを有効化にする方法

1. [管理] タブをクリックします。
[管理] コンソールが表示されます。
2. [オプション マネージャ] - [リクエスト - 変更 - 案件] をクリックします。
[オプション リスト] が表示されます。
3. [activity_log_security] をクリックします。
[オプションの詳細] ページが表示されます。
4. [編集] をクリックして、以下のオプション値のいずれかを選択します。

編集可

(デフォルト) アクティビティ ログのすべてのフィールドを、Web インターフェースまたは Web サービスを通して編集できるようにします。

書き込み保護

アクティビティ ログを読み取り専用で表示します。内部オプションを選択した場合、内部ユーザのみがログを編集でき、顧客は表示できません。

注: セキュリティ オプションが有効な場合、Web インターフェース、または Web サービスなどの外部ソースを通してログを編集しようとした場合、アクティビティ ログは読み取り専用であることを示すエラー メッセージが表示されます。

[保存] をクリックします。

5. [更新] をクリックして選択内容を確認します。ウィンドウを閉じます。

アクティビティ ログのセキュリティが有効になります。

重要: [activity_log_security] オプションはアンインストールできません。
[オプション マネージャ] - [リクエスト - 変更 - 案件] で、オプションの値を [編集可] または [書き込み保護] に変更することのみが可能です。

Web スクリーン ペインタへの影響

アクティビティ ログのセキュリティ機能 \$NX_ACTIVITY_LOG_SECURITY には、majic 内の alg、chgalg、issalg オブジェクトの以下の属性 (time_spent、time_stamp、および description) が含まれています。

例: cm.maj 内のオブジェクト alg の \$NX_ACTIVITY_LOG_SECURITY

この例では、cm.maj 内のオブジェクト alg について、\$NX_ACTIVITY_LOG_SECURITY が 3 つの属性に表示されています。

```
time_spent DURATION $NX_ACTIVITY_LOG_SECURITY {ON_POST_VAL  
update_cr_timespent( call_req_id ) 50 ;  
} ;  
time_stamp DATE $NX_ACTIVITY_LOG_SECURITYÂ Â Â { ON_NEW DEFAULT NOW ; } ;  
descriptionÂ Â Â Â STRING Â Â Â $NX_ACTIVITY_LOG_SECURITY;
```

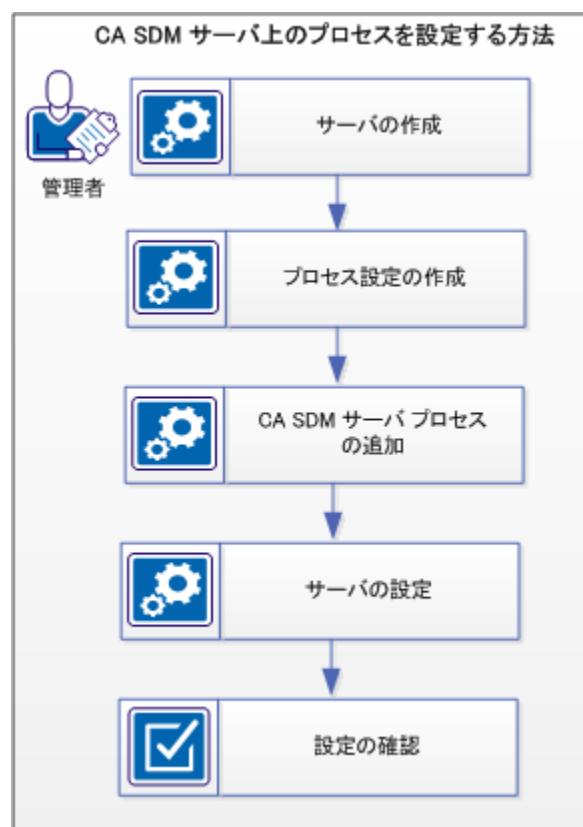
Web Screen Painter で、キーワードの値が WRITE_NEW と評価された場合、
[新規レコードのみ更新可能] フィールドは無効です。

注: Web Screen Painter の詳細については、「実装ガイド」を参照してください。

CA SDM サーバのプロセスを設定する方法

管理者は、CA SDM サーバのパフォーマンスを向上させるために、プロセスおよびデーモンを追加または変更できます。環境内のオブジェクトマネージャ、Web エンジン、WebDirector、および CA SDM サーバのその他のプロセスを設定できます。複数のサーバにわたってプロセスを追加すると、ボリュームやパフォーマンスを向上させたり、セキュリティを強化したりすることができます。

以下の図では、CA SDM サーバ上でプロセスを設定する方法を示します。



次の手順に従ってください:

1. [サーバを作成します](#) (P. 81)。
2. [プロセス設定を作成します](#) (P. 83)。
3. [CA SDM サーバプロセスを追加します](#) (P. 84)。

4. サーバを設定します。サーバの設定方法の詳細については、「**CA SDM サーバの設定方法**」シナリオまたは「**実装ガイド**」を参照してください。
5. [設定を確認します](#) (P. 100)。

サーバの追加

既存のサーバが存在しない場合、CA SDM 展開にインストールするすべてのサーバのサーバレコードを追加します。

次の手順に従ってください:

1. CA SDM の設定に応じて、以下のサーバにログインします。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンドサーバ
2. [管理] タブで、[システム] - [サーバ] を選択します。
[サーバリスト] ページが開きます。
3. CA SDM 構成に応じて、[新規作成] をクリックして以下のサーバのサーバレコードを追加します。
 - 標準: セカンダリ サーバ
 - 高可用性: アプリケーション サーバまたはスタンバイ サーバ[サーバの新規作成] ページが開きます。
4. サーバに応じて、サーバの各フィールドに入力します。
5. [保存] をクリックします。
サーバの詳細を追加しました。

サーバフィールドの作成

サーバを作成すると、以下のフィールドが表示されます。

ホスト名

サーバのローカル ホスト名を指定します。ローカル ホスト名は、`usp_servers` テーブル内の `local_host` 列に格納されます。

重要: `usp_server` テーブルにホスト名が大文字と小文字を区別して入力されていることを確認します。

タイムゾーン

サーバが存在するタイムゾーンを指定します。[エンドユーザのタイムゾーンを使用] オプションがオフの場合、またはサービスタイプにタイムゾーンが指定されていない場合は、このタイムゾーンがシステムのイベントのトリガに使用されます。

レコードステータス

サーバの状態を示します。[アクティブ] のステータスは、サーバが CA SDM 環境に含まれていることを示します。

重要: 非アクティブなサーバが存在する場合、そのサーバ上で CA SDM サービスを開始しないようお勧めします。このアクションにより、予期しない動作が発生する場合があります。

サーバタイプ

設定するサーバのタイプを指定します。お使いの CA SDM 設定に応じて、以下のサーバタイプを選択できます。

- 高可用性：アプリケーションサーバまたはスタンバイサーバ
- 標準：セカンダリサーバ

設定済み

高可用性設定にのみ使用できます。設定されたサーバの状態を示します。このフィールドのデフォルト値は [いいえ] です。そのサーバで正常に `pdm_configure` を実行した後、値は [はい] に更新されます。サーバレコードの自動的に入力されたフィールド値のいずれかを編集すると、[設定済み] フィールドが [いいえ] に変わります。

プロセス設定の作成

CA SDM インストール用のプロセス設定を作成するか、要件に適合するように既存の設定を変更できます。

プロセス設定の作成では、以下の点を考慮します。

- 従来の設定では、セカンダリ サーバ用ではなく、プライマリ サーバ用の設定を作成します。すべてのセカンダリ サーバ設定の詳細は、プライマリ サーバ用に作成された設定に含まれている必要があります。たとえば、セカンダリ サーバ ホスト名の詳細を持つ **Web エンジン** を追加するには、プライマリ サーバ用の設定を開き、必要な詳細を追加します。
- 高可用性設定タイプについては、特定のサーバに対してのみ設定を作成できます。バックグラウンドサーバとスタンバイ サーバに対して、同じ設定を作成してください。

次の手順に従ってください:

1. [管理] タブで、[システム] - [構成] を選択します。
[構成リスト] ページが開きます。
2. [新規作成] をクリックして、サーバ設定を追加します。
[構成の新規作成] ページが開きます。
3. 以下のフィールドを指定します。

重要: 任意のローカライズ言語のすべての入力フィールドには、英文字のみを入力してください。

構成名

作成する設定に割り当てる名前を指定します。

高可用性

標準設定または高可用性設定タイプに対して設定が作成されるかどうかを示します。設定が高可用性設定タイプに対して有効な場合は、[はい] を選択します。

注: いずれかの設定タイプ（高可用性または標準）に対して作成される設定は、もう一方の設定タイプに対しては実装できません。

ホスト名

設定のホスト名を指定します。ホスト名は、[サーバ] ページで設定されたサーバレコードから取ります。[検索] ボタンをクリックして、CA SDM インストールに追加されたサーバを検索できます。

レコードステータス

サーバ設定レコードがアクティブかどうかを指定します。

現在の設定

選択した CA SDM サーバ上で設定が適用されることを示します。このフィールドは読み取り専用であり、サーバ設定ユーティリティ (pdm_configure) の実行時に選択する設定に基づいて更新されます。

4. [保存] をクリックします。

設定が保存されます。設定を保存した後、オブジェクト マネージャ、Web エンジン、WebDirector およびその他のプロセスを追加する新しいタブが、ページ上で有効になります。

注: 設定を保存すると、[ホスト名] および [高可用性] フィールドは読み取り専用になります。

[構成リスト] ページの [リスト内で編集] をクリックし、プロセス設定のレコードステータスを変更します。

注: 選択されたサーバの現在の設定が使用中の場合、レコードステータスを変更できません。

CA SDM サーバプロセスの追加

環境内のオブジェクト マネージャ、Web エンジン、WebDirector、および CA SDM サーバのその他のプロセスを設定できます。CA SDM プロセスを設定する前に、以下の情報を理解しておくことをお勧めします。

重要: CA SDM プロセスを追加した後、サーバで pdm_configure ユーティリティを実行することにより、特定のサーバを再設定します。

オブジェクト マネージャ

オブジェクト マネージャは、すべての CA SDM オブジェクトを管理します。各オブジェクト マネージャには関連付けられた名前があり、オブジェクト マネージャはその名前を使用してほかのオブジェクトと通信します。マルチプロセッサ サーバを備えたエンタープライズ システムでは、オブジェクト マネージャを追加して、処理負荷を分散できます。設定タイプに応じて、CA SDM は、以下のサーバ上にデフォルトのオブジェクト マネージャをインストールします。

- 標準：プライマリ サーバ
- 高可用性：すべてのサーバ

注: デフォルトのオブジェクト マネージャは変更できませんが、サーバにオブジェクト マネージャを追加することは可能です。

Web エンジン

Web エンジンとは、Web クライアントの Web ページの準備を行います。すべてのシステムに 1 つ以上の Web エンジンがあります。各 Web エンジンとは、オブジェクト マネージャに接続して、CA SDM オブジェクトへのすべてのリクエストを処理します。各 Web エンジンとは、直接実行およびアクセスできます。直接アクセスでは、すべての Web ブラウザは、特定の Web エンジンの特定の CGI インターフェースにアクセスします。この方法では、すべてのクライアントが 1 つの Web エンジンに接続して Web エンジンが過負荷になり、ほかの Web エンジンが未使用の状態になることがあります。このような重い負荷を処理するために、1 つの WebDirector に複数の Web エンジンを割り当てることができます。Web エンジンへのリクエストは、すべて WebDirector に送られます。その後、WebDirector は、最も使用可能な Web エンジンにクライアントをリダイレクトします。

設定タイプに応じて、CA SDM は、以下のサーバ上にデフォルトの Web エンジンをインストールします。

- 標準：プライマリ サーバ
- 高可用性：すべてのサーバ

WebDirector

WebDirector はオプションであり、1つのサーバ上に複数の **Web** エンジンがインストールされている場合に使用されます。 **WebDirector** は、ユーザから接続リクエストを受信し、リクエストを処理する **Web** エンジンを選択して、その **Web** エンジンにリクエストをリダイレクトします。このプロセスは、エンドユーザに透過的に行われます。エンドユーザは、設定されている **Web** エンジンの数にかかわらず、常に同じ URL で **CA SDM** にアクセスします。 **WebDirector** は以下の目的に使用できます。

- セキュア ソケット (SSL) を効果的に使用するように **CA SDM** を設定する。

HTTPS プロトコルを使用することで、**Web** トランザクションを暗号化して、パスワードなどの重要なデータのセキュリティ保護を最大限に高めることができます。ただし、SSL を使用するページはブラウザにキャッシュできないため、パフォーマンスが低下することがあります。

- 特定の **Web** エンジン (1つまたは複数) にログインを転送するように設定する。

ユーザが認証された後、**WebDirector** はセッションを別の **Web** エンジンに移動できます。これは、別の HTTP サーバ上の **Web** エンジンであってもかまいません。この設定により、**Web** エンジン用に SSL を設定してパスワードの保護を高め、トランザクションでは HTTP プロトコルを使用することができます。

- **WebDirector** を複数定義して、それぞれが異なる **Web** エンジンのグループを処理するように設定する。

この設定は、地域的に離れた組織がエンドユーザの近くに **Web** エンジンのグループを設置する場合に有効です。

別名

別名は、オブジェクト マネージャの **Slump** 名として作成できる容易に識別可能な名前です。特定のオブジェクト マネージャまたはオブジェクト マネージャのグループの別名を作成できます。これらの別名は、**CA SDM** プロセスの設定時にオブジェクト マネージャ名の代わりに使用できます。別名は、**CA SDM** のオプション機能です。

ナレッジ デーモン

標準設定タイプにのみ適用されます。

ナレッジデーモンは、**CA SDM** のナレッジベース（ナレッジ ドキュメント、承認プロセス、許可、通知など）を提供します。**CA SDM** は、デフォルトでは、プライマリ サーバにナレッジデーモンを設定します。ホスト名を変更して、セカンダリ サーバにデーモンを移動することができます。

ログイン ユーザ認証

標準設定タイプにのみ適用されます。

CA SDM は、デフォルトでは、プライマリ サーバにログイン ユーザ認証デーモンを設定します。ホスト名を変更して、セカンダリ サーバにデーモンを移動することができます。

LDAP 仮想 DB

標準設定タイプにのみ適用されます。

CA SDM は、デフォルトでは、プライマリ サーバに **LDAP** 仮想データベース デーモンを設定します。ホスト名を変更して、セカンダリ サーバにデーモンを移動することができます。

リポジトリ デーモン

標準設定タイプにのみ適用されます。

リポジトリ デーモンにより、リポジトリ ディレクトリに保存された添付ファイル レコードを検索することができます。**CA SDM** の **Web UI** を使用して、これらのプロセスをセカンダリ サーバにのみ追加できます。**Web UI** 経由でプロセスを追加した後、**CA SDM** の設定中に特定のオプションを有効にします。プロセスの有効化の詳細については、サーバ構成のオンライン ヘルプを参照してください。

Visualizer

標準設定タイプにのみ適用されます。

CA SDM サーバ上に Visualizer を設定して、Web サービスを使用できます。CA SDM の Web UI を使用して、これらのプロセスをセカンダリサーバにのみ追加できます。Web UI 経由でプロセスを追加した後、CA SDM の設定中に特定のオプションを有効にします。プロセスの有効化の詳細については、[サーバ構成のオンラインヘルプ](#)を参照してください。

Tomcat サーバ用の REST Web サービス

標準設定タイプにのみ適用されます。

REST Web サービスにより、CA SDM の Web UI を設定して外部と通信できます。CA SDM の Web UI を使用して、これらのプロセスをセカンダリサーバにのみ追加できます。Web UI 経由でプロセスを追加した後、CA SDM の設定中に特定のオプションを有効にします。プロセスの有効化の詳細については、[サーバ構成のオンラインヘルプ](#)を参照してください。

サポート オートメーション

標準設定タイプにのみ適用されます。

CA SDM の Web UI を使用して、これらのプロセスをセカンダリサーバにのみ追加できます。Web UI 経由でプロセスを追加した後、CA SDM の設定中に特定のオプションを有効にします。プロセスの有効化の詳細については、[サーバ構成のオンラインヘルプ](#)を参照してください。セカンダリサーバごとにサポート オートメーションプロセスを1つだけ追加できます。以下のサポート オートメーションサーバを設定できます。

SA メイン サーバ

サポート オートメーションをインストールするサーバを指定します。SA メインサーバは、セカンダリサーバにのみ追加できます。

SA 専用のオブジェクト マネージャ サーバ

サポート オートメーション設定用のオブジェクト マネージャが存在するサーバ。セカンダリサーバ上に専用のオブジェクト マネージャサーバを設定できます。

注: SA メインサーバが設定されている場合のみ、専用のオブジェクト マネージャサーバを追加できます。

SA メッセージ ルーティング サーバ

セカンダリ サーバ上にメッセージ ルーティング サーバを設定して、複数のリモート コントロール セッションを管理し、アシスタンス セッション中のパフォーマンスを向上させることができます。

SA ソケット プロキシ サーバ

セカンダリ サーバ上にソケット プロキシ サーバを設定して、メイン サーバから、暗号化/復号化など、CPU を集中的に使用するサポート オートメーション操作の負荷を軽減することができます。

UNI コンバータ

UNIX プラットフォームで実行されるサーバのいずれか 1 つに、UNI コンバータを追加できます。以下のサーバに UNI コンバータを追加できます。

- 標準：プライマリ サーバ、セカンダリ サーバ
- 高可用性：アプリケーション サーバ

TNG コンバータ

Windows プラットフォームで実行されるサーバのいずれか 1 つに、TNG コンバータを追加できます。以下のサーバに TNG コンバータを追加できます。

- 標準：プライマリ サーバ、セカンダリ サーバ
- 高可用性：アプリケーション サーバ

注: TNG コンバータを管理しているデーモン マネージャは、ほかのデーモンによって起動および停止されます。CA SDM デーモンがシャットダウンした後に TNG コンバータでイベントを取得する必要がある場合、TNG コンバータをサービスとして開始および停止します。

オブジェクト マネージャの追加

CA SDM サーバにオブジェクト マネージャを追加することにより、システム全体のパフォーマンスが向上します。CA SDM は、すべてのサーバにデフォルトのオブジェクト マネージャをインストールします。デフォルトのオブジェクト マネージャは変更できませんが、任意の CA SDM サーバにオブジェクト マネージャを追加して、サーバのパフォーマンスを向上させることができます。設定タイプに応じて、CA SDM は、以下のサーバ上にデフォルトのオブジェクト マネージャをインストールします。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ。

次の手順に従ってください：

1. [管理] タブで、[システム] - [環境設定] を選択します。
[構成リスト] ページが開きます。
2. オブジェクト マネージャを追加する設定を選択します。
[構成の詳細] ページが開きます。
3. [オブジェクト マネージャ] タブを選択します。
[オブジェクト マネージャのリスト] ページが開き、サーバに対して設定されているオブジェクト マネージャが表示されます。デフォルトのオブジェクト マネージャ (存在する場合) もリストに表示されます。
4. [オブジェクト マネージャの追加] をクリックします。
[オブジェクト マネージャの新規作成] ページが開きます。
5. 以下のフィールドを指定します。

重要： 任意のローカライズ言語のすべての入力フィールドには、英文字のみを入力してください。

ホスト名

オブジェクト マネージャを追加するホストの名前を指定します。

[検索] ボタンをクリックして、CA SDM インストールに追加されたサーバを検索できます。

高可用性設定タイプでは、ホスト名は読み取り専用で、設定の作成時に指定したホスト名に基づいて自動的に入力されます。

表示名

オブジェクト マネージャの表示名を指定します。表示名がクライアントに表示され、クライアントがどのオブジェクト マネージャに接続しているかを示します。

オブジェクト マネージャのグループ

オブジェクト マネージャの追加先のグループ名を指定します。

重要: 任意のローカライズ言語のオブジェクト グループ名には、英文字のみを入力してください。

オブジェクト マネージャをグループ化して、Web エンジンの特定のグループにサービスを提供するように、グループを割り当てることができます。この機能は、通常、プライマリ サーバから地域的に離れた場所に Web エンジンがあり、オブジェクト マネージャと Web エンジンを一緒に配置する場合に必要となります。この場合、ローカルの Web エンジンに割り当てられているオブジェクト マネージャをグループ化し、これらの Web エンジンを、このオブジェクト マネージャのグループに割り当てます。

マスクの許可

オブジェクト マネージャ用のマスクを指定します。マスクの許可機能は、接続を受け入れるクライアントをオブジェクト マネージャに通知します。

たとえば、Web エンジンは、`web:seattle:1`、`web:seattle:2`、`web:texas:1`などの名前のオブジェクト マネージャに接続しようとします。`web:seattle.*`などのマスクの許可を指定して、`seattle`のすべての接続を受け入れ、その他の接続を拒否することができます。また、`web:.*`などのマスクを指定して、Web エンジンからの接続を受け入れ、クライアントからの接続を拒否することもできます。

レコード ステータス

オブジェクト マネージャがアクティブであるか、非アクティブであるかを指定します。

注: オブジェクト マネージャのレコード ステータスを非アクティブに設定する前に、オブジェクト マネージャと関連付けられた Web エンジンの間のリンクを削除する必要があります。

6. [保存] をクリックします。

追加したオブジェクト マネージャが、[オブジェクト マネージャ リスト]に表示されます。

Web エンジンまたは WebDirector の追加

Web エンジンは、オブジェクト マネージャに接続して、CA SDM オブジェクトへのすべてのリクエストを処理します。WebDirector はオプションであり、1 つのサーバ上に複数の Web エンジンがインストールされている場合に使用されます。任意のサーバに WebDirector を設定できます。CA SDM の設定に応じて、CA SDM は、デフォルトの Web エンジンを以下のサーバにインストールします。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ。

次の手順に従ってください：

1. [管理] タブで、[システム] - [構成] を選択します。
[構成リスト] ページが開きます。
2. Web エンジンまたは WebDirector を追加する設定を選択します。
[構成の詳細] ページが開きます。

注：初めて構成を変更している場合は、まず構成を作成します。構成を変更する場合、常に既存のものを作成またはコピーします。必要な場合には、このプロセスによって前の構成に戻ることができます。

3. [Web エンジン/WebDirector] タブを選択します。
[Web エンジン/WebDirector のリスト] ページが開き、サーバに設定されている Web エンジンおよび WebDirector が表示されます。
 - 標準：デフォルトでは、Web エンジンはプライマリ サーバに存在します。任意のサーバに WebDirector を追加できます。
 - 高可用性：デフォルトでは、Web エンジンはすべてのサーバに存在します。任意の CA SDM サーバに WebDirector を追加できます。
4. [Web エンジン/WebDirector の追加] をクリックします。
[Web エンジン/WebDirector の新規作成] ページが開きます。

5. 以下のフィールドを指定します。

重要: 任意のローカライズ言語のすべての入力フィールドには、英文字のみを入力してください。

ホスト名

Web エンジンまたは WebDirector のホスト名を指定します。[検索] ボタンをクリックして、サーバを検索できます。

高可用性設定タイプでは、ホスト名は読み取り専用で、設定の作成時に指定したホスト名に基づいて自動的に入力されます。

タイプ

Web エンジンまたは WebDirector を設定するかどうかを指定します。選択されているオプションに基づいて、自動的に関連するフィールドに入力されます。

- Web エンジンを設定する場合は、[Web エンジン] を選択します。
- WebDirector を設定する場合は、[WebDirector] を選択します。

注: 適切なオプションを選択したことを確認します。設定を保存した後は、プロセス タイプを編集できません。

WebDirector

Web エンジンに割り当てられている WebDirector を指定します。

[検索] ボタンをクリックして、サーバに追加された WebDirector を検索できます。

注: Web エンジンの負荷分散スキームまたは SSL ログイン（またはその両方）を実装する場合は、同じ WebDirector に少なくとも 2 つの Web エンジン割り当てる必要があります。

CGI 名

Web エンジンに一意の CGI 名を指定します。IIS または Apache を HTTP サーバとして使用している場合、これは実際の CGI 実行可能ファイルの名前です。Tomcat を HTTP サーバとして使用している場合、これはサーブレット パラメータです。

例: (Web エンジン) pdmweb1、pdmweb2、(WebDirector) pdmweb_d1、および pdmweb_d2。

デフォルト: pdmweb.exe (CGI 名は一意である必要があります)。

CGI ポート番号

CA SDM Web クライアントが接続できるポートを指定します。 CGI ポート番号は、Tomcat サーバが実行されているポートと同じです。

デフォルト : 8080

プロトコル

Web エンジンにアクセスするためのプロトコルを指定します。

- Web エンジンがすべての CA SDM Web クライアント ユーザ認証リクエストを処理するように設定する場合は、HTTPS を選択します。
- Web エンジンが、（セキュリティ保護されたログイン Web エンジンによってユーザ認証が行われた後）すべての Web クライアントのユーザ認証以外のすべてのリクエストを処理するように設定する場合は、HTTP を選択します。

レコード ステータス

Web エンジンまたは WebDirector がアクティブであるか、非アクティブであるかを指定します。

注: WebDirector のレコード ステータスを非アクティブに設定する前に、WebDirector と関連付けられた Web エンジン間のリンクを削除します。

オブジェクト マネージャ

Web エンジンに割り当てるオブジェクト マネージャを指定します。

デフォルト

デフォルトのオブジェクト マネージャを Web エンジンに割り当てるように指定します。

いずれか

より大きな **willingness** 値を持った任意の使用可能なオブジェクト マネージャに **Web** エンジンが接続できることを指定します。**willingness** 値は、新しいクライアントを受け入れるサーバの可用性です。**willingness** 値にゼロを指定すると、**Web** エンジンがセッションを受け入れなくなります。

選択

Web エンジン用のオブジェクト マネージャを指定できます。このオプションを選択すると、設定に複数のオブジェクト マネージャまたは別名を追加するオプションが提供されます。

6. [保存] をクリックします。

追加した **Web** エンジンまたは **WebDirector** が、[**Web** エンジン/**WebDirector** のリスト] に表示されます。

別名の追加

別名は、**CA SDM** のオプション機能です。特定のオブジェクト マネージャまたはオブジェクト マネージャのグループの別名を作成できます。別名を作成する前に、以下のタスクを実行します。

- オブジェクト マネージャを定義して、そのいくつかをグループに追加します。

たとえば、**domsrvr:group1:11**、**domsrvr:seattle:12**、**domsrvr:seattle:13**、**domsrvr:Tacoma:11** とします。

- オブジェクト マネージャのグループに一致する正規表現を入力します。

たとえば、ワシントンにある **Java** クライアントをシアトルにあるオブジェクト マネージャに接続する場合は、それらを **/domsrvr:seattle.*** に接続します。または、**SEATTLE** という別名を定義し、それに値 **/domsrvr:seattle.*** を割り当てることができます。

- **Web** エンジンを定義し、その **Web** エンジンに別名を割り当てます。

重要: オブジェクト マネージャ グループ用の別名を作成した場合は、オブジェクト マネージャ グループを変更した後にそれぞれの別名を必ず変更してください。

次の手順に従ってください:

1. [管理] タブで、[システム] - [環境設定] を選択します。
[構成リスト] ページが開きます。
2. 別名を追加する設定を選択します。
[構成の詳細] ページが開きます。
3. [別名] タブを選択します。
[別名リスト] ページが開き、サーバに対して作成された別名が表示されます。
4. [別名の追加] をクリックします。
[別名の新規作成] ページが開きます。
5. 以下のフィールドを指定します。

重要: 任意のローカライズ言語のすべての入力フィールドには、英文字のみを入力してください。

名前

作成した別名の名前を指定します。

定義

別名に関連付けられている正規表現を指定します。別名の定義には、以下の形式が使用されます。

`domsrvr:[<グループ>:][<ホスト ID><ID>][.*]`

デフォルト: `/domsrvr:.*`

レコードステータス

別名がアクティブであるか、非アクティブであるかを指定します。

6. [保存] をクリックします。
追加した別名が [別名リスト] に表示されます。

追加プロセスの追加

CA SDM では、サーバに対して、サポート オートメーション サーバ、Visualizer、LDAP、KT、TNG/UNI、BopLogin リポジトリ デーモン、REST Web サービス プロセスを設定できます。

次の手順に従ってください:

1. [管理] タブで、[システム] - [構成] を選択します。
[構成リスト] ページが開きます。
2. 追加プロセスを追加する設定を選択します。
[構成の詳細] ページが開きます。
3. [追加プロセス] タブを選択します。
[追加プロセスのリスト] には、デフォルト プロセスと共にサーバに対して設定されるプロセスのリスト (存在する場合) が表示されます。
4. [プロセスの追加] をクリックします。
[プロセスの新規作成] ページが開きます。
5. 必要に応じて以下のフィールドに値を入力します。

重要: 任意のローカライズ言語のすべての入力フィールドには、英文字のみを入力してください。

プロセス

追加する CA SDM サーバ プロセスを示します。

リポジトリ デーモン

標準設定タイプにのみ適用されます。

サーバに対して設定するリポジトリ デーモンを指定します。
リポジトリ デーモンは、添付ファイル リポジトリをサポートしています。CA SDM は、デフォルトでは、プライマリ サーバにリポジトリ デーモンを設定します。ホスト名を変更して、セカンダリ サーバにデーモンを移動することができます。

SA メイン サーバ

標準設定タイプにのみ適用されます。

サーバに対して設定する SA メイン サーバを指定します。1 つの SA メイン サーバのみを設定できます。

SA 専用オブジェクト サーバ

標準設定タイプにのみ適用されます。

サポート オートメーション設定用の専用オブジェクト マネージャを指定します。プライマリまたはセカンダリのいずれかのサーバ上で、1 つの専用オブジェクト サーバのみを指定できます。

注: SA メイン サーバが設定されている場合のみ、専用のオブジェクト マネージャ サーバを追加できます。

SA メッセージ ルーティング サーバ

標準設定タイプにのみ適用されます。

サーバに対して設定するメッセージ ルーティング サーバを指定します。セカンダリ サーバ上にメッセージ ルーティング サーバを設定して、複数のリモート コントロール セッションを管理し、アシスタンス セッション中のパフォーマンスを向上させることができます。

SA ソケット プロキシ サーバ

標準設定タイプにのみ適用されます。

サーバに対して設定するソケット プロキシ サーバを指定します。セカンダリ サーバ上にソケット プロキシ サーバを設定して、メインサーバから、暗号化/復号化など、CPU を集約的に使用する操作の負荷を軽減します。

Tomcat サーバ用の REST Web サービス

標準設定タイプにのみ適用されます。

サーバの REST Web サービス設定を指定します。REST Web サービスにより、CA SDM の Web UI を設定して外部と通信できます。CA SDM の Web UI を使用して、これらのプロセスをセカンダリサーバにのみ追加できます。Web UI 経由でプロセスを追加した後、CA SDM の設定中に特定のオプションを有効にします。プロセスの有効化の詳細については、サーバ構成のオンラインヘルプを参照してください。

TNG コンバータ

Windows プラットフォームで実行されるサーバのいずれか 1 つに、TNG コンバータを追加できます。以下のサーバに TNG コンバータを追加できます。

標準：プライマリ サーバ、セカンダリ サーバ。

高可用性：アプリケーション サーバ。

注：デーモンマネージャが TNG コンバータを管理している場合、このデーモンはほかのデーモンによって起動および停止されます。CA SDM デーモンがシャットダウンした後に、TNG コンバータでイベントを取得する場合、TNG コンバータ サービスを開始および停止します。

UNI コンバータ

UNIX イベントに応答するように設定されている UNI コンバータを指定します。これらのイベントは、チケットを作成し、Service Desk のほかの作業をトリガするようにフィルタおよび設定できます。UNIX プラットフォームで実行されるサーバのいずれか 1 つに、UNI コンバータを追加できます。以下のサーバに UNI コンバータを追加できます。

標準：プライマリ サーバ、セカンダリ サーバ。

高可用性：アプリケーション サーバ。

Visualizer Tomcat サーバ

標準設定タイプにのみ適用されます。

サーバに対して設定する **Visualizer** を指定します。

CA SDM サーバ上に **Visualizer** を設定して、Web サービスを使用できます。CA SDM の Web UI を使用して、これらのプロセスをセカンダリ サーバにのみ追加できます。Web UI 経由でプロセスを追加した後、CA SDM の設定中に特定のオプションを有効にします。プロセスの有効化の詳細については、[サーバ構成のオンラインヘルプ](#)を参照してください。

注: セカンダリ サーバ上で設定できる **Visualizer Tomcat** サーバは1つのみです。

ホスト名

追加したプロセスをホストするサーバを指定します。[検索] ボタンをクリックして、サーバを検索できます。

レコード ステータス

追加したプロセスがアクティブであるか、非アクティブであるかを指定します。

6. [保存] をクリックします。

追加したプロセスが[追加プロセスのリスト]ページに表示されます。

設定の確認

- 設定が完了してサービスが正常に開始された後、**pdm_status** またはタスク マネージャ コマンドを実行して新しく追加されたデーモンを確認します。
- 現在の設定が、**pdm_configure** で選択した設定によって更新されていることを確認します。

第 3 章: REST サンプル モバイル ユーザ インターフェース

REST サンプル モバイル ユーザ インターフェースでは、アナリスト用と従業員用の 2 種類のユーザ インターフェースが提供されます。このサンプルはまた、管理者、レベル 1 アナリスト、および従業員の役割をサポートしています。CA SDM へのログイン後、管理者とレベル 1 アナリストの役割でアナリスト インターフェースが表示されます。従業員役割では従業員用のインターフェースのみ表示されます。ログインが無効な場合、CA SDM はログイン リクエストを拒否し、メッセージを表示します。管理者が自動優先順位計算を無効に設定している場合、作成および編集ページで[優先度] フィールドが表示されます。

重要: この機能は CA SDM リリース 12.9 で提供されるサンプルプログラムにのみ適用されます。これは、REST サービス アプリケーション自体で制限された仕様ではありません。

自動検索候補または自動補完を使用するフィールドでは、担当者やインシデント領域などの自動候補リストから値を選択する必要があります。値を選択しないと、ユーザがフィールドに入力した値はクリアされます。

注: ブラウザの「戻る」または「進む」オプションは使用せず、REST インターフェースで提供されているボタンを使用してナビゲートすることをお勧めします。たとえば、前のページに戻る場合は、[ホーム] や [キャンセル] を選択してください。

REST は、CA SDM の構成中に設定します。ただし、サンプルのモバイル インターフェースは[手動](#) (P. 105)で有効化します。

アナリストは以下のタスクを実行できます。

- アナウンスメントの表示。
デフォルト: 登録日によって並べ替え
- CA SDM がアナリストに割り当てたインシデントの表示。
- 割り当て済みおよび未割り当てのインシデントの表示。
- インシデントの並び替え。
デフォルト: オープン日によって並べ替え。

- インシデントの検索。
- インシデントを作成する。
- インシデントのステータス、緊急度、影響度の変更。
- アクティビティ ログのコメントの表示および更新、コールバックまたは調査の指定。

デフォルト：アクティビティの日付によって並べ替え。

従業員は以下のタスクを実行できます。

- アナウンスメントの表示。
- エンド ユーザが作成したオープンおよびクローズされたインシデントの表示。
- オープン日などによりインシデントを並び替え。
- インシデントを作成する。
- アクティビティ ログのコメントの更新。
- インシデントの検索。
- インシデントのステータスをオープンからクローズ、またはクローズからオープンに変更。

注: アスタリスクは必須フィールドを示します。

このセクションには、以下のトピックが含まれています。

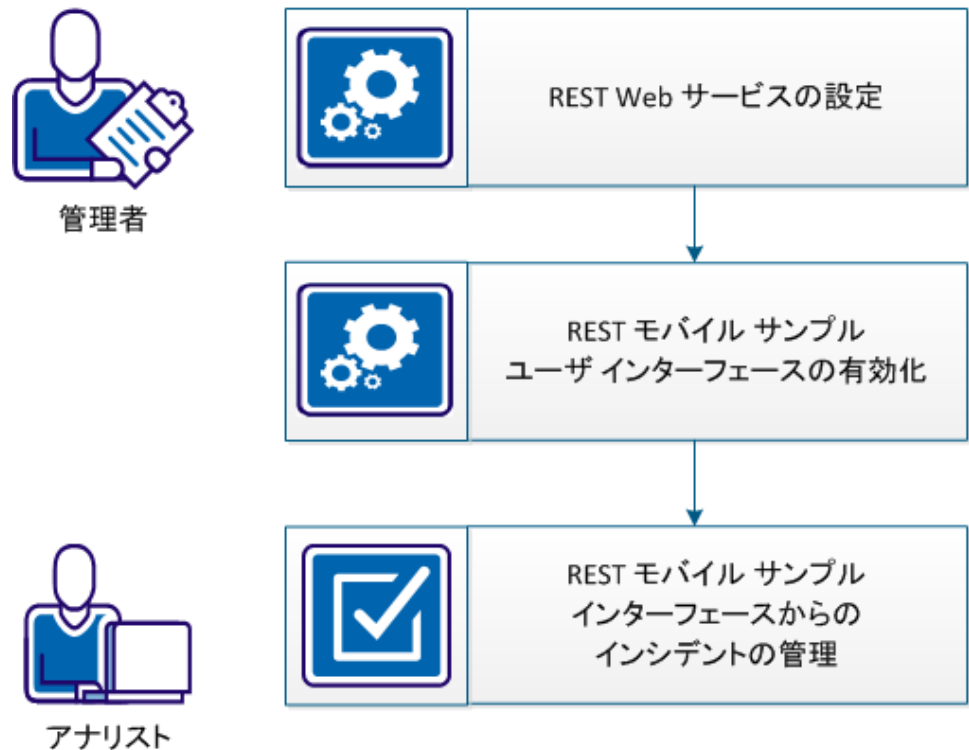
[REST モバイル サンプル ユーザ インターフェースを展開する方法 \(P. 103\)](#)

REST モバイル サンプル ユーザ インターフェースを展開する方法

REST モバイル サンプル ユーザ インターフェースを使用すると、アナリストはモバイルデバイス上でインシデントを管理できます。管理者は製品の設定時に REST Web サービスを有効にし、CA SDM コンピュータ上にファイルをコピーして、REST モバイル サンプル ユーザ インターフェースを有効にすることができます。アナリストは、モバイルインターフェースを使用して、エンドユーザが CA SDM で開いたインシデントを管理します。

以下の図は、管理者が REST Web サービスを有効にし、それにより、アナリストがキュー内のインシデントを管理できるようになる方法を示しています。

REST モバイル サンプル ユーザ インターフェースを展開する方法



次の手順に従ってください:

1. [REST Web サービスを設定します](#) (P. 104)。
2. [REST モバイル サンプル ユーザ インターフェースを有効化します](#) (P. 105)。
3. [REST モバイル サンプル ユーザ インターフェースからのインシデントを管理します](#) (P. 106)。

REST Web サービスの設定

管理者は CA SDM の設定時に REST Web サービスを有効にします。CA SDM のデフォルトの環境設定では、REST Web サービスは有効化されません。

次の手順に従ってください:

1. 以下のいずれかを実行します。
 - CA SDM をインストールし、環境設定ダイアログ ボックスが表示されるまで待機します。
 - すでに CA SDM がインストールされていて、REST Web サービスが設定されていない場合は、コマンドライン インターフェースから `pdm_configure` を実行します。Windows で、[スタート] - [プログラム] - [CA] - [Service Desk マネージャ] - [設定] をクリックします。

[環境設定] ダイアログ ボックスが開きます。
2. [一般設定]、[システム アカウント]、[データベース]、および [Web インターフェース] ダイアログ ボックスで設定情報を確認します。
3. [REST Web サービス] ダイアログ ボックスが開きます。
4. [REST Web サービスの設定] オプションを有効にします。
5. REST Tomcat ポートを指定します。

デフォルト : 8050
6. REST Tomcat シャットダウン ポート ポートを指定します。

デフォルト : 8055
7. [次へ] をクリックし、CA SDM の設定を続行します。

設定が完了します。

REST モバイル サンプル ユーザ インターフェースの有効化

MDB への好ましくないアクセスを防ぐために、CA SDM のデフォルトの設定では REST モバイル サンプル ユーザ インターフェースは無効にされています。このインターフェースは、管理者が手動で有効にします。

次の手順に従ってください:

1. REST Web サービスがインストールおよび設定されている CA SDM コンピュータ上で、以下のディレクトリを見つけます。

```
$NX_ROOT/samples/sdk/rest/mobiledemo
```

2. このディレクトリを以下の場所にコピーします。

```
$NX_ROOT/bopcfg/www/CATALINA_BASE_REST/webapps
```

注: Tomcat を再起動する必要はありません。

REST モバイル サンプル ユーザ インターフェースが有効化されます。

3. (オプション) REST サンプル ユーザ インターフェースを無効にする場合は、/webapps ディレクトリから mobiledemo ディレクトリを削除します。

REST モバイル サンプル インターフェースからのインシデントの管理

アナリストまたは従業員は、モバイル デバイス上で REST モバイル サンプル インターフェースを表示して、キュー内のインシデントを管理できます。たとえば、アナリストは、インシデント 30 を開いて、内部専用のコメントをログに記録できます。

次の手順に従ってください:

1. モバイル デバイス上で以下の URL にアクセスします。

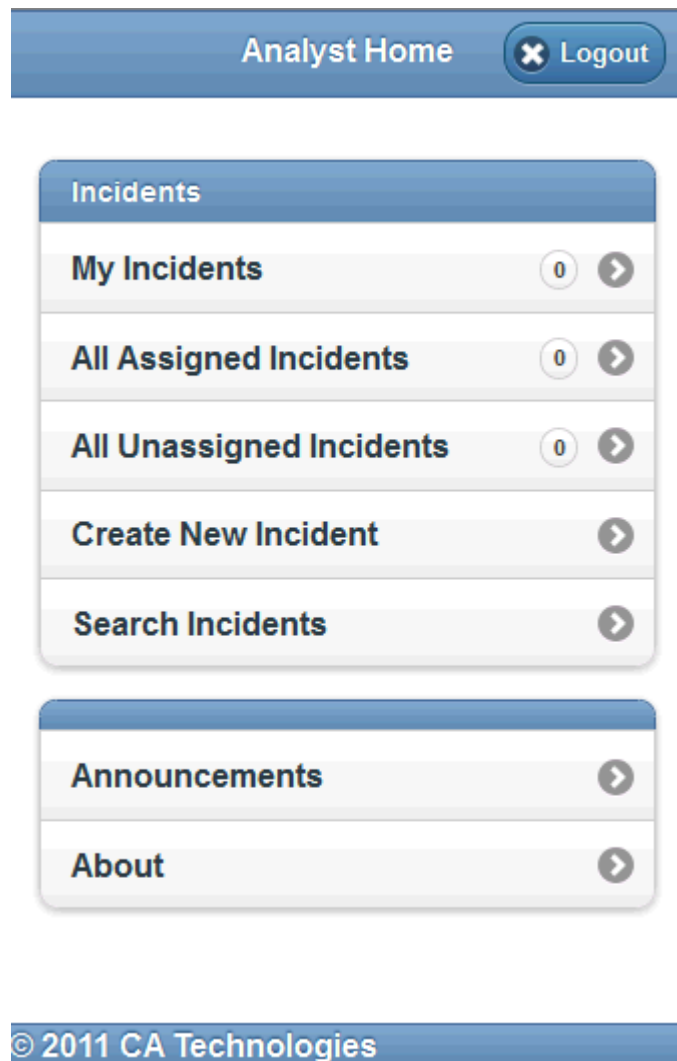
`http://hostname:REST-Tomcat-port/mobiledemo/login.html`

サンプル REST モバイル インターフェースのログイン ページが表示されます。

2. 認証情報を使用して、CA SDM にログインします。
REST モバイル アナリスト用のホーム ページが表示されます。
3. [割り当て済みインシデント] を選択します。
4. インシデントを選択します (例: インシデント 30)。
5. 詳細ページで [アクティビティの作成] を選択します。
6. ドロップダウン リストから [ログ コメント] を選択します。
7. [内部] オプションから [はい] を選択します。
8. コメントを入力し、[保存] を選択します。

例: アナリスト インターフェース ホーム ページ

以下は、REST サンプル アナリスト モバイル ホーム ページの画像です。



例：従業員インターフェース ホーム ページ

以下は、REST サンプル従業員モバイル ホーム ページの画像です。

The screenshot displays a mobile application interface for an employee home page. At the top, a blue header bar contains the text "Employee Home" and a "Logout" button with a close icon. Below the header, there are two main sections. The first section, titled "Customer Service", includes three items: "Create a new Incident" with a right arrow, "Announcements" with a right arrow, and "About" with a right arrow. The second section, titled "Look up my existing tickets", includes two items: "My open incidents" with a count of "0" and a right arrow, and "My closed incidents" with a count of "0" and a right arrow. Below these sections is a "Look up Incident Number" section featuring a text input field and a "Go" button with a star icon. At the bottom, a blue footer bar displays the copyright notice "© 2011 CA Technologies".

例：従業員によるインシデントの作成

この例では、従業員は、サーバ上の REST インターフェースにログインし、自分のコンピュータで発生したネットワークの問題のインシデントを作成します。

次の手順に従ってください：

1. 従業員は、REST モバイル インターフェースにログインします。
2. 従業員は、[インシデントの新規作成] を選択します。
3. 従業員は、以下の情報を指定します。
 - 自分の電話番号を入力します
 - 自分の電子メール アドレスを入力します
 - [緊急度] ドロップダウン リストから [3- 迅速に] を選択します
 - [インシデント領域] に「ネットワーク」と指定します
 - インシデントの概要を入力します
たとえば、従業員がラップトップから会社ネットワークにアクセスできないことなどを概要として入力します。
 - （必須）インシデントの説明を入力します
説明として、たとえば、ネットワーク上でのエンドユーザのラップトップ名やハードウェアの詳細などを入力します。
4. 従業員は、[保存] を選択します。
インシデントが作成され、インシデント番号がメッセージにより表示されます。

第 4 章: CA SDM Mobile Enabler の設定

CA SDM Mobile Enabler r2.0 は現在、CA SDM リリース 12.9 と共に展開されます。管理者は、ユーザがモバイル アプリケーションを使用できるように、いくつかの設定手順を実行する必要があります。

このセクションには、以下のトピックが含まれています。

[CA SDM Mobile Enabler](#) (P. 111)

[前提条件の確認](#) (P. 118)

[Open Space へのパッチ適用](#) (P. 118)

[\(オプション\) フォーム フィールドを非必須として設定する](#) (P. 121)

[\(オプション\) アップグレード後の承認互換性の適用](#) (P. 122)

[CA SDM Mobile Enabler へのアクセス](#) (P. 122)

CA SDM Mobile Enabler

CA SDM Mobile Enabler は、ユーザのモバイル デバイスから CA SDM のコア機能の一部および Open Space にアクセスする共通のインターフェースです。CA SDM Mobile Enabler では、以下のモバイル機能を使用できます。

- [アナリスト キュー](#) (P. 112) - CA SDM で作成されたチケットに対するアクティビティを表示および実行します。
- [承認](#) (P. 113) - ワークフロー エンジンによって作成された割り当て済みワーク項目に対して承認または応答します。
- [Open Space](#) (P. 116) - コミュニティで質問を登録または質問に回答します。コミュニティがユーザの質問に答えることができない場合は、チケットを発行します。

CA SDM Mobile Enabler にログインすると、ログイン ページから使用する機能を選択できます。また、ログインした後に、機能を有効または無効にできます。[設定] 画面に移動し、[Add/ Remove Capabilities] をタップします。選択対象として、Mobile Enabler で追加される機能のみ表示されます。スワイプして機能を切り替え、認証情報を入力し、[ログイン] をタップします。

アナリスト キュー

Analyst Queue 機能により、ログインしたユーザは以下の **CA SDM** コア機能にアクセスできるようになります。

- ログインする場合（インシデント、リクエスト、問題、案件、および変更要求のみ）、ホーム画面の **CA SDM** からチケットの数を表示します。各タイル上のバッジ数は、最後のリフレッシュ以降、新規および更新されたチケット数を表示します。

注: ホーム画面が **CA SDM** からのすべてのチケットを表示するとは限りません。デフォルトでは、すべてのチケットがすべてのユーザに割り当てられたことを示します。このデフォルト フィルタは変更できます。

- ホーム画面からのチケット タイプ タイルをタップし、チケットのリストを表示します。各チケット タイプをフィルタし、選択した情報のみ表示します。たとえば、インシデント リストからの [フィルタ] アイコンをタップし、[割り当て] - [優先度 (高)] を選択します。リストはリフレッシュされ、選択したインシデントのみ表示されます。

注: **CA SDM** サーバでカスタマイズされ、**CA SDM** スコアボードに表示されるフィルタも、この機能に表示されます。

- チケットを検索します。検索領域でタップし、検索キーワードを入力します。入力を進めると、検索結果が表示されます。チケット番号またはチケットの概要に基づいてチケットを検索できます。
- チケットをタップし、詳細を表示します。また、添付ファイルおよびアクティビティ ログ（存在する場合）も表示できます。

- [さらにアクションを表示] (機能の右上の隅からの矢印アイコン) をタップし、チケットのアクションを実行します。
 - ステータスをエスカレートまたは更新、またはチケットを他のユーザに転送します。
 - このチケットへのコメントを追加します。
 - チケットへの添付ファイルを追加します。添付ファイルの許可サイズは **3 MB** 以下です。
 - カメラを使用して、スナップショットを作成します。
 - ギャラリーを使用して、イメージを選択します (この機能は .jpeg、.jpg、および .png 画像形式のみサポートします)。
- **重要: CA SDM Mobile Enabler の Web アプリケーションから添付ファイルを表示するには、Web ブラウザの「ポップアップをブロックする」オプションをオフにします。**
- リフレッシュ間隔 (デフォルトでは、それは **4 分** に設定) を変更します。システム メニューで [設定] - [機能固有の設定] をタップします。ポーリング間隔を増加 (プラス記号 (+)) または減少 (マイナス記号 (-)) させます。
- この機能で表示される機能を選択します。たとえば、ログインユーザを選択して、インシデントのみを表示できます。[設定] 画面に移動し、[機能の追加/削除] をタップします。スワイプして、機能を有効または無効にします。

承認

承認機能は、保留中のワークフロー タスクに迅速でシームレスに応答するために使用されます。承認機能は、モバイルユーザに、タスクの完了に必要なすべての情報を提供します。

ログインしたユーザは、この機能の以下のコア機能にアクセスできます。

- 機能の簡単なツアーを表示します。この機能を次回使用する場合は、このツアーを表示しないことを選択できます。再度ツアーを表示する場合は、[設定]、[承認] セクションの [機能固有の設定] に移動し、[製品ツアーの表示] チェック ボックスをオンにします。

- 以下のタスクを表示します。
 - CA SDM と統合される以下のワークフロー エンジンからの保留中のタスク：
 - CA SDM Classic Workflow
 - IT Process Automation Manager (ITPAM)
 - CA Workflow (CAWF)
 - ユーザに割り当てられるワークフロー タスク。 ログインしたユーザが PAMAdmins グループの一部である場合、承認機能から任意の ITPAM タスクを表示し応答できます。
 - ユーザが属するグループに割り当てられるワークフロー タスク。
 - CA SDM Classic Workflow については、CA SDM グループに割り当てられたタスクは表示されず、個人に割り当てられたタスクのみ表示されます。
 - ログインしたユーザが PAMAdmins グループの一部である場合、承認機能から任意の ITPAM タスクを表示し応答できます。
 - CA SDM チケット担当者か依頼者かにかかわらず、ユーザの応答が必要なワークフロー タスク。 たとえば、金融承認タスクが、直接 CA SDM と関連しないユーザによって実行される場合があります。

注: ワークフロー エンジンがダウンしている場合、およびユーザが関連するワーク項目を使用していない場合には、承認は、ワーク項目またはエラー メッセージを表示しません。 任意の時点で、ワークフロー エンジンが作動し始めると、関連するワーク項目が表示されるようになります。 しかし、すでにワーク項目を使用している場合にサーバがダウンすると、承認はエラー レポートを表示します。

- タスクが保留中の時間ごとに、入力を待機している保留中のタスク数を示す棒グラフを表示します。 この棒グラフでは、新しいタスクを識別すると共に、それらがどれくらいの時間待機しているかを視覚的に判断できます。
- 保留中の時間によってフィルタされたタスクのリストを表示します。 グラフ上のバーをタップするか、または画面の上端のプルダウンを使用します。 たとえば、1 時間前のバーをタップすると、最後の 1 時間に作成または変更され、承認待ちのすべてのタスクが表示されます。
- 保留中のタスクを検索します。 [検索] 領域に検索テキストを入力します。 入力に伴って、検索結果が更新されます。 タスク記述からのチケット番号、優先度、またはキーワードを使用して検索できます。

- リスト内のタスクをタップすることにより、ワーク項目の詳細を表示します。詳細を参照するときに、以下のアクションを実行できます。
 - ワーク項目の入力フォームを、ワークフロー エンジン フォームとほぼ同じように表示します。カスタム承認フォームは、変更せずにモバイルデバイスで自動的に使用できます。これらは、モバイル デバイス上でのレンダリングのために再フォーマットされます。
 - チケットアイコン  をタップして関連する CA SDM チケット情報を表示することにより、ワーク項目についてさらに詳細に理解できます。この情報には、ビジネス上の理由、実装およびバックアウト手順、連絡先、担当者、情報、優先度、SLA、重大度などが含まれる可能性があります。
 - 関連するチケット タブにリスト表示された電話番号または電子メールアドレスをタップすることにより、依頼者、担当者などを呼び出するか、または電子メールを送信します。この情報は、CA SDM チケットにこの連絡先情報が含まれる場合にのみ表示されます。
 - 関連する変更要求チケットの添付ファイルをダウンロードして表示します。ダウンロードされたドキュメントを開くために、追加のビューア ソフトウェアをモバイルデバイスにインストールすることが必要になる可能性があります。
- 重要:** CA SDM Mobile Enabler の Web アプリケーションから添付ファイルを表示するには、Web ブラウザの「ポップアップをブロックする」オプションをオフにします。
- 注:** Android ポップアップ ブラウザ上で添付ファイルをダウンロードすると、エラー メッセージが表示されます。ポップアップ ブラウザの左側にある矢印をタップします。ポップアップ ブラウザがメインブラウザに変換され、添付ファイルをダウンロードできます。
- 詳細フォームに必要な情報を入力して、[サブミット] をタップすることによりワーク項目に応答します。複数のタスクが保留中の場合、ユーザの応答に対して次のタスクが自動的に開かれます。また、機能の右上隅の早送り矢印をタップすることにより、次のワーク項目を開くことができます。

- サポートからのリクエストに対して、システムメニューで「設定」 - 「機能固有の設定」を選択することにより、デバッグ情報を有効にします。「トレース」ドロップダウンをタップして、オプションを選択します。「オン」オプションを選択して、デバッグ情報を有効にします。「詳細」オプションを選択すると、より詳細な情報が表示されます。CA SDM サーバ上の `$NX_ROOT¥log¥approve.log` ディレクトリ内のログ情報を表示できます。サポートセッションを完了した場合、このオプションを無効にして追加のサーバオーバーヘッドを回避するよう推奨します。
- システムメニューで「設定」 - 「機能固有の設定」をタップすること、および「日時形式」を選択することにより、日時形式を変更します。機能をリフレッシュすると、変更された日時形式のみ反映されます。
- タスク リスト ページの右上隅のシステムメニューをタップし、「更新」を選択することにより、ワーク項目の現在のリストをリフレッシュします。
- 「機能固有の設定」ページにある「ポーリング」間隔を変更することにより、承認タイルがどれくらいの頻度で更新されるか指定するリフレッシュ時間間隔を変更します。
- 指定された時間の内に機能が応答しない場合、応答タイムアウトオプションが有効になり、ログインしたユーザにメッセージが表示されます。ログインユーザとして、システムメニューで「設定」 - 「機能固有の設定」を選択することで、この時間を（分単位で）設定できます。デフォルトでは、「タイムアウト(分)」オプションは2分に設定されています。この時間を増加（プラス（+）記号）、または減少（マイナス（-）記号）させることができます。このスケジュールされたタイムアウト内にこの機能が応答しない場合、ログインユーザにエラーメッセージが表示されます。メッセージプロンプトに対して「OK」をクリックすると、ユーザは、承認機能のログインページに戻ります。

Open Space

Open Space 機能では、ログインユーザが、モバイルデバイス上の CA Open Space の以下のコア機能にアクセスできます。

- ホーム画面に、CA Open Space から登録される最新の質問数を表示します。登録は、「おすすり」、「最新」、「フォロー中」などのタグに従って分類されます。デフォルトでは、「最新」の質問が表示されます。

- (CA SDM で CA Open Space が設定されている場合) ホーム画面に、この機能でユーザが作成するチケット (CA Open Space サーバ上でシステム管理者によって設定されるリクエストまたはインシデント) の数が表示されます。
- ホーム画面から質問タイルをタップして、関連する登録を表示します。たとえば、ドロップダウンから [最新] などのオプションを選択して、最新の登録のみを表示します。
- すべてのソースから登録を検索します。[検索] テキストボックスに検索条件を入力し、Enter キーをタップします。すべてのソースからの検索結果が表示されます。ドロップダウンから、[グローバル] を選択して CA Open Space サーバ上で有効になっているすべてのデータソースから検索するか、または [質問] を選択してこの機能でリスト表示された質問から検索することができます。
- リクエストまたはインシデントを検索します。
- 質問をタップして、詳細な登録内容を表示します。[さらにアクションを表示] (機能の右上隅の矢印アイコン) をタップして、以下の手順に従います。
 - この登録内容に応答する
 - この登録内容に従う、または従わない
 - 登録内容を共有する
 - 登録内容でユーザの質問が解決されない場合は、サービス デスク チケットをオープンします。

注: リクエスト フォームに新しいフィールドを追加するには、システム管理者は、CA Open Space サーバ上でフィールドを設定する必要があります。同様に設定されたフィールドが、Open Space 機能に表示されます。CA Open Space サーバで設定できるフィールド数は5つです。フィールドを設定する方法の詳細については、「CA Open Space Administration Guide」を参照してください。

- 更新間隔 (デフォルトでは4分に設定) を変更します。システムメニューで [設定] - [機能固有の設定] をタップします。ポーリング間隔を増加 (プラス記号 (+)) または減少 (マイナス記号 (-)) させます。
- この機能で表示される機能を選択します。たとえば、ログインユーザは、[質問] のみを表示するよう選択できます。[設定] 画面に移動し、[機能の追加/削除] をタップします。スワイプして、機能を有効または無効にします。

前提条件の確認

CA SDM Mobile Enabler を設定する前に、以下の要件を確認します。

- [認定モバイルオペレーティングシステム](#) (P. 118)
- アナリストキュー機能および承認機能にアクセスするには、CA SDM Mobile Enabler をインストールするサーバ上に CA SDM リリース 12.9 をインストールし設定する必要があります。また、同じサーバ上で REST もインストールされ、設定されます。詳細については、「*CA Service Desk Manager 実装ガイド*」を参照してください。
- Open Space 機能にアクセスするには、CA SDM サーバに CA Open Space r2.0 をインストールし設定する必要があります。詳細については、「*CA Open Space Implementation Guide*」を参照してください。
- アナリストキューのログインユーザを REST Web サービス API 役割と関連付けました。この役割の *管理*、*セキュリティ*、および *参照* 機能アクセスが、表示または変更のアクセスレベルで割り当てられていることを確認します。機能アクセス、アクセスレベル、および役割の詳細については、「*CA Service Desk Manager 管理者ガイド*」を参照してください。

認定モバイルオペレーティングシステム

CA SDM Mobile Enabler は、以下のモバイルオペレーティングシステム用のネイティブブラウザで認定されています。

- iOS 5.1 以降
- Android 4.x

Open Space へのパッチ適用

ご使用のオペレーティングシステムに応じて、CA SDM Mobile Enabler を展開して Open Space 機能にアクセスする前に、CA Open Space サーバ上で以下のパッチを適用します。

オペレーティングシステム	パッチ番号
Windows	RO61737
Linux	RO61738

CORS 設定の有効化

Open Space モバイル機能を使用するには、CORS（Cross-Origin Resource Sharing）設定を有効化します。

重要: このプロセスは、CA SDM Mobile Enabler のネイティブ アプリケーションではなく、Web ベース アプリケーションにのみ適用可能です。

次の手順に従ってください:

1. CORS 設定を有効にする前に、[Open Space 用のパッチが適用済み](#) (P. 118)であることを確認します。
2. Open Space サーバにログインします。
3. 以下のディレクトリに移動します。
OSOP_HOME/tomcat.7.xx/webapps/ROOT/WEB-INF
4. web.xml ファイルを開きます。
5. XML ファイル内の最後の `</filter>` タグの後に以下のコンテンツを追加します。

```
<filter>
<filter-name>CORS</filter-name>
<filter-class>com.thetransactioncompany.cors.CORSFilter</filter-class>
<init-param>
<param-name>cors.allowGenericHttpRequests</param-name>
<param-value>true</param-value>
</init-param>

<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
<init-param>
<param-name>cors.allowSubdomains</param-name>
<param-value>true</param-value>
</init-param>
<init-param>
<param-name>cors.supportedMethods</param-name>
<param-value>GET, HEAD, POST, OPTIONS, PUT, DELETE</param-value>
</init-param>
```

```
<init-param>
<param-name>cors.supportedHeaders</param-name>
<param-value>Origin, Accept, Authorization, Content-Type,
X-Requested-With</param-value>
</init-param>
<init-param>
<param-name>cors.exposedHeaders</param-name>
<param-value>X-Test-1, X-Test-2</param-value>
</init-param>
<init-param>
<param-name>cors.supportsCredentials</param-name>
<param-value>true</param-value>
</init-param>

<init-param>
<param-name>cors.maxAge</param-name>
<param-value>3600</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>CORS</filter-name>
<url-pattern>*</url-pattern>
</filter-mapping>
```

6. (オプション) 特定のドメインが <osop> サーバにアクセスする場合は、以下の手順に従います。

- a. XML ファイル内の以下の行に移動します。

```
<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
```

- b. cors.allowOrigin param-value を CA SDM サーバの以下のサブドメイン情報で置換します。

http://<server_Name>:<Port_Number>

注: スペースで区切って複数のサブドメインを追加できます。

7. ファイルを保存します。
8. Open Space サーバを再起動します。
CORS 設定が有効になります。

(オプション)フォーム フィールドを非必須として設定する

デフォルトでは、ITPAM ワークフロー エンジンから派生する承認機能のすべての入力フィールドが必須です。ITPAM バージョンに応じて、システム管理者はこれらのフィールドを非必須にできます。

次の手順に従ってください:

1. CA SDM サーバにログインし、NX.env ファイルを開きます。
2. このファイル内に以下の変数を追加します。
`NX_MOBILE_WFM_ITPAM_ALL_FIELDS_ARE_REQUIRED`
3. 変数値を設定します。
4. ファイルを保存します。
5. 変数値および ITPAM バージョンに応じて、以下の変更を適用できます。
 - 変数が設定されていない場合、ITPAM 3.1、4.0 以降のすべてのフィールドがデフォルトで必須になります。
 - この変数値が [はい] に設定されている場合、ITPAM 3.1、4.0 以降のすべてのフィールドが必須になります。
 - この変数値が [いいえ] に設定されている場合、ITPAM 3.1 のすべてのフィールドは、最小長および最大長の制約に従います。ITPAM 4.0 以降の文字列入力フィールドの最小長および最大長は、承認機能では適用できません。そのため、変数値を [いいえ] に設定した場合、すべてのフィールドが非必須になります。

(オプション)アップグレード後の承認互換性の適用

最新の機能を持つ最新の承認機能にアクセスし、一貫したユーザ操作性を得るには、NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE 変数を [はい] に設定します。

このオプションを設定すると、以前のバージョンの承認機能にログインを試みた場合、この機能をアップグレードするよう指示され、ログインが拒否されます。

次の手順に従ってください:

1. CA SDM サーバにログインし、NX.env ファイルを開きます。
2. このファイル内に以下の変数を追加します。
`NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE`
3. 変数値を [はい] に設定します。
4. ファイルを保存します。
5. CA SDM サーバを再起動します。

CA SDM Mobile Enabler へのアクセス

モバイルデバイスから CA SDM Mobile Enabler の Web アプリケーションにアクセスするには、以下の URL を使用します。

`http(s)://<CA_SDM_Server_Name>:<REST_Port_Number>/casdm`

注: モバイルデバイスで CA SDM Mobile Enabler の Web アプリケーションを使用するユーザに、この URL を通知します。

モバイルデバイスでネイティブ モバイル アプリケーションとして CA SDM Mobile Enabler を使用するには、以下の手順に従います。

1. Google Play (Android ユーザの場合) または App Store (iOS ユーザの場合) に移動します。
2. CA Service Desk Manager を検索します。
3. CA Service Desk Manager アプリケーションをインストールします。

インストールが正しく終了した後、ユーザの携帯電話に CA SDM アイコンが表示されます。

第 5 章：業務構造の定義

このセクションには、以下のトピックが含まれています。

[ビジネスストラクチャの作成](#) (P. 124)

[業務インフラストラクチャの定義](#) (P. 137)

[マルチテナンシー](#) (P. 141)

ビジネス ストラクチャの作成

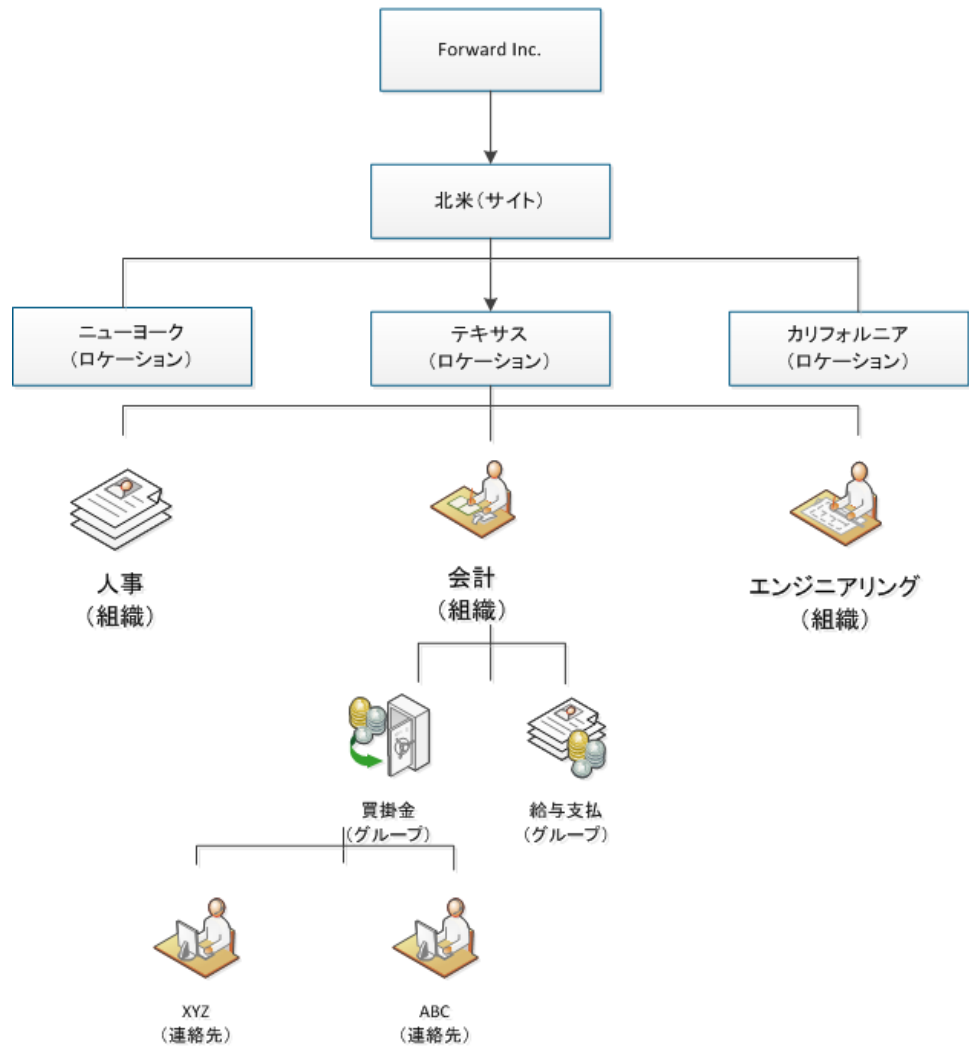
ビジネス ストラクチャは、Unicenter Service Desk 環境内のエンタープライズのカスタマイズされた論理的な表現です。このシナリオは、管理者がエンタープライズのビジネス ストラクチャを作成して、分散ロケーションにまたがる連絡先、グループ、およびアセットを管理および追跡する方法を説明します。ビジネス ストラクチャを作成した後、サイト、組織、またはグループごとのリクエストを分析するためのレポートを生成できます。

例

架空の会社 **Forward** 社は、さまざまな地域に広がる複数のオフィスに対してリクエスト処理システムを使用しています。この会社は、さまざまな事業セグメントから発生するリクエストの数とタイプを分析するために、Unicenter Service Desk の実装を計画しています。

以下の図は、架空の会社 **Forward** 社を使用して、ビジネス ストラクチャの概要の例を示しています。

ビジネス ストラクチャの例



効果的な追跡と意思決定を促進するために、組織は、以下の要素を追跡する必要があります。

- 連絡先、連絡先グループ、およびロケーション
- さまざまなロケーションのアセット

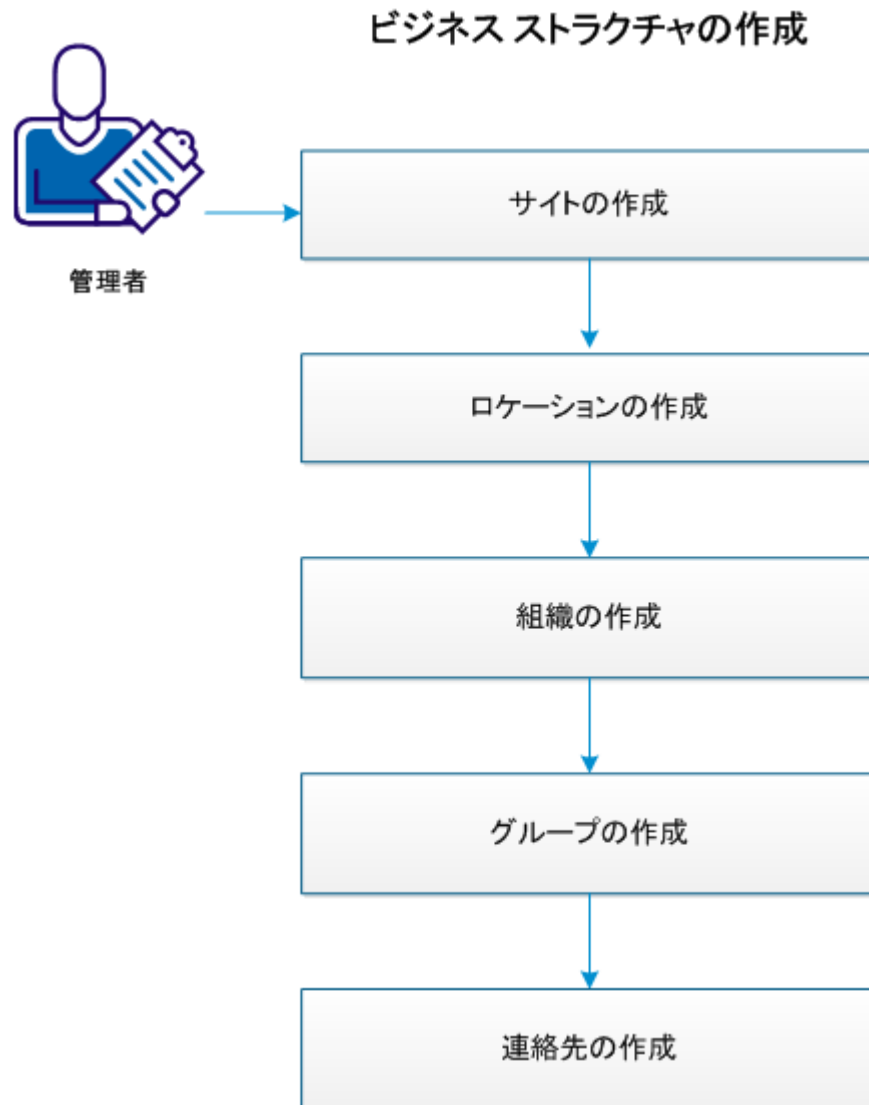
ビジネス ストラクチャを作成することにより、**Forward** 社の管理チームは、以下のアクションを実行できます。

- サイト、組織、およびグループごとにリクエストを分析するレポートの生成
- リクエストプロセスにおけるギャップの修正措置を実装することによる全体的な効率の向上

ビジネス ストラクチャを作成する方法

ビジネス ストラクチャを作成するには、ビジネスにおけるサイトと組織の論理的な階層を定義し、次に連絡先とグループをそれぞれのサイトおよび組織に関連付けます。

以下の図は、管理者が典型的なビジネス ストラクチャで、どのようにオブジェクトを定義できるかを示しています。



次の手順に従ってください:

1. [サイトの作成](#) (P. 128)
2. [ロケーションの作成](#) (P. 129)
3. [組織の作成](#) (P. 130)
4. [グループの作成](#) (P. 131)
5. [連絡先の作成](#) (P. 132)

サイトの作成

サイトは、組織が 1 つ以上のロケーションを持つ地域です。

たとえば、北米は、ニューヨーク、カリフォルニア、およびテキサスにロケーション（オフィス）を持つサイトです。

注: マルチテナンシーを有効にしている場合は、ドロップダウン リストから適切なテナントを選択します。

次の手順に従ってください:

1. **Unicenter Service Desk** スコアボードのメニュー バーで、[ファイル] - [新規サイト] を選択します。
[サイトの新規作成] ウィンドウが開きます。
2. 必要に応じて、サイトに固有の情報を入力します。
3. [保存] をクリックします。
サイト レコードが作成および保存されます。

ロケーションの作成

ロケーションは、オフィスの住所などの物理的な場所です。たとえば、ニューヨーク、カリフォルニア、およびテキサス オフィスの住所は、北米サイトのロケーションになります。

ロケーションを作成すると、そのロケーションの連絡先とリソースの管理に役立ちます。ロケーションを作成した後、それをサイトに割り当てることができます。

次の手順に従ってください:

1. スコアボードのメニュー バーで [ファイル] - [新規ロケーション] を選択します。
[ロケーションの新規作成] ページが開きます。
2. ロケーションに固有の情報を入力し、タブの以下のコントロールを使用してロケーションを設定します。

住所

ロケーションの実際の住所を指定します。

自動割り当て

このロケーションのメンバに、自動的にチケット（リクエスト、変更要求、および案件）を割り当てます。

リクエスト領域の更新

ロケーションのメンバに自動的に割り当てるリクエスト領域を選択します。

変更カテゴリの更新

ロケーションのメンバに割り当てる変更カテゴリを選択します。

案件カテゴリの更新

ロケーションのメンバに割り当てる案件カテゴリを選択します。

グループの更新

自動的なチケットの割り当てに対して、更新するグループを選択します。

重要: リクエスト領域およびカテゴリを更新した後、各リクエスト領域およびカテゴリの自動割り当てを個別に有効にします。

3. [保存] をクリックします。
ロケーションの詳細が保存されます。
4. (オプション) 手順 1 ～ 3 を繰り返して、さらにロケーションを追加します。

組織の作成

組織は、社内部門または部署、または外部企業を表わします。組織は、チケット、構成アイテム (CI) クラス、および連絡先に割り当てることができます。

たとえば、組織の構成アイテムを定義して、組織が使用するハードウェア、ソフトウェア、およびサービスを指定できます。

注: マルチテナンシーを有効にしている場合は、ドロップダウン リストから適切なテナントを選択します。

次の手順に従ってください:

1. スコアボードのメニュー バーで [ファイル] - [新規組織] を選択します。
[組織の新規作成] ページが開きます。
2. 組織に固有の情報を入力し、以下のフィールドで組織の詳細を指定します。

住所

組織に関連付けるロケーションの住所を表示します。組織にロケーションを割り当てると、自動的にフィールドに入力されます。

環境

組織が使用する構成アイテム (機器、ソフトウェア、サービスなど) を表示します。組織と 1 つ以上の構成アイテムに関連付けることができます。組織に構成アイテムを関連付けると、管理者がさまざまなロケーションで組織によって使用されるリソースを追跡するのに役立ちます。

3. [保存] をクリックします。
組織の詳細が保存されます。
4. (オプション) 手順 1 ～ 3 を繰り返して、さらに組織を追加します。

グループの作成

グループは、特定の責任範囲を担う連絡先の集合体です。グループを定義すると、チケット解決の責任が複数の担当者で共有されている場合に、その責任を割り当てることができます。たとえば、Dallas Human Resources というグループが、自社のダラス支社の人事を担当しているとします。この支社の従業員に問題が発生した場合は、その問題を Dallas Human Resources グループに割り当てることができます。

注: マルチテナンシーを有効にしている場合は、ドロップダウン リストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

次の手順に従ってください:

1. スコアボードのメニュー バーで [ファイル] - [新規グループ] を選択します。
[グループの新規作成] ページが開きます。
2. 以下のフィールドでグループの詳細を指定することにより、このグループおよび組織に固有の情報を入力します。

通知

連絡先情報およびグループに通知する方法を定義します。

住所

ロケーションにグループを割り当てます。

組織情報

機能組織、管理組織、部門、コスト センター、またはベンダー情報を指定します。

環境

環境（装置、ソフトウェア、サービスなど）を指定します。

メンバー

連絡先を追加または削除します。

サービス契約

グループに関連付けられているサービス契約の一覧を表示します。

自動割り当て

グループ メンバシップに基づいたチケットの自動割り当ての一覧を表示します。

特記事項および特殊処理

VIP またはセキュリティ リスクのタイプなどの特記事項および特殊処理のタイプの一覧を表示します。[連絡先の特殊処理の更新] をクリックして、特殊処理メンバーを検索します。

3. [保存] をクリックします。

グループ レコードが保存され、[グループの詳細] ページが開きます。グループの構成用に以下のボタンが用意されています。

環境の更新

[連絡先詳細] - [環境] タブでこのボタンをクリックし、グループの [構成アイテムの検索] ウィンドウを表示します。このページで考慮するアセット用検索条件を指定できます。新しい構成アイテムを作成し、連絡先の [更新] ウィンドウをそれぞれ使用して、アセットを検索できます。

メンバの更新

このボタンは、[メンバー] - [サービス契約] - [自動割り当て] - [メンバー] タブで連絡先を表示します。このグループの連絡先を追加および削除できます。

4. (オプション) 手順 1 ～ 3 を繰り返して、必要に応じてさらにグループを追加します。

連絡先の作成

連絡先は、アナリストや顧客など、システムを定期的に使用する人物です。ビジネス ストラクチャおよびグループを作成した後、連絡先を作成して、それぞれのロケーションおよび組織にマップします。

連絡先は以下の方法で作成できます。

- 手動での連絡先の作成

CA SDM スコアボードを使用して連絡先を作成する場合は、この方法を使用します。

- LDAP データベースからのデータの使用

CA SDM インストールが、LDAP (Lightweight Directory Access Protocol) サーバにアクセスするように設定されている場合で、必要なオプションがインストールされている場合には、この方法を使用します。

手動での連絡先の作成

連絡先情報用に LDAP などのアクティブなディレクトリを使用しない場合、CA SDM で連絡先を手動で作成できます。

注: マルチテナンシーを有効にしている場合は、ドロップダウン リストから適切なテナントを選択します。

次の手順に従ってください:

1. スコアボードのメニュー バーで [ファイル] - [新規連絡先] を選択します。

[連絡先の新規作成] ウィンドウが開きます。

2. 連絡先に応じて、以下のフィールドに入力します。

テナント

連絡先（マルチテナンシー インストール用）に関連付けられているテナントを指定します。

ID の連絡先

連絡先の一意的識別子を指定します。デフォルトのユーザ認証が使用されている場合、ユーザのログイン時にこのフィールドの値がパスワードとして使用されます。

ユーザ ID

連絡先のユーザ名を示します。連絡先はこの値を使用してシステムにログインします。

サービス タイプ

連絡先が受けることのできるサポートのレベルを指定します。

データ パーティション

この連絡先のデータ パーティションを指定します。この値によって、この連絡先がアクセスできるレコードが決まります。

アクセス タイプ

アクセス タイプを指定します。アクセス タイプによって、連絡先がアクセスできるシステム機能が決まります。

利用可能

連絡先がチケット割り当てに使用可能かどうかを示します。

セルフサービスの保存を確認

セルフサービス インターフェースからレコードが保存されるときに、連絡先が確認を受け取るかどうかを示します。

アナリストのテナント グループ

(アナリストの連絡先タイプのみ) アナリストが担当するテナント グループを指定します。

3. 連絡先を設定するには、タブで使用可能な以下のコントロールを使用します。

通知

連絡先情報と連絡先に通知する方法を定義します。

- この連絡先に対する各メッセージの緊急度レベルで使用する通知方法を選択します。

たとえば、通常レベルのアクティビティの場合は、電子メールを使用して連絡先に通知し、緊急レベルのアクティビティの場合は、ポケットベルの電子メールを使用して通知できます。

- 各通知の緊急度レベルに有効なワークシフトを選択します。

たとえば、通常のワークシフト（週 5 日、1 日に 8 時間）を標準レベル、24 時間のワークシフトを緊急レベル通知に割り当てます。

住所

連絡先の住所を示します。

組織情報

連絡先の部署または管理組織、部門、コスト センター、ベンダー情報を指定します。

環境

機器、ソフトウェア、およびサービスなどの連絡先の環境を指定します。

グループ

連絡先をグループ（共通の責任範囲を担う連絡先の集合体）に割り当てます。

役割

1 つ以上の役割に連絡先を割り当てます。

サービス契約

連絡先に関連付けられているサービス契約を表示します。

特殊処理

特殊処理を必要とする連絡先をリストし、訪問者またはセキュリティ リスクのタイプなどの特殊処理タイプを検索したり、連絡先を特殊処理タイプに関連付けたりします。

イベント ログ

セルフ サービスとナレッジのアクティビティなど、連絡先に関連付けられるイベントをリストします。

アクティビティ

連絡先のアクティビティ ログをリストします。

4. [保存] をクリックします。

連絡先情報が保存されます。

LDAP データベースからの連絡先の使用

LDAP（Lightweight Directory Access Protocol）サーバにアクセスするように製品インストールが設定されている場合で、必要なオプションがインストールされている場合は、LDAP データベースのデータを使用して連絡先を作成および更新できます。これで、ネットワーク ユーザ データとの連絡先を簡単に同期できるようになります。

以下の手順に従います。

1. スコアボードのメニュー バーで [ファイル] - [LDAP からの新規連絡先] を選択します。
[LDAP ディレクトリの検索] ページが表示されます。
2. LDAP エントリ リストを開くのある特定のレコードに制限するには、1 つ以上のフィルタを入力します。
3. [検索] をクリックします。
[LDAP エントリ リスト] ページに、フィルタ条件に一致したレコードが表示されます。
4. 連絡先を作成するには LDAP エントリをクリックします。
LDAP 情報の一部が入力された状態で、[連絡先の新規作成] ページが表示されます。
5. 必要に応じて追加情報を入力します。
6. 連絡先を設定するには、タブで使用可能な以下のコントロールを使用します。

通知

連絡先情報と連絡先に通知する方法を定義します。

住所

組織を関連付けるロケーションの住所を指定します。

組織情報

連絡先の部署または管理組織、部門、コスト センター、ベンダー情報を指定します。

環境

機器、ソフトウェア、およびサービスなどの連絡先の環境を指定します。

グループ

連絡先をグループ（共通の責任範囲を担う連絡先の集合体）に割り当てます。

役割

1 つ以上の役割に連絡先を割り当てます。

サービス契約

連絡先に関連付けられているサービス契約を表示します。

特殊処理

特殊処理を必要とする連絡先をリストします。また、連絡先を検索したり、訪問者やセキュリティ リスクのタイプなどの特殊処理タイプに連絡先に関連付けることができます。

イベント ログ

セルフ サービスとナレッジのアクティビティなど、連絡先に関連付けられるイベントをリストします。

アクティビティ

連絡先のアクティビティ ログをリストします。

7. [保存] をクリックします。

連絡先情報が保存されます。

8. （オプション）手順 1 ～ 7 を繰り返して、さらに連絡先を追加します。

ビジネス ストラクチャの作成と連絡先およびグループの関連付けが正常に完了しました。これで、サイト、組織、またはグループごとにリクエストを分析するためのレポートを生成できます。

業務インフラストラクチャの定義

CA SDM を使用してサービス デスクを実装する場合、重要なことは、以下の項目を設定して業務インフラストラクチャを定義することです。

- 構成アイテムのファミリーとクラス
- 製造者とモデル
- サービス ステータス
- ベンダーとベンダー タイプ

以下の情報は、各オブジェクトの一般的な説明であり、製品内でオブジェクトがどのように使用されているかを説明しています。

注: 各オブジェクトの定義方法の詳細については、オンライン ヘルプを参照してください。

オブジェクト定義の要求

オブジェクトを定義する際は、最初にオブジェクト階層の最下層の定義を行います。これにより、高い階層のオブジェクトを定義する際に、下位の階層の既存のオブジェクトから選択することができます。たとえば、クラスにはファミリーが入っている（参照されている）ので、まずファミリーを定義し、その後にクラスを定義します。同様に、構成アイテムは階層の最上位にあるため、関連するすべてのオブジェクトを定義してから、最後に構成アイテムを定義する必要があります。したがって、データ オブジェクトは次の順序で定義します。

最初に定義	2 番目に定義	3 番目に定義
ファミリー	クラス	構成アイテム
メーカー	モデル	構成アイテム
サービス ステータス	構成アイテム	
ベンダー タイプ	ベンダー	構成アイテム

ファミリーおよびクラス

ファミリーは、構成アイテムを属性によって分類したもので、各構成アイテムには有用な属性が割り当てられます。クラスは、会社がサポートする構成アイテムの一般的なカテゴリを定義したものです。ファミリーは、ハードウェア、ソフトウェア、サービスなど、構成アイテムの広範なカテゴリです。クラスは、広いファミリー カテゴリに含まれる詳細なカテゴリです。たとえば、ハードウェアというファミリーには、モデム、ルータ、リピータ、ブリッジなどのクラスが含まれます。

構成アイテムをファミリーやクラスに分類すると、構成アイテムの管理が容易になります。たとえば、特定のファミリーまたはクラスに属している構成アイテムのリストを生成できます。

製造者とモデル

製造者は、会社と関係のあるさまざまな構成アイテムの製造者を定義したものです。モデルには、特定の製造者が会社を提供した製品情報を含めます。たとえば、特定のソフトウェア会社を製造者として定義し、その製造者が会社を提供する各アプリケーションをモデルとして定義できます。

製造者とモデルを定義すると、構成アイテムの管理が容易になります。たとえば、特定の製造者が提供するモデルのリストや、特定のモデルの構成アイテムのリストを生成できます。

サービス ステータス

サービス ステータスは、構成アイテムの準備状況を定義したものです。サービス ステータスの例として、[動作中]、[修理中]、[中断]などがあります。サービス ステータスを定義すると、会社にある構成アイテムの可用性や使用状況をトラッキングできます。たとえば、その時点で修理に出されている構成アイテムのリストを生成できます。

ベンダー タイプとベンダー

ベンダー タイプは、構成アイテムを提供する会社のタイプを定義するベンダーの分類です。たとえば、構成アイテムをリースするベンダーをリース会社として分類し、サービスを提供するベンダーをプロバイダとして分類できます。

ベンダーは、会社製品やサービスを提供する供給会社を、会社のタイプや主要連絡先などの情報も含めて特定します。構成アイテムで参照する以外にも、ユーザの連絡先レコードでベンダーを参照できます。

ベンダー タイプとベンダーの定義は、構成アイテムを分類する便利な方法の1つです。たとえば、特定のベンダー タイプに含まれるベンダーのリストや、特定ベンダーから提供されている構成アイテムのリストを生成できます。

設定項目

構成アイテムは、業務インフラストラクチャを構成するデバイス、ソフトウェア、およびサービスです。構成アイテムに関連付けられている情報は、構成アイテムを一意に識別し、正確なロケーションを示します。構成アイテムは、連絡先（プライベート構成アイテム）や組織（共有構成アイテム）に関連付けることができます。構成アイテムを使用することにより、次のようなものを識別、表示および指定することができます。

- 名前、クラス、およびファミリーによる構成アイテムの識別
- 在庫情報の指定
- 構成アイテムを定義する追加プロパティの指定
- 構成アイテムに関連付けられたコメントの記録と参照
- 構成アイテムのロケーション情報の指定
- サービス タイプなど、構成アイテムに対するサービス情報の指定
- 構成アイテムに割り当てた連絡先および組織の参照と定義
- 構成アイテム間の階層関係およびピアツーピア関係の識別
- 構成アイテムに関連付けられたチケットの参照

構成アイテムに対して、この情報をすべて定義する必要はありません。ただし、最適な数の構成アイテム情報を定義しておけば、IT 組織の影響度分析を実施する際に、状況を明確に把握できます。

関連項目：

[構成アイテムの作成](#) (P. 685)

[連絡先、ロケーション、組織 CI](#) (P. 689)

[CI 関係](#) (P. 694)

外部のアセット管理ツール

CA SDM インストールは、CA NSM、CA Asset Management、CA APM などの他のアセット管理ツールと統合できます。CA SDM のこれらのツールのアセット管理機能は、以下のとおりです。

- CA NSM には、アセット情報を CA SDM に追加する pdm_nsmimp ユーティリティ（Windows 用のみ）が用意されています。

- **CA Asset Management** は、ハードウェアおよびソフトウェア インベントリの完全な機能セットを提供します。**CA SDM** クライアントで **CI** を表示した場合、[アセット ビューア] ボタンをクリックして、アセットに関して検出された追加情報を表示できます。

CA SDM と **CA Asset Management** の統合は、これらの製品を同じ **MDB** にインストールしたときにアクティブになります。

- **CA Asset Portfolio Management** には、アセット ライフサイクル機能がすべて備わっています。**CA SDM** クライアントで **CI** を表示した場合、[アセット ビューア] ボタンをクリックして、アセットに関する追加のファイナンス情報を表示できます。

CA SDM と **CA Asset Portfolio Management** の統合は、これらの製品を同じ **MDB** にインストールしたときにアクティブになります。

注: **CA SDM** のインストールとその他のアセット管理ツールとの統合の詳細については、「実装ガイド」を参照してください。

マルチ テナンシー

マルチテナンシーでは、**CA SDM** の単一の実装を複数の独立したテナント（およびそのユーザ）で共有できます。テナント ユーザは、その役割およびテナントの階層に従って、定義された方法で相互に対話します。通常、役割または階層ごとに付与されたアクセスでない場合、各テナントは **CA SDM** 実装を自身で使用するためだけに表示します。別のテナントのデータを更新または表示することはできません。

マルチテナンシーでは、テナントがハードウェアとアプリケーションのサポート リソースを共有できます。これにより、独立した実装の多くの利点を活かしながら、両方のコストを下げることができます。

注: マルチ テナンシーのインストールおよび環境設定の詳細については、「実装ガイド」を参照してください。

サービス プロバイダ

サービス プロバイダは、CA SDM マルチテナンシー インストールにおけるプライマリ テナント（所有者）です。CA SDM インストールに追加された最初のテナントは、常にサービス プロバイダ テナントになります。サービス プロバイダ テナントは、親テナントを持つことができません。

CA SDM は、特権ユーザ（通常 Windows では ServiceDesk、Linux/UNIX では srvcdesk）をサービス プロバイダ テナントに関連付けます。

以下の CA SDM タスクをどれでも実行できるのは、サービス プロバイダ テナントのみです。

- CA SDM オプションの設定
- ナレッジ マネジメント オプションの設定
- サポート オートメーション オプションの設定
- テーブルまたは列の作成
- テナントの作成、編集、または削除
- テナントへのサブテナントの許可
- パブリック データの更新

注: 管理者は、テナント ユーザに、自分のデータ以外のデータへのアクセスを許可できます。サービス プロバイダ以外のテナント アナリストは、アナリストのテナントが含まれるように各機能へのアクセスが更新された場合以外は、自身のテナントおよびサブテナントのみにアクセスできます。たとえば、役割定義では、その役割内のユーザの特定のテナント グループへの読み取りおよび書き込みアクセスを個別に設定できます。

重要: 最初に作成されたテナントは、サービス プロバイダとして設定されます。その後、[サービス プロバイダ] チェック ボックスおよび[レコード ステータス] フィールドは読み取り専用になります。

関連項目:

[サービス プロバイダ管理](#) (P. 143)

[テナントのアクセス](#) (P. 146)

[テナントの作成](#) (P. 159)

サービス プロバイダ管理

サービス プロバイダは、テナントに自身の設定の管理を許可できます。テナント管理者は、すべてのテナントで同じ管理タスクのサブセットにアクセスできるため、`ADMIN_TREE` テーブルは自体はテナント化されません。むしろ、デフォルトのテナント管理者の役割では、テナント管理者が利用可能な管理機能が定義されます。

テナント管理者としてユーザを指定するには、そのユーザの役割の [テナント管理者] を選択します。

マルチテナンシーの仕組み

マルチテナンシーがアクティブであれば、各連絡先アクセス権を、すべてのテナント（パブリック）、シングルのテナント、またはテナントグループ（ユーザによる定義または製品による保守）に付与できます。連絡先の役割で、アクセス権を制御し、アクセス権によって、読み取りアクセス権と書き込みアクセス権を個別に指定します。テナントアクセスは役割に依存しており、連絡先はセッション中に役割を変更できるため、連絡先のテナントアクセスも変更されることがあります。

マルチテナンシーがインストールされている場合、ほとんどの **CA SDM** オブジェクトには、オブジェクトを所有するテナントを指定するテナント属性が含まれます。オブジェクトは、テナント属性とその使用方法に応じて、以下の 3 つのグループに分かれます。

テナントなし

テナント属性を使用しないでオブジェクトを定義します。これらのオブジェクト内のすべてのデータは、パブリックです。

例：優先度および緊急度

テナントが必要

（DBMS ではなく **CA SDM** によって強制される）`null` にできないテナント属性を使用してオブジェクトを定義します。これらのオブジェクト内のデータはすべて、個々のテナントに関連付けられます。パブリックデータはありません。

例：チケットテーブル（リクエスト、案件、および変更要求）

テナントが任意

NULL にできるテナント属性を使用してオブジェクトを定義します。これらのオブジェクト内のデータの一部はパブリックであり、一部は特定のテナントに関連付けられています。各テナントのオブジェクトのビューは、パブリック データとそのテナント固有のデータのマージされたビューです。

例：カテゴリおよびロケーション

ユーザがデータベースにクエリを実行すると、CA SDM は、ユーザがアクセス権を持つテナントに属するオブジェクトに結果を制限します。この制限は、有効なすべてのデータ パーティション制限に加えて適用されます。つまり、表示されるのは、アクセスが許可されているテナントに属するデータのみで、テナント（必須）テーブルとテナント（オプション）テーブルのデータは表示されません。

テナント ユーザがデータベース オブジェクトの作成または更新を要求すると、CA SDM は、ユーザの現在の役割で更新が許可されるテナントにオブジェクトが属していることを確認します。また、あるオブジェクトから他のオブジェクトへのすべての外部キー（SREL）参照が、パブリック（テナントなしの）オブジェクト、同じテナントのオブジェクト、またはテナント階層においてオブジェクトのテナントの上位にあるテナントのオブジェクトに対するものであることを確認します。すなわち、テナントありのオブジェクトは、その親テナントに属するオブジェクト、その親の親に属するオブジェクトなどを参照できます。

オブジェクトを作成するユーザが、複数のテナントの更新アクセス権を持っている場合、そのユーザは直接または間接的にテナントを明示的に指定する必要があります。

注：SREL 参照制限には、例外が 1 つあります。特定の SREL 参照（インシデントの担当者など）は、含んでいるオブジェクトのテナント階層内のテナントに属するオブジェクトを参照することができます。このような参照は、CA SDM オブジェクト スキーマ (Majic) で `SERVICE_PROVIDER_ELIGIBLE` として指定されます。`SERVICE_PROVIDER_ELIGIBLE` フラグが重要になるのは、サービス プロバイダ テナントがテナント階層でオブジェクトのテナントより上にない場合のみです。サービス プロバイダ テナントが階層にある場合は、テナント検証ルールによりサービス プロバイダの参照が許可されます。

オブジェクトの作成または更新を要求するサービス プロバイダ ユーザには、テナント ユーザと同じ制限が適用されます。ただし、サービス プロバイダ ユーザには、パブリック オブジェクトを作成または更新する権限を与えることができます。この権限は、サービス プロバイダ ユーザのアクティブな役割によって制御します。

注: CA SDM でテナント データの更新が制限されている場合、エラー メッセージによりデータ パーティション制限が通知されます。このエラー メッセージが表示された場合は、データ パーティション制限またはマルチテナンシー制限のいずれかが有効です。

マルチテナンシー オプション

マルチ テナンシーは、以下のマルチ テナンシー オプションのいずれかをインストールしてアクティブにします。

- **オフ** - マルチ テナンシーは使用されません。マルチテナンシー機能は利用できず、オブジェクトにテナント属性がありません。このオプションは、新しい CA SDM インストールのデフォルト設定です。
- **セットアップ** - マルチテナンシー機能は、管理者に対して有効です。したがって、テナント関連のオブジェクトおよび属性を表示および編集できます。ただし、CA SDM によってテナンシー制限は適用されないため、管理者以外のユーザには変更は表示されません。この設定により、管理者はテナントの定義やテナントへのオブジェクトの割り当てなどのタスクを実行することで、CA SDM の通常の使用に影響を与えずにマルチテナンシーを準備できます。
- **オン** - マルチ テナンシーは完全に機能します。すべてのユーザにそれぞれ適切な UI 変更が表示され、CA SDM によってテナンシー制限が適用されます。

注: マルチテナンシー適用のその他のオプションなど、マルチ テナンシーのインストールおよび実装の詳細については、「実装ガイド」を参照してください。

テナント情報

マルチテナンシーをインストールする場合（セットアップ モードまたはフル適用モードのいずれかで）、テナントを作成および更新します。テナントに維持される情報は、以下の 2 つの属性を除いて組織に維持されるデータと似ています。

ロゴ

テナントのロゴが記載された画像ファイルへの URL を提供します。ロゴは、[テナントの詳細] ページ自体で表示され、テナント ユーザによって表示される Web フォームまたはテナントに関連付けられたオブジェクトを表示する Web フォームで CA ロゴの代わりとしても表示されます。

サービス プロバイダ

テナントがサービス プロバイダかどうかを示します。サービス プロバイダ テナントは、常に最初に追加されたテナントです。管理者が最初のテナントを追加すると、以下の結果になります。

- 最初のテナントがサービス プロバイダになります。この指定は変更できません。
- 特権ユーザ（通常は ServiceDesk）およびすべてのシステム連絡先（System_AHD_Generated など）は、新規サービス プロバイダ テナントに属するように設定されます。

注: システム ユーザ「Administrator」は、Windows でのみ追加され、テナントは割り当てられません。特権ユーザは、テナントを手動で Administrator に割り当てる必要があります。

テナントのアクセス

CA SDM ユーザの役割は、アクセス認証とユーザ インターフェースの両方を制御します。ユーザが利用可能な役割のセットは、そのユーザのアクセス タイプによって異なります。マルチテナンシーでは、ユーザが役割の範囲内でアクセスできるテナントまたはテナント グループを制御できます。

[役割の詳細] ページの [権限] タブには、[テナントのアクセス] ドロップダウンリストと [テナント書き込みアクセス] ドロップダウンリストがあります。 [テナントのアクセス] は表示専用で、 [テナント書き込みアクセス] は作成および更新できます。

以下の関連付けを役割に割り当てることができます。

テナントアクセスと同じ([テナント書き込みアクセス]のみ)

[テナント書き込みアクセス] を [テナントのアクセス] 設定と同じに設定します。 [テナント書き込みアクセス] のデフォルトあり、 [テナント書き込みアクセス] でのみ有効です。

すべてのテナント

テナント制限を削除します。 **CA SDM** では、このアクセス権を持つ役割内のユーザは、データベース内の任意のオブジェクトを表示したり（読み取りアクセス）、データベース内のテナント化されたオブジェクトを更新（書き込みアクセス）することができます。 [すべてのテナント] アクセス権を持つユーザがオブジェクトを作成する場合、 **CA SDM** では新規オブジェクトのテナントを選択する必要があります。

単一テナント

役割のテナントアクセスを、指定されたテナントに設定します。 このオプションを選択すると、特定のテナントを選択可能な 2 つ目のフィールドが **Web UI** に表示されます。 **CA SDM** では、このアクセス権を持つ役割内のユーザは、指定されたテナントに関連付けられたオブジェクトしか表示したり（読み取りアクセス）、作成および更新（書き込みアクセス）することができません。 この選択は、 [テナントのアクセス] または [テナント書き込みアクセス] のいずれかに有効です。

テナントグループ

役割のテナントアクセスを、ユーザ定義のテナントグループまたはシステムによって維持されるテナントグループに設定します。 [テナントグループ] オプションを選択すると、特定のテナントグループを選択可能な 2 つ目のフィールドが **Web UI** に表示されます。 **CA SDM** では、この役割を持つユーザは、このグループ内のいずれかのテナントに関連付けられたオブジェクトした表示したり（読み取りアクセス）、作成および更新（書き込みアクセス）することができません。 テナントグループアクセス権を持つユーザがオブジェクトを作成する場合、 **CA SDM** では新規オブジェクトのテナントを選択する必要があります。 この選択は、 [テナントのアクセス] または [テナント書き込みアクセス] のいずれかに有効です。

連絡先のテナント

役割のテナント アクセスを、その役割を使用する連絡先のテナントに設定します。CA SDM では、このアクセス権を持つ役割内のユーザは、自身のテナントに関連付けられたオブジェクトしか表示したり（読み取りアクセス）、作成および更新（書き込みアクセス）することができません。この選択は、[テナントのアクセス] または [テナント書き込みアクセス] のいずれかに有効です。

連絡先のテナント グループ(アナリストのみ)

アナリストの役割アクセスを、アナリストの連絡先レコードで指定されているように、アナリストが作業するテナント グループに設定します。この役割を持つユーザがアナリストでない場合、この選択には[連絡先のテナント] と同じ効果があります。[テナントのアクセス] または [テナント書き込みアクセス] のいずれかに有効です。

連絡先のサブテナント グループ

役割のテナント アクセスを、その役割を使用する連絡先のサブテナント グループに設定します。CA SDM では、このアクセス権を持つ役割内のユーザは、自身のサブテナント グループに関連付けられたオブジェクトしか表示したり（読み取りアクセス）、作成および更新（書き込みアクセス）することができません。この選択は、[テナントのアクセス] または [テナント書き込みアクセス] のいずれかに有効です。

連絡先のスーパーテナント グループ

役割のテナント アクセスを、その役割を使用する連絡先のスーパーテナント グループに設定します。CA SDM では、このアクセス権を持つ役割内のユーザは、自身のスーパーテナント グループに関連付けられたオブジェクトしか表示したり（読み取りアクセス）、作成および更新（書き込みアクセス）することができません。この選択は、[テナントのアクセス] または [テナント書き込みアクセス] のいずれかに有効です。

連絡先の関連するテナント グループ

役割のテナント アクセスを、その役割を使用している関連するテナント グループに設定します。CA SDM では、このアクセス権を持つ役割内のユーザは、自身の関連するテナント グループに関連付けられたオブジェクトしか表示したり（読み取りアクセス）、作成および更新（書き込みアクセス）することができません。この選択は、[テナントのアクセス] または [テナント書き込みアクセス] のいずれかに有効です。

現在の役割のアクセス権に関係なく、すべてのユーザがパブリック データを表示できます。[パブリックの更新] チェック ボックスによって、役割内のサービス プロバイダ ユーザがパブリック データの作成または更新を許可されるかどうかは制御されます。テナント ユーザ（サービス プロバイダ以外のテナントに属するユーザ）は、役割にかかわらずパブリック データを更新することができません。

関連項目:

[役割のテナント アクセスの編集](#) (P. 149)

役割のテナント アクセスの編集

役割のテナント アクセスを割り当てたり、編集することができます。

役割のテナント アクセスを編集する方法

1. [セキュリティと役割の管理] - [役割管理] - [役割リスト] に移動します。
[役割リスト] が表示されます。
2. 役割をクリックします。
[役割の詳細] ページが表示されます。
3. [編集] をクリックします。
[役割の更新] ページが表示されます。
4. [テナントのアクセス] および [テナント書き込みアクセス] のオプションを選択します。

注: これらの設定で別のオプションを選択する場合は、注意してください。

5. [保存] をクリックします。

役割の更新されたテナント アクセス オプションが保存されます。

テナントの使用条件

使用条件ステートメントは、エンドユーザが **CA SDM** にログインしたときの最初のページに表示される文言です。このステートメントは、ユーザに製品の正しい使用方法について通知します。ユーザは、**CA SDM** へのログインを続行する前にこの条件に同意する必要があります。試行されたセッション ログイン後に、標準ログおよびユーザ イベント ログにエントリが書き込まれます。

使用条件に対して、以下のアクションを実行できます。

- 使用条件ステートメントを作成、更新、削除できます。
- 使用条件ステートメントをテナントに関連付けられます。

注: 使用条件ステートメントテナントに関連付けるには、マルチテナンシーを有効にし、1 つ以上のテナントを設定する必要があります。

- ログインするたびに、エンドユーザにステートメントを承諾させることができます。
- 空の使用条件ステートメントを提示し、エンドユーザに最初のステートメントを無視させることができます。

関連項目:

[使用条件を設定する方法 \(P. 151\)](#)

使用条件を設定する方法

使用条件ステートメントは、エンドユーザが **CA SDM** にログインした場合に初期ページのステートメントと共に表示されます。このステートメントは、ユーザに製品の正しい使用方法について通知します。ユーザは、**CA SDM** へのログオンを続行する前にこの条件に同意する必要があります。エンドユーザが [承諾] を選択すると、**CA SDM** はログインを続行し、メインフォームを表示します。ユーザが [拒否] を選択すると、**CA SDM** はログインに戻ります。試行されたセッションログイン後に、標準ログおよびユーザ イベント ログにエントリが書き込まれます。

一般的には、連絡先テナントの使用条件ステートメントを設定します。連絡先テナントが非アクティブな使用条件ステートメントで設定されている場合、使用条件が設定されていない場合、または [使用条件] ドロップダウンリストで [<空>] が選択されている場合は、**CA SDM** にテナントの親、祖父などの使用条件ステートメントが表示されます。どのレベルでも使用条件が検索されない場合、**CA SDM** はログインを続行します。テナントに空の使用条件ステートメントを設定した場合、**CA SDM** はログインを続行してメインフォームを表示します。

使用条件は以下のようにして設定できます。

1. マルチテナンシーを有効にします。
2. 1つ以上のテナントを設定します。
3. 使用条件ステートメントを定義します。
4. 特定の使用条件ステートメントを使用するようにテナントを更新します。

注: 使用条件ステートメントの作成および変更に関する詳細情報については、オンラインヘルプを参照してください。

ユーザ インターフェースの影響

マルチテナンシー機能をインストールすると、ユーザの役割に関連付けられた権限およびテナント アクセスに応じて、ユーザ インターフェースが変更されます。変更は、テナント ユーザおよびサービス プロバイダ ユーザの両方に影響します。

テナント ユーザ

ユーザの役割が 1 つのテナントに制限され、ユーザが管理者でない場合、すべてのページ上でデフォルト **CA Technologies** ロゴの代わりにカスタムテナント ロゴを使用できます。この置換は、テナントの [テナントの詳細] ページでロゴが定義されているかどうかによって異なるため、テナント別のオプションです。

管理者以外のテナント ユーザのユーザ インターフェースの変更点は、更新または編集（[編集] ボタン、またはリスト ページの [新規作成] ボタン）を許可するメニュー項目またはボタンがパブリック オブジェクトに表示されないという点のみです。これは、テナント ユーザにパブリック オブジェクトを更新する権限がないためです。

テナント管理者

テナントが任意のオブジェクトを参照する、シングル テナントにアクセスできるテナント管理者の場合は、別のインターフェースの変更点があります。これらのオブジェクトのリスト ページには、リスト行がパブリック データかどうかを指定する [パブリック] 列が自動的に表示されます。また、検索フィルタの最初の要素は、以下の選択肢が含まれた [パブリック データ] ドロップダウン リストです。

- 含む（デフォルト）
- 除外
- のみ

複数のテナントにアクセスできるテナント管理者には、テナント化されたオブジェクトのリスト ページに [テナント] 列が表示されます。この列は、テナントが任意のテーブルのリストで [パブリック] 列の代わりに表示されます。

テナントグループを表示できるユーザ

ユーザの役割で複数のテナントにアクセスできる場合、またはサービスプロバイダユーザに「パブリックの更新」許可がある場合、CA SDM リストフォームは以下のように変更されます。

テナントなしのオブジェクト

テナントなしのオブジェクトには、パブリック データのみ含まれています。サービスプロバイダユーザは、そのロールに「パブリックの更新」許可がある場合にのみ、テナントされていないオブジェクトを作成または更新できます。この許可がない場合、「更新」ボタン自体やリストページの「新規作成」ボタンなど、更新または編集を行うことができるメニュー項目やボタンが UI に表示されません。テナントユーザはパブリック オブジェクトを更新できないため、これらのユーザの場合、テナントなしのオブジェクトに「編集」ボタンやリストページの「新規作成」ボタンは表示されません。

テナントが必要なオブジェクト

テナントが必要なオブジェクトには、特定のテナントと関連付けられたデータのみが含まれます。これらのオブジェクトのリストフォームには、最後のリンク列の後に「テナント」列が自動的に表示されます。さらに、検索フィルタには、ユーザがリストを 1 つのテナントに制限できるようにするテナントセレクトが含まれます。

テナントが任意のオブジェクト

テナントが任意のオブジェクトには、パブリック データとテナント固有のデータの両方が含まれます。これらのオブジェクトのリストフォームには、「テナント」列が自動的に表示されます（空のテナントは、パブリック オブジェクトを示します）。また、検索フィルタには、テナントセレクトと「パブリック データ」ドロップダウンリスト（テナント管理者に表示されるのと同じもの）の両方が含まれています。

注: マルチテナンシー システムで、テナントが必要なテーブルにテナントされていないデータが間違って含まれている場合は、テナントが必要なテーブルに「パブリック データ」ドロップダウンリストが表示され、「AHD05358 There were nn untenanted active xxx objects at Service Desk startup」というメッセージが表示されます。

複数テナントを更新できるユーザ

ユーザの役割で複数のテナントにアクセスできる場合、またはサービスプロバイダのユーザの役割に「パブリックの更新」権限がある場合（サービスプロバイダで作業するアナリストにとっては通常です）、詳細ページは以下のように変更されます。

テナントなしのオブジェクト

テナントなしのオブジェクトには、パブリック データのみ含まれています。「パブリックの更新」権限を持つサービスプロバイダユーザの詳細ページは、変更されません。ユーザが「パブリックの変更」権限のない役割にいるか、サービスプロバイダに属さない場合、テナントなしのオブジェクトの読み取り専用ページは「編集」ボタンが表示されません。

テナントが必要な既存のオブジェクト

テナントが必要なオブジェクトには、特定のテナントと関連付けられたデータのみが含まれます。テナントが必要な既存のオブジェクトの詳細ページには、標準ページヘッダの一部としてオブジェクトのテナントが表示されます。

テナントが任意のオブジェクト

テナントが任意のオブジェクトには、パブリック データとテナント固有のデータの両方が含まれます。これらのオブジェクトの詳細ページは、ユーザがサービスプロバイダに属するかどうかと、「パブリックの更新」権限を持つ役割にいるかどうかによって異なります。

- サービスプロバイダユーザの役割に「パブリックの更新」権限がある場合、詳細ページはテナントが必要なオブジェクトの場合と同じです。
- ユーザのロールに「パブリックの更新」権限がない場合、またはユーザがサービスプロバイダに属していない場合、パブリック オブジェクトの詳細ページに「編集」ボタンはありません。他の詳細ページは、テナントが必要なオブジェクトと同じです。

サポート オートメーション の影響度

サポート環境でのマルチテナンシーの影響は、エンドユーザとアナリストテナントに配置されたテナント制限と役割制限によって異なります。サービスプロバイダは、パブリックおよびテナント固有の両方のデータの読み取り/書き込み許可を管理します。たとえば、アナリストはパブリックキューおよびテナント固有のキューからアシスタンスセッションを処理できますが、アナリストは各テナントで有効になっているライブアシスタンスツールだけを使用できます。

サポート オートメーション アクセス権を持つエンドユーザについては、外部キー (FK) グループが所有テナントを含めるように変更されない限り、エンドユーザの所有テナントのサブテナントでないテナントへの書き込みアクセス権をエンドユーザが保有するように設定しないでください。エンドユーザがログインテナントを選択するか、この基準を満たさないテナントのチケットを介して招待された場合は、サポート オートメーション エンドユーザ クライアントにアクセスしようとする、エラーを受信します。エンドユーザの所有テナントがサービスプロバイダテナントである場合は、この制限は適用されません。

サポート オートメーション アクセス権を持つアナリストについては、外部キー (FK) グループが所有テナントを含めるように変更されない限り、アナリストの所有テナントのサブテナントでないテナントへの書き込みアクセス権をアナリストが保有するように設定しないでください。この基準を満たさないテナントで、アナリストがエンドユーザを処理するか、またはチケットからエンドユーザを招待しようとする、アナリストにエラーが表示されます。

テナントへの読み取りアクセス権のないアナリストとエンドユーザはサポート オートメーション クライアントを起動することができません。アナリストについては、メイン サポート オートメーション タブなどから、この場合は **CA SDM** に警告メッセージが表示されます。

以下の役割を使用してサポート オートメーション ユーザを管理することができます。

サポート オートメーション アナリスト

ライブアシスタンスを使用して、エンドユーザのサポートを提供します。サービスプロバイダは適切なテナントのアクセスを決定し、ライブアシスタンス ツールおよび自動タスクへの読み取り/書き込みアクセスを有効にすることができます。

重要: サービス プロバイダ以外のアナリストが親、兄弟または無関係なテナントへの書き込みアクセス権を持っている場合は、そのテナントの各機能へのアクセスを更新する必要があります。テナントへの読み取りアクセスがないアナリストはサポート オートメーション アナリスト クライアントを起動できず、メインの [サポート オートメーション] タブまたはチケットなどから、警告メッセージが **CA SDM** に表示されます。

サポート オートメーション 管理者

アナリストとエンドユーザにサポート オートメーション 環境を設定します。サービス プロバイダはテナント アクセスを決定し、[リスト] フォームおよび[詳細] フォームにテナント ドロップダウン リストを表示することができます。これらのフォームを使用すると、マルチテナンシー環境でサポート オートメーション データを検索、作成、変更する場合、特定のテナントまたはパブリック データを選択することができます。

注: キュー、プライバシー レベルおよびチャットプリセットのようなオブジェクトはオプションのテナントです。

ナレッジ マネジメント の影響

ナレッジ環境へのマルチテナンシーの影響は、ユーザに適用されるテナント制限によって異なります。

テナント ユーザ

役割が 1 つのテナントに制限される場合、テナントのロゴをデフォルトで代用します。

テナント管理者

管理者が、パブリック データとテナント固有のデータの両方を表示できるようにします。これらのオブジェクトのリスト ページには、リスト行がパブリックかどうかを指定する [パブリック] 列が自動的に表示されます。

ナレッジを検索するときに、フィルタには、[含む] (デフォルト)、[除外フィルタ] および [のみ] という選択肢が含まれた [パブリック データ] ドロップダウン リストが表示されます。

注: 承認プロセス テンプレート、カテゴリ、ドキュメント、ファイル、フォーラムなどのオブジェクトは、テナントが任意です。

ナレッジ カテゴリとドキュメント

ナレッジ ドキュメントおよびナレッジ カテゴリはどちらもテナントが任意です。テナントが任意のオブジェクトとパブリック オブジェクトについて、以下の情報を考慮してください。

- パブリック ナレッジ ドキュメントは、パブリック ナレッジ カテゴリの下にのみ追加できます。
- パブリック ナレッジ カテゴリは、パブリック カテゴリの下にのみ追加できます。
- テナント カテゴリは、パブリック カテゴリおよびテナントのカテゴリの下に追加できます。
- テナント ドキュメントは、テナント カテゴリの下にのみ追加できます。
- パブリック ドキュメントとテナント化されたドキュメントは、パブリック カテゴリに追加できます。

注: ソースとターゲットのテナントが同じ場合、またはターゲットがパブリックの場合のみ、カテゴリの切り取り/コピー/貼り付け機能を使用できます。

リポジトリはテナントが任意として定義されるため、管理者はテナントごとに異なるリポジトリを作成できます。

ドキュメントとイメージが同じテナントに設定されている場合のみ、埋め込みイメージを使用できます。添付ファイルフォルダ、添付ファイル、ドキュメント リンクへの添付ファイルも、テナントが任意として定義されます。

FAQ 評価

テナント ユーザの **FAQ** 評価を表示するときは、パブリック ドキュメントに関する以下の情報を考慮してください。

- パブリック ドキュメントは、テナント ユーザより多くのユーザによって表示されます。

パブリック ドキュメントの **FAQ** 評価は、テナントの特定のドキュメントより高くなります。

- テナントはそれぞれニーズが異なるため、使用パターンはテナントごとに異なります。

CA SDM の [Self-Service] ホーム ページの [上位解決策] には、上位 5 つのパブリック ドキュメントおよびテナントの上位 5 つのドキュメントが表示されます。

[管理] タブの [ナレッジ] - [解決策に関する調査] - [FAQ 設定] を選択することで、上位解決策を設定できます。

ナレッジ レポート カード

ナレッジ レポート カードを使用すると、アナリストと管理者がドキュメント作成、発行、ヒット数、および投票のようなさまざまなメトリックを表示できます。このレポートは、アナリスト、カテゴリ、および組織ごとに所定期間使用します。

ナレッジ レポート カードを使用して 1 つのテナントにアクセスできる役割の情報を提供する場合、データはテナント基準によって制限されます。

Multi-Tenancy の使い方

CA SDM マルチテナンシー機能を管理するには、以下の手順に従います。

テナントの表示

任意のテナント リストからテナントを表示できます。

注: この機能は、マルチテナンシーが（サーバ上またはセットアップ モードのいずれかで）インストールされている場合にのみ使用できます。

テナントを表示するには、以下の手順に従います。

1. [管理] タブで、[セキュリティと役割の管理] を選択します。

2. [テナント] をクリックします。
[テナント リスト] が表示されます。
3. (オプション) [テナント リスト] からテナントを選択します。
[テナントの詳細] ページが表示されます。

注: テナント リストは、[テナント グループの詳細] や [構成アイテムの影響を受けるテナント] などのページにも表示されます。

テナントの作成

製品を使用してテナントを作成できます。

テナントを作成する方法

1. [管理] タブで、[セキュリティと役割の管理] - [テナント] を選択します。
[テナント リスト] ページが表示されます。

注: [セキュリティと役割の管理] - [テナント] オプションは、マルチテナンシーがインストールされている場合（[オン] または [セットアップ]）にのみ使用できます。

2. [新規作成] をクリックします。
[テナントの新規作成] ページが表示されます。
3. 必要に応じて編集可能なフィールドを完了します。

名前

テナントの名前が表示されます。

サービス プロバイダ

テナントがサービス プロバイダであるかどうかを識別します。最初に作成されたテナントは常にサービス プロバイダになります。

テナント番号

(情報のみ) テナント番号が表示されます。このフィールドは、CA SDM では使用されません。

レコード ステータス

テナントをアクティブまたは非アクティブに設定します。

親テナント

このテナントの上に別のテナントを指定して、このテナントをテナント階層におけるサブテナントにします。

サブテナントを許可

このテナントがサブテナントを持つことができるようにします。テナントは設定を変更することができません。

テナントの深さ

(情報のみ) このテナントの深さを指定します。

スーパーテナントグループ

(情報のみ) このテナントと、テナント階層内のすべての上位テナントが含まれる、システム管理のテナントグループを示します。

サブテナントグループ

(情報のみ) このテナントと、テナント階層内のすべての下位テナントが含まれる、システム管理のテナントグループを示します。

外部キーグループ

(情報のみ) このテナントに属するデータ内の SREL から参照できるテナントが含まれる、システム管理のテナントグループを示します。外部キーグループは、スーパーテナントグループと同じです。

関連テナントグループ

(情報のみ) このテナントのスーパーテナントおよびサブテナントグループの両方で構成される、システム管理のテナントグループを示します。

使用条件

テナントの使用条件文を指定します。

ロゴ

テナントロゴファイルの URL を指定します。どの Web イメージタイプでも指定できます。

ロケーション

ロケーションルックアップページを表示します。

連絡先

連絡先ルックアップページを表示します。

注: 連絡先がそれぞれのテナントと関連付けられていない場合、[電子メールアドレス] フィールドと [ポケットベルの電子メールアドレス] フィールドは非アクティブです。

4. [保存] をクリックします。
テナントが作成されます。
5. ウィンドウを閉じます。
6. [テナント リスト] を右クリックし、[更新] をクリックします。
[テナント リスト] が更新され、作成したテナントが表示されます。
7. (オプション) このテナントをユーザ定義テナント グループに割り当てるには、[テナント グループ] タブで [テナント グループの更新] をクリックします。

テナントの編集

[管理] タブからテナントを編集できます。

注: この機能は、マルチテナンシーが (サーバ上またはセットアップ モードのいずれかで) インストールされている場合にのみ使用できます。

テナントを編集する方法

1. [管理] タブで、[セキュリティと役割の管理] を選択します。
2. [テナント] をクリックします。
[テナント リスト] が表示されます。
3. テナントを右クリックし、[編集] をクリックします。
[テナントの更新] ページが表示されます。

注: 既存のテナントを編集すると、[サブテナント] タブと [構成アイテム] タブが表示されます。

4. 適切な変更を加え、[保存] をクリックします。
5. [テナントの更新] ページを閉じます。
[テナント リスト] が表示されます。
6. 右クリックして [更新] を選択します。
更新された [テナント リスト] が表示されます。

テナント階層

テナント階層は、ユーザがテナントに親テナントを割り当てる場合、システムにより作成または変更される構造化されたテナントグループです。テナントは親のサブテナントになり、その階層においてより高いテナント（存在する場合）になります。

注: サービスプロバイダは複数の独立した階層を作成できます。またはまったく作成しないことも可能です。テナント階層のあるシステム内にも、スタンドアロンテナントを定義できます。

通常、サブテナントはスーパーテナント内の一部分を表します。サブテナントは、自身のビジネスルールおよびデータを持つことができます。また、スーパーテナントのデータはサブテナントに読み取り専用方式で自動的に「プッシュ」されます。

CA SDM がサポートするテナント階層の深さは無制限です。ただし、サービスプロバイダは、テナントの総数およびテナント階層の深さ（デフォルトは4レベル）を制限できます。また、サービスプロバイダは、各テナントがサブテナントを持つことができるかどうかを決定します。

注: サービスプロバイダはテナント階層に参加できますが、必須ではありません。サービスプロバイダが親テナントを持つことはできません。

サブテナントの作成

サブテナントを使用すると、組織目的およびデータ共有目的のテナント階層を構築して変更することができます。テナントをテナント階層に配置するには、親テナントをそれに割り当てます。

サブテナントを作成する方法

1. [管理] タブで、[セキュリティと役割の管理] - [テナント] を選択します。

[テナント リスト] が表示されます。

注: [セキュリティと役割の管理] - [テナント] オプションは、マルチテナンシーがインストールされている場合にのみ使用できます。

2. 編集する既存のテナントをクリックするか、または [新規作成] をクリックします。

[テナントの詳細] ページが表示されます。必要なデータまたは変更を入力します。

3. 親テナントを選択します。

注: [親テナント] ドロップダウンには、サブテナントを持つことを許可されたテナントのみが表示されます。

4. [保存] をクリックします。

テナントは親テナントのサブテナントです。

注: テナントがサブテナントである場合は、そのテナントは親テナントのサブテナント グループに属し、そのサブテナントのサブテナントがある場合などでも同様です。親テナントはサブテナントのスーパーテナント グループに加入し、そのスーパーテナントのスーパーテナントがある場合などでも同様です。各テナントは、もう 1 つの関連するテナント グループに加入します。

システム保守テナント グループ

CA SDM は、テナント階層の各テナント（テナントはテナント名）で 3 つのテナント グループを自動的に生成して保守します。

- **tenant_subtenants** (テナント、その子テナント、およびそれらの下位のテナント)
- **tenant_supertenants** (テナント、その親テナント、およびその上位のスーパーテナント)
- **tenant_relatedtenants** (単一の階層全体)

システム保守テナント グループは、ユーザ定義テナント グループと同じように使用できます。ただし、変更できるのはそれらの名前および説明のみです。

テナント グループの表示

テナント グループ情報を表示して、グループ メンバーを表示できます。

注: この機能は、マルチテナンシーが（サーバ上またはセットアップ モードのいずれかで）インストールされている場合にのみ使用できます。

テナント グループ リストを表示する方法

1. [管理] タブで、[セキュリティと役割の管理] を選択します。
2. [テナント グループ] をクリックします。

[テナント グループ リスト] が表示されます。

注: システムによって維持されているテナント グループを表示するか非表示にするかを選択できます。

3. (省略可) リストからテナント グループを選択します。
テナント グループ情報が表示されます。
4. 必要な場合はテナント グループを変更します。

テナント グループの作成

製品を使用してテナント グループを作成できます。

テナント グループを作成する方法

1. [管理] タブで、[セキュリティと役割の管理] を選択します。
2. [テナント グループ] をクリックします。

[テナント グループ リスト] が表示されます。

注: [セキュリティと役割の管理] - [テナント グループ] オプションは、マルチテナンシーがインストールされている場合（[オン] または [セットアップ]）にのみ使用できます。

3. [新規作成] をクリックします。
[テナント グループの新規作成] ページが表示されます。
4. 以下のフィールドを指定します。

テナント グループ名

テナント グループの名前が表示されます。

レコード ステータス

テナント グループをアクティブまたは非アクティブに設定します。

説明

テナント グループの説明が表示されます。

5. [保存] をクリックします。
テナント グループが作成されます。

6. ウィンドウを閉じます。
[テナント グループ リスト] が表示されます。
7. [テナント リスト] を右クリックし、[更新] を選択します。
[テナント グループ リスト] が更新されます。
8. [テナント グループの詳細] ページの [テナントの更新] をクリックして、テナント メンバーをグループに追加します。

テナント グループの編集

テナント グループを編集して、そのメンバーと詳細情報を管理できます。

注: この機能は、マルチテナンシーが（サーバ上またはセットアップ モードのいずれかで）インストールされている場合にのみ使用できます。

テナント グループを編集する方法

1. [管理] タブで、[セキュリティと役割の管理] を選択します。
2. [テナント グループ] をクリックします。
[テナント グループ リスト] が表示されます。
3. テナント グループを右クリックし、[編集] をクリックします。
[テナント グループの更新] ページが表示されます。
4. 適切な変更を加え、[保存] をクリックします。
5. ウィンドウを閉じます。
[テナント グループ リスト] が表示されます。
6. ウィンドウを右クリックし、[更新] を選択します。
更新された [テナント グループ リスト] が表示されます。

テナント データの割り当て

既存のオブジェクトのテナントは **Web** インターフェースから変更できないため、**CA SDM** では既存のオブジェクトの詳細ページの表示バージョンと編集バージョンのどちらでもテナントが同じ形式で表示されます。

テナントされたオブジェクトを編集するとき、編集ページのドロップダウンリストは、ベース オブジェクトやテナント階層においてその上にあるすべてのオブジェクトと同じテナントにより所有されるパブリックな値、またはサービス プロバイダによって所有されるパブリックな値（ドロップダウンリストが **SERVICE_PROVIDER_ELIGIBLE** 属性に適用される場合）に自動的に限定されます。

詳細ページでは、テナントされたオブジェクトに関連付けられたルックアップフィールドに変更はありません。複数のテナントにアクセスできるユーザがテナント化されたテーブルへのルックアップリンクをクリックした場合、**Web** エンジンによってルックアップは属性に適した値に自動的に制限され、バナー メッセージがポップアップ検索またはリスト ページに表示されます。

注: テナント制限は検索フィルタに表示されず、ユーザはそれらを変更できません。

テナントが必要なオブジェクトの作成を要求すると、テナントはセレクト (ルックアップまたはドロップダウン リストのいずれか) になります。

テナント フィールドが空の場合、フィールドに入力することで直接、またはテナントを示す属性（「影響を受けるエンドユーザ」など）を指定することで間接的にテナントの値を指定できます。 インターフェースには以下のサフィックスが表示されます。

(T)

テナントを示す属性を指定します。これは、テナントが必要なテーブルへのルックアップです。

(TO)

オプションでテナントを示す属性を指定します。これは、テナントが任意のテーブルへのルックアップです。

web.cfg プロパティは、これらのインジケータのテキストを制御します。

テナント属性自体を除いて、テナントを示す属性は、**dtlDropdown** マクロを使用して作成された場合でも常にルックアップとして表示されます。

テナント化された値をルックアップするか、テナントを示すフィールドに自動入力すると、CA SDM によりテナントが自動的に設定されます

(SERVICE_PROVIDER_ELIGIBLE フィールドにサービス プロバイダ オブジェクトへの参照を入力した場合のみテナントが設定されません)。テナントが設定されると、テナントを示すフィールドのルックアップは、既存のテナント化されたオブジェクトと同様に制限されます。

注: オブジェクトを保存するまで、テナント フィールドは編集可能なままです。テナントを直接更新することで変更できます。テナントを変更すると、以前のテナントに属するオブジェクトへの参照を含む、テナントを示すフィールドはすべて CA SDM により自動的にクリアされます。

CA SDM では、通常、テナント セレクタは空に初期化されています。この動作は、いくつかの方法で変更できます。

- [クイック プロファイル] などのページから [新規作成] ページを開きます。このページでは、テナントを示すフィールドに値が事前に入力されます。
- [テナントを維持] ユーザ環境設定を設定します。
これは、新しいオブジェクトのテナントを、最後に表示または更新した詳細ページと同じテナント、または最後のリスト ページの検索フィルタ制限と同じテナントに初期化する、新しいユーザ環境設定です。
- テナントを明示的に指定する URL を使用してページを開きます。
これは、事前定義済み URL には用意されていませんが、テナントを指定するメニュー項目またはボタンをサイトで作成可能にするために使用できます。

注: 別の CA Technologies 製品 (CA APM など) またはコマンドラインインターフェースから構成アイテムを作成する場合、オブジェクトはパブリックです。

関連項目:

[テナント化されたオブジェクトの作成](#) (P. 167)

テナント化されたオブジェクトの作成

サービス プロバイダは、案件、リクエスト、変更要求などのオブジェクトにテナント固有のデータを追加できます。[スコアボード] タブから作成されたチケット (インシデントなど) にテナントを追加できます。

インシデントにテナント データを追加する方法

1. [ファイル] - [新規インシデント] をクリックします。
2. 以下のいずれかの手順に従います。
 - a. [テナント] ドロップダウンからテナントを選択します。
 - b. [影響を受けるエンド ユーザ] (またはテナントを示す他のフィールド) をクリックします。
[連絡先の検索] ページが表示されます。ユーザを検索します。
テナントによって検索をフィルタできます。
 - c. [影響を受けるエンド ユーザ] フィールドに名前を入力します。
テナント データは自動的に入力されます。
3. インシデントの作成を続けます。

アクティビティ通知

アクティビティ通知は、通知の内容と、チケットの履歴の各種イベントの通知を受信する連絡先の両方を制御します。

マルチテナンシー環境では、通知ルールはテナントが任意のオブジェクトです。パブリック通知ルールはすべてのチケットに適用されます。テナント化されたルールは、ルールと同じテナントを持つチケット、またはそのサブテナント階層内のテナントにのみ適用されます。テナント制限は、ルール自体で指定された条件に加えて適用されます。

関連項目:

[通知ルールのコピー](#) (P. 168)

通知ルールのコピー

デフォルトの通知ルールは、パブリック オブジェクトとして保存されます。マルチテナンシーがインストールされている場合、各テナントの通知ルールのコピーを作成する必要があります。作成しないと、[連絡先の更新] オプションが制限されます。

通知ルールを更新する方法

1. [管理] タブで、[通知] - [通知ルール] に移動します。
[通知ルール リスト] が表示されます。

2. [シンボル] 列でルールをクリックします。
[通知ルールの詳細] ページが表示されます。
3. [ファイル] - [コピー] をクリックします。
通知ルールの更新を再開します。

リポジトリ

リポジトリ (`doc_rep`) オブジェクトは、テナントが任意です。テナントは、自身のリポジトリを定義でき、添付ファイルなどのオブジェクトのパブリック リポジトリを定義して、ナレッジ ドキュメントを発行できます。各テナントに自身のデフォルト リポジトリを設定でき、デフォルトのパブリック リポジトリを指定できます。

すべての添付ファイルは、パブリックであるか、または 1 つのテナントと関連付けられます。テナントに自身のデフォルト リポジトリがない場合、テナント化されたそのオブジェクトのデフォルトとしてパブリック リポジトリが表示されます。

第 6 章：統合検索による複数の検索エンジンの統合

統合検索機能により、CA SDM ビルトイン ナレッジ ベースの機能が拡張されます。

- ナレッジ検索を実行すると、内部ナレッジ データベースの検索結果に外部検索エンジンの検索結果が追加されます。CA Open Space、Microsoft SharePoint、および Google 用の検索アダプタ設定が標準で用意されています。
- 統合検索のアーキテクチャは柔軟です。CA の統合検索 SDK を使用してカスタム検索アダプタを作成することにより、他の検索エンジンのサポートを追加できます。SDK インターフェースでは、統合検索による拡張に関する情報とサンプル ソース コードが提供されます。
- CA SDM チケットおよびナレッジ記事に含まれる情報を外部検索エンジンで検索することもできます。新しい Crawler Surface コンポーネントにより、外部検索エンジン クローラが CA SDM 情報を容易に検出できるようになります。クローラはこの情報をクローラのリポジトリに格納します。インデックスが作成されたこの情報は、統合検索を使用して検索できます。チケットおよびナレッジ記事の添付ファイルもサポートされています。

統合検索機能の主要なコンポーネントは、以下のとおりです。

- 統合検索の設定
- クローラの設定
- SDK カスタム検索アダプタ

統合検索の設定

統合検索機能は、以下のコンポーネントで構成されています。

UI コンポーネント

CA SDM アナリストのユーザが検索引数を入力し、検索リクエストを統合検索サーバに送ることができます。

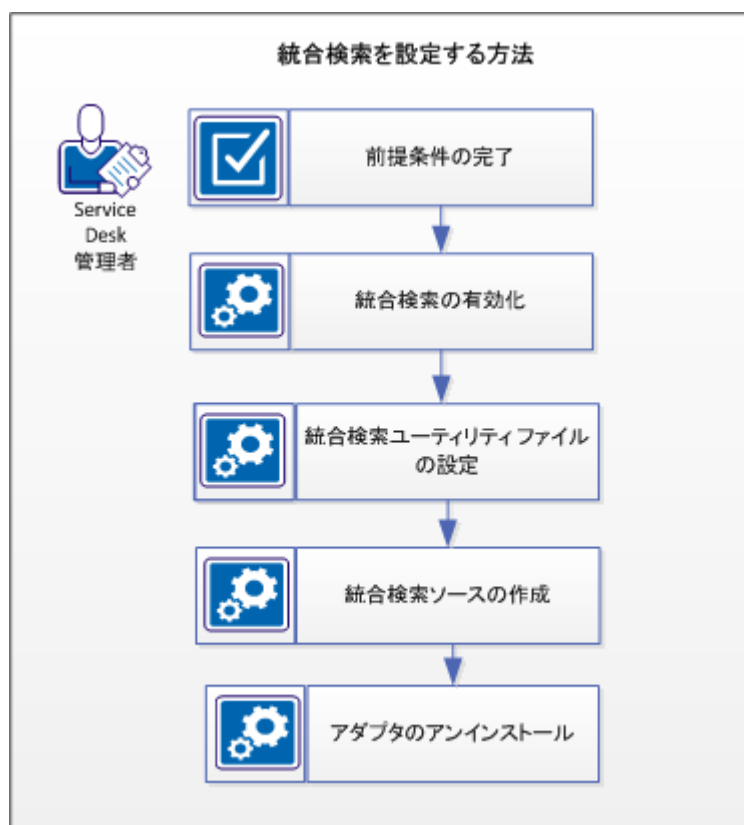
CAFedSearch サークレット

統合検索機能のメイン コンポーネントであり、REST インターフェースを使用します。統合検索サーブレットは、CA SDM アプリケーション内の専用 Tomcat インスタンスで実行されます。

プラグイン検索アダプタ

プラグイン検索アダプタは、CA SDM アプリケーションを外部検索エンジンに接続するインターフェースとして機能し、一般的な検索リクエストを検索エンジン固有の形式に変換して、検索エンジン呼び出します。統合検索サーブレットは、設定された検索エンジンの結果を CA SDM UI コンポーネントに返します。

以下の図は、CA SDM アプリケーションで統合検索を設定する方法を示しています。



次の手順に従ってください：

1. [前提条件の完了](#) (P. 174)
2. [統合検索の有効化](#) (P. 175)
3. [統合検索ユーティリティファイルの設定](#) (P. 176)
4. [CA SDM での統合検索ソースの作成](#) (P. 183)

前提条件の完了

以下の前提条件を満たしている必要があります。

- CA SDM アプリケーションのインストール時に、統合検索の設定ウィザードで[統合検索]オプションが選択されていることを確認します。
- 統合検索に使用する検索エンジンを検討し、決定します。
- Google プラグイン検索アダプタを設定するためのアクティブな Google アカウントがあることを確認します。 Google API キーおよび Google カスタム検索エンジン ID も必要です。詳細については、Google カスタム検索エンジン (<https://www.google.com/cse/all>) を参照してください。
- SharePoint サーバ上の IIS が基本認証で設定されていることを確認します。Microsoft SharePoint アダプタでは、基本認証が必要です。デフォルトでは、SharePoint での基本認証はオフになっています。SharePoint で基本認証を有効化する方法の詳細については、Microsoft SharePoint のマニュアルを参照してください。

注: IIS の _vti_bin の基本認証を有効にしてください。

- CA Open Space と統合するには、バージョン 2.0 SP1 のオンプレミス ソリューションが必要です。詳細については、CA Open Space のマニュアルを参照してください。CA Open Space SaaS 製品は、現時点ではサポートされていません。

統合検索の有効化

CAFedSearch サーブレットと FSCrawl サーブレットをホストするために、専用の Tomcat インスタンスがインストールされます。統合検索 Tomcat は、Daemon Manager によって制御されます。この Tomcat は、CA SDM が実行またはシャットダウンされると、それに合わせて自動的に起動または停止されます。

統合検索 (FS) Tomcat で設定するインストール オプションは、以下のとおりです。

統合検索の設定

CA SDM アプリケーションをインストールする際にこのオプションが選択されていることを確認します。Tomcat オプションはこのオプションを選択した後にのみ使用可能です。

Tomcat ポート

統合検索 Tomcat ポートを指定します。デフォルト ポートは 8040 です。

Tomcat シャットダウン ポート

統合検索 Tomcat のシャットダウン ポートを指定します。デフォルト ポートは 8045 です。

統合検索用の設定 XML ファイルの生成

統合検索を設定するため、および編集エラーを減少させるために、ユーティリティ ファイルの `fs_adapters_cli` が用意されています。Windows 用の バッチ ファイルと、Linux および UNIX 用のシェルスクリプトが提供されています。ユーティリティ ファイルは Java アプリケーションで、2 つの Jar ファイルに含まれています。

CA Open Space、Google、および SharePoint アダプタ用の 3 つのテンプレート ファイルが提供されています。 `adapters-config.xml` ファイルは、ユーティリティへの入力と出力の両方に使用されます。 `adapters.properties` ファイルはユーティリティへの入力に使用されます。このファイルは、アダプタに関して必要なすべての設定パラメータを保持します。 `jfedsearch.log` ファイルには、ログ ファイル情報が含まれます。

`fs_adapters_cli` ユーティリティは、`adapters-config.xml` ファイルを設定するために使用されます。ユーティリティ ファイルは、`adapters-config.xml` のエントリを追加または削除することによって、アダプタをインストールおよびアンインストールします。個々のアダプタの XML 設定ファイルが生成されます。その後これらのファイルは、`<import>` Bean ディレクティブによって `adapters-config.xml` に含められます。必ず `adapters-config.xml` のクリーンコピーを取っておいてください。

- アダプタをインストールする場合、アダプタの登録およびインポート用の 2 つのファイルが `adapters-config.xml` ファイルに追加されます。
- アダプタをアンインストールする場合、アダプタの登録およびインポート用の 2 つのファイルが `adapters-config.xml` ファイルから削除されます。

ユーティリティ ファイルの使用の詳細については、「統合検索ユーティリティ ファイル」および「検索アダプタを設定するためのユーティリティ ファイルの呼び出し」を参照してください。

統合検索ユーティリティファイル

fs_adapters_cli ユーティリティ ファイルは、CA SDM \$NX_ROOT¥samples¥cafedsearch ディレクトリにあります。この場所には、以下のユーティリティ ファイル コンポーネントがあります。

- スクリプト ファイル :
 - fs_adapters_cli.bat (Windows 用)
 - fs_adapters_cli.sh (Windows 以外)
- JAR ファイル :
 - fs_adapters_config_cli.jar
 - fs_adapters_config_schema.jar
- テンプレート :
 - openspace-tmpl.xml
 - google-tmpl.xml
 - sharepoint-tmpl.xml
- プロパティ :
 - adapters.properties

統合検索ユーティリティ ファイルをインストールするには、以下のコマンドを実行します。

```
fs_adapters_cli -i -k <key> -b <bean> -t <filename> -p <filename> -o <filename> [-c <filename>]
```

ユーティリティ ファイルに関するヘルプを参照するには、fs_adapters_cli - h オプションを使用します。以下の属性オプションを使用できます。

-b (オプション)

アダプタをマップするための属性値です。アダプタ Bean の実際の ID を参照します。指定しない場合は、-k に指定した値が -b の値として使用されます。

-c (オプション)

設定されたすべてのアダプタが含まれるメイン XML ファイルです。

-h (オプション)

統合検索ユーティリティのヘルプを提供します。

-i

アダプタをインストールするために使用されるオプションを指定します。

-k

アダプタのキー属性を指定します。

-o

生成される出力 XML ファイル名を指定します。XML テンプレートと SharePoint プロパティ ファイルのマージされたコンテンツを作成および更新するための XML ファイルの名前です。

-p (オプション)

アダプタ定義 XML テンプレートとマージするプロパティ ファイル名を示します。

-t

アダプタを定義するための XML テンプレート ファイルの名前を指定します。

-u

アダプタをアンインストールするためのアダプタ XML ファイルの名前を指定します。

検索アダプタを設定するためのユーティリティファイルの呼び出し

検索エンジンには、特別に作成されたプラグイン アダプタが必要です。プラグイン検索アダプタは、一般的な検索リクエストを検索エンジン固有の形式に変換し、検索エンジン呼び出して、検索リクエストを返します。

注: CA SDM がマルチテナンシーに対して設定されている場合は、使用しているテナントが検索エンジンに渡されます。統合検索は、マルチテナンシーをサポートしています。これを利用して、単一の SharePoint 実装でテナントによってデータを分離できます。

重要: `adapters.properties` ファイルの値にはアンパサンドまたはスペースを使用しないでください。

次の手順に従ってください:

1. パスワード暗号化ユーティリティを使用して、検索アダプタのパスワードを暗号化します。パスワードを暗号化するには、以下の CA SDM ディレクトリに移動します。

```
$NXROOT¥bin
```

2. 暗号化されたパスワードを生成するには、以下のコマンドを実行します。

```
encrypt_pwd [-e] <search engine password>
```

デフォルト オプションは、`-e` です。

3. 以下の CA SDM ディレクトリから `adapters.properties` ファイルを開きます。

```
$NX_ROOT¥samples¥cafedsearch
```

4. `adapters.properties` ファイルを編集します。設定するアダプタ用の適切なパラメータを指定してください。

5. SharePoint の場合は、`adapters.properties` ファイルの以下の値を更新します。

```
sharepoint_username=
```

SharePoint アクセス用のユーザ名を入力します。

```
sharepoint_password=
```

手順 1 に示されている SharePoint アクセス用の暗号化されたパスワードを入力します。

```
sharepoint_hostname=
```

ホスト名を入力します。

sharepoint_domainName=

ドメイン名を入力します。

sharepoint_protocol=

通信プロトコル (http または https) を入力します。

sharepoint_portNumber=

ポート番号を入力します。デフォルトは 80 です。

6. Google の場合は、adapters.properties ファイルの以下の値を更新します。

google_googleCx=

使用する Google カスタム検索アカウントを決定するために Google が使用する一意のキー値を入力します。

google_googleApiKey=

Google によるアプリケーションの ID の決定を支援する一意のキー値を入力します。API コンソールでキーを取得するには、JSON/Atom Custom Search API をアクティブにします。この API は、Simple API Access 用の新しい API キーを提供します。

7. CA Open Space の場合は、adapters.properties ファイルの以下の値を更新します。

openspace_protocol=

通信プロトコル (http または https) を入力します。

openspace_portNumber=

CA Open Space のポート番号を入力します。デフォルトは 8686 です。

openspace_default_tenant_userName=

CA SDM がマルチテナンシーに対して設定されていない場合は、CA Open Space で検索を実行するためのユーザ名を入力します。

openspace_default_tenant_password=

CA Open Space の暗号化されたパスワードを入力します。詳細については、「Step1」を参照してください。

openspace_default_tenant_companyHost=

テナントの会社ホストの詳細を入力します。

- a. CA SDM マルチテナンシーの場合は、各テナントのエントリを openspace-tmpl.xml に追加します。

たとえば CA SDM に「Tenant 1」というテナント名が含まれている場合は、openspace-tmpl.xml ファイルで以下の値を指定する必要があります。

```
<entry key="Tenant1">
    <bean
class="com.ca.ServicePlus.cafedsearch.adapters.openspace.Op
enSpaceCompanyDetail">
        <property name="userName"
value="$(openspace_tenant1_userName)"/>
        <property name="password"
value="$(openspace_tenant1_password)"/>
        <property name="companyHost"
value="$(openspace_tenant1_companyHost)"/>
    </bean>
</entry>
```

- b. Tenant 1 用の以下のエントリを adapters.properties ファイルに追加します。

openspace_tenant1_userName=

openspace_tenant1_password=

openspace_tenant1_companyHost=

openspace-tmpl.xml ファイル内のすべての必要なテナントについて、手順 a および b を繰り返します。

8. 設定するアダプタごとに 1 回ずつ fs_adapters_cli を呼び出します。

- CA Open Space アダプタを設定する場合は、以下の例のように Bean 値として OpenSpaceSearchAdapter を指定し、テンプレートとして openspace-tmpl.xml を指定します。

```
fs_adapters_cli -i -k OpenSpace -b OpenSpaceSearchAdapter -t
"openspace-tmpl.xml" -o "openspace.xml"
```

- Google アダプタを設定する場合は、以下の例のように Bean 値として GoogleSearchAdapter を指定し、テンプレートとして google-tmpl.xml を指定します。

```
fs_adapters_cli -i -k Google -b GoogleSearchAdapter -t
"google-tmpl.xml" -o "google.xml"
```

- SharePoint アダプタを設定する場合は、以下の例のように Bean 値として SharePointSearchAdapter を指定し、テンプレートとして sharepoint-tmpl.xml を指定します。

```
fs_adapters_cli -i -k SharePoint -b SharePointSearchAdapter -t  
"sharepoint-tmpl.xml" -o "sharepoint.xml"
```

-k および -o 属性値を任意の名前で変更します。統合検索ユーティリティ ファイルおよび属性の詳細については、「統合検索ユーティリティ ファイル」を参照してください。

9. インストールの後にエラーがある場合は、以下の CA SDM ディレクトリにあるログ ファイルを確認します。

```
$NXROOT¥log¥j fedsearch.log
```

10. 必要に応じて、登録用のユーザ独自の XML ファイルを作成することもできます。アダプタ エントリはすべて、以下のディレクトリにある adapters-config.xml に登録されます。

```
$NX_ROOT¥samples¥cafedsearch
```

11. 登録用のユーザ独自の XML ファイルを作成するために、既存の adapters-config.xml ファイル名のコピーを作成することもできます（オプションの手順）。変更された adapters-config.xml ファイルには、任意の名前を付けてください。たとえば、「xyz.xml」というファイル名にします。

-c オプションと変更された XML ファイル（xyz.xml）を使用してアダプタを登録します。

12. bean.xml <import resource="adapters-config.xml"/> のリソース値を変更します。

13. adapters-config.xml または変更された xyz.xml（手順 11）と以下の CA SDM ディレクトリにあるすべての関連アダプタ固有 XML ファイル（Google 用の google.xml、CA Open Space 用の openspace.xml、および SharePoint 用の sharepoint.xml）をコピーします。

```
$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥cafedsearch¥WEB-INF
```

14. 統合検索 Tomcat インスタンスを再起動します。

```
pdm_tomcat_nxd - c STOP - t FS
```

```
pdm_tomcat_nxd - c START - t FS
```

統合検索アダプタが設定されます。

15. 以下の CA SDM ディレクトリにあるエラー ログ ファイルを検証して確認します。

```
$NX_ROOT¥log¥j fedsearch.log
```

CA SDM での統合検索ソースの作成

CA SDM Web UI は、CAFedSearch サーブレットと疎結合されています。CA SDM で検索ソースを設定して新しいレコードを作成します。

次の手順に従ってください:

1. Service Desk 管理者として CA SDM アプリケーションにログインします。
2. [管理] - [ナレッジ] - [統合管理] - [検索ソース] を選択して、統合検索エンジンを表す新しいレコードを作成します。

検索ソースには、ユーザに対して表示される統合検索ソースの名前が含まれます。

注: コード値は、`adapters-config.xml` 内のエントリのキー値属性と一致している必要があります。

新しいカスタム検索アダプタによるナレッジ ソリューションの検索

新しいカスタム検索アダプタを使用して、CA SDM アプリケーションのナレッジ ドキュメントおよび記事を検索します。

次の手順に従ってください:

1. CA SDM Service Desk 管理者としてログインします。
2. [管理] - [ナレッジ] - [統合検索] - [検索ソース] に移動します。
3. 新しい検索ソースのコード キー値を追加します。
4. [保存] をクリックします。
5. 新しいチケットまたは既存のチケットを使用して [ナレッジ マネジメント] に移動します。
6. 作成したナレッジ ソースを検索します。[フィルタの表示] をクリックし、検索条件を入力して [検索] をクリックします。

検索情報が表示されます。

検索アダプタのアンインストール

検索アダプタをアンインストールするには、`-u` オプションの付いた `fs_search_cli` ユーティリティ コマンドを使用します。以下のユーティリティ ファイル コマンドを使用してください。

```
fs_adapters_cli -u -k <key> -b <bean> [-c <filename>] -f <filename>]
```

`-u`

検索アダプタをアンインストールするには `-u` オプションを指定します。

`-k`

インストール時に入力したキー名値を指定します。

`-b`

インストール時に入力した **Bean** 値を指定します。

`-c`

ユーティリティを使用して検索アダプタを設定しているときに新しい検索アダプタ設定 XML を作成した場合は、その名前を指定します。

`-f`

インストール時に生成された出力ファイル名を入力します。

詳細については、「ユーティリティによる検索アダプタの設定」を参照してください。

たとえば、Google 検索アダプタをアンインストールする場合は、以下の手順を実行します。

次の手順に従ってください:

1. Google 検索アダプタをアンインストールするための `-u` オプション付きのユーティリティ ファイル コマンドを実行します。

```
fs_adapters_cli -u -k Google -b GoogleAdapter -f Google.xml
```

2. `adapters-config.xml` によって Google に関する登録が削除されることを確認して検証します。

3. `google.xml` ファイルが以下の CA SDM ディレクトリから削除されます。

```
$NX_ROOT¥samples¥cafedsearch
```

4. `adapters-config.xml` を以下のディレクトリにコピーします。

```
$NX_ROOT¥samples¥cafedsearch¥WEB-INF
```

この場所から `google.xml` ファイルを削除します。

5. FS Tomcat を再起動します。

```
pdm_tomcat_nxd - c STOP - t FS
```

```
pdm_tomcat_nxd - c START - t FS
```

6. CA SDM UI で、このアダプタ（今回は **Google**）のアクティブな検索ソース エントリを確認します。
7. 他の外部検索アダプタをアンインストールする場合は、手順 1 ～ 6 を繰り返します。

Crawler Surface の設定

クローラは検索エンジンの一部であり、自動的にインターネットを参照して検索語のインデックスを作成します。**Crawler Surface** は、**CA Service Desk Manager** アプリケーションに対する新しい読み取り専用の **Web** ベース インターフェースです。外部検索エンジンは **Java Server Page (JSP)** テクノロジーを使用して情報を検索できます。**Crawler Surface** は、情報をプレーンテキストで提供します。また、チケットおよびナレッジドキュメントへの個別のハイパーリンクも提供します。このハイパーリンクをたどることにより、情報の詳細を参照できます。**Microsoft SharePoint 2010** および **SharePoint 2013** を使用すると、**Crawler Surface** をクロールできます。**Crawler Surface** のメインコンポーネントは、**FSCrawl** サブレットです。

注: クローラに対して公開される **CA Service Desk Manager** 情報の内容は、設定ファイルによってカスタマイズできます。フォームの変更は不要です。

以下の図は、**SharePoint** 用の **Crawler Web Surface** を設定する方法を示します。



次の手順に従ってください：

1. [前提条件の完了](#) (P. 187)
2. [CA Service Desk Manager ユーザの Crawler Surface の作成](#) (P. 187)
3. [Tomcat リモート IP アドレス フィルタの設定](#) (P. 188)
4. [Crawler Surface ユーザ ID の設定](#) (P. 190)
5. [SharePoint クローラの設定](#) (P. 199)

前提条件の完了

Microsoft SharePoint Server 用の Crawler Surface の設定を開始するには、以下の前提条件を満たしておく必要があります。

- CA SDM アプリケーションのインストール時に [統合検索の設定] オプションが有効であることを確認します。
- 検索結果情報にアクセスするための専用ユーザ ID があることを確認します。このユーザ ID によって、Crawler Surface での情報提供が制御されます。CA SDM マルチテナンシー構成の場合は、テナント情報の分離を可能にする追加のユーザ ID を作成します。

CA SDM ユーザの Crawler Surface の作成

CA SDM の設定では、テナントごとに情報を分離するためにユーザ ID を作成します。

Crawler Surface のユーザ ID を作成するプロセスは、一般ユーザ用の CA SDM ユーザ ID の作成と同じです。CA SDM アプリケーションでアクセスタイプと役割が「クローラ」である連絡先を作成します。連絡先の作成の詳細については、CA Service Desk Manager 管理者オンラインヘルプを参照してください。

クローラのアクセスタイプと役割により、CA SDM データへのユーザの読み取り専用アクセスが可能になります。

Tomcat リモート IP アドレス フィルタの設定

SharePoint Server をホストしているリモート システムを指定するように、Tomcat リモート IP アドレス フィルタ設定を変更します。IPV4 および IPV6 アドレスがサポートされます。

Crawler Surface は、CA SDM 情報にアクセスするために Tomcat リモート IP アドレス フィルタ メカニズムを使用します。Tomcat フィルタ メカニズムでは、IP アドレス パターン（CA SDM 管理者が管理しています）を使用して、許可されている IP アドレスを照合します。デフォルトでは、リモート IP アドレス フィルタは、「127.0.0.1」のループバック アダプタ IP アドレスで設定されています。実稼働環境での安全な通信のために、クローラと Crawler Surface の間で SSL を使用することを検討してください。

次の手順に従ってください:

1. CA SDM の設定に応じて、以下のサーバにログインします。
 - 標準：プライマリまたはセカンダリ サーバ
 - 高可用性：アプリケーションサーバ
2. 以下の CA SDM ディレクトリにある web.xml ファイルを開きます。
`$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥fscrawl¥WEB-INF`
3. web.xml ファイルのバックアップを取ります。
4. 「<filter-name>Remote Address Filter</filter-name>」セクションを見つけます。<filter> 内の <param-value> のパターンを変更します。

このパラメータでは、IP アドレス パターンの範囲を指定できます。また、SharePoint をホストするリモート マシンからのアクセスを可能にします。Tomcat リモート IP アドレス フィルタの詳細については、Apache Tomcat のドキュメントを参照してください。
5. XML ファイルを保存します。
6. 統合検索 Tomcat を再起動します。

注: ユーザが統合検索 Tomcat を再起動するとき、ユーザはどんな統合検索も実行できません。
7. Tomcat リモート IP アドレス フィルタ値が変更されます。また、Crawler Surface に、リモート マシンからアクセスできるようになりました。

注: 設定されていない IP アドレスから Crawler Surface にアクセスしないでください。CA SDM UI にリダイレクトされます。

8. Crawler Surface には、他の Web アプリケーションと同様に URL によってアクセスします。SharePoint のログ記録を検証するには、ブラウザに以下の URL を入力します。

`http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/index.jsp?farm=<FarmName>`

注: URL のすべての要素は、大文字と小文字が区別されます。

hostname

統合検索 Tomcat の完全修飾ドメイン名を指定します。

port number

CA SDM アプリケーションをインストールおよび設定したときに統合検索 Tomcat に割り当てられたデフォルトのポート番号を定義します。統合検索 Tomcat へのアクセスに使用されます。

fscrawl

サーブレットの名前を指定します。サーブレット名では大文字と小文字が区別されます。常に「fscrawl」と指定してください。

index.jsp

Crawler Surface 設定のテストに使用できるページの名前を指定します。

<FarmName>

crawler_surface_config.xml 内の各 <farm> に、<sdm_user> エントリが含まれます。認証されたユーザと一致する必要があります。ユーザ認証に失敗している場合、リクエストは CA SDM Web UI にリダイレクトされます。<sdm_user> は、CA SDM オブジェクトマネージャ レベルでのデータ アクセスを制御します。この <farm> レベルのセキュリティ層により、テナントから別のテナントのデータへのアクセスが防止されます。

Crawler Surface ユーザ ID の設定

Crawler Surface を変更するには、`crawler_surface_config.xml` ファイル内の Crawler Surface ユーザ ID を設定します。

重要: ブラウザの言語設定を確認してください。SharePoint の動作は、検索リクエストで使用される言語の影響を受けます。

次の手順に従ってください:

1. インストール設定に応じて、Crawler Surface をホストしている以下の CA SDM サーバにログインします。
 - 標準: プライマリまたはセカンダリ サーバ
 - 高可用性: アプリケーションサーバ

2. 以下の CA SDM ディレクトリにある `crawler_surface_config.xml` を開きます。

```
$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥fscrawl¥WEB-INF
```

3. `crawler_surface_config.xml` ファイルのバックアップを取ります。

重要: 実稼働サーバに最終的な変更を移植する前に、テスト環境で XML ファイルのすべての変更を実施します。

4. 元のファイルで、各 `<farm>` セクション下の `<sdm_user>CHANGE_THIS</sdm_user>` を見つけて、`CHANGE_THIS` を以前に作成したクローラ ユーザ ID に置換します。
5. 必要に応じて、XML オブジェクト属性をさらに変更および制限できます。

注: 詳細については、「Crawler Surface XML 設定ファイル」を参照してください。

6. XML ファイルを保存します。
7. ファイルを再ロードするために統合検索 Tomcat を再起動します。

Crawler Surface XML ファイルが変更されます。

Crawler Surface XML 設定ファイル

crawler_surface_config.xml ファイルには、以下の XML セクションが含まれています。

<objects>

Crawler Surface がオブジェクトに関して公開するオブジェクトおよび属性に関する情報を指定します。objects セクションでは、クローラに公開される各オブジェクトタイプの詳細ページのレイアウトについて説明します。このセクションは、個別のレコードの選択内容を制御しません。<objects> セクションはログイン情報 セクションのコレクションです。

各オブジェクトはログイン情報 セクションで定義されます。これらのオブジェクトのデフォルト指定は次のように指定されます。

KD

ナレッジ ドキュメントを指定します。

chg

変更要求を指定します。

iss

案件を指定します。

in

インシデントを指定します。

pr

問題を指定します。

cr

リクエストを指定します。

XML ファイルには、CA SDM で詳細ページの <head> セクションを作成する以下のセクションが含まれます。

<name>

公開されるオブジェクトの Majic オブジェクト名を指定します。

<note>

オブジェクトの簡単な説明用の場所を指定します。この要素はドキュメント目的のみです。Crawler Surface はこの要素を無視します。

<last_mod_dt>

最終変更日時を格納する属性名を指定します。このタイムスタンプは検索エンジン クローラに公開されるので、検索エンジンはレコードが更新されたかどうかを判断できます。多くのクローラは増分クロール中にこのタイムスタンプを使用します。更新されたタイムスタンプにより、レコードが最後にクロールされた後にレコードが変更されたことがわかります。レコードが最後のクロール以降更新されていない場合、検索エンジン クローラはクロールをスキップします。

<title>

詳細ページのタイトルに使用される属性を指定します。検索エンジンは検索結果で返されるドキュメントのタイトルとしてこの要素を使用します。この要素エントリは、詳細ページの <head> 内の HTML <title> タグを生成します。ナレッジ ドキュメントについては、「Title」がナレッジ ドキュメントのデフォルトのタイトルになります。概要は、インシデント、問題、リクエスト、変更要求、および案件のタイトルに使用されます。

<meta_data>

メタデータとして公開される 1 つ以上のプロパティを指定します。メタデータは、検索エンジンがそのインデックスにドキュメントの追加の特性を格納することを可能にします。メタデータは直接検索されませんが、検索結果をフィルタするときに使用されます。このセクションは、詳細ページの <head> 内の HTML <meta> タグを生成します。

<meta_data> セクション内のエントリにはそれぞれ 1 つ以上の <property> エントリが含まれます。<property> 要素はそれぞれ <name> 要素および <content> 要素から構成されます。

<name>

メタデータ プロパティの名前を指定します。

<content>

メタデータの値として使用されるオブジェクトの属性を指定します。

<property> の <name> と <content> 要素の各ペアは、HTML <meta> タグを生成します。検索エンジンクローラはデフォルトでは以下の 2 つのメタデータ プロパティを使用します。

説明

ドキュメントの短い概要を格納する検索エンジンのメタデータ プロパティを指定します。

作成者

ドキュメントの作成者を指定します。

CASDMTENANT メタデータ プロパティも各オブジェクトに対してデフォルトで設定されます。このプロパティは CA SDM 固有のメタデータ プロパティです。CA SDM がマルチテナンシーに対して設定されている場合、Crawler Surface は、検索エンジンのクローラにオブジェクトのテナント名を公開するためにこのプロパティを使用します。後ほど、統合検索中に、検索エンジンから返された結果は、このメタデータ プロパティに基づいてフィルタされます。

XML ファイルには、CA SDM で詳細ページの **<body>** セクションを作成する以下のセクションが含まれます。

<additional_attributes_to_index>

Crawler Surface が公開するオブジェクトからの属性のリストを示します。複数のエントリを入力する場合は、カンマおよびスペースで区切ります。たとえば、「**PROBLEM, RESOLUTION, SD_ASSET_ID.name**」のように入力します。

<activity_logs>

アクティビティ ログがあるオブジェクトのアクティビティ ログからの Crawler Surface によって公開される情報を示します。 **<activity_logs>** セクションにはログイン情報、**<select_criteria>**、**<rel_attr>** および **<attributes>** の要素が含まれます。

ログイン情報

オブジェクトのアクティビティ ログ エントリが含まれるオブジェクト名を指定します。たとえば、以下のアクティビティ ログ オブジェクトです。

- インシデント、問題およびリクエストは *alg* です。
- 変更要求は *chgalg* です。
- 案件は *issalg* です。
- ナレッジ ドキュメントは *O_COMMENTS* です。

<select_criteria>

公開されるアクティビティ ログ オブジェクトをフィルタすることを可能にします。この要素は頻繁に発生する単語を減少させることによりユーザの検索結果の関連性を増加させるのに重要です。たとえば、*chgalg* の **<select_criteria>** には以下の Magic Where 節が含まれます。

```
"type IN ('ST', 'UPD_RISK', 'CB', 'RS', 'LOG', 'TR', 'ESC', 'NF', 'UPD_SCHED')"
```

この基準は、ユーザがコメントを入力することを可能にするアクティビティ ログ エントリのみを含み、初期またはドキュメントの添付のような固定テキストを持ったアクティビティ ログ エントリを除去します。

<rel_attr>

アクティビティ ログ エントリとその親オブジェクトを関連付ける方法を指定します。<rel_attr> サブセクションには <parent_obj_attr> および <join_attr> 要素が含まれます。

<parent_obj_attr>

親オブジェクトに SREL（または外部キー ポインタ）が含まれるアクティビティ ログの属性を示します。たとえば、change_id は chgalg の属性です。

<join_attr>

<parent_obj_attr> に格納される親オブジェクトの関連付け属性 (Rel Attr) を示します。たとえば、chgalg の <join_attr> は ID です。以下のコマンドの使用によりこれらの値を確認できます。

```
bop_sinfo -df chgalg
```

bop_sinfo -df chgalg コマンドの使用によりこれらの値を両方とも確認できます。その出力は、change_id の値が SREL -> chg.id で、ISS が SREL -> iss.persistent_idであることを示します。

<attachments>

このサブセクションは、親オブジェクトと共に添付ファイルのコンテンツのインデックスを作成できるように、検索エンジンのクローラに添付ファイルを公開することを可能にします。<attachments> セクションは、添付ファイルがあるオブジェクトに対してのみ許可されます。

添付ファイルは Crawler Surface によって特別な方式で処理されます。Crawler Surface からクローラに各添付ファイルのコンテンツを送信するのではなく、Crawler Surface はその代りに、CA SDM から添付ファイルをダウンロードするためにクローラが従うことができるハイパーリンクを公開します。後ほど、統合検索中に、添付ファイルが検索結果に含まれている場合、ハイパーリンクをクリックすると、直接添付ファイルが表示されるのではなく、親オブジェクトがユーザに表示されます。

<attachments> セクションには ログイン情報、<rel_attr>、<attmnt_id>、および <is_parent_updated> 要素が含まれます。

ログイン情報

この要素は、添付ファイルをその親オブジェクトにリンクする Majic オブジェクトを指定します。

<rel_attr>

このサブセクションはアクティビティ ログでの動作と同じ動作をします。親オブジェクトを添付ファイルにリンクするこのオブジェクトに親オブジェクトを関連付ける方法を指定します。

<attmnt_id>

この要素は、添付ファイルを指しているこのリンク オブジェクトの属性を指定します。

<is_parent_updated>

Crawler Surface に対してオブジェクトの最終変更日を公開する方法を指定します。ナレッジ ドキュメント (KD) のような一部のオブジェクトに対して添付ファイルが追加される場合、ナレッジ ドキュメントの最終変更日は更新されません。検索エンジンが増分クロールを実行している場合、最終変更日は重要です。

<configuration_items>

構成アイテムのリストが含まれるオブジェクトに使用されます。このセクションには ログイン情報、<rel_attr>、および <attributes> 要素が含まれます。

ログイン情報

アクティビティ ログと添付ファイルでの動作と同じ動作をします。

<rel_attr>

アクティビティ ログと添付ファイルでの動作と同じ動作をします。

<attributes>

この要素は添付ファイルでの動作と同じ動作をします。

<multi-farm_datasets>

<objects> セクションの後に <multi-farm_datasets> セクションがあります。<objects> セクションは Crawler Surface によって公開できる CA SDM オブジェクトおよび属性を定義しますが、<multi-farm_datasets> はレコードの選択方法を指定します。<multi-farm_datasets> セクションは <farm> セクションのコレクションです。

<farm>

<farm> セクションはそれぞれ、クローラに公開される CA SDM 情報を制御します。クローラが設定される場合、<farm> セクションは URL で指定されます。<farm> セクションで指定された情報のみが、クローラに公開されます。各 <farm> セクションには <name>、<data_sets>、および <sdm_user> 要素が含まれます。<name>

注: この値では、大文字と小文字が区別されます。

<data_sets>

公開されるオブジェクトおよびそれらのレコードの選択方法を指定します。このサブセクションには 1 つ以上の ログイン情報 要素が含まれます。オブジェクト要素にはそれぞれ <name> および <select_criteria> 要素が含まれます。

<name>

<objects> セクションで定義される ログイン情報 を参照します。

<select_criteria>

この要素は、オブジェクトのレコードを選択するために使用される Majic を指定します。

<sdm_user>

この要素は、このファームにアクセスするときに使用する必要がある CA SDM ユーザ ID を指定します。ユーザ ID は、アクセス タイプと役割が「クローラ」である必要があります。

sdm_domsrvr_name

大量のインデックス データに対しては、Crawler Surface 用のオブジェクト マネージャを割り当てます。デフォルトは、domsrvr です。

sharepoint_properties_file

この値は、デフォルトで以下の CA SDM ディレクトリにある SharePoint プロパティ ファイルの名前です。

`NX_ROOT\CATALINA_BASE_FS\lib`

CA SDM がマルチテナンシーに対して設定されている場合に統合検索と Crawler Surface の両方によって使用される設定パラメータが含まれます。

注: CA SDM がマルチテナンシーに対して設定されている場合、このファイル内の sharepoint_version パラメータを更新して、使用している SharePoint のバージョンを反映させてください。

<list_form_number_of_records_per_object>

このパラメータは、Crawler Surface がオブジェクトのリスト ページで示すハイパーリンクの数を設定するために使用します。

<send_wait_timeout>

この値は、Crawler Surface がオブジェクト マネージャからの応答を待つ時間（秒単位）を制御します。この時間が経過するとタイムアウトになります。

SharePoint クローラの設定

SharePoint のコンテンツをクロールおよび検索するようにクローラを設定します。

クローラは高スループットを実現するマルチスレッドアプリケーションですが、CA SDM のパフォーマンスを低下させる場合があります。これを回避するには、以下の手順が実行されていることを確認します。

- Crawler Surface に同時にアクセスする SharePoint クローラの数に常時制限されるように設定します。
- SharePoint クローラ影響ルールを使用してクローラを調整します。
- 1 日のうちでピーク時以外の時間帯にクローラが実行されるようにスケジュールを設定します。
- crawler_surface_config.xml でオブジェクト マネージャの <sdm_domsrvr_name> を Crawler Surface に割り当てます。詳細については、「Crawler Surface XML 設定ファイル」を参照してください。
- CA SDM 高可用性の場合は、アプリケーション サーバ全体を Crawler Surface に割り当てます。

次の手順に従ってください：

1. [SharePoint でのコンテンツ ソースの作成](#) (P. 200)
2. [クローラ ルールの作成](#) (P. 201)
3. [SharePoint でのクローラの実行](#) (P. 202)
4. [SharePoint でのメタデータの設定](#) (P. 203)
5. [SharePoint でのクローラ データの確認](#) (P. 204)

SharePoint でのコンテンツソースの作成

注: SharePoint に固有の設定の名前は、使用している SharePoint のバージョンに依存して変わる可能性があります。SharePoint でのコンテンツソース作成の詳細については、Microsoft SharePoint のマニュアルを参照してください。

SharePoint クローラが処理するコンテンツのタイプを識別するためのコンテンツソースを作成します。

次の手順に従ってください:

1. Microsoft SharePoint の全体管理コンソールにログインします。
2. [サービス アプリケーションの管理] - [Search Service Application] をクリックします。
3. 新しいコンテンツソースを作成するために、[コンテンツソース] をクリックします。
4. [名前] にコンテンツソースのデータ名として「CA SDM」と入力します。
5. [コンテンツソースの種類] を [Web サイト] に設定します。
6. [開始アドレス] に以下の URL を入力します。
`http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/listObject.jsp?farm=<Farm Name>`
7. クローラが Crawler Surface 以外をクロールすることを防ぐために、ページの深さを 2、サーバホップを 1 に制限することを確認してください。これは、添付ファイルをクロールできる最小推奨値です。
8. [保存] をクリックします。

クロール ルールの作成

クロール ルールにより、SharePoint の Web Crawler Surface URL のクロール 方法が定義されます。以下のクロール ルールを定義します。

- SharePoint に Crawler Surface をクロールさせるクロール ルール。
- SharePoint が添付ファイルにアクセスすることを可能にするクロール ルール。

次の手順に従ってください:

1. Microsoft SharePoint の全体管理コンソールにログインします。
2. [サービス アプリケーションの管理] - [Search Service Application] をクリックします。
3. [クロール ルール] をクリックします。新しいクロール ルールを作成します。
4. ブラウザに以下の URL を入力します。

`http:// <sdmhostname>:<FS_Tomcat_Port>/fscrawl/*farm=<farm-name>*`

重要: Crawler Surface URL は大文字と小文字を区別します。SharePoint では、大文字のホスト名が小文字に変更されます。SharePoint 2010 の場合は、[大文字と小文字を区別する] チェック ボックスがオンになっていることを確認します。

5. クローラを設定するために、[このパスにあるアイテムをすべて含める] をオンにします。
6. [複合 URL (疑問符 (?) が含まれる URL) をクロールする] チェック ボックスをオンにします。
7. [別のコンテンツ アクセス アカウントを指定する] をオンにします。
8. Crawler Surface の CA SDM ユーザ アカウント名およびパスワードを入力します。
9. CA SDM 添付ファイル用の 2 番目のクロール ルールを作成します。

`http://<sdmhostname>:<FS_TOMCAT_PORT>/CAisd/*`

10. デフォルト認証を指定します。

注: Crawler Surface は、ベーシック認証を使用します。CA SDM リポジトリ デーモンは、SharePoint によって直接サポートされない、独自の BOPSID セキュリティを使用します。任意のユーザ ID およびパスワードを指定するか、[匿名アクセス] をオンにします (使用しているバージョンの SharePoint でこのオプションを利用できる場合)。

- SharePoint 2013 の場合は、[別のコンテンツ アクセス アカウントを指定する] をオンにします。 [匿名アクセス] オプションをオンにします。
- SharePoint 2010 の場合は、デフォルト コンテンツ アクセス アカウント (NT AUTHORITY\NETWORK SERVICE) を選択します。

Microsoft SharePoint のクローラ ルールが作成されます。

SharePoint でのクローラの開始

SharePoint のコンテンツ ソースのフル クロールまたは増分クローラを開始して、検索コンテンツのインデックスを作成します。

次の手順に従ってください:

1. Microsoft SharePoint の全体管理ページに移動します。
2. [サービス アプリケーションの管理] - [Search Service Application] をクリックします。
3. [コンテンツ ソース] をクリックします。 SharePoint Crawler Surface に対して設定したコンテンツ ソースを選択します。
4. [フル クロールの開始] または [増分クローラの開始] を選択します。

フル クロールでは、コンテンツ ソースのすべてのコンテンツがクローラされます。フル クロールは、増分クローラよりも完了までに時間がかかり、より多くのリソースを使用します。

増分クローラでは、インデックスは完全なまま維持され、最後に成功したクローラ以降に追加または変更されたコンテンツのみクローラされます。詳細については、Microsoft SharePoint のマニュアルを参照してください。

SharePoint でのメタデータの設定

注: このトピックは CA SDM マルチテナンシー環境に適用可能です。

クローラは、CA SDM メタデータを検出すると、クロールされたプロパティとして SharePoint にメタデータを格納します。これらのプロパティは、CA SDM Crawler Surface の初期のフル クロール中に検出されます。 SharePoint クローラはメタデータを検出し、クロールされたプロパティを作成します。

メタデータは、<head> セクションの <meta> タグを使用して、追加の情報を詳細ページでクローラに渡すために使用されます。 この情報は検索およびフィルタリングに使用可能です。 CA SDM がマルチテナンシーに対して設定されている場合、Crawler Surface はテナント メタデータ情報のみを公開します。

統合検索を実行すると、結果を適切にフィルタするためにテナント名が検索エンジンに渡されます。

次の手順に従ってください:

1. Microsoft SharePoint の全体管理コンソールにログインします。
2. [サービス アプリケーションの管理] - [Search Service Application] - [メタデータ] (SharePoint 2010) または [検索スキーマ] (SharePoint 2013) をクリックします。
3. SharePoint のクロールが CA SDM データで成功することを確認します。
4. [管理プロパティ] をクリックします。
5. [新しい管理プロパティ] をクリックします。
6. プロパティ名として「CASDMTENANT」と入力します。
「CASDMTENANT」は、CA SDM オブジェクトのテナント名を示しています。 サブ テナント情報は表示されません。
7. [プロパティの種類] として [テキスト] を選択します。
8. 下へスクロールします。 [マッピングの追加] をクリックします。
9. クロールプロパティの「CASDMTENANT」を検索して選択します。
10. [OK] をクリックして新しい管理プロパティを保存します。

SharePoint のメタデータが設定されます。

SharePoint でのクローラ データの確認

検索結果を表示するために SharePoint のクローラ データを確認します。

次の手順に従ってください:

1. CA SDM Service Desk 管理者としてログインします。
2. 新しいチケットまたは既存のチケットの [ナレッジ マネジメント] タブをクリックします。
3. SharePoint 検索ソースを選択します。
4. 検索キーを入力します。 [検索] をクリックします。
クローラによって検索結果が表示されます。

トラブルシューティング

Crawler Surface には、通常使用される一連のログ ファイルがあります。

1. 統合検索のデバッグを有効にする場合は、以下の CA SDM ディレクトリに移動します。

```
$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥cafedsearch¥WEB-INF
```

2. log4j.properties ファイルを開き、デバッグ モードへの情報を変更します。

3. fscrawl のデバッグを有効にするには、以下の CA SDM ディレクトリに移動します。

```
$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥fscrawl¥WEB-INF
```

4. log4j.properties ファイルを開き、デバッグ モードへの情報を変更します。

5. SharePoint Crawler Surface の設定時に発生した構文エラーを修正するには、以下の CA SDM ディレクトリにある jfscrawl ログ ファイルを開きます。

```
$NX_ROOT¥Logs ディレクトリ
```

6. 構文エラーを見つけた場合は、XML ファイルを修正し、統合検索 Tomcat を再起動します。ログは、以下の場所にあります

```
$NX_ROOT¥logs¥jfscrawl.log
```

たとえば、<meta_data> タグを間違って壊した場合、ログには以下のエラーが示されます。

```
08/06 15:43:52.624 [pool-2-thread-1] ERROR FSCrawlApplicationListener 302
XmlException::Problem loading
config_file::C:¥PROGRA~2¥CA¥SERVIC~1¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥fscrawl¥WEB-INF¥crawler_surface_config.xml:274:8: error: </meta_dataxxxx> does not
close tag <meta_data>
```

```
08/06 15:43:52.625 [pool-2-thread-1] ERROR FSCrawlApplicationListener 144
crawler_surface_config.xml could not be loaded, cannot read.
```

7. 構文エラーがない場合は、以下のメッセージが表示されます。

```
08/06 15:46:27.924 [pool-2-thread-1] INFO FSCrawlApplicationListener 58 fscrawl
context had been loaded successfully.
```

8. CA SDM へのアクセスを試みるまでは示されていなかった他のすべてのエラーを修正します。

たとえば、`crawler_surface_config.xml` の `<additional_attributes_to_index>` 要素内のインシデントに対して不明な属性 `xxxxx` を公開するようにリクエストされたとします。Crawler Surface アプリケーションはエラーを検出しません。しかし、Crawler Surface がオブジェクトマネージャにリクエストを送信するときに、エラーが検出され、`stdlog.x` ファイルで以下のようにレポートされます。

```
08/06 15:51:23.92 SDMSERVER domsrvr 10860 ERROR domset.c 8049 Unknown attribute
"xxxxx" requested from domset MLIST_STATIC of factory
```

9. `bop_sinfo -d` コマンドを使用してエラーを解決します。
10. `crawler_surface_config.xml` ファイルを変更します。
11. 統合検索 Tomcat を再起動します。

Crawler Surface オブジェクトはエラーなしで設定されます。

SDK インターフェースによる新しいカスタム アダプタの作成

重要: 代替のカスタム アダプタを作成および展開するために、CA 統合 SDK のサンプル ソース コードが用意されています。ただし CA サポートは、実際のカスタム コードを記述するためのサポートを提供しません。CA では、CA Service Desk Manager アプリケーションに付属している SDK サンプル ソース コード以外の追加のアダプタの作成および展開を積極的にサポートしていません。

CA 統合検索 SDK アーキテクチャは、拡張用に設計されています。SDK には、カスタム アダプタを開発するために必要なすべての JAR ファイルが含まれます。サンプル Eclipse プロジェクトのインポートが可能であり、カスタム検索アダプタを作成するための Ant ビルドターゲットも提供されています。SDK は以下の CA SDM ディレクトリにあります。

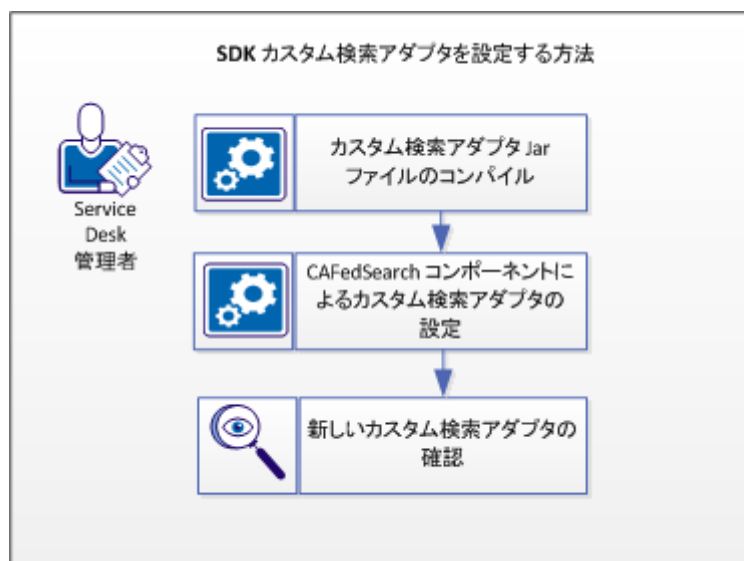
```
$NX_ROOT¥samples¥sdk¥fedsearch¥adapters-source.tar.gz
```

以下のアダプタのソース コードは、追加のカスタム アダプタを記述するために使用できます。

- Google
- CA Open Space
- Microsoft SharePoint

注: CAFedSearch サーブレット用のソース コード、その基礎となるフレームワーク、およびセキュリティ フィルタは提供されていません。Crawler Surface のどのコンポーネント用のソース コードも提供されていません。

SDK コンポーネントは Java で記述されており、jar ファイル (cafedsearch-adapter-sdk-1.0.0.jar) として共有されます。SDK は、ユーザーが独自の検索アダプタを開発および展開できるシンプルなインターフェースを提供します。



次の手順に従ってください：

1. [カスタム検索アダプタ Jar ファイルのコンパイル](#) (P. 209)
2. [CAFedSearch コンポーネントによる新しいカスタム検索アダプタの設定](#) (P. 212)
3. [新しいカスタム検索アダプタの確認](#) (P. 214)

新しいカスタム アダプタ Jar ファイルのコンパイル

カスタム アダプタ jar ファイルを正常にコンパイルします。

次の手順に従ってください:

1. 新しいカスタム検索アダプタをコンパイルします。Java クラスパスに以下の jar ファイルがあることを確認します。

jsr311-api-1.0.jar

この jar ファイルは、以下の CA SDM ディレクトリにあります。

`%NX_ROOT%\java\lib\CXF\`

cafedsearch-core.jar

このファイルは、以下のディレクトリにあります。

`%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib`

cafedsearch-adapter-sdk-1.0.0.jar

このファイルは、以下のディレクトリにあります。

`%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib`

log4j-1.2.15.jar (オプション)

このファイルは、以下のディレクトリにあります。

`%NX_ROOT%\java\lib`

2. SearchAdapter クラスを拡張し、抽象メソッド用の実装を提供する新しい Java クラスを記述します。

search

CAFedSearch コンポーネントは、検索メソッドパラメータを呼び出して渡します。これらのパラメータは、クライアントからの検索リクエストごとに SearchOptions パラメータに組み込まれます。

注: CAFedSearch コンポーネントは Java クラスの 1 つのインスタンスのみを管理するため、ユーザの実装はスレッドセーフであることを確認してください。検索操作ごとに、検索メソッドが同じインスタンスで呼び出されます。

3. 検索メソッド用の SearchOptions パラメータには、以下のメソッドがあります。

getSearchTerms()

検索文字列を取得する方法を指定します。

getStartIndex()

開始インデックス メソッド（クライアントが項目の検索を開始する番号）を指定します。インデックスは 1 から開始します。

getItemsPerPage()

クライアントが予期する検索結果の最大数を指定します。

注: 他の Java クラス メソッドを使用することもできます。例:
getUserId()

4. 検索結果を取得するために、収集された情報を外部検索エンジン API に送信します。

注: Java クラス メソッドの詳細については、Java のマニュアルを参照してください。

5. 検索メソッドは、**ResultCollection** クラスのインスタンスを返します。**ResultCollection** のインスタンスを作成し、以下のメソッドを使用して、値を入力します。

setSources(String name)

検索アダプタの名前を指定します。この名前は大文字と小文字が区別されます。また、ユーティリティ設定ファイルで指定されている名前と正確に一致する必要があります。利便性のために **SearchAdapter** によって **getName()** メソッドが提供されるため、このメソッドを使用してください。

以下に例を示します。

```
results.setSources(getName());
```

setTotalResults (int total)

検索結果の総数を指定します。

setStartIndex(int startIndex)

結果の開始インデックスを指定します。この値は、検索エンジンからの結果に従います。

```
results.setStartIndex(startIndex);
```

6. **setSearchResultItems** メソッドを呼び出すことで、**ResultItems** のコレクションを **ResultCollection** オブジェクトに渡す必要があります。**ResultItem** のインスタンスを一度に追加するには、**addSearchResultItem()** メソッドを使用します。

注: **ResultCollection** Java クラスの詳細については、Java のマニュアルを参照してください。

7. **ResultItem** クラスには、以下の重要なメソッドがあり、そのメソッドは、各検索結果項目（行）に対して入力する必要があります。

setContentText(String txt)

検索結果の実際のコンテンツを設定するメソッドを指定します。

setContentHTML(String txt)

HTML (HTML タグを含めることができる) コンテンツを設定するメソッドを指定します。検索エンジンが強調表示された HTML を与える場合は、このメソッドを使用して、強調表示されたテキストを設定します。

注: 検索エンジンにこの機能がない場合は、テキストを強調表示する単純な Java クラス メソッドを記述できます。CA Open Space アダプタには、検索結果内の検索語を太字にする単純なメソッドを持っています。

setTitleHTML(String titleHTML)

HTML タイトル (HTML タグを含めることができる) を設定するメソッドです。

setTitleText(String titleText)

プレーン タイトル (HTML タグを含めることができない) を設定するメソッドです。

setSource(String source)

ソース属性を設定するメソッドです。典型的な呼び出しは `item.setSource(getName());` になります。

注: 検索アダプタがさらにほかの jar ファイルを必要とする場合は、`build.xml` をカスタマイズすることによって、アダプタ jar ファイルをコンパイルして用意します。Ant バイナリが `build.xml` を使用するのに必要です。jar ファイルをコンパイルして作成するには、Ant を使用して `build.xml` 内のターゲットを実行します。この `build.xml` は、ソース (src) フォルダとともに保持してください。 `build.properties` ファイルはオプションです。Ant バイナリの詳細については、Ant のヘルプを参照してください。

jar ファイルが正常にコンパイルされました。

CAFedSearch コンポーネントによる新しいカスタム検索アダプタの設定

CA SDM 検索ソースを作成するために、CAFedSearch コンポーネントを使用して、新しい検索カスタム アダプタ jar ファイルを設定します。

次の手順に従ってください:

1. jar ファイルを `dist¥lib` ディレクトリ（「新しいカスタム アダプタ Jar ファイルのコンパイル」で作成）から以下の CA SDM ディレクトリにコピーします。
2. 以下の CA SDM ディレクトリに移動します。
3. カスタム検索アダプタ用の新しいテンプレート XML ファイルを作成します。たとえば、`XYZ-tmpl.xml` ファイルを作成します。
4. このテンプレート ファイルには、以下のセクションが含まれています。

```
%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib
```

2. 以下の CA SDM ディレクトリに移動します。

```
$NX_ROOT\sample\cafedsearch¥
```

```
<?xml version="1.0" encoding="UTF-8"?>

<beans default-autowire="byName"
xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-2.5.xsd
http://cxf.apache.org/core
http://cxf.apache.org/schemas/core.xsd
http://cxf.apache.org/jaxrs
http://cxf.apache.org/schemas/jaxrs.xsd"
xmlns:cxf="http://cxf.apache.org/core"
xmlns:jaxrs="http://cxf.apache.org/jaxrs"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.springframework.org/schema/beans">

    <bean autowire="autodetect"
        class=" com.abc.xyz.XYZAdapter "
        id="XYZAdapterConfiguration" scope="singleton">
        <property name="username" value="${xyz_username}"/>
        <property name="password" value="${xyz_password}"/>
    </bean>
```



```

<bean autowire="autodetect" class="com.abc.xyz.XYZAdapter"
id="XYZSearchAdapter" init-method="init" destroy-method="destroy"
depends-on="XYZAdapterConfiguration">
    <property name="config"
ref="OpenSpaceAdapterConfiguration" />
</bean>
</beans>

```

5. 手順 4 で検索アダプタに関して指定した入力値に基づくプロパティ値を作成できます。

adapters.properties ファイルの xyz_username および xyz_password を追加し、プロパティの値を指定します。

6. ユーティリティ ファイルを実行して、カスタム検索アダプタ用の設定 XML を生成します。

```
fs_adapters_cli -i -k XYZ -b XYZSearchAdapter -t "XYZ-templ.xml " -o "xyz.xml"
```

7. xyz.xml ファイルが作成され、adapters-config.xml ファイルに登録されます。

8. xyz.xml ファイルと adapters-config.xml を以下の CA SDM ディレクトリにコピーします。

```
$NX_ROOT¥samples¥cafedsearch¥WEB-INF
```

9. 以下のコマンドを実行して統合検索 Tomcat サービスを再起動します。
pdm_tomcat_nxd - c STOP - t FS
pdm_tomcat_nxd - c START - t FS

10. CA SDM UI で、XYZ アダプタ用の統合検索ソースを作成します。

統合検索ソースの詳細については、「[CA SDM での統合検索ソースの作成](#) (P. 183)」を参照してください。

11. CA SDM で、[ナレッジ マネジメント] タブに移動します。[XYZ] チェック ボックスをオンにして、検索操作を実行します。

新しいカスタム検索アダプタが CAFedSearch コンポーネントによって正常に設定されました。

新しいカスタム検索アダプタの確認

REST クライアントを使用して新しいカスタム検索アダプタの機能を確認します。

次の手順に従ってください:

1. インターネットから REST クライアントをダウンロードします。

<https://code.google.com/p/rest-client/>

2. Java を使用してクライアントを起動します (JRE が必要)。

3. REST クライアント UI に以下の URL を入力します。

```
http://sdmhostname:<FS_Tomcat_Port>/cafedsearch/sdm/search?q=search&userid=<sdmuserid>&source=<Adapter Name>
```

4. CA SDM セキュリティ インターセプタをオフにします。以下のファイルを編集するために開き、「<jaxrs:inInterceptors>」セクションをコメントアウトします。

```
$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥cafedsearch¥WEB-INF¥beans.xml
```

注: セキュリティ フィルタをオフにすることは、実稼働環境では推奨されません。新しいカスタム検索アダプタの機能を確認するために、テスト環境でセキュリティ フィルタをオフにします。

5. 新しいカスタム検索アダプタが正しく機能していることを確認します。検索結果が表示されない場合は、ログを確認するか、ログのレベルをデバッグ レベルに引き上げます。

CORS (Cross-Origin Resource Sharing) フィルタの追加

CORS (Cross-Origin Resource Sharing) フィルタを Web インターフェースおよび統合検索 (FS) Tomcat に追加すると、Web クライアントインターフェースに統合検索機能が設定されます。このフィルタを使用して、異なる生成元 (cross-origin) のリクエストのリストを追加できます。デフォルトでは、Web インターフェース設定には任意の生成元のリクエストを示す "*" が指定されており、異なる生成元 (cross-origin) または同一生成元 (same-origin) のいずれかが許可されます。ユーザの環境で設定された CA SDM Web インターフェース サーバのリストを使用して、この設定をさらに制限することをお勧めします。

Web インターフェース クライアント設定を編集して異なる生成元のリクエストを許可するには、以下の手順に従います。

次の手順に従ってください：

1. Web インターフェース設定を編集するには、以下の CA SDM ディレクトリに移動します。

```
$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_FS¥webapps¥cafedsearch¥WEB-INF¥web.xml
```

2. web.xml ファイルを開き、以下を確認します。

```
<web-app><filter><init-param><param-name>cors.allowOrigin</param-name>
```

3. <param-value> タグの内容を、ドメインのスペース区切りリストで更新します。たとえば、Web インターフェースのベース URL アドレス：

```
<param-value>http://web01:8080 http://web02:8080  
http://web03:8080</param-value>
```

4. web.xml ファイルを保存します。Tomcat が自動的に再起動されます。
5. Web クライアントインターフェース上の [統合検索] 構成をテストして確認します。正しく機能することを確認してください。
6. CA SDM の設定を実行した後に Web インターフェースの更新を保持するには、web.xml.tpl ファイルに同じ更新を繰り返します。

REST による CAFedSearch サブレットの呼び出し

CAFedSearch サブレットは RESTful インターフェースを提供し、これによってカスタム検索クライアント、プログラム、およびユーザ インターフェース (UI) が検索リクエストを送信できます。

この RESTful インターフェースは、OpenSearch 仕様に準拠する HTTP Collection GET リクエストのみを受け入れます。また、JSON および XML 応答をサポートします。各リクエストには、CA SDM RESTful または SOAP Web サービスから取得できる Service Desk BOPSID トークンが含まれている必要があります。

次の手順に従ってください:

1. CA SDM RESTful Web サービスを使用して BOPSID トークンを取得します。
2. ログイン認証情報と共に `rest_access` リソースに対する HTTP POST リクエストを送信することによって、REST アクセス キーを取得します。

`bopsid` リソースに対する HTTP POST リクエストを送信することによって、REST アクセス キーを使用して BOPSID トークンを取得することもできます。
3. CA SDM RESTful Web サービスへのリクエストの送信の詳細については、以下の CA SDM ディレクトリにあるサンプル ファイルを参照してください。

```
NX_ROOT¥samples¥sdk¥rest¥java
```

4. 統合検索 API を使用して検索するには、検索リソースに対して HTTP GET リクエストを送信し、CA SDM URL を介して検索条件と BOPSID トークンを渡します。

GET

```
http://<sdmhostname>:<FS_TOMCAT_PORT>/cafedsearch/sdm/search?q=<searchTerms>&source=<adapterName>&BOPSID=<bopsidToken>&userid=<userId>
```

`searchTerms`

キーワードのスペース区切りリストを指定します。エンコードされた URL である必要があります。

`adapterName`

アダプタ設定ユーティリティを使用して、[検索ソース] レコードの [コード] フィールドで指定されている検索エンジン名を指定します。

サポートされるその他の引数は、以下のとおりです。

index

検索結果に求められる最初のインデックスを指定します。**1**以上の整数である必要があります。

page

検索結果に求められる最初のページを指定します。**1**以上の整数である必要があります。

size

検索クライアントが要求するページ当たりの結果数を指定します。

type

有効な値は「JSON」または「XML」です。

第 7 章: ポリシーの実装

このセクションには、以下のトピックが含まれています。

[ポリシーの実装](#) (P. 219)

ポリシーの実装

サービス デスクを設定する場合に重要な要素となるのは、業務プロセスに最適な方法でポリシーを実装することです。

CA SDM には事前定義済みのポリシー実装が用意されており、これは一部のサイトでそのまま使用することができ、それ以外のサイトでも最初のひな形として役立ちます。すべてのポリシー定義領域で初期設定の実装を確認して、要件が満たされている部分と、修正が必要な部分を調べます。

通知

CA Service Desk Manager では、チケットのアクティビティ（調査中、エスカレート）とイベント（チケットのオープンなど）について、主要な担当者に通知を自動的に送信できます。さらに、ナレッジ レポートカード（KRC）およびサポート オートメーション Assistance セッションに関して主要な担当者に通知できます。重要なアクティビティまたはイベントが発生した場合、CA Service Desk Manager は以下の役割がある通知メッセージを生成します。

- チケット アクティビティまたは通知イベントの識別
- チケットの参照
- その他の情報の通知
- 代替的な連絡先の識別

システム アクションの結果生成されたチケットの通知メッセージを表示できます。システム アクションには、履歴情報を通してチケットを開く、閉じる、変更することが含まれます。

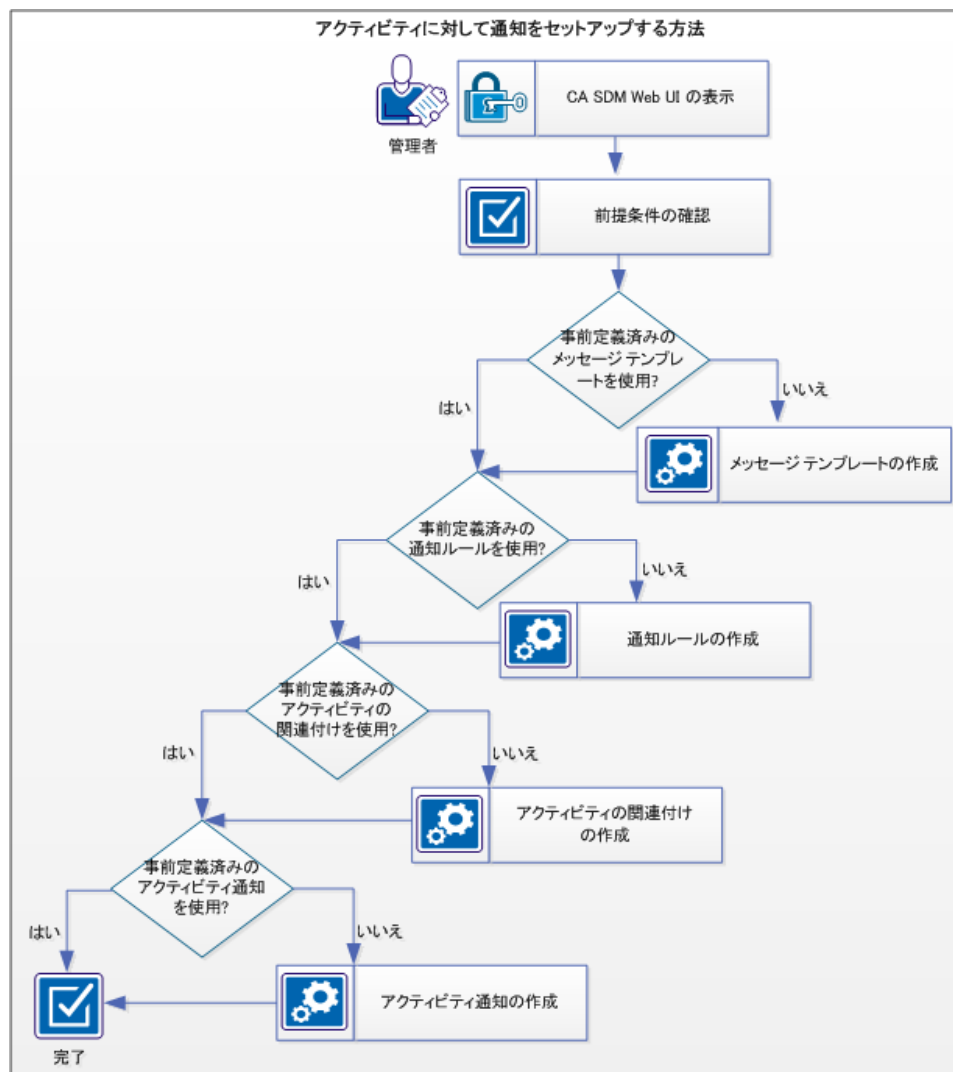
自動通知を設定するには、以下のタスクを行います。

- 通知を生成するアクティビティのタイプを決定するアクティビティ通知を定義します。
- アクティビティ通知で通知の送信に使用できるオブジェクトの連絡先を決定するオブジェクト連絡先通知を定義します。
- メッセージの送信方法を指定します。

アクティビティに対して通知をセットアップする方法

特定のアクティビティについて送信される通知を定義できます。アクティビティとは、チケットの解決、顧客満足度調査（個別）の送信、ナレッジレポートカードの実行など、ユーザが実行するアクションのことです。コールを返す、レコードのキャンセルやクローズ、ステータスの更新などの日常のアクティビティも、通知が送信されるアクティビティです。

以下の図は、アクティビティに対して通知をセットアップする方法を示しています。



次の手順に従ってください:

1. [CA SDM Web UI を開きます](#) (P. 222)。
2. [前提条件を確認します](#) (P. 222)。
3. 事前定義済みのメッセージテンプレートを使用しない場合、[メッセージテンプレートを作成します](#) (P. 225)。
4. 事前定義済みの通知ルールを使用しない場合、[通知ルールを作成します](#) (P. 229)。

5. 事前定義済みのアクティビティの関連付けを使用しない場合、[アクティビティの関連付けを作成します](#) (P. 231)。
6. 事前定義済みのアクティビティ通知を使用しない場合、[アクティビティ通知を作成します](#) (P. 231)。

CA SDM Web UI の表示

CA SDM の設定に応じて、以下のサーバから Web UI にログインします。

- 標準：プライマリまたはセカンダリ サーバ
- 高可用性：アプリケーションサーバまたはバックグラウンドサーバ

前提条件を確認します。

セットアップを開始する前に、以下の前提条件を確認します。

- [通知に URL を追加するオプションをインストールしている](#) (P. 222)。
- [受信者用の通知方法を確認している](#) (P. 223)。
- 連絡先と関連付けられていない電子メール アドレスに通知を手動で送信する場合、[一時電子メール アドレスを許可](#) (P. 223) します

通知に URL を追加するオプションのインストール

Change_Request テーブルと Workflow_Task テーブルの web_url フィールドには URL 値が格納されます。この URL 値を使用すると、ユーザは Web インターフェースを介して特定の変更要求またはワークフロー タスクにアクセスできます。電子メール通知で使用する場合、ユーザは特別な検索などを実行しなくても、URL をクリックして Web インターフェースにアクセスできます。

通知内に URL ハイパーリンクを実装するには、以下のようにシステムを設定します。

1. CA SDM Web インターフェースのインストールと環境設定を行います。CA SDM Web インターフェースの設定の詳細については、「[実装ガイド](#)」を参照してください。
2. CA SDM Web エンジンの場所を指定するには、オプション マネージャを使用して、web_cgi_url オプションの設定とインストールを行います。たとえば、http://hostname/scripts/pdmcgi.exe のように指定します。高可用性設定では、hostname は、アプリケーションサーバまたはロード バランサを指している必要があります。

受信者用の通知方法の確認

通知を送信する連絡先が、その特定の通知方法に割り当てられていることを確認します。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理] - [連絡先] を選択します。
[連絡先の検索] ページが開きます。
2. フィルタを使用して連絡先を検索し、検索結果から通知する連絡先を選択します。
[連絡先の詳細] ページが開きます。
3. [連絡先詳細] タブの [通知] を選択します。
4. 通知方法を確認します。通知の優先度に基づいて、必要なオプションを選択します。たとえば、任意の緊急の通知に関して電子メール通知を送信するとします。[緊急] フィールドで [電子メール] オプションを選択します。
5. 通知方法を変更するには、[編集] をクリックし、オプションを変更して、[保存] をクリックします。
連絡先の通知方法が確認されます。

一時電子メール アドレスの許可

一時電子メールアドレスは、システム内で連絡先に関連付けられていないアドレスです。一時電子メールアドレスは以下のような場合に役立ちます。

- エンドユーザがオフィスの外にいるか、または標準の電子メール アカウントへのアクセスに問題がある。
- アナリストがユーザとの対話の追跡に電子メールを使用する。

- アナリストがユーザの一時電子メールアドレスに手動通知を送信する。
- アナリストが、手動通知で更新されるアクティビティ ログを表示できる。

受信者は、受信者の電子メールアドレスが連絡先レコードと関連付けられていない、またはチケットを更新する権限がないと、一時電子メールアドレスに返信できません。

注: 一時電子メールアドレスは、常に **SMTP** 電子メールアドレスであり、優先方法が **SMTP** をサポートする場合のみ、サポートされます。一時電子メールアドレスのセットアップ方法の詳細については、[オンラインヘルプ](#)を参照してください。

次の手順に従ってください:

1. [管理] タブで [オプション マネージャ] - [通知] を選択します。
[オプション リスト] ページが開きます。
2. notification_allow_temp_address をクリックします。
[notification_allow_temp_address オプションの詳細] ページが開きます。
3. [編集] をクリックします。
4. [インストール] をクリックします。
[notification_allow_temp_address オプションの詳細] ページが開きます。
5. [ウィンドウを閉じる] をクリックします。
6. **CA SDM** サーバを再起動します。CA SDM サーバを起動する方法の詳細については、**CA SDM** の設定に応じて、**CA SDM** サーバの再起動シナリオを参照するか、または「[管理ガイド](#)」で情報を検索してください。
これで、一時電子メールアドレスを手動通知に使用できるようになりました。

メッセージ テンプレートの作成

通知メッセージ用に使用する値が含まれるメッセージ テンプレートを作成します。複数の通知メッセージを送信する場合、メッセージ テンプレートを使用して、作業負荷を軽減できます。

注: マルチテナンシーがインストールされている場合は、ドロップダウン リストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで [通知] - [メッセージ テンプレート] を選択します。
[メッセージ テンプレート リスト] ページが開きます。
2. [新規作成] をクリックします。
[メッセージ テンプレートの新規作成] ページが開きます。
3. 必要に応じてフィールドにデータを入力します。

シンボル

このメッセージ テンプレートの一意の識別子を定義します。

オブジェクト タイプ

このテンプレートに関連付けられたオブジェクト タイプを指定します。たとえば、チケットに関連する任意の通知に対するリクエスト/インシデント/問題を選択します。

レコード ステータス

テンプレートのステータスをアクティブまたは非アクティブに指定します。メッセージ テンプレートを使用するために、ステータスを [アクティブ] に設定します。

自動通知

アクティビティが発生すると、このテンプレートに関連付けられた通知を自動的に送信するよう指定します。たとえば、初期通知を設定し、通知するオブジェクトを設定し、メッセージ テンプレートを設定したのに、通知をオンにする準備ができていないとします。この場合、[自動通知] を選択しません。自動通知を開始する準備ができていない場合、このチェック ボックスをオンにします。通知がアクティブになり、設定したとおりに実行されます。

通知レベル

この通知の送信の相対的な重要性を示します。たとえば、関連するアクティビティが発生した場合、連絡先に電子メール通知をすぐに送信する場合は、[緊急]を選択します。

通知メッセージタイトル

メッセージの概要タイトルを指定します。変数を使用して、メッセージタイトルにインシデント番号を挿入できます。たとえば、`@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}` のように指定します。

通知メッセージ本文

メッセージの内容を指定します。変数を使用して、メッセージにアナリスト名、エンドユーザ名、および説明を挿入できます。例：

@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}。

担当者： @{call_req_id.assignee.combo_name}

顧客： @{call_req_id.customer.combo_name}

説明： @{call_req_id.description}

表示するには次の URL をクリックします。

@{call_req_id.web_url}

キーワード **ARTIFACT** を使用して、アーチファクトが送信メッセージ、メッセージテンプレート、通知、および自動応答で処理される方法を指定することができます。キーワード **ARTIFACT** は、以下の値を使用します。

- **なし** - アーチファクトの検証を指定しません。この値は、キーワードを使用しないと同じです。
- **保護済み** - 確認用のハッシュに対してチケットを検証します。確認に失敗した場合、アーチファクトは無効であると見なされ、アーチファクト ({{object_id}}) をフィルタリング検索した場合、フィルタリングは失敗します。
- **セキュア** - チケット番号の暗号化を解除します。値が有効なパスワードでない場合、アーチファクトは無効であると見なされ、フィルタリングがアーチファクト ({{object_id}}) を検索する場合、フィルタリングは失敗します。

HTML メッセージ

受信者に表示される **HTML** メッセージを指定します。受信者が携帯電話や **PDA** などの外部デバイスでメッセージを受信する場合、メッセージはプレーンテキストのみで表示されます。[**HTML** メッセージの編集] をクリックして **HTML** エディタを開きます。

クイック表示

受信者に表示される形式でメッセージが表示されます。

HTML ソース

HTML ソース コードにメッセージが表示されます。

4. [保存] をクリックします。

メッセージテンプレートが作成されます。

通知ルールを作成

通知ルールを作成して、通知する連絡先および状況を指定します。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで [通知] - [通知ルール] を選択します。
[通知ルールのリスト] ページが開きます。
2. [新規作成] をクリックします。
[通知ルールの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

シンボル

この通知ルールの一意の識別子を定義します。たとえば、「Ticket Description Update」と入力します。

オブジェクトタイプ

ルールが適用されるオブジェクトを定義します。たとえば、チケットに関連するアクティビティに対するリクエスト/インシデント/問題を選択します。

4. [保存と続行] をクリックします。
5. [条件] をクリックして、このルールの条件の定義に使用できるマクロを選択します。条件を定義するには、以下のいずれかのアクションを実行します。

注: 通知ルールに条件を指定しないと、アクティビティが発生するたびすべての連絡先に通知されます。

- リストからのマクロを検索して選択します。
 - [新規作成] をクリックしてマクロを作成します。
6. [メッセージテンプレート] をクリックして、このルール用に作成したメッセージテンプレートを追加します。以下のいずれかを実行します。
 - リストからテンプレートを検索して選択します。

- 「新規作成」をクリックしてメッセージテンプレートを作成します。

7. 通知先として適切な連絡先を以下のタブで選択します。

注: 通知先となる連絡先を検索して追加選択するには、各タブに表示される「連絡先の更新」ボタンをクリックします。

オブジェクトの連絡先

チケットに関する通知を受信する、選択されたオブジェクトタイプで使用可能な組織、ベンダー、および構成アイテムを表示します。たとえば、影響を受けるエンドユーザ、または影響を受けるエンドユーザの管理組織を選択して通知できます。

連絡先

通知ルールに追加された人物が、チケットに対する関連付けによらず、表示されます。

連絡先タイプ

アナリスト、顧客など、通知ルールで同じ分類として定義されたユーザが表示されます。

8. 「保存」をクリックします。

通知ルールが作成されます。

アクティビティの関連付けの作成

オブジェクト属性とアクティビティを関連付けて、関連するオブジェクト属性に対する変更を追跡します。たとえば、インシデントレコードの[説明]フィールドのオブジェクト属性と[フィールド更新]アクティビティを関連付けます。これにより、インシデントの説明が更新されるたびに通知を送信できます。オブジェクト属性に設定できるアクティビティ通知は1つのみです。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで [通知] - [アクティビティの関連付け] を選択します。
[アクティビティ関連付けリスト] ページが開きます。
2. [新規作成] をクリックします。
[アクティビティ関連付けタイプの新規作成] ページが開きます。
3. 以下のフィールドを指定します。

シンボル

この関連付けの一意の識別子を定義します。

コード

アクティビティ関連付けの内部コードを定義します。

オブジェクトタイプ

属性を適用するオブジェクトの名前を指定します。たとえば、[リクエスト/インシデント/問題] を選択します。

オブジェクトタイプ属性

アクティビティタイプを関連付けるオブジェクト属性を定義します。たとえば、インシデントレコードの[説明]フィールドのオブジェクト属性を入力します。

アクティビティタイプ

アクティビティのタイプを示します。たとえば、選択したオブジェクト属性がいつ更新されるかを確認には、[フィールド更新] を選択します。

ログに自分を追加

このアクティビティの関連付けが監査ログにログ エントリを作成するかどうかを決定します。

4. [保存] をクリックします。
[アクティビティ関連付けタイプの詳細] ページが開きます。
5. [ウィンドウを閉じる] をクリックします。
アクティビティの関連付けが作成されます。

アクティビティ通知の作成

通知とアクティビティを関連付けます。アクティビティが発生した場合、関連する通知は選択された連絡先に送信されます。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。テナントごとに別々の手動通知のアクティビティ通知を保持したり、手動通知のアクティビティ通知をコピーしたりすることはできません。

次の手順に従ってください:

1. [管理] タブで [通知] - [アクティビティの通知] を選択します。
[アクティビティ通知リスト] ページが開きます。
2. [新規作成] をクリックします。
[アクティビティ通知の新規作成] ページが開きます。
3. 以下のフィールドを指定します。

シンボル

このアクティビティ通知の一意の識別子を定義します。

コード

アクティビティ通知の内部コードを定義します。

有効なアクティビティ:

このアクティビティが適用されるオブジェクトを指定します。

4. [保存と続行] をクリックします。
[アクティビティ通知の更新] ページが開きます。

5. 以下のフィールドを指定します。

内部

内部従業員のみがアクティビティ通知を使用できるか、またはアクティビティ通知がエンドユーザに表示されるかを指定します。

レコード ステータス

アクティビティ通知がアクティブであるか、非アクティブであるかを定義します。アクティビティの関連付けを使用するために、ステータスをアクティブに設定します。

関連チケット アクティビティ

チケット上のアクティビティ ログがすべての関連するチケットに継承されるかどうかを指定します。アクティビティ ログの継承は、関連するインシデント、問題および変更要求に対してのみ有効です。

注: マルチテナンシーを使用する場合は、以下のアクションを実行します。

- [関連チケット アクティビティ] ドロップダウン リストから適切なテナントタイプを指定します。
- テナント フィールドにテナントの名前を入力するか、検索アイコンをクリックしてテナントを検索します。

オブジェクト タイプ

アクティビティを適用するオブジェクトの名前を指定します。

6. [通知ルール] タブで、[通知ルールの更新] をクリックします。以下のいずれかの操作を実行します。
 - 検索条件を入力して [検索] をクリックし、検索結果から通知ルールを選択します。
 - [新規作成] をクリックして通知ルールを作成します。

7. (通知の受信者に調査を送信する場合) [調査] タブを選択し、[調査通知を定義します](#) (P. 235)。調査を使用すると、顧客フィードバックを収集して分析することができます。アクティビティ ログは、調査通知を送信したとき、および調査通知に関する顧客からの応答を受信したときに生成されます。

注: [調査] タブは、ナレッジ ドキュメント、ナレッジ ドキュメント コメント、およびナレッジ レポート カードを除く、すべてのオブジェクト タイプに適用されます。[オブジェクト タイプ] リストから指定した場合、[アクティビティ通知の更新] ページには、[調査] タブの代わりに、[電子メール] タブが表示されます。[電子メール] タブでは、この通知に関連付ける 1 つ以上の電子メール メッセージを検索したり、電子メール メッセージを新規に定義したりできます。

8. (通知が送信された後にイベントをトリガする場合) [イベント] タブを選択します。イベントは、ある一定の時間が経過した後、案件管理システムによって行われる手順です。アクティビティ通知がトリガされた場合、選択したイベントが発生します。たとえば、インシデントのステータスを更新すると、[クローズ] になります。イベントを検索して[イベントの更新] ボタンをクリックし、イベントをアクティビティ通知に追加します。
9. [保存] をクリックします。
[アクティビティ通知の詳細] ページが開きます。
10. [ウィンドウを閉じる] をクリックします。

アクティビティ通知が作成されます。エラーが送信メール サーバ上で発生した場合は、電子メール通知は送信されず、`$NX_ROOT/site/mail_queue` ディレクトリのキューに入れられます。メール サーバが再度アクティブになると、一定の間隔の後で、電子メールを処理して送信します。[電子メールの再試行間隔の変数を設定し](#) (P. 235)、メール サーバがビジーだったときにキューに入れられた電子メールをリサイクルできます。

ユーザが以下のいずれかのアクションを実行するまで、送信メール サーバは、送信に失敗した通知電子メール メッセージを再サブミットします。

- 送信メール通知を処理するメール デーモン (`pdm_mail_nxd`) を停止します。
- 手動で、メッセージを `$NX_ROOT/site/mail_queue` ディレクトリから削除します。

調査通知の定義

必要に応じて、以下のフィールドに入力します。

調査を送信する

調査をアクティブにするか、非アクティブにするかを示します。オンにした場合、選択したアクティビティ通知がトリガされたときに、調査が連絡先に送信されます。

調査の初期設定

検索アイコンを使用してデフォルトの調査を指定するか、テキストボックスに独自の調査を指定します。

調査メッセージタイトル

調査のタイトルを入力します。

調査メッセージ本文

連絡先へのメッセージを入力します。連絡先が受信する調査通知のメッセージには URL が組み込まれます。ユーザは、Web ブラウザを使用して、この URL から調査フォームにアクセスし、回答することができます。

電子メール再試行間隔の変数を設定する

メール サーバへの電子メールの送信失敗を再試行する時間間隔（秒）を定義できます。

注: CA SDM では、送信メール サーバが受信したのに配信できなかったメッセージは、送信を再試行しません。これらのメッセージについては、送信メール サーバの再試行機能およびポリシーがある場合は有効です。

再試行はメッセージ単位で行われます。メール サーバが一定の期間使用できない場合、すべてのメッセージが一度に送信されるのではなく、メッセージのそれぞれのタイマが期限切れになったときに再試行されます。ただし、送信メール デーモンを再起動した場合、すべての未送信メッセージはその時間に送信されるように試行します。また、それらがすべて送信に失敗した場合、それらの再試行タイマはすべて同時にリセットされます。

NX.env ファイルの設定 (NX_EMAIL_RETRY_INTERVAL) は再試行間隔を制御します。1 つ以上のサーバでデフォルトの再試行間隔の設定を変更できます。

次の手順に従ってください:

1. CA SDM の設定に応じて、以下のサーバにログインします。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンドサーバ。
2. `$NX_ROOT` ディレクトリに移動します。
3. テキスト エディタ (ワードパッドなど) を使用して `NX.env` ファイルを開きます。
4. `NX_EMAIL_RETRY_INTERVAL` 間隔の値を、以下のように変更します。

```
NX_EMAIL_RETRY_INTERVAL=number_of_seconds
```

```
NX_EMAIL_RETRY_INTERVAL
```

失敗した電子メールの試行を再試行する時間間隔 (秒) を定義します。

number_of_seconds

各電子メールの再試行間隔の秒数を指定します。デフォルトは 600 秒 (10 分) です。使用できる最小値は 20 秒です。最小値の 20 秒未満の値または 2000000 秒を超える値を設定した場合は、デフォルト値の 10 分が使用されます。

5. ファイルを保存して閉じます。
6. CA SDM サーバを再起動します。CA SDM サーバを起動する方法の詳細については、CA SDM の設定に応じて、**CA SDM サーバの再起動シナリオ**を参照するか、または「**管理ガイド**」で情報を検索してください。
変更は有効になっています。

オブジェクトの連絡先通知を作成する方法

オブジェクトの連絡先通知では、チケットのフィールドの現在値に基づいて受信者に通知できます。通知先の個人を指定する代わりに、通知方法などで、オブジェクトを指定します。たとえば、`[To]` フィールドを指定して、チケットの定義後にこの値が変更された場合でも、`[To]` フィールドに現在指定されているユーザが通知先になるようにできます。

次の手順に従ってください:

1. 「管理」タブで、「通知」-「オブジェクトの連絡先通知」を選択します。
「オブジェクトの連絡先通知リスト」ページが開きます。

2. [新規作成] をクリックします。
[オブジェクトの連絡先通知の新規作成] ページが開きます。
3. 以下のフィールドを指定します。

シンボル

オブジェクトの連絡先通知に対する一意の識別子を定義します。

ステータス

オブジェクトの連絡先通知がアクティブであるか、非アクティブであるかを指定します。

オブジェクトタイプ

属性の適用先のオブジェクト名が表示されます。

オブジェクト属性名

([シンボル] フィールドの) オブジェクトの連絡先通知の名前を、CA 内部コードである **Majic** で示します。属性名は、[オブジェクトタイプ] の選択内容によって異なります。

- [オブジェクトタイプ] が [案件] または [ワークフロー タスク] である場合、属性名は担当者、依頼者、またはグループになります。これらは、**chg** オブジェクト内の属性名であり、**Change_Request** テーブルのフィールドにマップされます。
- [オブジェクトタイプ] が [案件のアクティビティ ログ] の場合、属性名の先頭文字列は、その属性を **chg** オブジェクトの特定インスタンスにリンクしている、アクティビティ ログ オブジェクト内の属性名である必要があります。属性名は **change_id.group** のようになります。

説明

オブジェクトの連絡先通知について説明します。

4. [保存] をクリックします。
新しいオブジェクトの連絡先通知が、[オブジェクトの連絡先通知リスト] に表示されます。

注: オブジェクトの連絡先通知の設定の詳細については、オンラインヘルプを参照してください。

手動通知受信者リスト

〔手動通知構成〕 ページにリクエスト、インシデントおよび問題を表示する〔使用可能な受信者〕のデフォルトセットをセットアップできます。〔使用可能な受信者〕は、連絡先オブジェクト（〔影響を受けるエンドユーザ〕など）や個別の連絡先名を、手動通知の受信者として容易に設定できるため、アナリストの手動通知プロセスを合理化します。

〔オブジェクトの連絡先の受信者〕を追加すると、〔オブジェクトの連絡先〕として表示される個別の連絡先が（重複エントリを統合して）〔受信者〕リストに追加されます。同じ連絡先が、〔担当者〕や〔影響を受けるエンドユーザ〕などの異なる〔連絡先オブジェクト〕として複数回参照されることもあります。〔関係者リスト〕の連絡先オブジェクトのようない部分のエントリは、〔受信者〕リストに複数のエントリを追加できます。

〔連絡先〕と〔連絡先オブジェクト〕をリスト追加すると、それらは〔使用可能な受信者〕リストに残ります。この動作により、初期の〔使用可能な受信者〕リストを変更せずに受信者を削除できます。

例: 〔使用可能な受信者〕リストの動作

デフォルトの受信者が、どのように手動アクティビティ通知プロセスを合理化するかを以下に示します。

〔オブジェクトの連絡先の受信者〕には以下のエントリが含まれます。

- **UserA** は、「担当者」および「影響を受けるエンドユーザ」連絡先オブジェクトに属します。
- 〔関係者リスト〕には複数の連絡先名が含まれます。たとえば、**UserB** や **UserC** などです。

以下の操作を実行します。

- **UserA** を参照する両方の〔連絡先オブジェクト〕を〔受信者〕リストに追加します。

1 つの **UserA** エントリのみが〔受信者〕リストに表示されます。

- ミスを再現するため、〔受信者〕リストから **UserA** を削除します。

UserA の名前を探してリストに追加しなおすために、チケットを参照する必要はありません。 **UserA** は、〔使用可能な受信者〕リストに含まれているため、迅速に〔受信者〕リストに追加しなおすことができます。

- ミスを再現するため、UserC のような [関係者リスト] に含まれる連絡先名を 1 件削除します。
[関係者リスト] に、[オブジェクトの連絡先の受信者] から連絡先名を追加しなおすことができます。重複エントリは統合されるため、[受信者] リストから削除されなかった [関係者リスト] 内の他の連絡先は影響されません。

以前の担当者への通知

チケットの保存時に主要フィールドに対する変更を検出するための、[以前の担当者] または [グループ] の値を定義できます。以前の値を使用すると、チケットの転送時に以前の担当者に通知したり、チケットの優先度が上がったときに現在のグループと以前のグループの両方に通知することができます。

チケットの以前の値のフィールドは、メモリにのみ存在するローカルフィールドです。データベースには存在しません。フィールドには、チケットの保存操作時に値が入力され、通知処理の完了時にクリアされます。以前の値のフィールドは、アクティビティ関連付けを通して特定のアクティビティタイプと関連付けられます。

チケットの以下のキー フィールドへの変更を検出する以前の値を定義できます。

フィールド	リクエスト、インシデント、問題	変更要求	案件
ステータス	はい	はい	はい
アクティブ	はい	はい	はい
担当者	はい	はい	はい
リクエスト領域/カテゴリ	はい	はい	はい
グループ	はい	はい	はい
影響度	はい	はい	はい
優先度	はい	はい	はい
緊急度	はい	いいえ	いいえ
重大度	はい	いいえ	いいえ

オブジェクトタイプ（リクエスト、インシデント、問題、変更要求、または案件）ごとに指定できるいくつかの連絡先があります。指定すると、アクティビティの発生時に現在の連絡先と以前の連絡先に通知できます。

- **担当者** - チケットの処理を割り当てられていた担当者
- **以前の担当者** - 前にチケットの処理を割り当てられていた担当者
- **グループ** - チケットの処理を割り当てられていたグループ
- **以前のグループ** - 前にチケットの処理を割り当てられていたグループ

通知ルールが保存されると、[以前の担当者] および [以前のグループ] フィールドが [オブジェクトの連絡先通知リスト] ページに表示されます。

例: キー フィールドの現在の値と以前の値の設定

以下の使用例は、管理者がキー フィールドの現在の値と以前の値を設定して、リクエストが別の場所に転送されたときに以前のサポート担当者に通知されるようにする方法を示しています。

1. **状況** - サポート担当者は、チケットが別の場所に転送されて、通知されなかったためにいら立っています。
2. **タスク** - 管理者は、[担当者] および [以前の担当者] オブジェクト連絡先を、[転送] アクティビティ通知の通知ルールに追加します。メッセージテンプレートを添付し、リクエスト フォームで通知する現在の担当者と以前の担当者を指定します。
3. **アクション** - リクエストが保存されると、リクエストの [担当者] および [以前の担当者] フィールドに入力されます。アクティビティが発生すると（チケットが転送されると）、ルールの条件が評価されます。
4. **結果** - 条件が満たされた場合、チケット アクティビティが現在の担当者に送信されたことを示す通知メッセージが以前の担当者に送信されます。

チケット転送時の連絡先への通知例

CA SDM チケットが転送された場合、現在の連絡先と以前の連絡先の両方に通知できます。

例: チケットの転送時に現在の連絡先と以前の連絡先の両方に通知する

1. [管理] タブで、[通知] - [アクティビティの通知] を参照します。
[アクティビティ通知リスト] ページが表示されます。
2. [転送] アクティビティ通知を選択します。
[Transfer Activity Notification Detail] ページが表示されます。
3. [オブジェクトタイプ] フィールドで、[リクエスト/インシデント/問題] を選択します。
4. [通知ルール] タブの [シンボル] で、[転送通知のデフォルトルール] を選択します。
[転送通知のデフォルトルール] ページが表示されます。
5. [オブジェクトの連絡先] タブで、[オブジェクトの連絡先の更新] をクリックします。
6. [検索] をクリックします。
[Notification Rule Update Recipients] ページが表示されます。
7. [オブジェクトの連絡先] リストで、左側のリストから [担当者] および [以前の担当者] を選択し、連絡先選択ボタン (>>) をクリックします。

選択したアイテムが右側のリストに追加されます。

注: 複数のオブジェクトの連絡先を選択するには、Ctrl キーまたは Shift キーと左マウス ボタンを使用します。
8. [OK] をクリックします。
9. 通知ルールを保存します。
[オブジェクトの連絡先リスト] に選択したオブジェクトの連絡先が表示されます。
10. [転送通知のデフォルトルール] ページで、[メッセージテンプレート] をクリックします。テンプレートを選択し、[自動通知] オプションが有効であることを確認します。
11. リクエストを作成し、担当者を指定し、[保存] をクリックします。

12. [リクエストの詳細] ページで、[ファイル] メニューの [アクティビティ]、[転送] の順に選択します。
13. 新しい担当者を指定し、[保存] をクリックします。
転送アクティビティが発生すると、通知が現在の担当者と以前の担当者の両方に送信されます。

構成アイテムの通知

構成アイテム (CI) 通知を使用すると、特定の CA SDM チケットと関連付けられる特定の CI と関連付けられるアクティビティ通知を定義することができます。この機能では、CI のユーザ、組織、およびベンダーに関する情報を追跡できます。

[通知ルール更新の受信者] ページでは、CI 保守組織、CI 主要連絡先などの CI オブジェクト連絡先を指定できます。

構成アイテムの主要連絡先への、案件に関する通知の例

特定の CA SDM チケットに関して特定の CI に送信される、主要連絡先のアクティビティ通知を定義できます。

例: 構成アイテムの主要連絡先への、案件に関する通知

1. [管理] タブで、[通知] - [アクティビティの通知] を参照します。
[アクティビティ通知リスト] ページが表示されます。
2. リストから [初期] アクティビティ通知を選択します。
[Initial Activity Notification Detail] ページが表示されます。
3. 使用するオブジェクト タイプを選択します。
4. [通知ルール] タブで、[Default Notification Rule] を選択します。
[Default Notification Rule] ページが表示されます。
5. [Default Message Template] リンクを選択し、[自動通知] オプションが有効であることを確認します。
6. [オブジェクトの連絡先] タブを選択し、[オブジェクトの連絡先の更新] をクリックします。
[オブジェクトの連絡先通知の検索] ページが表示されます。
7. [検索] をクリックします。オブジェクトの連絡先のリストが表示されます。

8. 左側のリストから CI の [主要連絡先] を選択し、連絡先選択対象ボタン (≥) をクリックします。

選択したアイテムが右側のリストに追加されます。

複数のオブジェクトの連絡先を選択するには、**Ctrl** キーまたは **Shift** キーと左マウス ボタンを使用します。リクエストの場合は 1 つのオブジェクト、変更要求または案件の場合は複数のオブジェクトを追加できます。

オブジェクトの連絡先が右側のリストに表示されます。

9. [OK] をクリックします。

10. 通知ルールを保存します。

[オブジェクトの連絡先リスト] に選択したオブジェクトの連絡先が表示されます。

11. 以下のタスクを完了します。

- [Service Desk] タブで、既存の CI を作成または更新します。
- [オブジェクトの連絡先] タブにリストされている主要連絡先を追加します。選択したオブジェクトの連絡先が [構成アイテムの詳細] ページに表示されます。
- CI を案件に追加します。

アクティビティ イベントが発生すると、ルールが実装されて条件が評価されます。条件の基準が満たされた場合、チケット アクティビティについて説明する通知メッセージが、この通知ルールに関連付けられた CI のすべての連絡先に送信されます。

通知ログ リーダ

通知ログ リーダには、ログイン ユーザ宛てに届いた通知が、日付、緊急度、およびステータス別に表示されます。通知ログ リーダでは、以下の操作を実行できます。

- 表示順序を変更できます。また、新しいメッセージを受信したら自動的に通知ログ リーダを表示するようにメニュー オプションを設定できます。
- 通知メッセージをダブルクリックすると、通知に関連付けられたチケットの詳細ページが表示されます。

- 分析のために選択基準を入力してデータベースを検索したり、フィールドに入力したデータに基づいて通知メッセージを選択したりして、通知メッセージを監視できます。たとえば、[メッセージステータス] フィールドを [クリアされていません] に変更すると、クリアされていない通知メッセージのみを一覧表示できます。
- 通知のリストを管理可能なサイズに保つために、通知メッセージをクリアできます。クリアされた通知は、通知ログリーダーへの初回アクセス時には表示されませんが、必要に応じて表示できます。

通知ログリーダーのオプションの設定

通知ログリーダーのオプションを設定して、案件に対して新しいメッセージを受信したときの通知方法を定義できます。

通知ログリーダーのオプションを設定する方法

1. [ServiceDesk] タブで、[表示] - [ログリーダー] を参照します。
[通知ログリーダー] ページが表示されます。
2. 各通知の左にあるチェックボックスを使用して、以下のオプションを設定します。項目を選択して、[選択のクリア] や [選択範囲の削除] のような操作を実行できます。

ヘッダ

メッセージのヘッダが表示されます。ヘッダには通常、チケット番号とアクティビティタイプが含まれます。

開始日

通知が [ログリーダー] ウィンドウに送信された日付と時刻が表示されます。

ステータス

通知のステータスが表示されます。

緊急度

通知の緊急度のレベル（低、通常、高、または緊急）を定義します。これは、各アクティビティの相対的な重要度を示します。緊急度レベルは事前定義されていますが、通知方法やアクティビティの関連付けなど、通知のその他の要素について、システム管理者がセットアップする必要があります。さらにシステム管理者は、連絡先とグループに使用する通知方法を、緊急度レベルごとに定義する必要があります。

メッセージ テキスト

通知メッセージのフルテキストです。

ログ リーダにすべての変更が表示されます。

3. [閉じる] をクリックします。

[通知ログ リーダ] ページが閉じ、オプションが設定されます。

パーソナリ化した応答

パーソナリ化した応答を作成し、作成した応答を、アクティビティをレコードに追加するときにリクエスト、案件、および変更要求レコードに添付できます。たとえば、パーソナリ化した応答は、[アクティビティ] メニューから表示可能な[ステータスの変更] ウィンドウまたは[ログ コメント] ウィンドウで追加できます。

パーソナリ化した応答の作成

リクエスト、案件、および変更要求レコードに追加するパーソナリ化した応答を作成できます。

パーソナリ化した応答を作成する方法

1. [管理] タブで、[Service Desk] - [パーソナル応答] に移動します。
[パーソナル応答] リスト ページが表示されます。
2. [新規作成] をクリックします。
[パーソナリ化した応答の新規作成] ページが表示されます。
3. ページ内のフィールドに値を入力します。

応答担当者

応答を所有する連絡先を指定します。このフィールドを空欄にしておくと、すべてのアナリストがこの応答を使用できます。

応答

この応答を受け取る全員に配信するテキストを指定します。このフィールドには、最大 1000 文字まで入力できます。

また、以下のように変数を使用することもできます。

```
チケットの ref_num: @{call_req_id.ref_num}  
担当者: @{call_req_id.assignee.combo_name}  
顧客: @{call_req_id.customer.combo_name}  
説明: @{call_req_id.description}
```

4. この応答を使用できるレコードのタイプを選択します。[保存]をクリックします。

パーソナリ化した応答が作成されます。

パーソナリ化した応答の変数の置き換え

パーソナリ化した応答テキストには変数を埋め込むことができます。変数を使用すると、情報を対応するリクエスト、変更要求、案件、問題、またはインシデントに置き換えることができます。変数の構文は、アクティビティ通知メッセージのテンプレートや手動通知アクティビティメッセージのテキストなど、**CA SDM** 製品の他の部分で使用されている構文と同じです。情報を置き換えられるのは、対応するリクエスト、変更要求、案件、問題、またはインシデントの情報のみです。アクティビティ通知メッセージのテンプレートおよび手動通知アクティビティメッセージのテキストでは、アクティビティ ログ レコードの情報に置き換えることもできます。

各オブジェクトタイプ（リクエスト、変更要求、案件、インシデント、および問題）のチェック ボックスをオンにすると、選択時に応答がフィルタ処理されます。オフになっているオブジェクトタイプは、応答で使用できません。たとえば、リクエストのチェック ボックスのみがオンの場合、応答はリクエストのアクティビティにのみ表示されます。

1 つの応答をすべてのオブジェクトタイプ（リクエスト、変更要求、案件、問題、またはインシデント）に使用できます。属性はオブジェクトによって異なるので、（案件の応答でリクエスト番号を置き換えるなど）オブジェクトにない情報は置き換えられません。

サンプルの応答テキストで各オブジェクトタイプの変数を以下のように置き換えてみます。

```
This is Request # '{@call_req_id.ref_num}'  
This is Change Order # ' '{@change_id.chg_ref_num}'  
This is Issue # '{@issue_id.ref_num}'
```

リクエストの場合は、以下のように置き換えられます。

```
This is Request # 'cr_demo:11'  
This is Change Order # "  
This is Issue # "
```

変更要求の場合は、以下のように置き換えられます。

```
This is Request # "  
This is Change Order # 'chg_demo:3'  
This is Issue # "
```

案件の場合は、以下のように置き換えられます。

```
This is Request # "  
This is Change Order # "  
This is Issue # 'iss_demo:6'
```

〔この応答を次に表示〕チェック ボックスを活用すると、対応するオブジェクト（リクエスト、変更要求、案件、問題、またはインシデント）に適した置換変数を使用してさまざまな応答を作成できます。

