

CA Service Desk Manager

実装ガイド

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

このドキュメントで参照されている CA Technologies ブランドおよび製品は以下のとおりです。

- CA IT Asset Management (以前の CA Asset Portfolio Management (CA APM))
- 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	15
概要.....	15
対象読者.....	16
CA SDM デフォルト ユーザ リスト	17
サーバ コンポーネント	18
 第 2 章: アップグレード	 31
CA SDM アップグレードの計画方法	31
データベースに関する考慮事項	33
ナレッジ マネジメント に関する考慮事項	38
DocType 検証.....	38
カスタマイズ内容の保持	39
LREL の移行に関する考慮事項	45
ステータス 遷移に関する考慮事項	47
電子メールのアップグレード	48
Migration Console の仕組み	51
マイグレーション ログ ファイル	52
手動によるマイグレーションの開始	52
前のリリースから CA CMDB をアップグレードする方法	53
64 ビット Linux/UNIX 上でデータを CA SDM r12.9 にマイグレートする方法	56
64 ビット Windows 上でデータを CA SDM r12.9 にマイグレートする方法	57
例: サポートされていない Windows 環境からのマイグレート	57
例: サポートされていない非 Windows 環境からのマイグレート	58
サポート オートメーション のデータのマイグレーション	59
サポート オートメーション データベースをマイグレートする方法	59
部門をテナントに変換する方法	61
CA サポート オートメーション データのエクスポート	62
サポート オートメーション データのインポート	64
マイグレーション後に サポート オートメーション 役割アクセスを設定する方法	65
カスタム CA Business Intelligence ユニバースのマイグレート方法	65
カスタム ユニバースのバックアップ方法	66
CA Business Intelligence ユニバースのインストール	66
ユニバース リンクの更新	67
アップグレード後の構成	67

プライマリまたはセカンダリ以外のサーバの非アクティブ化	68
EEM 8.4 サーバを使用する既存のユーザのサポート	68
CA Workflow と CA EEM のアップグレード方法	68
サーバプロセス設定の保持	69
CA SDM および CA IT PAM 統合の有効化	70
Web エンジンおよびブラウザ キャッシュのクリア	70
WebDirector およびサーバの設定	71
LREL マイグレーションの後	71
アクセス タイプの編集	75
優先順位計算の有効化	76
インシデントに [インシデントの優先度] フィールドを追加する方法	77
従業員チケットへの [緊急度] フィールドの追加	78
セルフサービス ユーザ用にチケットの値を設定する方法	78
ステータス移行のアクティブ化	82
移行タイプのアクティブ化	83
機能アクセス領域のカスタマイズ	84
SITEMODS.JS ファイル	86
アクセス タイプの調整	86
データ パーティション設定の調節	87
役割のマイグレート後のヘルプセットの変更	88
デフォルトの制約設定	89
IIS Web インターフェース (CAisd) の開始	90
カスタマイズした HTML フォームの変更	90
ナレッジマネジメントを r11.2 からアップグレードする方法	91
CA SDM r12.x から ナレッジマネジメントをアップグレードする方法	94

第 3 章: 計画 97

CA SDM デフォルトおよび推奨ポート リスト	97
高可用性を計画する方法	100
高可用性のための CA SDM アーキテクチャ	102
高可用性設定を選択する条件	104
高可用性設定の考慮事項	105
CA MDB のインストールの計画	114
CA MDB に関する考慮事項	115
CA SDM のインストールの計画	118
CA SDM に関する考慮事項	122
CA NSM のインストール計画	135
CA EEM と CA Workflow のインストール計画	135
CA EEM に関する考慮事項	137

CA Workflow に関する考慮事項.....	138
CA Process Automation インテグレーションの計画	144
セキュリティに関する考慮事項.....	145
CA Process Automation との SSL 通信をセットアップする方法	145
CA Business Intelligence のインストール計画	149
レポートの考慮事項.....	151
レポートのベスト プラクティス	155
実装方針.....	155
Firefox での Windows 認証の有効化.....	156

第 4 章: インストール 159

ソフトウェアの実装方法.....	159
CA SDM サーバの設定方法	161
プライマリ サーバの設定	163
サーバの追加.....	163
セカンダリ サーバの設定	165
バックグラウンド サーバの設定	165
スタンバイまたはアプリケーション サーバの設定	166
サーバの詳細の確認.....	168
標準設定から高可用性設定に変換する方法	169
すべてのセカンダリ サーバの非アクティブ化	170
バックグラウンド サーバの設定	170
セカンダリ サーバのタイプの変更	171
スタンバイ サーバおよびアプリケーション サーバの設定	172
サーバの詳細の確認.....	174
高可用性設定から標準設定に変換する方法	175
前提条件を確認します。	176
すべてのアプリケーション サーバおよびスタンバイ サーバの非アクティブ化.....	176
プライマリ サーバの設定	177
サーバの詳細の確認.....	178
セカンダリ サーバの設定	178
サーバの詳細の確認.....	179
CA MDB をインストールする方法.....	179
MDB のインストール	180
製品の統合と互換性の情報の特定	180
SQL Server へのインストール (Windows)	181
Oracle でのインストール (Windows)	183
Oracle へのインストール (Linux/UNIX)	186
リモート MDB の HP-UX へのインストール	188

CA SDM をインストールする方法	188
Oracle 環境変数	190
SQL Server へのインストール (Windows)	190
Oracle でのインストール (Windows)	193
Oracle へのインストール (Linux/UNIX)	198
Visualizer 設定	200
セカンダリ サーバ上に Visualizer を設定する方法	200
サポート オートメーション コンポーネントの設定	201
Web Screen Painter をインストールする方法	207
CA SDM と CA NSM の統合をインストールおよび設定する方法	208
統合に関する考慮事項の確認	210
CA NSM 統合コンポーネントのインストール	211
CA SDM Event Converter	214
統合後の考慮事項の確認	215
CA NSM 統合の確認	216
CA NSM 統合のトラブルシューティング	246
CA NSM 統合の使用	253
CA EEM をインストールする方法	262
CA EEM のインストール (Windows)	263
CA EEM SDK の FIPS 準拠モード設定	265
CA EEM のインストール (UNIX)	265
CA Workflow をインストールする方法	266
CA Workflow のインストール (Windows)	267
CA Workflow のインストール (UNIX)	268
スタンドアロン CA Workflow IDE のインストール	269
CA Workflow IDE クライアントのアンインストール (Windows および Linux)	271
CA Business Intelligence for CA SDM をインストールする方法	272
CA Business Intelligence のインストールの計画	273
CA Business Intelligence のインストール	274
CA Business Intelligence のインストールの確認	275
インストールの確認	276
インストール ログ	277

第 5 章: 環境設定 279

製品の設定	279
CA SDM コンポーネントの設定	280
CA CMDB 監査ログのセットアップ	282
CA Cohesion ACM と CA CMDB の統合方法	282
AIX 上の CA CMDB Visualizer 設定	282

CA CMDB との互換性のためのサードパーティ スクリプトの変更	283
CA CMDB レポートのターゲット サーバを切り替える方法	284
Web インターフェースの設定方法	284
Web エンジンまたは WebDirector の追加	285
Web インターフェースの設定	289
Web インターフェースの開始	290
CA Business Intelligence for CA SDM を実装する方法	291
前提条件の確認	293
CA Business Intelligence の設定	293
レポートの確認	313
統合 Windows 認証を CA SDM 用に設定する方法	314
前提条件の確認	315
IWA 用の IIS の設定	316
IWA 用の CA SDM の設定	317
IWA のテスト	318
自動ポリシーの実行	319
ナレッジ レポート カードの実行	320
ナレッジ マネジメント サンプル データのインポート	321
検索エンジンの設定	322
pdm_k_reindex- Knowledge Re-Index Utility	322
Crawler Surface 用の Domserver を設定するための新しいタグ	324
CA Workflow の構成方法	324
CA Workflow の開始と停止	325
自動ログイン（外部認証）のセットアップ	329
自動ログイン用のワーク リストおよびワークフロー マネージャの設定	331
自動ログイン用のワークフロー デザイン環境の設定	332
CA Workflow オプション	333
問題管理サンプル ワークフローの設定方法	334
PC の注文サンプル ワークフローの設定方法	336
変更管理プロセス定義の例	338
CA Process Automation ワークフロー インテグレーションの設定方法	342
CA Process Automation および CA SDM インストールの確認	343
CA Process Automation ワークフロー オプションの設定	343
CA Process Automation ユーザ管理	348
CA EEM を使用して CA SDM から CA Process Automation へのシングル サインオンをサポートす る方法	349
自動ログイン（CA MDB 認証）のセットアップ	351
単一エントリ ポイントの設定	353
マルチテナンシーを実装する方法	354
マルチ テナンシー	357

マルチテナンシーを実装する方法	362
Multi-Tenancy の有効化	377
テナント データのエクスポートおよびインポートの方法	387
マルチテナンシーで使用するユーティリティ	390
自動フェールオーバーを有効にする方法	400

第 6 章: カスタマイズ 405

第 7 章: カスタマイズの概要 407

認証モジュールを外部サーバに移動する方法	408
前提条件を確認します。	410
外部認証を使用するための CA SDM の設定	411
CA SDM サーバを再起動する方法	412
認証の確認	416
通知方法のカスタマイズ	416
通知プロセス	417
通知方法の変数	417
カスタマイズした通知方法を作成する方法	423
クエリとメッセージのカスタマイズ	426
スコアボード クエリ	427
ITIL 固有のクエリ	434
アクティビティ通知メッセージのカスタマイズ	435
Web インターフェースのカスタマイズ	443
Web Screen Painter を使用してスキーマをカスタマイズする方法	444
Web Screen Painter を使用して Web インターフェースをカスタマイズする方法	465

第 8 章: リストフォーム上のデータグリッドリストの変更 487

HTML テンプレート (HTML フォーム)	493
HTML タグ	499
サーバの変数	526
サポートされているサーバ操作	533
高度なカスタマイズ	543

第 9 章: イベント ログ データ保存カスタマイズ 577

CA Business Intelligence レポートのカスタマイズ	580
CA Business Intelligence インフラストラクチャ	580
開発環境	582

フレームワーク	584
インフラストラクチャへのスキーマ変更	587
レポートおよびフォルダ構造	591
新規 Crystal レポートの CA Business Intelligence への移動	596
既存の Access レポートを CA Business Intelligence に移動させる方法	598
開発から実稼働への移動	598
レガシー レポートのカスタマイズ	599
カスタム レポートのデザイン	600
レポートの生成方法	610
レポート テンプレートの参照	612
Crystal レポートのカスタマイズ	628

第 10 章: CA CMDB の入力 631

データベースへの入力	631
GRLoader によるデータベースへの入力方法	631
GRLoader を使用したデータのインポート	632
ファミリとクラスの割り当て	633
CA APM データのロード方法	633

第 11 章: MDR ランチャの使用 635

MDR ランチャ	636
MDR 用語	637
MDR マッピング	639
MDR 起動	639
CMDBf ビューア	639
CA CMDB で MDR を定義する	640
MDR URL の定義	645
MDR 起動 URL	646
URL 置換のパラメータ	648
GRLoader を使用した統一	650
CI の統一	651
GRLoader を使用して 1 つの CI に複数の MDR を定義する	652
MDR CI と CA CMDB CI 間のマップ	652
CMDBf ビューア用の MDR の設定方法	654
MDR Web ブラウザ インターフェースの起動	654
CA Cohesion 統合	655

第 12 章: Web サービスの管理

657

Web サービスの管理	657
CA SDM コンポーネント	658
SOAP Web サービス クライアントに関するヒント	658
Java クライアント	659
SOAP Web Services Configuration	661
Web サービスの再展開	662
Web サービスのセキュリティ	663
SOAP エラー処理	666
ロック エラー	667
タイムアウト	667
エラー コード	668
Web サービスのインストール	670
設計時の機能をアクティブにする方法	670
外部仕様	671
ユーザ アクセス認証	671
ユーザ名/パスワード認証	672
パブリック キー インフラストラクチャ (PKI) 認証	673
セッションおよび権限	680
アクセス コントロール/管理	681
オブジェクト	693
システムの更新とキャッシュ	695
カテゴリおよびプロパティ	696
XML オブジェクトの戻り値	697
ITIL 方式	699
インシデント/問題作成	699
インシデント/問題のクエリ	700
問題へのインシデントの添付	701
変更要求への問題の添付	701
設定項目	701
Web サービスの利用	702
ログイン	702
共通タスクを実行する方法	702
REST と SOAP	707
REST セキュリティ	707
Web サービス オプション	709

第 13 章: その他の製品の統合 711

CA Workflow インテグレーション	711
CA Workflow のコンポーネント	712
CA Workflow へのアクセス	715
CA Portal インテグレーション	717
CA SDM Web インターフェースのアクセシビリティの確認	718
CA Portal のインストールと起動	718
CA Portal で SSL を使用するための CA SDM の設定	720
メインフレーム製品のインテグレーション	725
CA SDM 側のデータのロード	725
CAISDI を現在使用している CA 製品	725
CAISDI の使用を予定している CA 製品	727
CA Business Service Insight 統合	728
CA SDM での CA BSI 情報の表示	729

第 14 章: samples ディレクトリ 735

samples ディレクトリのコンテンツ	735
メッセージカタログを変更する方法	735
call_mgt	736
data	737
macro_lock	737
multi-tenancy	737
pdmconf	738
reporting	738
sdk	739
views	739

第 15 章: 補足コンテンツのロード 741

sd_content.dat	741

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。

[概要](#) (P. 15)

[対象読者](#) (P. 16)

[CA SDM デフォルト ユーザ リスト](#) (P. 17)

[サーバ コンポーネント](#) (P. 18)

概要

このマニュアルには、企業で **CA SDM** を正しく実装するために必要な情報が記載されています。主な内容として、以下の作業方法についての説明があります。

- 新規インストールとアップグレード両方の計画と準備
- 必要な製品コンポーネントすべてのインストールとアップグレード
- 製品コンポーネントの設定
- その他の **CA Technologies** 製品との統合

注: このマニュアルでは、一部の **CA Technologies** 製品との統合の詳細は説明しません。このマニュアルで説明しない **CA SDM** の統合の詳細については、<http://ca.com/jp/support> の「**CA Unicenter Service Desk** 統合化グリーンブック」を参照してください。

注: システム要件を含む最新のリリース ノート、およびオプションの **readme** ファイル（ある場合）は、<http://ca.com/support> で参照できます。

対象読者

このマニュアルは、CA SDM のインストール方法、アップグレード方法、および構成方法について理解する必要のあるユーザを対象としています。このマニュアルに記載の情報を使用すると、以下のユーザが特定のタスクを実行できます。

- システム管理者と管理者：このマニュアルに記載の情報およびオペレーティングシステムに関する自身の知識を活用して、初めて製品のインストールを実行したり、製品バージョンをアップグレードしたり、実装要件に基づいて製品を構成したりできます。
- インテグレータ：このマニュアルに記載の情報および CA Technologies 製品に関する自身の知識を活用して、CA SDM を一部の CA Technologies 製品と統合できます。

注：このマニュアルでは、一部の CA Technologies 製品との統合の詳細は説明しません。このマニュアルで説明しない CA SDM の統合の詳細については、<http://ca.com/jp/support> の「CA Unicenter Service Desk 統合化グリーンブック」を参照してください。

- ユーザ：必要な場合にはこのガイド内の情報を使用して、製品とコンポーネントをインストールできます。

このガイド内の情報を使用するには、以下が必要となります。

- 現在の実稼動環境に応じた、Windows や UNIX オペレーティングシステムに関する実務上の知識
- オペレーティングシステムの基本的な管理タスクを実行する能力
- また、動作環境によっては、メインフレーム、モバイルデバイス、およびサーバのインストールにも精通している必要があります。

注：このマニュアル全体を通して、NX_ROOT について言及されています。NX_ROOT とは、CA SDM のインストールパスが格納されている環境変数のことです。この NX_ROOT 変数は、CA SDM の環境変数の設定に使用する NX.env 環境設定ファイルに設定されています。

NX_ROOT の定義の例

@NX_ROOT=C:\Program Files\CA\Service Desk Manager

CA SDM デフォルト ユーザ リスト

以下のリストは、標準的な CA SDM 実装におけるデフォルト ユーザ情報を示しています。

OS	製品	デフォルト ユーザ名	OS レベルか?	作成方法
Windows	CA SDM	ServiceDesk	○	自動
	CA EEM	EiamAdmin		デフォルトのパスワード : EiamAdmin
	CA MDB SQL Server	ServiceDesk	×	環境設定時に MDB 内に作成
	CA MDB Oracle	mdbadmin	×	環境設定時に MDB 内に作成
UNIX	CA SDM	srvcdesk	○	手動で作成
	CA MDB Oracle	mdbadmin	×	環境設定時に MDB 内に作成
Linux	CA SDM	srvcdesk	○	手動で作成
	CA MDB Oracle	mdbadmin	×	環境設定時に MDB 内に作成

サーバコンポーネント

CA SDM には、CA SDM の設定に応じて、異なるサーバ上で連携して動作するコンポーネントがあります。実装を開始する前に、以下のコンポーネントについての基本的知識を理解しておく必要があります。

Daemon Manager (pdm_d_mgr)

起動ファイル `pdm_startup` 内の定義に従ってプロセスセットを開始します。Daemon Manager は、失敗したコンポーネントの開始をデフォルトで最大 10 回試行します。すべての CA SDM コンポーネントのステータスを確認するには、`pdm_status` ユーティリティを使用します。`pdm_d_refresh` ユーティリティを使用すると、失敗としてマーク済みのプロセスをもう 1 サイクル（新たに 10 回）試行するように Daemon Manager に指示できます。

デーモンマネージャは、すべての CA SDM サーバ上で実行されます。

Message Dispatcher (sslump_nxd)

共通バスまたはメッセージ受け渡しシステムとして機能します。相互通信が必要なコンポーネントは、最初に Message Dispatcher に登録されます。Message Dispatcher は、コンポーネントからメッセージが送信されると、そのタイプのメッセージを受信するように登録されているコンポーネントにそのメッセージを配信します。2 つのコンポーネントの通信頻度が高く、Message Dispatcher によるメッセージの受け渡しが非効率な場合は、それらのコンポーネント間に高速チャネルが作成されます。登録されているコンポーネントのリストは、`slstat` ユーティリティを使用して確認できます。

メッセージディスパッチャは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ。

Database Agent (platform_agent)

データベースに対して SQL クエリを実行します。Database Agent は、CA SDM の論理スキーマに従って、該当レベルの SQL を物理データベース プラットフォームの SQL に変換します。

注: Database Agent は、一時的な切断および失敗したクエリを検出し、データベースとの再接続と通信を試行します。このコンポーネントは、短時間のネットワーク障害や一時的な切断など、短期サービス中断のみを対象としています。保守時のデータベースサービスのシャットダウンなど、長期サービス中断向けではありません。Database Agent は、定義された回数 (デフォルトでは 3 回) だけ、数分間のみ接続を再試行します。サービスの中断が数分以上続く場合は、接続試行を停止します。この場合、データベースが再び使用可能になったら、CA SDM を再起動する必要があります。

データベース エージェントは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準: プライマリ サーバ。
- 高可用性: すべてのサーバ。

Agent Provider (platform_prov_nxd)

Database Agent を開始または停止します。多数の Database Agent がデフォルトで実行されています。多数のデータベース クエリの処理のために Database Agent の数を増やす必要がある場合、Agent Provider は Database Agent を開始します。必要な Database Agent の数が減ったら、Agent Provider は不要な Database Agent を終了します。

エージェントプロバイダは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準: プライマリ サーバ。
- 高可用性: すべてのサーバ。

Virtual Database (bpvrtddb_srvr)

複数のオブジェクト マネージャの操作を有効にします。プライマリ サーバまたはセカンダリ サーバで実行されているすべてのオブジェクト マネージャが **Virtual Database** に接続し、**Virtual Database** が仲介となって **Database Agent** へのそれぞれのアクセスを制御します。たとえば、新しい範囲のチケット参照番号を取得するとき、**Virtual Database** は一度に 1 つのオブジェクト マネージャだけが参照番号を含むテーブルにアクセスするように制御できます。**Virtual Database** は、オブジェクト マネージャに対してデータベース情報のキャッシングも実行します。

仮想データベースは、**CA SDM** の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリ サーバ。
- 高可用性：すべてのサーバ

Continuous Archive and Purge (arcpur_srvr)

CA SDM 管理者の構成に従って、アーカイブとパージのルールを実行します。

アーカイブとパージの常時実行は、**CA SDM** の設定に応じて、以下のサーバ上で実行されます。

- 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

Database Monitor (dbmonitor_nxd)

CA MDB 内の共通テーブル（たとえば、*ca_contact*）の変更を監視します。

データベース監視は、**CA SDM** の設定に応じて、以下のサーバ上で実行されます。

- 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 Daemon (pdm_mail_nxd)

送信電子メール通知を送信します。

メールデーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリ サーバ
- 高可用性：すべてのサーバ。

Mail Eater (pdm_maileater_nxd)

チケットの作成と更新に関する受信電子メールを受け入れます。

Mail Eater デーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

Notification Manager (bpnotify_nxd)

Windows 環境で通知を管理します。通知マネージャは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリ サーバ。
- 高可用性：アプリケーション サーバ、バックグラウンド サーバ、およびスタンバイ サーバ。

Spell Checker (lexagent_nxd)

クライアントからのリクエストに従ってスペルチェックを実行します。スペルチェッカは、すべての CA SDM サーバ上で実行されます。

Text API Daemon (pdm_text_nxd)

コマンドラインや電子メールなどの外部インターフェースを使用してチケットを作成および更新します。Text API デーモンは、すべての CA SDM サーバ上で実行されます。

Timed Event (animator_nxd)

延期イベントを実行します。多くのサービス タイプまたはサービス契約を使用する実装では、**Timed Event** エンジンで追跡する必要があります。アクティブなイベントが多数存在する場合があります。このような場合、プライマリ サーバのオブジェクト マネージャを完全に **Timed Event** エンジン専用として使用する必要があります。必要に応じて、プライマリ サーバまたはセカンダリ サーバのほかのオブジェクト マネージャを製品へのアクセス用に構成できます。

Timed Event デーモンは、**CA SDM** の設定に応じて、以下のサーバ上で実行されます。

- 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

Time-To-Violation (ttv_nxd)

サービス タイプの予測違反時間を計算します。違反までの時間 (**Time-To-Violation**) デーモンは、**CA SDM** の設定に応じて、以下のサーバ上で実行されます。

- 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

Proctor Daemon (pdm_proctor_nxd)

(Windows のみ) プライマリ サーバおよびセカンダリ サーバで、デーモン マネージャの指示に従って **CA SDM** コンポーネントを起動および再起動します。セカンダリ サーバをインストールするときに、**pdm_proctor_nxd** プロセスが **CA SDM Remote Daemon Proctor** サービスとしてインストールされます。プライマリ サーバを起動すると、**Daemon Manager** は **Remote Daemon Proctor** に対して、**Message Dispatcher** に接続するように指示します。その後、デーモン マネージャは **Remote Daemon Proctor** に対して、起動ファイル **pdm_startup** のプロセス セットで定義されているコンポーネントをセカンダリ サーバで開始するように指示します。**Proctor** デーモンは、高可用性設定ではすべての **CA SDM** サーバ上で実行されます。

Object Manager (domsrvr)

CA SDM のサーバプロセスとして機能します。プライマリ サーバをインストールすると、デフォルトで 2 つのオブジェクト マネージャがインストールされます。1 つは製品への接続用、もう 1 つは Web Screen Painter 専用です。これにより、本番稼動環境に影響を及ぼすことなく、変更をテストできます。セカンダリ サーバをインストールするときに、追加のオブジェクト マネージャを構成できます。

Timed Event エンジンなどのクライアントが接続するプライマリサーバでは、必ずデフォルトのオブジェクト マネージャが実行されている必要があります。

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。

pdm_userload を使用してこれらのレコードを操作する場合には、*pdm_cache_refresh* ユーティリティを使用してオブジェクト マネージャに新しいデータを取得させることもできます。オブジェクト マネージャは、高可用性設定ではすべての CA SDM サーバ上で実行されます。

Method Engine (spel_srvr)

オブジェクト マネージャの SPEL コード、イベント、マクロなどを実行します。すべてのオブジェクト マネージャをそれぞれ独自のメソッドエンジンで実行することをお勧めします。

メソッドエンジンは、すべての CA SDM サーバ上で実行されます。

Login Server (boplogin)

認証されたユーザ セッションを管理します。

ログインサーバは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリ サーバ
- 高可用性：すべてのサーバ

LDAP Virtual Database (ldap_virtddb)

LDAP ディレクトリとやり取りします。メソッドエンジンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリまたはセカンダリ サーバ
- 高可用性：バックグラウンドまたはアプリケーション サーバ

ナレッジ マネジメント Search Daemon (bpebr_nxd)

ナレッジ ベース検索を実行します。CA SDM の開始時に、bpebr_nxd デーモンはデータベース内のナレッジ ドキュメント データをメモリにキャッシュします。ドキュメント ベースの規模が大きい場合は、メモリ リソースの問題が発生する可能性があります。bpebr_nxd デーモンのサイズ要件は、以下のとおりです。

ナレッジ マネジメント 検索

- 100,000 ドキュメント
- メモリ サイズ = 332,000 KB

ナレッジ マネジメント デーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

ナレッジ マネジメント/Keyword Indexing Daemon (bpeid_nxd)

ナレッジ ベースにインデックスを作成します。

キーワードインデックス作成デーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

ナレッジ マネジメント FAQ Ratings Daemon (bu_daemon)

ナレッジ マネジメント の FAQ 評価を計算します。これは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

Knowledge Report Card Daemon (krc_daemon)

ナレッジマネジメントのナレッジレポートカード (KRC) 機能の計算を実行します。アナリストやマネージャは、この機能を使用して、各自のナレッジ貢献度を各種マトリックスビューで表示したり、どの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を提供できます。提供される情報は、ナレッジドキュメントの作成プロセスを向上し、カスタマに最高のサポートを提供するために、さまざまな方法で使用できます。

ナレッジレポートカードデーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

ナレッジ マネジメント Daemon (kt_daemon)

ナレッジベース管理およびナレッジ管理ロジックを管理します。また、通知とドキュメント承認プロセスも管理します。ナレッジマネジメントデーモンは、すべての CA SDM サーバ上で実行されます。

Repository Daemon (rep_daemon)

CA SDM と ナレッジ マネジメント/Keyword Search Daemon の添付ファイルリポジトリを管理します。リポジトリデーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリまたはセカンダリ サーバ
- 高可用性：すべてのサーバ。

Version Control Daemon (pdm_ver_nxd)

プライマリサーバとセカンダリサーバ間のスキーマファイルを同期して、両方のサーバで同じスキーマが使用されるようにします。バージョン管理デーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

Apache Tomcat Web Server (javaw)

Microsoft Internet Information Server (IIS) を CA SDM へのアクセス用 Web サーバとして使用しているかどうかにかかわらず、特定の機能を実装できるようにします。対象となる機能には、CA Workflow、グラフ項目、添付ファイル、および Web サービスがあります。

Apache Tomcat Web サーバは、Apache Tomcat コントローラ (*pdm_tomcat_nxd*) を使用して管理できます。Apache Tomcat Web サーバは、すべての CA SDM サーバ上で実行されます。

Web Engine (webengine)

Microsoft IIS または Apache Tomcat Web サーバで実行されている *pdmweb.cgi* を使用して Web ブラウザに接続します。CA SDM の設定に応じて、以下のサーバ上で WSP のために少なくとも 1 つの Web エンジンが存在する必要があります。

標準：プライマリ サーバ

高可用性：アプリケーション サーバ、スタンバイ サーバ、およびバックグラウンドサーバ

このプロセスによって、WSP スキーマデザイナーがスキーマファイルを実際に書き込めるようになります。Web エンジンには、製品にアクセスするために Web ブラウザで使われる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。Web エンジンには、すべての CA SDM サーバ上で実行されます。

RF Broker (pdm_rfbroker_nxd)

(高可用性設定にのみ適用可能)。サーバの役割を管理し、それを設定全体にわたって制御します。このデーモンは、高可用性設定ではすべてのサーバ上で実行されます。バックグラウンドおよびスタンバイサーバに関する情報を取得したり、

ServerStatusMonitor クラス内の情報 (Slump ID、ノード名、サーバタイプなど) の更新を行います。サーバステータス変更や休止リクエストのブロードキャストメッセージを受信し、障害が発生したノードがバックグラウンドサーバであるときに

ServerStatusMonitor オブジェクトに転送する **SLUMP_NODE_GONE** メッセージに登録します。このデーモンは、標準設定には適用できません。

Login User Authentication (bopauth_nxd)

[システム ログイン名] フィールドを使用してオペレーティングシステムのユーザアカウントの検証および連絡先レコードのロックアップを実行し、ユーザとアクセスタイプを一致させます。

自身のビジネスで **CA SDM** をほかのクライアントビジネス用に提供している場合は、1つのクライアントロケーションのセカンダリサーバ上にログインサーバを配置できます。その後、外部認証をアクセスタイプで有効にできます。これにより、自身のビジネスシステム上にクライアントのユーザアカウントを作成する必要がなくなります。これは、**CA SDM** の設定に応じて、以下のサーバ上で実行されます。

- 標準: プライマリまたはセカンダリ (設定されている場合) サーバ
- 高可用性: バックグラウンドまたはアプリケーション (設定されている場合) サーバ

Interval Logger (pdm_intrvlog_nxd)

システムをデバッグするためのデバッグ情報を収集します。これは、すべての **CA SDM** サーバ上で実行されます。

QRY KPI Daemon (kpi_qry_daemon)

SQL クエリを実行してデータベース内のキーパフォーマンスインジケータを更新します。**QRY KPI** デーモンは、**CA SDM** の設定に応じて、以下のサーバ上で実行されます。

- 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

SYS KPI Daemon (kpi_sys_daemon)

システム タイプのキー パフォーマンス インジケータを収集し、データベースに書き込みます。SYS KPI デーモンは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリ サーバ
- 高可用性：すべてのサーバ。

Confirm Database (confirm_db)

データベース アクセスを確認するためのユーティリティ。これは、すべての CA SDM サーバ上で実行されます。

Data Dictionary (ddictbuild)

データ辞書を作成するためのユーティリティ。これは、すべての CA SDM サーバ上で実行されます。

ログ ファイルの設定 (pdm_logfile)

ログ ファイル サイズの制限を表示または設定するためのユーティリティ。これは、すべての CA SDM サーバ上で実行されます。

Report Manager (pcrpt_nxd)

PC レポートのためのユーティリティ。これは、すべての CA SDM サーバ上で実行されます。

RPC Server (rpc_srvr)

アウトバウンド SOAP Web サービス コールを行うために使用されます。これは、すべての CA SDM サーバ上で実行されます。

CA SA Tomcat (sa_tomcat)

CA SA Tomcat は、サポート オートメーションを実行するために使用されます。任意の CA SDM サーバ上で設定されます。

CAWF Tomcat (cawf_tomcat)

CA ワークフローを実行するために使用される Tomcat インスタンス。任意の CA SDM サーバ上で設定できます。

Visualizer Tomcat (viz_tomcat)

Visualizer を実行するために使用される Tomcat インスタンス。CA SDM の設定に応じて、以下のサーバ上で設定できます。

- 標準：すべてのサーバ
- 高可用性：アプリケーション サーバ

Event Manager (ehm_nxd)

イベントマネージャは、CA NSM から来るイベントを管理します。イベントマネージャは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

ナレッジ マネジメント インデックス デーモン (bpeid_nxd)

ナレッジ ドキュメントのインデックス作成を行います。これは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 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

Registration Server (mdb_registration_nxd)

MDB 登録リクエストを処理するためのエージェント。登録サーバは、CA SDM の設定に応じて、以下のサーバ上で実行されます。

- 標準：プライマリ サーバ
- 高可用性：すべてのサーバ

第 2 章: アップグレード

このセクションには、以下のトピックが含まれています。

[CA SDM アップグレードの計画方法](#) (P. 31)

[Migration Console の仕組み](#) (P. 51)

[前のリリースから CA CMDB をアップグレードする方法](#) (P. 53)

[64 ビット Linux/UNIX 上でデータを CA SDM r12.9 にマイグレートする方法](#) (P. 56)

[64 ビット Windows 上でデータを CA SDM r12.9 にマイグレートする方法](#) (P. 57)

[例: サポートされていない Windows 環境からのマイグレート](#) (P. 57)

[例: サポートされていない非 Windows 環境からのマイグレート](#) (P. 58)

[サポート オートメーションのデータのマイグレーション](#) (P. 59)

[カスタム CA Business Intelligence ユニバースのマイグレート方法](#) (P. 65)

[アップグレード後の構成](#) (P. 67)

CA SDM アップグレードの計画方法

CA SDM アップグレードの計画に関する以下の考慮事項を確認します。

- CA SDM は、サポート対象のプラットフォームで、r11.2、r12.0、r12.1、r12.5、r12.6、r12.7 から r12.9 へのアップグレードをサポートしています。Windows の場合、r11.2、r12.0、r12.1、r12.5、r12.6、r12.7 から CA SDM r12.9 に直接アップグレードできます。
- CA SDM を Linux または UNIX 上にインストールしている場合は、r12.5 より前のバージョンから CA SDM r12.9 へのアップグレードには複数の手順が必要になります。インストールが古いバージョンの製品 (Linux/UNIX 上の r11.2、r12.0、r12.1 など) で実行されている場合は、<uskd> r12.9 の自動アップグレードスクリプトを実行する前に、CA SDM r12.5 の自動アップグレードスクリプトを実行し、CA SDM をサポート対象のプラットフォームおよびデータベースに移動する必要があります。カスタマイズがある場合は、r12.9 への最後の自動アップグレードスクリプトを実行した後に、それらのカスタマイズを 1 回だけ適用する必要があります。

- Unicenter Service Desk r6.0 や r11.1 など、これより前のバージョンの製品を使用している場合は、まず CA SDM r11.2 にアップグレードしてから CA SDM r12.9 にアップグレードする必要があります。
- マイグレーションの前に **NX.env** ファイルに変数を手動で追加した場合は、マイグレーションの完了後に変数を再度手動で追加します。
- CA SDM は ITIL のみをサポートします。非 ITIL システムからアップグレードした場合、CA SDM r12.9 インストールによって、現在の環境が ITIL 環境に更新されます。
- CA SDM r11.2 と CA SDM r11.1 の組み合わせをインストールしている場合は、CA SDM r12.9 に直接アップグレードすることはできません。まず CA CMDB を r11.2 にアップグレードしてから、r12.9 アップグレードを実行する必要があります。この処理によって、CA SDM r11.2 が r12.5 にアップグレードされ、CA CMDB r11.2 も r12.5 にアップグレードされます。CA CMDB r12.0 および r12.1 から CA SDM r12.9 に直接アップグレードすることもできます。

注: 以前のバージョンからのアップグレードの詳細については、「CA SDM 実装ガイド r11.2」を参照してください。アップグレードパッチやサポートが必要な場合は、弊社テクニカルサポートの Web サイト (<http://ca.com/jp/support>) をご覧ください。

- 現在のリリースの CA SDM にアップグレードする前に、以下のことを理解しておいてください。
 - [データベースに関する考慮事項](#) (P. 33)
 - [カスタマイズ内容の保持](#) (P. 39)
 - [LREL のマイグレーションに関する考慮事項](#) (P. 45)
 - [ステータス遷移に関する考慮事項](#) (P. 47)
 - [電子メールに関する考慮事項](#) (P. 48)
 - UTF-8 ロケールは Linux/UNIX プラットフォーム上にインストールする必要があります。
- CA SDM は、Linux/UNIX で、通知メールの送信処理に **smtp_mail** スクリプトを使用しなくなりました。以前からのユーザで **smtp_mail** を使用しており、最新リリースにアップグレードする場合は、CA SDM のメール通知機能を有効にするために、管理者がデフォルトのメールボックスの詳細ページを使用して、適切なメール オプションを設定する必要があります。

データベースに関する考慮事項

CA SDM r12.9 にアップグレードする前に、データベースに関する以下の情報に留意してください。

- 標準のデータベース バックアップ手順によって既存のデータベースをバックアップしてください。
- (すべての非 Windows マシンに該当) 以前のリリースの CA SDM が Oracle 10gr2 データベースと共に設定されている場合、CA SDM r12.9 にアップグレードする前に、Oracle 11gr2 クライアントをインストールしてください。

重要: アップグレード前に、\$NXROOT/NX.env ファイル内の Oracle ホームパスを oracle11g r2 クライアントのパスに変更してください。

- アップグレードすると、webLicenseCt KPI のすべてのバージョン (アクティブおよび非アクティブ) が使用できなくなり、関連する KPI データはすべて無効になります。これらのデータは依然として usp_kpi_data テーブルに残っていますが、レポート作成時に取得されません。OOTB KPI ルールの [KPI データ (システム)] (デフォルトでは非アクティブ) を実行することで、このデータを削除できます。

重要: この KPI ルールを実行することにより、他のシステム KPI によって収集されたデータもアーカイブされたりパージされたりするため、usp_kpi_data テーブルで提供されるデータを確認することをお勧めします。

注: 新しい KPI である webConcurrentTotalLicenseCt は、該当する期間中に CA SDM にログインしたユーザの数を一意に計算するために CA SDM r12.9 で使用されます。詳細については、「実装ガイド」を参照してください。

- 標準のアーカイブ手順によってインストール ディレクトリ (\$NX_ROOT) をアーカイブしてください。このアクションによって、データ移動の量が抑えられ、ディスク領域を節約できます。

- コマンドプロンプトから適切なスクリプトを実行してデータベースの重複レコードを識別してください。

注: このスクリプトはセカンダリ サーバで実行してください。SQL クエリ アナライザを使用してこのスクリプトを実行する場合は、SQLCHECK.SQL スクリプトを編集し、コマンドを実行する前に EXIT 引数を削除します。

- (Oracle) インストール メディアの ¥Migrate ディレクトリにある OracleCheckr12UniqueIndexes.sql を実行します。
- (SQL Server) [コマンドプロンプト] ウィンドウを開いて以下のとおり SQLCHECK.SQL を実行します。

```
cd $NX_ROOT¥samples¥views¥SQLServer
```

以下のコマンドを入力します。

```
Sqlcmd - E - e < SQLServer¥SQLCHECK.SQL
```

注: CA SDM r12.9 にアップグレードした後、これらのファイルはサーバ上の `$NX_ROOT/samples/views/SQLServer` または `$NX_ROOT/samples/views/Oracle` で見つけることができます。

重要: これらのスクリプトでは、重複レコードを識別できます。マイグレーションを続行する前に識別された重複レコードを削除します。

- Windows の場合、r11.2、r12.0、r12.1、r12.5、r12.6、および r12.7 から直接アップグレードできます。
- CA SDM を UNIX または Linux 上にインストールしている場合は、r12.5、r12.6、および r12.7 からアップグレードできます。
- サポートされていない UNIX/Linux オペレーティングシステムおよびデータベースにこれより前のバージョン (CA SDM r11.2、r12.0、r12.1 など) がインストールされている場合は、CA SDM r12.5 にアップグレードする必要があります。次に、アップグレードの前に、CA SDM をサポートされているオペレーティングシステムおよびデータベースに移動します。

- CA SDM r11.2 システムを、サポートされているデータベース（SQL Server および Oracle）にアップグレードします。

注: サポートされているデータベースの詳細については、「リリースノート」を参照してください。

- Unicenter Service Desk r11.0 から CA SDM r11.2 にアップグレードしてから、サポートされたデータベースへのデータのマイグレーションを実行します。
- 長いハイフンなどの特殊な Windows 文字を、Windows 以外のシステム上の CA SDM またはナレッジマネジメントに入力する場合、その文字はデータベースに正常に格納されません。
- Ingres - Ingres データベースを使用している場合は、アップグレードする前にデータを Oracle または SQL Server に変換します。

注: 変換方法については、データベースのドキュメントを参照してください。

- Oracle - Oracle では、構成アイテムの登録において、大文字と小文字を区別しないインデックスをサポートしません。Oracle へのマイグレーションを開始する前に、SQLPlus および Oracle DB がホスト名を使用して通信できることを確認してください。通信に失敗する場合は、Oracle がループバック アダプタを使用して構成されていないかを確認します。

注: Oracle データベースがインストールされたダブルバイト文字環境でマイグレートを行う場合は、オープンカーソルの上限数を 500 以上に増やしてください。詳細については、ORA-01000（ORA-01000 最大オープンカーソル数を超過しました）に関する Oracle のドキュメントを参照してください。

- SQL Server - SQL Server を使用している場合、現在のリリースの CA SDM にアップグレードするときは、設定済みデータベースのユーザ ID に対応するデフォルトのデータベースは CA MDB である必要があります。デフォルトのデータベースが CA MDB でない場合、Migration Console は失敗し、以下のメッセージが表示されます。

「テーブル *acctyp_v2* が MDB に存在しません」

- Tomcat - (Unicenter Service Desk r11.0、r11.1、または CA SDM r11.2) Tomcat を外部認証用に設定した場合、現在の製品リリースにアップグレードした後に Tomcat を外部認証用に再設定します。

- **テーブルの更新** - マイグレーション中に発生する以下のテーブル更新を考慮してください。
 - **ステータス テーブル** - 同じコード値がデータベース内に存在しない場合、このテーブルも適切なステータス レコードで更新されます。たとえば、*Cr_Status* はコード *AEUR* (エンド ユーザ応答待機中) で更新されます。
 - **機能領域** - マイグレーションの際、役割ごとに各 *usp_functional_access* レコードの行が自動的に追加されます。 マイグレーションにより、*usp_role* テーブルに含まれる各 CA SDM r12.0 および r12.1 機能領域のアクセス レベルが同じレベルに設定されます。新しい機能領域は、参照フィールドを使用してマップされます。
- **外部キー** - 以下の情報を考慮してください。
 - テーブル (プライマリ キーが **UUID** になっている) を参照する外部キー (SREL) は、整数タイプから **UUID** タイプ (または **BYTE 16**) に変更されます。

注: 外部キー値を使用して **SREL** 属性を設定する方法については、「*CA SDM テクニカル リファレンス ガイド*」を参照してください。
 - 古い CA SDM システムでデータを大量にロードするために外部キー制約を削除した場合は、アップグレードを実行する前に、忘れずに外部キー制約を再作成する必要があります。制約を削除するスクリプトは以下の場所にあります。
 - **Oracle**
`$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql`
 - **SQL Server**
`$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql`

注: *OracleAddConstraints.sql* か *SQLServer/SQLAddConstraints.sql* のいずれかの適切なスクリプトを実行することで、削除した制約を再度適用します。これらのスクリプトは制約削除スクリプトと同じディレクトリにあり、ファイル内に指示が記載されています。

- **MDB - MDB** により、多様な IT 管理データに対して一貫したデータベーススキーマを使用できます。MDB の開発中に、CA SDM 環境のデータエレメントがこのスキーマに組み込まれました。データエレメントのサイズが大きくなる可能性があるため、データベース全体のサイズも大きくなる可能性があります。

注: 標準データ要素が MDB 用に定義されている列幅を越えた場合、更新プロセスではこれらの要素内のデータが切り捨てられます。アップグレード時に切り捨てが行われると、アラートメッセージが表示されます。

- **分散化セットアップ - CA SDM の設定に応じて、サーバを以下のパターンでアップグレードすることをお勧めします。**

- **標準**

- プライマリ サーバ
- (オプション) 1つ以上のセカンダリ サーバ

- **高可用性**

- バックグラウンド サーバ
- 1つ以上のスタンバイ サーバ
- 1つ以上のアプリケーション サーバ

- **リモートデータベースのセットアップ** - 以下の情報を考慮してください。

新しい MDB を使用してデータベースサーバをアップグレードしてから、プライマリ サーバをアップグレードすることをお勧めします。データベースサーバがリモートの場合は、アップグレードを実行する前に、データベースサーバで CA MDB インストールを実行します。

- SQL Server の MDB データベースを使用している場合は、リモート MDB に接続する前に、クライアント コンピュータに `sqlcmd` がインストールされている必要があります。

ナレッジ マネジメント に関する考慮事項

CA SDM r12.9 にアップグレードする前に、以下のナレッジ マネジメント 情報に留意してアップグレードを実行してください。

- FAST ESP 検索エンジンを使用していた CA SDM の旧リリースからアップグレードする場合は、EBR 検索エンジンに変更する必要があります。FAST ESP ライセンスは、2013 年 5 月に有効期限が切れます。EBR 検索エンジンに変更するには、[オプションマネージャ]-[検索エンジン]をクリックし、`ebr_version` を編集して KT 検索エンジンを指定します。
- [CA SDM r11.2 から ナレッジ マネジメント をアップグレードする](#) (P. 91) 方法
- [CA SDM r12.x から ナレッジ マネジメント をアップグレードする](#) (P. 94) 方法

DocType 検証

CA SDM の旧リリースでは、`web.cfg` の `HtmlDoctype` プロパティで、HTML フォームから生成された HTML 用に以下の DocType を使用していました。

```
HtmlDoctype <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

`web.cfg` の `HtmlDoctype` プロパティは、CA SDM r12.9 では以下のように表示されます。

```
HtmlDoctype <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"  
"http://www.w3.org/TR/html4/frameset.dtd">
```

通常、この行は、ページの最初のリストに表示されます。

注: CA SDM r12.9 にアップグレードしたら、`HtmlDoctype` プロパティの値がカスタマイズしたフォーム内で変更されていることを確認してください。テキストエディタで `$NX_ROOT/bopcfg/www/wwwroot/html` ディレクトリから HTML ファイルを開き、DocType 値を検証できます。

カスタマイズ内容の保持

製品をカスタマイズしている場合は、CA SDM r12.9 にアップグレードする前に、以下の情報を考慮してください。

注: アップグレードが完了する前に **Migration Console** を閉じた場合、そ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。

- **カスタム レポート** - 前のバージョンでデータベース テーブルにアクセスするレポートをカスタマイズしていた場合、r12.9 では、データベース テーブルは新しい名前のテーブルに移動され、列名が変更されています。

注: データベース テーブルの詳細については、「**CA SDM テクニカルリファレンス ガイド**」を参照してください。

- **カスタマイズしたフォーム** - CA SDM r12.9 にアップグレードしても、CA SDM の旧リリースで行ったカスタマイズは保持されます。ただし、アップグレード後は、カスタマイズされたフォームで CA SDM r12.9 の機能を表示できません。
- **カスタマイズした管理ツリー** - Unicenter Service Desk r11.0 で管理ツリーをカスタマイズした場合、その変更はアップグレードされません。これは、役割ベースのユーザ インターフェースをサポートするためにアーキテクチャが変更されているためです。アップグレードされない管理ツリーのカスタマイズ内容には、新しいノードの追加、既存のノード名の変更、アクセス タイプの変更、またはほかのデータの変更が含まれます。カスタマイズを使用するには、以下の手順に従います。
 1. アップグレードを実行する前に、Unicenter Service Desk r11.0 の管理ツリーを確認し、アップグレード後に使用するカスタマイズ内容を書き留めます。
 2. アップグレードが完了した後、管理ツリーのカスタマイズ内容を適用する役割を識別します。
 3. カスタマイズ内容を、該当する CA SDM r12.9 の役割ベースの管理ツリーに適用します。
 4. 必要な機能が保持されていることを確認およびテストします。
- **カスタマイズしたフォーム上のボタン** - `/site/mods/html` 内のカスタマイズしたフォーム上のボタンのうち、コードの `msgtxt (n)` 部分が引用符で囲まれていないものは、アップグレード後、ボタン名の代わりにエラー メッセージが表示されます。

たとえば、`detail_cr.htmlpl` フォームで正しいボタン名を表示するには、`msgtxt(441)` を引用符を使用して以下のように変更します。

```
ImgBtnCreate("btnchg", "msgtext(441)", "detailSave('NEW_CHANGE')",  
true, 0, msgtext(440)); // Save and Create Change Order
```

- **カスタマイズ内容の保持**- CA SDM r12.9 の機能が必要で、カスタマイズ内容を前のバージョンから保持する場合は、r12.9 の機能が設定されている CA SDM r12.9 のベース フォームでカスタマイズをやり直します。

注: `acctypedtl.rpt` レポートと `acctypesum.rpt` レポートをカスタマイズしていた場合、CA SDM r12.9 の戻りデータは古くなります。

- **通知ルール** - 以前の CA SDM インストールからデフォルトのアクティビティ通知（[連絡先]、[オブジェクトの連絡先]、および[連絡先タイプ]）を削除している場合に、この機能を保持するには、マイグレーションを実行する前に、削除したデフォルトの連絡先を書き留めます。新しいバージョンにアップグレードした後、通知のデフォルトの連絡先を再度削除してください。
- **役割ベースの機能** - アップグレードを実行すると、役割ベースの機能に問題が生じる可能性があります。以下の情報について検討します。
 - 以下のフォームのうち、カスタマイズしたフォームは、CA SDM r12.9 の Web Screen Painter で読み取り専用として見なされます。また、これらのフォームには、カスタムコードを使用できる `xxx_site.htmlpl` バージョンが含まれます。
 - `ahdtop.htmlpl`
 - `menu_frames.htmlpl`
 - `reports.htmlpl`
 - `std_body.htmlpl`
 - `std_footer.htmlpl`
 - `std_head.htmlpl`
 - `styles.htmlpl`
 - `msg_cat.js`
 - `menu_frames_role.htmlpl`

- **カスタマイズした HTMPL ファイル** - 以下の情報を考慮してください。
 - アップグレード後も、カスタマイズしたすべての HTMPL ファイルはデフォルト メニュー バー設定を保持します。ポップアップ ウィンドウは、役割ベースのユーザ インターフェースの結果、主なページタブからのそのメニュー バーを継承します。アップグレード後は、カスタマイズした HTMPL ファイルは旧リリースのカスタマイズしたフォームでは使用できません。
 - CA SDM r12.9 では、旧リリースのカスタマイズされた HTMPL ファイルの一部が使用されません。マイグレーション スクリプトは、ファイルに *incompatible_for_r2_9* という拡張子を追加する perl スクリプト `$NX_ROOT/bin/migrate_to_r12_9_web_check.pl` を実行します。マイグレーションの完了後、`$NX_ROOT/site/web_check_files.txt` をテキスト エディタで開き、r12.9 で互換性のないフォームのリストを確認してください。
 - CA SDM の旧リリースの `list_dblocks.html` ファイルをカスタマイズした場合、このフォームは CA SDM r12.9 では正常に動作しません。`list_dblocks.html` がツリーの他の部分に表示されるように管理ツリーをカスタマイズした場合、そのカスタマイズはマイグレーション後に機能しません。新しい URL およびフォームを使用するようにフォームを手動で変更します。そのためには、[セキュリティと役割の管理]、[メニュー ツリー リソース] をクリックして [現在のロック] を開きます。以下の CA SDM r12.9 文字列でリソースを更新します。

```
OP=SEARCH+FACTORY=record_lock+QBE.NN.lock_time=NULL
```

- **外部キー** - アップグレード処理中、外部キーをリセットしようとしたときに参照整合性の問題が検出されると、`migration.log` ファイルにエラーが記録されます。関連付けられている外部キーには、事前定義済みの有効な参照が設定されます。
- **サーバおよび WebDirector の設定** - 以前のインストールが追加のサーバまたは WebDirector を使用するように設定されていた場合は、まず特定のサーバの設定を作成し、CA SDM サーバ設定ユーティリティ (`pdm_configure`) を実行する必要があります。設定の作成の詳細については、「管理ガイド」を参照してください。
- **CA サポート オートメーション 部署** - 部署をテナントにマイグレートする場合は、このデータを変換してから、CA SDM r12.9 内のサポート オートメーション を有効化および設定します。

カスタマイズした HTML フォームの名前の変更

CA SDM の旧リリースで HTML フォームをカスタマイズした場合、CA SDM r12.9 にアップグレードする前に、スクリプトを実行してその名前を変更します。このスクリプトは、すべての CA SDM サーバ上で実行します。
`migrate_to_r12_9_web_check.pl` スクリプトは、`site/mods` ディレクトリ内のカスタマイズされたすべての Web フォーム、スタイルシート、Java スクリプト、イメージ、およびマクロの名前を変更します。これらのファイルの名前を変更しておく、カスタマイズしたフォームを識別しやすくなります。

次の手順に従ってください:

1. コマンドプロンプトから、`pdm_perl`
`$NX_ROOT/bin/migrate_to_r12_9_web_check.pl` を実行します。
このスクリプトは、カスタマイズしたフォームに `incompatible_for_r12_9` という拡張子を追加します。
2. テキストエディタで `$NX_ROOT/bin/migrate_to_r12_9_web_check.pl` を開きます。
`r12.9` で互換性のないフォームのリストが表示されます。

注: このスクリプトは、CA SDM の旧リリースのようにバックアップフォルダのファイルを既存または `site/mods` ディレクトリに復元しません。

関連項目:

[カスタマイズ内容の保持](#) (P. 39)

ユーザ インターフェースのマイグレーションに関する考慮事項

CA SDM r12.9 にアップグレードする前に、ユーザ インターフェースのマイグレーションに関する以下の情報に留意してください。

- マイグレーションではフォームが自動的にバックアップされます。CA SDMr11.2、r12.0、r12.1、または r12.5 でカスタマイズされた HTMPL フォームを使用していた場合は、CA SDM r12.9 にアップグレードした後、それらを再度カスタマイズする必要があります。
- アップグレード後、ノートブック コントロールを含むすべてのカスタマイズされた HTMPL フォームを変更して、新しい Web マクロを追加し、適切なタブ グループ名を指定してください。WSP で、`<PDM_NOTEBOOK>` ステートメントを `<PDM_MACRO name=startNotebook>` に、`<PDM_TAB>` ステートメントを `<PDM_MACRO name=TAB>` に変更します。

関連項目：

[リスト フォーム上のデータ グリッド リストの変更](#) (P. 487)

[詳細フォーム上のノートブックの変更](#) (P. 489)

copy_inactive Web オプション

新しい CA SDM r12.9 では、オプション マネージャで `copy_inactive web` オプションがインストールされません。このため、非アクティブ オブジェクトへのリンクはコピーされません。CA SDM r12.5 または r12.6 からアップグレードする場合、マイグレーションによってこのオプションがインストールされるので、非アクティブオブジェクトへのリンクがコピーされます。

`copy_inactive` オプションをインストールしない場合は、以下の情報に留意してください。

- CA SDM は、非アクティブ オブジェクトを指し示す SREL をコピーしません（SREL が必須の場合を除く）。

たとえば、`org1` という組織に非アクティブなロケーションがあるとします。この場合、`org1` をコピーすると、新しい組織にはロケーションがありません。しかし、SREL が必要な場合、CA SDM はこのルールを無視してロケーションをコピーします。たとえば、CA SDM はルールを無視し、非アクティブ クラスを持つ CI をコピーできます。

- CA SDM は、LREL（多対多）関係を非アクティブ オブジェクトにコピーしません。

たとえば、`CITest1` という CI が、非アクティブな組織 `org2` に関連付けられているとします。この場合、`CITest1` をコピーすると、`org2` は新しい CI にリンクされません。

重要：これらのルールは、チケットをテンプレートから作成した場合でも、チケットをコピーするときに適用されます。`copy_inactive` をインストールしたかどうかに関係なく、このルールの例外は非アクティブ領域およびカテゴリです。これらは、既存のチケットからコピーされず、テンプレートから入力されません。

LREL の移行に関する考慮事項

List Relationship (LREL) は、2 つのオブジェクト間の関連付けを表します。LREL には左側 (lhs) と右側 (rhs) の関係があります。関係の各側は、データ関係が含まれた **Majic** オブジェクトの属性です。

本製品の以前のリリースでは、**.maj** LREL ステートメントおよびオブジェクトで、多対多の DBMS データ関係を説明していました。現在は、多対多関係に LREL Majic ステートメントを使用しません。代わりに、各テーブルに関係の両側が格納されます。オブジェクトは、標準的な BREL ステートメントで関係にアクセスします。たとえば、変更要求と CI の関係を把握するには、新しい **usp_lrel_asset_chgnr** テーブルおよび対応する **lrel_asset_chgnr** オブジェクト内を確認します。

LREL の変更点によって、データベース内に属性名を格納しなくてもよくなります。関係の 2 つの側は、結合とインデックス作成が容易な外部キーの単一関係 (SREL) です。必要に応じて、関係に追加の関係属性を含めることができます。

アップグレード中、LREL テーブルデータが **r12.9** にマイグレートされる際に、以下のアクティビティが発生します。

- システムによって、LREL 関係のあるテーブルおよびオブジェクトが <rellevel> テーブルおよびオブジェクトに自動的にマイグレートされます。
- 新規テーブル名は、**usp_lrel_lhsName_rhsName** 形式を使用して付けられます。
たとえば、**usp_lrel_asset_chgnr** テーブルは、アセットと左側の関係を、変更要求と右側の関係を持っています。
- 対応するオブジェクト名は、**lrel_lhsName_rhsName** 形式を使用して付けられます。
たとえば、**lrel_asset_chgnr** オブジェクトは、**usp_lrel_asset_chgnr** テーブルに対応します。
- データベース制限により、一部の名前が短縮されます。
- データは古いテーブルから **r12.9** テーブルにマイグレートされ、すべての CA SDM コードはこれらのテーブルを使用するように変更されます。
- システムでは、**bmlrel** などの古い LREL データベース テーブルを使用しなくなります。ただし、参考用に、古いテーブルにはデータが保持されます。

- 新規オブジェクトへの後方関係（BREL）属性によって、それぞれに関連する Majic オブジェクト定義内の元の LREL 属性が置き換えられます。
- `CreateLrelRelationship()` Web サービス メソッドなどのサポートされた API を使用している場合、コードは期待どおりに動作します。
- LREL スタイルのカスタム関係を追加している場合は、CA SDM によって r12.9 テーブルにマイグレートされます。
- 古い LREL テーブルに直接アクセスする、サイト定義のコードまたはレポートは、システムでそれらのテーブルを使用しなくなるため、古いデータで動作します。コードとレポートが正常に動作するように、r12.9 テーブルを使用するようコードを更新することをお勧めします。

重要: コードがレガシー LREL オブジェクトまたはテーブルに直接アクセスする場合は、マイグレーション後コードは動作に失敗します。マイグレーションの前にコードを更新することをお勧めします。たとえば、コードで Majic ステートメントを使用して、LREL 関係を確立している場合、直接テーブルに値を挿入するのではなく、`createLrelRelationships()` メソッドを使用します。

注: サイト定義のコードやレポートが、データベースに直接アクセスしていたり、lrel1 オブジェクトなどのレガシー LREL Majic オブジェクトを処理したりしている場合は、それらが正常に動作しているかどうかを確認するようお勧めします。コードを更新して、Web サービスなどのサポートされたインターフェースを使用できます。また、必要なテーブル名も更新します。レポートの場合は、新しい DBMS テーブル参照でクエリを更新できます。

ステータス遷移に関する考慮事項

CA SDM r11.2、r12.1、および r12.1 から CA SDM r12.9 にアップグレードした後、ステータス遷移を使用する場合は、以下の情報に留意します。

- r12.9 にアップグレードしたとき、ステータス遷移は非アクティブになっています。

注: チケット形式上で表示されるカスタマイズ済みステータス コードの説明は、すべてアップグレード処理中も保持されます。

- アップグレード後、*Status_Policy_Violations* オプションがインストールされ、デフォルトで「Warn」に設定されます。この設定によって、未定語の遷移が可能になりますが、警告がログに記録されます。
- オプションを「Allow」に設定した場合は、未定義のトランザクションは記録されません。

注: *Status_Policy_Violations* 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。

電子メールのアップグレード

CA SDM では、[オプション マネージャ] - [電子メール] 受信メール オプションが、対応するオプションを提供する [メールボックス]

(*usp_mailbox* テーブル) に置き換わっています。[電子メール] 送信メール オプションは、これまでどおり [オプション マネージャ] にあります。アップグレードの際、CA SDM では、CA SDM r12.9 で提供されるデフォルトの [メールボックス] 設定の代わりに既存の電子メール設定を使用して、メールボックスを設定します。各電子メール オプションは、EMAIL_ATTACHMENT_DIR を除いて (不要になりました)、*usp_mailbox* テーブル内のオプションにマップされます。設定されていないオプションは、テーブル内では NULL に設定されます。

注: デフォルト メールボックスのアクティブ化およびメールボックス オプションの使用法の詳細については、「管理ガイド」およびオンラインヘルプを参照してください。

以下の表に、電子メール オプションから削除され、*usp_mailbox* テーブルで提供されるオプションと、メールボックスの詳細ページのラベルを示します。

電子メール オプション	usp_mailbox オプション	デフォルトのメールボックスの詳細ラベル
EMAIL_ALLOW_ANONYMOUS	allow_anonymous	匿名を許可
EMAIL_ATTACHMENT_DIR	N/A	N/A 注: EMAIL_ATTACHMENT_DIR は廃止されたため、このオプションが設定され、EMAIL_ATTACHMENT_REPOSITORY が設定されていなかった場合は、手動で [添付ファイル リポジトリ] を選択する必要があります。
EMAIL_ATTACHMENT_REPOSITORY	attmnt_repository	添付ファイル リポジトリ
EMAIL_FORCE_ATTACHMENT_SPLITOUT	split_out_attachment	添付ファイルを強制的に分割
EMAIL_IS_ATTACHMENT	attach_email	電子メール全体を添付
EMAIL_SAVE_UNKNOWN_EMAILS	save_unknown_emails	不明な電子メールを保存

電子メール オプション	usp_mailbox オプション	デフォルトのメールボックスの詳細ラベル
MAIL_EATER_IMAP_HOST_PORT	host_port	ポートのオーバーライド
MAILEATER_CHECK_MAIL_INTERVAL	check_interval	チェック間隔
MAILEATER_HOST	host_name	ホスト名
MAILEATER_LOGIN_PASSWORD	password	パスワード
MAILEATER_LOGIN_USERID	userid	ユーザ ID
MAILEATER_POP3_HOST_PORT	host_port	ポートのオーバーライド
MAILEATER_SECURITY_LEVEL	security_lvl	セキュリティ レベル
MAILEATER_SERVER_TYPE	email_type	電子メール タイプ

重要: [添付ファイル リポジトリ] 設定は **r12.9** では廃止されているため、引き続きメールボックスにポーリングを実行する前に、[添付ファイル リポジトリ] を指定する必要があります。

Maileater.cfg に関する考慮事項

以前は *maileater.cfg* ファイルに含まれていた情報は、**r12.9** では *usp_mailbox_rule* テーブルにマップされます。 *maileater.cfg* から *usp_mailbox_rule* へのマッピングに関する以下の情報を考慮してください。

- 行頭の「-i」は、大文字と小文字の区別がないことを表しており、*filter_ignore_case* フィールドにマップされます。
- 検索フィルタ「Subject: *…」は、以前はフィルタする際の正規表現を表していました。「Subject:」は削除され、「^」記号に置き換わっています。残りの値は *filter_string* フィールドにマップされます。*Filter_type* は「件名の内容」タイプに設定されます。
- 「TEXT_API xxx」は、ルールに対して処理されるオブジェクトを表します。文字列「TEXT_API」は削除され、残りは *action_object* フィールドにマップされます。*action_operation* フィールドは「オブジェクトの作成/更新」に設定されます。

- ユーザへの応答には通常「PDM_MAIL …」が含まれています。
「PDM_MAIL」を設定している場合は、reply_method を「1800」に設定し、それ以外は「NULL」に設定したままにします。
- -s パラメータが設定されている場合は、テキストから件名フィールドを削除し、この値で reply_subject を設定します。
- 機能によって、エントリの順序が管理されます 有効な行には、いずれも、100 から始まり、100 ずつインクリメントされるシーケンス番号が設定されます。

usp_mailbox_rule 内のその他のフィールドは、以下のように設定されます。

フィールド	値
メールボックス	デフォルト
action_write_to_log	0
action_log_prefix	null
delete_flag	0
description	pdm_maileater.cfg ファイルからマイグレートされます。
reply_failure_html	<指定しない場合、デフォルトのアクションを継承します>
reply_failure_text	<指定しない場合、デフォルトのアクションを継承します>
reply_success_html	<指定しない場合、デフォルトのアクションを継承します>
reply_success_text	<指定しない場合、デフォルトのアクションを継承します>
text_api_defaults	null
text_api_ignore_incoming	null
action_subject_handling	null
last_mod_dt	null
last_mod_by	null
inclusion_list	"*"
email_address_per_hour	-1

フィールド	値
exclusion_list	null
log_policy_violation	1

Migration Console の仕組み

Migration Console を使用して、CA SDM のマイグレーションおよびアップグレード処理を実行できます。コンソールによって、CA SDM r11.2 などの既存のインストールが自動的に検出されます。アップグレードは、インストールメディアから、または[手動で](#) (P. 52)開始できます。

注: カスタマイズした Web フォームが CA SDM r12.9 と互換性がない場合、マイグレーション コンソールには、これらのフォームが `site/mods/www/html` ディレクトリに移動されたことを示すメッセージが表示されます。これらのフォームの詳細については、`site/mods/` ディレクトリの `Web_Forms_Changed.txt` ファイルを参照してください。

重要: CA SDM Migration Console では、部署はテナントに変換されません。マルチテナンシー環境でサポート オートメーションを設定する場合は、CA サポート オートメーション r6.0 SR1 eFix5 部署を r12.9 テナントに[個別にマイグレート](#) (P. 61)してから、CA SDM 内のサポート オートメーションを有効化する必要があります。

コンソールによって、以下のタスクが実行されます。

1. 製品が CA SDM r11.2、r12.0、r12.1、r12.5、r12.6、または r12.7 であることを確認します。
2. パスワードが FIPS 140-2 準拠形式に変換されます。
3. MDB 更新が適用されます。

重要: リモート MDB のバージョンは CA MDB r1.5 以降である必要があります。これ未満の場合、マイグレーションは失敗します。

4. LREL データがマイグレートされます。
5. カスタマイズされたファイルが UTF-8 に変換されます。

6. アクセス タイプのレコードが CA SDM r12.9 の役割およびアクセス タイプのレコードに変換されます。
7. 役割ベースの操作に対するユーザ スコアボード クエリがマイグレートおよびアップグレードされます。
8. 通知ルールおよび通知メッセージ テンプレートを使用できるよう、既存の通知がマイグレートおよびアップグレードされます。

注: [アップグレードの実行] を選択して [インストール] をクリックした後は、マイグレーションおよびアップグレードをロールバックできません。処理が終了する前に Migration Console を閉じた場合、処理は引き続きバックグラウンドで実行されます。

関連項目:

[CA MDB をインストールする方法](#) (P. 179)

[製品の設定](#) (P. 279)

[サポート オートメーション のデータのマイグレーション](#) (P. 59)

[前のリリースから CA CMDB をアップグレードする方法](#) (P. 53)

マイグレーション ログ ファイル

マイグレーションやアップグレード中に問題が発生した場合、マイグレーション ログに全プロセスのレコードが記録されています。以下の場所で、このログにアクセスできます。

```
$NX_ROOT/log/pdm_migrationr12_9.log
```

手動によるマイグレーションの開始

以下のコマンドを使用して、手動でアップグレードを開始できます。

■ Windows

```
$NX_ROOT\bin\migrate_to_r12_9.vbs
```

■ Linux/UNIX

```
$NX_ROOT/bin/migrate_to_r12_9.sh
```

注: マイグレーションが「スキーマ検証」エラーで失敗する場合は、上記のコマンドを使用して再度アップグレードを実行してください。

前のリリースから CA CMDB をアップグレードする方法

CA CMDB を、r11.2 や r12.0、r12.1 などの旧リリースから CA SDM r12.9 にアップグレードできます。マイグレーションをキャンセルする場合は、スクリプトを実行して、Migration Console を再起動する必要があります。スクリプトは、`C:/CMDB/bin` など、本製品の `/bin` ディレクトリ内にあります。たとえば、Linux または UNIX でマイグレーションをキャンセルする場合は `migration_to_r12.9.sh` スクリプトを実行します。

注: スタンドアロンの CA CMDB リリースからアップグレードしている場合は、CA SDM r12.9 でスタンドアロン CA CMDB の機能を引き続き使用できます。CA CMDB および CA SDM のある環境からアップグレードしている場合、または CA CMDB のない CA SDM 環境からアップグレードしている場合は、アップグレードの際に CA SDM r12.9 のフルインストールが実行されます。

以下のように CA CMDB をアップグレードします。

1. インストールメディアから CA SDM インストーラを起動します。

インストーラによって、CA CMDB r11.2 など、製品のバージョンが検出されます。

注: CA SDM と CA CMDB を組み合わせたインストールをアップグレードしている場合は、検出された環境が CA SDM ではなく CA CMDB リリースとしてインストーラに表示されます。

2. [次へ] をクリックします。

マイグレーションが完了するまで CA SDM およびナレッジマネジメントを使用しないように促す警告が表示されます。

3. [次へ] をクリックします。

Visualizer が検出された場合は、手動でアンインストールするように要求されます。

重要: Visualizer をアンインストールした後、再起動し、CA SDM インストーラを再度開始する必要があります。

4. 使用許諾契約の条件に同意して [インストール] をクリックします。
データがバックアップされ、サービスがシャットダウンされます。

注: CA CMDB のアップグレードでは、データベースはバックアップされません。

インストールが完了した後、**Migration Console** に、マイグレーションドキュメントを確認するように促す警告が表示されます。

5. [マイグレート] をクリックします。

Migration Console によって、システム データがロードされ、MDB が更新され、サービスがリサイクルされます。

注: プロセス中、マイグレーション ログをアクティブに表示できます。

6. コンソールによって、テーブルが検証され、データが処理され、バックアップが実行されて、製品が **r12.9** にアップグレードされます。

[CA SDM 環境設定] が表示されます。

7. (オプション) CMDB のみを設定します。

スタンドアロンの CA CMDB 環境からアップグレードしている場合は、**[CMDB のみを設定]** チェック ボックスが **[一般設定]** フォームに表示されます。

重要: 設定中に、CA CMDB スタンドアロンバージョンから CA SDM にマイグレートすると、**[CMDB のみを設定]** チェック ボックスが表示されます。**[CMDB のみを設定]** チェック ボックスをオフにして **[次へ]** をクリックすると、CA CMDB を再度設定することはできません。**[戻る]** をクリックしても、**[CMDB のみを設定]** チェック ボックスは使用できません。**[環境設定]** ダイアログに、この動作を警告するメッセージが表示されます。設定が完了して再起動する前に、その設定をキャンセルした場合は、**[CMDB のみを設定]** チェック ボックスは使用できます。

[CMDB のみを設定] チェック ボックスは、CA SDM 環境変数 **NX_CMDB** の値を制御します。環境変数は、サポート オートメーション 機能が設定されているかどうかを制御します。チェック ボックスがオフになっている場合、サポート オートメーション は設定可能ですが、それ以外の場合は設定できません。環境変数は Web フォームの動作に影響を与える場合があります。

スタンドアロンの CA CMDB 環境からアップグレードしており、CA SDM r12.9 でスタンドアロン CA CMDB の機能を使用する場合は、サポート オートメーション を設定することはできません。

8. 環境に応じて、設定を完了します。

64 ビット Linux/UNIX 上でデータを CA SDM r12.9 にマイグレートする方法

注: この情報は 64 ビットの Linux/UNIX 環境にのみ適用されます。

次の手順に従ってください:

1. Oracle 32 ビット クライアントをインストールします。
2. Oracle_Server_SID との接続を確立します。
3. ローカル ネット サービス名を作成し、接続をテストします。
4. TWO_TASK 変数をエクスポートします。
5. 以下の例に示すとおり、ORACLE_HOME および PATH 変数を編集して oracle_client ホームを追加し、サーバ ホームを削除します。

```
ORACLE_HOME= /opt/app/product/11.2.0/client_1  
PATH= /opt/app/product/11.2.0/client_1/bin
```

注: 前の例に示すとおり、NX.env の ORACLE_HOME を更新します。

6. 以下の例に示すとおり、LD_LIBRARY_PATH および LIBPATH を 32 ビット バイナリであるクライアント ライブラリに設定します。

```
LD_LIBRARY_PATH=/opt/app/product/11.2.0/client_1/lib
```

7. 以下の例に示すとおり、ORACLE_HOME を client_home に設定して pdm_configure を実行します。

```
C:¥app¥Administrator¥product¥11.2.0¥client_1¥
```

8. CA SDM r12.9 をインストールします。

64 ビット Windows 上でデータを CA SDM r12.9 にマイグレートする方法

注: この情報は 64 ビットの Windows 環境にのみ適用されます。

CA SDM r12.9 にデータをマイグレートするには、以下の手順に従います。

1. Oracle 32 ビット クライアントをインストールします。
2. Oracle_Server_SID との接続を確立します。
3. ローカル ネット サービス名を作成し、接続をテストします。
4. 以下の例に示すとおり、PATH 変数を編集して oracle_client ホームを追加し、サーバ ホームを PATH から削除します。

C:¥app¥Administrator¥product¥11.2.0¥client_1¥bin

5. 以下の例に示すとおり、ORACLE_HOME を client_home に設定して pdm_configure を実行します。

C:¥app¥Administrator¥product¥11.2.0¥client_1¥

6. CA SDM r12.9 をインストールします。

例: サポートされていない Windows 環境からのマイグレート

この例では、Windows 2003 (32 ビット) 上に CA SDM r11.2 および SQL Server 2005 がインストールされています。データをマイグレートし、Windows 2008 64 ビット システム上で CA SDM r12.9 および SQL Server 2008 にアップグレードします。

次の手順に従ってください:

1. 同じコンピュータで CA SDM r12.9 にマイグレートします。
2. SQL Server 2005 を 2008 にアップグレードします。
3. MDB データベースをバックアップします。
4. Windows 2008 (64 ビット) 上に CA SDM r12.9 をインストールします。
5. 手順 3 で実行した MDB バックアップをロードします。
6. \$NX_ROOT¥site¥mod フォルダを古いコンピュータから新しいコンピュータに移動します。
7. NX.env ファイルを更新し、変数をカスタマイズします。

8. Attachment フォルダを古いコンピュータから新しいコンピュータに移動します。
9. 新しいコンピュータで構成を再度実行します。
10. オプション マネージャで、必要な場所のコンピュータ詳細を更新します。

例：サポートされていない非 Windows 環境からのマイグレート

この例では、Redhat Enterprise Linux 4 上に CA SDM r11.2 および Oracle 10g がインストールされています。データをマイグレートし、Redhat Enterprise Linux 6 上で CA SDM r12.9 および ora> 11g R2 にアップグレードします。

次の手順に従ってください：

1. 同じコンピュータで CA SDM r12.5 にマイグレートします。
2. MDB データベースをバックアップします。
3. Redhat Enterprise Linux 6 上に CA SDM r12.5 および Oracle 11g R2 をインストールします。
4. 手順 2 で実行した MDB バックアップをロードします。
5. \$NX_ROOT¥site¥mod フォルダを古いコンピュータから新しいコンピュータに移動します。
6. NX.env ファイルを更新し、変数をカスタマイズします。
7. Attachment フォルダを古いコンピュータから新しいコンピュータに移動します。
8. 新しいコンピュータで構成を再度実行します。
9. オプション マネージャで、必要な場所のコンピュータ詳細を更新します。
10. CA SDM r12.5 から r12.9 にマイグレートします。

サポート オートメーションのデータのマイグレーション

以下の環境から CA SDM r12.9 に CA サポート オートメーション r6.0 SR1 eFix5 のデータをマイグレートできます。

- Unicenter Service Desk r11.2
- CA SDM r12.0
- CA SDM r12.1
- CA SDM のない CA サポート オートメーション r6.0 SR1 eFix5

注: データのマイグレーションは、CA サポート オートメーション r6.0 SR1 eFix5 からのみ可能です。マイグレーションの前に、CA サポート オートメーション r6.0 SR1 eFix5 データベースのフルバックアップを実行することをお勧めします。

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 r12.9 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。

サポート オートメーション データベースをマイグレートする方法

マイグレーション ツールを使用して、サポート オートメーション データベースから CA SDM データベースにデータをマイグレートできます。サポート オートメーション の名前も CA SDM データベースの命名規則に変換されます。サポート オートメーション を初めて使用する前に、サポート オートメーション データベースから CA SDM データベースにデータをマイグレートしてください。

以下のプロセスで、データのマイグレート方法について説明します。

1. インストール メディア上のスクリプトを使用して、CA サポート オートメーション データを エクスポート (P. 62) します。

エクスポートツールによって、データが **.DAT** 形式に変換されます。データをマイグレートする際、ツールによって、以下の主要な手順が実行されます。

- サポート オートメーション データベース スキーマを **CA SDM** データベースにインポートします。

このスキーマによって、サポート オートメーション で使用される必要なテーブルが作成されます。

- サポート オートメーション データベース マイグレーション XML から **CA SDM** データベースにデータをマイグレートします。

CA SDM マイグレーション ツールによって、必要な **UUID** が生成され、サポート オートメーション **ID** と **CA SDM UUID** 間の関係を表す必要なレコードが作成されます。

2. **CA SDM** サーバ上の以下のディレクトリに、**CA** サポート オートメーション データ エクスポート フォルダをコピーします。

NX_ROOT/site/sbmigration/SA60

データのエクスポートが完了します。

3. **CA** サポート オートメーション マイグレーション ツールを使用して、**CA SDM** にデータを [インポート](#) (P. 64) します。

データがデータベースにロードされ、マイグレーションが完了します。

履歴データのマイグレーション

CA サポート オートメーション **r6.0 SR1 eFix5** データベースから履歴データの全部をマイグレートする必要はない場合、履歴データの一部をページできます。ページスクリプトのセットアップで、データベースに残す日数を設定できます。

以下の場所からのページスクリプトをダウンロードできます。

ftp://ftp.ca.com/pub/supportbridge/6.0/patch-01/purge_history_6.0_sp1.zip

部門をテナントに変換する方法

部門のマイグレーションは、CA サポート オートメーション r6.0 SR1 eFix5 からのみ可能です。これらの部門をテナントに変換して、サポート オートメーション 環境内でマルチテナンシーを使用できます。各部門を部門固有のテナントとして個々にマイグレートできます。最初のデータインポート中に、テナントが任意のテーブル内の行はすべてテナント化されます。

重要: CA SDM でサポート オートメーションを有効化する前に、このデータをマイグレートします。

以下の手順で、部門をテナントにマイグレートできます。

1. インストールメディア上のスクリプトを使用して、部門データを[エクスポート](#) (P. 62) します。

単一の部門またはすべての部門をエクスポートできます。

2. エクスポートツールによって、データが **.DAT** 形式に変換されます。
ツールには、部門エクスポートのステータスが表示されます。

3. CA SDM サーバ上の以下のディレクトリに、CA サポート オートメーションデータエクスポートフォルダをコピーします。

`NX_ROOT/site/sbmigration/SA60`

データのエクスポートが完了します。

4. CA サポート オートメーションマイグレーションツールを使用して、CA SDM にデータを[インポート](#) (P. 64) します。

データがデータベースにロードされ、マイグレーションが完了します。

注: サポート オートメーションの環境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。

CA サポート オートメーション データのエクスポート

CA サポート オートメーション r6.0 SR1 eFix5 データをエクスポートするには、CA SDM で使用される *.DAT* 形式に変換します。部門を個別のテナントにエクスポートし、パブリック環境にデータをインポートできます。エクスポート ツールではプロセスをログに記録し、エクスポートが完了した後、ログ ファイルの出力ディレクトリを表示します。エクスポートプロセスでは、各テーブルの正常な出力を記録し、予期しない状況やエラーが発生した場合にはそれを示します。

重要: 部門のマイグレーションは、CA サポート オートメーション r6.0 SR1 eFix5 からのみ可能です。

CA サポート オートメーション データをエクスポートする方法

1. 以下のディレクトリのインストール メディアから *SA60Export* スクリプトを実行します。

/casd.nt/SAMigration

注: ファイル拡張子は、使用しているオペレーティング システムによって異なります。たとえば、Windows では「bat」が使用され、UNIX では、Bourne シェル スクリプトの場合は「sh」、C シェルの場合は「csh」、korn シェルの場合は「ksh」が使用されます。

CA サポート オートメーション マイグレーション ツールが表示されます。

2. 以下の手順に従います。
 - a. CA サポート オートメーション r6.0 SR1 eFix5 「WEB-INF」インストール親ディレクトリを入力します。
 - b. CA サポート オートメーション データをエクスポートするディレクトリを入力します。

注: エクスポートが完了した後、このフォルダを CA SDM サーバ上の *NX_ROOT/サイト/sbmigration/SA60* ディレクトリに移動させてください。

- c. (オプション) パスワードがエクスポート可能かどうかを指定します。このオプションを選択した場合、ユーザ、デフォルト認証情報、および自動タスク認証情報のパスワードがエクスポートされます。
- d. (オプション) 単一の部門またはすべての部門をエクスポートします。このオプションを選択した場合、ドロップダウンリストにすべてのアクティブな部門が表示されます。

3. [実行] をクリックします。

[プロセス ステータス] に、マイグレートされるデータベース テーブルやテーブル内のレコード数など、エクスポートに関する情報が表示されます。

ツールによって回復できないエラーが検出されると、メッセージが表示されます。

注: ツールバーまたはファイル メニューから [停止] を選択して、エクスポートを停止できます。

データのエクスポートが完了します。

4. 環境に応じてサポート オートメーション を設定し、実装します。

注: サポート オートメーション オプション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 データのインポート

.DAT 形式に変換してから、サポート オートメーション データをインポートします。サポート オートメーションマイグレーション スクリプトを使用して、CA SDM にデータをインポートできます。USDK> をインストールし、設定した後、ユーティリティを呼び出します。pdm_perl コマンドを使用して sa_migrate.pl を実行することもできます。

NX_ROOT¥bin¥ディレクトリ内のスクリプトにアクセスできます。マイグレーション スクリプトによって、データベース制約を管理するためのテーブル処理、対応する CA SDM オブジェクトの作成、テナント列の値のマッピングといったタスクが実行されます。

CA SDM 内のマイグレーション関連ファイルのデフォルトの場所は、NX_ROOT/site/sbmigration ディレクトリです。たとえば、インポート設定ファイルは、NX_ROOT/site/sbmigration/config フォルダ内にあります。sa_migration_config.dat ファイルには、id、prop_name、value、および prop_description 列が CA SDM データ フォーマットで格納されています。

ディレクトリには、CA サポート オートメーション r6.0 SR1 eFix5 エクスポート データ、マイグレーション ユーティリティ コード、Perl スクリプトなどが格納されています。

サポート オートメーション データをインポートする方法

1. CA SDM サービスを開始します。

サービスが開始され、実行されていることを確認できます。

2. コマンドラインで以下を入力します。。

```
pdm_perl <NX_ROOT>¥bin¥sa_migrate.pl
```

サポート オートメーション データがエクスポート パッケージからデータベースにロードされます。

マイグレーション後に サポート オートメーション 役割アクセスを設定する方法

マイグレーションの前に サポート オートメーション を設定する場合、役割アクセスは正常に設定されます。マイグレーション後に サポート オートメーション を設定する場合は、各役割の サポート オートメーション アクセス フィールドに適切な値を設定してください。役割アクセスが正常にセットアップされていないと、サポート オートメーション アナリスト インターフェースまたはエンド ユーザ インターフェースにアクセスできません。

以下のプロセスで、マイグレーション後に サポート オートメーション 役割アクセスを設定する方法について説明します。

1. `supportautomation_url` オプションをインストールします。
2. サポート オートメーション にアクセスする各役割に サポート オートメーション アクセス フィールドを設定します。

注: `supportautomation_url` オプションのインストールまたは サポート オートメーション アクセス役割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。

カスタム CA Business Intelligence ユニバースのマイグレート方法

以下の手順で、カスタム ユニバースをマイグレートできます。

1. カスタマイズ手順に従って、カスタム ユニバースを **CA SDM** ユニバースにリンクします。
2. サイト定義のユニバースまたはレポートの *biar* ファイルをバックアップします。
3. 現在のリリースからユニバースをインストールします。
4. 現在のリリースからのユニバースをカスタム ユニバースにリンクします。

カスタム ユニバースのバックアップ方法

カスタム ユニバースを CA SDM ユニバースにリンクした場合は、CA SDM r12.9 ユニバースおよびレポートをインストールする前に、以下の操作を実行します。

1. インポート ウィザードを使用して、サイト定義のユニバースまたはレポートの *biar* ファイルのバックアップを作成します。
2. Universe Designer を起動します。
3. カスタム ユニバースをインポートします。
4. ユニバースのコピーをローカル ドライブに保存します。
カスタム ユニバースがバックアップされます。

関連項目：

[開発から実稼働への移動](#) (P. 598)

CA Business Intelligence ユニバースのインストール

ユニバースをインストールして、CA Business Intelligence r12.0 ユニバースおよびレポートを置き換えます。

ユニバースをインストールする方法

1. CA Service Desk Manager の DVD #2 から、setup.exe を実行します。
2. [製品のインストール] タブを選択します。
3. 画面をスクロール ダウンして、[CA Business Intelligence 環境設定] を選択します。

CA Service Desk Manager コンポーネントのインストーラ ウィザードが表示されます。

4. [次へ] をクリックして、ユーザ クレデンシャルを入力します。

注: CA SDM がコンピュータにインストールされていない場合は、CA SDM のホスト名を指定します。

5. [完了] をクリックします。

CA Business Intelligence r12.0 ユニバースおよびレポートが置き換えられ、r12.9 レポートがサブフォルダに作成されます。

ユニバース リンクの更新

CA SDM r12.9 では、ユニバース名は変更されていませんが、ユニバースへのユニバース リンクを更新する必要があります。リンクを更新しないと、レポートを実行したり、ユニバースをインポートするときに、ユニバース接続の問題が発生することがあります。以下のエラーメッセージが表示されることがあります。

Unable to resolve core universe ID

ユニバース リンクを更新するには

1. カスタム ユニバースのバックアップに使用したコンピュータで Universe Designer を起動します。
2. [File] - [Open] を選択して、カスタム ユニバースを開きます。
3. [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。
4. [Links] タブをクリックします。
5. [Name] 列で [CA SDM ユニバース] をクリックします。
[Change Source] ボタンが有効になります。
6. [Change Source] ボタンをクリックします。
7. CA SDM の .unv ファイルがある場所へ移動して選択します。
注: .unv ファイルは通常、CA Universes フォルダにあります。
8. [Open] をクリックして、次に [OK] をクリックします。
ユニバース リンクが更新されます。
9. カスタム ユニバースをエクスポートします。

アップグレード後の構成

アップグレードが完了したら、製品を構成します。構成ウィザードを使用して、既存のカスタマイズを確認します。

注: アップグレード後の構成を完了せずに [環境設定] ダイアログ ボックスを閉じた場合は、コマンドラインから `pdm_configure -s` を実行してください。

プライマリまたはセカンダリ以外のサーバの非アクティブ化

アップグレードした後、プライマリ サーバとして `usp_servers` テーブルに入力されないサーバはすべて、セカンダリ サーバに変換されます。アップグレードする前に `usp_servers` テーブルに追加したサーバで、セカンダリ サーバでもプライマリ サーバでもないサーバが存在する場合は、アップグレード後にそのサーバを非アクティブにします。プライマリ サーバの Web UI からサーバを非アクティブにできます。詳細については、オンライン ヘルプを参照してください。

EEM 8.4 サーバを使用する既存のユーザのサポート

CA SDM r12.9 は、EEM 8.4 サーバと互換性のない EEM 12.5 SDK を使用します。EEM 8.4 サーバを使用している既存のユーザをサポートするには、EEM 8.4 SDK パッチを CA SDM r12.9 サーバに適用する必要があります。このパッチの詳細については、CA サポート オンラインを参照してください。

CA Workflow と CA EEM のアップグレード方法

CA SDM r12.9 に CA Workflow および CA EEM を別々にインストールします。

r12.9 にマイグレートする場合、CA EEM r8.4 SP4 以降および CA Workflow r1.1.132 以降にアップグレードする必要があります。

注: CA EEM r8.1 から r8.4 SP4 に直接アップグレードできます。

CA EEM および CA Workflow をアップグレードするには、以下のタスクを実行します。

1. CA SDM r12.9 にアップグレードされていることを確認します。
2. ドライブにインストール メディアを挿入します。
3. CA EEM をインストールします。
4. CA Workflow をインストールします。

CA Workflow および CA EEM をインストールした後、オプション マネージャで適切なオプションを手動で設定します。アップグレードされたオプションをよく確認します。CA Workflow のデフォルトの Tomcat ポートは 8080 ではなく、プロセス マネージャのデフォルトの URL は `pmService` ではありません。

注: `cawf_pm_url` オプションは、デフォルトの `http://<wf_hostname>:<wf_tomcat_port>/pm/service/pmService2` に変更されています。CAWF 通信が正しく機能するように、「pmService」から「pmService2」に手動で変更する必要があります。

重要: 以前に eIAM CA SDM ユーザ認証を使用していた場合は、CA EEM をアップグレードした後で、オプションマネージャの [セキュリティ] から `eiam_hostname`、`use_eiam_artifact`、および `use_eiam_authentication` 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。

サーバプロセス設定の保持

CA SDM の以前のリリースでは、サーバプロセス設定 (`pdm_edit.pl` スクリプトを使用して作成される) に関する情報は、`$NX_ROOT/samples/pdmconf` ディレクトリにある `pdm_startup.dat` ファイルに格納されます。このサーバプロセス設定を CA SDM r12.9 で保持するには、`pdm_startup.dat` ファイルを処理して、後で `pdm_configure` コマンドを使用して適用できる設定を生成する必要があります。

次の手順に従ってください:

1. プライマリ サーバの Web UI にログインし、以前の CA SDM リリースに含まれているすべてのセカンダリ サーバを追加します (まだ追加していない場合)。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. `SNX_ROOT/bin` ディレクトリに移動して、`pdm_edit_migration` コマンドラインツールを実行します。このツールは、CA SDM の従来の設定に対してのみ適用可能です。

このツールが正常に実行された場合、アクティブ状態で新しい設定が作成されます。正常に実行されなかった場合、非アクティブ状態で新しい設定が作成されます。CA SDM Web UI で、[管理] タブから [システム] - [環境設定] に移動し、新しい設定を確認します。アクティブな設定のみをサーバに適用できます。

注: ツールが正常に実行されない場合は、`pdm_startup.dat` ファイル内の問題のあるエントリを修正し、ツールを再実行してください。

3. `pdm_configure` をプライマリ サーバで実行してこの新しい設定を適用します。詳細については、「サーバ設定ヘルプ」を参照してください。

CA SDM および CA IT PAM 統合の有効化

アップグレードした後以下の手順に従うことにより、CA SDM と CA IT PAM 4.0 以降の統合を確保します。

1. [オプション マネージャ] - [CA IT PAM ワークフロー] に移動し、以下のオプションの値を変更します。
2. caextwf_processdisplay_url の値を
`http://<wf_hostname>:<wf_tomcat_port>/itpam/Web.jsp?page=runtimeeditor&ROID=` に設定します。
3. caextwf_worklist_url の値を
`http://<wf_hostname>:<wf_tomcat_port>/itpam?page=tasklist` に設定します

重要: CA SDM を、CA EEM 8.4 を使用する CA IT PAM と統合する場合は、CA EEM 8.4 SDK パッチが CA SDM に適用されていることを確認します。このパッチの詳細については、CA サポート オンラインを参照してください。

Web エンジンおよびブラウザ キャッシュのクリア

CA SDM r12.9 にアップグレードした後、pdm_webcache ユーティリティを実行して Web エンジンとブラウザのキャッシュをクリアする必要があります。

```
pdm_webcache -b -H
```

```
-b
```

ブラウザ キャッシュをクリアするようユーザに警告します。

```
-H
```

Web エンジンキャッシュをクリアします。

WebDirector およびサーバの設定

アップグレードした後、サーバおよび WebDirector を設定することをお勧めします。

Web Director およびサーバを構成する方法

以前のバージョンが追加のサーバまたは WebDirector を使用するように設定されていた場合は、サーバおよび WebDirector を設定し、その設定をアップグレードの後に適用できます。

詳細については、「[管理ガイド](#)」を参照してください。

LREL マイグレーションの後

マイグレーションの後、以下の確認手順を実行します。

1. 新規テーブル コンテンツに対してクエリを実行し、テーブルに正しいデータが格納されていることを確認します。
2. 各サイト定義レポートを更新し、レポートデータが新しい LREL テーブルから取得されていることを確認します。
3. サイト定義レポートをテストします。

廃止されたオブジェクトとテーブル

以下のオブジェクトおよびテーブルは、CA SDM のこのリリースでは廃止されました。マイグレーション中、システムによってデータが r12.9 LREL テーブルにコピーされます。システムでは LREL テーブルおよびオブジェクトを使用しますが、古いテーブルには参考用に、アップグレード時に存在したデータが保持されます。

注: LREL 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。

DBMS 名	オブジェクト名
Attachment_Lrel	attmnt_lrel
Business_Management_Repository_Lrel	bmlrel
Chgcat_Group	chgcat_grp

Chgcat_Loc	chgcat_loc
Chgcat_Workshift	chgcat_workshift
Group_Loc	grp_loc
Isscat_Group	isscat_grp
Isscat_Loc	isscat_loc
Isscat_Workshift	isscat_workshift
Knowledge_Lrel_Table	kmlrel
Lrel_Table	lrel1
Pcat_Group	pcat_grp
Pcat_Loc	Pcat_Loc
Pcat_Workshift	pcat_workshift
Wftpl_Group	wftpl_grp

LREL テーブルとオブジェクト

マイグレーションでは、多対多のデータ関係を管理するために、自動的に以下のテーブルおよびオブジェクトを作成します。

DBMS 名	オブジェクト名
usp_lrel_asset_chgnr	lrel_asset_chgnr
usp_lrel_asset_issnr	lrel_asset_issnr
usp_lrel_att_cntlist_macro_ntf	lrel_att_cntlist_macro_ntf
usp_lrel_att_ctplist_macro_ntf	lrel_att_ctplist_macro_ntf
usp_lrel_att_ntflist_macro_ntf	lrel_att_ntflist_macro_ntf
usp_lrel_attachments_changes	lrel_attachments_changes
usp_lrel_attachments_issues	lrel_attachments_issues
usp_lrel_attachments_requests	lrel_attachments_requests
usp_lrel_aty_events	lrel_aty_events
usp_lrel_bm_reps_assets	lrel_bm_reps_assets
usp_lrel_bm_reps_bmhiers	lrel_bm_reps_bmhiers
usp_lrel_cenv_cntref	lrel_cenv_cntref

usp_lrel_dist_cntlist_mgs_ntf	lrel_dist_cntlist_mgs_ntf
usp_lrel_dist_ctplist_mgs_ntf	lrel_dist_ctplist_mgs_ntf
usp_lrel_dist_ntflist_mgs_ntf	lrel_dist_ntflist_mgs_ntf
usp_lrel_false_action_act_f	lrel_false_action_act_f
usp_lrel_false_bhv_false	lrel_false_bhv_false
usp_lrel_kwrds_crsolref	lrel_kwrds_crsolref
usp_lrel_notify_list_cntchgntf	lrel_notify_list_cntchgntf
usp_lrel_notify_list_cnttssntf	lrel_notify_list_cnttssntf
usp_lrel_notify_list_cntntf	lrel_notify_list_cntntf
usp_lrel_ntfr_cntlist_att_ntfrlist	lrel_ntfr_cntlist_att_ntfrlist
usp_lrel_ntfr_ctplist_att_ntfrlist	lrel_ntfr_ctplist_att_ntfrlist
usp_lrel_ntfr_macrolist_att_ntfrlist	lrel_ntfr_macrolist_att_ntfrlist
usp_lrel_ntfr_ntflist_att_ntfrlist	lrel_ntfr_ntflist_att_ntfrlist
usp_lrel_oenv_orgref	lrel_oenv_orgref
usp_lrel_status_codes_tsktypes	lrel_status_codes_tsktypes
usp_lrel_svc_grps_svc_chgcat	lrel_svc_grps_svc_chgcat
usp_lrel_svc_grps_svc_isscat	lrel_svc_grps_svc_isscat
usp_lrel_svc_grps_svc_pcat	lrel_svc_grps_svc_pcat
usp_lrel_svc_grps_svc_wftpl	lrel_svc_grps_svc_wftpl
usp_lrel_svc_locs_svc_chgcat	lrel_svc_locs_svc_chgcat
usp_lrel_svc_locs_svc_groups	lrel_svc_locs_svc_groups
usp_lrel_svc_locs_svc_isscat	lrel_svc_locs_svc_isscat
usp_lrel_svc_locs_svc_pcat	lrel_svc_locs_svc_pcat
usp_lrel_svc_schedules_chgcat_svc	lrel_svc_schedules_chgcat_svc
usp_lrel_svc_schedules_isscat_svc	lrel_svc_schedules_isscat_svc
usp_lrel_svc_schedules_pcat_svc	lrel_svc_schedules_pcat_svc
usp_lrel_true_action_act_t	lrel_true_action_act_t
usp_lrel_true_bhv_true	lrel_true_bhv_true

LREL 変換の確認

データマイグレーション中、システムによって、多対多関係を管理する LREL テーブルが追加されます。新規テーブルのコンテンツと、更新されたサイト定義コードおよびレポートを確認できます。

LREL テーブル内のデータを確認する方法

1. テーブル コンテンツに対してクエリを実行し、正しいデータが格納されていることを確認します。
2. 各サイト定義レポートを更新し、レポートデータが新しい LREL テーブルから取得されていることを確認します。
3. 新しい DBMS テーブル参照でクエリを更新します。
4. サイト定義レポートおよびコードをテストします。新しい LREL テーブルおよび、Web サービスなどのサポートされたインターフェースを使用するために、コードを更新します。必要に応じて、コード内のテーブル名を更新します。

データベース カスタマイズの確認

データベースのカスタマイズが本製品の現在のリリースに正しくマイグレートされたことを確認できます。

データベース カスタマイズを確認する方法

1. データベース管理製品または Web Screen Painter のいずれかを使用して、カスタマイズした各テーブルを確認します。
2. カスタマイズしたファイルが以下のディレクトリに存在することを確認します。

`$NX_ROOT/site/mods/`

Web フォーム カスタマイズの確認

Web フォームのカスタマイズが本製品の現在のリリースに正しくマイグレートされたことを確認できます。

Web フォーム カスタマイズを確認する方法

1. カスタマイズしたフォームが `$NX_ROOT/site/mods/www/html` ディレクトリに存在することを確認します。
2. Web フォームがブラウザ内で正しく開くことを確認します。
3. Web フォームが Web スクリーン ペインタで正しく開くことを確認します。

アクセス タイプの編集

CA SDM r11.2 からのアップグレードプロセスを開始すると、すべてのアクセス タイプに対応する役割が自動的に作成され、役割にアクセス権と権限が正しく割り当てられます。r12.9 で新しい役割を利用する場合は、アクセス タイプ用に役割を作成できます。

アクセス タイプ用に役割を作成する方法

1. [管理] タブをアクセスする権限を持ったユーザとして Web インターフェイスにログインします。
2. [管理] タブをクリックします。
3. 左側のツリーで、[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。
使用可能なアクセス タイプがすべて表示されます。
4. 使用可能なアクセス タイプを 1 つクリックします。
[アクセス タイプの詳細] ページが表示されます。
5. [役割] タブをクリックします。
6. アクセス タイプ用に新しい役割を選択し、[役割の更新] をクリックします。

新しい役割がアクセス タイプに関連付けられます。

注: カスタムの役割を作成して、その役割をアクセス タイプに割り当てることもできます。役割の作成の詳細については、「管理ガイド」を参照してください。

優先順位計算の有効化

優先順位計算は、問題とインシデントの「優先度」、「緊急度」、および「影響度」の値を自動的に設定するための値のセットです。CA SDM の新規インストールでは、デフォルトの優先順位計算が、問題およびインシデント チケット タイプに対してデフォルトで有効化されています。ただし、以前のリリースからアップグレードしている場合は、デフォルトの優先順位計算は非アクティブになります。

別の優先順位計算を作成してアクティブ化する場合、チケットの値には、インシデントまたは問題と関連付けられたアクティブな優先順位計算の設定が反映されます。アクティブな優先順位計算がない場合は、ユーザーが手動でチケット上の「優先度」やその他の値を設定できます。

注: 従業員および顧客インターフェース上のカスタマイズされたフォームは、以前のバージョンと同じ方法で動作します。セルフサービス ユーザーは、優先順位計算の設定にかかわらず、「優先度」を直接変更できます。

マイグレーション後に優先順位計算を有効化するには、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」に移動します。
「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または別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。
「優先順位計算の更新」ページが表示されます。
3. ステータスを「アクティブ」に設定します。
4. 以下の 1 つ以上のチケット タイプを選択します。

インシデント

この優先順位計算でインシデント チケットを管理できるようになります。インシデントを管理できるのは、アクティブな優先順位計算 1 つのみです。

問題

この優先順位計算で問題チケットを管理できるようになります。問題を管理できるのは、アクティブな優先順位計算 1 つのみです。

5. [保存] をクリックします。

別の優先順位計算をアクティブにしない限り、デフォルトの優先順位計算の値が新規チケットに適用されます。優先順位計算を使用する新規チケットでは、[優先度] フィールドは読み取り専用です。

注: テナントおよびチケット用に優先順位計算を定義する詳細については、「管理ガイド」およびオンライン ヘルプを参照してください。

インシデントに[インシデントの優先度]フィールドを追加する方法

インシデントの優先度は、緊急度と影響度の値の合計です。インシデントの優先度は、インシデント チケット タイプ 専用です。

`use_incident_priority` オプションをインストールし、**Web Screen Painter** を使用して [インシデントの詳細] ページフォームに追加すると、[インシデントの優先度] の値がインシデント上に表示されます。

インシデントに [インシデントの優先度] フィールドを追加するには、以下の手順に従います。

1. [オプション マネージャ] - [リクエスト マネージャ] から、`use_incident_priority` オプションをインストールします。
2. **Web Screen Painter** を使用して、[インシデントの詳細] ページに [インシデントの優先度] フィールドを追加します。

`use_incident_priority` オプションをインストールしている場合は、保存した [インシデントの詳細] ページに [インシデントの優先度] の値がページに表示されます。`use_incident_priority` オプションがインストールされていない場合は、[インシデントの優先度] の値はゼロになります。

注: `use_incident_priority` オプションでは、[インシデントの優先度] の値のみを管理します。このオプションは、優先順位計算には関係ありません。

関連項目:

[セルフ サービス ユーザ用の緊急度範囲の設定 \(P. 79\)](#)

従業員チケットへの[緊急度]フィールドの追加

デフォルトでは、[緊急度] フィールドは従業員インシデントまたはリクエスト上に表示されません。ただし、`urgency_on_employee` オプションを使用して、[緊急度] フィールドを追加できます。

注: `urgency_on_employee` オプションをアンインストールし、優先順位計算を無効にすると、セルフサービスユーザの [リクエストの詳細] ページおよび [インシデントの詳細] ページに [優先度] フィールドが表示されます。

従業員チケットに [緊急度] フィールドを追加するには、[オプション マネージャ]-[リクエスト マネージャ] から、`urgency_on_employee` オプションをインストールします。[緊急度] フィールドが従業員インシデントまたはリクエスト上に表示されます。セルフサービスユーザは、インシデント上の値をオーバーライドできます。

セルフサービス ユーザ用にチケットの値を設定する方法

セルフサービス ユーザに表示される [緊急度] と [優先度] の値を制御できます。`web.cfg` ファイルで設定するプロパティによって、ユーザがチケットを作成または編集する際に表示される選択肢を管理できます。

セルフサービス ユーザ用にチケットの値を設定する際には、以下を考慮してください。

1. `web.cfg` パラメータの各オーバーライド値には、1 つ以上の値を指定します。
2. [\[緊急度\] の値](#) (P. 80) には、0 ～ 4 の間の数を 1 つ以上指定します。
3. [\[優先度\] の値](#) (P. 82) には、1 ～ 5 の間の数を 1 つ以上または「なし」という言葉を指定します。
4. 各値はスペースで区切ります。
5. チケットに表示されるデフォルト値として、リストの一番上に表示される値を指定します。必要に応じて、読みやすくなるように、リスト内にデフォルト値を繰り返し使用できます。

関連項目:

[セルフ サービス ユーザ用の緊急度範囲の設定 \(P. 79\)](#)[緊急度のプロパティ値 \(P. 80\)](#)[セルフ サービス ユーザ用の優先度範囲の設定 \(P. 80\)](#)[優先度のプロパティ値 \(P. 82\)](#)

セルフ サービス ユーザ用の緊急度範囲の設定

セルフサービスのインシデントおよびリクエストでは、**web.cfg** ファイルにデフォルトの「緊急度」の値を設定できます。「緊急度」の値の範囲を設定すると、従業員、VIP 従業員、ゲストなどのセルフサービス ユーザがチケット上に「緊急度」の値を設定できるようになります。セルフサービス ユーザに表示される選択肢は、**web.cfg** に設定した値の範囲に基づきます。

セルフ サービス ユーザ用にデフォルトの「緊急度」の範囲を設定する方法

- 適切なディレクトリの **web.cfg** ファイルを開きます。
 - (Windows) %NX_ROOT%\bopcfg\www¥
 - (UNIX) \$NX_ROOT/bopcfg/www/
- 各パラメータに、1 つ以上の [「緊急度」のプロパティ値 \(P. 80\)](#) を指定します。各値はスペースで区切ります。

ESCEmpUrg

VIP 従業員がチケットの「緊急度」をオーバーライドする方法を指定します。

EmpUrg

従業員がチケットの「緊急度」をオーバーライドする方法を指定します。

AnonymousUrg

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。

3. *web.cfg* を保存します。

新規チケットで、従業員、VIP 従業員またはゲストは、*web.cfg* 内の値の範囲に基づいて [緊急度] の値を設定できます。

例: リクエスト上でゲストに緊急度の値を 2 つだけ表示する

1. *web.cfg* を開きます。
2. *AnonymousUrg* パラメータを「0 4」に設定します。例: *AnonymousUrg* 0.4
3. *web.cfg* を保存します。

セルフサービス ユーザに表示される [緊急度] の値は、[1- なるべく早く] および [5- 即時] になります。デフォルトの緊急度は、[1- なるべく早く] です。

緊急度のプロパティ値

web.cfg には、セルフサービス ユーザによるチケットの緊急度のオーバーライド方法を制御するための設定があります。以下の緊急度プロパティ値を使用できます。

- 0 - ユーザは緊急度を「1- なるべく早く」に設定できます。
- 1 - ユーザは緊急度を「2- 早く」に設定できます。
- 2 - ユーザは緊急度を「3- 迅速に」に設定できます。
- 3 - ユーザは緊急度を「4- 極めて迅速に」に設定できます。
- 4 - ユーザは緊急度を「5- 即時」に設定できます。

セルフ サービス ユーザ用の優先度範囲の設定

セルフサービス ユーザがチケット上の [優先度] の値をオーバーライドできるように、有効な優先度の範囲を設定できます。優先度の範囲を設定すると、顧客、従業員、またはゲストは、*web.cfg* 内の値の範囲に基づいて [優先度] の値を設定できます。

セルフサービス ユーザ用に優先度の範囲を設定する方法

1. 適切なディレクトリの **web.cfg** ファイル上で
 - (Windows) %NX_ROOT%\bopcfg\www\
 - (UNIX) \$NX_ROOT/bopcfg/www/
2. 各パラメータに、1 つ以上の [\[優先度\] プロパティ値](#) (P. 82) を指定します。

CstPrio

顧客がチケットの [優先度] をオーバーライドする方法を指定します。

EmpPrio

従業員がチケットの [優先度] をオーバーライドする方法を指定します。

AnonymousPrio

従業員がチケットの [優先度] をオーバーライドする方法を指定します。

3. **web.cfg** を保存します。

新規チケットで、顧客、従業員、またはゲストは、**web.cfg** 内の値の範囲に基づいて [優先度] の値を設定できます。

例: ゲストに優先度の値を 2 つだけ表示する

1. **web.cfg** を開きます。
2. **AnonymousPrio** パラメータを [なし 4] に設定します。例：
AnonymousPrio なし 4
3. **web.cfg** を保存します。

ゲストがチケットを操作する際、[緊急度] の値は「なし」または「4」になります。デフォルト値は「なし」です。

優先度のプロパティ値

`web.cfg` には、セルフサービス ユーザによるチケット優先度のオーバーライド方法を制御するための設定があります。以下の優先度プロパティ値を使用できます。

- なし - ユーザは優先度を「なし」に設定できます。
- 1 - ユーザは優先度を「1」（最も高い優先度）に設定できます。
- 2 - ユーザは優先度を「2」に設定できます。
- 3 - ユーザは優先度を「3」に設定できます。
- 4 - ユーザは優先度を「4」に設定できます。
- 5 - ユーザは優先度を「5」（最も低い優先度）に設定できます。

ステータス移行のアクティブ化

アップグレード後は、すべての事前定義済みステータス移行が非アクティブになっているため、ステータス移行は有効ではありません。必要なチケットステータス移行フローに対応するために、これらのステータス移行をアクティブ化して、変更できます。

注: チケット形式上で表示されるカスタマイズ済みステータス コードの説明は、すべてアップグレード処理中も保持されます。

ステータス移行をアクティブ化する方法

1. [管理] タブで [Service Desk] ノードを展開して、以下のチケットタイプのいずれかを選択します。
 - 変更要求
 - 変更要求移行
 - 案件
 - 案件移行
 - リクエスト/インシデント/問題
 - インシデント移行
 - 問題移行
 - リクエスト移行
- [移行リスト] が表示されます。

2. [移行リスト] ページの [フィルタを表示] をクリックします。
ページの上部に、追加検索フィールドが表示されます。
3. [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。
ページの下部の [移行リスト] に、すべての非アクティブな移行が表示されます。
4. 編集対象の移行を開きます。
5. [レコードステータス] ドロップダウンリストから [アクティブ] を選択します。
6. [保存] - [ウィンドウを閉じる] をクリックします。
7. [検索] をクリックします。
[移行リスト] にアクティブな移行が表示されます。

注: ステータス移行の詳細については、「管理ガイド」およびオンラインヘルプを参照してください。

移行タイプのアクティブ化

デフォルトでは、本製品で提供される事前定義済み移行タイプは、すべて非アクティブになっているため、[ステータス移行] ボタンは有効ではありません。必要なステータス移行フローに対応するために、これらの移行タイプをアクティブ化して、変更できます。

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] ページの [フィルタを表示] をクリックします。
ページの上部に、追加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] にすべての非アクティブな移行タイプが表示されます。
3. 移行タイプのタイトルを右クリックし、メニューから [編集] を選択します。

4. [レコードステータス] ドロップダウンリストから [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] にアクティブな移行タイプが表示されます。

機能アクセス領域のカスタマイズ

機能アクセス領域は、ユーザのアクセス権を制限できるようにするオブジェクトのグループです。CA SDM の以前のバージョンでは、コードコンポーネントへのアクセスを制限するために、8 つの修正済み機能アクセスグループが含まれていました。

マイグレーション中に、機能アクセスグループが各役割の新しい機能アクセス領域にマイグレートされます。マイグレーションでは、Majic の変更、デフォルトの参照データ、および新しい機能アクセス領域への役割のマッピングが自動的に処理されます。

マイグレーションの後、以下の操作を考慮してください。

- 既存および新規の機能アクセス領域へのオブジェクトのマッピングと、各領域への役割の権限のマッピングを確認します。機能アクセス領域を確認するには、Web Screen Painter を使用します。
- 権限を再度マップするか変更する場合は、CA SDM を使用します。ユーザに機能とオブジェクトへの適切なアクセス権があることを確認します。

注: デフォルトの権限と、新しい機能アクセス領域へのオブジェクトのマッピングの詳細については、製品のサポート Web サイトを参照してください。機能アクセス領域の変更または追加の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。

以下の表は、機能アクセス領域とコードコンポーネントのマッピングを示しています。

機能アクセス領域	コードコンポーネント	新規
管理	admin	いいえ
インシデント/問題/リクエスト	call_mgr	いいえ

変更要求	change_mgr	いいえ
インベントリ	inventory	いいえ
案件	issue_mgr	いいえ
ナレッジ ドキュメント	kd	いいえ
通知	notify	いいえ
参照	reference	いいえ
セキュリティ	security	いいえ
アナウンスメント	announcement	はい
インシデント/問題/リクエスト参照	call_mgr_reference	はい
インシデント/問題/リクエスト テンプレート	call_mgr_template	はい
変更要求テンプレート	change_mgr_template	はい
変更要求参照	change_reference	はい
構成アイテム	ci	はい
構成アイテム共通	ci_common_ro	はい
構成アイテム参照	ci_reference	はい
連絡先	contact	はい
グループ	group	はい
案件テンプレート	issue_mgr_template	はい
案件参照	issue_reference	はい
ロケーション	location	はい
通知の参照	notification_reference	はい
組織	organization	はい
優先付け	prioritization	はい
サービス レベル	service_level	はい
サイト	site	はい
ストアド クエリ	stored_queries	はい
調査	survey	はい
テナント管理	tenant_admin	はい

タイムゾーン	timezone	はい
ワークフロー参照	workflow_reference	はい
ワークシフト	workshifts	はい

マイグレーション後のアクセスレベルの変更

マイグレーションの後、すべての役割の機能アクセスレベルを確認できます。オブジェクトが別の機能アクセス領域に移動されたために、以前は拒否された一部の状況で、ユーザが一部の画面にアクセスできるようになりました。また、以前はアクセスできたフォームへのアクセスを拒否される場合もあります。新しい機能アクセス領域によって、元の機能アクセス領域のうち2つの権限が管理される場合、両方の状況が発生する可能性があります。

注: デフォルトの権限と、新しい機能アクセス領域へのオブジェクトのマッピングの詳細については、製品のサポート **Web** サイトを参照してください。アクセスレベルの変更または追加の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。

SITEMODS.JS ファイル

以前のバージョンの **sitemods.js** ファイルに、HTML ページから呼び出されるコード行が追加されていた場合、そのコードを動作させるには、最新の **sitemods.js** ファイルにマージする必要があります。

アクセスタイプの調整

CA SDM の以前のリリースでアクセスタイプとデータパーティションをカスタマイズしていた場合は、アップグレード後のナレッジマネジメントデータパーティション設定に問題がある可能性があります。このカスタマイズによって、カテゴリとドキュメントで許可グループ設定に問題が発生することがあります。たとえば、ユーザがアクセスできる情報が制限されます。

注: データパーティションまたはアクセスタイプを削除して作成し直した場合でも、アップグレード後にアクセスタイプとデータパーティションの設定を確認する必要があります。

アクセス タイプを調整する方法

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. [セキュリティと役割の管理] - [役割管理] - [役割リスト] をクリックします。
[役割リスト] が表示されます。
3. 役割ごとに、以下の手順を実行します。
 - a. 役割を右クリックし、[編集] を選択します。
 - b. [権限] タブの [データ パーティション名] フィールドを確認します。

このフィールドが空の場合、選択されたアクセス タイプに関連付けられたデータ パーティションがないため、ユーザには制限がなく、許可グループをセットアップした場合でも、製品内のすべてのドキュメントやカテゴリにアクセスできます。

この操作は管理者には適切ですが、全役割向けではありません。役割に関連付けられているデータ パーティションがない場合は、データ パーティションを作成または変更できます。

データ パーティション設定の調節

システムに役割を設定した後、パーティション制約を調節できます。本製品の現在のリリースにアップグレードした後、パーティション制約を調節して、適切な権限が正常に機能していることを確認できます。

データ パーティションの制約を調節する方法

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] を参照します。
[データ パーティションの制約リスト] ページが表示されます。
2. 以下のテーブルの Majic コード制約設定を確認します。

SKELETONS

ナレッジ ドキュメントに使用されるテーブルを指定します。

O_INDEXES

ナレッジカテゴリに使用されるテーブルを指定します。

テーブル制約設定が検証されます。

3. [フィルタを表示] をクリックし、以前使用したデータ パーティションを入力します。

注: [検索] 領域の [テーブル名] フィールドを使用して、リストの表示項目を絞り込むこともできます。たとえば、[テーブル名] フィールドに「**SKELETONS**」または「**O_INDEXES**」と入力し、[検索] をクリックします。

役割のマイグレート後のヘルプ セットの変更

CA SDM では、アップグレードした後、マイグレートされたすべての役割に対して完全なオンライン ヘルプが提供されます。オンライン ヘルプ システムの必要性に応じて、すべての役割のヘルプ セットを変更できます。

役割のヘルプ セットを変更するには、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] - [役割リスト] を参照します。

[役割リスト] ページが表示されます。

2. 顧客など、変更する役割を開きます。

[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。

4. [Web インターフェース] タブを選択します。

[ヘルプ ビュー] をクリックします。

選択した役割の使用可能なヘルプ セットのリストが表示されます。

5. 顧客などのヘルプ セットを選択します。

6. 役割を保存します。

役割のヘルプ ビューが、選択したオンライン ヘルプ セットに変更されます。

[ヘルプ セットの詳細] を選択し、[ヘルプを表示] ボタンをクリックして、オンライン ヘルプ セット内のトピックを表示することもできます。

デフォルトの制約設定

制約のデフォルト設定を以下に示します。

顧客 (like) および従業員 (like) 用のデータ パーティションの制約設定

顧客 (like) および従業員 (like) 用のデータ パーティションの制約設定は、以下のようになります。

SKELETONS テーブル

表示の制約：

```
'SKELETONS READ_PGROU in @root.pgrou or
READ_PGROU.[pgrou] contained_roles.role in @root.id) and
ACTIVE_STATE = 0'
```

更新前のおよび削除の制約：

```
'id = 0' (ID=0 はアクセスなし)
```

O_INDEXES テーブル

表示の制約：

```
READ_PGROU in @root.pgrou or READ_PGROU.[pgrou]
contained_roles.role in @root.id
```

更新前のおよび削除の制約：

```
WRITE_PGROU in @root.pgrou OR WRITE_PGROU.[pgrou]
contained_roles.role IN @root.role
```

CA SDM アナリスト (like)、ナレッジ マネージャ (like)、およびナレッジ エンジニア (like) 用の制約設定

CA SDM アナリスト (like)、ナレッジ マネージャ (like)、およびナレッジ エンジニア (like) 用の制約設定は、以下のようになります。

SKELETONS テーブル

表示の制約：

```
(ACTIVE_STATE >= 0 )and (READ_PGROU in @root.pgrou or
READ_PGROU.[pgrou] contained_roles.role in @root.id) OR
(ACTIVE_STATE > 0 AND ASSIGNEE_ID = @root.id) OR (ACTIVE_STATE =
0 AND OWNER_ID = @root.id)) Active
```

更新前のおよび削除の制約：

```
(ACTIVE_STATE >= 0) AND (WRITE_PGROU in @root.pgrou OR
WRITE_PGROU.[pgrou] contained_roles.role IN @root.role) OR
(ACTIVE_STATE > 0 AND ASSIGNEE_ID = @root.id) OR (ACTIVE_STATE =
0 AND OWNER_ID= @root.id)) Active
```

O_INDEXES テーブル

表示の制約：

READ_PGROU in @root.pgroups or READ_PGROU.[pgrou]
contained_roles.role in @root.id

更新前のおよび削除の制約：

WRITE_PGROU in @root.pgroups OR WRITE_PGROU.[pgrou]
contained_roles.role IN @root.role

IIS Web インターフェース (CAisd) の開始

IIS を統合した CA SDM r11.2 Windows インストールをアップグレードした後、CA SDM IIS Web インターフェース (CAisd) は停止します。引き続き IIS 統合を使用する場合は、アップグレードの完了後、手動で CAisd を開始します。

重要： IIS 7.0 を使用する場合は、CGI およびメタベース互換コンポーネントをインストールする必要があります。

カスタマイズした HTMPL フォームの変更

CA SDM をアップグレードしたら、ノートブック コントロールを含むカスタマイズしたすべての HTMPL フォームを変更して、Web マクロを追加し、適切なタブ グループ名を指定してください。

カスタマイズしたフォームごとに、WSP を使用して <PDM_NOTEBOOK> ステートメントを <PDM_MACRO name=startNotebook> に、<PDM_TAB> ステートメントを <PDM_MACRO name=TAB> に変更します。

注意： WSP の使い方の詳細については、「Web スクリーン ペインタ オンライン ヘルプ」を参照してください。

関連項目：

[リスト フォーム上のデータ グリッド リストの変更 \(P. 487\)](#)

[詳細フォーム上のノートブックの変更 \(P. 489\)](#)

ナレッジ マネジメント を r11.2 からアップグレードする方法

r11.2 から CA SDM r12.9 への自動アップグレードによって、ナレッジ マネジメント 環境がアップグレードされます。 アップグレードを完了するには、以下の手順を実行します。

1. ドキュメントの解決方法で作成されたリンクをデータベースにマップして、壊れたリンクを特定します。

注: デフォルトの「壊れたリンクのフラグ」ポリシーを使用して、壊れたリンクを特定します。

2. [管理] タブで、[ナレッジ] - [自動ポリシー] - [スケジューリング] を選択します。

[自動ポリシー] ページが表示されます。

3. [自動ポリシー計算の実行] チェック ボックスをオンにします。
4. 計算を行う時間間隔を選択して、[保存] をクリックします。
指定された日時にポリシーの処理が開始されます。

5. [管理] タブで、[ナレッジ] - [システム] - [一般設定] を選択します。

[システム] ページが開きます。

6. 以下の情報を入力します。

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 r12.9 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 r12.9 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。UNC 認証情報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。

7. pdm_k_reindex を以下のように実行します。

pdm_k_reindex -pm

解決方法フィールド内のドキュメント リンクおよび埋め込みイメージを修正します。

重要：アップグレード後、*pdm_k_reindex -pm* を実行すると、重大なエラーが発生することがあります。エラーが発生した場合は、[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、[発行済みドキュメントの編集許可] オプションを [完全な権限を持つユーザはドキュメントの編集が可能] に変更してから、*run pdm_k_reindex -pm* を実行します。

pdm_k_reindex -ml

解決方法フィールド内のドキュメント リンクを修正してデータベースにマップします。

pdm_k_reindex

ドキュメントのインデックスを作成し、ナレッジ環境で検索できるようにします。

ナレッジ マネジメント 環境が r12.9 にアップグレードされます。

注: アップグレード後、ナレッジ ドキュメントを印刷すると、ドキュメントの [解決方法] セクションの後に大きなスペースが挿入されることがあります。このスペースは、以前のリリースからドキュメント テンプレートをアップグレードする際の問題によって挿入されます。この印刷問題の解決方法の詳細については、リリース ノートを参照してください。

重要: アップグレード後、CA SDM の以前のリリースの ナレッジ マネジメント 通知データでは、r12.9 通知エンジンが使用されます。たとえば、ナレッジ レポート カードなどのオブジェクト タイプ用にデフォルトのアクティビティ通知および通知ルールがあります。

CA SDM r12.x から ナレッジ マネジメント をアップグレードする方法

r12 または r12.1 から CA SDM r12.9 への自動アップグレードによって、ナレッジ マネジメント 環境がアップグレードされます。アップグレードを完了するには、以下の手順を実行します。

1. ドキュメントの解決方法で作成されたリンクをデータベースにマップして、壊れたリンクを特定します。

注: デフォルトの「壊れたリンクのフラグ」ポリシーを使用して、壊れたリンクを特定します。

2. [管理] タブで、[ナレッジ] - [自動ポリシー] - [ポリシー] - [スケジューリング] を参照します。

[スケジューリング] ページが表示されます。

3. [最終更新] フィールドの [自動ポリシー計算の実行] チェック ボックスをオンにします。
4. [スケジュール] テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして日付を選択します。
5. 計算を行い、ポリシーを実行する時間間隔を選択します。
6. [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。

7. [管理] タブで、[ナレッジ] - [システム] - [一般設定] を参照します。

[一般設定] ページが開きます。

8. 以下の情報を入力します。

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 r12.9 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 r12.9 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/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。UNC 認証情報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。

9. (キーワード検索を実装している場合) コマンドプロンプトで以下のコマンドを入力します。

