CA Identity Manager

管理ガイド

r12.5

本書及び関連するソフトウェア ヘルプ プログラム（以下「本書」と総称）は、ユーザへの情報提供のみを目的とし、CA はその内容を予告なく変更、撤回することがあります。

CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、複製、開示、修正、複製することはできません。本書は、CA または CA Inc. が権利を有する秘密情報であり、かつ財産的価値のある情報です。ユーザは本書を開示したり、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使用することはできません。

上記にかかわらず、本書に記載されているソフトウェア製品に関連して社内でユーザおよび従業員が使用する場合に限り、該当するソフトウェアのライセンスを受けたユーザは、合理的な範囲内の部数の本書の複製を作成できます。ただし CA のすべての著作権表示およびその説明を各複製に添付することを条件とします。

本書のコピーを作成する上記の権利は、ソフトウェアの該当する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、そのライセンスが終了した場合には、ユーザは CA に本書の全部または一部を複製したコピーをすべて CA に返却したか、または破棄したことを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 は本書を現状有姿のまま提供し、商品性、お客様の使用目的に対する適合性、他者の権利に対する不侵害についての黙示の保証を含むいかなる保証もしません。 また、本書の使用に起因し、逸失利益、投資の喪失、業務の中断、営業権の損失、データの損失を含むがそれに限らない、直接または間接のいかなる損害が発生しても、CA はユーザ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。

本書に記載されたソフトウェア製品は、該当するライセンス契約書に従い使用されるものであり、該当するライセンス契約書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。

本書の制作者は CA および CA Inc. 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 Section252.227-7014(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 © 2009 CA. All rights reserved. 本書に記載された全ての商標、商号、サービスマークおよびロゴは、それぞれ各社に帰属します。

CA 製品リファレンス

このマニュアルでは、以下の CA 製品について説明します。

- CA Identity Manager
- CA SiteMinder® Web Access Manager
- CA Directory
- CA Enterprise Log Manager
- CA Role & Compliance Manager

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: ロールの計画 17

ロールの決定 17
ロールの種類 17
ロールの目的 18
委任管理者 18
委任の手順 19
委任の例 20
ロールの特性 20
ロール プロファイル 21
ロールのタスク 21
アカウント テンプレート 22
メンバ ルール、管理ルール、および所有者ルール 22
スコープ ルール 23
ルールの一般的なガイドライン 27
アクションの追加および削除 27
メンバ ポリシー 28
管理ポリシー 29
ロールの計画のチェックリスト 30

第 2 章: 管理ロール 31

管理ロールと管理タスク 31
管理ロールと Identity Manager 環境 31
管理ロールとユーザ コンソール 32
新規管理ロールの作成 32
管理ロールの新規作成 33
管理ロールのプロファイルの定義 33
ロールの管理タスクの選択 34
管理ロールのメンバ ポリシーの定義 35
管理ロールの管理ポリシーの定義 36
管理ロールの所有者ルールの定義 37
管理ロールの確認 37
ユーザによるロールの自己割り当ての許可 37

第 3 章: 管理タスク 39

管理タスクの計画 39
管理タスクの例 40
管理タスクの使用法オプション 43
デフォルトの管理タスク 44
カスタム管理タスクの作成方法 45
タスクのプロファイルの定義 46
管理タスクの[プロファイル]タブ 47
ロールのユーザ定義のカスタム属性 50
タスク スコープの定義 53
検索画面設定 54
タスクのタブの選択 61
[アカウント]タブ 62
[スケジュール]タブ 64
タスクのフィールドの表示 65
使用しているロールの表示 65
イベントへのワークフロー プロセスの割り当て 65
Active Directory の前提条件 66
sAMAccountName 属性 66
グループのタイプとスコープ 66
アプリケーション機能の外部タスク 68
外部タブ 68
[外部 URL]タブ 69
高度なタスク コンポーネント 70
ビジネス ロジック タスク ハンドラの作成 70
管理タスクおよびイベント 72
プライマリ イベントおよびセカンダリ イベント 72
タスクのイベントの表示 73
未変更のプロファイルに生成されるイベント 73
管理タスクの処理 74
同期段階の処理 75
非同期段階の処理 75

第 4 章: セルフサービス タスク 79

CA Identity Manager のセルフサービス タスク 79
自己管理ロールへのアクセス制限 80
セルフサービス タスクへのアクセス 80
企業の Web サイトへのセルフサービス リンクの埋め込み 81
複数のセルフサービス タスクの設定 82

第 5 章: ユーザ 85

ユーザの作成 85
ユーザの管理 86
ユーザの変更 86
エンドポイント アカウントの表示または変更 87
ユーザへのロールの割り当て 88
[ロール メンバ/管理者の変更]タスクでのロールの割り当て 88
[ユーザの変更]タスクでのロールの割り当て 89

第 6 章: パスワード管理 91

CA Identity Manager のパスワード管理 91
パスワード ポリシー 92
パスワード ポリシーの作成 93
正規表現の指定 93
パスワード ポリシーの管理 95
パスワード構成の設定 96
高度なパスワード オプションの設定 98
SiteMinder と組み合わせたパスワード ポリシー 99
パスワードのリセットまたはアカウントのロック解除 109
GINA または Credential Provider のインストール 109
GINA の設定 110
クレデンシャル プロバイダの設定 112
レジストリの設定 113
Windows ログイン用パスワードのリセット 116
パスワードの同期 116
パスワード同期エージェントのインストール 117
パスワード同期エージェントが機能するしくみ 120
アカウントレベルのパスワード品質チェック 121
パスワード品質の実施 122
パスワード同期の設定 122
フェイルオーバ 122
ログ メッセージの有効化 123
インストールの確認 123

第 7 章: グループ 125

静的グループの作成 125
動的グループの作成 126
動的グループ クエリのパラメータ 127

ネスト グループの作成 129
静的グループ、動的グループ、ネスト グループの例 131
グループ管理者 132

第 8 章: 管理対象のエンドポイント アカウント 135

ユーザの複数アカウント 135
Identity Manager ユーザ 136
グローバル ユーザ 136
エンドポイント システムのアカウント 136
ユーザへのエンドポイント アカウント付与 137
CA Identity Manager でエンドポイントを設定する方法 137
エンドポイント タイプの定義 138
ユーザ コンソールでエンドポイントを作成します。 139
エンドポイントの検索および関連付け 139
エンドポイントのカスタム属性の拡張 142
アカウント タスク 143
プロビジョニング済みアカウントの作成 144
例外アカウントの作成 144
孤立アカウントの割り当て 145
システム アカウントの割り当て 145
エンドポイント アカウントの削除 146
エンドポイント アカウントのパスワード変更 147
複数のアカウントに対するアクションの実行 147
詳細なアカウント操作 148
アカウントに対するグローバル ユーザの変更 148
自動検索が機能するしくみ 149
アカウントの削除 150
削除保留の使用 151
削除されたアカウントの再作成 151

第 9 章: プロビジョニング ロール 153

プロビジョニング ロールとアカウント テンプレート 153
ロールおよびテンプレート タスク 154
プロビジョニング ロールの作成 154
プロビジョニング ロールのインポート 155
プロビジョニング ロールへの新規所有者の割り当て 156
アカウント テンプレートの作成 157
プロビジョニング ロールによって作成されたアカウントのパスワード 157

プロビジョニング ロール イベントの処理順序 158
アカウント テンプレートの属性 161
機能と初期属性 161
属性のルール文字列 162
属性の値 164
詳細なルール式 164
ルールの文字列と値の組み合わせの使用 165
ルールのサブストリング 165
複数値のルール式 166
明示的なグローバル ユーザ属性ルール 168
組み込みルール関数 168
プロビジョニング ロールのパフォーマンス 170
JIAM オブジェクト キャッシュ 171
セッション プーリング 172
既存環境用のプロビジョニング タスク 172

第 10 章: 同期 173

サーバ間のユーザの同期 173
インバウンド同期 173
プロビジョニング マネージャ操作のステータス 173
インバウンド同期のフェールオーバ 174
アウトバウンド同期 174
パスワード同期の有効化 176
ユーザの作成または変更タスクにおけるユーザの同期 176
プロビジョニング マネージャでの同期 177
グローバル ユーザで同期がずれる理由 179
グローバル ユーザ同期 179
ユーザ同期のチェック 182
グローバル ユーザまたはロールの同期 182
アカウント テンプレート同期 183
アカウントの同期 187

第 11 章: アイデンティティ ポリシー 191

アイデンティティ ポリシー 191
アイデンティティ ポリシー セットの計画ワークシート 192
アイデンティティ ポリシー セットの作成 193
アイデンティティ ポリシー セットのプロファイルの定義 193
ポリシー セット メンバ ルールの作成 194

アイデンティティ ポリシーの作成 194
アイデンティティ ポリシー セットの所有者の指定 203
アイデンティティ ポリシー セットの管理 203
ユーザとアイデンティティ ポリシーとの同期の方法 204
自動的なユーザ同期の設定 205
手動によるユーザの同期化 206
ユーザ同期化の確認 207
Identity Manager 環境のアイデンティティ ポリシー セット 208
例: ユーザ属性を自動的に追加する 208
例: リソースおよび権限付与の割り当て 209
例: コンプライアンスの適用 210
例: 職務の分離の実行 211

第 12 章: CA Role & Compliance Manager 統合 213

CA Role & Compliance Manager の統合 213
Smart Provisioning 214
CA Identity Manager および CA RCM の通信方法 214
共有情報 217
動的通知 218
CA RCM ロール モデル 218
CA RCM との統合を設定する方法 219
CA RCM 統合の前提条件 221
CA RCM で接続を設定する方法 221
CA Identity Manager で接続を設定する方法 236
CA RCM 内の CA Identity Manager データ分析 243
コネクタ ジョブの定義 244
コネクタ ジョブの実行とスケジュール 247
コネクタ ジョブを監視する方法 247
サジェストされたプロビジョニング ロール 247
サジェスト ロールの条件 250
サジェスト ロールの表示 252
プロビジョニング ロールのスコア 253
[サジェストされたプロビジョニング ロール]のデフォルト設定 254
コンプライアンス メッセージおよびパターン メッセージ 258
コンプライアンス メッセージ 258
パターン メッセージ 259
メッセージの種類 261
承認タスク内のコンプライアンスおよびパターン メッセージ 262
コンプライアンス メッセージとパターン メッセージの履歴 263

コンプライアンスおよびパターン メッセージ サポートの設定方法 263

第 13 章: CA Enterprise Log Manager 統合 269

CA Enterprise Log Manager の機能 269
CA Enterprise Log Manager コンポーネント 270
統合の制限 270
CA Enterprise Log Manager を CA Identity Manager に統合する方法 270
追加の CA Enterprise Log Manager リポートまたはクエリの CA Identity Manager への統合 280
[Enterprise Log Manager ビューア]タブの設定 281

第 14 章: タスク永続性 283

自動化されたタスクの永続ガベージ コレクションとアーカイブ 283
[反復]タブ 284
[サブミット済みタスクのクリーンアップ]タブ 285
ジョブの即時実行 286
[新規ジョブのスケジュール] 286
既存のジョブの変更 287
[反復タスクの削除] 287
タスク永続性データベースの移行方法 288
tpmigration125.properties ファイルの更新 289
JAVA_HOME 変数の設定 289
runmigration ツールの実行 290

第 15 章: コンプライアンスのサポート 291

CA Identity Manager でのコンプライアンスのサポート 291
ユーザ資格の認証 291
認証プロセスのしくみ 292
ユーザ認証の設定方法 292
ユーザ認証プロセスの開始 297
確認通知の送信 297
[ユーザの認証]タスクの使用 298
認証プロセスの終了 298

第 16 章: レポート 299

概要 299
スナップショット レポートを実行する方法 300
レポートの設定 301

スナップショット データベース接続の作成 302
スナップショット定義の作成 302
スナップショット データのキャプチャ 310
スナップショット定義とレポート タスクの関連付け 311
接続のレポート タスクへの関連付け 312
レポートのリクエスト 312
レポートの表示 313
スナップショット以外のレポートの実行方法 314
レポートの設定 315
レポート用の接続の作成 316
接続のレポート タスクへの関連付け 316
レポートのリクエスト 317
レポートの表示 319
レポート オプションの設定 320
カスタム レポートの作成および実行方法 321
Crystal Reports でのレポートの作成 321
レポート パラメータ XML ファイルの作成 322
レポートとレポート パラメータ XML ファイルのアップロード 326
レポート タスクの作成 327
デフォルトのレポート 331