各オブジェクトに対する置換変数の書式は以下のとおりです。

オブジェクト

リクエスト/インシデント/問題

変更要求

案件

変数の書式

@{call_req_id.attr}

@{change_id.attr}

@{issue_id.attr}

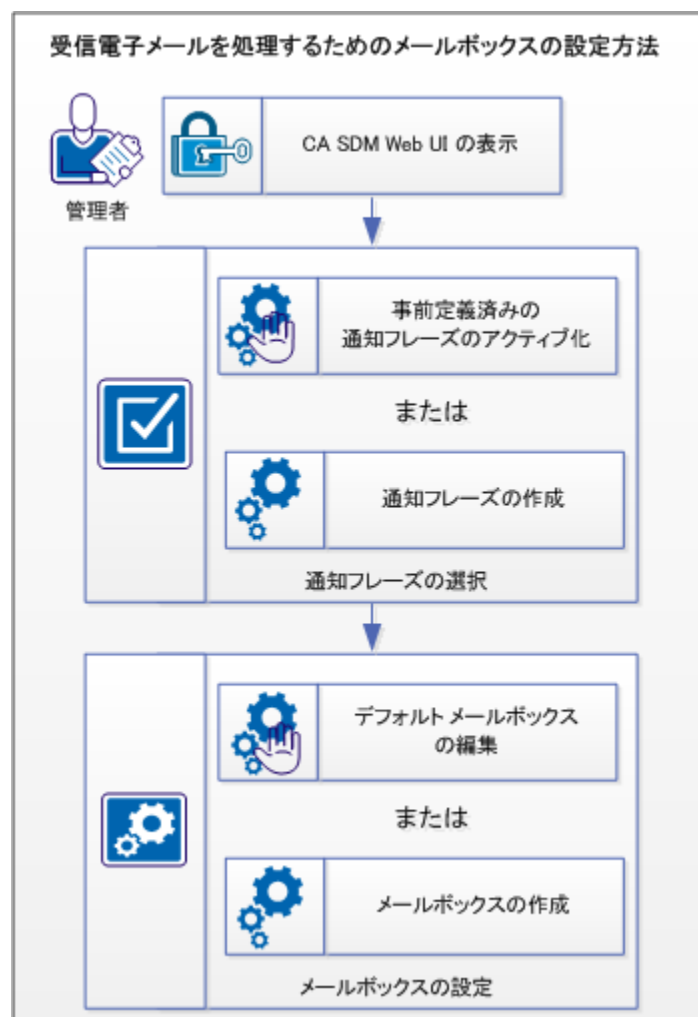
置き換えは、応答が〔ユーザの説明〕フィールドにコピーされるときに実行されます。応答は、〔パーソナリ化した応答〕ドロップダウン リストで選択され、ドロップダウン リストからフォーカスがなくなるときにコピーされます。

受信電子メールを処理するためのメールボックスの設定方法

電子メールでは、従業員や顧客などのエンドユーザと通信することができます。CA SDM のメールボックスは、ユーザからの受信電子メールを処理し、電子メールに従ってアクションを実行します。たとえば、インシデントを作成するために、ユーザが電子メールを CA SDM に送信したとします。メールボックスは、電子メールを確認し、インシデントを作成して、インシデントが正常に作成されたことを示す通知をユーザに送信します。

CA SDM では、アクティブで、組織で使用可能なデフォルト メールボックス（デフォルトという名前の）を提供します。デフォルト メールボックスを変更したり、追加のメールボックスを作成したり、あるいはそれら両方を行うことができます。メールボックスを作成した後、またはデフォルトのメールボックスを変更した後、メールボックスルールを定義します。メールボックスルールを使用すると、メールボックスから取得したメッセージに対して発生するさまざまなアクション、返答またはその両方を設定できます。

以下の図は、メールボックスを設定して、受信電子メールを処理する方法を示しています。



次の手順に従ってください:

1. [CA SDM Web UI を開きます](#) (P. 222)。
2. [通知フレーズを選択します](#) (P. 249)。
 - [事前定義済みの通知フレーズをアクティブ化します](#) (P. 250)。
 - [通知フレーズを作成します](#) (P. 251)。
3. [メールボックスを設定します](#) (P. 257)。
 - [デフォルトのメールボックスを編集します](#) (P. 257)。
 - [メールボックスを作成します](#) (P. 263)。

CA SDM Web UI の表示

CA SDM の設定に応じて、以下のサーバから Web UI にログインします。

- 標準：プライマリまたはセカンダリ サーバ
- 高可用性：アプリケーションサーバまたはバックグラウンドサーバ

通知フレーズの選択

通知フレーズは、電子メールの送信者に送信されます。たとえば、インシデントが正常に作成されたことを確認するために送信されます。CA SDM は、デフォルトでは非アクティブに設定されている事前定義済みの通知フレーズを提供します。フレーズをアクティブ化および変更できます。また、組織の要件に最も適合する通知フレーズも作成できます。

以下のオプションから選択します。

- [事前定義済みの通知フレーズのアクティブ化](#) (P. 250)。
- [通知フレーズの作成](#) (P. 251)

事前定義済みの通知フレーズのアクティブ化

デフォルトでは、事前定義済みの通知フレーズは非アクティブに設定されています。通知フレーズをアクティブにすると、通知でフレーズを使用できるようになります。

注: マルチテナンシーをインストールしている場合は、ドロップダウン リストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで [通知] - [通知フレーズ] を選択します。
[通知フレーズ リスト] ページが開きます。
2. 通知フレーズを検索します。
3. アクティブ化するフレーズをクリックします。たとえば、[履歴を通知 - 変更] を選択します。
[通知フレーズの詳細] ページが開きます。
4. [編集] をクリックします。
[通知フレーズの更新] ページが開きます。
5. [アクティブ] ドロップダウン リストから [アクティブ] を選択します。
6. (オプション) 必要に応じて、その他の[フィールド](#) (P. 251) を変更します。たとえば、フレーズを変更します。
7. [保存] をクリックします。
[通知フレーズの詳細] ページが開きます。
8. [ウィンドウを閉じる] をクリックします。
通知フレーズがアクティブ化されます。

通知フレーズの作成

標準化されたテキストおよびマクロを含む通知フレーズを作成できます。この通知フレーズは、ユーザからの電子メールへの返信として送信されます。

注: マルチテナンシーをインストールしている場合は、ドロップダウン リストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで [通知] - [通知フレーズ] を選択します。
[通知フレーズ リスト] ページが開きます。
2. [新規作成] をクリックします。
[通知フレーズの新規作成] ページが開きます。
3. 必要に応じて、[通知フレーズのフィールド](#) (P. 251) にデータを入力します。
4. [保存] をクリックします。
通知フレーズが作成されます。

通知フレーズのフィールド

以下のフィールドに入力して、通知フレーズを編集または作成します。

シンボル

このレコードの一意の識別子を定義します。

コード

`usp_notification_phrase` テーブルで、通知フレーズに使用する一意の値を指定します。`usp_notification_phrase` テーブルには、通知メッセージテンプレートで使用できる一般的なフレーズがリストされます。

`usp_notification_phrase` テーブルの詳細については、「[テクニカルリファレンス ガイド](#)」を参照してください。

フレーズ

通知用のフレーズを指定します。プレーンテキストバージョンとHTMLバージョンの両方を指定できます。HTML ではほとんどの空白が単一のスペースとして処理されるため、改行または段落をタグで指定する必要があります。

たとえば、以下のプレーン テキスト フレーズは、機密に関する注意事項の通知フレーズで使用されます。

この電子メール、およびこれに添付されているファイルは、宛名として記載されている人物だけが読むことができるものであり、極秘情報が記載されている場合があります。許可なく閲覧、使用、開示、または配布することを禁じます。この電子メールの意図されている受信者でない場合は、この電子メール、およびそれで転送された任意のファイルを削除して、送信者にすぐに通知します。

以下の HTML フレーズを使用して、通知リストを表示するようにユーザに求めることができます。

通知リストを表示するには次の URL をクリックしてください：

`@{call_req_id.web_url}+HTML=cr_lr.html+INSTANCE=@{ID}`

フレーズの詳細については、[通知コードとフレーズ](#) (P. 252)のトピックを参照してください。

通知コードおよび通知フレーズ

通知フレーズを使用すると、テキストや定型句を入力したり、各通知テンプレートに保持したりしなくても、多数の異なる通知メッセージに、標準化された情報やテキストを追加できます。以下に例を示します。

チケットへの追加情報を追加するためこの通知へ返答

フレーズは、テキストを複数のメッセージテンプレートで使えるようにテキスト標準化します。たとえば、単一のレコード内の機密に関する注意事項のような共通の句を保持し、複数のメッセージテンプレートでそれを使用できます。さらに通知フレーズは、応答通知のようなメッセージへの返答や Web の URL リンクにも役立ちます。CA SDM はフレーズを提供し、ユーザは独自のフレーズを作成できます。メッセージテンプレートで使用するフレーズは、グローバルにアクティブ、または非アクティブに設定できます。（通知フレーズはデフォルトでは非アクティブです。）フレーズが非アクティブの場合、フレーズを使用するすべてのメッセージテンプレート内でフレーズの使用が中止されます。

通知フレーズは、受信電子メールメッセージに対する自動応答にも使用できます。このタイプのメッセージ用の処理コンテキストは他とは異なり、メッセージで使用するフレーズの一部のマクロ（`ref_num`、`web_url` など）で使われるプレフィックス（`change_id.`、`issue_id.`、`call_req_id.`）が省略されます。この結果、通知テンプレートと電子メール自動応答とで通知フレーズを共有することはできません。

CA SDM が提供するフレーズの例を以下に示します。

シンボル	コード	フレーズ
履歴を通知 - 変更	<code>notify_history_chg</code>	通知リストを表示するには以下の URL をクリックします。 <code>@{change_id.web_url}+HTMPL=chg_lr.html+INSTANCE=@{ID}</code>
履歴を通知 - 案件	<code>notify_history_iss</code>	通知リストを表示するには以下の URL をクリックします。 <code>@{issue_id.web_url}+HTMPL=iss_lr.html+INSTANCE=@{ID}</code>
履歴を通知 - リクエスト / インシデント / 問題	<code>notify_history_cr</code>	通知リストを表示するには以下の URL をクリックします。 <code>@{call_req_id.web_url}+HTMPL=cr_lr.html+INSTANCE=@{ID}</code>

例: 新しいフレーズ

ユーザが作成できるフレーズの例を以下に示します。

シンボル	コード	フレーズ
機密通知	ConfidentialNotice	この電子メール、およびこれに添付されているファイルは、宛名として記載されている人物だけが読むことができるものであり、極秘情報が記載されている場合があります。許可なく閲覧、使用、開示、または配布することを禁じます。あなたが、この電子メールの宛名として記載されている受信者でない場合は、この電子メール、およびこれに付随するファイルすべてのファイルを削除し、すぐに送信者にご連絡ください。
インシデント通知応答	IncidentReply	インシデントにコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。 %incident_id=@{call_req_id.ref_num}
インシデント URL 通知	IncidentURL	表示するには次の URL をクリックします。 @{call_req_id.web_url}

注: テキスト形式と HTML 形式のメッセージテンプレート、または電子メールの自動応答にはそれぞれ個別のフレーズを使用します。HTML では、ほとんどの空白が 1 つのスペースに統合されるため、改行や段落の区切りはタグで指定する必要があります。テキスト形式のメッセージに含まれる HTML タグは、タグとして処理されずに表示されます。

通知フレーズの構文

以下に示すマクロ構文を使用して、メッセージテンプレートおよび電子メール返答メッセージに通知フレーズを挿入できます。

```
@{notification_phrase[code].phrase}
```

code

メッセージフレーズ (usp_notification_phrase) テーブルの ConfidentialNotice のような一意のコード値を指定します。

注: usp_notification_phrase テーブルには、通知メッセージテンプレートが使用できる共通のフレーズが記載されています。
usp_notification_phrase テーブルの詳細については、「テクニカル リファレンス ガイド」を参照してください。

以下に例を示します。

```
@{notification_phrase[IncidentURL1].phrase}
```

```
@{notification_phrase[RequestReply].phrase}
```

CA SDM がマクロを検出する際、usp_notification_phrase テーブルのフレーズ テキストにより構文が置換されます。一致するコードが存在しない場合 (あるいはそれが非アクティブである場合)、空の文字列によりマクロが置換されます。標準ログ (STDLOG) にはエラーは書き込まれず、潜在的 問題の解決に役立つ警告メッセージが記録されます。

注: ほかのフレーズに埋め込むフレーズの深さは、NX_MAX_EXPAND_DEPTH 環境変数 (P. 558) で設定した最大値に制限されま す。この制限により、フレーズの処理中に偶然、自己参照 (自身に埋め 込まれる)、または循環参照 (埋め込まれているフレーズにフレーズが埋め 込まれる) が発生する問題を防ぐことができます。

例: メッセージにおける通知フレーズの表示

この例では、通知フレーズが通知メッセージにどのように表示されるかを 示します。この例では、以下のコードおよび句を使用します。

コード	フレーズ
ConfidentialNotice	この電子メール、およびこれに添付されているファイルは、宛名と して記載されている人物だけが読むことができるものであり、極秘 情報が記載されている場合があります。許可なく閲覧、使用、開示、 または配布することを禁じます。この電子メールの意図されている 受信者でない場合は、この電子メール、およびそれで転送された任 意のファイルを削除して、送信者にすぐに通知します。

コード	フレーズ
IncidentReply	インシデントにコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。 %incident_id=@{call_req_id.ref_num}
IncidentURL	表示するには次の URL をクリックします。 @{call_req_id.web_url}

以下のメッセージ テンプレートには通知フレーズが含まれます。

@{call_req_id.type.sym} @{call_req_id.ref_num} クローズされています。
 担当者： @{call_req_id.assignee.combo_name}
 顧客： @{call_req_id.customer.combo_name}
 説明： @{call_req_id.description}

@{notification_phrase[IncidentURL].phrase}
 @{notification_phrase[IncidentReply].phrase}

@{notification_phrase[ConfidentialNotice].phrase}

メッセージでフレーズは以下のように表示されます。

インシデント 1234 はクローズされています。
 担当者： アナリスト、Joe
 顧客： Doe, John
 説明： これは私の問題の説明です。

表示するには次の URL をクリックします。
<http://helpdesk/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=chg+SKIPLIST=1+QBE.EQ.id=400723>

インシデントにコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。
 %incident_id=1234

この電子メール、およびこれに添付されているファイルは、宛名として記載されている人物だけが読むことができるものであり、極秘情報が記載されている場合があります。許可なく閲覧、使用、開示、または配布することを禁じます。この電子メールの意図されている受信者でない場合は、この電子メール、およびそれで転送された任意のファイルを削除して、送信者にすぐに通知します。

メールボックスの設定

CA SDM は、メール サーバに接続するデフォルトのメールボックスを提供します。このデフォルトのメールボックスを設定して、パスワード、ユーザ名、ホスト名などを変更できます。また、組織の要件に合わせて、追加のメールボックスを作成することもできます。メールボックスは単一のグローバルな定義セットではなく、それぞれが自身の定義を持つことができます。複数のメールボックスを定義し、各メールボックスに異なるテンプレートやデフォルト値を使用できます。複数の定義により、テナントごとに個別のメールボックスを使用させたり、テナントや組織ごとに異なるメールボックスを使用させたり、各メールボックスに異なる動作を実行させたりすることができます。

以下のいずれかまたは両方を選択します。

重要: メールボックスルールを設定する前に、関連するメールボックスを非アクティブに設定することをお勧めします。そうしないと、メールサーバが最初の変更と最後の変更の間に取得するメッセージが、メッセージの取得時に有効になっているルールで処理されます。

- [デフォルトのメールボックスを編集します](#) (P. 257)。
- [メールボックスを作成します](#) (P. 263)。

デフォルト メールボックスの編集

CA SDM では、組織の受信メール配信の要件に合わせて編集できるアクティブなデフォルト メールボックスを提供します。

次の手順に従ってください:

1. [管理] タブで [電子メール] - [メールボックス] を選択します。
[メールボックス リスト] ページが開きます。
2. [名前] 列で [デフォルト] をクリックします。
[デフォルト メールボックスの詳細] ページが開きます。
3. [編集] をクリックします。

4. 必要に応じて他のフィールドを指定するか、更新します。

チェック間隔

メールサーバが新しい電子メールに対してポーリングされるまでの時間を指定します。

アクティブ

メールボックスのステータスを示します。

電子メール タイプ

メールサーバが使用するプロトコルを指定します。CA SDM は、POP3 と IMAP4 の両方をサポートしています。IMAP4 を選択した場合、CA SDM は、メールボックスの [受信トレイ] フォルダのみをポーリングします。

ホスト名

電子メールサーバのホスト名を指定します。

ポートのオーバーライド

デフォルトのポート番号がオーバーライドされている場合は、ポート番号を指定します。

ユーザ名

メールサーバのユーザ ID を指定します。

パスワード

メールサーバのパスワードを指定します。

セキュリティレベル

SMTP セキュリティ レベルを指定します。

添付ファイルリポジトリ

電子メールの添付ファイルが格納されるリポジトリを指定します。

電子メール全体を添付

電子メール全体を添付ファイルとして許可するかどうかを指定します。

添付ファイルを強制的に分割

電子メール全体が添付ファイルとして追加される場合、電子メール内の添付ファイルをすべて分割するかどうかを指定します。電子メールおよびその添付ファイルが個別のファイルに分割され、チケットに添付されます。[電子メール全体を添付] オプションが選択されている場合のみ適用可能です。

匿名を許可

チケットが匿名のメールから作成できるかどうかを指定します。

不明な電子メールを保存

メールボックスで定義されたルールが処理しなかった電子メールを保存するかどうかを指定します。これらの電子メールは `$NX_ROOT/site/mail_unknown` に格納されます。

返信先アドレスの使用

別の電子メール アドレスを返信に使用するかどうかを指定します。

TLS の使用

電子メールでトランスポート レイヤ セキュリティのサポートを使用するかどうかを指定します。

CA 認証パス

信頼できる証明書が展開されているパスを指定します。

注: 高可用性設定では、バックグラウンドサーバとスタンバイサーバの両方の同じ場所に信頼された証明書を展開してください。CA SDM は、CA 証明書の Base 64 エンコード (PEM) 形式をサポートします。

5. (オプション) 必要に応じて[メールボックス ルール](#) (P. 270)および[ポリシー](#) (P. 269)を作成または更新します。

注: 1つのメールボックスに適用するルールは、別のメールボックスに関連付けることはできません。別のメールボックスに対して同じルールを再使用するには、それらのルールを別のメールボックス用に再作成します。また、既存のメールボックスをコピーすることもできます。

重要: メールボックスルールを設定する前に、関連するメールボックスを非アクティブに設定することをお勧めします。そうしないと、メールサーバが最初の変更と最後の変更の間に取得するメッセージが、その時に有効になっているルールで処理されます。

6. [保存] をクリックします。

デフォルト メールボックスへの変更は保存されて適用されます。最初のポーリングは1秒後に発生します。

複数のメールボックス

CA SDM は、複数のメールボックスを処理し管理することができます。メールボックスは単一のグローバルな定義セットではなく、それぞれが自身の定義を持つことができます。複数のメールボックスを定義し、各メールボックスに異なるテンプレートやデフォルト値を使用できます。複数の定義により、テナントごとに個別のメールボックスを使用させたり、テナントや組織ごとに異なるメールボックスを使用させたり、各メールボックスに異なる動作を実行させたりすることができます。複数のメールボックスの設定には、管理インターフェースを使用します。メールボックスには以下のテーブルが含まれます。

- `usp_mailbox` - メールボックスを定義します。
- `usp_mailbox_rule` - 各メールボックスにルールを指定します。
メールボックスのルールにより、**Text API** デフォルトが提供されるため、インターフェースに固有に構成された他のソフトウェアやパラメータ（カテゴリ、担当者など）を使用して電子メールインターフェースを作成できます。

注: IMAP サーバは、単一のアカウントで使用する複数のメールボックスをサポートしますが、代替メールボックスはサポートされていません。サポートされているのは、デフォルトの受信トレイのみです。

複数のメールボックスでルールを使用する方法

プライマリ サーバ上の **Mail Eater** (`pdm_maileater_nxd`) コンポーネントは、メールボックス接続とルールを使用して、1 つ以上のメールサーバ上の 1 つ以上のアカウントからメッセージを読み取って処理します。**Mail Eater** は、メールボックスを順に処理し（一度に 1 つのメールボックスのみが処理されます）、シーケンス番号順にルールを処理します。

複数のメールボックスは以下のようにルールを使用します。

1. プライマリ サーバの起動時に、**Mail Eater** は以下のテーブルを読み取ります。

usp_mailbox

メール サーバへの接続を表します。

usp_mailbox_rules

接続 (**usp_mailbox**) に適用されるルールを表します。

Contact_Method

自動応答に使用される連絡方法を表します。

Document_Repository

添付ファイルを保存するドキュメント リポジトリを表します。

Mail Eater は、これらのテーブルのいずれかのオブジェクトに変更（追加オブジェクトの追加も含む）が加えられると、その変更を自動的に検出します。**usp_mailbox** または **usp_mailbox_rule** に変更が加えられた場合、変更の適用後、影響を受けたメールボックスのポーリング間隔は 1 秒に再スケジュールされます。

2. 各メールボックスで定義された間隔で、**Mail Eater** は、関連するアカウントの受信トレイ内の各電子メールを取得し、以下のように電子メールを処理します。
 - a. 電子メールアドレスのポリシー違反を確認します。**Mail Eater** が違反を検出すると、処理が停止し、メールボックスの定義に従って標準ログに反映されます。
 - b. 電子メールを、そのメールボックスに属する各ルール (**mailbox_rule**) と比較します。
 - c. 一致するルールが検出された場合、ポスト用にそのメッセージを **Text API** にサブミットし、ルールに対して指定されたアクションに基づき、必要に応じてユーザに応答します。

応答電子メールでは、フィルタ文字列でオブジェクトが識別され、処理に **Text API** が使用されます。処理が完了した後、応答は宛先アドレスまたは差出人アドレスのいずれかに送られます。
 - d. **Mail Eater** が一致するルールを検出すると、その後、他のルールの確認は行われず、**Mail Eater** は、受信トレイ内の次の電子メールを処理します。
 - e. 一致するルールが検出されないと、メッセージは破棄されます。

3. **Mail Eater** が受信トレイ用の電子メールをすべて処理した後、処理済みのメッセージおよび破棄されたメッセージはメール サーバからパージされ、次の処理間隔がスケジュールされます。

メールボックスの作成

メールサーバに接続し、ホスト、ユーザ、パスワードなどの値を設定するために設定するメールボックスを作成できます。

次の手順に従ってください:

1. [管理] タブで [電子メール] - [メールボックス] を選択します。
[メールボックス リスト] ページが開きます。
2. [新規作成] をクリックします。
[メールボックスの詳細] ページが開きます。
3. 必要に応じてフィールドにデータを入力します。

チェック間隔

メールサーバが新しい電子メールに対してポーリングされるまでの時間を指定します。

アクティブ

メールボックスのステータスを示します。

電子メール タイプ

メールサーバが使用するプロトコルを指定します。CA SDM は、POP3 と IMAP4 の両方をサポートしています。IMAP4 を選択した場合、CA SDM は、メールボックスの [受信トレイ] フォルダのみをポーリングします。

ホスト名

電子メールサーバのホスト名を指定します。

ポートのオーバーライド

デフォルトのポート番号がオーバーライドされている場合は、ポート番号を指定します。

ユーザ名

メールサーバのユーザ ID を指定します。

パスワード

メールサーバのパスワードを指定します。

セキュリティレベル

SMTP セキュリティ レベルを指定します。

添付ファイルリポジトリ

電子メールの添付ファイルが格納されるリポジトリを指定します。

電子メール全体を添付

電子メール全体を添付ファイルとして許可するかどうかを指定します。

添付ファイルを強制的に分割

電子メール全体が添付ファイルとして追加される場合、電子メール内の添付ファイルをすべて分割するかどうかを指定します。電子メールおよびその添付ファイルが個別のファイルに分割され、チケットに添付されます。[電子メール全体を添付] オプションが選択されている場合のみ適用可能です。

匿名を許可

チケットが匿名のメールから作成できるかどうかを指定します。

不明な電子メールを保存

メールボックスで定義されたルールが処理しなかった電子メールを保存するかどうかを指定します。これらの電子メールは `$NX_ROOT/site/mail_unknown` に格納されます。

返信先アドレスの使用

別の電子メール アドレスを返信に使用するかどうかを指定します。

TLS の使用

電子メールでトランスポート レイヤ セキュリティのサポートを使用するかどうかを指定します。

CA 認証パス

信頼できる証明書が展開されているパスを指定します。

注: 高可用性設定では、バックグラウンドサーバとスタンバイサーバの両方の同じ場所に信頼された証明書を展開してください。CA SDM は、CA 証明書の Base 64 エンコード (PEM) 形式をサポートします。

4. [ルール] タブで [新規作成] をクリックして、メールボックスルールを作成します。

[メールボックス ルールの新規作成] ページが開きます。

注: 1つのメールボックスに適用するルールは、別のメールボックスに関連付けることはできません。別のメールボックスに対して同じルールを再使用するには、それらのルールを別のメールボックス用に再作成します。また、既存のメールボックスをコピーすることもできます。

重要: メールボックスルールを設定する前に、関連するメールボックスを非アクティブに設定することをお勧めします。 そうしないと、メールサーバが最初の変更と最後の変更の間に取得するメッセージが、その時に有効になっているルールで処理されます。

5. 必要に応じて[メールボックス ルールのフィールド](#) (P. 270)に入力し、[保存] をクリックします。
6. [ポリシー] タブを選択してメールボックス ポリシーを定義し、特定のタイプの電子メールの不正使用から組織を保護します。必要に応じて[メールボックス ポリシーのフィールド](#) (P. 269)に入力し、[保存] をクリックします。

メールボックスが作成されます。

複数のメールボックスを使用している場合、Mail Eater

(pdm_maileater_nxd) コンポーネントは、メールボックス接続とルールを使用して、1つ以上のメールサーバ上の1つ以上のアカウントからメッセージを読み取って処理します。Mail Eater は、CA SDM の設定に応じて、以下のサーバで実行されます。

- 標準: プライマリ サーバ
- 高可用性: バックグラウンドサーバ

Mail Eater は、メールボックスを順にポーリングし（一度に 1 つのメールボックスのみが処理されます）、以下のようにシーケンス番号順にルールを処理します。

- a. プライマリ サーバまたはバックグラウンドサーバの起動時に、**Mail Eater** はデータベースの以下のテーブルを読み取ります。

usp_mailbox

メールサーバへの接続を表します。

usp_mailbox_rules

接続（**usp_mailbox**）に適用されるルールを表します。

Contact_Method

自動応答に使用される連絡方法を表します。

Document_Repository

添付ファイルを保存するドキュメントリポジトリを表します。

Mail Eater は、これらのテーブルのいずれかのオブジェクトに変更（追加オブジェクトの追加も含む）が加えられると、その変更を自動的に検出します。**usp_mailbox** または **usp_mailbox_rule** に変更が加えられた場合、変更の適用後、影響を受けたメールボックスのポーリング間隔は 1 秒に再スケジュールされます。

- b. 各メールボックスで定義された間隔で、**Mail Eater** は、関連するアカウントの受信トレイ内の各電子メールを取得し、以下のように電子メールを処理します。
- c. 電子メールアドレスのポリシー違反を確認します。**Mail Eater** が違反を検出すると、処理が停止し、メールボックスの定義に従って標準ログに反映されます。
- d. 電子メールを、そのメールボックスに属する各ルール（**mailbox_rule**）と比較します。

- e. 一致するルールが検出された場合、ポスト用にそのメッセージを **Text API** にサブミットし、ルールに対して指定されたアクションに基づき、必要に応じてユーザに応答します。

応答電子メールでは、フィルタ文字列でオブジェクトが識別され、処理に **Text API** が使用されます。処理が完了した後、応答は宛先アドレスまたは差出人アドレスのいずれかに送られます。

- f. **Mail Eater** が一致するルールを検出すると、その後、他のルールの確認は行われず、**Mail Eater** は、受信トレイ内の次の電子メールを処理します。
- g. 一致するルールが検出されないと、メッセージは破棄されます。

Mail Eater が受信トレイ用の電子メールをすべて処理した後、処理済みのメッセージおよび破棄されたメッセージはメールサーバからパージされ、次の処理間隔がスケジュールされます。

メールボックス ポリシーの作成

受信トレイへのメール配信に必要な任意のアクション、応答またはその両方に適用されるポリシーを作成できます。

メールボックス ポリシーを作成する方法

1. [管理] タブで、[電子メール] - [メールボックス] を選択します。
[メールボックス リスト] ページが表示され、属性がリスト表示されます。
2. ポリシーを設定するメールボックスの名前をクリックします。
[メールボックスの詳細] ページが表示されます。
3. [ポリシー] タブをクリックします。
メールボックスに関連付けられたポリシーの詳細が表示されます。
4. [編集] をクリックします。
フィールドを編集できます。
5. 必要に応じて [フィールド](#) (P. 268) にデータを入力します。
6. [保存] をクリックします。
メールボックス ポリシーが設定され、すぐに有効になります。

電子メール アドレス/時間

1 時間当たりの、1 つの電子アドレスにおける最大電子メール数を指定します。以下の値を指定できます。

- -1 - 無制限（デフォルト）
- 0 - 電子メールは不可
- 1 - 最大数の電子メールを許可します。

違反をログに記録

標準ログに違反を記録します。以下の値を指定できます。

- ログに記録しない
- 最初の違反のみ（デフォルト）
- すべての違反

注： [最初の違反のみ] オプションは、メールボックス ポリシーに違反するメッセージに関連付けられた電子メールアドレスのリストを保持し、ログの記録においてそのリストを使用して、ログ エントリが重複しないようにします。Mail Eater デーモンが再起動されると、このリストはクリアされます。ただし、[最初の違反のみ] オプションから他のいずれかのオプションに設定を変更し、また [最初の違反のみ] オプションに戻した場合、この設定の下でログに記録された電子メールアドレスのリストはクリアされません。メールボックスでこの設定を使用している間に多数の違反がログに記録される場合は、Mail Eater デーモンを定期的に再起動してリストをクリアするか、[ログに記録しない] オプションを使用することを推奨します。

リレーション リスト

電子メールを処理することのできる電子メールアドレスまたはドメインを指定します。リストに一致する電子メールのみが許可されます。複数のアドレスまたはドメインを指定するには、カンマ、セミコロン、スペース文字、または改行で区切ります。アスタリスク (*) の単独でのエントリは「世界ドメイン」となり、除外リストに含まれないすべてのドメインに一致します。

除外リスト

電子メールを処理することのできない電子メールアドレスまたはドメインを指定します。複数のアドレスまたはドメインを指定する場合は、カンマ、セミコロン、スペース、または改行で区切ります。

注: 除外リスト内のアドレスは、包含リスト内のどの値にも優先します。包含リスト内のアドレスは、除外リスト内のドメインに優先します。本来は禁止されるはずのドメイン内の特定の送信者を個別に除外することができます。除外リスト内のドメインは、包含リスト内の世界ドメインに優先します。世界ドメインは除外リスト内では無効です。

メールボックス ポリシーのフィールド

以下のフィールドを使用してポリシーを実装できます。

電子メール アドレス/時間

すべての電子メールアドレスからそのメールボックスに送信できる 1 時間あたりの電子メールの数を指定します。制限を超えた電子メールアドレスは、電子メールアドレスは除外リストに追加されます。ユーザが除外リストから電子メールアドレスを削除するまで、その送信者の電子メールアドレスからのメッセージは、そのメールボックスでは処理されなくなります。

違反をログに記録

stdlog ファイルで、ポリシーに違反する電子メールアドレスをログに記録するかどうかを指定します。

リレーション リスト

電子メールの送信が許可されている電子メールアドレス（たとえば user@company.com）または電子メール ドメイン（たとえば company.com）を指定します。

各メールボックスのデフォルトの包含リストはアスタリスク (*) です。アスタリスクは、このリストでは単独で完全な名前として、ワールドドメインを指定し、除外リストに含まれていないすべての電子メールドメインを表します。この表現は、包含リストが許可されたドメインの完全なリストか、または除外リスト内のドメインに対する例外かどうかというあいまいさを、以下のように防ぎます。

- ワールドドメインが含まれる包含リストは、包含リスト内の他のすべてのエントリは除外リストの例外であり、除外リスト内のドメインかアドレスのみが（包含リスト内の特定のアドレスを除いて）ブロックされることを指定します。

- ワールドドメインを含まない包含リストは、包含リストにリスト記載されているアドレスおよびドメインのみ、または、送信者のドメイン（特定のアドレスが包含リストに載っていない場合）かアドレスが、除外リストにない場合にのみ送信できることを指定します。

除外リスト

電子メールの送信が許可されていない電子メールアドレス（たとえば `user@company.com`）または電子メールドメイン（たとえば `company.com`）を指定します。

注: メールボックス ポリシーは単一の関連するメールボックスのみに関連します。受信できる電子メールの最大数に違反したために、1つのメールボックスの除外リストに自動的に追加されたアドレスは、ほかのメールボックスの除外リストには自動的に追加されません。また、電子メールの数はほかのメールボックスでは使用されません。

[メールボックス ルール]フィールド

必要に応じて、以下のメールボックス ルールのフィールドに入力します。

シーケンス

ルールのシーケンス番号を指定します。メッセージが、最も小さいシーケンス番号から順にルールと照合されます。

メールボックス

このルールが属するメールボックスを指定します。

アクティブ

ルールをアクティブまたは非アクティブに設定します。

フィルタ

フィルタ パターンで電子メールのどの部分を検索するか、たとえば、件名の内容などを指定します。詳細については、「[メールボックス ルールのパターン マッチング](#) (P. 276)」を参照してください。

フィルタ文字列

電子メールの内容と照合する正規表現文字列を指定します。たとえば、`[ ¥t¥r¥n]request[ ¥t¥r¥n]` などです。プレースホルダ `{{object_id}}` では、特定のチケットとメッセージを関連付けるために使用する Text API に対するアーチファクト値を指定することができます。詳細については、「[フィルタ文字列オブジェクト ID の制限](#) (P. 278)」および「[正規表現の特殊文字](#) (P. 279)」を参照してください。

大文字と小文字を区別しない

パターンと一致する場合、大文字と小文字を区別するかどうかを指定します。

アクション

フィルタ条件が一致する場合に実行されるアクションを指定します。たとえば、オブジェクトの作成/更新などです。

注: ルール アクションの詳細については、「[管理ガイド](#)」を参照してください。

アクション オブジェクト

メッセージアクションが適用されるチケットのタイプを表示します。たとえばリクエストなどです。

最小アーチファクト タイプ

許可するアーチファクト確認の最小タイプを設定します。

なし

アーチファクトの検証を指定しません。この値は、入力ファイルにキーワードを追加しないのと同じです。さらに、**Text API** チケット ID コマンドを受理します。

保護済み

確認用のハッシュに対してチケットを検証します。確認が失敗する場合、アーチファクトは無効とみなされます。また、フィルタリングがアーチファクト（`{{object_id}}`）を検索する場合、電子メールはフィルタリングに失敗します。

セキュア

暗号化されたデータ ブロックからチケット番号を検証します。値が、有効な暗号化済みのチケット番号ではない場合、アーチファクトは無効とみなされます。また、フィルタリングがアーチファクト（`{{object_id}}`）を検索する場合、電子メールはフィルタリングに失敗します。

注: 設定されているタイプよりセキュアなタイプが許可されます。つまり、最小タイプを「保護済み」と設定すると、「保護済み」と「セキュア」の両方が許可されますが、「なし」は許可されません。さらに、「保護済み または「セキュア」が選択された場合、**Text API** チケット ID コマンドは受理されません。アーチファクトの詳細については、「[アーチファクトの使用上の考慮事項 \(P. 281\)](#)」を参照してください。

応答

自動応答を送信する通知方法を指定します。たとえば電子メールなどです。このオプションを設定しない場合、応答は返されません。応答は、メッセージに対するアクションが成功したか失敗したかを示し、通知とは別のものです。複数のメールボックスを使用している場合は、通知方法を使用して[電子メールの応答を設定する](#) (P. 289) ことをお勧めします。

応答サブジェクト

応答の件名文字列を指定します。たとえば、「Service Desk の応答」などです。

stdlog への書き込み

フィルタが一致する場合、標準ログ (stdlog) に電子メール テキストを書き込みます。

ログ エントリのプレフィクス

標準ログ エントリに電子メール テキストを書き込む場合に追加するプレフィックスを指定します。このオプションを使用して、ルールに一致するログ エントリを有効にします。

件名行の追加

処理の前に、元のメッセージからメッセージ本文に件名行を追加します。件名行は最後に追加するか先頭に追加できます。あるいは追加しないこともできます。件名行は、メッセージに対するアクションにより、チケットの [説明] か [ログ コメント] に添付されます。

Text API デフォルト

フィルタが一致した場合の Text API 用の追加のデフォルト コマンドを指定します。text_api.cfg ファイルの [EMAIL_DEFAULTS] セクションの内容と組み合わせます。[TextAPI デフォルト] フィールドには、メールボックスルールに一致した電子メールからのチケットに適用される TextAPI キーワード コマンドを入力します。メッセージが既存のチケットに影響を与える場合、コマンドは適用されません。

[TextAPI デフォルト] コマンドを指定するには、[TextAPI デフォルト] フィールドで各行に 1 つずつコマンドを入力します。コマンドの形式は以下のとおりです。

OBJECT.FIELD=value

注: 先頭のパーセンテージ記号 (%) は含めないでください。これは、同コマンドが電子メールの本文に埋め込まれている場合にのみ必要なものです。

コマンドの形式の例は、以下のとおりです。

REQUEST.PRIORITY=3

PROBLEM.CATEGORY=Facilities

INCIDENT.GROUP=Plumbing

Text API 受信を無視

フィルタが一致した場合にさらに Text API の詳細を無視することを指定します。text_api.cfg ファイルの [EMAIL_IGNORE_INCOMING] セクションの内容と組み合わせます。

[TextAPI 受信を無視] フィールドには、受信電子メール メッセージ内での使用を許可しない TextAPI キーワードコマンドをリスト表示します。このフィールドに記載されたコマンドが、受信電子メール メッセージ内にある場合、すべて無視されます。

[TextAPI 受信を無視] コマンドを指定するには、以下の手順に従います。

- a. [TextAPI 受信を無視] フィールドに、各行に 1 つずつコマンドを入力します。
- b. コマンドの形式は以下のとおりです。

OBJECT.FIELD

注: 先頭のパーセンテージ記号 (%) は含めないでください。これは、同コマンドが電子メールの本文に埋め込まれている場合にのみ必要なものです。

コマンドの形式の例は、以下のとおりです。

CHANGE.ASSIGNEE

PROBLEM.GROUP

REQUEST.EFFORT

- c. `text_api.cfg` ファイルの `[KEYWORDS]` セクションに、いずれかのフィールドに使用されるすべてのコマンドを定義します。このファイルは、`CA SDM` インストールディレクトリの「`site`」サブディレクトリに保存されます。

詳細

ルールに関する情報を指定します。

成功テキスト

メッセージが正常に処理された場合に送信される応答メッセージの、プレーンテキストコンテンツを指定します。以下に例を示します。

リクエストを更新していただきありがとうございます。 サポート技術者から、24 時間以内にご連絡を差し上げます。

また、すでに作成されている場合は、通知フレーズを入力することもできます。たとえば、電子メール自動応答に通知フレーズを使用できます。

リクエストをサブミットしていただきありがとうございます。

`@{notification_phrase[notification phrase code].phrase}`

成功 HTML

メッセージが正常に処理された場合に送信される応答メッセージの、HTML コンテンツを指定します。以下のオプションを選択すると、HTML テキストの編集やプレビューを実行できます。

成功 HTML の編集

HTML をフォーマットできる HTML エディタを開きます。

クイック表示

HTML をプレビューします。

HTML ソース

HTML ソースを表示します。

また、たとえば、以下のような通知フレーズを使用することもできます。

リクエストをサブミットしていただきありがとうございます。 </p>

`@{notification_phrase[notification phrase code].phrase}</p>`

失敗テキスト

メッセージが正常に処理されなかった場合に送信される応答メッセージの、プレーンテキストコンテンツを指定します。また、すでに作成されている場合は、通知フレーズを入力することもできます。たとえば、以下のテキストを使用できます。

リクエストをサブミットしていただきありがとうございます。

@{notification_phrase[notification phrase code].phrase}

失敗 HTML

メッセージが正常に処理されなかった場合に送信される応答メッセージの、HTML コンテンツを指定します。

メールボックス ルールの作成

受信メッセージの特定のキーワードまたは要素を認識し、それらのキーワードや要素を含む受信メッセージに対して必要なアクション、応答、またはその両方を実行するルールを作成できます。

注: 1つのメールボックスに適用するルールは、別のメールボックスに関連付けることはできません。別のメールボックスに対して同じルールを再使用するには、それらのルールを別のメールボックス用に再作成します。また、既存のメールボックスをコピーすることもできます。

重要: メールボックスルールを設定する前に、関連するメールボックスを非アクティブに設定することをお勧めします。そうしないと、メールサーバが最初の変更と最後の変更の間に取得するメッセージが、その時に有効になっているルールで処理されます。

メールボックス ルールを作成する方法

1. [管理] タブで [電子メール] - [メールボックス ルール] を選択します。

[メールボックス ルール リスト] ページが表示され、ルールがリスト表示されます。

2. [新規作成] をクリックします。

[メールボックス ルールの詳細] ページが表示されます。

3. 必要に応じて [フィールド](#) (P. 270) にデータを入力します。

4. [保存] をクリックします。

メールボックスルールが作成され、有効になります。

メールボックス ルールのアクション

メールボックスルールを使用すると、以下のうちいずれかの電子メールアクションを実行できます。

- 電子メールを無視 - 電子メールを処理せず、返信もしません。
このアクションは、「退席中」や「メール配信エラー」のようなシステムレベルメッセージに使用すると便利です。
- 電子メールを無視して返信 - 電子メールを処理せず、送信者に返信します。応答成功メッセージを使用して電子メールに返信します。応答失敗メッセージは無視されます。
- オブジェクトの更新 - フィルタ文字列を使用してオブジェクト ID（たとえば電子メール内の %Incident:{{object_id}}%）を判断し、Text API に更新リクエストを送信します。オブジェクト ID が検出されない場合、Text API は動作しません。
このアクションは、通常、オブジェクト ID が埋め込まれている電子メールの返信を処理します。オブジェクト ID が存在しない場合、通常、障害応答メッセージが送信されます。
- オブジェクトの作成/更新 - フィルタ文字列を使用してオブジェクト ID（たとえば電子メール内の %Incident:{{object_id}}%）を判断し、Text API に更新リクエストを送信します。オブジェクト ID が検出されると、Text API はチケットを更新します。オブジェクト ID が検出されない場合、Text API はチケットを作成します。
このアクションは、電子メールに含まれる Text API キーワードの有無にかかわらず、メールデーモン（Mail Eater）の標準的な動作です。

注: メールボックスルールの設定に関する詳細については、オンラインヘルプを参照してください。

メールボックスルールのパターン マッチング

メールボックスルールは、パターンマッチングに正規表現を使用します。メールボックスルールで正規表現に適用される以下の空白文字を考慮します。

¥t

水平タブを指定します。

¥r

キャリッジリターン文字を指定します。

¥n

ラインフィードまたは改行文字を指定します。

テキストの改行を表す文字は、オペレーティングシステム、メールサーバおよびメールクライアントによって異なる場合があります。例：

- UNIX では `¥n` を使用します。
- Microsoft では `¥r¥n` を使用します。
- マッキントッシュでは `¥r` を使用します。
- Mac OS X では `¥n` を使用します。

ある特定の状況では、CA SDM のメール処理の要素は、これらの改行文字の 1 つを別の文字と交換または置換して、メッセージのテキストや添付パラメータのように、異なるテキスト要素の相違を確立または保持します。その結果、行またはパラグラフの区切りを使用する場合は、フィルタを構築して `¥r` または `¥n` のいずれか検索された方に一致できるようにします。2 つのキーワードの間に改行を指定する場合は、フィルタを構築して 1 つ以上の `¥r` および `¥n` 文字のシーケンスが一致できるようにします。

メッセージを送信するメールクライアントによる行の折り返しが原因で、テキストの真中に不必要な改行が表示される場合があります。これは、フィルタ文字列がメッセージの本文を検索する場合、フィルタ文字列に一致するはずですが、スペースはキャリッジリターン、ラインフィードまたはそれら両方に変更することができます。あるいは、キャリッジリターン、ラインフィードまたはそれら両方はスペースの後に挿入できます。メッセージが HTML で構成されていて、箇条書きリストか番号付きリストまたはインデントされたパラグラフが含まれている場合、タブはメールクライアントがメッセージを変換して送信した後で表示することもできます。フィルタ文字列の真中にスペースを含める場合は、さまざまなサイズの任意のスペースを表す正規表現のブロックを使用します。このブロックは、`[¥t¥r¥n]+`（左角かっこ、スペース、バックスラッシュ、`t`、バックスラッシュ、`r`、バックスラッシュ、`n`、右角かっこ、プラス記号）で、1 つ以上のスペース、タブ、キャリッジリターンおよびラインフィードの任意のシーケンスを表します。

例: `[¥t¥r¥n]` を使用してキーワードと正確に一致させる

この例では、キーワード「request」と一致させ、かつ以下の単語のような他の可能なキーワードと一致させないために、どのように空白文字を使用すればよいのかを説明します。

```
requester
requesting
requested
orequestra
```

キーワードの **request** のみと一致させるには、キーワードの **request** の前後に 1 つ以上の空白文字を以下のように置きます。

```
[ ¥t¥r¥n]request[ ¥t¥r¥n]
```

Mail Eater は、**request** という単語または文の一部としての単語のみに一致させますが、**requester** など、別の単語の一部に一致させることはありません。

フィルタ文字列オブジェクト ID の制限

制限は、電子メールの中でオブジェクト識別子（たとえば **%Incident : {{object_id}}%**）を決定するメールボックスルールフィルタ文字列に適用されます。オブジェクト識別子（**{{object_id}}**）を囲むテキストはコンテンツと長さの両方において明白である必要があります。テキストは、テキスト間にあるチケット ID アーチファクト値の始まりおよび終わりを明確に定義する必要があります。

以下の制限は、**Mail Eater** がチケット ID アーチファクト値の開始をどのように解釈するかに適用されます。

- **{{object_id}}** プレースホルダはフィルタ文字列の最初の要素にすることはできません。少なくとも 1 文字は必要です。また、通常、特殊なキーワード、または文字、数および記号のシーケンスは、オブジェクト ID キーワードに先行する必要があります。
- **{{object_id}}** プレースホルダの直前の文字は、チケット ID アーチファクト値の一部になりえる、反復可能かオプションの文字（意味（プラス記号（+）、アスタリスク（*）または疑問符（?）が続く文字））にすることはできません。反復可能かオプションの文字は、それらが空白文字である場合を除いて、チケット ID アーチファクト値の開始がいまいになるという危険があります。空白文字（スペース、タブ、キャリッジリターン、ラインフィード）はチケット ID アーチファクト値の一部であってはなりません。
- **{{object_id}}** プレースホルダの直前の文字は、チケット ID アーチファクト値の一部になりえる文字が含まれる、反復可能かオプションのかっこでくくった一連の文字にすることはできません。

以下の制限は、Mail Eater がチケット ID アーチファクト値の長さをどのように解釈するかに適用されます。

- `{{object_id}}` プレースホルダはフィルタ文字列の最後の要素にすることはできません。1 つ以上の文字を `{{object_id}}` プレースホルダの後に含める必要があります。
- `{{object_id}}` プレースホルダの直後の文字は、チケット ID アーチファクト値の一部になりえる、反復可能かオプションの文字（意味（プラス記号（+））、アスタリスク（*）または疑問符（?）が続く文字）にすることはできません。反復可能かオプションの文字は、それらが空白文字である場合を除いて、チケット ID アーチファクト値の最後がいまいになるという危険があります。空白文字（スペース、タブ、キャリッジリターン、ラインフィード）はチケット ID アーチファクト値の一部であってはなりません。
- `{{object_id}}` プレースホルダの後の最初の文字は、チケット ID アーチファクト値の一部になりえる文字にすることはできません。
- `{{object_id}}` プレースホルダの直前および直後に以下の文字は使用しないでください。
 - すべて大文字またはすべて小文字
 - 数字
 - プラス記号（+）
 - スラッシュ（/）
 - カンマ（,）
 - ピリオド（.）。これは、改行を除くすべての文字を表すことができるため、このリストにあるすべての文字になりえるからです。

これらのいずれの文字もチケット ID アーチファクト値に含めることができます。かっこでくくったセット（フィルタ チェックでいずれの文字にも一致する、かっこ間の複数の文字）を `{{object_id}}` プレースホルダの前か後に置く場合は、かっこでくくったセットにこれらのいずれの文字も含めることはできません。

正規表現の特殊文字

メールボックス ルールのフィルタのパターン マッチングは、C スタイルの特殊文字を使用する ASCII 正規表現のルールに従います。

重要: 正規表現で特殊文字を使用する場合は、ユーザが **Regex** 構文に精通していることをお勧めします。

たとえば、メールボックス ルールの正規表現に適用する **Regex** パターンについては、以下の特殊文字を考慮します。

¥t

水平タブを指定します。メールボックス ルールのフィルタ文字列では、**¥t** は、テキスト（またタブ）の先頭および終わりと一致し、**Mail Eater** に特有です。

¥r

キャリッジリターン（現在行の先頭に戻る）を指定します。

注: メッセージの件名または送信者アドレスの検索に **¥r** は使用しないでください。

¥n

改行（ラインフィードとキャリッジリターンの組み合わせ）を指定します。

注: メッセージの件名または送信者アドレスの検索に **¥n** は使用しないでください。

¥t、**¥r** および **¥n** は、メールボックス ルールの正規表現で最もよく出現する特殊文字です。

例: ¥t、¥r および ¥n の使用

[¥t]request[¥t]

単語 **request** のテキストを検索します。角かっこはセットからの任意の 1 文字に一致し、これにはスペースも含まれます。したがって、**[¥t]** はスペースまたはタブと一致します。

[¥r¥n]+critical[¥t¥r¥n]

単語 **critical** のテキストを行の先頭、メッセージの先頭、または行の全コンテンツで検索します。角かっこはセットの任意の 1 文字に一致し、+（プラス記号）は 1 つ以上の前の文字に一致します。したがって、**[¥r¥n]+** は 1 つ以上のキャリッジリターンおよび改行に一致します。

メールボックス ルール内の通知フレーズのサンプル テキスト

この例は、メールボックス ルールに通知フレーズを含める場合に使用できるサンプル テキストを表示します。フレーズに改行または他のフォーマットが含まれている場合は、プレーン テキストおよび HTML に通知フレーズの別のバージョンを定義します。

[メールボックス ルールの更新] ページの [応答成功] タブで、[成功 テキスト]、[成功 HTML] または両方のフィールドに以下のテキストを使用します。

■ 成功テキスト

Thank you for submitting your request.
@{notification_phrase[IncidentURL1].phrase}

■ 成功 HTML

リクエストをサブミットしていただきありがとうございます。</p>
@{notification_phrase[IncidentURL1H].phrase}</p>

注: [管理] タブ、[通知]、[通知フレーズ] で定義されている通知フレーズの詳細については、オンライン ヘルプを参照してください。

関連項目:

[通知コードおよび通知フレーズ](#) (P. 252)

[通知フレーズの構文](#) (P. 254)

アーチファクトの使用上の考慮事項

電子メール アーチファクトとは、転送された電子メールに含まれている電子メール アドレスなど、メール プロセスから発生するものを指します。テキスト API は、応答サポートのチケット ID (参照番号など) が含まれているアーチファクトを使用します。チケット ID が見つかったら、既存のテキスト API キーワード (%INCIDENT_ID など) がテキスト API の入力に設定されて追加されます。Mail Eater は、メッセージ内でアーチファクトを見つけることにより、応答が特定のチケットに関連付けられているか識別します。

メールボックス ルールでは、テキスト API が使用するアーチファクトおよび値を指定することができます。たとえば、インシデントのルールを `Incident:{{object_id}}%` として定義できます。ルールが `Incident:1234` を見つけると、テキスト API は `%INCIDENT_ID=1234` (1234 はインシデントの `ref_num` です) を使用します。アーチファクトは電子メール内で一意であり、容易に検索される必要があるため、アーチファクトを `%Incident:{{object_id}}%` のように、より際立たせることができます。パーセント記号 (%)、空白、またはアーチファクト値に表示できないその他の文字は、`{{object_id}}` の後ろに置く必要があります。大文字および小文字、数字、右上がりスラッシュ、カンマ、およびプラス記号は、潜在的に値の一部です。セキュアなアーチファクトは、暗号化の後に Base64 エンコードされたものです。セキュアなアーチファクトを使用しない場合は、アーチファクトに続く文字をチケット ID サフィックス (ある場合は、そのチケットのタイプに設定されている) に含めることはできません。

メールボックス ルールのフィルタ文字列を使用してチケット ID アーチファクトを識別する場合は、キーワード `{{object_id}}` は、フィルタ文字列内の予想されるチケット ID アーチファクトの位置を示します。メールボックスルールが大文字と小文字を区別しないとしても、このキーワードは大文字と小文字を区別します。

例: 電子メール アーチファクトの使用

以下の例では、変更リクエスト チケットに対してメールボックス ルールで使用するアーチファクトのフォーマットを示します。

使用法: `%REQUEST=@{call_req_id.ref_num}%`

例: `%REQUEST=1234%`

メールボックス ルールのフィルタ文字列を作成する場合は、以下の条件を考慮します。

- 明確な境界は、チケット ID アーチファクトと、その前後に続くキーワードとの間に存在する必要があります。この境界テキストに空白テキストを含めることを強くお勧めします。

- チケット ID アーチファクトの開始に一致する可能性のある、繰り返し可能または省略可能なパターンの `{{object_id}}` キーワードに先行するフィルタ文字列の部分では終了しないでください。また、長さがあいまいなパターンでは終了しないでください。たとえば、フィルタ文字列には `request(er|ed|ing)?{{object_id}}` を含めることはできません。というのも、この構築は、末尾の `er`、`ed`、または `ing` が、先頭のテキストの最後であるか、または保護されていないチケット ID のプレフィックスの一部であるか、のあいまいさの原因になるためです。
- `{{object_id}}` キーワードに続くフィルタ文字列の部分は、チケット ID アーチファクトの最後に一致する場合がある繰り返し可能または省略可能なパターンで開始したり、長さがあいまいなパターンで開始することはできません。また、少なくとも 1 つの空白の要素を含んでいる必要があります。以下に例を示します。
 - フィルタ文字列は `{{object_id}}[A-Z]?` を含めることはできません。というのも、`[A-Z]?` はチケット ID アーチファクトの最後の文字と一致する場合があるためです。
 - フィルタ文字列は `{{object_id}}Item` で終了することはできません。というのも、アイテムが、プレーンテキストまたは保護されているアーチファクトのチケット ID のサフィックス、または安全なアーチファクト内の文字としてチケット ID アーチファクトに表示される可能性があるためです。
 - `{{object_id}}Item` は使用できます。というのも、スペースはチケット ID アーチファクトの一部にすることができないこと、そして保護されているかプレーンのチケット ID アーチファクトの一部ではないためです。ただし、`[ ¥t¥r¥n]+` は `{{object_id}}` の後に改行を挿入するメールプログラムを補うため、`{{object_id}}[ ¥t¥r¥n]+Item` (左角かっこ、スペース、バックスラッシュ、`t`、バックスラッシュ、`r`、バックスラッシュ、`n`、右角かっこ、プラス記号、`+Item`) の方が優れています。

- 別のメールボックス ルールのフィルタ文字列を作成する場合は、別のメールボックス ルールのフィルタ文字列が完全に含まれている、あるいは、`{{object_id}}` キーワードの前または後の部分に、別のメールボックス ルール フィルタ文字列のその部分が完全に含まれているフィルタ文字列を使用しないようにします。これらのフィルタが検査される順序によっては、1つのフィルタを対象としたメッセージ一致は、2つのフィルタ文字列を区別する追加のテキストに一致するチケット ID アーチファクトの一部を使用する別のフィルタにも一致する場合があります。

管理ガイド- すべての受信メッセージに一致するメールボックス ルールの作成方法

この新規トピックは、「管理ガイド」の「ポリシーの実装」の章にある「電子メールの管理」-「メールボックス ルール」セクションに関するものです。

ほかのメールボックス ルールではフィルタされないすべての受信メッセージに一致するメールボックス ルールを作成できます。

このタイプのルールを作成するには、フィルタを「件名の内容」に、フィルタ文字列をピリオドとアスタリスク 1 つずつ（「.*」）に設定します。

- ピリオドは、改行を除く文字に一致します。
- アスタリスクは、直前の記号が 0 個以上出現するパターンに一致します。

結果として、この組み合わせは、改行以外の 0 個以上の文字に一致します。

例:「すべてに一致」メールボックス ルール

この例では、「.*」の組み合わせを使用して、すべての受信メッセージに一致する方法を示します。

```
Filter = "件名の内容"  
Filter String = ".*"
```

メールボックス ルールの[TextAPI デフォルト]と[TextAPI 受信を無視]設定の使用方法

〔TextAPI デフォルト〕 および 〔TextAPI 受信を無視〕 フィールドを使用して、受信メールボックス ルールのデフォルト値を指定したり、受信電子メールで受け入れない TextAPI コマンドを指定したりできます。これらのフィールドは、〔EMAIL_DEFAULTS〕 セクションで設定されているデフォルト値や、text_api.cfg ファイルの〔EMAIL_IGNORE_INCOMING〕 セクション内にある禁止コマンドリストと連携します。メールボックス ルールの定義と text_api.cfg ファイルの定義との間に競合が生じた場合は、メールボックス ルールに設定された値が適用されます。

〔TextAPI デフォルト〕 フィールドには、メールボックス ルールに一致した電子メールからのチケットに適用される TextAPI キーワード コマンドを入力します。メッセージが既存のチケットに影響を与える場合、コマンドは適用されません。

TextAPI デフォルト コマンドを指定するには、以下の手順に従います。

1. 〔TextAPI デフォルト〕 フィールドに、各行に 1 つずつコマンドを入力します。
2. コマンドの形式は以下のとおりです。

OBJECT.FIELD=value

注: 先頭のパーセンテージ記号 (%) は含めないでください。これは、同コマンドが電子メールの本文に埋め込まれている場合にのみ必要なものです。

コマンドの形式の例は、以下のとおりです。

REQUEST.PRIORITY=3
PROBLEM.CATEGORY=Facilities
INCIDENT.GROUP=Plumbing

「TextAPI 受信を無視」フィールドには、受信電子メールメッセージ内での使用を許可しない TextAPI キーワード コマンドをリスト表示します。このフィールドに記載されたコマンドが、受信電子メールメッセージ内にある場合、すべて無視されます。

「TextAPI 受信を無視」コマンドを指定するには、以下の手順に従います。

1. 「TextAPI 受信を無視」フィールドに、各行に 1 つずつコマンドを入力します。
2. コマンドの形式は以下のとおりです。

OBJECT.FIELD

注: 先頭のパーセンテージ記号 (%) は含めないでください。これは、同コマンドが電子メールの本文に埋め込まれている場合にのみ必要なものです。

コマンドの形式の例は、以下のとおりです。

CHANGE.ASSIGNEE

PROBLEM.GROUP

REQUEST.EFFORT

3. text_api.cfg ファイルの [KEYWORDS] セクションに、いずれかのフィールドに使用されるすべてのコマンドを定義します。このファイルは、CA SDM インストールディレクトリの「site」サブディレクトリに保存されます。

電子メール応答を設定する方法

メールボックスで使用する電子メール通知は、電子メールに応じて連絡先に送信される応答に固有のものです。たとえば、連絡先が電子メール通知内の応答リンクをクリックすると、応答メールがメールボックスに送信されるように、電子メールを設定できます。

注: この設定は標準の電子メール通知とは異なります。

次の手順に従ってください:

1. [CA SDM Web UI を開きます](#) (P. 222)。
2. [受信電子メール用のメールボックスを設定](#) (P. 247) していることを確認します。
3. [メール サーバを設定します](#) (P. 287)。
4. (オプション) 連絡先定義に通知電子メール アドレスを指定します。
注: [管理] タブで、[セキュリティと役割の管理] - [連絡先] を選択し、編集する連絡先を選択します。
5. [電子メール通知方法を変更します](#) (P. 289)。

CA SDM Web UI の表示

CA SDM の設定に応じて、以下のサーバから Web UI にログインします。

- 標準: プライマリまたはセカンダリ サーバ
- 高可用性: アプリケーション サーバまたはバックグラウンド サーバ

メール サーバの設定

イベントの通知 (自動および手動通知) は単一のメール サーバ定義を使用して送信されます。

次の手順に従ってください:

1. [管理] タブで [オプション マネージャ] - [電子メール] を選択します。
[オプション リスト] ページが開きます。
2. インストールする [電子メールのオプション](#) (P. 288) をクリックします。
[オプションの詳細] ページが表示されます。

3. [編集] をクリックし、フィールドを必要に応じて指定し、[インストール] をクリックします。
メール サーバは通知（送信メール）を送信するように設定されます。
4. 関連する [オプション リスト] オプションがすべて設定されるまで、手順を繰り返します。

電子メール オプション

電子メール インターフェースでは、電子メール通知を送信します。ユーザは、電子メールを使用してチケットを作成できます。

mail_from_address

電子メール通知の送信者アドレスを指定します。アドレスのフォーマットは、「表示名<user@company.com>」です。

mail_login_password

SMTP サーバのログインパスワードを指定します。

mail_login_userid

SMTP サーバのログインユーザ ID を指定します。

mail_max_threads

SMTP サーバとの通信を同時に試みることができる最大接続数を指定します。

mail_reply_to_address

電子メール通知の返信先アドレスを定義します。このオプションは、電子メールの返信先が送信元と一致しない場合に役立ちます。デフォルト値は、送信者アドレスと同じです。

mail_smtp_domain_name

SMTP サーバのドメイン名を定義します。値を **NONE** に設定すると、ドメイン名を削除できます。

mail_smtp_hosts

電子メール通知の SMTP サーバホスト名を、スペース区切りのリストで指定します。

mail_smtp_host_port

デフォルトの SMTP ポートを上書きするために SMTP ポートを指定します。

mail_smtp_security_level

SMTP セキュリティ レベルを指定します。次の値を指定できます。0 = セキュリティなし、1 = 基本的な認証、2 = NTLM、3 = MD5、4 = ログイン。このオプションを 1 に設定した場合は、mail_login_password と mail_login_userid オプションを設定してください。ほとんどの SMTP サーバでは、認証は必要ありません。

mail_smtp_use_tls

電子メールでトランスポート レイヤ セキュリティ (TLS) の使用法を指定します。有効な設定は Yes (TLS を使用)、および No (TLS を使用しない) です。

mail_ca_cert_path

信頼できる証明書が展開されているパスを指定します。

注: 高可用性設定では、すべての CA SDM サーバの同じ場所に信頼された証明書を展開する必要があります。CA SDM は、CA 証明書の Base 64 エンコード (PEM) 形式をサポートします。

電子メール通知方法の変更

電子メール応答を設定する電子メール通知方法を変更します。

次の手順に従ってください:

1. [管理] タブで [通知] - [通知方法] - [電子メール] を選択し、[編集] をクリックします。
2. [電子メール通知方法の更新] ページで [SMTP サポート] チェックボックスをオンにし、SMTP を有効にします。
3. [通知方法] として **pdm_mail [- F from_email_address] [- T reply_to_email_address]** を入力します。

from_email_address

メッセージの送信元アドレスとして使用されるアドレスを指定します。このアドレスは、送信メール サーバに設定されている送信者アドレスを上書きします。

reply_to_email_address

応答を送信するアドレスを指定します。このアドレスは、送信メールサーバに設定されている返信先アドレスを上書きします。

返信先アドレスが送信メールサーバの構成に設定されていて、返信先アドレスが通知方法に指定されていない場合は、送信メールサーバの構成の返信先アドレスは通知方法と共に使用されます。

注: キーワード「\$(REPLY_FROM)」がいずれかのアドレスとして指定されている場合、そのアドレスはメールボックスのユーザ名およびメールサーバホスト名から構成されます。このキーワードはメールボックスルールが通知方法を使用する場合にのみ有効です。それを使用する通知方法は他の目的に使用することはできません。たとえば、ユーザ名 =dev、サーバ名 =mail32.ca.com、

\$(REPLY_FROM)=dev@mail32.ca.com となります。このキーワードは、メールサーバが電子メールドメイン名と同じメールサーバ名を受け入れるように設定されている場合にのみ使用します。このキーワードは注意して使用してください。ホスト名がメールボックス構成で完全にドメイン拡張されていない（たとえば mailserver1.customer7.com の代わりに mailserver1）場合は、フィールドインタープリタによって自動的に拡張されません。

注: from_email_address と reply_to_email_address は、ユーザがメッセージを読むと、メッセージの [送信元] および [返信先] ヘッダに表示されるアドレスです。アドレスが同一の場合は、from_address のみを指定できます。

4. [保存] をクリックします。

電子メール通知方法が変更されます。連絡先が電子メール通知に応答すると、応答はデフォルトでは指定されたメールボックスにアドレス指定されます。

関連項目:

[pdm_mail ユーティリティ -- 電子メール情報の送信](#) (P. 1352)

代替送信者アドレスによる識別

最初にメッセージを送信した電子メールアドレスとは別の電子メールアドレスを使用する送信者を **CA SDM** が識別できるように、メッセージの件名に **-m** パラメータを使用することができます。スペースおよび **CA SDM** が認識する電子メールアドレスが後ろに続く **-m** キーワードは、件名行の最後の要素である必要があります。件名に **-m** パラメータを使用する場合は、以下の情報を考慮します。

- 実際の送信元アドレス、および **-m** で指定される代替アドレスはどちらも包含リストおよび除外リストで検証されます。
- 代替アドレスとして指定される電子メールアドレスには、表示名ではなくアドレスのみが含まれている必要があります。
- 件名行で複数の単語が **-m** パラメータに続く場合、代替アドレスは認識されません。

メールボックス ポーリング

エラーが送信メール サーバ上で発生した場合は、電子メール通知は送信されず、**%NX_ROOT%¥site¥mail_queue** ディレクトリのキューに入れられます。メールサーバが再度アクティブになると、一定の間隔の後で、電子メールを処理して送信します。メールサーバがビジーだったときにキューに入れられた電子メールをリサイクルする間隔を変更することができます。

ユーザが以下のいずれかを実行するまで、送信メールサーバは、送信に失敗した通知電子メール メッセージを再サブミットします。

- 送信メール通知を処理するメール デモン (**pdm_mail_nxd**) を停止します。
- 手動で、メッセージを **%NX_ROOT%¥site¥mail_queue** ディレクトリから削除します。

電子メール再試行間隔の変数を設定する

メールサーバへの電子メールの送信失敗を再試行する時間間隔（秒）を定義できます。

注: **CA SDM** では、送信メールサーバが受信したのに配信できなかったメッセージは、送信を再試行しません。これらのメッセージについては、送信メールサーバの再試行機能およびポリシーがある場合は有効です。

再試行はメッセージ単位で行われます。メールサーバが一定の期間使用できない場合、すべてのメッセージが一度に送信されるのではなく、メッセージのそれぞれのタイマが期限切れになったときに再試行されます。ただし、送信メールデーモンを再起動した場合、すべての未送信メッセージはその時間に送信されるように試行します。また、それらがすべて送信に失敗した場合、それらの再試行タイマはすべて同時にリセットされます。

NX.env ファイルの設定 (**NX_EMAIL_RETRY_INTERVAL**) は再試行間隔を制御します。1つ以上のサーバでデフォルトの再試行間隔の設定を変更できます。

次の手順に従ってください:

1. **CA SDM** の設定に応じて、以下のサーバにログインします。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンドサーバ。
2. **\$NX_ROOT** ディレクトリに移動します。
3. テキストエディタ (ワードパッドなど) を使用して **NX.env** ファイルを開きます。
4. **NX_EMAIL_RETRY_INTERVAL** 間隔の値を、以下のように変更します。

```
NX_EMAIL_RETRY_INTERVAL=number_of_seconds
```

```
NX_EMAIL_RETRY_INTERVAL
```

失敗した電子メールの試行を再試行する時間間隔 (秒) を定義します。

number_of_seconds

各電子メールの再試行間隔の秒数を指定します。デフォルトは 600 秒 (10 分) です。使用できる最小値は 20 秒です。最小値の 20 秒未満の値または 2000000 秒を超える値を設定した場合は、デフォルト値の 10 分が使用されます。

5. ファイルを保存して閉じます。
6. **CA SDM** サーバを再起動します。**CA SDM** サーバを起動する方法の詳細については、**CA SDM** の設定に応じて、**CA SDM** サーバの再起動シナリオを参照するか、または「**管理ガイド**」で情報を検索してください。
変更は有効になっています。

サービスレベルアグリーメント

サービスレベルアグリーメント（SLA）またはサービスタイプは、サービスデスクとカスタマの間の契約であり、通常はサービスデスクが提供するサービスのレベルを表します。このレベルのサービスが提供されない場合、サービスデスクにはペナルティが課せられます。たとえば、サービスデスクが「サービス単位の支払い」条件で契約を結んでいる場合、サービスレベルを満たせなかったサービスに対しては完全な支払いを受けられません。したがって、ほとんどのサービスデスクではサービスレベルアグリーメントを非常に重要と考えており、これらの契約に規定されたサービスタイプを提供できるように最善の努力を払っています。

さらに、ほとんどのサービスデスクでは、サービスレベルアグリーメントの達成または違反に関して、詳細な記録を残しています。CA SDM で定義されたサービスタイプは、サービスデスクの担当者がサービスレベルアグリーメントを達成し、サービスレベルアグリーメントの達成確認に必要なレコードを記録できるように設計されています。

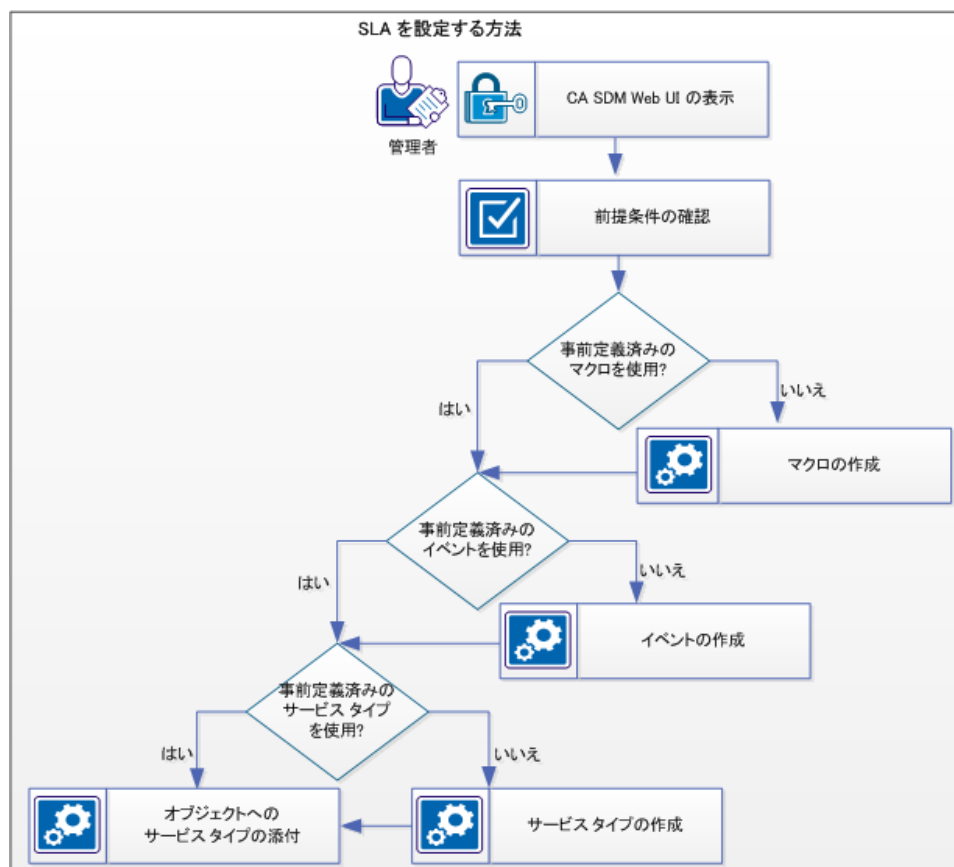
SLA を設定する方法

CA SDM では、SLA またはサービス タイプは、サービス デスク アナリストが顧客に提供するサービスのレベルを表します。エンタープライズのコミットメントおよびスケジュール（特定のチケットに関連付けられている）を追跡するため、イベントがサービス タイプに添付されています。イベントは、サービス タイプの違反が発生し、その後に実行されるアクションの条件を定義するために使用されます。イベントにはそれぞれ、条件、true 時のアクション、false 時のアクションという 3 つの一般的な動作特性があります。

- 条件は、チケットの測定可能な状態を識別します。
- アクションには、一定時間が経過した後で条件が true または false であった場合に自動的に実行されるプロセスを指定します。

例: システム管理者は、ハードウェアリクエスト用の 24 時間の SLA をセットアップしたい場合があります。それに失敗すると、カスタマ サポート マネージャとアナリストに電子メール通知が送信されます。この例は、SLA に対して電子メール通知を設定する方法を説明するために、シナリオ全体にわたって使用されます。

以下の図は、24 時間の設定を行う方法を示しています。違反時に電子メール通知を送信する SLA :



次の手順に従ってください:

1. [CA SDM Web UI を開きます](#) (P. 222)。
2. [前提条件を確認します](#) (P. 296)。
3. 事前定義済みのマクロを使用しない場合、[マクロを作成します](#) (P. 304)。
4. 事前定義済みのイベントを使用しない場合、[イベントを作成します](#) (P. 306)。
5. 事前定義済みのサービス タイプを使用しない場合、[サービス タイプを作成します](#) (P. 310)。
6. [オブジェクトにサービス タイプを添付します](#) (P. 312)。

CA SDM Web UI の表示

CA SDM の設定に応じて、以下のサーバから Web UI にログインします。

- 標準：プライマリまたはセカンダリ サーバ
- 高可用性：アプリケーション サーバまたはバックグラウンドサーバ

前提条件を確認します。

サービス レベル アグリーメントを設定する前に、以下の手順を完了したことを確認します。

- 組織の要件に必須の [SLA オプション](#) (P. 296) をインストールしている。
- [受信者用の通知方法を確認している。](#) (P. 223)
- SLA 違反に対する電子メール通知を送信する場合、および事前定義済みのメッセージを使用しない場合、[メッセージテンプレートが作成されている](#) (P. 225)。

SLA オプション

組織の要件に応じて、SLA のセットアップに必須の SLA オプションをインストールします。

たとえば、「古い」SLA 処理 (オプション マネージャに `classic_sla_processing` オプションがインストールされていると有効になります) では、チケットに適用できるサービス タイプが常に 1 つに限られます。チケットの属性ごとに異なるサービス タイプが関連付けられている場合、ランクの高いサービス タイプが使用されます。サービス タイプのランクはサービス タイプの作成時に定義され、最高ランクが 1、次位が 2 というようになります。たとえば、案件のサービス タイプが「解決 (12 時間)」 (ランク 2) であり、その同じ案件に優先度コード 1 が割り当てられているとします。優先度コード 1 のサービス タイプは「解決 (04 時間)」 (ランク 1) です。ランクの高い方のサービス タイプによって、関連付けられた案件のサービス動作が決まります。この例では、解決策 (4 時間) が解決策 (12 時間) よりもランクが高いため、解決策 (4 時間) のサービス タイプが案件に適用されます。 -

以下のオプションは、オプション マネージャからインストールできます。

注: オプションのインストールまたはアンインストールの詳細については、[オンラインヘルプ](#)を参照してください。

オプション	説明

change_allow_sla_downgrade	システムが変更要求のサービス タイプを自動的にダウングレードできるようにすることによって、chg_sla オプションの動作を変更します。 chg_sla オプションでは、複数の変更要求属性から最適なサービス タイプが選択されますが、変更要求の現在のサービス タイプをより低いランクのサービス タイプと置き換えることはできません。このオプションをインストールすると、属性のいずれかが変更されるたびに、影響を受けるすべての属性のサービス タイプが評価されます。新しいサービス タイプのランクが、現在の変更要求のサービス タイプのランクより低い場合でも、変更要求のサービス タイプは、見つかったタイプの中で最も高いランクに設定されます。 ランクの値が最も低いサービス タイプが、最も良いサービスとみなされます。評価されたサービス タイプのランクがすべて同じ（ランクの値が空のサービス タイプも含む）場合は、データベース内で最初に作成されたサービス タイプが選択されます。 このオプションが正常に機能するようにするには、chg_sla オプションをインストールする必要があります。 案件用およびリクエスト用の同様のオプションをインストールできます。
ttv_enabled	違反までの時間デーモンを実行します。このデーモンは、オープンされているすべてのチケットとタスクの SLA を監視します。このプロセスでは、SLA 違反がセットされませんが、チケットまたはタスクが現在のステータスで違反になる日付が記録されます。チケットまたはタスクが更新されるとこの時間も更新されます。違反までの時間の他のオプションを正常に機能させるには、このオプションをインストールする必要があります。 重要: このオプションでは、classic_sla_processing オプションをインストールする必要はありません。
set_sla_evt_open_date	変更要求、案件、またはリクエストを開いた日付/時刻の値を、アタッチされたイベントの開始日付/時刻として使用します。アタッチされたイベントは、チケットが保存されるとただちにトリガされます。

受信者用の通知方法の確認

通知を送信する連絡先が、その特定の通知方法に割り当てられていることを確認します。

次の手順に従ってください:

1. 「管理」タブで、「セキュリティと役割の管理」 - 「連絡先」を選択します。

「連絡先の検索」ページが開きます。

2. フィルタを使用して連絡先を検索し、検索結果から通知する連絡先を選択します。

「連絡先の詳細」ページが開きます。

3. 「連絡先詳細」タブの「通知」を選択します。

4. 通知方法を確認します。通知の優先度に基づいて、必要なオプションを選択します。たとえば、任意の緊急の通知に関して電子メール通知を送信するとします。「緊急」フィールドで「電子メール」オプションを選択します。

5. 通知方法を変更するには、「編集」をクリックし、オプションを変更して、「保存」をクリックします。

連絡先の通知方法が確認されます。

メッセージ テンプレートの作成

通知メッセージ用に使用する値が含まれるメッセージテンプレートを作成します。複数の通知メッセージを送信する場合、メッセージテンプレートを使用して、作業負荷を軽減できます。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで [通知] - [メッセージテンプレート] を選択します。
[メッセージテンプレート リスト] ページが開きます。
2. [新規作成] をクリックします。
[メッセージテンプレートの新規作成] ページが開きます。
3. 必要に応じてフィールドにデータを入力します。

シンボル

このメッセージテンプレートの一意の識別子を定義します。

オブジェクトタイプ

このテンプレートに関連付けられたオブジェクトタイプを指定します。たとえば、チケットに関連する任意の通知に対するリクエスト/インシデント/問題を選択します。

レコードステータス

テンプレートのステータスをアクティブまたは非アクティブに指定します。メッセージテンプレートを使用するために、ステータスを [アクティブ] に設定します。

自動通知

アクティビティが発生すると、このテンプレートに関連付けられた通知を自動的に送信するよう指定します。たとえば、初期通知を設定し、通知するオブジェクトを設定し、メッセージテンプレートを設定したのに、通知をオンにする準備ができていないとします。この場合、[自動通知] を選択しません。自動通知を開始する準備ができていない場合、このチェックボックスをオンにします。通知がアクティブになり、設定したとおりに実行されます。

通知レベル

この通知の送信の相対的な重要性を示します。たとえば、関連するアクティビティが発生した場合、連絡先に電子メール通知をすぐに送信する場合は、[緊急]を選択します。

通知メッセージタイトル

メッセージの概要タイトルを指定します。変数を使用して、メッセージタイトルにインシデント番号を挿入できます。たとえば、`@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}` のように指定します。

通知メッセージ本文

メッセージの内容を指定します。変数を使用して、メッセージにアナリスト名、エンドユーザ名、および説明を挿入できます。例：

@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}。

担当者： @{call_req_id.assignee.combo_name}

顧客： @{call_req_id.customer.combo_name}

説明： @{call_req_id.description}

表示するには次の URL をクリックします。

@{call_req_id.web_url}

キーワード **ARTIFACT** を使用して、アーチファクトが送信メッセージ、メッセージテンプレート、通知、および自動応答で処理される方法を指定することができます。キーワード **ARTIFACT** は、以下の値を使用します。

- **なし** - アーチファクトの検証を指定しません。この値は、キーワードを使用しないと同じです。
- **保護済み** - 確認用のハッシュに対してチケットを検証します。確認に失敗した場合、アーチファクトは無効であると見なされ、アーチファクト ({{object_id}}) をフィルタリング検索した場合、フィルタリングは失敗します。
- **セキュア** - チケット番号の暗号化を解除します。値が有効なパスワードでない場合、アーチファクトは無効であると見なされ、フィルタリングがアーチファクト ({{object_id}}) を検索する場合、フィルタリングは失敗します。

HTML メッセージ

受信者に表示される **HTML** メッセージを指定します。受信者が携帯電話や **PDA** などの外部デバイスでメッセージを受信する場合、メッセージはプレーンテキストのみで表示されます。[**HTML** メッセージの編集] をクリックして **HTML** エディタを開きます。

クイック表示

受信者に表示される形式でメッセージが表示されます。

HTML ソース

HTML ソース コードにメッセージが表示されます。

4. [保存] をクリックします。

メッセージテンプレートが作成されます。

電子メール通知マクロの作成

マクロを作成し、そのマクロを使用してオブジェクトにアクションを追加したり、特定の特性や条件を検索したりできます。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで、[イベントとマクロ] - [マクロ] を選択します。
[マクロ リスト] ページが開きます。
2. [新規作成] をクリックします。
[マクロの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

シンボル

マクロの簡潔な識別子を入力します。

マクロ タイプ

このマクロのタイプを選択します。選択したマクロ タイプによって、指定が必要な残りのデータが制御されます。

注: CA SDM で CA IT PAM ワークフローが設定されている場合、選択できるのは [CA IT PAM アクションの実行] のみです。CA SDM で CA Workflow が設定されている場合、選択できるのは [CA Workflow アクションの実行] のみです。

オブジェクト タイプ

マクロを実行するオブジェクトのタイプを選択します。

4. [続行] をクリックします。

選択したマクロ タイプに基づいて、マクロに必要な残りのデータにも値が入力されます。

注: 例に従って、SLA 違反に対して電子メール通知を送信するマクロタイプとして [複数の通知マクロ \(P. 304\)](#) を選択します。その他のマクロタイプの詳細については、[オンラインヘルプ](#)を参照してください。

複数の通知マクロ

このマクロ タイプを実行すると、1 つ以上の連絡先に通知を送信できます。送信するメッセージ、メッセージの受信者、および緊急度レベルを指定できます。

次の手順に従ってください:

1. [メッセージテンプレート] フィールドにテンプレート名を直接入力するか、または検索アイコンをクリックして目的のテンプレートを選択します。このテンプレートは、通知メッセージの作成に使用されます。
2. [保存] をクリックします。
3. 通知先として適切な連絡先を以下のタブで選択します。

注: 通知先となる連絡先を検索して追加選択するには、各タブに表示される[連絡先の更新] ボタンをクリックします。

オブジェクトの連絡先

チケットに関する通知を受信する、選択されたオブジェクト タイプで使用可能な組織、ベンダー、および構成アイテムを表示します。たとえば、通知する影響を受けるエンドユーザ、または影響を受けるエンドユーザの組織を選択できます。

連絡先

通知マクロに追加された人物が、チケットに対する関連付けによらず、表示されます。

連絡先タイプ

アナリスト、顧客など、通知マクロで同じ分類として定義されたユーザが表示されます。

4. [保存] をクリックします。
複数の通知マクロが作成されます。

イベントの作成

イベントを作成し、このイベントにマクロを添付します。このイベントは、特定の時間が経過した後に実行されます。マクロが添付されている場合、アクションが実行されます。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。

次の手順に従ってください:

1. [管理] タブで、[イベントとマクロ] - [イベント] を選択します。
[イベント リスト] ページが開きます。
2. [新規作成] をクリックします。
[イベントの新規作成] ページが開きます。
3. イベントのフィールドおよび構成情報を入力します。
[保存] をクリックします。
4. このイベントにマクロを追加するには、[アクション情報](#) (P. 308) を入力します。
新しいイベントが保存されます。

関連項目:

[\[イベント\] のフィールド](#) (P. 306)

[\[構成情報\] のフィールド](#) (P. 307)

[アクション情報のフィールド](#) (P. 308)

[イベント]のフィールド

イベントを追加または編集するには、以下のフィールドに入力します。

名前

イベントの名前です。

オブジェクトタイプ

案件、リクエスト、変更要求、ワークフロー タスク、ナレッジ ドキュメント、ナレッジ レポート カード、アシスタンス セッション、または顧客満足度調査（個別）にイベントが添付されているかどうかが表示されます。

このフィールドは、イベントを作成する場合にのみ編集できます。イベントを更新する場合、このフィールドは読み取り専用です。

レコードステータス

イベントがアクティブか、非アクティブかを示します。アクティブなイベントのみ使用できます。

[構成情報]のフィールド

構成情報を追加または編集するには、以下のフィールドに入力します。

遅延時間

イベントがトリガされるまでの時間を指定します。

延期時間の繰り返し

イベントが再度トリガされるまでの時間間隔を指定します。

時間のリセットを許可する

サービス デスク アナリストが[延期時間]を変更できるかどうかを指定します。 イベントをサービス タイプ イベント（解決（4 時間）などのサービス レベルに関連付けられたイベント）として使用する場合は、このオプションをオンにします。

ワークシフト

サービス タイプを有効にする日付、曜日、および時間を指定します。

終了時イベント フラグ

イベントの完了後に実行するアクションを指定します。

イベントの繰り返し

案件がクローズされるまで、指定した間隔でイベントを繰り返します。

履歴の保存

イベントで実行されたアクティビティの履歴を記録します。

履歴なし

イベントの履歴を記録しません。 イベントは[イベント履歴] ウィンドウに表示されません。

条件

イベントによって確認される条件を示すマクロ（イベントに関連付けられている場合）が表示されます。

テキスト

イベント設定を定義します。このフィールドは、一部のアクション マクロでは特定の目的に使用されます。たとえば、「イベントの連絡先に転送」アクションマクロでは、チケットの転送先となる人物のユーザ ID が格納されます。

アクション情報のフィールド

イベントに関連付けるアクションを以下のように選択します。

1. [アクション情報] タブをクリックします。
2. [True/False 時のアクション マクロにサービス レベル アグリーメント違反を設定] チェック ボックスのいずれかまたは両方をオンにします。これらのチェック ボックスをオンにすると、イベントの **True** または **False** 条件が発生したときに、SLA（サービス レベル アグリーメント）違反がログに記録されます。

注: SLA 違反をログに記録するために、アクション リストの **True** または **False** 条件に対して適切なマクロを指定します。

3. [True 時の更新アクション] をクリックします。
[マクロの検索] ページが開きます。
4. イベント条件が **true** の場合に実行されるマクロを検索します。
5. 左側のリストから目的のマクロを選択し、[詳細 (>>)] をクリックします。
選択されたマクロが右側のリストに追加されます。
6. 目的のマクロがすべて右側のリストに追加されたら、[OK] をクリックします。
選択したマクロが [True 時のアクションのマクロ リスト] に表示されます。
7. [False 時の更新アクション] をクリックし、上記の手順を繰り返して、イベント条件が **False** の場合に実行するマクロを選択します。

サービス タイプのカスタマイズ

要件を満たすサービス タイプを作成できます。また、事前定義済みのサービス タイプを変更できます。

次の手順に従ってください:

1. [管理] タブで、[Service Desk] - [サービス タイプ] を選択します。
[サービス タイプ リスト] ページが開きます。
2. [新規作成] をクリックします。
[サービス タイプの新規作成] ページが開きます。
3. マルチテナンシーをインストールしている場合は、ドロップダウン リストから適切なテナントを選択します。パブリック (共有) オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。
4. 必要に応じて、以下のフィールドに入力します。

シンボル

サービス タイプの一意的識別子を定義します。この例では、`24_hr_resolution` としてシンボルを割り当てます。

ランク

サービス タイプのランクを定義します。この例では、ハードウェア リクエスト チケットは複数のサービス タイプと関連付けられる可能性があります。ランク値により、適用可能なサービス タイプが決定します。低いランクのサービス タイプが、最も高い優先度となります。

「1」を入力します。

ワークシフト

サービス タイプを有効にする日付、曜日、および時間を指定します。ワークシフトには以下のルールが適用されます。

- ワークシフトをサービス タイプに適用する場合、それをすぐに反映させるには、該当するワークシフトのサービスを停止して再起動します。
- サービス タイプにワークシフトが指定されており、イベントにワークシフトが指定されていない場合、サービス タイプのワークシフトが有効になります。

- イベントにワークシフトが指定されており、サービス タイプにワークシフトが指定されていない場合、サービス タイプのワークシフトは無視されます。
- イベントにもサービス タイプにもワークシフトが指定されている場合、サービス タイプのワークシフトは無視されます。

タイムゾーン

サービス タイプのタイム ゾーンを指定します。[エンド ユーザのタイムゾーンを使用] オプションがオフの場合は、このタイムゾーンを使用してシステム内のイベントをトリガします。

エンド ユーザのタイムゾーンを使用

イベントをトリガするために、影響を受けるエンド ユーザのタイムゾーンを指定します。

違反コスト

サービス タイプの時間制限に違反した場合に発生するコストを指定します。

5. [保存] をクリックします。

サービス タイプが保存されます。

6. サービス タイプ イベントを添付するには、適切なタブ([リクエスト]、[変更要求]、[変更要求タスク]、[案件]、または[案件タスク])を選択し、[サービス タイプ イベントの追加] をクリックします。

[サービス タイプ イベントの新規作成] ページが開きます。

7. [イベント] をクリックします。

[イベント リスト] ページが開きます。

8. 以下のいずれかの操作を実行します。

- [新規作成] をクリックして、イベントを作成します。イベントのフィールドおよび構成情報を入力します。このイベントにマクロを追加するには、[アクション情報](#) (P. 308)を入力します。
- リストからいずれかの既存のイベントを選択します。イベントを検索するためにフィルタ条件を使用できます。

選択または作成したイベントは、[イベント] フィールドに表示されます。

9. [続行] をクリックします。

サービス タイプの詳細ページが、添付されたイベント付きで表示されます。

オブジェクトへのサービス タイプの添付

サービス タイプは、連絡先、組織、カテゴリ、および優先度コードなどの各種オブジェクトに関連付けることができます。例に従って、[インシデント領域] にサービス タイプを関連付けます。この場合は、[ハードウェア] です。

次の手順に従ってください:

1. SLA を割り当てる関連するチケットを開きます。
2. [インシデント領域] フィールドで [ハードウェア] をクリックします。
[ハードウェア リクエスト/インシデント/問題領域の更新] ページが開きます。
3. [編集] をクリックします。
4. [サービス タイプ] をクリックします。
[サービス タイプ リスト] ページが開きます。
5. 作成した **24_hr_resolution** サービス タイプを検索します。
6. 検索結果から [24_hr_resolution] をクリックします。
[ハードウェア リクエスト/インシデント/問題領域の更新] ページが開き、更新されたサービス タイプが表示されます。
7. [保存] をクリックします。

サービス タイプは、ハードウェア インシデント領域に添付されます。

サービス タイプ イベントの延期または再開

サービス タイプ イベントを延期または再開できます。

イベントを延期する方法

1. [Service Desk] タブのリスト ページから目的のチケットを選択します。
チケットの詳細ページが表示されます。
2. [サービス タイプ] タブを選択します。
チケットに追加されたすべてのサービス タイプ イベントのリストが表示されます。
3. [延期] をクリックします。
[原因] ページが表示されます。
4. イベントの延期の理由を入力し、[OK] をクリックします。
チケット詳細ページには、「延期」としてイベントのステータスが表示されます。

イベントを再開する方法

1. [Service Desk] タブのリスト ページから目的のチケットを選択します。
チケットの詳細ページが表示されます。
2. [サービス タイプ] タブを選択します。
チケットに追加されたすべてのサービス タイプ イベントのリストが表示されます。
3. [再開] をクリックします。
[原因] ページが表示されます。
4. イベントの再開の理由を入力し、[OK] をクリックします。
チケット詳細ページには、「保留中」としてイベントのステータスが表示されます。

サービス ターゲットを作成する方法

サービス レベル アグリーメント違反を最小限にするため、チケット解決方法の各段階を評価するサービス ターゲットテンプレートのセットを作成できます。サービス タイプのように、サービス ターゲットにはそれぞれ、完了時間の条件および予測が含まれます。ただし、サービス ターゲットは作用機序を提供しません。

チケット作成中に、サービス タイプは、チケット解決方法の各段階を追跡する 1 つ以上のサービス ターゲットを割り当てます。チケットが変わるごとに、アクティブなターゲットは条件を評価します。条件に一致する場合、チケットとアクティビティ ログは実際の完了時間を表示します。時間が予測時間を超える場合、チケットはターゲットが間に合わなかった時間の長さを表示します。

サービス ターゲットを使用すると、以下のアクションが可能になります。

- 同じサービス タイプのチケットが、同じサービス ターゲットに付随することを確認します。
- チケットが必要時間フレーム内に閉じられたかどうかをモニタします。
- サービス ターゲットが完了するまでの残り時間（分）などの情報を表示します。

サービス ターゲット テンプレートを作成する場合、以下の点を考慮します。

- サービス ターゲットを満たすために必要な結果を考慮します。チケット データを評価するために、既存の条件、またはサイト定義の条件マクロを使用します。サービス ターゲットを管理するために、必要に応じてマクロをカスタマイズするか、新しいマクロを記述します。
- SLA 許諾契約に基づいて、予測違反および罰則の費用を計算します。
- サービス タイプには少なくとも 1 つのサービス ターゲット テンプレートを割り当てます。

次の手順に従ってください：

1. リクエスト、インシデント、問題、変更要求または案件を管理する[サービス ターゲット テンプレートを作成](#) (P. 315) します。
2. [サービス ターゲット テンプレートをサービス タイプにリンクさせます](#) (P. 317)。
3. サービス ターゲット テンプレートの詳細を、リクエスト、インシデント、問題、変更要求などのチケット カテゴリに割り当てるか、チケットを発行します。

チケット作成時に、適切なテンプレートがサービス タイプに基づいて自動的にチケットに添付されます。ユーザがチケットを作成するごとに、サービス ターゲットのステータスは自動的に [サービス タイプ] タブに表示されます。

サービス ターゲット テンプレートの作成

サービス ターゲット テンプレートを作成して、リクエスト、インシデント、問題、案件、または変更要求に対するサービス ターゲット テンプレートを測定することができます。このテンプレートは、作成後に、サービス タイプにリンクできます。

注: マルチテナンシーがインストールされている場合は、[テナント] フィールドにテナントを指定します。

次の手順に従ってください:

1. [管理] タブで、[Service Desk] - [サービス ターゲット テンプレート] を選択します。
[サービス ターゲット テンプレート リスト] ページが開きます。
2. [新規作成] をクリックします。
[サービス ターゲット テンプレートの新規作成] ページが開きます。
3. [オブジェクトタイプ] フィールドからチケット タイプを選択して、[続行] をクリックします。
4. 必要に応じて以下のフィールドに値を入力します。

名前

サービス ターゲットの簡潔な識別子を定義します。

オブジェクトタイプ

このサービス ターゲットのチケット タイプを指定します。

ターゲット期間

サービス ターゲットを完了するまでの最大時間を「hh:mm:ss」の形式で指定します。

ワークシフト

サービス ターゲットで時間の計算に使用する業務時間の範囲を含むワークシフトを指定します。例: M-F 08:00-17:00。

コスト

サービス ターゲットを満たせない場合に関連付けられる予定コストなどの情報を定義します。

レコード ステータス

このターゲットがアクティブであるか、非アクティブであるかを示します。

条件

チケットデータを評価してサービス ターゲットが満たされているかどうかを判断する、条件のマクロまたはサイト定義の条件の名前を指定します。

必要な結果

サービス ターゲットが完了されたかどうかを示す **True** または **False** の値を指定します。

実際日時の設定を許可

ユーザがサービス ターゲットの日付および時間を設定できるかどうかを指定します。

実際日時のリセットを許可

ユーザがサービス ターゲットの日付および時間をリセットできるかどうかを指定します。

5. [保存] をクリックします。

サービス ターゲット テンプレートが作成されます。

サービス ターゲット テンプレートをサービス タイプにリンク

サービス ターゲット テンプレートをサービス タイプにリンクすると、サービス タイプが割り当てられた場合にターゲットが自動的にチケットに添付されます。サービス ターゲット テンプレートはサービス タイプに一度だけ割り当てることができます。サービス タイプにはさまざまなサービス ターゲットをリンクできます。

次の手順に従ってください:

1. [管理] タブで、[Service Desk] - [サービス タイプ] を選択します。
[サービス タイプ リスト] ページが開きます。
2. サービス タイプを選択します。
[サービス タイプの詳細] ページが開きます。
3. 選択したオブジェクト タイプのターゲット タブを選択します。たとえば、リクエストのサービス ターゲットを作成した場合は、[リクエスト ターゲット] タブを選択して、問題、インシデント、およびリクエスト チケットを管理します。
4. [サービス ターゲット テンプレートのリンク] をクリックします。
[リンクされたサービス ターゲット テンプレートの新規作成] ページが開きます。
5. 値を直接入力するか、虫眼鏡アイコンをクリックしてサービス タイプを検索します。
6. [続行] をクリックします。
7. 必要に応じて、サービス ターゲット テンプレートに変更を加えます。
8. [保存] をクリックします。

サービス ターゲット テンプレートは、サービス タイプにリンクされています。

サービス ターゲットのチケット カウンタおよびタイマの表示

アナリストが1つのチケットにサービス ターゲットのセットを割り当てている場合は、各ターゲットのステータスおよび完了期限を表示できます。

サービス ターゲットのチケット カウンタおよびタイマを表示する方法

1. **Service Desk** タブで、インシデント、問題、リクエスト、変更要求、または案件のリストを表示します。

チケットの詳細ページが表示されます。

2. **[サービス タイプ]** タブをクリックします。

サービス タイプの詳細情報が、チケットの下部に表示されます。

3. **[ターゲット]** 列で、詳細情報の **[サービス ターゲット]** をクリックします。

[チケット カウンタおよびタイマ] セクションが、**[割り当て済み サービス ターゲットの詳細]** ページの下部の近くに表示されます。**[割り当て済み サービス ターゲットの詳細]** ページには、以下のフィールドが表示されます。

名前

サービス ターゲットの名前を表示します。

ターゲット期間

サービス ターゲットを実行するために配分された時間の長さを表示します。この値は、チケットを編集しない限り、オーバーライドできません。

ワークシフト

サービス ターゲットの時間の計算に使用されるスケジュールを表示します。

条件

チケット データを評価して、作業がターゲット期間内に完了可能かどうかを決定する、条件のマクロ、またはサイトに定義された条件のマクロを表示します。

必要な結果

条件のマクロ、またはサイトに定義された条件のマクロの必要な結果を表示します。

コスト

ターゲットを達成できなかった場合に発生するペナルティを表示します。この情報は、チケットにも表示されます。

ターゲット日/時間

ターゲットの完了期限を表示します。チケットが保留ステータスにあるか、サービス ターゲットが達成された場合、このフィールドは空白です。

実際日/時間

条件が満たされた日時、またはユーザが「実際日時の設定」をクリックした日時を指定します。

残り時間

サービス ターゲットの残り時間の長さを表示します。負の値は、ターゲット期間を超えた時間の長さを示します。

実際日時の設定を許可

実際の時間を設定できるかどうかを表示します。「はい」は、サービス ターゲットの実際日/時間を設定できることを示します。「いいえ」は、実際日/時間をオーバーライドできないことを示します。

実際日時のリセットを許可

時間の計測を再開できるかどうかを表示します。「はい」は、サービス ターゲットの実際日/時間をリセットできることを示します。「いいえ」は、実際日/時間をリセットできないことを示します。

最終変更日/時間

このチケットが最後に変更された日付を表示します。

最終変更者

チケットを最後に編集したユーザの名前を表示します。

サービス タイプ

このサービス ターゲットを添付したサービス タイプの名前を表示します。

サービス ターゲット テンプレート

このサービス ターゲットを作成するために使用されたサービス タイプにリンクされたサービス ターゲット テンプレートの名前を表示します。

保留再計算からターゲット日/時間をロック

チケットが保留状態になるか、延期された場合に、自動的に更新されないようにターゲット日/時間をロックします。

最終開始日/時間

最後にサービス ターゲット タイマが開始された時間を表示します。

チケット ステータス

チケットの [ステータス] フィールドの値を表示します。

保留ステータス

チケット ステータスによりチケットが保留状態になったかどうかを表示します。

最終保留日/時間

チケットが最後に保留状態になった時間を表示します。

保留数

チケットが保留状態になった回数を表示します。

最終解決日/時間

最後にチケットが解決済みステータスに移行した時間を表示します。

解決数

チケットが解決済みステータスに変更された回数を表示します。

最終クローズ日/時間

最後にチケットがクローズ ステータスに変更された時間を表示します。

クローズ数

チケットがクローズ ステータスに変更された回数を表示します。

チケット オープン日/時間

チケットがオープンされた日時を表示します。

チケット解決日/時間

チケットが解決された日時を表示します。

チケット クローズ日/時間

チケットがクローズされた日時を表示します。

サービス ターゲット ステータスの表示

オープンチケットに、各サービス ターゲットのステータスを表示できます。残り時間や違反コストなどのステータス情報は、作業に優先順位を付けるのに役立ちます。

サービス ターゲット ステータスを表示する方法

1. Service Desk タブで、インシデント、問題、リクエスト、変更要求、または案件のリストを表示します。

それぞれのチケット リストが、以下のサービス ターゲット情報と共に表示されます。

サービス ターゲット

次のサービス ターゲットが予定されている時間を表示します。

予測違反

サービス タイプの時間制限に違反したときに発生するコストを表示します。

2. リスト ページから目的のチケットを選択します。

チケットの詳細ページが表示されます。

3. [サービス タイプ] タブを選択します。

注: サービス ターゲットは、管理者がセットアップした条件を満たすチケットに表示されます。優先順位計算により、ターゲット情報の計算および表示の方法が異なる場合があります。

チケットが事前定義済みのターゲット条件を満たす場合は、サービス ターゲットに関する以下の情報がサービス ターゲット リストに表示されます。

アクション

現在の日付と時間を[実際日/時間]に設定またはリセットします。

ターゲット

チケットの現在のサービス ターゲットを指定します。

ターゲット日/時間

このサービス ターゲットが予定されている日時を指定します。チケットが保留ステータスにある場合は、この値が空白です。

実際日/時間

ターゲット条件が満たされた時間を指定します。値が表示されない場合は、ターゲット条件が満たされていません。

残り時間

チケットが保留状態にある場合に、サービス ターゲットの残り時間の長さを指定します。サービス ターゲットが達成されている場合は、余った時間が「残り時間」フィールドに表示されます。負の値は、達成されなかったターゲット日以降の経過時間の長さを示します。

違反コスト

ターゲットを達成できなかった場合に発生するペナルティを表示します。この情報は、チケットにも表示されます。

サービス契約

SLA モデルには、サービス契約が含まれています。サービス契約では、特定の組織を対象として、サービス タイプ、リクエスト領域、案件カテゴリ、変更カテゴリなどの SLA を定義します。このような定義は、プライベート カテゴリおよびプライベート サービス タイプと呼ばれます。

注: プライベートなカテゴリおよびサービス タイプは、サービス契約が使用されるチケットでのみ使用できます。

チケットに適用可能なサービス契約は、チケットの影響を受ける組織によって決まります。この組織は、常にチケットの「影響を受けるエンドユーザ」の組織です（これは、連絡先レコードの「組織」フィールドです）。チケットに対して選択できるのは、サービス契約に一覧表示される領域やカテゴリのみです。また、適用できる唯一のサービス タイプは、契約上のプライベート サービス タイプです。このように選択肢が限定されているため、特定の組織の SLA が間違っただけの組織の SLA と混同されることはありません。

また、サービス契約では、サービス タイプを、優先度やアセットなどのチケット上の共通参照フィールドにマップします。このマッピングによって、サービス タイプとチケットの属性が関連付けられます。たとえば、組織の契約では、5 つの各優先度オブジェクトに対してサービス タイプを割り当てることができます。特定の優先度でチケットを作成すると、マップされたサービス タイプが適用されます。

カテゴリとサービス タイプは契約の外部で定義することができ、パブリックであると判断されます。パブリック定義が使用されるのは、チケットにサービス契約がない場合です。サービス契約がないという状況は、エンドユーザに組織がない場合や、組織の契約が非アクティブである場合に発生することがあります。パブリック定義は、有用なバックアップまたはデフォルトのメカニズムです。パブリック サービス タイプは、カテゴリやほかの参照フィールドオブジェクトで直接設定されます。

適用可能なすべてのサービス タイプがチケットに割り当てられます。この操作により、SLA のすべての要素が表示可能になり、適用されます。以下に例を挙げます。

- 2 日以内に技術者を派遣する必要があるサービス タイプをプリンタに設定します。
- 優先度オブジェクトのサービス タイプに、1 時間以内のコールバックが必要であることを指定します。

両方のサービス タイプを適用すると、これらの必要なアクションが実行されます。

また、複数のサービス タイプをトラッキングすると、チケットの優先度を設定する場合に役立ちます。たとえば、壊れたキーボードのチケットには、優先度の低いサービス タイプが割り当てられます。ただし、その影響を受けるエンドユーザがキーボードを緊急に必要としている場合には、サービスの優先度を上げることができます。

注: SLA モデルはデフォルトで有効になっています。以前のバージョンの CA SDM では、単一のサービス タイプのみがチケットに適用されていました。サービス タイプの選択には、あらゆるサービス タイプの中から最高ランクのタイプを検索する処理も含まれていました。ランク スキームを使用したモデルは、オプションの `classic_sla_processing` をインストールすることによって、現在でも使用できます。

サービス契約のマイグレーション

CA SDM をマイグレーションとしてインストールすると、オプションの `classic_sla_processing` がデフォルトでオンになるため、SLA 処理をマイグレーション前と同様に継続できます。この継続により、適切なサービス契約を作成するまで時間の余裕ができ、最終的に `classic_sla_processing` を無効にすることも可能になります。

サービス契約を作成するときは、サービス タイプ、リクエスト領域、およびカテゴリを作成する必要はありません。サービス契約の詳細ウィンドウにある [コピー] ボタンを使用すると、既存のオブジェクトを契約にコピーできます。

以前のインストールでチケット タイプに対して `support_lev` フィールドを必須と指定していた場合は、この制限を削除する必要があります。`support_lev` フィールドが引き続き存在していて、現在のモデルで値を設定していない場合、新しいチケットでは必須フィールドエラーが発生します。このエラーは、オブジェクトリクエスト (`cr`)、案件 (`iss`)、または変更要求 (`chg`) に影響を与えます。

違反までの時間

SLA モデルの使用を開始すると、CA SDM の違反までの時間 (TTV) システムが役に立ちます。このシステムを使用すると、チケットをトラッキングし、予測される違反時間に応じてチケットの優先度を設定できます。このシステムでは、アクティブなすべてのチケットを監視して、各サービスタイプに対して予測される違反時間を設定します。違反時間とコストに応じてチケットのレポートや並べ替えができるため、最も緊急度やコストが高い案件を最初に解決できます。

TTV システムではアクティブなチケットをすべて監視し、バックグラウンドで SLA イベントを評価して、SLA 違反フラグを設定するイベントを検出します。イベントは実行されませんが、システムはチケットのその時点の状態を監視して各イベントの結果を予測します。評価の結果、SLA 違反フラグを設定することになった場合、チケットのサービスタイプが違反までの時間の値で更新されます。この値が、SLA 違反を確定するイベントが実際に発生する日時になります。

チケットの挿入時または更新時に、評価が実行されます。チケットは高い頻度で更新されるので、評価には短時間の遅れが生じます。遅延の間隔は、`ttv_evaluation_delay` オプションで制御します。遅延が解消されると、TTV システムは SLA 違反フラグを設定する可能性があるすべての SLA イベントを評価します。

各イベントには、条件および条件の結果に応じて開始するアクション（マクロ）をオプションで設定します。適切なパフォーマンスを実現するために、イベントテンプレート情報が TTV システムによってキャッシュされ、定期的に更新されます。直近に更新したイベントテンプレートを含めて TTV が計算した予測には、数分の誤差がでる可能性があります。

注: TTV の予測は、各チケットの [サービス タイプ] タブに表示されます。TTV システムは、`ttv_enabled` オプションでアクティブにします。

タイムゾーンとワークシフト

自動化されたアプリケーション実行に対し、業務上の要求は複雑化しています。この状況に対応するため、CA SDM は、必要な数のタイムゾーンとワークシフトを定義、記録して、簡単に情報を参照できるようになりました。

- タイムゾーンは、ユーザや CI などが存在する地域のタイムゾーンを識別します。
- ワークシフトは、イベント監視中の期間またはサービス タイプや SLA の作業時間が有効になっている期間を定義します。

イベントに適切に対応するには、イベントの発生時刻に基づいて実行アクションを決定することが重要です。管理者が定義したタイムゾーンとワークシフトは、すべての CA SDM 機能で使用できます。

関連項目:

[ワークシフトのセットアップ](#) (P. 329)

[タイムゾーン](#) (P. 530)

タイムゾーンのセットアップ

タイムゾーンコードは、ユーザがシステムに普段アクセスするタイムゾーン（つまり、ユーザの地域のタイムゾーン）または **CI** が存在する地域のタイムゾーンを定義します。営業時間は、**CA SDM** サーバのタイムゾーンに常に入力されます。これは、営業時間を常に一定の基準で比較できることを意味します。

複数のタイムゾーンにまたがって正確な時間を表現できるように、タイムゾーンは、**CA SDM** の機能に基づいて、サービスタイプ、エスカレーション、および影響を受けるエンドユーザへの全体的な対応を管理するために使用されます。ユーザがログインした場所または **CI** が存在する場所のタイムゾーンとサーバが稼働している場所のタイムゾーンの間の差は、**CA SDM** によって自動調整されます。タイムゾーンでは、グリニッジ標準時（GMT）の時間形式を使用します。

注: タイムゾーンを定義する方法については、オンラインヘルプを参照してください。

サービス タイプの複数のタイム ゾーンを管理する方法

CA SDM サーバおよびユーザは別々のタイム ゾーンに配置することができます。時間差によって、ユーザはサービス タイプの有効期限の日時を見逃してしまう場合があります。

時間差を修正するために、CA SDM を設定してエンド ユーザのタイム ゾーンにサービス タイプの有効期限を表示させるようにすることができます。別々のタイム ゾーンの 2 人のユーザが同じチケットを表示した場合、各ユーザはローカル コンピュータのタイム ゾーンに基づいて有効期限の値を表示できます。ただし、開始時間の値には常にサーバのタイム ゾーンが反映されます。

エンド ユーザ タイム ゾーンに対して設定するには、以下の手順に従います。

1. サーバ名とタイム ゾーンを識別するサーバコードを作成します。
2. サービス タイプを作成するか更新します。 [エンド ユーザのタイム ゾーン] フィールドを [はい] に設定します。
[はい] の値により、[有効期限] は各ユーザのタイム ゾーンに応じて表示されて、更新されます。

例: 任意のユーザのタイム ゾーンにサービス タイプの有効期限を表示します。

この例では、CA SDM を設定して、任意のユーザのタイム ゾーンにサービス タイプの有効期限を表示します。サーバとユーザは別々のコンピュータ上、および別々のタイム ゾーンにいます。

サーバ名とタイム ゾーンを識別するサーバコードを作成する方法

1. ホスト サーバの [管理] タブで、[Service Desk] - [アプリケーションコード] を選択します。
2. [コード] - [サーバ] をクリックします。
[サーバリスト] が表示されます。
3. [ローカル ホスト サーバ] をクリックします。
[サーバ名の詳細] ページが表示されます。
4. タイム ゾーンを設定します。たとえば、タイム ゾーンを GMT (EU) に設定します。ローカル ホスト名は、サーバの NX.env に保存されている NX_LOCAL_HOST 値と一致する必要があります。
5. [保存] をクリックします。

ホスト サーバは新しいタイム ゾーンを使用します。ユーザがチケットを表示すると、開始時間にサーバのタイム ゾーンが反映されます。

サービス タイプを作成する方法

1. [管理] タブで、[サービス タイプ] を選択します。
サービス タイプのリストが表示されます。
2. [解決 (優先度 1)] または優先度 1 のリクエストを管理する別のサービス タイプをクリックします。
[サービス タイプの更新] ページが表示されます。
3. [エンド ユーザのタイム ゾーンを使用] チェック ボックスをオンにします。
4. [保存] をクリックします。
サービス タイプのレコードが更新されます。

チケット上にタイム ゾーンを表示する方法

1. 別のコンピュータで、リクエスト チケットを開き、優先度を 1 に設定します。
注: サービス ターゲットを使用している場合は、チケットに値を設定してターゲットが優先度 1 の解決を使用するようにします。
2. チケットを表示して、[サービス タイプ] タブをクリックします。
[開始時間] にはサーバのタイム ゾーンが反映されます。[有効期限] にはエンド ユーザのローカル コンピュータの時間が反映されます。
3. リクエスト チケットを表示するページを閉じます。
4. エンド ユーザのローカル コンピュータでタイム ゾーンを変更します。
5. エンド ユーザのローカル コンピュータにチケットのサービス タイプを表示して、ユーザのタイム ゾーンに基づいて対応する有効期限の値を表示します。
[有効期限] には新しいタイム ゾーンが反映されます。

注: サーバ タイプまたはサーバ コードに関する詳細情報については、オンラインヘルプを参照してください。

ワークシフトのセットアップ

ワークシフトは、イベントまたはスケジュールが有効な曜日、日付、および時間を識別します。曜日か日付、または曜日と日付の両方を指定できます。時刻の指定は省略可能です。

注: ワークシフトを定義する方法については、オンライン ヘルプを参照してください。

チケットのイベントを監視する場合、ワークシフトが定義するのは、イベントを監視している時間、つまり、クロックが動作している時間です。たとえば、定義済みのイベント「P1、アクティブ：案件を担当者に通知」を使用しており、優先度 1 の案件を 4:45 PM にオープンし、ワークシフト スケジュールが 9:00 AM～5:00 PM である場合、監視しているイベントによって翌日の 9:45 AM に通知が自動的に案件担当者に送信されます。

注: ワークシフトは、チケットを連絡先に自動的に割り当てる目的でも使用します。

関連項目:

[サポート ストラクチャの確立](#) (P. 449)

セキュリティ

CA SDM の使用をユーザに許可する前に、必ずセキュリティをセットアップして以下を決定しておきます。

- ユーザにアクセスを許可するシステム
- ユーザに割り当てるアクセス レベル
- ログイン時のユーザの認証方法

注: セキュリティ管理タスクを実行する方法の詳細については、オンライン ヘルプを参照してください。

CA EEM と CA Workflow のユーザ ベース環境設定

CA EEM はユーザ情報 (ID) の中央リポジトリです。CA EEM は、ほかのアプリケーションに対するユーザ認証とアクセスを定義します。複数の CA Technologies 製品をインストールしている場合、一部の製品では CA EEM を使用して ID とアクセス ポリシーを保存できます。CA SDM は、認証にのみ CA EEM を使用します。CA EEM は CA SDM の環境設定オプションではないため、個別にインストールする必要があります。

ユーザ レコードの CA EEM リポジトリは、以下のソースのいずれかになります。

- 外部 LDAP ディレクトリ
- MDB 内の独自の内部テーブル

CA EEM には、MDB を使用するように設定された場合のために LDAP インターフェースが用意されています。

注: CA EEM で使用する MDB テーブルは、CA SDM で使用するものとは異なります。

組織が Active Directory、eTrust Directory などのディレクトリ サーバを使用する場合は、ユーザ ベースとしてそのディレクトリを使用するように CA EEM を設定することを検討してください。この設定により、CA EEM を使用するほかのアプリケーションから、ディレクトリ内のユーザにアクセスできるようになります。CA EEM はアクセス管理を一元化するので、通常は単一のサーバにインストールします。

注: インストールの詳細については、「実装ガイド」を参照してください。

CA Workflow

CA SDM のインストール時に、埋め込みワークフロー エンジンの CA Workflow をオプションでインストールできます。CA Workflow はすべてのユーザ情報の取得に CA EEM を使用するため、CA EEM はすべての認証試行と特定の権限付与を管理します。CA Workflow は CA SDM の連絡先レコードは検知しません。

注: CA Workflow のアクセス設定の詳細については、「実装ガイド」を参照してください。

CA SDM

CA SDM は連絡先情報を MDB テーブルに保存します。これらのテーブルは CA EEM と関係ありません。CA SDM では、アクセスや ID の管理に CA EEM を使用しません。CA SDM 自体のアクセスおよびセキュリティ管理は、アクセス タイプとデータ パーティションを使用して行います。

CA SDM は、認証にのみ CA EEM を使用します。CA EEM を使用して CA SDM のユーザを認証する場合は、CA EEM をインストールします。CA SDM を CA EEM と統合すると、CA SDM オペレーティング システム認証は CA EEM 認証に変更されます。

注: CA EEM のインストールの詳細については、「実装ガイド」を参照してください。CA EEM と CA SDM を統合するには、[オプション マネージャ] - [セキュリティ] で *eiam_hostname*、*use_eiam_artifact*、*use_eiam_authentication* の各オプションを設定する必要があります。これらのオプションの詳細については、オンライン ヘルプを参照してください。

CA SDM ユーザ ベースは CA EEM のユーザ ベースとは独立しています。したがって、CA Workflow ユーザ ベースからも独立しています。CA Workflow の利点は、CA SDM の外部の担当者にワークフロー項目を割り当て、この担当者が項目を完了できることです。この機能は、CA EEM が組織の LDAP サーバを指定している場合に役立ちます。

CA SDM とのインテグレーションには制限があります。ワーク項目は、実際の CA SDM の連絡先レコードに直接割り当てることができません。以下の条件が両方とも満たされる場合のみ、CA SDM の連絡先にワーク項目を割り当てることができます。

- CA SDM の連絡先に対応するレコードが CA EEM にある
- これらのレコードに一致するユーザ ID がある

まとめると、以下のようになります。

- CA SDM は MDB を使用して連絡先情報を保存します。また、CA SDM は LDAP のインテグレーションにより、LDAP サーバから情報を取得して、新しい連絡先レコードを作成し、既存の連絡先とこのディレクトリを同期することができます。
- CA EEM は、ユーザ管理の一元化を実現する CA のソリューションです。複数の CA 製品をインストールしている場合、すべての製品で CA EEM を使用して ID とアクセス ポリシーを管理している可能性があります。

- CA EEM では、ユーザ情報の保存に、外部 (LDAP) ディレクトリを指定するように設定することも、MDB を使用するように設定することもできます。MDB を使用するように設定した場合のために、CA EEM には LDAP インターフェースが用意されています。

注: MDB 内で CA EEM が使用するテーブルは、CA SDM が使用するテーブルとは異なります。

- CA Workflow は常に CA EEM を使用してユーザ情報を取得し、認証を行います。ワーク項目は、CA EEM が管理しているユーザにのみ割り当てることができます。また、CA EEM で定義されたユーザのみが、CA Workflow の IDE とワークリストの Web UI にアクセスできます。

以下の情報は、本製品のさまざまな環境設定オプションと、これらのオプションが CA SDM と CA Workflow のインテグレーションに及ぼす影響について説明しています。CA Workflow を使用するのに最適な設定と（オプションで）LDAP ディレクトリ サーバを選択します。

関連項目:

[CA EEM と CA Workflow のユーザ ベース環境設定 \(P. 330\)](#)

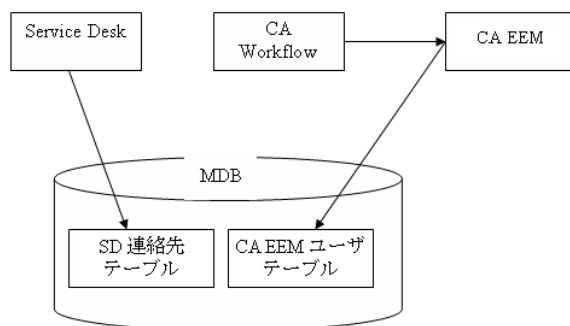
[CA EEM の LDAP 環境設定 \(P. 335\)](#)

初期設定の環境設定

CA SDM と CA Workflow が初期設定のインストールでユーザ情報を保存する場所は以下のとおりです。

- CA SDM では、MDB 内の CA SDM 連絡先テーブルにユーザ情報を保存します。
- CA Workflow では、CA EEM を使用して、MDB 内の CA EEM ユーザ テーブルにユーザ情報を保存します。

以下の図は、製品がどこにユーザ情報を保存するかを表しています。

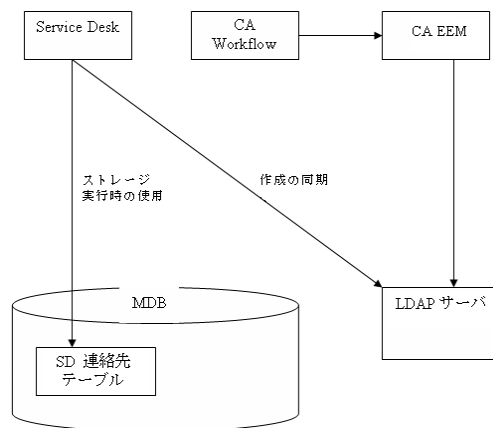


サイトで **CA Workflow** または **LDAP** ディレクトリ サーバをほとんどあるいはまったく使用しない場合は、初期設定の環境設定の使用を検討してください。この環境設定にはいくつか制限があります。**CA Workflow** ユーザはそれぞれ **CA EEM** ユーザ レコードを必要とします。

外部 LDAP サーバの環境設定

CA SDM と **CA Workflow** で同じ **LDAP** ディレクトリ サーバを使用すると、連絡先を簡単に管理できます。ユーザのメインディレクトリとして **LDAP** サーバをすでにサイトで使用している場合、この環境設定は特に便利です。**CA SDM** の **LDAP** 機能を使用すると、連絡先レコードのユーザ ID とディレクトリ内のユーザ ID が一致するため、**CA SDM** アナリストにワーク項目を円滑に割り当てることができます。**CA SDM** で認証に **CA EEM** を使用すると、インテグレーションはより円滑になります。

以下の図は、**LDAP** ディレクトリ内のすべてのユーザが **CA Workflow** ワークリスト **Web** アプリケーションに自動的にアクセスするシナリオを表しています。この設定でも **CA SDM** はユーザ レコードのために **MDB** の連絡先テーブルを使用しますが、これらのレコードを **LDAP** サーバ レコードからインポートして定期的に同期することができます。

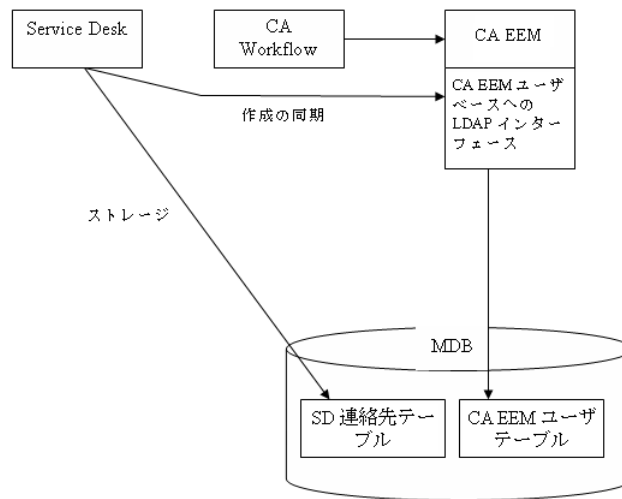


関連項目：

[LDAP ディレクトリ データ](#) (P. 380)

CA EEM の LDAP 環境設定

外部ディレクトリではなく MDB を使用してユーザ情報を保存するように CA EEM を設定すると、CA EEM は LDAP インターフェースを使用してユーザディレクトリを公開します。サイトで外部 LDAP サーバを使用しない場合、LDAP ソースとして CA EEM を使用するように CA SDM を環境設定すると、外部 LDAP の環境設定を利用できます。LDAP サーバを使用していないサイトで CA EEM でユーザ管理を統合する場合、この環境設定は便利です。他の CA 製品でも CA EEM が使用されているため、ユーザ管理を大幅に簡略化できます。



注: この環境設定を使用できるのは、MDB を使用するように CA EEM を設定した場合に限られます。CA EEM を外部 LDAP サーバに設定した場合は、CA EEM ではなく、同じ LDAP サーバを指定するように CA SDM を設定します。

アップグレード

以前のバージョンの CA SDM をアップグレードする場合や多数の連絡先レコードをバッチでロードする場合は、ユーザを CA EEM に手動で追加して CA Workflow にアクセスできるようにする必要があります。

CA EEM r8.4 SP4 CR05 ユーザストアの設定

CA EEM r8.4 SP4 CR05 は、外部 LDAP ディレクトリまたは内部 MDB テーブルにユーザレコードを保存するように設定できます。CA EEM で外部 LDAP ディレクトリを使用する場合は読み取り専用のインターフェースになるため、CA EEM インターフェースでユーザの追加や変更を行うことはできません。

次の手順に従ってください:

1. [スタート] - [プログラム] - [CA] - [Embedded Entitlements Manager] - [EEM UI] をクリックします。

CA EEM ユーザ インターフェースが表示されます。

2. [設定] タブをクリックします。
3. [EEM Server] サブタブをクリックします。
4. 左側のペインで、[グローバル ユーザ/グローバル グループ] リンクをクリックします。
5. 右側のペインで、以下のオプションのいずれかを選択します。
 - 内部データ ストアに格納
 - Reference from an external directory
 - CA SiteMinder から参照

注: [Reference from an external directory] オプションを選択すると、LDAP サーバの詳細を入力するように求められます。

6. [保存] をクリックします。

CA EEM のユーザ ストアの環境設定を完了します。

注: CA EEM の詳細については、CA EEM のオンラインヘルプを参照してください。

CA EEM r12 CR02 ユーザ ストアの設定

CA EEM r12 CR02 は、外部 LDAP ディレクトリまたは内部 MDB テーブルにユーザ レコードを保存するように設定できます。CA EEM で外部 LDAP ディレクトリを使用する場合は読み取り専用のインターフェースになるため、CA EEM インターフェースでユーザの追加や変更を行うことはできません。

次の手順に従ってください:

1. [スタート] - [プログラム] - [CA] - [Embedded Entitlements Manager] - [Admin UI] をクリックします。

CA EEM ユーザ インターフェースが表示されます。

2. [設定] タブをクリックします。
3. [User Store] サブタブをクリックします。
4. 左側ペインで、ユーザ ストアのリンクをクリックします。

5. 右側のペインで、以下のオプションのいずれかを選択します。
 - 内部のユーザストアに格納します。
 - 外部の LDAP ディレクトリから参照します。
 - CA SiteMinder から参照

注: [Reference from an external directory] オプションを選択すると、LDAP サーバの詳細を入力するように求められます。
6. [保存] をクリックします。

CA EEM のユーザストアの環境設定を完了します。

注: CA EEM の詳細については、CA EEM のオンラインヘルプを参照してください。

ユーザとグループの追加

外部ディレクトリを参照するように CA EEM を設定した場合、CA EEM のユーザ インターフェースを使用してユーザを追加することはできません。CA EEM は LDAP サーバの読み取り専用インターフェースとなります。ユーザレコードを更新するには、特定の LDAP サーバ製品に付属のインターフェースを使用する必要があります。

新しいユーザレコードを追加する方法

1. [スタート] - [プログラム] - [CA] - [Embedded Entitlements Manager] - [Admin UI/EEM UI] をクリックします。
2. CA EEM 管理者のユーザ名とパスワードを使用してログインします。これらの値は CA EEM のインストール中に指定します。CA EEM は個別にインストールする必要があります。CA SDM の環境設定オプションではありません。
3. [Manage Identities] タブをクリックします。
4. 左側のペインで [ユーザ] タブをクリックし、既存のユーザレコードの検索や更新を行います。

注: CA EEM グループを管理するには、[グループ] タブをクリックします。
5. ユーザフォルダの左にあるアイコンをクリックします。

ユーザレコードを作成するためのフォームが表示されます。

6. フォームに入力し、[保存] をクリックします。

新しい CA EEM ユーザ レコードが MDB に保存されます。

注: 既存のユーザ レコードを編集する手順やグループ レコードを保守する手順は、この手順に似ています。詳細については、CA EEM のオンライン ヘルプを参照してください。

CA EEM での CA Workflow アクセスの設定

CA Workflow へのログインはすべて CA EEM によって認証されます。CA Workflow IDE またはワークリスト アプリケーションにアクセスするには、ユーザは CA EEM ユーザ レコードを持つ必要があります。CA SDM の環境設定時に指定した CA Workflow の管理者には、完全なアクセス権があります。

Workflow のインテグレーションのために、CA SDM によって初期設定でこのユーザが使用されます。このユーザ アカウントは、オプション マネージャで `cawf_username` オプションと `cawf_password` オプションで設定されます。これらのオプションで設定したユーザ名とパスワードが正しいこと、およびこのユーザが CA EEM 内で CA Workflow のすべてのリソースにアクセスできることを確認する必要があります。

また、CA Workflow では、CA EEM を使用して CA Workflow の特定の機能へのアクセスを制限することもできます。このアクセスは、IDE とプロセスという 2 つのリソース クラスで管理します。

- IDE リソースには、*login* という 1 つのアクションがあり、これによって IDE へのログイン アクセスが許可されます。CA Workflow IDE アプリケーションにログインするには、このアクションを実行する権限がユーザにある必要があります。
- プロセス リソースには、*start* という 1 つのアクションがあり、これによってプロセス インスタンスを開始する機能が与えられます。ワークリスト Web アプリケーション内からプロセスを開始する場合、ユーザはこのアクションを実行する許可を持っている必要があります。

注: CA EEM で管理しているユーザはすべて、CA Workflow ワークリスト アプリケーションにアクセスしてワーク項目タスクを表示および実行できます。この権限は、ワークリストから新規インスタンスを開始する場合のみ有効です。これらのリソース クラスは、CA EEM 内の CA SDM アプリケーション インスタンスで定義されます。CA EEM Web ユーザ インターフェースにログインする際、ここで説明するリソース、ポリシー、およびグループを表示するために、CA SDM アプリケーション インスタンスを指定する必要があります。

IDE にログインする必要があるユーザ、またはプロセス インスタンスを開始する必要があるユーザは、上記で説明したリソースやアクションの権限を持っている必要があります。CA SDM 環境設定は、これらのリソースへのアクセス権を与える 2 つのポリシーを CA EEM に追加します。便宜上、これらのポリシーはアプリケーション インスタンス内の、ワークフロー管理者とワークフロープロセス開始者の 2 つのグループにアクセス権を与えます。ワークフロー管理者グループにユーザを追加するだけで、IDE へのアクセス権をこれらのユーザに与えることができます。ユーザをワークフロープロセス開始者グループに追加すると、これらのユーザはワークリストアプリケーションからプロセスを開始できるようになります。

上記のグループでユーザを追加または削除する方法

1. CA EEM Web UI にログインします。
2. ログイン ページで、CA SDM アプリケーションを選択し、CA EEM の管理者名とパスワードを指定します。
3. CA EEM のメインページで、[Manage Identities] を選択します。
4. [ユーザの検索] を選択し、検索基準を入力して検索を実行します。

5. 結果リストからユーザを選択します。
6. ユーザの詳細画面の [アプリケーション グループ メンバシップ] セクションで、グループ メンバシップを追加または削除します。
注: このセクションが表示されない場合は、[アプリケーション ユーザの詳細の追加] ボタンをクリックします。
7. 操作が完了したら、[保存] をクリックします。
変更が適用されて、ユーザが追加または削除されます。

CA Workflow ワーク項目の割り当て

CA Workflow ワーク項目の役割は、人間にも人間以外の特定の機能にも割り当てることができます。人間以外の特定の機能としては、カスタム Java オブジェクト、コマンドライン プロセス、別の CA Workflow プロセス インスタンスなどがあります。人間の実行者に関しては、CA EEM ユーザ リポジトリであるグローバル ユーザ リストに、ワーク項目の役割を設定します。このリストには、ユーザ ID をセミコロンで区切って指定する必要があります。以下に例を示します。

`ServiceDesk; abeju01; My Group`

この例の場合、ワーク項目はユーザの **ServiceDesk** と **abeju01**、および **My Group** に属しているすべてのユーザに割り当てられます。つまり、これらすべてのユーザがこのワーク項目を完了できます。

注: これらすべてのユーザとグループは CA EEM で管理する必要があります。つまり、**My Group** は CA EEM 内のグループであり、CA SDM 内のグループではありません。

ワーク項目を単一のユーザに動的に割り当てるには、役割ユーザ リストを **\$MyUser** に設定します。

注: 文字列は二重引用符で囲まないでください。

プロセス定義で、**MyUser** という文字列属性を宣言します。ワーク項目を作成すると、**MyUser** 内の値がワーク項目の割り当てに使用されます。つまり、単一のユーザ名であれ、セミコロンで区切ったユーザ名のリストであれ、有効な値を **MyUser** に割り当てる必要があります。この割り当ては、ワーク項目で使用される前に行う必要があります。

ユーザ ID を変数に割り当てる例は、PC の注文定義デモにあります。このデモでは、CA SDM 連絡先レコードのユーザ ID と、CA EEM 内の対応するユーザレコードのユーザ ID は一致するものとします。PC の注文デモでは、Web サービス インターフェースを使用して、CA SDM からユーザ ID を取得する方法がわかります。ユーザ ID は、チケットから取得できます（担当者、カテゴリ担当者など）。

ワーク項目を割り当てる方法

1. CA Workflow IDE を起動します。
2. 編集するプロセス定義名をダブルクリックします。
プロセス定義が [プロセス デザイナ] ウィンドウに表示されます。
3. [役割] タブを選択します。
4. 役割を追加または更新します。
5. 利用可能なアクター リストから [グローバル ユーザ リスト] を選択し、[編集] をクリックします。
6. CA EEM ユーザ ID のリストをセミコロンで区切って入力します。CA EEM に認識されているユーザをブラウズし、選択するには、[Browse] ボタンを使用します。

セキュリティに関する考慮事項

CA SDM を初めてインストールすると、連絡先レコードに定義された明示的なアクセス タイプを持っていないあらゆる連絡先に対して、最大のアクセス権を与えるようにシステムがセットアップされます。事前定義済みセキュリティ実装に追加の変更を加えることができます。最低限、アプリケーションの使用を許可する前に、以下の手順を実行する必要があります。

1. システムに対して適切な初期設定値を決めるために、定義済みのアクセス タイプを確認します。

管理者は初期設定のアクセス タイプとして設定されていますが、ほとんどのサイトでこれは適切な値ではありません。たとえば、サイトによっては、IT 組織のほとんどのメンバに対して、読み取り専用のアクセス権を割り当てる場合があります。初期設定のアクセス タイプとして CMDB ユーザを設定すれば、追加的な権限が必要ない限り、新規ユーザにアクセス タイプを設定する必要がなくなります。同様に、ほとんどのユーザに環境設定を編集する権限が必要な場合は、初期設定のアクセス タイプとして CMDB アナリストを設定します。

2. 該当しない連絡先には明示的にアクセスタイプを割り当てます。

たとえば、初期設定のアクセスタイプとして **CMDB ユーザ**を設定している場合に、アナリストのアクセスタイプを割り当てるには、対象アナリストの連絡先レコードを変更します。

注: 詳細については、オンラインヘルプを参照してください。

CA Process Automation の CA EEM 認証

CA SDM および CA Process Automation は HTTP 上で Web サービス交換を使用して通信します。製品間で必要最低限の機密情報を通過させるためにあらゆる手段が講じられますが、悪意のあるエンティティはユーザ名、パスワードおよび機密情報にアクセスする場合があります。計画的な措置を講じることによって、サーバ通信を安全に保護することができます。

CA Process Automation 認証については、以下の推奨事項を考慮します。

- オプションとして、CA Process Automation を設定して CA EEM を認証サーバとして使用することができます。CA Process Automation は、CA EEM 内でデフォルトのグループおよびポリシーを実装します。デフォルトグループとポリシーは、組織のニーズに合わせて変更できます。
- CA EEM を使用すると、認証の目的でプレーンテキストユーザ名およびパスワードを通過する必要性が削減されます。マルチテナンシーを使用している場合、CA Process Automation 内でマルチテナンシーを有効にするには、CA EEM が必要です。

注: この統合で認証セキュリティを獲得するために、CA EEM を使用するように CA SDM を設定する必要はありません。ただし、CA EEM は CA Process Automation マルチテナンシーの実装に必要です。CA Process Automation でマルチテナンシーを実装する方法の詳細については、CA Process Automation ユーザガイドドキュメントを参照してください。CA Process Automation を設定して CA EEM を認証サーバとして使用する方法の詳細については、CA Process Automation インストールおよび構成ドキュメントを参照してください。

- **CA Process Automation** を設定し、HTTPS 上でセキュアな通信を使用して通信できるようにします。HTTPS URL は SSL/TLS を使用してプレーンテキスト交換を排除する一方で、偶発的または悪意のある漏えいから専有およびその他の機密データを保護します。

注: CA Process Automation を設定して HTTPS を使用するように設定する方法については、CA Process Automation インストールおよび構成ドキュメントを参照してください。

ユーザ認証

CA SDM には、アクセス タイプの一部としてカスタマイズできるユーザ認証ソリューションが備わっています。同じ認証機能が、すべての CA SDM インターフェースと、ほかの CA 製品によって使用されます。

注: 必要に応じて、別のコンピュータに CA SDM ユーザ認証をセットアップできます。詳細については、「実装ガイド」を参照してください。

認証に柔軟性がある場合、Windows、HTTPD ユーザ検証、LDAP 認証など、外部の認証メカニズムを利用できます。オペレーティングシステムのパスワード、PIN、ゲストユーザアクセス、アクセスなしなどのさまざまな内部認証オプションから選択することもできます。

CA SDM がユーザを認証する仕組み

CA SDM は、連絡先レコードに定義されたユーザ ID に基づいてユーザを認証します。また、ユーザがシステムへのアクセスをリクエストすると、以下の処理が実行されます。

1. 外部ユーザ ID が使用可能である場合（HTTPD または Windows 検証から）、CA SDM はログイン ID によって連絡先を参照します。連絡先が見つかり、外部認証を認めるアクセス タイプであった場合、ユーザは製品へのアクセスを許可されます。
2. 外部認証が認められなかった場合、CA SDM はユーザ ID とパスワードの入力を求めます。製品はユーザ ID の連絡先レコードを参照して、アクセス タイプを取得し、このアクセス タイプの指定に従ってユーザの認証を行います。

多くのインストールでは、定義済みアクセス タイプの認証の定義はユーザのタイプに対して適切になっています。ただし、状況によっては、定義済みアクセス タイプに対して認証情報を変更したり、一部のユーザに異なる認証方法を使用するために新しいアクセス タイプを定義したりする必要があります。定義済みアクセス タイプでは、認証設定を確認して、必要性が満たされているかどうか、設定を変更する必要があるかどうか、または追加のタイプを定義すべきかどうかを判断する必要があります。

外部認証

CA SDM では、以下の条件をすべて満たした場合、ユーザはユーザ ID を入力しなくてもシステムにアクセスできます。

- ユーザに外部認証が設定されていること。
- ユーザの外部で認証されたユーザ ID が、連絡先テーブル内の連絡先と関連付けられていること。
- 連絡先レコードのアクセス タイプの認証定義で外部認証が許可されていること。

外部認証では、以下の場合にユーザはシステムへのアクセスが許可されません。

- ユーザが安全でないサーバを経由してアクセスしようとしている。
- ユーザがアクセスしようとしているが、外部認証が許可されないアクセス タイプに割り当てられている。

外部認証を使用する事前定義済みアクセス タイプはありません。ユーザに外部認証を使用する場合は、従業員、アナリスト、および管理者のアクセス タイプを変更して外部認証を設定することを検討してください。外部認証を受け入れるかどうかは、各サイトの要件やユーザのさまざまなタイプによって決まります。外部認証を使用する場合は、サーバの環境設定でファイルとディレクトリへのアクセスを管理します。アクセス タイプの認証を定義するとき、以下のように用途を決定できます。

- **Windows** でのユーザ ログインや HTTPD サーバによる検証など、すでに実装されているどの外部認証も使用しない。
- 実装されている認証を使用し、それに基づいてアクセスを許可または拒否する。

注: 外部認証が許可されない場合、ユーザは指定した検証タイプに基づいて認証されます。

以下は、外部認証のいくつかの例です。

- 管理者アクセス権を持っているユーザが **Windows** コンピュータにログインした場合、ユーザはログイン情報を再入力せずに管理タスクを実行できます。
- HTTPD サーバ検証を持っているユーザの場合、ユーザはログイン情報を再入力せずに **Web** インターフェースにアクセスできます。管理者のアクセス タイプによりアナリストの **Web** ユーザ タイプが指定されるため、アナリストの適切な **Web** インターフェースが自動的に表示されます。

注: 外部認証の詳細については、*統合 Windows 認証を CA SDM 用の実装する方法*のシナリオを参照してください。

検証タイプ

検証タイプは、以下の状況でのみユーザを認証します。

- ユーザのアクセス タイプが外部認証を認めていない場合
- ユーザのアクセス タイプは外部認証が認められているが、ユーザが外部で正常に検証されなかった場合（たとえば、ユーザがセキュリティ機能のないサーバからアクセスしようとした場合）

CA SDM には、以下の検証オプションが用意されています。

- **アクセスなし** - このタイプのユーザがアクセスを許可されるのは、外部認証が認められており、正常に検証された場合のみです。
- **オープン** - このタイプのユーザは、ほかの認証を求められずにアクセスできます。
 - **OS** - このタイプのユーザは、アクセスするためにオペレーティングシステムのパスワードを入力します。検証に使用されるオペレーティングシステムは、ユーザ検証ホストを実行しているオペレーティングシステムです。このオプションは、管理者、アナリスト、および従業員のアクセス タイプの初期設定の検証タイプです。

注: ユーザ検証ホストの詳細については、「実装ガイド」を参照してください。

- **PIN** - このタイプのユーザは、連絡先レコードの [PIN] フィールドに、パスワードとして適切な値を入力することでアクセスできます。 [PIN] フィールドは、PIN を検証タイプとして選択するときに、フィールドの属性名を入力して定義します。PIN は、カスタマアクセス タイプの初期設定の検証タイプです。この検証タイプでは、PIN としてカスタマ ID (contact_num) フィールドの値を使用します。

注: 連絡先テーブルに定義されているオブジェクトである cnt オブジェクトの属性名のリストについては、「テクニカル リファレンス ガイド」を参照してください。

ログイン ユーザ数およびセッション数

以下の KPI は、各ユーザが開いたセッション数に関係なく、システム (CA SDM Web UI、SOAP Web サービス、REST Web サービスなど) にログインしているライセンスされている一意のユーザ数をカウントします。

注: ライセンスされているユーザに対して、[ライセンスの有無] チェックボックスが、連絡先の [アクセス タイプ] ページ ([管理] タブで [セキュリティと役割の管理] - [アクセス タイプ] に移動し、連絡先を検索) で選択されていることを確認します。

- webConcurrentLicenseCt
- webConcurrentSOAPLicenseCt
- webConcurrentRESTLicenseCt
- webConcurrentTotalLicenseCt

以下の KPI は、各ユーザが開いたセッション数に関係なく、システムにログインしているライセンスされていない一意のユーザ数をカウントします。

- webConcurrentNonLicenseCt
- webConcurrentSOAPNonLicenseCt
- webConcurrentRESTNonLicenseCt
- webConcurrentTotalNonLicenseCt

以下の KPI は、間隔中に開始した一意のセッション数をカウントします。

- webSessionCt
- webSOAPSessionCt
- webRESTSessionCt

KPI の説明の詳細については、KPI 詳細ページ（[管理] タブで、[Service Desk] - [KPI] に移動し、KPI を検索）を参照してください。別のセッションタイプからこれらの KPI がカウントする方法の詳細については、「[別のセッションタイプから KPI がカウントする方法 \(P. 347\)](#)」を参照してください。

別のセッションタイプから KPI がカウントする方法

システムには、さまざまなセッションタイプが定義されています。以下の表に、KPI がこれらのセッションをカウントする方法を示します。

注: すべての事前定義済みの KPI は、非アクティブとしてインストールされます。KPI がシステムで機能を開始するには、アクティブに設定する必要があります。[管理] タブで、[Service Desk] - [KPI] を選択し、非アクティブな KPI を検索します。KPI を開き、[アクティブ化] をクリックします。

重要: 同じ名前を持つ重要業績評価指標 (KPI) は、複数のバージョンを同時にアクティブにできません。

セッションタイプ	セッションタイプの説明	KPI 別にカウント
Web クライアント	Web ブラウザセッション	■ webSessionCt ■ webConcurrentLicenseCt ■ webConcurrentNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Java クライアント	Java クライアントセッション	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Web サービス	SOAP Web サービスセッション	■ webSOAPSessionCt ■ webConcurrentSOAPLicenseCt ■ webConcurrentSOAPNonLicenseCt

ユーティリティ	サーバユーティリティセッション	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
ポータル	ポータルセッション	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
ナレッジチャット	ナレッジチャットセッション	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
メールサーバ	メールサーバセッション	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
カスタムアプリケーション	カスタムアプリケーションセッション	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
PDA クライアント	PDA クライアントセッション	■ webSessionCt ■ webConcurrentLicenseCt ■ webConcurrentNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
REST クライアント	REST Web サービスセッション	■ webRESTSessionCt ■ webConcurrentRESTLicenseCt ■ webConcurrentRESTNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt

例: KPI のユーザ数の計算

ライセンスされている 1 人のエンドユーザ（[ライセンスの有無] チェックボックスがオン）と、ライセンスされていない 2 人のエンドユーザが Web セルフ サービス インターフェースにログインし、いくつかのアナウンスメントを確認しています。

同時に、ライセンスされている 5 人のアナリスト（[ライセンスの有無] チェックボックスがオン）がアナリスト インターフェースにログインし、インシデントに対して作業しています。アナリストの 1 人は、SOAP Web サービス インターフェースにもログインしています。

- **webConcurrentLicenseCt KPI** は、各ユーザが使用しているインターフェースの数に関係なく、**6** という数を表示し、現在 **6** つのライセンスが使用されていることを示します。
- **webConcurrentNonLicenseCt KPI** は、各ユーザが使用しているインターフェースの数に関係なく、**2** という数を表示し、システムにライセンスされていない **2** 人のユーザがログインしていることを示します。
- **webSessionCt KPI** には、**8** という数が表示されます。これは、合計 **8** 人のユーザが **CA SDM** の **Web UI** にログインしていることを意味しています。
- **webSOAPSessionCt KPI** には、**1** という数が表示されます。これは、**1** 人のユーザが **SOAP Web** サービス インターフェースにログインしていることを意味しています。

(高可用性設定にのみ適用可能)例: KPI の別のノードからのユーザ数の計算

ライセンスされたアナリストが、バックグラウンドサーバからアナリスト インターフェースにログインし、インシデントに対して作業しています。同じアナリストが、アプリケーションサーバからアナリスト インターフェースにログインしています。**webConcurrentLicenseCt KPI** には、ユーザのログイン元のノードまたはサーバの数に関係なく、**1** という数を表示されます。これは、現在 **1** つのライセンスが使用されていることを意味しています。

内部ログ

特定のアクセス タイプに対して、内部ログの表示を認めるかどうかを定義できます。内部ログの表示が認められると、連絡先に対して各 [ログへのアクティビティの記録] ウィンドウに [内部] とラベルが付いたチェックボックスが表示されます。このボックスをオンにすると、アクティビティが内部として設定されます。アクティビティが内部と設定されると、内部ログの表示を認められたアクセス タイプを持つ連絡先のみが、このアクティビティを表示したり、通知を受けたりするようになります。

CA SDM インテグレーション

アクセス タイプは、**CA SDM** とほかの **CA** 製品を併用している場合、同じアクセス タイプを持つ連絡先のユーザ タイプも識別します。同じアクセス タイプを持つ連絡先がほかの製品を使用する場合、この製品に対するユーザ権限はこのアクセス タイプに管理者が指定した値によって決定されます。

データ パーティションの関連付け

データ パーティションは個別の連絡先に割り当てることができますが、アクセス タイプに基づいて割り当てることをお勧めします。データ パーティションをさまざまなアクセス タイプに関連付けた後、特定のアクセス タイプに連絡先を関連付けて、その連絡先のデータ パーティションを定義できます。アクセス タイプは、連絡先データ パーティションを無効化する特殊なオプションを備えています。

アクセス タイプにデータ パーティションを関連付けるには、サイトにとってわかりやすいデータ パーティションをセットアップし、アクセス タイプを定義または変更するときにその中から 1 つ選択します。

重要: ほかの **CA SDM** セキュリティ設定が、データ パーティションよりも優先されることがあります。

データ パーティションをセットアップする方法

データ パーティションは **CA SDM** データベースのサブセットであり、このサブセットを使用することで、チケットやその他のデータ レコードに対するユーザ アクセスをコンテンツに基づいて管理できます。

たとえば、ユーザによるデータベース参照を、ユーザの組織に割り当てられた構成アイテムに限定できます。また、ユーザによる更新を、割り当てられたチケットのみに制限し、ほかの構成アイテムに対しては読み取り専用アクセスのみを許可することもできます。

データ パーティションは、制約のセットで構成されます。データ パーティションの制約は、データ パーティションと制約タイプで管理されているテーブルを識別します。制約タイプは、作成、削除、更新、表示など、データ パーティション内でユーザが実行できる操作を指定します。まずデータ パーティションをアクセス タイプに割り当て、次にこのアクセス タイプをユーザの連絡先レコードに割り当てます。制約と制約タイプを使用して、**CA SDM** データベース テーブル内のレコードに対するユーザのアクセスを管理します。

また、これらを使用して、データ パーティションとは別に制約を表示できます。たとえば、データ パーティションとは関係なく、特定のテーブルのすべての制約を表示できます。

前提条件を確認します。

データ パーティションをセットアップする前に、以下の前提条件を確認します。

- [データ セキュリティ構造とポリシー](#) (P. 351)
- [データ パーティションのセットアップ](#) (P. 351)
- [制約の指定](#) (P. 352)

データ セキュリティ構造とポリシー

データ セキュリティの計画には、データベースの特定部分へのアクセスに対する制限の適用が含まれます。これらの制限は、役割またはアクセス タイプのいずれかによって個別の連絡先に強制的に適用できます。

役割

役割のユーザがアクセスを許可される機能を定義します。個別の連絡先レコード、またはアクセス タイプに 1 つ以上の役割を割り当てて、連絡先に関連付けられているすべてのアクセス タイプに対して機能へのアクセスを定義できます。

アクセス タイプ

連絡先が Web インターフェースにログインする場合の認証方法を定義します。たとえば、アクセス タイプは、Web Screen Painter を使用して、連絡先が Web フォームまたはデータベース スキーマを変更できるかどうか、どの役割が連絡先に使用可能かを決定します。

Service Desk 管理者は、事前定義済みのアクセス タイプを変更でき、また新規に作成できます。役割を通して個別のユーザまたはユーザのグループに制限を適用できます。

以下を識別します。

- オブジェクト、およびこれらのオブジェクトに強制的に適用する制限のタイプ。
- データ パーティションを適用するユーザと役割。データ パーティションは、連絡先に直接適用でき、役割に基づいてデータ パーティションを割り当て、すべての連絡先にこの役割を直接またはアクセス タイプを通して割り当てることをお勧めします。

データ パーティションのセットアップ仕様

データ パーティションは無制限に定義できます。各データ パーティションは、データ パーティションで制限する各データベース テーブルに対する制約と検証のセットです。データ パーティションの各テーブルに対しては、**SQL WHERE** 節と同様の形式で指定する基準によって、レコードの表示、更新、作成、または削除の独立した権限を指定できます。アクセスするレコードや結合するレコードの任意の属性に対し、ユーザの連絡先レコードにある任意のデータを使用して制限を設定できます。この設定により、データ パーティションを定義する際の柔軟性が大幅に高まります。たとえば、連絡先テーブルのベンダー フィールドを使用すると、**CA SDM** への直接アクセスを許可されたベンダーに対してデータ パーティションの制限を設定できます。

CA SDM では、パフォーマンス上の理由により、データ パーティションの制約に直積結合を使用できません。直積結合は、「**OR**」を含む制約の結果であり、すべての結合テーブルを **OR** の両辺の指定で完全に制限します。データ パーティションの制約が直積結合にならないように十分に注意して、以下のコマンドを入力します。

Windows

```
bop_cmd -f $NX_ROOT\bopcfg\interp\bop_diag.frg "check_queries()"
```

UNIX

```
bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"
```

重要: このプログラムでフラグを設定するデータ パーティションは、適切に更新する必要があります。

制約の指定

Majic でオブジェクト定義用のメタ言語を使用して、制約と検証テストを指定します。

注: 詳細については、「テクニカル リファレンス ガイド」を参照してください。

Majic で定義する制約は、**SQL WHERE** 節に非常に似ていますが、以下のようないずれかの違いがあります。

- 制約内に記述する属性名には、オブジェクト属性名を指定し、スキーマから取得したデータベースの属性名は使用しません。

- 以下の形式で名前を指定すると、ログインユーザの連絡先レコードの属性値を参照できます。*att_name* は、目的の属性の Majic 名です。 -

@root.att_name

たとえば、@root.location を指定すると、現在の連絡先のロケーション ID が参照されます。

結合は、以下の形式で指定します。*foreign-key* は、データ パーティション制約を記述するテーブルの SREL 属性の Majic 名です。

attribute-in-referenced-table は、結合するテーブルの属性の Majic 名です。

foreign-key.attribute-in-referenced-table

たとえば、インシデント レポートに関連付けられたアセットの保守ベンダーを参照するには、以下のように指定します。

resource.vendor_repair

これは再帰的指定です。たとえば、以下のように指定すると、ベンダーの名前を参照できます。

resource.vendor_repair.name

Change_Request テーブル（変更要求情報の保存に使用）に適用できる有効な制約の例を以下の表に示します。

制約タイプ	コードと説明
View	assignee.organization = @root.organization この指定では、ユーザは担当者の組織がユーザの組織と同じである変更要求のみを表示できます。
Pre-Update	requestor = @root.id この指定では、ユーザは自分自身がコール元または依頼者である変更要求のみを更新できます。

ただし、以下の例のような式の両辺で結合を使用する制約は記述できません。

assignee.org = requestor.org

データ パーティション制御テーブルの表示

制御テーブルは、Service Desk 管理者がデータ パーティションを使用して、制限を強制的に適用できるテーブルのリストです。これらのテーブルでは、ユーザ アクセスを制限できるオブジェクトおよびテーブルを確認できます。

注: 制御テーブルを追加または削除したり、オブジェクト名を変更したりすることは、できません。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理] - [データ パーティション] - [データ パーティション制御テーブル] を選択します。
[制御テーブル] リストが表示されます。
2. (オプション) [フィルタを表示] をクリックし、1 つ以上の検索フィールドに入力します。
3. 表示するテーブル名を選択します。
[データ パーティション制御テーブルの詳細] ページが開きます。

データ パーティションの制約の作成

データ パーティションの制約は、そのデータ パーティションに割り当てられたユーザによるデータベース レコードへのアクセスを制限します。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理]-[データ パーティション] - [データ パーティションの制約] を選択します。
[データ パーティションの制約リスト] ページが開きます。
2. [新規作成] をクリックします。
[データ パーティションの制約の新規作成] ページが開きます。
3. 必要に応じて、[\[データ パーティションの制約\] フィールド](#) (P. 356) に入力します。
4. 必要に応じて、タブ内の情報を入力します。

制約

データ パーティションに割り当てられているユーザが表示、作成、更新、または削除できるテーブル内のレコードを制御する基準を指定します。たとえば、ユーザが割り当てられた案件の更新のみを実行できるよう指定できます。データ パーティションに割り当てられているユーザが、条件に一致しないレコードをリクエストすると、そのレコードは読み取り専用を設定されます。

制限: 4000 バイト

SQL 変換

制約の定義が SQL 形式で表示されます。[制約] タブで入力した条件が検証され、基礎となる SQL WHERE 句が構築されます。この変換は、検証用に [SQL 変換] タブに表示されます。

5. [保存] をクリックします。

制約が保存され、データ パーティションに追加されます。

例: CAB 割り当てに関するデータ パーティションの制約の作成

ログインユーザが所属する CAB に割り当てられた変更要求のみの更新をユーザに許可するデータ パーティションの制約を作成できます。

CAB 変更要求のユーザ割り当てに関するデータ パーティションの制約を作成するには、データ パーティション内の Change_Request 制御テーブルの制約値を以下のように割り当てます。

- 制約タイプ：更新前
- 制約の仕様： `cab.[group]group_list.member IN (@root.id)`

ログインユーザは、ユーザが所属する CAB に割り当てられた変更要求のみ更新できます。

関連項目

[\[データ パーティションの制約\] のフィールド](#) (P. 356)
[制約の定義](#) (P. 358)

[データ パーティションの制約]のフィールド

以下のフィールドに入力し、[データ パーティションの制約] フィールドを追加または変更します。

データ パーティション名

制約が定義されているデータ パーティションの名前を指定します。

テーブル名

制約によって制御されるデータベース テーブルを指定します。

制約タイプ

定義する制約のタイプです。データ パーティションのテーブルごとに 6 つの制約タイプがあります。

作成

レコードの作成前に満たす必要がある基準を指定します。データ パーティション内のユーザが、作成テスト条件に一致しないレコードを作成しようとする、制約に関連付けられたエラー メッセージが表示され、レコードが保存されません。

デフォルト

セミコロンで区切って 1 つ以上の割り当てステートメントを指定して、レコードの格納時に新しいレコードの空フィールドに割り当てる値を定義します。割り当てステートメントの構文は次のようになります。
att_name は、レコードの属性の Majic 名です。**value** は、整数、引用符で囲んだ文字列、現在のユーザの連絡先レコードの Majic 属性への参照 (**@root.att_name**) のいずれかを指定します。

`att_name=value`

チケットのために更新されるテーブルの場合、初期設定値は表示のときにレコードに入れられ、新しいレコードの初期画面に表示されます。参照フィールド (Majic SREL) に初期設定値を割り当てるには、固定 ID の形式でコーディングします。固定 ID は、オブジェクト名に続けてコロンと整数の ID を指定した値です。たとえば、初期設定の指定に以下の値を入力することで、カテゴリに初期設定値を指定できます。PCAT は SREL のターゲットであり (Majic ファイルで示すとおり)、12345 は目的のカテゴリの ID 番号です。

```
category='PCAT:12345'
```

以下のコマンドを使用して、オブジェクトの固定 ID を一覧表示できます。

```
bop_odump domsrvr pcat "" sym
```

削除

レコードを削除する場合に満たす必要がある基準を指定します。データ パーティション内のユーザが、削除条件に一致しないレコードを削除しようとする、制約に関連付けられたエラー メッセージが表示され、レコードが削除されません。

更新前

管理対象のテーブル内で、ユーザがデータ パーティションで更新できるレコードを指定します。データ パーティション内のユーザが、更新前条件に一致しないレコードをリクエストすると、レコードは読み取り専用になり、制約と共に定義されたエラー メッセージが表示されます。

更新

レコードの保存時に満たす必要がある基準を指定します。データ パーティション内のユーザが、更新条件に一致しないレコードを保存しようとする、制約に関連付けられたエラー メッセージが表示され、レコードが保存されません。

表示

管理対象のテーブル内で、ユーザがデータ パーティションで表示できるレコードを指定します。ユーザが明示的に指定した選択基準に加えて、この制約が、データ パーティション内でユーザが選択したすべてのリストに自動的に適用されます。

表示できるのは、ほかのテーブルとの結合と、現在のユーザまたはログインユーザの連絡先レコードにある **Majic** 属性を **@root.att_name** の形式で参照した値です。以下に有効な例を示します。

```
requestor.organization = @root.organization  
requestor.organization.name = 'MIS'  
assignee = @root.id  
assignee.organization = @root.organization
```

注: 作成、削除、更新前、および更新の各制約タイプは、他のテーブルとの結合をサポートするようになりました。また、**@root.attribute** の形式で、現在のユーザの連絡先レコードの属性を参照できます。

レコード ステータス

制約がアクティブであるか、非アクティブであるかを示します。

エラー メッセージ

制約条件が満たされない場合に、ユーザにメッセージが表示されます。たとえば、「自分に割り当てられた案件しか更新できません」、「自分の所属する組織の案件しか作成できません」、「自分の連絡先レコードは更新できますが、データ パーティションは変更できません」などを指定できます。

制約の定義

条件を Majic 形式 (CA SDM オブジェクトの定義に使用されるメタ言語) で指定します。

〔制約タイプ〕が〔表示〕の場合は、他のテーブルへの結合と、ログイン済みユーザの連絡先レコードにある Majic 属性への @root.att_name 参照を、条件に含めることができます。〔制約タイプ〕が〔表示〕以外の場合は、別のテーブルへの結合と、ログイン済みユーザの連絡先レコードにある Majic 属性への @root.att_name 参照を含めることはできません。

〔制約タイプ〕が〔初期設定〕の場合は、新規レコードの保存時に空のフィールドに割り当てられる値を指定する、セミコロンで区切られた 1 つまたは複数のステートメントを指定できます。割り当てステートメントの構文は、以下のとおりです。

```
att_name=value
```

att_name はレコードの Majic 属性の名前で、値には整数、引用符で囲まれた文字列、またはログイン済みユーザの連絡先レコードの Majic 属性への @root.att_name 参照を指定できます。CA SDM でのデフォルト値の使用方法は、以下のように影響を受けるテーブルによって異なります。

案件のように CA SDM によって更新されたテーブルの場合、デフォルト値はレコードを表示するときにレコードに設定され、新規レコードを初めて表示するときに表示されます。デフォルト値を参照フィールド (Majic SREL) に割り当てするには、テーブル名の後にコロンと整数 ID を付けた固定 ID の形式で指定します。たとえば、カテゴリの初期設定値を指定するには、以下のように指定します。

```
category='PCAT:12345'
```

PCAT は Majic ファイルに設定されている SREL のターゲットで、12345 は目的のカテゴリの ID 番号です。以下の形式のコマンドで、テーブルの固定 ID を表示できます。

```
bop_odump domsrvr pcat "" sym
```

データ パーティションの作成

データ パーティションは **CA SDM** データベースのサブセットです。このサブセットを使用すると、チケットなどのデータ レコードへのユーザ アクセスを内容に基づいて制御できます。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理]-[データ パーティション] - [データ パーティション リスト] を選択します。
[データ パーティション リスト] ページが開きます。
2. [新規作成] をクリックします。
[データ パーティションの新規作成] ページが開きます。
3. 必要に応じてフィールドにデータを入力します。

データ パーティション

データ パーティションの一意の識別子を定義します。

レコード ステータス

パーティションがアクティブであるか、非アクティブであるかを示します。

4. [保存] をクリックします。
5. [新規成約] をクリックし、制約の定義をパーティションに添付します。
6. [保存] をクリックします。

データ パーティションがデータ パーティション制約と共に保存されます。

関連項目

[データ パーティションの制約の作成](#) (P. 355)

アクセス タイプの作成

アクセス タイプによって、セキュリティのあらゆる側面が定義されます。事前定義のアクセス タイプがいくつか用意されている以外に、それらを変更したり、新しいアクセス タイプを作成したりできます。ユーザの各アクセス タイプは、以下のようなシステムの動作を制御します。

- ユーザのログイン時に CA SDM が Web 認証を実行する仕組み。
- ユーザのアクセス レベル。
- ユーザが Web Screen Painter を使用して Web フォームまたはデータベース スキーマを変更できるかどうか。
- ユーザに使用可能な役割であるもの。

次の手順に従ってください：

1. [管理] タブで、[セキュリティと役割の管理] - [アクセス タイプ] を選択します。

[アクセス タイプ リスト] ページが開きます。

デフォルト：15

2. [アクセス タイプの新規作成] ページで、必要に応じて、[新規作成] をクリックし、[\[アクセス タイプ\] のフィールド](#) (P. 361) に入力します。
3. タブを使用して、以下のタスクを完了します。
 - [アクセス タイプに対する Web 認証の設定](#) (P. 363)
 - [Web スクリーン ペインタのアクセス タイプへの割り当て](#) (P. 365)
 - [役割のアクセス タイプへの割り当て](#) (P. 365)
4. [保存] をクリックします。

アクセス タイプが作成されます。

[\[アクセス タイプ\] のフィールド](#)

［アクセスタイプの新規作成］、［アクセス タイプの詳細］、［アクセス タイプの更新］の各ページには、以下のフィールドが表示されます。

シンボル

アクセス タイプの一意の識別子を指定します。

デフォルトにする

このアクセス タイプが連絡先に関連付けられたデフォルトかどうかを示します。

レコードステータス

このアクセス タイプがアクティブであるか、非アクティブであるかを指定します。

説明

アクセス タイプについて説明します。このフィールドを使用して、アクセス タイプの特性を識別しやすくします。

内部通知を受け取る

このアクセス タイプに関連付けられる連絡先が、チケットに関連付けられたアクティビティの内部通知を受信するかどうかを指定します。

アクセス レベル

ユーザが別のユーザに付与できるアクセス タイプを決定します。割り当てるアクセス タイプのアクセス レベルがユーザ自身のアクセス タイプの許可レベルより低い場合のみ、別のユーザの連絡先レコードにアクセス タイプを割り当てることができます。レベルは以下のとおりです。

- 管理（最高レベル）
- アナリスト
- カスタマ/従業員
- なし（最低レベル）

ライセンスの有無

この連絡先がライセンス付きのアクセス タイプかどうかを指定します。ライセンスなしのアクセス タイプに割り当てられた連絡先は、自分の個人データの表示または更新のみできます。

注: KPI は、システム (CA SDM の Web UI、SOAP Web サービス、REST Web サービスなど) から、ユーザの同時実行の使用状況をカウントします。たとえば、webConcurrentLicenseCt KPI は、間隔内に CA SDM の Web UI にログインしている ([ライセンスの有無] オプションが選択された) 一意のユーザの最大数をカウントします。ログイン ユーザおよびライセンスを付与されたユーザ数の詳細については、「管理ガイド」を参照してください。

アクセス タイプに対する Web 認証の設定

Web 認証と検証タイプを構成するには、ユーザが CA 製品にアクセスしようとしたときの、このアクセス タイプに割り当てられた役割の認証方法を指定します。 [Web 認証] タブ内の以下のフィールドに入力します。

外部認証を許可

HTTPD サーバまたはオペレーティング システムなどによって連絡先が外部で認証されるようにする場合は、このチェック ボックスを選択します。 このオプションを選択した場合は、このアクセス タイプのユーザが、インストール中に設定される適切な外部メソッドによって検証されます。 外部認証が行われたかどうか（ユーザが、セキュアでないサーバ経由でアクセスしようとしていないことなど）が確認されます。また、ログイン ID の使用により、システムの有効な連絡先としてユーザが定義されているかどうかも確認されます。 次に、アクセス タイプを使用して、使用すべき正しいインターフェースが特定されます。

検証タイプ

外部認証が許可されなかったユーザ、または失敗したユーザの認証方法が表示されます（ユーザがセキュリティ保護されていないサーバ経由でアクセスしようとした、など）。 使用できるオプションは以下のとおりです。

アクセスなし

外部認証が許可され、有効である場合以外は、CA 製品へのアクセスが拒否されます。

オープン

CA 追加の認証が要求されず、製品アクセスが常に許可されます。

OS

オペレーティング システムのユーザ名およびパスワード経由で、CA 製品へのアクセスが許可されます。

PIN/PIN 番号

このタイプのユーザは、自分の連絡先レコードの [PIN] フィールドに正しい値を入力した場合にのみ、アクセスできます。 [PIN] オプションを選択した場合、使用するフィールドの属性名を [PIN フィールド] ボックスに入力することで、連絡先レコードのどのフィールドに PIN を格納するかを選択できます。

CA EEM

CA EEM 経由で、CA 製品へのアクセスが許可されます。このオプションは、CA SDM が CA EEM に統合されている場合にのみ使用可能です。

Web スクリーン ペインタのアクセス タイプへの割り当て

Web Screen Painter (WSP) ユーティリティを使用すると、CA SDM ユーザは Web フォームやスキーマをビルドおよび発行できます。また、[Web Screen Painter] タブは、Web Screen Painter プレビュー セッション用のデータベース アクセスを制御します。WSP の詳細については、*Web Screen Painter* のオンライン ヘルプを参照してください。

[Web Screen Painter] タブのアクセス タイプに付与する権限を選択します。

フォームを変更する

変更内容を他のユーザが使用できないように、既存のフォームを変更できます。

スキーマを変更する

変更内容を他のユーザが使用できないように、既存のスキーマを変更できます。

フォームを発行する

変更したフォームをすべてのユーザが使用できるようにします。

スキーマの発行

変更したスキーマをすべてのユーザが使用できるようにします。

プレビュー セッションによりデータベースを更新する

プレビュー セッション中にユーザがデータベースを変更できるようにします。デフォルトでは、プレビュー セッション中にデータベースは変更できません。

役割のアクセス タイプへの割り当て

役割をアクセス タイプに割り当てると、その役割に割り当てられた連絡先による機能領域へのアクセスが制限されます。

次の手順に従ってください:

1. このアクセス タイプについて、以下の役割を選択します。

レポートニング役割

このタイプのレポート アクセスを定義します。

REST Web サービス API 役割

このタイプの、REST Web サービスへのアクセスを定義します。

SOAP Web サービス API 役割

このタイプの、SOAP Web サービスへのアクセスを定義します。

コマンドライン ユーティリティ役割

このタイプの、コマンドラインユーティリティへのアクセスを定義します。

2. [役割の更新] をクリックします。
[役割の検索] ページが開きます。
3. 目的の役割のみリストするための検索条件を入力し、[検索] をクリックします。
[割り当て済み役割] - [更新] ページが開き、検索条件に一致する役割がリストされます。
4. このアクセス タイプに割り当てる役割を左側のリストから選択します。複数のアイテムを選択するには、**Ctrl** キーを押しながら左マウスボタンをクリックします。
5. 目的の役割をすべて選択した後、二重の右矢印をクリックします。
選択した役割が右側の [割り当て済み役割] リストに移動します。
6. [OK] をクリックします。
[アクセス タイプの詳細] ページが開き、割り当てられた役割が [役割] タブにリストされます。
7. [保存] をクリックします。
変更が保存されたことを示す確認メッセージと共に、[アクセス タイプの詳細] ページが開きます。
8. ログイン時にこのアクセス タイプのデフォルトとして使用する役割を選択し、[デフォルトの役割の設定] をクリックします。

デフォルト役割の選択が保存されます。

役割へのデータ パーティションの追加

データ パーティションがリンクされている役割に切り替えます。役割は、割り当てられているデータ パーティションに対してのみアクセス権があります。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。
[役割リスト] ページが開きます。
2. 役割を選択し、[編集] をクリックします。
3. [権限] タブに移動し、[データ パーティション名] をクリックします。
4. データ パーティション リストからデータ パーティション名を検索して選択します。
5. [権限] タブで、[連絡先データ パーティションより優先する] を選択します。[連絡先データ パーティションより優先する] をオンにすると、役割データ パーティションが強制的に適用され、それ以外の場合は連絡先データ パーティションが強制的に適用されます。
6. [保存] をクリックします。

データ パーティションの制約のテスト

データ パーティションの制約をテストして、作成した制限が連絡先に適切に適用されることを確認します。データ パーティションの制約によってアクセスが制限されると想定されているデータ レコードの表示と編集を試行します。

次の手順に従ってください:

1. データ パーティションの制限を適用した連絡先を使用して、CA SDM にログインします。
2. データ パーティションの制約が適用されるオブジェクト データへのアクセスを試行します。

制限が設計通りに機能する場合、データ パーティションが正常に作成および適用されたことを示しています。

役割に基づいた権限への ナレッジ マネジメント データ パーティションの制約の設定

ナレッジ マネジメント データ パーティションが有効になっていて、デフォルトでは **CA SDM** 内でグループと役割の権限を使用することができます。以前のリリースからアップグレードしている場合は、マイグレーション ツールがデータ パーティションの制約を更新します。

以前のリリースで、カスタム データ パーティションの制約を使用してナレッジ許可を管理していた場合は、**O_INDEXES** テーブルと **SKELETONS** テーブルの制約を手動で更新してください。環境に応じてデフォルトのデータ パーティションの制約を表示して変更を適用することができます。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理] - [データ パーティション] - [データ パーティションの制約] を選択します。
[データ パーティションの制約リスト] ページが開きます。
2. [フィルタを表示] をクリックし、検索は以下の検索条件を使用します。
 - [データ パーティション] 検索に「**Service Desk アナリスト**」と入力します。
 - [テーブル] 検索に「**O_INDEXES**」と入力します。
3. [制約] タブを変更して [表示の制約] タイプを編集し、以下のように「**READ_PGROUP in @root.pgroups**」を置換します。

`READ_PGROUP in @root.pgroups OR
READ_PGROUP.[pgroup]contained_roles.role IN @root.id`
4. 制約を保存します。
5. [制約] タブを変更して [削除の制約] タイプおよび [更新前の制約] タイプを編集し、以下のように「**WRITE_PGROUP in @root.pgroups**」を置換します。

`WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.[pgroup]contained_roles.role IN @root.role`
6. 制約を保存します。
7. データ パーティション内の **SKELETONS** テーブルで、手順を繰り返して [表示の制約]、[削除の制約]、および [更新前の制約] を更新します。
データ パーティション制約が更新されます。

調査

カスタマ調査により CA SDM 管理者は、サービスデスクのパフォーマンスに関して、カスタマフィードバックを組織的に収集および分析できます。サイトのニーズに応じて、調査をカスタマイズできます。

調査を目的としたシステムの環境設定

調査を使用するには、以下の 2 つの手順に従って、システムを適切に環境設定する必要があります。

1. **CA SDM Web** インターフェースのインストールと環境設定を行います。ユーザが調査のために URL にアクセスすると、**Web** インターフェースによって調査がフォーマットされて調査情報が入力されます。詳細については、「実装ガイド」を参照してください。
2. **CA SDM Web** エンジンの場所を指定するには、オプション マネージャを使用して、**web_cgi_url** オプションの設定とインストールを行います。詳細については、「システムの動作の制御」の章とオンライン ヘルプを参照してください。

調査の準備

標準のリストウィンドウである [カスタマ調査リスト] を使用して、調査を準備します。たとえば、このウィンドウを使用して、すべての調査を表示したり、入力した検索基準に基づいてサブセットを表示したりすることができます。また、調査の新規作成、特定の調査の詳細表示、およびその時点で一覧表示されている調査のレポート作成を実行できます。

各調査では、以下の項目を定義できます。

- 検索とレポートに使用できる名前
- カスタマに調査の目的を説明する紹介文
- カスタマに回答を求めるために整然と構成された質問のリスト（各質問には選択肢のセットが含まれます）
- ユーザが自由な形式で意見を書き込めるオプション領域
- ユーザが調査をサブミットした後で表示される完了メッセージ

注: 調査を作成する方法の詳細については、オンライン ヘルプを参照してください。

調査通知の定義

[アクティビティ通知の更新] ページの [調査] タブでは、アクティビティ通知の調査通知を定義できます。選択したアクティビティ通知がトリガされると、アクティビティを開始した連絡先は調査通知を受け取ります。アクティビティ ログは、調査通知が送信されたとき、および調査通知に関する顧客からの応答が受信されたときの両方で生成されます。

調査通知を設定するには

1. [管理] タブで、[通知] - [アクティビティの通知] を参照します。
[アクティビティ通知リスト] が表示されます。
2. 目的のアクティビティ通知を選択します。
詳細ページが表示されます。
3. [編集] ボタンをクリックします。
[アクティビティ通知の更新] ページが表示されます。
4. 必要に応じてフィールドを編集します。
5. ドロップダウン リストから該当するオブジェクト タイプを選択します。
6. [調査] タブをクリックします。
このタブには以下のフィールドが含まれます。

調査を送信する

このチェック ボックスでは、調査をアクティブまたは非アクティブにできます。オンにした場合、選択したアクティビティ通知がトリガされたときに、調査が連絡先に送信されます。

調査の初期設定

検索アイコンを使用してデフォルトの調査を指定するか、テキスト ボックスに独自の調査を指定します。

通知方法

以下のいずれかの通知方法を選択します。

- 電子メール
- 通知
- ポケットベルの電子メール

調査メッセージ タイトル

調査のタイトルを入力します。

調査メッセージ本文

連絡先へのメッセージを入力します。連絡先が調査の通知を受け取る際に、メッセージの本文に自動的に URL が挿入されます。連絡先は、Web ブラウザからこの URL にアクセスして、調査フォームを確認して情報を記入できます。

7. アクティビティ通知を保存します。

選択したアクティビティ通知がトリガされると、アクティビティを開始した連絡先は調査通知を受け取ります。

調査のレポート

CA SDM では、Web クライアントの [管理] タブから、通常の方法で調査のレポートを作成できます。たとえば、[カスタム調査リスト] ウィンドウでは、[ファイル] メニューから [レポート] を選択し、[概要] または [詳細] のいずれかのレポートを選択します。また、各詳細ウィンドウで [フォームの印刷] を選択して、調査、質問、および回答のフォーム データを印刷することもできます。

また、CA SDM データベースに保守されている調査データに基づいて、独自のレポートを作成することもできます。

顧客満足度調査(個別)

顧客満足度調査（個別）では、CA SDM の管理者が、望ましい調査サンプルの対象者を選択し、これを指定の調査に一致させることができます。次に管理者は、指定時刻に調査が行われるように、ターゲットを絞ったリクエストを回答者に配信できます。この手順を行うことで、管理者はオープンな調査期間を設定できる柔軟性を確保すると同時に、リクエスト、変更要求、および案件に関連して、アクティビティ ベースの調査やカテゴリ ベースの調査を実行する機能も維持できます。

顧客満足度調査（個別）の目的は、調査を管理するメカニズムを提供することです。この機能は、一時的に監視する必要がある調査フォーム（たとえば、毎年短い期間に限って実行する調査や、長時間オフラインになる調査など）の場合に役立ちます。

重要: 多くの連絡先に調査を送信する場合は、`NX.env` で `1073741824` など、より高い制限に `NX_SURVEY_ILIMIT` のデフォルト値を設定します。

注: 顧客満足度調査（個別）の作成方法の詳細については、オンラインヘルプを参照してください。

Web サービス

Web サービスはデータ交換標準に準拠しており、以下のことができます。

- オペレーティング環境に関係なく、アプリケーションが HTTP を介してさまざまなサーバと通信できます。
- ほとんどのアプリケーションが CA 製品の機能にアクセスできます。
- Web サービスクライアントが、チケットの作成、アセットの更新、ナレッジベースの検索などさまざまな操作を実行できます。

注: 詳細については、「実装ガイド」の「Web サービスの管理」を参照してください。

第 8 章：ユーザ アカウントの設定

このセクションには、以下のトピックが含まれています。

[連絡先](#) (P. 373)

[連絡先の定義](#) (P. 373)

[グループ](#) (P. 375)

[連絡先タイプ](#) (P. 376)

[特殊処理タイプ](#) (P. 377)

連絡先

優れたサービス デスクを構築するには、システムにアクセスするユーザを定義することが重要です。CA SDM では、ユーザを連絡先と呼びます。連絡先をセットアップ、管理するために、以下のようなタスクを実行できます。

- 連絡先を手動でセットアップします。
- 責任の範囲を定義したグループに連絡先を分類します。
- CA SDM の連絡先をシステムの使用方法に応じて論理的なグループに分類し、このグループを連絡先タイプとして設定します。
- CA SDM 連絡先レコードに LDAP ユーザ情報をインポートします。
- 連絡先に役割を割り当て、アクセス可能なシステム機能を定義します。
- 連絡先に、VIP（Very Important Person）のような特殊処理タイプを割り当てます。

連絡先の定義

CA SDM を使用するユーザはすべて、連絡先として定義する必要があります。ユーザの連絡先レコードでは、システムが必要とする以下のようなユーザ情報を定義します。

基本的な識別情報

ユーザ名や連絡先タイプなど、基本的な識別情報を定義します。連絡先を選択するとき、またはほかのコンテキストで連絡先情報を入力するとき、連絡先の名前は主要な識別情報として使用されます。

ログイン

ユーザ ID などのログイン情報を定義します。場合によっては、ログイン時にパスワードとして検証される PIN フィールドも定義します。ユーザ ID は、ユーザに割り当てるアクセス タイプの判断や認証を行うために、連絡先テーブル内のユーザを識別します。セキュリティの設定によっては、連絡先 ID などのほかのフィールドを PIN フィールドとして指定できます。また、ユーザはこれをログイン時のパスワードとして使用できます。

セキュリティ

システムのセキュリティ設定に応じて、連絡先レコードに割り当てられたアクセス タイプまたは初期設定のアクセス タイプを定義します。また、ユーザのアクセス タイプは、LDAP ディレクトリ グループのメンバシップに基づいて割り当てることもできます。

システムに対してユーザを認証する方法、ユーザが表示できる Web インターフェース、ユーザがアクセスできる製品機能など、セキュリティのあらゆる側面がユーザのアクセス タイプによって決定されます。

セキュリティ管理は、Web インターフェースの機能です。

サービス タイプ

ユーザが受けるサービスのレベルを指定します。連絡先のサービス タイプによって、ユーザが受けるサービスのレベルが定義されます。サービス レベル アグリーメント (SLA) は、CA SDM のカスタマと交渉して決定します。サービス タイプは、CA SDM が SLA を実装するためのメカニズムとして動作します。サービス タイプとユーザの連絡先レコードを関連付けると、影響を受けるエンドユーザとしてそのユーザを指定したチケットを作成するときに、チケットのサービス タイプのレベルを少なくとも連絡先のサービス タイプと同じレベルにできます。

サービスタイプの使用による SLA の設定は、管理者が Web インターフェースを使用して行います。

自動割り当て

ワーク シフトや使用可能状況（アナリストの連絡先タイプのみで使用）などの自動割り当て情報を定義します。自動割り当てに使用できるかどうかを判断できるように、アナリストの連絡先をセットアップできます。自動割り当てが有効なのは、リクエストの場合だけです。自動割り当ては、リクエスト領域定義の一部として定義します。また、この定義は、アナリストが所属しているグループにもリンクします。

ユーザ通知メッセージの送信方法

連絡先の通知情報を定義します。これには、以下のものが含まれます。

- 通知に使用されるさまざまな電子メールアドレスおよび電話番号
- 各種の緊急度レベルを持つ通知に使用されるメソッド
- 通知が受信されるときワーク シフト

通知の遅延の計算では、連絡先のタイムゾーンが考慮されます。連絡先のタイムゾーンが設定されていない場合は、代わりにサーバのタイムゾーンが使用されます。サーバのタイムゾーンを使用すると、通知がワーク シフト設定の範囲外とみなされる時間帯に送信されることがあります。

組織情報（ロケーション、組織、部門など）では、所属する組織に基づいて連絡先をグループ化します。たとえば、連絡先とロケーションを関連付けると、連絡先は物理的な所在地にリンクされて、自動割り当ての決定に役立ちます。組織には、サービス タイプを割り当てることができます。この設定を行うと、個々の連絡先ではなく、組織で SLA を簡単に管理できます。

ユーザが所属するグループ

連絡先は、サービス デスク内で特定の範囲の責任を担うグループに分類できます。連絡先のセットアップと定義は、**Web** インターフェースを使用して実行できます。

グループ

グループは、共通の責任範囲を分担する連絡先の集合体です。CA SDM では、定義済みのグループ連絡先タイプを使用してグループを実装します。この設定により、グループは特別なタイプの連絡先になります。グループの基本情報は連絡先と同じですが、グループはリクエストを自動的に割り当てるための重要な要素でもあります。リクエスト領域、ロケーション、およびワーク シフトを、グループに関連付けることができます。この属性は、グループ内の連絡先がリクエストの自動割り当てを受ける状況と時間を決定するために使用されます。

注: グループの定義については、オンライン ヘルプを参照してください。

連絡先タイプ

連絡先タイプは、CA SDM のユーザをシステムの使用方法で論理的なグループに分類するために使用します。たとえば、システムで提供される定義済みの連絡先タイプには、アナリスト、カスタマ、グループなどがあります。これらの定義済みの連絡先タイプはほとんどの CA SDM 実装の要件を満たしていますが、必要に応じて、定義済みの連絡先タイプを変更したり、新しい連絡先タイプを作成したりすることができます。ユーザを連絡先として定義するときに、連絡先タイプと各ユーザを関連付けることができます。

注: 連絡先タイプの定義の詳細については、オンライン ヘルプを参照してください。

連絡先タイプに基づく動作の決定

連絡先タイプは、状況に応じて表示する連絡先（および与える権限）を決定します。たとえば、リクエストまたは案件など、チケットのタイプを手動で割り当てる場合、担当者指定するフィールドにはアナリストの連絡先タイプを持つ担当者を指定する必要があります。このフィールドに表示される選択リストから連絡先を選択する場合は、アナリストのタイプを持つ連絡先だけが選択リストに表示されます。異なるタイプの連絡先を入力しても、アナリストの検索画面が表示されるだけです。

注: 連絡先タイプの重要な機能は、定義済みのグループ連絡先タイプを介して、連絡先のグループで実装されます。

連絡先タイプに基づく通知のセットアップ

通知は連絡先タイプに基づいてセットアップでき、特定タイプのすべての連絡先に通知メッセージを送信できます。

関連項目:

[通知](#) (P. 219)

連絡先タイプに基づく連絡先の選択

連絡先タイプに基づいて、さまざまなコンテキストでユーザを選択できます。たとえば、連絡先を表示するほとんどのリストと選択ウィンドウには検索フィールドがあり、検索基準として連絡先タイプを選択できます。

特殊処理タイプ

特に注意を必要とする人物の連絡先を示す特殊処理タイプを定義できます。**CA SDM** の特殊処理タイプを使用できます。また、独自のタイプを作成することもできます。特に注意を必要とする人物である影響を受けるエンドユーザを特定するチケットを表示して検索することができます。たとえば、アナリストはスコアボードで **V.I.P.** フォルダを参照し、影響を受けるエンドユーザとして **VIP** が指定されているチケットを特定することができます。

特殊処理タイプが特定できる連絡先の例を以下に示します。

- 経営者のような重要人物（VIP）
- サポート更新処理中の顧客
- 特殊な処理や機器を必要とする障害を持つ顧客
- 訪問者
- システムリソースを誤用または悪用している疑いのある連絡先

1つの連絡先に1つ以上の特殊処理タイプが割り当てられる場合、[影響を受けるエンドユーザ] フィールド内の、その連絡先を特定するチケットには警告バナーかアイコンまたは両方が表示されます。チケットフィールドと特殊処理タイプを使用することで、チケットを追跡し、関連性はあるものの別々と思われる2つの連絡先タイプを区別できます。たとえば、VIP（影響を受けるエンドユーザ）には、代わりに動作するアシスタント（依頼者）がいます。[影響を受けるエンドユーザ] がVIP特殊処理タイプに割り当てられた連絡先である場合、アナリストはより正確にチケットに優先することができます。

関連項目:

[特殊処理連絡先を設定する方法](#) (P. 378)

[特殊処理タイプに対する連絡先の関連付け](#) (P. 379)

[LDAP ディレクトリ データ](#) (P. 380)

特殊処理連絡先を設定する方法

特殊処理連絡先を設定するには、以下の手順を実行します。

1. 特殊処理タイプを作成します。
2. [任意の数の特殊処理タイプに連絡先を関連付けます](#) (P. 379)。同様に、特殊処理タイプは多数の連絡先を持つことができます。

1 つ以上の特殊処理タイプに関連付けられた連絡先は、連絡先の詳細フォームおよびクイック プロファイル ブラウザ (各ページの上にあるバナーを使用して) で見分けられます。このバナーは、連絡先に割り当てられた各特殊処理タイプのアラートアイコンおよびアラートテキストを表示します。

また、影響を受けるエンドユーザとして識別されるチケットは、以下のように表示されます。

- アラートアイコンとアラートテキストは、チケットの詳細フォームの一番上のバナーに表示されます。
- アラートアイコンはチケット リスト内に表示されます。
- スコアボードには各チケット タイプの V.I.P. フォルダ およびサブフォルダが含まれます。[V.I.P.] VIP 特殊処理連絡先である影響を受けたエンドユーザのチケットが含まれます。

注: V.I.P. スコアボードフォルダは、アナリスト役割用に表示されます。

詳細情報

[特殊処理タイプに対する連絡先の関連付け](#) (P. 379)

[LDAP ディレクトリ データ](#) (P. 380)

特殊処理タイプに対する連絡先の関連付け

視覚障害のあるユーザ、セキュリティ上のリスクをもたらす連絡先など、特別な要件を持つエンドユーザに影響するチケットをアナリストに警告するため、連絡先に特殊処理タイプを割り当てることができます。

特殊処理タイプに対して連絡先を関連付けるには、以下の手順に従います。

1. [連絡先の詳細] ページで、[特殊処理] タブを選択します。
[関連特殊処理リスト] タブは、連絡先に関連付けられている特殊処理タイプをリストにします。
2. [連絡先の更新] の [特殊処理] ボタンをクリックします。
[検索フィルタ] が表示されます。
3. 連絡先に関連付ける特殊処理タイプを検索します。
[特殊処理の更新] ページが表示されます。
4. 左の列から 1 つ以上の処理タイプを選択し、移動ボタン (>>) を使用してタイプを右の列に移動します。 [OK] をクリックします。

注: 移動ボタン (<<) を使用してタイプを右の列から左の列に移動すると、連絡先から関連付けを削除することができます。 検索アイコンをクリックして、目的の値を検索できます。

連絡先は処理タイプに関連付けられています。

チケットが [影響を受けるエンドユーザ] フィールドで連絡先を指定すると、CA SDM は、処理するタイプに応じて以下のいずれかを表示します。

- アラート バナーは、チケットで影響を受けるエンドユーザの [連絡先の詳細] に表示されます。
- アラート テキストは、チケットの詳細ページの一番上、およびクイック プロファイル内にバナーとして表示されます。
- チケット リストは、連絡先行をハイライトしてアラート フラグを表示します。
- V.I.P. フォルダは、アナリスト役割のスコアボードに表示されます。フォルダには、VIP 特殊処理タイプを持つ連絡先（影響を受けるエンドユーザ）に関連付けられているすべてのチケットが含まれています。

LDAP ディレクトリ データ

Lightweight Directory Access Protocol (LDAP) は、TCP/IP ネットワークを介してディレクトリ サービスのクエリや変更を行うためのネットワーク通信プロトコルです。LDAP ディレクトリはツリー構造をしており、ネットワーク上でユーザ、グループ、コンピュータ、プリンタなどのエンティティを管理するためのエントリが含まれています。

CA SDM は、LDAP ディレクトリにアクセスするように設定できます。この設定により、いくつかの方法で LDAP データを使用できるようになります。

- LDAP ユーザ レコードと連絡先を同期します。同期は以下の方法で行うことができます。
 - **ログイン時** - ユーザが製品にログインしたときに、そのユーザの LDAP レコードが存在し、対応する連絡先レコードが存在しない場合、LDAP 情報に基づいて連絡先レコードが自動的に作成されます。
 - **新規連絡先** - 手動で連絡先レコードを作成する場合、LDAP レコードを選択し、新しい連絡先レコードの対応するフィールドをその属性値にマージできます。
 - **バッチ更新** - バッチ ジョブを実行して、対応する LDAP レコードの情報をを使用した、連絡先レコードのインポート処理および更新処理を自動化できます。

注: LDAP の同期は一方方向です。LDAP データは連絡先の作成および更新に使用できますが、製品は LDAP ディレクトリの更新をサポートしていません。

- LDAP グループ メンバシップに基づいて CA SDM アクセス タイプを割り当てます。
- CA SDM 認証を実行する別の方法を実装します。

ldap_virtb コンポーネントは、オペレーティング システムのタイプにかかわらず、CA SDM の設定に応じて、以下のサーバ上で LDAP 統合機能を提供します。

- 標準：プライマリまたはセカンダリ サーバ。
- 高可用性：バックグラウンドサーバまたはアプリケーション サーバ。

注：ldap_virtb コンポーネントの詳細については、「[実装ガイド](#)」を参照してください。\$NX_ROOT/bopcfg/majic/ldap.maj ファイルは、LDAP 属性と連絡先レコード属性の間のマッピングを指定します。

重要：CA SDM で LDAP データを検索、表示、インポートするには、LDAP レコードの姓フィールドにエントリがある必要があります。

重要：CA SDM ではページング検索がサポートされており、LDAP ディレクトリの全レコードを検索できます。また、ページング検索では、任意の数の LDAP レコードから新しい連絡先レコードをインポートしたり、既存の連絡先レコードと同期したりすることができます。ただし、これらの機能には制限があります。SunOne Directory Server または Novell eDirectory の LDAP サーバはページング検索をサポートしていません。そのため、Sun Java System Directory Server または Novell eDirectory を使用している場合、これらの機能は使用できません。この場合実行できるのは、検索、インポート、および NX_LDAP_MAX_FETCH で指定した数の LDAP レコードの同期のみになります。ページング検索の詳細については、「[NX.env ファイル \(P. 398\)](#)」を参照してください。

LDAP オプションの設定

LDAP ディレクトリ データにアクセスするように CA SDM を設定できます。

LDAP ディレクトリ データにアクセスするように CA SDM を設定するには、以下の手順に従います。

1. Web インターフェースのオプション マネージャを使用して、LDAP オプションを手動でインストールします。

注: 基本的な LDAP 統合に必要なオプションは、以下の表の「説明」列に必須と記述されています。オプションと記述されているオプションは、必須オプションをすべてインストールしている場合にのみ追加できる機能です。これらのオプションをインストールするときに指定する値は、\$NX_ROOT/NX.env ファイルに書き込まれます。LDAP オプションとそのインストール手順の詳細については、オンライン ヘルプを参照してください。

2. CA SDM サービスを再起動します。

変更内容が適用されます。

オプション	デフォルト値	説明
default_ldap_tenant		マルチテナンシー インストールでは必須。LDAP からインポートした連絡先のデフォルトのテナント割り当てを指定します。 [オプション値] フィールドを設定するときは、テナントの UUID を使用する必要があります。 注: テナントの UUID は、データベース クエリから取得できます。たとえば、「SELECT * FROM ca_tenant」のようになります。
ldap_enable	○	必須 CA SDM で LDAP 統合を有効にします。
ldap_host		必須 LDAP データベース サーバのホスト名または IP アドレスを指定します。
ldap_port	389	必須 LDAP サーバのポート番号を指定します。

オプション	デフォルト値	説明
ldap_dn		必須 LDAP サーバのログオン識別名を指定します。 例: CN=Joe、CN=Users、DC=KLAND、DC=AD、DC=com LDAP サーバが匿名バインドをサポートする場合、この値は空でもかまいません。
ldap_pwd		必須 LDAP サーバのログオン識別名のパスワードを指定します。 LDAP サーバが匿名バインドをサポートする場合、この値は空でもかまいません。
ldap_search_base		必須 LDAP スキーマ ツリーの検索の開始ポイントを指定します。 (UNIX) 開始するコンテナを指定する必要があります。以下に例を示します。 CN=Users、DC=KLAND、DC=AD、DC=com (Windows) コンテナを指定する必要はありません。スキーマ ツリーの一番上から開始されます。以下に例を示します。 DC=KLAND、DC=AD、DC=com
ldap_filter_prefix	(&(objectClass=user)	LDAP ユーザ検索時に自動生成されるフィルタに適用するプレフィックスを指定します。 注: この変数は、ldap_user_object_class option に置き換えられています。この変数はオプションマネージャでは使用できませんが、NX.env ファイル内で手動で設定できます。
ldap_filter_suffix	)	LDAP ユーザ検索時に自動生成されるフィルタに適用するサフィックスを指定します。 注: この変数は、ldap_user_object_class option に置き換えられています。この変数はオプションマネージャでは使用できませんが、NX.env ファイル内で手動で設定できます。
ldap_user_object_class	person	必須 LDAP ユーザ検索時に自動生成されるフィルタに適用する LDAP objectClass 属性の値を指定します。

オプション	デフォルト値	説明
ldap_enable_group	○	オプション。LDAP グループ メンバシップに基づいた CA SDM アクセス タイプの割り当てを有効にします。
ldap_group_object_class	group	ldap_enable_group がインストールされている場合のみ必須。グループ検索時に自動生成されるフィルタに適用するオブジェクト名を指定します。
ldap_group_filter_prefix	(&(objectClass=group)	LDAP グループ検索時に自動生成されるフィルタに適用するプレフィックスを指定します。 注: この変数は、ldap_group_object_class に置き換えられています。この変数はオプション マネージャでは使用できませんが、NX.env ファイル内で手動で設定できます。
ldap_group_filter_suffix	)	LDAP グループ検索時に自動生成されるフィルタに適用するサフィックスを指定します。 注: この変数は、ldap_group_object_class に置き換えられています。この変数はオプション マネージャでは使用できませんが、NX.env ファイル内で手動で設定できます。
ldap_enable_auto	○	オプション。LDAP データからの連絡先レコードの自動生成を有効にします。
ldap_sync_on_null	○	オプション。対応する LDAP ユーザ属性に NULL 値が設定されている場合、既存の CA SDM 連絡先の属性は NULL データで上書きされます。
ldap_service_type	Active Directory	オプション。このオプションは、CA SDM オペレーティング環境が Windows であり、かつ、LDAP ディレクトリが Active Directory でない（たとえば、eTrust や Novell）場合に使用します。 注: UNIX オペレーティング環境では、このオプションがインストールされていない場合にのみ、「Non AD」機能が使用されます。このオプションがインストールされている場合、サービス タイプは Active Directory に設定されます。

オプション	デフォルト値	説明
ldap_enable_tls	×	オプション。LDAP 処理中にトランスポート レイヤセキュリティ (TLS) を有効にするかどうかを指定します。

LDAP 統合の確認

必要な LDAP オプションをインストールした後、CA SDM ユーザはすべての連絡先属性フィールドに値を手動で入力する必要はありません。状況に応じて LDAP データをインポートできます。

LDAP 統合が正しく設定されていることを確認するには、Web インターフェースを使用して以下の手順に従います。問題が発生した場合は、「[トラブルシューティング \(P. 397\)](#)」の章を参照してください。

LDAP レコードを検索およびインポートできることを確認する方法

1. [Service Desk] タブで [ファイル] - [LDAP からの新規連絡先] を選択します。

[LDAP ディレクトリの検索] ウィンドウが表示されます。

2. フィルタ条件を指定し、[検索] をクリックします。たとえば、[姓] フィールドに「b%」と入力すると、姓が「B」で始まる LDAP ユーザ エントリのリストを取得できます。

注: LDAP ディレクトリに何千件もエントリがあり、フィルタで検索対象を絞り込まない場合、リクエストはすべての LDAP ユーザ レコードを取得しようとします。この場合、リクエストがタイムアウトして、レコードが 1 件も返されない可能性があります。

フィルタ条件に一致する検索結果が表示されます。

3. エントリを選択します。

インポートした LDAP 情報が入力された状態で、[連絡先の新規作成] ウィンドウが表示されます。

4. [保存] をクリックします。

連絡先レコードが作成されます。

LDAP データを使用して連絡先を更新できることを確認する方法

注: この手順を実行する前に、前の手順で使用したエントリの属性値を任意の LDAP 編集ツールで変更できるかどうかを確認することをお勧めします。連絡先が最新の LDAP データで更新されることを確認できます。

1. [Service Desk] タブで [検索] - [連絡先] を選択します。
[連絡先の検索] ウィンドウが表示されます。
2. フィルタ条件を指定して、対応する LDAP ユーザ エントリを持つ連絡先を検索します。たとえば、前の手順で作成した連絡先を検索します。
フィルタ条件に一致する検索結果が表示されます。
3. LDAP データで更新する連絡先を選択します。
CA SDM 連絡先情報が入力された状態で、[連絡先情報] ページが表示されます。
4. [編集] をクリックします。
[Contact Update] ページが表示されます。
5. [LDAP のマージ] をクリックします。
[LDAP エントリ リスト] ページには、選択された CA SDM 連絡先に一致するすべての LDAP ユーザ エントリのリストが表示されます。
他のエントリの LDAP ディレクトリを検索するには、[フィルタの表示] をクリックし、フィルタ条件を指定して、[検索] をクリックします。
注: LDAP ディレクトリに何千件もエントリがあり、フィルタで検索対象を絞り込まない場合、リクエストはすべての LDAP ユーザ レコードを取得しようとしています。この場合、リクエストがタイムアウトして、レコードが 1 件も返されない可能性があります。
6. 興味のある LDAP エントリをクリックします。
[LDAP の詳細] ページには、選択したエントリの属性値が表示されます。選択したエントリが更新する連絡先のものであることを確認し、[ウィンドウを閉じる] をクリックします。

7. [LDAP エントリ リスト] ページで、更新する連絡先に最も一致したエントリを右クリックし、[連絡先へのマージ] を選択します。

現在の LDAP 属性値が入力された状態で、[Contact Update] ウィンドウが再び表示されます。連絡先を作成または最後に更新した後で LDAP データが変更されている場合、その変更は連絡先の属性フィールドに反映されます。

注: ldap_sync_on_null オプションがインストールされている場合、LDAP エントリの属性フィールドが NULL 値で、対応する連絡先属性に値が指定されていると、連絡先データを保存したときに連絡先レコードの値は NULL 値で上書きされます。

8. [Contact Update] ページで [保存] をクリックします。

対応する LDAP データで連絡先が更新されます。

連絡先の自動作成

新規ユーザが CA SDM にログインする場合は常に、対応する LDAP ユーザレコードから連絡先を自動的に作成するよう CA SDM を設定できます。

この機能を有効にするには、必須のすべての LDAP オプションおよび ldap_enable_auto オプションをインストールします。

以下のように、連絡先レコードが自動的に作成されます。

1. CA SDM にログインするユーザの連絡先レコードがなくてもログイン名が LDAP レコードに存在すれば、LDAP データが自動的にインポートされ、連絡先レコードが作成されます。
2. 自動的に作成された連絡先レコードは、初期設定のアクセス タイプのセキュリティ設定を継承します。
3. 作成された連絡先には、アクセス タイプを明示的に割り当てることができます。また、アクセス タイプは、ユーザの LDAP グループのメンバシップに基づいて割り当てることができます。

このプロセスは完全にバックグラウンドで実行され、ユーザにとってはほかのログインセッションと同じように見えます。

LDAP グループに基づいたアクセス タイプの割り当て

LDAP グループのメンバシップに基づいて連絡先にアクセス タイプの値を自動的に割り当てるよう、CA SDM を設定できます。アクセス タイプの自動割り当てが有効で、連絡先の作成に使用した LDAP ユーザ レコードが属する LDAP グループに CA SDM アクセス タイプのいずれかが関連付けられている場合、そのアクセス タイプが自動的に連絡先に割り当てられます。それ以外の場合、連絡先は初期設定のアクセス タイプを継承します。

アクセス タイプの自動割り当てを有効にするには、`ldap_enable_group` オプションと `ldap_group_object_class` オプションをインストールする必要があります。

注: 必要なオプションのインストール、および LDAP グループとアクセス タイプの関連付けの詳細については、オンライン ヘルプを参照してください。

LDAP データを使用した連絡先のバッチ インポート

`pdm_ldap_import` コマンドラインユーティリティを実行すると、LDAP データを使用してバッチ モードで CA SDM 連絡先を作成できます。

注: 既存の連絡先が対応する LDAP エントリと同期されていない場合、`pdm_ldap_import` を実行すると、連絡先が作成されるだけでなく、既存の連絡先が更新されます。`pdm_ldap_sync` バッチ処理を使用すると、既存の連絡先を更新できますが、新しい連絡先は作成できません。

`pdm_ldap_import` 構文を以下に示します。

```
pdm_ldap_import -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]  
-l "ldap_where_clause"
```

検索する LDAP レコードの `userid` を指定します。置き換える変数は「?」文字で示します。たとえば、`userid = ?` とします。デフォルト値は `userid = ?` です。この特別な事例では、`id` は連絡先属性 `ldap_dn` にマップされます。

注: `ldap.maj` ファイルで定義されているキーワードを使用してください。`memberOf = 'group_dn'` の構文を使用して検索することもできます。

`-c "contact_where_clause"`

(省略可) 連絡先レコードがすでに存在するかどうかを判断する方法を指定します。連絡先レコードが存在しない場合、新しい連絡先レコードが挿入されます。連絡先レコードが存在しているが、最新のLDAP データと同期されていない場合、連絡先レコードが更新されます。

`-u "userid"`

(省略可) `pdm_ldap_import` プログラムが実行されるログイン名を指定します。

注: `pdm_ldap_import` でワイルドカードを使用すると、複数のレコードを指定できます。

例: LDAP データを使用したバッチ インポート

以下の例では、userid `jsmith11` の 1 つの LDAP レコードがインポートされます。

```
pdm_ldap_import -l "userid = 'jsmith11'"
```

以下の例では、文字 `C` から始まる `userid` を持つ LDAP レコードがすべてインポートされます。

```
pdm_ldap_import -l "userid = 'c%'"
```

以下の例では、ディレクトリ内のすべての LDAP ユーザレコードがインポートされます。

```
pdm_ldap_import -l "userid = '%'"
```

関連項目:

[LDAP データを使用した連絡先のバッチ更新 \(P. 392\)](#)

日付と時間による連絡先のバッチ インポート

`pdm_ldap_import` ユーティリティは、特定の日付と時間の前または後に作成された LDAP レコードをインポートするように設定できます。この機能を有効にするには、以下の内容を含む `ldap.mod` ファイルを作成します。

```
OBJECT ldap {  
  ATTRIBUTES LDAP_Entry {  
    whenCreated whenCreated STRING ;  
  };  
};
```

このコードは、LDAP オブジェクトに **whenCreated** 属性を追加します。

whenCreated 属性を使用して、レコードをフィルタするためのルールは以下のとおりです。

- **>=** 演算子または **<=** 演算子のみを使用する。
- **Z** を含め、日付/時間の値の文字をすべて指定する。明示的に指定しない部分（時間など）にはすべて **0** を指定します。
- 日付/時間をフィルタの最初に指定する。文字列の先頭に **0** は使用しません。
- 先頭に世紀を指定しない。たとえば、**2008** 年を指定するには、**08** を使用します。

注：日付/時間の値は一重引用符で囲む必要があります。

例: **whenCreated** 属性を使用した LDAP エントリのインポート

以下の例では、**2008** 年 **3** 月 **11** 日以降に作成された LDAP エントリを **whenCreated** 属性を使用してインポートします。

```
Pdm_ldap_import -l "whenCreated >= '080312000000Z'"
```

例: **whenCreated** 属性を使用した LDAP レコードの検索

以下の例では、**2008** 年 **3** 月 **11** 日以降に作成された LDAP レコードを、**pdm_ldap_test** で **whenCreated** 属性を使用して検索します。

```
pdm_ldap_test.exe -f "whenCreated>=080312000000Z" -a whenCreated
Starting ldap_test.exe...
LDAP Directory Type : active directory
Service Desk Platform : windows
Search Base : DC=kirklandsd,DC=ca,DC=com
Search Filter : (&(objectClass=person)(whenCreated>=080312000000Z))
Administrator Username :
CN=Administrator,CN=Users,DC=kirklandsd,DC=ca,DC=com
Administrator Password : *****
LDAP Host : gecko.kirklandsd.ca.com
LDAP Port : 389
LDAP API Version : 3
DN: CN=aixmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
    whenCreated(17)(0): 20080312035327.0Z
DN: CN=hpmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
    whenCreated(17)(0): 20080312035425.0Z
DN: CN=sunmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
    whenCreated(17)(0): 20080312035726.0Z
3 Total LDAP records found...
```

概要データおよびログ データのバッチ インポート

`pdm_ldap_import` コマンドは、各実行のすべてのアクティビティの詳細ログを保守します。`ldap_logging.0-n` ログ ファイルは、`$NX_ROOT/log` ディレクトリに保存されます。

以下は、コマンドラインで `pdm_ldap_import` が返す概要データの例です。

```
pdm_ldap_import Starting...
pdm_ldap_import Summary:  Processed(21) Updated(1) No Matches(7) New Contacts(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_import Complete...
```

以下の表で、概要データについて説明します。

ステータス	カウント	説明
Processed (処理済み)	21	対応する LDAP エントリを持つ CA SDM 連絡先の数。
Updated (更新済み)	1	対応する LDAP エントリに別の情報が含まれていたために更新された連絡先レコードの数。
No Matches (一致なし)	7	対応する LDAP エントリを持たない CA SDM 連絡先レコードの数。
New Contacts (新規連絡先)	11	対応する LDAP エントリに基づいて作成された、新しい連絡先レコードの数。
Multiple Matches (複数一致)	0	<code>ldap_search_base</code> オプションによって定義されたとおり、複数の連絡先レコードが一致する LDAP エントリの数。
Empty Filter (空のフィルタ)	2	有効な検索フィルタの生成に使用できなかった LDAP エントリの数。
Errors (エラー)	0	処理中にエラーが発生した LDAP エントリの数。たとえば、CA SDM によって必要とされるフィールド ([姓] など) に値が含まれていない LDAP レコードは、エラーとして数えられてインポートできません。

LDAP データを使用した連絡先のバッチ更新

LDAP データを使用してバッチ モードで連絡先レコードを更新するには、`pdm_ldap_sync` ユーティリティを実行します。

重要: このユーティリティは、**CA SDM** で定義されている **LDAP** 連絡先の既存のテナントを上書きします。テナント値をそのまま残したい場合は、**NX_RETAIN_TENANT_VALUE** 変数を手動で追加することによって **NX.env** を変更し、「yes」に設定する必要があります。この変数が「no」に設定されていたり、なかったり、または正しく設定されていない場合、ユーティリティはテナント情報を上書きします。

注: `pdm_ldap_sync` ユーティリティは、既存の連絡先を対応する **LDAP** エントリと同期しますが、連絡先は作成しません。連絡先を作成するには、`pdm_ldap_import` バッチ プロセスを使用します。

`pdm_ldap_sync` の構文は以下のとおりです。

```
pdm_ldap_sync -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]  
-l "ldap_where_clause"
```

一致する **LDAP** レコードの検索方法を決定します。置き換える変数は「？」文字で示します。たとえば、`userid = ?` です。初期設定値は `id = ?` です。この特別な事例では、`id` は連絡先属性 `ldap_dn` にマップされます。

```
-c "contact_where_clause"
```

(オプション) 一致する **LDAP** レコードを検索するときにどの連絡先を使用するかを決定します。

デフォルト: `"ldap_dn IS NOT NULL"`

```
-u "userid"
```

(オプション) `pdm_ldap_sync` を実行するユーザ ID を指定します。

注: 複数のレコードを指定するには、`pdm_ldap_sync` でワイルドカードを使用します。

例:

次の例では、対応する LDAP レコードがある連絡先レコードのベースラインを確立しています。

```
pdm_ldap_sync -l "userid = ?" -c ""
```

次の例では、デフォルトのパラメータを使用して、LDAP の識別名がある連絡先をすべて更新しています。

```
pdm_ldap_sync
```

次の例では、単一の連絡先を更新しています。

```
pdm_ldap_sync -l "userid = ?" -c "userid = 'jsmith11'"
```

関連項目:

[LDAP データを使用した連絡先のバッチ インポート \(P. 388\)](#)

概要データとログ データのバッチ更新

pdm_ldap_sync コマンドは、実行されるたびにすべてのアクティビティの詳細なログを保守します。ldap_logging.0-n ファイルは、\$NX_ROOT/log ディレクトリに保存されます。

以下は、コマンドラインで pdm_ldap_sync が返す概要データの例です。

```
pdm_ldap_sync Starting...
pdm_ldap_sync Summary:  Processed(21) Updated(1) No Matches(7) No Changes(11)
Multiple Matches(0) Empty Filter(2) Errors(0)
pdm_ldap_sync Complete...
```

この概要データの説明は以下の表のとおりです。

ステータス	カウント	説明
Processed（処理済み）	21	対応する LDAP エントリを持つ CA SDM 連絡先の数。
Updated（更新済み）	1	対応する CA SDM 連絡先レコードと情報が異なる LDAP エントリの数。
No Matches（一致なし）	7	対応する LDAP エントリを持たない CA SDM 連絡先レコードの数。

ステータス	カウント	説明
No Changes（変更なし）	11	対応する CA SDM 連絡先レコードと情報が同じ LDAP エントリの数。
Multiple Matches（複数一致）	0	一致する連絡先レコードが CA SDM 内に複数ある LDAP エントリの数。この値は ldap_search_base オプションで定義します。
Empty Filter（空のフィルタ）	2	有効な検索フィルタの生成に使用できなかった LDAP エントリの数。
Errors（エラー）	0	処理中にエラーが発生した LDAP エントリの数。

LDAP 認証

CA SDM にログインするユーザを認証するために、LDAP を使用できます。LDAP 認証を使用できるのは、CA SDM に CA EEM 認証コンポーネントが統合されている場合です。このコンポーネントによって、ホストオペレーティングシステムが実行する初期設定の検証プロセスが置き換えられます。外部 LDAP ディレクトリを使用するように CA EEM が設定され、アクセスタイプレコードでユーザの検証タイプとして OS 認証が選択されている場合にのみ、LDAP 認証は適用されます。

CA EEM 機能をアクティブにすると、ログインリクエストは CA EEM サーバでチェックされます。ログインリクエストが認められるのは、以下の状況が発生した場合のみです。

- 指定したユーザ ID が CA SDM の連絡先レコードと一致する場合
- ユーザ ID が CA EEM のユーザプロフィールと一致する場合
- ユーザ ID とパスワードの組み合わせが、CA EEM によって正常に検証された場合

注: CA EEM を使用した認証、および認証モジュールを外部サーバに移動する方法の詳細については、「[実装ガイド](#)」を参照してください。アクセスタイプのセットアップの詳細については、オンラインヘルプを参照してください。

トランスポートレイヤ セキュリティ

CA SDM は、LDAP を処理するときにトランスポートレイヤセキュリティ (TLS) を使用するよう設定できます。安全な通信プロトコルである TLS は、Secure Socket Layer (SSL v3) セキュリティの後継です。TLS を有効にするには、`ldap_enable_tls` オプションをインストールします。

重要: この機能を有効にすると、CA SDM と LDAP サーバの間の通信がすべて暗号化されます。この機能を無効にすると、データ通信 (LDAP サーバへのアクセスに使用する管理用ログインおよびパスワードを含む) はすべてクリアテキストで送信されます。

注: TLS の設定の詳細については、LDAP サーバおよびオペレーティングシステムのドキュメントを参照してください。`ldap_enable_tls` オプションの使用方法については、オンラインヘルプを参照してください。

属性マッピング

CA SDM 連絡先レコードの属性値は、`$NX_ROOT/bopcfg/majic/ldap.maj` ファイルに指定した属性マッピング定義に基づいて LDAP ユーザの属性値と同期されます。

`ldap.maj` からの以下の抜粋は、マッピングを示しています。左の列 (id) の属性名は CA SDM 連絡先属性名です。真ん中の列 (`distinguishedName`) は対応する LDAP 属性名です。

<code>id</code>	<code>distinguishedName</code>	<code>STRING 512;</code>
<code>last_name</code>	<code>sn,pzLastName</code>	<code>STRING ;</code>
<code>first_name</code>	<code>givenName,pzFirstName</code>	<code>STRING ;</code>
<code>middle_name</code>	<code>initials,pzMiddleName</code>	<code>STRING ;</code>
<code>userid</code>	<code>uid,sAMAccountName,pzUserName</code>	<code>STRING ;</code>
<code>phone_number</code>	<code>telephoneNumber,pzWorkPhoneNumber</code>	<code>STRING ;</code>

SREL (単一関連付け、または別のデータベース テーブル内の外部キー) が CA SDM に存在する場合、連絡先属性値は対応する LDAP 値と同期されます。SREL が存在しない場合、LDAP 同期処理時に自動的に作成されません。

注: デフォルトでは、属性マッピングは Microsoft Active Directory LDAP スキーマに合わせて設定されます。必要な場合は、`mod` ファイルを使用してマッピングを変更できます。

属性マッピングを変更する方法

デフォルトの属性マッピングは変更することが可能です。

デフォルトの属性マッピングを変更するには、以下の手順を実行します。

1. `$NX_ROOT/site/mods/majic` に移動して、`mod` ファイルを開きます。
2. 以下のとおりに、`mod` ファイルで **MODIFY** ステートメントを使用します。
 - **MODIFY** ステートメントは、必ずファイルの先頭に入力する必要があります。
 - **MODIFY** ステートメントに続いて、以下の例に示した構文を使用して、`ldap.maj` ファイルにない追加のフィールドを指定する必要があります。
 - 属性名にハイフン文字が含まれているフィールドを定義する場合は、その属性名を一重引用符で囲む必要があります。引用符で囲まないと、`mod` ファイルを作成するときに、構文エラーが発生して属性が失敗します。たとえば、以下の属性名を一重引用符で囲む必要があります。

```
c_nx_string1 'swsd-secret-question' STRING ;
```

3. `mod` ファイルを保存して閉じます。
4. CA SDM サービスを再起動します。

重要: 構文または大文字と小文字に相違があると、Web エンジンを開始しません。

変更は適用されます。

例: MODIFY ステートメントの使用

以下は、2 つの既存のフィールドを変更して、新しいフィールドを追加する方法を示した例です。

```
//  
// CA SDM userid 属性を ADAM Userid にマップする  
//  
MODIFY ldap userid cn ;  
MODIFY ldap middle_name middleName ;  
OBJECT ldap LDAP {  
  ATTRIBUTES LDAP_Entry{  
    contact_num employeeNumber STRING ;  
  };  
};
```


トラブルシューティング

LDAP サーバとの通信でトラブルシューティングを行うときに特に考慮する必要があるのは、2 つの LDAP が同じように実装されていることはほとんどないという点です。CA SDM ユーティリティを使用すると、LDAP 統合が正しく機能していることを確認できます。

注: CA SDM は、Microsoft Active Directory、eTrust、および iPlanet との統合に対しては、事前設定されています。ほかの LDAP サーバとのインテグレーションを行うときは、多くの場合、両側での変更や調整が必要となります。

デーモンまたはプロセスのステータスの表示

ldap_virtldb プロセスは、CA SDM と LDAP 仮想データベースの間のやり取りを管理します。

すべての CA SDM デーモン (UNIX) またはプロセスのステータスを表示する方法

1. コマンドラインでパラメータを付けずに `pdm_status` を実行します。

`pdm_status`

`pdm_status` コマンドを実行すると、コマンドを実行したシステム上のすべての CA SDM デーモン (UNIX) またはプロセス (Windows) のステータスが表示されます。

DAEMON		STATUS	HOST	PID	SLUMP	CONNECT	TIME

--							
Agent antfarm		Running	antfarm	455	Tue Feb 17	17:55:12	
Ddict_rd	(ddictrd)	Completed	antfarm				
Data Dictionary	(ddictbuild)	Completed	antfarm				
...							
User Validation	(boplgln)	Running	antfarm	456	Tue Feb 17	17:55:21	

2. `ldap_virtldb` プロセスのステータスをコマンド出力で確認します。

slstat コマンド

bopLDAP が接続されていることを確認するには、以下のコマンドをパラメータを付けずに実行します。

`slstat`

bopLDAP のステータスをコマンド出力で確認します。

NX.env ファイル

基本的な LDAP オプションが適切にインストールされていることを確認するには、\$NX_ROOT/NX.env ファイルを参照します。

どの LDAP オプションがインストールされているかに応じて、NX.env ファイルには以下の記述のような行が含まれます。

```
@NX_LDAP_DN=qouser
@NX_LDAP_ENABLE=Yes
@NX_LDAP_ENABLE_AUTO=Yes
@NX_LDAP_HOST=myserver
@NX_LDAP_PORT=389
@NX_LDAP_PwD=0BUNQXo7CmgbThZLCiMKIwJlA3UXdVNA0jUpHjstfDt2LBIDPgwtWA==
@NX_LDAP_SEARCH_BASE=dc=mycontroller, dc=xyz, dc=com
@NX_LDAP_SERVICE_TYPE=Active Directory
@NX_LDAP_SYNC_ON_NULL=Yes
@NX_LDAP_USER_OBJECT_CLASS=person
```

重要： Sun Java System Directory Server および Novell eDirectory サーバはページング検索をサポートしていないため、LDAP 検索、インポート、および同期の各呼び出しのレコード数は NX_LDAP_MAX_FETCH の値に制限されます。デフォルト値は 100 です。これらの LDAP サーバのどちらかを使用している場合、NX.env ファイルに NX_LDAP_MAX_FETCH を追加して LDAP レコードの最大数を指定することをお勧めします。NX_LDAP_MAX_FETCH は、LDAP サーバの LDAP_SIZELIMIT_EXCEEDED または LDAP_ADMINLIMIT_EXCEEDED の値より小さい任意の値に設定できます。

関連項目：

[LDAP オプションの設定](#) (P. 382)

pdm_ldap_test

LDAP ディレクトリへの接続の確認、検索オプションが適切に設定されていることの確認、TLS の環境設定の確認を行うには、`pdm_ldap_test` コマンドラインユーティリティを使用します。

デフォルトでは、`pdm_ldap_test` は、LDAP オプションをインストール、編集、またはアンインストールするときに入力される `$NX_ROOT/NX.env` ファイルのパラメータ設定を使用します。デフォルトを上書きするには、`pdm_ldap_test` コマンドラインでパラメータを指定します。

このコマンドで利用できるパラメータを確認するには、以下のコマンドを入力します。

```
pdm_ldap_test -h
```

重要: UNIX では、一部の **CA SDM** ユーティリティを実行する前に `LIBPATH` を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して `LIBPATH` を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

LDAP サーバへの接続の確認

LDAP サーバへの接続を確認するには、パラメータを付けずに `pdm_ldap_test` を実行します。

```
pdm_ldap_test
```

LDAP サーバへの接続成功

正常に接続されている場合は、以下のような出力が表示されます。

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(Administrator) (Success)
LDAP API Verion 3
```

接続失敗: サーバダウンまたは不適切な名前/ポート

サーバダウンや、不適切な LDAP サーバ名またはポートを指定したことが原因で接続が失敗した場合は、以下のような出力が表示されます。

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(junk,389): (Success)
ldap_bind_s(Administrator) (Server Down)
```

接続失敗: 無効な LDAP_DN または LDAP_PWD

不適切な LDAP_DN または LDAP_PWD を指定したことが原因で接続が失敗した場合は、以下のような出力が表示されます。

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(junk) (No Such Object or Invalid Credentials)
```

検索パラメータの表示

検索パラメータの設定が正しいことを確認するには、パラメータを付けずに pdm_ldap_test を実行します。

```
pdm_ldap_test
```

検索成功

検索が正常に実行された場合は、以下のような出力が表示されます。

```
DN: CN=John A. Smith,CN=Users,DC=COMPUTERTEST
    c(2)(0): US
    displayName(14)(0): John A. Smith
    mail(14)(0): account02@mycompany.com
    givenName(4)(0): John
    initials(1)(0): a
    distinguishedName(38)(0): CN=John a.