```
pdm_k_reindex factory:all
```

重要：all 変数の大文字と小文字は区別されます。factory:ALL と入力すると、ログ ファイルにエラーが表示されます。

ナレッジマネジメント 環境が r12.9 にアップグレードされます。

注：アップグレード後、ナレッジ ドキュメントを印刷すると、ドキュメントの [解決方法] セクションの後に大きなスペースが挿入されることがあります。このスペースは、以前のリリースからドキュメントテンプレートをアップグレードする際の問題によって挿入されます。この印刷問題の解決方法の詳細については、リリース ノートを参照してください。

重要：アップグレード後、CA SDM の以前のリリースのナレッジ マネジメント 通知データでは、r12.9 通知エンジンが使用されます。たとえば、ナレッジ レポート カードなどのオブジェクトタイプ用にデフォルトのアクティビティ通知および通知ルールがあります。

第 3 章: 計画

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 デフォルトおよび推奨ポート リスト](#) (P. 97)

[高可用性を計画する方法](#) (P. 100)

[CA MDB のインストールの計画](#) (P. 114)

[CA SDM のインストールの計画](#) (P. 118)

[CA NSM のインストール計画](#) (P. 135)

[CA EEM と CA Workflow のインストール計画](#) (P. 135)

[CA Process Automation インテグレーションの計画](#) (P. 144)

[CA Business Intelligence のインストール計画](#) (P. 149)

[実装方針](#) (P. 155)

[Firefox での Windows 認証の有効化](#) (P. 156)

CA SDM デフォルトおよび推奨ポート リスト

CA SDM をインストールするには、各種ポートおよびポート範囲をファイアウォール上でオープンにする必要があります。このポート情報は、サイト管理者やセキュリティ管理者が、CA SDM のインストールと設定だけでなく、ほかの CA Technologies ソリューションやサードパーティ製品との統合を行う際に役立ちます。

ファイアウォール上でオープンにする必要のあるポートは、*NX.env* ファイル内の設定によって異なります。デフォルトでは、CA SDM により、可用性に基づいて適切なポートが選択されます。1024 未満のポートはシステムによって予約されていますが、最大 65335 までポート番号をリクエストできます。

以下の *NX.env* 変数によって、開始ポート（2100）と、プロセスを起動するためのオープンポートの特定でシステムが使用する増分（プラス 1）が設定されます。

- NX_SLUMP_FIXED_SOCKETS=1
- NX_SLUMP_SECONDARY_SOCKET=2100

以下のリストに、CA SDM の標準インストールにおけるデフォルトおよび推奨ポート（およびポート範囲）を示します。

データベース

- Oracle : 1521
- SQL Server : 1433

CA SDM

- FTP : 21
- SMTP : 25
- HTTP : 80
- HTTPS : 8080
- HTTPS（セカンダリ） : 8081
- POP3 : 110
- IMAP : 143
- LDAP : 389
- WebEx : 1270
- mstsc : 1389
- oaserver : 1706
- Slump ソケット : 2100
- qserver : 2234
- Proctor ソケット : 2300
- 通信 : 2365
- Apache Tomcat : 8080
- Apache Tomcat シャットダウン :
- Apache Tomcat 上の SSL : 8443

CA CMDB

- Visualizer : 9080
- Visualizer Apache Tomcat シャットダウン : 9085
- CA Cohesion ACM : 9000
- CA Cohesion ACM Tomcat シャットダウン : 9005

CA EEM

管理ポート : 5250

CA Workflow

- Apache Tomcat : 8090
- Apache Tomcat シャットダウン : 8095

REST

- Apache Tomcat : 8050
- Apache Tomcat シャットダウン : 8055

CA Business Intelligence

注: BusinessObjects を処理するためのファイアウォール ポートの詳細については、「BusinessObjects Enterprise XI r2 展開および設定ガイド」を参照してください。

- Apache Tomcat : 8080
推奨 : 8070
- Apache Tomcat リダイレクト : 8443
- Apache Tomcat シャットダウン : 8075
- セカンダリ Apache Tomcat シャットダウン : 8005
- ODBC ドライバ : 1706
- BusinessObjects Central Management Server (CMS) : 8080
- BusinessObjects アプリケーション サーバ : 6400
- ODBC DSN (OpenAccess データベース) : 1706
- BEA WebLogic : 7001

<EBR> 検索

- ベース ポート : 13000

ポータル サーバ

- Apache Tomcat : 8080
- Apache Tomcat シャットダウン : 8085
- SSL 機能 : 8443
- Portal_Safe_List : 8444

サポート オートメーション

- メイン サーバ (ソケット サーバ) 内部 : 7005
- メイン サーバ (ソケット サーバ) 外部 : 10443
- ソケット プロキシ サーバ (ソケット 設定メイン サーバ) 内部 : 7005
- ソケット プロキシ サーバ (ソケット 設定メイン サーバ) 外部 : 10444
- メッセージルーティング サーバ (ソケット 設定) 外部 : 10444
- Apache Tomcat : 8070
- Apache Tomcat シャットダウン : 8075

Visualizer

- Apache Tomcat : 9080
- Apache Tomcat シャットダウン : 9085

高可用性を計画する方法

高可用性設定は、サーバの停止に対する回復性やアプリケーションの可用性を向上させると共に、ローリング メンテナンスをサポートすることによってエンドユーザの中断を最小限に抑えます。この設定には、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が必要です。プライマリおよびセカンダリサーバを備えた以前の設定は現在、標準設定と呼ばれます。

CA SDM は、標準設定または高可用性設定のどちらを使用するようにも設定できます。また、ある設定から別の設定に変換することもできます。

高可用性設定は、以下の方法により CA SDM の全体的な可用性を向上させます。

- 単一障害点を削減することによって、アプリケーション障害、ハードウェア障害、またはメンテナンスによる CA SDM アプリケーションのダウンタイムを最小限に抑えます。

- サーバのローリング メンテナンスをサポートすることによって、CA SDM のダウンタイムを最小限に抑えます。つまり、いずれかのサーバがメンテナンス状態にある間も、ユーザはアプリケーションでの作業を続けることができます。

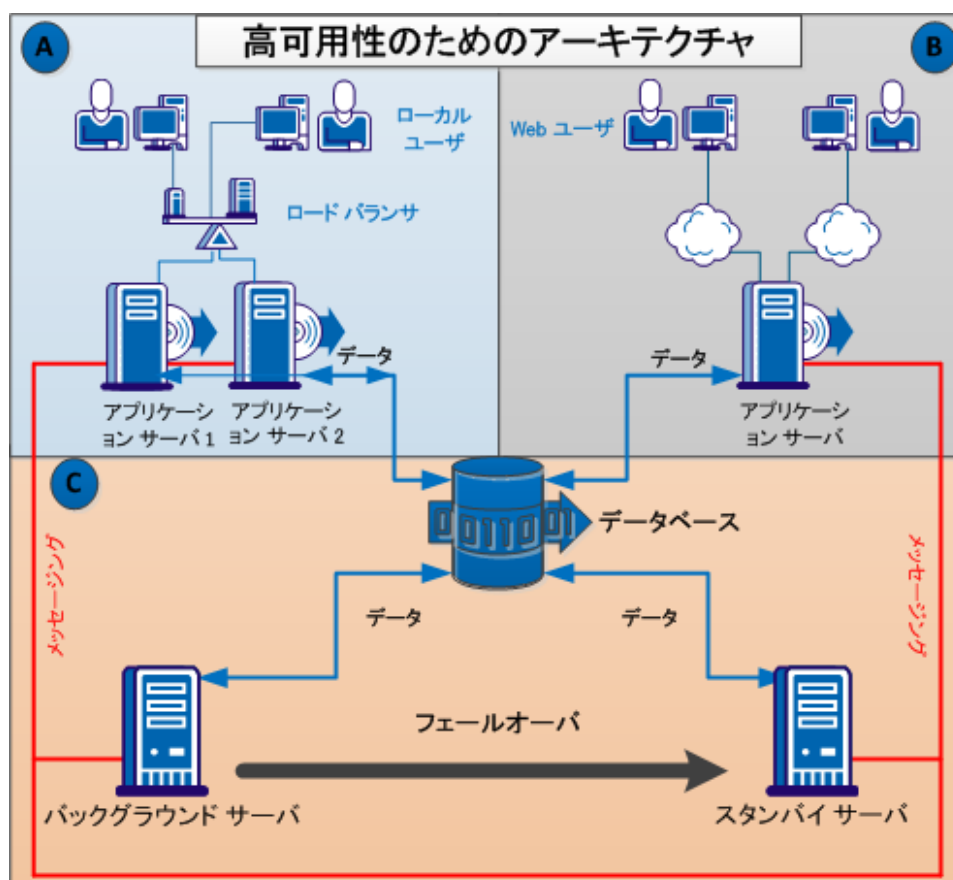
高可用性の計画および設定の詳細については、「実装ガイド」を参照するか、マニュアルの高可用性シナリオを直接確認してください。

高可用性設定をセットアップする前に、以下の計画に関する考慮事項を確認してください。

- [高可用性のための CA SDM アーキテクチャ](#) (P. 102)
- [高可用性設定を選択する条件](#) (P. 104)
- [高可用性設定の考慮事項](#) (P. 105)

高可用性のための CA SDM アーキテクチャ

高可用性設定には、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が含まれています。単一障害点を削減するために、これらの各サーバはデータベースに直接接続されています。アーキテクチャのすべてのコンポーネントは、内部の CA プロトコルを使用して通信します。以下の図は、CA SDM 実装の例を示しています。



このアーキテクチャは、3つの異なる場所 A、B、C にわたって分散しています。場所 A には、ロードバランサを介してユーザにサービスを提供している 2 つのアプリケーションサーバがあります。場所 B には、ユーザに直接サービスを提供しているアプリケーションサーバがあり、場所 C にはバックグラウンドサーバ、スタンバイサーバ、およびデータベースがあります。各サーバは、データベースに直接接続しています。青色の線は、データベースとの間のフローを示しています。赤色の線は、コンポーネント間の内部通信を示しています。

バックグラウンドサーバ

バックグラウンドサーバは、高可用性アーキテクチャの中核です。このサーバは、その他のサーバに補助的なサービスを提供し、CA SDM のすべてのシングルトンプロセスを実行します。プロセスをシングルトンとして指定できるのは、SDM インストールでその単一のコピーしかアクティブにできない場合です。管理者のアクセスタイプを持つユーザだけが、バックグラウンドサーバにアクセスできます。可用性を向上させるために、スタンバイサーバはバックグラウンドサーバをシャドウイングします。何らかの障害が発生した場合や、ローリングメンテナンスを実行する場合は、スタンバイサーバをバックグラウンドサーバとして切り替えることができます。

スタンバイサーバ

スタンバイサーバの主な機能は、バックグラウンドサーバのウォームスタンバイとして機能することです。スタンバイサーバは、バックグラウンドサーバと同じハードウェアおよび OS プラットフォームを備えています。スタンバイサーバは、バックグラウンドサーバ上で実行されるすべてのプロセスを実行できます。スタンバイサーバは、システムの通常の動作中はアイドル状態のままですが、データベース変更の内部の CA SDM システムメッセージをリスンすることによって、重要なキャッシュを更新し続けます。バックグラウンドサーバに障害が発生した場合や、ローリングメンテナンスが必要になった場合は、スタンバイサーバをバックグラウンドサーバに昇格させることによって、アプリケーションサーバおよびエンドユーザへの中断を最小限に抑えることができます。この切り替えを実行するために、ユーティリティを呼び出すことができます。

スタンバイサーバは、バックグラウンドサーバ上で通常実行されるプロセスの小さなサブセットだけを実行しています。スタンバイサーバ上で Web インターフェースにログオンすることはできません。

アプリケーション サーバ

アプリケーション サーバには、Web、SOAP、RESTful Web サービスなどのさまざまなインターフェース経由でエンド ユーザにサービスを提供するために必要な、すべての **CA SDM** コンポーネントが含まれています。アプリケーション サーバは互いに独立しており、短期間のバックグラウンドサーバの停止に対する回復性を備えています。ユーザは、アプリケーション サーバにアクセスします。アプリケーション サーバを個別に削除し、新しい休止機能を使用してサービスに戻ることができます。休止機能を使用すると、現在のユーザは自分の作業を完了し、代替アプリケーション サーバにサインインすることができます。

高可用性設定を選択する条件

高可用性設定により、可用性が向上し、ダウンタイムが削減され、ローリング メンテナンスがサポートされます。以下のいずれかの要因に当てはまる場合は、高可用性設定を検討してください。

- **CA SDM** に高い可用性が必要である。
- **CA SDM** サーバをより独立させ、障害に対するより高い回復性を持たせる必要がある。
- **CA SDM** のインストール全体をダウンさせることなく、**CA SDM** サーバを削除してサービスに戻す機能が必要である。
- ローリング メンテナンス中のダウンタイムをほぼゼロにする必要がある。

高可用性設定の考慮事項

高可用性設定の実装を決定する前に、以下の点を考慮することをお勧めします。

一般的な注意事項

標準設定の計画に関する考慮事項はすべて、高可用性設定にも有効です。標準設定の計画の詳細については、「実装ガイド」を参照してください。

- 1つのバックグラウンドサーバ、少なくとも1つ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が必要になるため、追加のハードウェアコストが予測されます。スタンバイサーバとバックグラウンドサーバの設定は同じである必要があります。
- リモートデータベースサーバと、Knowledge Tools インデックス ファイル、Knowledge Tools インポート/エクスポート ファイル、アーカイブ パージ出力ファイル、および添付ファイル リポジトリを共有するためのサーバが必要になります。バックグラウンドおよびスタンバイサーバからこれらのファイルにアクセスできるようにするには、共有された場所が必要です。Linux および UNIX インストールでは、NFS マウントを使用できます。Windows インストールには、UNC サポートが追加されています。
- バックグラウンドおよびスタンバイ動作のためにサーバが追加された場合でも、CA SDM のパフォーマンスは同じままになると予測されます。展開するアプリケーションサーバが増えた場合は、パフォーマンスが向上する可能性があります。
- 各サーバはデータベースに直接接続するため、DBMS レベルでのリソース競合が増加します。DBMS サーバのハードウェア構成を増やすことをお勧めします。詳細については、システム情報を参照してください。
- 標準設定の高可用性設定への変換は、手作業で行われます。通常、実装の規模が大きいほど複雑になるため、CA サービスに支援を求める必要がある可能性があります。

- 高可用性設定にマイグレートするには、標準設定で **CA SDM r12.9** にアップグレードしてから、高可用性設定に変換します。
- 各アプリケーションサーバの **ping** の時間や待ち時間を同じレベルにするために、バックグラウンドおよびスタンバイ サーバを同じネットワーク サブネットにインストールします。
- バックグラウンドおよびスタンバイ サーバを、すべてのユーザが良好にネットワーク接続できる中央の場所に配置することを検討してください。アプリケーションサーバは集中的に配置することも、世界中に分散させることもできます。
- 高可用性設定には、常に、**1**つのバックグラウンドサーバと少なくとも**1**つのスタンバイサーバが必要です。
 - (推奨) バックグラウンドサーバとその他のすべてのスタンバイサーバの両方が同じ設定になっていることを確認してください。この処理により、フェールオーバー中にスタンバイサーバが新しいバックグラウンドサーバになったとき、スタンバイサーバが古いバックグラウンドサーバと同様に機能できます。
 - スタンバイサーバは、任意の数だけ設定できます。**CA SDM** の可用性を向上させるために、バックアップデータセンターまたは惨事復旧サイトに**1**つのスタンバイサーバを配置することを検討してください。
 - 高可用性実装には、最低**1**つのアプリケーションサーバが必要です。可用性を向上させるために**2**つのアプリケーションサーバを、また **Web** トラフィックを制御するためにロードバランサを配置することをお勧めします。
 - **CA SDM** 管理者以外のユーザは、バックグラウンドサーバへのログインを許可されていません。また、スタンバイサーバへのログインが許可されたユーザはいません。

- すべての CA SDM サーバから電子メール通知を送信できます。このオプションを制限するか、または設定する方法は現在ありません。高度可用性構成のすべてのサーバは、メールサーバに接続をしている必要があります。
 - エンドユーザインタラクションに起因する電子メール通知は、ユーザが接続されているアプリケーションサーバから送信されます。
 - バックグラウンドプロセス（添付イベントを処理するアニメータなど）に起因する電子メール通知は、バックグラウンドサーバで実行中の `pdm_mail_nxd` ユーティリティによって送信されます。
 - バックグラウンドサーバの故障中に、バックグラウンドサーバがスタンバイサーバとしてアップ状態になった場合、キュー内の電子メールが送信されます。

フェールオーバーに関する考慮事項

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。

データベースに関する考慮事項

- 直接接続は、各サーバからほかのサーバに対してだけでなく、各サーバからデータベースに対しても存在します。CA SDM サーバが DMZ 内にある場合は、この接続用に、ファイアウォール ポートを開くか、トンネルプロキシテクノロジーを実装する必要があります。また、DBMS ベンダーとのライセンス契約も考慮してください。
- すべての CA SDM サーバにデータベース クライアントをインストールするようにしてください。
- 高可用性設定では、すべてのサーバが 1 つのデータベースに接続します。データベースは単一障害点になる場合があるため、DBMS の可用性を向上させるためにデータベース クラスタリングを利用することを検討してください。
- Windows プラットフォームでは、Microsoft SQL Server のみがネイティブにサポートされています。たとえば、実装が Windows や Linux などの異種のオペレーティング システムを含むサーバで構成されている場合は、Linux では Microsoft SQL Server がサポートされていないため、DBMS として Oracle を選択してください。
- pdm_isql ユーティリティはアプリケーション サーバでのみ動作します。

システム構成、管理、および操作

- SOAP Web サービスと RESTful Web サービスは、アプリケーション サーバでのみサポートされます。WebDirector は、すべての CA SDM サーバ上で設定できます。
- アプリケーション サーバは互いに独立しているため、WebDirector は、同じアプリケーション サーバ上で実行されている Web エンジンにしかサービスを提供できません。WebDirector は、アプリケーション サーバにわたる Web エンジンにはサービスを提供できません。
- 高可用性設定でのサーバの独立性は高いため、ほとんどのコマンドラインユーティリティはローカルサーバでのみ機能します。たとえば、`pdm_status` では、このコマンドを実行しているサーバ上で実行されている CA SDM プロセスのみが表示されます。`pdm_webcache` ユーティリティでは、それが発行されたサーバ上のフォーム キャッシュしか更新されません。
- プライマリ サーバで動作する `pdm_d_mgr` によって CA SDM プロセスを起動および停止する標準設定とは異なり、高可用性設定では各サーバ上のプロセスが個別に制御されます。
- アプリケーション サーバをシャットダウンするには、`pdm_halt` コマンドの代わりに新しい `pdm_server_control` を使用することをお勧めします。シャットダウンの前に、アクティブなユーザに別のアプリケーションサーバに移動するよう求めることができます。これは、休止オプションを使用してユーザに通知することによって実行できます。
- `pdm_edit` ユーティリティが新しいグラフィカルユーザインターフェースに置き換えられたため、以前は必要だった設定ファイルの手動による変更の多くがなくなりました。

- 標準設定とは異なり高可用性設定では、バックグラウンドサーバの Web UI の [オプション マネージャ] から `bopauth_host` オプションを使用して、認証サーバの詳細を指定できます。高可用性設定のために、`pdm_edit` でこの設定変更を行う必要はありません。認証サーバが使用できない場合、ユーザはログインできません。

注: 標準設定では、セカンダリ サーバを使用して、CA SDM を別のシステムや別のハードウェア プラットフォーム上で実行されている認証システムに統合させることができます。

- 不正なサーバが高可用性設定に参加できないようにするために、サーバはすべて、設定する前にバックグラウンドサーバの Web UI で定義する必要があります。
- 高可用性設定でのサーバの役割やその他の情報は、[管理] タブで変更できます。サーバ定義を変更する前に、CA SDM サービスを停止します。変更を有効にするには、サーバの再設定が必要です。
- 設定ユーティリティを実行することによって、サーバを標準設定と高可用性設定の間で変更できます。必ず、実装内のすべてのサーバを変更してください。データは影響を受けずに残りますが、設定を変更するには手動の更新が必要になります。
- CA SDM r12.9 へのマイグレート時は、最新の `pdm_startup` ファイルを使用します。以前のバージョンの CA SDM のファイルを使用しないでください。たとえば、`pdm_edit` ユーティリティによって生成されたファイルなどです。
- 高可用性をサポートするために `NX.env` に新しい環境変数が追加されています。これらの変数値はシステムによって自動的に管理されます。

重要: 指示がない限り、`NX.env` を手動で変更しないでください。

- 新しい機能によって、チケット番号および数値レコードキーが生成されます。データベースが破損する可能性を回避するために、**Key_Control** テーブルをロードしたり、手動で変更したりしないでください。
- 高可用性設定では、**Knowledge Tools** デーモンを別のサーバに移動することはできません。**kt_daemon** は現在、すべてのサーバ上で実行されます。その他のすべての **Knowledge Tools** デーモンは、バックグラウンドサーバ上でシングルトンとして実行されます。
- **Knowledge Tools** は現在、ナレッジエクスポート/インポート機能によって使用される **EBR** インデックス ファイルおよび入出力ファイルの場所への **Windows** 上の **UNC** ファイルパスをサポートしています。この機能は、高可用性設定と標準設定の両方に使用できます。

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。

- バージョン管理により、**server_secondary_custom.ver** ファイルで設定されるファイル (**html**、**.maj**、**.mod**、**.sch** など) がバックグラウンドサーバから配布されます。起動時、スタンバイまたはアプリケーションサーバは、更新されたファイルをバックグラウンドサーバから取得するためにバージョン管理クライアントを実行します。
- アーカイブ/ページは、バックグラウンドサーバ上で実行され、出力ファイルへの **Windows** 上の **UNC** ファイルパスをサポートします。この機能は、高可用性設定と標準設定で使用できます。
- リポジトリがリモートサーバ上に存在する場合、受信電子メールの添付ファイルは、**pdm_maileater** によって格納されます。
- デーモンマネージャが **procsets** を変更できるようにし、このアクションに対して **pdm_dmnmode** コマンドを実行しないようにします。

一般的な Web ユーザ インターフェースに関する考慮事項

- Web サーバは、高可用性設定のすべてのサーバ上で必要です。
- フェールオーバーのためにバックグラウンドサーバが使用できない場合は、[遅延したサーバ応答] フォームが Web ユーザに表示されます。スタンバイサーバがバックグラウンドサーバに昇格されると、ユーザは自分の作業の再開を許可されます。
- web_cgi_url オプションの値は、以下を指している必要があります。
 - 複数のアプリケーションサーバが存在する場合は、ロードバランサ。
 - アプリケーションサーバが 1 つしか存在しない場合は、アプリケーションサーバ。

添付ファイルに関する考慮事項

- 共有ファイルリポジトリにアクセスするためのドキュメントリポジトリプロセスを複数設定することによって、添付ファイルの可用性を向上させることができます。

Web Screen Painter に関する考慮事項

- Web Screen Painter (WSP) は、バックグラウンドサーバ上でのみ使用できます。
- WSP のフォーム変更を発行して、更新されたフォームがインストール内のすべてのサーバに配布されるようにするには、推奨される手順に従ってください。詳細については、シナリオ「**Web Screen Painter を使用して、スキーマをカスタマイズする方法**」、および「**Web Screen Painter を使用して、Web インターフェースをカスタマイズする方法**」を参照してください。
- すべてのサーバ上で実行される仮想データベース層デーモン。CA SDM データベースのカスタマイズとオブジェクト定義をすべてのサーバにインストールします。

レポートの考慮事項

- CA Business Intelligence は、代替アプリケーション サーバからデータを自動的に取得できます。この機能を設定すると、CA SDM レポートの可用性を向上させることができます。
- BOXI は、バックグラウンド サーバに統合されていません。このため、バックグラウンド サーバの Web UI からレポートを表示できません。バックグラウンドサーバの Web UI から [レポート] タブを選択すると、エラー メッセージが表示されます。

オプション マネージャに関する考慮事項

- オプション マネージャからオプションをインストールまたはアンインストールできるのは、バックグラウンドサーバの Web UI からだけです。変更を設定内のすべてのサーバに伝播するには、ローリング メンテナンスの手順を使用します。ローリング メンテナンスの実行の詳細については、「CA SDM サーバでのローリングメンテナンスの実行」のシナリオを参照してください。

Web サービスに関する考慮事項

- Web サービスは、アプリケーション サーバ上でのみ設定できます。
- webservices_domsrvr オプションは、オプション マネージャには存在しなくなりました。NX.env を変更することによって、各アプリケーション サーバ上で NX_WEBSERVICES_DOMSRVR 変数を独立して設定できます。

一般的な統合に関する考慮事項

- CA SDM Web ユーザ インターフェースへの URL は、正しく設定されたアプリケーション サーバを指している必要があります。
ca_application_registration には、他の CA 製品によって使用される CA SDM のインストールへの URL が含まれています。この URL は、最初に設定される CA SDM サーバ (最も一般的にはバックグラウンドサーバ) を指しています。管理機能を使用してこの値を変更できるのは、CA SDM 管理者だけです。ロードバランサを使用している場合は、この URL が単一のアプリケーション サーバではなく、ロードバランサを指すようにします。詳細については、オンラインヘルプを参照してください。

- ほとんどのエンド ユーザ インタラクション、およびほかのソフトウェア製品との統合は、アプリケーション サーバレベルで実行されます。アプリケーション サーバのフェールオーバーはありません。アプリケーション サーバが使用できなくなると、そのアプリケーション サーバの Web サービスも使用できなくなります。アプリケーション サーバの可用性を向上させるためにロード バランサを展開して、異なるアプリケーション サーバ間でリクエストをルーティングできます。
- IP アドレスが関係するため、NSM は 1 つのアプリケーション サーバにしか統合できません。そのサーバがダウンしているときは、NSM 統合を使用できません。
- アプリケーション サーバのいずれかに CA Workflow をインストールする必要があります。そのアプリケーション サーバがダウンすると、CA Workflow 統合は使用できなくなります。

変換における注意事項

- バックグラウンド サーバは、プライマリ サーバにのみ変換できます。
- プライマリ サーバは、バックグラウンド サーバにのみ変換できます。
- セカンダリ サーバは、スタンバイ サーバまたはアプリケーション サーバにのみ変換できます。
- スタンバイ サーバまたはアプリケーション サーバは、セカンダリ サーバにのみ変換できます。

統合検索に関する考慮事項

- 統合検索機能を有効にして使用するには、アプリケーション サーバの設定時に統合検索オプションを選択します。

CA MDB のインストールの計画

CA MDB を正常にインストールおよび設定するには、以下の情報を使用して情報を調査および収集してください。

- **調査** - 「CA 管理データベースの概要」を確認し、CA MDB についてよく理解し、展開方針を決定します。また、CA MDB を CA SDM で使用する際に注意する必要がある SQL Server または Oracle に関する問題についても確認します。

- **SQL Server** - SQL Server で製品とコンポーネントを正しく構成できるように、以下の手順を実行します。
 - インストールおよび構成を実行するコンピュータで TCP/IP を有効にします。
 - 以下の情報を使用できます。
 - SQL Server を実行しているサーバの名前付きインスタンス
 - SQL Server のデータベース ユーザ名およびパスワード
 - SQL Server のデータベース ポート番号
 - **Oracle** - 以下の情報を使用できます。
 - Oracle データベースはローカルかリモートか
 - 表領域の作成は必要か
 - ネット サービス名
 - DBA ユーザ名およびパスワード
 - データ表領域名およびインデックス表領域名
 - 表領域の完全パス
 - システム識別子 (SID) やリスナ ポートなどの JDBC 接続情報
- 注: 入力するデータベース情報がわからない場合は、サーバ構成のオンラインヘルプを参照してください。

関連項目:

[CA MDB をインストールする方法 \(P. 179\)](#)

CA MDB に関する考慮事項

CA MDB をインストールする前に、正しく実装できるよう以下の情報を考慮してください。

- **AIX** - AIX コンピュータでは、ARG/ENV リストの最大許容スペースが CA MDB をインストールするのに不十分である場合があります。このような場合に、ARG/ENV リストの現在の最大サイズの設定を知るために、コマンド `lsattr -lsys0 -ancargs -Fvalue` を実行します。戻り値が 50 に満たなければ、次のコマンドを実行してサイズを増やしてください:
`chdev -l sys0 -a ncargs=50`。

- **Oracle** - 以下の情報を考慮してください。
 - CA MDB のパッチを適用する前に、**Oracle** バックアップを実行します。バックアップは、**DBA** またはパッチ スクリプトによって行うことができます。パッチ スクリプトでは、**Oracle Recovery Manager (RMAN)** によって、**OS** 認証を使用してデータベースをバックアップします。**RMAN** の設定でデータベースのアーカイブ ログ (**ARCHIVELOG** モード) が有効になっている必要があります。あるいは、データベース管理者によってバックアップ済みである場合、**-ORA_BACKUP** のパラメータに「no」を指定することで、パッチ スクリプトによるバックアップをしない設定にすることもできます。
注: パッチは **RMAN** コマンドで **OS** 認証を使用します。
 - CA MDB インストールを実行する **Oracle** ユーザには、以下のデータベース管理者権限を割り当てる必要があります。
 - **DBA** 役割 (`connect sys as sysdba; grant dba to installation_user;`)。
 - **SYSDBA** 役割 (`connect sys as sysdba; grant sysdba to installation_user;`)。
 - **mdbadmin** ユーザに、さまざまなシステム テーブルおよびビューへの権限を付与する機能 (`connect sys as sysdba; grant all privileges on "sys"."TABLE_NAME" to installation_user with grant option;`)。TABLE_NAME として想定される値は、COL\$, DBA_CONSTRAINTS、DBA_CONS_COLUMNS、DBA_INDEXES、DBA_IND_COLUMNS、DBA_OBJECTS、DBA_OBJECT_TABLES、DBA_REGISTRY、DBA_TABLES、DBA_TABLESPACES、DBA_TAB_COLUMNS、DBA_TAB_PRIVS、DBA_VIEWS、DBMS_REGISTRY、EXPDEPACT\$, EXPDEPOBJ\$, EXPPKGACT\$, EXPPKGOBJ\$, KOPM\$, OBJ\$, TS\$, USER\$ です。
- **リモートクライアント (UNIX および Linux のみ)** - リモートクライアントから **CA MDB** を作成すると、**CA MDB** 作成プロセスはコード 95 を返して終了し、テーブル領域パスで指定されたディレクトリがクライアント コンピュータにも **Oracle** サーバにも存在しない場合は「Failed to create the table space (テーブル領域の作成に失敗しました)」というメッセージがインストール ログに記録されます。
- **CA MDB コンポーネント インストール (SQL)** - **CA MDB** コンポーネント インストーラ インターフェースに、[データベース サーバ名] フィールドが表示されます。クラスタ化されている場合は、このフィールドはローカルサーバ名またはクラスタ ノード名を示しています。**SQL Server** に接続する際に使用するネットワーク名を使用してください。

- **特殊文字（UNIX、Linux、および Windows）** - 以下の情報を考慮してください。
 - （UNIX および Linux） CA MDB の作成を行うデータベース管理者のユーザ ID に、特殊文字を含めることはできません。また、以下の制限が適用されます。
 - DBA ユーザおよびテーブル領域名では、# および _ の特殊文字がサポートされます。その他の特殊文字は、サポートされません。
 - DBA パスワードおよび MDBADMIN パスワードでは、~、#、%、^、-、+、_、{、}、[、]、:、.、および ? がサポートされます。特殊文字その他の特殊文字は、サポートされません。
 - Oracle 表領域パス、MDB ターゲットディレクトリ、MDB ソースディレクトリ、および MDB パッチディレクトリ DIR では、~、%、^、_、-、+、[、]、{、}、: の特殊文字がサポートされます（パスが二重引用符で囲まれている場合はスペース文字もサポートされますが、連続したスペース文字はサポートされません）。
 - （Windows） CA MDB の作成を行うデータベース管理者のユーザ ID に、特殊文字を含めることはできません。また、以下の制限が適用されます。
 - DBA ユーザおよびテーブル領域名では、#、\$、および _ の特殊文字がサポートされます。その他の特殊文字は、サポートされません。
 - DBA パスワードおよび MDBADMIN パスワードでは、~、!、#、\$、*、()、_、+、`、-、{、}、[]、¥、:、'、?、.、/、および @ の特殊文字がサポートされます。その他の特殊文字は、サポートされません。
 - Oracle 表領域パス、MDB ターゲットディレクトリ、MDB ソースディレクトリ、および MDB パッチディレクトリでは、~、!、#、\$、()、_、+、`、-、{、}、および [] の特殊文字がサポートされます（パスが二重引用符で囲まれている場合はスペース文字もサポートされます）。

- **テーブル領域** - 以下の情報を考慮してください。
 - CA MDB では、一時テーブルを保存するために、システムの一時テーブル領域が使用されます。このためには、50 MB 以上の空き領域が必要です。CA MDB に既存のテーブル領域を使用することを決定した場合、テーブル領域には最低 200 MB のディスクの空き領域が必要です。使用可能な領域がこの要件に満たない場合は、CA MDB の作成に失敗します。
 - データ テーブル領域またはインデックス テーブル領域の作成に CA MDB 作成プロセスが使用され、サイズ パラメータが数字で指定されていない場合、コード 350 が返され、CA MDB インストール ログには作成プロセスがテーブル領域の作成に失敗したことを示すエラー（rc=189）が記録されます。
- **ユーザ権限および管理者権限** - 管理者権限を持たないユーザによって CA MDB 作成プロセスが開始された場合、作成プロセスは失敗します。CA MDB インストール ログに、エラー「ORA-00942: table or view does not exist（テーブルまたはビューが存在しません）」が記録されます。

関連項目：

[CA MDB をインストールする方法](#) (P. 179)

CA SDM のインストールの計画

CA SDM を正常にインストールおよび設定するには、以下の情報を使用して情報を調査および収集してください。

- **ログイン権限** - 以下の手順を実行します。
 - (Windows) 管理者としてログインし、完全な管理者権限を取得します。
 - (UNIX) root ユーザとしてログインし、root アカウントへの適切な権限を取得します。

■ **調査** - 以下の手順を実行します。

- リリース ノートとオプションの **readme** ファイル（ある場合）の両方を参照します。この情報を参照して理解するまでは、インストールを開始しないでください。

注: システム要件を含む最新のリリース ノート、およびオプションの **readme** ファイル（ある場合）は、<http://ca.com/support> で参照できます。

- インストール メディアがあることを確認します。

注: コンピュータにインストール メディア用の適切なドライブがない場合は、**CA SDM** をインストールするコンピュータにメディア コンテンツをコピーします。その後、インストールを開始します。ネットワーク経由のリモート インストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始する必要がある場合もあります。

重要: インストール ファイルのうち見つからないものがある場合、**CA SDM インストール DVD** を **Windows XP オペレーティング システム** にマウントしないでください。インストールが失敗します。

- **CA SDM** との使用を認定されたサードパーティ製ソフトウェア製品のリスト用の **Certification Matrix** を確認します。

注: 最新の **Certification Matrix** は、<http://www.ca.com/jp/support/> で参照できます。

- 製品コンポーネントの情報に目を通し、基本的知識を理解します。
- 製品がサポートする各種実装方針を把握します。組織に最適な実装方針を決定する際には、ネットワークの可用性、使用可能な帯域幅、および応答性を考慮します。
- インストールするコンポーネントごとに、実装に関する考慮事項を確認します。

■ **インストール ホーム ディレクトリ** - 以下の手順を実行します。

- 製品をインストールするホーム ディレクトリを決定します。製品のデフォルトのホーム ディレクトリは **C:\Program Files\CA\Service Desk Manager** です。
- 製品（**Java Runtime Environment (JRE)** や **Apache Tomcat** など）が使用する共有コンポーネントをインストールするホーム ディレクトリを決定します。共有コンポーネントのデフォルトのホーム ディレクトリは **C:\Program Files\CA\SC** です。

- **データベース - CA SDM で使用するデータベース (SQL Server か Oracle のどちらか) を決定し、データベースをインストールします。続いて、以下の手順を実行します。**
 - SQL Server インストールおよび構成を実行するコンピュータで TCP/IP を有効にします。
- **プライマリ/セカンダリ サーバおよびユーザ設定 - 以下の手順を実行します。**
 - 製品のインストールの最後にプライマリ サーバおよびオプションのセカンダリ サーバの両方を確実に設定するために、以下の情報を用意しておきます。
 - プライマリ サーバおよびセカンダリ サーバのドメイン ネーム システム (DNS)
 - サーバの名前または別名
 - 接続を確立するオブジェクト マネージャの名前または別名
 - セカンダリ サーバの名前または IP アドレス
 - すべての CA SDM によって通信に使用される Slump ソケット ポート
 - セカンダリ サーバによってプライマリ サーバからのメッセージのリスニングに使用される Proctor ソケット ポート
 - 製品のインストールの最後に製品管理用のアカウント情報を確実に設定できるように、特権のある制限ユーザの名前とパスワードを用意しておきます。
 - (UNIX および Linux) 特権ユーザを手動で作成します。Windows では、このユーザは製品の設定中に自動的に作成されますが、Linux では手動でこのユーザを作成する必要があります。

注: 高可用性のためのサーバ設定については、「高可用性用にサーバを設定する方法」のシナリオを参照してください。

- **Web インターフェース設定** - 以下の手順を実行します。
 - 製品のインストールの最後に Web インターフェースを確実に設定できるように、以下の情報を用意しておきます。
 - Web ホスト名および Web サーバ
 - (Windows NT のみ) CA SDM サーバによって使用される Web サイト
 - シャットダウンリクエスト用の Tomcat ポート番号およびソケット ポート番号
- **ブラウザおよびアンチウイルス ソフトウェア** - 以下の手順を実行します。
 - (Firefox) 任意で Windows 認証 (エンタープライズシングル サインオン) を有効にします。
 - インストールの速度が低下するため、アンチウイルス ソフトウェアを一時的に無効にします。インストール後は、必ずアンチウイルス ソフトウェアを再度有効にしてください。
- **Web Screen Painter** - CA SDM をインストールする際、Web Screen Painter が自動的にプライマリ サーバ上にインストールされます。インストールメディアを使用して、別のコンピュータに Web Screen Painter をインストールできます。
- **ファイル名の作成** - CA SDM では 8.3 形式のファイル名作成が必要です。8.3 形式のファイル名作成および disable8dot3 レジストリ エントリの詳細については、オペレーティング システムのヘルプおよびサポート ドキュメントを参照してください。

関連項目:

[CA SDM をインストールする方法](#) (P. 188)

[サーバ コンポーネント](#) (P. 18)

[実装方針](#) (P. 155)

[Firefox での Windows 認証の有効化](#) (P. 156)

CA SDM に関する考慮事項

CA SDM をインストールする前に、正しく実装できるように以下の情報を考慮してください。

- **Apache サーバ (UNIX および Linux)** - UNIX または Linux で Apache サーバを使用している場合、インストールされている Apache によってはルートディレクトリからの FollowSymLinks オプションが無効である場合があります。この場合、設定ファイルが CA SDM のインストール中に作成された /opt/CAisd シンボリックリンクを使用しているため、このままでは Apache は CA SDM に統合されません。CA SDM を Apache と連携できるようにするには、ルートディレクトリからの FollowSymLinks オプションを有効にするか (httpd.conf ファイルで設定する必要があります)、\$NX_ROOT/bopcfg/www/CAisd_apache.conf ファイルを変更して、シンボリックリンクを実際のパスに置き換えます。CAisd_apache.conf ファイルでは /opt/CAisd という記述をすべて、CA SDM の実際のパス (たとえば、/opt/CA/ServiceDeskManager) に置き換えます。変更を加え保存したら、変更を適用するために Apache サーバを停止して開始します。
- **ブラウザ** - 以下の情報を考慮してください。
 - (Firefox) 以下の情報を考慮してください。
 - [ナレッジカテゴリ] の HTML エディタ ページで切り取り、コピー、貼り付け機能を使用すると、「*Unprivileged Script*」エラーが発生する場合があります。[OK] をクリックして mozilla.org の技術情報を表示してください。スクリプトがクリップボードにアクセスできるようにする方法が掲載されています。
 - Latin-1 特殊文字をファイル名に含む添付ファイルを表示すると、[名前をつけて保存] のポップアップダイアログボックスが表示されます。ファイルをディスクに保存するか、[開く] をクリックしてファイルを開くアプリケーションを選択してください。
 - (Windows 2003 上の Internet Explorer 8) インターネットセキュリティのレベルが「高」に設定されている場合、Web ページを正しく表示するには、CA SDM URL および「*about:blank*」を「信用済みサイト」に追加する必要があります。

- (Google ツールバー) CA SDM Web インターフェースのウィンドウ上部にタイトルバー テキストが正常に表示されない可能性があります。
- (Internet Explorer 8.0) CA SDM Web インターフェースにアクセスすると、断続的にメモリの使用量が増加することがあります。これは現行バージョンの Internet Explorer の既知の問題です。メモリを開放するには、定期的に CA SDM のメイン Web ページを最小化してください。
- **CA Workflow** - 以下の情報を考慮してください。
 - 設定中、特権ユーザの認証情報が間違っていた場合、CA SDM は起動する場合がありますが、CA Workflow は起動に失敗します。認証情報が間違っていると、以下のような状態が発生します。
 - CA Workflow はインストールされません。
/site/Workflow/wekinstall.log に「bad username/password」エラーが記録されます。
 - Tomcat が CPU を過剰使用したり、ログ ファイル
/log/pdm_tomcat_CAWF.log に大量のセキュリティ マネージャ例外および「AbandonedObjectPool is used」というメッセージが記録されます。

この状況を修正するには、特権ユーザの認証情報を使ってオペレーティング システムに再ログインし、特権ユーザのユーザ名およびパスワードを確認します。次に、CA SDM 設定を実行し、正しい特権ユーザ名/パスワードを指定します。特権ユーザ パスワードが変更されている場合は、設定を実行して新しいパスワードを設定する必要があります。

- CA Workflow のインストールが完了した後、特権ユーザの認証情報が変更された場合、CA Workflow プロセスは失敗する場合があります。以下の手順に従います。
 - a. CA Workflow IDE にログインし、デフォルトの CA SDM Web サービス アクターを変更します。
 - b. [アクター] タブを選択し、JavaScript ツリーを展開し、[USDInitializer] をクリックします。
 - c. [グローバル属性の取得] をダブルクリックします。

- d. スクリプトセクションの以下のフィールドに、CA SDM 特権ユーザ名およびパスワードを入力します。

USD_Username = ""

USD_Password = ""

- e.

\$NX_ROOT¥data¥workflow¥actors¥r12_Service_Desk_Actors_en_US.xml ファイル内のこれらの値を変更します。

- データベース（サポート対象すべて） - 以下の情報を考慮してください。
 - CA SDM のデータベースを構成した後にもう一度構成作業を行い、その際に別のデータベースタイプを選択すると、構成は機能しません。たとえば、最初の構成時に **SQL Server** を指定し、その後 **Oracle** データベースを指定したような場合です。これを回避するには、2 回目の構成を行う前にコンピュータを再起動してください。
 - データベース接続情報が異なる場合は、それに続く構成では受け付けられません。データベース接続情報の変更によって、追加的な構成が必要となった場合は、まず **\$NX_ROOT¥NX.env** ファイルを削除してください。
 - **Argis 8.0** から **CA Asset Portfolio Management r11.2** にアップグレードし、**CA MDB**（データベース）を **CA SDM** と共有している場合、**CA SDM** を使用してアセットファミリにアセットを追加したり、アセットを更新したりする際に問題が発生する場合があります。このエラーの発生を回避するには、以下のいずれかの方法で **CA SDM** に拡張テーブルを定義する必要があります。
 - **WSP** を使用してテーブルおよびフォームを定義し、テーブルエントリを参照および編集します。
 - 以下のガイドラインに従って、テーブルおよびフォームを手動で編集します。
 - a. **\$NX_ROOT¥bopcfg¥majic¥assetx.maj** ファイルに、**majic** ファイルの作成に使用されるテンプレートが含まれています。これによって **CA SDM** のアセット拡張テーブルの列を特定します。このファイルをコピーし、ファイルにある指示に従って適切に編集します。

- b. データベースの列を定義するために、`$NX_ROOT¥site¥mods` ディレクトリに `.sch` ファイルを作成します。
`$NX_ROOT¥site¥assetx_schema.sch` および
`$NX_ROOT¥site¥assetx_index.sch` はテンプレートとして使用でき、コピーして、アセット拡張テーブルに合わせて適切に編集することができます。

注: アセット拡張データを表示するためのフォームを作成するには、WSP を使用します。

■ **SQL Server** - 以下の情報を考慮してください。

- 新しいバージョンの SQL Server では、以前のバージョンの SQL Server よりも厳密なユーザ パスワード認証が使用されます。CA SDM データベース パスワードが、SQL Server で定義されたパスワード ポリシーに準拠していることを確認してください。CA SDM データベース パスワードが SQL Server 2005 パスワード ポリシーに準拠していない場合、CA SDM の環境設定は機能しません。
- (SQL Server 2005 上の Microsoft クラスタ環境) クラスタがフェールオーバーする際に、どのクラスタ化ノードがアクティブであるかにかかわらず、CA SDM が今までどおり同じサーバ名に接続できるように、クラスタ内に SQL Virtual ノード名の別名を作成する必要があります。

■ **Oracle** - 以下の情報を考慮してください。

- Oracle データベースを使用する設定で CA SDM を UNIX ベースのシステムにインストールする場合は、Oracle のインストールの際に指定されたグループに、特権ユーザが属している必要があります。Oracle インストール グループは、*oralnst.loc* という名前のファイルで確認することができます。
- 64 ビット コンピュータで 64 ビット Oracle データベースを構成する場合、システム ライブラリ パス（Oracle Solaris および Linux では LD_LIBRARY_PATH、AIX では LIBPATH）に 32 ビット Oracle ライブラリが指定されている必要があります。32 ビット Oracle ライブラリは \$ORACLE_HOME/lib32 にあります。このことは設定時および実行時ともに同様です。
- 64 ビット コンピュータで 64 ビット Oracle 11g データベースを構成する場合、サーバに Oracle 32 ビット クライアントをインストールする必要があります。データベースを構成する場合、システム ライブラリ パス（Oracle Solaris および Linux では LD_LIBRARY_PATH、AIX では LIBPATH）に 32 ビット Oracle ライブラリが指定されている必要があります。この手順は、構成とランタイムの両方に必要です。また、Oracle クライアントに ネット サービス名を作成し、Oracle データベース サーバインスタンスを指定します。
- Oracle データベースで、既存の表領域を使用する場合は、CA SDM を環境設定する前に、少なくとも 400 MB のデータ表領域と 100 MB のインデックス表領域をそれぞれ用意しておく必要があります。

- **外部マウント ドライブ** - 20 以上の外部マウント ドライブがある Linux に CA SDM をインストールする場合、インストール ウィザード ページが表示されてからインストール進捗状況ページが表示されるまでに時間がかかる場合があります。これは正常な動作であり、その後インストールは再開されます。

- **Install Shield および InstallAnywhere** - 以下の情報を考慮してください。
 - CA SDM のインストールを実行しようとして Install Shield エラーが発生した場合は、*msiexec.exe* が実行を停止するまで待ってください。それから製品のインストールを行ってください。
 - UNIX または Linux 上で CA SDM インストールを開始した後、停止すると、インストールのルートに *install.dir.#####* というディレクトリが作成される場合があります。これは InstallAnywhere の機能です。これらのファイルは必要ありません。削除しても支障ありません。
- **インストール ホーム ディレクトリ** - CA SDM をインストールする際には、CA 共有コンポーネントを CA SDM のインストール ディレクトリ (NX_ROOT) と同じディレクトリにインストールしないでください。
- **インターナショナル** - 以下の情報を考慮してください。
 - マルチバイトのオペレーティング システム（簡体字中国語や日本語など）にインストールするとき、自分のユーザ名や CA SDM 特権ユーザのユーザ名にマルチバイト文字を使用しないでください。使用するとインストールが失敗します。
 - マルチバイト文字をインストール時や設定時のパスに含めないでください。含めると、インストールや環境設定が失敗します。
 - CA SDM は、Linux および UNIX プラットフォームでは UTF-8 ロケールで実行される必要があります。
 - デフォルトの CA SDM インストールでは、[期間] 名（[管理] タブの [Service Desk] - [アプリケーション データ] - [コード] - [期間]）は英語で表示されます。例えば、TODAY、YESTERDAY、THIS MONTH などのように表示されます。製品のローカライズ版では、管理者は必要に応じて [期間] 名をローカライズすることができます。デフォルトの期間を削除または変更しないでください。
 - CA SDM の日付フォーマットでは、ローカライズされた日付書式指定子（フランス語の *jj/MM/AAAA* など）のような国際指定子をサポートしていません。構文は、「*DD/MM/YYYY*」のような一般的な指定子に限られます。しかし、国際的に使用される様々な短い日付形式の多くは、これらの一般的な指定子から作成できます（例えば、「*YYYY.MM.DD*」のように、日本語の一般的な短い日付形式を作成できます）。

- テキスト形式の電子メール送信通知では、国際環境で利用される文字エンコードが電子メールのメッセージに正しく指定されるように、`NX_SMTP_HEADER_CHARSET` および `NX_SMTP_BODY_CHARSET` のオプションを `NX.env` ファイルで直接編集する必要がある場合があります。正しい文字コードが指定されていないと、受信者の電子メールシステムでメッセージが正しく表示されない可能性があります。これらのオプションのデフォルト値は、すべてのプラットフォーム上で UTF-8 に設定されています。
- UNIX または Linux で英語版以外の Oracle を使用している場合は、`pdm_init` を実行する前に `NLS_LANG` 環境変数を設定する必要があります。Oracle データベース管理者は Oracle のドキュメントで `NLS_LANG` の設定値を確認してください。

重要: `NLS_LANG` を設定しないと、Oracle クライアントはデフォルトで `American_America.US7ASCII` に設定されます。たとえば、環境でマルチバイト日本語をテストする場合は、`NLS_LANG` を `JAPANESE_JAPAN.UTF8` にセットします。

注: `NLS_LANG` 変数の設定は、`pdm_init` を実行する前に同じシェルで行う必要があります。たとえば、`setenv NLS_LANG GERMAN_GERMANY.WE8ISO8859P1` のように設定します。

- 国際ユーザは、必要に応じて `web.cfg` の `DateFormat` プロパティを変更して、日付や日時のフォーマットを地域に合わせて調整してください。
- 国際ユーザは、必要に応じてスペルチェック語彙集（オプションマネージャの `LEX_LANG` オプション）を地域に合わせて調整してください。
- CA SDM サーバ英語版は、英語以外の 9 言語の環境で動作することが確認されています。Windows については、サポートされている Windows Server オペレーティングシステムの完全ローカライズ版であることが必要です。具体的には、英語コア上で `Language Interface Pack` や `MUI` が動作している Windows オペレーティング環境はサポートされていません。

また、CA SDM のローカライズ版は、該当するローカライズ版の Windows Server オペレーティング環境でのみサポートされています。すべての場合において、コントロールパネルの「地域と言語のオプション」ウィンドウで「Unicode 対応でないプログラムの言語」（デフォルトのシステム Windows ANSI コード ページ）を正しく設定することで、認証された言語がサポートされます。

注: Windows Server オペレーティング システムのローカライズ版の詳細については、Microsoft の Global Development and Computing Portal の Localized Microsoft Operating Systems のリストを参照してください。

- CA SDM およびナレッジマネジメントで SQL Server を使用している場合、日本語文字を含むナレッジ検索が正常に動作するためには、SQL Server が Windows 照合順序を選択してインストールされている必要があります。SQL Server のインストール時に、データの照合順序オプションを必ず指定してください。

- **IPv4 - Linux** へのインストールでは、`/etc/hosts` ファイルに、IP アドレス、コンピュータ名、完全修飾コンピュータ名による IPv4 エントリを含める必要があります。エントリの例は、以下のようになります。

```
127.0.0.1 localhost.localdomain localhost
141.202.211.11 usbegp11.ca.com usbegp11
```

- **短いファイル名** - Windows オペレーティング システムで短いファイル名を無効にしている場合は、CA SDM をインストールする前に有効にしてください。短いファイル名を有効にするとともに、環境変数 `TEMP` および `TMP` も短いファイル名に設定する必要があります（例：「`c:\temp`」）。これは短いファイル名を有効にした後、インストールを実行する前に行ってください。

注: 詳細については、Microsoft のヘルプとサポート Web サイトで Microsoft サポート技術情報の記事 121007 を参照してください。

- **特殊文字およびスペース（ディレクトリ、メディアパス、およびフォルダ名）** - 以下の情報を考慮してください。
 - （UNIX および Linux）インストール メディアをローカルハードドライブにコピーする場合、ディレクトリパスにスペースや特殊文字（`#` など）が含まれていないことを確認してください。場所にスペースまたは特殊文字が含まれていると、インストールは正常に実行されません。
 - （UNIX、Linux、および Windows）インストール メディアパスおよびフォルダ名内にスペースを指定しないでください。指定した場合、インストールは正常に実行されません。

■ **Tomcat** - 以下の情報を考慮してください。

- Tomcat は、製品のインストール中にデフォルトの CA SDM Web サーバとして設定されます。IIS (Windows) または Apache (UNIX または Linux) をデフォルトの Web サーバとして使用する場合は、設定を実行して要求されたときに IIS または Apache を選択するか、設定を再実行して IIS または Apache を選択してください。
- Tomcat がプライマリ サーバ上で外部認証を使用するように設定されている場合は、認証されていないユーザが添付ファイルを使用できるように、セカンダリ サーバで、Web エンジンおよびリポジトリのデーモンを設定する必要があります。セカンダリ サーバに Tomcat をインストールした場合は、外部認証は使用できません。
- CA SDM のインストールでは、Tomcat ポートは 8080 に設定されます。CA Asset Portfolio Management や製品の Service Delivery Suite といったほかの CA 製品の場合も、デフォルトで Tomcat のポートは 8080 に設定されます。同じサーバに複数の CA 製品をインストールする場合は、すべての製品が正常に動作するように、2 つ目以降の CA Technologies 製品のインストールでは 8080 以外のポート番号を選択してください。CA SDM で Tomcat のポートを 8080 以外に設定する変更は、製品のインストールを実行するか、すでにインストール済みの場合は設定を再実行します。指示に従って Tomcat で使用する利用可能なポート番号を指定してください。
- 再起動後、CA SDM Tomcat プロセスが正常に起動しない場合があります。この場合は、以下のコマンドを使用して TOMCAT を停止し、再度起動してください。

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

■ **ユーザおよび認証** - 以下の情報を考慮してください。

- システムがシャドウ ファイルを使用していて、`/etc/passwd` ファイルのパスワードフィールドが「x」になっているとユーザ認証は失敗します。
- HP で、システム パスワードが `/etc/shadow` に格納されるようにセキュリティの設定をしている場合（この場合、`/etc/passwd` ファイルでは、実際のパスワードは「x」で置き換えられます）、CA SDM ユーザ認証は失敗し、ユーザは CA SDM にログインできません。
- 特権ユーザ用に設定されたパスワードは、ネットワーク ドメインによって適用されるパスワードポリシー制約に準拠している必要があります。ドメインによる制約に準拠していない場合、CA SDM の環境設定は機能しません。

- **Web インターフェースおよび Internet Information Services (IIS)** - Windows 2008 上で IIS 7.0 を使用するように Web インターフェースを設定する場合、IIS 7.0 の CGI およびメタベース互換コンポーネントをインストールする必要があります。IIS 管理互換モジュールをインストールすることで、サーバマネージャの [役割] セクションを使用してこれらのコンポーネントを追加できます。
- **Web Screen Painter** - 以下の情報を考慮してください。
 - CA SDM インストールの一部として WSP をインストールする場合、正常に動作するように WSP を設定する必要があります。
 - テスト モードでの Web Screen Painter プレビュー セッションでは、検索フィルタは未発行の新規テーブルでは無視されます。

関連項目:

[CA SDM をインストールする方法](#) (P. 188)

CA CMDB コンポーネント

CA CMDB は以下の標準コンポーネントを提供します。

CA CMDB Web インターフェース ページ

- CI のプロパティおよび関係を定義し、追跡します。
- 変更の影響および根本原因の分析をサポートします。

CMDB Visualizer

- CI 関係をグラフィック表示します。
- 計画機能をサポートします。

バージョン指定

- CI の変更履歴および関係を表示します。
- スナップショットと指定マイルストーンを比較します。

Common Asset Viewer

- 複数の製品にわたるアセット属性の一般的な表示を提供します。
- 製品サポートの開始点の役割を果たします。

CI 調整

- インポートされた CI データを CMDDB 内の既存 CI と関連付けます。
- 既存アセット レジストリ API を使用します。

リポジトリ

- CI、関係、ファミリーなどのデータ ストアを提供します
- MDB 内に存在します。

統合

- CA Service Desk、CA NSM、CA Asset Portfolio Management、CA EEM などとの統合機能を標準装備しています。

レポート

以下の CI レポートを提供します。

- サマリ
- 詳細
- 変更された CI
- CI ファミリ
- CI 関係
- 関係ツリー

サポート オートメーション の計画に関する考慮事項

適切な サポート オートメーション 設定を計画する際に役立つ情報を調べて収集するのに、以下の情報を使用できます。

- リリース ノートを読んで、サポート オートメーション 用の要件を理解します。

- **サーバとネットワーク** - 以下のサポートされている サポート オートメーション サーバ モードを考慮してください。
 - **メインサーバ** - サポート オートメーション はメイン アプリケーション サーバを使用します。サーバによって、ソケット ベースおよび HTTP ベースの通信が提供されます。
 - **ソケット プロキシサーバ** - サポート オートメーション は、Web サーバと同一層でソケット プロキシを使用します。これによって、暗号化/復号化処理をメイン サーバからオフロードし、ソケット直接接続でスケーラビリティをサポートできるようにします。
 - **メッセージルーティング サーバ (MRS)** - サポート オートメーション では、高帯域幅と予測不能のトラフィックをメイン アプリケーション サーバから切り離すことで、サーバの拡張性をサポートしています。また、ネットワーク ルーティング ショートカットによって、リモート コントロール接続を使用した地理的なスケーラビリティを実現しています。
- **サーバのサイジング** - 以下のサーバ変数を考慮してください。
 - **エンドユーザおよびアナリスト接続のネットワーク特性** - サーバの負荷は、メッセージルーティング コンポーネントのデータに正比例します。帯域幅の小ささ、遅延度の高さ、およびパケット損失の多さは、サーバに負荷をかける大きな要因となります。ネットワーク条件が最適であれば（帯域幅が大きい、遅延が少ない、パケット損失が少ない）、サーバ上の処理速度は高まります。1 分間あたりのアナリスト ユーザおよびエンドユーザの同時ログイン総数（セルフサービス ユーザを含む）が、サーバに大きい負荷をかける場合もあります。
 - **接続タイプ** - HTTP 接続数に対するソケット接続数は、以下のよう
にサーバに影響します。
 - 主にソケット接続を通じて接続する場合、サーバ上の負荷は軽くなり、ハードウェアの性能が高ければ、アプリケーションはネットワークではなく CPU による制約を受けます。ハードウェアでは同時接続数は制限されませんが、ネットワークでは接続が制限される場合があります。
 - HTTP で接続する場合、Web サーバとアプリケーション サーバ上の負荷は高くなり、大幅に拡張されていない限り、アプリケーションは CPU による制約を受けます。

- **リモート コントロールの使用** - リモート コントロールが実行されている場合は常に、継続的に大量のネットワーク帯域幅が使用されます。エンドユーザとアナリスト間のすべてのトラフィックは、サーバを経由します。リモート コントロールの同時接続数には、サイジング評価において重要な役割を果たします。

注: リモート コントロールは、ライブ アシスタンス ツールセット内における唯一の高帯域幅ツールです。チャットおよび自動化機能は、低帯域幅です。スクリーンショットおよびファイル転送は、ファイルが転送される短期間、高帯域幅を使用する場合があります。

サポート オートメーション ネットワークと帯域幅に関する考慮事項

エンドユーザ コンピュータ上で消費される帯域幅の量は、以下のように、使用するツールによって異なります。

- チャット機能および自動化機能では、必要となる帯域幅の量は大きくありません。これらの機能をサポートするには、**56 kbps** 以下のダイヤルアップ モデムが適切です。
- リモート コントロール機能では、必要となる帯域幅の量は増大します。ただし、ライブ アシスタンス リモート コントロールでは、リモート コントロールセッションの画質とリフレッシュ レートを抑えることによって、自動的に低帯域幅環境に適応されます。

帯域幅の量は、使用する接続モデルによっても異なります。**2** つの接続モデルが使用可能です。

- **HTTP 接続** - サーバへの HTTP 接続のみが許可された制限的なファイアウォールの内側にエンドユーザがいる場合に使用します。
- **SSL 直接ソケット** - エンドユーザが SSL ポート **443** 上の接続を使用して、サーバに接続する場合に使用します。

以下の表は、使用するツールに依存する必要な帯域幅を示しています。

ツール/帯域幅	チャット/自動化	リモート コントロール
3 KBps 以下 (28.8 kbps ダイヤルアップ)	高速で即応性も高い	低速
5 KBps 以下 (56 kbps ダイヤルアップ)	高速で即応性も高い	画質劣化時に適する

50 KBps 以下 (ケーブル/ADSL)	高速で即応性も高い	高速で即応性も高い
100 KBps 以下 (LAN)	高速で即応性も高い	高速で即応性も高い

CA NSM のインストール計画

CA NSM の正常なインストールおよび環境設定を計画する際には、CA NSM のマニュアル (「リリース ノート」および **Readme** ファイルを含む) を参照してください。

CA EEM と CA Workflow のインストール計画

CA EEM および CA Workflow の正常なインストールおよび環境設定を計画する際、情報の調査と収集に以下の情報が役立ちます。

- **調査** - 以下の手順を実行します。
 - リリース ノートおよびオプションの **Readme** ファイル (利用可能な場合) の両方を含め、CA EEM および CA Workflow のドキュメントを確認します。

注: CA EEM は、CA SDM 内の設定オプションではありません。CA EEM は、別途インストールする必要があります。

 - CA Workflow と共に使用できる既存の CA EEM インストールがあるかどうかを確認します。ある場合は、CA EEM を再度インストールしないでください。その代わりに、CA Workflow をインストールし、既存の CA EEM インストールを参照させます。
 - CA EEM 管理パスワードをメモします。このパスワードはインストール中に必要になります。

- **CA Workflow のインストール** - 以下の手順を実行します。
 - CA Workflow をインストールする前に、CA EEM がインストールされていることを確認します。この製品をインストールするまで、CA Workflow をインストールできません。
 - CA SDM r12.9 と一緒に CA Workflow を使用する場合、CA サポートオンラインから CA SDM r12.7 ISO をダウンロードして、CA Workflow をインストールします。
 - CA SDM の Tomcat ポート番号は、CA Workflow ではデフォルトで 8080 と 8090 に設定されます。これらのポート番号が別の製品によってすでに使用されている場合は、競合しないように、CA SDM および CA Workflow のポート番号を変更します。
- **CA EEM および AIX** - AIX 上に CA EEM をインストールする際、AIX がネットワーク情報サービス (NIS) 用に設定されている場合は、CA EEM および CA SDM をインストールする前に、*dsa* という名前のユーザを追加してください。これを行うには、以下の手順に従います。
 1. ユーザ ID *dsa* でユーザを作成します。
 2. *dsa* ホームディレクトリを `/opt/CA/eTrustDirectory/dxserver` に設定します。ディレクトリが存在しない場合は、手動で作成します。

注: この手順は CA EEM リリース 8.3 以前の場合にのみ必要です。CA EEM 8.4 のホームディレクトリは、`/opt/CA/Directory/dxserver` に変更されており、インストール中に自動的に作成されます。
 3. *dsa* を `/opt/CA/eTrustDirectory` およびすべてのサブディレクトリの所有者に設定します。*dsa* を所有者に設定するには、以下のようなコマンドを使用できます。

```
chown -R dsa /opt/CA/eTrustDirectory
```
 4. ユーザ、ホームディレクトリ、および `/opt/CA/eTrustDirectory` の所有権が存在することを確認します。

関連項目:

[CA EEM をインストールする方法](#) (P. 262)

[CA Workflow に関する考慮事項](#) (P. 138)

[CA Workflow をインストールする方法](#) (P. 266)

[スタンドアロン CA Workflow IDE のインストール](#) (P. 269)

CA EEM に関する考慮事項

CA EEM をインストールする前に、正しく実装できるように以下の情報を考慮してください。

- **マイグレーション** - CA SDM r12.9 にマイグレートする場合、CA SDM のインストール後に CA EEM r8.4 SP4 CR05 以降にアップグレードします。
- **外部 LDAP データストア** - CA EEM が外部 LDAP データストアを使用するように設定されている場合、特権ユーザを LDAP ディレクトリ内に作成する必要があります。

注: 外部 LDAP サーバ構成の詳細については、「[管理ガイド](#)」を参照してください。

関連項目:

[CA EEM をインストールする方法](#) (P. 262)

CA Workflow に関する考慮事項

CA Workflow をインストールする前に、正しく実装できるように以下の情報を考慮してください。

- CA SDM 構成に応じて、以下の CA SDM サーバに CA Workflow がインストールされます。
 - 標準：プライマリまたはセカンダリ サーバ
 - 高可用性：いずれかのアプリケーション サーバ
 - CA MDB データベース ユーザまたはパスワード - 以下の情報を考慮してください。
 - CA SDM の初回インストール後に CA MDB データベース ユーザまたはパスワードを変更した場合は、CA Workflow のインストールを再実行して、CA Workflow が変更を適用して CA SDM と通信できるようにする必要があります。CA Workflow のインストールを再実行すると、CA SDM により CA Workflow 用の新しいユーザ名とパスワードが自動的に設定されます。CA Workflow のインストール時に、値を手動で変更することはできません。
- 注：UNIX および Linux に CA Workflow をインストールする場合は、事前に Oracle 環境変数を設定する必要があります。ORACLE_HOME 変数が設定されないと、インストールリンク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。
- 新しいデータベースへのマイグレーションを実行する場合は、[ワークフローマイグレーションユーティリティ](#) (P. 140)を実行します。
 - **IPv6** - Linux サーバが IPv6 サポートに設定されている場合は、CA Workflow IDE にログインできない場合があります。この状況を解決するには、\$NX_ROOT¥site¥Workflow¥Client にある ide.sh スクリプトファイルの 2 行目を「VMARGS=」から「VMARGS=-Djava.net.preferIPv4Stack=true」に変更します。その後、スクリプトファイルを保存し、CA Workflow IDE を再度起動します。
 - **Tomcat** - 以下の情報を考慮してください。
 - Tomcat を起動できず、その結果 CA Workflow および Web インターフェースが使用できない場合は、Tomcat のメモリを増やしてください。

注：この状況の対処法の詳細については、<http://ca.com/support> でナレッジベースの記事 TEC418959 を検索してください。

- CA Workflow のインストール中、CA SDM と CA EEM は、Tomcat 専用のポート番号を共有します。CA Workflow をインストールまたは使用しているときに Tomcat に問題が生じた場合は、サービスを[停止して再起動](#) (P. 326)してください。
- オプション マネージャで指定した CA Workflow ホスト名は、CA Workflow をインストールしたサーバの `NX.env` ファイルの `NX_LOCAL_HOST` 変数と一致する必要があります。ホスト名の大文字および小文字を正確に一致させる必要があります。
- Tomcat のポート (8080) や特権ユーザのユーザ ID/パスワード (ServiceDesk/ServiceDesk) といったインストール時のデフォルトを変更した場合は、CA Workflow が正常に機能するように、以下のようにデフォルトの定義およびアクターを変更してください。
- Workflow IDE にログオンします。

以下の手順に従って、デフォルトの Service Desk Web サービス アクターを変更します。

- a. [アクター] タブをクリックします。
- b. [Web サービス] ツリーを展開します。
- c. [Unicenter_Service_Desk_Web_Service] アクターを右クリックし、[プロパティ] を選択します。
- d. WSDL URL エントリの内容を選択してコピーします。
- e. アクターの名前を変更し、[OK] をクリックします。
- f. [Web サービス] ツリーを右クリックし、[アクターの追加] を選択します。
- g. [名前] フィールドに「Unicenter_Service_Desk_Web_Service」と入力します。
- h. [WSDL URL] エントリに、上でコピーしたコンテンツを貼り付けます。
- i. Tomcat の構成で選択したポート番号と同じになるように、URL のポート番号を変更します。
- j. [OK] をクリックします。

- CA Workflow を CA SDM サーバにインストールした後、以下の手順に従って、CA SDM と CA Workflow の統合が正常に機能するようにします。
 - CA Workflow IDE にログインし、デフォルトの CA SDM Web サービス アクターを変更します。
 - [アクター] タブを選択し、[JavaScript] ツリーを展開し、[USDInitializer] をクリックします。
 - [Get Global Attributes] をダブルクリックします。
 - スクリプトセクションの以下のフィールドに、CA SDM 特権ユーザ名およびパスワードを入力します。

USD_Username = ""

USD_Password = ""
 - \$NX_ROOT¥data¥workflow¥actors¥r12_Service_Desk_Actors_en_US.xml ファイル内のこれらの値を変更します。

関連項目:

[CA Workflow をインストールする方法](#) (P. 266)

ワークフロー マイグレーション ユーティリティ

Workflow Data Migration Tool は、ある CA Workflow データベースから別のデータベースにデータを移動させるためのものです。このユーティリティを使用して、サポートされている任意のデータベースから、サポートされている別のデータベースにデータを移動でき、これによって最新の CA Workflow スキーマにデータを移動できます。

Workflow Data Migration Tool は、GUI と Bean の両方で提供されます。

- **GUI** - migration.jar
- **Bean** - datamover.jar

注: これらの Java コマンドを実行するには、2 つの JAR ファイル (datamover.jar および migration.jar) を手動で解凍し、Java パスに抽出する必要があります。migration.zip ファイルは、¥winsrvr.cd1¥CA_tps.nt¥CAFLOW¥Resources ディレクトリ内のインストールメディア上にあります。

コマンドラインからのマイグレーション ユーティリティの実行

マイグレーション ツールは `datamover.jar` 内で `Bean` として提供されます。コマンドラインからマイグレーション ツールを実行できます。

マイグレーション ユーティリティの実行

```
java -cp <ドライバ jar ファイル> com.ca.workflow.util.DataMover <ソース DB ドライバ名>  
<ソース DB URL> <ソース DB ユーザ名> <ソース DB パスワード> <ターゲット DB ドライバ名> <ター  
ゲット DB URL> <ターゲット DB ユーザ名> <ターゲット DB パスワード> <トランザクションあたり  
のエントリ数> [製品キー (カンマ区切り)]--fetchsize=15 [オプション]
```

例

```
java -cp iijdbc.jar;datamover.jar com.ca.workflow.util.DataMover  
ca.ingres.jdbc.IngresDriver  
jdbc:ingres://155.35.26.105:EI7/mdb;cursor=readonly;auto=multi;group=workflow_admin_group root iloveca ca.ingres.jdbc.IngresDriver  
jdbc:ingres://tadra01-w2k3-v:EI7/mdb;cursor=readonly;auto=multi;group=workflow_admin_group tadra01 ca#33333 50 wekProductKey1 --clean-target --fetchsize=15
```

ドライバ jar ファイル

ソースおよびターゲットのドライバ ファイルを示します。セミコロン (;) を使用して複数のドライバ ファイルを区切ります。

ソース DB ドライバ名

ソース データベース ドライバを指定します。

ソース DB URL

ソース データベースの URL を指定します。

ソース DB ユーザ名

ソース データベース ユーザを指定します。

ソース DB パスワード

ソース データベースのパスワードを指定します。

ターゲット DB ドライバ名

ターゲット データベース ドライバを指定します。

ターゲット DB URL

ターゲット データベースの URL を指定します。

ターゲット DB ユーザ名

ターゲット データベース ユーザを指定します。

ターゲット DB パスワード

ターゲット データベースのパスワードを指定します。

トランザクションあたりのエントリ数

1 つのトランザクションに移動するエントリの数を指定します。この数が大きすぎると、Ingres のトランザクション ログをオーバーランする可能性があります。推奨のデフォルト設定は、50 です。

clean-target

データ転送を続行する前に、指定した製品キーに関連するデータをターゲット データベースからすべて削除します。製品キーが指定されていない場合は、データ転送を続行する前に、ターゲット データベースからすべてのデータが削除されます。このオプションは、事前のマイグレーションが実行途中で失敗した場合、ターゲット データベースをクリーンアップするために使用できます。

fetchsize

-fetchsize コマンドライン オプションが指定されている場合に、スクロール可能な結果セットで一度にフェッチされる行の数を指定します。指定しない場合は、ソース データベースのデフォルト フェッチ サイズが使用されます。Ingres には、スクロール可能な結果セットで一度に取得される行数のデフォルト値がありません。この場合、コマンドライン オプションとして指定されていない場合は、デフォルトとして 10 行が使用されます。

製品キー

データをマイグレートする製品キーを指定します。これはオプションのパラメータです。指定する場合は、単一の製品キーか、複数の製品キーのカンマ区切りリストのいずれかを指定します。製品キー パラメータが指定されている場合、マイグレーションユーティリティでは、指定された製品キーによって制限されたソース データベースからデータをマイグレートします。このパラメータが省略されている場合は、すべてのワークフロー データが製品キーにかかわらずマイグレートされます。

ログ ファイル

コマンドラインからデータを転送すると、ログ ファイルが作成されます。

ドライバ ファイル

すべてのドライバ ファイルをマイグレーション ツールのディレクトリに配置するか、データベース ドライバ JAR ファイルの場所を指定する必要があります。

GUI からのマイグレーション ユーティリティの実行

GUI からマイグレーションを実行する方法

1. コマンドラインで、以下のコマンドを入力します。

```
java -cp datamover.jar;migration.jar -Dwflg="c:\wf.log" -Dtxlimit="0"  
com.ca.workflow.util.WFMigration
```

[Workflow Data Migration Tool] ダイアログ ボックスが表示されます。

2. [Source Database] と [Target Database] の両方のセクションで、[Database Type] ドロップダウン メニューからデータベースの種類を選択します。

ドライバ名および URL は自動的に更新されます。必要に応じて、これらのデフォルト値を変更できます。

- Ingres の場合は、-ijdbc.jar を使用します。
- Oracle 10g の場合は、ojdbc14.jar を使用します。
- Oracle 11g の場合は、ojdbc5.jar を使用します。
- MS SQL 2000 の場合は、msutil.jar、msbase.jar、mssqlserver.jar を使用します。
- MS SQL 2005 の場合は、sqljdbc.jar を使用します。
- Sybase Adaptive Server Enterprise 12.5.4 の場合は、jconn3.jar を使用します。
- Sybase Adaptive Server Enterprise 15.0 の場合は、jconn3.jar を使用します。

重要: CA SDM でサポートされるデータベースのリストについては、リリース ノートを参照してください。

3. 適切なフィールドに入力します。
4. [Start] をクリックします。

データマイグレーションが開始されます。マイグレーション中、ダイアログボックス下部のステータスが更新されます。

CA Process Automation インテグレーションの計画

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 Process Automation インテグレーションを計画する際には、以下を考慮してください。

- CA Process Automation 製品をインストールして設定するための時間を確保します。
- サーバアーキテクチャが CA Process Automation と CA SDM をサポートする場合、両製品が単一のサーバ上で共存できるかどうかを評価します。CA Process Automation または CA SDM のコンポーネントが同じサーバ上で共存できない場合は、各製品を別のサーバにインストールすることを検討してください。
- 両方の製品がインストールされており、独立して動作していることを確認するための時間を考慮に入れます。
- CA SDM を、CA EEM 8.4 を使用する CA Process Automation と統合する場合は、CA EEM 8.4 SDK パッチが CA SDM に適用されていることを確認します。このパッチの詳細については、CA サポート オンラインを参照してください。

注: CA SDM および CA Process Automation の製品要件の詳細については、「CA SDM リリース ノート」を参照してください。CA Process Automation がサポートするプラットフォーム、必要な手順、およびインストールのオプションの詳細については、CA Process Automation のインストールおよび環境設定ドキュメントを参照してください。

セキュリティに関する考慮事項

リリース ノートの正規の最小要件に加えて、CA Process Automation のインストールに関する以下の推奨事項を考慮してください。

- 認証サーバとして CA EEM を使用するように CA Process Automation を設定してください。CA EEM によって、認証時にユーザ名とパスワードが平文で渡されるのを回避できます。
- CA Process Automation にマルチテナンシーを使用している場合、CA EEM のインストールは必須です。

注: CA Process Automation にマルチテナンシーを実装する詳細については、CA Process Automation のインストールおよび環境設定ドキュメントを参照してください。

- CA SDM でマルチテナンシーを使用する場合は、CA EEM のインストールが必要です。

注: マルチテナンシーを使用していない場合は、CA SDM 用の CA EEM の設定はオプションです。

- HTTPS によるセキュアな通信を使用して通信するように CA Process Automation を設定してください。HTTPS URL では、SSL/TLS が使用され、平文の交換が行われないため、偶然または悪意による漏えいから極秘データやその他の機密データが保護されます。

注: HTTPS を使用するように CA Process Automation を設定する詳細については、CA Process Automation のインストールおよび環境設定ドキュメントを参照してください。

CA Process Automation との SSL 通信をセットアップする方法

セキュリティ上の理由から、CA Process Automation を実装する際に、SSL 通信が必要な CA Process Automation のインストールまたは再設定を選択した場合があります。CA Process Automation を SSL 通信を必要とするように設定するには、CA SDM などの統合アプリケーションに、通信用の CA Process Automation キーストアからの証明書が必要になります。

CA Process Automation との SSL 通信をセットアップするには、以下の手順に従います。

1. CA Process Automation HTTPS アドレスを使用するように CA SDM オプションを設定します。

2. CA Process Automation キーストア証明書をファイルにエクスポートし、CA SDM にそのファイルをコピーします。
3. CA SDM pdm_keystore_mgr ユーティリティを使用して、CA SDM に証明書ファイルをロードします。
4. CA SDM アーキテクチャに該当する場合は、Version Control ファイルを更新して、すべてのセカンダリ サーバに CA SDM キーストアを配信します。
5. CA SDM を再起動します。

CA Process Automation で SSL が有効化されている場合に通信を有効化する方法

CA Process Automation が SSL を使用して通信する場合は、CA SDM サーバを CA Process Automation と通信するように設定する必要があります。

CA Process Automation で SSL が有効化されている場合に通信を有効化するには、以下の手順に従います。

1. CA SDM を起動せずに、ブラウザで CA Process Automation を使用できることを確認します。CA Process Automation URL を記録し、オプション マネージャ内の CA Process Automation ワークフロー オプションを設定する際に参照します。
2. CA SDM にログインし、オプション マネージャの CA Process Automation ワークフロー オプションをインストールまたは変更します。以下の各オプションで、SSL 対応 CA Process Automation アプリケーションに接続するための構文として、`http://server:8080` の代わりに `https://server:8443` を使用します。ただし、CA Process Automation インストールが 8443 の SSL ポートの代わりに別のポートを使用している場合は、適切なポート番号を指定します。
 - `caextwf_endpoint`
 - `caextwf_processdisplay_url`
 - `caextwf_worklist_url`

注: 値が実際の CA Process Automation インストール値と一致しない場合、CA SDM は CA Process Automation と通信できず、ランタイムエラーが発生します。CA Process Automation インストーラがポート 8443 の代わりに別のポートを選択した可能性があるため、値が実際の CA Process Automation インストール値と一致しているかどうかを確認します。

3. CA Process Automation サーバで、以下のファイル内の **KEYSTOREID** エントリと **itpam.web.keystorealias** エントリを見つけます。

```
C:\Progra~1\ITPAM\server\c2o\%.config\0asisConfig.properties
```

4. **KEYSTOREID** をコピーします。 **keytool** コマンドを発行した後にパスワードとして **KEYSTOREID** 値を貼り付けられるように準備しておきます。
5. CA Process Automation サーバで、コマンドライン上に 1 つの行として以下の **keytool** コマンドを発行します。

```
C:\Progra~1\ca\sc\jre\1.6.0_00\bin\keytool.exe -keystore
C:\Progra~1\ITPAM\server\c2o\%.config\c2o\keystore -export -alias
<keystorealias> -file itpam.cer
```

keytool ユーティリティによって、パスワードを入力するよう求められます。

6. パスワードとして **KEYSTOREID** 値を貼り付けるか入力します。

keytool ユーティリティによって、最後のパラメータ (**-file itpam.cer**) を使用して **itpam.cer** という名前のファイルが作成されます。**itapm.cer** ファイルには、CA SDM との通信に必要な証明書情報が含まれています。

7. CA SDM サーバ上に以下の場所のいずれかに、**itpam.cer** ファイルを移動させます。

- (Windows) %NX_ROOT%\bin
- (UNIX) \$NX_ROOT/bin

8. 以下のコマンドを入力して、CA SDM に CA Process Automation 証明書情報をインポートします。

```
(Windows) pdm_perl %NX_ROOT%\bin\pdm_keystore_mgr.pl
-import %NX_ROOT%\bin\itpam.cer
(UNIX) pdm_perl $NX_ROOT/bin/pdm_keystore_mgr.pl -import $NX_ROOT/bin itpam.cer
```

pdm_keystore_mgr.pl スクリプトによって、以下の場所にキーストアファイルが生成されます。

- (Windows) %NX_ROOT%\pdmconf\nx.keystore
- (UNIX) \$NX_ROOT/pdmconf/nx.keystore

9. *nx.keystore* は、CA SDM の設定に応じて、以下の CA SDM サーバに配信される必要があります。

- 標準：セカンダリ サーバ。
- 高可用性：アプリケーション サーバおよびスタンバイ サーバ。

以下のいずれかの場所から、*server_secondary.ver* ファイルを開きます。

- (Windows) %NX_ROOT%\site\server_secondary.ver
- (UNIX) \$NX_ROOT/site/server_secondary.ver

10. Version Control 用に、以下の情報を追加して *server_secondary.ver* を変更します。

```
[SSL_Keystore]
filename = "nx.keystore"
directory = "$NX_ROOT/pdmconf"
component_type = "file"
o_mode = "RW"
g_mode = "RW"
w_mode = "RW"
file_ctl
```

注：Version Control の管理の詳細については、「Administration Guide」を参照してください。

11. CA SDM を再起動します。

CA SDM サーバは SSL が有効化された CA Process Automation アプリケーションと通信できます。

注：CA Process Automation ワークフロー オプション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。

CA Business Intelligence のインストール計画

CA Business Intelligence の正常なインストールおよび環境設定を計画する際、情報の調査と収集に以下の情報が役立ちます。

- **調査** - 以下の手順を実行します。
 - リリース ノートを読んで、CA Business Intelligence の要件を理解します。
 - リリース ノートおよびオプションの Readme ファイル（利用可能な場合）の両方を含め、CA Business Intelligence ドキュメントを確認します。

注: サポートされている環境およびハードウェア要件の詳細なリストについては、CA Business Intelligence DVD にある種々のサポートされているプラットフォームのドキュメントを参照してください。これらのドキュメントには、Web アプリケーション サーバ、Web ブラウザ、およびオペレーティング システムの特定のバージョンおよびパッチ レベルの要件が含まれます。

- **インストール ホーム ディレクトリ** - CA Business Intelligence をインストールするホーム ディレクトリを決定します。デフォルトの場所は、以下のとおりです。
 - Windows 32 ビット コンピュータ : C:\Program Files\CA\SC\CommonReporting3
 - x64 コンピュータ : C:\Program Files X(86)\CA\SC\CommonReporting3
 このディレクトリが存在しない場合は、インストールを開始する前に作成してください。
- **アンチウイルス ソフトウェア** - CA Business Intelligence をインストールするコンピュータへのアンチウイルス ソフトウェア スキャンをすべて一時的に無効にします。
- **アプリケーション サーバのサポート** - CA SDM と CA Business Intelligence との統合では、CA Business Intelligence アプリケーション サーバとして Apache Tomcat のみをサポートします。
- **Web Browser Support** -- CA Business Intelligence 3.2 SP5 は以下の Web ブラウザをサポートします。

ブラウザ OS	ブラウザ	JVM
Apple Mac OS X	Safari 5	Apple 1.6.0_xx

ブラウザ OS	ブラウザ	JVM
Microsoft Windows	Firefox 3.6	Sun 1.5.0_xx Sun 1.6.0_xx
	Firefox 8 注: 最新の Firefox リリースはについては、 Mozilla によってリリースされた後、最小限の テストを行ってから約 2 週後にサポートしま す。	Sun 1.6.0_xx
	IE 6.0 SP3	Sun 1.5.0_xx Sun 1.6.0_02+
	IE 7.0	Sun 1.5.0_xx Sun 1.6.0_02+
	IE 8.0 注: 互換モードのみがサポートサポートされ ます。	Sun 1.6.0_xx
	IE 9.0 注: 互換モードのみがサポートサポートされ ます。	Sun 1.6.0_xx

重要: CA Business Intelligence インストールは CA SDM r12.9 では Windows プラットフォームのみに制限されています。ただし、サポートされるすべてのプラットフォームで、CA Business Intelligence を CA SDM と統合できます。

関連項目:

[レポートの考慮事項 \(P. 151\)](#)

[CA Business Intelligence と CA SDM の統合 \(P. 305\)](#)

レポートの考慮事項

CA Business Intelligence をインストールする前に、正しく実装できるように以下の情報を考慮してください。

- このリリースに含まれている CA SDM r12.9 レポートを表示するには、CA Business Intelligence r3.2 (BusinessObjects Enterprise リリース 3.1) のインストールが必要です。
- CA Business Intelligence r2.1 (BusinessObjects Enterprise リリース 2) はサポートされていません。
- CA Business Intelligence r3.0 は、r12.1 から r12.5 へのアップグレードプロセス中にインストールできます。
- インストールは、選択したインストールタイプ (カスタムまたは新規) によって異なります。
- 新規およびカスタムの両方のインストールでインストーラを実行する前に、BusinessObjects 管理者アカウントに資格情報を定義する必要があります。
- 構成管理サーバ (CMS) がポート 6400 (デフォルト) にインストールされている必要があります。インストールされていない場合は、セットアップ中に CA Business Intelligence の設定に失敗します。
- CA SDM ユーザは、レポートを使用する前に CMS 内の管理者のリストに追加される必要があります。
- Business Objects 用のアプリケーションサーバとして使用するために Apache Tomcat 5.5.20 をインストールする場合は、追加の設定手順を実行する必要があります。
- Business Objects の既存のインストールがある SAP Business Objects ユーザは、CA Business Intelligence をインストールおよび設定するか (推奨)、既存の Business Objects インストールを使用することができます。
- Firefox を使用して InfoView にアクセスする場合は、CA Business Intelligence 3.2 によってサポートされている Firefox バージョンを使用する必要があります。
- Business Objects と共に提供される JRE のバージョンを、特定の環境に適したバージョンに変更する必要がある場合があります。
- CA Business Intelligence のインストール後、呼び出しが可能でも、Crystal Reports エクスプローラおよび Desktop Intelligence はサポートされていません。

新規インストールとカスタム インストール(Windows)

新規インストールとカスタム インストールには、いくつかの違いがあります。インストールのフローは、選択したインストール タイプによって異なります。

New

1 台のコンピュータにすべてのコンポーネントをインストールします。すべてのサーバおよびクライアント コンポーネントの完全な展開を単一のコンピュータ上に短時間で設定するには、このインストール タイプを選択します。新規インストールによって、以下が提供されます。

- MySQL (CMS 情報を保存するためのデータベースとして)
- Apache Tomcat (アプリケーション サーバとして)

注: BusinessObjects Enterprise では、ユーザとグループ、セキュリティレベル、BusinessObjects Enterprise コンテンツ、およびサーバに関する情報を格納するためのデータベースが必要となります。CMS が管理するプライマリ データベースは、CMS データベースと呼ばれます。CA Business Intelligence のインストール時に、使用する CMS を指定し、認証に必要なパラメータを入力します。CMS データベースの要件および準備の詳細については、CA Business Intelligence の「実装ガイド」を参照してください。

カスタム

選択したコンポーネントをコンピュータにインストールします。分散化展開を実行する場合、または既存の展開にサーバを追加する場合に、インストールするコンポーネントを指定するには、このインストール タイプを選択します。

重要: Microsoft SQL または Oracle データベースに BusinessObjects CMS をインストールする場合は、カスタム インストールを実行します。

カスタム インストールには、以下のオプションが用意されています。

MySQL をインストールするか、以下のような既存の CMS を使用します。

- Oracle
- Microsoft SQL
- Apache Tomcat - Apache Tomcat インスタンスのインストールを制御できます。

BusinessObjects 管理者の認証情報

新規インストールおよびカスタム インストールのインストーラを実行する前に、**BusinessObjects** 管理者パスワードを指定する必要があります。

このパスワードは、大文字と小文字の混在する、6 文字以上の長さである必要があります、どのような形式であっても **administrator** という言葉を含めることはできません。以下の文字タイプの 2 つ以上を含める必要があります。

- 大文字
- 小文字
- 数値
- 句読点

BusinessObjects Enterprise XI アプリケーション サーバ

BusinessObjects Enterprise では、**Web** アプリケーションの構成要素であるサーバサイドスクリプトを処理するために、アプリケーションサーバが必要になります。

CA Business Intelligence のインストール時、使用するアプリケーションサーバを指定し、必要な設定パラメータを入力します。**CA Business Intelligence** では、**Apache Tomcat 5.5.20** をインストールするためのオプションを選択できます。また、既存のアプリケーションサーバを使用することもできます。

BusinessObjects 用のアプリケーションサーバとして使用するために **Apache Tomcat 5.5.20** をインストールする場合は、以下を実行します。

- **Java 2 Standard Edition JDK 1.5** をインストールします。
- 環境変数 **\$JAVA_HOME** を **JDK 1.5** ホームディレクトリに設定します。
- **Apache Tomcat 5.5.20** をインストールし、**Java** 仮想マシンのパスを、システム上の **Java 2 Standard Edition JRE 1.6** がインストールされているディレクトリに設定します。
- **CA Business Intelligence** のカスタム インストールを実行します。
- **[Web Server Configuration]** 画面で、**BusinessObjects XI** 用に **Tomcat** の新しいコピーをインストールするかどうかを確認するプロンプトが表示されたら、**[No]** を選択します。
- アプリケーションサーバのリストから **Tomcat** を選択します。

- [Install Directory] フィールドに Apache Tomcat 5.5.20 Web サーバの場所を入力し、インストールを実行します。
- CA Business Intelligence のインストールを完了した後に、CA Business Intelligence 環境設定を実行します。

注: (デフォルト以外の外部アプリケーションサーバを使用して)すでに JDK 1.5 と共に CA Business Intelligence をインストールしており、InfoView Web Intelligence ツールにアクセスするクライアント環境で JRE 1.6 を使用する場合は、要求されたときに 1.4.2 JRE をインストールしないでください。代わりに、JRE 1.6 をクライアント環境にインストールしてください。JRE 1.6 をインストールした後、必要に応じてブラウザを再起動してください。JRE 1.6 は、Oracle の Web サイトからダウンロードできます。

BusinessObjects (SAP)の既存のインストール

SAP BusinessObjects を使用している場合、既存の BusinessObjects が CA Business Intelligence を使用せずにインストールされているのであれば、互換性およびサポート性を最大化するために、CA Business Intelligence をインストールし、設定することをお勧めします。ただし、既存の BusinessObjects インストールを使用したい場合は、CA Business Intelligence のインストール手順をスキップし、セクション「CA Business Intelligence の設定方法」に進むことができます。

注: BusinessObjects Enterprise Release 3 を使用しており、アプリケーションサーバとして Tomcat を展開している必要があります。また、Web Intelligence のライセンスを取得している必要があります。Crystal Reports に関しては、ランタイム ライセンス以上を取得している必要があります。

Firefox を使用した InfoView へのアクセス

Firefox を使用して BusinessObjects InfoView にアクセスする場合は、Java 仮想マシン (Java ランタイム) 1.5.0_xx および 1.6.0_02+ を備えた Firefox 2 を使用する必要があります。

注: サポートされているプラットフォームおよびリリース レベルの詳細については、「*BusinessObjects Enterprise XI for Windows ガイド*」を参照してください。

レポートのベスト プラクティス

CA Business Intelligence のインストール、管理、および使用の際には、以下のベスト プラクティスを使用してください。

- 各 CA 製品につき 1 つのユニバースをインストールして管理します。必要に応じて、ユニバースのリンクを作成できます。
- カスタマイズしたユニバースにサービス パック、パッチ、およびその他の更新を適用する前に、すべてのカスタマイズをバックアップします。
- デフォルトのユニバースは変更しないでください。代わりに、コピーして、そのコピーを変更します。そうしないと、サービス パック、パッチ、およびその他の更新を適用したときに、カスタマイズが消去される場合があります。
- 自分専用のフォルダを作成します。
- レポートが実行を停止した場合、Central Management Server (CMS) が動作していることを確認します。
- 事前定義済みレポートは上書きしないでください。
- カスタム レポートを作成する際には、常にベースとして事前定義済みレポートを使用します。これによって、すべてのレポートのフォーマットに一貫性を持たせやすくなります。

注: これらのタスクを完了する詳細については、BusinessObjects Enterprise のドキュメントを参照してください。

実装方針

CA Service Desk の実装方針を計画する際、ネットワークの可用性、使用可能な帯域幅、および応答性に加え、以下の情報を考慮してください。

- **一元化** - すべての製品コンポーネントを 1 つのプライマリ サーバ上にインストールおよび設定します。これはデフォルトのインストールです。負荷分散とフェールオーバーのために複数のオブジェクト マネージャおよび Web エンジンを実装できますが、ビジネスがこの実装を超えて成長する可能性があります。

- **分散化** - サービスを受信するクライアントに近いサーバ上に製品コンポーネントをインストールおよび設定します。たとえば、多数のサブネットがある企業の支社には、**Web** クライアントを使用する多くのアナリストが存在する場合があります。セカンダリ サーバをこの支社に配置すると、ネットワーク トラフィックおよび応答時間が削減されます。セカンダリ サーバではキャッシングが実行されるため、支社とプライマリ サーバ間のネットワーク トラフィックも削減されます。このタイプの実装でも、負荷分散とフェールオーバーのために複数のオブジェクトマネージャおよび **Web** エンジンを実装できます。
- **グローバル** - リージョンと呼ばれる 2 つ以上の一元化された実装または分散化された実装で構成されます。リージョンのプライマリ サーバでは、マスタ リージョン間との最小限の情報が複製されます。これによって、単一のリージョンに、ほかのすべてのリージョンに関する必要な情報があることとなります。アナリストは、これを利用してすべてのリージョンからのチケットを認識して、必要がある場合にのみリージョンに接続できます。分散化実装を採用するにはネットワーク帯域幅の制限が大きい場合に、このタイプの実装が有効です。たとえば、支社が複数の国にあり、速度の遅いリンクで相互接続している場合が考えられます。

注: 詳細については、「[高可用性のための CA Service Desk アーキテクチャ \(P. 102\)](#)」を参照してください。

Firefox での Windows 認証の有効化

NT LAN Manager (NTLM) 認証では、Windows ドメインにログインした Windows ユーザのログイン認証情報が自動的に同じドメインの IIS Web サーバに渡されます。デフォルトでは、Firefox では Windows 認証が有効化されていません。実装の準備として、Firefox で Windows 認証を有効にする必要があります。

Firefox で Windows 認証を有効にする方法

1. Firefox を起動します。
2. 以下の URL に移動します。

`about:config`

3. 詳細設定を変更することを確認します。

[設定名] リストが表示されます。

4. 設定名 `network.automatic-ntlm-auth.trusted-uris` を見つけて、ダブルクリックします。

[Enter string value] ダイアログ ボックスが表示されます。

5. 完全な URL (`http://web.example.com` など) またはサーバ名 (`web.example.com` など) を入力して、信頼済みサイトのリストを指定します。

注: 末尾のスラッシュは入力しないでください。複数のサーバを指定する場合は、カンマで区切ります。特定のドメイン内のすべてのサーバを指定できますが、一般的なワイルドカードは機能しません。たとえば、`*.example.com` ではなく `.example.com` と指定する必要があります。

6. [OK] をクリックします。
7. Firefox を再起動します。

第 4 章: インストール

このセクションには、以下のトピックが含まれています。

[ソフトウェアの実装方法](#) (P. 159)

[CA SDM サーバの設定方法](#) (P. 161)

[標準設定から高可用性設定に変換する方法](#) (P. 169)

[高可用性設定から標準設定に変換する方法](#) (P. 175)

[CA MDB をインストールする方法](#) (P. 179)

[CA SDM をインストールする方法](#) (P. 188)

[Web Screen Painter をインストールする方法](#) (P. 207)

[CA SDM と CA NSM の統合をインストールおよび設定する方法](#) (P. 208)

[CA EEM をインストールする方法](#) (P. 262)

[CA Workflow をインストールする方法](#) (P. 266)

[CA Business Intelligence for CA SDM をインストールする方法](#) (P. 272)

[インストールの確認](#) (P. 276)

[インストールログ](#) (P. 277)

ソフトウェアの実装方法

CA SDM の実装は、以前のリリースからのアップグレードか初めて製品をインストールするのに加えて、オペレーティング システム、データベース、統合する製品など、多数の要素に基づいて行います。ソフトウェアを実装するには、通常、以下の手順に従います。

1. リリース ノートに文書化されている実装についての考慮事項を確認します。
2. 以前のバージョンからアップグレードする場合は、データベース、コンソール、および CA Workflow をアップグレードする手順に従ってください。
3. CA MDB をインストールします。

データベース (SQL Server または Oracle) が CA SDM プライマリ サーバ以外のサーバにインストールされている場合は、リモート データベース サーバ (つまり、SQL Server または Oracle がインストールされているコンピュータ) に CA MDB をインストールします。CA MDB とプライマリ サーバが同じコンピュータ上にある場合は、CA MDB は自動的にインストールされます。

4. プライマリ サーバまたはオプションのセカンダリ サーバのいずれかに CA SDM をインストールします。

Web Screen Painter がサーバ上に自動的にインストールされるため、インストールの完了後に Web フォームおよびスキーマをカスタマイズできます。

5. (オプション) CA SDM の環境設定中に CA CMDB Visualizer を有効にします。
6. (オプション) CA SDM の環境設定中に サポート オートメーション を有効にします。

重要: CA サポート オートメーション r6.0 SR1 eFix5 部署をテナントに移行する場合は、このデータを変換してから、CA SDM r12.9 内の サポート オートメーション を有効化および設定します。

7. (オプション) CA SDM の環境設定中に REST API を有効にします。
8. (オプション) 認証用に CA EEM をインストールします。
9. (オプション) ビジネス プロセスを管理するために CA Workflow をインストールします。
10. (オプション) BusinessObjects テクノロジを使用してレポートを管理するために CA Business Intelligence をインストールします。
11. (オプション) CA NSM Integration をインストールします。

関連項目:

[CA EEM をインストールする方法](#) (P. 262)

[CA Workflow をインストールする方法](#) (P. 266)

[CA MDB をインストールする方法](#) (P. 179)

[インストール ログ](#) (P. 277)

[CA SDM をインストールする方法](#) (P. 188)

[インストールの確認](#) (P. 276)

[Web インターフェースの開始](#) (P. 290)

CA SDM サーバの設定方法

システム管理者は、以下の場合に、CA SDM サーバを設定します。

- CA SDM の新規インストールを完了した後、高可用性設定または標準設定を実装する場合。
- 最新バージョンの CA SDM にアップグレードした後、高可用性設定または標準設定を実装する場合。

注: 特定の設定（たとえば、標準）を持った CA SDM をインストールまたはアップグレードし、別の設定（たとえば、高可用性）を実装する場合は、変換シナリオまたは「実装ガイド」を参照してください。

以下の図では、標準設定で CA SDM サーバを設定する方法を示します。



以下の図では、高可用性設定で CA SDM サーバ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. CA SDM の設定に応じて、以下を実行します。
 - [プライマリ サーバを設定します](#) (P. 163)。
 - [バックグラウンドサーバの設定](#) (P. 165)
2. 既存のサーバがない場合は、[サーバを追加します](#) (P. 163)。
3. CA SDM の設定に応じて、以下を実行します。
 - [セカンダリ サーバを設定します](#) (P. 165)。
 - [スタンバイサーバおよびアプリケーションサーバの設定](#) (P. 166)
4. [サーバの詳細を確認します](#) (P. 168)。

プライマリ サーバの設定

セカンダリ サーバを設定する前に、プライマリ サーバを設定する必要があります。

次の手順に従ってください:

1. プライマリ サーバとして設定するサーバにログインします。
2. `pdm_configure` コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
3. 設定タイプとして [標準] を選択し、プロンプトに従って設定を完了します。詳細については、「[サーバ設定ヘルプ](#)」を参照してください。
プライマリ サーバが設定されます。

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。

セカンダリ サーバの設定

プライマリ サーバを設定した後に各セカンダリ サーバを設定します。この設定は、プライマリ サーバとの通信を確立するために必要です。

次の手順に従ってください：

1. セカンダリ サーバとして設定するサーバにログインします。
2. `pdm_configure` コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
3. 設定タイプとして [標準] を選択し、プロンプトに従って設定を完了します。詳細については、「[サーバ設定ヘルプ](#)」を参照してください。
セカンダリ サーバが設定されます。
4. セカンダリ サーバとして設定する各サーバ上で手順 1 ～ 3 を繰り返します。

バックグラウンド サーバの設定

アプリケーション サーバまたはスタンバイ サーバを設定する前にバックグラウンドサーバを設定します。

次の手順に従ってください：

1. バックグラウンドサーバとして設定するサーバにログインします。
2. `pdm_configure` コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
3. 設定タイプとして [高可用性] を選択し、プロンプトに従って設定を完了します。詳細については、「[サーバ設定ヘルプ](#)」を参照してください。
バックグラウンドサーバが設定されます。

スタンバイまたはアプリケーション サーバの設定

バックグラウンド サーバを設定した後、各スタンバイおよびアプリケーション サーバを設定します。この設定は、バックグラウンド サーバとの通信を確立するために必要です。

重要: (推奨) バックグラウンド サーバとその他のすべてのスタンバイサーバの両方が同じ設定になっていることを確認してください。この処理により、フェールオーバー中にスタンバイ サーバが新しいバックグラウンドサーバになったとき、スタンバイ サーバが古いバックグラウンドサーバと同様に機能できます。

次の手順に従ってください：

1. スタンバイ サーバまたはアプリケーション サーバとして設定するサーバにログインします。
2. `pdm_configure` コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
3. 設定タイプとして [高可用性] を選択し、プロンプトに従って設定を完了します。詳細については、「[サーバ設定ヘルプ](#)」を参照してください。
4. スタンバイ サーバおよびアプリケーション サーバとして設定する各サーバ上で手順 1～3 を繰り返します。

スタンバイ サーバおよびアプリケーション サーバを設定しました。

5. 1つ以上のアプリケーション サーバがあり、別のアプリケーションサーバとの間のリクエストを追跡するためにロード バランサを使用する場合は、[ロード バランサを設定](#) (P. 167) します。

注: CA SDM 通知でロード バランサ URL またはアプリケーション サーバ URL をリンクに使用するには、以下の手順に従います。

- a. バックグラウンド サーバにログインします。
- b. [管理] タブで [オプション マネージャ] - [通知] を選択します。
- c. `web_cgi_url` オプションの値を、以下のものを指すように変更します。
 - 複数のアプリケーション サーバが存在する場合は、ロード バランサ。
 - アプリケーション サーバが 1 つしか存在しない場合は、アプリケーション サーバ。

ロード バランサの設定

アプリケーション サーバが 1 つ以上ある場合は、アプリケーション サーバをモニタするためにロード バランサを設定します。

次の手順に従ってください:

1. アプリケーション サーバにログインします。
2. HealthServlet.war ファイルを \$NX_ROOT/samples/HealthServlet ディレクトリから \$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps ディレクトリにコピーします。
3. CA SDM サービスを再起動するか、または CA SDM Tomcat を再起動します。
4. その他すべてのアプリケーション サーバに対して、手順 1 ～ 3 を繰り返します。
5. 各アプリケーション サーバ上の以下の healthservlet URL をモニタするためにロード バランサを設定します。

`http://<Machine_name>:<Port_number>/HealthServlet/GetHealth`

- 休止応答をアプリケーション サーバの healthservlet URL から受信した場合、ロード バランサはそのサーバから他のアプリケーション サーバにリクエストをすべてリダイレクトする必要があります。たとえば、アプリケーション サーバが 58677 秒間休止される場合、以下の応答が送信されます。

`Quiesce time remaining :58677 seconds`

- アプリケーション サーバが正常で、休止が必要ない場合、以下の応答がサーバの healthservlet から送信されます。

`Currently no Quiesce time set. Return code : -1`

6. 各ロード バランサ上のセッション永続性を設定します。このプロセスにより、1 つのアプリケーション サーバから送信されたリクエストは同じアプリケーション サーバに確実に戻されます。

サーバの詳細の確認

すべてのサーバを設定した後、各サーバが正しく設定され、使用可能になっていることを確認します。

(高可用性設定の場合)次の手順に従ってください:

1. すべてのバックグラウンド、スタンバイ、およびアプリケーションサーバが実行されていることを確認します。
2. バックグラウンドサーバの **Web UI** にログインします。
3. [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。
4. スタンバイ サーバおよびアプリケーション サーバのレコードに対応する [設定済み] フィールドに [はい] が表示されていることを確認します。
5. [レコード ステータス] が [非アクティブ] に設定されている場合は、サーバを編集して [アクティブ] に設定します。いずれかのサーバのレコード ステータスを変更した場合は、そのサーバを再設定します。

サーバが高可用性設定で正常に設定されました。

注: [サーバの詳細] ページでいずれかのローカル ホスト エントリをクリックすると、そのサーバの詳細を表示できます。

(標準設定の場合)次の手順に従ってください:

1. プライマリおよびすべてのセカンダリ サーバが実行されていることを確認します。
2. プライマリ サーバの **Web UI** にログインします。
3. [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。
4. [レコード ステータス] が [非アクティブ] に設定されている場合は、サーバを編集して [アクティブ] に設定します。レコード ステータスを変更した場合は、そのサーバを再設定してください。

サーバは正常に設定されました。

標準設定から高可用性設定に変換する方法

標準設定から高可用性設定に変換する前に、すべてのサーバ上で CA SDM r12.9 にアップグレードしたか、またはすでにこれをインストールしていることを確認してください。

以下の図は、標準設定から高可用性設定に変換する方法を示しています。



次の手順に従ってください:

1. 高可用性設定を計画します。詳細については、計画シナリオまたは「実装ガイド」を参照してください。
2. セカンダリサーバ上のすべてのサービスを停止します。
3. [すべてのセカンダリサーバを非アクティブ化します](#) (P. 170)。

4. [バックグラウンド サーバを設定します](#) (P. 170)。
5. [セカンダリ サーバのタイプを変更します](#) (P. 171)。
6. スタンバイまたはアプリケーション サーバを設定します。
7. サーバの[詳細を確認します](#) (P. 174)。

すべてのセカンダリ サーバの非アクティブ化

高可用性設定用にサーバを設定する前に、すべてのセカンダリ サーバを非アクティブ化してください。

次の手順に従ってください:

1. プライマリ サーバの Web UI にログインします。
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. セカンダリ サーバのホスト名をクリックします。
[サーバの詳細] ページが開きます。
4. [編集] をクリックします。
5. [レコードステータス] を [非アクティブ] に変更します。
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。
6. [保存] をクリックします。
セカンダリ サーバが非アクティブに設定されます。
7. ほかのすべてのセカンダリ サーバに対して、手順 3 ~ 6 を実行します。
すべてのセカンダリ サーバが非アクティブに設定されます。

バックグラウンド サーバの設定

アプリケーション サーバまたはスタンバイ サーバを設定する前にバックグラウンド サーバを設定します。

次の手順に従ってください:

1. プライマリ サーバにログインします。

2. `pdm_configure` コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
3. 設定タイプとして [高可用性] を選択し、プロンプトに従って設定を完了します。詳細については、「[サーバ設定ヘルプ](#)」を参照してください。
バックグラウンドサーバが設定されます。

セカンダリ サーバのタイプの変更

バックグラウンドサーバを設定した後、すべてのセカンダリ サーバのサーバタイプをアプリケーションサーバおよびスタンバイサーバに変更し、それらのサーバをアクティブ化します。

次の手順に従ってください：

1. バックグラウンドサーバが実行されていることを確認します。
2. バックグラウンドサーバの **Web UI** にログインします。
3. [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。
4. すべてのセカンダリサーバの [レコードステータス] を [アクティブ] に設定します。
5. 必要に応じて、すべてのセカンダリサーバのサーバタイプをアプリケーションサーバまたはスタンバイサーバに変更します。
すべてのセカンダリサーバのサーバタイプが変更されます。

スタンバイ サーバおよびアプリケーション サーバの設定

バックグラウンド サーバを設定した後、各スタンバイおよびアプリケーション サーバを設定します。この設定は、バックグラウンド サーバとの通信を確立するために必要です。

重要: (推奨) バックグラウンド サーバとその他のすべてのスタンバイサーバの両方が同じ設定になっていることを確認してください。この処理により、フェールオーバー中にスタンバイ サーバが新しいバックグラウンドサーバになったとき、スタンバイ サーバが古いバックグラウンドサーバと同様に機能できます。

次の手順に従ってください：

1. セカンダリ サーバにログインします。
2. `pdm_configure` コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
3. 設定タイプとして [高可用性] を選択し、プロンプトに従って設定を完了します。詳細については、「[サーバ設定ヘルプ](#)」を参照してください。
4. スタンバイ サーバおよびアプリケーション サーバとして設定する各サーバ上で手順 1～3 を繰り返します。

スタンバイ サーバおよびアプリケーション サーバを設定しました。

5. 1 つ以上のアプリケーション サーバがあり、別のアプリケーションサーバとの間のリクエストを追跡するためにロードバランサを使用する場合は、[ロードバランサを設定](#) (P. 167) します。

注: CA SDM 通知でロードバランサ URL またはアプリケーションサーバ URL をリンクに使用するには、以下の手順に従います。

- a. バックグラウンド サーバにログインします。
 - b. [管理] タブで [オプション マネージャ] - [通知] を選択します。
 - c. `web_cgi_url` オプションの値を、以下のものを指すように変更します。
 - 複数のアプリケーション サーバが存在する場合は、ロードバランサ。
 - アプリケーション サーバが 1 つしか存在しない場合は、アプリケーション サーバ。
6. [サーバの詳細を確認します](#) (P. 174)。

ロード バランサの設定

アプリケーション サーバが 1 つ以上ある場合は、アプリケーション サーバをモニタするためにロード バランサを設定します。

次の手順に従ってください:

1. アプリケーション サーバにログインします。
2. HealthServlet.war ファイルを `$NX_ROOT/samples/HealthServlet` ディレクトリから `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps` ディレクトリにコピーします。
3. CA SDM サービスを再起動するか、または CA SDM Tomcat を再起動します。
4. その他すべてのアプリケーション サーバに対して、手順 1 ～ 3 を繰り返します。
5. 各アプリケーション サーバ上の以下の healthservlet URL をモニタするためにロード バランサを設定します。

`http://<Machine_name>:<Port_number>/HealthServlet/GetHealth`

- 休止応答をアプリケーション サーバの healthservlet URL から受信した場合、ロード バランサはそのサーバから他のアプリケーション サーバにリクエストをすべてリダイレクトする必要があります。たとえば、アプリケーション サーバが 58677 秒間休止される場合、以下の応答が送信されます。

`Quiesce time remaining :58677 seconds`

- アプリケーション サーバが正常で、休止が必要ない場合、以下の応答がサーバの healthservlet から送信されます。

`Currently no Quiesce time set. Return code : -1`

6. 各ロード バランサ上のセッション永続性を設定します。このプロセスにより、1 つのアプリケーション サーバから送信されたリクエストは同じアプリケーション サーバに確実に戻されます。

サーバの詳細の確認

すべてのサーバを設定した後、各サーバが正しく設定され、使用可能になっていることを確認します。

次の手順に従ってください:

1. すべてのバックグラウンド、スタンバイ、およびアプリケーションサーバが実行されていることを確認します。
2. バックグラウンドサーバの **Web UI** にログインします。
3. [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。
4. スタンバイ サーバおよびアプリケーション サーバのレコードに対応する [設定済み] フィールドに [はい] が表示されていることを確認します。
5. [レコード ステータス] が [非アクティブ] に設定されている場合は、サーバを編集して [アクティブ] に設定します。いずれかのサーバのレコード ステータスを変更した場合は、そのサーバを再設定します。

サーバが高可用性設定で正常に設定されました。

注: [サーバの詳細] ページでいずれかのローカル ホスト エントリをクリックすると、そのサーバの詳細を表示できます。

高可用性設定から標準設定に変換する方法

高可用性設定から標準設定に戻すことができます。以下の図は、高可用性設定から標準設定に変換する方法を示しています。



次の手順に従ってください:

1. [前提条件を確認します。](#) (P. 176)
2. アプリケーション サーバおよびスタンバイ サーバ上のすべてのサービスを停止します。
3. [すべてのアプリケーション サーバおよびスタンバイ サーバを非アクティブ化します](#) (P. 176)。
4. [プライマリ サーバを設定します](#) (P. 163)。

5. [アプリケーション サーバおよびスタンバイ サーバのタイプを変更します](#) (P. 178)。
6. [セカンダリ サーバを設定します](#) (P. 165)。
7. [サーバの詳細の確認](#) (P. 179)

前提条件を確認します。

標準設定に変換する前に、以下の前提条件を確認します。

1. 標準設定を計画していること。詳細については、「[実装ガイド](#)」の「計画」を参照してください。
2. プライマリ サーバとして設定できるのは、バックグラウンドサーバだけです。
3. セカンダリ サーバとして設定できるのは、スタンバイ サーバおよびアプリケーション サーバだけです。

すべてのアプリケーション サーバおよびスタンバイ サーバの非アクティブ化

標準設定用にサーバを設定する前に、すべてのアプリケーション サーバおよびスタンバイ サーバを非アクティブ化してください。

次の手順に従ってください:

1. バックグラウンドサーバの **Web UI** にログインします。
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. アプリケーションサーバのホスト名をクリックします。
[サーバの詳細] ページが開きます。
4. [編集] をクリックします。
5. [レコードステータス] を [非アクティブ] に変更します。

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。

6. [保存] をクリックします。

アプリケーション サーバが非アクティブに設定されます。

7. ほかのすべてのアプリケーション サーバおよびスタンバイ サーバに対して、手順 3 ～ 6 を実行します。

すべてのアプリケーション サーバおよびスタンバイ サーバが非アクティブに設定されます。

プライマリ サーバの設定

セカンダリ サーバを設定する前に、プライマリ サーバを設定する必要があります。

次の手順に従ってください:

1. バックグラウンド サーバの **Web UI** にログインします。
2. バックグラウンド サーバの **Web UI** を使用して、バックグラウンド サーバを非アクティブにします。
3. **pdm_configure** コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
4. 設定タイプとして [標準] を選択し、プロンプトに従って設定を完了します。詳細については、「サーバ設定ヘルプ」を参照してください。
プライマリ サーバが設定されます。

サーバの詳細の確認

プライマリ サーバを設定した後、すべてのアプリケーション サーバおよびスタンバイ サーバのサーバタイプをセカンダリ サーバに変更し、それらのサーバをアクティブ化します。

次の手順に従ってください：

1. プライマリ サーバが実行されていることを確認します。
2. プライマリ サーバの Web UI にログインします。
3. [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。
4. すべてのアプリケーション サーバおよびスタンバイ サーバの[レコードステータス] を[アクティブ] に設定します。
5. すべてのアプリケーション サーバおよびスタンバイ サーバのサーバタイプをセカンダリ サーバに変更します。

すべてのアプリケーション サーバおよびスタンバイ サーバのサーバタイプが変更されます。

セカンダリ サーバの設定

プライマリ サーバを設定した後に各セカンダリ サーバを設定します。この設定は、プライマリ サーバとの通信を確立するために必要です。

次の手順に従ってください：

1. 新しいセカンダリ サーバとして設定するアプリケーションまたはスタンバイ サーバにログインします。
2. `pdm_configure` コマンドを使用して、設定を開始します。
[サーバ構成の選択] 画面が開きます。
3. 設定タイプとして[標準]を選択し、プロンプトに従って設定を完了します。詳細については、「[サーバ設定ヘルプ](#)」を参照してください。
セカンダリ サーバが設定されます。
4. セカンダリ サーバとして設定する各サーバ上で手順 1～3 を繰り返します。

サーバの詳細の確認

すべてのサーバを設定した後、各サーバが正しく設定され、使用可能になっていることを確認します。

次の手順に従ってください:

1. プライマリおよびすべてのセカンダリ サーバが実行されていることを確認します。
2. プライマリ サーバの Web UI にログインします。
3. [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。
4. [レコード ステータス] が [非アクティブ] に設定されている場合は、サーバを編集して [アクティブ] に設定します。レコード ステータスを変更した場合は、そのサーバを再設定してください。

サーバは正常に設定されました。

CA MDB をインストールする方法

注: このコンポーネントをインストールする前に、[CA MDB のインストールを計画する](#) (P. 114) ようにしてください。

重要: UNC パスを使用した DVD イメージのマッピングは、CA MDB インストーラではサポートされていません。

CA SDM で使用するデータベース (SQL Server と Oracle のいずれか) が CA SDM プライマリ サーバとは異なるコンピュータ上にインストールされている場合、リモート データベース サーバ (すなわち SQL Server または Oracle がインストールされているコンピュータ) に CA MDB を手動でインストールします。CA MDB とプライマリ サーバが同じコンピュータ上にある場合は、CA MDB を手動でインストールする必要はありません。CA SDM のインストール中に、CA SDM によって CA MDB が自動的にインストールされます。

注: プライマリ サーバ上に管理データベースをインストールする場合は、データベース サーバをホストしているリモート コンピュータ上で CA MDB のインストールを開始して実行する必要があります。

関連項目:

[CA MDB のインストールの計画](#) (P. 114)

[SQL Server へのインストール \(Windows\)](#) (P. 181)

[Oracle でのインストール \(Windows\)](#) (P. 183)

[Oracle へのインストール \(Linux/UNIX\)](#) (P. 186)

MDB のインストール

MDB のインストールでは、以下の要件が適用されます。

- MDB インストールを実行して SQL データベースを異なるサーバにインストールする場合は、SQL Native Client、クライアントツール、および管理ツールが CA CMDB クライアントにインストールされている必要があります。
- すべての Oracle データベース セットアップで、Oracle クライアントソフトウェアもインストールする必要があります。Oracle クライアントソフトウェアは、Oracle の Web サイトからダウンロードできます。

製品の統合と互換性の情報の特定

CA サポート オンラインが提供する情報を使用して、CA SDM およびその他の製品と CA MDB の互換性を理解できます。

- CA Service Accounting および CA Service Catalog の統合ガイド - CA MDB のバージョンと、ほかの製品が CA MDB と統合できるように CA MDB 互換性パッチをインストールする必要があるかどうかを判別する方法について説明しています。
- CA 管理データベースのバージョン混在インストール - CA MDB の互換性について説明しています。

CA MDB との統合の情報を特定する方法

1. ブラウザを開いて、<http://support.ca.com> に移動します。
CA サポート オンラインのページが表示されます。
2. CA サポート オンラインにログオンします。
3. 左ペインにある [ドキュメント] リンクをクリックします。
[ドキュメント] ページが表示されます。

4. ドロップダウン リストから [CA Service Catalog] - [r12] - [US English] を選択します。 [実行] をクリックします。

CA Service Catalog のドキュメント リストが表示されます。

5. 「統合ガイド J02775-1E」の PDF リンクをクリックします。
[CA Accounting と CA Service Catalog Service の統合ガイド] が表示されます。

6. [以前のバージョンの MDB ブックマークを使用する CA 製品との有効化] をクリックします

この情報を、製品と CA MDB を統合する際に使用できます。

互換性情報を特定する方法

1. ブラウザを開いて、<http://support.ca.com> に移動します。
CA サポート オンラインのページが表示されます。
2. CA サポート オンラインにログオンします。
3. [サポート] ペインで [ナレッジ ベース検索] をクリックします。
[ナレッジ ベース検索] ページが表示されます。
4. [検索] フィールドに「**MDB104 互換性**」と入力します。 [検索] をクリックします。
[ナレッジ ベース検索結果] が表示されます。
5. [CA 管理データベースのバージョン混在インストール] リンクをクリックします。
[CA 管理データベースのバージョン混在インストール] ドキュメントが表示されます。

SQL Server へのインストール(Windows)

高可用性設定を使用しており、使用している CA MDB が CA SDM サーバとは別のコンピュータにインストールされている場合は、リモートデータベース サーバ (SQL Server がインストールされているコンピュータ) に CA MDB をインストールする必要があります。

次の手順に従ってください:

1. ドライブにインストール メディアを挿入します。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、**CA SDM** をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

2. リストから言語を選択し、[言語の選択] をクリックします。

インストール メニューが表示されます。

注: インストール メニューが自動的に表示されない場合は、インストール メディアのルートにある **setup.exe** ファイルをダブルクリックしてインストールを開始します。

3. [製品のインストール] タブをクリックします。

4. **CA MDB** をクリックします。

5. インストールを続行するには、画面の手順に従います。

6. 入力を求められたら、データベース タイプとして **SQL Server** を選択し、**SQL Server** の適切な情報を入力します。

注: 入力する **SQL Server** の情報がわからない場合は、サーバ構成のオンラインヘルプを参照してください。

7. 引き続き画面の指示に従って **CA MDB** のインストールを完了します。

CA MDB が **SQL Server** にインストールされます。

関連項目:

[インストール ログ](#) (P. 277)

Oracle でのインストール (Windows)

高可用性設定を使用しており、使用している CA MDB が CA SDM サーバとは別のコンピュータにインストールされている場合は、リモート データベース サーバ (SQL Server がインストールされているコンピュータ) に CA MDB をインストールする必要があります。

次の手順に従ってください:

1. ドライブにインストール メディアを挿入します。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、CA SDM をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモート インストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

インストール メニューが表示されます。

注: インストール メニューが自動的に表示されない場合は、インストール メディアのルートにある `setup.exe` ファイルをダブルクリックしてインストールを開始します。

2. [製品のインストール] タブをクリックします。
3. CA MDB をクリックします。
4. インストールを続行するには、画面の手順に従います。
5. 入力を求められたら、データベース タイプとして Oracle を選択し、Oracle の適切な情報を入力します。

注: 入力する Oracle の情報がわからない場合は、サーバ構成のオンライン ヘルプを参照してください。

6. Oracle データベースを設定するための情報を入力および選択します。

CA SDM では、MDB が置かれている Oracle データベースを指定する ネット サービス名が必要です。また、そのデータベースのシステム識別子 (SID) も必要です。これらの名前は異なることもありますが、同じ MDB データベースを指定します。CA SDM には 2 つの名前の値が必要です。これは、CA SDM が Oracle クライアント テクノロジーと JDBC テクノロジーの両方を使用してデータベースにアクセスするからです。

注: サービス名および SID の詳細については、Oracle のマニュアルを参照してください。

データのデフォルト値のロード

Oracle データベースにデフォルトの **CA SDM** データをロード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、**CA SDM** のデフォルトのシステム データが **Oracle** データベースにロードされます。システムのデフォルト値を変更した場合は、このオプションにより、値が置き換えられます。初回インストールの場合は、このチェック ボックスをオンにします。初回インストールでない場合、このオプションは既存のデータを置換します。このチェック ボックスをオフにすると、デフォルト データはロードされません。

リモート データベース

Oracle データベースが **CA SDM** プライマリ サーバ以外のサーバにインストールされていることを示します。**CA SDM** インストールを実行する前に、リモート データベース サーバ (すなわち、**Oracle** がインストールされているコンピュータ) に **CA MDB** を手動でインストールします。

Oracle サーバがローカルである (選択されていない) 場合、MDB がまだ作成されていないと **CA SDM** は **MDB** を作成します。

テーブル領域の作成

MDB データベース用のテーブル領域を作成するか、またはすでに作成済みのテーブル領域を使用するかを指定します。

- テーブル領域がすでに手動で作成されている場合は、このチェック ボックスをオフにします。既存のテーブル領域の名前を指定します。製品の [テーブル領域パス] フィールドが無効になり、[データ テーブル領域名] フィールドおよび [インデックス テーブル領域名] フィールドが有効になります。
- このチェック ボックスをオンにして **MDB_DATA** および **MDB_INDEX** のデフォルト名でテーブル領域を作成します。テーブル領域パスを指定します。[データ テーブル領域名] フィールドおよび [インデックス テーブル領域名] フィールドは無効になります。

注: Oracle Automated Storage Manager (ASM) を使用している場合は、CA SDM インストールを実行する前に、Oracle テーブル領域を手動で作成します。Oracle がインストールされて ASM に設定された場合、MDB のインストール中に Oracle テーブル領域を作成することはできません。ASM が仮想ストレージを使用しているのに、物理ディレクトリを検索することになるため、この構成では正常にテーブル領域を作成することができません。

ネット サービス名

MDB が置かれている Oracle データベースのネット サービス名を指定します。データベースがリモートの場合は、ローカルコンピュータ上の Oracle クライアント内で定義されたネット サービス名を使用します。CA SDM では Oracle クライアントのローカルインストールを使用してデータベースにアクセスしますが、Oracle サーバ上のサービス名とは異なるネット サービス名が指定されている場合があります。

mdbadmin ユーザ パスワード

mdbadmin ユーザ パスワードを指定します。既存のパスワードを入力するか、CA SDM がユーザを作成する場合は新しいパスワードを指定します。

DBA ユーザ名

DBA アクセス権（通常は SYS）を持つ Oracle ユーザの名前を指定します。このフィールドは、Oracle サーバがローカルコンピュータ上で実行されている場合のみ使用されます。

DBAパスワード

DBA ユーザのパスワードを指定します。このフィールドは、Oracle サーバがローカルコンピュータ上で実行されている場合のみ使用されます。

データ テーブル領域名

[テーブル領域の作成] チェック ボックスがオンになっている場合は、指定されたデータ テーブル領域名を作成します。このフィールドは、Oracle サーバがローカルコンピュータ上で実行されている場合のみ使用されます。

インデックス テーブル領域名

[テーブル領域の作成] チェック ボックスがオンになっている場合は、指定されたインデックス テーブル領域名を作成します。このフィールドは、**Oracle** サーバがローカル コンピュータ上で実行されている場合のみ使用されます。

テーブル領域パス

前述のテーブル領域が存在しない場合に作成される、テーブル領域の物理的なロケーションのディレクトリ パスを指定します。このフィールドは、**Oracle** サーバがローカル コンピュータ上で実行されている場合のみ使用されます。

Oracle ホーム パス

Oracle ホーム パスのディレクトリ パスを指定します。

JDBC 接続性

JDBC 接続性を使用するかどうかを指定します。**CA SDM** のコンポーネントの中には **JDBC** テクノロジを使用してデータベースにアクセスするものがあります。こういったコンポーネントの場合は、**Oracle** サーバに関する特定の情報が必要となります。

以前に設定したデータベース ホスト名、**SID**、およびリスナ ポートを識別します。

CA MDB が **Oracle** にインストールされます。

関連項目:

[インストール ログ](#) (P. 277)

Oracle へのインストール (Linux/UNIX)

高可用性設定を使用しており、使用している **CA MDB** が **CA SDM** サーバとは別のコンピュータにインストールされている場合は、リモートデータベース サーバ (**SQL Server** がインストールされているコンピュータ) に **CA MDB** をインストールする必要があります。

注: **Oracle** 環境が正しくセットアップされており、アクセス可能であることを確認してください。

次の手順に従ってください:

1. インストール メディアをドライブにマウントします。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、**CA SDM** をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

2. インストール メディアのルートディレクトリに移動し、以下のコマンドを実行して、インストールを開始します。