第 17 章: ワークフロー 335

ワークフローの概要 335
WorkPoint プロセス図 336
ワークフローと電子メール通知 336
WorkPoint のマニュアル 337
Workflow の制御メソッド 338
ワークフローを有効にする方法 339
WorkPoint 管理ツールの設定 339
JBoss における WorkPoint Administrative Tool の設定 340
WebLogic における WorkPoint 管理ツールの設定 341
WebSphere における WorkPoint 管理ツールの設定 343
WorkPoint Designer の開始 344
テンプレート メソッド 345
プロセス テンプレート 345
テンプレート メソッドの使用方法 349
タスクおよびイベント 349
参加者リゾルバ: テンプレート メソッド 356
ワークフロー例: ユーザの作成 362

WorkPoint メソッド 364
WorkPoint メソッドの使用方法 364
WorkPoint プロセス 365
ワークフロー アクティビティ 370
参加者リゾルバ: WorkPoint メソッド 372
WorkPoint Designer のプロセス 382
ジョブとプロセス インスタンス 385
ワークフロー アクティビティの実行 387
ワークフロー サーバによるアクティビティの完了 388
Workpoint ジョブの表示 389
既存の[承認]タブへの[ジョブの表示]タブの追加 390
承認タスクにおける[ジョブの表示]タブの表示 391
イベント レベル ワークフローのワークフロージョブの表示 391
タスク レベル ワークフローのワークフロー ジョブの表示 391
ポリシーベース ワークフロー 392
デフォルトのワークフロー プロセス 392
ポリシー順序 393
ルールのオブジェクト 394
ルールの評価 395
ポリシーの例 396
ポリシーベース ワークフローの設定方法 397
承認ポリシーの設定方法 398
ポリシーベースのワークフロー ステータス 399
オンライン リクエスト 400
オンライン リクエスト タスク 400
オンライン リクエスト プロセス 402
オンライン リクエスト履歴 403
オンライン リクエストの使用 403
ワークフロー アクション ボタン 404
承認タスクのワークフロー ボタン 405
Identity Manager でのボタン設定 406
ワークフロー アクション ボタンの追加 407
ワーク リストと作業アイテム 409
ワーク リストの表示 410
作業アイテムの保留 411
作業アイテムの委任 412
作業アイテムの再割り当て 416

第 18 章: 電子メール通知 421

CA Identity Manager の電子メール通知 421
SMTP の設定 421
JBoss 上での SMTP の設定 422
WebLogic 9.2 での SMTP の設定 423
WebSphere 上での SMTP の設定 423
電子メール通知の有効化 424
電子メールを送信するためのイベントまたはタスクの設定 425
電子メールのコンテンツ 426
電子メール テンプレート 427
テンプレート ディレクトリ 429
電子メール テンプレートの作成 430
電子メールのカスタム テンプレート 430
テンプレートのエレメント 431
Identity Manager タグの拡張 432
電子メール テンプレート API 433
追加のメソッド 445
Javadoc リファレンス 448
電子メール テンプレートの展開 448
テンプレート セット 448
テンプレート名 449

第 19 章: アクセス ロール 451

CA Identity Manager のアクセスロール 451
アクセスロールが権限を管理する方法 451
例: 間接的なプロファイル属性の変更 452
アクセス ロールの作成 453
アクセス ロールの作成の開始 453
アクセス ロールのプロファイルの定義 453
アクセス ロールのメンバ ポリシーの定義 454
アクセス ロールの管理ポリシーの定義 454
アクセス ロールの所有者ルールの定義 455

第 20 章: システム タスク 457

デフォルトのシステム タスク 458
Identity Manager のタスク ステータス 458
Identity Manager がタスク ステータスを判別するしくみ 460
[サブミット済みタスクの表示]タブ 461

サブミット済みタスクの検索 462
［タスクの詳細の表示］ 465
イベントの詳細の表示 466
［サブミット済みタスクの表示］タブのカスタマイズ 467
［ユーザ履歴］タブ 470
ユーザ履歴の表示に関する検索属性 471
［ユーザ履歴］タブのカスタマイズ 472
ユーザ アクティビティの表示タスク 475
Bulk Loader 476
Bulk Loader タスクの管理ロールへの追加 476
Bulk Loader の使用法 477
フィーダ タスクに関する電子メール通知の有効化 480
［Bulk Loader］タスクのスケジュール 480
「Bulk Loader」の解析ファイルの変更 481
Bulk Loader の Web サービス サポート 481
Bulk Loader のメモリに関する注意事項 482
セレクト ボックス データ 482
ロジカル アトリビュート ハンドラ 483
ロジカル アトリビュート ハンドラの作成 484
ロジカル アトリビュート ハンドラのコピー 484
ロジカル アトリビュート ハンドラ ForgottenPasswordHandler の作成 485
ロジカル アトリビュート ハンドラの削除 486
ロジカル アトリビュート ハンドラの変更 486
ロジカル アトリビュート ハンドラの表示 486
JDBC 接続管理 487
JDBC 接続の作成 487
サブミット済みタスクのクリーンアップ 487
［反復］タブ 488
［サブミット済みタスクのクリーンアップ］タブ 491
反復タスクの削除 491
Enterprise Log Manager 接続の設定 492
Enterprise Log Manager 接続の削除 493

付録 A: デフォルトのタスクとロール 495

デフォルトのセルフサービス タスク 495
自己登録 495
忘れたパスワード 495
忘れたパスワードのリセット 496
忘れたユーザ ID 496

パスワードサービス 496
デフォルトの管理タスク 496
ホーム 497
管理ロール 499
認証 501
グループ 502
組織 504
ポリシー 505
プロビジョニング ロール 507
レポート 508
システム 508
ユーザ 510
デフォルトの管理ロール 512
アクセス ロール マネージャ 513
管理ロール マネージャ 513
認証プロセス マネージャ 514
認証マネージャ 514
委任マネージャ 514
グループ マネージャ 515
組織マネージャ 515
パスワード マネージャ 516
プロビジョニング ロール マネージャ 516
プロビジョニング同期マネージャ 516
セキュリティ マネージャ 517
自己委任 517
自己マネージャ 517
System Manager 518
ユーザ マネージャ 518
デフォルトのワークフロー承認ロール 519

索引 521

第 1 章: ロールの計画

ロールを計画するには、業務および組織でどのようなロールが必要か、ユーザおよびユーザのアプリケーション アクセスの管理をどのように委任するか、について決定します。 これらの決定事項に基づいて、各ロールの特性を決めていきます。

このセクションには、以下のトピックが含まれています。

ロールの決定 (17 ページ)
委任管理者 (18 ページ)
ロールの特性 (20 ページ)
ロールの計画のチェックリスト (30 ページ)

ロールの決定

以降のセクションには、有用なロールの決定を行ううえで役に立つ情報が記載されています。

ロールの種類

必要なロールの種類を決定するには、以下のテーブルを参照します。

ロールの種類	目的
管理ロール	Identity Manager ユーザ コンソールで実行するタスクが含まれます。 ■ 管理タスク。ユーザ、組織、グループ、ロール、タスクの管理に使用します。 ■ 外部タスク。レポーティング アプリケーションへのユーザ属性の通知など、ビジネス アプリケーションで機能します。
プロビジョニング ロール	電子メール システムなど、管理対象エンドポイントに存在するアカウントを定義するアカウント テンプレートが含まれます。 アカウント テンプレートでは、ユーザ属性とアカウントのマッピング方法も定義できます。
アクセス ロール	アクセス ロールを使用すると、CA Identity Manager または他のアプリケーションの権限を付与することができます。

Identity Manager 環境のロールを管理します。この環境は、ユーザ、グループ、組織、および関連付けられたタスクとロールを管理する管理ネームスペースのビューです。Identity Manager 環境を作成するには、「CA Identity Manager Configuration Guide」を参照してください。

管理ロールは、すべての Identity Manager 環境で必要です。 プロビジョニング ロールは、既存のユーザに追加のアカウントを割り当てる場合に必要です。 アクセス ロールは、CA Identity Manager または他のアプリケーションに追加の権限を付与する場合に必要です。

ロールの目的

ロールを有効に使用するには、ユーザのニーズと管理者の職責における以下のような質問について考えておく必要があります。

- どの部門および組織に管理対象のユーザがいるか。
- 管理対象エンドポイントで、ユーザはどのようなアカウントを追加で必要としているか。
- どのユーザを他のユーザの管理者とするか。
- 誰が管理者を管理するか。
- 各ロールで必要な管理タスクとアクセス タスクは何か。
- 誰がロールとタスクを作成するか。
- どのようにすれば、ロールを使用して作業を委任できるか。

  最後の質問は、ユーザの管理業務とアプリケーションへのアクセス付与業務の共有に関するものです。 委任モデルの詳細については、「委任された管理（18 ページ）」を参照してください。

上記の質問の回答に基づいて、必要なロールの数と種類を決定します。

委任管理者

Identity Manager のユーザとして、ユーザとアプリケーションへのユーザ アクセスを個人で管理することも、その作業を委任することもできます。 管理権限の委任とは、ロールを使用して、ユーザ管理とアプリケーションへのアクセス権付与の作業を共有することです。

管理権限の委任では、各ロールにルールが含まれており、どのユーザが以下の図の機能を実行するかが記述されています。

機能	定義
ロール所有者	ロールを変更する
ロール管理者	ユーザおよび他のロール管理者へロールを割り当てる
ロール メンバ	ロールを使用して管理を実行したり、タスクにアクセスしたりする

これらの機能をユーザ間で分担することで、下位レベルの管理者にユーザ管理を、高位レベルの管理者にロールの割り当てと変更を委任することができます。

注意: 管理者は、ロールの割り当て、または管理ロールの使用が可能な Identity Manager ユーザです。 ユーザ は Identity Manager のユーザで、管理ロールまたはアクセス ロール、あるいはその両方を持つことができます。

プロビジョニング ロールに対しては、管理者ルールおよび所有者ルールを作成して、管理を委任することができます。 ただし、Identity Manager では、プロビジョニング ロールに対してメンバ ルールを作成できません。 代わりに、プロビジョニング ロール メンバ/管理者の変更を使用して、ルール メンバを追加または削除します。

委任の手順

「ロールの目的」に基づいてロールの使用を決定すると、次のように委任管理が発生します。

1. 誰がロールの所有者、管理者、またはメンバであるか、というルールを使用して、管理者がロールを作成します。
2. ロールの所有者は、変更が必要になったときにロールを変更します。
3. ロール管理者
   - 追加のロール管理者を割り当てます(オプション)。
   - 追加のロール メンバを割り当てます(オプション)。

   ユーザの中には、ロールで定義されているルールを満たしており、すでにロール管理者またはメンバである人もいます。

4. ロール メンバは次のロールを使用します。
   - 管理ロールのメンバは、Identity Manager 環境において、ユーザおよび他のオブジェクトを管理します。
   - アクセス ロールのメンバは、ビジネス アプリケーションの機能を実行します。
   - プロビジョニング ロールのメンバは、そのロールのポリシーで定義されているアカウントを使用します。

委任の例

誰がメンバまたは管理者になれるかを決めるルールを使用して、ロール作成することができます。 次に、そのロールを割り当てて、(対象のルールを満たしていない)他のユーザが、ロールのメンバまたは管理者になることができるようにします。

次に例として、エンド ユーザのビジネス アプリケーション権利を管理している管理者について考えてみましょう。

- Jeff は Accountant ロールに関するロール所有者であり、ロールで変更が必要な場合は、Jeff がロールを変更します。
- David と Lisa は、そのロールのロール管理者です。 彼らは、ロール メンバとして地域のユーザを割り当てます。
- 他のユーザは、ロール メンバとして割り当てられていないロール メンバです。 ただし、これらのメンバは、ロール メンバであるというルールを満たしています。

  ロール メンバは Accountant ロールを使用して発注を行い、財務アプリケーションでその他のタスクを実行します。

「ロールの特性」のセクションでは、ロールのルールについて、および他の特性について詳しく説明しています。

ロールの特性

ロールを作成すると、以下の表に示す特性を定義することができます。

特性	定義
ロールのプロファイル	ロールの一般的な特性。
タスク	管理ロールのタスク。
アカウント テンプレート	プロビジョニング ロールの管理対象エンドポイントのアカウントを定義するテンプレート。