Smith,CN=Users,DC=COMPUTERTEST
    objectGUID(3)(0): 314738
    pager(12)(0): ###-111-1111
    postalCode(5)(0): 11111
    SAMAccountName(7)(0): account02
    sn(6)(0): Smith
    telephoneNumber(12)(0): ###-342-6265
    userPrincipalName(16)(0): account02@COMPUTERTEST
```

```

DN: CN=Mike Johnson,CN=Users,DC=COMPUTERTEST
    displayName(10)(0): Mike Johnson
    givenName(4)(0): Mike
    distinguishedName(34)(0): CN=Mike

Johnson,CN=Users,DC=COMPUTERTEST
    objectGUID(12)(0): 312328
    SAMAccountName(7)(0): account03
    sn(5)(0): Johnson
    userPrincipalName(16)(0): account03@COMPUTERTEST

```

検索失敗: 無効な SEARCH_BASE

無効な SEARCH_BASE を指定したことが原因で検索が失敗した場合は、以下のような出力が表示されます。

```

Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)

ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (No Such Object or Referral)

```

検索失敗: SIZELIMIT_EXCEEDED、TIMEOUT

検索の絞り込みが十分でないフィルタを指定すると、SIZELIMIT_EXCEEDED メッセージまたは TIMEOUT メッセージが表示されて検索が失敗することがあります。ほとんどの LDAP サーバでは、検索リクエストで返す処理結果に対して、サイズの制限を設定しています。この制限を超えると、SIZELIMIT_EXCEEDED メッセージが表示されます。検索リクエストにかかる時間がデフォルトのタイムアウトである 20 秒よりも長くなると、リクエストがタイムアウトし、以下のような TIMEOUT エラー メッセージが表示されます。

```

Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (TIMEOUT or SIZELIMIT_EXCEEDED)

```

検索失敗: レコードが返されない

初期設定のフィルタが適切でないと、検索が失敗する場合があります。
`pdm_ldap_test` がレコードを返さない場合は、必ず **Using filter** 行を確認してください。このフィルタは、`LDAP_FILTER_PREFIX` および `LDAP_FILTER_SUFFIX`、または `LDAP_OBJECT_CLASS` オプションによって生成される基本的なフィルタです。

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabs
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() 0 records
```

検索の絞り込み

検索結果を絞り込む検索条件を基本的なフィルタに追加するには、`pdm_ldap_test` コマンドで `-f` パラメータを使用します。フィルタでは、LDAP の適切な構文と LDAP スキーマ属性名を使用する必要があります。フィルタは二重引用符で囲み、演算子を評価する順序を明確にするためにカッコを使用する必要があります。

たとえば、`sn=Account_10001` のレコードをすべて検索するには、以下のコマンドを使用します。

```
pdm_ldap_test -f "(sn=Account_10001)"
```

`pdm_ldap_test` ユーティリティは、以下の等価演算子をサポートします。

等価演算子	説明
=	等しい
<=	以下
>=	以上
~=	like

pdm_ldap_test ユーティリティは、以下のブール演算子をサポートします。

ブール演算子	説明
&	および
	または
!	NOT

AND および OR 演算子は、検索フィルタ内の丸かっこ () で囲まれた各指定に適用されます。NOT は、丸かっこで囲まれた最初の指定にのみ適用されます。これらの演算子は常に、検索フィルタの間ではなく、適用する検索フィルタの前に指定します。また、以下の例のように、演算子は任意の数のフィルタに適用できます。

```
"(&(sn=Brown)(initials=A))"
```

```
"(|(sn=Brown)(sn=Smith))"
```

```
"(!sn=Brown)"
```

値がある属性名の確認

LDAP ユーザまたはグループのレコードに定義されている属性を確認するには、pdm_ldap_test コマンドで `-a "*" -f` パラメータと `-f` パラメータを使用します。このテストは、連絡先属性にマップできる LDAP 属性があるかどうかを確認する場合や、連絡先レコードを作成または更新するときに、特定の属性に値があり、その値を使用できるかどうかを確認する場合に役立ちます。

以下の例は、iPlanet Directory の出力です。

```
pdm_ldap_test -a "*" -f sn=Account_1000001

2 LDAP records found...

DN: cn=Account_1000001,ou=200K_Plus,o=SmartLabs
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): Person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): Top
```

```
DN: cn=Account_1000001,ou=2_Plus,o=SmartLabs
mail(28)(0): ThisIsTheMailingAddressField
uid(13)(0): Login_1000001
givenName(17)(0): GivenNameOfPerson
sn(15)(0): Account_1000001
objectClass(13)(0): inetOrgPerson
objectClass(20)(1): organizationalPerson
objectClass(6)(2): Person
objectClass(18)(3): ndsLoginProperties
objectClass(3)(4): Top
```

以下の例は、Active Directory の出力です。

```
Ldap_test -a "*" -f (&(sn=Brown)(initials=A))"
```

```
1 LDAP records found...
```

```
DN: CN=John A. Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
objectClass(3)(0): top
objectClass(6)(1): person
objectClass(20)(2): organizationalPerson
objectClass(4)(3): user
cn(16)(0): John A. Smith
sn(5)(0): Brown
givenName(7)(0): John
initials(1)(0): A
distinguishedName(55)(0): CN=John A.
Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
displayName(16)(0): John A. Smith
memberOf(52)(0): CN=Domain Admins,CN=Users,DC=mycontroller,DC=xyz,DC=com
sAMAccountName(7)(0): smijo04
userPrincipalName(25)(0): smijo04@mydomain.xyz.com
objectCategory(63)(0):
CN=Person,CN=Schema,CN=Configuration,DC=mycontroller,DC=xyz,DC=com
```

LDAPトレースのオン

CA SDM 内で LDAP の使用状況を監視するには、`pdm_logstat` ユーティリティを使用して、ログのトレースをオンにします。

`pdm_logstat` コマンドの構文は以下のとおりです。

```
pdm_logstat -f ldap_virtldb.c 1000
```

コマンドに続けて出力される `stdlog` のメッセージを参照すると、接続プロセスのステータスを把握できます。

ldap_virtldb プロセスが開始されたことの確認

LDAP メッセージに関して **stdlogs** を分析する場合、最初に調べる行は **ldap_virtldb** プロセスを開始する指定行です。CA SDM が LDAP の検出を開始するのは、このプロセスが開始されたときです。

注: LDAP インテグレーション オプションをインストールまたはセットアップしていない場合でも、このプロセスは動作します。

```
06/03 17:00:18.27 cpasdl bopLDAP 1964 SIGNIFICANT ldap_virtldb.c
```

```
680 STARTUP of LDAP_virtldb
```

必須オプションがすべてインストールされていることの確認

定義されていない必須の LDAP オプションがある場合、以下の例のように、オプションが未定義であることが **stdlog** に出力されます。

```
06/03 17:00:18.72 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtldb.c 1023 LDAP Server  
port id missing  
06/03 17:00:18.78 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtldb.c 1023 LDAP Server  
distinguished name missing  
06/03 17:00:18.78 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtldb.c 1023 LDAP Server  
distinguished name password missing
```

LDAP が正常に接続されたことの確認

stdlog のエントリを調べると、LDAP が正常に接続されたことを確認できます。以下の例のように、LDAP サーバとの接続が正常に確立されたことがエントリに示されます。

```
06/05 12:35:10.41 cpasdl bopLDAP 1912 SIGNIFICANT ldap_virtldb.c 958 LDAP_SRVR  
connecting to host(Francisco.us.danconia.net) port(389)  
06/05 12:35:11.01 frisco bopLDAP 1912 SIGNIFICANT ldap_virtldb.c 1002 LDAP_SRVR  
binding with username(simon)
```

LDAP 接続が使用できないことの確認

何らかの理由で LDAP サーバに接続できない場合、[LDAP エントリ] や [LDAP をマージ] などの LDAP 機能は使用できません。また、検索結果も返されません。このような状況で操作を実行しようとする、以下の例のようなメッセージが `stdlog` に出力されます。

```
06/03 17:00:32.25 cpasdl bopLDAP 1964 SIGNIFICANT ldap_virtddb.c 219 LDAP server
not available; 'register_producer' not processed
```

```
06/05 10:52:57.63 cpasdl bopLDAP 1896 SIGNIFICANT ldap_virtddb.c 219 LDAP server
not available; 'select_full' not processed
```

```
06/05 10:52:57.66 cpasdl web:local 1868 ERROR sel_data_cache. 611 Error in ldap
Select_Cache method got_initial_count: LDAP server not available; 'select_full' not
processed
```

```
06/05 10:52:57.66 cpasdl bopLDAP 1896 SIGNIFICANT ldap_virtddb.c 219 LDAP server
not available; 'select_cancel' not processed
```

実際に使用されるフィルタの確認

CA SDM は、オプションマネージャで定義された検索ベースやフィルタ、またはユーザが入力した検索基準に基づいて、LDAP ディレクトリからレコードをフェッチします。検索リクエストで実際に生成されたフィルタを確認するには、以下のメッセージを調べます。

```
06/24 14:18:28.32 mcxxx04- bopLDAP 3844 TRACE ldap_virtddb.c 853 Starting select
full: base=DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person)(|(sn=Jones)(pzLastName=Jones)));
attributes=(uid,sAMAccountName,pzUserName,distinguishedName)
```

フェッチされる属性の確認

CA SDM は、オプションマネージャで定義された検索ベースやフィルタに基づいて、LDAP ディレクトリからレコードをフェッチします。

SEARCH_BASE や、`ldap.maj` および `ldap_group.maj` で定義した属性マッピングが適切であることを確認するには、以下のメッセージを調べます。

```
06/24 14:18:28.39 mcxxx04- bopLDAP 3844 TRACE ldap_virtddb.c 766 Starting
select short: base=CN=John D. Jones,CN=Users,DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person));
attributes=(modifyTimestamp,sn,pzLastName,givenName,pzFirstName,initials,pzMiddle
Name,uid,sAMAccountName,pzUserName,telephoneNumber,pzWorkPhoneNumber,mobile,pzMob
ilePhoneNumber,department,pzDepartment,facsimileTelephoneNumber,pzFaxPhoneNumber,
pager,mail,pzEmailAddress,streetAddress,pzAddress,l,pzCity,st,pzState,postalCode,
pzPostalCode,c,pzCountry,o,memberOf)
```

LDAP データが使用可能かどうかの確認

CA SDM が LDAP オブジェクトの ID 属性に対してマッピングを正常に実行できる場合は、\$NX_ROOT/bopcfg/majic/ldap.maj で定義した属性がエントリごとに取得されます。正常に実行できない場合は、属性が未定義であると通知するメッセージがログ ファイルに記録されます。以下のようなメッセージになります。

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'modifyTimestamp '
```

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE   ldap_virtdb.c   1396 Value not
available for 'telephoneNumber,pzWorkPhoneNumber'
```


第 9 章：役割の管理

注: Web インターフェースに関するほかの事項については、「Web インターフェースの構成」を参照してください。

このセクションには、以下のトピックが含まれています。

[役割](#) (P. 409)

[事前定義役割](#) (P. 410)

[役割ベースのセキュリティ](#) (P. 412)

[役割ベースのナビゲーション](#) (P. 423)

[カスタム役割の実装方法](#) (P. 433)

[カスタム メニュー ツリーの实装方法](#) (P. 435)

[役割レコードの作成](#) (P. 437)

[タブ レコードの作成](#) (P. 438)

[メニュー バー レコードの作成](#) (P. 439)

[Web フォーム レコードの作成](#) (P. 440)

[メニュー ツリーのコピー](#) (P. 442)

[メニュー ツリーの作成およびカスタマイズ](#) (P. 443)

[ヘルプ セットの作成および発行](#) (P. 445)

[役割の切り替え](#) (P. 446)

役割

役割とは、CA SDM セキュリティおよびユーザ インターフェースのナビゲーションを制御するプライマリ レコードのことです。各役割では、ユーザがタスク（ビジネス組織内で遂行する役割に一般に割り当てられているもの）を実行するために必要な機能のみを公開することで、システムの限定ビューを定義します。

ユーザのデフォルトの役割によって、ログオン時に表示されるシステムビューが決定されます。複数の役割が割り当てられているユーザは、ログアウトして再度ログインすることなく、役割を切り替えてシステムのさまざまなビューを表示できます。

事前定義役割

デフォルト構成の事前定義の役割を使用したり、その役割をビジネス要件に合うように変更したり、新規役割を作成したりできます。

以下の表で、CA SDM にインストールされている事前定義役割について説明します。以下の役割は、ITIL v3 ベストプラクティスに合わせてデザインされているため、IT 部門を ITIL 準拠にするために必要なサイト固有のカスタマイズの量が削減されます。

CA SDM は ITIL のみをサポートします。また、CA SDM ドキュメントは ITIL 対応で記述されています。詳細については、[「ITIL の環境設定」](#) (P. 72)を参照してください。

役割タイプ	役割名	説明
エンド ユーザ	構成ビューア	基本的な CI 表示と社内からの調査タスクを実行します。
	顧客	社外から基本的なセルフサービス タスクを実行します。
	従業員	社内から基本的なセルフサービス タスクを実行します。
アナリスト	構成アナリスト	構成アイテムのライフ サイクル プロセス内でタスクを実行し、社内から CMDB の 2 次サポートを提供します。
	顧客サービス担当者	社外のユーザ（通常は顧客）をサポートします。
	ナレッジアナリスト	ナレッジ管理のライフ サイクル プロセス内でタスクを実行します。
	レベル 1 のアナリスト	社内から 1 次サポートを提供します。
	レベル 2 のアナリスト	より高度な専門知識を必要とする 2 次サポートを社内から提供します。
	サポート オートメーションアナリスト	ライブ アシスタンス環境内で 1 次サポートを提供します。

役割タイプ	役割名	説明
マネージャ	ベンダー アナリスト	ベンダー固有のハードウェアなど、IT 環境の限られたセグメントを社外からサポートします。
	変更マネージャ	変更要求プロセスを管理します。通常は、変更要求チケットで作業するアナリスト以外になります。
	顧客サービス マネージャ	顧客サービス担当者および外部サポートプロセスを管理します。
	インシデント マネージャ	インシデントプロセスを管理します。通常は、インシデントチケットで作業するアナリスト以外になります。
	ナレッジ マネージャ	ナレッジアナリスト、ナレッジドキュメントの再割り当てとエスカレーション、および日常的なナレッジ管理を監督します。
	問題マネージャ	問題プロセスを管理します。通常は、問題チケットで作業するアナリスト以外になります。
	Service Desk マネージャ	エスカレーションを処理し、レベル 1 のアナリストを監督します。また、サービス デスク操作全体を管理することもあります。
管理者	管理者	CA SDM およびナレッジマネジメントの実装における管理タスクを実行します。この役割は、通常、製品のインストール、設定、および統合を行います。
	構成管理者	CA CMDB の実装に関連する管理タスクを実行します。この役割は通常、CMDB、構成アイテムインフラストラクチャ、およびデータ構造を管理します。
	ナレッジマネジメント 管理者	ナレッジ管理設定を設定し、監視します。
	Service Desk 管理者	カテゴリ、連絡先、サービス タイプ、根本原因の作成と更新のような、データおよびプロセスに関する管理タスクを実行します。

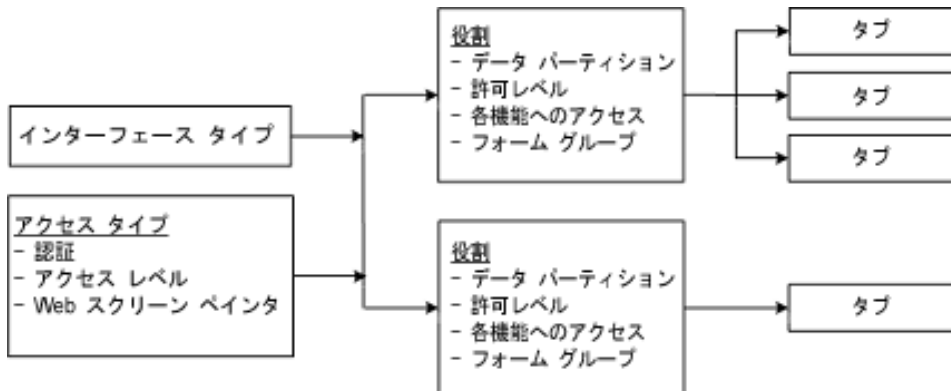
役割タイプ	役割名	説明
	サポート オートメーション 管理者	キューおよびアナリスト ツールの権限の設定のような、サポート オートメーション 環境に関連する管理タスクを実行します。
	システム管理者	オプションの設定、統合の構成、Web フォームの変更など、CA SDM の実装、設定、およびカスタマイズ（適応化）に関連した管理タスクを実行します。
	テナント管理者	特定のテナントまたはサポート組織に固有のマルチテナンシー管理タスクを実行します。

役割ベースのセキュリティ

アクセス タイプおよび役割は、CA SDM セキュリティを制御する主要なコンポーネントです。

以下の図は、役割がその他のシステム オブジェクトと相互に関係し、役割ベースのセキュリティを提供する仕組みの概要を示しています。

注: その他のセキュリティについては、[「セキュリティ」](#) (P. 329)を参照してください。



アクセス タイプについて

ユーザの各アクセス タイプは、以下のようなシステムの動作を制御します。

- ユーザのログイン時に CA SDM が Web 認証を実行する仕組み
- ユーザのアクセス レベル
- Web Screen Painter を使用した Web フォームまたはデータベース スキーマの変更をユーザに認めるかどうか
- ユーザが使用可能な役割

連絡先レコードの作成または更新時にアクセス タイプを選択すると、アクセス タイプと連絡先を関連付けることができます。

以下の表に、定義済みのアクセス タイプ、リンクされた役割、および概要を示します。

アクセス タイプ	リンクされた役割	説明
管理	■ 管理者（デフォルト） ■ 構成管理者 ■ 従業員 ■ レベル 2 のアナリスト ■ Service Desk 管理者 ■ システム管理者 ■ テナント管理者	主要な管理役割すべてに最高レベルのセキュリティ アクセスを提供します。実装時および管理時に使用します。 注: 管理アクセス タイプは事前設定されているため、管理者はリンクされている任意の役割に切り替えることができます。たとえば、管理者はログインし直さずに従業員役割に切り替えて、システムの別のビューを表示することができます。
顧客	■ 顧客	セルフサービス ビューを使用する社外の顧客に高度に制限されたアクセスを提供します。
従業員	■ 従業員	セルフサービス ビューを使用する社内の従業員に高度に制限されたアクセスを提供します。新規インシデントの作成とインシデント ページの更新に使用します。

アクセス タイプ	リンクされた役割	説明
IT 担当者	■ 構成アナリスト ■ 従業員 ■ レベル 2 のアナリスト (デフォルト) ■ ナレッジ アナリスト ■ ナレッジ マネジメント 管理者 ■ ナレッジ マネージャ	IT 部門で働いているが、サポート チームのメンバーではないユーザにアナリスト指向のアクセスを提供します。このアクセスは、ナレッジ マネジメント へのアクセスを必要とするユーザのために設計されています。
ナレッジ マネジメント	■ 構成管理者 ■ 構成アナリスト ■ 構成ビューア ■ 従業員 ■ ナレッジ アナリスト ■ ナレッジ 管理 マネージャ (デフォルト) ■ ナレッジ マネージャ ■ レベル 2 のアナリスト	ナレッジ マネジメント 機能を管理するユーザに合わせた管理アクセスを提供します。
プロセス管理	■ 変更 マネージャ ■ 構成アナリスト ■ 従業員 ■ インシデント マネージャ (デフォルト) ■ レベル 2 のアナリスト ■ 問題 マネージャ ■ Service Desk マネージャ	主要なプロセス管理役割を実行するユーザに合わせたアクセスを提供します。

アクセス タイプ	リンクされた役割	説明
サービス デスク 管理	■ 顧客サービス マネージャ ■ 構成アナリスト ■ 従業員 ■ レベル 1 のアナリスト ■ レベル 2 のアナリスト ■ Service Desk マネージャ (デフォルト)	IT サポートまたは外部顧客サポート機能を管理するユーザ (通常、第一線のサポート管理者) に合わせたアクセスを提供します。
サービス デスク スタッフ	■ 構成アナリスト ■ 構成ビューア ■ 顧客サービス担当者 ■ 従業員 ■ レベル 1 のアナリスト (デフォルト) ■ レベル 2 のアナリスト	サポート タスクを実行するユーザに合わせたアクセスを提供します。アクセスは、第一線のサポートを行うユーザに合わせられます。
サポート オートメーション 管理	■ サポート オートメーション 管理者	サポート オートメーション 管理を行うユーザにアクセスを提供します。
サポート オートメーション アナリスト	■ サポート オートメーション アナリスト	エンドユーザにライブ アシスタンスを提供するユーザにアクセスを提供します。
ベンダー スタッフ	■ ベンダー アナリスト	自社製品 (特定のブランドのハードウェアなど) に直接関連する項目についてのみ対応する外部ベンダーに、高度に制限されたアクセスを提供します。

役割レコード

役割は、アクセス タイプに割り当てたり、ユーザの連絡先レコードに直接割り当てたりすることができます。 役割の割り当てに競合が発生した場合は、連絡先の役割の割り当てが優先されます。

各役割レコードは、以下のコンポーネントで構成する必要があります。

- 1つのフォーム グループ
- 1つのユーザ インターフェースのタイプ
- 複数の機能のアクセス設定
- 1つ以上のタブ
- 1つのヘルプ セット

以下のオプションのコンポーネントも各役割の定義に含めることができます。

- メニュー ツリー
- スコアボード
- メニュー バー
- ツールバー
- 1つのデータ パーティション
- ナレッジ マネジメント アクセス
- サポート オートメーション アクセス レベル
- レポートの **Web** フォーム
- 実行リソース

機能アクセス領域

機能アクセス領域は、チケットレコードおよび他のシステムコンポーネントへの役割レベルアクセスを定義します。 `usp_functional_access_type` テーブルでは領域を定義し、`usp_functional_access_level` テーブルではユーザアクセスを記述します。

デフォルトの機能アクセス領域は以下の表のとおりです。

名前	コード名	新規
管理	admin	×
インシデント/問題/リクエスト	call_mgr	×
変更要求	change_mgr	×
インベントリ	inventory	×
案件	issue_mgr	×
ナレッジドキュメント	kd	×
通知	notify	×
参照	reference	×
セキュリティ	security	×
アナウンスメント	announcement	○
インシデント/問題/リクエスト参照	call_mgr_reference	○
インシデント/問題/リクエストテンプレート	call_mgr_template	○
変更要求テンプレート	change_mgr_template	○
変更要求参照	change_reference	○
構成アイテム	ci	○
構成アイテム共通読み取り専用	ci_common_ro	○
構成アイテム参照	ci_reference	○
連絡先	contact	○
グループ	group	○
案件テンプレート	issue_mgr_template	○
案件参照	issue_reference	○

ロケーション	location	○
マルチサイト管理	multisite_admin	○
マルチサイト参照	multisite_reference	○
通知の参照	notification_reference	○
組織	organization	○
優先付け	prioritization	○
サービス レベル	service_level	○
サイト	site	○
ストアドクエリ	stored_queries	○
サポート オートメーション	sa	○
調査	survey	○
テナント管理	tenant_admin	○
タイムゾーン	timezone	○
ワークフロー参照	workflow_reference	○
ワークシフト	workshifts	○

機能アクセス領域を追加する方法

機能アクセス領域を追加すると、既存の役割には自動的に変更アクセス権が付与されます。適切な権限を付与するためにアクセス レベルを確認して変更することができます。

機能アクセス領域を追加するには、以下の手順に従います。

1. [管理] タブで [セキュリティと役割の管理] - [機能アクセス] を選択します。
2. [新規作成] をクリックします。
[機能アクセス リストの新規作成] ページが表示されます。
3. [機能アクセス領域] フィールドを必要に応じて指定します。
4. [保存] をクリックします。
[機能アクセスの詳細] ページが表示されます。

5. [1つ](#) (421P.)以上の役割に (419P.)アクセス レベルを適用します。

注: 機能アクセス領域に関する詳細情報については、[オンライン ヘルプ](#)を参照します。

多くの役割にアクセス レベルを適用する

機能アクセス領域については、各役割にアクセス レベルを設定して時間を節約することができます。役割管理を使用する代わりに、機能アクセス領域を適切な役割アクセス レベルで更新します。

多くの役割にアクセス レベルを適用するには、以下の手順に従います。

1. [管理] タブで [セキュリティと役割の管理] - [機能アクセス] を選択します。
2. 機能領域の名前をクリックします。
3. [役割] タブで、[リスト内で編集] をクリックします。
4. 必要に応じて各役割を確認して更新します。以下のアクセス レベルがあります。

なし

機能オブジェクトへの役割のアクセスを拒否します。

表示

機能オブジェクトへの読み取り専用機能を許可します。

変更

機能オブジェクトへの読み取り/書き込みアクセスを許可します。

5. 引き続き役割を選択してアクセス レベルを選択します。
6. (オプション) [すべて変更] をクリックします。
7. [保存] をクリックします。

役割への変更はすぐに適用されます。

注: 役割および機能アクセス レベルの詳細については、オンラインヘルプを参照してください。

例: アナウンスメントのアクセスレベルを変更する

この例では、アナウンスメント機能アクセス領域の役割アクセス レベルを変更できることを示します。

1. [管理] タブで [セキュリティと役割の管理] - [機能アクセス] を選択します。
[機能アクセスの詳細] ページが表示されます。
2. [アナウンスメント] をクリックします。
3. [役割] タブで、[リスト内で編集] をクリックします。
4. [レベル 2 アナリスト] を選択します。
5. [アクセス レベル] から [表示] を選択します。
レベル 2 アナリスト役割のアクセス レベルが [表示] の値と共にハイライトされます。
6. [構成アナリスト] を選択します。
7. [アクセス レベル] から [変更] を選択します。
構成アナリストのアクセス レベルが [変更] の値と共にハイライトされます。
8. [保存] をクリックします。
変更を確認するメッセージが表示されます。
9. レベル 2 アナリスト役割としてログインします。
10. [アナウンスメントの表示] を選択します。
[アナウンスメント] ページが表示されます。
11. [アナウンスメント] をクリックします。
レベル 2 アナリストとして、アナウンスメントのみを表示できることを確認するメッセージが表示されます。

12. 構成アナリストに役割を設定します。
13. [アナウンスメントの表示] を選択します。
[アナウンスメント] ページが表示されます。
14. [アナウンスメント] をクリックします。
[アナウンスメントの更新] ページが表示されます。 構成アナリストとして、アナウンスメントを変更できます。

役割にアクセス レベルを適用する

役割管理を使用してユーザがユーザ インターフェースにアクセスする方法を変更することができます。役割のアクセス レベルを変更すると、ユーザ インターフェースはアクセス レベルに基づいてオブジェクト、ページ、およびメニュー アイテムのみを表示します。たとえば、役割が連絡先を作成できなくなった場合は、[ファイル] メニューから [新規連絡先] が省略されます。

役割にアクセス レベルを適用するには、以下の手順に従います。

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。
2. [役割リスト] で、役割名を右クリックし、ショートカット メニューから [編集] を選択します。
3. [各機能へのアクセス] タブで [リスト内で編集] をクリックします。
4. 機能名をクリックします。
行が強調表示されます。
5. 以下のアクセス レベルを使用して機能アクセス領域を必要に応じて更新します。

なし

機能オブジェクトへの役割のアクセスを拒否します。

表示

機能オブジェクトへの読み取り専用機能を許可します。

変更

機能オブジェクトへの読み取り/書き込みアクセスを許可します。

6. [保存] をクリックします。

変更を確認するメッセージが表示されます。役割はすぐに指定されたアクセスレベルで機能アクセス領域を使用できます。

7. 役割としてログインし、メニュー、ページオプションおよびボタンを確認することにより、アクセス レベルを検証します。

例: レベル 2 アナリスト役割のチケット変更アクセス権の付与

この例では、レベル 2 アナリストのチケット変更アクセス権を付与した場合、ユーザ インターフェイスがどのように変更されるかを示します。

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。

[役割リスト] が表示されます。

2. [レベル 2 アナリスト] を右クリックし、ショートカット メニューから [編集] を選択します。

3. [各機能へのアクセス] タブで [リスト内で編集] をクリックします。

4. [インシデント/問題/リクエスト参照] を選択します。

5. [アクセス レベル] で [変更] を選択します。

アクセス レベルが [変更] に更新されます。

6. [保存] をクリックしログアウトします。

変更を確認するメッセージが表示されます。

7. レベル 2 アナリスト役割としてログインします。

8. [検索] - [インシデント] を選択します。

9. [検索] をクリックし、インシデントを開きます。

[インシデント詳細] ページには [リスト内で編集] ボタンが含まれます。レベル 2 アナリストとして、チケットを変更できます。

データ パーティション

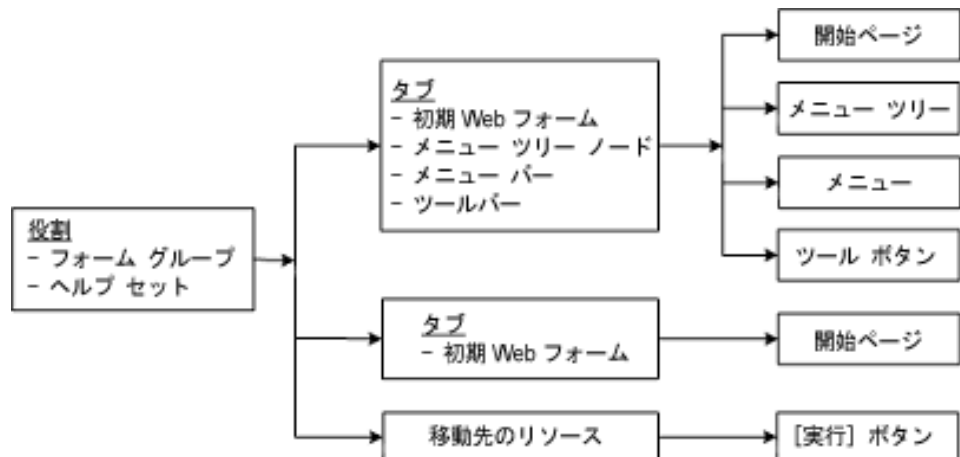
データ パーティションは **CA SDM** データベースの一部であり、これを使用してレコードレベルでアクセスを制御できます。役割にデータ パーティションを関連付けて、**Web** インターフェースを通じてアクセスされるチケットやほかのレコードへのアクセスを制限できます。

データ パーティションを管理する方法については、[「データ パーティションの関連付け」](#) (P. 350)を参照してください。

役割ベースのナビゲーション

各ユーザの **Web** インターフェースの表示は、役割によって定義されます。複数の役割割り当てを持つユーザは、**Web** インターフェースの複数の表示を切り替えることができます。

以下の図は、役割がその他のオブジェクトと相互に関係し、ユーザ インターフェースの役割ベースの表示を作成する仕組みを示しています。



Tabs

タブはグラフィカルに表示される、役割にリンクしたエンティティで、その役割を持つユーザに機能を示します。ユーザがシステムにログインすると、メイン ウィンドウにユーザのデフォルトの役割に割り当てられたタブが表示されます。

タブは、Web インターフェースのメイン ウィンドウに主要な細分領域を定義するものです。各タブは、タブを使用する 1 つ以上の役割に対して適切なセットのユーザ インターフェース機能を公開するように構成されます。

すべての役割には、1 つ以上のタブが必要となります。役割には 1 つ以上のタブを関連付けることができます。各タブには、メイン ウィンドウでの表示順序を制御するシーケンス番号が割り当てられます。役割に関連付けられているタブが 1 つだけの場合は、タブではなくタブの開始ページが表示されます。

タブは、以下の種類の表示機能を含めるように構成できます。

- ユーザがタブを選択したときに表示される開始ページ（デフォルトの Web フォーム）です。開始ページは、すべてのタブの必須エレメントです。各タブに 1 つの開始ページを割り当てることができます。

注: 開始ページにビジネス オブジェクトからのグラフィック レポートが表示されるよう設定できます。これにより、ユーザは実行時にレポートを生成できます。詳細については、[「CA Business Intelligence レポート」](#) (P. 981)を参照してください。

- [ファイル]、[表示]、[検索]などのコマンドのドロップダウン リストを提供するメニュー バーです。メニュー バーは任意です。各タブに 1 つのメニュー バーを割り当てることができます。
- ツールバー。頻繁に使用するメニュー コマンドに簡単にアクセスできるツール ボタンが提供されます。ツールバーはオプションです。

CA SDM には、事前定義のタブがいくつか用意されています。事前定義のタブを役割に割り当てたり、事前定義のタブを変更したり、カスタム タブを作成したりできます。

重要: ウィンドウで表示しきれない数のタブを割り当てないでください。より大きなシーケンス番号のタブがウィンドウの表示可能な領域からはみ出し、ユーザがタブにアクセスできなくなります。

重要: 含めるタブは、作成または編集している役割に割り当てられたフォームグループに属するフォームを持つタブのみにしてください。たとえば、[顧客] タブや [従業員] タブを [管理者] の役割に割り当てないでください。割り当てた場合、ユーザがそのタブにアクセスしようとするとエラーになります。役割のフォームグループは、[役割の詳細] ページの [カスタム フォーム グループ] フィールドで指定します。また、[役割リスト] ページの [フォーム グループ] 列にも表示されます。各フォームグループに含まれる Web フォームのリストについては、[「フォームグループ」](#) (P. 1405)を参照してください。

事前定義タブ

以下の表に、各役割に割り当てられている事前定義タブを示します。タブはシーケンス番号順にリストされており、ウィンドウでは左から右に表示されます。

注: 多くの場合、同じ表示名を持つタブが複数あります。たとえば、管理者役割の [Service Desk] タブでは CA SDM 機能へのフルアクセスが提供されますが、変更マネージャ役割の [Service Desk] タブでは変更要求により焦点が当てられています。

役割	タブ
管理者	■ フルメニューおよびスコアボードを伴った Service Desk タブ ■ ナレッジ タブ ■ フルメニュー ツリーを伴う管理タブ ■ レポート タブ - 管理者 ■ 変更カレンダー タブ ■ CA CMDB タブ ■ サポートオートメーション タブ
変更マネージャ	■ レポート タブ - 変更マネージャ ■ Service Desk タブ - 変更マネージャ ■ 変更カレンダー タブ
構成管理者	■ CA CMDB タブ ■ 管理タブ - 構成管理者

役割	タブ
構成アナリスト	■ CA CMDB スコアボード - 構成アナリスト
構成ビューア	■ CA CMDB スコアボード - 構成ビューア
顧客	■ 顧客タブ
顧客サービス マネージャ	■ Service Desk タブ - 顧客サービス マネージャ ■ ナレッジ タブ ■ レポート タブ - 顧客サービス マネージャ
顧客サービス担当者	■ Service Desk タブ - 顧客サービス担当者 ■ クイック プロファイル タブ ■ ナレッジ タブ
従業員	■ 従業員タブ
インシデント マネージャ	■ レポート タブ - インシデント マネージャ ■ Service Desk タブ - インシデント マネージャ ■ ナレッジ タブ
ナレッジアナリスト	■ Service Desk タブ - ナレッジアナリスト ■ ナレッジ タブ ■ ナレッジ マネジメント スケジュール ■ ナレッジ レポート カード タブ ■ レポート タブ - ナレッジアナリスト
ナレッジ マネージャ	■ Service Desk タブ - ナレッジ マネージャ ■ ナレッジ タブ ■ ナレッジ マネジメント スケジュール ■ 管理タブ - ナレッジ マネージャ ■ ナレッジ レポート カード タブ ■ レポート タブ - ナレッジ マネージャ
ナレッジ マネジメント 管理者	■ 管理タブ - ナレッジ 管理者
レベル 1 のアナリスト	■ Service Desk タブ - レベル 1 アナリスト ■ クイック プロファイル タブ ■ ナレッジ タブ

役割	タブ
レベル 2 のアナリスト	■ Service Desk タブ - レベル 2 アナリスト ■ ナレッジ タブ ■ 変更カレンダー タブ
問題マネージャ	■ レポート タブ - 問題マネージャ ■ Service Desk タブ - 問題マネージャ ■ ナレッジ タブ
Service Desk 管理者	■ 管理タブ - Service Desk 管理者
Service Desk マネージャ	■ レポート タブ - Service Desk マネージャ ■ Service Desk タブ - Service Desk マネージャ ■ ナレッジ タブ ■ 変更カレンダー タブ
サポート オートメーション 管理者	■ Service Desk タブ - レベル 1 アナリスト ■ サポート オートメーション タブ ■ サポート オートメーション 管理 ■ クイック プロファイル タブ ■ ナレッジ タブ
サポート オートメーション アナリスト	■ Service Desk タブ - レベル 1 アナリスト ■ サポート オートメーション タブ ■ クイック プロファイル タブ ■ ナレッジ タブ
システム管理者	■ 管理タブ - システム管理者
テナント管理者	■ 管理タブ - テナント管理者
ベンダー アナリスト	■ Service Desk タブ - ベンダー アナリスト

Web フォーム

Web フォームでは、CA SDM Web インターフェースに表示されるページを定義します。

Web フォームには、以下の 4 つのタイプがあります。

- ビジネス オブジェクト レポート URL
- HTML ページ
- 実行リソース
- カスタム (サードパーティ Web ページの URL など)

カスタム Web フォームの作成については、[「Web フォーム レコードの作成」](#) (P. 440)を参照してください。

フォーム グループ

フォーム グループは、役割で利用できる CA SDM Web インターフェースのページセットを定義します。役割ごとに 1 つずつフォーム グループがあります。ユーザは、自分の役割に割り当てられたフォーム グループに含まれる Web ページのみを表示できます。

インターフェース タイプにはそれぞれ関連付けられているフォーム グループ (そのインターフェース タイプを持つユーザが参照できるページを定義する HTML ファイルのセット) があります。

CA SDM には以下の事前定義済みフォーム グループが用意されています。

- アナリスト
- 顧客
- 従業員
- ITIL

デフォルトの環境設定での事前定義済みフォーム グループの使用、事前定義済みフォーム グループの変更、Web スクリーン ペインタを使用した新規フォーム グループの作成を実行できます。また、各事前定義済み [フォーム グループ](#) (P. 1405)に含まれる HTML ファイル名のリストを表示することもできます。

メニュー ツリー

メニュー ツリーはノード (メニュー ツリー リソース) の階層リストで、このリストは Web インターフェースのメイン ウィンドウの左側にあるナビゲーション ペインに表示されます。

役割には、システムの数多くの機能領域にアクセスするためのノードを提供するメニュー ツリーを指定できます。たとえば、事前定義の管理者役割に、システムおよび役割管理の管理機能、Service Desk 管理機能などへのノードを含むメニュー ツリーを指定できます。

役割にメニュー ツリーが含まれる場合、メニュー バーから指定のリソース セットにアクセスでき、そのリソース セットからシステムの機能領域にアクセスできます。

CA SDM には、以下の役割の事前定義メニュー ツリーが用意されています。

- 管理者 (admin_tree)
- CA CMDB 管理者 (cmdb_adm_tree)
- ナレッジ管理マネージャ (kt_adm_tree)
- ナレッジマネージャ (kt_mgr_tree)
- サポート オートメーション 管理者 (sa_admin_tree)
- サービス デスク管理者 (sd_adm_tree)
- システム管理者 (sys_adm_tree)
- テナント管理者 (tn_admin_tree)

事前定義メニュー ツリー レコードの [名前] フィールド、[レコード ステータス] フィールド、および [説明] フィールドは編集できますが、メニュー ツリー リソースを追加または削除してこれらのフィールドをカスタマイズすることはできません。

カスタム メニュー ツリーを生成するには、新規メニュー ツリー レコードを作成するか、事前定義のメニュー ツリーのいずれかをコピーしてカスタマイズします。

注: 各メニュー ツリー レコードの変更不可の [内部] フィールドは、メニュー ツリーをカスタマイズできるかどうかを示します。[内部] フィールドの値が [はい] の場合は、カスタマイズ不可の事前定義のメニュー ツリーであることを示します。値が [いいえ] の場合は、カスタマイズ可能なサイト定義のメニュー ツリーであることを示します。[メニューのカスタマイズ] ボタンが表示されるのは、[内部] フィールド値が [いいえ] のメニュー ツリー詳細レコードに対してのみです。

メニュー ツリーをタブに添付すると、そのタブにアクセスできるすべての役割に対して使用可能になります。

メニュー ツリー リソース

メニュー ツリー リソースでは、ユーザがメニュー ツリーからアクセスできる項目を定義します。

メニュー ツリー リソースは、名前、説明、および表示される **Web** ページを制御する **Web** エンジンによって使用される **HTML** ファイル名の **URL** フラグメントで構成されます。

メニュー バー

メニュー バーは、**Web** インターフェースのメイン ウィンドウでメニューのリストを左右方向に表示するユーザ インターフェース エlement です。各メニューには、オプションやコマンドのドロップダウン リストが含まれています。作成した任意のカスタム役割に対して、カスタム メニュー バーを定義できます。

メニュー バー レコードでは、メニュー バーがアクセスできるメニュー項目を制御する **HTML** フォームを指定します。

注: メニュー バーの機能を定義するには、**Web** スクリーン ペインタ アプリケーションを使用する必要があります。事前定義のメニュー バーまたはカスタム メニュー バーの機能を構成する方法の詳細については、**Web** スクリーン ペインタのオンライン ヘルプを参照してください。

以下の表に、事前定義メニュー バーおよびそのメニュー バーを使用する事前定義タブを示します。

メニュー バー	関連タブ
管理	■ 管理タブ - 構成管理者 ■ 管理タブ - ナレッジ管理者 ■ 管理タブ - ナレッジ マネージャ ■ 管理タブ - Service Desk 管理者 ■ 管理タブ - システム管理者 ■ 管理タブ - テナント管理者 ■ フル メニュー ツリーを伴う管理タブ

メニュー バー	関連タブ
CA CMDB	■ CA CMDB タブ - フルメニューおよびスコアボードを含む
変更カレンダー	■ 変更カレンダー タブ
ナレッジ	■ ナレッジ タブ ■ ナレッジ マネジメント スケジュール
Service Desk	■ フルメニューおよびスコアボードを伴った Service Desk タブ
Service Desk-変更マネージャ	■ Service Desk タブ - 変更マネージャ
Service Desk-顧客サービス マネージャ	■ Service Desk タブ - 顧客サービス マネージャ
Service Desk-顧客サービス担当者	■ Service Desk タブ - 顧客サービス担当者
Service Desk-Incident Manager	■ Service Desk タブ - インシデント マネージャ
Service Desk-ナレッジアナリスト	■ Service Desk タブ - ナレッジアナリスト
Service Desk-ナレッジマネージャ	■ Service Desk タブ - ナレッジマネージャ
Service Desk-レベル 1 アナリスト	■ Service Desk タブ - レベル 1 アナリスト
Service Desk-レベル 2 アナリスト	■ Service Desk タブ - レベル 2 アナリスト
Service Desk - 問題マネージャ	■ Service Desk タブ - 問題マネージャ
Service Desk-Service Desk マネージャ	■ Service Desk タブ - Service Desk マネージャ
Service Desk タブ-ベンダー アナリスト	■ Service Desk タブ - ベンダー アナリスト
サポート オートメーション アナリスト	■ サポート オートメーション タブ - サポート オートメーション アナリスト

ツールバー

ツールバーは、メニューの右側に 1 つ以上のツール ボタンを表示する機能を追加することで、メニュー バーの機能を拡張します。

ツール ボタンは、ツールバー上にアイコンで表示されます。ユーザはツール ボタンをクリックすることによって、頻繁に使用するメニュー オプションまたはコマンドに簡単にアクセスできます。

注: ツールバーの機能を定義するには、**Web** スクリーン ペインタ アプリケーションを使用します。事前定義済みのツールバーまたはカスタム ツールバーの機能を設定する方法の詳細については、**Web** スクリーン ペインタのオンライン ヘルプを参照してください。

実行リソース

[実行] ボタンを使用すると、特定のレコードを簡単に検索できます。

実行リソースは、**Web** フォームの一種です。役割に実行リソースが関連付けられている場合、ユーザがその役割でログインすると、**CA SDM** のメイン ウィンドウおよびすべてのポップアップ ウィンドウの右上隅に [実行] ボタンが表示されます。[実行] ボタンには、ユーザ インターフェースに 2 つの関連フィールドがあります。

- ドロップダウン リスト。検索対象のレコードの種類を選択します（たとえば、[変更要求]）。
- テキスト ボックス。特定のレコードを識別する値を入力します（たとえば、「135」を入力して変更要求 135 を検索します）。

役割に実行リソースを割り当てると、その役割のユーザが検索できるレコードの種類を指定できます。たとえば、事前定義の管理者役割には、以下の実行リソースがあります。

- 変更要求
- ドキュメント (ID 別)
- インシデント
- 案件
- ナレッジ
- 問題

- リクエスト
- ユーザ (ID 別)
- ユーザ (名前別)
- ユーザ (電話番号別)

ヘルプ セット

ヘルプセットは、ユーザの役割割り当ておよび現在の役割設定に従って、ユーザが利用可能なオンライン ヘルプ トピックの集まりです。たとえば、管理者役割を使用してログインした場合、管理者ヘルプセットに含まれるオンライン ヘルプ トピックを表示できます。従業員役割に切り替えた場合、従業員ヘルプセットを表示できます。

事前定義の各役割には、対応する事前定義のヘルプセットが用意されています。定義した任意のカスタム 役割に対して、カスタム ヘルプセットを作成できます。

注: ヘルプセット定義の使用方法については、オンライン ヘルプを参照してください。

カスタム役割の実装方法

多くのサイトでは事前定義の役割で十分ですが、カスタム役割を作成し、社内のサイト固有のビジネス ニーズを満たすよう調整する必要がある場合があります。

以下に、新しい役割を実装する場合に必要なタスクのプロセスを示します。ここに示す例では、変更要求チケットを確認し、承認するタスクを持つアナリストの小さなグループの役割を実装する方法について説明します。

カスタム役割を実装するには、以下の例で説明されているタスクを実行します。

1. 以下のフィールド値を使用して、新しい役割レコードを作成します。

役割名

変更アナリスト

コード

chg_anal

カスタム フォーム グループ

アナリスト

優先ドキュメント

インシデント

2. [権限] タブの [データ パーティション] フィールドで、[Service Desk アナリスト] を選択します。
3. [各機能へのアクセス] タブの [変更要求] フィールドで、[変更] を選択します。
4. [Web インターフェース] タブに以下の値を入力します。

Web ユーザ インタフェースのタイプ

アナリスト

ヘルプ ビュー

変更アナリスト

5. 以下のタブを選択します。
 - レポート タブ - 変更アナリスト
 - Service Desk タブ - 変更アナリスト
 - 変更カレンダー タブ
6. [レポート Web フォーム] タブで以下のレポートを選択します。
 - ステータスの優先度別のアクティブな変更要求の推移
 - 週末ごとのアクティブな変更要求
 - 失敗したサービス タイプの変更カテゴリ別の変更要求
7. [移動先のリソース] タブに変更要求リソースを追加します。

8. 新しい役割に適したすべてのコンテンツを含むカスタム ヘルプ セット「変更アナリスト」を作成します。

詳細については、[「ヘルプ セットの作成および発行」](#) (P. 445)を参照してください。

9. 新しい役割に適した機能を使用して以下のカスタム タブを作成します。

- レポート タブ - 変更アナリスト
- Service Desk タブ - 変更アナリスト

10. 新しい役割に適したすべてのノードを含むカスタム メニュー ツリーを作成します。

詳細については、[「カスタム メニュー ツリーの実装方法」](#) (P. 435)を参照してください。

カスタム メニュー ツリーの実装方法

多くのサイトでは事前定義のメニュー ツリーで十分ですが、カスタム メニュー ツリーを実装して、役割をカスタマイズする必要がある場合があります。

ほとんどの場合、事前定義済みメニュー ツリーのコピーから始めて、階層内のノードを追加、削除、または再編成するほうが簡単です。または、メニュー ツリーを作成して、ノードの新しい階層をすべて作成することもできます。

役割でカスタム メニュー ツリーを使用可能にするには、以下のいずれかの方法を使用します。

- 元の `admin_tree` を表示するタブの Web フォーム（開始ページ）内にあるメニュー ツリーを置換します。
- Web フォームを作成し、新しいメニュー ツリーを備えた新しい Web フォームをタブに配置します。

カスタム メニューを実装するには、以下の手順を実行します。

1. 事前定義済みのメニュー ツリーのいずれかをコピーします。

注: [コード] フィールドに入力した値をメモします。

2. 以下のフィールド値を使用して、Web フォームを作成します。

- タイプ: HTML

- リソース:

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=admin_main_role.html  
+KEEP.tree_code=menu_tree_code
```

注: menu_tree_code には、ステップ 1 で作成したメニュー ツリーコードの値を指定します。admin_main_role.html コードでは、メニュー ツリーとして KEEP.tree_code 変数の値を使用します。

3. 以下のフィールド値を使用してタブ レコードを作成します。

- 開始ページ: ステップ 2 で作成した Web フォーム

- メニュー バー: [管理]

注: [管理] は数多くの役割で使用する汎用メニュー バーであり、役割に固有のメニュー バーではありません。

4. 手順 3 で作成したタブをカスタム メニュー ツリーへのアクセスを付与する役割に割り当てます。

5. CA SDM をログアウトしてから、再度ログインします。

[管理] タブに、ユーザのカスタム メニュー ツリーが表示されます。

関連項目:

[Web フォーム レコードの作成 \(P. 440\)](#)

役割レコードの作成

管理者は、サイト固有のビジネス要件を満たす、カスタマイズされた役割を作成できます。

役割を作成するには、以下の手順に従います。

1. 「管理」タブで、「セキュリティと役割の管理」 - 「役割管理」 - 「役割リスト」を選択します。
「役割リスト」ページが表示されます。
2. 「新規作成」をクリックします。
「役割の新規作成」ページが表示されます。
3. 以下のフィールドを指定します。

役割名

役割を識別する名前を指定します。この名前がユーザ インターフェイスに表示されます。

コード

役割をシステムで識別するコードを指定します。

注: レコードを保存した後に、このフィールド値を変更することはできません。

レコード ステータス

役割がアクティブであるか、非アクティブであるかを示します。

デフォルトにする

この役割がデフォルト役割であるかどうかを示します。

カスタム フォーム グループ

事前定義フォーム グループまたはカスタム フォーム グループを指定します。

優先ドキュメント

システムにチケットを入力するために、この役割で使用するドキュメントを指定します。

説明

役割の目的の説明です。この説明は「役割リスト」ページに表示され、ユーザを適切な役割に割り当てる際に役立ちます。

「保存」をクリックします。

役割の定義が保存され、「役割の詳細」ページが表示されます。

タブ レコードの作成

Web インターフェースのメイン ページに表示するカスタム タブを作成できます。タブ レコードを役割レコードに関連付けると、その役割に割り当てられたユーザがそのタブを使用できるようになります。

タブを作成するには

1. 「管理」タブで、「セキュリティと役割の管理」 - 「役割管理」 - 「タブ」を選択します。
「タブ リスト」ページが表示されます。
2. 「新規作成」をクリックします。
「タブの新規作成」ページが表示されます。
3. 以下のフィールドを指定します。

タブ名

管理インターフェース内でタブを識別する名前を指定します。たとえば、タブ名は「タブ リスト」ページに表示されます。

コード

システムがタブを識別するコードを指定します。

注: 一度定義したコードを変更することはできません。

レコードステータス

タブがアクティブであるか、非アクティブであることを示します。

表示名

ユーザ インターフェースでタブにグラフィカルに表示される名前を指定します。

開始ページ

ユーザがこのタブを選択したときにメイン ウィンドウに最初に表示される **Web** フォームを指定します。

重要: 開始ページとメニュー バーは同じフォーム グループに属している必要があります。 開始ページとメニュー バーが異なる [フォーム グループ \(P. 1405\)](#) に属しているタブを定義した場合、ユーザがタブにアクセスしたときにエラーが発生します。

メニュー バー

ユーザがこのタブを選択したときにメイン ウィンドウに表示されるメニュー バーを指定します。

[保存] をクリックします。

タブが作成されます。

メニュー バー レコードの作成

カスタマイズされたメニュー バーを作成して、ユーザ定義役割のシステム機能へのアクセスを制御できます。

メニュー バーを作成するには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [メニュー バー] に移動します。
[メニュー バー リスト] ページが表示されます。
2. [新規作成] をクリックします。
[メニュー バーの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

メニュー バー名

(必須) メニュー バーを識別する名前を指定します。 このフィールドを使用して、メニュー バーから使用できる機能を識別しやすくなります。

コード

(必須) 製品でメニュー バーを識別するコードを指定します。 一度定義したコードを変更することはできません。

レコード ステータス

メニュー バーがアクティブであるか、非アクティブであるかを示します。

HTMLPL 名

メニュー バーの定義を含む HTMLPL フォームの名前を指定します。
メニュー バーは Web Screen Painter を使用して設計されます。

説明

メニュー バーの説明です。この説明を使用して、このメニュー バーとそれを使用する役割を識別しやすくします。

[保存] をクリックします。

メニュー バーの定義が保存され、[メニュー バーの詳細] ページが表示されます。

Web フォーム レコードの作成

管理者は独自の Web フォームを作成し、タブの開始ページ、タブに表示するレポート、[実行] ボタンのリソース、または別の URL にすることができます。

Web フォームを作成する方法

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [Web フォーム] に移動します。
[Web フォーム リスト] ページが表示されます。
2. [新規作成] をクリックします。
[Web フォームの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

Web フォーム名

(必須) Web フォームを識別する名前を指定します。

レコード ステータス

このフォームがアクティブであるか、非アクティブであるかを示します。

コード

(必須) システムが Web フォームを識別するコードを指定します。一度定義したコードを変更することはできません。

注: このフィールドでは、Web スクリーン ペインタのマルチフレーム フォーム用に [プロパティ] タブの `web_form_name` を指定します。

タイプ

作成する Web フォームのタイプを指定します。

- **HTML ページ** -- 作成するいずれかのカスタム タブの開始ページとして使用する Web ページが表示されます。
- **レポート** - 任意のタブに表示される CA SDM レポートを指定します。
- **実行リソース** - 「[実行] ボタン」のリソースを指定します。
- **その他** - URL を使用してほかの外部の Web ページにアクセスします。

説明

Web フォームの説明を入力します。このフィールドを使用して、Web フォームの内容、表示場所、および目的をさらに詳しく説明します。

リソース

Web フォームを呼び出すコードを指定します。このコードには、コマンドライン コードまたは URL を使用できます。

例: 単純な html フォーム「`menu_tab_dflt.html`」を開きます。
`$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=menu_tab_dflt.html`

[保存] をクリックします。

メニュー ツリーのコピー

既存のメニュー ツリーをコピーして、カスタマイズされたメニュー ツリーの出発点として使用できます。

メニュー ツリーをコピーするには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [メニュー ツリー] を選択します。
[メニュー ツリー リスト] ページが表示されます。
2. コピーするメニュー ツリーをクリックします。
[メニュー ツリーの詳細] ページが表示されます。
3. [ファイル] - [コピー] をクリックします。
[メニュー ツリーの新規作成] ページが表示されます。
4. 以下のフィールドを指定します。

メニュー ツリー名

(必須)。このメニュー ツリーを識別するために割り当てる名前を指定します。

コード

(必須)。システムがメニュー ツリーを識別するコードを指定します。一度定義したコードを変更することはできません。

レコード ステータス

このメニュー ツリーがアクティブであるか、非アクティブであるかを示します。

説明

メニュー ツリーの説明を入力します。この説明を使用して、メニュー ツリーとそれを使用する役割に関する追加の詳細を示すことができます。

[保存] をクリックします。

新しいメニュー ツリーの [メニュー ツリーの詳細] ページが表示されます。

5. [メニューのカスタマイズ] をクリックします。
元のメニュー ツリーのコピーが表示されます。

6. 必要に応じてメニュー ツリーをカスタマイズします。

注: メニュー ツリー リソースの追加、削除、および編集については、オンライン ヘルプを参照してください。

メニュー ツリーの作成およびカスタマイズ

提供されているデフォルト メニュー ツリーのいずれかを基にして、メニュー ツリーを作成しカスタマイズできます。

メニュー ツリーを作成およびカスタマイズする方法

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [メニュー ツリー] を選択します。
[メニュー ツリー リスト] ページが表示されます。
2. [新規作成] をクリックします。
[メニュー ツリーの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

メニュー ツリー名

(必須) このメニュー ツリーを識別するために割り当てる名前。

コード

(必須) システムがメニュー ツリーを識別するコード。一度定義したコードを変更することはできません。

レコード ステータス

このメニュー ツリーがアクティブであるか、非アクティブであるかを示します。

説明

メニュー ツリーの説明です。この説明を使用して、メニュー ツリーとそれを使用する役割に関する追加の詳細を示すことができます。

4. [保存] をクリックします。
5. [メニューのカスタマイズ] をクリックします。

メニュー ツリーをカスタマイズできるフォームが表示されます。この時点では、メニュー ツリーには最上位ノードのみが存在し、その名前はメニュー ツリー名として入力した文字列になります。

6. メニュー ツリー内のノードを右クリックし、[ノードの新規作成] を選択します。

[ノードの新規作成] ページが表示されます。

7. 以下のフィールドを指定します。

ノード名

ノードの名前を入力します。この名前がメニュー ツリーに表示されます。

説明

ノードの説明を入力します。この説明を使用して、ノードの目的をさらに定義できます。

リソース

リソース名をフィールドに直接入力するか、検索アイコンをクリックしてリストからリソースを選択します。メニュー ツリー リソースによって、ユーザがメニュー ツリーからノードを選択したときに実行されるアクションが決まります。

8. メニュー ツリーに表示するノードのセットを作成するために必要なだけ、ステップ 6 および 7 を繰り返します。

注: メニュー ツリー リソースの追加、削除、および編集については、オンライン ヘルプを参照してください。

9. [保存] をクリックします。

メニュー ツリーの定義が保存され、[メニュー ツリーの詳細] ページが表示されます。

ヘルプ セットの作成および発行

定義した任意のカスタム 役割に対して、カスタム ヘルプ セットを作成できます。

ヘルプ セットを作成および発行するには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [ヘルプ セット] を選択します。

[ヘルプ セット リスト] ページが表示されます。

2. [新規作成] をクリックします。

[ヘルプ セットの新規作成] ページが表示されます。

3. 以下のフィールドを指定します。

ヘルプ セット名

このヘルプ セットの一意の名前です。

インターフェース タイプ

ヘルプ セットのインターフェース タイプ（アナリスト用、従業員用、顧客用など）です。

レコードステータス

ヘルプ セットがアクティブであるか、非アクティブであるかを示します。

ファイル名プレフィックス

このヘルプ セット用に生成されたヘルプ ファイルに付加するプレフィックスです。名前にはスペースを使用しないでください。

注: プレフィックスを割り当てるとヘルプ セットに属するファイルを識別できるようになるので、割り当てることをお勧めします。たとえば、アナリストのヘルプ セットのプレフィックスには「ANAL」などを使用できます。

内部

ユーザ定義ヘルプ セットの場合は自動的に [いいえ] に設定されます。このフィールドの値は変更できません。

4. [保存] をクリックします。

[コンテンツ] タブが表示されます。

5. [コンテンツの定義] をクリックします。
[選択したヘルプの更新] ウィンドウが開きます。

6. ヘルプセットに含めるコンテンツを選択します。

重要: トピックの中には必須のものがあり、これらは選択の有無にかかわらず新規ヘルプセットに含められます。たとえば、**CA SDM** ホーム ページなどの前付トピックは常に含められます。また、ネストされたトピックはそのコンテナ トピックに依存します。ネストされたトピックを含めると、そのコンテナ トピックが自動的に含められます。たとえば、「スコアボードの使用」トピックを選択した場合、そのヘルプセットを発行するとき、コンテナ トピック「**CA SDM** のナビゲート」が含められます。

7. [OK] をクリックします。
[選択したヘルプの更新] ウィンドウが閉じ、コンテンツのリストが [コンテンツ] タブに表示されます。

8. [発行] をクリックします。

これにより、選択したトピックをヘルプシステムにパッケージすることでヘルプセットが生成され、**Web** ブラウザで表示できるようになります。

9. 発行プロセスが完了するまでしばらく待機し、メニューバーから [表示] - [更新] を選択します。

[ヘルプを表示] ボタンがアクティブになります。

10. [ヘルプを表示] をクリックします。

カスタム ヘルプ セットがデフォルトの **Web** ブラウザに表示されます。

役割の切り替え

複数の役割を割り当てられているユーザは、ログアウトしてから再度システムにログインしなくても、役割を切り替えることができます。役割は、ユーザのアクセス タイプまたは連絡先レコードに割り当てられます。

注: 詳細については、「[ユーザ アカウントの設定 \(P. 373\)](#)」を参照してください。

役割を切り替えるには

1. CA SDM のメイン ページの右上隅にある [役割] ドロップダウン リストから目的の役割を選択します。
2. [役割の設定] をクリックします。

ログインしているユーザの現在の役割に応じて、Web インターフェースおよび使用可能な機能が変わります。

第 10 章：サポート ストラクチャの確立

このセクションには、以下のトピックが含まれています。

- [モデル](#) (P. 450)
- [CA Workflow](#) (P. 453)
- [CA Process Automation Workflow の統合](#) (P. 457)
- [共有コード](#) (P. 465)
- [ステータス コード](#) (P. 468)
- [タスク タイプ](#) (P. 473)
- [リクエスト/インシデント/問題領域](#) (P. 476)
- [変更要求と案件カテゴリ](#) (P. 481)
- [チケットの自動クローズ](#) (P. 488)
- [関連チケットアクティビティ](#) (P. 490)
- [優先順位計算](#) (P. 493)
- [ステータス遷移および従属属性のコントロール](#) (P. 513)
- [セルフ サービスのためのステータス遷移](#) (P. 524)
- [タイマ](#) (P. 529)
- [タイム ゾーン](#) (P. 530)
- [添付ファイルライブラリをセットアップする方法](#) (P. 533)
- [アナウンスメント](#) (P. 546)
- [ストアドクエリのセットアップ](#) (P. 548)
- [シーケンス番号](#) (P. 550)
- [監査ログの使用](#) (P. 551)
- [CA ネットワークとシステム管理の統合](#) (P. 551)
- [CA SDM Web ページの印刷](#) (P. 552)
- [Web インターフェイスでのレコード ロック動作](#) (P. 553)
- [サポート構造](#) (P. 554)
- [CAPA ヘルプの有効化](#) (P. 554)

モデル

CA SDM は、以下のサービス デスク モデルをサポートします。

- 内部モデル
- 外部モデル
- 結合モデル

注: Web インターフェースを使用して、選択したモデルを実装する方法の詳細については、オンライン ヘルプを参照してください。

内部モデル

内部サービス デスクの場合、会社が従業員に用意した製品やサービスを対象として、従業員の質問や問題に対してサポートを行います。CA SDM で以下のように内部サービス デスクを運用する場合、リクエストがサポートの基本単位です。

- リクエストとは、従業員の質問や問題に対応するためのチケットのことで、サポート組織が所有および管理しているインフラストラクチャに合わせて設計されます。
- 変更要求とは、サポート対象である業務インフラストラクチャの変更を管理するためのチケットです。内部サービス デスクは、多くの場合、第 1 のチケットとしてリクエストを使用しており、リクエストの結果としてインフラストラクチャの変更が必要になった場合に変更要求を添付することになります。

内部サービス デスクを運用する場合は、以下の操作を実行します。

- ニーズを満たしているかどうかを調べるには、Web インターフェースの管理機能を使用して、従業員のアクセス タイプを確認します。ほとんどの連絡先がサポートのためにサービス デスクを使用する従業員である場合、「従業員」を初期設定のアクセス タイプに設定できます。初期設定値として設定すると、サービス デスクでサポートする各従業員の連絡先に対してアクセス タイプを設定する手間が省けます。
- ニーズを満たしているかどうかを調べるには、Web インターフェースの管理機能を使用して、従業員の連絡先タイプを確認します。

- 連絡先が、適切なアクセス タイプと連絡先タイプに設定されていることを確認します。たとえば、初期設定のアクセス タイプとして従業員を設定する場合、アナリストのアクセス タイプとしてアナリストの連絡先も設定する必要があります。

連絡先タイプは通常、連絡先を作成する方法に基づいて自動的に割り当てられますが、状況によっては連絡先タイプが定義されない場合もあります。サポートを求めてサービス デスクを使用する従業員は従業員の連絡先タイプを持っている必要があります、サポート デスクのアナリストとして働く従業員はアナリストの連絡先タイプを持つ必要があります。

Web インターフェースの管理機能を使用して、連絡先を管理できます。

従業員をサポートする内部サービス デスクの場合、サポート構造は、従業員が作成するリクエストや変更要求と、これらのリクエストや変更要求をサポートする基本的な機能で構成されます。管理者は、サポート構造をセットアップします。

外部モデル

外部サービス デスクの場合、自社から製品またはサービスを購入したカスタマを対象として、製品またはサービスに関連した質問や問題に対してサポートを行います。**CA SDM** で外部サービス デスクを運用する場合、案件がサポートの基本単位です。案件とは、カスタマが購入した製品やサービスをサポートするために、カスタマの質問または問題に対応することを目的としたチケットのことです。

外部サービス デスクを運用する場合は、以下の操作を実行します。

- ニーズを満たしているかどうかを調べるには、**Web** インターフェースの管理機能を使用して、カスタマのアクセス タイプを確認します。ほとんどの連絡先がカスタマである場合、初期設定のアクセス タイプとして「カスタマ」を設定できます。
- ニーズを満たしているかどうかを調べるには、**Web** インターフェースの管理機能を使用して、カスタマの連絡先タイプを確認します。
- 連絡先が、適切なアクセス タイプと連絡先タイプに設定されていることを確認します。たとえば、初期設定のアクセス タイプとしてカスタマを設定する場合、アナリストのアクセス タイプに対応してアナリストの連絡先も設定する必要があります。

連絡先タイプは通常、連絡先を作成する方法に基づいて自動的に割り当てられますが、状況によっては連絡先タイプが定義されない場合があります。サポートを求めてサービス デスクを使用するカスタマはカスタマの連絡先タイプを持つ必要があり、サービス デスクを運営するアナリストはアナリストの連絡先タイプを持つ必要があります。

Web インターフェースの管理機能を使用して、連絡先を管理できます。

カスタマをサポートする外部サービス デスクの場合、サポート構造は、主にカスタマが作成する案件と、これらの案件をサポートする基本的な機能で構成されます。管理者は、本章の後半で説明する情報に基づいて、サポート構造をセットアップする必要があります。トピックごとに、ユーザのモデルに情報が適用されるかどうか記載されています。

結合モデル

会社によっては、内部と外部の両方のサービス デスク モデルを運用することが必要です。このような場合は、以下のいずれかの操作を実行します。

- 内部と外部のサービス デスク モデルを個別のサービス デスク インストールによって分離します。
- 両方のモデルをサポートするよう **CA SDM** をセットアップします。

内部サポートと外部サポートの境界線があいまいであり、サービス デスクのアナリストを従業員とカスタマの両方をサポートできるように訓練する場合は、このセットアップ方法が役に立ちます。たとえば、自社製品を購入した従業員がいる場合や、会社のインフラストラクチャに問題や疑問を抱えるカスタマがいる場合などが考えられます。

管理者は、案件、リクエスト、変更要求、およびこれらをサポートする基本的な機能で構成される内部と外部を結合したサービス デスクに対応するサポート構造をセットアップする必要があります。内部と外部のサービス デスクを結合したモデルを運用する場合は、サポート構造をセットアップする前に以下の操作を実行します。

- ニーズを満たしているかどうかを調べるには、**Web** インターフェースの管理機能を使用して、カスタマと従業員のアクセス タイプを確認します。ほとんどの連絡先がカスタマである場合、初期設定のアクセス タイプとして「カスタマ」を設定できます。ほとんどの連絡先がサポートのためにサービス デスクを使用する従業員である場合、「従業員」を初期設定のアクセス タイプに設定できます。

- ニーズを満たしているかどうかを調べるには、**Web** インターフェースの管理機能を使用して、カスタマと従業員の連絡先タイプを確認します。
- 連絡先が、適切なアクセス タイプと連絡先タイプに設定されていることを確認します。たとえば、デフォルトのアクセス タイプとしてカスタマを設定する場合、アナリストのアクセス タイプに対応してアナリストの連絡先も設定し、従業員のアクセス タイプに対応して従業員の連絡先も設定する必要があります。

通常、連絡先タイプは、その連絡先を作成した方法に基づいて以下のように自動的に割り当てられますが、場合によっては連絡先タイプが定義されないことがあります。

- サポートを求めてサービス デスクを使用するカスタマは、カスタマの連絡先タイプを持っている必要があります。
- サポートを求めてサービス デスクを使用する従業員は、従業員の連絡先タイプを持っている必要があります。
- サポートデスクのアナリストとして働く従業員は、アナリストの連絡先タイプを持っている必要があります。

Web インターフェースの管理機能を使用して、連絡先を管理できます。

関連項目：

[連絡先タイプ](#) (P. 376)

[アクセス タイプについて](#) (P. 413)

CA Workflow

CA Workflow プロセス定義は任意の **CA SDM チケットタイプ** (P. 72) と関連付けることができます。個々のチケットに適用されるプロセス定義は、そのチケットが割り当てられる変更カテゴリ、案件カテゴリ、またはリクエスト/インシデント/問題領域によって決まります。

CA Workflow プロセス定義がカテゴリまたは領域と関連付けられている場合、チケットがそのカテゴリまたは領域に割り当てられると、**CA Workflow** は定義からプロセス インスタンスを作成します。プロセス インスタンスの進捗状況は、チケットの [ワークフロー タスク] タブに表示されます。

CA SDM インストール時にオプションで **CA Workflow** をインストールしたり、オプションマネージャで以下のようないくつかのオプションを更新することで **CA Workflow** の別のインスタンスを使用するように **CA SDM** を指定することができます。

CAWF_USERNAME

CA Workflow に対してフルアクセス権（「IDE」と「プロセス」リソースへのアクセス権の付与）を持つ **CA EEM** ユーザを指定します。

CAWF_PASSWORD

`cawf_username` のパスワードを指定します。

CAWF_PM_LOCATION

ロケーションを指定します：`http://<サーバ>:8090/pm/`

CAWF_PM_URL

URL を指定します：

`http://<wf_hostname>:<wf_tomcat_port>/pm/services/pmService2`

CAWF_WL_LOCATION

ロケーションを指定します：`http://<サーバ>:8090/wl/`

CAWF_WL_URL

URL を指定します：`http://<server>:8090/wl/services/wlService`

これらのオプションは、**CA Workflow** に対するさまざまなエンドポイントを指定します。ほとんどの場合、**CA Workflow** のロケーションに一致するように、サーバとポートの値を更新することだけで済みます。

重要： **CA Workflow** サーバを変更すると、古いサーバ上のプロセス定義やプロセスインスタンスにリンクされている既存のカテゴリ、領域、またはチケットが使用できなくなります。

実行時の Workflow

チケットが、**CA Workflow** プロセス定義にリンクされたカテゴリまたは領域と共に保存されると、定義のインスタンスが作成されます。インスタンスの進捗状況は、チケットの「ワークフロータスク」タブに表示されます。**CA Workflow** にはブランチがあるため、完了したワーク項目と保留中のワーク項目だけが表示されます。

完了したワーク項目と保留中のワーク項目、およびワークフロー全体のステータスが、[ワークフロー タスク] タブに表示されます。[アクティビティ名] リンクをクリックすると、各ワーク項目の完了に使用する CA Workflow ワークリスト Web アプリケーションが表示されます。

[ワークフロー] タブのデータは、CA Workflow サーバから直接フェッチされます。CA Workflow サーバが使用できない場合は、エラーメッセージがタブに表示されます。

Workflow プロセス定義の選択

CA Workflow プロセス定義には、変更カテゴリ、案件カテゴリ、またはリクエスト/インシデント/問題領域とリンクする `usd_persid` という文字列属性が必要です。この属性は、入力パラメータとして設定する必要があります。CA SDM で CA Workflow インスタンスを起動すると、`usd_persid` がチケットの一意の ID である `persistent_id` に設定されます。`usd_persid` の用途の 1 つは、CA Workflow から CA SDM に Web サービス コールを行うことです。

重要: 変更カテゴリおよび案件カテゴリでは、CA SDM の内部 (古い) ワークフロー システムまたは CA Workflow アプリケーションのいずれかを使用できます。2 つを同時に使用することはできません。リクエスト/インシデント/問題領域は、CA Workflow アプリケーションのみを使用できます。古い内部ワークフロー システムでは、リクエスト、インシデント、または問題チケットがサポートされていません。

CA Workflow プロセス定義を選択する方法

1. 変更カテゴリまたは案件カテゴリを選択します。たとえば、変更カテゴリを選択するには、[管理] タブで [Service Desk]、[変更要求]、[カテゴリ] を選択します。
[変更カテゴリ リスト] ページが表示されます。
2. 編集する変更カテゴリのシンボルをクリックします。
[変更カテゴリの詳細] ページが表示されます。

3. [ワークフロー] タブで [CA Workflow を使用] ボタンをクリックします。

注: この手順を続行し、カテゴリを保存すると、カテゴリに添付されている CA SDM スタイル ワークフローが削除されます。

選択ページが表示され、使用可能な CA Workflow プロセス定義が一覧表示されます。

4. CA Workflow プロセス定義を 1 つ選択します。

[カテゴリ] に選択内容が入力されます。

5. [保存] をクリックします。

このカテゴリは、選択したプロセス定義で更新されます。

6. (オプション) カテゴリを編集し、CA Workflow 定義のハイパーリンクをクリックして、リンクしている CA Workflow プロセス定義を変更します。

プロセス定義の選択ページが表示されます。

注: CA Workflow プロセス定義が選択ページに表示されるのは、この定義に `usd_persid` という文字列属性がある場合のみです。定義で起動すると、この属性はチケットの `persistent_id` 値に設定されます。CA Workflow プロセス定義では、オプションで `label` という文字列入力パラメータを含めることができます。label を定義すると、その値がチケット番号に設定されます。チケット番号は、CA Workflow ワークリストに表示され、ワークアイテムのコンテキスト提供が容易になります。

ワークフロー タスク

ワークフロー タスクでは、特定のカテゴリまたは領域に関連付けられたチケットで完了する必要があるアクティビティを指定します。プロパティや、カテゴリまたは領域の他の側面と同様に、カテゴリを選択すると、タスクは自動的にチケットに追加されます。ワークフロー タスクを定義すると、以下の操作を実行できます。

- 完了するタスクのタイプの指定とその説明の入力
- 各タスクへのシーケンス番号の割り当て
- タスクを完了するユーザの指定
- 各タスクで使用できる特定の状態を割り当てて実行する、タスク解決の進捗状況の確認

タスクのステータスが変わるときに、特定の動作を実行できます。動作では、ワークフロー タスクが特定の状態になったときに開始する特定のタスクまたはプロセスを定義します。たとえば、動作を定義して、承認タスクが保留中ステータスになったときに特定のマネージャに電子メール通知を送信することができます。

注: ワークフロー タスクを作成する方法とタスクの動作を定義する方法については、オンライン ヘルプを参照してください。

CA Process Automation Workflow の統合

CA Process Automation は、企業 IT 環境内のハードウェアおよびソフトウェア管理タスクの自動化とトラッキングを行う機能を備えたスタンドアロン CA 製品です。CA Process Automation によって、タスクの自動化とユーザ間のやりとりの管理が可能になります（たとえば、実稼働環境内のコンプライアンスと正確性の承認および通知に関するもの）。

CA SDM および CA Process Automation を統合すると、CA SDM 内のキーポイントから CA Process Automation ワークフロー機能の利点を活用できます。CA SDM と CA Process Automation の統合を効果的なものにするには、両方の製品を理解する必要があります。

関連項目:

[CA Process Automation コンポーネント](#) (P. 458)

[実行時の CA Process Automation の CA SDM との統合](#) (P. 459)

[プロセス定義を作成する方法](#) (P. 460)

[開始リクエストフォームの作成](#) (P. 461)

[CA Process Automation プロセス定義の添付](#) (P. 463)

CA Process Automation コンポーネント

CA Process Automation は、CA Process Automation プロセス管理の一部として広範囲のアクティビティを促進する、複数の機能および構造を提供します。ただし、CA SDM との統合については、以下の CA Process Automation コンポーネントのみが CA Process Automation 統合に不可欠です。

- **プロセス定義** - さまざまな個人またはパーティによって開始および終了されるように、特定の順序で構成された集合的な一連のタスク、手順、および条件を識別します。このコンポーネントはすべての CA Process Automation コンテンツの中心基盤です。
- **開始リクエスト フォーム** - エンドユーザのための記述的情報が含まれているオブジェクト。開始リクエスト フォームではユーザにプロセス定義を提示する一方でプロセス定義の技術的詳細を非表示にします。
- **キーワード** - 開始リクエスト フォームに添付されている事前定義済みの語句のリスト。
- **自動化ライブラリ** - プロセス定義および開始リクエスト フォームを保存して表示する CA Process Automation 内の領域。
- **ライブラリ パスまたは参照パス** - 自動化ライブラリ内でプロセス定義および開始リクエスト フォームを編成して説明するフォルダ構造。
- **プロセス インスタンス** - プロセス定義の中で定義されているルールを実行するアクティブなエンティティ。プロセス定義状態が完了するまで、プロセス インスタンスは進行します。
- **プロセス インスタンスのログ メッセージ** - プロセス インスタンスのアクティビティの進捗状況を説明する設定可能な実行中のレコード。ログ メッセージカテゴリは CA SDM にとって CA Process Automation との統合に役立ちます。

注: CA Process Automation コンポーネントの定義の範囲は CA SDM 内の使用に制限されています。CA Process Automation コンポーネントおよび機能の詳細については、CA Process Automation ドキュメントを参照してください。

実行時の CA Process Automation の CA SDM との統合

統合を有効にすると、CA SDM ユーザは以下を経験することができます。

- [新規リクエスト]、[新規変更要求]、または[新規案件]で、CA Process Automation プロセス インスタンスがチケットのカテゴリまたは領域に基づいて開始します。概要情報は、すぐに[ワークフロー タスク] タブに表示されます。
- リクエスト領域、変更カテゴリ、または案件カテゴリが変更されると、添付された CA Process Automation プロセス インスタンスが終了して新しいプロセス インスタンスが開始します。
- CA Process Automation プロセス インスタンスがまだ終了していない場合、CA SDM ユーザがリクエスト、変更要求、または案件を閉じようと試行しても、ユーザはチケットを閉じることができません。代わりに、ユーザは最初にチケットをキャンセルする必要があります。キャンセルステータスは、チケットが閉じる前に CA Process Automation プロセス インスタンスを終了します。
- ユーザがチケットから移動せずに、プロセス インスタンスの状態を把握したい場合は、[チケットのワークフロー タスク] タブをクリックします。[ワークフロー タスク] タブは、プロセス インスタンスの開始日、終了日、現在の状態、およびプロセス インスタンスのパスを示すメッセージの現在の監査証跡を表示します。
- ユーザが全プロセスに関連のあるプロセス インスタンスの現在のパスを参照する場合、ユーザは[ワークフロー タスク] タブの[プロセスの表示] ボタンを選択します。[プロセスの表示] ボタンは、プロセス インスタンス全体のグラフィカルなスナップショットを起動し、現在のパスを表示します。
- ユーザがユーザアクションの待機中に CA Process Automation インタラクティブ リクエスト フォームを参照する場合、ユーザは[ワークフロー タスク] タブで任意のエントリを選択できます。[ワークフロー タスク] タブには、CA Process Automation タスク リストに表示されるプロセス インスタンス メッセージの監査証跡が含まれています。

注: ユーザが CA SDM の [プロセスの表示] ボタンまたは CA Process Automation プロセス インスタンス メッセージを選択すると、システムは単一のブラウザセッションに CA Process Automation ユーザ名とパスワードを入力するようにプロンプトを表示します。最初のプロンプトの後で、システムは CA SDM ブラウザが閉じるまで、ユーザに再度プロンプトを表示しません。

プロセス定義を作成する方法

プロセス定義を作成する場合は、CA Process Automation にコンテンツを追加して CA SDM に表示されるようにします。CA Process Automation グラフィカルプロセス デザイナを使用してプロセス定義の作成、テスト、およびチェックインを行います。CA SDM では、CA Process Automation プロセスを開始するマクロを作成することもできます。

注: CA Process Automation マクロの作成については、オンライン ヘルプを参照してください。

CA Process Automation でプロセス定義を作成するには、以下の手順に従います。

1. 管理ユーザとして CA Process Automation クライアントにログインします。
2. CA Process Automation グラフィカルプロセス デザイナを使用してプロセス定義の作成、テスト、およびチェックインを行います。プロセス定義を使用して作業を行う場合は、CA Process Automation ユーザ ドキュメントの手順を使用します。

注: プロセス定義を使用する前にチェックインに失敗した場合、ワークフローは CA SDM で正常に動作できません。

以下のプロセス定義アイテムは CA SDM で使用可能です。

プロセス名

[リクエスト領域]、[変更カテゴリ]、および [案件の詳細] ページに表示されます。プロセス名は、チケットの [ワークフロー タスク] タブにも表示されます。プロセス名は、アナリストおよびチケットを管理する他のユーザに CA SDM へのプロセス定義を説明します。

プロセス参照パス

[リクエスト領域]、[変更カテゴリ]、および [案件の詳細] ページに表示されます。プロセス参照パスは、[チケットのワークフロー タスク] タブにも表示されます。プロセス参照パスは、エンドユーザにプロセスの目的について説明する場合に役立ちます。たとえば、"/Processes/Approval" は有用ではありません。代わりに、"/Office Supplies/Approvals/Over-200-USD" のような参照パスは、200 米ドルを超える注文を管理するワークフローを説明します。

プロセス ログ メッセージ

[CA SDM チケットのワークフロー タスク] タブに表示されます。デフォルトでは、アクティビティのレコードはプロセス インスタンスと共に保存されます。プロセス ログ メッセージには [プロセス] カテゴリがあります。プロセス デザイナは、CA SDM チケットの [ワークフロー タスク] タブに表示するカスタム メッセージを作成できます。

注: ログ メッセージを管理する `caextwf_log_categories` オプションの設定については、「実装ガイド」を参照してください。

開始リクエストフォームの作成

開始リクエスト フォームを作成したら、プロセス定義に関連付けて、チェックインします。[開始リクエスト フォーム] プロパティに適切なキーワードを含めます。適切なキーワードが [開始リクエスト フォーム] プロパティにない場合は、開始リクエスト フォームおよびその関連するプロセス定義は CA SDM に表示されません。

開始リクエストフォームを作成する方法

1. 管理ユーザとして CA Process Automation クライアントにログインします。
2. CA Process Automation ライブラリを開き、開始リクエスト フォームのパスに移動します。

開始リクエスト フォームは CA Process Automation ライブラリの右ペインに表示されます。

3. リストから [開始リクエスト フォーム] を選択します。
ショートカット メニューが表示されます。
4. [プロパティ] を選択します。
[ライブラリ オブジェクトのプロパティ] ページが表示されます。
5. (オプション) [一般] タブをクリックし、開始リクエスト フォームの説明を変更します。CA SDM 管理者に開始リクエスト フォームおよび関連するプロセス定義の適切な使用条件を識別する説明を追加します。

6. [キーワード] タブをクリックします。
[キーワード] タブはアクティブです。
7. [ab+] アイコンをクリックします。
空のリストに行が追加されます。
8. 行をクリックします。
点滅するカーソルが行をハイライトし、行に入力できることを示します。
9. 以下の値のうちの 1 つを入力してキーワードを適切なチケット領域またはカテゴリに関連付けます。たとえば、開始リクエスト フォームを CA SDM リクエスト領域で使用できるようにするには、**pcat** キーワードを入力します。

チケット	使用キーワード
リクエスト領域	pcat
変更カテゴリ	chgcac
案件カテゴリ	isscat

10. 個々の適用可能なキーワードのリストに行を追加します。たとえば、リクエスト領域および変更カテゴリの両方に開始リクエスト フォームを表示するには、1 つの行を **chgcac** キーワードに追加してもう 1 つの行を **pcat** キーワードに追加します。
11. [OK] をクリックします。
CA Process Automation はキーワードと説明を保存し、[ライブラリ オブジェクトのプロパティ] ダイアログ ボックスを閉じます。
12. 開始リクエスト フォームをチェックインします。

注: 開始リクエスト フォームのチェックインに失敗した場合、フォームは CA SDM に表示されません。

CA Process Automation 開始リクエスト フォーム情報が CA SDM 開始リクエスト フォーム リストに表示されます。CA SDM 管理者は、CA SDM 開始リクエスト フォームを [リクエスト領域]、[変更カテゴリ]、または [案件カテゴリの詳細] ページでプロセス定義と関連付けることができます。

以下の開始リクエスト フォーム アイテムが CA SDM に表示されます。

開始リクエストフォーム名

[リクエスト領域]、[変更カテゴリ]、または [案件カテゴリ] リスト ページに表示されます。

開始リクエストフォームの参照パス

[リクエスト領域]、[変更カテゴリ]、または [案件カテゴリ] リスト ページに表示されます。

開始リクエストフォームの説明

[リクエスト領域]、[変更カテゴリ]、または [案件カテゴリ] リスト ページに表示されます。このフィールドでのテキストでは、開始リクエスト フォームが特定のリクエスト領域、変更カテゴリ、または案件カテゴリの選択に適切であることを説明します。

CA Process Automation プロセス定義の添付

CA Process Automation プロセス定義を CA SDM チケット領域またはカテゴリに添付する場合は、CA SDM チケット領域またはカテゴリと CA Process Automation プロセス定義との間に静的な接続を作成します。

CA SDM ユーザがチケットを作成または編集してチケット カテゴリを選択すると、関連する CA Process Automation プロセス定義はプロセス インスタンスで起動します。プロセス インスタンスについての関連情報はチケットの [ワークフロー タスク] タブに表示されます。

プロセス定義を添付する方法

1. [管理] タブで、[Service Desk] を選択します。
2. [チケット領域] または [カテゴリ] に移動します。
[領域] または [カテゴリ リスト] が表示されます。
3. チケット領域またはカテゴリを作成または編集します。
[更新] ページが表示されます。

4. [ワークフロー] タブをクリックします。

CA Process Automation オプションが CA SDM オプション マネージャにインストールされている場合、[ワークフロー] タブで [CA IT PAM を使用] ボタンを使用できます。

5. [CA IT PAM を使用] をクリックします。

[CA IT PAM 開始リクエスト フォーム リスト] が表示されます。リストの各行が CA Process Automation 開始リクエスト フォームです。

注: CA Process Automation、CA Workflow または CA SDM 内部ワークフローを使用して別のチケット領域またはカテゴリを管理することができます。ただし、1つのカテゴリが一度に使用できるのは1つのワークフロー ツールだけです。

6. [名前] 列の値をクリックしてこの開始リクエスト フォームに関連付けられたプロセス定義を選択します。

[CA IT PAM 開始リクエスト フォーム リスト] が閉じます。プロセス定義名およびプロセス定義参照パスが [ワークフロー] タブに表示されます。

7. [保存] をクリックします。

システムがプロセス設定を保存します。ユーザが指定されたチケット領域またはカテゴリで作成する次のチケットは、自動的にワークフローを添付し、プロセス インスタンスを作成します。[チケットのワークフロー タスク] タブに、プロセス インスタンス情報の概要が表示されます。さらに、ユーザは、[ワークフロー タスク] タブの [プロセスの表示] をクリックすることにより、プロセス インスタンスに関する追加情報にアクセスできます。

共有コード

CA SDM では、さまざまなタイプのチケットで特定の基本的なコード（優先度コード、重大度コード、影響コード、緊急度コードなど）を共通して使用します。リクエストと変更要求は同じコードを共有し、すべてのタイプのチケットはその他のコードを共有します。

共有コードについては、以下の情報を考慮します。

- デフォルトでは、コードのランク設定に数値が使用されますが、
- コードをカスタマイズすることもできます。
- ただし、共有コードの追加や削除はできません。
- 影響コード、優先度コード、重大度コード、および緊急度コードを使用できます。

サービス デスク モデルに基づいて、以下のコードをセットアップします。

共有コード	説明
優先度	すべてのサービス デスク モデルでセットアップする必要があります。
重大度	内部と結合のサービス デスク モデルでセットアップする必要があります。
影響度	内部と結合のサービス デスク モデルでセットアップする必要があります。
緊急度	内部と結合のサービス デスク モデルでセットアップする必要があります。

注: Web インターフェースの管理機能を使用してこれらのコードをカスタマイズする方法については、オンライン ヘルプを参照してください。

関連項目:

[優先度コード](#) (P. 466)

[重大度コード](#) (P. 466)

[影響コード](#) (P. 467)

[緊急度コード](#) (P. 467)

優先度コード

優先度コードは、サービス デスクがチケットに対応するランク順を示します（つまり、チケットの注意レベルを指定します）。優先度コードは、リクエスト、変更要求、および案件に指定します。したがって、これらはすべてのサービス デスク モデルに適用されます。

優先度を使用する場合、イベントを監視して、手動または自動でチケットをエスカレートすることができます。多くのサービス デスク インストールでは、優先度コードをスコアボードで使用して、アナリストにリクエストや変更要求のリアルタイム ステータスを通知します。

優先度コードにサービス タイプを割り当てると、優先度コードの指定時にチケットにサービス タイプが自動的に割り当てられます。この手順により、割り当てられた優先度に基づいて、チケットに特定レベルのサービスを関連付けることができます。たとえば、システム定義のサービス タイプ（4 時間解決）は、優先度 1 と自動的に関連付けられます。したがって、優先度 1 が割り当てられるチケットは、このサービス タイプに自動的に割り当てられます（4 時間解決サービス タイプと関連付けられたすべてのサービス タイプ イベントなど）。

関連項目：

[サービス レベル アグリーメント \(P. 293\)](#)

重大度コード

重大度コードは、リクエストの影響を受ける機器の障害の程度を示します。重大度コードは、リクエストのみに指定します。したがって、これらは内部と結合のサービス デスク モデルだけに適用されます。

注： 重大度が優先度の同義語として扱われていることがよくあります。サイトによっては、優先度のみを使用し、重大度をまったく使用していません。問題の技術的な深刻さ（重大度）と問題解決に要求される迅速性（優先度）を区別するには、重大度コードと優先度コードを使用します。

影響度コードの値は、インシデントの優先度の計算に役立ちます。

影響コード

影響コードは、システムの機能に対するチケットの影響の大きさを表します。たとえば、変更要求がシステム全体の機能に影響を与える場合、このチケットには大きな影響を表す値が割り当てられます。影響コードは、リクエストと変更要求のみに指定します。したがって、これらは内部と結合のサービス デスク モデルだけに適用されます。

注: 影響コードと[緊急度コード](#) (P. 467)は似ていますが、使用する目的が異なります。

緊急度コード

緊急度コードは、システム ユーザが送信するリクエストの重要性を表します(つまり、実稼動環境全体に対するリクエストの重要性を表します)。たとえば、リクエストに指定する障害によって会社の業務に悪い影響が及ぶ場合は、緊急度コードの値を [5- 即時] にします。緊急度コードは、リクエストのみに指定します。したがって、これらは内部と結合のサービス デスク モデルだけに適用されます。

緊急度コードと影響コードは異なる目的で使用しますが、これらは似ているために混同されることがよくあります。たとえば、中核的なデータ センターで起きた火事を報告するリクエストは、[3- 単一グループ] の影響と [5- 即時] の緊急度となる場合があります。火事は複数のグループに影響を与えますが、必ずしも組織全体に影響を与えるわけではないため、これらのコードが適用されます。データ センターは業務に不可欠であるので、即時処置が必要な緊急度となります。

ステータスコード

ステータスコードは、項目のステータスをトラッキングするために使用します。リクエスト、変更要求、案件、およびワークフロータスクは、それぞれ異なるステータスコードによって追跡されます。いずれの場合でも、必要に応じて使用できる定義済みのステータスコードがあります。また、定義済みのステータスコードを変更したり、サイトに固有な新しいコードを定義したりすることもできます。サービスデスクモデルに基づいて、以下のコードをセットアップします。

ステータスコード	説明
リクエスト	内部と結合のサービスデスクモデルでセットアップする必要があります。
変更要求	内部と結合のサービスデスクモデルでセットアップする必要があります。
案件	外部と結合のサービスデスクモデルでセットアップする必要があります。
タスク	すべてのサービスデスクモデルでセットアップする必要があります。

ステータスコードを使用すると、アナリストは進捗状況を注意深く追跡できるように、ステータスに基づいて情報の並べ替えや選択を行うことができます。ステータスコードを定義するときにコードを詳細に定義しておく、アナリストが実際に項目のステータスを指定するときに、より正確に状況を表現することができます。

ステータスコードは、アクティブまたは非アクティブとして設定できます。ステータスコードを非アクティブにすると、アナリストはこのコードを使用できなくなりますが、将来使用できるように設定はそのまま残されます（つまり、データベースからは削除されません）。後でステータスコードを使用することにした場合は、設定に戻ってアクティブに変更するだけで済みます。

注: リクエスト、インシデント、および問題チケットに同じ領域定義を使用できます。これらの領域は、[管理] タブではリクエスト/インシデント/問題の領域と呼ばれています。ここでは、略してリクエスト領域と呼びます。

リクエスト ステータス コード

以下の表で、リクエスト チケットの事前定義済みのステータス コードについて説明します。

リクエスト ステータス コード	説明
確認済み	リクエストの受信が確認されました。
クローズ	リクエストは完全に解決されました。
クローズ - 未解決	リクエストはクローズされましたが、引き続き解決する必要があります。
修正中	リクエストは修正のため保留中です。
保留	リクエストのサービス タイプ イベントは保留中です。
開く	リクエストは定義されており、完了の監視と管理のために使用されています。
問題-クローズ	問題リクエストは完全にクローズされました。
問題-修正済み	問題リクエストは修正されましたが、クローズされていません。
問題-オープン	リクエストは、問題として識別されました。
調査中	リクエストはオープンされましたが、追加の調査と分析のために保留中です。
作業中	リクエストを修正するための作業を実行中です。

リクエスト ステータスを識別するためにサイトで別の用語を使用している場合は、目的に合ったステータス コードを定義して定義済みのステータス コードを無視するか、または使用状況に合わせて定義を変更する必要があります。たとえば、以下のコードのように、追加のリクエスト ステータス コードを定義できます。

リクエスト ステータス コード	説明
重複	リクエストはオープンされましたが、ほかのユーザの既存のリクエストと重複している可能性があります。

ステータス コード

リクエスト ステータス コード	説明
Emergency	すぐに対応する必要がある重大なリクエストです。
レポート	リクエストは解決されてクローズされましたが、管理レベルでレポートする必要があります。
テスト	リクエストは解決されましたが、クローズするまで 1 週間テストする必要があります。

変更要求ステータス コード

以下の表で、変更要求チケットの事前定義済みのステータス コードについて説明します。

変更要求ステータス コード	説明
承認中	変更要求がオープンされ、承認を待っています。
承認済み	変更要求が承認されました。
キャンセル済み	変更要求がキャンセルされました。
クローズ	変更要求が完了しました。
保留	変更要求のサービス タイプ イベントは保留中です。
実装中	変更要求を実装しています。
開く	サービス要求は変更要求内で定義され、変更要求は完了の監視と管理のために使用されています。
拒否	変更要求が拒否されました。
解決日	変更要求が解決されました。
RFC	変更のリクエストが送信されました。
停止	変更要求のワークフロー タスクが停止しています。
確認中	変更要求を確認しています。
Backed Out	実装済み変更要求が取り消されました。
実装済み	変更は実装されました。

変更要求のステータスを識別するためにサイトで別の用語を使用している場合は、必要に応じたステータスコードを定義して定義済みのステータスコードを無視するか、使用状況に合わせて定義を変更する必要があります。たとえば、以下の表に示すように、追加の変更要求ステータスコードを定義できます。

カスタマイズされたリクエスト ステータスコード 説明	
重複	変更要求はオープンされましたが、ほかのユーザの既存の変更要求と重複している可能性があります。
Emergency	すぐに対応する必要がある重大な変更要求です。
レポート	変更要求は完了してクローズされましたが、管理レベルでレポートする必要があります。

クローズコード

クローズコードを使用して、成功または失敗などの変更要求の最終結果を定義します。クローズコードは手動で設定するか、変更要求のステータスがクローズ、完了、または解決済みになった場合にステータスの更新アクティビティの一部として設定します。

注: クローズコードの作成と定義および *require_closure_code* と *force_closure_code* オプションの詳細については、オンラインヘルプを参照してください。

案件ステータスコード

以下の表で、案件チケットの事前定義済みのステータスコードについて説明します。

案件ステータスコード	説明
承認 中	案件がオープンされ、承認を待っています。
キャンセル済み	案件がキャンセルされました。
クローズ	案件が完了しました。

案件ステータスコード	説明
保留	案件のサービス タイプ イベントは保留中です。
実装中	案件を実装しています。
開く	解決まで監視して管理できるように、案件を定義してオープンしました。
停止	案件のワークフロー タスクが停止しています。
トランザクション中	この案件に関してカスタマのトランザクションを実行しています。
確認中	案件を確認しています。

案件のステータスを識別するためにサイトで別の用語を使用している場合は、必要に応じたステータス コードを定義して定義済みのステータスコードを無視するか、使用状況に合わせて定義を変更する必要があります。たとえば、以下のように、追加の案件ステータス コードを定義できます。

カスタマイズされた案件ステータスコード	説明
重複	案件はオープンされましたが、ほかのユーザの既存の案件と重複している可能性があります。
Emergency	すぐに対応する必要がある重大な案件です。
レポート	案件は完了してクローズされましたが、管理レベルでレポートする必要があります。

タスクステータスコード

タスクステータスコードは、ワークフロー タスクのさまざまな状態を表します。これは、チケットステータスとは別に、案件または変更要求ワークフローの各タスクの状態を表すステータス情報です。ワークフロー タスクを使用すると、アナリストは、チケット内の各タスクの完了にかかった時間をトラッキングできます。

以下の表で、ワークフロー ステータスの事前定義済みのステータス コードについて説明します。

タスクステータスコード	説明
承認	タスクが承認されました。
キャンセル済み	タスクがキャンセルされました。これ以上更新できません。
完了	タスクが完了しました。
保留中	タスクが開始されました。
拒否	タスクが拒否されました。
再オープン	タスクが再オープンされました。
再オープン- 待機	以前のタスクが再オープンされました。
スキップ	タスクがスキップされました。
待機	タスクは開始されていません。

ワークフロー タスクのステータスを識別するためにサイトで別の用語を使用している場合は、必要に応じたステータス コードを定義して定義済みのステータス コードを無視するか、使用状況に合わせて定義を変更する必要があります。

各タスク ステータス コードに対しては、タスクがこの状態に達したときに開始する動作のタイプを割り当てることができます。これより、タスクの完了に向けて、進捗状況のより詳細な情報が提供されます。また、蓄積関数を使用して、チケットの完了に必要な時間とコストをトラッキングすることもできます。

タスクタイプ

タスク タイプをセットアップすると、特定のワークフロー タスクの動作とタスク ステータス コードを決定するのが容易になります。タスクの各タイプに対して特性を定義するために、使用できるタスク ステータスコードや特定の状態を指定できます。

変更要求と案件の両方でワークフロー タスクを使用するため、どのサービス デスク モデルにもタスク タイプをセットアップします。タスク ステータス コードは、各タスクに関連付ける動作を特定します。たとえば、有効な状態として承認、拒否、保留中、待機を使用できるように承認タスク タイプを設定できます。承認タスク タイプが保留中の状態になった場合、特定のマネージャやアナリストなどに通知を送信できるようになります。

タスク タイプは、アクティブまたは非アクティブとして設定できます。タスク タイプを非アクティブにすると、アナリストはこのコードを使用できなくなりますが、将来使用できるように設定はそのまま残されます（データベースからは削除されません）。タスク タイプを後で使用する場合は、アクティブとしてもう一度マークします。

注: Web インターフェースの管理機能を使用して、[タスク タイプ リスト] ページに、定義済みのタスク タイプを表示できます。

例: タスクステータスコード

以下の表に、ステータス コードの例をいくつか示します。

タスク ステータス コード	説明
承認	チケットを承認または拒否します。
グループ タスクの終了	グループ タスクを終了します。
グループ タスクの開始	グループ タスクを開始します。
承認の開始	チケットの開始を承認します。

この例では、グループ タスクの開始とグループ タスクの終了の 2 つのタイプは、完了する必要がある案件/変更カテゴリ内にタスクのグループを定義します。グループ内のタスクは、どのような順序でも実行できます。グループ タスクの開始が保留中の状態になると（開始済み）、このグループ内のタスクもすべてこの状態になります。

注: タスク タイプの使用方法については、オンライン ヘルプを参照してください。

インシデント トラッキングによって、アナリストはインシデントに対して1つ以上のフラグを選択してインシデントを追跡できます。アナリストが指定した情報から、レポートするインシデントの評価基準が提供されます。たとえば、アナリストはインシデントが誤って割り当てられたことを示すことができます。レポートで誤って割り当てられたチケットの割合が多い場合、組織は割り当てを調整する必要があることがわかります。

たとえば、アナリストは組織が以下のような処理を行うための情報を指定できます。

- SLA 対応を改善し、サポート組織の低いレベルで解決することができます。
- 間違って割り当てられているチケットを識別します。
- 解決にリモート制御ツールが使用されたチケットを把握できます。

efficiency_tracking オプション マネージャ オプションをインストールすることによって、アナリストはインシデントの詳細ページの「効率性トラッキング」タブに表示されるトラッキング オプションを使用できるようにします。

注: インシデント トラッキングの詳細については、オンライン ヘルプを参照してください。

インシデントトラッキングのインストール

インシデントに特定のフラグを設定し、アナリストがインシデントを追跡できるオプションをインストールできます。アナリストが指定する情報は、レポート用インシデントに関するメトリックを組織に提供します。オプションをインストールすると、トラッキング フラグが「インシデント 詳細」ページの「効率性トラッキング」タブに表示されます。

インシデントトラッキングをインストールするには、以下の手順に従います。

1. 「管理」タブで、「オプション マネージャ」-「リクエスト マネージャ」を参照します。

「オプション リスト」が表示されます。

2. **efficiency_tracking** をクリックします。

デフォルト値が設定された「**efficiency_tracking** オプションの詳細」ページが表示されます。

3. [編集] をクリックします。

デフォルト値が設定された[`efficiency_tracking` オプションの更新] ページが表示され、[説明] を編集することができます。

4. [インストール] をクリックします。

[`efficiency_tracking` オプションの詳細] ページが表示されます。

5. [ウィンドウを閉じる] をクリックします。

インシデント トラッキングがインストールされました。ただし、[効率性トラッキング] タブはインシデント詳細ページ上には表示されません。

6. CA SDM を再起動します。

[効率性トラッキング] タブはインシデント詳細ページ上に表示されます。

リクエスト/インシデント/問題領域

リクエスト領域では、リクエスト、インシデント、問題のチケットを分類できる論理グループを定義します。たとえば、アプリケーションに関連するチケットは事前定義済みアプリケーション領域に割り当てることができます。アナリストがチケットをリクエスト領域に割り当てると、そのリクエスト領域に関連付けられた情報がすべてチケットに自動的に入力されます。たとえば、サービス タイプを指定した場合、チケットおよびそれに関連するすべてのサービス タイプ イベントに、このサービス タイプが関連付けられます。

注: リクエスト、インシデント、および問題チケットに同じ領域定義を使用できます。これらの領域は、CA SDM の [Web Interface Administration] タブではリクエスト/インシデント/問題の領域と呼ばれています。ここでは、略してリクエスト領域と呼びます。

リクエスト領域のステータスは、アクティブまたは非アクティブに設定できます。リクエスト領域を非アクティブにすると、アナリストが使用できなくなりますが、データベースからは削除されません。後でリクエスト領域を使用する場合は、ステータスをアクティブに戻すだけです。

リクエスト領域を使用すると、以下の操作を実行できます。

- チケットのグループや担当者のフィールドにデフォルト値を指定します。
- デフォルトのサービス タイプをリクエスト領域に割り当てることによって、チケットにサービスのレベルを自動的に関連付けます。
- 調査をリクエスト領域に関連付けます。
- 独自のカスタム リクエスト領域を定義することによって、領域単位でチケットを選択し、レポートを作成します。最終的にリクエストの傾向を研究し、問題の原因を分析します。表示を特定の分類に集中させることで、このような研究結果をさらに効果的に活用し、意義のあるものにすることができます。

以下の定義済みのリクエスト領域が **CA SDM** と共にインストールされます。

- アプリケーション
- 電子メール
- ハードウェア
- ネットワーク
- プリンタ
- ソフトウェア

ソフトウェアは、さらにいくつかのリクエスト領域に分類されます。

注: リクエスト領域の定義と編集については、オンライン ヘルプを参照してください。

関連項目:

[\[リクエスト/インシデント/問題領域\] プロパティ \(P. 478\)](#)
[セルフ サービスのリクエスト/インシデント/問題領域の定義 \(P. 480\)](#)

[リクエスト/インシデント/問題領域]プロパティ

プロパティを使用して、特定のリクエスト領域にカスタムの属性または特性を追加できます。プロパティをリクエスト領域に追加した場合は、アナリストがチケットをその領域に割り当てると、関連付けられたプロパティがチケットの「プロパティ」タブに自動的に表示されます。たとえば、プロパティを定義済みの電子メールリクエスト領域に追加して、電子メールサーバまたはメールボックス サイズを指定できます。

プロパティを定義するときに、値を必須にするか省略可にするかを指定できます。[必須の値が含まれるプロパティ \(P. 478\)](#)の場合、ユーザは値を入力してから（またはデフォルト値をそのまま使用して）チケットを保存する必要があります。

既存のチケットを別のリクエスト領域に割り当てた場合の動作は、**keep_tasks** オプションによって決まります。

- **keep_tasks** がインストールされていない場合、既存のプロパティ（およびワークフロー タスク）がチケットから削除され、新たに割り当て先となったリクエスト領域に関連付けられているプロパティまたはタスクが追加されます。
- **keep_tasks** がインストールされている場合、既存のプロパティおよびタスクがチケットに保持され、新たに割り当て先となったリクエスト領域に関連付けられているプロパティまたはタスクが追加されます。

注: プロパティをリクエスト領域に追加し、プロパティの検証ルールを定義する方法については、オンラインヘルプを参照してください。

プロパティ検証ルール

事前定義した値のセットにプロパティ値の入力を制限する検証ルールを定義できます。たとえば、「オペレーティング システム」というプロパティを定義した場合、**Windows**、**UNIX**、および **Linux** が選択肢として含まれているドロップダウン リストを検証ルールとして定義できます。

検証ルールなしで定義されたプロパティは、自由形式のテキスト ボックスとしてユーザに表示され、任意のテキスト文字列を入力できます。検証ルールを指定することで、領域およびカテゴリ値に関するレポートの複雑性やエラーの発生が軽減されます。

注: プロパティの検証ルールは再利用可能です。特定のプロパティに固有のものではありません。既存の検証ルールはすべて、変更カテゴリ、案件カテゴリ、またはリクエスト/インシデント/問題領域で定義されたプロパティに適用できます。

プロパティが添付されているカテゴリまたは領域にユーザがチケットを割り当てると、そのプロパティに設定した検証ルールのタイプに応じて、以下のコントロールの1つがチケットの「プロパティ」タブに表示されます。

- テキスト編集ボックス - 定義済みの検証ルールはありません。また、デフォルト値は指定できません。表示された例に従って値を入力する場合などが想定されます。
- チェックボックス - オン/オフで状態を指定するチェックボックスが「プロパティ」タブに表示されます。デフォルトでは、チェックマークが付いていません。ユーザはデフォルトを使用するか、チェックボックスをオンにできます。チェックマークが付いているボックスは、チケットの詳細ページに表示され、「値」列に「はい」が入力されます。オフのボックスは、「値」列に「いいえ」が表示されます。
- ドロップダウンリスト - 事前定義されたオプションのセットが含まれたドロップダウンリストが、「プロパティ」タブに表示されます。デフォルト値を定義した場合、ドロップダウンリストを初めて表示すると、そのデフォルト値が選択されます。ユーザが選択したオプションは、チケットの詳細ページの「値」列に表示されます。

セルフ サービスのリクエスト/インシデント/問題領域の定義

「セルフ サービスに含める」オプションでは、セルフ サービスのチケットに含めるリクエスト/インシデント/問題の領域を定義できます。また、アナリストに表示されるセルフ サービス シンボルとは異なるセルフ サービス シンボルを定義することもできます。チケットが保存されると、セルフ サービス シンボルは「リクエスト/インシデント/問題領域」フィールドに表示されます。チケットがアナリスト インターフェースに表示される場合は、領域の通常のシンボルが表示されます。セルフ サービス ユーザは、シンボルを編集することが許可されていません。シンボルは読み取り専用です。

セルフ サービスのリクエスト/インシデント/問題領域を定義するには、以下の手順に従います。

1. 「管理」タブで、「Service Desk」 - 「リクエスト/インシデント/問題」 - 「領域」を選択します。

「リクエスト/インシデント/問題領域リスト」が表示されます。

2. 「リスト内で編集」を選択します。

ページの上部に、編集可能なフィールドが表示されます。

3. 「シンボル」リストで編集する任意のインシデント/問題/リクエスト領域を開きます（Hardware.pc.install など）。

4. 以下のフィールドを指定します。

セルフ サービスに含める

このリクエスト/インシデント/問題領域をセルフ サービス インターフェースに表示するかどうかを示します。

セルフ サービス シンボル

セルフ サービス インターフェースのこのリクエスト/インシデント/問題領域に一意的識別子を指定します。

アクティブ

リクエスト/インシデント/問題領域がアクティブか非アクティブかを指定します。

リクエスト/インシデント/問題領域はセルフ サービスに対して定義されます。

5. 「保存」をクリックします。

リストを再表示すると、更新されたリクエスト/インシデント/問題領域が [リクエスト/インシデント/問題領域リスト] に表示されます。

変更要求と案件カテゴリ

変更カテゴリと案件カテゴリでは、変更要求と案件を整理できる論理的なグループ分けが定義されます。

注: リクエスト/インシデント/問題領域と異なり、変更要求カテゴリおよび案件カテゴリは以下のように別々に管理されます。

- 変更カテゴリは、内部および結合 CA SDM モデルに対してセットアップします。
- 案件カテゴリは、外部および結合 CA SDM モデルに対してセットアップします。

カテゴリを使用して、チケットの特定フィールドに初期設定値を指定できます。初期設定のサービス タイプをカテゴリに割り当てることで、チケットにサービスのレベルを自動的に関連付けることができます。また、調査とカテゴリの関連付けも実行できます

各カテゴリを対象として、チケットと関連付ける属性や特性を指定できます。また、チケットへの対応に必要なタスクをすべて指定したワークフローを作成できます。ワークフロー タスクに関連付けられる動作を定義すると、タスクのステータスが変更されたときや、アクティビティがチケットをクローズしたときに、主要な担当者に通知できるようになります。

アナリストがチケットをカテゴリに割り当てると、そのカテゴリに関連付けられた情報がすべてチケットに自動的に入力されます。たとえば、サービス タイプを指定した場合、チケットおよびそれに関連するサービス タイプ イベントに、このサービス タイプが関連付けられます。

注: カテゴリの定義と編集については、オンライン ヘルプを参照してください。

関連項目:

[事前定義済み変更カテゴリ](#) (P. 482)

[事前定義済み案件カテゴリ](#) (P. 482)

[チケットのカテゴリを変更する場合のルール](#) (P. 483)

[カテゴリのプロパティ](#) (P. 484)

[セルフ サービスに変更および案件カテゴリを定義する](#) (P. 487)

事前定義済み変更カテゴリ

以下の定義済み変更カテゴリのセットが CA SDM と共にインストールされます。

- 追加
- Change
- 移動
- Retire

注: これらのすべてのカテゴリ セットは、さらに具体的なカテゴリに細分されます。たとえば、変更カテゴリのセットには、サーバとワークステーションを変更するためのカテゴリが含まれます。

事前定義済み案件カテゴリ

以下の定義済みの案件カテゴリ CA SDM と共にインストールされます。

- Hardware.pc.install
- Software.pc.install

任意のカテゴリのステータスを、アクティブまたは非アクティブとして設定できます。カテゴリを非アクティブにすると、アナリストはこのコードを使用できなくなりますが、データベースからは削除されません。後でカテゴリを使用する場合は、ステータスをアクティブに変更します。

チケットのカテゴリを変更する場合のルール

以下のルールはワークフロー タスクにのみ影響します。

- 古いカテゴリで **CA Workflow** または **Classic Workflow** を使用し、新しいカテゴリで **CA Process Automation** を使用する場合、**CA Process Automation** のプロセス定義は **CA Process Automation** サーバ上のワークフローにリンクされます。
- 古いカテゴリと新しいカテゴリの両方で **CA SDM** ワークフローを使用する場合、以前のリリースのルールが適用されます。
- 新しいカテゴリで **CA Workflow** または **CA Process Automation** を使用し、古いカテゴリで **CA SDM** ワークフローを使用する場合は、以下のようになります。
 - 未完了または保留中の状態にある **CA SDM 6.0** スタイルのワークフロー タスク（更新可能なタスク）はすべて、**KEEP_TASKS** オプションの設定に関係なく、キャンセル ステータスに設定されます。完了したワークフロー タスクはそのまま残されますが、再オープンすることはできません。
 - 未完了かつ非アクティブの状態にあるタスク（待機ステータスになっているタスクなど）はすべて削除されます。
 - **CA Workflow** または **CA Process Automation** 定義のインスタンスが作成されます。
- 新しいカテゴリで **CA SDM** ワークフローを使用し、古いカテゴリで **CA Workflow** または **CA Process Automation** を使用する場合は、以下のようになります。
 - **CA Workflow** または **CA Process Automation** インスタンスは、強制的に終了ステータスに設定されます。
 - 新しいカテゴリのワークフロー タスクは、通常どおりに追加されます。

- 古いカテゴリと新しいカテゴリの両方で **CA Workflow** を使用する場合は、以下のようになります。
 - 古いカテゴリと新しいカテゴリで同じプロセス定義を指定している場合は、以前のカテゴリのインスタンスが引き続き実行されます。
 - 古いカテゴリと新しいカテゴリで異なるプロセス定義を指定している場合、古いインスタンスは終了ステータスに設定され、新しいカテゴリからインスタンスが作成されます。

CA SDM ワークフローでは、実行中の **CA Workflow** または **CA Process Automation** インスタンスのチケットはクローズできません。 **CA Workflow** を使用するチケットでは、蓄積、優先処理、およびタスクの挿入の機能が無効になります。

カテゴリのプロパティ

プロパティは、特定のカテゴリにカスタムの属性または特性を追加するのに使用します。 プロパティをカテゴリに追加した場合は、アナリストがチケットをそのカテゴリに割り当てると、関連付けられたプロパティがチケットの [プロパティ] タブに自動的に表示されます。

たとえば、メモリ サイズやプロセッサ タイプなどを指定するには、定義済みのソフトウェア.PC.インストール案件カテゴリにプロパティを追加します。

プロパティを定義する際、値の入力を必須にするかどうかを指定できます。 必須の値が含まれるプロパティの場合、ユーザは値を入力してから（またはデフォルト値をそのまま使用して）チケットを保存する必要があります。

カテゴリ プロパティの保存

既存のチケットを別のカテゴリに割り当てた場合の動作は、**keep_tasks** オプションによって決まります。

- **keep_tasks** がインストールされていない場合、既存のプロパティおよびワークフロー タスクがチケットから削除され、新たに割り当て先となったカテゴリに関連付けられているプロパティまたはタスクが追加されます。

- **keep_tasks** がインストールされている場合、既存のプロパティおよびワークフロー タスクがチケットで保持され、新たに割り当て先となったカテゴリに関連付けられているプロパティまたはタスクが追加されます。

注: プロパティを変更カテゴリまたは案件カテゴリに追加し、プロパティの検証ルールを定義する方法については、オンライン ヘルプを参照してください。

プロパティ検証ルール

事前定義した値のセットにプロパティ値の入力を制限する検証ルールを定義できます。たとえば、「オペレーティング システム」というプロパティを定義した場合、**Windows**、**UNIX**、および **Linux** が選択肢として含まれているドロップダウン リストを検証ルールとして定義できます。

検証ルールなしで定義されたプロパティは、自由形式のテキスト ボックスとしてユーザに表示され、任意のテキスト文字列を入力できます。検証ルールを指定することで、領域およびカテゴリ値に関するレポートの複雑性やエラーの発生が軽減されます。

注: プロパティの検証ルールは再利用可能です。特定のプロパティに固有のものではありません。既存の検証ルールはすべて、変更カテゴリ、案件カテゴリ、またはリクエスト/インシデント/問題領域で定義されたプロパティに適用できます。

プロパティが添付されているカテゴリまたは領域にユーザがチケットを割り当てると、そのプロパティに設定した検証ルールのタイプに応じて、以下のコントロールの 1 つがチケットの [プロパティ] タブに表示されます。

- テキスト編集ボックス - 定義済みの検証ルールはありません。また、デフォルト値は指定できません。表示された例に従って値を入力する場合などが想定されます。
- チェック ボックス - オン/オフで状態を指定するチェック ボックスが [プロパティ] タブに表示されます。デフォルトでは、チェックマークが付いていません。ユーザはデフォルトを使用するか、チェックボックスをオンにできます。チェックマークが付いているボックスは、チケットの詳細ページに表示され、[値] 列に [はい] が入力されます。オフのボックスは、[値] 列に [いいえ] が表示されます。

- ドロップダウン リスト - 事前定義されたオプションのセットが含まれたドロップダウン リストが、[プロパティ] タブに表示されます。デフォルト値を定義した場合、ドロップダウン リストを初めて表示すると、そのデフォルト値が選択されます。ユーザが選択したオプションは、チケットの詳細ページの [値] 列に表示されます。

セルフ サービスに変更および案件カテゴリを定義する

〔セルフ サービスに含める〕 オプションを使用してセルフ サービスのチケットに含める変更および案件カテゴリを定義します。 また、アナリストに表示されるセルフ サービス シンボルとは異なるセルフ サービス シンボルを定義することもできます。 チケットが保存されると、セルフ サービス シンボルが〔変更（または案件）カテゴリ〕 フィールドに表示されます。 チケットがアナリスト インターフェースに表示される場合は、カテゴリの通常のシンボルが表示されます。

セルフ サービスに変更（または案件）カテゴリを定義する方法

1. 〔管理〕 タブで、〔Service Desk〕 - 〔変更要求（または案件）〕 - 〔カテゴリ〕 を選択します。
〔カテゴリ リスト〕 ページが表示されます。
2. 〔リスト内で編集〕 を選択します。
ページの上部には、編集可能なフィールドが表示されます。
3. 〔シンボル〕 リストから目的の役割を選択します。
4. 以下のフィールドを指定します。

セルフ サービスに含める

このカテゴリをセルフ サービス インターフェースに表示するかどうかを指定します。

デフォルト : Yes

セルフ サービス シンボル

セルフ サービス インターフェースのこのカテゴリに一意の識別子を指定します。

アクティブ

カテゴリがアクティブであるか、非アクティブであるかを指定します。

カテゴリはセルフ サービスに対して定義されます。

5. 〔保存〕 をクリックします。
リストを再表示すると、更新されたカテゴリが〔変更（または案件）カテゴリ リスト〕 に表示されます。

チケットの自動クローズ

構成可能な設定を使用してチケット（リクエスト/インシデント/問題、変更要求、または案件）の自動クローズを行うことができます。チケットが「解決済み」ステータスに設定されると、チケットは指定された営業時間数内に自動的にクローズされます。チケットがクローズされる前に、エンドユーザーに送信された「自動クローズ」アクティビティ通知に営業時間数が表示されます。この時間数は変更可能で、テナントに固有です。設定可能な時間数が終わる前にステータスが変わると、チケットのクローズがキャンセルされます。

管理者は、以下のアクションを実行できます。

- 「自動クローズ」チケット設定を定義して、エンドユーザーに対して、チケットが自動的にクローズするまでの営業時間数を制御します。
- 「自動クローズ」アクティビティ通知を設定して、チケットに自動クローズがスケジュールされると、適切な連絡先に通知するようにします。

マルチテナンシーを使用する場合は、以下を考慮します。

- システムは、テナントに固有の自動クローズ設定が検索されない場合、デフォルトのパブリックの自動クローズを使用します。
- 各テナントに1つの自動クローズ設定があります。

注: これらの手順の実行に関する詳細情報については、[オンラインヘルプ](#)の自動クローズ設定の情報を参照してください。

関連項目:

[自動クローズチケット設定を定義する方法](#) (P. 489)

[自動クローズアクティビティ通知を定義する方法](#) (P. 490)

自動クローズ チケット設定を定義する方法

チケットが閉じる（すべてのチケット タイプ）までの営業時間数を定義するには、以下のようにします。

1. [管理] タブで、[Service Desk] - [アプリケーション データ] - [コード] - [自動クローズ] を選択します。
2. リスト ページで [新規作成] をクリックします。
3. 詳細ページで以下のフィールドを指定します。

シンボル

システム設定名を定義します。

リクエスト/インシデント/問題/変更要求/案件

チケットが解決済みステータスに設定されてからチケットが閉じられるまでの営業時間数を定義します。その時間数が終了する前にステータスが変更された場合、チケットのクローズはキャンセルされます。0（ゼロ）時間は、自動クローズがチケット タイプに実装されないことを示します。

説明

レコードの簡単な説明が表示されます。

ステータス

レコードがアクティブであるか、非アクティブであるかを指定します。

自動クローズ設定が定義されます。

4. [保存] - [ウィンドウを閉じる] をクリックします。

リストを再表示すると、新しい設定が [自動クローズ リスト] ページに表示されます。

自動クローズ アクティビティ通知を定義する方法

デフォルトの自動クローズ アクティビティ通知の設定を変更し、自動クローズがチケットにスケジュールされた場合は適切な連絡先を通知することができます。アクティビティはすべての **CA SDM** チケット タイプに有効で、リクエスト/インシデント/問題、変更要求および案件のデフォルトの通知ルールが含まれています。

自動クローズ アクティビティ通知を定義するには、以下の手順に従います。

1. [管理] タブで、[通知] - [アクティビティ通知] を選択します。
2. リスト ページで [自動クローズ アクティビティ通知] を選択して開きます。
3. デフォルトの自動クローズ通知ルールを更新し、通知を受信する連絡先を指定します。
4. [保存] - [ウィンドウを閉じる] をクリックします。

更新された自動クローズ アクティビティ通知は、リストを再表示したときに [アクティビティ通知リスト] に表示されます。

関連チケット アクティビティ

アクティビティが **CA SDM** チケットに生成された場合、アクティビティを 1 つ以上の関連チケットに伝達できます。たとえば、インシデントから作成されている問題レコードは、問題が解決されたときにインシデントレコードを更新できます。アクティビティが発生すると、アクティビティ ログは以下の情報が含まれる関連チケットに生成されます。

- 関連チケット アクティビティ タイプ (ステータスの更新など)
- 連絡先名
- 親チケット タイプおよびその参照番号
- アクティビティ ログの説明 (進行中からオープンに更新されたステータスなど)

アクティビティ ログは、各アクティビティ通知内に設定されたプロパティに基づいて、関連チケットに伝達されます。 関連チケットの属性は変更されません。 以下の関係が伝達されます。

- 問題はすべてのアクティブなインシデントに伝達されます。
- 変更要求はすべてのアクティブな問題およびインシデントに伝達されます。

システム管理者として、以下のアクションを実行できます。

- アクティビティ通知を設定して関連チケット アクティビティを伝達します。
- 関連チケット アクティビティ通知を設定し、アクティビティが関連チケットに伝達される場合は、適切な連絡先を通知します。

注: これらの手順の実行に関する詳細情報については、オンラインヘルプのアクティビティ通知情報を参照してください。

関連項目:

[アクティビティのログ記録](#) (P. 580)

[関連チケットにアクティビティ通知を定義する方法](#) (P. 492)

[関連チケット アクティビティ通知を定義する方法](#) (P. 493)

関連チケットにアクティビティ通知を定義する方法

各アクティビティ通知に設定されたプロパティに基づいて関連チケットにアクティビティ ログを伝達することができます。 関連チケットの属性は変更されません。

関連チケット アクティビティにアクティビティ通知を定義するには、以下の手順に従います。

1. [管理] タブで、[通知] - [アクティビティ通知] を選択します。
2. 編集する適切なアクティビティ通知を開きます。
3. 詳細ページで、[関連チケット アクティビティ] チェック ボックスをクリックしてアクティブのマークを付けます。

注: マルチテナンシーを使用する場合は、以下の手順に従います。

- [関連チケット アクティビティ] ドロップダウン リストから適切なテナント タイプを指定します。
 - [テナント] フィールドにテナント名を入力するか、検索アイコンをクリックしてテナントを検索します。
4. (オプション) デフォルトの通知ルールを更新し、通知を受信する連絡先を指定します。
 5. [保存] - [ウィンドウを閉じる] をクリックします。

更新されたアクティビティ通知は、リストを再表示したときに [アクティビティ通知リスト] に表示されます。

関連チケット アクティビティ通知を定義する方法

関連チケット アクティビティ通知のデフォルト設定を変更し、アクティビティ ログが関連チケット（リクエスト/インシデント/問題、変更要求および案件）に伝達された場合は適切な連絡先に通知することができます。

関連チケット アクティビティ通知を定義するには、以下の手順に従います。

1. [アクティビティ通知リスト] ページで [関連チケット アクティビティ通知] を開きます。
2. [編集] をクリックして詳細ページで 1 つ以上のフィールドを必要に応じて変更します。
3. (オプション) デフォルトの通知ルールを更新し、通知を受信する連絡先を指定します。
4. [保存] - [ウィンドウを閉じる] をクリックします。

更新された関連チケット アクティビティ通知は、リストを再表示したときに [アクティビティ通知リスト] に表示されます。

優先順位計算

優先順位計算は、問題とインシデントについて優先度、緊急度、影響度フィールドを自動的に設定する事前定義済みの値のセットです。優先順位計算は、ビジネス ニーズや IT 機能のためにインシデントと問題を管理するのに役立ちます。ITIL では、緊急度と影響度の値に基づくデータ計算を使用してチケットの優先度を設定することを推奨しています。サポート組織は、各計算固有のプロセス、この計算によってサービス レベル アグリーメント (SLA) が決定される方法、およびシステム内のその他の重要なイベントに基づいてこの計算を定義します。この計算にはまた、インシデントと問題にリンクされた CI のクリティカリティも含めることができます。チケットの優先度を設定すると、実質的には、以下のことを達成するのに役立ちます。

- チケットへの IT リソースの割り当て
- 顧客に対するサービスの向上
- コストの削減

優先順位計算のための CA SDM ソリューションには、以下のコンポーネントが含まれています。

- 緊急度と影響度の値に基づいた優先順位計算マトリックス
- 緊急度と影響度のデフォルト値
- [影響を受けるサービス]、[オープン日]、[影響を受けるエンドユーザ]、およびインシデント領域または問題領域に基づいた緊急度と影響度の調整オプション
- 緊急度または影響度を手動で変更するための [理由の入力] オプション
- テンプレートからチケットを作成するための [テンプレートに対して有効化] オプション

CA SDM をインストールすると、デフォルトの優先順位計算によってチケットの値が自動的に管理されます。デフォルトの優先順位計算の設定は変更できます。また、追加の優先順位計算を作成して、インシデントや問題を管理することもできます。優先順位計算では、重要度のレベルとチケット処理の一貫性を向上させるため、ビジネス シナリオに基づいて、結果を定義します。ユーザがオーバーライドできる設定もありますが、この値はデータ駆動型であるため、チケットに優先度を設定できません。マルチテナンシーの場合、管理者またはテナントは、各テナントに固有の設定を使用して、追加の優先順位計算を作成できます。

アナリストがインシデントか問題を開く場合、システムは、アクティブな優先順位計算およびチケット値を自動的に使用して、優先度、緊急度および影響度の設定を作成します。設定は以下のうち 1 つ以上のフィールドに基づきます。

- 緊急度
- 影響度
- 影響を受けるエンドユーザ
- インシデント/問題領域
- 開設日
- 影響を受けるサービス

必要に応じて、アナリストは緊急度と影響度の値を無視できます。オプションマネージャの設定により、従業員がインシデントの緊急度値を無視できるのは、**urgency_on_employee** オプションがインストールされている場合のみになります。理由の入力フラグが有効の場合に、緊急度または影響度の値を無視して [保存] をクリックすると、変更の理由を入力するためのエスカレートの詳細ページが表示されます。

チケット優先順位計算、手動優先、理由情報はすべて新規アクティビティログに表示されます。優先順位計算の調整が発生しない場合、システムはアクティビティ ログ エントリを作成しません。

注: 旧バージョンからマイグレートした場合、優先順位計算はデフォルトでは無効です。優先順位計算を有効にしたり、カスタマイズを保持したりする方法については、「実装ガイド」を参照してください。

優先順位計算でチケットの値を管理する方法

システムは、アクティブな優先順位計算設定に基づいて問題とインシデントの値を調節し、アナリストがチケットをより効率的に処理できるように支援します。以下の表は、問題、インシデント、Web サービス、電子メール、およびテキスト API の優先順位計算およびユーザアクションに基づいて優先順位計算がフィールドを変更する方法について簡単に説明しています。

アクション	自動 フィールドの変更	説明
ユーザは影響を受けるサービスを変更します。	影響度 優先度	システムは、サービス タイプの CI のサービス影響度の値を評価して新しい影響度の値を計算します。サービス タイプの CI は CI として定義されており、それらのクラスはエンタープライズ サービス ファミリで定義されています。チケットのオープン日がブラックアウト ウィンドウのタイム フレーム内にある場合、システムは [影響度の増加] フィールドに基づいて新しい影響度の値を増加します。新しい値が初期影響度の値より大きい場合にのみ、システムは影響度の値を置換します。
ユーザはインシデント領域を変更します。	緊急度	緊急度の値は、新しい値がデフォルト値よりも大きい場合にのみ変更します。

アクション	自動 フィールドの変更	説明
ユーザは、[インシデント領域] および [影響を受けるエンドユーザ] を変更します。	緊急度 優先度	ユーザが最初に [インシデント領域] フィールドを設定すると、緊急度の値はユーザが [影響を受けるエンドユーザ] を設定した後で変更されます。優先順位計算は優先度を設定します。
ユーザは [緊急度] および [影響度] を変更します。	優先度 影響度	システムは、サービス タイプの CI のサービス影響度の値を評価して新しい影響度の値を計算します。チケットのオープン日がブラックアウトウィンドウによって定義された時間内にある場合、システムは [影響度の増加] フィールドに基づいて新しい影響度の値を増加します。新しい値が初期影響度の値より大きい場合のみ、システムは影響度の値を置換します。 管理者が [理由の入力] を設定する場合、ユーザは変更の理由を指定する必要があります。 ユーザが緊急度または影響度の値を変更した場合は、ユーザが再度それらを変更しない限り、これらの値はチケットの作成またはチケットの更新全体を通して変わりません。ただし、システムは、次にユーザがチケットを更新するときに、緊急度または影響度に対して上書きされた値を更新できます。 システムが緊急度と影響度を調節した後で、優先順位計算は優先度の値を設定します。
ユーザはナレッジ ドキュメントに基づいて新規インシデントを選択し、システムは ナレッジ ドキュメントを上書き (P. 506) します。	影響度 緊急度	システムは、値がデフォルトの優先順位計算の値よりも大きいかわいかに関係なく、常にナレッジ ドキュメントまたはナレッジ ソリューションの値を使用します。 たとえば、優先順位計算が [3- 単一グループ] の影響度の値と [3- 迅速に] の緊急度の値を持っており、ナレッジ ドキュメントが [2- 複数グループ] の影響度の値と [4- 極めて迅速に] の緊急度の値を持っている場合、システムはナレッジ ドキュメントからそのインシデントに値を適用します。優先度の値は、常に優先順位計算に基づいています。

アクション	自動 フィールドの変更	説明
ユーザは問題またはインシデントの解決策としてナレッジ ドキュメントを受け入れます。	影響度 緊急度	システムは、影響度と緊急度に対してナレッジ ドキュメントからの値を使用します。また、システムは、優先順位計算を使用して優先度の値を設定します。
ユーザは新規インシデントを選択することによって、ナレッジ ドキュメントからインシデントを引き出します。	影響度 緊急度 優先度	システムは優先順位計算の値を使用します。
ユーザはナレッジ ドキュメントからインシデントを引き出しますが、システムは ナレッジ ドキュメントを上書き (P. 506)しません。	影響度 緊急度 優先度	システムは、ユーザがナレッジ ドキュメントまたはナレッジ ソリューションにインシデントを作成する方法に関係なく、優先順位計算値を使用します。
チケットは問題またはインシデントの解決策としてナレッジ ドキュメントを受け入れます。また、システムはナレッジ ドキュメントを上書きしません。	影響度 緊急度 優先度	システムは、問題またはインシデントからの値を使用します。優先度の値は優先順位計算に基づいています。
読み取り専用モードのチケットは、問題またはインシデントの解決策としてナレッジ ドキュメントを受け入れます。また、システムはナレッジ ドキュメントを上書きします。	影響度 緊急度 優先度	システムは、ナレッジ ドキュメントからの影響度と緊急度の値（値が空でない場合）を使用します。ナレッジ ドキュメントの影響度および緊急度の値が空の場合、システムは、問題またはインシデントからの値を使用します。優先度の値は優先順位計算に基づいています。
編集モードのチケットは、問題またはインシデントの解決策としてナレッジ ドキュメントを受け入れます。また、システムはナレッジ ドキュメントを上書きします。	影響度 緊急度 優先度	システムは、問題またはインシデントの値を使用します。優先度の値は優先順位計算に基づいています。

セルフサービス チケットの保存後に優先順位計算によって生成される緊急度値

優先順位計算では、セルフサービス ユーザがインシデントを保存するまで緊急度値は意図的に生成されません。VIP 従業員、従業員、匿名ユーザなど、セルフサービス ユーザが生成された値を表示できるのは、チケットの保存後です。

セルフサービス ユーザの場合、優先順位計算では、以下の設定と値を使用して緊急度値が生成されます。

- **Urgency_On_Employee** が、オプション マネージャで [はい] に設定されている
- [緊急度のオーバーライド] の値が、インシデントのアクティブな優先順位計算で有効になっている
- **AnonymousUrg** (匿名ユーザ用)、**ESCEmpUrg** (VIP 従業員用)、**EmpUrg** (その他のすべての従業員用) など、**Web.cfg** の緊急度の設定
- [領域の緊急度] の値
- 手動のユーザ オーバーライド

以下の表に、優先順位計算によってセルフサービス インシデントの緊急度値がどのように設定されるかをまとめます。

セルフサービス ユーザのアクション	緊急度値
ユーザは、[緊急度] にデフォルトを使用し、[インシデント領域] を空のままにして、インシデントを保存しました。	チケットには、 web.cfg からのデフォルトの緊急度値が表示されます。
ユーザは、[緊急度] 値をオーバーライドした後でインシデントを保存しました。	[領域の緊急度]、 web.cfg 、または優先順位計算の設定にかかわらず、チケットには、ユーザが選択した緊急度の値が表示されます。
ユーザは、[インシデント領域] を選択した後でインシデントを保存しました。 [インシデント領域] には、事前定義の [領域の緊急度] の値がありません。	チケットには、 web.cfg からのデフォルトの緊急度値が表示されます。

セルフサービス ユーザのアクション	緊急度値
ユーザは、事前定義の「領域の緊急度」の値が入っている「インシデント領域」を選択した後でインシデントを保存しました。インシデントのアクティブな優先順位計算で、「緊急度のオーバーライド」オプションも有効になっています。	「領域の緊急度」の値が web.cfg の緊急度よりも大きい場合、チケットには「領域の緊急度」の値が表示されます。ただし、ユーザがチケットを作成または編集している間は、更新された「緊急度」フィールドは表示されません。ユーザがインシデントを保存すると、そのインシデントについて更新された「緊急度」フィールドが表示されます。
ユーザは、事前定義の「領域の緊急度」の値が入っている「インシデント領域」を選択した後でインシデントを保存しました。ただし、インシデントのアクティブな優先順位計算で、「緊急度のオーバーライド」オプションは無効になっています。	チケットには、 web.cfg からの緊急度値が表示されます。
ユーザは、事前定義の「領域の緊急度」の値が入っている「インシデント領域」を持つ既存のインシデントを編集しました。	「緊急度」ドロップダウンリストに、「領域の緊急度」の値と適用可能なすべて web.cfg 値が表示されます。

注: セルフサービス ユーザの緊急度値の設定方法については、「実装ガイド」を参照してください。

優先順位計算の設定方法

優先度のようなチケット値は、デフォルトで優先順位計算に基づいています。優先度や危険度の初期値は **web.cfg** 内にあり、調節が可能です。**web.cfg** にはゲスト、VIP ユーザおよび従業員のような、さまざまなユーザのための個別設定があります。

注: 旧バージョンからマイグレートした場合、優先順位計算はデフォルトでは無効です。[カスタマイズされたインシデント] ページおよび[問題の詳細] ページは、正常に操作するために、追加の構成が必要でした。優先順位計算を有効にしたり、カスタマイズを保持したりする方法については、「実装ガイド」を参照してください。

優先順位計算を設定するには、以下の手順に従います。

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [優先順位計算] を選択します。
[優先順位計算リスト] が表示されます。
2. デフォルトの優先順位計算を右クリックし、ショートカットメニューから[編集]を選択します。
デフォルトの[優先順位計算の詳細] ページに、インシデントと問題のチケットが表示されます。
3. デフォルトの優先順位計算を確認し、値を適宜調節します。優先順位計算の値を設定する場合は、作業環境における以下の問題を考慮します。
 - **案件のエスカレーション** - チケットを、特定のVIPにエスカレートさせる必要がある場合、緊急度の値を増やすことができます。
 - **クリティカルCI** - クリティカルCI用に各CIのサービス影響度を設定できます。
 - **クリティカルサービス稼働時間** - CIが高い可用性を必要とする場合、ブラックアウトウィンドウを追加します。
 - **ブラックアウトウィンドウ** - CI関連のチケットが特定のブラックアウトウィンドウを使用する場合、優先順位計算のサービス影響度の値を増やすことができます。
4. 必要に応じて、ユーザがチケット設定を変更できるように、手動優先設定を使用します。

5. 問題とインシデントで、優先順位計算を別個に管理する場合は、[チケットタイプを設定](#) (P. 503) します。

6. [保存] をクリックします。

次の新規または更新チケット上、またはナレッジドキュメント上で、アクティブな優先順位計算の値に応じてフィールドが更新されます。

7. 各チケットタイプに、追加の優先順位計算を作成するかどうかを検討します。マルチテナンシーに対しては、追加の優先順位計算を作成しアクティブにして、各テナントのチケットを管理します。

注: この手順の詳細については、オンラインヘルプを参照してください。

複数の優先順位計算

1つ以上の優先順位計算を設定できます。ただし、1つのアクティブな優先順位計算のみが、問題、インシデント、またはそれら両方を処理します。たとえば、問題にアクティブな優先順位計算を使用し、インシデントに別のものを使用することができます。また、将来使用できるように、複数の非アクティブ優先順位計算を保存することもできます。

マルチテナンシーの優先順位計算の割り当て

管理者またはテナントは、テナント固有の優先順位計算を作成して、インシデントまたは問題を管理できます。マルチテナンシーの優先順位計算を割り当てるときは、以下の点を考慮してください。

- 優先順位計算がテナントに割り当てられていないとき、その計算はパブリックであると見なされます。パブリックの優先順位計算のステータスは、アクティブまたは非アクティブのどちらかです。優先順位計算がテナントに割り当てられると、その計算はパブリックとは見なされなくなります。
- テナントに優先順位計算が割り当てられていない場合は、デフォルトの優先順位計算またはパブリックのアクティブな別の優先順位計算によって、問題とインシデントが自動的に管理されます。
- 1つの優先順位計算は1つのテナントの問題とインシデントを管理します。ただし、テナント固有の個別の優先順位計算で各チケットタイプを処理できます。たとえば、企業によっては、インシデントを処理するための優先順位計算と、問題を管理するための優先順位計算を別々に用意します。

- パブリックの優先順位計算がアクティブのときにテナントが独自の優先順位計算を作成した場合、テナント固有の優先順位計算はそれぞれのテナントのチケットにのみ適用されます。

たとえば、デフォルトの優先順位計算がアクティブである場合、ある企業テナントは `new_priority_calculation` という名前の、テナント固有の優先順位計算を作成できます。 `new_priority_calculation` の設定と構成は、その企業のインシデントと問題にのみ適用されます。

- テナントが優先順位計算を非アクティブにした場合は、システムによってパブリックのアクティブな優先順位計算が使用され、そのテナントの問題とインシデントが管理されます。

たとえば、デフォルトのアクティブな優先順位計算があるときに、ある企業がテナント固有の優先順位計算を無効にします。システムではデフォルトの優先順位計算を使用してその企業のインシデントと問題を管理するため、優先順位計算はその企業について有効なままです。

注: テナント固有の優先順位計算レコードの削除はテナントが行うことができるため、インシデントと問題を管理するパブリックの優先順位計算の非アクティブ化は管理者が行うことをお勧めします。テナント固有の優先順位計算の作成は、管理者またはテナントが行うことができます。

- マルチテナンシーを無効にするときに、テナントを管理するアクティブな優先順位計算が複数ある場合は、インシデントと問題を管理するための優先順位計算を 1 つだけ残します。たとえば、インシデントを管理するための優先順位計算と、問題进行处理するための優先順位計算を除いて、その他すべての優先順位計算を非アクティブにすることができます。

注: マルチテナンシーの詳細については、「実装ガイド」を参照してください。

優先順位計算にテナントを割り当てる方法

マルチテナンシーの場合、優先順位計算にテナントを割り当てるができます。最初に、パブリックの優先順位計算を非アクティブにします。次に、テナントを優先順位計算に割り当て、その優先順位計算をアクティブにします。

優先順位計算にテナントを割り当てるには、以下の手順に従います。

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [優先順位計算] を選択します。
[優先順位計算リスト] が表示されます。
2. パブリックの優先順位計算をそれぞれ編集します(デフォルトなど)。ステータスを[非アクティブ]に設定し、[保存]をクリックします。
パブリックの優先順位計算が無効になります。
3. 影響度、緊急度、および優先度についてテナント固有の設定を使用して、テナントごとに優先順位計算を作成または編集します。
[優先順位計算の作成] ページまたは[優先順位計算の更新] ページが表示されます。
4. [名前] フィールドでテナントを指定します。
5. [ステータス] フィールドで[アクティブ]を選択します。
6. [保存]をクリックします。
影響度、緊急度、および優先度に関するテナント固有の値が、新しいインシデントまたは問題で適用されます。

注: 優先順位計算の作成および編集については、オンライン ヘルプを参照してください。

優先順位計算に対するチケットタイプの考慮

優先順位計算用のチケットタイプを設定する場合、以下を考慮します。

- デフォルト優先順位計算では、インシデントと問題の両方のチケットタイプを管理することができます。

- 前のリリースからマイグレートしている場合、デフォルトの優先順位計算を有効にするか、または問題とインシデントを管理するために優先順位計算を作成します。
- 多数の優先順位計算を実行できますが、特定のチケットタイプを処理できるのは1つのアクティブな優先順位計算のみです。たとえば、1つのアクティブな優先順位計算は問題を管理できます。また、別の優先順位計算はインシデントを管理できます。
- 優先順位計算を作成する際、アクティブな優先順位計算がすでに特定のチケットタイプを処理している場合は、まずアクティブな優先順位計算中のチケットタイプを無効にします。たとえば、優先順位計算で問題を管理する場合は、アクティブな優先順位計算で問題チケットタイプを無効にし、問題を管理するアクティブな優先順位計算を作成します。

注: マイグレーション間に優先順位計算を有効化し、チケットタイプを設定する方法の詳細については、「実装ガイド」を参照してください。

優先順位計算にチケットタイプを設定する

優先順位計算が管理するチケットタイプを指定できます。優先順位計算がアクティブな場合、新規チケットで、優先度、影響度、および緊急度の値を管理します。

優先順位計算にチケットタイプを設定する方法

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [優先順位計算] を選択します。
[優先順位計算リスト] が表示されます。
2. 優先順位計算を右クリックし、[編集] を選択します。
[優先順位計算の更新] ページが表示されます。
3. 以下のオプションの1つ以上を選択するかクリアします。

インシデント

優先順位計算を有効または無効にして新規インシデントを管理します。

問題

優先順位計算を有効または無効にして新規の問題チケットを管理します。

4. [保存] をクリックします。

CA SDM は優先順位計算の設定を使用して新規インシデント、問題またはそれら両方のチケットの値を管理します。

チケット テンプレートを使用して優先度値を計算する

チケット テンプレートで優先度を計算する場合は、[テンプレートに対して有効化] オプションを使用して優先度計算を設定します。このオプションを有効にすると、[緊急度] と [影響度] の値はテンプレートからになりますが、[優先度] フィールドは優先順位計算レコードからです。優先度値は読み取り専用として表示されます。

このオプションを有効にしない場合は、[緊急度]、[影響度]、[優先度] フィールドはテンプレートからの値になります。[優先度] フィールドは編集できます。また、それが保存されるまで、チケットの優先順位計算は行われません。

チケット テンプレートを使用して優先度値を計算する方法

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [優先順位計算] を選択します。
[優先順位計算リスト] が表示されます。
2. テンプレートを使用して優先度の計算に使用する優先順位計算を選択します。
また、優先順位計算を作成し、チケット テンプレートを使用して優先度値を計算することもできます。
3. [優先順位計算リスト] から [テンプレートに対して有効化] を選択します。
4. [保存] をクリックします。
オプションは有効になりました。

優先度値の計算におけるナレッジドキュメントの使用

ナレッジドキュメントを使用して優先度を計算するには、フィールドマッピングを更新します。フィールドマッピングを設定すると、アナリストはナレッジドキュメントからインシデントまたは問題のチケットを作成できます。ナレッジドキュメントは、チケットの影響度と緊急度の値を計算します。影響度または緊急度の値がない場合、その値は優先度の計算から生成されます。

重要: ナレッジドキュメントによって計算された影響度と緊急度の値をすでに含むチケットを変更し、保存する場合、ナレッジマネジメントで設定された値は優先度の計算により上書きされます。監査ログにこれらのアクティビティが表示されます。

優先度の値を計算するためにナレッジドキュメントを使用するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [Service Desk インテグレーション] を選択します。
2. [フィールドマッピング] を選択します。
[フィールドマッピング] ページが表示されます。
3. 影響度と緊急度については、以下の該当するチェックボックスをオンにします。

空の Service Desk 値への取り込み

ナレッジマネジメントの情報をを使用して、案件またはリクエストのフィールドにデータを取り込むかどうかを指定します。

Service Desk 値の上書き

[ナレッジマネジメント] 列に一覧表示されたフィールドに対応する、案件またはリクエストのフィールドを指定します。

注: 影響度および緊急度に対して、[Service Desk 値の上書き] フィールドは無効だが[空の Service Desk 値への取り込み]は有効である場合、影響度および緊急度のナレッジ値でインシデント値は上書きされます。

4. [保存] をクリックします。

優先度値を計算するため、ナレッジドキュメントの影響度と緊急度の値を使用して、インシデントと問題が作成されます。値がない場合、チケットは、アクティブな優先度計算から値を取得します。チケットタイプに対してアクティブな優先度計算がない場合、システムにより、優先度、緊急度、および影響度のフィールドはクリアされます。

影響度値を手動で無効化

問題かインシデントに対する影響度値を手動で無効にすると、チケットタイプを管理するアクティブな優先順位計算が自動的に優先度値を調節します。

手動で影響度値を無効化するには、以下の手順に従います

1. 変更する問題またはインシデントの詳細ページを開きます。
2. 影響度値を変更します。
チケットタイプを管理するアクティブな優先順位計算がある場合、優先度の値は優先度計算の設定に基づいて自動的に変更されます。
3. インシデントを保存します。
[インシデントの詳細] ページのアクティビティ ログに、影響度値の変更が反映されます。

例: 手動で新規インシデントの影響度値を無効化

1. インシデントを作成します。
デフォルトでは、緊急度の値は [3- 迅速に] です。影響度の値は [3- 単一グループ] です。優先度の値は 3 です。
2. [1- 組織全体] の影響度値を無視します。
優先度の値は、インシデントを管理するアクティブな優先順位計算の値に基づいて自動的に変更されます。
3. インシデントを保存します。
[インシデントの詳細] ページのアクティビティ ログに、影響度値の変更が反映されます。

緊急度の値を手動で上書きする

緊急度の値をチケットに手動で上書きする場合、チケットタイプを管理するアクティブな優先順位計算は自動的に優先度の値を調節します。

緊急度の値を手動で上書きする方法

1. 変更するインシデントの詳細ページを開きます。
2. 緊急度の値を変更します。

チケットタイプを管理するアクティブな優先順位計算がある場合、優先度の値は優先度計算の設定に基づいて自動的に変更されます。

3. インシデントを保存します。

[インシデントの詳細] ページのアクティビティ ログに緊急度の値の変更が反映されます。

例: 手動で新規インシデントの緊急度の値を上書きする

1. インシデントを作成します。

デフォルトでは、緊急度の値は [3- 迅速に] です。影響度の値は [3- 単一グループ] です。優先度の値は 3 です。

2. 緊急度の値を [5- 即時] に上書きします。

優先度の値は、インシデントを管理するアクティブな優先順位計算の値に基づいて自動的に変更されます。

3. インシデントを保存します。

インシデントの詳細ページでアクティビティ ログは、緊急度の値の変化を反映します。

問題またはインシデントに対する影響度の自動調節

エンタープライズ サービスのファミリを使用して定義された構成アイテムについては、問題またはインシデントに対する影響度値を自動的に調節できます。問題またはインシデント領域を選択し、[影響を受けるサービス]を選択すると、エンタープライズ サービス CI 用の CI サービス影響度設定および優先順位計算に基づき、影響度が自動的に調節されます。

問題またはインシデントに対する影響度を自動的に調整するには、以下の手順に従います。

1. エンタープライズ サービス タイプの CI 用の問題またはインシデントを作成します。
2. [影響を受けるサービス]を選択します。
3. 問題またはインシデント領域を選択します。

チケットタイプを管理するアクティブな優先順位計算がある場合、影響度値は、影響を受けるサービスの優先順位計算とサービス影響度値の[影響度の増加]値（ブラックアウト ウィンドウの影響度評価に使用される）に基づいて変わります。

エンタープライズ サービス CI セットに対するサービス影響度が[1- 組織全体]の設定で、デフォルトの優先順位計算を使用しており、問題かインシデントがブラックアウト ウィンドウ中に開かれない場合、問題またはインシデント内の影響度値は1に設定され、チケットの優先度値は2に上がります。

4. チケットを保存します。
[インシデントの詳細] ページのアクティビティ ログに、影響度値の変更が反映されます。

問題またはインシデントの影響度の調節例

以下の例では、問題またはインシデントの影響度を調節する方法を示します。

1. **CI-APC** という名前のエンタープライズ サービス **CI** を作成し、ファミリーエンタープライズ サービス下に含める一つとしてクラスを設定します。

たとえば、その他サービス、ビジネス サービス、またはインフラストラクチャ サービスとしてクラスを設定できます。

2. 構成アイテム詳細フォームの [サービス] タブで、[サービス影響度] フィールドを [2- 複数グループ] に設定します。
3. [Service Desk] タブで、インシデントを作成し、[影響を受けるサービス] を [CI-APC] に設定します。
4. チケットを保存します。

インシデントの [影響度] フィールドでは、選択された影響を受けるサービス (CI-APC) のサービス影響度からの値が反映されます。この場合、[影響度] の値は [2- 複数グループ] に設定されます。

注: デフォルトの優先順位計算を使用していて、現在のチケットがブラックアウトウィンドウ期間中に作成された場合、[影響度] の値は 1 だけ増加します。また、その場合は、[影響度] の値はその後 [1- 組織全体] に設定されます。

注: 構成アイテムの作成の詳細については、オンライン ヘルプを参照してください。

問題またはインシデントの緊急度の自動調節

問題とインシデントに対する緊急度および優先度は、特殊処理を必要とする「影響を受けるエンドユーザ」を指定するか、「領域の緊急度」値を持つ問題/インシデント領域を指定することにより、自動的に調節できます。

「緊急度のエスカレート」が有効な状態で連絡先に特殊処理を割り当てる場合、または問題/インシデント領域に「領域の緊急度」を設定する場合、問題/インシデント内の緊急度値は、優先順位計算および「影響を受けるエンドユーザ」に対する領域の緊急度値に応じて、自動的に調節されます。

問題またはインシデントの緊急度を自動調節するには、以下の手順に従います。

1. 問題かインシデントを作成します。
2. 「影響を受けるエンドユーザ」を選択します。高い緊急度については、「影響を受けるエンドユーザ」に「緊急度のエスカレート」が有効な特殊処理を必要とするユーザを選択します。

チケットタイプを管理するアクティブな優先順位計算がある場合、緊急度値はアクティブな優先順位計算の「緊急度の増加」値に基づいて変わります。

3. 問題またはインシデント領域を選択します。

チケットタイプを管理するアクティブな優先順位計算がある場合、緊急度値は問題/インシデント領域の定義における「領域の緊急度」値に基づいて変わります。

4. チケットを保存します。

チケットに特殊処理が必要であることを示す確認メッセージが表示されます。「問題/インシデントの詳細」ページのアクティビティログに、緊急度値の変更が反映されます。

問題またはインシデントの緊急度の調節例

以下の例では、問題またはインシデントの緊急度を調節する方法を示します。

1. [管理] タブで、**Non-VIP** という名前の連絡先を作成します。
2. **VIP** という名前の特殊処理連絡先を作成し、緊急度のエスカレート値をオンに設定します。
3. **Test Area** という名前の領域を作成し、領域の緊急度を [2- 極めて迅速に] に指定します。
4. **Service Desk** タブで、インシデントを作成します。
5. 影響を受けるエンドユーザには、**Non-VIP** を選択します。
6. インシデント領域で、[テスト領域] を選択し、チケットを保存します。

[緊急度] フィールドには、インシデント領域定義からの領域の緊急度の値が反映されます。この場合、緊急度は [2- 極めて迅速に] に設定されます。

7. [VIP への影響を受けるエンドユーザ] を変更し、チケットを保存します。

デフォルトの優先順位計算マトリックスが使用されている場合、緊急度の値は 1 つ増えて、[1-即時] に設定されます。チケットに特殊処理が必要であることを通知する確認メッセージが表示されます。[インシデントの詳細] ページのアクティビティ ログに緊急度の値の変更が反映されます。

注: 作成する連絡先および領域の詳細については、[オンライン ヘルプ](#)を参照してください。

ステータス遷移および従属属性のコントロール

以下の設定可能なコントロールを使用して、変更要求、案件、インシデント/問題/リクエストのチケット ステータス フローを制限し、各チケット ステータスに表示されるフィールド、つまり必須フィールドを決定することができます。

遷移

インシデント/問題/リクエスト、案件、または変更要求のフォーム上で使用可能なステータスをユーザが選択する方法を制御します。たとえば、問題のステータスが「オープン」の場合、遷移フローを使用することで、アナリストのみが「クローズ」ステータスに更新できるようにすることができます。この例では、アナリストに他のステータス オプションがないため、問題管理プロセスが強化されます。

遷移により、完全なステータス リストのサブセットを定義し、現在のステータスに基づいて、デフォルトの新しい（または次の）チケット ステータスを指定することができます。それぞれのチケット タイプに対して、独自のステータス遷移を定義できます。エンドユーザのステータス ワークフローを制限する必要がある場合は、遷移の使用を検討してください。

従属属性

チケット ステータスに応じて、属性を必須（必ず指定）またはロック済み（更新不可）として指定する方法を制御します。たとえば、変更マネージャは、変更要求の承認後に、アナリストによる概要属性の編集を防止することができます。ステータスに基づいて特定の属性を制限する必要がある場合は、属性コントロールの使用を検討してください。

注: オプションマネージャ（一般オプション）の「ステータス ポリシー違反」オプションを構成することによって、システムで強制されるステータス ポリシーの厳密さを指定できます。このオプションは、統合やマクロなど、自動化されたシステム プロセスにのみ適用されます。

関連項目:

[ステータス移行および従属属性コントロールでの作業](#) (P. 514)

[ステータス移行の設定](#) (P. 514)

[ベスト プラクティス: 事前定義済みステータス移行](#) (P. 522)

ステータス移行および従属属性コントロールでの作業

ステータス移行および従属属性コントロールで作業するには、以下の手順に従います。

1. [管理] タブで、環境に対して適切なテナント、連絡先および役割を設定します。
2. **Service Desk** ノードで、チケット タイプ (変更要求など) を指定し、[ステータス] を選択します。
[ステータス リスト] ページにアクティブなステータス コードが表示されます。
3. 適切なステータス コード ([確認済み] など) を編集し、チケットのステータスの詳細ページの下にあるタブで使用可能なコントロールを使用して以下を実行します。
 - [ステータス移行の設定](#) (P. 514)
 - [従属属性コントロールの設定](#) (P. 516)

注: それぞれのチケット タイプに一意の移行および従属属性コントロールを設定できます。

ステータス移行の設定

完全なステータス リストのサブセットを設定し、現在のステータスに基づいてチケットのデフォルトの次のステータスを指定することができます。ステータスがチケットの詳細フォームで変更された場合、移行が実施されます。

ステータス移行を設定する方法

1. チケットのステータスの詳細ページの下で [移行] タブをクリックします。
[移行リスト] ページに、ステータスの有効な移行がすべて表示されます。
注: 設定された時、リンクした移行タイプはインシデントおよびリクエスト移行リストに表示されます。
2. [移行の更新] ボタンをクリックします。
[チケット ステータス移行の更新] ページが表示されます。

3. 以下の確認ボックスを必要に応じて設定します。

許可

ステータスに有効な移行を指定します。このオプションを使用して、ステータス ワークフローを制限します。

デフォルト

(オプション) デフォルトのステータス移行を指定します。ユーザがチケットの詳細フォームでデフォルト移行ボタンをクリックした場合、またはユーザ (Web サービス ユーザを含む) がステータスを <d> 値に更新した場合、CA SDM はデフォルト移行を適用します。デフォルト移行は、各ステータスにつき 1 つのみです (マルチテナントシステムでは、各テナントにつき 1 つ)。

要コメント

(オプション) チケットでステータスを変更する場合、移行のアクティビティ ログ コメントが必要であることを指定します。

注: このオプションは、CA SDM チケットのみに適用されます。Web サービスやリスト内で編集機能などのように他の領域には適用されません。

4. (オプション) [名前] 列のステータス コードを選択してその詳細を更新します。
5. [保存] をクリックします。

新規ステータスで設定された移行のリストが移行リストに表示されます。アナリストがチケット フォームで [ステータス] ドロップダウンを選択すると、新規ステータス リストが表示されます。

注: ステータス移行を定義する手順の詳細については、オンラインヘルプを参照してください。

従属属性コントロールの設定

チケット ステータスに表示する、または必要なフィールドを決定できます。

注: チケット ステータスに「必須」の従属属性を設定する前、チケットのリスト ページに表示される [リスト内で編集] オプションには必要な属性フィールド値が表示されない場合があることに注意してください。必要な属性フィールド値が保存されたチケットの一部になっておらず、[リスト内で編集] の形式で表示されない場合、チケットは保存されません。従って、アナリストは、[リスト内で編集] オプションを使用する代わりにチケットの詳細ページで必要な従属属性フィールド値を編集する必要があります。

従属属性コントロールを設定する方法

1. チケットのステータス詳細ページで、ページの下にある [従属属性コントロール] タブを選択します。
[属性コントロール リスト] が表示されます。
2. [作成] をクリックします。
[ステータスの従属属性コントロールの更新] ページが表示されます。
3. 以下のフィールドを指定します。

テナント

(オプション) マルチテナンシーがインストールされているシステムで、オプションのテナント名を指定します。テナントが指定されている場合、従属はそのテナントおよびそのサブテナントにのみ適用されます。

属性

制御する属性の名前（「概要」など）を指定します。

ロック済み

属性をロック済みとして指定します。ステータスに関連付けられたロック済みの属性は、同じステータスのチケットで更新することはできません。ステータスが変更される場合、属性はロック解除されます。

必須

属性を必須として指定します。ステータスに必要な属性は、同じステータスのチケットにヌル値を使用できません。

4. [保存] をクリックします。

ページを再表示すると、ステータスの新規属性コントロールが [属性コントロール リスト] に表示されます。ユーザがチケット ステータスを更新すると、システムは新規ステータスに対応する必要な属性のリストを取得し、チケット フォームを必要に応じて更新します。ユーザが必須フィールドに入力せずにチケットを閉じようとする、エラー メッセージがチケット フォームの一番上に表示されます。

注: 従属属性コントロールを定義する手順の詳細については、[オンラインヘルプ](#)を参照してください。

Web サービス メソッド

以下のステータス遷移および従属属性コントロール SOAP Web サービス メソッドを設定できます。

getValidTransitions

チケットの遷移をリスト表示します。このメソッドは、既存の **getValidTaskTransitions** メソッドを模範としていますが、引数をチケットまたはステータスにすることができます。

getDependentAttrControls

固定 ID によって指定されたオブジェクトの属性に対するロック済みおよび必須の属性を一覧表示します。ステータス属性は現時点ではサポートされています。

注: SOAP Web サービス メソッドの詳細については、「[テクニカル リファレンス ガイド](#)」を参照してください。

事前定義済み移行フロー

各チケットタイプについては、製品に提供された事前定義済みのステータス移行を使用し、それらを変更して希望の移行フローに合わせることができます。

注: ステータス移行は **CA Workflow** などの統合間で共有できるため、明示的に要求されない限り、事前定義済みステータス移行を非アクティブにしないでください。

事前定義済み移行のリストを表示するには、以下の手順に従います。

[管理] タブで、**Service Desk** ノードを展開し、以下のうちの1つを選択します。

- 変更要求移行
- 案件移行
- リクエスト/インシデント/問題移行

[移行リスト] には、チケット（インシデント/リクエスト/問題、変更要求および案件）がそのライフサイクルを通して継続する方法を制御できる事前定義済みの移行が表示されます。

注: 移行を定義して変更する手順の詳細については、**オンラインヘルプ**を参照してください。

インシデント移行フロー

下表は、事前定義済みのインシデント移行フローです。

現在のステータス	デフォルト移行	次に移行可能なステータス
確認済み	進行中<d>	回避済み、ベンダー待機中、キャンセル済み、クローズ、未解決クローズ、進行中、オープン、変更待ち、解決済み
回避済み		確認済み、回避済み、エンドユーザ応答待機中、クローズ、未解決クローズ、進行中、解決策を拒否、調査中、解決済み
エンドユーザ 応答待機中	調査中<d>	クローズ、未解決クローズ、進行中、オープン、調査中、解決済み

現在のステータス	デフォルト移行	次に移行可能なステータス
ベンダー待機中	調査中<d>	確認済み、クローズ、未解決クローズ、進行中、オープン、変更待ち、調査中、解決済み
キャンセル済み		クローズ
クローズ		開く
未解決クローズ		確認済み
未解決クローズ		クローズ
未解決クローズ		開く
保留		確認済み、クローズ、進行中、オープン、変更待ち、解決済み
進行中	調査中<d>	確認済み、エンドユーザ応答待機中、ベンダー待機中、クローズ、未解決クローズ、オープン、変更待ち、調査中、解決済み
Pending Change (変更の保留)	調査中<d>	確認済み、クローズ、進行中、オープン、解決済み
調査中	解決済み<d>	クローズ、オープン、解決済み
解決日	クローズ<d>	エンドユーザ応答待機中、クローズ、オープン

問題移行フロー

下表は、事前定義済みの問題移行フローです。

現在のステータス	デフォルト移行	次に移行可能なステータス
確認済み	進行中<d>	確認済み、承認済み、キャンセル済み、クローズ、修正中、オープン、拒否、調査中
分析完了	承認済み<d>	確認済み、キャンセル済み、クローズ、修正中
承認済み	修正中<d>	クローズ、修正済み、変更待ち
ベンダー待機中	調査中<d>	確認済み、クローズ、未解決クローズ、修正済み、進行中、オープン、変更待ち、調査中
キャンセル済み	クローズ<d>	クローズ、未解決クローズ、オープン

現在のステータス	デフォルト移行	次に移行可能なステータス
未解決クローズ		確認済み、クローズ、オープン
修正中	修正済み<d>	承認済み、キャンセル済み、修正済み、修正中、調査中、拒否
固定	クローズ<d>	クローズ
保留	調査中<d>	確認済み、クローズ、修正済み、進行中、オープン、変更待ち、調査中
進行中	調査中<d>	確認済み、承認済み、キャンセル済み、クローズ、修正中、変更待ち、拒否、調査中
既知のエラー	修正中<d>	クローズ、修正中、修正済み
開く	確認済み<d>	確認済み、承認済み、キャンセル済み、クローズ、修正中、進行中、拒否、調査中
Pending Change (変更の保留)	修正済み<d>	クローズ、修正済み、調査中
拒否	クローズ<d>	クローズ、未解決クローズ、オープン
調査中	分析完了<d>	確認済み、分析完了、承認済み、キャンセル済み、クローズ、修正中、修正済み、拒否

案件移行フロー

下表は、事前定義済みの案件移行フローです。

現在のステータス	デフォルト移行	次に移行可能なステータス
確認済み	進行中<d>	エンドユーザ応答待機中、ベンダー待機中、クローズ、未解決クローズ、進行中、オープン、変更待ち、解決済み
エンドユーザ 応答待機中	調査中<d>	確認済み、クローズ、未解決クローズ、進行中、オープン、調査中、解決済み
ベンダー待機中	調査中<d>	確認済み、クローズ、進行中、オープン、変更待ち、調査中、解決済み
キャンセル済み	クローズ<d>	クローズ

現在のステータス	デフォルト移行	次に移行可能なステータス
クローズ		確認済み、オープン
未解決クローズ		確認済み、クローズ、オープン
保留		確認済み、クローズ、進行中、オープン、変更待ち、解決済み
進行中	調査中<d>	確認済み、エンドユーザ応答待機中、ベンダー待機中、クローズ、未解決クローズ、オープン、変更待ち、調査中、解決済み
開く	確認済み<d>	確認済み、セルフサービスによって回避、エンドユーザ応答待機中、ベンダー待機中、クローズ、未解決クローズ、進行中、変更待ち、解決済み
Pending Change (変更の保留)	調査中<d>	確認済み、クローズ、進行中、オープン、調査中、解決済み
調査中	解決済み<d>	クローズ、オープン、解決済み、エンドユーザ応答待機中、クローズ、オープン

変更要求移行フロー

下表は、事前定義済みの変更要求移行フローです。

現在のステータス	デフォルト移行	次に移行可能なステータス
承認中	承認済み<d>	承認済み、キャンセル済み、クローズ
承認済み	スケジュール済み<d>	キャンセル済み、クローズ、実装中、スケジュール済み
Backed Out		承認中、クローズ、オープン、RFC
キャンセル済み		クローズ
顧客保留		キャンセル済み、クローズ、実装中、拒否、スケジュール済み、検証中
保留		キャンセル済み、クローズ、実装中、スケジュール済み
実装中		取り消し、キャンセル済み、クローズ、顧客保留、拒否、スケジュール済み、ベンダー保留、検証中

現在のステータス	デフォルト移行	次に移行可能なステータス
開く	RFC<d>	承認中、キャンセル済み、クローズ、顧客保留、実装中、拒否、RFC、スケジュール済み、ベンダー保留
拒否	クローズ<d>	承認中、キャンセル済み、クローズ
RFC	承認中<d>	承認中、キャンセル済み、クローズ、顧客保留、実装中、オープン、拒否、スケジュール済み、ベンダー保留
Scheduled	実装中<d>	キャンセル済み、クローズ、顧客保留、実装中、ベンダー保留、検証中、キャンセル済み、クローズ、実装中、スケジュール済み、取り消し、クローズ

ベストプラクティス: 事前定義済みステータス移行

製品で提供される事前定義済みステータス遷移は、新規インストールでは「アクティブ」、アップグレード後は「非アクティブ」です。[移行リスト] ページに一覧表示されるステータスごとに、デフォルトのステータス移行（次のステータス）があります。デフォルトのステータス移行のパスがベストプラクティスを表しています。遷移リストページに一覧表示されるその他のステータス遷移は、さまざまなチケット管理ワークフローを実行するために提供されます。ただし、リクエスト、インシデント、問題、および変更要求を管理するための適切なワークフローが実行されるようにすることができるのは、このベストプラクティスを使用する「アクティブ」ステータスの遷移だけです。このベストプラクティスは、チケットの解決への移動およびIT環境内でのクローズを促進するのに役立ちます。

たとえば、[移行リスト] ページに一覧表示される以下の事前定義済みインシデント移行は、インシデントの解決とクローズを促進するために[非アクティブ]に設定されます。

ステータス	新規ステータス	デフォルト	ステータスの説明	レコードステータス
確認済み	クローズ	いいえ	「確認済み」から「クローズ」へ	非アクティブ
確認済み	未解決クローズ	いいえ	「確認済み」から「未解決クローズ」へ	非アクティブ

ステータス	新規ステータス	デフォルト	ステータスの説明	レコードステータス
確認済み	オープン	はい	「確認済み」から「オープン」へ	非アクティブ
エンドユーザ 応答待機中	確認済み	いいえ	「エンドユーザ応答待機中」から 「確認済み」へステータスを遷移 します	非アクティブ
エンドユーザ 応答待機中	オープン	いいえ	「エンドユーザ応答待機中」から 「オープン」へステータスを遷移 します	非アクティブ
ベンダー待機 中	確認済み	いいえ	「ベンダー待機中」から「確認済 み」へステータスを遷移します	非アクティブ
ベンダー待機 中	クローズ	いいえ	「ベンダー待機中」から「クロー ズ」へステータスを遷移します	非アクティブ
ベンダー待機 中	オープン	いいえ	「ベンダー待機中」から「オープ ン」へステータスを遷移します	非アクティブ
クローズ	確認済み	いいえ	「クローズ」から「確認済み」へ	非アクティブ
未解決クロー ズ	確認済み	いいえ	「未解決クローズ」から「確認済 み」へステータスを遷移します	非アクティブ
未解決クロー ズ	クローズ	いいえ	「未解決クローズ」から「クロー ズ」へステータスを遷移します	非アクティブ
保留	確認済み	いいえ	「保留」から「確認済み」へステ ータスを遷移します	非アクティブ
保留	クローズ	いいえ	「保留」から「クローズ」へステ ータスを遷移します	非アクティブ
保留	オープン	いいえ	「保留」から「オープン」へステ ータスを遷移します	非アクティブ
進行中	確認済み	いいえ	「進行中」から「確認済み」へス テータスを遷移します	非アクティブ
進行中	クローズ	いいえ	「進行中」から「クローズ」へス テータスを遷移します	非アクティブ

ステータス	新規ステータス	デフォルト	ステータスの説明	レコードステータス
進行中	オープン	いいえ	「進行中」から「オープン」へステータスを遷移します	非アクティブ
オープン	クローズ	いいえ	「オープン」から「クローズ」へステータスを遷移します	非アクティブ
変更待ち	確認済み	いいえ	「変更待ち」から「確認済み」へステータスを遷移します	非アクティブ
変更待ち	クローズ	いいえ	「変更待ち」から「クローズ」へステータスを遷移します	非アクティブ
変更待ち	オープン	いいえ	「変更待ち」から「オープン」へステータスを遷移します	非アクティブ
調査中	オープン	いいえ	「調査中」から「オープン」へステータスを遷移します	非アクティブ

セルフ サービスのためのステータス遷移

ステータス遷移では、ある状態から別の状態（たとえば「オープン」から「クローズ」）へのチケットの移行を制御することができます。セルフ サービスを使用する従業員の場合は、インシデントおよびリクエストの詳細フォーム上に、[ステータス遷移](#) (P. 513)を示すボタンを含めることができます。

インシデントまたはリクエストの遷移がアクティブな遷移タイプにリンクしている場合には、インシデントとリクエストのプロセスワークフローのステータス遷移ボタンが従業員用インターフェースに表示されます。遷移タイプによって、ボタンのテキストを定義し、チケット詳細フォームの動作を制御します。ボタンが定義されると、従来の「インシデントのクローズ」（または「リクエストのクローズ」）、および「インシデントの再オープン」（または「リクエストの再オープン」）ボタンがチケット詳細フォームに表示されなくなります。代わりに、従業員は、管理者が設定したステータス遷移ボタンを使用して、インシデントまたはリクエストのステータスのみを変更できます。

デフォルトでは、製品に付属する事前定義済みの遷移タイプはすべて非アクティブです。このため、ステータス遷移ボタンは有効ではありません。システム管理者として、事前定義済みの遷移タイプをアクティブにして変更するか、またはステータス遷移ワークフローに適合する遷移タイプを作成することもできます。遷移タイプを作成または変更した後で、それらを任意のインシデントまたはリクエストのステータス遷移にリンクすることができます。

注: 遷移タイプの詳細については、「オンライン ヘルプ」を参照してください。

関連項目:

[セルフ サービスの移行のしくみ](#) (P. 525)

[移行の移行タイプを作成または更新する方法](#) (P. 526)

[移行タイプを移行にリンクする方法](#) (P. 527)

[事前定義済み移行タイプのアクティブ化](#) (P. 527)

セルフ サービスの移行のしくみ

移行タイプおよび対応するステータスは、従業員がいつチケットをクローズして再オープンできるかを以下のようにして制御します。

1. アクティブな移行タイプは管理者によってインシデント（またはリクエスト）ステータス移行にリンクしています。
2. 従業員はセルフ サービスを使用して、インシデントを作成します。
3. インシデントに割り当てられたアナリストは解決策を見つけてチケットを解決済みステータスに移動します。
4. チケットが解決済みステータスにある場合は、従業員詳細フォームに解決方法を承諾または解決方法を拒否するステータス移行ボタンが表示されます。
 - 従業員が解決方法を承諾すると、「解決済み」から「クローズ」への移行が発生します。
 - 従業員が解決方法を拒否すると、「解決済み」から「オープン」への移行が発生します。
5. 従業員がボタンをクリックした後、表示される解決方法フォームに注釈を追加できます。

移行の移行タイプを作成または更新する方法

システム管理者として、[移行タイプ リスト] ページで、インシデントおよびリクエストのステータス移行ワークフローに新しい移行タイプを作成したり、既存の移行タイプを更新することができます。

ステータス移行に移行タイプを作成するには、以下の手順に従います。

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [移行タイプ] を選択します。
2. リスト ページで [作成] をクリックします。
3. 詳細ページでフィールドを必要に応じて編集します。
ステータス移行に移行タイプが作成されます。

4. [保存] をクリックします。

新規移行タイプは、ページを再表示したときに [移行タイプ リスト] に表示されます。

移行タイプを更新するには、以下の手順に従います。

1. [移行タイプ リスト] ページで編集する任意の移行タイプを開きます。
2. 必要に応じてフィールドを編集します。
3. [保存] をクリックします。

更新された移行タイプが [移行タイプ リスト] に表示されます。

移行タイプを移行にリンクする方法

ステータス移行が移行タイプにリンクすると、従業員チケット詳細フォームに解決方法を承諾または解決方法を拒否するステータス移行ボタンが表示されます。移行タイプをステータス移行にリンクするには、以下の手順に従います。

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [インシデント（またはリクエスト）移行] を選択します。
2. [リクエスト移行リスト] ページまたは [インシデント移行リスト] ページで編集する任意のステータス移行を開きます。
3. [移行タイプ] フィールドで目的の移行タイプを指定します。
4. [保存] をクリックします。

移行タイプはステータス移行にリンクされます。

事前定義済み移行タイプのアクティブ化

デフォルトでは、製品に付属する事前定義済みの遷移タイプはすべて非アクティブです。このため、ステータス遷移ボタンは有効ではありません。これらの移行タイプをアクティブ化して変更し、希望する移行フローに対応させることができます。

事前定義済み移行タイプをアクティブ化する方法

1. [移行タイプリスト] ページで [フィルタの表示] を選択します。
ページの上部には、追加の検索フィールドが表示されます。
2. [レコードステータス] フィールドで [非アクティブ] を選択し、[検索] をクリックします。
[移行タイプリスト] は、非アクティブな移行タイプをすべて表示します。
3. 該当する移行タイプを右クリックし、メニューから [編集] を選択します。
4. [レコードステータス] フィールドで [アクティブ] を選択します。
5. [保存] - [ウィンドウを閉じる] をクリックします。
6. [検索] をクリックします。
[移行タイプリスト] は、アクティブな移行タイプを表示します。

関連項目:

[インシデント ステータス遷移の事前定義済み遷移タイプ \(P. 528\)](#)

[リクエスト ステータス遷移の事前定義済み遷移タイプ \(P. 528\)](#)

インシデント ステータス遷移の事前定義済み遷移タイプ

以下の表は、インシデント ステータス遷移の事前定義済み遷移タイプについて説明しています。

シンボル	ボタン テキスト	フォーム ヘッダ テキスト	インシデント ステータス 移行
インシデント解決方法の承認ボタン	承諾	解決方法を承認	「解決済み」から「クローズ」
インシデント解決方法の拒否ボタン	拒否	解決方法を拒否	「解決済み」から「オープン」
インシデントのクローズ拒否ボタン	リクエストのクローズ	リクエストのクローズ	■ 「解決済み」から「未解決クローズ」 ■ エンド ユーザ応答 待機中 ■ ベンダー待機中 ■ 進行中 ■ 確認済み

リクエスト ステータス遷移の事前定義済み遷移タイプ

以下の表では、リクエスト ステータス遷移の事前定義済み遷移タイプを示します。

注: リクエストのクローズ リクエスト ステータスは、インシデントの解決済みステータスと同じです。

シンボル	ボタン テキスト	フォーム ヘッダ テキスト	リクエスト ステータス 移行
リクエスト解決方法の承認ボタン	承諾	解決方法を承認	「クローズ リクエスト」から「クローズ」

シンボル	ボタン テキスト	フォーム ヘッダ テキスト	リクエスト ステータス移行
リクエスト解決方法の拒否ボタン	拒否	解決方法を拒否	「クローズ リクエスト」から「オープン」
クローズ リクエストのリクエスト ボタン	リクエストのクローズ	リクエストのクローズ	■ 「オープン」から「キャンセル済み」 ■ エンド ユーザ応答 待機中 ■ ベンダー待機中 ■ 承認中 ■ 確認済み
リクエストのクローズ ボタン	クローズ	クローズ リクエスト	「進行中」から「クローズ」

タイマ

タイマは、さまざまなしきい値を持つストップウォッチとして機能し、アナリストに経過時間を知らせます。タイマには、各しきい値の時間を設定することができ、タイマの色やビープ音の設定も変更できます。また、各しきい値に達したときにリマインダを表示するように設定できます。サービスデスクのアナリストはストップウォッチを制御できません。これを制御できるのは管理者だけです。

リクエストは、タイマを使用する唯一のチケット タイプです。したがって、タイマは内部および結合のサービス デスク モデルでセットアップします。

タイマには、以下の定義済みのしきい値があります。

期間のしきい値	色
00:00:00	緑
00:01:00	黄
00:05:00	赤

定義済みの値では、タイマは緑で開始されます。1分経過すると、タイマは黄色に変わります。5分経過すると、タイマは赤に変わります。アナリストがリクエストを詳細ウィンドウに表示すると経過時間が表示され、新しいリクエストを選択するたびにこの時間がリセットされます。このプロセスに手順を追加したり、既存の手順を変更したりすることができます。

タイマは、アクティブまたは非アクティブとして設定できます。タイマを非アクティブとして設定すると、タイマはプロセスで使用されなくなりますが、将来使用できるように設定はそのまま残されます（つまり、データベースからは削除されません）。後でタイマを使用することにした場合は、設定に戻ってアクティブとしてマークします。

タイムゾーン

CA SDM システムでは、サーバ、サービス タイプ、連絡先、および場所に対し、特定のタイムゾーンをセットアップできます。特定のタイムゾーンに適用されるローカル サービス タイプおよび企業全体に適用されるグローバル サービス タイプをセットアップできます。このセットアップにより、管理者がサーバのタイムゾーンを確認し、さまざまなタイムゾーンに合わせてワーク シフトの時間を手動で調整する必要がなくなります。

関連項目:

[サービス タイプ イベント トリガ](#) (P. 531)

[タイムゾーン イベント トリガ](#) (P. 531)

[タイムゾーンのルール](#) (P. 532)

サービス タイプ イベントトリガ

サービス タイプでは、指定した延期時間が経過した後にトリガされるイベントを定義します。

例: ワークシフトスケジュールによるイベントトリガ

この例では、サービス タイプに関連付けられたワーク シフト スケジュールによって、イベントが実際にトリガされる時刻が以下のように制約されます。

- ワーク シフトは午前 8:00 ～午後 5:00。
- イベント遅延は 3 時間。
- 現在のサーバの時間は午後 3:00。

以下の理由から、イベントは翌日の午前 9:00 にトリガされます。

- 現在のサーバの時間によると、当日のワーク シフトはあと 2 時間残っています（現在の時間は午後 3 : 00 で、ワーク シフトの終了時間は午後 5:00）。
- イベント遅延は 3 時間です。この遅延のうち 2 時間は、当日のワーク シフトで使用されます（午後 3:00 ～午後 5:00）。1 時間は翌日のワーク シフトに繰り越されます（午前 8:00 ～午前 9:00）。

したがって、このイベントは翌日の午前 9:00 に開始されます。

タイムゾーン イベントトリガ

イベントのトリガ時間は、サービス タイプに関連付けられたタイム ゾーンの制約を受けます。

例: タイムゾーンによるイベントトリガ

この例では、サービス タイプに関連付けられたタイム ゾーンによって、イベントが実際にトリガされる時刻が以下のように制約されます。

- ワーク シフトは午前 8:00 ～午後 5:00。
- イベント遅延は 3 時間。
- 現在のサーバの時間は午後 3:00。
- タイム ゾーンの現在の時間は午後 12:00。

以下の理由から、イベントは当日の午後 6:00 にトリガされます。

- 現在のサーバの時間によると、当日のワーク シフトはあと 2 時間残っています（現在の時間は午後 3 : 00 で、ワーク シフトの終了時間は午後 5:00）。
- 現在のタイム ゾーンの時間によると、当日のワーク シフトはあと 5 時間残っています（現在の時間は午後 12 : 00 で、ワーク シフトの終了時間は午後 5:00）。
- イベント遅延は 3 時間（タイム ゾーンの時間で午後 12:00 ～午後 3:00、サーバの時間で午後 3:00 ～午後 6:00）です。

したがって、イベントはサーバの時間で午後 6:00、タイム ゾーン的时间で午後 3:00 に開始されます。

タイム ゾーンのルール

サーバ、場所、およびサービス タイプにタイム ゾーンを指定できます。また、チケットの影響を受けるエンド ユーザのタイム ゾーンを使用するように CA SDM に指定することもできます。CA SDM では、以下のルールに従って、イベントのトリガに使用するタイム ゾーンが決定されます。

- **影響を受けるエンド ユーザのタイム ゾーン - CA SDM** では、以下の条件を満たす場合、このルールを使用します。
 - [Use End User Time Zone] オプションがオンの場合
 - チケットの影響を受けるエンド ユーザにタイム ゾーンが指定されている場合
- **影響を受けるエンド ユーザのロケーション タイム ゾーン - CA SDM** では、以下の条件を満たす場合、このルールを使用します。
 - [Use End User Time Zone] オプションがオンの場合
 - チケットの影響を受けるエンド ユーザにタイム ゾーンが指定されていない場合
 - 影響を受けるエンド ユーザ ロケーションにタイム ゾーンが指定されている場合
- **サービス タイプのタイム ゾーン - CA SDM** では、以下の条件を満たす場合、このルールを使用します。
 - サービス タイプにタイム ゾーンが指定されている場合
 - [Use End User Time Zone] オプションがオフの場合

- **サーバのタイムゾーン - CA SDM** では、以下の条件を満たす場合、このルールを使用します。
 - サーバにタイムゾーンが指定されている場合
 - [Use End User Time Zone] オプションがオフの場合
 - サービスタイプにタイムゾーンが指定されていない場合
- **タイムゾーンのサポートなし - CA SDM** では、以下の条件を満たす場合、このルールを使用します。
 - サービスタイプにタイムゾーンが指定されていない場合
 - [Use End User Time Zone] オプションがオフの場合
 - サーバレコードがない場合

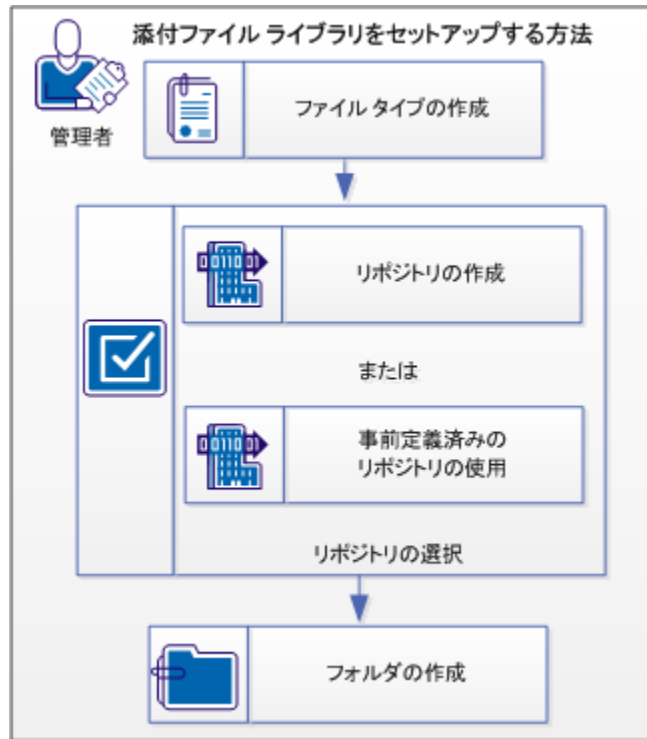
添付ファイル ライブラリをセットアップする方法

さまざまな **CA SDM** エンティティに、さまざまなタイプの添付ファイルを追加できます。たとえば、顧客は、インシデントにエラーのスナップショットを添付できます。管理者は、ユーザが添付ファイルをアップロードまたはダウンロードできる添付ファイル ライブラリをセットアップします。

添付ファイルは以下のように分類できます。

- **保存済み**：Web サーバは、HTTP プロトコルを使用して、リポジトリに格納済み添付ファイルをアップロードおよび格納します。アナリストが保存された添付ファイルを確認する際は、リポジトリからファイルを取得し、ローカルで表示します。ファイルの保存に Web サーバを使用すると、ユーザ インターフェースからファイルの保存や取得を実行できます。
- **リンク**：データベース内にファイルへのリンクのみを保存します。

以下の図は、添付ファイル ライブラリをセットアップする方法を示しています。



次の手順に従ってください:

1. [CA SDM Web UI を開きます。](#) (P. 222)
2. [ファイル タイプを作成します](#) (P. 535)。
3. [リポジトリを選択します](#) (P. 536)。
 - [リモート コンピュータ上でリポジトリをセットアップします](#) (P. 538)。
 - [リポジトリを作成します](#) (P. 539)。
 - [事前定義済みのリポジトリを使用します](#) (P. 539)。
4. [フォルダを作成します](#) (P. 545)。

CA SDM Web UI の表示

CA SDM の設定に応じて、以下のサーバから Web UI にログインします。

- 標準：プライマリまたはセカンダリ サーバ
- 高可用性：アプリケーション サーバまたはバックグラウンド サーバ

ファイル タイプの作成

CA SDM は、添付ファイルをサポートする事前定義済みのファイル タイプを提供します。たとえば、事前定義済みのファイル タイプとして、Adobe Acrobat は、添付ファイルとして pdf ファイル形式をサポートします。ファイル タイプを作成することもできます。たとえば、インシデントのスナップショットをアップロードするために JPEG ファイル タイプを作成します。

次の手順に従ってください：

1. CA SDM の設定に応じて、以下の CA SDM サーバから Web UI にログインします。
 - 標準：プライマリまたはセカンダリ サーバ
 - 高可用性：アプリケーション サーバまたはバックグラウンド サーバ
2. [管理] タブで、[添付ファイル ライブラリ] - [ファイル タイプ] を選択します。
[ファイル タイプ リスト] ページが開きます。
3. [新規作成] をクリックします。
[ファイル タイプの新規作成] ページが開きます。
4. 以下のフィールドを指定します。

タイプ

ファイル タイプまたは関連するソフトウェア アプリケーション (Word ドキュメント、イメージ、実行可能ファイルなど) を指定します。

拡張子

基本ファイル名に追加して、ファイル タイプを示す文字を指定します。たとえば、doc という拡張子は Microsoft の Word ドキュメントを示します。

アイコン名

このファイル タイプの識別に使用されるアイコンを含む画像ファイルの名前を指定します。

ステータス

レコードがデータベース内でアクティブになっていて、使用できるかどうかを示します。

5. [保存] をクリックします。
ファイル タイプが作成されます。

リポジトリの選択

添付ファイルはリポジトリに格納されます。また、ユーザが添付ファイルを使用して作業を行う前に、リポジトリをセットアップする必要があります。組織の要件に最も適合する数のリポジトリを追加できます。たとえば、添付ファイルとイメージを格納するために別々のリポジトリを追加することもできます。また、リポジトリにフォルダを追加してファイルをさらに分類してから、適切なロケーションにファイルをアップロードすることもできます。

すべてのクライアント インターフェースは、以下の場合を除き、添付ファイルのアップロードおよびダウンロードを実行するために既存のリポジトリにアクセスできます。

- 共有ファイル リポジトリにアクセスできるのは、共有ファイルにアクセス可能なコンピュータでリポジトリ デーモンを実行している場合のみです。リポジトリ レコード（詳細フォーム）のサーバ名は、共有ファイルにアクセス可能な **Windows** コンピュータの名前にする必要があります。また、**CA SDM** リポジトリ デーモンもそのコンピュータで実行する必要があります。
- **zip** ファイルのダウンロードは、そのファイルがアップロードされた時期に基づいて実行されます。旧リリースからの添付ファイルは、解凍せずにダウンロードされます。クライアント コンピュータでファイルを解凍しないと、クライアント インターフェースからアップロードされた添付ファイルも解凍せずにダウンロードされます。つまり、クライアントのダウンロード リクエストの処理中に、サーバでファイルが解凍されて返されます。

分散型アーキテクチャにより、必要性に応じてサイトでリポジトリを設定できます。リポジトリのサブレットは、必ずしも添付ファイルの保存先と同じサーバ上に存在する必要はありません。サイトでは、分散したすべてのリポジトリにアクセスできる中心的なサブレットを使用することも、リポジトリ サーバごとに専用のサブレットを使用することもできます。

リポジトリを設定する場合は、以下のセットアップ方法を検討してください。

- **保護された CA SDM サーバ上のリポジトリ サーバ**：ファイアウォールに守られ、保護された CA SDM サーバ上のリポジトリ サーバを使用するサイトでは、同じコンピュータでサブレットを実行する必要はありません。別の CA SDM サーバ上または制限がないほかの CA SDM サーバ上で実行されているサブレットを指定しても、そのリポジトリに対して正常にアップロードやダウンロードを行うことができます。リポジトリ サーバとサブレット サーバ間のネットワークに応じて、アップロードとダウンロードに何らかのパフォーマンスの影響が発生する場合があります。リモート リポジトリを設定する場合、リモートサーバ上にリポジトリと共に別のサーバをインストールして設定し、アップロードパスにローカルパスを設定するのが最適な方法です。詳細については、「[リモート コンピュータでのリポジトリのセットアップ](#) (P. 538)」を参照してください。
- **リポジトリ サーバと同じコンピュータ上のサブレット**：添付ファイルのアップロードとダウンロードで最適なパフォーマンスを実現したいサイトで、ネットワーク パフォーマンスが重視され、非常に大きなファイルを添付する場合は、このセットアップ方法を検討してください。この方法では、サーバの Tomcat ポート（通常は 8080）を開くので、コンピュータがファイアウォールで守られている場合は注意する必要があります。

CA SDM は事前定義済みのリポジトリを提供しています。また、組織の要件に最も適合するリポジトリを作成できます。以下のオプションから選択します。

- [リポジトリを作成します](#) (P. 539)。
- [事前定義済みのリポジトリを使用します](#) (P. 539)。

リモート コンピュータでのリポジトリのセットアップ

デフォルトでは、リポジトリは、CA SDM の設定に応じて以下のサーバに配置されます。

- 標準：プライマリ サーバ
- 高可用性：バックグラウンドサーバ

デフォルト リポジトリは、これらのサーバからサブレットとリポジトリ デーモン (`rep_daemon`) の両方を使用します。リモート コンピュータでリポジトリを作成するには、CA SDM の設定に応じて、以下のサーバをインストールおよび設定します。

- 標準：セカンダリ サーバサブレットはプライマリ サーバで実行され、`rep_daemon` はセカンダリ サーバで実行されます。
- 高可用性：バックグラウンドサーバ。サブレットはアプリケーション サーバで実行され、`rep_daemon` はバックグラウンドサーバで実行されます。

高可用性設定では、`rep_daemon` は、デフォルトではすべてのサーバで実行されます。

標準設定では、`rep_daemon` は、デフォルトではプライマリ サーバで実行されます。また、この設定では、`rep_daemon` がセカンダリ サーバで実行されることを確認する必要があります。

(標準設定のみ) 次の手順に従ってください:

1. [管理] タブで、[システム] - [環境設定] を選択します。
[構成リスト] ページが開きます。
2. セカンダリ サーバの設定を選択します。
[構成の詳細] ページが開きます。
3. [追加プロセス] をクリックします。
[追加プロセスのリスト] が表示されます。
4. [プロセスの追加] をクリックします。
5. [プロセス] として [リポジトリ デーモン] を選択します。
6. [保存] をクリックします。
リポジトリがセカンダリ サーバ上にセットアップされます。

添付ファイル リポジトリの作成

組織の要件に応じて、1つの大きなリポジトリ、または複数の小さなリポジトリを持つことができます。リポジトリの属性はすべてリポジトリ レコードで定義されるため、リポジトリの移動や結合は簡単です。

次の手順に従ってください:

1. [管理] タブで、[添付ファイル ライブラリ] - [リポジトリ] を選択します。

[リポジトリ] ページが開きます。

2. [新規作成] をクリックします。

[リポジトリの新規作成] ページが開きます。

注: 自身がサービス プロバイダである場合は、[リポジトリの新規作成] ページから適切なテナントを選択します。パブリック (共有) オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

3. 必要に応じて、リポジトリのフィールドに入力します。

4. [保存] をクリックします。

リポジトリが作成されます。

事前定義済みの添付ファイル リポジトリの使用

事前定義済みのリポジトリ (Service Desk、ナレッジ、またはイメージ) を使用できます。組織の要件に最も適合するように、リポジトリを編集できます。

次の手順に従ってください:

1. [管理] タブで、[添付ファイル ライブラリ] - [リポジトリ] を選択します。

[リポジトリ リスト] ページが開きます。

2. 編集するリポジトリを右クリックし、[編集] を選択します。

[リポジトリの更新] ページが開きます。

3. 必要に応じてフィールドを編集します。詳細については、「[リポジトリ] のフィールド」を参照してください。
4. [保存] をクリックします。
リポジトリ定義が保存されます。

[リポジトリ]のフィールド

以下のフィールドは、リポジトリの編集または作成に使用されます。

名前

リポジトリを一意に識別するための名前を指定します。たとえば、**Incident Images** リポジトリには、インシデントに関連するすべてのイメージを格納できます。

リポジトリタイプ

リポジトリに格納する内容のタイプを示します。たとえば、イメージ添付ファイルを格納するには、[イメージ] を選択します。

デフォルト

これが、指定されたりポジトリタイプのデフォルトリポジトリかどうかを示します。たとえば、ユーザがインシデントを作成中であり、そのインシデントに添付ファイルを添付する場合には、選択内容に対してデフォルトのリポジトリが表示されます。1つのリポジトリのみデフォルトに設定できます。

ファイルの制限サイズ(KB)

ユーザがリポジトリにアップロード可能なファイルの最大サイズをキロバイト単位で定義します。

アップロード パス

リポジトリにアップロードされたファイルが存在する場所の、完全なルート ディレクトリ パスまたは UNC パスを指定します。

UNC 認証情報

[アップロード パス] フィールドで指定した UNC パスにアクセスするための認証情報を指定します。[UNC 認証情報] をクリックして、[認証情報の検索] ページを開きます。

- 指定した UNC パスにアクセスするための認証情報をすでに作成している場合は、そのフィールドを使用して検索し、認証情報を選択します。
- 認証情報を作成する場合は、[新規作成] をクリックします。認証情報の作成の詳細については、「[UNC 認証情報の作成 \(P. 544\)](#)」を参照してください。

バックグラウンド サービス

サーバーレットパスおよび rep_daemon 用のバックグラウンド サーバ サービスを指定します。

なし

バックグラウンド サーバが、サーバーレットパスまたは rep_daemon 用に使用されないことを示します。このオプションを選択する場合は、[サーバーレット サーバ] フィールドおよび [リポジトリ サーバ] フィールドに値を入力します。

サーブレットのみ

サーブレットがバックグラウンドサーバでホストされることを示します。このオプションを選択すると、[サーブレットサーバ] フィールドには[バックグラウンドサーバ] の値が自動的に入力されます。[リポジトリサーバ] フィールドに値を入力します。バックグラウンドサーバがシャットダウンする場合、およびスタンバイサーバが新しいバックグラウンドサーバに昇格する場合には、[サーブレットサーバ] フィールドに新しいバックグラウンドサーバの値が入力されます。

デーモンのみ

`rep_daemon` がバックグラウンドサーバで実行されていることを示します。このオプションを選択すると、[リポジトリサーバ] フィールドには[バックグラウンドサーバ] の値が自動的に入力されます。[サーブレットサーバ] フィールドに値を入力します。バックグラウンドサーバがシャットダウンする場合、およびスタンバイサーバが新しいバックグラウンドサーバに昇格する場合には、[リポジトリサーバ] フィールドに新しいバックグラウンドサーバの値が入力されます。

サーブレットとデーモン

バックグラウンドサーバが、サーブレットパスおよび `rep_daemon` 用に使用されることを示します。このオプションを選択すると、[サーブレットサーバ] フィールドおよび[リポジトリサーバ] フィールドには[バックグラウンドサーバ] の値が自動的に入力されます。バックグラウンドサーバがシャットダウンする場合、およびスタンバイサーバが新しいバックグラウンドサーバに昇格する場合には、これらのフィールドに新しいバックグラウンドサーバの値が入力されます。

サーブレットサーバ

サーブレットが実行されているサーバを指定します。

リポジトリサーバ

`rep_daemon` が稼働中のサーバを指定します。

アーカイブ タイプ

リポジトリの内容に対して実行するアーカイブとパージアクションを指定します。

なし

アーカイブとパージのプロセスは実行されません。

アーカイブとパージ

履歴レコードは、[アーカイブ] フィールドで指定したファイルに書き込まれ、データベースからパージされます。

パージのみ

履歴レコードはデータベースからパージされますが、アーカイブファイルには書き込まれません。

アーカイブ パス

アーカイブ プロセスで、リポジトリ内のファイルが移動されるディレクトリ パスまたは UNC パスを指定します。

UNC 認証情報

UNC パスにアクセスするための認証情報を指定します。[UNC 認証情報] をクリックして、[認証情報の検索] ページを開きます。

- 指定した UNC パスにアクセスするための認証情報をすでに作成している場合は、そのフィールドを使用して検索し、認証情報を選択します。
- 認証情報を作成する場合は、[新規作成] をクリックします。認証情報の作成の詳細については、「[UNC 認証情報の作成](#) (P. 544)」を参照してください。

使用できないファイル タイプ

ユーザがリポジトリにアップロードできないファイルの拡張子。

注: このフィールド値が感嘆符 (!) で始まる場合、そのファイルタイプを現在のリポジトリで使用できます。たとえば、リスト内の値が「jpg.gif」の場合は、拡張子が .jpg と .gif のファイルがリポジトリで禁止されていることを示します。ただし、値が「!jpg.gif」の場合は、拡張子が .jpg と .gif のファイルのみがリポジトリで使用できることを示します。

UNC 認証情報の作成

UNC パスを使用して、ユーザが **CA SDM** サーバから共有リソースにアクセス可能にするための **UNC 認証情報**を作成します。

重要: **CA SDM** サーバがドメインにあり、共有場所が **WORKGROUP** にある場合、**UNC** コンポーネントは動作しません。また、**CA SDM** サーバ用の管理者パスワードおよび共有場所が異なる場合、それは動作しません。

次の手順に従ってください:

1. [一般設定] ページの [UNC 認証情報] をクリックするか、または [管理] タブで、[セキュリティと役割の管理] - [UNC 認証情報] を選択します。

[認証情報リスト] ページが開きます。

2. [新規作成] をクリックします。

[認証情報の新規作成] ページが開きます。

3. 必要に応じて以下のフィールドに値を入力します。

シンボル

検索時に認証情報を容易に識別するために一意の識別子を指定します。

ユーザ ID

UNC パスにアクセスするためのユーザ名を指定します。ユーザは、Service Desk サーバへのアクセス権を持つローカルまたはドメインの Windows ユーザにすることができます。

パスワード

UNC パスにアクセスするためのパスワードを指定します。

アクティブ

UNC 認証情報がアクティブであるか、非アクティブであるかを指定します。非アクティブな認証情報は使用できません。

4. [保存] をクリックします。

UNC 認証情報が作成されます。

フォルダの作成

フォルダを使用して、リポジトリ内のドキュメントを分類します。たとえば、**Images** リポジトリ下に **Error Images** フォルダを作成できます。このフォルダには、ユーザに表示されたすべてのエラー メッセージのスナップショットを含めることができます。**Service Desk** の添付ファイル リポジトリ タイプにはフォルダを作成できません。

次の手順に従ってください:

1. [管理] タブで、[添付ファイル ライブラリ] - [リポジトリ] を選択します。
[リポジトリ リスト] ページが開きます。
2. フォルダを作成するリポジトリを右クリックして、[フォルダの追加] を選択します。
[フォルダの新規作成] ページが開きます。
3. フォルダの名前およびそのコンテンツの説明を入力します。
4. [権限] タブを選択して、適切な[アクセス権](#) (P. 545) を指定します。
5. [保存] をクリックします。
フォルダが作成されます。

アクセス権

リポジトリ内のフォルダに以下のアクセス権を追加できます。

親から継承

このフォルダが、その親フォルダと同じ許可設定を持っていることを示します。このオプションは、サブフォルダに対してのみ表示されます。

グループによるコントロール

指定したグループに対する、このフォルダの読み取りまたは書き込みアクセス権を示します。このオプションは、すべてのフォルダおよびサブフォルダに対して表示されます。

全員に書き込み許可を付与

すべてのユーザが、フォルダに対して書き込みアクセス権を持つことを示します。

全員に読み取り許可を付与

すべてのユーザがフォルダに対して読み取りアクセス権を持つことを示します。読み取り許可では、フォルダを表示することはできますが、フォルダを編集または削除したり、フォルダにファイルを保存したりすることはできません。管理者権限があるユーザは、所属する許可グループがフォルダを編集できない場合でも、フォルダを編集できます。ドキュメントへのアクセスレベルが異なる複数の許可グループに所属するユーザには、より高いアクセスレベルが付与されます（たとえば、一方のグループに読み取り専用アクセスがあり、別のグループに書き込みアクセスがある場合、ユーザには書き込みアクセスが付与されます）。

注： [全員に書き込み許可を付与] チェック ボックスをオンにすると、 [全員に読み取り許可を付与] チェック ボックスが自動的にオンになります。

使用可能なグループ

すべてのグループを表示します。このリストからグループを選択できます。たとえば、グループを選択し、 [書き込み許可があるグループ] に対して [>] をクリックして、そのグループ内のすべてのユーザに、このフォルダに対する読み取りおよび書き込みアクセス権を付与します。 [フィルタの表示] を使用して条件を指定し、グループをフィルタします。

アナウンスメント

CA SDM を使用してユーザへのアナウンスメントを登録できます。アナウンスメントは、着信コールの回数を減らし、チケットを主体的に解決して生産性を高め、影響を受けるすべてのユーザに重要な情報を伝えるのに役立ちます。ユーザは格納されている複数のアナウンスメントをスクロールして参照できます。

注： アナウンスメントは、すべてのサービス デスク モデルで使用します。

新しいアナウンスメントを追加したり、既存のアナウンスメントを更新したりすることができます。アナウンスメントは、CA SDM のデータ参照機能の一部です。したがって、アクセス タイプを使用して、アナウンスメントを作成できる連絡先を制御できます。

アナウンスメントは、以下のどちらかまたは両方を指定できます。

ロケーション

都市、建物、フロアなど、物理的なロケーションを指定します。

組織

組織 ID を指定します。組織をアナウンスメントに設定すると、その組織に割り当てられた個人のみがアナウンスメントを参照できます。

ロケーションまたは組織をアナウンスメントに設定すると、そのロケーションまたは組織の連絡先のみがアナウンスメントを受信できます。どの連絡先でも、ロケーションまたは組織によって制限されていないアナウンスメントはすべて参照できます。たとえば、どちらも設定されていない場合、すべての場所と組織の連絡先がアナウンスメントを参照できます。

注: Web インターフェースの管理機能を使用して、アナウンスメントを指定できます。アナウンスメントの定義方法については、オンラインヘルプを参照してください。

関連項目:

[内部アナウンスメントの表示設定](#) (P. 547)

[アナウンスメントの緊急度の指定](#) (P. 548)

内部アナウンスメントの表示設定

「アナウンスメントの新規作成」ページの「内部」チェックボックスを使用して、アナウンスメントを内部ユーザーに表示するかどうかを制御できます。ユーザーが内部向けの項目を表示できるかどうかは、ログインユーザーのアクセスタイプの「内部ログを表示する」設定で制御します。

アナウンスメントの緊急度の指定

アナウンスメント レコードの緊急度は指定できます。

アナウンスメントの緊急度を指定するには、以下の手順に従います。

1. アナウンスメントを作成するか、または、[アナウンスメントの詳細] ページに移動して既存のアナウンスメントを編集します。
2. [アナウンスメント タイプ] ドロップダウン リストから以下のいずれかの値を選択します。

通常

黒いテキストで表示されます。

勧告

オレンジ色のテキストで表示されます。

緊急

赤いテキストで表示されます。

[保存] をクリックします。

アナウンスメント レコードは、[アナウンスメント リスト] ページ内でコードが色分けして表示されます。

ストアド クエリのセットアップ

CA SDM では、ストアド クエリを使用して以下の 2 種類のデータを作成できます。

- スコアボードクエリを使用すると、該当する項目のカウンタ フィールドを追加して、Web インターフェース スコアボードをカスタマイズできます。
- KPI クエリを使用すると、カウンタの値で特定の期間の履歴情報を取得して、Web ベースのレポートの作成で使用できます。

ストアドクエリは、すべてのサービスデスクモデルで使用します。ストアドクエリは、ユーザに新しいページを表示することを目的としていません。

ユーザに使用を許可するストアドクエリは、管理者が定義します。管理者は、**CA SDM** でインストールされた定義済みストアドクエリを使用できます。また、独自のクエリを定義することもできます。**Web** インターフェースの管理機能を使用して、ストアドクエリを定義できます。

ストアドクエリの定義に関する以下の情報を考慮してください。

- 有効なストアドクエリ節は、適切な **select** ステートメントに統合され、基礎となる **DBMS** エンジンに渡されて処理されます。**SELECT** ステートメントを開発するには、以下のディレクトリにあるオブジェクト定義ファイルを参照してください。
 - Windows : `installation-directory¥bopcfg¥majic` ディレクトリ
 - UNIX : `$NX_ROOT/bopcfg/majic` ディレクトリ
- ストアドクエリでは、**SQL WHERE** 節を指定するときに、データベースレベルのフィールド名ではなく、オブジェクトや属性のステートメントを使用します。
- **CA SDM** では、ストアドクエリで直積結合を使用できません。作成したストアドクエリが直積結合になっていないか、システムに応じて以下のコマンドを入力して確認します。
 - Windows : `bop_cmd -f installation-directory¥bopcfg¥interp¥bop_diag.frg "check_queries()"`
 - UNIX : `bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"`

実行後、フラグがついたクエリはすべて更新し、直積結合を解消してください。

- **URL** ストアドクエリは、ストアドクエリの作成時に提供されるオプションです。**URL** ストアドクエリは、クエリを実行し、ナレッジマネジメントでのみ使用される数値の結果を返します。

注: オブジェクト定義の構文の詳細については、「テクニカルリファレンスガイド」を参照してください。ストアドクエリの定義の詳細については、オンラインヘルプを参照してください。

シーケンス番号

チケットをオープンすると、チケットには使用可能な次のシーケンス番号が自動的に割り当てられます。たとえば、前回オープンされたリクエストが 5 だった場合、使用可能な次の番号は 6 になります。

重要: CA SDM の新しいバージョンをインストールした後は、すべてのチケットの内部レコード ID が 1 にリセットされます。重複したレコード ID が作成されないように、バックアップデータを復元する前にチケットを作成しないでください。

リクエスト、変更要求、および案件の採番方法をカスタマイズするには、それぞれの採番スキームに固有のプレフィクスまたはサフィックスを含めます。たとえば、リクエストを月別にトラッキングする場合は、リクエストの採番スキームに月の識別情報としてプレフィクスまたはサフィックスを追加できます。

注: Web インターフェースの管理機能を使用してチケットの採番方法をカスタマイズする方法については、オンライン ヘルプを参照してください。

それぞれのチケットのタイプに異なる採番スキームを定義するので、すべてのサービス デスク モデルに採番スキームをセットアップします。リクエスト、変更要求、および案件の採番形式は、シーケンス番号設定で変更できます。初期設では、新しいチケットは連続する整数で採番されます。チケットの実際の番号フィールドは数値フィールドではなく文字列フィールドなので、管理者は、新しいチケットのチケット番号生成時にプレフィクスまたはサフィックスとして使用できる追加の文字列値を指定できます。たとえば、リクエスト、変更要求、およびインシデントのプレフィクスとして r:、c:、および i: を指定できます。この設定により、ユーザはさまざまなチケット タイプを簡単に区別できるので、混乱を防ぐことができます。

インシデントと問題は採番スキームをリクエストと共有します。これは、インシデントと問題が、内部的にはタイプが異なるリクエストであるためです。

監査ログの使用

CA SDM では、以下の情報を記録する監査ログを作成します。

- 案件に関するすべての変更 (Issue)
- 要求に関するすべての変更 (Call_Req)
- 変更要求に関するすべての変更 (Change_Request)
- データ パーティション (Domain) テーブルに関するすべての変更
- 変更に関連付けられている人物のログイン ID と、関連付けられた曜日/日付/タイム スタンプ
- 更新、挿入、および削除の前後の値
- 連絡先の作成
- nr オブジェクトに対するアクティビティの作成と更新

注: 監査ログには、連絡先データ パーティション フィールドへの変更のみが収集され、その他の連絡先レコードの更新は収集されません。

監査ログ機能は自動的にインストールされるため、機能を有効にするには、オプション マネージャを使用して、2 つの監査ログ オプション `audit_ins` および `audit_upd` をインストールできるようにします。これらのオプションをインストールすると、[管理] タブの [Service Desk] - [監査ログ リスト] を選択して、監査ログにアクセスできるようになります。ユーザは、ビルトインの検索ツールを使用して監査ログ リストを検索したり、監査ログ リストを使用してレポートを生成したりすることができます。

注: オプションの値のインストールおよび設定方法については、オンライン ヘルプを参照してください。

CA ネットワークとシステム管理の統合

イベント管理メッセージ レコードを定義し、CA NSM でメッセージ レコードアクションを関連付けることで、リクエストの自動作成、既存リクエストへのコメントの添付、または CA SDM へのアナウンスメントの登録を実行できます。

注: CA NSM 統合の詳細については、「実装ガイド」を参照してください。

CA SDM Web ページの印刷

CA SDM は、ボタンとノートブック タブをフォーマットするために背景グラフィックを使用します。多くのブラウザのデフォルトの設定では、これらの背景画像を印刷しないようになっています。そのため、ブラウザのメニューまたは **CA SDM** のメニューで [ファイル] - [印刷] を選択した場合、印刷されたページにはボタンやタブの角だけが表示されます。

Internet Explorer で CA SDM Web ページを印刷する方法

1. [ツール] - [インターネット オプション] を選択します。
[インターネット オプション] ダイアログ ボックスが表示されます。
2. [詳細設定] タブを選択します。
3. 下にスクロールして [印刷] を表示し、[背景の色とイメージを印刷する] オプションをオンにします。
印刷された **CA SDM Web** ページには背景グラフィックが含まれます。

Firefox で CA SDM Web ページを印刷する方法

1. [ファイル] - [ページ設定] を選択します。
2. [書式とオプション] タブを選択します。
3. [背景色と背景画像も印刷] チェック ボックスをオンにします。
印刷された **CA SDM Web** ページには背景グラフィックが含まれます。

Web インターフェイスでのレコード ロック動作

ユーザが Web インターフェイスを使用してデータベース レコードを編集する際は、デフォルトでレコードに対する独占的なロックが 2 分間与えられます。 `web.cfg` ファイル内の `ExclLockSeconds` プロパティを使用して、デフォルトの時間を変更できます。

データベース レコードがユーザの変更によって更新される場合は、以下の条件に従います。

- ユーザが割り当てられた時間内に編集し変更内容をサブミットできれば、変更内容がデータベースに反映されます。

データベース レコードがロックされている間、ほかのユーザ (Web および Web 以外のユーザ) はレコードを表示することはできますが編集することはできません。ロックされているレコードを別のユーザが編集しようとする、エラー メッセージが表示されます。

- ユーザが割り当てられた時間内に編集し変更内容をサブミットできなければ、レコードのロックは自動的に解除され、ほかのユーザがレコードを編集できるようになります。

ユーザが更新をサブミットすると、タイムスタンプがチェックされ、ほかのユーザによってレコードが変更されていないことが確認されます。その後、以下の処理が実行されます。

- 独占的なロックが解除されてからレコードが変更されていない場合は、ユーザの更新情報がデータベースに保存されます。
- ロックが期限切れになった後にほかのユーザがレコードを編集した場合は、保存しようとするエラー メッセージが返されて、変更は保存されません。ユーザは編集プロセスをやり直して、変更内容を再入力する必要があります。

関連項目:

[環境設定ファイルの変更](#) (P. 629)

サポート構造

サービスデスクのサポート構造は、問題の解決に必要なコンポーネントで構成されます。サポートモデル（内部、外部、または両方）に一致するように、CA SDM サポート構造をセットアップできます。

注: 案件、リクエスト、および変更要求は、サイトのニーズに合わせてカスタマイズできます。詳細については、「実装ガイド」およびオンラインヘルプを参照してください。

CAPA ヘルプの有効化

CA Productivity Accelerator (CAPA) は、CA SDM アナリスト Web フォームのコンテキスト依存インアプリケーションパフォーマンスサポートを提供します。CAPA プレーヤパッケージは、CA SDM アナリスト Web ページのコンテキストヘルプメニューと直接統合します。CAPA ヘルプコンテンツと CA SDM の統合は、ヘルプメニュースクリプトを介して達成されます。これらのスクリプトは、CA SDM の [ヘルプ] メニュードロップダウンおよび右クリックで表示されるコンテキストヘルプから、CAPA の記録したヘルプコンテンツを起動します。

注: このトピックには、CAPA 記録ツール、CAPA ヘルプコンテンツの取得と設定、Smart Help のインストールに関する情報は含まれていません。

CA SDM は、各 Web フォームを一意に認識する一意の識別子を提供します。識別要素が CA SDM の一番上のフレームに存在する場合、CAPA 記録ツールは Web アプリケーションフォームを認識できます。トップフレームが認識されると、すべてのサブフレームがこのアプリケーションの一部であると見なされます。また、別のドメインからロードされるサブフレームも識別する必要があります。識別されない場合は、CA SDM の一部と見なされません。CAPA ヘルプを有効にするには、ヘルプコンテンツを準備し、CAPA ヘルプを起動するオプションを設定する必要があります。

注: HTML ファイルをカスタマイズするには、CAPA レコーダの `ias_helper.js` ファイルからの呼び出し方法を使用して `html` フォームを認識します。

CAPA ヘルプは、CA SDM 従業員、顧客、または PDA インターフェースではサポートされていません。CAPA をサポートするブラウザの詳細については、CAPA のドキュメントを参照してください。

次の手順に従ってください：

1. 以下の CA SDM ディレクトリから `capa.properties` ファイルを開きます。

`%NX_ROOT/bopcfg/www/wwwroot`

2. ファイル内の以下の値を変更します。

- `Enable_Alerts = 0`。このオプションでは、CA SDM Web ページをロードするときに、ブラウザ コンソール内で JavaScript 警告メッセージが確認および表示されます。

3. ファイルを保存します。

4. CA SDM ディレクトリ内の `web.cfg` ファイルに移動し、`DebugScript=1` を追加し、Web エンジンを実行します。

記録されたコンテンツが CAPA サーバで準備、発行、および展開されます。

5. `capa.properties` ファイルを開き、以下の値を変更します。

- `Enable_For_Recording = 0`
- `Show_Learn_Links = 1`。この値では、CA SDM ヘルプ メニューおよび右クリックで表示される [ヘルプ] コンテキストメニューに CAPA ヘルプのオプションが表示されます。
- `Server_Name` = CAPA 発行コンテンツが展開されるサーバの名前。
- `Server_Port` = CAPA 発行コンテンツが展開される CAPA サーバ ポート。たとえば TOMCAT ポート。
- `Virtual_Dir` = CAPA 発行コンテンツが CAPA サーバ上に展開される仮想ディレクトリ。
- `Namespace` = アプリケーション コンテキスト ネームスペース。たとえば、`app.SDM.Project123;en`。
- `Enable_Alerts = 0`

6. ファイルを保存します。

CA SDM アナリスト Web フォームから CAPA ヘルプを実行する準備ができています。

第 11 章：システムの動作の制御

このセクションには、以下のトピックが含まれています。

[オプション マネージャの使用](#) (P. 557)

オプション マネージャの使用

CA SDM Web クライアントでは、[管理] タブからオプション マネージャを使用して以下のアクションを実行できます。

- 使用可能なすべてのオプションのリストを入手します。
- 関連付けられているアプリケーション、簡潔な説明、そのステータスなど、各オプションの概要を表示します。
- 特定のオプションの詳細を表示する

オプションの詳細情報を表示しているときには、オンライン ヘルプでそのオプションの機能の詳細を確認できます。オンライン ヘルプには、オプションを変更する際に実行する必要がある特別なアクションについても記載されています。たとえば、一部のオプションでは、オプションをインストールまたはアンインストールした後にオプションを有効にするには、CA SDM サーバを再起動する必要があります。オンライン ヘルプの説明にも、それが示されています。

- すべてのオプションのステータスを概要レベルで確認する
- 使用可能なオプションのいずれかをアンインストールします（バックグラウンドサーバでのみ適用可能）。

オプションの多くは、CA SDM のインストール時にインストールされ、あらかじめ設定されます。オプション マネージャを使用してオプションをインストールまたはアンインストールすると、一部またはすべての初期設定が変更される可能性があります。

- 定義済みの任意のオプションのインストール（バックグラウンドサーバでのみ適用可能）

注: リリース サイクル中に、ユーザからのリクエストに応じて、CA SDM サポートを通してオプションが提供されることがあります。これらのオプションの詳細については、CA SDM サポートにお問い合わせください。オプションマネージャの使用方法的詳細については、オンライン ヘルプを参照してください。

システム環境を変更する方法

CA SDM では、環境テンプレート ファイル (NX.env.tpl) 内で指定された環境変数を使用して、特定の動作を決定します。システムの動作の一部は、環境変数を使用して変更できます。通常はオプション マネージャを使用してシステムの動作を制御しますが、CA テクニカル サポートから特定の環境変数を直接変更するように指示されることもあります。

環境テンプレート ファイルを編集する場合は、以下の点に注意してください。

- このファイルに設定する環境変数は、プロセスが実行されるプロセス空間内の環境変数を設定して無効化することができます。この設定は、特定の状況では役立ちますが、通常は必要ありません。変数の設定の前に (@) 記号を付けると、その変数はプロセス空間の変数によって上書きされません。上書きを許可する特定の理由がない限り、テンプレート ファイルの変数名の前には必ず @ 記号を付けてください。
- このファイルのコメント文字は、シャープ記号 (#) と感嘆符 (!) です。感嘆符は、オプションの無効化にも使用できます。

重要: テンプレート ファイル (NX.env.tpl) を変更し、設定プロセスで環境ファイルに変更を適用できるようにします。環境ファイル (NX.env) は絶対に直接変更しないでください。

次の手順に従ってください:

1. システム環境に応じた環境テンプレート ファイル (.tpl) をバックアップします。
 - UNIX - \$NX_ROOT/pdmconf/NX.env.tpl
 - Windows - インストール ディレクトリ¥pdmconf¥NX.env_nt.tpl-

2. CA SDM の設定に応じて、以下のサーバ上の環境テンプレート ファイルを編集します。

- 標準：プライマリ サーバ
- 高可用性：いずれかのスタンバイ サーバ

注：このファイルは、任意のテキスト エディタを使用して表示および変更できます（Windows ユーザはワードパッドを使用します）。

3. サポート技術者の指示に従って変更を行い、ファイルを保存します。
4. プライマリ サーバまたはスタンバイ サーバ上で環境設定ユーティリティを実行し、環境テンプレート ファイルに行った変更を実際の環境ファイルに適用します。

注：環境設定ユーティリティの実行方法については、「実装ガイド」を参照してください。

5. CA SDM の設定に応じて、以下のいずれかのアクションを実行します。
 - 標準：プライマリ サーバを再起動して、環境ファイルに行った変更を適用します。

- 高可用性： [すべての CA SDM サーバを再起動します \(P. 57\)](#)。

注：システムのシャットダウンを回避するため、CA SDM サーバ全体を再起動するのではなく、特定のプロセスのみを再起動するようにサポート技術者から指示されることがあります。

イベント

オブジェクトに添付されているイベントを設定し、設定されたアクションを実行することができます。 イベントとは、一定時間経過後に実行される手順です。たとえば、「優先度 1」に設定されている案件が 1 時間以内に受信されない場合、イベントによってサービスデスク アナリストにメッセージが送信されるようにできます。システムの他の部分では、サービス タイプなどのイベントを使用します。

リクエスト、インシデント、問題、変更要求、案件、連絡先、構成アイテム、グローバル テナントおよび特定のテナントにイベントを定義できます。 CA SDM は、遅延時間とワークシフトに基づいてイベント実行時間を予定します。

注：イベントの詳細については、オンライン ヘルプを参照してください。

マクロ

マクロとは、条件またはアクションを定義する小さなスクリプトです。イベントまたは動作が実行されたときに、1つ以上のアクションマクロを実行できます。マクロを実行する前に条件付きマクロを使用して、実行するアクションマクロのセットを決定できます。

以下の領域でマクロを使用できます。

- イベント
- 案件または動作変更テンプレート
- アクティビティ通知

製品にはいくつかのマクロが含まれています。ユーザは追加のタイプを作成できます。

注: カスタマは、アクションマクロまたは条件付きマクロを追加できませんが、サイト定義の条件を使用して単純な条件を作成できます。サイト定義の条件は単純なマクロで、GUI ダイアログ ボックスから作成できます。これらは、条件タイプのマクロの代わりとなるものではありません。

各マクロでは、マクロで使用するオブジェクト タイプを指定する必要があります。サイト定義の条件を作成してリクエストの値を確認する場合は、タイプをリクエストに設定する必要があります。イベントおよび動作のマクロを選択すると、CA SDM では、タイプがイベントまたは動作に一致するマクロのみが表示されます。

マクロ タイプ

マクロには以下のタイプがあり、それぞれ用途を表しています。

アクション

案件の優先度を上げるなど、いくつかのタイプのアクションを実行します。

イベントの添付

変更、案件、リクエスト、連絡先、または構成アイテムにイベント オブジェクトを添付します。

条件

いくつかの true/false 条件を評価します。

CA IT PAM アクションの実行

CA IT PAM アクションを実行します。CA IT PAM は、電子承認を必須にできるタスク グループの管理とレポートを有効にするワークフローエンジンです。

CA Workflow アクションの実行

CA Workflow アクションを実行します。CA Workflow では、特定のカテゴリまたは領域に関連付けられたチケットで行われるアクティビティの追跡など、ユーザの環境でワークフロー プロセスを管理できます。

リモート参照

サーバ上で外部プログラムを起動します。

複数通知

1 つ以上の連絡先に通知を送信します。このマクロ タイプは、メッセージ、受信者、および緊急度レベルを指定できるため特に便利です。

Site-Defined 条件

true/false 条件、およびサービス レベルを適用するチケットの属性に基づいてイベントを作成します。たとえば、リクエストの優先度が 1 でまだ割り当てられない場合は true を返すような条件付きマクロを作成できます。この条件は、リクエストを作成した直後に実行されるイベントに添付できます。

イベントでのマクロの使用

[イベントの詳細] で、[イベント条件] フィールドに条件付きマクロを必要に応じて指定できます。また、[Execute on True] および [Execute on False] 列に任意の数のマクロを指定することもできます（条件付きマクロを除く）。イベントが実行されると、まず条件付きマクロが評価されます。評価結果が true の場合、[True] 列内のすべてのマクロが実行されます。評価結果が false の場合、[False] 列内のすべてのマクロが実行されます。条件付きマクロは、担当者が設定されているかどうかや、優先度レベル、サービス タイプ違反などを確認できます。イベント条件マクロが指定されていない場合、イベントは自動的に True マクロを実行します。

イベントの詳細で、あらゆるタイプのマクロを選択して、連絡先に通知を行ったり、コンテキストオブジェクトに値を設定したり、リモート参照を実行したり、ほかのイベントを添付したりすることができます。

案件および変更カテゴリの動作でのマクロの使用

案件カテゴリおよび変更カテゴリの動作でマクロを使用することもできます。カテゴリの詳細で、[ワークフロー] タブを参照して、ワークフローのステータスを選択できます。ワークフローの詳細で、[動作] ボタンをクリックします。イベントと同様、条件および結果のアクションを設定できます。

動作の詳細の[移行] タブで、条件付きタイプのマクロを指定して、タスクがそのステータスから移行できるかどうかを決定できます。このマクロは、ユーザがタスクのステータスを別の値に変更しようとしたときに実行されます。条件の評価結果が **false** の場合、ステータスの更新は許可されません。

実際のワークフロー タスクは、カテゴリ テンプレート内のテンプレートから作成されます。タスクのステータス値を変更して保存すると、カテゴリ テンプレートに指定されている動作が実行されます。つまり、条件および結果のアクションが実行されます。

注: イベントをワークフロー タスクに添付するには、イベントの添付マクロを使用してください。

複数通知でのマクロの使用

複数通知

複数の通知のメッセージ本文は、選択したオブジェクトのテーブルを直接ポイントします。このため、オブジェクト テーブル上のフィールド（たとえば、CR (Call_Req)）を参照するときに、フィールドの属性名を参照できます。コール リクエスト チケットの説明情報を指定する場合は、メッセージ本文に以下を入力できます。

説明: @{description}

QREL (クエリ関係) は、SQL タイプ WHERE 節によって定義されたオブジェクトのリストを含んでいる関係です。QREL を複数通知マクロの説明に追加できます。act_log QREL <-- alg の説明に QREL を入力したい場合は、通知マクロに以下を使用できます。

@{act_log.0.description}

置換変数を使用すると、通知メッセージの関連性を強めて、より動的になります。これらの置換変数は、@{attribute_path_here}の形式で表します。attribute_path_here は、CA SDM オブジェクトの属性です。通知を送信すると、指定した属性値で変数が置き換えられます。

アクティビティ ログまたは複数通知からの通知には、常に何らかのベース コンテキスト（参照ポイント）が含まれていて、通常これはチケットまたはワークフロー タスクです。複数通知では、[通知マクロタイプ] フィールドはベース オブジェクトを指定します。@{}構文を使用して、そのオブジェクトのあらゆる属性を参照できます。

例：タイプがリクエストの複数通知は、「cr」（Call_Req）オブジェクト内のあらゆる属性を参照できます。リクエストの説明を含めるには、@{description}を指定します（ドット表記を使用して、ほかのオブジェクトへの参照を続けることができます）。たとえば、リクエスト担当者の姓を含めるには、{assignee.last_name}を指定します。

サイト定義の条件付きマクロの使用

サイト定義の条件

条件付きマクロは、1つ以上の *Atomic* 条件で構成されています。各アトムは、1つの属性の値をテストします。このため、ユーザが担当者およびカテゴリの値に基づいて条件を定義する場合、条件付きマクロは担当者用とカテゴリ用にそれぞれ1つのアトムを使用します。イベントで条件付きマクロを使用した場合は、個々のアトムがブール演算子（主に「AND」または「OR」）で結合されます。

条件付きマクロの詳細には、以下のようなアトムのリストが表示されます。このリストは、左から右に向かって読まれます。

属性	演算子	値	論理演算子	意味
Assignee	等しい	Jones	および	担当者は Jones で、
財務	より小さい	600	または	コストは 600 未満の整数値であるか、
グループ	Empty/NULL		および	[グループ] フィールドが空である。

注：論理的なコネクタ（AND、OR）は2つの原子を接続します。one および two という2つのアトムがある場合、これらはアトム one の結合子で結合されます。アトム two の結合子は使用されません。さらに、属性値によっては一部の演算子を使用できません。たとえば、属性が「担当者」の場合、演算子に「より小さい」を使用すると無効になります。条件付きマクロの作成の詳細については、オンライン ヘルプを参照してください。

第 12 章：自動割り当ての設定

このセクションには、以下のトピックが含まれています。

[自動割り当て](#) (P. 565)

[自動割り当ての関係](#) (P. 566)

[自動割り当てメソッド](#) (P. 566)

[自動割り当てを実装し始める方法](#) (P. 567)

[デフォルトのグループと担当者](#) (P. 574)

[自動割り当てを有効にする](#) (P. 575)

[自動割り当て設定](#) (P. 576)

[割り当て制御](#) (P. 577)

[アクティビティのログ記録](#) (P. 580)

[追加の属性に対するアクティビティ ログの有効化](#) (P. 581)

[自動割り当てのトレース](#) (P. 582)

[ストアドクエリ](#) (P. 582)

[自動割り当てでのチケット割り当て方法](#) (P. 583)

[自動割り当てでのワークフロー タスクの割り当て方法](#) (P. 590)

[構成アイテムベースの自動割り当て](#) (P. 594)

自動割り当て

CA SDM の自動割り当てにより、アナリストへのチケットの割り当て処理を自動化することで、チケットの管理に必要な時間を大幅に縮小できます。この自動化の結果、作業負荷の分散と作業スケジュールの調整に関連するタスクをよりいっそう効率的にすることができます。

自動割り当てを設定して、以下の要因に基づいてチケットを割り当てることができます。

- どのアナリスト グループがどのチケットまたはタスクを操作するか
- いつ仕事を終了する必要があるか
- どのロケーションが、影響を受ける顧客にサービスを提供するか
- 各アナリストの作業負荷および可用性
- チケットと関連付けられた構成アイテムの属性の値

注: [構成アイテムに基づいた自動割り当て](#) (P. 594)を行うと、リクエスト/インシデント/問題のグループ固有の割り当てのみ作成できます。

自動割り当ては一度にすべて実装する必要はありません。段階的に導入する戦略を作成できます。たとえば、選択されたチケットタイプ、アナリストグループ、またはロケーションでのみ有効にすることから始めることができます。

自動割り当ての関係

自動割り当て処理には、多くの **CA SDM** エlement が必要になることがあります。Element の関連付けは以下のとおりです。

- 領域およびカテゴリとグループ/ロケーション/ワークシフトの関連付け
- グループとロケーション/ワークシフトの関連付け
- **CA Workflow** テンプレートと連絡先の関連付け

自動割り当ての管理を簡単にするために、すべての関係はいずれの関連Element からでも保守できます。たとえば、アナリストグループを変更カテゴリに関連付ける場合、[変更カテゴリの詳細] ページまたは [グループの詳細] ページのいずれかの関連付けを維持できます。

自動割り当てメソッド

以下の基本メソッドを使用すると、チケットを自動的に割り当てることができます。

場所に基づいた自動割り当て

以下のアイテムに基づいてすべてのチケットタイプに割り当てを作成します。

- グループ、ロケーション、およびワークシフトに関連付けられた領域とカテゴリ
- ロケーションおよびワークシフトに関連付けられたグループ
- 連絡先に関連付けられた **CA Workflow**

注: 場所に基づいた自動割り当ては単に自動割り当てと呼ばれます。

構成アイテムに基づいた自動割り当て

リクエスト、問題、およびインシデントのチケットタイプのグループ割り当てを以下に基づいて作成します。

- 構成アイテムに関連付けられたチケットに関連する領域
- 連絡先/グループ情報の記録に使用された構成アイテムの属性

任意のリクエスト/インシデント/問題領域で使用するよう選択できるアルゴリズムは 1 つのみであるため、場所に基づいた自動割り当ておよび構成アイテムに基づいた自動割り当ては排他的オプションです。場所に基づいた自動割り当ておよび構成アイテムに基づいたメソッドは、作成された場合、どちらもチケットを割り当てるのに使用されます。ただし、構成アイテムに基づいた自動割り当ては、リクエスト/インシデント/問題チケットの領域または構成アイテムが変更された場合にもチケットの割り当てを再評価するため、異なります。構成アイテムに基づいた自動割り当てが指定されたのに、チケットのグループ割り当てを正常に生成しない場合、**Area_Defaults** オプションに相談することによって [領域] のデフォルトの [グループ] および [担当者] の値を使用してチケットを割り当てるべきかどうか決定します。

自動割り当てを実装し始める方法

選択されたアナリスト グループおよびアナリストの自動割り当てを実装し始めるには、以下のガイドラインに従います。

1. 自動割り当てを有効にする 1 つ以上の領域またはカテゴリを識別します。

注: サイトの領域およびカテゴリの設定を確認するには、**CA SDMWeb** インターフェースでそれらの設定を調べます。手順については、オンライン ヘルプを参照してください。

2. デフォルトでは、自動割り当ては無効です。自動割り当てを使用する [領域およびカテゴリ](#) (P. 568) に対してのみ、これを有効にします。
3. 指定した領域またはカテゴリと、その領域またはカテゴリを介して割り当て対象のチケットとなる [アナリストグループ](#) (P. 568) との関係を作成します。
4. [アナリスト](#) (P. 569) グループの各メンバを使用可能としてマークします。

領域とカテゴリ

注: 領域およびカテゴリの設定時には、[デフォルトのグループおよび担当者](#) (P. 574)を設定することを検討してください。

リクエスト、インシデント、および問題チケットの自動割り当てを設定するには、[リクエスト/インシデント/問題領域の詳細] ページの [自動割り当て] タブで以下のコントロールを使用します。

- グループの更新
- ロケーションの更新
- ワークシフトの更新

注: 自動割り当てを有効にするチェック ボックスも、これらの各ページの [自動割り当て] タブにあります。 ページが編集モードのときのみ表示されます。

インターフェースの以下のページには、変更要求と案件の自動割り当てを設定するための同じコントロールがあります。

- 変更カテゴリの詳細
- 案件カテゴリの詳細

アナリストグループ

自動割り当てを設定するには、少なくともアナリストグループと領域またはカテゴリとの関係を定義する必要があります。 担当者は、指定された自動割り当て基準をすべて満たしたグループから選択されます。 追加の制約が定義されていない場合、チケットは、アクティブなチケットが最も少ないグループメンバーに自動的に割り当てられます。

領域またはカテゴリにグループが関連付けられていない場合は、デフォルトのグループと担当者が割り当てられます。 これらのデフォルトが定義されていない場合、チケットは手動割り当てのままです。

グループと領域/カテゴリとの関係は、[area detail] ページまたは [カテゴリの詳細] ページで保守できます。

あるいは、以下のコントロールを使用することにより、[グループの詳細] ページの [自動割り当て] タブで同じ関係を維持できます。

- リクエスト領域の更新
- 変更カテゴリの更新
- 案件カテゴリの更新
- ロケーションの更新

アナリスト

[アナリストの詳細] ページのフィールドにより、自動割り当て可能なアナリストかどうかを判別することができます。

アナリストは、使用可能とマークされている場合のみ自動割り当て可能です。

[アナリストの詳細] ページには、自動割り当てを有効にする [使用可能] チェック ボックスがあります。

アナリストが自動割り当てを使用可能かどうかを自身で制御できるようにすることを検討してください。ストアドクエリを使用することで、アナリストが使用可能かどうかを監視できます。

注: ワークフロー タスクの自動割り当てでは、[使用可能] チェック ボックスは考慮に入れられません。

[作業スケジュール] フィールドにより、アナリストは指定した作業スケジュール中だけチケットが自動割り当てされるようにすることができます。作業スケジュールが割り当てられていなくても、使用可能とマークされているアナリストは、自動割り当てできないその他の制約がない限り、いつでも自動割り当てできます。

グループ内の連絡先ではなく、グループに対してチケットの自動割り当てを行う方法

CA SDM での自動割り当てでは、連絡先レコードで「利用可能」オプションが選択されている連絡先にチケットが割り当てられます。ただし、グループ内の連絡先ではなく、グループにインシデント/案件/変更要求/リクエストを割り当てることもできます。NX_AUTOASG_GROUP_ONLY オプションを使用してグループに対する自動割り当て動作を制御します。このオプションをインストールすることによって、個人の連絡先ではなくグループに対してチケットの自動割り当てを行うことができます。NX_AUTOASG_GROUP_ONLY オプションは Web インターフェースでは利用できないため、コマンドプロンプトからインストールしてください。

次の手順に従ってください:

1. インストールされている CA SDM のバージョンがリリース 12.9 Cumulative 2 パッチ以降であることを確認します。
2. CA SDM サーバでコマンドプロンプトを開きます。
3. 以下のコマンドを実行します。

```
pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst
```

デフォルトでは、pdm_configure の実行後、ユーザが nx.env ファイルに追加する新しいオプションは保存されません。以下のように -t オプションを指定することにより、変更を保存できます。

```
pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst -t
```

コマンドにより、CA SDM 内の以下のファイルが新しいオプションで更新されます。

- Windows -- NX_ROOT/NX.env and NX_ROOT\pdmconf\nx.env.nt.tpl
- UNIX/Linux -- NX_ROOT/pdmconf/NX.env.tpl

4. CA SDM インストールフォルダ内の NX.env ファイルを開き、変数 @NX_AUTOASG_GROUP_ONLY=1 を見つけます（ファイルの末尾にあります）。
5. NX_ROOT/pdmconf 以下にある nx.env.nt.tpl ファイルを開き、@NX_AUTOASG_GROUP_ONLY=1 オプションを見つけます。
6. CA SDM デーモン サーバ サービスを再起動します。
CA SDM により、グループに対してのみチケットが自動割り当てされます。
7. [CA SDM サーバを再起動します](#) (P. 57)。

ロケーションに基づく自動割り当て

サービス領域の規模が大きく、さまざまなカスタマ コミュニティにサービスを提供する数多くのロケーションが含まれている場合、以下のように、ロケーションを自動割り当て設定の要因として使用することができます

- **領域またはカテゴリに割り当てられたロケーション** - ロケーションを領域やカテゴリに割り当てた場合、一致するロケーションが見つかった場合にのみ、その領域やカテゴリのチケットが自動的に割り当てられます。たとえば、以下の場所に適格なアナリストが存在すると、リクエストチケットは自動的に以下のロケーションに割り当てられます。

1. 影響を受けるアセットのロケーション
2. 影響を受ける顧客のロケーション

影響を受けるアセットまたは顧客にロケーションが指定されていない場合は、リクエストがデフォルトのグループと担当者に割り当てられます。これらのデフォルトが定義されていない場合、リクエストは手動割り当てのままです。ロケーションと領域/カテゴリとの関係は、[\[area detail\]](#) ページまたは[\[カテゴリの詳細\]](#) ページで保守できます。

- **グループに割り当てられたロケーション** - ロケーションをグループに関連付けると、そのグループのメンバーのみが、そのロケーションに属しているチケットの自動割り当ての対象となります。グループ詳細ページを使用すると、グループとロケーションの関係を保守できます。

ロケーションと領域、カテゴリ、またはグループとの関係を保守するには、[\[ロケーションの詳細\]](#) ページの[\[自動割り当て\]](#) タブで以下のコントロールを使用します。

- リクエスト領域の更新
- 変更カテゴリの更新
- 案件カテゴリの更新
- グループの更新

例: 自動割り当て設定でのロケーションの使用

以下は、自動割り当て設定でロケーションを使用する方法の例です。

- **指定したロケーションのみのチケットの自動割り当て** - 他のロケーションのチケットは、デフォルトのグループと担当者を受け取るか、手動割り当てのままとなります。たとえば、ある企業の本社に数多くのユーザがいて、支社にはより小さなユーザのグループが存在するとします。本社に配置されているアナリストグループはローカルユーザにサービスを提供し、モバイルアナリストグループは支社を訪問します。本社のアナリストにのみチケットの自動割り当てを設定し、モバイルアナリストには手動でチケットを割り当てることができます。
- **ユーザまたはアセットのロケーション別のチケットの自動割り当て** - 自動割り当ての対象を、影響を受けるユーザまたはアセットのロケーションと一致するロケーションのアナリストグループに制限できます。たとえば、企業に数多くのオフィスがあり、各オフィスからのチケットがそのオフィスに配置されているグループによってのみ処理されているとします。各グループを、適切な領域またはカテゴリ、および適切なロケーションに関連付けることができます。自動割り当てロジックにより、適切なロケーションのグループのみから対象となるアナリストが選択されます。

ワークシフト別の自動割り当て

領域/カテゴリをワークシフトに関連付けることによって、自動割り当てを制限できます。ワークシフトは、チケットが自動割り当て可能である時間枠を決定します。ワークシフトの時間外にオープンされたチケットは、デフォルトのグループおよびアナリストに割り当てられるか、または手動割り当て待ちとなります。

また、ワークシフトでは、グループやアナリストが自動割り当て可能かどうかを制御できます。

- グループに作業スケジュールを割り当てた場合、そのグループ内のアナリストは、その作業スケジュール中にオープンされたチケットへのみ自動割り当てできます。

注: グループのワークシフトは、[グループの詳細] ページの [作業スケジュール] フィールドで指定します。

- 個々のアナリストに作業スケジュールを割り当てた場合、アナリストは、その作業スケジュール中にオープンされたチケットへのみ自動割り当てできます。

注: アナリストのワークシフトは、[グループの詳細] ページの [作業スケジュール] フィールドで指定します。

チケット作成中、自動割り当てロジックは、割り当て可能基準を満たす、グループ内でアクティブなチケットが最も少ないアナリストを識別しようとします。適切なアナリストが識別されない場合、チケットはデフォルトのグループと担当者に割り当てられます。これらのデフォルトが定義されていない場合、チケットは手動割り当てのままです。

変更要求または案件と関連付けられたワークフロー タスクの場合、自動割り当てではより単純な選択方法が使用されます。担当者は、ワークフロー テンプレートに関連付けられたグループから選択されます。ワークフロー タスクの担当者は、グループ以外の任意の連絡先タイプに設定できます。タスクが保留中ステータスに変わると、変更要求または案件の割り当て済みワークフロー タスクが最も少ない連絡先が自動割り当てによって選択されます。不要な結果を回避するため、親の変更要求カテゴリまたは案件カテゴリで自動割り当てが有効になっていない場合、タスクは自動的に割り当てられません。ワークフロー タスクではサービスデスクの組織に入っていない外部のアナリストが対応する場合があります、アナリストの使用可能状態について、使用可能フラグを使用した管理をアナリスト自身に任せることには正確性に問題があります。

注: ワークフロー タスクの自動割り当ては、使用可能フラグを評価せず、**CA Workflow** 処理を使用するように設定されたカテゴリには使用できません。

ワークシフトを領域またはカテゴリに関連付けるには、[area detail] ページまたは [カテゴリの詳細] ページを使用するか、[ワークシフトの詳細] ページで以下のコントロールを使用します。

- リクエスト領域の更新
- 変更カテゴリの更新
- 案件カテゴリの更新

例：自動割り当て設定でのワークシフトの使用

以下は、自動割り当て設定でワークシフトを使用する方法の例です。

- **稼働しているシフトへのチケットの自動割り当て** - サービス デスクが 1 日 24 時間稼働している場合は、チケットが開かれたときに、ネットワーク障害の問題が稼働しているシフトに割り当てられるように自動割り当てを設定することをお勧めします。
- **特定のシフトの間みの自動割り当ての実行** - 一部の領域またはカテゴリの自動割り当てをさらに限定できます。たとえば、サイトのアプリケーション アナリストが昼間勤務時間中にのみ勤務する場合、アプリケーションの問題を昼間勤務時間中にのみ自動割り当てします。

デフォルトのグループと担当者

設定した自動割り当てロジックが、適切なグループまたは担当者を識別できないと、チケットはデフォルトのグループと担当者に割り当てられます。これらのデフォルトは、以下の **Web** インターフェース ページの [グループ] フィールドと [担当者] フィールドで指定できます。

- リクエスト/インシデント/問題領域の詳細
- 変更カテゴリの詳細
- 詳細：案件

自動割り当てで適切なグループまたは担当者を識別できず、デフォルトが指定されていない場合、チケットは手動割り当てのままです。

自動割り当てを有効にする

自動割り当てを設定する際に使用できるオプションおよびコントロール。以下のように、自動割り当て処理を実行するかどうかを制御できます。

- リクエスト、インシデント、および問題をその領域に割り当てるには、[リクエスト/インシデント/問題領域の詳細] ページの [自動割り当てを有効にする] タブを使用します。
- 変更要求、案件、およびワークフロー タスクの場合は、[自動割り当て] タブを選択し、[変更カテゴリの詳細] ページ、[案件カテゴリの詳細] ページ、および [CA ワークフロー テンプレートの詳細] ページで [自動割り当てを有効にする] チェック ボックスをオンにします。

注: [自動割り当てを有効にする] チェック ボックスを表示するには、[編集] をクリックします。

例: リクエスト/インシデント/問題領域の自動割り当ての有効化

この例では、リクエスト/インシデント/問題領域の自動割り当てを有効にする方法を示します。

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [領域] を参照します。
[リクエスト/インシデント/問題領域リスト] ページが表示されます。
2. 自動割り当てを設定する領域をクリックします。
[リクエスト/インシデント/問題領域の詳細] ページが表示されます。
3. [編集] をクリックします。
[リクエスト/インシデント/問題領域の更新] ページが表示されます。

4. [自動割り当て] タブを選択し、以下のように、以下のフィールドに入力します。

自動割り当てモード

自動割り当ての実行方法を指定します。[構成アイテムを基準] オプションを使用して、割り当て可能な CI 属性の値に基づいて自動割り当てを行います。

- **無効** - [領域のデフォルト] オプションがインストールされている場合に、このオプションに基づいて自動割り当てを行います。
- **構成アイテムを基準** - 割り当て可能な CI 属性の値に基づいて自動割り当てを行います。
- **ロケーションを基準** - ロケーション値に基づいて自動割り当てを行います。

割り当て可能な CI 属性

グループ割り当てに使用する構成アイテム属性を指定します。値を直接入力するか、虫眼鏡アイコンをクリックして属性を検索します。

5. [保存] をクリックします。

リクエスト/インシデント/問題領域が有効になり、デフォルト値が使用されます。デフォルト値は、領域に割り当てられたリクエスト、インシデント、または問題のチケットに対して自動的に入力されます。

自動割り当て設定

オプション マネージャの自動割り当て設定 (autoasg_override) オプションを使用すると、チケット作成時に設定されたアナリストまたはグループを自動割り当てにより無効化するかどうかを決定できます。

自動割り当てで制御する前に、CA SDM のその他の機能により担当者やグループが設定されている場合があります。このオプションに以下のいずれかの値を設定して、システムをカスタマイズできます。

0

既存の担当者やグループが認識されます。チケットの作成中に担当者またはグループが設定された場合、自動割り当て処理は実行されません。

1

既存の担当者やグループが無視されます。自動割り当て処理は続行され、担当者またはグループを検索しようとします。

担当者やグループは以下のさまざまな方法で設定できます。

- アナリストによって手動で
- Area_Defaults および Assignee_set オプション
- リクエスト テンプレート
- CA NSM インテグレーション

注: 自動割り当て設定オプションをアンインストールすると、デフォルトモードの 0 で稼働します。

割り当て制御

自動割り当てを設定する際に使用できるオプションおよびコントロール。自動割り当て処理が発生する前に、CA SDM の機能によりチケットの [担当者] フィールドまたは [グループ] フィールド、あるいはその両方が影響を受ける場合があります。割り当て制御を確認してから、自動割り当てを実行することをお勧めします。

手動割り当て

アナリストは、チケットの作成時に担当者やグループを手動で選択できます。

Assignee_set オプション

CA SDM のデフォルトでは、ログインしたユーザがアナリストの場合、そのユーザがリクエストの担当者に自動的に設定されます。 オプションマネージャのオプション **Assignee_set** を使用して、この動作を管理することができます。 このオプションは通常、初期設定でインストールされています。

Iss assignee_set

Iss assignee_set オプションでは、ログインしているユーザがアナリストである場合、そのユーザが自動的に案件の担当者として設定されます。 このオプションは **Assignee_set** に似ていますが、設定されるのはリクエストではなく案件の担当者です。

Area_Defaults

[**Area_Defaults**] オプションでは、リクエストの詳細ページでリクエスト領域を指定するときの動作を指定できます。 このオプションにより、リクエスト領域が変更された場合にいつでも担当者およびグループを設定できます。 このオプションでは、リクエスト領域の担当者およびグループの初期設定を使用して、この処理が実行された後に、自動割り当て処理が実行されます。

このオプションは、初期設定ではインストールされません。

注: **Category_Defaults** オプションには、変更要求用と同様の機能があります。 **Iss_Category_Defaults** オプションには、案件用の同様の機能があります。

必須担当者/グループのオプション

オプションマネージャでは、割り当て解除されたチケットの作成を制御するいくつかのオプションを使用できます。 これらオプションの対象は広範囲にわたり、自動割り当てが有効かどうかにかかわらず、表示されたすべてのチケットタイプの作成が影響を受けます。 表示された条件が満たされない場合、新規チケットまたは更新されたチケットを保存することはできません。

以下のオプションにより、担当者を指定しないチケットの作成が制御されます。

require_change_assignee

アプリケーション：変更要求マネージャ

説明：変更要求チケットの「担当者」フィールドを必須にします。

require_issue_assignee

アプリケーション：案件マネージャ

説明：案件チケットの「担当者」フィールドを必須にします。

require_incident_assignee

アプリケーション：リクエストマネージャ

説明：インシデントチケットの「担当者」フィールドを必須にします。

require_problem_assignee

アプリケーション：リクエストマネージャ

説明：問題チケットの「担当者」フィールドを必須にします。

require_request_assignee

アプリケーション：リクエストマネージャ

説明：リクエストチケットの「担当者」フィールドを必須にします。

以下のオプションにより、グループを指定しないチケットの作成が制御されます。

require_change_group

アプリケーション：変更要求マネージャ

説明：変更要求チケットの「グループ」フィールドを必須にします。

require_issue_group

アプリケーション：案件マネージャ

説明：案件チケットの「グループ」フィールドを必須にします。

require_incident_group

アプリケーション：リクエストマネージャ

説明：インシデントチケットの「グループ」フィールドを必須にします。

require_request_group

アプリケーション：リクエスト マネージャ

説明：リクエスト チケットの[グループ]フィールドを必須にします。

require_problem_group

アプリケーション：リクエスト マネージャ

説明：問題チケットの [グループ] フィールドを必須にします。

テンプレート

テンプレートを使用して、新規のリクエスト、変更要求、または案件の値を設定できます。 [担当者] および [グループ] は、テンプレートの影響を受けるフィールドです。

CA Network and Systems Management インターフェース

CA NSM と CA SDM が統合されていて、CA NSM イベントからリクエストを作成する場合、ライタルール定義内の `user_parms` パラメータが Text API に渡されます。CA SDM のライタ プロセス (tngwriter) は、テキストを Text API に送信する前にそれを変更するための独自の置換パラメータを定義します。キーワード `LOG_AGENT` が入力 of の最後に追加され、リクエストの `log_agent` が設定されます。

注: CA NSM アラート管理システムから CA SDM に渡される追加のフィールドすべてについて、`Text_API.cfg` ファイルを更新する必要があります。このファイルは Web サービス、電子メールおよび AHD.DLL との統合に使用されます。

関連項目：

[キーワード](#) (P. 650)

アクティビティのログ記録

自動割り当てでは、情報はイベントとしてチケットのアクティビティ ログに記録されます。自動割り当ての成功または失敗、および処理中に発生した異常などが記録されます。

追加の属性に対するアクティビティ ログの有効化

アクティビティ ログには、オブジェクトの属性値の変更が表示されます。すべてのチケットタイプ、従来のワークフロー タスク、調査、連絡先、構成アイテムなどのオブジェクトには、アクティビティ ログを使用できます。WSP では、追加の属性に対するアクティビティ ログを有効にすることができます。

注: アクティビティ ログの単純な属性（文字列、整数、日付、期間、および SREL タイプを含む）を表示できます。リスト タイプのアクティビティ ログ（QREL や BREL など）は表示できません。

次の手順に従ってください:

1. WSP を開き、スキーマ デザイナを起動します。
2. 追加の属性の変更や追加を行うテーブルを選択します。
3. 属性ごとに、[サイト定義 UI_INFO] フィールドに +AUDITLOG() を追加します。

重要: AUDITLOG フラグを追加する場合は、アクティビティ ログが重複しないようにするために `val_fieldupdate_site()` 関数を削除することも必要です。

4. スキーマを保存して発行します。
5. WSP を再度開き、適切な詳細フォームに新しい属性を追加します。
6. CA SDM を開き、追加の属性に対するアクティビティの関連付けを定義します。
7. 変更をテストします。

たとえば、オブジェクトの以前に保存されたインスタンスを開き、影響を受ける属性を変更して、適切なアクティビティ ログが表示されることを確認します。

自動割り当てのトレース

複雑な自動割り当ての実装では、自動割り当てにより予期せぬ指定が行われる場合があります。トレースを有効にすると、処理フローを簡単に理解することができます。トレースは通常はオフになっていますが、オンにすると多数のメッセージが `$NX_ROOT¥log` の `stdlog` ファイルに書き込まれます。これらのメッセージでは、自動割り当てによるさまざまな指定を確認することができます。

大量インストールでトレースを実行する場合は注意が必要です。生成された多数のメッセージによりログファイルが大きくなり、最終的には折り返されてしまう可能性があるからです。非常にアクティブなシステムでは、パフォーマンスが低下する場合があります。トレースは、`pdm_logstat` ユーティリティで制御します。このユーティリティで使用するパラメータは、大文字小文字が区別されますので、必ず表記どおりに入力してください。

トレースをオンにするには、各 CA SDM サーバで以下のコマンドを実行します。