```
sh ./setup.sh
```

3. リストから言語を選択し、[言語の選択] をクリックします。

インストール メニューが表示されます。

4. [製品のインストール] タブをクリックします。

5. CA MDB をクリックします。

6. インストールを続行するには、画面の手順に従います。

7. 入力を求められたら、データベース タイプとして **Oracle** を選択し、**Oracle** の適切な情報を入力します。

注: 入力する **Oracle** の情報がわからない場合は、サーバ構成のオンライン ヘルプを参照してください。

8. 引き続き画面の指示に従って **CA MDB** のインストールを完了します。

CA MDB が **Oracle** にインストールされます。

関連項目:

[インストール ログ](#) (P. 277)

リモート MDB の HP-UX へのインストール

リモート MDB を HP-UX にインストールできます。

次の手順に従ってください:

1. CA サポート ポータルから HP-UX 用の CA MDB インストーラをダウンロードするか、または CA テクニカル サポートから同じインストーラを入手します。
2. インストーラを任意の場所に展開します。
3. CA MDB フォルダにすべてのユーザがアクセスできることを確認します。

例: `chmod - R 777 mdb`

4. Oracle フォルダに移動して、以下のコマンドを実行します。

```
./setupmdb.sh -DBVENDOR=oracle -DBHOST=<DBHOST_NAME> -DBNAME=<ORACLE_SID>  
-DBUSER=<DB_User_SYS_name> -DBPASSWORD=<DB_User_SYS_password>  
-MDB_ADMIN_PSWD=<MDB_ADMIN_PASSWORD>  
-ORA_TBLSpace_PATH=<Oracle_Table_Space_path> -MANIFEST=Service_Desk  
-WORKSPACE=Service_Desk -JRE_DIR=<JRE_PATH> -MDB_COMMON_DIR=<mdb_Common_DIR>
```

5. たとえば、以下のコマンドを実行します。

```
./setupmdb.sh -DBVENDOR=oracle -DBHOST=hostname -DBNAME=mdb -DBUSER=SYS  
-DBPASSWORD=mdbpassword -MDB_ADMIN_PSWD=mdbpassword  
-ORA_TBLSpace_PATH=/sdhome/oracle/oracle/product/10.2.0/db_1/oradata/mdb  
-MANIFEST=Service_Desk -WORKSPACE=Service_Desk  
-JRE_DIR=/sdhome/opt/Sharedcomponents/JRE/1.6.0_00  
-MDB_COMMON_DIR=/sdhome/opt/Sharedcomponents/Mdb
```

CA MDB のインストールが完了し、インストールが成功したことを示すメッセージが表示されます。

CA SDM をインストールする方法

注: このコンポーネントをインストールする前に、[CA SDM のインストールを計画する \(P. 118\)](#)ようにしてください。また、Linux および UNIX へのインストールの場合、色のプロパティが白地に白い文字に設定されていると、ポップアップ メッセージの中にはっきりと表示されないものがあります。

CA SDM を起動してサーバにインストールすると、製品を使用するための以下のファイル、コンポーネント、および機能がインストールされます。

- サーバの機能は、インストール後の製品の設定方法に基に基づきます。
- SQL Server または Oracle インターフェース
- ODBC インターフェース

重要: ODBC インターフェースのインストールは、CA Business Intelligence を備えた CA SDM の Business Objects レポート機能用 ODBC ドライバに単にアクセスできるようにすることを目的としています。ほかのアプリケーションでの ODBC ドライバの使用は、CA Technologies で直接的にはサポート、認定、または保証されていないため、各自の責任で使用してください。

- Web インターフェース
- CA CMDB

重要: 設定中に、CA CMDB スタンドアロンバージョンから CA SDM にマイグレートすると、[CMDB のみを設定] チェック ボックスが表示されます。[CMDB のみを設定] チェック ボックスをオフにして [次へ] をクリックすると、CA CMDB を再度設定することはできません。[戻る] をクリックしても、[CMDB のみを設定] チェック ボックスは使用できません。[環境設定] ダイアログに、この動作を警告するメッセージが表示されます。設定が完了して再起動する前に、その設定をキャンセルした場合は、[CMDB のみを設定] チェック ボックスは使用できます。

[CMDB のみを設定] チェック ボックスは、CA SDM 環境変数 NX_CMDB の値を制御します。環境変数は、サポート オートメーション機能が設定されているかどうかを制御します。チェック ボックスがオフになっている場合、サポート オートメーション は設定可能ですが、それ以外の場合は設定できません。環境変数は Web フォームの動作に影響を与える場合があります。

- Visualizer
- サポート オートメーション

CA SDM の環境設定中、サポート オートメーション を設定した後に、*supportautomation_url* オプションをインストールします。こ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。

重要: CA SDM をアンインストールすると、CA Workflow もアンインストールされます。

関連項目:

[CA SDM のインストールの計画](#) (P. 118)

[SQL Server へのインストール \(Windows\)](#) (P. 190)

[Oracle でのインストール \(Windows\)](#) (P. 193)

[Oracle へのインストール \(Linux/UNIX\)](#) (P. 198)

Oracle 環境変数

CA SDM のインストールまたはマイグレートの前に、Oracle の環境変数を以下のように設定します。

- ORACLE_HOME 環境変数が正しく設定されていることを確認します。
重要: Oracle 32 ビット クライアント変数が Windows 以外にエクスポートされる場合は、TWO_TASK 変数をエクスポートする必要があります。
- 32 ビット Oracle ライブラリ (64 ビット Oracle では通常 \$ORACLE_HOME/lib32) を、ライブラリ パス変数 LD_LIBRARY_PATH (AIX では LIBPATH) に追加します。

SQL Server へのインストール(Windows)

CA SDM を起動してサーバにインストールすると、以下のコンポーネントおよび機能がインストールされます。

- サーバの機能は、インストール後の製品の設定方法に基づきます。
- SQL Server インターフェース
- Web インターフェース
- ODBC インターフェース

重要: ODBC インターフェースのインストールは、CA Business Intelligence を備えた CA SDM の Business Objects レポート機能用 ODBC ドライバに単にアクセスできるようにすることを目的としています。ほかのアプリケーションでの ODBC ドライバの使用は、CA Technologies で直接的にはサポート、認定、または保証されていないため、各自の責任で使用してください。

次の手順に従ってください:

1. ドライブにインストール メディアを挿入します。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、**CA SDM** をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

2. リストから言語を選択し、[言語の選択] をクリックします。

インストール メニューが表示されます。

注: インストール メニューが自動的に表示されない場合は、インストール メディアのルートにある **setup.exe** ファイルをダブルクリックしてインストールを開始します。

3. [製品のインストール] タブをクリックします。
4. [CA SDM] をクリックします。
5. インストールを続行するには、画面の指示に従います。

構成ウィザードが表示されます。

注: インターネットプロトコルバージョン 4 (IPv4) ホストおよびインターネットプロトコルバージョン 6 (IPv6) ホストがネットワーク上に共存している場合は、製品の設定を始める前に、これらのテクノロジーに対応した適切な移行方針、ツール、およびメカニズムが整っていることを確認してください。サーバの構成の詳細については、「**管理ガイド**」を参照してください。

6. 製品の構成情報を入力および選択します。

注: ウィザードに表示されるフィールドの詳細については、オンラインヘルプを参照してください。

7. 引き続き画面の指示に従って、インストールを完了します。
CA SDM が SQL Server にインストールされます。
8. インストールが完了したら、**pslist.exe** のダウンロードおよび実行に関する手順が表示されます。これらの手順を完了させて[次へ]をクリックしてください。
9. CA SDM をインストール（または CA CMDB スタンドアロン システムから CA SDM にマイグレート）した後、**cmdb_update_ambiguity** ユーティリティを実行します。**-h** コマンドを使用して、必須オプションを表示します。不明確性インデックスの計算の詳細については、「*管理ガイド*」を参照してください。

注: 拡張テーブルの検証手順の間に設定に失敗した場合は、データベース接続が案件になる場合があります。構成を再度実行し、指定したデータベース接続情報が正しいことを確認してください。

関連項目:

[インストール ログ](#) (P. 277)

[インストールの確認](#) (P. 276)

[Web インターフェースの開始](#) (P. 290)

Oracle でのインストール(Windows)

CA SDM を起動してサーバにインストールすると、以下のコンポーネントおよび機能がインストールされます。

- サーバの機能は、インストール後の製品の設定方法に基に基づきます。
- Oracle インターフェース
- Web インターフェース
- ODBC インターフェース

CA MDB または CA SDM をインストールするには、管理者である必要があります。

重要: ODBC インターフェースのインストールは、CA Business Intelligence を備えた CA SDM の Business Objects レポート機能用 ODBC ドライバに単にアクセスできるようにすることを目的としています。ほかのアプリケーションでの ODBC ドライバの使用は、CA Technologies で直接的にはサポート、認定、または保証されていないため、各自の責任で使用してください。

次の手順に従ってください:

1. ドライブにインストール メディアを挿入します。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、CA SDM をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

2. リストから言語を選択し、[言語の選択] をクリックします。

インストール メニューが表示されます。

注: インストール メニューが自動的に表示されない場合は、インストール メディアのルートにある `setup.exe` ファイルをダブルクリックしてインストールを開始します。

3. [製品のインストール] タブをクリックします。

4. [CA SDM] をクリックします。
5. インストールを続行するには、画面の指示に従います。

構成ウィザードが表示されます。

注: インターネットプロトコルバージョン 4 (IPv4) ホストおよびインターネットプロトコルバージョン 6 (IPv6) ホストがネットワーク上に共存している場合は、製品の設定を始める前に、これらのテクノロジーに対応した適切な移行方針、ツール、およびメカニズムが整っていることを確認してください。サーバの構成の詳細については、「*管理ガイド*」を参照してください。

6. Oracle データベースを設定するための情報を入力および選択します。

CA SDM では、MDB が置かれている Oracle データベースを指定する ネット サービス名が必要です。また、そのデータベースのシステム識別子 (SID) も必要です。これらの名前は異なることもありますが、同じ MDB データベースを指定します。CA SDM には 2 つの名前の値が必要です。これは、CA SDM が Oracle クライアントテクノロジーと JDBC テクノロジーの両方を使用してデータベースにアクセスするからです。

注: サービス名および SID の詳細については、Oracle のマニュアルを参照してください。

データのデフォルト値のロード

Oracle データベースにデフォルトの CA SDM データをロード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、CA SDM のデフォルトのシステム データが Oracle データベースにロードされます。システムのデフォルト値を変更した場合は、このオプションにより、値が置き換えられます。初回インストールの場合は、このチェック ボックスをオンにします。初回インストールでない場合、このオプションは既存のデータを置換します。このチェック ボックスをオフにすると、デフォルト データはロードされません。

リモート データベース

Oracle データベースがリモート サーバにインストールされていることを示します。CA SDM インストールを実行する前に、リモート データベース サーバ（すなわち、Oracle がインストールされているコンピュータ）に CA MDB を手動でインストールします。

Oracle サーバがローカルである（選択されていない）場合、MDB がまだ作成されていないと CA SDM は MDB を作成します。

テーブル領域の作成

MDB データベース用のテーブル領域を作成するか、またはすでに作成済みのテーブル領域を使用するかを指定します。

- テーブル領域がすでに手動で作成されている場合は、このチェック ボックスをオフにします。既存のテーブル領域の名前を指定します。製品の [テーブル領域パス] フィールドが無効になり、[データ テーブル領域名] フィールドおよび [インデックス テーブル領域名] フィールドが有効になります。

- このチェック ボックスをオンにして **MDB_DATA** および **MDB_INDEX** のデフォルト名でテーブル領域を作成します。テーブル領域パスを指定します。[データ テーブル領域名] フィールドおよび [インデックス テーブル領域名] フィールドは無効になります。

注: Oracle Automated Storage Manager (ASM) を使用している場合は、CA SDM インストールを実行する前に、Oracle テーブル領域を手動で作成します。Oracle がインストールされて ASM に設定された場合、MDB のインストール中に Oracle テーブル領域を作成することはできません。ASM が仮想ストレージを使用しているのに、物理ディレクトリを検索することになるため、この構成では正常にテーブル領域を作成することができません。

ネット サービス名

MDB が置かれている Oracle データベースのネット サービス名を指定します。データベースがリモートの場合は、ローカル コンピュータ上の Oracle クライアント内で定義されたネット サービス名を使用します。CA SDM では Oracle クライアントのローカルインストールを使用してデータベースにアクセスしますが、Oracle サーバ上のサービス名とは異なるネット サービス名が指定されている場合があるためです。

mdbadmin ユーザ パスワード

mdbadmin ユーザ パスワードを指定します。既存のパスワードを入力するか、CA SDM がユーザを作成する場合は新しいパスワードを指定します。

DBA ユーザ名

DBA アクセス権 (通常は SYS) を持つ Oracle ユーザの名前を指定します。このフィールドは、Oracle サーバがローカル コンピュータ上で実行されている場合のみ使用されます。

DBAパスワード

DBA ユーザのパスワードを指定します。このフィールドは、Oracle サーバがローカル コンピュータ上で実行されている場合のみ使用されます。

データ テーブル領域名

[テーブル領域の作成] チェック ボックスがオンになっている場合は、指定されたデータ テーブル領域名を作成します。このフィールドは、Oracle サーバがローカル コンピュータ上で実行されている場合のみ使用されます。

インデックス テーブル領域名

[テーブル領域の作成] チェック ボックスがオンになっている場合は、指定されたインデックス テーブル領域名を作成します。このフィールドは、Oracle サーバがローカル コンピュータ上で実行されている場合のみ使用されます。

テーブル領域パス

前述のテーブル領域が存在しない場合に作成される、テーブル領域の物理的なロケーションのディレクトリ パスを指定します。このフィールドは、Oracle サーバがローカル コンピュータ上で実行されている場合のみ使用されます。

Oracle ホーム パス

Oracle ホーム パスのディレクトリ パスを指定します。

JDBC 接続性

JDBC 接続性を使用するかどうかを指定します。CA SDM のコンポーネントの中には JDBC テクノロジを使用してデータベースにアクセスするものがあります。こういったコンポーネントの場合は、Oracle サーバに関する特定の情報が必要となります。

以前に設定したデータベース ホスト名、SID、およびリスナ ポートを識別します。

7. 引き続き画面の指示に従って、インストールを完了します。

CA SDM が Oracle にインストールされます。

8. インストールが完了したら、`pslist.exe` のダウンロードおよび実行に関する手順が表示されます。これらの手順を完了させて[次へ]をクリックしてください。
9. CA SDM をインストール（または CA CMDB スタンドアロン システムから CA SDM にマイグレート）した後、`cmdb_update_ambiguity` ユーティリティを実行します。`-h` コマンドを使用して、必須オプションを表示します。不明確性インデックスの計算の詳細については、「[管理ガイド](#)」を参照してください。

関連項目:

[インストール ログ](#) (P. 277)

[インストールの確認](#) (P. 276)

[Web インターフェースの開始](#) (P. 290)

Oracle へのインストール (Linux/UNIX)

CA SDM を起動してサーバにインストールすると、以下のコンポーネントおよび機能がインストールされます。

- サーバの機能は、インストール後の製品の設定方法に基づきます。
- Oracle インターフェース
- Web インターフェース
- ODBC インターフェース

重要: ODBC インターフェースのインストールは、CA Business Intelligence を備えた CA SDM の Business Objects レポート機能用 ODBC ドライバに単にアクセスできるようにすることを目的としています。ほかのアプリケーションでの ODBC ドライバの使用は、CA Technologies で直接的にはサポート、認定、または保証されていないため、各自の責任で使用してください。

注: Oracle 環境が正しくセットアップされており、アクセス可能であることを確認してください。

次の手順に従ってください:

1. インストール メディアをドライブにマウントします。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、CA SDM をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

2. インストール メディアのルートディレクトリに移動し、以下のコマンドを実行して、インストールを開始します。

```
sh ./setup.sh
```

3. リストから言語を選択し、[言語の選択] をクリックします。

インストールメニューが表示されます。

注: Linux および UNIX へのインストールの場合、色のプロパティが白地に白い文字に設定されていると、ポップアップ メッセージの一部がはっきりと表示されない場合があります。

4. [製品のインストール] タブをクリックします。

5. [CA SDM] をクリックします。
6. インストールを続行するには、画面の指示に従います。

構成ウィザードが表示されます。

注: インターネットプロトコルバージョン 4 (IPv4) ホストおよびインターネットプロトコルバージョン 6 (IPv6) ホストがネットワーク上に共存している場合は、製品の設定を始める前に、これらのテクノロジーに対応した適切な移行方針、ツール、およびメカニズムが整っていることを確認してください。サーバの構成の詳細については、「管理ガイド」を参照してください。

7. 製品の構成情報を入力および選択します。

注: ウィザードに表示されるフィールドの詳細については、オンラインヘルプを参照してください。

8. 引き続き画面の指示に従って、インストールを完了します。

CA SDM が Oracle にインストールされます。

9. CA SDM をインストール（または CA CMDB スタンドアロン システムから CA SDM にマイグレート）した後、`cmdb_update_ambiguity` ユーティリティを実行します。-h コマンドを使用して、必須オプションを表示します。デフォルトで Oracle に設定されているため、Linux/Unix 環境では -d オプションは必要ありません。

注: 不明確性インデックスの計算の詳細については、「管理ガイド」を参照してください。

関連項目:

[インストール ログ \(P. 277\)](#)

[インストールの確認 \(P. 276\)](#)

[Web インターフェースの開始 \(P. 290\)](#)

Visualizer 設定

CA SDM のインストール中に Visualizer を設定できます。[Visualizer の設定] チェック ボックスをオンにすると、Visualizer 設定用のパネルが表示されます。

ウィザードの [次へ] ボタンをクリックすると、設定情報が検証されます。検証に成功した後、Visualizer 設定タスクによって、検証された Visualizer 設定情報が使用されます。

セカンダリ サーバ上に Visualizer を設定する方法

セカンダリ 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 の環境設定中、および *pdm_edit* ユーティリティを使用することで、セカンダリ サーバ上に Visualizer を開始して、設定します。

注: CA CMDB Visualizer のセカンダリ インストールでセカンダリ Web サービスを使用するように設定する場合は、ドロップダウンメニューからサーバ名を選択します。デフォルトの選択肢は [プライマリ] です。

次の手順に従ってください:

1. 環境設定ウィザードの [Visualizer] ページで [Visualizer の設定] を選択します。
2. Web ホストとしてセカンダリ CA SDM サーバを選択し、Web ホストポートを入力します。

セカンダリ CA SDM サーバ上で設定を実行している場合は、ドロップダウンメニューを使用して、使用可能な Web サービス ホスト [general.primary_server_node] および [general.local_host] プロパティ値を選択できます。

3. セカンダリ Visualizer サーバの CA SDM ポート番号を入力します。

4. 引き続き画面の指示に従って、インストールを完了します。
Visualizer がセカンダリ CA SDM サーバ上にインストールされ、設定されます。
5. コマンドプロンプトを開き、`$NX_ROOT¥samples¥pdmconf` フォルダに移動します。以下のコマンドを実行します。
`pdm_perl pdm_edit.pl`
メニューが表示されます。
6. Visualizer Tomcat サーバを編集するには、「Z」を入力します。Visualizer Tomcat サーバを追加するには、「A」を入力します。
ホスト名の入力を要求するメッセージが表示されます。
7. セカンダリ ホスト名を入力します。
セカンダリ ホスト名が保存され、テンプレートのリストが表示されます。
8. `pdm_edit.pl` ユーティリティの指示に従います。
セカンダリ Visualizer Tomcat の設定が完了します。

サポート オートメーション コンポーネントの設定

CA SDM では、以下のサポート オートメーション コンポーネントをインストールして設定します。

- エンドユーザ クライアント
- 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
- サーバ

以下のコンポーネントは、別途インストールして、設定します。

- エンドユーザ エージェント
- 自動タスク エディタ IDE

重要: CA SDM の環境設定中に サポート オートメーション を設定し、さらに、CA SDM のインストール後に `supportautomation_url` オプションをインストールする必要があります。`supportautomation_url` 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。

サポートオートメーション サーバモードの設定

インストール中に以下の サポート オートメーション サーバ モードを設定できます。

- **メインサーバ** - メインサーバ設定タイプを選択すると、[ホスト名または IP] フィールドのデフォルト値がローカルホスト名に設定されます。すべてのパラメータをメインサーバ用に入力する必要があります。ただし、[内部ポート] セクションおよび [ソケットサーバ] セクションの [IP にバインド] を除きます。これらのパラメータは、オプションです。

注: CA SDM の設定タイプに従って、以下の CA SDM サーバ上でメインサーバを設定してください。

- **標準:** プライマリサーバ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。

重要: `supportautomation_url` オプションを設定する際、この URL にはサポートオートメーションのメインサーバの URL を使用する必要があります。プロキシサーバやロードバランササーバを参照させないでください。これは、標準モデルにのみ適用できます。高可用性設定では、この URL はロードバランサ、メインサーバ、またはプロキシサーバを指すことができます。

注: [メインサーバ] オプションを選択し、しかも 1 つ以上のソケットプロキシサーバを設定することも計画している場合は、ソケットサーバのホスト名と、ソケットプロキシホストの外部ポートを設定する必要があります。ソケットプロキシが複数ある場合は、[ソケットサーバ] で、ロードバランササーバのホストおよび外部ポートを設定します。

- **ソケットプロキシサーバ** - CA SDM の設定に基づいて、以下のサーバ上でソケットプロキシサーバの設定タイプを選択できます。
 - **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。

フィールドのデフォルト値が表示されます。すべてのパラメータをソケットプロキシサーバ用に入力する必要があります。ただし、[ソケット設定] セクションの [IP にバインド] を除きます。このパラメータは、オプションです。

- メッセージルーティング サーバ - CA SDM の設定に基づいて、以下のサーバ上でメッセージルーティング サーバの設定タイプを選択できます。
 - 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。

フィールドのデフォルト値が表示されます。すべてのパラメータをメッセージルーティング サーバ用に入力する必要があります。ただし、[ソケット設定] セクションの [IP にバインド] を除きます。このパラメータは、オプションです。

セカンダリ サーバ上での サポート オートメーション の設定

セカンダリ CA SDM サーバ上に サポート オートメーション を設定できます。

次の手順に従ってください：

1. 環境設定ウィザードで サポート オートメーション を選択します。
2. ソケット サーバ上のホスト名とポートなど、セカンダリ サーバの設定タイプに適した情報を入力します。

重要： サポート オートメーション サーバを定義した後、そのプライマリまたはセカンダリ サーバとしてのロールは変更できません。

3. 引き続き画面の指示に従って、インストールを完了します。

サポート オートメーション がセカンダリ CA SDM サーバ上にインストールされ、設定されます。

4. プライマリ サーバ上で、コマンドプロンプトを開き、`$NX_ROOT\samples\pdmconf` フォルダに移動します。

5. 以下のコマンドを実行します。

```
pdm_perl pdm_edit.pl
```

メニューが表示されます。

6. サポート オートメーション Tomcat サーバを編集するには、「M」を入力します。サポート オートメーション Tomcat サーバを追加するには、「A」を入力します。
ホスト名とサーバタイプの入力を要求するメッセージが表示されます。
7. セカンダリ ホスト名およびサーバタイプを入力します。
セカンダリ ホスト名が保存され、テンプレートのリストが表示されます。
8. `pdm_edit.pl` ユーティリティの指示に従います。
セカンダリ サポート オートメーション Tomcat の設定が完了します。

バックグラウンド サーバ上での サポート オートメーション の設定

高可用性設定を選択している場合は、バックグラウンドサーバ上でサポート オートメーションを設定できます。高可用性設定では、バックグラウンドサーバ上でメインサーバを設定します。

次の手順に従ってください:

1. 環境設定ウィザードでサポート オートメーションを選択します。
2. [構成の選択] ページで、[サーバ設定] ドロップダウンから [高可用性] を選択します。詳細については、オンライン ヘルプを参照してください。
3. [一般設定] ページで、[設定タイプ] ドロップダウンから [バックグラウンドサーバ] / [スタンバイサーバ] を選択します。
4. [サポート オートメーション] ページで、[メインサーバ] オプションを選択します。
5. [ソケット設定] と [Tomcat 設定] の詳細を入力します。
6. 指示に従ってウィザードを完了します。
バックグラウンドサーバ上でサポート オートメーション が設定されます。

アプリケーション サーバ上での サポート オートメーション の設定

高可用性設定を選択している場合は、アプリケーションサーバ上でサポート オートメーションを設定できます。ソケットプロキシまたはメッセージルーティングサーバは、アプリケーションサーバ上での有効なサポート オートメーションサーバモードです。

次の手順に従ってください:

1. 環境設定ウィザードで サポート オートメーション を選択します。
2. [構成の選択] ページで、[サーバ設定] ドロップダウンから [高可用性] を選択します。詳細については、オンライン ヘルプを参照してください。
3. [一般設定] ページで、[設定タイプ] ドロップダウンから [アプリケーション サーバ] を選択します。
4. [サポート オートメーション] ページで、[メッセージルーティングサーバ] または [ソケット プロキシサーバ] オプションを選択します。
5. [ソケット設定] と [Tomcat 設定] の詳細を入力します。
6. 指示に従ってウィザードを完了します。

アプリケーション サーバ上で サポート オートメーション が設定されます。

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。

Web Screen Painter をインストールする方法

スキーマや Web インターフェースをカスタマイズするための Web Screen Painter をインストールします。

次の手順に従ってください:

1. CA SDM の設定に応じて、Web Screen Painter をインストールする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、あるいは任意のリモート コンピュータ
- 高可用性: バックグラウンド サーバ

重要: WSP は、バックグラウンドサーバ上でのみ実行できます。WSP インストーラでは、その他の任意のサーバ上でのインストールは停止されませんが、スタンドアロンまたはスタンバイ サーバやアプリケーションサーバ上では実行できません。たとえば、バックグラウンドサーバ以外のサーバに WSP をインストールしたとします。[スタート] メニューに WSP のショートカットが表示されます。このショートカットをクリックすると、エラーメッセージが表示されます。

2. ドライブにインストール メディアを挿入します。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、CA SDM をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

3. リストから言語を選択し、[言語の選択] をクリックします。

インストール メニューが表示されます。

注: インストール メニューが自動的に表示されない場合は、インストールメディアのルートにある `setup.exe` ファイルをダブルクリックしてインストールを開始します。

4. [製品のインストール] タブをクリックします。

5. [Web Screen Painter] をクリックします。
6. 言語を選択して、[OK] をクリックします。
7. 引き続き画面の指示に従って、Web Screen Painter のインストールを完了します。

Web Screen Painter がインストールされました。

CA SDM と CA NSM の統合をインストールおよび設定する方法

CA NSM インテグレーションによって、以下のことを実行できます。

- CA NSM のイベント管理システムとアラート管理システムによって検出されたネットワーク管理の問題を自動制御する。
- CA NSM とインシデント管理によって検出されたクリティカルなイベントを自動調整する。
- ネットワーク管理者および Service Desk スタッフからの影響度を測定する。
- 大量のリクエストやインシデントを回避する。
- リクエストやインシデントを自動的に更新する。
- ネットワークおよびサービス サポート管理のベスト プラクティスとして、ビジネスルールを実装する。
- 新規のリクエストやインシデントの発生を自動ディスパッチする。
- CA SDM とのやり取りを自動化して、一部の手作業をなくすことにより、カスタマ サポート スタッフの作業を削減する。
- 組織で問題が発生するとただちにリクエストやインシデントが自動的に作成されるため、問題発生時にユーザがオープンするリクエストやインシデントの数が低減する。

以下の図は、CA SDM と CA NSM の統合をインストールおよび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. [統合に関する考慮事項を確認します](#) (P. 210)。
2. [CA NSM 統合コンポーネントをインストールします](#) (P. 211)。
3. [CA SDM Event Converter を実行します](#) (P. 214)。
4. [統合後の考慮事項を確認します](#) (P. 215)。
5. 必要に応じて、[CA NSM 統合のトラブルシューティングを行います](#) (P. 216)。
6. [CA NSM 統合を使用します](#) (P. 253)。

関連項目：

[所有アセットの作成](#) (P. 216)

[イベント コンソール メッセージの監視](#) (P. 218)

[フィルタ ルールに関する考慮事項](#) (P. 219)

[CA NSM 統合のトラブルシューティング](#) (P. 246)

統合に関する考慮事項の確認

統合を開始する前に、以下の考慮事項を確認します。

- WSDL の修正プログラムを使用して CA SDM および CA NSM r11.2 SP2 cum1 をインストールおよび設定していることを確認します。
- CA SDM と CA NSM を統合するときにデフォルト設定を変更すると、予期しない結果が発生する場合があります。統合中に多数の CA SDM リクエストが一度に作成されないようにするには、\$NX_ROOT (UNIX) または installation-directory (Windows) にある NX.env ファイル内の以下のパラメータが NO に設定されていることを確認します。

```
@NX_TNG_OBJECT_UPDATED_SUBSCRIBE=NO  
@NX_TNG_OBJECT_ADDED_SUBSCRIBE=NO  
@NX_TNG_OBJECT_DELETED_SUBSCRIBE=NO  
@NX_TNG_OBJECT_STATUS_UPDATED_SUBSCRIBE=NO
```

- CA SDM の設定に応じて、以下のサーバ上で CA NSM 統合をインストールできます。
 - 標準：プライマリまたはセカンダリ、あるいはその他の任意のスタンドアロンサーバ。
 - 高可用性：いずれかのアプリケーション サーバまたはその他の任意のスタンドアロンサーバ。

重要：スタンドアロンサーバに CA NSM 統合をインストールするには、そのスタンドアロンサーバに [CA NSM 統合コンポーネントをインストール](#) (P. 211) します。高可用性設定では、このコンポーネントがいずれかのアプリケーション サーバを指すようにします。

- CA SDM と CA NSM を同じコンピュータにインストールする場合は、CA NSM 統合をインストールする必要はありません。この統合は自動的に有効になります。
- (Windows) CA SDM と CA NSM を別のコンピュータにインストールする場合は、CA SDM の設定に応じて、以下のいずれかのアクションを完了します。
 - 標準：CA NSM サーバにセカンダリ サーバをインストールおよび設定するか、または CA NSM サーバに [CA NSM 統合コンポーネントをインストール](#) (P. 211)します。
 - 高可用性：CA NSM サーバにいずれかのアプリケーション サーバをインストールおよび設定するか、または CA NSM サーバに [CA NSM 統合コンポーネントをインストール](#) (P. 211)して、いずれかのアプリケーション サーバを指すようにします。
- (UNIX) CA SDM と CA NSM を別のコンピュータにインストールする場合は、CA SDM の設定に応じて、以下のいずれかのアクションを完了します。
 - 標準：CA NSM サーバにセカンダリ サーバをインストールします。
 - 高可用性：CA NSM サーバにアプリケーション サーバをインストールします。

CA NSM 統合コンポーネントのインストール

CA SDM と CA NSM が同じコンピュータにインストールされていない場合や、スタンドアロン サーバに CA NSM 統合をインストールする場合は、CA NSM 統合コンポーネント（または Event Converter）をインストールする必要があります。このコンポーネントは、Windows コンピュータ上でのみ実行されます。

次の手順に従ってください：

1. CA NSM サーバまたはスタンドアロン サーバにログインします。
2. ドライブにインストール メディアを挿入します。

重要：インストールメディアに使用できる適切なドライブがコンピュータにない場合は、CA SDM をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

3. リストから言語を選択し、[言語の選択] をクリックします。

インストール メニューが開きます。

注: インストール メニューが自動的に表示されない場合は、インストール メディアのルートにある **setup.exe** ファイルをダブルクリックしてインストールを開始します。

4. [製品のインストール] タブをクリックします。
5. [CA NSM Integration] をクリックします。
6. 画面の指示に従い、入力を求められたら以下の情報を入力します。

- Slump ホスト名
- Slump ホスト IP アドレス
- Slump ポート ID
- NSM リポジトリ

インストーラによって、**NX.env** ファイルと、**Event Converter** を開始および停止するための **Windows** サービスが作成されます。

7. 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: いずれかのアプリケーション サーバ。
8. 以下のディレクトリに移動し、**topology.cfg** ファイルを開きます。

`$NX_ROOT/site/eh`

9. このファイルに以下の情報が含まれていることを確認します。

```
# <remote_node>:uniconv uniconvert IP_ADDR_tngfilter:tngfilter uni
IP_ADDR_tngcnv:tngcnv tngcnv <IP_ADDR_tngfilter>:tngfilter tng
IP_ADDR_tngfilter:tngfilter filter_nxd <IP_ADDR_tngwriter>:tngwriter -
IP_ADDR_tngwriter:tngwriter ehwriter - -
```

IP_ADDR_tngcnv

CA NSM Event Converter プロセスを実行しているサーバの IP アドレスを指定します。

IP_ADDR_tngfilter

CA SDM を実行しているサーバの IP アドレスを指定します。

IP_ADDR_tngwriter

CA SDM を実行しているサーバの IP アドレスを指定します。

10. ファイルを保存します。
CA NSM 統合コンポーネントがインストールされます。
11. [\(UNIX のみ\) Event Converter を設定します](#) (P. 213)。
Event Converter が設定されます。

(UNIX のみ) Event Converter の設定

CA SDM と CA NSM を統合した後、コンバータも設定する必要があります。

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、[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。
3. Event Converter がインストールされている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。
4. [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。
5. [プロセスの追加] をクリックします。
[プロセスの新規作成] ウィンドウが開きます。
6. [プロセス] として [UNI コンバータ] を選択します。
7. Event Converter がインストールされているサーバの IP アドレスを入力します。
8. [保存] をクリックします。
9. CA SDM の設定に応じて、以下のサーバ上で pdm_configure を実行します。
 - 標準: プライマリ サーバ。
 - 高可用性: アプリケーション サーバ。
10. 新しい環境設定は、次回サーバを起動したときに有効になります。
重要: 再設定するときは、データベースを初期化しないでください。

11. 特権ユーザとして、CA NSM サーバで `pdm_proctor_init` を実行して、CA SDM Proctor を開始します。
12. 特権ユーザとして、CA SDM サービスを再起動し、CA SDM デーモンを開始します。デーモンのステータスを表示するには、`pdm_status` を実行します。

Event Converter が設定されます。

CA SDM Event Converter

この情報は、Windows 動作環境での CA NSM Integration にのみ適用されます。Windows サーバで CA SDM の環境設定を実行するときは、CA SDM Event Converter を以下の 2 つの異なる方法でインストールできます。

- Windows サービスとしてインストールする
- コンバータの起動と停止に使用できる CA SDM デーモン サーバの一部としてインストールする

CA SDM サーバのインストール上では CA SDM の設定に応じて、いずれかの方法を使用してコンバータを起動できますが、クライアント上では Windows サービスとしてしか起動できません。

注: CA SDM が何らかの理由でシャットダウンした場合、Event Converter の実行を継続して、NSM からのメッセージを引き続き受信することができます。CA SDM がダウンしている間に NSM から受信したすべてのメッセージは、CA SDM の再起動後にキューに追加されて処理されます。

Event Converter の削除 (Windows サービス)

デーモンマネージャを使用して Event Converter の起動と停止を行う場合は、以下のコマンドを使用して、Windows サービスから Event Converter を削除します。

```
tngcnv -u
```

以下のコマンドを使用して、Event Converter を Windows サービスとして再インストールできます。

```
tngcnv -i
```

Event Converter の削除(デーモン マネージャ)

デーモン マネージャは、コンバータの起動と停止を行うだけではなく、誤って停止したコンバータの再起動も行います。 *pdm_status* を使用すると、コンバータが稼働しているかどうかを確認したり、コンバータがローカルとリモート（セカンダリ）サーバのどちらで稼働しているかを特定できます。

Windows のサービス マネージャを使用して Event Converter の起動と停止を行う場合は、デーモン マネージャの起動設定から Event Converter を削除します。

tngcnv の行を有効または無効にするには、CA SDM の設定に応じて以下のサーバにログインし、CA SDM の Web UI から [システム] - [環境設定] に移動します。

- 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。

重要：この変更は CA SDM 環境設定を再実行すると元に戻ります。環境設定の実行後もこの変更を維持する場合は、*pdm_startup.tpl* を変更します。

統合後の考慮事項の確認

統合プロセスの実行中に選択する場合は、以下の情報を検討してください。

- CA NSM イベントの受信プロセスと CA SDM でのリクエストの作成プロセスを実行する前に、すべてのコンポーネントをインストールして設定し、それらがアクティブな状態であることを確認する必要があります。
- イベントが失われるのは、Event Converter サービスが停止した場合のみです。CA SDM システムがダウンした場合、つまり Microsoft Windows の [サービス] パネルでシステムを停止するのではなく一時停止した場合、Event Converter サービスが CA NSM イベントをキューに投入します。CA SDM を再起動すると、キューに投入されたイベントが処理されます。

- CA NSM Event Converter サービスでは、NX_TNGCNV_QUEUE_SIZE 環境変数で指定された最大数までイベントをキューに投入します。
- CA SDM との統合後に CA NSM リポジトリをリビルドすると、CA SDM メニューのエントリが失われます。メニューのエントリを復元するには、CA NSM Windows コンピュータで統合を再実行する必要があります。これを行うには、*installation-directory*\bin にある integAHD.exe を実行します。
- CA NSM イベントの生成中に CA NSM Event Converter を起動すると、Event Converter を完全に初期化する前に発生したイベントが失われます。

CA NSM 統合の確認

CA NSM 統合を確認するには、以下のアクションを完了します。

- [所有アセットの作成](#) (P. 216)
- [イベント コンソール メッセージの監視](#) (P. 218)
- [フィルタ ルールに関する考慮事項](#) (P. 219)

所有アセットの作成

多くの CA Technologies 製品では、アセットを CA MDB に作成しますが、アセットは自動的に CA SDM で使用できるようにはなりません。通常、CA SDM の組織では、正式なプロセスで取得された、組織所有のアセットのみを追跡します。ほかの CA Technologies 製品によってネットワーク上で検出された一部のデバイスを自動的に CA SDM で使用できるようにすることはできません。たとえば、会社を訪問したコンサルタントのラップトップ コンピュータは、CA SDM の組織には関係ありません。

CA MDB 内で検出されたアセットを CA SDM で使用できるようにするには、アナリスト用 Web インターフェースの [アセットの検索] フォームまたは [アセットの新規作成] フォームで検出されたアセットの選択ダイアログ ボックスを使用します。

注: 検出されたアセットの選択ダイアログ ボックスは、Web クライアントで使用できます。

WorldView インテグレーションを使用している場合は、`pdm_nsmimp` コマンドラインユーティリティを実行することで、検出されたアセットを CA SDM で使用できるように設定できます。CA NSM 2D/3D マップと Unicenter Explorer では、リクエストのアクセスおよび作成が可能です。管理対象オブジェクトを右クリックすると、[リクエストの作成] と [リクエスト リスト] という 2 つのメニュー オプションが表示されます。これらのメニュー オプションは、CA SDM と統合される際、CA NSM に追加されます。

検出されたアセットの登録方法

`pdm_discimp` ユーティリティは、CA SDM 以外によって検出されたアセットのバッチ登録に使用します。このユーティリティを使用して、ほかのソフトウェア製品で登録されたアセットの CA 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。このユーティリティは、インタラクティブなバッチプロセスです。

このロジックは、[アセットの検索] および [アセット リスト] Web フォームから起動可能な [検出されたアセット] ダイアログ ボックスのロジックに似ています。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ています。

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。

CA MDB の構造と CA SDM アーキテクチャの理由から、処理するレコードを選択するために以下のクエリが実行されます。

1. クエリによって、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。
2. 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ときに、1 つ目のクエリからのアセットが登録用に選択されます。

注: このプロセスはパフォーマンスに影響を与える場合があります。

イベント コンソール メッセージの監視

CA SDM の基本的なインストール環境では、監視対象オブジェクトのステータスの変化と管理オブジェクトの新規追加が自動的に監視されます。AHD.DLLを使用してWindowsのコンソールメッセージを監視して、CA SDM サーバにイベントメッセージを送信するように環境を設定できます。

CA SDM にイベントを送信する際には、AHD.DLLを使用することをお勧めします。ただし、イベント コンソールをUNIXシステムで実行している場合は、その他のメソッドも使用できます。

CA NSM のイベント管理では、応答するイベントを特定し、自動的に開始するアクションを1つ以上指定できます。メッセージおよび関連付けられたアクションを定義すると、イベントが発生するたびにアクションが自動的に実行されます。

CA SDM との統合後にイベントメッセージが発生した場合は、CA SDM に汎用イベントデータを送信して、以下の操作を実行できます。

- リクエストを作成するか、既存のリクエストを更新する
- アナウンスメントを作成して CA SDM スコアボードに登録する

注: リクエストおよびアナウンスメント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。

統合を開始するには、以下の手順に従います。

1. AHD.DLL を使用して、CA NSM msg_action レコードを作成します。
2. cawto コマンドを使用して、そのメッセージレコードをイベント コンソールに渡します。

注: システムの統合が完了したことを確認できるまでは、CA SDM に含まれているデフォルトのフィルタとライターールを使用してください。CA NSM イベントによってリクエストが作成されたことを確認できるまでは、デフォルトのルールを変更または削除しないでください。CA NSM メッセージ用の文字列を作成する場合は、スペース、コロン、コロン、スペースの組み合わせ (::) は使用しないでください。使用した場合、メッセージが使用されるときに解析エラーが発生する場合があります。

汎用イベント データの送信 (UNIX の場合のみ)

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リングするためには、CA NSM Event Management のメッセージアクションで `unicnv` デーモンを使用します。

Windows で `AHD.DLL` を使用するのと同じ方法で汎用イベント データを使用して、リクエストを自動的に生成できます。このメソッドは UNIX で推奨されるメソッドです。

アナウンスメントの自動登録

CA SDM を CA NSM と統合すると、CA NSM でアナウンスメントを作成して CA SDM スコアボードに登録できます。

フィルタ ルールに関する考慮事項

インテグレーションを正しく設定した後に、定義に従ってイベントによってリクエストが作成または更新されている場合は、フィルタ ルールを変更して不要なイベントをフィルタできます。

フィルタ ルールを記述する場合のヒントをいくつか以下に示します。

- フィルタ ルールを変更する場合は、必ず **CA SDM** を再起動します。
- フィルタ ルールをテストする場合は、デフォルトのライター ルールを使用します。
- フィルタ ルールに `node_ID`、`user_ID`、または `event_ID` パラメータを記述する際は、受信イベントの大文字小文字を区別します。大文字小文字を区別して正確に指定するには、テストするパラメータに **CA NSM** のイベントを作成します。この処理によって、必要な情報を指定されたリクエストが作成されます。リクエストの大文字小文字はフィルタ ルールの大文字小文字と一致させます。このルールは、受信コンソール メッセージの大文字と小文字にも適用されます。
- **CA NSM** メッセージ用の文字列を作成する場合は、スペース、コロン、コロン、スペースの組み合わせ (`::`) は使用しないでください。使用した場合、メッセージが使用されるときに解析エラーが発生する場合があります。

- 特定のイベントのフィルタ ルールをコーディングする場合、イベントの受信テキストは、「Object_Status_Updated minor」のようなフォーマットになります。以下のテキストを探すフィルタ ルールをコーディングします。

```
tng:::*:*:*:*:Object_Status_Updated.*minor.*:::(0,1)
```

- イベント記述の空白文字は、実際には印刷不能な文字列である可能性があります。空白文字の代わりに、ピリオドとアスタリスク（*）の付いた 1 文字以上の文字列を含めるようにフィルタを記述します。また、イベント テキストの末尾に出現する可能性のある印刷不能な文字列については、イベント テキストの末尾にピリオドおよびアスタリスク（*）を付けます。
- フィルタで複数のパラメータ（*node_ID*、*user_ID*、*event_ID* など）を組み合わせる場合は、最初にパラメータを 1 つだけ記述して、そのフィルタの動作を確認します。その後、次のパラメータを追加して、最初のパラメータと合わせて動作することを確認するというように、順次パラメータを追加していきます。
- デバッグが簡単にできるように、最も具体的なフィルタ ルールを先頭に置き、最も一般的なルールを最後に置くようにします。

イベント ライタ ルールは、フィルタ ルールの場合と同じデバッグ手順セットに従います。CR_CREATE アクションを使用していて、テンプレートを含めた場合は、該当のテンプレートが存在することを確認します。

イベントを自動的にフィルタする方法

ネットワーク デバイスおよびその他のイベント ソースによって生成されたエラーおよびイベント メッセージに対処するリクエストが自動的に作成されるように CA SDM を設定できます。イベントのフィルタ方法を定義することで、イベントの発生を自動的に検出して、イベントの処理に指定したアクションを開始できます。この方法により、運用効率全体が向上して、エラーの発生を削減できます。

CA SDM を設定して、以下の操作を実行できます。

- ホスト、コンテンツ、タイプ、および CA NSM のその他の情報に基づいてイベントをフィルタする
- ネットワーク デバイスによって生成されたエラーおよびイベント メッセージに対処するリクエストを自動的に作成する
- イベントに対する応答としてコマンドを自動的に実行する

イベントを自動的にフィルタするには、以下の手順に従います。

- 特別な処理が必要なイベントを指定するフィルタ ルールを定義する
- イベントの発生時に自動的に実行されるアクションを指定するイベント ライタ ルールを定義する

フィルタ ルールおよびイベント ライタ ルールでは、データの送受信に汎用イベント データ構造を使用します。これらのルールの定義にはテキスト エディタを使用しますが、格納および編集は **CA SDM** サーバでのみ行います。

すべてのイベントがフィルタ ルールおよびイベント ライタ ルールによる処理の対象になります。フィルタ ルールおよびイベント ライタ ルールで処理するイベントの例を以下に示します。

- ハードウェア障害
- スケジュールされたバッチ プロセスの障害
- CPU の過剰使用
- ページング レートの増加
- 異常なファイルアクティビティ
- 異常なセキュリティ状態

複数の異なるコンピュータに設定できるフィルタ デーモン、イベント ライタ デーモン、およびイベント ソースの数には制限がありません。これらのエレメントのロケーションおよび関連付けは、**CA SDM** サーバのトポロジ ファイルに格納されます。

注: **CA NSM** とインテグレートすると、**uniconv** デーモンを使用してリクエストを自動的に生成できます(これは **UNIX** で推奨されるメソッドです)。**uniconv** は **CA NSM** イベント管理のメッセージ アクションに使用されます。

汎用イベント データ

イベントに関する情報は、*汎用イベントデータ*構造を使用してやり取りします。汎用イベント データ構造は、以下のデータ エLEMENTで構成されます。

ソース タイプ

残りのイベントのフォーマットを示します。

ノード ID

デバイスの名前または ID を示します。

ユーザ ID

ユーザ名または ID（該当する場合）を示します。

メジャー ソース

ソース アプリケーション ID を示します。

マイナー ソース

イベントのエージェントまたは詳細な説明を示します。

日付/時間

イベントの日付と時刻を示します。

イベント ID

イベントをトリガしたソース イベント文字列を示します。

イベント データ

関連付けられているイベント データを示します。

Severity

イベントの重要度を示します。

ハンドル

ルールに起因した、デーモンによって指定される文字列を示します。

ハンドル ソース

ハンドルを割り当てたデーモンの ID を示します。

ハンドル ステータス

create、update、または terminate のステータスを示します。

件数

更新件数を示します。

フィルタ ルールのセットアップ

フィルタは、イベント ソースから情報を受け取ります。受け取った情報はイベント ライタに渡すことができます。ネットワーク デバイスによって多数のイベント メッセージが生成されるため、フィルタ ルールを使用して、リクエストの作成に使用可能なイベント メッセージを分離することができます。フィルタ ルールを使用すると、以下の操作を実行できます。

- 報告するネットワーク イベントまたはトラップを特定し、それらのレポート方法を指定する。
- 各タイプのイベントまたはトラップを報告するときに実行する処理を制御する。有効なアクションには、無視、レポート作成、マーク付けがあります。

CA NSM とインテグレートした場合は、フィルタを実行することで、CA NSM によって管理される、SNA および TCP/IP ネットワークなど、すべてのシステムからのイベントを管理できます。

イベントをフィルタすると、特定のノード、ユーザ、またはワークステーションに関する特定の情報を取得して、イベント ライタに渡すことができます。イベント フィルタ ルールを定義して特定のニーズに合わせて選別することができるので、疑わしいイベントを特定して、問題が発生する前に修正できます。

注: UNIX の正規表現を熟知していると、フィルタ ルールを記述する際に役立ちます。UNIX の正規表現は Windows でも使用できます。

フィルタ ルールの定義

フィルタ ルールでは、UNIX の正規表現によるマッチングを使用して、イベントのフィルタ ルールが一致するかどうかを判断し、フィルタ の指定されていないイベントをブロックします。特殊フィルタ (ID=5) は、未編集の受信汎用イベントを作成者に渡します。フィルタ を実行すると、フィルタされたイベントのみが渡され、*filter* のハンドル ソースおよび *create*、*update*、または *terminate* のハンドル ステータスが割り当てられます。

CA SDM では、汎用イベントデータ構造のメジャー ソース、イベント ID、ノード ID、およびユーザ ID の各フィールドを使用して、一致するフィルタ ルールを検索します。

重要: フィルタ ルールによって、イベントからイベント ライタ ルールを使用する別のデーモンに情報が渡され、さらにリクエストを自動的に作成できます。

フィルタ ルール ファイルの初期設定 `tngfilter_rule.dat` は、CA SDM サーバの `$NX_ROOT/site/eh/IP` (UNIX) または `installation-directory¥site¥eh¥IP` (Windows) に格納されています。`$NX_ROOT` または `installation-directory` は CA SDM がインストールされているディレクトリを表し、`IP` はフィルタ が保存されているコンピュータの IP アドレスを表します。このコンピュータは、通常、CA SDM サーバを表します。

このファイルには、各種のフィルタ ルールのセットアップ方法を記述した多くのコメント行も含まれています。コメント行はポンド記号 (#) で始まります。

フィルタ ルール ファイルを表示、更新、および保存するには、テキスト エディタを使用します。ただし、ファイルに余分なフォーマット文字を残すエディタは使用しないでください。Windows ユーザの場合は WordPad を、UNIX ユーザの場合は vi を使用することをお勧めします。

構文(フィルタ ルール)

フィルタ ルールの構文は以下のとおりです。

```
source_type:::node_ID:::user_ID:::event_ID:::filter
```

各項目は以下のとおりです。

ルール内の各フィールドは、**3 つのコロン (:::)** で区切ります。アスタリスク (*) をワイルドカード文字として使用できます。アスタリスクを使用した場合は、受信イベントがフィルタ ルールのパターンに一致するかどうかを判断するときに、パラメータの値を無視します。

注: フィルタ ルールの最初の **4 つ** のパラメータは、受信イベントとの比較パターンを記述します。このパターンを使用して、ルールの最後のパラメータで指定したフィルタで受信イベントを処理するかどうかを決定します。

パラメータ(フィルタ ルール)

source_type

フィルタにイベントを転送するソースのタイプを指定します。受信イベントのメジャー ソース フィールドは、このパラメータの値と比較されます。一般に、フィルタにイベントを送信するコンバータのタイプによって、このパラメータの値が決まります。有効な値は以下のとおりです。

uni

UNIX CA NSM コンバータを示します。

tng

Windows CA NSM コンバータを示します。

ソース タイプとイベント ID が比較されたときに、受信イベントがいくつかのルールに一致すると、ノード ID が比較されます。

node_ID

イベントの送信元であるノードの ID を指定します。このパラメータは受信イベントのノード ID と完全に一致している必要があります。一致していない場合、このフィルタルールは使用されません。アスタリスク (*) を使用すると、受信イベントがフィルタルールのパターンに一致するかどうかを判断するときに、ノード ID を無視します。

受信イベントのノード ID に一致するルールは、**node ID** にアスタリスク (*) が指定されているルールよりも優先されます。

ソースタイプ、イベント ID、およびノード ID が比較されたときに、受信イベントがいくつかのルールに一致すると、ユーザ ID が比較されます。

user_ID

イベントに関連付けられているユーザを示します。このパラメータを使用して、特定のユーザからのイベントに対して特定のアクションを実行します。特定のユーザが関連付けられていないイベントも多数あります。このパラメータに UNIX の正規表現を含めることはできません。正確なユーザ ID またはアスタリスクを指定する必要があります。アスタリスク (*) は初期設定されており、ルールを選択するときにユーザを無視することを示します。

イベントに関連付けられているユーザ ID に一致するルールは、**user ID** にアスタリスク (*) が指定されているルールよりも優先されます。

event_ID

イベント ID を指定します。UNIX の正規表現を使用できます。ピリオドおよびアスタリスク (*) は任意のイベント名に一致します。たとえば、**[Aa].*** と指定すると、大文字の A または小文字の a で始まるイベントと一致させることができます。

event_ID パラメータが（正規表現ではなく）テキストの場合は、汎用イベントのイベント ID と完全に一致している必要があります。部分一致は対象になりません。**event_ID** パラメータが正規表現の場合は、正規表現マッチの長さを使用して、イベントフィルタルールの **event_ID** と汎用イベントのイベント ID の一致の度合いを判断します。

ソースタイプとイベント ID が比較されたときに、受信イベントがいくつかのルールに一致すると、ノード ID が比較されます。

filter

受信イベントの処理に使用するフィルタとフィルタが使用するパラメータを指定します。フォーマットは以下のとおりです。

(*filter_id*, *filter_parameter1*, *filter_parameter2*, ...)

filter_id の有効な値は以下のとおりです。

値=0

すべてのイベントを報告します。

値=2

発生頻度の低いイベントを無視します。

値=3

filter_parameter1 で指定された長さより短い障害を無視します。

値=4

filter_parameter1 で指定された長さより短いバーストを無視します。

値=5

すべてのイベントを変更せずに宛先に渡します。

filter のパラメータ数は *filter_id* ごとに異なります。以下の表を参照してください。

filter_ID	filter_parameter1	filter_parameter2	filter_parameter3
0	0=いいえ、1=はい イベントを常に個別の問題として報告するかどうかを示します。	なし	なし
2	発生回数 イベントが重要であると認識されるまでの一定時間内にイベントが発生する回数を指定します。	間隔 イベントが発生してから重要であると認識されるまでの経過時間を秒数で指定します。	0=いいえ、1=はい イベントを常に個別の問題として報告するかどうかを示します。
3	間隔 イベントが発生してから重要であると認識されるまでの経過時間を秒数で指定します。	0=いいえ、1=はい イベントを常に個別の問題として報告するかどうかを示します。	なし

filter_ID	filter_parameter1	filter_parameter2	filter_parameter3
4	間隔 イベントが発生してから 重要であると認識される までの経過時間を秒数で 指定します。	0=いいえ、1=はい イベントを常に個別の問 題として報告するかどうかを示します。	なし
5	なし	なし	なし

注: フィルタ ルールの最初の 4 つのパラメータは、受信イベントとの比較パターンを記述します。このパターンを使用して、ルールの最後のパラメータで指定したフィルタで受信イベントを処理するかどうかを決定します。

イベント ライタ

イベント ライタは、重要なイベントがネットワークで検出されたときに CA SDM で実行する処理を指定します。 イベント ライタでは、イベント ソースから変換されたイベント（汎用イベント データ構造を使用するイベント） およびフィルタを介して渡されたイベントを使用して、リクエストを作成します。

イベント ライタを使用すると、以下のことが可能になります。

- イベント ソースから受信したイベントのタイプを識別する。
- イベント ライタがこのタイプのイベントを受信したときに実行するアクションを指定する。有効なアクションには、以下のものがあります。
 - リクエストの作成
 - 既存のリクエストの更新
 - コマンドの実行
- ログを記録するかどうかを指定する。

イベント ライタ ルールの定義

CA SDM をインストールすると、CA SDM サーバで実行される初期設定が指定されます。この初期設定では、単一のイベント ソース、フィルタ、およびライタをセットアップし、すべてのイベントをライタに渡すフィルタルールが設定されます。ライタ ルールの初期設定によって、受信するすべてのイベントのリクエストが作成されます。

ライタ ルール ファイルの初期設定 `tngwriter_rule.dat` は、CA SDM サーバの `$NX_ROOT/site/eh/IP` (UNIX) または `installation-directory¥site¥eh¥IP` (Windows) に格納されています。`$NX_ROOT` または `installation-directory` は CA SDM がインストールされているディレクトリを表し、`IP` は CA SDM サーバの IP アドレスを表します。

このファイルの内容を表示して、ライタ ルール定義の初期設定およびライタ ルールのフォーマットを記述したコメントを確認できます。コメントはファイルの先頭にあり、ライタ ルールはファイルの最後にあります。コメント行はポンド記号 (#) で始まります。

ライタ ルール ファイルを表示、更新、および保存するには、テキストエディタを使用します。ただし、ファイルに余分なフォーマット文字を残すエディタは使用しないでください。Windows ユーザの場合は WordPad を、UNIX ユーザの場合は vi を使用することをお勧めします。

構文(イベント ライタ ルール)

イベント ライタ ルールの構文は以下のとおりです。

```
event_ID:::device:::user_ID:::majorSrc:::minorSrc:::action:::template:::  
command:::logging:::event_token:::user_parms
```

各項目は以下のとおりです。

ルール内の各フィールドは、3 つのコロン (:::) で区切ります。アスタリスク (*) をワイルドカード文字として使用できます。アスタリスクを使用した場合は、イベント ライタ ルールが一致するかどうかを判断するときに、パラメータの値が無視されます。

パラメータ(イベントライタールール)

event_ID

イベントライタールールを適用するイベントの ID を指定します。UNIX の正規表現を使用できます。ピリオドおよびアスタリスク (*) は任意のイベント名に一致します。たとえば、[Aa].*と指定すると、大文字の A または小文字の a で始まるイベントと一致させることができます。

event_ID パラメータが（正規表現ではなく）テキストの場合は、汎用イベントのイベント ID と完全に一致する必要があります。部分一致は対象になりません。*event_ID* パラメータが正規表現の場合は、正規表現マッチの長さを使用して、イベントライタールールの *event_ID* と汎用イベントのイベント ID の一致の度合いを判断します。

device

オブジェクトの名前を指定します。通常はイベントに関連付けられているデバイスまたはホストです。ピリオドおよびアスタリスク (*) は初期設定されており、ルールを選択するときにソース オブジェクトを無視することを示します。

ソース タイプとイベント ID が評価されたときに、受信イベントがいくつかのルールに一致すると、デバイスが比較されます。受信イベントのデバイスに一致するルールは、*device* にアスタリスク (*) が指定されているルールよりも優先されます。

デバイス名の割り当てにルールを定義した場合は、このパラメータが役に立つことがあります。たとえば、米国に設置されているデバイスに **USxx** という名前を付けている場合は、このパラメータに **US.***と指定して、米国にあるデバイスからのイベントに対して特定のライターアクションを実行できます。

user_ID

イベントに関連付けられているユーザを示します。このパラメータを使用して、特定のユーザからのイベントに対して特定のアクションを実行します。特定のユーザが関連付けられていないイベントも多数あります。このパラメータに UNIX の正規表現を含めることはできません。正確なユーザ ID またはアスタリスクを指定する必要があります。アスタリスク (*) は初期設定されており、ルールを選択するときにユーザを無視することを示します。

ソース タイプ、イベント ID、およびデバイスが評価されたときに、受信イベントがいくつかのルールに一致すると、ユーザ ID が比較されます。 イベントに関連付けられているユーザ ID に一致するルールは、*user_ID* にアスタリスク (*) が指定されているルールよりも優先されます。

majorSrc

イベント ライタにイベントを転送するメジャー タイプのソースを自動的に表示します。 このパラメータは必須です。 パラメータの値は、イベント ソースによって決まります。 Windows の CA NSM からのイベントの場合、値は「tng」です。 UNIX の CA NSM からのイベントの場合、値は「uni」です。

minorSrc

イベント ライタにイベントを転送するマイナー タイプのソースを自動的に表示します。 CA NSM からのイベントの場合、このパラメータにはイベントタイプを含めます。すべてのイベントを受け入れる場合は、アスタリスク (*) を使用します。

action

イベント ライタがこのタイプのイベントを受信したときに実行するアクションを指定します。以下のいずれかの値を使用します。

CR_CREATE

イベントごとに新規リクエストを書き込みます。

CR_UPDATE

既存のリクエストが存在する場合は 1 つ以上のリクエストを更新します。リクエストが見つからない場合はリクエストを作成します。初期設定では、レコードは *log_agent* 属性および *affected_resource* 属性の一致によって検索されます。リクエストの属性のリストを指定すると、初期設定を無効化できます。

CR_UPDATE_ONLY

CR_UPDATE と同様ですが、一致するリクエストが見つからない場合、リクエストは作成されません。

COMMAND

command パラメータで指定されたコマンドを実行します。

注: CA SDM でリクエストまたは変更要求にアクセスできない場合は、一定の時間が経過すると更新を再試行します。

テンプレート

リクエストの作成に使用するリクエストテンプレートの名前を指定します。**action** が **CR_CREATE** 以外の場合は、このパラメータを指定する必要はなく、指定しても無視されます。

注: ルールを定義する前に、リクエスト テンプレートを作成しておく必要があります。

コマンド

action パラメータの値が **COMMAND** の場合に実行するコマンドを指定します。以下に示す代替引数をコマンドに組み込むことができます。これらの引数は、コマンドを実行すると実際の値に置き換わります。

&Node

デバイス名またはノード ID

&User

ユーザ名またはユーザ ID

&Date

イベント日付

&Time

イベント時刻

&Event-id

イベントをトリガしたソース イベント文字列

&Data

関連付けられているイベント データ

&Sev

イベントの重要度

&Major-src

ソース アプリケーション ID

&Minor-src

イベントのエージェント名または詳細な説明

&Handle

ルールに起因した、デーモンによって指定される文字列

&Src-handle

ハンドルを割り当てたデーモンの ID

&Status-handle

ハンドル ステータス (有効な値は **create**、**update**、または **terminate**)

ログ記録

ログを記録するかどうかを指定します。以下のいずれかの値を使用します。

NONE

標準のエラー ログ以外のログ記録を実行しません。 **NONE** は初期設定値です。

PDM

CA SDM ログ (**stdlog.0**) に内部の汎用イベントフォーマットでログを記録します。

SYS

UNIX **syslog** にログを記録します。このログは **Unicenter** コンソールに転送できます。イベントにメッセージ ID (**CAPD 13**) を割り当てることで、イベントを **Unicenter** コンソールで処理できます。

BOTH

CA SDM ログ (**stdlog.0**) と UNIX **syslog** の両方にログを記録します。

event_token

event_id (tng イベント メッセージ) または **event_id** に相当するすべてのメッセージ (ワイルドカードが指定された **event_id** など) に関連付けられている特定のリクエストを識別する 30 文字のユーザ定義タグです。 **event_token** はリクエストの属性で、CA NSM インターフェースによって生成された各リクエストに格納されます。ライタルールで **event_token** を指定しないと、文字列「tng_generated」が使用されます。この場合、ユーザは **event_token** 属性に一致するすべてのリクエストを更新できます。たとえば、同じアセットに関する 2 つの異なるメッセージによって固有のリクエストを更新できます。

各 CR_UPDATE ライタ ルールでは、固有のメッセージ要素と固有の *event_token* を指定します。 *event_token* は、一致するリクエストの検索および更新に使用されます。 初期設定では、メッセージを含むアクティビティ ログが、一致するリクエストに追加されます。 別の例では、ユーザは、CR_CREATE ライタ ルールを使用してリクエストを作成したときに使用した CR_UPDATE ライタ ルールに同じ *event_token* を指定すると、既存のリクエストのステータス属性を更新できます (たとえば、STATUS=CL (クローズ) を設定します)。

たとえば、以下の最初のライタ ルールを使用すると、ライタ プロセス (tngwriter) で、文字列「Event1」で識別される NSM イベントを受信するたびに、*event_token* が「SystemCritical」であるコール リクエストを作成します。 2 番目のライタ ルールを使用すると、ライタ プロセスで、文字列「Event2」で識別される NSM イベントを受信するたびに、*event_token* が「SystemCritical」であるすべてのコール リクエストのステータス値を「CL」に更新します。

```
Event1:...*:::*::tng:...*:::CR_CREATE::::::::::NONE:::SystemCritical:::  
Event2:...*:::*::tng:...*:::CR_UPDATE::::::::::NONE:::SystemCritical:::%SEARCH  
=EVENT_TOKEN;%STATUS=CL
```

user_parms

以下のタイプの情報が含まれます。

リクエストの属性値

リクエストの属性値を指定するには、*%ATTRIBUTE=value* という構文を使用します。 *ATTRIBUTE* は text_api.cfg で識別される属性名で、CA SDM Majic コール リクエストの属性にマップされます。 このファイルは、NX_ROOT/site (UNIX) または *installation-directory¥site* (Windows) に格納されています。

注: キーワードと値のペアを複数使用する場合は、各ペアをセミコロン (;) で区切ります。

たとえば、以下の最初のライタ ルールを使用すると、ライタ プロセス (tngwriter) で、文字列「Event4」で識別される CA NSM イベントを受信するたびに、担当者が「mccda04」でありカスタマが「nsm」であるコール リクエストを作成します。

```
Event4:...*:::*::tng:...*:::CR_CREATE::::::::::NONE::::::::::%ASSIGNEE=mccda04  
;CUSTOMER=nsm
```

既存のリクエストレコードを更新するときに一致させるリクエストの属性のリスト

一致させる属性のリストの構文について説明します。

一致させる属性のリストの構文は、`%SEARCH=attribute1[, attribute2 ...]` と指定します。`SEARCH` は固定のキーワードで、`attribute1`、`attribute2` などは `text_api.cfg` で指定した `ATTRIBUTE` の名前を表します。

属性の検索リストの初期設定は、「`asset_name`」（`DEVICE` または `UUID`）および `LOG_AGENT` です。`SEARCH` キーワードを指定すると、（一致させる）属性が検索リストの初期設定に追加されます。`SEARCH_EXPLICIT` キーワードを指定すると、検索リストの初期設定が完全に無効化されます。コール リクエストの検索には、`SEARCH_EXPLICIT` キーワードに続く属性のリストのみが使用されます。

たとえば、以下のライタルールを使用すると、ライタ プロセス（`tngwriter`）で、文字列「`Event2`」で識別される `CA NSM` イベントを受信するたびに、担当者が「`mccda04`」であるすべてのコール リクエストのステータス値を「`CL`」に更新します。

```
Event2:...*:::*::tng:...*:::CR_UPDATE::::::::::NONE:::SystemCritical:::%SEARCH=ASSIGNEE;%STATUS=CL;%ASSIGNEE=mccda04
```

属性値のリストにある属性が `SEARCH` または `SEARCH_EXPLICIT` リストにある場合は、検索に使用されます。検索リストにない場合は、コール リクエストの属性値の設定または更新に使用されます。どちらの場合も、同じライタルールには使用できません。

注: `text_api.cfg` および `CA SDM` での使用方法の詳細については、「管理ガイド」を参照します。

CA NSM イベント構造の対応する値で置き換えられる特殊パラメータ名

以下の特殊パラメータ名は、`user_parms` 文字列で任意に使用できます。

&Message

`CA NSM` メッセージに関連付けられているメッセージテキストです。

&Parm

`CA NSM` メッセージアクション画面の `AHD.DLL Parm` フィールドです。

&Uuid

CA NSM 全体で固有の ID です。

&Device

CA NSM メッセージを生成したデバイス（ホスト名など）です。

&Majorsrc

イベント ライタにイベントを転送するメジャー タイプのソースです。Windows の CA NSM からのイベントの場合、値は「tng」です。UNIX の CA NSM からのイベントの場合、値は「uni」です。

&Minorsrc

イベント ライタにイベントを転送するマイナー タイプのソースです。

&Node

CA NSM メッセージを生成したデバイス（ホスト名など）です。

&Addr

CA NSM メッセージを生成したホストの IP アドレスです。

&Username

CA NSM メッセージを生成したホストのユーザ名です。

&Date

CA NSM メッセージが生成された 1970 年以降の期間を表す整数です。

&Time

CA NSM メッセージの日付と時刻です(例: Tue Jul 4 10:23:37 2000)。

&Severity

CA NSM メッセージの重大度です。

&Tag

CA NSM メッセージに関連付けられているタグ データです。

たとえば、以下のライターールを使用すると、ライタープロセス (tngwriter) で、文字列「Event2」で識別される NSM イベントを受信するたびに、カスタマがイベント メッセージのユーザ名の値 (&Username) と同じであるコール リクエストを作成します。

```
Event2:...*:*:*:*:tng:...*:*:*:CR_CREATE::::::NONE::::::%CUSTOMER=&Username
```

event_token および *user_parms* を使用することで、リクエストのすべての属性の初期値を設定したり属性値を更新したりでき、更新するレコードを検索するときに一致させるフィールドを指定できます。唯一の制限は、既存のコール リクエスト レコードでは説明属性は更新されないということです。レコードの更新および説明フィールドを指定すると、説明のテキストが含まれているアクティビティ ログが既存のレコードに追加されます。

CA NSM メッセージ アクション レコード: ahd.dll AHD_Call<parms>...

ライターールの *user_parms* パラメータで指定した &Parm パラメータを置き換えるために使用可能な CA NSM メッセージ アクション レコードの AHD_Call にデータ (<parms...>) を指定することもできます。AHD_Call で指定したデータをこの方法で処理するには、データ (<parms...>) の前に「%」文字を挿入し、&Parm という「特殊パラメータ」をライターールの *user_parms* フィールドの任意の場所に指定する必要があります。

以下に、CA NSM メッセージ アクションとライターールの例を示します。これらが連動して機能すると、ライタープロセスで、文字列「Event3」で識別される NSM イベントを受信するたびに、担当者が「mccda04」に設定されたリクエストを作成します。

```
Ahd.dll AHD_Call %ASSIGNEE=mccda04
```

```
Event3:...*:*:*:*:tng:...*:*:*:CR_CREATE::::::NONE::::::&Parm
```

AHD4.5 以前の CA SDM からアップグレードするカスタマは、<parms...> フィールドをすでに使用している場合があります。たとえば、このデータを使用してライタ ルールを適用できます。この操作は変更せずに続行できます。「old」と「new」の両方のパラメータを使用する場合は、「%」文字を挿入して「old」<parms..> データと「new」データを連結する必要があります。

例：

```
ahd.dll AHD_Call old data
```

```
ahd.dll AHD_Call %new user_parms
```

```
ahd.dll AHD_Call old data%new user_parms
```

最初の「%」文字の前にあるデータは、コール リクエストの説明フィールドに入力された **CA NSM** イベント メッセージに連結されます。これは、**CA SDM** で従来处理されていた方法です。最初の「%」文字の後にあるデータは、ライタ ルールの **user_parms** パラメータで指定された **&Parm** パラメータを置き換えるために使用されます。

CA SDM ログ (stdlog.0) の構文

stdlog.0 ファイルのエントリの構文は以下のとおりです。

```
genDate genTime genNode genProc PID level codefile linenum msgID
:::msgDomain¥msgNode::: ::: :::msgGenDomain¥msgGenUser:::domainID
:::msgDate msgTime:::eventID arg tag::: :::IPAddr:filter:filterNum
:::majorSrc::: :::msgSrc:::msgType:::msgSrcNum::: :::platform
```

各項目は以下のとおりです。

ルール内の各フィールドは、3 つのコロン (:::) で区切ります。

genDate

ログ インシデントが生成されたシステム日付の月と日を示します。

genTime

ログ インシデントが生成されたシステム日付の時刻を示します。

genNode

ログ インシデントを生成したノードの名前を示します。値は通常、生成したノードの DNS 名の先頭の 8 文字です。stdlog.0 には同じノードで実行されるプロセスのエントリのみが含まれるので、この値は常に同じです。

genProc

ログ インシデントを生成したプロセスの名前 (ehwriter など) を示します。プロセス名は動作環境によって異なりますが、タスク マネージャのプロセスリスト (Windows) または ps コマンドの出力結果 (UNIX) に表示される名前に対応している必要があります。

PID

タスク マネージャのプロセス リスト (Windows) または ps コマンドの出力結果 (UNIX) に表示される、数値で表されたプロセス ID を示します。同じ名前の複数のプロセスが実行中の場合は、PID が重要になります。たとえば、通常、複数のデータベース エージェントが同じプロセス名で同時に実行されます。

level

プログラマが評価したメッセージの重要性を示します。使用可能な値は、FATAL、EXIT、RESTART、SIGNIFICANT、SEVERE、ERROR、MINIMUM、WARNING、INFORMATION、MILESTONE、TRACE、および VERBOSE です。

codefile

メッセージの生成元であるコード ソース ファイルの名前を示します。

lineum

メッセージが生成されたコード ソース ファイルの行番号を示します。

msgID

TNG イベントに割り当てられている ID を示します。

msgDomain

メッセージの送信元であるドメインの名前を示します。

msgNode

メッセージの送信元であるノードの名前を示します。

msgGenDomain

msgGenUser 値で識別されるユーザが TNG メッセージを生成した元のドメインを示します。

msgGenUser

TNG メッセージを生成したユーザのユーザ ID を示します。

domainID

TNG メッセージの生成元であるドメインの ID を示します。

msgDate

TNG メッセージが生成されたシステム日付の月と日を示します。

msgTime

TNG メッセージが生成されたシステム日付の時刻を示します。

eventID

イベントをトリガしたソース イベント文字列または SED スタイルの正規表現を示します。

arg

メッセージアクションのテキスト文字列に入力された変数を示します。たとえば、メッセージアクションのテキスト フィールドに「ahd.dll AHD_Call help me」と入力した場合、stdlog.0 の引数は「args=help me」と表示されます。

tag

TNG メッセージに関連付けられているタグ データを示します。

IPAddr

TNG メッセージを生成したホストの IP アドレスを示します。

filter

フィルタ ルール ファイルのプロセス名を示します。

filterNum

フィルタ ルール ファイルの番号を示します。

majorSrc

メジャー ソース (またはコンバータ タイプ) を示します。これは、ソース アプリケーション ID を表す文字列です。つまり、イベントの発生元が、Unicenter TNG for Windows (この場合の値は `tng`)、Unicenter for UNIX (この場合の値は `uni`)、または内部デーモン (この場合の値は `-`) のいずれであるかを表します。

msgScr

メッセージ ソースを示します。使用可能な値は、`CNV` (コンバータ)、`FLT` (フィルタ)、`NOS` (ソースなし)、および `WRT` (ライタ) です。

msgType

メッセージ タイプを示します。使用可能な値は、`CRT` (作成)、`DSC` (検出)、`TRM` (終了)、および `UPD` (更新) です。

msgSrcNum

メッセージ ソース番号を示します。

platform

メッセージの送信元の動作環境を示します。使用可能な値は、`AIX`、`AS400`、`DECOSF1`、`DGUX`、`DYNIX`、`HPUX`、`IRIX`、`MISERVER`、`MPRAS`、`MVS`、`NETWARE`、`SINIX`、`SOLARIS`、`SVR4MP`、`TANDEM`、`UNIXWARE`、`WNT` (Windows)、または `UNIX` エージェントによって定義された任意の値です。

イベント ライタ ルールのロード

ライタ ルールを変更または定義する場合は、CA SDM サーバ、または CA NSM コンバータ、フィルタ デーモン、ライタ デーモンなどのサポート プロセスを再起動せずに、これらの新規ルールまたは変更したルールをロードできます。このユーティリティを使用して、既存のライタ ルールをファイルに書き込むこともできます。

イベント ライタ ルールをロードするには、`wrrule` ユーティリティを使用します。

構文(イベント ライタ ルールのロード)

イベント ライタ ルールをロードする場合の構文は以下のとおりです。

```
wrtrule [-v] -c addr [-r rule_file] [-d dump_file]
```

パラメータ(イベント ライタ ルールのロード)

-v

詳細モードであることを示します。このユーティリティを実行すると、フィードバックが表示されます。

-c addr

slistat によって表示されるイベント ライタ の名前です。

-r rule_file

ロードするイベントが含まれているテキスト ファイルの名前です。

-d dump_file

現在のイベント ライタ ルールを書き込むファイルの名前です。以下のタイプの情報がファイルに書き込まれます。

- 保留中のイベント メッセージ
- プロセスで取得中のネットワーク リソース情報
- イベント ライタ ルール

注: **-r rule_file** と **-d dump_file** はいずれもオプションですが、いずれか一方を指定する必要があります。両方を指定することもできます。その場合は新規ルールが最初にロードされます。

注: イベント ライタ で1つ以上の **CA NSM** イベント メッセージを処理している場合は、新規のライタ ルールのロードリクエストを受信しても、ライタ が現在のメッセージの処理を完了するまで新規のロードは延期されます。たとえば、イベントがネットワーク リソース (アセット) 情報を待機しているので、ライタ がイベントを処理していることがあります。この場合は、リソース情報が取得されて **CA SDM** コール リクエストのリクエストが生成されるまでロード メッセージは延期されます。

ただし、現在のイベント ルールをファイルに書き込むリクエストは延期されずに実行されます。

フィルタされたイベントの管理

フィルタおよびイベントライタデーモンと、別のコンピュータにあるイベントソースとの関連付けは、トポロジファイル `topology.cfg` で管理されます。このトポロジファイルは、CA SDM サーバの `$NX_ROOT/site/eh` ディレクトリ (UNIX) または `installation-directory¥site¥eh` ディレクトリ

(Windows) に格納されています。トポロジファイルを使用することで、1つの場所でイベント処理システム全体を決定して管理できます。複数のクライアントに移動する代わりに、1つの場所でファイルを編集し、イベント処理システム全体のトポロジを決定できます。

注: CA SDM サーバの `$NX_ROOT/site/eh` ディレクトリ (UNIX) または `installation-directory¥site¥eh` ディレクトリ (Windows) には、フィルタおよびイベントライタルールも含まれています。

`topology.cfg` ファイルを表示、更新、および保存するには、テキストエディタを使用します。Windows ユーザの場合は WordPad を、UNIX ユーザの場合は vi を使用することをお勧めします。ファイルにフォーマット文字を残すテキストエディタは使用しないでください。

トポロジファイルのフォーマットは以下のとおりです。

```
name cmd [dest-name] [converter-type]
```

各項目は以下のとおりです。

name

ホスト名およびイベント処理デーモンの一意の名前を `hostname:daemon-name` の形式で指定します (たとえば、`ws2:uconv` など)。`daemon-name` は `slstat` に表示されます。

cmd

`$NX_ROOT/bin` ディレクトリ (UNIX) または `installation-directory¥bin` ディレクトリ (Windows) にある実行可能ファイルの名前 (`tngcnv`、`uniconvert`、`filter_nxd`、`ehwriter` など) を指定します。

dest-name

このデーモンから汎用イベントを受信するデーモンを指定します。たとえば、**ws2:filter1**、**ws3:wrtr** のように指定します。イベントライターデーモンには送信先デーモンはありません。すべてのデーモンのレコードは、トポロジ ファイルに登録されている必要があります。

converter-type

イベントの発生元が、**CA NSM for Windows**（この場合の値は **tng**）、**CA NSM UNIX**（この場合の値は **uni**）、または内部デーモン（この場合の値は **-**）のいずれであるかを指定します。

以下に、トポロジ ファイルの例を示します。

```
# maple:uniconv    uniconvert  maple:tngfilter  uni
maple:tngcnv      tngcnv      maple:tngfilter  tng
maple:tngfilter   filter_nxd  maple:tngwriter  -
maple:tngwriter   ehwriter    -                -
```

例

以下は、ある組織で **CA SDM** と **CA NSM** の統合インストールに、フィルタされたイベントを実装した際の例です。

CA SDM 管理者（Ken）は、**CA NSM WorldView** マップに重大なステータスが表示されたときにリクエストを自動的に作成するために、応答するイベントを識別するためのイベント フィルタ ルールを作成する必要があります。また、このタイプのイベントが受信されたときに実行するアクションを指定するためのイベント ライタ ルールも作成する必要があります。

Ken は、まず簡単な 1 つのフィルタ ルールを使用することを決めます。次に、システムを使い慣れてから、より複雑なルール セットを使用することにします。米国にあるサーバから重大イベントを取得することも決めます。このシステムでは、隣接した米国にあるすべてのサーバに **usaxxx** という名前を付ける、非常に簡単な規則を採用しています。

Ken はまず、**CA SDM** サーバの **\$NX_ROOT/site/eh/IP** ディレクトリにある **tngfilter_rule.dat** フィルタ ルール ファイルを編集します。この場合の **IP** は **CA SDM** サーバの **IP** アドレスを表します。ファイルの編集には余分な制御文字を追加しないテキスト エディタを使用できますが、ここでは **UNIX vi** エディタを使用します（**Windows** ユーザの場合は **WordPad** を使用することをお勧めします）。

tngfilter_rule.dat ファイルでは、ポンド記号 (#) はコメント文字を表します。ルールを読み取り時には、ポンド記号の後に続く文字列は無視されます。Ken が編集している tngfilter_rule.dat ファイルの行の大半はコメントに指定されていますが、以下の行があることに気がきます。

```
# Report All Events (separately)
uni::*:*:*:*:*:*:::(0,1)
tng::*:*:*:*:*:*:::(0,1)
```

これらの行は open filter、つまりイベントライタにすべてのイベントを渡すフィルタを構成するものです。

Ken は、これらの行を以下のように変更します。

```
# Report All Events (separately)
# uni::*:*:*:*:*:*:::(0,1)
tng::*:*:*:*:*:*::Object_Status_Updated.*Critical.*:::(0,1)
```

Ken が現在考慮しているのは Windows CA NSM のイベントのみなので、uni 行はコメントにします。Object_Status_Updated.*Critical.* イベントのみを渡すためのフィルタが必要なので、tng 行の event_ID フィールドに

「Object_Status_Updated.*Critical.*」と入力します。オブジェクトのステータスが重大になると、CA NSM によって Object_Status_Updated.*Critical.* イベントが生成されます。

Ken は、フィルタルールファイルを保存した後、CA SDM サーバの \$NX_ROOT/site/eh/IP にある tngwriter_rule.dat ライタルールファイルを編集します。この場合の IP は CA SDM サーバの IP アドレスを表します。

フィルタルールの場合と同様、このファイルの行の大半もコメントです。ファイルの最後の 2 行は、ライタルール定義の初期設定を示します。Ken は、Windows CA NSM からのイベントのみに注目するために、これら 2 行のうちの最初の行はコメントにします。

以下の手順に従って 2 行目をフォーマットします。

1. 重大イベントのみを渡すためのフィルタはすでに設定しているので、イベント ID の.*はそのまま残します。
2. 米国にあるサーバからのイベントのみを受け入れるために、デバイスフィールドに「usa.*」と入力します。
3. すべてのユーザからのイベントを受け入れるために、ユーザフィールドのアスタリスク (*) はそのまま残します。

4. 重大イベントごとに新規リクエストを書き込むために、アクションフィールドの **CR_CREATE** はそのまま残します。
5. システムに適切なリクエストテンプレートがすでに入力しているので、テンプレートフィールドにそのテンプレート名である **CriticalTemplate** を入力します。
6. その他のログ記録は必要ないので、ログフィールドの **NONE** はそのまま残します。

Ken の編集結果は以下のとおりです。

```
# .*::.*::.*::uni::.*::CR_CREATE:::::NONE
.*::usa.*::.*::tnq::.*::CR_CREATE::CriticalTemplate:::::NONE
```

Ken はライタールールファイルを保存してから、CA SDM サーバをリサイクルします。これで、イベントを受信してリクエストを自動的に書き込む準備ができました。

CA NSM 統合のトラブルシューティング

CA NSM を CA SDM と統合、設定、および使用する際に、エラーが発生する可能性があります。これらのエラーのトラブルシューティングを実行する際には、以下の情報を使用します。

- [2D/3D マップのエラーメッセージ \(Windows のみ\)](#) (P. 246)
- [サーバ設定の確認](#) (P. 248)
- [フィルタエラーメッセージ](#) (P. 250)
- [Slump 接続の確認](#) (P. 251)
- [ログ記録の有効化](#) (P. 252)

2D/3D マップのエラー メッセージ(Windows のみ)

2D/3D マップと Unicenter Explorer の統合部分で CA NSM エラーが発生する場合があります。

TNGWV オブジェクトの作成エラー = x

理由:

一般にこのエラーは、先にインテグレーションの解除を実行せずにインテグレーション スクリプトを複数回実行した場合に発生します (x は実行回数を表します)。

アクション:

CA SDM で CA NSM 2D/3D マップと Unicenter Explorer のインテグレーションの解除を実行してからインテグレーションを実行するには、以下の手順に従います。

1. コマンドラインに以下のように入力します。
`installation-directory¥bin¥deintahd.exe`
2. CA NSM オブジェクト ブラウザを開きます。 [方法] に移動してクリックして、メソッドのリストを表示します。
3. 名前の列に AHD メソッドが表示されたら、 [オブジェクト] メニューから [削除] を選択して AHD メソッドを削除します。
4. [Popup_Menu] をクリックして、メニューのリストを表示します。
5. 名前の列の下に AHDManagedObject が表示されたら、 [オブジェクト] メニューから [削除] を選択してオブジェクトを削除します。
6. [Popup_Menu] を開いたまま、名前の列の下に ManagedObjects が表示されるまでスクロールします。
7. メソッド名に AHD が含まれている ManagedObject を検索します。該当するメソッドが見つかったら、 [オブジェクト] メニューから [削除] を選択してメソッドを削除します。
8. [Jasmine_Menu_Action] をクリックして、Unicenter Explorer メソッドのリストを表示します。名前の列に USPSD メニュー アクションが表示されたら、 [オブジェクト] メニューから [削除] を選択してメニュー アクションを削除します。

9. [Jasmine_Menu_Object] をクリックして、Unicenter Explorer メニューのリストを表示します。名前の列に USPSD メニュー オブジェクトが表示されたら、[オブジェクト] メニューから [削除] を選択してオブジェクトを削除します。
10. オブジェクトブラウザを終了します。
11. コマンドラインに以下のように入力します。

```
installation-directory¥bin¥integAHD.exe
```

これで、2D/3D マップと Unicenter Explorer のインテグレーションが正常に完了します。2D/3D マップまたは Unicenter Explorer で管理オブジェクトを右クリックし、すべての CA SDM メニュー オプションが表示されることを確認します。

CAE0232E-リポジトリ エラー コード 22

理由:

このメッセージは、メソッドで指定された実行可能ファイルへのパスが間違っていることを示します。

アクション:

パスに `installation-directory¥bin` を追加するか、メソッドリストの `exe_name` フィールドを変更して実行可能ファイルへの完全パスを含めるようにします。

サーバ設定の確認

CA SDM サーバが UNIX または Windows コンピュータ上にあり、CA NSM が別の Windows コンピュータ上にある場合、CA SDM サーバが稼働している必要があります。CA NSM コンピュータで NSM Event Converter サービスを開始します。コンバータが稼働していることを確認するには、タスクマネージャでプロセスを調べます。Event Converter サービスが開始しているのに `tngcnv` が実行中のプロセスとして表示されない場合は、`installation-directory¥log` にある最新の `tngcnv.n` または `stdlog.n` ファイルを確認します。これらのファイルには、Event Converter が稼働していない理由が記載されています。

CA SDM サーバと CA NSM サーバが同じ Windows コンピュータにある場合は、CA SDM サービスが稼働している必要があります。コンピュータで CA NSM Event Converter サービスを開始します。コンバータが稼働していることを確認するには、タスク マネージャでプロセスを調べます。CA SDM サービスを開始しても `tngcnv` が実行中のプロセスとして表示されない場合は、以下の手順に従います。

1. ワードパッドを使用して、`installation-directory¥pdmconf` にある `pdm_startup` ファイルを編集します。このファイルには、以下のようなテキストが含まれています。

```
[ procset MAIN_PROCSET]
pdm_info
sw_ver_ctl
bnotify_nxd
PDMBASE
PDMBOP
FILTERING
```

`FILTERING` の行にセミコロン (;) が付いてコメントになっている場合は、セミコロンを削除します。

2. ファイルの先頭に戻り、以下のテキストを参照します。

```
[ procset FILTERING ]
tngfilter
tngwriter
ehc
; UNICNV_REPLACE
; tngcnv:NT_ONLY
```

上のいずれかのオプションにセミコロン (;) が付いてコメントになっている場合は、セミコロンを削除します。

3. このファイルの内容を変更した場合は、変更内容を保存してから CA SDM サーバをリサイクルします。

引き続き Event Converter が実行中のプロセスとして表示されない場合は、`installation-directory¥log` にある最新の `tngcnv.n` ファイルを確認します。このファイルには、Event Converter が稼働していない理由が記載されています。

フィルタ エラー メッセージ

Event Converter (tngcnv) が開始されない場合、またはコンバータが稼働しているのにリクエストが作成されない場合は、Event Converter が開始されない理由またはイベントを報告できない理由を示すエラー メッセージがログ ファイルに記録されることがあります。以下のエラー メッセージが 1 つ以上含まれている場合があります。

Can't resolve host name to an IP address

理由:

このメッセージは、CA SDM コンピュータまたは CA NSM コンピュータ、あるいはその両方にホスト エントリがないことを示します。

また、DNS が動作していないことや、正しい IP アドレスを返していないことを示す場合もあります。

アクション:

%SystemRoot%/system32/drivers/etc/hosts ファイルを確認します。ホスト ファイルには、CA SDM コンピュータと CA NSM コンピュータに関するエントリが含まれている必要があります。ホスト名を追加したら、コンバータ（または CA SDM サービス）を再起動します。エントリの例は以下のようになります。

```
127.0.0.1      localhost      # Local host loop back
141.202.211.11 usbegp11       # This is the NSM client box
141.202.211.12 usbegp12 ahdhost # This is the Service Desk host
                                     # (showing multiple entries)
```

Cannot find repository file

理由:

このメッセージは、クライアントの *installation-directory* にある NX.env に @NX_REPOSITORY パラメータが設定されていないことを示します。

アクション:

NX.env を編集し、リポジトリ名を追加します。名前が完全に一致していることを確認したら、ファイルを保存して、Event Converter を再起動します。

The dependency doesn't exist or has been marked for deletion

理由:

このメッセージは、削除が必要なコンバータに依存関係（おそらく MSSQL）が設定されている場合に発生します。

アクション:

regedt32 を実行して、[HKEY_LOCAL_MACHINE] - [System] - [Current Control Set] - [Services] を選択して、[AHD_Event_Converter] ツリーを開きます。- MSSQL 依存関係（またはその他の該当するエントリ）を削除して、Windows サーバを再起動します。

Destination unknown, Queuing events または No topology.cfg file entry for node; queuing event

理由:

このメッセージは、CA SDM サーバの topology.cfg ファイルを修正する必要があることを示します。

アクション:

必要に応じて topology.cfg ファイルを修正して、CA SDM および CA NSM コンバータをリサイクルします。以下に、AHD1 という名前の Windows コンピュータおよび TNG1 という名前の CA NSM コンピュータにある CA SDM の topology.cfg ファイルの例を示します。

```
TNG1:tngcnv      tngcnv      AHD1:tngfilter   tng
AHD1:tngfilter   filter_nxd  AHD1:tngwriter   -
AHD1:tngwriter   ehwriter    -                 -
```

Slump 接続の確認方法

CA NSM コンバータが稼働しているのにイベントの作成を確認できない場合は、CA SDM への Slump 接続を確認する必要があります。

接続を検証するには、以下の手順に従います。

1. CA SDM コンピュータ上でコマンドラインから *sstat* コマンドを使用します。

2. tngcnv への Slump 接続を探します。
見つからない場合、コンバータは CA SDM と通信していません。
3. CA NSM コンバータを再起動して、接続を再度確認します。
4. (引き続き接続が見つからない場合) *installation-directory*¥log にある *tngcnv.n* ファイルで tngcnv および Slump ログインに関するエラーを確認します。

ログ記録の有効化

Slump ログインに成功したのに新規イベントを確認できない場合は、ログ記録を有効にして、ログ ファイルを調べてイベントが CA NSM から発生していることを確認します。2D/3D マップで管理オブジェクトのステータスを変更するだけで、イベントを作成することができます。

ログ記録を有効にするには、\$NX_ROOT (UNIX) または *installation-directory* (Windows) にある *NX.env* を編集して、以下の行を挿入します。

```
@NX_LOG_LEVEL_BSTRAP=VERBOSE
```

これで、*installation-directory*¥log にある *tngcnv.n* ファイルを監視して、イベントが CA SDM に渡されているかどうかを特定できます。結果は以下のように表示されます。

```
09/17 16:35:58:01 tngcnv 477 MILESTONE convrtr.c 399
Sending 1:::dogwood:::9994011e-2f7e-11d1-a435-00c04fd478c9:::97/09/17
:::16:35:41:::Object_Status_Updated minor:::BV:141.202.211.0:Segment.1
IP:141.202.211.14 MAC: CNT: LOC: DSC:::3:::tngcnv:1:::tng:::WindowsNT:
:::CNV:::CRT:::1:::
```

この例のメッセージは、管理オブジェクトのステータスがマイナーに更新されたことを示します。

イベントが CA SDM に渡されていて、ログに表示されていることを確認した場合は、フィルタ ルールとライタ ルールの初期設定を使用していることを再度確認します。これらのルールの初期設定を使用していない場合は、デフォルトのフィルタ ルールとライタ ルールのファイルを復元し、サーバをリサイクルして、イベントを作成します。

イベントが CA SDM に渡されていないことを確認した場合は、イベント情報を渡す処理をする 2 つの CA NSM プロセス（`canotify.exe` および `caoprdrmn.exe`）が実行中であることを確認します。これらのプロセスが実行中でない場合は、CA NSM のドキュメントに記載されている手順に従ってプロセスを開始します。プロセスが実行中の場合は、CA NSM サポートに問い合わせてください。

CA NSM 統合の使用

以下の例では、CA NSM と CA SDM の統合を使用する方法を示します。

1. コンテンツが限定された[メッセージ レコードおよびメッセージ アクションを作成します](#) (P. 254)。
2. [cawto ユーティリティを使用してリクエストを作成または更新します](#) (P. 255)。
3. [サンプル ファイルを使用](#) (P. 256) して前のタスクを実行します。

注: 本セクションの例にはデフォルトの機能の設定例が含まれていますが、このタスクを完了するための唯一の方法ではありません。

コンテンツが限定されたサンプル メッセージ レコードおよびサンプル メッセージ アクション

CFNEW と CFUPDATE という 2 つのメッセージ レコードはそれぞれ 1 つのメッセージ アクションによって書き込まれます。これらのメッセージ レコードは、この例では、NSM を CA SDM にインテグレートするための基礎になっています（サンプル ファイルも含まれています）。クリーン、コンパクト、かつ堅牢で、管理が容易なインテグレーションを実現するために、以下の強力な機能を活用できます。

- tngwriter_rule.dat
- CR_UPDATE 関数および CR_UPDATE_ONLY 関数
- text_api キーワード リスト

注: この例では、コンテンツのほとんどないメッセージ レコードおよびメッセージ アクションの作成方法を示します。コンテンツは **cawto** コマンドに挿入されています。これについては後続の例に示します。別の方法として、必要なパラメータとコンテンツをメッセージ アクションの [テキスト] フィールドに直接入力することができます。また、これらの 2 つの方法を組み合わせて使用することもできます。

サンプル イベント管理メッセージ レコード

この統合を使用するときは、[Message Record - Detail] ページを使用して、イベント警告の先頭に「CFNEW」が含まれたイベントに対応するイベント管理メッセージ レコードの例を表示できます。

サンプルメッセージアクションリスト

この統合を使用する際、「CFNEW*」メッセージレコードに関連付けられているメッセージアクションリストを使用できます。項目をダブルクリックすると、メッセージアクションの一部として格納されている詳細情報が表示されます。統合を継続して使用する場合は、[アクション] フィールドに「EXTERNAL」が設定され、[テキスト] フィールドに標準統合テキストの値「AHD.dll AHD_Call」が設定されている詳細ビューを使用できます。

サンプルメッセージレコード (CFUPDATE で始まるイベントをスキャンするように設定されている場合)

この統合を使用する際、「CFUPDATE」で始まるイベントをスキャンするように設定されている、2 番目のメッセージレコードの詳細結果を表示できます。このメッセージレコードには、同一のメッセージアクションが作成されています（前の図の「CFNEW*」メッセージレコードを参照）。

リクエストを生成および更新する cawto コマンドの例

すでに作成済みのメッセージレコードを使用するには、CA NSM の「cawto」ユーティリティ/コマンドを使用して、CA NSM イベント管理からメッセージを送信します。「cawto」ユーティリティ/コマンドを使用すると、以下の 2 つの例に示されているコマンドフォーマットを使用して、リクエストを作成または更新できます。

注: この方法を使用すると、イベント管理コンソールに表示される警告メッセージを取得して、(CA SDM の対応フォーマットに変換するために) 再フォーマットできます。

NSM メッセージおよびアクションルールの作成後にメモリに格納された NSM イベント メッセージ レコードおよびメッセージアクションを更新するには、NSM イベント管理コンソールで「opreload」コマンドを実行します。

例 1: 新規リクエストを生成および更新する場合の「cawto」のフォーマット

新規リクエストを生成する場合は、以下の **cawto** フォーマットを使用します。

```
CAWTO -n <NSM-server-name>  
CFNEW;%STRING1=KEYWORD1;%CUSTOMER=ServiceDesk;%SUMMARY=Photos  
required;%CATEGORY=Applications;%DESCRIPTION=Description: Photos required  
Justification: required by regulations for entry
```

リクエストを更新する場合は、以下の **cawto** フォーマットを使用します。

```
CAWTO -n <NSM-server-name>  
CFUPDATE;%STRING1=KEYWORD1;%STATUS=Closed;%SUMMARY=Cancelled by ServiceDesk
```

例 2: 新規リクエストを生成および更新する場合の「cawto」の別のフォーマット

新規リクエストを生成する場合は、以下の別の **cawto** フォーマットを使用します。

```
CAWTO -n <NSM-server-name> CFNEW2;%EVENT_TOKEN=KEYWORD2;%SUMMARY=Server  
Installation Approved;%STATUS=Work in  
Progress;%CATEGORY=Hardware;%DESCRIPTION=Install new server and level V drops to  
existing server location within the data center. Also, install wiring on patch  
panel in router cabinet
```

リクエストを更新する場合は、以下の別の **cawto** フォーマットを使用します。

```
CAWTO - n <NSM-server-name>  
CFUPDATE2;%EVENT_TOKEN=KEYWORD2;%STATUS=Closed;%SUMMARY=Closed by Server Team
```

統合に使用するサンプル ファイル

以下に、CA NSM と CA SDM を統合するときに使用できるサンプル ファイルを示します。

- [topology.cfg](#) (P. 257)
- [tngifilter_rule.dat](#) (P. 257)
- [tngwriter_rule.dat](#) (P. 257)

topology.cfg

```
# <remote_node>:uniconv uniconvert <IP_ADDR_tngfilter>:tngfilter uni
<IP_ADDR_tngcnv>:tngcnv tngcnv <IP_ADDR_tngfilter>:tngfilter tng
<IP_ADDR_tngfilter>:tngfilter filter_nxd <IP_ADDR_tngwriter>:tngwriter -
<IP_ADDR_tngwriter>:tngwriter ehwriter - -
```

各項目の説明：

<IP_ADDR_tngcnv>

CA NSM Event Converter プロセスを実行しているサーバの IP アドレスです。

<IP_ADDR_tngfilter>

CA SDM を実行しているサーバの IP アドレスです。

<IP_ADDR_tngwriter>

CA SDM を実行しているサーバの IP アドレスです。

tngfilter_rule.dat

このファイルのデフォルトバージョンを変更せずに使用します。

tngwriter_rule.dat

tngwriter_rule.dat は以下のように表示されます。

```
# evt
id:::dev:::user:::majorSrc:::minorSrc:::action:::template:::cmd:::log:::event_tok
en:::user_parms
```

各項目は以下のとおりです。

event id

文字列または SED スタイルの正規表現です。

device

文字列、SED スタイルの正規表現、「*」、または空白です。

user

文字列、「*」、または空白です。

majorSrc

uniconverter の場合は文字列「uni」、tng コンバータの場合は「tng」です。

minorSrc

文字列または「*」です。

action

アクションのオプションです。以下のオプションを使用できます。

CR_CREATE

イベントごとに新規リクエストを書き込みます。

CR_UPDATE

既存のリクエストが存在する場合は 1 つ以上のリクエストを更新します。リクエストが見つからない場合はリクエストを新規作成します。デフォルトでは、レコードは **log_agent** および **affected_resource** (アセット) フィールドの一致によって検索されます。コール リクエストの属性のリストを指定することにより、デフォルトをオーバーライドできます。

CR_UPDATE_ONLY

CR_UPDATE と同様ですが、一致するリクエストが見つからない場合、新規リクエストは作成されません。

COMMAND

このテーブルの **cmd** 記述で指定された<cmd>を実行します。

template

リクエストの作成に使用するリクエストテンプレートの名前を指定します。**action** が **CR_CREATE** 以外の場合は、このパラメータを指定する必要はなく、指定しても無視されます。

注: ルールを定義する前に、リクエスト テンプレートを作成しておく必要があります。

cmd

シェルに渡されるコマンドです。COMMAND アクション以外のアクションでは無視されます。

ログ記録

ログのオプションです。以下のオプションを使用できます。

NONE

エラー ログ以外のログ記録を実行しません。

SYS

UNIX syslog (Unicenter メッセージ コンソール) にインシデントのログを記録します。

PDM

アプリケーション ログ (\$NX_ROOT/log) にインシデントのログを記録します。

BOTH

アプリケーション ログと syslog の両方にインシデントのログを記録します。

event_token

(オプション) これは、event_id (tng イベントメッセージ) または event_id に相当するすべてのメッセージ (ワイルドカードが指定された event_id など) に関連付けられている特定のリクエストを識別するために使用される 30 文字のユーザ定義タグです。

event_token はリクエストの属性で、TNG インターフェースによって生成された各リクエストに格納されます。ライタールールで event_token を指定しないと、文字列「tng_generated」が使用されます。この場合、ユーザは event_token 属性に一致するすべてのリクエストを更新できます。たとえば、同じアセットに関する 2 つの異なるメッセージによって一意のリクエストを更新できます。各 CR_UPDATE ライタールールでは、一意のメッセージ要素と一意の event_token を指定します。event_token は、一致するリクエストの検索および更新に使用されます。デフォルトでは、メッセージを含むアクティビティ ログが、一致するリクエストに追加されます。

別の例では、ユーザは、CR_CREATE ライタールールを使用してリクエストを作成したときに使用した CR_UPDATE ライタールールに同じ event_token を指定することで、既存のリクエストのステータス属性を更新できます (たとえば、STATUS=CL (クローズ) を設定します)。

user_parms

(オプション) 以下の 3 つのタイプの情報が含まれます。

- リクエストの属性値
- 既存のリクエスト レコードを更新するときに一致させるリクエストの属性のリスト
- TNG イベント構造の対応する値で置き換えられる特殊パラメータ名

リクエスト値と、属性のリストを指定する際は、%<KEYWORD>=<value> という構文を使用します。キーワードと値のペアを複数使用する場合は、各ペアをセミコロン (;) で区切ります。

リクエストの属性値を指定する際は、%<ATTRIBUTE>=<value> という構文を使用します。ATTRIBUTE は、\$NX_ROOT/site ディレクトリにある text_api.cfg で識別される属性名で、AHD majic リクエストの属性にマップされます。

一致させる属性のリストの構文

は、%SEARCH=<attribute1>[,<attribute2>.]と指定します。SEARCH は固定のキーワードで、attribute1、attribute2 などは text_api.cfg で指定した ATTRIBUTE の名前を表します。

以下の特殊パラメータ名は、user_parms 文字列で任意に使用できます。

&Message

CA NSM メッセージに関連付けられているメッセージテキストです。

&Parm

CA NSM メッセージアクションのダイアログボックスの AHD.DLL Parm フィールドです。

&Uuid

TNG 全体で一意的 ID です。

&Device

CA NSM メッセージを生成したデバイス（ホスト名など）です。

&Majorsrc

イベント ライタにイベントを転送するメジャー タイプのソースです。Windows の CA NSM からのイベントの場合、値は「tng」です。UNIX の CA NSM からのイベントの場合、値は「uni」です。

&Minorsrc

イベント ライタにイベントを転送するマイナー タイプのソースです。

&Node

CA NSM メッセージを生成したデバイス（ホスト名など）です。

&Addr

CA NSM メッセージを生成したホストの IP アドレスです。

&Username

CA NSM メッセージを生成したホストのユーザ名です。

&Date

CA NSM メッセージが生成された 1970 年以降の期間を表す整数です。

&Time

CA NSM メッセージの日付と時刻です（たとえば、Tue Jul 4 10:23:37 2000）。

&Severity

CA NSM メッセージの重大度です。

&Tag

CA NSM メッセージに関連付けられているタグ データです。

ここでは、「例 2：新規リクエストを生成および更新する場合の「Cawto」の別のフォーマット」に記載されている例を使用して、以下のイベントライターールのデフォルトのファイルを変更します。

```
*:....*:....*:....uni:....*:....CR_CREATE:.....:NONE
```

以下のように変更します。

```
CFNEW.*:....*:....*:....tng:....*:....CR_UPDATE:.....:NONE:.....&Parm;%SEARCH_EXPLICIT=STRING1
CFNEW2.*:....*:....*:....tng:....*:....CR_UPDATE:.....:NONE:.....&Parm;%SEARCH=Event_Token
CFUPDATE.*:....*:....*:....tng:....*:....CR_UPDATE_ONLY:.....:NONE:.....&Parm;%SEARCH_EXPLICIT=STRING1
CFUPDATE2.*:....*:....*:....tng:....*:....CR_UPDATE:.....:NONE:.....&Parm;%SEARCH=EVENT_TOKEN;%STATUS=CL
```

注: %SEARCH_EXPLICIT パラメータを使用すると、更新処理を実行する前に STRING1 フィールドのコンテンツを比較して、一致するリクエストを検索できます。text_api.cfg の詳細と、CA SDM でテキスト API を使用して CA NSM からリクエストを作成する方法については、「管理ガイド」を参照してください。

関連項目:

[イベントライターールの定義 \(P. 229\)](#)

CA EEM をインストールする方法

注: このコンポーネントをインストールする前に、正常なインストールを計画する方法についての情報を確認して、把握しておいてください。

CA SDM r12.9 のインストールメディアには、CA EEM r12 CR2 が用意されています。CA EEM は、CA Workflow や CA Service Management などの CA Technologies 製品のユーザに対する認証および権限の付与を実行します。認証とは、ユーザ ID とパスワード、あるいはその他の情報によって、ユーザが有効な製品ユーザであるかどうかを確認することを意味します。権限とは、ログインしたユーザが製品内の特定の機能にアクセスできることを意味します。

ユーザがログインしようとするたびに、CA EEM によってユーザの情報が認証されます。認証されると、アクセスが許可または拒否されます。たとえば、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 レコードを持っている必要があります。CA SDM 内で CA Workflow を使用して、ビジネス プロセスを管理するには、まず、サポートされている動作環境で CA EEM インストールを開始して実行します。その直後に、CA Workflow をインストールします。

重要: 既存の CA EEM インストールを CA Technologies 製品の認証に使用できる場合は、再度 CA EEM をインストールしないでください。その代わりに、CA Technologies 製品をインストールし、既存の CA EEM インストールを参照するようにします。ただし、CA SDM r12.9 と統合するには、少なくとも CA EEM r8.4 SP4 CR05 が必要です。

関連項目:

[CA EEM と CA Workflow のインストール計画](#) (P. 135)

[CA EEM のインストール \(Windows\)](#) (P. 263)

[CA EEM のインストール \(UNIX\)](#) (P. 265)

CA EEM のインストール (Windows)

サポートされている動作環境上で CA EEM インストールを開始して実行できます。

重要: 既存の CA EEM インストールを CA Technologies 製品の認証に使用できる場合は、再度 CA EEM をインストールしないでください。その代わりに、CA Technologies 製品をインストールし、既存の CA EEM インストールを参照するようにします。ただし、CA SDM r12.9 と統合するには、少なくとも CA EEM r8.4 SP4 CR05 が必要です。

CA EEM のインストール方法

1. (オプション) Java Runtime Environment (JRE) 1.5 がインストールされており、JAVA_HOME 変数が設定されていることを確認します。

注: CA EEM 8.4 以降ではこの手順をスキップできますが、CA SiteMinder と SAML を統合できないことを示す警告が表示されます。

2. ドライブにインストール メディアを挿入します。

重要: インストール メディアに使用できる適切なドライブがコンピュータにない場合は、**CA SDM** をインストールするコンピュータにメディアの内容をコピーします。その後、インストールを開始します。ネットワーク経由のリモートインストールの場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、インストールを開始できます。

3. [言語の選択] をクリックします。

インストール メニューが表示されます。

注: インストール メニューが自動的に表示されない場合は、インストールメディアのルートにある **setup.exe** ファイルをダブルクリックしてインストールを開始します。

4. [製品のインストール] タブをクリックします。

5. [CA Embedded Entitlements Manager] をクリックします。

6. 引き続き画面の指示に従って、CA EEM のインストールを完了します。

CA EEM がインストールされます。ほかの CA Technologies 製品をインストールできます。

注: CA SDM r12.9 から、CA EEM の 32 ビット版と 64 ビット版の両方のインストーラが同梱されるようになりました。32 ビットの Windows コンピュータでは、CA EEM は 32 ビット アプリケーションとして実行されます。64 ビット コンピュータでは、CA EEM は 64 ビット アプリケーションとして実行されます。

ただし、CA iTechnology iGateway が 64 ビット Windows コンピュータ上で 32 ビット アプリケーションとして実行されている場合は、CA EEM も 32 ビット アプリケーションとして実行されます。

関連項目:

[CA EEM と CA Workflow のインストール計画 \(P. 135\)](#)

CA EEM SDK の FIPS 準拠モード設定

CA EEM サーバを FIPS (Federal Information Processing Standard) 準拠モードに設定する場合は、CA EEM SDK を FIPS 準拠モードに設定することをお勧めします。

次の手順に従ってください:

1. NX_ROOT/pdmconf/eiam.config ファイルに移動します。
2. CA EEM Java SDK の FIPS 設定を ON に変更します。
3. eiam.config ファイルを保存します。

注: CA EEM C++ SDK の FIPS 設定はデフォルトで ON に設定されています。CA EEM SDK を FIPS 準拠モードに設定する方法の詳細については、CA EEM のマニュアルを参照してください。

CA EEM のインストール (UNIX)

Linux および UNIX 向けの CA EEM では自己解凍シェルスクリプトが使用され、それによってインストールプロセスを実行できます。インストールプロセスの実行中、ライセンス情報が示され、インストールパラメータの入力を求めるプロンプトが表示されます。インストールパラメータを入力したら、インストールが開始されます。

重要: 既存の CA EEM インストールを CA Technologies 製品の認証に使用できる場合は、再度 CA EEM をインストールしないでください。その代わりに、CA Technologies 製品をインストールし、既存の CA EEM インストールを参照するようにします。ただし、CA SDM r12.9 と統合するには、少なくとも CA EEM r8.4 SP4 CR05 が必要です。

CA EEM のインストール方法

1. ターゲット コンピュータで該当するインストール スクリプトを実行します。
 - (Linux) /lnxsvr.cd1/ca_tps.lnx/EEM/EEMServer.bin -i console
 - (AIX) /aixsvr.cd1/ca_tps.aix/EEM/EEMServer.bin -i console
 - (Oracle) /solsvr.cd1/ca_tps.sol/EEM/EEMServer.bin -i consoleファイルが解凍され、インストールが開始されます。

2. 「Y」と入力して、使用許諾契約書の契約条件に同意します（または、「N」と入力して、インストールを却下して中止します）。

インストールパラメータの入力を求めるプロンプトが表示されます。

3. CA EEM のインストールパスを入力します（または、デフォルト値をそのまま使用します）。

入力したインストールパラメータ値を確認する画面が表示されます。

4. 確認画面の情報が正しい場合は、「Y」を入力して、インストールを続行します。「N」を入力すると、インストーラは終了します。

5. EiamAdmin パスワードを入力します。

注: デフォルトの管理者ユーザ名は EiamAdmin です。

インストール手順は、コマンドラインパラメータと、インストールされる CA EEM パッケージのタイプによって異なります。

コンピュータへの CA EEM のインストールが完了します。

CA Workflow をインストールする方法

注: このコンポーネントをインストールする前に、正常なインストールを計画する方法についての情報を確認して、把握しておいてください。

重要: CA Workflow は、CA SDM r12.9 インストールメディアにはバンドルされません。CA Workflow を使用する場合、CA サポート オンラインから CA SDM r12.7 ISO をダウンロードして、CA Workflow をインストールします。

ユーザが CA Workflow にログインしようとするたびに、CA EEM によってその情報が認証されます。認証されると、アクセスが許可または拒否されます。CA Workflow IDE またはワークリストにアクセスするには、ユーザは CA EEM ユーザ レコードを持っている必要があります。

ビジネス プロセスを管理するには、CA EEM をインストールした後、任意の CA SDM サーバ上で CA Workflow のインストールを開始して実行します。

重要: CA Workflow をインストールした後 CA SDM をアンインストールすると、CA Workflow もアンインストールされます。

CA Workflow ログ (*pdm_install_wf.log* および *pdm_tomcat_CAWF.log*) は、\$NX_ROOT/log にあります。CA Workflow のインストールが正常に完了すると、\$NX_ROOT/site/Workflow/log に *wf_admin.log*、*wf_process.log*、*wf_security.log*、および *wl_debug.log* が格納されます。

関連項目:

[CA EEM と CA Workflow のインストール計画](#) (P. 135)

[CA Workflow のインストール \(Windows\)](#) (P. 267)

[CA Workflow の開始と停止](#) (P. 325)

[CA Workflow のインストール \(UNIX\)](#) (P. 268)

CA Workflow のインストール(Windows)

CA Workflow を使用して CA SDM 内のビジネス プロセスを管理します。

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: いずれかのアプリケーション サーバ
2. [CA サポート オンライン] から r12.7 ISO をダウンロードし抽出します。

3. リストから言語を選択し、[言語の選択] をクリックします。

インストール メニューが表示されます。

注: インストール メニューが自動的に表示されない場合は、インストールメディアのルートにある **setup.exe** ファイルをダブルクリックしてインストールを開始します。

4. [製品のインストール] タブをクリックし、[CA Workflow] をクリックします。
5. 引き続き画面の指示に従って、CA Workflow のインストールを完了します。

CA Workflow がインストールされます。さらに、CA SDM との連携用の設定を行います。

関連項目:

[問題管理サンプルワークフローの設定方法 \(P. 334\)](#)

[CA Workflow インテグレーション \(P. 711\)](#)

CA Workflow のインストール (UNIX)

CA Workflow を使用して CA SDM 内のビジネス プロセスを管理します。

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. [CA サポート オンライン] から r12.7 ISO をダウンロードし抽出します。
3. 抽出された ISO のルートディレクトリに移動し、以下のコマンドを実行して、インストールを開始します。

```
sh ./setup.sh
```

4. リストから言語を選択し、[言語の選択] をクリックします。
インストール メニューが表示されます。
5. [製品のインストール] タブをクリックし、[CA Workflow] をクリックします。
6. 引き続き画面の指示に従って、CA Workflow のインストールを完了します。

CA Workflow がインストールされます。さらに、CA SDM との連携用の設定を行います。

関連項目:

[問題管理サンプル ワークフローの設定方法](#) (P. 334)

[CA Workflow インテグレーション](#) (P. 711)

スタンドアロン CA Workflow IDE のインストール

CA SDM インストール メディアから Windows や Linux 上に CA Workflow IDE スタンドアロンクライアントをインストールできます。UNIX インストールでは、このクライアントによって、UNIX CA Workflow サーバへの接続が可能になります。ログイン GUI 内の URL を変更することで、動作環境にかかわらず、任意の CA Workflow サーバインストールを指定できます。

CA SDM は CA Workflow IDE のインストールには必要ありません。インストール ログの場所は、システムに CA SDM がある場合とない場合とで異なります。

- CA SDM が Windows や Linux にインストールされている場合、ログは以下の場所にあります。
\$NX_ROOT/logs
- CA SDM がインストールされていない場合、ログは以下の一時フォルダ内に配置されます。

Windows

%temp%

Linux

/tmp

次の手順に従ってください:

1. CA SDM r12.7 インストール メディアを開いて、CA Workflow IDE を選択します。
[CA SDM コンポーネント インストーラ] ウィザードが表示されます。
2. [Workflow クライアントのインストール場所] を指定し、[次へ] をクリックします。
インストールは終了です。

CA Workflow IDE インストールの確認

CA Workflow IDE インストールが正常に完了したことを確認する必要があります。

CA Workflow IDE インストールを確認する方法

1. CA SDM コンポーネント インストーラ ウィザードの [Workflow クライアントのインストール場所] フィールドで指定したディレクトリに移動します。
2. ディレクトリに以下が含まれることを確認します。
 - 「クライアント」 および 「アンインストール」 という名前のフォルダ
 - *version.txt* と *wekinstall.log* という名前のファイル

注: インストールにエラーがある場合や、フォルダとファイルが適切な場所がない場合は、*pdm_install_wf_client.log* を確認します。

Windows では、[スタート] メニューの [プログラム] - [CA] - [Service Desk Manager] - [CA Workflow IDE] を選択して、CA Workflow IDE を起動できます。

CA Workflow IDE クライアントのアンインストール (Windows および Linux)

次の手順に従ってください:

1. 以下のコマンドを実行します。

```
<install_location>/jre/bin/java" -cp  
"<install_location>/uninstall/uninstall.jar" run -silent
```

install_location

CA Workflow IDE クライアントがインストールされたルートフォルダを指定します。

■ Windows の例

CA Workflow IDE クライアントがインストールされたルートフォルダが「c:¥test」の場合

```
"c:¥test¥jre¥bin¥java" -cp "c:¥test¥uninstall¥uninstall.jar" run -silent
```

■ Linux の例

CA Workflow IDE クライアントがインストールされたルートフォルダが「/test」の場合

```
"/test/jre/bin/java" -cp "/test/uninstall/uninstall.jar" run -silent
```

2. CA Workflow IDE クライアントがインストールされたルートフォルダを削除します。
3. (Windows) 関連付けられた [スタート] メニューのショートカットを削除します。

CA Business Intelligence for CA SDM をインストールする方法

CABI（CA Business Intelligence）では、SAP Business Objects Enterprise Edition の一貫したインストールが提供されます。複数の CA 製品が CABI のライセンスを共有できます。CA SDM のインストールの一部として CABI をインストールできます。

以下の図に、CABI のインストールの方法を示します。



次の手順に従ってください:

1. [CA Business Intelligence のインストールを計画します。](#) (P. 273)
2. [CA Business Intelligence をインストールします。](#) (P. 274)
3. [CA Business Intelligence のインストールを確認します。](#) (P. 275)

CA Business Intelligence のインストールの計画

CABI for CA SDM の実装を計画する前に、以下の考慮事項を確認します。

- CABI 用の要件およびインストールの考慮事項を理解します。詳細については、「*CA Business Intelligence リリース ノート*」および「*CA Business Intelligence 実装ガイド*」を参照してください。
- CABI をインストールするコンピュータ上のすべてのアンチウイルスソフトウェアを一時的に無効にします。
- CA SDM と CABI との統合では、CABI アプリケーション サーバとして Apache Tomcat のみをサポートします。
- インストールするコンポーネントの場所を決定します。これらのコンポーネントには、システムを実行するために必要な特定のサブネット、コンピュータ、データベース、セキュリティ、またはクラスタ システムが含まれます。
- インストールのための以下の前提条件を確認します。
 - データベース サーバの詳細および認証の詳細が使用可能であること。
 - 新しい SQL Anywhere データベースをインストールするか、または既存の SQL Anywhere データベースを使用するための権限を持っていること。
 - Server Intelligence Agent (SIA) の名前が用意されていること。
 - Web アプリケーション サーバがインストールおよび設定されていること。
 - 選択したオペレーティング システムのインストール チェックリスト

注: CABI のインストールは、Windows プラットフォームに限定されます。ただし、サポートされるすべてのプラットフォームで、CABI を CA SDM と統合できます。

CA Business Intelligence のインストール

簡易またはカスタム モードを使用して、スタンドアロンサーバに CA Business Intelligence リリース 3.3 をインストールできます。

注: 高可用性設定では、CA Business Intelligence を別のサーバにインストールする必要があります。

簡易インストール

CA Business Intelligence をすべての必須およびオプション コンポーネントと共にインストールするには、簡易インストールを使用します。

次の手順に従ってください:

1. ドライブにインストール メディア DVD 2 を挿入します。
インストール メニューが開きます。
2. [言語の選択] リストから言語を選択します。
インストール メニューが開きます。
3. [製品のインストール] タブをクリックします。
4. [CA Business Intelligence インストール] をクリックします。
5. 引き続き画面の指示に従って CA Business Intelligence のインストールを完了します。

注: 詳細については、「*CA Business Intelligence 実装ガイド*」を参照してください。

6. 画面の指示に従ってコンピュータを再起動します。
7. CA Business Intelligence は、あらゆるパフォーマンス管理、レポート、クエリ、および分析アプリケーションをサポートします。CA Business Intelligence インストールを完了するには、CA Business Intelligence R3.3 SP1 (CABI 3.3 SP1 パッチ リリースは、SAP BOXI 3.1 SP6 パッチ リリースと同じです) パッチをインストールする必要があります。パッチをダウンロードしてインストールするには、以下のリンクを開きます。

ftp://ftp.ca.com/pub/CABI/CABI-3.x/boeXIR3_SP6/Windows/

注: パッチのインストールの詳細については、「*CABI 3.3 SP1 リリースノート*」を参照してください。

8. JDK7 をサポートするために CA Business Intelligence R3.3 SP1 パッチをアップグレードします。詳細については、`cabi-windows-boeXIR3_SP6¥Docs` フォルダの *Upgrading CABI 3.3 SP1 JDK to 7.pdf* を参照してください。

9. 以下の場所から `cabi33sp1hotfix` パッチを適用します。

`ftp://ftp.ca.com/pub/CABI/CABI-3.x/boeXIR3_SP6/Windows/`

注: パッチを適用する方法についての指示として、`readme.txt` を使用します。

CA Business Intelligence がインストールされました。

カスタム インストール

カスタム インストール オプションを使用すると、CA Business Intelligence の選択したコンポーネントをインストールできます。このオプションは、指定された SAP BusinessObjects Enterprise コンポーネントおよび役割に精通している場合にのみお勧めします。カスタム インストールは、選択するオペレーティング システムやデータベースによって異なります。詳細については、「*CA Business Intelligence 実装ガイド*」を参照してください。

CA Business Intelligence のインストールの確認

CABI サーバ上の CABI のインストールをチェックして、製品が正しくインストールさ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. [スタート] - [プログラム] - [BusinessObjects] - [BusinessObjects Enterprise] - [BusinessObjects Enterprise Java Infoview] を選択します。
2. 管理者パスワードを入力して、Infoview にログインします。ログインが成功した場合は、CABI のインストールが成功していることを示します。

インストールの確認

CA SDM をインストールしたら、以下の情報を使用して、インストールが正常に完了したことを確認してください。

1. パスのシステム環境変数が、製品用に指定したインストールディレクトリに設定されていることを確認します。デフォルトのホームディレクトリは **C:\Program Files\CA\Service Desk Manager** です。
2. 以下を確認してください。
 - a. [コントロールパネル]（[プログラムの追加と削除]）で、製品のエントリが表示されることを確認します。
 - b. [スタート] メニューから、以下のオプションが表示されることを確認します。
 - ドキュメントの表示
 - 環境設定ウィザードの開始
 - Web インターフェースの開始
 - テクニカルサポートに問い合わせてください。
 - Web Screen Painter を起動します。
 - CA SDM のアンインストール
3. Web インターフェースを開始できることを確認します。

重要： この情報を確認できない場合、製品は正しくインストールされていません。このような場合は、**CA SDM** のインストールを再度開始して、インストールを修正してください。

関連項目：

[Web インターフェースの開始 \(P. 290\)](#)

インストール ログ

CA SDM をインストールすると、インストール ログ ファイルが作成され、インストール中に発生したアクション、イベント、およびシステム変更が文書化およびリスト化されます。製品が正常にインストールされない場合、ログ ファイル内のエラーを確認して、製品を正常にインストールするための問題修正に役立てることができます。

ServiceDesk_r12_7_Install.log ファイルは、インストール ディレクトリの **¥log** フォルダにあります。リモート コンポーネントのインストールの場合、ログは **%TEMP%** ディレクトリにあります。メモ帳や vi エディタなどのテキスト エディタを使用して、ファイルを開きます。

注: 完了する前にインストールをキャンセルすると、インストール ログがデスクトップ (Windows) またはルート ディレクトリ (UNIX および Linux) 上に作成されます。

第 5 章：環境設定

このセクションには、以下のトピックが含まれています。

[製品の設定 \(P. 279\)](#)

[CA SDM コンポーネントの設定 \(P. 280\)](#)

[Web インターフェースの設定方法 \(P. 284\)](#)

[CA Business Intelligence for CA SDM を実装する方法 \(P. 291\)](#)

[統合 Windows 認証を CA SDM 用に設定する方法 \(P. 314\)](#)

[自動ポリシーの実行 \(P. 319\)](#)

[ナレッジレポートカードの実行 \(P. 320\)](#)

[ナレッジマネジメント サンプルデータのインポート \(P. 321\)](#)

[検索エンジンの設定 \(P. 322\)](#)

[CA Workflow の構成方法 \(P. 324\)](#)

[CA Process Automation ワークフロー インテグレーションの設定方法 \(P. 342\)](#)

[自動ログイン \(CA MDB 認証\) のセットアップ \(P. 351\)](#)

[単一エントリ ポイントの設定 \(P. 353\)](#)

[マルチテナンシーを実装する方法 \(P. 354\)](#)

[自動フェールオーバーを有効にする方法 \(P. 400\)](#)

製品の設定

CA SDM および選択した追加製品をインストールした後、製品が正しく連携するために実行する必要がある設定手順があります。製品を設定するには、以下の手順に従います。

- CA SDM コンポーネント（サーバ、データベース、Web インターフェース）を設定します。
- Web サーバとプライマリ サーバとが異なるコンピュータ上にある場合は、Web インターフェースを設定します。
- サポート オートメーション を設定します。
- 自動ポリシーのナレッジ ドキュメント ライフサイクル レポートを実装します。

- CA Business Intelligence を設定します。
- CA Workflow を設定します。
- マルチテナンシーの実装

注: 高可用性設定のためのサーバの設定については、「高可用性にサーバを設定する方法」のシナリオを参照してください。

関連項目:

[問題管理サンプルワークフローの設定方法 \(P. 334\)](#)

[CA SDM コンポーネントの設定 \(P. 280\)](#)

[Web インターフェースの設定方法 \(P. 284\)](#)

[自動ポリシーの実行 \(P. 319\)](#)

[マルチテナンシーを実装する方法 \(P. 354\)](#)

CA SDM コンポーネントの設定

インストール中に CA SDM を設定しない場合や、インストール後に手動で製品を設定する場合は、製品を使用して、プライマリ サーバとセカンダリ サーバ、データベース、Web インターフェース、および追加の設定オプションを設定できます。

SQL Server 上で製品およびコンポーネントを正常に設定できるように、インストールと環境設定を実行するコンピュータ上で TCP/IP を有効にします。

重要: CA SDM r12.9 には、AIX 用の tools.jar および javac は含まれていません。製品の設定を実行する前に、AIX に tools.jar をインストールする必要があります。REST Web サービスおよびサポート オートメーションの設定には、tools.jar ファイルが必要です。REST サンプルファイルを使用するには、AIX に javac をインストールする必要があります。AIX 用の Java SDK は、Linux 用の IBM の Web サイトの Linux 用 IBM ディベロッパキットセクションからダウンロードできます。Java SE の 32 ビットバイナリをダウンロードし、AIX コンピュータに JDK 1.6 SR10 をインストールします。JDK がインストールされた場所から tools.jar を <Shared Component>%JRE%1.6.0_10%lib にコピーし、javac を %JRE%1.6.0_10%bin にコピーします。JRE の場所は、NX_JRE_INSTALL_DIR 変数で確認することもできます。

注: インターネットプロトコルバージョン 4 (IPv4) ホストおよびインターネットプロトコルバージョン 6 (IPv6) ホストがネットワーク上に共存している場合は、サーバの構成を始める前に、これらのテクノロジーに対応した適切な移行方針、ツール、およびメカニズムが整っていることを確認してください。サーバの構成の詳細については、「[管理ガイド](#)」を参照してください。

製品コンポーネントを設定する方法

1. [スタート] - [プログラム] - [CA] - [Service Desk] - [環境設定] を選択します。

構成ウィザードが表示されます。

2. 製品の構成情報を入力および選択します。

注: ウィザードに表示されるフィールドの詳細については、サーバ構成のオンラインヘルプを参照してください。

3. 引き続き画面の指示に従って、製品の環境設定を完了します。

環境設定を初めて実行したときに、ほとんどのインストールで使用できる TCP サービス番号のデフォルト値が表示されます。TCP サービス番号を確認するには、Windows ワークステーションからサーバに対して telnet セッションを開きます。

- ネットワークで NIS を使用している場合は、以下を入力します。