特性	定義
メンバ ルール、 メンバ ポリシー	ユーザがロール メンバであるための条件を定義したメンバ ルール。 メンバ ポリシーは、メンバ ルールをスコープ ルールと組み合わせたものです。 **注**: プロビジョニング ロールには、メンバ ルールとメンバ ポリシーはありません。 ユーザをメンバにするには、[プロビジョニング ロール メンバ/管理者の変更]を使用します。
管理ルール、 管理ポリシー	■ 管理ルールは、ユーザがロール管理者であるための条件を定義します。 ■ 管理ポリシーは、ロールを割り当てるために、管理ルールをスコープ ルールと管理者権限に組み合わせたものです。
所有者ルール	ユーザがロール所有者であるための条件。
スコープ ルール	ロールによって管理されるオブジェクトの制限。
アクションの追加、 アクションの削除	ロール メンバまたは管理者としてユーザが追加または削除された場合の、ユーザプロファイルに対する変更です。

これらの特性については、以下のセクションで説明します。

ロール プロファイル

ロール プロファイルは、ロールの名前と説明、およびそのロールが有効であるかどうかを表します。 ロールが有効になっていると、ロールを作成してすぐに使用することができます。

ロールのタスク

管理ロールでは、1 つ以上の管理タスク(外部タスクなど)を、1 つ以上のカテゴリから選択できます。

アカウント テンプレート

各プロビジョニング ロールには、アカウント テンプレートが含まれています。 ここで、管理対象エンドポイントに存在するアカウントを定義できます。 たとえば、Exchange アカウントのエンドポイントでは、メールボックスのサイズを定義できます。 アカウント テンプレートでは、ユーザ属性とアカウントのマッピング方法も定義できます。

エンドポイントのタイプごとに、1 つ以上のエンドポイントを選択できます。 ロールが割り当てられているユーザは、エンドポイントのアカウントを受け取ります。

メンバ ルール、管理ルール、および所有者ルール

各ロールには、そのロールのメンバ、管理者、所有者になる資格に関するルールが含まれます。 したがって、ユーザは 1 つ以上のロールのメンバになることも、どのロールのメンバにもならないこともあります。

メンバ ルール、管理ルール、および所有者ルールでは、以下の表に示す条件が使用されます。

ルールの条件	例	ルールの構文
ユーザはいずれかの属性値と一致する必要があります。	役職の最初に「上級」が付くユーザ	条件 <ユーザ フィルタ>
ユーザは複数の属性値と一致する必要があります。	役職がマネージャ、地域が東部のユーザ	条件 <ユーザ フィルタ>
指定した組織にユーザが所属していなければなりません。	販売部門以下の組織内のユーザ	内<組織ルール>
ユーザは、組織の属性により指定される条件に適合する組織に所属する必要があります。	ビジネス タイプがゴールドまたはプラチナの組織に所属するユーザ	in organizations where <組織フィルタ>
ユーザは、指定された組織に所属し、特定のユーザ属性値と一致する必要があります。	役職がマネージャ、地域が東部で、販売またはマーケティング組織に所属するユーザ	条件 <ユーザ フィルタ> および所属組織 <組織ルール>
ユーザは特定のグループに所属する必要があります。	401K グループのメンバであるユーザ	who are members of group <グループ>

ルールの条件	例	ルールの構文
ユーザはロールのメンバである必要があります。	ヘルプ デスク ロールのメンバであるユーザ	以下のメンバである <ロール ルール>
ユーザはロールの管理者である必要があります。	セールス マネージャ ロールの管理者であるユーザ	以下の管理者である<ロール ルール>
ユーザはロールの所有者である必要があります。	ユーザ マネージャ ロールの所有者であるユーザ	以下の所有者である<ロール ルール>
ユーザは、グループの属性により指定される条件を満たすグループに所属している必要があります。	所有者が CIO のグループのメンバであるユーザ	who are members of group <グループ フィルタ>
ユーザは LDAP クエリに基づいた条件を満たす必要があります。	(Identity Manager ユーザ コンソールで作成されたクエリが不十分である場合は、LDAP ディレクトリを使用します)	クエリ ldap_query により返されたユーザ

一部のルールでは、値を複数値属性と比較する場合があります。 ルールを適用するには、複数値属性の少なくとも 1 つの値がルールに適合する必要があります。 たとえば、ルールが属性 A = 1 の場合、ユーザ X の属性 A の値が 1、2、3 であれば、ユーザ X は基準を満たしています。

ロールを作成するユーザが、ロールを変更できない場合があります。 ロールを変更できるようにするには、対象のユーザが所有者ルールの条件を満たすようにする必要があります。

注: 大規模な実装環境では、メンバ、管理、および所有者ルールを評価するのにかなりの時間を要することがあります。 ユーザ属性を含むルールに対する評価時間を短縮するには、メモリ内評価オプションを有効にします。 詳細については、「Configuration Guide」を参照してください。

スコープ ルール

メンバ ルールおよび管理ルールをスコープ ルールと組み合わせます。 スコープ ルールは、ロールが使用できるオブジェクトを制限します。

- ロール メンバのスコープ ルールは、ロールで管理できるオブジェクトを管理します。
- ロール管理者のスコープ ルールは、ロール メンバおよび管理者になることができるユーザを管理します。

オブジェクトには、タスクのプライマリ オブジェクトと任意のセカンダリ オブジェクトがあります。 たとえば、[ユーザの作成]タスクには、ユーザのプライマリ オブジェクト、およびグループのセカンダリ オブジェクトを持つ[グループ]タブが用意されています。

ほとんどのオブジェクト タイプに対して、以下の表のとおり、スコープ ルールのタイプを指定できます。

ルールの条件	例	ルールの構文
すべて	ロール メンバは、全オブジェクトを管理可能	すべて
オブジェクトは、1 つ以上の属性値に一致する必要があります。	役職の最初に「上級」が付くユーザ	where <フィルタ>

フィルタ オプションを選択すると、CA Identity Manager では、2 つのフィルタのタイプが表示されます。

<属性> <コンパレータ><値>

オブジェクトのプロファイルの属性は、指定された値と一致する必要があります。

<属性> <コンパレータ> 管理者の <ユーザ属性>

オブジェクトのプロファイルの属性は、管理者のプロファイル上の属性と一致する必要があります。 例: where マネージャ = 管理者の ID であるユーザ

以下の表で示されている追加オプションは、ユーザ オブジェクト、グループ オブジェクト、および組織オブジェクトで使用できます。

注: 以下は、ユーザ スコープ ルールの例を示しています。 その他のルールを作成して、管理者と、管理者が管理できるユーザとの間のさまざまな関係に対応できます。

ルールの条件	例	ルールの構文
ユーザはいずれかの属性値と一致する必要があります。	where 販売グループのメンバ、または携帯電話が null ではないユーザ	条件 <ユーザ フィルタ>
ユーザは複数の属性値と一致する必要があります。	where 役職 = マネージャ、かつ地域 = USA であるユーザ	条件 <ユーザ フィルタ>
指定した組織にユーザが所属していなければなりません。	オーストラリアまたはニュージーランドの組織に所属しているユーザ **注**: 組織スコープ ルールは、ルールに沿う組織の下位組織に適用され	内<組織ルール>

ルールの条件	例	ルールの構文
	ます。 たとえば、組織ルールが「Organization1 内」の場合、スコープルールは Organization1.1 および Organization1.2 に適用されますが、Organization1 には適用されません。	
ユーザは、組織の属性により指定される条件に適合する組織に所属する必要があります。	ビジネス タイプがゴールドまたはプラチナの組織に所属するユーザ	in organizations where <組織フィルタ>
ユーザは、指定された組織に所属し、特定のユーザ属性値と一致する必要があります。	where 役職 = マネージャ、かつ地域 = 東部、および所属組織が販売組織またはマーケティング組織であるユーザ	条件 <ユーザ フィルタ> および所属組織 <組織ルール>
ユーザのプロファイルの属性は、管理者のプロファイルの属性と一致する必要があります。	where マネージャ = 管理者のユーザ ID であるユーザ	where <ユーザ属性> <コンパレータ> 管理者の <ユーザ属性> **注**: 複数値属性では「等しくない」コンパレータを使用してください。
ユーザは、管理者と同じ組織に所属しています。	where Jeff(管理者)がメンバである組織に所属するユーザ	管理者の組織
ユーザは、管理者の属性に記載されている組織に所属しています。	ユーザの <管理属性> の値である	販売またはマーケティングの組織に所属しているユーザ

注: 以下に示すグループ スコープ ルールは、一例です。 その他のルールを作成して、管理者と、管理者が管理できるグループとの間のさまざまな関係に対応できます。

ルールの条件	例	ルールの構文
グループは、いずれかの属性値と一致する必要があります。	where グループ名 = 401K であるグループ名	where <グループ フィルタ>

ルールの条件	例	ルールの構文
グループは、指定した組織に所属している必要があります。	会計の組織に所属しているグループで、かつ	内<組織ルール>
グループは、いずれかの属性値に一致し、かつ指定した組織に所属する必要があります。	where ビジネス タイプ = 財務部、および所属組織が販売以下であるグループ	where <グループ フィルタ> および所属組織が <組織ルール>
グループは、管理者の属性に記載されている必要があります。	where 説明 = エンジニアリングであるグループ	where <グループ属性><コンパレータ> 管理者の <ユーザ属性> **注**: 複数値属性では「等しくない」コンパレータを使用してください。

注: 以下に示す組織スコープ ルールは、一例です。 その他のルールを作成して、管理者と、管理者が管理できる組織との間のさまざまな関係に対応できます。

ルールの条件	例	ルールの構文
組織は、いずれかの属性値と一致する必要があります。	where 組織名 = 財務部である組織	where <組織フィルタ>
組織は、指定した組織に所属している必要があります。	財務部の組織かつ	内<組織ルール>
組織は、いずれかの属性値に一致し、かつ指定した組織に所属する必要があります。	where 組織名 = 財務部および所属組織が財務部以下	where <組織フィルタ> および所属組織が <組織フィルタ>

詳細情報:

ルールの一般的なガイドライン (27 ページ)

ルールの一般的なガイドライン

作成するルールがどのようなタイプであっても、Identity Manager がそれらのルールをどのように処理するかを理解しておく必要があります。

演算子の評価

あるロールについてルールを作成する場合には、>=、<=、<、および > の演算子を使用します。 ただし、これらの演算子は、LDAP ディレクトリまたはリレーショナル データベースによって文字列として評価されます。 大半のユーザ ストアは、アルファベットをベースとして文字列を比較します。 したがって、500 と 1100 の比較では、5 は 1 よりも大きいため、ユーザ ストアで 500 の方が大きいと判断することがあります。

ユーザ ストアで文字列がこのように比較されないようにすることができます。 LDAP ディレクトリ サービス、またはリレーショナル データベース ソフトウェアのマニュアルを調べてください。

ルールにおける大文字/小文字の区別なし

管理ロールまたはアクセス ロールを作成する場合、作成するルールは、ユーザ ストアによって、大文字/小文字に無関係に、または大文字/小文字を区別して評価することができます。

ただし、作成または変更処理の最後に、その変更をユーザ ストアにコミットする前に、ルールは内部で大文字/小文字が区別されて評価されます。 たとえば、あるルールで title=manager という条件があるとします。このルールは、役職の値が「manager」であっても「Manager」であっても、ユーザ ストア オブジェクトを照合します。

アクションの追加および削除

Identity Manager で管理者がロールを与えたり、取り消したりしたときにロールのメンバシップが正しく管理されるようにするため、[アクションの追加]および[アクションの削除]を指定する必要があります。

- アクションの追加の結果、ユーザがロールのメンバ ルールのいずれかに適合する必要があります。 たとえば、ユーザ マネージャ ロールのメンバ ルールとして、ロール メンバの管理ロール属性値は「ユーザ マネージャ」であることが記述されている場合には、追加アクションで、管理ロール属性に「ユーザ マネージャ」を追加する必要があります。
- 削除アクションでは、ルールが無効になった場合に、ユーザがメンバ ルールに適合しないよう、ユーザのプロファイルを変更する必要があります。

各ロールには、2 つの追加アクションと 2 つの削除アクションを定義することができます。

管理者がロールのメンバを追加および削除できる場合は、追加アクションと削除アクションを定義します。 それ以外の場合は、RoleAdmins グループに所属するなどして、ユーザが、メンバ ルールに合わせたロールを持つようにします。 以下に例を示します。

- 管理者はロール A を割り当てることができるため、追加アクションまたは削除アクションが定義されます。
- ロール B では、「金融」グループのすべてのメンバがロールを持っている、というルールがあります。 このロールは割り当てることができないため、このロールには、追加アクションまたは削除アクションがありません。