```
pdm_logstat - f auto.pm milestone
```

トレースをオフにするには、各 CA SDM サーバで以下のコマンドを実行します。

```
pdm_logstat - f auto.pm
```

ストアドクエリ

アナリストの使用可能状況を監視するために、2つのストアドクエリが用意されています。CA SDM マネージャは、これらのストアドクエリを自分のスコアボードに追加することができます。

- **使用可能なアナリスト** - 自動割り当て可能とマークされたアナリスト
- **使用不可能なアナリスト** - 自動割り当て不可能とマークされたアナリスト

自動割り当てでのチケット割り当て方法

自動割り当てでは、以下のようにチケットが割り当てられます。

1. 新規チケットの最初の保存操作のときに、自動割り当てが呼び出されます。

領域またはカテゴリで自動割り当てが有効になっていない場合、処理は停止します。

2. 自動割り当てにより、`Autoasg_override` がインストールされているかどうかを確認されます。

これがインストールされておらず、チケットに担当者またはグループが割り当てられている場合、処理は停止します。

3. ワークシフトがチケットに関連付けられている場合、ワークシフトにチケットが含まれるかどうかを判断するためにオープン日が評価されます。

ワークシフトにチケットが含まれない場合、処理は停止し、自動割り当てはグループおよび担当者の初期設定を割り当てようとします。

4. 自動割り当てでは、チケットに関連付けられているグループがあるかどうか判断されます。

グループが関連付けられていない場合、処理は停止し、自動割り当てはグループおよび担当者の初期設定を割り当てようとします。

5. オープン日がワークシフトの時間枠の範囲外である場合、ワークシフトが関連付けられたそのグループは自動割り当てによりすべて排除されます。ワークシフトが関連付けられていないグループは、フィルタリングされません。

6. チケットに関連付けられたロケーションでは、以下のような結果になります。

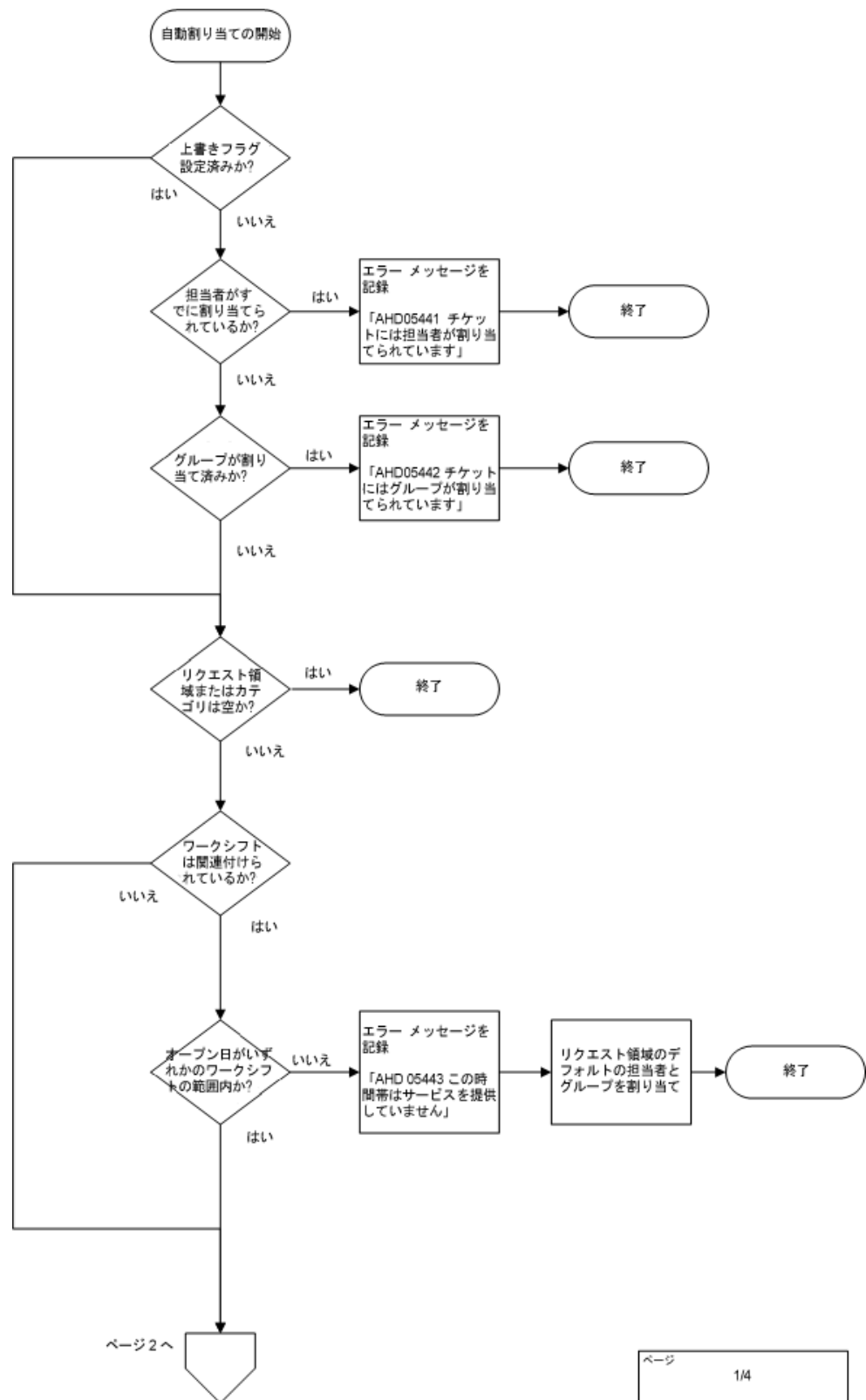
- このチケットがリクエストで、構成アイテムがある場合

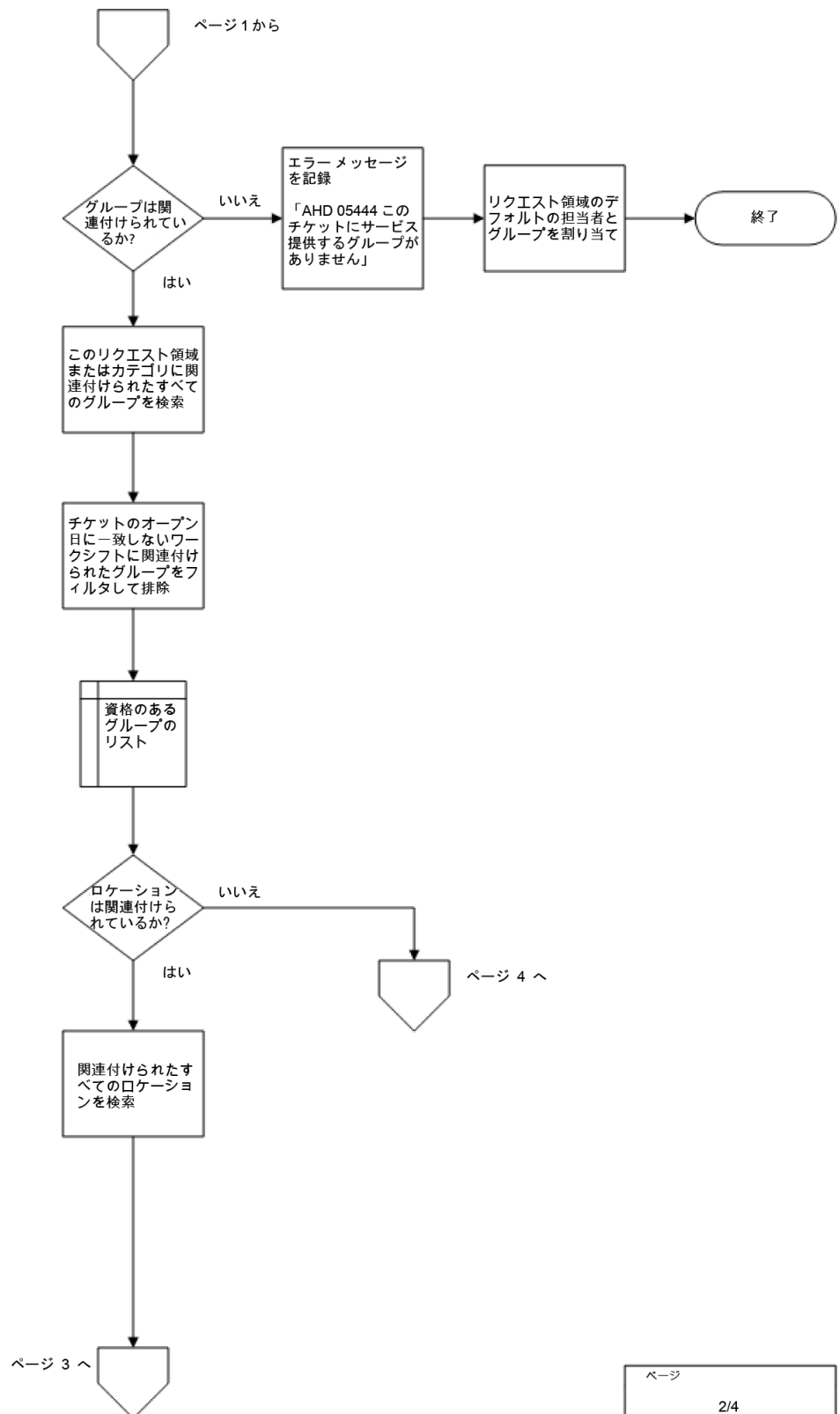
構成アイテムのロケーションが、リクエスト領域に関連付けられたロケーションと一致するかどうか確認されます。一致しない場合、処理は停止し、自動割り当てはグループおよび担当者の初期設定を割り当てようとします。一致する場合、顧客のロケーションが、領域またはカテゴリに関連付けられたロケーションと一致するかどうか確認されます。一致しない場合、処理は停止し、自動割り当てはグループおよび担当者の初期設定を割り当てようとします。

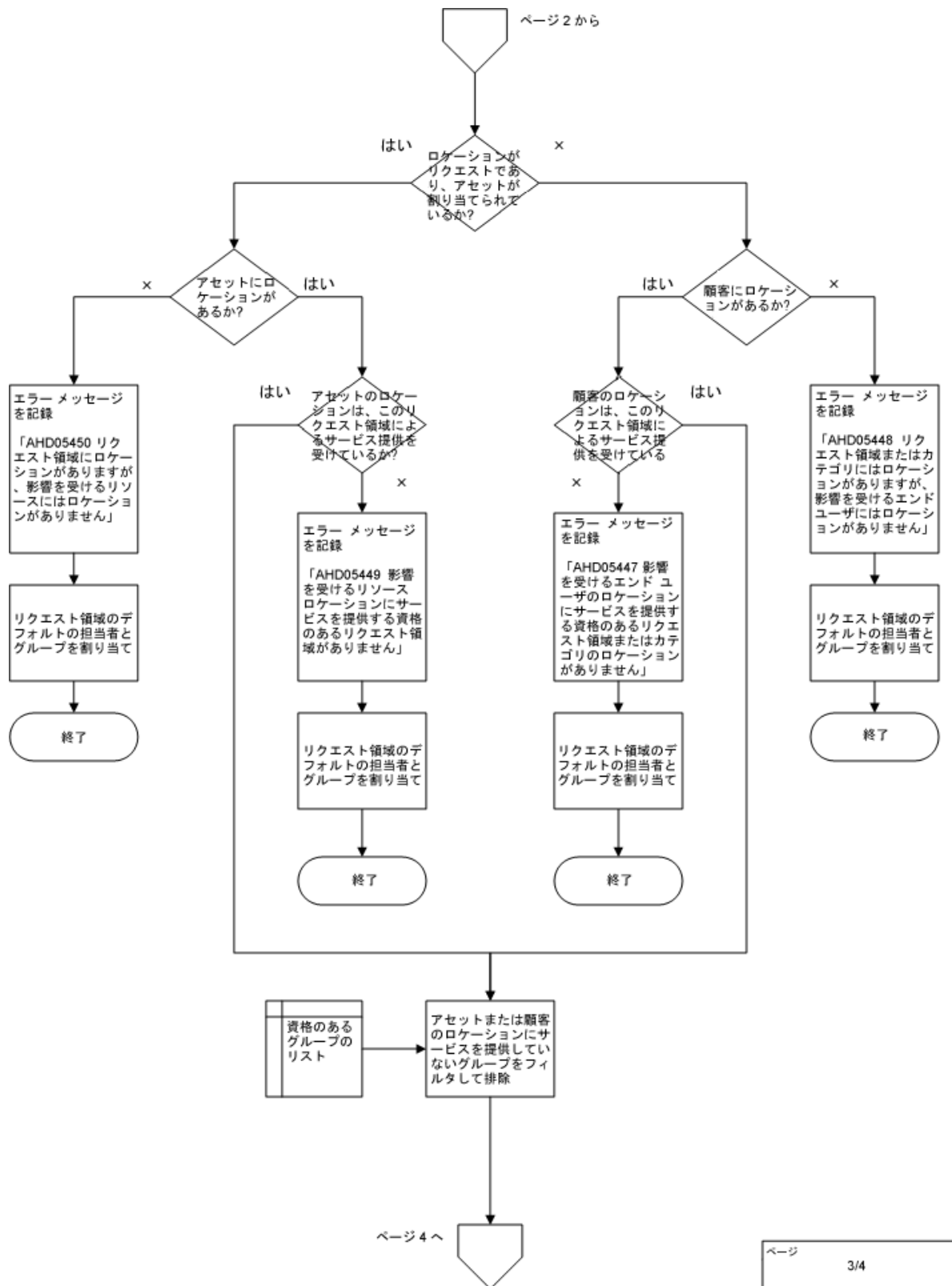
- ロケーションがリクエスト領域またはカテゴリに関連付けられている場合

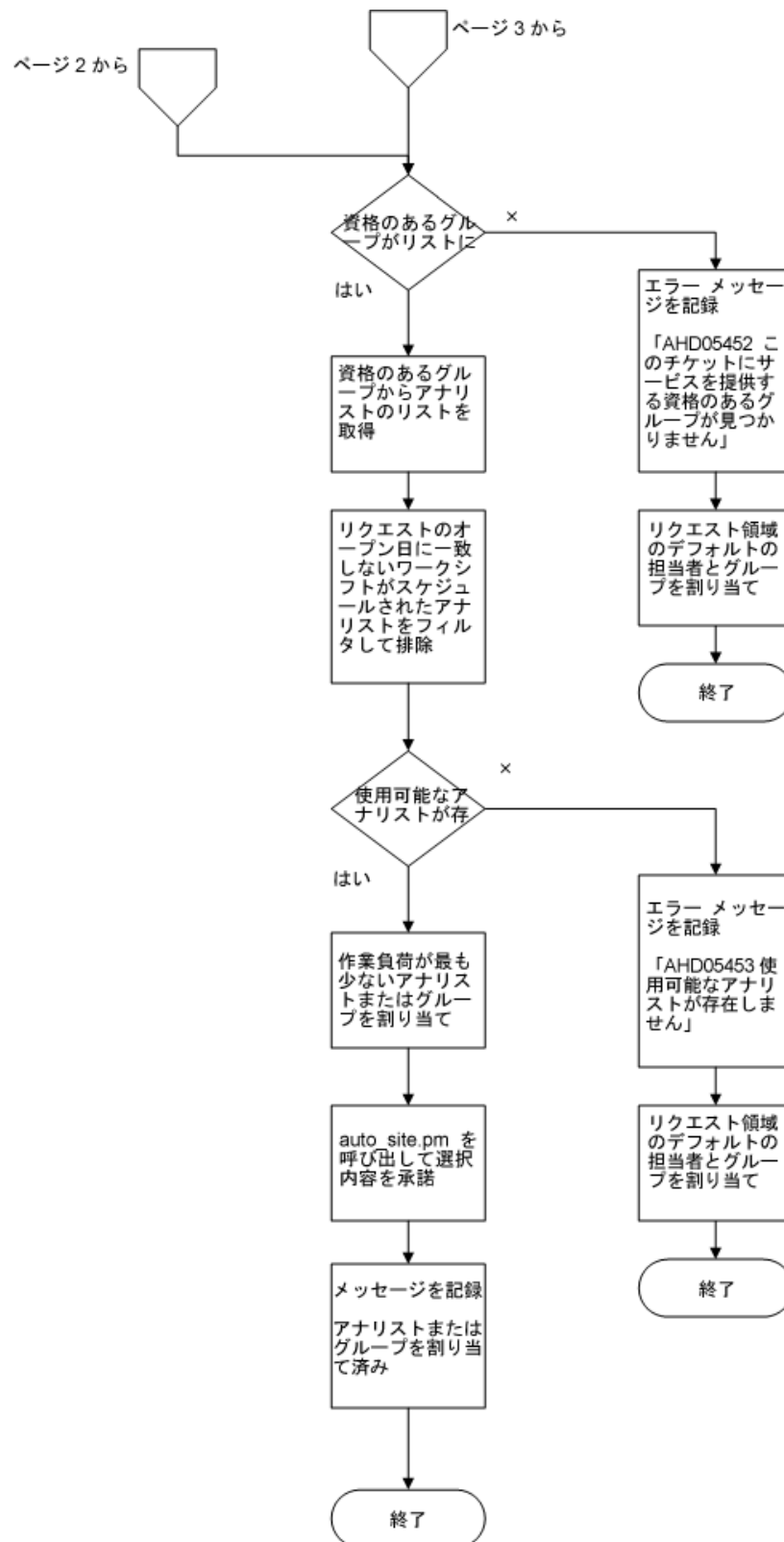
ロケーションがリクエスト領域および構成アイテムに関連付けられている場合（リクエストの自動割り当て処理中）、または顧客にロケーションが割り当てられていない場合、自動割り当て処理は停止します。

7. 適格なグループに関連付けられているロケーションが構成アイテムのロケーション（リクエストのみ）または顧客のロケーションと一致しない場合、自動割り当てによりそのグループは排除されます。グループがすべて排除された場合、処理は停止し、自動割り当てはグループおよび担当者の初期設定を割り当てようとします。
8. 自動割り当てにより、適格な残りのグループからそれぞれアナリストリストが作成されます。
9. 使用不可能なアナリストは排除されます。
10. 残ったアナリストの作業スケジュールがチェックされます。オープン日がアナリストの作業スケジュールの範囲外である場合、作業スケジュールを持つそれらのアナリストは排除されます。
11. アナリストがすべて排除された場合、処理は停止し、自動割り当てはグループおよび担当者の初期設定を割り当てようとします。
12. 残りのアナリストはすべて、割り当てられたアクティブなチケットの数に従ってランク付けされます。
13. アクティブなチケットの数が最も少ないアナリスト（および関連付けられたグループ）が、チケットに割り当てられます。ランクが同じアナリストが存在する場合は、グループ内の最初のアナリストが選択されます。







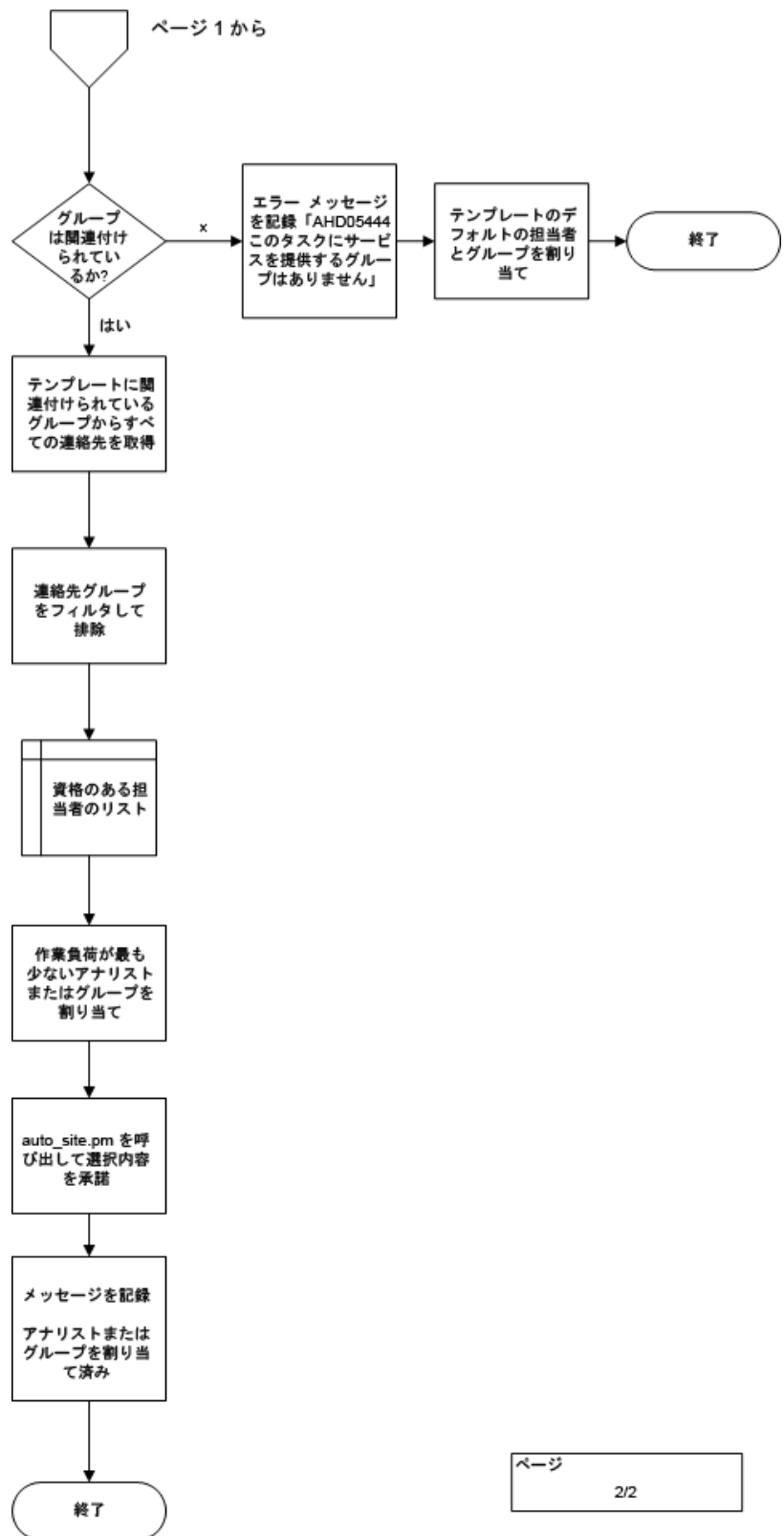


自動割り当てでのワークフロー タスクの割り当て方法

自動割り当てでワークフロー タスクを割り当てるために使用される処理ロジックは以下のとおりです。

1. 自動割り当ては、ワークフロー タスクのステータスが保留中に変わると呼び出されます。ワークフロー タスクを作成するときに使用したワークフロー テンプレートが自動割り当てに対して有効になっていない場合、処理は停止します。親の変更要求カテゴリまたは案件カテゴリが自動割り当てに対して有効になっていない場合、処理は停止します。
2. 自動割り当てにより、`Autoasg_override` がインストールされているかどうかチェックされます。これがインストールされておらず、タスクに担当者またはグループが割り当てられている場合、処理は停止します。
3. ワークフロー タスクを作成するときに使用したワークフロー テンプレートに連絡先が関連付けられているかどうかチェックされます。連絡先が関連付けられていない場合、処理は停止します。
4. ワークフロー タスクを作成するときに使用したワークフロー テンプレートにグループが現在関連付けられている場合、自動割り当てにより、そのグループのメンバーであるすべての連絡先のリストが作成されます。このリスト内で連絡先がグループの場合、その連絡先は排除されます。
5. 残りの連絡先はすべて、割り当てられたアクティブな変更要求タスクまたは案件タスクの数に従ってランク付けされます。
6. アクティブなタスクの数が最も少ない連絡先および関連付けられたグループが、タスクに割り当てられます。





構成アイテムベースの自動割り当て

構成アイテムベースの自動割り当てを使用すると、特定のシナリオに適用されるグループに固有の割り当てを作成できます。特定の領域、その割り当てを管理するチケットに関連付けられた構成アイテムの属性値に対して開かれたリクエスト/インシデント/問題チケットに、構成アイテムベースの自動割り当てを指定できます。

〔リクエスト/インシデント/問題〕で使用するアルゴリズムを1つのみ選択できるため、構成アイテムベースおよび場所ベースの自動割り当ては、排他的オプションです。構成アイテムベースおよび場所ベースの自動割り当てモードは、両方ともその作成時にチケットを割り当てますが、リクエスト/インシデント/問題が変更されるたびにチケットを再割り当てすることが、構成アイテムベースの自動割り当てのみが実行できる機能です。

例: リクエスト/インシデント/問題領域によるグループへのチケットの割り当て

`network_contact_uuid`（ネットワーク運用）属性を割り当て可能なCI属性値として、構成アイテムベースの自動割り当てを実行するためにネットワーク領域（リクエスト/インシデント/問題用）を構成する場合、ネットワーク領域に開かれたチケットは、チケットに関連付けられたCIの〔ネットワーク運用〕フィールドで指定されたグループにすべて自動的に割り当てられます。チケットと関連付けられているCIがない場合、CIの〔ネットワーク運用〕フィールド値が空の場合、またはグループを指定していない場合は、割り当ては発生しません。このような場合、システムは領域デフォルトのオプションマネージャに従って動作し、カテゴリの〔グループ〕と〔担当者〕フィールドを使用して、チケットを割り当てます。

構成アイテムに基づいた自動割り当てのしくみ

リクエスト/インシデント/問題チケットは、構成アイテムに基づいた自動割り当てが発生するように以下を指定する必要があります。

- 構成アイテムと領域。
- 領域では〔自動割り当て〕オプションが〔構成アイテムを基準〕に設定されている必要があります。

アナリストがこの領域にチケットを作成して割り当てる場合、または既存チケットで領域を変更する場合、CA SDM は領域の [割り当て可能な CI 属性] フィールドを調べます。CA SDM は、割り当て可能な CI 属性の値を属性の名前として使用し、チケットに関連付けられている構成アイテム上で同一の名前の属性を検索試行します。構成アイテムの属性にグループが含まれている場合、チケットはそのグループに割り当てられます。

以下の図では、構成アイテムに基づいた自動割り当てのプロセスをより詳細に説明します。

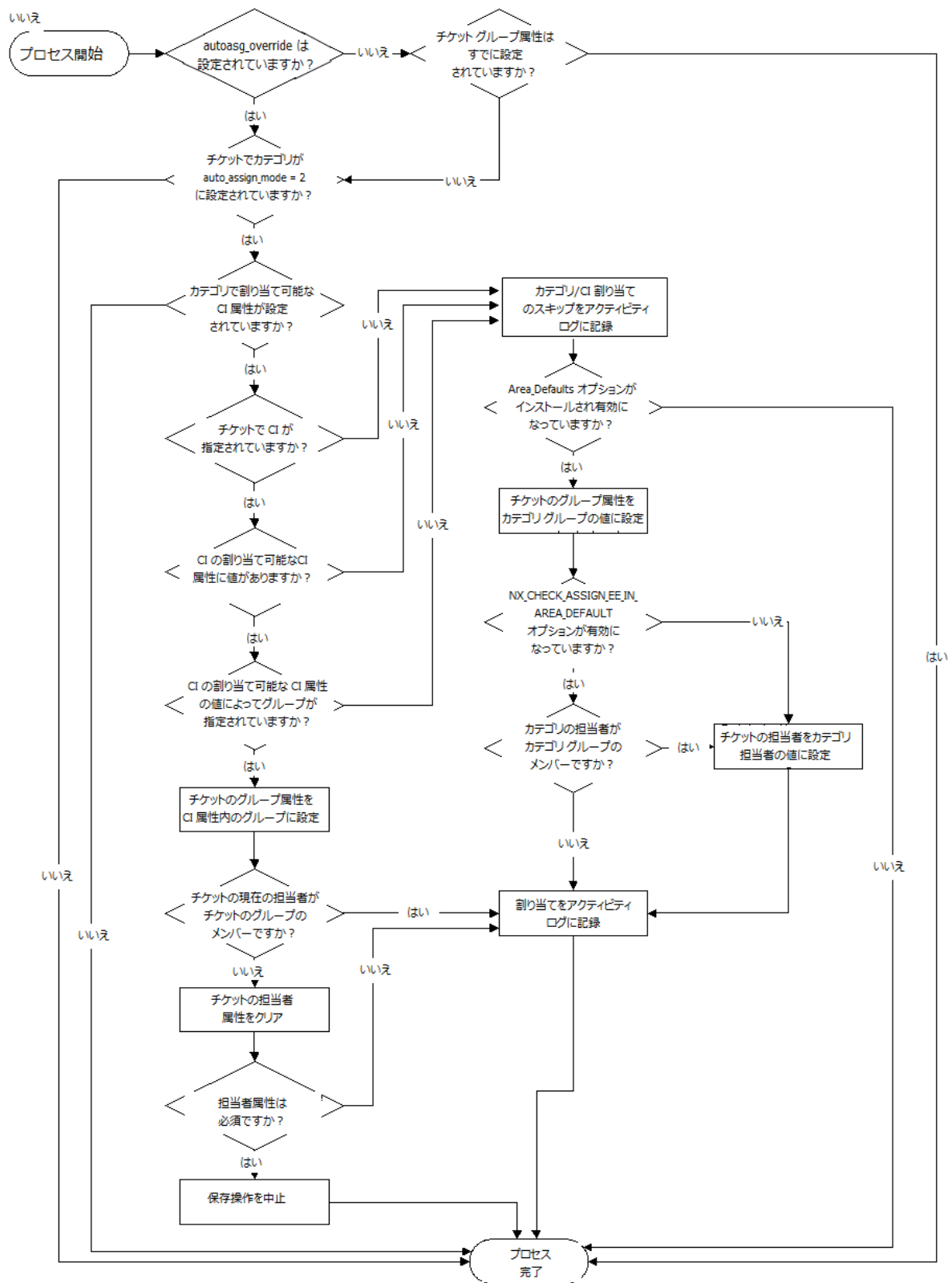
1. CA SDM は以下について確認します。
 - a. `autoasg_override` オプションが設定されていますか。
 - b. チケットは、その自動割り当ての `auto_assign_mode=2` で領域を指定していますか。
 - c. カテゴリは割り当て可能な CI 属性を指定していますか。
 - d. チケットは構成アイテムを指定していますか。
 - e. 構成アイテムには割り当て可能な CI 属性値がありますか。
 - f. 値は CI 属性内のグループを指定していますか。
 - g. チケットの担当者はチケット グループのメンバーですか。

2. 前の手順の質問の回答がすべて「はい」の場合、CA SDM は CI のグループ属性にチケットのグループ属性を設定し、アクティビティ ログの割り当てをログ記録します。

注: 図は、[領域] オプションが有効かどうかを決定するために構成アイテムに基づいた自動割り当てが

NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS 変数を使用する方法を示します。NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS は \$NX_ROOT¥ ディレクトリにある NX.env ファイルの変数です。

3. CA SDM は、チケットをグループに割り当てます。



関連項目:

[自動割り当て設定](#) (P. 576)

構成アイテムに基づいた自動割り当ての有効化

構成アイテムに基づいた自動割り当てでは、特定のシナリオに適用されるグループに特有の割り当てを作成することができます。特定の領域に開かれたリクエスト/インシデント/問題チケットについては、チケットに関連付けられた構成アイテムの属性の値がその割り当てを制御するように指定することができます。チケットのリクエスト/インシデント/問題領域または構成アイテムが変更されるたびに、構成アイテムに基づいた自動割り当てはチケットを再割り当てします。

注: オプションマネージャの `autoasg_override` オプションによって、自動割り当ての実行条件が制御されます。このオプションを **1** に設定した場合、**CA SDM** はすべての既存の担当者およびグループ設定を無視し、すべてのケースでチケットを自動的に割り当てます。チケットがまだ割り当てられていない場合のみ **CA SDM** で自動的に割り当てるようにするには、オプション値を **0** に設定します。

構成アイテムに基づいた自動割り当てを有効にする方法

1. [管理] タブで、[Service Desk] - [リクエスト/インシデント/問題] - [領域] を参照します。
[リクエスト/インシデント/問題領域リスト] が表示されます。
2. 編集する領域をクリックします。
[領域の詳細] ページが表示されます。
3. [編集] をクリックします。
[Update Area] ページが表示されます。
4. [自動割り当て] タブを選択し、以下のようにフィールドを指定します。

自動割り当てモード

自動割り当ての発生方法を指定します。[構成アイテムを基準] オプションを使用して自動割り当てが割り当て可能な **CI** 属性値に基づくようにします。

割り当て可能な CI 属性

グループ割り当てに使用する構成アイテム属性を指定します。値を直接入力するか、虫眼鏡アイコンをクリックして属性を検索します。

[保存] をクリックします。

自動割り当てが有効になります。CA SDM は、[割り当て可能な CI 属性] フィールドで指定した属性を使用して、構成アイテムに基づいた自動割り当てを実行します。

第 13 章：データベースの管理

このセクションには、以下のトピックが含まれています。

[データベース管理ユーティリティ](#) (P. 601)

[データベースの選択と設定](#) (P. 601)

[データベース ロード](#) (P. 602)

[データベースのバックアップ](#) (P. 605)

[データベースのリストア](#) (P. 606)

[データベース テーブル置換](#) (P. 606)

[データの修飾参照](#) (P. 609)

[ブラウザ キャッシュを使用したパフォーマンスの向上](#) (P. 626)

[環境設定ファイルの変更](#) (P. 629)

データベース管理ユーティリティ

CA SDM のシャットダウン中は、データベースを管理するためのユーティリティを実行できます。データベース管理ユーティリティを実行して、CA SDM の初期設定リポジトリ以外のデータベースを使用している場合は、データベース環境変数を設定する必要があります。

注: 環境変数の設定の詳細については、使用しているデータベースのマニュアルを参照してください。

データベースの選択と設定

データベースを選択し、CA SDM で使用するように設定できます。

データベースを選択および設定する方法

1. [データベース タイプ] ドロップダウン リストからデータベースを選択して、[次へ] をクリックします。

選択したデータベースを設定するためのページが表示されます。

2. データベース設定ページにデータベース情報を入力したら、[次へ]をクリックします。

データベースの設定が完了しました。

注: このページの [ヘルプ] ボタンを使用して、選択したデータベースのフィールドの環境設定情報を確認できます。

データベース設定ページには次のボタンが表示されます。

ヘルプ

現在のページのヘルプを起動します。

キャンセル

その時点までに行った環境設定内容をキャンセルします。

[戻る]

現在のページでその時点までに行った変更を保存することなく、前のページに戻ります。

次へ

現在のページで行ったすべての変更を保存した後、次のページに進みます。

データベース ロード

データベース ロード ユーティリティ (`pdm_userload`) は、CA SDM データベース レコードを追加、更新、および削除します。`pdm_userload` ユーティリティ用にフォーマット済みの ASCII 入力ファイルを作成し、ロードするテーブルと追加するオプションのフィールドを選択します。

重要: `pdm_userload` ユーティリティは、CA SDM データベースにアクセスします。アプリケーション ソフトウェアのプロセスと直接やり取りしません。`pdm_userload` を使用してデータベースに在庫項目を追加した場合は、アプリケーションを停止して再起動し、ヘルパ/選択リストを更新します。

`pdm_userload` ユーティリティは、アプリケーションがアクティブな状態でも実行できますが、システムのパフォーマンスは低下します。最適な結果を得るには、`pdm_userload` を実行する前に、バックグラウンドサーバが実行されていて、クライアントインターフェースを使用しているユーザが存在しないことを確認してください。

注:-相互参照されているフィールドのあるレコードを追加するには、`pdm_deref` ユーティリティを使用してください。

関連項目:

[データの修飾参照](#) (P. 609)

入力ファイルを作成および使用する方法

入力ファイルおよび `pdm_userload` ユーティリティを使用して、データベース テーブルに格納できます。

スクリプト ファイルのフォーマットは以下のとおりです。

- フィールド値は二重引用符で囲み ("value")、個々の値をカンマおよびスペースで区切ります ("value1", "value2")。
- 二重引用符をテキスト文字列に埋め込むには、二重引用符の前にバックslash (¥) を入力します。日付/時間フィールドを現在の日時に設定するには、入力値に `@NOW@` を使用します。
- 各レコードは、中かっこで囲んでスペースで区切る必要があります。以下に例を示します。

```
( { record field values } )
```

- 適切に区切られている場合、個々のフィールドが 1 行に収まっている限り、入力レコードは入力ファイル内の複数の行にまたがることができます。コメントなどの複数行にわたるフィールドの場合は、値に改行文字 (¥n) を含めて、データベース フィールドが表示されたときに強制的に改行することができます。
- 明示的な改行文字は、特別なフォーマットでのみ必要となります。通常の連続したテキストは、自動的に適切に改行されて表示されます。以下に例を示します。

```
"Record status is ¥"COMPLETE¥"
```

pdm_userload ユーティリティの入力ファイルを作成するには、以下の手順に従います。

1. ロードするテーブルと、そのテーブルで入力するフィールドを決定します。

ロードする各レコードの **Name** または **Symbol** キー フィールドを入力する必要があります。

2. ロードするテーブル用の適切な *filename.dat* ファイルのコピーを作成します。
3. 新たに作成した *filename.dat* ファイルのコピーを、以下のように編集します。

- a. ロードする各レコードのエントリを追加します。
- b. TABLE 行以降の、入力しないフィールドを削除します（以下の例を参照）。

```
TABLE table_name  
fieldname1 fieldname4 . . . fieldnameN
```

4. ファイルを保存し、エディタを終了します。
5. 以下の例のように、**pdm_userload** ユーティリティを実行し、ファイルを指定します。この例では、入力ファイル名は **myData.dat** です。

```
pdm_userload -f myData.dat
```

データベース テーブルに入力されます。

関連項目：

[pdm_userload—データベース レコードの追加、更新、および削除 \(P. 1340\)](#)

制約の削除と復元

名前が **ca_** から始まる **mdb** テーブル (**ca_contact_** など) には参照制約があり、**pdm_load**、**pdm_userload**、および **pdm_restore** ツールを使用してデータを大量にロードする際に影響が出ることがあります。これらのテーブルを大量にロードする必要がある場合は、大量のデータをロードする前に参照制約を削除しなければならないことがあります。

各 DBMS タイプには、制約を削除および復元するための 2 つの SQL スクリプトがあります。ca_*テーブルに影響を与えるデータの大量ロードを開始する前に、制約を削除するスクリプトを実行します。データのロードが完了したら、制約を復元するスクリプトを実行します。

SQL Server の場合、スクリプトは

installation-directory/samples/views/SQLServer ディレクトリにあります。制約を削除するには、以下のコマンドを実行します。

```
osql -E -e < SQLDropConstraints.sql
```

制約を復元するには、以下のコマンドを実行します。

```
osql -E -e < SQLAddConstraints.sql
```

Oracle の場合、スクリプトは *installation-directory¥samples¥views¥Oracle* ディレクトリにあります。

制約を削除するには、以下のコマンドを実行します。

```
sqlplus mdbadmin/ <password> < OracleDropConstraints.sql
```

制約を復元するには、以下のコマンドを実行します。

```
sqlplus mdbadmin/ <password> < OracleAddConstraints.sql
```

データベースのバックアップ

データベース バックアップ ユーティリティ `pdm_backup` を使用して、1 つのデータベース テーブル、複数のデータベース テーブル、または Unicenter Service Desk データベース全体の内容をバックアップすることができます。バックアップ ユーティリティは ASCII ファイルに出力します。このファイルは `pdm_restore` ユーティリティで使用できます。

処理の一環として、`pdm_backup` はまずデーモン (UNIX) またはサービス (Windows) を停止します。

関連項目:

[pdm_backup—ASCII ファイルへのデータベースの書き込み \(P. 1293\)](#)

データベースのリストア

データベース復元ユーティリティ `pdm_restore` は、`pdm_backup` から CA SDM データベースに出力ファイルをロードします。`pdm_restore` ユーティリティはまず、デーモン（UNIX）またはサービス（Windows）をシャットダウンします。次に、既存のデータベース レコードをすべて復元、消去、および置換します。`pdm_backup` で作成したフォーマット済みの ASCII ファイルを、`pdm_restore` ユーティリティの入力として使用します。

`pdm_restore` ユーティリティと `pdm_userload` ユーティリティは、データベースが突然破損した場合に CA SDM アプリケーションにアクセスするのにも使用できます。データベースが損傷してアプリケーションにアクセスできない状態になり、ほかの方法で対処できない場合は、環境設定を再度実行してデータベースを再初期化し、データベースを再構築して参照データとシステム テーブルを入力します。

この手順では、前にインストールしたときと同じ方法でデータベースが初期化されます。これで、CA SDM にアクセスできるようになります。`pdm_restore` ユーティリティを使用して、データベースの最新のバックアップ コピーを復元できます。

関連項目：

[pdm_restore—データベースの復元 \(P. 1330\)](#)

データベース テーブル置換

`pdm_replace` ユーティリティを使用して、すばやく簡単に CA SDM データベース テーブルのすべての内容を新しい情報に置換することができます。このユーティリティは、ルックアップ-テーブルを大量に変更する必要がある場合に便利です。

注: `pdm_replace` の入力ファイルのフォーマットは、`pdm_userload` と同じです。`pdm_extract` を使用して `pdm_replace` 用の入力ファイルを作成できますが、`pdm_backup` の出力を `pdm_replace` の入力として使用することはできません。

関連項目:

[pdm_replace—データベース テーブルの置換 \(P. 1327\)](#)
[入力ファイルを作成および使用する方法 \(P. 603\)](#)

データ抽出

`pdm_extract` ユーティリティは、CA SDM データベースからデータを抽出し、さまざまな形式で出力を生成します。このデータをさらに処理することも、スプレッドシートや別のデータベースなどのほかのソフトウェアアプリケーションに入力することもできます。

`pdm_extract` ユーティリティを使用すると、以下のことが可能になります。

- CA SDM データベース全体のダンプを出力します。
- 1 つ以上のデータベースのダンプを出力します。
- データベースから特定の情報を抽出して、以下のいずれかの形式で出力を生成します。
 - `pdm_userload` と互換性のある出力
 - カンマ区切り値 (CSV) 出力
 - 略式のレポート スタイル出力

関連項目:

[pdm_extract—データベースからのデータの抽出 \(P. 1304\)](#)

UNIX でのデータ抽出機能の使用

CA SDM のデータ抽出機能を UNIX で使用する前に、以下の手順に従う必要があります。

1. `$NX_ROOT` 環境変数に、インストール時に定義した CA SDM インストールディレクトリの完全パス名を指定します。
2. `PATH` 環境変数に `$NX_ROOT/bin` を追加します。
3. `umask` を `000` に設定します。

抽出するデータの選択

抽出するデータを選択するために、データ抽出機能は以下の規則に従って重要な SQL サブセットを使用します。

- 以下の SQL 関数は、サブセットで特別にサポートされています。
 - IS NULL、IS NOT NULL、LIKE
 - SELECT ステートメントと WHERE 節
- 以下の SQL 機能は、サブセットでサポートされていません。
 - Joins
 - 埋め込みタブと改行文字
 - SELECT、FROM、および WHERE 以外の節
 - SELECT ステートメントでのアスタリスク (*)
 - ネストされた SELECT ステートメント
 - 集約関数
- SQL のすべての予約語は、大文字で指定する必要があります。
- WHERE 節のトークンはすべてスペースで囲む必要があります。
- 日付/時間の仕様は、以下のいずれかの形式である必要があります。
 - グリニッジ標準時 (GMT) の 1970 年 1 月 1 日午前 0:00:00 からの経過秒数
`start_date<または>174182431500`
 - SQL DATE 形式
`start_date<または>DATE '2001-11-28'`
 - SQL TIMESTAMP 形式
`start_date<または>TIMESTAMP '2001-07-04 15:45:00'`

注: TIMESTAMP 形式は GMT を使用します。次のように適切な時間数を加算または減算してタイムゾーンを調整できます。例: 2001-03-23 14:00:00+02:00 または 2001-06-06 04:45 : 00-09:00。

データの修飾参照

`pdm_deref` ユーティリティは、さまざまなソースからのデータを CA SDM データベースへのロードに適したフォーマットに変換する修飾参照ツールで、相互参照されているフィールドの内部 ID を抽出します。また、ダウンタイムと SLA ダウンタイム値の計算にも使用できます。

`pdm_deref` ユーティリティは、データを以下のフォーマットのいずれかに変換します。

- `pdm_userload` と互換性のある出力（CA SDM データベースにロードするのに適しています）
- カンマ区切り値（CSV）出力
- 略式のレポートスタイル出力

関連項目：

[pdm_deref—ASCII データの修飾参照](#) (P. 1297)

`pdm_deref` の使用方法の例

以下の例は、CA SDM チケット トラッキング システム内で `pdm_deref` ユーティリティを使用する方法を示しています。

スプレッドシートに実装した既存のチケット トラッキング システムに Trouble Description、Technician First and Last Name、および Entry Date という列があり、それぞれ CA SDM Change_Request テーブルの description、assignee、および open_date フィールドに対応しています。Trouble Description フィールドには description フィールドと同じタイプのデータが含まれていますが、assignee フィールドは数値フィールドで、スプレッドシートの Technician フィールドは「last name, first name」の形式になっています。

pdm_derefを使用する方法

1. **Contact** テーブルに技術者の名前をロードします。
2. 既存の情報を設定した **pdm_deref** 入力ファイルを準備します。
3. 新しい連絡先名を担当者値にマップするための仕様ファイルを作成します。
4. **Change_Request** テーブルを更新するために使用する **pdm_userload** 入力ファイルを準備します。

以下に、この手順の詳細について説明します。

1. **Location** テーブル用の **pdm_userload** 入力ファイル **location.dat** を準備します。

```
TABLE ca.location
location_name address_2 address_2
{"Boulder NCC - NQ", "716 Main
    Street","Boulder, CO 84302"}
{"Colorado Springs NCC", "2765 Spring Street",
    "Colorado Springs, CO 84303"}
{"Denver NCC", "3765 Stoneridge Way", "Denver,
    CO 80254"}
```

2. データをロードします。

```
pdm_load -f location.dat
```

3. 元の情報を使用して入力ファイル **contact.dat** を準備します。

```
TABLE ca.contact
last_name first_name middle_name location pri_phone_number
{"Harrison", "Frank," "Harold", "NCC - HQ", "303-555-2333"}
{"Hertzog", "William", "I.", "Colorado Springs NCC", "303-966-1987"}
{"Lyman", "Jeanie", "L.", "Denver NCC", "303-966-5301"}
```

4. 修飾参照ツールの仕様ファイル **contact.spec** を準備します。

```
Deref
{
input = c_location
output = location_uuid
rule = "SELECT id FROM ca.location WHERE location_name=?"
}
```

重要: **SELECT** キーワードの前にスペースを入れないでください。Deref は、新しい連絡先の姓名を使用して、**Change_Request** テーブルをロードするための適切な数値 **ID** フィールドを取得します。また、疑問符 (?) で表されているフックは、指定した入力フィールドに対応します。フックの数と順序は入力フィールドと同じである必要があります。

5. pdm_deref を実行します。

```
pdm_deref -s contact.spec < contact.dat > contact.out
```

出力ファイル **contact.out** は以下のように表示されます。

```
TABLE ca.contact
last_name first_name middle_name location.uuid pri_phone_number
{"Harrison", "Frank", "Harold", "69499D5A2424884887E62EC9823F5E47",
"303-555-2333"}
{"Hertzog", "William", "I.", "86873FA40BA4234A8CF7A418D7C8B2DB",
"303-966-1987"}
{"Lyman", "Jeanie", "L.", "58AA42789957734E8BEE146D07F7AD49", "303-966-5301"}
```

6. contact.out ファイルを CA SDM データベースにロードします。

```
pdm_load -i -f contact.out
```

注: -i オプションを使用するには、pdm_load コマンドを使用する必要があります。

7. (UNIX のみ、省略可) 以下のように Convert_Ticket スクリプトを作成します。

```
#!/bin/sh
pdm_load -i $1
cat $2 | pdm_deref -s $3 | pdm_load -i
```

このスクリプトを以下のように実行します。

```
Convert Ticket location.dat contact.dat contact.spec
```

この例では、プロセスの速度を上げるために、-i フラグが付いた pdm_load が使用されています。こうした変更を定期的に行っている場合は、-i フラグを削除して、重複するレコードがないか pdm_load でチェックします。

以下に、修飾参照ツール仕様ファイルのその他の例を示します。

Deref

```
{
    input = first_name, last_name, middle_name
    output = assignee
    rule = " SELECT id from ca.contact ¥
           WHERE first_name=? ¥
           AND last_name=? ¥
           AND middle_name=? "
}
```

このルールにより、`first_name`、`last_name`、および `middle_name` という 3 つのフィールドが、適切な連絡先 UUID に変換されます。3 つの入力フィールドの 1 つでも欠けていると、ルールは適用されません。一致するものがない場合は、エラーメッセージが生成されて処理が続行されます。一致が複数ある場合は、最初の値が採用され、エラーメッセージが生成されて処理が続行されます。

dbadmin モードの使用

`dbadmin` モードは、オブジェクト レイヤを開始することなく、CA SDM システムのデータ操作レイヤを開始するユーティリティです。データベース全体をロックして、データの整合性に影響を及ぼすことなくローレベルのデータ保守を行うことができます。

たとえば、`pdm_extract`、`pdm_load`、`pdm_deref`、および `pdm_replace` を使用してシステム上のデータをバッチ更新する場合、`dbadmin` モードでは管理者は実質的にシステム全体のデータベースをロックすることができます。バックアップ (`pdm_backup`) ユーティリティおよび復元 (`pdm_restore`) ユーティリティは、システムを自動的に `dbadmin` モードに切り替えることにより、一貫したバックアップおよび復元を保証します。

`dbadmin` モードは、カスタマイズを行う際にデータ変更が完了するまでオブジェクト レイヤを開始しないようにする場合にも便利です。たとえば、既存システムで「必須」属性を `majic` で作成する場合に、必須属性が Null 値になっているオブジェクトがあると、それを更新しなければならないアニメータは混乱状態に陥ります。このような場合、システムを `dbadmin` モードに切り替え、`pdm_load` でオブジェクトを更新し、その後、システムを通常どおり起動させると解決できます。

システムを `dbadmin` モードに切り替えるには、以下の手順に従います。

1. Windows サービス マネージャを使用するか、コマンドラインから `pdm_halt` を実行して、CA SDM を停止します。

注: システムを停止する前に、警告アナウンスメントをユーザに送信し、ログインしているユーザがいらないかどうかをチェックすることをお勧めします。

2. コマンドラインで、以下のように入力します。このコマンドでは大文字小文字が区別されます。

```
pdm_d_mgr - s DBADMIN
```

注: 返されるメッセージはありませんが、コマンドプロンプトに戻る前に一時停止します。一時停止しない場合は、正しく入力されたかどうかスペルをチェックしてください。

3. `pdm_status` を実行して、システムが `dbadmin` モードで稼働していることを確認します。

注: システムが `dbadmin` モードで稼働している場合は、以下のステータスが返されます。これは、システムで安全に操作できるようになったことを示しています。

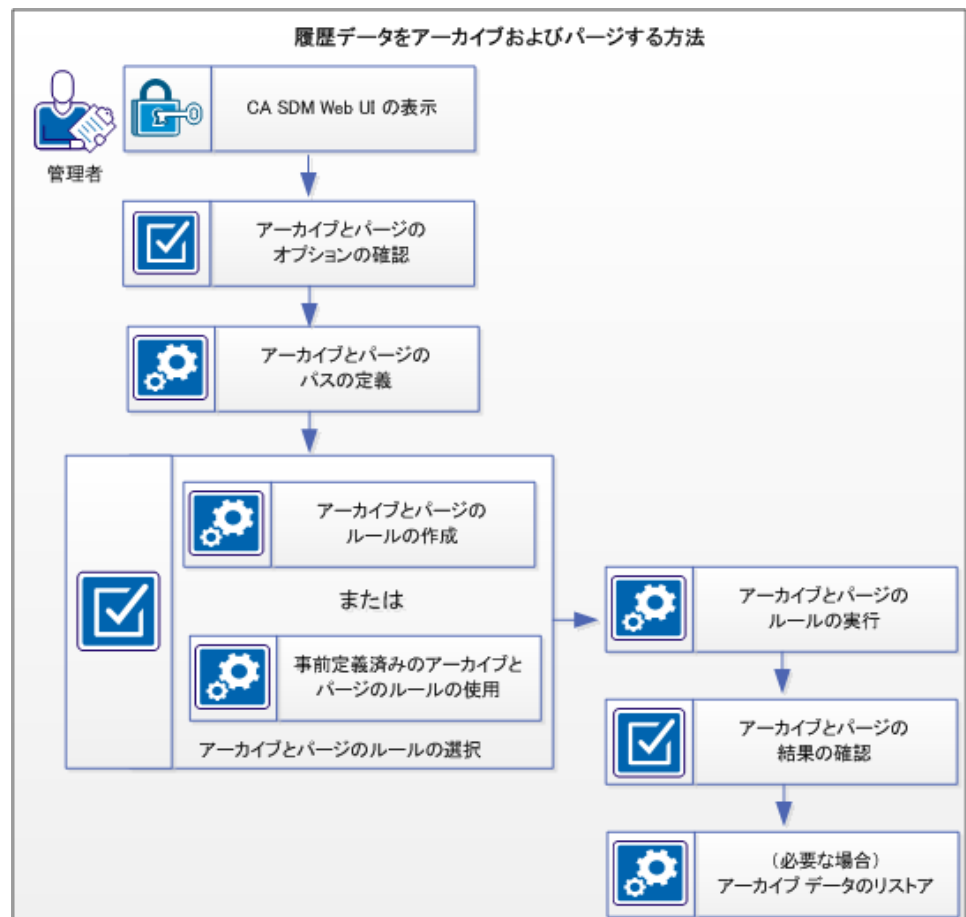
```
C:\>pdm_status  
Daemons が稼働していません。
```

4. すべての作業が完了したら、`pdm_halt` を実行して `dbadmin` モードを停止します。
5. 通常の手順に従って、システムを再起動します。

履歴データをアーカイブおよびパージする方法

データベースを管理可能なサイズに保ち、最適なパフォーマンスを得るには、システムから定期的に履歴レコードを削除します。ルールを作成するか、または事前定義済みのルールをアクティブにして、履歴レコードをアーカイブし、データベースからパージします。

以下の図は、履歴データをアーカイブおよびパージする方法を示しています。



次の手順に従ってください:

1. [CA SDM Web UI を開きます](#) (P. 222)。
2. [アーカイブとページのオプションを確認します](#) (P. 615)。
3. [アーカイブとページのパスを定義します](#) (P. 616)。
4. [アーカイブとページのルールを選択します](#) (P. 619)。
 - [アーカイブとページのルールを作成します](#) (P. 619)。
 - [事前定義済みのアーカイブとページのルールを使用します](#) (P. 623)。
5. アーカイブとページのルールを実行します。
6. [アーカイブとページの結果を確認します](#) (P. 624)。
7. (必要な場合) [アーカイブデータをリストアします](#) (P. 625)。

CA SDM Web UI の表示

CA SDM の設定に応じて、以下のサーバから Web UI にログインします。

- 標準: プライマリまたはセカンダリ サーバ
- 高可用性: アプリケーションサーバまたはバックグラウンドサーバ

アーカイブとページのオプションを確認します。

アーカイブとページのルールを設定する前に、組織の要件に応じて、インストールまたはアンインストールが必要なアーカイブおよびページオプションを確認します。たとえば、`default_schedule` オプションは、アーカイブとページのルールで使用するデフォルトのスケジュール (ワークシフト エントリ) を指定します。このオプション値を無効なワークシフト エントリ名または空の文字列に設定すると、ルールは指定したスケジュールで実行されません。オプション値フィールドに、`NX.env` ファイル内の `NX_DEFAULT_SCHEDULE` 変数を設定します。

[管理] タブで、[オプション マネージャ] - [アーカイブとページ] を選択します。必要なオプションをインストールまたはアンインストールします。

アーカイブとパージのパスの定義

アーカイブ データを格納する場所を定義できます。このパスは、リモート サーバのルート ディレクトリまたは UNC パスにすることができます。CA SDM の設定に応じて、UNC パスにアクセスするために、Windows で以下のサーバを実行する必要があります。

- 標準：プライマリ サーバ
- 高可用性：バックグラウンド サーバ

次の手順に従ってください：

1. CA SDM の設定に応じて、以下の CA SDM サーバから Web UI にログインします。
 - 標準：プライマリまたはセカンダリ サーバ
 - 高可用性：アプリケーション サーバまたはバックグラウンド サーバ
2. 添付ファイルをアーカイブおよびパージするには、以下の手順に従います。
 - a. [管理] タブで、[添付ファイル ライブラリ] - [リポジトリ] を選択します。
[リポジトリ] ページが開きます。
 - b. リポジトリ（[Service Desk] など）を右クリックし、[編集] をクリックします。
リポジトリの詳細ページが開きます。
 - c. 以下のフィールドを編集します。

アーカイブ タイプ

リポジトリの内容に対して実行するアーカイブおよびパージアクションを指定します。有効な値は以下のとおりです。

なし：アーカイブとパージのプロセスは実行されません。

アーカイブとパージ：履歴レコードは、[アーカイブ] フィールドで指定したファイルに書き込まれ、データベースからパージされます。

パージのみ：履歴レコードはデータベースからパージされますが、アーカイブ ファイルには書き込まれません。

アーカイブ パス

アーカイブ プロセスで、リポジトリ内のファイルが移動されるディレクトリ パスまたは UNC パスを指定します。

UNC 認証情報

UNC パスにアクセスするための認証情報を指定します。[UNC 認証情報] をクリックして、[認証情報の検索] ページを開きます。

- 指定した UNC パスにアクセスするための認証情報をすでに作成している場合は、そのフィールドを使用して検索し、認証情報を選択します。
- 認証情報を作成する場合は、[新規作成] をクリックします。認証情報の作成の詳細については、「[UNC 認証情報の作成](#) (P. 544)」を参照してください。

d. [保存] をクリックします。

3. 添付ファイル以外のデータをアーカイブおよびパージする場合は、以下の手順に従います。

- a. [管理] タブで、[アーカイブとパージ] - [アーカイブとパージの設定] を選択します。
- b. [アーカイブ パージルールのパス] に、アーカイブおよびパージされるデータを格納するパスを入力します。
- c. アーカイブ データの格納に UNC パスを使用する場合は、[UNC 認証情報] をクリックします。

[認証情報の検索] ページが開きます。

- 指定した UNC パスにアクセスするための認証情報をすでに作成している場合は、そのフィールドを使用して検索し、UNC 認証情報を選択します。
- 認証情報を作成する場合は、[新規作成] をクリックします。認証情報の作成の詳細については、「[UNC 認証情報の作成](#) (P. 544)」を参照してください。

d. [保存] をクリックします。

アーカイブとパージのパスが定義されます。

UNC 認証情報の作成

UNC パスを使用して、ユーザが CA SDM サーバから共有リソースにアクセス可能にするための UNC 認証情報を作成します。

重要: CA SDM サーバがドメインにあり、共有場所が **WORKGROUP** にある場合、UNC コンポーネントは動作しません。また、CA SDM サーバ用の管理者パスワードおよび共有場所が異なる場合、それは動作しません。

次の手順に従ってください:

1. [一般設定] ページの [UNC 認証情報] をクリックするか、または [管理] タブで、[セキュリティと役割の管理] - [UNC 認証情報] を選択します。

[認証情報リスト] ページが開きます。

2. [新規作成] をクリックします。

[認証情報の新規作成] ページが開きます。

3. 必要に応じて以下のフィールドに値を入力します。

シンボル

検索時に認証情報を容易に識別するために一意の識別子を指定します。

ユーザ ID

UNC パスにアクセスするためのユーザ名を指定します。ユーザは、Service Desk サーバへのアクセス権を持つローカルまたはドメインの Windows ユーザにすることができます。

パスワード

UNC パスにアクセスするためのパスワードを指定します。

アクティブ

UNC 認証情報がアクティブであるか、非アクティブであるかを指定します。非アクティブな認証情報は使用できません。

4. [保存] をクリックします。

UNC 認証情報が作成されます。

アーカイブとパージのルールを選択

適切なアーカイブとパージのルールを選択する必要があります。たとえば、以下について考えてみます。

- [アーカイブとパージのルールを作成します](#) (P. 619)。たとえば、ナレッジ マネジメント フォーラム用のアーカイブとパージのルールを作成します。
- [事前定義済みのアーカイブとパージのルールを使用します](#) (P. 623)。たとえば、KPI データのアーカイブとパージに事前定義済みのルールを使用します。

アーカイブとパージのルールの作成

アーカイブまたはパージを実行するには、ルールを作成します。ルールでは、アーカイブする内容とタイミングを定義します。

例: アーカイブとパージのルールを作成して、削除されたフォーラムをデータベースから除去します。

次の手順に従ってください:

1. [管理] タブで、[アーカイブとパージ] - [アーカイブとパージのルール] を選択します。
[アーカイブとパージのルール リスト] ページが開きます。
2. [新規作成] をクリックします。
[アーカイブとパージのルールの新規作成] ページが開きます。
3. 必要に応じて、[アーカイブとパージのルール フィールド](#) (P. 621) に入力します。
 - ナレッジ ドキュメントとして [構成 オブジェクト名] を選択します。
 - [追加クエリ] として KS_TYPE=20 を追加します。
4. [保存] をクリックします。
[アーカイブとパージのルール リスト] ページに新しいルールが表示されます。

例: arcpur_cfg.xml ファイルおよび itil_arcpur_cfg.xml ファイル内にオプションの設定ルールを作成して、KPI_Ticket_Data ノードをアーカイブおよびページできます。

次の手順に従ってください:

1. CA SDM の設定に応じて、以下のサーバにログインします。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンドサーバ
2. 以下のファイルは、\$NX_ROOT/site/cfg/ ディレクトリにあります。
 - arcpur_cfg.xml
 - itil_arcpur_cfg.xml
3. ファイルを編集して、KPI_Ticket_Data ノードで end_time (last_mod_dt) を定義します。これは、アーカイブおよびページのためにレコードを選択する基準を指定します。
4. KPI_Ticket_Data テーブルのレコードをチケットテーブルのレコード (cr、chg、iss など) にリンクします。これにより、KPI_Ticket_Data テーブルのレコードに関連付けられているすべてのチケットがアーカイブおよびページされます。
5. KPI_Ticket_Data ノードにはチケット ノードとの SREL 関係がなく、2つのフィールド obj_name および obj_id によってチケットとリンクされます。obj_name 値には、cr、chg、または iss を使用でき、obj_id 値は ticket id となります。各チケット オブジェクトの main_obj を定義します。

以下に、チケット オブジェクト cr の main_object 定義の例を示します。

```
<!-- KPI Ticket Data -->
<main_obj>
<name>KPI チケット データ</name>
<internal_name>KPI チケット データ</internal_name>
<factory>ktd</factory>
<default_query>obj_name='cr'</default_query>
<date_field>end_time</date_field>
<ref_by value="obj_id">cr.id</ref_by>
</main_obj>
```


注: この設定ルールは **cr** のレコードに対してのみ選択できます。
ref_by タグは、**cr** の ID の値に対する KPI チケットデータ内の **obj_id** の値と一致することがあります。一致している場合、KPI チケットデータのレコードは、**cr** レコードによって参照されているため、この KPI チケットデータ レコードはアーカイブおよびページされません。

- すべてのチケット オブジェクトの設定ルールを追加した後、**CA SDM** の設定に応じて、以下のいずれかを実行します。

- [標準設定で CA SDM サーバを再起動します \(P. 57\)](#)。
- [高可用性設定で CA SDM サーバを再起動します \(P. 57\)](#)。

設定ルールが、[アーカイブとページのルールの詳細] フォームで選択可能な設定オブジェクト名になります。

新しいアーカイブとページのルールのフィールド

以下のフィールドを使用して、ルール定義の定義または編集を行うことができます。

ルール名

ルールの一意の識別子を指定します。

ステータス

このルールがアクティブであるかどうかを示します。非アクティブなルールは、反復プロセスに対してスケジュールされている場合でも 1 回しか実行されません。

スケジュール

ルールを有効にする必要があるワークシフトを指定します。

再帰間隔

このルールを実行する頻度を指定します。

アーカイブ ファイル名

履歴レコードを格納するファイルの名前を指定します。アーカイブとページのパスを定義したときに指定したファイル名を入力します。詳細については、「[アーカイブとページのパスの定義 \(P. 616\)](#)」を参照してください。

操作タイプ

ルールで実行する必要がある以下の操作のタイプのいずれかを指定します。

アーカイブとパージ

履歴レコードをファイルにアーカイブし、アーカイブされたレコードをデータベースからパージします。

パージのみ

履歴レコードをデータベースからパージしますが、アーカイブファイルには書き込みません。

アーカイブのみ(テスト実行)

履歴レコードをデータベースからパージせずにアーカイブ ファイルに書き込みます。このオプションは、新規に作成したアーカイブ/パージのルールまたは編集したルールをテストするために使用します。

設定。オブジェクト名

このルールでアーカイブとパージが行えるデータベース オブジェクトの名前を指定します。[オブジェクト名] フィールドには、[構成オブジェクト名] フィールドでの選択内容に従って自動的に値が入力されます。

非アクティブ日数

レコードを非アクティブにするまでの日数を指定します。この日数を過ぎると、レコードをアーカイブしてデータベースからパージできます。

追加クエリ

既存の非アクティブ レコードのうち、特定のレコードをアーカイブおよびパージします。同じオブジェクトの有効期限切れレコードのサブセットをアーカイブおよびパージするときに使用する別のルールを作成する場合は、このフィールドを使用します。ストアドクエリの場合と同じ構文を使用します。

以下のクエリでは、優先度が 1 の割り当て済みの非アクティブ リクエスト レコードのみをアーカイブおよびパージします。

```
priority = 1 AND (assignee IS NOT NULL OR group IS NOT NULL) and active = 0
```

以下のクエリ形式により、レコードが期間に基づいてアーカイブおよびパージされます。

```
close_date < EndAtTime(¥'LAST_YEAR¥')
```

事前定義済みのアーカイブとパージのルールの使用

CA SDM で事前定義済みのルールを使用して、履歴データをアーカイブおよびパージすることができます。これらの事前定義済みのルールは、デフォルトでは非アクティブに設定されます。ルールを使用するには、アクティブにします。

例: 事前定義済みのルールを使用して、KPI データをアーカイブおよびパージします。

次の手順に従ってください:

1. [管理] タブで、[アーカイブとパージ] - [アーカイブとパージのルール] を選択します。
2. KPI データに対する以下の事前定義済みのルールのいずれかを検索します。
 - KPI チケット データ
 - KPI データ (システム)
 - KPI データ (ストアドクエリ)
 - KPI データ (SQL)

3. 検索結果からルールを選択します。
4. [編集] をクリックして、[アーカイブとページのルールのフィールド](#) (P. 621) を変更します。

重要: [ステータス] フィールドで [アクティブ] オプションを選択していることを確認します。

5. [保存] をクリックします。

事前定義済みのルールが使用可能になります。

アーカイブとページの結果の確認

スケジュールしたアーカイブとページのルールの結果を確認します。以下のアクションのいずれかまたは両方を実行します。

- [アーカイブとページの履歴の表示](#) (P. 624)
- アーカイブとページのログ ファイルの表示

アーカイブとページの履歴の表示

各アーカイブとページのルールの履歴を表示できます。たとえば、ルール別にページされたオブジェクトを表示します。

次の手順に従ってください:

1. [管理] タブで、[アーカイブとページ] - [アーカイブとページの履歴] を選択します。

[アーカイブとページの履歴リスト] ページが開きます。

2. [フィルタの表示] をクリックし、フィルタ条件を指定します。たとえば、指定した時間フレームのエントリのみを表示するため、最も早い開始日を入力します。

注: [その他の検索指数] フィールドを表示するには、[Spigot] アイコンをクリックします。このフィールドは、SQL や Majic の知識を持つエキスパートユーザのみを対象としています。このフィールドでは、標準の検索フィルタ フィールドでは使用できない検索指数を指定できます。その他の検索指数を指定するには、このフィールドに SQL WHERE 節を入力します。

一致するルールのリストが表示されます。

3. ルール設定を確認するルール名をクリックします。

[アーカイブとページのルールの詳細] ページが開きます。

アーカイブとパージのログ ファイルの表示

`$NX_ROOT/log/` ディレクトリの `arcpur.log` ファイルを確認して、スケジュールされたアーカイブとパージのルールを実行する間に発生したエラーを検索できます。

注: `arcpur.log` ファイルのサイズ制限は、`$NX_ROOT/NX.env` で以下のように定義されています。

```
# The size limit for the Archive and Purge log file and data file.  
@NX_ARCPUR_FILESIZE=2000000000
```

アーカイブとパージにより、各ログ ファイルのファイル制限に達した後、`arcpur.log.0`、`arcpur.log.1` から `arcpur.log.9` が作成されます。

アーカイブ データのリストア

再度データベースで必要になった場合に、アーカイブ データをリストアできます。

次の手順に従ってください:

1. `dbadmin` モードでデーモンを起動します。 `dbadmin` モードではアクセスが制限されるため、`pdm_load` を安全に実行して、アーカイブ データをリストアできます。 `CA SDM` の設定に応じて、以下のサーバで `pdm_d_mgr -s DBADMIN` コマンドを実行します。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンド サーバ
2. ルート ディレクトリ、またはアーカイブ データを格納した `UNC` ロケーションに移動します。
3. アーカイブ データ ファイル (`.dat` ファイル) を検索します。
4. `CA SDM` の設定に応じて、以下のサーバにファイルをコピーします。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンド サーバ
5. データ ファイルに対して `pdm_load` を実行します。 以下に例を示します。

```
pdm_load -a -f 2004611T1726_Call_Request.dat
```
6. `pdm_load` コマンドに関する問題がある場合は、以下の手順に従います。
 - a. エラーがないか、コマンドラインおよび `$NX_ROOT/log/arcpur.log` を確認します。

- b. [CA SDM サーバを再起動します \(P. 57\)](#)。
- 7. 次のサイクルでレコードがアーカイブおよびページされないようにするには、以下の手順に従います。
 - a. レコードを更新して、再度アーカイブされるようにします。
 - b. 関連付けられたアーカイブとページのルールを非アクティブにします。

ブラウザ キャッシュを使用したパフォーマンスの向上

CA SDM Web インターフェースは、JavaScript、スタイルシート、およびイメージファイルを数多く使用します。これらのファイルは、サイズが非常に大きく、パフォーマンスに影響を及ぼす場合があります。

Web インターフェースのパフォーマンスを向上させるには、ユーザのブラウザにこれらのファイルがキャッシュされるように HTTP サーバを設定して、ファイルが 1 日に 1 回だけロードされるようにします。

Web インターフェースのパフォーマンスが向上します。

注: デフォルトのインストールでは、Apache および IIS のキャッシュは自動的に設定されますが、手動で設定することもできます。

Microsoft Internet Information Server の設定

CA SDM ディレクトリからロードしたファイルが、ロードしてから 1 日で期限切れになることをブラウザに通知するように Microsoft Internet Information Server (IIS) を設定できます。この場合、ブラウザは、ファイルを何回使用するかにかわらず、1 日 1 回だけこれらのファイルに関するクエリをサーバに送信します。

Microsoft Internet Information Server を設定する方法

1. インターネット サービス マネージャ アプリケーションを起動します (Windows 2000 および XP の場合は、[プログラム] - [管理ツール] - [インターネット サービス マネージャ] を選択します)。
2. CA SDM のファイル フォルダへ移動します。通常、このフォルダの名前は CAisd です。
 - a. CA SDMWeb インターフェースを実行するサーバの横にあるプラス記号をクリックします。
 - b. [既定の Web サイト] の横にあるプラス記号をクリックします。
 - c. CAisd まで、下へスクロールします。
3. CAisd フォルダを右クリックし、[プロパティ] を選択します。
[プロパティ] ページが表示されます。
4. [HTTP ヘッダー] タブをクリックします。
5. [コンテンツに有効期限を設定する] チェック ボックスをオンにします。
6. [有効期間] オプションを選択し、テキスト フィールドに「1」と入力し、ドロップダウン リストから [日間] を選択します。
7. [OK] をクリックします。
プロパティが保存され、ただちに有効になります。

Apache の設定

CA SDM ディレクトリからロードしたファイルが、ロードしてから 1 日で期限切れになることをブラウザに通知するように Apache を設定できます。この設定の場合、ブラウザは、ファイルを何回使用するかにかかわらず、1 日 1 回だけこれらのファイルに関するクエリをサーバに送信します。

Apache を設定するには、環境設定ファイルのテキストを更新します。初期設定のインストールでは、ステートメントが含まれるように、`apache.conf` ディレクトリ内のアクティブな環境設定ファイル (通常は、`httpd.conf`) を以下のように変更します。

```
Include installation-directory/bopcfg/www/CAisd_apache.conf
```

Installation-directory は、完全パスで置き換えてください。Windows では、パスは通常、`c:\Program Files\CA\CA SDM` となります。UNIX では、*installation-directory* は `$NX_ROOT` の値で置き換えてください。

Include ステートメントによって参照される `CAisd_apache.conf` ファイルには以下のテキストが含まれます。ここでも、*installation-directory* は Include ステートメントの場合と同じ完全パスで置き換えます。

```
<IfModule mod_alias.c>
    Alias /CAisd installation-directory/bopcfg/www/wwwroot/
<IfModule mod_expires.c>
    <Directory installation-directory/bopcfg/www/wwwroot>
        ExpiresActive On
        ExpiresDefault "access plus 1 day"
    </Directory>
</IfModule>
</IfModule>
```

CA SDM ファイルのブラウザ キャッシュが有効になるように Apache を手動で設定するには、`CAisd_apache.conf` のステートメントのようなステートメントを Apache 環境設定ファイルにインクルードします。それらをファイルに直接追加することも、初期設定のインストールのように個別のファイルを参照する Include ステートメントを追加することもできます。

Apache 環境設定ファイルへの変更は、Apache をリサイクルした直後に有効になります。

キャッシュのクリア

HTTP サーバ自体がロードする JavaScript、イメージ、スタイルシート、HTML またはヘルプ ファイルを変更した場合、それらのブラウザ キャッシュをクリアするようにユーザに指示する必要があります。

注: HTML ファイルへの変更を有効にするには、Web エンジンのリサイクルするか、または `pdm_webcache` ユーティリティを使用する必要があります。開発環境では、環境設定ファイルのプロパティ `SuppressHtmlCache` を指定するとこの作業を省略できます。

Internet Explorer のブラウザ キャッシュをクリアする方法

1. [ツール] - [インターネット オプション] の順に選択します。
[インターネット オプション] ダイアログ ボックスが表示されます。

2. [ファイルの削除] をクリックします。
確認ウィンドウが表示されます。

3. [OK] をクリックします。
ブラウザ キャッシュがクリアされます。

Firefox のブラウザ キャッシュをクリアする方法

1. [ツール] - [最近の履歴を消去] を選択します。
2. [今すぐ消去] ボタンをクリックします。
ブラウザ キャッシュがクリアされます。

環境設定ファイルの変更

CA SDM Web インターフェースをインストールすると、必要に応じて変更できる、サンプルの Web エンジン構成ファイル (*web.cfg*) がインストールされます。*web.cfg* ファイル自体に役立つコメントが含まれており、ファイルを表示して内容を確認できます。適切なディレクトリから *web.cfg* ファイルを開くことができます。

- (Windows) %NX_ROOT%\bopcfg\www¥
- (UNIX) \$NX_ROOT/bopcfg/www/

注: charset などの追加の環境設定変数の一部は、オプションマネージャでも使用できます。これらには、Web インターフェースの [管理] タブを使用してアクセスできます。詳細については、オンラインヘルプを参照してください。

AllowInactiveSrelEntry

レコードが参照テーブル内の非アクティブなレコードを参照しているときにレコードを保存できるかどうかを指定します。

- このプロパティを指定しなかった場合、またはゼロに設定した場合は、非アクティブな参照テーブルのエントリ（リクエストステータスや変更カテゴリ）はドロップダウンリストに含まれなくなり、ルックアップフィールドや階層検索フィールドに指定できなくなります。
- このプロパティを **1** に設定すると、参照テーブルエントリで非アクティブフラグが無視されます。

このフラグの設定にかかわらず、すでに非アクティブな参照テーブルへの参照が含まれているレコードは、参照を変更せずに保存できます。フラグは、新しいフィールド値にだけ影響します。

AnnouncementLength

カスタマ用インターフェースおよびアナリスト用インターフェースの両方の初期画面に表示される、アナウンスメントの最大数を指定します。**CA SDM** には、最新のアナウンスメントが最初に表示され、このパラメータで指定した数のアナウンスメントが続いて表示されます。アナリスト用インターフェースのユーザは、[検索] メニューで [アナウンスメント] を選択して、その他のアナウンスメントを表示できます。

デフォルト値は **10** で、最新のアナウンスメントから **10** 件表示します。

AnonymousPrio

ゲストユーザが作成したチケット用の有効な優先度を指定します。これらのユーザは、各自のチケットに **AnonymousPrio** リストの優先度を **1** つだけ指定できます。優先度リスト内のエントリは、スペースで区切ります。各エントリは、**1~5** の数字または単語「なし」である必要があります。最初に、ゲストユーザが作成したチケット用の初期設定の優先度を指定します。これで、リストで繰り返し表示できます。

AnonymousPrio の有効な値は、配布された優先度のシンボル名に対応します。**Java** クライアントを使用してこれらのシンボル名をカスタマイズできますが、初期設定名で優先度を参照し続ける必要がある **AnonymousPrio** の仕様には影響を与えません。**1** が最も高い優先度に対応します。

デフォルト値は「なし」で、この場合はゲストユーザが作成したすべてのリクエストに優先度が設定されません。

自動入力

ユーザがルックアップフィールドにデータを入力し、**Tab** キーを押してフィールドから出たときに、**Web** インターフェースがルックアップフィールドを自動入力することを指定します。自動入力オプションが選択されている場合にユーザがデータを入力すると、ブラウザはサーバに更新が正しいかどうかを確認します。これにより、フィールドにフルネームが入力されるか（ユーザが名前の一部を指定した場合）、ポップアップ検索ウィンドウが表示されます（ユーザが正しくない情報またはあいまいな情報を入力した場合）。

このプロパティはオプションです。**Autofill** はデフォルトで有効になっているため、このプロパティ ID を指定しないか「**Yes**」に設定した場合、**Tab** キーを押してルックアップフィールドから出ると、自動的にデータベースが検索されます。このプロパティを「**No**」に設定した場合、自動入力は行われず、レコードが保存されるまでルックアップフィールドは確認されません。

CAisd

CA SDM Web サーバが必要とするファイルが含まれている **HTTP** サーバ内の別名または仮想ディレクトリへのパス（先頭のスラッシュを含む）を指定します。このプロパティの値は通常、**UNIX** と **Windows** のどちらでも **/CAisd** です。**Apache** サーバの場合は、環境設定ファイルの **Alias** ステートメントで定義します。**IIS** の場合は、ディレクトリの [プロパティ] ウィンドウの [エイリアス] フィールドと一致する必要があります。

CGI

Web インターフェースに付属している **CGI** 実行可能プログラムの名前（.exe サフィックスなし）を指定します。

デフォルト： pdmweb

注： このプログラムの名前を変更した場合、このプロパティを更新する必要があります。

CgiReport

Web インターフェースに付属している **Web** レポートの **CGI** 実行可能プログラムの名前（.exe サフィックスなし）を指定します。

デフォルト： pdm_cgireport

注： このプログラムの名前を変更した場合、このプロパティを更新する必要があります。

ContactAutoDesc

カスタマ用インターフェースおよび従業員用インターフェースで作成された新規案件およびリクエストの説明に、連絡先の名前を挿入するかどうかを指定します。このプロパティを指定しないか、**0**を指定した場合、連絡先の名前は新規案件およびリクエストの説明に自動的に追加されません。このプロパティに**1**を指定した場合は、連絡先の名前が、カスタマ用インターフェースおよび従業員用インターフェースで作成された案件およびリクエストの説明に自動的に挿入されます。このプロパティは、アナリスト用インターフェースには影響しません。

ContactAutoDescWithIP

カスタマ用インターフェースおよび従業員用インターフェースで作成された新規案件およびリクエストの説明に、連絡先の IP アドレスを挿入するかどうかを指定します。このプロパティを指定しないか、**0**を指定した場合、IP アドレス情報は新規案件およびリクエストの説明に追加されません。このプロパティと **ContactAutoDesc** プロパティの両方に**1**を指定した場合は、連絡先の名前と IP アドレスが、カスタマ用インターフェースおよび従業員用インターフェースで作成された案件およびリクエストの説明に自動的に挿入されます。このプロパティは、アナリスト用インターフェースには影響しません。**ContactAutoDesc** が**1**以外の場合は、無視されます。

CstPrio

カスタマ用 **Web** インターフェースで作成した案件用の有効な優先度を指定します。カスタマ用インターフェースのユーザは、各自の案件に **CstPrio** リストの優先度を**1**つだけ指定でき、アナリストがリストにない値に変更した場合は案件の優先度を更新することはできません。

優先度リスト内のエントリは、スペースで区切ります。各エントリは、**1**～**5**の数字または単語「なし」である必要があります。最初に、カスタマ用インターフェースで作成した案件用の初期設定の優先度を最初に指定します（これで、リストで繰り返し表示できます）。

デフォルト：なし、3、4、5

CstPrio の有効な値は、配布された優先度のシンボル名に対応します。**Java** クライアントを使用してこれらのシンボル名をカスタマイズできますが、初期設定名で優先度を参照し続ける必要がある **CstPrio** の仕様には影響を与えません。**1** が最も高い優先度に対応します。

DateFormat

日付のエレメントの順序を指定します。

デフォルト：YYYY/MM/DD hh:mm a(am,pm)

シンボル	説明
M	月を 1 桁または 2 桁で出力します。
MM	月を 2 桁で出力します。
D	日を 1 桁または 2 桁で出力します。
DD	日を 2 桁で出力します。
YY	年を 2 桁で出力します。
YYYY	年を 4 桁で出力します。
H	時間を 24 時間形式で 1 桁または 2 桁で出力します。
HH	時間を 24 時間形式で 2 桁で出力します。
H	時間を 12 時間形式で 1 桁または 2 桁で出力します。
hh	時間を 12 時間形式で 2 桁で出力します。
M	分を 1 桁または 2 桁で出力します。
mm	分を 2 桁で出力します。
S	秒を 1 桁または 2 桁で出力します。
ss	秒を 2 桁で出力します。
a(am, pm)	am と pm を文字列として出力します。

DateFormatNoTime

DateFormat と同じ定義を、時間部分を除いて指定します。

DebugSource

CA SDM フォーム上で標準的なブラウザの右クリック メニューを有効にします。このプロパティを設定しない場合は、フォームを右クリックすると CA SDM のメニューが表示されます。このプロパティを設定する場合は注意してください。ブラウザの標準の右クリック メニューの一部のオプションによって実行エラーが発生することがあります（このため、通常は無効になっています）。Internet Explorer の場合は、DebugSource プロパティが設定されていなくても、Ctrl キーを押しながら右クリックすることで、ブラウザの標準の右クリック メニューを表示できます。

DebugTrace

Web エンジンでトレース情報を `stdlog` ファイルに書き込みます。

重要: このプロパティは通常の使用時には設定しないでください。CA サポートが要求した場合にのみ使用してください。

EmpPrio

従業員用 Web インターフェースで作成したリクエスト用の有効な優先度を指定します。従業員用インターフェースのユーザは、各自のリクエストに EmpPrio リストの優先度を 1 つだけ指定でき、アナリストがリストにない値に変更した場合はリクエストの優先度を更新することはできません。

優先度リスト内のエントリは、スペースで区切ります。各エントリは、1～5 の数字または単語「なし」である必要があります。最初に、従業員用インターフェースで作成したリクエスト用の初期設定の優先度を最初に指定します（これで、リストで繰り返し表示できます）。

デフォルト: なし、3、4、5

EmpPrio の有効な値は、配布された優先度のシンボル名に対応します。Java クライアントを使用してこれらのシンボル名をカスタマイズできますが、初期設定名で優先度を参照し続ける必要がある EmpPrio の仕様には影響を与えません。1 が最も高い優先度に対応します。

ExclLockSeconds

「編集」をクリックした後にレコードに対する独占的なロックが与えられる最大時間（秒単位）を指定します。この時間が経過すると、**Web** エンジンがロックを解除し、ほかのユーザがレコードを更新できるようになります。**ExclLockSeconds** が期限切れになった後でユーザが保存しようとする、**Web** エンジンがロックの再取得を試行します。この試行は、ロックが解除されているときにほかのユーザがレコードを更新しなかった場合だけ成功します。ロックの再取得試行が失敗した場合、ユーザは更新情報を再入力する必要があります。

デフォルト：120（2分）

この引数はオプションです。指定しなかった場合はデフォルト値と見なされます。

注：**ExclLockSeconds** の値は、**Timeout** の値よりも小さくする必要があります。**ExclLockSeconds** は秒単位で指定し、**Timeout** は分単位で指定します。

FormCacheMax

各ユーザの **Web** エンジンのメモリに維持する最大フォーム数を指定します。**Web** エンジンが常に、各ユーザが最近使用したフォームを **FormCacheMax** に指定されている数だけ維持します。この数を超えるフォームは、タイムアウトの対象になります。タイムアウトになったフォームは、メインページの「戻る」または「進む」ボタンでアクセスできず、ポップアップフォームでサブミットできなくなります。

デフォルト：10

フォームのタイムアウト機能により **Web** エンジンのメモリを節約できますが、ユーザが手動でそれらを更新しなければならないこともあります。**FormCacheMax** を - 1 に設定して、フォームのタイムアウト機能を無効にできます。

FormTimeout

フォームが **Web** エンジンに維持される最小時間（秒単位）を指定します。この時間が経過すると、フォームはキャッシュから削除される対象となります。ユーザは常に、フォームをサブミットする前に少なくともこのパラメータで指定された秒数の間、フォームを操作できます。また、**Web** エンジンが常に、各ユーザが最近使用したフォームを **FormCacheMax** に指定されている数だけ維持します。

StayCacheList プロパティを使用して、特定のフォームがタイムアウトにならないように指定できます。

デフォルト： 180（3 分）

FormTitle

CA SDM Web フォームを表示している **Web** ブラウザのタイトルバーに含める文字列を指定します。**FormTitle** の値は、表示されている特定のフォームのタイトルに追加されます。

デフォルト： CA SDM

たとえば、デフォルト値のままで **Microsoft Internet Explorer** を使用してアナウンスメントの詳細フォームを表示した場合、タイトルバーは以下のように表示されます。

アナウンスメントの詳細 - CA SDM - Microsoft Internet Explorer

このプロパティはオプションです。指定しなかった場合、アナリスト用 **Web** インターフェースのタイトルには定数値が表示されません。カスタム用インターフェースと **PDA Web** インターフェースにはデフォルト値が表示されます。

HitTrackFile

使用したすべての **Web** ページのログを受け取るファイルの完全パスを指定します。ユーザがページをリクエストするたびに、このファイルに 1 行が書き込まれます。ファイルは無限に大きくなるため、このプロパティを指定する場合は注意が必要です。

注： タイムスタンプ、ユーザ ID、データベース レコード ID、および **HTMPL** フォーム名を含むレコードがこのファイルに追加されます。レコードの形式を変更することができます。大きくなりすぎないように、定期的にこのファイルを管理する必要があります。

このプロパティはオプションです。指定しなかった場合、ヒットトラッキングファイルは書き込まれません。

HtmlplCacheSize

HTMPL キャッシュのサイズを指定します。このサイズを超えると、最も使用回数の少ないフォームがキャッシュから削除されます。

デフォルト： 1000

ListAllMaximum

リスト全体を表示するリクエストが行われた場合にリストに表示する最大レコード数を指定します。この数を超えると、そのリクエストはパフォーマンスを低下させるため許可されていないことを示す警告メッセージがポップアップ表示されます。

デフォルト： 2500

ListAllWarn

リスト全体を表示するリクエストが行われた場合にリストに表示する最大レコード数を指定します。この数を超えると、そのリクエストがパフォーマンスを低下させることを示す警告メッセージと確認を求めるメッセージがポップアップ表示されます。

デフォルト： 1000

ListBottomMaximum

一番下までスクロールするリクエストが行われた場合にリストに表示する最大レコード数を指定します。この数を超えると、そのリクエストはパフォーマンスを低下させるため許可されていないことを示す警告メッセージがポップアップ表示されます。

デフォルト： 2500

ListBottomWarn

一番下までスクロールするリクエストが行われた場合にリストに表示する最大レコード数を指定します。この数を超えると、そのリクエストがパフォーマンスを低下させることを示す警告メッセージと確認を求めるメッセージがポップアップ表示されます。

デフォルト： 1000

ListPageLength

検索実行後にリスト ページに表示する見つかったレコードの最大数を指定します。

デフォルト： 10

LogoutURL

ユーザが CA SDM からログアウトした後に表示する Web ページの完全な URL を指定します。このプロパティはオプションです。指定なかった場合、ログアウトするとログイン フォームが表示されます。

Lr_Refresh

ログリーダーの更新間隔を秒単位で指定します。このプロパティにゼロ以外の値を指定した場合、指定した間隔（最小間隔は 30 秒）で通知ログリーダーが更新されます。

このプロパティはオプションです。指定しなかった場合、ログリーダーは 5 分（初期設定値の 300 秒）ごとに更新されます。このプロパティにゼロを指定すると、ログリーダーは自動的に更新されなくなります。

MacroPath

Web エンジンが PDM_MACRO タグによってリクエストされたファイルを検索するディレクトリパスのリストを指定します。複数のディレクトリをスペースで区切って指定できます。ディレクトリ名に環境変数を含めることもできます。この場合、環境変数の前にドル記号を付けます（例：\$NX_ROOT）。Windows の場合も UNIX の場合も、バックスラッシュ（¥）ではなく、スラッシュ（/）を使用してパスコンポーネントを区切ってください。このプロパティは必須です。通常、以下のように設定します。

```
$NX_ROOT/site/mods/macro $NX_ROOT/bopcfg/www/macro
```

MatchesFound

ルックアップフィールドのユーザのキーがあいまいなためにドロップダウン選択リストと共に編集フォームを再表示する必要がある場合に、フィールドの下に表示するメッセージのテキストを指定します。このプロパティはオプションです。指定しなかった場合、初期設定の「複数一致します」になります。

MaxRecordsAutoSuggest

自動検索候補または自動補完により検索フィールドの下に表示されるレコード数を指定します。

デフォルト：25

MaxSelectList

ルックアップフィールドのユーザのキーがあいまいなために編集フォームを再表示する必要がある場合に、ドロップダウン選択リストに表示する一致する項目の最大数を指定します。一致する項目がこの数より多く見つかった場合は、「一致が多すぎます」に指定したメッセージが表示されます。

MinCharsAutoSuggest

自動検索候補または自動補完により候補が表示されるまで検索フィールドに入力する必要がある最小文字数を指定します。

デフォルト：3

MouseoverPreviewDelayTime

リンク上にカーソルを移動してからマウスオーバー プレビューが表示されるまでの遅延時間をミリ秒単位で指定します。

遅延時間が経過する前にリンクからカーソルを移動した場合、プレビューは表示されません。

デフォルト：1000

NoMatchesFound

ルックアップ フィールドのユーザのキーが正しくないために編集フォームを再表示する必要がある場合に、フィールドの下に表示するメッセージのテキストを指定します。このプロパティはオプションです。指定しなかった場合、初期設定の「一致が見つかりません」になります。

PreLogin Timeout

ログイン前に **Web** エンジンがセッションをアクティブに保つ最大時間（分単位）を指定します。ユーザがログインフォームをリクエストしたときに、**Web** エンジンユーザがログインを完了すると予期して、自動的にセッションを開始します。指定した時間内にユーザがログインしないと、**Web** エンジンユーザはセッションを破棄します。その後ユーザがログインすると、**Web** エンジンユーザはセッションを作成します。この処理は、ユーザに透過的に行われます。

このプロパティは、エンドユーザに影響を与えません。パフォーマンスの向上、つまり **Web** エンジンのメモリ使用量とセッションの破棄および再作成に伴うオーバーヘッドのバランスを取ることを目的としています。このプロパティはオプションです。指定しなかった場合、初期設定の1分間になります。

RedirectingURL

WebDirector がこの **Web** エンジンにリクエストを送信するのに使用する URL を指定します。このプロパティには、**Web** エンジンの完全な URL（http を含む）を指定します。**WebDirector** を使用している場合、このプロパティは必須です。使用していない場合は、無視されます。

SchedExpMaximum

SchedExpMaximum

一度にエクスポートできるスケジュール イベントの数の制限を指定します。

デフォルト：1000

重要: デフォルトでは、**CA SDM** が一度に処理できる最大数をエクスポートします。このデフォルト値を増加させるとシステムが不安定になる場合があります。ユーザが **SchedExpMaximum** で指定された値を超えてエクスポートしようとする、ユーザのエクスポート リクエストを拒否するメッセージが表示されます。

SellistCacheExclude

SellistCacheExclude

<PDM_SELECT> リスト用のキャッシュから除外するファクトリ（オブジェクト）の名前を指定します。パフォーマンスを向上させるために、**Web** エンジンでは通常、<PDM_SELECT>（ドロップダウン）リストと階層検索リストで使用されている小さなテーブルの内容を独自のメモリにキャッシュします。データ パーティションの制約を使用している場合は、テーブルのキャッシュが行われないようにして、異なるユーザが異なるテーブル ビューを受け取るように指定します。また、このプロパティの値にテーブルを含めると、**Web** エンジンでは起動時にレコードカウントを照会する必要がなくなり、起動時のパフォーマンスが多少向上します。このプロパティはオプションです。指定する場合は、1 つ以上のオブジェクト名をスペースで区切って含める必要があります。

SellistCacheMax

SellistCacheMax

Web エンジンにキャッシュできる、テーブル内のレコードの最大数を指定します。**Web** エンジンでは、キャッシュ サイズを上限としてテーブルのすべての内容を独自のメモリに維持し、これらのテーブルを使用して<PDM_SELECT>リストを作成するパフォーマンスを向上させます。このプロパティに大きい値を指定すると、パフォーマンスは向上しますが、メモリ使用量が多くなります。

デフォルト : 10

SelListCacheMax は、リクエスト、案件、および変更要求のカテゴリなど、階層検索リストで使用されるテーブルでは無視されます。**Web** エンジンには常に、階層検索リストで使用されているテーブルのすべての内容を独自のメモリに格納します。これらのテーブルに値が大量にある場合は、**SelListCachePreload** プロパティを指定してください。

SelListCachePreload

起動時に **Web** エンジンの選択キャッシュにロードする 1 つ以上のテーブルを指定します。このプロパティに指定されていないテーブルは、それが初めて使用されるときにロードされます。**SelListCacheMax** の値が大きい場合、または階層検索リスト（カテゴリなど）に大量のレコードがある場合は、**SelListCachePreload** にテーブルを指定することをお勧めします。これにより、ユーザがテーブルを使用して初めてフォームにアクセスしたときの応答時間が遅くなることを防止できます。

SelListCachePreload プロパティには、オブジェクト名をスペースで区切って指定します。各オブジェクト名の後ろには、属性名のオプションのリストを括弧で囲んで指定できます。リストに指定した属性は、**Web** エンジンにロードされます。属性を指定しなかった場合は、オブジェクトの共通名と関連付け属性の値だけがロードされます。これはドロップダウン検索には充分ですが、階層検索では充分でないことがあります。階層検索フォーム（`hiersel_xx.html`、`xx` はオブジェクト名）を変更した場合は、フォームで使用されているすべての属性が **SelListCachePreload** プロパティに指定されていることを確認します。属性を指定しなかった場合は、フォームが使用されたときにキャッシュがリロードされます。

SelListCachePreload プロパティはオプションです。指定しなかった場合は、ユーザがドロップダウン選択または階層検索を使用してフォームをリクエストするまで選択キャッシュに何もロードされません。

```
chgcat(description owning_contract) chgstat crs isscat(description
owning_contract) issstat pcat(description cr_flag in_flag pr_flag
owning_contract) pri tskstat urg pcat_cr(description cr_flag in_flag pr_flag
owning_contract) pcat_pr(description cr_flag in_flag pr_flag owning_contract)
pcat_in(description cr_flag in_flag pr_flag owning_contract)
```

StayCacheList

表示されている時間にかかわらず、フォーム キャッシュから削除しないフォームの名前を指定します。このプロパティにより、フレーム表示の固定フレームがセッション終了まで維持されます。ほかのフォームが永久的にキャッシュされないように、注意して使用する必要があります。初期設定は以下のとおりです。

```
scoreboard.html top_splash.html buttons.html hiersel_admin_tree.html
```

SuppressHtmlCache

ページがリクエストされるたびに、ページの内容を定義しているすべてのファイルを **Web** エンジンが再読み込みすることを指定します。**HTML** ファイルの解析では、**Web** エンジンの処理に大幅に時間がかかり、ほとんどのページで **PDM_INCLUDE** タグが使用されるため、通常は複数の物理ファイルが読み込まれます。**Web** エンジン通常、同じページに関する以降のリクエストに直ちに応えられるように、解析済みのファイルを独自のメモリに保存します。これによりパフォーマンスは大幅に向上しますが、変更を適用するためには **Web** エンジンをリサイクルしなければならないため、新しいページや更新されたページを作成しているユーザの利便性は損なわれます。

このプロパティはオプションです。値を指定する必要はありません。指定した場合、**Web** エンジン解析済みファイルをキャッシュしなくなり、**HTML** ファイルに行った変更が直ちに適用されます。パフォーマンスに対する影響が大きいため、このプロパティは実稼動環境では指定しないでください。

SuppressLoginAndLogoutMsg

ユーザが **Web** インターフェースのログインまたはログアウトを行うたびに、**Web** エンジンが **CA SDM** のログ ファイルにメッセージを記録しないことを指定します。

このプロパティはオプションです。指定しなかった場合、ユーザがログインまたはログアウトするたびに **Web** エンジンメッセージをログに記録します。

SuppressMacroCache

新しいページがリクエストされるたびに、保存されているすべてのマクロを **Web** エンジンが破棄することを指定します。 **Web** エンジンは通常、マクロに関する以降のリクエストに直ちに 대응できるように、解析済みのマクロを独自のメモリに保存します。これによりパフォーマンスは向上しますが、変更を適用するためには **Web** エンジンのリサイクルしなければならないため、新しいマクロや更新されたマクロを作成しているユーザの利便性は損なわれます。

このプロパティはオプションです。指定した場合、**Web** エンジンは解析済みマクロをキャッシュしなくなり、マクロに行った変更が直ちに適用されます。パフォーマンスに対する影響が大きいため、このプロパティは実稼動環境では指定しないでください。

Timeout

ユーザのセッションがアイドル状態になっていられる時間（分単位）を指定します。この時間が経過するとセッションは自動的に終了し、すべてのサーバリソースが解放されます。

注: Timeout の値は、ExclLockSeconds の値よりも大きくする必要があります。ExclLockSeconds は秒単位で指定し、Timeout は分単位で指定します。

TooManyMatches

ルックアップフィールドのユーザのキーがあいまいで、キーに一致する項目数が **MaxSelectList** の値を超えた場合に、フィールドの下に表示するメッセージのテキストを指定します。このプロパティはオプションです。指定しなかった場合、初期設定の「一致が多すぎます」になります。

UpdatedAnnouncementsPopup

ブラウザが新しいアナウンスメントをチェックする間隔を指定します。アナウンスメントが見つかり、ポップアップウィンドウにアナウンスメントが自動的に表示されます。間隔値は分単位で指定します。ブラウザパフォーマンスへの影響が少なくなるように、この変数は 5（分）より大きい値に設定することをお勧めします。

UseDirector

WebDirector がこの Web エンジンを実行するタイミングを指定します。指定可能な値は以下の表のとおりです。

値	説明
×	Web エンジンは、WebDirector に依存しません。これが初期設定値です。
○	WebDirector は、ログイン フォームを含むすべてのセッションを開始する必要があります。ユーザが Web エンジンに直接接続しようとする、Web エンジンは WebDirector に照会を求めます。
AfterLogin	Web エンジンは、ユーザを認証した後に、WebDirector にセッションを照会します。UseDirector AfterLogin に設定されている Web エンジンが単独で認証を行います。このため、この Web エンジンは、セキュリティ保護を最大限高めることができるようにセキュア ソケット (SSL) を使用する対象になります。
BeforeLogin	Web エンジンは、ユーザを認証する前に、WebDirector にセッションを照会します。UseDirector BeforeLogin に設定されている Web エンジンは、ログイン ページを表示せず、ログイン パスワードを受け付けません。

このプロパティはオプションです。指定しなかった場合、Web エンジンは WebDirector を使用しません。

UseNestedTabs

詳細フォームにネストされたタブ コントロール表示するかどうかを指定します。

デフォルト：有効

WebDirectorSlumpName

この Web エンジンにサービスを提供する WebDirector の名前を指定します。このプロパティを指定する必要があるのは、複数の WebDirector を実行している場合、または初期設定の web:director 以外の Slump 名を使用するように WebDirector を設定した場合だけです。

WebDirector を使用している場合、このプロパティはオプションです。使用していない場合は、無視されます。

WillingnessValue

Web エンジンがセッションを受け入れる **willingness** 値を 0 ～ 10 の範囲で指定します。WebDirector を使用している場合にのみ、このプロパティは使用されます。この値は、同じ WebDirector に関連付けられているほかの Web エンジンの **willingness** 値と比較されます。

WebDirector は、Web エンジンの **willingness** 値に応じてセッションを Web エンジンに転送します。**willingness** 値がほかの Web エンジンの約 2 倍である Web エンジンには、2 倍のセッションを処理します。

WillingnessValue にゼロを指定すると、Web エンジンがセッションを受け入れなくなります。この値は、UseDirector が AfterLogin に設定されている場合に役立ちます。

WebDirector を使用している場合、このプロパティはオプションです。使用していない場合は、無視されます。指定しないと、Web エンジンの **willingness** 値は 5 に設定されます。

WorkFrameTimeout

Web エンジンが内部サーバ リクエストに対する応答を待機する最大時間を秒単位で指定します。この時間が経過すると、リクエストが失敗します。通常の Web ページ以外のサーバ データを必要とする CA SDM Web インターフェース機能には、ワークフレームが使用されます。これには、自動入力、カテゴリ プロパティのロード、スコアボード数の更新などの機能が含まれます。CA SDM へのワークフレームのリクエストが失敗することはありません。ただし、ほかのサーバ（ナレッジ マネジメント などの統合製品）へのワークフレーム リクエストは、ターゲットサーバが稼働していない場合、またはネットワークの問題によりターゲットサーバにアクセスできない場合に失敗することがあります。**WorkFrameTimeout** プロパティには、リクエストが失敗したと見なされてほかのリクエストがワークフレームを使用できるようになるまでの時間を指定します。

注: **WorkFrameTimeout** は、ワークフレームが必要な環境ですべてのワークフレームが使用されている場合のみチェックされます。このため、リモートサーバが応答するまでの時間は、**WorkFrameTimeout** に指定されている時間よりも長くなります。**WorkFrameTimeout** の値は最小値です。

このプロパティはオプションです。指定しなかった場合、Web エンジンには 30 秒のワークフレーム タイムアウト値を使用します。

第 14 章: Text API の使用

このセクションには、以下のトピックが含まれています。

[Text API](#) (P. 647)

Text API

Text API は、テキストベースの入力を使用して、CA SDM データベース内で案件、リクエスト、連絡先、アセットなどのオブジェクトを作成および更新できるインターフェースです。*Text API* を使用すると、ユーザがアクセス可能なフィールドの大部分に値を割り当てることができます。

重要: CA SDM では、すべての入力文字列が UTF-8 形式である必要があります。それ以外の形式を使用すると、データが破損する可能性があります。[pdm_unconv ユーティリティ](#) (P. 1337) を使用すると、ローカルの文字セットから UTF-8 に、または UTF-8 からローカルの文字セットにデータを変換できます。

Text API には、以下のインターフェースを使用してアクセスできます。

- コマンドライン
- 電子メール
- CA NSM

注: Web サービスを、アプリケーション統合用の *Text API* の代替機能として使用できます。

関連項目:

[変換メソッド](#) (P. 660)

コマンドライン インターフェース

`pdm_text_cmd` コマンドを使用して、Text API コマンドライン インターフェースを有効にします。処理するテーブルや実行する操作などの情報は、`pdm_text_cmd` コマンドのパラメータを使用して指定できます。

Text API に入力した情報は、入力ファイルの形式で、または STDIN から直接、`pdm_text_cmd` コマンドに渡されます。

注: コマンドプロンプトからパラメータを渡す場合は、Ctrl + Z キー (Windows)、または Ctrl + D キー (POSIX) を使用します。

重要: `bop_cmd` および `pdm_text_nxd` コマンドのパラメータとして単一引用符または二重引用符を使用することはできません。

関連項目:

[pdm_text_cmd—Text API コマンドライン インターフェース \(P. 1333\)](#)

CA Network and Systems Management インターフェース

CA NSM と CA SDM が統合されていて、CA NSM イベントからリクエストを作成する場合、ライタールール定義内の `user_parms` パラメータが Text API に渡されます。CA SDM のライタープロセス (`tngwriter`) は、テキストを Text API に送信する前にそれを変更するための独自の置換パラメータを定義します。キーワード `LOG_AGENT` が入力の最後に追加され、リクエストの `log_agent` が設定されます。

注: CA NSM アラート管理システムから CA SDM に渡される追加のフィールドすべてについて、`Text_API.cfg` ファイルを更新する必要があります。このファイルは Web サービス、電子メールおよび AHD.DLL との統合に使用されます。

関連項目:

[キーワード \(P. 650\)](#)

入力フォーマット

Text API への入力は以下の方法で指定されます。

- コマンドライン インターフェースでは、入力は通常、`pdm_text_cmd` コマンドに渡すテキスト ファイルに指定されます。
- 電子メール インターフェースでは、入力は電子メールのテキスト内に指定されます。正規表現を指定して、ターゲット オブジェクト ID を検索できます。

どちらのインターフェースを使用しても、同じ方法で Text API への入力をフォーマットします。

入力の基本フォーマットは以下のとおりです。

```
%keyword=value
```

または

```
%PROPERTY={{property_label}}value
```

Text API コマンドの通常の動作では、2 つ以上の矛盾するコマンドが存在する場合は最後のコマンドが優先されますが、以下の例外があります。

- メッセージに、メールボックス ルール フィルタ文字列と一致する有効なチケット ID 成果物、または複数の Text API チケット ID コマンドが含まれている場合、最初のおカレンスが使用されます。また、チケット ID 成果物（メールボックス ルール フィルタ文字列を使用して識別される）は、最初に検出されたコマンドにかかわらず、どの Text API チケット ID コマンドよりも優先されます。
- メッセージに複数のログ コメント Text API コマンドが含まれる場合、すべてのコメントがポストされますが、それらがチケット アクティビティ ログに表示される順序は異なる場合があります。

フィルタに一致するすべてのチケット ID 成果物（有効かどうかにかかわらず）と、メッセージ内の Text API チケット ID コマンド（適用可能かどうか、あるいは適用されたかどうかにかかわらず）はすべて、メッセージがポストされる前にコメント化されます。メールボックス ルール フィルタによって識別されたチケット ID 成果物は「-((...))-」と表示されます。Text API チケット ID コマンドの先頭のパーセンテージ記号（%）は、2 つの開かっこ「(」とコマンドの後に続く 2 つの閉かっこ「)」に変換されます。ログ コメント（%LOG=...）付きの別の Text API コマンドの後に Text API チケット ID コマンドがある場合、コメント化された Text API チケット ID コマンドは個別のログ コメントになります。

注: ログコメントは、1つのメッセージ内で複数回使用できて、さらに各オカレンスが適用される唯一の **Text API** コマンドです。ほかのコマンドでは、**Text API** は最後のオカレンスのみを使用します。これは、ほかのコマンドの複数のオカレンスは相互に矛盾するためです。複数のログコメントコマンドによって個別のログコメントメッセージがチケットにポストされますが、その順序は必ずしも決まっていません。

また、**Text API** チケット ID コマンドがメッセージの先頭、またはほかの 2 つの **Text API** コマンドの間に存在する場合、そのコマンドはログコメントに変換されます。前のコマンドがログコメント (**%LOG=...**) または更新の説明 (**%DESCRIPTION=...**) である場合、コマンドは個別のログコメントになるのではなく、前のコマンドに追加されます。

HTML のみが送信され、プレーンテキストバージョンが含まれていない着信メッセージでは、メッセージ本文が失われます。空のメッセージ本文を使用した任意のメールボックスルールフィルタにメッセージが一致する場合、空の説明または引用されたメッセージの件名をチケットの説明全体として、チケットを作成できます。

キーワード

Text API に対する入力として 2 種類のキーワードを使用できます。

- 1 つは、更新可能なさまざまなテーブルのフィールドに直接関係するキーワードのグループで、**text_api.cfg** ファイルの **[KEYWORDS]** セクションで定義します。たとえば、[案件の詳細] フォームのほとんどのフィールドは **[KEYWORDS]** セクションで定義します。これらのキーワードを使用して、更新または作成するレポート内のフィールドの値を設定できます。たとえば、以下の行は案件の優先度を 5 に設定します。

```
%PRIORITY=5
```

text_api.cfg ファイルの **[KEYWORDS]** セクションには、すべてのキーワードが列挙されています。追加のキーワードを定義できます（たとえば、ユーザのデータベーススキーマをカスタマイズする際に、追加したフィールドへの **Text API** のアクセスを許可する場合など）。

- `text_api.cfg` ファイルの内容にかかわらず、特殊なキーワードが常に以下のように定義されています。

キーワード	説明
ASSET	チケットに項目を添付するのに使用します（リクエスト、案件、および変更要求で有効）。指定する値は項目名で、すでに存在している必要があります。チケットには複数の項目を添付できるため、このキーワードは複数回指定できます。
ATTACHMENT	チケットに電子メール添付ファイルを追加するのに、電子メールインターフェースによって内部的に使用されます。
DESCRIPTION	チケットの説明フィールドに使用する値を指定します。キーワードを明示的に指定せずに入力を Text API に送信した場合は、このキーワードが使用されます。メッセージがキーワードで始まり、チケット ID 成果物またはキーワードを含む場合、Mail Eater によって自動的にこのキーワードが適用されます。 <code>text_api.cfg</code> の[OPTIONS]セクションの以下のエントリを使用して、DESCRIPTION キーワードが更新でどのように処理されるかを変更できます。 UPDATE_DESC_IS_LOG このオプションを YES に設定した場合、この値が使われてログコメントが作成されます。このオプションを NO に設定した場合、既存の説明フィールドがこの値で上書きされます。
FROM_EMAIL FROM_EMAIL_OVERRIDE	<code>ca_contact</code> レコードの「電子メールアドレス」フィールドに対して照合するのに、電子メールインターフェースによって使用されます。これはチケットの <code>log_agent</code> としても使用されます。両方を指定すると、FROM_EMAIL が無視されます。 注: FROM_EMAIL はメッセージの送信者アドレスで、Mail Eater によって自動的に設定されます。
FROM_PERSID	操作の <code>log_agent</code> を定義するために、コマンドラインインターフェースによって使用されます（たとえば、 <code>ca_contact</code> レコードにユーザ ID がない場合など）。 <code>-p</code> パラメータが指定されている場合、このキーワードは <code>pdm_text_cmd</code> によって自動的に渡されます。値は、 <code>ca_contact</code> レコードの <code>persistent_id</code> に対して照合されます。

キーワード	説明
FROM_USERID	操作の log_agent を定義するのに、コマンドラインインターフェースでのみ使用します。-u パラメータが指定されている場合、このキーワードは pdm_text_cmd によって自動的に渡されます。値は、連絡先のユーザ ID に対して照合されます。
LOG	ログ エントリを作成するのに使用します（リクエスト、変更要求、案件、および連絡先で有効）。メッセージがキーワードで始まらず、チケット ID 成果物またはキーワード、あるいは DESCRIPTION キーワードのいずれかを含む場合、 Mail Eater によって自動的にこのキーワードが適用されます。
LOG_AGENT	操作の log_agent を定義するために、 CA NSM インターフェースによって使用されます。値は連絡先レコードの ID フィールドに対して照合されます。
PROPERTY	プロパティの値を設定するのに使用します（リクエスト、変更要求、および案件でのみ有効）。等号記号と値が後ろに続くほかのキーワードとは異なり、 PROPERTY キーワードの構文には以下のようにプロパティ ラベルを含める必要があります。 PROPERTY={{property_label}}value データベースに表示されるとおりに <i>property_label</i> を指定する必要があります。
SEARCH	アセットの複数のチケットを更新するクエリで使用するキーワードのリストを指定するために、コマンドラインインターフェースと CA NSM インターフェースでのみ使用します。値は、検索で使用するキーワードのリストです。 SEARCH キーワードは CA NSM インターフェースによって自動的に設定されます。
SEARCH_EXPLICIT	CA NSM インターフェースで指定された SEARCH キーワードを無効化するために、 CA NSM インターフェースでのみ使用します。提供された値は SEARCH キーワードと同じです。

関連項目:

[pdm_text_cmd—Text API コマンドラインインターフェース \(P. 1333\)](#)

キーワードの入力規則

キーワードの入力フォーマットには、以下の規則が適用されます。

- すべてのキーワード（PROPERTY を含む）の前にパーセント（%）記号を付けます。パーセント記号は列 1 にある必要があります。最初の空白ではない行の入力の行頭がパーセント記号ではない場合、チケット ID アーチファクトとキーワードのどちらが検出されたかによって、%DESCRIPTION= または %LOG= が受信データのプレフィックスとして使用されます。%DESCRIPTION が設定された場合、最初のキーワードまでのメッセージの内容がチケットの説明として公開されます。%LOG= が設定された場合、最初のキーワードまでのメッセージの内容がログ コメントとして公表されます。
- キーワード内、パーセント記号とキーワードの間、およびキーワードと等号（=）記号の間にはスペースを使用しないでください。
- 値を引用符で囲まないでください。等号（=）記号以降のすべてのデータは値とみなされます。
- キーワードでは大文字と小文字が区別されません。
- 入力に重複したキーワードが含まれる場合、最後のキーワードが使用されます。重複するキーワードが存在しない場合、キーワード/値ペアを指定する順序は重要ではありません。
- キーワードの値は、Web インターフェースの対応するフィールドに指定する場合と同様に指定します。たとえば、アナリストの連絡先タイプを指定するには、データベースにこの値が整数で格納されている場合も、%CONTACT_TYPE=Analyst を使用します。CONTACT_TYPE キーワードは text_api.cfg に定義されていて、格納されている値と一致するように [指定した値を変換します](#) (P. 660)。

注: 値で大文字と小文字が区別されるかどうかは、基礎となる DBMS によって決まります。

- 文字列データは、複数行に渡っていてもかまいません。

チケットを更新するための電子メールのフォーマット

チケットを作成または更新するために、電子メール メッセージをフォーマットできます。

チケットを作成または更新するために電子メール メッセージをフォーマットするには、以下のフィールドを使用します。

受信者

特権ユーザ用に設定されている **CA SDM** の連絡先に割り当てられているメールボックス名を指定します。

送信者

電子メールを送る人を指定します。適用されるメールボックス ルールで [匿名を許可] オプションが指定されていない限り、この人物は、**ca_contact** テーブルで定義されている必要があります。

注: From アドレスは通常ユーザの電子メール プログラム構成の一部です。また、通常はメッセージ単位で設定されません。

添付ファイル

Text API に添付ファイルを送るため、電子メールにドキュメントおよび他のファイルを添付します。

件名

チケットを作成する場合は特に、メールボックス ルール内のキーワードに一致させます。

本文

Text API を使用して、電子メールの本文を指定します。チケットを作成または更新するチケットのタイプにより、キーワード **ISSUE_ID**、**REQUEST_ID** または **CHANGE_ID** を指定できます。

電子メール メッセージの開始および終了区切り文字

電子メール インターフェースによっては、メール メッセージの最初または最後に、電子メール インターフェースの誤動作を招く情報（たとえば、MIME エンコーディング）が追加されることがあります。ご使用の電子メール インターフェースで情報を追加する場合、`start-request` と `end-request` という区切り文字を使用できます。- 電子メール インターフェースは、`start-request` より前と `end-request` より後に入力された情報を無視します。

注: Mail Eater は RTF か HTML 形式のみの電子メールをサポートしません。

例: `start-request` と `end-request` 区切り文字の使用例を、以下に示します。

```
"start-request"
message_body
"end-request"
```

Text API におけるアーチファクトの使用

Text API は、電子メール通知の件名と本文を処理します。メールボックスルールを使用すると、Text API が使用するアーチファクトおよび値を識別できます。たとえば、インシデントに対するルールを `Incident:{{object_id}}` と定義した場合、`Incident:1234` が Text API 用に `%INCIDENT_ID=1234` と変換されていることがわかります。`1234` はインシデント用の `ref_num` です。アーチファクトは、電子メールにおいて一意で、見つけやすくする必要があります。そのため、アーチファクトを `%Incident : {{object_id}}%` のように、より特徴的にすることができます。

文字、数字、カンマ、スラッシュ (/)、プラス記号 (+)、または等号 (=) は、アーチファクトに使用されることがあるため、`{{object_id}}` キーワードはこれら以外の字に続けます。このように記述しない場合、アーチファクトに続く文字が値の一部であると誤解されたり、アーチファクトの値に含まれる文字が、アーチファクトに続く文字であると誤解される可能性があります。

Mail Eater を使用して以下を実行できます。

1. Text API によってサポートされる適切なチケット、または他のオブジェクトにマップする電子メール内のアーチファクト (`Incident:1234` など) を検出します。
2. アーチファクトを Text API トークン (`%INCIDENT_ID=1234` など) に変換します。

3. **Mail Eater** は、タグ付けされたメッセージを **Text API** にサブミットします。**Text API** は電子メールを処理して、**Text API** に含まれるテキスト、コマンド、または両方を適切なチケットに適用し、**Text API** が受信した電子メールメッセージが正常に適用されたかどうかを示す自動応答電子メールを生成します。実行されたアクションによって、通知電子メールメッセージも、チケットの作成のような特定のイベントを示すために、別々に送信されます。

チケットを更新する通知応答のセットアップ方法

Text API デーモン (`pdm_text_nxd`) は、コマンドラインや電子メールのような外部インターフェースからの情報を使用してチケットを作成し更新します。ユーザ（連絡先）が電子メール通知に返信するとチケットを更新できるように、電子メールで **Text API** を使用するようセットアップできます。返信のテキストはログ コメント アクティビティとしてチケットに追加されます。

チケットを更新する通知応答をセットアップするには、以下の手順に従います。

1. 連絡先が使用する通知方法を `pdm_mail -T reply_email_address`、または `pdm_mail -F reply_email_address` に設定します。`reply_email_address` は、メールボックスの受信アドレスを指定します。連絡先が電子メールの返信をクリックすると、返信しようとしているメッセージの **From** または **Reply-To** アドレスが宛先のアドレスに挿入されます。

`-T` は **Reply-To** アドレスを設定します。`-F` は **From** アドレスを設定します。別のアドレスが返信用として指定されていない場合は、このアドレスが使用されます。

注: **Reply-To** アドレスを使用しない、または使用できないメールプログラムもあります。

2. **Text API** キーワードを使用して、メールボックスルールを作成または更新します。

メールボックスルールフィルタにおけるユーザ定義のアーチファクトは、以下の **Text API** キーワードを置換します。

オブジェクト	Text API キーワード	ID
インシデント	%INCIDENT_ID	Ref_num
問題	%PROBLEM_ID	Ref_num

オブジェクト	Text API キーワード	ID
リクエスト	%REQUEST_ID	Ref_num
Chg_ref_num	%CHANGE_ID	Chg_ref_num
案件	%ISSUE_ID	Ref_num

3. ルールに一致する通知フレーズを作成または更新します。
4. 通知フレーズを使用するメッセージテンプレートを作成または更新します。
5. ステップ 2 で作成したメッセージテンプレートを以下のように更新し、ステップ 4 で作成または更新したメッセージテンプレートを指定します。

注: 各ステップの実行に関する詳細については、オンライン ヘルプを参照してください。

ユーザが通知を受信し、それに対して応答すると以下のアクションが実行されます。

1. フィルタ文字列が検出されると、プレースホルダによって示される関連するチケット ID キーワードや値がある場合は、メッセージに追加されます。
2. 一致するチケット ID アーチファクトが検出されると、対応するチケットが、ログ コメント、新規の説明、またはメッセージ内のテキストに一致するその他の値、キーワード、コマンドのいずれかを使用して更新されます。
3. 一致するチケット ID アーチファクトが検索されない場合、説明およびメッセージ内のテキスト、キーワード、コマンドに一致する他のパラメータを使用して、チケットが作成されます。

インシデント通知に対する応答のセットアップ方法の例

この例では、インシデント通知に対する応答をセットアップする方法を示します。

インシデント通知に対する応答をセットアップするには、以下の手順に従います。

1. 以下のフィールドおよび値を使用して、メールボックス ルールを作成します。
 - フィルタ - 本文の内容
 - フィルタ文字列 - %Incident : {{object_id}}%
 - 大文字と小文字を区別しない - はい
 - アクション - オブジェクトの更新
 - アクション オブジェクト - インシデント
2. 以下のルールを含む通知フレーズを作成します。
 - シンボル - インシデント応答
 - コード - インシデント応答
 - アクティブ - アクティブ
 - 説明 - インシデント/問題/リクエストへの返答に埋め込むコメント
 - フレーズ - @{{call_req_id.type.sym}} にコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。

%Incident : {call_req_id.ref_num}%

注: メールボックス ルールの自動応答テキストでは、プレフィックス `call_req_id` を省略します。このプレフィックスは、メールボックス ルールのテキストがすでに含まれているコンテキストを適用します。また、コンテキスト内ですでに動作している場合、このようなコンテキスト変更は有効ではありません。

3. 以下の通知フレーズを使用するメッセージテンプレートを作成または更新します。

- 通知メッセージ本文

これは、簡単な通知です。

@{notification_phrase[IncidentURL1].phrase}

4. ステップ 1 で作成したメッセージテンプレートを以下のように更新し、ステップ 3 で作成したメッセージテンプレートを指定します。

メッセージテンプレート - メールボックス ルール名

エンド ユーザによるチケットの更新例

エンド ユーザ (John Smith) が電子メール通知に返信し、インシデント チケットを更新する方法の例を以下に示します。

電子メールの本文 (Body) か件名 (Subject) には、オブジェクト ID が含まれます。フィルタ文字列内の `{{object_id}}` プレースホルダは、オブジェクト ID を表します。

1. 以下の説明を含む通知が John Smith に送信されます。

インシデントにコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。

%Incident:1234%

2. John Smith は、通知に以下のように返信します。

これは私の応答です...

3. Mail Eater は、John Smith の電子メールを以下のテキスト バージョンで受信します。

これは私の応答です...

送信者: Service Desk

送信日時: 2009 年 9 月 18 日、水曜日 (午前 10:22)

受信者: Smith, John

件名: 簡単な通知

これは、簡単な通知です。

インシデントにコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。

%Incident:1234%

4. Mail Eater は順番にルールを処理し、%Incident:1234% アーチファクトを検索します。

これは私の応答です...

送信者: Service Desk

送信日時: 2009 年 9 月 18 日、水曜日 (午前 10:22)

受信者: Smith, John

件名: 簡単な通知

これは、簡単な通知です。

インシデントにコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。

%INCIDENT_ID=1234

5. Mail Eater は、Text API キーワードおよび {{object_id}} 値を %INCIDENT_ID= statement に追加し、{{object_id}} 値が検出された個所にマーカーを付けます。以下のテキストは、Text API に送信されるデータを示しています。太字のテキストは、Mail Eater によって追加された値を示します。

%LOG=これは私の応答です...

送信者: Service Desk

送信日時: 2009 年 9 月 18 日、水曜日 (午前 10:22)

受信者: Smith, John

件名: 簡単な通知

これは、簡単な通知です。

インシデントにコメントを追加するには、この電子メールに返信するか、以下の行を（自分で作成した行に）追加してください。

%Incident:-((...))-%

%FROM_EMAIL=john.smith@company.com

%INCIDENT_ID=1234

6. Text API は、Incident 1234 にログ コメントを追加します。

変換メソッド

text_api.cfg に定義されている多くのキーワードには、指定した値をデータベース格納に適した値に変換するための関連するメソッドがあります。この機能により、基礎的な実装の知識がないユーザでも、Web インターフェースの場合と同じように値を指定できます。

構成ファイルには、`ISSUE.PRIORITY` や `CONTACT.CONTACT_TYPE` など、このタイプのキーワード定義の例がいくつかあります。キーワードの追加定義が必要になった場合（たとえば、データベーススキーマのカスタマイズ時に追加したフィールドへのアクセス権を **Text API** に付与するなど）、以下のいずれかの事前定義済みメソッドを使用できます。

メソッド	出力タイプ
<code>lookup_actbool</code>	INTEGER
<code>lookup_asset_by_name</code>	UUID
<code>lookup_asset_by_persid</code>	UUID
<code>lookup_chg_category</code>	STRING
<code>lookup_chg_status</code>	STRING
<code>lookup_cnt_by_email</code>	UUID
<code>lookup_cnt_by_last_first_middle</code>	UUID
<code>lookup_cnt_by_logonid</code>	UUID
<code>lookup_cnt_by_persid</code>	UUID
<code>lookup_cnt_meth</code>	INTEGER
<code>lookup_cnt_type</code>	INTEGER
<code>lookup_company</code>	UUID
<code>lookup_cr_status</code>	STRING
<code>lookup_cr_template</code>	STRING
<code>lookup_domain</code>	INTEGER
<code>lookup_grc</code>	INTEGER
<code>lookup_group</code>	UUID
<code>lookup_impact</code>	INTEGER
<code>lookup_iss_category</code>	STRING
<code>lookup_iss_status</code>	STRING
<code>lookup_loc</code>	UUID
<code>lookup_mfr_model</code>	UUID
<code>lookup_nr_family</code>	INTEGER
<code>lookup_org</code>	UUID

メソッド	出力タイプ
lookup_person_contacting	INTEGER
lookup_position	INTEGER
lookup_priority	INTEGER
lookup_prob_category	STRING
lookup_product	INTEGER
lookup_resource_status	INTEGER
lookup_service_lvl	STRING
lookup_severity	INTEGER
lookup_state	INTEGER
lookup_timezone	STRING
lookup_type_of_contact	INTEGER
lookup_urgency	INTEGER
lookup_workshift	STRING

変換する必要がある値が、これらの定義済みメソッドで対応できない場合は、カスタム メソッドを記述する必要があります。メソッドは、入力として **STRING** 値を取り、出力として値 (**INTEGER**、**STRING**、または **UUID**) を返す必要があります。値を判断できない（つまり、設定されない）ことを示すのに -1 (または "-1") の値を返します。**UUID** の場合は、"(uuid) NULL" を返します。

たとえば、ユーザ ID を **ca_contact** テーブル参照に変換するメソッドを作成した場合、**Administrator** などの入力値がメソッドに渡され、**Administrator** のユーザ ID に対応した **ca_contact** テーブル ID がメソッドから返されます。

環境設定ファイルにキーワードを定義する方法により、同じフィールドに複数のキーワードマッピング（指定された値に応じた異なる変換メソッドなど）を定義することができます。たとえば、担当者にいくつかの異なるキーワードマッピングを指定して、異なる入力値に基づいてどのように値を設定するかを定義することができます。入力がユーザ ID、姓/名/ミドルネーム、および実際の **ca_contact** ID（たとえば、**793ED69B4E87A545BD8E911834D829FC**）の場合、変換が不要な **ca_contact** ID を除いて、各キーワードは異なる変換メソッドにマップされます。

環境設定ファイル

`text_api.cfg` ファイルは、更新可能な各種テーブルのフィールドに直接関係するキーワードを定義します。このファイルは、特定の定義済みの値（キーワードなど）を検索するための参照情報として、また **Text API** を設定するためのメカニズムとして使用します。ただし、初期設定の環境設定ファイルは、変更しなくてもほとんどのインストール環境で機能します。

`text_api.cfg` ファイルは、以下のディレクトリにあります。

- UNIX - `$NX_ROOT/site`
- Windows - インストールディレクトリ¥`site`。例： `C:¥Program Files¥CA¥Service Desk¥site`

環境設定ファイルはいくつかのセクションに分かれていて、各セクション内には特定の属性が定義されています。属性は以下の形式で定義されています。

キーワード=値

キーワードの大文字小文字は区別されませんが、値の大文字小文字は区別されます（[`OPTIONS`]セクションを除く）。

注：`text_api.cfg` ファイルは、任意のテキストエディタを使用して表示および変更できます。

重要： `CA NSM` アラート管理システム コンポーネントと統合している場合は、`CA SDM` に渡されるすべての追加フィールドについて `text_api.cfg` を更新する必要があります。

関連項目：

[キーワード](#) (P. 650)

Options

`text_api.cfg` ファイルの [OPTIONS] セクションでは処理オプションを定義します。これはサイトによって異なる可能性があります。たとえば、入力データ形式を判断したり、改行を許可するフィールドを指定したり、電子メールインターフェースを使用して案件、リクエスト、または変更要求を更新できるようにするかどうかを指定したりするオプションがあります。このセクションのすべてのオプションは設定可能です。

`VALID_TABLE_LIST` からテーブル名を削除して、Text API がこれらのテーブルにアクセスできないように設定することはできますが、このリストにテーブル名を追加することはできません。

デフォルト

Text API を使用するインターフェースごとに `text_api.cfg` ファイルで提供されている [XX_DEFAULTS] セクションを使用します（電子メールインターフェース用の [EMAIL_DEFAULTS] やコマンドラインインターフェース用の [CMD_DEFAULTS] など）。[XX_DEFAULTS] セクションには、ユーザが直接指定しなかった場合に必要なフィールドやプロパティのデフォルト値が定義されています。XX は、CMD や EMAIL などのインターフェースタイプを指します。

初期設定値を設定するには、以下のいずれかの形式を使用します。

- `table_name.keyword=value`

keyword は、[KEYWORDS]セクションに定義するか、データベース内にプロパティとして定義する必要があります。*keyword* に関連付けられているあらゆるメソッドが自動的に *value* に適用されます。以下に例を示します。

`ISSUE.PRIORITY=1`

`PRIORITY` キーワードは `text_api.cfg` で定義され、指定した値をデータベース内の対応する値と一致するように変換するためのルックアップを実行します。ここでは、値 `1` が、ベースにあるデータベース内の優先度シンボル `1` に対する値 `5` に変換されます。この機能を使用すると、ユーザは Web インターフェースと同様の方法で値を指定できます。

■ `table_name.PROPERTY={{property_label}}value`

`property_label` は、データベース内にプロパティとして定義されている必要があります。

どちらの形式でも、`table_name` は、[OPTIONS]セクションの `VALID_TABLE_LIST` に定義されているいずれかの値（Issue、Request、Contact など）である必要があります。

関連項目：

[変換メソッド](#) (P. 660)

入力無視

`text_api.cfg` ファイルには、Text API を使用するインターフェースごとに `[..._IGNORE_INCOMING]` セクションが 1 つ存在します（たとえば、CA NSM インターフェース用の `[TNG_IGNORE_INCOMING]`、その他の CA 製品が使用する外部インターフェース用の `[EXT_IGNORE_INCOMING]` など）。これらのセクションは、入力で無視されるフィールドとプロパティを定義します（形式は、「`=value`」を指定することを除いて「初期設定」で説明したのと同じです）。この機能により、ユーザが特定の値を設定できないようにすることができます。これにより、カスタマに電子メールインターフェースの使用を許可する場合などに、セキュリティ保護を高めることができます。

IGNORE セクションと、対応する `[..._DEFAULTS]` セクションを組み合わせることで、ユーザが特定の値を設定できないようにして、それらの初期設定値を提供できます。たとえば、電子メールインターフェースユーザが案件の優先度を設定できないようにするには、以下の値を指定します。

```
[EMAIL_DEFAULTS]
ISSUE.PRIORITY=2
[EMAIL_IGNORE_INCOMING]
ISSUE.PRIORITY
```

この場合、ユーザが電子メールメッセージの本文に指定するあらゆる優先度が無視され、電子メールインターフェースによって作成されるすべての案件に自動的に優先度 2 が割り当てられます。

入力例

以下の例は、電子メールメッセージの本文で、またはコマンドラインインターフェースの入力として使用するファイル内で使用できる入力を示しています。

例: 最初の行にキーワードが含まれていない場合

この例では、最初の行の最初の列に `%keyword` がないため、リテラル `%DESCRIPTION=` がメッセージの先頭に追加されます。この追加によって、説明フィールドが「This entire text goes to the description field」に設定されます (`text_api.cfg` の `[OPTIONS]` セクションの `LINEFEEDS_ALLOWED` エントリにあるフィールドのリストに `ISSUE.DESRIPTION` が含まれているため、改行はそのまま残ります)。

```
This entire text goes
into the description field
%PRIORITY=None
```

例: 最初の行にキーワードが含まれている場合

この例では、`PRIORITY` キーワードは `text_api.cfg` に定義されていて、指定した値をデータベース内の対応する値と一致するように変換するためのルックアップを実行します。ここでは、値 `None` が、ベースにあるデータベース内の優先度シンボル `1` に対する値 `0` に変換されます。この機能を使用すると、ユーザは Web インターフェースと同様の方法で値を指定できます。

```
%description=This is my description
%priority=None
%CATEGORY=Upgrade.PC
%PROPERTY={{Current CPU}}266 mhz
%PROPERTY={{Current Harddrive}}1 gig
%PROPERTY={{Requested Upgrade}}4 gig harddrive
```

指定した値は、前の例と同様に、チケットの説明フィールドと優先度フィールドを設定するのに使用されます (キーワードの大文字小文字は区別されません)。

`Upgrade.PC` の値が検索され、チケットのカテゴリ フィールドが適切に設定されます。

以下のラベルに一致する 3 つのプロパティ値が設定されます。

- Current CPU
- Current Harddrive
- Requested Upgrade

第 15 章: CA SDM サーバにわたるシステム カスタマイズのバージョン管理方法

CA SDM のバージョン管理は、すべての CA SDM サーバ（クライアントおよびサーバ）にわたるシステムのカスタマイズを管理するのに役立ちます。CA SDM の設定に応じて、以下のクライアントおよびサーバが使用されます。

- 標準設定

- クライアント：セカンダリ サーバ
- サーバ：プライマリ サーバ

- 高可用性設定

- クライアント：アプリケーション サーバおよびスタンバイ サーバ
- サーバ：バックグラウンド サーバ

例: システム管理者として、CA SDM の `detail_osp_server.html` ページにフィールドを追加しました。ここで、クライアントとサーバにわたってこの変更を同期します。この例は、カスタマイズがどのように同期されるかを説明するために、シナリオ全体にわたって使用されます。

以下の図は、CA SDM サーバにわたってシステム カスタマイズのバージョン管理を行う方法を示しています。



次の手順に従ってください:

1. [前提条件を確認します](#) (P. 671)。
2. CA SDM で変更を行います。この例では、CA SDM の HTML ページに新しいフィールドを追加します。
3. [サーババージョン管理ファイルを変更します](#) (P. 671)。
4. クライアントで CA SDM をリサイクルします。
5. [クライアントでカスタマイズを確認します](#) (P. 681)。

前提条件の確認

以下の前提条件を確認します。

- `ver_ctl` オプションにアップグレード値が設定されていることを確認します。バージョンの相違が検出されると、影響を受けたコンポーネントのアップグレードがクライアントで試行されます。アップグレードが成功すると、サーバとクライアントの接続が継続されます。失敗すると、接続は終了します。`ver_ctl` オプションの詳細については、オンラインヘルプを参照してください。
- (CA SDM の設定に応じて) プライマリ サーバまたはバックグラウンドサーバの `$NX_ROOT¥site¥mods` ディレクトリに `server_secondary_custom.ver` ファイルが作成されることを確認します。バージョン管理コンポーネントへのカスタマイズを、すべてこのファイルで実行する必要があります。ファイルが存在しない場合は、同じ場所にそれを確実に作成します。

サーババージョン管理ファイルの変更

カスタマイズ (HTML ページでのフィールドの追加など) を完了した後、サーババージョン管理ファイルでバージョン管理コンポーネントを追加または更新します。バージョン管理コンポーネントは、ファイル、ディレクトリ、または `client_nx.env` 環境変数ファイルを表すことができます。

次の手順に従ってください:

1. CA SDM の設定に応じて、以下のサーバにログインします。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンドサーバ
2. 以下のディレクトリに移動します。
`$NX_ROOT¥site¥mods`
3. `server_secondary_custom.ver` ファイルを開きます。

4. 以下のコンポーネントを追加します。

```
[ MY_USP_SERVERS_HTML ]  
  
directory="$NX_ROOT/site/mods/www/html/web/analyst/Analyst"  
  
filename="detail_usp_servers.html"  
  
version="2.0 , 20121119"  
  
o_mode="RW"  
  
g_mode="RW"  
  
w_mode="RW"  
  
file_ctl
```

注: バージョン管理コンポーネントの追加または更新の詳細については、「[バージョン管理コンポーネント](#) (P. 672)」を参照してください。

5. server_secondary_custom.ver ファイルを保存します。

バージョン管理コンポーネントが、バージョン管理ファイルに追加されます。

バージョン管理コンポーネント

新しいコンポーネントを定義するには、

- 以下の構文を使用します。斜体の項目は管理者が指定するデータを表しています。コンポーネント名とバージョンパラメータは、常に必須です。その他のパラメータは、*control-type* の値によっては必須です。その他の項目はすべてキーワードを表しており、以下の例のとおり正確に入力する必要があります。

```
[ コンポーネント名 ]  
  
version = "x.x, yyyyymmdd"  
  
control-type  
  
filename = "ファイル名"  
  
directory = "ディレクトリ"  
  
link = "リンクディレクトリ"  
  
source = "ソースディレクトリ"  
  
effectivity = "有効性の仕様"
```

```
checksum
min_release = "リリース"
max_release = "リリース"
component_type = "ファイルタイプ"
o_mode = "所有者モード"
g_mode = "グループモード"
w_mode = "ワールドモード"
```

注: パラメータの詳細については、「[バージョン管理のパラメータ](#) (P. 673)」を参照してください。バージョン管理ファイルの構造と構文の詳細については、\$NX_ROOT¥site ディレクトリにインストールされている .ver ファイルを参照してください。これらのファイルには、役に立つコメントと設定例が含まれています。

既存のコンポーネントエントリを更新するには、

- パラメータを変更します。たとえば、バージョン番号を変更します。

コンポーネントからコントロールを削除するには、

- 以下のようにコンポーネントを編集します。

```
! uncontrol component-name
```

バージョン管理のパラメータ

Version Control では以下のパラメータを使用します。

[コンポーネント名]

Version Control での項目の名前を指定します。名前は一意でなければならない、角かっこで囲む必要があります。コンポーネント名では大文字小文字は区別されません。このパラメータは、コンポーネント定義を開始するのに必須のパラメータです。

`version="x.x. yyymmdd"`

コンポーネントのバージョンを定義するバージョン番号 (**x.x**) と日付 (**yyymmdd**) を指定します。このパラメータは必須で、二重引用符で囲む必要があります。**Version Control** は、サーバとクライアントのバージョン番号と日付を比較してコンポーネントのバージョンを確認します。クライアントとサーバ間でコンポーネントが同期されていると見なされるためには、バージョン番号と日付の両方が一致している必要があります。また、**checksum** プロパティが有効な場合、ファイルが更新される前にチェックサムの確認が行われます。

control-type

このコンポーネントの **Version Control** のタイプを指定します。
control-type の有効な設定は以下のとおりです。

設定	説明
<code>dir_ctl</code>	コンポーネントがディレクトリを表すことを指定します。ディレクトリへのパスを指定するには、ディレクトリ パラメータを指定する必要があります。ファイル名パラメータを指定して、ディレクトリ内の一連のファイルをフィルタするファイル名パラメータを指定することもできます。UNIX でも Windows でもサブディレクトリはアップグレードされません。
<code>file_ctl</code>	コンポーネントがファイルを表していることを指定します。ファイルへのパスを指定するには、ディレクトリおよびファイル名パラメータを指定する必要があります。
<code>nxenv_ctl</code>	コンポーネントが <code>client_nx.env</code> ファイルを表していることを指定します。このファイルは、内部の CA SDM 環境変数を保存するのに使用されます。 CA SDM Version Control およびオプションマネージャは、このファイルを自動的にメンテナンスします。 <code>nxenv_ctl</code> コンポーネントは 1 つだけで、コンポーネント名は CLIENT_NXENV にする必要があります。
<code>ver_ctl</code>	これが初期設定の Control タイプです。コンポーネントが汎用である（つまり、特定の外部オブジェクトに関連付けられていない）ことを指定します。汎用コンポーネントを使用して、クライアント全体の Version Control 、または自動アップグレードには大きすぎるファイルまたはディレクトリの Version Control を提供することができます。 Control タイプが <code>ver_ctl</code> のコンポーネントはアップグレードできません。サーバが UPGRADE モードのときに <code>ver_ctl</code> コンポーネントのバージョンが一致しないと、クライアントの接続が失敗します。

filename = "ファイル名"

Version Control でのファイルの名前を指定します。ディレクトリの仕様は含まれていません。このパラメータは、**file_ctl** コンポーネントで必須ですが、ディレクトリ (**dir_ctl**) 管理コンポーネントではオプションです。ディレクトリ コンポーネントと共に使用した場合、ファイル名パラメータは **dir_ctl** コンポーネントに関連付けられているファイルを制限するファイルマスクとして機能します。たとえば、**dir_ctl** コンポーネントのファイル名が ***.README** の場合、そのディレクトリでアップグレードされるファイルにはファイル名が「**.README**」で終了しているファイルだけが含まれるようになります。

directory = "ディレクトリ"

dir_ctl コンポーネントのディレクトリへのパスを指定します。または、**file_ctl** コンポーネントのファイルが含まれているディレクトリへのパスを指定します。このパラメータは、**ver_ctl** および **nxenv_ctl** コンポーネントでは無視されます。ディレクトリ パスは、引用符で囲む必要があります。先頭に\$が付いている環境変数への参照を含むことができます。

注: Windows サーバの場合でも、必ずバックスラッシュではなくスラッシュを使用してパス名のサブディレクトリを区切ってください。

link = "リンクディレクトリ"

前述したディレクトリ パラメータと同じ形式で、クライアント上のリンク ディレクトリを指定します。このパラメータは、**file_ctl** および **dir_ctl** コンポーネントではオプションで、**ver_ctl** および **nxenv_ctl** コンポーネントでは無視されます。指定した場合、Linux クライアントがアップグレードされると、ディレクトリ パラメータによって指定されたロケーションにコピーされた実際のファイルを指すシンボリックリンクがリンク ディレクトリに配置されます。**Windows** クライアントがアップグレードされると、リンク ロケーションとディレクトリ ロケーションの両方に実際のファイルがコピーされます。

source = "ソースディレクトリ"

(オプション パラメータ) サーバが配布するファイルを取得可能な、サーバ上の異なるディレクトリを指定します。このパラメータの形式は、前述したディレクトリ パラメータの形式と同じです。このパラメータは、クライアントに配布するファイルが、サーバ上のディレクトリ ロケーションにある同じファイルと異なる場合に役立ちます。このパラメータは、ソースディレクトリからファイルを取得して、それをディレクトリ パラメータによって指定されたクライアント上のロケーションに配布することをサーバに通知するのに使用します。ソース パラメータを指定した場合は、ディレクトリ パラメータを指定する必要があります。

effectivity = "有効性の仕様"

(オプション) クライアントがこのコンポーネントを取得するかどうかを指定します。これにより、一部のクライアントへのダウンロードを除外することができます。クライアントが有効性の仕様に含まれていない場合、クライアントはコンポーネントを取得しません。このパラメータを指定しなかった場合、すべてのクライアントがコンポーネントを受け取ります。有効性の仕様では、以下の記号を使用します。

+(プラス記号)

クライアント グループを追加することを示します。

-(マイナス記号)

クライアント グループを除外することを示します。

有効なクライアント グループは、以下のとおりです。

- SUN4SOL
- AIX
- LINUX
- LINUX390
- HP
- WINDOWS_CLIENTS
- UNIX_CLIENTS

たとえば、以下の仕様は、UNIX クライアントだけがファイルを取得することを示します。

```
effectivity = "+ UNIX_CLIENTS"
```

checksum

クライアント上のコンポーネントのチェックサムがサーバ上の対応するチェックサムと一致しなかった場合に、コンポーネントをアップグレードすることを指示します。ディレクトリに適用した場合、チェックサムは各ファイルに適用されます。

```
min_release = "リリース"および max_release = "リリース"
```

このコンポーネントの配布先にする最も古いクライアントと最も新しいクライアントを指定します。server_default.ver ファイル内のステートメントは、リリースを定義します。これらのパラメータは、以下の形式になっています。Gaxx はリリースを示し、それに続く値はリリースに関連付けられている genlevel です。

```
! Release GA50 50MV000900 50W7T000900
```

```
! Release GA45 45MW000900 50WTT000900
```

順番は、GA50の方がGA45よりも新しいことを示しています。

component_type

使用するコンポーネントのタイプを指定します。以下のタイプのコンポーネントが使用されます。

設定	説明
file	これは初期設定のコンポーネントタイプです。クライアントにコピーしたファイルを、ディレクトリ パラメータで示されているサーバ上のロケーションから直接取得することを指定します。

設定	説明
exe_file	クライアントにコピーするファイルを、クライアントのオペレーティングシステムに依存する以下のサーバ上のロケーションから取得することを指定します。 ■ windows (Windows) ■ sun4Sol (Solaris) ■ hp (HP-UX) ■ aix (AIX) ■ linux (Linux) ■ linux390 (Linux390) これらのサブディレクトリのロケーションは、ディレクトリ パラメータ設定に依存します。このパラメータを設定した場合、サブディレクトリは指定したディレクトリの下に配置されます。それ以外の場合、CA SDM のメインインストール ディレクトリの bin ディレクトリに配置されます。

o_mode = "所有者モード"

ファイルの所有者に対してファイル アクセス許可を指定します。

g_mode = "グループモード"

ファイル所有者のグループに属しているユーザのファイル アクセス許可を指定します (UNIX クライアントでのみ使用されます)。

w_mode = "ワールドモード"

ファイル所有者のグループに属していないユーザのファイル アクセス許可を指定します (UNIX クライアントでのみ使用されます)。

3 つのモード パラメータを使用して、サーバ上で同じ実行可能ファイルの異なるバージョンを管理できます。これらは、クライアントにコピーしたときにファイルのアクセス制御を指定します。これらのパラメータは、アップグレード操作中にだけ使用されます。これらは以下の意味を持つ 1~3 個の文字で構成されます。

設定	説明
R	読み取り
W	書き込み
X	実行

PC クライアントは書き込み許可と実行許可を無視します。

1 つ以上のファイル アクセス モードを任意の組み合わせで指定できます。UNIX クライアントの場合、ファイルには指定したアクセス モードが与えられます。PC クライアントの場合、**w_mode** を指定したかどうかにより、ファイルは書き込み可能または読み取り専用になります。

クライアントでの CA SDM の再起動

クライアント サーバで **CA SDM** を再起動して、カスタマイズでクライアント バージョン管理ファイルを更新します。

注: [スタート] - [設定] - [コントロール パネル] - [管理ツール] - [サービス] を選択します。[CA SDM Server] を右クリックし、[開始] を選択してサーバを再起動または開始します。

次の手順に従ってください:

1. 標準設定では、セカンダリ サーバを再起動します。
2. 高可用性設定では、以下の手順に従います。
 - a. すべてのスタンバイ サーバを再起動します。
 - b. [アクティビティの少ないアプリケーション サーバを選択します](#) (P. 40)。
 - c. アクティビティの少ないアプリケーション サーバを再起動します。
 - d. [ほかのアプリケーション サーバを停止します](#) (P. 41)。
 - e. アプリケーション サーバを起動します。
 - f. ほかのアプリケーション サーバに対して手順 d および e を実行します。

クライアントは、サーバに接続して、管理されているコンポーネントのリストを送信します。サーバは、そのリストとサーバに保存されているマスタ リストを比較します。クライアント上の影響を受けるコンポーネントがアップグレードされます。

アクティビティの少ないアプリケーション サーバの選択

ユーザ アクティビティが最も少ないアプリケーション サーバを選択します。各アプリケーション サーバに対して以下のコマンドを実行し、アクティブなセッションが最少または存在しないサーバを選択します。

```
pdm_webstat
```

注: このコマンドは、SOAP または REST Web サービス セッションをキャプチャしません。

ほかのアプリケーション サーバの停止

アプリケーション サーバを停止する前に、アプリケーション サーバ上のすべてのアクティブなユーザに対して、アクティビティの少ないアプリケーション サーバに移動するように通知します。アクティビティの少ないアプリケーション サーバにすべてのユーザを移動する前に、そのサーバを再起動したことを確認します。

次の手順に従ってください:

1. (推奨) 停止するアプリケーション サーバ上のすべてのアクティブなサポート オートメーション アナリストに対して、そのセッション情報を持つ CA SDM でチケットを作成するように通知します。このプロセスにより、セッション情報が失われないようになります。たとえば、サポート オートメーション アナリストが、ハードウェアの問題を解決するために顧客とセッション中だとします。このような場合、アプリケーション サーバがシャット ダウンする前に、サポート オートメーション アナリストは、そのセッション情報を使用して CA SDM で問題を作成できます。
2. アプリケーション サーバ上のすべてのアクティブなユーザに対して、再起動したアクティビティの少ないアプリケーション サーバに移動するように、通知（電子メール通知など）を送信します。この通知には、更新されたアプリケーション サーバの詳細を含めることができます。

3. アプリケーション サーバ上で、以下のコマンドを実行します。

```
pdm_server_control [-h] -q interval -s server_name
```

-h

ヘルプ ページを表示します。

-q interval -s server_name

ローカルまたはリモート アプリケーション サーバに指定された時間間隔内に休止するよう通知します。この間隔は、サーバがオフラインになるまでの秒数です。**server_name** なしでこのオプションを使用した場合は、ローカルサーバが休止するよう通知されます。このオプションは、バックグラウンドまたはスタンバイサーバには使用できません。

アプリケーション サーバ上のすべてのアクティブなユーザにポップアップメッセージが表示され、サーバのシャットダウンとシャットダウンまでに残された時間が通知されます。ユーザは自分の作業を保存し、その時間内にログアウトする必要があります。アプリケーションサーバは指定された時間の後に停止します。ユーザが自分の作業を再開するには、ほかのアプリケーションサーバにログオンします。サポート オートメーション アナリストはチケットを参照して、それらのユーザの作業を再開できます。

アプリケーション サーバが正常に停止されます。

クライアントでのカスタマイズの確認

カスタマイズがすべて同期されたか確認するために、クライアントのバージョン管理ファイルを確認します。

次の手順に従ってください:

1. CA SDM の設定に応じて、以下のクライアントにログインします。

- 標準: セカンダリ サーバ
- 高可用性: スタンバイ サーバおよびアプリケーション サーバ

2. 以下の場所にある `stdlog` ファイルを開きます。

```
$NX_ROOT¥Log
```

3. サーバで実行したすべてのカスタマイズが、クライアントに適用されているかどうかを確認します。

第 16 章：構成アイテムの管理

このセクションには、以下のトピックが含まれています。

[Web インターフェースの使用](#) (P. 683)
[連絡先、ロケーション、組織 CI](#) (P. 689)
[CI 関係](#) (P. 694)
[バージョン指定](#) (P. 703)
[他の CA 製品での CI 属性の表示](#) (P. 735)
[CMDBf ドライバの使用](#) (P. 736)
[CMDB Visualizer](#) (P. 736)
[検出されたアセットの追加](#) (P. 740)
[アセットフラグと CI フラグ](#) (P. 741)
[CI 調整](#) (P. 743)
[ステージング済みトランザクションの管理](#) (P. 767)
[CA CMDB データ保守](#) (P. 795)
[構成監査および制御機能 \(CACF\)](#) (P. 811)

Web インターフェースの使用

以下の機能を使用すると、現在の役割に応じて構成アイテム (CI) のユーザ タスクと管理タスクを実行できます。

- スコアボードでは、ユーザ タスクの実行と CI および CI 関係の管理が可能です。
- [管理] タブでは、CI と関係に関する管理タスクを実行できます。
- CMDB Visualizer では、CI と関係を視覚化するためのユーザ タスクと管理タスクを実行できます。

関連項目:

[構成アイテムの表示](#) (P. 684)
[構成アイテムの作成](#) (P. 685)
[構成アイテムの更新](#) (P. 686)
[CI と保守ウィンドウの関連付け](#) (P. 687)
[関連付けられた変更ウィンドウの表示](#) (P. 687)
[構成アイテムの履歴表示](#) (P. 688)
[構成アイテムの非アクティブ化](#) (P. 688)
[構成アイテムの再アクティブ化](#) (P. 689)

構成アイテムの表示

スコアボードを使用して、構成アイテムをオープンし、構成アイテムに関する情報を表示できます。

構成アイテムをオープンして表示するには、以下の手順に従います。

1. スコアボードで、[検索] - [構成アイテム] をクリックします。
[構成アイテムの検索] ペインが表示されます。
2. 検索基準を入力し、[検索] をクリックします。
構成アイテムリストが表示され、検索結果が一覧表示されます。
3. (オプション) 名前列の構成アイテムをクリックすることでも、構成アイテムをオープンして詳細情報を表示できます。
[構成アイテム詳細] が表示されます。

注: CI を作成した後で、ID 属性が空白 (値がない) の場合は、構成アイテムの詳細ページに表示されないものがあり、CI ファミリに適用されません。ただし、空白以外の値の ID 属性は常に表示されます。

構成アイテムの作成

スコアボードを使用して、構成アイテムを作成できます。

構成アイテムを作成するには、以下の手順に従います。

1. スコアボードで、[ファイル] - [新規構成アイテム] をクリックします。

[構成アイテムの新規作成] ページが表示されます。

2. [名前] フィールドに構成アイテムの固有の名前を入力します。
3. [クラス] フィールドに構成アイテムのクラスを入力するか、フィールドの上にある[検索]アイコンをクリックしてクラスを指定します。
4. 新規構成アイテムに適用する残りのフィールドをすべて指定します。

注: 構成アイテムの作成に必須のフィールドは、[名前] と [クラス] のみです。

5. [継続] をクリックします。

[構成アイテムの新規作成] ページに追加のタブとフィールドが表示されます。

6. 必要に応じて、[属性] タブの適切なフィールドにデータを入力します。

タブに表示される属性は、構成アイテムに設定したクラスのファミリーによって異なります。ここで入力する内容は、ビジネス プロセスや、格納および表示する必要がある構成アイテムの情報によって異なります。

7. [保存] をクリックします。

構成アイテムの作成を確認するメッセージが表示されます。

構成アイテムの更新

スコアボードを使用して、構成アイテムを変更できます。

構成アイテムを変更するには、以下の手順に従います。

1. スコアボードで、構成アイテムを指定してオープンします。
[構成アイテムの詳細] ページが表示されます。
2. [編集] をクリックします。
[構成アイテムの更新] ページが表示されます。
3. このページの該当するタブを選択してフィールドに新しいデータを入力し、構成アイテムの情報を更新します。[保存] をクリックします。
構成アイテムの変更を確認するメッセージが表示されます。

注: - a オプションを使用することにより CI が更新される場合には常に、属性が変更されない場合にも、構成アイテム リストに表示されている CI の最終変更日付およびユーザが更新されます。この更新は、CI がユーザ インターフェースで編集された（そして変更なしで保存された）か、または GRLoader を使用して更新された場合に、行われます。

CI と保守ウィンドウの関連付け

CI への保守アクセスを管理するため、CI を 1 つ以上の非グローバル保守ウィンドウに関連付けることができます。

CI と保守ウィンドウを関連付けるには、以下の手順に従います。

1. [構成アイテムの詳細] ページに移動します。
2. [保守ウィンドウ] タブをクリックします。
[保守ウィンドウ リスト] が表示されます。
3. [保守ウィンドウの更新] をクリックします。
[保守ウィンドウの検索] ページが表示されます。
4. 必要な保守ウィンドウの情報を指定します。
5. [検索] をクリックします。
[使用可能なウィンドウ] ページが表示されます。
6. [使用可能な変更ウィンドウ] リスト内の任意の必要なウィンドウを、
[関連付けられた変更ウィンドウ] リストに移動させます。
7. [OK] をクリックします。

CI、変更ウィンドウ、および新しいウィンドウの関連付けが保存されます。

関連付けられた変更ウィンドウの表示

特定の期間中に CI がどの程度影響を受けるかを判断するために、その CI に関連付けられた保守ウィンドウを表示できます。

CI に関連付けられた変更ウィンドウを表示するには、以下の手順に従います。

1. [構成アイテムの詳細] ページに移動します。
2. [保守ウィンドウ] タブをクリックします。
関連付けられた保守ウィンドウが表示されます。

構成アイテムの履歴表示

構成アイテムの履歴を表示できます。

構成アイテムの履歴を表示する方法

1. 構成アイテムを検索して開きます。
[構成アイテムの詳細] ページが表示されます。
2. [バージョン指定] タブをクリックします。
[バージョン指定] ページが表示されます。
3. [ログの表示] をクリックします。

構成アイテムの履歴が一覧表示されます。

注: [ログの表示] は左側のペインで選択されているものを無視します。

構成アイテムの非アクティブ化

使用しない構成アイテムが発生した場合、構成アイテムの詳細を編集して、構成アイテムを非アクティブにできます。ステータスが非アクティブになると、その構成アイテムはスコアボードの [構成アイテム リスト] から削除されます。構成アイテムは削除できません。

注: ファミリやクラスの非アクティブ化は、ファミリやクラスに属する既存の CI に影響を及ぼしません。そのファミリやクラスに CI を新規に作成できなくなるだけです。

構成アイテムを非アクティブにするには、以下の手順に従います。

1. 構成アイテムを検索して開きます。
[構成アイテムの詳細] ページが表示されます。
2. [編集] をクリックします。
[構成アイテムの更新] ページが表示されます。

3. [アクティブ] ドロップダウン リストから [アクティブ] を選択します。 [保存] をクリックします。

ステータスの変更を確認するメッセージが表示されます。アクティブ構成アイテムのリストに、非アクティブにした構成アイテムが表示されなくなります。関係が非アクティブにされるまでは、構成アイテムは既存の関係内に表示され続けます。

構成アイテムの再アクティブ化

非アクティブにした構成アイテムが必要になった場合、構成アイテムを再びアクティブにできます。

構成アイテムを再アクティブ化するには、以下の手順に従います。

1. 構成アイテムを検索して開きます。
[構成アイテムの詳細] ページが表示されます。
2. [編集] をクリックします。
[構成アイテムの更新] ページが表示されます。
3. [アクティブ] ドロップダウン リストから [アクティブ] を選択します。 [保存] をクリックします。

ステータスの変更を確認するメッセージが表示されます。アクティブ構成アイテムのリストに、再アクティブ化した構成アイテムが表示されます。

連絡先、ロケーション、組織 CI

CA CMDB のインストールでは、ベース オブジェクトの連絡先、ロケーション、組織に対して CI を定義できます。これらの CI はそれに従い管理することが可能で、必要に応じて別の CI との関係を確立することができます。カスタマによっては、ベース オブジェクトを CI 属性としてのみ採用するよりもこのアプローチのほうが、適切に環境設定管理プロセスをサポートします。

関連項目:

[ベース オブジェクトからの CI の作成 \(P. 690\)](#)

[CI のベース オブジェクトの選択 \(P. 691\)](#)

[ベース オブジェクトの CI の詳細の編集 \(P. 691\)](#)

[ベース オブジェクトの CI 属性の編集 \(P. 692\)](#)

[GRLoader を使用したベース オブジェクト CI の作成 \(P. 693\)](#)

ベース オブジェクトからの CI の作成

スコアボードを使用して、ベース オブジェクトから構成アイテムを作成できます。

ベース オブジェクトから構成アイテムを作成するには、以下の手順に従います。

1. [ファイル] - [新規構成アイテム] を選択します。
[構成アイテムの新規作成] ページが表示されます。
2. CI フィールドを入力します。[名前] と [クラス] は必須です。[継続] をクリックします。

注: ホスト名、シリアル番号、MAC アドレス、および DNS 名などの一般的な CI 属性は、ベース オブジェクトの CI には該当しません。
[構成アイテムの新規作成] ページが表示されます。
3. この CI が示すオブジェクトを定義するために、ベース オブジェクトのリンクをクリックします。
4. オブジェクトを選択します。既存のオブジェクトを検索するか、[新規作成] をクリックしてオブジェクトを作成します。オブジェクトを作成する場合は、[保存] をクリックして次へ進みます。
選択したオブジェクトが [構成アイテム詳細] ページのトップに表示されます。
5. [保存] をクリックします。
選択したオブジェクトの主要な属性が、[構成アイテムの詳細] ページの [属性] タブに表示されます。

CI のベース オブジェクトの選択

構成アイテムのベース オブジェクトを選択できます。

CI のベース オブジェクトを選択するには、以下の手順に従います。

1. ベース オブジェクトのファミリー（連絡先、ロケーション、または組織）に属する CI を選択します。

[構成アイテムの詳細] ページが表示されます。

2. [編集] をクリックします。

[構成アイテムの更新] ページが表示されます。

3. トップセクションで、ベース オブジェクトに必須のフィールドを入力します。値を直接入力するか、虫メガネのアイコンをクリックしてオブジェクトを検索します。たとえば、連絡先を検索するには、[連絡先の検索] ウィンドウで1つ以上の検索フィールドを入力し、[検索] をクリックします。表示されたリストの中から連絡先を選択します。

4. [保存] をクリックします。

選択したオブジェクトが、同じファミリーの別の CI によってすでに示されている場合は、エラー メッセージが表示されます。別のオブジェクトを選択すると、CI を変更できます。

ベース オブジェクトの CI の詳細の編集

CI が示すベース オブジェクトの属性（代替 CI ID や注意事項など）は、ほかの [構成アイテム詳細] ウィンドウでの操作と同様の方法で編集できます。

CI が示すベース オブジェクトの属性を編集するには、以下の手順に従います。

1. ベース オブジェクトのファミリーに属する CI を選択します。

[構成アイテムの詳細] ページが表示されます。

2. ページのトップにあるオブジェクトのリンクをクリックします。

オブジェクトの [詳細] ページが表示されます。

3. [編集] をクリックします。
オブジェクトの [更新] ページが表示されます。
4. 必要に応じてフィールドを編集して、[保存] をクリックします。
[更新] ページが閉じます。
[構成アイテムの詳細] ページの [属性] タブに表示される属性の 1 つを変更している場合は、ページが更新された後にその変更内容が表示されます。

ベース オブジェクトの CI 属性の編集

ベース オブジェクトの構成アイテムの属性を編集できます。

CI の属性を編集するには、以下の手順に従います。

1. オブジェクトのファミリ（連絡先、ロケーション、または組織）に属する CI を選択します
[構成アイテムの詳細] ページが表示されます。
2. [編集] をクリックします。
[構成アイテムの更新] ページが表示されます。
3. [属性] タブで [編集] をクリックします。
[更新] ページが表示されます。
4. 必要に応じてフィールドを編集して、[保存] をクリックします。
[更新] ページが閉じます。
5. [保存] をクリックします。
[構成アイテム詳細] ページに変更した CI が表示されます。

GRLoader を使用したベース オブジェクト CI の作成

GRLoader を使用して、既存のベース オブジェクトからベース オブジェクト CI を作成できます。

GRLoader を使用して既存のベース オブジェクトからベース オブジェクト CI を作成する方法

1. 以下を指定する XML を作成します。

- CI 名
- ファミリ
- クラス

2. XML をサブミットします。

ベース オブジェクトが作成され、GRLoader に、CI が 1 つ読み込まれて挿入されたことが表示されます。

例: 既存の連絡先から CI を作成

以下は、既存の連絡先 **Gibbs, Keith** から CI を作成する例です。

```
<GRLoader>
<ci>
  <name>Gibbs, Keith</name>
  <family>連絡先</family>
  <class>技術職</class>
  <base_contact>Gibbs, Keith</base_contact>
</ci>
</GRLoader>
```

CI 関係

CA SDM の機能は、構成アイテム間の関係によって変わります。CI 関係には以下の特徴があります。

- 関係タイプは、2つの構成アイテムがどのような関係にあるかを定義します。
- 階層関係タイプは、プロバイダ/従属のペアとして定義します。たとえば、A（プロバイダ）はBをホストします（*hosts*）。B（従属）はAにホストされます（*is hosted by*）。
- 非階層関係タイプは、ピアツーピアとして定義します。たとえば「接続する」の場合、どちらの側も同等です。

[CMDB 関係] タブを使用して、以下の関係機能を実行できます。

- [アクティブ] フィールドで検索し、アクティブまたは非アクティブな関係を表示する。表示されます。
- [構成アイテムの関係リスト] で関係のリンクをクリックし、[構成アイテムの関係の詳細] ページを表示する。

関連項目:

[構成アイテム関係タイプ](#) (P. 695)

[関係タイプの作成](#) (P. 695)

[構成アイテム関係の管理](#) (P. 696)

[構成アイテム関係の作成](#) (P. 697)

[CI 間の関係の表示](#) (P. 697)

[CI 関係の非アクティブ化](#) (P. 698)

[CI 関係の再アクティブ化](#) (P. 698)

[CI 関係の非アクティブ化（リスト内で編集）](#) (P. 699)

[GRLoader を使用した CI 関係の非アクティブ化](#) (P. 700)

[GRLoader を使用した CI 関係の復活](#) (P. 701)

[データベースからの CI 関係の削除](#) (P. 702)

[CI 関係履歴および比較](#) (P. 702)

構成アイテム関係タイプ

CA SDM では、構成アイテム間の関係、つまり両者の関連付けを表現する、事前定義済み関係タイプのリストを利用できます。関係タイプの表現内容は、フォーカスになっている構成アイテムによって変わります。たとえば、プロバイダ CI は従属 CI をサポートします（関係タイプは「サポートする」）が、この従属 CI はプロバイダ CI によってサポートされています（関係タイプは「サポートされる」）。同一の関係を表す表現は複数あり、表示される関係タイプラベルは、関係が「プロバイダ>従属」であるか「従属>プロバイダ」であるかによって変わります。

注: CA CMDB が提供する関係タイプの詳細については、「[CA CMDB テクニカル リファレンス](#)」を参照してください。

関係タイプの作成

関係タイプを作成し、関係を作成または更新する際に使用できます。

関係タイプを作成する方法

1. [管理] タブの左側のペインで、CA CMDB フォルダを展開します。
2. [構成アイテム関係タイプ] をクリックします。
[構成アイテム関係タイプ リスト] が右側のペインに表示されます。
3. [新規作成] をクリックします。
[構成アイテム関係タイプの新規作成] ページが表示されます。
4. 以下のフィールドを指定します。

「プロバイダ>従属」ラベル

プロバイダから従属への関係を表し、関係タイプのリストに表示される名前です。たとえば、「サービス」または「管理する」は、「プロバイダ>従属」関係です。

「従属>プロバイダ」ラベル

従属からプロバイダへの関係を表し、関係タイプのリストに表示される名前です。たとえば、「サービスを提供される」または「管理される」は、「従属>プロバイダ」関係です。

ピアツーピア

プロバイダ CI および従属 CI が存在せず、代わりに 2 つの同等な CI で構成される関係を指定します。たとえば、「接続する」「フェールオーバーする」は、ピアツーピア関係です。

アクティブ

関係タイプをリストに表示し、構成アイテム関係で選択できるようにします。

5. [保存] をクリックします。

関係タイプが作成され、関係を作成または更新するときに利用できるようになります。

構成アイテム関係の管理

[構成アイテムの関係] ページには、必要な設定が 1 か所にすべて揃っており、構成アイテム関係のプロセスが簡略化されます。

このページを使用して、以下のタスクを実行できます。

- 2 つの構成アイテム間のプロバイダ/従属関係を切り替えます。

[反転] をクリックすると、関係のプロバイダ構成アイテムと従属構成アイテムが切り替わります。これにより、フォーカス CI が変わります。逆の関係が有効でない場合、[反転] をクリックすると、[関係] フィールドがクリアされます。
- [シンボル]、[説明]、[コスト] などの省略可能フィールドを設定します。

[省略可] をクリックして、オプションのフィールドを設定します。

シンボルが指定されていない場合は、関係が作成される際に、**cmdb**
bmhier: というプレフィクスと一意の番号が付けられた一意のシンボルが自動的に作成されます。

注: ユーザのインストールが CA Network および Systems Management (CA NSM) に統合される場合、CA NSM リポジトリおよびコストを指定するように促されます。

構成アイテム関係の作成

フォーカスのある構成アイテムから CI 関係を追加できます。

フォーカス CI から関係を追加する方法

1. 関係を追加する CI を選択します。
[CI の詳細] ページが表示されます。
2. [編集] をクリックします。
[CI の更新] ページが表示されます。
3. [CMDDB 関係] - [新規作成] をクリックします。
[Create CI Relationship] ページが表示されます。
4. プロバイダ CI を指定します。虫眼鏡のリンクをクリックすると、CI を検索できます。
注: 目的の関係に応じて、[反転] をクリックしてプロバイダ/従属の位置を切り替えることができます。
5. [関係タイプ] を指定します。虫眼鏡のリンクをクリックすると、関係タイプを検索できます。
6. 別の CI を指定します（デフォルトは、従属 CI）。虫メガネのアイコンをクリックすると、CI を検索できます。
7. [保存] をクリックします。
関係が作成されます。

CI 間の関係の表示

CI 間の関係を表示できます。

CI 間の関係を表示する方法

1. 構成アイテムに移動します。
[構成アイテムの詳細] ページが表示されます。
2. [CMDDB 関係] タブを選択します。
CI 間の関係のリストが表示されます。

CI 関係の非アクティブ化

CI 関係のステータスを非アクティブに設定して、CI 関係を非アクティブ化できます。

関係を非アクティブ化する方法

1. [構成アイテムの詳細] ページに移動し、[CMDB 関係] - [編集] をクリックします。

編集モードで [CMDB 関係] タブが表示されます。

2. 関係を選択し、その行のリンクをクリックします。
[構成アイテム関係の詳細] ページが表示されます。

3. [編集] をクリックします。

4. [アクティブ] 属性を [非アクティブ] に設定します。[保存] をクリックします。

関係が非アクティブになります。[構成アイテム関係の詳細] ページの [アクティブ] 属性には、非アクティブ属性の値が表示されます。

CI 関係の再アクティブ化

削除された CI 関係を再アクティブ化できます。

削除された CI 関係を再アクティブ化する方法

1. [構成アイテムの詳細] ページに移動します。
[構成アイテムの詳細] ページが読み取り専用モードで表示されます。
2. [編集] をクリックします。
[構成アイテムの詳細] ページが編集モードで表示されます。
3. [CMDB 関係] タブをクリックします。
4. 任意の行でリンクをクリックすると、[構成アイテム関係の詳細] ページが表示されます。

5. [編集] をクリックします。
[構成アイテム関係の更新] ページが表示されます。
6. [アクティブ] 属性を [アクティブ] に変更します。[保存] をクリックします。
関係が再アクティブ化されます。

CI 関係の非アクティブ化(リスト内で編集)

[リスト内で編集] 機能を使用して、1 つ以上の CI 関係を非アクティブ化できます。

1 つ以上の CI 関係を非アクティブ化する方法

1. [管理] タブの左側のペインで、CA CMDB フォルダを開きます。
CA CMDB ノードを展開して、サブフォルダを表示します。
2. [構成アイテムの関係リスト] フォルダをクリックします。
3. (オプション) 検索フィルタを指定します。
4. [検索] をクリックします。
CI 間の関係が右側のペインに表示されます。
注: 初期設定では、すべての関係が表示されます。
5. リストの右上にある [リスト内で編集] をクリックします。
[Relationship Edit in List] コントロールが表示されます。
6. 変更する関係が含まれている行を選択します。
選択した行が表示され、各コントロールに該当する関係の値が入力されます。
7. [アクティブ] 属性を [非アクティブ] に設定します。
ハイライトされた関係のみを非アクティブ化する場合は、[保存] をクリックします。フィルタ検索で絞り込んだ関係をすべて非アクティブ化する場合は、[すべて変更] をクリックします。

GRLoader を使用した CI 関係の非アクティブ化

GRLoader を使用して XML をサブミットし、CI 関係を非アクティブ化できます。

GRLoader を使用して関係を非アクティブ化する方法

1. 関係タグを使用して以下を指定する XML を作成します。
 - プロバイダ構成アイテム
 - 従属構成アイテム
 - 関係タイプ
2. `delete_flag` を `true` に設定します（あるいは、`yes` または `1`）。
3. XML をサブミットします。
CI 関係が削除されます。

注: GRLoader の詳細については、CA CMDB の「テクニカル リファレンス ガイド」を参照してください。

例: GRLoader を使用した CI 関係の削除

以下の XML の例では、`ci_1` と `ci_2` 間の「接続する」という関係を削除します。

```
<GRLoader>
  <relation>
    <dependent>
      <name>ci_2</name>
    </dependent>
    <type>connects to</type>
    <provider>
      <name>ci_1</name>
    </provider>
    <delete_flag>true</delete_flag>
  </relation>
</GRLoader>
```


GRLoader を使用した CI 関係の復活

XML をサブミットするため、GRLoader を使用して CI 関係を復活できます。

GRLoader を使用して、CI 関係を復活するには、以下の手順に従います。

1. 以下を識別するために、関係タグを使用する XML を記述します。
 - 関係タイプ
 - 従属構成アイテム
 - プロバイダ構成アイテム
2. delete_flag を false（または、no か 0）に設定します。
3. XML をサブミットします。

CI Relationship が復活されます。

注: GRLoader の詳細については、「CA CMDB テクニカル リファレンス ガイド」を参照してください。

例: CI Relationship の復活

以下の XML の例では、ci_1 と ci_2 間の「接続する」という関係を復活させます。

```
<GRLoader>
  <relation>
    <dependent>
      <name>ci_2</name>
    </dependent>
    <type>connects to</type>
    <provider>
      <name>ci_1</name>
    </provider>
    <delete_flag>false</delete_flag>
  </relation>
</GRLoader>
```

データベースからの CI 関係の削除

CI の関係を削除することによって、非アクティブにするだけでなく、データベースから永久に削除することができます。

データベースから関係を削除する方法

1. [CI 関係リスト] に移動します。
CI 関係リストが表示されます。
2. 任意の関係行を右クリックし、[削除] を選択します。
関係はデータベースから削除されます。

重要: 削除された関係にシンボルが定義されている場合、同じシンボルのすべての関係がデータベースから削除されます。

CI 関係履歴および比較

[バージョン指定] タブには CI 関係が表示されます。このタブを使用すると、以下の操作を実行できます。

- CMDDB 内の任意の CI 用の関係履歴を表示します。関係への変更は、関係が作成、更新、削除されるときに、自動的にログに記録されます。CI の現在および過去の履歴関係をすべて表示できます。
注意: 以前のバージョンの CA CMDDB で作成された関係は、監査履歴情報を持ちません。
- すべてのスナップショットまたはマイルストーンの関係を比較します。

バージョン指定

バージョン指定は、CMDB の権限が与えられた状態を構成するすべての CI のライフ サイクルを追跡し管理することにより、IT インフラストラクチャを制御しやすくします。バージョン指定は、オブジェクトの履歴の監査にも適用されます。バージョン管理は、IT インフラストラクチャをコントロールする以下の機能を提供します。

スナップショット

CI を更新した場合など、オブジェクトへの任意の更新の値に加えた変更に対して自動的に記録されます。バージョン指定によって、コンピュータのメモリ サイズが変更された後のハードウェア CI の完全な状態を記録したスナップショットが作成されます。バージョン指定ではスナップショットを表示することができます。どの CI 属性が変更されたかを示すこともできます。また、バージョン指定では、その CI のほかのすべてのスナップショットの履歴と比較することもできます。この重要な情報は、CI の可用性やパフォーマンスに対する変更の影響を考慮する場合に必要になります。

マイルストーン

実稼働の最初の日や 1 月のベースラインなどの、ユーザが定義したラベルを含む特殊な用途のスナップショットとして記録されます。このようなラベルを使用すると、特定のスナップショットをより簡単に検索できます。

重要：マイルストーンは、変更仕様、検証ポリシー、管理対象変更状態、および管理対象属性には適用されません。

比較

CI を標準として働く別の CI と比較します。どの CI も比較のための標準として使用できますが、特定の CI を **標準 CI** として動作させる目的専用とすることをお勧めします。標準 CI を使用することで、同じファミリー内の別の運用 CI の比較対象となる標準構成を定義することができます。たとえば、組織は **Server Large** を標準 CI として定義し、このサーバのタイプを定義する属性値を定義することができます。あるファミリーの標準 CI はそのファミリー内の運用 CI の属性となることができ、それを使用して CI の現在の状態または状態の履歴を、関連する標準構成と比較することができます。他の比較のように、この情報を印刷するか、またはカンマ区切りのファイルとしてそれをエクスポートできます。

マイルストーンが共有されない、変更不可能なベースラインとして動作できるのに対し、標準 CI は CI 向けの共有、動的ベースラインを提供します。

重要: 標準 CI は、CI 調整に使用されるあらゆる属性に対する値を含んではなりません。

変更仕様

ユーザが CI に対する変更要求に指定した、スケジュール済みまたはスケジュールされていない保留中の変更仕様を表示します。変更仕様は CI の現在の状態と比較できます。たとえば、計画値を CI の現在の状態と比較します。この比較では、変更との競合を示したり、スケジュール内の重複した変更を識別したりすることができます。

バージョン指定を使用すると、以下のタスクを実行できます。

- すべての CI 変更の自動キャプチャ
- 日付または属性変更に基づく任意の時点での CI のスナップショット
- 詳細なログ、基本ビューおよび高度なビューなどのさまざまなレベルでの表示
- その他のスナップショット、CI に対してユーザが定義したマイルストーン、または標準 CI との複数属性の比較
- CA SDM の変更チケットが状態を変更するたびに自動的に作成されるスナップショット

注: この自動スナップショットは、変更仕様、検証ポリシー、管理対象変更状態、および管理対象属性には適用されません。

- 詳細なフィルタリングと印刷および CSV エクスポート サポートとの比較

関連項目：

[バージョン指定の用途](#) (P. 705)
[共有アセットと CI 監査証跡レコード](#) (P. 706)
[バージョン指定の用語](#) (P. 706)
[バージョン指定データのソース](#) (P. 710)
[CA SDM 変更管理統合](#) (P. 711)
[CA APM 統合](#) (P. 713)
[CI バージョン指定管理](#) (P. 714)
[CA SDM 変更管理](#) (P. 734)
[構成監査および制御機能 \(CACF\)](#) (P. 811)
[CI バージョン指定および将来の状態](#) (P. 838)

バージョン指定の用途

バージョン管理には以下の使用方法があります。

問題の判別

CI に関する問題を修正するには、CI の環境内で何が変更されたかを理解する必要があります。バージョン指定では、現在の障害状態と、過去の任意の時点での状態が示されます。これにより、この 2 つの状態を比較して、考えられる問題を特定できます。

パフォーマンス計画およびキャパシティ計画の立案

パフォーマンス計画やキャパシティ計画の担当者は、CI の履歴を洗い直すことによって、パフォーマンスの障害の特定や、将来のシステム拡張計画を、いっそう効果的に行えます。

コンプライアンス

CI の状態を、そのファミリの標準 CI と比較できます。変更管理ライフサイクル内の任意の時点での状態を比較して、CI が標準に準拠していることを確認したり、修正が必要な属性を特定したりするのに役立ちます。

変更検証

どのユーザーが検証ポリシーを変更したか、リクエストの日付、ユーザーが変更した属性や値などの、オブジェクトの監査履歴を表示できます。特定の日付間の変更を比較対照することができます。

共有アセットとCI 監査証跡レコード

バージョン指定機能には、CA APM に加えられた変更の監査証跡が含まれます。バージョン指定機能は、各 CA APM の変更に関連付けられた属性ログ エントリから直接行う、CA CMDB から CA APM へのコンテキスト内起動もサポートしています。CA APM 監査証跡情報は、CA APM 監査ロギングが有効な CA CMDB ファミリの CI/アセットでのみ利用できます。

CA APM 監査証跡情報を含む [バージョン指定] タブは、ロギングが有効化されているすべてのファミリをサポートします。

デフォルトでは、CA APM はアセット属性の変更をログに記録しません。CA APM で管理された CI/アセットで CA CMDB バージョン指定を使用するには、ロギングが必要なアセット属性ごとに [監査証跡データの保存] オプションを有効にする必要があります。

注: 監査を有効にする方法の詳細については、CA APM のマニュアルを参照してください。

アセットの属性が CA APM で変更されると、キャッシュ アクティビティが原因で、[属性] タブのデータの前に CI の詳細ページの [バージョン指定] タブのデータが更新される場合があります。値を再同期するには、[編集] ボタンをクリックしてください。

バージョン指定の用語

バージョン指定は、サービス トランジションの可視化と追跡を提供します。バージョン指定は一般的に、命名規則を使用して、サービス トランジションの日付、順序、および意味を識別します。この記録を使用して、構成アイテム (CI) の特定の状態の識別および比較ができます。

例: バージョンの比較

給与アプリケーション CI の場合、バージョン 3 をバージョン 2 と比較すれば、拡張機能などの新バージョンの変更点を把握できます。

関連項目：

[状態](#) (P. 707)

[バージョン](#) (P. 707)

[スナップショット](#) (P. 707)

[カテゴリ](#) (P. 708)

[マイルストーン](#) (P. 709)

[標準 CI](#) (P. 709)

状態

バージョン指定のコンテキストでは、CI の「状態」は、ある一時点での CI のすべての属性値を表します。CI の状態は、複数の MDR から返される属性変更の結果になることもあります。

バージョン

バージョンは、製品の分解構造や構成構造内の CI などの、識別されるオブジェクトのインスタンスです。バージョンは、変更履歴のトラッキングや監査に使用します。

スナップショット

スナップショットは、ある一時点のオブジェクトの状態を完全に記録したものです。たとえば、標準的な CI には、関連付けられたスナップショットが多数あります。スナップショットでは、オブジェクトに発生したすべての変更イベントを 1 分間隔で集約します。たとえば、CI を 1 分の間に複数回更新（編集および保存）した場合、CA SDM によって、その 1 分間の更新をすべてキャプチャしたスナップショットが 1 つ作成されます。

「スナップショット」は、時間と日付をベースにしたスナップショットを指しており、「マイルストーン」や「標準 CI」と同様、一般的な用語です。有用性の高い時点を見つけやすいように、CA SDM では、スナップショットに意味のあるラベルを付けることができます。ラベルを付けたスナップショットを、マイルストーンと呼びます。

オブジェクトが変更されるたびに、CA SDM によってスナップショットが自動的に作成されるため、手動の操作は必要ありません。バージョン指定では、オブジェクトへのすべての変更をキャプチャします。たとえば、ユーザ インターフェースを使用して作成されたスナップショットや、MDR で生成され、GRLoader または CA CMDB の Web サービスから CMDB に送信されたスナップショットがあります。

カテゴリ

「カテゴリ」は、属性のクラスを分類するものです。カテゴリは主に、属性を表示するタブの名前になっています。

注: タブ名に見られないアイテム（たとえば、名前、シリアル番号、アクティブ フラグなど）は、タブ名でないカテゴリに割り当てられています。

例: タブとカテゴリ

以下の例では、カテゴリがどのようにタブに対応しているかを示しています。

- 「ディスク容量」は「属性」タブに表示されるので、カテゴリは「属性」です。
- 「IP アドレス」は「在庫」タブに表示されるので、カテゴリは「在庫」です。
- 「マイルストーン」は「一般」カテゴリに表示されます。
- 「標準 CI」は「分類」カテゴリに表示されます。
- 「関係」は「関係」カテゴリに表示されます。

マイルストーン

「マイルストーン」は、イベント、論理的なブレイクポイント、または蓄積した変更群に目印を付けるために、必要に応じて作成するラベル付きの CI スナップショットです。マイルストーンには、スナップショットが作成された時点の CI の実際の状態が含まれます。マイルストーンを使用すると、CI の履歴上の重要な時点をすばやく識別し、移動することができます。マイルストーンの作成は、「日付」スナップショットの作成に相当します。

マイルストーンは CI 特有のもので、共有はできません。サービスなどの上位レベルのオブジェクトにマイルストーンを作成する場合、そのオブジェクトのサブコンポーネントにはマイルストーンは自動作成されません。複数のサブコンポーネントから構成されているオブジェクトにマイルストーンを作成する場合は、複数の従属マイルストーンを作成できます。

マイルストーンは静的で、変更および削除はできません。ユーザがマイルストーンを作成する場合、スナップショットは CI の現在の状態で作成されます。後で表示されたり比較に使用されたりする場合、マイルストーンは常に過去の一時点を参照します。適切なマイルストーンの命名規則を使用すると、CI ライフサイクルの重要な時点の識別に役立ちます。

重要：マイルストーンは、変更仕様、検証ポリシー、管理対象変更状態、および管理対象属性には適用されません。

標準 CI

「標準 CI」は、ある CI ファミリを概念化した構成で、同一ファミリ内に「実在する」CI インスタンスとのベースライン比較に使用します。標準 CI は、現実のものを示しているという意味で実在する CI である場合もあれば、比較の目的でのみ存在する場合があります。標準 CI には、以下の関連付けがあります。

- 標準 CI は、複数の CI で共有できます。
- 1 つの CI が持てる標準 CI は、常にその CI と関連付けられた標準 CI 1 つだけです。標準 CI が変更された場合、その変更は、標準 CI と関連付けられた CI との比較に反映されます。
- 1 つのファミリに、複数の標準 CI があります。たとえば、あるファミリには、「標準テストサーバ」、「標準実稼働サーバ」、「標準受け入れサーバ」という名前の標準 CI があります。検索するときに標準 CI であることが識別しやすいように名前を付けることをお勧めします。

標準 CI は、それ自体が CI であるため、管理が可能です。ほかの CI 同様、監査証跡、セキュリティ、変更履歴などを持ちます。特定の CI に対して標準 CI を定義した後、標準 CI を使用して、企業標準に準拠しているかどうかを検証できます。

「日付」や「時刻」という概念は、標準 CI とスナップショットやマイルストーンを比較するときには適用されません。比較の目的で使用されるのは標準 CI の属性値だけで、標準 CI 固有のスナップショットやマイルストーンは適用されません。

例: 標準 CI の利用

会社が、ある「従業員ワークステーション」構成を標準 CI として定義し、**Hardware.Workstation** ファミリの実際のデスクトップ コンピュータと比較したとします。この比較によって、標準 CI のメモリの値が **2 GB** であるのに、あるコンピュータには **1 GB** の RAM しか搭載されていないことが明らかになります。

バージョン指定データのソース

監査ログ機能をサポートする任意のコンポーネントでオブジェクトを作成したり変更したりするたびに、バージョン指定データが生成されます。スナップショットは複数のソースから個別に生成されます。各スナップショットは区別が付きません。環境が適切に設定されていれば、CI および CI 間の関係が変更されるたびに、スナップショットが自動的に生成されます。

すべての **CA CMDB** ファミリでバージョン指定を利用できます。**CA Service Desk** ベースのファミリに属する CI は、バージョン指定を利用できるように、**CA CMDB** のファミリに変換する必要があります。

バージョン指定データには、以下のソースがあります。

- **CA CMDB の CI 更新** - ユーザ インターフェースからの共通 CI 属性およびファミリ固有 CI 属性の更新。
- **CA CMDB 関係の更新** - [編集] 機能および [リスト内で編集] 機能を使用して、[関連付け] タブおよび [CI Relationship List] の関係を更新した場合です。

- **GRLoader** GRLoader を使用した、CI の挿入と、属性更新、関係更新、標準 CI 割り当ておよびマイルストーンのインポート。GRLoader を使用して MDR から更新を送信した場合、MDR ソースも記録され、ソースから直接、属性の変更を追跡できます。

注: 詳細については、「テクニカル リファレンス ガイド」を参照してください。

- **CA SDM の変更履歴** - 変更チケットと関連付けられたすべての CI のスナップショットが自動的に生成されます。CI がオープン、クローズ、アクティブ、解決済みになるときに、スナップショットが最高 4 つまで記録されます。
- **CA Asset Portfolio Management (CA APM) の CI 変更** - ロギングが有効になった CA APM による CI の変更。
- **変更検証** - 変更仕様、検証ポリシー、管理対象変更状態、および管理対象属性への更新。

注: CA SDM または以前の CA CMDB リリースで作成した CI の場合は変更のみが含まれます。名前、ファミリー、クラスなどの初期属性値は記録されず、スナップショットにも表示されません。また、CA Service Desk または以前のバージョンの CA CMDB で作成された関係の場合は、監査履歴情報がありません。

CA SDM 変更管理統合

バージョン指定データは、CA SDM 変更チケットと関連付けられた CI に対して生成します。変更チケットがオープンからアクティブ、解決済み、クローズへと移るたびに、関連付けられた CI のスナップショットが記録されます。したがって、CI がオープン、クローズ、アクティブ、解決済みになるときに、スナップショットが作成されます。変更要求と関連付けられた CI がない場合、スナップショットは記録されません。

注: バージョン指定機能に特別な設定は不要で、統合インストールで自動的にサポートされます。

バージョン指定機能は、以下のように変更チケットを処理します。

1. CI の状態を、チケットがオープンになった時点と現時点とで比較します。
2. 要求されたすべての変更が適切に実行され、不要な変更が発生していないかを検証します。
3. 変更が確認されると、チケットはクローズになります。

監査プロセスの場合は、変更前と変更後の CI の状態を容易に比較できます。この比較情報によって、以下に示すような変更要求の前と後の CI の状態を含む疑問を解消することができます。

- 要求どおりに適切な変更が行われたか?
- 変更チケット以外にどんな変更が CI に発生したか?
- 変更はいつ発生したか?
- 変更の前後で、この CI と標準設定をどのように比較するか?

CA APM 統合

バージョン指定は、CA APM により、その CI に対して加えられた変更を表示します。バージョン指定は、各 CA APM の変更に関連付けられた属性ログ エントリから直接行う、CA CMDB から CA APM へのコンテキスト内起動もサポートしています。CA APM 監査証跡情報は、CA APM 監査ロギングが有効な CA CMDB ファミリの CI でのみ利用できます。

注: CI の属性が CA APM で変更されると、キャッシュ アクティビティが原因で、[属性] タブのデータの前に CI の詳細ページの [バージョン指定] タブのデータが更新される場合があります。値を再同期するには、[編集] ボタンをクリックしてください。

初期設定では、CA APM は CI 属性の変更を記録しません。CA APM で管理された CI で [バージョン指定] を使用するには、ロギングが必要なアセット属性ごとに [監査証跡データの保存] オプションを有効にする必要があります。

デフォルトでは、CI が CA APM で更新されてから、CMDB のバージョン指定で利用可能になるまで 10 分の遅延があります。この遅延を変更するには、統合インストール内の @NX_DBMONITOR_TIMER_MINUTES 変数を変更します。

注: アセットの属性ロギングを有効にする方法の詳細については、CA APM ドキュメントを参照してください。

関連項目:

[CA APM 統合機能](#) (P. 713)

CA APM 統合機能

CA SDM には、以下の CA APM との以下の統合機能があります。

- CA APM CI とアセット間で異なる共有レコードと監査ログ
- CI/アセット情報を取得するための CA CMDB および CA APM のコンテキスト起動
- 共有の拡張テーブル フィールド
- CA APM が主要連絡先を変更した場合の CA SDM の連絡先の更新
- CI ファミリを使用するための CA APM アセット タイプの変更

CI バージョン指定管理

CI の履歴、関連付けられたスナップショット、マイルストーン、スケジュールされていない変更、およびその他のビューを表示および管理することができます。ナビゲートには左側のペインを使用し、CI の詳細および監査ログの表示には右側のペインを使用します。

注: バージョン指定は、管理対象属性履歴と管理対象変更状態履歴に対して同様に機能します。たとえば、[管理対象属性履歴] タブには、管理対象属性に関するバージョン指定情報が表示されます。

変更仕様とそれに関連付けられた変更要求を識別するには、バージョン指定情報を使用します。バージョン指定では、スケジュールされた開始日を持たない変更要求に対応する、スナップショット ビュー内の変更仕様のスケジュールされていない変更が識別されます。CACF の変更仕様のスナップショットとログを表示できます。

例: スケジュールされていない変更

この例では、ユーザが管理対象属性の値を変更しようとしています。構成アイテムの詳細ページで、スナップショット内のスケジュールされていない変更を表示する [バージョン指定] タブを表示します。このスナップショットには、日付、時間、ユーザ名、属性値などの、変更に関する情報が表示されます。

左側のペインでスナップショットまたはマイルストーンを選択すると、右側のペインには CI の状態、イベント、または比較の属性値が表示されます。左側のペインには、CI のスナップショットまたはマイルストーンを日付と時刻で表示したり（基本モード）、CI の特性で表示したり（詳細モード）、CI の管理に役立つ以下のリンクを含めて表示することができます。

マイルストーンの作成

CI の状態にラベルを付けます。

ログの表示

フィルタされていない CI 履歴を表示します。

基本 / 詳細

スナップショットの表示形式を切り替えます。

空の値を表示しない

空白のデータ フィールドをフィルタできます。選択されていない場合は、すべての CI 属性が表示されます。

印刷とエクスポート

表示されているバージョン指定のデータを印刷したり、切り取りおよび貼り付けして保存したりできます。

ログの表示

ログを使用すると、構成アイテムの履歴を表示できます。[フィルタ] オプションを使用して、ログの行をフィルタすることもできます。[印刷] および [エクスポート] を使用すれば、表示されているバージョン指定のデータを印刷したり、切り取りおよび貼り付けして保存したりできます。

[バージョン指定] 情報ペインには、以下のフィールドが表示されます。

- カテゴリ
- 日付
- ログ
- 属性
- 新しい値
- 古い値
- 変更者
- MDR

注: 以前のリリースの CA SDM または CA CMDB で作成した CI の場合、ログには属性の変更だけが表示されます。CI の初期の属性値は表示されません。以前のリリースの CA SDM または CA CMDB で作成された関係には、監査履歴情報がなく、ログに表示されません。

ログのフィルタリング

〔フィルタ〕フィールドにシンプルな文字列を入力して、ログをフィルタできます。大文字と小文字は区別されません。フィルタの文字列がログの行のどこかと一致した場合に、その行が表示されます。フィルタでは特殊文字やワイルドカードは使用できません。フィルタ基準と一致するログの行が表示され、一致しない行は表示されません。

表示を更新するのに、**Enter** キーを押したり更新したりする必要はありません。ログの表示はキーストロークが入力されるたびにフィルタされます。これは、日付、ログ、属性、古い値、新しい値、MDR、および名前のすべてのフィールドに適用されます。

構成アイテムの履歴表示

構成アイテムの履歴を表示できます。

構成アイテムの履歴を表示する方法

1. 構成アイテムを検索して開きます。
〔構成アイテムの詳細〕 ページが表示されます。
2. 〔バージョン指定〕 タブをクリックします。
〔バージョン指定〕 ページが表示されます。
3. 〔ログの表示〕 をクリックします。

構成アイテムの履歴が一覧表示されます。

注: 〔ログの表示〕 は左側のペインで選択されているものを無視します。

CI のログの印刷

CI のログは印刷することができます。

CI のログ履歴を印刷するには、以下の手順に従います。

1. CI を選択し、[バージョン指定] タブをクリックします。
2. [ログの表示] リンクをクリックします。
3. (オプション) 必要なフィルタ基準を入力して、ログの行を表示/非表示します。
4. [印刷] をクリックします。

プリンタ専用のウィンドウが開きます。CI の [バージョン指定] レポートが表示されます。

5. Web ブラウザ ウィンドウで [ファイル] - [印刷] をクリックし、レポートのコピーを印刷します。

書式設定済みのテキストが、定義されているプリンタに送信されます。

CSV エクスポートのサポート

CA CMDB のログのコンテンツは、カンマ区切り値 (CSV) 形式ファイルにエクスポートでき、サードパーティ製のレポート ツールやアプリケーションにインポートできます。エクスポートは、画面に表示されている内容をベースにします。また、フィルタを使用したり解除したりできます。

関連項目:

[データのエクスポート](#) (P. 730)

統合された CA SDM および CA APM のログ

CI のログには、CA CMDB の機能を使用した変更のほかに、CA SDM の変更チケットアクティビティからの更新イベント、および CA APM の更新も含まれます。

関連項目:

[CA APM 統合](#) (P. 713)

コンテキストでの MDR の起動およびソース識別

CA CMDB では、特定の CI ログ エントリに対する MDR データ プロバイダを、ログから直接、コンテキストで起動できます。また、変更仕様へのコンテキストでも起動できます。この起動機能によって、以下の操作を実行できます。

- GRLoader の入力に MDR が <mdr_name>、<mdr_class>、および <federated_asset_id> タグを使用している場合、ソース MDR までさかのぼって属性変更を追跡する。

注: 詳細については、CA CMDB の「テクニカル リファレンス ガイド」を参照してください。

- CI の属性が 1 つ以上の MDR によって更新されている状況を識別する。この状況は、複数の MDR が CI 定義にデータを個別に提供した場合に発生します。
- 信頼できるソースとして動作している MDR を特定します。

注: CA SDM または以前の CA CMDB リリースで作成されたログ エントリからは、MDR をコンテキストで起動することはできません。また、CA Cohesion ACM では、ほとんどの属性や関係に MDR 起動情報が提供されますが、一部の属性や関係では提供されないものもあります。

属性名

ログに表示される属性名は、ユーザ インターフェースに表示される属性名と一致しています。内部オブジェクト名は反映されません。たとえば、CA CMDB は、「mtce_type」の代わりに「保守タイプ」を表示します。

カスタム ファミリおよびカスタム属性のロギング

カスタマイズしたファミリおよび属性のロギングを有効にするには、MDR 属性と監査トリガを新たに指定します。新しいファミリや属性を作成する場合は、メタデータ ファイルも作成して、ログに表示される人間が読み取れる属性名を指定する必要があります。指定しない場合、内部オブジェクト名が表示されます。

注: 詳細については、「管理ガイド」の「CA CMDB の拡張」を参照してください。

マイルストーンの作成

GRLoader を使用して、ユーザ インターフェースからマイルストーンを作成できます。

ユーザ インターフェースからマイルストーンを作成するには、以下の手順に従います。

1. CI を選択し、[バージョン指定] タブをクリックします。
2. [マイルストーンの作成] をクリックします。
3. マイルストーンの説明を入力します。 [保存] をクリックします。
[マイルストーンの作成] ページが閉じます。
4. [表示] - [更新] を選択します。

基本ビューで、新しいスナップショットが現在の日時と共に表示されます。これが作成したマイルストーンです。 マイルストーン表示に切り替えると、割り当てた名前の付いた対象のスナップショットだけが表示されます。 マイルストーンは、降順の日付/時間シーケンスで、一番最近のものをトップにして表示されます。

GRLoader を使用してマイルストーンを作成するには、以下の手順に従います。

1. CI の XML に <milestone> タグを追加します。
2. マイルストーンを CI と関連付けたときと同じ調整ルールを適用します。

注: マイルストーン タグの値には、マイルストーンと関連付けたラベルを入れます。

3. CI の XML を保存し、閉じます。
マイルストーンが作成されます。

注: 詳細については、CA CMDB の「テクニカル リファレンス ガイド」を参照してください。

例: GRLoader を使用したマイルストーンの作成

以下の GRLoader のサンプルでは、「**Fiscal year end 2008**」というマイルストーンを作成しています。

```
<ci>
<name>server1 </name>
<milestone>Fiscal year end 2008</milestone>
</ci>
```

標準 CI の作成

ほかの CI の作成と同じようにして、標準 CI を作成できます。

ユーザ インターフェースで標準 CI を作成するには、以下の手順に従います。

1. [ファイル] メニューから [構成アイテムの新規作成] を選択します。
2. 新しい標準 CI で使用するファミリを選択します。
3. 通常の CI と同じように属性を定義します。

標準 CI が作成されます。

注: どの CI でも標準 CI に指定できますが、以下の注意が必要です。

- 通常の CI と混同されないように、標準 CI は命名規則に従う。
- 標準 CI は、同じファミリに対する CI ベースラインとしてのみ機能する。
- 標準 CI には、調整に使用される属性（たとえば、MAC アドレス、シリアル番号、代替 CI ID、DNS など）を割り当てない。
- 標準 CI は通常の CI と区別がつかないため、スコアボード上に表示され、CI の合計にカウントされる。
- 標準 CI は、事業体オブジェクトの実際のインスタンスを何も示さないのが最も望ましい姿である。

CI への標準 CI の割り当て

[構成アイテムの詳細] ページを使用して、標準構成アイテムを構成アイテムに割り当てることができます。 [リスト内で編集] を使用して、標準 CI を CI のリストに割り当てることができます。

[構成アイテムの詳細] ページを使用してファミリの標準 CI を CI に割り当てるには、以下の手順に従います。

1. CI を選択し、[編集] をクリックします。
[構成アイテムの更新] ページが表示されます。
2. [標準 CI] フィールドの横にあるアイコンをクリックします。
CI リストが表示されます。
3. 標準 CI とする CI を選択します。 [保存] をクリックします。
標準 CI が割り当てられます。

[リスト内で編集] を使用して標準 CI を CI のリストに割り当てるには、以下の手順に従います。

1. [スコアボード] タブまたは [管理] タブから、検索フィルタを指定して、詳細リストに 1 つの CI または複数の CI を表示させ、[検索] をクリックします。
検索基準と一致した CI が一覧表示されます。
2. 結果リストの右上にある [リスト内で編集] ボタンをクリックします。
[CI Edit in List] コントロールが表示されます。
3. CI を含む行を選択し、標準 CI に割り当てます。
選択した行がカラーで強調表示されます。
4. [標準 CI] フィールドの横にあるアイコンをクリックします。
CI リストが表示されます。
5. 標準 CI とする CI を選択します。 1 つの CI を更新する場合は [保存] をクリックし、リスト内のすべての CI を更新する場合は [すべて変更] をクリックします。
標準 CI が 1 つの CI ([保存] の場合) またはリスト内のすべての CI ([すべて変更] の場合) に割り当てられます。

注: どの CI でも標準 CI に指定できますが、以下の注意が必要です。

- 通常の CI と混同されないように、標準 CI は命名規則に従う。
- 標準 CI は、同じファミリに対する CI ベースラインとしてのみ機能する。
- 標準 CI には、調整に使用される属性（たとえば、MAC アドレス、シリアル番号、代替 CI ID、DNS など）を割り当てない。
- 標準 CI は通常の CI と区別がつかないため、スコアボード上に表示され、CI の合計にカウントされる。

標準 CI は、事業体オブジェクトの実際のインスタンスを何も示さないのが最も望ましい姿である。

GRLoader を使用した CI への標準 CI の割り当て

標準 CI を CI に割り当てるには、CI の説明に `<standard_ci>` タグを含めます。

注: 詳細については、CA CMDB の「テクニカル リファレンス ガイド」を参照してください。

例: CI への標準 CI の割り当て

標準ワークステーション構成という名前の CI に格納された標準ワークステーション構成がある場合、GRLoader を使用して以下に示す XML をロードし、その標準 CI を「Joe のワークステーション」に割り当てることができます。

```
<ci>
  <name> Joe のワークステーション </name>
  <class>Server</class>
  <standard_ci> 標準ワークステーション構成 </standard_ci>
</ci>
```

基本ビューの使用

スナップショットは、基本表示または詳細表示から選択できます。どちらのモードにも、同じ種類のバージョン指定データが表示されます。基本表示では、CIの状態を容易に表示することができます。

CIの状態を表示するために基本表示を使用するには、以下の手順に従います。

1. ユーザインターフェースでCIを開き、[バージョン指定] タブをクリックします。

既存のスナップショットがページの左側に一覧表示されます。

2. [スナップショット タイプ] ドロップダウン リストからスナップショット タイプを選択します。

注: 標準CIがフォーカスCIに指定されている場合は、スナップショットまたはマイルストーンのリストのトップに表示され、CI名の右に「標準CI」インジケータが付きます。標準CIをクリックしたときに表示される属性は、標準CIのもので、フォーカスCIの属性ではありません。

スナップショット

日付/時間に基づいて識別されたすべてのCIのスナップショットおよび標準CIを一覧表示します。これはデフォルトのオプションです。

マイルストーン

ユーザ定義したすべてのマイルストーンおよび標準CIを一覧表示します。

CIの状態は右側のペインに表示されます。

下部の情報テキスト領域には、マウス ポインタがポイントしている項目に関する情報が表示されます。スナップショット、マイルストーン、または標準CIをポイントしている場合は、作成された日時に関する情報およびスナップショットのタイプが表示されます。

注: 2つ以上のスナップショット、マイルストーンまたは標準CIを選択して比較できます。

詳細表示の使用

スナップショットは、基本表示または詳細表示から選択できます。どちらのモードにも、同じ種類のバージョン指定データが表示されます。詳細表示では、スナップショットを属性タイプ、値、およびタイムスタンプに基づいて表示できます。また、詳細表示は、任意のスナップショット間の比較を、属性、マイルストーン、または標準 CI を条件に行えます。ツリー階層は、CI の各属性のフォルダを表示します。また、各属性フォルダには属性の値の履歴が含まれます。階層は、以下のように分類されます。

```
ルート
  属性名
    属性値 1
    属性値 2
```

階層により、特定の属性に固有の値の履歴がひとめでわかります。

詳細表示を使用するには、以下の手順に従います。

1. ユーザインターフェースで CI を開き、[バージョン指定] タブをクリックします。
既存のスナップショットがページの左側に一覧表示されます。
2. [詳細設定] をクリックします。
[詳細選択] にフォルダ階層が表示されます。
3. フォルダ階層を移動し、表示したい情報が含まれているフォルダをクリックします。

日付

基本表示と同じ日付/時間に基づいて、スナップショットが一覧表示されます。CI に 30 以上のスナップショットがある場合、年/月に基づいてさらに細分化される場合があります。標準 CI がフォーカス CI に割り当てられている場合は、標準 CI もこのフォルダ内に一覧表示されます。

マイルストーン

基本表示と同じユーザ定義マイルストーンがすべて一覧表示されます。標準 CI がフォーカス CI に割り当てられている場合は、標準 CI もこのフォルダ内に一覧表示されます。

標準 CI の属性は、[標準 CI] という特別なツリー リーフ ノードとして表示されます。[標準 CI] 値は、標準 CI 値が存在する属性に対してのみ表示されます。値が設定されていない属性には表示されません。

関係

CI のすべての関係（過去および現在）が含まれています。フォルダ階層によって、以下の情報が提供されます。

関係

関係タイプ

パートナー CI

ステータスおよび日付

[関係タイプ] には、「含まれる」、「ホストする」、「通信する」などの関係の種類が表示されます。

[パートナー CI] は、関係と関連付けられた CI の名前です。

[ステータスおよび日付] には、指定した日付および時間の関係のステータスが表示されます。ステータスの値には以下のものが含まれます。

- 関係作成済み - 関係が作成されたときの CI の状態です。
- 関係終了済み - この CI は関係に関連付けられていません。この関係はパートナー側ではまだ存在していますが、フォーカス CI は含まれていません。
- 関係削除済み - 関係は削除済みとしてマークされています。
- 関係変更済み - 関係は削除済みの状態から再アクティブ化されています。
- 新規パートナー/タイプ - 関係のパートナー側は新しい CI に割り当てられ、同時に関係タイプが変更されました。
- 新規関係タイプ - 2 つの CI 間の関係タイプは変更されています。
- パートナー CI 割り当て済み - 関係のパートナー側は変更されています。

4. 属性値をクリックします。

属性値が設定された時点の CI の状態が完全な形で表示されます。

例:[ディスク領域の表示]属性での詳細表示の使用

以下の例で、[詳細選択]にはディスク領域が 10 GB、20 GB、100 GB と増えた例が表示されます。

ルート
ディスク領域
10 GB
20 GB
100 GB

値のいずれかをクリックすると、変化が起きた日時やほかの属性の状態、およびディスク領域が変更されたときにオープンになっていた変更要求を確認できます。

スナップショットの詳細表示

スナップショットの詳細は、基本表示または詳細表示で参照できます。たとえば、基本ビューには、CI へのスケジュールされていない変更のスナップショットが表示されます。

スナップショットの詳細を表示するには、以下の手順に従います。

1. ユーザインターフェースでオブジェクトを開き、[バージョン指定] タブをクリックします。

既存のスナップショットのリストがページの左側に表示されます。

2. スナップショットをクリックします。

基本表示および詳細表示の右側のペインに詳細が表示されます。項目を 1 つのみ選択した場合、右側のペインには、選択したスナップショット、マイルストーン (CI の場合のみ)、または標準に関する情報が表示されます。

表示されるデータには、以下の詳細およびインジケータが含まれます。

空の値を表示しない

空白のデータ フィールドをフィルタできます。このチェック ボックスがオフの場合は、すべての CI 属性が表示されます。

[Bolded Value]フィールド テキスト

最後にスナップショット記録して以降に属性または関係が変更されていることを表しています。標準 CI の詳細を表示している場合は、すべての値が太字になっています。

値

値にカーソルをポイントすると、属性の以前の値および最終変更時刻を表示します。この情報は、[バージョン指定] タブの下部にあるテキスト領域に表示されます。

「(空白)」値

以前の値がクリアされたかどうかを示します。

関係カテゴリ

タイプやパートナー CI など、関係に関する情報を表示します。

コンテキストでの MDR の起動およびソース識別

CI の詳細エントリからプロバイダ MDR をコンテキストで起動できます。

注: CA SDM または以前のバージョンの CA CMDB で作成された CI は、MDR 情報および更新者情報が不足している場合があります。また、CA Cohesion ACM では、ほとんどの属性や関係から MDR をコンテキストで起動できますが、一部の属性や関係は対応していません。

ソース MDR までさかのぼって属性変更を追跡できます。

CI の属性が 1 つ以上の MDR によって更新されている場合に削除できます。この状況は、複数の MDR が CI 定義にデータを個別に提供した場合に発生します。

どの MDR が権限のあるソースとして動作しているかを識別できます。

特定の日付における CI の状態の表示(基本表示)

基本表示を使用して、特定の日付における CI の状態を表示できます。

ある日付の CI の状態を表示するには、以下の手順に従います。

1. CI を選択し、[構成アイテムの詳細] ページに移動します。
2. [バージョン指定] タブをクリックします。

CI の基本ビューが表示されます。

3. 表示する日付を選択します。

表示の右側に、選択した日付の CI の状態が表示されます。

特定の日付における CI の状態の表示(詳細表示)

〔詳細選択〕を使用すると、特定の日付の CI の状態を表示できます。

ある日付の CI の状態を表示するには、以下の手順に従います。

1. CI を選択し、〔構成アイテムの詳細〕ページに移動します。
2. 〔バージョン指定〕タブをクリックし、〔詳細設定〕をクリックします。

〔詳細選択〕ツリーが表示されます。

3. 〔日付〕フォルダを展開します。
4. 表示する CI の日付のチェック ボックスを選択します。

その日付の CI の状態が表示されます。

属性を設定した MDR の起動

CI の履歴が MDR を参照している場合は、MDR を起動して CI の詳細を表示できます。

MDR を起動して CI の詳細を表示する方法

1. CI を選択し、〔構成アイテムの詳細〕ページに移動します。
2. 〔バージョン指定〕タブをクリックします。
3. 〔ログの表示〕をクリックするか、表示する CI のスナップショットまたはマイルストーンを選択します。
4. 調べる属性の行を選択します。
5. CI 履歴が MDR を参照している場合は、MDR リンクをクリックします。

プロバイダ MDR に、そのほかの CI の詳細が表示されます。

スナップショットの印刷

選択した日付時点のスナップショットを印刷できます。

次の手順に従ってください：

1. オブジェクトを選択し、[バージョン指定] タブをクリックします。
2. 基本ビューを選択します。
3. [スナップショット タイプ] ドロップダウン リストから [スナップショット] を選択します。
4. 左側の日付リストの日付をクリックします。
5. [印刷] をクリックします。

プリンタ フレンドリなウィンドウが表示され、そのオブジェクトに関する [バージョン指定] レポートが表示されます。

6. **Web** ブラウザ ウィンドウで [ファイル] - [印刷] をクリックし、レポートを印刷します。

書式設定済みのテキストが、定義されているプリンタに送信されます。

CI のマイルストーンの印刷

選択した日付時点の CI のマイルストーンを印刷できます。

選択した日付時点の CI のマイルストーンを印刷するには、以下の手順に従います。

1. CI を選択し、[バージョン指定] タブをクリックします。
2. 基本ビューまたは詳細ビューから目的のマイルストーンを選択します。
3. [印刷] をクリックします。

プリンタフレンドリなウィンドウが表示され、その CI に関する [バージョン指定] レポートが表示されます。

4. **Web** ブラウザ ウィンドウで [ファイル] - [印刷] をクリックし、レポートを印刷します。

書式設定済みのテキストが、定義されているプリンタに送信されます。

データのエクスポート

[CSV へのログのエクスポート] ページでは、スナップショットおよびログ情報をカンマ区切り値 (CSV) 形式でエクスポートできます。データは [エクスポート] ページに表示されます。書式設定済みデータは取得した表示の内容に基づきます。行には区切り線が引かれ、カンマで区切られた各値は二重引用符で囲まれます。[バージョン指定] タブで選択したフィルタリングおよびデータ比較が、エクスポート用にフォーマットされた内容です。

CI データをエクスポートするには、以下の手順に従います。

1. オブジェクトを選択し、[バージョン指定] タブをクリックします。
2. CI の目的のビューをクリックします。
たとえば、[ログの表示]、スナップショットの比較、マイルストーン (CI のみ) などをクリックします。
3. [エクスポート] をクリックします。
[CSV へのログのエクスポート - CI] ページが表示されます。
4. [すべて選択] アクション (コンテキストメニューまたはキーボードショートカットのいずれか) を使用します。
5. 切り取りと貼り付けを使用して、書式設定済みページから CSV ファイルまたはサードパーティ製のアプリケーションヘデータを転送できます。たとえば、Excel のスプレッドシートをエクスポートできます。
データがエクスポートされます。

CI ファミリの変更とスナップショット

ファミリーを変更すると、CI のスナップショットに影響します。

スナップショットには、以下の異なる種類の属性が含まれています。

- 共通属性
- ファミリ固有の属性

CI のファミリーを変更すると、以下のようにスナップショットに影響します。

- CI に関連付けられているファミリー固有の属性が変わる。
- スナップショットの詳細に、スナップショットの作成時点のファミリーが反映される。

CI のファミリーによって、CI の属性が決まります。ファミリー固有の属性を変更してから CI のファミリーを変更すると、変更したファミリー固有の属性が CI に含まれなくなります。CI のファミリーを変更しても、共通属性には影響しません。

例: CI に関連付けられたファミリーの変更

この例では、CI のファミリー変更がどのように CI のスナップショットに影響するかを示します。

時間	ステータス/変更
0	CI はファミリー 1 です。
1	ファミリー 1 固有の属性値が 1 つ変更されました。
2	共通の属性値がいくつか変更されました。
3	CI のファミリーが、ファミリー 1 からファミリー 2 に変更されました。この変更が発生すると、すべてのファミリー 1 固有の属性がこの CI から利用できなくなります。
4	ファミリー 2 固有の属性値が 1 つ変更されました。
5	共通の属性がいくつか変更されました。
6	CI のファミリーが、ファミリー 1 に戻されました。この変更が発生すると、すべてのファミリー 2 固有の属性値がこの CI から利用できなくなりますが、以前のファミリー 1 固有の属性が復元されます。
7	共通の属性がいくつか変更されました。
8	ファミリー 1 固有の属性が 1 つ変更されました。

この例では、時間 7 のスナップショットには、時間 3 または 4 で行った変更の情報は含まれていません。これらの変更は、ファミリー 2 固有の属性に対する変更になります。

スナップショットの比較(基本ビュー)

2 つ以上のスナップショット、マイルストーン、または標準 CI を比較できます。

スナップショット、マイルストーン、または標準 CI を比較する方法

1. CI を選択し、[構成アイテムの詳細] ページに移動します。
2. [バージョン指定] タブをクリックします。
3. [スナップショット タイプ] ドロップダウン リストから [マイルストーン] または [スナップショット] を選択します。

マイルストーンまたはスナップショットが一覧表示されます。

4. 2 つ以上のスナップショット、マイルストーンまたは標準 CI を選択します。

比較ビューに以下の結果が表示されます。

- 列に、スナップショットとマイルストーンの相違点が表示されます。
- 各行には、選択したスナップショットの属性値が表示されます。
- 異なる部分のある属性のみが表示されます。スナップショットが同一でない場合は、日付が表示されます。
- 標準 CI の比較では時間は考慮されません。そのため、[日付] フィールドには「標準 CI」が設定されます。
- 比較結果は、印刷したり、CSV ファイルにエクスポートしたりできます。

スナップショットの比較(詳細ビュー)

2 つ以上のスナップショット、マイルストーン、または標準 CI を比較できます。

詳細ビューでスナップショット、マイルストーンまたは標準 CI を比較する方法

1. CI を選択し、[構成アイテムの詳細] ページに移動します。
2. [バージョン指定] タブをクリックし、[詳細設定] をクリックします。
[詳細選択] に CI が表示されます。
3. フォルダ階層を移動し、スナップショットの比較に使用する値を見つけます。
4. 各スナップショットで比較する値を選択します。

CI の比較結果が表示されます。たとえば、選択したフォルダの値を基準に、スナップショットの比較結果が表示されます。

比較ビューに以下の結果が表示されます。

- 列に、スナップショットとマイルストーンの相違点が表示されます。
- 各行には、選択したスナップショットの属性値が表示されます。
- 異なる部分のある属性のみが表示されます。スナップショットが同一でない場合は、日付が表示されます。
- 標準 CI の比較では時間は考慮されません。そのため、[日付] フィールドには「標準 CI」が設定されます。
- 比較結果は、印刷したり、CSV ファイルにエクスポートしたりできます。

注: 詳細ビューでは、2 つの CI 間の関係に、関係タイプが割り当てられていない場合があります (たとえば、CA NSM によって作成された CI)。そのような関係ノードは、(空白) として識別されます。

CA SDM 変更管理

バージョン指定データは、CA Service Desk 変更チケットと関連付けられた各 CI に対して自動的に生成されます。変更チケットがオープンからアクティブ、解決済み、クローズへと移るたびに、関連付けられた CI のスナップショットが記録されます。バージョン指定により、以下を実行できます。

- 変更管理ライフサイクルの任意の時点で、CI の状態を同じファミリの標準 CI と比較します。
- CI が標準に準拠しているかどうかを確認し、修正が必要な属性を特定するのに役立ちます。
- 変更要求ライフサイクルの任意の時点だけでなく、その間の任意の日付または時間を指定して CI の状態を比較できます。
- マイルストーンなど、変更の各段階の進捗状況を表示します。

CA Service Desk と CA CMDB 間の統合の例として、CI のサービス管理ライフサイクル中に変更を監査する方法を示します。この例では、変更要求はハードウェアサーバのコンポーネントをアップグレードするために使用されます。

変更要求を作成し、CI と関連付けるには、以下の手順に従います。

1. [ファイル] - [新規変更要求] をクリックし、CA Service Desk 変更チケットを作成します。
2. 「ハードドライブを 500 GB にアップグレード」など、変更要求の情報や要求の概要を入力します。
3. [構成アイテム] タブをクリックし、次に [構成アイテムの更新] をクリックします。
4. CI の検索基準を指定し（たとえば、ハードウェアサーバ名）、[検索] をクリックします。
5. [影響を受ける構成アイテム] フォームで、変更チケット（たとえば、手順 4 のハードウェアサーバなど）に関連付けられた CI を選択し、その CI を [影響を受ける構成アイテム] リストに追加します。[OK] をクリックします。
6. 変更要求を保存します。

変更を実行するには、以下の手順に従います。

1. CI に変更を加えます。たとえば、物理コンピュータにハードディスクを取り付け、そのハードウェア サーバ CI の [ディスク容量] 属性を更新します。
2. 変更要求をクローズします。
3. 変更が完了したことを確認します。CI を表示して [バージョン指定] タブをクリックし、変更前後の CI のスナップショットを比較します。

変更要求のオープン時とクローズ時の CI の状態の比較から、ハードウェア サーバのハードドライブのサイズが、変更前の **100 GB** から変更完了後に **500 GB** になっている点と、変更が発生した日時がわかります。オープン時とクローズ時の間に変更されたほかの属性も把握できます。

他の CA 製品での CI 属性の表示

他の CA 製品内の構成アイテム属性を表示するには [共通アセット ビューア] ページを使用できます。

ほかの CA 製品の [構成アイテムの属性] を確認するには、以下の手順に従います。

1. 構成アイテムを検索してオープンします。
2. [アセット ビューア] をクリックします。
[共通アセット ビューア] ページが表示されます。
3. [所有リソース] タブのリンクをクリックすると、ほかの CA 製品からの属性情報を確認できます。
4. 終了したら [ウィンドウを閉じる] をクリックします。

他の CA 製品内の構成アイテム属性が表示されました。

CMDBfドライバの使用

CA SDM は、MDR 全体の CI 統一の結果を表示する CMDBf ビューアを提供します。[構成アイテム詳細] ページ（または CI リストの CI 右クリックで表示されるメニュー）から [CMDBf ビューア] をクリックすると、統一 CMDB と MDR の CI 属性を同時に表示できます。[統一表示] ページで [取得] をクリックすると、すべての統一 MDR からの情報を更新できます。読みやすくするために、CA CMDB メタデータ ファイルでは MDR 属性名および CA CMDB 属性名を調整することができます。

注: この機能には、クエリをサポートする MDR が必要です。MDR CMDBf エンドポイントを編集して、その結果を [統一表示] で表示できます。詳細については、「実装ガイド」を参照してください。

CI に統一データがない場合、ビューアは CA CMDB 属性のみを表示します。

CMDB Visualizer

CA SDM により、IT コンポーネント（構成アイテム、つまり CI）とビジネスサービスを連携させることができます。CA CMDB は CI のグループが連携してビジネスサービスを提供する場合と同じように、CI 間の関係を定義します。CMDB Visualizer により、CI の関係の全体像を把握することができ、関係を管理する機能が提供されます。Visualizer を使用して、フォーカス CI（対象の CI）から 9 レベルまで関連する CI を表示することができます。

注:（高可用性設定のみ）アプリケーション サーバの休止期間中に Visualizer がサーバへリクエストを行うと、以下のメッセージが表示されます。

「この CMDB Visualizer サーバは保守のために xx:xx 以内にシャットダウンするようにスケジュールされています。作業内容を保存して、ログアウトしてください。」

メッセージボックスは非表示にできますが、休止期間中は上部パネルにメッセージが表示されます。サーバの休止がキャンセルされると、キャンセルに関するメッセージが表示されます。

CA はプロバイダ/従属モデルを使用して CI 間の関係を定義します。ビジネス サービスに関連するすべての CI はそのビジネス サービスへのプロバイダです（従属）。ほとんど同じ方法で、プロバイダは別の CI に依存する従属になることもできます。Visualizer を使用して以下のプロバイダ/従属分析を実行することができます。

参照

すべての CI のフィルタされていないビューを表示します。

影響分析

フォーカス CI（プロバイダ）を開始し、その従属を検索します。

根本原因

ビジネス サービス（従属）を開始し、そのサービスへのプロバイダであるすべての CI を表示します。

原因と結果の構成アイテム

1 つの検索で影響度分析と根本原因を組み合わせます。

関係のトレース

可能性のある関係をレベル別にすべて表示します。CI を 1 つだけ選択する場合、このフィルタは「参照」ビューを表示します。

最短パス

レベル別に関係の最短経路を表示します。

CMDB Visualizer を使用して、以下のアクションを実行できます。

- 設定可能なグラフィカル ビューから複数のレベルの CI を視覚化
- 進捗状況表示のモニタまたはキャンセル
- 柔軟な基準を使用した検索
- CI ファミリ、関係タイプおよびその他の属性に基づいたフィルタ
- CI の関係を表示
- 2 つの CI 間の関係をトレース
- 依存関係連鎖を視覚化
- Visualizer から直接 CA CMDB を呼び出す

- CI 属性とプロパティの表示
- グラフ メタデータを保存
- グラフ レイアウトを印刷
- 表示されたグラフ上で特定の CI を検索
- （役割に応じて） CI を作成
- （役割に応じて） 新しい CI 関係を作成
- スクラッチ パッドを使用してストア キー CI を保存
- CI ステータスを表示
- Visualizer のレイアウトで CI を表示または非表示にする
- ロール ベースのデータ セキュリティ
- 外部 MDR を起動
- Visualizer 機能のオンライン ヘルプを表示

関連項目：

[根本原因の分析](#) (P. 739)

[Visualizer 管理](#) (P. 739)

根本原因の分析

Visualizer と CMDBf ビューアを併用し、根本原因を分析できます。

根本原因を分析するには、以下の手順に従います。

1. Visualizer で、特定の問題状態（たとえば、動作が遅い、使用不可など）にある Service CI を検索します。
2. CI を右クリックし、[フォーカス CI の作成] を選択します。
3. 以下の基準に基づき、[根本原因] フィルタを選択します。
 - クラス タイプ： N/A
 - 「従属 > プロバイダ」関係： 根本原因分析のためにすべての関係が表示されます。
4. [表示] をクリックします。

生成されたグラフに、フォーカス CI に関連するすべての CI が、フィルタの指定に基づいて表示されます。CI の間のパスにはすべて、デフォルト レベルへの中間 CI が含まれます。
5. CI に移動し、フォーカス CI 条件の根本原因の候補としてインシデント、問題または最近の変更を確認します。
6. 特定の CI のコンテキスト内で CA CMDB を起動します。
7. [CMDBf ビューア] をクリックします。

[統一表示] は CI の MDR プロバイダのリストで表示されます。
8. 最新の MDR 属性を取得するには、[取得] をクリックします。

[MDR 属性] が更新されます。

Visualizer 管理

Visualizer 管理インターフェースは、CA CMDB Visualizer の設定の編集に使用できます。これらの機能を使用できるのは、管理者権限を持つ役割のみです。

以下のタブは、セカンダリ サーバで実行される Visualizer では無効です。これらのタブは、その他のすべての CA SDM サーバで有効です。

[Visualizer 設定]タブ

サーバおよび構成アイテムの表示情報の設定を可能にします。

[関係スタイル] タブ

関係のグラフィカル特性を定義します。

[CI ステータス] タブ

CI グラフィカル特性を定義します。

[フィルタ] タブ

C I 分析のためのフィルタを作成、編集、削除します。

[アイコン設定] タブ

CMDB Visualizer が r11.2 から リリース 12.9 にアップグレードされると、CI ファミリがそれぞれのアイコンイメージにマップされます。

注: Visualizer の定義の詳細については、CMDB Visualizer のオンライン ヘルプを参照してください。

検出されたアセットの追加

MDB（管理データベース）内の未所有アセットを、使用可能な所有構成アイテムに変換できます。

検出されたアセットを追加する方法

1. [構成アイテム リスト] ページで [検出されたアセット] ボタンをクリックします。
[検出されたアセットの検索] ページが表示されます。
2. [検索] をクリックし、[検出されたアセット リスト] を表示します。
3. 構成アイテムとして追加するアセットをリストから選択して右クリックし、表示されるポップアップメニューから [構成アイテムの新規作成] を選択します。
[構成アイテムの新規作成] ウィンドウが表示されます。フィールドの一部は、対象アイテムの情報が入力済みになっています。
4. 対象アイテムに適用する残りのフィールドを入力し、[継続] をクリックします。

注: 構成アイテムの作成に必須のフィールドは、[名前] と [クラス] のみです。

5. 必要に応じて、[属性] タブの適切なフィールドにデータを入力します。
構成アイテム用に選択したクラスのファミリーは、タブ上で表示される属性を決定します。ここで入力する内容は、ビジネス プロセスや、格納して表示したい構成アイテムの情報によって、異なります。
6. [保存] をクリックします。
検出されたアセットが追加されます。

アセット フラグと CI フラグ

2 つの一般的な属性フラグによって、フィルタリングのために CI/アセットのタイプをさらに詳細に分類したり、CA SDM やその他の CA APM などの製品に表示するエンティティを制御したりすることができます。

フラグは以下のとおりです。

構成アイテム (はい/いいえ)

構成アイテムを指定します。

アセット (はい/いいえ)

アセットを指定します。

デフォルトでは、CA CMDB によって作成された CI はフラグが「CI」に設定され、「アセット」には設定されません。この設定は必要に応じて無効にできます。CI も「アセット」に設定できます。CA CMDB では、「はい」に設定されたアセットフラグを変更することはできません。一般に、アセットが CA APM で作成された場合、アセットフラグは「はい」に設定されます。

これらのフラグは、すべての CI の詳細フォームおよび CI 検索機能に表示されます。値は、CI の詳細フォーム、GRLoader、および CA CMDB Web サービスで更新できます。[リスト内で編集] 機能でも、新規フラグの複数レコードでの更新がサポートされています。

〔CI〕フラグのオブジェクト属性名は **is_ci** です。〔アセット〕フラグのオブジェクト属性名は **is_asset** です。これらは、bool を参照する SREL 属性の名前です。属性名は、GRLoader XML タグとして使用できます。たとえば、GRLoader を使用して CI を作成するときに〔アセット〕フラグのデフォルト値を変更するには、以下の XML を追加して新しい CI を定義します。