```
ypcat services | grep slump.
```

出力には、以下のような行が含まれます。

```
slump nnnn/tcp #This is required for slump to work!
```

- ネットワークで NIS を使用していない場合は、以下を入力します。

```
grep slump /etc/services.
```

出力には、以下のような行が含まれます。

```
#slump nnnn/tcp
```

[TCP サービス番号] フィールドに番号 *nnnn* を入力します。

注: 拡張テーブルの検証手順の間に設定に失敗した場合は、データベース接続が案件になる場合があります。構成を再度実行し、指定したデータベース接続情報が正しいことを確認してください。高可用性設定のためのサーバの設定については、「高可用性にサーバを設定する方法」のシナリオを参照してください。

CA CMDB 監査ログのセットアップ

CA CMDB が監査ログに使用するオブジェクトとトリガの定義、属性、および html 形式が、本製品では変更されています。

CA CMDB r12.9 監査ログをセットアップする方法

1. `site/mods/extension.mod` (*extension* は拡張名) をすでに作成している場合は、`cmdb_write_audit_log_site` トリガを削除します。

本製品のこのリリースでは、監査は自動的に作成および有効化されます。

2. ログに記録する各属性に `'UI_INFO("AUDIT_LOG")'` を追加します。
3. 本製品で提供される新しいテンプレートを使用して、既存の HTML フォームをマイグレートします。

注: 属性および HTML フォームの詳細については、「管理ガイド」を参照してください。

CA Cohesion ACM と CA CMDB の統合方法

パッチを使用して、CA Cohesion ACM と CA CMDB を統合できます。CA テクニカルサポートに連絡して、CA CMDB および CA Cohesion ACM のご使用のリリース専用のパッチを取得してください。

AIX 上の CA CMDB Visualizer 設定

IBM AIX が該当

CA SDM では、デフォルトで、すべての動作環境に CMDB Visualizer をインストールします。必要に応じて、CA CMDB Visualizer を設定できます。IBM AIX では、追加のセキュリティ ポリシー ファイルが必要になります。

IBM AIX 上で CMDB Visualizer を設定する方法

1. CMDB Visualizer が設定されていることを確認します。
2. 制約のないポリシー ファイル（バージョン 1.4.2 以上）を IBM の Web サイトの「Unrestricted JCE policy files」のページからダウンロードします。

注: ポリシー ファイルをダウンロードするには、IBM の Web サイトで登録を行ってください。

3. 共有コンポーネント JRE ディレクトリ（デフォルトの場合
所: /opt/CA/SC/JRE/1.6.0_10/lib/security）にある local_policy.jar ファイルおよび US_export_policy.jar ファイルを、IBM の Web サイトからダウンロードしたポリシー ファイルに置き換えます。

4. 以下のコマンドを使用して、Visualizer を停止して、開始します。

```
pdm_tomcat_nxd -c STOP -t VIZ  
pdm_tomcat_nxd -c START -t VIZ
```

CMDB Visualizer が IBM AIX 上に設定されます。

CA CMDB との互換性のためのサード パーティ スクリプトの変更

現在の製品リリースに含まれるスクリプトでは、ext_asset 属性の名前が、ID に変更されます。ID 属性を使用するほかの CA Technologies 製品と CA CMDB の互換性のために、CA SDM Web サービスを利用するサードパーティ スクリプトを変更して、CA CMDB 拡張テーブルを更新できます。

CA CMDB 向けにサード パーティ スクリプトを変更する方法

1. 変更するサードパーティ スクリプトを開きます。
2. ext_asset の SQL 参照をすべて ID に置き換えます。

スクリプトは、現在の製品リリースとの互換性を確保します。

CA CMDB レポートのターゲット サーバを切り替える方法

通常は、単一の CA Cohesion ACM システムが単一の CA CMDB サーバに CI データをエクスポートして、CA CMDB レポートを作成します。以下を実行することによって、CI データをエクスポートするターゲット CA CMDB サーバを切り替えることができます。

1. CI データをエクスポートするターゲットとして CA CMDB サーバを使用し、CA CMDB レポートを実行します。
2. CA Cohesion ACM サーバサービスを再起動します。
3. CI データをエクスポートする別のターゲット CA CMDB サーバに切り替え、CA CMDB レポートを実行します。
4. （オプション）手順 2 ～ 3 を繰り返します。

Web インターフェースの設定方法

CA SDM をインストールする際、Web インターフェース（一般にブラウザ インターフェースとも呼ばれます）が自動的にインストールされます。インストールの一部として Web インターフェースを設定できます。

CA SDM の設定に応じて、Web サーバを選択します。以下のユース ケースを考えてください。

- **標準**：Web サーバとプライマリ サーバが同じコンピュータ上に存在する場合は、追加のアクションは必要ありません。ただし、Web サーバを使用しており、プライマリ サーバが別のコンピュータ上にインストールされている場合は、プライマリ サーバとセカンダリ サーバの両方をインストールおよび設定します。
- **高可用性**：Web サーバとバックグラウンド サーバが同じコンピュータ上に存在する場合は、追加のアクションは必要ありません。ただし、Web サーバを使用しており、バックグラウンド サーバが別のコンピュータ上にインストールされている場合は、バックグラウンド サーバとアプリケーション サーバの両方をインストールおよび設定します。エンドユーザの Web インターフェースがバックグラウンド サーバからホストされることはありません。Web インターフェースは、アプリケーション サーバ上でのみホストする必要があります。

CA SDM の設定に応じて、Web サーバが存在し、かつ Web インターフェースのインストールおよび設定を計画しているコンピュータを以下の CA SDM サーバから選択します。

- 標準：セカンダリ サーバプライマリ サーバのインストール後に、このサーバをインストールします。
- 高可用性：アプリケーション サーバ。バックグラウンドサーバのインストール後に、このサーバをインストールします。

重要：デフォルトでは、Tomcat がデフォルトの Web サーバです。Web サーバとして IIS を使用する場合は、手動で製品を設定し、IIS を選択します。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。

Web インターフェースを設定するには、以下の手順に従います。

1. （必須）Windows または UNIX のセカンダリ サーバ上の Web エンジン を有効にします。
2. （必須）[Web インターフェースを設定](#) (P. 289) します。

[Web インターフェースを開始](#) (P. 290) します。

関連項目：

[Web インターフェースの開始](#) (P. 290)

[Web インターフェースの設定](#) (P. 289)

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 エンジンを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。

Web インターフェースの設定

CA SDM のインストール時に **Web** インターフェース用に指定されたデフォルト設定が要件を満たさない場合は、*installation-directory¥bopcfg¥www* ディレクトリにある **web.cfg** ファイルを修正します。メモ帳やワードパッドなど、フォーマットまたは制御文字を追加しないテキスト エディタを使用して、ファイルを編集します。

ファイルの各エントリは、プロパティ名が含まれた 1 行の文字列で構成されます。オプションでその後に値が含まれることがあります。ポンド記号 (#) で始まる行はコメント行として扱われ、無視されます。

注: **web.cfg** ファイル内のエントリの詳細については、「管理ガイド」を参照してください。

Web インターフェースの開始

Web インターフェースを開始し、CA SDM 使用するには、デーモン サーバ サービスとデータベース サーバが起動していることを確認する必要があります。セカンダリ サーバを構成した場合（プライマリ サーバとは異なるコンピュータに常駐する Web サーバに Web インターフェースをインストールした場合など）、プライマリ サーバ サービスを開始する前に Remote Daemon Proctor サービスを実行している必要があります。

- (Windows) サービスを開始するには、[コントロール パネル]（[管理ツール]-[サービス]）を開きます。次に、[CA SDM Remote Daemon Proctor] を右クリックし、[開始] を選択します。
- (Linux) サービスを開始するには、コマンドプロンプトを開き、`pdm_client` コマンドを実行します。

サービスを開始した後、Web インターフェースを開始できます。Web インターフェースを開始する方法は、Web インターフェースを開始するコンピュータがプライマリ サーバかセカンダリ サーバか、IIS を使用しているかどうかによって異なります。また、内部 Web サイトから Web インターフェースを開始することもできます。

- Web インターフェースを開始するには、[スタート] - [プログラム] - [CA] - [Service Desk Manager] - [Service Desk Manager Web Client] を選択します。
- プライマリ サーバでないコンピュータまたはセカンダリ サーバから Web インターフェースを開始するには、Web ブラウザを開き、以下の URL を入力します。

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

この URL 中の *servername* は CA SDM Web サーバをホストしているコンピュータの名前です。

- プライマリ サーバでないコンピュータまたはセカンダリ サーバから Web インターフェースを開始する場合、Web サーバとして IIS を使用している場合は、Web ブラウザを開き、以下の URL を入力します。

`http://servername/CAisd/pdmweb.exe`

- 内部 Web サイトから Web インターフェースにアクセスするには、Web ページの URL に `/pdmweb.exe` を追加します。ガイドとして、以下の HTML コード例を参考にしてください。

A HREF=`http://<server-name>:<port-no>/CAisd/pdmweb.exe`

この URL 中の *server-name* はコンピュータ名を、*port-no* は Web サーバがリスニングに使用しているポートを指します。

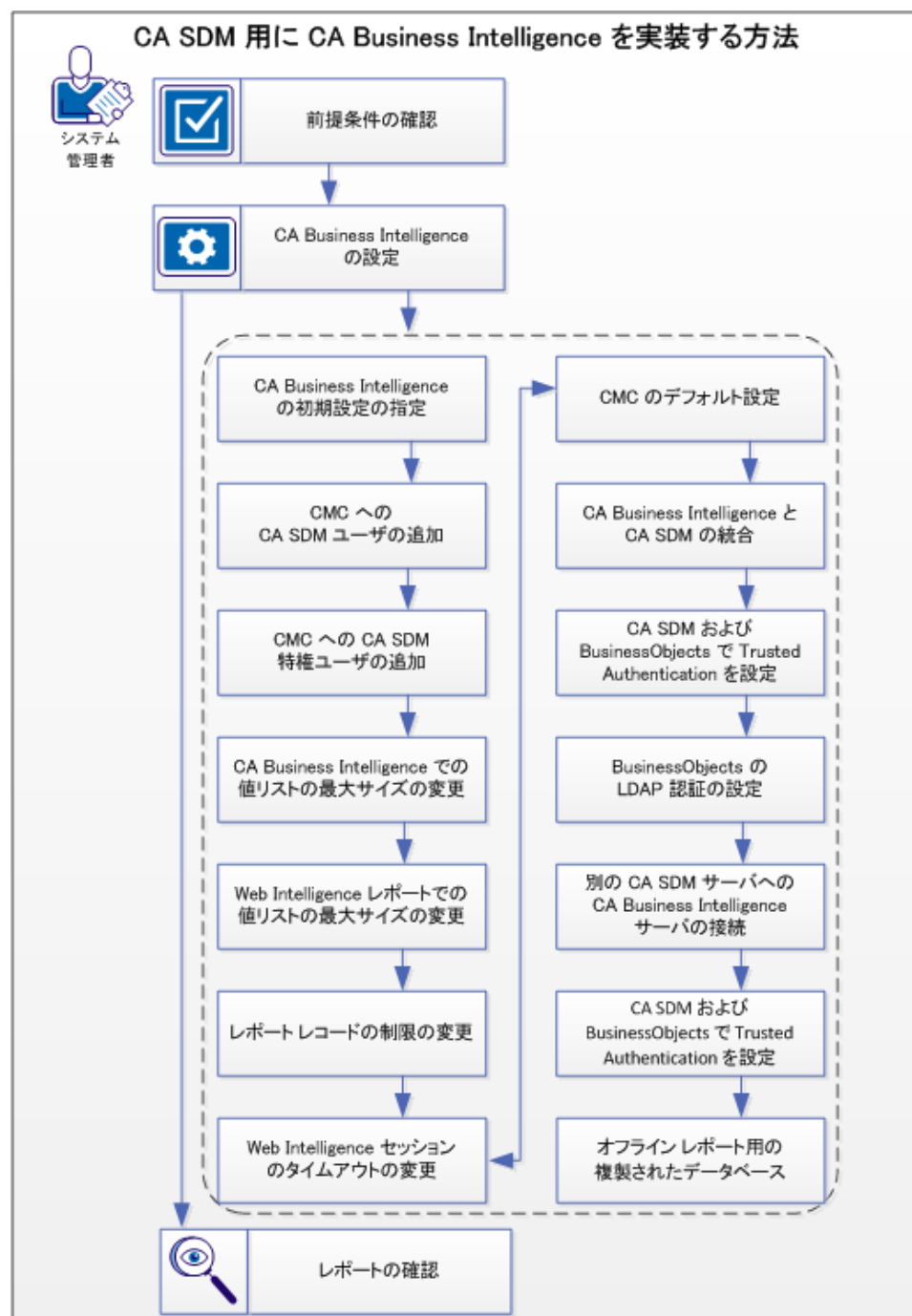
注: Internet Explorer ブラウザのセキュリティが「高」に設定されている場合、Web インターフェースを開始すると、コンテンツに関する警告メッセージが表示されます。このメッセージを回避するには、Web サイトを信頼済みサイトに追加するか、セキュリティのレベルを下げます。

高可用性では、デフォルトのインストールおよび設定でデフォルトの Web インターフェースがすぐに使用できます。

CA Business Intelligence for CA SDM を実装する方法

CA Business Intelligence は、CA SDM が情報を提供したり、経営上の意思決定をサポートしたりするために使用する一連のレポートおよび分析ソフトウェアです。CA SDM は、CA Business Intelligence を使用して統合および分析を行い、さまざまなレポート オプションを通して情報を提供します。CA SDM からレポートを生成するには、管理者は CA Business Intelligence をインストールおよび設定して CA SDM と統合する必要があります。

以下の図は、CA Business Intelligence for CA SDM を実装する方法を示しています。



次の手順に従ってください:

1. [レポートに関する考慮事項を確認します。](#) (P. 293)
2. [CA Business Intelligence を設定します。](#) (P. 293)
3. [レポートを確認します。](#) (P. 313)

前提条件の確認

CA Business Intelligence for CA SDM の実装を計画する前に、以下の考慮事項を確認します。

- CA SDM r12.9 は CA Business Intelligence バージョン 3.3 を使用します。
- CA Business Intelligence をインストールするには、Central Management Server (CMS) がポート 6400 上にインストールされていることが必要です。
- レポートを使用する前に、レポートへのアクセスが必要な CA SDM ユーザを CMS 管理者のリストに追加する必要があります。
- BusinessObjects の既存のインストールを所有している SAP BusinessObjects ユーザが CA Business Intelligence をインストールおよび設定することをお勧めします。
- Firefox を使用してレポートを表示する場合は、「CA SDM リリース ノート」を参照して推奨されるバージョンを確認してください。
- JRE のサポートされるバージョンについては、「CA SDM リリース ノート」を参照してください。
- CA SDM では、Crystal Reports エクスプローラおよび Desktop Intelligence はサポートされていません。
- 高可用性設定を使用している場合は、CA Business Intelligence をインストールするための別のサーバがあります。

CA Business Intelligence の設定

インストールが成功したら、CA Business Intelligence を設定できます。CA SDM からレポートを生成できるようにするには、必須の設定を実行します。CA Business Intelligence を CA SDM と統合する前に、ユーザの追加やセキュリティ パラメータの設定などの必須の設定がいくつか必要です。

次の手順に従ってください:

1. CA Business Intelligence の設定を行います。
2. データ範囲の値および結合パラメータを設定します。
3. CA SDM のユーザおよびグループを追加します。
4. デフォルトの CA SDM 特権ユーザ アカウントを追加します。
5. デフォルトのセキュリティおよび Web Intelligence 設定を変更します。
6. CA Business Intelligence を CA SDM に統合します。
7. BusinessObjects および CA SDM 用の信用できる認証を設定します。
8. (オプション) BusinessObjects の LDAP 認証を設定します。
9. (標準設定にのみ適用可能) CA Business Intelligence サーバを別の CA SDM サーバに接続します。
10. 値のリストの最大サイズを変更します。
11. Web Intelligence セッションのタイムアウト値を変更します。

CA Business Intelligence の初期設定の指定

この手順によって、CA SDM ユニバースおよびレポートのロード、グループの作成、オプションで、グループごとに 1 人のユーザの作成、グループの権限の確立が実行されます。

次の手順に従ってください:

1. CA Business Intelligence サーバ上のドライブにインストール メディア DVD 2 を挿入します。インストール メニューが自動的に表示されない場合は、インストール メディアのルートにある **setup.exe** ファイルをダブルクリックしてインストールを開始します。

注: インストール メディアを使用できる適切なドライブがコンピュータにない場合は、CA Business Intelligence をインストールするコンピュータにメディアの内容をコピーします。その後、構成を開始します。ネットワーク経由のリモート設定の場合は、ネットワーク上でドライブかフォルダを共有してから、ネットワーク経由で接続し、設定を開始できます。

2. リストから言語を選択し、[言語の選択] をクリックします。
[インストール メニュー] が表示されます。
3. [製品のインストール] タブをクリックします。
4. [CA Business Intelligence 環境設定] をクリックします。
5. [CA Business Intelligence 環境設定] で以下のフィールドに入力します。

BI 管理者ユーザ名

管理者グループに属する CA Business Intelligence ユーザのユーザ名を指定します。ユーザ名は、新しくインストールされる CA Business Intelligence インストールの管理者です。

BI 管理者パスワード

CA Business Intelligence 管理ユーザのパスワードを指定します。

Service Desk 管理者ユーザ名

CA SDM 管理者のユーザ名を指定します。

Service Desk 管理者パスワード

CA SDM の特権ユーザのパスワードを指定します。

デフォルト ユーザの作成

CA Business Intelligence でデフォルト グループおよび対応するユーザを作成します。

CA SDM とは別のコンピュータに CA Business Intelligence をインストールした場合は、[CA Business Intelligence 環境設定] に以下のフィールドが表示されます。

Service Desk プライマリ ホスト

設定に応じて、CA SDM サーバのホスト名を入力します。

- 標準：プライマリ サーバ。
- 高可用性：アプリケーション サーバ。

ODBC ポート

CA SDM ODBC ドライバのポート番号を指定します。

推奨：19987。

ODBC インストール場所

ODBC のインストールのカスタムの場所がデフォルトの場所と異なる場合は、カスタムの場所を指定します。

6. CA Business Intelligence 環境設定を確認します。

フェールオーバー設定の実行

このプロセスは、高可用性設定にのみ適用できます。複数のアプリケーションサーバが設定されている場合は、フェールオーバーの設定を行うことができます。アクティブなユーザセッションをほかのアプリケーションサーバにリダイレクトするようにフェールオーバーを設定します。また、複数のアプリケーションサーバ間の負荷分散を設定することもできます。

次の手順に従ってください：

1. 管理者としてコマンドプロンプトを呼び出します。
2. CA Business Intelligence サーバ上で、`C:\¥Windows¥SysWOW64` から `odbcad32.exe` を実行します。

[DataDirect OpenAccess SDK ODBC Driver Setup] ダイアログボックスが表示されます。

注：指定されたパスは、Windows 64 ビット インストールに対して有効です。
3. [General] タブで、アプリケーションサーバの詳細を入力します。
4. [Failover] タブで、代替アプリケーションサーバの詳細を以下の構文で入力します。

(Host=AppServer1:Port=19987,Host=AppServer2:Port=19987,...)
5. 負荷をサーバ間で分散させるための [Load Balancing] を選択します。負荷は、[General] タブで詳細が指定されているサーバおよび [Failover] タブで詳細が指定されているサーバ間で分散されます。サーバはランダムに選択されます。

注：フェールオーバーまたは負荷分散の設定には [Force SQL_DRIVER_NOPROMPT] を選択します。
6. [Apply] をクリックし、[OK] をクリックします。

高可用性設定の設定後の設定が完了します。

日付範囲の値および結合パラメータの設定方法

CA Business Intelligence をインストールしたら、以下のタスクを実行します。

- CA Business Intelligence の日付範囲フィルタが正しく機能するように、日付範囲の値を設定する。
- ユニバースの外部結合がサポートされるように、結合パラメータを設定する。

次の手順に従ってください：

1. CA Business Intelligence がインストールされたコンピュータで、以下の場所に移動します。

```
C:\Program Files\CA\SC\CommonReporting3\BusinessObjects Enterprise
12.0\win32_x86\dataAccess\connectionServer\odbc\
```

2. テキスト エディタを使用して、odbc.prm ファイルを開き、<Configuration> セクションに移動して、日付範囲の値を設定するための行を探します。

```
<Parameter Name="USER_INPUT_DATE_FORMAT">{%d 'yyyy-mm-dd'}</Parameter>
```

3. 以下のように、この行に「hh:mm:ss am/pm」を追加します。

```
<Parameter Name="USER_INPUT_DATE_FORMAT">{%d 'yyyy-mm-dd hh:mm:ss
am/pm'}</Parameter>
```

4. 結合パラメータを設定するために、以下の行を探します。

```
<Parameter Name="EXT_JOIN">NO </Parameter>
```

5. 以下のように、この行の「NO」を「YES」に置き換えます。

```
<Parameter Name="EXT_JOIN">YES</Parameter>
```

6. 以下の行を探します。

```
<Parameter Name="OUTERJOINS_GENERATION">NO</Parameter>
```

7. 以下のように、この行の「NO」を「FULL_ODBC」に置き換えます。

```
<Parameter Name="OUTERJOINS_GENERATION">FULL_ODBC</Parameter>
```

8. OUTERJOINS_GENERATION パラメータの後に以下の 3 行を追加します。

```
<Parameter Name="LEFT_OUTER"></Parameter> <Parameter  
Name="RIGHT_OUTER"></Parameter> <Parameter  
Name="OUTERJOINS_COMPLEX">Y</Parameter>
```

9. odbcd.prm ファイルを保存します。
10. Business Objects Enterprise サービスを再起動します。

日付範囲の値および結合パラメータが設定されます。CA Business Intelligence で日付範囲フィルタが機能し、ユニバースの外部結合がサポートされるようになります。

CMC への CA SDM ユーザの追加

CMC は、InfoView およびほかの BusinessObjects アプリケーションへのユーザのアクセスを制御できる管理ユーティリティです。CMC を使用すると、フォルダおよびドキュメントにセキュリティおよびユーザアクセス権限を割り当てることができます。

注: 構成フェーズ中、オプションのチェック ボックスを使用して、CMC にサンプルユーザを追加するかどうかを指定します。このオプションをオンにした場合、CMC にいくつかのサンプルユーザが追加されます。レポート環境にユーザ権限と認証のオプションを定義するときに、これらのサンプルをモデルとして使用できます。サンプルユーザの詳細については、「*管理者ガイド*」を参照してください。

次の手順に従ってください:

1. CA Business Intelligence サーバの [スタート] メニューで、
[BusinessObjects XI Release 3.1] - [BusinessObjects Enterprise] -
[BusinessObjects Enterprise Central Management Console] を選択します。
[CMC Management Console] ページが開きます。
2. 特権ユーザの名前とパスワードを入力します。
3. [認証] リストで [Enterprise] を選択します。
4. [ログオン] をクリックします。
CMC のホーム ページが開きます。
5. CMC ホーム ページの [整理] セクションで [ユーザーとグループ] を
クリックします。

6. [管理] - [新規] - [新しいユーザー] をクリックします。
[新しいユーザー] ダイアログ ボックスが表示されます。
7. [認証の種類] リストで [Enterprise] を選択します。
8. [アカウント名] で、CA SDM ユーザ ID を指定します。
9. [プロパティ] タブで、以下のようにパスワード情報と設定を指定します。

パスワード

パスワードを入力し、確認のためにもう一度入力します。このパスワードは、CA SDM ユーザのパスワードと同一である必要があります。パスワードの長さは最大で 64 文字です。

このパスワードは大文字小文字混在の 6 文字以上の文字列である必要があります、どのような形式でも **administrator** という単語を含めることはできません。また、以下の文字の種類のうち 2 つ以上を含める必要があります。

- 大文字
- 小文字
- 数値
- 句読点

パスワードを無期限にする

チェック ボックスをオンにします。

ユーザーは次回ログオン時にパスワード変更が必要

このチェック ボックスはデフォルトでオンになっています。ユーザーに対して初回ログオン時にパスワードの変更を強制しない場合は、チェック ボックスをオフにします。

10. データ パーティションまたはテナンシー制約を使用してレポートのデータ アクセスを制限するには、[データベース認証を有効にする] チェック ボックスをオンにします。表示されたフィールドで、ユーザーの CA SDM アカウント名とパスワードを指定し、確認のためにもう一度パスワードを入力します。

11. [アクション] - [所属するグループ] をクリックして、ユーザが属する必要のあるグループを指定します。
12. [グループに追加] をクリックして、使用可能なグループを表示します。デフォルトでは、このユーザは [Everyone] グループのメンバーになります。
13. [利用可能なグループ] 領域で、追加するグループを 1 つ以上選択します。
14. [>] 矢印をクリックしてグループを追加します。
15. [OK] をクリックします。

[所属するグループ] ダイアログボックスが表示され、ユーザがメンバーとして属するグループがリストされます。

注: ユーザとグループを追加してデータ パーティションセキュリティを構成する方法の詳細については、「[管理ガイド](#)」を参照してください。

CMC への CA SDM 特権ユーザの追加

CA SDM ユニバース接続は、データへのアクセス時に CA SDM の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。このユーザアカウントを新規の CA Business Intelligence ユーザとして CMC に追加されます。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し、[レポート] タブからレポートをテストする場合に、このユーザを使用する必要があります。[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。

次の手順に従ってください:

1. CMC の [ユーザーとグループ] 管理エリアをクリックします。
2. [アカウント名] で、CA SDM の特権ユーザアカウントを選択します。
3. [プロパティ] タブで、パスワード情報を指定します。
4. [データベース認証を有効にする] チェック ボックスをオンにします。表示されたフィールドで、特権ユーザのアカウント名とパスワードを指定し、確認のためにもう一度パスワードを入力します。
5. [所属するグループ] タブをクリックして、特権ユーザが属するグループを指定します。
6. [グループに追加] ボタンをクリックして、使用可能なグループを表示します。

7. [利用可能なグループ] 領域で、[Administrators] および [CA Universe Developer] を選択します。
8. [>] 矢印をクリックしてこれらのグループを追加します。
9. [OK] をクリックします。
[所属するグループ] タブが表示され、ユーザがメンバーとして属するグループがリストされます。

CA Business Intelligence での値リストの最大サイズの変更

CA Business Intelligence をインストールすると、Crystal Reports の値リストに対してデータベースから 1 回で返される値の最大数が自動的に 5,000 レコードに設定されます。パフォーマンス向上のために、サイズをこれより小さく変更し、値のリストが数回に分けてユーザに返されるようにすることができます。

注: Web Intelligence レポート サーバのパフォーマンス向上の詳細については、BusinessObjects のドキュメントを参照してください。

次の手順に従ってください:

1. 以下のレジストリ キーを作成します。

```
HKEY_CURRENT_USER\SOFTWARE\Business Objects\Suite  
12.0\CrystalReports\DatabaseOptions\LOV
```

注: 作成されたレジストリ キーにより、

```
HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite  
12.0\CrystalReports\DatabaseOptions\LOV
```

レジストリ キーの設定がオーバーライドされます。

2. 文字列値として MaxRowsetRecords を追加します。

3. **MaxRowsetRecords** の値を、レポートに必要な値の最大数に設定します。たとえば、**2000** に設定した場合、パラメータの最低レベルで **2000** 個の値が返されます。

注: ゼロ（無制限）の値は、**BusinessObjects Enterprise** または **Crystal Reports Server** では無効です。**Crystal Report** が **InfoView** からアクセスされる場合は常に、値がゼロに設定されている（つまり最大の値リスト）場合、値を入力するためにより長い時間が必要です。

4. 必要に応じて、影響を受けるサービスまたはアプリケーションを再起動します。

注: レポートがユニバースに基づいている場合、これらのレジストリ キーは返される値リストに影響を与えません。

Web Intelligence レポートでの値リストの最大サイズの変更

CA Business Intelligence をインストールすると、**Web Intelligence** レポートの値リストに対してデータベースから 1 回で返される値の最大数が自動的に **5,000** レコードに設定されます。パフォーマンス向上のために、サイズをこれより小さく変更し、値のリストが数回に分けてユーザに返されるようにすることができます。

注: **Web Intelligence** レポート サーバのパフォーマンス向上の詳細については、**BusinessObjects** のドキュメントを参照してください。

次の手順に従ってください:

1. **Central Management Console** にログインします。
2. [サーバー] をクリックします。
3. [WebIntelligenceProcessingServer] を右クリックし、[プロパティ] を選択します。
4. [値の一覧の最大サイズ (エントリ)] の値を増やします。
5. **Web Intelligence Processing Server** を保存して再起動します。

注: [値の一覧の最大サイズ (エントリ)] の値を大きくすると、**Web Intelligence** のパフォーマンスが低下する可能性があります。システムパフォーマンスに応じて適切な値を設定してください。

レポートレコードの制限の変更

CA Business Intelligence をインストールすると、ユーザが Crystal Reports でクエリまたはレポートを実行したときにサーバがデータベースから取得するレコードの数が自動的に 20,000 レコードに設定されます。この設定を変更して、レポートを実行したときにユーザの期待どおりのレコードセットが返されるようにできます。

注: Crystal Reports Page Server に対して実行できる管理タスクの詳細については、BusinessObjects のドキュメントを参照してください。

次の手順に従ってください:

1. BusinessObjects Enterprise を使用して、Central Management Console にログインします。
2. サーバが表示されるページに移動します。
3. [Crystal Reports Page Server] をクリックします。
4. [プロパティ] タブで、[プレビューまたは最新表示時に読み取るデータベース レコード数] フィールドの設定を無制限のレコードに変更するか、特定のレコード制限を指定します。
5. [保存] をクリックします。
6. Crystal Report Page Server を再起動します。

レポート レコードの制限が変更され、レポートを実行する際に使用されます。

Web Intelligence セッションのタイムアウトの変更

ユーザは、デフォルトで Web Intelligence アプリケーションに対してフルコントロールのアクセス権を持っています。

Web Intelligence アプリケーションのセッションは、デフォルトで 20 分でタイムアウトします。セッションがタイムアウトすると未保存のレポートは失われ、ユーザがアプリケーションを使用するにはログオンし直す必要があります。

管理者は、**Central Management Console (CMC)** を使用して、接続セッションのタイムアウト値を変更できます。

次の手順に従ってください:

1. **CMC** のホーム ページで [サーバー] を選択します。
[サーバー] ウィンドウが開きます。
2. [サーバー名] 列で [Web_IntelligenceReportServer] を選択します。
3. [アイドル接続タイムアウト] フィールドに適切なタイムアウト値(分数)を入力します。
4. [保存] をクリックします。
サーバが再起動された後、変更が適用されます。
5. [OK] をクリックします
セッションのタイムアウト値が設定されます。

CMC のデフォルト設定

ほとんどのレポート設定は、**CA Business Intelligence** インストール中に自動的に実行されます。レポート設定には、以下のアクションが含まれます。

- 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
- プログラム オブジェクトの展開
- **Web Intelligence** 設定の構成

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。ユーザのアクセス権は、各ユーザが属する **CA SDM** グループに基づいて決まります。

注: **BusinessObjects CMC** の詳細については、「*CA Business Intelligence 実装ガイド*」を参照してください。

CA Business Intelligence と CA SDM の統合

CA Business Intelligence をインストールした後、CA SDM が CA Business Intelligence と正常に統合されるように、Web レポート オプションを更新します。

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] - [Web レポート] を選択します。

[オプション リスト] が表示されます。

2. 以下の Web レポート オプションに正しい値を設定します。

bo_server_auth

レポートに使用する認証の種類を指定します。以下の種類の認証を指定できます。

- secEnterprise - (デフォルト) BusinessObjects で別個のアカウントおよびグループを作成してそれらを CA Business Intelligence で使用する場合、または Windows NT ユーザ データベース、LDAP サーバ、または Windows AD サーバでユーザ階層が設定されていない場合は、認証の種類としてエンタープライズ認証を指定します。

注: secEnterprise オプションを指定する前に、[CA SDM レポート ユーザを BusinessObjects Central Management Console \(CMC\) に追加](#) (P. 298)します。CMC で、CA SDM で構成した名前およびパスワードと同じ内容を入力します。

- secLDAP - すでに LDAP ディレクトリ サーバを設定済みで、BusinessObjects の LDAP ユーザ アカウントおよびグループを CA Business Intelligence で使用する場合は、認証の種類として LDAP 認証を指定します。

LDAP アカウントを BusinessObjects にマップすると、ユーザは CA Business Intelligence に LDAP ユーザ名とパスワードでアクセスできるようになります。これにより、BusinessObjects 内で個々のユーザおよびグループ アカウントを再作成する必要がなくなります。

- **secWinAD** - Windows 2000 環境を使用しており、BusinessObjects の既存のアクティブ ディレクトリ ユーザ アカウントおよびグループを CA Business Intelligence で使用する場合は、認証の種類として Windows AD 認証を指定します。
- **secExternal** - BusinessObjects 認証ソリューションをサードパーティ認証ソリューションとインテグレートする場合（たとえば、JCIFS と Tomcat を使用）、認証の種類として外部認証を使用します。この認証の種類を使用するには、ユーザがパスワード入力なしでログオンできるように BusinessObjects で信用できる認証を設定する必要があります。

注: 代替のセキュリティ オプションの詳細については、「*CA Business Intelligence 実装ガイド*」を参照してください。

bo_server_cms

CA Business Intelligence で使用する BusinessObjects の情報データベースを管理する、Central Management Server (CMS) の名前を指定します。

bo_hostname には、CA Business Intelligence がインストールされているコンピュータのホスト名を使用します。デフォルトの **bo_cms_port** は 6400 です。

注: 高度なサーバ構成オプションの詳細については、「*CA Business Intelligence インストールガイド*」を参照してください。

bo_server_location

CA Business Intelligence がインストールされているコンピュータのホスト名を指定します。 **bo_hostname** を指定します。 CA SDM は、BusinessObjects サーバからレポートを要求するためのレポート URL 用にこの URL を使用します。 CMS の場所は、ホスト名およびポートで指定します。

注: 各オプションの詳細については、「*CA Business Intelligence 実装ガイド*」を参照してください。

3. [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。
4. [ウィンドウを閉じる] をクリックします。
5. CA SDM Server という名前のサービスを停止して開始します。
Web レポートの設定が正しく構成され、CA SDM で使用できるようになります。これで Web ベースのレポートを設定できます。
注: Web ベースのレポートのセットアップについては、「管理ガイド」を参照してください。

CA SDM および BusinessObjects で信用できる認証を設定する方法

信用できる認証では、CA SDM と CA Business Intelligence を統合する際にシングルサインオンのシンプルなフォームを使用することができます。シングルサインオンでは、ユーザはセッションにログオンする際、パスワードを 1 回入力するだけで済みます。

次の手順に従ってください：

1. CA SDM をインストールして構成します。
2. CA Business Intelligence をインストールして構成します。
3. 管理者として CMC にログインします。
4. 信用できる認証をセットアップするために、Central Management Console (CMC) にアクセスします。
5. CA SDM 連絡先および BusinessObject ユーザを作成します。
6. CA SDM Web レポート オプションをインストールして `bo_server_auth` オプションを [エンタープライズ] に設定します。
注: `bo_server_auth` 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。
7. BusinessObjects Apache Tomcat を循環させます。
8. CA SDM サーバを Windows サービス内で循環させます。

CA Business Intelligence での信用できる認証の設定

CA Business Intelligence に信用できる認証を設定するには、最初に **web.xml** ファイルを編集する必要があります。

次の手順に従ってください：

1. 管理者として **CMC** にログインし、[認証] 管理領域に移動します。
[Enterprise] ページが表示されます。
2. ページの下部にある [信用できる認証を有効にする] オプションを選択し、[共有シークレット] フィールドにテキスト文字列を指定します。

注：共有シークレットは、信用できる認証パスワードの作成に使用されます。

3. 信用できる認証のリクエストのタイムアウト値を入力します。

注：タイムアウト値によって、**CMS** がクライアント アプリケーションからの **IEnterpriseSession.logon()** コールを待つ時間が決まります。

4. [更新] をクリックします。

信用できる認証が設定されました。

CA SDM に信用できる認証を設定する

CA SDM に信用できる認証を設定するには、TrustedPrincipal.conf ファイルを編集する必要があります。

次の手順に従ってください：

1. 以下のディレクトリにある TrustedPrincipal.conf ファイルを開きます。
NX_ROOT¥bopcfg¥www¥CATALINA_BASE¥webapps¥CAisd
2. この行
SharedSecret=<CMC に入力した共有シークレット>
を編集して以下を反映します。
SharedSecret=xxxx
(ここで、xxxx は手順 3 で CMC に入力した共有シークレットです)
3. [保存] をクリックします。
4. 設定するすべてのアプリケーション サーバに対して、手順 1～3 を繰り返します。
5. CA Business Intelligence Tomcat サーバをリサイクルします。
CA SDM に信用できる認証が設定されました。

注: バックグラウンドサーバの URL からレポートを起動するには、CA SDM バックグラウンドサーバで信用できる認証を設定する必要があります。

BusinessObjects の LDAP 認証の設定

LDAP 認証を設定するときには、LDAP サーバの管理クレデンシャル「cn」の値を完全修飾名（名、姓）にする必要があります。LDAP 認証を設定すると、ユーザのログイン名を使用するように LDAP 属性を再マップできるようになります。

重要: LDAP 認証を設定する場合、BusinessObjects のユーザ アカウント名は、CA SDM 連絡先のユーザ ID と一致する必要があります。

次の手順に従ってください：

1. Central Management Console (CMC) の [認証] 管理領域にアクセスします。
2. [LDAP] をダブルクリックします。

3. [LDAP ホストの追加 (ホスト名:ポート)] フィールドに、LDAP ホストの名前とポート番号を入力します。たとえば、「myserver:123」と入力します。
4. [追加] をクリックして、[OK] をクリックします。
5. [LDAP サーバーの種類] リストからサーバタイプとして [カスタム] を選択します。
6. CMS 構成ウィザードの指示に従って設定を完了します。
BusinessObjects LDAP 認証が設定されます。

注: LDAP 認証の設定方法の詳細については、CMS オンライン ヘルプおよび「*BusinessObjects Enterprise Administrator's Guide*」を参照してください。

別の CA SDM サーバへの CA Business Intelligence サーバの接続

これは、別のサーバにインストールされている CA SDM の別のインスタンスからレポートを生成するために必要です。

次の手順に従ってください：

1. [CA SDM サーバの ODBC DSN を作成します](#) (P. 310)。
2. [この CA SDM サーバに CA SDM ユニバースを接続します](#) (P. 311)。

CA SDM サーバ用の ODBC DSN の作成

ODBC DSN を作成するには、ODBC データ ソース アドミニストレータを使用します。

次の手順に従ってください：

1. Windows の ODBC データ ソース アドミニストレータ（[データ ソース (ODBC)]）を開始します。
2. [ODBC データ ソース アドミニストレータ] フォームで、[システム DSN] タブを選択し、[追加] を選択します。
3. [データ ソースの新規作成] フォームで、[DataDirect OpenAccess] ドライバを選択し、[完了] を選択します。
4. [DataDirect OpenAccess ODBC 32 Setup] フォームで、ODBC 名を割り当てて、[Advanced] を選択します。

使用する命名規則は casd_hostname です。たとえば、CA SDM サーバのホスト名が MyServer の場合、casd_MyServer を使用します。

5. [OpenAccess Database Configuration] フォームで、[Add] を選択します。
6. [OpenAccess Database Setup] フォームで、以下の情報を入力します。
 - Name - casd_hostname を指定します。
 - IP Address - CA SDM サーバの IP アドレスを指定します。
 - Port - 19987 を指定します。
 - Type - [SQL] を選択します。
7. [OK] をクリックします。
8. [Open Access Database Configuration] フォームで、[OK] を選択します。
9. [DataDirect OpenAccess ODBC 32 Setup] フォームで、[Database] ドロップダウンから [casd_hostname] を選択し、[OK] を選択します。
ODBC DSN が作成されました。

サーバへの CA SDM ユニバースの接続

接続を確立するために、BusinessObjects Enterprise の Designer を使用します。

次の手順に従ってください：

1. [スタート] メニューから [BusinessObjects XI Release 3.1] - [BusinessObjects Enterprise] - [Designer] を参照します。
2. 以下のクレデンシャルを指定して Designer にログインします。
 - System - CA Business Intelligence がインストールされているサーバのホスト名を指定します。
 - User name - CA Business Intelligence 管理ユーザ（通常は Administrator）の名前を指定します。
 - Password - CA Business Intelligence 管理ユーザのパスワードを指定します。
 - Authentication - [Enterprise] を選択します。[Designer] ウィンドウが表示されます。

3. [File] - [Import] をクリックします。
[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 Universes] フォルダを選択し、CA SDM ユニバースを選択して [OK] を選択します。

注: Designer の使用が今回初めての場合は、最初に [Browse] を選択して [CA Universes] フォルダを選択する必要があることがあります。
5. [Universe successfully imported] メッセージで [OK] をクリックします。
[Universe] ウィンドウが表示されます。
6. [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。
7. [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。
8. [Edit] を選択します。
9. [Data source name] ドロップダウン リストから作成した ODBC DSN (casd_hostname) を選択し、[User name] と [Password] に CA SDM の特権ユーザとパスワードを指定します。
10. [Next] - [Test Connection] をクリックし、表示される [Universe Connection] ダイアログ ボックスの手順に従って操作します。
11. [OK] をクリックして操作を完了します。
12. [File] - [Export] 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. [Domain] ドロップダウン リストから [CA Universes] を選択します。
14. [Groups] リストから [Everyone] を選択します。
15. [OK] をクリックします。
ユニバースがエクスポートされてサーバへの接続が確立されます。

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。

レポートの確認

レポートが問題なく確実に生成されるようにするために、CA Business Intelligence の設定を確認します。

次の手順に従ってください：

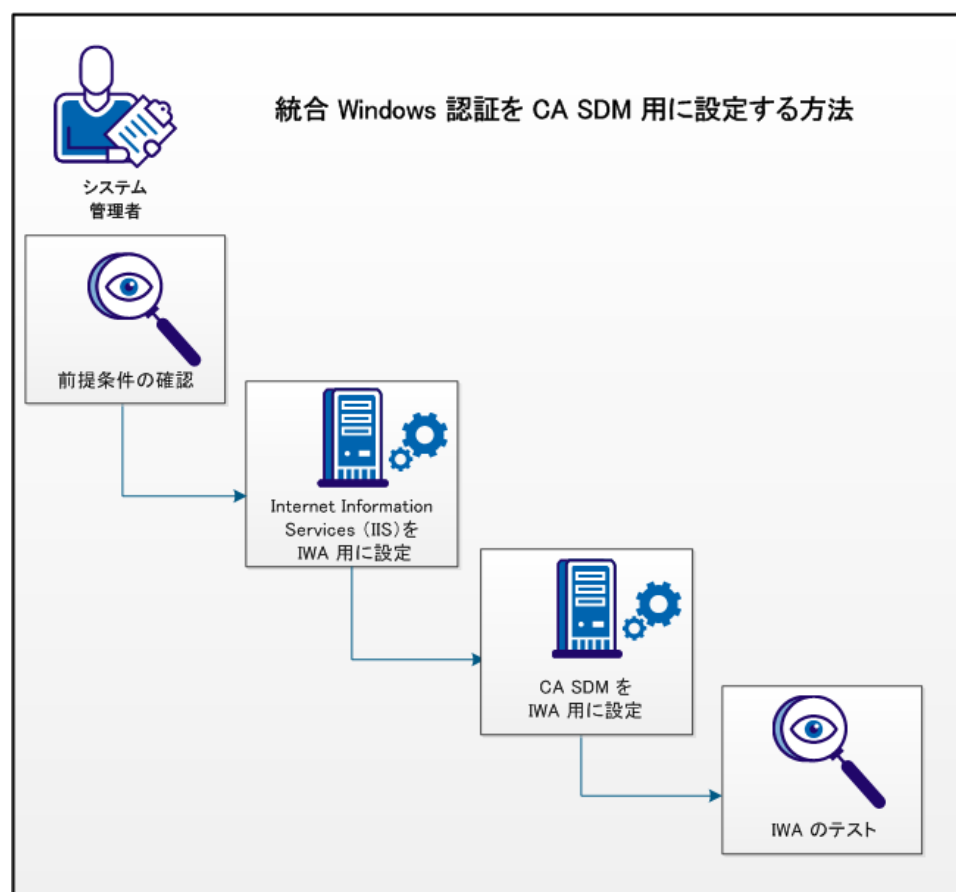
1. [レポート] タブをクリックします。
[Web レポート] ページが開きます。
2. [InfoView] をクリックします。
Business Objects InfoView ウィンドウが開きます。
3. [ドキュメントリスト] リンクをクリックします。
4. [パブリック フォルダ] - [CA Reports] - [CA Service Desk] を展開します。
5. 左側のペインで、[アセット] フォルダを選択します。
6. [アセット リスト] レポートをダブルクリックします。

レポートでは、0 件以上の検索結果が返されます。CA Business Intelligence が CA SDM 用に設定されます。

統合 Windows 認証を CA SDM 用に設定する方法

システム管理者は、既存の外部認証方法を通して CA SDM ユーザを認証できます。このシナリオでは、統合 Windows 認証 (IWA) を使用して Microsoft Active Directory (AD) を介して CA SDM ユーザを認証するプロセスについて説明します。IWA を使用する管理者などの CA SDM アクセス タイプを設定すると、選択されたアクセス タイプのユーザは AD を介して直接認証されます。

以下の図は、IWA を CA SDM 用に設定する方法を示しています。



IWA を CA SDM 用に設定するには、以下のタスクを完了します。

1. [前提条件の確認](#) (P. 315)
2. [Internet Information Services \(IIS\) を IWA 用に設定します。](#) (P. 316)
3. [CA SDM を IWA 用に設定します。](#) (P. 317)

4. [IWA のテスト](#) (P. 317)

前提条件の確認

外部認証を CA SDM 用に設定する前に、以下の要件を確認します。

- サーバが CA SDM 用に設定されている。
- 設定に応じて、以下のサーバ上で IIS 7.0 がインストールされている。
 - 標準設定：プライマリ サーバ。
 - 高可用性：アプリケーション サーバ。
- CA SDM が IIS 7.0 を使用するように設定されている。
- 外部認証が必要なアクセス タイプのリストが存在する。たとえば、CMDDB 管理者、従業員、CMDDB ユーザなど。

IWA 用の IIS の設定

IWA を有効にするように IIS サーバを設定します。この設定によって、IIS の認証モードが匿名から **Windows 認証** に変更されます。この設定の後、サーバは認証リクエストを外部ソースにリダイレクトし始めます。

次の手順に従ってください：

1. 設定に応じて、以下のサーバに管理者としてログインします。
 - 標準：プライマリまたはセカンダリ サーバ。
 - 高可用性：バックグラウンドサーバ。
2. [管理ツール]-[インターネット インフォメーション サービス マネージャ] を開きます。
3. [サーバ名] ノードを展開します。ここで、[サーバ名] は **CA SDM** サーバの名前です。
4. [サイト] - [既定の Web サイト] - [CAisd] ノードを展開します。
[CAisd ホーム] ページが開きます。
5. [認証] アイコンをダブルクリックします。
[認証設定] ページが開きます。
6. 既存の [状態] の値をクリックすることによって、[匿名認証] を無効にします。
7. 既存の [状態] の値をクリックすることによって、[Windows 認証] を有効にします。
8. IIS を再起動して変更を適用します。

IIS が IWA 用に設定されます。

IWA 用の CA SDM の設定

選択した各アクセス タイプに対して IWA を設定します。外部認証に対してアクセス タイプを設定すると、CA SDM は、そのアクセス タイプの連絡先を外部認証します。

以下の手順に従います。

1. システム管理者として **CA SDM** にログインします。
2. [管理] - [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。
3. 外部認証が必要なアクセス タイプをクリックします。
[アクセス タイプの更新] フォームが開きます。
4. [Web 認証] タブを選択し、[外部認証を許可] チェック ボックスをオンにします。
5. [検証タイプ] ドロップダウン リストから適切な値を選択します。以下の値について説明します。

アクセスなし

選択したアクセス タイプがアクセスを許可されていないことを指定します。

オープン

アクセスがすべてに対して開いていることを指定します。

OS

CA SDM にアクセスするには、CA SDM サーバのオペレーティング システムの認証情報が必要なことを指定します。EEM を設定している場合は、ログイン リクエストが EEM サーバにリダイレクトされます。

PIN

選択した CA SDM 連絡先レコードフィールドの値が認証に必要なことを指定します。たとえば、[検証タイプ] として [Pin] を選択し、[PIN フィールド] ドロップダウンから [連絡先番号] を選択した場合は、ユーザの連絡先番号が認証に必要なになります。

注: [検証タイプ] は IWA の検証には使用されず、ユーザが CA SDM ログインフォームを通してログインしたときに使用されます。CA SDM ログインページは、ユーザが [ログアウト] リンクをクリックした場合、または認証情報が IIS 認証情報に一致しない場合にのみ表示されます。

6. [保存] をクリックします。

その他のアクセス タイプに対して外部認証を設定するには、手順 1 ～ 6 を繰り返します。

IWA のテスト

CA SDM に対応する連絡先レコードを持つユーザ ID を使用して IWA をテストします。ログインが成功した場合は、IWA が正常に設定されていることを示します。

次の手順に従ってください：

1. 設定に応じて、CA SDM に対応する連絡先レコードを持つユーザ ID を使用し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。

注: オプションマネージャで LDAP オプションがインストールされている場合は、任意の Active Directory 連絡先から CA SDM に新しい連絡先を作成することもできます。

2. ブラウザを起動し、CA SDM の URL を入力します。

Service Desk のホーム ページが開きます。

IWA が正常に設定されています。

自動ポリシーの実行

ナレッジマネジメントでは、自動ポリシー機能によってデフォルトの自動ポリシーのセットが提供されます。これを使用することで、組織のナレッジ管理の効率性と有効性の向上を図ることができます。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。

「自動ポリシー リスト」ページには、管理できるポリシーの詳細が表示されます。このページを表示するには、「管理」タブを選択して、「ナレッジ」 - 「自動ポリシー」を選択します。

各ポリシーには、処理中にドキュメントが一致した場合に実行されるストアドクエリが含まれています。処理が完了すると、ライフサイクルポリシーレポートが **CA SDM** スコアボードに表示されます。レポートを表示するには、「ナレッジ ドキュメント」 - 「自動ポリシー」を選択します。スコアボードでは、アナリストは独自のドキュメントを管理できます。また、デフォルトでは、管理者は各役割のすべてのドキュメントを管理できます。

レポートを実装するには、自動ポリシー スケジューラを使用してバッチ処理を実行する必要があります。スケジューラは、設定に応じて以下の CA SDM サーバ上で実行され、レポートを表示するために必要なデータを表示します。

- 標準：プライマリまたはセカンダリ
- 高可用性：バックグラウンド

完了したら、[ナレッジ レポート カード](#) (P. 320)を実行します。

自動ポリシー スケジューラを実行する方法

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 スケジューラが表示されます。
2. 以下のフィールドを指定します。
 - **最終更新** - [自動ポリシー計算の実行] チェック ボックスをオンにします。
 - **スケジュール** - CA SDM が計算を実行してポリシーを実行する日時を指定します。
3. [保存] をクリックします。

ナレッジ レポート カードの実行

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 カードを実行する方法

1. [管理] タブをクリックします。
2. [ナレッジ] - [ナレッジ レポート] を参照します。
[ナレッジ レポート カード] が表示されます。

3. 以下のフィールドにデータを入力して、[保存] をクリックします。
 - **最終更新日** - [計算の実行] チェック ボックスをオンにします。
 - **スケジュール** - CA SDM が計算を実行してレポート カードを実行する日時を指定します。

注: 自動ポリシーとナレッジ レポート カードの使用方法については、「管理ガイド」を参照してください。

ナレッジ マネジメント サンプル データのインポート

Knowledge Broker および Knowledge Accelerator からのサンプル ナレッジ データが用意されており、このデータを使用できます。 サンプル ナレッジ データを使用する場合は、そのデータを ナレッジ マネジメント データ ベースにインポートする必要があります。

注: サンプル ファイルはローカライズされていません。 サンプルデータのインポートはローカライズ環境では動作しません。

高可用性の場合は、バックグラウンドサーバから `ImportSampleData.bat` または `ImportSampleData.sh` を実行します。

Windows インストール

1. `$NX_ROOT\samples\data` に移動して、`SampleData.zip` を同じディレクトリに解凍します。
2. コマンド ウィンドウから、`$NX_ROOT/bin` に移動し、`ImportSampleData.bat` を実行します。

UNIX インストール

1. `$NX_ROOT/samples/data` から `tar -xvf SampleData.tar` コマンドを実行します。
2. コマンド ウィンドウから、`$NX_ROOT/bin` に移動し、`ImportSampleData.sh` を実行します。

検索エンジンの設定

デフォルトにより、CA SDM と一緒に EBR 検索エンジンがインストールされます。

注: 検索エンジン 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。

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。

Crawler Surface 用の Domserver を設定するための新しいタグ

CA SDM にインデックス用の大きなデータがある場合、CA SDM 環境全体への影響を最小限に抑えるためにユーザの CA SDM の設定に応じて Crawler Surface 専用のサーバを用意する必要があります。

- 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

CA SDM サーバを設定する方法の詳細については、サーバ構成のオンライン ヘルプを参照してください。

インデックス作成に対応するために以下の新しい 2 つのタグが `crawler_surface_config.xml` ファイルに導入されました。

- 新しいタグ `root¥general_configuration¥sdm_domsvr_name` が `crawler_surface_config.xml` ファイルに導入されました。このタグにより、Crawler Surface 専用の domserver インスタンスの名前を指定できます。

デフォルト：domsvr

この値はデフォルト domserver（オブジェクト マネージャ）インスタンス名です。

- もう 1 つの新しいタグは、`root¥general_configuration¥` の `crawler_surface_config.xml` ファイル `sharepoint_properties_file` に導入されました。このタグにより、Crawler Surface が CA SDM データのインデックスを作成する SharePoint 用でない場合、ユーザが編集して空にすることができます。

デフォルト：sharepoint

この値は `NX_ROOT¥CATALINA_BASE_FS¥lib` でデフォルトで使用可能な `sharepoint.properties` ファイルの名前です。

CA Workflow の構成方法

CA SDM インストールで使用するために CA Workflow を設定するには、このセクションに記載されているタスクを実行します。

関連項目:

[CA Workflow の開始と停止](#) (P. 325)

[自動ログイン（外部認証）のセットアップ](#) (P. 329)

[自動ログイン用のワーク リストおよびワークフロー マネージャの設定](#) (P. 331)

[自動ログイン用のワークフロー デザイン環境の設定](#) (P. 332)

[CA Workflow オプション](#) (P. 333)

[問題管理サンプル ワークフローの設定方法](#) (P. 334)

[PC の注文サンプル ワークフローの設定方法](#) (P. 336)

[変更管理プロセス定義の例](#) (P. 338)

CA Workflow の開始と停止

CA Workflow をインストールする前に、まず CA SDM サーバをインストールして設定する必要があります。デフォルトの CA SDM Tomcat は、CA SDM デーモン マネージャによって自動的に設定、開始、停止されます。

pdm_tomcat_nxd コマンドラインユーティリティも、Tomcat インスタンスの開始および停止に使用できます。

次の手順に従ってください:

1. （従来の構成にのみ適用可能）セカンダリ サーバで開始される特定のプロセスを設定します。
 - a. pdm_edit（プライマリ サーバ上で）を実行します。
 - b. CA SDM サービスをリサイクルします。

これによって、各種環境変数が、CA Workflow のインストールと実行が必要なセカンダリ サーバに対してバージョン管理されます

2. CA SDM 構成に応じて、CA Workflow を以下のサーバにインストールし設定します。

- 標準：プライマリまたはセカンダリ サーバ
- 高可用性：いずれかのアプリケーション サーバ

3. `pdm_tomcat_nxd -d start -t CAWF` を実行します。

これで CA Workflow が手動で開始されます。

注：CA Workflow を停止するには、`pdm_tomcat_nxd -d stop -t CAWF` を実行します。

4. CA SDM 構成に応じて、CAWF オプショ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：バックグラウンドサーバ

これによって、CA Workflow が自動的に開始および停止されるようになり、CA SDM と CA Workflow 間の通信が可能になります。

関連項目：

[pdm_tomcat_nxd - Tomcat インスタンスの開始または停止 \(P. 326\)](#)

pdm_tomcat_nxd - Tomcat インスタンスの開始または停止

`pdm_tomcat_nxd` ユーティリティは、デーモンプロセスおよびコマンドラインユーティリティとして実行されます。ユーティリティを使用して、以下を実行できます。

- コマンドラインユーティリティからのリクエストを処理し、特定の Tomcat インスタンスの START および STOP を実行する。
- Tomcat の STATUS を返す。
- デーモンの EXIT を実行し、Tomcat インスタンスを停止する。

また、デーモンによって、Tomcat 「リスナ」サブレットからのリクエストが処理され、Tomcat インスタンスが停止または開始される際にステータスが更新されます。

`pdm_tomcat_nxd` コマンドラインユーティリティによって、Tomcat デーモンに **START**、**STOP**、**STATUS**、および **EXIT** の各リクエストが転送されます。あるいは、Tomcat デーモンを使用せずに、特定の Tomcat インスタンスの **START** または **STOP** を直接実行することも可能です。

`pdm_tomcat_nxd` によって、単一の CA SDM サーバ上で起動された複数のデーモンが提供されます。各デーモンは、特定の Tomcat インスタンス 1 つを管理します。各デーモンは、特定の Tomcat およびサーバ名で初期化されます。この 2 つを使用して、デーモンの **Slump** アドレス、デーモンの「リスナ」の **Slump** アドレス、および Tomcat インスタンスが定義されている Catalina Base ディレクトリが構成されます。この変更は、新しい Tomcat 名パラメータによってサポートされます。

以下のコマンドを使用して、`pdm_tomcat_nxd` デーモンを起動します。デーモンが起動されると、指定された Tomcat 名で自動的に Tomcat インスタンスが開始されます。

注: 以下の例では、デフォルトの Tomcat 名は空です（「ServiceDesk」を意味します）。

```
pdm_tomcat_nxd -s [ -t tomcat ]
```

例: 特定のサーバ上の特定の Tomcat デーモンへのリクエストの送信

リクエストが **STATUS** の場合、メッセージは、まず Tomcat 「リスナ」に送信されます。応答がない場合、リクエストは次に Tomcat デーモンに送信されます。デフォルトのサーバ名は `NX_LOCAL_HOST` です。デフォルトの Tomcat 名は空です（「ServiceDesk」を表します）。

```
pdm_tomcat_nxd -c <request> [-t <tomcat_name> ] [-S <server_name> ]
```

リクエスト

STOP | SHUTDOWN | START | STATUS | EXIT

例: このサーバ上の特定の Tomcat の (Tomcat デーモンを使用せずに) 開始または停止

```
pdm_tomcat_nxd -d <request> [ -t <tomcat_name> ]
```

リクエスト

STOP | START

例: Tomcat インスタンスの開始および停止に使用する Tomcat コマンドの表示

```
pdm_tomcat_nxd -T [ -t <tomcat_name> ]
```

デーモンプロセスは、開始すると、**server_name** および Tomcat 名（空でない場合）で構成されたプロセス名を使用して、Slump サーバにログインします。コマンドラインユーティリティは、この名前を使用して、デーモンにメッセージを送信します。コマンドラインユーティリティが使用する Tomcat 「リスナ」に **STATUS** リクエストが送信されるように、リスナプロセス名も **server_name** および **tomcat_name**（空でない場合）で構成されます。また、デーモンは、Tomcat 名（空でない場合）で構成されたログファイル名を使用して、Tomcat インスタンスのログファイルを開きます。以下の例は、**daemon_name**、**listener_name**、およびログファイル名の各変数を表しています。

```
daemon_name
```

```
"pdm_tomcat -" +  
server_name  
[ + "-" + tomcat_name ] if tomcat_name is non empty
```

```
listener_name = server_name + "-" +  
"container-pdmContextListener"  
[ + "-" + tomcat_name ] if tomcat_name is non empty
```

```
tomcat_log = pdm_tomcat +  
"-" + tomcat_name + ] if tomcat_name is non empty  
".log"
```

コマンドラインユーティリティまたはデーモンプロセスが Tomcat インスタンスを開始または停止すると、コマンド（**catalina_cmd**）が多様な NX 環境変数を使用して生成されます。以下の環境変数は、**NX_JAVA_OPTIONS** および **NX_TOMCAT_HOTSPOT** を除いて、すべて必要です。この 2 つは HP システム上でのみ使用されます。

環境変数（デフォルトの ServiceDesk Tomcat インスタンス用）は、名前の中に Tomcat 名が組み込まれません。これに対し、その他の Tomcat インスタンス用の環境変数では、オプションで、Tomcat 名を変数名の一部として使用できます。ただし、Tomcat 名 (XXX) を指定する必要がある NX_XXX_CATALINA_BASE を除きます。Tomcat の特定の環境変数が存在しない場合は、デフォルトの環境変数名が使用されます。

```
CATALINA_BASE | NX_XXX_CATALINA_BASE
NX_TOMCAT_INSTALL_DIR + [ _XXX ]
NX_TOMCAT_INSTALL_DIR + [ _XXX ]
NX_JRE_INSTALL_DIR + [ _XXX ]
NX_JDBC_DRIVER + [ _XXX ]
NX_JAVA_OPTIONS + [ _XXX ]
NX_JDBC_DRIVER_CLASSPATH + [ _XXX ]
NX_TOMCAT_HOTSPOT + [ _XXX ]
```

自動ログイン(外部認証)のセットアップ

変更要求、リクエスト、インシデント、問題、および案件を操作する際の CA Workflow ワークリスト タスクのログインプロセスを自動化するために、自動ログインをセットアップできます。自動ログインを使用すると、ワークリストリンクをクリックする際にユーザ ID とパスワードを入力する必要がなくなります。自動ログインでは、ワークリストのログインに、Windows オペレーティングシステムのドメイン認証情報を使用します。

注: 自動ログインが正しく機能するためには、ユーザが CA EEM 内のワークフロー管理者、ワークフロー プロセス開始者、またはワークフロー SuperUser のグループに含まれている必要はありません。これらのグループでは、ワークフロー デザイン環境にログインしたユーザに複数のアクセス レベルが提供されます。

ワークリスト タスクの自動ログインをセットアップする方法 (Windows のみ)

1. [CA Workflow をインストールして設定します。](#) (P. 266)
2. [自動ログイン用のワークリストおよびワークフロー マネージャを設定します。](#) (P. 331)
3. ユーザを認証する際に外部ディレクトリ (Microsoft Active Directory など) を参照するように CA EEM を設定します。詳細については、CA EEM のドキュメントを参照してください。

注: ワークリストにアクセスするために、また自動ログインが正しく機能するためには、ユーザに **CA EEM ユーザ レコード** と、同じユーザアカウントに一致する有効な **CA SDM 連絡先レコード** がある必要があります。項目をワークリストに表示し、**CA EEM** 内のワークフロー管理者、ワークフロー プロセス開始者、およびワークフロー **SuperUser** の各グループを利用するには、有効な **CA EEM ユーザ レコード** が必要です。

4. **CA SDM** にログインします。
5. **[管理]** タブをクリックします。
6. 左側のツリーで、**[オプション マネージャ] - [CA Workflow]** をクリックします。

[オプション リスト] が表示されます。

7. **cawf_username** 内のユーザ名および **cawf_password** 内のパスワードが **CA EEM** 内にセットアップされたドメイン上で有効なユーザであることを確認します。有効なユーザでない場合は、**CA EEM** を使用して、ドメインにユーザを追加します。

重要: オプション マネージャでは、**cawf_username** および **cawf_password** の値は、インストール後に **CA SDM** を設定したときに特権ユーザ名および特権ユーザ パスワードとして指定した値に基づいて設定されています。外部ディレクトリを参照するように **CA EEM** を設定するときに、**CA SDM** の環境設定で指定された特権ユーザが使用できないと、自動ログインは機能しません。このような場合には、**CA EEM** を使用してドメインにユーザを追加するか、**CA EEM** にセットアップされている有効なドメイン ユーザを含めるように **cawf_username** および **cawf_password** 内の情報を変更します。

8. **CA SDM** にログインし、適切なカテゴリで変更要求、リクエスト、インシデント、問題、または案件を作成します。

注: 変更要求、リクエスト、インシデント、問題、または案件を作成する前に、カテゴリが **CA Workflow** を使用するように設定されていて、**CA Workflow** 定義に関連付けられていることを確認します。

これで、ワークリスト内のリンクをクリックし、ユーザ ID とパスワードの入力を求められることなくログインできます。

関連項目:

[自動ログイン用のワークフロー デザイン環境の設定 \(P. 332\)](#)

自動ログイン用のワークリストおよびワークフロー マネージャの設定

ワークリストおよび Workflow Manager で自動ログインを有効にするには、ワークリストと Workflow Manager の web.xml ファイル（wl.xml および pm.xml）で変数 *automaticLoginEnabled* の値を true に変更します。エントリは、両方の web.xml ファイルで同じです。

```
<env-entry>
  <env-entry-name>automaticLoginEnabled</env-entry-name>
  <env-entry-value>true</env-entry-value>
  <env-entry-type>java.lang.Boolean</env-entry-type>
</env-entry>
```

ワークリストおよびワークフロー マネージャの初期値は、応答ファイル内の設定に基づいてインストール中に定義されます。

```
# Enable or disable Automatic Login (also known as Single Sign On or SSO)
```

```
-P serverAction.automaticLoginEnabled="true"
```

自動ログイン用にワークリストおよびワークフロー マネージャを設定する方法

1. 以下のディレクトリの pm.xml および wl.xml ファイルに移動します。

```
$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_WF¥conf¥Catalina¥localhost
```

2. pm.xml および wl.xml を編集し、以下の行の値を変更します。

- （編集前） <Environment name="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="false"/>
- （編集後） <Environment name="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="true"/>

3. 以下のコマンドを使用して、Tomcat サーバを停止します。

```
pdm_tomcat_nxd -d STOP -t CAWF
```

4. 以下のコマンドを使用して、Tomcat サーバを開始し、これらの 2 つのフォルダを再作成します。

```
pdm_tomcat_nxd -d START -t CAWF
```

5. ワークフロー タスクのあるチケットにアクセスし、タスクのうちの 1 つを選択します。
6. ワークリストが表示され、自動ログインが成功します。

注: 別の CA EEM サーバを参照するように CA Workflow を再設定する場合は、CAWF Tomcat をシャットダウンし、
`$NX_ROOT¥bopcfg¥www¥CATALINA_BASE_WF¥webapps` にある `pm` および `wl` フォルダを両方とも削除する必要があります。そのうえで、CAWF Tomcat を再起動し、新しい CA EEM サーバ情報でこれらのフォルダを再作成します。

自動ログイン用のワークフロー デザイン環境の設定

ワークフロー デザイン環境用の自動ログインは、コマンドラインパラメータ `-auto` を使用して有効化します。

CA Workflow オプション

以下のオプションは、CA Workflow 機能を制御します。

重要: CA Workflow と CA EEM をインストールした後、オプションマネージャで、ポート番号などのオプションを手動で設定する必要があります。たとえば、CA Workflow では別個の Tomcat Web アプリケーションが使用されるため、デフォルトのポート 8080 を使用できません。ポートの競合を避けるため、デフォルト値として 8090 が使用されます。詳細については、「実装ガイド」を参照してください。

cawf_hostname

CA Workflow がインストールされているサーバのホスト名を指定します。この変数は、CA Workflow が CA SDM メディアからインストールされている場合にのみ設定します。それ以外の場合は、このオプションをインストールしないでください。

cawf_password

CA Workflow IDE ユーザのパスワードを指定します。CA Workflow のインストール中に、CA SDM コンポーネントインストーラウィザードは、[ワークフロー ユーザ パスワード] の値を使用して cawf_password を設定します。

cawf_pm_location

CA Workflow プロセス マネージャ アプリケーションの場所を指定します。URL は以下の形式で指定します。

http://<wf_hostname>:8090/pm

cawf_pm_url

CA Workflow プロセス マネージャの Web サービス URL を指定します。URL は以下の形式で指定します。

http://<wf_hostname>:8090/pm/services/pmService2

cawf_username

CA Workflow IDE ユーザの CA Workflow ユーザ名を指定します。CA Workflow のインストール中に、CA SDM コンポーネントインストーラウィザードは、[ワークフロー ユーザ名] の値を使用して cawf_username を設定します。

cawf_wl_location

CA Workflow ワークリスト マネージャ アプリケーションの場所を指定します。URL は以下の形式で指定します。

http://<wf_hostname>:8090/wl

cawf_wl_url

CA Workflow ワークリストの Web サービス URL を指定します。URL は以下の形式で指定します。

`http://<wf_hostname>:8090/wl/services/wlService`

重要: 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には、CA SDM サーバを再起動する必要があります。高可用性設定では、必ずしも、すべてのオプションですべてのサーバの再起動が必要になるわけではありません。サーバを再起動する前には、「サーバ再起動リスト」を確認してください。

問題管理サンプル ワークフローの設定方法

問題管理サンプル ワークフローによって、特定の問題チケットの変更要求を作成すべきかどうかを決定する手順を把握できます。問題の担当者は、問題をリサーチした後、推奨事項を作成するための問題調査を実行します。この調査によって、承認者は問題の影響度を把握することができ、変更管理によって解決する必要があるかどうかわかります。このワークフローの基本的概念（問題の痛み/価値分析）は、ITIL v3 から得られています。

注: 以下のプロセスで CA SDM の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。

問題管理サンプル ワークフローを設定する方法

1. 以下の値を使用して、アナリスト（たとえば、アナリストの Jane さん）の CA SDM 連絡先を作成します。

連絡先タイプ

[アナリスト] を選択します。

データ パーティション

[Service Desk アナリスト] を選択します。

アクセス タイプ

[Service Desk スタッフ] を選択します。

電子メール アドレス

電子メール アドレスを入力します。

注: 必要に応じて、テストとして自分の電子メール アドレスを入力してください。

Notifications Method

低、通常、高、または緊急通知用の電子メールを選択します。

2. 以下の値を使用して、管理者（たとえば、管理者の Joe 氏）の CA SDM 連絡先を作成します。

連絡先タイプ

[マネージャ] を選択します。

データ パーティション

[Service Desk 管理者] を選択します。

アクセス タイプ

[Service Desk 管理者] を選択します。

電子メール アドレス

電子メール アドレスを入力します。

注: 必要に応じて、テストとして自分の電子メール アドレスを入力してください。

Notifications Method

低、通常、高、または緊急用の通知を選択します。

3. Jane アナリストおよび Joe 管理者の CA SDM 連絡先に関連付けられた EEM ユーザ レコードを作成します。

注: EEM レコードのユーザ ID は、連絡先レコードのユーザ ID と一致している必要があります。EEM ユーザ レコードの作成の詳細については、EEM オンライン ヘルプを参照してください。

4. Joe 管理者を Jane アナリストの連絡先レコード上に管理者として割り当てます。
5. CI (Exchange Server など) を作成します。
6. 根本原因コード (RAM アップグレードが必要、など) を作成します。
7. 問題領域 (ProblemMgmt.SampleWF など) を作成します。

8. ProblemMgmt.SampleWF 問題領域を問題管理サンプル ワークフローに関連付けます。
9. 以下の属性を使用して、問題チケットを作成します。

問題領域

[ProblemMgmt.SampleWF] を選択します。

設定項目

[Exchange Server] を選択します。

Asignee

[アナリスト、Jane] を選択します。

10. Jane アナリストとして CA SDM にログインし、ワークフロー設定をテストします。

注: ワークフローの最初のフォームを完了する前に、問題調査を完了する必要があります。ワークフロー タスクの実行の詳細については、CA Workflow オンラインヘルプを参照してください。

関連項目:

[自動ログイン \(CA MDB 認証\) のセットアップ \(P. 351\)](#)

[自動ログイン \(外部認証\) のセットアップ \(P. 329\)](#)

[CA Workflow の開始と停止 \(P. 325\)](#)

PC の注文サンプル ワークフローの設定方法

PC の注文サンプル ワークフローによって、新しい PC を注文する変更管理プロセスを把握できます。

注: 以下のプロセスで CA SDM の各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。

PC の注文サンプル ワークフローのセットアップおよびテストする方法

1. 以下の値を使用して、従業員（たとえば、従業員の William さん）の CA SDM 連絡先を作成します。

連絡先タイプ

[従業員] を選択します。

データ パーティション

[従業員] を選択します。

アクセス タイプ

[従業員] を選択します。

電子メール アドレス

電子メール アドレスを入力します。

注: 必要に応じて、テストとして自分の電子メール アドレスを入力してください。

Notifications Method

低、通常、高、または緊急通知用の電子メールを選択します。

2. 以下の値を使用して、アナリスト（たとえば、アナリストの Jane さん）の CA SDM 連絡先を作成します。

連絡先タイプ

[アナリスト] を選択します。

データ パーティション

[Service Desk アナリスト] を選択します。

アクセス タイプ

[Service Desk スタッフ] を選択します。

電子メール アドレス

電子メール アドレスを入力します。

注: 必要に応じて、テストとして自分の電子メール アドレスを入力してください。

Notifications Method

低、通常、高、または緊急通知用の電子メールを選択します。

3. William 従業員および Jane アナリストの CA SDM 連絡先に関連付けられた EEM ユーザ レコードを作成します。

注: EEM レコードのユーザ ID は、連絡先レコードのユーザ ID と一致している必要があります。EEM ユーザ レコードの作成の詳細については、EEM オンライン ヘルプを参照してください。

4. 変更カテゴリ (PC.Order など) を作成します。
5. 変更カテゴリの担当者として Jane アナリストを割り当てます。
6. 以下の属性を使用して、変更要求チケットを作成します。

変更カテゴリ

[PC.Order] を選択します。

Assignee

[アナリスト、Jane] を選択します。

7. Jane アナリストとして CA SDM にログインし、ワークフロー設定をテストします。

注: ワークフロー タスクの実行の詳細については、CA Workflow オンライン ヘルプを参照してください。

変更管理プロセス定義の例

この例では、以下の ITIL v3 ガイドラインに従って、変更管理プロセス定義によって変更要求を管理する方法を示します。

- リスク アセスメント
- 競合分析と影響度分析
- 変更マネージャと CAB の両方による承認
- 実装アセスメントと確認

注: この例では、CA SDM が CA Workflow を使用していること、および変更管理プロセス定義が設定されていることを前提とします。変更管理プロセス定義の詳細方法については、「管理ガイド」を参照してください。

承認に向けて変更要求を準備する方法

この例では、変更カテゴリを設定して、承認に向けて変更要求を準備します。管理者は、変更管理プロセス定義を使用するように変更カテゴリを設定し、グループと連絡先を設定します。依頼者は、リスク アセスメント調査を実施して、競合分析と影響度分析を実行し、変更分析を実行します。

注: 変更カテゴリの設定方法および変更管理プロセス定義の使用方法の詳細については、「オンライン ヘルプ」および「管理ガイド」を参照してください。

承認に向けて変更要求を準備するには、以下の手順に従います。

1. 管理者としてログインし、以下のオプションを使用して変更カテゴリを作成または編集し、[CA Workflow を使用] をクリックします。
 - **CAB - CAB** グループを選択します。
 - **グループ - 実装グループ**を指定します。
 - **リスク調査 - [一般]** を選択します。
 - **CA Workflow 定義名** - ([ワークフロー] タブから) [変更管理] - [Service Desk r12.1] を選択します。
2. 以下の CA SDM ユーザ ID と連絡先を作成して、CA SDM および CA EEM でそれぞれのグループに割り当てます。
 - **Don Requester** - 変更要求を作成する連絡先。
 - **John Approver** - 変更マネージャとして変更要求を承認する実装グループのマネージャ。CAB 承認者の役目を果たす CAB グループのマネージャ。
 - **Sue Implementer** - 変更要求ワーク項目も実施する実装グループのメンバー。
3. Don Requester としてログインして、以下の値で変更要求を作成します。
 - **依頼者** - Don Requester を指定します。
 - **カテゴリ** - 変更管理プロセス定義を使用する変更カテゴリを指定します。
 - **タイプ** - [正常] を選択します。
 - **要求の概要/要求の説明** - 変更要求の理由を指定します。

- **スケジュール開始日** - 開始日を指定します。
- **スケジュール期間** - 期間を指定します。
- **CI** - ([構成アイテム] タブから) 影響を受ける構成アイテムを指定します。

Don Requester が、電子メール通知を受け取り、リスク アセスメント調査を実施します。 [変更要求の詳細] ページに [ステータス] - [RFC] が表示されます。

4. [リスク調査] をクリックして、変更要求のリスクが高くなるようにリスク アセスメント調査の質問に回答します。 [サブミット] をクリックして、 [確認] をクリックします。

システムにより、変更要求のリスク値が生成されます。依頼者が電子メール通知を受け取り、競合分析と影響度分析を開始します。

注: [タスクの実行] ページで [確認] をクリックした後でのみ、次のタスクに移動することができます。

5. [ワークフロー タスク] タブで、リンクに従って変更要求の [競合] タブに移動します。
6. [競合分析] をクリックして、CI に対するスケジュールの競合をすべて解決します。
7. [構成アイテム] タブで、 [影響度分析] をクリックして、各 CI に関する情報を確認します。
8. [構成アイテム] タブで、 [影響度エクスプローラ] をクリックして [CMDDB 関係] タブに移動し、関連する CI への変更要求の影響度を検討します。
9. [タスクの実行] ページに移動して、 [確認] をクリックします。

Don Requester が、電子メール通知を受け取り、変更分析を実行します。

10. [ワークフロー タスク] タブで、リンクに従って変更要求の [変更分析] タブに移動します。変更要求を確認するための質問に回答し、 [サブミット] をクリックします。

John Approver が、電子メールの通知を受け取り、変更要求を承認します。 [変更要求の詳細] ページに、ステータスとして [承認中] が表示されます。

- **CAB 承認** - はい

変更要求を承認して実装する方法の例

この例では、変更管理プロセス定義を使用して変更要求を管理する場合に実行する、承認者向けタスクと実装タスクを示します。承認者は、変更分析の情報を確認して変更要求を承認します。実装グループのメンバーとして、変更要求について割り当てられた作業を実施し、変更要求の結果を表す実装後レビューを行います。

注: 変更管理プロセス定義の使用方法的詳細については、「管理ガイド」を参照してください。

変更要求を承認して実装するには、以下の手順に従います。

1. **John Approver** としてログインして、変更要求をオープンします。
2. [ワークフロー タスク] タブで、リンクに従って変更要求の [変更管理承認] タブに移動し、[承認] をクリックします。

この変更要求はリスクが高いため、ステータスは [承認中] になります。この例では、変更諮問委員会 (CAB) のメンバーとして **John Approver** も使用しているため、**John Approver** が、電子メール通知を受け取り、CAB メンバーとして変更要求を確認します。

3. [CAB 承認] タブの [承認] をクリックします。
[変更要求の詳細] ページで、[ステータス] が [承認済み] として表示されます。**Sue Implementer** が、電子メール通知を受け取ります。
4. **Sue Implementer** としてログインして、変更要求をオープンします。
5. [ワークフロー タスク] タブで、[タスクの実行] ページに移動し、[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。
6. [ワークフロー タスク] タブで、リンクに従って [実装完了] タブに移動します。
7. 変更要求の進捗状況を表すための質問に回答し、[完了] をクリックします。

変更要求がクローズします。[変更要求の詳細] ページに、[ステータス] が [実装済み] として、および [クローズコード] が [成功] として表示されます。**Sue Implementer** が、電子メール通知を受け取り、PIR を実行します。

8. [ワークフロー タスク] タブで、リンクに従って [PIR] タブに移動します。
9. [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。

変更要求がクローズします。[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。[ワークフロー タスク] タブに、[変更要求のクローズ] リンクと追加情報が表示されます。[変更要求アクティビティ] タブに、変更管理プロセス定義の最終ステータスが表示されます。

CA Process Automation ワークフロー インテグレーションの設定方法

CA Process Automation ワークフロー インテグレーションを設定するには、以下の手順に従います。

1. CA Process Automation および CA SDM がスタンドアロン エンティティとして動作していることを確認します。
重要: CA Process Automation が FIPS モードに設定されている場合は、EEM サーバおよび EEM SDK も FIPS モードに設定する必要があります。EEM SDK を FIPS モードに設定する方法の詳細については、CA EEM のマニュアルを参照してください。
2. CA Process Automation ワークフロー オプションを設定します。
3. 必要なグループおよびユーザ ID を作成し、CA SDM ユーザに CA Process Automation への適切なアクセス権を付与します。

関連項目:

[CA Process Automation および CA SDM インストールの確認](#) (P. 343)

[CA Process Automation ワークフロー オプションの設定](#) (P. 343)

[CA Process Automation ユーザ管理](#) (P. 348)

[CA EEM を使用して CA SDM から CA Process Automation へのシングルサインオンをサポートする方法](#) (P. 349)

CA Process Automation および CA SDM インストールの確認

サーバアーキテクチャが両方の製品をサポートする場合、単一のサーバ上で共存できるように CA Process Automation と CA SDM を統合できます。CA Process Automation または CA SDM のコンポーネントが同じサーバ上で統合できない場合は、各製品を別のサーバにインストールすることを検討してください。

CA Process Automation および CA SDM を設定する前に、両方の製品がインストールされていて、独立して動作していることを確認します。

注: CA SDM および CA Process Automation の製品要件の詳細については、「CA SDM リリース ノート」を参照してください。

CA Process Automation および CA SDM のインストールを確認する方法

1. CA SDM がホストされているサーバ上でブラウザを開き、CA Process Automation ユーザが CA Process Automation にログインできることを確認します。以下のプレースホルダをターゲット CA Process Automation インストールと一致するように変更してください。

`http(s)://<server>:CA Portal/itpam`

2. 以下の URL を入力します。以下のプレースホルダをターゲット CA Process Automation インストールと一致するように変更してください。

`http(s)://<server>:CA Portal/itpam/JNLRequestProcessor?processType=startUI`

CA Process Automation 製品が CA SDM ホストからアクセスできます。

CA Process Automation ワークフロー オプションの設定

CA Process Automation ワークフロー オプションを設定する際、CA SDM と CA Process Automation 間の接続を指定します。認証に CA EEM を使用している場合は、CA EEM ホスト名も指定します。

CA Process Automation ワークフロー オプションを設定する方法

1. [管理] タブで、[オプションマネージャ]-[CA IT PAM ワークフロー] を選択します。

[オプションリスト] が表示されます。

2. 各オプションの名前を右クリックし、コンテキストメニューから「編集」を選択します。以下のオプションを設定します。

`caextwf_eem_hostname`

CA EEM サーバの名前を指定します。たとえば、*pam.host.com* は認証ホストを示します。CA Process Automation で CA EEM を認証サーバとして使用するように設定した場合のみ、`caextwf_eem_hostname` をインストールします。CA SDM は、ユーザ名とパスワードを CA EEM トークンに変換するためにこの値を使用します。これにより、ユーザ名とパスワードは HTTP でプレーンテキストで渡されません。

注: CA Process Automation インストールで CA EEM を使用していない場合は、`caextwf_eem_hostname` オプションに値を設定しないでください。また、`caextwf_eem_hostname` をインストールしないでください。必要でないのに `false` 値を設定したり、`caextwf_eem_hostname` をインストールしたりすると、統合は失敗します。

`caextwf_endpoint`

CA Process Automation ホスト名、ポート、および必須の `/itpam/soap` パスを含めることにより、CA Process Automation Web サービスを参照する URL を指定します。たとえば、

「`http://pam.host.com:pam-Tomcat-port/itpam/soap`」はエンドポイントを示します。CA EEM を使用する場合、CA Process Automation と CA SDM 間の統合が正常に動作するには、`caextwf_eem_hostname` オプションのインストールが必要です。

`caextwf_log_categories`

CA SDM のリクエスト、変更要求、および案件の「ワークフロー タスク」タブに表示する、CA Process Automation プロセスインスタンス ログ カテゴリ名のカンマ区切りリストを指定します。たとえば、*Operator,Response,MyOwnCategory* は 3 つのログ カテゴリを提供します。

CA SDM および CA Process Automation のプロセス デザイン担当者の業務上の意思決定に基づいて `caextwf_log_categories` をインストールします。このオプションを使用して、リクエスト、変更要求、および案件の「ワークフロー タスク」タブに表示するデフォルト データを調整します。

`caextwf_log_categories` オプションをインストールすると、プロセス カテゴリおよびユーザが指定するカテゴリに含まれるすべての CA Process Automation プロセス インスタンス ログ メッセージが、[ワークフロー タスク] タブに表示されます。

`caextwf_log_categories` をインストールしないと、プロセス カテゴリの CA Process Automation プロセス インスタンス ログ メッセージのみが、[ワークフロー タスク] タブに表示されます。

注: CA Process Automation の事前定義済みログ メッセージカテゴリ、およびカスタム メッセージカテゴリの定義については CA Process Automation リファレンス ドキュメントを参照してください。

`caextwf_processdisplay_url`

ホスト名および必須の

`/itpam/JNLRequestProcessor?processType=startUI&roid` パスを提供することにより、CA Process Automation プロセス インスタンスのグラフィカル スナップショットを起動する方法を指定します。たとえば、

`http://pam.host.com:pam-Tomcat-port/itpam/JNLRequestProcessor?processType=startUI&roid=` はプロセス インスタンスのスナップショットを起動します。リクエスト、変更要求、または案件の[ワークフロー タスク] タブで、[プロセスの表示] を選択すると、スナップショットが表示されます。

CA Process Automation と CA SDM の統合を正しく機能作させるには、`caextwf_processdisplay_url` オプションをインストールする必要があります。

caextwf_worklist_url

ホスト名および必須の /itpam?webPage=mytaskfilter&view=tasklist パスを提供することにより、プロセス インスタンス パスを指定します。たとえば、

「<http://pam.host.com:pam-Tomcat-port/itpam?webPage=mytaskfilter&view=tasklist>」と指定すると、CA SDM ユーザは、注意の必要な CA Process Automation プロセス インスタンスのリストを表示できるようになります。CA SDM ユーザが、リクエスト、変更要求、または案件の「ワークフロー タスク」タブにリスト表示された任意のタスクに関連付けられたリンクを選択すると、CA Process Automation にリストが表示されます。

CA Process Automation と CA SDM の統合を正しく機能させるには、caextwf_worklist_url オプションをインストールする必要があります。

caextwf_ws_password

caextwf_ws_user オプションの CA Process Automation ユーザ名に関連付けられた管理パスワードを指定します。CA SDM では、ユーザ名とパスワードを使用して、CA Process Automation Web サービス機能にアクセスし、開始リクエスト フォームの選択、プロセス定義情報の選択、プロセスインスタンス情報の選択などの統合アクティビティを実行します。

CA Process Automation と CA SDM の統合には、caextwf_ws_password オプションのインストールが必要です。指定するパスワードおよびユーザ名には、CA Process Automation への適切なアクセス権が必要です。ただし、CA SDM 連絡先レコード内に存在する CA Process Automation ユーザ名とパスワードは必要ありません。

caextwf_ws_user

caextwf_ws_password オプションの CA Process Automation ユーザ名に関連付けられた CA Process Automation 管理ユーザ名を指定します。CA SDM では、ユーザ名とパスワードを使用して、CA Process Automation Web サービス機能にアクセスします。これらのサービスは、開始リクエスト フォームの選択、プロセス定義情報の選択、プロセスインスタンス情報の選択、プロセス インスタンスの起動などの統合アクティビティを実行します。

CA Process Automation と CA SDM 間の統合が動作するには、**caextwf_ws_user** オプションのインストールが必要です。指定するユーザ名およびパスワードには、CA Process Automation への適切なアクセス権が必要です。ただし、CA SDM 連絡先レコード内に存在する CA Process Automation ユーザ名とパスワードは必要ありません。

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。

プロセス インスタンス データがなくても、CA SDM と CA Process Automation は通信できます。CA SDM および CA Process Automation では、CA Process Automation プロセス定義および CA Process Automation 開始リクエスト フォームをいつでも作成できます。

注: CA Process Automation プロセス定義および CA Process Automation 開始リクエスト フォームの作成の詳細については、「管理ガイド」および CA Process Automation ユーザ ドキュメントを参照してください。

CA Process Automation ユーザ管理

CA Process Automation と CA SDM は、スタンドアロン製品として、それぞれに認証と認可に関する要件があります。 サービス指向アーキテクチャ (SOA) 統合戦略をサポートするために、認証に CA EEM を使用するよう両製品を設定できます。

CA EEM を認証サーバに設定して CA Process Automation をインストールすると、インストーラによって、デフォルトで、いくつかのポリシーと 4 つの重要なエンティティが作成されます。

- 2つのアプリケーションユーザ、itpamadmin および itpamuser。 CA Process Automation 3.1 SP1 の場合は pamadmin および pamuser。
- 2つのアプリケーショングループ、ITPAMAdmins および ITPAMUsers。 CA Process Automation 3.1 SP1 の場合は PAMAdmins および PAMUsers。

CA Process Automation を使用する CA SDM ユーザは、ITPAMAdmins (CA Process Automation 3.1 SP1 では PAMAdmins) と ITPAMUsers に分かれます。

- CA SDM アナリストは、業務に以下のものを伴う場合、ITPAMUsers (CA Process Automation 3.1 SP1 では PAMUsers) のメンバである必要があります。
 - CA Process Automation 操作リクエスト フォームの承認、拒否、またはその他の応答
 - ユーザに割り当てられた CA Process Automation プロセス インスタンスのリスト作成
 - CA Process Automation の [プロセス ステータス] 画面の [プロセスの表示] ボタンをクリックして、グラフィカル表示の表示 CA Process Automation ITPAMUsers (3.1 SP1 では PAMUsers) グループには、グラフィックへのアクセスを許可する追加の CA Process Automation ポリシーが必要です。
- CA SDM アナリストは、業務に以下のものを伴う場合、ITPAMAdmins (3.1 SP1 では PAMAdmins) のメンバである必要があります。
 - CA Process Automation プロセス定義または開始リクエスト フォーム、あるいはその両方の作成およびチェック
 - CA Process Automation 内でのプロセス インスタンスの直接終了処理
プロセス インスタンスの終了処理は、必要な統合手順の管理上の例外です。

- CA Process Automation プロセス インスタンス タスクの委任
- ユーザが CA SDM オプション マネージャに定義されたユーザ名である場合
- CA SDM ユーザは、業務に以下のものを伴う場合、CA Process Automation へのアクセス権は必要ありません。
 - CA Process Automation インスタンスを起動するリクエスト、変更要求、および案件の作成
 - CA Process Automation インスタンス ステータスおよびタスク情報を表示する [ワークフロー] タブの確認
 - CA Process Automation プロセス終了の原因となるリクエスト、変更要求、または案件のステータスの変更（変更要求のキャンセルなど）
 - CA SDM リクエスト領域、変更カテゴリ、案件カテゴリでの CA Process Automation プロセス定義の選択

注: CA EEM 設定の詳細については、CA Process Automation のドキュメントを参照してください。

CA EEM を使用して CA SDM から CA Process Automation へのシングル サインオンをサポートする方法

CA SDM と CA Process Automation を統合している場合、CA SDM から CA Process Automation へのシングル サインオンを以下のようにしてセットアップできます。

1. 以下の要件が満たされていることを確認します。
 - CA SDM と CA Process Automation が同一の CA EEM を使用するよう設定されている。
 - CA SDM にログインするユーザは CA Process Automation のユーザでもある。

- CA EEM がユーザ ストアとして内部データベースを使用する場合、ユーザはグローバルな権限を持っているか、同じフォルダに属している必要があります。そうでない場合は、CA EEM が外部ディレクトリや CA Siteminder などの外部ユーザ ストアを参照する際、シングルサインオンをアクセスするために、ユーザはそのストアのユーザである必要があります。
2. CA SDM DVD インストール メディアから CA EEM をインストールするか、既存の CA EEM インストール (CA Process Automation 用の CA EEM など) を使用します。
 3. CA SDM の [管理] タブの [オプション マネージャ] - [セキュリティ] フォルダから、以下のオプションをインストールします。
 - eiam_hostname
 - use_eiam_authentication

注: [オプション マネージャ] - [CA Process Automation] フォルダのオプション caextwf_eem_hostname はインストールする必要はありません。ただし、インストールする場合には、値が eiam_hostname オプションと同じである必要があります。
 4. CA SDM を再起動します。
 5. CA Process Automation にユーザを作成するには、以下の手順に従います。
 - a. EiamAdmin ユーザ ID などの管理ユーザを使用して、CA Process Automation アプリケーション コンテキストを使用する CA EEM にログインします。
 - b. [ID の管理] タブをクリックし、[ユーザ] フォルダの横のアイコンをクリックします。

- c. [新規ユーザ] ページ上部の [名前] フィールドは、CA SDM 連絡先テーブル内のユーザ ID と一致する必要があるユーザ ID です。
- d. [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、以下を実行します。
 - リスト表示されるグループのどちらかまたは両方を追加します。CA Process Automation にログインするためには、これらの2つのグループの少なくとも1つを追加します。
 - [姓]、[名]、[表示]、[パスワード] などの [新規ユーザ] のフィールドを入力します。
6. 同じユーザ ID を使用して CA SDM 連絡先テーブル内のユーザを作成します。ユーザの [アクセス タイプの検証タイプ] フィールドが CA EEM に設定されていることを確認します。

CA EEM で指定したこのユーザとパスワードを使用して、CA EEM および CA SDM にログインできます。

自動ログイン(CA MDB 認証)のセットアップ

変更要求、リクエスト、インシデント、問題、および案件を操作する際の CA Workflow ワークリスト タスクのログインプロセスを自動化するために、自動ログインをセットアップできます。自動ログインを使用すると、ワークリスト リンクをクリックする際にユーザ ID とパスワードを入力する必要がなくなります。自動ログインでは、ワークリストのログインに、Windows オペレーティング システムのドメイン認証情報を使用します。

注: 自動ログインが正しく機能するためには、ユーザが CA EEM 内のワークフロー管理者、ワークフロー プロセス開始者、またはワークフロー SuperUser のグループに含まれている必要はありません。これらのグループでは、ワークフロー デザイン環境にログインしたユーザに複数のアクセス レベルが提供されます。

ワークリスト タスクの自動ログインをセットアップする方法 (Windows のみ)

1. [CA Workflow をインストールして設定します。](#) (P. 266)
2. [自動ログイン用のワークリストおよびワークフロー マネージャを設定します。](#) (P. 331)

3. ユーザを認証する際に **CA MDB** を使用するよう **CA EEM** を設定します。**CA Workflow** をインストールおよび設定する際に、ワークフロー ユーザ名およびワークフロー ユーザ パスワードが **CA EEM** に自動的に追加されます。詳細については、**CA EEM** のドキュメントを参照してください。

注: ワークリストにアクセスするには、ユーザは **CA EEM** ユーザ レコードを持っている必要があります。

4. **CA SDM** にログインし、適切なカテゴリで変更要求、リクエスト、インシデント、問題、または案件を作成します。

注: 変更要求、リクエスト、インシデント、問題、または案件を作成する前に、カテゴリが **CA Workflow** を使用するよう設定されていて、**CA Workflow** 定義に関連付けられていることを確認します。

これで、ワークリスト内のリンクをクリックし、ユーザ ID とパスワードの入力を求められることなくログインできます。

関連項目:

[自動ログイン用のワークフロー デザイン環境の設定 \(P. 332\)](#)

単一エントリポイントの設定

CA SDM と CA Service Management を統合すると、単一エントリポイントによって、CA Service Catalog へのシングルサインオンが可能になります。

単一エントリポイントを設定する方法

1. catalog_server 一般オプションをインストールします。

注: 詳細については、オプション マネージャのオンライン ヘルプを参照してください。

2. CA SDM を再起動します。
3. CA SDM の [従業員セルフサービス] ページに移動します。
4. [カタログサービスの参照] をクリックします。

CA Service Management のログオン ページが表示されます。

CA EEM が CA SDM と CA Service Management の両方で設定されている場合、単一エントリポイントによって、CA Service Catalog へのシングルサインオンが可能になります。シングルサインオンが設定されている場合は、CA Service Management のログオン ページは表示されません。

注: CA SDM の [従業員セルフサービス] にゲストとして入った場合は、シングルサインオンは利用できません。

CA Service Management にシングルサインオンを設定する方法

1. CA EEM セキュリティ オプション eiam_hostname および use_eiam_authentication がインストールされていることを確認します。
2. CA EEM 内にユーザをセットアップし、これらのユーザが CA Service Management ユーザでもあることを確認します。
3. [管理] タブをクリックします。
4. [セキュリティと役割の管理] フォルダを開きます。
5. [アクセス タイプ] をクリックします。
6. [従業員] 役割を選択します。
7. [Web 認証] タブの検証タイプが [CA EEM-Use CA Embedded Entitlements Manager] に設定されていることを確認します。
8. 定義済み CA EEM ユーザとしてログインし、[従業員セルフサービス] ページに移動します。

9. [カタログ サービスの参照] をクリックします。
CA Service Management メイン ページが表示されます。

マルチテナンシーを実装する方法

サービス プロバイダは、CA SDM マルチテナンシー インストールのプライマリ テナントです。

注: サービス プロバイダおよびマルチテナンシーの詳細については、「[管理ガイド](#)」を参照してください。

[**setup**] モード以外のモードでマルチテナンシーを有効にするには、まずテナントを定義し、テナントが必要なオブジェクトおよびテナントが任意のオブジェクト内のテナント属性に必要なだけ値を入力する必要があります。ただし、テナントが必要なオブジェクトにテナントを割り当てる前に、マルチテナンシーの適用を選択できます。テナントが必要なテーブルでテナントが **Null** のオブジェクトは、すべてのユーザーに表示されるパブリック オブジェクトとして扱われます。これらのオブジェクトは、ユーザーインターフェースによって検出されて更新されます。**CA SDM** では、マルチテナンシー適用の程度に応じて、テナントが必要なオブジェクトを更新してテナントを適用するように求める場合があります。

注: テナントが必要なオブジェクトのインスタンスを更新する前に、テナントを作成する必要があります。また、**pdm_settenant** ユーティリティと **pdm_buildtenant** ユーティリティは、マルチテナンシーをアクティブ化して属性の設定を完了した後に使用できます。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誤って含まれている場合、テナントが必要なテーブルにパブリック データのドロップダウン リストが表示されます。

重要: **pdm_buildtenant** を実行する前に、サービス プロバイダを設定する必要があります。

マルチテナンシーを実装するには、以下の手順に従います。

1. [マルチテナンシーのオプションを \[setup\] に設定](#) (P. 377) し、CA SDM を再起動します。テナントの状態 ([setup] 、 [on] 、 [on(allow)]) を変更するたびに、サービスをサイクルする必要があります。

重要: マルチテナンシーが [setup] モードの場合、Web インターフェースの変更はサービス プロバイダ管理者に対してアクティブになり、テナンシー関連のオブジェクトおよびデータが Web インターフェースで表示および編集可能になります。ただし、テナンシーの制限は適用されないため、サービス プロバイダ管理者以外のユーザには製品インターフェースの変更は表示されません。このため、マルチテナンシーの準備中に、テナントされていないモードで引き続き製品を使用できます。

2. [既存のテナント実装をテナント オブジェクトにマップします。](#) (P. 379)
3. [テナント列に値を入力します](#) (P. 380)。

注: 連絡先のテナント列に値を入力してから、テナント化されている連絡先を使用してほかのオブジェクトのテナント列に値を入力することをお勧めします。

4. テナントが必要なテーブルすべてにテナントが設定されていることを確認します。
5. [テナントを作成します。](#) (P. 382)

重要: 作成する最初のテナントは、サービス プロバイダ テナントである必要があります。サービス プロバイダ テナントを作成したら、CA Service Desk からログアウトし、サービス プロバイダとして再度ログインします。このようなログインを簡単に行うには、特権ユーザ

(ServiceDesk など) としてログインします。このような特権ユーザは、サービス プロバイダ テナントに自動的に所属するためです。別の連絡先としてログインする場合は、最初に pdm_settenant を使用して、連絡先をサービス プロバイダに割り当てます。

6. [テナント グループを作成します。](#) (P. 384)

7. [\[マルチテナンシー\] オプションを \[オン\] に設定します。](#) (P. 377)

このオプションを選択した後、サービスを再起動して以下の手順を実行します。

- a. 特権ユーザ名（通常は **ServiceDesk**）を使用してログインします。
- b. 特権ユーザがサービス プロバイダ テナントに割り当てられていることを確認します。
- c. マルチテナンシーの制限が適用されていることを確認します。

重要: 非テナント データがデータベースに残っている場合は、マルチテナンシー適用レベルを **[warn]** または **[allow]** に設定できます。つまり、テナントが必要なテーブルを **Null** のテナントで更新できるため、テナントを含めるように更新されていないチケットに対して、**SLA**（サービス レベル アグリーメント）または添付イベントが実行された場合にデータが失われなくなります。

注: `pdm_settenant` は、実装の完了状況の監視（`-r` オプションを指定）、およびテナントの一括更新（必要な場合）の両方に対してマルチテナンシーがアクティブになった後でも実行できます。

8. データ パーティションの制約およびロールをバックアップします。

マルチテナンシーでは、要求されるデータ パーティションの制約について制約数と複雑さの両方が軽減されるため、制約を簡素化できます。変更を加える前に、**Domain_Constraint** テーブルと **usp_role** テーブルの両方をバックアップします。

9. 不要なデータ パーティションの制約を削除します。

単一テナンシー用に定義されたドメイン制約の多くは、マルチテナンシーをアクティブ化した後で不要になるため、削除することができます。これらの不要な制約を削除すると、クエリのパフォーマンスが向上します。

10. 確認および監査を行います。

`pdm_settenant -r` を実行して、テナントが必要なテーブルにテナントを追加入力する必要があるかどうかを確認します。カテゴリやアクティビティ通知などのテナントが任意のテーブルにテナントを追加する必要があるかどうかを確認します。

11. (オプション) 問題が発生した場合は、マルチテナンシーを無効にします。実装後に問題が発生した場合は、オプションで以下の手順を実行できます。
 - a. `Domain_Constraint` テーブルおよび `usp_role` テーブルを復元します。
 - b. [マルチテナンシー] オプションを [セットアップ] に戻します。
 - c. システムを再起動します。

テナント列への入力を継続し、元に戻すことが必要な問題をすべて修正する間、サイトでは以前の操作を再開できます。

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非テナント データが誤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。

マルチ テナンシー

マルチテナンシーを使用すると、複数の独立したクライアント (テナント) およびそれらのユーザが製品の単一の実装を共有できるようになります。テナントは、ハードウェアおよびアプリケーション リソースを共有し、これにより両方のコストが削減されます。

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。

- 役割 - **CA SDM** ユーザの役割は、アクセス許可を管理します。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。
- テナント階層 - テナント階層は、テナントに親テナントを割り当てるときにシステムによって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。

通常、各テナントは自身のデータを使用するためにのみ実装を参照できます。各テナントは、別のテナントのデータを更新または表示できません。

サービス プロバイダ テナント

サービス プロバイダは、他のエンティティにサービスを提供します。マルチテナンシー実装では、サービス プロバイダはプライマリ テナント（所有者）であり、他のテナントを管理します。

サービス プロバイダ テナントは、以下のタスクを実行できます。

- 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

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、その階層において親または上位テナント（存在する場合）のサブテナントになります。スーパーテナントは、同じテナント階層において別のテナント（その相対サブテナント）より上位のテナントです。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。

Service Desk Manager 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。必要な場合、サービス プロバイダは、テナント階層に属することができます。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。

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。

テナント属性およびオブジェクト

マルチテナンシーがアクティブな場合、各連絡先（ユーザ）アクセス権を、すべてのテナント（パブリック）、シングルテナント、またはテナントグループ（ユーザ定義またはシステム保守）に付与できます。連絡先の役割はアクセスを制御し、読み取りおよび書き込みアクセスを独立して指定します。テナントアクセスは、役割に依存しています。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実装されている場合、ほとんどのデータオブジェクトには、その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

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。データベース管理システムではなく、**Service Desk Manager**がこの制限を実施します。これらのオブジェクト内のすべてのデータは、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。各テナントは、パブリックデータおよびそのテナント固有データがマージされたビューでオブジェクトを表示します。

例：カテゴリおよびロケーション

マルチ テナンシー アクセス

ユーザがデータベースに対してクエリを実行した場合、CA SDM は、返される結果を、そのユーザがアクセス権を持つテナントに属するデータ オブジェクトに制限します。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。ユーザは、テナントが必要なテーブルおよびテナントが任意のテーブル内のデータ、および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を参照します。

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、以下の事項が検証されます。

- オブジェクトがユーザの現在の役割で更新可能なテナントに属していること。
- 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）参照が以下のいずれかであること。
 - パブリック（テナントなし）オブジェクト
 - 同じテナントからのオブジェクト
 - テナント階層でオブジェクトの上位のテナントのオブジェクト。
つまり、テナント 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。

注: SREL 参照制限には例外があります。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、製品オブジェクトスキーマで `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。

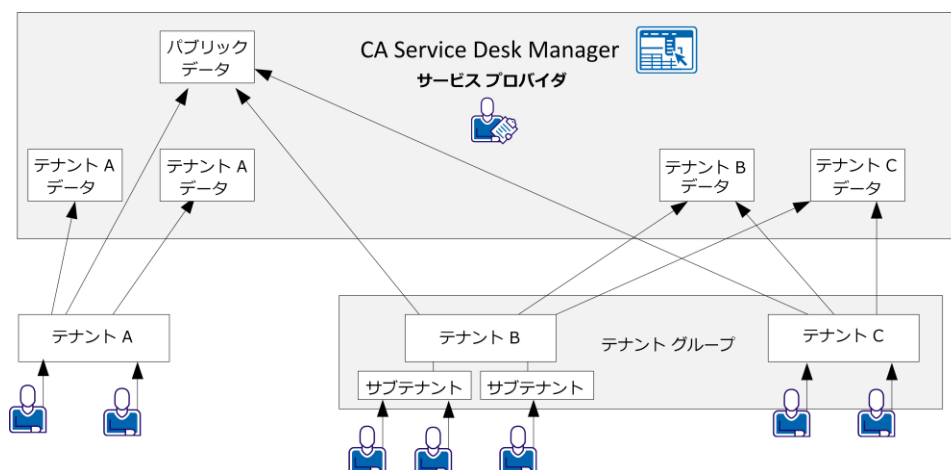
オブジェクトを作成するユーザが、複数のテナントの更新アクセス権を持っている場合、そのユーザは直接または間接的にテナントを明示的に指定する必要があります。

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: 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。

例: CA SDM データへのテナント アクセス

この例では、テナント A、テナント B、およびテナント C が CA SDM 内の自身のデータおよびパブリック データにアクセスする方法を示します。



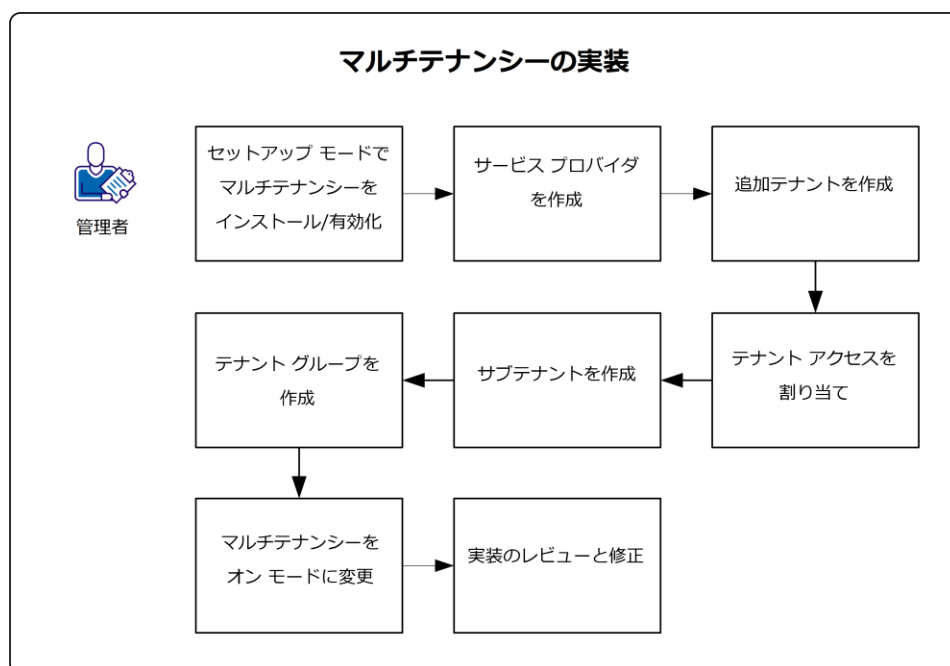
この例では、各テナントがアクセスできるデータを矢印で示しています。

- テナント A ユーザは、テナント A のデータおよびパブリック データにアクセスできます。
- テナント B およびそのサブテナント ユーザは、テナント B のデータおよびパブリック データにアクセスできます。
- テナント C ユーザは、テナント C のデータおよびパブリック データにアクセスできます。
- テナント B、そのサブテナント、およびテナント C は同じテナント グループに属するため、ユーザはテナント B、テナント C、およびパブリック データを参照できます。

マルチテナンシーを実装する方法

以下の図に、CA SDM 特権ユーザである管理者が、初めてマルチテナンシーを実装する方法を示します。初めから終わりまで、CA SDM の実装は以下のように変化します。

1. 単一のクライアントが単一の実装を使用します。
2. 複数の独立したクライアント（テナント）およびそれらのユーザが単一の実装を共有します。各テナントは、自身のデータを使用するためにのみ実装を参照できます。



管理者は、CA SDM 管理インターフェースを使用して以下の手順を実行します。

1. [セットアップ モードでマルチテナンシーをインストールおよび有効にする](#) (P. 363)。
2. [サービス プロバイダ テナントを作成する](#) (P. 364)。
3. [追加のテナントを作成する](#) (P. 366)。
4. [役割にテナント アクセス権を割り当てる](#) (P. 369)。

5. [サブテナントを作成する](#) (P. 372)。
6. [テナント グループを作成する](#) (P. 372)。
7. [マルチテナンシーをオン モードに変更](#) (P. 374) してサービスを再起動する。
8. [実装を確認して問題を修正する](#) (P. 376)。

マルチテナンシーのインストールおよび有効化

マルチテナンシーを有効にするには、製品のマルチテナンシー オプションをインストールし、セットアップ モードを有効にします。セットアップ モードでは、マルチテナンシー機能を管理者向けに有効にします。このモードでは、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、テナンシー制限はシステムによって適用されないため、管理者以外のユーザには変更は表示されません。このモードにより、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、製品の通常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。

重要: マルチテナンシーが [setup] モードの場合、Web インターフェースの変更はサービス プロバイダ管理者に対してアクティブになります。これにより、テナンシー関連のオブジェクトおよびデータを Web インターフェースで表示できるようになります。ただし、テナンシーの制限は適用されないため、サービス プロバイダ管理者以外のユーザには製品 インターフェースの変更は表示されません。このため、マルチテナンシーの実装中に、引き続き製品を使用できます。

次の手順に従ってください:

1. 管理者として CA SDM にログインし、[管理] タブをクリックします。
2. 左側のツリーで、[オプション マネージャ] - [マルチテナンシー] をクリックします。
[オプション リスト] ページが表示されます。
3. [multi_tenancy] をクリックします。
[multi_tenancy オプションの詳細] ページが表示されます。
4. [編集] をクリックします。
[更新オプション] ページが表示されます。

5. [オプション値] ドロップダウン リストから [セットアップ] を選択します。
6. [インストール] をクリックします。
[multi_tenancy] オプションがインストールされます。
7. [更新] ボタンをクリックします。
ページに変更内容が表示されます。
8. ウィンドウを閉じます。
[オプション リスト] ページが再表示されます。
9. サービスを再起動します。
マルチテナンシーをセットアップ モードで実装する準備ができました。

サービス プロバイダ テナントの作成

サービス プロバイダ テナントを作成できます。最初のテナントを作成する場合、以下が適用されます。

1. 最初のテナントは常にサービス プロバイダになります。
重要: この指定は変更できません。テナント作成ページにある [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です。
2. 特権ユーザ（通常 Windows では ServiceDesk、Linux/UNIX では srvcdesk）は、サービス プロバイダ テナントに関連付けられます。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: Windows には、Administrator システム ユーザが用意されています。特権ユーザは、テナントを Administrator ユーザに手動で割り当てる必要があります。

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] - [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. 以下のフィールドを指定します。

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

この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。

テナント番号

(情報のみ) テナント番号が表示されます。CA SDM はこのオプションを使用しません。

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

ロケーションを指定するためのロケーションルックアップページを表示します。

連絡先

連絡先を指定するための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。
サービスプロバイダ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、作成したサービスプロバイダテナントが表示されます。
7. CA SDM からログアウトします。

テナントの作成

CA SDM を使用して、新しいテナントを作成できます。必要に応じてテナントを自由に作成し、クライアントにサポートを提供する複数の会社を管理できます。

次の手順に従ってください:

1. サービス プロバイダのメンバーとして管理インターフェースにログインします。このログインを簡単に行うには、特権ユーザ (ServiceDesk など) としてログインします。このユーザは、自動的にサービス プロバイダ テナントに属します。
2. [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。

3. [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。
4. 以下のフィールドを指定します。

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。それ以降、このチェック ボックスは読み取り専用になります。

テナント番号

(情報のみ) テナント番号が表示されます。CA SDM はこのオプションを使用しません。

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

ロケーションを指定するためのロケーションルックアップページを表示します。

連絡先

連絡先を指定するための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。

5. [保存] をクリックします。

テナントが作成されます。

6. ウィンドウを閉じます。
7. [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。
8. (オプション) 作成する各テナントに対して手順 3 ～ 6 を繰り返します。

役割へのテナント アクセス権の割り当て

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は、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。マルチテナンシーがインストールされている場合、役割の詳細ページには、テナント アクセス権の割り当てまたは編集が可能な追加のオプションが表示されます。

注: テナント ユーザに対しては、各自のデータ以外のデータへのアクセス権を付与できます。非サービス プロバイダ テナント アナリストは、自分のテナントおよびサブテナントに対するアクセス権のみを持ちます。しかし、機能アクセス権を更新することにより、アナリストのテナントを追加できます。たとえば、役割を定義して、その役割のユーザに対して特定のテナント 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。

次の手順に従ってください:

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. テナントアクセスを割り当てる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。このページの [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。
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。

テナント アクセスと同じ

[テナントのアクセス]の設定と同じアクセス権を設定します。この値は、[テナント書き込みアクセス] ドロップダウン リストのデフォルトで、[テナント書き込みアクセス] オプションのみで選択できます。

すべてのテナント

テナント制限を削除します。このアクセス権を持つ役割のユーザは、以下の操作を実行できます。

- データベースのオブジェクトを表示する（読み取りアクセス権）。
- データベースでテナント オブジェクトを作成および更新する（アクセス権）。

[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 アクセス権を、指定し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するためのフィールドが表示されます。この役割のユーザは、指定されたテナントに関連付けられたオブジェクトにのみアクセスできます。

テナント グループ

役割のテナント アクセス権を、ユーザ定義またはシステム管理のテナント グループに設定します。このオプションを選択すると、特定のテナント グループを選択するためのフィールドが表示されます。この役割のユーザは、指定されたグループ内のテナントに関連付けられたオブジェクトにのみアクセスできます。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。

連絡先のテナント

役割のテナント アクセス権を、その役割を使用する連絡先のテナントに設定します。この役割のユーザは、自分のテナントに関連付けられたオブジェクトにのみアクセスできます。

連絡先のテナント グループ

アナリストの役割のアクセス権を、アナリストが作業を行うテナント グループ（アナリストの連絡先レコードで指定される）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。このオプションは、アナリストに対してのみ使用できます。

連絡先のサブテナント グループ

役割のテナント アクセス権を、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。この役割のユーザは、自分のサブテナント グループに関連付けられたオブジェクトにのみアクセスできます。

連絡先のスーパーテナント グループ

役割のテナント アクセス権を、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。この役割のユーザは、自分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にのみアクセスできます。

連絡先の関連するテナント グループ

役割のテナント アクセス権を、その役割を使用する連絡先の関連テナント グループに設定します。この役割のユーザは、自分の関連テナント グループに関連付けられたオブジェクトにのみアクセスできます。

パブリックの更新

役割に属するサービス プロバイダ ユーザがパブリック データを作成または更新する権限があるかどうかを制御します。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。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。

[保存]をクリックします。

役割に対してテナント アクセス権が割り当てられます。ユーザがデータベースにクエリを実行した場合、Service Desk Manager は、返される結果を、そのユーザの役割に関連付けられているテナントに属するデータ オブジェクトに制限します。

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定義および変更できます。テナントをテナント階層に配置するには、テナントに親テナントを割り当てます。

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] - [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。

テナント詳細ページが表示されます。このページでは、必要なデータまたは変更を入力できます。

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 リストには、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の場合、そのテナントは親テナントのサブテナント グループに属します。親テナントは、サブテナントのスーパーテナント グループに属します。各テナントは、他方のテナントの関連するテナント グループに属します。

テナントグループの作成

テナント グループは、CA SDM オブジェクトへのアクセス権を共有するテナントの集合です。テナント グループを使用すると、テナントへのアクセス権を分類、管理、および制御できます。テナントまたはテナントのグループに対して役割を割り当てることができます。マルチテナンシーがアクティブである場合、各役割は、すべてのテナント（パブリック）、単一のテナント、または単一のテナント グループに関連付けられます。役割が複数のテナントへのアクセスを必要とする場合は、テナント グループを使用します。たとえば、特定の地理上の場所に属するテナントで構成されるテナント グループにアナリストを割り当てることができます。

テナント階層の各テナントに対して、以下の 3 つのテナント グループが自動的に生成され、管理されます（**tenant** はテナント名）。

- **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、システム保守テナント グループについてはその名前および説明のみを変更できます。

例: 役割 A がテナント A、テナント B、テナント J へのアクセス権を必要とする場合

各テナントに対して役割を個別に割り当てる代わりに、以下の手順に従います。

1. テナント グループを作成し、テナント A、テナント B、およびテナント J をそのグループに追加します。
2. 役割 A をそのテナント グループに割り当てます。

役割 A に割り当てられたユーザ（連絡先）は、テナント グループ（テナント A、B、J で構成される）にアクセスできます。

次の手順に従ってください:

1. サービス プロバイダとしてログインし、[管理] タブをクリックし、[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。
9. (オプション) 作成する各テナントグループに対して手順3～6を繰り返します。

マルチテナンシーのオンモードへの変更

マルチテナンシー オプションをオンモードに変更して、実装したマルチテナンシーが完全に機能するようにできます。このようにすると、各テナントは自身のデータを使用するためにのみ実装を参照できます。各テナントは、別のテナントのデータを更新または表示できません。

次の手順に従ってください:

1. 管理者として CA SDM にログインし、[管理] タブをクリックします。
2. 左側のツリーで、[オプションマネージャ] - [マルチテナンシー] をクリックします。
[オプションリスト] ページが表示されます。

3. [multi_tenancy] をクリックします。
[multi_tenancy オプションの詳細] ページが表示されます。
4. [編集] をクリックします。
[更新オプション] ページが表示されます。
5. [オプション値] ドロップダウンリストから [セットアップ] を選択します。
6. [編集] をクリックします。
[更新オプション] ページが表示されます。
7. [オプション値] ドロップダウンリスト内の以下の値から、[オン] (デフォルト) を選択します。

オン

(デフォルト) テナントが **NULL** であり、テナントを持つテーブルへの **SREL** が利用できない場合、テナントが必要なテーブルへのチェックインを禁止します。

オン(警告)

テナントが必要なオブジェクトが **NULL** テナントで作成または更新された場合、エラーをログに書き込みますが、チェックインして処理を継続できます。

オン(許可)

テナントが必要なオブジェクトが **Null** テナントで作成または更新された場合、警告をログに書き込みますが、チェックインして処理を継続できます。

8. [保存]、[更新] の順にクリックします。
ページに変更内容が表示されます。
9. ウィンドウを閉じます。
[オプション リスト] ページが再表示されます。
10. サービスを再起動します。
マルチテナンシーが完全に機能するようになります。

実装の確認と問題の修正

マルチテナンシーの実装を確認し、見つかった問題を修正します。

次の手順に従ってください:

1. 特権ユーザ名（通常は **ServiceDesk**）を使用してログインします。
2. [管理] タブをクリックし、[テナントリスト] を参照します。
[テナント名] で特権ユーザのプロバイダが [はい] として表示されます。
3. [連絡先リスト] を参照して、マルチテナンシー制限が適用されていることを確認します。

テナントが必要なテーブルにテナントなしデータが誤って含まれている場合は、以下のメッセージが [連絡先リスト] に表示されます。

AHD05358 nn 件のテナントなしのアクティブな連絡先オブジェクトが CA Service Desk Manager の起動時にあります

重要: テナントなしデータがデータベースに存在する場合、マルチテナンシー オプション モードを [オン (警告)] または [オン (許可)] に設定できます。これらのモードを使用すると、**NULL** テナントが含まれるテナントが必要なテーブルを更新できます。この方法を使用すると、テナントが含まれないチケットに対して、サービス レベル アグリーメント (SLA) または関連イベントがに実行されるときに、データの損失を防ぐことができます。

4. (オプション) 問題が発生した場合はマルチテナンシーを無効にして、以下の手順に従います。
 - a. **Domain_Constraint** テーブルおよび **usp_role** テーブルを復元します。
 - b. マルチテナンシー オプションを [セットアップ] に戻します。
 - c. システムを再起動します。

元に戻すことが必要な問題をすべて修正する間、サイトでは以前の操作を再開できます。

Multi-Tenancy の有効化

本製品を使用して、マルチテナンシーを有効化できます。

マルチテナンシーの有効化方法

1. [管理] タブをクリックします。
2. 左側のツリーで、[オプション マネージャ] - [マルチテナンシー] をクリックします。
[オプション リスト] ページが表示されます。
3. [multi_tenancy] をクリックします。
[multi_tenancy オプションの詳細] ページが表示されます。
4. [編集] をクリックします。
[更新オプション] ページが表示されます。
5. [オプション値] ドロップダウン リストから、以下のオプションのいずれかを選択します。

オフ

マルチテナンシー機能を無効にします。

セットアップ

マルチテナンシーを [setup] モードで有効にします。このモードでは、編集可能なテナント関連のオブジェクトと属性が、サービス プロバイダ管理者の **CA SDM** に表示されますが、テナンシーの要件は適用されません。他のユーザは、マルチテナンシーがインストールされていないかのように作業を続行できます。

オン

マルチテナンシーのオプションが完全に機能します。以下の値を選択することもできます。

- **strict** - (デフォルト) テナントが **Null** の場合、**CA SDM** はテナントが必要なテーブルへのチェックインに失敗し、製品はデフォルトを **SREL** からテナント化されたテーブルに設定できません。
- **warn** - テナントが必要なオブジェクトが **Null** テナントで作成または更新された場合に、**CA SDM** はエラーをログに書き込みますが、チェックインして処理を継続できます。
- **allow** - テナントが必要なオブジェクトが **Null** テナントで作成または更新された場合に、**CA SDM** は警告をログに書き込みますが、チェックインして処理を続行できます。

注: **ca_tenant** テーブルに値を入力していない場合は、[オプション値] ドロップダウンリストで **[setup]** を選択する必要があります。マルチテナンシーを新たに実装する場合は、**[setup]** を選択します。

6. [インストール] をクリックします。
[**multi_tenancy**] オプションがインストールされます。
7. [更新] ボタンをクリックします。
ページに変更内容が表示されます。
8. ウィンドウを閉じます。
[オプション リスト] ページが再表示されます。
9. サービスを再起動します。

新しいテナントを初期化する方法

サービスプロバイダとして、カテゴリ、データパーティション、チケットテンプレートなどの新規テナント用データの標準セットの作成が必要になる場合があります。これを実行するには、**pdm_extract** または **pdm_tenant_extract** を使用して、必要なデータが含まれる **pdm_userload** 入力ファイルを作成します。

必要に応じて、テキストエディタでこのファイルを編集できます。続いて、**pdm_userload** を引数 **-t** を指定して使用し、入力ファイルをデータベースにロードして、新しいテナントにテナント列を設定できます。**pdm_userload** の **-t** 以外の引数の詳細については、「管理ガイド」を参照してください。

新しいテナントを初期化するには、以下の手順に従います。

1. **ca_tenant** テーブル内にテナントを作成します。
オンラインの [\[テナントの作成 \(P. 382\)\]](#) ページを使用します。
2. 前述のとおり標準データをロードします。
`pdm_userload -t` を使用して、テナントを設定します。
3. 新しいテナントの連絡先レコードを作成します。
外部データをロードするか、`pdm_userload -t` を使用します。

既存のテナント実装をテナントオブジェクトに変換する方法

現在マルチテナンシーによって提供されている機能の一部は、以前はデータパーティションおよび別の **CA SDM** オブジェクトを使用して実現されていました。実装をマルチテナンシーに変換する場合、最初に踏むべき手順は、以前使用していたオブジェクト内のデータを新しいテナントオブジェクトにマップすることです。以前使用していたオブジェクトを、「事前テナント」オブジェクトと呼びます。このような要件が当てはまるサイトの大部分では、**org** (組織) オブジェクトが事前テナントオブジェクトになります。事前テナントオブジェクトには、以下のアプローチを使用できます。

1. 事前テナントオブジェクトが **org** でない場合、その **Majic** オブジェクト定義によって **TENANT_REQUIRED** が指定されていることを確認します。
2. 以下の場所にある **buildtenant.xml** ファイル内の事前テナントオブジェクトから新しいテナントオブジェクトへの属性マッピングを確認します。

`$NX_ROOT/samples/multi_tenancy`

注: **buildtenant.xml** を `$NX_ROOT/site/cfg` ディレクトリにコピーする必要があります。また、**buildtenant.xsd** は **buildtenant.xml** と同じディレクトリにある必要があります。そうでない場合、エラーが表示されます。製品のインストール時に **buildtenant.xsd** は `$NX_ROOT/site/cfg` に格納されるため、このファイルをコピーする必要はありません。

デフォルト設定は **org** をベースとしています。事前テナントオブジェクトが **org** でない場合は、ファイルを編集する必要があります。

3. [pdm buildtenant -f](#) を実行します。 (P. 391)

事前テナント オブジェクト別に新しいテナントが作成され、事前テナント オブジェクト内のテナント属性が新しいテナントを参照するように設定されます。

4. CA SDM にログインし、テナント オブジェクトと事前テナント オブジェクトの両方を確認します。

注: 単一のテナント オブジェクトに複数の事前テナント オブジェクトをマップする必要がある場合もあります。このような場合は、影響を受ける事前テナント オブジェクトを手動で更新してから、使用しないテナントを削除または非アクティブ化します。

テーブル内のテナント属性に値を入力する方法

テーブル全体またはテーブルのサブセットのテナント属性に値を入力するには、`pdm_settenant` ユーティリティを使用します。このユーティリティでは、設定ファイルを使用して、テナント化するオブジェクトを選択し、オブジェクトのテナントを取得する場所を指定します。テナントを明示的に指定するか、テナント化するオブジェクト内の **SREL** リファレンスからテナントを取得するよう指定します。

`pdm_settenant` を使用して、テーブル内のテナント属性に値を入力するには、以下の手順に従います。

1. 設定ファイルを作成または編集します。

設定ファイルを通して、テナント属性を設定する行を選択し、テナント属性の値のソースを指定します。本製品では、以下の場所に、サンプルの `settenant.xml` ファイルを用意しています。

`$NX_ROOT/samples/multi_tenancy`

注: サンプルの `settenant.xml` ファイルを編集することも、ファイルを作成して `$NX_ROOT/site/cfg` ディレクトリにコピーすることも可能です。また、`settenant.xsd` は `settenant.xml` と同じディレクトリにある必要があります。そうでない場合、エラーが表示されます。製品のインストール時に `settenant.xsd` は `$NX_ROOT/site/cfg` に格納されるため、このファイルをコピーする必要はありません。

2. [pdm_settenant -f \[configuration file\] -r](#) を実行します。 (P. 393)

`pdm_settenant` ユーティリティが設定ファイルを読み取り、設定ファイルで定義されている各ルールを順次処理します。

このユーティリティを使用して、まず **cnt**（連絡先）オブジェクト内のテナント属性に値を入力し、次に **cnt** オブジェクトをソースとして使用して、ほかのオブジェクトにテナントを入力することをお勧めします。

cnt オブジェクトが正常にテナント化された後、ほかのテーブルにテナントを設定するためのベースとして使用するには、以下の手順に従います。

- a. 設定ファイル内で **type="SREL"** を使用して **TenantRule** を指定し、**cnt** オブジェクトを参照する属性がほかのテーブル内にテナントを設定するようにします。
 - b. （オプション） **type="Name" <tenantname>** を使用して **TenantRule** を指定し、テーブルの一部にテナントを明示的に指定します。
3. 新しい設定ファイルで **pdm_settenant** を実行します。
 4. 必要に応じて、**pdm_settenant** を再実行します。

オブジェクトのテナント列に値を入力した後、そのオブジェクトへの **SREL** を **TenantRule** のベースとして使用し、ほかのオブジェクトにテナントを設定できます。

例: SREL タイプ構文

SREL タイプ構文では、テナント値が指定されていない **cnt** オブジェクトをチェックし、リンクされた組織オブジェクトからのテナント値を使用します。