追加アクションおよび削除アクションを定義する場合には、管理ロール属性を使用することを検討してください。Identity Manager はこの属性を使用して、ユーザのロール リストを格納することができます。 たとえば、あるユーザが従業員ロールのメンバとして追加されたときに、ユーザの管理ロール属性に「従業員」を追加する、という追加アクションを設定することができます。 「自己管理者」および「ユーザ マネージャ」のロールをすでに持っているマネージャに対して、管理者が「従業員」ロールを割り当てると、そのマネージャの管理ロール属性には、「自己管理者」、「ユーザ マネージャ」、「従業員」の値が含まれることになります。

管理ロール属性を使用するには、既知の属性である %ADMIN_ROLE_CONSTRAINT% をユーザ プロファイルの複数値属性にマップする必要があります。 詳細については、「CA Identity Manager Configuration Guide」を参照してください。

重要: アクションの追加を定義する場合、定義対象のロールを参照するルールを設定しないでください。 たとえば、あるメンバをロール A に含めることによって、ロール A のメンバを作成する追加アクションは定義しないでください。 このようにすると、ポリシー サーバが再起動される、という再帰的なエラーが生じます。

メンバ ポリシー

メンバ ポリシーは、あるユーザがメンバ ルールを満たしている場合に、そのユーザが、ポリシーで定義されているスコープを持つことを表します。 以下の図は、2 つのメンバ ポリシーを持つロールを示しています。

- 最初のポリシーは、ロール メンバで Jones という Manager がいた場合、そのメンバは Sales Office におけるユーザのロールを使用すること、およびそれらのユーザを 401k グループのメンバとして管理できることを表しています。

- 2 番目のポリシーは、ロール メンバが Bend 市にいる場合、そのロール メンバは、Oregon 州のユーザに関するロールを使用すること、およびそれらのロール メンバを、Smith という Group Admin のグループのメンバとして管理できることを表しています。

メンバ ポリシー

	メンバ ルール	ユーザ スコープ ルール	
	(マネージャ ="Jones") の場合	(オフィス="Sales") の場合	(グループ名 ="401K") の場合
	(市区町村 = "Bend") の場合	(都道府県="OR") の場合	(グループ管理者 = "Smith") の場合

管理ポリシー

管理ポリシーは、あるユーザが管理ルールを満たしている場合に、そのユーザが、ポリシーで定義されているユーザ スコープおよび管理者権限を持つことを表します。 ユーザ スコープは、ロールが使用される場所を定義します。 管理者権限は、ロール管理者がメンバを管理できるかどうか、またはロールの管理者を管理できるかどうかを定義します。

以下の図は、次のように定義される 2 つのの管理ポリシーを持つロールを示しています。

- 最初のポリシーでは、IT Admin が、Boston のユーザについて、メンバおよび管理者を追加および削除することができます。
- 2 番目のポリシーでは、Sales の管理者が、Ohio のメンバについて追加および削除することができます。

管理ポリシー

	管理ルール	ユーザ スコープ ルール	メンバの管理	管理者の管理	
	(従業員タイプ = "IT Admin")の場合	(市区町村="Boston")の場合	☑	☑	
	(オフィス= "Sales") の場合	(都道府県= "Ohio") の場合	☑	☑	

ロールの計画のチェックリスト

ロールを作成する前に、ロールの特性に関する以下のチェックリストを使用します。

ロールの特性	詳細
ロールのプロファイル	ロールの名前と説明を定義し、[有効]ステータスを設定します。
タスク	管理タスクとアクセス タスクが含まれます。
アカウント テンプレート	エンドポイント(プロビジョニング ロールのみ)に存在するアカウントを定義するアカウント テンプレートが含まれます。
メンバ ポリシー	各メンバ ポリシーを以下のように定義します。 ■ メンバ ルール - 誰がロールを使用できるか ■ スコープ ルール - ロール メンバはどのオブジェクトを管理できるか ■ アクションの追加 - メンバになったユーザのプロファイルがどうなるか ■ アクションの削除 - メンバとして削除されたユーザのプロファイルがどうなるか
管理ポリシー	各管理ポリシーを以下のように定義します。 ■ 管理ルール - ユーザをメンバまたは管理者として誰が管理するか ■ スコープ ルール - 管理者がどのユーザをメンバまたは管理者として管理できるか ■ アクションの追加 - 管理者になったユーザのプロファイルがどうなるか ■ アクションの削除 - 管理者として削除されたユーザのプロファイルがどうなるか
所有者ルール	ロールを変更できるユーザを定義します。

第 2 章: 管理ロール

このセクションには、以下のトピックが含まれています。

管理ロールと管理タスク (31 ページ)
新規管理ロールの作成 (32 ページ)
管理ロールの確認 (37 ページ)
ユーザによるロールの自己割り当ての許可 (37 ページ)

管理ロールと管理タスク

個々のビジネス要件に基づいて、オブジェクトの管理に必要なタスクを含むロールを作成します。 たとえば、ユーザを管理するタスクを含むロールと、その作成したロールを管理するタスクを含む別のロールを作成することができます。

また、以下のようなタスクを含むロールを個別に作成することもできます。

- ユーザを管理する管理者用のタスク
- 管理者を管理するタスク
- 管理ロールを管理するタスク
- アクセス ロールを管理するタスク

注: 出荷時に含まれる CA Identity Manager のデフォルトの管理ロールを使用することもできます。 デフォルトの管理ロールには、上記のリストのようにカテゴリにグループ化されたタスクが含まれます。

管理ロールと Identity Manager 環境

Identity Manager 環境にログインすると、ユーザ アカウントに 1 つまたは複数の管理ロールが割り当てられています。 各管理ロールには、Identity Manager 環境で使用する[ユーザの作成]などのタスクが含まれます。

たとえば、中央の Identity Manager 環境では、管理ロール である Help Desk (ヘルプデスク) にパスワードをリセットするタスクが含まれます。 このロールには、ユーザは必ず IT 担当の従業員でなければならない、というメンバ ルールがあります。 IT 担当の従業員が中央の Identity Manager 環境にログインすると、Help Desk (ヘルプ デスク) ロールが割り当てられており、その Identity Manager 環境に登録されているユーザのパスワードをリセットできます。

管理ロールとユーザ コンソール

Identity Manager 環境は、ユーザ コンソールを使用して表示できます。 以下の表のように、割り当てられた管理ロールによってコンソールに表示される項目が変わります。

割り当てられたロール	ユーザ コンソールのフォーマット
システム マネージャ ロール	すべてのオブジェクトと、これらのオブジェクトを管理するためのデフォルトの管理タスクすべてのカテゴリ リスト
複数タイプのオブジェクトを管理するためのロール	管理権限のあるオブジェクトのタイプごとに 1 つのアイテムを含むカテゴリ リスト
[ユーザ]など、1 つのタイプのオブジェクトを管理するためのロール	カテゴリ リストを含まないそのオブジェクトに対するタスク([ユーザの変更]など)
承認ロール	[ワーク リスト]画面 管理者に承認待機中のタスクがある場合に表示されます(たとえば、自己登録のユーザは承認が必要です)。

複数のオブジェクトを管理できる場合、変更できるオブジェクトがカテゴリ リスト形式で表示されます。これらは[ユーザ]や[グループ]などで、画面の上部にタブとして表示されます。 タブを選択して割り当てられたロールのタスクを表示します。

注: お使いのインターネット ブラウザがカスケーディング スタイル シート(CSS)をサポートしていない場合、ユーザ コンソールでは別のフォーマットを使用します。 このフォーマットの設定については、「Configuration Guide」を参照してください。

新規管理ロールの作成

ロールの要件が確認できたら、管理ロールを作成できます。 ロールの要件には、そのロールを使用するユーザ、管理するオブジェクト、および管理するオブジェクトが存在する環境が含まれます。

管理ロールの新規作成

User Console から管理ロールを作成します。

管理ロールを作成する方法

1. 管理ロールを作成するタスクのロールを持つ CA Identity Manager アカウントにログインします。

   たとえば、環境の最初のユーザは System Manager(システム マネージャ)ロールを持ちます。このロールには[管理ロールの作成]タスクが含まれます。

2. [ロールおよびタスク]の下にある[管理ロール]の[管理ロールの作成]を選択します。

3. ロールを新規作成するか、コピーするかを選択します。

   [プロファイル]タブが表示されるので、管理ロールの定義を開始します。

4. 管理ロールのプロファイルを定義します。

管理ロールのプロファイルの定義

[プロファイル]タブで、ロールの基本的な特性を定義します。

プロファイルを定義する方法

1. 名前と説明を入力し、そのロールに対して定義されるその他のカスタム属性を設定します。

   注: [プロファイル]タブに、管理ロールに関する追加情報を指定するカスタム属性を指定することができます。 この追加情報は、多数のロールを含む環境におけるロール検索を簡易化できます。

2. 作成後、すぐにこのロールを使用できるようにする場合は、[有効]を選択します。

3. ロールの管理タスクを選択します。(34 ページ)

詳細情報:

ロールのユーザ定義のカスタム属性(50 ページ)

ロールの管理タスクの選択

[タスク]タブでロールに含める管理タスクを選択します。 異なるカテゴリのタスクを含めたり、別のロールで使用されているタスクをコピーできます。

管理タスクを選択する方法

1. [カテゴリでフィルタ]フィールドで、カテゴリを選択します。

   利用できるタスクのカテゴリを表示するには、下矢印のアイコンをクリックします。

2. [タスクの追加]フィールドでロールに含めるタスクを選択します。

   CA Identity Manager により、ロールのタスクのリストにタスクが追加されます。

3. その他に追加するタスクがある場合は、手順 1 および 2 を繰り返します。

4. ロールからタスクを削除するにはそのタスクの[マイナス]アイコン( )をクリックします。

5. 管理ロールのメンバ ポリシーを定義します(35 ページ)。

管理ロールのメンバ ポリシーの定義

[メンバ]タブでメンバ ポリシーを作成します。これによって、ロール メンバに含めるユーザを決定します。

メンバ ポリシーを定義するには、以下の手順に従います。

1. メンバ ポリシーを定義するには、[追加]をクリックします。 メンバ ポリシーには以下のルールが含まれます。
   - ユーザがロール メンバであるための要件を定義したメンバ ルール。

     注: 以下の演算子は、メンバ ルールの中で数字を文字として扱います。
     - より小さい(<)
     - 以下(<=)
     - より大きい(>)
     - 以上(=>)

     たとえば、「10」は「1」の後、「2」の前です。
   - ロールのタスクに使用可能なプライマリ オブジェクトとセカンダリ オブジェクトを制限するスコープ ルール。

     たとえば、ロールが、ユーザをグループに割り当てることでユーザを変更するタスクを含む場合、ユーザ スコープ ルールで検索対象ユーザ(プライマリ オブジェクト)を制限し、グループ スコープ ルールで割り当て可能なグループ(セカンダリ オブジェクト)を制限します。

   注: 1 つ以上のスコープの質問に回答を入力してください。 スコープ ルールによって、ロール内のタスクに使用可能なプライマリ オブジェクトとセカンダリ オブジェクトが制限されます。 たとえば、ロールが、ユーザをグループに割り当てることでユーザを変更するタスクを含む場合、ユーザ スコープ ルールで検索対象ユーザ(プライマリ オブジェクト)を制限し、グループ スコープ ルールで割り当て可能なグループ(セカンダリ オブジェクト)を制限します。
2. [メンバ]タブに[メンバ ポリシー]が表示されることを確認します。
   - ポリシーを編集するには、左側の右矢印記号をクリックします。
   - 削除するには、マイナス記号アイコンをクリックします。
3. [メンバ]タブの[管理者は、このロールのメンバを追加および削除できます。]というチェックボックスをオンにします。ただし、メンバ ルールへの適合のみをメンバの条件とする場合は、この限りではありません。

   この機能を有効にすると、画面が拡張します。

4. 拡張された領域で[アクションの追加]と[アクションの削除]を定義します。これらは、ユーザをロール メンバとして追加または削除する条件を指定します。

   重要: アクションの追加を定義する場合、定義対象のロールを参照するルールを設定しないでください。 たとえば、ロール A のメンバに含まれることで、ロール A のメンバを作成するアクションの追加は定義しないでください。この処理でエラーが発生する場合があります。たとえば、ユーザがロール A のメンバとなる条件として、ロール A のメンバであることを定義しないでください。