```
<is_asset>YES</is_asset>
```

CI 調整

複数のデータ ソースが同じビジネス オブジェクトを参照するときに、それらのデータ ソースが処理する識別情報が異なっている場合、それらのソースからの更新によって更新する CI が 1 つのみの場合は、調整が役立ちます。あいまいさは、CI が一意でない可能性があることを表します。時には CI が CMDB 内で「重複」している場合や、CI トランザクションに複数のターゲット CI がある場合があります。これらが発生すると、CMDB が不正な状態になる場合があります。不正な CMDB では、CMDB の値が無効化されるため、不適切な業務行為につながる可能性があります。

自動 CI 調整は、CA CMDB の重要な利点であり、手動でのデータ保守に比べて大幅に時間を節約できます。CI 調整プロセスでは、いくつかの特定の識別属性を使用します。ただし、自動調整では、以下が発生する可能性があります。

- 一致の正の誤検出 (False positive)

CI を作成せずに、既存の CI が更新されます。

- 一致の負の誤検出 (False negative)

既存の CI を更新せずに、新規 CI が作成されます。同様の識別属性を持つ一連の CI があいまいであるのは、それらが、同様の識別属性を持つ実在する同一のビジネス オブジェクトに類似しているためです。

CA Service Desk Manager は、以下の調整アプローチをサポートしています。

MDR ベースの調整(受動)

CMDB は、MDR ベースの調整プロセスに基づいて、すべてのあいまいなデータを調整することができます。

あいまいな構成アイテムの識別および解決(反作用)

CMDB での既存の CI の識別および管理によって、あいまいな構成アイテムを識別して解決します。

トランザクション ワーク エリアの使用による着信データの確認および変更(事前対応)

トランザクション ワーク エリア (TWA) を使用して CMDB にロードする前に、着信データを確認して変更します。

関連項目：

[MDR-Based 調整 \(P. 744\)](#)

[あいまいな CI を識別して解決する方法 \(P. 746\)](#)

[トランザクションワーク エリア \(TWA\) を使用した着信データの確認と変更 \(P. 761\)](#)

MDR-Based 調整

MDR ベースの調整は、管理データ リポジトリで実行され、*MDB* 内に、実在の同じオブジェクトを参照する複数の *CI* が発生することを抑制します。

MDR ベースの調整では、単一の *CI* に関する情報を通信する際に、*MDR* は、常に同じ統一アセット ID を使用する信用できるソースとして扱われます。特定の *MDR* から特定の統一アセット ID への更新は、識別属性が変更された場合も、常に同じ *CI* を更新します。

このドキュメントで説明されている *MDR* ベースの調整、調整管理、およびトランザクションワーク エリア (TWA) を使用することによって、調整プロセスを制御することができます。ただし、調整管理および TWA を適切に使用するには、まず、*CA SDM* がどのように調整属性を使用するかを理解しておく必要があります。

重要: 任意の外部データ プロバイダ (*CA Cohesion ACM* など) を再インストールまたは再初期化する場合は、*CMDB* でその *MDR* 定義を非アクティブにしてから再アクティブにしてください。MDR によってその統一アセット ID が再利用されると、*CI* データのオーバーレイが予期せず発生する可能性があります。

関連項目：

[MDR の調整での CI の一致方法 \(P. 745\)](#)

[MDR の調整での CI の識別方法 \(P. 745\)](#)

MDR の調整での CI の一致方法

MDR ベースの調整では、以下のプロセスを使用して、一致する適切な CI を識別します。

1. トランザクションで ID が指定される場合、CI が特定され、調整が完了します。
2. トランザクションで ID が指定されない場合、CA SDM は、統一 ID 属性が指定されているか、また CI に一致するかどうかを確認します。一致する CI が存在する場合、トランザクションは一致する CI に対して調整を行います。
3. トランザクションで ID または統一識別属性が指定されない場合、CI トランザクションは、以下のセクションに示されている[識別属性](#) (P. 745)を使用します。

MDR の調整での CI の識別方法

MDR ベースの調整は、以下の優先順位を使用して CI を特定します。

1. ID (トランザクションで ID が指定される場合、調整は正常です。)
2. 統一 ID 属性
 - 統一アセット ID
 - MDR 名
 - MDR クラス
3. CI 識別属性
 - テナント (マルチテナンシーがインストールされている場合)
 - 名前
 - シリアル番号
 - MAC アドレス
 - システム名
 - 代替アセット ID
 - DNS 名

あいまいな CI を識別して解決する方法

CI を基準に CI のあいまいさを管理することをお勧めします。いずれの場合でも、構成管理者は、あいまいさが存在する場合に検出して最適な方法を決定する必要があります。CA SDM では、すでに CMDb にあるあいまいな構成アイテムを識別して管理するために広範なアプローチを行います。

不明確性インデックスとは、識別属性に基づいて構成アイテム (CI) が一意でない可能性を示す運用上の測定手段です。不明確性インデックスによって、CMDb 内に「重複した」CI がある可能性、またはトランザクションに複数の CI ターゲットがある可能性を測定できます。

重要: データベース クエリを使用して CI を手動で削除すると、CI の不明確性インデックスのためにエラーが発生する場合があります。これらのエラーを回避するには、`cmdb_update_ambiguity` ユーティリティを実行し、`-full` パラメータを 1 に設定します。このパラメータは、`cmdb_update_ambiguity.bat` またはシェルスクリプトを実行したときに、正確な不明確性インデックスを確実に受信するのに役立ちます。

あいまいな CI を識別して解決するには、以下の手順に従います。

1. あいまいな CI を識別します。
 - すべての CI の不明確性インデックスを計算する
 - あいまいな CI のリストをスコアボードで確認する
2. 各 CI の ID 属性が有効であるかどうかを判断する
3. 次のいずれかのアクションによって、あいまいな CI を解決します。
 - ID 属性を変更する
 - あいまいさの管理から CI を除外する
 - CI を非アクティブ化することによって CI の更新を拒否する
 - CI を置き換える

関連項目:

[CI のあいまいさの例 \(P. 747\)](#)

[あいまいな CI を識別し、それらの ID 属性が有効であるかどうかを判断する方法 \(P. 748\)](#)

[あいまいな CI を解決する方法 \(P. 757\)](#)

CI のあいまいさの例

4 つの異なるデータ ソースのデータが CMDB にロードされます。各データ ソースは独自の ID 特性サブセットを使用しています。この不一致性が原因で、CMDB の中には必要とされるもの以上の CI が存在しています。

以下に、CI のあいまいさの例を示します。

例: あいまいな構成アイテム

以下の 4 つの構成アイテムが CMDB に存在します。

- 名前 (Server1) DNS 名 (dns1) シリアル番号 (serial1)
- 名前 (Server1) DNS 名 (dns1)
- 名前 (Server2) DNS 名 (dns1) シリアル番号 (serial1)
- 名前 (Server3) MAC アドレス (mac1)

共有している ID 特性により、Server1 と Server2 の 2 つのインスタンスが互いにあいまいです。Server3 はあいまいではありません。

すべての CI には不明確性インデックスが関連付けられています。不明確性インデックスは大まかに、任意の ID 属性に一致する既存の CI の数です。インデックスが大きいほど ID に一致する CI の数が増えるので、CI データが不正に入力された可能性および追加 CI が不正に作成された可能性も大きくなります。不明確性インデックスがゼロの CI は、すべての ID の中で一意であるので、あいまいではありません。

前述の各 CI の不明確性インデックスは以下のとおりです。

- Server1 の 1 つ目のインスタンス: 名前 + DNS 名 + シリアル番号に一致する他の CI の数 = $1 + 2 + 1 = 4$
- Server1 の 2 つ目のインスタンス: 名前 + DNS 名に一致する他の CI の数 = $1 + 2 = 3$
- Server2: 名前 + DNS 名 + シリアル番号に一致する他の CI の数 = $0 + 2 + 1 = 3$
- Server3: 名前 + MAC アドレスに一致する他の CI の数 = $0 + 0 = 0$

関連項目:

[不明確性インデックスを計算する方法 \(P. 749\)](#)

[\[管理\] タブからのあいまいな構成アイテムの表示 \(P. 755\)](#)

[スコアボードからのあいまいな構成アイテムの表示 \(P. 756\)](#)

あいまいな CI を識別し、それらの ID 属性が有効であるかどうかを判断する方法

ゼロ以外の不明確性インデックスを持つすべての CI を調査して、それが一意であるかどうかや、不正な調整によって間違って作成されたかどうかを判断します。CI 自体にあいまいさはありませんが、その他の CI と比較したときにあいまいさが生じます。1 つのシステムの中には多数のあいまいな CI のセットが存在する可能性があります。それぞれの CI セットには、共通の ID 属性値を持つ CI が含まれます。

CI のあいまいさを調査するときは、同じセットに含まれる他の CI のあいまいさも調査することになります。1 つの CI のあいまいさを解決すると、同じセットに含まれる他の CI のあいまいさも少なくなります。

CA SDM は調整管理ツールを備えています。このツールを使用すると、あいまいな CI およびあいまいな CI がメンバーである CI セットを検出できます。あいまいさの根本原因を調査することで、あいまいさを解決できます。

あいまいさを管理するときは、以下の手順に従います。

1. すべての CI の不明確性インデックスを計算します。
2. スコアボードを使用して、あいまいな CI のリストを表示します。スコアボードには、すべてのあいまいな CI が、あいまいさの大きいものから小さいものの順で一覧表示されます。
3. スコアボードであいまいさの最も大きい CI から調査を開始します。
 - a. それと同じあいまいさセットに含まれるすべての CI を調査します。個々の CI の詳細フォーム上にある [調整] タブには、同じあいまいさセットに属するその他すべての CI が一覧表示されます。
 - b. セット内のすべての CI が正当であるかどうかや、調整の段階で誤りが生じているかどうかを判断します。ID 属性を確認して、セット内の CI が正しく作成されたものか、擬陰性の調整マッチングによって作成されたものかを判断します。
4. セット内の擬陰性の CI を特定します。

擬陰性の調整マッチングが行われ、追加の CI が作成されていると判断した場合は、有効な CI と、間違って作成された CI を特定します。ID 属性とその他の属性（最終更新日、関連する問題や案件、その他の要素など）を考慮します。

不明確性インデックスを計算する方法

あいまいさの管理を始める前に、既存の CI および CI トランザクションの不明確性インデックスを更新してください。CI および CI トランザクションの不明確性インデックスを更新するには、`cmdb_update_ambiguity` コマンドを実行します。

重要: CI または CI トランザクションのあいまいさを測定するには、`Run cmdb_update_ambiguity` を 1 回以上実行します。このコマンドを実行しないと、不明確性インデックスはすべて 0（ゼロ）となり、あいまいさがなくなることになります。

このユーティリティはあいまいさ管理の前または最中に実行できます。ユーティリティの定期的な実行をスケジュールすれば、不明確性インデックスによってシステムの最新状態がわかります。

不明確性インデックスを使用する方法

1. ユーティリティの実行に必要なパラメータを決定します。
2. ユーティリティを実行します。
3. CA SDM Web クライアントを起動し、[あいまいな CI リスト] または [あいまいな CI トランザクション リスト] に移動して、あいまいさを管理します。

関連項目:

[あいまいな CI を識別して解決する方法 \(P. 746\)](#)

cmdb_update_ambiguity コマンド

以下と同じコマンド構文を入力すると、CI および CI トランザクションの不明確性インデックスを計算できます。

```
cmdb_update_ambiguity [parameters] - m { ci | twa | all }
```

コマンドパラメータについては、[cmdb_update_ambiguity パラメータ](#) (P. 752)を参照してください。

デフォルトでは、構成アイテムのスキューンは最後のスキューン日から行われます。「-full 1」が指定されている場合は、完全なスキューンが実行されます。

例: Microsoft SQL Server データベース上で構成アイテムのあいまいさを計算する

以下のコマンドは、TWA 内にある既存のすべての CI とトランザクションの不明確性インデックスを計算します。

```
cmdb_update_ambiguity - m all - d MSSQL - u servicedesk - p dbpassword -s dbserver1
```

例: Oracle データベース上で構成アイテムのあいまいさを計算する

以下のコマンドは、CI の不明確性インデックスを計算し、データベース情報を指定します。

```
cmdb_update_ambiguity - m ci - d Oracle - u mdbadmin - p dbpassword -s server1 -port 1521 - SID orcl
```

環境設定ファイルを使用する方法

環境設定ファイルに多数の `cldb_update_ambiguity` パラメータを指定できます。オペレーティング システム ツールを使用して、暗号化されたフォームでパラメータ設定をセキュアにするために環境設定ファイルを使用できます。有効なキーワードおよび対応するコマンドライン オプションはパラメータ テーブルに一覧表示されます。

注: コマンドライン上および環境設定ファイル内の両方のパラメータを指定すると、コマンドライン値は環境設定ファイルの値を上書きします。

例: 環境設定ファイルを使用して Microsoft SQL Server データベースのパラメータを指定する

以下のコマンドは環境設定ファイル `ambiguity_mssql.cfg` を実行します。

```
cldb_update_ambiguity -m all -c ambiguity_mssql.cfg
```

設定ファイルの形式

環境設定ファイル オプションは、キーワード=値として指定されます。**Windows** で、ディレクトリ区切り記号にはダブル バックスラッシュ (\\) または単一の右上がりスラッシュ (/) を使用できます。パス名は二重引用符 (") で囲むことはできません。

有効なキーワードおよび対応するコマンドライン オプションは、パラメータ テーブルに一覧表示されます。

注: 列 1 のハッシュ記号 (#) はコメント行を開始します。

例: Microsoft SQL Server の構成設定

```
#Sample configuration file for Microsoft SQL Server
DBType=MSSQL
DBUser=servicedesk
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=C:\Program Files\CA\Service Desk Manager\log
LogLevel=ERROR
SchemaName=dbo
```

例: Oracle の構成設定

```
#Sample configuration file for Oracle
DBType=Oracle
DBUser=mbadmin
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=/tmp/ambiguity/log
LogLevel=INFO
DBPort=1521
DBSID=orcl
SchemaName=mbadmin
```

cmdb_update_ambiguity パラメータ

コマンドライン上または環境設定ファイル内（パラメータによってはコマンドライン上のみ）にパラメータを指定できます。コマンドライン上では、引用符（"）を使用して任意のパス名とスペースを囲みます。環境設定ファイル内では、引用符を使用しません。コマンドライン上および環境設定ファイル内でパラメータを指定した場合は、コマンドラインの値が環境設定ファイルの値に優先します。

cmdb_update_ambiguity コマンドは、以下のパラメータを使用します。

オプション	環境設定ファイル 値 のキーワード	注意事項
-m	(該当なし) twa、ci、all	(必須) コマンドラインのみ twa = TWA のみのあいまいさを計算します。 ci = CI のみのあいまいさを計算します。 all = CI と TWA のあいまいさを計算します。

-d	DBType	MSSQL または Oracle	(必須。 Windows のみ。) データベース タイプ。 Linux/UNIX では、Oracle のみがサポートされていて、このオプションは必要ありません。
-u	DBUser	<db ユーザ名>	(必須) データベース ユーザ名。 スペースが含まれるユーザ名は、二重引用符で囲む必要があります (例: -u "sys as sysdba")。 引用符は環境設定ファイルでは必要ありません。
-p	DBPassword	<db パスワード>	(必須) データベース ユーザのパスワード スペースが含まれるパスワードは、二重引用符で囲む必要があります (例: -p "secret code")。 引用符は環境設定ファイルでは必要ありません。
-c	(該当なし)	<環境設定ファイル>	(オプション) コマンドラインのみ 環境設定ファイルのフルパス名。 パス名にスペースがある場合は、二重引用符で囲む必要があります。
-log	LogLocation	<ログ ファイルを配置するディレクトリ>	(任意指定) ログ ファイル ディレクトリ。 デフォルトは NX_ROOT¥log ディレクトリです。
-level	LogLevel	INFO、ERROR、DEBUG	(任意指定) ログ ファイルに書き込む詳細のレベル。 デフォルト値は「ERROR」です。
-s	DBHost	<サーバ名>	(必須) データベース サーバのホスト名。 Microsoft SQL Server の名前付きインスタンスを使用するには、コマンドラインに server¥¥instance、または環境設定ファイルに server¥¥¥¥instance を指定します。

-CI	CI	<CI UUID>	(任意指定) 指定された構成アイテムおよびそれを使用するあいまいなすべての構成アイテムのあいまいさを計算します。
-full	(該当なし)	0,1	(オプション) コマンドラインのみ ユーティリティを前回実行した後に更新された CI のみを考慮することによって、スキャンのパフォーマンスを最適化します。 1 に設定した場合、不明確性インデックスの計算ですべての CI のフルスキャンが強制されます。デフォルトは 0 です。このパラメータは、トランザクションのあいまいさの計算には適用されません。このユーティリティでは常に、TWA 内のすべてのトランザクションが評価されます。
-port	DBPort	<ポート番号>	(必須。 Oracle のみ) Oracle ポート番号
-SID	DBSID	<SID 名>	(必須。 Oracle のみ) Oracle SID 名
-h	(該当なし)		(任意指定) ヘルプの使用法のメッセージを出力します。
-schema	SchemaName	<db スキーマ名>	(任意指定) デフォルトは、Oracle の場合が mdbadmin、Microsoft SQL Server の場合が dbo です。

関連項目:

[cmdb_update_ambiguity コマンド](#) (P. 750)

[管理]タブからのあいまいな構成アイテムの表示

cmdb_update_ambiguity ユーティリティを実行したら、[管理] タブからあいまいな CI を表示して、管理できます。

あいまいな CI を表示するには、[管理] タブで、[CA CMDB] - [調整管理] - [あいまいな構成アイテム] を参照します。

[あいまいな CI リスト] ページに、不明確性インデックスが 0（ゼロ）より大きい、あいまいな CI のリストが表示されます。

注: [あいまいな CI リスト] ページまたは [あいまいな CI トランザクションリスト] ページの [フィルタのクリア] をクリックしても、[その他の検索引数] フィールドの内容（あいまいさ > 0）は消去されません。

関連項目:

[\[管理\] タブからのあいまいな構成アイテムの表示 \(P. 755\)](#)

スコアボードからのあいまいな構成アイテムの表示

cmdb_update_ambiguity ユーティリティを実行したら、スコアボードからあいまいな CI を表示して、管理できます。

スコアボードからあいまいな CI を表示する方法

1. CA SDM スコアボードを表示している場合は、CMDDB フォルダを展開します。
2. [調整管理] - [あいまいな構成アイテム] を参照し、以下の 1 つをクリックします。
 - すべて
 - 前日更新
 - 先週更新
 - 先月更新

0（ゼロ）以上のインデックスを持つあいまいな構成アイテムのリストが表示されます。

注: [あいまいな CI リスト] ページまたは [あいまいな CI トランザクション リスト] ページの [フィルタのクリア] をクリックしても、[その他の検索引数] フィールドの内容（あいまいさ > 0）は消去されません。

関連項目:

[あいまいな CI を識別して解決する方法 \(P. 746\)](#)

あいまいな CI を解決する方法

あいまいな CI を識別し、それらの ID 属性が有効であるかどうかを判断したら、以下のいずれか 1 つまたは複数の方法を使用して、同じあいまいさセットに含まれる CI 間のあいまいさを解決します。

ID 属性を変更する

ID 属性が完全でないか有効でないかと判断した場合は、CI が一意になるように Web インターフェース、GRLoader、または CMDbF を使用して CI の ID 属性を設定します。

注: MDR によって CI が更新されるとき、手動で行った調整変更が解除される可能性があります。

あいまいさの管理から CI を除外する

CI の ID 特性が正しく、既知の有効なあいまいさを表していると判断した場合は、あいまいさの管理リストおよびその他の CI のあいまいさの計算からその CI を削除し、あいまいでないとマークできます (あいまいさを除外)。

CI を非アクティブ化することによって CI の更新を拒否する

CI の ID 属性が正しくなく、それらの属性を使用する更新によってデータの破損が生じると判断した場合は、その CI を非アクティブにして、それ以上の更新を禁止できます。情報を生成しているユーザまたは MDR はエラーを受け取り、トランザクション全体が拒否されます。

CI を置き換える

CMDb に対する更新は管理者が制御しきれなくなる場合があるため、無効な ID データは有効な非 ID 属性データと共にシステム内にある必要があります。トランザクション属性の受信データは、置き換える CI に透過的にリダイレクトできます。

注: CI 間で属性データを透過的にリダイレクトすると、混乱を生じさせる可能性があります。トランザクションデータは、トランザクションの ID 属性によって判断される CI と同じ CI に保存されない場合があります。前の各方法を使用できないためにこの方法を使用する場合は、注意してください。

構成アイテムをあいまいさの管理から除外する方法

特定の CI が 0 よりも大きい不明確性インデックスを受信しても、そのままの状態にしておく必要がある場合があります。 [あいまいさを除外] チェック ボックスがオンになっている CI は、不明確性インデックスまたはあいまいさの管理機能の一部として見なされません。

構成アイテムのあいまいさを除外する

Web インターフェースから CI の [あいまいさを除外] オプションを更新できます。

構成アイテムのあいまいさを除外する方法

1. [あいまいな CI リスト] ページで、あいまいさの管理対象から除外する CI を選択します。
[構成アイテムの詳細] ページが表示されます。
2. [編集] をクリックします。
[構成アイテムの更新] ページが表示されます。
3. [調整] タブの [あいまいさを除外] チェック ボックスをオンにし、[保存] をクリックします。
不明確性インデックスの計算およびその他のあいまいさ管理機能から CI が除外されます。

GRLoader を使用してあいまいさを除外する方法

GRLoader を使用して CI に `not_ambiguous` フラグを設定することにより、CI の [あいまいさを除外] オプションを更新できます。

`not_ambiguous` の値は以下のとおりです。

はい(1)

あいまいさの管理から CI を削除します。他の CI の ID 属性とは関係なく、CI は一意の ID と見なされます。CI の不明確性インデックスはゼロのままです。

いいえ(0) (デフォルト)

この CI はあいまいさの管理に適しています。CI の ID 属性の一意性によって、不明確性インデックスが決まります。この CI の ID 属性は、他の CI のあいまいさを評価する際に考慮されます。

注: GRLoader の詳細については、CA CMDB の「テクニカル リファレンス ガイド」を参照してください。

更新を拒否する方法

CI を非アクティブとしてマークすると、その CI に対する更新は実行できなくなります。指定された CI (名前、シリアル番号、MAC アドレスなどのいずれかで) のデータを拒否して、MDR に拒否を知らせるようになる場合は、CI を [非アクティブ] に設定します。

このようにして、問題のデータをすぐに拒否してソースにそれを反映させることによって、MDR は拒否された入力を修正することができます。

CI を Web インターフェースで非アクティブに設定するには、CI を編集し、それを [非アクティブ] に設定して、[保存] をクリックします。GRLoader または CMDBf Web サービスを使用して CI を非アクティブに設定することもできます。非アクティブ化した CI は再アクティブ化することもできます。

あいまいな構成アイテムの置き換え

あいまいな CI を置き換えて、データが特定のターゲット CI にリダイレクトされるようにすることができます。置き換え済みの CI は表示できます。置き換え済み CI は非アクティブであり、それらに対する Web インターフェース更新はすべて無視されます。

注: GRLoader または CMDBf の Web サービスによって CI の置き換えに送信された更新は、CI の置き換えにリダイレクトされます。ただし、ID 属性に対する更新は無視されます。

あいまいな構成アイテムを置き換える方法

1. [あいまいな CI リスト] ページで、フォーカスとなる（置き換える）CI を選択します。

[構成アイテムの詳細] ページが表示されます。

2. [編集] をクリックします。

[構成アイテムの更新] ページが表示されます。

3. [調整] タブをクリックします。

フォーカス CI と互いにあいまいなすべての CI が表示されます。

フォーカス CI で置き換える CI を決めます。リスト内の各 CI をクリックして [構成アイテム詳細] ページを開くことによって検査します。

4. フォーカス CI で置き換える 1 つ以上のあいまいな構成アイテムを選択し、[置き換え] をクリックします。

選択した CI がフォーカス CI に置き換えられます。

[管理]タブからの CI の置き換えの表示

[管理] タブから、CI の置き換えを表示できます。

置き換え済みの CI を表示するには、[管理] タブで、[CA CMDB] - [調整管理] - [CI の置き換え] を参照します。

[CI の置き換えリスト] が表示されます。

スコアボードからの CI の置き換えの表示

置き換え済みの CI はスコアボードから表示できます。

スコアボードから CI の置き換えを表示する方法

1. CA SDM スコアボードを表示している場合は、CMDDB フォルダを展開します。
2. [調整管理] フォルダを展開します。
3. [CI の置き換え] ノードをクリックします。
[CI の置き換えリスト] が表示されます。

トランザクション ワーク エリア (TWA) を使用した着信データの確認と変更

TWA ステージング領域にデータをコピーすることによって、CI および関係トランザクションを実行する前に予行することができます。予行領域で、Web インターフェース、またはネイティブ SQL を使用して CI と関係进行操作できます。

また、既存の CI を更新する必要がある場合に新しい CI が作成されないように、CI トランザクションを検証することもできます。この方法で、ターゲット CI にトランザクションを手動で一致させることができるように、各トランザクションと、更新が可能な潜在的 CI を表示します。同様に、正しい CI を参照するように関係トランザクションを検証できます。

不明確性インデックスとは、識別属性に基づいて構成アイテム (CI) が一意でない可能性を示す運用上の測定手段です。不明確性インデックスによって、CMDDB 内に「重複した」CI がある可能性、またはトランザクションに複数の CI ターゲットがある可能性を測定できます。

あいまいな CI トランザクションを確認および変更するには、以下の手順に従います。

1. あいまいな CI トランザクションを識別します。
 - すべての CI トランザクションの不明確性インデックスを計算する
 - あいまいな CI トランザクションのリストをスコアボードで確認する
2. 各 CI トランザクションの ID 属性が、対象となる CI に一致するかどうかを判断します。
3. 次のいずれかのアクションによって、あいまいな CI トランザクションを解決します。
 - ID 属性を変更する
 - ターゲット CI を指定する

関連項目：

[CI トランザクションのあいまいさの例](#) (P. 763)

[あいまいな CI トランザクションを識別する方法](#) (P. 765)

[あいまいな CI トランザクションを解決する方法](#) (P. 766)

[トランザクション ワーク エリア](#) (P. 768)

[TWA へのデータ入力](#) (P. 770)

[TWA 内のデータの更新に Web インターフェースを使用する方法](#) (P. 783)

[ステージング済みトランザクションの管理](#) (P. 767)

[CMDDB にトランザクションをロードする方法](#) (P. 789)

[手動調整](#) (P. 786)

[TWA の管理](#) (P. 791)

CI トランザクションのあいまいさの例

さまざまなデータ ソースのトランザクション データが CA CMDB にロードされます。各データ ソースは独自の ID 特性サブセットを使用するため、トランザクションのターゲット CI を完全に識別しない場合があります。この不一致性が原因で、CA CMDB の中には有効なもの以上の CI トランザクションが存在する可能性があります。

以下に、CI トランザクションのあいまいさの例を示します。

例: あいまいな CI トランザクション

TWA の中に以下の CI トランザクションが存在しています。

- 名前 (Server1) DNS 名 (dns1) 、シリアル番号 (serial1)

CA CMDB の中に以下の CI が存在しています。

- 名前 (Server2) DNS 名 (dns1)
- 名前 (Server3) DNS 名 (dns1) 、シリアル番号 (serial1)
- 名前 (Server4) MAC アドレス (mac1) 、シリアル番号 (serial1)

共有している ID 特性により、Server1 トランザクションは CA CMDB の Server2、Server3、および Server4 と互いにあいまいです。

すべての CI トランザクションには不明確性インデックスが関連付けられています。不明確性インデックスは大まかに、CI トランザクションで指定される任意の ID 属性に一致する既存の CI の数から 1 を引いた数です。インデックスが大きいほどトランザクション ID に一致する他の CI の数が増えるので、不一致な CI データが入力された可能性および追加 CI が不正に作成された可能性も大きくなります。不明確性インデックスがゼロの CI トランザクションは、すべての CI の中で一意の ID 属性を持っているか、ターゲット CI が指定されているので、あいまいではありません。

例: 不明確性インデックスの計算

TWA の中に以下の CI トランザクションが存在しています。

- 名前 (Server1) DNS 名 (dns1)、シリアル番号 (serial1)
- 名前 (Server2) DNS 名 (dns1)、シリアル番号 (serial1)

CA CMDB の中に以下の CI が存在しています。

- 名前 (Server1) DNS 名 (dns1)、シリアル番号 (serial1)
- 名前 (Server2) DNS 名 (dns1)、シリアル番号 (serial1)、Mac アドレス (mac1)

1 つ目のトランザクション (Server1) の場合、Server1 CI の ID 属性と完全に一致するので、不明確性インデックスは 0 です。このトランザクションに対して唯一可能性のあるターゲット CI は Server1 CI です。

2 つ目のトランザクション (Server2) は Server1 CI および Server2 CI と互いにあいまいです。

Server2 トランザクションの不明確性インデックスは以下のコンポーネントで構成されています。

- 名前 (Server2) に一致する CI の数 = 1
- DNS 名 (dns1) に一致する CI の数 = 2
- シリアル番号 (serial1) に一致する CI の数 = 2

CI の共有 ID 特性に基づき、Server2 トランザクションの不明確性インデックスは $(1 - 1) + (2 - 1) + (2 - 1) = 2$ です。

あいまいな CI トランザクションを識別する方法

トランザクションデータをロードする前に、あいまいな CI ターゲットを持つトランザクションを確認して変更できます。また、ターゲット CI はないけれども、1 つ以上の既存の構成アイテムの識別属性を持っている CI トランザクションを解決することもできます。この解決手順により、適切な CI が更新され、不正なデータまたは不一致なデータが作成されないようにすることができます。

[CI トランザクションの詳細] ページの [調整] タブには、フォーカス CI トランザクションと互いにあいまいなすべての CI が一覧表示されます。CI 属性を調査して(最終更新日、関連する問題や案件、その他の要素など)、トランザクションに対応するターゲット CI を識別します。

注: CI または CI トランザクションのいずれかのあいまいさを表示するには、[cmdb update ambiguity ユーティリティ \(P. 750\)](#)を使用して不明確性インデックスを計算する必要があります。

詳細については、「[トランザクションワークエリア \(TWA\) を使用した着信データの確認と変更 \(P. 761\)](#)」を参照してください。

[管理]タブからのあいまいなトランザクションの表示

[管理] タブからあいまいなトランザクションを表示して、管理できます。

あいまいなトランザクションを表示するには、[管理] タブで、[CA CMDB] - [調整管理] - [あいまいな CI トランザクション] を参照します。

不明確性インデックスが 0 (ゼロ) より大きい CI トランザクションのリストが表示されます。

注: [あいまいな CI リスト] ページまたは [あいまいな CI トランザクションリスト] ページの [フィルタのクリア] をクリックしても、[その他の検索引数] フィールドの内容 (あいまいさ > 0) は消去されません。

スコアボードからのあいまいなトランザクションの表示

スコアボードからあいまいなトランザクションを表示して、管理できます。

スコアボードからあいまいなトランザクションを表示する方法

1. CA SDM スコアボードを表示している場合は、CMDDB フォルダを展開します。
2. [調整管理] - [あいまいな CI トランザクション] を参照し、以下の 1 つをクリックします。

- すべて
- 前日更新
- 先週更新
- 先月更新

0（ゼロ）以上の不明確性インデックスを持つ CI トランザクションのリストが表示されます。

注： [あいまいな CI リスト] ページまたは [あいまいな CI トランザクション リスト] ページの [フィルタのクリア] をクリックしても、[その他の検索指数] フィールドの内容（あいまいさ > 0）は消去されません。

あいまいな CI トランザクションを解決する方法

あいまいな CI トランザクションを識別し、それらの ID 属性またはターゲット CI が有効であるかどうかを判断したら、以下のいずれかの方法を使用して、CI トランザクション間のあいまいさを解決します。

ID 属性を変更する

ID 属性が完全でないか有効でないと判断した場合は、CI が一意になるように Web インターフェースを使用して CI の ID 属性を設定できます。

ターゲット CI を指定する

ターゲット CI が設定されていないか有効でないと判断した場合は、あいまいなトランザクションに対して CI を指定できます。これによって、トランザクションで指定される ID 属性の値に関係なく、そのデータは特定のターゲット CI に送られます。

あいまいな CI トランザクションに対するターゲット CI の指定

あいまいなトランザクションに対して CI を指定することによって、トランザクションで指定される ID 属性の値に関係なく、そのデータが特定のターゲット CI に送られるようにすることができます。

あいまいな CI トランザクションに対してターゲット CI を指定する方法

1. [あいまいなトランザクション リスト] ページで CI トランザクションを選択します。
[構成アイテム トランザクションの詳細] ページが表示されます。
2. [編集] をクリックします。
[構成アイテム トランザクションの更新] ページが表示されます。
3. [調整] タブで、リストから CI を選択し、トランザクションのターゲット CI に指定します。[ターゲットの設定] をクリックし、[保存] をクリックします。
選択した CI がトランザクションのターゲット CI になります。

ステージング済みトランザクションの管理

CA CMDB には、データを CA CMDB にロードする前に保存する機能があります。この「ステージングされた」データは、トランザクションとしてトランザクションワークエリア (TWA) に保存されます。ステージング済みトランザクションは、CI または関係を作成あるいは更新する作業単位になります。TWA には、指定された 1 つの CI または関係について多数のトランザクションを保存できます。

CMDB にロードするデータは、コミットする前にキャプチャして、変更することができます。

- 非標準データをクリーンアップし、標準化できます。
- 不完全なデータを補完します。たとえば、「NY」で始まる CI 名に対して、そのロケーションを「ニューヨーク」に設定することが可能。
- 既存のルックアップテーブル (SREL) と一致しないデータを修正できます。
- 将来の時刻を指定して、トランザクションの実装をスケジュールできます。

- データをロードする前に、トランザクションを CA CMDB 内の既存の CI に一致させます。
- 単一または既存の CI を更新する必要がある場合に、CI および関係トランザクションを検証して、無効なデータまたは新しい CI が作成されないようにします。ターゲット CI にトランザクションを手動で一致させることができるように、各トランザクションと、更新が可能な潜在的 CI を表示します。

TWA を使用すると、調整プロセスをプロアクティブに管理するときに便利です。GRLoader を構成して TWA にデータをロードできます。その場合、CA CMDB では、間違った CI を作成、更新、または参照する可能性のあるトランザクションを処理するため、トランザクション データを変更できます。

詳細については、「[トランザクション ワーク エリア \(TWA\) を使用した着信データの確認と変更 \(P. 761\)](#)」を参照してください。

トランザクション ワーク エリア

CA SDM にはトランザクション ワーク エリア (TWA) が用意されています。ここで、CMDB にデータをロードする前に CI および関係データを検査して変更します。

TWA プロセスは以下のように実行されます。

1. TWA に[データをロード](#) (P. 770) します。コンテンツには、CI トランザクションまたは関係トランザクションを含めることができます。入力プロセスでは、レコードは調整されません。ここでは、以下のいずれかの方法を使用して CI トランザクション レコードおよび関係トランザクション レコードを単にワーク エリアに読み込みます。
 - GRLoader – XML データを読み取り、-littwa オプションまたは -littwar オプションを使用して TWA に格納します。
 - ネイティブ SQL – 標準的な SQL 処理を使用して、TWA にデータを格納します。
 - Web インターフェースを使用して、CI トランザクションまたは関係トランザクションを作成します。

2. (オプション) データをロードする前に、CMDDB 内の既存の CI に対するトランザクションを手動で調整します。また、[データのロードをシミュレート \(P. 776\)](#)することにより、一連のトランザクションが新規の CI を作成する（これにより、他の CI に新たなあいまいさが発生します）または関係を作成する可能性があるかどうかを事前に判別することもできます。

詳細については、「[トランザクションワーク エリア \(TWA\) を使用した着信データの確認と変更 \(P. 761\)](#)」を参照してください。

3. データを変更します。TWA は、以下のソースから変更できます。

CA SDM ユーザ インターフェース

Web ベースのユーザ インターフェースでは、ワーク エリア内のトランザクションを表示および変更できます。

ネイティブ SQL

複数のトランザクションに多くの変更を加える場合は、ネイティブ SQL によって TWA 内のデータを変更できます。

注: ネイティブ SQL を使用して加える変更は、CA SDM のすべてのセキュリティを迂回することができます。

4. GRLoader は、`-lftwa` オプションまたは `-lftwai` オプションを使用して、TWA から CA CMDB にデータをロードします。TWA の各行は個別のトランザクションとして扱われます。
 1. GRLoader 実行後にエラーが発生した場合、トランザクションが未完了であることを示すエラー コードがトランザクションに出力されます。（今後再試行を効率的に実行できます。）
 2. 他のすべてのレコードは、終了したトランザクションとして識別されます。
5. トランザクションの結果を確認し、エラーがある場合は Web インターフェイスを使用して修正します。必要に応じて手順 3 と手順 4 を繰り返します。

以下の点に注意してください。

- カスタム ファミリまたはカスタム属性を作成し、それらの列をワーク エリアに表示するには、カスタマイズされた列を含めるようにワーク エリアを変更してください。詳細については、「[TWA オブジェクトの拡張 \(P. 791\)](#)」を参照してください。
- TWA を利用するには、最新バージョンの GRLoader を使用してください。以前のリリースの GRLoader が含まれている製品を使用している場合は、GRLoader を最新バージョンにアップグレードしてください。
- TWA 内のトランザクションに対する変更は、監査されません。

TWA へのデータ入力

入力データは、以下を含む多数のソースから取得できます。

- GRLoader を使用してデータをインポートする、CA Cohesion ACM、CA Wily CEM、CA Wily Introscope、および CA Spectrum のような CA 製品
- GRLoader を使用してデータをインポートするその他の MDR
- 別の CMDB
- Microsoft Excel スプレッドシート
- データベース テーブル
- ベンダーにより選択された ETL ツール

詳細については、「[データベースの制約 \(P. 795\)](#)」を参照してください。

GRLoader を使用して TWA にデータをロードする方法

以下の GRLoader オプションは TWA の使用をサポートしています。

-littwa

初期状態の TWA に XML データをロード。

-littwar

準備状態の TWA に XML データをロード。

-lftwa

TWA から CMDB にトランザクションをロード。

-lftwai

TWA から CMDB にトランザクションをロードし、成功したトランザクションを非アクティブ化。

GRLoader 入力 XML ドキュメントは、変更せずに CMDB または TWA にロードできます。

GRLoader を **-littwa** (TWA にロード) オプションを選択して使用すると、トランザクションワークエリアにデータをロードできます。Grloader 構成ファイルで以下のように指定します。

```
grloader.loadtotwa=yes
```

TWA モードでは、CI および関係を直接作成する代わりに、GRLoader を使用して情報をトランザクションワークエリアに挿入します。TWA にロードされたデータは、編集、変更および検証することができます。データ変更プロセスの完了後、**-lftwa** または **-lftwai** を使用して個別のトランザクションを CMDB にロードできます。

CI データを CMDB にロードする場合は、CI の自動調整が行われます。調整が正常に終了すると、1 つのビジネス オブジェクトのデータによって CMDB 内の 1 つの CI が更新されます。CI トランザクションを TWA にロードする場合、自動調整は行われません。TWA では、1 つの CI をターゲットとする ID 属性を持つ複数のトランザクションが表示されます。「TWA にロード」モードで新しい行が追加される場合、その行が既存の CI に完全に一致する場合でも、TWA 内の既存の行は更新されません。同じ CI 定義であっても TWA に何度も表示されます。

GRLoader がデータ値を検証するのは、CMDB 内にオブジェクトを作成するため「TWA からロード」モード (-lftwa または -lftwai) で実行されている場合、あるいはシミュレーションモード (-simci または - simrel) で実行されている場合です。詳細については、「[TWA の操作をシミュレートする方法](#) (P. 776)」を参照してください。GRLoader が「TWA にロード」 (-lftwa または -lftwar) モードで実行されている場合、データ値は検証されません。

-lftwai パラメータ（または環境設定オプション

grloader.loadtotwa.inactivate）は正常にロードされた TWA のトランザクションを非アクティブにします。正常にロードしたトランザクションが非アクティブにマークされた後は、アーカイブ/パージを使用して TWA から永久にパージできます。

例: CMDB へのロード

以下のコマンドを使用して、CMDB にデータを直接ロードします。

```
grloader ... -i mydata.xml -a -n
```

XML ファイル mydata.xml には以下が含まれます。

```
<GRLoader>
  <ci>
    <name>server1</name>
    <class>Server</name>
  </ci>
</GRLoader>
```

例: TWA へのロード

以下のコマンドを使用して、TWA にデータをロードします。その結果、CMDB にロードする前にデータを操作できます。

```
grloader ... -i mydata.xml -lftwa
```

関連項目:

[XML 入力](#) (P. 773)

[lookup](#) (P. 773)

[日付の形式](#) (P. 774)

[EMPTY](#) (P. 775)

XML 入力

GRLoader では XML 入力データを使用します。TWA にロードする際、データベース内の標準列名に一致する列名が含まれている場合、競合の発生を防ぐために以下の XML 列がマッピングされます。

元の XML 名	マッピング後のデータベース列
tenant	tgt_tenant
id	tgt_id
delete_flag	tgt_delete_flag

関係には、以下のマッピングが適用されます。

元の XML 名	マッピング後のデータベース列
name	provider_name または dependent_name
dns_name	provider_dns_name または dependent_dns_name
delete_flag	tgt_delete_flag

TWA データベース テーブルからロードする場合、マッピングは逆になります。

lookup

TWA 内のルックアップ (SREL) 属性にデータを指定する場合、GRLoader のネイティブ XML で指定する場合と同じ形式が必要です。ルックアップ属性は、CA SDM の関連するテーブルに定義されている特定の値のセットのみを受け入れます。これらの属性には、割り当てが実施されるために満たす必要のある追加の制限事項や例外がある場合があります。XML、SQL または TWA Web インターフェースのいずれを使用した場合も、指定される値は同じです。

属性が SREL かどうかを判断するには、「CA CMDB テクニカル リファレンス」の以下のセクションを参照してください。

- ファミリおよびクラス (SREL 属性の識別)
- 連絡先およびその他のルックアップ フィールド
- 既存のテーブルのデータに対して検証されたフィールド (SREL)

例: lookup XML

lookup パラメータを指定して代替 SREL 列を設定する例を以下に示します。

```
<ci>
<name>server1</name>
<owner lookup="userid">mckpe99</owner>
</ci>
```

TWA では、区切り文字で囲んだ代替 SREL 列をデータ値の末尾に追加することで、同様のことを実行できます（以下の `grloader.workarea.delimiters` を参照）。同等のトランザクションが、トランザクション作業領域に以下のように表示されます。

ID	名前	所有者
100	server1	mckpe99 {userid}

上記の区切り文字は、`grloader` 環境設定ファイルで設定することもできます。

```
grloader.workarea.delimiters=xy
```

この `x` と `y` は異なる文字で、通常はワーク エリアに表示されません。

日付の形式

GRLoader は、XML で以下の日付形式をサポートしています。

- `datefmt=UTC`
- `datefmt=localtime`（デフォルト）

例: datefmt XML

```
<ci>
<name>server1</name>
<purchase_date datefmt="UTC"> 1241197235</purchase_date>
</ci>

<ci>
<name>server3</name>
<purchase_date> 2009/05/01</purchase_date>
</ci>
```

同等のトランザクションが、トランザクション作業領域に以下のように表示されます。

ID	名前	purchase_date
101	server1	1241197235
102	server2	2009/05/01

注: 日付がスラッシュ (/) のような特殊文字を含んでいる場合、フォーマットは「localtime」とみなされます。日付に特殊文字が含まれていない場合、日付は UTC であると判断されます。

EMPTY

GRLoader は、XML で、CMDB 内のフィールドをクリアする `update_if_null` オプションをサポートしています。以下の例では、`server1` の所有者フィールドをクリアします。この属性が存在しない場合、所有者フィールドは影響を受けません。TWA を使用する場合、代わりにキーワード `EMPTY` を使用できます。

例: update_if_null XML

```
<ci>
<name>server1</name>
<owner update_if_null="yes"></owner>
</ci>
```

TWA では、文字列値としてキーワード `EMPTY` を指定することによって、データベース値をクリアします。同等のトランザクションが、作業領域に以下のように表示されます。

ID	名前	所有者
102	server1	EMPTY

`grloader.emptyvalue` 構成オプションを使用すると、キーワード値を設定できます。

```
grloader.emptyvalue=xxxx
```

`xxxx` は任意の文字列を表します。通常、この文字列はワーク エリア データには表示されません。

TWA の操作をシミュレートする方法

以下のオプションを使用することにより、一連のトランザクションが新しい CI または関係を作成（また、これにより、他の CI に新しいあいまいさを作成）できるかどうかを事前に決定することができます。

-simci

CI トランザクションのみの処理をシミュレートします。トランザクションが CI を作成または更新するかどうかを決定するために使用できます。-simci オプションを使用する場合、GRLoader によってデータ検証が実行されます。

-simrel

関係トランザクションのみの処理をシミュレートします。関係トランザクションが関係を作成または更新するかどうかを決定するために使用できます。- simrel オプションは、プロバイダと従属 CI の存在の関係を確認して、関係タイプなどを検証します。

シミュレーション モードからの出力は TWA または _err.xml ファイルに送信されます。通常の読み込みモードでは、_err.xml ファイルには、CI 入力および CI が挿入されたか更新されたかを示すコメントが含まれます。シミュレーションを使用する場合、CI または関係が挿入されたか更新されたかを示す GRLoader メッセージが他の関連するエラー メッセージと共に CI トランザクション リストに表示されます。トランザクションの状態は変わりません。

シミュレーションは、**grloader.simulateloadci** と

grloader.simulateloadrelation のオプションを使用することによって、環境設定ファイルで有効にすることもできます。

注: GRLoader 入力で CI および関係を同時に作成する場合、- simrel オプションが処理できるのは実際の CI だけで、予定されている CI は処理できません。この制限があるため、-simci と - simrel は相互に排他的です。

SQL を使用して TWA 内のデータを更新する方法

TWA は、MDB に保存され、SQL クエリを使用して直接更新できます。

関連項目：

[TWA テーブル](#) (P. 777)

[TWA SQL 列名](#) (P. 778)

[TWA への新規レコードの挿入](#) (P. 781)

[ODBC ドライバの使用方法](#) (P. 781)

[TWA における CI ID](#) (P. 782)

[トランザクション ステータスを設定する方法](#) (P. 782)

[CA SDM とテーブルを共有する方法](#) (P. 783)

TWA テーブル

トランザクション作業領域（TWA）テーブルには、以下が含まれます。

ci_twa_ci

すべての CI ファミリの属性を含む単一のテーブルです。このテーブルのデータは正規化されずに保存されるため、ユーザやサービスがこのコンテンツを理解して操作することができます。

ci_twa_relation

ci_twa_ci テーブルを補完します。このテーブルには、CI 関係情報が含まれています。

TWA の列名は GRLoader で使用する属性に一致しますが、いくつかの例外があります。

注: 属性については、CA CMDB の「テクニカル リファレンス ガイド」を参照してください。

TWA SQL 列名

ci_twa_ci および ci_twa_relation テーブルの列名は、一部の例外を除き、CI 属性および関係属性の名前と一致します。

ci_twa_ci と ci_twa_relation に共通の TWA フィールド

apply_after_dt(指定日後に適用の日付)

GRLoader は、現在の日付が指定日後に適用の日付より後である場合にのみトランザクションを実行します。日付経過後の秒数で指定します。値がゼロ (0) の場合、このフィールドは無視されます。

tran_chg_ref_num(変更要求)

このトランザクションに関連付けられた変更要求 ID を指定します。GRLoader に -chg オプションを指定すると、この属性を使用して、特定の変更要求番号を持つトランザクションのみが選択されます。

注: -chg オプションの使用方法の詳細については、「[変更要求番号によるフィルタ](#) (P. 791)」を参照してください。

tran_status(トランザクション ステータス)

トランザクションのステータスを指定します。以下のいずれかの値である必要があります (tran_status=1 のトランザクションのみが実行されます) 。

値	簡単な説明	詳細な説明
0	初期	デフォルト値。GRLoader をこのトランザクションで実行するには、手動で準備完了に移行する必要があります
1	準備完了	このトランザクションを適切な CI または関係テーブルにロードする準備ができました
2	成功	トランザクションは正常に処理されました。
3	警告 :	ca_owned_resource/bmhier にロード中に警告が検出されました
4	エラー	ca_owned_resource/bmhier にロード中にエラーが検出されました
40000+	カスタマイズに使用 します	

tran_message(メッセージ)

ロードまたはシミュレーションの結果を示す GRLoader メッセージです。

tran_dt(トランザクションの日付)

現在の情報が古いトランザクションデータで誤って上書きされないようにします。トランザクションの実行日と CI の最終変更日が比較され、CI の日付の方が新しければ、そのトランザクションは GRLoader に拒否されます。

ターゲット CI よりも日付が古いためにトランザクションが GRLoader に拒否された場合は、そのトランザクションがまだ適用可能であることを確認し、トランザクションの日付をターゲット CI よりも新しい日付に手動で設定して、GRLoader を再実行してください。

tgt_delete_flag(アクティブ)

ターゲットの CI または関係を非アクティブ化します。この値は 1 に設定します。「delete_flag」を 1 に設定するのとは異なります。delete_flag を 1 に設定した場合は、トランザクションの削除を意味します。

ci_twa_ci の列

以下の列名に加えて、CI 属性の名前も SQL 文の列名として指定できます。

tgt_id(ターゲット CI)

ターゲット CI の UUID を指定します。手動調整を実行するときに使用します。

superseded_by(次で置き換え)

置き換えられた CI の UUID を指定します。

tgt_tenant(テナント)

ターゲット CI に割り当てられたテナント名を指定します。
Grloader のユーザに適切な権限がある場合は、CI 作成時にのみテナントを割り当てることができます。マルチテナンシーが有効になっている場合にのみ適用されます。

ci_twa_relation の列

以下の列名に加えて、関係属性の名前も SQL 文の列名として指定できます。

SQL を使用して関係トランザクションを定義するときは、以下のデータベース列名を使用します。

`provider_name` (プロバイダ名)

`provider_mac_address` (プロバイダ MAC アドレス)

`provider_serial_number` (プロバイダ シリアル番号)

`provider_system_name` (プロバイダ ホスト名)

`provider_asset_num` (プロバイダ アセット番号)

`provider_dns_name` (プロバイダ DNS 名)

`provider_tenant` (プロバイダ テナント)

および

`dependent_name` (従属名)

`dependent_mac_address` (従属 MAC アドレス)

`dependent_serial_number` (従属シリアル番号)

`dependent_system_name` (従属ホスト名)

`dependent_asset_num` (従属アセット番号)

`dependent_dns_name` (従属 DNS 名)

`dependent_tenant` (従属テナント)

プロバイダ CI または従属 CI の UUID がわかっている場合は、以下のフィールドを使用できます。

`provider_id` は、プロバイダ CI の UUID を指定します。

`dependent_id` は、従属 CI の UUID を指定します。

注: `provider_tenant` および `dependent_tenant` が適用されるのは、マルチテナンシーが有効になっている場合のみです。

TWA への新規レコードの挿入

CA SDM の外部から `ci_twa_ci` および `ci_twa_relation` テーブルに新しいレコードを挿入できます。

`ci_twa_ci` および `ci_twa_relation` テーブルにレコードを挿入するには、以下のようにして ID 列に 0 を指定します。

```
insert into ci_twa_ci values(id, name) values(0,'test-ci');
insert into ci_twa_relation values(id, type) values(0,'test-relation-type');
```

注意: マルチテナンシーが有効になっている場合は、必要に応じて `tenant`、`tgt_tenant`、`provider_tenant`、または `dependent_tenant` 属性を指定します。テナントを指定せずに TWA トランザクションを作成すると、パブリックなテナントが使用されます。

ODBC ドライバの使用方法

TWA をロードするために、GRLoader の代わりに SQL を使用できます。ネイティブ SQL サービスではなく、CA SDM に付属している ODBC ドライバを使用することを推奨します。ODBC ドライバを使用すると、以下の面で利点があります。

- パフォーマンス
- セキュリティ
- データベースの独立
- データを一括編集するツールが実行されており、CA SDM サーバでデータベースの更新が同時に発生する可能性のある環境でのデータ整合性

注意

- CA SDM ODBC ドライバのみが、マルチテナンシー、データパーティション、ロールアクセスなどのセキュリティ機能を保持します。ネイティブ DBMS ドライバを使用して実行される SQL には、セキュリティが実行されません。
- ネイティブ SQL を使用して更新を実行する場合、頻繁にデータのバックアップを作成してください。

TWA における CI ID

ci_twa_ci テーブルでは、ID、tgt_id、および superseded_by の 3 つの識別属性が CI トランザクションに関連付けられています。以下に、これらの属性について説明します。

- ID はトランザクションシーケンス番号です。このフィールドは変更できません。ID 1 から 2,000,000,000 までは、CA SDM サーバ外部の TWA を変更するシステムで使用するために予約されています。ID 2,000,000,001 からおよそ 40 億までは、CA SDM で使用するために予約されています。システムで ID が不足した場合は、テーブルを再初期化します。
- tgt_id、provider_id、または dependent_id は、ターゲット CI の UUID です。手動調整を実行する場合は、常にこのフィールドを設定します。
- superseded_by は、置き換える CI の UUID です。このフィールドは、トランザクションの置き換える CI を手動で指定するたびに設定してください。

トランザクション ステータスを設定する方法

各トランザクションのトランザクションステータス (tran_status) を TWA 内に設定することができます。GRLoader を使用してトランザクションを処理するには、ステータスを準備完了 (tran_status=1) に設定する必要があります。

値	簡単な説明	詳細な説明
0	初期	デフォルト値。GRLoader をこのトランザクションで実行するには、手動で準備完了に移行する必要があります
1	準備完了	このトランザクションを適切な CI または関係テーブルにロードする準備ができました
2	成功	トランザクションは正常に処理されました。
3	警告 :	ca_owned_resource/bmhier にロード中に警告が検出されました
4	エラー	ca_owned_resource/bmhier にロード中にエラーが検出されました

値	簡単な説明	詳細な説明
40000+	カスタマイズに使用 します	

GRLoader - lftwa が 2 回以上実行された場合、ステータスは初回実行後に更新されますが、それ以降の実行ではトランザクションが見つかりません。Grloader -lftwa を実行するたびに、事前にトランザクションの準備完了ステータスをリセットしてください。

TWA テーブルでの XML データの表記方法については、前のセクションの XML 例を参照してください。

CA SDM とテーブルを共有する方法

(SQL Server のみ)

SQL を使用して ci_twa_ci テーブルおよび ci_twa_relation テーブルを更新する場合は、以下のように、last_mod_dt 列を手動で設定します。

```
SET last_mod_dt = DATEDIFF(s, '19700101', GETUTCDATE())
```

例: last_mod_dt の設定

以下に、last_mod_dt を設定する例を示します。

```
UPDATE ci_twa_ci
    SET tran_status=1,
        last_mod_dt = DATEDIFF(s, '19700101', GETUTCDATE())
    WHERE tran_status=1
```

注: TWA テーブルの更新が、Web インターフェースまたは GRLoader に表示されるまでに数分かかる場合があります。更新タイミングの詳細については、「NX_DBMONITOR_TIMER_MINUTES オプション」を参照してください。

TWA 内のデータの更新に Web インターフェースを使用する方法

TWA ステージング領域にデータをコピーすることによって、CI および関係トランザクションを実行する前に予行することができます。ステージング領域では、Web インターフェースを使用して CI と関係进行操作できます。

また、単一または既存の CI を更新する必要がある場合に、CI および関係トランザクションを検証して、無効なデータまたは新しい CI が作成されないようにすることもできます。この方法で、ターゲット CI にトランザクションを手動で一致させることができるように、各トランザクションと、更新が可能な潜在的 CI を表示します。

トランザクション ワーク エリアを管理するには、[管理] タブを選択し、CA CMDB、[トランザクション ワーク エリア] ノードに移動します。このノードからトランザクション ワーク エリアのページを管理できます。

注: 詳細については、オンライン ヘルプを参照してください。

関連項目:

[CI トランザクションの管理](#) (P. 785)

[あいまいな CI トランザクションの管理](#) (P. 786)

[手動調整](#) (P. 786)

CI トランザクションの管理

「CI トランザクションの詳細」ページには、トランザクションの空白ではない属性がすべて表示されます。「空の値を表示しない」チェックボックスをオフにすると、すべての CI 属性が表示されます。属性情報の詳細については、属性名にカーソルをポイントしてください。

以下を実行できます。

- トランザクションの表示
- トランザクションの作成
- トランザクションの編集
- トランザクションの変更の保存、またはキャンセル（編集モード）
- 元のトランザクションデータのリセット（編集モード）
- データの表示または非表示の選択（「属性」タブ）
- ターゲット CI の設定（「調整」タブ）

1 つのトランザクションを保存したら、そのトランザクションの「調整」タブをクリックして、そのターゲット CI にあいまいさがないことを確認します。あいまいさがある場合は、[ターゲット CI を指定 \(P. 767\)](#) できます。データ入力すべて完了したら、[データのロードをシミュレート \(P. 776\)](#) して、データを検証し、調整を確認できます。

重要： この Web インターフェースを使用して TWA に入力するデータは、「[GRLoader を使用して TWA にデータをロードする方法 \(P. 771\)](#)」で説明されているルールに準拠している必要があります。

Web UI では TWA 内の大文字と小文字を区別するデータが検証されないため、入力するデータがルックアップ値と正確に一致していることを確認してください。GRLoader を実行する場合は、- I オプションを指定して、大文字と小文字を区別するルックアップを有効にすることができます。

注： tgt_id または superseded_by はトランザクションでは UUID として保存されますが、Web インターフェースでは CI 名として表示されます。

あいまいな CI トランザクションの管理

トランザクションデータをロードする前に、あいまいな CI ターゲットを持つトランザクションを確認して変更できます。また、ターゲット CI はないけれども、1 つ以上の既存の構成アイテムの識別属性を持っている CI トランザクションを解決することもできます。この解決により、適切な CI が更新され、不正なデータまたは不一致なデータが作成されないようにすることができます。

1 つのトランザクションを保存したら、そのトランザクションの [調整] タブをクリックして、そのターゲット CI にあいまいさがないことを確認します。あいまいさがある場合は、[ターゲット CI を指定 \(P. 767\)](#) できます。データ入力がすべて完了したら、[データのロードをシミュレート \(P. 776\)](#) して、データを検証し、調整を確認できます。

TWA 内のデータの調整については、「[トランザクションワークエリア \(TWA\) を使用した着信データの確認と変更 \(P. 761\)](#)」を参照してください。

手動調整

手動で CI トランザクションを調整するには、トランザクションの識別属性に一致するターゲット CI を判別し、そのトランザクションの `tgt_id` をターゲット CI の UUID に設定します。

GRLoader は、`tgt_id` を指定するトランザクションを処理するときに、そのトランザクションの識別属性が変更されていると、ターゲット CI をトランザクション情報で更新して、CI を再登録します。

ターゲット CI は、トランザクションで明示的に指定できます。また、[調整] タブを使用してターゲット CI を選択することもできます。

詳細については、「[トランザクションワークエリア \(TWA\) を使用した着信データの確認と変更 \(P. 761\)](#)」を参照してください。

あいまいな CI トランザクションに対するターゲット CI の指定

あいまいなトランザクションに対して CI を指定することによって、トランザクションで指定される ID 属性の値に関係なく、そのデータが特定のターゲット CI に送られるようにすることができます。

あいまいな CI トランザクションに対してターゲット CI を指定する方法

1. [あいまいなトランザクション リスト] ページで CI トランザクションを選択します。
[構成アイテム トランザクションの詳細] ページが表示されます。
2. [編集] をクリックします。
[構成アイテム トランザクションの更新] ページが表示されます。
3. [調整] タブで、リストから CI を選択し、トランザクションのターゲット CI に指定します。[ターゲットの設定] をクリックし、[保存] をクリックします。
選択した CI がトランザクションのターゲット CI になります。

関係トランザクションの管理

関係トランザクション リストには、関係トランザクションのデータ入力が表示されます。

このページを使用して、以下の操作を実行できます。

- 関係トランザクションの検索

このリストでは、以下の操作を実行できます。

- 関係トランザクションの作成
- リストでの編集 (ID 属性を除く)

関係トランザクションの更新

単一の関係トランザクションのデータを表示し変更できます。[関係トランザクションの詳細] ページでは、以下を実行することができます。

- 関係トランザクションの作成
- トランザクションの表示

- トランザクションの編集
- トランザクションの変更の保存、またはキャンセル（編集モード）
- 元のトランザクションデータのリセット（編集モード）

関係トランザクションを更新するには、以下の手順に従います。

1. [編集] をクリックします。
[関係トランザクションの更新] ページが表示されます。
2. フィールドを変更し完了します。
3. [アクティブ] を選択します。
4. [保存] をクリックします。

関係トランザクションが保存されます。

データ入力がすべて完了したら、データのロードをシミュレートして、データを検証し、調整を確認できます。

重要: この Web インターフェースを使用して TWA に入力するデータは、[「GRLoader を使用して TWA にデータをロードする方法 \(P. 771\)」](#)で説明されているルールに準拠している必要があります。

Web UI では TWA 内の大文字と小文字を区別するデータが検証されないため、入力するデータがルックアップ値と正確に一致していることを確認してください。GRLoader を実行する場合は、`-I` オプションを指定して、大文字と小文字を区別するルックアップを有効にすることができます。

注: `provider_id` または `dependent_id` はトランザクションでは UUID として保存されますが、Web インターフェースでは CI 名として表示されます。

CMDB にトランザクションをロードする方法

CI および関係を作成するために XML 入力を使用する代わりに、以下のオプションを指定して TWA を入力ソースとして選択することができます。

-lftwa (TWA からロード)

-lftwai (TWA からロードし非アクティブ化)

注: err.xml ファイルを使用する他の GRLoader モードとは異なり、TWA からロードを実行すると、トランザクションの [メッセージ] フィールドにエラーメッセージが返されて表示されます。

トランザクションが処理されると、GRLoader は各トランザクションの成功または失敗を示すトランザクションステータスを設定します。

GRLoader -lftwa を連続して複数回実行する場合は、GRLoader の実行と実行の間にトランザクションのステータスを [準備] に設定します。これは、GRLoader は、すでにロード済みのデータをロードしないためです。

このトランザクションは、XML 入力を使用して GRLoader を実行する場合と同じように TWA から実行されます。トランザクションセキュリティは、TWA トランザクションを最初にロードしたユーザではなく、TWA からロードを実行したユーザに基づいて実行されます。

トランザクションが正常に処理されると監査が発生します。

注: ロードを実行する前に、シミュレーションオプション (-simci および -simrel) を使用して、一連のトランザクションが新規 CI または関係を作成するかどうかを事前に判別することができます。詳細については、「[TWA 操作をシミュレートする方法](#) (P. 776)」を参照してください。

関連項目:

[データ回帰を防ぐ方法](#) (P. 790)

[変更要求番号によるフィルタ](#) (P. 791)

データ回帰を防ぐ方法

CI のトランザクションデータは TWA にありますが、他のアクションが CMDDB 内でその CI を更新し、TWA のトランザクションデータを無効にしてしまうことがあります。不要なデータ回帰を防ぐために、GRLoader は、TWA の tran_dt ([トランザクションの日付]) フィールドと CI last_update_dt ([最終変更日]) フィールドまたは relationship last_mod_dt ([最終変更日]) フィールドを比較します。last_update_dt がより最近の場合、GRLoader は TWA のトランザクションを拒否し、tran_message 列にエラーメッセージを記入します。

以下のいずれかの操作を実行して、この状態を解決することができます。

- Web インターフェースを使用して、CI または関係の tran_dt フィールド ([トランザクションの日付]) フィールドを適切な値に編集する。
- GRLoader オプションを
grloader.workarea.ignore_transaction_dates="yes" に設定し、トランザクションの日付を無視してデータを挿入する。

注: トランザクションが、ターゲット CI の日付よりも古いために GRLoader に拒否された後で、そのトランザクションを実行することが必要になった場合は、トランザクションの日付をターゲット CI よりも新しい日付に手動で設定し、GRLoader を再実行してください。

警告: [トランザクションの日付を無視] オプションを無視すると、データのバックレベル化または回帰が発生することがあります。同じ GRLoader の -lftwa を実行して単一の CI または関係が複数回更新された場合、CI の最終変更日 (last_update date) は最初の更新時の現在時刻に設定されます。同じ CI または関係に対して複数の更新を許可するには、追加チェックを実行し、GRLoader の起動後に CI または関係が更新されたかどうかを確認します。起動後に更新された場合、その更新は許可されます。

変更要求番号によるフィルタ

GRLoader の `-chg` オプションを使用して、変更チケットに関連付けられたトランザクションのみを選択できます。変更番号によるフィルタを実行するには、変更要求属性 (`tran_chg_ref_num`) を適切な変更要求番号に設定する必要があります。

注: CMDB にロードされた場合、変更要求文字列は検証されません。

例: 変更チケットによるフィルタ

以下のオプションは、変更要求 **23434** に関連付けられたトランザクションのみをロードします。

```
grloader -lftwa -chg 23434
```

TWA の管理

TWA は、以下の管理を適用することをお勧めします。

- TWA の拡張 – 任意の OOB ファミリを拡張する場合や、独自のカスタム ファミリを定義する場合に必要です。
- TWA のアーカイブとページ
- TWA と CA Cohesion ACM を併用する方法
- データベースの制限事項

関連項目:

[TWA オブジェクトの拡張 \(P. 791\)](#)

[TWA のアーカイブとページ \(P. 792\)](#)

[TWA GRLoader のコマンド オプション \(P. 793\)](#)

[TWA GRLoader 構成ファイル オプション \(P. 794\)](#)

[TWA と CA Cohesion ACM を併用する方法 \(P. 795\)](#)

[データベースの制限事項 \(P. 795\)](#)

TWA オブジェクトの拡張

CA CMDB ファミリ スキーマに変更を加える場合、TWA スキーマにも同様の変更を加える必要があります。カスタム ファミリまたは属性が定義されていない場合、TWA を変更する必要はありません。

TWA オブジェクトを拡張する方法

1. 「管理ガイド」の「CA CMDB の拡張」に記載されている手順を使用して、ユーザ定義のファミリおよび属性をカスタマイズします。
2. Web スクリーン ペインタ スキーマ デザイナを使用して、新しいファミリ属性を `ci_twa_ci` スキーマに追加します。

新しい属性を `ci_twa_ci` スキーマに追加するには、以下の手順に従います。

1. Web スクリーン ペインタ スキーマ デザイナ を使用して、`ci_twa_ci` テーブルのスキーマを開きます。
2. 必要なファミリ属性を拡張テーブルに追加します。
3. 変更した `ci_twa_ci` スキーマを発行します。

注: 新しい属性は、タイプ **STRING** であり、最長テキスト値を保持する必要があります。

3. 以下のように、カスタム ファミリのメタデータを **TWA** に追加します。
 1. Web スクリーン ペインタを使用して、`cmdb_metadata_site_families.htmlpl` ファイルを開きます。
 2. カスタム ファミリ用に作成された適切な `cmdb_metadata_extension.htmlpl` ファイルに `PDM_INCLUDE` を追加します。

TWA のアーカイブとページ

TWA を保持するために、CA SDM は以下のアーカイブとページのルールを提供します。

CI 休止トランザクション

削除のマークが付いた CI トランザクションをアーカイブしてページします。

CI トランザクション成功

正常に完了した CI トランザクションをアーカイブしてページします。

関係休止トランザクション

削除のマークが付いた関係トランザクションをアーカイブしてページします。

関係トランザクション成功

正常に完了した関係トランザクションをアーカイブしてページします。

ルールが実行される頻度またはそれらを有効にするかどうかを選択できます。

TWA のアーカイブとパージを有効にするためのルールは、カスタマイズおよび有効化できます。TWA を頻繁に使用するユーザは、DBMS によって課される TWA 内のレコード数の制限に注意してください。

TWA 内のすべてのデータをクリアするために TWA を再初期化する必要がある場合は、以下の手順に従います。

- すべてのトランザクションを非アクティブに設定する
- アーカイブ パージを実行する

重要: TWA 内のすべてのレコードを削除する目的で SQL を使用しないでください。必要なヘッダレコードが削除されます。

TWA GRLoader のコマンド オプション

CA SDM は、GRLoader TWA の処理で使用する以下のコマンド オプションを提供します。

-littwa

初期状態に XML をロードします。

-littwar

準備状態に XML をロードします。

-lftwa

TWA からトランザクションをロードします。

-lftwai

TWA からトランザクションをロードし、成功したトランザクションを非アクティブにします。

-chg *nnnn*

-lftwa および -lftwar で使用されます。変更要求 *nnnn* に関連付けられたトランザクションのみをロードします。

注: CMDDB にロードされた場合、変更要求文字列は検証されません。

-l

ルックアップ属性の大文字と小文字を区別しません。このオプションを使用しない限り、デフォルトでは、ルックアップ属性の自由形式テキストは大文字と小文字を区別して処理されます。

-simci

CI トランザクションが CI を作成または更新できるかどうかを決定します。このオプションを使用する場合、GRLoader は CI のみに対するエラーチェックを実行します。

-simrel

関係トランザクションが関係を作成または更新できるかどうかを決定します。このオプションは、プロバイダと従属 CI の存在の関係を確認したり、関係タイプを検証したりします。

TWA GRLoader 構成ファイル オプション

CA CMDDB では、GRLoader 構成ファイルに以下の TWA オプションが用意されています。

grloader.emptyvalue=EMPTY

grloader.loadfromtwa=yes

grloader.loadfromtwa.inactivatesuccessful=yes/no

grloader.loadtotwa=yes

grloader.loadtotwa.ready=yes/no

grloader.workarea.delimiters={ }

grloader.workarea.ignore_transaction_dates=yes

grloader.simulateloadci=yes/no

grloader.simulateloadrelation=yes/no

TWA と CA Cohesion ACM を併用する方法

TWA を CA Cohesion ACM の処理と併用するには、CA Cohesion ACM r5 にパッチ RO08739 を適用してください。このパッチを適用すると、CA CMDB の [レポート定義のエクスポート] の [エクスポート] オプションタブにある [その他のオプション] フィールドで `-ittwa` オプションを指定できます。GRLoader コンポーネントをアップグレードします。不明な点がある場合は、CA のサポートにお問い合わせください。

データベースの制限事項

TWA では、基盤となるデータベースに以下のデータ制限事項があります。

- TWA と Microsoft SQL Server を使用する場合、1 つのデータ トランザクションの合計サイズが 8060 バイトを超えないようにする必要があります。
- dbload および pdm_load ユーティリティを使用する場合、ロード操作は 512 列に制限されます。
- Oracle では、列数が 1000 に制限されています。CA CMDB をカスタマイズする場合、すべてのファミリ（CA 提供およびユーザ定義を含む）における属性合計数が 1000 を超えないようにしてください。
- SQL Server 2005 の制限事項を以下の表に示します。

制限タイプ	制限値 (32 ビットおよび 64 ビット)
表 (横) 1 つあたりの列数	30000
ベース テーブル 1 つあたりの列数	1024
SELECT 構文 1 つあたりの列数	4096
1 行あたりのバイト数	8060
テーブル 1 つあたりの行数	使用可能なストレージ容量により制限

CA CMDB データ保守

CMDB のデータ保守を実行するタスクには管理者権限が必要です。これらのタスクには、構成アイテムおよび関係情報の管理に使用するファミリ、クラスおよび関係タイプの設定方法が含まれます。

関連項目:

[CA CMDB のファミリー クラス構造 \(P. 796\)](#)

[単一の CI のファミリー/クラスの変更 \(P. 797\)](#)

[CI のリストのファミリー/クラスの変更 \(P. 797\)](#)

[GRLoader を使用したファミリー/クラスの変更 \(P. 798\)](#)

[CA CMDB の拡張 \(P. 799\)](#)

CA CMDB のファミリー クラス構造

CA CMDB には、初期設定の構成アイテム ファミリーおよびファミリーが含まれる CI クラスが用意されています。

注: デフォルトの CA CMDB ファミリー/クラス構造の詳細については、「CA CMDB テクニカル リファレンス ガイド」を参照してください。

注: 以下の Service Desk および CA APM ベース ファミリーには固有の CA CMDB 拡張テーブルはありません。

- コンピュータ
- ベース オブジェクトとしての連絡先
- ハードウェア
- ベース オブジェクトとしてのロケーション
- ベース オブジェクトとしての組織
- その他
- プロジェクト
- ソフトウェア

CA CMDB では、これらのベース ファミリーの CI に対応する [構成アイテムの詳細] ページには、追加のフィールドが含まれており、[属性] タブがありません。ファミリー特有の属性の追跡、バージョン指定、スナップショットおよびベースラインなどの CA CMDB の高度な機能を利用するには、ファミリーおよびクラスの変更機能を使用して、これらの CI を CA CMDB ファミリーに変換することをお勧めします。

単一の CI のファミリ/クラスの変更

単一の CI のファミリおよびクラスを変更することができます。

単一の CI のファミリおよびクラスを変更するには、以下の手順に従います。

1. 変更する CI を選択します。
2. [編集] をクリックします。
[構成アイテムの更新] ページが表示されます。
3. CI の [クラス] 値を変更します。クラスを選択することによって、CI のファミリも決定されます。値を直接入力するか、虫メガネのアイコンをクリックしてクラスのリストを選択します。
4. [保存] をクリックします。

単一の CI のファミリおよびクラスが変更されます。

CI のリストのファミリ/クラスの変更

リストの CI のファミリおよびクラスを変更することができます。

CI のリストのファミリ/クラスを変更するには、以下の手順に従います。

1. [構成アイテムリスト] で、[フィルタを表示] をクリックします。
2. 編集する CI を検索するために、1 つ以上の [検索] フィールドに入力します。
3. [検索] をクリックします。
[構成アイテムリスト] に、検索基準と一致したすべての CI が表示されます。
4. [リスト内で編集] をクリックします。
[構成アイテムリスト] に、選択したすべての CI の変更可能なフィールドが表示されます。
5. 必要に応じてファミリおよびクラスを編集します。
6. [すべて変更] をクリックします。
7. [保存] をクリックします。

[構成アイテムリスト] を更新すると、CI も更新されて表示されます。

GRLoader を使用したファミリ/クラスの変更

GRLoader を使用して、CI のファミリおよびクラスを変更することができます。

GRLoader を使用してファミリ/クラスを変更するには、以下の手順に従います。

1. CI 属性を変更するための XML コードを作成します。
2. GRLoader を使用し、変更する CI をオープンします。
3. GRLoader から XML を実行し、CI 属性を変更します。

CI のファミリおよびクラスが変更されます。

例: オープン CI のクラスを「ドキュメント」に設定する

オープン CI のクラスを「ドキュメント」に設定する場合の XML フラグメントの例を、以下に示します。

```
<ci>
  <name> ドキュメント番号 1
  <class> ドキュメント
</ci>
```

重要: 単一の CI のファミリ属性とクラス属性の両方を同時に更新しないでください。両方を変更するには、GRLoader を個別に呼び出し、CI 更新を個別に実行する必要があります。

CA CMDB の拡張

CA CMDB は、ビジネス ニーズに応じて拡張し、追加のファミリ、クラス、および属性を含めることができる、高度に柔軟なシステムです。新規属性は、ファミリ固有の属性または共通の属性（すべてのファミリに適用可能）にできます。CA CMDB には、業界標準に準拠した多数のクラスおよび属性を持つ事前定義されたファミリが用意されていますが、一部のビジネス ケースでは、以下のことを行う必要があります。

- 新規属性を追加して、1つまたは複数の CI ファミリを拡張する。たとえば、オフィス キャンパスのデバイスごとに GPS 座標を追加するために、`gps_coordinate` 属性を定義して、目的のファミリに追加できます。1つのファミリを拡張する場合は、Web Screen Painter のスキーマ デザインを使用して、既存の拡張テーブルに新規属性を定義します。また、属性を追加する場合は、その属性を使用する詳細ページ、属性タブ、メタデータ フォームも必ず変更する必要があります。詳細については、「[ファミリ属性の追加](#) (P. 801)」を参照してください。
- 共通属性を追加して、すべての CI ファミリを拡張する。詳細については、「[共通属性の追加](#) (P. 801)」を参照してください。
- 既存のファミリに新規クラスを追加して、システム内の分類をさらに詳細にする。たとえば、汎用サーバクラスではなく、サーバデバイスのモデルごとに別々のクラスを作成できます。詳細については、「[新規 CI クラスの定義](#) (P. 803)」を参照してください。
- 既存の拡張テーブルとその属性を使用して、新規のファミリを追加する。新規ファミリを使用すると、CI を整理または分類できます。詳細については、「[新規 CI ファミリの定義](#) (P. 803)」を参照してください。

- 既存のクラス構造やファミリ構造が要件に合わない場合は、最低限の属性セットでやり直すことができます。新しい拡張テーブルを使用して新規ファミリを追加する場合は、**Web Screen Painter** のスキーマ デザイナを使用して、新しい拡張テーブルとその属性を定義する必要があります。また、表示および更新に必要な新しいフォームも作成します。詳細については、「[新規属性フレームワークの作成 \(P. 804\)](#)」を参照してください。

重要: CA CMDB の拡張には、CA SDM と、CA CMDB データ構造およびテーブルに関する専門知識が必要なほか、**Web スクリーンペインタ (WSP)** の扱い方に慣れている必要があります。CA CMDB ファミリおよび属性を拡張する前に、**CA Services** に問い合わせることと、以降のセクションを読んで完全に理解することをお勧めします。

新規 CA CMDB 属性の追加

新規 CA CMDB 属性の追加には、入念な計画が必要です。CA CMDB には、事前定義のファミリおよびクラス内に多数の属性が用意されているので、これらの属性がニーズを満たしているかどうかを確認してから、カスタマイズを検討してください。

新規の属性が必要であると判断した場合は、以下のことを行う必要があるかどうかを検討し、大幅な追加は控えることをお勧めします。

- 既存のファミリに 1 つ以上の新規属性を追加する
- 1 つ以上のファミリに新規属性を追加する
- すべてのファミリに適用される新規の共通属性を追加する

新規の属性を追加することで、既存のファミリを拡張できます。たとえば、オフィス キャンパスの一部のデバイスが GPS 座標に割り当てられている場合は、該当する CI ファミリに `gps_coordinate` 属性を追加できます。詳細については、「[ファミリ属性の追加 \(P. 801\)](#)」を参照してください。

属性の要件を特定した後、新規ファミリおよびクラスの使用が必要であると判断した場合は、「[新規 CA CMDB ファミリまたはクラスの追加 \(P. 802\)](#)」を参照してください。

ファミリー属性の追加

Web Screen Painter のスキーマ デザイナを使用して、1 つまたは複数の既存のファミリーに新規属性を追加できます。Web Screen Painter のスキーマ デザイナにより、新規属性を含めるようにデータベースが更新され、関連付けられている CA SDM テーブルおよびファイルも更新されます。テーブルおよびファイル変更を手動で更新するよりも、この方法をお勧めします。

新規属性をファミリーに追加するには、以下の手順に従います。

1. Web Screen Painter のスキーマ デザイナを使用して、ファミリーの拡張テーブルに対応するスキーマを開きます。
2. 目的の属性を拡張テーブルに追加します。
3. 変更された拡張テーブルを発行します。

注: GRLoader およびバージョン指定では、追加操作をしなくても新規属性が自動的に取り込まれますが、ロギングを有効にすることをお勧めします。ロギングは監査目的で必要です。バージョン指定を有効にして、すべてのスナップショットを記録します。

ロギングを有効にするために、属性の UI_INFO が **AUDITLOG** に設定されていることを確認します。

新規ファミリー属性の作成後、その属性をユーザが表示および更新できるように個々の表示フォームに追加し、その拡張テーブルに固有のメタデータフォームにも追加する必要があります。詳細については、「[フォームへの属性の追加](#) (P. 807)」を参照してください。

また、バージョン指定には、列見出しおよび関連の標準 CI の属性に関する情報を含むメタデータが必要です。作成する新規属性すべてに対して、新規メタデータを定義します。詳細については、「[メタデータの作成](#) (P. 808)」を参照してください。

共通属性の追加

共通属性は、nr オブジェクトの **ca_owned_resource** テーブルに保存されます。このテーブルには、以下のカスタマイズ可能なフィールドがあります。

- smag_1
- smag_2

- smag_3
- smag_4
- smag_5
- smag_6

すべての CI ファミリの中で、必要なカスタマイズされた属性の数が 6 つ以下の場合は、これらのテーブルを使用すると便利です。

出荷時の設定では、これらのカスタム フィールドは、どのフォームにも表示されません。CA CMDB ユーザが smag_*n* フィールドを表示および更新できるようにするには、Web Screen Painter (WSP) を使用して、必要に応じて表示フォームにこれらのフィールドを追加します。すべてのログイン機能と GRLoader 機能は、すでに有効になっています。

注: Web Screen Painter のスキーマ デザインの操作手順については、CA Service Desk の「実装ガイド」の「カスタマイズ」の章、および Web Screen Painter オンライン ヘルプの「データベース スキーマのカスタマイズ」セクションを参照してください。

新規 CA CMDB ファミリまたはクラスの追加

新規 CA CMDB ファミリの追加には、入念な計画が必要です。CA CMDB には、事前定義されたファミリとクラスが多数用意されているので、これらのファミリやクラスがニーズを満たしているかどうかを確認してから、カスタマイズを検討してください。ニーズを満たしていない場合、以下のいずれかを行うことで、一部の要件は満たすことができます。

- 既存のファミリに新規クラスを定義する
- 既存の拡張テーブルを使用する新規ファミリを定義する

既存の拡張テーブルがニーズを満たしていないと判断した場合は、このセクションをスキップして「[新規属性フレームワークの作成 \(P. 804\)](#)」セクションに進み、必要な拡張テーブルおよびフォームを作成してください。

新規 CI クラスの定義

新規クラスを追加して、より高いレベルの分類の詳細度をサポートすることができます。たとえば、CA CMDB に用意されている **Hardware.Server** ファミリのクラスを使用する代わりに、別のサーバデバイスのほかのクラスを定義できます。

構成アイテム クラスを新規作成する前に、適切なクラスが [構成アイテム クラス リスト] に用意されていないかどうかを確認してください。

注: クラスの新規セットを制御するために新規ファミリも必要な場合は、このトピックを飛ばして、「[新規 CI ファミリの定義 \(P. 803\)](#)」に進んでください。これで、新規クラスの定義に戻って、新規ファミリにクラスを入力できます。

管理インターフェースを使用して CI クラスを定義するには、以下の手順に従います。

1. [構成アイテム クラス リスト] に移動します。
2. [新規作成] をクリックします。
[構成アイテム クラスの新規作成] ページが表示されます。
3. 新規クラスに、固有の名前を入力します。
4. [ファミリ] フィールドに適切なファミリ名を入力するか、フィールドの上のアイコンをクリックしてファミリを検索します。
5. [レコードステータス] フィールドが [アクティブ] に設定されていることを確認します。
6. [保存] をクリックします。

新しい CI クラスが定義され、新規 CI を作成できるようになります。

新規 CI ファミリの定義

構成アイテム ファミリを新規作成する前に、[構成アイテム ファミリ リスト] に適切なファミリがすでに存在するかどうかを確認します。存在しない場合は、既存の属性を使用して CI を整理または分類する代わりに、新規ファミリを作成できます。

必要な新規ファミリで既存の拡張テーブル（またはデフォルト テーブル）を使用できない場合は、「[新規属性フレームワークの作成 \(P. 804\)](#)」に概説されているその他の準備をすべて行います。新規の拡張テーブルを使用して、新規ファミリを定義できます。

管理インターフェースを使用して CI ファミリを定義するには、以下の手順に従います。

1. [構成アイテム ファミリ リスト] に移動します。
2. [新規作成] をクリックします。
[構成アイテム ファミリの新規作成] ページが表示されます。
3. 新規ファミリに、固有の名前を入力します。
4. [レコードステータス] フィールドが [アクティブ] に設定されていることを確認します。
5. [拡張名] フィールドで、作成するファミリのタイプを示す拡張テーブルを選択します。先ほど作成した新規の拡張テーブルを選択することもできます。

たとえば、タイプが指定されていないハードウェアのファミリを追加する場合は、「`ci_hardware_other`」を選択します。このタイプにより、クラスが新規ファミリを使用する構成アイテムを作成するときに、[属性] タブに適切な属性が表示されるようになります。[拡張名] フィールドでテーブル名を選択しなかった場合は、新規ファミリから構成アイテムを作成すると、デフォルトテーブルが使用され、デフォルト属性のみが表示されます。

6. [説明] フィールドに説明を入力します。
入力した説明は、[構成アイテム ファミリ リスト] に、参考情報として表示されます。
7. [保存] をクリックします。
構成アイテム ファミリが定義されます。

新規ファミリが定義されたので、「[新規 CI クラスの定義 \(P. 803\)](#)」に記述されているようにクラスを追加できます。

新規属性ワークフレームの作成

要件に合う既存のクラス構造やファミリ構造がない場合は、最低限の新規属性セットでやり直すことができます。これには、新規の拡張テーブルと、その他の関連する構造の作成が必要です。

CA CMDB 管理インターフェースを使用して、新規の拡張テーブルに基づいて新しい CI ファミリを定義する前に、**Web Screen Painter** のスキーマ デザイナを使用して、新規の拡張テーブルを作成します。

新規の拡張テーブルを使用するには、以下に対して HTML フォームを新規作成することも必要です。

- 新規の CI の詳細ページ
- 関連付けられている属性が表示される、新規の「属性」タブ
- 新規のメタデータ フォームとメタデータ

CA CMDB には、これらの HTML フォームの作成に使用できるテンプレートが用意されています。以降のセクションでは、必要事項について詳しく説明します。

注: Web Screen Painter のスキーマ デザイナの操作手順については、CA Service Desk の「実装ガイド」の「カスタマイズ」の章、および Web Screen Painter オンライン ヘルプの「データベース スキーマのカスタマイズ」セクションを参照してください。

CA CMDB ユーザ インターフェイスで新規フレームワークを使用するには、以下を定義します。

- 新規の拡張テーブルを使用する 1 つ以上の CI ファミリ
- CI をタイプごとに分類するための CI クラス

関連項目:

[新規 CA CMDB ファミリまたはクラスの追加 \(P. 802\)](#)

拡張テーブルの新規作成

新規拡張テーブルに基づいてファミリを定義する前に、新規テーブルでデータベースを更新し、そのテーブルに関する情報で CA CMDB スキーマを更新する必要があります。

拡張テーブルを作成するには、以下の手順に従います。

1. Web Screen Painter のスキーマ デザイナを使用して、新規の拡張テーブルと拡張名を定義します。
2. 新規拡張テーブルを保存して発行します。

注: WSP のスキーマ デザイナでは、CA CMDB にロギング トリガが自動的に作成されます。

次のセクションに進み、CI の詳細ページを作成します。

CI の詳細ページの作成

CI の詳細ページは、新規拡張テーブルに関連付けられている CI の属性表示のサポートに必要です。

CI の詳細ページを作成するには、以下の手順に従います。

1. Web Screen Painter のスキーマ デザイナを使用して、[ファイル] メニューから [新規作成] を選択し、`detail_extension.template` に基づいてフォームを作成します。
2. この新規のフォームを **`detail_extension.htmlpl`** という名前で保存します。この *extension* は、拡張テーブルの名前です。
3. 文字列 **`***EXTENSION***`** を新規拡張テーブルの名前（すでに定義済み）に置き換え、ファイルに記載されている指示に従います。
4. すべての変更を行って、ファイルを保存します。

CI の詳細ページには、以下の 2 つの属性セクションがあります。

- `cmdb_detail.htmlpl` という名前の共通属性セクション。
- `nr_cmdb_extension_tab.htmlpl` という名前のファミリー固有のセクション（[属性] タブ）。この *extension* は、新規拡張テーブルの名前です。

次のセクション「[CI の \[属性\] タブの作成](#) (P. 806)」に進みます。

CI の [属性] タブの作成

[属性] タブには、CI のファミリー固有の属性が表示されます。

[属性] タブを作成するには、以下の手順に従います。

1. Web Screen Painter のビジュアル エディタを使用して、[ファイル] メニューから [新規作成] を選択し、`nr_cmdb_extension_tab.template` に基づいてフォームを作成します。
2. このファイルを **`nr_cmdb_extension_tab.htmlpl`** という名前で保存します。この *extension* は、新規拡張テーブルの名前です。
3. 文字列 **`***EXTENSION***`** を新規拡張テーブルの名前（すでに定義済み）に置き換え、ファイルに記載されている指示に従います。
4. すべての変更を行ってファイルを保存し、発行します。

次のセクションに進み、[属性] タブをロードします。

フォームへの属性の追加

Web Screen Painter のスキーマ デザイナを使用して拡張テーブルに新規属性を作成した後、表示や更新に使用されるあらゆるフォームにその属性を追加する必要があります。ファミリー固有の新規属性の場合は、変更が必要なフォームは、**nr_cmdb_extension_tab.htmlpl** という名前の [属性] タブのみです。この *extension* は、拡張テーブルの名前です。このフォームは、すべての新規属性を含むように編集する必要があります。

属性フォームを編集するには、以下の手順に従います。

1. Web Screen Painter のビジュアルエディタを使用して、[ファイル] メニューから [開く] を選択し、該当のフォームにアクセスします。
2. 新規属性をフォームにドラッグ アンド ドロップします。

注: CA CMDB に用意されているフォームは、Web Screen Painter のビジュアルエディタを使用した編集に適していないため、[ソース] タブで Web Screen Painter のテキスト エディタを使用してください。

3. フォームを保存して発行します。

メタデータ フォームをまだ作成していない場合は、「[メタデータ フォームの作成](#) (P. 807)」セクションに進みます。フォームに新規属性のメタデータを定義するには、「[メタデータの作成](#) (P. 808)」セクションに進みます。

メタデータ フォームの作成

新規拡張テーブルには、列見出し、およびバージョン指定のための標準 CI 情報を定義するための独自のメタデータ フォームが必要です。

メタデータ フォームを作成するには、以下の手順に従います。

1. Web Screen Painter のビジュアルエディタを使用して、[ファイル] メニューから [開く] を選択し、**cmdb_metadata_extension.template** にアクセスします。
2. このファイルを **cmdb_metadata_extension.htmlpl** という名前で保存します。この *extension* は、新規拡張テーブルの名前です。
3. 文字列 *****EXTENSION***** を新規拡張テーブルの名前（すでに定義済み）に置き換え、ファイルに記載されている指示に従います。
4. すべての変更を行ってフォームを保存し、発行します。

次のセクションに進み、メタデータ フォームをロードします。

メタデータの作成

メタデータには、属性列の見出しに関する情報と、バージョン指定機能に必要な標準 CI 情報が含まれます。

重要: スナップショットでの正確なデータ、バージョン指定での適切なタイトル、標準 CI の比較の正常な実行を保証するために、メタデータには入念な計画が必要です。

メタデータを作成するには、以下の手順に従います。

1. Web Screen Painter のビジュアル エディタを使用して、[ファイル] メニューから [開く] を選択し、**cmdb_metadata_extension.htmlpl** にアクセスします。この *extension* は、拡張テーブルの名前です。
2. フォームに表示される指示に従って、新規拡張テーブルの各属性に対して、指示された行をコピーおよび変更します。

注: 以下の属性は必須ですが、メタデータは必要ありません。

- ID
- Last_modified_by
- Etc (提供予定)

3. すべての変更を保存して発行します。

メタデータを既存の CA CMDB ファミリに追加している場合は、[バージョン指定] タブに変更の監査が正しく表示されます。しかし、新規拡張テーブルに対してメタデータを定義している場合は、属性に対して新規のファミリおよびクラスを設定する必要があります。詳細については、「[CA CMDB ファミリまたはクラスの新規追加 \(P. 802\)](#)」を参照してください。

これで、新規拡張テーブルの構造が整いました。属性に対して新規ファミリを定義するには、「[新規 CI ファミリの定義 \(P. 803\)](#)」に進みます。

例

このサンプルシナリオでは、製造、出荷、レンタル輸送その他の目的でインベントリをトラッキングするために、**Automobile** ファミリと **Sedan** クラスを作成します。もちろん、ほかの **automobile** クラスの多くを作成することもできます。この例は、デモ目的でのみ提供されています。

手順 1: 拡張テーブルを新規作成する

1. Web Screen Painter のスキーマ デザイナで、[Add Extension Table] をクリックします。
2. 新規拡張テーブルの名前を入力します。この例では **vehicle** です。
拡張テーブル **zvehicle** が作成され、そのプロパティが表示されます。
注: アプリケーションに用意されているテーブルと区別できるように、新規のテーブル名にはすべて、先頭に「z」が付加されます。
3. [テーブル情報] タブで、[ファンクショングループ] フィールドを **inventory** に設定します。その他のフィールドには、デフォルト値が自動入力されます。
4. 必要に応じて、列および属性情報を新規追加します。
5. 新規拡張テーブルを保存して発行します。

手順 2: ファミリを新規作成する

ファミリを作成するには、以下の手順に従います。

1. [CI Family List] に移動します。
2. [新規作成] をクリックします。
[構成アイテム ファミリの新規作成] ページが表示されます。
3. 新規ファミリに、固有の名前を入力します。この例では **Automobile** です。
4. [レコードステータス] が [アクティブ] に設定されていることを確認します。
5. 拡張テーブル名を選択します。この例では **zvehicle** です。
6. [保存] をクリックします。
CI ファミリが新規作成されます。

手順 3: クラスを新規作成する

1. [CI Family List] に移動します。
2. [新規作成] をクリックします。
[構成アイテム クラスの新規作成] ページが表示されます。
3. 新規クラスに、固有の名前を入力します。この例では **Sedan** です。

4. 「レコードステータス」が「アクティブ」に設定されていることを確認します。
5. ファミリを選択します。この例では **Automobile** です。
6. 「保存」をクリックします。
CI クラスが新規作成されます。

手順 4: CI の詳細フォームを新規作成する

CI の詳細フォームを作成するには、以下の手順に従います。

1. Web Screen Painter のビジュアルエディタで、`detail_extension.template` フォームを開きます。
2. テンプレートを **detail_zvehicle.htmlpl** という名前で保存します。
新規フォームは、`NX_ROOT¥site¥mods¥wsp¥project¥web¥analyst` に保存されます。
3. 新規フォームで、*****EXTENSION***** のすべてのインスタンスを **zvehicle** に置き換えます。
4. 新規の CI 詳細フォームを保存して発行します。

手順 5: 属性タブを作成する

属性タブ フォームを作成するには、以下の手順に従います。

1. Web Screen Painter のビジュアルエディタで、`nr_cmdb_extension_tab.template` フォームを開きます。
2. テンプレートを **nr_cmdb_zvehicle_tab.htmlpl** という名前で保存します。
新規フォームは、`NX_ROOT¥site¥mods¥wsp¥project¥web¥analyst` に保存されます。
3. 新規フォームで、*****EXTENSION***** のすべてのインスタンスを **zvehicle** に置き換えます。
4. 必要に応じて、フォームに属性を追加します。
5. 新規の属性タブ フォームを保存して発行します。

手順 6: メタデータ フォームを作成する

メタデータ フォームを作成するには、以下の手順に従います。

1. Web Screen Painter のビジュアルエディタで、`cmdb_metadata_extension.template` フォームを開きます。
2. テンプレートを **cmdb_metadata_zvehicle.htmlpl** という名前で保存します。
新規フォームは、`NX_ROOT¥site¥mods¥wsp¥project¥web¥analyst` に保存されます。
3. *****EXTENSION***** のすべてのオカレンスを **zvehicle** に置き換えます。
4. 見出しおよび属性のプレースホルダを使用して、ファミリー固有のすべての属性のメタデータを追加します。
5. 新規のメタデータ フォームを保存して発行します。

構成監査および制御機能(CACF)

構成監査および制御機能 (CACF) は、変更管理、構成管理 (CMDDB)、検出管理の 3 つの基準を統合し、変更が正確に実行され、不正な変更が発生していないことを検証します。

変更検証は、CMDDB がすべての変更を正確に反映していることを確認するのに役立ちます。また、検出管理ツールは変更を検証します。

変更検証には、以下の利点があります。

変更管理

- 許可された変更の正常な実行の検証
- 誤って実行された変更の検出
- 不正な変更の検出
- 管理レポート
- 属性レベルまでの変更の完全監査
- 重複または競合する変更の検出

環境設定管理

- CMDB により、すべての管理対象 CI の正確な現在の状態を保持
- CI の将来の状態と変更仕様案を表示する機能
- CI の完全監査

CACF には、2 つの主なセクション、CMDB 管理インターフェース、および変更管理インターフェースがあります。以下のセクションでは、これらの詳細について説明します。

関連項目：

[CACF の管理およびポリシー定義 \(P. 813\)](#)

[管理対象属性 \(P. 830\)](#)

[管理対象変更状態 \(P. 830\)](#)

[変更仕様 \(P. 833\)](#)

[変更検証の実行方法 \(P. 838\)](#)

[監査データのアーカイブおよびパージ方法 \(P. 844\)](#)

[変更検証戦略の実装 \(P. 845\)](#)

[変更検証の計画および実装 \(P. 850\)](#)

[変更検証のベスト プラクティス \(P. 858\)](#)

[CI 属性値の更新の手動検証 \(P. 862\)](#)

[例：特定のロケーションからのみ非承認の更新を許可する \(P. 868\)](#)

[例：組織内のラップトップのアップグレード \(P. 869\)](#)

[例：検証されていない変更要求の除外 \(P. 871\)](#)

[例：一致する変更要求が存在しない場合に CI 更新を許可する \(P. 871\)](#)

[例：すべての更新を CA Configuration Automation から TWA に延期する \(P. 872\)](#)

[例：ポリシー結果をテストとしてのみログに記録する \(P. 873\)](#)

[例：CI 更新を拒否する \(P. 873\)](#)

[例：仕様なしで作成された変更要求を許可する \(P. 874\)](#)

[例：仕様なしで作成された変更要求を許可しない \(P. 874\)](#)

[例：選択されたソースからの非承認の挿入を許可する \(P. 875\)](#)

[例：実稼働以外の CI の非承認の更新を許可する \(P. 875\)](#)

CACF の管理およびポリシー定義

CMDB 管理者は、管理対象の CI と属性、およびそれらの更新ポリシーを定義します。[管理] タブの **CA CMDB** セクションにある [構成コントロール] ノードの **CACF** コンポーネントを管理します。また、変更要求、CI、インシデントフォーム、[管理] タブの [構成の監査] ノードから **CACF** 変更仕様を定義し、表示します。

管理者は、通常の変更の許可、権限のある信頼できるデータ ソースの定義、**CACF** の管理対象とする CI および CI 属性の定義について検討する必要があります。誤って実行された変更や非承認の変更（または差分）が発生した場合、**CA SDM** は新しい値を許可し、インシデントの作成または **TWA** へのデータのコピーを行って後の処理に備えます。**CA SDM** では、これらの処理のすべての組み合わせを使用できます。

重要：構成管理者は、使用する環境の[変更検証戦略を策定する \(P. 845\)](#)必要があります。変更が承認されていない場合、または変更が変更チケットに一致しない場合でも、**CACF** のデフォルト ポリシーはすべての CI への変更を許可します。

変更検証ポリシーの実装は、動的または事前にスケジュールして行うことができます。これらのポリシーは、汎用また特殊な用途向けに定義できます。変更検証ポリシーは、**CA SDM** が以下のイベントにどのように応答するかを指定します。

権限のない MDR からの更新

特定の **MDR** が特定の属性に対して権限があることを示します。権限のない **MDR** からの CI 属性の更新は、選択的に許可または拒否できます。

たとえば、一致する変更要求が存在しても、**CA Application Configuration Manager** が CI の IP アドレスを更新するのを禁止するポリシーを定義します。ソース **MDR** が **Spectrum** である場合にのみ、IP アドレスへの更新を許可します。

非承認の変更

対応する変更要求が存在しない場合、CI への更新を検出および管理します。非承認の変更による CI データの挿入、更新要求を管理するポリシーを指定します。

たとえば、「server* in New York」のような名前の CI に変更があったときのポリシーを定義し、一致する変更要求がない場合は、CI を更新する代わりに TWA ヘデータをロードします。

誤って実行された変更

変更要求が正しく [実装](#) (P. 816) されない場合に検出を行います。

監査機能は、ポリシーおよび CACF オブジェクトの定義への変更を表示する機能を構成マネージャに提供します。更新が許可されていたとしても許可されていなかったとしても、CACF は CI に対して試行された各更新をログに記録します。このログによって、どのポリシーが CI への変更を許可または却下したかを判断できます。

構成管理者は、どの変更要求ステータスが編集可能な変更を表すか、また、どの変更要求ステータスが検証状態を表すかを定義します。デフォルトでは、変更要求が RFC の変更状態にある場合に変更仕様を編集できます。また、変更要求が検証中にある場合に変更検証が実行されます。オプションで、関連する変更仕様がすべて正常に実行されたときに、変更チケットを自動的に昇格またはクローズすることができます。

重要: 構成管理者が、複数のアクティブな検証ポリシーを使用して [インシデントの作成] オプションを有効にすると、パフォーマンスが低下する場合があります。

注: デフォルトでは、CACF は、変更検証を行って変更要求の属性値の更新を正常な変更として有効にします。この変更は検証中ステータスで有効になります。構成管理者は [この動作を変更](#) (P. 830) できます。

関連項目:

[変更アナリストによる変更仕様の定義](#) (P. 815)

[変更検証](#) (P. 816)

[変更マネージャによる変更仕様の使用](#) (P. 817)

[構成監査および制御機能の動作](#) (P. 818)

変更アナリストによる変更仕様の定義

変更検証の変更管理インターフェースは、変更チケット注文フォームへ統合されています。変更アナリストは、通常、変更要求を作成するときに変更仕様を作成します。変更アナリストは、変更したい特定の CI および CI 属性に対して変更を定義します。

変更アナリストは、以下のテンプレートのいずれかを使用して変更仕様を記述できます。

- 正確な CI、CI 属性、および値
たとえば、変更が実装された後、server1 の IP アドレスを 10.10.10.10 に設定します。
- CI 属性および値。CI 名は省略
たとえば、変更の後、変更要求に添付されたすべての CI のメモリを 8 GB にアップグレードします。
- 属性が検出されない場合に設定する属性値
たとえば、変更の後、CMDB に CI がすべてニューヨークに存在すると反映します。
- 検出値を使用
たとえば、変更の前に新しい IP アドレスが不明でも、IP アドレスが変更されることは確実な場合です。権限のある MDR が検出した値を CI の IP アドレスに設定します。

変更要求が承認されるとき、変更仕様は同じ承認プロセスの一部として承認されます。仕様への以降の変更は禁止することができます。また、完全に監査されます。

変更検証

変更検証は、変更仕様に従って変更要求が実行されていることを確認するのに役立ちます。変更要求が検証中などの変更管理状態に入った後や、何らかの CI 更新が発生した場合に、検証が実行されます。このとき、任意の MDR または Web クライアントユーザからのデータが CMDB へインポートされると、CACF は受信した属性データをアクティブな変更仕様と比較します。CI 属性データが一致する場合、CACF は変更を検証します。受信データが変更要求仕様に一致しない場合、ポリシーに従って差分を修正するアクションが実行されます。

実行されるポリシーは以下のアクションのいずれかになります。

- トランザクションからの単一の属性の更新を拒否する。
- トランザクション全体（すべての属性および値のペアを含む）を拒否する。
- トランザクションの承認および検証後に処理するよう、TWA へトランザクション全体をロードする。
- 各差分を表すインシデントを作成する。

注: このアクションは、既存の通知および自動化をトリガすることができます。複数のインシデントの作成を防止するために、非承認の変更の検出では、単一の CI へのすべての非承認の変更に対して単一のインシデントのみを作成します。

- 権限のあるソース MDR からデータを受信する場合、トランザクションを無条件に許可する。

たとえば、CMDB 管理者は、実稼働サーバへの変更が誤って実行されたときにインシデントを作成するポリシーを定義できます。権限のある MDR からインポートされたデータが保留中の変更仕様に一致しない場合、CACF はインシデントを作成します。ポリシーでは、一致しないインポートデータによる CI 更新を許可または拒否できます。また、変更マネージャでは、値が計画した変更仕様と正確に一致しなくても、新しく検出された値を許可することができます。

注: 複数の検出が変更仕様の検証中に実行される場合、検出データは以前に検証された変更を無効にできます。検証の終了時、CI はすべての変更仕様が反映された状態です。

変更マネージャによる変更仕様の使用

変更マネージャは以下のアクションを実行できます。

- 各変更仕様の検証ステータスの表示と変更

たとえば、変更マネージャは、どの変更仕様が（検証待ちステータスにある）変更要求 **12345** に対して保留中かを確認します。

- 非承認または誤って実行された変更のインシデントの管理

たとえば、変更マネージャは、どの変更が検証に失敗したか、また、どの変更が追加の調査を必要とするかを確認します。

- 手動操作を必要とする変更の管理

たとえば、変更要求は、検出できない変更に対して手動検証が必要であること、また、変更アナリストがタスクを完了する必要があることを指示します。

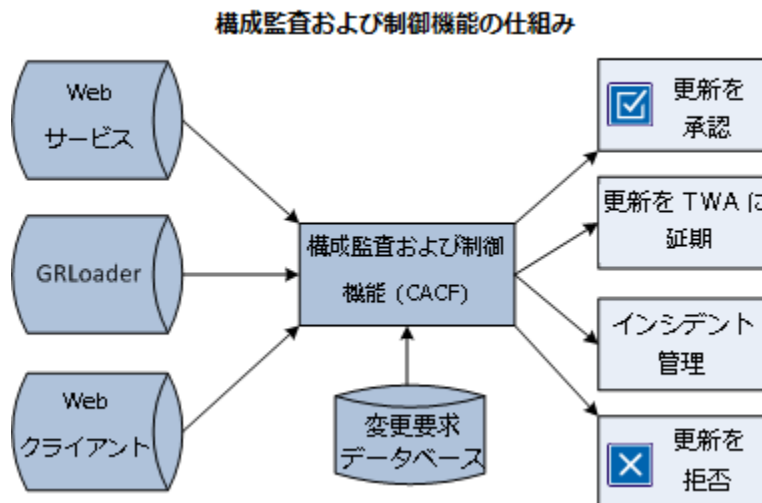
たとえば、変更マネージャは、変更要求 **12345** が **10** 個の異なる変更仕様を指定していることを調査して特定します。入力ミスのため、変更仕様番号 **9** は不正でキャンセルできます。

監査機能は、変更仕様への各更新および変更仕様への任意のオーバーライドのステータスを表示する変更機能を提供します。スコアボードは、実行中のシステムのステータスおよび操作または調査を必要とするすべての例外条件を表示します。**CA Business Intelligence** レポートは、環境の健全性を監視できるよう、構成マネージャ ポリシーの効率性を長期にわたり表示します。

構成監査および制御機能の動作

CACF は CMDB にデータをロードする前の受信 CI データを管理します。この検証は、各変更要求が正常に実行されていることを確認するのに役立ちます。また、非承認の変更を自動的に検出して管理します。構成管理者 (CMDB 管理者) は、要求された変更に対して発生したすべての差分に CA SDM がどのように応答するかを決定する検証ポリシーを定義します。

以下の図に、CACF の動作を示します。



1. 受信 CI データは、Web サービス、GRLoader、MDR、Web インターフェースからロードされ、CMDB 内の CI に対して属性の更新を要求します。
2. 構成管理者が作成した検証ポリシーに基づいて、CACF は以下のアクションを 1 つ以上完了します。
 - CACF が更新を許可し、CMDB 内の CI データを変更します。
 - CACF は後で処理するよう、TWA へ更新を延期します。
たとえば、変更マネージャが、TWA 内のトランザクションを処理します。
 - CACF はインシデントを作成し、ユーザにチケットを管理させます。
たとえば、インシデント管理プロセスは、レポート作成のためにインシデントを管理する必要があります。
 - CACF が更新を拒否します。CI データはデータベースで変更されません。

検証ポリシー

構成マネージャと変更マネージャが変更検証ポリシーを承認すると、これらの決定は **CA SDM** 変更検証ポリシーへ転記されます。システムは多くの検証ポリシーを持つことができます。CI 更新が行われると、CACF は更新された各属性に対して単一の検証ポリシーを選択します。このポリシーは、CI を更新することができます。また、一致する変更仕様がする場合に、TWA のエントリを作成したり、インシデントを作成したりすることができます。

注: Web クライアントを使用して更新をモニタする場合は、検証ポリシーで MDR クラス パターンを「Web Client」（大文字と小文字は区別されます）に指定してください。Web クライアントを使用して更新をモニタする際、このパターンの使用は英語版およびローカライズ版両方の **CA SDM** に適用されます。

重要: 環境でどのポリシーが必要かを決定するには、組織の目標とこれらのポリシーをどう適用するかを入念に検討する必要があります。

検証ポリシーの選択

CI 更新が行われると、CACF は更新された各属性に対してポリシーを選択します。この選択内容は、更新のソース、ターゲット CI、および一致する変更仕様が存在するかどうかによって異なります。複数のポリシーが一致する場合、CACF は属性更新を管理する最小のシーケンス番号を持った単一のポリシーを選択します。

注: CACF では、複数のポリシーを選択して、複数の属性を更新する単一のトランザクションを管理できます。たとえば、新しい説明および IP アドレスを持った CI の更新は、2 つの異なるポリシーをトリガできます。

各ポリシーには、CACF がポリシーの選択に使用する 4 つのセクションがあります。

ID と優先度

ポリシーを識別し、ポリシーを評価する順番を指定します。

変更要求のアライメント

属性更新がどれくらい既存の変更仕様に一致するかに基づいてトランザクションを選択します。

トランザクション フィルタ

このポリシーを適用するデータ ソースを指定します。

CI フィルタ

このポリシーを適用する CI を指定します。

これらの各フィルタをパスすれば、ポリシーは属性更新に一致します。ポリシーがトランザクションに一致しない場合、CACF はそのポリシーを無視し、システムのその他のポリシーを評価します。CACF がポリシーをすべて無視した場合、デフォルトでは CI 属性の更新が行われます。

検証ポリシーのフィルタ構文

汎用ポリシーの作成を支援するため、変更要求のアライメント、トランザクションフィルタ、CI フィルタでは、アスタリスクを終了パターン文字のワイルドカードとして許可しています。否定を示すには、これらのフィルタの先頭に感嘆符を使用します。

重要: ポリシー パターンルールは、変更仕様で計画された値ルールとは異なります。ポリシー フィルタでは、埋め込みのアスタリスク (*)、または「より大きい」(>) や「より小さい」(<) などの特殊文字を使用できません。

ポリシー フィルタは、CI 名や CI クラスなどの検証ポリシー選択パターンに対して、大文字と小文字を区別します。これらの属性で大文字と小文字を区別しないように定義していたとしても同様です。

注: 空白（フィールドで値を指定していない）のポリシー フィルタは空白の値のみに一致しますが、アスタリスクを使用したポリシー フィルタはすべての値に一致します。

以下の検証ポリシーの例では、以下の情報について考えてみましょう。

- Policy1 は、CI 名 (prod*)、属性 (IP アドレス) で一致する変更仕様が存在する場合を選択します。
- Policy2 は、CI 名 (prod*)、属性 (IP アドレス) で非承認の更新が存在する場合を選択します。
- Policy3 は、MDR (Cohesion) から CI 名 (test*)、属性 (インストール済みメモリ) を選択します。
- Policy4 は、空白の CI 名、属性 (インストール済みメモリ) を選択します。

以下のリストでは、これらのポリシーに対して起こりうる結果について説明します。

- CI (test2)、属性 (インストール済みメモリ) への更新が発生した場合、Policy3 が更新を管理します。CACF は Policy1 と Policy2 を無視します。
- CI (prod3)、属性 (インストール済みメモリ) への更新が発生し、一致する変更仕様が存在する場合、Policy1 が更新を管理します。

- CI (development4)、属性 (IP アドレス) への更新が発生した場合、一致するポリシーが存在しないため、CACF は新しい IP アドレスで CI を更新します。
- CI (prod1)、属性 (ディスク容量) への更新が発生した場合、属性 (ディスク容量) 用のポリシーは存在しません。CACF は、新しい値で CI を更新します。この例では、CACF はディスク容量属性を管理しません。
- Policy4 は空白の名前を持つ CI とのみ一致します。空白の CI 名は無効なため、変更は実行されません。

シーケンス番号による検証ポリシーの優先付け

複数のポリシーが属性更新に一致する場合、CACF は最小のシーケンス番号を持ったポリシーを選択します。以下のポリシーとそのシーケンス番号について考えてみましょう。

- ポリシー名 (Policy1)、シーケンス (1000)、CI (prod*)
- ポリシー名 (Policy2)、シーケンス (2000)、CI (prod-NY*)

CI (prod1) への更新が発生した場合、Policy1 がトランザクションを管理します。CI (prod-NY-1) への更新が発生した場合も、シーケンス番号が少ないため、Policy1 がトランザクションを管理します。この例では、Policy2 は有効になりません。

以下のポリシーの例で示すように、最も特殊なポリシーがより少ないシーケンス番号を持つようにシーケンス番号を変更することを推奨します。

- ポリシー名 (Policy1)、シーケンス (2000)、CI (prod*)
- ポリシー名 (Policy2)、シーケンス (1000)、CI (prod-NY*)

CI (prod1) への更新が発生した場合、Policy1 がトランザクションを管理します。CI (prod-NY-1) への更新が発生した場合、シーケンス番号が少ないため、Policy2 がトランザクションを管理します。

変更要求のアライメント

ポリシーは、CI 属性の更新がどれくらい変更仕様に一致するかに基づいてフィルタを行います。CI の更新後、CACF は CI とその属性名の両方に一致する変更仕様を検索します。この検索では、変更仕様を検証できます。この変更要求のアライメントは、以下のような場合に実行されます。

- この属性と CI に対する変更仕様が存在する。
- この CI に対する（変更仕様を含まない）変更要求が存在する。

- 新しい CI を示す非承認の挿入トランザクションが発生する。CI に添付された変更要求はなし。
- 既存の CI を示す非承認の更新トランザクションが発生する。CI に添付された変更要求はなし。

変更要求が、変更検証がアクティブになる変更状態にある場合のみ、一致する変更要求が検索されます。クローズ、非承認、未スケジュール、または実行されていない変更要求は、一致する変更要求の検索対象になりません。

CACF は、トランザクションの変更要求のアライメントを決定した後、対応するポリシーの検索を実行します。ポリシーは、1 つ以上の変更要求のアライメントのタイプを管理できます。

仕様がある変更要求

CI および既存の属性名の更新を指示する変更仕様がある変更要求を示します。

変更要求(仕様なし)

CI の更新を指示する変更仕様がない変更要求を示します。

非承認の挿入

定義によって、検証状態で一致する変更要求がない挿入された CI を示します。

重要：非承認の挿入を禁止するポリシーでは、管理対象属性の *名前* または *任意の管理対象属性* を指定する必要があります。名前にはアクティブな管理対象属性を指定します。

CACF は、トランザクションに管理対象外の属性のみが含まれている場合、常に非承認の挿入を許可して更新を行います。

非承認の更新

検証状態で一致する変更要求がない更新された CI を示します。

関連項目：

[例：仕様なしで作成された変更要求を許可する \(P. 874\)](#)
[属性への非承認の変更の防止 \(P. 855\)](#)

例: 変更要求のアライメント ポリシー

以下のポリシーの例では、変更要求のアライメントを指定します。

- ポリシー名 (legacy) は、CI (*)、属性 (任意の管理対象属性)、アライメント (変更要求 (仕様なし))、アクション (属性更新を許可) をフィルタします。
- ポリシー名 (new) は、CI (*)、属性 (任意の管理対象属性)、アライメント (変更要求 (仕様あり))、アクション (変更仕様に一致する場合にのみ更新を許可) をフィルタします。
- ポリシー名 (no-rogue) は CI (*)、属性 (任意の管理対象属性)、アライメント (非認証の挿入、非認証の更新)、アクション (常にトランザクション全体をキャンセル、インシデントの作成) をフィルタします。

これらの例では、以下の機能が提供されます。

- ポリシー (legacy) は、CACF の実装前に行ったため変更仕様がない CA SDM r12.6 変更要求を許可し、CI を更新します。
- ポリシー (new) は、一致する変更仕様があるすべての新規変更要求に対して変更検証を実施します。
- ポリシー (no-rogue) は、検証がアクティブな状態の変更要求がない場合に CI への更新を禁止します。

トランザクション フィルタ

ポリシーは、[属性名、MDR 名、MDR クラス、および更新を実行するユーザの役割](#) (P. 821)などのトランザクションのソースに基づいてトランザクションをフィルタします。

注: Web インターフェースからログオンしたユーザのみをフィルタする場合は、MDR クラスにキーワード「**Web Client**」を指定します。連絡先のユーザ ID には、MDR 名を指定します。ユーザを識別する方法は、検証ポリシーにのみ適用されます。製品のその他の部分では使用できません。

例: トランザクション フィルタ

以下のポリシーの例で、トランザクション フィルタを指定します。

- ポリシー名 (root_access) は、CI (*)、属性 (任意の管理対象属性)、役割 (管理者)、アクション (属性更新を許可) をフィルタします。
- ポリシー名 (cohesion_not_authorized) は、CI (*)、属性 (IP アドレス)、MDR クラス (Cohesion)、アクション (古い属性値を保持) をフィルタします。
- ポリシー名 (john) は、CI (user1*)、属性 (任意の管理対象属性)、MDR 名 (user1)、MDR クラス (Web Client)、アクション (属性更新を許可) をフィルタします。

これらの例では、以下の機能が提供されます。

- ポリシー (root_access) は、管理者アクセスを持ったすべてのユーザにすべての値の更新を許可します。このタイプのポリシーには、少ないシーケンス番号を設定することを推奨します。
- ポリシー (cohesion_not_authorized) は、MDR クラス (Cohesion) のすべての MDR が、フィルタされた CI の IP アドレスで更新されるのを防ぎます。この例では、権限のない MDR がデータを更新するのを防ぐ方法を示します。
- ポリシー (user1) は、Web クライアントを使用した場合のみ、user1 に連絡先が所有する CI の更新を許可します、この例では、特定のユーザにそれらのデータに対するフル コントロールを与える方法を示します。

CI フィルタ

ポリシーは、更新された CI の特徴に基づいてトランザクションのフィルタを行います。この選択条件には、CI 名、クラス、優先度、サービスタイプ、および場所が含まれます。

重要: CI フィルタは、更新が発生する前の CI の属性値に基づいて行われます。受信したトランザクション データの値ではありません。

例: CI フィルタ ポリシー

以下のポリシーの例で、CI フィルタを指定します。

- ポリシー名 (**priority1**) は、サービス タイプ (解決 (優先度 1))、アクション (変更仕様に一致する場合にのみ更新を許可、インシデントの作成) をフィルタします。
- ポリシー名 (**prod-NY**) は、CI (**prod***)、場所 (**NY**)、属性 (任意の管理対象属性)、アクション (変更仕様に一致する場合にのみ更新を許可) をフィルタします。
- ポリシー名 (**prod-not-NY**) は、CI (**prod***)、場所 (**!NY**)、属性 (任意の管理対象属性)、アクション (属性更新を許可) をフィルタします。

これらの例では、以下の機能が提供されます。

- ポリシー (**priority1**) に変更要求が一致するには、サービス タイプ「解決 (優先度 1)」を持った CI が必要です。このポリシーは、CMDB 内で最も重要な CI を高度に制御するのに役立つベストプラクティスです。また、このポリシーを完了するには、変更管理下のすべての変更に対して変更仕様があることを検証する必要があります。
- ポリシー (**prod-NY**) に変更要求が一致するには、場所「NY」に CI が存在する必要があります。ポリシーのフィルタに場所を使用すると、サイト間を基準として変更検証を徐々に実装するのに役立ちます。
- ポリシー (**prod-not-NY**) には、場所パターンで CI が NY に存在していないことを指定する場合の感嘆符の使用例を示します。

ポリシー アクション

CACF がポリシーを選択した後、ポリシーのアクション セクションで属性更新の結果が決定されます。このセクションでは、**CMDDB** の整合性に影響する検証ポリシーの最も重要な部分を指定します。このセクションは、変更管理ワークフロー、関連する通知、および作成したインシデントにも影響します。

ポリシーには、以下のいずれかの更新動作があります。

変更仕様に一致する場合にのみ更新を許可

変更仕様に一致する場合という条件付きで、受信した属性の更新を **CI** に適用します。この更新は、変更要求で検証がアクティブな状態にある場合に実行されます。このオプションを選択すると、変更検証が有効になります。

属性更新を許可

受信した **CI** への属性更新を無条件に適用します。このオプションは、すべての変更検証を実質的に無効にします。権限のある信頼できるデータ ソースがあり、変更要求を必要としない場合、通常の変更に対してこの動作を使用します。

常にトランザクション全体をキャンセル

一致する変更仕様が存在する場合でも、このトランザクションによる更新およびその他の属性更新をキャンセルします。この動作は、更新の権限がない **MDR** による **CI** の更新を禁止するために使用します。任意のポリシーがトランザクションをキャンセルすると、別のポリシーで変更が許可されていたとしても、トランザクション全体がキャンセルされます。

たとえば、権限のない **MDR** による **CI** の挿入や名前など共通の属性名の指定を禁止するためにこの動作を指定します。

古い属性値を保持

単一の属性更新をキャンセルしますが、トランザクションによるその他の属性の更新を許可します（ポリシーが許可している場合）。**MDR** に属性レベルの権限がない場合に、この動作を使用します。

検証ポリシーでは、失敗した検証を修正する場合に、インシデントを自動的にクローズするよう指定できます。ポリシーには、受信したトランザクションデータを **TWA** にコピーするよう指定できます。このタイプのポリシーは、権限のない **MDR** からのデータを **CMDB** の更新前に確認する必要がある場合に役立ちます。

構成マネージャに **TWA** レコードを作成した **CACF** ポリシーを識別させるために、**TWA** の「変更要求」フィールドはそれを作成したポリシーの名前に設定されます。**TWA** へのデータの書き込みは、**CMDB** 内の **CI** の更新とは関係ありません。したがって、ポリシーは **CI**、**TWA** への書き込み、またはその両方を更新できます。

ポリシーのスケジュール設定

検証ポリシーの有効化と無効化の日付を指定できます。構成管理者は、ポリシーの自動変更をスケジュールすることができます。

複数のポリシー

より多くの検証ポリシーを環境に導入して、より多くの属性を管理するようになると、ポリシー間でより多くの重複が存在するようになり、ポリシーの管理が次第に煩雑化します。たとえば、サーバ **CI** 用に 1 つのポリシーがあり、**NY** の **CI** 用に別のポリシーがあるとします。この場合、**NY** のサーバ **CI** 用の適切なポリシーを検討する必要があります。複数のポリシーが単一の属性に対して制御を行う可能性がある場合、ポリシーのシーケンス番号を使用して 1 つのポリシーを優先させることができます。より多くの属性を管理するようになると、より多くのポリシーで単一のトランザクションを管理する可能性は増加します。

単一のトランザクションに対しての複数のアクティブなポリシーがある場合は、以下の点に注意してください。

- 選択されたポリシーが **TWA** へのデータの書き込みを要求する場合、データは **TWA** にも書き込まれる。
- 選択されたポリシーがトランザクションのキャンセルを要求する場合、**CACF** はトランザクション全体をキャンセルする。

重要： createAsset Web サービス（GRLoader と CMDBf を含む）を使用する機能は、トランザクションを 3 つの個別のトランザクション、2 つの挿入、および 1 つの更新に分割します。**CI** 拡張テーブルへの更新がキャンセルされても、**ca_owned_resource** への更新が許可される場合があります。拡張テーブル内の **CI** ファミリ固有の属性への更新は、挿入ではなく更新として検出される場合があります。

例：複数のポリシー

以下の例では、複数のポリシーを指定します。

- ポリシー名 (IP Address)、属性 (IP アドレス)、アクション (属性更新を許可)
- ポリシー名 (Memory Installed)、属性 (インストール済みメモリ)、アクション (トランザクションをキャンセル)
- ポリシー名 (Disk Capacity)、属性 (ディスク容量)、アクション (古い属性値を保持)

これらの例では、以下の機能が提供されます。

- トランザクションが IP アドレスのみを更新する場合、更新が実行されます。
- トランザクションがインストール済みメモリのみを更新する場合、更新は実行されません。
- トランザクションが IP アドレスとインストール済みメモリの両方を更新する場合、トランザクションは Web インターフェースでキャンセルされます。
- トランザクションが Web インターフェース内の [IP アドレス] と [ディスク容量] の両方を更新する場合、[IP アドレス] は更新され、[ディスク容量] は更新されません。
- トランザクションが Web インターフェース内の [IP アドレス] と [インストール済みメモリ] の両方を更新する場合、どちらの属性も更新されません。

インシデントの統合

検証ポリシーがインシデントの作成を要求した場合、CACF は以下のようにオープン インシデントの数を減らすことができます。

- CACF は、単一の CI への非承認の変更に対して、オープン インシデントを 1 つのみ作成します。その他の非承認の変更は、非承認の変更に対して作成された単一のオープン インシデントを更新します。
- CACF は、各変更仕様の検証エラーに対して、オープン インシデントを 1 つのみ作成します。その他の変更仕様の検証エラーは、オープン インシデントを更新します。

管理対象属性

管理対象属性は、CACF による変更検証の適用対象となる CI 属性を示します。デフォルトでは、このリストには CI 名と任意の管理対象属性が含まれます。変更検証戦略の一部として、管理したい CI 属性を追加します。[管理] タブの CA CMDB セクションにある [構成コントロール]、[管理対象属性] ノードで、管理対象属性を変更検証戦略の一部として定義します。

CACF は、管理対象外の属性（リストに含まれていない属性）に対して変更検証を行いません。管理対象外の属性は、通常どおり更新されます。

重要: 変更検証は、検証ポリシーで [常にトランザクション全体をキャンセル] 動作を指定しない限り、管理対象外の属性を無視し、CI の更新を許可します。

注: CACF が変更仕様の計画値を受信した CI トランザクションデータと比較する場合にのみ、管理対象属性の定義内の大文字と小文字は区別されます。大文字と小文字の区別は、ポリシーの選択パターンには適用されません。常に大文字と小文字が区別されます。

CI 属性名のリストについては、CA CMDB の「テクニカルリファレンスガイド」を参照してください。

管理対象変更状態

CACF は、どの変更要求ステータスを CACF が管理するかを指定するために管理対象変更状態を使用します。CACF は、管理対象変更状態を使用して、システムに対する CI 更新の変更検証を適用する方法または時期を制御します。これらの変更状態は、組織の要件に応じてカスタマイズできます。

管理対象変更状態は、CA CMDB の[管理]タブにある[構成コントロール]、[管理対象変更状態] ノードで設定します。

注: CACF は、[管理対象変更状態] にリスト表示される変更要求と変更要求状態を無視します。

以下のリストでは、[管理対象変更状態]のオプションについて説明します。

変更仕様は編集可能

変更要求の変更仕様を編集可能にするかどうかを指定します。通常、変更要求が承認された後は要求を変更できません。また、更新は検証中状態の少数のオーバーライドオプションによる実行に制限されます。

変更検証はアクティブ

変更要求がこのステータスの場合に、CIで検出された変更に対して変更検証を行うかどうかを指定します。変更要求および関連する変更仕様は、それらが正常に実行されたことを検証するために任意の受信トランザクションと比較されます。

CACFは、すべてのCIの管理対象属性値への変更をすべて監視します。CACFは、CIの各属性レベルの変更を検証し、それを変更検証がアクティブな状態にある変更仕様のリストと比較します。

変更仕様がこの状態に入ると、特定のCIのないすべての変更仕様が拡張されます。変更要求に添付されたCIのリストを使用して新しい変更仕様を作成される場合に、この拡張が発生します。

変更仕様がこの状態を終了すると、[変更の実行後に設定]の検証ステータスを持った変更仕様のリストが実行されます。このアクションは、各変更仕様で指定した計画値でCIを更新します。

実装状態

変更がCIに対して実行または実装されている状態を表すかどうかを指定します。変更要求がこの遷移状態に入った場合、CIの属性値は一時的なもので、保留中の変更仕様の要求によって更新されることがあります。CACFはこれらの非承認の変更を行いませんが、検証結果に対する変更も行いません。通常、変更検証プロセスは、変更要求の実行が完了した後に、受信した属性データの比較のみを行います。

変更仕様のオーバーライド ボタンを表示

変更アナリストに変更仕様を制御可能にするかどうか、また、どの制御レベルを与えるかを指定します。一部の实装では、変更アナリストは必要に応じて変更仕様を編集することができます。その他の実装では、変更アナリストは変更仕様を[オーバーライド](#) (P. 842)または[キャンセル](#) (P. 843)できます。

検証後に変更要求を推奨

CACF がすべての変更仕様を検証した後に、変更要求を次のデフォルト状態に自動的に昇格するかどうかを指定します。

デフォルトの管理対象変更状態

変更仕様が作成、上書き、検証、無視されたときの変更要求の状態を定義できます。

以下のリストでは、例として、**CA SDM** によって提供されるデフォルトの管理対象変更状態の定義について説明します。

RFC

この状態では、変更要求の仕様を定義します。ただし、変更検証は行われません。変更要求がこの状態の場合に検出された **CI** への変更は、通常、非承認と見なされます。

承認中

この状態の変更仕様は **RFC** と同じ特徴を持ちます。編集は可能ですが、検証は行われません。

変更要求の承認後、変更仕様は同じ承認プロセスの一部として承認されます。**CACF** は、仕様への追加変更を禁止し、完全な監査を行います。

実装中

CI への変更が行われます（非認証または検証中でない場合）。この状態の変更要求に対して検証を実行する場合は、この変更状態の定義を変更します。

確認中

変更仕様は編集できません。ただし、アナリストは変更仕様をオーバーライドすることができます。この状態では、[変更検証はアクティブ](#) (P. 838)です。

変更仕様

変更要求には、CI に対して要求される特定の CI の変更を定義する変更仕様が含まれます。変更要求が検証状態に入ると、CACF は変更仕様を使用して、CI への実際の変更が正常に完了したことを検証および確認します。変更要求、CI、または「管理」タブの CA CMDB セクションにある「構成コントロール」、[変更仕様] ノードから変更仕様を作成します。

変更仕様には、以下の主なセクションがあります。

変更要求番号

変更をリクエストする変更要求を指定します。

CI 名

更新する CI の名前が含まれます。

[CI 名] フィールドを空白のままにすると、変更仕様を変更要求に定義されたすべての CI に適用することができます。このオプションは、変更要求の対象となるすべての CI が同じ管理対象属性と計画値を使用している場合に使用します。変更仕様は、変更要求ステータスが管理対象変更状態から変更検証がアクティブな状態に遷移したときに、変更要求に添付されたすべての CI に対して適用されます。

属性名

更新する管理対象属性の名前を指定します。

[任意の管理対象属性] を選択すると、任意の管理対象属性を変更要求の検証中に変更できます。この場合、複数の属性を更新できるため、計画値は指定できません。

計画値

変更を実行した後の属性の期待値を指定します。変更要求が検証状態へ移行し、CI が Web インターフェース、GRLoader または Web サービスによって更新された後、CACF は、一致を判断するために計画値を受信データと比較します。

正確な値が不明な場合は、計画値に[特殊文字](#) (P. 834)を埋め込むことができます。

ステータス

[検証保留中] などの[変更仕様のステータス](#) (P. 840)を指定します。

計画値が不明でも値が変更される可能性がある場合は、[検出値を使用]に変更仕様のステータスを設定できます。この動作では、CACF が変更仕様を検証する前に、CI の更新を検出する必要があります。計画値にアスタリスクを使用できない数値フィールドや SREL では、この動作が必要です。

計画値の設定に役立つよう、[検出された属性履歴]タブには MDR によって最近検出されたすべての値がリスト表示され、実際に許可されているか、または CMDB へロードされているかを判断できます。ユーザが適切な計画値パターンを決定できるよう、このタブには、形式、大文字と小文字の区別、および値に関するその他の情報が表示されます。

関連項目：

[特殊文字](#) (P. 834)

[一括ロードの定義](#) (P. 836)

[一括変更の定義](#) (P. 836)

[CI バージョン指定および将来の状態](#) (P. 838)

特殊文字

正確な値が不明な場合、特殊文字を埋め込むことができます。アスタリスクのワイルドカードを使用すると、任意の数の文字と一致します。パターンは、検出されたデータに同じ順番で一致する必要があります。また、スペースは重要です。

たとえば、計画値として「10.*.*」を入力し、10 から始まるすべての IP アドレスに一致させます。または、2 つのピリオドの間に任意の値を入力します。

たとえば、受信する server_type の値に「Windows 2003 (WIN32) 5.2.Service Pack 2 (Build 3790) Intel x86」が含まれるとします。この値を検証するには、変更仕様で計画値に「*Service Pack 2 *」を指定します。

計画値の先頭の単語は、検出値がその値で始まる必要があることを示します。同様に、計画値の先頭と末尾のアスタリスクは、検出値が任意の値で開始および終了することを示します。

以下の表に、アスタリスクの使用例を示します。

計画値	検出値	一致または一致なし
a	b	一致なし
a	a	一致
a	aba	一致
a	bab	一致
a*	a	一致
a*	ab	一致
a*	ba	一致なし
*a	a	一致
*a	ab	一致なし
*a	ba	一致

感嘆符で始まるパターンは、値の否定になります。感嘆符は、パターン内の最初の文字としてのみ使用できます。たとえば、10.!.*.*.のパターンは使用できません。

文字列値内に含まれている数値を比較するには、計画値の最初の文字として大なり記号(>)または小なり記号(<)を使用します。先頭に感嘆符がある場合は、2番目の文字にする必要があります。

重要: CACF は、検出値や計画値のパターン内の先頭または末尾の非数値を無視します。

以下の表では、感嘆符、大なり記号、および小なり記号の使用方法についての例を示します。

計画値	検出値	一致または一致なし
>200	aaa 201 bbb	一致
>200GB	aaa 200 bbb	一致なし
>200GB	300 GB	一致
!<200GB	200 バイト	一致

計画値	検出値	一致または一致なし
!<200	200 ビット	一致

計画値が不明でも値が変更される可能性がある場合は、[検出値を使用]に変更仕様のステータスを設定できます。この動作では、CACFが変更仕様を検証する前に、CIの更新を検出する必要があります。計画値にアスタリスクを使用できない数値フィールドやSRELでは、この動作が必要です。

計画値の設定に役立つよう、[検出された属性履歴]タブにはMDRによって最近検出されたすべての値がリスト表示され、実際に許可されているか、またはCMDDBへロードされているかを判断できます。ユーザが適切な計画値パターンを決定できるよう、このタブには、形式、大文字と小文字の区別、および値に関するその他の情報が表示されます。

一括ロードの定義

新しいCIを、それらのCIを定義した変更要求を最初に作成せずに管理すると、CMDDB環境内で問題が発生します。多数のCIを定義する場合は、以下の情報を考慮してください。

- ユーザID、MDR、または役割によって制限された非承認の挿入を正常に完了するよう許可する特殊な一括ロードポリシーを定義します。
- すべての新規CIを検証や後で処理するようTWAに再ルーティングする特殊な一括ロードポリシーを定義します。このアクションには、既存の特殊な一括ロードポリシーも必要です。

一括変更の定義

多数のCIへの同一の変更（CIの収集のためのロケーションを変更する場合など）を定義するには、以下の手順に従います。

1. 変更要求を作成します。
2. 変更を説明する1つの変更仕様を定義し、CI名は空白のままにします。
3. すべてのCIを変更要求に添付します。

実装の前に変更の正確な詳細がわからない場合（たとえば、新しいサーバを取得したが、CI名しかわからない場合）は、以下の手順に従います。

1. 変更要求を作成します。
2. 属性名として「任意の管理対象属性」を指定する変更仕様を作成します。
3. 計画値は不明なため、空のままにします。
4. 変更管理プロセスを使用してチケットを移動します。
5. 変更要求が、検証がアクティブな状態にあるときに検出が実行された場合は、受信 CI データが CI にロードされます（ポリシーで許可されている場合）。
6. CI に対するすべての検出が完了したら、変更マネージャは変更仕様を手動検証としてマークする必要があります。

多数の CI に対する異なる変更が多く存在する場合には、以下の手順に従います。これはたとえば、複数のサーバをあるロケーションから別のロケーションに移動すると同時に、各サーバに一意の IP アドレスを割り当てる場合などです。

1. 変更要求の作成
2. スプレッドシートを作成し、各行に変更要求番号、CI、および新しい属性値をリストします。各行が個別の変更仕様になります。
3. スプレッドシートを GRLoader でロードして、必要な変更仕様を作成します。
4. 変更要求とその変更仕様を通常どおりに昇格させます。

注: GRLoader の使用方法の詳細については、CA CMDB の「テクニカル リファレンス ガイド」を参照してください。

CI バージョン指定および将来の状態

CI の詳細フォームの [バージョン指定] タブで変更仕様を表示すると、詳細情報が提供され、変更要求とそれに対応する変更仕様を識別できます。このタブには、その変更が適用されたかのように、CI の将来の状態も表示されます。変更要求のスケジュールされた日付の時点における CI のスナップショットが表示されます。変更要求がまだスケジュールされていない場合は、スケジュールされていない変更として表示されます。

バージョン指定には、以下のような機能があります。

- 重複した変更仕様や競合する変更仕様をすばやく識別します。
- 詳細ビューの [MDR] 列にある変更要求リンクをクリックすることによって、変更仕様を直接起動したり、対応する変更の詳細を表示したりすることができます。
- スケジュールされていない変更を示すスナップショットは、指定されていない将来のある時点にスケジュールされている変更を示します。
- 変更要求番号は、スナップショット ラベルの右側に示されている各変更仕様と共に表示されます。
- 情報テキストは下部のペインに表示され、変更仕様に関する以下の情報をホバー テキストとして示します。
 - 変更要求番号
 - スケジュール済みの変更の日付（変更要求でスケジュールされた日付が指定されている場合）
 - 締め切り日（変更要求で締め切り日が指定されている場合）

変更検証の実行方法

ユーザが CI への保存を要求すると、CA SDM は、すべての一致を検索するときに適用可能な変更仕様を検索します。以下の情報は、適用可能な変更仕様について説明しています。

- 変更仕様内の CI は、保存される CI と同じです。
- 変更要求は、[変更検証はアクティブ] の状態で定義された管理対象変更状態にあります。
- 変更仕様内の属性は、更新される属性と同じです。

- 変更仕様はアクティブです。
- 更新されている管理対象属性や有効なポリシーが存在しない場合、保存は制限なく続行されます。

受信データの値が変更仕様に正確に一致する場合、CACF は、その変更仕様を検証済みと見なします。ポリシーによっては、検証時に、変更検証で作成されたインシデントがすべてクローズされます。

検証は、変更要求およびベースとなるすべての変更仕様を検証されている間に、Web クライアント、Web サービス、または GRLoader からの情報によって CI が更新されたときに実行されます。変更要求に対するすべての検証が完了すると、変更要求は必要に応じて、次の変更要求状態に自動的に昇格できます。

受信データの値が変更仕様内の値に一致しない場合は、誤って実装された変更または失敗した変更とみなされ、ポリシーに応じて、インシデントが作成されるか、またはインシデントに追加されます。

たとえば、CA SDM では適用可能な変更仕様が検索されませんが、変更要求が、変更検証がアクティブな状態で存在します。これらの変更要求はターゲット CI を指定しますが、変更仕様を含んでいません。CACF は、仕様がない変更要求を処理するポリシーでこの変更を管理します。

- 適用可能な変更仕様や仕様がない変更要求が存在しない場合、保存操作は非承認とみなされます。
- すべての属性が処理されると、受信データを要求したポリシーはすべて TWA トリガに書き込まれます。

関連項目：

[変更仕様の管理](#) (P. 840)

[変更仕様のステータス](#) (P. 840)

[失敗した検証の管理](#) (P. 842)

[検出不可能な属性の管理](#) (P. 843)

変更仕様の管理

変更が実行または実装された後、変更要求は **CACF** で管理される変更状態に入ります。この変更状態では変更検証がアクティブに設定されます。変更要求がこの状態にある場合、**CACF** は関連するすべての **CI** アクティビティを確認し、各変更仕様のステータスをスコアボードにレポートします。

スコアボードは、必要な変更が正しく実行されたことを確認したり、変更要求によって要求された手動検証を実行したりするために、変更マネージャによって使用されます。

変更要求に対するすべての検証が完了した後、変更要求は必要に応じて、すべての変更仕様が自動的に非アクティブとマークされる次の変更要求状態（通常は「クローズ」）に自動的に昇格することができます。

変更仕様のステータス

変更仕様は、ステータスを使用して、実行する検証のタイプや検証の現在の状態を示します。これらのステータス値は、検証プロセス中に変更検証操作を記録する際に検証ログでも使用されます。

初期ステータス

変更仕様の作成時に、**CACF** で実行する検証のタイプを指定するために使用されます。これらのステータスは最終ではなく、変更仕様がこれらのいずれかのステータスにある場合、変更要求は検証済みとはみなされません。

検証保留中 - 変更仕様が検証されていないか、または変更が **CI** 更新を待機しています。

手動検証が必要 - 変更要求に対する変更が検証されるときに、手動検証が必要になります。

検出値を使用 - 検証時に検出値を **CI** にコピーします。検証前に計画値が不明な場合に使用します。

変更の実行後に設定 - 検証が完了した後、**CI** 属性を計画値に設定します。このステータスは、**CI** 属性が検出可能でないときに、その属性を設定するために使用します。たとえば、変更が完了した後、**CI** の主要連絡先を **User1** に設定します。

最終ステータス

完了した変更仕様を示し、最終とみなされます。すべての変更仕様がこれらのいずれかの最終状態に入ると、変更要求は、次のデフォルト状態への昇格の対象になります。

検証済み - 変更仕様が正常に検証されました。

手動で検証済み - 変更仕様が手動で検証されました。

検出値を使用 - CI が検出値で更新されました。

計画値に設定済み - 変更要求の検証の後、CI が計画値で更新されました。

計画値を承認済み - CI が計画値で更新され、検証中に上書きされました。

検出値を承認済み - CI が最後の検出値で更新され、検証中に上書きされました。

変更なし - 検証時に計画値が CI に一致し、検証は必要ありませんでした。

キャンセル - 変更仕様が変更マネージャによって [キャンセルされました](#) (P. 842)。

操作ステータス

変更仕様に、検証のための手動操作が必要なことを示します。CA SDM は、これらのステータスをリスト フォームに赤色で強調表示します。これらのステータスは最終ではなく、変更仕様がこれらのいずれかのステータスにある場合、変更要求は検証済みとはみなされません。

検証失敗 - 検出で発見された値が、変更要求で指定された値と異なります。変更アナリストは、変更は正しく実行されたが変更要求が誤って指定されたのか、または変更要求は正しく、変更により再び検証が必要なのかどうかを判断する必要があります。管理対象変更状態の定義や現在の変更要求ステータスに応じて、変更アナリストは、失敗した変更仕様をオーバーライド、変更、またはキャンセルすることができます。

手動検証が必要 - 変更仕様を最終とマークできるようにするには、その前に手動検証が必要です。

アクション オーバーライド ステータス

変更検証中に開始するアクションを示します。これらのステータスは最終ではなく、変更仕様がこれらのいずれかのステータスにある場合、変更要求は検証済みとはみなされません。

計画値の承認 - CI 属性を計画値でオーバーライドすることを要求します。

検出値の承認 - CI 属性を最後の検出値でオーバーライドすることを要求します。

レポート ステータス

検証ログがログ記録の目的で表示し、変更仕様では使用されないポリシー操作の結果を示します。

更新を許可 - ポリシーによって CI を更新するための要求が許可され、そのポリシーはどの変更仕様にも一致しませんでした。

失敗した検証の管理

検証が失敗した場合は、スコアボード内の [CMDB]、[構成の監査]、[検証失敗] ノードに、失敗した検証と手動の操作が必要な変更仕様の数が赤色で表示されます。変更仕様は、[変更要求]、[構成アイテム] または [管理] タブの [変更仕様] タブでも表示できます（検証ステータスは [検証失敗]）。検証が失敗した場合、変更アナリストは操作を行うか、または次の検出が実行されるまで待機することができます。

管理対象変更状態で [変更仕様のオーバーライド ボタンを表示] アクションが許可されている場合、変更アナリストは変更仕様を開いてデータを確認し、以下のいずれかのオプションをクリックすることにより、検証を最終状態に移行してクローズすることができます。

検出値の承認

アナリストは、変更仕様は正しくなく、検出ツールが正しい値を検出したと判断します。

計画値の承認

アナリストは、検出ツールが間違っているか、または検出を実行しなかったと判断し、正しく検出されたかのように計画値を受け入れます。

キャンセル

変更要求のこの部分は実行されず、この仕様はキャンセルされます。

検出不可能な属性の管理

変更仕様に手動検証が必要な場合、構成アナリストは変更を手動で検証する必要があります。スコアボード内の[CMDB]、[構成の監査]、[手動操作]ノードに、手動の操作が必要な変更仕様の数が赤色で表示されます。変更仕様は、[変更要求]、[構成アイテム]または[管理]タブの[変更仕様]タブでも表示できます（検証ステータスは[手動検証が必要]）。

管理対象変更状態で[変更仕様のオーバーライド ボタンを表示]アクションが許可されている場合、変更アナリストは変更仕様を開いてデータを確認し、以下のいずれかのオプションをクリックすることにより、検証を最終状態に移行してクローズすることができます。

検証済みとしてマーク

属性を検出できず、手動で検証された場合に使用されます。

キャンセル

変更要求のこの部分は実行されず、この仕様はキャンセルされます。

監査データのアーカイブおよびパージ方法

定期的なデータベース メンテナンスの一部として、古くなった検証ログ エントリ、CACF 監査履歴、および CI 監査履歴をアーカイブおよびパージすることをお勧めします。

重要： CACF CA Business Intelligence は通常、年単位の概要を含む現在の月単位レポートを作成します。ログ、CACF 監査履歴、および CI 監査履歴テーブルに対するアーカイブ パージルールのデフォルトのアーカイブ パージ時間の値は 30 日です。検証ログ エントリ、インシデント、および変更要求の間のデータの整合性を確保するために、アーカイブとパージのルールで同じ値を使用します。レポート要件に応じて、30 日のデフォルト値をより大きな値に変更することもできます。

監査データをアーカイブおよびパージするには、以下の操作を実行します。

1. 現在の「インシデント」ルールを使用して、*nn* 日より古い非アクティブなインシデントをアーカイブおよびパージします。

CA SDM は、関連付けられたインシデントをアーカイブおよびパージした後でのみ、検証ログ エントリをアーカイブおよびパージします。変更要求をインシデントに関連付けた場合、CA SDM は、その変更要求がアクティブかどうかを確認しません。

2. 現在の「変更要求」ルールを使用して、*nn* 日より古い非アクティブな変更要求をアーカイブおよびパージします。

CA SDM は、関連付けられた変更要求をアーカイブおよびパージした後でのみ、検証ログ エントリと変更仕様をアーカイブおよびパージします。インシデントを変更要求に関連付けた場合、CA SDM は、その変更要求をアーカイブおよびパージしません。

3. インシデントを作成しなかった非承認の変更には、「非承認変更の検証ログ」ルールを使用します。

このルールを使用して、*nn* 日より古い検証ログ エントリをアーカイブおよびパージします。定義上、非承認の変更は変更要求に関連付けられていません。

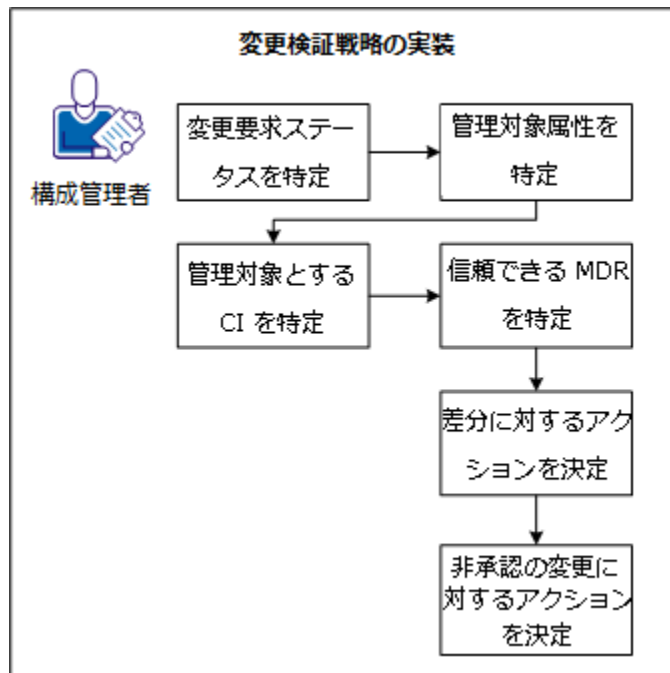
4. 「CMDDB 監査」ルールを使用して、「変更仕様履歴」、「検証ポリシー履歴」、「管理対象変更状態履歴」、および「管理対象属性履歴」タブに表示されている情報をアーカイブします。これらは、対応する「変更仕様」、「検証ポリシー」、「管理対象変更状態」、および「管理対象属性」詳細フォームに示されています。CA SDM は、これらの情報を ci_audit テーブル内に格納します。

変更検証戦略の実装

構成管理者は、CMDB 環境の変更検証戦略をどの程度積極的に実装するかを決定します。変更検証戦略が必要な変更管理プロセスの領域を特定します。これらの領域には、管理対象の属性、変更検証がアクティブであることを示す変更要求状態、変更仕様を変更できる時期、および権限のある MDR が含まれます。

たとえば、MDR1 からの IP アドレス属性への更新のみを許可します。また、CACF によって差分や非承認の変更が検出された場合の適切なアクションを決定します。

以下の図は、構成管理によって変更検証戦略がどのように実装されるかを示しています。



1. [変更要求状態の指定](#) (P. 846)。
2. [管理対象属性の指定](#) (P. 846)。
3. [管理対象の CI の指定](#) (P. 847)。
4. [権限のある MDR の指定](#) (P. 848)。
5. [差分に対するアクションの決定](#) (P. 849)。
6. [非承認の変更に対するアクションの決定](#) (P. 849)。

変更要求状態の指定

構成管理者は、変更が実行された後、CI に対して変更検証が有効になる変更要求状態を指定します。変更状態は、特定の状態で変更仕様を編集できるかどうかなどの、特定の条件を判断するのに役立ちます。たとえば、CI への更新を要求する変更要求の RFC 変更状態を確認します。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [構成コントロール] - [管理対象変更状態] をクリックします。
2. [RFC] をクリックして変更状態の詳細を確認するか、またはまだ定義されていない変更要求状態を作成します。

注: デフォルトでは、「RFC」の変更要求状態では変更仕様の編集のみが可能です。「実装中」状態では変更仕様を編集できません。「検証中」状態では変更検証が可能であり、変更マネージャやその他の許可されたユーザに対してオーバーライド ボタンが表示されます。

3. CACF オプションと、変更要求がこの状態に入った場合の動作を指定します。
4. [保存] をクリックします。

管理対象属性の指定

変更検証戦略でどの CI 属性を管理するかを指定します。たとえば、変更検証で IP アドレス (alarm_id) 属性を管理します。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [構成コントロール] - [管理対象属性] をクリックします。
2. [新規作成] をクリックします。
3. 以下の手順に従います。
 - a. [属性名] として「alarm_id」と入力します。
 - b. [属性ラベル] として「IP Address」と入力します。

- c. ドロップダウン リストから [初期検証ステータス] を選択します。
デフォルト: [検証保留中]
- d. (オプション) 変更仕様の計画値の比較で大文字小文字の区別を適用する場合は、[大文字と小文字を区別する] オプションを選択します。
デフォルト: 無効
- e. [保存] をクリックします。

管理対象の CI の指定

検証ポリシーで管理する CI を指定します。たとえば、名前が **NY_Server** で始まるすべての高優先度 CI の IP アドレス (**alarm_id**) を管理します。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [構成コントロール] - [検証ポリシー] をクリックします。
2. [新規作成] をクリックします。
3. 以下の手順に従います。
 - a. シーケンス (**100** など) を入力します。
 - b. ポリシー名として「**NY Server IP Addresses**」と入力します。
 - c. 適切な [変更要求のアライメント] オプションを選択します。
たとえば、検証ポリシーで、[変更要求 (仕様なし)] を除くすべてのオプションを許可します。
4. トランザクションと CI のフィルタを指定するには、以下の手順に従います。
 - a. [管理対象属性] ドロップダウン リストから [IP アドレス] を選択します。
 - b. [役割パターン] に入力するか、またはアスタリスクのままにしてすべての役割に適用します。

- c. [ロケーションパターン] として「**NY**」と入力します。
- d. [CI 名パターン] として「**NY_Server***」と入力します。

たとえば、このフィルタで **NY_Server1**、**NY_Server2** などの名前の **CI** を検証します。

- 5. [更新動作] ドロップダウン リストから [変更仕様に一致する場合にのみ更新を許可] を選択します。
- 6. (オプション) ポリシーを試したり、標準ログに結果のみを表示したりして、アクティブな **CMDDB** 環境に影響を与えないようにする場合は、[ログ専用モード] を使用します。
- 7. [保存] をクリックします。

権限のある MDR の指定

CMDDB 環境内の権限のある **MDR** を指定します。たとえば、**MDR1** として識別した **CA Configuration Automation** からの **CI** への更新を許可します。**MDR2** として識別した **Web** サービスからの更新を権限がないと見なし、これらの要求を **TWA** に送信します。

次の手順に従ってください:

- 1. [NY Server IP Addresses] ポリシーを開き、[編集] をクリックします。
- 2. [MDR 名パターン] として「**MDR1**」と入力します。
注: **MDR2** という名前の **MDR** を除外して、**MDR1**、**MDR3** などを許可する場合は、パターンとして「**!MDR2**」と入力します。
- 3. 別の検証ポリシー（「**MDR2 NY Server**」など）を作成します。
- 4. 以下のフィールドを除き、既存のポリシーと同じ情報を入力します。
 - a. [MDR 名パターン] として「**MDR2**」と入力します。
 - b. [更新動作] として [常にトランザクション全体をキャンセル] を選択します。
 - c. [TWA へのデータの書き込み] ドロップダウン リストから [常に実行] を選択します。
- 5. [保存] をクリックします。

差分に対するアクションの決定

差分に対するアクションを決定します。たとえば、CI への変更が、変更要求で指定された値に一致していない場合です。検証ポリシーで、差分に対するインシデントを作成します。

次の手順に従ってください:

1. 作成した「MDR2 NY Server」ポリシーを開き、[編集] をクリックします。
2. [インシデントの作成] ドロップダウン リストから [はい] を選択し、テンプレートを割り当てます。
3. [保存] をクリックします。
4. エンドユーザが、MDR2 から CI を更新するために、変更仕様を含む変更要求を作成します。
5. MDR2 が、変更要求で定義された変更仕様の計画値に一致しない値を使用して CI 更新を要求した場合、CACF はインシデントを作成します。

非承認の変更に対するアクションの決定

非承認の変更に対するアクションを決定します。たとえば、CACF が、どのアクティブな変更要求のどの変更仕様も含まない CI への変更を検出します。構成管理者は、これらのタイプの要求を拒否します。

次の手順に従ってください:

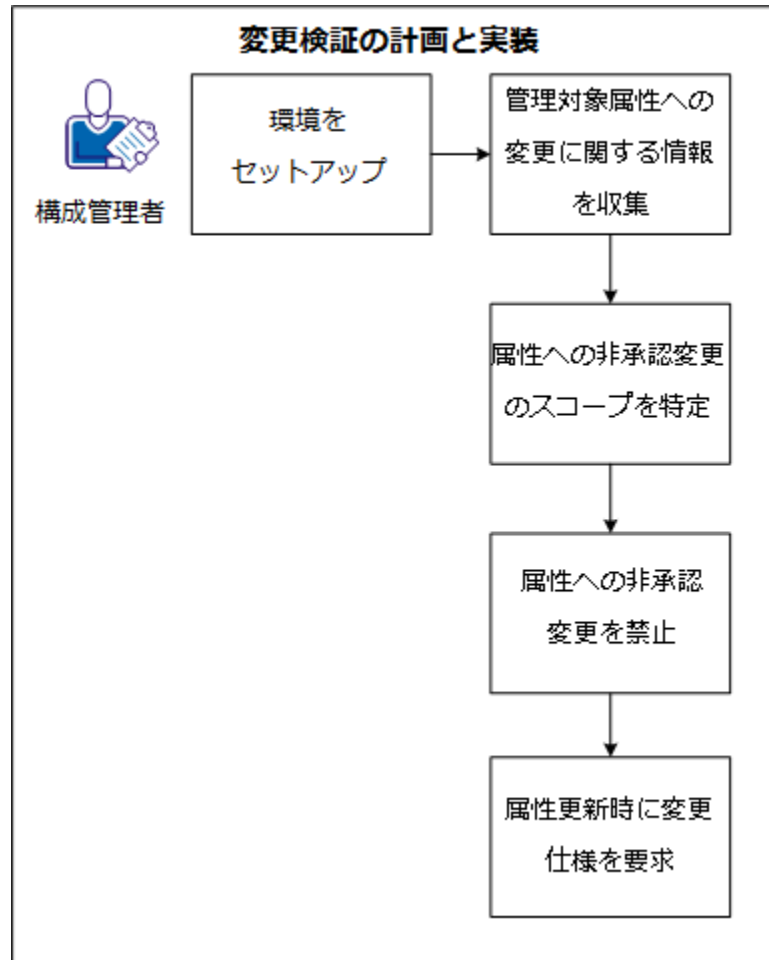
1. 検証ポリシーを作成し、その名前として「Rogue NY Server」と入力します。
2. 適切なパターン フィールドに入力します。
3. [変更要求のアライメント] オプションとして [非承認の挿入] と [非承認の更新] のみが選択されていることを確認します。
4. [更新動作] ドロップダウン リストから [変更仕様に一致する場合にのみ更新を許可] を選択します。
5. [インシデントの作成] ドロップダウン リストから [はい] を選択し、テンプレートを割り当てます。
6. [保存] をクリックします。

変更検証の計画および実装

構成マネージャは、CMDB に正しいデータが含まれるように変更検証を実装する必要があります。変更マネージャは、変更が確実に正しく実行されるように支援する必要があるため、非承認の変更に関心を持ち、発生する非承認の変更の数や発生源のデータソースを把握します。両方のマネージャが変更検証の実装に合意することによって、組織に大きな価値が提供されます。変更マネージャは、変更管理プロセスへのどの変更も実稼動環境に決して害を与えることがないように支援する必要があります。

構成マネージャと変更マネージャは保守フェーズにおける実装に合意して、構成管理者が、特定のロケーションおよびそれらのロケーションにある特定の CI に対するポリシーを実装するようにします。このシナリオでは、検証ポリシーを組織のより広範囲な対象者に対して実装するフェーズの例について説明します。

以下の図は、構成管理者が、変更検証を実装するフェーズの例を示しています。



1. [環境のセットアップ](#) (P. 852)。
2. [管理対象属性への変更に関する情報の収集](#) (P. 852)。
3. [属性への非承認の変更の範囲の決定](#) (P. 854)。
4. [属性への非承認の変更の防止](#) (P. 855)。
5. [属性の更新時の変更仕様の必要化](#) (P. 857)。

環境のセットアップ

構成管理者が常に CI を更新できるように環境をセットアップします。構成管理者は、変更要求を指定することなく、必要に応じて CMDB で CI を作成および更新することができ、正しい CI データを提供すると信頼されています。

次の手順に従ってください:

1. 以下の情報を使用して、**Policy0.1** という名前の検証ポリシーを作成します。
 - シーケンスとして「**1**」と入力します。
 - 説明として「**管理者に常に CI の更新を許可する**」と入力します。
 - すべての「変更要求のアライメント」オプションを選択します。
 - 「役割パターン」として**構成管理者**を入力します。
 - 「MDR クラスパターン」として **Web クライアント**を入力します。
 - 「CI 名」と「クラス」、およびその他のすべてのパターンとしてアスタリスク (*) を入力します。
 - 「管理対象属性」の「任意の管理対象属性」を選択します。
2. 「更新動作」アクションとして「属性更新を許可」を選択します。
3. 「保存」をクリックします。

構成管理者が常に CI を更新できるように許可するのみのポリシーが有効になります。

管理対象属性への変更に関する情報の収集

どのような CI が更新されているか、変更のソースは何か、だれが変更を行っているか、および属性や対応する CI のための検証計画を定義するときに役立つように指定されている値を識別するには、特定の CI 管理対象属性への変更に関する情報を収集する必要があります。たとえば、IP アドレス (alarm_id) へのすべての変更の範囲を把握し、これを CA SDM の標準ログ (stdlog) に記録します。組織内で発生する属性への変更の数によっては、これらの情報の収集に数週間かかることがあります。

1. 管理対象属性として IP アドレス (alarm_id) を定義します。
2. 環境内の管理対象変更状態として「実装中」および「検証中」を定義し、両方の状態で検証をアクティブにします。

3. 以下の情報を使用して、**Policy1.1** という名前の検証ポリシーを作成します。
 - シーケンスとして「**3000**」と入力します。
 - 説明として「**IP アドレスへのすべての変更をログに記録する**」と入力します。
 - すべての「変更要求のアライメント」オプションを選択します。
 - 「CI 名」と「クラス」、およびその他のすべてのパターンとしてアスタリスクを入力します。
 - 「ログ専用モード」を有効にします。
4. 「保存」をクリックします。
5. 数週間後、**stdlogs**を確認して更新のソースを表示します。

たとえば、このログには非承認の CI 更新や、一致する変更要求を含む更新が表示されます。
6. **NY**にいるユーザが、変更要求を作成せずに CI の IP アドレスを更新したことを特定します。
7. 分析を完了したら、ポリシーを編集して「アクティブ」を「非アクティブ」に設定することによって **Policy1.1** を非アクティブ化します。

属性への非承認の変更の範囲の決定

IP アドレス属性への非承認の変更の範囲を決定します。非承認の変更の範囲がわかっていると、非承認の変更の組織への影響を把握するのに役立ちます。たとえば、[ログ専用モード] オプションを使用した前の分析に基づいて、NY に配置されている「test」で始まる CI の IP アドレスに対して変更要求のない変更が発生した場合は常にインシデントを作成します。このプロセスで作成される新しいインシデントを無視するように組織内の変更マネージャに連絡します。

次の手順に従ってください:

1. 以下の初期の実装操作を完了します。
 - 管理対象変更状態として「実装中」を定義し、[実装状態] オプションを有効にします。
 - 管理対象変更状態として「検証中」を定義し、[検証後に変更要求を推奨] オプションを無効にします。
 - まだ定義されていない場合は、管理対象属性として IP アドレス (alarm_id) を定義します。
2. 以下の情報を使用して、Policy2.1 という名前の検証ポリシーを作成します。
 - シーケンスとして「3001」と入力します。
 - このポリシーに関する説明を入力します。たとえば、「非承認の挿入および非承認の更新が発生すると、インシデントが作成されます。その他のすべての変更には影響しません。」と入力します。
 - アライメントとして [非承認の挿入] と [非承認の更新] を選択します。
 - [管理対象属性] ドロップダウンリストから [IP アドレス] を選択します。
 - [CI 名] として「test*」、[ロケーション] として「NY」、その他のすべてのパターンとしてアスタリスクを入力します。
 - [属性更新を許可]、[インシデントの作成] に対して [はい]、およびアクションから [インシデントテンプレート] を選択します。
3. [保存] をクリックします。

このフェーズを完了すると、CACF は、NY 内のすべてのコンピュータに対してインシデントを作成します。インシデントを確認した後、以下の情報を検出します。

- いくつかの MDR は、同じ CI に対して異なる IP アドレスを報告しています。
 - 一部の MDR には権限があり、その他の MDR には権限がありません。
 - 一部の CI は、ロケーション、ファミリー、名前、サービス タイプなどに基づいて管理しないでください。
4. 変更マネージャはほかの IT マネージャと会い、非承認のデータを確認するために、CMDB、CI 詳細フォーム、検証ログ、および属性名別のフィルタリングを確認します。
 5. 組織は、優先度 1 のサーバのみを管理するために Policy 2.1 内の CI フィルタを更新することを決定します。

属性への非承認の変更の防止

CMDB データの整合性を確保し、更新の変更要求を要求するために IP アドレス属性への非承認の変更を防ぎます。変更要求では CI を指定する必要があります。IP アドレスに対しては、変更を行うための変更仕様は必要ありません。変更検証は、属性レベルではなく CI/変更要求レベルで実行されます。たとえば、非承認の更新を防ぎ、インシデントを作成して、それらの変更をリクエストするユーザを追跡します。

次の手順に従ってください:

1. Policy1.1 と Policy2.1 を「非アクティブ」に設定し、これらのポリシーを無効にします。
2. 以下の情報を使用して、Policy 3.1 を作成します。
 - シーケンスとして「3100」と入力します。
 - 説明として「変更要求のない非承認の変更を禁止する」と入力します。
 - アライメントとして「非承認の更新」を選択します。
 - 「CI 名」として「test*」、[ロケーション] および [任意の管理対象属性] として「NY」、その他すべてのパターンとしてアスタリスクを入力します。

- [常にトランザクション全体をキャンセル] アクションを選択します。
3. [保存] をクリックします。
 4. 以下の情報を使用して、Policy3.2 を作成します。
 - シーケンスとして「**3200**」と入力します。
 - 説明として「**IP アドレスへの変更に対して変更要求を必要とする**」と入力します。
 - アライメントとして[変更要求(仕様なし)] を選択します。
 - [CI 名] として「**test***」、[ロケーション] として「**NY**」、その他のすべてのパターンとしてアスタリスクを入力します。
 - [管理対象属性] ドロップダウンリストから[IP アドレス] を選択します。
 - アクションとして[属性更新を許可] を選択します。
 5. [保存] をクリックします。

変更に対して変更要求が必要なため、このポリシーでは非承認の変更が拒否されます。

属性レベルでの変更には変更仕様は必要ないため、構成マネージャは、変更要求に定義されていないデータも更新されていることを確認します。たとえば、IP アドレスの変更と同時にインストール済みメモリを増やす変更をリクエストした場合、変更要求があるため非承認の変更とはみなされません。構成マネージャは、変更要求を自動的に検証および昇格し、属性レベルで検証を行いたい場合もあります。

属性の更新時の変更仕様の必要化

構成マネージャは、CMDB 内のデータが、変更要求で指定されていない変更に対する複数の更新を受け取ることに懸念を示します。たとえば、ユーザは、インストール済みメモリ (phys_mem) および IP アドレス (ip_address) の値を同時に変更できます。前のフェーズでは、変更要求が存在するので、CACF はこのリクエストを非承認の変更とはみなしません。

構成マネージャは、属性レベルで変更検証を実施したいと考えます。構成管理者は、IP アドレスの更新時に変更仕様の使用を要求し、非承認の更新が試みられない場合にインシデントを作成するためのポリシーを作成します。

次の手順に従ってください:

1. 構成マネージャは、IP アドレスに対する変更には変更仕様が含まれている必要があることを変更アナリストに連絡します。
2. Policy3.1 および Policy3.2 を「非アクティブ」に設定し、これらのポリシーを無効にします。
3. 以下の情報を使用して、Policy4.1 を作成します。
 - シーケンスとして「**4000**」と入力します。
 - 説明として「**IP アドレスへの変更に対して変更仕様を必要とする**」と入力します。
 - アライメントとして「非承認の挿入」、「非承認の更新」、および「変更要求（仕様なし）」を選択します。
 - 「CI 名」として「**test***」、「ロケーション」として「**NY**」、その他のすべてのパターンとしてアスタリスクを入力します。
 - 「管理対象属性」ドロップダウンリストから「**IP アドレス**」を選択します。
 - アクションとして「常にトランザクション全体をキャンセル」を選択します。
4. 「保存」をクリックします。
5. 以下の情報を使用して、Policy4.2 を作成します。
 - シーケンスとして「**4100**」と入力します。
 - 説明として「**IP アドレスへの変更に対して変更仕様を必要とする**」と入力します。
 - アライメントとして「変更要求（仕様あり）」を選択します。

- [CI 名] として「test*」、[ロケーションパターン] として「NY」と入力します。
- [管理対象属性] ドロップダウンリストから [IP アドレス] を選択します。
- アクションとして [変更仕様に一致する場合にのみ更新を許可] を選択します。

6. [保存] をクリックします。

環境に変更検証を実装するための適切な実例フェーズを正常に完了しました。変更検証戦略を拡大して、より多くの属性、CI、MDR、およびテナントを含めることができます。

変更検証のベストプラクティス

変更検証を実装するときは以下のベストプラクティスを考慮します。

- 少数のポリシーを定義する。
- 負論理（ポリシー パターン内の感嘆符）の使用を避ける。
- 単一 CI の更新保存は少数のポリシーに一致する必要がある。
- 数的階層構造でポリシーを整理する。
- 変更検証ポリシーを実装する前に、[ログ専用モード] ポリシーを使用する。
- 複数のポリシーで更新されている単一の属性を管理する場合のポリシーの重複を最小化する。
- CACF が作成するインシデントの数を制限する。
- CACF データのアーカイブとパージを実装する。

関連項目：

[ポリシーの整理](#) (P. 859)

[Multi-Tenancy に関する考慮事項](#) (P. 860)

[CACF の役割と機能アクセス](#) (P. 860)

ポリシーの整理

ポリシーのトラッキングを行うために複数の計画を使用できます。多層的なアプローチを使用することを推奨します。将来の挿入を可能にするために、ポリシー番号は100ずつ増やします。

この戦略に対して以下の階層例を検討します。

基本ポリシー

100,000 ～ 199,999

- 変更管理者に挿入の実行を許可する
- MDR クラス (xxxx) による挿入を許可しない
- インシデント作成からテスト CI をすべて除外する

一時または短期ポリシー

200,000 ～ 299,999 : 今週の一括ロード

アプリケーション固有のポリシー

- 301,000 ～ 301,999 : 以下の一般的なアプリケーション固有のポリシーの例外
たとえば、NY ポリシーでの server1
- 311,000 ～ 311,999 : サービス タイプの優先度 1 解決に関連するポリシー
- 320,000 ～ 320,999 : NY に関連するポリシー
- 331,000 ～ 331,999 : Lisle に関連するポリシー

テクノロジー固有のポリシー

- 410,000 ～ 410,999 : サーバに関連するポリシー
- 411,000 ～ 411,999 : ネットワークに関連するポリシー

デフォルト ポリシー

前述のポリシーが自分の環境に当てはまらない場合は、これらのポリシーを使用できます。

900,000 ～ 999,999 : 管理対象属性（[任意の管理対象属性]）へのすべての更新などのデフォルト ポリシーには変更仕様が必要です。

Multi-Tenancy に関する考慮事項

マルチテナンシー環境で CACF を使用する場合は以下の情報を考慮します。

- 管理対象属性、検証ポリシー、変更要求、および変更仕様はテナント化されています。
- それぞれの階層の上のテナントは CACF オブジェクトをすべて表示できます。

たとえば、あるテナントが管理対象属性を作成すると、このアクションにより、階層内のテナントによる重複する管理対象属性の作成が防止されることがあります。階層には一意のポリシー シーケンス番号が必要です。

- 属性への変更を管理するポリシーを決定するには、オブジェクト (CI) のテナント階層からのポリシーのみを考慮します。
- サブテナントは、それぞれのローカル ポリシーにより低いシーケンス番号を割り当てることで、スーパーテナントをオーバーライドするポリシーを作成できます。
- CACF ではテナント レベルのポリシーおよび階層内にあるその親のみ考慮されます。
- CACF では、変更を実行するその連絡先のテナントは考慮されません。

注: 検証ポリシーはシステムに固有で、ユーザまたは役割によって変化しません。

CACF の役割と機能アクセス

以下の表は、CACF が使用するデフォルトの役割を示しています。

役割/機能アクセス	管理	CI	インシデント/問題/リクエスト	変更要求
管理者	変更	変更	変更	変更
構成管理者	変更	変更	変更	変更
構成アナリスト	表示	変更	変更	変更
構成ビューア	なし	表示	変更	表示
変更マネージャ	表示	変更	変更	変更

役割/機能アクセス	管理	CI	インシデント/問題/リクエスト	変更要求
サービス デスク 管理者	変更	変更	変更	変更
サービス デスク マネージャ	表示	変更	変更	変更
システム管理者	変更	変更	表示	表示
レベル 1 のアナリスト	表示	表示	変更	表示
レベル 2 のアナリスト	表示	変更	変更	変更
インシデント マネージャ	表示	表示	変更	変更
問題 マネージャ	表示	表示	変更	変更

管理

CACF 管理、ポリシー、および属性管理の作成、更新、および表示を示します。

CI

CI および関係属性データの作成、更新、および表示を示します。

インシデント/問題/リクエスト

非承認の変更および誤って実行された変更による差分を含む、未処理の CACF 案件の変更および表示を示します。

変更要求

変更仕様の作成、更新、および表示を示します。

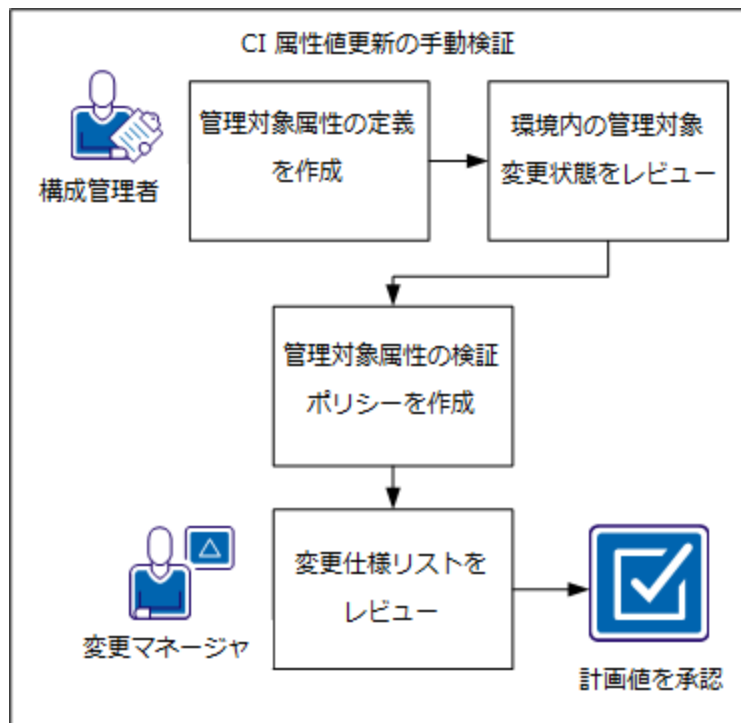
たとえば、変更マネージャの役割では CACF ポリシーの表示および属性の管理が行えますが、それらを更新することはできません。

重要： 変更要求への更新アクセスおよびそのステータスにより、誰が変更仕様を編集できるかが決まります。たとえば、変更管理者は、変更マネージャにこのアクセスを提供できます。

CI 属性値の更新の手動検証

構成管理者は、CA SDM 環境にインストール済みメモリ (phys_mem) 属性用の検証ポリシーが必要だと判断します。構成管理者は、CA SDM には値を検出する MDR がないため、「手動検証が必要」ステータスの管理対象属性定義を作成します。構成管理者は、管理対象状態を確認し、検証ポリシーを作成します。変更マネージャは、CI のインストール済みメモリの値への更新をリクエストする変更要求を確認します。この変更リクエストは手動で検証する必要があります。

以下の図は、構成管理者がどのように検証ポリシーを作成し、変更マネージャがどのように手動で CI 属性値の更新を検証するかを示しています。



1. [管理対象属性定義の作成](#) (P. 863)。
2. [環境での管理対象変更状態の確認](#) (P. 864)。
3. [管理対象属性用の検証ポリシーの作成](#) (P. 864)。
4. [変更仕様リストの確認](#) (P. 866)。
5. [計画値の承認](#) (P. 867)。

管理対象属性定義の作成

構成管理者は、インストール済みメモリ (phys_mem) 属性用の管理対象属性定義を作成します。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [構成コントロール] - [管理対象属性] をクリックします。
2. [新規作成] をクリックします。
3. [属性名] として「**phys_mem**」と入力します。
4. [属性ラベル] として「**インストール済みメモリ**」と入力します。
5. [初期検証ステータス] ドロップダウンリストから [手動検証が必要] を選択します。
6. (オプション) 変更仕様の計画値の比較で大文字小文字の区別を適用する場合は、[大文字と小文字を区別する] オプションを選択します。

デフォルト: 無効

7. [保存] をクリックします。
管理対象属性が保存されます。

環境での管理対象変更状態の確認

構成管理者は、CA SDM 環境の管理対象変更状態を確認します。変更要求のステータスが、検証中などの CACF による管理対象の変更状態に変わると、変更検証が開始されます。

注: 構成管理者は、変更検証を開始する変更要求ライフサイクルの状態をカスタマイズできます。管理者は、実装開始時にユーザが変更仕様を変更できる状態もカスタマイズできます。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [構成コントロール] - [管理対象変更状態] をクリックします。
2. [実装中] をクリックして、管理対象ステータスの詳細ページを開きます。
3. 管理対象ステータスに関する詳細を確認します。

たとえば、「実装中」ステータスで変更仕様の編集を可能にし、[変更検証はアクティブ] を有効にすることができます。これはアクティブな変更検証プロセスの例であり、変更要求が「実装中」ステータスに設定されているときに値を編集できることを示しています。

4. ページを閉じます。

管理対象属性用の検証ポリシーの作成

検証ポリシーでは、MDR が属性値を検出し、そのデータで CMDB の更新を試みるときの CACF の動作を指定します。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [構成コントロール] - [検証ポリシー] をクリックします。
2. [新規作成] をクリックして詳細ページを開きます。
3. ポリシーのシーケンスとして「**1000**」と入力します。

注: 環境内のほかの検証ポリシーの優先度に基づき、より高い数またはより低い数を入力できます。

4. **RAM Management** などのポリシー名とポリシーの簡単な説明を入力します。
5. [変更要求のアライメント] で [非承認の挿入] および [非承認の更新] を選択します。
6. ポリシーで特定の **MDR** によるインストール済みメモリ (**phys_mem**) 属性の更新を禁止するには、以下のタスクを実行します。
 - [管理対象属性] として [インストール済みメモリ] を選択します。
 - [役割パターン] を入力するか、またはアスタリスクを使用してすべての役割に適用します。
 - [CI 名パターン] を入力するか、またはアスタリスクを使用してすべての **CI** に適用します。
 - [クラスパターン] を入力するか、またはアスタリスクを使用してすべてのクラスに適用します。
 - [更新動作] として [古い属性値を保持] を選択します。

注: Web インターフェース経由でログインしているユーザにのみ、この属性への更新を許可する場合は、[MDR 名パターン] に「**Web Client**」と入力します。
7. [保存] をクリックします。
8. ページを閉じます。

変更仕様リストの確認

「RFC」ステータスの変更要求で、**server1** という名前の **CI** のインストール済みメモリ (**phys_mem**) 属性の値を変更したいとします。変更マネージャは、変更仕様の検証ステータスを「手動検証が必要」に設定します。変更マネージャは、**CA SDM** 内の変更仕様を確認できます。

次の手順に従ってください:

1. 変更マネージャは、変更要求を「RFC」から「検証中」に移行します。
手動検証による変更仕様はすべて「手動検証が必要」になります。
2. 変更要求の「構成管理」タブから「変更仕様」タブを選択します。
このタブでは、手動検証が必要なすべての変更仕様が赤で強調表示されます。

注: 「CA CMDB」-「構成の監査」-「変更仕様」をクリックすると、「管理」タブからも変更仕様を確認できます。また、「関連チケット」タブで「変更仕様」タブを選択すると、**CI** から変更仕様を確認できます。

3. 検証ステータスとして手動検証が必要な変更仕様を検索します。
たとえば、変更要求 **21** の変更仕様にはこのステータスが含まれます。
4. 構成アイテム **server1** のインストール済みメモリ属性に適した値を調べます。

注: 追加の調査が必要な変更仕様を示すために、検証に失敗した変更仕様も赤で表示されます。

計画値の承認

変更マネージャは、CI の正しい属性値を調べ、変更リクエストに対して適切な判断を下します。

次の手順に従ってください:

1. 変更仕様を開いて、詳細ページを表示します。
2. CI の特定のインストール済みメモリ (phys_mem) 属性を調べ、計画値を確認します。
3. 変更仕様の変更要求が「検証中」状態にあることを確認します。
4. 「計画値の承認」をクリックします。

「検証ステータス」が「計画値を承認済み」に変わります。

注: 「計画値の承認」をクリックすると、CI は計画値で自動的に更新されます。

管理対象属性の値を手動で正常に検証できました。

例：特定のロケーションからのみ非承認の更新を許可する

この例では、ニューヨーク オフィスにあるサーバ CI を修理する必要があります。サーバを修理するベンダーもニューヨークに住んでいます。アセット マネージャは、欠陥のあるすべてのサーバをニューヨークに輸送するように組織に要求します。構成管理者は、ハードウェアがニューヨークに到着したら、CI への非承認の更新を許可したいと考えます。構成管理者は、保守ベンダー属性用の検証ポリシーを作成して、ベンダーがサーバを受け取ったことをニューヨークの Service Desk アナリストが確認できるようにします。

次の手順に従ってください：

1. 以下の管理対象属性を作成します。
 - [属性名] として「**vendor_repair**」と入力します。
 - [初期検証ステータス] ドロップダウン リストから [検証保留中] を選択します。
 - 管理対象属性の詳細として、[ラベル] と [説明] に「**保守**」と入力します。
2. 以下の管理対象変更ステータスを作成します。
 - [変更要求ステータス] として「**ベンダー保留**」と入力します。
 - [変更検証はアクティブ] オプションを有効にします。
3. 以下の検証ポリシーを作成します。
 - [変更要求のアライメント] として [非承認の挿入] および [非承認の更新] を選択します。
 - ポリシーのシーケンス番号を入力します。
たとえば、「**201**」と入力します。
 - [CI 名パターン] として「**server***」と入力します。
 - [クラス パターン] として「**Server**」と入力します。
 - [ロケーション パターン] として「**New York**」と入力します。
 - [更新動作] ドロップダウン リストから [属性更新を許可] を選択します。

4. Service Desk アナリストは、サーバ CI の変更要求と変更仕様を作成し、ロケーションにニューヨークを指定します。
5. Service Desk アナリストは、[変更要求ステータス] を [ベンダー保留] に設定します。
6. Service Desk アナリストは、サーバ CI のロケーションをニューヨークに更新します。

たとえば、シカゴ オフィスからニューヨークに欠陥のあるサーバが輸送される場合、Service Desk アナリストが、サーバがニューヨークに到着したことを確認します。

7. Service Desk アナリストは、CI にベンダー情報を入力します。

変更要求は、CI ロケーションがすべてニューヨークに設定され、変更仕様がすべて検証された後にクローズします。

例：組織内のラップトップのアップグレード

この例では、アセット マネージャは、組織内のすべてのラップトップを Windows XP から Windows 7 にアップグレードしたいと考えています。構成管理者は、Windows XP オペレーティング システムを搭載しているラップトップをすべてフィルタするために、製品バージョン属性用の検証ポリシーを作成します。構成管理者は、「検出値を使用」ステータスの管理対象属性定義を作成し、管理対象状態を確認し、検証ポリシーを作成します。CA SDM が、オペレーティング システムの更新を必要とするラップトップの CA Configuration Automation から CMDB への更新を受信して、アセット管理チームがアップグレードを完了させます。

次の手順に従ってください：

1. 以下の管理対象属性を作成します。
 - [属性名] として「**product_version**」と入力します。
 - [属性ラベル] として「**製品バージョン**」と入力します。
 - [初期検証ステータス] ドロップダウン リストから [検出値を使用] を選択します。
 - 管理対象属性の詳細としてラベルと説明を入力します。

2. 以下の検証ポリシーを作成します。
 - 組織内のほかのポリシーに基づくシーケンスを入力します。
たとえば、「**101**」と入力します。
 - [CI 名パターン] として「**Windows* XP***」と入力します。
 - [クラス パターン] として「**Workstation**」と入力します。
 - (オプション) 組織内の特定のオフィスとポリシーを関連付ける場合は、[ロケーション パターン] を入力します。
 - [更新動作] ドロップダウン リストから [変更仕様に一致する場合にのみ更新を許可] を選択します。
 - [インシデントの作成] ドロップダウン リストから [はい] を選択します。
3. 各ラップトップ CI の製品バージョン管理対象属性に、**Windows 7** を指定する変更要求と変更仕様を作成します。
4. 変更要求を「実装中」ステータスに移行して、アセット管理チームがアップグレードを開始するのを待ちます。
5. 実装が完了したら、変更要求を「検証中」に移行します。
CA Configuration Automation によりラップトップ情報が検出され、CMDB にデータがインポートされます。
6. CACF が検出したすべての差分を [オープン CACF インシデント] リストで確認します。
7. インシデントを 1 つ選択し、CA Configuration Automation が検出したラップトップに関する詳細を確認します。
8. [変更要求の作成] をクリックして CI とチケットを関連付け、未処理の変更に対する製品バージョンの変更仕様を指定します。
残りの変更がすべて完了したことが検出で確認されるまで待ちます。
9. CACF が作成するすべての新しいインシデントに対して、必要に応じて手順 6 ～ 8 を繰り返します。

例：検証されていない変更要求の除外

この例では、構成管理者は、一致する変更要求の CI 更新のみを許可したいと考えています。ニューヨークにあるサーバクラス内の CI のみ検証済みの変更要求に対して更新します。差分がある場合はインシデントが作成されます。

次の手順に従ってください：

1. 検証ポリシーを作成します。
2. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として [任意の管理対象属性] を選択します。
 - c. [ロケーション パターン] として「**NY**」と入力します。
 - d. [クラス パターン] として「**Server**」と入力します。
 - e. [更新動作] として [変更仕様に一致する場合にのみ更新を許可] を選択します。
 - f. [インシデントの作成] ドロップダウン リストから [はい] を選択します。
3. ポリシーを保存します。

例：一致する変更要求が存在しない場合に CI 更新を許可する

この例では、構成管理者は、一致する変更要求が存在しない場合でも、**test*** という名前のすべての CI の更新を許可したいと考えています。このポリシーでは、管理者の役割のすべてのユーザからの更新が承認されます。

次の手順に従ってください：

1. 検証ポリシーを作成します。
2. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として [任意の管理対象属性] を選択します。
 - c. [CI 名パターン] として「**test***」と入力します。
 - d. [役割パターン] として「**Administrator***」と入力します。

- e. [更新動作] として [属性更新を許可] を選択します。
 - 3. ポリシーを保存します。
 - 4. 管理者の役割を持つユーザが、**test5** という名前の CI の変更仕様を作成します。
- CI が正常に更新されます。

例: すべての更新を CA Configuration Automation から TWA に延期する

この例では、構成管理者は、すべての CI 更新を CA Configuration Automation から TWA に延期したいと考えています。このポリシーでは、CMDDB 内の CI は更新されず、代わりに、すべての非承認の変更に対するデータがさらなる評価のために TWA に書き込まれます。

次の手順に従ってください:

- 1. 検証ポリシーを作成します。
- 2. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として [任意の管理対象属性] を選択します。
 - c. [変更要求のアライメント] として [非承認の挿入] と [非承認の更新] を選択します。
 - d. [MDR クラス パターン] として「**CCA**」と入力します。
 - e. [更新動作] として [常にトランザクション全体をキャンセル] を選択します。
 - f. [TWA へのデータ書き込み] オプションで [常に実行] を選択します。
- 3. ポリシーを保存します。

例: ポリシー結果をテストとしてのみログに記録する

この例では、構成管理者は、CMDB 環境に実装する前に新しいポリシーをテストしたいと考えています。ログ専用オプションでは、CACF がポリシーの潜在的な CI への影響度を標準ログ ファイルに書き込むことができます。

次の手順に従ってください:

1. 検証ポリシーを作成します。
2. アライメント、フィルタ、およびアクションの情報を入力します。
3. [ログ専用モード] オプションを選択します。
4. ポリシーを保存します。
5. ポリシーの実行をシミュレートするためのポリシー仕様およびフィルタ条件に一致する CI 更新を実行した後、標準ログ ファイルを確認します。

例: CI 更新を拒否する

この例では、構成管理者は、Cohesion という名前の MDR からの IP アドレス (alarm_id) 属性への更新のみ拒否したいと考えています。このポリシーでは、CMDB 内の CI の IP アドレスは更新されませんが、ほかの属性が更新される場合があります。CACF がさらなる評価のために、TWA にすべての属性を書き込みます。

次の手順に従ってください:

1. 管理対象属性リストに IP アドレス (alarm_id) を追加します。
2. 検証ポリシーを作成します。
3. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として [IP アドレス] を選択します。
 - c. [変更要求のアライメント] として [非承認の挿入] と [非承認の更新] を選択します。
 - d. MDR パターンとして「Cohesion」と入力します。

- e. [更新動作] として [古い属性値を保持] を選択します。
 - f. [TWA へのデータ書き込み] オプションで [常に実行] を選択します。
4. ポリシーを保存します。

例：仕様なしで作成された変更要求を許可する

この例では、構成管理者は、ユーザが仕様なしで作成した変更要求を信頼したいと考えています。このポリシーでは、CI テキストにすべての変更が正確に記載されていて、CI 更新が可能だと仮定します。

次の手順に従ってください：

1. 検証ポリシーを作成します。
2. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として [任意の管理対象属性] を選択します。
 - c. アライメントとして [変更要求（仕様なし）] を選択します。
 - d. [更新動作] として [属性更新を許可] を選択します。
3. ポリシーを保存します。

例：仕様なしで作成された変更要求を許可しない

この例では、構成管理者は、ユーザが仕様なしで作成した変更要求を信頼したくないと考えています。このポリシーでは、仕様のない変更要求を無視してインシデントを作成します。

次の手順に従ってください：

1. 検証ポリシーを作成します。
2. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として [任意の管理対象属性] を選択します。
 - c. アライメントとして [変更要求（仕様なし）] を選択します。

- d. [更新動作] として [常にトランザクション全体をキャンセル] を選択します。
 - e. [インシデントの作成] ドロップダウン リストから [はい] を選択し、インシデント テンプレートを選択します。
3. ポリシーを保存します。

例: 選択されたソースからの非承認の挿入を許可する

この例では、構成管理者は、選択されたソースからの新しい CI を許可したいと考えています。z/OS MDR では変更要求を必要とせずに、CI を作成できます。

次の手順に従ってください:

1. 検証ポリシーを作成します。
2. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として [任意の管理対象属性] を選択します。
 - c. アライメントとして [非承認の挿入] を選択します。
 - d. [MDR クラス パターン] に「z/OS」と入力します。
 - e. [更新動作] として [属性更新を許可] を選択します。
3. ポリシーを保存します。

例: 実稼働以外の CI の非承認の更新を許可する

この例では、構成管理者は、Spectrum MDR からの IP アドレス属性への更新を許可したいと考えていますが、名前を *PROD* で始めることができません。

次の手順に従ってください:

1. 検証ポリシーを作成します。
2. 以下の手順に従います。
 - a. シーケンス番号を入力します。
 - b. [管理対象属性] として IP アドレス (alarm_id) を選択します。

- c. アライメントとして「非承認の更新」を選択します。
 - d. 「CI 名パターン」として「**IPROD***」と入力します。
 - e. 「MDR クラス パターン」として「**Spectrum**」と入力します。
 - f. 「更新動作」として「属性更新を許可」を選択します。
3. ポリシーを保存します。

第 17 章: <MDR> の管理

この章では、MDR を定義する方法、データをインポートする方法、CI をそのソースにマップする方法、起動パラメータを定義する方法、ソース MDR に戻って起動する方法、および MDR を使って統一 CI 情報をマップし表示する方法について説明します。

このセクションには、以下のトピックが含まれています。

[MDR とは](#) (P. 877)

[MDR Launcher](#) (P. 879)

[MDR を起動するための URL を定義する](#) (P. 880)

[CA APM の MDR プロバイダをセットアップする](#) (P. 882)

[CA CMDB から CA APM のコンテキストでの起動](#) (P. 883)

[MDR Federation をサポートする CI 優先度](#) (P. 883)

[CA Cohesion ACM MDR](#) (P. 886)

[GRLoader の使用](#) (P. 891)

[CI の命名規則および命名制限](#) (P. 891)

[system_name の命名規則](#) (P. 893)

[CMDBf ドライバの使用](#) (P. 895)

[CMDBf マッピングのメタデータ ファイルの更新方法](#) (P. 895)

MDR とは

CA、IBM、HP、Microsoft などの企業からの代表で構成されるワーキンググループ、Configuration Management Database Federation (CMDBf) は、MDR (管理データリポジトリ) を、構成アイテム (CI) に関する情報をまとめたものと定義しています。

MDR ランチャの実装時に MDR とその CI の間の関係を作成するには、次の操作を行います。

1. MDR を定義します。
2. MDR を参照する CI を定義します。

CI が、存在しない MDR を参照することはできませんが、MDR と関係を定義せずに CI を定義することはできます。更新時に MDR 情報を追加したり、MDR ランチャの能力を活用するよう編集したりすることが可能です。

複数の MDR で同じ CI が検出されることがあります。CI を検出した後、各 MDR がその CI を管理しようとしします。MDR は以下のようなアクションを実行することがあります。

- CI に関する詳細な属性を検出する。
- CI の状態を変更しようとする。

例: 複数の MDR が 1 つの CI を検出した場合

ある CI が、ネットワーク管理ソフトウェアと、アセット管理ソフトウェアパッケージの両方で検出されたとします。

- ネットワーク管理ソフトウェアは、ネットワーク構成およびネットワーク トポロジに関する情報を管理します。
- アセット管理ソフトウェアには、その CI のコストや減価償却、ライセンス、および保守契約に関する情報が入っています。

MDR のクラスおよび MDR 名

IT 企業には多数の MDR が存在することがあります。各 MDR には、MDR 名 (mdr_name) という ID が与えられています。MDR には mdr_name としてホスト サーバ名が使用されることが多い (同一ホスト上に複数の MDR が存在できるように) ため、mdr_name に MDR クラス (mdr_class) を付加して、各 MDR を一意に特定できるようにします。

CA Cohesion ACM は、CA CMDB と密接に統合されたアセット検出ツールです。CA CMDB に定義した各 CA Cohesion ACM MDR には、必ず Cohesion という mdr_class を付加します。

注: CA Cohesion ACM の詳細については、CA Cohesion ACM のオンラインヘルプを参照してください。CA Cohesion ACM と CA CMDB の統合については、「CA Cohesion ACM 実装ガイド」を参照してください。

MDR に CA SDM を実装する方法

MDR には通常、CA CMDB よりも詳細な CI 情報が入っています。しかし、一般的には 1 つの MDR がほかの MDR の存在を認識しなかったり、ある CI とほかの CI との関係、特にほかの MDR 内にある CI との関係を無視したりする場合があります。CA CMDB は、MDR ソースの枠を超えて CI を管理することに焦点を当てているため、このような環境に最適です。

CA CMDB はすべての CI のすべての属性を格納するようには意図されていません。その代わり、まとめて管理する必要のある最も重要な属性を一元管理します。変更管理のコントロール下にある属性は、CMDB が管理する属性の好例です。CA CMDB で管理されない属性には、MDR 起動機能を使用してアクセスできます。さらに、CA CMDB には CMDBf ビューアが用意されています。これは複数の CMDB および MDR 全体を通して、CI 属性を並べて比較できるものです。

CA SDM への MDR の定義

[管理] タブでは、CA CMDB に MDR を定義付けることができます。

MDR に CI をインポートする前に、MDR を定義する必要があります。存在しない MDR に統一された CI をインポートしようとするすると失敗します。

注: MDR を定義する方法については、「実装ガイド」を参照してください。

MDR Launcher

MDR ランチャはオープン統合ツールです。MDR ランチャを使用すれば、Web ページを使用して、コーディングを必要とせずに、ほぼすべての MDR のデータを参照することができます。MDR ランチャを使用すると、CI を参照する際に、CI に関する詳細情報を取得することと、CI を制御することが可能になります (MDR がそのような制御をサポートしている場合)。

MDR ランチャの用途には、以下のようなものがあります。

- ハードウェアサーバの詳細ページから、CA Cohesion を起動し、変更を確認する。
- 空調 CI の詳細から、ベンダーの Web ページを起動し、診断情報やインシデント レポートを参照する。
- 契約 CI から、契約管理システムを起動し、契約の詳細を把握する。
- SLA CI から、CA サービスを起動し、変更を行う前にサービス レベル アグリーメントを確認する。
- サーバ CI から、CA Remote Control を起動し、サーバを制御して診断や問題の修復を実行する。

MDR を起動するための URL を定義する

CA CMDB は、URL を使用してソース MDR との Web ページセッションを開始して MDR ランチャーを操作します。CA CMDB で使用する URL を定義します。

MDR の URL を定義するには

1. [管理] タブをクリックします。
2. 左側のペインで、CA CMDB の [MDR 管理] ツリーを開きます。
3. [MDR リスト] をクリックします。
[管理データ リポジトリ (MDR) リスト] ページが表示されます。
4. 既存の MDR をクリックします（または、新規 MDR を作成して保存します）。
[MDR プロバイダ定義] ページが表示されます。
5. [編集] をクリックします。
[MDR 定義の更新] ページが表示されます。
6. 以下のパラメータをすべて設定します。

ホスト名

MDR の Web ページを配信する Web サーバのネットワーク アドレスまたは DNS 名を指定します。

ポート

ホスト名 Web サーバが使用するポート番号を指定します。

パス

Web ページへのパスを、ページ自身も含めて指定します。

Parameters (パラメータ)

MDR に目的の CI を定義する際に使用するパラメータを指定します。CA CMDB はこの情報を MDR に登録します。

ユーザ ID

MDR へのアクセスを許可された共通のユーザ ID がある場合は、そのユーザ ID を指定します。

共有シークレット

CA CMDB と MDR 間で共有する情報を指定します。CA Cohesion MDR については、ここで指定した値が、「com.cendura.security.oneclickauth.secret」の CA Cohesion のプロパティ ファイルで指定した値に一致する必要があります。

CMDBf ネームスペース

ローカル ID としてクエリに渡される `federated_asset_id` を指定します。CA CMDB の場合、値は `http://cmdb.ca.com/r1` です。

CMDBf Timeout

(オプション) CMDBf エンドポイント クエリの時間制限を指定します。デフォルトは 10 秒です。

CMDBf エンドポイント

MDR の Query Service エンドポイントを指定します。CMDBf Viewer および更新された MDR データの取得に必要です。MDR プロバイダとして CA CMDB を使用する場合、値は `http://cmdb_hostname:cmdb_port/axis/services/QueryPort` です。

定義を保存します。

URL が定義されます。

注: さらに、URL に置換変数を含めて、MDR に対する CI の限定を追加できます。詳細については、「実装ガイド」を参照してください。

CA APM の MDR プロバイダをセットアップする

CA APM のプロバイダとなる MDR をセットアップできます。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [MDR 管理] - [MDR リスト] をクリックします。
2. [新規作成] をクリックして、CA APM の MDR を指定します。

MDR プロバイダ定義が表示されます。

3. 以下の、必要な MDR プロバイダ情報を入力します。
 - ボタン名 - 「APM」またはその他の有効なボタン名を指定します。「APM」というボタン名を使用することをお勧めします。
 - MDR 名 - CA Asset Portfolio Management r11.3.4 の場合は「APM」と指定し、CA APM r12.6 の場合は「ITAM」と指定します。
 - MDR クラス - 「GLOBAL」と指定します。
 - ホスト名 - CA APM の Web サーバのネットワーク アドレスまたは DNS 名を使用して、CA APM のサーバ名が指定されます。
 - コンテキスト内起動用 URL -
`http://{hostname}:{port}/{path}?{parameters}` と指定します。この URL は変更しないでください。

MDR プロバイダ フォームのパスとパラメータ値には、必要な CA APM コンテキスト内起動の情報が自動的に入力されます。

4. [保存] をクリックします。

CA APM の MDR プロバイダがセットアップされます。

注: MDR ランチャーの詳細については、「実装ガイド」を参照してください。

CA CMDB から CA APM のコンテキストでの起動

CA CMDB MDR ランチャー機能は、CA APM と CA CMDB が同じ MDB を共有している場合の、CA APM のコンテキストでの起動をサポートしています。CA CMDB の UI では、特殊な CA APM MDR プロバイダ定義を作成する際に、[構成アイテムの詳細] フォームの [属性] タブに [コンテキストで起動] ボタンが表示されます。

CA APM MDR 定義には、従来の MDR の機能がすべて含まれます。CA CMDB のバージョン指定機能でも、それぞれの CA APM の変更に関連付けられた属性ログエントリから直接行うコンテキストでの起動がサポートされています。

重要: 他の MDR と異なり、CA APM の MDR はそれぞれの CI やアセットに自動的に関連付けられます。GLOBAL の MDR クラスおよび APM の MDR 名は、CA Asset Portfolio Management r11.3.4 MDR の MDR を識別するために使用されます。GLOBAL の MDR クラスおよび ITAM の MDR 名は、CA APM r12.6 MDR を識別するために使用されます。CA APM の MDR の使用は、他の MDR と完全な互換性があります。これは、CI が同じ場合でも同様です。

MDR Federation をサポートする CI 優先度

構成アイテムのプロパティ（属性）によって、MDR Federation の目的のアセットが識別されます。

統一アセット ID

個人はさまざまな組織にさまざまな ID で把握されます。個人は、以下のような ID で呼ばれます。

- 親しい友人から呼ばれる独特のニックネーム
- 運転免許証（個人に関連付けられた固有の ID）
- 国民兵役 ID（義務兵役サービスカードなど）
- 健康保険証の番号
- 住民票コード

これらの固有の ID はそれぞれが個人を参照しますが、これは適切なりボジトリに個人を記述するのに使用される場合のみ有効になります。

これと同じように、CI には、ソース MDR と関連付けるための ID を複数与えることができます。各 CI は、1 つの MDR から 1 つの ID で把握されます。この ID を統一アセット ID と呼びます。CI を 1 つ以上の MDR に関連付けるプロセスを、CI のマッピングと呼びます。

マッピングは、以下のいずれかの方法で CI がロードされた場合に行われます。

- [管理] ユーザインターフェースを使用した CI マッピングの定義
- GRLoader ユーティリティを使用した CI のロード

MDR 名

MDR 名は、XML や GRLoader を使用してデータをエクスポートする際に、CA CMDB に対する MDR を識別します。MDR は通常、自分自身の識別方法に対する独自の命名規則を持っています。それは、ホスト名に、識別用のインスタンス名またはインスタンス番号を付加するというものです。特定のホストには 1 つしか MDR が存在しないため、多くの場合は MDR がホストサーバ名に設定されます。**CMDBf ビューアに必要です。**

重要: CA Asset Portfolio Management リリース 11.3.4 の MDR 名は APM、CA APM r12.6 の MDR 名は ITAM です。どちらの製品もサポートされますが、製品を実装する前に supportconnect.ca.com で製品の使用可能状況を確認することをお勧めします。

MDR クラス

MDR クラスは、MDR をグループ化するカスタマによって定義されます。

注: CMDBf の MDR クラスは CMDBf の表示に必要です。

重要: MDR 名と MDR クラスを組み合わせたものは、企業内で一意である必要があります。

CA Cohesion ACM のインストールによる MDR 定義

CA Cohesion ACM MDR には、次のような要件があります。

- CA CMDB サーバ上の MDR 定義で指定した `mdr_name` は、ターゲットとなる CA Cohesion ACM サーバ上の `cendura.properties` ファイル内にある `com.cendura.installation.name` 属性の値と完全に一致する必要があります。
- CA Cohesion ACM MDR には、Cohesion という MDR クラスが与えられている必要があります。
- MDR には、CA Cohesion ACM サーバのホスト名とポート番号を指定する必要があります。

MDR ランチャを起動するには、`cendura.properties` ファイルで次の部分を編集します。

```
# -- Configure One-Click Authentication --
com.cendura.security.oneclickauth.secret=shared_secret
com.cendura.security.oneclickauth.scheme=
com.cendura.security.oneclickauth.user=userid
```

重要: `cendura.properties` ファイルで指定するシークレットは、MDR 定義内の共有シークレットと一致させる必要があります。

MDR ランチャはプロパティ ファイル内で指定されたユーザID でログオンするため、プロパティ ファイルのセキュリティ属性を継承します。CI 属性の更新などの機能を使用するには、このユーザに十分な権限が設定されていることを確認します。

注: ユーザを作成してそのユーザのセキュリティ オプションを設定する方法や、プロパティ ファイルをカスタマイズする方法の詳細については、「CA Cohesion ACM 実装ガイド」を参照してください。

CA Cohesion ACM MDR

CA Cohesion ACM サーバのデータをインポートする前に、CA Cohesion ACM MDR を定義する必要があります。CA Cohesion ACM の MDR には、Cohesion という MDR クラスを指定します。

例: Cohesion1 という MDR 定義の場合

Cohesion1 という MDR 定義の場合、XML では cohesion_server という MDR 名と、Cohesion という MDR クラスが指定されます。これらの値は、CI をインポートする際に必要となります。

ボタン名

Cohesion1

MDR 名

cohesion_server

MDR クラス

Cohesion

アクティブ

アクティブ

所有者

CMDBAdmin

説明

シカゴの CA Cohesion ACM サーバ

ホスト名

cohesion_server

Port

8090

パス

CAisd/html/cmdb_cohesion.html

パラメータ

hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id}

userid

cohesion_userid

共有秘密

Chicago01

コンテキストで起動する URL

http://cmdb_hostname:8080/{path}?{parameters}

さらに、このサーバは **Cendura** サーバなので、上記の値は、以下の例に示すとおり、サーバ上にある **cendura.properties** ファイルの値とも一致させる必要があります。

```
com.cendura.security.oneclickauth.secret=Chicago01
com.cendura.installation.name=cohesion_server
```

URL 構文を変更して、特別な要件に対応することができます。

MDR を手動で CI に関連付ける方法

[CA CMDDB 管理] タブで、ツリーの [MDR 管理] ブランチにある統一 CI マッピング機能を使用して、MDR を CI に手動で関連付けることができます。

CI を MDR に関連付ける前に、次の操作を行います。

1. MDR が存在しない場合は、作成します。
2. CI 定義が存在しない場合は、作成します。
3. MDR に接続する CI の固有の統一アセット ID の指定 この ID は MDR 独自のものなので、このドキュメントの対象外になります。

注: 統一アセット ID を指定するには、使用する MDR のドキュメントを参照してください。

CA Cohesion の自動インポート

CA Cohesion ACM から直接 CI をインポートするには、CA Cohesion ACM レポートを実行して、ホスト名、ポート、ユーザ ID およびパスワードを CA CMDB サーバに指定します。CA CMDB に MDR が定義されていれば、Cohesion は XML を自動的に生成して、CI、関係、および CI 上で MDR ランチャを実行するために必要な情報を作成します。レポートは自動的に CI を CA CMDB にインポートします。

注: CA Cohesion ACM からの CI のエクスポートの詳細については、[レポート] - [Report Templates] タブからアクセスできるオンライン ヘルプを参照してください。

MDR への CI のマッピング

各 MDR は `federated_asset_id` を使用して CI を識別するため、1 つの CI を複数の MDR に関連付けることができます。`federated_asset_id` は複数の MDR 間で重複してもかまいませんが、1 つの MDR 内では固有である必要があります。各 MDR には、固有の MDR クラスと MDR 名を指定する必要があります。

重要: CI または MDR プロバイダが非アクティブになると、その CI または MDR プロバイダに関連付けられている統一 CI マッピングもすべて非アクティブになります。

MDR データ プロバイダ定義を作成したら、以下の操作を行います。

1. MDR を参照する CMDB 内に CI を作成します。
2. MDR 定義が機能することを確認します。

MDR は CI のコンテキスト内からしか起動できないため、CI コンテキストを持たない MDR 定義から直接テストすることはできません。

統一 CI マッピング リストは、[管理] タブの [統一 CI マッピング] ノードにあります。

特定の MDR コンテキストで CI を表示するには、MDR の [起動] ボタンをクリックします。

開かれた構成アイテムのコンテキストで、ターゲット MDR が起動します。

例: CI のマッピング

1. [管理] タブをクリックします。
2. [MDR 管理] - [統一 CI マッピング] に移動します。
[統一 CI マッピング] リストが表示されます。
3. [CI 名] フィールドに、「server1」と入力します。

以下の列に値が表示されます。

統一アセット ID

1000234

1000235

CI 名

server1

server1

MDR プロバイダ

Cohesion1

Cohesion2

アクティブ

アクティブ

アクティブ

Cohesion1 MDR プロバイダは、サーバ 1 の存在を認識しており、Cohesion2 MDR プロバイダもサーバ 1 の存在を認識しています。この例では、各 Cohesion MDR が独自にサーバに対して固有の ID を割り当てています。

4. CI 名「server1」をクリックします。
server1 の [構成アイテムの詳細] ページが表示されます。このページには「Cohesion1」および「Cohesion2」という起動ボタンが表示されます。
5. いずれかの MDR プロバイダ起動ボタンをクリックします。
CI に関する詳細が表示されます。

MDR 定義の管理

MDR 定義の管理は、柔軟なプロセスです。CI が MDR 定義を参照していても、MDR 定義のパラメータを変更することが可能です。たとえば、MDR が定義され、CI がロードされた後でも、ボタン名、ホスト名、ユーザ ID、共有シークレットその他を変更することができます。

CA Cohesion ACM のレポート

CA Cohesion ACM を使用すると、レポートの自動更新をスケジュールできます。この機能により、CMDDB を CA Cohesion ACM MDR 内のデータと同期させるプロセスを簡素化できます。無効なパスワード（パスワードの変更や期限切れによる）など、よくあるエラーによって、データのインポートがうまくいかないことがあります。データ インポートのバックグラウンド実行中に発生する可能性のあるエラーが通知されるようにするためには、CA Cohesion ACM で CA CMDDB エクスポート レポートの [通知] オプションを有効にします。そうすると、インポートのエラーが発生したときにレポートが電子メールで送信されます。スケジュール済みタスクとしてバックグラウンドで Cohesion レポートを実行する場合は、通知オプションを有効にすることをお勧めします。

注: 定期的に CA CMDDB エクスポート レポートの実行をスケジュールする方法については、「CA Cohesion ACM Product Guide」を参照してください。

GRLoader の使用

CI をロードするために GRLoader を使用する場合は、MDR ランチャが機能するように XML の以下のフィールドを入力する必要があります。

- <mdr_class>
- <mdr_name>
- <federated_asset_id>

XML 内の <mdr_name> および <mdr_class> に指定する値は、MDR 定義内で指定されている値と完全に一致させる必要があります。

重要: MDR が参照する CI をインポートする前に、管理インターフェースを使用して、MDR 名および MDR クラスを定義しておく必要があります。XML で指定された MDR が定義されていない場合、CI はインポートされません。

GRLoader は、XLS および XLSX 形式のスプレッドシートからの CI および CI 関係のインポートをサポートします。CA SDM に CI データをロードするには、ソースデータを XML または Microsoft Excel スプレッドシートにフォーマットする必要があります。

注: GRLoader を使用したスプレッドシートデータのロードの詳細については、CA CMDB の「テクニカルリファレンスガイド」を参照してください。

CI の命名規則および命名制限

CI には以下の命名規則と命名制限があります。

- CI 名

すべての CI リストで使用される一般的な名前や表示名です。名前の長さの合計が 255 文字を超えないようにする必要があります。CI 名を固有にする必要はありませんが、全体の中で固有にしておくことをお勧めします。また、MDR によって名前が決定される状況の場合、このフィールドに入力する際は、MDR 管理者がユーザに可読な形式の CI 名にするよう、特に注意することをお勧めします。

■ ソフトウェア CI

サードパーティのソフトウェアの場合は、CI で [管理] タブを使用して手動で作成する名前と同じ命名規則に準拠します。命名規則を一致させることにより、CA Cohesion ACM で検出された CI と手動で作成された CI との整合性を保つことができます。この規則に準拠していない場合、ソフトウェアインスタンスは 1 つのみにも関わらず、CI が複数作成される可能性があります。

■ システム名属性の使用

システム名属性は、単一の CI を特定のホスト名に一意に関連付けるものです。

既存の CI と同じシステム名を指定する複数の CI がインポートされる場合、調整機能によって 1 つの CI のみがインポートされるようになります。

例

次の出力行は、サーバ CI（プロバイダ）、ソフトウェア CI（従属）、およびその間の runs 関係を示しています。その結果として作成される関係は、Apache ソフトウェアを実行するサーバを示します。

```
CI: 名前: Server1      クラス: Server   システム名: Server1
CI: 名前: Apache1     ON Server1      クラス: Software
関係: Server1 runs Apache1   ON Server1
```


system_name の命名規則

ほかの MDR を CA Cohesion ACM やさらにほかの MDR と統合し、CI を適切に調整できるようにするには、ソフトウェア CI およびすべての MDR について以下の命名基準に従うことをお勧めします。CA Cohesion ACM でも同じ基準に従っています。

system_name

ソフトウェア CI を一意に指定します。ソフトウェア CI を含む関係を定義するときに、CI 定義内の **system_name** と同じものを指定します。同一のホスト名上のディレクトリに、同一ソフトウェアの同一バージョンの複数のインスタンスをインストールする場合、固有性が保たれるように **system_name** を変更します。**system_name** の長さの合計が 255 文字を超えないようにする必要があります。この制限に違反した場合、データが壊れる可能性があります。

system_name は必ず、単一ホスト上にあるソフトウェアの各インスタンスに固有の ID となる必要があります。

構文は以下のとおりです。

ホスト名 | ソフトウェア名 | バージョン | ビジネス アプリケーション

縦線(|)記号

構文の結合内の複数のフィールドを区切って、検索機能を利用できるようにします。

hostname

ソフトウェアに含まれるホスト名を指定します。

ソフトウェア名

ソフトウェアの一般的な名前を指定します。

version

可能な場合は、ソフトウェアのバージョン番号を指定します。

ビジネス アプリケーション

ホスト名上のソフトウェアの各インスタンスに与える固有の ID を指定します。ソフトウェアのインスタンスがビジネス アプリケーションやサービスと関連付けられている場合は、そのサービスの名前を修飾子にします。 ビジネス アプリケーションを確定できない場合は、インストールディレクトリを使用してソフトウェアを識別できます。このフィールドの長さの合計が 255 文字を超える場合は、省略記号 (...) を使用して、255 文字を超えないようにフィールドの長さの合計を短くします。

UI の検索機能の使用例

UI の検索機能を使用して、ソフトウェア CI を検索するには、以下の例を参照してください。

ユース ケース	名前	system_name
ホスト上のソフトウェア CI xxx の検索		xxx%
ソフトウェアのすべてのイ ンスタンスの検索	yyy	yyy%
ソフトウェアのすべてのイ ンスタンスの検索	yyy バージョン 123.0	yyy% % % 123.0%

上記の検索で返される結果リストには、[名前] フィールドのみが表示されます。

```
mac_address      Null - ソフトウェアには不要
asset_num        Null - ソフトウェアには不要
serial_number    Null - ソフトウェアには不要
dns_name         Null - ソフトウェアには不要
```

CMDBf ドライバの使用

CA SDM は、MDR 全体の CI 統一の結果を表示する CMDBf ビューアを提供します。[構成アイテム詳細] ページ（または CI リストの CI 右クリックで表示されるメニュー）から [CMDBf ビューア] をクリックすると、統一 CMDB と MDR の CI 属性を同時に表示できます。[統一表示] ページで [取得] をクリックすると、すべての統一 MDR からの情報を更新できます。読みやすくするために、CA CMDB メタデータ ファイルでは MDR 属性名および CA CMDB 属性名を調整することができます。

注: この機能には、クエリをサポートする MDR が必要です。MDR CMDBf エンドポイントを編集して、その結果を [統一表示] で表示できます。詳細については、「実装ガイド」を参照してください。

CI に統一データがない場合、ビューアは CA CMDB 属性のみを表示します。

CMDBf マッピングのメタデータ ファイルの更新方法

属性比較をわかりやすくするために、CA CMDB メタデータ ファイルを使って MDR 属性名と CA CMDB 属性名を置換できます。CA CMDB マッピングがない MDR 属性の場合、統一ビューには MDR から送信された属性名が表示されます。CMDBf データ プロバイダにメタデータを定義して、以下を実行できます。

- CA CMDB 属性名を使用して MDR 属性値を表示する
- MDR プロバイダ属性を統一ビューに表示されないようにする
- CA CMDB が対応していない MDR プロバイダ属性を表示する

メタデータは、`cmdb_metadata_federation_viewer_site_attr.htmlpl` ファイルを使って定義します。このファイルには、ファイルを更新する方法が記載されています。メタデータは、すべての CMDB ファミリ（共通属性）またはファミリ固有の属性に適用できます。

外部の MDR 属性名を CA CMDB ラベルにマップするには、`cmdbmetadata` マクロで次のフィールドを使用し、それぞれの `cmdb_metadata_extentiontable.htmlpl` フォームを更新します。

- `mdr_attr` - 置換される MDR 属性の名前
- `mdr_name` - 置換する MDR の名前 正規表現がサポートされています。

例: 属性マッピング

次の 3 つのメタデータ ステートメントは、名前が「myMdr」、または「MDR」で始まるすべてのプロバイダで、CA CMDB の「phys_mem」属性とプロバイダ属性の「mdr_memory」を同一とするメタデータを定義します。また、他のすべてのプロバイダについては、「physical_memory」と「phys_mem」が同一とされます。

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp=" MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=" .*">
```

例: 属性の非表示

次のメタデータ ステートメントは、「myMdr」という名前のすべてのプロバイダで、MDR プロバイダの「widget_cost」属性を非表示にします。

```
<macro name=cmdbMetadata hide_provider_attr="YES"
provider_attr="widget_cost" provider_name="myMdr">
```

例: 属性ラベルの設定

次のメタデータ ステートメントは、CMDBf ビューアの属性カテゴリの下に、ラベル「External Memory Capacity」で属性名「ext_mem_capacity」を定義します。

```
<macro name=cmdbMetadata attr=" ext_mem_capacity" category="Attributes"
heading="External Memory Capacity" help="Total external memory">
```

関連項目:

[MDR 属性値を CA CMDB 属性名で表示する方法](#) (P. 897)

[MDR プロバイダ属性を非表示にする方法](#) (P. 898)

[CA CMDB が対応していない MDR 属性を定義する方法](#) (P. 899)

[CMDBf データ プロバイダ メタデータの定義](#) (P. 899)

MDR 属性値を CA CMDB 属性名で表示する方法

メタデータは、MDR プロバイダ属性と CA CMDB 属性の間に関連を作成できるため、それらを一緒に表示して相違の確認やラベルの共有が可能です。デフォルトでは、マッピングがない MDR 属性はビューアで「**CMDB になし**」と表示されます。

CA CMDB 属性と MDR プロバイダ属性を同一とする `cmdbMetadata` マクロ引数には次のものがあります。

- `attr` – CA CMDB 属性名
- `provider_attr` – MDR プロバイダ属性名
- `provider_name` – MDR プロバイダ名
- `provider_name_regexp` – MDR プロバイダ名正規表現

`provider_name` または `provider_name_regexp` が必要です。

例: MDR 属性と CA CMDB 属性名の関連付け

以下の 3 つのメタデータ ステートメントは、それぞれ次のアクションを実行します。

- 「myMdr」という名前のすべてのプロバイダについて、CA CMDB の「`phys_mem`」属性とプロバイダ属性の「`mdr_memory`」を同一とする
- 名前が「MDR」で始まるすべてのプロバイダについて、CA CMDB の「`phys_mem`」属性とプロバイダ属性の「`mdr_memory`」を同一とする
- 他のすべてのプロバイダについて、「`physical_memory`」と「`phys_mem`」を同一とする

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=".*">
```

MDR プロバイダ属性を非表示にする方法

一部の MDR プロバイダ属性は、統一ビューに表示する必要はありません。ある MDR プロバイダのメタデータを、特定の MDR プロバイダに対して非表示にできます。このオプションは MDR プロバイダ属性にのみ適用され、CA CMDB 属性には適用されません。

プロバイダ属性を非表示にする `cmdbMetadata` マクロ引数には次のものがあります。

- `hide_provider_attr` – "YES" – hides the MDR provider attribute
- `provider_attr` – MDR プロバイダ属性名
- `provider_name` – MDR プロバイダ名
- `provider_name_regexp` – MDR プロバイダ名正規表現

`provider_name` または `provider_name_regexp` が必要です。

例: MDR のみの属性を非表示にする

次のメタデータ ステートメントは、「myMdr」という名のすべてのプロバイダに対して MDR プロバイダの「`widget_cost`」属性を非表示にします。

```
<macro name=cmdbMetadata hide_provider_attr="YES" provider_attr="widget_cost"
provider_name="myMdr">
```

CA CMDB が対応していない MDR 属性を定義する方法

CA CMDB 属性に対応していない MDR プロバイダ属性のラベルとヘルプテキストを定義できます。統一ビューでの属性のラベルは、[ファミリになし] になります。

MDR プロバイダ属性を定義する `cmdbMetadata` マクロ引数には次のものがあります。

- `attr` - CA CMDB 属性名
- `category` - 属性が表示されるカテゴリの名前
- `heading` - 属性の見出しラベル
- `help` - 属性の簡単な説明

例: MDR のみの属性を定義する

次のメタデータ ステートメントは、統一ビューの属性カテゴリの下に、ラベル「External Memory Capacity」で属性名「`ext_mem_capacity`」を定義します。

```
<macro name=cmdbMetadata attr="ext_mem_capacity" category="Attributes"
heading="External Memory Capacity" help="Total external memory">
```

CMDBf データ プロバイダ メタデータの定義

統一ビューでのデータの表示方法を制御できます。

CMDBf ビューアのメタデータを定義する方法

1. Web スクリーン ペインタを使って、
`cmdb_metadata_federation_viewer_site_attr.htm` ファイルを開きます。
2. 必要なメタデータの変更を判断します。
注: このファイルには、サンプルテンプレートが用意されています。
3. 適切なテンプレートをコピーし、ファイル内の指示に従って必要な引数に置き換えます。
4. 変更を保存して発行します。

第 18 章：変更の管理

このセクションには、以下のトピックが含まれています。

- [CA SDM での変更管理 \(P. 901\)](#)
- [変更管理コンポーネント \(P. 902\)](#)
- [変更カレンダーの表示 \(P. 904\)](#)
- [CAB の役割 \(P. 904\)](#)
- [変更マネージャの役割 \(P. 906\)](#)
- [変更マネージャの役割に割り当てるタスクの定義 \(P. 908\)](#)
- [変更カテゴリ、ステータス、およびリスク レベル \(P. 909\)](#)
- [変更要求スコアボードの表示 \(P. 910\)](#)
- [変更要求のストアドクエリの定義 \(P. 911\)](#)
- [変更マネージャ オプションの設定 \(P. 912\)](#)
- [変更カレンダー \(P. 913\)](#)
- [変更要求のスケジュール方法 \(P. 928\)](#)
- [変更ウィンドウのスケジュール方法 \(P. 933\)](#)
- [競合分析と衝突検出 \(P. 937\)](#)
- [CA Workflow の視覚化 \(P. 938\)](#)
- [CA Workflow 用の変更管理プロセス定義 \(P. 940\)](#)
- [CAB コンソールとレポートの作成 \(P. 964\)](#)
- [リスク評価 \(P. 971\)](#)
- [影響度エクスプローラ \(P. 975\)](#)

CA SDM での変更管理

CA SDM 変更管理は、変更マネージャ、変更コーディネータ、および変更諮問委員会（CAB）メンバーが構成アイテム コンポーネントおよびサービスに関する変更リクエストの確認および承認を調整するための機能セットです。たとえば、新たなセキュリティ脆弱性が本番稼動環境に生じないようにするため、変更マネージャはすべての構成アイテム コンポーネントおよびサービスを承認および承認できます。変更マネージャは CAB を主導し、変更要求を最終的に承認する責任を負います。

変更管理には以下の機能があります。

- ITIL プロセスに従って IT の変更をインシデント管理および問題管理に関連付ける。

- 構成アイテムのサービス管理情報（たとえば、特定の構成アイテムに対して記録された変更回数、変更の実行日など）を表示する。
- 複数の変更要求が同じ構成アイテムに対して同時に変更を要求した場合の衝突を検出する。
- 変更カレンダー内に変更ウィンドウを作成し保存する。
- カレンダーで変更要求を作成する。
- 変更に伴うリスクを評価する。

注: 変更管理手順に関する詳細については、オンライン ヘルプの「変更管理」を参照してください。

変更管理コンポーネント

変更管理には以下のコンポーネントがあります。

変更カレンダー

構成アイテムおよびサービスに関するスケジュール済み、完了、失敗、および進行中のすべての変更リクエストを含む[変更イベントをグラフィカルな表示](#) (P. 913)で、設定可能な[カレンダー表示](#) (P. 928)に表示します。また、カレンダーには凍結期間を表す中断日も表示されます。ユーザは、日次、週次、および月次カレンダー ビューのコンテキストメニューから変更要求を作成できます。この機能は、変更マネージャ、レベル 2 のアナリスト、および CAB メンバーが使用します。

変更スケジューラ

構成アイテム変更が許可または禁止される[スケジュールされた期間](#) (P. 934)を変更カレンダーに表示します。変更マネージャは、この機能を使用してその期間のスケジュールと CI の関連付けを表示および作成します。

競合分析と衝突検出

変更要求を分析することで、エラーの発生リスクの確率が高くなる潜在的な実装競合を特定することができます。この機能は変更マネージャが使用します。

ワークフローの視覚化

変更リクエストの承認プロセスを表示します。この機能は変更マネージャが使用します。

CAB コンソールとレポートの作成

CAB の承認が必要な変更要求のオンライン承認をすばやく実行できる [ダッシュボード](#) (P. 964) を表示します。

変更マネージャは、CA SDM を使用して、変更に対して提案されたリクエストのうち CAB による確認の準備が整ったリクエストの詳細が含まれたレポートを作成し、すべての CAB メンバーに電子的に配布できます。

注: 適切な権限を持ったユーザは、変更管理のコンプライアンス、予測、傾向、およびボリュームが事前定義されたレポートを、CA Business Intelligence を使用して BusinessObjects InfoView に表示できます。

リスク評価

サブミットされた各変更リクエストのリスク アセスメントを添付できます。リスク調査オプションを使用すると、調査を作成してリスクの評価を行い、評価結果を変更カテゴリに関連付けることができます。リスク調査には、1 つ以上の選択形式の質問が含まれています。

影響度エクスプローラ

変更要求に添付された複数構成アイテムの、構成アイテム間関係を表示します。影響度エクスプローラは [変更要求の詳細] ページから起動し、オンデマンドで [影響度分析](#) (P. 975) を実行します。この機能は変更マネージャが使用します。

変更検証

変更が正確に実行され、許可されていない変更が実行されていないことを確認し、CMDB にすべての管理対象 CI の現在の正確な状態が含まれるようにします。

変更カレンダーの表示

CA SDM は、変更カレンダーで日付を選択した後に変更要求を表示または作成できる、（ITIL および COBIT 標準に準拠した）さまざまな変更管理機能を起動できます。新しい変更要求は、選択された日に自動的にスケジュールされます。

変更カレンダーは、変更スケジュール、変更要求および CI における競合、不一致、および潜在的なリスクをレポートします。カレンダーを使用して、今後の変更予定や IT 環境への潜在的な影響などを把握できます。

変更カレンダーを表示するには

1. [変更カレンダー] タブをクリックします。
変更カレンダーのフィルタ フィールドが表示されます。
2. 検索フィールドに値を入力して、目的の変更要求のスケジュールを示すカレンダー ビューを表示します。
3. [検索] をクリックします。
変更要求カレンダーには、検索条件に一致する情報が表示されます。

CAB の役割

変更諮問委員会（CAB）は、CI コンポーネントおよびサービスの変更リクエストの確認と承認または拒否を調整します。CAB メンバーは、以下の業務を担当します。

- 運用システムに対する重要な変更をすべて確認する。
- 変更マネージャから要請されたすべての CAB ミーティングに出席する。
- 変更に対してサブミットされたすべてのリクエストを確認して、影響、実装に必要なリソース、および継続的なコストを判断する。
- 変更カレンダーのスケジュールおよび調整作業に参加する。
- すべての変更が適切に評価され、優先度が正しく設定されるようにする。
- インストールの完了後の確認作業に参加する。

関連項目:

[CAB プロセスの仕組み](#) (P. 905)

[CAB グループへのメンバーの割り当て](#) (P. 905)

CAB プロセスの仕組み

CAB には実稼働システムに対する重要な変更をすべて確認する責任があります。変更リクエストの承認が必要な場合は CAB メンバーに通知され、メンバーは以下の処理を行います。

1. CAB による確認が必要な変更リクエストのリストを作成します。
2. CAB コンソールを開き、リクエストの情報を表示します。
3. リクエストに関連付けられた正当化事由、実装計画、構成アイテム、サポート ドキュメントを表示し、承認するか拒否するかを決定します。
4. 変更リクエストを承認または拒否すると、リスト内の次の変更リクエストが自動的に表示されます。

変更をリクエストした個人には変更リクエストの CAB ステータスが更新されたことが自動的に通知されます。

関連項目:

[CAB の役割](#) (P. 904)

CAB グループへのメンバーの割り当て

[メンバーの更新] ページを使用して、メンバーを CAB グループに割り当てることができます。

CAB グループにメンバーを割り当てるには

1. [グループの詳細] ページで、[メンバー] タブを選択します。
2. [メンバーの更新] をクリックします。
[連絡先の検索] ページが表示されます。

3. 目的の連絡先を表示するための検索条件を入力し、[検索] をクリックします。
[メンバーの更新] ページが表示され、検索条件に一致する連絡先がリストされます。
4. 左側のリストで、このグループに割り当てる連絡先を選択します。複数のアイテムを選択するには、**Ctrl** キーを押しながら左マウス ボタンをクリックします。
5. 目的の連絡先をすべて選択したら、選択ボタン (>>) をクリックします。
選択した連絡先が右側の [メンバー] リストに移動します。
6. [OK] をクリックします。
[グループの詳細] ページが表示され、[メンバー] タブに選択した連絡先がリストされます。

変更マネージャの役割

変更マネージャは、企業全体の変更管理プロセスおよび変更要求の最終承認を担当します。また、変更管理メトリック分析レポートを生成し、以下の作業も実行します。

- 変更リクエストを確認し、必要に応じて適切な利害関係者および承認者を追加する。
- 衝突の検出やカレンダーのスケジュール競合の検出などによって、案件を解決する。
- インストール、復旧、およびフォールバック計画のアクセシビリティおよび安定性を確認する。
- 変更によるリスクを理解し、変更に割り当てるリスク レベルが適切であるかどうかを確認する。
- それぞれの担当領域での変更を監視して、テクノロジー変更管理要件に準拠しているかどうかを確認する。
- それぞれの担当領域を代表して、リスク レベルの高い変更による影響を週次の CAB ミーティングで伝える。

- インストールが完了した後で、インストールの問題および変更エラーを確認する。
- 変更の依頼者、利害関係者、承認者、実装担当者、およびサポートグループのエスカレーションポイントとしての役目を果たす。

関連項目:

[変更マネージャの役割の仕組み](#) (P. 907)

変更マネージャの役割の仕組み

変更マネージャは、動作環境への変更要求を監視して、運用チームのメンバーがビジネスポリシーおよびプロセスに従っていることを確認する責任があります。変更カレンダーで、単一または一連の構成アイテムの変更が許可されている中断日および凍結期間をスケジューリングすることで、変更要求の競合といった問題の解決を促進できます。さらに変更マネージャは、以下の処理を実行できます。

1. 変更要求の承認をオンラインですばやく実行したり、変更のリクエストを管理するための CAB コンソールを監視する。
2. 検討中の変更要求に関係するメンバーで構成される CAB を編成し、変更要求を確認するための定期的な CAB ミーティングを実施する。
3. 変更に対して提案されたリクエストのうち CAB による確認の準備が整ったリクエストの詳細が含まれたレポートを作成して、すべての CAB メンバーに電子的に配布する。
4. 変更の各リクエストをリアルタイムで確認し、CAB ミーティングで下された CAB による決定に従ってレコードを更新する。
5. BusinessObjects InfoView を使用して、コンプライアンス、予測、傾向、およびボリューム レポートを管理し、オンデマンドレポートを作成する。
6. それぞれの担当領域を代表して、リスク レベルの高い変更による影響を CAB ミーティングで伝える。
7. 変更によるリスクを評価し、変更に割り当てるリスク レベルが適切かどうかを確認する。

変更マネージャの役割に割り当てるタスクの定義

変更マネージャの役割に割り当てるタスクを定義できます。

変更マネージャの役割に割り当てるタスクを定義するには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。
[役割リスト] ページが表示されます。
2. 変更マネージャの役割を選択します。
変更マネージャの [役割の詳細] ページが表示されます。
3. [編集] をクリックします。
変更マネージャの [役割の更新] ページが表示されます。
4. 以下のタブとフィールドを使用して、変更マネージャの役割に対応するタスクおよびアクセス許可を設定します。
 - 権限
 - 各機能へのアクセス
 - Web インターフェース
 - ナレッジマネジメント
 - KT ドキュメントの表示設定
 - タブ
 - レポート Web フォーム
 - 移動先リソース
 - テナント読み取りアクセス
 - テナント書き込みアクセス
5. [保存] - [ウィンドウを閉じる] をクリックします。
変更マネージャの役割レコードが更新されます。

注: 変更マネージャの [役割の詳細] ページに表示されるタブの詳細については、オンラインヘルプの「役割管理」を参照してください。

変更カテゴリ、ステータス、およびリスクレベル

サービス環境内での変更要求の運用方法を定義できます。CA SDM のインストール時に設定されたデフォルト値を編集するか、独自の値を定義できます。

変更要求のデフォルト値を管理するには

1. [管理] タブで、[Service Desk] - [変更要求] を選択します。
2. [変更要求] ノードを展開し、以下のうちいずれかを選択します。
 - カテゴリ
 - 変更のタイプ
 - クローズ コード
 - 競合ステータス
 - リスク レベル
 - リスク 調査
 - ステータス
 - ワークフロー タスク ステータス コード
 - ワークフロー タスク タイプ選択したアイテムの [リスト] ページが表示されます。
3. 編集するアイテムを選択します。
[更新の詳細] ページが表示されます。
4. ページの一番下にあるタブで使用可能なコントロールを使用して、環境内での変更要求の運用方法を定義します。
5. [保存] - [ウィンドウを閉じる] をクリックします。
更新されたアイテムがリストに表示されます。

変更要求スコアボードの表示

変更要求スコアボードには、変更要求、競合、およびレベル 2 のアナリスト、変更マネージャ、変更コーディネータ、または CAB メンバーに割り当てられたスケジュール済みのタスクが表示されます。ユーザは、割り当て済みのレコードおよび未割り当てのレコードを優先度順に表示できます。

変更要求スコアボードを表示するには

1. CA SDM スコアボードで [変更要求] に移動します。
2. フォルダを展開し、以下に関する入れ子フォルダを表示します。
 - 割り当て済みまたは未割り当てのオープン アイテムおよびクローズ アイテム
 - 解決済みまたは未解決の競合
 - 本日または次週に開始されるスケジュール済みタスク
3. 表示するアイテムのフォルダを選択します。
[リスト] ページが表示されます。
4. (オプション) [フィルタを表示] をクリックし、1 つ以上のフィールドに値を入力して、目的のコメントのみをリストするように検索条件を指定します。
5. [検索] をクリックします。
[リスト] ページには、検索条件に一致するアイテムの概要が表示されます。
6. (オプション) [リスト内で編集] ボタンをクリックして、アイテムに関連付けることのできる追加フィールドを表示します。

変更要求のストアドクエリの定義

変更要求スコアボードでユーザが使用可能なストアドクエリの定義は、管理者が行います。管理者は、CA SDM の定義済みストアドクエリを変更できます。また、独自のクエリを定義することもできます。

変更要求のストアドクエリを定義するには

1. [管理] タブで、[Service Desk] - [アプリケーション データ] - [ストアドクエリ] を選択します。
[ストアドクエリ リスト] が表示されます。
2. 編集するストアドクエリを選択します。
[ストアドクエリの詳細] ページが表示されます。
3. [編集] をクリックします。
[ストアドクエリの更新] ページが表示されます。
4. 必要に応じて、フィールドの値を編集します。
5. [保存] - [ウィンドウを閉じる] をクリックします。
更新されたストアドクエリが [ストアドクエリ リスト] に表示されます。

例: ログイン ユーザが所属する CAB に割り当てられた変更要求を一覧表示するストアドクエリを定義する

この例は、ログイン ユーザが所属する CAB に割り当てられた変更要求のみを一覧表示するストアドクエリの作成方法を示しています。

ストアドクエリを作成するには

1. スコアボードに移動し、[ストアドクエリの更新] ページを表示します。
2. フィールド値を以下のように編集します。
 - a. [スコアボードの使用法] を選択します。
 - b. [タイプ] に [変更要求] を設定します。

c. Where 節を以下のように入力します。