```
<Object name="cnt">  
<TenantRule type="SREL">organization</TenantRule>  
<Where>tenant is null</Where>  
</Object>
```

例: 名前タイプ構文

名前タイプ構文では、テナント値が指定されていない **org** オブジェクトをチェックし、そのテナントフィールドに実際のテナントオブジェクトの名前を設定します。

```
<Object name="org">  
<TenantRule type="Name">Tenant A</TenantRule>  
<Where>tenant is null</Where>  
</Object>
```

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 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。

テナントデータのエクスポートおよびインポートの方法

サービスプロバイダは、既存のマルチテナンシー実装からテナントデータを抽出し、新しいシステムにインポートできます。

注: データのボリュームによっては、抽出プロセスに数時間かかることがあります。抽出およびインポートの実行は、以下のような複数のフェーズを経る必要がある場合があります。

初期

ベースラインを抽出し、後続のフェーズで使用する制御ファイルを作成します。

Update

制御ファイルを使用して、前回の実行以降に変更されたデータのみを抽出します。

最終

「更新」と同じ手順を実行しますが、アニメーションも抽出する点が異なります。アニメーションは、「初期」と「更新」の両フェーズでは省略されます。

あるデータベースからデータを抽出し、別のデータベースにインポートするには、以下の手順に従います。

1. [pdm_tenant_extract](#) (P. 398) の初期フェーズを実行し、ベースラインデータを抽出します。これによって、後続のフェーズで使用する制御ファイルが作成されます。
2. 抽出したデータ用に新しくクリーンな MDB を準備します。

重要: 初期フェーズからの出力を、当該製品やほかの製品で使用されていないデータベースにロードする必要があります。初期フェーズのデータからロードした各テーブルは、ロード前に切り捨てが行われています。データベースがすでに使用されている場合、この切り捨てによって、データが失われる可能性があります。

3. 新しいシステムに特権のある連絡先が重複して表示されるのを避けるために、特権のある連絡先を非アクティブにする必要があります。抽出したデータをロードする前に、CA SDM にログオンし、これらの連絡先のステータスを「非アクティブ」に変更します。
4. データロード中に参照に関する問題を回避するために、制約を削除する適切なスクリプトを実行します。
 - (Oracle) \$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql を実行します。
 - (SQL Server) \$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql を実行します。

5. [pdm_userload](#) (P. 400) を使用して、初期フェーズからのデータを手順 2 および 3 で準備したクリーンな MDB にロードします。
6. [pdm_tenant_extract](#) の更新フェーズか最終フェーズを実行し、前のフェーズ以降に作成または変更された追加データを抽出します。
[pdm_tenant_extract](#) では、手順 1 で作成した制御ファイルを使用して、前のフェーズで処理されたデータを判別します。
7. [pdm_userload](#) を使用して、手順 5 で抽出したデータを、前のフェーズからロードしたデータが含まれているのと同じ MDB にロードします。

注: このユーティリティの詳細については、[pdm_userload](#) (P. 400) を参照してください。

8. すべてのデータが新しいデータベースにインポートされるまで、手順 5 と 6 を繰り返します。最終フェーズを最後に実行する必要があります。
9. 新しいデータベースの完全性を保護するために、制約を追加する適切なスクリプトを実行して、手順 3 で削除した制約を回復します。
 - (Oracle) `$NX_ROOT/samples/views/Oracle/OracleAddConstraints.sql` を実行します。
 - (SQL Server)
`$NX_ROOT/samples/views/SQLServer/SQLAddConstraints.sql` を実行します。
10. [pdm tenant delete](#) (P. 396) を使用して、元のデータベースから抽出したデータを削除します。
11. 抽出したテナントと関連付けられたすべてのリポジトリがターゲット設定にコピーされていることを確認します。

添付ファイルおよびリポジトリを管理する方法

添付ファイルはリポジトリに格納されます。パブリック リポジトリなど、抽出したテナントと関連付けられたすべてのリポジトリをターゲットシステムにコピーする必要があります。この処理は主に手動による操作で、手順は以下のとおりです。

1. 最初にターゲット システムにデータをロードした後、すべてのリポジトリの場所に固有の情報を再定義します。このタスクでは、以下の値を変更します。
 - [サーバ名]
 - アップロードパス

- サブレット パス
 - アーカイブ パス
2. 必要なすべてのディレクトリおよびフォルダを手動で作成します。
 3. 最終フェーズからデータをロードした後（あるいはロード中に）、前の場所から新しいリポジトリ場所に添付ファイルをすべてコピーします。

これらの手順を完了すると、ターゲットシステムにある添付ファイルはすべて正常に参照します。ただし、添付ファイルのコピーはソースシステムに残ります。これらの不要な添付ファイルの削除には、[pdm_clean_attachments.pl ユーティリティを使用](#) (P. 392) します。

マルチテナンシーで使用するユーティリティ

本セクションでは、マルチテナンシー環境を管理するために使用するユーティリティについて説明します。

注: 必須のパラメータは「{ }」で囲まれ、オプションのパラメータは「[]」で囲まれます。

関連項目:

[pdm_buildtenant - 別のオブジェクトからのテナントの作成](#) (P. 391)

[pdm_clean_attachments - テナントデータインポート後の重複する添付ファイルの削除](#) (P. 392)

[pdm_settenant - オブジェクトへのテナントの割り当て](#) (P. 393)

[pdm_tenant_delete - データベースからのテナントデータの削除](#) (P. 396)

[pdm_tenant_extract - テナントデータの抽出](#) (P. 398)

[pdm_userload - テナントデータのロード](#) (P. 400)

pdm_buildtenant - 別のオブジェクトからのテナントの作成

pdm_buildtenant ユーティリティは、別のオブジェクトからテナントを作成する場合に使用します。すでにデータ パーティションおよび別の **CA SDM** オブジェクトを使用して、マルチテナンシーで提供されるようになった機能の一部を実現している場合があります。実装をマルチテナンシーに変換するには、最初に **pdm_buildtenant** を使用して、以前に使用していたオブジェクトのデータを新しいテナント オブジェクトにマップします。

重要: **pdm_buildtenant** を実行する前に、サービス プロバイダを設定する必要があります。

このセクションでは、以前テナントに似た情報を保持するために使用されていたオブジェクトを、「事前テナント」オブジェクトと呼びます。このような要件を持つサイトの大部分では、**org**（組織）オブジェクトがテナント前オブジェクトとなりますが、どのテナント前オブジェクトであっても以下のアプローチを使用できます。

pdm_buildtenant ユーティリティでは、テナント オブジェクトがテナント前オブジェクトから構築されます。このアプリケーションでは、テナント前オブジェクトごとに新しいテナントが作成され、新しいテナントを参照するようにテナント前オブジェクトのテナント属性が設定されます。このユーティリティの構文は以下のとおりです。

```
pdm_buildtenant [-h] | [-f [configuration_file]]
```

-f configuration_file

（オプション）テナント前オブジェクトからテナントを作成する場合のルールを指定する構成ファイルの場所を指定します。この引数が含まれていない場合、**pdm_build** テナントでは、**\$NX_ROOT/site/cfg** ディレクトリの構成ファイルが使用されます。このファイルでは、テナント前オブジェクトが **org** であることが想定されています。**org** でない場合は、**pdm_buildtenant** を使用する前に構成ファイルを編集する必要があります。

注: **buildtenant.xml** を **\$NX_ROOT/site/cfg** ディレクトリにコピーする必要があります。また、**buildtenant.xsd** は **buildtenant.xml** と同じディレクトリにある必要があります。そうでない場合、エラーが表示されます。製品のインストール時に **buildtenant.xsd** は **\$NX_ROOT/site/cfg** に格納されるため、このファイルをコピーする必要はありません。

-h

pdm_buildtenant の使用情報を表示します。

構成ファイルの形式を以下に示します。

```
<?xml version="1.0" encoding="utf-8" ?>
<BuildTenant>
  <Object from="MajicObjectName">
    <Attribute from="sourceAttribute1" to="tenantAttribute1" />
    <Attribute from="sourceAttribute2" to="tenantAttribute2" />
  </Object>
</BuildTenant>
```

Object タグの *from* 属性は、テ事前テナント オブジェクトを示しています。各 Attribute タグは、テナント前オブジェクトから新しいテナントの属性にコピーされる属性を識別します。

重要: UNIX でのマルチテナンシーの実装では、`pdm_settenant` および `pdm_buildtenant` ユーティリティを実行する前に、`pdm_task` を実行して、`LIBPATH` をエクスポートする必要があります。これらのユーティリティを実行する前に、`pdm_task` を実行しないと、システム エラーが発生します。 `../pdm_task` を使用してコマンドを実行します。

pdm_clean_attachments - テナント データ インポート後の重複する添付ファイルの削除

テナント データをインポートした後、不要な添付ファイルを削除する必要があります。このユーティリティの構文は、以下のようになります。

```
pdm_perl pdm_clean_attachments.pl [-h] | [-n repository_name] | [-S|-K]
```

-h

コマンドライン ヘルプを表示するように指定します。

-n repository_name

処理するリポジトリの名前を指定します。指定されない場合、すべてのリポジトリが処理されます。

-S

CA SDM リポジトリのみを処理するように指定します。

-K

ナレッジマネジメント および埋め込みイメージ リポジトリのみを処理するように指定します。

注: 引数なしで `pdm_clean_attachments.pl` コマンドを実行すると、すべてのリポジトリが処理されます。

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_settenant - オブジェクトへのテナントの割り当て

テナントを定義した後、`pdm_settenant` ユーティリティを使用して、ほかのオブジェクト内のテナント列を設定する必要があります。このユーティリティの構文は、以下のようになります。

```
pdm_settenant [-h] [-f [configuration_file] [-r] [-d domsrvr]
```

`-d domsrvr`

(オプション) 使用する `domsrvr` を指定します。この引数が指定されない場合、`pdm_settenant` ではデフォルトの `domsrvr` が使用されます。

`-f configuration_file`

(オプション) 更新するデータとファイル更新のルールを指定する、環境設定ファイルの場所を指定します。この引数を指定しなかった場合、`pdm_settenant` では、`$NX_ROOT/site/cfg` ディレクトリの構成ファイルが使用されます (構成ファイルが `$NX_ROOT/site/cfg` ディレクトリにコピーされた後)。

注: サンプルの `settenant.xml` ファイルを編集することも、ファイルを作成して `$NX_ROOT/site/cfg` ディレクトリにコピーすることも可能です。また、`settenant.xsd` は `settenant.xml` と同じディレクトリにある必要があります。そうでない場合、エラーが表示されます。製品のインストール時に `settenant.xsd` は `$NX_ROOT/site/cfg` に格納されるため、このファイルをコピーする必要はありません。

以下のサンプル XML コードは、このファイルの形式を示しています。

```
<?xml version="1.0" encoding="utf-8" ?>
<SetTenant>
  <Object name="MajicObjectName">
    <TenantRule type="SREL">MajicColumnName</TenantRule>
    <Where>tenant is null</Where>
  </Object>
  <Object name="MajicObjectName">
    <TenantRule type="Name">TenantName</TenantRule>
    <Where>tenant is null</Where>
  </Object>
</SetTenant>
```

各 Object タグは、テナント化される CA SDM オブジェクトを示しています。TenantRule タグは pdm_settenant がテナントを決定する方法を示しており、Where タグでテナント化されるオブジェクトが指定されます。TenantRule タグには、以下の 2 つのタイプがあります。

- type="Name"

名前によって明示的なテナントを指定します。

- type="SREL"

オブジェクト内の SREL 属性を指定します。pdm_settenant は、SREL によって参照されているオブジェクトのテナントをコピーします。

-h

pdm_settenant の使用法が表示されます。

-r

テナントが必要なテーブルごとに行の合計数および null テナント列のある行数を表示するレポートを出力します。

注: -f および -r 引数がどちらも指定されている場合、pdm_settenant は更新の完了後にレポートを出力します。-r 引数のみが指定されている場合、pdm_settenant はレポートを出力しますが、データは更新されません。

引数なしで pdm_settenant を実行すると、使用法が表示されます。デフォルトの環境設定ファイルを使用して pdm_settenant を実行するには、configuration_file 引数なしで -f オプションを指定します。pdm_settenant ユーティリティが設定ファイルを読み取り、設定ファイルで定義されている各ルールを順次処理します。\$NX_ROOT/log ディレクトリ内の pdm_settenant.log ファイルに出力が書き込まれます。

`pdm_settenant` を必要なだけ実行することができます。最初のパスにはかなりの時間を要する場合があります（大規模なサイトでは数時間かかる場合もあります）。その後のパスでは未更新の行を処理するだけなので、実行速度が速くなります。これにより、マルチテナンシー オプションをインストールする前に、データベースを準備できます。

重要: UNIX でのマルチテナンシーの実装では、`pdm_settenant` および `pdm_buildtenant` ユーティリティを実行する前に、`pdm_task` を実行して、`LIBPATH` をエクスポートする必要があります。これらのユーティリティを実行する前に、`pdm_task` を実行しないと、システム エラーが発生します。 `../pdm_task` を使用して、コマンドを実行します。

オブジェクトへのテナントの割り当てに関する注意事項

テナントを定義した後、`pdm_settenant`（オブジェクトへのテナントの割り当て）ユーティリティを使用して、ほかのオブジェクト内のテナント列を設定できます。オブジェクトのテナントを変更する際は、データの整合性を維持するため、関連するテナント化オブジェクトのテナンシーを変更すべきかどうかを考慮する必要があります。これらのオブジェクトの同期の維持に失敗すると、CI、関係、MDR、バージョン指定などからデータが欠落したように見えるようになります。以下の CA CMDB オブジェクトがテナント化されています。

- `nr` - CI 定義
- `nr_com` - CI に関連付けられているログ エントリ
- `bmhier` - CI に関連付けられている関係
- `mdr_idmap` - MDR プロバイダ定義
- `ci_mdr_idmap` - CI/MDR 統一マッピング

`pdm_settenant` を使用してテナンシーを変更する場合、各 CI に対して、以下の手順を実行してデータを同期します。

- CI オブジェクト名の `nr` を指定します。
- `nr_com` の CI に関連付けられたログ エントリを変更して、新しいテナントのログ エントリを表示できるようにします。

注: `pdm_settenant` コマンドの詳細については、「管理ガイド」を参照してください。

例: テナントとログを変更するための XML

以下の XML は、CITest という名前の CI を T2 に変更し、nr_com 内の対応するログ エントリも変更します。

```
<TenantRule type="Name">T2</TenantRule>
<Where>name = 'CITest'</Where>
</Object>
<Object name="nr_com">
<TenantRule type="Name">T2</TenantRule>
<Where>asset_id.name = 'CITest'</Where>
¥</Object>
```

pdm_tenant_delete - データベースからのテナント データの削除

pdm_tenant_delete ユーティリティを使用すると、指定したテナントのすべてのデータがデータベースから削除されます。

重要: *ca_* テーブル上の参照制約を、*pdm_tenant_delete* を実行する前に削除し、後で回復する必要があります。

このユーティリティの構文は、以下のようになります。

```
pdm_tenant_delete -h|-t tenant_name [-C|-R] [-Q]
```

-h

pdm_tenant_delete の使用方法が表示されます。

-t *tenant_name*

削除するデータのテナント名を指定します。

注: データを削除するためにこのユーティリティを使用するには、まずテナントを非アクティブに設定する必要があります。

-C

テナントのすべての連絡先を非アクティブに設定するように指定します。連絡先は製品間で共有されている可能性があるため、デフォルトの論理では、明示的に要請されない限り、連絡先の一括削除や一括非アクティブ化が実行されないようにしてください。

注: -R オプションが指定された場合、このオプションは無視されます。

-R

テナント オブジェクト自体も含めて、`ddict.sch` 内で `CA_COMMON` に設定されているすべてのテナント化済みテーブル内のすべての行を削除するように指定します。

重要: これらのテーブルは複数の製品間で共有されるため、このオプションの使用には注意が必要です。

-Q

データベース クエリをできるだけ速く実行するためのクイック クエリ処理を指定します。この引数が指定されない場合、ユーティリティではバックグラウンドクエリ処理を使用して、クエリ処理を除いてアイドル状態の場合にのみクエリを実行します。この引数によって、実行時間は短縮されますが、アクティブなシステムへの影響は大きくなります。

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_tenant_extract - テナント データの抽出

pdm_tenant_extract ユーティリティを使用すると、指定したテナントのすべてのデータがデータベースから抽出されます。データは *pdm_userload* 形式で抽出されるため、別のデータベースへのロードが容易になります。このユーティリティの構文は、以下のようになります。

```
pdm_tenant_extract -h | -c control_file [-d domsrvr] [-g yes|no] [-o output_file]
                    -p phase [[-t tenant_name]...] [-Q] [table1 [table2...]]
```

-h

pdm_tenant_extract の使用方法が表示されます。

-c control_file

このテナント抽出用制御ファイルの場所を指定します。初期フェーズでは、ファイルは指定した場所に作成されます（事前に存在してはいけません）。更新フェーズおよび最終フェーズでは、ファイルが存在している必要があります。

-d domsrvr

（オプション）使用する **domsrvr** を指定します。

-g yes|no

（オプション）パブリック データが出力ファイルに含まれているかどうかを指定します。この引数が指定されない場合、すべてのテーブルからのパブリック データが含まれています。

-o output_file

（オプション）出力ファイルの場所を指定します。この引数が指定されない場合、出力は **stdout** に送られます。

-p phase

抽出のフェーズを指定します。以下のいずれかの値を使用します。

I - 初期

U - 更新

F - 最終

-t *tenant_name*

抽出するテナントの名前を指定します。この引数は初期フェーズでは必須で、複数のテナントで繰り返し使用できます。更新フェーズおよび最終フェーズでは有効ではありません。

-Q

データベース クエリをできるだけ速く実行するためのクイック クエリ処理を指定します。この引数が指定されない場合、ユーティリティではバックグラウンドクエリ処理を使用して、クエリ処理を除いてアイドル状態の場合にのみクエリを実行します。

table1 [table2...]

(オプション) 抽出するテーブルを指定します。省略した場合、すべてのテーブルが抽出されます。

重要: 初期フェーズからの出力を、**CA SDM** やほかの製品で使用されていないデータベースにロードする必要があります。初期フェーズのデータからロードした各テーブルは、ロード前に切り捨てが行われています。データベースがすでに使用されている場合、この切り捨てによって、データが失われる可能性があります。

注: データ ロード中に参照に関する問題を回避するために、制約を削除する適切なスクリプトを実行します

(\$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql または \$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql)。ロードが完了した後、同じディレクトリ内にある適切な xxxAddConstraints.sql スクリプトで制約を再適用します。

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。

関連項目:

[テナントデータのエクスポートおよびインポートの方法 \(P. 387\)](#)

pdm_userload - テナント データのロード

pdm_userload ユーティリティは **CA SDM** データベースにデータをロードするために使用します。マルチテナンシーがインストールされていない場合でも、このユーティリティを使用できます。マルチテナンシーでは、追加の引数 (-t) に対するサポートが追加されます。テナント化されたテーブルに挿入/更新された行のテナント列に **ID** を挿入する必要のあるテナントの名前を、この引数によって指定します。指定したテナントは、あらかじめデータベース内に存在している必要があります。

データを抽出する際、以下の手順に従って、**stdlog** のエラーを回避します。

1. データのロードを開始する前に、以下を実行して、**CA SDM** をシャットダウンし、**DBADMIN** モードで再起動します。

Windows

pdm_d_mgr -s DBADMIN を実行します。

UNIX

pdm_init -s DBADMIN を実行します。

2. データ ロード後、**pdm_halt** コマンドを使用して、**CA SDM** をシャットダウンします。
3. 通常モードで **CA SDM** を再起動します。

注: **pdm_userload** ユーティリティの詳細については、「管理ガイド」を参照してください。

自動フェールオーバーを有効にする方法

サーバ状態監視は、サーバが運転負荷にどのように反応するかを観察し、クライアントリクエストへの反応性を追跡します。この監視の目的は、サーバが必要なタスクを行うために十分な容量を常に保持するようにすることによって、サーバ故障を防ぐことです。ほとんどの標準的な状態監視ツールは **HTTP** および **HTTPS** プロトコルによるリモートサーバ監視をサポートします。

CA SDM の自動的なフェールオーバー機能は、以下の HTTP ベースの標準インターフェースを公開します。

- 状態監視インターフェース：バックグラウンドサーバの状態を監視する HTTP(S) インターフェース。また、バックグラウンドサーバの可用性または必要なタスクを行う機能への悪影響が生じたときに、選択されたスタンバイサーバのフェールオーバーを開始する信頼できるフェールオーバー決定を下します。
- フェールオーバー開始インターフェース：サービス断絶を生じることなく、新しいバックグラウンドサーバとして選択されたスタンバイサーバをシームレスに昇格する HTTP (S) インターフェース。

次の手順に従ってください：

1. バックグラウンドサーバおよびすべてのスタンバイサーバに Apache Tomcat をインストールします。

注：Tomcat が JRE 1.7 を使用していることを確認し、Tomcat が CA SDM コンポーネントに対して設定されているポート番号を使用していないことを確認します。

2. (オプション) インストールした Tomcat サーバに SSL を設定します。SSL の設定の詳細については、「[SSL 認証の設定方法](#)」シナリオ、または「[管理者ガイド](#)」を参照してください。
3. バックグラウンドサーバにログインします。
4. healthservlet を展開します。以下の手順に従います。
 - a. `$NX_ROOT/samples/HealthServlet` フォルダから `TOMCAT_HOME/webapps` フォルダに `HealthServlet.war` ファイルをコピーします。
 - b. Tomcat を再起動します。

`HealthServlet.war` ファイルが `webapps` フォルダに展開されます。展開を確認するには、`HealthServlet` フォルダが同じ `webapps` フォルダに作成されたことを確認します。

展開が正常に終了すると、`healthservlet` がヘルスチェックを実行する準備ができます。このチェックには、SLUMP のステータスの確認、および `health.xml` ファイルで定義されている CA SDM プロセスの状態の確認が含まれます。`health.xml` ファイルは、以下の場所にあります。

`TOMCAT_HOME/webapps/HealthServlet/WEB-INF/classes`

5. (オプション) 組織の要件に基づいて、**health.xml** をカスタマイズします。たとえば、**webengine** プロセスを監視する場合があります。CA SDM で定義されるように、正しい **tagname** を持ったプロセスを **health.xml** ファイルに追加します。**tagname** を探すには、以下の手順に従います。
 - a. `$NX_ROOT/pdmconf` ディレクトリから **pdm_startup.i** ファイル、および **pdm_startup** ファイルを開きます。
 - b. 両方のファイルで監視するプロセスを探します。
 - c. 両方のファイルで、変数を照合することにより対応する **tagname** を検索します。

たとえば、**webengin** プロセスは、**pdm_startup.i** ファイルで以下のように定義されています。

```
#define WEBENGINE(_TAG,_HOST,_SLUMP_NAME,_DOMSRVR, _CFG, _WEBDIRECTOR, _RPC_NAME)
```

webengin プロセスは、**pdm_startup** ファイルで以下のように定義されています。

```
WEBENGINE(webengine, $NX_LOCAL_HOST, web:local, domsrvr, $NX_ROOT/bopcfg/www/web.cfg, "", "rpc_srvr:%h")
```

この例から、**webengine** プロセスの **tagname** が **webengine** であることがわかります。

重要: 新しいプロセスを作成している場合、既存のプロセスが **pdm_startup** ファイルでコメントアウトされ、新しいエントリが作成されます。新しいプロセス エントリの中の **tagname** を探すようにします。

重要: **health.xml** をカスタマイズする場合は、**XML** にエラーがないことを確認し、**XML** への変更を反映するため、確実に **Tomcat** を再起動します。

6. すべてのスタンバイ サーバで手順 4 および 5 を実行します。
7. 選択されたサードパーティ ツールを設定して、定期的にバックグラウンド サーバの状態を監視します。状態を監視するには、以下の **HTTP URL** を使用します。

```
http(s)://Background_server_name:port_number/HealthServlet/GetHealth
```

8. バックグラウンドサーバの健全性が下がったときにフェールオーバーロジックを開始するように、選択されたサードパーティ ツールを設定します。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るようにフェールオーバーロジックを設定することをお勧めします。フェールオーバーロジックで以下のフェールオーバーサブレットを使用します。

重要: 事前定義済みユーザのみがアクセス権限を持つように SSL 上のフェールオーバーサブレットを設定することを推奨しました。また、これはフェールオーバーを開始するサードパーティ ツールを設定するときにも当てはまります。

`http(s)://Standby_server_name:port_number/HealthServlet/FailoverServlet`

自動フェールオーバーが有効になります。

9. 設定が正常に終了すると、サードパーティ ツールは `healthservlet` URL を使用して、バックグラウンドサーバの状態監視を開始します。
 - 各サーバタイプには、一連の独自のプロセスがあります。SLUMP およびすべての CA SDM プロセスが正しく動作していれば、サードパーティ ツールは事前定義済みペイロードを持つバックグラウンドサーバからの HTTP 200 レスポンスを以下のように受け取ります。

`AA-Server-Status: All OK!`

`AA-Server-Role: BG`
 - SLUMP または CA SDM プロセスが動作を停止し、再開できない場合は、サードパーティ ツールは事前定義済みペイロードを持つバックグラウンドサーバから HTTP 503 レスポンスを以下のように受け取ります。

`AA-Server-Status: NOT OK!`

`AA-Server-Role: BG`
10. HTTP 503 応答を受け取った場合、サードパーティ ツールは自動的にフェールオーバーロジックを開始します。

第 6 章: カスタマイズ

このセクションには、以下のトピックが含まれています。

[カスタマイズの概要](#) (P. 407)

[認証モジュールを外部サーバに移動する方法](#) (P. 408)

[通知方法のカスタマイズ](#) (P. 416)

[クエリとメッセージのカスタマイズ](#) (P. 426)

[Web インターフェースのカスタマイズ](#) (P. 443)

[イベント ログ データ保存カスタマイズ](#) (P. 577)

[CA Business Intelligence レポートのカスタマイズ](#) (P. 580)

[レガシー レポートのカスタマイズ](#) (P. 599)

第 7 章: カスタマイズの概要

CA SDM を使用すると、さまざまな IT サービス管理機能を実現できます。CA SDM には、サービス管理のニーズを満たす幅広い機能およびベストプラクティスが用意されています。

CA SDM は、デフォルトではほとんどの IT 組織で使用されるプロセスおよび用語と一致するように実装されますが、組織に固有のニーズに合わせて拡張することもできます。CA SDM には以下のようなさまざまなカスタマイズアプローチが用意されているので、各組織に固有のニーズを満たすことができます。

- エンド ユーザによるパーソナル化
- システム規模の環境設定
- ツール ベースでの適応化
- コード レベルでのカスタマイズ

上記のように、CA SDM をカスタマイズするためのさまざまな方法が用意されています。

認証モジュールを外部サーバに移動する方法

CA SDM 内の認証モジュールは、ユーザ認証を行うシングルトン デーモンです。認証モジュールは、標準設定ではプライマリ サーバ上で、高可用性設定ではバックグラウンドサーバ上で実行されます。以下のいずれかのシナリオでは、認証モジュールを外部サーバに移動します。

- 標準設定

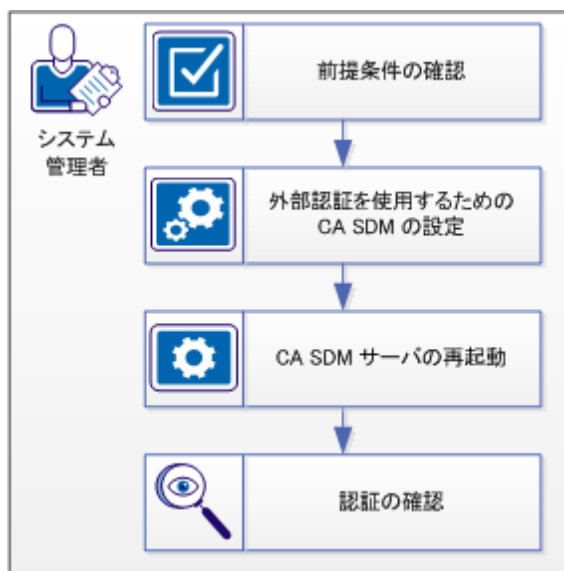
- プライマリ サーバが UNIX または Linux プラットフォーム上にあり、Windows 認証が必要な場合は、認証モジュールを Windows セカンダリ サーバに移動します。
- プライマリ サーバが Solaris プラットフォーム上にあり、CA EEM 認証が必要な場合は、CA SDM が Solaris 上の CA EEM 統合をサポートしていないため、認証モジュールをセカンダリ サーバに移動します。

- 高可用性設定

- バックグラウンドサーバが UNIX または Linux プラットフォーム上にあり、Windows 認証が必要な場合は、認証モジュールを Windows アプリケーション サーバに移動します。
- バックグラウンドサーバが Solaris プラットフォーム上にあり、CA EEM 統合が必要な場合は、CA SDM が Solaris 上の EEM 統合をサポートしていないため、認証モジュールをアプリケーション サーバに移動します。

注: 選択した外部サーバには、CA SDM がインストールされている必要があります。認証モジュールを外部サーバに移動すると、それが単一障害点になります。たとえば、認証モジュールをアプリケーション サーバに移動した場合は、そのアプリケーション サーバがダウンすると、ユーザはログインできなくなります。

以下の図は、認証モジュールを移動する方法を示しています。



認証モジュールを外部サーバに移動するには、以下のタスクを完了します。

1. 前提条件を確認します。
2. [認証モジュールの移動用に CA SDM を設定します。](#) (P. 411)
3. [CA SDM サーバを再起動します。](#) (P. 412)
4. [認証を確認します。](#) (P. 416)

前提条件を確認します。

CA SDM サーバのプラットフォームの分析は、認証モジュールを外部サーバに移動する方法を決定するのに役立ちます。

次の手順に従ってください：

- 設定タイプに基づいて、以下のサーバのオペレーティング システムを識別します。
 - 標準：プライマリ サーバ。
 - 高可用性：アプリケーション サーバ。
- 以下のモデルから、必要な認証のタイプを識別します。
 - UNIX または Linux 上の CA SDM 実装の場合は Windows 認証。
 - Solaris 上の CA SDM 実装の場合は CA EEM 認証。
- 選択した外部サーバに CA SDM がインストールされていることを確認します。

外部認証を使用するための CA SDM の設定

認証リクエストを外部サーバにリダイレクトするには、認証モジュールが存在するターゲット サーバのホスト名を指定する必要があります。認証モジュールを移動するように **CA SDM** を設定するプロセスは、**CA SDM** の標準設定と高可用性設定では異なります。

標準設定

次の手順に従ってください：

1. 管理者としてプライマリ サーバにログインします。
2. コマンドプロンプトから、ディレクトリを `NX_ROOT` 下の `samples¥pdmconf` に変更し、`pdm_perlpdm_edit.pl` を実行します。
3. `pdm_edit.pl` のトップ メニューで、「U」と入力し、Enter キーを押します。
[User Validation server] サブメニューが表示されます。
4. 「E」と入力して外部サーバのホスト名を指定し、Enter キーを押します。
5. プライマリ サーバの場合は「primary」と入力し、セカンダリ サーバの場合はホスト名を入力して、Enter キーを押します。

外部サーバへの認証リクエストのリダイレクトが設定されます。

高可用性設定

次の手順に従ってください：

1. 管理者としてバックグラウンド サーバの Web インターフェースにログインします。
2. [管理] タブを選択します。
3. [オプションマネージャ] - [セキュリティ] を展開します。
4. [オプション] リストの `[bopauth_nxd_host]` エントリをクリックします。
[bopauth_nxd_host オプションの詳細] ページが表示されます。
5. [編集] をクリックします。
6. [オプション値] ドロップダウン リストから、ターゲット サーバのホスト名を選択します。

7. [保存] をクリックします。

注: デフォルトでは、認証モジュールはバックグラウンドサーバ上で実行されます。

外部サーバへの認証リクエストのリダイレクトが設定されます。

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 \(P. 412\)](#)。
- [高可用性設定で CA SDM サーバを再起動します \(P. 412\)](#)。

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 \(P. 413\)](#)。
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. 414)。
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. 414)。
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。

認証の確認

認証タイプに基づいて、Windows または CA EEM に対応する連絡先レコードを持つユーザ ID を使用して認証を確認します。ログインが成功した場合は、認証モジュールが正常に移動されたことを示します。

次の手順に従ってください：

1. ブラウザを起動し、CA SDM の URL を入力します。
2. 認証タイプに基づいて、Windows または CA EEM に対応する連絡先レコードを持つユーザ名を使用して CA SDM にログインします。

モジュールが正常に移動されている場合は、Service Desk のホーム ページが開きます。

通知方法のカスタマイズ

CA SDM の自動通知方法は、サービス デスク管理プロセスの主要担当者に通知を出します。標準的な通知方法は以下のとおりです。

- 電子メール
- 通知（ログ）
- ポケットベルの電子メール

カスタマイズした通知方法を定義して、新しい送信方法（ボイスメール、掲示板、特定のプリンタなど）を指定することもできます。別のアプリケーションからデータにアクセスして、通知メッセージにデータを含めることもできます。

通知プロセス

案件、変更要求、およびリクエストに関して出されるチケット通知は、チケットの保存時に以下のようにして処理されます。

- 通知方法が電子メールなどの「通知」以外の場合、通知プロセッサは、リストの連絡先ごとに通知方法を実行します。一般にこの方法では、新しいプロセスで開始される実行可能ファイルやシェルスクリプトを使用します。通知の詳細は、実行可能ファイル/スクリプトから簡単にアクセスできる環境変数内に保存されます。
- 通知プロセッサは、[アクティビティ通知の詳細] ウィンドウの [メッセージテンプレート] ノートブック ページで指定された [通知メッセージタイトル] と [通知メッセージ本文] の情報を使用して、リクエストされた通知ごとに `NX_NTF_MESSAGE` 環境変数と `NX_NTF_SUMMARY` 環境変数を設定します。受信者が有効な連絡先の場合、その連絡先の [連絡先の詳細] レコードの情報を使用して、追加の環境変数が作成されます。
- 通知で [ファイルに書き込む] オプションが選択されている場合は、詳細情報のテキスト ファイルが作成されるため、通知方法はこのファイルからより詳細な情報を取得できます。
- 通知を受信する連絡先のリストは、[アクティビティ通知の詳細] ウィンドウの [オブジェクト]、[連絡先]、[タイプ]、[調査] の各ノートブック ページで指定された情報から作成されます。連絡先の通知方法が通知レベルと一致し、オプション マネージャの `log_all_notify` オプションがインストールされている場合、通知は最初に通知ログに生成されます。

通知方法の変数

作成される変数には以下の 2 種類があり、これらを通知方法で使用できます。

基本の環境変数

通知オプションの [ファイルに書き込む] を選択したかどうかには関係なく、最初の変数セットは、送信されるすべての通知に対して作成されます。これらの変数は、標準の通知方法がアクセスできる環境変数として環境内に書き込まれます。通知方法の [ファイルに書き込む] オプションを選択した場合、これらの変数は通知セクションの通知ファイルにも書き込まれます。

以下の環境変数は、通知に関する基本情報を提供します。これらの変数は、対応する値が空の場合でも常に定義されます。

環境変数	説明
NX_NTF_MESSAGE	完全なメッセージテンプレートテキスト(すべての変数が完全に展開されて含まれる)
NX_NTF_SUMMARY	完全なメッセージテンプレートヘッダ(すべての変数が完全に展開されて含まれる)
NX_NTF_URGENCY	通知の緊急度 (1 は低、4 は緊急)

以下の環境変数は、受信者が **CA SDM** の有効な連絡先の場合にのみ作成されます。この場合、環境変数は、以下の表に示す受信者の連絡先の詳細レコードの値を使用して設定されます。

変数	[連絡先の詳細]ウィンドウのフィールド
NX_NTF_BEEPER_PHONE	ポケットベル番号
NX_NTF_COMBO_NAME	姓、名、Middle Name
NX_NTF_CONTACT	ID の連絡先
NX_NTF_EMAIL_ADDRESS	電子メールまたはポケットベルの電子メールのアドレス (通知タイプによって異なる)
NX_NTF_FAX_PHONE	FAX 番号
NX_NTF_PUBLIC_PHONE	電話番号
NX_NTF_USERID	ユーザ ID
NX_NTF_VOICE_PHONE	その他 電話番号

注: これらの変数は、対応する値が空の場合は作成されません (ただし、NX_NTF_CONTACT は空にできないため、必ず変数が作成されます)。

属性変数

2 番目の変数セットは属性変数と呼ばれ、通知方法を定義するときに「ファイルに書き込む」を選択した場合にのみ使用できます。これらの変数は通知ファイルにのみ書き込まれ、環境には書き込まれません。形式は以下のとおりです。

`NX_NTF_attribute[.secondary_attribute]=value`

各項目は以下のとおりです。

属性

値を取得する属性の名前。これはオブジェクトに定義されている属性名です。任意のオブジェクトのすべての属性名の詳細については、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。通知に関連付けられる最も一般的なオブジェクトは、チケット(オブジェクト名はチケットのタイプによって異なり、リクエストの場合は `cr`)と、受信者を特定する連絡先(オブジェクト名は `cnt`)です。たとえば、チケットの `description` 属性の環境変数は、通知ファイルでは以下のように示されます。

`NX_NTF_DESCRIPTION=This is a sample description.`

secondary_attribute

最初の属性が別のオブジェクトの内部 ID である場合は、よりわかりやすい情報を示すために、ドット表記を使用してセカンダリ属性が添付されることがよくあります。データベース用語では、属性とは単なるデータ値ではなく、別のテーブルの行を指す外部キーです。この未処理のキー値を使用しても、ほとんど意味がありません。このようなフィールドの多くは、自動的に解決または逆参照されます。この場合、**secondary_attribute** は参照されるテーブルの値になります。たとえば、担当者の連絡先レコードの固有 ID として実際に保存される **assignee** 属性の値を書き込む代わりに、以下の例に示すように、連絡先オブジェクトの **combo_name** 属性を参照する担当者の名前が書き込まれます。

NX_NTF_ASSIGNEE.COMBO_NAME=Armstrong, Beth

属性に値がない場合、対応する値は(NULL)または空白になるのが一般的です。以下に例を示します。

NX_NTF_CALL_BACK_DATE=(NULL)

NX_NTF_GROUP.COMBO_NAME=

注: チケットと受信者の両方に存在する属性変数は **NX_NTF_ID** (id 属性) です。これはオブジェクトの固有データベース ID です。

通知ファイル

通知方法の定義時に「ファイルに書き込む」オプションを選択すると、すべての基本環境と属性変数がテキストファイルに書き込まれます。このファイルは、通知方法スクリプトまたはプログラムの実行前に閉じられます。この通知ファイルは、連絡先に対する通知方法が呼び出されるたびに書き込まれます。これは、ほかの方法では取得できない関連情報を通知スクリプトに渡す、便利な機能です。

通知ファイルの完全パスは、通知方法のプロセスで使用できる `NX_NTF_FILENAME` 環境変数で設定されます。ファイル名は、通知方法を定義するときに [通知方法] フィールドに入力した値の終わりにも追加されます。たとえば、[通知方法] に「`pdm_perl - w mymethod.pl`」と入力すると、実際のプロセスでは「`pdm_perl - w mymethod.pl unique_notification_file_name`」が実行されます。

重要: 管理者は通知ファイルをクリーンアップすることができます。大量の通知を使用するサイトでは、1日に何千もの通知ファイルが作成されることになるため、ファイルをクリーンアップすることは非常に重要です。ファイルは、標準の一時ディレクトリ (Windows では `TEMP`、UNIX では `TMP`) に置かれます。通知方法のスクリプトまたはプログラムの終了時に、ファイルを削除するという方法もあります。

通知ファイルは、複数のセクションに分割された標準テキスト ファイルです。各行には属性/値ペアまたはセクションマーカが記述されています。各通知ファイルには以下に説明するような 3 つのセクションがあります。セクションは、後ろに改行のある「-----」で始まります。

`SECTION=obj`。obj はチケットのオブジェクト タイプを示します。

`Iss`

案件に関する情報を提供します。

`Chg`

変更要求に関する情報を提供します。

`Cr`

リクエストに関する情報を提供します。

`SECTION=cnt`

受信者に関する情報を提供します。

`SECTION=notification`

基本の環境変数から得られるものと同じ情報を提供します。

注: 実際に、チケットおよび受信者のセクション名は、そのセクションの属性のオブジェクト名です。任意のオブジェクトのすべての属性名の詳細については、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。

各セクションには、属性/値ペアの行が数行含まれ、それぞれが対応するオブジェクトの属性を表します。これらの行の形式と意味についての詳細は、このセクションの「属性変数」に記載されています。

属性値の改行は、通知ファイルの新しい行として再現されます。通知方法プロセスでは、**NX_NTF** およびセクション マーカーで開始する属性または値の行のみを使用することができます。通知方法プロセスで通知ファイルを使用する前に、サンプル ファイルを生成してそのコンテンツを確認します。

関連項目:

[属性変数](#) (P. 419)

[基本の環境変数](#) (P. 417)

Perl スクリプトの使用

ほとんどの通知方法では、実行可能ファイルまたはシェルスクリプトを呼び出して環境変数を読み取り、メッセージを送信します。このアクションは、ほとんどの **UNIX** サーバでは問題なく動作しますが、**Windows** サーバでは環境変数の読み取りで問題が発生します。

Windows での環境の問題は、Perl スクリプトを使用して解決できます。**CA SDM** には、すぐに使用できる、**pdm_perl** という Perl インタープリタが含まれています。**pdm_perl** を使用して通知方法として呼び出された Perl スクリプトでは、環境変数を確実に取得できます。Perl スクリプトは環境変数値を読み取ってフォーマットし、ポケットベルの呼び出しや電子メールの送信など、ほかの通知を続けて処理します。

Windows ベースのサーバの場合は、`launchit` ユーティリティの使用を検討します。このユーティリティには、適切な環境変数を設定し、コマンドプロンプトに似たシェル環境でスクリプトやプログラムを呼び出す機能があります。

たとえば、ここで説明している複数の環境変数を読み取る `read_env.pl` という Perl スクリプトを作成するとします。この場合は、[通知方法の詳細] ウィンドウの [通知方法] フィールドに以下のように入力して、そのスクリプトを通知用に呼び出すことができます。

```
pdm_perl script_path/read_env.pl
```

この通知方法は Perl インタープリタを起動し、`read_env.pl` スクリプトの命令を実行します。

カスタマイズした通知方法を作成する方法

カスタマイズした通知手順を作成するには、以下の手順に従います。

1. メッセージテンプレートを処理し、受信者に送信するためのスクリプトを作成します。スクリプトは、プラットフォームに応じた実行可能ファイルとして作成できます。サードパーティやパブリック ドメインのインタープリタを使用することもできます。- 一般には、UNIX では Bourne のシェル スクリプトが使用され、Windows では .bat ファイルが使用されます。特別なテンプレートが必要なスクリプトの場合は、テンプレートを作成する必要があります。
2. Web インターフェースを使用して、サイトに新規の通知方法を追加します。

関連項目：

[スクリプトの作成](#) (P. 423)

[通知方法の追加](#) (P. 424)

スクリプトの作成

以下の手順に従って、通知方法のスクリプトを作成します。

1. 通知の配布方法（たとえば、特定のプリンタでの印刷など）を決定します。
2. 通知メッセージの内容を決定します。

3. 通知に含めるメッセージテンプレートの情報を指定します。
4. 通知を送信するスクリプトを設定します。
5. このスクリプトを実行可能ファイルに含め、CA SDM サーバのパスに置きます。

通知方法の追加

スクリプトを作成したら、新規の通知方法を CA SDM に定義する必要があります。通知方法の追加には、2つの方法があります。

- Web インターフェースを使用
- UNIX シェル スクリプトを使用

関連項目：

[Web インターフェースを使用した通知方法の追加 \(P. 424\)](#)

[UNIX シェル スクリプトを使用した通知方法の追加 \(P. 425\)](#)

Web インターフェースを使用した通知方法の追加

Web インターフェースを使用して通知方法を追加します。

Web インターフェースを使用して通知方法を追加する方法

1. [管理インターフェース] の [通知] から [通知方法] を選択します。
[通知方法リスト] が表示されます。
2. [新規作成] ボタンをクリックします。
[通知方法の新規作成] ウィンドウが表示されます。
3. 以下のフィールドにデータを入力します。

シンボル

(必須) 通知方法を特定します。

ファイルに書き込む

このチェック ボックスをオンにすると、通知方法のコンテキスト情報がファイルに書き込まれます。

説明

通知方法の説明を入力します。

通知方法

通知方法の実行可能スクリプトの完全パスを指定します。システムパスを使用してスクリプトまたはプログラムを解決できる場合は、フルパスの指定は不要です。Windows サーバの場合は、**launchit.exe** ユーティリティを使用してスクリプトまたはプログラムを呼び出すことを検討してください。

注: **launchit** ユーティリティの詳細については、オンラインヘルプを参照してください。

注: 通知方法は **CA SDM** サーバから実行されるため、通知方法スクリプトをサーバのパスからアクセスできるディレクトリに置くか、スクリプトの完全パスを指定する必要があります。UNIX の場合、実行しているシェルによっては、以下のコマンドを実行してパスを確認できます。

```
which pathname_to_script
```

通知方法で問題が生じた場合は、**\$NX_ROOT/log** ディレクトリ (UNIX)、または **\$NX_ROOT¥log** ディレクトリ (Windows) にあるログを確認してください。

UNIX シェル スクリプトを使用した通知方法の追加

以下の手順では、通知メッセージをサービス デスク プリンタ **SDPR2** に送信する通知メソッドのシェル スクリプトを作成します。この例では、メッセージテンプレートのメッセージヘッダおよびメッセージテキストから通知メッセージを構成します。

1. 通知テキストを作成して送信するシェル スクリプトは、以下のようにして設定します。

```
#!/bin/sh
echo "
TO:      $NX_NTF_USERID
SUBJECT: $NX_NTF_SUMMARY
MESSAGE:
$NX_NTF_MESSAGE" |lp -dSDPR2
```

2. 実行可能ファイルに **sd_print** という名前を付け、サイトの共通スクリプトで使用するディレクトリ (たとえば **/usr/local/netbin** など) に置きます。

3. `chmod` を使用して、このシェル スクリプトを実行可能ファイルにします。
4. [管理インターフェース] の [通知] から [通知方法] を選択します。
5. [ファイル] メニューから [新規作成] を選択します。
6. 以下のフィールドにデータを入力します。

シンボル

SDPR2

説明

バックアップ通知をサービス デスクのプリンタ **SDPR2** に送信します。

通知方法

`/usr/local/netbin/sd_print`

7. [保存] ボタンをクリックして、新規レコードを保存します。次に [ウィンドウを閉じる] をクリックして、詳細ウィンドウを閉じます。

クエリとメッセージのカスタマイズ

CA SDM は、情報を絞り込むための機能を多数備えており、その時々状況に見合ったリクエスト、変更要求、および案件に的を絞って作業に専念できます。たとえば、クエリの保存機能を使用すると、管理インターフェースまたは **Web** インターフェースのスコアボードで関連情報を確認することができます。また、チケットアクティビティの主要担当者への通知メッセージをカスタマイズする機能もあります。

ストアドクエリを使用すると、ユーザに関連するチケットに絞って、管理インターフェースおよび **Web** インターフェースのスコアボード領域にあるカウンタ フィールドをカスタマイズできます。- アクティビティ通知メッセージをカスタマイズして、アクティビティ ログ オブジェクトの属性および特定のチケットの情報を含めることができます。

関連項目:

[スコアボードクエリ](#) (P. 427)

[ITIL 固有のクエリ](#) (P. 434)

[アクティビティ通知メッセージのカスタマイズ](#) (P. 435)

スコアボード クエリ

データベース内のテーブルの 1 つである **Cr_Stored_Queries** では、ストアドクエリを定義します。このストアドクエリは SQL クエリに似ています。これを使用して、管理インターフェースおよび Web インターフェースのスコアボード領域にあるノードのカウンタ フィールドをカスタマイズできます。カウンタ フィールドには、クエリと一致するレコードの件数が表示されます。たとえば、ログイン ユーザに割り当てられている各種リクエストの数を表示することができます。 -

ユーザは、各自のスコアボードに表示されるカウンタ フィールドをカスタマイズできます（これについてはオンライン ヘルプを参照してください）。ただし、ストアドクエリとしてこれらのカウンタ フィールドに示される各種リクエストについては、最初にシステム管理者が定義する必要があります。スコアボード クエリの詳細については、「管理ガイド」を参照してください。

注: データベース クエリの値が **NULL** の場合は、スコアボードのカウントが正しい値になりません。たとえば、スコアボード クエリの指定が **assignee.organization = xyz** で、レコードの担当者フィールドが空白 (**NULL**) の場合、そのレコードはスコアボードのカウントに含まれません。

ログイン ユーザのストアド クエリ

[ストアドクエリの詳細] ウィンドウの [Where 節] と [ラベル] の 2 つのフィールドは、必ず定義する必要があります。この両方のフィールドには、ログイン ユーザ用にカスタマイズした式を含めることができます。 - スストアドクエリはテーブル名と列ではなく、オブジェクトと属性を参照します。ログイン ユーザ用にカスタマイズされたストアドクエリは、以下の 2 つから構成されます。 -

オブジェクト(たとえば、リクエストの場合は cr)

一般にオブジェクトは、等号 (=) の左側に指定されます。ストアドクエリのこの部分の構文は、以下のとおりです。

```
att_name[.att_name...].SREL_att_name
```

ストアドクエリには必ずタイプを指定します。タイプはクエリの実行対象のオブジェクト名で、クエリのコンテキストを示します。上記の構文では、最初の **att_name** をコンテキスト オブジェクトの属性名にする必要があります。

ログイン ユーザ(このユーザの cnt オブジェクトのインスタンス)-

ログイン ユーザの属性に基づいてチケットを選択する場合は、ログイン ユーザを等号(=)の右側に指定する必要があります。- ストアドクエリのこの部分の構文は、以下のとおりです。

`@att_name[.att_name...].SREL_att_name`

注: オブジェクトおよび属性の詳細については、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。

cr オブジェクトの構文

リクエスト (cr) オブジェクトを参照する場合は、以下の構文を使用します

`att_name[.att_name...].SREL_att_name`

以下の例では、チケットの処理を割り当てられた担当者のロケーションを指定します。この例では、ストアドクエリのタイプが cr オブジェクトを暗黙的に示しているため、オブジェクト名は省略されています。

`assignee.location=@cnt.location AND active=1`

担当者"%y"たんとうしゃ

リクエスト オブジェクトの属性で、対応するテーブルの `assignee` フィールドにマップします。たとえば `assignee` 属性は、`SREL agt` を指定した cr オブジェクトで定義されます。つまり、`agt` ファクトリを参照します。`agt` ファクトリは `cnt` オブジェクト定義の一部です。

ロケーション

`cnt` オブジェクトの属性で、連絡先テーブルの `c_l_id` フィールドにマップしています。`location` 属性は、`SREL loc` を指定した `cnt` オブジェクトで定義されます。つまり、`loc` オブジェクトを参照します。

WHERE 節

以下の例は、WHERE 節にコーディングできる値を示します

`assignee.location=@cnt.location AND active=1`

ストアドクエリのタイプがリクエストである場合、このクエリは担当者とログイン ユーザのロケーションが同じであるアクティブ リクエストをすべて選択します。-

ラベル

cnt オブジェクトの属性は、WHERE 節に含める場合と同じ方法でラベルに含めることができます。ラベル内で cnt オブジェクトの属性を使用する場合の例を以下に示します。

```
@cnt.location.name Calls
```

このラベルにはロケーションの名前が含まれます。たとえば Phoenix である場合、ラベルがウィンドウに表示されるときに @cnt.location.name が Phoenix に置き換わり、Phoenix Calls というラベルが表示されます。

IN キーワード

IN キーワードを使用すると、ストアドクエリで結合を作成せずに 2 つ以上のテーブルを参照できます。そのため、クエリ実行の効率が飛躍的に高まります。IN キーワードは、以下のようにコーディングします。

```
SREL_att_name IN ( value1 [, value2 [,...]] )
```

たとえば、リクエストクエリは以下のようにコーディングできます。

```
category.sym IN (¥'Soft¥', ¥'Email¥')
```

この結果の SQL WHERE 節は以下のようになります。

```
category IN (SELECT persid FROM prob_ctg WHERE sym LIKE 'Soft%' OR sym = 'Email')
```

IN を使用する理由の 1 つは、直積を避けるためです。たとえば、以下のクエリの結果は直積となり、効率が非常に悪くなります。

```
assignee.last_name LIKE 'MIS%' OR group.last_name LIKE 'MIS%'
```

IN を使用すると直積が作成されず、以下の例に示すように、結合さえも作成されません。

```
assignee.last_name IN 'MIS%' OR group.last_name IN 'MIS%'
```

注: 通常 IN の右側のリストを囲むために使用するかっこは、リストに 1 つしか値がない場合は省略することができます。これと同様に、データパーティションを変換することにより、データパーティション内での結合を避ける必要があります。

```
assignee.last_name LIKE 'Smith'
```

変換後

```
assignee = U'374683AA82ACE34AB999A042F3A0BA2E'
```

各項目は以下のとおりです。

U

値が uuidであることを示します。

'374683AA82ACE34AB999A042F3A0BA2E'

単一引用符で囲まれた 32 文字は、実際の uuid の文字列表現です。

このようにすると、多少明確さに欠けますが、結合を避けることができます。IN を使用すれば、上記のクエリを以下の例のように記述できます。この場合、最初の例の明確さと、2 つ目の例の効率の良さを保つことができます。

```
assignee.last_name IN 'Smith'
```

CA SDM では、QREL リストまたは BREL リストに適用される IN 節をサポートしています。たとえば、特定のアセット (ID は 374683AA82ACE34AB999A042F3A0BA2E) の親となるアセットを持つリクエストをすべて検索する場合、該当の Where 節は以下のようになります。

```
affected_resource.[parent]child_hier.child IN  
(U'374683AA82ACE34AB999A042F3A0BA2E')
```

この IN 節の最初の部分 (*affected_resource*) は、*cr* (リクエスト) オブジェクトの *SREL* (外部キー) であり、*Network_Resource* テーブルを指しています。*child_hier* の部分は、階層関係を指す *hier* オブジェクトのリストです。最後の部分 (*child*) は、IN サブクエリの *where* 節の最初の部分を形成します。*374683AA82ACE34AB999A042F3A0BA2E* の部分は、*child* に一致する外部キー値です。*[parent]* は、返されるサブクエリを指定します。ID 値は UUID の文字列表現であるため、そのように指定し、
「U'374683AA82ACE34AB999A042F3A0BA2E'」と記述する必要があります。

以下の例は実際に生成される SQL で、特定のアセットの親となっているアセットを持つリクエストをすべて返します。

```
SELECT Call_Req.id FROM Call_Req WHERE Call_Req.affected_rc IN (SELECT hier_parent
FROM Asset_Assignment WHERE hier_child = U'374683AA82ACE34AB999A042F3A0BA2E')
```

複数の親に対してクエリを実行する場合は、以下のように SQL の () 内にカンマで区切って指定します。

```
affected_resource.[parent]child_hier.child IN (U'374683AA82ACE34AB999A042F3A0BA2E',
U'374683AA82ACE34AB999A042F3A0BA2E')
```

角かっこ ([]) で囲まれた属性名は、サブ節の **SELECT** 部分を形成するために使用されます。以下の例のように、Unicenter Service Desk バージョン 6.0 に装備されているグループストアドクエリでは、角かっこ表記は使用しません。

```
(assignee = @cnt.id OR group.group_list.member IN (@cnt.id)) AND active = 1
```

注: 角かっこ表記が使用されていない場合、SQL サブシステムは、これをドット表記部分の最初のシンボルの属性名と見なします。この例の場合は、*group_list* オブジェクトに「*group*」という名前の属性があるため、問題なく処理されます。ただし、別の名前が指定されていた場合は、**Where** 節の解析は失敗します。同等の節で角かっこを使用した場合は、以下のようになります。

```
(assignee = @cnt.id OR group.[group]group_list.member IN (@cnt.id)) AND active = 1
```

注: ドット表記は延長できません。たとえば、以下の例は無効です。

```
affected_resource.[parent]child_hier.child.name IN ('chicago1')
```

優先度ベースのクエリ

データベースの **Priority** テーブルには、**sym** および **enum** の 2 つの列があります。ユーザに対して表示される値は **sym** の値です。ただしアプリケーションは、**enum** 値に基づいて **sym** を参照します。現時点では、**sym** 値の初期設定は 1～5 で、対応する **enum** 値はこれと逆になります。

例

Sym	列挙
1	5
2	4
3	3
4	2
5	1

そのため、ストアドクエリを作成していて 5 の値を参照する場合、**.sym** を使用して検索する属性を指定しなければ、実際には優先度 1 を検索することになります。

重要: 本製品によって割り当てられたデフォルトの **enum** 値を変更しないでください。新規の **sym** 値を追加する場合は、**enum** の最大値から続けて割り当ててください。

時間ベースのクエリ

期間を指定して、時間ベースのストアドクエリを作成できます。期間は、現在の日付を基準にして指定します。たとえば、本日、昨日、先週、先月などを指定できます。期間の名前には、**TODAY** や **YESTERDAY** などがあります。ストアドクエリの時間を参照するには、以下の 2 つのビルトイン関数のいずれかを使用します。

StartAtTime (timespan-name)

期間として記述されている期間の開始点を参照します。

EndAtTime (timespan-name)

期間として記述されている期間の終了点を参照します。

ストアドクエリの構文ルールにより、期間名は単一引用符で囲み、各単一引用符の前にバックスラッシュを付ける必要があります。たとえば、先週の開始点を参照するには、以下のように指定します。

```
StartAtTime(¥'PAST_WEEK¥')
```

期間の参照を含むストアドクエリは、時間の経過に伴って定期的に更新する必要があります。たとえば、「昨日」という期間は深夜 0 時に切り替わります。期間を更新するための [開始時間]、[終了時間]、[トリガ時間] は、[期間の詳細] ウィンドウで指定します。

開始時間

[開始時間] には、期間の開始時期を絶対期間または相対期間で指定します。以下の表は、[期間の詳細] ウィンドウの [開始時間] セクションのフィールドの説明です。

年

2000 などの具体的な年、または +1（翌年）や -1（昨年）などの相対的な年

月

1（1 月）から 12（12 月）までの具体的な月、または +1（翌月）や -1（前月）などの相対的な月

日

1 ～ 31 の具体的な日、または +1（翌日）や -1（昨日）などの相対的な日

時間

0 ～ 24 の具体的な時間、または +1（1 時間後）や -1（1 時間前）などの相対的な時間

分

1 ～ 59 までの具体的な分、または +1 や -1 などの相対的な分

終了時間

[終了時間] には、期間の終了時期を絶対期間または相対期間で指定します。[期間の詳細] ウィンドウの [終了時間] セクションのフィールドは、[期間の詳細] ウィンドウの [開始時間] セクションのフィールドと同じです。

トリガ時間

[トリガ時間] フィールドは、期間の参照を含むストアドクエリの **WHERE** 節を再作成して、ストアドクエリを更新するタイミングを指定します。以下の表に示すように、[トリガ時間] には、現在の時間からの相対時間を指定する必要があります。

年

-1（昨年）から +36（36 年後）の間の相対的な年数

月

-1（前月）から +11（11 か月後）の間の相対的な月数

日

-1（昨日）から +31（31 日後）の間の相対的な日数

時間

-1（1 時間前）から +23（23 時間後）の間の相対的な時間

分

+9（9 分後）から +59（59 分後）の間の相対的な分数

ITIL 固有のクエリ

問題およびインシデントは、「**type**」属性の 2 つの値である、インシデントを表す「I」と問題を表す「P」のいずれかを指定したリクエストです。

以下のストアドクエリは、担当者の組織またはグループの組織が、ログインしているアナリストの組織と同じであるインシデントをすべて取得します。

```
assignee.organization IN @cnt.organization OR group.organization IN @cnt.organization) AND active = 1 AND type = ¥'I¥'
```

問題に関するクエリはインシデントと同じですが、**type = ¥'P¥'** となる点が異なります。

アクティビティ通知メッセージのカスタマイズ

リクエストのアクティビティが発生したときに、自動的に通知メッセージを送信することができます。

注: 通知メッセージ、およびアクティビティ通知の定義手順の詳細については、「管理ガイド」を参照してください。

[アクティビティ通知の詳細] ウィンドウで定義する必要のある 2 つのフィールドは、[通知メッセージ件名] と [通知メッセージ本文] です。この 2 つのフィールドには、アクティビティ ログ オブジェクト（リクエスト/インシデント/問題の場合は **alg**、変更要求の場合は **chgalg**、案件の場合は **issalg**）の属性を含めることができます。この 3 つのアクティビティ ログ オブジェクトはほとんど同じで、アクティビティに関する特定のリクエストを識別できます。

アクティビティ通知の属性のフォーマット

以下に示したプロパティを使用すると、オプションで個々の属性をフォーマットおよびエスケープできます。この機能は、HTML 標準に合わせて属性内のデータをエスケープする必要がある場合に、HTML 通知をフォーマットするときに特に役立ちます。

フォーマットを含めるには、以下の構文を使用します。

```
@{property=value property=value:attribute_name}
```

プロパティ値のペアは少なくとも 1 つのスペースで区切られ、大文字小文字は区別されません。フォーマットプロパティと属性名は、コロンで区切ります。プロパティが指定されていない場合は、属性に対してフォーマットもエスケープも実行されません。

使用できるフォーマットプロパティは以下の表のとおりです。

Property	説明
DATE_FMT	属性の日付形式を指定します。有効な値は以下のとおりです。 MM/DD/YYYY MM-DD-YYYY DD/MM/YYYY DD-MM-YYYY YYYY/MM/DD YYYY-MM-DD 日付属性に対してのみ有効です。文字列に埋め込まれている日付は、このプロパティの影響を受けません。

Property	説明
ESC_STYLE=NONE HTML URL	フォーマットされたテキストのエスケープ タイプを指定します。 有効な値は以下のとおりです。 NONE 初期設定。コンテンツの本文に特別な処理を行わないことを指定します。 HTML HTML テキストの場合に、以下の文字に対して特別な処理を行います。 ■ &を&amp;に変換 ■ "を&quot;に変換 ■ <を&lt;に変換 ■ >を&gt;に変換 URL 英数字および「@*-_.#」以外のすべての文字を「%xx」に変換します。この「xx」は、変換された文字の 16 進コーディングです。

Property	説明
JUSTIFY=LEFT CENTER RIGHT TRUNCATE WRAP LINE	フォーマットされたテキストの両端揃えを指定します。以下に有効な値を示します。 TRUNCATE （フォーマットする場合の初期設定）正の整数の場合は、WIDTH プロパティの値にテキストを切り捨てます。ESC_STYLE=HTML の場合は、「<」と「>」を「&lt;」と「&gt;」に置き換えて HTML フォーマットを除去します（KEEPLINKS と KEEPTAGS を参照してください）。 LEFT CENTER RIGHT 必要に応じて、文字の切り捨てやスペースの埋め込みを行い、WIDTH で指定されたとおりの文字数にします。改行が埋め込まれている場合は、1 つのスペースに置き換えられます。 ESC_STYLE=HTML の場合は、出力テキストは<pre>タグと</pre>タグで区切られます。WIDTH 引数には正の整数を指定する必要があります。 WRAP テキストの折り返しで単語の境界を無視しない(単語内に改行を入れない) ことを除き、LEFT と同じです。 LINE TRUNCATE と同じです。ただし ESC_STYLE=HTML の場合は、埋め込まれている改行も、すべて
タグに置き換えられます。
KEEPLINKS=YES NO	KEEPLINKS=YES を指定すると、JUSTIFY=LINE または JUSTIFY=TRUNCATE のアクションは、HTML のアンカー タグ（アクション：）を保持するように変更されます。ただし、「<」文字と「>」文字はすべて変換されます。KEEPTAGS と同時に指定することはできません。ESC_STYLE=HTML の場合にのみ有効です。
KEEPNL=YES NO	PDM_FMT の標準アクションでは、埋め込まれているすべての改行と後続のスペースが、1 つのスペースに変換されます。KEEPNL=YES が指定されている場合は、埋め込まれている改行は保持されます。JUSTIFY=LINE の場合、この引数は無視されます。
KEEPTAGS=YES NO	KEEPTAGS=YES が指定されている場合、すべての HTML タグを保持するように、JUSTIFY=LINE または JUSTIFY=TRUNCATE のアクションが変更されます。KEEPLINKS と同時に指定することはできません。ESC_STYLE=HTML の場合にのみ有効です。

Property	説明
PAD=YES NO	PAD=NO を指定すると、PDM_FMT は空の文字列を 1 つのスペースに変換しません。WIDTH がゼロ以外の場合や、JUSTIFY が TRUNCATE または WRAP の場合は、これが標準のアクションです。
WIDTH=nn	ゼロ以外の場合は、WIDTH で指定したとおりの文字数にテキストがフォーマットされます。

たとえば以下のように指定すると、HTML 固有の文字をエスケープし、改行を表す
を追加して、すべての HTML リンクをリンクとして保持することにより、HTML 通知のリクエストの説明をフォーマットすることができます。

```
@{ESC_STYLE=HTML JUSTIFY=LINE KEEPLINKS=YES:call_req_id.description}
```

リクエストの open_date を欧文形式にフォーマットするには、以下のよう指定します。

```
@{DATE_FMT=DD-MM-YYYY:call_req_id.open_date}
```

アクティビティ ログ オブジェクトの属性

アクティビティ ログ オブジェクトの属性を含めるには、以下を [通知メッセージ件名] または [通知メッセージ本文] に含めます。

```
@{att_name}
```

オブジェクト名 (alg、chgalg、または issalg) はデフォルトなので、指定する必要はありません。たとえば、アクティビティのタイプをメッセージタイトルに含めるには、タイトルに含める内容と共に、[通知メッセージ件名] フィールドに以下を入力します。

```
@{type}
```

アクティビティの説明をメッセージ本文に含めるには、本文に含める他のものに加え、以下のように [通知メッセージ本文] フィールドに入力します。

```
@{description}
```

特定の変更要求に関する情報

通知をトリガした特定の変更要求に関する情報を示すメッセージでは、
[通知メッセージ件名] または [通知メッセージ本文] フィールドに、変更要求オブジェクトを参照するアクティビティ ログ オブジェクトが含まれている必要があります。参照は、以下の形式で入力します。

`@{change_id.chg_att_name}`

この参照では、以下の情報が適用されます。

@

この式を置き換えることを示します。

change_id

変更要求オブジェクト (chg) の特定インスタンスにリンクする、アクティビティ ログ オブジェクトの属性。

chg_att_name

chg オブジェクトの任意の属性。

たとえば、変更要求の優先順位をメッセージ タイトルに含めるには、タイトルに含める内容と共に、以下を [通知メッセージ件名] に入力します。

`@{change_id.priority.sym}`

変更要求を報告した担当者（影響を受けるエンドユーザ）をメッセージ本文に指定するには、本文に含めるほかのものに加え、以下のように [通知メッセージ本文] フィールドに入力します。

`@{change_id.requestor.combo_name}`

特定の変更要求の再オープン番号を指定し、以下のようにメッセージを表示させる場合は、以下の構文を使用します。

Reopen Change Order @{change_id.chg_ref_num}

注: 通知をトリガした案件に関する情報を提供するメッセージでは、[通知メッセージ件名] または [通知メッセージ本文] フィールドに、案件オブジェクト **iss** を参照するアクティビティ ログ オブジェクトの属性が含まれていることが必要です。この方法については、このセクションで説明したリクエストおよび変更要求に関する情報、および「**CA SDM テクニカルリファレンスガイド**」で説明しているオブジェクトおよび属性に関する情報を参考にしてください。

たとえば、案件の優先順位をメッセージタイトルに含めるには、タイトルに含める追加情報と共に、以下を [通知メッセージ件名] に入力します。

@{issue_id.priority.sym}

特定のリクエストに関する情報

通知をトリガした特定のリクエストに関する情報を示すメッセージでは、[通知メッセージ件名] または [通知メッセージ本文] フィールドに、リクエストオブジェクトを参照するアクティビティ ログ オブジェクトが含まれている必要があります。この参照は、以下の形式で入力します。

`@{call_req_id.cr_att_name}`

@

この式を置き換えることを示します。

call_req_id

リクエスト オブジェクト (**cr**) の特定インスタンスにリンクする、アクティビティ ログ オブジェクトの属性。

cr_att_name

cr オブジェクトの任意の属性。

たとえば、リクエストの影響をメッセージ タイトルに含めるには、タイトルに含める内容と共に、[通知メッセージ件名] フィールドに以下を入力します。

`@{call_req_id.impact.sym}`

影響を受けるリソースをメッセージ本文に指定するには、本文に含める他のものに加え、以下のように [通知メッセージ本文] フィールドに入力します。

`@{call_req_id.affected_resource.name}`

特定のリクエストの再オープンを番号で指定し、以下のようにメッセージを表示させる場合は、以下の構文を使用します。

Reopen Request `@{call_req_id.ref_num}`

リクエスト（または変更要求や案件）そのものに関連するメッセージを送信する方法は、この他にもいくつかあります。リクエストそのものに関連する場合は、参照の「**call_req_id**」の部分は不要です（指定できません）。したがって、このような場合は、以下の形式を使用する必要があります。

「`@{call_req_id.ref_num}`」ではなく「`@{ref_num}`」

Web インターフェースのカスタマイズ

CA SDM Web インターフェース（別名、ブラウザ インターフェース）は、CA SDM の機能をインターネットを介して提供します。これらの機能には、チケットをオープン、更新、クローズする機能や、アナウンスメントを表示およびポストする機能、サポートするデータ テーブルにアクセスする機能などがあります。このこれらの機能を使用すると、ナレッジ ベースを自力で参照できるため、サービス デスクへのコール数が減り、解決時間を短縮できます。Web インターフェースは完全なカスタマイズが可能で、多くの Web ブラウザで使用できます。

Web インターフェースのインストールと設定を行うと、既存の Web インターフェースに統合したり、ニーズに合わせてカスタマイズしたりできます。カスタマイズするには、HTML、およびサイトで使用している Web ブラウザに関する知識が必要です。

注: WSP のデザイン ビューは、CA SDM コントロール (PDM_MACRO) に関する機能です。CA SDM コントロールが含まれていないフォームを使用する場合、使用できるのは[ソース]タブのみです。従業員および顧客の Web フォームは CA SDM コントロールが含まれていないため、[デザイン] タブではなく [ソース] タブに表示されます。一部のアナリスト フォームも CA SDM コントロールが含まれていないため、[ソース] タブに表示されます。

重要: CA SDM r12.9 では、\$NX_ROOT\$¥site¥mods¥www¥macro ディレクトリ内の pdm_macro のためのカスタマイズされた .mac ファイルは使用されなくなっています。マクロはカスタマイズできません。

重要: カスタマイズのデザインやデバッグ（オンライン ヘルプ システムなどのドキュメントを含む）は、テクニカル サポートのサポート対象外です。テクニカル サポートによって提供されるのは、CA SDM Web インターフェースをカスタマイズするための一般情報です。カスタマイズする場合、カスタマイズの責任はすべてユーザ自身が負うものであることに留意してください。CA SDM テクニカル サポートでは、カスタマイズについてユーザが理解するための支援を提供します。

ここで説明するカスタマイズ方法に関するサポートは、その方法およびファシリティを記載のとおりに行うまでの範囲に限られます。記載されていない機能を使用したり、記載されている機能でも記載の機能範囲を超えて使用することのないように注意してください。上記のような使用はサポートの対象外であり、カスタマイズとは一見無関係なシステム障害やシステムの不安定を引き起こす可能性があります。このような理由から、テクニカルサポートでは、問題を再現するためにカスタマイズを削除するようお客様にお願いすることがあります。あらゆる不測の場合に備えて、**site/mods** ディレクトリ ツリーに変更を加えるときはガイドラインに確実に従い、変更ログを保存しておく必要があります。複雑または広範囲に及ぶ変更が頻繁に加えられるサイトでは、ソフトウェアエンジニアリングプロジェクトとして **CA SDM** カスタマイズに取り組み、ソース コントロールの統制、テストの実行、および実稼動へのリリースの管理を行うことを検討する必要があります。

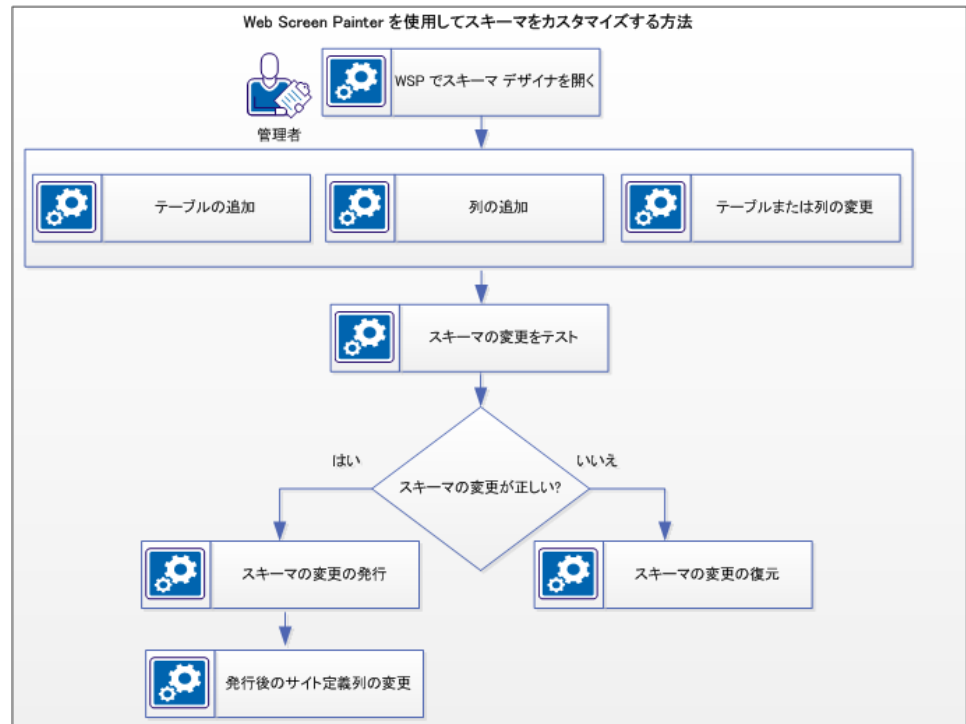
リリース間でカスタマイズをマイグレートする際に固有の課題に対処しなければならない場合があるため、カスタマイズの内容を保存できる製品の開発に力を入れて取り組んでいます。ただし、製品のカスタマイズは必ず本書の記載に従って行われることを前提としており、特にカスタマイズ内容が **site/mods** ツリーに配置されていることが重要です。また、レベル 2 のサポートからシステムのパッチが提供された場合、このパッチも上記と同じ前提に基づいて作成されています。カスタマイズの統制の取れていないシステムで、パッチの適用やアップグレードを行うことは、往々にしてコストのかさむシステム ダウンダウンタイムを引き起こす危険を伴います。本書の指示に従い、安全なソフトウェア エンジニアリング方式を実行して、このような危険を回避してください。

注: Web インターフェースのセキュリティ設定方法および構成方法の詳細については、「管理ガイド」を参照してください。

Web Screen Painter を使用してスキーマをカスタマイズする方法

CA SDM のデータベース スキーマを変更するには、**Web Screen Painter** のスキーマ デザイナを使用します。スキーマ デザイナには、このスキーマを確認および変更するためのグラフィカル ユーザ インターフェースが用意されています。

以下の図は、Web Screen Painter を使用してスキーマをカスタマイズする方法を示しています。



次の手順に従ってください:

1. [Web Screen Painter に関する考慮事項を確認します](#) (P. 446)。
2. [WSP でスキーマ デザインを開きます](#) (P. 446)。
3. [テーブルを追加する](#) (P. 447) か、[列を追加する](#) (P. 450) か、[テーブルまたは列を変更します](#) (P. 456)。
4. スキーマの変更をテストします。たとえば、物理データベースに何からの変更を加える前に、そのスキーマを使用して Web フォームを作成、更新、および表示します。Web フォームの作成の詳細については、「[WSP を使用して Web インターフェースをカスタマイズする方法](#) (P. 465)」を参照してください。
 - スキーマの変更が正しい場合は、[スキーマの変更を発行します](#) (P. 457)。
 - スキーマの変更が正しくない場合は、[スキーマの変更を元に戻します](#) (P. 463)。
5. (必要な場合) [発行後にサイト定義列を変更します](#) (P. 463)。

Web Screen Painter に関する考慮事項の確認

Web Screen Painter を使用する前に、以下の情報を考慮してください。

- WSP を使用して既存の列の長さを変更することはできません。また、その他のツールを使用して、既存の列の長さを変更しないでください。既存の列の長さの変更はサポートされていないため、CA SDM データベースにアクセスしている他のアプリケーションの実行が失敗する可能性があります。

重要: これらのアクションによって CA SDM が失敗する場合があるため、フィールドを短くしたり、既存のフィールドを削除したりしないでください。

- 基礎となるデータベースの最大レコード長を誤って超える場合があるため、既存のテーブルに列を追加するときは注意してください。CA SDM で使用しているデータベースの仕様を確認し、基礎となるデータベースの許容範囲内で変更を行ってください。
- データベース スキーマへの変更を発行する場合のダウンタイムは避けられません。これは、加えた変更内容や基礎となるデータベースの容量によって、わずかで済む場合もあれば、かなり長い時間を要する場合があります。
- CA SDM を初めて使用する場合は、実稼動環境に適用する前に、テスト段階ですべての変更を加える方が簡単です。
- データベース スキーマの変更前後に実行する必要がある一般的な手順を確認してください。
- スキーマをカスタマイズする際は、特定の手順を使用します。ほとんどの場合、手順の説明の後に、標準データベース スキーマに加える変更の例を示します。

WSP でスキーマ デザイナを開く

スキーマ デザイナでの作業を開始するには、CA SDM サーバに WSP がインストールされていることを確認してください。WSP 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。

次の手順に従ってください:

1. CA SDM の設定に応じて、WSP がインストールされている以下の CA SDM サーバにログインします。
 - 標準: プライマリ サーバ
 - 高可用性: バックグラウンド サーバ
2. CA SDM サーバにインストールされているオペレーティング システムに応じて、以下のいずれかのアクションを使用して WSP を起動します。
 - (Windows) [スタート] メニューから、[すべてのプログラム] - [CA] - [CA SDM] - [Web Screen Painter] を選択します。
 - (UNIX) パスに `$NX_ROOT/bin` を指定してコマンド `pdm_wsp` を入力します。

Web Screen Painter ログイン ウィンドウが開きます。

3. ログイン ID を入力します。
4. [ツール] - [スキーマ デザイナ] を選択します。

[スキーマ デザイナ] ウィンドウが開きます。[スキーマ デザイナ] ウィンドウの左側には、CA SDM のデータベースがツリー表示されます。テーブルと列は、それぞれのオブジェクト名で表示されます。表示名がテーブルまたは列のオブジェクト名と異なる場合は、オブジェクト名と共に表示名が括弧で囲まれて表示されます。

テーブルの追加

データベースにテーブルを追加するには、スキーマ デザイナを使用します。

次の手順に従ってください:

1. [編集] - [テーブルの追加] を選択します。

[テーブルの新規追加] ダイアログ ボックスが開きます。
2. [新規テーブル名] フィールドにテーブル名を入力し、[OK] をクリックします。今後使用される標準テーブルとの競合を避けるために、サイト定義テーブルの名前を文字「z」で開始するようにしてください。ユーザが追加しなかった場合は、テーブル名の先頭に「z」が自動的に追加されます。

3. 必要に応じて、以下のフィールドに入力します。

名前

(読み取り専用です) テーブルのオブジェクト名を指定します。たとえば、**cr** テーブルのオブジェクト名は「**cr**」です。

表示名

内容がわかるようなテーブル名を指定します。たとえば、**cr** テーブルの表示名は「リクエスト」です。このフィールドに新しい名前を入力すると、テーブルの表示名を変更できます。

スキーマ名

(標準テーブルでは読み取り専用) **pdm_userload** など、**CA SDM** ユーティリティでテーブルを参照するために使用する名前を入力します。サイト定義テーブルでは、デフォルトのスキーマ名はオブジェクト名です。このフィールドに新しい値を入力して、スキーマ名を変更することができます。

DBMS 名

物理 **DBMS** にあるテーブルを参照するために使用する名前を指定します。このフィールドは、すべてのテーブルで読み取り専用です。サイト定義テーブルでは、常にスキーマ名と同じです。

表示フィールドのデフォルト(共通名)

このテーブルを参照するフィールドについて、UI に表示される列を指定します。たとえば、リクエストの [担当者] フィールドは、連絡先テーブルの参照フィールドです。連絡先テーブルの共通名は **combo_name** (姓、名、ミドルネーム) であるため、参照される連絡先のコンボ名は、担当者として表示されます。共通名の値は変更できません。

外部キー フィールド(関連付け属性)

このテーブルを参照するフィールドについて、データベースに格納される列を指定します。たとえば、リクエストの [担当者] フィールドは、連絡先テーブルの参照フィールドです。連絡先テーブルの関連付け属性は **ID** であるため、リクエストの担当者列には、参照される連絡先の **ID** が格納されます。関連付け属性の値は変更できません。

ファンクション グループ

テーブル内のレコードに対して、ユーザのアクセス レベルを管理するグループ名を指定します。連絡先の各アクセス タイプでは、各ファンクション グループのテーブルデータについての読み取り権限を与えるか、変更権限を与えるか、またはアクセス権を与えないかを指定します。ドロップダウン リストから新しい値を選択して、関連付け属性の値を変更できます。

重要: スキーマ デザイナには、[詳細] タブがあります。このタブ上の情報は、CA Technologies のサポート担当者およびサイト担当者が使用するものです。スキーマ デザイナの使用時にこのタブを操作することはほとんどないため、本書では説明しません。

4. テーブルを保存するには、以下のいずれかを実行します。
 - テスト システムで作業している場合は、[ファイル] - [保存] を選択します。
 - 実稼働システムで作業している場合は、[ファイル] - [保存してテスト モードに設定] を選択します。

これにより、変更がデータベースに保存され、オブジェクト エンジンへの変更を定義するファイル (`wsptest.mods`) がサーバ上に作成されます。このファイルは、CA SDM インストール ディレクトリの `site/mods/majic` サブディレクトリに格納されます。

`wsptest.mods` ファイルが作成されると、オブジェクト エンジンがリサイクルされ、新しい変更が使用されるようになります。この処理は、スキーマの複雑さに応じて、数秒から数分かかります。

メッセージが表示されます。[はい] をクリックして続行します。`wsptest.mods` ファイルが影響するのは、`wsp_domsrvr` オプションで指定されたオブジェクト エンジンのみです。同じサーバ上の他のオブジェクト エンジンはこのファイルを処理せず、このファイルが他のサーバに配布されることはありません。また、テスト モードの新規テーブルと列は、ローカル オブジェクトとしてオブジェクト エンジンに定義されます。つまり、これらのテーブルと列はオブジェクト エンジンで認識されており、Web フォームで使用できます。ただしデータベース内には存在しないため、他のユーザには影響しません。CA SDM の標準ユーザは WSP オブジェクト エンジンを使用しないため、テストしているスキーマ変更の影響を受けません。

テーブルが追加されます。

列の追加

データベースに列を追加するには、スキーマ デザイナを使用します。

次の手順に従ってください:

1. 列を追加するテーブルを選択（またはテーブルの既存の列を任意に選択）します。
2. [編集] - [列の追加] を選択します。

[列の新規追加] ダイアログ ボックスが開きます。

3. [新規列名] フィールドに列名を入力し、[OK] をクリックします。
今後使用される標準列との競合を避けるために、列の名前を文字「z」で開始するようにしてください。

WSP は、「z」の有無を確認し、必要に応じて列名の先頭に「z」を追加します。

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

(表示専用) 列のオブジェクト名を指定します。たとえば、連絡先の alt_phone 列のオブジェクト名は「alt_phone」です。

表示名

内容がわかるような列名を指定します。このフィールドに新しい表示名を入力すると、列の表示名を変更できます。たとえば、連絡先 alt_phone 列の表示名は「その他の電話番号」です。

スキーマ名

(標準テーブルでは読み取り専用) pdm_userload など、CA SDM ユーティリティで列を参照するために使用する名前を入力します。サイト定義テーブルでは、デフォルトのスキーマ名はオブジェクト名です。このフィールドに別の値を入力して、スキーマ名を変更することができます。

DBMS 名

(すべてのテーブルで読み取り専用) 物理 DBMS にあるテーブルを参照するために使用する名前を指定します。サイト定義テーブルでは、DBMS 名 は常にスキーマ名と同じです。

説明

列の簡単な説明を入力します。

フィールド タイプ

(標準テーブルにあるすべての標準列と保存済みサイト定義列では読み取り専用) 列のデータ タイプを指定します。ドロップダウンから値を選択すると、新しいサイト定義列のフィールドタイプを、指定または変更することができます。以下に、使用できるフィールドタイプのリストを示します。

INTEGER

数値を示します。

STRING

テキスト文字列を示します。[文字列長] フィールドは、文字列の文字数を示します。

DATE

日時を示します。データベースに格納される値は、1970年1月1日の深夜 0 時以降の秒数です。

DURATION

期間を示します。データベースに格納される値は、秒数を表す整数です。

DOUBLE

実数 (浮動小数点数) を示します。

SREL

他のテーブルに対する外部キー参照を示します。SREL テーブルフィールドは、参照先のテーブルを指定します。データベースに格納される値は、参照されるテーブルの関連付け属性で、整数または文字列を指定できます。本製品に表示される値は、参照されるテーブルの行の共通名です。外部キー値を使用して SREL 属性を設定する方法については、「*テクニカル リファレンス ガイド*」を参照してください。

BREL

このテーブルに対する**SREL**が指定されたすべてのオブジェクトのセットを表す仮想列を示します。この列は、オブジェクトエンジンのみに存在し、データベースに物理的に格納されません。**CA Technologies** のテクニカル サービスから指示があった場合にのみ、このフィールド タイプを選択してください。

QREL

[詳細] タブの**Where**節で選択したオブジェクトのセットを表す仮想列を示します。この列は、オブジェクト エンジンのみに存在し、データベースに物理的に格納されません。**CA Technologies** のテクニカル サービスから指示があった場合にのみ、このフィールド タイプを選択してください。

DERIVED

[詳細] タブで指定されている式に従い、別の列の値を使用してオブジェクト エンジンが構築した仮想列を示します。この列は、オブジェクト エンジンのみに存在し、データベースに物理的に格納されません。**CA Technologies** のテクニカル サービスから指示があった場合にのみ、このフィールド タイプを選択してください。

文字列長

文字列の長さです。文字列以外の列である場合、このフィールドは空です。すべての標準列と保存したサイト定義列では、読み取り専用になります。このフィールドに **1~32767** の整数を入力して、新しいサイト定義の **STRING** 列の長さを指定したり、変更したりすることができます。

SRel テーブル

SREL 列で参照されるテーブルです。**SREL** 以外の列である場合、このフィールドは空です。すべての標準列と保存したサイト定義列では、読み取り専用になります。ドロップダウン リストから値を選択すると、新しいサイト定義 **SREL** によって参照されるテーブルを指定できます。

新規作成時のデフォルト値

テーブルの新しい行を定義するときこの列に割り当てられるデフォルト値です。これは、フィールドタイプに適した値にする必要があります。一部のキーワード値は、特定のフィールドタイプでのみ使用できます。

NOW

DATE列に対して、現在の日時を指定します。

USER

連絡先テーブルの SREL 列のアクティブ ユーザを指定します。

保存時の設定値

テーブルの行を更新するときこの列に割り当てられる値です。これは、フィールドタイプに適した値にする必要があります。一部のキーワード値は、特定のフィールドタイプでのみ使用できます。

NOW

DATE列に対して、現在の日時を指定します。

USER

連絡先テーブルの SREL 列のアクティブ ユーザを指定します。

必須

このチェック ボックスをオンにした場合、テーブルの行を保存する前に、その行に含まれる列に必ず値を入力する必要があります。標準列とサイト定義列の両方に、このオプションを設定できます。また、設定したオプションを無効にすることもできます。ただし、サイトで設定した場合を除いて、標準列のオプションはオフにできません。

新規レコードのみ更新可能

このオプションをオンにした場合、テーブルの行を最初に作成したときにのみ列の値を指定でき、それ以降は値を変更できません。標準列とサイト定義列の両方に、このオプションを設定できます。また、設定したオプションを無効にすることもできます。ただし、サイトで設定した場合を除いて、標準列のオプションはオフにできません。

pdm_userload のキー

このオプションをオンにした場合、入力値が既存の行の更新値であるかどうか判断するために、列が **pdm_userload** によってテストされます。このオプションは、**STRING** 列でのみ使用できます。このオプションは、標準テーブルのすべての列で読み取り専用になります。

DBMS のインデックス関連のオプション

これらのオプションでは、物理 DBMS のインデックス列の特性を指定します。これらのオプションは、サイト定義テーブルの列でのみ使用できます。

一意

テーブル内で、列が一意であることを指定します。つまり、この列では同じ値を持つ **2** つの行は存在しません。

昇順

DBMSインデックスが、この列によって昇順に並べ替えられます。選択できるのは、昇順と降順のいずれか一方だけです。

降順

DBMSインデックスが、この列によって降順に並べ替えられます。選択できるのは、昇順と降順のいずれか一方だけです。

重要: スキーマ デザイナには、[詳細] タブがあります。このタブ上の情報は、CA Technologies のサポート担当者およびサイト担当者が使用するものです。スキーマ デザイナの使用時にこのタブを操作することはほとんどないため、本書では説明しません。

5. 列を保存するには、以下のいずれかを実行します。

- テスト システムで作業している場合は、[ファイル] - [保存] を選択します。
- 実稼働システムで作業している場合は、[ファイル] - [保存してテスト モードに設定] を選択します。

これにより、変更がデータベースに保存され、オブジェクト エンジンへの変更を定義するファイル (`wsptest.mods`) がサーバ上に作成されます。このファイルは、CA SDM インストール ディレクトリの `site/mods/majic` サブディレクトリに格納されます。

`wsptest.mods` ファイルが作成されると、オブジェクト エンジンがリサイクルされ、新しい変更が使用されるようになります。この処理は、スキーマの複雑さに応じて、数秒から数分かかります。

メッセージが表示されます。[はい] をクリックして続行します。`wsptest.mods` ファイルが影響するのは、`wsp_domsrvr` オプションで指定されたオブジェクト エンジンのみです。同じサーバ上の他のオブジェクト エンジンはこのファイル进行处理せず、このファイルが他のサーバに配布されることはありません。また、テスト モードの新規テーブルと列は、ローカル オブジェクトとしてオブジェクト エンジンに定義されます。つまり、これらのテーブルと列はオブジェクト エンジンで認識されており、Web フォームで使用できます。ただしデータベース内には存在しないため、他のユーザには影響しません。CA SDM の標準ユーザは WSP オブジェクト エンジンを使用しないため、テストしているスキーマ変更の影響を受けません。

列がテーブルに追加されます。

テーブルまたは列の変更

テーブルまたは列の情報を変更するには、スキーマ デザイナで目的のテーブルまたは列をクリックしてから、該当のフィールドに新しい情報を入力します。変更できる情報は、テーブルまたは列のステータスによって異なります。

標準テーブル

〔表示名〕、〔説明〕、〔ファンクション グループ〕の各フィールドを変更できます。

標準列

〔表示名〕フィールド、〔説明〕フィールド、〔新規作成時のデフォルト値〕、〔保存時の設定値〕を変更できます。さらに、〔必須〕または〔新規レコードのみ更新可能〕のチェック ボックスがオフの場合は、これらをオンにすることもできます。これらのチェック ボックスがデフォルトでオンになっている場合、オフにすることはできません。ただし、ユーザが自分でオンにした場合はオフにできます。

サイト定義テーブル

テーブルが発行されていない場合は、〔名前〕フィールド以外のすべてのフィールドを変更できます。新規のテーブルを保存した後で〔名前〕フィールドを変更することはできません。発行済みのサイト定義テーブルでは、〔表示名〕、〔説明〕、および〔ファンクション グループ〕フィールドのみを変更できます。

サイト定義列

列が発行されていない場合は、〔名前〕フィールド以外のすべてのフィールドを変更できます。新規の列を保存した後で〔名前〕フィールドを変更することはできません。発行済みのサイト定義列では、〔表示名〕フィールド、〔説明〕フィールド、〔新規作成時のデフォルト値〕、〔保存時の設定値〕と、〔必須〕、〔新規レコードのみ更新可能〕、〔pdm_userload のキー〕の各チェック ボックス、および DBMS インデックスのオプションのみを変更できます。

スキーマの変更の発行

スキーマの変更が完了したら、変更を発行して、すべてのユーザが変更を利用できるようにします。WSP では、新規作成または更新したテーブルと列がそれぞれ、データベースの `wsptbl` テーブルと `wspcol` テーブルに格納されます。

次の手順に従ってください:

1. オブジェクトエンジンと CA SDM ユーティリティ プログラムを対象として、スキーマの変更を定義するファイルを新規作成/更新します。WSP では、`wsp_webengine` オプションで指定された Web エンジン（デフォルトでは `web:local`）に、以下のファイルを作成します。

`wsp.mods`

Web Screen Painter で管理されている、オブジェクト エンジンに対するスキーマ変更がすべて記述されます。

`wsp_schema.sch`

Web Screen Painter で管理されている、すべてのテーブルおよび列が記述されます。

`wsp_index.sch`

Web Screen Painter で管理されているテーブルの DBMS インデックスが記述されます。

`wsp.altercol`

WSP で作成され、DBMS には未定義の新規列の名前が指定されます。

`wsp.altertbl`

WSP で作成され、DBMS には未定義の新規テーブルの名前が指定されます。さらに、WSP は、オブジェクト エンジンに備えたすべての CA SDM サーバに `wsp.mods` ファイルを配布します。

2. [ファイル] - [保存] - [発行] を選択します。

CA SDM サーバ上に必要なファイルが作成されますが、これらがリサイクルされることはありません。このため、この操作の直後は新規ファイルの影響はありません。ただし、ファイルの作成後は、次回 CA SDM サービスがリサイクルされるときに、これらのファイルが使用されます。

3. 標準設定を使用している場合は、以下の手順に従います。

- プライマリ サーバ上の **CA SDM** サービスをシャットダウンし、以下のコマンドを実行します。

```
pdm_publish
```

このコマンドは、物理 **DBMS** を変更し、新規スキーマの情報を格納します。

重要: **pdm_publish** プロセスを実行すると、ほかのユーザに重大な影響を及ぼします。スキーマの変更の発行は慎重に計画するようにしてください。**CA SDM** の変更要求を使用してスキーマ発行のスケジュールを調整し、事前の承認を得ることをお勧めします。

4. 高可用性設定を使用している場合は、以下の手順に従います。

- a. 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。

バックグラウンドサーバ上でサポート 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スケジュール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。

- b. バックグラウンドサーバ上の **CA SDM** サービスをシャットダウンします。

重要: **WSP** から「保存して発行」が実行された後、スタンバイまたはアプリケーションサーバ上の **CA SDM** サービスを再起動しないでください。このアクションによって、高可用性設定が中断されます。スタンバイまたはアプリケーションサーバ上の **CA SDM** サービスが停止されているときに、サービスを開始したい場合は、**CA SDM** サービスを開始する前に、サーバ上で `pdm_server_control -v` コマンドを実行してバージョン管理を抑制します。

重要: アクティビティの発行中にバックグラウンドサーバに障害が発生した場合は、**WSP** の変更を回復するようにしてください。詳細については、「[バックグラウンドサーバの障害時の WSP 変更の回復 \(P. 461\)](#)」を参照してください。

- c. 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。

- d. スキーマの変更を使用して DBMS を更新するには、元のバックグラウンドサーバ（現在のスタンバイサーバ）上で以下のコマンドを実行します。

`pdm_publish`

`pdm_publish` コマンドは、CA SDM の次の起動でスタンバイサーバとバックグラウンドサーバの同期を抑制する制御ファイルを作成します。このアクションは、`pdm_publish` によって実行されたスキーマファイルの変更を保持するために必要です。このコマンドは、スキーマの変更の正常な発行の後、必要に応じて 2 番目のフェールオーバーを実行します。正常な発行の最後に、以下のメッセージがユーザに表示されます。

このスタンバイサーバで `pdm_publish` によって CA Service Desk Manager を開始し、フェールオーバーを実行しますか? (Y/N)

- 「Y」と入力すると、`pdm_publish` はスタンバイサーバ上で CA SDM サービスを開始し、自動的にフェールオーバーを実行します。すべてのアプリケーションサーバ上でスキーマの変更を適用するには、手順 g に進みます。
 - 「N」と入力した場合は、手順 e に進みます。
- e. スタンバイサーバ（元のバックグラウンドサーバ）上で CA SDM サービスを開始します。

この起動では `pdm_publish` によって作成された制御ファイルが検出されますが、スタンバイサーバとバックグラウンドサーバの同期は実行されません。同期が実行されないため、この起動では `pdm_publish` によって実行された変更が保持されます。

重要: `pdm_publish` の後に元のバックグラウンドサーバにフェールオーバーできないとサービスが中断されるため、これらの指示に正確に従うようにしてください。

- f. スタンバイ サーバ（元のバックグラウンドサーバ）を再度バックグラウンドサーバにするには、そのサーバ上で以下のコマンドを実行します。

```
pdm_server_control - b
```

このサーバが再度スタンバイサーバになったときにバージョン管理が正常に機能するように、このコマンドでは制御ファイルも削除されます。

- g. 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** 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。

指定した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スケジュール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。ユーザが自分の作業を再開するには、更新されたアプリケーションサーバにログオンします。

- h. すべてのスタンバイサーバを再起動します。

バックグラウンドサーバ障害中の WSP 変更の回復

アクティビティの発行中にバックグラウンドサーバに障害が発生した場合は、MDB スキーマの変更を回復することができます。

重要： 実稼働環境で回復手順を直接実行することは推奨されません。まず、テストまたは開発環境で検証するようにしてください。

次の手順に従ってください：

- 発行前にバックグラウンドサーバがクラッシュした場合は、最後に保存されたスキーマの変更が MDB 内に保持されます。新しいバックグラウンドサーバにログインし、発行タスクを再開します。

- 発行後にバックグラウンドサーバがクラッシュした場合は、以下のアクションを実行します。
 - a. クラッシュしたバックグラウンドサーバ上の **CA SDM** サービスを停止します。
 - b. 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を選択します。
 - c. クラッシュしたバックグラウンドサーバの以下のファイルを、スタンバイサーバ上の同じ場所にコピーします。
 - "\$NX_ROOT\$/site/mods/majic/wsp.mods"
 - "\$NX_ROOT\$/site/mods/wsp.altertbl"
 - "\$NX_ROOT\$/site/mods/wsp.altercol"
 - "\$NX_ROOT\$/site/mods/wsp_index.sch"
 - "\$NX_ROOT\$/site/mods/wsp_schema.sch"
 - d. スキーマの変更を発行し、自動フェールオーバーを実行するには、スタンバイサーバ上で以下のコマンドを実行します。

`pdm_publish`
 - e. スキーマの変更の正常な発行の後に表示されるメッセージプロンプトで「Y」を選択します。

CA SDM サービスが、スタンバイサーバ上で起動されます。

注: 自動フェールオーバーが実行されない場合は、スタンバイサーバから `pdm_server_control -b` コマンドを実行して、その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。
 - f. 各アプリケーションサーバを休止してリサイクルします。すべてのスタンバイサーバを再起動します。詳細については、「[スキーマの変更の発行](#) (P. 491)」を参照してください。

スキーマの変更の復元

テスト モードでスキーマの変更を行った後で、スキーマの変更の方針が変わった場合は、発行済みバージョンのスキーマに復元できます。スキーマの変更を元に戻すと、ほかのユーザに影響を与える可能性があります。そのため、このオプションを使用できるのは、**WSP** にオブジェクトエンジンと **Web** エンジンを提供する **wsp_domsrvr** オプションと **wsp_webengine** オプションの両方がインストールされている場合のみです。

次の手順に従ってください:

1. [ファイル] - [テストモードの復元] を選択します。

WSP によって **wsptest.mods** ファイルが削除され、**WSP** オブジェクトエンジンによってスキーマが発行済みバージョンに復元されます。

wsptest.mods ファイルが削除されると、**WSP** オブジェクトエンジンがリサイクルされ、その内部スキーマが再構築されます。この処理は、スキーマの複雑さに応じて、数秒から数分かかります。

オブジェクトエンジンのリサイクルが完了すると、アクティブ スキーマは発行済みバージョンに戻ります。

注: 新しいスキーマを使用するように変更された **Web** フォームは自動的に元に戻されないため、発行済みバージョンのスキーマで使用されると正しく動作しない場合があります。

発行後のサイト定義列の変更

WSP では、発行後のサイト定義スキーマ変更を標準スキーマと同様に扱うため、その後の変更は制限されています。**DBMS** および **WSP** の外部のスキーマを手動で更新することにより、サイト定義列を削除したり、サイト定義文字列の列の長さを変更したりすることができます。次に、**pdm_wspupd** スクリプトを実行してデータベース **wspcol** テーブルを更新し、**WSP** と外部変更を同期させます。

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. CA SDM インストールディレクトリ内の `site/mods` サブディレクトリに移動します。
3. `wsp_schema.sch` ファイルを編集し、不要なサイト定義列を削除するか、サイト定義の `STRING` 列の長さを変更します。これらの更新は、この手順でサポートされている変更のみです。`wsp_schema.sch` ファイルは、任意の標準的なテキストエディタを使用して編集できます。

重要: 列を削除するためのインデックス オプション (`UNIQUE` など) が指定された場合、`wsp_index.sch` ファイルを削除して列の参照を削除します。その列がテーブル中で唯一のインデックス作成済みの列である場合は、テーブルに対するすべての参照を `wsp_index.sch` から削除してください。
4. `wsp_schema.sch` に加えたのと同じ変更を使用して `majic/wsp.mods` ファイルを編集します。
 - 不要なサイト定義の列を削除します。
 - サイト定義の `STRING` 列の長さを変更します。
5. コマンドプロンプトを使用して、以下のコマンドを入力します。

```
pdm_wspupd
```

`pdm_wspupd` スクリプトは `wsp_schema.sch` を読み取り、データベース内の `wspcol` テーブルと比較して、相違がある場合はそれをコンソール行に書き込みます。たとえば、以下の出力を参照してください。

```
PDM_WSPUPD - wsp_schema.sch から wspcol テーブルを更新しました
```

```
現在の DBMS 情報に対する wsp_schema.sch を読み込んでいます...
```

```
Web Screen Painter スキーマ情報に対する wspcol テーブルを読み込んでいます...
```

```
STRING 列 zSales0rg.description の長さが 350 から 400 に変更されました
```

```
列 zSales0rg.sym が wsp_schema.sch にありません - wspcol 行を削除します
```

```
pdm_wspupd は、Web Screen Painter が管理する列 1 と削除する列 1 を見つけました。  
wsp_schema.sch に対応するように DBMS が手動で更新されていることを確認し、"Y"と応答して  
wspcol を更新するか、他の応答によってキャンセルします。
```


6. pdm_wspupd が検出した変更が、wsp_schema.sch に加えた変更と完全に一致するかどうかを確認します。一致する場合は「Y」と入力して変更を確認します。

更新が確認されると、このスクリプトは CA SDM の標準ユーティリティを使用して wspcol テーブルを更新します。その後、スキーマデザイナーはユーザの変更を表示します。

7. CA SDM サーバを停止します。
8. お使いの DBMS 用のユーティリティを使用して、変更した列の DBMS 定義を変更します。
 - wsp_schema.sch から削除したデータベースから任意の列を削除します。
 - wsp_schema.sch で変更した文字列列のデータベース長を変更します。

DBMS に加える変更は、wsp_schema.sch に加えた変更と完全に一致するようにしてください。

9. wsp_schema.log ファイルを削除します。
10. [スキーマの変更を発行します](#) (P. 457)。
11. CA SDM サーバを起動します。

Web Screen Painter を使用して Web インターフェースをカスタマイズする方法

Web Screen Painter (WSP) を使用すると、プログラミングなしで、サイトの要件を満たすように Web フォームをカスタマイズできます。

一部のナレッジマネジメント フォームは、WSP のデザイン ビューではカスタマイズできません。これらのフォームは、以下の方法でカスタマイズできます。

- ドキュメント ビュー - このページの内容は、ドキュメントの作成時に使用されたドキュメントテンプレートによって決定されます。これらのテンプレートは、[ドキュメント] - [ドキュメントテンプレート] の [管理] タブで変更できます。
- ナレッジカテゴリ ドキュメント リスト - このページは Web Screen Painter で変更できますが、ユーザ環境設定でも管理できます。[環境設定] 画面では、ドキュメントリストに表示するドキュメントプロパティの定義、および 1 ページに表示するドキュメント数を、ユーザごとにパーソナリゼーションできます。

次の手順に従ってください:

1. [Web Screen Painter を起動します](#) (P. 466)。
2. [前提条件を確認します](#) (P. 466)。
3. [カスタマイズするフォームを選択します](#) (P. 467)。
 - [フォームを作成します](#) (P. 468)。
 - [既存のフォームを開きます](#) (P. 470)。
4. [フォームのカスタマイズ](#) (P. 471)

WSP は常に、WSP がインストールされているサーバ上の変更を保存します。保存されたファイルは、ほかの WSP ユーザがプレビューセッションからアクセスできるようになります。ただし、CA SDM の標準ユーザに対しては表示されません。これは、WSP が `site/mods/wsp` ディレクトリ内のすべてのファイルを保存し、このディレクトリが CA SDM の標準セッションでは使用されないためです。

5. テスト システムで Web フォームの変更を行っている場合は、[テストシステムから実稼働システムにマイグレートします](#) (P. 491)。
6. [フォームの変更を発行します](#) (P. 491)。
7. (必要な場合) [発行後にフォームを削除します](#) (P. 493)。

前提条件を確認します。

カスタマイズを開始する前に、以下の前提条件を確認します。

- Web フォームに追加するスキーマがカスタマイズされている。
- (高可用性設定のみ) Web フォームを正常に発行するために、以下の前提条件が確認されている。
 - (推奨) すべての CA SDM サーバ上で CA SDM サービスが稼働中である。そうでない場合、WSP は稼働中の CA SDM サーバ上でのみ発行します。
 - (必須) すべての CA SDM サーバ上で少なくとも 1 つの Web エンジンインスタンスが実行されている。

Web Screen Painter の起動

Web フォームをカスタマイズするには、WSP を起動します。

次の手順に従ってください:

1. Web Screen Painter がインストールされているコンピュータにログインします。
2. WSP を起動します。
 - (Windows) [スタート] - [プログラム] - [CA] - [Service Desk] - [Web Screen Painter] をクリックします。
 - (UNIX) パスに `$NX_ROOT/bin` を指定してコマンド `pdm_wsp` を入力します。

重要: UNIX を使用している場合は、WSP を使用するために **Firefox** がインストールされていることを確認してください。

Web Screen Painter ログイン ウィンドウが開きます。

3. 認証情報を入力します。
WSP にメイン フォームが表示されます。

カスタマイズするフォームの選択

フォームを作成するか、またはカスタマイズする既存のフォームを開くことができます。以下のいずれかを選択します。

- [フォームを作成します](#) (P. 468)。
- [既存のフォームを開きます](#) (P. 470)。

フォームの作成

WSP でフォームを作成します。

次の手順に従ってください:

1. [ファイル] - [新規] をクリックします。
[フォームの新規作成] ダイアログ ボックスが開きます。
2. 必要に応じて、以下のフィールドに入力します。

インターフェースまたはファイル タイプ

フォームのファイル タイプを示します。たとえば、HTML フォームを作成するには、インターフェース（アナリスト、顧客、従業員、デフォルト、または PDA）を選択します。その他のファイル タイプのフォームを作成するには、タイプ（CSS スタイルシート、HTML、または JavaScript）を直接選択します。インターフェースまたはファイル タイプを選択すると、選択したファイル タイプで使用可能なすべてのテンプレートのリストが WSP の [ファイル名] フィールドに表示されます。

フォーム グループ

新しいフォームまたはファイルを作成する（CA SDM のインストールで定義された）フォーム グループを示します。フォーム グループを定義していない場合は、初期設定のフォーム グループのみが一覧表示されます。

ファイル名

選択したインターフェースまたはファイル タイプ用のテンプレートを示します。テンプレートは、新規作成するフォームまたはファイルのタイプに必要な基本的な要件を満たしています。

新規リストまたは詳細フォーム用のテーブルの選択

新しいリストまたは詳細フォームを作成できる CA SDM テーブルを示します。このフィールドには、選択したインターフェース（アナリスト、顧客、従業員、デフォルト、または PDA）に従ってデータが入力されます。

注: 詳細フォームまたはリスト フォームは、フォーム グループのテーブルごとに 1 つしか作成できません。そのため、すでにテーブルにフォームが存在する場合は、フォームを作成するのではなく、既存のフォームを編集してください。複数バージョンのフォームが必要な場合は、追加するバージョンを含んだフォーム グループを 1 つ以上作成します。

3. [新規] をクリックします。
4. カスタマイズ用のフォームが表示されます。以下の 2 つのタブが表示されます。

デザイン

詳細フォーム、リスト フォーム、およびメニュー バー フォームで使用でき、ユーザに対して表示されるものと似たレイアウトで、フォームのコントロールが表示されます。これは、エンドユーザに対するフォームの実際の表示を示すものではありません。これを確認するには、[ツール] - [プレビュー] を選択します。

ソース

メモ帳形式のエディタにより、フォームのソース コードをレビューおよび編集できます。一部のフォームは [ソース] タブでのみ編集可能です。このようなフォームの場合、編集ウィンドウには [ソース] タブのみが表示され、[デザイン] タブは無効になります。

フォームがカスタマイズ用に準備されます。

重要: 詳細フォームまたはリスト フォームを作成または編集する場合は、「list_」および「detail_」プレフィックスを使用して、HTML ファイルに名前を付けてください。たとえば、list_test.html、detail_test.html のような名前にします。このプレフィックスにより、フォームを正しくプレビューできます。また、カスタム名を使用して詳細テンプレートを保存する場合は、<PDM_WSP> タグも手動で編集する必要があります。例：<PDM_WSP mode=edit preview="test.html+OP=CREATE_NEW" factory=cr>。

関連項目:

[Web フォームグループの作成方法](#) (P. 498)

既存のフォームを開く

WSP で既存のフォームを開いてカスタマイズします。

次の手順に従ってください:

1. [ファイル] - [開く] を選択します。
[フォームを開く] ダイアログ ボックスが開きます。
2. インターフェース（[アナリスト]、[カスタマ]、[従業員]、[デフォルト]）またはファイルタイプ（[CSS スタイルシート]、[JavaScript]、[HTML]）、および編集するフォームが含まれているフォーム グループを選択します。
3. 目的のフォームをリストから選択するか、またはその名前をテキストボックスに入力します。

ファイル名をテキストボックスに入力すると、入力した文字と一致する最初のファイル名まで [ファイル名] リストが自動的にスクロールされます。[ステータスのファイル] ドロップダウン リストを使用して、表示するファイルのリストを制限できます。

発行停止された変更により変更済みのサイト(+)

WSP で変更された未発行のファイルのみをリストに表示します。
このようなファイルは、ファイル名の後にプラス記号 (+) が付きます。

変更済みのサイト(*)

ユーザのサイトで変更されたフォーム（発行済みおよび発行停止の両方）のみをリストに表示します。発行停止ファイルには、ファイル名の後にプラス記号 (+) が付きます。発行済みのサイト変更には、ファイル名の後にアスタリスク (*) が付きます。

すべて

何の制約もせずにすべてを表示します。発行停止ファイルには、ファイル名の後にプラス記号 (+) が付きます。発行済みのサイト変更には、ファイル名の後にアスタリスク (*) が付きます。

4. [開く] をクリックします。
フォームが表示され、カスタマイズ用に準備されます。

フォームのカスタマイズ

WSP で編集するフォームを開いた後、ツールバー、メニュー コマンド、およびショートカットを使用してフォームをカスタマイズできます。以下のカスタマイズを実行できます。

- [コントロールの挿入](#) (P. 471)
- [コントロールのプロパティの編集](#) (P. 475)
- [メニューバーの変更](#) (P. 476)
- [スタイルシートの変更](#) (P. 481)
- [マウスオーバー プレビュー フォームの変更](#) (P. 485)
- [リスト フォーム上のデータ グリッド リストの変更](#) (P. 487)
- [詳細フォーム上のノートブックの変更](#) (P. 489)
- [HTML および JavaScript ファイルの変更](#) (P. 490)

コントロールの挿入

フォームにコントロールを追加します。たとえば、フォームにテキストボックスを追加します。

以下のコントロールは、リスト フォームと詳細フォームの両方に挿入できます。

コントロール	アイコン	説明
行の挿入		選択したコントロールを現在の行の最後のコントロールにします（以降のコントロールは次の行に移動します）。
行の削除	N/A	現在選択されているコントロールと同じ行にあるコントロールをすべて削除します。
テキストボックス		文字列またはテキスト フィールドを編集するための、1 行または複数行のテキスト ボックスを挿入します。
ドロップダウン		テーブルと比較検証されるフィールドを編集するためのドロップダウン リストを挿入します。

コントロール	アイコン	説明
ルックアップ		テーブルと比較検証されるフィールドを編集するための、ルックアップ コントロールを挿入します。このコントロールはテキストボックスで構成され、そのラベルには選択フォームをポップアップ表示するハイパーリンクが含まれています。
ボタン		ボタンを挿入します。
階層ルックアップ		ルックアップ コントロールと似ていますが、階層的なセクタ構造のフィールド（リクエスト カテゴリなど）に対して使用される点が異なります。
日付		日付フィールドを挿入します。このコントロールはテキストボックスで構成され、そのラベルには日付セクタをポップアップ表示するハイパーリンクが含まれています。

以下のコントロールは、詳細フォームでのみ使用できます。

コントロール	アイコン	説明
チェック ボックス		チェックボックスを挿入します。
HTML エディタ		HTML を含むテキスト フィールドを編集するために、HTML エディタを挿入します。
読み取り専用テキストボックス		編集できないテキスト フィールドを挿入します。 -
読み取り専用ルックアップ		編集できないルックアップ フィールドを挿入します。 - このフィールドは、定義する詳細フォームをポップアップ表示するハイパーリンクとして表示されます。
読み取り専用		編集できない日付フィールドを挿入します。 -
ノートブック		ノートブックを挿入します。詳細フォームで利用できるノートブックは 1 つだけです。そのため、このコントロールを挿入できるのは、ノートブックが含まれていないフォームのみです。

以下のコントロールは、リスト フォームでのみ使用できます。

コントロール	アイコン	説明
リスト		リストを挿入します。リスト フォームで利用できるリストは1つだけです。そのため、このコントロールを挿入できるのは新規のリスト フォームのみです。

次の手順に従ってください:

1. コントロールを追加する位置でフォームを右クリックし、[コントロールの挿入] を選択します。
ドロップダウン リストが表示されます。
2. [\[コントロールの挿入\] ダイアログ ボックスのオプション](#) (P. 474) を選択します。
コントロールが、フォーム上に配置されます。
3. フォームがエンド ユーザにどのように表示されるかを確認するには、[ツール] - [プレビュー] を選択します。外観は CA SDM の標準ウィンドウに似ており、ボタンとメニューの大部分は機能しますが、標準セッションではありません。そのため、標準セッションのように使用しないでください。
4. [ファイル] - [保存] をクリックします。
コントロールがフォームに追加されました。

コントロール ダイアログ ボックス オプションの挿入

［ファイル］メニューから［コントロールの挿入］ダイアログ ボックスを開きます。このダイアログ ボックスには、編集用を選択するフォームのセクションに対応するすべての UI コントロールのリストが表示されます。

このダイアログ ボックスには、以下のオプションがあります。

前に挿入

リストから選択したコントロールを、ベース フォーム上で現在選択されているコントロールの前に挿入し、挿入したコントロールを現在選択されているコントロールに変更します。

後に挿入

リストから選択したコントロールを、ベース フォーム上で現在選択されているコントロールの後ろに挿入し、挿入したコントロールを現在選択されているコントロールに変更します。

戻る

現在選択されているコントロールを、フォーム上の前のコントロールに移動します。

Next

現在選択されているコントロールを、フォーム上の次のコントロールに移動します。

プロパティ

現在選択されているコントロールの［プロパティ］ダイアログ ボックスを開きます。

クローズ

コントロールの挿入フォームを閉じます。

挿入後にフォームを閉じる

(有効時) [前に挿入] または [後ろに挿入] をクリックしたときに、選択されたコントロールを挿入して [コントロールの挿入] ダイアログ ボックスを閉じます。

(無効時) [前に挿入] または [後ろに挿入] をクリックしたときに、選択されたコントロールを挿入します。 [コントロールの挿入] ダイアログ ボックスは開いたままになるので、別のコントロールを挿入したり、現在選択されているコントロールのプロパティを要求したりできます。このチェック ボックスをオフにした場合、再び選択するか、または WSP セッションを終了するまで [挿入後にフォームを閉じる] チェック ボックスはオフのままです。

デフォルト：有効

コントロールのプロパティの編集

コントロールのプロパティを編集します。

次の手順に従ってください:

1. コントロールを選択して、F4 キーを押します。
[プロパティ] ダイアログ ボックスが開きます。
2. 必要に応じて、プロパティを変更してください。たとえば、[キャプション] プロパティは、コントロールの上に表示されるヘッダラベルを指定します。このプロパティを指定するには、[キャプション] プロパティの右側にあるセルに適切な値を入力します。
3. [プロパティ] ダイアログ ボックスを閉じます。
4. フォームがエンドユーザにどのように表示されるかを確認するには、[ツール] - [プレビュー] を選択します。外観は CA SDM の標準ウィンドウに似ており、ボタンとメニューの大部分は機能しますが、標準セッションではありません。そのため、標準セッションのように使用しないでください。
5. [ファイル] - [保存] をクリックします。
コントロールのプロパティが変更され、フォームが保存されます。

メニュー バーの変更

名前の先頭に「**menubar_**」が付いているフォームは、メニュー バーを定義します。メニュー バーのデザイン ビューでは、上部にメニューが表示されます。メニュー項目をクリックしてメニューを下に移動することはできますが、それ以外、デザイン ビューでメニュー バーを直接編集することはできません。メニュー バーを編集するには、メニュー項目をダブルクリックして、メニュー デザイナを表示します。

注: メニューおよびメニュー バーのフォームは、アナリスト用インターフェースでのみ使用されます。顧客用インターフェースと従業員用インターフェースでは、ドロップダウン リストではなく、実際のリンクが含まれている「起動バー」が使用されます。カスタム用または従業員用の起動バーをカスタマイズするには、それぞれのインターフェースからフォーム **std_body_site.html** を編集します。

次の手順に従ってください:

1. [ツール] - [メニュー デザイナ] を選択するか、またはメニューバーフォームの [デザイン] タブに表示されたメニューをダブルクリックします。
[メニュー デザイナ] ダイアログ ボックスが表示されます。
2. メニュー項目を追加または編集するには、[\[メニュー デザイナ\] ダイアログ \(P. 477\)](#) ボックス内のフィールドに入力します。メニュー項目の追加の詳細については、「[メニュー項目で使用する関数 \(P. 479\)](#)」を参照してください。
3. [OK] をクリックして、ダイアログ ボックスを閉じます。
4. フォームがエンド ユーザにどのように表示されるかを確認するには、[ツール] - [プレビュー] を選択します。外観は **CA SDM** の標準ウィンドウに似ており、ボタンとメニューの大部分は機能しますが、標準セッションではありません。そのため、標準セッションのように使用しないでください。
5. [ファイル] - [保存] をクリックします。
フォームのメニュー バーが変更されます。

[メニュー デザイナ]ダイアログ ボックス

注: メニュー デザイナにアクセスできるのは、menubar_admin.html など、フォーム名が「menubar_」で始まる HTML フォームを編集する場合のみです。

[ツール] メニューから [メニュー デザイナ] を選択するか、またはメニューバー フォームの [デザイン] タブに表示されたメニューをダブルクリックすると、[メニュー デザイナ] ダイアログ ボックスが表示されます。[メニュー デザイナ] ダイアログ ボックスを使用すると、開いているフォームに、メニューバー、メニュー、サブメニュー、メニュー コマンドを追加できます。[メニュー エディタ] ダイアログ ボックスには、以下のコントロールがあります。

メニュー リスト

メニュー リストから、変更するメニュー アイテムを選択します。メニュー ラベルを変更するには、リストからメニュー ラベルを選択して、[キャプション] テキスト ボックスに新しい名前を入力し、[適用] をクリックします。

追加

メニュー リストの最後に新しいアイテムを追加するには、このボタンをクリックします。

挿入

メニュー リストで、選択したアイテムの上に新しいアイテムを挿入するには、このボタンをクリックします。

削除

選択したアイテムをメニュー リストから削除するには、このボタンをクリックします。

 選択したメニュー アイテムが 1 つ上のレベルへ移動します。

 選択したメニュー アイテムが 1 つ下のレベルへ移動します。

 メニューではなく、サブメニューまたはコマンドとしてアイテムを定義する場合などは、選択したメニュー アイテムを 1 レベル右へ移動します。

 サブメニューまたはコマンドではなく、メニューとしてアイテムを定義する場合などは、選択したメニュー アイテムを 1 レベル左へ移動します。

注: 1 レベルのインデントのみ使用できます。

キャプション

選択したメニュー アイテムの名前を入力します。 詳細については、「キャプション」を参照してください。

関数

ユーザがメニューをクリックしたときに実行する JavaScript 関数を入力します。 詳細については、メニューで役立つ定義済みの関数など、関数プロパティに関する説明を参照してください。

ID

メニュー アイテムに割り当てる HTML/JavaScript ID を入力します。

ホット キー

メニュー アイテムのホットキーを選択する方法に関して、CA SDM に命令する文字をリスト形式で入力します。メニュー キャプションに表示されるホットキーには下線が付きます。 一般に、CA SDM は、すでに使用しているキーではなく、メニューのキャプションにある最初のキーをホットキーとして選択します。選択をこれらの文字に限定するために、ここで1つ以上の文字を指定できます。また、これらの文字が選択されないように、1つ以上の文字の前に、説明ポイントを指定できます。

イメージ

メニュー アイテムの横に表示する画像の場所を入力します。

内部

関数で呼び出す JavaScript を現在のウィンドウの文脈で実行する必要がある場合（ポップアップの詳細ウィンドウなど）、このオプションを選択します。メイン フォームの文脈で関数を実行する必要がある場合は、このオプションはオフにします。

変数

メニュー アイテムに割り当てる JavaScript 変数を入力します。

ツール バー

最上位以外のメニュー アイテムに対応するツール バー アイコンおよびヒントを追加できます。

アイコン ファイル

ツールバー アイコンの位置を示します。

ヒント

ヒントのテキストを指定します。

OK

ダイアログ ボックスを閉じて変更を保存するには、このボタンをクリックします。

キャンセル

変更を保存せずにダイアログ ボックスを閉じるには、このボタンをクリックします。

メニュー項目で使用する関数

CA SDM の大部分のフォームには、関数を制御するメニュー バーがあります。メニューバーは、`menubar_xx.htmlpl` という名前の HTMLPL フォームによって生成されます。既存のメニューバーをカスタマイズしたり、新規のメニューバーを定義する場合は、WSP を使用することをお勧めします。

以下の事前定義済み関数を、メニュー項目から呼び出されるスクリプトで使用すると便利です。

upd_frame(form)

メイン ウィンドウのコンテンツ フレームに新しいフォームをロードします。

create_new(factory, use_template, width, height [,args])

新しいレコードを定義するフォームがポップアップします。

Popup_window(name, form[, width, height [,features [,args]]])

新しいウィンドウがポップアップします。

showDetailWithPersid(persid)

詳細レコードがポップアップします。

これらの関数には、以下の用語および定義が適用されます。

form

`xxx.htmlpl` という形式の HTMLPL ファイル名、または操作コード（たとえば `CREATE_NEW`）です。

factory

データベース オブジェクトの名前です。

use_template

true または false です。

width

フォームの幅を表します。デフォルトは 0 です。

height

フォームの高さを表します。デフォルトは 0 です。

features

ウィンドウの機能のリストです。標準の **window.open** 関数と同じ形式を使用します。

args

フォームに指定した操作の引数です。「キーワード=値」の形式で 1 つ以上の引数を指定します。

persid

フォーム **factory:ID** の固定 ID です。

スタイルシートの変更

WSP を使用して CSS（カスケードスタイルシート）ファイルを編集または作成できます。

注: パフォーマンス上の理由により、CA SDM スタイルシートは、2 つの形式で配布されます。つまり、個々のファイル（`search_filter.css` など）と、個々のファイルからコメントや余分な空白を取り除いて 1 つにまとめた組み合わせファイル（`analyst_styles.css` など）です。WSP では常に個々のファイルを編集します。組み合わせファイルを直接編集することはできません。スタイルシートの変更を発行すると、必要に応じて、関連付けられた組み合わせファイルが自動作成されます。

次の手順に従ってください:

1. CCS スタイルシート ファイルを作成するか、または開きます。
スタイルシートのソース ビューが表示されます。
2. ソース ビューで直接編集することも、[ツール] - [スタイル デザイナ] を選択してスタイル デザイナを表示することもできます。
3. 必要に応じて、[\[スタイル デザイナ\] ダイアログ ボックス \(P. 482\)](#) の各フィールドに入力します。ただし、余白や枠線などのように、スタイル デザイナでは表示も編集もできないスタイル属性も多数あります。これらの属性は、ソース ビューで編集する必要があります。
4. スタイル デザイナで [OK] をクリックします。
WSP によってスタイルシートが再フォーマットされ、ソース ビューが更新されます。
5. [ファイル] - [保存] をクリックします。
スタイルシートがカスタマイズされます。

[スタイル デザイナ]ダイアログ ボックス

スタイル デザイナでは、スタイル シートを変更したり、カスタマイズすることができます。デフォルトでは、[スタイル デザイナ] ダイアログ ボックスを開くと、[フォントと色] タブに以下のコントロールが表示されます。

スタイル クラス

ドロップダウン リストから、変更するスタイル エLEMENTを選択します。

追加

新しいスタイル クラスを追加するには、このボタンをクリックします。

名前の変更

[スタイル クラス] ドロップダウン リストで選択したスタイル クラスの名前を変更するには、このボタンをクリックします。

削除

[スタイル クラス] ドロップダウン リストで選択したスタイル クラスを削除するには、このボタンをクリックします。

使用できるフォント

このプロパティには、システムにインストールされているフォントが一覧表示されます。選択したフォントを[使用できるフォント] リストと[選択したフォント] リストの間で移動するには、とをクリックします。

選択したフォント

このプロパティでは、ブラウザでスタイル クラス エLEMENTの描画に使用される優先フォントの階層 リストを指定します。ブラウザでは、実行中のシステムにインストールされているフォントのうち、リスト内の最初のフォントが使用されます。

階層内で選択したフォントを上下に移動するには、とをクリックします。

フォント サイズ

ドロップダウン リストからフォント サイズを選択します。

太字

ドロップダウン リストからフォント スタイルを選択します。

斜体

ドロップダウン リストからフォント スタイルを選択します。

文字飾りなし

テキストの飾りや特殊効果が必要ない場合は、このオプションを選択します。

下線

テキストに下線を付ける場合は、このオプションを選択します。

取り消し線

テキスト自体に線を引く場合は、このオプションを選択します。

オーバーライン

テキストの上に線を引く場合は、このオプションを選択します。

前景色

〔前景色〕プロパティの右側にある〔参照〕 ボタンをクリックして、テキストエレメントの前景色を選択します。次に、カラーパレットから目的の色を選択して、〔OK〕 をクリックします。

背景色

〔背景色〕プロパティの右側にある〔参照〕 ボタンをクリックして、テキストエレメントの背景色を選択します。次に、カラーパレットから目的の色を選択して、〔OK〕 をクリックします。

透明

スタイルエレメントの背景を透明にする場合は、このオプションを選択します。

スタイルエレメントのサンプルは、ダイアログ ボックスの最下部にあるプレビュー領域に表示されます。

スタイルエレメントの位置を設定するには、〔位置〕 タブをクリックします。〔位置〕 タブには、以下のコントロールが含まれています。

位置

ドロップダウン リストから、いずれかのエレメント位置を選択します。位置プロパティでは、エレメントを静的、絶対、または相対のいずれかの位置に配置します。〔静的〕を選択すると、通常のフローに従ってエレメントが配置されます。〔絶対〕を選択すると、ページの任意の位置にエレメントが配置されます。〔相対〕を選択すると、通常的位置に対して相対的にエレメントが移動します。

左揃え

エレメントのテキスト ボックスの左マージンの値を入力します。ドロップダウン リストからサイズを選択します。このプロパティは、選択された位置が「静的」の場合は無効になります。

トップ

エレメントのテキスト ボックスの上部マージンの値を入力します。ドロップダウン リストからサイズを選択します。このプロパティは、選択された位置が「静的」の場合は無効になります。

幅

エレメントのテキスト ボックスの幅の値を入力します。ドロップダウン リストからサイズを選択します。

高さ

エレメントのテキスト ボックスの高さの値を入力します。ドロップダウン リストからサイズを選択します。

Z-Index

エレメントのテキスト ボックスのスタック順の値を入力します。スタック順の値が大きいエレメントは、常に値が小さいエレメントよりも前に表示されます。**Z-Index** を使用できるのは、エレメントの位置に「絶対」を設定した場合のみです。

注: エレメントのスタック順には、負の値も設定できます。

エレメントの特定プロパティを設定するには、「その他」タブをクリックします。「その他」タブには、以下のコントロールが含まれています。

表示

ドロップダウン リストからエレメントの表示タイプを選択します。表示プロパティでは、エレメントの内容が表示領域に収まらなかった場合にどのように表示するかを設定します。

オーバフロー

ドロップダウン リストからエレメントのオーバフローのタイプを選択します。オーバフロー プロパティでは、エレメントの内容が設定した表示領域に収まらなかった場合の動作を設定します。

表示形式

ドロップダウン リストからエレメントの表示形式のタイプを選択します。表示形式では、エレメントをどのように表示するかを設定します。

カーソル

ドロップダウン リストからエレメントのカーソルのタイプを選択します。カーソルプロパティでは、エレメントにポインタを移動したときに表示されるカーソルのタイプを指定します。

OK

このダイアログ ボックスを閉じて変更を保存するには、このボタンをクリックします。

キャンセル

[スタイル デザイナ] ダイアログ ボックスを閉じるには、このボタンをクリックします。

マウスオーバー プレビュー フォームの変更

マウスオーバー プレビューを使用すると、リンクをクリックしたり、新しい Web ページを開かずに現在のフォームの主要な詳細を表示できます。マウスオーバー プレビューは、リストまたは詳細フォーム上のオブジェクト リンクに一定の時間カーソルを合わせると表示されます。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。マウスオーバー プレビューは、デフォルトでは読み取り専用モードのすべてのリストおよび詳細フォーム上で表示されます。

マウスオーバー プレビューは、デフォルトで **preview_** フォームを持たないフォーム用に作成できます。また、CA SDM 環境で作成したカスタムフォーム用にマウスオーバー プレビューを作成することもできます。

以下の事前定義済みマウスオーバー プレビュー フォームを使用できます。

- **preview_chg.htmlpl** (変更要求)
- **preview_cnt.htmlpl** (連絡先)
- **preview_cr.htmlpl** (リクエスト)
- **preview_in.htmlpl** (インシデント)
- **preview_iss.htmlpl** (案件)
- **preview_KD.htmlpl** (ナレッジ ドキュメント)

- preview_nr.htmlpl（構成アイテム）
- preview_pr.htmlpl（問題）

次の手順に従ってください:

1. カスタマイズ用に以下のいずれかのフォームを開きます。
 - デフォルトでは **preview_** フォームを持たない既存のフォームを開きます。たとえば、**detail_loc.htmlpl** などです。
 - 既存のマウスオーバー プレビュー フォームを開きます。たとえば、**preview_chg.htmlpl** などです。
2. フォームをカスタマイズします。たとえば、フォームにカスタム コントロールを追加または削除します。
3. [ファイル] - [名前を付けて保存] をクリックし、プレフィクスとして **preview_** を使用してファイル名を指定して、[保存] をクリックします。たとえば、**preview_loc.htmlpl** と入力します。

マウスオーバー プレビュー フォームが作成され、カスタマイズされます。

第 8 章: リスト フォーム上のデータ グリッド リストの変更

データ グリッド リストを使用すると、製品ページの内容を、新しいページを開かずにリスト形式で表示できます。このデータ コントロールにはテーブル内のデータ ソースからのアイテムが表示されます。これにより、アイテムの選択、アイテムのソート、およびデータの取得ができます。たとえば、インシデント リスト フォーム上の展開および折りたたみオプションなどです。

次の手順に従ってください:

1. リスト フォームを開きます。
2. デザイン ビューで、フォームの下部、ラベル付きフィールドの下にある青い領域を見つけます。ソース ビューを使用する場合、データ グリッドはコードの以下の行の間にあります。