5. 管理ロールに管理ポリシーを定義します(36 ページ)。

管理ロールの管理ポリシーの定義

[管理]タブで、ユーザをこのロールのメンバおよび管理者として追加または削除することができるユーザを定義します。

管理ポリシーを定義するには、以下の手順に従います。

1. [管理者の管理]オプションを選択可能にするには、[管理者は、このロールの管理者を追加および削除できます。]というチェックボックスをオンにします。

   この機能を有効にすると、画面が拡張します。

2. ロールの管理者権限を持つユーザを追加または削除した場合、拡張された領域で[アクションの追加]と[アクションの削除]を定義します。

3. 管理ポリシーを定義します。管理ポリシーには、管理ルール、スコープ ルール、および 1 つ以上の管理者権限が含まれます([メンバの管理]または[管理者の管理])。

   注: 異なるルール、およびそれらのルールに適合する管理者のそれぞれ異なる権限を含む複数の管理ポリシーを追加できます。

4. ポリシーを編集するには、左側の矢印記号をクリックします。 削除するには、マイナス記号アイコンをクリックします。

5. 管理ロールの所有者ルールを定義します(37 ページ)。

管理ロールの所有者ルールの定義

[所有者]タブで、そのロールの所有者になることができるユーザ、すなわちロールを変更できるユーザに関するルールを定義します。

所有者ルールを定義するには

1. 所有者ルールを定義します。これでロールを変更できるユーザが決まります。
2. [送信]をクリックします。

   タスクが送信されたことを示すメッセージが表示されます。 ユーザがそのロールを使用可能になるまで、少し時間がかかることがあります。

このロールの作成時に[有効]を選択した場合、ロールが使用可能になります。 ユーザがメンバ ルールの条件に適合している場合、そのユーザは Identity Manager 環境にログインしてロールのタスクを使用できるようになります。

管理ロールの確認

ロールが作成されたことを確認するには、[管理ロール]-[管理ロールの表示]を選択してから、ロール名を選択します。

または、[システム]-[サブミット済みタスクの表示]を選択して、ロールの作成タスクが完了したことを確認します。

ユーザによるロールの自己割り当ての許可

環境には、ユーザが自己割り当てできるロールが存在する可能性があります。 たとえば、ユーザの作業アイテムを他のユーザに委任できるように、ユーザによる委任マネージャロールの登録を許可することができます。

ユーザが自己割り当て可能なロールを制御するには、[ロールの自己管理マネージャ]タスクで基準を設定します。

ユーザによるロールの自己割り当てを許可する方法

1. [ロールの自己管理マネージャ]タスクを以下のように変更します。
   a. [ロールおよびタスク]-[管理タスクの変更]を選択し、[ロールの自己管理マネージャ]タスクを検索します。
   b. [タブ]タブを選択します。

      タスクに適用されるタブのリストが CA Identity Manager に表示されます。

c. 編集する[ロールの自己管理マネージャ]タブの横にある右矢印アイコンを選択します。

d. 以下のフィールドに値を入力します。

[以下のルールに適合する管理ロールのみ表示]

CA Identity Manager でユーザが自己割り当てできるロールを決定するために使用する基準を指定します。

新規ルールを追加するには、プラス(+)アイコンをクリックします。

[管理ロール管理者として使えるユーザ]

ユーザが自己割り当てできるロールの管理者を指定します。

ユーザが自己割り当てできるロールは、このフィールドで選択したユーザが管理者となり、さらに、[以下のルールに適合する管理ロールのみ表示]フィールドで指定した基準に適合する必要があります。

[リスト画面]

ユーザがロールの自己割り当てを選択できるロールのリストについて、列とフォーマットを指定します。

e. [OK]をクリックした後、[送信]をクリックします。

2. [ロールの自己管理マネージャ]タスクをロールに追加し、その機能を持たせるユーザにロールを割り当てます。

第 3 章: 管理タスク

このセクションには、以下のトピックが含まれています。

管理タスクの計画 (39 ページ)
管理タスクの使用法オプション (43 ページ)
デフォルトの管理タスク (44 ページ)
カスタム管理タスクの作成方法 (45 ページ)
タスクのプロファイルの定義 (46 ページ)
タスク スコープの定義 (53 ページ)
タスクのタブの選択 (61 ページ)
タスクのフィールドの表示 (65 ページ)
使用しているロールの表示 (65 ページ)
イベントへのワークフロー プロセスの割り当て (65 ページ)
Active Directory の前提条件 (66 ページ)
アプリケーション機能の外部タスク (68 ページ)
高度なタスク コンポーネント (70 ページ)
管理タスクおよびイベント (72 ページ)
管理タスクの処理 (74 ページ)

管理タスクの計画

管理ロールは、オブジェクトをきめ細かく管理する複数の管理タスクから構成されます。たとえば、以下の管理タスクを使用してユーザ オブジェクトを管理できます。

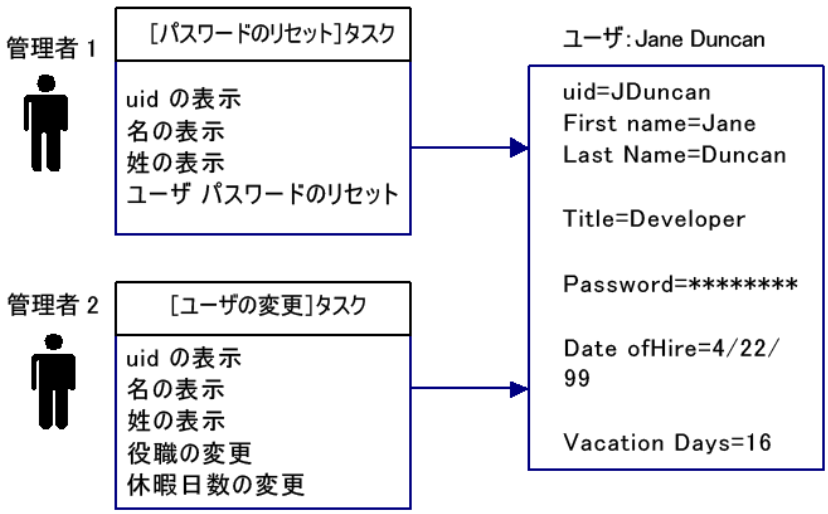
- ユーザの作成
- ユーザの表示
- ユーザの変更
- ユーザ パスワードのリセット

要件に完全に合致するように、各タスクを作成または変更します。 次に、適切な管理タスクを組み合わせて管理ロールにし、管理者に割り当てます。 これらのロールにより、オブジェクトの管理に必要な完全な権限が管理者に付与されます。

管理タスクの作成を計画するには、管理対象とするオブジェクト(ユーザ、グループ、組織、ロール、またはタスク)と、そのタスクを使用する管理者を決定します。 以下に例を示します。

- ユーザを管理するために、ヘルプ デスク管理者には、ユーザ ID や役職などのユーザ属性を管理するタスクが必要です。
- アプリケーションへのユーザのアクセス権を管理するには、ユーザをアクセス ロールのメンバにするタスクを他の管理者に割り当てる必要があります。
- ヘルプ デスク管理者が使用するロールを管理するために、より上位の管理者には、管理ロールを管理するタスクが必要です。

1 つの種類のオブジェクト(たとえば、ユーザ)について、異なる管理者が異なる属性を管理するようにタスクを作成することができます。 たとえば、以下の図は 2 人の管理者が 1 人のユーザを管理する例です。



- 管理者 1 は[ユーザ パスワードのリセット]タスクを持っています。この管理者は、従業員のユーザ ID および名前の参照や、パスワードのリセットができます。
- 管理者 2 は[ユーザの変更]タスクを持っています。この管理者は、従業員のユーザ ID および名前の参照や、役職および休日の変更ができます。

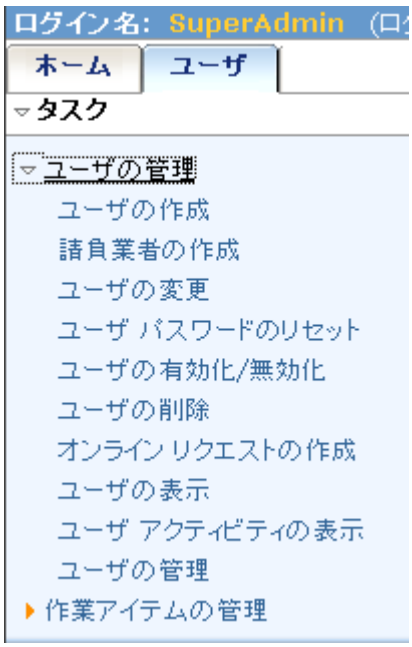
管理タスクの例

管理タスクを作成する際、タスクの画面の内容とレイアウトを定義します。それには以下が含まれます。

- タスクの名前
- タスクが表示されるカテゴリ

- タスクで使用するタブとフィールド、およびフィールドの表示プロパティ
- 管理者が検索クエリで使用可能なフィールド、および検索結果に表示されるフィールド

タスクのエレメントを理解するため、[ユーザの変更]タスクを例に説明します。 この例では、[ユーザ]はカテゴリ、[ユーザの管理]はサブカテゴリ、[ユーザの変更]はタスクです。 タスクの作成時にカテゴリとタスクの名前を作成します。



[ユーザの変更]を選択すると、検索画面が表示されます。 検索画面には、表示または変更するオブジェクトの検索オプションが表示されます。 各オプションはフィルタと呼ばれます。フィルタは、検索するオブジェクトに関して制限を設定します。

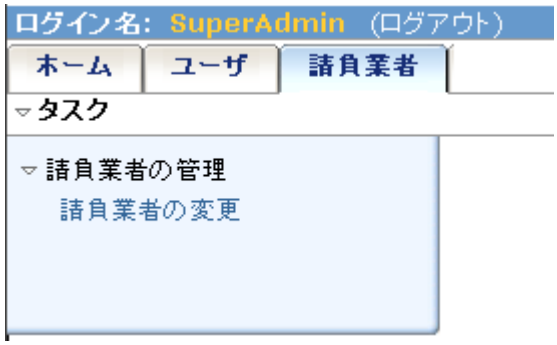
検索画面の入力後、タブ付きの画面が表示されます。 たとえば、以下の図は[ユーザの変更]タスクの場合のタブです。 最初に[プロファイル]タブが開き、ユーザ属性が表示されます。他のタブにはユーザのロールとグループの権限が表示されます。

作成するタスクについて、含めるタブと、タブの順序および内容を決めます。

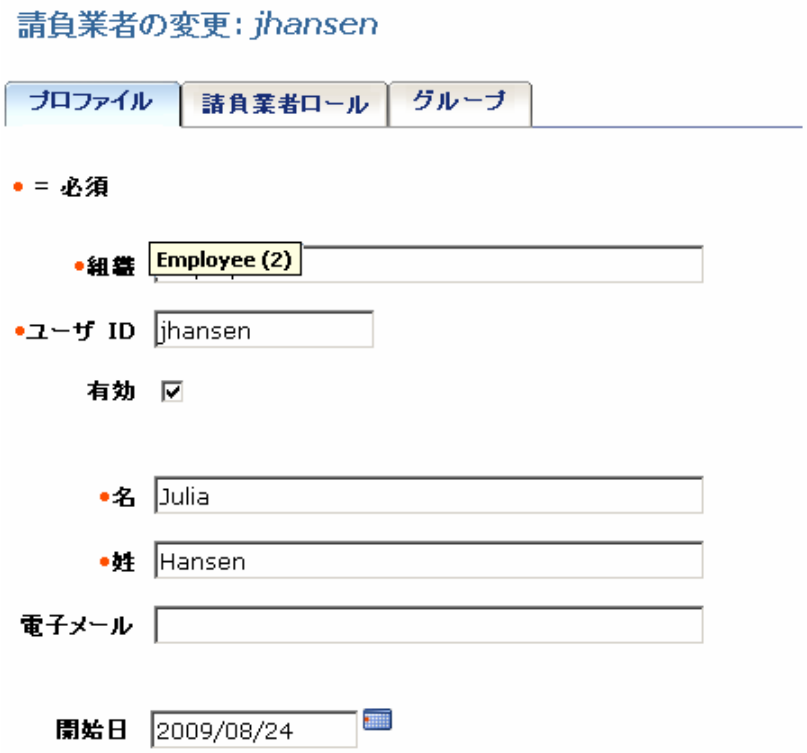
たとえば、[ユーザの変更]タスクをテンプレートに使用して、契約者の変更タスクを作成できます。このタスクでは、以下のアイテムが変更されます。

- [プロファイル]タブのフィールド
- タスクに含めるタブとその内容
- タスクが表示されるカテゴリ

  新しいカテゴリである「契約者」の下にこのタスクを作成できます。



[契約者の変更]タスクには、ユーザの変更タスクの[プロファイル]タブに含まれるフィールドの一部と、契約の開始日や契約者の会社など他のフィールドが含まれます。 管理者が契約者を探す場合、契約者の名前、会社、および契約の開始日で検索できます。