```
cab.[group]group_list.member IN (@cnt.id) AND active = 1
```

3. [保存] - [ウィンドウを閉じる] をクリックします。

ストアドクエリが [ストアドクエリ リスト] に表示されます。

関連項目:

[CAB コンソールとレポートの作成 \(P. 964\)](#)

変更マネージャ オプションの設定

変更マネージャの役割に割り当てるオプションを設定できます。

変更マネージャオプションを設定するには

1. [管理] タブで [オプション マネージャ] を選択します。
2. [変更要求マネージャ] ノードを展開します。
[オプション リスト] が表示されます。
3. 必要なオプションを右クリックし、コンテキスト メニューから [編集] を選択します。
[オプションの更新] ページが表示されます。
4. 必要に応じてオプションを編集します。
5. [保存] - [ウィンドウを閉じる] をクリックします。
更新されたオプションは、オプション リストに表示されます。

変更カレンダー

変更カレンダーには、実装の開始時間と終了時間が設定された変更イベントがグラフィカルに表示されます。変更スケジュールがカレンダーで表示されるため、アナリストやマネージャは、イベントの発生日時とそのイベントが環境、組織、およびリソースに与える影響をすぐに把握できます。

カレンダーを使用すると、日次、週次、および月次のビューから変更要求を作成できます。また、スケジュールされている変更要求をグローバル変更ウィンドウで表示することもできます。1か月に複数の変更ウィンドウが存在する場合、ブラックアウトウィンドウグループなどのように1つのグループにまとめられます。ウィンドウの詳細情報を個別に表示するには、ドリルダウンして週次または日次ビューを参照するか、ポップアップ情報を表示します。

注: 変更ウィンドウではなく変更要求スケジュールのみ[エクスポート](#) (P. 915)できます。

関連項目:

[変更要求へのスケジュール情報の追加](#) (P. 913)

[iCalendar イベント テンプレート](#) (P. 914)

[iCalendar へのスケジュールのエクスポート](#) (P. 915)

[スケジュール ビュー](#) (P. 916)

[スケジュール ビューの環境設定](#) (P. 918)

変更要求へのスケジュール情報の追加

変更要求を作成または編集するときに、スケジュール情報を追加できます。

スケジュール情報を追加する方法

1. 以下のいずれかの操作を実行します。
 - [ファイル] - [新規変更要求] をクリックします。
 - 変更要求をオープンし、[編集] をクリックします。

2. 以下のスケジュール フィールドに値を入力します。

タイプ

ITIL 変更タイプを [標準]、[正常]、または [緊急] として指定します。カテゴリの新規変更要求を初期化するために **CA SDM** が使用する変更カテゴリの変更タイプを、デフォルト値として定義することもできます。

スケジュール開始日

変更要求の開始日を指定します。

期間

「00:00:00」の形式で、変更要求の期間を指定します。

スケジュールには、スケジュールの開始日と期間が設定されている変更要求のみが含まれます。タイプは変更要求をスケジュールでグループ化するのに役立ちますが、スケジュールに直接影響することはありません。

3. 変更要求の作成を続行します。
4. 完了したら、[保存] をクリックします。

スケジュール情報が変更要求に追加されます。

iCalendar イベント テンプレート

iCalendar イベント テンプレートでは、iCalendar 形式でエクスポートする情報を制御します。

以下の定義済みのテンプレートが **CA SDM** と共にインストールされます。

- 変更スケジュール
- KnowledgeScheduleCreation
- KnowledgeScheduleExpired

- KnowledgeScheduleReview
- KnowledgeScheduleStart

注: 事前定義されている iCalendar イベント テンプレート コードは、編集はできますが、削除と新規作成はできません。

重要: web.cfg 内の SchedExpMaximum 変数は、エクスポートを許可するイベントの最大数を制御します。デフォルト値 (1000) を増やすとシステムが不安定になる場合があります。ユーザが SchedExpMaximum で指定された値を超えてエクスポートしようとする、ユーザのエクスポート リクエストを拒否するメッセージが表示されます。

iCalendar へのスケジュールのエクスポート

CA SDM では、iCalendar の標準形式で変更要求をエクスポートできます。このデータ交換では、Microsoft Outlook や Lotus Notes を含む、広く使用されている多数のカレンダー アプリケーションに変更要求スケジュールをインポートできます。

注: スケジュールをエクスポートするときに [保存] オプションではなく [オープン] オプションを選択すると、カレンダー プログラムによってはファイルが正確にインポートされない場合があります。ナレッジ マネジメント スケジュールおよび変更要求スケジュールにおけるこの問題を回避するには、[オープン] オプションではなく、[保存] オプションを選択します。エクスポート済みファイルを保存した後、カレンダー プログラムのインターフェースを介してインポートします。変更 (ブラックアウトと保守) ウィンドウはエクスポートできません。変更要求のみエクスポートできます。

重要: データは、現在のビューに基づいてエクスポートされます。32 日のように期間を指定してエクスポートする場合は、リスト ビューからエクスポートを行う必要があります。リスト ビュー以外でエクスポートすると、ビューは 1 か月または 1 週間で切り捨てられ、残った部分のみがエクスポートされます。

変更カレンダーを表示する方法

1. [変更カレンダー] タブをクリックします。
変更カレンダーのフィルタ フィールドが表示されます。
2. 検索フィールドに値を入力して、目的の変更要求が含まれているカレンダーまたはリスト ビューを表示します。

3. [エクスポート] をクリックします。

[Schedule Export] ページが表示されます。

重要: web.cfg 内の SchedExpMaximum 変数は、エクスポートを許可するイベントの最大数を制御します。デフォルト値 (1000) を増やすとシステムが不安定になる場合があります。ユーザが SchedExpMaximum で指定された値を超えてエクスポートしようとする、ユーザのエクスポート リクエストを拒否するメッセージが表示されます。

4. iCalendar ファイルを保存する場所を入力します。

現在のビューのイベントすべてが含まれる iCalendar ファイルが、指定された場所に保存されます。

スケジュールビュー

CA SDM には以下のスケジュール ビューが用意されています。

リスト

スケジュールの開始日と終了日で並べ替えられたリスト ページを表示します。

月

1 か月分のカレンダーを表示します。

このビューでは、変更要求はグループごとに表示されます。エントリごとに 1 件以上の変更要求がまとめられています。グループの上にマウス ポインタを置くと、グループ内の変更要求の詳細情報が表示されます。グループにフォーカスがあるときに **Alt + 右方向キー** を押すか、グループをクリックすると、n 日ビューのコンテンツが表示されます。

週

1 つの列に 1 週間分の情報を表示します。最初の曜日として設定された曜日が先頭になります。

ビューには、変更が個別に表示されます。また、その週にスケジュールされた変更要求の詳細情報も表示されます。

日

1 日分の変更要求を表示します。

ビューには、変更が個別に表示されます。また、その日にスケジュールされた変更要求の詳細情報も表示されます。

n 日間

ドロップダウン セレクタで指定された日数分の変更要求を表示します。

ビューには、変更が個別に表示されます。また、指定した日数の間にスケジュールされた変更要求の詳細情報も表示されます。

スケジュール ビューの移動

方向キーと **Tab** キーを使用して、スケジュール ビューを移動できます。以下のキーボードショートカットを使用できます。

タブ

後の日付に移動します。スケジュールの最後のセルでこのキーを押すと、[検索] ボタンに移動します。

Shift + Tab キー

前の日付に移動します。スケジュールの最初のセルでこのキーを押すと、[翌月] ボタンに移動します。

Shift + 方向キー

カレンダー内の日付を方向キーの方向に移動します。

右方向キー

現在フォーカスがある日付またはイベントのコンテキスト メニューを表示します。コンテキスト メニューがない場合は、次に大きい日付に移動します (Shift + 右方向キーと同様です)。

Alt + 右方向キー

現在フォーカスがある日付またはイベントのポップアップ情報を表示します。ポップアップ情報がない場合は、次に大きい日付に移動します (Shift + 右方向キーと同様です)。

下方向キー

現在のセルの次のイベントに移動します。現在のセルにイベントがない場合、またはフォーカスがすでに最後のイベントにある場合は、下のセルの日付に移動します（Shift + 下方向キーと同様です）。

上方向キー

現在のセルの前のイベントに移動します。フォーカスがイベントにならない場合は、上のセルの日付に移動します（Shift + 上方向キーと同様です）。

カレンダービューのホットキー

各スケジュールビューは、ボタンへのホットキーアクセスをサポートしています。サポートされているホットキーは以下のとおりです。

Alt + 0

リストビューに切り替えます。

Alt + 1

日次ビューに切り替えます。

Alt + 7

週次ビューに切り替えます。

Alt + 3

月次ビューに切り替えます。

Alt + 9

n 日ビューに切り替えます。

Alt + <

現在のビューの前の期間に移動します。

Alt + >

現在のビューの次の期間に移動します。

スケジュールビューの環境設定

月次または週次のスケジュールビューを設定するには、スケジュールを定義する HTML フォームの <head> セクションで `pdm_macro` ステートメントを指定します。このフォームを編集するには、Web スクリーンペインタのソースビューを使用することをお勧めします。

スケジュールを表示するフォームには以下が含まれている必要があります。

- schedConfig マクロ
- 少なくとも 1 つの schedAttr マクロ
- 少なくとも 1 つの schedGroup マクロ

環境設定マクロは独立したソース ファイルに保存し、メイン ソース ファイル内の `pdm_include` ステートメントで参照します。独立したファイルに保存することにより、メイン ソース ファイルを変更せずに、スケジュールを設定できます。

たとえば、変更カレンダー フォーム `list_chgsched.htmlpl` の環境設定マクロを `list_chgsched_config.htmlpl` というファイルに保存します。ナレッジライフサイクル スケジュールでは、同じマクロを使用して `list_kdsched_config.htmlpl` を変更します。

`list_chgsched_config.htmlpl` と `list_kdsched_config.htmlpl` は以下のディレクトリにあります。

```
$NX_ROOT¥bopcfg¥www¥html¥web¥analyst¥
```

schedAttr マクロ - 保存済みの属性の指定

`schedAttr` マクロでは、リストで選択した各項目の保存済みの属性を指定します。保存済みの属性は、月次ビューではポップアップ情報、月次ビュー以外のビューでは詳細情報または概要情報として使用できます。また、JavaScript 関数の `setSchedEvents()` で使用できます。有効なマクロ引数の値は以下のとおりです。

`attr=xxxx`

(必須) 変更要求やナレッジ ドキュメントなどのスケジュール上のオブジェクトの属性を指定します。ドット付きの属性を使用できます。属性名キーワードの `CInn` を変更カレンダーで使用する、保存済みの情報を持つ、変更要求に関連付けられた最初の `nn` 件の `CI` を含むことを指定できます。

注: この引数は、`schedAttr` マクロで唯一の必須の引数です。

attrRef=.COMMON_NAME|xxxx

SREL 属性のために保存された参照テーブルの属性を保存します（非 SREL 属性は無視されます）。指定する属性名の先頭にはドットを付ける必要があります。

デフォルト：.COMMON_NAME

label=

n 日ビューに属性のラベルを表示します。

デフォルト：属性の Majic DISPLAY_NAME

ident=1|0

属性がオブジェクトの識別子（変更要求の参照番号など）かどうかを指定します。識別子属性は、ポップアップ情報や n 日ビューで、グループ名の前にラベルなしで表示されます。

デフォルト：0

detail=1|0

月次ビュー以外のビューの詳細情報に属性を表示するかどうかを指定します。詳細情報は、ビューの [概要のみ] チェック ボックスがオフのときに表示される情報です。

デフォルト：1

hoverInfo=1|0

月次ビューでグループ上にマウス ポインタが置かれた場合や、グループにフォーカスがあるときにユーザが Alt + 右方向キーを押した場合に、属性をポップアップ情報に表示するかどうかを指定します。

デフォルト：0

summary=1|0

月次ビュー以外のビューの詳細情報に属性を表示するかどうかを指定します。詳細情報は、ビューの [概要のみ] チェック ボックスがオフのときに表示される情報です。

デフォルト：0

注: CA SDM では、属性は、schedAttr マクロと同じ順序で概要情報、詳細情報、またはポップアップ情報に表示されます。

schedConfig マクロ - スケジュールの環境設定

schedConfig マクロでは、フォームにスケジュールが含まれていることを明示し、基本的な環境設定情報を提供します。有効なマクロ引数の値は以下のとおりです。

autosearch=1|0

現在選択されている期間以外のビューをユーザが選択したときに、スケジュールフォームでサーバからデータを再ロードするかどうかを指定します。値を **1**（デフォルト）に設定すると、ユーザが検索フィルタの日付選択範囲から **1** 日以上外れたビューを選択したときに、フォームで検索が自動的に行われます。値を **0** に設定すると、検索を開始するにはユーザが「検索」ボタンを押す必要があります。

defaultView=0|1|7|30|99

0（リスト）、**1**（日次）、**7**（週次）、**30**（月次）、または **99**（*n* 日）で、検索フィルタのデフォルトのビューを指定します。

defaultView 用の指定は、検索フィルタの初期表示のみに影響します。スケジュールを表示した後、CA SDM は、自動的にフィルタビューの選択と現在のビューを連携させます。

デフォルト：30

firstday=0|1|2|3|4|5|6|7

0（日曜）と **6**（土曜）の間の数値で月次ビューの最初の曜日を指定します。

デフォルト：0

export=xxx|0

iCalendar 形式でのエクスポートで使用するテンプレートのコード名を指定します。値を **0** に設定すると、エクスポートの機能とボタンが無効になります。

デフォルト：ChangeSchedule

legend=1|2|0

スケジュール上のグループの名前と形式を表す凡例の場所を指定します。値を **1** に設定すると、スケジュールの上に凡例が表示されます。**2** に設定すると、スケジュールの下に凡例が表示されます。凡例を表示しない場合は、値を **0** に設定します。

デフォルト：2

maxGroups=0/n

カレンダーの月次ビューの 1 つのセルに表示するグループの最大数を指定します。

1 日に対して maxGroups を超えるグループがスケジュールされている場合、CA SDM には maxGroups から 1 を引いた数のグループのみが表示され、最後のグループが [あと nn 件の変更] ハイパーリンクに置き換わります。ユーザは、このハイパーリンクにマウスオーバーするかクリックして、グループの一覧を参照できます。値を 0 に設定すると、この機能は無効になり、カレンダーのセルに表示されるイベントの数は無制限になります。

デフォルト : 4

nday=(n,n,...)

n 日ビューのドロップダウン リストの選択肢を指定します。

ドロップダウン リストで表示する日数のリストを指定します。0 を指定すると、n 日ドロップダウン リストはスケジュールに表示されなくなります。指定した最初の値がドロップダウン リストのデフォルト値になります。

デフォルト : (3,7,14,28)

round=(hr,min)|0

変更要求やナレッジ ドキュメントをグループにまとめるときにスケジュールの開始日と終了日の丸めを行うかどうかを指定します。丸めを行わない場合は round=0 を指定します。

デフォルトでは、スケジュールの開始日と終了日でオブジェクトはグループ化されます。CA SDM の日付にはすべて時間が含まれます。丸めを行わない場合、1 分でも違っていると別のグループに分類されます。丸めを指定すると、開始日を前の時間または分に調整したり、終了日を後の時間または分に調整したりしてグループ化が行われます。

丸めの値には、時間または分のどちらかを指定します（両方は指定できません）。たとえば以下のように、指定した値の最も近い倍数に時間は丸められます。

round=(0,15) 毎時 0 分、15 分、30 分、45 分のうち、最も近い時間に丸められます。

round=(0,30) 毎時 0 分、30 分のうち、最も近い時間に丸められます。

round=1 最も近い正時に丸められます。

round=12 午前 12 時と午後 12 時のうち、最も近い半日に丸められます。

round=24 最も近い日に丸められます。

デフォルト : (0,15)

timefmt=24hr|([am],[pm])

スケジュールのカレンダー ビューの時間形式を指定します。

デフォルト値は 24hr で、24 時間形式 (0:01 ~ 23:59) で時間を表示します。ほかの値 (am、pm) は、午前/午後のどちらかまたは両方を示すサフィックスを付けることを指定します。

注: schedConfig 引数はすべてオプションです。

schedGroup マクロ - イベントグループの指定

schedGroup マクロでは、項目グループの名前とカラー コードを指定します。月次ビューでは、1 つのイベントにグループのすべての項目が集約されます。月次ビュー以外のビューでは、各項目が属するグループの形式で個別の項目が表示されます。有効なマクロ引数の値（オプション）は以下のとおりです。

grpname=xxx

（必須）グループの名前を指定します。マクロは自動的にグループの番号を割り当て、その番号を schedGroup_xxx という名前の JavaScript 変数に割り当てます。xxx はグループの名前になります。この変数は、グループに属するイベントを作成するために setSchedEvents() 関数で 사용됩니다。

注: この引数は、schedGroup マクロで唯一の必須の引数です。

label=xxx

グループのラベルを指定します。値を指定すると、すべてのビューでラベルが表示されます。

legend=xxx|0

スケジュールの下部に表示される凡例にグループの説明を表示します。現在のビューにグループが 1 件でも存在すると、凡例にグループの説明が表示されます。0 を指定すると、グループは凡例から常に除外されます。

デフォルト：0

color=black|color

このグループの項目のテキストの色を指定します。color は、CSS 形式（有効な Web カラー名または # で始まる 16 進数値のどちらか）で指定できます。

例：赤の場合、「#FF0000」または「red」と入力します。

デフォルト：black

bgcolor=white|color

このグループの項目の背景色を指定します。bgcolor は、CSS 形式（有効な Web カラー名または # で始まる 16 進数値のどちらか）で指定できます。

例：赤の場合、「#FF0000」または「red」と入力します。

デフォルト：white

style=normal|bold|italic

このグループのテキストのスタイルを、normal（通常）、bold（太字）、italic（斜体）から指定します。

デフォルト：normal

変更カレンダーの中断ウィンドウおよび保守ウィンドウの設定

`list_chgsched_config.htmlpl` の `PDM_MACRO` ステートメントを編集して、変更ウィンドウの色、ラベル、凡例、およびアイコンを変更します。

注: `schedGroup` マクロを使用して変更カレンダーのウィンドウのフォーマットを変更する場合、変更スケジューラのフォーマットとの一貫性を保つには、`schedule.css` も更新する必要があります。

変更ウィンドウを設定するには、以下の手順に従います。

1. テキスト エディタまたは WSP で `list_chgsched_config.htmlpl` フォームを開きます。

このファイルは以下のディレクトリにあります。

```
$NX_ROOT¥bopcfg¥www¥html¥web¥analyst¥
```

2. `schedGroup` マクロの `PDM_MACRO` ステートメントを以下のように変更します。

保守ウィンドウの場合

```
<PDM_MACRO NAME=schedGroup grpname=maintWindow
  bgcolor=lightgreen
  label="Maintenance"
  legend="Maintenance Window"
  icon= "confirmation_12.png">
```

中断ウィンドウの場合

```
<PDM_MACRO NAME=schedGroup grpname=blackoutWindow style=italic color=white
  bgcolor=black
  label="Blackout"
  legend="Blackout Window"
  icon= "warning_12.png">
```

bgcolor

ウィンドウの背景色を指定します。

label

ウィンドウのラベルとして「中断」または「保守」を指定します。

legend

変更カレンダーに表示する凡例のテキストを指定します。

icon

12x12 ピクセルの Web グラフィックへのオプションの URL を指定します。

このアイコンは、変更要求がすべて保守ウィンドウ内に収まる場合、または中断ウィンドウと重なる場合に、変更要求またはグループと共に変更カレンダーに表示されます。

3. フォームを保存します。

変更ウィンドウが設定されます。

setSchedEvents() JavaScript 関数

setSchedEvents() JavaScript 関数はスケジュールのイベントを作成します。新しいグループ オブジェクトを表示する場合は、この関数を変更します。事前定義されたグループ オブジェクトがデフォルトで表示されます。

CA SDM では、スケジュール検索フィルタで選択されたオブジェクト（変更要求またはナレッジ ドキュメント）ごとに 1 回ずつ **setSchedEvents()** が呼び出されます。この関数は、2 番目の関数 **schedEvent()** を呼び出してイベントのグループ ID、開始日、および終了日を渡し、オブジェクトのイベントを作成します。

setSchedEvents() 関数では、1 つのオブジェクトに対して任意の数のイベント（ゼロを含む）を作成できます。変更カレンダー（[list_chgsched.html](#)）のデフォルトの **setSchedEvents()** 関数は、変更要求ごとに 1 つのイベントを作成し、変更タイプ別に変更要求をグループ化します。この関数は、以下のようにコード化されます。

```
1.     function setSchedEvents( chg )
2.     {
3.         var grpnum;
4.         switch( chg["chgtype"] - 0 ) {
5.             case 100: grpnum = schedGroup_std; break;
6.             case 300: grpnum = schedGroup_emer; break;
7.             default: grpnum = schedGroup_norm; break;
8.         }
9.         chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.    }
```

case パラメータには、変更タイプ ID を指定します。case ID を一覧表示するには、「変更タイプの作成」を参照してください。

この関数には、`schedAttr` マクロによって指定された属性を含む JavaScript オブジェクトの引数が 1 つ指定されています。行 4 から 8 の `switch` ステートメントでは、変更要求の `chgtype` 属性を確認し、前述の `schedGroup` マクロによって定義された `schedGroup_xxxx` 変数の 1 つから適切なグループ番号を割り当てます。行 9 では、`schedEvent()` 関数が呼び出され、以前割り当てたグループ番号およびスケジュールの開始日と終了日が渡されて、スケジュールにイベントが作成されます。開始日と終了日は、事前に `schedAttr` マクロで指定されているため、引数オブジェクトにあります。

変更要求のスケジュール方法

変更要求に関連付けられたすべての構成アイテムのスケジュールを表示できます。変更要求を作成、編集、または表示する場合、あるいは変更カレンダーを更新する場合は、スケジュール情報を考慮してください。スケジュールを表示することで、スケジュールの衝突を避けることができます。

スケジュールを表示および更新するには、以下の手順に従います。

1. 変更要求を作成するか、開きます。
2. 構成アイテムを変更要求に関連付けます。

注: 構成アイテムを変更要求に関連付けないと、[スケジューラ] ボタンをクリックしたときにエラーメッセージが表示されます。

3. [スケジューラの表示] をクリックします。

変更スケジューラに以下のビューが表示されます。

日単位

(デフォルト) 選択された日時に対応する変更要求の期間を表示します。変更要求に日付が関連付けられていない場合、ビューのデフォルトは現在の日付になります。

週単位

現在の週の実装開始日を含む変更要求の期間を表示します。この実装開始日は変更カレンダーの開始日に変更することができます。

注: スケジュール期間によって、スケジュールの網かけ部分の長さが決まります。たとえば、期間を 2 時間に設定した変更要求を作成すると、指定の 2 時間の期間を表す薄い黄色の網かけがスケジューラに表示されます。

4. (オプション) 構成アイテムをクリックして、詳細情報を表示します。構成アイテム名の上にポインタを移動して、完全な名前を表示します。
5. (オプション) [実際の導入開始日] または [期間] を変更します。
 - a. [スケジュールの表示] をクリックして、更新されたスケジュールをプレビューします。
 - b. [スケジュールの更新] をクリックして、スケジュールを更新します。

注: スケジュールは編集モードでのみ変更できます。

6. 変更要求を保存します。
7. 変更カレンダーを更新して、グローバルおよびCIに関連する変更ウィンドウを確認します。

変更スケジュールの使用例

以下の例は、変更要求を作成するときの変更スケジュールの使用方法を示しています。

1. [Service Desk] タブで [ファイル] - [新規変更要求] を選択します。
[変更要求の新規作成] ページが表示されます。
2. [構成アイテム] タブで [構成アイテムの更新] アイテム] タブを選択します。
[構成アイテムの検索] ページが表示されます。
3. 構成アイテムを作成するか検索します。
4. [影響を受ける構成アイテム] ページを使用して、構成アイテムを変更要求に追加します。
5. [OK] をクリックします。
[変更要求の新規作成] ページが更新されます。
6. [スケジュール] ボタンをクリックします。
[変更要求のスケジュール] ページが表示されます。
7. ビューを選択して、以下のいずれかを実行します。
 - テーブルセル内をクリックして、[スケジュール開始日] を変更します。
 - [スケジュール開始日] をクリックして、日付ヘルパを使用します。
8. [期間] を変更して、[スケジュールの表示] をクリックします。
変更されたスケジュールのプレビューが表示されます。
9. [スケジュールの更新] をクリックします。
スケジュールは変更内容で更新されます。
10. 変更要求を保存します。

構成アイテムの最大数の設定

変更スケジューラに表示する構成アイテムの最大数を設定できます。

構成アイテムの最大数を設定するには

1. `NX.env` を開きます。

このファイルは以下のディレクトリにあります。

```
$NX_ROOT¥
```

2. `@NX_CHANGE_SCHEDULER_MAX_CI_CNT` の値を変更して、必要な最大数を設定します。

注: デフォルトでは、変数は **100** に設定されています。 **100** より大きい値を構成アイテムの最大数として設定すると、最初の **100** 件が表示された後で警告メッセージが表示されます。

3. `NX.env` を保存し、CA SDM を再起動します。

構成アイテムの最大数が設定されます。

例: 構成アイテムの最大数を 25 に設定する

以下の設定では、構成アイテムの最初の 25 件のみが変更スケジューラに表示されます。

```
@NX_CHANGE_SCHEDULER_MAX_CI_CNT=25
```

変更要求期間の背景色の変更

変更要求期間の背景色は変更できます。`schedule.css` の以下の行を変更して、変更要求の期間を表す緑色のバーの強調表示を変更します。

背景色を変更するには

1. `schedule.css` を開きます。

このファイルは以下のディレクトリにあります。

```
$NX_ROOT¥bopcfg¥www¥wwwroot¥css
```

重要: `$NX_ROOT¥sdk` にも `schedule.css` という名前のファイルがあります。このファイルには、`css` コントロールに関する役に立つコメントが含まれています。

2. 以下の行を目的のカラー コードに変更します。

```
td.noBorderBackColor{border-left:none;border-right:none;background-color:#F6E3CE;}
td.withBorderBackColor{border-right:none;border-left:1px
solid;background-color:#F6E3CE;}
```

3. `schedule.css` を保存します。

以下の例では、変更期間の背景色は `#FF0000` です。

例: 変更期間の背景色を `#FF0000` に変更する

```
td.noBorderBackColor{border-left:none;border-right:none;background-color:#FF0000;
}
td.withBorderBackColor{border-right:none;border-left:1px
solid;background-color:#FF0000;}
```

変更スケジューラにおける変更ウィンドウの色の変更

変更ウィンドウを示す色を変更するには、`schedule.css` の一部の行を変更します。

注: `schedule.css` を編集して変更スケジューラのウィンドウのフォーマットを変更する場合、変更カレンダーで使用する `schedGroup` マクロも変更しないと変更スケジューラのフォーマットとの一貫性が保たれません。

背景色を変更するには

1. テキスト エディタで `schedule.css` を開きます。

このファイルは以下のディレクトリにあります。

```
$NX_ROOT¥bopcfg¥www¥wwwroot¥css
```

2. 以下の行を目的のカラー コードに変更します。

```
.schedConflict { background-color: #ff0000; font-size: 4px }  
.schedBusy { background-color: #0176ff; font-size: 4px}  
.schedCurrent { background-color: #008000; font-size: 4px; }  
.schedMW { background-color: #40ff40; font-size: 4px; }  
.schedBW { background-color: black; font-size: 4px; }  
.schedNone {font-size: 4px; }  
.schedDialog { width: 100%; height: 4px; margin-left: 0px; margin-right: 0px;  
margin-top: 4px; margin-bottom: 4px; }
```

3. `schedule.css` を保存します。

背景色が変わります。

関連項目:

[schedConfig マクロ - スケジュールの環境設定 \(P. 921\)](#)

変更ウィンドウのスケジュール方法

変更ウィンドウをスケジュールして、変更カレンダーに表示できます。保守ウィンドウは、構成アイテムの変更を許可する期間を設定し、ブラックアウトウィンドウは、構成アイテムの変更を禁止する期間を設定します。変更ウィンドウを利用することで、重要な業務プロセスへの影響を最小限に抑えるよう変更をスケジュールできます。CA SDM では、変更ウィンドウをグローバルレベルまたはシステムレベルで実装できます。

変更ウィンドウをスケジュールするには、以下の手順に従います。

1. 変更カレンダーを表示して、変更ウィンドウを設定する期間を確認します。
2. 組織に適した変更ウィンドウを作成します。

保守ウィンドウ

構成アイテムまたは構成アイテムのセットを変更できるスケジュール期間を示します。変更にはダウンタイムを伴うことがあるため、これらのウィンドウは重要な業務プロセスへの悪影響を最小限に抑えるために使用します。一般に、スケジュール済みの変更は保守ウィンドウ内に発生することが必要です。

中断ウィンドウ

構成アイテム変更が発生しないようにするスケジュール期間を示します。中断としては、サポート体制が手薄な期間（例：連休）、企業イベント、業務的に重要な時期（例：年度末）などが考えられます。一般に、スケジュール済みの変更は中断ウィンドウ外にのみ発生することが必要です。

グローバル変更ウィンドウ

組織全体に対して発生するブラックアウトまたは保守のウィンドウを示します。たとえば、米国の東部時間帯で 11 月に始まり、1 月に終了する「Holiday」という名前の [グローバル](#) (P. 937) ブラックアウトウィンドウを作成します。このブラックアウトウィンドウは、これらの日付間の緊急性のない変更を許可しません。すべての CI に適用されるため、グローバル変更ウィンドウは特定の CI には関連づけられません。

3. （オプション）変更ウィンドウの再帰パターンを指定します。
4. 変更カレンダーを開きます。

凡例には、スケジュール内の変更ウィンドウを識別するためのアイコンと色見本が表示されます。

5. 構成アイテムに関連付けられた変更要求を作成します。
6. 変更スケジューラを使用して、変更カレンダーを更新します。

注: 変更ウィンドウの作成方法の詳細については、オンラインヘルプを参照してください。

変更ウィンドウの表示

変更カレンダーで変更ウィンドウを表示し、関連する CI の変更が許可または禁止されている期間を確認できます。

変更ウィンドウを表示する方法

1. [管理] タブで、[Service Desk] - [変更要求] - [変更ウィンドウ] をクリックします。
[変更ウィンドウ リスト] が表示されます。
2. 表示する変更ウィンドウを選択します。
変更ウィンドウが表示されます。
3. (オプション) [編集] をクリックします。
変更ウィンドウを変更できます。
4. ウィンドウを保存するか閉じます。
[ウィンドウの詳細] ページが表示されます。

CI と保守ウィンドウの関連付け

CI が保守を受ける期間を管理するため、CI を保守ウィンドウに関連付けることができます。

CI と保守ウィンドウを関連付けるには、以下の手順に従います。

1. [変更ウィンドウの詳細] ページに移動します。
2. [関連付けられた CI] タブをクリックします。
[関連付けられた CI] リストが表示されます。
3. [構成アイテムの更新] をクリックします。
[CI グループの検索] ページが表示されます。
4. 必要な CI の情報を指定します。
5. [検索] をクリックします。
[使用可能な CI] ページが表示されます。
6. [使用可能な CI] 内の必要な CI をすべて [関連付けられた CI] リストに移動します。
7. [OK] をクリックします。
[変更ウィンドウの詳細] ページが表示されます。
8. [保存] をクリックします。
CI が保守ウィンドウに関連付けられます。

変更ウィンドウ、CI および選択されたウィンドウの関連付けが保存されます。

関連付けられた CI の表示

特定の期間中にどの CI が影響を受けるかを判断するために、非グローバルの保守ウィンドウと関連付けられる CI を表示できます。

保守ウィンドウと関連付けられた CI を表示するには、以下の手順に従います。

1. [変更ウィンドウの詳細] ページに移動します。
2. [関連付けられた CI] タブをクリックします。
関連付けられた CI が表示されます。

中断ウィンドウの作成例

以下の例では、組織が特定の期間の変更要求をスケジュールしないことを示すためのブラックアウト ウィンドウを作成します。このブラックアウト ウィンドウは 48 時間持続され、ローカル時間で毎週金曜日の午後 6:00 に再現します。

次の手順に従ってください:

1. [管理] タブで、[Service Desk] - [変更要求] - [変更ウィンドウ] をクリックします。
[変更ウィンドウ リスト] が表示されます。
2. [新規作成] をクリックします。
[変更ウィンドウの新規作成] ページが表示されます。
3. 適切なフィールドに以下のように入力します。
 - a. ウィンドウ名に「**Friday_Blackout**」と入力します。
 - b. ウィンドウのタイプに [ブラックアウト] を選択します。
 - c. ステータスに [アクティブ] を選択します。
 - d. 日付ヘルパを使用して、[開始日] に次の金曜日の午後 6:00 を選択します。
 - e. 日付ヘルパを使用して、[終了日] に次の日曜日の午後 6:00 を選択します。
 - f. タイム ゾーンを選択します。
 - g. (オプション) 中断ウィンドウの説明を入力します。
 - h. [反復パターン] タブで [週次] を選択します。
 - 再帰を 1 週間ごとに設定します。
 - 再帰の終了日を選択します。
4. 中断ウィンドウを保存して閉じます。
5. [変更ウィンドウ リスト] を更新します。
6. [変更カレンダー] を開いて更新します。
中断ウィンドウがスケジュールに表示されます。

グローバル保守ウィンドウの作成

組織のグローバル保守ウィンドウを作成します。たとえば、サーバまたはCI別の保守ウィンドウは定義せず、週末にグローバル変更を完了したいとします。

次の手順に従ってください:

1. [変更ウィンドウ リスト] ページに移動します。
2. [新規作成] をクリックします。
3. [変更ウィンドウの新規作成] ページが表示されます。
4. 保守ウィンドウの必要なフィールドに入力するか変更を加えます。
5. [保守] の [タイプ] を設定します。
6. [グローバル] チェック ボックスがオンになっていることを確認します。

注: グローバル保守ウィンドウはCIと関連付けることができません。

7. [開始日]、[終了日]、および [タイムゾーン] を入力します。
8. [保存] をクリックします。

グローバル保守ウィンドウが保存されます。

競合分析と衝突検出

重複分析では、同じ構成アイテムに対する複数の変更が同時に実装用にスケジュールされる場合に発生する衝突が検出され、表示されます。変更管理チームは、以下の方法でスケジュールの衝突を処理します。

- 変更カレンダーを使用して変更要求関連の構成アイテム衝突を確認し、潜在的な影響を抑えるよう調整する。
- ログで衝突を検索して検出する。

注: スケジュールの衝突の処理方法については、オンライン ヘルプを参照してください。

CA Workflow の視覚化

CA Workflow を視覚化すると、変更要求ワークフロー タスクの進捗状況を監視できます。プロセス ビューアには、完了したステップや未完了ステップ、およびワークフローの進行における現在位置を含む、CA Workflow プロセスの各実行ステップがグラフィックで表示されます。

また、プロセスが変更/案件カテゴリまたはリクエスト/インシデント/問題領域に関連付けられている場合、プロセス ビューアには、CA Workflow プロセスのステータスおよびパスも表示されます。

ワークフローの視覚化方法

ワークフローを視覚化するには以下の手順に従います。

1. CA Workflow プロセスを変更カテゴリに関連付けます。
2. その変更カテゴリを使用して変更要求を作成します。
3. [ワークフロー タスク] タブで [プロセスの表示] ボタンをクリックし、プロセス ビューアを起動します。

注: CA Workflow プロセスをカテゴリまたは領域に関連付ける方法については、オンライン ヘルプを参照してください。

プロセスビューアの使用例

この例は、**CA Workflow** をインストールしてオプションを有効にした後に、デフォルトの変更カテゴリを使用してシステムでプロセスビューアを使用する方法を示しています。

1. [管理] タブで、[Service Desk] - [変更要求] - [カテゴリ] に移動します。
[変更カテゴリ リスト] ページが表示されます。
2. [シンボル] 列から [追加.IT.その他] を選択します。
追加.IT.その他の [変更カテゴリの詳細] ページが表示されます。
3. [編集] をクリックします。
追加.IT.その他の [変更カテゴリの更新] ページが表示されます。
4. [ワークフロー] タブをクリックします。
[CA Workflow] チェック ボックスをオンにします。
[ワークフロー定義リスト] が表示されます。
5. [PC の注文 - Service Desk リリース 12.9] を選択します。
プロセス名が [CA Workflow 定義名] フィールドに入力されます。
6. [保存] をクリックします。
[変更カテゴリの詳細] ページが更新されます。
7. ウィンドウを閉じます。
8. [追加.IT.その他] カテゴリを使用して変更要求を作成し、保存します。
[ワークフロー タスク] タブに [PC の注文 - Service Desk リリース 12.9] プロセスおよび [ワーク項目リスト] が表示されます。
9. [ワークフロー タスク] タブで [プロセスの表示] ボタンをクリックします。
プロセスビューアが開きます。

注: ワークフロー タスクの最新の進捗状況を表示するには、プロセスビューアを更新します。

CA Workflow 用の変更管理プロセス定義

変更管理プロセス定義では、標準、正常、または緊急の変更要求が管理されます。変更管理プロセス定義では、CA Workflow の一部として、最初の変更リクエスト以降のすべての変更要求タスクが実装後レビューによって管理されます。各タスクが完了すると、変更管理プロセス定義は変更要求ステータスとアクティビティ ログを更新します。また、変更管理プロセス定義は完了する必要があるタスクに関する電子メールを連絡先またはグループに送信します。

変更管理プロセス定義には、以下の機能があります。

- 変更要求のタイプと関連するリスク レベルを分析し、変更の実装に必要な承認レベルを決定します。
- 変更管理のベースとして使用できるサンプル基盤を提供します。
- リスク評価、影響度と競合の分析、および変更マネージャと CAB の両者による承認に関して、ITIL v3 標準に準拠しています。
- CA SDM の以下の変更管理機能を組み込んでいます。
 - リスク評価調査
 - ビジネス ケース
 - 競合分析
 - 影響度分析
 - クローズ コード
 - ステータス コード
 - 変更タイプ
 - CAB および CAB 承認フラグ

関連項目：

[CA Workflow](#) (P. 453)

変更管理プロセス定義のコンポーネント

変更管理プロセス定義には、以下のコンポーネントがあります。

- **変更管理プロセス定義** - 変更要求プロセス全体を管理するプロセス定義です。すべてのアクティビティおよびサブ アクティビティは、現在の CA Workflow ベスト プラクティスに従って例外を処理します。プロセス定義ファイルの名前は、*r12_Change_Mgmt_[en_language].xml* です。たとえば、英語のプロセス定義の名前は *r12_Change_Mgmt_en_US.xml* です。

注: CA Workflow ベスト プラクティスについては、
https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/7956/7956_tecdoc.html を参照してください。

- **グループ メンバーの取得および通知プロセス定義** - グループに対する電子メール通知を管理する構成要素です。グループ メンバーの取得および通知プロセス定義は、入力としてグループの UUID を受け取ります。グループ メンバーの取得および通知プロセス定義は、通知フラグに応じてすべてのグループ メンバーまたはグループのマネージャのみに電子メールを送信できます。プロセス定義ファイルの名前は、*r12_Get_Group_Mem_Notify_[en_language].xml* です。たとえば、英語のプロセス定義ファイルの名前は *r12_Change_Mgmt_en_US.xml* です。
- **グループ メンバーの取得および通知アクター** - グループ メンバーの取得および通知プロセス定義を呼び出すアクターです。アクター ファイルの名前は、*r12_Get_Group_Mem_Notify_Actor_[en_language].xml* です。たとえば、英語のアクター ファイルの名前は *r12_Get_Group_Mem_Notify_Actor_en_US.xml* です。
- **日時変換** - 入力として日付と時刻を受け取り、承認フォームの [スケジュール開始日] および [スケジュール終了日] フィールドに判読可能な日付と時刻の文字列を設定します。日時変換アクターは、CA Workflow の JavaScript アクターです。アクター ファイルの名前は、*r12_Date_Time_Convert_Actor_[en_language].xml* です。たとえば、英語のアクター ファイルの名前は *r12_Date_Time_Convert_Actor_en_US.xml* です。

変更管理プロセス定義の設定方法

変更管理プロセス定義を設定するには、以下の手順に従います。

1. **CA Workflow** を使用して、アクティビティ ノード、サブ アクティビティ、および通知に関する [ドキュメントを確認](#) (P. 942) します。
2. 変更プロセスの管理を担当する [CAB および実装グループ](#) (P. 944) を作成します。
3. [連絡先を作成](#) (P. 945) し、CAB または実装グループに割り当てます。
4. 変更管理プロセス定義の [電子メール通知を設定](#) (P. 943) します。
5. デフォルトの Tomcat サーバ ポート (8090) を使用しない場合は、**CA Workflow** と **CA SDM** が適切に通信できるように [Tomcat サーバを設定](#) (P. 946) します。
6. 変更管理プロセス定義を使用するために、[1 つ以上の変更カテゴリを設定](#) (P. 947) します。
7. オプション マネージャに [Category Defaults オプションをインストール](#) (P. 948) します。

アクティビティ ノードと属性に関するドキュメントの表示

変更管理プロセス定義に含まれるアクティビティ ノードと属性はすべてドキュメントに記載されているため、**CA Workflow** を使用してアクティビティ ノードと属性に関する情報を表示できます。必要な場合は、組織のニーズに合わせてプロセス定義のフローを変更できます。

注: アクティビティ ノードと属性の表示については、**CA Workflow** のマニュアルを参照してください。

アクティビティ ノードと属性に関するドキュメントを表示する方法

1. **CA Workflow** アプリケーションで [変更管理] をクリックし、**Service Desk r12.1** のプロセス定義を開きます。
CA Workflow に変更管理プロセス定義が表示されます。
2. アクティビティ ノードをダブルクリックします。
アクティビティ ノードが開きます。

3. [プロパティ] タブの [説明] フィールドで、ノードに関する詳細を確認します。
4. アクティビティ ノードのプロパティを終了します。
5. (オプション) プロセス定義ウィンドウの下部にある [属性] タブに移動します。
6. 属性をダブルクリックするか、属性の上にマウス ポインタを置きます。
[属性] ページが開き、その属性に関する情報が表示されます。

サブ アクティビティの表示

変更管理プロセス定義では、CA Workflow のサブ アクティビティを使用してワークフローが簡素化されます。 変更管理プロセス定義を使用しながら、必要に応じてサブ アクティビティを確認およびカスタマイズできます。

サブ アクティビティを表示する方法

1. CA Workflow アプリケーションで [変更管理] をクリックし、Service Desk r12.1 のプロセス定義を開きます。
CA Workflow に変更管理プロセス定義が表示されます。
2. プラス (+) 記号が付いたノードを左クリックし、[タブで開く] または [インラインで開く] を選択します。
サブ アクティビティの詳細が、新しいタブまたはプロセス定義アクティビティの横に表示されます。

変更管理の連絡先に対する電子メール通知の設定方法

変更管理タスクの割り当てとステータス変更に関する電子メール通知が送信されます。 電子メール通知には、追加のレビューが必要なワーク リストまたは変更要求へのリンクが含まれています。 電子メール通知は変更管理プロセス定義によって送信されるため、電子メールの設定が必要です。

変更管理の連絡先に対する電子メール通知を設定するには、以下の手順に従います。

1. [管理] タブで、[オプション マネージャ] - [電子メール オプション] を選択します。
[オプション リスト] が表示されます。
2. 組織に適した電子メール オプションを設定します。

注: 電子メールの設定については、オンライン ヘルプを参照してください。

変更管理プロセス グループの作成方法

承認と追加タスクを担当する変更管理プロセス グループを作成する場合は、以下の点を考慮してください。

- CA SDM と CA EEM の名前が一致する限り、任意のグループ名を使用できます。
- CA SDM のグループ名は、CA EEM のグループ フォルダ名とも一致する必要があります。
- 各グループには複数のメンバーが必要です。
- グループのメンバーは CA SDM と CA EEM で一致します。たとえば、CA SDM の CAB グループに 4 人のメンバーがいる場合は、CA EEM の CAB グループにも同じメンバーがいます。

注: CA SDM および CA EEM のグループの作成については、オンライン ヘルプおよび CA EEM のマニュアルを参照してください。

変更管理グループを作成するには、以下の手順に従います。

1. [管理] タブで、[セキュリティと役割の管理] - [グループ] を選択します。
[グループの検索] ページが表示されます。
2. [新規作成] をクリックします。
[新規グループの作成] ページが表示されます。
3. CA SDM で以下のグループを作成します。
 - **CAB グループ** - 変更カテゴリまたは変更要求に関連付けられた CAB グループです。
 - **実装グループ** - 変更カテゴリまたは変更要求に割り当てられた実装グループです。

4. [保存] をクリックします。
[グループの詳細] ページが表示されます。
5. CA EEM で同じグループを作成します。

関連項目:

[CAB グループの管理](#) (P. 966)

[CAB グループの割り当て](#) (P. 968)

変更管理プロセスの連絡先の作成方法

変更管理プロセス定義を使用するときは、変更プロセス全体で承認と追加タスクを担当する連絡先を作成します。連絡先を[変更管理プロセスグループ](#) (P. 944)に割り当てることもできます。

変更管理プロセスの連絡先を作成するには、以下の手順に従います。

1. [管理] タブで、[セキュリティと役割の管理] - [連絡先] を選択します。
[連絡先の検索] ページが表示されます。
2. [新規作成] をクリックします。
[連絡先の新規作成] ページが表示されます。
3. 有効な電子メール アドレスを持つ以下の連絡先を作成し、適切なグループに割り当てます。
 - **依頼者** - 変更リクエストをサブミットする 1 人以上の連絡先です。
 - **変更マネージャ** - 実装グループのマネージャである連絡先です。
実装グループに所属する変更マネージャは 1 人のみです。
 - **CAB マネージャ** - CAB グループのマネージャである連絡先です。
CAB グループに所属する CAB マネージャは 1 人のみです。

[連絡先の詳細グループ] タブに、現在のグループ割り当てが一覧表示されます。

4. [実装グループの詳細] ページの [メンバー] タブで、変更マネージャと CAB マネージャにマネージャ フラグを設定します。
5. [保存] をクリックします。

以下の連絡先に関して、[メンバー] タブに [マネージャ] - [はい] が表示されます。

- 変更マネージャ
- CAB マネージャ

6. CA EEM で同じ連絡先を作成し、CA EEM のグループに割り当てます。

注:連絡先名として、有効なユーザ名やシステム ログインを使用できます。CA SDM および CA EEM の連絡先の作成については、オンライン ヘルプおよび CA EEM のマニュアルを参照してください。

CA Workflow Tomcat サーバ用の代替ポートの指定

CA Workflow Tomcat サーバがデフォルト ポート (8090) 以外のポートで実行されている場合は、CA Workflow が CA SDM と通信できるようにポートを設定します。

CA Workflow Tomcat サーバ用の代替ポートを指定する方法

1. CA Workflow アプリケーションを起動します。
[CA Workflow] ページが表示されます。
2. [アクター] タブをクリックします。
[アクター タイプ/アクター] リストが表示されます
3. [JavaScript] - [USD_Initializer] を選択します。
[アクティビティ オプション CA Workflow] ページが表示されます。
4. [グローバル属性の取得] をダブルクリックします。
[JavaScript 操作] ページが表示されます。
5. WFTomcatPort の値を CA Workflow Tomcat が使用する新しいポートに変更します。
6. [OK] をクリックします。

CA Workflow が CA SDM と通信できるように Tomcat サーバが設定されます。

変更カテゴリの設定

変更管理プロセス定義の変更カテゴリを指定すると、そのカテゴリを使用するすべての新規変更要求で自動的に変更管理プロセス定義が起動されます。事前設定されたすべての変更カテゴリの値が変更要求に自動的に入力されます。

変更カテゴリを設定する方法

1. [管理] タブで、[Service Desk マネージャ] - [変更要求] - [カテゴリ] を選択します。
[変更カテゴリ リスト] が表示されます。
2. 変更カテゴリを作成するか、または既存の変更カテゴリを開きます。
[変更カテゴリの詳細] ページが表示されます。
3. [ワークフロー] タブで、[CA Workflow を使用] をクリックします。
4. [CA Workflow 定義] リンクをクリックします。
[CA Workflow 定義リスト] が表示されます。
5. [変更管理] - [Service Desk r12.1] をクリックします。
6. [OK] をクリックします。
[変更カテゴリの詳細] ページが表示されます。
7. (オプション) [CAB]、[グループ]、および[リスク調査] を割り当てます。
8. [保存] をクリックします。

このカテゴリを使用する次の新しい変更要求で、変更管理プロセス定義が自動的に起動し、変更カテゴリの値が使用されます。

注: 変更カテゴリの作成および編集方法については、オンライン ヘルプを参照してください。

オプション マネージャへの Category_Defaults オプションのインストール

Category_Defaults オプションでは、カテゴリ フィールドを使用して変更要求の [CAB]、[グループ]、および [リスク調査] が入力されます。たとえば、あるカテゴリに指定した CAB グループは、そのカテゴリを使用するすべての新しい変更要求に表示されます。

オプション マネージャに Category_Defaults オプションをインストールする方法

1. [管理] タブで、[オプション マネージャ] - [変更要求マネージャ] - [Category_Defaults] を選択します。
[オプション リスト] が表示されます。
2. [Category_Defaults の編集] を右クリックします。
[Category_Defaults の更新オプション] ページが表示されます。
3. [インストール] をクリックします。
4. CA SDM サービスを再起動します。
新しい変更要求にカテゴリの値が自動的に取り込まれます。

変更管理プロセス定義の動作のしくみ

依頼者が変更管理プロセス定義を使用するカテゴリで変更要求を保存すると、変更管理プロセス定義が自動的に呼び出されます。

以下の手順は、CA SDM で変更管理プロセス定義がどのように動作するかを示しています。

1. 依頼者は、以下の情報を含む変更要求を開いて保存します。

依頼者

変更要求を開いたユーザを識別します。

変更カテゴリ

変更要求カテゴリを識別します。

タイプ

変更要求のタイプ（標準、正常、緊急など）を識別します。このタイプをワークフロープロセスの一部として更新することもできます。

概要/説明

変更要求の理由について説明します。

スケジュール開始日

開始日を識別します。

期間

変更の予定期間を指定します。

CI

影響を受ける CI を少なくとも 1 つ識別します。

変更管理プロセス定義が起動します。依頼者は、リスク評価調査を実行するように求める電子メール通知を受信します。

2. 依頼者は、変更要求をレビューし、変更要求によるサーバ、アプリケーション、およびユーザへの影響について説明する [リスク評価調査](#) (P. 956) を実行します。

変更管理プロセス定義によって回答が分析されます。これによって、リスクが判定され、変更要求が適切なプロセスパスに従っていることが保証されます。依頼者は、競合および影響度分析を実行するように求める電子メール通知を受信します。

3. [競合および影響度分析](#) (P. 957) では、依頼者がスケジュールの競合をチェックし、CI に対する変更要求の影響を分析します。

依頼者は、変更分析を実行するように求める電子メール通知を受信します。

4. [変更分析](#) (P. 958) では、依頼者が変更のタイプ、変更の理由、ビジネスへの影響、および変更の全体的な影響を識別してサブミットします。

変更マネージャは、変更要求を承認するように求める電子メール通知を受信します。変更要求が高リスクである場合は、CAB グループも通知を受信します。

5. 変更マネージャは、変更分析をレビューし、レビューに関するコメントを入力します。変更マネージャは、[変更要求を承認するか、拒否するか、または不完全としてマーク](#) (P. 957) します。

これに合わせて「変更要求の詳細」ページが更新され、以下のいずれかのアクションが実行されます。

- 変更要求が承認され、CAB 承認が必要でない場合は、実装グループが通知を受信します。変更要求の「ステータス」 - 「承認済み」が表示されます。
- 変更要求が承認され、追加の CAB 承認が必要である場合は、CAB のマネージャとメンバーが承認を求める通知を受信します。変更要求の「ステータス」 - 「承認中」が表示されます。
- 変更要求が拒否された場合は、変更要求の「ステータス」 - 「拒否」が表示されます。
- 変更要求が不完全としてマークされた場合は、変更要求の「ステータス」 - 「不完全」が表示されます。

6. 実装グループのメンバーは、承認された変更要求に関して[実装の開始](#) (P. 961)を確認し、変更を実装します。

変更要求の「ステータス」 - 「実装中」が表示されます。

7. 実装マネージャは、作業が完了すると、変更結果の詳細について説明するために[実装後レビュー](#) (P. 963) (PIR) を実行します。

CA Workflow によって変更要求が閉じられます。変更要求の「クローズコード」と「ステータス」 - 「実装済み」が表示されます。

関連項目:

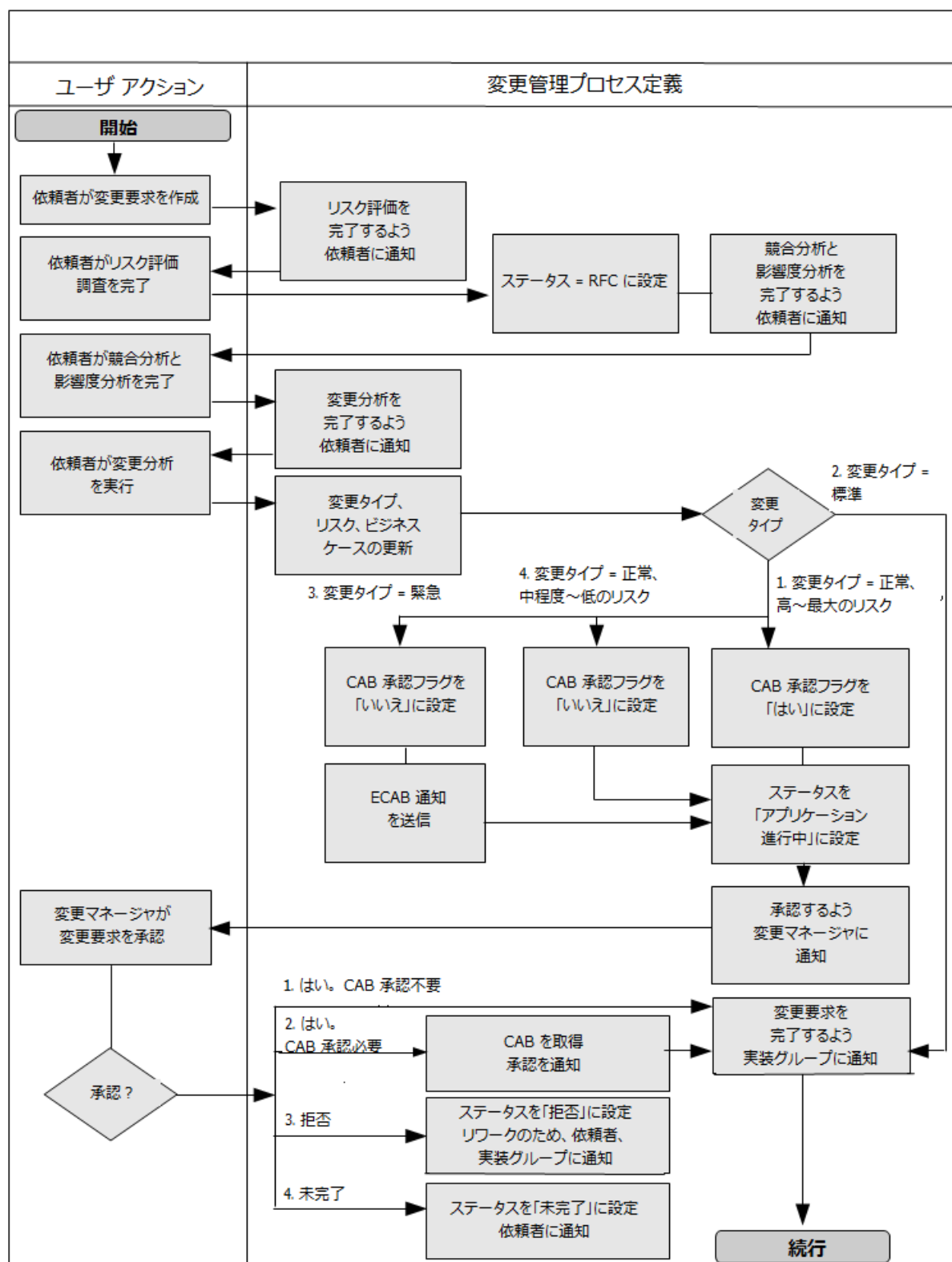
[デフォルトのリスク調査の表示](#) (P. 972)

[リスク調査の実装方法](#) (P. 972)

[変更管理プロセス定義の設定方法](#) (P. 942)

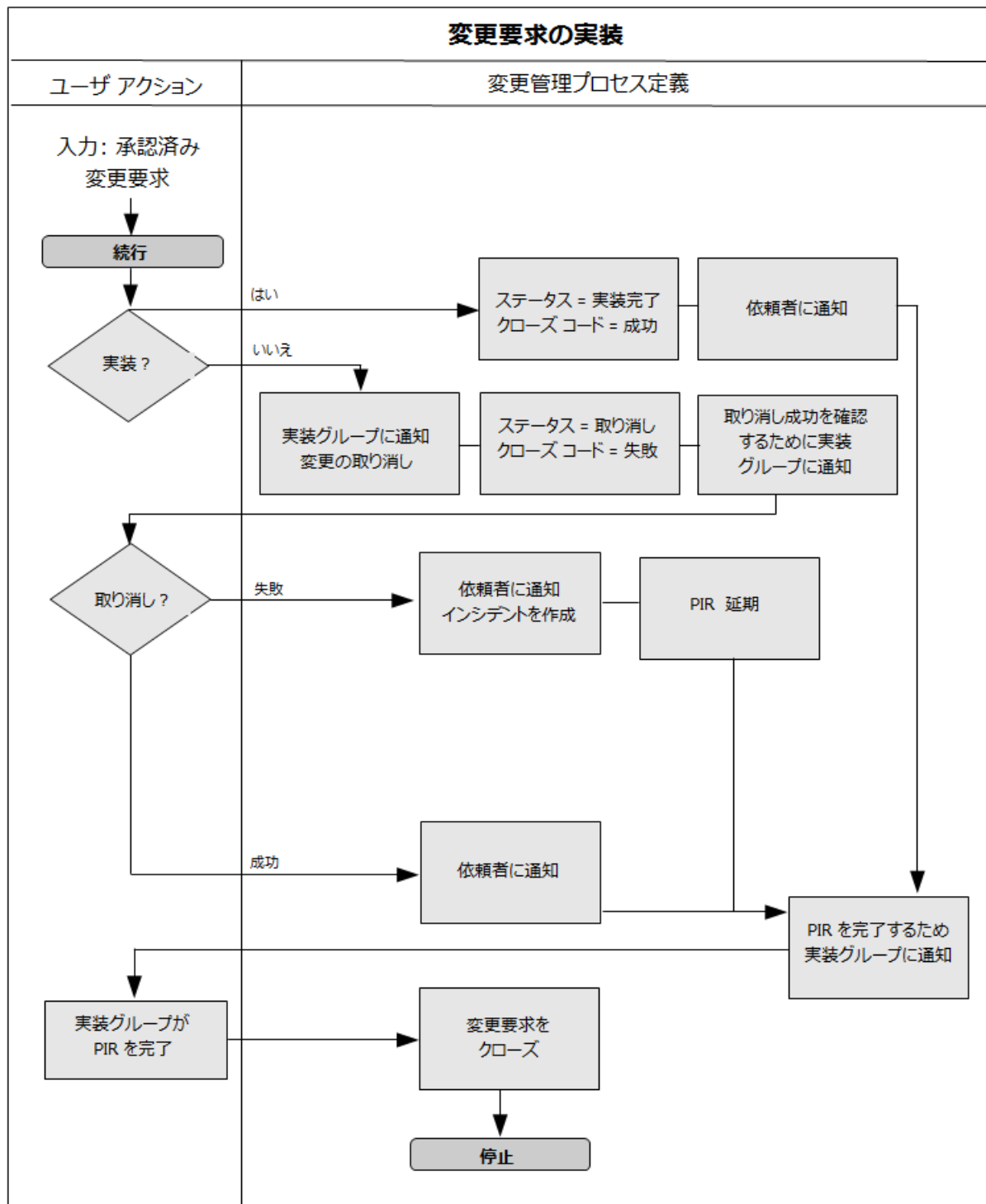
CM プロセス定義による CO 承認の管理方法

以下の図は、[変更管理プロセス定義](#) (P. 948)が新しい変更要求の承認をどのように管理するかを示しています。



CM プロセス定義による CO 実装の管理方法

以下の図は、[変更管理プロセス定義](#) (P. 948)が変更要求の実装をどのように管理するかを示しています。



リスク評価調査の実行

変更要求を作成すると、その変更要求に関するリスク評価調査を実行するように通知されます。依頼者は、システムやサービスを変更する前に、変更カテゴリに属する変更要求のリスクを特定、評価、および定量化します。

リスク評価調査を実行する方法

1. [リスク評価調査] の電子メール通知リンクをクリックして変更要求を開きます。

[変更要求の詳細] ページが表示されます。

2. [ワークフロー タスク] タブで、[依頼者のリスク評価調査] リンクをクリックし、調査の実行手順に従います。

CA Workflow のワーク リストが表示されます。

3. [タスク] タブで、[実行] リンクをクリックします。

[タスクの実行] ページが表示されます。

4. 手順をメモして、リンクをクリックします。

[リスク調査] が表示されます。

5. 変更管理プロセス ワークフローによって変更の適切なリスク パスが正確に評価されるように、調査の質問に慎重に回答します。

6. [サブミット] をクリックします。

[タスクの実行] ページが表示されます。

7. [確認] をクリックします。

[変更要求の詳細] ページに [ステータス] - [RFC] が表示されます。依頼者は、競合および影響度分析を実行するように求める電子メール通知を受信します。

関連項目:

[URL からリスク調査に直接アクセスする方法 \(P. 974\)](#)

競合および影響度分析の実行

競合および影響度分析では、依頼者がスケジュールの競合をチェックし、CI に対する変更要求の影響を分析します。

競合および影響度分析を実行する方法

1. 電子メール通知リンクをクリックして変更要求を開きます。
[変更要求の詳細] ページが表示されます。
2. [ワークフロー タスク] タブで、[依頼者の影響度および競合分析] リンクをクリックします。
[タスク] ページが表示されます。
3. [タスク] タブで、[実行] リンクをクリックします。
[タスクの実行] ページが表示されます。
4. [影響度および競合分析] の手順をメモして、リンクをクリックします。
[変更要求の詳細] ページが表示されます。
5. [変更要求の競合] タブで [競合分析] をクリックして、すべてのスケジュール競合および未処理の競合を解決します。すべての競合を解決してから変更を実装してください。
[競合リスト] が表示されます。
6. [構成アイテム] タブで [影響度分析] をクリックして、CI に関する詳細情報を確認します。
[構成アイテム リスト] が表示されます。
7. [構成アイテム] タブで、各 CI に関する情報を確認するため、[項目] タブで [影響度エクスプローラ] をクリックします。
[影響度エクスプローラ] が表示されます。
8. CI の関係をグラフィカルに表示するため、[Visualizer] をクリックします。
注: [Visualizer] ボタンは、CA CMDB がインストールされている場合にのみ使用できます。
9. [タスクの実行] ページに戻り、[確認] をクリックします。
[ワークフロー タスク] タブに、変更分析を起動するためのリンクが表示されます。依頼者は、変更分析を実行するように求める電子メール通知を受信します。

関連項目:

[影響度エクスプローラ](#) (P. 975)

[影響度エクスプローラからの CMDB Visualizer の起動](#) (P. 979)

変更分析の実行

変更分析では、依頼者が以下の情報を識別して記録します。

- 変更のタイプ
- 変更の原因
- ビジネスへの影響
- 変更の全体的な影響

変更分析を実行する方法

1. 電子メール通知リンクをクリックして変更要求を開きます。
[変更要求の詳細] ページが表示されます。
2. [ワークフロー タスク] タブで、[依頼者変更分析フォーム] リンクをクリックします。
[タスク] ページが表示されます。
3. [タスク] タブで、[実行] リンクをクリックします。
[変更分析] ページが表示されます。
4. [変更分析] タブで、変更要求を確認するための質問に回答して [サブミット] をクリックします。たとえば、分析内容を要約し、変更要求の目的について説明します。必要な場合は、変更要求が繰り返しと再作業のどちらであるかを示します。ビジネスへの影響と変更の全体的な影響について要約します。

変更のタイプとリスクに基づいて、以下のアクションが実行されます。

- 変更のタイプが「正常」で、リスクが「高」～「極度」である場合は、[変更要求の詳細] ページに以下が表示されます。
 - [CAB 承認] - [はい]
 - [ステータス] - [承認中]

変更要求を承認するように変更マネージャに通知されます。変更マネージャが承認すると、追加の承認を行うように CAB グループに通知されます。

- 変更のタイプが「正常」で、リスクが「中」～「低」である場合は、[変更要求の詳細] ページに以下が表示されます。

- [CAB 承認] - [いいえ]
- [ステータス] - [承認中]

変更要求を承認するように変更マネージャに通知されます。

- 変更のタイプが「標準」である場合は、変更を実装するように実装グループに通知されます。
- 変更のタイプが「緊急」である場合は、[変更要求の詳細] ページに [CAB 承認] - [いいえ] が表示されます。

ECAB に通知されます。ECAB が変更要求を処理すると、[変更要求の詳細] ページに [ステータス] - [承認中] が表示され、変更マネージャが変更要求を承認するように求める通知を受信します。

変更要求を承認するか、拒否するか、または不完全としてマークします。

変更管理プロセス定義を使用する変更要求の承認プロセスは、変更要求のタイプとリスクレベルに基づいて行われます。変更要求の承認者は、変更要求の以下の値によって決まります。

- 変更要求のタイプが「正常」で、リスクが「中」～「低」である場合は、変更マネージャの承認のみが必要です。
- 変更要求のタイプが「正常」で、リスクが「高」～「極度」である場合は、CAB メンバーの承認が必要です。
- 変更要求のタイプが「標準」である場合は、承認は必要ありません。変更要求を処理するように実装グループに通知されます。
- 変更のタイプが「緊急」である場合は、ECAB グループに通知されます。変更要求の [ステータス] - [承認中] が表示されます。変更要求を承認する準備ができると、変更マネージャに通知されます。

承認者は、変更分析の情報をレビューし、変更要求を承認するか、拒否するか、または不完全としてマークするかを決定します。

変更要求を承認するか、拒否するか、または不完全としてマークする方法

1. 電子メール通知リンクをクリックして変更要求を開きます。

[変更要求の詳細] ページが表示されます。

2. [ワークフロー タスク] タブで、[変更マネージャ承認フォーム] リンクをクリックします。
[タスク] ページが表示されます。
3. [タスク] タブで、[実行] リンクをクリックします。
[CAB 承認] または [変更マネージャ承認] ページが表示されます。
4. [変更分析] タブで、変更要求に関する追加情報を確認します。
5. 必要な承認レベルに基づいて、以下のいずれかの承認タブを選択し、承認の質問に回答します。

変更マネージャ承認

変更要求に関する変更マネージャの意思決定について説明します。

CAB 承認

変更要求に関する CAB 承認者の意思決定について説明します。

6. 以下のいずれかの承認レベルを選択します。

承認

変更要求を承認します。

拒否

変更要求を拒否します。

不完全

変更要求を不完全としてマークします。

[結果] ページが表示されます。承認レベルに基づいて、以下のアクションが実行されます。

- 変更要求を承認し、追加の CAB 承認が必要でない場合は、[変更要求の詳細] ページに [ステータス] - [承認済み] が表示され、実装グループが作業の開始を求める通知を受信します。
- 変更要求を承認し、CAB 承認が必要である場合は、[変更要求の詳細] ページに [ステータス] - [承認中] が表示されます。また、CAB グループも通知を受信します。
- 変更要求を拒否すると、[変更要求の詳細] ページに [ステータス] - [拒否] が表示され、依頼者と実装グループが通知を受信します。
- 変更要求が不完全である場合は、[変更要求の詳細] ページに [ステータス] - [不完全] が表示され、依頼者が通知を受信します。

関連項目:

[CAB プロセスの仕組み](#) (P. 905)

[CAB 承認](#) (P. 968)

[CAB の役割](#) (P. 904)

変更要求の実装

実装グループは、特定の変更要求に関して 1 つ以上のワーク項目を実行します。実装グループのメンバーは、変更に関する情報を報告します。

次の手順に従ってください:

1. 実装グループのメンバーとして CA SDM にログインし、変更要求を開きます。
[変更要求の詳細] ページが開きます。
2. [追加情報] - [ワークフロー タスク] タブで、[変更要求の実装] リンクをクリックします。
[タスク リスト] ページが開きます。
3. [タスク] タブで、[実行] リンクをクリックします。
[タスクの実行] ページが開きます。
4. 変更要求のレビュー確認手順に従い、[確認] をクリックします。
[変更要求の詳細] ページに [ステータス] - [実装中] が表示されます。
5. 変更を行います。たとえば、変更要求によって Exchange Server 1 と Exchange Server 2 にウィルス対策プログラムのパッチをインストールするように指示された場合は、社内のガイドラインと標準に従って変更要求を完了します。
6. [ワークフロー タスク] タブで、[実装完了フォーム] リンクをクリックします。
[タスク] ページが開きます。

7. [タスク] タブで、[実行] リンクをクリックします。
[実装完了] ページが開きます。
8. [実装完了] タブで、実装グループによる変更要求の実装方法について説明するための質問に回答して、以下のいずれかのオプションをクリックします。

完了

すべての変更要求タスクが正常に完了したことを示します。変更要求の[ステータス]が[実装完了]に設定され、[クローズコード]が[成功]に設定されます。

未完了

変更要求の1つ以上の項目が完了できないことを示します。

依頼者は、変更要求の完了または取り消しに関する通知を1つ以上受信します。また、以下のいずれかの方法でシステムが応答します。

- 変更要求が完了した場合は、[変更要求の詳細] ページに以下が表示されます。
 - [ステータス] - [実装完了]
 - [クローズコード] - [成功]

実装後レビューを実行するように実装グループに通知されます。

- 変更要求が完了しなかった場合は、[変更要求の詳細] ページに以下が表示されます。
 - [ステータス] - [取り消し]
 - [クローズコード] - [失敗]

取り消しに成功したかどうかを判定するように実装グループに通知されます。

取り消しに成功した場合は、実装後レビューを実行するように実装グループに通知されます。取り消しに失敗した場合は、インシデントが作成され、実装後レビューを実行するように実装グループに通知されます。

実装後レビューの実行

実装グループは、作業が完了すると、変更結果について説明する実装後レビュー（PIR）を実行します。実装グループのメンバーは、通常、変更要求を実装してから 3 ～ 7 日後に PIR を実行します。ただし、変更管理プロセス定義では、このタスクの割り当てに対してデフォルトで 10 秒の遅延が設定されています。

実装後レビューを実行する方法

1. 実装グループのメンバーとして CA SDM にログインし、変更要求を開きます。
[変更要求の詳細] ページが表示されます。
2. [ワークフロー タスク] タブで、[実装後レビュー] リンクをクリックします。
[タスク リスト] が表示されます。
3. [タスク] タブで、[実行] リンクをクリックします。
[PIR] ページが表示されます。
4. [PIR] タブで、解決方法について説明するための質問に回答して [サブミット] をクリックします。
[変更要求の詳細] ページに [ステータス] - [クローズ] が表示されます。

ActivityNode Actor が見つかりませんでした:オブジェクトの更新 - Service Desk r12

症状:

CA Workflow コマンド ウィンドウに以下のエラーが表示されます。

ActivityNode Actor が見つかりませんでした:オブジェクトの更新 - Service Desk r12

解決方法:

1. CA Workflow アプリケーションにログインします。
2. [アクター] タブをクリックします。
3. [プロセス フォルダ] を選択します。

4. [ファイル] - [新規アクター] を選択します。
 5. ドロップダウン リストから [オブジェクトの更新 - Service Desk r12] を選択します。
 6. [OK] をクリックします。
- 新しいアクターが変更管理プロセス定義の一部として使用されます。

変更要求が閉じない

症状:

ワークフローの最後のステップで、変更要求が閉じません。CA Workflow プロセス インスタンスのステータスが[実行中]と表示され、Actor Fault エラーが発生します。

解決方法:

変更要求を閉じるときに、必要なすべてのフィールド（[根本原因] など）が設定されていることを確認してください。

CAB コンソールとレポートの作成

CAB コンソールは、CAB の承認が必要な変更要求のオンライン承認をすばやく実行できるダッシュボードです。変更マネージャおよびその他の CAB メンバーは、コンソールを使用して変更要求の詳細（および関連のワークフロー タスクと構成アイテム）を表示し、変更要求を承認または拒否します。CAB コンソールを使用すると、チーム メンバーは変更要求を確認、承認、または拒否して、次の変更要求の処理をすぐに続行できます。変更要求リクエストの場合、CAB は要求を直接満たすか、適切なグループにリクエストをエスカレートまたは照会して、リクエストを処理できます。

変更マネージャは、CA SDM の概要レポートおよび詳細レポートを作成するための組み込みオプションを使用して、以下の処理を実行できます。

- 承認済みおよび拒否済み変更要求を報告する。
- 承認待ちの変更要求を報告する。

概要と詳細のレポートを印刷または表示するには、レポートに含めるレコードを最初に選択します。リストページの検索機能を使用して、レポートの特定のレコードを選択できます。

たとえば、変更要求リストから検索条件を入力して、CAB による承認待ちの変更要求のリストを作成し、このリストを使用してレポートを生成できます。

注: CA SDM での概要レポートおよび詳細レポートの生成方法については、オンラインヘルプの「レポートの生成」を参照してください。

関連項目:

[CAB グループの管理](#) (P. 966)

[CAB グループの割り当て](#) (P. 968)

[CAB 承認](#) (P. 968)

[CAB コンソールのプロパティの変更](#) (P. 969)

[変更管理のレポート](#) (P. 970)

CAB グループの管理

検討中の変更要求に関係するメンバーで構成される CAB グループを作成および管理できます。CAB グループには、アプリケーション チームのメンバー、開発マネージャ、コンポーネント担当者、QA 担当者、サポート担当者、および必要であるとみなされるその他の関係者を含めることができます。

注: CAB グループを実装する前に、業務構造に適した連絡先を設定する必要があります。

CAB グループを作成するには

1. [管理] タブで [グループ] を選択します。
[グループの検索] ページが表示されます。
2. [新規作成] をクリックします。
[新規グループの作成] ページが表示されます。
3. 必要に応じてフィールドにデータを入力します。
4. [保存] をクリックします。
[グループ リスト] ページに CAB グループが表示されます。

CAB グループにメンバーを割り当てるには

1. [グループの詳細] ページで、[メンバー] タブを選択します。
2. [メンバーの更新] をクリックします。
[連絡先の検索] ページが表示されます。
3. 目的の連絡先を表示するための検索条件を入力し、[検索] をクリックします。
[Members Update] ページが表示され、検索条件に一致する連絡先がリストされます。
4. 左側のリストで、このグループに割り当てる連絡先を選択します。複数のアイテムを選択するには、Ctrl キーを押しながら左マウス ボタンをクリックします。

5. 目的の連絡先をすべて選択したら、選択ボタン (>>) をクリックします。

選択した連絡先が右側の [メンバー] リストに移動します。

6. [OK] をクリックします。

[グループの詳細] ページが表示され、[メンバー] タブに選択した連絡先がリストされます。

CAB グループを変更カテゴリに追加するには

注: 変更要求の CAB フィールドがデフォルトで CAB グループに設定されるよう、Category_Defaults オプションがインストールされていることを確認してください。

1. [管理] タブで、[CA SDM] - [変更要求] - [カテゴリ] を選択します。

[変更カテゴリ リスト] が表示されます。

2. リストからカテゴリを選択します。

[変更カテゴリの更新] ページが表示されます。

3. CAB フィールドから適切な CAB グループを選択します。

4. 必要に応じて他のフィールドにデータを入力します。

5. [保存] をクリックします。

[変更カテゴリの詳細] ページに、保存に成功したことを示すメッセージが表示されます。

6. [ウィンドウを閉じる] をクリックします。

CAB グループは、変更カテゴリおよび変更要求に関連付けられます。

関連項目:

[Area Defaults](#) (P. 578)

[変更要求と案件カテゴリ](#) (P. 481)

CAB グループの割り当て

変更要求を実装する前に確認を行う CAB グループを割り当てることができます。

CAB グループを変更要求に割り当てるには

1. 変更要求リストで目的の変更要求を選択します。
[変更要求の詳細] ページが表示されます。
2. [編集] をクリックします。
3. [詳細] 領域で CAB を選択します。
[グループ リスト] ページが表示されます。
4. CAB グループを選択します。
5. [保存] - [ウィンドウを閉じる] をクリックします。
CAB グループが変更要求に割り当てられます。

CAB 承認

[CAB 承認] フィールドを [はい] に設定した場合、変更諮問委員会 (CAB) は、変更要求を実装する前に、その変更要求を承認する必要があります。承認プロセスの実行中に変更マネージャが [承認] または [拒否] をクリックすると、変更要求ステータスは [承認済み] または [拒否] にそれぞれ変わります。

注: 別のステータス値を使用する場合は、Web スクリーン ペインタを使用して [承認] ボタンまたは [拒否] ボタンのコードを更新します。

関連項目:

[CAB コンソールのプロパティの変更](#) (P. 969)

CAB コンソールのプロパティの変更

Web スクリーン ペインタを使用して、CAB Console の Web フォームに表示される CAB コンソールのプロパティを変更できます。たとえば、以下の操作を実行できます。

- [承認] ボタンおよび [拒否] ボタンの名前を変更する。これらのボタンは、Web フォーム `orderwf_approval_console.html` (CA Workflow タスク) および `order_approval_console.html` (変更要求) のプロパティです。
- 'REJ' 値または 'APR' 値を変更して、[承認] ボタンおよび [拒否] ボタンのステータス値をカスタマイズする。
 - [タスクの拒否] ボタンをクリックすると、関数 `approve_reject( 'REJ' )` が呼び出されます。
 - [タスクの承認] ボタンをクリックすると、関数 `approve_reject( 'APR' )` が呼び出されます。

重要: ボタンに関連付けることができるのは、アクティブな移行のみです。ボタンに関連付けられている事前定義済みステータス移行を非アクティブにしないでください。非アクティブ化すると、事前定義済みステータスが機能しなくなります。

CAB コンソールのプロパティを変更するには

1. Web スクリーン ペインタで、変更する CAB コンソール フォームを開きます。

Web スクリーン ペインタが開き、フォームが表示されます。
2. [デザイン] タブで、変更するコントロールを右クリックし、プロパティを選択します。

[プロパティ -<コントロール>] ページが表示されます。
3. 新しい値をそれぞれ入力してプロパティを変更します。

フィールドの外側をクリックするか、[プロパティ] ページを閉じると、変更がすぐに反映されます。

Web スクリーン ペインタでプロパティを選択すると、プロパティの重要度の概要が、プロパティ フォームの下部に表示されます。

注: Web スクリーン ペインタの詳細については、「実装ガイド」を参照してください。

例: ワークフロー タスクの変更の CAB Console のカスタマイズ

この例では、Web スクリーン ペインタを使用したタスク ステータスのカスタマイズ方法を示します。

1. Web スクリーン ペインタで、Web フォーム `orderwf_approval_console.html` を開きます。
Web スクリーン ペインタが開き、フォームが表示されます。
2. [デザイン] タブで [タスクの拒否] ボタンを右クリックし、[プロパティ] を選択します。
[プロパティ - ボタン] ページが開きます。
3. 関数 `approve_reject( 'REJ' )` を検索します。
'REJ' はタスク ステータス「拒否」のステータス コードです。
4. 'REJ' の新しい値を入力します。
フィールドの外側をクリックするか、[プロパティ] ページを閉じると、変更がすぐに反映されます。
Web スクリーン ペインタでプロパティを選択すると、プロパティの重要度の概要が、プロパティ フォームの下部に表示されます。

変更管理のレポート

適切な権限を持った変更マネージャは、BusinessObjects InfoView を使用して以下の処理を実行できます。

- オペレーティング システム、変更カテゴリ、グループ、実装担当者、リスク、ステータス、実装日、影響される構成アイテム (CI)、およびインシデントまたは問題チケットから発生した変更別に変更ボリュームを報告する。
- 実装が成功した変更を変更カテゴリ、緊急度、優先度、影響、特定成功率、および変更リクエストの依頼者のグループ別にグループ分けして報告する。
- 失敗した変更をカテゴリ、緊急度、優先度、影響、復旧の理由、特定期間内の失敗率、および変更リクエストの依頼者のグループ別にグループ分けして報告する。
- 変更カテゴリ、変更コーディネータ、変更マネージャ、リスク レベル、優先度、および特定期間に影響を受けた構成アイテム別にグループ分けされた変更リクエストの合計数を報告する。

InfoView ウィンドウの左側のペインで事前定義レポートに移動すると、レポートの表示、スケジュール、変更、または実行や、レポートの履歴およびプロパティの表示を行うことができます。

注: BusinessObjects InfoView の使用方法については、オンライン ヘルプの「CA Business Intelligence」を参照してください。

リスク評価

リスク アセスメント機能を使用すると、環境内のシステムまたはサービスを変更する前に、変更カテゴリに属する変更要求のリスクを特定、評価、および定量化できます。リスク調査を作成してリスクを評価し、その調査を変更カテゴリに関連付けます。ユーザは、変更要求を作成して変更カテゴリを指定するときに、そのカテゴリに関連付けられた調査に記入してサブミットすることができます。

リスク調査には、1つ以上の選択形式の質問が含まれています。各回答には、重み付け値が設定されています。変更要求を作成するとき、ユーザは該当する回答を選択し、調査をサブミットします。リスク レベルは、ユーザが選択した回答の重み付け値に基づいて評価されます。

関連項目:

[リスク調査の展開例](#) (P. 973)

[デフォルトのリスク調査の表示](#) (P. 972)

リスク調査の実装方法

リスク調査は以下のように実装します。

1. 組織のリスク レベルを設定します。
2. リスク調査を作成するか、デフォルトのリストから選択します。
3. リスク調査の質問と回答を作成または変更します。
4. リスク調査のリスク範囲を変更します。
5. リスク調査を変更カテゴリに関連付けます。
6. リスク調査を変更カテゴリに関連付けると、リクエストの依頼者が指定された変更カテゴリを使用して変更要求を保存するときに [リスク調査] ボタンが表示されます。
7. リスク調査の結果に基づいた評価済みリスクを表示します。
8. (オプション) [アクティビティ] メニューで評価済みリスク値を上書きします。

注: リスク調査の作成および変更の詳細については、オンライン ヘルプを参照してください。

デフォルトのリスク調査の表示

CA SDM では、変更カテゴリに関連付けることができるデフォルトのリスク調査が設定されています。

デフォルトのリスク調査を表示するには

1. [Service Desk] - [変更要求] - [リスク調査] に移動します。
2. [リスク調査名] 列から [一般] を選択します。
[General Risk Survey Detail] ページが表示されます。

3. [調査の表示] をクリックします。

リスク調査の質問、回答、および各回答の重み付け値が表示されます。
この調査は、組織内の一般的な変更に適用されます。

4. 調査を閉じます。
5. 表示される [General Risk Survey Detail] ページを閉じます。

リスク調査の展開例

この例は、デフォルトの変更カテゴリを使用して、システムのデフォルトのリスク調査を展開する方法を示しています。

1. [Service Desk] - [変更要求] - [カテゴリ] に移動します。
[変更カテゴリ リスト] が表示されます。
2. [シンボル] 列から [追加.IT.その他] を選択します。
追加.IT.その他の [カテゴリの詳細] ページが表示されます。
3. [編集] をクリックします。
追加.IT.その他の [変更カテゴリの更新] ページが表示されます。
4. [リスク調査] をクリックします。
[リスク調査テンプレートの検索] が表示されます。
5. リスク調査を検索します。この例では、[一般] のリスク調査を検索して選択し、詳細フォームに追加します。
[リスク調査] フィールドには一般のリスク調査が表示されます。
6. 保存してウィンドウを閉じます。

[追加.IT.その他] カテゴリを使用して変更要求を作成すると、変更要求を保存するときに [リスク調査] ボタンが表示されます。

URL からリスク調査に直接アクセスする方法

動的 URL を提供することによって、ユーザは CA Workflow のタスクの内部から URL を介して変更要求のリスク調査に直接アクセスすることができます。 *KEEP.UsingURL=1* パラメータにこの動的 URL を追加することによって、リスク調査が URL で直接アクセスされていることを示すことができます。

CA Workflow に動的な URL を以下のようにして作成します。

1. CA Workflow プロセス定義を開いてユーザにリスク調査を完了するためのアクティビティ ノードを追加します。
2. アクティビティ ノード内で、適切な構文を使用して動的 URL を追加します。以下の例のように *KEEP.UsingURL=1* パラメータを追加して検証します。

```
http://<ホスト名>:<ポート>/CAisd/pdmweb.exe?CNT_ID=<連絡先の ID>+CRID=<変更要求の ID>+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

ホスト名

アプリケーション サーバのホスト名を指定するか、一連のアプリケーション サーバにリダイレクトできるロードバランサの URL を指定します。

ポート

CA SDM がインストールされているポートを指定します。

連絡先の ID

リスク調査を完了する連絡先の内部 ID を指定します。

変更要求の ID

リスク調査に関連付けられた変更要求の内部 ID を指定します。

以下の例はサンプル URL を表示します。

```
http://hostname:8080/CAisd/pdmweb.exe?CNT_ID=21A7CC606A3011DEA39AA8010000A800+CRID=400009+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

重要: 動的 URL に *KEEP.UsingURL=1* パラメータを追加しない場合、ユーザがリスク調査をサブミットした後にエラーが表示され、リスクレベルは計算されません。

3. CA Workflow プロセス定義を保存します。
4. 変更カテゴリを作成し、リスク調査および CA Workflow プロセス定義を変更カテゴリに関連付けます。

変更の保存

5. この変更カテゴリで変更要求を開いて保存し、CA Workflow プロセスのインスタンスを作成します。
6. CA Workflow プロセスの一部として、ユーザはタスクに割り当てられてリスク調査を完了します。事前に説明されたように、ユーザは URL をクリックします。
7. ユーザは URL を使用して、CA SDM にログインし、変更要求のリスク調査のコンテキストに直接移動します。
8. ユーザは、表示が成功か失敗かを示す調査とメッセージをサブミットします。

正常にサブミットされた場合、リスク レベルは変更要求で計算されて更新されます。

影響度エクスプローラ

影響度エクスプローラは、組織内における変更を管理および制御するための高度なツールです。影響度エクスプローラを使用すると、変更マネージャは変更要求に添付された構成アイテムを調査したり、添付された構成アイテムまたはその子構成アイテムを直接操作したりすることができます。

影響度エクスプローラには、以下の利点があります。

- 変更要求に添付されたすべての構成アイテムを表示する
- 添付された構成アイテムのすべての子およびピアツーピア関係を表示する
- 関連する構成アイテムを変更要求に添付できる
- 添付された構成アイテムについて逐次的に関連する構成アイテムの子孫リストを表示する
- 構成アイテムの CMDB Visualizer を起動できる

関連項目:

[影響度エクスプローラの起動 \(P. 976\)](#)
[添付された構成アイテムの調査 \(P. 976\)](#)
[影響度エクスプローラでの構成アイテムの表示 \(P. 977\)](#)
[変更要求への関連する構成アイテムの追加 \(P. 978\)](#)
[構成アイテム子孫リストの表示 \(P. 978\)](#)
[影響度エクスプローラからの CMDB Visualizer の起動 \(P. 979\)](#)
[影響度エクスプローラの設定 \(P. 979\)](#)

影響度エクスプローラの起動

影響度エクスプローラは、変更要求の [構成 アイテム] タブからアクセスできます。

影響度エクスプローラを起動するには

1. [変更要求の詳細] ページを開きます。
2. [構成 アイテム] タブを選択します。
3. [影響度エクスプローラ] をクリックします。
[影響度エクスプローラ] ページが表示されます。

注: [変更要求の詳細] ページを閉じると、[影響度エクスプローラ] ページも閉じます。

注: 複数の変更要求から影響度エクスプローラを起動すると、複数の [影響度エクスプローラ] ページが表示されます。

添付された構成アイテムの調査

影響度エクスプローラ ツリーには、変更要求に添付された各構成アイテムのノードが含まれています。プラス (+) 記号は、構成アイテムに 1 つ以上の子構成アイテムがあることを示します。

注: 100 件を超える構成アイテムが変更要求に添付されていても、表示されるのは最初の 100 件のみです。

添付された構成アイテムの関係を表示するには、構成アイテムのプラス (+) 記号をクリックします。関連する構成アイテムがツリーに表示されます。関連する構成アイテムの名前のほかに、ツリーには関係タイプが角かっこで囲まれて表示されます。

注: 変更要求に 100 件を超える添付された構成アイテムが存在する場合、最初の 100 件のみ表示されます。次の 100 件を表示するには、[詳細...] をクリックします。

影響度エクスプローラでの構成アイテムの表示

影響度エクスプローラ ツリーには、変更要求にリンクされた各構成アイテムのノードが表示されます。プラス (+) 記号は、構成アイテムに 1 つ以上の子構成アイテムがあることを示します。

構成アイテムを表示するには

1. 左側のペインで構成アイテムのノードをクリックします。

右側のペインに [構成アイテムの詳細] ページが表示されます。

注: 構成アイテムを右クリックし、コンテキストメニューで [表示] を選択して、[構成アイテムの詳細] ページを右側のペインに表示することもできます。

2. 左側のペインの上部にある [変更要求] ノードをクリックします。

[変更要求の詳細] ページが表示されます。

注: 変更要求に 100 件を超える添付された構成アイテムが存在する場合、最初の 100 件のみ表示されます。次の 100 件を表示するには、[詳細...] をクリックします。

変更要求への関連する構成アイテムの追加

構成アイテム関係を調査しながら、関連する構成アイテムを変更要求に添付できます。

関連する構成アイテムを変更要求に追加するには

1. 変更要求の「構成 アイテム」タブをクリックします。
「構成アイテム リスト」ページが表示されます。
2. 「影響度エクスプローラ」をクリックします。
影響度エクスプローラ ツリーに、添付された構成アイテムが表示されます。
3. 添付された構成アイテムノードのプラス記号 (+) をクリックします。
ノードに関連する構成アイテムが表示されます。
4. 関連する構成アイテムを右クリックして、コンテキスト メニューから「変更要求に追加」を選択します。
添付された新しい構成アイテムが変更要求の「構成 アイテム」タブに表示されます。

構成アイテム子孫リストの表示

どの構成アイテムの場合も、関連する構成アイテム（子孫と呼ばれる）の行を表示できます。各構成アイテムの基本情報のほかに、構成アイテム子孫リストには派生元の構成アイテムをレベル 1 とした関係レベルが表示されます。構成アイテムの子要素はレベル 2 で始まり、その子要素はレベル 3 というように続きます。追跡した関係の中で構成アイテムが 2 回以上出現した場合、その構成アイテムに最も近い関係レベルのみ表示されます。

例: 1つの構成アイテムに対応する複数の子孫パス

複数の関係が存在するため、子孫検索によってレベル 2 とレベル 4 に同じ関連する構成アイテムが見つかります。子孫構成アイテムは、レベル 2 にのみ表示されます。

構成アイテムの子孫を一覧表示するには

1. [変更要求の詳細] ページで、[構成 アイテム] タブを選択します。
2. [影響度エクスプローラ] をクリックして、添付された構成アイテムを表示します。
3. 必要に応じて構成アイテムのノードを展開します。
4. 構成アイテムを右クリックして、[リスト派生] を選択します。
構成アイテムの子孫リストが表示されます。

影響度エクスプローラからの CMDB Visualizer の起動

影響度エクスプローラには、添付された構成アイテムまたは関連する構成アイテムから CMDB Visualizer を起動できる機能があります。

影響度エクスプローラから CMDB Visualizer を起動する方法

1. [変更要求の詳細] ページで、[影響度エクスプローラ] をクリックします。
[影響度エクスプローラ] ページが表示されます。
2. 構成アイテムを右クリックし、コンテキストメニューから [Launch Visualizer] を選択します。
構成アイテムをフォーカスとして、CMDB Visualizer を起動します。

影響度エクスプローラの設定

管理者は、以下のように影響度エクスプローラを設定できます。

- 添付された構成アイテムに対して表示する子構成アイテムの数を指定する
- 構成アイテム子孫リストに表示する関係レベルの数を指定する
- 子構成アイテムを非表示にする

表示する子構成アイテムの数は、
`NX_IMPACT_EXPLORER_MAX_CHILD_NODES` 設定を `NX.env` 構成ファイルに追加することで設定できます。初期設定は **100** です。

例: 子構成アイテムの表示件数の設定

以下の設定を使用して、影響度エクスプローラには、添付された構成アイテムの子構成アイテムが一度に **10** 件のみ表示されます。

```
@NX_IMPACT_EXPLORER_MAX_CHILD_NODES=10
```

構成アイテム子孫リストのデフォルトの深さは **9** レベルです。深さは、
`NX_IMPACT_EXPLORER_MAX_LEVELS` 設定を `NX.env` 構成ファイルに追加することで設定できます。

例: 子孫レベルの数の設定

以下の設定を使用して、構成アイテム子孫リストには派生元の構成アイテムとこれに隣接する子構成アイテムのみが表示されます。

```
@NX_IMPACT_EXPLORER_MAX_LEVELS=2
```

以下のオプション マネージャのオプションを使用して、特定タイプの子構成アイテムを非表示にします。

```
IMPACT_EXPLORER_EXCLUDE_HIER=boolean
```

`IMPACT_EXPLORER_EXCLUDE_HIER` オプションがインストールされていて、「Yes」に設定されている場合、[構成アイテムの詳細] ページの [CMDDB 関係] タブで関連付けられた子構成アイテムは、影響度エクスプローラ ツリまたは構成アイテム派生リストには表示されません。

注: CA CMDDB を使用して関連付けられた子構成アイテムは表示されます。

第 19 章: レポートの管理

このセクションには、以下のトピックが含まれています。

[CA Business Intelligence レポート](#) (P. 983)

[レポート シナリオ](#) (P. 984)

[レポート コンポーネント](#) (P. 984)

[レポート データ フロー図](#) (P. 988)

[InfoView での Web ベースのレポートの表示](#) (P. 989)

[セキュリティと認証](#) (P. 990)

[既存の CA Business Intelligence サーバが CA SDM サーバを指す方法](#) (P. 997)

[レポートへのデータ パーティション セキュリティのセットアップ方法](#) (P. 999)

[オフライン レポート用の複製されたデータベース](#) (P. 1002)

[ロールベースのレポート](#) (P. 1002)

[Web ベースのレポート](#) (P. 1013)

[重要業績評価指標 \(KPI\)](#) (P. 1016)

[一時的なレポート](#) (P. 1030)

[一時的なレポートの例](#) (P. 1032)

[ダッシュボード レポート](#) (P. 1038)

[CA Business Intelligence レポートの作成](#) (P. 1039)

第 20 章: CA Business Intelligence レポート

CA Business Intelligence は Web ベースのコンポーネントで、CA SDM およびさまざまな一般的データ ソース (SQL Server、Oracle、オープン データベース接続 (ODBC) など) と統合された Business Objects テクノロジがパッケージされています。

CA Business Intelligence は、デフォルトのレポート システムとして BusinessObjects Enterprise を使用します。CA SDM、ナレッジ マネジメント および サポート オートメーション には、事前定義済みレポートが用意されています。

CA Business Intelligence のレポート機能を使用すると、以下のことを実行できます。

- 既存のレポートをカスタマイズする
- Business Objects レポート データをドリルダウンして、グラフおよび集計したグループにデータを表示する
- レポートのインスタンスを異なる出力フォーマットにエクスポートする
- 一時的なレポートを作成する
- 新しいレポートを発行し、承認されたユーザに配布する
- レポートが指定時間に実行されるようにスケジュールする
- すべての CA SDM チケット タイプの日常作業をモニタするダッシュボード レポートの使用

注: レポートへのアクセスは、CA SDM データ パーティション セキュリティによって制限されています。

レポートシナリオ

BusinessObjects Enterprise と統合されている CA Business Intelligence では、以下のレポートシナリオがサポートされています。

- **役割ベースのレポートの作成**：承認されたユーザは、CA SDM の [レポート] タブで各自の役割に定義されたレポートを表示し、[InfoView] ボタンをクリックして、BusinessObjects InfoView で個人のレポートを管理できます。CA SDM では、InfoView インターフェースを使用して、情報をレポート形式で収集、整理、および提供します。InfoView では、事前定義のレポートがパブリック フォルダにグループ化されます。
- **Web ベースのレポートの作成**：Web ベースのレポートは、CA SDM、ナレッジマネジメント、CMDB、およびサポート オートメーションの事前定義レポートです。これは、Web Intelligence または Crystal Reports を使用して作成されます。このレポートには InfoView からアクセスし、サイト固有のレポートを定義するためのモデルとして使用できます。
- **一時的なレポートの作成**：一時的なレポートは、Web Intelligence プラグインベースのインターフェースを使用して、InfoView から作成および管理されます。レポートは、個人の作業領域（マイ フォルダ）に格納して管理できます。一時的なレポートの作成機能は、クエリを記述せずに簡単に基本レポートを作成することを望むユーザ向けです。
- **ダッシュボードレポートの作成**：ダッシュボードレポートを作成すると、CA SDM のすべてのチケットタイプ（リクエスト/インシデント/問題、変更要求または案件）に対する日常作業を InfoView で監視できるようになります。各レポートには、アクティブなチケットに従事する上位アナリストに関する分析が含まれているため、各アナリストの進捗状況を監視できます。事前定義済みの個別のダッシュボードレポートや、単一のビュー内ですべての CA SDM 日常作業を表示する企業ダッシュボードを使用できます。

レポートコンポーネント

BusinessObjects Enterprise およびその関連ツールと BusinessObjects Crystal Reports XI の組み合わせは、CA BI アーキテクチャのバックボーンになります。

Crystal レポートは CA Business Intelligence の主要コンポーネントとして提供されますが、レポートの作成および保守ツールである Crystal Reports XI は CA Business Intelligence の一部として提供されません。Crystal Reports XI は個別にライセンスされる製品であり、BusinessObjects Enterprise から購入して CA Business Intelligence と共に使用できます。

注: Microsoft Access の事前定義レポートは開発が終了し、CA SDM と共に提供されなくなりました。

CA Business Intelligence レポート環境を管理、監視、および設定するには、以下のコンポーネントを使用します。

- **CA SDM データベース/Domsrvr/ODBC ドライバ** : レポートデータは SQL Server または Oracle CA SDM データベースに保存されます。BusinessObjects レポート アプリケーション (Crystal Reports および Web Intelligence) は、CA SDM オブジェクト エンジン (domsrvr) と直接接続されている ODBC ドライバを使用して、データベースにアクセスします。データ パーティションやテナンシーの制限を含む CA SDM のすべてのセキュリティは、レポートに自動的に適用されますが、ユーザのレポート環境には適用されません。CA SDM の既存のデータ パーティションで機能するようにレポート環境をセットアップできます。

注: レポート環境用のデータ パーティションセキュリティを設定する方法については、「[レポート用のデータ パーティションセキュリティのセットアップ方法](#) (P. 990)」を参照してください。

- **Central Management Server (CMS)** : 各レポート プロセスで使用されるすべてのオブジェクトを格納する中央リポジトリです。
- **Central Management Console (CMC)** : すべての BusinessObjects 管理機能へのアクセスを提供する管理コンポーネントです。CMC を使用して、レポートの展開や、InfoView のアクセス権とフォルダ権限のユーザへの割り当てを実行できます。CMC を使用するレポート環境用に、ユーザの権限、役割、および認証オプションを設定する必要があります。

注: CA Business Intelligence を使用する前に、レポート環境用のユーザの権限、役割、および認証オプションを設定する必要があります。セキュリティの定義の詳細については、「[セキュリティと認証](#)」 (P. 990) を参照してください。

- **BusinessObjects ユニバース** : レポートに使用するクラス (テーブル) およびオブジェクト (列) を記述します。CA SDM ユニバースは、インストール中にインストールと設定が実行されます。インストールが完了すると、ユニバース接続が CA SDM のさまざまなグループおよびユーザに割り当てられます。
- **Designer** : BusinessObjects のコンポーネントの 1 つで、CA SDM スキーマと Business Objects レポート ツール間のメタレイヤである CA SDM ユニバースを変更できます。また、インポート/エクスポート ウィザードによって、CMS 内でのオブジェクトへの入力や抽出が簡略化されます。
- **デフォルトの事前定義レポート** : 事前定義レポートは Web ベースの CA SDM レポートおよびナレッジマネジメント レポートであり、Web Intelligence または Crystal Reports を使用して作成されます。レポートは、サイト固有のレポートを定義するためのモデルとして使用できます。
- **InfoView** : BusinessObjects InfoView は Web インターフェースです。承認された CA SDM ユーザは、これを使用して Web Intelligence、Crystal Reports、またはその他のレポート タイプの表示、実行、およびスケジュールを行うことにより、Web ベースの事前定義レポートを操作できます。レポートは、InfoView 内のパブリック セクションにあるフォルダに保存されます。
- **一時的なレポート** : 一時的なレポートでは、Web Intelligence プラグインベースのインターフェースを使用してレポートを作成および管理できます。このツールは、クエリを記述せずに簡単に基本レポートを作成することを望むユーザ向けです。

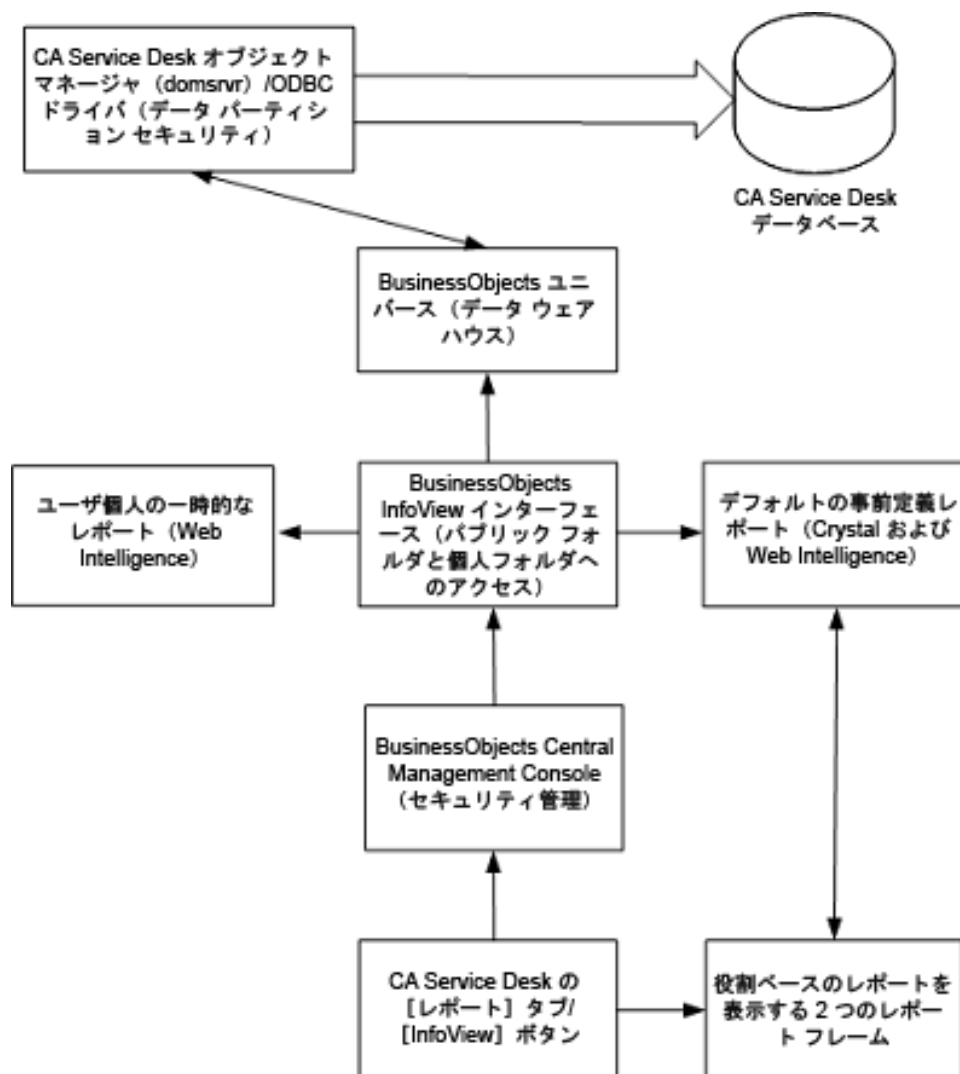
注: 一時的なレポートの使用例については、「[一時的なレポート](#) (P. 1030)」を参照してください。
- **ダッシュボード レポート** : ダッシュボード レポートを使用すると、CA SDM のすべてのチケット タイプ (リクエスト/インシデント/問題、変更要求または案件) に対する日常作業を BusinessObjects InfoView で監視できるようになります。各レポートには、アクティブなチケットに従事する上位アナリストに関する分析が含まれているため、各アナリストの進捗状況を監視できます。

- **CA SDM の [レポート] タブ**: 承認されたユーザは、CA SDM の [レポート] タブに各自の役割ベースのレポートを表示し、このタブの [InfoView] ボタンをクリックして **InfoView** で個人のレポートを管理できます。

注: 役割ベースのレポートを管理し、新しいレポートを [レポート] タブに表示する方法については、「[Web ベースのレポート \(P. 1013\)](#)」を参照してください。

レポート データ フロー図

以下の図は、BusinessObjects Enterprise と統合されている CA Business Intelligence のコンポーネント データ フローと実行を示したものです。



InfoView での Web ベースのレポートの表示

CA SDM では、BusinessObjects InfoView インターフェースを使用して、情報をレポート形式で収集、整理、および提供します。

重要: すべてのレポートでは、レポートを生成するために [日付] フィールドを更新する必要があります。その他のフィールドはオプションです。

次の手順に従ってください:

1. CA SDM の [レポート] タブで、[InfoView] ボタンをクリックします。
[InfoView] ホーム ページが表示されます。
2. [ヘッダ] パネルから、[ドキュメントリスト] を選択します。
[ドキュメントリスト] のパブリック フォルダには、CA SDM レポート、管理ツール、サンプルなどが表示されます。フォルダを選択すると、その内容が詳細パネルに表示されます。[ドキュメントリスト] でアクセスできるフォルダは、管理者から付与された権限によって異なります。
たとえば、CMDB のレポートを表示するには、CA Service Desk/CMDB に移動します。レポートのリストが詳細パネルに表示されます。
3. レポートをダブルクリックします。
レポート フォームが表示されます。このフォームには、選択したレポートを生成するための入力フィールドが含まれています。
4. 選択したレポートを生成するには、関連する情報を入力します。

例: 時間範囲レポートで追加された CI を開く場合は、追加された CI、CI テナント名などを表示する時間範囲を入力する必要があります。

重要: Oracle データベースを使用しているときに、すべての変更影響レポート、CI 関係レポート、および根本原因分析レポートを生成する場合は、CMDB フォルダから [Oracle (These Reports will work on Oracle Only)] をクリックしてレポートにアクセスします。これらのレポートを SQL Server フォルダから生成すると、レポートは生成されず、エラーメッセージが表示されます。同様に、SQL データベースを使用しているときに、すべての変更影響レポート、CI 関係レポート、および根本原因分析レポートを生成する場合は、CMDB フォルダから [SQL Server (These Reports will work on SQL Server Only)] をクリックしてレポートにアクセスします。

注: レポートを生成するには、すべてのフィールドに入力する必要があります。

5. [OK] をクリックします。
レポートが表示されます。

注: BusinessObjects InfoView には、BusinessObjects InfoView の使用方法を説明したユーザ ガイドが含まれています。ユーザ ガイドにアクセスするには、InfoView 内のヘルプ アイコンをクリックします。

セキュリティと認証

BusinessObjects Enterprise のデフォルトのセキュリティ設定は、CA Business Intelligence の環境設定を使用して行います。この構成により、フォルダ、ユニバース、ユニバース接続とツールのセキュリティ ポリシーが決まります。ユーザの追加方法、グループへのユーザのマッピング方法、および一部の環境設定オプションの設定方法も提供されます。

CA Business Intelligence レポートの設定では、具体的には以下の作業を行います。

- セキュリティのセットアップ
- レポートの展開
- ユニバースの展開
- Web Intelligence 設定の構成

インストールが完了すると、ユニバース接続が CA SDM 内の個々のグループおよびユーザに割り当てられます。

管理者は、BusinessObjects CMC にログオンしていつでもデフォルト設定を変更できます。ユーザには、各自が属する CA Business Intelligence グループに基づいて InfoView フォルダへのアクセスが承認されます。

グループとユーザ

以下の表に示すグループが、CA Business Intelligence の構成時に Central Management Server (CMS) に追加されます。これらのグループは、同じ名前を持つ CA SDM 役割に関連しています。構成フェーズ時に、サンプルユーザを CMS に追加するかどうかを指定するオプションのチェックボックスが使用可能となっていました。このチェックボックスをオンにした場合、デフォルトの CMS 構成では、各グループに 1 人のサンプルユーザが含まれています。CMC では、ユーザ権限や認証オプションをレポート環境に設定する場合のモデルとしてこれらのサンプルユーザを使用できます。

グループ名	ユーザ名
変更マネージャ	変更マネージャ ユーザ
顧客サービス マネージャ	顧客サービス マネージャ ユーザ
ナレッジ マネージャ	ナレッジ マネージャ ユーザ
ナレッジアナリスト	ナレッジアナリスト ユーザ
サービス デスク マネージャ	サービス デスク マネージャ ユーザ
インシデント マネージャ	インシデント マネージャ ユーザ
問題マネージャ	問題マネージャ ユーザ

Infoview 内の CA SDM データ パーティション

CA SDM データ パーティションと InfoView の関係に関する以下の情報を考慮してください。

- アナリストは、デフォルトのレポーティング役割のアクセス タイプを使用して、CA SDM または InfoView の [レポート] タブから CA Business Intelligence に接続します。
- CA SDM のログイン認証情報は、InfoView の認証情報に一致している必要があります。管理者は、secLDAP や secEnterprise などの認証方法を設定します。CA SDM が CA Business Intelligence にログインすると、次に CA Business Intelligence が ODBC 経由で CA SDM にログインします。
- CA Business Intelligence のアナリスト ログインが CA SDM ログインに関連付けられます。CA Business Intelligence は、この CA SDM ログインと、そのログインのアクセス タイプに関連付けられたレポーティング役割を使用します。アナリストに CA SDM ログインが関連付けられていない場合、CA Business Intelligence はシステムのデフォルト値を使用します。システムのデフォルト値は、Universe Designer の ODBC パラメータ、およびアクセス タイプのレポーティング役割で定義されています。
- ユーザにレポートが表示されないようにするために、管理者は、レポートまたはそのレポートを含むフォルダへのアクセスを無効にすることができます。

ユニバースとユニバース接続

デフォルトの構成には、CA SDM ユニバースとユニバース接続にアクセスするためのセキュリティ ポリシーも含まれています。フルアクセスを許可するために、すべてのデフォルト グループがフル コントロール アクセス権を持つように定義されています。

グループ名	アクセス レベル
変更マネージャ	フル コントロール
顧客サービス マネージャ	フル コントロール
ナレッジアナリスト	フル コントロール
ナレッジ マネージャ	フル コントロール
Service Desk マネージャ	フル コントロール

グループ名	アクセスレベル
インシデント マネージャ	フル コントロール
問題 マネージャ	フル コントロール

レポート フォルダ

デフォルトの構成には、CA SDM と ナレッジ マネジメント 用の定義済みレポートが格納されているフォルダ セットも含まれています。各 CA SDM グループは、これらのフォルダのサブセットへのアクセス権を持つように構成されています。

フォルダ名	グループ名	アクセスレベル
集計	■ 変更 マネージャ	■ 表示
	■ 顧客サービス マネージャ	■ 表示
	■ ナレッジ マネージャ	■ アクセスなし
	■ ナレッジ アナリスト	■ アクセスなし
	■ Service Desk マネージャ	■ フル コントロール
	■ インシデント マネージャ	■ 表示
	■ 問題 マネージャ	■ 表示
アセット	■ 変更 マネージャ	■ オンデマンド表示
	■ 顧客サービス マネージャ	■ 表示
	■ ナレッジ マネージャ	■ アクセスなし
	■ ナレッジ アナリスト	■ アクセスなし
	■ Service Desk マネージャ	■ フル コントロール
	■ インシデント マネージャ	■ 表示
	■ 問題 マネージャ	■ 表示

フォルダ名	グループ名	アクセスレベル
変更要求 (すべてのサブフォルダを含む)	■ 変更マネージャ ■ 顧客サービス マネージャ ■ ナレッジ マネージャ ■ ナレッジアナリスト ■ Service Desk マネージャ ■ インシデント マネージャ ■ 問題マネージャ	■ フル コントロール ■ アクセスなし ■ アクセスなし ■ アクセスなし ■ 表示 ■ 表示 ■ 表示
案件 (すべてのサブフォルダを含む)	■ 変更マネージャ ■ 顧客サービス マネージャ ■ ナレッジ マネージャ ■ ナレッジアナリスト ■ Service Desk マネージャ ■ インシデント マネージャ ■ 問題マネージャ	■ アクセスなし ■ フル コントロール ■ アクセスなし ■ アクセスなし ■ アクセスなし ■ アクセスなし ■ アクセスなし
リクエスト (すべてのサブフォルダを含む)	■ 変更マネージャ ■ 顧客サービス マネージャ ■ ナレッジ マネージャ ■ ナレッジアナリスト ■ Service Desk マネージャ ■ インシデント マネージャ ■ 問題マネージャ	■ アクセスなし ■ アクセスなし ■ アクセスなし ■ アクセスなし ■ フル コントロール ■ 表示 ■ アクセスなし
ナレッジ マネジメント	■ 変更マネージャ ■ 顧客サービス マネージャ ■ ナレッジ マネージャ ■ ナレッジアナリスト ■ Service Desk マネージャ ■ インシデント マネージャ ■ 問題マネージャ	■ アクセスなし ■ 表示 ■ フル コントロール ■ 表示 ■ スケジュール ■ 表示 ■ 表示

フォルダ名	グループ名	アクセスレベル
調査	■ 変更マネージャ	■ アクセスなし
	■ 顧客サービス マネージャ	■ アクセスなし
	■ ナレッジ マネージャ	■ 表示
	■ ナレッジアナリスト	■ アクセスなし
	■ Service Desk マネージャ	■ フル コントロール
	■ インシデント マネージャ	■ 表示
	■ 問題マネージャ	■ 表示
インシデント管理 および問題管理	■ 変更マネージャ	■ アクセスなし
	■ 顧客サービス マネージャ	■ アクセスなし
	■ ナレッジ マネージャ	■ 表示
	■ ナレッジアナリスト	■ アクセスなし
	■ Service Desk マネージャ	■ スケジュール
	■ インシデント マネージャ	■ フル コントロール
	■ 問題マネージャ	■ フル コントロール

アクセスレベル

デフォルトの構成では、グループとユーザ用の以下のアクセス レベルが含まれています。

アクセスなし

すべてのアクセス許可を「指定されていません」に設定します。

表示

フォルダ、レポート、およびユニバースの表示をユーザに許可します。レポートにデータが含まれている場合、ユーザはデータを開いて操作できます。レポートにデータが含まれていない場合、ユーザはそのレポートをリフレッシュできません。デフォルトでは、ユーザはレポートを編集し、個人フォルダに保存してそこでリフレッシュできます。「別のフォルダへのオブジェクトのコピー」を拒否する権限を個別に設定することで、個人フォルダへの社内ドキュメントのコピーを明示的に防ぐことができます。

スケジュール

レポートのスケジュール設定をユーザーに許可しますが、リアルタイムでのリフレッシュは許可しません。

オンデマンド表示

リアルタイムでのレポートのリフレッシュをユーザーに許可します。レポートが **Web Intelligence** ドキュメントである場合、リフレッシュを実行するには、ユニバースとユニバース接続への [オンデマンド表示] アクセスも必要となります。

フルコントロール

フォルダ内での新規レポートの作成、既存のレポートの変更、およびアイテムの削除をユーザーに許可します。

詳細設定

先行するアクセス レベルがニーズに合わない場合、[詳細] を選択すると、さらに細かいレベルのアクセスが提供されます。

ユーザーまたはグループのアクセス レベルが [詳細] に設定されていると、[ビュー]、[スケジュール]、[オンデマンド表示]、または [フルコントロール] の選択によって割り当てられる権限よりもさらに細かい権限の制御が可能になります。

BusinessObjects フォルダでは、継承されたセキュリティが使用されます。上書き制限が低いレベルに適用されている場合を除き、上位フォルダレベルで自分および自分のグループに割り当てられているのと同じ権限が、低いレベルのフォルダに付与されます。デフォルトの権限は、フォルダレベルおよびグループ レベルで提供されます。ユーザーは、フォルダおよび下位フォルダ内のすべてのオブジェクトに関して自分のグループの権限を継承します。

CA Business Intelligence は、管理者および全員という 2 つのグループと共にインストールされます。全員グループにはスケジュールのアクセス レベルが割り当てられているため、すべてのレポート オブジェクトのスケジュールおよび表示を実行できます。

関連項目:

[レポート フォルダ](#) (P. 993)

既存の CA Business Intelligence サーバが CA SDM サーバを指す方法

CA Business Intelligence サーバがすでにある場合は、以下のようにして CA SDM サーバを指定できます。

1. [新規 ODBC データ ソースを作成](#) (P. 997) します。
2. [ユニバースを構成](#) (P. 998) します。
3. [ユニバースをエクスポート](#) (P. 999) します。
4. InfoView を起動して、接続を確認します。

ODBC データ ソースを作成する

CA Business Intelligence サーバ上の ODBC データ ソースは、ODBC データ ソース アドミニストレータを使用して作成できます。

ODBC データソースを作成するには、以下の手順に従います。

1. [スタート] - [すべてのプログラム] - [管理ツール] - [データ ソース (ODBC)] に移動します。
ODBC データ ソース アドミニストレータが表示されます。
2. [システム DSN] タブを選択し、[追加] をクリックします。
[データ ソースの新規作成] ページが表示されます。
3. [DataDirect OpenAccess] を選択し、[完了] をクリックします。
[DataDirect OpenAccess ODBC Setup] ページが表示されます。
4. ODBC 名フィールドで `casd_servername` を指定します。
5. [詳細設定] をクリックします。
詳細設定ページが表示されます。
6. [追加] をクリックします。
[Open Access Database Setup] ページが表示されます。
7. 以下のフィールドを指定します。
 - [名前] 。 `casd_servername` を指定します。
 - [IP アドレス] 。 `servername` または IP アドレスを指定します。

注: *servername* に Ping を実行して IP アドレスを特定し、その IP アドレスを *servername* の代わりに使用できます。

- [ポート]。1706 を指定します。
 - [タイプ]。(オプション)サーバで使用するデータベースを指定します。このフィールドは、参照情報としてのみ使用されます。
8. [OK] をクリックします。
 9. [データベース] ドロップダウンリストから *casd_servername* を選択します。
 10. [OK] をクリックします。
- ODBC データ ソースが作成されます。

ユニバースの設定

ODBC データ ソースを作成したら、CA SDM と CA Business Intelligence 間の接続を確立することによって、ユニバースを設定する必要があります。

ユニバースを設定する方法

1. Designer を起動し、管理者としてログインします。
2. [File] - [Import] をクリックします。
[Import Universe] ページが表示されます。
3. CA SDM ユニバースを参照して選択し、[OK] をクリックします。
ユニバースが正常にインポートされたことを示すメッセージが表示されます。
4. [File] - [Parameters] をクリックします。
[Universe Parameters] ページが表示されます。
5. [Edit] をクリックします。
[Edit CA SDM connection] ページが表示されます。
6. CA SDM の特権ユーザ (ServiceDesk など) のユーザ名とパスワードを指定します。
7. データ ソース名から *casd_servername* を選択し、[Next] をクリックします。

8. [Test Connection] をクリックして、CA SDM ユニバースが CA Business Intelligence と通信していることを確認します。
9. [Next] 、 [Next] 、 [Finish] の順にクリックします。
ユニバースが設定されます。

ユニバースのエクスポート

ユニバースを設定したら、Designer からユニバースをエクスポートする必要があります。

ユニバースをエクスポートする方法

1. [File] - [Export] をクリックします。
[Export Universe] ダイアログ ボックスが表示されます。
2. [Continue] をクリックします。
3. [OK] をクリックします。
ユニバースがエクスポートされます。

レポートへのデータ パーティション セキュリティのセットアップ方法

CA Business Intelligence レポートへのアクセスは、CA SDM のデータ パーティション セキュリティによって制限されます。データ パーティション およびテナンシー制限を含むすべての CA SDM セキュリティが自動的にレポートに適用されます。

自分のレポート環境のデータ パーティション セキュリティは、構成フェーズ時には適用されません。CA SDM の既存のデータ パーティション で機能するようにレポート環境をセットアップします。

このタスクを実行するには、以下のツールを使用します。

- **BusinessObjects の Central Management Console (CMC)** : BusinessObjects Enterprise ユーザの認証と権限を管理できます。
- **BusinessObjects Designer** : CA SDM スキーマとレポート ツール間のメタレイヤである CA SDM、ナレッジマネジメント、CMDDB、およびサポート オートメーション 用のユニバースを変更できます。
- **CA SDM Security and Role Management** - ユーザがアクセスできるデータを指定するためにデータ パーティションセキュリティをセットアップできます。

CMC への CA SDM 特権ユーザの追加

ユニバース接続は、データへのアクセス時に **Service Desk** の特権ユーザおよびパスワードを使用するようにデフォルトで構成されています。このユーザを新しい **CA Business Intelligence** ユーザとして **CMC** に追加する必要があります。このユーザの追加には、2 つの目的があります。まず、レポートにデータパーティションセキュリティをセットアップする場合にこのユーザが必要になること、次に、**CA SDM** の [レポート] タブからレポートを最初にテストするときにこのユーザを使用できることです。[レポート] タブでは、**CA SDM** および **CA Business Intelligence** の両方に定義されているユーザが必要となります。

「実装ガイド」での説明に従って、**CA SDM** ユーザを **CMC** に追加し、**CA SDM** 特権ユーザ アカウントを構成します。

ユニバース データベースのクレデンシャルの定義

ユニバースでは、**BusinessObjects** ユーザ アカウントに関連付けられているデータベース クレデンシャルを使用する必要があります。

注: 管理者ユーザ アカウントではなく、特権ユーザ アカウントを使用して **BusinessObjects Designer** にサイン オンしていることを確認してください。

ユニバース データベースのクレデンシャルを定義する方法

1. [スタート] メニューから、[すべてのプログラム] - [BusinessObjects XI] - [BusinessObjects Enterprise] - [Designer] を参照します。
2. Designer にログインします。
[Designer] ウィンドウが表示されます。
3. [ファイル] - [インポート] を選択します。
[Import Universe] ダイアログ ボックスが表示されます。
4. ドロップダウン リストから **CA SDM**、ナレッジ マネジメント、**CMDB**、または サポート オートメーション ユニバースのフォルダを選択します。
注: Designer を初めて使用する場合は、[参照] - [CA Universes] を選択します。
5. インポート フォルダのファイル パスを [Import Folder] ボックスで確認します。
6. [OK] をクリックします。
[universe] ウィンドウが表示されます。
7. [File] - [Parameters] を選択します。
[Universe Parameters] ダイアログ ボックスが表示されます。
8. [Definition] タブで [Edit] をクリックします。
[Login Parameters] ダイアログ ボックスが表示されます。
9. [Use database credentials associated with Business Objects user account] チェック ボックスをオンにします。
10. [Next] - [Test Connection] をクリックし、表示されるユニバース接続ダイアログ ボックスの手順に従って操作します。
11. [OK] をクリックして完了します。
12. [ファイル] - [エクスポート] を選択します。
[Export Universe] ダイアログ ボックスが表示されます。
13. [ドメイン] ドロップダウンから使用するユニバースを選択します。
14. [グループ] リストから [全員] を選択します。
15. [OK] をクリックして、ユニバースの変更をエクスポートします。

データ パーティションの設定

「セキュリティと役割の管理」では、データ パーティションに割り当てられているすべてのレポート ユーザに対してデータベース レコードへのアクセスを制限する、データ パーティション制約を作成します。

注: データ パーティション制約の設定の詳細については、[「データ パーティションのセットアップ」](#) (P. 351)を参照してください。

オフライン レポート用の複製されたデータベース

CA SDM にインストールされたレポート コンポーネントに影響する可能性があるパフォーマンスの問題に対処するには、オフライン レポートのために複製されたデータベースを作成します。

注: オフライン レポート用の複製されたデータベースの作成方法については、`NX_ROOT¥samples¥reporting` ディレクトリに置かれたサンプルのドキュメントとスクリプトを参照してください。

ロールベースのレポート

CA SDM では、ロールベースのレポートが [レポート] タブの 2 つのレポート フレームに表示されます。各フレームにはグラフィカル ビューが使用されています。このビューによって、ユーザはレポート データをドリルダウンし、データをグラフおよび集計したグループに表示できます。ロールベースのレポートを管理し、新規 BusinessObjects レポートを [レポート] タブに表示できます。

[レポート リスト] ページには、使用可能なレポートの詳細が含まれます。このページを表示するには、選択したフレームに表示される [レポート リスト] アイコンをクリックします。

役割への役割ベース レポートの定義

役割に割り当てられたユーザがシステムにログインしたときに [レポート リスト] ページに表示されるレポート Web フォームを管理できます。

役割に役割ベース レポートを定義する方法

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] に移動します。

[役割リスト] ページが表示されます。以下に示すデフォルトの役割をレポートに使用できます。

- 変更マネージャ
- 顧客サービス マネージャ
- ナレッジ マネージャ
- ナレッジアナリスト
- サービス デスク マネージャ
- インシデント マネージャ
- 問題 マネージャ

2. リストからいずれかのレポート 役割を選択します。

[Role Detail Form] ページが表示されます。このページには、以下のタブがあります。

権限

役割に割り当てる権限レベルを定義できます。

各機能へのアクセス

各 CA SDM 機能領域への役割のアクセス権を定義できます。

Web インターフェース

ユーザにアクセスを許可する Web ページやオンライン ヘルプ コンテンツを定義することによって、役割の Web インターフェースをカスタマイズします。

ナレッジ マネジメント

役割の ナレッジ マネジメント 権限を指定します。

KTドキュメントの見やすさ

役割に対して表示を許可するドキュメント ステータス（ドラフト、廃止済み、発行済みなど）を指定します。

タブ

この役割に割り当てられているユーザが CA SDM にログインすると表示されるタブを定義できます。

レポート Web フォーム

この役割に対して使用できるようにするレポート Web フォームを定義します。

実行リソース

この役割の [実行] ドロップダウン リストに表示されるレコードタイプを指定します。 [役割の詳細] ページで、 [レポート Web フォーム] タブを選択します。

3. [レポート Web フォーム] タブをクリックします。
[レポート Web フォーム リスト] ページが表示されます。 このページには、使用可能なレポートに関する詳細が表示されます。
4. [Web フォームの更新] をクリックします。
[Web フォームの検索] ページが表示されます。
5. Web フォームを表示するための検索条件を入力し、[検索] をクリックします。
[Web Forms Assigned Update] ページが表示され、検索条件に一致するフォームがリストされます。
6. 左側のリストで、この役割に対して表示する Web フォームを選択します。複数のアイテムを選択するには、Ctrl キーを押しながら左マウスボタンをクリックします。
7. 必要なフォームをすべて選択したら、[選択] ボタンをクリックします。
選択したフォームが右側の [Web Forms Assigned] リストに移動します。
8. [OK] をクリックします。
[役割の詳細] ページが表示され、選択した Web フォームが [レポート Web フォーム] タブにリストされます。

[レポート]タブへの新規レポートの表示

CA SDM 内でレポートの使用が承認されると、そのレポートは InfoView のパブリック セクションに移動し、承認されたユーザがレポートを参照できるようになります。レポートを CA SDM に追加する場合、管理者は追加の手順をいくつか実行する必要があります。

CA Business Intelligence で作成された新規レポートを CA SDM の [レポート] タブに表示できます。このタスクを実行するには、以下のツールを使用します。

- Web スクリーン ペインタ
- 役割管理

開始する前に、以下の操作を実行します。

- CA SDM で機能するよう CA Business Intelligence をインストールして環境設定する。

注: インストールの詳細については、「[実装ガイド](#)」および「[CA Business Intelligence インストールガイド](#)」を参照してください。

- ユーザの権限、役割、および[認証](#) (P. 990) のオプションを自分のレポート環境に設定する。

手順 1: 新規レポートを呼び出すための 2 つの Web フォーム レコードの作成

デフォルトでは、認定ユーザが新規レポートを表示できる 2 つのレポートフレームが [レポート] タブにあります。この手順では、2 つの Web フォーム レコードを作成し、これらの新規レコードを指す URL を定義します。

レポートを呼び出すための 2 つの Web フォーム レコードを作成するには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [Web フォーム] に移動します。
[Web Forms List] ページが表示されます。
2. [新規作成] をクリックします。
[Web フォームの新規作成] ページが表示されます。

3. 以下のフィールドに値を入力します。

Web フォーム名

Web フォームを識別する名前を指定します。必須フィールドです。

例：アセット リスト レポート

レコード ステータス

[アクティブ] を指定します。

コード

システムが Web フォームを識別する一意のコード値を指定します。
一度定義したコードを変更することはできません。

例：asset_list

注：[コード] フィールドに入力した値をメモします。

タイプ

[レポート] を選択します。

説明

(オプション) Web フォームの簡単な説明を入力します。

リソース

新しいレポートを呼び出す URL を指定します。

例：[役割管理] の [Web フォーム] リストからアセット リスト Web フォームを開き、このフォームに表示される URL を指定します。

```
$BOServerURL?sPath=[Home],[Public+Folders],[CA+Reports],[CA+Service+Desk]  
,[Asset]&sDocName=Asset+List&sViewer=html
```

4. [保存] をクリックします。

Web フォームの定義が保存され、[Web フォームの更新] ページが表示されます。

5. 手順 1 から 3 を繰り返して、2 つ目のレポート URL を呼び出す 2 つ目の Web フォーム レコードを作成します。[コード] フィールドに入力した値をメモします。

手順 2: マルチフレーム ページの作成および新規レポートの割り当て

Web スクリーン ペインタでは、フレームセットと呼ばれる 2 つの縦方向のフレームが含まれるマルチフレーム Web ページを作成します。次に、手順 1 で作成した Web フォーム レコードをフレームセットに割り当てます。

注: このページは、任意の数のフレームを使用して作成できます。フレームを追加すると、[レポート] タブの表示が制限されることに注意してください。

マルチフレーム ページを作成してレポートを割り当てるには

1. Web スクリーン ペインタで、[ファイル] - [新規] を選択します。
[フォームの新規作成] ダイアログ ボックスが表示されます。
2. インターフェースおよびフォーム グループのフィールドに適切な値を入力します。
3. [ファイル名] リストから **multiframe.template** を選択します。
4. [新規] をクリックします。
multiframe.html ウィンドウが表示されます。
5. [コントロール] - [フレームセットの挿入] を選択します。
[フレームセットの挿入] ダイアログ ボックスが表示されます。
6. デフォルトの設定は変更せず、[OK] をクリックします。
縦方向の 2 つのフレームがフレームセットに表示されます。
7. 左側の縦方向フレームを右クリックし、ショートカット メニューから [プロパティ] を選択します。
[Properties - Frameset] ダイアログ ボックスが表示されます。
8. **web_form_name** 属性の横にある空白のフィールドを選択し、[...] ボタンをクリックします。
[Enter Web Form Name] ダイアログ ボックスが表示されます。
9. 最初のレポートのコード値を指定します。
例: `asset_list`
10. レポート Web フォーム名が見つかったら、[検証] をクリックします。
11. 右側の縦方向フレームを右クリックし、2 つ目のレポートのコード値を指定してから、そのレポートを検証します。

12. multiframe.html ページを保存します。 ファイル名をメモします。

例： report_mframe.html

13. [ファイル] - [発行] を選択します。

フォームを発行すると、すべての CA SDM ユーザがそのフォームを使用できるようになります。 アナリスト役割の場合、このファイルは Program Files/CA/Service Desk/Site/mods/www/html/web/analyst/report_mframe.html に作成されます。

注: マルチフレーム Web フォームを CA SDM で検索する場合は、[管理] タブで、[セキュリティと役割の管理] - [役割管理] - [Web フォーム] に移動します。 [コード] 列では、Web スクリーンペインタのマルチフレーム フォームの [プロパティ] タブで web_form_name を指定します。

手順 3: [レポート] タブの開始ページの作成

[役割管理] で、手順 2 で作成したマルチフレーム Web ページを呼び出すための開始ページを作成します。

[レポート] タブの開始ページを作成するには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [Web フォーム] に移動します。
[Web Forms List] ページが表示されます。
2. [新規作成] をクリックします。
[Web フォームの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

Web フォーム名

Web フォームを識別する名前を指定します。 このフィールドは必須です。

例： 開始ページ

レコード ステータス

アクティブまたは非アクティブを指定します。

コード

システムが Web フォームを識別する一意のコード値を指定します。
一度定義したコードを変更することはできません。

例： start_page

タイプ

HTMLPL を指定します。

説明

(オプション) Web フォームの簡単な説明を指定します。

リソース

新しいレポートを呼び出す URL を指定します。

例： [Web フォーム リスト] ページで管理者レポートのマルチフレーム レコードを選択します。フォームに表示される URL を指定します。パスの最後に、新しいマルチフレーム ページ (report_mframe.html) を指定します。

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMLPL=report_mframe.html
```

[保存] をクリックします。

新しい開始ページ レコードが [Web フォーム リスト] ページに表示されます。

手順 4: [レポート]タブのレコードの作成および開始ページの割り当て

[役割管理] で、新しい [レポート] タブを作成し、手順 3 で作成した開始ページを指定します。

タブを作成し、レポートを呼び出す開始ページを割り当てるには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [タブ] を選択します。
[タブ リスト] ページが表示されます。
2. [新規作成] をクリックします。
[タブの新規作成] ページが表示されます。

3. 以下のフィールドを指定します。

タブ名

管理インターフェース内でタブを識別する名前を指定します。たとえば、タブ名は「タブ リスト」ページに表示されます。

例：「レポート」タブ

コード

システムがタブを識別するコードを指定します。一度定義したコードを変更することはできません。

例：reports_tab

レコードステータス

「アクティブ」を指定します。

表示名

タブのグラフィカル ユーザ インターフェースに表示される名前を指定します。

例：「レポート」タブ

開始ページ

ユーザがこのタブを選択したときにメイン ウィンドウに最初に表示される Web フォームを指定します。

例：開始ページ

4. 「保存」をクリックします。

このフォームが「Web フォーム リスト」ページに表示されます。

手順 5: 役割レコードへのタブ レコードの割り当て

「役割管理」で、「役割の詳細」ページに一覧表示されている目的の役割に「レポート」タブを割り当てます。この役割に割り当てられているユーザがシステムにログインすると、Web インターフェースに新しい「レポート」タブが表示されるようになります。

タブ レコードを役割レコードに割り当てるには

1. 「管理」タブで、「セキュリティと役割の管理」 - 「役割管理」 - 「役割リスト」を選択します。

「役割リスト」ページが表示されます。

2. [役割] リストから目的の役割を選択します。
[役割の詳細] ページが表示されます。
3. このページの下部で [タブ] を選択し、次に [タブの更新] を選択します。
新しいタブが [タブ リスト] に表示されます。

[InfoView] ボタンの開始ページの作成

新しいウィンドウで **BusinessObjects InfoView** を開く [InfoView] ボタンを、[レポート] タブにオプションで追加できます。このオプションは、[レポート] タブ レコードに表示される開始ページ オプションから制御されます。

[InfoView] ボタンの開始ページを作成するには

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [Web フォーム] に移動します。
[Web Forms List] ページが表示されます。
2. [新規作成] をクリックします。
[Web フォームの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

Web フォーム名

(必須) Web フォームを識別する名前を指定します。

例 : InfoView ページ

レコード ステータス

アクティブまたは非アクティブを指定します。

コード

システムが Web フォームを識別するコード値を指定します。

例 : info_view_page

タイプ

HTMLPL を指定します。

説明

(オプション) Web フォームの説明を入力します。

リソース

レポート フレームを呼び出す URL を指定します。

例： [Web フォーム リスト] ページで管理者 InfoView レコードを選択します。 フォームに表示される URL を指定します。 パスの最後に、 [レポート] タブの新しい開始ページ (start_page) を指定します。

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=show_report_frames.html+KEEP.report_form=start_page
```

[保存] をクリックします。

InfoView の 開始ページが [Web フォーム リスト] ページに表示されます。

手順 7: [レポート]タブ レコードへの [InfoView]ボタンの開始ページの割り当て

[役割管理] で、手順 6 で作成した [InfoView] ボタンの開始ページを [レポート] タブ レコードに割り当てます。

[Infoview]ボタンの開始ページ レコードを[レポート]タブ レコードに割り当てるには

1. [役割管理] の [タブ リスト] ページから新しい [レポート] タブ Web フォーム レコードを選択します。
詳細ページが表示されます。
2. [編集] を選択します。
[タブの更新] ページが表示されます。
3. [開始ページ] フィールドで、 [InfoView] ボタンの新しい開始ページを指定します。
4. [保存] をクリックします。

ユーザが [レポート] タブを開くと、 [InfoView] ボタンがフォームの右上隅に表示されます。

Web ベースのレポート

CA Business Intelligence では、CA SDM および ナレッジ マネジメント 用の Web ベースの事前定義レポートのセットがインストールされます。これは、BusinessObjects Enterprise Web Intelligence または Crystal Reports を使用して作成されます。レポートは、サイト固有のレポートを定義するためのモデルとして使用できます。

これらのレポートは、インストール後に CA Business Intelligence レポート サーバに自動的に展開されるフォルダに格納されます。

フォルダとドキュメントにセキュリティを割り当てて、グローバルにアクセスを許可するか、特定のロールにアクセスを許可するか、または個々のユーザにアクセスを許可するかを指定できます。

注: BusinessObjects InfoView には、BusinessObjects InfoView の使用方法を説明したユーザ ガイドが含まれています。ユーザ ガイドにアクセスするには、InfoView 内のヘルプ アイコンをクリックします。定義済みレポートの使用に関する一般的な情報については、オンライン ヘルプを参照してください。

関連項目:

[BusinessObjects InfoView インターフェース \(P. 1013\)](#)

[レポートへの移動 \(P. 1014\)](#)

[InfoView の環境設定 \(P. 1014\)](#)

[レポートのスケジュール \(P. 1015\)](#)

[データ分析のセットアップ \(P. 1016\)](#)

[レポートの発行と配布 \(P. 1016\)](#)

BusinessObjects InfoView インターフェース

アナリストおよびマネージャは、CA SDM の [レポート] タブで、各自の役割に定義されたレポートを使用したり、[InfoView] ボタンをクリックして個人のレポートを管理したりできます。InfoView では、ユーザは Crystal Reports のレポートや Web Intelligence のドキュメント、およびその他のオブジェクトにアクセスし、各自の環境設定に合わせてこれらを整理できます。

InfoView で使用できる機能はコンテンツ タイプによって異なりますが、一般的には Web ブラウザでの情報の表示、(Microsoft Excel などの) ほかのビジネス アプリケーションへの情報のエクスポート、および指定した場所への情報の保存が可能です。

注: InfoView で表示されるフォルダおよびオブジェクトは、ユーザに割り当てられたグループ (役割) によって異なります。

レポートへの移動

InfoView ウィンドウの左側のペイン内のフォルダに移動して、レポートの表示、スケジュール、変更、または実行や、レポートの履歴およびプロパティの表示を行うことができます。

レポートを表示する方法

1. 以下のいずれかの方法を使用して、InfoView を開きます。
 - CA SDM の [レポート] タブで、[InfoView] ボタンをクリックします。
 - [スタート] メニューから、[すべてのプログラム] - [BusinessObjects XI] - [BusinessObjects Enterprise] - [BusinessObjects Enterprise Java InfoView] を参照します。
[InfoView] ホーム ページが表示されます。
2. 左側のペインで、フォルダ構造 [パブリック フォルダ/CA レポート/CA SDM] に移動します。
3. 表示するレポートのタイプに対応するフォルダをクリックします。
4. 表示する情報のタイプのレポート名をクリックします。
レポートが BusinessObjects InfoView に表示されます。

InfoView の環境設定

ユーザは、一般的な環境設定を設定して、InfoView が開始されるユーザ個人のダッシュボード ページ (Web Intelligence の My InfoView ツールで設計) を指定できます。Web Intelligence および Crystal Reports でのユーザ個人の表示環境設定も設定できます。

レポートのスケジュール

InfoView では、レポートのスケジュールがサポートされています。一時的なレポートの場合、スケジュールされたレポートは [マイ フォルダ] セクションに格納されます。 レポートが「オープン時にリフレッシュ」するように設定されている場合、エンドユーザがレポートを表示するたびに、システムはデータベースにアクセスして最新情報を取得します。ユーザは、特定の時間に実行するようにレポートをスケジュールできます。

管理者は、適切なスケジュール日付が反映されるようにカレンダーを定義できます。たとえば、ユーザはタイミングと頻度を指定する [When] オプションを使用して、該当する就業日を表示して就業日以外は非表示となるカレンダーを選択できます。

注: レポートのスケジュールの詳細については、BusinessObjects のドキュメントを参照してください。

スケジュールでは、ユーザは以下のことを実行できます。

- スケジュールのタイミングと頻度（即時、毎時、月次、週次など）を指定する。
- 宛先（受信トレイ、ファイルの場所、電子メール受信者など）を指定する。
- レポートを送信する受信トレイを指定する。
- 出力形式 (Web Intelligence、Crystal Report、Microsoft Excel、Adobe Acrobat など) を指定する。
- キャッシュ オプションを指定する。デフォルトでは、ドキュメント結果は Output File Repository Server に格納されます。ユーザは、キャッシュのフォーマットおよびロケールを選択することで、レポートを Web Intelligence Report Server にキャッシュするように指定できます。
- リクエストを処理するサーバグループを選択する。定義済みのイベントが選択された場合、オブジェクトは追加の条件またはイベントが発生した場合にのみ実行されます。

注: InfoView のパブリック フォルダ セクションでのデータ制限を CA SDM データ パーティションによって管理している場合、パブリック フォルダに含まれているスケジュール済みレポートを各ユーザに定義する必要があります。

データ分析のセットアップ

レポートデータの表示方法を調整するための拡張ツールセットを提供するインタラクティブビューアを使用できます。グループから担当者や実際のリクエストなど、さまざまな詳細レベルにドリルダウンできます。

インタラクティブビューアを使用すると、以下の操作を実行できます。

- データを別の「ブロック」フォーマット（円グラフなど）で表示することで、レポートのデザインを変更する。たとえば、レポート内で右クリックし、[Turn table to] を選択すると、レポートデザイン機能が表示されます。
- レポートの並べ替え、レポートの分割、計算、フィルタリング、ランク付けなどのさまざまなタスクを実行する。
- ほかのユーザやグループと情報を共有する。

レポートの発行と配布

InfoView ユーザは、レポートデータを Excel、PDF、または CSV 形式で保存して、ファイルの場所、受信トレイ、電子メールアドレス、または FTP サイトに配布できます。

CA SDM 内でレポートの使用が承認されると、そのレポートはパブリックセクションに移動し、承認されたユーザがレポートを参照できるようになります。フォルダとドキュメントにセキュリティを割り当てて、グローバルにアクセスを許可するか、特定の役割にアクセスを許可するか、または個々のユーザにアクセスを許可するかを指定できます。セキュリティは BusinessObjects の Central Management Console で管理されています。

重要業績評価指標 (KPI)

重要業績評価指標 (KPI) は、管理上の注意または構成のチューニングが必要になることのあるサービス管理環境の領域を識別するために使用できる評価基準です。

CA SDM Web インターフェースを使用して、重要業績評価指標 (KPI) の定義を構成します。重要業績評価指標 (KPI) が生成するデータは CA SDM データベースに格納され、[Web ベースのレポート \(P. 1013\)](#)の作成に使用できます。

注: 重要業績評価指標 (KPI) のクエリの定義に加えて、チケットがオープンまたはクローズになった場合や、特定のフィールドが変更された場合に CA SDM チケット データを取得する KPI デーモンを構成することもできます。

周到に計画された重要業績評価指標 (KPI) のセットを定義して監視することにより、それぞれの企業の業績関連目標の進捗状況を評価し、IT 環境に関する戦略的意志決定を推進するための重要なデータを収集できます。

注: KPI のデータベース テーブルの詳細については、「テクニカル リファレンス ガイド」を参照してください。

KPI タイプ

CA SDM には、3 種類の KPI タイプが用意されています。

- **システム KPI** は CA SDM と共にインストールされます。必要に応じてカスタマイズできますが、新しいシステム KPI を作成することはできません。
- **ストアドクエリ KPI** は、ストアドクエリをコールして、データベースからメトリックを取得します。ストアドクエリ KPI はカスタマイズすることができます。また、製品にインストールされている事前定義済みの例を変更して使用することもできます。
- **SQL KPI** を使用すると、完全な SQL クエリを KPI に直接組み込むことができます。SQL KPI はカスタマイズすることができます。また、製品にインストールされている事前定義済みの例を変更して使用することもできます。

注:

- KPI の全 3 タイプの設定の詳細については、「オンライン ヘルプ」を参照してください。
- KPI は、事前定義済みか、ユーザ作成されたかにかかわらず、削除できません。KPI が不必要になった場合、レコード ステータスを非アクティブに設定することで、非アクティブ化できます。

事前定義済み KPI

各タイプのいくつもの KPI が **CA SDM** と共にインストールされます。このガイドを読みながら、それらの KPI を確認していくと役に立ちます。

事前定義済みのストアドクエリおよび **SQL KPI** は、元の定義のまま使用することも、独自に定義をカスタマイズするためのモデルとして活用することもできます。

事前定義済みのシステム KPI は、元の定義のまま使用することも、必要に応じていくつかのフィールドを変更することもできます。

注: ほとんどの事前定義済み KPI は、デフォルトでは非アクティブステータスに設定されています。**Web** インターフェースでこれらを表示するには、**[KPI リスト]** ページをフィルタして、非アクティブな重要業績評価指標 (KPI) を表示します。

KPI デーモン

KPI デーモンは、KPI メトリックデータの取得、組織およびストレージを管理します。デーモンは連続的に実行されて、さまざまなシステムリソースから指定された間隔でデータを集めます。

KPI の更新時間がくると、KPI デーモンは以下のように他のシステムコンポーネントとやり取りします。

- **システム KPI** - ターゲットデーモン (**WebEngine**、**domsrvr**、**bpvrtddb** または **db_agents**) にリクエストを送信して、カウントデータまたは期間データを取得します。
- **ストアドクエリ KPI** - **domsrvr** にリクエストを送信して、カウントデータを収集します。
- **SQL KPI** - **domsrvr** にリクエストを送信して、カウント、合計、最大、または期間のデータを収集します。

KPI デーモンがリクエストされたデータを受信すると、結果のメトリックがデータベースに格納されます。

注: 計算された期間は、営業時間ではなくチケット内でのリアルタイムな値の変更に基きます。

システム KPI

システム KPI を使用して、CA SDM プロセスの操作に関連するメトリックデータを収集できます。

サポートされているプロセス タイプは以下のとおりです。

- **domsrvr** - CA SDM のオブジェクト マネージャ (サーバ プロセス) です。また、オブジェクト マネージャにより、さまざまなクライアントのレコードおよびテーブルのキャッシュも行われます。
- **bpvrtddb** - BOP Virtual Database サーバです。CA SDM 環境で複数のオブジェクト マネージャを操作できます。オブジェクト マネージャが、データベース エージェントへのアクセスを仲介する仮想データベースに接続します。たとえば、チケット参照番号の新しい範囲を取得する場合、仮想データベースにより、一度に 1 つのオブジェクト マネージャのみが該当する参照番号を含むテーブルにアクセスすることが保証されます。

CA SDM の設定に応じて、オブジェクト マネージャは、以下のサーバの仮想データベースに接続します。

- 標準：プライマリ サーバまたはセカンダリ サーバ上で実行されるすべてのオブジェクト マネージャは、プライマリ サーバの仮想データベースに接続します。
- 高可用性：すべてのオブジェクト マネージャは、オブジェクト マネージャが実行されているのと同じサーバの仮想データベースに接続します。たとえば、アプリケーション サーバで実行されるオブジェクト マネージャは、アプリケーション サーバの仮想データベースにのみ接続します。

仮想データベースは、さらにオブジェクト マネージャ用にデータベース情報のキャッシュを実行します。

- **db_agents** - データベース エージェントにより SQL クエリが実行されます。また、CA SDM とデータベース管理システム (DBMS) 間のその他のやり取りが処理されます。データベース エージェントは CA SDM データベース スキーマに準拠し、SQL コードを特定の DBMS (たとえば Oracle) が必要とする形式に変換します。

- **webengine** - Microsoft の IIS または Apache Tomcat Web サーバで実行中の pdmweb cgi を介して、Web ブラウザをオブジェクトマネージャへ接続する CA SDM コンポーネントです。

CA SDM の設定に応じて、WSP スキーマ デザイナがスキーマ ファイルを書き込むには、以下のサーバ上に WSP 用の Web エンジンが必要です。

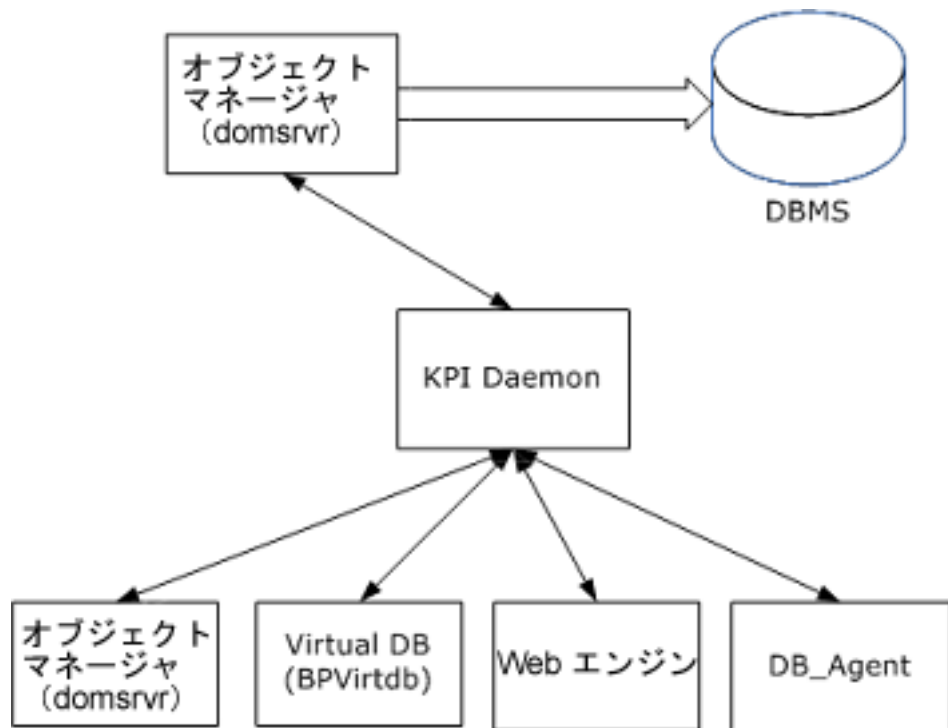
- 標準：プライマリ サーバ
- 高可用性：バックグラウンドサーバ

Web エンジンは、ユーザ クライアント Web ブラウザ用のオブジェクトマネージャの実際のクライアントです。Web エンジンにより、接続されたユーザの .html Web フォームがキャッシュされます。

pdm_webcache ユーティリティを使用してキャッシュを操作したり、pdm_webstat ユーティリティを使用して接続統計を確認したりすることができます。

注: これらのプロセスの詳細については、「実装ガイド」を参照してください。

以下の図は、システム KPI のデータ フローを示したものです。



システム KPI はそれぞれ、以下のメトリック タイプのうちの 1 つを作成します。

- カウント
- 期間

システム KPI の例

- 以下の例は、BOP 仮想データベースに送信された更新リクエストの件数を取得するものです。

```
updateCt
```

- 以下の例は、BOP 仮想データベースに送信された更新、挿入、および削除のリクエストが完了するまでにかかる時間を報告するものです。

```
virtddbUpdateResponseDt
```

ストアドクエリ KPI

ストアドクエリ KPI を使って、CA SDM データベースから取得されたカウント メトリックに基づいたレポートを生成できます。

CA SDM には、事前定義済みストアドクエリのセットが用意されています。これらの多くは、ストアドクエリと同様に役に立ちます。さらに、必要に応じてこれらをカスタマイズしたり、自分で使うクエリを書くためのモデルとして活用することができます。

すべてのストアドクエリ KPI には、カウントのメトリック タイプが用意されています。

注: ストアドクエリを使用すると、Web インターフェース スコアボード用の [カウンタ] フィールドあるいは KPI メトリックのいずれか、または両方を作成することができます。KPI 定義の中でストアドクエリを使用するには、クエリを KPI 使用法に対して有効化しておく必要があります。詳細については、[「ストアドクエリの設定」](#) (P. 548)を参照してください。

ストアドクエリ KPI の例

- 以下の例は、担当者のロケーションにおけるオープン変更要求の件数を取得するものです。

```
@cnt.location.name Changes
```

- 以下の例は、現在の日付の真夜中までに SLA に違反すると予想されるワークフロー タスクの件数を取得するものです。

Issue Workflow Tasks that will Violate an SLA today

SQL KPIs

SQL KPI はストアドクエリ KPI よりも柔軟性に優れています。SQL KPI では、以下のタイプのメトリックを作成するために CA SDM データベースに自分のクエリを書き込むことができます。

- 合計
- カウント
- 最大
- 期間

注: ご使用の SQL コードは SQL92 構文に準拠している必要があります。

SQL KPI には、以下の注意事項が適用されます。

- これらのクエリ例の SQL コードを確認するには、[KPI リスト] ページからクエリ定義を開きます。

注: 詳細については、オンライン ヘルプを参照してください。

- @ 記号は SQL KPI ではサポートされていません。代わりに、以下の例に示す構文と属性の別名を使用します。

```
SELECT * FROM cr WHERE assignee_last_name = "Smith"
```

この例の場合、事前定義済みの属性別名を使用することもできます。
[Attribute Alias Detail] ページは以下のように表示されます。

```
" オブジェクト名          = cr
" 別名                    = assignee_last_name
" ステータス              = アクティブ
" 別名の値                = assignee.last_name
```

例: SQL クエリ KPI

- この事前定義済みの例は、すべての保留中の変更要求ワークフロー タスクの予定コストの合計を算出するものです。

保留中の変更要求ワークフロー タスクの予定コストの合計

- この事前定義済みの例は、クローズされ、再オープンされたアクティブな変更要求の件数を取得するものです。

再オープンされた変更要求の数

KPI フィールド

以下の表で、KPI フィールドについて説明します。Sys S.Q. および SQL 列は、各フィールドが属する KPI タイプ（システム、ストアドクエリまたは SQL）を示します。

注: フィールドがオプションとして指定されていない限り、すべてのフィールドは必須です。

フィールド	Sys.	S.Q.	SQL	説明
KPI 名	X	X	X	KPI の表示名を示します。編集不可です。
タイプ	X	X	X	レコードをシステム、ストアドクエリまたは SQL KPI として定義します。編集不可です。
既存のバージョンを維持する	X	X	X	レコードが更新された場合に重要業績評価指標（KPI）レコードの現在のバージョンが保持されることを指定します。NX.env ファイルにある @NX_ALWAYS_KEEP_KPI_VERSIONS が [No] に設定されている場合、編集可能です。
バージョン	X	X	X	重要業績評価指標（KPI）レコードのバージョン番号を示します。レコードが更新されるたびに、バージョン番号は自動的に増えます。編集不可です。
レコードステータス	X	X	X	KPI がアクティブ（データを収集する）か、非アクティブ（データを収集しない）かを指定します。[KPI リスト] ページで [リスト内で編集] 機能を使用した場合にのみ、編集可能です。

フィールド	Sys.	S.Q.	SQL	説明
メトリックタイプ	X	X	X	KPI が実行する計算のタイプを指定します。 ■ ストアドクエリ KPI は常に [カウント] です。 ■ システム KPI は [カウント] または [期間] の場合もあります。 ■ SQL KPI は [カウント]、[合計]、[最大] または [期間] の場合もあります。 SQL タイプの KPI のみ場合は編集可能です。
更新時間	X	X	X	データベースから KPI メトリックを取得するための時間間隔を指定します。値は編集可能です。更新時間は HH : MM : SS フォーマットで指定します。
プロセスタイプ	X			システム KPI (P. 1019) メトリックは以下の CA SDM プロセスから作成される場合があります。 ■ domsrvr - オブジェクトマネージャ ■ bpvirtddb - BOP 仮想データベース サーバ ■ db_agents - データベース エージェント ■ webengine - CA SDM Web クライアント
システム名前	X			システム KPI の内部名です。編集不可です。
ユーザコンテキスト		X	X	(オプション) CA SDM 連絡先のユーザ ID を指定します。連絡先の役割およびテナントの割り当てにより、KPI によって作成されるメトリックのデータパーティション化が決まります。値は編集可能です。
ストアドクエリ		X		この KPI によってコールされたストアドクエリの名前です。値は編集可能です。
SQL クエリ			X	クエリのための SQL コードです。値は編集可能です。
説明	X	X	X	(オプション) KPI の詳細な説明です。値は編集可能です。

チケットデータの取得

チケットがさまざまな処理状態に置かれている期間をレポートするために、チケットがオープンまたはクローズされた場合や、以下の値が変更された場合に **CA SDM** チケット データを取得するように **KPI** デーモンを構成できます。

- アクティブ
- 担当者
- 領域またはカテゴリ
- グループ
- 影響度
- 組織
- 優先度
- 根本原因
- ステータス
- サービス タイプ

チケットの取得を有効にするには、[Options Manager KPI] フォルダに用意されている **KPI** チケット データ テーブル オプションをインストールします。

新規チケットおよび更新されたチケットのデータ収集が可能になります。チケット データは **usp_kpi_ticket_data** データベース テーブルに書き込まれ、**Web** ベースのレポートの生成に使用できます。

注: 詳細については、オンライン ヘルプを参照してください。

チケットの取得には、以下の注意事項が適用されます。

- **KPI** デーモンは、**usp_kpi_ticket_data** テーブルにチケット情報を取り込むために 30 分ほどかかる場合があります。
- **support_lev** フィールドでは、**classic_sla_processing** オプションがインストールされている場合、サービス タイプの処理を追跡できます。**classic_sla_processing** オプションを使うと、**CA SDM** バージョン 6.0 以前でもサービス タイプの処理が可能になります。
- ただし、この機能を有効にすると、**CA SDM** のパフォーマンスが低下する場合があります。

関連項目:

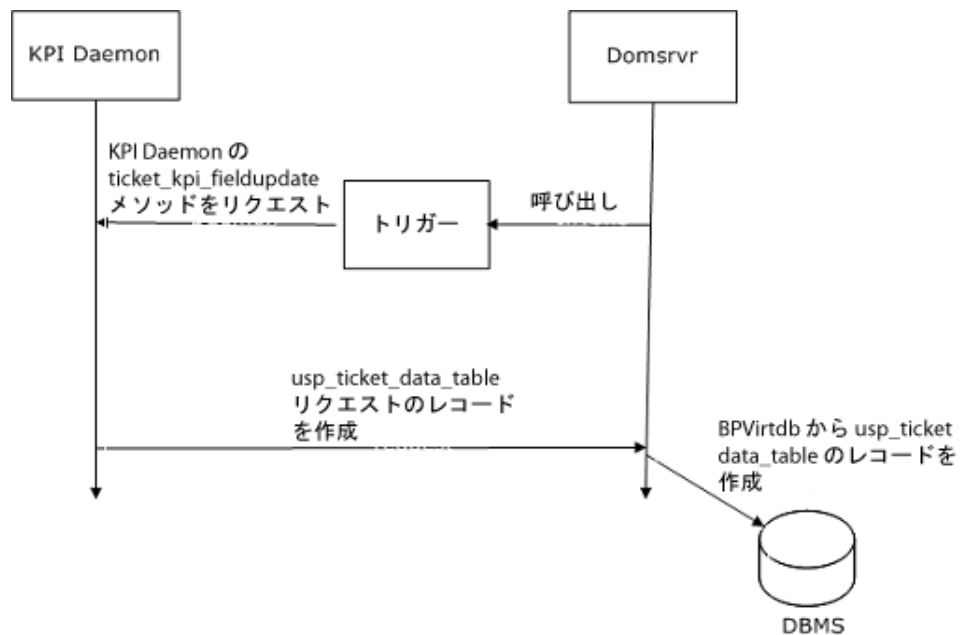
[NX.env ファイル](#) (P. 1028)

KPI チケット データのフロー

KPI チケット データ テーブル機能は、トリガ メカニズムで動作します。
kpi_ticket_data_table オプションがインストールされている場合、KPI デーモンは、以下のイベントをトラッキングするために CA SDM チケット オブジェクトの監視を開始します。

- 新規チケットのオープン
- 1つ以上の監視されたフィールドに対する変更の確認
- チケットのクローズ

これらのイベントのうちいずれかが発生すると、POST_CI トリガが実行されます。トリガにより、トリガ属性リストを持つ BPMMessage が KPI デーモンに送られ、以下のデータ フロー図に示されるように、usp_kpi_ticket_data テーブルに戻りデータが追加されます。



KPI チケット データ テーブルのレコード タイプ

usp_kpi_ticket_data テーブルには、以下のような 5 つの操作タイプがあります。

- INIT (0)
- NO_INIT_REC (1)
- REOPEN (2)
- UPDATE (3)
- CLOSE (4)

タイプ値 (丸かっこに示される整数値) は操作フィールドに格納されます。前のレコードの `end_time` は `prev_time` フィールドに格納されます。`ktd_duration` フィールドには期間が格納されます。期間は、`prev_time` を引いた `end_time` として計算されます。前のレコードは以下のルールで定義されます。

1. INIT レコードは、チケットが作成されたことを示します。
2. UPDATE レコードはチケットへの更新ごとに作成されます。前の UPDATE レコードが存在する場合、前の UPDATE レコードから同じチケットフィールドへ `prev_time` が取得されます。前の UPDATE レコードが存在しない場合、UPDATE レコードに対してどのレコードが最も時間的に接近している `end_time` 値を持っているかによって、`prev_time` が INIT、NO_INIT_REC または REOPEN レコードから取得されます。
3. CLOSE レコードは UPDATE と同じです。
4. チケットが再オープンされる場合、アクティブ フィールド値を表示するために単一の REOPEN レコードが作成されます。REOPEN レコードには、同じアクティブ フィールド用の前の CLOSE レコードから `prev_time` が取得されます。
5. チケットがオプションマネージャ オプションをオンにする前に作成された場合、チケットには INIT レコードのない更新用のレコードが含まれる場合があります。この場合は、NO_INIT_REC レコードが作成され、最初に遭遇する非 INIT レコードから `prev_time` が取得されます。

注: テーブル フィールドの詳細なドキュメントについては、「テクニカルリファレンス ガイド」を参照してください。

トラブルシューティング

重要業績評価指標 (KPI) の使用時に発生する可能性のある問題を診断することができます。

KPI デーモンが実行中であることの確認

KPI デーモンが実行中であることを確認するには、以下のように `pdm_status` コマンドラインユーティリティを実行します。

```
pdm_status
```

以下のような出力を確認します。

```
KPI Daemon myserver Running myserver 3568 Wed Feb 06 07:23:53
```

NX.env ファイル

基本的な KPI 構成が適切に設定されていることを検証するには、`$NX_ROOT/NX.env` ファイルを確認します。

ご使用の環境に KPI チケット データ テーブル オプションがインストールされていれば、`NX.env` ファイルには以下が含まれます。

```
#####  
# NX_KPI_TICKET_DATA_TABLE  
# Enable the collection of changed fields from ticket objects  
# (like Requests, Issues and Change Orders) to write record entries  
# into the usp_kpi_ticket_data table.  
#####  
@NX_KPI_TICKET_DATA_TABLE=Yes
```



```
#####
# NX_KPI_FUZZ_TIME
# Specifies a tolerable delay for each KPI within which kpi_daemon
# sends a request to retrieve KPI data when this kpi's refresh time
# is timeout
#####
@NX_KPI_FUZZ_TIME=20
```

注: @NX_KPI_FUZZ_TIME のデフォルト値は 20 秒です。この値は、0 ～ 40 秒の範囲内で変更できます。40 秒を超える値が設定された場合は、40 秒が適用されます。

```
#####
# NX_ALWAYS_KEEP_KPI_VERSIONS
# The keep_version attribute in Kpi table is displayed on the KPI
# Detail Edit form as a checkbox. The NX_ALWAYS_KEEP_KPI_VERSIONS
# option specifies that checkbox is read-only and is always checked.
#####
@NX_ALWAYS_KEEP_KPI_VERSIONS=Yes
```

KPI デーモントレースのオン

KPI デーモン アクティビティを監視するには、pdm_logstat ユーティリティを使用して、ログのトレースをオンにします。

KPI デーモンのトレースをオンにするには、以下のコマンドを実行します。

```
pdm_logstat -f cache_table_mgr.c VERBOSE
```

KPI デーモンのトレースをオフにするには、以下のコマンドを実行します。

```
pdm_logstat -f cache_table_mgr.c
```

KPI デーモン アクティビティに関連するエントリ用の stdlog.0 ファイルを検証します。

以下の例は、ホスト コンピュータおよび domsrvr への正常な KPI デーモン接続を示しています。

```
02/06 05:42:14.58 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT kpi_daemon.c 117 KPIDaemon ready for
action!
02/06 05:42:14.80 garbo-2k3-bb domsrvr 792 SIGNIFICANT connmgr.c 2314 Connecting client
kpi_daemon:garbo-2k3-bb
02/06 05:42:14.81 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT main.c 220 KPI daemon connected with domsrvr
```

以下の例は、webSessionCT という名称の KPI におけるエラーを示しています。

```
01/16 13:24:46.74 jed web:local 2152 ERROR sys_kpi.c 96 Invalid KPI metric type: 1382180215 (KPI name:webSessionCT)
```

以下の例は、KPI デーモン アクティビティを示しています。

```
02/06 07:23:50.47 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache Table manager created Kpi_Obj (KPI dob record_id:9003) (KPI type:2)
02/06 07:23:50.53 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache Table manager created Kpi_Obj (KPI dob record_id:9103) (KPI type:1)
```

注: KPI タイプの詳細については、[「KPI チケットデータテーブルのレコードタイプ」](#) (P. 1027) を参照してください。

一時的なレポート

一時的なレポートは、InfoView で Web Intelligence を使用して作成されます。一時的なレポートを作成できます。

注: 一時的なレポートの詳細については、BusinessObjects Enterprise のドキュメントを参照してください。ドキュメントにアクセスするには、InfoView 内のヘルプアイコンをクリックします。

Web Intelligence インターフェース

InfoView の Web Intelligence には、クエリを記述せずに簡単に基本レポートを作成したいユーザ向けに、カスタム レポート ツールが用意されています。Web Intelligence では、事前定義のレポートモデルとテンプレートを使用して、データ接続、クエリ、およびデータの関連性が管理されるため、データ フィールドをテンプレート上にドラッグ アンド ドロップするだけで表形式またはマトリックス形式のレポートを作成できます。InfoView の「ユーザ ガイド」に記載されているすべての InfoView 機能を使用できます。

Web Intelligence ドキュメントでは、ユニバースと呼ばれる BusinessObjects オブジェクトを参照してレポートを作成します。BusinessObjects ユニバースで新規レポートを構築します。CA Business Intelligence 製品には、CA SDM ユニバースが付属しています。

一時的なレポートの作成機能の仕組み

一時的なレポートの作成機能の仕組みは、以下のとおりです。

1. 最初に InfoView で CA SDM ユニバースを選択して、一時的なレポートを開始します。
2. ユニバースは、企業のビジネス情報を含む CA SDM データベースにマップされます。ユニバースに接続すると、Web Intelligence によって自動的にドキュメント エディタ (InfoView の [Web Intelligence Document Preferences] ページで選択したもの) が起動されます。

注: 環境設定の詳細については、InfoView の「ユーザ ガイド」を参照してください。

3. ユニバースを使用して、レポート フォームで使用するためのデータをクラスと呼ばれるフォルダにグループ化されたオブジェクトから取得するクエリを作成します。また、各クラスには、1 つ以上のサブクラスを含めることもできます。サブクラスには、上位レベルのクラス内のオブジェクトのさらなるサブカテゴリであるオブジェクトが含まれます。クラスとオブジェクトは、[データ] タブにツリー構造 (階層) で表示されます。

注: Web Intelligence ドキュメントのクエリの作成方法については、BusinessObjects Enterprise ドキュメントを参照してください。

4. 必要なオブジェクトを [Result Objects] ペインに追加してクエリを作成し、クエリ フィルタ プロパティの定義が完了すると、クエリを実行できます。クエリを実行すると、ユニバースからデータベースへの問い合わせが行われ、クエリに含まれる各オブジェクトの要求に対応するデータが取得されます。クエリを実行するには、ツールバーで [クエリの実行] をクリックします。

重要: クエリのオブジェクトを選択する場合、オブジェクト、測定方法、およびフィルタは必ず 1 つのユニバース ベース クラスとそのサブクラスから選択します。複数のベース クラスからのオブジェクト、測定方法、およびフィルタをクエリに含めた場合、予期しない結果を受け取ったり、パフォーマンスが低下したりする可能性があります。

一時的なレポートの例

Web Intelligence およびクエリ例を使用して、デフォルトの CA SDM ユニバースを使用した一時的なレポートを作成できます。 レポートを作成する場合は、レポートを定期的に保存するようにしてください。 Web Intelligence 接続セッションがタイムアウトすると、レポートに加えた変更内容が失われます。

注: セッションタイムアウト値の変更の詳細については、「[実装ガイド](#)」を参照してください。

例: 優先度 1 および 2 のすべてのオープン リクエストをすべてのユーザに表示

この例では、レポートの生成前に追加データを収集するプロンプト値を指定します。

例: 優先度 1 および 2 のすべてのオープン リクエストをすべてのユーザに表示

1. メニュー バーで [新規] - [Web Intelligence Document] をクリックします。
[New Web Intelligence Document] ページが表示されます。
2. [Universe] 列で CA SDM ユニバースを選択します。
Web Intelligence ドキュメントがユニバース情報と共に左側のペインに表示されます。
注: ナビゲーションを向上するには、左側のペインで [添付サービス タイプ] フォルダを閉じます。
3. 左側のペインで [リクエスト] を見つけてから、[リクエストの詳細] フォルダを展開します。スクロール バーを使用してフォルダを見つめます。
4. 以下のオブジェクトをそれぞれ選択し、[Results Objects] で左側のペインから右上のペインにそのオブジェクトをドラッグ アンド ドロップします。
 - 概要
 - 優先度シンボル
 - Customer Combo Name

5. 以下のオブジェクトを選択し、[Query Filters] で右下のパネルにこれらのオブジェクトをドラッグアンドドロップします。完了したら、[リクエストの詳細] フォルダを閉じます。
 - ステータス シンボル
 - 優先度シンボル
6. [リクエストフィルタ] フォルダを展開し、[Query Filters] で右下のパネルにユーザ ID フィルタによる [Customer Combo Name] をドラッグアンドドロップします。
7. [Query Filters] ペインで、[Status Symbol] フィルタの [In list] 矢印をクリックし、[等しい] 演算子を選択します。
8. [Operand Type] メニューのリストから値を選択します。
[List of Values] ダイアログ ボックスが表示されます。
9. [Status Symbol] リストで、[開く] を選択してから、緑の矢印をクリックします。
値が [Value(s) Selected] フィールドに表示されます。
10. [OK] をクリックします。
11. [Query Filters] ペインで、[Priority Symbol] フィルタの [In list] ドロップダウンをクリックし、[In List] 演算子を選択します。
12. [Priority Symbol] リストで、1 および 2 を複数選択してから、緑の矢印をクリックします。
値 1 および 2 が [Value(s) Selected] フィールドに表示されます。
13. [OK] をクリックします。
14. ツールバーの [クエリの実行] をクリックして、レポートを生成します。
注: ユーザ ID クイック フィルタによる [Customer Combo Name] ではプロンプト機能が使用されるため、[プロンプト] ダイアログ ボックスが表示されます。このダイアログを使用すると、レポートを生成する前に追加のデータを収集できます。
15. [プロンプト] ウィンドウで、最初のオプション [すべて] を選択してから、緑の矢印ボタンをクリックします。
すべてのユーザ名が [Select Customer] リストに表示されます。
16. [クエリの実行] をクリックして、レポートを生成します。
新しいウィンドウにレポートが表示されます。

17. レポート タイトルをダブルクリックし、テキスト ボックスに「すべてのユーザの優先度 1 & 2 のオープン リクエスト」と入力します。 フォント サイズは 16 またはそれ以外のサイズに変更できます。
18. レポートのほかの要素を変更するには、[プロパティ] タブをクリックします。
19. データを顧客の姓別でサブグループ化するには、[Customer Last Name] 列内のセルの任意データを右クリックして、[Set as Section] を選択します。
20. [保存] をクリックし、[名前を付けて保存] オプションで場所を指定します。

例: [作業中]ステータスが含まれていないすべてのオープン リクエストの表示

この例では、オープン リクエストの合計数を返す、カウント レポート機能を指定します。

例: [作業中]ステータスが含まれていないすべてのオープン リクエストの表示

1. メニュー バーで [新規] - [Web Intelligence Document] をクリックします。
[New Web Intelligence Document] ページが表示されます。
2. [Universe] 列で CA SDM ユニバースを選択します。
Web Intelligence ドキュメントがユニバース情報と共に左側のペインに表示されます。
注: ナビゲーションを向上するには、左側のペインで[添付サービス タイプ] フォルダを閉じます。
3. 左側のペインで [リクエスト] を見つけてから、[リクエストの詳細] フォルダを展開します。(スクロール バーを使用してフォルダを見つめます。)
4. 以下のオブジェクトをそれぞれ選択し、[Results Objects] で左側のペインから右上のペインにそのオブジェクトをドラッグ アンド ドロップします。
 - ステータス シンボル
 - 参照番号
 - 概要

5. [Status Symbol] オブジェクトを選択し、[Query Filters] で右下のパネルにこれをドラッグアンドドロップします。[リクエストの詳細] フォルダを閉じます。
6. [Request Filters] フォルダを展開し、[Query Filters] で右下のパネルにアクティブなフィルタをドラッグアンドドロップします。
7. [Query Filters] ペインで、[Status Symbol] オブジェクトの [In list] 矢印をクリックし、[Not Equal to] 演算子を選択します。
8. [Operand Type] メニューから [作業中] を選択します。
9. メイン ツールバーの [Edit Report] を選択します。
[Report Viewer] が開きます。
10. レポートで [参照番号] 列を選択します。このアクションにより、レポート ツールバーの [Insert Sum] コマンドが使用できるようになります。
11. [Insert Sum] コマンドをクリックし、メニューから [カウント] を選択します。
12. レポート内で、[Status Symbol] のセルを右クリックし、コンテキスト メニューから [Set as Section] を選択します。
13. メイン ツールバーの [Refresh Data] をクリックして、レポートを実行します。
14. [保存] をクリックします。
このレポートには、[作業中] のステータスが含まれていないリクエストの合計数 (カウント) が表示されます。

例: 姓が「C」で始まるユーザの過去 30 日間のすべてのクローズ リクエストの表示

この例では、クローズ日と顧客の姓のプロンプト値を指定し、これらの値に基づいてすべてのクローズ リクエストが返されるようにします。

例: 姓が「C」で始まるユーザの過去 30 日間のすべてのクローズ リクエストの表示

1. メニュー バーで [新規] - [Web Intelligence Document] をクリックします。
[New Web Intelligence Document] ページが表示されます。

2. [Universe] 列で CA SDM ユニバースを選択します。

Web Intelligence ドキュメントがユニバース情報と共に左側のペインに表示されます。

注: ナビゲーションを向上するには、左側のペインで[添付サービス タイプ] フォルダを閉じます。

3. 左側のペインで [リクエスト] を見つけて展開し、[リクエストの詳細] フォルダを展開します。スクロール バーを使用してフォルダを見つけます。
4. 以下のオブジェクトをそれぞれ選択し、[Results Objects] で左側のペインから右上のペインにそのオブジェクトをドラッグアンドドロップします。
 - 参照番号
 - クローズ日
 - 顧客の姓
 - 概要
5. 以下のオブジェクトをそれぞれ選択し、[Query Filters] で右下のパネルにこれらのオブジェクトをドラッグアンドドロップします。
 - ステータス シンボル
 - クローズ日
 - 顧客の姓
6. [Status Symbol] フィルタの [In list] 矢印をクリックし、[Operand Type] メニューのリストから値を選択します。

[List of Values] ダイアログ ボックスが表示されます。
7. [Status Symbol] リストで以下の値を選択します。
 - クローズ
 - クローズ-未解決
 - クローズ リクエスト
 - 問題はクローズしました
 - 問題 - 修正済み
 - 解決済み

8. 緑の矢印をクリックします。
値が [Value(s) Selected] フィールドに表示されます。
9. [OK] をクリックします。
10. [Query Filters] ペインで、[クローズ日] オブジェクトの [In list] 矢印をクリックし、[Between] 演算子を選択します。
11. [In list] 矢印をクリックし、1つ目および2つ目の [Operand Type] メニューから [プロンプト] を選択します。
12. [Customer Last Name] オブジェクトの [In list] 矢印をクリックし、[Matches pattern] 演算子を選択します。
13. [In list] 矢印をクリックし、[Operand Type] メニューから [プロンプト] を選択します。
14. [In list] 矢印の横に表示される [Prompt Properties] アイコンをダブルクリックします。
[プロンプト] ダイアログ ボックスが表示されます。
15. [プロンプト] テキストフィールドに、顧客の姓のパターンを入力します。
16. [OK] をクリックします。
17. ツールバーの [クエリの実行] をクリックして、レポートを生成します。

注: クローズ日オブジェクトと顧客の姓オブジェクトでは、プロンプト機能が使用されるため、[プロンプト] ダイアログ ボックスが表示されます。このダイアログを使用すると、レポートを生成する前に追加のデータを収集できます。
18. [プロンプト] ウィンドウで、各プロンプトのプロンプト値を以下のように選択または入力します。
 - Enter Close Date (Start) : 今日の日付よりも 30 日前の日付を指定します。
 - Enter Close Date (End) : 今日の日付を指定します。
 - Enter a pattern for Customer Last Name : C% を指定します。
19. [クエリの実行] をクリックして、レポートを生成します。
新しいウィンドウにレポートが表示されます。

20. レポートのタイトルをダブルクリックして、テキストボックスに「姓が「C」で始まるユーザの過去 30 日間のすべてのクローズリクエストの表示」と入力します。フォントサイズは 16 またはそれ以外のサイズに変更できます。
21. レポートのほかの要素を変更するには、[プロパティ] タブをクリックします。
22. [保存] をクリックし、[名前を付けて保存] オプションで場所を指定します。

ダッシュボードレポート

ダッシュボードレポート機能を使用して、**BusinessObjects InfoView** の中ですべての **CA SDM** チケットタイプ（リクエスト/インシデント/問題、変更要求、案件）、ナレッジマネジメント、サポートオートメーション、および **CMDB** に関する日々の業務を監視することができます。各レポートには、アクティブなチケットに従事する上位アナリストに関する分析が含まれているため、各アナリストの進捗状況を監視できます。

ダッシュボードレポート機能では、以下のことを実行できます。

- アクティブなチケットに関する概要および詳細情報を優先度、アナリスト、カテゴリ、またはグループごとに表示できます。
- 一定の期間内に解決されたチケットの数やその他の情報を把握できます。
- レポートを .xls や .pdf. といった他のフォーマットで編集、印刷、追跡、保存できます。

事前定義済みの個別のダッシュボードレポートや、単一のビュー内ですべての **CA SDM** 日常作業を表示する企業ダッシュボードを使用できます。企業ダッシュボードでは、すべてのチケットタイプ（リクエスト/インシデント/問題、変更要求、リクエスト）に関する日々の業務に関する重要な情報を優先度、アナリスト、カテゴリ、またはグループごとに共有できます。

注: ダッシュボードレポート機能を使用する際、「**BusinessObjects InfoView User's Guide**」の「**Working with Dashboard and Analytics**」に記載されている **InfoView** 機能を使用することができます。ユーザガイドにアクセスするには、**InfoView** 内のヘルプアイコンをクリックします。

InfoView でのダッシュボードおよびレポートの表示

管理者アカウントでログオンし、**BusinessObjects InfoView** でレポートを表示することができます。**InfoView** でユーザに表示されるフォルダやレポートは、ユーザがログオンしているアカウント、およびそのアカウントに付与されている権限によって異なります

InfoView でダッシュボードのレポートを確認するには

1. CA SDM にログインします。
2. [レポート] タブで、[InfoView] ボタンをクリックします。
InfoView が Web ブラウザに表示されます。
3. InfoView ツールバーで、[ドキュメント リスト] を選択します。
フォルダとオブジェクトがナビゲーション エリアに表示されます。
4. [パブリック フォルダ] - [CA レポート] - [CA SDM Dashboards] を選択します。
[変更要求]、[インシデント]、[案件]、[問題]、[リクエスト]、[環境設定]、[ナレッジ] の各フォルダが表示されます。
5. 該当するレポートを選択します。
レポートが右側のペインに表示されます。
6. レポートを表示するにはタイトルをダブルクリックします。
レポートが開いて表示されます。

CA Business Intelligence レポートの作成

CA SDM 用の CA Business Intelligence レポートを作成できます。

関連項目：

[CA SDM ODBC ドライバ](#) (P. 1040)

[BusinessObjects レポート用の SQL の作成](#) (P. 1041)

[PDM 関数](#) (P. 1042)

[属性の別名](#) (P. 1045)

[pdm isql による対話的な SQL](#) (P. 1045)

CA SDM ODBC ドライバ

Business Objects レポート アプリケーション（Crystal Reports および Web Intelligence）は、データへのアクセスに、CA SDM オブジェクト エンジン（domsrvr）に直接アクセスする ODBC ドライバを使用します。

この接続には、多くのメリットがあります。

- BusinessObjects レポートで使用される SELECT ステートメントは、オブジェクトや属性への参照に CA SDM 名（Majic 名）を使用します。たとえば、連絡先に関するレポートの SELECT ステートメントは以下のように記述できます。

```
SELECT combo_name FROM cnt WHERE last_name LIKE 'smith%'
```
- CA SDM ODBC ドライバは、combo_name などの属性や cnt などのオブジェクトを、対応する DBMS 名にマップできます。
- データ パーティションおよびテナンシー制限を含むすべての CA SDM セキュリティが自動的にレポートに適用されます。BusinessObjects と CA SDM 間のすべての接続が CA SDM 連絡先に関連付けられます。また、CA SDM ODBC では入力 SELECT ステートメントを編集して、エンドユーザのレポート役割に関連付けられたセキュリティ制限を実施します。BusinessObjects がデータベースに直接接続することはありません。
- CA SDM 属性の別名機能が、CA SDM データベースを「平坦化」（非正規化）します。属性の別名は、CA SDM オブジェクトの追加の属性です。これによって、結合されたテーブルの属性をクエリを使用して明示的な結合なしで参照することができ、ベースのテーブルをレポートビューのように使用できます。
- CA SDM ODBC ドライバは、クエリでの日付のリテラルの使用をサポートしており、CA SDM 内部日付形式の値を標準 DBMS 日付に自動変換します。

重要: CA SDM ODBC ドライバは、BusinessObjects レポート（Crystal および Web Intelligence）に対してのみサポートされます。CA SDM はスタンドアロン ODBC クライアントを提供しておらず、ODBC ドライバを BusinessObjects 以外のアプリケーションで使用することはお勧めしません。

BusinessObjects レポート用の SQL の作成

BusinessObjects レポートで使用するすべての SQL ステートメントは、CA SDM ODBC ドライバによって処理されます。ODBC ドライバは、標準の SQL 92 SELECT ステートメントを、以下の変更および拡張と共にサポートしています。

- CA SDM オブジェクト名が DBMS テーブル名の代わりに使用され、CA SDM 属性名が DBMS 列名の代わりに使用されます。
- CA SDM 属性の別名は、列名が有効である、クエリの任意の位置で使用できます。ODBC ドライバは、属性の別名参照を 1 つ以上の結合に置き換えます。

注: 詳細については、[属性の別名](#) (P. 1045)を参照してください。

- CA SDM DERIVED 属性 (combo_name など) は、選択リストでのみ使用できます。WHERE 節内も含めて、クエリのそれ以外の部分では、サポートされていません。

注: ユニバースには Combo Name With Userid オブジェクトが多数用意されています。たとえば、「管理ガイド」に含まれるアドホック レポートのサンプルでフィルタとして使用されている Customer Combo Name With Userid オブジェクトなどがあります。これらのオブジェクトを使用すると、Web Intelligence での一時的なクエリでコンボ名をフィルタプロンプトとして使用でき、コンボ名を WHERE 節に含められないという制限を回避できます。これらのオブジェクトはフィルタプロンプトにコンボ名とユーザ ID を両方とも提示しますが、生成される SQL クエリでは選択されたユーザ ID のみ使用してください。

- クエリには日付のリテラルを以下のいずれかの形式で含めることができます。

```
d'yyyy-mm-dd hh:mm:ss xm' (xm は am または pm)
ts'yyyy-mm-dd hh:mm:ss'
```

これらのリテラルは、クエリの任意の位置で使用できます。ODBC ドライバは、これらを CA SDM 内部日付形式 (1970 年 1 月 1 日午前 0:00 から起算した秒数) に自動変換します。

PDM 関数

特別な CA SDM 機能やデータ型の動作を支援するため、ODBC ドライバは SQL を拡張して多数のクエリ関数を追加サポートしています。ドライバがサポートしているすべての関数は文字列「Pdm」で始まっており、以下の表に記載されているような PDM 関数として知られています。

PDM 関数	説明
PdmAddDays([date], count)	引数を 1 つ指定した場合、引数に指定されている日数が、本日の日付に加算されて結果が返されます。引数を 2 つ指定した場合、2 番目の引数に指定されている日数が、最初の引数に指定されている日付列の値に加算されて結果が返されます。この関数はクエリの任意の位置で使用できます。
PdmAddMonths([date], count)	引数を 1 つ指定した場合、引数に指定されている月数が、本日の日付に加算されて結果が返されます。引数を 2 つ指定した場合、2 番目の引数に指定されている月数が、最初の引数に指定されている日付列の値に加算されて結果が返されます。引数を 1 つ指定する形式はクエリ内の任意の場所で使用できます。引数を 2 つ指定する形式は選択リスト内でのみ使用できます。
PdmDay([date])	引数なしで使用すると、現在の日付が整数で返されます。引数を 1 つ指定した場合、その引数に指定した日付カラムの値に関連付けられた日付が返されます。引数なしの形式はクエリ内の任意の場所で使用できます。引数を 1 つ指定する形式は選択リスト内でのみ使用できます。
PdmDownTime(slaName , workshift, startDate, endDate)	指定した SLA とワークシフトの条件下で 2 つの日付間のダウンタイムを計算します。この関数は選択リスト内でのみ使用できます。
PdmMonth([date])	引数なしで使用すると、現在の月が 1 ～ 12 の整数で返されます。引数を 1 つ指定した場合、その引数に指定した日付列の値に関連付けられた月が返されます。引数なしの形式はクエリ内の任意の場所で使用できます。引数を 1 つ指定する形式は選択リスト内でのみ使用できます。
PdmMonthName([date])	引数なしで使用された場合は、現在の月をローカライズされた名前（「1 月」、「2 月」など）で返します。引数を 1 つ指定した場合、その引数に指定した日付列の値のローカライズされた名前が返されます。引数なしの形式はクエリ内の任意の場所で使用できます。引数を 1 つ指定する形式は選択リスト内でのみ使用できます。

PDM 関数	説明
PdmDay([date])	引数なしで使用すると、現在の日付が整数で返されます。引数を 1 つ指定した場合、その引数に指定した日付カラムの値に関連付けられた日付が返されます。引数なしの形式はクエリ内の任意の場所で使用できます。引数を 1 つ指定する形式は選択リスト内でのみ使用できます。
PdmSeconds(date)	引数に指定された日付列の値が、1970 年 1 月 1 日午前 0:00 から起算した秒数としての raw 形式で返されます。この関数は選択リスト内でのみ使用できます。この引数は必須です。
PdmString(column)	引数に指定された列の値に相当する文字列が返されます。この関数には UUID 列、日付列、または文字列列を使用できます。この関数は選択リスト内でのみ使用できます。

PDM 関数	説明
PdmToday()	PdmToday() [timeAdj [, day [, month [, year]]]]) 現在の日付（1970 年 1 月 1 日から起算した秒数）を、引数に基づいて調整して返します。 timeAdj : -1 - 時刻が一日の始まり（0:00:00）に合わされます。 +1 - 時刻が一日の終り（23:59:59）に合わされます。 day : 負の値 - 指定した日数で日付が調整されます。 正の値 - 指定した絶対値（と月末のどちらか小さい方）に日が設定されます。 month : 負の値 - 指定した月数で日付が調整されます。 正の値 - 指定した絶対値（と 12 月のどちらか小さい方）に月が設定されます。 year : 負の値 - 指定した年数で日付が調整されます。 正の値 - 指定した絶対値に年が設定されます。 調整は、年、月、日の順で適用されます。0 が指定された引数や省略された引数は無視されます。
PdmYear([date])	引数なしで使用すると、現在の年が 4 桁の整数で返されます。引数を 1 つ指定した場合、その引数に指定した日付列の値に関連付けられた年が返されます。引数なしの形式はクエリ内の任意の場所で使用できます。引数を 1 つ指定する形式は選択リスト内でのみ使用できます。

属性の別名

属性の別名は CA SDM オブジェクトの追加属性で、結合テーブルのデータを Majic ドット結合構文を使用して参照します（構文 `srelname.attrname` は、外部キー `srelname` で参照されるテーブルの属性 `attrname` への参照）。CA SDM リリース 12.9 には事前定義済みの属性の別名が多数用意されており、通常、その名前は対応する Majic 結合と同じで、結合を示すドットが下線に置き換えられています。たとえば、リクエストの担当者に関する情報をリストするレポートについては、以下の SELECT ステートメントが使用されます。

```
SELECT ref_num, assignee_combo_name, assignee_organization_name
FROM cr WHERE customer_last_name LIKE 'smith%'
```

CA SDM ODBC ドライバは必要に応じて結合を自動的に作成して、属性の別名によって参照されているテーブルにアクセスします。CA SDM 管理者役割のユーザは、属性の新しい別名をオンラインで簡単に追加できます。これは、オブジェクトに対応するビューを一度に 1 列ずつ展開する方法になっています。

[属性別名] テーブルにアクセスするには、[管理] タブを選択し、[CA SDM] - [コード] - [属性の別名] を参照します。

pdm_isql による対話的な SQL

コマンドラインユーティリティ `pdm_isql` が CA SDM と共に提供され、SQL SELECT ステートメントの対話式入力が可能になります。`pdm_isql` に入力された SELECT ステートメントは、CA SDM ODBC ドライバに送信され、SQL SELECT ステートメントを BusinessObjects 外でテストできます。

`pdm_isql` を使用するには

1. `$NX_ROOT/bin` がパスに含まれていることを確認します。
2. 以下のコマンドを入力します。

```
pdm_isql
```

3. `pdm_isql` のプロンプトで、以下のコマンドを入力します。
`connect username*password@casd_hostname`
(*username* と *password* は有効な CA SDM ログイン クレデンシャル、*hostname* は Web エンジンを持つ CA SDM サーバ)
4. SQL の `SELECT` ステートメントを入力し、直後にセミコロンを 1 つ指定します。

第 21 章: CA SDM でのレポートの生成

このセクションには、以下のトピックが含まれています。

- [レポートの生成](#) (P. 1047)
- [データベース ビュー](#) (P. 1047)
- [レポート方法のセットアップ](#) (P. 1051)
- [レポート形式](#) (P. 1052)
- [列の並べ替え順の変更](#) (P. 1053)
- [概要レポートと詳細レポート](#) (P. 1053)
- [分析レポート](#) (P. 1054)

レポートの生成

CA SDM には、さまざまなビルトイン レポート機能とオプションが用意されており、以下の操作を実行できます。

- アセットや個々の変更要求、案件、インシデント、問題などのフォームの印刷
- 変更要求、案件、インシデント、問題、リクエスト、構成アイテムのリストの概要レポートまたは詳細レポートの生成
- 分析レポートの生成

注: CA SDM レポートの使用方法については、オンライン ヘルプの「レポートの生成」を参照してください。 CA SDM に組み込まれているレポート機能を使用する以外にも、CA SDM データベースのテーブルやビューに基づくカスタム レポートを作成および生成することができます。カスタム レポートの詳細については、「実装ガイド」を参照してください。

データベース ビュー

CA SDM データベースは、サービス デスクを運用するために入力および使用されるデータのリポジトリです。 CA SDM では、いくつかのデータベース ビューが用意されており、データベースのカスタマイズしたレポートを作成できます。

これらのビューには以下の 2 つのタイプがあります。

- 基本設定
- 詳細設定

関連項目:

[ビューのフィールドの説明](#) (P. 1357)

基本ビュー

基本ビューは **CA SDM** のテーブルに基づいています。基本ビューでは、リクエスト、インシデント、問題、変更要求、案件、アセット、または連絡先/グループが実装で利用されている場合に限り、データが表示されます。

基本ビューを使用すると、以下を含むさまざまなレポートを設計および生成できます。

- リクエスト領域で並べ替えられた、優先度 **1** のオープン リクエストの詳細リストと概要リスト。
- 優先度で並べ替えられた、**24** 時間以上オープンとなっている、レベル **1** グループに割り当てられた変更要求の詳細リストと概要リスト。
- 優先度、割り当てられたグループ、または優先度と割り当てられたグループで並べ替えられた、指定した日数以上オープンとなっている案件の件数。

以下の基本ビューが用意されています。

ビュー名	説明
View_Contact_Full	すべての連絡先（連絡先のタイプ、場所、組織、およびサービス タイプを含む）
View_Contact_to_Environment	すべての連絡先とその環境（アセット）
View_Group	データベースで定義されているすべてのグループ
View_Group_To_Contact	連絡先のグループ割り当て内でのすべての連絡先（マネージャを含む）

ビュー名	説明
View_Request	すべてのリクエスト（サービス タイプ、重大度、緊急度、カテゴリ、アセット、影響度数、名前別の担当者、名前別の顧客、グループ、ステータス、および優先度を含む）
View_Act_Log	リクエスト アクティビティのログ情報（アクティビティのタイプおよびアナリスト名を含む）
View_Request_to_Act_Log	アクティビティ ログを含むすべてのリクエスト（このビューにより View_Request と View_Act_Log が結合されます）
View_Request_to_Properties	リクエストとそのプロパティ（プロパティがリクエストに割り当てられていない場合は特に、すべてのリクエストが表示されるとは限りません）
View_Change	すべての変更要求（ステータス、優先度、カテゴリ、組織、名前別の影響を受けるエンド ユーザ、名前別の依頼者、名前別の担当者、グループ、サービス タイプ、および影響度数を含む）
View_Change_Act_Log	変更要求のアクティビティ ログ情報
View_Change_to_Change_Act_Log	アクティビティ ログを含むすべての変更要求（このビューにより View_Change と View_Change_Act_Log が結合されます）
View_Change_to_Properties	変更要求とそのプロパティ（プロパティが変更要求に割り当てられていない場合は特に、すべての変更要求が表示されるとは限りません）
View_Change_to_Change_WF	変更要求とそのワークフロー タスク（ワークフロー タスクが変更要求に割り当てられていない場合は特に、すべての変更要求が表示されるとは限りません）
View_Change_to_Assets	変更要求とそのアセット（変更要求にアセットがない場合は特に、すべての変更要求が表示されるとは限りません）
View_Change_to_Requests	添付されたリクエストに関する基本情報を含む変更要求（このビューにより View_Change と Call_Request テーブルが結合されますが、リクエストが変更要求に添付されていない場合は特に、すべての変更要求が表示されるとは限りません）

ビュー名	説明
View_Issue	すべての案件（ステータス、優先度、カテゴリ、組織、名前別の影響を受けるエンドユーザ、名前別の担当者、グループ、サービス タイプなどを含む）
View_Issue_Act_Log	案件アクティビティ ログ情報
View_Issue_to_Issue_Act_Log	アクティビティ ログを含むすべての案件（このビューにより View_Issue と View_Issue_Act_Log が結合されます）
View_Issue_to_Properties	案件とそのプロパティ（プロパティが案件に割り当てられていない場合は特に、すべての案件が表示されるとは限りません）
View_Issue_to_Issue_WF	案件とそのワークフロー タスク（ワークフロー タスクが案件に割り当てられていない場合は特に、すべての案件が表示されるとは限りません）
View_Issue_to_Assets	案件とそのアセット（案件にアセットがない場合は特に、すべての案件が表示されるとは限りません）

高度なビュー

高度なビューは、CA SDM の `audit_log` テーブルに基づいています。

注: これらのビューを使用する前に、オプション マネージャで `audit_ins` オプションと `audit_upd` オプションのいずれかまたは両方をインストールして、システムを再起動する必要があります。

高度なビューを使用すると、特定の状態のチケット（つまり、リクエスト、変更要求、または案件）の期間に関するレポートを作成できます。たとえば、以下のようなレポートを作成できます。

- 2002 年 1 月 1 日にオープンされたリクエストに関して、オープンから L2 への割り当てまでの期間を表示する
- 2002 年 1 月 1 日にオープンされた案件に関して、優先度 2 にエスカレートされる前に優先度 3 に置かれていた期間を表示する

以下の高度なビューが用意されています。これらは、CA SDM データベースの `audit_log` テーブルのビューで、特にステータス、優先度、グループ、または担当者の属性に対するクエリを実行します。

ビュー名	説明
View_Audit_Status	時間で並べ替えられたステータス別のすべてのチケット（ステータスを持たないチケットは含まれない）
View_Audit_Priority	時間で並べ替えられた優先度別のすべてのチケット
View_Audit_Group	時間で並べ替えられたグループ割り当て別のすべてのチケット（グループを持たないチケットは含まれない）
View_Audit_Assignee	時間で並べ替えられた個々の割り当て別のすべてのチケット（担当者を持たないチケットは含まれない）

重要： 高度なビューでデータを表示するには、オプション マネージャを使用して、監査ロギング オプションをインストールする必要があります。詳細については、監査オプション `audit_ins` と `audit_upd` に関するオンラインヘルプの説明を参照してください。

関連項目：

[オプション マネージャの使用](#) (P. 557)

レポート方法のセットアップ

レポート方法を使用すると、レポートを選択した場合のレポート結果の送信先を指定できます。例では、[レポート] メニューで使用可能な概要レポートと詳細レポート、および [分析] メニューから利用可能なレポートを示します。定義済みのレポート方法がいくつか用意されており、これらの方法を変更することもできます。

注： レポート方法を定義する方法については、オンライン ヘルプを参照してください。

レポート形式

\$NX_ROOT/fig/cfg (UNIX) または installation_directory¥fig¥cfg (Windows) にある dataent.fmt ファイルを使用すると、印刷するレポートのさまざまなデータ表示形式をカスタマイズできます。このファイルは、任意のテキストエディタを使用して表示および変更できます (Windows では、ワードパッドを使用して編集してください)。

ファイルにある以下の行は、日時の表示形式を制御します。

```
default_date = "long_date"
short_date = "M/D/YY// Enter a date as MM/DD/YY"
long_date = "MM/DD/YYYY// Enter a date as MM/DD/YY"
default_tod = "hour_12"
hour_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
default_date_time = "date_time12"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Enter a date and time as MM/DD/YY hh:mm:ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Enter a date and time as MM/DD/YY 00:00:00-23:59:59"
```

たとえば、ヨーロッパの日時形式に合わせて、これらの行を以下のように変更できます。

```
default_date = "long_date"
short_date = "D/M/YY// Enter a date as DD/MM/YY"
long_date = "DD/MM/YYYY// Enter a date as DD/MM/YYYY"
default_tod = "hour_24"
hour_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
default_date_time = "date_time24"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Enter a date and time as MM/DD/YY hh:mm:ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Enter a date and time as MM/DD/YY 00:00:00-23:59:59"
```

注: pdm_extract を使用して CA SDM データベースから別のシステムにデータをエクスポートし、dataent.fmt ファイルに指定された日付フォーマットを使用してデータを抽出する場合は、pdm_extract を呼び出すときに -d フラグを使用します。

列の並べ替え順の変更

管理者は、Web スクリーン ペインタを使用して、レポートに表示される列の並べ替え順を変更できます。

データは以下の順で並べ替えることができます。

- 昇順（A から Z、0 から 9、または最も古い日付から最新の日付）
- 降順（Z から A、9 から 0、または最新の日付から最も古い日付）

注: 詳細については、Web スクリーン ペインタのヘルプを参照してください。

概要レポートと詳細レポート

CA SDM には、概要と詳細のレポートを作成するための組み込みオプションがあります。リスト ウィンドウの検索機能を使用して、レポートの特定のレコードを選択できます。たとえば、[リクエスト リスト] ウィンドウで検索条件を入力して、レポートの生成に使用できるリクエストのリストを作成できます。

概要レポートと詳細レポートを印刷または表示するには、先にレポートに含めるレコードを選択する必要があります。また、任意の詳細ページで [ファイル] メニューの [フォームの印刷] を選択して、各レコードについて 1 ページの詳細レポートを印刷することもできます。新規に作成したレコードのレポートを印刷するには、最初にレコードを保存する必要があります。

注: レポートの使用方法については、オンライン ヘルプを参照してください。

分析レポート

CA SDM の「管理」タブには、サービス デスク プロセスに関するグローバルおよび詳細な視点の以下のビルトイン分析レポートが用意されています。

- リクエスト レポート/案件レポート
- リクエスト領域レポート/案件カテゴリ レポート
- 優先度別のリクエスト領域レポート/優先度別の案件カテゴリの生成レポート

当日、過去 30 日間、過去 1 年間などの分析レポートを表示できます。

関連項目：

[リクエスト レポートまたは案件レポートの生成 \(P. 1054\)](#)

[リクエスト領域レポートまたは案件カテゴリ レポートの生成 \(P. 1055\)](#)

[優先度別のリクエスト領域レポートまたは優先度別の案件カテゴリ レポートの生成 \(P. 1055\)](#)

リクエスト レポートまたは案件レポートの生成

リクエスト レポートまたは案件レポートでは、オープンしたリクエスト数または案件数、クローズしたリクエスト数または案件数、平均オープン時間、およびクローズまでの平均時間などの統計を、指定した期間について表示できます。このレポートは、日付の古いものから新しいものへ並べ替えられます。

Web インターフェースからリクエストレポートまたは案件レポートを生成する方法

1. 「管理」タブを選択します。
2. 「Service Desk」ノードと「分析」ノードを展開します。
3. 「リクエスト」または「案件」を選択します。
4. 目的の期間に合わせて、適切なレポートを選択します。

リクエスト領域レポートまたは案件カテゴリ レポートの生成

リクエスト領域レポートまたは案件カテゴリ レポートでは、各リクエスト領域または案件カテゴリを対象として、指定した期間にオープンしたリクエスト数または案件数を表示します。このレポートは、リクエスト領域または案件カテゴリを基準にしてアルファベット順に並べ替えられます。

Web インターフェースからリクエスト領域レポートまたは案件カテゴリ レポートを生成する方法

1. [管理] タブを選択します。
2. [Service Desk] ノードと [分析] ノードを展開します。
3. [リクエスト] または [案件] を選択します。
4. 目的の期間に合わせて、適切なレポートを選択します。

優先度別のリクエスト領域レポートまたは優先度別の案件カテゴリ レポートの生成

優先度別のリクエスト領域レポートまたは優先度別の案件カテゴリ レポートでは、各リクエスト領域または案件カテゴリを対象として、指定した期間にオープンしたリクエスト数または案件数を優先度別に表示します。このレポートは、優先度（最高から最低へ）で並べ替えられ、さらにリクエスト領域または案件カテゴリごとにアルファベット順に並べ替えられます。

Web インターフェースから優先度別のリクエスト領域レポートまたは優先度別の案件カテゴリ レポートを生成する方法

1. [管理] タブを選択します。
2. [Service Desk] ノードと [分析] ノードを展開します。
3. [リクエスト] または [案件] を選択します。
4. 目的の期間に合わせて、適切なレポートを選択します。

第 22 章：ナレッジの管理

このセクションには、以下のトピックが含まれています。

[ナレッジ マネジメント](#) (P. 1057)

[ナレッジ マネジメントの手順の検索](#) (P. 1058)

[ナレッジとマルチテナンシー](#) (P. 1059)

[ナレッジベースのセットアップ方法](#) (P. 1059)

[ナレッジベースのドキュメントの使用方法](#) (P. 1062)

[ナレッジ検索](#) (P. 1070)

[REST Web サービスを介して CAFedSearch サブレットを呼び出す方法](#) (P. 1071)

[フォーラム](#) (P. 1072)

[ナレッジ ツリー ドキュメント](#) (P. 1072)

[ナレッジ ドキュメント スケジュール](#) (P. 1073)

[エクスポート/インポートへのアクセス](#) (P. 1084)

[Web サービス](#) (P. 1104)

ナレッジ マネジメント

ナレッジ管理は、ナレッジの検索、分類、および発行という概念のことを指しています。ナレッジ管理では、情報をすばやく効率的に取得して、ユーザまたはグループに提供します。取得して利用可能となった情報は、ナレッジベースと呼ばれます。

ユーザは、検索エンジンを使用してナレッジベースにアクセスします。ナレッジ マネジメントでは、ナレッジベースに格納されているコンテンツを作成および管理できます。グループや役割を使えるように、カテゴリとドキュメントに権限を設定します。ナレッジ マネジメントは、複雑な問題に対する解決策を顧客に提供するうえで便利です。効果的なナレッジ管理では、使いやすく操作しやすいプロセスを通して迅速に解決策を提供できるようになります。

ナレッジを効果的に管理するためには、以下を実行します。

- コンテンツをその内容がわかるように階層化する
- 既存のナレッジの不足部分を特定する
- 更新とメンテナンスを実行してコンテンツの関連性を維持する
- 利用可能なコンテンツの価値を測定する

関連項目：

[役割に基づいた権限への ナレッジ マネジメント データ パーティション
の制約の設定 \(P. 368\)](#)

ナレッジ マネジメントの手順の検索

CA SDM では、このガイド、およびオンライン ヘルプでナレッジ マネジメントの実行手順について説明しています。

オンライン ヘルプでナレッジ マネジメントの実行手順を探す方法

1. CA SDM にログインします。

CA SDM のメイン ページが表示されます。

2. 以下のいずれかの操作を実行します。

- [ヘルプ] をクリックし、メイン メニューの [ヘルプ] からオンライン ヘルプの [管理]-[ナレッジ マネジメント] に移動します。

ナレッジ マネジメントのトピックが表示されます。階層を移動して、必要な情報を探すことができます。

- [ヘルプ] をクリックし、メイン メニューの [このウィンドウのヘルプ] を選択します。

オンライン ヘルプに、目的のページのヘルプ トピックが表示されます。

ナレッジとマルチテナンシー

ナレッジ ドキュメントおよびナレッジ カテゴリは、特定のテナントの専用とすることも、複数のテナントで共有することも、パブリックとして公開することもできます。ナレッジ ドキュメントを検索すると、その結果はチケットに関連付けられているテナントで表示可能なドキュメントに限定されます。FAQ 検索の結果はテナント固有となります。パブリックのテナント ドキュメントの評価は、テナントごとに別々にしておく必要があります。

以下の設定をテナント レベルで管理できます。

- アクション コンテンツ
- ドキュメント テンプレート
- ナレッジ承認プロセス
- 推奨ドキュメント
- ナレッジ マネジメント ROI
- レポート

これ以外のすべての ナレッジ マネジメント システム設定は、サービス プロバイダ レベルでグローバルに管理されます。

注: マルチテナンシーは [管理] タブを使用してオプション マネージャで構成します。

ナレッジ ベースのセットアップ方法

効果的なナレッジ管理とは、単に巨大なナレッジ ベースを構築することだけにとどまりません。関連性のある正確なコンテンツを管理するプロセスと手順を導入することも必要です。

ナレッジ ベースをセットアップするには、以下のタスクを実行します。

1. ナレッジベースの使われ方とその範囲を分析します。
2. 対象の顧客およびその顧客に必要となると想定される情報を検討します。

3. 長期計画を作成して、顧客サポートが必要になると想定される案件を特定します。識別した問題は、ナレッジ ベースに格納する必要のあるコンテンツを決定する場合の指針になります。
4. ナレッジ ベースの構築を実行します。このデータは作成、分類、管理、および保護する必要があります。これらの機能はすべて ナレッジ マネジメント を使用して実行できます。

サンプル ナレッジ データのインポート

Knowledge Broker、HowTo、および Right Answers のサンプル ナレッジ データが用意されており、使用できます。

サンプル ナレッジ データを使用するには、このデータを ナレッジ マネジメント データベースにインポートします。

注: KT サンプル データの詳細については、「[実装ガイド](#)」を参照してください。

ナレッジ ベースの監視

ナレッジ ベースの有効性の監視には、以下のレポート ツールを使用できます。これらのツールを使用すると、ドキュメントの有用性および問題解決時の有効性に関する統計を表示できます。

ナレッジ レポート カード

作成しているドキュメントに関する統計を一覧します。ユーザごとに、個別のナレッジ レポート カードが用意されます。

Web ベースのレポート

ナレッジがユーザのニーズを満たしている度合いを示す、各種のメトリックを確認できます。一般的に使用される機能には、以下のものがあります。

- アクセス頻度の最も高いドキュメントを一覧する
- まったく結果を返さなかったユーザ検索を表示する

ナレッジ ベースのインデックスの再作成

検索設定に以下の変更を加えた場合は、Knowledge Re-index Utility を使ってナレッジベースのインデックスを再作成する必要があります。

- ナレッジのインポート後
- パーサ設定の変更後
- 一括削除後
- 検索障害の発生時

既存のドキュメントはインデックスを再作成されるまで、同義語、ノイズワード、特殊用語、およびほかの検索パラメータに加えられた変更をまったく反映していないため、インデックス再作成が必要となります。すべての新規同義語、ノイズワード、および特殊用語のインデックスを再作成して、ナレッジベースのキーワード検索が最新かつ正確に保たれるようにしてください。

Knowledge Re-indexing はコマンドラインから実行します。
`pdm_k_reindex.exe` が、Knowledge Re-Indexing の実行可能ファイルです。

注: ナレッジベースのドキュメントのインデックス再作成は、データベースのサイズによっては処理に時間がかかる可能性があります。変更を加えた後は、Knowledge Re-Indexing Utility を実行することをお勧めします。

バッチ処理とインスタント処理用のインデックス作成およびインデックス解除のキュー設定

インデックス作成とインデックス解除によってバッチ処理が実行され、1回の実行であらかじめ定義された数のドキュメントが追加されます。このようなバッチ処理は、パフォーマンス最適化のために使用されます。バッチに含まれるドキュメントが多くなると、システムのパフォーマンスが向上します。

処理できるドキュメントの数は制限されています。この制限は、ドキュメントおよびリンクされている添付ファイルのサイズに依存します。ドキュメントのサイズは、純粋なテキストと添付ファイルに基づいて計算されます。イメージとフォーマット要素は計算されません。

注: [管理] タブで [添付ファイル ライブラリ] - [リポジトリ] と移動し、リポジトリを編集して [ファイルの制限サイズ (KB)] を設定すると、添付ファイルのサイズを制限できます。

最大バッチ サイズの推奨値は 2 MB から 12 MB です (NX.env ファイルの EBR_MAX_INDEX_BATCH_SIZE パラメータと平均ドキュメント サイズに従う)。

- 添付ファイルを含むドキュメントの平均サイズが 0.1 MB 程度の場合は、NX.env の以下のデフォルト設定をそのまま使用してください。

```
@EBR_MAX_INDEX_BATCH_SIZE=128
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=1
@NX_EBR_INDEX_QUEUE_ONLINE=Yes
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
```

この設定は、1 回のバッチには 128 ドキュメントが含まれており、バッチの実行間隔が 10 秒、インデックス再作成時の 2 回のバッチ間の待機間隔が 1 秒であることを表しています。

- 添付ファイルを含むドキュメントの平均サイズが 0.5 MB 程度の場合は、NX.env のデフォルト設定をそのまま使用してください。

```
@EBR_MAX_INDEX_BATCH_SIZE=25
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=10
@NX_EBR_INDEX_QUEUE_ONLINE=No
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
```

この設定は、1 回のバッチには 25 ドキュメントが含まれており、バッチの実行間隔が 10 秒、インデックス再作成時の 2 回のバッチ間の待機間隔が 10 秒であることを表しています。

ナレッジ ベースのドキュメントの使用方法

ナレッジ ドキュメントによって、ナレッジ ベースに格納されているナレッジの情報を参照できます。質の高いナレッジの作成には、複数のユーザからの入力が必要となります。各個人は、ナレッジ ドキュメントのライフサイクルの個々のステージの中で、特定のタスクの実行を担当します。ナレッジ ドキュメントはナレッジ ベースに格納され、以下のような進行プロセスの一部として管理されます。

1. ナレッジ ベースに追加するコンテンツを識別します。

2. ナレッジ ドキュメントを作成します。

ナレッジ ドキュメントは、一部の組織が所有者に割り当てるカテゴリに配置されます。

注: ドキュメントを作成または更新すると、所有者の受信トレイに格納されます。受信トレイ内のアイテムは、発行されるまで解決方法として表示されず、ナレッジ ベースにも追加されません。

3. ドキュメントを修正します。

ドキュメントがスコアボードの[受信トレイ]フォルダに到着すると、ユーザは各自に割り当てられた役割に従ってドキュメントを変更し、自分の割り当てタスクを実行できます。

ドキュメントに対してフル（読み取り/書き込み）アクセス権を持つすべてのユーザがドキュメントを変更できます。現在の所有者はドキュメントに対するフルアクセス権を持っていますが、明示的な書き込み許可は必ずしも持っているとは限りません。ドキュメントに問題が見つかった場合、ユーザは新しいバージョンを作成するか、以前のバージョンにロールバックできます。

4. ドキュメントをサブミットします。

ナレッジは、顧客または従業員のセルフサービス インターフェースからサブミットする以外に、**CA SDM** からサブミットできます。このオプションを使用すると、アナリストが既存のチケットから新しい解決方法をサブミットできます。また、この方法の場合は、問題とその解決方法のリンクが作成されるため、似たような問題を抱える別のユーザが解決方法を検索するときにも役立ちます。

5. ドキュメントを発行します。

ドキュメントが承認プロセス サイクルを一巡すると、そのドキュメントを発行できます。発行済みのドキュメントはナレッジ ベースの一部となり、開始日から表示可能となります。この日付のデフォルトは現在の日付です。このドキュメントを表示できるのは、ドキュメントの読み込み権限を付与されているグループのみです。完全なアクセス権のあるユーザの場合は、発行済みのドキュメントを編集できます。

6. 以下のタスクを実行するかどうかを評価して決定します。

- **ドキュメントの発行停止** - ドキュメントの所有者、ナレッジ マネージャ、または管理者は、編集のためにドキュメントを発行停止できます。

- **再作業バージョンの作成** - 完全な編集許可のあるユーザは、発行済みドキュメントをオンラインで表示や検索ができる状態としたまま、そのドキュメントの再作業ドラフトバージョンを作成できます。再作業バージョンはドキュメントのコピーとして開始され、検証および再発行後、ナレッジベースで置き換えられます。
- **ドキュメントの廃止** - ドキュメントの所有者、ナレッジマネージャ、またはシステム管理者は、ナレッジベースからドキュメントを廃止できます。

実行されるタスクおよび各タスクの実行者は、組織内の承認プロセス構造に一致するよう定義できます。

注: ナレッジアクティビティは、連絡先の詳細ページの [イベント ログ] タブからトラッキングできます。たとえば、エンドユーザがナレッジドキュメントを表示すると、イベント ログは更新されて、実行されたアクションとそのドキュメントへのリンクを表示します。さらに、ユーザがドキュメントを開いていた期間もトラッキングします。

CA SDM からのナレッジのサブミット

ナレッジベースへの追加が必要だと考えられるナレッジを入手した場合は、そのナレッジをサブミットして検討できます。セルフサービスインターフェースからナレッジをサブミットする以外に、**CA SDM** からもサブミットできます。アナリストの場合は、既存のチケットから新しい解決方法をサブミットできます。このチケットには、問題とその解決方法のリンクが含まれます。また、似たような問題を抱える別のユーザが解決方法を検索するときにも役立ちます。同時に多数のオープン チケットを設定できる組織では、貴重な時間を節約できます。

すべてのナレッジ ドキュメントは、ナレッジカテゴリに割り当てられている必要があります。**CA SDM** の [インシデント/リクエスト領域] がナレッジマネジメントのナレッジカテゴリに一致すると、そのカテゴリはナレッジのサブミット用に自動的に選択されます。

セルフサービスからのナレッジのサブミット

デフォルトでは、ナレッジ マネジメント にログインしたユーザは誰でも、[ナレッジのサブミット] ページで検討するナレッジをサブミットできます。このページを使い、顧客は、ローカルの **Service Desk** 担当者に連絡することなく、ナレッジをサブミットできます。ナレッジをサブミットすると、そのナレッジは発行プロセスを経て確認と編集が行われ、ナレッジベースに追加されます。

[ナレッジのサブミット] ページに表示されたすべてのフィールドに、情報を入力することが重要です。[概要] フィールドへの入力では特に注意してください。通常、このフィールドには、サブミットするドキュメントの簡潔な概要が記述されます。

ドキュメント属性

ドキュメント属性を設定することは、ご使用のナレッジ プール内のドキュメントを管理するのに役立ちます。ドキュメント属性を更新して、ドキュメントに新しいサブジェクト エキスパートまたは所有者を割り当てることができます。また、ナレッジベースでそのドキュメントが使用可能になる日付および期限切れになる日付を指定できます。別のドキュメント テンプレートを選択して、各ドキュメントのデザインを変更することができます。

ドキュメント権限

ドキュメントに対する権限の設定、表示、および編集ができます。これらの権限は、さまざまなグループに割り当てることができます。権限を設定するにあたって、ドキュメントのプライマリ カテゴリから権限を継承するか、新規の権限を指定するかを決めることができます。デフォルトでは、ドキュメントのプライマリ カテゴリからの権限が継承されます。デフォルトでは、アクセス権限はドキュメント レベルではなくカテゴリ レベルで処理されます。

重要: ナレッジ ドキュメントを作成する場合、ドキュメント権限には後の承認プロセスによってドキュメント上に割り当てることができるユーザーが含まれていることを確認します。グループがドキュメントに割り当てられる場合、そのグループからのユーザーにはドキュメントを表示する権限がない場合があります。ドキュメントが特定のユーザーに割り当てられている場合、デフォルトのデータ パーティションの制約によって、そのユーザーはドキュメントを表示できます。

解決方法の編集

ナレッジ マネジメント でナレッジ ドキュメントを作成するときは、HTML エディタを使用できます。この機能を使用すると、ナレッジ ドキュメントの [解決方法] フィールドを **WYSIWYG (What You See Is What You Get)** 形式で変更できます。HTML エディタを使用すると、HTML コードを入力することなくドキュメントを作成したり、テキストをフォーマットしたり、グラフィックやテーブルを挿入したり、ほかのドキュメントへのリンクを作成したりできるため、作成プロセスが改善されます。このことによって作成プロセスが短縮され、さらに分類のためにドキュメントを編集することも容易になります。

HTML エディタでは以下の操作が実行できます。

- **HTML コードの表示** - HTML エディタ ツールバーの [デザイン モード] タブおよび [ソース モード] タブを使用すると、異なるビューを切り替えることができます。
- **テキストのフォーマット** - [HTML エディタ] ウィンドウにドキュメントのテキストを直接入力できます。このテキストは、ツールバーおよびメニュー オプションを使用して後からフォーマットできます。
- **グラフィックの挿入** - イメージ ライブラリからイメージを選択するか、独自のグラフィックをアップロードして、HTML テキストにグラフィックを挿入できます。
- **テーブルの挿入** - ナレッジ ドキュメントでは、大量の情報を整然と表示させることができます。テーブルを使用すると、そのような情報を行と列に簡潔に表示できます。

- **ほかのドキュメントへのハイパーリンクの挿入** - ナレッジ ドキュメントの作成時または変更時に、ナレッジ ドキュメントにハイパーリンクを挿入できます。このようにして、ほかの関連ドキュメントまたは URL にナレッジ ドキュメントをリンクできます。HTML エディタを [デザイン モード] で使用すると、ハイパーリンクは下線付きの青いテキストとして表示されます。
- **アクション コンテンツの挿入** - アクション コンテンツ (ライブ アクション URL) をナレッジ ドキュメントの [解決方法] フィールドに挿入できます。このアクション コンテンツをエンドユーザーがクリックすると、インシデントが作成されたり、何らかのアクションが実行されます。

ドキュメントの発行準備

ナレッジ ドキュメントをサブミットした後は、属性と権限を設定して発行の準備をします。設定やカテゴリのようなコントロールを割り当てることは、ドキュメントを効率的に分類するために重要です。

関連項目:

[ナレッジ ベースのドキュメントの使用方法](#) (P. 1062)

[ドキュメント属性](#) (P. 1065)

[ドキュメント権限](#) (P. 1065)

ドキュメントの発行

ドキュメントが承認プロセス サイクルを一巡すると、そのドキュメントを発行できます。発行済みのドキュメントはナレッジ ベースの一部となり、開始日から表示可能となります。この日付のデフォルトは現在の日付です。このドキュメントを表示できるのは、ドキュメントの読み込み権限を付与されているグループのみです。

ナレッジ ドキュメントがいったん発行されると、通常、ユーザはドキュメントを変更できなくなります。変更できるようにするには、最初にドキュメントを発行停止します。この間、ナレッジ ドキュメントはオフラインになり、ユーザからは参照できなくなります。ドキュメントの所有者、ナレッジ マネージャまたはシステム管理者は、[リワーク] ボタンおよび[発行停止] チェック ボックスを使用して、ドキュメントを発行停止することができます。ドキュメントを発行停止すると、そのドキュメントは[ドラフト] ステータスに戻ります。管理ユーザは、ワークフロー プロセスの次の手順を選択できます。

ドキュメントのバージョン管理

ナレッジ マネジメント のドキュメント バージョニング機能を使用すると、編集権限を持つアナリストはドキュメントの再作業ドラフト バージョンを作成できます。再作業バージョンはドキュメントのコピーとして開始され、検証および再発行後、ナレッジ ベースで置き換えられます。最初にドキュメントを発行停止する必要はありません。

編集権限を持つユーザは、以下のバージョン管理タスクも実行できます。

- ドキュメントのドラフト バージョンを保存します。
- 現在のバージョンで問題が見つかった場合は、以前のバージョンのドキュメントにロールバックします（ドラフトまたは発行済み）。[ドキュメントの更新] ページの[バージョン] タブで、ロールバックする別のバージョンを選択し、現在のバージョンと置き換えることができます。
- ナレッジ ベースで保存、削除、およびアーカイブされたドキュメント バージョンの番号を追跡する。

CA SDM Scoreboard の[ナレッジ ドキュメントの受信トレイ] は、保存され割り当てられたドキュメントや、再作業ドラフト ドキュメントなど、すべてのステータスのドキュメントに対するリポジトリです。

ドキュメント バージョンの管理方法

管理者は以下のステップを実行して、ドキュメント バージョンをセットアップして管理できます。

1. 発行済みドキュメントを編集して再作業ドラフト バージョンを作成できるユーザを確認します。各連絡先レコードに使われている役割で編集権限を制御します。

2. 承認プロセス テンプレートを定義し、ドキュメントのライフサイクルで完了するタスクやステップをグループ化します。 デフォルトでは、ビルトイン承認プロセス テンプレートでドキュメントを作成できます。
3. ドキュメント承認プロセスを使用するかどうか決定します。 承認プロセスを省略することが許可されているアナリストは、再作業ドラフトバージョンを作成するとき、どのタスクから開始するかを指定できます。
4. ドキュメント バージョン保守用にアーカイブとパージのルールを作成します。

ドキュメントの有効期限

通常、発行したドキュメントは、有効期限になるとリタイアされます（つまり、ドキュメントは、ナレッジベースおよび承認プロセスから削除されます）。

ドキュメントのアーカイブとパージ

ナレッジプールのサイズは、アーカイブとパージ機能を使って管理できます。この機能では、古くなって使用されていないドキュメントが自動的に削除されます。アーカイブとパージ機能では、現在のドキュメントのみが返されるようになるため、ナレッジ検索の効率が向上します。

アーカイブとパージはバックグラウンドプロセスとして実行され、構成したルールに従って **CA SDM** データベースの非アクティブ レコードを自動的に削除します。これらのルールは、一定の時間間隔で **CA SDM** オブジェクトに作用します。

ナレッジ検索

ナレッジマネジメント では、以下の方法でナレッジを取得できます。

カテゴリ参照

カテゴリから解決策を検索します。各カテゴリで追加のサブカテゴリを使用すると、案件に最も関連性が高いと考えられるいくつかの解決策に検索結果を絞り込むことができます。

注: カテゴリを使用してナレッジ ドキュメントを検索する場合、検索結果には、ドキュメントのリストと共に検索に使用されたキーワード数が表示されます。丸かっこ内の数は、キーワードが少なくとも 1 つ含まれるナレッジ ベースのドキュメントの総数です。たとえば、「live assistance」という文字列を検索する場合に、3 つのドキュメントのそれぞれにそのキーワードが少なくとも 1 つ含まれている場合は、「live assistance(3)」と表示されます。

カウントは、指定した検索条件に従ってフィルタされません。そのため、リストに表示されるドキュメント数と一致しない場合があります。また、カウントには、pdm_k_reindex によって処理されたドキュメントのみが含まれます。そのため、指定した文字列が含まれても、直近の pmd_k_reindex の後に発行されたドキュメントはカウントに含まれません。

かっこ内のカウントをオフにするには、以下を \$NX_ROOT/NX.env ファイルに追加します。

```
@EBR_SHOW_WORDS_DF=No
```

ナレッジ ツリー

一連の質問を通して関連性のある解決策を探します。質問に対する回答を基に、最も関連性が高いと考えられる解決策を入手します。

ブックマーク

ブックマーク リストに含まれている頻繁に表示されたドキュメントにアクセスできます。

REST Web サービスを介して CAFedSearch サブレットを呼び出す方法

CAFedSearch サブレットでは、検索クライアントが検索リクエストを送信できる RESTful インターフェースが表示されます。このサブレットには、顧客が独自の検索エンジンを統合できるようにするプラグインアダプタが含まれます。

RESTful インターフェースは、OpenSearch 形式を使用して HTTP Collection GET リクエストを受け入れます。

次の手順に従ってください:

1. REST アクセス キーを取得するには、ログイン認証情報と共に `rest_access` リソースに対する HTTP POST リクエストを送信します。
2. REST アクセス キーを使用して BOPSID トークンを取得するには、`bopsid` リソースに対する HTTP POST リクエストを送信します。詳細については、「*管理者ガイド*」の「*Web サービス メソッド*」を参照してください。

また、以下の場所でサンプル ファイルを参照できます。

```
NX_ROOT¥samples¥sdk¥rest¥java
```

統合検索 API を使用して検索を実行します。検索リソースに対する HTTP GET リクエストを送信し、CA SDM URL を通して検索条件および BOPSID トークンを渡します。詳細については、「*管理ガイド*」を参照してください。

フォーラム

フォーラムを使用すると、既存の案件について意見を交換できます。フォーラムを使用すると、ドキュメントをグローバルに共有できます。また、既存の課題に関しナレッジ共有やブレインストーミングを一緒に行う事前定義済みのグループ間で、ドキュメントを共有できます。

フォーラムにより、一般的な質問や使い勝手のヒントなどに関する意見交換が可能になり、ナレッジの貢献範囲が広がります。新しいフォーラムは、[ナレッジ] タブおよび **Service Desk** チケットから作成できます。

ナレッジ ツリー ドキュメント

ナレッジ ツリー デザイナは、ナレッジ ツリーをすばやく簡単に作成するためのビジュアル ツールです。ナレッジ ツリーは、特定分野の専門家の知識を表すものです。ナレッジ ツリー デザイナを使用すると、アナリストおよびナレッジ エンジニアは、解決方法が見つかるまで一連の質問と考えられる回答をユーザーに提供する詳細なツリーを作成できます。このツールによって、専門のスク립ティング スキルやプログラミング スキルが不要になり、アナリストはサブジェクト エキスパートと協力してツリー デザインの作成に専念できます。

ナレッジ ツリーはデザインが複雑になる場合があります。このため、図を作成してデザインをマップしてから、ナレッジ ツリーを作成することをお勧めします。この図には、一連の質問、考えられる応答、および関連付けられた解決方法を含める必要があります。作成する図に含まれる質問と応答の階層は、ナレッジ ツリーを作成するときの出発点になります。

ナレッジ ツリーの図にマップしたら、ナレッジ ツリー デザイナを使用してツリーを作成します。

ナレッジドキュメント スケジュール

ナレッジドキュメント スケジュールには変更マネージャ、ナレッジマネージャ、およびレベル 2 アナリストが用意されており、ナレッジマネジメント ライフサイクルにおける主要イベントの上位レベルのビューを提供します。以下のイベントはナレッジドキュメント用にスケジュールすることができます。

- サブミット
- 発行
- レビュー
- 有効期限

[ナレッジマネジメント スケジュール] タブでは、[変更カレンダー] タブのカレンダと類似のフォーマットでカレンダーを表示させることができます。ただし、開始時刻と終了時刻が表示される代わりに、特定の日付だけが表示されます。

マクロ ステートメントの設定については、[「ビューのスケジュールの構成」](#) (P. 918)を参照してください。

ナレッジドキュメント スケジュールも iCalendar フォーマットにエクスポートできます。

注: いくつかのカレンダ プログラムにスケジュールをエクスポートする場合、[保存] の代わりに [オープン] オプションを選択すると、ファイルは正しくインポートされません。ナレッジマネジメント スケジュールおよび変更要求スケジュールにおけるこの問題を回避するには、[オープン] オプションではなく、[保存] オプションを選択します。エクスポート済みファイルを保存した後、カレンダ プログラムのインターフェースを介してインポートします。

ナレッジ スケジュール フィルタ

ナレッジ スケジュール フィルタには以下のフィールドが表示されます。

テナント

テナントによる検索をフィルタします。このフィールドは、マルチテナンシー インストール環境における特権ユーザに対して表示されます。

イベントタイプ

以下のイベントタイプによる検索をフィルタします。

- サブミット
- レビュー
- 発行
- 廃止

スケジュール開始日

指定された時間フレームに対するエントリのみを表示させるために、履歴をフィルタする範囲の先頭の日を指定します。

スケジュール終了日

指定された時間フレームに対するエントリのみを表示させるために、履歴をフィルタする範囲の最後の日を指定します。

スケジュール タイムゾーン

検索結果を表示するタイムゾーンを指定します。

注: タイムゾーンを選択していない場合、イベントは現在のタイムゾーンで表示されます。

所有者

ドキュメントを管理する担当者名を指定します。担当者名を「姓、名」のフォーマットで入力するか、または[連絡先の検索]ダイアログ ボックスを開いて、担当者を特定し選択します。

担当者

レコードを処理する担当者名を指定します。担当者名を「姓、名」のフォーマットで入力するか、または[連絡先の検索]ダイアログ ボックスを開いて、担当者を特定し選択します。

サブジェクト エキスパート

ドキュメントの内容についての専門知識を持つ担当者名を指定します。担当者名を「姓、名」のフォーマットで入力するか、または[連絡先の検索]ダイアログ ボックスを開いて、担当者を特定し選択します。

ステータス

検索を実行するには、以下のドキュメント ステータスのうちの 1 つを選択します。

- ドラフト
- 発行済み
- 廃止済み

カテゴリ

取得したドキュメントをフィルタ処理するカテゴリを定義します。

〔カテゴリ〕 ボックスにカテゴリの名前を入力するか、または〔カテゴリの検索〕 ウィンドウを開きます。〔検索〕をクリックすると、指定したカテゴリに関連付けられたドキュメントのみが返されます。

初期ビュー

確認が必要なナレッジマネジメント カレンダのビューを以下から選択します。

月

〔開始日〕 フィールドで指定された最も初期の実装開始日を含む月のひと月分のカレンダーが表示されます。 カレンダーには、範囲内の各変更に関する概要情報（変更番号、開始時刻と終了時刻、および最初に影響を受ける構成アイテム）が表示されます。

週

〔開始日〕 フィールドで指定された最も初期の実装開始日から始まって、7 つの連続する日が 1 つの列に表示されます。 カレンダーには、指定した範囲内の各変更に関する概要情報（変更番号、開始時刻と終了時刻、概要説明、担当者、グループ、および最初に影響を受ける 10 個の構成アイテム）が含まれます。

日

〔開始日〕 フィールドで指定された曜日のみが表示される以外は、〔週〕 ビューに似たビューが表示されます。

n 日間

指定された日数分連続する以外、〔週〕 ビューに似たビューが表示されます。

リスト

標準的な CA SDM のリスト ページが表示されます。

注: [詳細] アイコンをクリックすると、[その他の検索引数] フィールドを表示することができます。このフィールドは、SQL や Majic の知識を持つエキスパート ユーザのみを対象としています。このフィールドでは、標準の検索フィルタ フィールドでは使用できない検索引数を指定できます。このフィールドに SQL WHERE 節を入力して、追加の検索引数を指定できます。

[ナレッジ スケジュール]ビュー

[ナレッジ ドキュメント スケジュール]には、以下のビューがあります。

月

[スケジュール開始日] フィールドで指定された最も初期の実装開始日を含む月のひと月分のカレンダーが表示されます。カレンダーには、範囲内の各変更に関する概要情報（変更番号、開始時刻と終了時刻、および最初に影響を受ける構成アイテム）が表示されます。

ナレッジ ドキュメント スケジュールには、以下の例外を除き、[Change Orders Month] ビューに似た機能があります。

- ナレッジ イベントには、日付（時間なし）だけが含まれます。また、イベント タイプは、期間および変更タイプごとにグループ化される変更要求と同様に、ナレッジ イベントをグループ化します。
- イベント タイプには、schedGroup マクロにより、以下の事前定義済みのデフォルトの色が決められています。
 - サブミット - 黒
 - レビュー - 緑
 - 発行 - 青
 - 廃止 - 赤

注: 過去のレビュー日が見つかる場合は、レビューが行われなかったことを示しています。

週

〔スケジュール開始日〕フィールドで指定された最も初期の実装開始日から始まって、7つの連続する日が1つの列に表示されます。カレンダーには、指定した範囲内の各変更に関する概要情報（変更番号、開始時刻と終了時刻、概要説明、担当者、グループ、および最初に影響を受ける10個の構成アイテム）が含まれます。

日

〔スケジュール開始日〕フィールドで指定された曜日のみが表示される以外は、〔週〕ビューに似たビューが表示されます。

n 日間

指定された日数分連続する以外、〔週〕ビューに似たビューが表示されます。

リスト

標準的な CA SDM のリスト ページが表示されます。

スケジュールビューの環境設定

月次または週次のスケジュールビューを設定するには、スケジュールを定義する HTML フォームの <head> セクションで `pdm_macro` ステートメントを指定します。このフォームを編集するには、Web スクリーン ペインタのソースビューを使用することをお勧めします。

スケジュールを表示するフォームには以下が含まれている必要があります。

- `schedConfig` マクロ
- 少なくとも1つの `schedAttr` マクロ
- 少なくとも1つの `schedGroup` マクロ

環境設定マクロは独立したソースファイルに保存し、メインソースファイル内の `pdm_include` ステートメントで参照します。独立したファイルに保存することにより、メインソースファイルを変更せずに、スケジュールを設定できます。

たとえば、変更カレンダー フォーム `list_chgsched.html` の環境設定マクロを `list_chgsched_config.html` というファイルに保存します。ナレッジライフサイクルスケジュールでは、同じマクロを使用して `list_kdsched_config.html` を変更します。

list_chgsched_config.html と list_kdsched_config.html は以下のディレクトリにあります。

\$NX_ROOT¥bopcfg¥www¥html¥web¥analyst¥

schedConfig マクロ - スケジュールの環境設定

schedConfig マクロでは、フォームにスケジュールが含まれていることを明示し、基本的な環境設定情報を提供します。有効なマクロ引数の値は以下のとおりです。

autosearch=1|0

現在選択されている期間以外のビューをユーザが選択したときに、スケジュールフォームでサーバからデータを再ロードするかどうかを指定します。値を 1（デフォルト）に設定すると、ユーザが検索フィルタの日付選択範囲から 1 日以上外れたビューを選択したときに、フォームで検索が自動的行われます。値を 0 に設定すると、検索を開始するにはユーザが「検索」ボタンを押す必要があります。

defaultView=0|1|7|30|99

0（リスト）、1（日次）、7（週次）、30（月次）、または 99（n 日）で、検索フィルタのデフォルトのビューを指定します。

defaultView 用の指定は、検索フィルタの初期表示のみに影響します。スケジュールを表示した後、CA SDM は、自動的にフィルタ ビューの選択と現在のビューを連携させます。

デフォルト：30

firstday=0|1|2|3|4|5|6|7

0（日曜）と 6（土曜）の間の数値で月次ビューの最初の曜日を指定します。

デフォルト：0

export=xxx|0

iCalendar 形式でのエクスポートで使用するテンプレートのコード名を指定します。値を 0 に設定すると、エクスポートの機能とボタンが無効になります。

デフォルト：ChangeSchedule

legend=1|2|0

スケジュール上のグループの名前と形式を表す凡例の場所を指定します。値を **1** に設定すると、スケジュールの上に凡例が表示されます。**2** に設定すると、スケジュールの下に凡例が表示されます。凡例を表示しない場合は、値を **0** に設定します。

デフォルト : 2

maxGroups=0/n

カレンダーの月次ビューの **1** つのセルに表示するグループの最大数を指定します。

1 日に対して **maxGroups** を超えるグループがスケジュールされている場合、**CA SDM** には **maxGroups** から **1** を引いた数のグループのみが表示され、最後のグループが [あと **nn** 件の変更] ハイパーリンクに置き換わります。ユーザは、このハイパーリンクにマウスオーバーするかクリックして、グループの一覧を参照できます。値を **0** に設定すると、この機能は無効になり、カレンダーのセルに表示されるイベントの数は無制限になります。

デフォルト : 4

nday=(n,n,...)

n 日ビューのドロップダウン リストの選択肢を指定します。

ドロップダウン リストで表示する日数のリストを指定します。**0** を指定すると、**n** 日ドロップダウン リストはスケジュールに表示されなくなります。指定した最初の値がドロップダウン リストのデフォルト値になります。

デフォルト : (3,7,14,28)

round=(hr,min)|0

変更要求やナレッジ ドキュメントをグループにまとめるときにスケジュールの開始日と終了日の丸めを行うかどうかを指定します。丸めを行わない場合は **round=0** を指定します。

デフォルトでは、スケジュールの開始日と終了日でオブジェクトはグループ化されます。**CA SDM** の日付にはすべて時間が含まれます。丸めを行わない場合、**1** 分でも違っていると別のグループに分類されます。丸めを指定すると、開始日を前の時間または分に調整したり、終了日を後の時間または分に調整したりしてグループ化が行われます。

丸めの値には、時間または分のどちらかを指定します（両方は指定できません）。たとえば以下のように、指定した値の最も近い倍数に時間は丸められます。

round=(0,15) 毎時 0 分、15 分、30 分、45 分のうち、最も近い時間に丸められます。

round=(0,30) 毎時 0 分、30 分のうち、最も近い時間に丸められます。

round=1 最も近い正時に丸められます。

round=12 午前 12 時と午後 12 時のうち、最も近い半日に丸められます。

round=24 最も近い日に丸められます。

デフォルト : (0,15)

timefmt=24hr|([am],[pm])

スケジュールのカレンダー ビューの時間形式を指定します。

デフォルト値は 24hr で、24 時間形式 (0:01 ~ 23:59) で時間を表示します。ほかの値 (am、pm) は、午前/午後のどちらかまたは両方を示すサフィックスを付けることを指定します。

注: schedConfig 引数はすべてオプションです。

schedAttr マクロ - 保存済みの属性の指定

schedAttr マクロでは、リストで選択した各項目の保存済みの属性を指定します。保存済みの属性は、月次ビューではポップアップ情報、月次ビュー以外のビューでは詳細情報または概要情報として使用できます。また、JavaScript 関数の setSchedEvents() で使用できます。有効なマクロ引数の値は以下のとおりです。

attr=xxxx

(必須) 変更要求やナレッジドキュメントなどのスケジュール上のオブジェクトの属性を指定します。ドット付きの属性を使用できます。属性名キーワードの CInn を変更カレンダーで使用すると、保存済みの情報を持つ、変更要求に関連付けられた最初の nn 件の CI を含むことを指定できます。

注: この引数は、schedAttr マクロで唯一の必須の引数です。

attrRef=.COMMON_NAME|xxxx

SREL 属性のために保存された参照テーブルの属性を保存します（非 SREL 属性は無視されます）。指定する属性名の先頭にはドットを付ける必要があります。

デフォルト：.COMMON_NAME

label=

n 日ビューに属性のラベルを表示します。

デフォルト：属性の Majic DISPLAY_NAME

ident=1|0

属性がオブジェクトの識別子（変更要求の参照番号など）かどうかを指定します。識別子属性は、ポップアップ情報や n 日ビューで、グループ名の前にラベルなしで表示されます。

デフォルト：0

detail=1|0

月次ビュー以外のビューの詳細情報に属性を表示するかどうかを指定します。詳細情報は、ビューの [概要のみ] チェック ボックスがオフのときに表示される情報です。

デフォルト：1

hoverInfo=1|0

月次ビューでグループ上にマウス ポインタが置かれた場合や、グループにフォーカスがあるときにユーザが Alt + 右方向キーを押した場合に、属性をポップアップ情報に表示するかどうかを指定します。

デフォルト：0

summary=1|0

月次ビュー以外のビューの詳細情報に属性を表示するかどうかを指定します。詳細情報は、ビューの [概要のみ] チェック ボックスがオフのときに表示される情報です。

デフォルト：0

注: CASDM では、属性は、schedAttr マクロと同じ順序で概要情報、詳細情報、またはポップアップ情報に表示されます。

schedGroup マクロ - イベントグループの指定

schedGroup マクロでは、項目グループの名前とカラーコードを指定します。月次ビューでは、1つのイベントにグループのすべての項目が集約されます。月次ビュー以外のビューでは、各項目が属するグループの形式で個別の項目が表示されます。有効なマクロ引数の値（オプション）は以下のとおりです。

grpname=xxx

（必須）グループの名前を指定します。マクロは自動的にグループの番号を割り当て、その番号を **schedGroup_xxx** という名前の JavaScript 変数に割り当てます。**xxx** はグループの名前になります。この変数は、グループに属するイベントを作成するために **setSchedEvents()** 関数で使用されます。

注：この引数は、**schedGroup** マクロで唯一の必須の引数です。

label=xxx

グループのラベルを指定します。値を指定すると、すべてのビューでラベルが表示されます。

legend=xxx|0

スケジュールの下部に表示される凡例にグループの説明を表示します。現在のビューにグループが1件でも存在すると、凡例にグループの説明が表示されます。0を指定すると、グループは凡例から常に除外されます。

デフォルト： 0

color=black|color

このグループの項目のテキストの色を指定します。**color** は、CSS 形式（有効な Web カラー名または # で始まる 16 進数値のどちらか）で指定できます。

例：赤の場合、「#FF0000」または「red」と入力します。

デフォルト： black

bgcolor=white|color

このグループの項目の背景色を指定します。**bgcolor** は、CSS 形式（有効な Web カラー名または # で始まる 16 進数値のどちらか）で指定できます。

例：赤の場合、「#FF0000」または「red」と入力します。

デフォルト： white

`style=normal|bold|italic`

このグループのテキストのスタイルを、**normal**（通常）、**bold**（太字）、**italic**（斜体）から指定します。

デフォルト：normal

setSchedEvents() JavaScript 関数

setSchedEvents() JavaScript 関数はスケジュールのイベントを作成します。新しいグループ オブジェクトを表示する場合は、この関数を変更します。事前定義されたグループ オブジェクトがデフォルトで表示されます。

CA SDM では、スケジュール検索フィルタで選択されたオブジェクト（変更要求またはナレッジドキュメント）ごとに 1 回ずつ **setSchedEvents()** が呼び出されます。この関数は、2 番目の関数 **schedEvent()** を呼び出してイベントのグループ ID、開始日、および終了日を渡し、オブジェクトのイベントを作成します。

setSchedEvents() 関数では、1 つのオブジェクトに対して任意の数のイベント（ゼロを含む）を作成できます。変更カレンダー（[list_chgsched.html](#)）のデフォルトの **setSchedEvents()** 関数は、変更要求ごとに 1 つのイベントを作成し、変更タイプ別に変更要求をグループ化します。この関数は、以下のようにコード化されます。