```
<PDM_MACRO name=lsStart>
```

```
<PDM_MACRO name=lsEnd>
```

以下の例は、デザイン ビューのデータ グリッド領域を示しています。

 締め切り日 (最早) need_by	 締め切り日 (最遅) need_by	 オープン日時 (最早) open_date
 解決日時 (最早) resolve_date	 解決日時 (最遅) resolve_date	 クローズ日時 (最早) close_date
 完了予定日時 (最早) est_comp_date	 完了予定日時 (最遅) est_comp_date	 完了日時 (最早) actual_comp_date
 最小予定コスト QBE.GE.est_cost	 最大予定コスト QBE.LE.est_cost	 最短予定期間 QBE.GE.est_total_time
 最小コスト QBE.GE.cost	 最大コスト QBE.LE.cost	 最短期間 QBE.GE.actual_total_time
If End If 変更要求番号 chg_ref_num テンプレート template_na		

データ グリッド領域のプラス記号は、行の拡張セクション（リスト フォーム グリッド内の行のプラス記号をクリックしたときにのみ表示するフィールド）の始まりを示しています。ソース ビューでは、以下のコードでプラス記号を生成します。

```
<PDM_MACRO name=lsCol attr=open_date label="Open Date" sort="DESC" startrow=yes>  
startrow=yes パラメータは行の開始を指定し、行の拡張セクションを開始します。
```

3. 列をドラッグ アンド ドロップしてリストに移動します。列は行の主要部と拡張セクションの間で移動できます。既存のコントロールをグリッド領域の後ろに移動することはできません。
4. リスト列を挿入するには、コントロールまたは青背景の任意の場所を右クリックし、[列の挿入] または [コントロールの挿入] を選択します。
 - [列の挿入] を選択した場合、**WSP** は現在選択されているコントロールの左側に列を挿入します。
 - [コントロールの挿入] を選択した場合、**WSP** は目的のコントロールをフォームに追加するための [コントロールの挿入] ダイアログ ボックスを表示します。
5. フォームがエンド ユーザにどのように表示されるかを確認するには、[ツール] - [プレビュー] を選択します。外観は **CA SDM** の標準ウィンドウに似ており、ボタンとメニューの大部分は機能しますが、標準セッションではありません。そのため、標準セッションのように使用しないでください。
6. [ファイル] - [保存] をクリックします。
リスト フォーム上のデータ グリッド リストが変更されます。

詳細フォーム上のノートブックの変更

ネストされたタブ（ノートブック）コントロールを使用すると、現在のフォーム内の主要な詳細を展開したり、折りたたんだりできます。たとえば、インシデント詳細フォームのタブの配置をカスタマイズできます。デザインビューから、[ノートブック] コントロールを使用して、まだネストされたタブが含まれていない詳細フォームにネストされたタブを追加できます。ノートブックを修正するには、ノートブックをダブルクリックします。ドラッグアンドドロップを使用して、ノートブック タブを追加、挿入、削除し、そのキャプションを変更できます。また、タブを選択し、上向きまたは下向きの矢印ボタンをクリックして、順序を変更できます。[新しい行] チェック ボックスでは、選択されているタブをノートブック ヘッダの新しい行から開始するかどうかを指定します。

次の手順に従ってください:

1. 詳細フォームを開きます。
2. デザイン ビューで、数字付きの最初のラベルを含むフォームの青い領域を見つけます。

ソース ビューを使用する場合、ノートブック領域はコードの以下の行の間にあります。

```
<PDM_MACRO name=startNotebook hdr=cng_nb>  
<PDM_MACRO name=endNotebook>
```

注: CA SDM r12.6 では、ノートブックにネストされたタブを追加できます。WSP では、上位レベル タブ（他のタブを含むタブ）をタブ グループと呼びます。WSP では、タブ グループは青いノートブック領域全体にまたがる濃い青のバーとして示され、数字付きのラベルがその中央に表示されます。下位レベルのタブ（他のタブを含まないタブ）は、タブと呼ばれます。WSP では、下位レベルのタブは角丸の長方形として表示されます。

3. タブをクリックして選択します。タブを選択すると、ノートブックの最下部に、そのタブの内容へのリンクが表示されます。

ドラッグ アンド ドロップを使用して、ノートブック内でタブおよびタブ グループを移動できます。タブ グループを移動すると、そのグループ内のすべてのタブも一緒に移動します。

4. タブまたはタブ グループを挿入するには、コントロールまたはノートブックの青背景を右クリックし、[タブの挿入]、[タブ グループの挿入]、または[コントロールの挿入]を選択します。

[タブの挿入] または [タブ グループの挿入] を選択した場合、WSP は現在選択されているコントロールの左側に新しいタブまたはタブ グループを挿入します。[コントロールの挿入] を選択した場合、WSP は目的のコントロールをフォームに追加するための [コントロールの挿入] ダイアログ ボックスを表示します。

5. フォームがエンド ユーザにどのように表示されるかを確認するには、[ツール] - [プレビュー] を選択します。外観は CA SDM の標準ウィンドウに似ており、ボタンとメニューの大部分は機能しますが、標準セッションではありません。そのため、標準セッションのように使用しないでください。

[ファイル] - [保存] をクリックします。

HTML および JavaScript ファイルの変更

WSP のソース ビューを使用して、HTML フォームおよび JavaScript フォームを編集できます。HTML ファイルまたは JavaScript ファイルを開いて、必要な変更を行います。

注: パフォーマンス上の理由により、CA SDM JavaScript の一部のファイルは、2 つの形式で配布されます。つまり、個々のファイル

(window_manager.js など) と、個々のファイルからコメントや余分な空白を取り除いて 1 つにまとめた組み合わせファイル (std_head.js など) です。WSP では常に個々のファイルを編集します。組み合わせファイルを直接編集することはできません。スタイルシートの変更を発行すると、必要に応じて、関連付けられた組み合わせファイルが自動作成されます。

テストシステムから実稼働システムへのマイグレート

WSP のデザイン段階での目標の 1 つは、実稼働データベース上で、フォームの変更とテストを安全に行えるようにすることでした。この目標は、サーバ上の **Web Screen Painter** のみのディレクトリ ツリー、**Web Screen Painter** 専用のサーバプロセス、読み取り専用のプレビュー セッションなどの機能により達成されています。-- しかし、ユーザの多くは、独立したテストシステム環境でフォームを変更してから、以下を実行して、完成したフォームを別の実稼働システムにマイグレートすることを望んでいます。

1. マイグレートする HTML フォームを、テストシステムの `site/mods/www/html` にある適切なサブディレクトリから、実稼働システムの `site/mods/wsp/project` にある同じサブディレクトリにコピーします。
2. マイグレートする CSS、JavaScript、および HTML ファイルを、テストシステムの `site/mods/www/wwwroot` にある適切なサブディレクトリから、実稼働システムの `site/mods/www/wwwroot/wsp/project` にある同じサブディレクトリにコピーします。

注: CA SDM の設定に応じて、実稼働システムの以下のサーバ上のファイルおよびフォームをコピーしてください。

- 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

注: 手順 1 および 2 のコピー操作は、お使いのオペレーティングシステムでサポートされているどの方法で行ってもかまいません。Windows ユーザは、ディレクトリ パスのスラッシュ (/) をバックスラッシュ (\) に置き換えてください。

フォームの変更の発行

変更の完了後、変更を発行して、すべての CA SDM ユーザが変更を利用できるようにします。発行すると、すべての CA SDM サーバに、新規フォームまたは改訂されたフォームが反映されます。

次の手順に従ってください:

1. [ファイル] - [発行] を選択します。

保存されていない変更がある場合は、変更の保存を要求するメッセージが表示されます。次に、保留中のすべての **Web Screen Painter** の変更（以前のセッションで保存された変更や、**Web Screen Painter** のほかのユーザによって保存された変更も含む）を示す確認ダイアログ ボックスが表示されます。デフォルトでは、すべての変更が発行対象として選択されています。発行する変更の選択を変更するには、その変更をクリックします。

2. 選択が完了したら、[OK] をクリックします。
3. （高可用性設定のみ）いずれかの **CA SDM** サーバ上で **Web** エンジンが実行されていない場合は、**WSP** が発行に失敗した **CA SDM** サーバのリストを含むエラー メッセージが表示されます。以下の手順に従います。

- a. **CA SDM** サーバ（エラー メッセージで指定されたサーバ）を設定して修正を行います。

- b. **WSP** でファイルを編集して `<PDM_IF 0>` マクロ内にスペース文字を追加し、保存します。

- c. 手順 1 に戻って、**Web** フォームを再発行します。

注: 設定の変更をまったく行わない場合は、バックグラウンドサーバの `nx_root/site/mods/www` フォルダをほかのすべてのサーバに手動でコピーする必要があります。

4. （高可用性設定のみ）発行中にバックグラウンドサーバがクラッシュした場合は、[HTMLPL の変更を回復します](#) (P. 492)。
5. （マウスオーバー プレビュー フォームの場合）変更を発行した後、以下のコマンドを実行します。

```
pdm_webcache - H
```

Web キャッシュがリフレッシュされます。**WSP** は、選択された変更を、すべてのサーバ上のすべてのアクティブなユーザから使用可能にします。

HTMLPL の変更の回復

アクティビティの発行中にバックグラウンドサーバに障害が発生した場合は、**HTMLPL** の変更を回復します。

重要: 実稼働環境で回復手順を直接実行することは推奨されません。まず、テストまたは開発環境で検証するようにしてください。

次の手順に従ってください:

1. クラッシュしたバックグラウンド サーバの以下のディレクトリに移動します。
`$NX_ROOT$/site/mods/www/wwwroot/wsp/project/web`
2. この **web** フォルダのすべての内容をコピーします。
3. 新しいバックグラウンド サーバにログインし、コピーしたすべての内容を `$NX_ROOT$/site/mods/www/wwwroot/wsp/project/web` フォルダ内に貼り付けます。
4. 新しいバックグラウンド サーバで変更の発行を再開します。詳細については、「[フォームの変更の発行](#) (P. 491)」を参照してください。

発行後のフォームの削除

削除できるフォームは、サイトで変更したフォームのみです。発行済みフォームを削除するリクエストは、変更の発行時に有効になります。

保留中の削除リクエストをキャンセルするには、[ファイル] - [フォームの削除の取り消し] を選択します。発行後にフォームの変更を元に戻します。発行済みフォームを変更する唯一の方法は、それをもう一度編集することです。

HTML テンプレート (HTMPL フォーム)

CA SDM Web インターフェースのフォームは、HTML テンプレートとして、.html のサフィックスを持つファイルで配布されます。本書ではこれを「HTMPL フォーム」と呼びます。

HTMPL フォームには、標準 HTML (JavaScript を含む) と言語拡張が含まれます。この言語拡張は、標準 HTML をブラウザに配布する Web エンジンと呼び出した CA SDM サーバデーモン (またはサービス) によって解釈されたものです。このような拡張には、以下のものがあります。

- サーバ変数の参照。これは、名前の前のドル記号で示されます。CA SDM データベースの列の値、Web エンジン設定プロパティの参照、またはその他のサーバ情報です。

- サーバ上でのタスク（CA SDM データベースからの情報の読み取りなど）の実行を Web エンジンに命令する特別なタグ。これらのタグの名前は、<PDM_...> または <pdm_...> の形式になります。

注: WSP を使用して CA SDM フォームをカスタマイズするために、HTML 拡張や HTML そのものについて理解する必要はありません。

関連項目:

[サーバの変数](#) (P. 526)

[HTML タグ](#) (P. 499)

テンプレートの命名規則

基本的な 4 種類の HTML 파일을識別するために、以下の命名規則が使用されます。xxx は、オブジェクトを表しています。

テンプレートタイプ	名前
リスト（検索フィルタと結果）	list_xxx.html
読み取り専用の詳細フォームと詳細編集フォームを組み合わせたもの（アナリスト用インターフェース）	detail_xxx.html
読み取り専用の詳細フォーム	detail_xxx_ro.html
詳細編集フォーム	detail_xxx_edit.html

オブジェクトの定義およびプロパティは、以下の場所にあります。

- (UNIX) \$NX_ROOT/bopcfg/majic/*.maj
- (Windows) *installation-directory*\bopcfg\majic*.maj

CA SDM を定義するオブジェクトや属性の詳細については、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。

HTML ファイルディレクトリ

CA SDM に用意されている Web インターフェースについては、「管理ガイド」で説明されています。これらのインターフェースを実装するために使用する一連の HTML ファイルは、以下の表に示すようにオペレーティング システムごとに用意されています。

オペレーティング システム	HTML ファイルがあるディレクトリ
Windows	<i>Installation-directory¥bopcfg¥www¥html¥web¥interface</i>
UNIX	<i>\$NX_ROOT/bopcfg/www/html/web/interface</i>

この表で *interface* はインターフェースの名前（アナリスト、顧客、または従業員）を示しています。

注: ゲスト用インターフェース ファイルのディレクトリはありません。デフォルトでは、このインターフェースでは従業員用インターフェース ファイルが使用されます。ゲスト ユーザ用インターフェースを変更するには、ユーザの **System_Anonymous** に関連付けられているアクセス タイプを変更します。現在のユーザが既知のユーザであるか、またはゲストであるかに応じて、顧客用のファイルと従業員用のファイルはこのドキュメントで説明されている **<PDM_IF>** テンプレート コマンドを使用して動的に変更されます。

html ディレクトリには、以下の 3 つのサブディレクトリが含まれます。

default

すべてのインターフェースに共通の HTML ファイルが含まれています。Web エンジンでは、ファイルの検索時に、現在のユーザのインターフェースに対応するディレクトリを最初に検索し、その後で default ディレクトリを検索します。

pda/analyst: (UNIX)

pda¥analyst: (Windows)

モバイルデバイス用インターフェースで使用する HTML ファイルが含まれています。Unicenter Service Desk r11.0 のモバイルデバイス用インターフェースは、アナリストのみを対象として提供しています。

`web/interface/legacy`: (UNIX)

`web¥interface¥legacy`: (Windows)

現在はもう使用されていない、以前のリリースの CA SDM の HTML ファイルが含まれています。CA SDM のインストール時に以前のリリースからアップグレードすると、このディレクトリが自動的に作成されます。カスタマイズしたファイルが、**legacy** ディレクトリ内のどのファイルも参照しない場合は、**legacy** ディレクトリを削除できます。

提供されている HTML ファイルに直接変更を加えることは決してしないでください。変更する場合は、WSP を使用するか、対象ファイルを `site/mods` ディレクトリに手動でコピーしてから変更を加えてください。CA SDM Web サーバは新規フォームを検索するときに、適切な `site/mods` ディレクトリを検索してから、配布ディレクトリを検索します。各インターフェースの標準の `site/mods` ディレクトリは、以下のとおりです。

オペレーティング システムで変更した HTML ファイルのディレクトリ

Windows	<code>installation-directory¥site¥mods¥www¥html¥interface¥interface</code>
UNIX	<code>\$NX_ROOT/site/mods/www/html/interface/interface</code>

注: フォームを変更して `install directory¥site¥mods¥www¥html¥interface` ディレクトリに保存すると、ユーザが属するフォーム グループとは無関係に、フォームはすべてのユーザに公開されます。変更したフォームを `install directory¥site¥mods¥www¥html¥interface¥interface` ディレクトリに保存すると、そのフォーム グループに属していると定義されている連絡先のみが変更されたフォームを参照できます。

上記の表で **interface** はインターフェースの名前（アナリスト、顧客、または従業員）を示しています。ゲスト用インターフェース ファイルのディレクトリはありません。このインターフェースでは従業員用インターフェース ファイルが使用されます。変更した HTML ファイルを `site/mods` ディレクトリに保存することには、CA SDM のメンテナンス リリースや新規リリースをインストールしてもこのディレクトリがそのまま保持されるという利点があります。また、オリジナルファイルを残したまま、変更後のファイルを `site/mods` ディレクトリに保存することで、最初に配布された HTML ファイルの正確なコピーが常に確保された状態になります。

以下の表に、主な HTML テーブルを示します。各 Web インターフェース ページには、それぞれ主要な機能があります。ただし、<PDM_FORM>ブロックをテンプレートに追加すると、Web インターフェースがサポートされる操作に直接アクセスできます。たとえば、メインメニューを変更して、中間ページを介さずに案件をサブミットするフィールドを含めたり、検索基準フィールドや検索ボタンをリスト フォームに追加したりできます。

Web ページ	HTML テンプレート
メイン フォーム	menu_frames.htmlpl
変更要求の表示/作成/更新	detail_chg.htmlpl
変更要求のリストの表示	list_chg.htmlpl
案件の表示/作成/更新	detail_iss.htmlpl
案件のリストの表示	list_iss.htmlpl
リクエストの表示/作成/更新	detail_cr.htmlpl
リクエストのリストの表示	list_cr.htmlpl
アナウンスメントの詳細情報の表示	detail_cnote_html
アナウンスメントのリストの表示	list_cnote.html
Login	login.htmlpl

注: テンプレートの完全なリストが必要な場合は、このセクションの最初の表に記載されているディレクトリの内容を確認してください。

Web フォーム グループ

カスタマイズした Web ページを 1 つまたは複数のフォーム グループにまとめることができます。フォーム グループのディレクトリは、以下のディレクトリに含まれます。

Windows

```
install-directory¥site¥mods¥www¥html¥web¥interface
install-directory¥site¥mods¥www¥wwwroot¥subdirectory
```

UNIX

```
$NX_ROOT/site/mods/www/html/web/interface
$NX_ROOT/site/mods/www/wwwroot/subdirectory
```

各フォーム グループは、これらのディレクトリのサブディレクトリになります。カスタマイズしたフォームのディレクトリは、アクセス タイプの [カスタム フォーム グループ] フィールドで指定します。

ユーザがフォームをリクエストすると、Web エンジン是最初に、カスタム フォーム グループの適切なディレクトリを検索します。次に、ユーザの Web インターフェースの標準ディレクトリを検索し、最後に **default** ディレクトリを検索します。1 つの Web インターフェースに対して複数のアクセス タイプを定義し、それぞれに異なるカスタム フォーム グループを指定できます。このようにすると、標準インターフェースのフォームの大部分を利用しながら、ユーザ タイプごとに特別なフォームを定義できます。

wwwroot のいずれかのサブディレクトリ (**css**、**html**、**img**、または **scripts**) にあるファイルが Web ページからリクエストされた場合も、同様のプロセスが発生します。Web エンジンにはフォーム **CAisd/img/xxx.gif** の HTML 参照を調べて、以下のいずれかの **gif** ファイルに変換します (最初に見つかった **xxx.gif** が選択されます)。

- **/CAisd/sitemods/img/formgroup/xxx.gif**
- **/CAisd/sitemods/img/xxx.gif**
- **/CAisd/img/xxx.gif**

Web フォームグループの作成方法

Web フォームグループを作成するには、以下の手順に従います。

1. 事前定義済みのアナリスト、顧客、または従業員フォーム グループ以外にフォーム グループが必要な場合は、**WSP** の [ファイル] メニューから [名前を付けて保存] を選択し、[フォームに名前を付けて保存] ダイアログ ボックスで [フォーム グループを追加] ボタンをクリックして、フォーム グループを作成します。たとえば、アナリスト用インターフェースに 2 つのカスタマイズフォームを追加する場合は、**Analyst1** および **Analyst2** というフォーム グループを作成します。定義するインターフェースが事前定義済みのフォーム グループに当てはまらない場合にも、新規フォーム グループを作成できます。

2. Web インターフェース (Web Screen Painter のプレビュー セッションではない) で、[管理] メニューから [セキュリティ] - [アクセス タイプ] を選択します。次に、アクセス タイプをクリック (またはアクセス タイプを作成) し、[アクセス タイプの詳細] ウィンドウの [カスタム フォーム グループ] ドロップダウン リストを使用して、アクセス タイプにフォーム グループを割り当てます。CA SDM は、連絡先のログイン時にアクセス タイプを判別し、カスタム フォーム グループを使用して、`site/mods` ディレクトリ構造のどこからカスタム フォームを検索するかを特定します。フォーム グループのディレクトリ内でフォームが見つからない場合、最初にユーザのアクセス タイプの標準ディレクトリ内が検索され、次に `default` ディレクトリが検索されます。
3. WSP で、[ファイル] メニューから [保存] を選択するか、カスタマイズした HTML 파일을 手動で以下のディレクトリにコピーしてください。

Windows :

`installation-directory\%site%\mods\www\html\web\form_group_name`
ディレクトリ

UNIX : `$NX_ROOT/site/mods/www/html/web/form_group_name`

新規 Web フォーム グループを設定し、適切なサブディレクトリにサポート ファイルをコピーしたら、Web サービスを再起動して変更を反映させる必要があります。

HTML タグ

このセクションでは、HTML タグを追加する PDM コマンドについて説明します。

関連項目:

[PDM EVAL: プリプロセッサ変数の値を挿入 \(P. 500\)](#)
[PDM FORM: セッション ID により HTML フォームを開始 \(P. 501\)](#)
[PDM FMT: サーバ変数のテキストをフォーマット \(P. 501\)](#)
[PDM IF: 条件付き処理 \(P. 504\)](#)
[PDM INCLUDE: 別のファイルからの挿入 \(P. 506\)](#)
[PDM JSCRIPT: 条件付きでの JavaScript ファイルの挿入 \(P. 507\)](#)
[PDM LINK: HTML 操作を呼び出すハイパーリンクの作成 \(P. 508\)](#)
[PDM LIST: データベース行のリストのフォーマット \(P. 509\)](#)
[PDM MACRO: マクロ ファイルからテキストを挿入 \(P. 513\)](#)
[PDM NOTEBOOK: ノートブックの作成 \(P. 520\)](#)
[PDM PRAGMA: サーバ情報の指定 \(P. 521\)](#)
[PDM SCOREBOARD: スコアボードツリーの構築 \(P. 522\)](#)
[PDM SET: サーバ変数の値の設定 \(P. 523\)](#)
[PDM TAB: ノートブック内のタブの作成 \(P. 524\)](#)
[PDM WSP: WSP プレビューのコントロール \(P. 524\)](#)

PDM_EVAL: プリプロセッサ変数の値を挿入

`pdm_eval` タグは、プリプロセッサ変数の値を Web エンジン パーサの入力に挿入する場合に使用します。このタグをマクロ内で使用した場合、マクロが完了するまでタグは機能しません。

`pdm_eval` タグは、`pdm_include` や `pdm_macro` と同様に機能します。変数の値がタグの位置にコーディングされるのと同様に、パーサ内のこのタグの位置にテキストが挿入されます。

`pdm_eval` の構文を以下に示します。

```
<PDM_EVAL TEXT=PRE.name>
```

name

(必須) プリプロセッサ変数の名前。この変数の値が、Web エンジンの入力に挿入されます。

PDM_FORM: セッション ID により HTML フォームを開始

<PDM_FORM>と</PDM_FORM>を Web インターフェースの任意の HTML テンプレートに追加することで、サーバ変数の SID（セッション ID）と FID（フォーム ID）を表す 2 つの非表示フィールドを含む HTML フォームを作成できます。オプションの OP オペランドは、PDM_LINK タグと同様に、サポートされている操作の 1 つを表す非表示フィールドを追加作成します。自動生成された非表示フィールドを除き、<PDM_FORM>と</PDM_FORM>は、標準 HTML の<form>タグおよび</form>タグと同じ方法で使用されます（拡張の一部として<form>タグと</form>タグが生成されます）。

PDM_FMT: サーバ変数のテキストをフォーマット

<PDM_FMT>タグと</PDM_FMT>タグは、サーバ変数（\$args.xxx）の引数に従って挿入されたテキストブロックをフォーマットする場合に使用します。

注: <PDM_FMT> は、\$prop.xxx 変数などのリテラルでは無視されます。

以下の表は、これらのタグの説明です。

プロパティ	説明
ESC_STYLE= NONE C HTML JS JS2 URL	フォーマットされたテキストのエスケープ タイプを指定します。有効な値は以下のとおりです。 NONE デフォルト設定。コンテンツの本文に特別な処理を行わないことを指定します。 C C プログラムの場合に、'、"、¥、¥r、`、および¥n の文字に対して特殊な処理を行います。これらの文字はエスケープされます。 HTML HTML テキストの場合に、以下の文字に対して特別な処理を行います。 & を &amp; に変換 ' を &apos; に変換 " を &quot; に変換 < を &lt; に変換 > を &gt; に変換 JS JavaScript テキストの場合に、以下の文字に対して特別な処理を行います。 ' を %27 に変換 " を %22 に変換 / を %2F に変換 ¥ を %5C に変換 ¥r を %0D に変換 ¥n を %0A に変換 JS2 JS と同じですが、文字「/」に対しては特別な処理を行いません。また、特別な処理を行う文字に以下の 2 つが追加されます。 - % を %25 に変換 - 改行にサフィックス「%0A」を付ける URL 英数字および「@*-_.#」以外のすべての文字を「%xx」に変換します。この「xx」は、変換された文字の 16 進コーディングです。

プロパティ	説明
JUSTIFY=LEFT CENTER RIGHT TRUNCATE WRAP LIN	フォーマットされたテキストの両端揃えを指定します。以下に有効な値を示します。 TRUNCATE デフォルト設定。「<」と「>」を「&lt;」と「&gt;」に置き換えて HTML フォーマットを除去します。 注: 詳細については、KEEPLINKS と KEEPTAGS に関する以下の情報を参照してください。 LEFT CENTER RIGHT 必要に応じて文字の切り捨てやスペースの埋め込みを行い、WIDTH で指定されている文字数にします。改行が埋め込まれている場合は 1 つのスペースに置き換えられ、出力テキストは <pre>タグと</pre>タグで区切られます。WIDTH 引数には正の整数を指定する必要があります。 WRAP テキストの折り返しで単語の境界を無視しない(単語内に改行を入れない) ことを除き、LEFT と同じです。 LINE TRUNCATE と同じです。ただし、埋め込まれている改行も、すべて
タグに置き換えられます。
KEEPLINKS=YES NO	KEEPLINKS=YES が指定されている場合、JUSTIFY=LINE または JUSTIFY=TRUNCATE のアクションが変更され、HTML のアンカー タグ (アクション:) が保持されるようになります。ただし、これ以外の「<」と「>」はすべて変換されます。KEEPTAGS と同時に指定することはできません。
KEEPNL=YES NO	PDM_FMT の標準アクションでは、埋め込まれているすべての改行と後続のスペースが、1 つのスペースに変換されます。 KEEPNL=YES が指定されている場合は、埋め込まれている改行は保持されます。JUSTIFY=LINE の場合、この引数は無視されます。
KEEPTAGS=YES NO	KEEPTAGS=YES が指定されている場合、すべての HTML タグを保持するように、JUSTIFY=LINE または JUSTIFY=TRUNCATE のアクションが変更されます。KEEPLINKS と同時に指定することはできません。
PAD=YES NO	PAD=NO を指定すると、PDM_FMT は空の文字列を 1 つのスペースに変換しません。WIDTH がゼロ以外の場合や、JUSTIFY が TRUNCATE または WRAP の場合は、これが標準のアクションです。

プロパティ	説明
WIDTH= <i>nn</i>	ゼロ以外のときは、WIDTH で指定したとおりの文字数にテキストがフォーマットされます。

<PDM_FMT>に WIDTH または JUSTIFY の指定がない場合、囲まれたテキストはフォーマットされずに、<pre>と</pre>で囲まれます。

たとえば、複数行にまたがる説明を作成するには、以下のように入力します。 -

```
<PDM_FMT WIDTH=50 JUSTIFY=WRAP>$args.description</PDM_FMT>
```

複数列にまたがる出力を作成するには、以下のように入力します。 -

```
<PDM_FMT><PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.last_name</PDM_FMT>
<PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.first_name</PDM_FMT>
<PDM_FMT WIDTH=20 JUSTIFY=TRUNCATE>$cst.middle_name</PDM_FMT>
</PDM_FMT>
```

PDM_IF: 条件付き処理

以下のタグは、テキストに条件を含める場合に使用します。 <PDM_IF>ブロックは、HTMPL ファイル内の任意の場所に置くことができます。HTML や JavaScript のほか、HTML タグ内に置くことも可能です。 <PDM_IF> と <PDM_ELIF> (else if) は、名前と値のペアではなく、プロパティとして、単純な条件節を取ります。 - 節が **true** の場合は、開始タグと終了タグの間にあるテキストがファイルに含まれます。節が **false** の場合は、開始タグと終了タグの間のテキストは破棄されます。終了タグには、<PDM_ELIF>、<PDM_ELSE>、または</PDM_IF>を指定できます。

<PDM_ELSE>タグと<PDM_ELIF>タグはオプションです。この両方を指定する場合は、すべての<PDM_ELIF>タグを<PDM_ELSE>の前に指定する必要があります。<PDM_IF>と<PDM_ELSE> (または<PDM_ELSE>が省略されている場合は</PDM_IF>)の間には、<PDM_ELIF>タグをいくつでも指定できます。

<PDM_IF>および<PDM_ELIF>内の条件の構文を、以下に示します。

- 0 は false、それ以外の数字はすべて true
- "" は false、"any-string" は true
- "value op value" と指定すると、左の値と右の値が、演算子 (op) に従って評価されます。両方の値が数値の場合 (オプションで先頭に - または + を付けることが可能)、両方の数値が比較されます。それ以外場合、これらの値は文字として比較されます (ASCII 照合)。以下に有効な op 値を示します。

op 値	説明
==	等しい
!=	等しくない
>=	以上 (¥>= または >= と記述する必要がある)
<	より小さい (¥< または < と記述する必要があります)
>	より大きい (¥> または > と記述する必要があります)
<=	以下 (¥<= または <= と記述する必要がある)
&	左右の値のビット論理和を実行します。何らかのビットが設定された場合は True、何も設定されていない場合は false です。
%	左の値が右の値の倍数である場合は true が返され、それ以外の場合は false が返されます (2 次元テーブルを作成するときに便利です)。
:	UNIX の grep コマンドのように、バイト指向のパターンマッチを実行します。右の値で指定した正規表現が、左の値に含まれている場合、true が返されます。

例：

```
<PDM_IF $count ¥>= 10> . . .  
<PDM_ELIF $count &lt; 5> . . .  
<PDM_ELSE> . . .  
</PDM_IF>
```

PDM_IF ステートメントには複数の条件を指定できます。条件は、&&（論理積）または||（論理和）のいずれかの結合子で区切ります。どちらの結合子を先に指定しても構いません。Web エン진은、左から右へ結合子に達するまで条件を検証します。最初の条件が **true** で結合子が||である場合、Web エン진은それ以降の評価を続行せず、条件全体が **true** であると判断します。最初の条件が **false** で結合子が&&である場合、Web エン진은それ以降の評価を続行せず、条件全体が **false** であると判断します。それ以外の場合は、条件の評価結果が確定しないので、結合子の後の条件も評価されます。

PDM_INCLUDE: 別のファイルからの挿入

<PDM_INCLUDE>タグは、別のファイルのテキストを HTML ファイルに挿入する場合に使用します。<PDM_INCLUDE>タグは、別のファイルの内容に置き換わります。

挿入されるファイルに<PDM_INCLUDE>タグを含めることもできます。ネストの深さに制限はありません。

<PDM_INCLUDE>タグは、以下のプロパティをサポートしています。

プロパティ	説明
FILE=filename	（必須）挿入するファイルを指定します。Web エン진은現在のユーザのアクセスタイプで定義されている方法で、HTML ファイルで使用するディレクトリを検索します。

プロパティ	説明
FIXUP=[YES NO]	(オプション) このファイルを標準 HTML テンプレート ファイルなどの Web インターフェースで解釈するかどうか (たとえば、先頭にドル記号 (\$) が付いている変数を展開し、PDM_LIST や PDM_FORMAT などの CA SDM タグを解釈するかどうか) を指定します。YES は、標準 HTML テンプレート ファイルとしてファイル进行处理することを示します。NO は、挿入されるファイルをリテラル テキストとして処理することを示します。デフォルトは YES です。 注: 以前のリリースとの互換性を保つために、YES の代わりに TRUE または 1、NO の代わりに FALSE または 0 を指定することもできます。ただし、このような指定は今後サポートされなくなる可能性があるため、新しいページでは使用しないでください。
propname=value	プロパティの propname を指定の値にします。プレフィクス「\$prop」を propname に付けると、挿入されたファイルからプロパティ値にアクセスできます。たとえば、以下のように指定すると、挿入されたファイルから \$prop.menubar を参照できます。 <PDM_INCLUDE ... menubar=no> グローバル プロパティを web.cfg 環境設定ファイルに指定することもできます。web.cfg の詳細については、「管理ガイド」を参照してください。 注: 以前のリリースとの互換性を保つために、<PDM_INCLUDE> で指定されているプロパティ値は、先頭に「prop.」を付けない \$propname の形式で参照することもできます。ただし、このような指定は今後サポートされなくなる可能性があるため、新しいページでは使用しないでください。

PDM_JSCRIPT: 条件付きでの JavaScript ファイルの挿入

<PDM_JSCRIPT> タグは、JavaScript ファイルを条件付きでフォームに挿入する場合に使用します。このタグには、以下の 2 つの形式があります。

```
<PDM_JSCRIPT file=xxxx.js [include=yes|no]>
```

Pdm_jscript に file=xxx.js が指定されている場合、このフォームに JavaScript ファイル xxx.js が必要であることを示します。Web エンジンでは、フォームに必要な JavaScript ファイルのリストに、このファイルを追加します。タグはフォームの解析中に処理され、pdm_if の影響を受けません。つまり、挿入先ファイル、挿入されるファイル、またはマクロ内で pdm_jscript タグがファイルを参照すると、そのファイルが JavaScript ファイルのリストに追加されます。

オプションの引数 `include=no` を指定すると、Web エンジンでこのタグを無視することができます。この引数は条件付きでタグを処理することを指定するもので、主にタグがマクロ内で呼び出される場合に使用します。たとえば、以下のような `dtlTextbox` マクロがあるとします。

```
<PDM_JSCRIPT file=spellcheck.js include=&{spellchk}>
```

これは、`spellchk=yes` が指定されている `dtlTextbox` マクロを含むフォームに、JavaScript ファイルの `spellcheck.js` が必要であることを示します。

以下は、`pdm_jscript` タグのもう 1 つの形式です。

```
<PDM_JSCRIPT insert=here>
```

`pdm_jscript` に `insert=here` を指定すると、すべての必須 JavaScript ファイルに標準 HTML `<script>` タグを挿入することが、Web エンジンに対して要求されます。このタグ形式は HTML の生成段階で処理されるため、`pdm_if` の影響を受けます。`insert=here` が指定された `pdm_jscript` タグは `std_head_include.htmlpl` に含まれるため、事実上すべてのフォームに存在します。

注: Web エンジンがスクリプト タグを挿入するのは、`pdm_jscript insert=here` を初めて検出した場合のみです。

PDM_LINK: HTML 操作を呼び出すハイパーリンクの作成

`<PDM_LINK>` および `</PDM_LINK>` を任意の Web インターフェース HTML テンプレートに追加し、HTML 操作を呼び出すリンクを作成できます。`<PDM_LINK>` タグは標準の HTML `<a href=...>` タグを生成し、類似した引数を使用しますが、URL の代わりに CA SDM 操作を指定できます。

形式を以下に示します。*operation* はサポートされる操作を表します。

```
<PDM_LINK OP=operation> ... </PDM_LINK>
```

例 :

```
<PDM_LINK OP=MENU> Menu </PDM_LINK>
```

```
<PDM_LINK OP=CREATE_NEW FACTORY=iss> Submit Issue </PDM_LINK>
```

```
<PDM_LINK OP=LOGOUT> Logout </PDM_LINK>
```

PDM_LIST: データベース行のリストのフォーマット

<PDM_LIST> タグと </PDM_LIST> タグは、複数のレコードに出力される HTML の反復セクションを区切る場合に使用します。 - <PDM_LIST> と </PDM_LIST> の間の内容は、出力するレコードごとに 1 回ずつ繰り返されます。 PDM_LIST には、以下の 2 つのタイプがあります。

- リストを暗黙で指定するオブジェクト属性の内容のリスト。たとえば、リクエスト オブジェクトのプロパティ属性は、そのリクエストに関連付けられているプロパティのリストです。このタイプの PDM_LIST には、常に **SOURCE** プロパティがあります。
- 明示的な **Where** 節が指定されたリスト。このタイプの PDM_LIST には、常に **WHERE** プロパティがあります。

オブジェクト属性<PDM_LIST>では、以下のプロパティを使用します。

プロパティ	説明																						
ESC_STYLE= NONE C HTML JS JS2 URL	フォーマットされたテキストのエスケープ タイプを指定します。有効な値は以下のとおりです。 NONE デフォルト設定。コンテンツの本文に特別な処理を行わないことを指定します。 C C プログラムの場合に、'、"、¥、¥r、`、および¥n の文字に対して特殊な処理を行います。これらの文字はエスケープされます。 HTML HTML テキストの場合に、以下の文字に対して特別な処理を行います。 <table> <tr><td>&</td><td>を &amp; に変換</td></tr> <tr><td>'</td><td>を &apos; に変換</td></tr> <tr><td>"</td><td>を &quot; に変換</td></tr> <tr><td><</td><td>を &lt; に変換</td></tr> <tr><td>></td><td>を &gt; に変換</td></tr> </table> JS JavaScript テキストの場合に、以下の文字に対して特別な処理を行います。 <table> <tr><td>'</td><td>を %27 に変換</td></tr> <tr><td>"</td><td>を %22 に変換</td></tr> <tr><td>/</td><td>を %2F に変換</td></tr> <tr><td>¥</td><td>を %5C に変換</td></tr> <tr><td>¥r</td><td>を %0D に変換</td></tr> <tr><td>¥n</td><td>を %0A に変換</td></tr> </table> JS2 JS と同じですが、文字「/」に対しては特別な処理を行いません。また、特別な処理を行う文字に以下の 2 つが追加されます。 - % を %25 に変換 - 改行にサフィックス「%0A」を付ける URL 英数字および「@*-_.#」以外のすべての文字を「%xx」に変換します。この「xx」は、変換された文字の 16 進コーディングです。	&	を & に変換	'	を ' に変換	"	を " に変換	<	を < に変換	>	を > に変換	'	を %27 に変換	"	を %22 に変換	/	を %2F に変換	¥	を %5C に変換	¥r	を %0D に変換	¥n	を %0A に変換
&	を & に変換																						
'	を ' に変換																						
"	を " に変換																						
<	を < に変換																						
>	を > に変換																						
'	を %27 に変換																						
"	を %22 に変換																						
/	を %2F に変換																						
¥	を %5C に変換																						
¥r	を %0D に変換																						
¥n	を %0A に変換																						

プロパティ	説明
LENGTH= <i>nn</i>	出力行数を指定します（初期設定はすべての行）。
PREFIX= <i>prefix</i>	リスト内のレコードから属性への参照にプレフィックスを指定します。これらの属性は、<PDM_LIST> と </PDM_LIST> の間のテキスト内で、 <i>\$prefix.attr_name</i> という形式で参照されます。PREFIX プロパティは、オブジェクト変数リストではオプションです。PREFIX の指定がない場合は、SOURCE の値がプレフィックスにも使用されます。
SEARCH_TYPE=DISPLAY GET_DOB	リスト フォームを作成するためにサーバが使用する方法を指定します。 DISPLAY フォーム全体に対して単一のクエリを出すことを指定します。 GET_DOB フォームの行ごとに別のクエリを出すことを指定します。 この選択はリストのパフォーマンスに影響します。リストの複雑さ（リストを表示するために必要な結合数）や DBMS の性質に応じて選択する必要があります。GET_DOB のパフォーマンスは DISPLAY よりも予測可能で、デフォルトでは GET_DOB が選択されています。
SORT= <i>index-name</i>	並べ替えで使用するインデックス名を指定します。この引数のデフォルトは DEFAULT、つまり基礎となるファクトリの最初の並べ替えインデックスです。
SOURCE= <i>source</i>	このリストを定義しているオブジェクト変数を指定します。このフィールドは必須です。PDM_LIST ステートメント自体では、 <i>source</i> の前にドル記号（\$）を付けないでください。PREFIX プロパティが指定されていない場合は、 <i>source</i> はリスト上のレコードの属性への参照のプレフィックスとしても使用され、 <i>\$source.attr_name</i> という参照形式をとります。参照として使用される場合は、 <i>source</i> の先頭にドル記号を付ける必要があります。
START= <i>nn</i>	最初の出力行を指定します（初期設定はゼロ）。

例：

```
<table border>
<tr>
<th>Child Change Order Number</th>
<th>Summary</th>
</tr>
<PDM_LIST SOURCE=args.children>
<tr>
<td>$args.children.chg_ref_num</td>
<td>$args.children.summary</td>
</tr>
</PDM_LIST>
</table>
```

プレフィックスの指定がないため、リストされたレコードの属性への参照には、ソース値である `$args.children` がプレフィックスとして付けられます。

Where 節 PDM_LIST では、以下のプロパティを使用します。

プロパティ	説明
FACTORY= <i>name</i>	検索対象のオブジェクトのクラスを指定します。このプロパティは必須です。
LENGTH= <i>nn</i>	出力行数を指定します（初期設定はすべての行）。
ORDER_BY= <i>attr-name</i>	並べ替えの基準となる属性名を指定します。DESC（降順）またはASC（昇順）の修飾子を含めることができます。
PREFIX= <i>prefix</i>	リスト内のレコードから属性への参照にプレフィックスを指定します。これらの属性は、 <code><PDM_LIST></code> と <code></PDM_LIST></code> の間のテキスト内で、 <code>\$prefix.attr_name</code> という形式で参照されます。Where 節のリストでは、PREFIX プロパティは必須です。
START= <i>nn</i>	最初の出力行を指定します（初期設定はゼロ）。
WHERE= <i>where-clause</i>	検索のための Where 節を指定します。（ドット付きの）属性を含めることができます。このプロパティは必須です。

以下に例を示します。

```
<table>
<tr>
<th>Child Change Order Number</th>
<th>Summary</th>
</tr>
<PDM_LIST PREFIX=list FACTORY=chg WHERE="status = 'OP'">
<tr>
<td>$list.chg_ref_num</td>
<td>$list.summary</td>
</tr>
</PDM_LIST>
</table>
```

PDM_MACRO: マクロ ファイルからテキストを挿入

<PDM_MACRO>タグは、マクロ ファイルを HTML ファイルに挿入する場合に使用します。これは PDM_INCLUDE と同様に機能しますが、以下の 2 点が大きく異なります。

- PDM_MACRO によって挿入されるファイルには、必須の引数と、デフォルト値を持つ引数が含まれる、正規の引数リストがあります。
- PDM_MACRO によって挿入されるファイルは、現在のユーザのアクセス ポイントとは関係なく、常に環境設定プロパティ MacroPath で指定されたディレクトリから挿入されます。

NAME=*macroname*

(必須) 挿入するマクロを指定します。Web エンジンではサフィックス「.mac」を追加し、環境設定ファイルのプロパティ MacroPath で指定されたパスでファイルを検索します。

挿入されるマクロに応じて、他のプロパティが必須になることもあります。マクロ ファイルの一般的なレイアウトを以下に示します。

```
コメント
#args
name1 [= value1]
name2 [= value2]
...
#data
data to insert
```

以下に、ファイルのレイアウトを各行について説明します。

- **コメント** - マクロ内で **#args** ステートメントの前に置かれる有効なステートメントはコメントのみです。コメントであることは、先頭に **#** 記号または **//** を付けて示します。
- **#args** - 上記のとおりコーディングする必要があります。つまり、列 1 に **#** 記号を指定し、その行にはほかの情報を記述しません。このステートメントにより、引数の定義やコメントを指定する **args** セクションが開始されます。
- **name [= value]** - マクロの引数を定義します。マクロで有効なのは、**args** セクションで明示的に指定された引数のみです。**args** セクションで引数に指定される値は、その引数のデフォルト値です。デフォルト値を持たない引数は必須であり、**<PDM_MACRO>**ステートメント自体のコール元で指定する必要があります。
- **#data** - 上記のとおりコーディングする必要があります。つまり、列 1 に **#** 記号を指定し、その行にはほかの情報を記述しません。このステートメントにより、データセクション(**PDM_MACRO** を使用してファイルに挿入されるマクロの一部となるもの) が開始されます。データセクションの内容は、データセクションの先頭部分のコメント行も含めて、コール元ファイルにすべて挿入されます。
- **data to insert** - コール元ファイルに挿入するデータです。以下の形式で、引数への参照をこのデータに含めることができます。
- **&{arg_name}** - これらの参照は、コール元が指定した引数の値に置き換わります。コール元で値が指定されていない場合は、デフォルト値に置き換わります。

一般に、**Web** エンジンは、初めて使用するときに一度だけマクロ ファイルを読み取り、解析したマクロを **Web** エンジン自体のメモリに保存します。これによりパフォーマンスが向上しますが、マクロを開発するユーザにとっては不便です。その場合は、環境設定ファイルのプロパティ **SuppressMacroCache** を使用すると、**Web** エンジンのこの動作が抑制され、新しいフォームの処理を開始するたびにメモリ内のすべてのマクロが破棄されるようになります。

PDM_MACRO タグのコメントアウト

<PDM_MACRO>タグをコメントアウトするには、P の前に感嘆符を入力し、<!PDM_MACRO>のように記述します。フォームのコメントアウトした部分がブラウザで処理されないようにするには、<!PDM_MACRO>タグの前に<PDM_IF 0>を、コメントアウトした行の後に</PDM_IF>を記述します。

例：

```
<PDM_IF 0>
```

```
<!PDM_MACRO NAME=dtlDropdown hdr="Status" attr=status lookup=no  
evt="onBlur=YYY"detailSyncEditForms(this)YYY">  
<!PDM_MACRO NAME=dtlDropdown hdr="Priority" attr=priority lookup=no  
evt="onBlur=YYY"detailSyncEditForms(this)YYY">
```

```
</PDM_IF>
```

WSP で使用する事前定義済みマクロ

CA SDM には、多数の事前定義済みマクロが用意されています。これらの大部分は、JavaScript テキストを挿入して、Web フォームの要素を作成します。これらのマクロを使用してフォームを作成および変更するには、Web Screen Painter を使用します。

詳細フォームのマクロ

以下に、詳細フォーム マクロのリストを示します。

button

グラフィック ボタンを挿入します。

dtlCheckbox

詳細フォームにチェック ボックスを挿入します。

dtlDate

詳細フォームに日付フィールドを挿入します。

dtlDateReadonly

詳細フォームに読み取り専用の日付フィールドを挿入します。

dtlDropdown

詳細フォームにドロップダウン リストを挿入します。

dtlEnd

詳細フォームを終了します。

dtlEndTable

詳細フォーム内のテーブルを終了します。

dtlForm

詳細フォームを開始します。

dtlHTMLEditBox

HTML エディタを含むテキスト ボックスとして、詳細フォーム フィールドを挿入します。

dtlHier

階層ルックアップにより外部テーブルと比較検証されるテキスト ボックスとして、詳細フォーム フィールドを挿入します。

重要: HTMPL ファイルで **dtlHier** マクロを **dtlLookup** に変更しないことをお勧めします。オートコンプリートが正しく動作するように、オプションマネージャの **suppress_web_hier_search** オプションを代わりに使用してください。

dtlLookup

外部テーブルと比較検証されるテキスト ボックスとして、詳細フォーム フィールドを挿入します。

dtlLookupReadOnly

外部テーブルへの読み取り専用ハイパーリンクとして、詳細フォーム フィールドを挿入します。

dtlReadOnly

詳細フォームに読み取り専用のテキスト フィールドを挿入します。

dtlStart

詳細フォームの最初のテーブルを開始します。

dtlStartExpRow

詳細フォームの展開可能な行を開始します。

dtlStartRow

詳細フォームの標準行を開始します。

dtlTextbox

詳細フォームにテキスト ボックスを挿入します。

contactLookup

contactLookup マクロは、連絡先ルックアップを作成します。 このマクロには、以下の引数があります。

```
contactLookup("&{header}","&{frameName}","&{factory}","&{lookupName}");
```

header

ルックアップ ヘッダを指定します。

frameName

(必須) フォーム名を指定します。

factory

ファクトリを指定します。

デフォルト : agt

lookupName

(必須) ルックアップ名を指定します。

また、以下のように指定して、このエレメントを有効または無効にすることもできます。

```
contactLookupDisable( Name, bDisable )
```

bDisable=**■ true**

エレメントを無効にします。

■ false

エレメントを有効にします。

dtlCheckboxReadonly

dtlCheckboxReadonly マクロは、HTML 詳細フォームに読み取り専用のチェックボックス フィールドを指定します。このマクロには、以下の引数があります。

```
detailCheckboxReadonly("&{hdr}", "&{attr}", &{colspan}, "$args.&{attr}", "&{on}", "&{off}");
```

hdr

ヘッダのテキストを指定します。

デフォルト: "\$args.&{attr}.DISPLAY_NAME"

attr

(必須) 属性の名前を指定します。

on = "X"

フィールドがオンのときに読み取り専用のフォームに表示する値を指定します。

off = ""

フィールドがオフのときに読み取り専用のフォームに表示する値を指定します。

colspan = 1

フォームの列数を指定します。

読み取り専用のフォームでも、編集フォームでも、フィールドは「on」引数および「off」引数に指定したとおりに表示されます。

注: このマクロは、編集モードでも常に読み取り専用であることを除き、**dtlCheckbox.mac** に似ています。

リスト フォームのマクロ

IsCol

リスト フォーム内の列を指定します。

IsEnd

リスト フォームのリスト部分を終了します。

lsStart

リスト フォームのリスト部分を開始します。

lsWrite

リスト フォームの反復セクションにテキストを挿入します。

sfDate

検索フィルタに日付フィールドを挿入します。

sfDropdown

検索フィルタにドロップダウン リストを挿入します。

sfEnd

検索フィルタを終了します。

sfHier

階層ルックアップにより外部テーブルと比較検証されるテキストボックスとして、検索フィルタ フィールドを挿入します。

sfLookup

外部テーブルと比較検証されるテキスト ボックスとして、検索フィルタ フィールドを挿入します。

sfStart

検索フィルタを開始します。

sfStartRow

検索フィルタ内の行を開始します。

sfTextbox

検索フィルタにテキスト ボックスを挿入します。

メニュー バーのマクロ

以下に、メニューバー マクロのリストを示します。

endMenu

メニュー バー内のメニューを終了します。

menulitem

メニューのグローバル項目を定義します。

endMenubar

メニューバーを終了します。

menultemLocal

現在のウィンドウから呼び出されるメニューの項目を定義します。

menubarItem

メニューバー内のメニューを定義します。

startMenu

メニューバー内のメニューを開始します。

startMenubar

メニューバーを開始します。

PDM_NOTEBOOK: ノートブックの作成

CA SDM アナリスト インターフェースの一部のフォームでは、ネストされたタブ（ノートブック）を使用します。ネストされたタブでは、画面の同じ物理領域に複数のフィールドセットを配置できます。ただし、一度に1つのフィールドセットのみが表示されます。ユーザは、ノートブックの上部にあるタブ名をクリックするか、**Alt+n** のアクセス キー（*n* はタブ番号）を押して、表示するフィールドセットを選択できます。たとえば、ノートブックを使用するフォームの1つに「詳細：案件」

（`detail_iss.htmlpl`）があります。ノートブックの内容を変更する場合や、ノートブックが含まれていないフォームにノートブックを挿入する場合は、**WSP** を使用することをお勧めします。

ノートブックの終了をマークするタブは以下のとおりです。

```
<PDM_MACRO name=endNotebook>
```


PDM_PRAGMA: サーバ情報の指定

<PDM_PRAGMA>タグは、フォームのリリースやバージョンなど、Web エンジンで使用する情報を指定する場合に使用します。このタグは HTML コードを生成せず、フォームの任意の場所に指定できます。使用できる引数は以下のとおりです。

引数	説明
RELEASE=value	このフォームに対応する CA SDM のリリース番号を指定します。この値は、Unicenter Service Desk r11.0 のすべてのフォームで「110」です。\$prop.release 変数を使用してフォーム内でアクセスできます。
SITEMOD=value	フォームに適用されている変更を特定するサイト定義の文字列を指定します。\$prop.sitemod 変数を使用してフォーム内でアクセスできます。
VERSION=value	フォームのバージョン番号を特定する CA Technologies 定義の文字列を指定します。\$prop.version 変数を使用してフォーム内でアクセスできます。
OVERIDE=YES NO	この PDM_PRAGMA ステートメントの値が、前の PDM_PRAGMA ステートメントの値をオーバーライドするかどうかを指定します。

CA Technologies では PDM_PRAGMA ステートメントを使用して、フォームのバージョンを記録します。Unicenter Service Desk r11.0 のすべてのフォームには、以下の PDM_PRAGMA ステートメントが含まれています。

```
<PDM_PRAGMA RELEASE=110>
```

また、std_head.html フォームには、以下の JavaScript ステートメントも含まれています。

```
cfgFormRelease = "$prop.release" - 0;
```

CA SDM Web インターフェースは、PDM_PRAGMA ステートメントと `cfgFormRelease` 変数により、Unicenter Service Desk r11.0 のフォームと以前のリリースのフォームを識別します。Unicenter Service Desk r6.0 以前のリリースは、PDM_PRAGMA ステートメントをサポートしていません。

通常は、フォームの最高レベルのファイル（つまり PDM_INCLUDE で挿入されないファイル）内の PDM_PRAGMA ステートメントのみを使用して、`$prop.release`、`$prop.sitemod`、および `$prop.version` が設定されます。また、以前の PDM_PRAGMA ステートメントで設定された空でない値が、PDM_PRAGMA ステートメントによってオーバーライドされることはありません。OVERRIDE=YES を指定すると、PDM_PRAGMA ステートメントが前の PDM_PRAGMA ステートメントをオーバーライドすること、または挿入されたファイル内の PDM_PRAGMA ステートメントを使用することを指定できます。

PDM_SCOREBOARD: スコアボード ツリーの構築

<PDM_SCOREBOARD>タグは、メイン フォームの左側に表示されるスコアボードを生成するために使用します。以下のプロパティを使用します。

TARGET=value

スコアボードのノードをクリックしてリクエストされるリストのターゲット フレーム名を指定します。リストは指定されたターゲットにロードされます。ターゲットには、リンクのターゲット属性でサポートされる任意の値を指定できます。デフォルト値は `_self`（PDM_SCOREBOARD タグが含まれるウィンドウ）です。

<PDM_SCOREBOARD>タグを含む HTML フォームにも、`fldrtree.js` JavaScript ファイルを含める必要があります。このファイルを含めるには、以下のステートメントをフォームの <HEAD> セクションに指定します。

```
<SCRIPT LANGUAGE="JavaScript" SRC="$CAisd/CAisd/fldrtree.js"></SCRIPT>
```

さらに、ツリー内の番号の発効日を表示するために、`scoreboard_asof_data` という名前のリンクを挿入することをお勧めします。このタグの使用例については、配布ファイル `scoreboard.htmlpl` を参照してください。

スコアボードに挿入されるクエリは、現在のユーザの **User_Query** テーブル（オブジェクト名 **usq**）の内容によって定義されます。このテーブルのレコードは、ツリーの各行（フォルダまたはノード）を定義します。

最初は、**User_Query** テーブルにユーザのエントリはありません。**User_Query** エントリのないユーザは、それぞれのアクセス タイプに関連付けられているスコアボード クエリの初期設定のセットを受信します。管理者権限のあるユーザは、アクセス タイプのスコアボードの初期設定をカスタマイズすることもできます。

PDM_SET: サーバ変数の値の設定

<PDM_SET>タグは、サーバ変数に値を割り当てるために使用します。以下に構文を示します。

```
<PDM_SET arg.name[+]=value>
```

arg

（必須）変数タイプを指定します。標準的に使用される引数を指定する必要があります。

注: \$ の文字は使用しません。

名前

（必須）変数名を指定します。

+

（オプション）変数の既存値に値を追加することを指定します。前後にスペースを入れることはできません。

=

（必須）上記のとおり指定する必要があります。前後にスペースは入れません。

値

（必須）変数に割り当てるテキスト、または追加するテキストを指定します。

PDM_SET タグを前処理フェーズで使用して、プリプロセッサ変数を作成または更新することもできます。

関連項目:

[Web エンジンの前処理](#) (P. 556)

PDM_TAB: ノートブック内のタブの作成

PDM_MACRO name=startNotebook hdr=cng_nb> タグは、ノートブック タブを定義するために使用します。ノートブックの内容を変更する場合や、ノートブックが含まれていないフォームにノートブックを挿入する場合は、WSP を使用することをお勧めします。

PDM_WSP: WSP プレビューのコントロール

<PDM_WSP> タグは、WSP のプレビュー機能を制御するために使用します。このタグは HTML コードを生成せず、フォームの任意の場所に指定できます。

デフォルトでは、WSP はフォーム名を調べて、フォームのプレビュー方法を決定します。

- 詳細フォーム（フォーム名は `detail_factory.htmlpl`）の場合、フォームは編集ビューに表示されます。ビューには、適切なテーブル内で最後に作成された行から取得したデータが表示されます。ユーザが表示を許可されているデータがテーブル内に存在しない場合は、行を作成するフォームが表示されます。通常、WSP のプレビューセッションでデータベースを更新することはできません。編集ビューに表示されるフォームでは、すべての機能をプレビューできます。ただし、読み取り専用のプレビューセッションから出された保存リクエストは無視されます。このことを視覚的に確認できるように、[保存] ボタンは [保存しない] ボタンに変更されます。
- リスト フォーム（フォーム名は `list_factoryhtmlpl`）の場合、フォームはリスト ビューに表示されます。リストには、適切なテーブルで最後に作成された行から取得されたデータが表示されます。ユーザが表示を許可されているデータがテーブル内に存在しない場合、フィルタが開いた状態で、検索ビューにフォームが表示されます。
- それ以外のフォームの場合、WSP はデータベースのコンテキストなしでフォームのみを表示します。

このデフォルト動作は、フォームの任意の場所に **PDM_WSP** タグを指定して変更できます。たとえば、ノートブック タブのフォームを、関連付けられている詳細フォームに表示したり、別のフォームで指定された環境で呼び出されるフォームに、前提条件の引数を指定したりできます。可能な引数は以下のとおりです。

プロパティ	説明
FACTORY=value	このフォームで使用するオブジェクト エンジン ファクトリを指定します。
PREVIEW=name.html value / いいえ	プレビュー URL を指定します。このプロパティには、xxxx.html 形式の HTML ファイル名、CA SDM の URL（「OP=」で始まる場合は変更なしで使用されます）、またはフォームがプレビューできないことを通知するキーワードの「no」を指定できます。 OP= 以外で始まる値の場合、フォーム{factory}または{factory:}の参照は、ユーザが表示を許可された参照ファクトリで最後に作成された行の ID または固定 ID にそれぞれ置き換えられます。
WHERE=value	プレビューされるフォームに表示する各行または複数行を検索する Where 節を指定します。
MODE=value	作成された URL のモードを指定します。以下のいずれかになります。 ■ GENERAL 一般的な形式。PREVIEW の引数を調べて、モードを決定します。 detail_xxxx.html - READONLY list_xxxx.html - LIST その他 - GRONK ■ READONLY。読み取り専用ビュー内の詳細ファイル ■ EDIT。編集ビュー内の詳細ファイル ■ LIST。リスト ファイル ■ GRONK。詳細不明のファイル。この場合、ファイルは無効と見なされます。

サーバの変数

CA SDM の情報は、ドル記号 (\$) が先頭に付く変数を使用して、HTML テンプレートに組み込まれます。各ページは、テンプレート ファイルに記述されている変数を使用して作成されます。以下の変数はページ上に配置することも、条件ステートメントで使用することもできます。

- 簡易変数
- プロパティ変数
- 環境変数
- ビジネス オブジェクト変数
- リスト変数

簡易変数

簡易変数は、Web ページに渡されるフラグを指定します。簡易変数にアクセスするには、ドル記号 (\$) が先頭に付く変数名を使用します。これで変数の値が使用可能になります。このような変数として、**\$CAisd** や **\$cgi** などが挙げられます。テンプレート内に **\$CAisd** を記述すると、メインの CA SDM Web サーバインストールディレクトリが置き換えられます。**\$cgi** は **pdmweb.exe** プログラムの URL を参照します。簡易変数は、それを使用する HTML ファイルの上部に記述します。

すべての HTML ファイルで使用できる変数を以下に示します。

\$ACCESS.group

ユーザ アクセス権限オブジェクトには、現在のログイン ユーザのファンクション グループ *group* に関する権限の設定が含まれます。たとえば **\$ACCESS.admin** には、**admin** ファンクション グループの権限値が含まれます。有効な権限値は以下のとおりです。

- 0—アクセスなし
- 1—表示
- 2—変更

この変数は、ログイン フォームでは使用できません。

\$cgi

pdmweb.exe プログラムの URL。

\$cst

現在のログインユーザのデータ オブジェクト。この変数は、ログインフォームでは使用できません。\$cst.attrname の形式（たとえば、\$cst.first_name）で指定して、このオブジェクトの個々の属性を参照できます。

\$CAisd

メインの CA SDM Web サーバインストールディレクトリの URL。

\$MachineName

web.cfg ファイルに定義されている MachineName。

注: web.cfg の詳細については、「管理ガイド」を参照してください。

\$ProductName

NX.env ファイルに定義されている製品名。

\$SESSION

セッション オブジェクトには、セッション ID（\$SESSION.SID）を含むすべてのセッション変数、および web.cfg ファイルに定義されているすべての変数が保存されます。

注: web.cfg の詳細については、「管理ガイド」を参照してください。

\$USER_STATE

ユーザ定義の状態情報。

プロパティ変数

プロパティ変数は、環境設定ファイル web.cfg のプロパティを表します。HTML テンプレート ファイルから web.cfg ファイルのエントリ（ユーザ定義のエントリも含む）にアクセスするには、プレフィクス「\$prop」を付けます。

たとえば、以下に示す web.cfg ファイルの行は、リスト フォームの 1 ページに表示されるエントリ数を指定します。

ListPageLength 10

以下のように指定すると、この変数を HTML テンプレート内で参照できます。

`$prop.ListPageLength`

特殊タグの<PDM_INCLUDE>を使用して別のファイルをテンプレートに組み込む場合は、<PDM_INCLUDE>タグの属性として追加のプロパティを指定できます。挿入ファイル内のプロパティも、**web.cfg** プロパティと同じ方法で参照できます。<PDM_INCLUDE> 属性として指定されているプロパティの名前が **web.cfg** プロパティと同じ場合、挿入ファイル内の **web.cfg** プロパティがオーバーライドされます。

たとえば、以下の<PDM_INCLUDE>タグは、**std_body.html** ファイル内で参照できる**\$prop.menu** というプロパティを作成します。

```
<PDM_INCLUDE FILE=std_body.html menu=no>
```

注: 環境設定ファイルのプロパティ **xxx** は、**\$prop.xxx** または **\$SESSION.xxx** で参照できます。どちらの方法でも同じ値が返されます。ただし、**\$prop.xxx** 構文の方がサーバのオーバーヘッドが少ないため、**\$prop.xxx** 構文を使用することをお勧めします。

web.cfg のプロパティのほかにも、**\$prop** を指定してアクセスできる事前定義済みプロパティがいくつかあります。これらのプロパティは以下のとおりです。

\$prop.browser

使用されているブラウザを特定する文字列。Internet Explorer の場合は「IE」です。

\$prop.combo_name

現在のユーザ名を「last_name, first_name middle_name」の形式で含む文字列。

prop.factory

現在のフォームに関連付けられているファクトリを含む文字列。たとえば、リクエストの場合は「cr」、案件の場合は「iss」になります。

\$prop.FID

現在のフォームのフォーム ID（数値）を含む文字列。

\$prop.form_name

現在の HTML テンプレート名 (xxx.html の形式) を含む文字列。

\$prop.form_name_1

フォーム名の最初の下線の前にあるサブ文字列を含む文字列。たとえば、フォーム名が detail_chg_edit.html の場合、form_name_1 は「detail」です。

\$prop.form_name_2

フォーム名の最初の下線と最後の下線（またはドット）の間にあるサブ文字列を含む文字列。たとえば、フォーム名が detail_chg_edit.html の場合、form_name_2 は「chg」です。

\$prop.form_name_3

フォーム名の最後の下線とドットの間にあるサブ文字列を含む文字列。たとえば、フォーム名が detail_chg_edit.html の場合、form_name_3 は「edit」です。フォームのファイル名が detail_xxx.html になる組み合わせ詳細フォームでは、\$prop.form_name_3 は現在のビュー（「ro」または「edit」のいずれか）に設定されます。

\$prop.release

フォームのリリース レベルを含む文字列。このプロパティの詳細については、「PDM_PRAGMA ステートメント」を参照してください。

\$prop.SID

現在のセッションのセッション ID (数値) を含む文字列。

\$prop.sitemod

フォームのサイト定義の変更名を含む文字列。このプロパティの詳細については、「PDM_PRAGMA ステートメント」を参照してください。

\$prop.user_type

「アナリスト」、「顧客」、「従業員」、または「ゲスト」を含む文字列。

\$prop.version

フォームのバージョンを含む文字列。このプロパティの詳細については、「PDM_PRAGMA ステートメント」を参照してください。

関連項目:

[PDM PRAGMA : サーバ情報の指定](#) (P. 521)

環境変数

環境変数は、**NX.env** 環境設定ファイル内のエントリを表します。**NX.env** 内のエントリを **HTMPL** テンプレートから参照するには、プレフィクス「**\$env**」を付けてください。

たとえば、**NX.env** の行のうち、**CA SDM** サーバのホスト名を指定する行は以下ようになります。

```
@NX_SERVER=hostname
```

以下のように指定すると、この変数を **HTMPL** テンプレート ファイルから参照できます。

```
$env.NX_SERVER
```

ビジネス オブジェクト変数

ビジネス オブジェクト変数は、案件やリクエストなどの **CA SDM** オブジェクトを表します。オブジェクトにアクセスするには、変数名、ピリオド (.)、表示する属性名の順に続けて指定する必要があります。たとえば、慣例上オブジェクトが変数 **args** で表される案件の場合は、以下のように指定することで、説明、オープン日、担当者の電話番号お、案件のアクティビティ数、最初のアクティビティの説明を表示できます。

```
$args.description  
$args.open_date  
$args.assignee.phone_number  
$args.act_log.length  
$args.act_log.0.description
```

変数名の前後に空白がない場合は、大かっこを使用して変数名を区切ることができます。たとえば、**\$foo bar** と **\${foo}bar** はどちらも有効です。変数 **args** を使用して、非属性値（「サポートされる操作」で説明している **\$args.KEEP.name** など）にアクセスすることもできます。

非属性値が定義されていない可能性もあります。たとえば、2 つの異なる場所からフォームにアクセスしている場合に、そのうちの 1 つだけが **\$args.KEEP.foo** の値を提供していることがあります。この場合は、以下の構文を使用して **\$args** 参照にデフォルト値を指定できます。**variable** が未定義の場合は、コロンの後の文字列が参照の代わりに使用されます。

```
${args.variable:default}
```

タイムゾーン日付変数

タイムゾーン日付変数は、ビジネス オブジェクト変数の中でも特殊なものです。タイムゾーン日付変数は、整数で表される協定世界時 (UTC) を、ユーザのブラウザのタイムゾーンに合わせて文字列の日付に変換する手段を提供します。以下の変数は、整数の日付を表します。

`$args.attr_name_INT_DATE`

例： `$args.open_date_INT_DATE`

ファクトリ データ変数

ファクトリ データ変数は、ビジネス オブジェクト変数の中でも特殊なものです。ファクトリ データ変数は、参照オブジェクトに関する情報に置き換わります。ファクトリ データ変数は、以下の 7 つです。

`$args.attr_name.COMMON_NAME`

属性が参照するテーブルの共通名（外部から読み取り可能な文字列）。たとえば、[リクエストの詳細] フォームでは、`$args.assignee.COMMON_NAME` の値は担当者のコンボ名（「姓、名、middle name」）です。

`$args.attr_name.COMMON_NAME_ATTR`

属性が参照するテーブル内の共通名の属性名。たとえば、[リクエストの詳細] フォームでは、`$args.assignee.COMMON_NAME_ATTR` の値は「combo_name」です。

`$args.FACTORY_attr_name`

指定された属性に関連付けられているファクトリの名前。たとえば、[リクエストの詳細] フォームでは、`$args.FACTORY_assignee` の値は「agt」です。

`$args.LENGTH_attr_name`

属性の最大長。たとえば、[リクエストの詳細] フォームでは、`$args.LENGTH_summary` の値は 240 です。

`$args.attr_name.REL_ATTR`

属性の関連付け属性（外部キー）。たとえば、[リクエストの詳細] フォームでは、`$args.assignee.REL_ATTR` の値は担当者の [ID] フィールドの値です。

`$args.attr_name.REL_ATTR_ATTR`

属性が参照するテーブル内の `rel_attr` の属性名。たとえば、[リクエストの詳細] フォームでは、`$args.assignee.REL_ATTR_ATTR` の値は「id」です。

`$args.REQUIRED_attr_name`

「0」または「1」の文字列で、参照属性が必須かどうかを示します。

`$args.attr_name.SELECTIONS`

`attr_name` の有効な選択肢のリスト。`attr_name` が別のテーブルへの参照でない場合、または `attr_name` が参照するテーブルのサイズが環境設定ファイルの `SelListCacheMax` プロパティを超える場合、この値は空の文字列になります。それ以外の場合、`SELECTIONS` 変数は、参照されるテーブル内のすべてのエントリの共通名と関連付け属性を含む文字列になります。後続の値は文字列「@,@」で区切られます。つまり、この変数の値は、以下の形式になります。

`"cname1@,@rel_attr1@,@cname2@,@rel_attr2"`

`$args.factory_SEL_UNDER_LIMIT`

「0」または「1」の文字列で、`factory` に対応するテーブル内の現在の行数が、環境設定ファイルのプロパティ `SelListCacheMax` の値よりも小さいかどうかを示します。ただし、この変数は今後サポートされなくなる可能性があるため、新規フォームでは `SELECTIONS` 変数を使用してください。

ドット付きの参照を含むファクトリ データ変数（`COMMON_NAME`、`REL_ATTR`、および `SELECTIONS`）は、どのような長さのドット付き参照でも使用できます。たとえば、[リクエストの詳細] フォームでは、`$args.assignee.organization.COMMON_NAME` は、担当者の組織の外部名に置き換わります。

リスト変数

リスト変数はデータを反復する場合に使用します。この変数にアクセスするには、「PDM_LIST：データベース行のリストのフォーマット」の説明に従ってリスト タグを記述します。

サポートされているサーバ操作

CA SDM Web ページをユーザの Web ページに統合するために、以下の操作がサポートされています。

CREATE_NEW

指定のテーブルにユーザが行を作成できる、汎用インターフェースを提供します。オブジェクト名を指定する必要があります。デフォルトにより、オブジェクト名が *xxx* の場合、*detail_xxx_edit.htmlpl* というテンプレートが使用されます。*.htmlpl* ファイルは、HTMLPL プロパティを指定することによってオーバーライドできます。

必須の指定子

FACTORY=*object-name*

オプションの指定子

ALG_PRESET=*preset_expression*
ALG_PRESET_REL=*preset_expression*
CREATE_ALG=*activity_log_type*
HTMLPL=*zdetailxxx_factory.htmlpl*
KEEP.*attr_name*=*value*
PRESET=*preset_expression*
PRESET_REL=*preset expression*
SET.*attr_name*=*value*
use_template=1 | 0 (0 は初期設定値)

注: CREATE_NEW で HTMLPL 指定子を使用するためには、参照されるフォームの名前が命名規則 *zdetailxxx_factory.htmlpl* に従っている必要があります。つまり、文字列「*zdetail*」で始まり、その後に任意の英数字 (Null 文字列も含む)、下線、およびファクトリ名を続ける必要があります。

ENDSESSION または LOGOUT

現在のログインセッションを終了します。 **ENDSESSION** が推奨の操作です。

GENERIC_LIST

ユーザがデータベース内の任意のテーブルからリストを表示できる、汎用インターフェースを提供します。オブジェクト名を指定する必要があります。デフォルトにより、オブジェクト名が **xxx** の場合、**list_xxx.htmlpl** というテンプレートが使用されます。**.htmlpl** ファイルは、HTMLPL プロパティを指定することによってオーバーライドできます。

必須の指定子

FACTORY=object-name
KEEP.attr_name=value

DISPLAY_FORM

ユーザがカスタム フォームを表示できる、汎用インターフェースを提供します。

必須の指定子

HTMLPL=htmlpl_file

注: **JUST_GRONK_IT** は **DISPLAY_FORM** に置き換えられます。既存の実装では、**JUST_GRONK_IT** を引き続き使用でき、**DISPLAY_FORM** とまったく同様に機能します。 **DISPLAY_FORM** が推奨の操作です。

MENU

web.cfg ファイルの **Menu** プロパティで定義されているメイン メニュー ページを表示します。

オプションの指定子

HTMLPL=menufile

menufile は、代替メイン メニュー ファイルの名前です。

PAGE_EXTENSION

Web マスタがインターフェースに拡張を追加指定できるようにします。

必須の指定子

`NAME=html_file`

`html_file` は、環境設定ファイル `UserPageExtensions` ディレクティブに記述されているファイル名の 1 つです。

オプションの指定子

`REQUIRES_LOGIN=1`

この指定がある場合、ユーザがログインしていない場合は、最初にログインページが表示されます。この指定がない場合は、ユーザがログインしているかどうかを確認せずにファイルが表示されます。

RELOG

ログインページを表示します。

SEARCH

データベース内のテーブルを検索できる汎用インターフェースを提供します。この操作では、適切な `search_xxx.htmlpl` が作成されていることを前提としています。`xxx` は、`bopcfg` の `majic` ディレクトリにある各種 `.maj` ファイルで定義されている *object-name* (オブジェクト名) を表します。

注: 詳細については、「CA SDM テクニカル リファレンス ガイド」を参照してください。デフォルトでは、この検索の結果は `list_xxx.htmlpl` に表示されますが、HTMLPL プロパティを指定して無効化できます。

必須の指定子

`FACTORY=object-name`

`QBE.op.attr_name=value`

オプションの指定子

`ALG_PRESET=preset_expression`

`ALG_PRESET_REL=preset_expression`

`CREATE_ALG=activity_log_type`

`HTMLPL=list_htmlpl_file`

`KEEP.attr_name=value`

SEC_REFRESH

セキュリティ サブシステムからのユーザ アクセス情報を更新します。この操作のハイパーリンクは、メニュー画面の変更権限 (**admin** 機能グループ) を持つユーザに対して表示されます。セキュリティ プログラムによってユーザ アクセス権限が更新された後で、この操作を行って、アクセス情報を更新できます (すべてのユーザのセキュリティ情報が更新されます)。

注: セキュリティの更新は非同期プロセスです。セキュリティが更新されると、標準ログ ファイル (**stdlog**) にメッセージが記録されます。

SET_MENU

この操作は、**HTMPL** 変数で **MENU** が使用されている場合の **MENU** と同様の動作をします。唯一の相違点は、この操作では、デフォルトのメニュー フォームを、**HTMPL** プロパティで指定されているメニュー フォームにも設定することです。

必須の指定子

HTMPL=html_file

注: この操作を行うと、Web サービスが再起動されるまでの間、**web.cfg** の **MENU** セットがオーバーライドされます。

SHOW_DETAIL

指定されたテーブルに含まれる行の読み取り専用の詳細情報をユーザが表示できる、汎用インターフェースを提供します。 - 固定 **ID** 名を指定する必要があります (オブジェクト名は、この固定 **ID** 名から推測されます)。デフォルトでは、オブジェクト名が **xxx** の場合、**detail_xxx_ro.html** というテンプレートが使用されます。この **.html** ファイルは、**HTMPL** プロパティを指定して無効化できます。

必須の指定子

PERSID=persistent-id

オプションの指定子

ALG_PRESET=preset_expression
ALG_PRESET_REL=preset_expression
CREATE_ALG=activity_log_type
HTMPL=readonly_detail_html_file

UPDATE

テーブルを編集するための汎用インターフェースを提供します。編集可能な詳細フォームをユーザに対して表示するためには、ID とオブジェクト名を渡す必要があります。デフォルトでは、ユーザは 2 分間だけレコードに排他的にアクセスでき、この時間内にサブミットした変更は必ずデータベースに反映されます。

必須の指定子

PERSID=*persistent-id* または
SET.id=*id-of-row-to-update* FACTORY=*object-name*

オプションの指定子

NEXT_PERSID=*persistent-id* (正常に更新された後で表示するレコードの ID)
KEEP.attr_name=*value*
KEY.attr_name=*value*
HTMPL=*zdetailxxx_factory.html*

注: UPDATE で HTMPL 指定子を使用するためには、参照されるフォームの名前が命名規則 *zdetailxxx_factory.html* に従っている必要があります。つまり、文字列「*zdetail*」で始まり、その後に任意の英数字 (Null 文字列も含む)、下線、およびファクトリ名を続ける必要があります。

注: web.cfg の詳細については、「管理ガイド」を参照してください。

操作変数

以下の表は、サポートされている各操作に対して設定できる変数の一覧です。

変数	説明	オペレーション
ALG_PRESET	CREATE_ALG 変数を受けて作成されるアクティビティログの 1 つまたは複数の属性の値を指定します。CREATE_ALG が指定されていない場合、ALG_PRESET と ALG_PRESET_REL は無視されます。	CREATE_NEW
ALG_PRESET_REL		SEARCH SHOW_DETAIL

変数	説明	オペレーション
CREATE_ALG	操作の副次的な影響として作成されるアクティビティ ログのアクティビティ ログ タイプを指定します。新しいアクティビティ ログの属性の値を指定するには、ALG_PRESET 変数または ALG_PRESET 変数を使用します。 アクティビティ ログが作成されるタイミングは、以下に示すように操作によって異なります。 CREATE_NEW アクティビティ ログは、新規レコードの保存時に作成されます。新規レコードを保存しなかった場合、アクティビティ ログは作成されません。 SEARCH アクティビティ ログは、リストフォームからレコードが選択されたときに作成されます。レコードを選択せずに表示した場合（リストフォームのマウスオーバーメニューから [表示] コマンドを明示的に選択した場合）、アクティビティ ログは作成されません。 SHOW_DETAIL アクティビティ ログは、レコードを表示する前に作成されます。	CREATE_NEW SEARCH SHOW_DETAIL
FACTORY	検索、作成、または更新するオブジェクトのクラスを指定します。\$NX_ROOT/bopcfg の *.maj ファイルで OBJECT として指定されている任意の名前を使用できます。これらの名前は「CA SDM テクニカル リファレンス ガイド」に列挙されています。	CREATE_NEW GENERIC_LIST SEARCH UPDATE
HTMPL	HTMPL の作成者がテンプレート命名規則のデフォルトをオーバーライドして、デフォルトのテンプレートではなく HTMPL ファイルを明示的に指定して表示できるようにします。 注: CREATE_NEW または UPDATE で HTMPL 指定子を使用するときは、参照されるフォームの名前が命名規則 zdetailxxx_factory.html に従っている必要があります。xxx は任意の文字、factory はファクトリ名を表します。	CREATE_NEW DISPLAY_FORM JUST_GRONK_IT MENU SEARCH SET_MENU SHOW_DETAIL UPDATE

変数	説明	オペレーション
KEEP.name	保存してページ間で渡すことのできる値を指定します。	CREATE_NEW GENERIC_LIST SEARCH UPDATE
KEY.attr_name	SET.attr_name に類似していますが、この指定子は attr_name をロックアップする点が異なります。attr_name は、別のテーブルまたはオブジェクトへの参照である必要があります。	UPDATE
NEXT_PERSID	次に表示されるレコードの固定 ID を指定します。	UPDATE
PERSID	表示されるレコードの固定 ID を指定します。これは、以下のいずれかの方法で指定できます。 直接指定。ファクトリ名、コロン (:)、一意のデータベース ID (整数) からなる固定 ID を指定します。たとえば、PERSID=chg:1234 は、データベース ID が 1234 の変更要求を指定します。 間接指定。ファクトリ名、コロン (:)、属性名、2 つ目のコロン (:)、値からなる固有 ID を指定します。この形式の PERSID は、指定された値の属性を持つ、指定されたファクトリのレコードを指定します。たとえば、PERSID=chg:chg_ref_num:demo:3 は、参照番号が demo:3 の変更要求を指定します。	SHOW_DETAIL UPDATE
PRESET PRESET_REL	CREATE_NEW 変数を受けて作成されるレコードの 1 つまたは複数の属性の値を指定します。CREATE_NEW が指定されていない場合、PRESET は無視されます。	CREATE_NEW

変数	説明	オペレーション
QBE.op.attr_name	検索の実行時に使用する値を指定します。これらの値は QBE キーワードを使用して識別されます。 attr_name は設定可能なチケットの任意の属性名を、 op は検索時に属性に対して使用される以下の演算子を示しています。 EQ： 値と等しい NE： 値と等しくない GT： 値よりも大きい LT： 値よりも小さい GE： 値以上 LE： 値以下 NU： NULL NN： 非 NULL IN： SQL LIKE 式と一致 KY： 入力されたテキストを含む QBE 変数が定義されていない場合は、標準の検索ウィンドウが表示されます。	SEARCH
SET.attr_name	チケットの作成時に使用する属性名を指定します。 attr_name は、設定できるチケット内の属性を示します。属性名は、基礎となるオブジェクトによって異なります。すべてのオブジェクトとその属性は、bopcfg の Majic ディレクトリ内にある *.maj ファイルに記述されています。また、これらは「CA SDM テクニカル リファレンス ガイド」に列挙されています。	CREATE_NEW UPDATE
SET.id	更新する行のデータベース ID を指定します。	UPDATE
SKIPLIST	1 に設定されている場合、結果が 1 つの検索は検索結果リストに表示されません。代わりに、読み取り専用の詳細が直接表示されます。	SEARCH
use_template	1 に設定されている場合、SEARCH 操作はテンプレートのリストを返します。選択された返されたテンプレートは、新規レコードの情報を設定するために CREATE_NEW 操作で使用されます。この変数は、変更要求、案件、およびリクエストで使用できます。	CREATE_NEW SEARCH

関連項目:

[PRESET、PRESET_REL、ALG_PRESET、および ALG_PRESET_REL の構文 \(P. 541\)](#)

PRESET、PRESET_REL、ALG_PRESET、および ALG_PRESET_REL の構文

URL のキーワードである PRESET、PRESET_REL、ALG_PRESET、および ALG_PRESET_REL は、チケットおよびそのアクティビティ ログの属性の初期値をそれぞれ指定します。以下の 2 つの形式を使用できます。

[ALG_]PRESET=attr:value

指定されたチケットまたはアクティビティ ログの属性を、指定の値に設定します。たとえば、以下のように指定すると、新規チケットの説明は「Hello:」に設定されます。

PRESET=description:Hello

[ALG_]PRESET_REL=attr:obj.relattr:testattr:value

指定されたチケットまたはアクティビティ ログの属性を、他のデータベース テーブルからコピーされた値に設定します。値は、指定された *value* を *testattr* に持つ *obj* の *relattr* 属性からコピーされます。たとえば、以下のように指定すると、新規チケットのアナリスト属性は、xyz123 のユーザ ID を持つ連絡先の ID に設定されます。

PRESET_REL=analyst.cnt.id:user.id:xyz123

この形式を使用する場合、暗黙で指定されているクエリが固有のレコードを取得する必要があります。xyz123 というユーザ ID を持つ連絡先が複数ある場合、または 1 つもない場合は、上の例で示した PRESET 指定は無効になります。

PRESET、PRESET_REL、ALG_PRESET、および ALG_PRESET_REL の各キーワードは、必要に応じて URL 内で何回でも使用できるため、複数の属性を設定できます。または、1 つのキーワードオペランドで、複数の値を「@@」で区切って指定することもできます。区切り文字「@@」を使用する場合は、[ALG_]PRESET キーワードと[ALG_]PRESET_REL キーワードの値形式を混在させることはできません。以下に、チケットの説明、概要、およびアナリストの値を指定する方法の例を 2 つ示します。

```
PRESET=description:Hello+PRESET=summary:HelloThere+PRESET_REL=analyst:cnt.id:user  
id:xyz123  
PRESET=description:Hello@@summary:HelloThere+PRESET_REL=analyst:cnt.id:userid:xyz  
123
```

リクエスト、案件、インシデント、問題、および変更要求では、PRESET および PRESET_REL のいずれも、オブジェクトをアセットにリンクするキーワード属性 ASSET をサポートしています。ASSET 属性は、リクエスト/インシデント/問題の affected_resource 属性、または案件/変更要求のアセット LREL を更新します。

リンクの例

以下に示すリンクの例では、CA SDM へのパスは含まれていません。CA SDM のすべての URL は、以下の形式のコーディングで始まります。

`http://hostname[:port]/CAisd/pdmweb.exe`

この例では、*hostname* はサーバ名です。*port* (オプション) は、Tomcat を使用している場合にポート番号を指定します。以下の URL の例では、このコーディングは省略記号 (...) で示されています。

- 影響を受けるエンドユーザ (ユーザ ID は tooda01) を指定してリクエストを作成するには、以下の URL 例を使用します。

```
...?OP=CREATE_NEW+FACTORY=cr+PRESET_REL=customer:cnt.id:userid:toda01
```

- ユーザ ID tooda01 に割り当てられている、すべてのリクエストのリストを表示するには、以下の URL 例を使用します。

```
¥...?OP=SEARCH+FACTORY=cr+QBE.EQ.assignee.userid=toda01
```

- リクエスト 1234 の詳細フォームを表示するには、以下の URL 例を使用します。

…?OP=SHOW_DETAIL+FACTORY=cr+PERSID=cr:ref_num:1234 (読み取り専用ビュー)

…?OP=UPDATE+FACTORY=cr+PERSID=cr:ref_num:1234 (更新ビュー)

注: 認証に Web サービスを使用すると、ログオン要求を無視できます。
getBopsid() メソッドの詳細については、「CA SDM テクニカル リファレンス ガイド」を参照してください。

高度なカスタマイズ

Web Screen Painter 以外のツールを使用して HTML を変更する場合や、非常に複雑なカスタマイズが必要な場合、Web ページのカスタマイズのさまざまな要素を認識する必要があります。ただし、ほかの方法で CA SDM Web ページをカスタマイズする前に、まず WSP でのカスタマイズを試すことを強くお勧めします。WSP は、必要なカスタマイズのほとんどを実行できる機能を備えています。また、更新を site/mods ディレクトリに配置したり、発行済みファイルをすべてのサーバに配布するなどのハウスキーピング処理も自動的に行います。

Web エンジンとキャッシュ

CA SDM Web サーバの構造を理解していると、Web ページをカスタマイズする際に役立ちます。Web インターフェースでは、Tomcat などの J2EE サーブレット コンテナ、または Apache や Microsoft Internet Information Server (IIS) などの標準 HTTP サーバのいずれかを使用します。ユーザが CA SDM Web ページをリクエストすると、HTTP サーバは、提供されたプログラム pdmweb.exe を呼び出します。

pdmweb.exe が起動し、Web エンジンから呼び出される CA SDM デーモン（または Windows サービス）との接続を設定します。Web エンジンがユーザのリクエストを解釈します。ほとんどのリクエストの場合、Web エンジンはテンプレート（HTML）ファイルを参照し、標準 HTML に変換する必要があります。一般的な変換プロセスでは、Web エンジンは CA SDM サーバと通信してデータベースの読み取りや更新を行い、生成される HTML にデータベース情報を挿入する必要があります。完成した HTML は pdmweb.exe に送信され、次に pdmweb.exe がこの HTML をユーザのブラウザに返します。

最大限のパフォーマンスを発揮するために、通常、各 HTML ファイルは一度だけ読み取られます。Web エン진은、ファイルを解析して HTML への変換方法を決定した後で、解析したファイルをキャッシュに保存します。これにより、次に同じファイルがリクエストされたときの処理時間が大幅に短縮されます。キャッシュは実稼動環境では有益ですが、開発環境では不便です。これは、Web エンジンがリサイクルされるか、pdm_webcache ユーティリティが使用されるまで、HTML ファイルへの変更が有効にならないからです。開発環境では、環境設定ファイルのプロパティ SuppressHtmlCache を指定してこの動作を排除できます。ただし、実稼動環境で HTML キャッシュを無効にすると、Web エンジンの全体的なパフォーマンスに多大な影響を及ぼすため、これはお勧めできません。

注: 詳細については、「管理ガイド」を参照してください。

pdmweb.exe から送信される Web ページは、HTML ファイルを読み取り、読み取ったファイルから HTML を生成することにより生成されます。HTML テンプレート ファイルには、サフィックス .html が付いています。これらのテンプレート ファイルに変更を加えることで、CA SDM Web ページをカスタマイズできます。

pdm_webcache ユーティリティ

Web エンジンのキャッシュから HTML フォーム（1 つまたは複数）を削除するには、pdm_webcache ユーティリティを使用します。そうすることで、次回使用されるときにはそのフォームがディスクからフェッチされるため、フォームに加えた変更が有効になります。

```
pdm_webcache [-f form-name] [-g form-group] [-i interface] [-p process] [-v]
```

-f form-name

キャッシュから削除するフォーム名 (detail_cr.html など) を指定します。「%」（または「*」）をワイルドカード文字として使用し、複数のフォームを選択することもできます。以下に指定の例を示します。

-f detail%

すべての詳細フォームを選択します。

この引数はオプションです。この引数を省略すると、キャッシュ内のすべてのフォームが選択されます。

-g form-group

キャッシュから削除するフォーム グループ名 (Analyst など) を指定します。「%」 (または「*」) をワイルドカード文字として使用し、複数のフォーム グループを選択することもできます。以下に指定の例を示します。

-g Anal%

「Anal」で始まるフォーム グループをすべて選択します。

この引数はオプションです。この引数を省略すると、キャッシュ内のすべてのフォーム グループが選択されます。

-i interface

キャッシュから削除する Web インターフェースの名前 (analyst、customer、employee など) を指定します。「%」 (または「*」) をワイルドカード文字として使用できます。以下に指定の例を示します。

-i a%

アナリスト用インターフェース (analyst) が選択されます。

この引数はオプションです。この引数を省略すると、キャッシュ内のすべてのインターフェースが選択されます。

-p process

キャッシュを変更する Web エンジン プロセス名 (web:local など) を指定します。

この引数はオプションです。この引数を省略すると、すべての Web エンジンが選択されます。

-v

詳細出力を指定します。この引数を指定されている場合、pdm_webcache は、キャッシュから削除されたすべてのフォームのフルネームを以下の形式で表示します。

interface:form-group:form-name

この引数はオプションです。この引数を省略すると、pdm_webcache は、各 Web エンジンのキャッシュから削除されたフォームの数のみを報告します。

HTML テンプレートの変更方法

一般的に、HTML テンプレートには以下の 2 つのタイプの変更を加えることができます。

- ユーザに対して表示されるが、表示前に Web インターフェースによって修正されない変更。たとえば、適切なテンプレート ファイルへの参照を追加して、会社のロゴの GIF ファイルを Web インターフェース ページへ追加したり（「パス スルー」）、ページに JavaScript を追加して入力を検証したりできます。ユーザが HTML ファイルに加えた変更のうち PDM タグに含まれないものは、以下に定義されているように、ユーザに返される HTML に未変更のまま渡されます。
- テンプレートの置き換え可能なセクションの変更。たとえば、リクエストの詳細ページに新規のアプリケーション データを追加できます。

テンプレートの各種エントリを使用して、以下の処理を行うことができます。

- CA SDM の情報をユーザに表示する。
- クエリ ページを設定する。
- リンク タグを使用して、別の CA SDM ページへのリンクを作成する。

変更不可能なファイル

特定の HTML テンプレート ファイルと JavaScript ファイルには、CA SDM の多くの Web フォームで必要とされる情報が含まれています。これらのテンプレートに含まれる情報はリリースに依存するものであり、CA SDM Web インターフェースが正常に動作するために必要不可欠です。したがって、これらのファイルは、新しいバージョンの CA SDM がリリースされる際に必ず置換されます。これらのファイルに加えた変更はアップグレードされません。

この制約を受けるテンプレートは以下のとおりです。

ahdtop.html

CA SDM Web インターフェース全体で使われるスタイル、スクリプト、および JavaScript 変数が含まれています。このファイルは Web インターフェースのメインフレームセットに含まれ、セッション中は常に存在します。すべての CA SDM フォームが、ahdtop.html が含まれるウィンドウを参照する JavaScript 変数 ahdtop にアクセスできます。

menu_frames.html

CA SDM メイン フォームで使用する HTML フレームセットを定義します。

msg_cat.js

CA SDM JavaScript ファイル内で使用される、すべてのメッセージのテキストが含まれています。

reports.html

Web レポートに必要なデータが含まれています。

std_body.html

ほとんどの HTML テンプレートの BODY セクションの冒頭で使用される、標準的な情報が含まれています。

std_footer.html

ほとんどの HTML テンプレートの BODY セクションの最後で使用される、標準的な情報が含まれています。

std_head.html

ほとんどの HTML テンプレートの HEAD セクションの冒頭で使用される、標準的な情報が含まれています。

styles.html

CA SDM Web インターフェース全体で使用される CSS スタイルが含まれています。

これらのファイルを直接変更することはできませんが、補足情報を追加することはできます。制約を受ける xxx.html ファイル (menu_frames.html と reports.html を除く) には、それぞれ対応する xxx_site.html ファイルがあり、これらはカスタマイズが可能です。たとえば、ahdtop_site.html をカスタマイズして ahdtop.html に補足情報を追加したり、msg_cat_site.js をカスタマイズして新規メッセージを追加したりできます。

制約を受ける個々のファイルに対応する xxx_site.html ファイルは、メインファイルの後にロードされるため、これらのファイルでメインファイル内の JavaScript を無効化または変更することができます。これらのファイルに不適切な変更を加えると、CA SDM Web インターフェース全体で予期しない問題が発生する原因になるため、情報の追加は細心の注意を払って行ってください。

関連項目:

[HTTP サーバで使用するディレクトリ](#) (P. 552)

新規 HTML ファイルのガイドライン

CA SDM Web インターフェースに、ユーザ独自の HTML ファイルを追加することができます。この場合、独自の HTML ファイルを他の CA SDM インターフェースでも問題なく動作させるために、必ず以下のガイドラインに従ってください。

1. ファイルの<HEAD>セクション内の任意の場所に、以下のステートメントを挿入します。<TITLE>ステートメントがある場合は、その後に置きます。このステートメントは、CA SDM Web インターフェースに必要な JavaScript グローバル変数を定義し、ページを CA SDM ウィンドウ マネージャに登録します。

```
<PDM_INCLUDE FILE=std_head.html>
```

2. ファイルの<BODY>セクションに、以下の属性を挿入します。この属性を指定すると、CA SDM ウィンドウ マネージャがユーザのページをトラッキングできるようになります。

```
onUnload="deregister_window()"
```

3. ファイルの<BODY>セクションの冒頭に、以下のステートメントを記述します。「menubar=no」引数はオプションです。この引数を指定すると、CA SDM のメニュー バーが非表示になります。

```
<PDM_INCLUDE FILE=std_body.html [menubar=no]>
```

4. ファイルの<BODY>セクションの最後に、以下のステートメントを記述します。

```
<PDM_INCLUDE FILE=std_footer.html>
```

ユーザ定義の状態情報を追加する方法

多くの顧客が、CA SDM Web ページに独自の状態情報を埋め込むこと、およびユーザセッションに出力するすべての後続ページにその状態情報が CA SDM によって渡されることを希望しています。この情報は、HTML ファイル内に条件ステートメントを記述して呼び出すことができます。

ユーザセッションの状態情報は、リンクまたはフォーム内に特別な属性 `USER_STATE` を設定することによって取得できます。CA SDM Web エンジンにサブミットされると、ユーザに対して表示されるすべてのページで HTML 変数の `USER_STATE` が使用可能になり、`USER_STATE` に最後にサブミットされた値が設定されます。

以下の例は、販売員向けのページなど、一部のユーザ サイトから CA SDM へのエントリを設定する方法を示します。

- ハイパーリンクを使用します。

```
<a href="/CAisd/pdmweb.exe?USER_STATE=Sales">Service Desk</a>
```

- 非表示フィールドのあるフォームを使用します。

```
<form action="http://yourhost.com/CAisd/pdmweb.exe">  
<input type="hidden" name="USER_STATE" value="Sales">
```

Service Desk 用のボタンをクリックします。

```
<input type="submit">  
</form>
```

次に、状態情報に基づいて HTML フォームをカスタマイズできます。

```
<PDM_IF "$USER_STATE" == "Sales">
```

販売顧客のカスタム情報

```
<PDM_ELIF "$USER_STATE" == "Engineering">
```

技術者のカスタム情報

```
<PDM_ELSE>
```

その他のユーザの情報

```
</PDM_IF>
```

テンプレートからリクエストを直接作成する方法

URL を使用して、テンプレートからリクエストを作成することができます。

例

```
http://machinename/CAisd/pdmweb.exe?FACTORY=cr+OP=CREATE  
NEW+PERSID=cr:3106+use_template=1
```

cr:3106 はテンプレートの固定 ID です。

プリセット情報を使用してクイック クローズ チケットを設定する方法

クイック プロファイル表示で、クイック クローズ インシデントなどのクイック クローズ チケットを作成できます。クイック クローズ チケットを作成して、説明、概要、またはその他のフィールド情報を自動的に追加する場合、URL にプリセット文字列を追加します。

クイック クローズ チケット機能にプリセット文字列を追加するには、以下の手順に従います。

1. NX_ROOT/bopcfg/www/html/default から
NX_ROOT/site/mods/html/www/default に ahdtop_site.html ファイルをコピーします。
2. 適切な変数（クイック クローズ チケットのタイプに応じて）を使用して、[ahdtop_site.html](#) (P. 550) ファイルを編集します。
3. CA SDM にログインします。
4. クイック クローズ チケットを作成します。

プリセット情報がチケットに追加されます。

プリセット オプションを使用したクイック クローズ チケットの作成

クイック プロファイルで、クイック クローズ インシデントなどのクイック クローズ チケットを作成できます。クイック クローズ オプションによって、同一セッション内でインシデントを開いて解決する場合などに、1 回の手順で新規チケット開いて閉じることができます。クイック クローズ チケットを作成して、説明、概要、またはその他のフィールド情報を自動的に追加する場合、URL にプリセット文字列を追加できます。

プリセット オプションを使用してクイック クローズ チケットを作成する方法

1. NX_ROOT/bopcfg/www/html/default から
NX_ROOT/site/mods/html/www/default に ahdtop_site.html ファイル
をコピーします。
2. プリセット文字列を使用して適切な変数（クイック クローズ チケット
のタイプに応じて）を追加するには、ahdtop_site.html ファイルを編
集します。

- クイック クローズのインシデント - var quick_close_preset_in
- クイック クローズの問題 - var quick_close_preset_pr
- クイック クローズのリクエスト - var quick_close_preset_cr
- クイック クローズの案件 - var quick_close_preset_iss

たとえば、以下の文字列では、クイック クローズのインシデントにお
いて、説明に HelloIncident を設定し、概要に HelloIncidentSummary を
設定しています。

```
var quick_close_preset_in =  
"PRESET=description:HelloIncident@summary:HelloIncidentSummary";
```

3. CA SDM にログインします。
4. [Service Desk] タブで [表示] - [クイック プロファイル] を選択し
ます。
[クイック プロファイルの連絡先の検索] ページが表示されます。
5. 1 つ以上の連絡先用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。
[クイック プロファイル連絡先リスト] には、検索条件に一致する連
絡先が入力されます。
6. 連絡先を選択します。
その連絡先の情報が右側のペインに表示されます。
7. [クイック クローズ] をクリックします。
チケットがプリセット情報で作成されます。

HTTP サーバで使用するディレクトリ

CA SDM のインストールの初期設定では、HTTP サーバに対して以下の 2 つの仮想ディレクトリが定義されます。

- CAisd 仮想ディレクトリは、CA SDM インストールディレクトリ内の以下のディレクトリを直接指します。

Windows : *installation-directory¥bopcfg¥www¥wwwroot*

UNIX : *\$NX_ROOT/bopcfg/www/wwwroot*

- CAisd/sitemods 仮想ディレクトリは、CA SDM インストールディレクトリ内の以下のディレクトリを直接指します。

Windows : *installation-directory¥site¥mods¥www¥wwwroot*

UNIX : *\$NX_ROOT/site/mods/www/wwwroot*

これらの仮想ディレクトリには、以下のサブディレクトリがあります。

サブディレクトリ	保存内容
css	スタイルシート
help	Web インターフェースのヘルプ
html	HTML ファイル
img	グラフィック ファイル
scripts	JavaScript
sitemods	サイト定義のカスタマイズ

css、html、img、または scripts のディレクトリ内にあるファイルのカスタマイズバージョンを作成する場合、/CAisd 内のファイルは決して更新しないでください。この場合、/CAisd/sitemods 内の適切なサブディレクトリにファイルを格納してください。たとえば、/CAisd/css 内にあるスタイルシートを変更する場合は、変更したバージョンのファイルを /CAisd/sitemods/css に格納します。ファイルが sitemods のサブディレクトリ内にある場合、Web エン진은 HTML ファイルを解析する際に、\$CAisd で始まるファイル名を自動的に変更して、sitemods をポイントさせます。

/CAisd/sitemods ディレクトリを使用することには、以下のメリットがあります。

- 変更した配布ファイルのレコードを保持できます。
- 疑問や問題がある場合は、元のバージョンに簡単にアクセスできます。
- CA SDM のインストールは/CAisd/sitemods ディレクトリに何も格納しないため、メンテナンスや新規リリースのインストールプロセスが簡略化されます。

注: /CAisd/sitemods/help サブディレクトリはありません。ヘルプデータは HTML プレテンプレートではなく標準の HTML ファイルに保存されるため、Web エンジンではファイル参照を動的に変更することはできません。ヘルプをカスタマイズする必要がある場合は、/CAisd/help に変更を加える必要があります。

HTML サブディレクトリには、Web エンジンでの処理が不要な、頻繁に使用されるファイルがいくつか含まれています。これらをブラウザにキャッシュすると、パフォーマンスを向上させることができます。これらのファイルのカスタムバージョンを作成する場合は、ファイル内に他のカスタマイズ済みファイルへの参照が含まれていないかどうかを充分に確認してください。Web エンジンによる処理は行われないため、必要に応じて、手動で参照を sitemods に挿入する必要があります。

PDF 添付ファイルのダウンロード

Adobe Acrobat リリース 7.0 または 8.0 のアップグレード後、PDF 添付ファイルをダウンロードして CA SDM で表示しようとする、PDF ファイルが正しく表示されないか、空のウィンドウが表示される場合があります。CA SDM で以下の手順を実行することで、PDF ファイルを正しく表示できます。

1. \$NX_ROOT¥bopcfg¥www¥CATALINA_BASE¥webapps¥CAisd¥WEB-INF¥web.xml で、*forceDecompressOnDownload* パラメータを YES に設定します。

注: Linux の場合、\$NX_ROOT は /opt/CAisd です。

2. CA SDM サービスを再起動します。

参照テーブル内の情報の参照

データベース レコードを編集する詳細フォームの入力フィールドには、**SET.attr_name** という名前が設定されます。レコードを保存すると、**SET** フィールドのデータは基礎となるレコードに直接コピーされます。そのため、別のテーブルを参照する属性の入力フィールドには、そのテーブルの **REL_ATTR** (外部キー) を含める必要があります。通常これは、参照レコードの **id**、**persistent_id**、または **code** です。

ユーザが **REL_ATTR** の値を直接指定することはできず、別のテーブルを参照する属性の **SET** フィールドは非表示になります。フォームに表示されるフィールドには **KEY.attr_name** という名前が付き、参照されるレコードの共通名が含まれます。レコードを更新するためには、共通名を **REL_ATTR** に変換する必要があります。この操作は、以下の場合に行われます。

- ドロップダウンリストフィールドでは、**SET** 値はドロップダウンから直接指定されます。
- ルックアップフィールドで、ユーザがルックアップをクリックして項目を選択すると、選択された項目から **SET** 値がコピーされます。
- ルックアップフィールドで、ユーザがレコードを一意に特定するキーの一部を指定してラベルをクリックすると、ブラウザは **SET** 値をサーバにリクエストして、**SET** 値とフルキーをフォームにコピーします
- 環境設定ファイルの自動入力プロパティが指定または初期設定されており、ユーザがレコードを一意に特定するキーの一部を指定し、さらに [ノートブック] をクリックしてフィールドを終了した場合、ブラウザは **SET** 値をサーバにリクエストして、**SET** 値とフルキーをフォームにコピーします。

上記以外の場合は、**KEY** 値を指定し、**SET** 値を指定しないでレコードが保存されると、**Web** エンジンが保存中に値を解決します。一意の **SET** 値に解決できない **KEY** 値がある場合は、保存は行われず、編集フォームが再表示されます。

ルックアップを解決できないため保存が失敗し、フォームが再表示された場合は、ルックアップの実行対象となった各属性フィールドに対し、**HTML** 内で以下の変数を使用できます。

LIST_attr

一致したものをすべて含みます。通常これは、**<PDM_SELECT>**ステートメントの **SOURCE=**フィールドの右側に指定されます。

FLAGS_attr

以下のいずれかの値に設定されます。

0

最初の検索フィールドを表示します。

1

一致するものが、1 つ以上、MaxSelectList 未満見つかりました（この場合は、<PDM_SELECT>リストが表示されるのが一般的です）。

2

一致するものが見つかりませんでした。

3

MaxSelectList を超える数の一致が見つかりました。

SEARCH_STATUS_attr string

web.cfg ファイルから取得した TooManyMatches テキスト文字列が含まれています。

注: web.cfg の詳細については、「管理ガイド」を参照してください。

連絡先のルックアップの指定

編集可能フォームに連絡先（姓、名、Middle Name）を指定するときに、連絡先の名前をカンマ (,) またはスペースで区切ることができます。ただし、この両方を使用することはできません。名前にスペースが含まれている場合もあるため、カンマを使用することをお勧めします。

カンマとスペースを組み合わせることはできないため、カンマがある場合は、名前全体がカンマで区切られていることを意味します。カンマがない場合は、名前はスペースで区切られます。

情報は最終的に SQL クエリに渡されるため、パーセント記号 (%) はワイルドカード文字として処理されます。たとえば、「P%, J%」と指定すると、「Public, John」や「Penxa, Jane」、および姓が P で始まり名前が J で始まるすべての氏名と一致します（大文字小文字を区別するかどうかは、基礎となるデータベースによって異なります）。「P% J%」と指定した場合も、上記と同じ名前が検索されます。

ただし、「P%, Jon D」で指定した場合は、名前が Jon、ミドルネームのイニシャルが D、および姓が P で始まる連絡先がすべて検索されるわけではありません。これは、カンマが 1 つあるため、カンマのみが区切り文字として見なされるからです。つまりこの場合は、姓は「P%」で検索されますが、名前は「Jon D」で検索されます。このようなエラーを避けるには、「P%, Jon, D」と指定します。

Web エンジンの前処理

Web エンジンによる HTMLPL ファイルの処理は 2 つのフェーズに分かれています。

- 前処理フェーズでは、Web エンジンは HTMLPL ファイルと参照されるファイル (PDM_INCLUDE タグおよび PDM_MACRO タグが参照するファイルも含む) を読み取ります。前処理の出力は、Web エンジンの内部キャッシュのエントリになります。
- 生成フェーズでは、Web エンジンはキャッシュからフォームを読み取り、HTML を生成します。生成の出力は、ブラウザに配布される HTML になります。

前処理フェーズは、Web エンジンの使用期間全体を通じ、フォームごとに一度だけ実行されるのが普通です。生成フェーズは、フォームがリクエストされるたびに実行されます。

前処理フェーズで PDM_SET タグと PDM_EVAL タグを使用すると、Web エンジンが生成フェーズで利用できる情報 (HTML テキストなど) を生成して格納できます。

プリプロセッサ変数

プリプロセッサ変数は「\$PRE」の文字列で始まります。プリプロセッサ変数の作成および更新には、PDM_SET タグを使用します。このタグをプリプロセッサ変数で使用する場合の構文を、以下に示します。

```
<PDM_SET PRE.name[+]=value>
```

このタグはプリプロセッサ変数の割り当てまたは更新を行います（必要な場合は作成も行います）。このタグは、フォームの読み取り中に Web エンジンから検出された時点で処理されます。プリプロセッサ変数の PDM_SET に影響を与えるのは、不変 PDM_IF ステートメントだけです。それ以外は無視されます。

不変 PDM_IF の検出

Web エンジンは、フォームの解析時に不変 PDM_IF ステートメントを検出します。不変 PDM_IF とは、リテラル、環境変数、定数プロパティ、およびプロセッサ変数のみで構成される引数を持つステートメントです。Web エンジンは不変 PDM_IF を検出すると、その条件をすぐに評価します。これにより、以下のような影響が生じます。

- 不変 PDM_IF により実行されない PDM_SET タグと PDM_EVAL タグは、無視されます。プリプロセッサ変数を参照するほかのすべての pdm_eval タグと PDM_SET タグは、不変でない PDM_IF ステートメント内にある場合でも、処理時にすべて実行されます。
- 不変 PDM_IF により実行されないフォーム変数の参照は無視され、それらの値はフォームの使用時にフェッチされません。この方法を利用して、フォームのパフォーマンスを向上させることができます。たとえば、フォームに以下が含まれている場合、Web エンジンは、\$args.def の値をフェッチしてからフォームを表示します。

```
<PDM_IF "$env.NX_OTB_MARKET == "itil" && "$args.a" == 1>
<h1>This is form $args.def</h1>
</PDM_IF>
```

ただし、以下のセグメントが書き込まれている場合は、Web エンジンは最初の PDM_IF が不変であると判断し、\$NX_OTB_MARKET が「itil」の場合のみ \$args.def の値を取得します。

```
<PDM_IF "$env.NX_OTB_MARKET == "itil">
<PDM_IF "$args.a" == 1>
<h1>This is form $args.def</h1>
</PDM_IF>
</PDM_IF>
```

PDM_EVAL: プリプロセッサ変数からのテキストの挿入

PDM_EVAL タグは、プリプロセッサ変数の値を Web エンジン パーサの入力に挿入します。このタグをマクロ内で使用した場合、マクロが完了するまでタグは機能しません。

PDM_EVAL タグは、PDM_INCLUDE や PDM_MACRO と同様に機能します。変数の値がタグの位置にコーディングされるのとまったく同じように、パーサ内のこのタグの位置にテキストが挿入されます。

PDM_EVAL の構文を以下に示します。