新しいタスクには[Contractor Roles]タブも含まれ、このタブでは契約者のロールを追加します。

管理タスクの使用法オプション

Identity Manager では、管理タスクを使用する方法が 2 種類用意されています。

- タスクの選択

  カテゴリとタスクを選択してから、タスクを適用するオブジェクトを検索します。

  たとえば、ユーザのプロファイルを変更するには、[ユーザ]カテゴリを選択し、[ユーザの変更]タスクを選択します。 次に、変更するユーザを検索します。

- オブジェクトの選択

  [ユーザの管理]または[グループの管理]などの[管理]タスクを使用して、オブジェクトを検索します。 オブジェクトを選択すると、そのオブジェクトの管理に使用できるタスクの一覧を表示できます。 この方法はオブジェクト タスク ナビゲーションと呼ばれます。

  たとえば、この方法を使用してユーザを変更するには、[ユーザ]カテゴリを選択し、[ユーザの管理]タスクを選択します。 管理するユーザを検索して選択します。 検索結果の中からアイコンをクリックすると、その選択したユーザの管理に使用できるタスクのリストが表示されます。 このリストから[ユーザの変更]や他の適切なタスクを選択できます。

  また、管理タスク以外のタスクでも、タスク リストを設定できます。 たとえば、[メンバシップ]タブにタスク リストを追加することができます。 この場合、[メンバシップ]タブに表示されるメンバごとにタスク リストを使用できます。

  注: オブジェクトのタスク リストには、現在の管理者が使用可能なタスクのみが表示されます。

デフォルトの管理タスク

CA Identity Manager にはデフォルトの管理タスクおよびロールのセットが含まれており、管理コンソールにロール定義ファイルをインポートすると CA Identity Manager に追加されます。 管理コンソールに環境を作成して、デフォルトのロールの作成を選択すると、CA Identity Manager はロール定義ファイルを自動的にインポートします。

注: 特定のエンドポイント タイプのアカウント管理など、一部の機能をサポートするには、必要なロールやタスクを作成するために、追加のロール定義ファイルをインポートする必要がある場合があります。

多くの場合、インストール時のデフォルト タスクを使用できます。 ただし、[ユーザの作成]、[ユーザの変更]、[ユーザの表示]といったデフォルトのユーザ タスクの、[プロファイル]タブを変更する必要がある場合があります。 [プロファイル]タブには、ディレクトリ設定ファイルでユーザ オブジェクトに定義されているすべてのフィールドが含まれています。 タブに表示されるフィールド数を制限したり、フィールドの表示プロパティを変更することが可能です。

注: デフォルト タスクを直接変更するのではなく、変更するデフォルト タスクのコピーを作成することをお勧めします。

カスタム管理タスクの作成方法

管理タスクとは、ユーザが Identity Manager で実行できる管理機能です。 たとえば、[ユーザの作成]、[グループの変更]、[ロール メンバシップの表示]などの管理タスクがあります。

CA Identity Manager には、ビジネスのニーズに合わせて変更できるデフォルトの管理タスクが含まれています。

カスタム管理タスクを作成するときは、以下の手順に従います。

注: セクション「Active Directory の前提条件 (66 ページ)」には、CA Identity Manager で Active Directory ユーザ ストアを管理する場合の、その他の考慮事項が記載されています。

1. Identity Manager のユーザ コンソールで、[ロールおよびタスク]、[管理タスク]、[管理タスクの作成]を選択します。

   新しいタスクを作成するか、既存のタスクを元にしてタスクを作成するかが確認されます。

   たとえば、新しいタスクの基礎として[ユーザの変更]タスクを選択します。

2. [既存タスクのコピーの作成]を選択して、コピーするタスクを検索します。

   注: デフォルト タスクを直接変更するのではなく、デフォルト タスクのコピーを変更することをお勧めします。

3. [OK]を選択すると、次の 6 つのタブがある画面が表示されます。

タブ	目的	参照するトピック
[プロファイル]	作成するタスクのプロファイルを定義します	タスクのプロファイルの定義 (46 ページ)
検索	タスクで管理するオブジェクトの範囲を制限します	タスク スコープの定義 (53 ページ)
タブ	タスクのタブを選択および設計します	タスクのタブの選択 (61 ページ)
フィールド	すべてのタブに使用するフィールドを表示します	タスクのフィールドの表示 (65 ページ)
イベント	Identity Manager 環境でタスクがワークフローを使用する場合は、イベントごとにワークフロー プロセスを選択します	イベントへのワークフロー プロセスの割り当て (65 ページ)

タブ	目的	参照するトピック
使用しているロール	変更または表示しているタスクを含むロールが表示されます。	使用しているロールの表示(65 ページ)

注: カスタム管理タスクの作成の詳細については、「User Console Design Guide」を参照してください。

タスクのプロファイルの定義

[プロファイル]タブには、タスクの全般的な設定が含まれます。

注: 管理タスク プロファイル設定の詳細については、「User Console Design Guide」を参照してください。

タスクのプロファイルを定義する方法

1. タスクのオブジェクト(プライマリ オブジェクトと呼ばれます)の種類と、そのオブジェクトに対して実行するアクションを選択します。
2. 必須のフィールドを設定し、タスクの要件に合わせて適切なチェック ボックスをオンにします。

   注: 既存のタスクとプロファイル設定が似ているタスクを作成する場合、[別のタスクからのプロファイルのコピー]をクリックします。 このオプションでは、選択した既存のタスクのプロファイル設定を使用して、作成するタスクのプロファイル設定を指定します。 次に、新しいタスクのルールと説明を追加します。
3. (オプション)ビジネス ロジック タスク ハンドラをタスクに関連付けます。
4. このタブの設定が終了したら、次の手順「タスク スコープの定義(53 ページ)」に進みます。

管理タスクの[プロファイル]タブ

管理タスクの[プロファイル]タブを使用すると、管理タスクの全般的な設定を定義できます。

このタブには以下のフィールドが含まれます。

- 名前

  タスクの名前を定義します。

- タグ

  タスクの一意な識別子を定義します。 これは URL、Web サービス、またはプロパティ ファイルで使用されます。 タグには、ASCII 文字(a ～ z、A ～ Z)、数字(0 ～ 9)、またはアンダースコアを含めることが可能で、1 字目には文字かアンダースコアを使用します。

- 説明

  タスクの目的に関するメモを指定できます。

- Task Order

  タスクの表示順を指定します。 順序を指定しない場合、タスクはアルファベット順に表示されます。

- カテゴリ

  タスクのカテゴリを指定します。 カテゴリは、画面上部にタブとして表示されます。

- カテゴリ順

  カテゴリ タブの表示順を指定します。 たとえば、カテゴリの順序を 3 に設定すると、指定したカテゴリは 3 番目のタブとして表示されます。

- カテゴリ 2

  第 2 階層カテゴリを指定します。カテゴリ タブ リストの下にリンクとして表示されます。 第 2 階層カテゴリは、第 1 階層カテゴリのタブが選択されているときのみ表示されます。 たとえば、第 1 階層カテゴリの「従業員」と第 2 階層カテゴリの「従業員管理」を含むタスクを作成した場合、「従業員管理」カテゴリは、[従業員]タブの選択後にのみ表示されます。

- カテゴリ 2 順

  第 1 階層カテゴリに第 2 階層カテゴリが複数ある場合、第 2 階層カテゴリの表示順を指定します。

- カテゴリ 3

  第 3 階層カテゴリを指定します。このカテゴリは左のナビゲーション ペインに表示されます。 タスクは第 3 階層カテゴリの下に表示されます。 たとえば、デフォルトの環境では、システム マネージャ ロールまたはユーザ マネージャ ロールのユーザが、[ユーザ]タブを選択すると、第 3 階層カテゴリの[ユーザの管理]が表示されます。

- カテゴリ 3 順

  第 3 階層カテゴリの表示順を指定します。

- プライマリ オブジェクト

  タスクの操作対象であるオブジェクトを指定します。

- アクション

  オブジェクトで実行される操作を指定します。

- ユーザ同期化

  このタスクでユーザとアイデンティティ ポリシーを同期するかどうかを指定します。以下のオプションのいずれかを選択できます。

  - オフ(デフォルト)

    このタスクでユーザ同期化はトリガされないことを指定します。

  - タスク完了時

    タスクのすべてのイベントが完了した後に、ユーザ同期化プロセスを開始するように指定します。 この設定は、[ユーザの作成]、[ユーザの変更]、および[ユーザの削除]タスクのデフォルト同期化オプションです。 それ以外の他のタスクのデフォルト設定は、[オフ]です。

    注: 複数のイベントを含むタスクに対して[タスク完了時]オプションを選択すると、Identity Manager はそのタスク内のすべてのイベントが完了するまでユーザを同期化しません。 イベントの 1 つまたは複数がワークフローの承認を必要とする場合、その承認に数日かかることがあります。 すべてのイベントが完了されるまでアイデンティティ ポリシーが適用されないという事態を回避するには、[各イベント発生時]オプションを選択します。

  - 各イベント発生時

    タスク内の各イベントが完了したときに、Identity Manager で ユーザ同期化プロセス(204 ページ)を開始することを指定します。

    同じユーザに対するプライマリ イベントとセカンダリ イベントを持つタスクでは、ユーザ同期化を[各イベント発生時]に設定すると、[タスク完了時]オプションを選択した場合よりも、多くのアイデンティティ ポリシーがユーザに適用される可能性があります。

- アカウントの同期化

  プロビジョニングを有効にしている場合、プロビジョニング サーバに登録されているアカウントを同期します。

  - オフ(デフォルト)

    このタスクでアカウント同期化はトリガされないことを指定します。

  - タスク完了時

    タスクのすべてのイベントが完了した後に、アカウント同期化プロセスを開始するように指定します。

  - 各イベント発生時

    タスク内の各イベントが完了したときに、Identity Manager でアカウント同期化プロセスを開始することを指定します。

    注: パフォーマンスを最適化するには、[タスク完了時]を選択します。 ただし、複数のイベントを含むタスクに対して[タスク完了時]オプションを選択すると、Identity Manager はそのタスク内のすべてのイベントが完了するまでアカウントを同期化しません。 イベントの 1 つまたは複数がワークフローの承認を必要とする場合、その承認に数日かかることがあります。 Identity Manager がすべてのイベントの完了までアカウントの同期化を待機するという事態を回避するには、[各イベント発生時]オプションを選択します。

- メニューで非表示

  タスクをメニューに表示しません。 タスクを呼び出すのが URL または他のタスクのみであれば、このコントロールを有効にします。

- パブリック タスク

  Identity Manager にログインしていないユーザがタスクを使用できるようにします。 デフォルトのパブリック タスクは[忘れたパスワード]と[自己登録]です。

- 監査の有効化

  タスクに関する情報を監査データベースに記録します。 監査情報はレポートの生成に使用できます。 詳細については、「Configuration Guide」を参照してください。

- ワークフローの有効化

  ワークフロー エンジンをインストールしている場合、タスクに関連付けられている Identity Manager イベントによるワークフロー プロセスのトリガを使用可能にします。 たとえば、[グループの削除]タスクに関連付けられているイベントで、承認手順を含むワークフロー プロセスをトリガすることができます。

- Web サービスの有効化

  管理コンソールから WSDL(Web Services Description Language、Web サービス記述言語)出力を生成できる対象として、タスクを設定します。 リモートからのタスクのサブミットを使用する場合、このコントロールを有効にします。 詳細については、「Programming Guide for Java」を参照してください。

- ワークフロー プロセス

  イベント レベル ワークフローではなくタスク レベル ワークフローの設定を有効にします。 タスク レベルのワークフローは、タスク アクティビティが処理される前に発生します。 ワークフロー プロセス ジョブが開始するまで、イベントまたはネストされたタスクは実行されません。

- タスク優先度

  Identity Manager でタスクを実行する順序を決定します。 優先度が[高]のタスクは、優先度が[中]または[低]のタスクよりも前に実行されます。 タスクのデフォルト プロパティは[中]です。

  注: ステータスを表示するには、特定の優先度のタスクを検索してから[サブミット済みタスクの表示]を使用します。

- ビジネス ロジック タスク ハンドラ

  ビジネス ロジック タスク ハンドラ(70 ページ)をタスクと関連付けます。

- Workflow Action Buttons(ワークフロー アクション ボタン)