```
1.      function setSchedEvents( chg )
2.      {
3.          var grpnum;
4.          switch( chg["chgtype"] - 0 ) {
5.              case 100: grpnum = schedGroup_std; break;
6.              case 300: grpnum = schedGroup_emer; break;
7.              default: grpnum = schedGroup_norm; break;
8.          }
9.          chg.schedEvent( grpnum, chg["sched_start_date"], chg["sched_end_date"] );
10.     }
```

case パラメータには、変更タイプ ID を指定します。case ID を一覧表示するには、「変更タイプの作成」を参照してください。

この関数には、`schedAttr` マクロによって指定された属性を含む JavaScript オブジェクトの引数が 1 つ指定されています。行 4 から 8 の `switch` ステートメントでは、変更要求の `chgtype` 属性を確認し、前述の `schedGroup` マクロによって定義された `schedGroup_xxxx` 変数の 1 つから適切なグループ番号を割り当てます。行 9 では、`schedEvent()` 関数が呼び出され、以前割り当てたグループ番号およびスケジュールの開始日と終了日が渡されて、スケジュールにイベントが作成されます。開始日と終了日は、事前に `schedAttr` マクロで指定されているため、引数オブジェクトにあります。

エクスポート/インポートへのアクセス

ナレッジエクスポート/インポート ツールは、異なる ナレッジ マネジメント システム間でデータをマイグレートおよび同期できるほか、ナレッジ ドキュメントのエクスポートやインポートが可能です。このツールを使用して、エクスポート/インポート トランザクションを定義します。

注: マルチテナンシーがインストールされている場合、前のシステムからインポートされたテナント カテゴリおよびパブリック カテゴリはすべて新しいマルチテナンシー システムにパブリックとして表示されますが、インポートされたドキュメントはテナント固有となることがあります。

KEIT ページにアクセスするには、[管理] タブで、[ナレッジ] - [ドキュメント] - [エクスポート/インポート] を参照します。

[エクスポート/インポート] が表示され、以下の要素があります。

エクスポートトランザクション

エクスポートのリストが表示されます。

エクスポート/インポートテンプレート

編集できるテンプレートのリストを表示します。

インポート

インポートに使用できるパッケージのリストが表示されます。

インポートトランザクション

インポートのリストが表示されます。

注: Web インターフェースでナレッジをインポートまたはエクスポートする場合、ナレッジマネジメント ではデフォルトのコマンドライン ユーティリティ役割が使用され、ユーザが **CA SDM** にログインしている現在の役割は使用されません。デフォルトのコマンドライン ユーティリティ役割は、ユーザのアクセス タイプに設定されます。

ナレッジのエクスポート/インポート方法

エクスポート/インポート テンプレートでは、エクスポート/インポート トランザクションを定義できます。

次の手順に従ってください:

1. 以下のいずれかの手順を実行します。
 - エクスポート/インポート テンプレートを作成して、エクスポート パッケージを作成する。
 - 既存のエクスポート/インポート テンプレートを使用して、エクスポート パッケージを作成する。
2. 以下のいずれかの手順を実行して、別のシステムにデータをエクスポートします。
 - 標準設定で、[エクスポート/インポート テンプレートの詳細] ページの [エクスポート] をクリックします。
 - 高可用性設定では、Web インターフェースを使用してアプリケーション サーバからパッケージをエクスポートすることはできません。任意のサーバからパッケージをエクスポートするには、**pdm_ket** ユーティリティを使用します。
 - [エクスポート トランザクション] ページで、トランザクションを右クリックしてショートカット メニューの [再試行] をクリックします。
 - [pdm ket ユーティリティを使用する。](#) (P. 1100)

3. CA SDM の設定に応じて、以下のいずれかのアクションを実行して、パッケージからナレッジデータをインポートします。

- 標準設定で、デフォルトの `$NX_ROOT/site/keit/export` ディレクトリから目的のナレッジパッケージをコピーし、`$NX_ROOT/site/keit/import` ディレクトリに配置する。[ナレッジインポートパッケージリスト] ページでナレッジパッケージを右クリックし、ショートカットメニューから [インポート] をクリックします。
- 高可用性設定で、*UNC Shared Location*/export ディレクトリから目的のナレッジパッケージをコピーし、*UNC Shared Location*/import ディレクトリに配置する。Web インターフェースを使用してアプリケーションサーバからパッケージをインポートすることはできませんが、`pdm_kit` ユーティリティを使用すると、任意のサーバからパッケージをインポートできます。
- 対象の CA SDM インストール環境にナレッジパッケージをコピーして、`$NX_ROOT/site/keit/import` ディレクトリに配置する。
- [ナレッジインポートパッケージリスト] ページでナレッジパッケージを右クリックし、ショートカットメニューから [インポート] をクリックします。
- [インポートトランザクション] ページで、トランザクションを右クリックしてショートカットメニューの [再試行] をクリックする。
- [pdm_kit_txt ユーティリティを使用する。](#) (P. 1101)

注: ナレッジパッケージ名が [ナレッジインポート] ページに表示されるようにするには、名前にプレフィックスとして「`package_`」を付ける必要があります。

重要: r11.0 インポートユーティリティは名前が `pdm_kit_txt.exe` に変更され、r11.0 のテキストファイルをインポートできます。このユーティリティでは、r12.0 のインポート機能拡張はサポートされていません。

関連項目:

[パッケージのエクスポート/インポート](#) (P. 1089)

エクスポートトランザクション

パッケージ、テンプレートおよびステータスごとに、トランザクションを並べ替えることができます。KEIT トランザクションはすべて、以下のログファイルに記録されます。

stdlog

CA SDM 情報がログに記録されます。

keitstat.log

KEIT 操作に関する統計情報を示します。

keitinfo.log

KEIT 操作に関する詳細情報を示します。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナント データから除外するか、テナント データに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

[エクスポート トランザクション] ページには以下のフィールドがあります。

パッケージ

エクスポート パッケージ名が表示されます。

実行者

エクスポートを実行したユーザが表示されます。

開始時間

トランザクションの開始時刻が表示されます。

終了時間

トランザクションの終了時刻が表示されます。

ドキュメント数

エクスポートされたドキュメントの数が表示されます。

失敗件数

失敗したエクスポートの数が表示されます。

進捗 (%)

トランザクションの進捗状況が表示されます。

ステータス

トランザクションのステータスが表示されます。

インポートトランザクション

[インポート トランザクション] ページでは、いずれかの列をクリックすることによって、トランザクションをパッケージ、テンプレート、およびステータスで並べ替えできます。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナントデータから除外するか、テナントデータに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

このページには以下のフィールドがあります。

パッケージ

インポート パッケージ名が表示されます。

実行者

インポートを実行したユーザが表示されます。

開始時間

トランザクションの開始時刻が表示されます。

終了時間

トランザクションの終了時刻が表示されます。

ドキュメント数

インポートされたドキュメントの件数が表示されます。

失敗件数

失敗したインポートの件数が表示されます。

進捗 (%)

トランザクションの進捗状況が表示されます。

ステータス

トランザクションのステータスが表示されます。

関連項目:

[インポート設定の表示](#) (P. 1096)

ドキュメントのエクスポート/インポート

異なるナレッジマネジメントシステム間でデータをマイグレートして同期するには、ナレッジ管理の Knowledge Export/Import Tool (KEIT) を使用します。このツールを使用すると、ナレッジドキュメントをエクスポートおよびインポートできます。

KEIT テンプレートを作成すると、エクスポート/インポート トランザクションを定義できます。

注: r11.0 のナレッジデータをインポートするには、pdm_kit-txt ユーティリティを使用します。

パッケージのエクスポート/インポート

以下の構文はエクスポート パッケージを指定します。

- サーバ名
- 日付
- 開始時間

標準設定では、[管理] タブの [一般設定] ページにある [ナレッジ インポート/エクスポート ファイルのパス] オプションを更新することによってパッケージディレクトリを定義できます。デフォルトでは、「\$NX_ROOT/site/keit」を使用します。このパスを変更した後に [CA SDM サーバを再起動](#) (P. 57) します。

パッケージは以下のデフォルト ディレクトリに格納されます。

- エクスポート パッケージ
\$NX_ROOT/site/keit/export
- インポート パッケージ
\$NX_ROOT/site/keit/import

高可用設定では、[管理] タブの [一般設定] ページにある [ナレッジ インポート/エクスポート ファイルのパス] オプションを更新することによってパッケージディレクトリを定義できます。このパスは UNC 共有ドライブである必要があります。このパスを変更した後に [CA SDM サーバを再起動](#) (P. 57) します。パッケージは、以下のディレクトリに格納されます。

- エクスポート パッケージ
UNC Shared Location/export
- インポート パッケージ
UNC Shared Location/import

エクスポート/インポートの可用性に関する属性を追加するには、NX.env ファイルに以下の属性名を追加します。

@NX_KEIT_AVAILABLE_FIELDS

属性名を追加します。

@NX_KET_ADDL_FIELDS

属性名を追加します。新しい属性が別のオブジェクトへの SREL の場合は、ソース システムとターゲット システム間の同期に使用する属性名を追加します。

例: 属性の追加

```
@NX_KEIT_ADDL_FIELDS =
STATUS_ID.STATUS,DOC_TEMPLATE_ID.TEMPLATE_NAME
```

エクスポートディレクトリおよびインポートディレクトリには、以下のファイルが格納されています。

keit_config.xml

エクスポートまたはインポート パッケージの構成ファイルです。

data.xml

ナレッジ ドキュメントの値が保存されているデータ ファイルです。

rep.xml

data.xml ファイルで参照されるリポジトリです。

イメージ

ナレッジ ドキュメントに埋め込まれたイメージ ファイルを指定します。

エクスポート/インポート テンプレートの表示

ナレッジエクスポート/インポート ツール (KEIT) テンプレートを使用して、エクスポート/インポート トランザクションを定義します。

注: デフォルトのエクスポート/インポートテンプレートは「All-Docs」と呼ばれ、STATUS_ID フィールドは含まれていません。このテンプレートにより data.xml ファイルが作成され、[ドラフト] ステータスのドキュメントがインポートされます。STATUS_ID フィールドを [All-Docs] テンプレートに追加してからエクスポートすると、インポート時に元のドキュメントステータスが保持されます。

ナレッジ エクスポート/インポート テンプレートを表示するには

1. [管理] タブをクリックします。
[管理] コンソールが表示されます。
2. [ナレッジ] - [ドキュメント] をクリックします。
[エクスポート/インポート] - [エクスポート/インポート テンプレート] を選択します。

[ナレッジエクスポート/インポート テンプレート リスト] が表示されます。

3. [名前] 列のテンプレートをクリックします。

KEIT テンプレートが開きます。

注: リスト結果は、Excel にエクスポートして CA SDM の外部で使うことができます。エクスポートするには、リスト ページの [エクスポート] ボタンをクリックします。

エクスポート/インポート テンプレートの検索

[ナレッジエクスポート/インポート テンプレート設定] ページを使用してテンプレートを検索できます。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択してください。パブリック（共有）オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。テナント ドロップダウンリストが検索フィルタ内に表示されます。このドロップダウンリストで <empty> を選択すると、検索がパブリックになります。テナントの列はリスト ページにも表示されます。

ナレッジ エクスポート/インポート テンプレートを検索するには

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [エクスポート/インポート] - [エクスポート/インポート テンプレート] を参照します。

[ナレッジエクスポート/インポート テンプレート リスト] が表示されます。

2. [検索] をクリックし、検索パラメータを入力します。

検索結果が表示されます。

3. [フィルタを表示] をクリックします。

フィルタが表示されます。

4. 以下のオプションを使用して、検索を変更します。

パッケージ

パッケージ名で検索します。

変更日時(最早)

最も初期の変更日付で検索します。

変更日時(最遅)

最新の変更日付で検索します。

その他の検索指数

その他の検索指数が示されます。

検索結果が表示されます。

5. 検索結果内でテンプレートをクリックします。
テンプレートが開きます。

エクスポート/インポート テンプレートの作成

テンプレートの作成と変更には、[管理] タブの [Knowledge Export/Import Template Settings] ページを使用します。

ナレッジ エクスポート/インポート テンプレートを作成するには

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [エクスポート/インポート] - [エクスポート/インポート テンプレート] を参照します。
[ナレッジ エクスポート/インポート テンプレート リスト] が表示されます。
2. [新規作成] をクリックします。
[エクスポート/インポート テンプレートの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

テンプレート名

テンプレートの名前を示します。

説明

グループの簡単な説明を示します。

4. 以下のタブで、適切なフィールドにデータを入力します。

- [エクスポートフィールド](#) (P. 1094)
- [エクスポートフィルタ](#) (P. 1095)
- [インポート設定](#) (P. 1096)

[保存] をクリックします。

テンプレートが作成されます。

関連項目:

[エクスポート トランザクション](#) (P. 1087)

[インポート トランザクション](#) (P. 1088)

エクスポート フィールドの表示

エクスポート フィールドを表示するには、ナレッジ エクスポート/インポート テンプレート (KEIT) を作成します。

[エクスポート フィールド] タブが表示され、以下のフィールドがあります。

利用可能

エクスポートに使用できるナレッジ ドキュメント フィールドを表示します。

注: エクスポートやインポートの過程で、「ドラフト」などのドキュメント ステータスを保持する場合は、**STATUS_ID** を [エクスポート済み] 列に追加します。

エクスポート済み

エクスポートするドキュメント フィールドを指定します。

添付のエクスポート

ナレッジ ドキュメント ファイルの添付ファイルをエクスポートします。

〔ドキュメントの属性を選択〕セクションの矢印を使って、ドキュメント属性にエクスポートを追加できます。

注: Firefox を使用してエクスポート/インポート テンプレートを編集する場合、最初の編集で矢印を使った後のリストサイズは変わりません。テンプレートを閉じて編集モードで再オープンしてからもう一度矢印を使うと、リストサイズは変更されます。Internet Explorer を使う場合、この動作は生じません。

重要: KEIT で〔エクスポート済み〕になっている各フィールドは、〔インポート設定〕タブでデフォルトに選択されている場合より優先されます。〔インポート設定〕タブでエクスポート フィールドをデフォルトに選択している場合、デフォルト フィールドとして処理されません。

エクスポート フィルタの表示

エクスポート フィルタを表示するには、ナレッジ エクスポート/インポート テンプレート (KEIT) を作成します。

〔エクスポート フィルタ〕タブが表示され、以下のフィールドがあります。

カテゴリ

〔ナレッジ カテゴリ〕ページを表示します。このオプションを使って、カテゴリを〔エクスポート フィルタ〕タブのリストに追加します。

カテゴリの削除

カテゴリを〔エクスポート フィルタ〕タブのリストから削除します。

カテゴリのクリア

〔エクスポート フィルタ〕タブのカテゴリ リストをクリアします。

子カテゴリを含める

エクスポート済みカテゴリの子カテゴリからドキュメントをエクスポートします。

2 次カテゴリを含める

エクスポートされたドキュメントの 2 次カテゴリをエクスポートします。

選択したカテゴリにリンクされているすべてのドキュメントを含める

選択したカテゴリにリンクされているすべてのドキュメントをエクスポートします。

注: [2 次カテゴリを含める] を選択した場合のみ有効になります。

その他フィルタ

追加の WHERE 節を指定します。

インポート設定の表示

インポート設定を表示するには、ナレッジエクスポート/インポート テンプレート (KEIT) テンプレートを作成します。

[インポート設定] タブが表示されます。このタブには以下のフィールドが含まれています。

エラーしきい値 (%)

エラーの割合が指定された数字を超えた場合、インポート プロセスが停止し、ステータスが [失敗] に設定されます。

発行済みドキュメントより優先する

CA SDM サーバにある発行済みドキュメントよりインポートされたドキュメントを優先します。

未発行状態にあるドキュメントより優先する

CA SDM サーバにある未発行状態にあるドキュメントよりインポートされたドキュメントを優先します。

ドキュメントの上書き時にデフォルト値を使用

定義されたフィールドには、上書きされたドキュメントのデフォルト値が使用されます。

ドキュメントのインデックスを今すぐ作成

インポート プロセスの後に、ドキュメントにインデックスを作成します。

ステータス

[ドラフト]、[発行済み]、または [廃止済み] を選択します。

優先度

インポート設定の優先度レベルを指定します。

テンプレート

以下のデフォルトのテンプレートから 1 つを選択します。

- ビルトインのナレッジ ドキュメント
- ビルトインのナレッジ ツリー
- ビルトイン - クイック編集

所有者

[連絡先の検索] ページを開くと、所有者が設定できます。

作成者

[連絡先の検索] ページを開くと、作成者が設定できます。

サブジェクト エキスパート

[連絡先の検索] ページを開くと、サブジェクト エキスパートが設定できます。

担当者

[連絡先の検索] ページを開くと、担当者が設定できます。

失効日付

日付ヘルパを開きます。

レビュー日

日付ヘルパを開きます。

製品 ID

[製品の検索] ページを開くと、製品 ID が設定できます。

アセット

[構成アイテムの検索] ページが表示されます。

根本原因

[根本原因の検索] ページを開きます。

Service Desk の優先度

インポート設定の [Service Desk の優先度] を指定します。

重大度

インポート設定の [重大度レベル] を指定します。

影響度

インポート設定の [影響度レベル] を指定します。

緊急度

インポート設定の [緊急度レベル] を指定します。

エクスポート/インポート テンプレートの編集

[ナレッジエクスポート/インポート テンプレート リスト] ページに表示されるエクスポート/インポート テンプレートは、編集できます。

エクスポートまたはインポート テンプレートを編集する方法

1. [ナレッジ] - [ドキュメント] - [エクスポート/インポート] - [エクスポート/インポート テンプレート] へ移動します。

[ナレッジエクスポート/インポート テンプレート リスト] が表示されます。

2. テンプレートを選択します。

[Template Detail] ページが表示されます。

3. [編集] をクリックします。

適切なフィールドを変更します。

テンプレート名

テンプレートの名前を示します。

説明

グループの簡単な説明を示します。

4. 次のタブで、必要に応じてフィールドを変更します。

- [エクスポートフィールド](#) (P. 1094)
- [エクスポートフィルタ](#) (P. 1095)
- [インポート設定](#) (P. 1096)

5. [保存] をクリックします。

編集した内容が保存されます。

関連項目:

[インポート トランザクション](#) (P. 1088)

pdm_ket ユーティリティ - ナレッジ エクスポート ツール

pdm_ket ユーティリティは、Web インターフェースで作成したテンプレートに基づいて、ナレッジをソース コンピュータからナレッジ パッケージにエクスポートします。

添付ファイルとそれらのリンクはエクスポート時に **data.xml** にエクスポートされます。添付ファイルは、インポートする前にバックグラウンド サーバの以下のディレクトリに手動で移動します。

\$NX_ROOT/site/attachments/default

注: 高可用性設定では、添付ファイルの **UNC** パスを使用して **pdm_ket** ユーティリティを実行できます。

このユーティリティを使って以下を実行します。

- 関連するナレッジエクスポートテンプレートに基づいて環境設定ファイルを作成します。
- ドキュメントの **UUID** 付きのデータと、タイトル、サマリ、問題、解決方法などのコンテンツと、所有者やステータスなどのその他のドキュメント属性をエクスポートします。
- エクスポート済みドキュメントで使われるすべての固有イメージをエクスポートします（常にエクスポート）。
- エクスポート済みドキュメントで使われるすべての固有添付ファイルをエクスポートします（**EXP_ATTMNT** フィールド）。

ファイルはリモート リポジトリからローカルパッケージフォルダにコピーされます。

このユーティリティは以下のように呼び出します。

```
pdm_ket -n <template name> [-h] ]-v]
```

-n <template name>

エクスポートに使用するテンプレートの名前を定義します（大文字と小文字を区別する）。

-h

(オプション) ユーティリティのヘルプを表示します。

-v

(オプション) プログラム イベントの詳細ログ (bop_logging) を有効にします。通常、このオプションは、内部の問題を解決するために使います。

例: pdm_kit を使って my_template テンプレートでナレッジをエクスポートする

```
pdm_kit -n my_template
```

pdm_kit ユーティリティは、サードパーティのスケジューラを使ってナレッジ ドキュメントのエクスポートをスケジュールできます。

pdm_kit ユーティリティ - ナレッジ インポート ツール

pdm_kit ユーティリティは、パッケージの環境設定ファイルの設定に従って、インポート先にデータをインポートします。

重要: アプリケーション サーバからの pdm_kit ユーティリティを実行する前に、パッケージのパス (ローカルまたは UNC) がバックグラウンドサーバによってアクセス可能であることを確認します。バックグラウンドサーバがこのパスにアクセスできない場合、パッケージはアプリケーションサーバからインポートされません。

重要: r11.0 インポート ユーティリティは名前が pdm_kit_txt.exe に変更されており、r11.0 のテキスト ファイルをインポートできます。このユーティリティでは、リリース 12.9 のインポート機能拡張はサポートされていません。

これまでに pdm_kit ユーティリティによって参照されている参照済みデータには、インポート先サーバの実際の UUID または ID 値が取得されています。pdm_kit ユーティリティを実行すると、新しい userid パラメータが適用されます。pdm_kit ユーティリティは次のように動作します。

1. userid 値 (連絡先) または参照済み名 (アセットなどのフィールド) をインポート先の適切な UUID に置き換えて、ドキュメントをインポートします。
2. イメージをインポートします。

3. 添付ファイルをインポートします。
4. ローカルパッケージフォルダからリモート リポジトリにファイルをアップロードします。

注: 発行済みドキュメントの編集が無効な場合、インポートされたドキュメントはリワーク バージョンとして作成されます。

このユーティリティは以下のように呼び出します。

```
pdm_kit [-h] -f -u [-v]
```

-h

(オプション) インターフェースにユーティリティのヘルプを表示します。

-f

パッケージのパスを指定します。

-u

デフォルト ユーザを指定します。

-v

(オプション) プログラム イベントの詳細ログ (**bop_logging**) を有効にします。通常、このオプションは、内部の問題を解決するために使います。

注: 高可用性設定では、バックグラウンド サーバで **pdm_kit** ユーティリティを実行できます。また、**Windows** では、パッケージが **UNC** 共有ドライブに存在する場合、アプリケーション サーバで **pdm_kit** ユーティリティを実行できます。**Windows** 以外のプラットフォームでは、アプリケーション サーバで **pdm_kit** ユーティリティを実行できません。

例: **pdm_kit** を使ったパッケージのインポート

```
pdm_kit -f c:¥package_path -u ServiceDesk
```

ナレッジのエクスポートまたはインポートをユーザに許可

アナリストがエクスポートおよびインポート権限を付与できるようにするには、[管理] タブで役割リストを管理します。

エクスポート/インポート権限を付与する方法

1. [セキュリティと役割の管理] - [役割管理] - [役割リスト] に移動します。

[役割リスト] が表示されます。

2. アナリスト インターフェース タイプを持つ役割を選択します。

[役割の詳細] ページが表示されます。

3. [編集] をクリックします。

[役割の更新] ページが表示されます。

4. [ナレッジ] タブをクリックします。

以下のような操作を実行できます。

- [エクスポートを許可] チェック ボックスをオンにします。
- [インポートを許可] チェック ボックスをオンにします。
- 両方のチェック ボックスをオンにします。

5. [保存] をクリックします。

[役割の詳細] ページが再表示されます。

6. [ナレッジ] タブで変更内容を確認します。

[役割の詳細] ページを閉じます。

また、[役割の詳細] ページの [ナレッジ] タブでチェック ボックスをオフにして、ユーザによるエクスポート/インポートを制限することもできます。

Web サービス

ナレッジへは **SOAP Web** サービスからアクセスできます。さまざまな方法が用意されており、ドキュメントの検索、取得、作成、更新、その他の操作を実行できます。

注: SOAP Web サービスの詳細については、「[実装ガイド](#)」を参照してください。

第 23 章: ナレッジ マネジメント の管理

このセクションには、以下のトピックが含まれています。

[ナレッジ管理](#) (P. 1105)

[ナレッジ管理の手順の検索](#) (P. 1105)

[ナレッジマネジメントの役割と機能](#) (P. 1106)

[役割権限とドキュメントの表示/非表示の管理方法](#) (P. 1119)

[アクション コンテンツ](#) (P. 1120)

[ドキュメント承認プロセス](#) (P. 1126)

[自動ポリシー](#) (P. 1134)

[ナレッジ ドキュメントの制御](#) (P. 1140)

[ナレッジ マネジメント システムの設定](#) (P. 1206)

ナレッジ管理

ナレッジ マネジメント の管理設定を構成できます。[セルフ サービス ナレッジ オプション](#) (P. 1109)を設定することで、ユーザのニーズを満たせるほか、ナレッジの管理と配布を効率的、かつ効果的に実施できる環境を構築できます。システム オプションは、[管理] タブで設定します。ナレッジ権限は、グループまたは連絡先の役割に基づいて設定できます。ナレッジ マネジメント の機能と用途に適合する設定を適用できます。

重要: ナレッジ ベースでのインデックスの再作成や自動ポリシーとナレッジ レポート カードの計算には、時間がかかることがあります。このため、これらの処理は営業時間外またはシステム負荷が低いときに実行することをお勧めします。

ナレッジ管理の手順の検索

CA SDM では、このガイド、およびオンライン ヘルプでナレッジ管理の実行手順について説明しています。

オンライン ヘルプでナレッジ管理の実行手順を探す方法

1. CA SDM にログインします。

CA SDM のメイン ページが表示されます。

2. 以下のいずれかの操作を実行します。

- [ヘルプ] をクリックし、メインメニューの [ヘルプ] からオンラインヘルプの [管理] - [ナレッジ管理] に移動します。

ナレッジ管理のトピックが表示されます。階層を移動して、必要な情報を探することができます。

- [ヘルプ] をクリックし、メインメニューの [このウィンドウのヘルプ] を選択します。

オンラインヘルプに、目的のページのヘルプ トピックが表示されます。

ナレッジ マネジメント の役割と機能

ナレッジ マネジメント は幅広いユーザを対象としており、製品を管理する管理者やナレッジ マネージャから、問題を解決するためにシステムを使用している顧客や従業員までご利用いただけます。複数の役割を 1 人に割り当てることができますが、ナレッジ マネジメント には以下の基本的なユーザ役割があります。

- **顧客**：基本的なセルフサービス タスクを実行する外部エンドユーザ。
- **従業員**：基本的なセルフ サービス タスクを実行する内部エンドユーザ。
- **ナレッジアナリスト**：ナレッジ管理プロセスにおいて 1 つ以上の手順を担当するユーザ。このユーザは、サービス デスク アナリストと連携して品質ソリューションベースを作成し、管理します。
- **ナレッジ マネージャ**：ナレッジアナリストの管理者。この役割では、ナレッジ ドキュメントの再割り当てとエスカレーション以外に、ソリューションの日常的な管理側面を担当します。たとえば、カテゴリ構造の作成や承認プロセスの定義、およびノイズワード、特殊用語、同義語など、ナレッジ管理 マネージャの業務と比較して、より動的性質を持つ設定やオプションの管理を行います。

- **管理者**：1つの役割で CA SDM およびナレッジ マネジメント 製品のすべての機能にアクセスできる管理者。この役割は、CA SDM を実装するときにすべてのユーザと役割が適切に設定されていることを確認する場合や、CA SDM 環境であらゆる管理タスクを1人で担当する場合によく使用されます。
- **ナレッジ管理マネージャ**：ナレッジ管理プロセスの設定と監視を担当する管理者。この役割では、カテゴリ構造の作成、承認プロセスの定義、検索やセキュリティのデフォルト設定などを行います。

CA SDM 環境の各役割には、さまざまなレベルのアクセスが関連付けられています。各レベルは、各役割によって実行されるタスクの定義に役立ちます。

関連項目：

[ナレッジ マネジメント のユーザ インターフェース \(P. 1107\)](#)

[ナレッジ マネジメント の設定機能と管理機能 \(P. 1108\)](#)

[セルフサービス ナレッジ オプション \(P. 1109\)](#)

[ドキュメントとユーザ \(P. 1115\)](#)

[役割権限とドキュメントの表示/非表示の管理方法 \(P. 1119\)](#)

ナレッジ マネジメント のユーザ インターフェース

以下のユーザ インターフェースは、ナレッジの管理に役立ちます。

- **セルフサービス** - セルフサービス インターフェースでは、CA SDM を使用している顧客および従業員がナレッジ ドキュメントにアクセスしたり、さらに検討するためにナレッジをサブミットしたりできます。顧客はブックマークを検索、参照、または使用して、ナレッジ ドキュメントを検索および表示できます。
- **ナレッジ ドキュメント** - ナレッジ ドキュメント インターフェースでは、CA SDM スコアボードの [ナレッジ ドキュメント] ノードからアクセスして、システムのすべてのユーザが各自の受信トレイおよびフォローアップ コメントを表示できます。管理者は、未割り当てまたはインデックスのないドキュメント、ドキュメント ライフサイクルの自動ポリシー、およびユーザ フォーラムを管理します。

- **ナレッジ管理** - ナレッジ管理インターフェースでは、CA SDM の [ナレッジ] タブからアクセスして、ナレッジアナリストまたはナレッジマネージャがナレッジを検索、分類、および発行できます。 また、表示されたドキュメントを高度なオプションを使用してフィルタしたり、関連性や変更日などに基づいて結果を並べ替えたりできます。
- **ナレッジ管理** - ナレッジ管理インターフェースでは、CA SDM の [管理] タブにある [ナレッジ] ノードからアクセスして、管理者、ナレッジマネージャ、またはナレッジ管理者が各種のシステム オプションを設定できます。 これにより、ナレッジマネジメント の機能と用途に適合する設定が実現します。

ナレッジ マネジメント の設定機能と管理機能

ナレッジマネジメント では、以下の構成機能と管理機能を実行できます。

- ドキュメントの [解決方法] フィールドに挿入可能な「アクション コンテンツ」 (ライブアクション URL) を作成します。
- 承認プロセスを設定する、およびナレッジ ドキュメントのライフサイクルプロセスを定義します。
- ナレッジ ドキュメント承認プロセスの特定のタスクを自動化する自動ポリシーを設定します。
- コメント、ナレッジのサブミット、テンプレート、ドキュメント設定に関連するドキュメント オプションを設定します。
- ドキュメントで情報がどのように表示されるかを制御する、テンプレートを作成します。
- デフォルトのナレッジ マネジメント 検索エンジンを管理し、キーワード検索および自然言語検索の実行に使用するノイズワード、特殊用語、および同義語を設定します。
- ユーザがナレッジ ソリューションを検索したときにセルフ サービス インターフェースに表示される「推奨ドキュメント」を作成します。
- ドキュメントに簡単にアクセスできるようにするナレッジ カテゴリ構造を管理します。
- ナレッジ レポート カードの設定および全般的なシステム設定を実行します。

- ナレッジ ドキュメントのパフォーマンスに関する顧客フィードバックを収集して分析するための調査を定義します。
- ナレッジ マネジメント の **CA SDM** へのインテグレーションを管理する (フィールド マッピング、リクエストおよび案件の検索設定を含む)。

セルフサービス ナレッジ オプション

CA SDM を利用する顧客および従業員は、セルフサービス インターフェースを使用してナレッジ ドキュメントにアクセスできます。顧客はブックマークを検索、参照、または使用して、ナレッジ ドキュメントを検索および表示できます。顧客がドキュメントおよびサービスにアクセスできるようになると、回答を自分で見つけ出すことができ、これにより、リソースに対する負荷を減らすことができます。

セルフサービス ユーザ インターフェースでは、顧客は以下のナレッジ 解決策オプションを表示できます。

- **ナレッジ 解決策の検索** - 従業員および顧客は、キーワードおよびフレーズを [検索] フィールドに入力して、ナレッジ 解決策のリストを取得できます。このオプションは、[管理] - [ナレッジ] - [検索] - [検索設定] を選択して構成できます。
- **上位解決策の表示** - 従業員および顧客は、セルフサービス インターフェースで上位解決策のリストを表示できます。表示するドキュメントの数は、次の管理者設定によって決まります。[管理] - [ナレッジ] - [一般設定] - [上位解決策] - [表示ドキュメント数]
- **ナレッジ 調査を推進** - ユーザがナレッジ ドキュメントを開くと、そのドキュメントを参照して、一連の調査質問にアクセスできます。これらの質問の1つとして、プロンプトを使用して問題が解決したかどうかを顧客に尋ねることができる機能があります。このオプションは、[管理] - [ナレッジ] - [解決策に関する調査] - [調査の設定] を選択して構成できます。
- **ナレッジ の提案** - 従業員と顧客は、セルフサービス インターフェースでチケットを作成するとき、許可されている場合に、ナレッジ 提案のリストを表示できます。このオプションは、[管理] - [ナレッジ] - [Service Desk インテグレーション] - [ナレッジ の提案] を選択して構成できます。

高度な検索

高度な検索設定では、顧客と従業員は、問題の解決策の検索を改善するために、以下のオプションを使用できます。

ナレッジ マネジメント の検索

特定のキーワードを検索します。このキーワードは、予備的一致として動作します。

自然言語検索

語句を検索し、語句の近似性、語句の順序、および関連性を考慮します。

検索結果は、関連性に基づいて一覧表示されます。関連性は、指定した検索条件（[非常に良い]、[良い] など）に基づいて決定されます。最も関連性が高い（非常に良い）と評価されたドキュメントがリストの先頭に表示されます。

結果ごとに、リンクとして表示されるタイトル、ドキュメントの概要、およびドキュメントに関連する追加の統計（関連性の評価、ドキュメント ID、変更日、FAQ 評価、およびヒット数）が表示されます。

システム管理者が ナレッジ マネジメント をどのように構成したかによって、ユーザはナレッジ ドキュメントを開いたときに、インシデントのオープン、ドキュメントの評価、およびコメントの追加を実行できます。

ナレッジ ドキュメント情報

各ナレッジ ドキュメントには、ユーザに情報を提供する重要なドキュメント フィールドがあります。使用したドキュメント テンプレートによって、別のフィールドが表示されたり、ドキュメントに含まれるフィールドの表示方法が異なっていたりします。

タイトルはドキュメントを識別するものです。また、ドキュメントには以下の情報も含まれます。

概要

ドキュメントを要約し、問題を簡潔に説明します。

問題

その問題を説明します。

解決方法

プレーン テキストまたは HTML 形式で、問題の解決方法を説明します。

関連項目

現在のドキュメントに関連するドキュメントを一覧表示します。ドキュメントのハイパーリンクをクリックすると、関連ドキュメントを含む新しいページが開きます。

添付ファイル

ドキュメントに添付され、ダウンロード可能なファイルを一覧表示します。添付ファイルによって、ドキュメントに関する追加情報が得られます。

関連カテゴリ

ドキュメントに関連するカテゴリを一覧表示します。カテゴリのハイパーリンクをクリックすると、[検索ツール] ページが更新され、そのカテゴリが表示されます。

関連チケット

ドキュメントから開かれた、またはドキュメントを使用して解決されたリクエスト、インシデント、問題、案件、およびドキュメントにリンクします。

プロパティ

ドキュメントテンプレートで選択された追加のドキュメントプロパティを示します。デフォルトでは、変更日およびドキュメント ID が表示されます。

コメント

ドキュメントに対するユーザからのコメントを一覧表示します。コメントのほかに、連絡先名、電子メールアドレス、および日付が含まれます。

評価およびコメント

ドキュメントが質問への回答として役立ったかどうかに関する、フォローアップ コメントおよびフィードバックを示します。ドキュメントが役立ったかどうかを、以下の質問に基づいて評価できます。

- このドキュメントで問題が解決されましたか。
- このフォーラムはどの程度参考になりましたか。

以下のコメント タイプのいずれかを使い、コメントを追加したり、その対応を別のアナリストに割り当てたりすることもできます。

- 壊れたリンク
- 発行候補
- 廃止候補
- 情報が不正確
- 情報不足
- 新規コンテンツの推奨
- レビュー
- 解決策が機能しない

[ページ オプション] セクションを使用すると、以下の一連のアクションを実行できます。

- 編集
- ブックマークの追加/削除
- サブスクライブ
- 評価およびコメント
- 電子メール
- 新規フォーラム
- 新規インシデント
- このドキュメントに基づいた新規インシデント
- 印刷可能バージョン

関連項目：

[コメント タイプの作成](#) (P. 1143)

[セルフ サービス ポリシーの設定](#) (P. 1202)

アナウンスメント

アナウンスメントは、問題に対して解決策をすばやく提供するための方法です。アナウンスメントにより、広範囲にわたる問題への解決策を示したり、Service Desk に寄せられる回答依頼に対応できます。

現在のアナウンスメントは、システムに最初にログインしたときに、メインの CA SDM ウィンドウの右側のペインに表示されます。

ドキュメントの並べ替え

さまざまな順序でドキュメントを並べ替えることができます。

ドキュメントを並べ替えるには、以下の手順に従います。

1. [ナレッジ] タブで、左側のペインにあるカテゴリ リストから [ツリーノード] を選択します。
2. ノードを展開し、[カテゴリ] をクリックします。
[ドキュメントリスト] ページが表示されます。
3. [並べ替え] を使って、以下の順序でリストごとにドキュメントを並べ替えます。
 - FAQ 評価
 - ヒット数
 - 最近変更されたドキュメント
 - 解決策数

ドキュメントは、選択した順序で一覧表示されます。

ドキュメントの参照

ナレッジ ドキュメントを分類すると、よくある質問 (FAQ) に基づいて顧客が情報を参照できます。ナレッジ カテゴリを選択すると、関連するサブカテゴリおよびナレッジ ドキュメントが表示されます。表示するドキュメントを選択したり、サブカテゴリを選択して検索をさらに絞り込むことができます。

セルフサービス機能を向上させるには、最も使用頻度の高いドキュメントのリストを動的に表示します。

注: ユーザは、目的の項目に関する条件を指定できます。このとき、検索エンジンによって一致するナレッジ ドキュメントの検索が行われ、そのドキュメントが「推奨ドキュメント」リンクのセットとして [検索結果] ページに表示されます。検索クエリは、1 つ以上のドキュメントに含まれる可能性のある目的の概念を示すキーワードまたは一連の語句（フレーズ）として表現できます。詳細については、[「新規推奨ドキュメントの作成」](#) (P. 1187) を参照してください。

ドキュメントのブックマーク

アクセス頻度の高いドキュメントには、ブックマークを付けることができます。ドキュメントにブックマークを付けると、そのドキュメントは [ブックマーク] リストに追加されます。このリストを使用すると、頻繁に表示するドキュメントを簡単に検索できます。ドキュメントを [ブックマーク] リストに追加した後は、[ブックマーク] ボックスに [削除] ボタンが表示されます。あまりアクセスしなくなったブックマークは、リストから削除できます。

[あなたのブックマーク] フォルダには、最も参照頻度の高いドキュメントへのリンクが格納されます。[ナレッジ] タブの [カテゴリ] ペインで [マイ ブックマーク] をクリックすると、[ナレッジ ドキュメント リスト] ペインにブックマークを付けたドキュメントのリストが表示されます。

インシデントと問題

顧客は、ナレッジを検索するだけでは解決できない問題に直面することがよくあります。すべての問題の直接的な解決策が、ナレッジ ベースに記録されているわけではありません。解決できない問題が発生した場合、顧客はインシデントを作成してアナリストに送信し、詳しく調査してもらうことができます。このインシデントには、問題が記述されます。また、既存のナレッジ ドキュメントをベースとすることもできます。インシデントに追加される情報が多くなるほど、アナリストはそのインシデントを解決しやすくなります。

ナレッジ マネジメント では、ITIL で定義されている以下のような多数のアクティビティをサポートしています。

- インシデント管理
 - 後続のインシデントの調査および診断ではナレッジ検索を使用して既知のエラーを検索できる
 - インシデントの分類
- 問題管理
 - 問題が以前に発生している場合は、既知のエラー情報にアクセスし、問題を照合して解決方法を得る
 - 回避策に関する情報の管理およびアクセスの提供
 - 手順、作業指示、診断スクリプト、および既知のエラーに関する情報の記録（解決方法を導き出すための豊富なコンテンツ、編集ツール、測定、および定義可能な承認プロセスをサポート）
 - 問題分析（インシデントのリンクおよび分析を使用）

ドキュメントとユーザ

CA SDM スコアボードの [ナレッジ ドキュメント] ノードからアクセスできるナレッジ ドキュメント インターフェースでは、システムのすべてのユーザが各自の受信トレイおよびフォローアップ コメントを表示させることができます。管理者は、未割り当てまたはインデックスのないドキュメント、ドキュメント ライフサイクルの自動ポリシー、およびユーザ フォーラムを管理します。

ドキュメントの受信トレイ

CA SDM スコアボードの [ナレッジ ドキュメントの受信トレイ]（および [グループ受信トレイ]）には、ユーザまたはグループに割り当てられたドキュメントが含まれます。受信トレイは、保存済みおよび割り当て済みのドラフトやリワーク バージョンのドキュメントを含め、あらゆるステータスのドキュメントを格納する中央リポジトリです。

毎日のタスクのコンテナとなる受信トレイは、承認プロセスを管理するための重要なツールです。ドキュメントを作成または更新すると、所有者の受信トレイに格納されます。ユーザは、発行プロセスの一環として、受信トレイに表示されるアイテムに注意を払う必要があります。受信トレイ内のアイテムは、発行されるまで解決方法として表示されないことがあり、ナレッジベースにも追加されません。新規ドキュメント用の受信トレイを定期的に監視してください。

フォローアップ コメントの表示

CA SDM ナレッジ ドキュメント スコアボードの [フォローアップ コメント] 受信トレイには、ユーザまたはグループに割り当てられたコメントが含まれます。

割り当てられたフォローアップ コメントの概要情報は、[コメント リスト] ページで表示できます。

フォローアップ コメントを表示するには、[ナレッジ ドキュメント] - [フォローアップ コメント] を参照します。

ドキュメント属性

ドキュメント属性を設定することは、ご使用のナレッジプール内のドキュメントを管理するのに役立ちます。ドキュメント属性を更新して、ドキュメントに新しいサブジェクト エキスパートまたは所有者を割り当てることができます。また、ナレッジベースでそのドキュメントが使用可能になる日付および期限切れになる日付を指定できます。別のドキュメント テンプレートを選択して、各ドキュメントのデザインを変更することができます。

ドキュメント権限

ドキュメントに対する権限の設定、表示、および編集ができます。これらの権限は、さまざまなグループに割り当てることができます。権限を設定するにあたって、ドキュメントのプライマリ カテゴリから権限を継承するか、新規の権限を指定するかを決めることができます。デフォルトでは、ドキュメントのプライマリ カテゴリからの権限が継承されます。デフォルトでは、アクセス権限はドキュメント レベルではなくカテゴリ レベルで処理されます。

重要: ナレッジ ドキュメントを作成する場合、ドキュメント権限には後の承認プロセスによってドキュメント上に割り当てることができるユーザーが含まれていることを確認します。グループがドキュメントに割り当てられる場合、そのグループからのユーザーにはドキュメントを表示する権限がない場合があります。ドキュメントが特定のユーザーに割り当てられている場合、デフォルトのデータ パーティションの制約によって、そのユーザーはドキュメントを表示できます。

ナレッジ カテゴリ

各ドキュメントを、プライマリ カテゴリに割り当てます。たとえば、**Microsoft Word** に関連するナレッジは、**Microsoft Word** のカテゴリに追加する必要があります。また ナレッジ マネジメント では、ドキュメントを複数の 2 次カテゴリおよび他のドキュメントに関連付けることもできます。このようにして、さまざまなカテゴリにドキュメントを適切に分類できるので、首尾よく検索結果を得られるようになります。ドキュメント リンクを作成すると、リンクしたドキュメントのいずれかを表示したときに「関連項目」リンクが表示されます。この「参照」リンクを使用すると、リンクされているドキュメント間を直接移動できます。

添付ファイルの権限

添付ファイルの権限は、「管理」タブの「添付ファイル ライブラリ」-「リポジトリ」ノードで管理します。会社での必要性に基づいて、リポジトリ フォルダに権限を設定できます。

注: ドキュメントの権限は、リンクされている添付ファイルの権限と異なることがあります。

ドキュメントの添付ファイルの追加

ナレッジ ドキュメントを操作する場合は、そのドキュメントに補足のファイルまたは URL を添付できます。このような補足のファイルまたは URL を使用すると、ナレッジ ドキュメントに関連する追加情報に簡単にアクセスできます。添付されたファイルはリポジトリに格納されます。

「添付ファイル」タブを使用して、現在のドキュメントに添付されたファイルおよび URL を管理します。デフォルトのビルトインナレッジドキュメントまたはビルトインナレッジツリー テンプレートを使用して作成したドキュメントでは、添付ファイルへのリンクは「添付ファイル」という見出しの下に表示されます。

注: 「添付ファイル」タブは、発行済みドキュメントにのみ表示されます。未発行のドキュメントの場合、「添付ファイル」タブには「リポジトリ」、「ファイル」、「添付ファイル」の各ペイン、および現在ドキュメントに添付されている URL とファイルのリストが表示されます。

ドキュメントに添付ファイルを追加する方法

1. 編集対象のドキュメントを開きます。
2. 「添付ファイル」タブをクリックします。
3. 添付する URL を入力します。
4. 以下のいずれかの手順に従います。
 - 「ファイルの添付」をクリックして、システムからファイルを追加します。
 - 「ライブラリからのファイルを添付」をクリックして、「リポジトリ」リストから添付するファイルの名前を選択します。名前は「添付ファイル」タブに表示されます。

ドキュメント履歴の表示

ドキュメントに対して実行されたすべてのアクションの記録を確認できます。

ドキュメント履歴を表示するには、「ドキュメントの更新」ページで「履歴」タブをクリックします。

イベント リストが開き、各イベントの詳細が表示されます。「履歴」タブに表示される情報は参照専用であり、この情報を変更することはできません。

ドキュメント通知

CA SDM では、連絡先と呼ばれるユーザのリストをセットアップできます。特定のイベントの発生時に、このユーザに対して通知を行うことができます。通知プロセスによって、各個人にドキュメントのステータスの変化が通知され、全員がその進捗に関して最新の情報を得られます。ドキュメントに指定された通知を送信できるのは、このリストに表示されるユーザに対してのみです。

ドキュメントの変更

ドキュメントがスコアボードの[受信トレイ]フォルダに到着すると、ユーザは各自に割り当てられた役割に従ってドキュメントを変更して保存し、自分の割り当てタスクを実行できます（たとえば、あるアナリストはドキュメントの技術的な内容の確認を担当しますが、別のアナリストはフォーマットを確認します）。

ドキュメントに対するフルアクセス権を持つすべてのユーザがドキュメントを変更できます。現在の所有者はドキュメントに対するフルアクセス権を持っていますが、明示的な書き込み許可は持っていない可能性があります。所有者のみが、（[属性] タブで）ドキュメントの所有者を変更できます。

役割権限とドキュメントの表示/非表示の管理方法

環境内のユーザの役割権限を管理することにより、ナレッジマネジメントのセキュリティ権限をセットアップできます。これらの権限を使用して、ナレッジを表示または作成するためにアクセスできるユーザや、システムにログインするユーザの認証方法を設定できます。

ナレッジマネジメントの役割権限とドキュメントの表示/非表示を管理するには、以下の手順に従います。

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。

[役割リスト] ページが表示されます。

2. 必要な役割（ナレッジ マネージャなど）を選択します。

［役割の詳細］ ページと［役割の更新］ ページに、以下のタブが表示されます。

ナレッジ マネジメント

役割の ナレッジ マネジメント 権限を指定します。

KTドキュメントの見やすさ

役割に対して表示を許可するドキュメント ステータス（ドラフト、廃止済み、発行済みなど）を指定します。

3. タブ ページの設定を完了し、変更を保存します。

セキュリティ権限と役割権限が定義されます。

注: セキュリティのセットアップおよび役割の定義の詳細については、オンラインヘルプを参照してください。

アクション コンテンツ

「アクション コンテンツ」（ライブ アクション URL）を作成してナレッジ ドキュメントの［解決方法］フィールドに挿入できます。このアクション コンテンツをエンドユーザがクリックすると、インシデントの作成などのアクションが実行されます。アクション コンテンツを使用すると、ユーザは意識することなくかなりの程度の定義と分類を行うことができます。

ドキュメントに実際の「アクション コンテンツ」リンクを挿入する手順は単純です。また、コード化は必要ではありません。ナレッジ マネジメント HTML エディタは、HTML コードの生成を処理します。

注: アクション コンテンツは、外部アプリケーションとのインタラクションに主として使用されます。

関連項目:

[アクション コンテンツの表示 \(P. 1121\)](#)

[アクション コンテンツ（アクション URL）の作成 \(P. 1122\)](#)

[アクション コンテンツ（内部 HTML）の作成 \(P. 1123\)](#)

[アクション コンテンツの編集 \(P. 1124\)](#)

[アクション コンテンツの検索 \(P. 1124\)](#)

アクション コンテンツの表示

エンドユーザのアクションを定義できるライブアクション URL の詳細を表示できます。ナレッジマネジメントでは、ナレッジドキュメントを自動タスクにリンクできるため、ナレッジドキュメントにセルフサービススクリプトを埋め込むことができます。

アクション コンテンツを表示する方法

1. [管理] タブで、[ナレッジ] - [アクション コンテンツ] を参照します。
[アクション コンテンツ リスト] が表示されます。
2. このページには、アクションの詳細と実行オプションが表示されます。

名前

アクション コンテンツの名前が表示されます。

コード

アクション コンテンツをドキュメントにリンクする HTML コードを指定します。

アクション URL

何らかの種類のアクション（Web サイトを開く、フォームを開くなど）を実行する URL リンクを指定します。

検索

名前でアイテムを検索します。

フィルタを表示

[コメント リスト] ページのアイテムを検索します。1 つ以上の検索フィールドにデータを入力し、[検索] をクリックします。[アクション コンテンツ リスト] ページに、検索条件に一致するアイテムが表示されます。

新規作成

アクション コンテンツ リンクを作成します。

3. ナレッジマネジメントおよびサポート オートメーション で使用できるアクション コンテンツを検索します。
検索結果が表示されます。

アクション コンテンツ(アクション URL)の作成

ナレッジ ドキュメントにアクション コンテンツを作成できます。これらのアクション URL は、システムのすべてのユーザにアクセス可能な実際の Web サイトを起動できます。さらに、アクション URL をサーバ (KT デーモンが実行されているサーバ) の自動タスクにリンクすることもできます。また、これらのスクリプトを、ナレッジ ドキュメント、ツリー ドキュメント、ドキュメント テンプレート、およびナレッジ フォーラムに埋め込むことができます。

アクション コンテンツ(アクション URL)を作成する方法

1. [管理] タブで、[ナレッジ] - [アクション コンテンツ] を参照します。
[アクション コンテンツ リスト] ページが表示されます。
2. [新規作成] をクリックします。
[アクション コンテンツの新規作成] ページが表示されます。
3. フィールドに必要なデータを入力します。以下のフィールドには説明が必要です。

コード

このアクション コンテンツ アイテムに一意の識別子を指定します。

内部 HTML を使用

ナレッジ ドキュメントからサードパーティ アプリケーションに、ユーザ名やセッション ID などの情報を動的に渡すアプリケーション内に[内部リンクを作成](#) (P. 1123) します。このオプションは選択しないでください。

アクション URL

Web ページ、テンプレート、または自動スクリプトにリンクする URL を指定します。例: `http://www.ca.com`

[保存] をクリックします。

アクション コンテンツが作成されます。

アクション コンテンツ(内部 HTML)の作成

ナレッジ ドキュメントにアクション コンテンツを作成できます。これらのアクション URL はセルフ サービスのスクリプトおよびサードパーティ アプリケーションも起動できます。このリンクは動的に生成され、ターゲット アプリケーションに、ユーザ名のようなユーザに関する属性を自動的に転送します（例： `http://www.ca.com?USERNAME=BBB`）。ユーザ属性は HTML ファイルに指定されます。

内部 HTML ファイルを使用してアクション コンテンツを作成する方法

1. ターゲット アプリケーションにデータを渡す内部 HTML ファイルを作成します。

注: `act_content_sample.html` ファイルは次の場所で入手できます。
`NX_ROOT¥bopcfg¥www¥html¥default`

2. HTML ファイルを次の場所に保存します。
`NX_ROOT¥site¥mods¥www¥html¥default directory`
3. [管理] タブで、[ナレッジ] - [アクション コンテンツ] に移動します。
[アクション コンテンツ リスト] ページが表示されます。
4. [新規作成] をクリックします。
[アクション コンテンツの新規作成] ページが表示されます。
5. 以下のフィールドを指定します。

コード

このアクション コンテンツ アイテムに一意の識別子を指定します。

6. [内部 HTMLPL を使用] チェック ボックスをオンにします。
7. [アクション URL] フィールドに適切な HTMLPL ファイルを指定します。
例: act_content_sample.html

注: URL で形式 `SA_SCRIPT=[セルフ サービス スクリプト ID]` を使用することにより、サポート オートメーション スクリプトを使用することができます。

8. [保存] をクリックします。

アクション コンテンツが作成されます。ユーザがナレッジ ドキュメント内のこの[アクション コンテンツ リンク]をクリックすると、ユーザ名のようなユーザに関する属性はターゲット アプリケーションに動的に渡されます。

アクション コンテンツの編集

作成されて [アクション コンテンツ リスト] ページに表示されているアクション コンテンツは、編集できます。

アクション コンテンツを編集するには

1. [管理] タブで、[ナレッジ] - [アクション コンテンツ] を選択します。
[アクション コンテンツ リスト] が表示されます。
2. 編集するアイテムを選択します。
[アクション コンテンツ詳細] ページが表示されます。
3. [編集] をクリックします。
[アクション コンテンツの更新] ページが表示されます。
4. 必要に応じてフィールドを編集します。
5. [保存] をクリックします。
アクション コンテンツが更新されます。

アクション コンテンツの検索

検索条件を入力して [アクション コンテンツ リスト] にフィルタを適用することによって、必要なアイテムのみを表示できます。また、個々のアイテムを検索して表示または編集することもできます。

アクション コンテンツを検索するには

1. [管理] タブで、[ナレッジ] - [アクション コンテンツ] を選択します。
[アクション コンテンツ リスト] ページが表示されます。
2. [フィルタを表示] をクリックします。
[検索フィルタ] が表示されます。
3. 以下の 1 つ以上の検索フィールドに値を入力します。

名前

このアクション コンテンツ アイテムを識別します。

ステータス

このアイテムがアクティブであるか、非アクティブであるかを示します。

コード

このアクション コンテンツ アイテムに一意的識別子を指定します。

ナレッジ マネジメント URL

アクション URL が内部 Web ページ (.html) にリンクしていることを示します。

4. (オプション) [詳細] をクリックします。
追加フィールドが表示され、[アクション コンテンツ リスト] に表示されるアイテムを詳細に制限できます。
5. [検索] をクリックします。
[アクション コンテンツ リスト] ページに、検索条件に一致するアイテムが表示されます。項目を選択して、表示または編集できます。

注: リスト結果は、Excel にエクスポートして CA SDM の外部で使うことができます。エクスポートするには、リスト ページの [エクスポート] ボタンをクリックします。

ドキュメント承認プロセス

ナレッジベースを管理する管理者には、ドキュメントの編集と承認プロセスをカスタマイズする機能が不可欠です。承認プロセス テンプレートをデザインし、従業員のドキュメントを変更して全体に発行する方法、時期、対象ドキュメントを指定できます。承認プロセス テンプレートでは、ビジネス環境に最適なさまざまな承認プロセスを指定できます。実装する承認プロセスは、変更を重ねてより簡単に、または複雑にできます。

承認プロセス マネージャでは、承認プロセス テンプレートを定義できます。デフォルトでは、ビルトインの承認プロセス テンプレートが使用されます。ただし、テンプレートを新たに作成することも、既存のテンプレートを編集することもできます。承認プロセス テンプレートの作成では、ステータスを定義してテンプレートにタスクを追加します。承認プロセスには、ナレッジ ドキュメントに対して実行される一連のタスクが含まれます。各タスクは、承認プロセス テンプレートでタスクに割り当てられている所有者が実行します。

承認プロセスの各段階でドキュメントが関連付けられるさまざまな状態を示すステータスには、次のものがあります。

ドラフト

新しいドキュメントです。

発行済み

承認サイクルを一巡し、ナレッジベースの一部として表示可能となったドキュメントです。

Rework-Draft バージョン

ドキュメントのコピーの再作業バージョンです。検証および再発行後にナレッジベースで置き換えられます。

廃止済み

有効期限になったドキュメントです。独自のステータスを作成することもできます。これは後からタスクに関連付けます。

承認プロセス マネージャ

ナレッジ管理者は、承認プロセス マネージャを使用して以下のアクションを実行することができます。

- ナレッジ ドキュメントを読み込みできるグループと書き込み（または、編集）できるグループが決定されます。
- テンプレートを使用して作成されたドキュメントのライフサイクルを決定する、承認プロセス テンプレートのタスクを識別します。
- 承認プロセス中にドキュメントと関連付けることができるさまざまなステータスを定義します。

重要: ナレッジ ドキュメントを作成する場合、ドキュメント許可には後で承認プロセスを介してドキュメントに割り当てることができるユーザが含まれることを確認します。 そのグループからのユーザには、ドキュメントを表示する許可が必ずしも必要ではありません。 ドキュメントが特定のユーザに割り当てられる場合、デフォルトのデータ パーティションの制約を使用すると、ユーザはドキュメントを表示することができます。

ドキュメント編集のための承認プロセスの定義

ナレッジ管理者は、承認プロセスの前、および発行の後にドキュメントを編集できるユーザを指定できます。

注: 完全な（読み取り/書き込み）権限を持つユーザは発行されたドキュメントを編集できます。

ドキュメント編集のための承認プロセスを定義する方法

1. [管理] タブで、[ナレッジ] - [承認プロセス マネージャ] - [承認プロセス設定] を参照します。
[承認プロセス設定] ページが表示されます。

2. ドキュメントが発行される *前* にドキュメントを編集できるユーザを指定します。以下のいずれかのオプションを選択します。

タスクの担当者、担当者、またはユーザが適切なアクセス タイプ ビューで編集可能

以下の連絡先がドキュメントを編集できることを指定します。

- 現在のタスクに割り当てられている連絡先
- 現在のタスクのドキュメントの担当者として指定されている連絡先
- ナレッジマネージャ
- システム管理者

完全な権限を持つユーザが編集可能

ドキュメントへの書き込み許可があるユーザはドキュメントを編集できることを指定します。

3. ドキュメントが発行された *後* でドキュメントを編集できるユーザを指定します。以下のいずれかのオプションを選択します。

完全な権限を持つユーザは、発行済みドキュメントの編集が可能

完全な権限を持つユーザは、発行済みドキュメントを編集できることを指定します。

完全な権限を持つユーザは、発行済みドキュメントの属性を変更可能

ドキュメントへの書き込み許可を持つユーザは、構成アイテムまたは製品のような発行済みドキュメントの属性のみを変更できることを指定します。

ドキュメントの編集前に発行停止する必要がある

ドキュメントを編集する前に、ユーザがそれを発行停止にする必要があることを指定します。

[保存] をクリックします。

承認プロセスが定義されます。

承認プロセス テンプレートの作成

承認プロセス テンプレートのタスクは、テンプレートを使用して作成されたドキュメントのライフサイクルを定義します。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。

承認プロセス テンプレートを作成するには

1. [管理] タブから、[ナレッジ] - [承認プロセス マネージャ] - [承認プロセス テンプレート] を選択します。
[承認プロセス テンプレート リスト] が表示されます。
2. [新規作成] をクリックします。
[承認プロセス テンプレートの詳細] ページが表示されます。
3. テンプレートの名前および説明を入力します。
4. [保存] をクリックします。
[承認プロセス テンプレート詳細] ページに追加フィールドが表示されます。
5. このテンプレートを使用して、ドキュメントのリワーク バージョンを作成する場合、実行するタスクを選択します。
6. このテンプレートを使用して作成されたドキュメントの廃止を解除するときに実行するタスクを選択します。
7. [タスクの挿入] をクリックして、テンプレートに追加するタスクを作成します。
[新規タスクの作成] ページが表示されます。
8. フィールドに必要なデータを入力します。以下のフィールドには説明が必要です。

タスク

タスクに名前を付けます。

担当者

担当者をタスクに割り当てます。 検索アイコンをクリックして名前を選択できます。

注: タスクが作成された後で、[担当者の代替のリストを追加](#) (P. 1130) できます。

[保存] をクリックします。

承認プロセス テンプレートが作成されます。

関連項目:

[タスクへのその他担当者の追加](#) (P. 1130)

[承認プロセス テンプレートの編集](#) (P. 1131)

[承認プロセス テンプレートの検索](#) (P. 1131)

タスクへのその他担当者の追加

タスクを編集する場合、その他担当者を追加できます。

タスクにその他担当者を追加する方法

1. [承認プロセス テンプレート] リストから編集するタスクを選択します。
[タスクの詳細] ページが表示されます。
2. 必要に応じてフィールドを編集します。
3. 担当者リストで [追加] ボタンをクリックします。
[担当者の新規作成] ページが表示されます。
4. [担当者] フィールドで、タスクに割り当てる担当者の名前を入力するか、または検索アイコンをクリックして名前を選択します。
5. 必要に応じて手順 4 を繰り返してその他担当者のリストを作成します。
6. [保存] をクリックします。
その他担当者がタスクに追加されます。

承認プロセス テンプレートの編集

承認プロセス テンプレートを編集できます。

承認プロセス テンプレートを編集するには

1. [管理] タブから、[ナレッジ] - [承認プロセス マネージャ] - [承認プロセス テンプレート] を選択します。
[承認プロセス テンプレート リスト] が表示されます。
2. 編集するテンプレートを選択し、その名前をクリックします。
[承認プロセス テンプレートの詳細] ページが表示されます。
3. [編集] をクリックします。
[承認プロセス テンプレートの更新] ページが表示されます。
4. 必要に応じてフィールドを編集します。
5. [保存] をクリックします。
承認プロセス テンプレートが更新されます。

承認プロセス テンプレートの検索

検索条件を入力して [承認プロセス テンプレート] にフィルタを適用することによって、必要なアイテムのみを表示できます。また、個々のアイテムを検索して表示または編集することもできます。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナントデータから除外するか、テナントデータに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

承認プロセス テンプレートを検索するには

1. [管理] タブから、[ナレッジ] - [承認プロセス] - [承認プロセス テンプレート] を選択します。
[承認プロセス テンプレート リスト] ページが表示されます。
2. [フィルタを表示] をクリックします。
3. 該当するテンプレート名の最初のいくつかの文字を入力します。

4. (オプション) [詳細] をクリックします。

追加フィールドが表示され、[承認プロセス テンプレート リスト] に表示されるアイテムを制限できます。

5. [検索] をクリックします。

[承認プロセス テンプレート リスト] ページに、検索条件に一致するアイテムが表示されます。項目を選択して、表示または編集できます。

注: リスト結果は、Excel にエクスポートして CA SDM の外部で使うことができます。エクスポートするには、リスト ページの [エクスポート] ボタンをクリックします。

ドキュメント ステータスの定義

ユーザ定義のドキュメント ステータスを追加および削除できます。また、事前定義のドキュメント ステータスの名前および説明を変更できます。

関連項目:

[ドキュメント ステータスの作成](#) (P. 1132)

[ドキュメント ステータスの検索](#) (P. 1133)

[ドキュメント ステータスの編集](#) (P. 1133)

ドキュメント ステータスの作成

CA SDM システムに含まれるナレッジ ドキュメントに使用するドキュメント ステータスを作成できます。

ドキュメント ステータスを作成する方法

1. [管理] タブで、[ナレッジ] - [承認プロセス マネージャ] - [ドキュメント ステータス] を選択します。

[ドキュメント ステータス リスト] が表示されます。

2. [新規作成] をクリックします。

[ドキュメント ステータスの詳細] ページが表示されます。

3. ステータスの名前と説明を入力します。

4. [保存] をクリックします。

ドキュメント ステータスが作成されます。

ドキュメント ステータスの検索

検索条件を入力して [ドキュメント ステータス リスト] にフィルタを適用することによって、必要なアイテムのみを表示できます。また、個々のアイテムを検索して表示または編集することもできます。

ドキュメント ステータスを検索する方法

1. [管理] タブで、[ナレッジ] - [承認プロセス マネージャ] - [ドキュメント ステータス] を選択します。
[ドキュメント ステータス リスト] ページが表示されます。
2. [フィルタを表示] をクリックします。
3. 検索するステータス名の最初の数文字を入力します。
4. (オプション) [詳細] をクリックします。
追加のフィールドが表示されます。これらのフィールドを使用して、[ドキュメント ステータス リスト] に表示されるアイテムを制限できます。
5. [検索] をクリックします。
[ドキュメント ステータス リスト] ページに、検索条件に一致するアイテムが表示されます。項目を選択して、表示または編集できます。

注: リスト結果は、Excel にエクスポートして CA SDM の外部で使うことができます。エクスポートするには、リスト ページの [エクスポート] ボタンをクリックします。

ドキュメント ステータスの編集

ドキュメント ステータスを編集できます。

ドキュメント ステータスを編集する方法

1. [管理] タブで、[ナレッジ] - [承認プロセス マネージャ] - [ドキュメント ステータス] を選択します。
[ドキュメント ステータス リスト] が表示されます。
2. 編集するステータスを選択し、その名前をクリックします。
[ドキュメント ステータスの詳細] ページが表示されます。
3. [編集] をクリックします。
[ドキュメント ステータスの更新] ページが表示されます。

4. 必要に応じて [ステータス] フィールドおよび [説明] フィールドを編集します。
5. [保存] をクリックします。
ドキュメントステータスが更新されます。

自動ポリシー

管理者は、自分で定義したドキュメントライフサイクルのポリシーとアクションに基づいて、ナレッジドキュメント承認プロセスの特定のタスクを自動化できます。タスクを自動化することによって、解決策を求めているエンドユーザは問題をより速く解決できるようになります。また、他のユーザに問い合わせなくても問題を解決できるため、組織にとっても有益です。

自動ポリシーは、イベントおよびマクロと連携して機能します。

関連項目:

[自動ポリシーの表示](#) (P. 1134)

[自動ポリシーをセットアップする方法](#) (P. 1136)

[自動ポリシーの作成](#) (P. 1136)

[自動ポリシーの編集](#) (P. 1137)

[自動ポリシーのスケジュール](#) (P. 1138)

[ドキュメントライフサイクルポリシー レポートの表示](#) (P. 1139)

自動ポリシーの表示

自動ポリシーには、ドキュメントのライフサイクルプロセスのさまざまなステージ全体を通して、ドキュメントに修正のフラグを付ける条件、および発行または廃止用に昇格する条件を記述します。たとえば、壊れたリンクのあるナレッジベース内のドキュメントと一致する「壊れたリンクの修正」デフォルトポリシーを指定できます。問題を修正するタスクを、アナリストに割り当てることができます。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナント データから除外するか、テナント データに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

自動ポリシーを表示するには、[管理] タブ、[ナレッジ] - [自動ポリシー] - [ポリシー] を選択します。

[自動ポリシー リスト] ページには自動ポリシーの詳細が表示されます。デフォルト ポリシーを編集するか、または独自のポリシーを定義することができます。ポリシーはそれぞれ以下のコンポーネントに関連付けられます。

ストアドクエリ

ポリシーが処理中にドキュメントを識別して一致する場合、実行する一連のアクション マクロを含んでいます。処理後に、ストアドクエリ条件イベントは、役割ベースのナレッジ マネジメント ライフサイクル ポリシー レポートを **CA SDM** スコアボードに表示します。

管理者は、レポートを監視して、該当するドキュメント エディタにフィードバックおよびアドバイスを提供する責任を負います。

アクション マクロ

ユーザがフラグを設定したり、優先度を増加させたり、その他のアクションを実行することができるコードが含まれています。[マクロ] リストに表示されるマクロを変更するか、独自のマクロを作成することができます。

注: リスト結果は、Excel にエクスポートして **CA SDM** の外部で使うことができます。エクスポートするには、リスト ページの [エクスポート] ボタンをクリックします。

関連項目:

[ドキュメント ライフサイクル ポリシー レポートの表示 \(P. 1139\)](#)
[自動ポリシーのスケジュール \(P. 1138\)](#)

自動ポリシーをセットアップする方法

管理者は以下の手順を実行することにより、自動ポリシー機能をセットアップできます。

1. (必須) ナレッジマネジメント ライフサイクル ポリシー レポートを表示するのに必要なデータを示すために、バックグラウンドサーバ上で実行する自動ポリシー スケジューラにバッチ プロセスを定義する必要があります。このアクションの手順は、ナレッジ レポート カードにも適用されます。

注: 自動ポリシーの詳細については、「実装ガイド」を参照してください。

2. (必須) セキュリティと役割管理のため、[役割管理] の [ナレッジ ドキュメントの見やすさ] タブで、ドキュメントのライフサイクル中にユーザがドキュメントの表示や検索に使用する段階を定義します。
3. [自動ポリシー リスト] ページでは、デフォルトのポリシーを編集するか、独自のポリシーを定義することができます。

注: 新しいポリシーの場合、管理者はストアドクエリに [ライフ サイクル ポリシーを無視] フィールドを含める必要があります。そうしないと、このフィールドが [属性] タブに表示されません。

自動ポリシーの作成

アクションが発生するとアクティブになる自動ポリシーを作成できます。アクションとしては、ドキュメントの発行やドキュメントのナレッジ ベースからの廃止などが挙げられます。

注: マルチテナンシーがインストールされている場合は、ドロップダウン リストから適切なテナントを選択します。パブリック (共有) オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。

自動ポリシーを作成する方法

1. [管理] タブで、[ナレッジ] - [自動ポリシー] - [ポリシー] を参照します。

[自動ポリシーの新規作成] ページが開きます。

2. 該当するフィールドにポリシーの名前または説明を入力します。
3. ストアドクエリ名を入力するか、または検索アイコンを使用して選択します。
4. [アクションの追加] をクリックします。
[マクロ リスト] ページが表示されます。
5. [マクロ リスト] ページで、事前定義済みアクション マクロのうちの1つを選択するか、または独自のマクロを定義 ([新規作成] をクリック) します。
アクション マクロが [自動ポリシーの新規作成] ページの [アクション情報] リストに表示されます。
注: アクションマクロを削除できます。名前を右クリックし、ショートカットメニューから [削除] を選択します。
6. [保存] をクリックします。
新しいポリシーが [自動ポリシー] リストに表示されます。
7. (オプション) タイトルを右クリックして、ポリシーを編集します。
選択したポリシーは [ポリシーの更新] ページに表示されます。また、それを編集できます。

自動ポリシーの編集

自動ポリシーを更新できます。

自動ポリシーを編集するには

1. [管理] タブで、[ナレッジ] - [自動ポリシー] - [ポリシー] を参照します。
[自動ポリシー リスト] が表示されます。
2. 編集するポリシーを右クリックし、ショートカットメニューから [編集] を選択します。
[Update Automated Policy] ページが表示されます。
3. 必要に応じて入力フィールドを編集します。
4. [保存] をクリックします。
自動ポリシーは更新されます。

自動ポリシーのスケジュール

CA SDM が計算を実行し、ポリシーのバッチ処理を実行する日付および時間を指定できます。

自動ポリシーを予定する方法

1. [管理] タブを選択して、[ナレッジ] - [自動ポリシー] - [スケジューリング] を参照します。

[自動ポリシー] ページが表示されます。

2. 以下のフィールドを指定します。

最終更新日

[計算の実行] チェック ボックスを指定します。

スケジュール

テキスト ボックスまたはカレンダーのいずれかに日付を指定します。CA SDM が計算を実行し、ポリシーを実行する時間間隔を選択できます。

[保存] をクリックします。

指定された日時にポリシーが処理されます。

ドキュメントライフサイクル ポリシー レポートの表示

自動ポリシーが生成するドキュメント ライフサイクル ポリシー レポートを表示できます。

レポートを表示するには、[Service Desk] タブを選択し、[ナレッジ ドキュメント] - [自動ポリシー] - [ポリシー] を選択します。

ポリシーを選択する場合、以下の概要情報が [ドキュメント リスト] ページに表示されます。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナント データから除外するか、テナント データに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

タイトル

修正用にフラグが設定されたドキュメントや、発行または廃止用に昇格されたドキュメントのタイトルが表示されます。

ポリシー/アクション

ポリシー名、およびポリシーに定義されたアクション コンテンツを表示します。

属性

ポリシーの影響を受けるドキュメントのプロパティを表示します。

ナレッジドキュメントの制御

ナレッジドキュメントを開いてコメントを追加し、ナレッジをサブミットして、ナレッジツリードキュメントを表示します。また、テンプレートを選択してドキュメントのコンテンツや外観を指定することもできます。

管理者は、以下のタスクを実行して、ユーザによるドキュメントの操作方法を制御できます。

- ナレッジドキュメントやエンドユーザインターフェースのドロップダウンリストに表示される [コメントタイプ](#) (P. 1141) を定義します。
- ドキュメントのコメント、ナレッジのサブミット、およびドキュメントの表示に関する [設定](#) (P. 1207) を指定します。
- ドキュメントのコンテンツと外観を指定する [ドキュメントテンプレート](#) (P. 1148) を作成します。
- 別のリソースまたはシステムからナレッジコンテンツをエクスポート（またはインポート）します。高可用性設定では、CA SDM Web UI を使用してアプリケーションサーバからエクスポートまたはインポートすることはできません。アプリケーションサーバを使用してエクスポートまたはインポートするには、パッケージが UNC 共有ドライブ内に存在する場合は pdm_kit または pdm_ket ユーティリティを実行します。
- ドキュメントの [バージョン管理](#) (P. 1068) 機能を管理します。
- [ナレッジドキュメントのスケジュール](#) (P. 1073) を管理します。

関連項目：

[コメントタイプ](#) (P. 1141)

[ドキュメントテンプレート](#) (P. 1148)

[ナレッジドキュメントリンクを作成する方法](#) (P. 1157)

[ナレッジカテゴリ](#) (P. 1159)

[レポートおよびメトリック](#) (P. 1171)

[検索](#) (P. 1173)

[解決策に関する調査](#) (P. 1203)

コメントタイプ

アナリストは、ドキュメントのコンテンツに入力ミスや問題を発見した場合に、ドキュメントの修正を求めるコメントを追加し、その問題のフォローアップを別のアナリストに割り当てることができます。

管理者は、エンドユーザ インターフェースの各種リスト ビューに表示されるコメント タイプを定義できます。

コメント タイプの表示

ユーザは、ナレッジ ドキュメントを開いたときに、ドキュメントの修正、昇格、廃止などを求めるコメントを追加できます。 [コメント タイプ リスト] ページでは、コメント タイプの詳細を管理できます。

このページを表示するには、[管理] タブで、[ナレッジ] - [ドキュメント] - [コメント タイプ] を選択します。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナント データから除外するか、テナント データに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

[コメント タイプ リスト] ページが表示され、以下の列が表示されます。

名前

ドキュメントやエンドユーザ インターフェースのドロップダウン リストに表示されるコメント タイプのリストを表示します。以下のデフォルトのコメント タイプを編集するか、独自のコメント タイプを定義できます。

- 壊れたリンク
- 発行候補
- コンテンツが不明瞭
- 検索困難
- 一般コメント

- 情報が不正確
- 情報不足
- 新規コンテンツの推奨
- レビュー
- 解決策が機能しない

ユーザビューで表示

ユーザ インターフェース内のさまざまなリスト ビューにコメントを表示します。

フォローアップ必要

ユーザがこのタイプのコメントに応答する必要があるかどうかを指定します。

完了までの期間 (日数)

ユーザがこのタイプのコメントを事後確認する必要がある日数を定義します。

ステータス

このコメント タイプがアクティブであるか、非アクティブであるかを示します。

このページには、以下のボタンがあります。

検索

名前でアイテムを検索します。

フィルタを表示

[コメント リスト] ページ内のコメントを検索します。1 つ以上の検索フィールドにデータを入力し、[検索] をクリックします。[コメント タイプ リスト] ページに、検索条件に一致するアイテムが表示されます。

フィルタのクリア

フィルタをクリアします。

新規作成

コメント タイプを作成します。

注: リスト結果は、Excel にエクスポートして CA SDM の外部で使うことができます。エクスポートするには、リスト ページの [エクスポート] ボタンをクリックします。

コメント タイプの作成

[コメント タイプの新規作成] ページで、エンド ユーザ インターフェースの各種リスト ビューに表示されるコメント タイプを定義できます。

注: マルチテナンシーがインストールされている場合は、ドロップダウン リストから適切なテナントを選択します。パブリック (共有) オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

コメント タイプを作成する方法

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [コメント タイプ] を選択します。
[コメント タイプ リスト] ページが表示されます。
2. [新規作成] をクリックします。
[コメント タイプの新規作成] ページが表示されます。
3. 必要に応じてフィールドにデータを入力します。以下のフィールドには説明が必要です。

完了までの期間 (日数)

ユーザがこのタイプのコメントを事後確認する必要がある日数を定義します。

ユーザ ビューで表示

ユーザ インターフェース内のさまざまなリスト ビューにコメントを表示します。

フォローアップ必要

ユーザがこのタイプのコメントに応答する必要があるかどうかを指定します。

[保存] をクリックします。

新しいコメントタイプが [コメント タイプ List] ページに表示されます。

コメントタイプの編集

作成されて [コメント タイプ リスト] ページに表示されているコメントタイプは、編集できます。

コメントタイプを編集する方法

1. [コメント タイプ] リストで、以下のいずれかを行います。
 - コメントを選択し、[コメント タイプの詳細] ページで [編集] を選択します。
 - コメントを右クリックし、ショートカットメニューから [編集] を選択します。

コメント タイプの詳細ページが表示されます。

2. 必要に応じてフィールドにデータを入力します。
3. [保存] をクリックします。

更新されたコメントタイプが [コメント タイプ リスト] ページに表示されます。

ドキュメント通知

CA SDM では、連絡先と呼ばれるユーザのリストをセットアップできます。特定のイベントの発生時に、このユーザに対して通知を行うことができます。通知プロセスによって、各個人にドキュメントのステータスの変化が通知され、全員がその進捗に関して最新の情報を得られます。ドキュメントに指定された通知を送信できるのは、このリストに表示されるユーザに対してのみです。

フォローアップ コメント通知のセットアップ

[アクティビティ通知リスト] ページに一覧表示されるいくつかのデフォルトのアクティビティ通知を使い、フォローアップ コメントがユーザに割り当てられる場合にユーザへ通知するようセットアップできます。

スコアボード上の [フォローアップ コメント] キューは、割り当て済みおよび未割り当ての事後確認コメントのリポジトリです。

フォローアップ コメント通知をセットアップするには、以下の手順に従います。

1. [管理] タブで、[通知] - [アクティビティの通知] を参照します。
[アクティビティ通知リスト] ページが表示されます。
2. 以下のアクティビティの通知からいずれかを選択します。
 - フォローアップ コメントの割り当て
 - フォローアップ コメントのクローズ[アクティビティ通知の詳細] ページが表示されます。
3. [編集] をクリックします。
[アクティビティ通知の更新] ページが表示されます。
4. 必要に応じてフィールドを変更します。
5. [保存] をクリックします。
[アクティビティ通知の詳細] ページが表示されます。
6. [ウィンドウを閉じる] をクリックします。
変更したアクティビティ通知は、リストを再表示したときに [アクティビティ通知リスト] に表示されます。

ドキュメント設定の指定

システム管理者であれば、コメント、ナレッジのサブミット、およびナレッジツリー ドキュメントの表示に関する設定を指定できます。

ドキュメント設定を指定するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [ドキュメント設定] を選択します。
[ドキュメント設定] ページが表示されます。

2. 以下のフィールドを指定します。

ナレッジ ツリー ドキュメント ビュー

ナレッジ ツリー ドキュメントを開く表示モードを指定します。

「ツリー モードで開く」（デフォルト）を選択してナレッジ ツリーを直接開くか、または「ドキュメント モードで開く」を選択してドキュメント ビューでドキュメントを開きます。「ドキュメント モードで開く」を選択する場合は、「表示」をクリックしてナレッジ ツリーを表示させます。

コメント

ユーザがドキュメントのコメントをサブミットできるかどうか、およびドキュメントのコメントを表示できるかどうかを指定します。以下のいずれかのオプションを選択します。

- コメントのサブミットおよびコメントの表示を許可（デフォルト） - 開いているドキュメントの下部に「コメント」フィールドが表示され、ドキュメント用のコメントをサブミットできるようになります。開いているドキュメントにすでに関連付けられているコメントを表示できます。
- コメントのサブミットを許可、コメントの表示は不可 - 開いているドキュメントの右側に「コメント」フィールドが表示され、ドキュメント用のコメントをサブミットできるようになります。開いているドキュメントにすでに関連付けられているコメントは表示できません。
- コメントのサブミットも表示も不可 - コメントのサブミットも表示もできません。開いているドキュメントに「コメント」フィールドは表示されません。

ナレッジのサブミット

ユーザがサブミットしたドキュメント用のリポジトリを定義します。「添付ファイル ライブラリ」ペインで定義されたリポジトリの名前リストが生成されます。

以下の情報について検討します。

- 所有者が存在するカテゴリに属するドキュメントをアナリストが作成し、そのドキュメントをカテゴリ担当者に割り当てる場合。

カテゴリ担当者がそのドキュメントの担当者および所有者になります。

カテゴリ担当者はドキュメント割り当て通知を受信します。

- 所有者が存在しないカテゴリに属するドキュメントをアナリストが作成し、そのドキュメントをカテゴリ担当者に割り当てる場合。

そのドキュメントの担当者または所有者となる人は存在しません。

管理者の定義にしたがって KD 通知が送られます。

- アナリストがドキュメントを作成し、そのドキュメントをカテゴリ担当者に割り当てる場合。

そのユーザが担当者および所有者になります。

通知は送られません。

- 従業員または顧客が新しいドキュメントを作成した場合は、最初の 2 項目で述べられたアクションが CA SDM によって実行されます。

解決方法の最大サイズ

ドキュメントの [解決方法] フィールドに入力できる最大文字数を定義します。

制限： 指定可能な最大文字数は 256000 です。

デフォルト： 32768.

重複ドキュメントの回避

ユーザがナレッジ ドキュメントを作成する場合、類似ドキュメントの検索が強制的に実行されます。

期限切れ前の通知

ドキュメントが期限切れとなって通知が送信されるまでの日数を定義します。

デフォルト： 7

注： この値が適用されるのは、CA SDM で更新または作成されたドキュメントのみです。CA SDM r11.2 からドキュメントをマイグレートし、その有効期限がマイグレーションより前に設定されている場合、マイグレーションの後にドキュメントを更新しなければ、または更新するまでの間、このオプションは適用されません。

[保存] をクリックします。

ナレッジドキュメントまたはナレッジツリードキュメントを開くときに、変更が適用されます。

ドキュメントテンプレート

ドキュメントテンプレートは、ナレッジドキュメントのフォーマットやデフォルト コンテンツの管理に使うことができます。 どのナレッジドキュメントも、ドキュメントテンプレートを使ってプロパティや表示したときのデザインを定義します。デフォルトでは、新しいナレッジドキュメントにはビルトインのテンプレートが関連付けられています。

テンプレートエディタでは、以下を実行できます。

- ドキュメントテンプレートを設計する。作成したテンプレートは、[ドキュメントエディタ] ページの [コンテンツ] タブでドキュメントに関連付けることができます。
- ビルトインテンプレートおよび他のテンプレートを変更する
テンプレートを編集し、ドキュメントに関連付けるテンプレートを作成できます。 プロパティ オプションを選択できるほか、HTML エディタを使ってヘッダと本文の各セクションを編集できます。
- 親子リンクなどの[ナレッジ関係](#) (P. 1156)をサポートするように、以前のリリースのドキュメントテンプレートを更新します。

ドキュメントテンプレートの作成

ドキュメントテンプレートは、ナレッジベース内のドキュメントのコンテンツおよびデザインを指定します。 デフォルトのテンプレートを適用できます。

- ビルトインのナレッジドキュメント
- ビルトインのナレッジツリー
- ビルトイン - クイック編集

ドキュメント テンプレートを作成してドキュメントに関連付けない限り、ナレッジドキュメントとナレッジツリー ドキュメントの作成には、デフォルトのテンプレートが使用されます。

注: ナレッジドキュメントを作成している間に、ドロップダウンリストから適切なテナントを選択してください。パブリック（共有）オプションを指定すると、すべてのテナントで利用できるオブジェクトが作成されます。

ドキュメントテンプレートを作成するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [ドキュメントテンプレート] を参照します。
[ドキュメントテンプレート リスト] ページが表示されます。
2. [新規作成] をクリックします。
[ドキュメントテンプレートの新規作成] ページが表示されます。
3. 以下のフィールドを指定します。

テンプレート

(必須) テンプレート固有の名前を定義します。

詳細

現在のテンプレートを使用して作成したドキュメントに表示される静的コンテンツが表示されます。[HTML ソース] オプションを選択すると、[本文] フィールドで、本文の HTML コードを直接編集できます。[クイック表示] オプションを選択すると、[本文] フィールドは読み取り専用になり、実行時の表示と同様の、本文の静的なコンテンツが表示されます。

4. (オプション) [デフォルト値の設定] をクリックします。

[デフォルト値テンプレート] ページが表示されます。

ドキュメントを作成するときに、デフォルト値を設定できます。既存のドキュメント上でテンプレートを変更しても、影響はありません。

5. (オプション) ご使用のテンプレートに表示されている、[タイトル]、[概要]、[問題]、または[解決方法] といったフィールドを非表示にします。

質疑応答型のテンプレートのように単純なドキュメントが必要な場合、これらのフィールドを非表示にします。

6. [詳細の編集] をクリックします。

[HTML エディタ] ページが表示され、テンプレートを使用するドキュメントの静的コンテンツおよびレイアウトが指定できます。プレースホルダ タグを挿入するには、ツールバーを使用して、コードを編集します。

重要: テンプレートから、TAG_PARENT タグおよび TAG_RELATED タグを削除することにより、親、子および関連するリンクのようなナレッジ関係を削除できます。

7. [OK] をクリックします。

[詳細] フィールドには更新済みのコンテンツが表示されます。

8. (オプション) [クイック表示] をクリックします。

テンプレートに基づいて、ドキュメントに表示されると同じようにコンテンツが表示されます。

9. (オプション) [HTML 表示] をクリックします。

HTML コードとしてコンテンツが表示されます。

10. [保存] をクリックします。

[ドキュメントテンプレートの詳細] ページが表示されます。

11. [ウィンドウを閉じる] をクリックします。

テンプレートを使用する新規ドキュメントには、新規のコンテンツおよびレイアウトが表示されます。

テンプレートの名前は、リストを表示し直すと [テンプレート リスト] に表示されます。

注: テンプレートを使用しているドキュメントに加えた変更は、システムにログインすることにより新しいセッションが開始された後に表示されます。

ドキュメントテンプレートの編集

ナレッジマネジメントを使用すると、テンプレートの名前、レイアウトおよびコンテンツが編集できます。

ドキュメントテンプレートを更新するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [ドキュメントテンプレート] を参照します。

[ドキュメントテンプレート リスト] ペインが表示されます。

2. テンプレート名を選択します。

[ドキュメントテンプレートの更新] ページが表示されます。

3. [詳細の編集] をクリックします。

HTML エディタが開きます。

4. テンプレートの名前、コンテンツまたはレイアウトを変更します。以下のフィールドを変更することができます。

テンプレート

テンプレート固有の名前を定義します。このフィールドは必須です。

詳細

現在のテンプレートを使用して作成したドキュメントに表示される静的コンテンツが表示されます。[HTML ソース] オプションを選択すると、[本文] フィールドで、本文の HTML コードを直接編集できます。[クイック表示] オプションを選択すると、[本文] フィールドは読み取り専用になり、実行時の表示と同様の、本文の静的なコンテンツが表示されます。

5. テンプレートを使用するドキュメントの静的コンテンツおよびレイアウトを指定するには、[詳細の編集] をクリックします。

[HTML エディタ] ウィンドウが開きます。

6. プレースホルダ タグを挿入するには、ツールバーを使用して、コードを編集します。[OK] をクリックします。

[詳細] フィールドには更新済みのコンテンツが表示されます。

7. (オプション) [クイック表示] をクリックします。

コンテンツは、テンプレートに基づいたドキュメント形式で表示されます。

8. (オプション) [HTML 表示] をクリックします。

コンテンツは、HTML コードで表示されます。

9. [保存] をクリックします。

[ドキュメント テンプレートの詳細] ページが表示されます。

10. [ウィンドウを閉じる] をクリックします。

テンプレートを使用する新規ドキュメントには、新規のコンテンツおよびレイアウトが表示されます。

テンプレートの名前の変更は、リストを更新するときにリストに表示されます。

ドキュメント テンプレートの一覧表示

[ドキュメント テンプレート リスト] ページでは、ナレッジベースのドキュメントのコンテンツおよびデザインを指定するドキュメント テンプレートを作成および管理することができます。

以下のデフォルトのテンプレートが、製品と共にインストールされます。

- ビルトインのナレッジ ドキュメント
- ビルトインのナレッジ ツリー
- ビルトイン - クイック編集

ドキュメント テンプレートを作成してドキュメントに関連付けない限り、ナレッジ ドキュメントとナレッジ ツリー ドキュメントの作成には、デフォルトのテンプレートが使用されます。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナント データから除外するか、テナント データに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

ドキュメント テンプレートを一覧表示するには、[管理] タブから、[管理] - [ナレッジ] - [ドキュメント] - [ドキュメント テンプレート] を選択します。

[ドキュメント テンプレート リスト] ページが表示されます。このページには以下の列が含まれます。

テンプレート名

現在、本製品で定義されているドキュメント テンプレートが一覧表示されます。テンプレート名を選択して、[ドキュメント テンプレートの更新] ウィンドウを開きます。テンプレート名を右クリックして、[テンプレート名] ショートカット メニューを開きます。このメニューには、選択したテンプレートを処理するためのコマンドが表示されます。

デフォルト

新規ドキュメントにデフォルトでテンプレートが使用されている場合、またはドキュメントで指定したテンプレートが削除された場合、マークが表示されます。テンプレートをデフォルトに設定するには、テンプレート名を右クリックして、ショートカットメニューから「デフォルトに設定」を選択します。

注: ドキュメントを作成したり、ドキュメントに関連付けられたテンプレートを削除すると、デフォルトのテンプレートがドキュメントに関連付けられます。ただし、「ドキュメントの新規作成」ウィンドウまたは「ナレッジドキュメントの更新」ウィンドウの「属性」タブで別のテンプレートを指定した場合を除きます。

このページには、以下のフィールドがあります。

テンプレート

検索するテンプレートの名前を定義します。このフィールドが表示されるのは、「フィルタを表示」をクリックした場合のみです。

その他の検索指数

検索に使用する追加条件を定義します。このフィールドは、「Knowledge Search」ペインで「詳細」リンクをクリックした場合にのみ表示されます。

このページには、以下のボタンがあります。

フィルタのクリア

ペインまたはウィンドウのすべてのフィルタ フィールドの値を初期設定値に戻します。

新規作成

「ドキュメントテンプレートの新規作成」ウィンドウが開き、新しいドキュメントテンプレートを定義できます。

検索

指定した検索基準に一致する項目の検索を開始します。検索基準を指定しないと、適切なすべての項目（フォルダ/ドキュメント、連絡先、テンプレート、ノイズワード、許可グループなど）が返されます。

フィルタを表示/フィルタを非表示

現在のウィンドウ、ペイン、またはダイアログ ボックス上の項目の検索をフィルタ可能なフィールドの表示/非表示を切り替えます。

注: リスト結果は、Excel にエクスポートして CA SDM の外部で使うことができます。エクスポートするには、リスト ページの [エクスポート] ボタンをクリックします。

ドキュメント テンプレート リストのフィルタ

ドキュメント テンプレートを作成してドキュメントに関連付けない限り、ナレッジドキュメントとナレッジツリー ドキュメントの作成には、デフォルトのテンプレートが使用されます。[ドキュメント テンプレート リスト] ページでは、ナレッジベースのドキュメントのコンテンツおよびデザインを指定するドキュメント テンプレートを作成および管理することができます。このページからテンプレートをフィルタできます。

ドキュメント テンプレート リストをフィルタするには、以下の手順に従います。

1. [管理] タブをクリックします。
[管理] ページが表示されます。
2. [ナレッジ] - [ドキュメント] - [ドキュメント テンプレート] をクリックします。
ドキュメント テンプレート リストが表示されます。
3. 以下のような操作を実行できます。
 - [テンプレート名] の列からテンプレートを選択します。
テンプレートが開きます。
 - 検索機能を使用して、テンプレートを探します。
テンプレートの検索結果が表示されます。
 - 検索をフィルタするには、[フィルタの表示] を選択します。
テンプレート検索がフィルタされます。

ドキュメント テンプレートを更新してナレッジ関係のリンクを表示する

CA SDM の前のリリースのナレッジ ドキュメント テンプレートを更新し、ナレッジ関係を表示できます。{TAG_PARENT} および {TAG_RELATED} タグを追加してテンプレートを変更します。これにより、テンプレートを使用するドキュメントで、親子リンクやテナントなどのドキュメント関係を表示できるようになります。

テンプレートを変更してナレッジ関係を表示する方法

1. ナレッジ ドキュメント テンプレートを開きます。
[ドキュメント テンプレートの更新] ページが表示されます。
2. [編集] をクリックします。
3. HTML ソース ビューを選択します。
注: また、[詳細の編集] をクリックして HTML エディタを開き、{TAG_PARENT} と {TAG_RELATED} タグを追加することもできます。
4. [詳細の編集] ドロップダウンの [テンプレート プレースホルダの選択] を選択し、ドキュメント テンプレートにタグを追加します。
タグがテンプレートに追加されます。
5. テンプレートを保存して閉じます。
テンプレートが更新され、ナレッジ関係が表示されます。

ナレッジドキュメントリンクを作成する方法

ドキュメントリンクを作成することで、ナレッジマネジメント環境を管理できます。ナレッジ関係により、ドキュメント階層を作成できるほか、ナレッジドキュメントへの変更を管理できるようになります。

ナレッジ関係は、以下のように作成できます。

1. ナレッジドキュメントテンプレートを定義し、ビューモードで親子関係を表示、または非表示にします。
2. ナレッジドキュメントを作成、または変更します。

注: デフォルトでは発行停止されたナレッジドキュメントにのみリンクを追加できます。ドキュメントがすでに発行済みの場合は、編集モードまたは再作業モードでドキュメントを開いて、ドキュメントリンクを作成します。ドキュメントの権限は、承認プロセスの前、発行後に変更できます。

3. ナレッジマネジメント環境に合わせて、[関連ナレッジ] タブで以下のドキュメントリンクを必要なだけ作成します。

- ドキュメントを非階層の [参照] としてリンクする

ナレッジドキュメントを他の既存のドキュメントにリンクできます。

- 親または子としてドキュメントをリンクする

ナレッジドキュメントを親子関係でリンクできます。

注: 親ドキュメントを変更すると、子ドキュメントへの影響の可能性を示唆する警告が表示されます。

- グローバルドキュメントをテナントドキュメントにリンクする

ナレッジドキュメントは1つ、または複数のテナントにリンクできます。たとえば、子ドキュメントに、親ドキュメントとは異なるテナントがリンクされている場合があります。

ドキュメントリンクを作成すると [履歴] タブが更新されるため、変更をトラッキングできます。

4. ドキュメントを保存し、ユーザビューでドキュメントを開くとリンクが表示されることを確認します。

ドキュメントリンクが設定している権限に従って表示されていることを確認できます。

親子リンクの作成

ナレッジドキュメントに親子関係を作成できます。親子リンクを使い、環境内のユーザに合わせて関連ドキュメントを整理します。

親子リンクを作成する方法

1. ナレッジドキュメントを作成します。または編集モードでドキュメントを開きます。

ナレッジドキュメントが表示されます。

2. [関連ナレッジ] タブを選択します。

[カテゴリ] ページが表示されます。

注: [類似項目の検索] タブからでもリンクを作成できます。検索基準を使って、ドキュメントを探します。

3. [カテゴリ (X)] ペインでリンクしているドキュメントを探します。

[ドキュメント] ペインでドキュメントを右クリックし、[このドキュメントを親としてリンク] または [このドキュメントを子としてリンク] オプションを選択してドキュメント間にリンクを作成します。

ドキュメントリンクが作成されます。

参照リンクの作成

環境内のナレッジドキュメントに、参照関係を作成できます。参照関係は、環境内でナレッジ階層を管理するために使います。

参照リンクを作成する方法

1. ナレッジドキュメントを作成します。またはリワーク モードでドキュメントを開きます。

ナレッジドキュメントが表示されます。

2. [関連ナレッジ] タブを選択します。

[カテゴリ] ページが表示されます。

注: [類似項目の検索] タブからでもリンクを作成できます。

3. [カテゴリ (X)] ペインでリンクしているドキュメントを探します。

[ドキュメント] ペインでドキュメントを右クリックし、[このドキュメントを参照としてリンク] オプションを選択します。

ドキュメントリンクが作成されます。

ドキュメントリンクの削除

発行停止されたナレッジドキュメントから、親子関係などのリンクを削除できます。ドキュメントがすでに発行されている場合は、ドキュメントを編集またはリワークモードで開いてドキュメントリンクを削除します。

ドキュメントリンクを削除する方法

1. ナレッジドキュメントを開きます。
ドキュメントが表示されます。
2. [編集] をクリックします。
[ドキュメントの更新] ページが表示されます。
3. [関連ナレッジ] タブを選択します。
[カテゴリ] ページが表示されます。
4. [ドキュメントリンク] ペインに移動します。
5. コンテキストメニューの [このリンクを削除] オプションを選択し、リンクを削除します。
ドキュメントリンクが削除されます。

ナレッジ カテゴリ

ナレッジドキュメントは、ナレッジカテゴリに分類されます。ナレッジエンジニア、ナレッジマネージャおよび管理者はカテゴリを管理できます。これらの担当者は、ナレッジマネジメントを使用してカテゴリを作成、コピー、変更します。ただし、カテゴリを削除できるのは、ナレッジマネージャおよび管理者のみです。ナレッジカテゴリにカテゴリ構造を構築すると、サービスデスクの従業員、顧客、およびアナリストが関連ドキュメントへのナビゲーションに使用する、階層構造が作成されます。

各ドキュメントを、プライマリ カテゴリに割り当てます。たとえば、**Microsoft Word** に関連するナレッジは、**Microsoft Word** のカテゴリに追加する必要があります。またナレッジマネジメントでは、ドキュメントを複数の2次カテゴリおよび他のドキュメントに関連付けることもできます。このようにして、さまざまなカテゴリにドキュメントを適切に分類できるので、首尾よく検索結果を得られるようになります。

カテゴリ構造によって、以下の機能が実行されます。

- ナレッジ解決策を管理可能なグループに分類する
- アクセス権の割り当てを容易にする
- FAQ/参照を使用して解決策を検索できるようにする

インシデントからカテゴリの参照機能を使用するには、インシデント領域とナレッジカテゴリが一致している必要があります。ユーザがナレッジドキュメントに基づいてインシデントを作成すると、ドキュメントカテゴリはインシデント領域を設定します。このため、カテゴリとその領域は常に一致します。

- ドキュメントリンクを作成します。リンクしたドキュメントのいずれかを表示すると、[参照] リンクが表示されます。この [参照] リンクを使用すると、リンクされているドキュメント間を直接移動できます。

ナレッジ カテゴリの作成

各カテゴリを対象として、チケットと関連付ける属性や特性を指定したプロパティを定義できます。また、チケットへの対応に必要なタスクをすべて指定したワークフローを作成できます。

カテゴリを使って、チケット内の特定のフィールドにデフォルト値を指定できるほか、サービスタイプのデフォルトをカテゴリに割り当てることで、チケットにサービスレベルを自動的に関連付けることができます。アナリストがチケットにカテゴリを割り当てると、カテゴリに関連付けられたすべての情報がチケットに自動的に関連付けられます。

注: マルチテナンシーを使用している場合は、ナレッジドキュメントの検索フィルタにテナントのドロップダウンリストが表示されます。このドロップダウンリストで <empty> を選択すると、検索がパブリックになります。テナントの列はリストページにも表示されます。

カテゴリを作成する方法

1. [管理] タブで、[ナレッジ] - [ナレッジカテゴリ] を参照します。
[ナレッジカテゴリ] ページが表示されます。
2. 下にカテゴリを作成するカテゴリを右クリックします。ショートカットメニューから [新規カテゴリ] を選択します。
[カテゴリの新規作成] ページに [コンテンツ] タブが表示されます。

3. 必要に応じて[フィールド](#) (P. 1163)にデータを入力します。
4. [許可] をクリックします。
[権限] タブが表示されます。
5. 以下の許可オプションのうち 1 つをカテゴリに対して選択します。

親から継承

新しいカテゴリに親カテゴリと同じ許可が設定されるよう指定します。

注: [カテゴリの作成] ページを開く前にトップ カテゴリを選択すると、[親から継承] オプションは使用できません。

グループによるコントロール

グループにカテゴリ許可を指定し、カテゴリの読み取り、または書き込みアクセス権を設定します。

役割によるコントロール

役割にカテゴリ許可を指定し、カテゴリの読み取り、または書き込みアクセス権を設定します。

注: グループからロールにカテゴリ許可を変更するなどコントロールを変更する場合、そのカテゴリの前の許可が削除されることを示す警告が表示されます。

全員に書き込み許可を付与

すべてのユーザにカテゴリへの書き込み許可を指定します。書き込み許可があると、カテゴリの編集または削除ができます。

注: [全員に書き込み許可を付与] チェック ボックスをオンにすると、[全員に読み取り許可を付与] チェック ボックスが自動的にオンになります。

全員に読み取り許可を付与

すべてのユーザにカテゴリへの読み取り許可を指定します。読み取り許可では、カテゴリを表示することはできますが、編集や削除はできません。管理者権限があるユーザは、所属する許可グループがフォルダを編集できない場合でも、フォルダを編集できます。カテゴリへのアクセス レベルが異なる複数の許可グループに所属するユーザには、より高いアクセス レベルが付与されます（たとえば、一方のグループに読み取り専用アクセスがあり、別のグループに書き込みアクセスがある場合、ユーザには書き込みアクセスが付与されます）。

注: [全員に書き込み許可を付与] チェック ボックスをオンにすると、[全員に読み取り許可を付与] チェック ボックスが自動的にオンになります。

重要: 全員に許可を与えると、役割でも、グループでも同じようにアクセスできるようになります。許可を保存してから [全員] と [役割によるコントロール] を選択した場合は、[グループによるコントロール] が選択状態になります。

6. (オプション) [使用可能] および [選択済み] リストから特定のグループや役割に読み書き許可を指定します。

このオプションを使って、カテゴリの読み取り許可や書き込み許可を持つ役割とグループを管理します。[使用可能なグループ] / [使用可能な役割] リストから1つ以上の許可グループ、または役割を選択し、[追加] または [削除] ボタンを使って、選択したグループや役割を[書き込み許可があるグループ] / [書き込み許可がある役割] リスト、および[読み取り許可があるグループ] / [読み取り許可がある役割] リストに移動できます。

7. [保存] をクリックします。

[カテゴリの詳細] ページが表示されます。

8. [ウィンドウを閉じる] をクリックします。

[ナレッジカテゴリ] ペインが更新され、新しいカテゴリが表示されます。

関連項目:

[カテゴリ フィールド](#) (P. 1163)

カテゴリ フィールド

タイトル

カテゴリの名前を指定します。

説明

カテゴリの説明を入力します。

カテゴリ担当者

カテゴリの担当者を示します。カテゴリの所有者として定義されている連絡先には、[あなたのカテゴリ] という名前のナレッジ レポートカードのリンクが表示されます。このリンクからは、カテゴリとそこに含まれるドキュメントに関する統計情報を表示できます。また、各カテゴリの担当者は、新しいドキュメントを作成するユーザがアナリストでない場合やアナリストが[カテゴリ担当者の割り当て]を選択して新しいドキュメントを作成した場合に、そのドキュメントのデフォルト所有者になります。

ドキュメント テンプレート

このカテゴリに関連付けられているすべてのドキュメントで使用するドキュメント テンプレートを定義します。 [<空>] オプションを選択すると何も定義されませんが、デフォルトでは事前定義済みテンプレートが使用されます。

承認プロセス テンプレート

このカテゴリに関連付けられているすべての承認プロセスで使用するデフォルト テンプレートを定義します。 承認プロセス テンプレートでは、ドキュメントの発行前に実行する必要があるワークフロー手順を定義します。 デフォルトは [<空>] で、アプリケーションのデフォルト テンプレートが使用されます。

このカテゴリでフォーラムの作成を許可

アナリストがこのカテゴリ内でフォーラムを作成できるかどうか指定します。

[Request/Incident/Problem] エリア

管理者が担当領域を指定する際に定義する、リクエスト/インシデント/問題領域を指定します。 検索アイコンをクリックし、使用可能な領域から選択できます。

案件カテゴリ

管理者が担当領域を指定する際に定義する、案件カテゴリを指定します。 検索アイコンをクリックし、使用可能な領域から選択できます。

カテゴリの変更

ナレッジマネジメント 環境でカテゴリを変更できます。 カテゴリによって、作成後の変更要求や案件の内容が決定されます。 各カテゴリを対象として、チケットと関連付ける属性や特性を指定したプロパティを定義できます。また、チケットへの対応に必要なタスクをすべて指定したワークフローを作成できます。

カテゴリを使って、チケット内の特定のフィールドにデフォルト値を指定できるほか、サービス タイプのデフォルトをカテゴリに割り当てることで、チケットにサービス レベルを自動的に関連付けることができます。アナリストがチケットにカテゴリを割り当てると、カテゴリに関連付けられたすべての情報がチケットに自動的に関連付けられます。

カテゴリを変更する方法

1. [管理] タブで、[ナレッジ] - [ナレッジ カテゴリ] を参照します。
[ナレッジ カテゴリ] ページが表示されます。
2. 変更するカテゴリを右クリックし、ショートカットメニューから [カテゴリの編集] を選択します。
[カテゴリの更新] ページに [コンテンツ] タブが表示されます。
注: トップ カテゴリは削除も変更もできません。
3. 必要に応じて 1 つ以上の [フィールド](#) (P. 1163) を更新します。
4. [許可] をクリックします。
[権限] タブが表示されます。
5. 以下の許可オプションのうち 1 つをカテゴリに対して選択します。

親から継承

新しいカテゴリに親カテゴリと同じ許可が設定されるよう指定します。

注: [カテゴリの作成] ページを開く前にトップ カテゴリを選択すると、[親から継承] オプションは使用できません。

グループによるコントロール

グループにカテゴリ許可を指定し、カテゴリの読み取り、または書き込みアクセス権を設定します。

役割によるコントロール

役割にカテゴリ許可を指定し、カテゴリの読み取り、または書き込みアクセス権を設定します。許可を保存してから [全員] と [役割によるコントロール] を選択した場合は、[グループによるコントロール] が選択状態になります。

注: グループからロールにカテゴリ許可を変更するなどコントロールを変更する場合、そのカテゴリの前の許可が削除されることを示す警告が表示されます。

6. (オプション) カテゴリの読み書き許可を指定します。
このオプションを使って、カテゴリの読み取り許可や書き込み許可を持つ役割とグループを管理します。このオプションを選択するとページが更新され、[全員に書き込み許可を付与] および [全員に読み取り許可を付与] [チェックボックス](#) (P. 1169) が表示されます。

7. [保存] をクリックします。

変更されたカテゴリが [ナレッジ カテゴリ リスト] ページに表示されます。

カテゴリの削除

ナレッジ カテゴリ 構造からカテゴリを削除できます。カテゴリを削除する場合、選択したカテゴリのサブカテゴリおよび関連するドキュメントリンクをすべて削除するかどうかを指定できます。

注: この機能を使用できるのは、システム管理者とナレッジ マネージャのみです。

カテゴリを削除するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ナレッジ カテゴリ] を参照します。
[ナレッジ カテゴリ] ページが表示されます。
2. 削除するカテゴリを右クリックし、ショートカットメニューから [カテゴリの削除] を選択します。
[カテゴリの削除] ページが表示されます。

注: トップ カテゴリは削除また変更できません。

3. (オプション) 以下のいずれかの手順に従います。
 - [サブカテゴリを含める] チェック ボックスをオンにすると、選択したカテゴリのすべてのサブカテゴリが削除されます。
 - [サブカテゴリを含める] チェック ボックスをオフにすると、選択したカテゴリのすべてのサブカテゴリが最も近い使用可能な親カテゴリに移動します。
4. (オプション) 以下のいずれかの手順に従います。
 - [ドキュメントを含める] チェック ボックスをオンにすると、選択したカテゴリのドキュメントが削除されます。 [ドキュメントを含める] チェック ボックスをオンにすると、以下のオプションが表示されます。
 - [プライマリ カテゴリにのみリンクされたドキュメントを削除する] - このオプションを選択すると、[ナレッジ カテゴリ] ページでドキュメントのプライマリ カテゴリとして識別された選択済みカテゴリのドキュメントのみが削除されます。

- **「カテゴリにリンクされたドキュメントをすべて削除する」** -
このオプションを選択すると、選択したカテゴリのすべてのドキュメントが削除されます。
- **「ドキュメントを含める」** チェック ボックスをオンにすると、ドキュメントは選択したカテゴリから最も近い使用可能な親カテゴリに移動します。

[OK] をクリックします。

選択したカテゴリは削除されます。また、[ナレッジ カテゴリ] ペインが更新されます。

カテゴリの移動

カテゴリ、サブカテゴリ、および関連付けられたすべてのドキュメントリンクを、現在のロケーションから別のカテゴリに移動させることができます。

注: この機能は、ナレッジ マネジメント がインストールされている場合のみ使用できます。

カテゴリの切り取りと貼り付け

1. [管理] タブで、[ナレッジ] - [ナレッジ カテゴリ] を参照します。
[ナレッジ カテゴリ] ページが表示されます。
2. 移動させたいカテゴリを右クリックし、ショートカット メニューから [カテゴリの切り取り] を選択します。

選択したカテゴリ、サブカテゴリ、および関連付けられたすべてのドキュメント リンクがメモリに格納されます。

3. 切り取った情報を貼り付けるカテゴリを右クリックし、ショートカット メニューから [カテゴリの貼り付け] を選択します。

切り取ったカテゴリは、元のロケーションから選択したカテゴリの下に移動します。[ナレッジ カテゴリ] ペインが更新され、新しいカテゴリ構造が表示されます。

カテゴリをドキュメント リンク付きでコピー

カテゴリ、サブカテゴリ、および関連付けられたすべてのドキュメントリンクを選択し、元のロケーションから削除することなく、そのコピーを別のカテゴリに配置することができます。

カテゴリをドキュメント リンク付きでコピーし貼り付けるには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ナレッジ カテゴリ] を参照します。
[ナレッジ カテゴリ] ページが表示されます。
2. コピーしたいカテゴリを右クリックし、ショートカット メニューから [ドキュメント リンク付きのカテゴリのコピー] を選択します。
選択したカテゴリ、サブカテゴリ、および関連付けられたすべてのドキュメント リンクがメモリに格納されます。
3. コピーされた情報を貼り付けるカテゴリを右クリックし、ショートカット メニューから [カテゴリの貼り付け] を選択します。
コピーされた情報は、選択したカテゴリの下に表示されます。[ナレッジ カテゴリ] ペインが更新され、新しいカテゴリ構造が表示されます。

カテゴリをドキュメント リンクを付けずにコピー

カテゴリおよびサブカテゴリを選択し、元のロケーションから削除することなく、または関連するドキュメントはコピーしないで、それらのコピーを別のカテゴリに配置することができます。

カテゴリをドキュメント リンクを付けずにコピーし貼り付けるには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ナレッジ カテゴリ] を参照します。
[ナレッジ カテゴリ] ページが表示されます。
2. コピーしたいカテゴリを右クリックし、ショートカット メニューから [カテゴリのコピー] を選択します。
選択したカテゴリおよびサブカテゴリがメモリに格納されます。
3. コピーされた情報を貼り付けるカテゴリを右クリックし、ショートカット メニューから [カテゴリの貼り付け] を選択します。
コピーされた情報は、選択したカテゴリの下に表示されます。[ナレッジ カテゴリ] ペインが更新され、新しいカテゴリ構造が表示されます。

カテゴリの許可の管理

グループまたは役割に基づいて特定の読み取り/書き込み許可を付与することによって、ナレッジマネジメント環境でカテゴリの権限を管理できます。サブカテゴリをカテゴリに表示、編集、削除、または追加できるユーザを指定することができます。

注: ドキュメントとカテゴリに空の書き込み許可を使用することができません。書き込み許可を選択しない場合、空の書き込み許可が設定されます。空の書き込み許可を持つカテゴリおよびドキュメントを変更できるのは、特権ユーザだけです。

カテゴリの権限を管理する方法

1. [管理] タブで、[ナレッジ] - [ナレッジ カテゴリ] を参照します。
[ナレッジ カテゴリ] ページが表示されます。
2. 新規カテゴリを作成するカテゴリの下を右クリックし、ショートカットメニューから [新規カテゴリ] を選択して新規カテゴリの許可を管理します。
[カテゴリの新規作成] ページに [コンテンツ] タブが表示されます。
3. [許可] をクリックします。
[権限] タブが表示されます。
4. 以下の許可オプションのうち 1 つをカテゴリに対して選択します。

親から継承

新しいカテゴリに親カテゴリと同じ許可が設定されるよう指定します。

注: [カテゴリの作成] ページを開く前に [トップ] カテゴリを選択した場合、[親から継承] オプションは使用できません。

グループによるコントロール

グループにカテゴリ許可を指定し、カテゴリの読み取り、または書き込みアクセス権を設定します。

役割によるコントロール

役割にカテゴリ許可を指定し、カテゴリの読み取り、または書き込みアクセス権を設定します。

注: グループから役割に許可を設定するなどしてコントロールを変更した場合、既存の許可が削除されているとの警告が表示されます。

全員に書き込み許可を付与

すべてのユーザにカテゴリへの書き込み許可を指定します。書き込み許可があると、カテゴリの編集または削除ができます。

注: [全員に書き込み許可を付与] チェック ボックスをオンにすると、[全員に読み取り許可を付与] チェック ボックスが自動的にオンになります。

全員に読み取り許可を付与

すべてのユーザにカテゴリへの読み取り許可を指定します。読み取り許可では、カテゴリを表示することはできますが、編集や削除はできません。管理者権限があるユーザは、所属する許可グループがフォルダを編集できない場合でも、フォルダを編集できます。カテゴリへのアクセス レベルが異なる複数の許可グループに所属するユーザには、より高いアクセス レベルが付与されます（たとえば、一方のグループに読み取り専用アクセスがあり、別のグループに書き込みアクセスがある場合、ユーザには書き込みアクセスが付与されます）。

注: [全員に書き込み許可を付与] チェック ボックスをオンにすると、[全員に読み取り許可を付与] チェック ボックスが自動的にオンになります。

重要: 全員に許可を与えると、役割でも、グループでも同じようにアクセスできるようになります。許可を保存してから [全員] と [役割によるコントロール] を選択した場合は、[グループによるコントロール] が選択状態になります。

5. [使用可能] リストおよび[選択済み] リストから特定のグループまたは役割に適切な読み取り/書き込み許可を付与します。

[使用可能なグループ] / [使用可能な役割] リストから1つ以上の許可グループ、または役割を選択し、[追加] または [削除] ボタンを使って、選択したグループや役割を[書き込み許可があるグループ] / [書き込み許可がある役割] リスト、および[読み取り許可があるグループ] / [読み取り許可がある役割] リストに移動できます。

注: 許可リストに追加されたグループまたは役割はすべて、読み取り許可リストに自動的に追加されます。[全員に読み取り許可を付与] チェック ボックスをオンにする場合は、グループまたは役割を読み取り許可リストに追加する必要はありません。

6. [保存] をクリックします。
[カテゴリの詳細] ページが表示されます。
7. [ウィンドウを閉じる] をクリックします。
変更されたカテゴリが[ナレッジカテゴリ] ペインに表示されます。

レポートおよびメトリック

ナレッジベースの有効性の監視には、以下のレポート ツールを使用できます。

- ナレッジ レポート カード
- ナレッジ マネジメント の定義済み Web ベースのレポート
- 役割ベースの Web フォーム

これらのツールを使用すると、ドキュメントの有用性および問題解決時の有効性に関する統計を表示できます。

関連項目:

[ナレッジ レポート カード](#) (P. 1172)

[Web ベースのレポート](#) (P. 1173)

[役割ベースのレポート Web フォーム](#) (P. 1173)

ナレッジ レポート カード

ナレッジ レポート カードには、各エンド ユーザのナレッジに対する貢献度が表示され、どのナレッジ ドキュメントが最も効果的であるかについてのフィードバックが示されます。この情報に基づいて、ナレッジ ドキュメントを作成するプロセスや環境内のエンド ユーザに優れたサポートを提供するプロセスを改善することができます。

ナレッジ レポート カードの統計の定義

[ナレッジ レポート カード] ページでは、ナレッジ レポート カードの計算と通知の送信のスケジュールを定義し、ナレッジ レポート カードの通知電子メールの内容を定義できます。

注: ナレッジ レポート カードの計算が実行されている場合、再作業バージョンおよび廃止されたドキュメントは提供されません。

ナレッジ レポート カードの統計を定義する方法

1. [管理] タブで、[ナレッジ] - [ナレッジ レポート カード] を選択します。

[Report Card] ページが開きます。

2. 必要に応じて以下のフィールドに値を入力します。

最終更新日

レポート カード計算を実行します。

デフォルト: Deactivated

注: 計算が実行されず、データを提示するための統計が収集されなかった場合は、[ナレッジ] タブの[表示] メニューから[ナレッジ レポート カード] コマンドを指定したときに、「レポート カードの計算を実行してください」というメッセージが表示されます。

スケジュール

レポート カードをスケジュールします。

- レポート カードの計算の次回実行日: **xxx** 実行周期: **xxx** -- レポート カード統計を再計算する頻度を指定します。
 - レポート カードの電子メール通知の次回送信日: **xxx** 送信周期: **xxx** -- レポート カード通知を送信する頻度を指定します。
- デフォルト: 実行しない

- レポートカードの電子メールに表示する統計の期間：xxx -- レポートカード通知に情報を表示する時間を指定します。このフィールドは、[レポートカードの電子メール通知の送信周期] リストで[実行しない] 以外の値を選択した場合にのみ表示されます。

デフォルト：365 日

3. [保存] をクリックします。

ナレッジレポートカード統計が定義されます。

Web ベースのレポート

CA Business Intelligence では、定義済みナレッジマネジメントレポートのセットがインストールされます。これらのレポートは、CA SDM をインストールした後に CA Business Intelligence に自動的に展開されます。

レポートは、BusinessObjects Web Intelligence または Crystal Reports を使用して作成されます。承認されたユーザは、CA SDM の [レポート] タブでレポートを表示できます。

役割ベースのレポート Web フォーム

権限を与えられたマネージャまたはアナリストが [レポート] タブの [レポート リスト] アイコンをダブルクリックしたときに表示される、レポート Web フォームを定義できます。

レポート Web フォームは、[管理] - [セキュリティと役割の管理] - [役割管理] を選択し、[役割リスト] を使用して管理します。

検索

管理者は検索機能を使用して、以下のタスクを実行できます。

- ナレッジマネジメント検索エンジンの管理。ノイズワード、特殊用語および同義語を検索に含めるか除外するかの設定の定義。
- ドキュメントを解析するために使用する設定の定義。
- デフォルトの検索設定の定義。

- 検索結果に表示される「推奨ドキュメント」の作成。動的 FAQ のリスト表示を使用して、ユーザの推奨ドキュメントの活用を促進。

注: ドキュメントの権限は、リンクされている添付ファイルの権限と異なることがあります。

関連項目:

[KT 検索エンジン](#) (P. 1174)

[推奨ドキュメント](#) (P. 1187)

[デフォルト検索設定のセットアップ](#) (P. 1191)

[CA SDM インテグレーション オプション](#) (P. 1193)

KT 検索エンジン

CA SDM をインストールすると、KT 検索エンジンがデフォルトに設定されます。ナレッジベースの検索はナレッジドキュメントに制限されます。検索エンジンは、[管理] タブの [ナレッジ] - [検索] - [KT 検索エンジン] ノードにあります。

KT 検索エンジン ノードでは、以下のオプションを管理できます。

- ノイズワード
- 特殊用語
- 同義語

関連項目:

[ナレッジマネジメント 検索の利用](#) (P. 1174)

ナレッジ マネジメント 検索の利用

CA SDM をインストールすると、ナレッジマネジメントの検索エンジンがデフォルトの検索エンジンとして構成されます。ナレッジベースの検索はナレッジドキュメントに制限されます。

すべてのナレッジソースに対するアクセシビリティとデフォルトをユーザ役割に基づいて定義できます。デフォルトでは、ナレッジドキュメントはすべてのユーザ役割で検索できます。

次の手順に従ってください:

1. [管理] タブをクリックします。
[管理] コンソールが表示されます。
2. [オプション マネージャ] - [検索エンジン] をクリックします。
[オプション リスト] が表示されます。
3. ebr_version をクリックします。
[オプションの詳細] ページが表示されます。
[編集] をクリックして、[更新オプション] ページを表示させます。
4. [KT 検索エンジン] を選択します。
5. [保存] - [更新] をクリックします。
[オプションの詳細] ページが選択内容で更新されます。
6. [ウィンドウを閉じる] をクリックします。
7. CA SDM サービスをリサイクルします。

関連項目:

[ノイズワード、同義語および特殊用語 \(P. 1176\)](#)

[ノイズワードの指定 \(P. 1177\)](#)

[ノイズワードの編集 \(P. 1177\)](#)

[ノイズワードの表示 \(P. 1178\)](#)

[特殊用語の指定 \(P. 1179\)](#)

[特殊用語の編集 \(P. 1179\)](#)

[特殊用語の表示 \(P. 1180\)](#)

[同義語の指定 \(P. 1181\)](#)

[同義語の表示 \(P. 1182\)](#)

[同義語の編集 \(P. 1182\)](#)

[パーサ設定 \(P. 1183\)](#)

ノイズワード、同義語および特殊用語

CA SDM で実行される自然言語検索およびキーワード検索に影響する語句（同意語、ノイズワードおよび特殊用語）を定義できます。以下の用語の追加または削除は、ユーザに返される検索結果に重大な影響を及ぼします。

ノイズワード

通常、検索プロセスの役に立つわけではないので無視してもよい語句を指定します。たとえば、「a」、「an」、「the」などの冠詞や「or」、「to」などの前置詞は、一般にノイズワードとして識別されます。[ノイズワードリスト] ページでは、検索結果に影響を与えずにドキュメントおよびクエリで無視する語句を指定できます。

特殊用語

複数の単語で構成される用語、または特殊文字を含んでいる用語で、検索プロセス中は単一の語として識別させたい用語を指定します。たとえば、「TCP/IP」のスラッシュ (/)、「dial-up」のハイフン (-)、「LOCAL_SERVER」の下線など、英数字以外の文字が含まれる語句は、特殊用語として追加できます。どの語句を特殊用語として定義するかは、英数字以外の文字が含まれているために検索プロセス中に分割されてしまう用語について検討して決めます。

同義語

別の語句と同じ意味を持っている語句を指定します。同義語を追加することによって、特定の語句を検索するときに、それに対応する同義語がナレッジベースに存在する場合は、その情報も検索されます。1つの語句に複数の同義語を定義できます。定義したキーワードから反対の組み合わせも自動的に作成されます。たとえば、「コンピュータ」を「PC」の同義語として定義すると、「PC」は「コンピュータ」の同義語として自動的に定義されます。[同義語リスト] ページでは、ドキュメントおよびクエリを解析するときに、同じ意味で使用されるキーワード/同義語ペアを指定できます。キーワード/同義語ペアを指定すると、検索結果が向上します。

注: ノイズワード、特殊用語、同義語、またはパーサ設定を作成、変更、または削除したら、製品に付属の Knowledge Reindex ユーティリティを使用して、ナレッジベースのインデックスを再作成します。

ノイズワードの指定

〔ノイズワードの新規作成〕ページでは、検索結果に影響を与えずに、ドキュメントおよびクエリで無視する語句リストに新しい語句を追加できます。

ノイズワードを指定するには、以下の手順に従います。

1. 〔管理〕タブで、〔ナレッジ〕 - 〔検索〕 - 〔KT 検索エンジン〕 - 〔ノイズワード〕を選択します。
〔ノイズワードリスト〕ページが表示されます。
2. 〔新規作成〕をクリックします。
3. 〔ノイズワードの新規作成〕ページが表示されます。
4. ノイズワードとして定義する語句を〔ノイズワード〕フィールドに入力します。

注: 同義語またはキーワードとして存在するノイズワードを定義することはできません。

5. 〔保存〕をクリックします。

新しいノイズワードは、〔ノイズワードリスト〕ページに表示されます。新しいノイズワードを更新するには、〔編集〕ボタンをクリックします。

注: ノイズワード、特殊用語、同義語、またはパーサ設定を作成、変更、または削除したら、製品に付属の Knowledge Reindex ユーティリティを使用して、ナレッジベースのインデックスを再作成します。

ノイズワードの編集

〔ノイズワードリスト〕ページで作成済みのノイズワードを編集できます。

注: ノイズワード、特殊用語、同義語、またはパーサ設定を作成、変更、または削除したら、製品に付属の Knowledge Reindex ユーティリティを使用して、ナレッジベースのインデックスを再作成します。

ノイズワードを編集するには、以下の手順に従います。

1. 〔ノイズワード〕リストにある編集したいノイズワードを右クリックし、ショートカットメニューから〔プロパティ〕を選択します。
〔ノイズワードの更新〕ページが開きます。

2. [ノイズワード] フィールドに変更を入力します。

注: 同義語またはキーワードとして存在するノイズワードを定義することはできません。

3. [保存] をクリックします。

更新されたノイズワードは、[ノイズワードリスト] ページに表示されます。

注: ノイズワード、特殊用語、同義語、またはパーサ設定を定義、変更、または削除したら、製品に付属の **Knowledge Reindex** ユーティリティを使用して、ナレッジベースのインデックスを再作成します。

ノイズワードの表示

[ノイズワードリスト] ページで各ノイズワードの概要情報を表示できます。

各ノイズワードの概要情報を表示するには、[管理] タブから、[ナレッジ] - [検索] - [KT 検索エンジン] - [ノイズワード] を選択します。

[ノイズワードリスト] ページが表示されます。このページには以下のフィールドが含まれます。

ノイズワード

検索するノイズワードを定義します。このフィールドが表示されるのは、[フィルタを表示] をクリックした場合のみです。

その他の検索指数

検索に使用する追加条件を定義します。このフィールドは、[ナレッジ検索] ページで [詳細] リンクをクリックした場合にのみ表示されます。

ノイズワードリスト

リクエストの検索からフィルタアウトされたワードが表示されます。リストは、[検索] ボタンをクリックすると表示されます。[ノイズワード] フィールドに語句を入力した場合、指定した語句だけがリストに表示されます。[ノイズワード] ボックスに何も入力しない場合、本製品に対して定義されたすべてのノイズワードがリストに表示されます。

[ノイズワードリスト] ページでは、以下のタスクを実行できます。

- [ノイズワードの指定](#) (P. 1177)
- [ノイズワードの編集](#) (P. 1177)

特殊用語の指定

[特殊用語の新規作成] ページでは、ドキュメントおよびクエリを解析するときに、単一のキーワードとして処理される語句またはフレーズを指定できます。

特殊用語を指定するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [検索] - [KT 検索エンジン] - [特殊用語] を参照します。
[特殊用語リスト] ページが表示されます。
2. [新規作成] をクリックします。
[特殊用語の新規作成] ページが表示されます。
3. 特殊用語として定義する単語またはフレーズを [特殊用語] フィールドに入力します。
4. [保存] をクリックします。
[特殊用語の新規作成] ページが閉じて [特殊用語の詳細] ページが開くので、追加した単語またはフレーズを確認できます。[編集] ボタンを使用すると、新しい特殊用語を更新できます。新しい特殊用語は、[特殊用語リスト] ページに表示されます。

特殊用語の編集

特殊用語を編集できます。

特殊用語を編集するには、以下の手順に従います。

1. リスト中ある編集したい特殊用語を右クリックし、ショートカットメニューから [編集] を選択します。
[特殊用語の更新] ページが表示されます。

2. 特殊用語として定義する単語またはフレーズを「特殊用語」フィールドに入力します。
3. 「保存」をクリックします。
「特殊用語の更新」ページが閉じて「特殊用語の詳細」ページが開くので、追加した単語またはフレーズを確認できます。更新された特殊用語は、「特殊用語リスト」ページに表示されます。

特殊用語の表示

各特殊用語の概要情報を表示できます。

特殊用語を表示するには、「管理」タブから、「ナレッジ」-「検索」-「KT 検索エンジン」-「特殊用語」を選択します。

「特殊用語リスト」ページが表示されます。また、以下のフィールドを使用して、デフォルトで定義された特殊用語、または自分で定義した特殊用語を変更できます。

特殊用語

検索する特殊用語を定義します。このフィールドが表示されるのは、「フィルタを表示」をクリックした場合のみです。

その他の検索指数

検索に使用する追加条件を定義します。このフィールドは、「Knowledge Search」ペインで「詳細」リンクをクリックした場合にのみ表示されます。

特殊用語

クエリを解析するときに単一のキーワードとして処理される、スペースまたは文字（ハイフン、スラッシュなど）を含む語句またはフレーズが表示されます。「検索」をクリックする前に「特殊用語」フィールドに語句を入力した場合、リストにはその指定した語句のみが表示されます。「特殊用語」フィールドに何も入力しない場合、本製品に対して定義されたすべての特殊用語が一覧表示されます。

「特殊用語リスト」ページでは、以下のタスクを実行できます。

- [特殊用語の指定](#) (P. 1179)
- [特殊用語の編集](#) (P. 1179)

同義語の指定

同義語は、関連付けられているキーワードと同じまたはほぼ同じ意味を持つ語句またはフレーズです。

複雑な同義語（スペースやその他の区切り文字で区切られた複合語が含まれる同義語）を新しく定義する場合は、同一の特殊用語を作成して、その同義語が単一のエンティティとして処理されるようにします。たとえば、「コンピュータ・アソシエイツ」を「CA」の同義語として定義する場合は、「コンピュータ・アソシエイツ」も特殊用語として定義する必要があります。

注: ノイズワードとして存在する同義語またはキーワードを定義することはできません。

シノニムを作成するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [検索] - [KT 検索エンジン] - [同義語] を参照します。
[ソフトウェア リスト] ページが表示されます。
2. [新規作成] をクリックします。
[同義語の新規作成] ページが表示されます。
3. 同義語として定義する単語またはフレーズを [同義語] フィールドに入力します。
4. [保存] をクリックします。
[同義語の新規作成] ページが閉じて [同義語の詳細] ページが開くので、追加した単語またはフレーズを確認できます。[同義語リスト] ページに、新しい同義語が表示されます。

同義語の表示

各同義語の概要情報を表示できます。

同義語を表示するには、[管理] タブから、[ナレッジ] - [検索] - [KT 検索エンジン] - [同義語] を選択します。

[同義語リスト] ページが表示されます。以下のフィールドを使用して、デフォルトで定義されたキーワードまたは自分で定義したキーワードを変更できます。

キーワード

検索するキーワードを定義します。このフィールドが表示されるのは、[フィルタを表示] をクリックした場合のみです。

同義語

検索する同義語を定義します。このフィールドが表示されるのは、[フィルタを表示] をクリックした場合のみです。

その他の検索指数

検索に使用する追加条件を定義します。このフィールドは、[Knowledge Search] ペインで [詳細] リンクをクリックした場合にのみ表示されます。

同義語リスト

本製品で定義されたキーワード/同義語ペアが表示されます。[キーワード] 列に表示される 1 つのキーワードに対して、1 つ以上の同義語が [同義語] 列に表示されます。

[同義語リスト] ページでは、以下のタスクを実行できます。

- [同義語の指定](#) (P. 1181)
- [同意語の編集](#) (P. 1182)

同義語の編集

同義語は編集できます。

同義語を編集するには、以下の手順に従います。

1. [同義語] リストにある編集したい同義語を右クリックし、ショートカットメニューから [編集] を選択します。
[同義語の更新] ページが表示されます。

2. 同義語として定義する単語またはフレーズを [同義語] フィールドに入力します。
3. [保存] をクリックします。
[同義語の更新] ページが閉じて [同義語の詳細] ページが開くので、追加した単語またはフレーズを確認できます。更新された同義語は、[同義語リスト] ページに表示されます。

パーサ設定

ナレッジベースに発行されたドキュメントは解析され、タイトル、概要、問題、解決策の各フィールドを基にキーワードが作成されます。ユーザがナレッジベースを検索すると、ユーザクエリのキーワードとナレッジベースから解析されたキーワードが比較され、結果リストが生成されます。[パーサ設定] ページでは、ナレッジベースのドキュメントの解析に使用する設定を定義できます。

注: パーサ設定機能は、デフォルトの KT 検索エンジンのみで使用できます。

パーサ設定の定義

ナレッジベースに発行されたドキュメントは解析され、タイトル、概要、問題、解決策の各フィールドを基にキーワードが作成されます。ユーザがナレッジベースを検索すると、ユーザクエリのキーワードとナレッジベースから解析されたキーワードが比較され、結果リストが生成されます。

ナレッジベースのドキュメントの解析に使用する設定を定義するには、[ナレッジ] - [検索] - [パーサ設定] を選択し、[管理] タブを参照します。

パーサ設定が表示されます。設定を定義するには、以下のフィールドを使用します。

最大検索キーワード数

検索テキストが解析されるときに抽出されるキーワードの最大数を定義します。

デフォルト: 20

注: 有効な範囲は 1 ~ 100 です。CA SDM の管理者は、この範囲内であれば、特定のナレッジデータベースのパラメータおよび検索ニーズに従って値を変更することができます。検索キーワード数を少なくすると、パフォーマンスが向上します。

言語

解析処理に使用する言語のタイプを指定します。以下のいずれかの設定を選択します。

英語

必要に応じて、検索時に日本語固有の特定の処理が実行されます。

ヨーロッパ言語

検索時に、ヨーロッパ言語特有の処理のみが実行されます。

韓国語

検索時に、韓国語言語特有の処理のみが実行されます。

その他アジア言語

検索時に、その他のアジア言語用の処理が実行されます。

注: 中国語、日本語、または韓国語の環境で作業する場合、ナレッジマネジメントシステムを実装する前に、使用可能な解析方法および「[マルチバイト文字セット \(MBCS\) を使用する言語](#)」(P. 1186)の制約を理解し、ユーザがシステムに見合った期待を持てるようにしておく必要があります。

有効な文字範囲

ドキュメントの[タイトル]、[概要]、[問題]、[解決策]の各フィールドを解析するときに有効とする英数字の範囲を定義します。範囲外の英数字は、区切り文字として処理されます。

注: [特殊用語を識別] リストで[はい]を選択すると、特殊用語として定義された語句やフレーズは解析されません。

デフォルト: a-z。英字「a」から「z」が解析で有効な文字です。

[有効な文字範囲] フィールドには、解析に使用する適切な文字を含めておく必要があります。[有効な文字範囲] フィールドに含まれていない文字は削除されます。

各言語で推奨される値は以下のとおりです。

言語	有効な文字範囲
ドイツ語	a-zäöüß
スペイン語	a-záéíóúüñ
フランス語	a-zàâäçéèëïîôû
ポルトガルのブラジル	a-zàãäçéêíóúü
イタリア語	a-zàèéïü
中国語（簡体字）	a-z
日本語	a-z
中国語（繁体字）	a-z
韓国語	a-z

注：日本語には「a-z」の範囲のほかに、句読点を除くカタカナのリストが含まれます。

類似語を除外

検索で使用するグループから、構造が似ているキーワードを削除するかどうかを指定します。以下のいずれかの設定を選択できます。

はい

構造が似ているキーワードは検索基準から除外されます。

注：[はい]を選択すると、ドキュメントを保存または発行するときにも、類似語が除外されます。この設定は、[類似語を除外]ボックスが[はい]に設定されている場合にドキュメントが検索可能かどうかに影響を与えます。類似語はインデックスが作成されず、後のドキュメントの取得および検索で使用されません。

いいえ

構造が似ているキーワードは検索基準から除外されません。

デフォルト：いいえ

ノイズワードを除外

ドキュメントの [タイトル]、[概要]、[問題]、および [解決方法] の各フィールドを解析するときに、ノイズワードを除外するかどうかを指定します。以下のいずれかの設定を選択できます。

はい

ノイズワードは検索基準から除外されます。

いいえ

ノイズワードは検索基準から除外されません。

デフォルト： はい

特殊用語を識別

ドキュメントの [タイトル]、[概要]、[問題]、および [解決策] の各フィールドを解析するときに、特殊用語を単一エンティティとみなすか、または複数エンティティとみなすかを指定します。以下のいずれかの設定を選択できます。

はい

特殊用語は、検索基準で単一エンティティとして処理されます。

いいえ

特殊用語を構成する語句は、検索基準で別のエンティティとして処理されます。

デフォルト： はい

マルチバイト文字セットの検索制限

ナレッジマネジメント システムを実装する前には、使用可能な解析アプローチと MBCS 言語の制限について理解していることを確認し、ユーザの期待する結果が必ず得られるようにします。この制限は、日本語、中国語、韓国語のテキストを使ったシステム内での検索機能に影響します。検索メカニズムで使われるワード解析メカニズムは、[\[パーサ設定 \(P. 1183\)\]](#) ページで制御します。

英国、ヨーロッパ言語、韓国語設定の場合は、句読点、「空白」またはその両方の文字が単語の区切りに想定されます。この想定により、ドキュメントテキストは各単語に分割できるようになり、ノイズワードを無視できます。さらに、検索用語に既知の同義語や特殊用語を適用できます。

また、一部のアジア言語のテキストアプローチでは単語間にスペース区切り文字を使いませんが、アジア言語設定を選択した場合は解析ルーチンで文字ごとの解析アプローチを使うことでこの問題に対応します。この設定は、各文字をフルワードとして扱うようにパーサに指示します。設定は、検索対象のすべてのテキストに適用されます。言語設定により検索解析の動作が変わるため、言語設定をアジア言語に、またはアジア言語から変更する場合は、検索インデックス全体を作成しなおす必要があります。

推奨ドキュメント

CA SDM ユーザは、検索項目に関する基準を指定できます。検索エンジンは一致するナレッジドキュメントを検索し、それら見つかったドキュメントを検索結果ページ上に「推奨ドキュメント」のリンクとして表示します。検索クエリは、1つ以上のドキュメントに含まれる可能性のある必要とする概念を示すキーワードまたは一連の語句（フレーズ）として表現できます。

検索基準に適合するドキュメントのリストは並べ替えられ、関連性の高いものから順番に検索結果に表示されます。推奨ドキュメントは、ユーザが目的の情報を探す時間を短縮するのに役立ちます。

一致するドキュメントを一定の基準に従って迅速に並べ替えて表示するために、検索エンジンは条件タイプ（フレーズ、キーワード、またはカテゴリ）を使用してデータを収集します。条件タイプは、管理者が「推奨ドキュメントの作成」ページで設定します。

関連項目:

[推奨ドキュメントの作成](#) (P. 1187)

[推奨ドキュメント条件の編集](#) (P. 1189)

[推奨ドキュメントの表示](#) (P. 1190)

[推奨ドキュメントの検索](#) (P. 1190)

推奨ドキュメントの作成

管理者は、ユーザが検索項目の基準を指定したときに結果として表示される推奨ドキュメントを作成できます。

注: マルチテナンシーがインストールされている場合は、ドロップダウンリストから適切なテナントを選択します。パブリック（共有）オプションを指定すると、すべてのテナントで使用できるオブジェクトが作成されます。

推奨ドキュメントを作成する方法

1. [管理] タブで、[ナレッジ] - [検索] - [推奨ドキュメント] を参照します。
[推奨ドキュメント リスト] が表示されます。
2. [新規作成] をクリックします。
[推奨ドキュメントの新規作成] ページが表示されます。
3. 必要に応じて以下のフィールドに値を入力します。

ナレッジドキュメント

ナレッジドキュメントを指定するか、検索アイコンをクリックして [ナレッジドキュメントの検索] ページを開きます。

条件タイプ

検索エンジンがドキュメントを並べ替えて照合する [条件タイプ](#) (P. 1189) を指定します。

- 条件タイプが [全文一致]、[完全に一致するフレーズ]、または [キーワード] の場合、テキスト フィールドが表示されます。ドキュメントに記載されている概念を示す、フレーズやキーワードを入力できます。
- 条件タイプが [ナレッジカテゴリ] の場合、[ナレッジカテゴリ] リンクが表示されます。このドキュメントに関連付けるナレッジカテゴリを指定できます。

ステータス

このレコードのステータスをアクティブ、または非アクティブに定義します。

[保存] をクリックします。

新しい推奨ドキュメントがナレッジベースに保存され、[推奨ドキュメント リスト] ページに表示されます。

[条件タイプ]フィールド

検索エンジンは、以下の条件タイプでドキュメントを検索できます。

全文一致

検索テキストに入力した検索フレーズでドキュメントを検索します。フレーズ内の語句がすべて見つかった場合のみ一致します。

完全に一致するフレーズ

検索テキストに入力したそのままのフレーズでドキュメントを検索します。フレーズ内の語句とまったく同じ並びの語句が見つかった場合のみ一致します。

キーワード

検索テキストに入力したキーワードでドキュメントを検索します。すべてのキーワードが見つかった場合のみ一致します。

ナレッジカテゴリ

ナレッジカテゴリでドキュメントを検索します。推奨ドキュメントに設定されているカテゴリにユーザが移動する場合のみ一致します。

推奨ドキュメント条件の編集

推奨ドキュメント条件は更新できます。

推奨ドキュメント条件を編集する方法

1. [管理] タブで、[ナレッジ] - [検索] - [推奨ドキュメント] を参照します。
[推奨ドキュメント リスト] ページが表示されます。
2. 条件を編集するには、[条件] 列のタイトルを右クリックします。
[推奨ドキュメントの更新] ページが開きます。
3. 必要に応じてフィールドにデータを入力します。
4. [保存] をクリックします。
更新された条件が [推奨ドキュメント] リストに表示されます。

推奨ドキュメントの表示

各推奨ドキュメントの概要情報を表示できます。

推奨ドキュメントを表示するには、[管理] タブで [検索]、[推奨ドキュメント] の順に選択します。

[推奨ドキュメント リスト] ページが表示され、以下の列を一覧します。

条件

検索エンジンがドキュメントを並べ替えて照合する条件を指定します。

ナレッジドキュメント

結果セット内のドキュメントを表示します。

作成者

ナレッジドキュメントの作成者を定義します。

変更日

ドキュメントが最後に変更された日付を表示します。

[推奨ドキュメント リスト] ページでは、以下のタスクを実行できます。

- [推奨ドキュメントの作成](#) (P. 1187)
- [推奨ドキュメント条件の編集](#) (P. 1189)
- [推奨ドキュメントの検索](#) (P. 1190)

推奨ドキュメントの検索

検索機能を使用して [推奨ドキュメント リスト] にフィルタを適用することによって、必要なアイテムのみを表示できます。

注: マルチテナンシーがインストールされている場合、リスト ページには検索フィルタにテナントおよびパブリック データの設定が表示されます。パブリック データは、テナントデータから除外するか、テナントデータに包含することができます。パブリック オブジェクトのみ検索します。詳細ページで、ドロップダウン リストから適切なテナントを選択します。[<空>] を選択すると、オブジェクトはパブリックになります。

推奨ドキュメントを検索するには

1. [管理] タブで、[ナレッジ] - [検索] - [Recommended Results] を参照します。
[推奨ドキュメント リスト] が表示されます。
2. [フィルタを表示] をクリックします。
3. 必要に応じてフィールドにデータを入力します。以下のフィールドについて詳しく説明します。

タイプ

ドキュメントが推奨ドキュメントに合致し、推奨ドキュメント リンクとして表示されるための条件タイプを指定します。

Phrase/Keywords

推奨ドキュメントに含まれることが期待されるコンセプトであると判断できる検索クエリ情報を指定します。

[検索] をクリックします。

[推奨ドキュメント リスト] に、検索条件に一致するすべてのアイテムが表示されます。

デフォルト検索設定のセットアップ

検索フィールドを使用すると、ナレッジを検索する場合に表示されるデフォルトの検索オプションをセットアップできます。

注: この検索オプションは、ユーザが [環境設定] ウィンドウで定義する個人的な任意の検索設定によって上書きされます。また、[ナレッジ] タブの [ナレッジ検索] ペイン、または [管理] タブの [ナレッジ カテゴリ] ペインで指定された追加の検索オプションによっても上書きされます。

デフォルト検索設定をセットアップするには

1. [管理] タブで、[ナレッジ] - [検索] - [検索設定] に移動します。
[検索オプション] ページが表示されます。

2. 必要に応じて、以下のオプションを選択します。

推奨結果数

検索結果リストに表示されるドキュメント数を指定します。

デフォルト検索フィールド

キーワード検索の初期設定に含めるドキュメント フィールドを指定します。チェック ボックスをオンにすると、関連付けられたフィールドが検索の初期設定に追加されます。チェック ボックスをオフにすると、関連付けられたフィールドが検索の初期設定から除外されます。検索では、以下のドキュメント フィールドを検索に使用できます。

- タイトル
- 概要
- 問題
- 解決方法
- 添付ファイル

すべてのソースに対する検索設定

検索にすべてのナレッジ ソースを含めるかどうかを指定します。
たとえば、ナレッジ カテゴリやリクエスト領域が該当します。

チケット コンテキストの検索設定

Service Desk チケットに定義されているすべてのフィールド（インシデント、問題、案件、変更要求、またはリクエスト）を検索に含めるかどうかを指定します。

- これらのオプションを設定するには、以下の一致タイプのいずれかを選択します。
 - **語句の一部 (OR)** - ドキュメントに、[検索] フィールドのいずれかの語句が含まれる場合、そのドキュメントが結果セットに表示されます。これはデフォルトのオプションです。
 - **すべての語句 (AND)** - ドキュメントに、[検索] フィールドの語句がすべて含まれている場合のみ、そのドキュメントが結果セットに表示されます。

[保存] をクリックします。

デフォルト検索設定がセットアップされます。

CA SDM インテグレーション オプション

以下の環境設定オプションが CA SDM インテグレーションで使用できます。

フィールド マッピング

ナレッジ マネジメント 情報と共にどの CA SDM フィールドを取り込むか、および既存の情報を上書きするかどうかを指定します。

案件の検索設定

チケットの [ナレッジの検索] ボタンをクリックして、検索するフィールドを選択します。

Request Issue Search Configuration

チケットの [検索] ボタンをクリックして、検索するフィールドを選択します。

リクエスト/インシデント/問題検索の構成

チケットの [検索] ボタンをクリックして、検索するフィールドを選択します。

ナレッジの提案

チケットで [保存] ボタンをクリックする前に [View Knowledge] ボタンをクリックすると検索されるフィールドを選択します。

関連項目:

[フィールド マッピングの定義 \(P. 1193\)](#)

[案件の検索設定の定義 \(P. 1196\)](#)

[リクエスト/インシデント/問題の検索設定の定義 \(P. 1197\)](#)

[ナレッジ提案 \(P. 1198\)](#)

[案件カテゴリの定義 \(P. 1199\)](#)

[リクエスト/インシデント/問題領域の定義 \(P. 1201\)](#)

[セルフ サービス ポリシーの設定 \(P. 1202\)](#)

フィールド マッピングの定義

管理者は、[フィールド マッピング] ページを使用して、ナレッジ マネジメント 情報をどのフィールドに格納するか、および既存の情報を上書きするかどうかを指定できます。

ナレッジ マネジメント で使用するサービス デスク フィールドを定義するには

1. [管理] タブで、[ナレッジ] - [Service Desk インテグレーション] - [フィールド マッピング] を参照します。
[フィールド マッピング] ページが表示されます。
2. 必要に応じて以下のフィールドに値を入力します。

ナレッジ マネジメント から Service Desk 値を取り込む

サービス デスク の案件またはリクエストのフィールドに値を格納するために、ナレッジ マネジメント の情報を使用するかどうかを指定します。

- このチェック ボックスをオンにすると、[ナレッジ マネジメント]、[Service Desk の未設定値を生成します]、[Service Desk 値を上書きします] の各列のフィールドが使用できるようになり、サービス デスク の案件またはリクエストのフィールドに値を格納するために使用する ナレッジ マネジメント 情報を指定できます。
- このチェック ボックスをオフにすると、[ナレッジ マネジメント]、[Service Desk の未設定値を生成します]、[Service Desk 値を上書きします] のフィールドが使用できなくなります。この場合、ナレッジ マネジメント から作成されたサービス デスク の案件またはリクエストに対して、ユーザが手動で値を入力する必要があります。

デフォルト： このチェック ボックスはオンです。

Service Desk

[ナレッジ マネジメント] 列に一覧表示されたフィールドに対応する、案件またはリクエストのフィールドを指定します。

[Service Desk の未設定値を生成します] 列でオンにしたチェック ボックスごとに、[ナレッジ マネジメント] 列の対応するフィールドの情報が、案件またはリクエストに格納されます。

ナレッジ マネジメント

[Service Desk] 列にリストされているサービス デスク フィールドに対応する ナレッジ マネジメント フィールドを指定します。

[Service Desk の未設定値を生成します] 列でオンにしたチェック ボックスごとに、[ナレッジ マネジメント] 列の対応するフィールドの情報が、案件またはリクエストに格納されます。

「ナレッジマネジメント」列には、2つのドロップダウン リストが含まれます。

- 最初のドロップダウン リストは「Service Desk」列の「概要」フィールドに対応し、案件またはリクエストの「概要」フィールドに値を格納するために使用される、ナレッジマネジメントフィールド（「タイトル」、「概要」、または「問題」）を指定します。

デフォルト：概要。

- 2番目のドロップダウン リストは「Service Desk」列の「説明」フィールドに対応し、案件またはリクエストの「説明」フィールドに値を格納するために使用される、ナレッジマネジメントフィールド（「タイトル」、「概要」、または「問題」）を指定します。

- デフォルト：問題。

Service Desk の未設定値を生成する

ナレッジマネジメントからの情報を格納する、サービスデスクの案件またはリクエストの空フィールドを指定します。

- このチェック ボックスをオンにすると、サービス デスクフィールドに情報が含まれていない場合に、そのフィールドに対応する ナレッジ マネジメント フィールドから情報をマップすることができます。
- サービス デスク フィールドに対応する ナレッジ マネジメント フィールドから情報をマップしない場合は、このチェック ボックスをオフにします。

デフォルト：

サービスデスクの「概要」、「説明」、「製品」、「アセット」、および「リクエスト領域」の各フィールドに対応するチェック ボックスがオンになります。

Service Desk 値を上書き

ナレッジマネジメント 情報を使用して値を上書きする、サービス デスクの案件またはリクエストのフィールドを指定します。

- このチェック ボックスをオンにすると、サービス デスク フィールドの情報と、対応する ナレッジ マネジメント フィールドの情報が置き換えられます。
- サービス デスク フィールドの情報と、対応する ナレッジ マネジメント フィールドの情報を置き換えない場合は、このチェック ボックスをオフにします。

これらのチェック ボックスは、[Service Desk の未設定値を生成する] 列の対応するチェック ボックスがオンの場合にのみ使用可能になります。

デフォルト：すべての [Service Desk 値を上書きします] チェック ボックスがオフです。

[保存] をクリックします。

フィールド マッピングが定義されます。

案件の検索設定の定義

チケットの [ナレッジの検索] ボタンをクリックして検索する、案件内のフィールドを定義できます。選択するフィールドは、[案件の詳細] ウィンドウの [ナレッジ] タブにある [検索フィルタ] の対応するフィールドにコピーされます。[ナレッジ] タブを選択するか、[フィルタのリセット] ボタン ([ナレッジ] タブ) をクリックすると、チケットから [検索フィルタ] フィールドが生成されます。

ナレッジ ベースの検索で使用する案件のフィールドを定義するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [CA SDM インテグレーション] - [案件の検索設定] を選択します。

[CA SDM インテグレーション] ページが表示されます。

2. ナレッジベース検索で使いたいフィールドを選択します。

- 概要
- 説明
- 構成アイテム
- 優先度
- カテゴリ
- 根本原因
- 製品

注: [概要] フィールドと [説明] フィールドの両方を選択することはできません。

3. 詳細ページの [ナレッジ] タブが選択されているときにナレッジベースが自動的に検索されるようにする場合は、[案件の [ナレッジ] タブが選択された場合に検索を自動的に実行します。] オプションを選択します。

4. [保存] をクリックします。

案件の検索が設定されます。

リクエスト/インシデント/問題の検索設定の定義

チケットの [ナレッジの検索] ボタンをクリックして検索する、リクエスト、インシデントまたは問題に含まれるフィールドを定義できます。選択するフィールドは、[チケットの詳細] ページの [ナレッジ] タブにある [検索フィルタ] の対応するフィールドにコピーされます。[ナレッジ] タブを選択するか、[フィルタのリセット] ボタン ([ナレッジ] タブ) をクリックすると、チケットから [検索フィルタ] フィールドが生成されます。

ナレッジベースの検索で使用する、リクエスト、インシデント、または問題にあるフィールドを定義するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [CA SDM インテグレーション] - [リクエスト/インシデント/問題の検索設定] を選択します。
[CA SDM インテグレーション] ページが表示されます。
2. ナレッジベース検索で使用したいフィールドを選択します。

- 概要
- 説明
- 構成アイテム
- 重大度
- 影響度
- 緊急度
- 優先度
- リクエスト領域
- 根本原因

注: [概要] フィールドと [説明] フィールドの両方を選択することはできません。

3. 詳細ページの [ナレッジ] タブが選択されているときにナレッジベースが自動的に検索されるようにする場合は、[リクエストの [ナレッジ] タブが選択された場合に検索を自動的に実行します。] オプションを選択します。
4. [保存] をクリックします。

ナレッジベースの検索で使用する、リクエスト、インシデント、または問題にあるフィールドが設定されます。

ナレッジ提案

従業員と顧客は、セルフサービス インターフェイスで新しいチケットを作成するとき、許可されている場合に、ナレッジ提案のリストを参照できます。

ソリューションが検索され、チケットが保存されない場合、提案されたドキュメントは、文書形式のセルフ サービスの格付制度によって評価されます。この格付制度は、[検索設定] ページで定義されたセルフ サービス ポリシー設定により異なります。

取得されたデータは、レポートおよびダッシュボードに使用できます。また、チケットを正常に解決したドキュメントをフィルタできるナレッジベースを検索している間も使用できます。

セルフ サービスの利点は、サポート コールの回数が少ない形式であること、および余分なチケットが作成されない形式であることです。これは、運用コストの削減を意味します。

管理者は使用の前にこの機能を有効にしておく必要があります。また、セルフ サービス インターフェースでナレッジが提案される適切な案件カテゴリおよびリクエスト領域を設定しておく必要があります。

案件カテゴリの定義

チケットの作成時に顧客や従業員にナレッジを提案する案件カテゴリを定義できます。

また、[ナレッジの提案] 機能をアクティブまたは非アクティブとしてマークすることもできます。この機能を非アクティブとしてマークすると、顧客と従業員はこの機能を使用できなくなりますが、データベースでは後からでも使用できます。この機能を後で使用する場合は、アクティブとしてマークし直すことができます。

案件カテゴリに対するナレッジの提案を定義するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [Service Desk インテグレーション] - [ナレッジの提案] - [案件カテゴリ] を参照します。
[案件カテゴリに対するナレッジを提案する] ページが表示されます。
2. [ナレッジを提案しない] オプションを選択して、[ナレッジの提案] 機能をアクティブとしてマークします。

デフォルト： 非アクティブです。

この機能をアクティブとしてマークすると、以下のオプションが表示されます。

デフォルトのナレッジの処理:

提案済み

このオプションを指定すると、案件カテゴリのリストに定義されているものを除くすべての案件カテゴリについてナレッジを提案します。

推奨されない

このオプションを指定すると、案件カテゴリのリストに定義されているものを除くすべての案件カテゴリについてナレッジを提案しません。

以下を除いて、すべての案件カテゴリが対象:

リクエスト領域のリストを表示します。ここには、ナレッジがセルフ サービス インターフェースの従業員および顧客に提案されるか、されないかが示されています。セルフ サービス ユーザには、リクエスト領域の編集が許可されていません。リクエスト領域は読み取り専用です。

3. 以下のいずれかのボタンをクリックします。

追加

選択したリクエスト領域をリストに追加します。

削除

選択したリクエスト領域をリストから削除します。

[すべて削除]

リストからリクエスト領域をすべて削除します。

保存

リクエスト領域情報をナレッジ ベースに保存します。

案件カテゴリが定義されます。

リクエスト/インシデント/問題領域の定義

チケットの作成時に顧客や従業員にナレッジを提案するリクエスト、問題、およびインシデントの領域を定義できます。

また、[ナレッジの提案] 機能をアクティブまたは非アクティブとしてマークすることもできます。この機能を非アクティブとしてマークすると、顧客と従業員はこの機能を使用できなくなりますが、データベースでは後からでも使用できます。この機能を後で使用する場合は、アクティブとしてマークし直すことができます。

リクエスト/インシデント/問題領域を定義するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [CA SDM インテグレーション] - [ナレッジの提案] - [リクエスト/インシデント/問題領域] を参照します。

[リクエスト/インシデント/問題領域に対するナレッジを提案する] ページが表示されます。

2. [ナレッジを提案しない] オプションを選択して、[ナレッジの提案] 機能をアクティブとしてマークします。

デフォルト：非アクティブです。

この機能をアクティブとしてマークすると、以下のような追加のオプションが表示されます。

デフォルトのナレッジの処理:

提案済み

このオプションを指定すると、[リクエスト領域] リストに定義されているものを除くすべてのリクエスト/インシデント/問題領域についてナレッジを提案します。

推奨されない

このオプションを指定すると、[リクエスト領域] リストに定義されているものを除くすべてのリクエスト/インシデント/問題領域についてナレッジを提案しません。

以下を除いて、すべてのリクエスト/インシデント/問題領域が対象:

リクエスト領域のリストを表示します。ここには、ナレッジがセルフ サービス インターフェースの従業員および顧客に提案されるか、されないかが示されています。セルフ サービス ユーザには、リクエスト領域の編集が許可されていません。リクエスト領域は読み取り専用です。

[保存] をクリックします。

ナレッジの提案のリクエスト/インシデント/問題領域が定義されます。

セルフ サービス ポリシーの設定

1 セットのユーザ シナリオに基づいてドキュメントを評価する、セルフ サービスのポリシーを設定できます。

セルフ サービスのポリシーを設定するには、以下の手順に従います。

1. [管理] タブで、[ナレッジ] - [ドキュメント] - [CA SDM インテグレーション] - [ナレッジの提案] - [Self-Service Configuration] を参照します。

[検索設定] ページが表示されます。

2. 以下のユーザシナリオに基づいてドキュメントを評価し、回避されたチケットを保存する適切なポリシー設定を指定します。
 - ユーザは提案されたドキュメントを開きませんでした。
 - ユーザは提案されたドキュメントを開きました。
 - ユーザは問題の解決策として提案されたドキュメントに同意しました。
 - ユーザはナレッジを検索し、ドキュメントを開き、終了しました。
[保存] をクリックします。
セルフサービスのポリシー設定が保存されます。

解決策に関する調査

[解決策に関する調査] を使用すると、ナレッジドキュメントのパフォーマンスに関する顧客フィードバックを収集し、分析できます。調査の設定を変更するには、管理インターフェースから、[ナレッジ] - [解決策に関する調査] を選択します。調査は発行済みナレッジドキュメントに表示され、顧客、ゲスト、および従業員がそのナレッジドキュメントの効果を評価できます。

この機能には、以下のコンポーネントが含まれます。

- FAQ 設定
- 調査の設定

関連項目:

[FAQ 設定の定義 \(P. 1204\)](#)

[解決策に関する調査の設定の定義 \(P. 1206\)](#)

FAQ 設定の定義

[FAQ 設定] ページでは、各ドキュメントに割り当てられた FAQ 評価の算出基準となるパラメータを設定できます。FAQ 評価は、以下の基準に従って行われます。

- 過去にドキュメントがアクセスされた頻度
- ドキュメントが参考になった程度
- 時間の経過に伴い、ドキュメントの有効性が低下する程度

初期設定では、FAQ 評価の順（参考になった順）に並び替えられたドキュメントがドキュメント リスト ページに表示されます。最も参考になったドキュメントは、ドキュメント リストの先頭に「バブルアップ」されます。時間の経過に伴い、ユーザが問題の解決策を習得すると、ドキュメントはドキュメント リストの下の方へ移動します。

FAQ 設定を定義する方法

1. [管理] タブで、[ナレッジ] - [解決策に関する調査] - [FAQ 設定] を選択します。

[FAQ 設定] ページが表示されます。

2. 必要に応じて以下のフィールドに値を入力します。

最終更新日

FAQ 評価サービスを実行するかどうかを指定します。FAQ 評価の最終更新日が表示されます。

- [FAQ 評価サービスを実行する] チェック ボックスをオンにすると、このウィンドウの設定を使用して FAQ 計算サービスが実行されます。
- [FAQ 評価サービスを実行する] チェック ボックスをオフにすると、FAQ 計算サービスは実行されません。

スケジュール

FAQ 評価の更新頻度を定義します。このフィールドには、以下のコンポーネントが含まれます。

FAQ の計算周期

ドキュメントの FAQ 評価を更新する間隔を指定します。

デフォルト：1 日

開始時間

FAQ 評価の再計算を開始する時間を指定します。

デフォルト：00:00（午前 12:00）

終了時間

計算が終了しているかどうかに関わらず、FAQ 評価の再計算を終了する時間を指定します。

デフォルト：07:00（午前 7:00）

注：この設定は、本製品のインストール後に有効になります。たとえば、2008 年 4 月 19 日に本製品をインストールした場合、FAQ サーバが初めて実行されるのは 2008 年 4 月 20 日です。

推移

0 に達する前にドキュメント FAQ の評価を再計算する回数を定義します。指定した値に基づいてドキュメント FAQ の評価は低下し、最終的には 0 になります。FAQ 評価が 0 になったドキュメントはドキュメントリストの一番下に表示されます（リストが FAQ 評価順で並び替えられている場合）。

デフォルト：180

たとえば、ドキュメントの評価が 4（とても参考になった）で、推移値が 180 の場合は、FAQ 評価が 180 回再計算されると、ドキュメントの FAQ 評価は 0（ゼロ）になります。

注：初期設定では、FAQ バブルアップ計算には過去 180 日間の bu_trans データが必要です。ここで、180 は推移値です。したがって、FAQ の推移値に 365 を超える値に設定した場合は、bu_trans テーブルのアーカイブルールもそれに従って拡張する必要があります。

新規ドキュメント表示日数

新規作成したドキュメントまたはインポートしたドキュメントが、
[ナレッジ] タブの [新規ドキュメント] フォルダに表示される
日数を指定します。

デフォルト：5 日

評価

ユーザが開いたが評価していないドキュメントの評価の初期設定
（[参考にならなかった]、[多少参考になった]、[とても参
考になった]）を指定します。

デフォルト：多少参考になった

[保存] をクリックします。

FAQ 設定が定義されます。

解決策に関する調査の設定の定義

[調査の設定] ページでは、問題の解決や質問への回答のためにアクセス
したときにナレッジ ドキュメントを表示する方法を設定できます。

解決策に関する調査設定を定義する方法

1. [管理] タブで、[ナレッジ] - [解決策に関する調査] - [調査の設
定] を選択します。
[調査の設定] ページが表示されます。
2. 必要に応じて以下のフィールドに値を入力します。 [保存] をクリッ
クします。

解決策に関する調査の設定が定義されます。

ナレッジ マネジメント システム の 設定

（ログイン時に）[ナレッジ] タブに表示するデフォルトの情報、[管理]
タブの [ナレッジ カテゴリ] ペインに表示するカテゴリの形式、ナレッ
ジ マネジメント ホーム ページの [上位解決策] リストに一覧表示するド
キュメントの数を設定できます。

関連項目:

[一般設定の構成](#) (P. 1207)

一般設定の構成

ログイン時に [ナレッジ] タブに表示するデフォルトの情報、[管理] タブの [ナレッジ カテゴリ] ペインに表示するカテゴリの形式、ナレッジ マネジメント ホーム ページの [上位解決策] リストに一覧表示するドキュメントの数を設定できます。

次の手順に従ってください:

1. [管理] タブで、[ナレッジ] - [システム] - [一般設定] を選択します。

[一般設定] ページが開きます。

2. 必要に応じて以下のフィールドに値を入力します。

検索ツールの初期画面

初期設定で [ナレッジ] タブに表示される情報を指定します。以下のいずれかのオプションを選択できます。

- FAQ/検索でオープン - [カテゴリ]、[ナレッジ検索]、[ナレッジ ドキュメント リスト] ペインを表示します。
- ナレッジ ツリー ドキュメント ID でオープンする - フィールドで指定したドキュメント ID のナレッジ ツリーを表示します。ナレッジ ツリー ドキュメント自体に戻って、[カテゴリ]、[ナレッジ検索]、および [ナレッジ ドキュメント リスト] の各ペインに戻ることができます。 **デフォルト: FAQ/検索**

カテゴリ ビュー

〔管理〕 タブの 〔ナレッジ カテゴリ〕 ペインでドキュメント カテゴリを表示するフォーマットを指定します。以下のいずれかのオプションを選択できます。

- カテゴリをツリー ビューで表示 - 〔ナレッジ カテゴリ〕 ペインで、カテゴリを階層ツリー構造で表示します。カテゴリを展開すると、関連付けられたサブカテゴリが表示されます。この場合、ツリーのすべてのカテゴリを同時に表示できます。
- カテゴリをリスト ビューで表示 - 〔ナレッジ カテゴリ〕 ペインで、カテゴリをリストフォーマットで表示します。カテゴリを選択すると、そのカテゴリのサブカテゴリがリストに表示されます。一度に表示できるのは、現在のレベルのカテゴリかサブカテゴリのどちらかです。前のカテゴリ レベルに戻るには、〔1 つ上のレベル〕 リンクを使用します。

注: トップ カテゴリまたはその他のカテゴリで、カテゴリの数が 250 を超えている場合は、ツリー ビューではなく 〔カテゴリをリスト ビューで表示〕 オプションを使用してください。

上位解決策

CA SDM のホーム ページで 〔上位解決策〕 リストに表示するドキュメントの数を指定します。

デフォルト : 10

EBR インデックス ファイルのパス

EBR インデックス ファイルを格納する場所を定義します。ナレッジ ドキュメントを保存および発行する場合、CA SDM は EBR インデックス ファイルを作成します。設定タイプに応じて、EBR インデックス ファイルのパスを定義する際は以下の点を考慮します。

- **標準**： r11.2 または r12.X から CA SDM リリース 12.9 にアップグレードする場合は、UNC 共有パスを使用しないことを選択する場合があります。UNC パスを作成していない場合、CA SDM は、デフォルト パスを使用して EBR インデックス ファイルを格納します。UNC 共有ドライブを使用する場合は、ebr/ebr_ADM フォルダをデフォルトの場所（\$NX_ROOT/site/）から UNC 共有パスに手動でコピーします。
- **高可用性**： CA SDM r11.2 または r12.X から高可用性設定にアップグレードする場合は、UNC 共有パスを作成し、それを使用して EBR インデックス ファイルを格納する必要があります。UNC 認証情報は、デフォルトのパスでは必要ありません。UNC パスを作成した後、ebr/ebr_ADM フォルダをデフォルトの場所（\$NX_ROOT/site/）から UNC 共有パスに手動でコピーします。

重要： EBR インデックス ファイルのパスと KEIT ファイルのパスは、同じ UNC 認証情報を参照する必要があります。また、これをサポートするため、同じサーバ上にパスが存在する必要があります。

デフォルト： \$NX_ROOT/site/ebr

ナレッジ インポート/エクスポート ファイルのパス

インポート/エクスポート操作時に KEIT インポート/エクスポート パッケージを格納する場所を定義します。設定タイプに応じて、KEIT ファイルのパスを定義する際は以下の点を考慮します。

- **標準**： r11.2 または r12.X から CA SDM リリース 12.9 にアップグレードする場合は、UNC 共有パスを使用しないことを選択する場合があります。UNC パスを作成していない場合、CA SDM は、デフォルト パスを使用して KEIT ファイルを格納します。UNC 共有ドライブを使用する場合は、インポート/エクスポート パッケージフォルダをデフォルトの場所（\$NX_ROOT/site/keit）から UNC 共有パスに手動でコピーします。

- 高可用性：CA SDM r11.2 または r12.X から高可用性設定にアップグレードする場合は、UNC 共有パスを作成し、それを使用して KEIT ファイルを格納する必要があります。UNC 認証情報は、デフォルトのパスでは必要ありません。UNC パスを作成した後、インポート/エクスポート パッケージ フォルダをデフォルトの場所 (\$NX_ROOT/site/keit) から UNC 共有パスに手でコピーします。

重要：EBR インデックス ファイルのパスと KEIT ファイルのパスは、同じ UNC 認証情報を参照する必要があります。また、これをサポートするため、同じサーバ上にパスが存在する必要があります。

デフォルト：\$NX_ROOT/site/keit

UNC 認証情報

このオプションを使用してネットワーク共有ドライブにアクセスする UNC 認証情報を作成し、EBR インデックス作成ファイルおよびインポート/エクスポート パッケージにアクセスできます。[UNC 認証情報] リンクを使用して、UNC 認証情報を作成します。

注：UNC パスおよび UNC 認証情報は、高可用性設定の場合に必要です。UNC の詳細 (UNC パスまたは UNC 認証情報) を変更する場合は、CA SDM サービスを再起動します。

ドキュメント インデックス通知

ユーザが、ステータスに関する情報、またはドキュメントのインデックス作成エラーが発生した場合に、電子メール通知を受信するように設定します。これらの電子メール通知を受信するには、ca_contacts テーブルにユーザの電子メール アドレスが含まれている必要があります。担当者連絡先レコードの [通知] ページを使用して、通知方法を設定します。

重要：[ドキュメント インデックス通知] セクションでドキュメントのインデックス作成通知を受信できるように担当者を設定する必要があります。この連絡先の [通知] タブで、有効な電子メールアドレスを定義して、電子メールで通知できるようにします。

3. [保存] をクリックします。
一般的設定が構成されます。

注: CA SDM の以前のリリースから高可用性設定にマイグレートする場合、インポート/エクスポートパッケージを手動で **UNC** 共有ロケーション ([ナレッジインポート/エクスポート ファイルのパス] フィールドで指定) にコピーします。EBR インデックス ファイルについては、EBR/ebr_ADM フォルダを手動で **UNC** 共有ロケーションに移動するか、または `pdm_k_reindex` コマンド パスを実行できます。

第 24 章：サポートオートメーションの管理

このセクションには、以下のトピックが含まれています。

[環境でのサポートの自動化](#) (P. 1213)
[サポートオートメーションアナリスト管理](#) (P. 1217)
[サポートオートメーションのユーザ管理](#) (P. 1234)
[サポートオートメーションのアクティビティ通知管理](#) (P. 1241)
[サポートオートメーションページの適応化](#) (P. 1242)
[サポートオートメーションのシステムプロパティ](#) (P. 1246)
[サポートオートメーションのキュー管理](#) (P. 1246)
[チケットテンプレート管理](#) (P. 1249)
[管理設定](#) (P. 1250)
[サポートオートメーションツールをカスタマイズする方法](#) (P. 1252)
[セッションログ管理](#) (P. 1261)
[サポートオートメーションレポート](#) (P. 1262)
[ライブアシスタンスを使用したチケットの解決](#) (P. 1263)

環境でのサポートの自動化

プロセスとツールの組み合わせを使用して、サポート戦略を実装できます。CA SDM には、ライブアシスタンスを管理し、自動タスクを作成するツールのほか、それらをさまざまなサポートチャネルから配布するツールが用意されています。

関連プロセスを使い、以下を実行する環境を作成して管理します。

- 平均サポート コール時間の短縮
- サポートコスト全体の削減
- 解決率の引き上げ
- エンドユーザの満足度の向上

ライブ アシスタンス

ライブ アシスタンスは、アナリストとエンド ユーザ間のリモート インタラクションを強化するツールを使って、エンド ユーザにサポートを提供します。自動化されている、事前定義済みの応答を使ってエンド ユーザと通信できます。エンド ユーザのコンピュータに関する詳細情報を収集してサポートを提供します。

ライブ アシスタンスでは、以下のインターフェースを使います。

サポート オートメーション アナリスト インターフェース

アナリストはアシスタンス セッションでエンド ユーザと対話できるほか、サポートを提供できます。

End-User クライアント

エンド ユーザはアナリストとチャットし、アナリストはエンド ユーザのコンピュータにサポートを提供できます。

サポート オートメーション の接続性

アナリストとエンド ユーザが、互いに直接通信することはありません。2 人のユーザ間に直接のピア ツー ピア接続は必要ありません。データ転送はすべてサーバを介してルーティングされるため、エンド ユーザのコンピュータが厳格なファイアウォールの背後にあっても通信することができます。

以下の接続を使用して、エンド ユーザのコンピュータに接続できます。

ソケット

ソケット接続は最良の接続方法です。オーバーヘッドが少なく、遅延が最小限に抑えられている最も高速で効率的な接続タイプです。

HTTP (または HTTPS)

場合によっては、HTTP 接続の方が直接ソケット接続よりも接続性に優れています。これは、直接ソケット接続では企業のファイアウォールで遮断されることがあるためです。HTTP 接続では直接ソケット接続に比べて、ネットワーク トラフィックのオーバーヘッドが大幅に増えます。サーバへの接続のほとんどが HTTP の場合は、HTTP のオーバーヘッドとサーバでの処理のために、同時セッションの数がかなり少なくなります。

プロキシ

ソケット プロキシは、サポート オートメーション サーバが CPU 集中型の操作の一部を肩代わりする動作モードです。たとえば、メインサーバからの暗号化/復号化、論理的なネットワーク ポロジ内の DMZ（または同様のゾーン）に入ることができるサーバ コンポーネントの提供などがあります。

通常は、まず直接ソケット接続で接続を行います。直接ソケット接続が失敗した場合、HTTP で接続を試します。ただし、クライアント コンピュータでカスタム接続設定を指定すれば、この順番を変更できます。

注: 通信設定の詳細については、[オンライン ヘルプ](#)を参照してください。

End-User クライアント

エンドユーザクライアントは、ライブアシスタンスセッションでエンドユーザとアナリストを接続します。エンドユーザは、WebChat でアナリストとチャットしますが、サポート オートメーションアナリストインターフェースのツールを使う必要がある場合に、CA SDM はエンドユーザのコンピュータでこのクライアントを起動します。クライアント起動時に、エンドユーザに、それぞれの Web ブラウザに固有の手順が表示されます。

サーバの負荷

大規模な展開の場合、サーバの負荷が高いためにアプリケーションのパフォーマンスが低下することがあります。このため、次のように 1 つ以上のソケット プロキシサーバに処理の一部を任せることができます。

- すべてのアナリスト、またはクライアント（直接ソケットまたは HTTP のいずれかで接続している）の受信データおよび送信データの復号化と暗号化を任せる
- HTTP で接続しているクライアント間の HTTP トラフィックの処理をソケット プロキシに任せる

DMZ サーバコンポーネント

一部のネットワーク環境では、サポート オートメーション サーバ アプリケーションを実行しているアプリケーション サーバへの直接ソケットアクセスを許可すると、セキュリティ上のリスクになることがあります。このような環境では、**DMZ** 内でソケット プロキシを使うことで、インターネット ユーザとアプリケーション サーバ間に中継コンポーネントを配置できます。このシナリオの場合、ソケット プロキシによってメイン サーバの処理が一部軽減されます。

ソケット プロキシの動作

ソケット プロキシは、次のように機能します。

1. ソケット プロキシは、設定されている外部ポートでアナリストやエンド ユーザからの接続を待機します。
2. メイン サーバとの接続については、どの場合でも設定されている内部ポートでピア接続を確立します。これらの 2 つの接続は、それぞれエンド ユーザ接続とサーバ接続と呼ばれます。
3. エンド ユーザ接続は暗号化されますが、ソケット プロキシがエンド ユーザ接続上で受信および送信するデータの暗号化/復号化を行います。

注: サーバ接続は暗号化されません。

4. 受信データ パケットごとに、プロトコル構造とチェックサム値を検証してから、サーバ接続を通じてメイン サーバにデータが渡されます。
5. メイン サーバは暗号化と復号化処理をほかに任せます。
6. エンド ユーザまたはサーバが接続を閉じると、ソケット プロキシはそのピア接続を閉じます。

サポート オートメーション アナリスト管理

サポート オートメーション アナリストは、環境内のライブ アシスタンス セッションで複数のエンドユーザ リクエストをモニタして管理します。アナリストは、サポート オートメーション ツールを使ってエンドユーザ と対話し、ライブ アシスタンスを提供します。

アナリストはこのインターフェースに、インシデントなどの CA SDM チケットやサポート オートメーション タブからアクセスします。アナリストが使用するツールは、アクセス レベルを管理することで権限を設定できます。テナントごとに、サポート オートメーション ツールを有効または無効にできます。ツールがテナントに対して無効になっている場合、アナリストはアシスタンス セッションでそのツールを使用できません。

重要: サポート オートメーション アナリスト インターフェースは **Windows** でのみ実行されます。サポートされているオペレーティング システムの詳細については、「リリース ノート」を参照してください。

関連項目:

[はじめに](#) (P. 1217)

[アナリスト向けにライブ アシスタンスを設定する方法](#) (P. 1218)

[アナリストによるライブ アシスタンスの起動方法](#) (P. 1228)

[アナリスト向けにライブ アシスタンスを設定する方法](#) (P. 1229)

[エンドユーザがアシスタンス セッションに参加する方法](#) (P. 1230)

[アナリストがエンドユーザへのサポートを自動化する方法](#) (P. 1232)

[アナリストによるライブ アシスタンスの提供方法](#) (P. 1233)

はじめに

製品: CA SDM

リリース: リリース 12.9

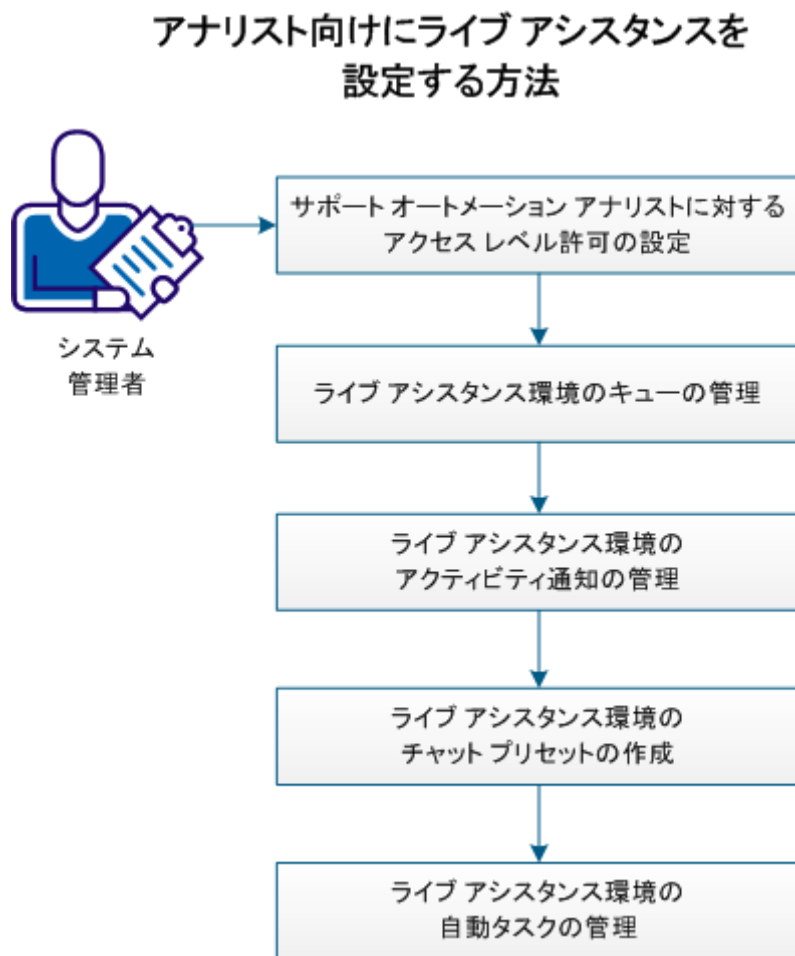
OS: Windows および Linux

このシナリオは、システム管理者が サポート オートメーション アナリスト向けにライブ アシスタンスを設定する方法について説明します。

アナリスト向けにライブ アシスタンスを設定する方法

システム管理者は、ライブ アシスタンスを設定し、アクセス レベルを管理してアナリストが使用できるツールの許可を設定できます。テナントごとに、サポート オートメーション ツールを有効または無効にできます。ツールがテナントに対して無効になっている場合、アナリストはアシスタンス セッションでそのツールを使用できません。

以下の図は、アナリスト向けにライブ アシスタンスを設定する方法を示します。



次の手順に従ってください:

1. [サポート オートメーション アナリストに対するアクセス レベル許可の設定](#) (P. 1219)
2. [ライブ アシスタンス環境のキューの管理](#) (P. 1221)

3. [ライブ アシスタンス環境のアクティビティ通知の管理](#) (P. 1223)
4. [ライブ アシスタンス環境のチャットプリセットの作成](#) (P. 1224)
5. [ライブ アシスタンス環境の自動タスクの管理](#) (P. 1226)

サポート オートメーション アナリストに対するアクセス レベル許可の設定

サポート オートメーション 権限を持つ **CA SDM** 役割を設定できます。ライブ アシスタンス環境のアナリストにサポート オートメーション のアクセス レベル、エンド ユーザにプライバシー レベルを設定し、役割権限を設定します。

以下のアクセス レベルがあります。

アナリスト

サポート環境内のエンド ユーザにライブ アシスタンスを提供する連絡先タイプを指定します。アクセスレベルは、アナリストが使用できるキュー、自動タスク、ツールを定義します。

エンド ユーザ

従業員や顧客など、アナリストからライブ アシスタンスを受ける連絡先タイプを指定します。

サポート オートメーション のアクセス レベルは、[管理] タブで管理します。

次の手順に従ってください:

1. ライブ アシスタンス環境のアナリストに適切なアクセス レベルを設定します。たとえば、アナリストまたはエンド ユーザなどです。

アナリストのアクセス レベルを作成し、特定のサポート オートメーションアナリスト インターフェース ツールを有効にするか、または有効にしないなど、システムでアナリストの権限を管理します。
2. 情報を確認し、ライブ アシスタンス環境内のエンド ユーザに適切なプライバシー レベルを選択します。

システムでプライバシー レベルを作成し、エンド ユーザのアクセス レベルを管理します。
3. アクセス レベルを役割に割り当てます。環境内の役割に、エンド ユーザのプライバシー レベルおよびアナリストのアクセス レベルを割り当てます。
 - a. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。

[役割リスト] ページが表示されます。
 - b. アクセス レベルを割り当てる役割、たとえば、Administrator をクリックします。

[役割の詳細] ページが表示されます。
 - c. [編集] をクリックします。

[役割の更新] ページが表示されます。
 - d. [権限] タブの [SA アクセス] ドロップダウン リストから、作成したアクセス レベルを選択し、[保存] をクリックします。

[役割の詳細] ページが表示されます。サポート オートメーションのアクセス レベルが役割に割り当てられていることを確認します。

サポート オートメーション のアクセス レベルを管理し、サポート 環境内の CA SDM 役割にそれらを割り当てます。サポート環境のサイズや構造はさまざまであるため、アクセス レベルの実装もそれぞれ異なります。

たとえば、小さなサポート環境では、1つのアクセス レベル内で分類された 1 人、または 2 人のアナリストで十分です。より大きなサポート環境の場合は、テナント管理者が多数のアナリスト アクセス レベルを設定し、それぞれに異なるアクセスとサポート権限を指定できます。

重要: マルチテナンシー環境では、サービス プロバイダに属していないアナリストには、それぞれのテナントとサブテナントへの書き込みアクセス権しかありません。ほかのテナントおよびサブテナントに、アナリストの書き込みアクセス権を与えることができます。このアクセスは、アクセスするテナントの機能アクセスをサービス プロバイダに属していないテナントを含むように更新することにより可能です。

ライブ アシスタンス環境のキューの管理

アシスタンス セッション リクエストは、キューを使って最も適切なアナリストにルーティングします。エンドユーザは、それぞれのコンピュータの問題のカテゴリを選択するか、説明を入力できます。それぞれのチケット（インシデントなど）は、適切なキューにルーティングされます。

はじめて製品をインストールした状態のデフォルトのキューの名前は **Support** です。さまざまなサポート リクエストの並べ替えやトラッキングをスムーズに実行できるように、ビジネス ニーズに合わせて複数のキューを設定できます。1つのテナントに割り当てられるデフォルトキューは1つだけです。テナント キューにデフォルトを割り当てない場合、またはデフォルトテナントキューが使用できない場合、システムはパブリック デフォルト キューを使います。キューあたりの作業時間を設定します。

システムは、キューをインシデント領域にマッピングすることでエンドユーザを配置する場所を自動的に判断します。領域とキューがマップされている場合、エンドユーザがカテゴリを選択すると、エンドユーザは適切なキューにルーティングされます。検索機能はインシデントや案件カテゴリの説明に適用されるため、関連するキューが特定されます。これにより、エンドユーザは最適なキューにのみルーティングされます。

次の手順に従ってください:

1. ライブ アシスタンス環境内のアナリストとテナントに合わせてキューをカスタマイズします。キューのカスタマイズでは、フィールドのデフォルトの値を変更してカスタマイズします。

キューのアクティブ化または非アクティブ化、チャットプリセット、カテゴリ、キュー時間、自動転送の設定、テナントおよびアナリストの権限の指定を行うことができます。

2. チェック ボックスをオンにして、デフォルト キューを割り当てます。

環境で設定されたキューと一致しないクエリをエンドユーザが入力する場合、エンドユーザをデフォルトのキューに誘導できます。また、環境内のテナントに合わせてキューをカスタマイズできます。

注: デフォルトのテナント キューが見当たらない、または使用できない場合は、パブリック キューが使われます。

3. キューの営業時間を入力します。

たとえば、業務時間中にサポート オートメーション サービスを有効にするなど、サポート環境内のユーザの可用性に基づいてキューを管理できます。

重要: ワークシフトは、サポート オートメーション 時間および個別のライブ アシスタンス キューの両方に割り当てられます。サポート オートメーション 時間および個別のキューに割り当てられた異なるワークシフトが割り当てられた場合、サポート環境内のアナリストおよびエンドユーザの競合の原因となる場合があります。

ライブ アシスタンス環境のアクティビティ通知の管理

システム管理者は、アクティビティが発生した場合に、エンドユーザおよびアナリストが通知を追跡および受け取る方法をカスタマイズできます。たとえば、アナリストがアシスタンス セッションを終了する場合に通知を送信できます。アシスタンス セッション リクエストがキューに入った時点でアナリストにアラートする電子メール通知を作成します。

環境に応じて、以下のデフォルト通知のいずれかを選択します（現在は非アクティブ）。

キュー エントリ通知

エンドユーザがアシスタンス セッション キューに参加する場合、およびアシスタンス セッションが別のキューに転送される場合、アナリストに通知します。

アナリスト通知

エンドユーザ キューの待機時間が時間切れになると、アナリストに通知します。有効期限のイベントは、CA SDM のイベント条件マクロで認識されます。

エンド ユーザをセッションに招待 - インシデント

アナリストによりインシデントまたはリクエスト アシスタンス セッションに招待されると、エンドユーザに通知します。

エンド ユーザをセッションに招待 - 案件

アナリストにより案件アシスタンス セッションに招待されると、エンドユーザに通知します。

セッション終了通知

アシスタンス セッションが終了すると、システムに通知します。

重要: Star などの外部システムでサポート オートメーション の機能を使う場合、デフォルトの `System_SA_User` 連絡先を **セッション終了通知** ルールに設定します。

次の手順に従ってください:

1. [管理] - [通知] - [アクティビティの通知] に移動します
[アクティビティの通知] ページが開きます。
2. 通知を選択します。
通知が選択され、その通知を使用できます。

ライブ アシスタンス環境のチャット プリセットの作成

よくある質問に対する一般的な応答を作成できます。応答を保存すれば、別のチャットセッションで再利用できるため、同じ応答を何度も入力する必要がなくなります。これらの保存された応答はチャット プリセットと呼ばれます。

各セッションの最初に、挨拶などのプリセットを自動的にエンド ユーザに送信できます。また、プリセットには現行セッションに固有の情報、たとえばアナリスト名を自動的に入力できます。

ライブ アシスタンス セッションでは、以下のプリセット タイプを使用できます。

チャット プリセット

エンド ユーザの質問に対してよく使われるテキストの応答です。

URL プリセット

エンド ユーザがアクセス可能なよく使われる URL です。

各チャット プリセットはローカライズできます。チャット プリセットはエンド ユーザのローカライゼーションと同期されるため、エンド ユーザはローカライズされた適正なプリセットを受け取ります。よくある質問や状況に対して事前定義済みの応答を使うことができます。

次の手順に従ってください:

1. 組織で典型的なアシスタンス セッションを理解します。
2. サポート オートメーション メニューから、[ツール] - [チャット プリセット] - [テキストプリセット リスト] を選択します。
[チャット テキストプリセット リスト] ページが表示されます。
3. [新規作成] をクリックします。
[チャット テキストプリセットの新規作成] ページが表示されます。
4. 以下のフィールドを指定します。

テナント

テナントを指定します。

セッション参加用のデフォルト チャット プリセット

選択すると、セッション参加用のデフォルト チャット プリセットとして定義します。

テキスト プリセット グループ

テキスト プリセット グループを指定します。

テキスト プリセット名

テキスト プリセット名を指定します。

プリセット テキスト

プリセットのテキストを指定します。

[保存] をクリックします。

テキスト チャット プリセットが作成されます。

5. (オプション) [編集] をクリックして [ローカライズされたチャット テキスト プリセット リスト] を変更します。

[チャット テキスト プリセットの更新] ページが表示されます。

6. ローカライゼーションのリンクをクリックします。

[チャット テキスト プリセット ローカライゼーションの詳細] ページが表示されます。

7. [編集] をクリックします。

[チャット テキスト プリセット ローカライゼーションの更新] ページが表示されます。

8. ローカライズされた名前およびテキストを入力して [保存] をクリックします。

ローカライズされたテキスト チャット プリセットのテキストが追加されます。

ライブ アシスタンス環境の自動タスクの管理

自動化タスク エディタをインストールして設定する必要があります。このエディタでは、サポート オートメーション アナリストがエンドユーザーにサポートを提供する際に使用する自動タスクを管理できます。自動タスクは、エンドユーザーの場合はナレッジ ドキュメントとセルフ サービス インターフェースから起動できます。アナリストの場合はアシスタンス セッション時に実行できます。自動タスクは、エンドユーザーのコンピュータに関する詳細情報をアナリストに提供します。エンドユーザーとやり取りして入力进行处理するセルフ サービスの自動タスクを作成します。これらのタスクとしては、ファイル システムやレジストリの変更、ソフトウェアのダウンロードとインストールなどがあります。

次の手順に従ってください:

1. 自動化タスク エディタをインストールします。

以下の場所を使用し、DVD のインストール メディアでインストーラを起動します。

`casd.nt¥SAScriptWriter`

注: サポート環境で、適切なユーザにインストーラをコピーして展開することもできます。自動化タスク エディタがインストールされ、デスクトップにショートカットが作成されます。

2. ダブルクリックして自動化タスク エディタを開きます。

3. [ツール] - [サーバ] をクリックします。

サーバの環境設定ダイアログが表示されます。

4. ホスト名とポートを入力します。

デフォルト: 8070

5. 自動化タスク エディタに対する読み取りまたは書き込みアクセス権を持つユーザ、たとえば、サポート オートメーション Analyst のユーザ名とパスワードを入力します。

6. [テスト] をクリックします。

このツールは、**webservices** コールを使用して **Service Desk** アプリケーションにアクセスし、アプリケーションが存在し、認証情報を使用してアクセスできるかどうかを確認します。

7. [OK] をクリックします。

自動タスクが作成され、サーバにアップロードされます。

パブリック タスクをアップロードし、特定のテナントやサブテナントに割り当てることができます。

重要: タスクおよびライブラリをサーバにアップロードできるのは、[パブリックの更新]フラグが有効なサービス プロバイダ テナントの役割のみです。タスク ライブラリ コンテンツおよび静的コンテンツはすべてパブリック データとして保存されます。

セットアップが完了し、アナリストは、このセットアップを使用してユーザをサポートできます。サポートオートメーションアナリストは、ライブアシスタンスセッションで複数のエンドユーザ リクエストを監視して管理します。アナリストは、サポート オートメーション ツールを使ってエンドユーザと対話し、ライブアシスタンスを提供します。アナリストは、インシデントなどの **CA SDM** チケットやサポート オートメーション タブからこのインターフェースにアクセスし、セッションを開始します。

アナリストによるライブ アシスタンスの起動方法

アナリストは以下のようにライブ アシスタンスを起動します。

1. アナリストは、以下のいずれかを実行します。
 - CA SDM にログインし、[サポート オートメーション] タブを選択します。
 - CA SDM チケットを開き、[サポート オートメーション] タブを選択します。
2. 32 ビット Java Runtime Environment (JRE) バージョン 1.6 以降がインストールされていない場合は、アナリストにインストールを指示するプロンプトが CA SDM に表示されます。サポート オートメーション アナリスト インターフェースは 64 ビット JRE をサポートしていません。

注: Safari ブラウザには 32 ビット JRE 1.6.0_30 以降が必要です。

CA SDM はサポート オートメーション アナリスト インターフェースを起動します。

注: sa_login_session テーブルでは、アナリストがサポート オートメーション アナリスト インターフェースを起動するたびに、またエンド ユーザが Web クライアントを起動するたびにレコードが作成されます。

sa_login_session テーブルの詳細については、CA SDM の「テクニカル リファレンス ガイド」を参照してください。

Java 接続オプションの設定

サポート オートメーション アナリスト インターフェースから サポート オートメーション サーバに接続できない問題は、Java 接続オプションを設定して解決できます。この問題は、アナリストのデフォルトのブラウザ設定が環境に合わせて正しく設定されていないために、ライブ アシスタンスを起動できない場合に生じます。アナリスト接続設定は、ブラウザ、または Java コントロール パネルから編集できます。

ブラウザの接続オプションを設定する方法

1. Internet Explorer などの Web ブラウザを開きます。
ブラウザが表示されます。
2. [ツール] - [インターネット オプション] の順に選択します。
[インターネット オプション] ダイアログ ボックスが表示されます。

3. 直接接続やプロキシサーバなど、適切な接続設定を行います。
4. [OK] をクリックします。
接続がオープンになります。

Java コントロール パネルの接続オプションを設定する方法

1. 以下のコマンドで Java コントロール パネルを開きます。

```
javaws -viewer
```


Java コントロール パネルが表示されます。
2. [一般] タブの [ネットワーク設定] をクリックします。
[ネットワーク設定] ダイアログが表示されます。
3. 直接接続やプロキシサーバなど、適切な設定を行います。
[OK] をクリックします。
接続がオープンになります。

アナリスト向けにライブ アシスタンスを設定する方法

次のように、ライブ アシスタンス環境のアナリストに役割とセキュリティ権限を設定し、サポート オートメーション アナリスト インターフェイスを設定します。

1. ライブ アシスタンス環境のアナリストに合わせて[役割](#) (P. 1234)と[サポート オートメーション アクセス レベル](#) (P. 1239)を作成、または変更します。

アナリストがアシスタンス セッションで使用するツールに必要な権限が得られるように、役割とアクセス レベルを更新します。
2. ライブ アシスタンス環境に[キュー](#) (P. 1246)を設定して管理します。
受信するライブ アシスタンス リクエストを適切にルーティングするキューを作成します。

3. ライブ アシスタンス環境に[アクティビティの通知](#) (P. 1241) を設定して管理します。

アシスタンス セッション リクエストがキューに入った時点でアナリストにアラートする電子メール通知を作成します。

4. ライブ アシスタンス環境に[チャットプリセット](#) (P. 1260) を設定して管理します。

アナリストがよくある質問や一般的な状況に対してあらかじめ設定されている応答を送信するために使用する、チャットプリセットを作成します。

5. ライブ アシスタンス環境に自動タスクを設定して管理します。

エンドユーザ コンピュータで特定のアクションを実行する自動タスクを作成します。

注: スクリプトを作成してサーバにアップロードするには、必ず自動化タスク エディタ IDE を使う必要があります。

エンドユーザがアシスタンス セッションに参加する方法

エンドユーザは、それぞれの CA SDM ホーム ページから、または電話や電子メールなどで直接ヘルプ デスクに連絡してアシスタンス セッションをリクエストします。サポート オートメーション アナリストは CA SDM チケットからエンドユーザをセッションに招待します。

1. エンドユーザは、以下の *どれでも* 実行できます。

- CA SDM ホーム ページからライブ チャットをリクエストする

ライブ チャットの起動ページが表示され、エンドユーザにインシデント領域と説明を尋ねます。エンドユーザが [続行] をクリックすると、セッションが開き、エンドユーザは適切なキューに入ります。

- 電子メール通知のリンクをクリックし、それぞれの認証情報とアナリストから受け取ったセッション参加コードを使ってアシスタンスセッションにログインする

エンドユーザが電子メール通知から参加する場合、キューに入ることはありません。

- [今すぐアナリストと対話] をクリックし、キューに入らずに済むようにセッション参加コードを入力する

注: サポート オートメーション エンドユーザ クライアントを起動すると、プログラムを起動するために実行可能ファイルがダウンロードされます。エンドユーザはクライアントを手動で開始しますが、セキュリティ上の理由から、実行可能ファイルの起動までの時間が制限されています。時間切れになった後に実行可能ファイルを起動しようとすると、エンドユーザのコンピュータにエラーメッセージが表示されます。

2. アナリストは、チャットを通じてエンドユーザにライブアシスタンスを提供します。エンドユーザは、それぞれの **Web** ブラウザを使ってアナリストとチャットします。または、エージェント実行可能ファイルを起動できます。

注: アナリストが **WebChat** でセッションを解決できない場合は、エンドユーザをアナリストセッション ウィンドウから招待し、サポートオートメーション インターフェースに用意されているすべてのツールが使えるようにできます。エンドユーザは、それぞれのコンピュータでクライアントを起動するリクエストを受け入れ、アナリストがこれらのツールが使えるようにする必要があります。

アナリストがエンド ユーザへのサポートを自動化する方法

アナリストは、ライブ アシスタンス ツールを使ってエンド ユーザのコンピュータで以下のタスクを実行します。

- ライブ チャット セッションのホスト
- ファイル システムの表示
 - ファイルとディレクトリの作成、変更、名前の変更、削除
 - エンド ユーザのコンピュータへのファイルやフォルダのコピーと転送
- システム レジストリの表示
 - レジストリ レコードの作成、編集、または削除
 - エンド ユーザ レジストリからのレジストリ値のエクスポート、またはインポート
- リモート コントロール アシスタンスを実行できる接続状態ではない場合に、エンド ユーザのスクリーンショットを取得する
- エンド ユーザのコンピュータのデスクトップの表示
- エンド ユーザのコンピュータのリモート コントロール
- エンド ユーザのコンピュータでのプログラムの起動
- エンド ユーザのコンピュータの再起動またはシャットダウン
- 自動タスクの実行

注: アナリストがライブ アシスタンス ツールを使用する方法の詳細については、[オンライン ヘルプ](#)を参照してください。

関連項目:

[サポート オートメーション のアクセス レベル管理](#) (P. 1239)

アナリストによるライブ アシスタンスの提供方法

アナリストはサポート オートメーション アナリスト インターフェースを使ってエンド ユーザにライブ アシスタンスを提供します。アナリストは、自分のキューにルーティングされたエンド ユーザを処理するほか、アシスタンス セッションの管理、権限のあるセッションへの参加などを行います。

1. エンド ユーザは、**CA SDM** ホーム ページから、またはインシデント、リクエスト、案件などのチケットからアシスタンス セッションをリクエストします。

2. エンド ユーザはキューに入ります。

注: エンド ユーザがアナリストの招待メールのリンクを使ってセッションに参加する場合、キューに入ることはありません。

キュー ルーティングのために、**CA SDM** リクエスト領域および案件カテゴリを設定します。

3. アナリストは、キューからエンド ユーザを選択します。
4. アシスタンス セッションが開始され、アナリストはライブ アシスタンスを提供します。

注: アナリストが [サポート オートメーション] タブからサポート オートメーション アナリスト インターフェースを起動する場合、アシスタンス セッションに **CA SDM** チケットは関連付けられません。

5. アナリストはアシスタンス セッションを閉じるときにチケットを作成し、そのステータスを **SA - オープン**または **SA - 解決済み**にします。あるいは、そのアシスタンス セッションを別のキューに転送します。
6. アナリストがセッションを閉じると、エンド ユーザは電子メール通知でセッション ログを受け取ります。

注: アナリストによるキューの処理方法とアシスタンス セッションの管理方法の詳細については、[オンラインヘルプ](#)を参照してください。

サポート オートメーション のユーザ管理

システム管理者とテナント管理者は、CA SDM の連絡先、役割権限、アクセス レベル、プライバシー レベルを設定してユーザ権限を定義します。以下に、サポート オートメーション を使用するユーザをリストします。

システム管理者

[管理] タブにある サポート オートメーション のすべてのデフォルトと機能を追加、編集、変更できる、システム全体にわたるアクセス権があります。システム管理者はテナントとアナリストを設定するほか、サポート オートメーション システムのプロパティのカスタマイズやシステム パスワードのリセットを実行します。

テナント管理者

テナント レベルの管理者権限があります。他のテナントを作成、または編集する権限やユーザ パスワードをリセットする権限はありません。サービス プロバイダ テナントで権限が決まります。

アナリスト

サポート環境内のエンド ユーザにライブ アシスタンスを提供するユーザ権限です。

エンド ユーザ

従業員や顧客など、サポート環境内のアナリストにライブ アシスタンスをリクエストできるユーザ権限です。

サポート オートメーション 役割権限を設定する方法

サポート オートメーション 権限を持つ CA SDM 役割を設定できます。以下のように、ライブ アシスタンス環境のアナリストに サポート オートメーション のアクセス レベル、エンド ユーザにプライバシー レベルを設定し、役割権限を設定できます。

1. ライブ アシスタンス環境のアナリストに適切なアクセス レベルを設定します。

アナリストのアクセス レベルを作成し、特定の サポート オートメーション アナリスト インターフェース ツールを有効、または無効にするなど、システムでアナリストの権限を管理します。

2. ライブ アシスタンス環境のエンド ユーザに適切なプライバシー レベルを設定します。

システムでプライバシー レベルを作成し、エンド ユーザのアクセス レベルを管理します。

3. アクセス レベルを役割に[割り当てます](#) (P. 1241)。

環境内の役割に、エンド ユーザのプライバシー レベルおよびアナリストのアクセス レベルを割り当てます。

注: アナリストのサポート オートメーション アクセス レベルの作成および変更の詳細、エンド ユーザのセキュリティ レベルの設定の詳細については、[オンライン ヘルプ](#)を参照してください。

サポート オートメーション 匿名ユーザと登録ユーザ

サポート オートメーション サーバは、CA SDM の権限に基づいて、登録ユーザまたは匿名ユーザを受け入れます。許可される場合は、ゲスト ユーザが匿名ユーザを CA SDM にログインさせることができます。サーバで認証されれば、以下へのアクセスを取得できます。

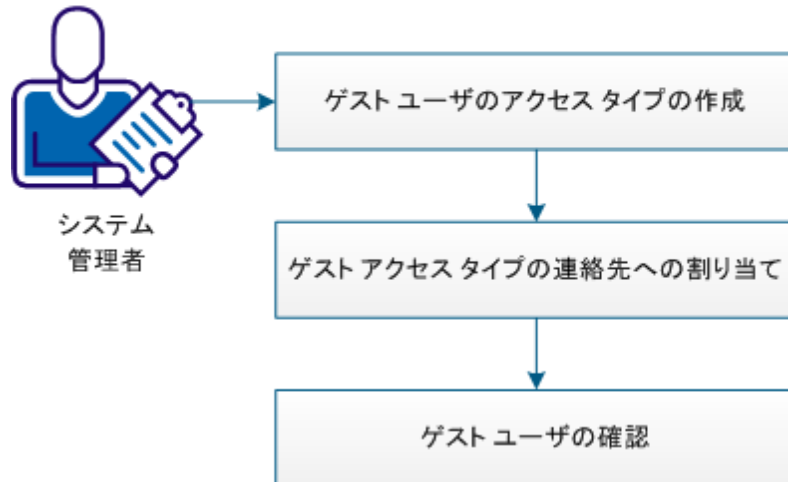
- ライブ アシスタンス
- セルフサービス
- 自動化タスク エディタ
- エンド ユーザ クライアント

ゲスト ユーザ向けにサポート オートメーションを設定する方法

システム管理者は、ライブ アシスタンス環境を設定して、ゲスト ユーザがアナリストと対話することを可能にします。特定のテナントにゲスト ユーザを設定するか、またはシステム全体でユーザを許可できます。テナントは、マルチテナンシー環境で複数の顧客に対してサービスを提供するソフトウェア アプリケーションの単一インスタンスを使用するユーザです。

以下の図は、システム管理者がライブ アシスタンス環境を設定して、ゲスト ユーザに対して以下を許可する方法を示しています。

ゲスト ユーザ向けにサポート オートメーション を設定する方法



次の手順に従ってください:

1. [ゲスト ユーザのアクセス タイプの作成](#) (P. 1237)
2. [ゲスト アクセス タイプの連絡先への割り当て](#) (P. 1238)
3. [ゲスト ユーザの確認](#) (P. 1239)

ゲストユーザのアクセスタイプの作成

認証なしでゲストユーザが CA SDM にログインできるようにするには、CA SDM で特定のアクセスタイプを作成します。サービスプロバイダの場合は、環境内のテナントごとにゲストアクセスタイプを作成できます。

次の手順に従ってください:

1. CA SDM にログインします。
2. [管理] タブで、[セキュリティと役割の管理] - [アクセスタイプ] をクリックします。
[アクセスタイプリスト] ページが開きます。
3. [新規作成] をクリックします。
[アクセスタイプの新規作成] ページが開きます。
4. 必要に応じてフィールドにデータを入力します。
5. [Web 認証] タブをクリックします。[検証タイプ] ドロップダウンリストで、[オープン - 常にアクセスを許可] を選択します。
6. [保存] をクリックします。
ゲストユーザ向けのアクセスタイプが作成されます。
7. (オプション) [アクセスタイプリスト] ページを右クリックし、[更新] を選択します。
ゲストアクセスタイプがリストに表示されます。

ゲスト アクセス タイプの連絡先への割り当て

アクセス タイプを作成した後、連絡先にゲスト アクセス タイプを割り当てて、ゲストがサポート オートメーションのライブ アシスタンス機能を使用できるようにします。ゲスト ユーザは、Web 認証を使用して CA SDM にログインします。連絡先は、システムを定期的に使用する人物です。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理] - [連絡先] をクリックします。
[連絡先の検索] ページが開きます。
2. [新規作成] をクリックします。
[連絡先の新規作成] ページが開きます。
注: 連絡先の変更も可能です。
3. [連絡先タイプ] ドロップダウン リストからゲストを選択します。
4. (オプション) 連絡先とテナントを関連付けて、連絡先をパブリックにします。この関連付けは、連絡先がリクエストの自動的な割り当てを受けるのに役立ちます。
5. [保存] をクリックします。
ゲスト アクセス タイプが連絡先に割り当てられます。

ゲスト ユーザの確認

アクセス タイプを割り当てた後、環境内に適切なユーザが存在することを確認できます。

次の手順に従ってください:

1. [管理] タブで、[セキュリティと役割の管理] - [連絡先] をクリックします。

[連絡先の検索] ページが開きます。

2. [連絡先タイプ] として、[ゲスト] および割り当てたアクセス タイプを選択します。

3. [検索] をクリックします。

[連絡先リスト] ページが表示されます。

連絡先タイプとアクセス タイプは [連絡先リスト] ページで使用できます。

この手順で、ゲスト ユーザ向けの サポート オートメーション の設定は完了です。

サポート オートメーション のアクセス レベル管理

サポート オートメーション のアクセス レベルを管理し、サポート環境内の **CA SDM** 役割にそれらを割り当てます。サポート環境のサイズや構造はさまざまであるため、アクセス レベルの実装もそれぞれ異なります。

小さなサポート環境では、1 つのアクセス レベル内で分類された 1 人、または 2 人のアナリスト、たとえば **Analyst** で十分です。より大きなサポート環境の場合は、テナント管理者が多数のアナリスト アクセス レベルを設定し、それぞれに異なるアクセスとサポート権限を指定できます。

重要: マルチテナンシー環境の場合、サービス プロバイダに属していないアナリストにはそれぞれのテナントとサブテナントへの書き込みアクセス権しかありません。このようなアナリストには、アクセスするテナントの機能アクセスをサービス プロバイダに属していないテナントを含むように更新することで、他のテナントとサブテナントへの書き込みアクセス権を与えることができます。

以下のアクセス レベルがあります。

アナリスト

サポート環境内のエンドユーザにライブ アシスタンスを提供する連絡先タイプを指定します。アクセス レベルは、アナリストが使用できるキュー、自動タスク、ツールを定義します。

エンド ユーザ

従業員や顧客など、アナリストからライブ アシスタンスを受ける連絡先タイプを指定します。

サポート オートメーション のアクセス レベルは、[管理] タブで管理します。

注: アナリストとエンドユーザ向けの サポート オートメーション のアクセス レベルの作成および変更の詳細については、[オンライン ヘルプ](#)を参照してください。

役割へのアクセス レベルの割り当て

環境内の既存の **CA SDM** 役割に サポート オートメーション のアクセス レベルを割り当てることができます。

役割にアクセス レベルを割り当てる方法

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。
[役割リスト] ページが表示されます。
2. アクセス レベルを割り当てる役割、たとえば、**Administrator** をクリックします。
[役割の詳細] ページが表示されます。
3. [編集] をクリックします。
[役割の更新] ページが表示されます。
4. [権限] タブの [SA アクセス] ドロップダウン リストから、作成したアクセス レベルを選択し、[保存] をクリックします。
[役割の詳細] ページが表示されます。サポート オートメーション のアクセス レベルが役割に割り当てられていることを確認します。

サポート オートメーション のアクティビティ通知管理

アクティビティ通知を使って、サポート オートメーション のアクティビティを管理できます。アシスタンス セッションの終了など、何らかのアクティビティが生じたときに、エンドユーザ、アナリスト、管理者が通知をトラッキングする方法、および受け取る方法をカスタマイズできます。

環境には以下のデフォルト通知が適しているため、いずれかを設定します。

キュー エントリ通知

エンドユーザがアシスタンス セッション キューに参加すると、アナリストに通知します。

アシスタンス セッションが別のキューに転送されると、アナリストに通知します。

アナリスト通知

エンドユーザ キューの待機時間が時間切れになると、アナリストに通知します。有効期限のイベントは、CA SDM のイベント条件マクロで認識されます。

エンド ユーザをセッションに招待 - インシデント

アナリストによりインシデントまたはリクエストからアシスタンス セッションに招待されると、エンド ユーザに通知します。

エンド ユーザをセッションに招待 - 案件

アナリストにより案件からアシスタンス セッションに招待されると、エンド ユーザに通知します。

セッション終了通知

アシスタンス セッションが終了すると、システムに通知します。

重要: Star などの外部システムでサポート オートメーション の機能を使う場合、デフォルトの **System_SA_User** 連絡先を **セッション終了通知** ルールに設定します。

サポート オートメーション ページの適応化

ビジネス ニーズに合わせて、エンド ユーザに表示する サポート オートメーション ページのデザインを設定できます。以下の適応化により、アシスタンス セッションに参加する前、およびセッションが完了した後にユーザに表示される内容を制御できます。

- エンド ユーザに表示されるすべてのページのヘッダおよびフッタをカスタマイズする
ヘッダとフッタの HTML コードを変更できます。また、スタイル定義を含んでいる CSS ファイルの場所も変更できます。
- 環境のローカライゼーション ニーズをカスタマイズする

すべてのアナリストおよびエンド ユーザのデフォルト ロケールを設定できます。

- エンド ユーザがログインし、アシスタンス セッションへの参加を待機しているときに表示されるページ レイアウトをカスタマイズする
ビジネスのニーズに合わせて、エンド ユーザに表示するページをカスタマイズできます。

注: アナリストとエンド ユーザに表示する サポート オートメーション ページの設定の詳細については、[オンライン ヘルプ](#)を参照してください。

ブランディング管理

セルフ サービスなどで、エンド ユーザが目にするページのヘッダやフッタをカスタマイズできます。ヘッダとフッタの **HTML** コードの変更のほか、スタイル定義を含む **CSS** ファイルの場所の変更も可能です。

各テナントには最大 **1** つのブランディング レコードがあり、これらをリストにして表示できます。テナントはそれぞれ独自のブランディングを作成できますが、ブランディングが定義されていないテナントはデフォルトのシステム設定を使います。また、ブランディングのローカライゼーションを有効にできるほか、有効なローカライゼーションについて、ローカライズされているすべてのブランディングのリストを表示できます。

重要: CA サポート オートメーション **r6.0 SR1 eFix5** からのブランディング カスタマイズでは、**CA SDM リリース 12.9** に自動的にマイグレートされません。ブランディング カスタマイズを確認し、**CA SDM** ブランディングに対応しているかどうかを検証することをお勧めします。必要に応じて、各部署のヘッダ、フッタ、および **CSS URL** をコピーして、**CA SDM** 内の対応するテナント（またはパブリック）に貼り付けて、ブランディング データをマイグレートしてください。

ローカライゼーション管理

ローカライゼーションでは、アプリケーションの要素を特定の言語に翻訳することで、同じインストールで複数の言語を同時にサポートできます。これらの要素にはシステム メッセージ、アイコンおよびコンテンツなどがあります。情報は、それぞれのネイティブ言語に関係なく、エンドユーザに最適な形式で表示されます。

サポート オートメーション のローカライズ バージョンを用意することで、グローバルな環境にも対応できます。各テナントは複数の言語を処理することが可能で、ローカライゼーションは複数のテナント間で使用できます。各テナントは、デフォルトのシステム設定をそのローカライゼーションと共有します。エンドユーザとアナリストが使う言語は、ライブアシスタンスを起動する前に、有効な言語リストから設定できます。アナリストはアシスタンス セッション内のエンドユーザと異なる言語を使うことができます。

ローカライズされた免責条項のテキストは編集できます。ローカライゼーションの作成や削除はできませんが、有効と無効の切り替えは可能です。

注: 管理者インターフェースはデフォルトのサーバ ローカライゼーションでのみ使用できます。

ページレイアウト設定

エンドユーザが **CA SDM** からライブ アシスタンスにログインすると、デフォルトの起動ページが表示されます。また、キューに保留されていた状態からログインした場合も、デフォルトのページが表示されます。

テナントに特別な設定が指定されていない場合は、パブリック設定がデフォルトになります。特別な独自の設定がないキューには、以下のパブリック設定を指定できます。

- Wait Page
- エンドユーザ起動後ページ
- セッション中
- 「Post-Logout」 ページ
- 調査の終了ページ

各ページには、URL を入力できるテキスト フィールド、このページを外部としてマークするためのチェック ボックスで構成される詳細ページがあります。

サポート オートメーション のシステム プロパティ

サポート オートメーション がアクティビティを処理する方法の多くはカスタマイズ可能であり、デフォルト インストールと異なる設定にすることができます。デフォルトのシステム オプション設定を使って、サポート オートメーション の動作をカスタマイズできます。たとえば、以下のサポート オートメーション オプションをカスタマイズできます。

- CA SDM の従業員や顧客のホーム ページからライブ チャットへのリンクを有効にする、または無効にする
- CA SDM の従業員や顧客のホーム ページからセッションに参加するリンクを有効にする、または無効にする
- エンドユーザが サポート オートメーション キュー上で待機中に接続を切断した場合に CA SDM インシデントを作成するオプションを有効または無効にします。

テナントのシステム プロパティの設定はオプションです。テナントがそのプロパティを定義していない場合は、サポート オートメーション はパブリック（共有）の設定を使用します。製品のインストールでは、デフォルトのパブリック プロパティを作成します。

注: サポート オートメーション システム プロパティの設定の詳細については、[オンライン ヘルプ](#)を参照してください。

サポート オートメーション のキュー管理

アシスタンス セッション リクエストは、キューを使って最も適切なアナリストにルーティングします。エンドユーザはそれぞれのコンピュータの問題のカテゴリを選択するか、説明を入力できます。それぞれのチケット（インシデントなど）は、適切なキューにルーティングされます。

はじめて製品をインストールした状態のデフォルトのキューの名前は **Support** です。さまざまなサポート リクエストの並べ替えやトラッキングをスムーズに実行できるように、ビジネス ニーズに合わせて複数のキューを設定できます。1つのテナントに割り当てられるデフォルトキューは1つだけです。テナント キューにデフォルトを割り当てない場合、またはデフォルト テナント キューが使用できない場合、システムはパブリック デフォルト キューを使います。キューあたりの作業時間を設定します。

システムは、キューをインシデント領域にマッピングすることでエンドユーザを配置する場所を自動的に判断します。領域とキューがマップされている場合、エンドユーザがカテゴリを選択すると、適切なキューにルーティングされます。検索機能はインシデントや案件カテゴリの説明に適用されるため、関連するキューが特定されます。これにより、エンドユーザは最適なキューにのみルーティングされます。

注: サポート オートメーション キューのカスタマイズとマッピングの詳細については、[オンラインヘルプ](#)を参照してください。

キュー管理

キューを設定することで、エンドユーザがアナリストから適切なライブアシスタンスを受けられるようにします。アシスタンスセッションへのエンドユーザのルーティングを改善するために、次のようにキューを管理します。

- ライブアシスタンス環境内のアナリストとテナントに合わせてキューをカスタマイズする

キューのアクティブと非アクティブを切り替えられるほか、テナントとアナリストの権限を指定できます。

- デフォルトのキューを割り当てる

環境で設定されたキューと一致しないクエリをエンドユーザが入力する場合、エンドユーザをデフォルトのキューに誘導できます。また、環境内のテナントに合わせてキューをカスタマイズできます。

注: デフォルトのテナント キューが見当たらない、または使用できない場合は、パブリック キューが使われます。

- キューの営業時間を割り当てる

たとえば、業務時間中にサポート オートメーション サービスを有効にするなど、サポート環境内のユーザの可用性に基づいてキューを管理できます。

重要: ワークシフトは、サポート オートメーション 時間および個別のライブアシスタンス キューの両方に割り当てられます。サポート オートメーション 時間と各ライブアシスタンス キューに割り当てるワークシフトが異なると、サポート環境内のアナリストとエンドユーザで競合が生じることがあります。

キューの概要の管理方法

アナリストが [キューの概要] ページで表示できるフィールドを選択できます。キューの概要に表示するフィールドは以下から選択できます。フィールドを作成することはできません。

- キュー
- 質問
- 待機時間
- 電子メール
- 会社
- IP アドレス
- 所有アナリスト
- カテゴリ
- 言語
- テナント

関連項目:

[キュー管理](#) (P. 1247)

[キュー時間を管理する方法](#) (P. 1249)

キュー時間を管理する方法

以下のように、アナリストの業務時間を配慮して、1日の特定の時間に、キューごとにサポート オートメーション を有効にできます。

- 各キュー、およびすべての自動サポート サービスに個別のスケジュールを作成します。

注: これらの設定により、セルフ サービス機能が制限されることはありません。

- サポート オートメーション サーバのサポート時間は、グローバル オープン ステータス、またはクローズ ステータスで定義します。1週間の各時間への登録は、サーバのグローバル ステータスと違うことを示します。
- サーバは、設定しているルールに基づいて各時間の最初の登録を使います。

このアクションでは、親テナント（またはパブリック）設定のサポート時間定義を効率的にマージできます。このアクションは、階層に「デフォルト クローズ」と「デフォルト オープン」が混在して使われている場合、直観とは反する結果になることがあります。

チケット テンプレート管理

アナリスト ユーザ インターフェイスで使用できるチケット テンプレートを指定できます。[インシデント] / [リクエスト] および [案件] チケット タイプのチケット テンプレートを選択できます。

テンプレートがデフォルトか、アクティブかを定義できます。チケット テンプレートを作成する場合、既存の CA SDM テンプレートから選択できます。デフォルト テンプレートはアクティブである必要があります。

テナントごとにチケット テンプレートを1つのみデフォルトとすることができます。

注: チケット テンプレートのカスタマイズの詳細については、オンライン ヘルプを参照してください。

管理設定

以下のサポート オートメーション の設定を定義して設定できます。

- メッセージルーティング サーバ
- エンド ユーザ権限 (プライバシー レベル)
- サポート オートメーション 時間

サポート オートメーション の設定を構成する方法

ビジネス ニーズに合わせて、サポート環境に適したサポート オートメーション 設定を構成できます。この設定により、メッセージルーティングサーバ、プライバシー レベル、サポート オートメーション 時間などの管理機能を制御できます。

- アシスタンス セッション時のパフォーマンスを改善するようにメッセージルーティングサーバを設定する

エンド ユーザをアナリストの優先ローカルサーバに接続できます。また、接続に失敗する場合は、セッションをメインのデフォルトサーバに接続します。

- 環境内のエンド ユーザにプライバシー レベルを設定する

環境内で使われているプライバシー レベルに基づいて、特定のサポート オートメーション アナリスト インターフェース ツールを有効にできます。

- サポート オートメーション 時間を営業時間に設定する、または常にオープンに設定する

サポート デスクがクローズしているときのライブ アシスタンス リクエストの処理を指示できます。たとえば、サポート デスクの営業時間やその他のサポート オプションについてエンド ユーザに知らせる Web ページを開きます。

注: サポート オートメーション 設定項目の設定については、[オンラインヘルプ](#)を参照してください。

メッセージ ルーティング サーバ

メッセージルーティングサーバ (MRS) を使用して、ローカルサーバの地理的なロケーションにもとづいて複数のリモートコントロールサーバを管理できます。MRSを使用すると、アシスタンスセッション中のパフォーマンスを向上するのに役立ちます。MRSを有効にすると、サポートオートメーションアナリストインターフェースおよびエンドユーザクライアントはアナリストの優先 (ローカル) サーバに接続して共有しようとし、接続に失敗した場合、共有セッションはメインのデフォルトサーバに戻ります。[ライブログ] は、アシスタンスセッション中に使用する MRS を記録します。

メッセージルーティングサーバオブジェクトは、作成、更新、削除のほか、有効化と無効化が可能です。

注: メッセージルーティングサーバの設定の詳細については、オンラインヘルプを参照してください。

サポートオートメーション プライバシー レベル

プライバシーレベルは、異なるエンドユーザに対して実行可能なアクションを設定してユーザプライバシーを保護するのに使用します。プライバシーレベルは CA SDM 役割と関連付けられます。高、中、低の3つのデフォルト権限がありますが、必要に応じてその他の定義も可能です。エンドユーザが使用できるプライバシーレベルを追加、更新、および削除できます。

プライバシーレベル名およびその説明を設定できます。また、そのプライバシーレベルで有効にするツールの機能 (ファイルエクスプローラ、リモートレジストリ、プログラムの実行など) を定義できます。

注: サポートオートメーションプライバシーレベルの設定の詳細については、オンラインヘルプを参照してください。

サポート オートメーション 時間

サポート オートメーション を設定して、特定の時間または常時動作させることができます。サポート環境内のエンドユーザのニーズに応じて営業時間を管理します。サポート オートメーション がクローズされている場合は、エンドユーザはサポート オートメーション の機能にアクセスできません。1つの手順で複数のワークシフトをすばやく変更できます。

重要: ワークシフトは、サポート オートメーション 時間および個別のライブ アシスタンス キューの両方に割り当てられます。サポート オートメーション 時間および個別のキューに割り当てられた異なるワークシフトが割り当てられた場合、サポート環境内のアナリストおよびエンドユーザの競合の原因となる場合があります。

注: サポート オートメーション 時間の設定の詳細については、[オンラインヘルプ](#)を参照してください。

サポート オートメーション ツールをカスタマイズする方法

ビジネス ニーズに合わせて、サポート環境に適した サポート オートメーション ツールを設定できます。この設定により、自動タスク、チャットプリセット、デフォルト認証情報および免責条項などの管理機能を制御できます。

- サポート オートメーション アナリストがエンドユーザにサポートを提供する際に使う自動タスク リストと分類をカスタマイズする
- よくある質問や状況に対する一般的な応答のチャットプリセットを設定する
- エンドユーザのコンピュータにアクセスできるようにするデフォルト認証情報を設定する
- セルフ サービス タスクを起動する前にエンドユーザに表示される免責条項をカスタマイズする

注: サポート オートメーション ツールの設定の詳細については、[オンラインヘルプ](#)を参照してください。

自動タスク

自動タスクとは、アナリストまたはエンド ユーザが従う自動プロセスを定義する一連の手順です。自動タスクの手順は、アナリストまたはエンド ユーザのコンピュータ上で特定のアクションを行う **VBScript** または **JavaScript** 内に書き込まれたルーチンです。自動化タスク エディタを使用して、新しい自動タスクおよびタスク手順を作成することができます。よくあるルーチンとしては、遠隔測定情報の収集、問題の診断、解決の実装などがあります。

自動タスクを実行すると、ログが更新されます。このログは、アシスタンス セッション ログにリンクしており、このログからアクセスします。自動タスク ログ内のエントリは、タイムスタンプ付きのテキスト エントリで構成されています。エントリは **Functions.LogMessage ()** または **WScript.Echo ()** をコールすると作成されます。

関連項目：

[自動タスクを実装する方法 \(P. 1255\)](#)

自動タスクを設定する方法

自動化タスク エディタをインストールして設定します。このエディタでは、サポート オートメーション アナリストがエンド ユーザにサポートを提供する際に使用する自動タスクを管理できます。自動タスクは、エンド ユーザの場合はナレッジ ドキュメントとセルフ サービス インターフェースから起動できます。アナリストの場合はアシスタンス セッション時に実行できます。自動タスクは、エンド ユーザのコンピュータに関する詳細情報をアナリストに提供します。エンド ユーザとやり取りして入力を処理するセルフ サービスの自動タスクを作成します。これらのタスクとしては、ファイル システムやレジストリの変更、ソフトウェアのダウンロードとインストールなどがあります。次のように、自動タスクを設定します。

1. 自動化タスク エディタをインストールします。

インストール メディア上の次の場所からインストーラを起動します。

`casd.nt¥SAScriptWriter`

注：インストーラをコピーし、サポート環境内の適切なユーザに展開することもできます。

自動化タスク エディタがインストールされます。

2. 自動化タスク エディタを開きます。

自動化タスク エディタのインストールでは、デスクトップ上にショートカットが作成されます。

3. 以下の接続パラメータを設定します。

- a. [ツール] - [サーバ] をクリックします。

[サーバの環境設定] ダイアログ ボックスが表示されます。

- b. ホスト名とポートを入力します。

デフォルト ポート : 8070

- c. 自動化タスク エディタに対する読み書きアクセス権を持つユーザ、たとえば、サポート オートメーション **Analyst** のユーザ名とパスワードを入力します。

- d. [テスト] をクリックします。

- e. [OK] をクリックします。

4. 自動タスクを作成し、サーバにアップロードします。

パブリック タスクをアップロードし、特定のテナントやサブテナントに割り当てることができます。

重要: タスクおよびライブラリをサーバにアップロードできるのは、[パブリックの更新] フラグが有効なサービス プロバイダ テナントの役割のみです。タスク ライブラリ コンテンツおよび静的コンテンツはすべてパブリック データとして保存されます。

自動タスクを実装する方法

自動タスクを使って、サポート環境のエンドユーザを支援できます。自動タスクは、エンドユーザのコンピュータで特定のアクションを完了しますが、アナリストやエンドユーザがそのプロセスを完了する必要はありません。これらのスクリプトは、遠隔測定情報の収集、コンピュータの問題の診断、解決策の実装などで役に立ちます。

自動タスクを実装するには、以下を実行します。

1. サポート オートメーションの機会を特定します。

エンドユーザがよく遭遇する問題を特定し、解決策をいくつか自動化することでサポート コストを削減できるか判断します。

2. 考えられる解決策の自動化を調査します。

よく見られる問題の解決策を調査し、使用を予定している診断プロセスに関するデータを収集します。

3. エンドユーザ サポートを自動化するタスクを設計します。

自動化タスク エディタを使い、各タスクでエンドユーザに望む操作性を設計します。

4. 自動タスクを実装してテストします。

自動タスクをテストし、サポート環境でよく見られる問題が解決され、サポート コストの削減に役立つことを確認します。

5. 自動タスクを展開して監視します。

自動タスクを環境内のエンドユーザに展開してアナリストがアシスタンスセッションでそれらを使用できるようにするほか、スクリプトをナレッジ ドキュメントに添付できます。

重要: マルチテナンシー環境で、アナリストにタスクやライブラリ コンテンツのアップロードを許可する場合は、アナリストの役割の [パブリックの更新] オプションを有効にする必要があります。

注: CA Technologies では、自動タスクや各コンポーネント、たとえば、自動タスク ステップのテンプレートやライブラリなどを作成するトレーニングを提供できるため、環境で活用できます。自動タスクの作成の詳細については、*CA Technologies* サービスにお問い合わせください。

自動タスク管理

自動タスクを作成し、サーバに関連付けることができます。自動化タスク エディタを使うには、すべての自動タスク関連のテーブルに対して読み書きアクセス権が必要です。このアプリケーションでは、自動タスクを役割やテナントに割り当てなどのユーザ管理機能を実行できます。

注: サービス プロバイダ アナリストとして複数のテナントにアクセスする場合は、サーバに対するタスクの更新操作でテナント コンテキストを選択できます。また、自動タスクをパブリックとして割り当てることもできます。

自動タスクの展開

自動化タスク エディタで作成およびテストした自動タスクは、アシスタンス セッション、またはセルフ サービスで使えるように **CA SDM** サーバに分類に従って展開します。自動タスク定義に含まれていない設定は、タスクを展開するときに設定します。

自動タスクは、自動化タスク エディタとサーバとの間で直接アップロードやダウンロードができます。自動タスクの分類を作成する際に、適切なテナントを選択します。スクリプトをサーバにアップロードする場合は、分類、またはアクセスするテナントを選択するか、スクリプトをパブリックとして設定します。また、自動タスクは **XSDF** ファイルからインポートできるほか、**XSDF** ファイルにエクスポートできます。

重要: マルチテナンシー環境で、アナリストにタスクやライブラリ コンテンツのアップロードを許可する場合は、アナリストの役割の「パブリックの更新」オプションを有効にする必要があります。

自動タスクのアップロード

アプリケーションで作成した自動タスクをアップロードできます。タスクを選択すると、ライブラリや静的コンテンツなど、すべての従属コンテンツも自動的にアップロードされます。

自動タスクをアップロードする方法

1. 自動化タスク エディタを開きます。
サポート オートメーション タスク エディタが表示されます。
2. アップロードする自動タスクを選択します。
3. タスクをアップロードする分類を選択します。
注: マルチテナンシー環境の特権ユーザの場合、自動タスクのアップロード時に適切なテナントを選択するか、タスクをパブリックにします。
4. ツールバーで、自動タスクのアップロードアイコンを選択します。
サポート オートメーション タスク エディタは、タスクをサーバにアップロードします。

自動タスクの編集

サーバから自動タスクをダウンロードし、自動化タスク エディタで編集できます。ダウンロードしたバージョン内のコンテンツで、サーバ上の既存のコンテンツよりも新しいものは、データベースにインポートされ、そのテナントの管理者が利用できるようになります。

自動タスクを編集する方法

1. 自動化タスク エディタを開きます。

サポート オートメーション タスク エディタが表示されます。

2. ツールバーで、自動タスクのアップロード アイコンを選択します。

[サーバから自動タスクを開く] ペインが表示されます。

3. ダウンロードする自動タスクを選択します。

注: マルチテナンシー環境の特権ユーザの場合、パブリック、またはテナント固有の自動タスクを編集できます。

4. [タスクを開く] をクリックします。

サポート オートメーション タスク エディタはタスクをクライアントにダウンロードし、アプリケーションで開きます。

ダウンロードによって、タスク作成者のコンピュータには従属コンテンツを含むテキスト ファイルが作成されます。

自動タスク認証情報

管理者権限が必要なタスク、たとえばソフトウェアのインストールなどを自動タスクとして実行できるようにするには、以下のようにします。

- テナントにデフォルト認証情報を定義し、自動タスク管理でそのデフォルトの認証情報を使うように設定する
- テナントにデフォルト認証情報を定義し、[アシスタンスセッション] ウィンドウの [実行者] ダイアログを使うように選択する
- タスクに自動タスク認証情報を定義し、[アシスタンスセッション] ウィンドウの [実行者] ダイアログを使うように選択する
- [アシスタンスセッション] ウィンドウの [実行者] ダイアログで認証情報を指定する

役割の割り当て

自動タスクを使用できる役割（たとえば **Analyst**、**Administrator**）を正しく割り当てます。個別に役割を選択して自動タスクを割り当てれば、その役割に属しているアナリストのみに実行を制限できます。サポート組織内のさまざまなスキルセットや経験レベルに合わせて管理できます。

エンド ユーザがセッションに入るときに自動的に実行する診断機能など、よく実行されるタスクを選択し、タスク レベルで役割を管理できます。

役割へのアクセスレベルの割り当て

環境内の既存の **CA SDM** 役割にサポート オートメーション のアクセス レベルを割り当てることができます。

役割にアクセス レベルを割り当てる方法

1. [管理] タブで、[セキュリティと役割の管理] - [役割管理] - [役割リスト] を選択します。
[役割リスト] ページが表示されます。
2. アクセス レベルを割り当てる役割、たとえば、**Administrator** をクリックします。
[役割の詳細] ページが表示されます。
3. [編集] をクリックします。
[役割の更新] ページが表示されます。
4. [権限] タブの [SA アクセス] ドロップダウン リストから、作成したアクセス レベルを選択し、[保存] をクリックします。
[役割の詳細] ページが表示されます。サポート オートメーション のアクセス レベルが役割に割り当てられていることを確認します。

チャット プリセット管理

よくある質問や状況に対する一般的な応答を作成できます。応答を保存すれば、他のチャットセッションで使えるため、同じ情報を何度も入力する必要がなくなります。

各セッションの最初に、挨拶などのプリセットを自動的にエンド ユーザに送信できます。また、プリセットには現行セッションに固有の情報、たとえばアナリスト名を自動的に入力できます。

アシスタンス セッションでは、以下のタイプのプリセットを使用できます。

チャット プリセット

エンド ユーザの質問に対してよく使われるテキストの応答です。

URL プリセット

エンド ユーザがアクセス可能なよく使われる URL です。

各チャット プリセットはローカライズできます。チャット プリセットはエンド ユーザのローカライゼーションと同期されるため、エンド ユーザはローカライズされた適正なプリセットを受け取ります。

チャット プリセットの管理方法

よくある質問や状況に対して事前定義済みの応答を使うことができます。

1. 組織で典型的なアシスタンス セッションを理解します。
2. 組織の必要性に基づいて、チャット プリセットと URL プリセットを作成します。
3. プリセットの使用をテナント固有とするかパブリックとするか指定します。
4. (オプション) プリセット ツリー構造を複製し、ローカライズ環境を管理します。
5. アシスタンス セッション時にチャットと URL プリセットを送信します。

注: チャット プリセットの設定の詳細については、[オンライン ヘルプ](#)を参照してください。

デフォルト認証情報

通常はエンド ユーザがシステム アクセス権限を持たないアクティビティの場合でも、エンド ユーザ コンピュータ上で自動タスクの実行が可能です。現在のエンド ユーザがコンピュータについてのシステム情報を表示する管理者権限を持たない場合、デフォルト認証情報を使用してアクセスを取得し、制限付きの自動タスクを実行できます。

注: デフォルト認証情報の設定の詳細については、[オンライン ヘルプ](#)を参照してください。

免責条項

エンドユーザがセルフ サービスのタスクを起動と免責条項テキストが表示され、続行には、これに同意する必要があります。

disclaimer のビジネス オブジェクトを作成、更新、および削除できます。

注: サポート オートメーション 免責条項の設定の詳細については、オンライン ヘルプを参照してください。

セッション ログ管理

セッション ログでは、アシスタンス セッション時にアナリストが実行したすべてのアクション、たとえば、使用したツールやチャットの詳細（ウィスパーを除く）を表示できます。セッション ログは出力し、電子メールでエンドユーザに送信できます。エンドユーザはログの表示や保存はできますが、ログを変更することはできません。

セッション ログの表示

アシスタンス セッションで実行するすべてのアクションは、セッション ログを更新します。たとえば、チャット ダイアログ（ウィスパリー会話を除く）、自動タスクの結果、特定の サポート オートメーション アナリスト インターフェース ツールの使用などによって更新されます。

セッション ログを表示する方法

1. アクティブ セッション ビューを開きます。
[アクティブ セッション] ページが表示されます。
2. ツールバー、または [セッション] メニューから [セッション ログ] を選択します。
[セッション ログ] ページが表示されます。
3. [今すぐ更新] をクリックします。
ページが更新されます。
4. （オプション） [自動更新] チェック ボックスをオンにします。
5. （オプション） [ログをディスクに保存] をクリックします。
[保存] ダイアログ ボックスが表示されます。セッション ログは、HTML ファイルとしてローカルに保存できます。

サポート オートメーション レポート

CA Business Intelligence では、事前定義済みの サポート オートメーション レポートのセットがインストールされます。CA SDM は、インストール中にこれらのレポートを自動的に BusinessObjects サーバに展開します。

サポート オートメーション Administrator 役割と サポート オートメーション Analyst 役割は、BusinessObjects InfoView を使って以下に関する詳細情報と概要情報を表示できます。

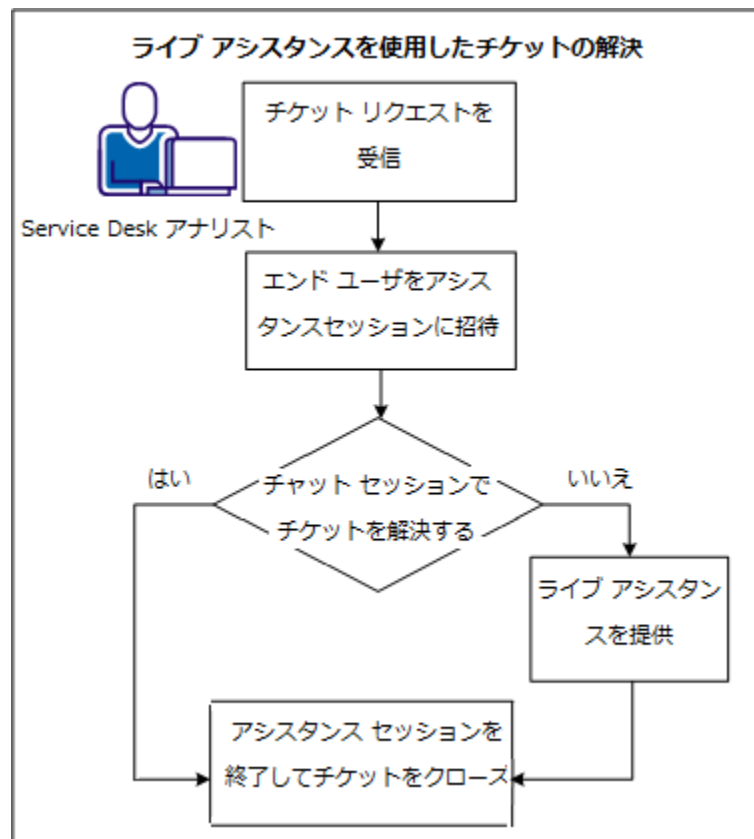
- アナリスト ログイン メトリック
- アシスタンス セッション メトリック
- キュー エントリ メトリック
- 自動タスク実行メトリック

- チケット カテゴリ別ツール使用状況
- サポート キューで待機しているエンドユーザ、アクティブなアシスタンス セッション、およびアクティブな（ログインした）アナリストに関するリアルタイム データ

注: BusinessObjects InfoView の使用方法については、オンライン ヘルプの「CA Business Intelligence」を参照してください。
ライブ アシスタンスを使用したチケットの解決

アシスタンス セッションでは、Service Desk アナリストが、CA SDM 内のエンド ユーザにチケットを解決するためのライブ アシスタンスを提供できます。コンピュータの問題が発生しているエンド ユーザに関する詳細を CA SDM チケットで確認します。ユーザとチャットし、ユーザをアシスタンス セッションに招待できます。CA SDM のサポート オートメーション機能を使用し、ライブ アシスタンスを使用して、チケットを解決します。たとえば、エンド ユーザは、ソフトウェア アプリケーションを使用してネットワーク接続問題に関するチケットを作成できます。

以下の図は、Service Desk アナリストがライブ アシスタンスを使用して、チケットを解決する方法を示しています。



以下の手順を実行して、CA SDM チケットを解決するためのライブ アシスタンスを提供します。

1. [チケット リクエストの受信](#) (P. 1265)。
2. [エンドユーザをアシスタンス セッションに招待](#) (P. 1266)。
3. [チャット セッションを使用したチケットの解決](#) (P. 1267)、または[ライブ アシスタンスの提供](#) (P. 1268)。
4. [アシスタンス セッションの終了およびチケットのクローズ](#) (P. 1269)。

チケット リクエストの受信

ユーザはそれぞれのコンピュータの問題について記述したチケットをサブミットします。電子メール アラートまたは CA SDM スコアボードからチケットの詳細を確認します。たとえば、ユーザは、それぞれのネットワークと同期するように設定したソフトウェア アプリケーションを使用できないことがあります。

次の手順に従ってください:

1. CA SDM にログインして、[スコアボード] - [あなたのキュー] を選択します。
2. チケットを開きます。
3. チケットの説明を確認します。
4. (オプション) 設定を誤っているソフトウェア アプリケーションに関する詳細情報の提供をユーザに依頼するコメントをチケットに追加します。

エンド ユーザをアシスタンス セッションに招待

チケットを解決するためにユーザをアシスタンス セッションに招待します。たとえば、エンドユーザのコンピュータのネットワーク設定に関する情報が必要になります。

次の手順に従ってください:

1. チケットの [詳細] ページの [サポート オートメーション] タブで、[エンドユーザを招待] をクリックします。
2. エンドユーザへの挨拶を入力します。
3. [起動] をクリックします。

サポート オートメーション アナリスト インターフェースが表示されるので、ユーザがアシスタンス セッションに参加するのを待ちます。

チャット セッションを使用したチケットの解決

チャットセッションを開始すると、ユーザが **CA SDM** から電子メール通知を受信します。この電子メールには、アシスタンスセッションへのリンクとチケットの詳細が含まれています。このリンクから、ユーザのコンピュータ上でサポートオートメーションエンドユーザクライアントを開きます。ユーザとチャットして、ユーザのチケットの解決方法を決定します。

注: エンドユーザが **URL** からアシスタンスセッションに参加できない場合は、ユーザに電子メールを送信して、[セルフ サービス] ホーム ページ上の [今すぐアナリストに参加] をクリックさせます。

次の手順に従ってください:

1. サポート オートメーション アナリスト インターフェース上の [チャット] タブをクリックします。
2. 以下のいずれかの操作を実行します。
 - [チャットプリセット] ドロップダウン リストから質問、ステートメント、または **URL** を選択します。
 - チャット ウィンドウにテキストを入力して、[送信] をクリックします。

たとえば、ソフトウェア アプリケーションの設定中に指定したネットワーク ポートについてエンドユーザに尋ねます。
 - エンドユーザに特定の **URL** をプッシュします。

エンドユーザは、それぞれのブラウザでリンクを手動で開きます。

ライブ アシスタンスの提供

サポート オートメーション アナリスト インターフェースを使用して、エンドユーザのコンピュータでさまざまな操作を実行することによりライブ アシスタンスを提供します。診断スクリプトの実行、ファイルシステムの参照、エンドユーザのコンピュータのリモート制御などの操作を実行します。たとえば、ユーザとチャットし、ソフトウェア アプリケーションの同期問題をライブ アシスタンスを使用することで解決できるか判断します。

次の手順に従ってください:

1. サポート オートメーション アナリスト インターフェースで、適切なツールのタブをクリックして、チケットを解決します。
 - 自動タスク -- 左ペインから自動タスクを選択し、[実行] をクリックします。たとえば、ソフトウェア アプリケーション用のネットワーク設定を行うスクリプトを実行することができます。
 - ファイル エクスプローラ -- ユーザのファイル システムを参照します。たとえば、ソフトウェア アプリケーションのインストール ディレクトリ内に特定のファイルを置くためにハード ドライブを参照できます。
 - ファイル 転送 -- コンピュータ間でファイルを転送します。たとえば、インストール ディレクトリ内の破損しているファイルを置換するためにコンピュータからファイルを転送できます。
 - リモート レジストリ -- エンドユーザ レジストリを参照し、レジストリ エントリを変更します。たとえば、ソフトウェア アプリケーションのレジストリ値を変更できます。
 - リモート システム ツール -- エンドユーザ コンピュータ上でプログラムを実行したり、コンピュータを強制的に再起動します。たとえば、ソフトウェア アプリケーションの設定 インターフェースを実行できます。
 - リモート コントロール -- エンドユーザのコンピュータをリモートで制御します。たとえば、エンドユーザ コンピュータを制御して、ソフトウェア アプリケーションを設定することができます。

- スクリーンショット -- エンドユーザ コンピュータのスクリーンショットをキャプチャします。たとえば、接続の問題によりリモート制御を正常に行えなくなった場合、スクリーンショットを表示してユーザをサポートすることができます。
- 2. [リモート コントロール] を選択し、会社のネットワークと同期するようにソフトウェア アプリケーションを設定します。
- 3. ソフトウェア アプリケーションが正常に同期し、チケットが解決されていることをユーザに確認します。

アシスタンス セッションを終了し、チケットをクローズします。

チケットが解決されたことを確認したら、チケットを更新し、アシスタンス セッションを閉じます。

次の手順に従ってください:

1. サポート オートメーション アナリスト インターフェース内の [終了] をクリックし、セッションを閉じます。
ユーザは、セッション ログの情報が記載された電子メール通知を受信します。
2. (オプション) [セッション ログ] をクリックすると、チャット ログ および サポート オートメーション ツール結果が表示されます。
3. サポート オートメーション アナリスト インターフェース上のチケット番号をクリックします。たとえば、インシデント 40 をクリックします。

CA SDM でインシデント 40 の詳細ページが表示されます。

4. [編集] をクリックします。
5. チケットのステータスを [SA - 解決済み] に変更します。
6. [保存と終了] をクリックします。

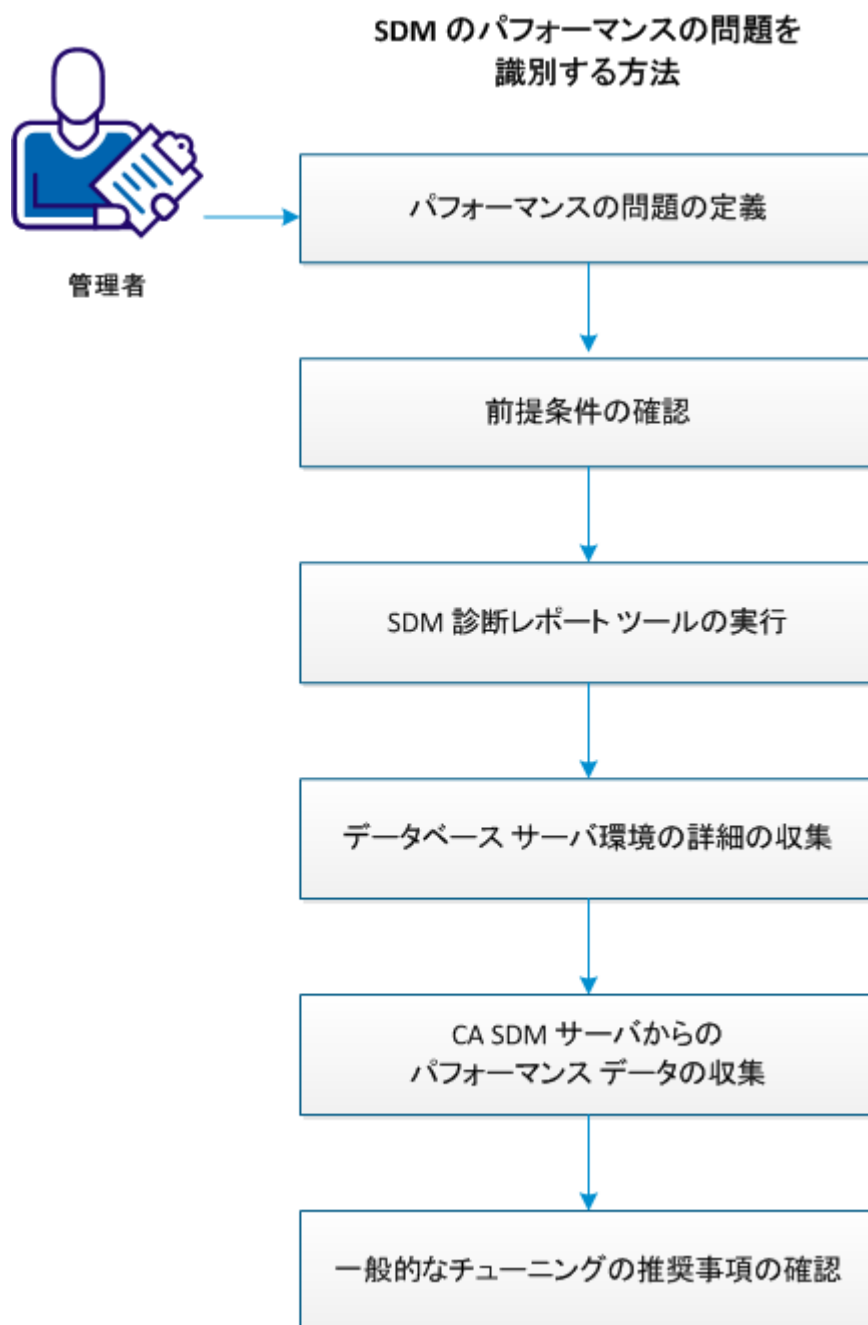
チケットのアクティビティ ログが保存され、ライブ アシスタンス プロセスが終了します。

第 25 章: CA SDM のパフォーマンスの問題を識別する方法

システム管理者は、インストール環境、リソース使用率、設定の詳細、およびその他の使用可能なシステム リソースに関する情報を収集します。たとえば、オペレーティング システムのタイプ、バージョンおよび利用可能なシステム リソースを特定して、コンピュータの設定情報を確認することができます。このデータは、CA SDM のパフォーマンスまたはメモリ関連の問題を識別および診断するのに役立ちます。CA 診断レポート ツールおよび期間ログ ユーティリティは、CA SDM 環境についての診断情報の収集に役立ちます。

以下の図は、CA SDM の診断情報を収集し、パフォーマンスの問題を識別する方法について説明しています。

Equation 2: CA SDM サーバのパフォーマンスの問題の識別



以下の手順に従います。

1. [パフォーマンスの問題を定義します](#) (P. 1273)。
2. 前提条件を確認します。
3. [CA SDM 診断レポート ツールを実行します](#) (P. 1275)。
 - Windows レポートの検証
 - UNIX レポートの検証
 - 収集された診断レポートの検証
4. [データベース サーバ環境の詳細を収集します](#) (P. 1281)。
5. CA SDM のパフォーマンス データを収集します。
6. 一般的な[チューニングの推奨事項を確認します](#) (P. 1286)。

パフォーマンスの問題の定義

最初にシステム情報を収集することで、パフォーマンスの問題を定義できます。以下の質問のリストを確認して、それらが問題に関連しているかどうかを判断します。

- ユーザはどのようなタスクを中断させる経験をしましたか。
- ユーザが最初に問題に気付いたのはいつですか。
- ハードウェアのアップグレードなど、最近環境に変更がありましたか。
- 製品のどの機能に問題が発生していますか。
- 問題の影響を受けるユーザは何人いて、それはどのようなタイプのユーザですか。
- 影響を受けないのはどのようなユーザですか。
- 問題を確認しているユーザの地理的なロケーションはどこですか。
- 影響を受けたユーザのアクセス レベルは何ですか。
- CA SDM を VMWare ESX サーバまたはその他の仮想化環境でホストしていますか。
- ESX サーバまたはホスト マシン上でほかにどのようなソフトウェアを実行していますか。
- この環境の仕様はどのようなものですか。

- 各コンピュータには CPU がいくつありますか。
- 各コンピュータにどれだけのメモリを設定していますか。

前提条件を確認します。

1. Windows オペレーティング システムの場合は、各 CA SDM サーバに `pslist.exe` ツールをインストールし、そのディレクトリ パス変数を追加します。
2. 診断ツールを実行する前に CA SDM サーバをインストールおよび設定してください。

注: 診断ツールを使用する前に、CA サポート オンラインに問い合わせることを推奨します。

Windows への Ps ツールのインストール

Windows インストールの場合は、`pslist.exe` ツールをインストールし、そのディレクトリ パス変数をシステム パス変数に追加します。

以下の手順に従います。

1. Microsoft から PS Tools Suite をダウンロードします。
2. 任意のディレクトリに `pstools.zip` を展開し、Windows の `%PATH%` 環境変数にディレクトリを追加します。
3. コマンドプロンプトから Local System ユーザとして `pslist.exe` を 1 度手動で実行し、使用許諾契約に同意します。Local System ユーザとして `pslist.exe` を実行するには、以下のコマンドを実行します。