```
<PDM_EVAL text=PRE.name>
```

PRE.name は、Web エンジンの入力に値が挿入されるプリプロセッサ変数の名前を指定します。

PDM_EVAL タグの実行は、不変 PDM_IF ステートメントで制御できます。

重要: UNIX では、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。このタスクの実行には、pdm_task を使用します。たとえば、ユーティリティを実行する前に、「pdm_task pdm_eval」と入力します。

フリーフォームによる詳細フォームのカスタマイズ

このセクションのトピックでは、フリーフォームによる詳細フォームのカスタマイズを実行する方法について説明します。

詳細フォームでの JavaScript の使用

WSP を使用して、詳細フォームに独自のフィールドを追加したり、デフォルトでフォームに設定されているフィールドを並べ替えたり、フィールドの編集特性を変更したりできます。しかし、新規フィールドをグリッドに追加するだけのカスタマイズでは不十分な場合もあります。そのような場合のために、<USKD>には、独自のカスタマイズを組み合わせることで詳細フォームにマージし、望みどおりの表示形式を簡単に実現できるようにするための JavaScript 関数が数多く用意されています。これらの機能の概要は、以下のとおりです。

- 詳細フォームの操作にまったく影響を与えることなく、あらゆる HTML を、DetailForm() ステートメントの前、または endDetail() ステートメントの後に置くことができます。

- **detailEndTable()** 関数を使用すると、詳細フォームのエレメントをグリッドに配置するテーブルを終了できます。このタスクの後で、独自の HTML を必要な形式で配置できます。この場合、サイトの HTML は詳細フォーム内に置かれるため、フォームのフィールドはユーザが[保存]をクリックすると Web エンジンにサブミットされます。
detailNextID()関数を使用して独自の HTML エレメントの ID フィールドを生成し、詳細フォームのマウスレス操作に関連付けることができます。この方法の例は、**xx_alg_tab.html** などのノートブック タブで確認できます。
- **dtlStartRow** マクロを指定した独自の HTML に従って、詳細フォームの標準フォーマットを再開できます。これにより 2 番目のグリッドが開始されますが、このグリッドのフィールドは、最初のグリッドの位置と同じとは限りません。この方法は、すべてのノートブック タブで使用されます。
- 行の最後にカスタム エレメントを挿入する場合は、**detailWriteRow()** 関数を使用すると、終了せずに行の内容を書き込むことができます。この方法の例は、**detail_cr.html** および **detail_iss.html** の 24 時間ボタンを生成するコードで確認できます。
- グリッドを配置するテーブルを終了せずに、エレメントの内容を行に明示的に指定するには、**detailRowHdr()** 関数を使用してヘッダテキストを指定し、**detailSetRowData()** 関数を使用してデータ テキストを指定します。この方法の例は、**detail_cr.html** および **detail_iss.html** のタイム フィールドを生成するコードで確認できます。
- フィールドの値を検証する関数を指定（通常はイベント ハンドラを使用）しており、ブラウザ側での検証時にその結果を報告（エラーのあるフィールドを太い赤枠で再描画し、フォーム上部の黄色い領域にエラー メッセージを表示）させたい場合は、**detailReportValidation()** 関数を使用します。この例は、**xx_candp_tab.html** の期間フィールドの検証で使用する **validate_duration()** 関数で確認できます。
validate_duration() 関数は、**val_type.js** ファイル内にあります。
- 詳細フォーム用に生成される HTML をレビューするには、標準関数の **document.write()** と **document.writeln()** の代わりに、**docWrite()** 関数と **docWriteIn()** 関数を使用します。その状態で、フォームの <HEAD> セクション内のどこかで **holdHTMLText()** 関数を呼び出すと、デバッグフォームがポップアップ表示されます。ここに、フォーム用に生成されたすべての HTML を示す TEXTAREA が表示されるため、フォームをレビューしたり、コピーして検証ツールに貼り付けたりできます。

変更を加えるときは、組み合わせ詳細フォームは読み取り専用ビューと編集ビューの両方に表示されることを忘れないでください。カスタマイズが明確に 1 つのビューだけに適用される場合は、以下のいずれかの方法で、現在のビューをテストできます。

- JavaScript では、`_dtl.edit` の式は編集ビューで `true` になり、読み取り専用ビューで `false` になります。
- JavaScript またはオープン HTML では、以下のステートメントを使用できます。

```
<PDM_IF "$prop.form_name_3" == "edit">
```

（編集ビューでのみ使用されます）

```
</PDM_IF>
```

または

```
<PDM_IF "$prop.form_name_3" == "ro">
```

（読み取り専用ビューでのみ使用されます）

```
</PDM_IF>
```

編集ビューと読み取り専用ビューのいずれか 1 つだけで使用するコードを、それぞれひとまとめにします。

`detailEndTable()`

この関数は、詳細フォームの要素をグリッドに配置する HTML テーブルを終了します。引数は使用しません。

`dtlStartRow()` マクロを使用して、新しいグリッドを開始できます。ただし、新しいグリッドの要素が前のグリッドの要素と同じ位置に配置されるとは限りません。

`detailNextID( [colspan,][lastelement] )`

この関数は、以下の形式の文字列を返します。

```
「ID=df_nn_nn TABINDEX=n onFocus=func onBlur=func」
```

HTML 要素にこの文字列を挿入すると、その要素は **CA SDM** のマウスレス操作の規則に準拠したものになります。これには、方向キーによるアクセスや、フォーカス位置を薄い黄色で表示することなどが含まれます。返される文字列はスペースで始まり、スペース以外の文字で終わります。

colspan

エレメントが置かれるグリッドの列数を指定します。この引数はオプションで、指定されない場合は初期設定の「1」になります。この引数を省略すると、エレメントはグリッドの 1 列に配置されるものと見なされます。これは方向キーの動作に影響します。 *colspan* 引数は、 *lastelement* 引数が指定されている場合でも省略できます。

lastelement

ID を生成するエレメントが行の最後のエレメントであるかどうかを指定するブール値です。この引数を省略すると、このエレメントの後に別のエレメントが続くと見なされます。これは方向キーの動作に影響します。

detailNextLinkID()

この関数は、以下の形式の文字列を返します。

```
「ID=dflnk_nn_nn TABINDEX=0 onFocus=func onBlur=func」
```

リンク エレメントを定義する HTML エレメントにこの文字列を挿入すると、そのエレメントは CA SDM のマウスレス操作の規則に準拠したものになります。これには、方向キーによるアクセスや、フォーカス位置を薄い黄色で表示することなどが含まれます。返される文字列はスペースで始まり、スペース以外の文字で終わります。

この関数は引数を使用しません。

detailReportValidation(field, has_error, emsg)

この関数は、外部フィールドの検証結果を報告します。検証でエラーがあることが報告されると、エラーのあるフィールドは太い赤枠で再描画され、フォーム上部の黄色い領域にエラー メッセージが表示されます。以降の `detailReportValidation()` のコールでフィールドにエラーがないことが報告されるまで、ユーザはレコードを保存できません。

`detailReportValidation()` 関数は、ブラウザ側で検証を行うように登録されているフィールドに対してのみ機能します。詳細フォーム マクロを使用して作成されたフィールドは、すべて検証を行うように自動的に登録されます。その他のフィールドは、`detailSetValidateFunction()` を使用して登録できます。

field

(必須) フィールドが含まれるフォーム エlement オブジェクトを指定します。これを取得するための最も簡単な方法は、検証を実行するハンドラにこの引数を渡すことです。標準の JavaScript 関数 `document.getElementById()` を使用することもできます。

has_error

(必須) フィールドにエラーがあるかどうかを示すブール値または整数値です。フィールドの設定にエラーがある場合、ユーザはレコードを保存できません。フィールドは太い赤枠で強調表示され、3 番目の引数に指定されているエラー メッセージが、フォーム上部の黄色い領域に表示されます。フィールドの設定のエラーが解除されると、これらの表示は元に戻ります。

emsg

has_error フラグが設定されている場合に、詳細フォーム上部の黄色い領域に表示するメッセージを指定するテキスト文字列です。*has_error* が設定されている場合は、この引数は必須です。

`detailSetValidate( hdrtext, is_required, maxsize )`

この関数は、`detailNextID()` で指定された ID を持つ最新のフィールドをブラウザ側で検証することを示します。必須フィールドと最大サイズのフィールドは、自動的に検証されます。ほかのフォームの検証は、JavaScript 関数、または `detailReportValidation()` をコールするイベントハンドラで行うことができます。

`detailSetValidate()` は、`detailNextID()` で作成された ID を持つ、サイトが独自に定義したフォーム フィールドに対してのみコールしてください。`detailSetValidate()` 関数は、検証するフィールドを作成した直後にコールする必要があります。詳細フォーム マクロで作成されたフィールドに対して `detailSetValidate()` をコールする必要はありません（コールすると予期しない結果が発生することがあります）。

hdrtext

(必須) エラー メッセージ内でフィールドを特定するための文字列を指定します。

is_required

(必須) フィールドが必須かどうかを指定するブール値または整数値です。ユーザがレコードを保存しようとする、すべての必須フィールドが指定されているかどうか自動的に検証されます。

maxsize

フィールドで利用できるデータの最大長を指定する整数です。ユーザがレコードを保存しようとする、*maxsize* 値が指定されたすべてのフィールドについて、データの長さが制限内であるかどうか検証されます。この引数は必須です。*maxsize* の検証を無効にするには、0 の値を指定します。

detailRowHdr(hdrtext, colspan, is_required)

この関数は、グリッド内の項目のヘッダ (TH) エLEMENTのテキストを格納します。テキストは、**detailWriteRow()**関数または **dtlStartRow** マクロが呼び出されない限り、フォームに実際に書き込まれません。

hdrtext

ヘッダ ELEMENTのテキストを指定します。この引数は必須です。

colspan

ELEMENTが置かれるグリッドの列数を指定します。この引数はオプションで、指定されない場合は初期設定の「1」になります。この引数を省略すると、ELEMENTはグリッドの 1 列に配置されるものと見なされます。これは方向キーの動作に影響します。*is_required* 引数が指定されている場合、*colspan* 引数を指定する必要があります。

is_required

hdrtext を、必須フィールドに対応するスタイルで表示するかどうかを指定します。この引数には、ブール値、数値、または文字列を指定できます。数字または文字列は、ゼロの場合は **false**、それ以外の場合は **true** と解釈されます。この引数はオプションです。省略されている場合、*hdrtext* は必須でないフィールドとしてスタイル設定されます。

detailSetRowData(text)

この関数は、グリッド内の項目のデータ (TD) エLEMENTの HTML テキストを格納します。テキストは、**detailWriteRow()**関数または **dtlStartRow** マクロが呼び出されない限り、フォームに実際に書き込まれません。この単一の引数が、格納されるELEMENTの HTML テキストになります。

detailWriteRow()

この関数は、現在の行に関して格納されている HTML を書き込みます。これにより、2つの HTML テーブル行が作成されます。1つはヘッダ (TH) ELEMENTに関する行で、もう1つはデータ (TD) ELEMENTに関する行です。この関数は、新しいデータELEMENTを開始する<td>タグも書き込みます。TD タグは **dtlStartRow** マクロによって自動的に閉じられるため、**detailWriteRow()**の後に続く HTML テキストに<td>タグを指定する必要はありません (指定することは間違いです)。この関数には引数がありません。

リスト フォームについて

このセクションには、**CA SDM** のリスト フォームの内部に関する参考情報を記載します。これらのフォームを変更するときは、**Web Screen Painter** デザイン ビューを使用することをお勧めします。

CA SDM のリスト フォームは、**PDM_MACRO** タグを使用して呼び出される以下のマクロで定義されます。

IsStart

リストを開始します。

IsCol

リスト内の列を定義します。

lsWrite

リストの `pdm_list` 部分にテキストを挿入します。

lsEnd

リストを終了します。

これらのマクロを使用するリストの一般的な形式を以下に示します。

```
<pdm_macro name=lsStart>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsEnd>
```

このリストでは、出力 HTML 内に以下の例のようなテキストが生成されます。

```
var rs = new Resultset();           From lsStart
rs.startList(); From lsStart
rs.header("hdr1"); From lsCol
rs.setData("attr1","options"); From lsCol
rs.header("hdr2"); From lsCol
rs.setData("attr2","options"); From lsCol
<PDM_LIST SOURCE=list> From lsEnd
rs.data(attr1) From lsCol/lsEnd
rs.data(attr2) From lsCol/lsEnd
</PDM_LIST> From lsEnd
```

例：出力リストは 2 つのセクションに分かれています。1 つは `<PDM_LIST>` タグの前にある設定セクション、もう 1 つは `<PDM_LIST>` タグと `</PDM_LIST>` タグの間にある実際のリストです。 `lsCol` マクロはプリプロセッサ変数と `<PDM_SET>` タグを使用して、リストの両セクションにデータを出力します。リストのリストセクション全体は、`lsEnd` マクロによって生成される `<PDM_EVAL>` タグによって作成されます。

独自の JavaScript をリストの設定セクションに含めるには、そのまま目的の場所に挿入します。独自のコードをリストのリストセクションに挿入するには、`lsWrite` マクロを使用します。

lsWrite マクロ

lsWrite マクロは、リストのリストセクション（<pdm_list>タグと </pdm_list>タグの間の部分）のテキストを指定します。このマクロのテキスト引数に指定されたテキストは遅延され、lsEnd マクロが実行されるまで出力 HTML に書き込まれません。

lsWrite [both=no|yes]

text="xxx"

both

テキストオペランドを、すぐに出力 HTML に書き込み、さらに遅延テキストバッファにも書き込むことを指定します。このように指定すると、後続の lsCol マクロによって出力される設定情報とリスト情報の両方の出力を条件によって無視する JavaScript を出力することができます。これはオプションで、初期設定は「no」です。

text

このマクロで生成されるテキストを指定します。指定されたテキストは、lsEnd マクロが実行されるまで遅延されます。

多くの場合、pdm タグおよびフォーム変数への参照を、lsWrite マクロのテキスト出力に挿入する必要があります。lsWrite マクロ自体の解析中に、Web エンジンがこれらのフォームを解釈しないようにするには、以下の構文規則に従います。

- lsWrite マクロで pdm_tag を生成する場合は、タグを囲む区切り文字の「<」と「>」を省略します。たとえば、リストのリストセクションに <pdm_else>ステートメントを挿入するには、以下のようにコーディングします。

```
<PDM_MACRO NAME=lsWrite text="pdm_else">
```

Web エンジンでは、最初の 4 文字が「pdm_」（または「PDM_」）であることを検出すると、「<」と「>」を自動的に挿入してからテキストを生成します。

- **lsWrite** マクロでフォーム変数への参照を生成する場合は、\$文字の代わりに@文字を使用して変数を指定してください。たとえば、リスト変数\$`list.persistent_id` への参照を生成するには、以下のようにコーディングします。

```
<PDM_MACRO NAME=lsWrite text="@list.persistent_id">
```

Web エンジンでは「@」を「\$」に自動的に変換してからテキストを生成します。リテラルの@記号を生成するには、前にバックスラッシュを付けます。

[リスト内で編集]カスタマイズ

一部のリストフォーム（リクエスト リストや案件リストなど）には、[リスト内で編集] ボタンがあります。このボタンが有効で結果セットが表示されている場合、ユーザは[リスト内で編集]をクリックして、検索フィルタの代わりに小型の編集フォームを表示することができます。この編集フォームを使用すると、ユーザはリストフォームからレコードを直接更新できます。さらに、目的の新しいデータを編集フォーム内に置き、[すべて変更]をクリックして、リスト内で選択されているすべてを更新することもできます。

リストデータの編集操作では、[保存] ボタンを押すまでサーバとの通信は行われません。ユーザが[保存]をクリックすると、すべての更新（フォーム上で黄色で強調表示されている部分）がサーバに送信されます。サーバは 1 つの操作ですべての変更を適用し、ステータス メッセージを返してリストを再表示します。

この機能のカスタマイズは、特定のリストフォームで [リスト内で編集] ボタンを有効にするかどうかの制御、またはユーザが [リスト内で編集] をクリックしたときに表示される編集フォームに示すフィールドの制御によって行います。

[リスト内で編集] ボタンをリスト フォームに配置するには、以下のステートメントをフォームの<HEAD>セクションに挿入します。

```
<SCRIPT LANGUAGE="JavaScript" SRC=$CAisd/CAisd/list_edit.js></SCRIPT>
```

このステートメントを追加するだけで、フォームにボタンが配置されます。ただし、ボタンを有効にするには、編集フォームの内容を指定する JavaScript ステートメントも、フォームに含める必要があります。これらのステートメントは、結果セットの指定の直前に、以下の形式で挿入してください。

ステートメント	Comments
<code>startListEdit(_search_filter);</code>	記載のとおり指定する必要があります。
<code>listEditStartRow();</code>	記載のとおり指定する必要があります。
<code>listEditField("attr"[, "hdr"]);</code>	ゼロ以上を指定します。
<code>listEditReadonly("attr", "hdr");</code>	ゼロ以上を指定します。
<code>endListEdit();</code>	記載のとおり指定する必要があります。

`endListEdit()` ステートメントの後には、結果セットを開始する `ResultSet()` ステートメントを指定する必要があります。編集フォーム内のフィールドとフォーム上での表示順序を指定するには、`listEditReadonly()` ステートメントまたは `listEditField()` ステートメントを 1 つ以上コーディングします。

`startListEdit( _search_filter );`

リスト編集フォームを開始します。これは、`startListEdit( _search_filter )` のとおりにコーディングする必要があります。

`listEditStartRow();`

リスト編集フォームのフィールドの新しい行を開始します。これは、`listEditStartRow();` のとおりにコーディングする必要があります。`listEditStartRow()` ステートメントは、`startListEdit()` ステートメントの直後に指定する必要があります。フォーム上のフィールドを指定する `listEditField()` ステートメントと `listEditReadonly()` ステートメントの間に、別の `listEditStartRow()` ステートメントを記述することもできます。


```
listEditField(attr_name[,hdr]);
```

リスト編集フォームに含める属性を指定します。

attr_name

編集フォームに含める属性の名前を指定します（必要な場合はドットを含めます）。リスト編集フォームに指定する属性は、結果セット内にも存在する必要があります。また、指定する **attr_name** は、属性を結果セットに追加する **rs.showData()** または **rs.showDataWithLink()** に指定されているものと同じであることが必要です。

属性は、検索フィルタに表示される場合と同じ形式で編集フォームに表示されます。検索フィルタにない属性は、20 文字のテキストボックスで編集します。

attr_name は必須の引数です。

hdr

編集フォームのフィールドのヘッダテキストを指定します。この引数はオプションです。省略されている場合、ヘッダテキストは検索フィルタから取得されます。**hdr** が省略されていて、属性が **attr_name** の検索フィルタのエントリにない場合、ヘッダテキストはデフォルトで引用符で囲まれた属性名になります。

```
listEditReadOnly(attr_name[,hdr]);
```

リスト編集フォームに含める、編集できない属性を指定します。このステートメントの引数は、**listEditField()** の引数と同じ意味を持ちます。

```
endListEdit();
```

リスト編集フォームを終了します。これは、**endListEdit();** のとおりにコーディングする必要があります。

独自の Web ページとの統合

CA SDM Web インターフェースの機能を独自の Web ページに統合し、ユーザに対してシームレスなインターフェースを表示できます。

注: Web エンジンには Web サーバと CA SDM サーバの間でゲートウェイとして機能する実行可能ファイルであり、1 人のユーザが同時に複数の接続を確立することができます。ただし、同時に複数のフレームで CA SDM Web エンジンプロセスへのオープン接続を確立することはできません。

Web インターフェースは、以下の方法で統合できます。

- いずれかの Web ページから適切な CA SDM Web ページへのリンクを作成し、Web インターフェースのメニュー ページを経由せずにアクセスできるようにします。
- 入力の収集とサポートされる操作の実行を直接行う HTML フォームを Web ページに追加し、CA SDM の Web データ エントリのページが表示されないようにします。
- HTML Web ベースのフォームをアクセス タイプに応じてユーザに関連付ける、Web フォーム グループを作成します。Web フォーム グループでは、管理インターフェースで使用するフォーム グループと同様に、独自の HTML ページをカスタマイズできます。

関連項目：

[サポートされているサーバ操作 \(P. 533\)](#)

CA SDM 関数へのリンク

メイン ページを経由せずに、CA SDM の主要な関数に直接リンクすることができます。これを行うには、CA SDM の情報が含まれる新しいウィンドウのポップアップ ウィンドウにアクセスするのが一般的です。Web ページを CA SDM ページに置き換えることもできます。

どちらの場合も、メイン ページとスコアボードは表示されず、リクエストされたページがユーザに対して標準セッションとして表示されます。アナリストの場合は、[ファイル] - [スコアボードの復旧] を選択すると、メイン ページとスコアボードが表示されます。ただし、このメニューは、メイン ページを省略した場合に表示されるページでのみ使用可能です。

メインページを経由しないリンクを作成するには、以下の形式の URL を指定します。

```
http://hostname[:port]/CAisd/pdmweb.exe?OP=operation+var=value+...
```

この URL 例で、*hostname* は Web サーバのホスト コンピュータです。*port* は、http サーバとして Tomcat を使用している場合にのみ必要なポート番号（通常は 8080）です。*operation* はサポートされる操作の 1 つ、*var=value* はその操作で利用できる 1 つ以上の変数です。

たとえば、リクエストを作成するためのフォームをロードするリンクは、以下のように指定できます。

```
<A HREF=http://hostname/CAisd/pdmweb.exe?OP=CREATE_NEW+FACTORY=cr>Define Request</A>
```

関連項目：

[リンクの例](#) (P. 542)

CA SDM へのフォームのポスト

サポートされる操作を参照する HTML フォームを Web ページに追加して、CA SDM の機能にアクセスすることもできます。操作（リクエストの作成など）を実行するための十分な情報が指定されたフォームがサブミットされると、そのほかの入力を収集するためのフォームを表示せずに操作が実行されます。

HTML フォームを Web ページに追加する場合は、以下の条件を満たす必要があります。

- フォームの ACTION は、pdmweb.exe の URL です。
- METHOD は POST です。
- SUBMIT ボタンの名前に、サポートされる操作のいずれかを指定します。または、サポートされる操作のいずれかを値として持つ、OP という非表示フィールドを作成します。

たとえば、リクエストを作成するページをロードする HTML フォームを作成するには、以下のように指定します。

```
<FORM ACTION=/CAisdCAisd/pdmweb.exe METHOD=POST>
<INPUT type=HIDDEN NAME=FACTORY VALUE=iss>
.
.
.
<INPUT type=SUBMIT NAME=CREATE_NEW VALUE=" OK ">
</FORM>
```

JavaScript のカスタマイズ

CA SDM Web インターフェースでは JavaScript を大量に使用しており、/CAisd/scripts ディレクトリに多数の JavaScript ファイルが含まれています。これらのスクリプト ファイルをカスタマイズする場合は、「[HTTP サーバで使用するディレクトリ \(P. 552\)](#)」で説明したように、変更したバージョンのファイルを /CAisd/sitemods/scripts に格納してください。

パフォーマンス上の理由から、/CAisd/scripts ディレクトリに置かれる JavaScript ファイルは、コメントおよび不要な余白を削除して圧縮されます。この圧縮によって、これらのファイルを読み取ることは困難になります。圧縮されていないバージョンの JavaScript ファイルは、すべて以下のいずれかのディレクトリ内にあります。

- (UNIX) \$NX_ROOT/sdk/scripts
- (Windows) \$NX_ROOT/sdk/scripts

JavaScript ファイル全体のカスタマイズ バージョンを作成することは、できる限り避けてください。各ファイルには多数の関数が含まれていますが、変更が必要なのはその中の 1 つだけという場合があります。ほとんどの場合は、変更した関数を JavaScript ファイルの `sitemods.js` に記述することで、個々の関数を無効化できます。JavaScript を変更する場合は、この方法で行うことを強くお勧めします。

sitemods.js

スケルトン ファイルの `sitemods.js` は、CA SDM と共に配布されます。このファイルは、配布されるすべての HTML ファイルの `<head>` セクションの最後に挿入されるため、ロードされる最後の JavaScript ファイルになります。最後のファイルなので、ここで定義されている関数によって、前に挿入された同じ名前の関数が無効化されます。これにより、配布されたコードを直接変更することなく、独自のバージョンの JavaScript 関数を配布できます。

この方法は、menubar.js や ahdmenus.js など、ロード時に <head> セクションで呼び出される関数に対しては無効です。

ただし、ほとんどの JavaScript 関数は以下の手順でカスタマイズできます。

1. 変更したバージョンの関数を sitemods.js に含めます。
2. 更新された sitemods.js のコピーを
CAisd/site/mods/www/wwwroot/scripts に格納します。

関連項目：

[メニューバーの変更](#) (P. 476)

コンテキストメニューの変更

CA SDM の多くのフォームで、オブジェクトを右クリックしてアクセスできるコンテキストメニューが使用されています。Web Screen Painter を使用して、項目を追加、削除、または変更し、コンテキストメニューを変更することができます。

注：メニュー項目の詳細については、Web Screen Painter ヘルプを参照してください。

従業員ユーザによる変更要求の更新および作成

初期設定では、ユーザは従業員用 Web インターフェースでは変更要求の表示のみが可能です。従業員として変更要求の作成および更新を行うには、以下の手順に従います。

1. Web に管理者としてサインオンして、[管理] タブをクリックします。
2. [セキュリティ] メニューから [アクセス タイプ] を選択します。
[アクセス タイプ リスト] が表示されます。
3. [従業員] リンクを選択して [従業員アクセス タイプの詳細] ウィンドウを表示します。
4. [各機能へのアクセス] タブで、[変更要求] を「変更」に設定して保存します。

5. [戻る] ボタンをクリックして[管理] タブに戻り、[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。
6. [従業員] をクリックして、[データ パーティションの詳細] ウィンドウを表示します。ウィンドウの[制限リスト] 部分で、以下の **Change_Request** テーブルの[タイプ] 列を確認します。
 - Pre-Update
 - Create
7. 編集する各テーブルで[テーブル名] リンクをクリックして、テーブルの[データ パーティションの制約の詳細] ウィンドウを表示します。
8. [編集] ボタンをクリックします。
9. 制約を以下のように編集します。

「id = 1」を「affected_contact = @root.id」に変更します。
10. [保存] をクリックします。

従業員ユーザとして **Web** インターフェースにログインしたときに、[変更要求の作成] リンクが表示されるようになります。

[クローズ済み変更要求]リンクの従業員スコアボードへの追加

本製品を使用して、[クローズ済みの変更] ノード オプションを従業員 **Web** インターフェース スコアボードに追加できます。

クローズ済みの変更ノードを追加する方法

1. 管理者として製品にログインします。
2. [Service Desk] タブをクリックします。
3. [ファイル] - [スコアボードのカスタマイズ] を選択します。

[スコアボードのカスタマイズ] ダイアログ ボックスが表示されます。
4. [役割] オプションをクリックし、ドロップダウン リストで[従業員] を選択します。
5. [ノードの新規追加] で[ノードのストアドクエリ] リンクをクリックします。

[ストアドクエリ リスト] ダイアログ ボックスが表示されます。
6. [ストアドクエリ] リストを検索して[クローズ済みの変更] を選択します。これは通常、コード **CHGUBIN7** として表示されます。

7. 左のスコアボード ツリーから項目を選択して、新しいノードの場所を指定します。
8. [ノードの新規追加] をクリックします。
[クローズ済みの変更] という新規ノードがスコアボード ツリーに追加されます。
9. [終了] をクリックします。

添付ファイルのダウンロード

CA SDM では、添付ファイルをダウンロードするときに、ユーザへの確認メッセージを出さずに、添付ファイルをブラウザのウィンドウに自動的に表示します。この操作は、添付ファイルがウィルスに感染している場合には危険です。

CA SDM には、添付ファイルを保存するか開くかについて確認する [名前を付けて保存] ダイアログ ボックスを表示できます。添付ファイルの保存を実行すると、添付ファイルをディスクに保存し、スキャンしてから開くことができるため、安全性が高くなります。特定タイプの添付ファイルについてのみ [名前を付けて保存] ダイアログ ボックスを表示するオプションもあります。

web.xml サブレットの環境設定ファイルで、[名前を付けて保存] ダイアログ ボックスが表示されるように設定できます。web.xml ファイルは以下のパスにあります。

Windows :

`$NX_ROOT¥bopcfg¥www¥CATALINA_BASE¥webapps¥CAisd¥WEB-INF¥web.xml`

Linux : \$NX_ROOT は「/opt/CAisd」です

第9章: イベントログ データ保存カスタマイズ

システム環境変数 `@NX_EVENT_LOG_EXCLUDE` (`NX.env` ファイル内で設定、CA SDM サービスの再起動が必要) によって、イベントログ (`event_log` テーブル) に保存されるデータの量を制御できます。この変数によって、[クイックプロファイル] ページのボタンとして起動可能な[最近のアクティビティ]の一部として追跡、レポート、および使用するイベントのみ保存できます。

この変数では、カンマによって、リスト項目を区切ります (例: `@NX_EVENT_LOG_EXCLUDE = FAQ,KD_OPEN`)。たとえば、以下の表にある LOGIN、LOGOUT イベントを使用すると (`@NX_EVENT_LOG_EXCLUDE` 値が LOGIN,LOGOUT)、製品ではログインおよびログアウト イベントが記録されません。

この変数を使用してイベントログに保存するデータをカスタマイズする際には、以下の情報を参照してください。

イベント	列挙	作成者	セット	コメント
LOGIN	1	CA SDM		ユーザがシステムにログインすることを指定します。
LOGOUT	2	CA SDM	numdata1	ユーザがログアウトすることを指定します (numdata1=ログアウトの原因: 0 - 正常 1 - タイムアウト 2 - 異常
CR_CREATE	3	CA SDM	sd_obj_type, sd_obj_id, kd, numdata1	ユーザがリクエストを作成することを指定します (numdata1=影響を受けるエンドユーザの ID)。
ISS_CREATE	4	CA SDM	sd_obj_type, sd_obj_id, kd, numdata1	ユーザが変更要求を作成することを指定します (numdata1=影響を受けるエンドユーザの ID)。

イベント	列挙	作成者	セット	コメント
CHG_CREATE	5	CA SDM	sd_obj_type, sd_obj_id, kd, numdata1	ユーザが案件を作成することを指定します (numdata1=影響を受けるエンドユーザの ID)。
EMAIL	6	ナレッジ マネ ジメント	kd	アナリストがドキュメントを電子メールで送信することを指定します。
LINK	7	ナレッジ マネ ジメント	kd, sd_obj_type, sd_obj_id	ユーザが解決策を受け入れ、チケットにリンクすることを指定します。
UNLINK	8	CA SDM	sd_id, sd_obj_type, sd_obj_id	ユーザが解決策をチケットからリンク解除することを指定します。
SEARCH	9	ナレッジ マネ ジメント	numdata1,	ユーザがナレッジを検索することを指定します (numdata1=CI_ASKED_QUES id)。
FAQ	10	ナレッジ マネ ジメント	numdata1	FAQ 検索を指定します (numdata1=O_INDEXES id (category))。
DT_ NAVIGATE	11	ナレッジ マネ ジメント	kd, numdata1, textdata1	ユーザが決定ツリーをナビゲートすることを指定します (numdata1=ES_NODES ID textdata1=パス)。
KD_ BOOKMARK	12	ナレッジ マネ ジメント	kd	ユーザが KD をブックマークに追加することを指定します。
KD_ COMMENT	13	ナレッジ マネ ジメント	kd, numdata1	ユーザが KD にコメントを追加することを指定します (numdata1=O_COMMENTS id)。

イベント	列挙	作成者	セット	コメント
KD_CREATE	14	ナレッジ マネ ジメント	sd_ob_type, sd_obj_id, kd	ユーザがドキュメントを作成することを指定します。CA SDM ID は、ナレッジのサブミットを使用してリクエストまたは案件から KD を作成するときに使用されます。
KD_OPEN	15	ナレッジ マネ ジメント	kd, numdata1	ユーザが KD を開くことを指定します (numdata1=BU_TRANS ID)。
KD_RATE	16	ナレッジ マネ ジメント		ユーザが KD を評価することを指定します (numdata1=BU_TRANS ID)。
KD_NEW	17	ナレッジ マネ ジメント	numdata1	ユーザが [ナレッジ] タブの [新規ドキュメント] フォルダをクリックすることを指定します。
NX_ATTACH_ AUDIT_TO_NEW_TI CKET	18	CA SDM		ユーザが新規チケットを開くと、現在のセッションのすべてのイベントは、デフォルトでチケットの [イベント ログ] タブ上に表示されます。 0 - チケットに関するイベントのみが、[イベント ログ] タブに表示されます。 1 - 現在のセッションのすべてのイベントが、チケットの [イベント ログ] タブに表示されます。
TICK_OPEN	19	CA SDM		チケットが表示されたことを示します。
TICK_SEARCH	20	CA SDM		ユーザがチケットを検索したことを示し、検索数をリンクします。
KD_PRNT	21	ナレッジ マネ ジメント	kd	ナレッジ ドキュメントが印刷されたことを示します。

CA Business Intelligence レポートのカスタマイズ

CA SDM スキーマでフィールドとテーブルが定義された後の時点から、CA Business Intelligence レポートをカスタマイズできます。

注: スキーマ変更の詳細については、「スキーマ デザイナでの変更の概要」を参照してください。

開始する前に、以下が実行されていることを確認してください。

- CA SDM と正常に連携するように CA Business Intelligence がインストールされ、環境設定されていることを確認します。
- レポート環境でユーザの権限、役割、認証オプション、およびデータパーティションセキュリティが確立していることを確認します。

注: CA Business Intelligence のセキュリティ設定の詳細については、「管理ガイド」を参照してください。

CA Business Intelligence インフラストラクチャ

エンタープライズ レポート インフラストラクチャである CA Business Intelligence (CA BI) を使用すると、CA SDM のユーザや役割を対象にレポートを作成、管理、保存、スケジュール、および配布できます。BusinessObjects Enterprise XI、Release 2 およびその関連ツールは、BusinessObjects Crystal Reports XI と共に、アーキテクチャのバックボーンとなります。CA SDM パッケージ版に含まれている BusinessObjects Enterprise ツールによって、CA SDM レポートの主要素を、業界最先端のビジネス インテリジェンス フレームワークに組み込むことができます。

注: Crystal レポートは CA BI の主要コンポーネントとして提供されますが、レポート作成およびメンテナンス用ツールである Crystal Reports XI は提供されません。Crystal Reports XI は別途ライセンスが必要な製品で、BusinessObjects から購入でき、CA BI と組み合わせて使用できます。

レポートコンポーネント

以下は、CA Business Intelligence インフラストラクチャに含まれる主なコンポーネントです。

- **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制限など、CA SDM セキュリティは、すべて自動的にレポートに適用されます。
- **Central Management Server** - Central Management Server (CMS) は、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。
- **セントラル管理コンソール** - セントラル管理コンソール (CMC) は、Business Objects の主要な管理機能です。すべての BusinessObjects 管理機能にアクセスできます。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。
- **BusinessObjects ユニバース** - ユニバースでは、データ ウェアハウスまたはトランザクション データベースのビジネス表現が提供されます。レポートで使用されるクラス (テーブル) およびオブジェクト (列) を表示します。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** - Designer は BusinessObjects Enterprise のツールです。このツールを使用すると、CA SDM スキーマと BusinessObjects 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、BusinessObjects Web Intelligence (WebI) または Crystal Reports を使用して作成されます。このレポートは、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 **WebI** や **Crystal Reports** またはその他のレポート タイプの表示、実行、スケジュールなどを行って、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。
- **アドホック レポート** - アドホック レポートでは、**WebI** 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します。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。

開発環境

CA SDM スキーマ変更を備えた CA BI インフラストラクチャの更新は、管理機能の 1 つです。変更したスキーマをレポートにプロモートする管理者は、実稼働環境とは別に、環境をセットアップする必要があります。

CA BI で使用されるツールには、Windows ベースのアーキテクチャを必要とするものがあります。これは、Linux/UNIX へのインストールでは、Windows コンピュータ上の CA BI が、Linux/UNIX 実稼働環境にインストールされた CA BI とやり取りするように設定する必要があることを意味します。実稼働で Windows サーバを使用している場合は、開発環境用に追加の Windows コンピュータを設定する必要があります。

ツール

CA SDM スキーマ変更を備えた CA BI インフラストラクチャの更新は、管理機能の 1 つです。実施したスキーマ変更をレポートにプロモートするには、開発環境に以下のツールが含まれている必要があります。

Business Objects Designer

このフルクライアントの Windows ツールは、Windows 向けの CA BI 基本インストールの一部として CA BI 実稼働サーバにインストールされます。CA BI サーバが非 Windows アーキテクチャである場合、または実稼働 CA BI アプリケーションサーバへのログイン アクセスが望ましくない場合は、Windows（開発）サーバ上に別途 CA BI インストールを作成する必要があります。開発 CA BI サーバのインストールによって、CA BI 実稼働サーバインストールのアーキテクチャにかかわらず、実稼働 CA BI オブジェクトにリモートでアクセスできます。

BusinessObjects Web Intelligence

この Web ベースのレポート作成ツールは、Web Intelligence (WebI) レポートを変更および作成するために使用します。BusinessObjects InfoView インターフェースから、WebI ツールにアクセスできます。WebI および InfoView ツールの管理権限は、CA BI 内部でのみ、具体的には BusinessObjects セントラル管理コンソール (CMC) ツールを使用することで得られます。

CA SDM ODBC ドライバ

CA SDM ODBC ドライバは、CA BI のインストールで提供されます。このコンポーネントによって、データ パーティションセキュリティが実施され、その間の WebI および Crystal Reports から CA SDM データへのアクセスが可能になります。ODBC ドライバは、CA BI アプリケーション サーバへの CA BI 基本インストールの一部としてインストールされます。また、CA BI が実行されていないコンピュータ上で、Crystal Reports XI クライアントと共に使用できるように、クライアントインストールとして使用することも可能です。

注: レポート環境のデータ パーティションセキュリティの定義については、「管理ガイド」を参照してください。

開発環境を作成する方法

開発環境を作成するには、以下の手順に従います。

1. サポートされている Windows オペレーティング システムがインストールされたサーバを確保します。
2. CA SDM をインストールして、環境設定します。
3. CA Business Intelligence をインストールして、環境設定します。
4. デフォルトの ODBC DSN 名を、casd_xxxxx から casd_yyyyyy に変更します。yyyyyy は、実稼働実装の DSN とまったく同じにします。

重要: 実際の接続プロパティにかかわらず、DSN 名は、開発と実稼働実装とで同一である必要があります。

5. (オプション) Crystal Reports XI をインストールして、環境設定します。

注: CA BI と同じコンピュータ上に Crystal Reports をインストールする必要はありません。CA SDM ODBC Driver が Crystal Reports コンピュータにもインストールされていて、DSN 名が、実際の接続プロパティにかかわらず、実稼働実装と同一の名前に変更されていれば、Crystal Reports を別のコンピュータにインストールできます。CA SDM ODBC ドライバを CA BI インストールとは別に個々にインストールする際の詳細については、ODBC ドライバのドキュメントを参照してください。

6. [フレームワークを作成します。](#) (P. 585)

フレームワーク

ツールが開発環境で使えるようになったら、次の手順は、スキーマ変更を製品のアップグレードでも保持するためのフレームワークの作成です。

重要 CA BI と共にインストールしたデフォルトの開発 CA SDM ユニバースは変更しないでください。そうでないと、スキーマ変更がパッチおよびアップグレードの処理中に上書きされるおそれがあります。CA SDM ユニバースを変更すると、CA BI インフラストラクチャ内のスキーマ変更が失われることになります。

BusinessObjects ユニバースは、CA BI インフラストラクチャ内のスキーマを説明するメタレイヤです。CA から供給されたユニバースを変更する代わりに、CA SDM ユニバースにリンクされた顧客固有のユニバースを作成できます。この方法を使用すると、アップグレード処理中に最小限の作業でローカルスキーマ変更を管理でき、CA SDM によるベースユニバースのアップグレードが可能になります。

BusinessObjects ユニバースのドキュメントに精通している CA SDM 顧客の場合は、ユニバースを結び付けるための文書化されたほかの手順を、BusinessObjects から入手可能であることに気付きます。ただし、ここでは、顧客による変更を保守するために CA がサポートしている手順のみを取り上げます。

デフォルトのユニバースには「CA SDM」という名前が付けられ、セントラル管理コンソール (CMC) 内の「CA Universes」フォルダに保存されます。このデフォルトユニバースは、ユニバースがリンクされている構造における「カーネル」ユニバースです。

CA SDM ユニバースは、名前を選択して付けることができます。名前は、レポートライターがレポートを作成する際に表示され、わかりやすい名前かどうかを確認できます。顧客ユニバースは、さまざまなユニバースがリンクされている構造における「派生」ユニバースです。

このフレームワーク内では、必要な数だけ派生ユニバースを管理できますが、スキーマ変更の管理に必要となるのは1つのみです。複数の派生ユニバースを使用して管理やセキュリティ要件を簡略化できる場合もありますが、実際には実稼働サポートのニーズに基づいて判断する必要があります。

派生ユニバースが複数ある環境では、必ず以下を実行してください。

- すべてのユニバースで、ユニバース ファイル名用の **z_** 命名規則を維持する。
- CA SDM 接続を使用して、[CA Customer Universe] フォルダにユニバースを保存する。
- カーネルユニバースへのリンクは削除しない。

スキーマ変更を CABI に昇格するフレームワークの作成

スキーマ変更を CA Business Intelligence に昇格させるためのフレームワークを作成するには、BusinessObjects Designer を使用します。

スキーマ変更を昇格させるフレームワークの作成

1. BusinessObjects Designer を開きます。
Designer のメニューから [File] - [New] を選択します。
[Universe Parameters] ウィンドウが表示されます。
2. [Definition] タブをクリックし、ユニバースのわかりやすい名前を [Name] フィールドに入力します。
3. (オプション) 説明を [Description] フィールドに入力します。
4. [Connection] ドロップダウンリストから [CA SDM] を選択します。
5. [Links] タブの [Add Link] ボタンをクリックします。
[Universe to Link] ダイアログ ボックスが表示されます。

6. [CA Universes] フォルダを展開して、以下のタスクを実行します。
 - a. CA Service Desk.unv ファイルを開きます。[Universe to Link] ダイアログ ボックスが閉じ、CA SDM ユニバースが[リンク] タブに表示されます。
 - b. [OK] をクリックして、[Universe Parameters] ダイアログ ボックスを閉じます。

Designer による派生ユニバースのリンクと作成の処理には数分かかることがあります。

7. 派生ユニバースが作成された後、以下のタスクを行います。
 - a. 必要に応じて以下のパラメータを変更します。
 - [File] メニューから [Parameters] を選択します。
 - [Parameter] タブをクリックします。
 - 「ANSI92 = YES」と指定します。
 - b. [Controls] タブをクリックし、以下のフィールドを実装に適した値に設定し、[OK] をクリックして値を保存し、パラメータのダイアログ ボックスを閉じます。
 - Limit size of result set
 - Limit execution time
 - Limit size of long text objects (最低 4000)
 - c. 階層を定義します。顧客階層はインポートされないため注意してください。
 - [Tools] - [Hierarchies] を選択します。
 - すべてのカスタム階層を選択して、[Add] 矢印ボタンをクリックします。すべての階層が右側へ移動します。

8. Designer のメニューで [File] - [Save] をクリックします。

[Save As] ダイアログ ボックスが表示されます。
9. わかりやすいファイル名を選択し、先頭に「z_」を付けて、[File Name] フィールドに指定します。たとえば、ユニバース名「ACME Anvil Co」はデフォルトで「ACME_Anvil_Co.unv」となっています。このファイル名を「z_ACME_Anvil_Co.unv」に変更してから保存します。

10. 派生したユニバースを以下のように CMS にエクスポートします。

- a. Designer のメニューから [File] - [Export] を選択します。
- b. [Domain] フィールドのドロップダウンリストから [<Browse>] を選択し、[CA Customer Universes] を見つけて選択します。
- c. [OK] をクリックして、ユニバースをローカル CMS にエクスポートします。

[Universe Successfully Exported] ダイアログ ボックスが表示されます。

これで、CA BI 全体におけるカスタム スキーマ変更を昇格されるフレームワークができました。

11. BusinessObjects InfoView に管理ユーザとしてログインし、以下を行います。

- a. [Public Folders] を選択します。
- b. InfoView のツールバーで [New] - [Folder] を選択します。
- c. [Folder Name] フィールドに、「Organization Name Reports」など、レポート ユーザにわかりやすい説明を入力します。
- d. [OK] をクリックして、[Public Folders] の下に作成されたフォルダを確認します。

これにより、組織により作成されるレポートを使用および保存するための最小限のフレームワークが作成されます。このフォルダ構造に追加できるサブフォルダやファイルの数に制限はありません。

インフラストラクチャへのスキーマ変更

CA BI 開発環境が確立され、記載されているスキーマ データのカスタマイズ用プロセスを使用して CA SDM にスキーマ変更を発行したら、スキーマ変更を CA BI インフラストラクチャにプロモートする準備が整います。新規スキーマをレポートの作成と変更で利用可能にすることができます。

派生ユニバースへのスキーマ変更の追加

CA BI インフラストラクチャへのスキーマ変更のプロモートは、派生ユニバースに新規スキーマ オブジェクトを追加するのと同じくらい簡単です。

注: 開始する前に、適切な手順が完了されていて、新規スキーマ オブジェクトが CA SDM のフレキシブルなスキーマに追加されていることを確認してください。

派生ユニバースにスキーマ変更を追加する方法

1. BusinessObjects Designer を開き、以下を実行して、ローカル ファイル システムに派生ユニバースをインポートします。

- a. Designer のメニューから [ファイル] - [インポート] を選択します。

[Universe Successfully Imported] ダイアログ ボックスが表示されます。

- b. [OK] をクリックします。

2. 以下のようにして、派生ユニバースの構造を更新します。

- Designer のメニューから [表示] - [構造の更新] を選択します。

以下の質問が表示されます。

- 「選択したテーブル内の古い列を更新しますか。」 [OK] をクリックします。

注: 「更新の必要はありません。」というメッセージが表示される場合は、CA SDM オブジェクト レイヤが新規スキーマで適切に更新されていないことを表しています。スキーマ変更を CA SDM に発行する手順を確認します。

- 「構造の更新：構造は正常に変更されました。」 [OK] をクリックします。

新しい列が、ウィンドウの右側のユニバース構造に表示され、新規オブジェクトが派生ユニバース内で使用できるようになります。

オブジェクトは、右ペインから左ペインに移動された後、CA BI ツールで使用できます。左ペインにオブジェクトを追加する際、[共通スキーマ変更](#) (P. 590) 標準に準拠していることを確認してください。

3. 新規オブジェクトを左ペインの目的の場所にドラッグ アンド ドロップします。
4. [保存] をクリックします。
5. **Designer** のメニューから [ファイル] - [エクスポート] を選択します。
[Universe Successfully Exported] ダイアログ ボックスが表示されます。
6. [OK] をクリックします。
派生ユニバース スキーマに追加された変更が、ローカル **CMS** にエクスポートされます。
7. **Designer** のメニューから [ツール] - [完全性のチェック] をクリックします。
 - a. 表示されるダイアログ ボックスで、[オブジェクトの解析] チェック ボックスをオンにします（ほかの設定は変更しないでください）。
 - b. [OK] をクリックします。完全性のチェックが開始されます。
注: 解析エラーはレポートされません。エラーが検出された場合、左ペインでオブジェクトを変更し、解析エラーが発生しないようにします。
8. ダイアログ ボックスを閉じるには、[OK] をクリックします。
9. 以下を実行して、派生ユニバースを **CMS** にエクスポートします。
 - a. **Designer** のメニューから [ファイル] - [エクスポート] を選択します。
 - b. [ドメイン] フィールドのドロップダウン リストから、[<Browse>] を選択し、[CA Customer Universes] を見つけて選択します。
 - c. [OK] をクリックし、ローカル **CMS** にユニバースをエクスポートします。
[Universe Successfully Exported] ダイアログ ボックスが表示されます。
10. 変更を保存し、**CA SDM** ユニバースをエクスポートします。
Web Intelligence や **Crystal Reports** などの **CA BI** レポート環境で変更を使用できるようになります。

共通スキーマ変更

ユニバースにスキーマ変更を実装できます。プロセスを理解しやすいように、以下の表に、対処する可能性のある共通スキーマ変更をリスト表示します。

Web スクリーン ペインタ内で定義されている フィールド タイプ	ユニバースでフィールドを使用するときは、以下の ルールに従ってください。 属性を右クリックし、以下を選択します。
INTEGER	[オブジェクト プロパティ] - [定義] タブで、「数 値」と入力します。
STRING	[オブジェクト プロパティ] - [定義] タブで、「文 字」と入力します。
DATE	[オブジェクト プロパティ] - [定義] タブで、「日 付」と入力します。 [オブジェクトの形式] - [数値] タブで、カテゴ リ「日付/時間」を選択し、形式「yyyy/MM/dd hh:mm:ss AM/PM」を選択します。
DURATION	[オブジェクト プロパティ] - [定義] タブで「数 値」と入力し、[オブジェクト プロパティ] - [定 義] タブで、「PdmSeconds (object.attr)」を選択 します。
SREL	CA SDM 属性の別名を作成します。
BREL	適用不可
QREL	適用不可
DERIVED	必要に応じて、派生したフィールドに格納された 値に適したデータ型およびオブジェクト形式を使 用します。[DERIVED] フィールドではどのような 結果も生成される可能性があるため、準拠すべき 特定の標準はありません。

Web スクリーン ペインタ内で定義されている フィールド タイプ	ユニバースでフィールドを使用するときは、以下の ルールに従ってください。 属性を右クリックし、以下を選択します。
特殊なケース：Local これは Web スクリーン ペインタ内で定義 されたデータ型ではありませんが、サポ ートされていないデータ型を示す際にユニ バースによって使用されることがあるデー タ型です。	[Local] フィールドは、タイプ「L」と共に、ユニ バースの右ペインに表示されます。これらの フィールドはドラッグできますが、ユニバースの 右ペインのクラスにはドロップできません。通常、 バイナリなどのフィールド データ タイプはユニ バースではサポートされません。ただし、オブジェ クトを作成し、[プロパティの編集] ダイアログ ボックスの「選択」ウィンドウに PdmString (object.attribute) を配置することで、ユニバース の左ペインに追加できます。

レポートおよびフォルダ構造

CA BI のインストールには、複数の Crystal Report XI および WebI レポート
オブジェクトが含まれています。レポートは、CA SDM フォルダ CA
Reports¥CA SDM に格納されます。

重要: CA SDM フォルダ構造に格納されている CA SDM ユニバースおよび
レポート オブジェクトは変更しないでください。

レポートおよびフォルダ構造について、以下の情報を考慮してください。

- フレームワークを作成するための手順では、InfoView のパブリック セ
クションにフォルダを追加する方法について説明しています。これは、
エンドユーザ専用のフォルダです。ユーザは、このフォルダ内に追加
のサブフォルダおよびレポート オブジェクトを作成できます。
- 各ユーザが一意の CA SDM ログイン ID によって CA BI へのアクセスを
許可される実装では、ユーザは [マイ フォルダ] セクション内に個人
用のレポートを保存できます。BusinessObjects では、ログインしたユー
ザに対してのみこれらのオブジェクトを表示することによって、この
フォルダへのセキュリティを実施しています。
- CA BI にアクセスするためのユーザ ID として、すべてのユーザに単一
のレポート ユーザ ID が与えられている実装では、すべてのユーザに対
して [マイ フォルダ] セクションが利用可能です。

Web Intelligence レポートの作成

Web Intelligence レポートを作成するには、CA Business Intelligence を使用します。

Web Intelligence レポートの作成

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. メニュー バーで [新規] - [Web Intelligence Document] をクリックします。
3. 開発フレームワークを定義する際に作成した派生ユニバースを選択します。

Web Intelligence レポート作成ツールが表示されます。

注: ドキュメントは定期的に保存してください。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。Web Intelligence 接続セッションのタイムアウト値を大きくする方法については、「管理ガイド」を参照してください。

4. Web Intelligence ツールバーから、[保存] - [名前を付けて保存] を選択します。
[ドキュメントを保存] ダイアログ ボックスが表示されます。
5. [一般] セクションの [タイトル] フィールドに、このレポートのわかりやすい名前を指定します。
6. [ロケーション] セクションで、適切なフォルダを選択します。
7. (オプション) 必要に応じて、プロパティを変更します。
8. [OK] をクリックして、レポートを保存します。

レポートが指定したフォルダに表示され、すべてのレポート ユーザから使用できます。

Web Intelligence レポートの変更

CA Reports¥CA Service Desk フォルダ構造に配信されたレポートを変更するには、CA Business Intelligence を使用します。

CA Business Intelligence レポートを変更する方法

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. 左ペインで、[CA Reports] フォルダ構造に移動し、必要な Web Intelligence レポートを開きます。
3. レポート名をクリックして、レポートを実行し、結果を表示します。
4. Web Intelligence ツールバーから、[ドキュメント] - [名前を付けて保存] を選択します。
[ドキュメントを保存] ウィンドウが表示されます。
5. [ロケーション] セクションで、適切なフォルダを選択します。
6. [OK] をクリックして、新規ロケーションにレポートを保存します。
7. [ドキュメントを保存] - [編集] を選択します。
8. [クエリの編集] をクリックします（ユニバース CA SDM の名前が [データ] タブに表示されます）。
9. [プロパティ] タブをクリックします。必要に応じて、ユニバースの横の下向き矢印をクリックします。CA SDM テキストが省略記号 (...) と共に表示されます。
10. 省略記号 (...) ボタンをクリックして、[ユニバース] ダイアログ ボックスを表示します。
[その他の使用可能なユニバース] ウィンドウが表示されます。

11. ユニバースの名前を選択し、[OK] をクリックします。

Web Intelligence によって、すべての既知のフィールドが CA SDM ユニバースからカスタムユニバースに自動的にマップされ、[Change Source] ダイアログボックスが表示されます。マップされた各フィールドの横に、緑色のチェックボックスが表示されます。すべてのフィールドが正しくマップされたら、[OK] をクリックして、変更を確認します。いずれかのフィールドに赤い「X」が表示された場合は、フィールド名の横の省略記号 (...) ボタンをクリックし、適切なフィールドを選択します。

12. Web Intelligence ツールバーから、[Edit Report] をクリックし、[プロパティ] タブを選択します。

13. [一般] ノードを展開します。

14. ドキュメントプロパティの値の横にある省略記号 (...) ボタンをクリックします。

[ドキュメントプロパティ] ダイアログボックスが表示されます。

15. [ドキュメントオプション] セクションで、[オープン時にリフレッシュ] チェックボックスをオンにします。

16. [保存] をクリックし、Web Intelligence を閉じます。

レポートが、適切なユニバースに関連付けられ、必要に応じて変更できます。

Crystal レポートの作成

Crystal Reports を使用して、レポートを CA Business Intelligence ユニバースに保存します。

Crystal レポートを作成する方法

1. Crystal Reports XI を起動します。

2. [File] - [New] - [Blank Report] を選択します。

[Database Expert] ダイアログボックスが表示されます。

3. [Create new Connection] ノードを展開し、[Universes] をクリックします。

[Business Objects Enterprise] ダイアログボックスが表示されます。

4. 管理者認証情報を使用して、BusinessObjects Enterprise にログオンします。

5. 派生ユニバースが含まれているフォルダに移動します。
6. 派生ユニバースを選択し、[開く] をクリックします。
[Business Objects Query Panel] ダイアログ ボックスが表示されます。
7. ユニバース ツリー構造から、適切な属性をクエリ パネルの選択セクションおよびフィルタ セクションにドラッグ アンド ドロップします。
8. クエリ作成プロセスが完了すると、標準の Crystal Reports デザイナー ツールが表示されます。
9. レポートを作成して、実行します。
注: レポートの作成と実行の詳細については、Crystal Reports のドキュメントを参照してください。
10. 以下を実行して、Business Objects Enterprise リポジトリにレポートを保存します。
 - a. [File] - [Save as] を選択します。
 - b. [Save as] ダイアログ ボックスで [Enterprise] を選択します。
 - c. 開発フレームワークを定義する際に作成したフォルダに移動し、BusinessObjects Enterprise に新規レポートを保存します。

新規レポートが Enterprise で使用可能になり、必要に応じて変更できます。

Crystal レポートの変更

Crystal Reports を使用して、CA Business Intelligence ユニバース内のレポートを変更します。

Crystal Reports XI レポートを変更する方法

1. Crystal Reports XI を開きます。
2. [File] - [New] - [Blank Report] を選択します。
データベース エキスパート ダイアログ ボックスが表示されます。
3. [Create new Connection] をクリックして展開します。
[Universes] をクリックします。
[Business Objects Enterprise] ダイアログ ボックスが表示されます。
4. 管理者として Business Objects Enterprise にログオンします。

5. クリックして、派生ユニバースが格納されているフォルダに移動し、派生ユニバースをクリックします。
[Open] をクリックします。
[Business Objects Query Panel] ダイアログ ボックスが表示されます。
6. ユニバース ツリー構造で属性を見つけ、クエリ パネルの選択およびフィルタ部分にドラッグアンドドロップします。
クエリ作成プロセスが完了すると、レポート ライタが標準の **Crystal Reports** デザイナ ツールと共に表示されます。
7. **Crystal Reports** の手順に従ってレポートを作成して、実行します。
8. 準備が完了したら、**Business Objects Enterprise** リポジトリにレポートを保存します。
 - a. [File] - [Save as] を選択します。
[Save as] ダイアログ ボックスが表示されます。
 - b. [Save as] ダイアログ ボックスの左側で、[Enterprise] アイコンをクリックします。
 - c. このドキュメントで前に作成した顧客固有のフォルダから始まるフォルダ構造へナビゲートし、[Save] をクリックしてこのレポートを **Business Objects Enterprise** に保存します。
9. 新規レポートが **Enterprise** で使用可能になり、必要に応じて変更できます。

新規 Crystal レポートの CA Business Intelligence への移動

CA Business Intelligence に Crystal レポートを移動することができます。

CA Business Intelligence に新しい Crystal レポートを移動させる方法

1. **Crystal Reports XI** を開きます。
2. [File] - [Open] を選択します。
[Open] ダイアログ ボックスが表示されます。
3. 左側で、[Enterprise] をクリックします。
[Log on to BusinessObjects Enterprise] ダイアログ ボックスが表示されます。

4. 管理者認証情報を使用して、BusinessObjects Enterprise にログオンします。
「CA Reports¥CA Service Desk」で始まるフォルダ構造に移動し、ターゲット レポート表示します。
5. ターゲット レポートを選択し、[Open] をクリックします。
レポートが Crystal Reports に表示されます。
6. [File] - [Save as] をクリックします。
[Save As] ダイアログ ボックスが表示されます。
7. 開発フレームワークを定義する際に作成したフォルダを指定します。
8. [Save] をクリックします。
9. Crystal Reports のメニューから、[Database] - [Database Expert] を選択します。
[Database Expert] ダイアログ ボックスが表示されます。
10. 左側のペインで [Create New Connection] - [Universe] を選択します。
11. 派生ユニバースを選択します。
12. このレポートで使用する属性をすべて、新規クエリにドラッグアンドドロップし、[OK] をクリックします。
13. すべての数式とセルで、元の属性を新規クエリからの属性に置換します。
14. 属性がすべて置換されたら、以下を実行します。
 - a. Crystal Reports のメニューから、[Database] - [Database Expert] を選択します。
 - b. [データベース エキスパート] ダイアログ ボックスで、元のクエリを選択し、2つのペインの中央で左向き矢印をクリックし、古いクエリを削除します。
 - すべての属性が正常に置換されていれば、元のクエリは問題なく削除され、引き続きレポートを変更できます。
 - 元の属性のいずれかがレポート内に残っている場合は、次のようなメッセージが表示されます。「レポートでは、1つ以上のテーブルから取得したフィールドを使用しています。続行しますか」
 - [キャンセル] をクリックし、レポートに戻ります。

- 削除の際に警告メッセージが表示されなくなるまで、元の属性をすべて新しいクエリからの属性に置換します。

レポートがカスタマイズできるようになります。

既存の Access レポートを CA Business Intelligence に移動させる方法

Microsoft Access の事前定義済みレポートは、CA SDM では開発および提供されなくなりました。ただし、以下の手順に従って、既存の Access レポートを CA Business Intelligence レポート環境に移動させることができます。

1. 適切な CA SDM スキーマ変更を CA Business Intelligence に追加します。
2. Web Intelligence または Crystal Reports を使用して、レポートを再書き込みします。

開発から実稼働への移動

この時点では、派生ユニバースは追加され、フォルダ構造は作成され、レポートは作成および変更されています。そのため、開発構造を実稼働に移動させることができます。この手順では、BusinessObjects インポートウィザードを使用します。

開発から実稼働に移動する方法

1. [スタート] メニューから [すべてのプログラム] - [BusinessObjects XI Release 2] - [BusinessObjects Enterprise] - [インポート ウィザード] の順に選択します。

インポート ウィザードインターフェースが表示されます。

2. [ソース環境] 画面で、Business Objects XI R2 を選択し、開発システムに必要な認証情報を入力します。
3. [宛先環境] 画面で、以下のオプションのいずれかを選択します。
 - **実稼働システム。** このオプションを選択すると、選択したすべてのオブジェクトが実稼働システムにすぐに移動されます。
 - **後で実稼働システムにインポートできる外部ファイル。** このオプションを選択すると、すべてのオブジェクトが Business Intelligence Archive Resource (BIAR) ファイルに格納されます。

4. [インポートするオブジェクトの選択] 画面で、すべてのオブジェクトをクリアし、「フォルダとオブジェクトのインポート」および「ユニバースのインポート」チェック ボックスをオンにします。

注: 警告が表示された場合は無視してください。

5. 目的のフォルダが含まれているフォルダ構造を選択し、移動させないオブジェクトのチェック ボックスをオフにします。
6. [ユニバースと接続のインポート オプション] 画面で、「選択した Web Intelligence および Desktop Intelligence ドキュメントによって直接使用されるユニバースと接続をインポートする」オプションをクリックします。
7. [ユニバース フォルダとユニバース] 画面で、ユニバースが格納される適切なフォルダを展開します。

注: 警告が表示された場合は無視してください。

8. [完了] をクリックします。

フォルダとレポートが実稼働コンピュータに直接移動された場合は、InfoView に変更が表示されます。オブジェクトを .bjar ファイルに配置された場合は、後でインポート ウィザードを使用し、ソース環境として .bjar ファイルを、宛先環境として実稼働サーバを選択します。

レガシー レポートのカスタマイズ

CA SDM では、レガシー レポートをカスタマイズすることや、独自のレポートをデザインすることができます。以下の操作を行うことができます。

- 必要な情報が含まれるように、レガシーの概要レポート、詳細レポート、および分析レポートをカスタマイズする（たとえばフィールドを追加する）。
- データベースから取得した情報を使いやすい形式で表示するレポートを新規に作成する。
- コマンドライン引数を組み込むことにより、変数情報の引数をレポートに渡す。たとえばフィールドの現在値や SQL の WHERE 節の式など、値や式を引数として使用できます。
- コマンドライン、スクリプト ファイル、またはメニュー オプションからレポートを生成する。

カスタム レポートを作成する方法

1. レポートをデザインします。
 - レポートに含めるデータを決定します。
 - データを処理するための SQL 風のクエリ、式、関数、およびデータを印刷ページ用にフォーマットするためのステートメントを含む、レポートテンプレートを作成します。 -
2. レポートは、以下のいずれかを使用して生成します。
 - コマンドライン
 - CA SDM のメニュー オプション
 - スクリプト ファイル

注: サードパーティ製のデータベース システムをお持ちの場合は、そのレポート生成ツールを使用して、CA SDM データベースのデータからレポートを作成できます。 - CA SDM に備わっているさまざまなデータベースビューにより、サードパーティ製のデータベース システムを使用して、カスタマイズしたレポートを簡単に作成できます。 - データベースのレポート作成の詳細については、ご使用のデータベース システムのマニュアルを参照してください。 データベース ビューの詳細については、「管理ガイド」を参照してください。

関連項目:

[Crystal レポートのカスタマイズ](#) (P. 628)

カスタム レポートのデザイン

カスタム レポートをデザインするには、以下についての基本的知識が必要です。

- SQL クエリの作成。
- プログラミング（特に C 言語）。

- レポート テンプレート プログラムの実行前に実行する必要のある、特別なプログラムまたはスクリプト ファイルの作成。たとえば、WHERE 節の条件などの引数を入力するように、ユーザに要求するプログラムを作成する必要があります。

注: カスタム レポートを作成する前に、必要なレポートがすでに提供されていないかどうかを確認してください。CA SDM は、Crystal や Microsoft Access の豊富なレポートに加え、ユーザによるレポートの実行を可能にするこれらの製品のランタイム バージョンも備えています。レポートの詳細については、「管理ガイド」を参照してください。

レポートに含める情報の選択

カスタマイズ レポートで使用する CA SDM データベース データの選択については、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。データベース テーブル、フィールド、説明、その他のデータベース情報が記載されています。

レポート テンプレートの作成方法

レポート テンプレートとは特定のデザインのレポートを生成するファイルで、CA SDM レポート プログラムで実行します。レポート テンプレートには、データのフェッチ方法、計算方法、および印刷方法を定義する変数式、関数、およびステートメントが含まれています。

レポート テンプレートを作成するには、以下のタイプのレポート ステートメントを記述したファイルを作成します。

ブロック ステートメント

データがフェッチされる CA SDM データベース テーブル、およびフェッチされたデータに対して実行するアクションを定義します。

レイアウト ステートメント

データ変数およびリテラル テキストの、レポート出力への表示方法を定義します。

注: .rpt ファイルは、すべて新しいディレクトリ (UNIX の場合は \$NX_ROOT/site/mods/rpt、Windows の場合は *installation-directory¥site¥mods¥rpt*) に保存してください。このディレクトリにより、CA SDM の最新リリースへのアップグレード時にファイルが保持されます。

関連項目:

[レポート テンプレートの参照](#) (P. 612)

[例: レポート テンプレート](#) (P. 607)

ブロック ステートメント

ブロック ステートメントは、レポート テンプレートにフレームワークを提供します。操作対象のデータを定義し、レポートの実行を制御するステートメントです。ブロック ステートメントの先頭に付ける名前は、レポート テンプレート内で固有である必要があります。このステートメントには、以下の 2 つのセクションがあります。

データ クエリ セクション

データベースからフェッチされるデータを定義する、SQL の **SELECT** 節、**WHERE** 節、および **SORT** 節が含まれます。

出力プログラム セクション

フェッチされたデータに対して実行するアクションを定義します。ここには、変数宣言、関数、および条件付きレポートの作成に使用できるその他のブロック ステートメント（ネストされたステートメントなど）が含まれます。データを **ASCII** テキストとしてフォーマットして印刷するレイアウト ステートメントを含めることもできます。

ブロック ステートメントの簡単な構文例を以下に示します。これは、この 2 つのセクション間の関係を表しています。

```
BLOCK blockname ("SELECT clause", "WHERE clause")
```

```
    SORT clause {output program statements}
```

参照セクションの **BLOCK** に関する説明には、詳細な構文例と各節およびパラメータの説明が記載されています。

レポート テンプレートのレイアウト ステートメント

レイアウト ステートメントは、変数およびリテラル テキストのレポート出力での形式を定義します。

- **PAGE HEADER** ステートメントと **PAGE FOOTER** ステートメントを使用すると、各レポート ページの上端と下端に情報を表示できます。

- **HEADER、HEADER2、FOOTER、および PRINT** の各ステートメントを、親 **BLOCK** ステートメントのかっこで囲んだセクションにネストすると、レポート出力に含まれるさまざまな **レポート セクション** のタイトルおよび集計を作成できます。

注: ネストするときは、レイアウト ステートメントで使用するかっこと、親 **BLOCK** ステートメント内にネストするステートメントを囲むかっこを混同しないように注意してください。

- リテラルテキストを組み込んでラベルや罫線文字を作成し、レポートのデザイン効果を高めることができます。

レイアウト ステートメントは以下のとおりです。

PAGE HEADER

各レポート ページの上端に情報を表示します。これは **BLOCK** ステートメントの外側に置かれます。

PAGE FOOTER

各レポート ページの下端に情報を表示します。これは **BLOCK** ステートメントの外側に置かれます。

HEADER

各レポート セクションの上端に情報を表示します。これは **BLOCK** ステートメントの内側に置かれます。

HEADER2

レポート セクションが複数ページにまたがる場合は、そのレポート セクションの後続の各ページの上端にもヘッダ情報を表示します。これは **BLOCK** ステートメントの内側に置かれます。

FOOTER

各レポート セクションの下端に情報を表示します。これは **BLOCK** ステートメントの内側に置かれます。

PRINT

レポート セクションにデータを表示します。これは **BLOCK** ステートメントの内側に置かれます。

以下の事前定義済み変数をレイアウト ステートメントで使用することもできます。

- CT は現在の時刻を印刷します。
- CD は現在の日付を印刷します。
- PG はページ番号を印刷します。

データ フィールド

レポートを生成したときにデータで置き換えられるような、レイアウト ステートメント内の変数です。 レポート テンプレートにフィールドを含める場合は、以下のガイドラインに従ってください。

- データ フィールドは角かっこ ([]) で囲みます。
- フィールドの角かっこは、各出力行でのフィールドの印刷スペースを定義します。 このスペースは、角かっこで区切られた文字数（角かっこ自体も含む）です。 変数の出力が印刷スペースよりも長い場合、その出力は切り捨てられます。 フィールドに十分な印刷スペースを確保するために、変数名と終了角かっこの間にスペースを追加できます。 たとえば、以下のように変数名の後にスペースを入れると、長い名前の連絡先を確実に表示できます。

```
[contact      ]
```

- 出力が 1 行の場合は、終了山カッコ (>) を使用してフィールドを閉じることができます。こうすると、印刷スペースが右余白まで拡大されます。たとえば、終了山カッコ (>) を **HEADER** ステートメントで使用すると、現在の日付が切り捨てられずに印刷できます。

```
[CD                >
```

注: フィールドが 2 行以上で変数が **MULTILINE** として設定されている場合、終了山カッコ (>) は終了角カッコ (I) とまったく同じ働きをします。**MULTILINE** 変数の印刷ステートメントが終了山カッコ (>) で閉じられている場合、開始角括弧 (I) と終了山カッコ (>) で定義されているフィールド内に収まるように、空白で文字が折り返されます。また、変数が **MULTILINE** でない場合は、終了山カッコ (>) を指定すると、すべてのデータが長さとは無関係に現在の行に表示されます。

- レイアウト ステートメント内のフィールドは、以前に定義された変数や列名を参照できます。
- 別のブロック ステートメント内の変数や列名を参照するには、以下の構文を使用します。

```
blockname::column | variable-name
```

リテラル テキスト

リテラル テキストを使用すると、レポートに補足情報を表示できます。リテラル テキストは、テンプレートで指定したとおりにレポート出力に表示されます。リテラル テキストをレイアウト ステートメントに含めるには、開始大カッコ (I) と終了大カッコ (I) の間の任意の行にリテラル テキストを置きます。引用符や角カッコの中に置かないでください。

この例では、**CA SDM** レポート プログラムで、「**ACME Company**」と「**Page:**」がリテラル テキストと解釈されます。

```
PAGE HEADER {
                ACME Company           Page: [PG]
}
```

関連項目:

[レポートテンプレートの FOOTER ステートメント \(P. 622\)](#)
[レポートテンプレートの PAGE FOOTER ステートメント \(P. 625\)](#)
[レポートテンプレートの HEADER ステートメント \(P. 623\)](#)
[レポートテンプレートの HEADER2 ステートメント \(P. 624\)](#)
[レポートテンプレートの PAGE HEADER ステートメント \(P. 626\)](#)
[レポートテンプレートの PRINT ステートメント \(P. 627\)](#)

レポートテンプレートの変数式

レポート出力に表示する値を、各変数に割り当てることができます。変数式を使用すると、以下のことが可能です。

- CA SDM データを操作する。
- 関数を使用して、フェッチした値を計算する。

以下の例では、[変更要求] ウィンドウの [chg_desc] フィールドの内容を参照する *desc* という変数を作成します。MULTILINE フラグを設定することで、この変数全体を複数行にわたって印刷できます。

```
desc = description MULTILINE;
```

以下の例では、説明を印刷します。出力は、角かっこで定義された長さになります。長い説明を表示するには、角かっこ内のスペースの数を増やしてください。

```
PRINT { [desc ] }
```

例: レポート テンプレート

以下の **Affected Contact Report** テンプレートは、レポートテンプレートの作成方法を示します。このテンプレートは、同一の影響を受ける連絡先を持つ、オープンな変更要求を列挙したレポートを生成します。

```

PAGE HEADER {
                                                    As Of: [CD>
                                                    [CT>
}
PAGE FOOTER {
                                                    Page: [PG>
}
BLOCK chg ("SELECT ¥
            chg_ref_num, description, priority, ¥
            status, category, assignee ¥
            FROM Change_Request",
            "WHERE #Change_Request.status = 'OP' ¥
            AND #Change_Request.requestor = #ca_contact.id ¥
            AND #ca_contact.last_name = ? ¥
            AND #ca_contact.first_name = ? ¥
            AND #ca_contact.middle_name = ? “ , $1, $2, $3)
{
            BLOCK st ("SELECT sym FROM Change_Status",
                        “WHERE code = ? “, chg::status) {}
            BLOCK (strlen(category)) cat ("SELECT sym FROM Change_Category",
                                            “WHERE code = ? “, chg::category) {}

HEADER {
            OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT
CHANGE ORDER Summary          Pri   Status   Category          Assignee
}
HEADER2 {
CHANGE ORDER Summary          Pri   Status   Category          Assignee
-----
}

            num = chg_ref_num;
            desc = description MULTILINE;
            pr = deref (priority);
            stat = st::sym;
            catgry = cat::sym;
            asgn = deref (assignee);

PRINT {
[num          ] [desc          ] [pr ] [stat  ] [catgry          ] [asgn ]
}
}

```

ページ ヘッダ

レポートの各ページ上端に印刷する内容を示します。**CD** および **CT** は、現在の日付と時刻を示す事前定義済みの変数で、各ページ上端のヘッダに表示されます。これらの各フィールドは、フィールドを右余白まで拡張できる山かっこで終わります。「作成日:」はフィールドの外側にあり、開始大かっこの後の同じ行内にあるため、レポート出力にはリテラルテキストとして表示されます。

```
PAGE HEADER {                               As Of:  [CD>
                                           [CT>
}
```

ページ フッタ

ページ番号がリテラルテキスト「Page:」と共に表示されます。

```
PAGE FOOTER {
                                           Page: [PG>
}
```

注: **PAGE HEADER** ステートメントと **PAGE FOOTER** ステートメントはグローバルなヘッダおよびフッタを生成するため、**BLOCK** ステートメントには含まれません。

レポート セクション

メインの **BLOCK** ステートメントと、そこにネストされたステートメントのレポートセクションが作成されます。通常は、レポートセクションはレポート内の唯一のデータ部分ですが、このレポートにはレポートセクションが1つしかありません。このブロックの一意の名前は **chg** です。

SELECT 節は、**WHERE** 節で指定した条件が満たされる場合に限り、レポートの3つの **FROM** テーブルについて、データに含める列を選択します。

WHERE 節の最後の 3 つの AND 式には疑問符が含まれています。これらの疑問符は、それぞれ\$1、\$2、および\$3 の各引数の値を取る引数ブレースホルダとしての役割を果たします。つまり、\$1 は ca_contact.last_name、\$2 は ca_contact.first_name、および \$3 は ca_contact.middle_name の値になります。\$1、\$2、および \$3 の各引数は、コマンドライン引数から値を取得します。

```
BLOCK chg ("SELECT ¥
...",
"WHERE ¥
...¥
AND #ca_contact.last_name = ? ¥
AND #ca_contact.first_name = ? ¥
AND #ca_contact.middle_name = ? “, $1, $2, $3)
```

レポート セクションのヘッダ

BLOCK ステートメントの出力プログラム セクションが開始大かっこから始まるように指定します。このステートメントは、SELECT 節および WHERE 節でフェッチされたデータに対して行う処理を指示しています。この例では、このレポート セクションにのみ適用される HEADER ステートメントと HEADER2 ステートメントがネストされています。HEADER2 は、レポート出力が複数のページになる場合にのみ印刷されます。

```
{
...
  HEADER {
      OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT
CHANGE ORDER Summary          Pri    Status  Category  Assignee
  }
  HEADER2 {
CHANGE ORDER Summary          Pri    Status  Category  Assignee
-----
  }
```

変数の割り当て

SELECT 節で指定されたデータに影響する変数式であることを示します。これらの変数式から、列の値や式の結果に変数が割り当てられます。これらの変数は、後続の PRINT ステートメント内のフィールドと一致します。

desc 変数に **MULTILINE** フラグが指定されているため、フィールドが切り捨てられることなく、複数の行に印刷または表示されます。 **deref** 関数は、参照される列に含まれる文字列式を返すために使用します。

```
num = chg_ref_num;  
desc = description MULTILINE;  
pr = deref (priority);  
stat = st::sym;  
catgry = cat::sym;  
asgn = deref (assignee);
```

印刷

印刷されるフィールドが含まれます。このステートメントに行のリテラルテキストを含め、レポートを見やすくすることもできます。最後の終了大かっこは、**BLOCK** ステートメントの出力プログラム セクションの開始大かっこに対応します。

```
PRINT {  
[num ] [desc          ] [pr] [stat] [catgry] [asgn          ]  
  
}  
}
```

関連項目:

[レポート コマンド](#) (P. 611)

レポートの生成方法

レポートテンプレートを作成したら、**CA SDM** レポートプログラムを実行してレポートを生成できます。このプログラムは、以下の方法で実行できます。

- コマンドライン
- **CA SDM** のメニュー オプション
- スクリプト ファイル

注: **UNIX** サーバを使用している場合は、レポート コマンドと併せてレポート出力リダイレクタ (**rpuiDsp**) パラメータを含めると、レポートの送信先（画面、ファイル、またはプリンタ）を選択するダイアログを表示できます。

関連項目:

[ダイアログの表示方法 \(UNIX のみ\)](#) (P. 612)

レポートコマンド

UNIX でレポートをコマンドラインから生成するには、以下の CA SDM レポート コマンドを使用する必要があります。

```
pdm_task report [-h][-e][-f][-F ffstring][-p pagelength] filename [command-line arguments]
```

注: レポート コマンドは、必要な環境変数を設定する `pdm_task` コマンドの直後に指定します。 コマンドライン引数を受け入れるようにデザインされたレポートの場合は、レポート テンプレート内の各引数に対して入力する必要があります。

Windows の場合は、以下の `rpt_srv` コマンドを使用します。

```
rpt_srv report-title
```

以下の例には、このセクションでレポート テンプレートの例として前述した「影響を受ける連絡先レポート (Affected Contact Report)」に必要な 3 つのコマンドライン引数 (Smith、Jane、および L) が含まれています。

```
pdm_task report /reports/myrpt.rpt Smith Jane L
```

引数が空の場合は、Null 文字列を使用する必要があります。たとえば、Jane Smith にミドルネームのイニシャルがない場合の構文は、以下のようになります。

```
pdm_task report /reports/myrpt.rpt Smith Jane ""  
rpt_srv %reports%\myrpt.rpt Smith Jane L
```

ダイアログの表示方法 (UNIX のみ)

レポート コマンドにレポート出力リダイレクタ (`rptuiDsp`) パラメータを指定して、ダイアログを表示することができます。このダイアログには、レポートの出力方法（ファイルに出力、`Xterm` ウィンドウに表示、プリンタに送信）を選択できるオプションが表示されます。

例：

```
pdm_task rptuiDsp report /reports/myrpt.rpt Smith Jane L
```

以下の例では、「Inventory Report」というタイトルがダイアログに追加されます。

```
pdm_task rptuiDsp report /reports/myrpt.rpt Smith Jane L "title:Inventory Report"
```

レポート テンプレートの参照

レポート テンプレートで、変数式、関数、およびステートメントを使用できます。

レポート テンプレートの変数式

変数式は、レポート テンプレートで印刷または表示されるデータを定義します。変数式は、レイアウト ステートメントまたはブロック ステートメントのどちらに置くこともできます。

変数式の構文

構文は、プログラム言語で使用するステートメントの構成を定めたルールです。この文字列は、以下のような構造を持っています。

```
variable-name = expression [flags]
```

変数式のフラグ

フラグは、変数式の結果をフォーマットします。テキスト フィールドをフォーマットするには、以下のフラグを使用します。

MULTILINE

データを切り捨てず、複数の行に表示します。

RIGHT

右端に揃えます。

以下のフラグは、数値フィールドをフォーマットするために使用します。

BLANKZERO

Null 値のフィールドとして機能し、ゼロは印刷されません。 -

BOOL

ゼロは **no**、ゼロ以外の値は **yes** に変換します。 -

REAL

浮動小数点で表示します（初期設定は整数）。

ZEROFILL

右側または左側にゼロを表示します。

以下のフラグは、日付および時間のフィールドをフォーマットするために使用します。

DATE

日付/時刻の日付部分のみを表示します。

DAYS

期間を日数で表示します。

HOURS

期間を時間で表示します。

MINUTES

期間を分で表示します。

SECONDS

期間を秒で表示します。

TIME

日付/時刻の時刻のみを表示します。

変数式の例

以下に、変数式の例を示します。

desc = description MULTILINE

変数式の特記事項

変数式は **BLOCK** ステートメント内で一意である必要があります。そのブロックに対する **SELECT** 節内の列と重複することはできません。異なる **BLOCK** ステートメント内であれば、同じ変数名を使用できますが、**1** つの **BLOCK** ステートメント内で繰り返し使用することはできません。

レポートテンプレートに式を含めるときは、以下の構文ルールに従ってください。

- 有効な **C** 式を使用します。
- 変数や列名は引用符で囲みません。
- 文字列定数は、一重引用符または二重引用符で囲みます。
- ネストされたブロックは、含まれる行が **1** 行だけの場合に限り参照できます。
- キーワードと同じ列名を含める場合は、列名の前にバックスラッシュ (¥) を付けてください。たとえば、**ALIAS** はキーワードで、¥**alias** は列名です。
- 環境変数 (**\$name** など) およびコマンドライン引数 (**\$n** など) を参照する場合は、ドル記号 (**\$**) を使用します。**n** は、コマンドラインでの引数の位置を表します。

- コマンドライン引数の数を指定する場合は、**\$#**を使用します。たとえば以下の式では、コマンドライン引数の数が **2** 以上の場合は追加の引数を引数として使用し、そうでない場合は引数の値を空の文字列に設定します。レポートテンプレート自体もコマンドライン引数と見なされます。つまり、引数の数は少なくとも **1** になります。

```
$# > 1 ? $1 : "
```

- **2** つの文字列を連結する場合は、以下のように**##**を使用します。

```
title = "This is the " ## "first line. "
```

```
long_name = fn
```

```
  first_name ## last_name
```

- 以下のキャストがサポートされています。

- (number)

- (string)

- (date_time)

- (duration)

- 別のブロック内の変数または列名を参照するには、その名前の前にブロック名と **2** つのコロンを付けます。以下に例を示します。

```
blockname::column | variable-name
```

レポート テンプレート関数

レポート テンプレートでは以下の関数を使用できます。

`is_null (expr)`

式が Null になる場合に `true` を返します。

```
false = 0
true = is_null (false)
```

`sqrt (expr)`

式の平方根を計算します。

```
nine = 9
three = sqrt (nine)
```

`pow (expr1, expr2)`

`expr1` を `expr2` 乗します。

```
two = 2
three = 3
eight = pow (two,three)
```

`log (expr, expr)`

式の自然対数を計算します。

```
ten = 10
result = log (ten)
```

`catname (expr, expr, expr)`

連絡先の名前を表す 3 つの文字列を、フィールドフォーマットファイルのルールに従って、カンマで区切られた 1 つの文字列にします。

```
last = "Murphy"
first = "Fred"
middle = "P"
contact_name=catname (last, first, middle)
```

`strlen (string)`

文字列の長さを返します。

```
buffer = "A thirty character long string"
thirty = strlen(buffer)
```


strindex (string, pattern [, start_index])

文字列内の最初のパターン マッチ、または **start_index** の後にある、次のパターン マッチのインデックスを返します。パターン マッチがない場合は -1 を返します。 -

```
buffer = "A thirty character long string"
zero = strindex(buffer, " [A-Z] ")
two = strindex(buffer, " [a-z] ")
```

substr (string, pattern [, length])

最初のパターン マッチの後の文字列部分を返します。長さが定義されているため、出力文字列の長さが制限されます。パターン マッチがない場合は、長さゼロの文字列を返します。

```
buffer = "A thirty character long string"
last_word = substr(buffer, " [a-z]*$ ")
first_capital_letter = substr(buffer, " [A-Z] ",
1)
```

substr (string, index [, length])

インデックスの後の文字列部分を返します。長さが定義されているため、出力文字列の長さが制限されます。パターン マッチがない場合は、長さゼロの文字列を返します。

```
buffer = "Summary: The network card displays a
code of ... "
summary = substr(buffer, 9)
30_char_summary = strindex(buffer, 9, 30)
```

以下の関数（擬似関数）は、変数式ではなくデータのブロックで実行します。一般にこれらの関数は、ネストされた **BLOCK** ステートメントのデータを取得するために、**BLOCK** ステートメント内に置かれます。

count (*block-name*)

BLOCK ステートメントで指定されたブロック内の行数を返します。
block-name は単純文字列にする必要があります。

```
BLOCK sample ("SELECT id FROM Contact") {  
  entries = count (sample)  
}
```

sum (*block-name*, *expr*)

指定されたブロックの各行の式を実行し、結果を合計します。

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request") {  
  difference = sum (sample, est_cost-actual_cost)  
}
```

average (*block-name*, *expr*)

ブロックの各行の式を実行し、結果の平均を返します。

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request"){  
  avg_difference = average (sample, est_cost-actual_cost)  
}
```

prev (*expr*)

式の、前の値を返します。最新の値が誤って上書きされることのないように、この関数は十分に注意して使用する必要があります。

downtime (*sla_schedule*, *expr1*, *expr2* [, *delay-block*, *expr*, *expr*])

SLA のダウンタイム計算を呼び出します。最初の引数は、ワークシフトを識別する文字列にする必要があります。残りの引数は開始時間と終了時間を表します。

expr1 はイベントの開始日/時刻です。

expr2 はイベントの終了日/時刻です。

この例では、**wrkshft** **BLOCK** でワークシフトのスケジュールをフェッチし、**evt_dly** **BLOCK** ステートメントで延期をフェッチします。次に **downtime** 関数がこれらのレコードを使用して、ダウンタイムを計算します。

```
BLOCK attev ("SELECT start_time, fire_time, event_tmpl, obj_id FROM
Attached_Events")
```

```
{
BLOCK evt ("SELECT persid, sym, work_shift FROM Events ", "WHERE persid = ?",
attev::event_tmpl) {}
BLOCK wrkshft ("SELECT sched FROM Bop_Workshift", "WHERE persid = ?",
evt::work_shift) {}

BLOCK evt_dly ("SELECT start_time, stop_time FROM Event_Delay", "WHERE obj_id = ?",
attev::obj_id) {}
total_downtime = downtime(wrkshft::sched,
attev::start_time, attev::fire_time,
evt_dly,
evt_dly::start_time, evt_dly::stop_time);
}
```

deref (column-name)

適切なテーブルを自動ルックアップして、ポインタの文字列表現を返します。

```
BLOCK chg ("SELECT organization FROM Change_Request") {
org = deref (organization)
}
```

この擬似関数はルックアップを呼び出すので、式でこの関数だけが指定されている場合のみ有効です。たとえば、以下の式は有効です。

```
model = deref (nr_model)
```

以下の式は無効です。

```
model = "model" ## deref (nr_model)
```

注: 変数やブロックへの前方参照はできません。

レポートテンプレートの BLOCK ステートメント

ブロック ステートメントはフェッチするデータが入っているデータベース テーブルを定義するもので、フェッチしたデータに対して実行するアクションを含むことができます。

BLOCK ステートメントの構文

構文は、プログラム言語で使用するステートメントの構成を定めたルールです。BLOCK の場合、この文字列の構造は以下のとおりです。

```
BLOCK blockname (  
    "SELECT [ALIAS,] field_name[, field_name ...]  
    FROM table_name[, table_name ...] "  
    [,"WHERE where_clause"][, arguments,] )  
    [SORT "sort clause"]  
{  
    output program statements  
}
```

BLOCK ステートメントのパラメータ

blockname

ブロックを識別します。各 *blockname* は一意である必要があります。

SELECT 節

二重引用符で区切って、*blockname* の後に置きます。フェッチされる列名を指定し、その後にキーワード **FROM**、列がフェッチされるテーブルが続きます。これは必須です。以下の例では 3 つのテーブルが指定されています。

```
"SELECT open_date, chg_ref_num ¥  
last_name, first_name ¥  
FROM Change_Request, ¥  
ca_contact"
```

以下のような SQL 別名を含めることはできません。

```
"SELECT open_date As OpenDate"
```

WHERE 節

(オプション) **SELECT** 節の後に続けて、選択する情報をさらに絞り込みます。文字列定数、または文字列を評価する式を使用できます。

WHERE 節が空の文字列の場合、すべてのレコードが返されます。

WHERE 節には、疑問符 (?) の構文を使用して、置換引数 (変数またはコマンドライン引数を参照する) を含めることができます。以下の **WHERE** 節は、上記の **SELECT** 節の後に続けることができます。

```
""WHERE #Change_Request.open_date >= ?" ¥  
AND #Change_Request.active_flag = 1 ¥  
AND #ca_contact.last_name = ? " , $1
```

注: WHERE 節は文字列を評価する式にできますが、SELECT 節は単独の文字列定数なので、WHERE 節と SELECT 節は区別する必要があります。そうすることで、より自由にデータを操作してレポートを生成できます。

SORT 節

(オプション) SELECT 節と WHERE 節の後に指定して、フェッチされたデータの行を並べ替えます。SORT 節の形式は SQL ORDER BY 節に似ています。以下に例を示します。

```
SORT "open_date"
```

Output program statements

レポートの実行を制御します。HEADER ステートメントが含まれている場合は、データ クエリの前に、ブロックのヘッダ テストが印刷されます。次にデータをクエリします。データが返されると、各ステートメントは記述順に実行されます。ただし、例外が 1 つあります。sum や average などのブロック関数は、出力プログラムの最後にあるものとして動作します。実際にこれらの関数では、次のデータ レコードが実行されなければ確実な値を計算ません。

重要: 出力プログラムはデータ クエリの結果に依存します。クエリからデータが返されない場合は、HEADER ステートメントを除き、出力プログラムは実行されません。

BLOCK ステートメントの例

以下の BLOCK ステートメントでは、変更要求の優先度と同じ整数値を持つ引数が渡されるものと仮定しています。WHERE 節では、最初に、渡される引数の数値 (\$#) を確認します。引数がある場合は、それを使用して式が評価され、WHERE 節が生成されます。ない場合は、Null の WHERE 節 (" ") に置き換えられます。

```
BLOCK chg ("SELECT priority FROM Change_Request",
$# > 1 ? "WHERE priority = " ## $1 : " ") {}
```

FOOTER ステートメントの例

以下に、FOOTER ステートメントの例を示します。

```
FOOTER {
    Summary Information:
        Total Failures: [Fail_count >
        Total Downtime: [Downtime >
}
```

BLOCK ステートメントの特記事項

HEADER、HEADER2、FOOTER、PRINT、および変数式は、かっこ内に置くことができます。ステートメントは、選択された各行に対して実行されます。

注: PAGE HEADER ステートメントと PAGE FOOTER ステートメントを、BLOCK ステートメントに含めることはできません。

レポートテンプレートの FOOTER ステートメント

このレイアウト ステートメントは、レポート セクションの下端に情報を表示します。

FOOTER ステートメントの構文

構文は、プログラム言語で使用するステートメントの構成を定めたルールです。FOOTER の場合、この文字列の構造は以下のとおりです。

```
FOOTER {parameters}
```

FOOTER ステートメントのパラメータ

パラメータは以下のとおりです。

CD

現在の日付を表示するために使用する事前定義済みの変数。

CT

現在の時刻を表示するために使用する事前定義済みの変数。

PG

現在のページ番号を表示するために使用する事前定義済みの変数。

column | variable-name

このフィールドには、以前の変数式の変数を指定することも、BLOCK ステートメントの SQL 節内の列への参照を指定することもできます。

literal-text

事前定義済みの変数と列、および変数名以外のテキストは、リテラルテキストとして解釈されます。FOOTER ステートメントに含めるリテラルテキストは、入力したとおりの横位置に表示されます。

FOOTER ステートメントの特記事項

FOOTER ステートメントはレポート セクションの下端に印刷されます。概要情報や統計を表示するために使用するのが一般的です。FOOTER ステートメントは **BLOCK** ステートメントに含めることができます

フィールドの内容は、角かっこで囲まれたスペース分の長さになります。このスペースに入りきらない文字は切り捨てられます。ただし、山かっこ (>) でフィールドを閉じると、スペースを右余白まで拡張して内容全体を表示できます。

別の **BLOCK** ステートメント内の変数や列名を参照するには、以下の構文を使用します。

```
blockname::column | variable-name
```

レポート テンプレートの HEADER ステートメント

このレイアウト ステートメントは、レポート セクションの上端に情報を表示します。

HEADER ステートメントの構文

構文は、プログラム言語で使用するステートメントの構成を定めたルールです。HEADER の場合、この文字列の構造は以下のとおりです。

```
HEADER {parameters}
```

HEADER ステートメントのパラメータ

このステートメントで有効なパラメータのリストおよび説明については、[「レポート テンプレートの PAGE HEADER ステートメント」](#) (P. 626)を参照してください。

HEADER ステートメントの例

以下に、HEADER ステートメントの例を示します。

```
HEADER {  
    Contact Summary Report  
    Contact Name    Contact Alias    Organization  
}
```

HEADER ステートメントの特記事項

HEADER ステートメントはレポート セクションの先頭に印刷され、BLOCK ステートメントに含めることができます。HEADER ステートメントは、セクションや列の見出しを表示するために使用するのが一般的です。

フィールドの内容は、角かっこで囲まれたスペース分の長さになります。このスペースに入りきらない文字は切り捨てられます。ただし、山かっこ (>) でフィールドを閉じると、スペースを右余白まで拡張して内容全体を表示できます。

注: MULTILINE 変数の印刷ステートメントが終了山かっこ (>) で閉じられている場合、開始角かっこ (l) と終了山かっこ (>) で定義されているフィールド内に収まるように、空白で文字が折り返されます。また、変数が MULTILINE でない場合は、終了山かっこ (>) を指定すると、すべてのデータが長さとは無関係に現在の行に表示されます。

別の BLOCK ステートメント内の変数や列名を参照するには、以下の構文を使用します。

```
blockname::column | variable-name
```

レポート テンプレートの HEADER2 ステートメント

このレイアウト ステートメントは、レポート セクションが複数ページにまたがる場合に、そのレポート セクションの後続の各ページの上端にもヘッダ情報を表示します。

HEADER2 ステートメントの構文

構文は、プログラム言語で使用するステートメントの構成を定めたルールです。HEADER2 の場合、この文字列の構造は以下のとおりです。

```
HEADER2 {parameters}
```

HEADER2 ステートメントのパラメータ

このステートメントで有効なパラメータのリストおよび説明については、「[レポート テンプレートの HEADER2 ステートメント](#) (P. 624)」を参照してください。

HEADER2 ステートメントの例

```
HEADER2 {  
    Contact Summary Report (continued)  
    Contact Name    Contact Alias    Organization  
}
```

HEADER2 ステートメントの特記事項

HEADER2 ステートメントは **BLOCK** ステートメントに含めることができます。

フィールドの内容は、角かっこで囲まれたスペース分の長さになります。このスペースに入りきらない文字は切り捨てられます。ただし、山かっこ (>) でフィールドを閉じると、スペースを右余白まで拡張して内容全体を表示できます。

別の **BLOCK** ステートメント内の変数や列名を参照するには、以下の構文を使用します。

```
blockname::column | variable-name
```

レポート テンプレートの PAGE FOOTER ステートメント

このレイアウト ステートメントは、各レポート ページの下端に情報を表示します。

PAGE FOOTER ステートメントの構文

```
PAGE FOOTER {parameters}
```

PAGE FOOTER ステートメントのパラメータ

このステートメントのパラメータは、列および変数名を使用できないことを除き、**FOOTER** ステートメントと同じです。このステートメントで有効なパラメータのリストおよび説明については、[「レポート テンプレートの PAGE FOOTER ステートメント」](#) (P. 625)を参照してください。

PAGE FOOTER ステートメントのパラメータの例

```
PAGE FOOTER {  
    Page Number: [PG>  
}
```

PAGE FOOTER ステートメントのパラメータの特記事項

フィールドの内容は、角かっこで囲まれたスペース分の長さになります。このスペースに入りきらない文字は切り捨てられます。ただし、山かっこ (>) でフィールドを閉じると、スペースを右余白まで拡張して内容全体を表示できます。

別の **BLOCK** ステートメント内の変数や列名を参照するには、以下の構文を使用します。

```
blockname::column | variable-name
```

レポート テンプレートの PAGE HEADER ステートメント

このレイアウト ステートメントは、各レポート ページの上端に情報を表示します。

PAGE HEADER ステートメントの構文

構文は、プログラム言語で使用するステートメントの構成を定めたルールです。PAGE HEADER の場合、この文字列の構造は以下のとおりです。

```
PAGE HEADER {parameters}
```

PAGE HEADER ステートメントのパラメータ

このステートメントのパラメータは、列および変数名を使用できないことを除き、FOOTER ステートメントと同じです。このステートメントで有効なパラメータのリストおよび説明については、[「レポート テンプレートの PAGE FOOTER ステートメント」](#) (P. 625)を参照してください。

PAGE HEADER ステートメントの例

```
PAGE HEADER {  
    Date of Report: [CD>  
    Time of Report: [CT>  
}
```

PAGE HEADER ステートメントの特記事項

PAGE HEADER ステートメントは、各レポート ページの上端に印刷されます。 レポート テンプレート ファイル内の任意の場所で定義できますが、BLOCK ステートメントに含めることはできません。

フィールドの内容は、角かっこで囲まれたスペース分の長さになります。このスペースに入りきらない文字は切り捨てられます。ただし、山かっこ (>) でフィールドを閉じると、スペースを右余白まで拡張して内容全体を表示できます。

別の BLOCK ステートメント内の変数や列名を参照するには、以下の構文を使用します。

```
blockname::column | variable-name
```

レポート テンプレートの PRINT ステートメント

このレイアウト ステートメントは、レポート セクションにデータを表示します。

PRINT ステートメントの構文

構文は、プログラム言語で使用するステートメントの構成を定めたルールです。PRINT の場合、この文字列の構造は以下のとおりです。

```
PRINT {parameters}
```

PRINT ステートメントのパラメータ

このステートメントに有効なパラメータのリストと説明については、フッタを参照してください。

PRINT ステートメントの例

```
PRINT {  
[num ] [desc          ] [pr]  [stat] [catgry] [asgn          ]  
}
```

PRINT ステートメントの特記事項

PRINT ステートメントは、レポート内でレポート セクションのデータを表示する場所に記述します。**PRINT** ステートメントは **BLOCK** ステートメントに含めることができます

フィールドの内容は、角かっこで囲まれたスペース分の長さになります。このスペースに入りきらない文字は切り捨てられます。ただし、山かっこ (>) でフィールドを閉じると、スペースを右余白まで拡張して内容全体を表示できます。

注: **MULTILINE** 変数の印刷ステートメントが終了山かっこ (>) で閉じられている場合、開始角かっこ (l) と終了山かっこ (>) で定義されているフィールド内に収まるように、空白で文字が折り返されます。また、変数が **MULTILINE** でない場合は、終了山かっこ (>) を指定すると、すべてのデータが長さとは無関係に現在の行に表示されます。

別の **BLOCK** ステートメント内の変数や列名を参照するには、以下の構文を使用します。

```
blockname::column | variable-name
```

Crystal レポートのカスタマイズ

このレポートを表示するためには、以下の条件を満たす必要があります。

- Crystal レポートを Crystal ディレクトリの `$NX_ROOT/bopcfg/rpt` にコピーし、Crystal レポート セレクタで使えるようにする必要があります。
- データベース クライアントが稼動しており、同じコンピュータまたは別のコンピュータで稼動しているデータベース サーバとの接続が確立されている必要があります。**CA SDM Client** を使用して Crystal レポートまたは **Access** レポートを実行するためには、特定のデータベースに対応したデータベース クライアントをインストールし、データベース サーバとの接続を確立する必要があります。

カスタム Crystal レポートを作成した後で、以下の操作を行います。

1. カスタム Crystal レポートを、以下の Crystal ディレクトリにコピーします。

`$NX_ROOT/bopcfg/rpt`

2. カスタム Crystal レポートのファイル名を、以下の環境設定ファイルに追加します。

`crystal.cfg`

これで、タスクバーの[スタート]メニューから、[プログラム]-[CA SDM]-[レポート]-[Service Desk レポート (Crystal Reports)]の順に選択して、Crystal レポートにアクセスできます。[Service Desk レポート (Crystal)]ウィンドウが表示されます。

重要: CA SDM クライアントはアップグレードできません。そのため、CA SDM サーバで Crystal レポートを作成して使用している場合、CA SDM のバージョンをアップグレードするときは、カスタム レポートが失われないように、すべてのカスタム レポートを別の場所にコピーする必要があります。アップグレードを行った後で、レポートを Crystal ディレクトリの `$NX_ROOT/bopcfg/rpt` にコピーして戻します。次に、レポートセクタからアクセスできるように、`crystal.config` ファイルに変更を加えます。

第 10 章: CA CMDB の入力

このセクションには、以下のトピックが含まれています。

[データベースへの入力](#) (P. 631)

[GRLoader によるデータベースへの入力方法](#) (P. 631)

[GRLoader を使用したデータのインポート](#) (P. 632)

[ファミリーとクラスの割り当て](#) (P. 633)

[CA APM データのロード方法](#) (P. 633)

データベースへの入力

IT インフラストラクチャの CI および関係を CMDB に入力することは、このアプリケーションを効率的に使用するための作業の一部です。CMDB へのデータ入力は、ビルトイン構成アイテム エディタまたは GRLoader を手動で使用するか、ほかのアセット管理ツールからアイテムをインポートすることにより実行できます。

注: 構成アイテム エディタの詳細については、オンライン ヘルプを参照してください。

GRLoader によるデータベースへの入力方法

構成アイテムと関係をロードしてデータベースに入力するには、以下のタスクを実行します。

1. 構成アイテムおよびその関係に関する情報を含む入力データを XML またはスプレッドシートに変換します。
2. CA CMDB GRLoader プログラムでは、入力として XML データを使用します。
3. GRLoader によって、データがデータベースにロードされます。

注: GRLoader のパラメータの詳細については、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。

関連項目:

[GRLoader を使用したデータのインポート \(P. 632\)](#)

GRLoader を使用したデータのインポート

CA SDM の GRLoader プログラムを使用してデータをインポートすると、XML ファイルまたは Excel スプレッドシート ファイルのデータに基づいて構成アイテムが作成されます。

次の手順に従ってください:

1. 「スタート」メニューから「ファイル名を指定して実行」を選択します。

2. 「cmd」と入力します。

DOS コマンドウィンドウが表示されます。

3. 以下のコマンドを入力します。

```
Grloader -u <username> -p <password> -s http://<ca_sdm_servername>:8080  
-i <xml_document or spreadsheet>
```

GRLoader が XML ファイル内のデータを使用して CI を作成します。このプロセスでエラーが検出されると、エラー ファイルが作成され、インポートできなかった CI およびその理由のリストが表示されます。

GRLoader のインポートが完了します。

4. CA SDM を起動し、CI データが正しく入力されたことを確認します。
5. CMDB Visualizer を起動し、関係データが正しく入力されたことを確認します。

データがインポートされ検証されます。

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。

ファミリーとクラスの割り当て

各 CI に分類スキームを適用します。このスキームには各 CI の割り当てと、以下の属性が含まれます。

- ファミリー - 同様の属性を持つ構成アイテムのコレクション
- クラス - ファミリー内の構成アイテムのサブセット

割り当ては以下の方法で作成できます。

- 各ハードウェア アセットについてファミリーおよびクラスを識別する製造者データを入力する。
- ファミリーおよびクラスのための空ではない値を入力ファイル内のそれぞれのカラムに含める。

CI のファミリーおよびクラスを既存のファミリーおよびクラスで解決できない場合、GRLoader ではその CI をインポートしません。

CA APM データのロード方法

CA Asset Portfolio Management (CA APM) Loader プログラムへの主な入力 は、CA APM インポート データの抽出が含まれたテーブルまたはビューです。このデータは、CMDB_Export_Asset_Data データベース テーブルまたは表示に含まれています。場合によっては、MDB へのインポート データは、ターゲットと同じデータベースに置かれています。しかし、多くの場合、インポート データは、たとえば補助データベース間でインポートする場合のように、別のデータベースに存在します。どちらの場合も、ソース データと同じデータベース上に表示を作成します。

CA APM データ ビューには、クラスおよびファミリーの属性が含まれません。また、異なる分類スキームを持つシステムから派生することもあります。たとえば、アセット データのソースが別の会社である場合、異なる分類システムが実施されている可能性があります。

CA_MODEL_DEF テーブルには、モデルの一覧表が含まれています。この一覧表は、CMDDB_Export_Asset_Data 内のデータと照合されます。合致した場合、インポートされるアセットにモデルのファミリーおよびクラスが割り当てられます。合致しなかった場合は、そのアセット用に新規モデルを定義してください。ソース CA_MODEL_DEF テーブルのエントリをターゲット MDB にコピーするか、または CA_MODEL_DEF テーブルを全面新規ハードウェア型およびモデル番号のエントリで更新するかを検討します。

第 11 章: MDR ランチャの使用

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、CI の統一データを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 ランチャ](#) (P. 636)

[MDR 用語](#) (P. 637)

[MDR マッピング](#) (P. 639)

[MDR 起動](#) (P. 639)

[CMDBf ビューア](#) (P. 639)

[CA CMDB で MDR を定義する](#) (P. 640)

[GRLoader を使用した統一](#) (P. 650)

[MDR CI と CA CMDB CI 間のマップ](#) (P. 652)

[CMDBf ビューア用の MDR の設定方法](#) (P. 654)

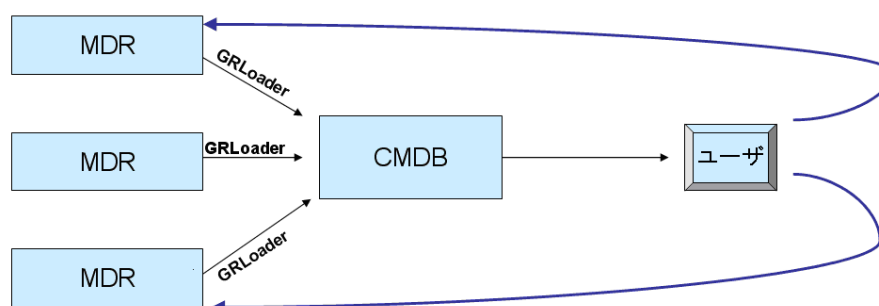
[MDR Web ブラウザインターフェースの起動](#) (P. 654)

[CA Cohesion 統合](#) (P. 655)

MDR ランチャ

CA CMDB を実装する主な目的の 1 つは、複数のデータベース ソース (MDR と呼ばれます) からのデータをまとめることです。しかし、CI には、常に、その MDR 起源に戻る参照が含まれている必要があります。

CA CMDB は、CI をインポートおよびロードするほか CI をその起源に関係付ける機能を提供します。また、CA CMDB で CI を表示するときに MDR ランチャ機能を使用することにより、以下の図に示すように、CI の起源のシステムにシームレスに戻ることができます。



MDR ランチャを使用すると、以下のように「閉ループ」変更管理プロセスを実行することができます。

1. 変更レコードを作成します。
2. 変更を行います。
3. MDR ソースをチェックすることにより変更を確認します。
4. CMDB を更新して、変更が行われたことを示します。

問題管理プロセスの視点から、以下の方法により **MDR** ランチャを使用できます。

1. 問題を検出します。
2. 影響を受けている従属 **CI** を特定するために **CI** 関係のデータを利用することにより、問題の重大度および感染力を調べます。
3. プロバイダ **CI** を調査することにより、問題の考えられる原因を特定します。
4. 必要に応じて **MDR** で利用可能な高度詳細情報を使用して詳細分析を行った後に、**MDR** を使用して適切な処置を行います。

MDR 用語

CMDB-MDR 統合では、以下の用語が使用されます。

管理データリポジトリ (**MDR**) は、**CI** に関するソース情報を含むソフトウェアまたはデータを表します。**MDR** には、通常、**CMDB** より多くの未調整 **CI** 情報が含まれていますが、それにはそのデータの管理サブセットが含まれています。

MDR クラス (**MDR_CLASS**) は、**CA CMDB** により同様に処理された複数の **MDR** をまとめるために使用されます。**COHESION**、**GLOBAL**、**cmdbf** という 3 つの特別な **MDR** クラスがあります。

MDR 名 (**MDR_NAME**) は、**MDR** が自分自身を参照するために使用する名前です。**mdr_name** と **mdr_class** の値の組み合わせが社内で一意であることを確認する必要があります。

統一アセット ID (**FEDERATED_ASSET_ID**) は **CI** の一意の **MDR ID** です。

異なる **CI** ファミリは、通常、データ プロバイダとして、それぞれ異なる **MDR** を使用します。しかし、1 つの **CI** が複数の **MDR** データ プロバイダを持つことは可能です。以下に例を示します。

CI ファミリ	MDR_CLASS
連絡先	人事管理システム
	電話帳
	シングル サインオン認証システム

CI ファミリ	MDR_CLASS
Document	ドキュメント管理システム
Air Conditioning（空調設備）	ドキュメント管理システム 契約管理システム 空調システム
メインフレーム	テープ管理システム DASD 管理システム パフォーマンス管理システム ジョブ スケジューラ
ストレージ	ストレージ管理システム 資産管理システム
Location	資産管理システム エデュケーション カレンダ オフィス ディレクトリ
ネットワーク	ネットワーク管理システム 問題管理システム

各 MDR クラスに複数の MDR が存在することができ、各 MDR は複数の CI にデータを提供できます。任意の CI がゼロまたは複数の MDR からデータを受け取ることができます。CI は、自身にデータを個別に提供させることもできます。たとえば、1 つのメインフレーム CI がディスク管理システム 1 によって提供されたデータを持つ一方、ほかのメインフレーム CI がディスク管理システム 2 およびジョブ スケジューラ 2 によって提供されたデータを持つことができます。CA CMDB は、CI 間の関係およびすべての CI の関連 MDR を管理します。

MDR マッピング

すべての MDR には、それ自体が管理する CI を識別する固有の方法があります。これらの識別子が MDR 間で同期されることは、ほとんどありません。たとえば、特定の連絡先 CI を参照する場合、各 MDR は、国民識別番号、電話番号、運転免許証番号、または社員 ID を使用できますが、これらはすべて同一人物を指します。これらの異なる識別子を MDB 内に維持されている同一の固有識別子 (UUID) に関係づけるプロセスを、マッピングと言います。マッピングは、GRLoader を使用してデータがインポートされたときに、CI に `<mdr_name>` `<mdr_class>` タグおよび `<federated_asset_id>` タグが含まれている場合に自動的に行われます。マッピングは、ユーザ インターフェースの管理機能によって手動で行うこともできます。それ自体に関連付けられたマッピングを持たない CI は、統一されていない CI と呼ばれます。すべての CI は、UUID を `federated_asset_id` として使用し、グローバル MDR に自動的にマップされます。

MDR 起動

CA CMDB ユーザ インターフェースを使用して CI を表示する場合、一連のボタンをクリックして、MDR ユーザ インターフェースを直接起動できます。フォーカス CI の MDR マッピング 1 つにつき、ボタンが 1 つあります。通常、この起動操作は、変更要求が正常に完了したことをユーザが確認する場合、またはデータが CMDB により収集されない場合に CI に関する追加情報を取得するために行われます。

CMDBf ビューア

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。

CA CMDB で MDR を定義する

CMDBf ビューアを使用する前に、CA CMDB に MDR を定義しておく必要があります。

CA CMDB に新規 MDR を定義する方法

1. [管理] タブで、[CA CMDB] - [MDR 管理] - [MDR リスト] に移動します。
2. [新規作成] をクリックします。
[MDR 定義の新規作成] 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。

テナント

この MDR のテナント所有者を指定します（マルチテナンシーがインストールされている場合）。

ボタン名

[構成アイテムの詳細] ページに表示する MDR ボタンのラベル。この名前は、各 MDR で一意とする必要があります。「コンテキスト起動」および CMDBf ビューアに必要です。

MDR 名

mdr_name フィールドで送信される XML データと一致する文字列。MDR には任意の文字列を使用できますが、多くの場合はホスト名が使用されます。この名前は、mdr_class と共に MDR の一意の名前を形成します。「コンテキスト起動」および CMDBf ビューアに必要です。

MDR クラス

XML の `mdr_class` フィールドで送信されるデータと一致するクラス。この名前は任意の文字列でかまいませんが、`mdr_name` フィールドと共に MDR の一意の ID を形成するものであることが必要です。グローバル MDR は MDR クラス GLOBAL で定義されます。

- CA Cohesion ACM MDR は、MDR クラス COHESION を指定する必要があります。このクラスは、パス、パラメータ、および「起動 URL」の各フィールドを CA Cohesion ACM のコンテキスト起動の必須値に自動的に設定します。
- CA Asset Portfolio Management r11.3.4 MDR は、MDR 名 APM および MDR クラス GLOBAL を指定する必要があります。このクラスは、パス、パラメータ、および「起動 URL」の各フィールドを CA Asset Portfolio Management r11.3.4 のコンテキスト起動の必須値に設定します。
- CA APM r12.5 MDR は、MDR 名 ITAM および MDR クラス GLOBAL を指定する必要があります。このクラスは、パス、パラメータ、および「起動 URL」の各フィールドを CA APM 12.5 のコンテキスト起動の必須値に自動的に設定します。
- CMDBf ビューアの場合、MDR クラスは `cmdbf` である必要があります。

アクティブ

この MDR 定義がアクティブか非アクティブかを示します。非アクティブ MDR 定義は論理的に削除されますが、検索ユーティリティを使用して再びアクティブにすることができます。

所有者

この MDR を担当する連絡先。

説明

自由形式のテキストで説明を入力します。

ホスト名

起動する Web ページをホストする Web サーバを含むホストのホスト名、DNS 名または IP アドレス。「コンテキスト起動」に必要です。

ポート

Web ページを配信する MDR の Web サーバによって使用される TCP/IP ポート。デフォルトはポート 80 です。「コンテキスト起動」に必要です。

パス

URL の疑問符 (?) の前の部分。この情報は、MDR ドキュメントから入手できます。

- `mdr_class` が Cohesion の場合、この値は自動的に「CAisd/html/cmdb_cohesion.html」に設定され、変更できません。
- `mdr_name` が APM で `mdr_class` が GLOBAL の場合、値は自動的に `apm/frmObject.aspx` に設定され、変更できません。
- `mdr_name` が ITAM で `mdr_class` が GLOBAL の場合、値は自動的に `ITAM/Pages/Asset.aspx` に設定され、変更できません。

Parameters (パラメータ)

URL の疑問符 (?) の後の部分。この情報は、MDR ドキュメントから取得できます。

- `mdr_class` が Cohesion の場合、この値は自動的に「hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id}」に設定され、変更できません。
- `mdr_name` が APM で `mdr_class` が GLOBAL の場合、値は自動的に
ObjectID={cmdb_asset_id}&obj=11&FUNCTION=1&WinID=OBFRASSET{cmdb_asset_id}&WinContainerID= に設定され、変更できません。
- `mdr_name` が ITAM で `mdr_class` が GLOBAL の場合、値は自動的に
ParentClass=Asset&assetid={cmdb_asset_id}&TicketID={itam_ticketid} に設定され、変更できません。

ユーザ ID

必要に応じて MDR ユーザ ログイン情報を指定します。この値は、URL に使用されている {userid} と置き換えられます。空白の場合、userid はデフォルトにより現在サインオンしているユーザに設定されます。

CA Cohesion ACM では、「共有秘密」は必要に応じて CA Cohesion ACM へのアクセスに使用される秘密です。この値は、URL に使用されている {password} と置き換えられます。

注: MDR 定義の詳細については、「*CA Cohesion ACM Implementation Guide*」を参照してください。

共有秘密

CA CMDB と MDR 間で共有する情報を指定します。この値は、URL に使用されている {password} と置き換えられます。CA Cohesion ACM MDR の場合、この値は

「com.cendura.security.oneclickauth.secret」の値に一致する必要があります。共有秘密の作成方法の詳細については、CA Cohesion ACM の「実装ガイド」で CA CMDB との統合を参照してください。CMDBf ビューアに必要です。

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。

URL to be Launched

デフォルト値は `http://{hostname}:{port}/{path}?{parameters}` です。
一部の MDR では、MDR 固有の必要要件に対応する必要がある場合に上書きされる可能性があります。「コンテキスト起動」で必須です。

`mdr_name` が APM で `mdr_class` が GLOBAL の場合、値は `http://{hostname}:{port}/{path}?{parameters}` です。

`mdr_name` が ITAM で `mdr_class` が GLOBAL の場合、値は `http://{hostname}:{port}/{path}?{parameters}` です。

Cohesion の `mdr_class` では、デフォルト値は `http://cmdb_hostname:cmdb_port/{path}?{parameters}` です。

各項目は以下のとおりです。

`cmdb_hostname` は、CA CMDB Web サーバのホスト名、DNS 名、または IP アドレスです。現在 CA CMDB Web サーバにアクセスしている現在のホスト名がデフォルトになります。

`cmdb_port` は、CMDB Web サーバの TCP/IP ポートです。デフォルトでは、CA CMDB Web サーバへのアクセスに使用される現在のポート番号が設定されます。

注: CA Cohesion ACM で SSL サポートを有効にしている場合、URL を次のように設定します。

`http://hostname:port/{path}?{parameters}+https=yes`

CA Cohesion ACM HTTPS サポートの有効化の詳細については、CA Cohesion ACM オンラインヘルプトピックの「Creating the HTTPS Certificate and Enabling HTTPS」を参照してください。

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。

4. [保存] をクリックします。

MDR が定義されます。

MDR URL の定義

起動 URL には、初期設定値として

`http://{hostname}:{port}/{path}?{parameters}` があります。この式は、MDR 固有の考慮事項に適応する必要がある場合は、変更することができます。

「コンテキスト起動」には、この URL が必要です。

`mdr_name` が APM または ITAM、`mdr_class` が GLOBAL の場合、デフォルト値は以下のようになります。

`http://{hostname}:{port}/{path}?{parameters}`

`mdr_class` が Cohesion の場合、初期設定値は以下のとおりです。

`http://{cmdb_hostname}:cmdb_port/{path}?{parameters}`

cmdb_hostname

CA CMDB Web サーバのホスト名、DNS 名、または IP アドレスを指定します。現在 CA CMDB サーバにアクセスしている現在のホスト名がデフォルトになります。

cmdb_port

CA CMDB Web サーバの TCP/IP ポートを指定します。CA CMDB Web サーバにアクセスするために使用されている現在のポート番号がデフォルトになります。

CA Cohesion ACM で SSL サポートを有効にしている場合、URL を次のように設定します。

`http://{hostname}:port/{path}?{parameters}+https=yes`

注: CA Cohesion ACM の HTTPS サポートの有効化の詳細については、CA Cohesion ACM のオンライン ヘルプを参照してください。

MDR 起動 URL

MDR 起動 URL には以下のデフォルト値があります。

`http://{hostname}:{port}/{path}?{parameters}`

MDR 固有の考慮事項に適応するように、この式を変更できます。「コンテキスト起動」には、この URL が必要です。

- `mdr_name` が APM または ITAM、`mdr_class` が GLOBAL の場合、デフォルト値は以下のようになります。

`http://{hostname}:{port}/{path}?{parameters}`

- `mdr_class` が Cohesion の場合、デフォルト値は以下のとおりです。

`http://{cmdb_hostname:cmdb_port}/{path}?{parameters}`

cmdb_hostname

CA CMDB Web サーバのホスト名、DNS 名、または IP アドレスです。
現在 CA CMDB サーバにアクセスしているホスト名がデフォルトになります。

cmdb_port

CA CMDB Web サーバの TCP/IP ポートです。CA CMDB Web サーバにアクセスするために使用されている現在のポート番号がデフォルトになります。

CA Cohesion ACM で SSL サポートを有効にしている場合、URL を次のように設定します。

`http://{hostname:port}/{path}?{parameters}+https=yes`

注: CA Cohesion ACM の HTTPS サポートの有効化の詳細については、Cohesion のオンラインヘルプを参照してください。

URL 置換の起動パラメータの定義

MDR を定義するときに、以下のパラメータを使用して表示用 URL を作成できます。これらのパラメータは、実行時に適切な値に置き換えられます。これらの変数は、前述のフィールドで指定する必要があります。

hostname は、MDR 定義の MDR ホスト名です。

alarm_id は、選択した CI の IP アドレスです。

federated_asset_ID は、MDR で選択した CI の一意の ID です。

cmdb_asset_id は、CI のアセット ID です。

port は、MDR 定義の MDR ポート番号です。

userid は、MDR 定義のユーザ ID です。空白の場合、*userid* はデフォルトにより現在サインオンしているユーザに設定されます。

password は、MDR 定義からの共有秘密です。

mdr_name は、MDR 定義の *mdr_name* です。

mdr_class は、MDR 定義の *mdr_class* です。

class は、選択した CI のクラスです。

family は、選択した CI のファミリーです。

path は、MDR 定義に記述されたパスです。

name は、選択した CI の名前です。

model は、選択した CI のモデルです。

manufacturer は、選択した CI の製造者です。

itam_ticketid は、CA APM にログインするためのチケット ID です。

例: MDR を起動する

CA CMDB のユーザが **server1** と命名されたサーバ CI を参照します。この CI は、**Comet** という名前の社内で開発されたアプリケーションへのマップを持っています。**Comet** は、**server1** を **server:server1** として一意に識別します。

Comet は、以下のプロパティを持つ MDR として定義されます。

- ホスト名 : **CometServer**
- ポート : **80**
- パス : **index.php**
- パラメータ : **item={federated_asset_id}**
- Launch_url: **http://{hostname}:{port}/{path}?{parameters}**

CA CMDB で、ユーザが **server1** CI の [属性] タブ上の **Comet** ボタンをクリックすると、Web ブラウザ ウィンドウが以下の URL を開きます。

http://CometServer:80/index.php?item=server:server1

URL 置換のパラメータ

MDR を定義するときに、以下のパラメータを使用して表示用 URL を作成できます。これらのパラメータは、実行時に適切な値に置き換えられます。これらの変数は、MDR フィールド定義で指定する必要があります。

{hostname}

MDR 定義の MDR ホスト名です。

{alarm_id}

選択した CI の IP アドレスです。

{federated_asset_ID}

MDR で選択した CI の一意の ID です。

{cmdb_asset_id}

CI のアセット ID です。

{port}

MDR 定義の MDR ポート番号です。

{userid}

MDR 定義のユーザ ID です。未指定の場合、userid は、現在サインオンしているユーザに初期設定されます。

{password}

MDR 定義の共有シークレットです。

{mdr_name}

MDR 定義の mdr_name です。

{mdr_class}

MDR 定義の mdr_class です。

{class}

選択した CI のクラスです。

{family}

選択した CI のファミリーです。

{path}

MDR 定義に記述されたパスです。

{name}

選択した CI の名前です。

{model}

選択した CI のモデルを指定します。

{manufacturer}

選択した CI の製造者を指定します。

例: URL 置換のパラメータの使用

CA CMDB のユーザが server1 と命名されたサーバ CI を参照します。この CI は、Comet と呼ばれる社内で開発されたアプリケーションへのマップを持っています。Comet は、server1 を server:server1 として一意に識別します。

Comet は、以下のプロパティを持つ MDR として定義されます。

- ホスト名 : CometServer
- ポート : 80
- パス : index.php
- パラメータ : item={federated_asset_id}
- Launch_url: http://{hostname}:{port}/{path}?{parameters}

CA CMDB で、ユーザが server1 CI の [属性] タブ上の Comet ボタンをクリックすると、Web ブラウザ ウィンドウが以下の URL を開きます。

`http://CometServer:80/index.php?item=server:server1`

GRLoader を使用した統一

GRLoader を使用する場合、以下の XML タグを XML ドキュメント内のすべての CI に入力する必要があります。これらのタグは、すべての MDR ファミリに適用されます。

- <mdr_name>
- <mdr_class>
- <federated_asset_id>

注: CA Cohesion ACM は、自動的に mdr_name、mdr_class および federated_asset_id を提供します。

この情報が XML 内に存在しない場合、CI の起源を決定できないので、「コンテキスト起動」は不可能です。

CI のソースを識別するために、XML を GRLoader に入力する前に、その XML を変更します。XML の変更は、テキスト エディタを使用してからグローバルに変更するか、プログラムで行うことができます。

注: MDR 識別と 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。

CI の統一

CI に対応する MDR が定義される前に、CI が CA CMDDB にロードされた場合、それは統一されません。これは、CI が MDR にまだ接続されていないことと、まだ「コンテキスト起動」をサポートしていないことを意味します。

CI を統一する方法

1. 必須 MDR を定義します。
2. 以下のいずれかの操作を実行します。
 - CI を手動でマップする。
 - レポート上の既存の CI の更新を許可した上で、CI を作成した CA Cohesion ACM レポートを再度実行する。

注: CA Cohesion ACM レポートの詳細については、「*CA Cohesion ACM Product Guide*」を参照してください。

3. CI を作成するために使用されたものと同じ入力ファイルを指定して GRLoader を再実行します。

CA CMDDB 調整エンジンにより MDR 情報が既存 CI にマージされます。

4. CI およびその MDR を記述する XML ドキュメントを作成し、GRLoader を更新モードで実行します。

CA CMDDB 調整エンジンが新規情報を既存 CI にマージします。既存 CI が統一されます。

例: CI のロケーションの指定

更新する CI を探すために十分な情報が調整エンジンに与えられていることを確認する必要があります。以下の例の場合、読みやすさを優先して終了タグを削除し、スペースを追加しています。

```
<ci>
  <name>          server3
  <mac_address>
  <serial_number>
  <asset_num>
  <dns_name>
  <mdr_name>      mdr_one
    <mdr_class> Cohesion
</ci>
```

GRLoader を使用して 1 つの CI に複数の MDR を定義する

GRLoader を使用して、1 つの CI に複数の MDR を定義することができます。

1 つの CI に複数の MDR を定義するには、XML ドキュメントで <ci> ノードを繰り返し、繰り返された各 <ci> ノードで異なる mdr_name および mdr_class を指定します。言い換えると、各 MDR は、CI にデータを与えるほかの MDR と関係なく、それ自体の属性を与えることができます。

例: 1 つの CI に複数の MDR を定義する

MDR1 と MDR2 の両方が server2 CI データを与える場合、XML ドキュメントは以下の例のようになります。この例の場合、読みやすくするために終了タグが削除され、スペースが追加されます。