  カスタムのアクション ボタンをワークフローの承認タスクに追加します。

- 別のタスクからのプロファイルのコピー

  他のタスクの[プロファイル]タブからデータをコピーします。

  たとえば、[ユーザの変更]タスクの[プロファイル]タブ設定をコピーして、名前と説明を追加することができます。

ロールのユーザ定義のカスタム属性

CA Identity Manager は、ロールに関する追加情報を指定できるユーザ定義のカスタム属性に対応しています。 この情報を、組織のロールをフィルタするために使用することもできます。 たとえば、企業環境では 1000 を超えるロールが存在する場合があります。そのような企業では、各ロールに業務部門や地域といった追加情報を指定することができます。 管理者は、このような追加情報を使用してロールの検索を簡易化することができます。

以下のロールについては、タスクの作成、変更、および表示にカスタム属性を使用できます。

- [管理ロール]
- [プロビジョニング ロール]
- [アクセス ロール]

ロールのカスタム属性を設定するには、以下の概要手順に従います。

1. 管理ロール、プロビジョニング ロール、またはアクセス ロールを作成、変更、または表示するタスクの[プロファイル]タブに、カスタム属性に対するサポートを追加します。
2. カスタム属性を含めるように、そのロールの検索画面およびリスト画面を設定します。

詳細情報:

ロールの[プロファイル]タブにおけるカスタム属性の設定(51 ページ)
検索画面の定義へのカスタム属性の追加(52 ページ)

ロールの[プロファイル]タブにおけるカスタム属性の設定

CA Identity Manager では、ロールを作成、変更または表示するタスクの[プロファイル]タブに最大 10 個のカスタム属性を設定することができます。

[プロファイル]タブにおけるカスタム属性の設定方法

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]をクリックします。

   [管理タスクの選択]画面が表示されます。
2. 変更する管理タスクを検索し、選択します。

   選択した管理タスクのタスクの詳細が表示されます。
3. [タブ]タブをクリックします。

   この管理タスク用に設定されたタブが表示されます。
4. 矢印アイコンをクリックし、[プロファイル]タブを編集します。

   [プロファイルの設定]画面が表示されます。
5. カスタム属性を[プロファイル]タブに追加し、わかりやすいラベルを入力するには、各[カスタム]フィールドの隣にあるチェック ボックスを選択します。
6. [OK]をクリックします。

   タスクをサブミットすると、変更されたタスクの[プロファイル]タブでカスタム属性が使用できるようになります。

   注: ロール検索でカスタム属性を使用するには、カスタム属性を表示するように検索画面を設定(52 ページ)してください。

検索画面の定義へのカスタム属性の追加

CA Identity Manager でロールをフィルタする場合は、検索画面で使用できる属性のみを使用できます。 定義したカスタム属性に基づいてロールをフィルタするには、ロールの検索画面にカスタム属性を追加する必要があります。

ロールの検索画面に対するカスタム属性の追加方法

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]をクリックします。

   [管理タスクの選択]画面が表示されます。

2. 変更するタスクを検索し、選択します。

   検索画面にカスタム属性を追加するには、カスタム属性を含むロールのタイプ(管理、プロビジョニング、またはアクセス)の変更または表示タスクを選択します。

   選択した管理タスクのタスクの詳細が表示されます。

3. [管理ロールの変更]画面で[検索]タブをクリックします。

   検索画面の詳細が表示されます。

4. そのタスクで使用できる検索画面定義のリストを表示するには、[参照]ボタンをクリックします。

   [画面定義の選択]ページが開きます。

5. 編集する検索画面定義を選択するか、既存の検索画面定義のコピーを作成します。

   [標準検索画面の設定]が表示されます。

6. 以下のテーブルにカスタム属性を追加します。

   - [ユーザが検索可能なフィールドを選択]
   - 検索結果に表示されるフィールドの選択

7. [プロファイル]タブを設定した際に指定した名前と一致するように、カスタム属性の名前を変更します。

8. 検索画面定義の変更を保存するには、[OK]をクリックします。

   [画面定義の選択]画面が再度開きます。

9. 作成、または編集した画面を選択し[選択]をクリックします。

10. 検索オプション リストから[すべての管理ロール]を選択します。

11. [送信]をクリックします。

    これで、検索画面の検索オプションにカスタム属性が追加され、検索結果に属性が表示されるようになりました。

タスク スコープの定義

[検索]タブでタスク スコープを定義すると、タスクに使用できるオブジェクトが制限されます。 たとえば、タスクのオブジェクトがユーザの場合、契約者であるユーザとしてスコープを定義します。

注: タスクにプライマリ オブジェクトがない場合、またはアクションが自己修正、自己表示、または承認である場合は、[検索]タブは表示されません。

[検索]タブで以下のように設定します。

検索画面

検索画面では、フィルタに基づいてタスクのスコープを制限します。 [参照]をクリックして、使用できる検索画面オプションを表示します。

注: 独自の検索画面(54 ページ)を作成できます。 既存の検索画面の変更バージョンを作成するには、検索画面を選択し、[コピー]をクリックします。 元の検索画面定義を変更することなく、検索画面を変更できます。 検索画面を作成するには、[新規]をクリックします。

検索オプション

検索オプションが表示されるのは、オブジェクトがロールまたはグループの場合のみです。

- 最初のオプションでは、検索画面に定義されているフィールドに基づいて検索が制限されます。 これらの制限で、管理者のスコープ内にあるすべてのグループまたはロールが検索されます。
- 指定のとおり、他のオプションで検索を制限します。

以下の点に注意してください。

- デフォルトで、グループ検索画面はフィルタをサポートしています。 つまり、管理者は基準を指定して、グループ検索のスコープを制限できます。 フィルタ機能を削除するには、フィールドをまったく含まない検索画面を作成して、検索クエリに含めます。
- オブジェクトがロールの場合、[検索]タブに表示される「フィルタリングはサポートされていません」は、このタスクでは、選択したオプションの基準に適合するロールが表示されることを意味します。 検索画面上で設定されている検索フィールドは無視されます。

変更されたオブジェクトは、管理者のスコープ内に残す必要があります。

このチェック ボックスを選択すると、タスクの変更により管理者のスコープからプライマリ オブジェクトが失われた場合、CA Identity Manager によりエラーが表示されます。 たとえば、管理者は「ユーザの変更」を使用してユーザの従業員タイプ属性をマネージャに変更するとします。 この変更により、このユーザは管理者のスコープから除外されることがあります。

検索画面設定

検索画面を設定して、タスクのスコープを制限し、ユーザが検索できるフィールドを制御します。 検索画面は 2 種類のオブジェクトに適用されます。

- プライマリ オブジェクト: タスクから変更または表示できるオブジェクト。
- セカンダリ オブジェクト: プライマリ オブジェクトに関連があるオブジェクト。

  たとえば、[ユーザの作成]タスクにグループ タブを含める場合、ユーザはプライマリ オブジェクトでグループはセカンダリ オブジェクトです。 グループ タブにはグループの検索画面が必要です。

  注: 検索画面の設定後は、プライマリ オブジェクトまたはセカンダリ オブジェクトを検索する任意のタスクに使用できます。

検索フィルタ

検索フィルタでは、検索によって返されるオブジェクトを制限します。 たとえば、オブジェクトがユーザの場合、契約者のみを見つけるように検索を制限できます。 [従業員タイプ]に「Contractor」を指定してユーザを検索するフィルタを設定できます。

検索用に以下のフィールドを設定できます。

[以下のルールに適合するオブジェクトのみ表示]

検索を制限するには、ユーザ定義フィルタと組み合わせる追加の基準を定義します。

このフィールドを使用するときは、以下の点に注意してください。

- プロビジョニング ロール検索の制限により、これらの基準は、ユーザが入力した同じ名前のフィルタ フィールドを上書きします。
- このフィールドを設定するときに使用した属性は、検索画面の使用可能な検索フィールドとして追加しないでください。

  たとえば、 検索画面を設定して、Enabled 属性が「Yes」に設定されているロールのみ表示する場合は、検索条件でユーザが指定できる属性のリストから Enabled 属性を削除します。

  削除しない場合は、ユーザが入力した条件は無視されます。

[デフォルトの検索フィルタ]

管理者が検索画面を使用する場合、デフォルトで表示されるフィルタを定義します。 たとえば、[Modify Contractor]タスクの検索画面を設定していて、管理者は通常、契約者の会社名で契約者を検索することがわかっている場合、デフォルト フィルタを「契約会社 = *」に設定できます。 管理者は、異なる検査基準を指定して、デフォルト フィルタを無効にできます。 デフォルト フィルタを設定すると、検索の開始前に管理者がフィルタを指定しなくても、返される結果の数が制限されるため、パフォーマンスが向上します。

[複数選択タスクで使用時にすべての検索結果を自動選択]

デフォルトですべての検索結果を選択することを指定します。 このチェック ボックスをオンにすると、検索結果リストのすべてのオブジェクトは、オブジェクト名の横のチェック ボックスがオンになって表示されます。

[自動的に検索を実行]

検索フィールドに検索結果が表示されるように指定します。

[単一の検索結果しかない場合、タスクの対象を自動的に設定]

1 つのオブジェクトのみが検索フィルタに適合する場合、タスクのプライマリ オブジェクトが自動的に設定されます。

たとえば、[ユーザの変更]タスクに関連付けられているユーザ検索画面でこのオプションを選択したとします。 管理者が[ユーザの変更]タスクを開き、検索フィルタを入力した結果、1 人のユーザのみが返された場合、CA Identity Manager ではそのユーザの[ユーザの変更]タスクを開きます。 管理者は、[ユーザの変更]タスクを開くためにユーザを選択する必要はありません。

注: この設定を適用するには、[自動的に検索を実行]も選択されている必要があります。

[検索フィルタの保存]

タスクの検索フィルタが現在のセッションのユーザ用に保存されるように指定します。タスク内で次の検索を実行すると、保存した検索フィルタが表示されます。

注: CA Identity Manager では、ユーザ セッション期間の検索フィルタが保存されます。 ユーザがログアウトすると、検索フィルタはクリアされます。

[組織内の検索]

検索画面に組織フィルタが表示されます。 このチェック ボックスをオンにすると、管理者は CA Identity Manager でオブジェクトを検索する組織を制限するフィルタを指定できます。 組織検索フィルタのデフォルトを指定するには、[組織検索]フィールドの検索画面を指定します。

[組織検索の保存]

検索対象となる組織が作成された場合、タスクの組織を保存するように指定します。タスク内で次の検索を実行すると、組織が表示されます。

［組織検索］

CA Identity Manager によって使用される検索画面で、管理者が組織を検索できるように指定します。

［デフォルトの組織検索スコープ］

管理者が検索画面を使用する際に表示される［デフォルトの組織検索スコープ］を指定します。 検索スコープによって、検索に含まれる組織ツリーのレベルが指定されます。 管理者は、検索画面で異なる検索基準を指定して［デフォルトの組織検索スコープ］を変更できます。

たとえば、契約者の情報をさまざまなレベルの組織ツリーに保存する環境にカスタマイズした［契約者の変更］タスク用に検索画面を設定した場合、［デフォルトの組織検索スコープ］を［かつ次より低い］に設定できます。

［単一式による検索］

検索画面に表示される検索フィルタのタイプを定義します。 このチェック ボックスをオンにすると、<attribute><comparator><value> など、単一の検索フィルタを指定できます。 このチェック ボックスをオフにすると、複数の検索フィルタを指定できます。 たとえば、<attribute1><comparator><value1> AND <attribute2><comparator><value2> です。 すべてのフィルタの条件に適合するオブジェクトが、検索結果に返されます。 前の例では、<value1> と <value2> を含むオブジェクトが検索結果として返されます。

［等号のみの検索］

管理者に「=」以外の検索演算子の使用を禁止します。

［結果の件数の表示］

一致した検索結果の数が表示されます。 このチェック ボックスがオンの場合、すべての検索で、「X 個の結果があります。」というメッセージが返されます。

［次に対しタスク ボタンを追加］ <task name>

別のタスクへのリンクを検索画面に追加します。 リンクはボタンとして表示されます。通常、このフィールドは、オブジェクト タスク ナビゲーションに設定されている検索画面に［作成］タスクを追加するために使用されます。

［オプションのラベル］

前のフィールドで選択したタスクのラベルを指定します。 このラベルはタスクのボタンに表示されます。

［次に対し複数削除ボタンを追加］ <task name>

管理者が複数オブジェクトを選択して削除できるタスクへのリンクを追加します。 リンクはボタンとして表示されます。
通常、このフィールドは、オブジェクトタスク ナビゲーションと共に使用します。