```
psexec.exe -s -i pslist.exe
```

注: CA SDM Windows サービスは Local System アカウントではない別のユーザアカウントで開始できます。このサービスについては、そのアカウントで `pslist.exe` を実行して使用許諾契約に同意してください。CA SDM のインストールと設定の完了後に `pslist.exe` が追加された場合は、`pslist` の使用許諾契約に同意したあとで CA SDM サービスを再起動してください。

CA 診断レポート ツールからの情報の収集

CA SDM インストール メディアには、パフォーマンスの問題の診断に関する情報の収集に役立つ診断レポート ツールが含まれています。診断ツールを使用してオペレーティング システムのタイプに関する情報を収集し、CA SDM インストールからのデータ収集に使用するコマンドを判断できます。

診断ツールを実行する前に CA SDM サーバを設定してください。

以下の手順に従います。

Windows

1. `$NX_ROOT` を CA SDM インストールルート ディレクトリとして設定します。

`$NX_ROOT` のデフォルトは、Windows では `C:\Program Files\CA\Service Desk` です。デフォルト ディレクトリは、インストール処理中に必要に応じて変更できます。

2. システム パス変数に `$NX_ROOT\bin` が含まれていることを確認します。

UNIX/Linux

1. `$NX_ROOT` を CA SDM インストールルート ディレクトリとして設定します。

`$NX_ROOT` のデフォルトは、`/opt/CAisd/` (UNIX または Linux オペレーティング システム) です。デフォルト ディレクトリは、インストール中に必要に応じて変更できます。

2. `$PATH` に `$NX_ROOT/bin` が含まれていることを確認します。

CA 診断ツールの実行

CA 診断ツールにより、<http://support.ca.com> で案件をアップロードする `$NX_ROOT¥diag¥rpt` ディレクトリに .CAZ ファイル (Windows OS) または .tar.gz (UNIX) が作成されます。

以下の手順に従います。

1. Windows の場合は `supp_diag.cmd`、UNIX の場合は `supp_diag.sh` を実行します。

診断ツールは完了するまで 5 ～ 10 分かかります。

2. データ収集プロセスが完了しない場合は、診断情報の収集時に `NX_ROOT¥diag¥<host_name>_supp_diag.log` ログ ファイルを確認して、エラーを確認します。

注: バックグラウンドのバッチ ジョブをキャンセルする場合は、**Ctrl + C** キーを押してバッチ ファイルをキャンセルします。MSINFO32.exe などの一部のプロセスは、引き続きバックグラウンドで実行されます。この診断ツールの使用に関する質問がある場合は、CA サポート オンラインにお問い合わせください。

3. スクリプト ディレクトリ構造に、スクリプト ファイル、診断 ZIP ファイル、およびログ ファイルの場所が表示されます。
 - `$NX_ROOT¥diag¥bin` ディレクトリにはスクリプト ファイルが含まれています。
 - `$NX_ROOT¥diag¥rpt` ディレクトリには診断 ZIP ファイル (Windows システムの場合は .caz 形式、UNIX システムの場合は .tar.gz 形式) が含まれています。
 - `$NX_ROOT¥diag¥misc_logs` ディレクトリには、ZIP ファイルに自動的に含めることができるログ ファイルが含まれています。
4. 使用しているオペレーティング システムに応じた適切な手順を実行して、収集されたファイルを解凍します。

Windows

- コマンド プロンプトを開きます。
- .CAZ ファイルがある `$NX_ROOT¥diag¥rpt` または任意のディレクトリに `cd` コマンドで移動します。
- 以下のコマンドを実行します。

```
$NX_ROOT¥diag¥bin¥cazipxp -u <package_name> .CAZ
```


UNIX

- コマンドプロンプトを開きます。
- .tar または .tar.gz ファイルがある \$NX_ROOT/diag/rpt または任意のディレクトリに cd コマンドで移動します。
- ファイルを圧縮解除して解凍します。

```
gunzip -d <package_name>.tar.gz  
tar -xvf <package_name>.tar
```

Windows レポートの検証

以下のリストでは、作成され、**CAZ¥tar** ファイル パッケージに含まれる Windows レポート ファイルについて説明します。

Ca.olf

ca_lic ディレクトリの CA ライセンス情報を指定します。

Lic98.log

ca_lic ディレクトリの CA ライセンスに関連するログ ファイルを指定します。

Lic98version.log

ca_lic ディレクトリの CA ライセンスに関連するログ ファイルを指定します。

Licdebug.log ログ

ca_lic ディレクトリの CA ライセンスに関連するファイルを指定します。

Drwatsoninfo.txt

コンピュータのワトソン博士の設定を指定します。

<ホスト名>_env.txt

コンピュータ上で設定されている環境変数を指定します。

<ホスト名>_slstat.txt

slstat コマンドの出力を指定します。

<ホスト名>_pdm_status.txt

slstat コマンドの出力を指定します。

<ホスト名>_dir_listing.txt

Service Desk インストール ディレクトリ リストを指定します。

<ホスト名>_pslist.txt

Microsoft の pslist ツール インストール時のプロセス リストを指定します。

<ホスト名>_MSINFO32.NFO

システム情報を収集する MSINFO 出力を指定します。

<ホスト名>_SYSTEMINFO.TXT

システム情報を指定します。

<ホスト名>_appevents.csv

過去 7 日間に作成されたアプリケーション イベント ログを指定します。

<ホスト名>_sysevents.csv

過去 7 日間に作成されたアプリケーション イベント ログを指定します。

<ホスト名>_hostinfo.txt

コンピュータ情報を指定します。

<ホスト名>_prodinstallinfo.txt

CA 製品のインストール情報を指定します。

<ホスト名>_caprod_registry.txt

インストールされている CA 製品のレジストリ情報を指定します。

<ホスト名>_softfeatures.txt

Service Desk にインストールされているソフトウェア機能のリストを指定します。

<ホスト名>_ipconfig.txt

IP 構成情報を指定します。

<ホスト名>_supp_diag.log

supp_diag ツールの実行中に作成されたログを指定します。

UNIX レポートの検証

以下のリストでは、作成され、**CAZ¥tar** ファイルに含まれる **UNIX** レポート ファイルについて説明します。

Ca.olf

ca_lic ディレクトリの **CA** ライセンス情報を指定します。

Lic98.log

ca_lic ディレクトリから **CA** ライセンスに関連するログ ファイルを指定します。

<ホスト名>_env.txt

コンピュータ上で設定されている環境変数を指定します。

<ホスト名>_slstat.txt

slstat コマンドの出力を指定します。

<ホスト名>_pdm_status.txt

slstat コマンドの出力を指定します。

<ホスト名>_dir_listing.txt

Service Desk インストール ディレクトリ リストを指定します。

<ホスト名>_pslist.txt

Microsoft の pslist ツール インストール時のプロセス リストを指定します。

<ホスト名>_uname.txt

uname オペレーティング システム コマンドの出力を指定します。

<ホスト名>_diskinfo.txt

df オペレーティング システム コマンドの出力を指定します。

<ホスト名>_freemem.txt

メモリ情報の出力を指定します。

<ホスト名>_supp_diag.log

supp_diag ツールの実行中に作成されたログを指定します。

<ホスト名>_prtconf.txt

Solaris および AIX コンピュータでの prtconf オペレーティング システム コマンドの出力を指定します。

<ホスト名>_solrev.txt

Solaris コンピュータの OS バージョンおよびパッチ情報を指定します。

<ホスト名>_netconf.txt

AIX コンピュータの IP 構成情報を指定します。

収集された診断レポートの検証

デフォルトの CA SDM ドキュメント ファイル/ディレクトリ リストには、CAZ¥tar ファイルの以下のレポートが含まれます。CAZ¥tar ファイルに含める追加のファイル/ディレクトリは、\$NX_ROOT¥diag¥misc_logs ディレクトリに配置して追加します。

- \$NX_ROOT/GENLEVEL または \$NX_ROOT/.GENLEVEL
- \$NX_ROOT/<COMPUTERNAME>.his
- \$NX_ROOT/NX.env
- \$NX_ROOT/NX.env.last
- \$NX_ROOT/log¥
- \$NX_ROOT/pdmconf¥
- \$NX_ROOT/pdmconf¥version
- \$NX_ROOT/bopcfg¥www¥*.cfg
- \$NX_ROOT/site¥mods¥
- \$NX_ROOT/site¥ddict.sch
- \$NX_ROOT/site¥eh¥
- \$NX_ROOT/bopcfg¥www¥CATALINA_BASE¥logs¥
- \$NX_ROOT/bopcfg¥www¥CATALINA_BASE¥webapps¥CAisd¥WEB-INF¥web.xml
- \$NX_ROOT/bopcfg¥www¥CATALINA_BASE¥webapps¥*.xml

データベース サーバ環境の詳細の収集

CA SDM のパフォーマンスの問題の識別に役立つデータベース サーバに関する詳細を収集できます。

次の手順に従ってください:

1. データベース サーバの場所（ローカルまたはリモートなど）を決定します。
2. DBMS バージョン、オペレーティング システム バージョン、およびパッチ レベルを決定します。
3. 使用しているデータベース タイプに適した手順を実行します。

- SQL Server に対して以下のクエリを実行し、結果を記録します。

```
select @@version  
SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY ('productlevel')
```

- Oracle に対して以下のクエリを実行します。

```
select * from v$version where banner like 'Oracle%';
```

4. アプリケーション サーバにインストールしているデータベース クライアントのバージョンを確認します。
5. 可能な場合は、オペレーティング システムやその他のデータベースなどの環境データに関する情報を収集します。
6. CA SDM と統合するネットワーク トポロジとトポロジ情報またはその他の製品を収集します。

たとえば、利用可能な PDF ファイルまたは図から製品に関する情報を見つけます。

CA SDM のパフォーマンス データを収集します。

複数のサーバ設定のさまざまな CA SDM サーバ上のリソース使用率データを収集し、各サーバで発生した問題を特定できます。収集されたデータセットは、CA SDM サーバのパフォーマンスまたはメモリ関連の問題を分析したり、トラブルシューティングしたりするために使用されます。期間ログユーティリティでは、CA SDM Web インターフェースを使用して診断データの収集を開始または停止できます。収集されたデータセットを CA サポート オンラインで共有して、CA SDM サーバの問題の識別や解決に役立てることができます。

期間ログユーティリティは、サーバからログデータを収集する `pdm_intrvlog_nxd` デーモンで実行されます。デーモンは、Service Desk サーバを起動した際に自動的に起動されます。

- 期間ログデーモンを手動で停止するには、`pdm_startup` から期間ログユーティリティのエントリを削除します。
- 期間ログデーモンを手動で起動するには、`$NX_ROOT/bin` フォルダにある `pdm_intrvlog_nxd.bat` ファイルをダブルクリックします。

期間ログを使用した使用率データの収集

CA SDM サーバのリソース使用率データを収集するには、期間ログ用にサーバを設定します。各サーバから収集するデータのタイプを選択したり、サーバのログ オプションをいつでも変更したりできます。

たとえば、特定のサーバの CPU 使用率オプションのみを選択した場合、このユーティリティは、そのサーバ上の CPU 使用率データのみを収集します。

以下の手順に従います。

1. CA SDM にログインします。
2. [管理] タブで、[システム] - [期間ログ] を選択します。
[期間ログ設定リスト] が開きます。
3. [新規作成] をクリックして、期間ログ設定を追加します。
[期間ログ設定の新規作成] ページが開きます。
4. 以下のフィールドを指定します。

サーバ名

ログ データを収集するサーバを指定します。期間ログに設定できるサーバのリストを表示するには、[検索] アイコンを使用します。

再帰間隔

サーバのログ データを収集する間隔を指定します。たとえば、反復間隔が 3 分に設定されている場合、ログは 3 分ごとに収集されます。

デフォルト: 3 分

最小: 2 分

有効

期間ログがサーバに対して有効か無効かを示します。有効な場合は、サーバに対して期間ログが収集されます。

注: スケジュールされた終了日の前に期間ログを停止するには、[有効] ステータスを [いいえ] に変更します。

レコード ステータス

期間ログ設定がアクティブであるか、非アクティブであるかを示します。

スケジュール開始日

ログ データを収集する開始日を指定します。開始日を入力しない場合は、設定がアクティブで有効になるまで、またはスケジュールされた終了日まで、期間ログが直ちに開始されます。

スケジュール終了日

ログ データを収集する終了日を指定します。終了日を入力しない場合は、設定がアクティブで有効になるまで、期間ログが引き続き実行されます。

5. サーバから収集する適切なログ オプションを選択します。

たとえば、CPU 使用率データのログを収集する場合は、[CPU 使用率]を選択します。

重要業績評価指標(CPU)で使用

Windows 上で `pslist -x` を、または UNIX 上で「`ps`」を実行することによって、サーバの CPU 使用率の統計を収集します。設定タイプに応じて、以下のサーバで診断データを収集できます。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ。

メモリ使用量

Windows 上で `pslist -m` を、または UNIX 上で「`ps`」を実行することによって、サーバのメモリ使用量データを収集します。設定タイプに応じて、以下のサーバで診断データを収集できます。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ。

ネットワークのステータス

オペレーティング システムから `netstat /b` または `/a` を実行することによって、すべてのアクティブな接続およびネットワークの統計の情報を収集します。設定タイプに応じて、以下のサーバで診断データを収集できます。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ。

タスクリスト

サーバ上で実行されているすべてのタスクのアプリケーションとサービスの情報を収集します。設定タイプに応じて、以下のサーバで診断データを収集できます。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ。

Web セッション数

`pdm_webstat` コマンドを実行することによって、Web エンジンプロセスの CA SDM セッションおよびユーザ統計を収集します。任意の CA SDM サーバのデータを収集できます。

サーバステータス

`pdm_status` コマンドを実行することによって、サーバ上のすべての CA SDM デーモンまたはプロセスに関する情報を収集します。任意の CA SDM サーバのデータを収集できます。

DB レポート

`db_report` コマンドを実行することによって、データベース レコードタイプの情報を収集します。任意の CA SDM サーバのデータを収集できます。

仮想 DB の情報

`pdm_vdbinfo` コマンドを実行することによって、キューに配置済みのデータベース リクエストに関連した情報を収集します。任意の CA SDM サーバのデータを収集できます。

サーバ接続の一覧表示

`pdm_listconn` コマンドを実行することによって、サーバのアクティブな接続に関する情報を収集します。任意の CA SDM サーバのデータを収集できます。

Slump プロセスの一覧表示

`slstat` コマンドを実行することによって、Slump 接続およびプロセスに関する情報を収集します。任意の CA SDM サーバのデータを収集できます。

6. [保存] をクリックします。

サーバで期間ログが設定されます。

7. (オプション) さらに期間ログ設定を作成するには、手順 1 ～ 5 を繰り返します。

8. `$NX_ROOT¥log` ディレクトリに移動して、生成されたログ ファイルを表示します。選択する期間ログ オプションに応じて、以下の出力ファイルが生成されます。

- `cpu_usage_hostname`
- `db_report_hostname`
- `memory_usage_hostname`
- `netstat_hostname`
- `pdm_listconn_hostname`
- `pdm_vdbinfo_hostname`
- `server_status_hostname`
- `session_counts_hostname`
- `tasklist_hostname`

重要: 出力ファイルの最大サイズは、デフォルトでは **30 KB** です。

`NX_env` ファイル内の `@NX_LOGFILE_LIMIT` 値を変更することにより、ファイルサイズを変更できます。生成された出力ファイルがファイルの最大サイズを超える場合、新しいファイルがサフィックス **1** で作成されます。以降に生成されるファイルには、順番にサフィックスが付付けられます。

収集されたログ データを **CA** サポートで共有して、**SDM** インストールの問題の識別に役立てることができます。

一般的なチューニングの推奨事項の確認

ベスト プラクティスとして、キー パフォーマンス インジケータおよびリソース消費を定期的に監視することをお勧めします。また、小さな問題が深刻になる前に、小さな問題を特定するための定期的なメンテナンスが行われていることを確認します。

問題があるのではないかと感じている場合、またはユーザからパフォーマンスの低下に関するクレームが出ている場合は、**CA** サポート オンラインを開き、期間ログ データ、**CA SDM** 診断ツール レポート、**CA SDM** 標準ログ、および問題に関する情報を送信してください。各 **CA SDM** サーバから **CA** サポートに情報を送信します。

以下のリストでは、パフォーマンスの問題の一般的な兆候について説明します。

- CA SDM 標準ログ (stdlog.x ファイル) に長いメッセージがある
- 「The following query took ##### milliseconds...」と記載されているメッセージを stdlog で検索します。
- pdm_vdbinfo 出力でのデータベース エージェントへのキューイング
- pdm_vdbinfo 出力で Queued Requests(#) を検索します。このコマンドは、OS プロンプトから手動で実行できます。このコマンドは、期間ログ スクリプトでも実行されます。
- 各 Web エンジンに多数のユーザが接続している。たとえば、200 人を超えるユーザ。

注: pdm_webstat を実行して、Web エンジンあたりの同時接続ユーザの数を表示します。このコマンドは、OS プロンプトから手動で実行できます。このコマンドは、期間ログ スクリプトでも実行されます。

- ユーザのクレーム

付録 A: 参照コマンド

本付録では、CA SDM で使用可能な参照コマンドの詳細について説明します。

このセクションには、以下のトピックが含まれています。

[bop_sinfo -- システム情報の表示](#) (P. 1290)
[dbmonitor_nxd -- データベース監視デーモン](#) (P. 1291)
[pdm_backup -- ASCII ファイルへのデータベースの書き込み](#) (P. 1293)
[pdm_cache_refresh -- データベースの更新](#) (P. 1294)
[pdm_configure -- 環境設定ウィンドウを開く](#) (P. 1296)
[pdm_d_refresh -- 失敗したデーモンの起動](#) (P. 1297)
[pdm_deref -- ASCII データの修飾参照](#) (P. 1297)
[pdm_discimp -- 検出されたアセットのインポート](#) (P. 1301)
[pdm_discupd -- 検出されたアセットの更新](#) (P. 1303)
[pdm_extract -- データベースからのデータの抽出](#) (P. 1304)
[pdm_halt -- デーモンまたはサービスの終了](#) (P. 1308)
[pdm_init -- デーモンの起動](#) (P. 1309)
[pdm_key_refresh -- キャッシュされたキー情報の更新](#) (P. 1309)
[pdm_lexutil -- CA SDM 語彙集の変更](#) (P. 1310)
[pdm_k_reindex -- Knowledge Re-Index Utility](#) (P. 1311)
[pdm_listconn -- アクティブな接続のリスト](#) (P. 1315)
[pdm_load -- データベース レコードの追加、更新、および削除](#) (P. 1318)
[pdm_logfile -- stdlog のカットオーバー サイズの変更](#) (P. 1320)
[pdm_log4j_config -- ユーティリティ - log4j プロパティ ファイルの変更](#) (P. 1321)
[pdm_proctor_init -- セカンダリ サーバでの proctor の開始](#) (P. 1327)
[pdm_replace -- データベース テーブルの置換](#) (P. 1327)
[pdm_rest_util - CA SDM RESTful Web サービス アプリケーションの管理](#) (P. 1329)
[pdm_restore -- データベースの復元](#) (P. 1330)
[pdm_status -- デーモンまたはプロセスのステータスの表示](#) (P. 1332)
[pdm_task -- 環境変数の設定](#) (P. 1333)
[pdm_text_cmd -- Text API コマンドライン インターフェース](#) (P. 1333)

[pdm uconv](#)--ローカルの文字セットから UTF-8 への変換 (P. 1337)
[pdm userload](#)--データベース レコードの追加、更新、および削除 (P. 1340)
[pdm webstat](#)--Web 使用状況の統計の表示 (P. 1343)
[report](#)--レポートの生成 (P. 1348)
[rpt_srv](#)--レポートの生成 (P. 1349)
[uniconv](#)--UNIX CA NSM Event Converter デーモンの起動 (P. 1351)
[pdm_mail](#) ユーティリティ -- 電子メール情報の送信 (P. 1352)
[pdm_server_control](#) ユーティリティ -- サーバの識別 (P. 1355)

bop_sinfo -- システム情報の表示

bop_sinfo ユーティリティは、単一の **Majic** 定義のオブジェクトに関する情報を表示します。「テクニカルリファレンスガイド」にリストされているオブジェクトでこのユーティリティを実行できます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
bop_sinfo [-s server] [-p] [-l] [-d] [f] [-q] [-t] [-m] [-a] object [-h]
```

-s server

クエリするサーバを指定します。

-p

プロシージャ情報を表示します。

-l

domset リストを表示します。

-d

すべての属性の名前およびタイプを含む、データベースのオブジェクト情報を表示します。

-f

rel_attr および **common_name** を含むファクトリ情報を表示します。

-q

関連付けられたテーブルのスキーマ名を表示します。

-t

オブジェクトのトリガを表示します。

-m

オブジェクトによって使用されるメソッドを表示します。

-a

属性の詳細を表示します。

オブジェクト

クエリするオブジェクトの名前。

-h

ユーティリティのヘルプを表示します。

例: dmn オブジェクトのシステム情報の表示

```
bop_sinfo -d dmn
```

Factory dmn

Attributes

id	INTEGER
producer_id	LOCAL STRING(20)
persistent_id	STRING(30)
sym	STRING(60) REQUIRED
delete_flag	SREL -> actbool.enum REQUIRED
desc	STRING(40)
tables	BREL <- dcon.dom_id {dom_id = ?}
last_mod	DATE
last_mod_by	SREL -> cnt.id
audit_userid	LOCAL SREL -> cnt.id

dbmonitor_nxd -- データベース監視デーモン

データベース監視デーモン (dbmonitor_nxd) を使用すると、外部の CA SDM から変更が加えられたときに、特定のデータベース テーブルの CA SDM キャッシュを更新できます。

dbmonitor_nxd の主な機能は、CA SDM で発生しなかった変更に対して、指定したテーブルで **CHANGE** 通知を生成することです。この機能を実行するために、このデーモンは定期的にデータベースにクエリし、外部的に変更された部分を判別して、**CHANGE** 通知を bpvirtdb_nxd サーバに送信します。bpvirtdb_nxd サーバは、すべての domsrvr サーバに変更を通知します。これにより、各 domsrvr は特定のデータベース オブジェクトのキャッシュを更新し、指定されたテーブルの変更をサブスクライブするその他のすべてのプロセスに通知します。

このメカニズムは、監視対象のテーブルに加えられる外部的な変更の頻度が高くない場合に適切に動作します。ただし、大規模な更新が外部的に行われると、多量の **CHANGE** 通知がブロードキャストされ、さまざまな **CA SDM** プロセスから数多くのデータベース クエリが発生することになり、**CA SDM** のパフォーマンスに多大な影響を与えます。

CA SDM のパフォーマンスへの影響を最小限にするために、本製品のこのリリースで **dbmonitor_nxd** has が更新されています。このデーモンではコマンドラインインターフェースがサポートされているため、ユーザは指定したテーブルの監視を開始および停止できます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
dbmonitor_nxd -c <command> -t <tables>
```

<command>

開始または停止を入力します。

<tables>

NX_DBMONITOR_TABLES 環境変数で指定した 1 つ以上のテーブルに一致するテーブル名、またはカンマで区切られたテーブル名のリストを指定します。

各リクエストが **dbmonitor_nxd** デーモンに送信されます。デーモンは該当するアクションを実行し、アクションが実行されたことを示すメッセージをユーザに返します。

- すでに開始されているテーブルに対して開始リクエストが呼び出された場合、アクションは実行されません。
- すでに停止されているテーブルに対して停止リクエストが呼び出された場合、アクションは実行されません。
- テーブルの監視が正常に停止または開始した場合、ログ メッセージも **stdlog** に書き込まれます。

注: デーモンが特定のテーブルに対して一時停止した場合、このテーブルからデータをキャッシュしているすべての **CA SDM** プロセスが古くなりますが、このキャッシュを更新するためのプロビジョンが行われないことがあります。

たとえば、BOPLGIN は連絡先レコード (`ca_contact` テーブルおよび `usp_contact` テーブル) をキャッシュしています。外部更新がデータベースにロードされている間、デーモンが `ca_contact` テーブルに対して一時停止している場合、このキャッシュは更新されません。BOPLGIN の場合、BOPLGIN にキャッシュされている重要な連絡先属性は、`ca_contact` テーブルではなく `usp_contact` テーブルから取得されるため、この影響をほとんど受けません。

注: デーモンが特定のテーブルに対して一時停止した場合、Web ユーザは、デーモンが一時停止している間に外部的に作成された詳細フォームを表示しているときに、テーブルの変更を表示できません。

pdm_backup—ASCII ファイルへのデータベースの書き込み

`pdm_backup` を実行すると、CA SDM を停止し、CA SDM データベースから ASCII ファイルに 1 つ以上のテーブルを書き込むことができます。この出力ファイルは `pdm_restore` の入力ファイルとして使用できます。`pdm_backup` では、データベースの内容およびアプリケーションの環境設定ファイルのバックアップが作成されます。

オペレーティング環境固有のバックアップツールがある場合は、`pdm_backup` ではなくそのツールを使用することをお勧めします。`pdm_backup` は一般的なツールなので、オペレーティング環境の組み合わせによっては速度が低下する場合があります。

注: 処理の一環として、`pdm_backup` はまずデーモン (UNIX) またはサービス (Windows) を停止します。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_backup [-d] [-g] [-v] -f filename [ALL | table1...tableN]
```

-d

データベースのデータのみをバックアップするように指定します。

-g

データベース以外のデータのバックアップのみが作成されます。つまり、ウィンドウ (フォーム) と、その他のデータベース以外のデータのバックアップのみが作成されます。

-v

詳細モードを指定します。コマンドの進捗状況に関するコメントが **stdout** に書き込まれます。

-f filename

出力ファイルを指定します。

ALL|table1...tableN

出力するすべてのファイルまたはテーブルを指定します。テーブルを複数指定する場合は、スペースで区切ります。

- テーブル名は、**\$NX_ROOT/site** (UNIX) または **installation-directory¥site** (Windows) に格納されている CA SDM データベース スキーマ ファイル **ddict.sch** にあります。 **\$NX_ROOT** または **installation-directory** は CA SDM をインストールしたディレクトリです。
- テーブルを指定しない場合は、ウィンドウ グループやメニュー登録ファイルなど、CA SDM データベース全体が出力されます。

制限

CA SDM がアクティブなときは、**pdm_backup** を実行することはできません。

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に **LIBPATH** を設定する必要があります。ユーティリティを実行する前に、**pdm_task** を使用して **LIBPATH** を設定します。たとえば、「**pdm_task pdm_clean_attachments ...**」と入力します。

関連項目:

[pdm_restore—データベースの復元](#) (P. 1330)

pdm_cache_refresh—データベースの更新

pdm_cache_refresh を実行すると、**pdm_userload** やその他のデータベース ユーティリティ (CA SDM 以外のデータベース ツールも含む) を使用してデータベースにロードしたデータを、CA SDM デーモンまたはプロセスで 사용할 수 있습니다。

ほとんどの **CA SDM** デーモンおよび実行可能ファイルでは、データベースレコードの動的メモリにキャッシュが保持されます。必要なデータがすでにキャッシュに保持されている場合、データベースへのアクセスが不要になり、パフォーマンスが向上します。**CA SDM** の実行可能ファイルはデータベースの更新を相互に通知するので、キャッシュは常に最新の状態に保たれます。ただし、**pdm_userload** などの外部ユーティリティやサードパーティ データベース ユーティリティからの更新は通知されません。新規データが外部ソースからデータベースにロードされた場合は、**pdm_cache_refresh** ユーティリティを使用して、キャッシュをデータベースから更新する必要がある実行モジュールに通知します。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_cache_refresh [-f filename] [-t tablenamelist] [-d] [-v]
```

-f filename

外部で変更されたデータベース テーブルのリストが含まれるテキスト ファイルを指定します。テキスト ファイルは1行以上で構成され、各行にはスペースで区切られた1つ以上のテーブル名が含まれます。

-t tablename

外部で変更された1つ以上のテーブルを指定します。リストに複数のテーブルが含まれる場合は、テーブル名をセミコロンで区切り、リスト全体を引用符で囲む必要があります。テーブルのリストについては、「テクニカル リファレンス ガイド」の付録「データ エレメント辞書」を参照してください。

たとえば、サードパーティ ユーティリティを使用して、ロケーションおよびサイトのデータを **CA SDM** データベースにロードしたとします。**CA SDM** デーモンにこれらのテーブルのキャッシュを更新するように通知するには、以下のコマンドを実行します。

```
pdm_cache_refresh -t "Location;Site"
```

-d

メッセージを **domsrvr** (**CA SDM** ドメイン サーバ) に送信します。ドメイン サーバでは、すべての選択リストがリロードされます。このとき、クライアントに表示されたすべてのリスト ウィンドウが点滅します。

-v

詳細モードを指定します。値 **1** は概要モードです。値 **2** では進捗情報メッセージがログ ファイルに出力されます。

重要: UNIX では、一部の **CA SDM** ユーティリティを実行する前に **LIBPATH** を設定する必要があります。ユーティリティを実行する前に、**pdm_task** を使用して **LIBPATH** を設定します。たとえば、「**pdm_task pdm_clean_attachments ...**」と入力します。

pdm_configure—環境設定ウィンドウを開く

pdm_configure を実行すると、**CA SDM** の環境設定ウィンドウが含まれるウィンドウを開くことができます。このウィンドウは、**CA SDM** をインストールした後に **CA SDM** の環境設定を行う場合や、**CA SDM** を実行した後に **CA SDM** の環境設定を変更する場合に使用します。**CA SDM** の環境設定を変更する理由として、以下が考えられます。

- データベース タイプまたはサーバの変更
- データの初期設定のリロード
- **CA SDM** システム アカウントのパスワードの変更
- 変更を適用するためのスキーマ ファイルのリビルド
- **CA SDM** の設定に応じて、以下のサーバを再設定します。
 - 標準：プライマリまたはセカンダリ サーバ
 - 高可用性：アプリケーション サーバまたはバックグラウンドサーバ

構文

このコマンドのフォーマットは、以下のとおりです。

pdm_configure

制限

pdm_init は、**CA SDM** サーバまたは **CA SDM Linux** クライアントで実行できます。**pdm_configure** を実行するには、特権ユーザまたはルート ユーザである必要があります。

pdm_d_refresh—失敗したデーモンの起動

`pdm_d_refresh` コマンドラインユーティリティは、主にリモートデーモンの設定に使用します。`pdm_d_refresh` は、起動に 10 回失敗したデーモンと、デーモンマネージャによって「実行不可」に設定されたデーモンを起動するように、デーモンマネージャに通知します。このユーティリティを実行すると、すべてのデーモンが「実行可能」に設定され、再起動カウンタがリセットされます。その後、デーモンマネージャにより、停止したすべてのデーモンの起動が試行されます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_d_refresh
```

重要: UNIX では、一部の **CA SDM** ユーティリティを実行する前に **LIBPATH** を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して **LIBPATH** を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

pdm_deref—ASCII データの修飾参照

`pdm_deref` を実行すると、ASCII フォーマットの入力を処理して、1 つのデータベーステーブルで見つかったデータを別のデータベーステーブルで見つかったデータと交換することができます。また、`pdm_userload` と互換性のあるファイルを **CA SDM** 以外のデータベースまたはスプレッドシートから作成したり、**CA SDM** 以外のデータベースまたはスプレッドシートのレポートまたは出力ファイルを作成したりすることもできます。

重要: SQL を熟知していない場合は、`pdm_deref` を使用しないでください。`$NX_ROOT/samples` (UNIX) または `installation-directory\samples` (Windows) の `export` および `import` ディレクトリには、標準セットの表示用 `specfile` が含まれます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
name pdm_deref - s specfile [-c|-e|-r] [-d] [-h] [-n] [-u] [-v] <filename
```

-s specfile

(必須) 交換するデータおよびデータ交換の条件を定義するファイルを指定します。

specfile には、以下のフォーマットで SQL コマンドのリストが含まれます (「att」および「atts」は属性)。

Deref

```
{
input = <入力ファイルからの"from" atts のリスト>
output = <出力ファイルへの"to" atts のリスト>
rule = "SELECT <出力 atts に指定する atts> ¥
      FROM <テーブル名> ¥
      WHERE <入力 1 と照合するテーブル名からの att> =?¥
      AND <入力 2 と照合するテーブル名からの att> = ? ¥
      OR <入力 3 と照合するテーブル名からの att> =?"
}
```

-c

以下のように、カンマ区切り値 (CSV) 出力が生成されます。

```
"field1","field2","field3"
```

-c、-e、および-r 出力フォーマット オプションを同時に指定することはできません。

-e

二重引用符を別の二重引用符でエスケープして、カンマ区切り値 (CSV) 出力を生成できます。以下に例を示します。

```
"Text with a "quoted string" in it"
```

-c、-e、および-r 出力フォーマット オプションを同時に指定することはできません。

-r

入力ファイルに列ラベルがない場合、出力が左揃えのフォーマットで生成されます。

```
"label":"value"
```

または

```
"value"
```

このオプションは、以下のようなラインプリンタ用です。

Field_Name : フィールド値

-c、**-e**、および**-r** 出力フォーマット オプションを同時に指定することはできません。

-d

診断情報が生成されます。

-h

ヘルプおよび使用法が表示されます。

-n

値が **0** の外部キーを **NULL** として処理しないことを指定します。この引数は、損傷したデータベースを復旧するような特殊な状況下でのみ使用します。

-u

ヘッダのない出力が生成されます。

-v [1|2]

詳細モードを指定します。値 **1** は概要モードです。値 **2** では進捗情報メッセージがログ ファイルに出力されます。

filename

(オプション) ASCII フォーマットの入力ファイルを処理するように指定します。省略すると、**stdin** が使用されます。

制限事項 : **UNIX** でのみ有効です。

UNIX で **pdm_deref** を使用する前に、**\$NX_ROOT** 環境変数を **CA SDM** インストールディレクトリのパスに設定し、**PATH** 環境変数に **\$NX_ROOT/bin** を含める必要があります。

例:pdm_deref を使用した入力用データの設定

この例では、pdm_deref を使用して入力用データを設定する方法を示します。

ca_location テーブルの以下のデータを例に考えます。

```
id      location_name_name
86873FA40BA4234A8CF7A418D7C8B2DB    "Boulder NCC"
```

以下の specfile のステートメントが使用されます。

```
Deref
{
input = place
output = location_uuid
rule = "SELECT id FROM ca_location WHERE location_name=?"
}
```

以下の入力に変更されます。

```
last_name, first_name, place
{"Potts", "Elmore", "Boulder NCC"}
```

以下の出力に変更されます。この出力は、pdm_userload を使用して ca.contact テーブルにロードできます。

```
last_name, first_name, location_uuid
{"Potts", "Elmore", "86873FA40BA4234A8CF7A418D7C8B2DB"}
```

例:pdm_deref を使用した出力用データの設定

この例では、pdm_deref を使用して出力用データを設定する方法を示します。

ca_contact テーブルの以下のデータを例に考えます。

```
id last_name first_name
"69499D5A2424884887E62EC9823F5E47"    "Potts"    "Elmore"
```


以下の specfile のステートメントが使用されます。

```
Deref
{
input = primary_contact_uuid
output = firstname, lastname
rule = "SELECT first_name, last_name FROM ca_contact
WHERE id=?"
}
```

以下の入力に変更されます。

```
location_name, primary_contact_uuid
{"Boulder NCC", "69499D5A2424884887E62EC9823F5E47"}
```

以下の出力に変更されます。この出力は、印刷したりスプレッドシートに送信したりできます。

```
location_name, firstname, lastname
{"Boulder NCC", "Elmore", "Potts"}
```

関連項目:

[pdm extract—データベースからのデータの抽出](#) (P. 1304)

pdm_discimp -- 検出されたアセットのインポート

CA SDM 以外で検出されたアセットをバッチ登録します。このプログラムを使用すると、ほかのソフトウェア製品で登録されたアセットの MDB を検索し、CA SDM のアセットとして登録して、CA SDM で使用することができます。

論理的には、アセットの検索/リスト Web フォームから起動できる [検出されたアセット] ダイアログボックスに似ています。[検出されたアセット] ダイアログボックスは対話型のバッチプロセスです。

このプログラムでは、各種パラメータを使用して `ca_logical_asset`、`ca_asset`、および `ca_logical_asset_property` の各テーブルのクエリを実行し、検出された値のうち新規の CA SDM アセットを登録しようとします。

構文

```
pdm_discimp [-l label] [-s serial number] [-t asset tag] [-n hostname] [-d dns name]  
[-m mac address] [-c asset class] [-v] [-r] [-o object manager]
```

アセットの選択基準（ワイルドカードには%を使用）：

l

このアセット ラベルに一致します。

s

このシリアル番号に一致します。

t

このアセット タグに一致します。

n

このホスト名に一致します。

アセットのプロパティの選択基準（ワイルドカードには%を使用）：

d

この DNS 名に一致します。

m

この MAC アドレスに一致します。

その他のオプション：

c

新しく所有したアセットの初期設定を、検出されたハードウェアに登録するときに割り当てるアセット クラス。

v

詳細/診断モードを指定します。

r

アセットを登録します。登録しないと、擬似モードで実行されます。

h

情報を表示します。

0

オブジェクトマネージャ（domsrvr）を処理に使用します。

注: 処理の結果、[アセット ラベル] が空白の場合は、[ホスト名] または [DNS 名] の値が [アセット ラベル] の値として使用されます。アセットには、CA SDM で使用するために登録されるラベルおよびアセットクラスが最低 1 つ必要です。

MDB の構造および CA SDM のアーキテクチャ制限により、2 つのクエリが実行され、適切なレコードを選択して処理できます。パフォーマンスが影響を受ける場合があるので注意してください。1 つ目のクエリでは、ラベル、シリアル番号、タグ、およびホスト名に一致する `ca_logical_asset` テーブルと `ca_asset` テーブルの間の結合から行が取得されます。次に、結果行それぞれについて、`ca_logical_asset_property` にクエリを実行して、`dns_name` と `mac_address` に一致するかどうかを調べます。2 つ目のクエリの結果で行が返された場合は、1 つ目のクエリからのアセットは登録用に選択されます。

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に `LIBPATH` を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して `LIBPATH` を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

pdm_discupd -- 検出されたアセットの更新

CA SDM 以外で検出されたアセットをバッチ更新します。このユーティリティを使用して、`pdm_discimp` コマンドによってインポートされたアセットを更新します。

構文

```
pdm_discupd [-t] [-v] [-d domsrvr]
```

条件

t

テスト

v

詳細/診断モードを指定します。

d

オブジェクトマネージャ（domsrvr）を処理に使用します。

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に LIBPATH を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して LIBPATH を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

pdm_extract—データベースからのデータの抽出

`pdm_extract` コマンドを実行すると、指定した CA SDM データベース テーブルまたは CA SDM データベース全体からデータを抽出し、ASCII フォーマットのテキストとして出力することができます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_extract [-c|-e|-r] [-d] [-h] [-u] [-v] [-C] [--B] [-f formatstring| ALL | table1 . . . TableN]
```

-c

以下のように、カンマ区切り値（CSV）出力が生成されます。

```
"field1","field2","field3"
```

-c、-e、および-r 出力フォーマット オプションを同時に指定することはできません。

-e

二重引用符を別の二重引用符でエスケープして、カンマ区切り値（CSV）出力を生成できます。以下に例を示します。

```
"Text with a "quoted string" in it"
```

-c、-e、および-r 出力フォーマット オプションを同時に指定することはできません。

-r

入力ファイルに列ラベルがない場合、出力が左揃えのフォーマットで生成されます。

```
"label": "value"
```

または

```
"value"
```

このオプションは、以下のようなラインプリンタ用です。

Field_Name: フィールド値

-c、-e、および-r 出力フォーマット オプションを同時に指定することはできません。

-d

ファイル\$NX_ROOT/fig/english/cfg/dataent.fmt (UNIX) または *installation-directory¥fig¥english¥cfg¥dataent.fmt* (Windows) の日付形式を使用します。必要に応じて編集できます。

-h

ヘルプおよび使用法が表示されます。

-u

ヘッダのない出力が生成されます。

-v

詳細モードを指定します。コマンドの進捗状況に関するコメントが **stdout** に書き込まれます。

-C

エンコーディングを **UTF-8** から他の文字セットに変更します。デフォルト出力は **UTF-8** です。

例：出力を **JIS** に変換するには、「**-C iso-2022-jp**」を実行します。

例：オペレーティングシステムのネイティブ文字セットにエンコードするには、「**DEFAULT**」または「**NATIVE**」を使用します。

-B-

変数 `NX_ADD_UTF8_BYTE_ORDER_MARK` が設定されている場合は、バイト順マークを抑制します。

`NX_ADD_UTF8_BYTE_ORDER_MARK` オプションは、ファイルに挿入されるシグネチャです。これによって、UTF-8 をサポートするエディタで、ファイルの UTF-8 の整合性が維持されるようになります。

注: これが必要になるのは、非 ASCII データの場合のみです。これがインストールされていない場合は、デフォルトの動作としてバイト順マーク (BOM) が省略されます。インストールされている場合は、「1」または「Yes」に設定します。

-f *formatstring*

formatstring (SQL サブセット ステートメント) に従って、特定のレコードおよびフィールドが抽出されます。

一定期間後の日付の場合は、以下の構文を使用します。

```
pdm_extract -v -f "select id, ref_num from Call_Req where open_date >=
DATE '2005-02-24'" > daterange1.txt
```

日付範囲の場合は、以下の構文を使用します。

```
pdm_extract -v -f "select id, ref_num from Call_Req where open_date >=
DATE '2004-01-20' and open_date < DATE '2004-02-25'" > daterange2.txt
```

注: YYYY-MM-DD フォーマットの日付は一重引用符で囲みます。

DATE の構文は以下のとおりです。

DATE 'yyyy-mm-dd'

yyyy = 年を表す整数 (1970～2038)

mm = 月を表す整数

dd = 日を表す整数

例:

DATE '2005-01-18'

DATE '1999-12-25'

タイムスタンプの構文：

```
TIMESTAMP 'yyyy-mm-dd hh.mm.ss[.nnnnnn][[+|-][hh.mm]]
```

yyyy = 年を表す整数（1970～2038）

mm = 月を表す整数

dd = 日を表す整数

hh = 時間を表す整数

mm = 分を表す整数

ss = 秒を表す整数

nnnn = ミリ秒を表す整数（省略可能）

[+|-][hh.mm] = タイムゾーン間隔（省略可能）

例：

```
TIMESTAMP '1998-04-28 12:00:00.000000'
```

```
TIMESTAMP '2004-10-17 18:30:45'
```

```
TIMESTAMP '2005-03-21 12:00:12+08:00'
```

```
TIMESTAMP '1999-05-10 09:12:23.005-03:30'
```

注:-d オプションは、出力のフォーマットにしか影響しないので不要です。

以下に、コマンドの使用例を示します。

```
pdm_extract -f "select * from Call_Req where open_date > TIMESTAMP '2004-01-12 12:00:00'"
```

この例では、open_date が 2004 年 1 月 12 日深夜 0 時以降の Call_Req テーブルからすべての列が抽出されています。

すべて

データベース内のすべてのテーブルから出力が抽出されます。

```
table1. . . tableN
```

指定したテーブルから出力が抽出されます。テーブル名はスペースで区切る必要があります。

オプションを指定しない場合、フォーマットは初期設定では pdm_userload と互換性のある ASCII ファイルになります。

関連項目:

[pdm_deref—ASCII データの修飾参照](#) (P. 1297)

[pdm_replace—データベース テーブルの置換](#) (P. 1327)

[pdm_userload—データベース レコードの追加、更新、および削除](#) (P. 1340)

[rpt_srv—レポートの生成](#) (P. 1349)

pdm_halt—デーモンまたはサービスの終了

pdm_halt を実行すると、そのシステムのすべての CA SDM デーモン (UNIX) または System Server Service (Windows) を終了できます。pdm_halt ユーティリティは、通常 30 秒で完了します。2 分以上ハングアップする場合は、Ctrl + C キーを押して pdm_halt を終了し、やり直してください。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_halt [-w] [-a] [time]
```

-w

デーモンが停止するのを待ちます。

-a

pdm_startup ファイルで定義されている Proctor をすべて停止します。

[time]

コマンド実行までの待機秒数を指定します。

制限

pdm_halt は、CA SDM サーバーまたは CA SDM UNIX クライアントで実行できます。pdm_halt を実行するには、特権ユーザである必要があります。

pdm_init—デーモンの起動

UNIX のみに適用

pdm_init を実行すると、そのシステムのすべての CA SDM 自動プロセスを起動できます。これらの自動プロセスはデーモンと呼ばれ、ユーザの作業中はバックグラウンドで継続的に実行されます。すべてのデーモンを起動できるわけではありません。特定のオペレーティングシステムでしか使用できないデーモンもあります。このコマンドで起動できるデーモンのリストについては、「サーバ管理」の章を参照してください。

注: 初回に起動しなかったデーモンの問題を解決してから pdm_d_refresh を使用すると、そのデーモンを起動できます。ほとんどの場合、初回に失敗したデーモンを起動するために実行中のデーモンを終了する必要はありません。

構文

```
pdm_init
```

制限

pdm_init は、CA SDM サーバーまたは CA SDM UNIX クライアントで実行できます。pdm_init を実行するには、特権ユーザである必要があります。

pdm_key_refresh—キャッシュされたキー情報の更新

pdm_key_refresh ユーティリティを使用すると、データベースのキーコントロールテーブルからキャッシュされたキー情報を更新できます。キーコントロール情報を更新する場合は、システムを停止して再起動する代わりにこのユーティリティを実行すると、CA SDM で新しいキー ID のベース値を強制的に使用することができます。

重要: キーコントロールテーブルを変更すると、データが破損することがあります。キーコントロールは、CA のテクニカルサポートから指示があった場合にのみ変更してください。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_key_refresh
```

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に LIBPATH を設定する必要があります。ユーティリティを実行する前に、*pdm_task* を使用して LIBPATH を設定します。たとえば、「*pdm_task pdm_clean_attachments ...*」と入力します。

pdm_lexutil--CA SDM 語彙集の変更

pdm_lexutil ユーティリティを使用して、Service Desk 語彙集を変更したり、スペルチェック辞書の語句を追加または削除したりできます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_lexutil -a | -d [-f] [-l] wordlist
```

-a

語句を追加します。

-d

語句を削除します。

-f

追加または削除する語句のリストを含むファイルまたは語彙集。

-l

語彙集の名前。

デフォルト : userdict.tlx

wordlist

追加または削除する語句。

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に LIBPATH を設定する必要があります。ユーティリティを実行する前に、*pdm_task* を使用して LIBPATH を設定します。たとえば、「*pdm_task pdm_clean_attachments ...*」と入力します。

pdm_k_reindex—Knowledge Re-Index Utility

ナレッジインデックス再作成ユーティリティの `pdm_k_reindex.exe` はナレッジマネジメントインストールディレクトリ内にあります。

注: ナレッジベースのドキュメントのインデックス再作成は、データベースのサイズによっては処理に時間がかかる可能性があります。変更を加えた後は、ナレッジインデックス再作成ユーティリティを実行することをお勧めします。高可用性設定では、フェールオーバー中にナレッジインデックス再作成ユーティリティを実行できません。

重要: UNIX では、一部の **CA SDM** ユーティリティを実行する前に **LIBPATH** を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して **LIBPATH** を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

次の手順に従ってください:

1. コマンドプロンプトを開きます。
2. ナレッジのインデックス再作成を実行するには、コマンドプロンプトで以下のコマンドを入力します。

以下に例を示します。

```
pdm_k_reindex
```

このコマンドでは、以下のオプションを使用できます。

-D

デバッグモード（コマンドウィンドウへの出力など）を定義します。

-v

詳細モード（`stdlog` ファイルへの出力など）を定義します。

-i

インデックスの再作成後に、インデックス再作成テーブルでテーブルインデックスを作成しません。

注:「-D」のようにプレフィックスとしてダッシュが使用されているパラメータは、ダッシュのないほかのパラメータの前に記述します。

その他のオプションは以下のとおりです。

File:reindex.txt

指定されたファイルにドキュメントのインデックスが再作成されます。

+i

インデックスが再作成されたテーブルのインデックスのみを作成します。このテーブルがインデックス再作成後の検索テーブルです。古いインデックスは、インデックス再作成の前に削除されます。

+t

検索テーブルおよびインデックス再作成テーブルの名前のみを切り替えます。

注:「+」プレフィックスは、このパラメータのみが適用されることを示します。

sdtout

コマンドウィンドウに表示される統計の頻度を定義します。デフォルトでは、ナレッジインデックス再作成ユーティリティは **1000** ドキュメントを処理するごとにコマンドウィンドウに統計を表示します。ただし、これより頻繁に統計が必要な場合もあります。以下のパラメータを使用します。

`pdm_k_reindex -i sdtout:10`

この場合、統計はドキュメント **10** 件ごとにコマンドウィンドウに表示されます。

これらのドキュメントは、ナレッジベース内にインデックスが再作成されます。

pdm_k_reindex を使用するタイミング

以下の検索設定を 1 つ以上変更した場合は、pdm_k_reindex ユーティリティを実行します。

- ノイズワード
- 同義語
- 特殊用語
- 言語
- 類似語を除外
- ノイズワードを除外
- 有効な文字範囲
- 特殊用語を識別

変更が行われると、該当するメッセージが [管理] タブの [ナレッジ] ノードに表示されます。

インデックス再作成のトラッキング

インデックス再作成の実行中は、ページの下半分にある [Re-Index Tracking] セクションで処理のステータスを表示できます。各フィールドの説明は以下のとおりです。

ドキュメント番号

処理済みのドキュメントの数を指定します。

平均サイズ(ワード)

現在のドキュメントのサイズを指定します。ワード数からノイズワード数を引いて計算されます。

速度(ドキュメント/秒)

1 秒あたりに処理されたドキュメントの数を指定します。

開始からの時間

開始してからのインデックス再作成処理の実行時間を示します。

残り時間

現在の速度と残りのドキュメント数から予定される残りの処理時間を指定します。

障害番号

失敗したドキュメントの数を表します（最大は 100）。失敗の数が最大値に達すると、管理者にはプロセスの継続またはキャンセルを要求するプロンプトが表示されます。

注: ノイズワード、特殊用語、同義語、またはパース設定を変更してインデックスを再作成しないと、[管理] タブの [ナレッジ] ノードに次回アクセスしたときにプロンプトが表示されます。変更内容が有効になるのは、Knowledge Re-Indexing ユーティリティを実行した後のみです。

インポートとインデックス再作成

コマンドラインから `pdm_kit.exe` を呼び出した場合は、`pdm_kit` ユーティリティによってドキュメントがデータベースにインポートされます。`pdm_kit` の実行が完了した後、コマンドライン オプションでドキュメントのインデックス作成およびインデックス再作成が無効にされていなければ、インデックス再作成ユーティリティ (`pdm_k_reindex.exe`) が自動的に呼び出されます。インデックス再作成処理のステータスおよび出力は、`$NX_ROOT¥log` ディレクトリの「`EBR_REINDEX.LOG`」に自動的に書き込まれます。

バッチ処理とインスタント処理用のインデックス作成およびインデックス解除のキュー設定

インデックス作成とインデックス解除によってバッチ処理が実行され、1 回の実行であらかじめ定義された数のドキュメントが追加されます。このようなバッチ処理は、パフォーマンス最適化のために使用されます。バッチに含まれるドキュメントが多くなると、システムのパフォーマンスが向上します。

処理できるドキュメントの数は制限されています。この制限は、ドキュメントおよびリンクされている添付ファイルのサイズに依存します。ドキュメントのサイズは、純粋なテキストと添付ファイルに基づいて計算されます。イメージとフォーマット要素は計算されません。

注: [管理] タブで [添付ファイル ライブラリ] - [リポジトリ] と移動し、リポジトリを編集して [ファイルの制限サイズ (KB)] を設定すると、添付ファイルのサイズを制限できます。

最大バッチ サイズの推奨値は 2 MB から 12 MB です (NX.env ファイルの EBR_MAX_INDEX_BATCH_SIZE パラメータと平均ドキュメント サイズに従う)。

- 添付ファイルを含むドキュメントの平均サイズが 0.1 MB 程度の場合は、NX.env の以下のデフォルト設定をそのまま使用してください。

```
@EBR_MAX_INDEX_BATCH_SIZE=128
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=1
@NX_EBR_INDEX_QUEUE_ONLINE=Yes
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
```

この設定は、1 回のバッチには 128 ドキュメントが含まれており、バッチの実行間隔が 10 秒、インデックス再作成時の 2 回のバッチ間の待機間隔が 1 秒であることを表しています。

- 添付ファイルを含むドキュメントの平均サイズが 0.5 MB 程度の場合は、NX.env のデフォルト設定をそのまま使用してください。

```
@EBR_MAX_INDEX_BATCH_SIZE=25
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=10
@NX_EBR_INDEX_QUEUE_ONLINE=No
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
```

この設定は、1 回のバッチには 25 ドキュメントが含まれており、バッチの実行間隔が 10 秒、インデックス再作成時の 2 回のバッチ間の待機間隔が 10 秒であることを表しています。

pdm_listconn—アクティブな接続のリスト

pdm_listconn ユーティリティを使用すると、クライアントとサーバ両方のアクティブな接続のリストを表示できます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_listconn [-c] [-s] [-s -c] [-t nn] [proc1 [proc2...]]
```

パラメータを指定しない場合、デフォルトのコマンドのフォーマットは以下ようになります。

```
pdm_listconn -s -t 2
```

-c

クライアント別に接続のリストを表示します。以下のように、クライアントごとに 2 行表示されます。

```
(n secs) client_type node|cproc
```

```
connected to alias (sproc) at time
```

n は、クライアントの応答にかかった秒数です。

client_type は、「vbop」、「animator daemon」、または「web engine」です。

node は、クライアントのノードの IP アドレスです。

cproc は、クライアントの Slump プロセス名です。

alias は、クライアントが接続しているサーバの別名です。

sproc は、サーバの Slump プロセス名です。

time は、接続時間です。

以下に例を示します。

```
(0 secs) vbop client 141.202.211.34|vbop-0x40120000:anthill:0
```

```
connected to CMD40120 on anthill (domsrvr) at 1999/02/19 10:44:16
```

-s

サーバ別に接続のリストを表示します（初期設定）。以下のように、サーバごとに 2 行表示されます。

```
(n secs) server alias (node|sproc) willingness willingness
```

```
count connected clients (use pdm_listconn -c -s to list clients by server)
```

n は、サーバの応答にかかった秒数です。

node は、サーバのノードの IP アドレスです。

alias は、クライアントが接続しているサーバの別名です。

sproc は、サーバの Slump プロセス名です。

willingness は、サーバが新規クライアントを受け入れる *willingness* 値です（0～100）。

count は、接続されたクライアントの数です。

以下に例を示します。

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients (use pdm_listconn -c -s to list clients by server)
  vbop client 141.202.211.34|vbop2 connected 1999/02/19 10:53:16
  vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 1999/02/19
10:44:17
```

-s -c

サーバ別に接続のリストを表示します。各サーバのクライアントの詳細も含まれます。以下のように、サーバごとに複数行表示されます。

```
(n secs) server  alias (node|sproc) willingness willingness
count connected clients:
client_type node|cproc connected time
```

各項目は以下のとおりです。

n は、サーバの応答にかかった秒数です。

node は、サーバのノードの IP アドレスです。

alias は、クライアントが接続しているサーバの別名です。

sproc は、サーバの Slump プロセス名です。

willingness は、サーバが新規クライアントを受け入れる *willingness* 値です (0~100)。

count は、接続されたクライアントの数です。

client_type は、「vbop」、「animator daemon」、または「web engine」です。

node は、クライアントのノードの IP アドレスです。

cpoc は、クライアントの Slump プロセス名です。

time は、接続時間です。

以下に例を示します。

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients:
  vbop client 141.202.211.34|vbop2 connected 1999/02/19 10:53:16
  vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 1999/02/19
10:44:17
```

-t nn

タイムアウト間隔を秒数で指定します。 `pdm_listconn` は、未知数のクライアントおよびサーバから情報を受信するため、最後のメッセージを受信してから指定したタイムアウト間隔が経過すると終了します。

デフォルト：2

proc1

1 つ以上の **Slump** プロセス名をスペースで区切って指定します。このユーティリティを使用すると、**Slump** プロセス名からのクライアントまたはサーバ情報が必要に応じて表示されます。

重要: UNIX では、一部の **CA SDM** ユーティリティを実行する前に **LIBPATH** を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して **LIBPATH** を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

pdm_load—データベースレコードの追加、更新、および削除

重要: `pdm_load` を使用すると、データが破損することがあります。このため、`pdm_load` を実行する場合は、必ず先にデータベースのバックアップを作成してください。また、`pdm_load` を使用するように指示されない限り、`pdm_userload` を使用してください。

`pdm_load` を実行すると、指定した入力ファイル（最大 112 属性）を使用して、**CA SDM** データベースを更新できます。

チケット（リクエストや案件など）をアップロードするときは、必ずチケット番号の文字列に一意のプレフィックスまたはサフィックスを追加してください。**CA SDM** では、この番号はシーケンス番号ではなく文字列として表示されるので、アップロードされたチケットに一意の番号が割り当てられるとは限りません。`awk` などのテキストプロセッサを使用して一意のプレフィックスまたはサフィックスを割り当てると、前に割り当てられた番号を **CA SDM** で上書きすることなく、チケットをアップロードすることができます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_load [-c] [-h] [-m] [-r] [-u] [-v] -f filename
```

入力ファイルのエントリは、以下のフォーマットに従います。

```
TABLE table_name
fieldname1 fieldname2 . . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

table_name は、ロードするテーブルの名前で、CA SDM データベース スキーマ ファイル `$NX_ROOT/site/schema.sch` (UNIX) または `installation-directory¥site¥schema.sch` (Windows) にあります。`$NX_ROOT` または `installation-directory` は CA SDM をインストールしたディレクトリです。

-f filename

入力 ASCII ファイルを指定します。

-c

入力ファイルとデータベースを比較して、実行された更新について報告します。更新は行いません。

-m

一括更新を指定します。 `pdm_load` を使用して多数のレコードを追加または削除する場合に指定します。このオプションを指定すると、クライアントのすべての更新通知が無効になり、`pdm_load` によるテーブルの処理が終了したときにテーブルのキャッシュ更新メッセージが送信されます。

-r

入力レコードに一致するデータベース レコードを削除します。

重要: このオプションを使用して `pdm_load` を実行する前に、データベースのバックアップ コピーを作成してください。古いデータベース レコードを削除した後で、削除したレコードを復旧する場合は、このバックアップ コピーを使用して CA SDM データベースを復元します。

-u

既存のレコードを更新します。新しいレコードはデータベースに挿入されません。

関連項目:

[pdm replace—データベース テーブルの置換 \(P. 1327\)](#)

[pdm userload—データベース レコードの追加、更新、および削除 \(P. 1340\)](#)

[pdm backup—ASCII ファイルへのデータベースの書き込み \(P. 1293\)](#)

[pdm restore—データベースの復元 \(P. 1330\)](#)

pdm_logfile—stdlog のカットオーバー サイズの変更

pdm_logfile では、stdlog.x のカットオーバー サイズを変更することができます。カットオーバーは、指定したバイト数が書き込まれると発生します。UNIX では、この値は pdm_init ごとにリセットされます。Windows では、pdm_halt および pdm_init ごとに設定が維持されます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_logfile [-L|-h]
```

または

```
pdm_logfile [-g -h] [-b bytes]
```

例

stdlog.x ファイルを 500,000 バイトでカットオーバーするように変更するには、以下のコマンドを実行します。

```
pdm_logfile -f STD -b 500000
```

-L

現在のカットオーバーのリストを作成します。

-q

pdm_logfile を Quiet モードで実行します。

-b bytes

カットオーバーが発生するまでに書き込まれるバイト数を指定します。

制限

CA SDM がアクティブなときに `pdm_load` を実行できますが、パフォーマンスが非常に低下する可能性があります。`pdm_load` は、CA SDM にログインしているユーザがいないときに実行することをお勧めします。

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に `LIBPATH` を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して `LIBPATH` を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

pdm_log4j_config ユーティリティ - log4j プロパティファイルの変更

`pdm_log4j_config.pl` ユーティリティを使用して、CA SDM の `log4j` プロパティファイル、Web コンポーネント、PDM_RPC、サポート オートメーション、REST、および CMDB Visualizer を設定できます。環境に基づいてユーティリティ バッチ スクリプトを実行します。Windows の場合は、コマンドラインから `pdm_log4j_config` を実行します。UNIX の場合は、`pdm_log4j_config.sh` ファイルを実行します。

このコマンドのフォーマットは、以下のとおりです。

```
pdm_log4j_config - f <コンポーネント> -d
pdm_log4j_config -h
pdm_log4j_config - f <component> [-a | -n <name>] [-l <log level>] [I <max # of log files>] [-s <max size of log files>] [-t <log level threshold>]
```

-f

変更する CA SDM の `log4j` 設定、または CA SDM のコンポーネントを指定します。以下のいずれかの値を入力します。

SDM_WEB、SDM_RPC、REST、SA または Viz。

注: 必須オプションを他のオプションと共に使用してください。

-d

`log4j.properties` の現在の設定を表示します。

-h

ユーティリティのヘルプを表示します。

-a

log4j.properties に対するすべての変更をグローバルに適用します。

-n

特定のクラス名またはパッケージ名のみ変更することを指定します。

bop_logging など特定のクラス名を指定するか、または
com.ca.ServicePlus など完全なパッケージ名を指定します。

-l

設定するログ レベルを指定します。

注: -a または -n オプションを指定します。

-i

設定する最大ファイル番号インデックスを指定します。

注: -a または -n オプションを指定します。

-s

設定する最大ファイルサイズを指定します。

注: -a または -n オプションを指定します。

重要: このパラメータを指定してコマンドを実行する前に、Visualizer
の log4j.properties ファイルのアペンダを Rolling File Appender に変更し
ます。アペンダを変更しないと、MaxFileSize により同じファイルにロ
グが生成されます。

-t

ログ レベルしきい値を指定します。

注: -a または -n オプションを指定します。

ユーティリティの使用例

以下に、pdm_log4j_config ユーティリティの使用例を示します。

- -l および -a 変数を使用して、プロパティ ファイルに設定されているすべてのロガーのログ詳細レベルを変更します。

たとえば、サポート オートメーション で設定されているすべてのロガーを **DEBUG** レベルに設定します。

```
pdm_log4j_config -f SA -a -l DEBUG
```

- -l および -n 変数を使用して、CA SDM log4j プロパティ ファイル内の特定のロガー クラスまたはパッケージ名のログ詳細レベルを変更します。

たとえば、以下のいずれかのサンプル コードを使用して、pdm_rpc パッケージのロガーを **DEBUG** に設定します。

```
pdm_log4j_config -f SDM_RPC -n pdm_rpc -l DEBUG
```

```
pdm_log4j_config -f SDM_RPC -n com.ca.ServicePlus.pdm_rpc -l DEBUG
```

- REST の log4j プロパティ ファイルで -i および -a 変数を使用して、すべてのアペンダ (**MaxBackupIndex** プロパティ) に対して作成するログ ファイルの最大数を変更します。

たとえば、すべてのアペンダのファイルの最大数を **9** に設定します。

```
pdm_log4j_config -f REST -a -i 9
```

- -i および -n 変数を使用して、特定のクラスまたは一連のクラス (**MaxBackupIndex** プロパティ) のアペンダに対して作成するように、CA SDM log4j プロパティ ファイルで設定されているログ ファイルの最大数を変更します。

たとえば、bop_logging のファイルの最大数を **7** に設定します。

```
pdm_log4j_config -f SDM_WEB -n bop_logging -i 7
```

- -s および -a 変数を使用して、任意のアペンダ (**MaxFileSize** プロパティ) に対して作成するように、REST log4j プロパティ ファイルに設定されている各ログ ファイルの最大サイズを変更します。

たとえば、すべてのアペンダのファイルの最大サイズを **9 MB** に設定します。

```
pdm_log4j_config -f REST -a -s 9MB
```

- `-s` および `-n` 変数を使用して、特定のクラスまたは一連のクラス（`MaxFileSize` プロパティ）のアペンダに対して作成するように、**CA SDM log4j** プロパティ ファイルで設定されている各ログ ファイルの最大サイズを変更します。

たとえば、`bop_logging` のファイルの最大サイズを **7 MB** に設定します。

```
pdm_log4j_config -f SDM_WEB -n bop_logging -s 7MB
```

- `-t` および `-a` 変数を使用して、サポート オートメーション **log4j** プロパティ ファイル（しきい値プロパティ）に設定されているすべてのアペンダのログ レベルしきい値を変更します。

たとえば、ログ レベルしきい値を **DEBUG** に設定します。

```
pdm_log4j_config -f SA -a -t DEBUG
```

注: `-t` パラメータ ログ レベルしきい値は `-l` パラメータ ログ レベルをオーバーライドします。ログ レベルとしきい値レベルを変更すると、サーブレットからの **DEBUG** ログはファイルに表示されません。

- `-t` および `-n` 変数を使用して、**CA SDM log4j** プロパティ ファイルに設定されている特定のクラスまたは一連のクラス（しきい値プロパティ）のアペンダのログ レベルしきい値を変更します。

たとえば、ログ レベルしきい値を **WARN** に設定します。

```
pdm_log4j_config -f SDM_WEB -n bop_logging -t WARN
```

- 以下のコマンドを実行して、**REST log4j** プロパティ ファイルの現在のロガーとアペンダの設定を表示します。

```
pdm_log4j_config -f REST -d
```

重要: `-l`、`-i`、`-s`、および `-t` 変数は、`-a` または `-n` オプションのいずれかと共に使用し、両方のオプションは使用しないでください。`-f` オプションは必須です。`-h` および `-d` オプションは、他のオプションとは相互に排他的です。

ログ ファイル更新間隔の手動変更

管理者は、CA SDM が `log4j.properties` ファイルの変更をモニタする頻度を変更できます。デフォルトでは、更新間隔は 60 秒に設定されます。SDM サーブレット、PDM_RPC、サポート オートメーション、CMDB Visualizer、および REST などの CA SDM コンポーネントは、log4j を使用してログを記録します。

次の手順に従ってください:

1. CA SDM サーバで以下のディレクトリを開きます。

`NX_ROOT`

2. 編集のために `NX.env` ファイルを開きます。
3. `NX_LOG4J_REFRESH_INTERVAL` 変数をミリ秒単位の値で変更します。

注: 負の値または数値以外の値を入力すると、値はデフォルトの 60 秒になります。

4. `NX.env` ファイルを保存します。

jsrvr.log アペンドの変更

デフォルトでは、PDMContextListener、pdmweb、UploadServlet、および pdm_report などのサーブレットは、INFO レベルのメッセージのログを jsrvr.log ファイルに記録します。jsrvr.log アペンドのしきい値レベルを変更して、INFO レベルより下のすべてのメッセージをログに記録できます。

次の手順に従ってください:

1. log4j.properties ファイル内のレベルを以下のしきい値に変更します。

```
log4j.appender.jsrvrlog.Threshold=debug
```

2. UploadServlet のログ レベルを変更します。

```
log4j.logger.com.ca.ServicePlus.uploadservlet=debug, jsrvrlog
```

3. jsrvr.log ファイルを開きます。

4. UploadServlet の DEBUG ログ メッセージが表示されることを確認します。

注: しきい値レベルを変更せずにログ レベルを変更すると、サーブレットからの DEBUG ログはファイルに表示されません。すべてのサーブレットに明示的なロガーが接続されているわけではありません。たとえば、log4j.properties ファイルには、pdmweb サーブレットの一部である pdmweb、BOServlet、pdm_export、pdm_report、および pdm_cache が含まれます。これらのサーブレットの DEBUG ログを確認するには、pdmweb ログ レベルを変更します。

jstd.log アペンドの変更

nonwebapp アプリケーションのログはすべて、jstd.log ファイルに個別にダンプされます。pdm_rpc など、このようなアプリケーションのログは、そのアプリケーションのログ レベルを変更することで表示できます。

次の手順に従ってください:

1. 以下のログ レベルを変更します。

```
log4j.logger.com.ca.ServicePlus.pdm_rpc=debug
```

2. log4j.properties を開き、ログ エントリが表示されることを確認します。

pdm_proctor_init—セカンダリ サーバでの proctor の開始

UNIX のみに適用

pdm_proctor_init を使用すると、セカンダリ サーバで proctor を起動できます。プライマリ サーバからデーモンを起動する前に、すべてのセカンダリ サーバを起動する必要があります。プライマリ サーバですべてのデーモンを終了したら、セカンダリ サーバで pdm_halt を使用してこの proctor を終了します。

注: プライマリ サーバでは pdm_proctor_init を使用しないでください。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_proctor_init
```

pdm_replace—データベース テーブルの置換

pdm_replace を実行すると、CA SDM データベース内のテーブルを削除して、`-f` オプションで指定した一時ファイルのテーブルと置換できます。

pdm_replace を実行した後にテーブル内にあるデータは、入力ファイルのデータのみです。pdm_replace を実行する前にテーブルをバックアップしてください。

注: 処理の一環として、pdm_replace はまずデーモン (UNIX) またはサービス (Windows) を停止します。

pdm_replace では、テキストファイルを入力として受け入れます。このファイルのフォーマットは、pdm_userload で使用されるフォーマットと同じです。pdm_extract を使用して pdm_replace 用の入力ファイルを作成できますが、pdm_backup の出力を pdm_replace の入力として使用することはできません。

重要: 入力ファイルには、置換しようとしているテーブルとは異なる名前を付けてください。たとえば、`ca_contacts` というテーブルを置換しようとしていて、入力ファイルに `ca_contacts.dat` という名前を付けた場合、入力ファイル (`ca_contacts.dat`) を指すように pdm_replace コマンドを実行すると、入力ファイルとテーブルの名前が同じため、実行後に入力ファイルが削除されます。

制限

- pdm_replace は、CA SDM の設定に応じて、以下のサーバでのみ実行できます。
 - 標準：プライマリ サーバ
 - 高可用性：バックグラウンド サーバ

重要：バックグラウンドサーバでこのコマンドを実行する前に、すべてのアプリケーションサーバとスタンバイサーバを停止したことを確認します。
- pdm_replace は、特権ユーザまたはルート ユーザのみが実行できます。
- CA SDM にログインしているユーザがいる場合は、pdm_replace を実行しないでください。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_replace [-v] -f filename
```

-v

詳細モードを指定します。

-f filename

以下のフォーマットで ASCII ファイルを指定します。

```
TABLE table_name
fieldname1 fieldname2 . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

このフォーマットは、pdm_userload で使用されるファイルのフォーマットと同じです。pdm_extract を使用して pdm_replace 用の入力ファイルを作成できますが、pdm_backup の出力を pdm_replace の入力として使用することはできません。

関連項目:

[pdm_extract](#)—データベースからのデータの抽出 (P. 1304)

[pdm_userload](#)—データベース レコードの追加、更新、および削除 (P. 1340)

pdm_rest_util - CA SDM RESTful Web サービス アプリケーション の管理

CA SDM はこのユーティリティを自動的に使用します。予期しないエラーが発生した後などにこのユーティリティを実行する場合は、手動で実行できます。この REST Web サービス ユーティリティは、REST サービス Web アプリケーションを展開します。このユーティリティは、専用の REST Tomcat インスタンスに REST アプリケーションを展開します。NX_ROOT¥bin ディレクトリ（Windows の場合は pdm_rest_util.bat、UNIX の場合は ./pdm_rest_util.sh）内のバッチ ファイルを使用して、ユーティリティを起動できます。

このコマンドの形式とオプションは、以下のとおりです。

```
pdm_rest_util - h | [-deploy] | [-undeploy]
```

-h

コマンド ライン ヘルプを出力します。

-deploy

すべての Majic ファクトリを生成、コンパイル、および展開します。

-undeploy

ローカル サーバ上の REST Web サービスの展開を解除します。

REST Web サービス アプリケーションの展開解除

pdm_rest_util ユーティリティを使用して、REST Web サービス アプリケーションを展開解除できます。たとえば、CA SDM の保守を実行する場合、その間 REST を展開解除できます。

次の手順に従ってください:

1. コマンドプロンプトを開きます。
2. 以下のコマンドを実行します。

```
pdm_rest_util -undeploy
```

REST Web サービス アプリケーションが展開解除されます。

重要: このユーティリティを使用して REST アプリケーションを展開解除する場合、CA SDM の再起動時に REST が自動的に再展開する可能性があります。CA SDM の設定を使用して、REST を無期限に無効にすることを推奨します。

pdm_restore—データベースの復元

pdm_restore を実行すると、CA SDM を停止し、CA SDM データベースからすべてのレコードを削除して、-f オプションで指定したファイルのレコードと置換することができます。pdm_restore を実行した後に CA SDM データベースにあるデータは、入力ファイルのデータのみです。

入力ファイルは、pdm_extract または pdm_backup を使用して作成する必要があります。これらで作成しない場合は、pdm_restore 用にフォーマットされます。pdm_backup はデータベース以外のデータをバックアップでき、pdm_restore はこのデータも復元できます。利用可能なバックアップおよび復元ツールがほかにある場合は、pdm_backup および pdm_restore の使用はお勧めしません。

注: 処理の一環として、pdm_restore はまずデーモン (UNIX) またはサービス (Windows) を停止します。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_restore [-d] [-g] [-n] [-w] [-v] -f filename
```

制限

pdm_restore は、CA SDM サーバーでしか実行できません。pdm_restore は、特権ユーザまたはルート ユーザだけが実行できます。高可用性設定を使用している場合は、以下の制限が適用されます。

- データベースをリストアしている場合は、バックグラウンドサーバでのみ pdm_restore コマンドを実行します。
- pdm_restore コマンドを実行する前に、すべてのサーバ（アプリケーション、バックグラウンド、およびスタンバイ）を停止したことを確認します。

重要: pdm_restore を使用すると、現在のデータベースが削除され、バックアップファイルで置換されるので、pdm_restore は pdm_backup でデータベースのフル バックアップを作成している場合のみ使用してください。CA SDM にログインしているユーザがいる場合は、pdm_restore を実行しないでください。

-d

データベースのデータのみが復元されることを指定します。

-g

データベース以外のデータのみが復元されます。ウィンドウ（フォーム）と、その他のデータベース以外のデータのみが復元されます。

-n

データベース以外のデータが復元された場合に、NX.env も復元されることを指定します。初期設定では、NX.env は復元されません。バックアップの作成元のサーバと同じサーバに復元する場合を除き、NX.env ファイルは復元しないでください。不正な NX.env を復元すると、データベースに意図しない影響を与えることがあります。

-w

データベース以外のデータが復元された場合に、web.cfg が復元されることを指定します。初期設定では、web.cfg は復元されません。

-v

詳細モードを指定します。

-f filename

pdm_backup で作成したフルバックアップを含む入力ファイルを指定します。

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に LIBPATH を設定する必要があります。ユーティリティを実行する前に、pdm_task を使用して LIBPATH を設定します。たとえば、「pdm_task pdm_clean_attachments ...」と入力します。

関連項目:

[pdm_userload—データベース レコードの追加、更新、および削除](#) (P. 1340)

[pdm_backup—ASCII ファイルへのデータベースの書き込み](#) (P. 1293)

[データベースのリストア](#) (P. 606)

pdm_status—デーモンまたはプロセスのステータスの表示

pdm_status を実行すると、そのシステムのすべての CA SDM デーモン (UNIX) またはプロセス (Windows) のステータスを表示できます。

出力は、以下のフォーマットで表示されます。

DAEMON		STATUS	HOST	PID	SLUMP	CONNECT	TIME
Agent anthill		Running	anthill	455	Tue Feb 17	17:55:12	
Ddict_rd	(ddictrd)	Completed	anthill				
Data Dictionary	(ddictbuild)	Completed	anthill				
...							
User Validation	(boplgln)	Running	anthill	456	Tue Feb 17	17:55:21	

構文

このコマンドのフォーマットは、以下のとおりです。

pdm_status

pdm_task—環境変数の設定

UNIX のみに適用

pdm_task ユーティリティでは、ラップを持たないコマンドの環境変数を設定できます。たとえば、pdm_task コマンドが、同じコマンドラインの report コマンドより前に来る必要があるのは、コマンドがスクリプトまたはコマンドラインから起動した場合のみです。メニューから report コマンドを実行する場合は、すべての環境変数はアプリケーションによって設定されるので、pdm_task を含める必要はありません。

注: クライアントでは、コマンドラインからレポートを生成できません。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_task command
```

command

ラップを持たない、つまり環境変数が自動的に設定されないコマンドを指定します。コマンドを使用して pdm_task を実行する方法については、「[report--レポートの生成](#) (P. 1348)」を参照してください。

pdm_text_cmd—Text API コマンドライン インターフェース

Text API の pdm_text_cmd コマンドを使用します。このコマンドを使用すると、リクエスト、変更要求、案件、アセット、連絡先など、さまざまなオブジェクトを作成および更新できます。

重要: pdm_text_nxd または bop_cmd のコマンドのパラメータとして単一引用符や二重引用符は使用できません。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_text_cmd - t table {-u from_userid - p from_persid} [-o operation] [-f input file]
[-T timeout] [-h]
```

-t table

(必須) 処理するテーブルを指定します。 **table** には、以下のいずれかの値を指定します (大文字小文字は区別されません)。

- アセット
- 連絡先
- 変更
- 案件
- リクエスト

注: 有効なテーブル名の完全なリストについては、**text_api.cfg** ファイルの [OPTIONS] セクションを参照してください。

-u from_userid | -p from_persid

(どちらかのオプションが必須) この操作の連絡先を指定します。

-u from_userid

ユーザ ID 値を使用して連絡先を指定します。

-p from_persid

連絡先レコードのオブジェクト固有 ID をを使用して連絡先を指定します。 **from_persid** は、**cnt:xxxx** の形式で指定する必要があります。 **xxxx** はオブジェクトの固定 ID です。

注: このオプションで指定した値は、適切なキーワード **%FROM_USERID** または **%FROM_PERSID** を使用して、**pdm_text_cmd** コマンドの入力の最後に追加されます。

-o operation

実行する操作を指定します。*operation* には、以下のいずれかの値を指定します（大文字小文字は区別されません）。

- **NEW** : オブジェクトを作成します。この値は、操作を指定しない場合のデフォルトになります。
- **UPDATE | UPD** : 既存のオブジェクトが見つからない場合はオブジェクトを作成し、見つかった場合はそのオブジェクトを更新します。
- **UPDATE_ONLY | UPDO** : 見つかったオブジェクトを更新します。見つからなかった場合は、何もしません。

UPDATE も UPDATE_ONLY も、コマンド入力に **%SEARCH** キーワードが必要です。pdm_text_cmd の 1 回の呼出しで実行できる操作は 1 つだけです。

-f input_file

処理するテキスト ファイルの完全パスを指定します。このファイルには、有効な **Text API** のコマンドが含まれます。ユーザがこのパラメータを省略した場合は、STDIN から入力されたコマンドが使用されます。**Text API** への入力には、以下の基本フォーマットを使用します。

%keyword=value

入力内で複数のコマンドを実行するには、パーセント記号を 5 つ以上（%%%%%）使用してコマンドリクエストを区切ります。

注: 有効なキーワードの詳細と **Text API** の入力フォーマットの詳細については、text_api.cfg ファイルを参照してください。

-T timeout

サーバからの応答を待機してタイムアウトするまでの秒数を指定します。初期設定は 30 秒です。

注: `pdm_text_cmd` を実行すると、Text API から返されたテキストベースの応答が表示されます。この応答には、正常終了を示すメッセージまたはエラー メッセージと、API を使用して送信された処理用のテキストがそのまま含まれます。コマンドが正常に完了して警告やエラーが表示されなかった場合は 0、コマンドは正常に完了したが警告が表示された場合は 1 が返されます。その他の戻り値は、エラーが発生したことを示します。

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に `LIBPATH` を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して `LIBPATH` を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

注: コマンドプロンプトからパラメータを渡す場合は、`Ctrl + Z` キー (Windows)、または `Ctrl + D` キー (POSIX) を使用します。

関連項目:

[Text API の使用](#) (P. 647)

入力例

`pdm_text_cmd` は、Text API のコマンドライン インターフェースです。このコマンドを使用すると、リクエスト、変更要求、案件、アセット、連絡先など、さまざまなオブジェクトを作成および更新できます。

例: 入力ファイルを使って案件を作成する

以下の例は、`pdm_text_cmd` 入力ファイルを使って案件を作成する方法を示します。

```
%DESCRIPTION=This is my Test.  
%PRIORITY=3
```

このファイルを処理するには、完全パスが `c:\input.txt` の場合、以下のコマンドを実行します。

```
pdm_text_cmd -t Issue -u user01 -f c:\input.txt
```

例: 入力ファイルを使って案件を更新する

以下の例は、案件 123 を優先度 2 に更新するための入力ファイルを示しています。

```
%SEARCH=ISSUE_ID
%ISSUE_ID=123
%PRIORITY=2
```

このファイルを処理するには、完全パスが c:¥update.txt の場合、以下のコマンドを実行します。

```
pdm_text_cmd -t Issue -o UPDATE_ONLY -u user01 -f c:¥update.txt
```

例: 入力ファイルを使って複数のリクエストを作成する

以下の例は、1 つの入力ファイルで複数のリクエストを作成する方法を示しています。このコマンドは、テストシステムでテストデータを作成する場合に便利です。

```
%DESCRIPTION=This is Test 1.
%PRIORITY=3
%
%DESCRIPTION=This is Test 2.
%PRIORITY=2
%
%DESCRIPTION=This is Test 3.
%PRIORITY=None
```

このファイルを処理するには、完全パスが c:¥testdata.txt の場合、以下のコマンドを実行します。

```
pdm_text_cmd -t Request -u user01 -f c:¥testdata.txt
```

pdm_uconv--ローカルの文字セットから UTF-8 への変換

pdm_uconv ユーティリティは、以前のリリースの CA SDM からのデータ変換や、他の CA Technologies 製品との統合を支援します。このユーティリティの最も一般的な用途は、ローカルの文字セットから UTF-8 への変換、および UTF-8 からローカルの文字セットへの変換です。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_uconv -h [-V] [-s] [-v] [-l | --list-code  
| --default-code | -L] [--cannon] [-x] [--to-callback | -c] [--from-callback | -i]  
[--fallback | --no-fallback] [-b] [-f] [--t] [--add-signature] [--remove-signature]  
[-o] [file ...]
```

-h

ヘルプ メニューを開きます。

-V

プログラム バージョンを出力します。

-s

無人操作を使用し、メッセージを抑制します。

-v

ユーティリティの進捗情報を表示します。

-l

利用可能なすべてのエンコーディングをリストします。有効なオプションは以下のとおりです。

--list-code

指定されたエンコーディングのみをリストします。

--default-code

デフォルト エンコーディングのみをリストします。

-L

利用可能なすべての文字変換機能をリストします。

--cannon

cnvrtrs.txt(5) フォーマットでリストを出力します。

-x

文字変換中の進捗状況を実行します。

--to-callback *callback*

変換先のエンコーディングに対してコールバックを使用します。

-c

出力に含まれる無効な文字を省略します。

--from-callback *callback*

変換元のエンコーディングに対してコールバックを使用します。

-i

入力に含まれる無効なシーケンスを無視します。

--callback *callback*

両方のエンコーディングに対してコールバックを使用します。

-b

ブロック サイズを指定します。

デフォルト : 4096

--fallback

フォールバック マッピングを使用します。

--no-fallback

フォールバック マッピングを使用しません。

-f

変換元のエンコーディングを設定します。

-t

変換先のエンコーディングを設定します。

--add-signature

U+FEFF Unicode シグネチャ文字 (BOM) を追加します。

--remove-signature

U+FEFF Unicode シグネチャ文字 (BOM) を削除します。

-o

出力をファイルに書き込みます。

例:**ローカルの文字セットから UTF-8 へ**

```
pdm_uconv -t utf-8 inputfile.txt > outputfile.txt
```

特定の文字セット(iso-2022-jp)から UTF-8 へ

```
pdm_uconv -f iso-2022-jp -t utf-8 inputfile.txt > outputfile.txt
```

UTF-8 からローカルの文字セットへ

```
pdm_uconv -f utf-8 inputfile.txt > outputfile.txt
```

UTF-8 から特定の文字セットへ

```
pdm_uconv -f utf-8 -t iso-2022-jp inputfile.txt > outputfile.txt
```

pdm_uconv ユーティリティには、以下の有効なコールバックが用意されています。

- substitute
- skip
- stop
- escape
- escape-icu
- escape-java
- escape-c
- escape-xml
- escape-xml-hex
- escape-xml-dec
- escape-unicode

pdm_userload—データベース レコードの追加、更新、および削除

pdm_userload ユーティリティを実行すると、指定した入力ファイルを使用して CA SDM データベースを更新できます。

重要: pdm_userload を実行する場合は、必ず先にデータベースのバックアップを作成してください。

チケット (案件やリクエストなど) をアップロードするときは、必ずチケット番号の文字列に一意のプレフィックスまたはサフィックスを追加してください。CA SDM では、この番号はシーケンス番号ではなく文字列として表示されるので、アップロードされたチケットに一意の番号が割り当てられるとは限りません。awk などのテキストプロセッサを使用して一意のプレフィックスまたはサフィックスを割り当てると、前に割り当てられた番号を CA SDM で上書きすることなく、チケットをアップロードすることができます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_userload [-a] [-c] [-h] [-r] [-v] [-u] [-m] -f filename
```

入力ファイルのフォーマット

入力ファイルのエントリは、以下のフォーマットに従います。

```
TABLE table_name
fieldname1 fieldname2 . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

table_name は、ロードするテーブルの名前で、CA SDM データベーススキーマファイル \$NX_ROOT/site/schema.sch (UNIX) または *installation-directory*¥site¥schema.sch (Windows) にあります。\$NX_ROOT または *installation-directory* は、CA SDM をインストールしたディレクトリです。

-f filename

入力 ASCII ファイルを指定します。

-a

単一の入力レコードに一致する既存レコードが複数あるかどうかに関係なく、既存レコードがすべて更新されます。このオプションを使用しない場合は、複数の既存レコードに一致する入力レコードは拒否されます。

重要: このオプションの使用には注意が必要です。

-c

入力ファイルとデータベースを比較して、実行された更新について報告します。更新は行いません。

-r

入力レコードに一致するデータベース レコードを削除します。**-a** オプションは、**-r** オプションと一緒に使用することができます。

注: このオプションを使用して **pdm_userload** を実行する前に、データベースのバックアップ コピーを作成してください。古いデータベース レコードを削除した後、削除したレコードを復旧する場合は、このバックアップ コピーを使用して **CA SDM** データベースを復元します。

-v

詳細モードを指定します。

-u

既存のレコードを更新します。新しいレコードはデータベースに挿入されません。

-m

一括更新を行います。**pdm_userload** を使用して多数のレコードを追加または削除する場合に指定します。このオプションを指定すると、クライアントのすべての更新通知が無効になり、**pdm_userload** によるテーブルの処理が終了したときにテーブルのキャッシュ更新メッセージが送信されます。

-x

ロケールに応じた数値入力フォーマットを使用します。

-t

テナントの名前または UUID を指定して、指定したテナントとロードされたすべてのデータを関連付けます。この引数は、マルチテナンシーがインストールされている場合にのみ有効です。

Pdm_userload は、TABLE ステートメントの新しい引数である「Truncate」と「NoNewID」をサポートしています。これらの引数は、必要に応じてテーブル名の後ろにかっこで囲んで指定します。以下に例を示します。

TABLE Call_Req (TRUNCATE, NONEWID)

Truncate

データをロードする前に、テーブルに対してデータベース固有の TRUNCATE コマンドを発行します。さらに、コマンドライン引数に関係なく、すべてのレコードを新しいものとみなして挿入のみのロジックを使用するように pdm_userload のロジックを強制的に変更します。

NoNewID

挿入されたデータに対して新しい ID を生成する (pdm_userload -i オプションのデフォルトロジックの) 代わりに、テーブル内の新しい行に入力制御ファイルの ID 値を使用します。

制限

CA SDM がアクティブなときに pdm_userload を実行できますが、パフォーマンスが非常に低下する可能性があります。pdm_userload は、CA SDM にログインしているユーザがいないときに実行することをお勧めします。

関連項目:

[pdm_replace—データベース テーブルの置換](#) (P. 1327)

[pdm_backup—ASCII ファイルへのデータベースの書き込み](#) (P. 1293)

[pdm_restore—データベースの復元](#) (P. 1330)

pdm_webstat—Web 使用状況の統計の表示

pdm_webstat を実行すると、1 つ以上の Web エンジン プロセスについて、CA SDM のセッションおよびユーザの統計が返されます。累積セッション、1 回あたりの最大セッション、および現在アクティブなセッションが表示されます。また、個々のユーザに関する情報も表示されます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_webstat [-r] [-d | -D] [-i] [-t timeout] [-p webengine process] [-n] [-h]
```

-r

タイトルやその他のフォーマットがない **raw** テキスト モードを指定します。単一の **Web** エンジン プロセスの出力内には改行はありません。ただし、各 **Web** エンジン プロセスの出力は常に新しい行で始まります。

raw テキスト モードでは、**-r** オプションを使用せずに **pdm_webstat** を実行したときと同じ順序でデータが表示されます。生成されたデータをスプレッドシートまたはその他のタイプのレポートで使用する場合は、**raw** テキスト モードを使用します。たとえば、以下の構文を使用するとします。

```
pdm_webstat -r
```

この場合、以下の情報が出力されます。

```
2005/10/11 10:31:49 web:local:0 12 4 2
2005/10/11 10:31:49 web:local:1 9 2 2
```

-d

ユーザセッションが表示される詳細な出力を指定します。**-d** オプションでは、現在のすべてのセッションが *userid@IPaddress* の形式で表示されます。ユーザ ID のないセッションが表示された場合、通常はセッションがログインされていないことを意味します。たとえば、以下の構文を使用するとします。

```
pdm_webstat -d
```

この場合、以下の情報が出力されます。

```
PDM_Webstat: Invoked at 10/11/2005 10:27:31
```

```
=====
Report from Webengine: web:local:0
```

```
=====
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
    @192.168.1.16
    usery@192.168.1.20
```

```
=====
Report from Webengine: web:local:1
```

```
=====
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
    SrvcPlus@192.168.1.14
    userx@192.168.1.8
```

-D

デバッグ用に詳細な出力が表示されます。このオプションは、CA のテクニカルサポートから指示があった場合にのみ使用してください。各セッションの内部情報が詳細出力に追加されます。たとえば、以下の構文を使用するとします。

```
pdm_webstat -D
```

この場合、以下の情報が出力されます。

```
PDM_Webstat: Invoked at 10/11/2007 10:28:10
```

```
=====
Report from Webengine: web:local:0
=====
```

```
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
    @192.168.1.16          SessionStat  1
    userx@192.168.1.20     SessionStat  5
=====
```

```
Report from Webengine: web:local:1
=====
```

```
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
    SrvcPlus@192.168.1.14  SessionStat  7
    userx@192.168.1.8     SessionStat  13
=====
```

-i

連続するレポート間の間隔を秒単位で指定します。-i 引数を指定すると、pdm_webstat は継続的に実行されます。その他の引数によって要求されたフォーマットでレポートが出力され、指定された秒数待機した後、再度レポートが出力されます。-i を使用すると、pdm_webstat は明示的にキャンセル（通常は **Ctrl+C** キーを使用）した場合にのみ終了します。たとえば、以下の構文を使用するとします。

```
pdm_webstat -i 5 -p web:local -r
```

この場合、以下の情報が出力されます。

```
09/21/2007 16:27:25 web:local 14 10 6
09/21/2007 16:27:30 web:local 17 10 9
09/21/2007 16:27:35 web:local 18 10 10
09/21/2007 16:27:41 web:local 21 13 13
```

-t timeout

タイムアウト値を秒数で指定します。このパラメータにより、pdm_webstat は指定された秒数だけ応答を待機してから終了します。初期設定は 30 秒です。

-p webengine_process

レポートする Web エンジンのプロセス名を指定します。初期設定では、すべての Web エンジン プロセスがレポートされます。プロセス名（別名 Slump 名）は、slstat 出力で表示される名前と同じで、必ず「web:」で始まります。

-n

レポートされた各 Web エンジンの通常のログ エントリを表示しないようにします。初期設定では、各 Web エンジンの概要をまとめたログ エントリが作成されます。

注: 初期設定では、パラメータをまったく指定しないと、実行中のすべてのプロセスの概要データが pdm_webstat によって表示されます。

pdm_webstat では、コマンドが正常に完了すると 0 が返され、エラー（タイムアウトになった場合やアクティブな Web エンジン プロセスがなかった場合など）が発生すると 0 以外が返されます。

例: パラメータを指定しなかった場合の pdm_webstat の出力

以下の例は、パラメータを指定せずに pdm_webstat を実行した場合の出力を示しています。

```
PDM_Webstat: Invoked at 10/11/2007 10:26:42
```

```
=====
Report from Webengine: web:local:0
```

```
=====
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
```

```
=====
Report from Webengine: web:local:1
```

```
=====
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
```

重要: UNIX では、一部の CA SDM ユーティリティを実行する前に LIBPATH を設定する必要があります。ユーティリティを実行する前に、`pdm_task` を使用して LIBPATH を設定します。たとえば、「`pdm_task pdm_clean_attachments ...`」と入力します。

report—レポートの生成

UNIX のみに適用

レポート プログラムでは、サーバでコマンドラインからレポートを生成することができます。コマンドラインまたはスクリプトで `report` コマンドを実行するには、`pdm_task` を含める必要があります。`pdm_task` コマンドでは、ラップを持たないコマンドの環境変数を設定します。レポートをスクリプトまたはコマンドラインから呼び出した場合にのみ、同じコマンドラインで `report` コマンドを使用して `pdm_task` を入力します。メニューから `report` コマンドを実行する場合は、すべての環境変数はアプリケーションによって設定されるので、`pdm_task` を含める必要はありません。

構文

このコマンドのフォーマットは、以下のとおりです。

```
pdm_task report [-h] [-e] [-f] [-F ffstring] [-p pagelength] filename [ command line arguments]
```

-e

コンパイル済みのスクリプトをエコーします（デバッグ用）。

-f

ページ間に改ページを使用します。

-F ffstring

オプションの改ページ文字列を設定します。

-p pagelength

ページ長を設定します。ページ長の初期設定は 66 です。

filename

レポートテンプレート。**report** コマンドを、テンプレート ファイルが保存されているディレクトリから実行しない場合、ファイルの完全なパス名を指定します。コマンドでは、出力は標準の出力（**stdout**）として送信されます。

command line arguments

レポートテンプレートで受信するパラメータを指定します。レポートがコマンドライン引数を受け取るように設計されている場合は、レポートテンプレートのパラメータごとにコマンドライン引数を入力する必要があります。引数が空の場合は、**Null** 文字列を入力します。

たとえば、以下のコマンドでは、コマンドライン引数として **Smith**、**Jane**、および **L** が渡されます。影響を受ける連絡先のレポートを生成するには、レポートテンプレートにこの 3 つのパラメータが必要です。

たとえば、以下のように入力します。

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt
```

以下の例では、**Jane Smith** にはミドル ネームのイニシャルがありません。

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt Smith Jane "
```

rpt_srv—レポートの生成

Windows でのみ有効です。

レポートプログラムでは、サーバでコマンドラインからレポートを生成することができます。コマンドラインまたはスクリプトで **report** コマンドを実行するには、**pdm_task** を含める必要があります。**pdm_task** コマンドでは、ラップを持たないコマンドの環境変数を設定します。レポートをスクリプトまたはコマンドラインから呼び出した場合にのみ、同じコマンドラインで **report** コマンドを使用して **pdm_task** を入力します。メニューから **report** コマンドを実行する場合は、すべての環境変数はアプリケーションによって設定されるので、**pdm_task** を含める必要はありません。

構文

このコマンドのフォーマットは、以下のとおりです。

```
rpt_srv - m [-h] [-e] [-f] [-F ffstring] [-p pagelength] [-C] [-B] filename  
[ command line arguments]
```

-m

レポートが、コマンドラインから手動で実行されていることを示します。

-e

コンパイル済みのスクリプトをエコーします（デバッグ用）。

-f

ページ間に改ページを使用します。

-F *ffstring*

オプションの改ページ文字列を設定します。

-p *pagelength*

ページ長を設定します。 ページ長の初期設定は 66 です。

-C

エンコーディングを UTF-8 から他の文字セットに変更します。 デフォルト出力は UTF-8 です。

例：出力を JIS に変換するには、「-C iso-2022-jp」を実行します。

例：オペレーティングシステムのネイティブ文字セットにエンコードするには、「DEFAULT」または「NATIVE」を使用します。

-B-

変数 NX_ADD_UTF8_BYTE_ORDER_MARK が設定されている場合は、バイト順マークを抑制します。

NX_ADD_UTF8_BYTE_ORDER_MARK オプションは、ファイルに挿入されるシグネチャです。これによって、UTF-8 をサポートするエディタで、ファイルの UTF-8 の整合性が維持されるようになります。

注:これが必要になるのは、非 ASCII データの場合のみです。これがインストールされていない場合は、デフォルトの動作としてバイト順マーク (BOM) が省略されます。インストールされている場合は、「1」または「Yes」に設定します。

filename

レポートテンプレートを指定します。 **report** コマンドを、テンプレートファイルが保存されているディレクトリから実行しない場合、ファイルの完全なパス名を指定します。コマンドでは、出力は標準の出力 (stdout) として送信されます。

command line arguments

レポートテンプレートで受信するパラメータを指定します。レポートがコマンドライン引数を受け取るように設計されている場合は、レポートテンプレートのパラメータごとにコマンドライン引数を入力する必要があります。引数が空の場合は、Null 文字列を入力します。

たとえば、以下のコマンドでは、コマンドライン引数として **Smith**、**Jane**、および **L** が渡されます。影響を受ける連絡先のレポートを生成するには、レポートテンプレートにこの 3 つのパラメータが必要です。

たとえば、以下のコマンドを入力します。

```
rpt_srv - m c:%reports%affected.rpt Smith Jane L
```

以下の例では、**Jane Smith** にはミドルネームのイニシャルがありません。

```
rpt_srv - m c:%reports%affected.rpt Smith Jane "
```

uniconv--UNIX CA NSM Event Converter デーモンの起動

UNIX のみに適用

CA SDM が CA NSM と統合されている場合は、uniconv を使用して一般的なイベントデータを送信し、CA SDM でデーモンをフィルタできます。uniconv は CA NSM Event Management のメッセージアクションで使用されます。

構文

このコマンドのフォーマットは、以下のとおりです。

```
uniconv - h &opnode - e '&text' [-n &
nodeid] [-u &userid] [-d &datem] [-t &
time']
```

制限

uniconv は、UNIX の \$NX_ROOT/bin から実行する必要があります。このユーティリティを使用するには、サイトが CA NSM と統合されている必要があります。

-h &opnode

uniconv を実行しているマシンのノード名を指定します（必須）。

-e &'text'

メッセージのフルテキストを指定します（必須）。

-n &nodeid

メッセージの送信元のノード名を指定します（必須）。

-u &userid

メッセージを送信したユーザのログイン ID を指定します。

-d &datem

システムの日付を *yy/mm/dd* フォーマットで指定します。

-t &'time'

システムの時間を指定します。

pdm_mail ユーティリティ -- 電子メール情報の送信

pdm_mail ユーティリティは、電子メール情報を pdm_mail_nxd プロセスに送信することによって電子メールを送信するために、通知で使します。pdm_mail ユーティリティはコマンドにも使用できますが、両方には使用できません。パラメータを使用しない場合、NX_NTF_xxxx 変数を使用してパラメータを渡すデフォルトの動作は有効です。

電子メールの場合、ユーティリティは以下のように呼び出されます。

```
pdm_mail [-i [-s subject] [-e email_address] [-q]] [-p] [-M] [-F] [-T] [-B] [-H] [-N]
[-R] [-h]
```

-i

NTF 変数ではなく **STDIN** を使用します。以下のパラメータは、**STDIN** 電子メール動作のみに使用されます。

-e

(受信者の) 電子メールアドレスを指定します。

-s

電子メールの件名を指定します。

-q

STDIN の表示プロンプトを無効にします。

-p

ポケットベルのロジックを利用します。このオプションには、通常の電子メールアドレスではなくポケットベルの電子メールアドレスを使用することが含まれます。平文テキストバージョンの通知のみが使用されます (**HTML** はありません)。

-M

本文で (**MIME** ではなく) 平文テキストのみを使用します。

-F

電子メールの送信者アドレスを指定します。

-T

電子メールの返信先アドレスを指定します。

-B-

本文の文字セットを指定します。これは、**UTF-8** をサポートしていないポケットベルの場合に役立つことがあります。

-H

ヘッダの文字セットを指定します。これは、**UTF-8** をサポートしていないポケットベルの場合に役立つことがあります。

-N

DSN (Delivery Status Notification) の **Notify** オプションを指定します。

-R

DSN (Delivery Status Notification) の Return オプションを指定します。

-h

ユーティリティのヘルプを表示します。

コマンドの場合、ユーティリティは以下のように呼び出されます。

メールサーバへのコマンド

```
pdm_mail -c option [parameter]
```

Mail Eater へのコマンド

```
pdm_mail -x option [parameter]
```

check_interval

(-x のみ) メール チェック間隔を指定した値に変更します (秒単位)。

report_interval

レポート間隔を指定した値に変更します (秒単位)。

report_now

ログへのレポートを強制します。カウンタはリセットされません。

send_q

(-c のみ) ローカル メール キューをリモート メール サーバに送信します。

トレース

トレースのオン/オフを切り替えます。

重要: UNIX では、一部の **CA SDM** ユーティリティを実行する前に **LIBPATH** を設定する必要があります。ユーティリティを実行する前に、**pdm_task** を使用して **LIBPATH** を設定します。たとえば、「**pdm_task pdm_clean_attachments ...**」と入力します。

pdm_server_control ユーティリティ -- サーバの識別

pdm_server_utility コマンドは、高可用性設定でサーバをバックグラウンドまたはスタンバイとして識別します。

コマンドプロンプトから以下のコマンドを実行します。

```
pdm_server_control -h | -b | -q interval [-s server_name] | -t | -c [-server_name]
```

-h

ヘルプ ページを表示します。

-b

ローカルのスタンバイ サーバにバックグラウンドサーバになるよう通知します。スタンバイ サーバが動作している必要があります。サーバが動作していない場合、開始されますがフェールオーバーは実行されません。フェールオーバーを開始するには、コマンドを再度実行します。

-q interval [-s server_name]

ローカルまたはリモート アプリケーション サーバに指定された時間間隔内に休止するよう通知します。この間隔は、サーバがシャットダウンするまでの秒数です。 **server_name** を指定せずにこのオプションを使用すると、ローカルサーバに休止するよう通知されます。このオプションは、バックグラウンドまたはスタンバイ サーバには使用できません。

-t

この CA SDM 高可用性サーバのタイプを表示します。

-c [-s server_name]

以前の休止リクエストをキャンセルするようにローカルまたはリモート アプリケーション サーバに通知します。

付録 B: ビューのフィールドの説明

このセクションには、以下のトピックが含まれています。

[ビューのフィールドの説明](#) (P. 1358)

[View Act Log](#) (P. 1358)

[View Audit Assignee](#) (P. 1360)

[View Audit Group](#) (P. 1360)

[View Audit Priority](#) (P. 1361)

[View Audit Status](#) (P. 1362)

[View Change Act Log](#) (P. 1362)

[View Change](#) (P. 1364)

[View Change to Assets](#) (P. 1369)

[View Change to Change Act Log](#) (P. 1370)

[View Change to Change WF](#) (P. 1371)

[View Change to Properties](#) (P. 1374)

[View Contact Full](#) (P. 1375)

[View Contact to Environment](#) (P. 1378)

[View Group](#) (P. 1379)

[View Group to Contact](#) (P. 1380)

[View Issue](#) (P. 1380)

[View Issue Act Log](#) (P. 1385)

[View Issue to Assets](#) (P. 1387)

[View Issue to Issue Act Log](#) (P. 1387)

[View Change to Request](#) (P. 1389)

[View Issue to Issue WF](#) (P. 1392)

[View Issue to Properties](#) (P. 1395)

[View Request](#) (P. 1396)

[View Request to Act Log](#) (P. 1401)

[View Request to Properties](#) (P. 1402)

ビューのフィールドの説明

フィールドの説明は、CA SDM 付属の基本ビューおよび高度なビューで使用できます。

以下の事項は、多くのテーブルに適用されます。

- [詳細] ビューでデータを表示するには、[管理]-[オプション マネージャ] - [監査ログ] にある [監査ロギング] をオンにする必要があります。

注: 監査ロギングの詳細については、オンライン ヘルプを参照してください。

- pdmtime は、GMT 形式 (1970 年 1 月 1 日からの経過秒数) の [日付] / [時間] フィールドを示します。
- 変更要求および変更指示という用語は、同じ意味で使用されます。

関連項目:

[CA SDM でのレポートの生成](#) (P. 1047)

View_Act_Log

以下に、リクエスト アクティビティ ログ テーブルの基本ビューを示します。ビューには、アクティビティ タイプおよびアナリストのフル ネームも表示されます。アクティビティ ログ テーブル (act_log) は、アクティビティ タイプ テーブル (act_type) および連絡先テーブル (ca_contact) と結合され、各アクティビティ ログ エントリの実際のアクティビティ タイプと、アクティビティを実行したアナリストが表示されます。テーブルの結合から抽出されたフィールドの中で、役に立つ可能性のあるフィールドは、このリストの最後に配置されます。

フィールド	備考
id	act_log.id : act_log テーブルに含まれるこのレコードの固有 ID。
persid	act_log.persid : act_log テーブルに含まれるこのレコードの固有 ID。先頭にオブジェクト ID (act_log を意味する alg) とコロンが付きます。

フィールド	備考
call_req_id	act_log.call_req_id : このアクティビティが属するコール リクエスト固定 ID のポインタ。 act_log.call_req_id = call_req.persid。
last_mod_dt	act_log.last_mod_dt : 最終変更日時 (pdmtime)
time_spent	act_log.time_spent : このアクティビティに費やされた時間。総秒数で保存されます。たとえば、「80」は 1 分 20 秒のことです。
time_stamp	act_log.time_stamp : ユーザが変更可能なアクティビティの日時 (pdmtime)
system_time	act_log.system_time : レコードの作成日時 (pdmtime)
analyst	act_log.analyst : アクティビティを実行したアナリストを取得する連絡先 uuid への uuid ポインタ。 act_log.analyst = ca_contact.contact_uuid。
description	act_log.description : このアクティビティの説明テキスト。ユーザによる変更が可能です。
action_desc	act_log.action_desc: 自動化されたアクションの説明テキスト。ユーザによる変更はできません。
type	act_log.type : アクティビティ タイプ テーブル内のレコードへのテキスト ポインタ。例: act_log.type=act_type.code。
knowledge_session	act_log.knowledge_session : 特定ユーザの特定セッションの ID。
knowledge_tool	act_log.knowledge_tool : NLS_FAQ や EXPERT など、検索に使用するナレッジ ツールのインジケータ。
internal	act_log.internal: このログ エントリが全ユーザに表示可能か内部専用かを示す整数フラグ (1 または 0) 。
activity_type	act_type.symActivity : act_log.type = act_type.code から派生したタイプ。
analyst_lastname	View_Contact_Full.last_name : act_log.analyst = ca_contact.contact_uuid から派生したアナリストの姓。
analyst_firstname	View_Contact_Full.first_name : アナリストの名。
analyst_middlename	View_Contact_Full.middle_name : アナリストのミドルネーム。

View_Audit_Assignee

以下に、担当者をトラッキングする監査ログの高度なビューを示します。このビューには、リクエストおよび変更要求ごとに担当者が変更される時間間隔が表示されます。リクエストまたは変更要求が、特定の担当者から担当者なしに変更された後、担当者なしから特定の担当者に変更された場合、このビューのリストには担当者なしの時間間隔は表示されません。このビューには、リクエストおよび変更要求の両方に対して以下のフィールドが表示されます。1つの `audobj_uniqueid` (リクエストまたは変更要求) に対して複数のエントリが表示される場合があります。

フィールド	備考
<code>audobj_uniqueid</code>	<code>audit_log.audobj_uniqueid</code> : 監査ログのオブジェクト固有 ID (<code>chg.id</code> または <code>call_req.id</code> を表す)
<code>from_val</code>	<code>audit_log.attr_after_val</code> : 「変更前」の担当者の値。
<code>to_val</code>	<code>audit_log.attr_after_val</code> : 「変更後」の担当者の値。
<code>from_time</code>	<code>audit_log.attr_from_time</code> : 担当者の割り当てが開始された時間 (<code>pdmtime</code>) 。
<code>to_time</code>	<code>audit_log.attr_from_time</code> : 担当者の割り当てが終了した時間 (<code>pdmtime</code>) 。

View_Audit_Group

以下に、グループをトラッキングする監査ログの高度なビューを示します。このビューには、リクエストおよび変更要求ごとにグループが変更される時間間隔が表示されます。リクエストまたは変更要求が、特定のグループからグループなしに変更された後、グループなしから特定のグループに変更された場合、このビューのリストにはグループなしの時間間隔は表示されません。このビューには、リクエストおよび変更要求の両方に対して以下のフィールドが表示されます。1つの `audobj_uniqueid` (リクエストまたは変更要求) に対して複数のエントリが表示される場合があります。

フィールド	備考
<code>audobj_uniqueid</code>	<code>audit_log.audobj_uniqueid</code> : 監査ログのオブジェクト固有 ID (<code>chg.id</code> または <code>call_req.id</code> を表す)

フィールド	備考
from_val	audit_log.attr_after_val : 「変更前」のグループの値。
to_val	audit_log.attr_after_val : 「変更後」のグループの値。
from_time	audit_log.attr_from_time : グループの割り当てが開始された時間 (pdmtime) 。
to_time	audit_log.attr_from_time : グループの割り当てが終了した時間 (pdmtime) 。

View_Audit_Priority

以下に、優先度をトラッキングする監査ログの高度なビューを示します。このビューには、リクエストおよび変更要求ごとに優先度が変更される時間間隔が示されます。このビューには、リクエストおよび変更要求の両方に対して以下のフィールドが表示されます。1つの `audobj_uniqueid` (リクエストまたは変更要求) に対して複数のエントリが表示される場合があります。

フィールド	備考
audobj_uniqueid	audit_log.audobj_uniqueid : 監査ログのオブジェクト固有 ID (リクエストの <code>call_req.id</code> または変更要求の <code>chg.id</code> を表す)
from_val	audit_log.attr_after_val : 「変更前」の優先度の値。
to_val	audit_log.attr_after_val : 「変更後」の優先度の値。
from_time	audit_log.attr_from_time : 優先度の特定の状態が開始された時間 (pdmtime) 。
to_time	audit_log.attr_from_time : 優先度の同じ状態が終了した時間 (pdmtime) 。

View_Audit_Status

以下に、ステータスをトラッキングする監査ログの高度なビューを示します。このビューには、リクエストおよび変更要求ごとにステータスが変更される時間間隔が示されます。このビューには、リクエストおよび変更要求の両方に対して以下のフィールドが表示されます。1つの **audobj_uniqueid**（リクエストまたは変更要求）に対して複数のエントリが表示される場合があります。

フィールド	備考
audobj_uniqueid	audit_log.audobj_uniqueid : 監査ログのオブジェクト固有 ID（リクエストの call_req.id または変更要求の chg.id を表す）
from_val	audit_log.attr_after_val : 「変更前」の優先度の値。
to_val	audit_log.attr_after_val : 「変更後」の優先度の値。
from_time	audit_log.attr_after_time : ステータスの特定の状態が開始された時間（pdmtime）。
to_time	audit_log.attr_after_time : ステータスの同じ状態が終了した時間（pdmtime）。

View_Change_Act_Log

以下に、すべての変更要求アクティビティ ログの基本ビューを示します。これは、変更要求アクティビティ ログ テーブル（**chgalg**）に、アクティビティ タイプ テーブル（**act_type**）および連絡先 テーブル（**ca_contact**）が結合されたビューで、実際のアクティビティ タイプの説明や、アクティビティを実行したアナリストのフル ネームなど、よりわかりやすいデータが表示されます。

フィールド	備考
id	chgalg.id : chgalg テーブルのこのレコードの固有 ID。
persid	chgalg.persid : chgalg テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (chgalg を意味する chgalg) とコロンが付きます。

フィールド	備考
change_id	chgalg.change_id : このアクティビティが属する変更要求 ID へのポインタ。 chgalg.change_id = chgalg.id
last_mod_dt	chgalg.last_mod_dt : 最終変更日時 (pdmtime)
time_spent	chgalg.time_spent : このアクティビティに費やされた時間。総秒数で保存されます。たとえば、「80」は 1 分 20 秒のことです。
time_stamp	chgalg.time_stamp : ユーザが変更可能なアクティビティの日時 (pdmtime)。
system_time	chgalg.system_time : レコードの作成日時 (pdmtime)。
analyst	chgalg.analyst : アクティビティを実行したアナリストを取得する連絡先 uuid への uuid ポインタ。 chgalg.analyst = ca_contact.contact_uuid
description	chgalg.description : このアクティビティの説明テキスト。ユーザによる変更が可能です。
action_desc	chgalg.action_desc : 自動化されたアクションの説明テキスト。ユーザによる変更はできません。
type	chgalg.type : アクティビティ タイプ テーブル内のレコードへのテキスト ポインタ。 chgalg.type = act_type.code
internal	chgalg.internal : このログ エントリが全ユーザ表示可能か内部専用かを示す整数フラグ (1 または 0)
knowledge_session	chgalg.knowledge_session : 特定ユーザの特定セッションの ID。
knowledge_tool	chgalg.knowledge_tool : NLS_FAQ や EXPERT など、検索に使用するナレッジ ツールのインジケータ。
analyst_lastname	View_Contact_Full.last_name : chgalg.analyst = ca_contact.contact_uuid から派生したアナリストの姓。
analyst_firstname	View_Contact_Full.first_name : アナリストの名。
analyst_middlename	View_Contact_Full.middle_name : アナリストのミドルネーム。
activity_type	act_type.sym : chgalg.type = act_type.code により参照されるアクティビティ タイプ。

View_Change

以下に、すべての変更要求の基本ビューを示します。ステータス、優先度、カテゴリ、組織、影響を受けるエンドユーザのフルネーム、依頼者のフルネーム、担当者のフルネーム、グループ名、IDなどが表示されます。変更リクエストテーブル (chg) を、多数あるその他のテーブルと結合すると、変更要求に関してよりわかりやすいデータを表示することができます。

フィールド	備考
id	chg.id : chg テーブルのこのレコードの固有 ID。
persid	chg.persid : chg テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (テーブル chg を意味する chg) とコロンが付きます。
chg_ref_num	chg.chg_ref_num : アナリストおよびカスタマが特定の変更要求の参照に使用する変更要求参照番号。
description	chg.description : アナリストまたはカスタマが作成した変更要求の詳細な説明。
status	chg.status : chgstat テーブルへのポインタとなる、変更要求ステータスの固有 ID。 chg.status = chgstat.code。
active_flag	chg.active_flag : この変更レコードをアクティブにするかどうかを決定する整数フラグ (1 または 0)。
start_date	chg.start_date : 最初のタスクが保留中になる日付 (pdmtime)。
open_date	chg.open_date : 変更要求の作成日 (pdmtime)。
last_mod_dt	chg.last_mod_dt : 最終変更日 (pdmtime)。
last_mod_by	chg.last_mod_by : この変更要求を最後に変更した連絡先を示す連絡先 uuid へのポインタ。 chg.last_mod_by = ca_contact.contact_uuid。
close_date	chg.close_date : 変更要求が非アクティブに設定された日付 (pdmtime)。
resolve_date	chg.resolve_date : 変更案件が、変更が解決したことを示すステータスに設定された日付 (pdmtime)。

フィールド	備考
rootcause	chg.rootcause : rootcause テーブルのレコードへのポインタ。 この変更要求を実行する必要があった元の状況を表します。 chg.rootcause = rootcause.id。
est_total_time	chg.est_total_time : この変更の完了にかかる合計予定時間 (pdmtime) 。
actual_total_time	chg.actual_total_time : この変更の完了にかかった合計時間 (pdmtime) 。
log_agent	chg.log_agent : ca_contact テーブルを参照するバイナリ固有 ID。変更の最初の作成者を参照します。 chg.log_agent = ca_contact.contact_uuid。
assignee	chg.assignee : 変更要求に現在割り当てられている連絡先 uuid へのポインタ。 chg.assignee = ca_contact.contact_uuid。
organization	chg.organization : この変更要求が所属する組織を表す内部組織 uuid へのポインタ。 chg.organization = ca_organization.organization_uuid。
group_id	chg.group_id : 変更要求に現在割り当てられているグループを表す連絡先 uuid へのポインタ。 chg.group_id = ca_contact.contact_uuid
affected_contact	chg.affected_contact : この変更要求用の影響を受けた連絡先を表す連絡先 uuid へのポインタ。 chg.affected_contact = ca_contact.contact_uuid
requestor	chg.requestor : 変更を要求したユーザを表す連絡先 uuid へのポインタ。 chg.requestor = ca_contact.contact_uuid
category	chg.category : この変更が分類されるカテゴリを取得する変更カテゴリ コードへのポインタ。 chg.category = chgcat.code
priority	chg.priority : この変更が分類される優先度を表す優先列挙型値へのポインタ。 chg.priority = pri.enum
need_by	chg.need_by : affected_end_user が変更を完了する必要がある日付 (pdmtime) 。
est_comp_date	chg.est_comp_date : この変更要求の完了予定日 (pdmtime) 。

フィールド	備考
actual_comp_date	chg.actual_comp_date : この変更要求の完了日 (pdmtime) 。
est_cost	chg.est_cost : この変更要求の予定コスト。
actual_cost	chg.actual_cost : この変更要求の実装コスト。
justification	chg.justification : 依頼者用のテキストフィールド。この変更が必要な理由を文書化できます。
backout_plan	chg.backout_plan : アナリスト用のテキストフィールド。この変更の復旧計画を文書化できます。
impact	chg.impact : この変更が影響を与えるリソースの範囲を示す impact テーブルレコードへのポインタ。 chg.impact = impact.enum
parent	chg.parent : 変更要求の階層を作成できる別の変更要求 ID へのポインタ。 chg.parent = chg.id
effort	chg.effort : この変更要求を実装する計画について説明するテキストフィールド。
support_lev	chg.support_lev : service desc レコードへのポインタ。この案件を完了するときの制約を自動化できます。 chg.support_lev = srv_desc.code
template_name	chg.template_name : 変更要求テンプレートの名前およびポインタ。 chg.template_name = chg_template.template_name
sla_violation	chg.sla_violation : この「変更要求に添付された SLA に違反」した回数を表す整数。
predicted_sla_viol	chg.predicted_sla_viol : (r5.5) Neugent 関連テクノロジーのフィールド。
macro_predict_viol	chg.macro_predict_viol : (r5.5) Neugent 関連テクノロジーのフィールド。
created_via	chg.created_via : interface テーブルのレコードへのポインタ。変更要求の作成に使用されたインターフェースを示します。 chg.created_via = interface.id
call_back_date	chg.call_back_date : 依頼者に今後連絡する日時を示す日時フィールド (pdmtime) 。

フィールド	備考
call_back_flag	chg.call_back_flag : chg.call_back_date の日時にアナリストに通知するかどうかを示すブール値。ユーザにはチェック ボックスとして表示されます。
string1	ユーザ定義可能なテキスト フィールド。
string2	ユーザ定義可能なテキスト フィールド。
string3	ユーザ定義可能なテキスト フィールド。
string4	ユーザ定義可能なテキスト フィールド。
string5	ユーザ定義可能なテキスト フィールド。
string6	ユーザ定義可能なテキスト フィールド。
service_date	chg.service_date : 外部ベンダーがこの変更要求にサービスを提供する予定日時 (pdmtime)。
service_num	chg.service_num : 外部ベンダーへのサービスまたは発注書番号を文書化するテキスト フィールド。
product	chg.product : product テーブルへのレコードのポインタ。この変更の影響を受ける製品を示します。 chg.product = product.id
actions	chg.actions : アクションを文書化するための大きなテキスト フィールド。
type_of_contact	chg.type_of_contact : toc テーブルのレコードへのポインタ。案件に対する affected_end_user の一般的な分類を示します。 chg.type_of_contact = toc.id
reporting_method	chg.reporting_method。変更要求の作成元を分類する repmeth テーブルのレコードへのポインタ。変更要求を作成するユーザにより選択されます。 chg.reporting_method = repmeth.id
person_contacting	chg.person_contacting : perscon テーブルのレコードへのポインタ。affected_end_user または依頼者の役割を示します。 chg.person_contacting = perscon.id
status_name	chgstat.sym : ユーザに表示されるステータスの説明。 chg.status = chgstat.code
priority_num	pri.sym : ユーザに表示される優先度の説明。 chg.priority = pri.enum

フィールド	備考
category_name	chgcat.sym : ユーザに表示される変更カテゴリ名。 chg.category = chgcat.code
organization_name	ca_organization.org_name : ユーザに表示される組織名。 chg.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name : 影響を受けるエンドユーザの姓。 chg.affected_end_user = ca_contact.contact_uuid
affected_end_user_firstname	ca_contact.first_name : 影響を受けるエンドユーザの名。 chg.affected_end_user = ca_contact.contact_uuid
affected_end_user_middlename	ca_contact.middle_name : 影響を受けるエンドユーザのミドルネーム。 chg.affected_end_user = ca_contact.contact_uuid
requester_lastname	ca_contact.last_name : 依頼者の姓。 chg.requestor = ca_contact.contact_uuid
requester_firstname	ca_contact.first_name : 依頼者の名。 chg.requestor = ca_contact.contact_uuid
requester_middlename	ca_contact.middle_name : 依頼者のミドルネーム。 chg.requestor = ca_contact.contact_uuid
business	ca_organization.org_name : ユーザに表示される依頼者の組織の名前。 chg.requestor = ca_organization.organization_uuid
assignee_lastname	ca_contact.last_name : 担当者の姓。 chg.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name : 担当者の名。 chg.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name : 担当者のミドルネーム。 chg.assignee = ca_contact.contact_uuid
groupID	ca_contact.contact_uuid : この変更要求に割り当てられたグループで使用される内部 ID のバイナリ表示。 chg.group_id = ca_contact.contact_uuid
group_name	ca_contact.last_name : この変更要求に割り当てられたグループの名前。 chg.group = ca_contact.contact_uuid

フィールド	備考
service_type	srv_desc.sym : この変更要求に割り当てられたサービス タイプの 名前。 chg.support_lev = srv_desc.code
impact_num	impact.sym : ユーザに表示される影響度の説明。 chg.impact = impact.enum
product_sym	product.sym : ユーザに表示される製品の説明。 chg.product = product.id
type_of_contact_sym	toc.sym : ユーザに表示される連絡先タイプの説明。 chg.type_of_contact = toc.id
rpting_method_sym	repmeth.sym : ユーザに表示されるレポート方法の説明。 chg.reporting_method = repmeth.id
person_contacting_sym	perscon.sym : ユーザに表示される連絡先担当者の説明。 chg.person_contacting = perscon.id

View_Change_to_Assets

以下のフィールドのリストに、変更要求およびそのアセットの基本ビューを示します。変更要求テーブル (chg) は、ネットワーク リソース テーブル (ca_owned_resource) と間接的に結合されており、各変更要求のアセット リストを取得することができます。このビューでは、アセットが割り当てられてない変更要求は、表示されない場合があります。

フィールド	備考
View_Change.*	前述の View_Change ビューに表示されるすべてのフィールド
assetID	ca_owned_resource.own_resource_uuid : アセット レコードの不変かつ内部で固有の ID として機能するバイナリ フィールド。
asset_serial_num	ca_owned_resource.serial_number : アセット レコードのシリアル番号。
asset_class	ca_resource_class.name : アセットが所属するクラスの簡単な説明。 ca_owned_resource.resource_class = ca_resource_class.id

フィールド	備考
asset_family	ca_resource_family.name: このアセットが所属するアセット ファミ リ。 ca_owned_resource.resource_class = ca_resource_class.id AND ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name : このアセットを識別するネッ トワーク名。

View_Change_to_Change_Act_Log

以下に、すべての変更要求およびそのアクティビティ ログの基本ビューを示します。このビューにより、**View_Change** ビューと変更要求アクティビティ ログ (chgalg) が結合され、変更要求およびそのアクティビティ ログに関する詳細な情報を表示できます。

フィールド	備考
View_Change.*	前述の View_Change ビューに表示されるすべてのフィールドを表示します。
chgalg_id	chgalg.id : chgalg テーブルのこのレコードの固有 ID。
chgalg_persid	chgalg.persid : chgalg テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (chgalg を意味する chgalg) とコロンが付きます。
change_id	chgalg.change_id : このアクティビティが属する要求 ID を変更するポインタ。 chgalg.change_id = chgalg.id
chgalg_last_mod_dt	chgalg.last_mod_dt : 最終変更日時 (pdmtime)
time_spent	chgalg.time_spent : このアクティビティに費やされた時間。総秒数で保存されます。たとえば、「80」は 1 分 20 秒のことです。
time_stamp	chgalg.time_stamp : ユーザが変更可能なアクティビティの日時 (pdmtime) 。
system_time	chgalg.system_time : レコードの作成日時 (pdmtime) 。

フィールド	備考
analyst	chgalg.analyst : アクティビティを実行したアナリストを取得する連絡先 uuid への uuid ポインタ。 chgalg.analyst = ca_contact.contact_uuid
chgalg_description	chgalg.description : このアクティビティの説明テキスト。ユーザによる変更が可能です。
action_desc	chgalg.action_desc : 自動化されたアクションの説明テキスト。ユーザによる変更はできません。
type	chgalg.type : アクティビティ タイプ テーブル内のレコードへのテキスト ポインタ。 chgalg.type = act_type.code
internal	chgalg.internal : このログ エントリが全ユーザ表示可能か内部専用かを示す整数フラグ (1 または 0)
knowledge_session	chgalg.knowledge_session : 特定ユーザの特定セッションの ID。
knowledge_tool	chgalg.knowledge_tool : NLS_FAQ や EXPERT など、検索に使用するナレッジ ツールのインジケータ。
chgalg_analyst_id	chgalg.analyst : アクティビティを実行したアナリストを取得する連絡先 uuid への uuid ポインタ。 chgalg.analyst = ca_contact.contact_uuid

View_Change_to_Change_WF

このビューは、View_Change ビューがワークフロー タスク テーブル (wf) に結合された結果です。変更要求およびそのワークフロー タスクの基本ビューが表示されます。ワークフロー タスクが割り当てられていない変更要求は、表示されない場合があります。

フィールド	備考
View_Change.*	前述の View_Change ビューに表示されるすべてのフィールドを表示します。
wf_id	wf.id : wf テーブルのレコードの固有 ID。
wf_persid	wf.persid : wf テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (wf を意味する wf) とコロンが付きます。

フィールド	備考
del	wf.del : これはブール値です。このレコードをユーザに表示されるかどうかを示します。
object_type	wf.object_type : このワークフロー タスクが添付されたレコード タイプ (chg など) の識別に使用するファクトリ名。
object_id	wf.object_id : このワークフロー タスクが添付されたレコードの識別に使用される固有 ID。 wf.object_id = chg.id
task	wf.task : このレコードが表すタスク タイプを参照する ID。 wf.task = tskty.code
wf_template	wf.wf_template : このワークフロー タスク レコードが作成されたテンプレートを参照する ID。 wf.wf_template = wftpl.id
sequence	wf.sequence : このワークフロー タスク レコードを CA SDM で表示および実行する順序 (昇順) を示す整数。
wf_status	wf.status : このワークフロー タスクの現在のステータスを示す tskstat レコードを参照する ID。 wf.status = tskstat.code
group_task	wf.group_task : このタスクがグループに属するかどうかを示すブール値
asset	wf.asset : ca_owned_resource テーブルのレコードを参照する UUID (バイナリ) ID wf.asset = ca_owned_resource.own_resource_uuid
creator	wf.creator : ca_contact テーブルのレコードを参照する UUID (バイナリ) ID このワークフロー タスクの作成者を示します。 wf.creator = ca_contact.contact_uuid
date_created	wf.date_created : このワークフロー タスクの作成日/タイムスタンプ (pdmtime)
wf_assignee	wf.assignee : ca_contact テーブルのレコードを参照する UUID (バイナリ) ID このワークフロー タスクに現在割り当てられている担当者を示します。 wf.assignee = ca_contact.contact_uuid

フィールド	備考
done_by	wf.done_by : ca_contact テーブルのレコードを参照する UUID (バイナリ) ID このワークフロー タスクを完了または承認した実行者を示します。 wf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date : ワークフロー タスクがアクティブなステータスに変わった開始日を示すタイムスタンプ (pdmtime)。
wf_est_comp_date	wf.est_comp_date: このタスクの完了予定日を示すタイムスタンプ (pdmtime)
est_duration	wf.est_duration : このワークフロー タスクの予定期間
completion_date	wf.completion_dat : このワークフロー タスクの完了日を示すタイムスタンプ (pdmtime)
actual_duration	wf.actual_duration : このワークフロー タスクの完了にかかった期間
wf_est_cost	wf.est_cost : このワークフロー タスクの予定コスト
cost	wf.cost : このワークフロー タスクの完了にかかったコスト
wf_description	wf.description : ワークフロー タスクの説明
wf_last_mod_dt	wf.last_mod_dt: このワークフロー タスクの最終変更日を示すタイムスタンプ (pdmtime)
wf_last_mod_by	wf.last_mod_by : 連絡先テーブルのレコードを参照する UUID (バイナリ) 固有の ID。このワークフロー タスクに対して変更を行った最後のユーザを示します。 wf.last_mod_by = ca_contact.contact_uuid

View_Change_to_Properties

このビューは、View_Change ビューがプロパティ テーブル (prp) に結合された結果です。変更要求および割り当てられたプロパティの基本ビューが表示されます。プロパティが割り当てられてない変更要求は、表示されない場合があります。

フィールド	備考
View_Change.*	前述の View_Change ビューに表示されるすべてのフィールドを表示します。
prp_id	prp.id : プロパティ レコードの固有 ID (整数)
prp_persid	prp.persid : wf テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (prp を意味する prp) とコロンが付きます。
object_type	prp.object_type : このプロパティ レコードが添付されたレコードタイプ (chg など) の識別に使用するファクトリ名
object_id	prp.object_id : このプロパティが添付されたレコードの識別に使用する固有 ID prp.object_id = chg.id
sequence	prp.sequence : このプロパティ レコードを CA SDM で表示する順序 (昇順) を示す整数
property	prp.property : prptpl テーブルのレコードを参照する ID このプロパティが作成されたテンプレートを表します。 prp.property=prptpl.code
value	prp.value : prp_description フィールドおよび prp.label フィールドに応じてユーザが入力した値
prp_last_mod_dt	prp.last_mod_dt : このプロパティの最終変更日を示すタイムスタンプ (pdmtime)
prp_last_mod_by	prp.last_mod_by: ca_contact テーブルのレコードを参照するバイナリ ID このレコードの最終変更者を示します。 prp.last_mod_by = ca_contact.contact_uuid
required	prp.required : レコードを保存する前にこのプロパティに prp.value を指定する必要があるかどうかを示すブール値
sample	prp.sample : example 値が表示されるテキスト フィールド。このフィールドにより、ユーザは最も有効な値を prp.value に入力することができます。

フィールド	備考
prp_description	prp.description : prp.value に入力する値の種類を説明するテキストフィールド
label	prp.label : prp.value フィールドに表示する簡単な説明

View_Contact_Full

以下のフィールドに、すべての連絡先の基本ビューを示します。このビューには、ca_contact テーブルのすべてのフィールドが表示されます。また、各連絡先の連絡先タイプの簡単な説明、ロケーション名、組織名、サービスタイプなど、参照されるフィールドも表示されます。このビューは、すでに ca_location、ca_organization、srv_desc、および ca_contact_type の各テーブルに結合されており、ca_contact テーブルの一部のフィールドの実際の名前およびシンボルを取得することができます。実際の名前およびシンボルは、ビューのフィールドリストの最後に配置されます。

フィールド	Remark
contact_uuid	ca_contact.contact_uuid : 各 ca_contact レコードのバイナリ固有 ID
middle_name	ca_contact.middle_name : この連絡先のミドルネーム
alias	ca_contact.alias : この連絡先の別名（多くの場合、略式名）
last_name	ca_contact.last_name : この連絡先の姓
first_name	ca_contact.first_name : この連絡先の正式な名
pri_phone_number	ca_contact.pri_phone_number : 連絡先の主要な電話番号
alt_phone_number	ca_contact.alt_phone_number : 連絡先のその他の電話番号
fax_number	ca_contact.fax_number : 連絡先のファックス番号
mobile_phone	ca_contact.mobile_phone : 連絡先の携帯電話番号
pager_number	ca_contact.pager_number : 連絡先のポケットベル番号
email_address	ca_contact.email_address : 連絡先の電子メールアドレス

フィールド	Remark
location_uuid	ca_contact.location_uuid : ca_location テーブルのレコードを参照する固有 ID (バイナリ)。連絡先の静的ロケーションを示します。 ca_contact.location_uuid = ca_location.location_uuid
floor_location	ca_contact.floor_location : 連絡先のフロア番号
pager_email_address	ca_contact.pager_email_address : 連絡先のポケットベルの電子メールアドレス
room_location	ca_contact.room_location : 連絡先の静的ロケーションの特定ルーム
contact_type	ca_contact.contact_type : ca_contact_type テーブルの行を参照する固有 ID (整数)。サービス デスク アプリケーション内のこの連絡先の一般的な機能を示します。 ca_contact.contact_type = ca_contact_type.id
inactive	ca_contact.inactive : このレコードの状態を示すブール値。サービス デスク内の標準検索にレコードを含めるか除外するかを指定します。
creation_user	ca_contact.creation_user : このレコードを作成したユーザの ID ca_contact.creation_user = ca_contact.userid
creation_date	ca_contact.creation_date : この連絡先の作成日時を示すタイムスタンプ (pdmtime)
last_update_user	ca_contact.last_update_user : この連絡先レコードを最後に更新した連絡先のユーザ ID ca_contact.last_update_user = ca_contact.userid
last_update_date	ca_contact.last_update_date : このレコードの最終変更日時を示すタイムスタンプ (pdmtime)
version_number	ca_contact.version number : 内部バージョン インジケータ
department	ca_resource_department : テーブルの行を参照する固有 ID (整数)。連絡先の部門を示します。 ca_contact.department = ca_resource_department.id
comment	ca_contact.comment : アナリスト用の自由形式のテキスト コメント フィールド。特定の連絡先の処理に影響を及ぼす重要事項を文書化することができます。

フィールド	Remark
company_uuid	ca_contact.company_uuid : ca_company テーブルの行を参照する固有 ID (バイナリ)。この連絡先が所属する会社を示します。 ca_contact.company_uuid = ca_company.company_uuid
organization_uuid	ca_contact.organizaiton_uuid : ca_organization テーブルの行を参照する固有 ID (バイナリ)。この連絡先の管理組織を示します。 ca_contact.organizaiton_uuid = ca_organization.organization_uuid
admin_organization_uuid	ca_contact.admin_organization_uuid : ca_organization テーブルの行を参照する固有 ID (バイナリ)。この連絡先の管理組織を示します。 ca_contact.admin_organization_uuid = ca_organization.organization_uuid
alternate_identifier	ca_contact.alternate_identifier : ユーザ定義 ID。通常はこの連絡先を一意に特定するためにユーザが使用するエンティティ。
job_title	ca_contact.job_title : ca_job_title テーブルを参照する固有 ID (整数)。この連絡先の標準化されたジョブタイトルを示します。 ca_contact.job_title = ca_job_title.id
job_function	ca_contact.job_function : ca_job_function テーブルを参照する固有 ID (整数)。連絡先のジョブ関数の標準化された一般的な説明を示します。 ca_contact.job_function = ca_job_function.id
mail_stop	ca_contact.mail_stop : メールの停止
cost_center	ca_contact.cost_center : ca_resource_cost_center テーブルを参照する固有 ID (整数)。連絡先の主要コストセンターを示します。 ca_contact.cost_center = ca_cost_center.id
userid	ca_contact.userid : この連絡先がサービスデスクへのログインに使用するユーザ ID
supervisor_contact_uuid	ca_contact.supervisor_contact_uuid : ca_contact テーブルの行を参照する固有 ID (バイナリ)。連絡先の階層が作成され、各連絡先のレポート構造が示されます。 ca_contact.supervisor_contact_uuid = ca_contact.contact_uuid

フィールド	Remark
exclude_registration	ca_contact.exclude_registration : 内部フラグ
delete_time	ca_contact.delete_time : 非アクティブ フラグが 1 に設定された日時を示すタイムスタンプ
contact_type_name	ca_contact_type.name : この連絡先の ca_contact.contact_type の簡単な説明
location_name	ca_location.name : この連絡先の静的ロケーションの簡単な説明
organization	ca_organization.org_name : この連絡先の ca_contact.organizaiton_uuid の簡単な説明
admin_organization	ca_organization.org_name : この連絡先の組織名の簡単な説明 ca_contact.admin_organization_uuid
service_type	srv_desc.sym : この連絡先の usp_contact.c_service_type の簡単な説明 ca_contact.contact_uuid = usp_contact.contact_uuid AND usp_contact.c_service_type = srv_desc.code
state_sym	ca_location.state : ca_state_provice テーブルの行を参照する固有 ID (整数)。都道府県など、人為的に定義された地理的な領域を示します。 ca_contact.location_uuid = ca_location.location_uuid AND ca_location.state = ca_state_province.id

View_Contact_to_Environment

以下のフィールドのリストに、連絡先およびその環境（アセット）の基本ビューを示します。このビューは連絡先テーブル（ca_contact）のビューですが、所有リソーステーブル（ca_owned_resource）にも結合されており、連絡先に関連付けられたすべてのアセットのリストを取得することができます。このビューを View_Contact_Full ビューと結合すると、各連絡先の連絡先タイプ、サービスタイプ、組織、およびロケーションを取得することができます。または、このビューを個々のテーブルと結合して、同じ情報を取得することもできます。

フィールド	備考
ca_contact.*	View_Contact_Full ビュー定義の中で定義される ca_contact フィールド

フィールド	備考
asset_uuid	ca_owned_resource.own_resource_uuid : ca_owned_resource テーブルのアセットを参照する固有 ID (バイナリ)
asset_name	ca_owned_resource.resource_name : このアセットの指定されたネットワーク名

View_Group

以下のフィールドのリストに、連絡先テーブルの基本ビューを示します。表示されるのは、グループの連絡先のみです。連絡先タイプ ID = 2308 は、グループタイプを示します。このビューを **CA SDM** のほかのテーブルと結合すると、よりわかりやすいデータをレポート用に取得することができます。たとえば、ロケーション (ca_location) テーブルと結合すると、グループのロケーションの名前および住所を見つけることができます。また、組織 (ca_organization) テーブルと結合すると、グループの機能組織名および管理組織名を取得することができます。

フィールド	備考
ca_contact.*	View_Group_Full ビュー定義の中で定義される ca_contact フィールド

以下の例に、テーブルの結合による作用と、レポートフィールドの抽出方法の例について説明します。1 つのテーブルのフィールド (右側) は、別のテーブルのフィールド (左側) に結合 (->) されます。テーブルとビューを適切に結合するには、データベースの結合における違いを理解する必要があります。以前のテーブルが **View_Group view** と結合されている場合は、以下のように定義されたフィールド (括弧内) をレポートに使用してください。

- View_Group.contact_type -> ca_contact_type.id (ca_contact_type.sym)
- View_Group.location_uuid -> ca_location.location_uuid (ca_location.location_name)
- View_Group.organization_uuid -> ca_organization.organization_uuid (ca_organization.org_name)
- View_Group.admin_organization_uuid -> ca_organization(2).organization_uuid (ca_organization(2). org_name)

View_Group_to_Contact

以下のフィールドのリストに、すべてのグループの連絡先（メンバー）の基本ビューを示します。これには、マネージャも含まれます。ここで、**View_Group** は **Group_Member** テーブルと結合された後、**ca_contact** テーブルと結合されています。**View_Group** のすべてのフィールドと、**ca_contact** テーブルにある姓名およびミドルネームが表示されます。**Group_Member** マネージャフラグも表示されます。グループメンバーのマネージャフラグは **1** または **0** で、メンバーはマネージャである（**yes = 1**）かマネージャでない（**no = 0**）かのどちらかになります。このビューに表示される情報のほとんどは、実際のメンバーではなくグループ自体に関するものです。このビューを使用すると、メンバー名など、特定のグループに関する情報を見つけることができます。

フィールド	備考
View_Group.*	View_Group 定義の中で定義される View_Group フィールド
member_lastname	ca_contact.last_name : グループメンバーの姓。
member_firstname	ca_contact.first_name : グループメンバーの正式な名。
member_middlename	ca_contact.middle_name : グループメンバーのミドルネーム。
grpmem_manager_flag	ca_contact.manager_flag : グループメンバー マネージャ（1 または 0）インジケータ。

View_Issue

以下に、すべての案件の基本ビューを示します。ステータス、優先度、カテゴリ、組織、依頼者のフルネーム、担当者のフルネーム、グループ名、ID などが表示されます。案件テーブル（**issue**）をその他の多くのテーブルと結合すると、案件に関してよりわかりやすいデータを表示できます。

フィールド	備考
id	issue.id : 案件テーブルに含まれるこのレコードの一意の識別子。
persid	issue.persid : 案件テーブルに含まれるこのレコードの一意の識別子。先頭にオブジェクト識別子（案件テーブルを意味する iss ）とコロンが付きます。

フィールド	備考
issue_ref_num	issue.iss_ref_num: アナリストおよび顧客が特定の案件の参照に使用する案件参照番号。
description	issue.description: アナリストまたは顧客が作成した案件の詳細な説明。
status	issue.status: issstat テーブルへのポインタとなる、案件ステータスの一意の識別子。 issue.status = issstat.code
active_flag	issue.active_flag: この案件をアクティブにするかどうかを決定する整数フラグ (1 または 0)。
start_date	issue.start_date: 最初のタスクが保留中になる日付 (pdmtime)。
open_date	issue.open_date: 案件の作成日 (pdmtime)。
last_mod_dt	issue.last_mod_dt: 最終変更日 (pdmtime)。
last_mod_by	issue.last_mod_by: この案件を最後に変更した連絡先を示す連絡先 uuid へのポインタ。 issue.last_mod_by = ca_contact.contact_uuid
close_date	issue.close_date: 案件が非アクティブに設定された日付 (pdmtime)。
resolve_date	issue.resolve_date: 案件のステータスが、案件が解決したことを示すステータスに設定された日付 (pdmtime)。
rootcause	issue.rootcause: rootcause テーブルへのレコードへのポインタ。この案件をログに記録する必要があった元の状況を表します。 issue.rootcause = rootcause.id
est_total_time	issue.est_total_time: この案件の完了にかかる合計予定時間 (pdmtime)。
actual_total_time	issue.actual_total_time actual: この案件の完了にかかった合計時間 (pdmtime)。
log_agent	issue.log_agent: ca_contact テーブルを参照する一意の識別子 (バイナリ)。案件の最初の作成者を参照します。 issue.log_agent = ca_contact.contact_uuid
assignee	issue.assignee: 変更要求に現在割り当てられている連絡先 uuid へのポインタ。 issue.assignee = ca_contact.contact_uuid

フィールド	備考
organization	issue.organization : この案件が所属する組織を表す内部組織 uuid へのポインタ。 issue.organization = ca_organization.organization_uuid
group_id	issue.group_id : 案件に現在割り当てられているグループを表す連絡先 uuid へのポインタ。 issue.group_id = ca_contact.contact_uuid
affected_contact	issue.affected_contact : この案件の影響を受けた連絡先を表す連絡先 uuid へのポインタ。 issue.affected_contact = ca_contact.contact_uuid
requestor	issue.requestor : この案件のログ記録を要求したユーザを表す連絡先 uuid へのポインタ。 issue.requestor = ca_contact.contact_uuid
category	issue.category : この案件が分類されるカテゴリを参照する案件カテゴリ コードへのポインタ。 issue.category = isscat.code
priority	issue.priority : この案件が分類される優先度を表す優先列举型値へのポインタ。 issue.priority = pri.enum
need_by	issue.need_by : affected_end_user が案件を完了する必要がある日付 (pdmtime) 。
est_comp_date	issue.est_comp_date : この案件の完了予定日 (pdmtime) 。
actual_comp_date	issue.actual_comp_date : この案件の完了日 (pdmtime) 。
est_cost	issue.est_cost : この案件の予定コスト。
actual_cost	issue.actual_cost : この案件の実装コスト。
justification	issue.justification : 依頼者用のテキスト フィールド。この案件が必要な理由を文書化できます。
backout_plan	issue.backout_plan : アナリスト用のテキスト フィールド。この案件の復旧計画を文書化できます。
impact	issue.impact : この案件が影響を与えるリソースの範囲を示す impact テーブル レコードへのポインタ。 issue.impact = impact.enum
parent	issue.parent : 案件の階層を作成できる別の案件 ID へのポインタ。 issue.parent = issue.id

フィールド	備考
effort	issue.effort : この案件を実装する計画について説明するテキストフィールド。
support_lev	issue.support_lev : service desc レコードへのポインタ。この案件を完了するときの制約を自動化できます。 issue.support_lev = srv_desc.code
template_name	issue.template_name : 案件テンプレートの名前および案件テンプレートへのポインタ。 issue.template_name = iss_template.template_name
sla_violation	issue.sla_violation : この案件に添付された SLA に違反した回数を表す整数。
predicted_sla_viol	issue.predicted_sla_viol : (r5.5) Neugent 関連テクノロジーのフィールド。
macro_predict_viol	issue.macro_predict_viol : (r5.5) Neugent 関連テクノロジーのフィールド。
created_via	issue.created_via : interface テーブルのレコードへのポインタ。案件の作成に使用されたインターフェースを示します。 issue.created_via = interface.id
call_back_date	issue.call_back_date : 依頼者に今後連絡する日時を示す日時フィールド (pdmtime) 。
call_back_flag	issue.call_back_flag : issue.call_back_date の日時にアナリストが通知するかどうかを示すブール値。ユーザにはチェック ボックスとして表示されます。
string1	ユーザ定義可能なテキストフィールド。
string2	ユーザ定義可能なテキストフィールド。
string3	ユーザ定義可能なテキストフィールド。
string4	ユーザ定義可能なテキストフィールド。
string5	ユーザ定義可能なテキストフィールド。
string6	ユーザ定義可能なテキストフィールド。
service_date	issue.service_date : 外部ベンダーがこの案件にサービスを提供する予定日時 (pdmtime) 。
service_num	issue.service_num : 外部ベンダーへのサービスまたは発注書番号を文書化するテキストフィールド。

フィールド	備考
product	issue.product : product テーブルへのレコードのポインタ。この案件の影響を受ける製品を示します。 issue.product = product.id
actions	issue.actions : アクションを文書化するための大きなテキストフィールド。
type_of_contact	issue.type_of_contact : toc テーブルのレコードへのポインタ。案件に対する affected_end_user の一般的な分類を示します。 issue.type_of_contact = toc.id
reporting_method	issue.reporting_method : 案件の作成元を分類する repmeth テーブルのレコードへのポインタ。案件を作成するユーザにより選択されます。 issue.reporting_method = repmeth.id
person_contacting	issue.person_contacting : perscon テーブルのレコードへのポインタ。affected_end_user または依頼者の役割を示します。 issue.person_contacting = perscon.id
status_name	issstat.sym : ユーザに表示されるステータスの説明。 issue.status = issstat.code
priority_num	pri.sym : ユーザに表示される優先度の説明。 issue.priority = pri.enum
category_name	isscat.sym : ユーザに表示される案件カテゴリ名。 issue.category = isscat.code
organization_name	ca_organization.org_name : ユーザに表示される組織名。 issue.organization = ca_organization.organization_uid
affected_end_user_lastname	ca_contact.last_name : 影響を受けるエンドユーザの姓。 issue.affected_end_user = ca_contact.contact_uid
affected_end_user_firstname	ca_contact.first_name : 影響を受けるエンドユーザの名。 issue.affected_end_user = ca_contact.contact_uid
affected_end_user_middlename	ca_contact.middle_name : 影響を受けるエンドユーザのミドルネーム。 issue.affected_end_user = ca_contact.contact_uid
assignee_lastname	ca_contact.last_name : 担当者の姓。 issue.assignee = ca_contact.contact_uid
assignee_firstname	ca_contact.first_name : 担当者の名。 issue.assignee = ca_contact.contact_uid

フィールド	備考
assignee_middlename	ca_contact.middle_name : 担当者のミドルネーム。 issue.assignee = ca_contact.contact_uuid
groupID	View_Group.contact_uuid : この案件に割り当てられたグループで使用される内部 ID のバイナリ表示。 issue.group_id = ca_contact.contact_uuid
group_name	View_Group.last_name : この案件に割り当てられたグループの名前。 issue.group = ca_contact.contact_uuid
service_type	srv_desc.sym : この案件に割り当てられたサービス タイプの名前。 issue.support_lev = srv_desc.code
impact_num	impact.sym : ユーザに表示される影響度の説明。 issue.impact = impact.enum
product_sym	product.sym : ユーザに表示される製品の説明。 issue.product = product.id
type_of_contact_sym	toc.sym : ユーザに表示される連絡先タイプの説明。 issue.type_of_contact = toc.id
rpting_method_sym	repmeth.sym : ユーザに表示されるレポート方法の説明。 issue.reporting_method = repmeth.id
person_contacting_sym	perscon.sym : ユーザに表示される連絡先担当者の説明。 issue.person_contacting = perscon.id
created_via_sym	interface.sym : issue.created_via = interface.id.
rootcause_sym	rootcause.sym : issue.rootcause = rootcause.id.

View_Issue_Act_Log

以下に、すべての案件アクティビティ ログの基本ビューを示します。これは、案件アクティビティ ログテーブル (chgalg) に、アクティビティタイプテーブル (act_type) および連絡先テーブル (ca_contact) が結合されたビューで、実際のアクティビティ タイプや、アクティビティを実行したアナリストのフルネームなど、よりわかりやすいデータが表示されます。

フィールド	備考
id	issalg.id : issalg テーブルのこのレコードの固有 ID。
persid	issalg.persid : issalg テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (issalg を意味する issalg) とコロンが付きます。
issue_id	issalg.issue_id : このアクティビティが属する案件 ID へのポインタ。 issalg.issue_id = issalg.id
last_mod_dt	issalg.last_mod_dt : 最終変更日時 (pdmtime) 。
time_spent	issalg.time_spent : このアクティビティに費やされた時間。総秒数で保存されます。たとえば、「80」は 1 分 20 秒のことです。
time_stamp	issalg.time_stamp : ユーザが変更可能なアクティビティの日時 (pdmtime) 。
system_time	issalg.system_time : レコードの作成日時 (pdmtime) 。
analyst	issalg.analyst : アクティビティを実行したアナリストを取得するための連絡先 uuid を参照するバイナリ固有 ID。 issalg.analyst = ca_contact.contact_uuid
description	issalg.description : このアクティビティの説明テキスト。ユーザによる変更が可能です。
action_desc	issalg.action_desc : 自動化アクションの説明テキスト。ユーザによる変更はできません。
type	issalg.type : アクティビティ タイプ テーブル内のレコードへのテキスト ポインタ。 issalg.type = act_type.code
internal	issalg.internal : このログ エントリが全ユーザ表示可能か内部専用かを示す整数フラグ (1 または 0) 。
knowledge_session	issalg.knowledge_session : 特定ユーザの特定セッションの ID。
knowledge_tool	issalg.knowledge_tool : NLS_FAQ や EXPERT など、検索に使用するナレッジ ツールのインジケータ。
analyst_lastname	View_Contact_Full.last_name : issalg.analyst = ca_contact.contact_uuid から派生したアナリストの姓。
analyst_firstname	View_Contact_Full.first_name : アナリストの名。
analyst_middlename	View_Contact_Full.middle_name : アナリストのミドルネーム。

フィールド	備考
activity_type	act_type.sym : issalg.type = act_type.code により参照されるアクティビティ タイプ。

View_Issue_to_Assets

以下のフィールドのリストに、案件およびそのアセットの基本ビューを示します。案件テーブル (issue) は、所有リソース テーブル (ca_owned_resource) およびその他のアセット関連テーブルと間接的に結合されており、各案件のアセット リストを取得することができます。アセットが割り当てられてない案件は、表示されない場合があります。

フィールド	備考
View_Issue.*	View_Issue ビューにリストされるすべてのフィールドを定義する View_Issue ビュー。
assetID	ca_owned_resource.own_resource_uuid : アセット レコードの不変かつ内部で固有の ID として機能するバイナリ フィールド。
asset_serial_num	ca_owned_resource.serial_number : アセット レコードのシリアル番号。
asset_class	ca_resource_class.name : アセットが所属するクラスの簡単な説明。 ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name : このアセットが所属するアセット ファミリ。 ca_owned_resource.resource_class = ca_resource_class.id AND ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name : このアセットを識別するネットワーク名。

View_Issue_to_Issue_Act_Log

以下に、すべての案件およびそのアクティビティ ログの基本ビューを示します。このビューにより、View_Issue ビューと View_Issue_Act_Log ビューが結合され、案件およびそのアクティビティ ログに関する詳細な情報を表示できます。実際のデータは、フィールドリストの最後にあります。

フィールド	備考
View_Issue.*	前述の View_Issue ビューの定義を参照してください。
issalg_id	issalg.id : issalg テーブルのこのレコードの固有 ID。
issalg_persid	issalg.persid : issalg テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (issalg を意味する issalg) とコロンが付きます。
issue_id	issalg.issue_id : このアクティビティが属する案件 ID へのポインタ。 issalg.issue_id = issalg.id
issalg_last_mod_dt	issalg.last_mod_dt : 最終変更日時 (pdmtime) 。
time_spent	issalg.time_spent : このアクティビティに費やされた時間。総秒数で保存されます。たとえば、「80」は 1 分 20 秒のことです。
time_stamp	issalg.time_stamp : ユーザが変更可能なアクティビティの日時 (pdmtime) 。
system_time	issalg.system_time : レコードの作成日時 (pdmtime) 。
analyst	issalg.analyst : アクティビティを実行したアナリストを取得するための連絡先 uuid へのバイナリ固有ポインタ。 issalg.analyst = ca_contact.contact_uuid
issalg_description	issalg.description : このアクティビティの説明テキスト。ユーザによる変更が可能です。
action_desc	issalg.action_desc : 自動化アクションの説明テキスト。ユーザによる変更はできません。
type	issalg.type : アクティビティ タイプ テーブル内のレコードへのテキスト ポインタ。 issalg.type = act_type.code
internal	issalg.internal : このログ エントリが全ユーザ表示可能か内部専用かを示す整数フラグ (1 または 0) 。
knowledge_session	issalg.knowledge_session : 特定ユーザの特定セッションの ID。

フィールド	備考
knowledge_tool	issalg.knowledge_tool : NLS_FAQ や EXPERT など、検索に使用するナレッジ ツールのインジケータ。
issalg_analyst_id	issalg.analyst : アクティビティを実行したアナリストを取得するための連絡先 uuid へのバイナリ固有ポイント。 issalg.analyst = ca_contact.contact_uuid

View_Change_to_Request

以下に、リクエストのみが割り当てられた変更要求の基本ビューを示します。このビューは、**View_Change** ビューがリクエスト テーブル (call_req) に結合された結果です。変更要求および関連付けられたリクエストの基本ビューが表示されます。

フィールド	備考
View_Change.*	前述の View_Change ビューに表示されるすべてのフィールドを表示します。
cr_id	call_req.id : call_req テーブルのこのレコードの固有 ID。
ref_num	call_req.ref_num : アナリストおよびカスタマが特定のリクエストの参照に使用するリクエスト参照番号
cr_summary	call_req.summary : 簡単に参照できるリクエストの概要。
cr_persid	call_req.persid : call_req テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (call_req テーブルを意味する cr) とコロンが付きます。
cr_description	call_req.description : アナリストまたはカスタマが作成したリクエストの詳細な説明。
cr_status	call_req.status : cr_stat テーブルのレコードを参照する固有 ID。このリクエストのステータスを示します。 call_req.status = cr_stat.code
cr_active_flag	call_req.active_flag : このリクエスト レコードをアクティブにするかどうかを決定する整数フラグ (1 または 0)

フィールド	備考
time_spent_sum	call_req.time_spent_sum : すべての act_log レコードの time_spent フィールドの派生合計。秒数で保存されます。たとえば、「80」は 1 分 20 秒のことです。
cr_open_date	call_req.open_date : リクエストの作成日を示すタイムスタンプ (pdmtime)。
cr_last_mod_dt	call_req.last_mod_dt:最終変更日を示すタイムスタンプ (pdmtime)。
cr_close_date	call_req.close_date : リクエストが非アクティブに設定された日付を示すタイムスタンプ (pdmtime)
cr_log_agent	call_req.log_agent : ca_contact テーブルを参照する固有 ID (バイナリ)。リクエストの最初の作成者を参照します。 call_req.log_agent = ca_contact.contact_uuid
cr_group_id	call_req.group_id : ca_contact テーブルのレコードを参照する固有 ID (バイナリ)。リクエストに現在割り当てられているグループを表します。 call_req.group_id = ca_contact.contact_uuid
cr_assignee	call_req.assignee: ca_contact テーブルのレコードを参照する固有 ID (バイナリ)。リクエストに現在割り当てられているユーザを表します。 call_req.assignee = ca_contact.contact_uuid
customer	call_req.customer : ca_contact テーブルのレコードを参照する固有 ID (バイナリ)。このリクエストの影響を受けるエンドユーザを表します。 call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id : 経理専門用語のインジケータとして使用できるテキストフィールド。このリクエストの経費を適切なコストセンターに請求できます。
affected_rc	call_req.affected_rc : ca_owned_resource テーブルの行を参照する固有 ID (バイナリ)。このリクエストが適用されるアセットを表します。 call_req.affected_rc = ca_owned_resource.own_resource_uuid.
cr_support_lev	call_req.support_lev : service desc レコードへのポインタ。このリクエストを完了するときの制約を自動化できます。 call_req.support_lev = srv_desc.code

フィールド	備考
cr_category	call_req.category : prob_ctg テーブルのレコードを参照する固有 ID。 このリクエストが所属するカテゴリを表します。 call_req.category = prob_ctg.persid
solution	call_req.solution: ソリューションを取得するためのコール ソリューションへのポインタ。 call_req.solution = crsol.persid
cr_impact	call_req.impact : impact テーブルの行を参照する固有 ID (整数)。 このリクエストが影響を与えているスコープを示します。 call_req.impact = impact.enum
cr_priority	call_req.priority: pri テーブルのレコードを参照する固有 ID (整数)。 このリクエストに関連付けられた作業の優先度をアナリストが決定する方法を示します。 call_req.priority = pri.enum
urgency	call_req.urgency : urgency テーブルの行を参照する固有 ID (整数)。 ユーザが考えるこのリクエスト解決の緊急度を文書化します。 call_req.urgency = urgency.enum
severity	call_req.severity : severity テーブルの行を参照する固有 ID (整数)。 この未解決リクエストの重大度を示します。 call_req.severity = sevrtty.enum
extern_ref	関連するチケットを指定します。
last_act_id	最終アクティビティの ID
cr_ticket	関連付けられたチケットを取得するためのトラブル チケットへのポインタ
cr_parent	call_req.parent : 変更要求の階層を作成できる別のリクエスト固定 ID への固定 ID ポインタ call_req.parent = call_req.persid
cr_template_name	call_req.template_name : このリクエストが指定されたテキスト値。 ほかの同様のリクエストのテンプレートとしてリストから選択できます。 cr_template.template = call_req.persid
cr_sla_violation	call_req.sla_violation : このリクエストに割り当てられた SLA に違反した回数を表す整数
cr_predicted_sla_viol	call_req.predicted_sla_viol : (r5.5) Neugent 関連テクノロジーのフィールド

フィールド	備考
cr_created_via	call_req.created_via : インターフェース テーブルのレコードへの整数ポインタ。変更要求がどのインターフェースから開始されたかを示します。 call_req.created_via = interface.id
cr_call_back_date	call_req.call_back_date : affected_end_user に今後連絡する日時を示すタイムスタンプ フィールド (pdmtime)
cr_call_back_flag	call_req.call_back_flag : call_req.call_back_date の日時にアナリストに通知するかどうかを示すブール値。ユーザにはチェック ボックスとして表示されます。
event_token	call_req.event_token : CA NSM でメッセージの照合に使用されます。
type	call_req.type : crt テーブルのレコードを参照するテキスト フィールド。このリクエストの ITIL タイプを示します。 call_req.type = crt.code
cr_string1	ユーザが定義可能な文字列
cr_string2	ユーザが定義可能な文字列
cr_string3	ユーザが定義可能な文字列
cr_string4	ユーザが定義可能な文字列
cr_string5	ユーザが定義可能な文字列
cr_string6	ユーザが定義可能な文字列
change	call_req.change : chg テーブルの行を参照する固有 ID (整数)。このリクエストの結果として作成された変更要求を示します。 call_req.change = chg.id.

View_Issue_to_Issue_WF

このビューは、View_Issue ビューがワークフロー タスク テーブル (isswf) に結合された結果です。案件およびそのワークフロー タスクの基本ビューが表示されます。ワークフロー タスクが割り当てられていない案件は、表示されない場合があります。

フィールド	備考
View_Issue.*	各フィールドの詳細については、前述の View_Issue の定義を参照してください。
wf_id	isswf.id : isswf テーブルのレコードの固有 ID。
wf_persid	isswf.persid : isswf テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (isswf) とコロンが付きます。
del	isswf.del : このレコードをユーザに表示するかどうかを示すブール値。
object_type	isswf.object_type : このワークフロー タスクが添付されたレコードタイプ (iss など) の識別に使用されるファクトリ名。
object_id	isswf.object_id : このワークフロー タスクが添付されたレコードの識別に使用される固有 ID。 isswf.object_id = issue.i :
task	isswf.task : このレコードが表すタスク タイプを参照する ID。 isswf.task = tskty.code
wf_template	isswf.wf_template : このワークフロー タスク レコードが作成されたテンプレートを参照する ID。 isswf.wf_template = wftpl.id
sequence	isswf.sequence : このワークフロー タスク レコードを CA SDM で表示および実行する順序 (たとえば、昇順) を示す整数。
wf_status	isswf.status : tskstat レコードを参照する ID。 このワークフロー タスクの現在のステータスを示します。 isswf.status = tskstat.code
group_task	isswf.group_task : このタスクがグループに所属するかどうかを示すブール値。
asset	isswf.asset : ca_owned_resource テーブルのレコードを参照するバイナリ固有 ID。 isswf.asset = ca_owned_resource.own_resource_uuid
creator	isswf.creator : ca_contact テーブルのレコードを参照するバイナリ固有 ID。 このワークフロー タスクの作成者を示します。 isswf.creator = ca_contact.contact_uuid
date_created	isswf.date_created : このワークフロー タスクの作成日/タイムスタンプ (pdmtime) 。

フィールド	備考
wf_assignee	isswf.assignee : ca_contact テーブルのレコードを参照するバイナリ固有 ID。このワークフロー タスクに現在割り当てられている担当者を示します。 isswf.assignee = ca_contact.contact_uuid
done_by	isswf.done_by : ca_contact テーブルのレコードを参照するバイナリ固有 ID。このワークフロー タスクを完了または承認した実行者を示します。 isswf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date : ワークフロー タスクがアクティブなステータスに変わった開始日を示すタイムスタンプ (pdmtime) 。
wf_est_comp_date	isswf.est_comp_date : このタスクの完了予定日を示すタイムスタンプ (pdmtime) 。
est_duration	isswf.est_duration : このワークフロー タスクの予定期間。
completion_date	isswf.completion_date : このワークフロー タスクの完了日を示すタイムスタンプ (pdmtime) 。
actual_duration	isswf.actual_duration : このワークフロー タスクの完了にかかった期間。
wf_est_cost	isswf.est_cost : このワークフロー タスクの予定コスト。
cost	isswf.cost : このワークフロー タスクの完了にかかったコスト。
wf_description	isswf.description : ワークフロー タスクの説明。

フィールド	備考
wf_last_mod_dt	isswf.last_mod_dt : このワークフロー タスクの最終変更日を示すタイムスタンプ (pdmtime) 。
wf_last_mod_by	isswf.last_mod_by : contact テーブルのレコードを参照するバイナリ固有 ID。 このワークフロー タスクに対して変更を行った最後のユーザーを示します。 isswf.last_mod_by = ca_contact.contact_uuid

View_Issue_to_Properties

このビューは、View_Issue ビューが案件プロパティ テーブル (issprp) に結合された結果です。案件および案件に割り当てられたプロパティの基本ビューが表示されます。 プロパティが割り当てられていない案件は、表示されない場合があります。

フィールド	備考
View_Issue.*	各フィールドの詳細については、前述の View_Issue の定義を参照してください。
prp_id	issprp.id : プロパティ レコードの整数固有 ID。
prp_persid	issprp.persid : prp テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (prp) とコロンが付きます。
sequence	issprp.sequence : このプロパティ レコードを CA SDM で表示する順序 (たとえば、昇順) を示す整数。
label	issprp.label : issprp.value フィールドに表示する簡単な説明。
value	issprp.value : prp_description フィールドおよび issprp.label フィールドにユーザーが入力した値。
prp_last_mod_dt	issprp.last_mod_dt : このプロパティの最終変更日を示すタイムスタンプ (pdmtime) 。
prp_last_mod_by	issprp.last_mod_by : ca_contact テーブルのレコードを参照するバイナリ ID。 このレコードの最終変更者を示します。 issprp.last_mod_by = ca_contact.contact_uuid
required	issprp.required : レコードを保存する前にこのプロパティに issprp.value を指定する必要があるかどうかを示すブール値。

フィールド	備考
sample	issprp.sample : サンプル値が表示されるテキストフィールド。ユーザは、このフィールドを参考にして最も有効な値を issprp.value に入力できます。
owning_iss	issprp.owning_iss : このプロパティが添付されたレコードの識別に使用する固有 ID。 issprp.object_id = issue.persid
prp_description	issprp.description : issprp.value に入力する値の種類を説明するテキストフィールド。

View_Request

以下に、すべてのリクエストの基本ビューを示します。リクエストテーブルが CA SDM のほかのテーブルと結合され、リクエストのサービスタイプ、重大度、緊急度、カテゴリ、優先度などの詳細が表示されます。また、リクエストの詳細も表示されます。リクエスト (call_req) テーブルのすべてのフィールドが選択されます。テーブルの結合によって抽出されたフィールドは、このフィールドリストの最後に表示されます。

フィールド	備考
id	call_req.id : call_req テーブルのこのレコードの固有 ID。
persid	call_req.persid : call_req テーブルのこのレコードの固有 ID。 先頭にオブジェクト ID (call_req テーブルを意味する cr) とコロンが付きます。
ref_num	call_req.ref_num : アナリストおよびカスタマが特定のリクエストの参照に使用するリクエスト参照番号。
summary	call_req.summary : 簡単に参照できるリクエストの概要。
description	call_req.description : アナリストまたはカスタマが作成したリクエストの詳細な説明。
status	call_req.status : cr_stat テーブルのレコードを参照する固有 ID。このリクエストのステータスを示します。 call_req.status = cr_stat.code

フィールド	備考
active_flag	call_req.active_flag : このリクエストレコードをアクティブにするかどうかを決定する整数フラグ (1 または 0) 。
open_date	call_req.open_date : リクエストの作成日を示すタイムスタンプ (pdmtime) 。
time_spent_sum	call_req.time_spent_sum : すべての act_log レコードの time_spent フィールドの派生合計。秒数で保存されます。たとえば、「80」は 1 分 20 秒のことです。
last_mod_dt	call_req.last_mod_dt : 最終変更日を示すタイムスタンプ (pdmtime) 。
close_date	call_req.close_date : リクエストが非アクティブに設定された日付を示すタイムスタンプ (pdmtime) 。
resolve_date	リクエストが解決した日付 (pdmtime)
rootcause	rootcause.id へのポインタ
log_agent	call_req.log_agent : ca_contact テーブルを参照するバイナリ固有 ID。 リクエストの最初の作成者を参照します。 call_req.log_agent = ca_contact.contact_uuid
assignee	call_req.assignee : ca_contact テーブルのレコードを参照するバイナリ固有 ID。リクエストに現在割り当てられているユーザを表します。 call_req.assignee = ca_contact.contact_uuid
group_id	call_req.group_id : ca_contact テーブルのレコードを参照するバイナリ固有 ID。 リクエストに現在割り当てられているグループを表します。 call_req.group_id = ca_contact.contact_uuid
customer	call_req.customer : ca_contact テーブルのレコードを参照するバイナリ固有 ID。 このリクエストの影響を受けるエンドユーザを表します。 call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id : 経理専門用語のインジケータとして使用できるテキストフィールド。このリクエストの経費を適切なコストセンターに請求できます。

フィールド	備考
affected_rc	call_req.affected_rc : ca_owned_resource テーブルの行を参照するバイナリ固有 ID。このリクエストが適用されるアセットを表します。 call_req.affected_rc = ca_owned_resource.own_resource_uuid.
support_lev	call_req.support_lev : service desc レコードへのポインタ。このリクエストを完了するときの制約を自動化できます。 call_req.support_lev = srv_desc.code.
category	call_req.category : prob_ctg テーブルのレコードを参照する固有 ID。このリクエストが所属するカテゴリを表します。 call_req.category = prob_ctg.persid
solution	call_req.solution : ソリューションを取得するためのコール ソリューションへのポインタ。 call_req.solution = crsol.persid
impact	call_req.impact : impact テーブルの行を参照する整数固有 ID。リクエストの影響範囲を示します。 call_req.impact = impact.enum
priority	call_req.priority : pri テーブルのレコードを参照する整数固有 ID。このリクエストに関連付けられた作業の優先度をアナリストが決定する方法を示します。 call_req.priority = pri.enum
urgency	call_req.urgency : urgency テーブルの行を参照する整数固有 ID。ユーザが考えるこのリクエスト解決の緊急度を示します。 call_req.urgency = urgncy.enum
severity	call_req.severity : severity テーブルの行を参照する整数固有 ID。この未解決リクエストの重大度を示します。 call_req.severity = sevrty.enum
extern_ref	関連付けられたチケットへの外部参照
last_act_id	最終アクティビティの ID
cr_ticket	関連付けられたチケットを取得するためのトラブル チケットへのポインタ

フィールド	備考
parent	call_req.parent : 変更要求の階層を作成できる別のリクエスト固定 ID への固定 ID ポインタ。 call_req.parent = call_req.persid
template_name	call_req.template_name : このリクエストが指定されたテキスト値。ほかの同様のリクエストのテンプレートとしてリストから選択できます。 cr_template.template = call_req.persid
sla_violation	call_req.sla_violation : このリクエストに割り当てられた SLA に違反した回数を表す整数。
predicted_sla_viol	Neugent で予測される、SLA に違反する可能性のあるリクエスト
macro_predicted_violation	Neugent で予測される、SLA に違反する可能性のあるリクエスト
created_via	call_req.created_via : interface テーブルのレコードへの整数ポインタ。変更要求の作成に使用されたインターフェースを示します。 call_req.created_via = interface.id
call_back_date	call_req.call_back_date : affected_end_user に今後連絡する日時を示すタイムスタンプフィールド (pdmtime) 。
call_back_flag	call_req.call_back_flag : call_req.call_back_date の日時にアナリストに通知するかどうかを示すブール値。ユーザにはチェック ボックスとして表示されます。
event_token	call_req.event_token : CA NSM でメッセージの照合に使用されます。
sched_token	call_req.sched_token : CA NSM でメッセージの照合に使用されます。
type	call_req.type : crt テーブルのレコードを参照するテキストフィールド。このリクエストの ITIL タイプを示します。 call_req.type = crt.code
string1	ユーザが定義可能な文字列

フィールド	備考
string2	ユーザが定義可能な文字列
string3	ユーザが定義可能な文字列
string4	ユーザが定義可能な文字列
string5	ユーザが定義可能な文字列
string6	ユーザが定義可能な文字列
problem	ITIL の問題
incident_priority	ITIL インシデントの優先度
change	call_req.change : chg テーブルの行を参照する整数固有 ID。このリクエストの結果として作成された変更要求を示します。 call_req.change = chg.id.
service_type	srv_desc.sym : 実際のサービス タイプ。 call_req.support_lev = srv_desc.code
severity_num	sevrty.sym : 実際の重大度数。 call_req.severity = sevrty.enum
urgency_num	urgncy.sym : 実際の緊急度数。 call_req.urgency = urgncy.enum
category_name	prob_ctg.sym : 実際のリクエスト領域（問題カテゴリ）。 call_req.category = prob_ctg.id
asset	ca_owned_resource.resource_name : 実際のアセット名。 call_req.affected_rc = ca_owned_resource.own_resource_uuid
impact_num	impact.sym : 実際の影響度数。 call_req.impact = impact.enum

フィールド	備考
assignee_lastname	ca_contact.last_name : 実際の担当者の姓。 call_req.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name : 実際の担当者の名。 call_req.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name : 実際の担当者のミドルネーム。 call_req.assignee = ca_contact.contact_uuid
customer_lastname	ca_contact.last_name : 実際に影響を受けるエンドユーザの姓。 call_req.customer = ca_contact.contact_uuid
customer_firstname	ca_contact.first_name : 実際に影響を受けるエンドユーザの名。 call_req.customer.ca_contact.contact_uuid
customer_middlename	ca_contact.middle_name : 実際に影響を受けるエンドユーザのミドルネーム。 call_req.customer = ca_contact.contact_uuid
group_name	View_Group.last_name : 実際のグループ名。
GroupID	View_Group.contact_uuid : 実際のグループ キー ID。
status_name	cr_stat.sym : 実際のステータス。
priority_num	pri.sym : 実際の優先度数。

View_Request_to_Act_Log

以下に、すべてのリクエストおよびそのアクティビティ ログの基本ビューを示します。 **View_Request** ビューを **View_Act_Log** ビューと結合すると、リクエストごとの各アクティビティに関する詳細を表示することができます。

フィールド	備考
View_Request.*	前述の View_Request セクションで定義されたフィールドを参照してください。
View_Act_Log.*	前述の View_Act_Log セクションで定義されたフィールドを参照してください。

View_Request_to_Properties

以下に、コール リクエストおよびそのプロパティの基本ビューを示します。このビューには、コール リクエスト (**call_req**) テーブルおよびリクエスト プロパティ (**cr_prp**) テーブルのすべてが表示されます。

フィールド	備考
View_Request.*	前述の View_Request セクションで定義されたフィールドを参照してください。
crprp_id	cr_prp.id : プロパティ レコードの整数固有 ID。
crprp_persid	cr_prp.persid : cr_prp テーブルのこのレコードの固有 ID。先頭にオブジェクト ID (cr_prp) とコロンが付きます。
sequence	cr_prp.sequence : このプロパティ レコードを CA SDM で表示する順序 (たとえば、昇順) を示す整数。
label	cr_prp.label : cr_prp.value フィールドに表示する簡単な説明。
value	cr_prp.value : prp_description フィールドおよび cr_prp.label フィールドにユーザが入力した値。
crprp_last_mod_dt	cr_prp.last_mod_dt : このプロパティの最終変更日を示すタイムスタンプ (pdmtime)。
crprp_last_mod_by	cr_prp.last_mod_by : ca_contact テーブルのレコードを参照するバイナリ ID。このレコードの最終変更者を示します。 cr_prp.last_mod_by = ca_contact.contact_uuid
required	cr_prp.required : レコードを保存する前にこのプロパティに cr_prp.value を指定する必要があるかどうかを示すブール値。

フィールド	備考
sample	cr_prp.sample : サンプル値が表示されるテキスト フィールド。ユーザは、このフィールドを参考にして最も有効な値を cr_prp.value に入力できます。
owning_cr	cr_prp.owning_cr : このプロパティが添付されたレコードの識別に使用する固有 ID。 cr_prp.object_id = call_req.persid
crprp_description	cr_prp.description : cr_prp.value に入力する値の種類を説明するテキスト フィールド。

付録 C: フォーム グループ

このセクションには、以下のトピックが含まれています。

[顧客フォーム グループ](#) (P. 1406)

[従業員フォーム グループ](#) (P. 1407)

[アナリスト フォーム グループ](#) (P. 1409)

顧客フォーム グループ

以下の Web フォームが、顧客フォーム グループに含まれます。

- about.html
- bin_form_np.html
- chg_lr.html
- cr_lr.html
- detail_iss.html
- detail_issalg.html
- detail_KD.html
- generic.html
- home.html
- iss_lr.html
- issue_status_change.html
- list_iss.html
- list_isscat.html
- list_KD.html
- menu_frames.html
- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html
- std_head.html
- std_header.html
- std_head_site.html

従業員フォームグループ

以下の Web フォームが、従業員フォームグループに含まれます。

- about.html
- bin_form_np.html
- buttons.html
- change_status_change.html
- chg_lr.html
- cr_lr.html
- detail_alg.html
- detail_chg.html
- detail_chgalg.html
- detail_cr.html
- detail_in.html
- detail_KD.html
- generic.html
- home.html
- iss_lr.html
- list_chg.html
- list_chgcat.html
- list_cr.html
- list_in.html
- list_KD.html
- list_pcat.html
- list_pcat_cr.html
- list_pcat_in.html
- menu_frames.html
- request_status_change.html
- show_error.html
- std_body.html
- std_body_site.html

- std_footer.html
- std_footer_site.html
- std_head.html
- std_header.html
- std_head_site.html

アナリスト フォーム グループ

以下の Web フォームは、アナリスト フォーム グループに含まれます。

A

- about.html
- acctyp_role_tab.html
- acctyp_web_auth_tab.html
- acctyp_wsp_tab.html
- admin_empty.html
- admin_main_role.html
- admin_tab_dflt.html
- admin_tree.html
- attmnt_content_tab.html
- attmnt_fields.html
- attmnt_permissions_tab.html
- attmnt_upload_popup.html
- att_mgs_event.html
- att_stype_event.html
- aty_chg_ntfr_tab.html
- aty_chg_svy_tab.html
- aty_cr_ntfr_tab.html
- aty_cr_svy_tab.html
- aty_iss_ntfr_tab.html
- aty_iss_svy_tab.html
- aty_kdComment_ntfr_tab.html
- aty_kd_ntfr_tab.html
- aty_mgs_ntfr_tab.html

B

- bhvtpl_todo_tab.html
- bhvtpl_trans_info_tab.html

- bin_form_np.html

C

- cancel.html
- cancel_empty.html
- category_content_tab.html
- category_permissions_tab.html
- chgcat_auto_assignment_tab.html
- chgcat_prptpl_tab.html
- chgcat_wftpl_tab.html
- chg_accumulate.html
- chg_causedreq_tab.html
- chg_close_all_child.html
- chg_expedite.html
- chg_lr.html
- chg_relchg_tab.html
- chg_relreq_tab.html
- cia_bmhier_tab.html
- cia_export_bmhier.html
- cia_export_nr.html
- cia_nr_tab.html
- cia_pwd_tab.html
- cia_sync_stat.html
- cnote_tracker.html
- cnt_addr_tab.html
- cnt_auto_assignment_tab.html
- cnt_env_tab.html
- cnt_grp_tab.html
- cnt_mem_tab.html
- cnt_notif_tab.html
- cnt_org_tab.html

- cnt_rem_tab.html
- cnt_role_tab.html
- cr_attach_chg.html
- cr_close_all_child.html
- cr_detach_chg.html
- cr_lr.html
- cr_relreq_tab.html

D

- dcon_constraint_tab.html
- dcon_sql_tab.html
- detail.template
- detail_acctyp.html
- detail_act_type_assoc.html
- detail_ADMIN_TREE.html
- detail_alg.html
- detail_arcpur_rule.html
- detail_asset.html
- detail_atev.html
- detail_atomic_cond.html
- detail_atmnt_edit.html
- detail_atmnt_error.html
- detail_atmnt_folder.html
- detail_atmnt_ro.html
- detail_attr_alias.html
- detail_aty.html
- detail_audlog.html
- detail_bhvtpl.html
- detail_bmcls.html
- detail_bmhier.html
- detail_bmrep.html

- detail_BU_TRANS.html
- detail_ca_cmpny.html
- detail_chg.html
- detail_chgalg.html
- detail_chgcat.html
- detail_chgstat.html
- detail_chgtype.html
- detail_CI_ACTIONS.html
- detail_CI_ACTIONS_ALTERNATE.html
- detail_CI_DOC_TEMPLATES.html
- detail_CI_STATUSES.html
- detail_CI_WF_TEMPLATES.html
- detail_cmth.html
- detail_cnote.html
- detail_cnt.html
- detail_cost_cntr.html
- detail_country.html
- detail_cr.html
- detail_crs.html
- detail_crsq.html
- detail_cr_prptpl.html
- detail_ctab.html
- detail_ctimer.html
- detail_ctp.html
- detail_dcon.html
- detail_dept.html
- detail_dmn.html
- detail_doc_rep.html
- detail_DOC_VERSIONS.html
- detail_EBR_ACRONYMS.html
- detail_EBR_LOG.html

- detail_EBR_NOISE_WORDS.html
- detail_EBR_SYNONYMS_ADM.html
- detail_event_log.html
- detail_evt.html
- detail_fmgrp.html
- detail_grc.html
- detail_g_cnt.html
- detail_g_loc.html
- detail_g_org.html
- detail_g_prod.html
- detail_g_qname.html
- detail_g_srvrs.html
- detail_g_tblmap.html
- detail_g_tblrule.html
- detail_help_set.html
- detail_hier_edit.html
- detail_hier_ro.html
- detail_ical_event_template.html
- detail_imp.html
- detail_in.html
- detail_iss.html
- detail_issalg.html
- detail_isscat.html
- detail_issstat.html
- detail_iss_wf.html
- detail_kc.html
- detail_KCAT.html
- detail_KD.html
- detail_KD_FILE.html
- detail_KD_QA.html
- detail_KD_SAVE_AS.html

- detail_KD_TASK.html
- detail_KD_TASK_cancel_rework.html
- detail_KD_TASK_retire.html
- detail_KD_template.html
- detail_KEIT_TEMPLATES.html
- detail_KT_ACT_CONTENT.html
- detail_KT_BLC.html
- detail_KT_FILE_TYPE.html
- detail_KT_FLG_TYPE.html
- detail_ldap.html
- detail_ldap_group.html
- detail_loc.html
- detail_LONG_TEXTS.html
- detail_lr_ro.html
- detail_macro.html
- detail_macro_type.html
- detail_menu_bar.html
- detail_menu_tree_name.html
- detail_mfrmod.html
- detail_mgs.html
- detail_mgsalg.html
- detail_mgsstat.html
- detail_NOTIFICATION.html
- detail_no_contract_sdsc.html
- detail_nr.html
- detail_nrf.html
- detail_nr_com.html
- detail_ntfl.html
- detail_ntfm.html
- detail_ntfr.html
- detail_options.html

- detail_org.html
- detail_O_COMMENTS.html
- detail_O_EVENTS.html
- detail_pcat.html
- detail_perscnt.html
- detail_position.html
- detail_pr.html
- detail_prefs.html
- detail_pri.html
- detail_prod.html
- detail_projex.html
- detail_prptpl.html
- detail_prpval.html
- detail_prpval_rule.html
- detail_prp_edit.html
- detail_QUERY_POLICY.html
- detail_rc.html
- detail_response.html
- detail_role.html
- detail_role_go_form.html
- detail_rptmeth.html
- detail_rrf.html
- detail_rss.html
- detail_sapolicy.html
- detail_saprobtyp.html
- detail_sdsc.html
- detail_sdsc_map.html
- detail_seq.html
- detail_sev.html
- detail_site.html
- detail_slatpl.html

- detail_svr_aliases.html
- detail_svr_zones.html
- detail_state.html
- detail_svc_contract.html
- detail_svy_atpl.html
- detail_svy_qtpl.html
- detail_svy_tpl.html
- detail_tab.html
- detail_tenant.html
- detail_tenant_group.html
- detail_tskstat.html
- detail_tskty.html
- detail_tspan.html
- detail_typecnt.html
- detail_tz.html
- detail_urg.html
- detail_USP_PREFERENCES.html
- detail_usp_servers.html
- detail_vpt.html
- detail_web_form.html
- detail_wf.html
- detail_wftpl.html
- detail_wrkshft.html
- dmn_dcon_tab.html
- edit_prop_dyn.html
- ed_image_pane.html
- evt_action_info.html
- evt_config_info.html

- G**
- generic.html

- get_comment.html
- g_profile_browser.html
- g_profile_browser2.html
- g_profile_browser3.html
- g_profile_browser_frameset.html
- g_profile_jump.html
- g_profile_scratchpad.html

H

- hierload_admin_tree.html
- hierload_KCAT.html
- hiersel_admin_tree.html
- hiersel_KCAT.html
- hourglass.html
- html_editor_create_change_order.html
- html_editor_create_ticket.html
- html_editor_frames.html
- html_editor_insert_image.html
- html_editor_insert_link.html
- html_editor_insert_table.html
- html_editor_tabs.html
- html_editor_toolbar.html

I

- insert_iss_wf.html
- insert_wf.html
- in_relreq_tab.html
- isscat_auto_assignment_tab.html
- isscat_prptpl_tab.html
- isscat_wftpl_tab.html
- issue_status_change.html
- iss_accumulate.html

- [iss_close_all_child.htmlpl](#)
- [iss_custfld_tab.htmlpl](#)
- [iss_expedite.htmlpl](#)
- [iss_lr.htmlpl](#)
- [iss_reliss_tab.htmlpl](#)
- [iss_resol_tab.htmlpl](#)

K

- [kd_action_forward.htmlpl](#)
- [kd_action_publish.htmlpl](#)
- [kd_action_reject.htmlpl](#)
- [kd_action_unpublish.htmlpl](#)
- [kd_action_unretire.htmlpl](#)
- [kd_attachments_tab.htmlpl](#)
- [kd_attributes_tab.htmlpl](#)
- [kd_categories_tab.htmlpl](#)
- [kd_content_tab.htmlpl](#)
- [kd_file_prop_tab.htmlpl](#)
- [kd_permissions_tab.htmlpl](#)
- [kd_qa_attributes_tab.htmlpl](#)
- [kd_qa_content_tab.htmlpl](#)
- [keit_tmpl_export_fields_tab.htmlpl](#)
- [keit_tmpl_export_filter_tab.htmlpl](#)
- [keit_tmpl_import_settings_tab.htmlpl](#)
- [keit_tmpl_name_tab.htmlpl](#)
- [kt_admin_attachments.htmlpl](#)
- [kt_admin_automated_policies.htmlpl](#)
- [kt_admin_document_settings.htmlpl](#)
- [kt_admin_faq_options.htmlpl](#)
- [kt_admin_general_settings.htmlpl](#)
- [kt_admin_integration.htmlpl](#)

- kt_admin_knowledge.html
- kt_admin_parse_settings.html
- kt_admin_report_card.html
- kt_admin_search_config_cr.html
- kt_admin_search_config_iss.html
- kt_admin_search_options.html
- kt_admin_survey_settings.html
- kt_admin_workflow_settings.html
- kt_architect.html
- kt_architect2.html
- kt_architect3.html
- kt_architect_delete_KCAT.html
- kt_architect_delete_KD.html
- kt_architect_frameset.html
- kt_architect_init.html
- kt_architect_javascript.html
- kt_architect_KCATs.html
- kt_architect_KCAT_path.html
- kt_architect_KDs.html
- kt_dtbuilder.html
- kt_dtbuilder2.html
- kt_dtbuilder3.html
- kt_dtbuilder_frameset.html
- kt_dtbuilder_node.html
- kt_dtbuilder_prompt_window.html
- kt_dtbuilder_save_dialog_window.html
- kt_dtbuilder_save_tree_form.html
- kt_dtbuilder_tree.html
- kt_email_document.html
- kt_faq_tree.html
- kt_main.html

- kt_main2.html
- kt_main3.html
- kt_main_role.html
- kt_permissions.html

L

- list.template
- list_acctyp.html
- list_act_type_assoc.html
- list_alg.html
- list_all_fmgrp.html
- list_all_lr.html
- list_architect_KDs.html
- list_architect_KDs_Pref.html
- list_arcpur_hist.html
- list_arcpur_rule.html
- list_atev.html
- list_atomic_cond.html
- list_atmnt.html
- list_attr_alias.html
- list_aty.html
- list_audlog.html
- list_bmcls.html
- list_bmhier.html
- list_bmrep.html
- list_bm_task.html
- list_bool.html
- list_ca_cmpny.html
- list_ca_logical_asset.html
- list_chg.html
- list_chgalg.html

- list_chgcat.html
- list_chgsched.html
- list_chgsched_config.html
- list_chgstat.html
- list_chgtype.html
- list_CI_ACTIONS.html
- list_CI_ACTIONS_ALTERNATE.html
- list_CI_DOC_TEMPLATES.html
- list_CI_STATUSES.html
- list_CI_WF_TEMPLATES.html
- list_cmth.html
- list_cnote.html
- list_cnt.html
- list_cost_cntr.html
- list_country.html
- list_cr.html
- list_crs.html
- list_crsq.html
- list_crs_cr.html
- list_crs_in.html
- list_crs_pr.html
- list_crt.html
- list_cr_kt.html
- list_ctab.html
- list_ctimer.html
- list_ctp.html
- list_dcon.html
- list_dept.html
- list_dmn.html
- list_DOC_VERSIONS.html
- list_EBR_ACRONYMS.html

- list_EBR_LOG.html
- list_EBR_NOISE_WORDS.html
- list_EBR_SYNONYMS_ADM.html
- list_event_log.html
- list_evt.html
- list_evtdly.html
- list_grc.html
- list_grpmem.html
- list_g_chg_queue.html
- list_g_cnt.html
- list_g_cr_queue.html
- list_g_iss_queue.html
- list_g_loc.html
- list_g_org.html
- list_g_prod.html
- list_g_qname.html
- list_g_srvrs.html
- list_g_tblmap.html
- list_g_tblrule.html
- list_g_tenant.html
- list_help_item.html
- list_help_set.html
- list_ical_event_template.html
- list_imp.html
- list_in.html
- list_iss.html
- list_issalg.html
- list_isscat.html
- list_issstat.html
- list_iss_kt.html
- list_iss_wf.html

- list_kc.html
- list_KCAT_LINKED.html
- list_KCAT_QA.html
- list_KCAT_tree.html
- list_KD.html
- list_kdsched.html
- list_kdsched_config.html
- list_KD_ATTMNT.html
- list_kd_CI_DOC_LINKS.html
- list_KD_FILE.html
- list_kd_INDEX_DOC_LINKS.html
- list_KD_QA.html
- list_KEIT_export_transactions.html
- list_KEIT_IMPORT_PACKAGES.html
- list_KEIT_import_transactions.html
- list_KEIT_TEMPLATES.html
- list_KT_ACT_CONTENT.html
- list_KT_BLC.html
- list_KT_FILE_TYPE.html
- list_KT_FLG_TYPE.html
- list_KT_FREE_TEXT.html
- list_KT_LIFE_CYCLE_REP.html
- list_ldap.html
- list_ldap_group.html
- list_loc.html
- list_LONG_TEXTS.html
- list_lr.html
- list_macro.html
- list_macro_type.html
- list_menu_bar.html
- list_menu_tree_name.html

- list_mfrmod.html
- list_mgs.html
- list_mgsalg.html
- list_mgsstat.html
- list_NOTIFICATION.html
- list_no_contract_sdsc.html
- list_nr.html
- list_nrf.html
- list_nr_com.html
- list_ntfl.html
- list_ntfm.html
- list_ntfr.html
- list_OA_TABLES.html
- list_options.html
- list_org.html
- list_O_EVENTS.html
- list_pcat.html
- list_pcat_cr.html
- list_pcat_in.html
- list_pcat_pr.html
- list_perscnt.html
- list_position.html
- list_pr.html
- list_pri.html
- list_prod.html
- list_prod_list.html
- list_prpval.html
- list_prpval_rule.html
- list_QUERY_POLICY.html
- list_QUERY_POLICY_ACTIONS.html
- list_rc.html

- list_rel_cat.html
- list_response.html
- list_role.html
- list_role_tab.html
- list_rptmeth.html
- list_rrf.html
- list_rss.html
- list_sapolicy.html
- list_saprobtyp.html
- list_sdsc.html
- list_sdsc_map.html
- list_seq.html
- list_sev.html
- list_showgrp.html
- list_site.html
- list_svr_aliases.html
- list_svr_zones.html
- list_state.html
- list_svc_contract.html
- list_svy_atpl.html
- list_svy_qtpl.html
- list_svy_tpl.html
- list_tab.html
- list_tenant.html
- list_tenant_group.html
- list_tskstat.html
- list_tskty.html
- list_tspan.html
- list_typecnt.html
- list_tz.html
- list_urg.html

- list_osp_servers.html
- list_vpt.html
- list_web_form.html
- list_wf.html
- list_wrkshft.html
- load_properties.html
- load_wait.html
- loc_address_tab.html
- loc_auto_assignment_tab.html
- log_reader.html
- log_reader_banner.html
- log_reader_fs.html
- log_sol_4itil.html

M

- macro_atomic_cond_tab.html
- macro_cnt_tab.html
- macro_ctp_tab.html
- macro_ntfl_tab.html
- macro_rrf_tab.html
- mactyp_exescript_tab.html
- mactyp_valscript_tab.html
- mapped_contracts_tab.html
- menubar.template
- menubar_admin.html
- menubar_architect.html
- menubar_chg_sched.html
- menubar_dtbuilder.html
- menubar_html_editor.html
- menubar_kt.html
- menubar_no.html

- menubar_sd.html
- menubar_sd_chg_manager.html
- menubar_sd_cust_mgr.html
- menubar_sd_cust_rep.html
- menubar_sd_hd_manager.html
- menubar_sd_inc_manager.html
- menubar_sd_know_analyst.html
- menubar_sd_know_manager.html
- menubar_sd_l1_analyst.html
- menubar_sd_l2_analyst.html
- menubar_sd_prb_manager.html
- menubar_sd_vendor_analyst.html
- menu_frames.html
- menu_tree_editor.html
- menu_tree_editor2.html
- menu_tree_editor3.html
- mgs_cnt_tab.html
- mgs_ctp_tab.html
- mgs_ini_tab.html
- mgs_ntfl_tab.html
- mgs_rem_tab.html
- multiframe.template
- multiframe_reports_admin.html
- multiframe_reports_chg_manager.html
- multiframe_reports_cust_mgr.html
- multiframe_reports_inc_mgr.html
- multiframe_reports_know_analyst.html
- multiframe_reports_know_mgr.html
- multiframe_reports_prb_mgr.html
- multiframe_reports_sd_mgr.html

N

- new_lr.html
- nf.html
- nosession.html
- nr_bm_tab.html
- nr_chg_tab.html
- nr_contact_tab.html
- nr_inc_tab.html
- nr_inv_tab.html
- nr_iss_tab.html
- nr_loc_tab.html
- nr_log_tab.html
- nr_org_tab.html
- nr_prb_tab.html
- nr_projex_tab.html
- nr_rel_tab.html
- nr_reqitil_tab.html
- nr_req_tab.html
- nr_serv_tab.html
- ntfl_ntfr_tab.html
- ntfr_aty_tab.html
- ntfr_cnt_tab.html
- ntfr_ctp_tab.html
- ntfr_ntfl_tab.html

O

- order_status_change.html
- org_address_tab.html
- org_env_tab.html

P

- pcat_auto_assignment_tab.html

- pcat_prptpl_tab.html
- pcat_wftpl_tab.html
- power_user_tips.html
- profile_browser.html
- profile_browser2.html
- profile_browser3.html
- profile_browser_frameset.html
- profile_envcnt.html
- profile_envorg.html
- profile_histcnt_chg.html
- profile_histcnt_cr.html
- profile_histcnt_in.html
- profile_histcnt_iss.html
- profile_histcnt_pr.html
- profile_historg_chg.html
- profile_historg_cr.html
- profile_historg_in.html
- profile_historg_iss.html
- profile_historg_pr.html
- profile_infocnt.html
- profile_infoorg.html
- profile_menu.html
- profile_qtemplate.html
- pr_attinc_tab.html
- pr_relreq_tab.html

R

- reports.html
- reports.html.tpl
- request_status_change.html
- role_auth_tab.html

- role_fnacc_tab.html
- role_goform_tab.html
- role_kt_ct_tab.html
- role_kt_docs_tab.html
- role_webform_tab.html
- role_web_interface_tab.html

S

- sapolicy_ac_tab.html
- sapolicy_pt_tab.html
- saprobttyp_dh_tab.html
- saprobttyp_rd_tab.html
- scoreboard.html
- scratchpad.html
- screen_reader_usage.html
- sdsc_chg_slatpl_tab.html
- sdsc_chg_wf_slatpl_tab.html
- sdsc_cr_slatpl_tab.html
- sdsc_iss_slatpl_tab.html
- sdsc_iss_wf_slatpl_tab.html
- sdsc_map_cnt_tab.html
- sdsc_map_grp_tab.html
- sdsc_map_nr_tab.html
- sdsc_map_pri_tab.html
- sdsc_map_urg_tab.html
- sd_kt_admin.html
- sd_main.html
- sd_main_role.html
- search_child_KCATs_filter.html
- show_error.html
- show_main_detail.html

- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html
- std_head.html
- std_head_site.html
- suggest_knowledge_isscat.html
- suggest_knowledge_list_isscat.html
- suggest_knowledge_list_pcat.html
- suggest_knowledge_pcat.html
- suggest_knowledge_search_options.html

T

- tab_detail.template
- tenant_address_tab.html
- tenant_groups_tab.html
- tenant_group_members_tab.html
- tskty_tskstat_tab.html

U

- update_lrel_bmrep.html
- update_lrel_chg.html
- update_lrel_chgcat.html
- update_lrel_cnt.html
- update_lrel_cr.html
- update_lrel_ctp.html
- update_lrel_goform.html
- update_lrel_help_content.html
- update_lrel_in.html
- update_lrel_iss.html
- update_lrel_isscat.html
- update_lrel_loc.html

- update_lrel_macro.html
- update_lrel_nr.html
- update_lrel_ntfl.html
- update_lrel_ntfr.html
- update_lrel_org.html
- update_lrel_pcat.html
- update_lrel_pr.html
- update_lrel_role.html
- update_lrel_tab.html
- update_lrel_tenant.html
- update_lrel_tenant_group.html
- update_lrel_tskstat.html
- update_lrel_webform.html
- update_lrel_wrkshft.html
- upd_chg_sched.html
- upload_file.html
- upload_success.html
- usq_update.html
- usq_update_control.html
- usq_update_fin.html
- usq_update_select.html
- usq_update_tree.html

V

- v30_date_helper.html

W

- wfdef.html
- wftpl_auto_assignment_tab.html
- wftpl_bhvtpl_tab.html
- working.html
- workitems.html

- wrkshft_auto_assignment_tab.html
- wrkshft_schedule_tab.html
- wspmain.html

X

- xfer_esc_chg.html
- xfer_esc_cr.html
- xfer_esc_iss.html
- xx_attmnt_tab.html
- xx_candp_tab.html
- xx_nr_tab.html
- xx_prop_tab.html
- xx_solnalg_tab.html
- xx_stype_tab.html
- xx_template_tab.html
- xx_wf_tab.html

付録 D: RFC 2251 LDAP 結果コード

このセクションには、以下のトピックが含まれています。

[LDAP のリターンコード](#) (P. 1435)

[LDAP サーバの戻り値](#) (P. 1435)

[LDAP クライアントの戻り値](#) (P. 1442)

[LDAP 関連の RFC 標準](#) (P. 1444)

LDAP のリターンコード

LDAP には、各種 LDAP リクエストを受けて LDAP サーバで生成される一連の操作結果コードがあります。これらのコードは、プロトコル操作のステータスを示し、サーバまたはクライアントの戻り値カテゴリにより分類されます。

LDAP サーバの戻り値

以下の表に、さまざまな戻り値を示します。

16 進数	10 進数	説明
0x00	0	LDAP_SUCCESS リクエストされたクライアントの操作が正常に完了したことを示します。
0x01	1	LDAP_OPERATIONS_ERROR 内部エラーが発生したことを示します。サーバは、さらに具体的なエラーに対応できず、リクエストに適切に応答することもできません。クライアントが誤りのあるメッセージを送信したことを示すわけではありません。
0x02	2	LDAP_PROTOCOL_ERROR サーバがクライアントから受信したリクエストが無効またはフォーマットが不正であることを示します。

16 進数	10 進数	説明
0x03	3	LDAP_TIMELIMIT_EXCEEDED クライアントまたはサーバにより指定された操作制限時間を 超えたことを示します。検索操作では、不完全な結果が返され ます。
0x04	4	LDAP_SIZELIMIT_EXCEEDED 検索操作中、クライアントまたはサーバにより指定されたサイ ズ制限を超えたことを示します。 不完全な結果が返されます。
0x05	5	LDAP_COMPARE_FALSE エラー状態ではありません。 比較操作の結果が false であるこ とを示します。
0x06	6	LDAP_COMPARE_TRUE エラー状態ではありません。 比較操作の結果が true であるこ とを示します。
0x07	7	LDAP_AUTH_METHOD_NOT_SUPPORTED バインド操作中、クライアントがリクエストした認証方法が LDAP でサポートされていないことを示します。
0x08	8	LDAP_STRONG_AUTH_REQUIRED 以下のいずれかを示します。 ■ バインドリクエストで、LDAP サーバが強力な認証のみを受 け入れます。 ■ クライアント リクエストで、クライアントがリクエストし た削除などの操作に強力な認証が必要です。 ■ 切断に関する一方的な通知で、LDAP サーバが、クライアン トとサーバの間の通信がセキュリティで保護されているが 予期せず失敗するか、セキュリティで保護されていないこ とを検出します。
0x09	9	Reserved.
0x0A	10	LDAP_REFERRAL エラー状態ではありません。 LDAPv3 で、サーバはリクエスト のターゲット エントリを保持しませんが、参照フィールド内の サーバは保持する可能性があります。

16 進数	10 進数	説明
0x0B	11	LDAP_ADMINLIMIT_EXCEEDED 管理権限により設定された LDAP サーバの制限を超えたことを示します。
0x0C	12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION 1 つ以上の重要な拡張機能が使用できないため、LDAP サーバでリクエストを満たすことができなかったことを示します。サーバがコントロールをサポートしないか、コントロールが操作タイプに適していません。
0x0D	13	LDAP_CONFIDENTIALITY_REQUIRED セッションが、機密性を確保するトランスポートレイヤセキュリティ (TLS) などのプロトコルで保護されていないことを示します。
0x0E	14	LDAP_SASL_BIND_IN_PROGRESS エラー状態ではありません。サーバでプロセスの次の手順の準備が完了したことを示します。クライアントは、サーバに同じ SASL メカニズムを送信して、プロセスを続行する必要があります。
0x0F	15	使用されません。
0x10	16	LDAP_NO_SUCH_ATTRIBUTE 変更操作または比較操作で指定した属性がエントリに存在しないことを示します。
0x11	17	LDAP_UNDEFINED_TYPE 変更操作または追加操作で指定した属性が LDAP サーバのスキーマに存在しないことを示します。
0x12	18	LDAP_INAPPROPRIATE_MATCHING 検索フィルタで指定した一致ルールが、属性の構文に定義したルールと一致しないことを示します。
0x13	19	LDAP_CONSTRAINT_VIOLATION 変更操作、追加操作、または DN の変更操作で指定した属性値が、属性の制約に違反していることを示します。サイズまたは内容のどちらかについて制約されます (バイナリではない文字列のみ)。

16 進数	10 進数	説明
0x14	20	LDAP_TYPE_OR_VALUE_EXISTS 変更操作または追加操作で指定した属性値が、その属性の既存値であることを示します。
0x15	21	LDAP_INVALID_SYNTAX 追加操作、比較操作、または変更操作で指定した属性値が、属性で認識できないか無効な構文であることを示します。
	22-31	使用されません。
0x20	32	LDAP_NO_SUCH_OBJECT ターゲット オブジェクトが見つからないことを示します。このコードは、以下の操作では返されません。 ■ 検索操作で、検索ベースは見つかったが、検索フィルタに一致するエントリは見つからない場合 ■ バインド操作
0x21	33	LDAP_ALIAS_PROBLEM 別名が修飾参照されたときにエラーが発生したことを示します。
0x22	34	LDAP_INVALID_DN_SYNTAX DN の構文が間違っていることを示します。ただし、DN 構文が正しく、LDAP サーバの構造ルールにより操作が許可されない場合、サーバからは以下のコードが返されます。 LDAP_UNWILLING_TO_PERFORM
0x23	35	LDAP_IS_LEAF 指定した操作をリーフ エントリで実行できないことを示します（このコードは現在 LDAP 仕様に含まれていませんが、この定数用に予約されています）。
0x24	36	LDAP_ALIAS_DEREF_PROBLEM 検索操作中、別名が付いたオブジェクト名を読み取る権限がクライアントにないこと、または修飾参照が許可されていないことを示します。
	37-47	使用されません。

16 進数	10 進数	説明
0x30	48	LDAP_INAPPROPRIATE_AUTH バインド操作中、クライアントでは正しく使用できない認証方法を、クライアントが使用しようとしたことを示します。たとえば、以下のような場合にこのエラーが発生します。 ■ 強力な認証が必要なのに、クライアントが簡単な認証を返した場合 ■ エントリにパスワードが定義されていないのに、クライアントが簡単なバインドの DN およびパスワードを返した場合
0x31	49	LDAP_INVALID_CREDENTIALS バインド操作中、以下のいずれかが発生したことを示します。 ■ クライアントから、間違った DN またはパスワードが渡されました。 ■ パスワードが期限切れのため無効になり、侵入者探知などの理由によってアカウントがロックされました。
0x32	50	LDAP_INSUFFICIENT_ACCESS リクエストされた操作を実行する十分な権限がコール元に割り当てられていないことを示します。
0x33	51	LDAP_BUSY LDAP サーバがビジー状態にあり、この時点でクライアント リクエストを処理できないことを示します。クライアントが待機してリクエストを再サブミットすると、サーバでクライアント リクエストを処理できる場合もあります。
0x34	52	LDAP_UNAVAILABLE 一般にシャットダウンが理由で、 LDAP サーバでクライアントのバインド リクエストを処理できないことを示します。

16 進数	10 進数	説明
0x35	53	LDAP_UNWILLING_TO_PERFORM サーバ定義の制限が理由で、LDAP サーバでリクエストを処理できないことを示します。このエラーは、以下の場合に返されます。 ■ エントリの追加リクエストが、サーバの構造ルールに違反している場合 ■ 属性の変更リクエストで、ユーザが変更できない属性が指定されている場合 ■ パスワード制限によりアクションが禁止されている場合 ■ 接続制限によりアクションが抑制されている場合
0x36	54	LDAP_LOOP_DETECT クライアントで別名または参照ループが検出されたため、このリクエストを完了できないことを示します。
	55-63	使用されません。
0x40	64	LDAP_NAMING_VIOLATION 追加操作または DN の変更操作がスキーマの構造ルールに違反することを示します。以下に例を示します。 ■ リクエストにより、別名の下位エントリが配置されている場合 ■ リクエストにより、格納ルールで禁止されているコンテナの下位エントリが配置されている場合 ■ エントリの RDN で、禁止された属性タイプが使用される場合
0x41	65	LDAP_OBJECT_CLASS_VIOLATION 追加操作、変更操作、または DN の変更操作が、エントリのオブジェクトクラスルールに違反することを示します。たとえば、以下のような場合にこのエラーが返されます。 ■ 追加操作または変更操作で、必須属性の値を指定しないでエントリを追加しようとした場合 ■ 追加操作または変更操作で、クラス定義が含まれない属性の値を使用してエントリを追加しようとした場合 ■ 変更操作で、必要に応じて属性を定義する補助クラスを削除せずに必須属性を削除しようとした場合

16 進数	10 進数	説明
0x42	66	LDAP_NOT_ALLOWED_ON_NONLEAF リクエストされた操作がリーフ エントリでのみ許可されることを示します。たとえば、以下のような場合にこのエラーが返されます。 ■ クライアントが親エントリで削除操作をリクエストした場合 ■ クライアントが親エントリで DN の変更操作をリクエストした場合
0x43	67	LDAP_NOT_ALLOWED_ON_RDN 変更操作で、エントリの相対識別名を形成する属性値を削除しようとしたことを示します。
0x44	68	LDAP_ALREADY_EXISTS 追加操作で既存のエントリを追加しようとしたこと、または変更操作でエントリの名前を既存のエントリ名に変更しようとしたことを示します。
0x45	69	LDAP_NO_OBJECT_CLASS_MODS 変更操作で、オブジェクト クラスの構造ルールを変更しようとしたことを示します。
0x46	70	LDAP_RESULTS_TOO_LARGE CLDAP 用に予約されています。
0x47	71	LDAP_AFFECTS_MULTIPLE_DSAS DN の変更操作で、1 つの LDAP サーバから別の LDAP サーバにエントリを移動させるために、複数の LDAP サーバが必要であることを示しています。
	72-79	使用されません。
0x50	80	LDAP_OTHER 不明なエラー状態を示します。これは NDS エラー コードの初期設定値で、その他の LDAP エラー コードにマップされません。

LDAP クライアントの戻り値

以下の表に、さまざまな戻り値を示します。

16 進数	10 進数	説明
0x51	81	LDAP_SERVER_DOWN LDAP ライブラリで、LDAP サーバへの初期接続を確立できないことを示します。LDAP サーバがダウンしているか、指定したホスト名またはポート番号が間違っています。
0x52	82	LDAP_LOCAL_ERROR LDAP クライアントにエラーが発生したことを示します。これは通常、動的メモリの割り当て失敗エラーです。
0x53	83	LDAP_ENCODING_ERROR LDAP サーバを対象とした LDAP リクエストをエンコードするときに、LDAP クライアントでエラーが発生したことを示します。
0x54	84	LDAP_DECODING_ERROR LDAP サーバからの LDAP の応答をデコードするときに、LDAP クライアントでエラーが発生したことを示します。
0x55	85	LDAP_TIMEOUT LDAP クライアントで待機中に、制限時間が超えたことを示します。
0x56	86	LDAP_AUTH_UNKNOWN 不明な認証方法により、ldap_bind または ldap_bind_s 関数が呼び出されたことを示します。
0x57	87	LDAP_FILTER_ERROR 無効な検索フィルタにより、ldap_search 関数が呼び出されたことを示します。
0x58	88	LDAP_USER_CANCELLED ユーザが LDAP 操作をキャンセルしたことを示します。
0x59	89	LDAP_PARAM_ERROR 無効なパラメータ値 (ID パラメータが Null など) により、LDAP 関数が呼び出されたことを示します。

16 進数	10 進数	説明
0x5A	90	LDAP_NO_MEMORY: LDAP 関数を呼び出すときに、動的メモリ割り当て関数が失敗したことを示します。
0B	91	LDAP_CONNECT_ERROR LDAP クライアントと LDAP サーバの接続を確立できない、または接続が切断されたことを示します。
0x5C	92	LDAP_NOT_SUPPORTED クライアントで、リクエストされた機能をサポートしていないことを示します。たとえば、LDAP クライアントが LDAPv2 クライアントとして構築されている場合、クライアントで LDAPv3 の機能が要求されると、ライブラリによりこのエラー コードが設定されます。
0x5D	93	LDAP_CONTROL_NOT_FOUND クライアントがリクエストしたコントロールを、LDAP サーバから送信されたサポート コントロール リストでライブラリが見つけれられないことを示します。
0x5E	94	LDAP_NO_RESULTS_RETURNED LDAP サーバから結果が送信されなかったことを示します。 <code>ldap_parse_result</code> 関数が呼び出されたときに、サーバの応答に結果コードが含まれていません。
0x5F	95	LDAP_MORE_RESULTS_TO_RETURN 結果メッセージに余分な結果が含まれていることを示します。 <code>ldap_parse_result</code> 関数への呼び出しにより、追加の結果コードが使用可能であることが明らかになった場合、ライブラリによりこのコードが設定されます。
0x60	96	LDAP_CLIENT_LOOP LDAP ライブラリでループが検出されたことを示します。通常、後続の参照のときに発生します。

16 進数	10 進数	説明
0x61	97	LDAP_REFERRAL_LIMIT_EXCEEDED 参照がホップ制限を超えたことを示します。ホップ制限により、クライアントがデータを取得するためにホップできるサーバの数が決まります。たとえば、以下のような状況を仮定してみます。 ■ ホップ制限が 2 に設定されています。 ■ 参照はサーバ D に対して行われます。サーバ B (1 ホップ) を介してサーバ C (2 ホップ) に接続し、そこからサーバ D (3 ホップ) に接続します。 この状況では、ホップ制限を超えてしまい、LDAP ライブラリによりこのコードが設定されます。

LDAP 関連の RFC 標準

以下の表は、LDAP 関連の RFC 標準に関する説明です。

RFC	説明
1274	The COSINE and Internet X.500 Schema
1275	Replication Requirements to provide an Internet Directory using X.500
1276	Replication and Distributed Operations extensions to provide an Internet Directory using X.500
1308	Executive Introduction to Directory Services Using the X.500 Protocol
1309	Technical Overview of Directory Services Using the X.500 Protocol
1430	A Strategic Plan for Deploying an Internet X.500 Directory Service
1488	The X.500 String Representation of Standard Attribute Syntaxes
1558	A String Representation of LDAP Search Filters
1617	Naming and Structuring Guidelines for X.500 Directory Pilots
1777	Lightweight Directory Access Protocol v2
1778	The String Representation of Standard Attribute Syntaxes
1779	A String Representation of Distinguished Names
1804	Schema Publishing in X.500 Directory

RFC	説明
1823	The LDAP Application Program Interface
1959	An LDAP URL Format
1960	A String Representation of LDAP Search Filters
2044	UTF -8, a transformation format of Unicode and ISO 10646
2164	Use of an X.500/LDAP Directory to support MIXER address mapping
2218	A Common Schema for the Internet White Pages Service
2247	Using Domains in LDAP/X.500 Distinguished Names
2251	Lightweight Directory Access Protocol (v3)
2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
2253	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names
2254	The String Representation of LDAP Search Filters
2255	The LDAP URL Format
2256	A Summary of the X.500(96) User Schema for use with LDAPv3
2279	UTF-8, a transformation format of ISO 10646
2293	Representing Tables and Subtrees in the X.500 Directory
2294	Representing the O/R Address hierarchy in the X.500 Directory Information Tree
2307	An Approach for Using LDAP as a Network Information Service
2377	Naming Plan for Internet Directory-Enabled Applications
2531	Content Feature Schema for Internet Fax
2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema
2589	Lightweight Directory Access Protocol (v3): Extensions for Dynamic Directory Services
2596	Use of Language Codes in LDAP
2649	An LDAP Control and Schema for Holding Operation Signatures
2657	RFC 2657 - LDAPv2 Client vs. the Index Mesh
2696	LDAP Control Extension for Simple Paged Results Manipulation
2713	Schema for Representing Java(tm) Objects in an LDAP Directory

RFC	説明
2714	Schema for Representing CORBA Object References in an LDAP Directory
2739	Calendar Attributes for vCard and LDAP
2798	Definition of the inetOrgPerson LDAP Object Class
2820	Access Control Requirements for LDAP
2829	Authentication Methods for LDAP
2830	Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security
2849	The LDAP Data Interchange Format (LDIF) - Technical Specification
2879	Content Feature Schema for Internet Fax (V2)
2891	LDAP Control Extension for Server Side Sorting of Search Results
3045	Storing Vendor Information in the LDAP root DSE
3062	LDAP Password Modify Extended Operation
3112	LDAP Authentication Password Schema
3296	Named Subordinate References in Lightweight Directory Access Protocol Directories
3377	Lightweight Directory Access Protocol (v3): Technical Specification
3384	Lightweight Directory Access Protocol (version 3) Replication Requirements