```
<ci>
  <name>      server2
  <mdr_name>  mdr1
  <mdr_class> Cohesion
  <diskspace> 500 gb
  <disktype>  SCSI-3
</ci>
<ci>
  <name>      server2
  <mdr_name>  mdr2
  <mdr_class> Service Assure
  <sla>
</ci>
```

CA CMDB は、上記の 2 つの CI を同一 CI に調整し、2 つの MDR のそれぞれを上記の 1 つの CI に関連付けます。

注: GRloader の 1 度または 2 度の実行で CI がインポートされる場合があることに注意してください。

MDR CI と CA CMDB CI 間のマップ

[ファイル]、[新規構成アイテム] オプションを使用して手動で CI を定義した後、この CI と、統一 MDR 内の CI との間に、マッピングを手動で定義する必要があります。CI を MDR に関連付ける方法は 2 つあります。

- CI を編集する
- [CA CMDB 管理] タブ上の [統一 CI マッピング] ノードを使用する

CI を編集してマッピングを作成するには、以下の手順に従います。

1. MDR に関連付ける CI の [構成アイテムの詳細] ページを表示します。
2. [編集] をクリックします。
3. [属性] タブを表示します。
4. [Add MDR] をクリックします。

CI が MDR と関連付けられます。

[統一 CI マッピング] ページを使用してマッピングを作成するには、以下の手順に従います。

1. [CA CMDB 管理] タブをクリックします。
2. [管理データ リポジトリ] ノードを開きます。
3. [統一 CI マッピング] ノードを選択します。
[統一 CI マッピング] リストが表示されます。
4. [新規作成] をクリックします。
[次の統一 CI マッピングを新規作成] ページが表示されます。
5. 統一 CI マッピングのフィールドにデータを入力して、CI と MDR を関連付けます。

CI 名

構成アイテムの識別に使用する名前。

統一アセット ID

ソース MDR で、この CI を識別するために使用する文字列 ID。ID は MDR ソフトウェアによって決定されます。

MDR 名

MDR (およびその MDR ボタン) を識別する名前。

アクティブ

このマッピング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。マッピングは非アクティブにすることができるだけで、削除することはできません。

6. [保存] をクリックします。

この CI と統一 MDR 内の CI との間のマッピングが定義されます。

CMDBf ビューア用の MDR の設定方法

CMDBf Viewer を使用するには、事前に以下を実行して、CMDBf クエリ サービスを指すように、統一 MDR プロバイダをセットアップします。

- 外部 MDR によって、InstanceIdConstraint クエリを処理できるクエリ サービスを取得します。
- [CI の詳細] ページに [CMDBf ビューア] ボタンを表示するために、ボタン名、MDR 名、および MDR クラスを設定します。
- MDR クラスを、**cmdbf** として定義します。
- CA CMDB の場合は、CMDBf ネームスペースを **http://cmdb.ca.com/r1** に設定します。その他の CMDB および MDR の場合は、該当するドキュメントを参照してください。
- タイムアウトはオプションです。デフォルトでは 10 秒に設定されています。
- 統一表示上に有効な [取得] ボタンを表示するために、CMDBf エンドポイント、ユーザ ID、および共有シークレットを定義します。

注: CMDBf エンドポイントに

「**http://servername:port/axis/services/QueryPort**」を指定することで、既存の CA CMDB システムを CMDBf プロバイダとしてセットアップできます。

- ホスト名は、CA CMDB がインストールされているコンピュータ（ローカル ホスト名またはコンピュータ名）です。
- ポートは CA CMDB が設定されているポートです。

MDR Web ブラウザ インターフェースの起動

CI と MDR 間のマッピングが作成された後、[属性] タブ上に 1 つのボタンが自動的に表示されます。複数の MDR がこの CI に関連付けられている場合、複数のボタンが表示されます。

MDR ボタンをクリックすると、新しいページが開き、MDR 定義内で定義されている MDR URL が完全に置換されて表示されます。

例: CA Cohesion の起動

CI がその MDR に正しく関連付けられている場合、[属性] タブに Cohesion ボタンが表示されます。ボタンが [属性] タブ上に表示されない場合には、表示されている CI のマッピングを確認します。この CI のマッピングが存在すること、およびターゲット MDR に起動可能な URL があることを確認してください。MDR を起動するボタンをクリックすると、CA Cohesion を起動するターゲット URL への新規ウィンドウが開きます。

CA Cohesion 統合

CA Cohesion ACM を CA CMDB に統合する場合、以下の点に注意してください。

- Cohesion を CA CMDB に統合する

注: Cohesion-CA CMDB 統合の詳細については、「*CA Cohesion ACM Implementation Guide*」を参照してください。

- Cohesion MDR から CI をインポートする

注: Cohesion MDR から CI をインポートする方法については、CA Cohesion ACM レポートの [レポート テンプレート] タブから利用できるオンライン ヘルプを参照してください。

- Cohesion MDR のコンテキスト起動

コンテキスト起動の統合が CA Cohesion ACM と最適に連動するように、Cohesion CMDB レポートを実行する前に [CA CMDB 管理] タブを使用して Cohesion MDR を定義することをお勧めします。

注: CA Cohesion ACM は、NIC または File System CI の固有の統一アセット ID をサポートしません。そのため、Cohesion は、NIC または File System CI の MDR ランチャをサポートしません。したがって、Cohesion ベースの NIC または File System CI は、インポートが正常に行われても、MDR ランチャ ボタンを表示しません。

第 12 章: Web サービスの管理

重要: Web サービスの詳細については、「CA SDM テクニカル リファレンス ガイド」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。

[Web サービスの管理](#) (P. 657)

[CA SDM コンポーネント](#) (P. 658)

[SOAP Web サービス クライアントに関するヒント](#) (P. 658)

[SOAP Web Services Configuration](#) (P. 661)

[Web サービスのセキュリティ](#) (P. 663)

[SOAP エラー処理](#) (P. 666)

[Web サービスのインストール](#) (P. 670)

[外部仕様](#) (P. 671)

[オブジェクト](#) (P. 693)

[ITIL 方式](#) (P. 699)

[Web サービスの利用](#) (P. 702)

Web サービスの管理

Web サービスとは、異なる動作環境同士であっても製品間の通信を可能にする、一連のデータ交換標準のことです。この機能はパーソナルコンピュータで Web サイトをブラウズするのと似ています。つまり、リモートの Web サイトが Solaris、AIX、Windows などいずれのホストオペレーティングシステム上にあってもアクセスできるのと同じことです。同様に、Web サービスを利用すると、動作環境にかかわらず HTTP プロトコルを介して製品がさまざまなサービスと通信することができます。たとえば、Microsoft Office 製品は UNIX サーバ上のプログラムと通信でき、Java Server Page は Windows サーバ上でホストされているサーバにアクセスできます。このプラットフォームに依存しない通信によって、強力なインテグレーションシステムが実現されます。

Web サービスではこのテクノロジーを利用するため、ほとんどの製品で CA SDM およびナレッジマネジメントの機能を使用することができます。Web サービスクライアントは、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。

CA SDM コンポーネント

CA SDM では、J2EE Web サービスのこのバージョンのインストール ファイルが以下のディレクトリに置かれています。

```
<NX_ROOT>/sdk/websvc/R11
```

注: <NX_ROOT> は CA SDM のルートになるインストール パスです。

SOAP Web サービス クライアントに関するヒント

CA SDM インストールのサンプル ディレクトリには、Web サービス用のサンプル Java クライアント アプリケーションが用意されています。このサンプルは、Web サービス クライアント アプリケーション 開発に役立ちます。

Web サービス メソッドの多くは、入力パラメータとして配列を必要とします。たとえば、`createIssue()` メソッドでは、`propertyValues` の空の配列を渡すことができます。これらの配列は省略できる場合もありますが、その場合は空の配列を渡す必要があります。Visual Studio .NET を使用して Web サービスにアクセスする場合は、以下のいずれかの方法で空の配列を指定します。

C#言語

```
String[] emptyArray = new string[0];
```

Visual Basic .NET

```
Dim emptyArray As String() = {}
```

Java

```
ArrayOfString attr = new ArrayOfString();  
attr.setString(new String[0]);  
ArrayOfString is a proprietary class.
```

`emptyArray` は、空の配列を受け付ける配列パラメータに渡すことができます。

注: CA SDM Web サービスは、World Wide Web コンソーシアム (W3C) によって確立された標準の Apache 実装を使用しています。オペレーティング環境の種類に関係なくクライアントがサービスにアクセスできることが理想ですが、ベンダの実装によってはアクセスできないこともあります。多くのプログラム環境では、Web サービス記述用語 (WSDL) からプロキシクラスを生成するためのツールを提供しています。

関連項目:

[Java クライアント](#) (P. 659)

Java クライアント

\$NX_ROOT/samples/sdk/websvc 内の TableOfContents.doc に、Java サンプルプログラムが複数記載されています。

各サンプルプログラムには、スクリプト ファイル `run_java_test.bat.txt` (Windows) および `run_java_test.sh.txt` (UNIX) を使用してコンパイルおよび実行する方法を説明したメモが含まれています。これらのスクリプトは、`org.apache.axis.wsdl.WSDL2Java` を使用して CA SDM Web サービスのクライアント側スタブ ファイルを生成する方法を示しています。

Axis 1.4 を使用する場合は、正常にスタブ ファイルを生成するために、`-w` パラメータが必要です。記載されたとおりに `WSDL2Java` を実行すると、サブディレクトリ `com/ca/www/UnicenterServicePlus/ServiceDesk` 内にスタブ ファイルが生成されます。以下のファイルが生成されます。

- `ArrayOfInt.java`
- `ArrayOfString.java`
- `ListResult.java`
- `USD_WebService.java`
- `USD_WebServiceLocator.java`
- `USD_WebServiceSoap.java`
- `USD_WebServiceSoapSoapBindingStub.java`。

以下のステートメントを使用して、これらのクラスをインポートします。

```
import com.ca.www.UnicenterServicePlus.ServiceDesk.*;
```

Web サービス メソッドの多くには、独自のクラス `ArrayOfString` タイプのパラメータがあります。たとえば、`createRequest()` メソッドの `attrVals`、`propertyValues`、および属性パラメータは、すべて `ArrayOfString` パラメータです。

`ArrayOfString` 変数に値を設定するには、変数をインスタンス化してから、以下のように `setString()` を使用します。

```
ArrayOfString attrVals = new ArrayOfString();
attrVals.setString(new String[]{"customer", customerHandle, "description",
"description text"});
```

空に設定する方法

```
attrVals.setString(new String[0]);
```

`List` メソッドからの戻り値として、別の独自クラス `ListResult` タイプの次のような変数を使用します。 `doQuery()`、 `getRelatedList()`、 `getNotificationsForContact()`、 `getPendingChangeTaskListForContact()`、および `getPendingIssueTaskListForContact()`。 `ListResult` には `listHandle` および `listLength` エレメントが含まれており、以下の例で示すとおり `getListHandle()` and `getListLength()` を使用して取得できます。

```
ListResult doQueryResult = new ListResult();
doQueryResult = USPSD.doQuery(sid, "iss", "active = 1");
int listHandle = doQueryResult.getListHandle();
int listLength = doQueryResult.getListLength();
```

`getListValues()` メソッドでは、`listHandle` を使用して、リストのサブセットから値を取得します。

`freeListHandles()` メソッドの `Handles` パラメータは、別の独自クラス `ArrayOfInt` です。 `ListResult` から取得した `listHandle` を使用して、`freeListHandles()` を呼び出します。

```
ArrayOfInt handleList = new ArrayOfInt();
handleList.setInteger(new java.lang.Integer []{ new
java.lang.Integer(listHandle) });
USPSD.freeListHandles(sid, handleList);
```

メソッドの中には、`javax.xml.rpc.holders.StringHolder` タイプの参照パラメータによる引き渡しがあるものもあります。たとえば、`createRequest()` には、このタイプのパラメータが `NewRequestHandle` と `NewRequestNumber` の 2 つあります。

```
StringHolder NewRequestNumber = new StringHolder();
StringHolder NewRequestHandle = new StringHolder();
String result;
result = USPSD.createRequest(sid, creatorHandle, attrVals, propertyValues, template,
attributes, NewRequestHandle, NewRequestNumber);
```

これによって、Request のハンドルおよび参照番号 (ref_num) は、NewRequestHandle.value および NewRequestNumber.value からそれぞれ取得できます。

SOAP Web Services Configuration

CA SDM SOAP Web サービスは、専用の Web 環境設定ファイルのエントリを使用して設定できます。以下の表に、設定オプションの名前および説明を示します。

オプション名	説明
design_mode_stubs	Web サービスを「デザイン モード」に設定します (CA SDM のみ)。
require_secure_logon	login() および loginService() Web メソッドを、https などの暗号化プロトコルを使用してコールする必要があります。
require_secure_connection	すべての Web メソッドを暗号化プロトコルを使用してコールする必要があります。
disable_user_logon	login() および loginService() の両方の Web メソッドを無効にするため、ログインには loginServiceManaged() だけが使用できます。

CA SDM では、Web サービス メソッドに渡された属性値の長さを検証することにより、実行している Tomcat サーバの完全性を保護しています。デフォルトでは、属性値の長さが 900,000 バイトを超えると Web サービス コールは Axis エラーを返します。

以下のパラメータを deploy.wsdd ファイルに設定します。

fatal_max_string_length

Web サービス メソッドが受け付ける属性値の最大長を設定します。

デフォルト : 900,000 バイト

validate_parameters

属性値の長さのチェックを実行するかどうかを設定します。検証をオフにする場合は、このパラメータを 0 に設定します。

デフォルト：1（オン）

exception_methods

属性値の長さの検証から除外する Web サービス メソッドのカンマ区切りリストを表示します。

関連項目：

[Web サービスの再展開](#) (P. 662)

Web サービスの再展開

新しい環境設定は、CA SDM Web サービスを再展開すると有効になります。Web サービスを再展開するには、以下の手順に従います。

1. コマンドプロンプトを開き、CLASSPATH 環境変数に必須の Axis jar ファイルを組み込みます。必須の Axis jar ファイルは<NX_ROOT>/java/lib にあります。

たとえば、Windows で設定する場合は、以下のコマンドを実行します。

```
set AXISHOME=%NX_ROOT%\java\lib
set
classpath= %AXISHOME%\axis.jar;%AXISHOME%\jaxrpc.jar;%AXISHOME%\saa.jar;%AXISHOME%\commons-logging.jar;%AXISHOME%\commons-discovery.jar;%AXISHOME%\wsdl4j.jar;%AXISHOME%\log4j-1.2.8.jar;%classpath%;
```

2. ディレクトリを <NX_ROOT>/sdk/websvc/R11（GA バージョン 6.0 Web サービスの場合は、<NX_ROOT>/sdk/websvc/60）に変更し、以下のコマンドを実行します。

```
java org.apache.axis.client.AdminClient undeploy.wsdd
java org.apache.axis.client.AdminClient deploy.wsdd
```

3. CA SDM サービスをリサイクルして、Tomcat をリサイクルします。以下のコマンドを使用して Tomcat をリサイクルすると、CA SDM 全体のシャットダウンを回避できます。

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

Web サービスが再展開されます。

4. 以下のデフォルト URL の Axis サービス一覧ページを表示して、実際に Web サービスが展開されていることを確認します。

```
http://<servername>:<port>/axis/services
```

注: 実際の URL は、インストールの設定によって異なります。

Web サービスのセキュリティ

Web サービスを展開する際は、セキュリティに関する重要な考慮事項を理解しておく必要があります。HTTP を使用する場合、その初期設定にはセキュリティ上の脆弱性があります。つまり、Web サービス コール内の全情報は、HTTP プロトコルを使用してネットワーク上のクライアントとサーバ間を平文で送信されてしまいます。この情報には、チケットに関する説明や連絡先名などのアプリケーションデータだけでなく、Web サービスのセッション ID (SID) が含まれます。さらに、Web サービス アプリケーションで使用するログイン方法によってはパスワードも含まれます。

Web サービスを展開する管理者は、この情報を熟読して十分に理解し、アプリケーションおよびネットワークの両方のレベルで追加の設定手順を実行して、Web サービス環境を確実に保護するように努めてください。

重要: HTTP で使用するデフォルトの Web サービスには、セキュリティ上の脆弱性があるため、パスワードの漏洩、セッションの固定、データの盗み見などのセキュリティの脅威に曝されています。

Web サービスを展開するときは、以下に示す相互に関連した 3 つのセキュリティ事項について考慮する必要があります。

- 展開をサポートするために必要なアプリケーション レベルのアクセス認証スキーマ
- 展開に必要なネットワーク レベルの追加機能
- Web サービス設定オプションを使って、これらの要件を施行する方法

以下に、各セキュリティ機能について説明します。

- **Web サービス アプリケーション レベルの認証スキーマ** - Web サービスにアクセスするには、Web サービス クライアント アプリケーションが Web サービス アプリケーションで認証される必要があります。Web サービスのアクセス認証用に 2 種類のスキーマが用意されています。ユーザ名/パスワードによる認証と、パブリック キー インフラストラクチャ (PKI) テクノロジによる認証です。どちらの認証もアクセス ポリシーを使用して、Web サービスのアクセス コントロール/管理 コンポーネントと連動します。アクセス認証およびアクセス管理は、Web サービスで最も重要なセキュリティ機能です。

ユーザ名/パスワードによる認証は、以下のセキュリティ設定コマンドを使用して無効にできます。

```
disable_user_logon
```

管理者はこのオプションを有効にする前に、Web サービスにアクセスするために企業で使用する各 Web サービス クライアントが別の認証方法 (PKI ベースのログイン方法) を実際にサポートできるかどうかを確認する必要があります。PKI テクノロジの大きなメリットは、システム ユーザ アカウントの管理 (つまり、システム ユーザのパスワードの管理、保存、および送信) が Web サービス クライアント アプリケーションで不要である点です。

- **ネットワーク レベルのセキュリティ設定** - ユーザ名/パスワード認証およびパブリック キー インフラストラクチャ (PKI) 認証のどちらの認証スキーマでも、HTTP を使用する場合は、特定のログイン方法 (および続いて送受信されるすべての情報) から返されるセッション ID が平文で送受信されることに注意してください。さらに、ユーザ名/パスワード認証スキーマを使用している場合、パスワードは保護されない平文の状態で Web サービス クライアント アプリケーションから Web サービスへ送信されます。製品開発中は、W3C による Web サービス セキュリティの勧告基準はありませんでした。このため、これらの Web サービスの実装では、安全なコンテキストを提供する WS セキュリティが使用されません。代わりに、ポイントツーポイントトランスポートレイヤセキュリティ (SSL/TLS) や、ネットワークレベルのその他のセキュリティ方式 (IPSec など) を使用してネットワークを保護してください。こうしないと、アプリケーションレベルの認証交換、およびそれに続いて送受信されるセッション ID とデータが、すべて平文のまま送受信されます。

重要: Web サービスを展開するときは、SSL (または https) を使用して、アプリケーションレベルの認証交換、および続いて送受信されるセッション ID とデータを保護することをお勧めします。

- **Web サービス設定** - 管理者は次の 2 つのセキュリティ設定コマンドを使用して、Web サービス アプリケーション レベルで、プロトコル レベルのセキュリティを施行した通信を確立できます。

`require_secure_login`

このセキュリティ機能では、`Login()`および `LoginService()` メソッドのコールに SSL (`https`) を使用する必要があります。この機能は、他の Web サービスにかかる SSL のオーバーヘッドを回避すると同時に、ユーザ名およびパスワードを保護することにも役立ちます。

重要: `require_secure_login` コマンドを使用すると、Web サービス アプリケーションは、`Login()`および `LoginService()`以外のメソッドについて、通信でプロトコル レベルのセキュリティが施行されていることを確認しません。このため、他のセキュリティ対策が講じられていない場合、`Login()`および `LoginService()`以外の Web サービス メソッドは保護されない状態で呼び出されるため、セキュリティが非常に脆弱になります。

`require_secure_connection`

このセキュリティ機能では、Web サービスにアクセスするために SSL を使用する必要があります。`https` が必要であるにも関わらず使用されない場合は、SOAP Fault が `UDS_SECURE_CHANNEL_REQUIRED` コードと共に返されます。

注: SSL の設定方法の詳細については、J2EE サブレット コンテナのドキュメントを参照してください。

関連項目:

[外部仕様](#) (P. 671)

SOAP エラー処理

Web サービス メソッドにエラーが発生した場合、SOAP Fault が返されます。SOAP Fault は Web サービスで発生する例外情報を返すための標準的な方法です。

SOAP Fault メッセージには標準化された<Message>および<Code>エレメントが含まれますが、重要なほとんどの情報は<Detail>エレメントに記述されています。<Detail>エレメントには<ErrorCode>と<ErrorMessage>エレメントが含まれます。<ErrorCode>エレメントでは、CA SDM または ナレッジ マネジメント 製品に固有のエラー コードの列挙が返されます。<ErrorMessage>エレメントには、エラーを説明する英語の文字列が含まれています。<ErrorMessage>エレメントは開発者が使用するのに適した内容です。ユーザに対してはより適切なメッセージを表示する必要があります。

以下の例は、CA SDM の getObjectValues() メソッドに不正なパラメータが渡された場合の SOAP Fault です。

```
<soap:Fault>
  <faultcode>soap:Client</faultcode>
  <faultstring>Error on fetch with attribute
list:persistent_id,first_name,last_nameParamErrorHere</faultstring>
  <detail>
    <ErrorCode>1001</ErrorCode>
    <ErrorMessage> Error on fetch with attribute list:
persistent_id,first_name,last_nameParamErrorHere </ErrorMessage>
  </detail>
</soap:Fault>
```

Microsoft .NET の管理コードを使用して作成されたクライアントを使用している場合は、Web サービス メソッドのコールに失敗すると「SOAPException」例外が発生します。エラーが発生すると、呼び出された操作がキャンセルされます。

エラーがサーブレット コンテナによって書き込まれる場合は、サーブレット コンテナのログに表示されます。それ以外の場合、エラー情報は **CA SDM** のログに書き込まれます。これらのログは以下のサブディレクトリに配置されています。

- **CA SDM** インストールディレクトリ内の
/bopcfg/www/CATALINA_BASE/logs サブディレクトリ
- **CA SDM** インストールディレクトリ内の /log サブディレクトリ、およびプレフィックスが「**stdlog**」のすべてのログのサブディレクトリ

注: これらのログを定期的に監視することをお勧めします。サーバは、独自のエラーを **CA SDM Web** サービスに報告せずにログに記録してしまうことがあるためです。

ロック エラー

更新中の **CA SDM** のオブジェクトはロックされます。オブジェクトを更新するメソッド (**updateObject()** または **transfer()** など) は以下のロック エラーコードを返すことがあります。

UDS_LOCK_ERR

このコードは、別のユーザがレコードを更新していることを示します。多くの場合、**ErrorMessage** エレメントには、ロックしているユーザのハンドルが返されます。

タイムアウト

CA SDM サーバの負荷が高い場合は、メソッドの実行に時間がかかることがあります。まれに、個々のプロセスが応答に失敗したり、他のエラーが発生したことが原因となり、メソッドの実行結果がまったく返されないことがあります。必要以上に動作が停止することを避けるため、**Web** サービス メソッドは一定時間を過ぎるとタイムアウトになります。**Web** サービス メソッドのタイムアウトは **CA SDM** サーバのタイムアウトのことで、**Web** サーバやネットワークなどのタイムアウトではありません。

注: **J2EE** アプリケーション サーバがリサイクルされた後の初回アクセス時には、**Web** サービスに数秒の遅れが生じます。これは、アプリケーションが初期化中であつたり、**DLL** やライブラリなどをロード中であるためで、**Web** サービス メソッドの 1 回目のコール時のみ発生します。それ以降のコールでは、これよりも早く結果が返されます。

メソッドがタイムアウトになった場合、以下のエラー コードが返されます。

UDS_TIMEOUT_ERR

操作が中止されたわけではありません。サーバは、リクエストを受信した可能性があり、その場合、時間はかかりますが正常に処理されます。
doSelect() メソッドを使用して数千のレコードを取得する場合に、このタイプの問題が発生することがあります。

注: *doSelect* メソッドの詳細については、「CA SDM テクニカル リファレンス ガイド」を参照してください。

エラーコード

Web サービス コールで返される可能性のある SOAP Fault の<ErrorCode>値は以下のとおりです。

エラー名	値	説明
UDS_OK	0	正常。
UDS_FAILURE	1	一般エラー。システム ログを確認してください。
UDS_BAD_PARAM	1000	メソッドに不正なパラメータが渡されました。このエラーは、必要なパラメータが見つからない場合、渡されたタイプが正しくない場合、または無効な値が使用された場合に発生します。
UDS_INTERNAL_ERR	1001	内部エラーが発生したことを示します。返される配列とシステム ログに説明が記述されています。
UDS_LOCK_ERR	1002	別のユーザやプロセスがロックしているオブジェクトを更新しようとしてしました。通常、オブジェクトをロックしている連絡先の ID が戻りデータに返されます。

エラー名	値	説明
UDS_UPDATE_ERR	1003	オブジェクトの更新中にエラーが発生しました。必要な属性がすべて設定されていることを確認してから、システム ログを確認してください。
UDS_CREATION_ERR	1004	オブジェクトの作成中にエラーが発生しました。必要な属性がすべて設定されていることを確認してから、システム ログを確認してください。
UDS_NOT_FOUND	1005	検索メソッドによって一致項目、または指定オブジェクトが見つかりませんでした。不正または無効なハンドルがメソッドに渡された場合に発生します。
UDS_SESSION_TIMEOUT	1006	実行しているメソッドがタイムアウトになりました。 CA SDM サーバの負荷が高い、またはメソッドが不正です。
UDS_SERVER_GONE	1007	CA SDM サーバ接続が切断されました。UDS メソッドが機能しなくなり、リスト参照が失われます。
UDS_FETCH_ERR	1008	リスト データの取得中にエラーが発生しました。
UDS_BAD_SESSION	1010	無効な SID が使用されました。
UDS_CNTXT_TIMEOUT	1011	SID がタイムアウトになりました。
UDS_SECURE_CHANNEL_REQUIRED	1012	Web サービス（または Web サービス メソッド）にアクセスするにはセキュリティで保護されたチャネル（ SSL など）が必要ですが、保護されていないチャネルを使用しようとしています。
UDS_SECURITY_VIOLATION	1013	試行した操作は CA SDM セキュリティに違反するため中止されました。
UDS_OVER_POLICY_LIMIT	3002	試行したリクエストはポリシーに定義された制限を越えるため拒否されました。

Web サービスのインストール

設定タイプに応じて、CA SDM は、以下のサーバに Web サービスをインストールします。

- 標準：プライマリ サーバとセカンダリ サーバの両方。Web サービスクライアントがセカンダリ サーバ上で URL を使用できるようにするには、セカンダリ サーバに Web エンジンを追加します。
- 高可用性：アプリケーション サーバ

Web サービスは、CA SDM サーバにインストールされているデフォルトのオブジェクト マネージャを使用します。ほかのオブジェクト マネージャを使用するには、オブジェクト マネージャの `webservice_domsrvr` オプションをインストールして設定します。

注: オブジェクト マネージャ、WebDirector、および Web エンジンの追加と設定については、「[管理ガイド](#)」を参照してください。

`webservice_domsrvr` オプションのインストールおよび設定については、[オンラインヘルプ](#)を参照してください。

設計時の機能をアクティブにする方法

CA SDM Web サービスには、Java バージョンの開発者向けにメソッドスタブ設定機能が用意されています。この機能を有効にすると、Web サービスは CA SDM サーバを無視してメソッドコールの擬似データを返します。このようにして、CA SDM サーバを動作させずに Web サービス コールを実行できます。

次の手順に従ってください:

1. `deploy.wsdd` を編集して、「`design_mode_stubs`」のセクションのコメント化を解除します。
2. サーバの展開を解除してから再展開します。
3. アプリケーション サーバを再起動します。

設計時の機能がアクティブになります。

注: 設計時の機能は CA SDM Web サービス メソッドのみに適用されます。

外部仕様

CA SDM を使用して、ユーザ アクセス認証の指定、およびアクセス コントロール/管理で利用できる機能の指定が可能です。

ユーザ アクセス認証

CA SDM Web サービスでは、2 種類のアクセス認証スキーマが用意されています。これらは、新しいアクセス コントロール、およびアクセス ポリシーを使用する管理機能に関連付けられています。

ユーザ名/パスワード

本製品の以前のリリースで説明されているように、ユーザ名およびパスワードを確認します。

パブリック キー インフラストラクチャ(PKI)テクノロジー

アクセスをリクエストしているユーザがプライベート キーの所有者であるかを確認します。

重要: 本バージョンの CA SDM Web サービスにアクセスするアプリケーションを使用する場合、まず初めにコード値を入力して CA SDM の Web サービス アクセス ポリシーを定義することをお勧めします。CA SDM のインストールおよび設定時には、デフォルトのアクセス ポリシーとしてコード「DEFAULT」が設定されています。

関連項目:

[アクセス ポリシーの定義 \(P. 682\)](#)

ユーザ名/パスワード認証

ユーザ名/パスワード認証を使用する場合、ユーザのアプリケーションは以下のいずれかの **Web** サービス メソッドを呼び出して **CA SDM Web** サービスにアクセスする必要があります。

注: ユーザ名パラメータで指定したログインユーザ (ポリシーで指定した代理連絡先ではありません) はセッション中に開始されたアクティビティに責任を持つことになります。ログインユーザには、すべてのファンクショングループセキュリティおよびデータパーティションが適用されます。

login (Username, Password)

このメソッドは下位互換性を維持するために用意されています。指定したユーザ名およびパスワードによってアクセス認証が実行されます。SID (セッション ID) はアクセスが認証された場合のみ返されます。これ以降の **Web** サービス コールすべてにこの SID が必要です。この SID が指定されている **Web** サービス アクセスすべてにアクセス ポリシーのデフォルトが適用されます。

Username および **Password** は必須フィールドで、平文で指定する必要があります。

loginService (Username, Password, Policy)

このメソッドは前述の **login** メソッドと同様にユーザ名とパスワードによってアクセス認証が行います。SID はアクセスが認証された場合のみ返されます。3 番目のパラメータに特定のアクセス ポリシーを指定して、これ以降の **Web** サービスすべてのアクセスを制御/管理できます。ポリシー パラメータが空の場合は、自動的にポリシーのデフォルトが適用されます。

Username および **Password** は必須フィールドで、平文で指定する必要があります。**Policy** も必須フィールドで、平文で指定する必要がありますが、空のままでも構いません。ポリシーで定義したポリシー コードを使用します。

ログインの検証方法は連絡先に割り当てられたアクセス タイプによって異なります。アクセス タイプ オブジェクトは **CA SDM** でホストされ、検証タイプを設定します。製品を使用して、アクセス タイプ レコードを表示できます。また、**getAccessTypeForContact()** Web メソッドを使用して、あらゆるアクセス タイプ オブジェクト情報を取得できます。

注: アクセス タイプの詳細については、「管理ガイド」を参照してください。

パブリック キー インフラストラクチャ(PKI) 認証

PKI 認証を使用する場合、ログイン リクエストの情報はプライベート キーで暗号化されます。この情報は、対応するパブリック キーのみで復号化できます。ログイン リクエストの応答は平文で返されます。

通常、**CA SDM Web** サービスにアクセスするアプリケーションにはポリシーが割り当てられます。**CA SDM Web** サービスは、デジタル証明書のパブリック キーと共にポリシーの詳細情報を格納します。アプリケーションはポリシー所有者として、デジタル証明書のプライベート キーとポリシー コード (ポリシー識別子) を使用してログイン リクエストを構築します。

loginServiceManaged (Policy, Encrypted_Policy)

CA SDM Web サービスのユーザ認証は次のように行われます。平文のポリシーコードを使用してポリシーを検索し、ポリシーに関連付けられたポリシー所有者のパブリックキーを取得します。次に暗号化されたポリシーコードを復号化し、復号化された情報をポリシーコードと照合してから、バックエンドサーバでセッションを開きます。平文のセッション ID (SID) が返され、以降のメソッド呼び出しで使用できます。ポリシーに関連付けられたパブリックキー (CA SDM に保管) に対応するプライベートキーは、ポリシー所有者のみが所有しています。

これ以降の Web サービス コールには、返されたセッション ID (SID) が必要です。ポリシーで指定した代理連絡先は、このセッション中の Web サービス アクティビティすべてに責任を持つことになります。この代理連絡先には、すべてのファンクショングループセキュリティおよびデータパーティションが適用されます。

重要: `Encrypted_Policy` パラメータは **BASE64** テキスト形式である必要があります。ユーザアプリケーションでは、バイナリ形式から **BASE64** テキスト形式への変換を正しく行う必要があります。

`Policy` は必須フィールドです。定義するときは、ポリシーに定義されている平文のポリシーコードを使用します。`Encrypted_Policy` (ポリシー所有者のプライベートキーで暗号化されたポリシーコードのデジタルシグネチャ) が必要です。`Encrypted_Policy` を定義するときは、ダイジェストアルゴリズム (SHA1)、および暗号化アルゴリズム (RSA) を使用します。

Java での loginServiceManaged の実装

以下では、証明書を生成し、それを使用して CA SDM Web サービスにアクセスする方法について説明します。

以下の例では、CA SDM 証明書を使用してログインを行い、2 つの Web サービス コールを実行します。`getBopsid()` Web サービス メソッドコールは、特定のユーザにリンクされているトークンを取得できます。このトークンを使用すると、パスワードを要求されることなく、リンクされたユーザとして CA SDM Web インターフェースにログインすることができます。これにより、異なるアプリケーション間のシームレスな統合が可能になります。

重要: 生成された BOPSID トークンは 30 秒後に無効になるため、すぐに使用してください。

重要: バージョン 1.4 の AXIS ツールの使用には既知の問題があります。詳細については、リリース ノートを参照してください。

次の手順に従ってください:

1. AXIS ツール WSDL2Java を使用してスタブ クラスを生成します。詳細については、PKI_loginServiceManaged_JAVA_steps ファイルの「AXIS Tool WSDL2Java によるスタブ クラスの生成」を参照してください。このファイルは、以下の場所にあります。

```
$NX_ROOT/samples/sdk/websvc/java/test1_pki
```

2. CA SDM サービスを起動します。
3. pdm_pki -p DEFAULT を実行します。

DEFAULT.p12 は現在のディレクトリに作成されます。このポリシーでは、パスワードはポリシー名と同じです（この場合は DEFAULT）。

注: このコマンドによって、証明書のパブリック キーも sapolicy テーブル/オブジェクトの pub_key フィールド（public_key 属性）に追加されます。

4. CA SDM にログインします。
5. [管理] タブで、[SOAP Web サービス ポリシー] - [ポリシー] を選択します。

[SOAP Web サービスのアクセス ポリシー リスト] ページが開きます。

6. [デフォルト] をクリックします。

[SOAP Web サービスのアクセス ポリシー詳細] ページが開きます。

7. [代理連絡先] フィールド（この例では ServiceDesk）を入力し、DEFAULT ポリシー レコードの [キーを所有] フィールドに [はい] が表示されていることを確認します。

8. DEFAULT.p12（コマンド pdm_pki が実行されるディレクトリから）、pkilogin.jsp という名前の JSP ファイル、および pkilogin.htm という名前の HTML ファイル（\$NX_ROOT/samples/sdk/websvc/java/test1_pki ディレクトリから）を以下のディレクトリにコピーします。

```
$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/axis
```

9. Axis ディレクトリにある HTML フォームを開きます。たとえば、
`http://localhost:8080/axis/pkilogin.htm`

適切なフィールドに入力します。

注: [ディレクトリ] フィールドは証明書ファイルの場所を示します。
パスを変更して正しい場所を反映します。

10. [Log me in!] をクリックします。

結果のページが表示されます。

11. BOPSID の URL をクリックします。

重要: この URL をすぐにクリックしてください。BOPSID のトークンは
約 30 秒で無効になります。

BOPSID を使用する URL のフォーマットは、以下のとおりです。

`http://<server name>:<port>/CAisd/pdmweb.exe?BOPSID=<BOPSID value>`

注: AIX 上で実行している Java クライアントプログラムに対して
`loginServiceManaged` メソッドを使用するには、`JAVA_HOME` にあるセキュ
リティ ポリシー ファイルセットに置き換える必要がある場合があります。
<http://www.ibm.com> にアクセスして、「developerworks java technology
security information AIX」で検索を行います。「developerWorks : Java
technology : Security」ドキュメントで、「IBM SDK Policy files」へのリンク
をたどります。制約のないポリシー ファイル (`local_policy.jar` と
`US_export_policy.jar`) をダウンロードします。`JAVA_HOME/lib/security` ディ
レクトリ内の元のファイルを、これらのファイルに置き換えます。

PKI 認証タイプの設定

PKI 認証を設定するには、まずアクセス ポリシーを作成する必要があります。プロセス フローは以下のとおりです。

アクセス ポリシーの作成

このタスクは、製品（Web インターフェースのみ）を使用して管理者が行います。各アクセス ポリシーには固有のテキスト コードを割り当てる必要があります。

パブリック キー/プライベート キー ペアと共にデジタル証明書を取得して、アクセス ポリシーに関連付ける

PKI アクセス認証の場合、ユーザ アプリケーションはパブリック キーとプライベート キーの両方が含まれるデジタル証明書を取得する必要があります。管理者はサードパーティの認証局（CA）、またはデジタル証明書をサポートするセキュリティ製品を利用してデジタル証明書を取得することができます。CA SDM では、サーバサイドユーティリティを使用してデジタル証明書を生成することもできます。このユーティリティは<NX_ROOT>/bin ディレクトリに配置されています。書式は以下のとおりです。

```
pdm_pki -p policy_code [-l certificate file] [-f] [-h]
```

-p

一意のポリシー コードを示します。

-f

ユーティリティが新しい公開鍵で既存の公開鍵を置き換えられるようにします。

-l

X509 V3 証明書に格納された公開鍵をロードします。

-h

コマンドライン ウィンドウにヘルプを表示します。

サードパーティ、CA Technologies、またはセキュリティ製品を利用してデジタル証明書を取得する場合は、CA SDM サーバと同じディレクトリにインポートしてからアクセス ポリシーに関連付けます。ユーザアプリケーションの管理者は、DER/ASN.1 フォーマットの X509 V3 証明書が含まれるデジタル証明書ファイルを取得する必要があります。

また、証明書にはパブリック キー/プライベート キー ペアのパブリック キーのみが含まれている必要があります。管理者は `-l` オプションを使用して、`pdm_pki` ユーティリティを呼び出し、証明書をロードします。ユーティリティにより、証明書のロード、パブリック キーの抽出、パブリック キーの BASE64 テキスト形式への変換が行われ、ポリシー コードで指定したアクセス ポリシーと共に保存されます。

`pdm_pki` ユーティリティによってデジタル証明書が生成されてから、管理者は CA SDM で、`-l` オプションを使わずにコマンドを呼び出します。すると、ユーティリティによってパブリック キー/プライベート キー ペア (RSA1024 ビット キー) が生成されます。パブリック キーは BASE64 テキスト形式に変換され、ポリシー コードで指定されているアクセス ポリシーと共に保存されます。X509 V3 証明書も作成され、パブリック キーと共にほかの情報も保持されます (パス フェーズの初期設定はポリシー コード)。最後に、X509 V3 証明書がプライベート キーと共に PKCS12 形式の標準証明書としてパッケージ化されます。その後、`policy_code.p12` というファイル名で保存されます。ファイル名はポリシー コードによって異なります。このファイルはクライアントにエクスポートできます。

注: アクセス ポリシーがすでに証明書のパブリック キーに関連付けられている場合、`pdm_pki` コマンドをコールする際に `-f` オプションを指定して、既存のパブリック キーを新しいパブリック キーで上書きする必要があります。

関連項目:

[アクセス ポリシーの定義 \(P. 682\)](#)

Web サービスへのログイン

PKI 認証が設定された Web サービスへのログイン プロセス フローは以下のとおりです。

プロセス	説明
電子証明書のロードおよび プライベート キーの抽出	デジタル証明書はユーザ側の安全なストレージに保存する必要があります。Web サービスへのログイン時にはこれが取得されて使用されます。 安全なストレージの例は以下のとおりです。 ■ Windows 証明書ストア ■ Java 証明書ストア (java_keytool ユーティリティで管理) ■ 証明書ストア (その他の CA Technologies セキュリティ製品によって作成)。 ユーザアプリケーションはユーザ環境に応じて、適切な API で電子証明書のロード、およびプライベート キーの抽出を行う必要があります。
プライベート キーによる 平文のポリシー コードのデジタル シグネチャの 作成	デジタル証明書から抽出されたプライベート キーは、ポリシー コードのデジタル シグネチャの生成に使用されます。デジタル シグネチャを作成すると、プライベート キーを使用してテキストのダイジェストが暗号化されます。ダイジェスト アルゴリズムは SHA1 の標準形式、暗号化アルゴリズムは RSA の標準形式を使用する必要があります。また、Web サービスにログインする前にバイナリ形式のデジタル シグネチャを BASE64 テキスト形式に変換する必要があります。 この情報をアーカイブするには、ユーザ環境に応じて適切な API をコールする必要があります。

プロセス	説明
Web サービス コールの呼び出し	ユーザアプリケーションは、平文のポリシー コードおよびポリシー コードの BASE64 テキスト形式のデジタル シグネチャを指定して、Web サービスの loginServiceManaged() メソッドを呼び出す必要があります。
返される SID の取得	アクセス リクエストが認証されると、平文の SID が自動的に返されます。

SID が生成されると、Web サービス セッションとアクセス ポリシーが正常に結び付けられます。ユーザアプリケーションはこの **SID** を使用してほかの Web サービス メソッドを呼び出すことができます。また、Web サービスへのアクセスはすべてこのアクセス ポリシーによって制御、および管理されます。

セッションおよび権限

ログイン時にユーザ名を指定したか、またはポリシーで代理連絡先を指定したかに関わらず、ログインが正常に検証されると、検証されたユーザ名に関連付けられた **SID** が返されます。このプロセスにより、各 **CA SDM** ユーザに適切なセキュリティ権限を割り当てて Web サービス アプリケーションを実行させることができます。

たとえば、表示可能なリクエストを制限するデータ パーティションを特定のユーザに割り当てることができます。ユーザがリクエスト情報を取得するときに **SID** を使用すると、**CA SDM** システムはデータ パーティションを使用します。

ファンクション グループ セキュリティも適用されます。たとえば、ユーザがコール マネージャ ファンクション グループにアクセスできないようにできます。これにより、コール マネージャ ファンクション グループへのアクセスが拒否されるので、リクエストの表示や作成などの Web サービス メソッドの呼び出しができなくなります。

アプリケーションがユーザの作業を終了するときは、**Logout()** メソッドをコールして **SID** を無効にします。

非アクティブな状態が一定時間経過すると、**SID** は有効期限切れになります。すなわち、**SID** はメソッドのコール間隔が一定のタイムアウト値を超えると期限切れになります。タイムアウト間隔はオプション マネージャで以下の **CA SDM** オプションを指定して設定します。

```
'webservice_session_timeout'
```

この値を **0** に設定した場合、**SID** はタイムアウトしません。このオプションが設定されていない場合は、デフォルトの **1** 時間に設定されます。**Web** サービス メソッドが有効期限切れの **SID** でコールされると、エラー コードと共にエラーが返されます。**1** 回目のエラー コードは **UDS_SESSION_TIMEOUT**、以降は **UDS_BAD_SESSION** となります。

SID をアクティブにしておくには、タイムアウトになる前に何らかの **Web** サービス メソッドをコールします。サーバを動作させずに **SID** をアクティブにしておくには、**serverStatus()**をコールします。

アクセス コントロール/管理

Web サービス チケットのフラッディングの問題を最小限に抑え、**CA SDM** サーバを安定稼働させるために、このバージョンの **CA SDM Web** サービスでは、アクセス コントロール/管理システムが採用されています。このシステムでは、信頼できるユーザ アプリケーションによって開始されたプログラム エラーや例外を発生させる可能性のある大量のサービス アクティビティを主に処理します。また、**CA SDM Web** サービスへの悪意あるユーザからのアクセスを制御する防壁としても機能します。**Web** サービス アプリケーションの管理者は、**CA SDM** でアクセス ポリシーを作成し、定義することができます。このポリシーにより、**Web** サービス アプリケーションからの **CA SDM Web** サービスへのアクセスを制御します。

注: デフォルトのアクセス ポリシーとしてコード「**DEFAULT**」が設定されています。この初期設定には、アクセス権限の制限はなく、ユーザ名/パスワード認証のセッションにのみ適用されます。

アクセス ポリシーの定義

SOAP Web サービス アクセス ポリシーを作成するには、管理者はアクセス ポリシーを定義する必要があります。

アクセス ポリシーを定義する方法

1. [管理] タブをクリックします。
2. 左側のツリーで、[SOAP Web サービス ポリシー] - [ポリシー] をクリックします。
[SOAP Web サービスのアクセス ポリシー 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。
[SOAP Web サービスのアクセス ポリシーの新規作成] ダイアログ ボックスが表示されます。
4. 新しいアクセス ポリシーの情報を入力します。

注: 操作数のデフォルト値が **-1** の場合、その操作数に制限はありません。値が **0** (ゼロ) の場合、その操作は許可されません。

シンボル

(必須) アクセス ポリシーのシンボル名を示します。

コード

(必須) このアクセス ポリシーを特定する一意のテキストを示します。

ステータス

(必須) アクセス ポリシーのステータスを示します。非アクティブなポリシーは使用されません。

代理連絡先

すべての Web サービス操作および CA SDM セキュリティで使用する連絡先を示します。

デフォルト

ポリシーのデフォルトを示します。このポリシーをデフォルトのポリシーに設定します。アクティブなデフォルト ポリシーは 1 つだけです。デフォルト ポリシーを作成すると、現在デフォルトに設定されているポリシーは自動的にデフォルトではなくなります。

キーを所有

(読み取り専用) パブリック キーがこのポリシーに関連付けられているかどうかを示します。このフィールドは、`pdm_pki` ユーティリティでパブリック キーがポリシーに関連付けられると更新されます。

代理を許可

代理権限を許可するかどうかを示します。このフィールドを設定すると、ポリシー所有者は `impersonate()` Web サービス メソッドを呼び出して代理ユーザの名前で Web サービス セッションを作成できます。セッションが作成されるときに、再度アクセス認証が行われることはありません。ただし、このメソッドを正常にコールできるのは、ユーザの新しいアクセス タイプの `access_level` が、ユーザのプロキシ アクセス タイプの `grant_level` 以下の場合のみです。

説明

このアクセス ポリシーの詳細説明を示します。

チケットの作成

1 時間あたりの実行可能なチケット (コール リクエスト、変更要求、案件) 挿入操作数を示します。

オブジェクトの作成

1 時間あたりの実行可能な CA SDM オブジェクト (チケット オブジェクト以外) 挿入操作数を示します。

オブジェクトの更新

1 時間あたりの実行可能な CA SDM オブジェクト更新操作数を示します。

添付ファイル

1 時間あたりの実行可能な添付ファイル関連の操作数を示します。

データのクエリ

1 時間あたりの実行可能なデータのクエリ操作数を示します。

ナレッジ

1 時間あたりの実行可能な knowledge 関連の操作数を示します。

5. [保存] をクリックします。

SOAP Web サービス ポリシーが定義されます。

カテゴリ別 Web サービス メソッド

CA SDM Web サービスの各メソッドは、特定のカテゴリに属します。各カテゴリとそのカテゴリに属するメソッドの一覧は以下のとおりです。

チケットの作成

- createTicket()
- createQuickTicket()
- createRequest()
- createChangeOrder()
- createIssue()

オブジェクトの作成

- logComment()
- createAsset()
- addAssetLog()
- createAssetParentChildRelationship()
- createObject()
- createWorkFlowTask()
- createActivityLog()
- notifyContacts()
- addBookmark()
- addComment()
- createFolder()

オブジェクトの更新

- addMemberToGroup()
- removeMemberFromGroup()
- closeTicket()
- createLrelRelationships()
- removeLrelRelationships()
- deleteWorkFlowTask()
- updateObject()
- transfer()

- escalate()
- attachChangeToRequest()
- detachChangeFromRequest()
- changeStatus()
- clearNotification()
- updateLrel()
- deleteBookmark()
- updateRating()

添付ファイル

- createAttmnt()
- createAttachment()
- attachURLLink()
- deleteAttmnt()
- deleteComment()
- removeAttachment()

データのクエリ

- impersonate()
- serverStatus()
- getBopsid()
- getConfigurationMode()
- getHandleForUserId()
- getAccessTypeForContact()
- getPermissionsGroup
- getObjectTypeInfoInformation()
- getRelatedList()
- getRelatedListValues()
- getGroupMemberListValues()
- getPendingChangeTasksForContact()
- getPendingIssueTasksForContact()
- getWorkFlowTemplates()

- `getWorkflowTemplateList()`
- `getTasksListValues()`
- `getNotificationsForContact()`
- `getPolicyInfo()`
- `getAssetExtensionInformation()`
- `getLrelValues()`
- `getObjectValues()`
- `doSelect()`
- `doQuery()`
- `getPropertyInfoForCategory()`
- `getValidTaskTransitions()`
- `getListValues()`
- `getListInfo()`
- `findContact()`
- `getAttmntInfo()`
- `getAttmntList()`
- `getBookmarks()`
- `getCategory()`
- `getComments()`
- `getContact()`
- `getDecisionTrees()`
- `getDocument()`
- `getDocumentTypes()`
- `getFolderInfo()`
- `getFolderList()`
- `getLrelLength()`
- `getPriorities()`
- `getRepositoryInfo()`
- `getStatuses()`
- `getTemplateList()`

ナレッジ

- createDocument()
- deleteDocument()
- doSelectKD()
- faq()
- attmntFolderLinkCount()
- getAttmntListPerKD()
- isAttmntLinkedKD()
- getDocumentByIDs()
- getKDListPerAttmnt()
- getQuestionsAsked()
- modifyDocument()
- rateDocument()
- search()

アクセス ポリシーが CA SDM によって更新されると、Web サービスは対応するポリシーの情報を動的に更新します。このポリシーによって制御されているアクティブな Web サービス セッションは、ポリシーの設定に従って引き続き制御されます。このポリシーで管理/制御される新規 Web サービス セッションは、最新の設定が使用されます。

注: 各メソッドの詳細については、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。

エラー タイプの定義

エラー タイプはチケット作成時に割り当てられます。また、アクセス ポリシーによって定義されます。CA SDM Web サービスのユーザ アプリケーションは、低レベルの Web メソッドを使用してチケット（リクエスト、変更要求、案件）を作成できます。この場合、エラー タイプを指定してチケットの問題を分類します。エラー タイプは高レベル メソッド `createTicket()` のみ使用できます。`createRequest()` などの低レベル メソッドではエラー タイプを使用しません。

関連項目:

[簡易 Web サービス アクセス \(P. 691\)](#)

Web サービスのエラー タイプ

CA SDM Web サービスでは、エラー タイプ定義セットを標準装備しています。これらはすべてのポリシーに作成することができます。「内部」エラー タイプとして指定されたこれらのデフォルト タイプは無効にできますが、削除することはできません。本製品では、[Web サービスのアクセス ポリシーの詳細] ページを使用して、新規ポリシーの作成時に設定されたデフォルトのエラー タイプを確認できます。

以下は、各内部エラー タイプについて説明しています。

ACCESS_ERROR

システムがリソース（ファイル、Web サイトなど）への接続、または検索に失敗したことを示します。

EXCEPTION_FATAL

アプリケーションの予期しないシャットダウンを示します。

EXCEPTION_RUNTIME

アプリケーション コードの実行中に例外が発生したことを示します。

LOGIN_ERROR

オペレータがアプリケーションへのアクセスに失敗したことを示します。

追加のエラー タイプ

アクセス ポリシーの管理者は、以下に示されているエラー タイプを追加することができます。

エラー タイプ	説明
チケット テンプレート	インシデント、エラー、案件、変更要求のテンプレートを示します。エラー タイプがレポートされた場合に、チケットを作成するために使用します。 注: 所有ポリシーの連絡先はエンド ユーザとして扱われます。 チケット タイプとチケット テンプレート名によってチケット テンプレートが定義されます。
デフォルト	このエラー タイプがポリシーのデフォルトであるかどうかを示します。1 ポリシーにつき設定できる問題タイプの初期設定は1つだけです。 注: ポリシーに関連付けられている既存のデフォルトエラー タイプは、新しいデフォルトエラー タイプで上書きされます。
アクティブ	アクティブなエラー タイプを表します。 注: 非アクティブなタイプはチケットを作成しません。
Internal	フィールドが読み取り専用であることを示します。これは、デフォルトの内部エラー タイプであるかどうかを表します。
シンボル	エラー タイプのシンボル名を示します。
コード	エラー タイプを特定する固有テキストを示します。
説明	エラー タイプの詳細な説明です。
重複処理	本製品によって同一チケットがすでに存在することが検出された場合のアクションを定義します

エラー タイプ	説明
戻りデータ	クライアント アプリケーションに返すために、Web メソッド「createTicket()」に指定するユーザ定義メッセージを示します。戻りデータは、アプリケーションのアクション(アプリケーションデータの戻り値)、またはエンドユーザに対して表示するメッセージ(ユーザデータの戻り値)を示すために使用できます。

関連項目:

[重複チケット処理](#) (P. 690)

重複チケット処理

Web サービス アクセス ポリシーは重複チケットを検出して処理できるので、チケットフラッド防止に役立ちます。以下の条件がすべて当てはまる場合、作成されたチケットが重複している可能性があります。

- すでに同じタイプ (cr、iss、chg) のチケットが少なくとも 1 つ存在し、かつアクティブである。
- 既存チケットが Web サービスによって作成された。
- 作成されるチケットと既存チケットのポリシーおよびエラー タイプが同じである。
- 既存チケットの「作成日」が、指定されたしきい値内である（オープン期間が 2 日未満である場合など）。

注: 作成日のフィールドは、重複データ検索の最大時間間隔を使用して設定されます。

- 重複 ID は、createTicket() メソッドを呼び出すときにユーザが指定した ID と一致します。

ユーザ自身が確認できる基準に基づいて、チケットが一意になるように分類することで重複を避けることができます。そのためには、createTicket Web サービス コールに任意の文字列パラメータを追加します。重複処理が有効な場合、他の重複処理基準が一致した後にこの文字列パラメータが調査され、このコールがこのメソッドに対して一意であるか、または重複するかが確定されます。

重複チケットの結果

チケット作成アクションの結果チケットが重複すると判断された場合、既存のエラー タイプを設定して以下のいずれかの動作を実行できます。

エラー タイプの再設定	結果
新規チケットを作成して重複を無視	新規チケットのハンドルと番号が返されます（デフォルト）。
新規チケットを作成せず、既存の重複チケットにアクティビティ ログを追加	チケットのハンドルと既存のチケット番号が返されます。
新規チケットを作成せず、代わりに CA SDM 標準 ログにエントリを追加	チケットのハンドルと既存のチケット番号が返されます。
新規チケットを作成し、重複チケットの子として添付	新規チケットのハンドルと番号が返されます。

簡易 Web サービス アクセス

CA SDM Web サービスには、既存の Web サービス メソッドの簡易バージョンである、簡略化された高レベルの Web サービス メソッドが用意されています。ほとんどのユーザアプリケーションは、CA SDM Web サービスのサービスを受ける前に数多くの Web サービス メソッド一式すべてを使用する必要はありません。ユーザ定義のアクセス ポリシー、およびポリシーで定義されたデフォルトのパラメータを使用すれば、CA SDM オブジェクトスキーマについてほとんど知らなくても、この高レベルの Web サービス メソッドを利用できます。また、これらの高度なメソッドにはサービスアウェアアプリケーションに必要な CA SDM の共通機能がほとんど含まれています。

この高レベルの Web サービス メソッドの使用法は以下のとおりです。

createTicket (SID, Description, Error_Type, Userid, Asset, DuplicationID)

このメソッドを使用するには、レポートされたエラーのエラー タイプを指定する必要があります。エラー タイプには作成するチケットに適したチケットテンプレートが必要です。また、チケットが重複した場合に実行されるアクションの定義、データ出力の指定、およびユーザアプリケーション用に定義されているアクセス ポリシーへの関連付けが必要です。

このメソッドが呼び出されると、**CA SDM Web** サービスにより、チケットの作成に必要な現在のアクセス ポリシーとエラー タイプが検索されます。**CA SDM Web** サービスが適切なエラー タイプの検索に使用する手順は以下のとおりです。

- 特定のエラー タイプ コードが入力され、ポリシーに関連付けられているエラー タイプと一致する場合、このエラー タイプが内部であるかどうかにかかわらず使用します。
- エラー タイプが指定されていない、または上記の手順でエラー タイプが見つからなかった場合、ポリシーに定義されているデフォルトのエラー タイプを使用。
- デフォルトのエラー タイプがポリシーに定義されていない、または上記の手順でエラー タイプが見つからなかった場合、定義されている内部エラー タイプを使用。

エラー タイプが定義されると、**CA SDM Web** サービスはそのタイプを使用してチケットを作成します。**Userid** が空で、アセット情報がチケットに追加される場合（入力が空でない場合）、アクセス ポリシーで定義された代理連絡先ユーザがチケットの作成に使用されます。チケットが作成されると、**CA SDM Web** サービスはエラー タイプで指定されているように、ユーザ データとアプリケーション データの両方を返します。

closeTicket (SID, Description, TicketHandle)

ユーザはこの関数をコールして、オープン チケットをクローズすることができます。この関数はオープン チケットのステータスを「クローズ」に設定し、アクティビティ ログに入力の説明を追加します。

logComment (SID, TicketHandle, Comment, Internal_Flag)

オープン チケットのアクティビティ ログに入力コメントのエントリを追加します。

getPolicyInfo (SID)

現在の **Web** サービス セッションを制御するポリシー情報を取得します。この情報でユーザ アプリケーション用のサーバ容量を知ることができます。容量にあわせて **Web** サービス コールを調整することをお勧めします。

これらの簡易 **Web** サービス API を使用できるので、ユーザは時間を割いてすべての **Web** サービス API と **CA SDM** スキーマを理解する必要はありません。簡易 **Web** サービス API はサービス アウェア アプリケーションを実現するプロセスを簡略化し、加速します。

オブジェクト

CA SDM では、各エンティティ（連絡先、案件など）をオブジェクトとして扱います。この高レベルのオブジェクトは、CA SDM サーバ上の以下のディレクトリにある **majic** (.maj) および **mod** (.mod) ファイルで定義されています。

`/bopcfg/majic`

カスタマイズしたオブジェクトは以下のディレクトリにあるファイルで定義されています。

`/site/mods/majic`

実質的に、オブジェクトはデータベース テーブルを包含する高レベルのラッパです。

オブジェクトはタイプ（ファクトリと呼ぶ場合もあります）によって定義されます。たとえば、リクエストオブジェクトは「**cr**」タイプです。各オブジェクトのタイプは、**majic** ファイルの「**OBJECT**」宣言で定義します。

注: CA SDM に標準で装備されているオブジェクトはすべて「CA SDM テクニカル リファレンス ガイド」に掲載されています。

オブジェクトには**属性**があり、これはデータベース テーブルで必須の列です（XML 属性とは異なります）。Web サービスの豊富なメソッドを使って属性値を取得することができます。ほとんどのメソッドを使用するには、属性の設定や値の取得をするために属性名が必要となります。属性名には、オブジェクト定義用の **majic** または **mod** ファイルで割り当てられている名前を使用します。属性名は実際のデータベースでの名前と異なる場合があります。属性は必要に応じてクライアント サイトで追加することができます。

注: 各オブジェクトのすべての属性の一覧については、「CA SDM テクニカル リファレンス ガイド」を参照してください。

Web サービスでは、ハンドルによってオブジェクトを一意に特定します。ハンドルは **objectType:ID** 形式の文字列値です。ここで **objectType** はオブジェクトタイプ（ファクトリ）名、ID は固有の値です。ID の値は CA SDM オブジェクトが必ず持つ「id」属性と一致します。ほとんどの場合、DBMS で「id」属性に対してインデックスが作成されるので、オブジェクトハンドルの一部である ID は、有効なクエリを作成するのに役立ちます。各オブジェクトはそのタイプに関わらず、「persistent_id」というオブジェクト属性に ID 値を格納します。

注: 以前のリリースでは、ハンドルの ID 部分は常に整数で表していました。Unicenter Service Desk r11.0 以降では、ID 部分を UUID の文字列表現（通常 32 文字）で表すこともできます。

UUID を使用するエンティティのオブジェクト名およびファクトリ名は以下のとおりです。

オブジェクト名	ファクトリ名
連絡先	cnt
アセット	nr
組織	org
ロケーション	loc
会社/ベンダー	ca_cmpny
モデル	mfrmod

ハンドルは**固定要素**です。つまり、特定のオブジェクトを表すハンドルは常に固有の値を持ち、データベースのマイグレーションが行われても変わりません。クライアントでは、ステータスや連絡先タイプなどの静的なオブジェクトを扱う際にこの固定性を利用することができます。

オブジェクトハンドルは CA SDM Web サービスを活用するための重要なポイントです。多くのメソッド、特にデータを更新するメソッドにはハンドルが必要です。オブジェクトデータを返すほとんどのメソッドにもオブジェクトハンドルを指定します。

システムの更新とキャッシュ

Web サービスはオブジェクト タイプ情報をキャッシュします。タイプ情報は、初めてタイプが参照されたときにキャッシュされ、応答に少し遅れが生じます。

サーバの応答やキャッシュの遅延を避けるために、予備のクライアントを実行して **Web** サービスをアクティブにし、頻繁に使用するオブジェクトタイプ情報をキャッシュすることをお勧めします。オブジェクトタイプ情報をキャッシュする最も簡単な方法は、`GetObjectTypeInfo()` メソッドを繰り返しコールすることです。この方法の使用を検討すべきオブジェクトタイプは以下のとおりです。

オブジェクト タイプ	定義
cr	Request
chg	変更要求
iss	Issue
cnt	連絡先
nr	アセット
wf	CA Workflow （変更要求）
iss_wf	CA Workflow （案件）
prp	プロパティ （変更および案件）
prptpl	プロパティ テンプレート (変更および案件)
cr_prp	リクエスト プロパティ
cr_prptpl	リクエスト プロパティのテンプレート

クライアント コードで参照するオブジェクト タイプの追加が可能です。

カテゴリおよびプロパティ

すべてのリクエスト オブジェクト、変更要求オブジェクト、案件オブジェクトにはチケットの性質を分類するためのカテゴリ フィールドがあります。カテゴリはプロパティ オブジェクトを持っている場合があります、カテゴリを割り当てる際チケットに添付されます。プロパティ オブジェクトが「必須」に指定されている場合は、チケットを保存する前に値を入力する必要があります（挿入および更新操作にも当てはまります）。

CA SDM Web サービスではチケットが作成されると自動的にデフォルト値が与えられます。デフォルト値 (currently, "-") は、CA SDM の各言語別メッセージ カタログから取得されます。

作成時にプロパティ値を設定するには、次の 3 種類のメソッド `createChangeOrder`、`createIssue`、`createRequest` を使用します。各メソッドでは、パラメータに値を指定してプロパティに渡すことができます。添付されるプロパティを確かめるには、チケットに割り当てるカテゴリに関連付けられたプロパティを調べる必要があります。最も簡単に使用できるメソッドは `getPropertyInfoForCategory()` です。

注: `getPropertyInfoForCategory()` の詳細については、「CA SDM テクニカル リファレンス ガイド」を参照してください。

プロパティに対する有効な値を識別するには、まず適切なプロパティ テンプレートのプロパティ検証ルールを特定します。これには、`getPropertyInfoForCategory` メソッドをコールする際に、`validation_rule` 属性をリクエストします。次に、そのルールに関連付けられた `validation_type` を取得します。タイプがドロップダウンの場合は、`getRelatedList` メソッドを使用して、ルールに関連付けられた値を取得し、`prpval_rule` オブジェクト内の「値」 `BREL` 属性を使用します。

注: 詳細については、「CA SDM テクニカル リファレンス ガイド」を参照してください。

`updateObject()` メソッドで更新操作を行った後にプロパティ値を設定するには、更新後にプロパティリストをクエリします。このタスクには `getRelatedList()` を使用できます。

Web サービス メソッドによるプロパティ値の検証は、現在サポートされていません。たとえば、ドロップダウン オプションの検証タイプを指定して検証ルールにプロパティ値を割り当てるには、ドロップダウン オプション検証ルールを作成する際に、追加コードを記述して、プロパティ値を作成する必要があります。チェック ボックス検証ルールにプロパティ値を割り当てないでください。

注: プロパティ検証ルールの詳細については、「管理ガイド」を参照してください。 **CA SDM** インターフェースを使用したプロパティ検証ルール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。

XML オブジェクトの戻り値

多くの **Web** サービス メソッドは、**CA SDM** オブジェクトを XML 形式で返します。**Web** サービスは、以下のルート要素で始まる XML の標準構造を使用します。

`<UDSObject>`

XML 形式は以下の表のとおりです。

XML エlement	タイプ	説明
<code><UDSObject></code>	N/A	ルート ノードを示します。
<code><Handle></code>	String	オブジェクト ハンドルを示します。
<code><Attributes></code>	シーケンス	属性値を示します。オブジェクト属性値のエレメントを 0 個以上保持します。

XML エlement	タイプ	説明
<code><attrName0 DataType = "typeEnum"></code>	String	<i>attrName0</i> を示します。これは CA SDM の majic (.maj) または mod (.mod) ファイルで定義されたオブジェクトの属性名です。 使用する Web メソッドによってはドット表記が使えます。 Element 値は属性値になります。Element の値が空の場合、オブジェクト属性の値も空/Null です。 DataType 属性には CA SDM 環境で使用する属性のデータ タイプを示す整数が入ります。

getObjectValues()をコールした場合、以下のような情報が返されます。

```
<UDSObject>
  <Handle>cnt:555A043EDDB36D4F97524F2496B35E75</Handle>
  <Attributes>
    <Attribute DataType="2003">
      <AttrName>first_name</AttrName>
      <AttrValue>first name</AttrValue>
      <DisplayValue>Yaakov</DisplayValue>
    </Attribute>
    <Attribute DataType="2005">
      <AttrName>organization</AttrName>
      <AttrValue>342</AttrValue>
      <DisplayValue>Accounting Crew</DisplayValue>
    </Attribute>
  </Attributes>
  <Lists>
    <List name="mylist1">
      <UDSObject>...</UDSObject>
      <UDSObject>...</UDSObject>
    </List>
  </Lists>
</UDSObject>
```

doSelect()などのメソッドは、<UDSObjectList>Elementに一連の<UDSObject>Elementを含めて返します。

<Lists>セクションには 0 個以上の<List>ノードが含まれます。<List> ノードには 0 個以上の <UDSObject> ノードが含まれます。 <List> エレメントは、通常、リスト値がリクエストされた場合のみ返されます。

特定のオブジェクトに関連する値のリストを返す場合は、`getRelatedListValues` メソッドを使用する必要があります。

`actlog` などの属性名をリクエストせずに、リストのみリクエストした場合は、<UDSObject>全体が<List>セクションに返されます。

ただし、`getDocument()`などの特殊なメソッドは除きます。属性をリクエストすると、データベース値が返されます。SREL 属性の場合、この値はあまり役立ちません。リクエストの `assignee` 属性をリクエストすると、Contact REL_ATTR（外部キー）が ID であるため、整数が返されます。Unicenter Service Desk r11.0 では、属性の戻りデータに DBMS のエレメント、および SREL が参照する共通名の値が含まれます。

ITIL 方式

デフォルトでは、Web サービスは ITIL 方式を完全にサポートします。CA SDM ITIL 機能によって ITIL 方式を利用できます。

インシデント/問題作成

CA SDM では、CA SDM Web サービスを使用してインシデントおよび問題を作成できるように、ITIL 方式をサポートしています。インシデントと問題は両方とも `cr` (Call_Req) オブジェクトに含まれます。レコードがインシデント、問題、またはリクエストのどれであるかは、`type` 属性で識別されます。インシデント、問題、またはリクエストを作成するには、`createRequest` メソッドをコールして `type` 属性に適切な値を指定します。

`type` 属性は `crt` (Call_Req_Type) オブジェクトへのポインタ (SREL) のため、値としてハンドルを渡す必要があります。

以下のコード例は、正しい crt オブジェクトハンドルを `createRequest` メソッドに渡して、インシデントや問題を作成する方法を示しています。パラメータとして `createRequest` に渡される名前と値のペアの中で `type` 属性を設定し、チケットを作成しています。

例: 問題用の構文

```
attrVals = {"summary", "A new problem", "description", "new problem", "type",  
            "crt:181"}  
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new  
String[0])
```

例: インシデント用の構文

```
attrVals = {"summary", "A new incident", "description", "new incident", "type",  
            "crt:182"}  
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new  
String[0])
```

関連項目:

[デフォルトのハンドル](#) (P. 703)

インシデント/問題のクエリ

インシデントまたは問題を取得するには、`cr` オブジェクトの `type` 属性を **Where** 節に含めます。アクティブなインシデントすべてを取得する **where** 節の例は以下のとおりです。この **where** 節は、`doSelect` や `doQuery` などの「`cr`」オブジェクトのクエリを実行するメソッドに使用できます。

```
type.id = 182 AND active = 1
```

「182」はインシデントタイプを表すハンドルの ID 部分です。

注: 詳細については、「[デフォルトのハンドル](#) (P. 703)」の `crt` (`Call_Req_Type`) オブジェクトの表を参照してください。正しいクエリの作成方法については、「[WHERE 節](#) (P. 428)」を参照してください。

問題へのインシデントの添付

問題には 1 つ以上のインシデントを関連付けることができます。インシデントの問題属性により、インシデントが問題に関連付けられます。

例: 問題へのインシデントの関連付け

この例では、新規に作成したインシデントを既存の問題に関連付ける方法を示します。

インシデントを問題に関連付けるには、**UpdateObject** を使用してインシデントの問題属性を設定します。以下のサンプルコードでは、問題属性を既存の問題チケットのハンドルに設定しています。

```
attributeValues = { "problem" , "cr:12346" }  
USPSD.UpdateObject(SID, incidentHandle, attributeValues, new String [0])
```

変更要求への問題の添付

インシデントおよび問題は、**attachChangeToRequest** メソッドによって変更要求にリンクさせることができます。以下のコードの例では、このメソッドを使用して、変更要求を作成すると同時に問題に添付しています。以下の例の「**cr:12347**」は問題のオブジェクトハンドルです。また、4 番目のパラメータには空のハンドルを渡しています。これにより、変更要求が作成されます。

```
UPSPSD.attachChangeToRequest(SID, creatorHandle, "cr:12347", "", new String[0],  
"activity description")
```

設定項目

ITIL 方式では、ハードウェア、ソフトウェア、およびその他の IT リソースを参照するのに「構成アイテム (CI)」という用語を使います。この用語は **CA Technologies** の所有するリソース データベース テーブルに格納されている「nr」オブジェクトを参照します。アセット オブジェクトを使用するすべてのメソッドは、CI と連携します。違いは使用している用語だけです。

Web サービスの利用

本セクションでは、**CA SDM Web** サービスの基本的な使用法について説明します。**Web** サービスを使用する場合のコード例は、以下の **CA SDM** インストールディレクトリにあります。

```
<NX_ROOT>/samples/sdk/websvc/java
```

サンプルコードは **SOAP** メッセージング用 **Apache Axis** を使用して **Java** で記述されています。

ログイン

Web サービス メソッドを使用する前に、**login()**、**loginService()**、**loginServiceManaged()** のうち、いずれかのメソッドを使用して **SID**（セッション ID）を取得する必要があります。最初の 2 つのメソッドには **CA SDM Web** クライアントと同一のユーザ名およびパスワードが必要です。検証方法は連絡先のアクセス タイプで指定します。3 番目のメソッドにはパブリック キー/プライベート キーのペアが必要です。プライベート キーで暗号化されたログイン リクエストがパブリック キーで復号化され、その逆も同様に実行されます。

関連項目：

[外部仕様](#) (P. 671)

共通タスクを実行する方法

柔軟で高機能な **API** を持つ **Web** サービスによって **CA SDM** を活用できますが、そのためには、以下の手順に従って、本製品で使用するオブジェクト構造について知っておく必要があります。

1. 「テクニカル リファレンス ガイド」でオブジェクトおよび属性の詳細について理解します。

本書にはシステムの各オブジェクトの属性がすべて掲載されています。ほとんどの **Web** サービス メソッドには属性名が必要なので、これはとても重要です。

2. Web サービス メソッド、特に一般的なメソッドを確認します。たとえば、アプリケーションでリクエストのアクティビティ ログすべてを表示する場合は、アクティビティ ログがリクエストに対してどのように関連付けられているかを最初に特定します。

「テクニカル リファレンス ガイド」では、リクエスト オブジェクトに、`act_log`（内部以外のログのみ）および `act_log_all`（すべてのアクティビティ ログ）という 2 種類のアクティビティ ログ リストがあることが示されています。

3. 必要な Web サービス メソッドを特定します。オブジェクトに添付されたリストを取得するには、`getRelatedList()` または `getRelatedListValues()` を使用します。

デフォルトのハンドル

本製品が提供するデフォルト データの中には、頻繁に使用するものがあります。これらのオブジェクト ハンドルを調べる手間を省くため、通常使用されるハンドルを以下に示します。

注: ハンドルは普遍ですが、判読可能なシンボルは編集することができます。

連絡先タイプ（オブジェクト名：ctp）

ハンドル	説明
ctp:2307	「アナリスト」タイプ
ctp:2310	「顧客」タイプ
ctp:2305	「従業員」タイプ
ctp:2308	「グループ」タイプ

影響度（オブジェクト名：imp）

ハンドル	説明
imp:1605	影響（なし）
imp:1600	影響 5（低）
imp:1601	影響 4（中低）

ハンドル	説明
imp:1602	影響 3（中）
imp 1603	影響 2（中高）
imp:1604	影響 1（高）

優先度（オブジェクト名：pri）

ハンドル	説明
pri:505	未割り当ての優先度（なし）
pri:500	優先度 5（低）
pri:501	優先度 4（中低）
pri:502	優先度 3（中）
pri:503	優先度 2（中高）
pri:504	優先度 1（高）

重大度（オブジェクト名：sev）

ハンドル	説明
sev:800	重大度 1（低）
sev:801	重大度 2（中低）
sev:802	重大度 3（中）
sev:803	重大度 4（中高）
sev:804	重大度 5（高）

コール リクエスト タイプ（オブジェクト名：crt）

ハンドル	説明
crt:180	Request
crt:181	問題
crt:182	Incident（インシデント）

連絡先に割り当てられたリクエスト、案件、または変更要求のクエリ

通常行われる最も一般的な操作は、アナリスト（担当者）に割り当てられたアクティブなリクエストの取得です。doQuery()（リスト参照の取得）、doSelect()（値を直接取得）などのメソッドを使用できます。担当者のハンドルがすでにわかっている場合、以下の Where 節を使用します。

```
assignee.id = U'<assigneeID>' AND active = 1
```

この Where 節では、<assigneeID> は連絡先ハンドルの ID 部分です。値は「555A043EDDB36D4F97524F2496B35E75」などのようになります。

リクエスト、変更要求、案件には「assignee」属性および「active」属性があり、その意味はこれら 3 つのオブジェクトで共通なので、この Where 節を使用できます。Where 節の「active = 1」部分は、アクティブなリクエストのみを検索することを示します。

アクティブ フラグ

ほとんどの CA SDM オブジェクトには「active」または「delete_flag」というフィールドがあります。これは Active_Boolean_Table オブジェクトまたは Boolean_Table オブジェクトを指す SREL ポインタのことです。クエリにこれらのフィールドを追加して、システム管理者が「非アクティブ」に設定したオブジェクトをフィルタすることもできます。クエリでは、

「delete_flag = 0」がアクティブなレコードの検索、「delete_flag = 1」が非アクティブなレコードの検索となります。たとえば、doSelect()を使用してアクティブなリクエスト ステータス オブジェクトのすべての値を取得する擬似コードは以下のようになります。

```
doSelect(SID, "crs", "delete_flag = 0", -1, new String[0]);
```

オブジェクトをアクティブまたは非アクティブに設定するには、値を true または false で表すブール オブジェクトのハンドルを渡す必要があります。このハンドルは変更されることはないので、コードに埋め込むことができます。以下にその値を示します。

Active_Boolean_Table	Boolean_Table
actbool:4551 = 'Active'	bool:200 = 'False'
actbool:4552 = 'Inactive'	bool:201 = 'True'

関連リストの長さの取得

`getObjectValues()`などを使用してオブジェクトから属性値を取得する場合、以下の属性値を使用して関連リストの長さを取得できます。

```
"<listName>.length"
```

たとえば、あるリクエストのアクティビティ ログ数を取得するには、以下の属性を `getObjectValues()`に渡します。

```
"act_log_all.length"
```

注: これは、このようなメソッドでリスト名を使用できる唯一の方法です。

REST（Representational State Transfer）は、World Wide Web などの分散ハイパーメディア システム用のソフトウェア アーキテクチャです。CA SDM REST API を使用すると、アプリケーション、インテグレーション、および Web 開発者は、タブレット コンピュータやスマートフォンなどのデバイス用の UI およびアプリケーションを構築できます。アナリスト、従業員、顧客などのユーザは、これらのデバイス上で UI またはアプリケーションを使用できます。たとえば、アプリケーション開発者は、アナリストがデバイスを使用してチケットを更新するための CA SDM UI を開発できます。

REST API は、インターネット上の名前またはリソースを識別する文字列である URI（Uniform Resource Identifier）を使用することによりリソースにアクセスします。CA SDM では、リソースはチケット、アセット、連絡先などのオブジェクトです。REST API を使用するアプリケーションは、URI に対して HTTP リクエストを行い、応答を解析します。このような識別方法を使用することで、ネットワーク上のリソースの表現と対話できるようになります。クライアントからサーバへの各リクエストは、そのリクエストを理解するために必要なすべての情報を持っており、サーバに格納されているコンテキストを使用しません。

開発者は、REST API を直接使用して、操作したいリソースに関する HTTP リクエストをサーバに送信します。開発者に必要なものは、HTTP クライアント ライブラリのみです。このライブラリは、ほとんどのプログラミング言語で利用可能です。REST API はオープン スタンドードに基づいているため、任意の Java プログラミング言語を使用してこの API にアクセスできます。

注: REST HTTP 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。

REST と SOAP

CA SDM は、REST と SOAP の Web サービス API を提供します。REST API は UI クライアントを対象としており、SOAP API はプログラムを対象としています。REST サービスは、リソースに関するサービスです（オブジェクトの操作、オブジェクト状態の変更、動詞ではなく名詞の使用）。SOAP サービスは、サービスを対象としています（メソッドのコール、動詞の使用、アクションの実行）。

REST には、SOAP と比べて以下の利点があります。

- REST は軽量、HTTP ベース、ステートレスである（スケーラビリティが高い）。
- REST はクライアントブックマークおよびキャッシュをサポートしている。
- REST はデータ コントラクトが緩い。
- REST は、WEB 2.0 や AJAX などのフロントエンド技術による利用が簡単。
- REST は、XML および JSON データ形式をサポートしている。
- REST はパフォーマンスの向上をもたらす。

REST セキュリティ

セキュリティでは、共有秘密鍵を使用するカスタム アプローチを含む、複数の認証メカニズムが使用されます。

CA SDM は、以下のセキュリティ認証スキームをサポートしています。

- REST Web サービス秘密鍵認証（ログインに SSL および HMAC を使用）
- REST ベーシック認証（クリアテキストのユーザ名/パスワード）
- REST BOPSID 認証（CA SDM BOPSID を検証）
- 外部（CA EEM）アーチファクト認証（CA EEM アーチファクト トークン）

秘密鍵認証の仕組み

CA SDM 秘密鍵認証は、以下を検証するプロセスです。

- リクエスト送信者のアイデンティティ。
- 送信者が登録済みのユーザかどうか。

秘密鍵認証では、各リクエストにリクエスト送信者のアイデンティティに関する情報が含まれている必要があります。また、CA SDM がユーザの真正性を検証するために使用できる追加情報も必要です。リクエストがこの検証テストに合格すると、そのリクエストは真性であることが確認されます。アクセス キー リクエストの認証中、CA SDM 秘密鍵認証は以下を行います。

1. クライアントにアクセス キーを割り当てます。アクセス キーは、リクエストを行うクライアントを識別し、キー値として CA SDM セッション ID を使用します。アクセス キーはリクエスト パラメータとして送信されるため、秘密ではありません。CA SDM にリクエストを送信する人は誰でも、リクエスト パラメータを使用できます。このため、秘密鍵が必要になります。
2. 秘密鍵を割り当てます。秘密鍵は、ログイン中に CA SDM によって動的に生成される 40 文字の英数字です。この秘密鍵は、データベースに格納される前に暗号化されます。
3. クライアントが提供する情報（秘密鍵を使用したリクエスト シグネチャ）を使用して、クライアントを識別し、リクエストが正当であることを確認します。この追加情報により、ユーザの偽装が防止され、CA SDM とリクエストの送信者のみが知る共有秘密を保有していることが示されます。

Web サービス オプション

以下のオプションは、Web サービス セッションを制御します。

`rest_webservice_access_duration`

REST Web サービス アクセス キーが有効期限が切れるまでアクティブ状態にある時間数を指定します。アクセス キーのタイムアウトは、非アクティブ状態の時間ではなく、アクセス キーが作成してからの期間に基づいて決定されます。アクセス キーが指定された期間に達すると、そのアクセス キーは使用されているかどうかに関係なく終了します。

オプションで、REST クライアントも、アクセス キー リクエスト中に特定のアクセス キーのアクセス キー時間を指定できます。この時間を指定するには、POST リクエスト ペイロードの一部として、`rest_access` リソースの `expiration_date` 属性に直接設定します。

有効範囲：1 ～ 8760 時間

デフォルト：168

`rest_webservice_disable_basic_auth`

REST Web サービスのベーシック認証を無効にします。

デフォルト：No

`rest_webservice_list_max_length`

REST Web サービスのクエリが返す行の最大数を指定します。

デフォルト：500

`rest_webservice_list_page_length`

REST Web サービスのクエリが返す行のデフォルト数を指定します。

有効範囲：1 ～ 500

デフォルト：25

`rest_webservice_resources_to_expose`

CA SDM が REST Web サービスを通して公開する Majic ファクトリ（リソース）のリストを指定します。このオプションにより、デフォルト動作がオーバーライドされます。デフォルトでは、CA SDM は REST Web サービスを通してすべてのファクトリを公開します。

このオプションに値を入力しない場合、デフォルトの動作により、`REST_OPERATIONS` プロパティが `NONE` に設定されていないすべての Majic ファクトリが公開されます。デフォルトでは、このプロパティが `NONE` に設定されている Majic ファクトリはありません。

REST_OPERATIONS プロパティを使用して、特定の HTTP CRUD (CREATE、READ、UPDATE、DELETE) メソッドを設定し、CA SDM が特定の Majic ファクトリを公開するようにします。

デフォルト : rest_access

例 : rest_access, cnt, grp, cr, crs, pri, alg, urg, imp, pcat, org

hmac_algorithm

REST Web サービスでのカスタム/秘密鍵認証用のシグネチャを計算するために使用するアルゴリズムを指定します。 Services.

デフォルト : HmacSHA1

string_to_sign_fields

デフォルトの REQUEST_METHOD、REQUEST_URI、および QUERY_STRING フィールドに加えて、REST Web サービスでのカスタム/秘密鍵認証用のシグネチャを計算するために使用するフィールドを指定します。

デフォルト : 空白

webservice_domsrvr

SOAP Web サービスによって使用されるオブジェクト エンジンの名前を指定します。 インストールされていない場合、SOAP Web サービスは「domsrvr」を使用します。

オプションの値には、「domsrvr:」で始まる文字列を指定する必要があります。

webservice_session_timeout

SOAP Web サービス セッションのタイムアウト値 (分) を設定します。 連続する Web メソッド コールの間隔が指定した値を超えた場合、セッション ID は期限切れとして識別されます。 その結果、そのセッションは無効になります。

アクティビティが原因でセッションが期限切れにならないようにするには、このオプションに 0 を指定します。 ただし、ログオフ ルーチンなどの他の原因によって無効になる場合もあります。

注: これらのオプションでは CA SDM サーバを再起動する必要があります。

第 13 章：その他の製品の統合

CA SDM を一部の CA Technologies 製品と統合できます。ただし、本書に CA Technologies 製品との統合の詳細をすべて記載しているわけではありません。

注：このセクションで説明しない CA SDM の統合の詳細については、<http://ca.com/jp/support> の「CA Unicenter Service Desk 統合化グリーンブック」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。

[CA Workflow インテグレーション](#) (P. 711)

[CA Portal インテグレーション](#) (P. 717)

[メインフレーム製品のインテグレーション](#) (P. 725)

[CA Business Service Insight 統合](#) (P. 728)

CA Workflow インテグレーション

ワークフローは、タスク、手順、関係する組織または個人、必要な入力と出力の情報、およびビジネス プロセスの各手順の管理と維持に必要なツールを意味します。ワークフロー サービスでは、ビジネス プロセスの管理に役立つ総合的な解決策を提供します。

一般に、ワークフローに最も適した表現は、ビジネス プロセス全体またはその一部の自動化です。その実行中は、一連の手続きのルールに従ってアクションを実行するためにドキュメント、情報、またはタスクが関係者の間でやり取りされます。

CA Workflow は汎用性が高く、高性能でスケーラブルなワークフロー管理システムで、ワークフローの定義、管理、および実行が可能な汎用ワークフロー ソリューションです。

CA Workflow は Web サービスを使用して CA SDM に統合されます。

CA Workflow のコンポーネント

CA Workflow では、ワークフロー埋め込みキットに含まれている以下のコンポーネントを使用します。

- [ワークフロー デザイン環境](#) (P. 712)
- [ワークフロー サーバ](#) (P. 714)
- [Worklist](#) (P. 714)

CA Workflow デザイン環境

CA Workflow デザイン環境を使用して、ワークフローを作成および管理します。CA Workflow デザイン環境は、プロセス定義とワークフロー インスタンスの作成および管理、ワークフローの関係者間のやり取りを制御するための主要なツールです。

会社では、ビジネス プロセスを作成して、リソース、手動アクティビティと自動アクティビティ、およびアクティビティの関連付けを特定して、会社のビジネス目標を実現します。ワークフローでは、ビジネス プロセスの各種アクティビティをプロセス定義で指定することで、ビジネス プロセス全体またはその一部を自動化します。このようなワークフローのアクティビティには、通常、フォーム、タスク、または情報を人やソフトウェアなどのリソース間でやり取りする処理が含まれます。

プロセス定義は、ビジネス プロセスを表すものです。プロセス定義は、ノード、イベント、役割、アクター、作業、およびプロセス開始条件とプロセス終了条件で構成されています。

プロセス定義はビジネス プロセスで実行が必要な処理を表すのに対し、プロセス インスタンスは実際に実行されている処理を表します。プロセス定義を実行することで、プロセス インスタンスを作成します。同じプロセス定義に複数のプロセス インスタンスを作成できます。このようなプロセス インスタンスは、プロセス定義インスタンスとも呼ばれます。

CA Workflow デザイン環境の開始 (Windows)

いつでも、CA Workflow デザイン環境を開始して、ワークフローを作成および管理できます。CA Workflow デザイン環境を開始するには、[スタート] - [すべてのプログラム] - [CA] - [Service Desk Manager] - [CA Workflow IDE] を選択します。

注: `$NX_ROOT\site\Workflow\Client` ディレクトリにある `ide.bat` ファイルをダブルクリックして、CA Workflow デザイン環境を開始することもできます。アプリケーション要件に対応するために IDE クラスパスに追加処理が必要な場合は、`ide.bat` の `APPCPATH` パラメータを変更し、その `ide.bat` を使用して IDE を起動する必要があります。

CA Workflow デザイン環境の開始 (Linux)

いつでも、CA Workflow デザイン環境を開始して、ワークフローを作成および管理できます。CA Workflow デザイン環境を開始するには、`$NX_ROOT/site/Workflow/Client` ディレクトリにある `ide.sh` ファイルを実行します。CA Workflow IDE は UNIX ではサポートされていません。

注: アプリケーション要件に対応するために、`ide.sh` ファイルには `APPCPATH` パラメータがあり、このパラメータを変更してクラスパスに追加することができます。

CA Workflow IDE パラメータ

CA Workflow デザイン環境にアクセスすると、ログイン画面が表示されます。ログイン画面には、ユーザ名、パスワード、および URL 接続があらかじめ入力されています。IDE へのアクセスを簡素化するために、ログイン画面を完全に省略するには、以下のコマンドラインパラメータを組み合わせ使用します。

```
-u <username>
-p <password>
-url <PM URL>
-t <eIAM Safe Session token>
```

ユーザ名とパスワード (-u と -p) を指定するか、トークン (-t) を指定して IDE を起動できます。- t トークンは、エクスポートされた文字列タイプの **SafeSession** (成果物とも呼ばれる) を参照します。このようにすると、親製品で既存の **SafeSession** を再使用できるようになり、ユーザ名とパスワードの入力を要求するメッセージが再度表示されることはありません。

- url は必須パラメータで、- u ユーザ ID メソッドと - p パスワードメソッドの組み合わせ、または - t トークンメソッドのどちらを使用する場合にも指定する必要があります。

例: [-u, -p, -url] または [-t, -url]

このファシリティを使用して IDE ログイン画面を省略するには、**ide.bat** ファイル (Microsoft Windows の場合) または **ide.sh** (Linux の場合) を編集して、これらのパラメータを Java コマンドに渡されるパラメータのリストに追加します。

注: このファシリティは、**ide.exe** では使用できません。

CA Workflow サーバ

CA Workflow サーバでは、ワークフロープロセスにランタイム実行と管理サービスを提供します。CA Workflow サーバは、以下のコンポーネントで構成されます。

- **Actor** アダプタ。ワークフロー アクティビティの機能を拡張できます。
- **プロセスエンジン**。プロセス定義インスタンスを実行します。
- **プロセスマネージャ**。プロセス定義とプロセスインスタンスを管理します。

すべてのワークフロークライアント、プロセスデザイナー、ワークリスト、および Java と Web サービス API では、CA Workflow サーバのサービスを使用します。

Worklist

ワークリストは、Web ブラウザ (<http://<hostname>:<port number>/wl> など) または埋め込み製品からの API 呼び出しを使用して起動できます。

CA Workflow へのアクセス

CA SDM は、共通ワークフロー エンジンを使用するワークフロー管理機能を提供します。このワークフロー システムでは、GUI によるワークフロー 定義環境、洗練された分岐機能、および承認取得時に CA SDM アプリケーションへ直接アクセスできないユーザとの対話機能が提供されています。CA Workflow 認証を使用し、CA Workflow グループに[ユーザを追加](#) (P. 716) できます。

CA EEM と CA Workflow

CA Workflow へのすべてのログインは、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 レコードを持っている必要があります。CA SDM の環境設定で指定した CA Workflow 管理者は、CA Workflow の全機能にアクセスできます。デフォルトではこの管理者が、CA SDM によって CA Workflow インテグレーションに使用されます。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されたユーザ名とパスワードが正しいことと、このユーザが CA EEM で CA Workflow のリソースの全機能にアクセスできることを確認する必要があります。

リソース クラス

また、CA Workflow は、CA EEM を使用して特定の CA Workflow 機能に対するアクセスを制限します。アクセスは以下の 2 つのリソース クラスによって制御されます。

IDE

IDE リソースには、IDE へのログイン アクセスのために *login* という名前の 1 つのアクションが設定されています。CA Workflow IDE アプリケーションにログインする場合、ユーザはこのアクションを実行する権限を持っている必要があります。

プロセス

プロセス リソースには、プロセス インスタンスを開始する機能のために *start* という名前の 1 つのアクションが設定されています。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。すべてのユーザは、CA Workflow のワークリスト 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。このアクセス権限は、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。

注: これらのリソース クラスは、CA SDM アプリケーション インスタンスと共に CA EEM 内で定義されます。CA EEM Web ユーザ インターフェースにログインすると、ここで説明したリソース、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。

CA Workflow のグループへのユーザの追加

IDE にログインする必要のあるユーザ、またはプロセス インスタンスを開始する必要のあるユーザには、リソースおよび 2 つのアクションに対する権限が付与されている必要があります。CA SDM 環境設定によって、これらのリソースへのアクセス権を与える 2 つのポリシーが CA EEM に追加されます。また、ポリシーへの権限を付与された 2 つのユーザ グループ、CA Workflow 管理者と CA Workflow プロセス開始者が追加されます。ユーザを CA Workflow 管理者グループに追加すると、これらのユーザに IDE へのアクセス権が与えられます。ユーザを CA Workflow 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。

CA EEM がインストールされているコンピュータ上でグループにユーザを追加/削除する方法

1. 以下のいずれかの手順を実行します。
 - CA EEM r8.4 SP4 CR05 の場合は、[スタート] - [プログラム] - [CA] - [Embedded Entitlements Manager] - [EEM UI] を選択します。
 - CA EEM r12 CR02 の場合は、[スタート] - [プログラム] - [CA] - [Embedded Entitlements Manager] - [Admin UI] を選択します。ログイン ウィンドウが表示されます。
2. CA SDM アプリケーションを選択して、CA EEM 管理者の名前とパスワードを入力します。
CA EEM のメイン ウィンドウが表示されます。
3. [ID の管理] 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] をクリックします。
5. 結果リストからユーザを選択します。
6. ユーザの詳細情報が表示されたら、[アプリケーション グループ メンバーシップ] セクションでグループ メンバーシップを追加または削除します。
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] をクリックします。
7. [保存] をクリックします。
ユーザがグループに追加されます。

CA Portal インテグレーション

CA Management Portal および CA Portal を通して CA SDM コンポーネントにアクセスできます。

注: CA Management Portal および CA Portal は CA SDM に含まれていないので、別途購入してライセンスを入手する必要があります。CA SDM では、ポータル管理を使用して CA SDM にアクセスするための最も基本的な情報のみが含まれています。詳細については、CA Portal および CA Management Portal Server Administration のオンライン ヘルプを参照してください。

CA SDM Web インターフェースのアクセシビリティの確認

CA SDM をシステムにインストールした後、tomcat サーバから Web インターフェースにアクセスできることを確認してください。ポータルとのインテグレーションが機能するには、tomcat から CA SDM Web インターフェースにアクセスする必要があります。

注: CA SDM LINUX サーバのインストールの場合は、LD_LIBRARY_PATH を \$NX_ROOT/sdk/lib に設定する必要があります。

CA Portal のインストールと起動

CA Portal のインストール、起動、および停止の詳細については、CA Portal の「導入ガイド」を参照してください。

注: CA Portal は、CA SDM がインストールされているシステムまたは別のシステムにインストールできます。

ポートレットの指定

本製品を使用して、ポータルに CA SDM ポートレットを指定することができます。

ポートレットを指定する方法

1. CA SDM にログインし、[管理] タブで [オプション マネージャ] - [検索] を選択します。

[オプション リスト] ウィンドウが表示されます。

2. Portal_Safe_List をクリックします。

[Portal_Safe_list オプションの詳細] ウィンドウが表示されます。

3. [オプション値] フィールドに、ポータルがインストールされているサーバのサーバ名とポート番号を *servername:portnumber* の形式で入力します。

注: こ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。

4. [インストール] をクリックします。
5. CA SDM デーモンを再起動します。
6. 管理者として CA Portal にログインします。

7. 有効な CA SDM ユーザであるユーザを作成します。ユーザの作成方法については、CA Portal のマニュアルを参照してください。

注: CA SDM でこの統合のユーザを認証する場合は、ユーザ名、有効な CA Portal セッション、および CA Portal インストール値の組み合わせ (PORTAL_SAFE_LIST オプションで終了した場合) を使用するため、ポータルでユーザの作成中に使用するパスワードが、同じユーザが CA SDM へのログインに使用するパスワードと異なることがあります。

8. CA Portal のメイン メニューバーから [ナレッジ] を選択します。
[ナレッジ] ページが表示されます。
9. 左側のペインにある [ナレッジ] バーで [ライブラリ] を選択します。
左側のペインにライブラリ ツリーが表示されます。
10. ライブラリ ツリーでフォルダを選択するか、必要に応じてフォルダを新規作成してから選択して、右側のペインにある [ナレッジ] バーで [ファイルの発行] を選択します。
[ファイルの発行] フォームが開きます。
11. [一般情報] タブの [コンテンツ] テキスト ボックスに以下の CA SDM ポートレットの URL を入力します。

```
http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=portalhostname:portalportnumber
```

注: URL の *hostname:portnumber* を CA SDM がインストールされている Web サーバの名前とポート番号に置き換えます。URL の *portalhostname:portalportnumber* をポータルがインストールされている Web サーバの名前とポート番号に置き換えます。

12. [タイトル] テキスト ボックスに「CA SDM」と入力します。
13. [詳細設定] をクリックします。
[ファイルの発行] フォームの [プロパティの詳細] ページが表示されます。
14. [MIME コンテンツ タイプ] フィールドに「*portal/variable-url*」と入力して、[発行] をクリックします。
発行したコンテンツが選択したライブラリ フォルダに表示されます。

15. このポートレットが表示されるようにワークスペースを設定します。
16. ログアウトしてから新規に作成したユーザとしてログインします。作成したポートレットの **CA SDM** に再度ログインしなくても、自動的にログインされるはずです。

注: ポートレットで **CA SDM** を実行している間は、[環境設定] ページで [ポップアップを非表示] を使用できません。また、環境設定の設定値に関係なく、常にポップアップ ウィンドウが使用されます。

CA Portal サーバへの接続

CA Portal サーバに接続するには、Web ブラウザを開き、ロケーションまたはアドレス フィールドに以下の URL を入力します。

`http://<servername>:<port#>/servlet/portal`

`<servername>`

ポータル サーバのサーバ名（または IP アドレス）を指定します。

`<port#>`

CA Portal サーバで監視するポート番号を指定します。ポート番号は CA Portal サーバのインストール時に指定します。ポートの初期設定は 8080 です。

CA Portal で SSL を使用するための CA SDM の設定

注: 実稼働環境では、信頼できる認証局から証明書入手することをお勧めします。

SSL を使用するように CA SDM を設定する前に、SSL なしでも CA Portal と CA SDM の統合が機能するかどうかを確認してください。SSL なしでも統合が機能する場合は、ポートレットを指定できます。

関連項目:

[ポートレットの指定](#) (P. 718)

自己署名入りの証明書を使用した SSL のセットアップ

自己署名入りの証明書を使用して CA SDM ポータルのインテグレーションをセットアップする方法

1. コマンドラインに以下のように入力します。

```
%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA
```

入力を要求するメッセージが表示されたら適切なデータを入力し、パスワード要求の両方に「changeit」と入力します。

証明書がセットアップされます。

2. 以下の場所にある `server.xml` ファイルを編集します。

```
$NX_ROOT/bopcfg/www/CATALINA_BASE/conf
```

3. 以下のセクションのコメントを解除して、保存します。

```
<!--  
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"  
    port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"  
    acceptCount="100" debug="0" scheme="https"  
    secure="true" useURIVValidationHack="false" disableUploadTimeout="true">  
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"  
    clientAuth="false" protocol="TLS" /></Connector>  
-->
```

4. `keystoreFile` 属性を `server.xml` に追加します。（手順 1 でコマンドを実行したときに、`.keystore` ファイルがユーザのホーム ディレクトリに作成されます）。参照を `keystoreFile` 属性に追加して、ファイルを保存します。編集後の `server.xml` ファイルは以下のようになります。

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"  
    port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"  
    acceptCount="100" debug="0" scheme="https" secure="true"  
    useURIVValidationHack="false" disableUploadTimeout="true">  
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"  
    clientAuth="false" protocol="TLS" keystoreFile="location/.keystore" />  
</Connector>
```

5. CA SDM を再起動します。
6. SSL 機能を確認するには、ブラウザに「`https://hostname:8443`」と入力します。[セキュリティ アラート] ダイアログ ボックスが表示されます。[はい] をクリックします。

注: SSL ではポート 8443 を使用します。

7. HTTPS とポート 8443 を使用するように CA SDM ポートレットを置き換えます。

`https://hostname:8443/CAisd/PortalServlet?`

`USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=portalhostname:portalportnumber`

CA Portal で SSL を使用する場合 CA SDM に接続

SSL を使用するように CA Portal が設定されている場合、CA SDM と CA Portal との間に信頼できる接続を確立できるように、CA Portal サーバ証明書をインポートできます。

Portal が SSL を使用する場合に CA SDM に接続する方法

1. CA Portal が設定されていて、SSL とともに機能することを確認します。

注: 確認方法については、CA Portal のマニュアルを参照してください。

2. 以下の手順に従って、CA Portal がインストールされているコンピュータから証明書をエクスポートします。

- a. 以下の場所で `server.xml` ファイルを探します。

`PORTAL_Install_Dir¥jakarta-tomcat-4.1.29¥conf`

- b. `server.xml` 内の以下の行に示されている、`keystore` の場所とパスワード (`pwd`) を書き留めてください。初期設定のパスワードは「`changeit`」(すべて小文字)です。ポータルセットアップ中、証明書の作成時にカスタムパスワードを使用した場合は、そのカスタムパスワードを使用しなければなりません。詳細については、CA Portal のマニュアルを参照してください。以下の手順と例では、「`changeit`」をデフォルトのパスワードとして使用しています。

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="150"
  enableLookups="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  useURIVValidationHack="false" disableUploadTimeout="true">
  <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="c:¥Program Files¥CA¥SC¥Unicenter Management
Portal¥UMPkeystore"
    keystorePass="changeit"
    clientAuth="false" protocol="TLS" />
</Connector>
```

- c. ポータル サーバ コンピュータの JRE bin ディレクトリ
(PORTAL_Install_Dir¥jre¥bin) に移動して、PORTAL Server 証明書を
ファイルにエクスポートする際に使用する keytool ユーティリ
ティにアクセスします。

- d. keytool ユーティリティにアクセスするには以下のコマンドを使用
します。

```
keytool -export -alias tomcat -file umpserver.cer -keystore "c:¥Program  
Files¥CA¥SC¥Unicenter Management Portal¥UMPkeystore"
```

keystore のパスワードを入力します : changeit

証明書はファイル <umpserver.cer> に格納されています。

注: パスワードの入力を要求するメッセージが表示されたら、必ず
手順 2b で取得したパスワードを使用してください。上記の例では、
「changeit」が手順 2b で書き留めたパスワードです。keystore の
場所も、手順 2b で取得したものです。

- 3. 以下のように、keytool ユーティリティを使用して、サーバから取得し
た証明書を、CA SDM インストールを含むコンピュータにインポートし
ます。

- a. CA SDM コンピュータで、JRE¥bin ディレクトリ（通常は以下の場所
にある）に移動します。

```
C:¥Program Files¥CA¥SC¥JRE¥bin
```

- b. CA SDM Java 仮想マシンが使用している認証局に証明書をイン
ポートする必要があります。

以下はインポートの例です。この例では、認証局は以下の場所に
あります。

```
C:¥Program Files¥CA¥SC¥JRE¥1.4.2_06¥lib¥security¥cacerts
```

pwd の入力を求めるメッセージが表示されたら、「changeit」と入
力します。「この証明書を信頼しますか?」への応答を求めるメッ
セージが表示されたら、「Yes」と入力します。

```
Keytool.exe -import -alias tomcat -trustcacerts -file umpserver.cer  
-keystore "C:¥Program Files¥CA¥SC¥JRE¥1.4.2_06¥lib¥security¥cacerts"
```

keystore のパスワードを入力します : changeit

```
Owner: [所有者:] CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us  
Issuer: [発行者:] CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny,  
C=us
```

```
Serial number: [シリアル番号:] 43ecb469
```

Valid from: [有効開始日時:] Fri Feb 10 10:42:33 EST 2006 終了日時: Thu May 11 11:42:33 EDT 2006

Certificate fingerprints [認証指紋] :

MD5: A1:AF:AE:92:39:2E:53:D5:1C:6D:FE:44:68:61:DD:5C

SHA1:

66:3A:BC:77:32:81:60:89:70:B9:EF:FB:74:3D:93:74:CD:8E:E2:D2

Trust this certificate? [この証明書を信頼しますか?] [no]: はい

Certificate was added to keystore [証明書は keystore に追加されました]

注: パスワードの入力を要求するメッセージが表示されたら、手順 2b で取得したパスワードを使用してください。上記の例では、「changeit」が手順 2b で書き留めたパスワードです。

4. \$NX_ROOT¥bopcfg¥www¥CATALINA_BASE¥webapps¥CAisd¥WEB-INF¥xml¥portal-xml-api.xml の下にあるファイル portal-xml-api.xml を編集するには、以下の手順に従います。

- a. 次の行にある http を https に置き換える。編集前:

```
<!DOCTYPE PORTAL SYSTEM
```

```
"http://127.0.0.1:8080/servlet/media/xml/api/request.dtd">
```

編集後:

```
<!DOCTYPE PORTAL SYSTEM
```

```
"https://127.0.0.1:8080/servlet/media/xml/api/request.dtd">
```

- b. ファイルを保存します。
- c. Portal_Safe_List がインストールされている場合は、ポート番号を 8443 に変更し、コンピュータ名をドメイン名を含むように変更します（例: computername.ca.com:8443）。

重要: ドメイン名を含むポータル証明書としてコンピュータ名にドメイン名を含めます。詳細については、CA Portal のマニュアルを参照してください。

5. CA SDM サーバをリサイクルします。
6. 以下の URL を使用して、CA Portal から CA SDM ポートレットに接続します。

```
http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=servername:8443
```

注: この URL 中の *servername* は、CA Portal がインストールされている Web サーバの名前に置き換えます。この URL 中のサーバ名には、ドメイン名を含める必要があります（例: servername.ca.com:8443）。この URL 中の *hostname:portnumber* は、CA SDM がインストールされている Web サーバの名前とポート番号に置き換えます。

関連項目:

[ポートレットの指定 \(P. 718\)](#)

メインフレーム製品のインテグレーション

CA SDM 側のデータ (.dat ファイル) は、メインフレーム製品のインテグレーションに関連付けられています。

CA SDM 側のデータのロード

メインフレーム製品の統合に関連付けられている CA SDM 側のデータ (.dat ファイル) は、.dat ファイルをメインフレーム製品名に関連付けているリストに存在します。

注: CA SDM サーバは、デフォルトでは、ITIL 方式を使用するように設定されています。

CA SDM 側のデータをロードして特定の統合を有効にするには、`pdm_userload -f integXXX.dat` を使用します。

これらのデータ ファイルは、`$NX_ROOT¥data¥integrations¥` に配信されます。

注: 統合の呼び出し元（メインフレーム製品側）を有効にする方法の詳細については、「*CA Common Services for z/OS - CA Service Desk Integration Guide*」を参照してください。

CAISDI を現在使用している CA 製品

CAISDI を現在使用している CA メインフレーム製品および関連する .dat ファイルは以下の表のとおりです。

CA 製品	プライマリ データ ファイル	ITIL 更新ファイル
CA Advantage EDBC	integEDBC.dat	
CA 1 Tape Management	integCA1.dat	itil_integCA1.dat

CA Allocate DASD Space and Placement	integAllocate.dat	itil_integAllocate.dat
CA Disk Backup and Restore	integDisk.dat	itil_integDisk.dat
CA TLMS Tape Management (CA TLMS)	integTLMS.dat	itil_integTLMS.dat
CA Vantage Storage Resource Manager (CA Vantage SRM)	integVantage.dat	itil_integVantage.dat
CA 7 Workload Automation (CA 7 WA)	integCA7.dat	itil_integCA7.dat
CA JARS Resource Accounting (CA JARS RA)	integJARS.dat integJARSMVS.dat	itil_integJARS.dat itil_integJARSMVS.dat
CA MIM Resource Sharing (CA MIM RS)	integMIM.dat	itil_integMIM.dat
CA OPS/MVS Event Management and Automation (CA OPS/MVS EMA)	integOPSMVS.dat	itil_integOPSMVS.dat
CA SYSVIEW Performance Management (CA SYSVIEW)	integSysview.dat	itil_integSysview.dat
CA NetMaster Network Management for TCP/IP (CA NetMaster NM for TCP/IP)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Management for SNA (CA NetMaster NM for SNA)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Automation (CA NetMaster NA)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster Network Operations for TCP/IP (CA NetMaster NO for TCP/IP)	integNetMaster.dat	itil_integNetMaster.dat
CA NetMaster File Transfer Management (CA NetMaster FTM)	integNetMaster.dat	itil_integNetMaster.dat
CA MICS Resource Management (CA MICS)	integNeuMICS.dat	itil_integNeuMICS.dat

CAISDI の使用を予定している CA 製品

CAISDI の使用を予定している CA メインフレーム製品および関連する .dat ファイルは以下の表のとおりです。

CA 製品	プライマリ データ ファイル	ITIL 更新ファイル
CA 2E	integ2e.dat	
CA Enterprise Workload Automation	integAutoSys.dat	
CA Bundl	integBundl.dat	
CA 11 Enterprise Workload Automation Restart and Tracking	integCA11.dat	
CA 接続	integConnect.dat	
CA Datamacs	integDatamacs.dat	
CA Date Simulator	integDate.dat	
CA Deliver	integDeliver.dat	itil_integDeliver.dat
CA Dispatch	integDispatch.dat	itil_integDispatch.dat
CA FAVER VSAM Data Protection	integFaver.dat	
CA FileAge	integFileAge.dat	
CA File Master Plus	integFileMaster.dat	
CA Filesave RCS Automated Recovery	integFileSave.dat	
CA Gen	integGen.dat	
CA GSS (共通コンポーネント)	integGSS.dat	
CA InterTest	integInterTest.dat	
CA JCLCheck Enterprise Workload Automation	integJCLCheck.dat	
CA Jobtrac Job Management	integJobtrac.dat	itil_integJobtrac.dat
CA LPD Report Convergence	integLPD.dat	
CA Optimizer	integOptimizer.dat	
CA Optimizer/II	integOptimizerII.dat	
CA Plex	integPlex.dat	
CA Scheduler Job Management	integScheduler.dat	

CA Spool Enterprise Print Management	integSpool.dat	itil_integSpool.dat
CA SymDump	integSymDump.dat	
CA Verify	integVerify.dat	
CA ビュー	integView.dat	itil_integView.dat

CA Business Service Insight 統合

CA Business Service Insight（CA BSI）を使用すると、サービスおよびサービス レベル パフォーマンス管理の統合、サービス評価およびサービス比較の活用など、IT サービス パフォーマンスを管理できます。CA BSI を使用すると、サービスのパフォーマンスがサービス レベル アグリーメント（SLA）に準拠しているかどうかを調べることができます。CA BSI は、サービス レベル管理（SLM）情報を CA SDM の Service Desk アナリストに提供して、組織のさまざまな IT サービスの変更を管理できるようにします。この SLM 情報により、よりすぐれた意思決定と IT サービスの提供が実現されます。

CA BSI との統合により、CA SDM の CI 詳細フォームにタブが追加されます。「Service Level Compliance」および「Modified Service Level by Metrics vs Target」レポートは、CA SDM エンタープライズ サービス ファミリ CI に関する情報を提供します。「Modified Service Level by Contract vs Target」レポートは、CA SDM 契約ファミリ CI に関する情報を提供します。

注: これらのタブは、CA BSI MDR への統一アセット マッピングがある CI についてのみ表示されます。

CA BSI に CA SDM を統合すると、CA BSI MDR に関連付けられている契約 CI のメトリック データを表示できます。リクエストをサブミットする前に、契約当事者（CA BSI エンティティ）を指定する必要があります。CA BSI の制限により、名前に特定の非英数字が含まれている契約当事者に関するメトリック データは正しく表示されません。契約当事者名には英数字を使用し、以下の文字は使用しないでください。

reserved = gen-delims / sub-delims

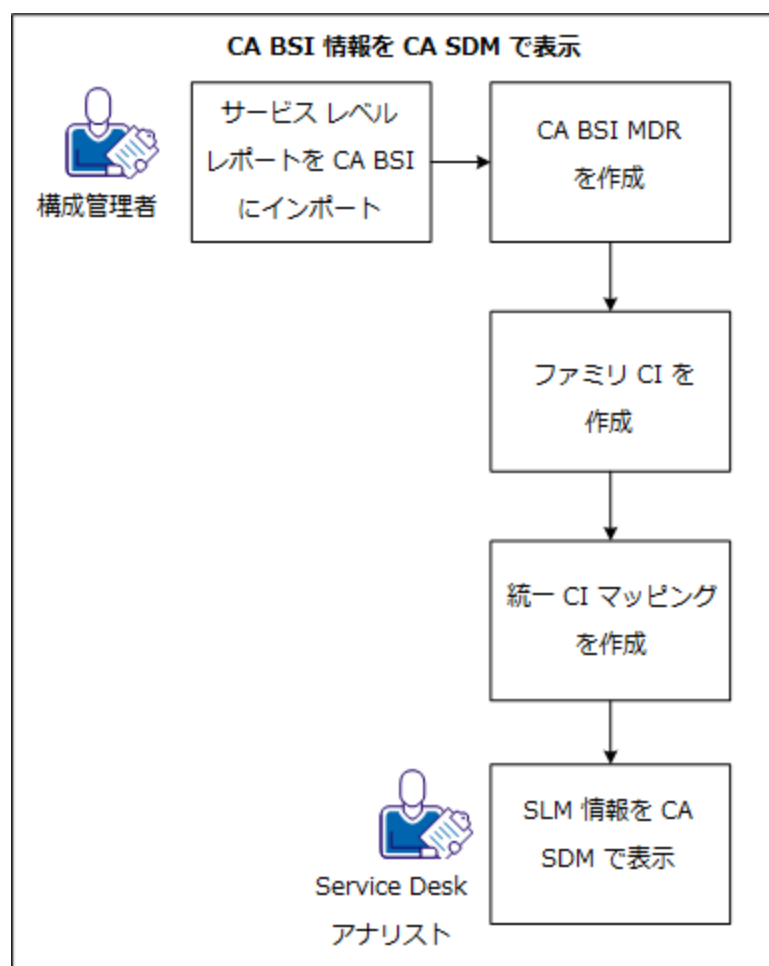
gen-delims = : / ? # [] @

sub-delims = ! \$ & ' () * + , ; =

CA SDM での CA BSI 情報の表示

IT サービスの変更の管理を改善したいと考えている組織が、CA BSI と CA SDM を統合することを決定したとします。統合を行うと、CA BSI は、サービス レベル管理 (SLM) 情報を CA SDM にエクスポートできるようになります。構成管理者は、レポートを CA BSI にインポートし、Service Desk アナリストが SLM 情報を表示できるように CA SDM を設定します。Service Desk アナリストは、この情報を活用して IT サービスの提供を改善します。

以下の図に、構成管理者が CA BSI を使用して SLM データを CA SDM にエクスポートして、Service Desk アナリストが SLM 情報を表示できるようにするための手順を示します。



1. [サービス レベル レポートを CA BSI にインポートします](#) (P. 730)。
2. [CA BSI MDR を作成します](#) (P. 730)。
3. [ファミリー CI を作成します](#) (P. 731)。

4. [統一 CI マッピングを作成します](#) (P. 732)。
5. [CA SDM で SLM 情報を表示します](#) (P. 733)。

サービス レベル レポートの CA BSI へのインポート

CA BSI は、デフォルトでサービス レベル準拠レポートを提供します。CA SDM の CI 詳細ページ [BSI サービス] タブが表示され、超過および違反の数が示されます。 *Modified Service Level by Metrics vs Target* および *Modified Service Level by Contract vs Target* レポートを CA BSI にインポートします。

次の手順に従ってください:

1. \$NX_ROOT/samples/BSI/bsireports.sql ファイルを CA BSI データベース サーバにコピーします。

この Oracle スクリプトには、CA BSI と CA SDM の統合に必要なレポート定義が含まれています。
2. SYSDBA 役割を持つユーザで CA BSI Oracle インスタンスに接続するか、またはデータベース所有者として接続します。

重要: このユーザは、データベースの更新権限を持っている必要があります。Oracle データベース管理者にこの権限が付与されていることを確認してください。

3. bsireports.sql スクリプトを実行し、エラーが発生しないことを確認します。

このレポートは、CA SDM 統合用に利用可能です。

CA BSI MDR の作成

構成管理者は、CA SDM で CA BSI 用の MDR を作成します。この MDR は、ホスト名や特権ユーザ ID など、CA BSI サーバに関する情報を提供します。

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] をクリックします。
3. 以下のサンプルデータを入力します。
 - クラス名として「BSI」と入力します。
 - ボタンおよび MDR 名のラベルを入力します。
たとえば、「BSI」と入力します。

- CA BSI サーバのホスト名を指定します。
- ユーザ ID として「sadmin」と入力し、共有秘密として「CA」と入力します。

注: この情報は、実際のユーザ名および組織によって異なります。
この情報については、CA BSI 管理者に確認してください。

- [コンテキストで起動する URL] フィールドのすべての内容を削除します。

4. [保存] をクリックしてウィンドウを閉じます。

CA SDM での CI の作成

CA SDM でエンタープライズ サービス CI および契約ファミリー CI を作成します。これらの CI は、CA SDM で表示する CA BSI データに対応しています。この例では、Service 1 および Contract 7 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] - [CI リスト] をクリックします。
2. [新規作成] をクリックします。
3. 以下の情報を入力します。
 - 名前として「**Service 1**」と入力します。
 - クラスとして「**Business Service**」と入力します。
4. [継続] をクリックします。
5. [保存] をクリックしてウィンドウを閉じます。
6. 以下の情報に基づいて別の CI を作成します。
 - 名前として「**Contract 7**」と入力します。
 - クラスとして「**License Agreement**」と入力します。
7. [継続] をクリックします。
8. [保存] をクリックしてウィンドウを閉じます。

統一 CI マッピングの作成

CA BSI と CA SDM の統合を完了するには、統一 CI マッピングを作成します。このマッピングにより、CI に関する情報が提供されます。この例では、Service 1 および Contract 7 を BSI MDR にマップします。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [MDR 管理] - [統一 CI マッピング] をクリックします。
2. [新規作成] をクリックします。
3. 以下のフィールドを指定します。
 - [構成アイテム名] と [統一アセット ID] として「**Service 1**」と入力します。
 - MDR 名として「**BSI**」と入力します。

重要: CA BSI にサービス名および契約名として同じ統一アセット ID を入力したことを確認します。
4. [保存] をクリックしてウィンドウを閉じます。
5. 別のマッピングを作成し、以下のフィールドに入力します:
 - [構成アイテム名] および [統一アセット ID] として **Contract 7** と入力します。
 - MDR 名として「**BSI**」と入力します。
6. [保存] をクリックしてウィンドウを閉じます。

CA SDM での SLM 情報の表示

Service Desk アナリストは、SLM 情報を参照して、組織内の IT サービスの変更を管理します。たとえば、Service 1 に関して発生した違反を分析できます。

次の手順に従ってください:

1. [管理] タブで、[CA CMDB] - [CI リスト] をクリックします。
2. CA BSI と統合したエンタープライズ サービスおよび契約ファミリー CI を検索します。
3. エンタープライズ サービス ファミリ CI を開き、BSI サービスおよび BSI サービス メトリックに関するタブを参照します。
4. [BSI サービス] をクリックして、CA BSI のサービス レベル準拠データから取得された超過および違反情報を参照します。

CA BSI の Service Level Compliance レポートから取得された、Service 1 の超過および違反データが表示されます。

5. [メトリックによる BSI サービス] をクリックして、CA BSI の Modified Service Level by Metric vs Target レポートから取得された、違反、準拠、およびターゲット情報を参照します。
6. CA BSI と統合した契約ファミリー CI を開き、[メトリックによる BSI 契約] タブをクリックします。

注: 契約 IC には、[メトリックによる BSI 契約] タブが含まれます。このタブに表示されるテキスト ボックスに契約当事者を入力して、CA BSI の Modified Service Level by Metric vs Target レポートから情報を取得します。

これで、CA BSI と CA SDM を統合して SLM 情報を CA SDM で参照できるようになりました。

第 14 章: samples ディレクトリ

このセクションには、以下のトピックが含まれています。

[samples ディレクトリのコンテンツ](#) (P. 735)

samples ディレクトリのコンテンツ

各種の外部インターフェースでできるように、`$NX_ROOT/samples` ディレクトリ内の複数のファイルを変更できます。これらのファイルは、さまざまなサブディレクトリにグループ化されています。`samples` ディレクトリ内のオリジナルファイルは実行可能ファイルではありません。

メッセージ カタログを変更する方法

メッセージ カタログを変更するには、以下の手順に従います。

1. `$nx_root¥bin` にある `pdm.xml` の形式を参照します。
2. `pdm.xml` のカスタマイズ コピーを作成し、`$nx_root¥msg_catalog` ディレクトリに配置します。
3. 前の手順から **XML** メッセージ ファイル内のメッセージを追加、変更、または追加して変更します。

call_mgt

リクエスト管理のカスタマイズに使用するサンプルが格納されています。

gencr.frg

このファイルと **bop_cmd** を組み合わせて使用すると、コマンドラインからリクエストを作成できます。すべての通知およびアクティビティログ エントリが発生しますが、リクエスト フォームが作成されてもサーバには表示されません。**bob_cmd** ユーティリティで **gencr.frg** を実行するには、**-u** パラメータを使用する必要があります。

gencr_readme.txt ファイルで構文および変更方法（必要な場合）を確認してください。このファイルは **\$NX_ROOT/site/mods/interp** に格納されますが、このディレクトリが存在しない場合は、作成する必要があります。例：**bop_cmd -d domsrvr -u nsm -f gencr.frg "gencr('My Description')"**

iss_site.mod

このファイルを使用すると、案件でサイトに適合したフィールドのアクティビティ ログを有効にできます。このファイルは、サイトに適合したフィールドに応じて変更された後、**\$NX_ROOT/site/mods/majic** に格納されます。

cr_site.mod

このファイルを使用すると、リクエストでサイトに適合したフィールドのアクティビティ ログを有効にできます。このファイルは、サイトに適合したフィールドに応じて変更された後、**\$NX_ROOT/site/mods/majic** に格納されます。

chg_site.mod

このファイルを使用すると、変更要求でサイトに適合したフィールドのアクティビティ ログを有効にできます。このファイルは、サイトに適合したフィールドに応じて変更された後、**\$NX_ROOT/site/mods/majic** に格納されます。

gencr_readme.txt

このファイルには、**gencr.frg** ファイルの使用方法が記載されています。

chg_site.spl

このファイルを変更すると、リクエストから変更要求を作成する場合の属性のマッピングを変更できます。このファイルは、変更された後、**\$NX_ROOT/site/mods/majic** に格納されます。

audlog_site.mod

このファイルを使用すると、サイトに適合したフィールドの監査ログを有効にできます。このファイルは、サイトに適合したフィールドに応じて変更された後、`$NX_ROOT/site/mods/majic` に格納されます。

Notify_add.spl (UNIX のみ)

このファイルを使用すると、リクエストのログ エージェント、担当者、およびグループをリクエスト通知リストに追加できます。このファイルは `$NX_ROOT/site/mods/majic` に格納されます。

Notify_replace.spl (UNIX のみ)

このファイルを使用すると、リクエストのログ エージェント、担当者、およびグループを、変更後にリクエスト通知リストに追加できます。このファイルは `$NX_ROOT/site/mods/majic` に格納されます。

data

このディレクトリには、**CA SDM** 内のほとんどのデータベース テーブル用の論理データ モデルを記述するファイルが格納されています。また、このデータ ディレクトリには ナレッジ マネジメント 用のサンプルデータも格納されています。

macro_lock

このファイルには、マクロによって設定されたロックを解除するために `bop_cmd` を使用して実行できる `spel` フラグメントが含まれています。

multi-tenancy

このディレクトリには、マルチテナンシーを管理するためのサンプルファイルが格納されています。

関連項目:

[既存のテナント実装をテナント オブジェクトに変換する方法 \(P. 379\)](#)
[テーブル内のテナント属性に値を入力する方法 \(P. 380\)](#)

pdmconf

web.xml.tpl
pdm_startup.tpl
pdm_edit_usage_notes.htm
alias_install.bat
web.cfg.tpl
pdm_startup.i.tpl
pdm_edit.pl
README_files

これらのファイルはすべて、各種のデーモンを実行するように設定されたプライマリ サーバとセカンダリ サーバの起動ファイルを作成するために、`pdm_edit.pl` で使用されます。

reporting

このディレクトリには、オフライン レポートを設定するためのドキュメントおよびサンプルが格納されています。

関連項目：

[オフライン レポート用の複製されたデータベース](#) (P. 313)

sdk

このディレクトリには、CA SDM の SOAP Web サービス コールの作成に使用するサンプル ファイルが格納されています。

TableOfContents.doc に使用可能なサンプルの詳細が説明されています。このファイルは、以下のディレクトリにあります。

`$NX_ROOT¥samples¥sdk¥websvc`

PKI_loginServiceManaged_JAVA_steps.doc および
PKI_loginServiceManaged_PERL_steps.doc では、デジタル証明書によるログイン用に ServiceDesk を設定する方法が説明されています。このファイルは、以下のディレクトリにあります。

`$NX_ROOT¥samples¥sdk¥websvc¥java¥test1_pki`

以下は、PERL および JAVA サンプルの例と場所です。

- PERL サンプル

`$NX_ROOT¥samples¥sdk¥websvc¥perl¥test1_pki`

例 : loginServiceManaged() Web サービス コール

- Java サンプル

`$NX_ROOT¥samples¥sdk¥websvc¥java¥test1_pki`

例 : loginServiceManaged() および getBopsid() Web サービス コール

`$NX_ROOT¥samples¥sdk¥websvc¥java¥test2_basic`

例 : Combined CreateRequest() および CreateChangeOrder() を結合した Web サービス コール

views

このディレクトリには、マイグレーション、マルチテナンシー管理などのプロセス用のデータベース スクリプトが格納されています。

関連項目 :

[データベースに関する考慮事項 \(P. 33\)](#)

[マルチテナンシーを実装する方法 \(P. 354\)](#)

第 15 章：補足コンテンツのロード

このセクションには、以下のトピックが含まれています。

[sd_content.dat](#) (P. 741)

sd_content.dat

CA SDM の補足コンテンツは `sd_content.dat` にあります。このデータ ファイルには、変更カテゴリおよび根本原因のレコードが含まれています。コマンド ウィンドウからデータをロードするには、`$NX_ROOT/data` に移動して以下のコマンドを実行します。

```
pdm_load -f sd_content.dat
```