検索フィールドと検索結果

検索画面の別の部分で、管理者が検索クエリに使用するフィールド、および検索結果を表示するフィールドを選択します。

[ユーザが検索可能なフィールドを選択]

管理者が検索クエリの作成に使用するフィールドを選択します。

フィールドをさらに追加するには、検索フィールド テーブルの下にあるリスト ボックスのフィールドを選択します。

フィールドを選択した後で、フィールドの右にある上矢印と下矢印のアイコンを使用して、表示する順序を変更できます。

注: 管理者の検索対象フィールドが指定されない場合、CA Identity Manager では自動的に検索が開始されます。

検索結果に表示されるフィールドの選択

Identity Manager の検索結果に表示されるフィールドを選択します。 検索クエリに使用できないフィールドを選択できます。

フィールドをさらに追加するには、検索フィールド テーブルの下にあるリスト ボックスのフィールドを選択します。

[スタイル]

検索結果に表示するフィールドを選択する場合、以下のスタイル オプションのいずれかを選択できます。

- 論理値の表示名

  true であるすべての結果のフィールド名が表示されます。 たとえば、[有効]をユーザのアカウント ステータスを示す属性名として入力すると、すべてのアクティブなユーザ アカウントの検索結果に、[有効]が表示されます。

- [チェックマーク]

  属性値に基づき、選択されたチェックマークとして値が表示されます。 たとえば、ユーザ アカウントの有効/無効状態を表すためにチェックマーク スタイルを選択した場合、CA Identity Manager ではすべてのアクティブなアカウントに選択されたチェックマークが表示されます。

- 複数値文字列

  別個の行に複数値属性の値が表示されます。 値はアルファベット順に表示されます。

- Read-Only Checkbox(値を読み取り専用チェック ボックス)

  値を読み取り専用チェック ボックスとして表示します。

- 文字列

  値をテキスト文字列として表示します。

- [タスク]

  フィールドにタスク リストを追加します。 ユーザが右矢印アイコンをクリックすると、検索フィールドに関連付けられたオブジェクトに対して実行できるタスクのリストが表示されます。 たとえば、タスク リストを検索結果の[姓]フィールドに追加した場合、そのフィールドの矢印アイコンをクリックすると、選択したユーザに対して実行できるタスクのリストが表示されます。

  この設定を使用して、属性値をタスクへのリンクとして表示することもできます。

  [タスク]スタイルを選択している場合、[スタイル]列の横に右矢印アイコンが表示されます。 矢印をクリックすると、[フィールドのプロパティ]ダイアログ ボックスが開きます。 このダイアログ ボックスを使用して、タスク リストを設定します。

並べ替え可能

このチェック ボックスを選択すると、検索結果を 1 つまたは複数のフィールドによって並べ替えることができます。

検索結果のデフォルトの並べ替え順の設定

検索結果の表示順を指定します。 検索結果の表示は、はじめにリストの最初のフィールド、次に順番に残りの各フィールドによって並べ替えられます。 [降順]チェック ボックスを選択すると、降順に結果が並べ替えられます。

[フィールドが変更されたオブジェクトの選択]フィールドの名前

ユーザが[選択]ボタンをクリックすると、指定されたフィールドに変更が加えられたオブジェクトが選択されるように指定します。

Return N results per page(ページ毎の結果 N を戻す)

ページごとに表示できる結果の数を選択します。 検索結果が指定した数を超える場合、各結果ページへのリンクが表示されます。

検索画面のユーザ定義ヘルプ

検索画面にカスタム テキストを追加する場合、対応する HTML テキスト ボックスでテキストを定義します。 以下の領域にテキストを追加できます。

- ページの先頭または末尾
- 作成の前または後
- 結果の前または後

検索画面のタイプ

Identity Manager には、以下の事前設定の検索画面があります。

アクセス ロール検索画面

[アクセス ロール検索画面]を使用して、特定の基準に適合するアクセス ロールを見つける検索フィルタを設定できます。

アクセス タスク検索画面

[アクセス タスク検索画面]を使用して、特定の基準に適合するアクセス タスクを見つける検索フィルタを設定できます。 この検索画面は、表示または変更するアクセス タスクを見つけるとき、またはアクセス ロールにタスクを追加するときに使用されます。

管理ロール検索画面

[管理ロール検索画面]を使用して、特定の基準に適合する管理ロールを見つける検索フィルタを設定できます。

管理タスク検索画面

[管理タスク検索画面]を使用して、特定の基準に適合する管理タスクを見つける検索フィルタを設定できます。 この検索画面は、表示または変更する管理タスクを見つけるとき、または管理ロールにタスクを追加するときに使用されます。

承認検索画面

[承認検索画面]を使用すると、承認タスクの上部に表示される内容を設定できます。

[Begin Certification User Search]画面

[Begin Certification User Search]画面を使用すると、証明書が必要と設定するユーザを見つける検索フィルタを設定できます。 選択されたユーザは、証明書のステータスが証明書が必要に設定されます。

認証ユーザの検索画面

[認証ユーザの検索]画面を使用すると、証明書が必要なユーザを見つける検索フィルタを設定できます。

[Delegation Search Screen]

[Delegation Search Screen]を使用すると、委任されたユーザとして追加する新規ユーザを見つける検索フィルタを設定できます。 委任されたユーザは、別のユーザのワークフローの作業アイテムを表示および解決する権限を一時的に付与されるユーザです。

ユーザの有効化/無効化検索画面

[ユーザの有効化/無効化検索画面]を使用すると、特定の基準に一致するユーザを有効化/無効化する検索フィルタを設定できます。

[End Certification User Search]画面

[End Certification User Search]画面を使用すると、証明書のサイクルが完了したユーザを特定する検索フィルタを設定できます。

[エンド ユーザ使用許諾契約の検索画面]

[エンド ユーザ使用許諾契約の検索画面]を使用すると、自分のアイデンティティに基づいたアプリケーション固有のページを使用して、[自己登録]タスクを設定できます。

検索および関連付け検索

[検索および関連付け検索画面]を使用すると、特定の基準に一致する検索および関連付け定義の検索フィルタを設定できます。

[Feeder File Upload Search]画面

[Feeder File Upload Search]画面を使用すると、アップロードするフィーダ ファイルを参照できます。 フィーダ ファイルは、大量の管理対象オブジェクトに繰り返しのアクションを自動的に実行するために使用します。

忘れたパスワードの検索画面/忘れたユーザ ID の検索画面

[忘れたパスワードの検索画面]を使用すると、アイデンティティを確認する情報をユーザに求めるように、[忘れたパスワード]タスクを設定できます。

グループ検索画面

グループ検索画面を使用すると、財務組織内のグループなど、グループの検索フィルタを設定できます。

アイデンティティ ポリシー セット検索画面

[アイデンティティ ポリシー セット検索画面]を使用すると、特定の基準に一致するアイデンティティ ポリシー セットを見つける検索フィルタを設定できます。

ロジカル アトリビュート ハンドラ検索画面

[ロジカル アトリビュート ハンドラ検索画面]を使用すると、ロジカル アトリビュート ハンドラを見つける検索フィルタを設定できます。 この検索画面は、ロジカル アトリビュート ハンドラを見つけて設定を表示または変更するときに使用します。

レポート管理検索画面

[レポート管理検索画面]を使用すると、表示または削除するレポートを見つける検索フィルタを設定できます。

NonCertified User(証明されていないユーザ)検索画面

[NonCertified User(証明されていないユーザ)検索画面]を使用すると、証明期間の終了までに証明されなかったユーザを見つける検索フィルタを設定できます。

組織検索画面

[組織検索画面]を使用すると、組織の選択を特定の下位組織に制限する検索フィルタを設定できます。

プロビジョニング ロール検索画面

[プロビジョニング ロール検索画面]を使用すると、プロビジョニング ロールを取得する検索フィルタを設定できます。

[Account Template Search]画面

[Account Template Search]画面を使用すると、アカウント テンプレートを取得する検索フィルタを設定できます。

パスワード ポリシー検索画面

[パスワード ポリシー検索画面]を使用して、特定の基準に適合するパスワード ポリシーを見つける検索フィルタを設定できます。

Snapshot Definition(スナップショット定義)検索画面

[Snapshot Definition(スナップショット定義)検索画面]を使用すると、表示、変更、または削除するスナップショット定義を見つける検索フィルタを設定できます。

標準検索画面

[標準検索画面]を使用すると、カスタムの管理対象オブジェクトを見つけるフィルタを設定できます。

ユーザ検索画面

[ユーザ検索画面]を使用すると、特定の基準に一致するユーザを見つける検索フィルタを設定できます。 たとえば、契約者であるユーザを検索できます。

[検索]タブに入力してから、タスクのタブを選択します。

タスクのタブの選択

[タブ]タブで、タブ名を指定し、タブの設定を変更します。各タブはタスクに含めるフィールドのセットです。 デフォルトのタブを含めたり、新しいタブを作成することができます。 たとえば、[ユーザの変更]タスクには、以下のタブが含まれます。

- プロファイル
- アクセス ロール
- 管理ロール

- グループ
- 作業アイテムの委任

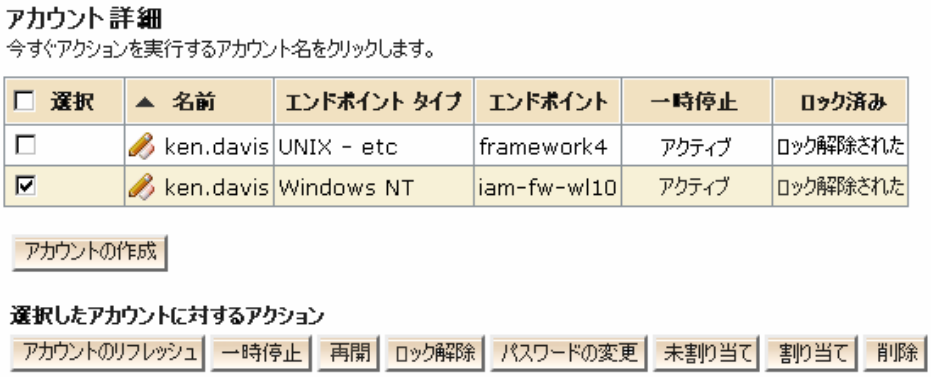
タブの定義を編集するには、タブ名の横にある[編集]アイコン( )をクリックします。

詳細情報:

[アカウント]タブ(62 ページ)
[スケジュール]タブ(64 ページ)

[アカウント]タブ

[アカウント]タブには、プロビジョニング ロールを割り当てたユーザの管理エンドポイントのアカウントが表示されます。 通常、このタブは、ユーザを表示または変更できるタスクに追加されます。



[アカウント]タブを[ユーザの変更]タスクに追加すると、管理者はユーザのアカウントに対して他のアクションを実行できます。 以下に例を示します。

- アカウントの一時停止または再開
- 不正または不適切なアクセスによって自動的にロックされたアカウントのロック解除。たとえば、Identity Manager のパスワード ポリシーに設定されているログイン失敗回数の上限を超えると、アカウントはロックされます。
- 1 つ以上のアカウントでのユーザ パスワードの変更。
- ユーザに対するアカウントの割り当てと割り当て解除。

[アカウント]タブで設定可能な他のオプションの詳細については、[アカウントの設定]タブのユーザ コンソール ヘルプを参照してください。

[アカウント]タブを使用するための前提条件

[アカウント]タブを使用するには、プロビジョニング サポートを使用して Identity Manager を設定する必要があります。また、Identity Manager 環境にプロビジョニング ディレクトリが存在する必要があります。

注: 環境にプロビジョニング サポートを設定するには、「Configuration Guide」を参照してください。

[アカウント]タブのフィールド

[アカウント]タブには、ユーザがエンドポイント システムで保持しているアカウントに関する詳細情報が表示されます。

以下に、重要なフィールドの一部を示します。

- 名前: アカウントのログイン名、電子メール名、またはその他の名前。
- エンドポイント タイプ: アカウントに関連付けられているエンドポイントのタイプ。LDAP ディレクトリなど。
- エンドポイント: アカウントに関連付けられている特定のエンドポイント。
- 一時停止: 3 つの状態のうちの 1 つ。
  - アカウントが有効な場合は、アクティブが表示されます。
  - アカウントが無効の場合は、一時停止が表示されます。
  - 再開、または一時停止できない場合は、有効化を保留中(手動)が表示されます。 アカウントを再開、または一時停止するにはエンドポイント システムにログインする必要があります。
  - エンドポイントと通信できないために状態を取得できない場合、[利用不可]と表示されます。
- ロック済み: アカウントがロックされているかどうかを示します。 ユーザが誤ったパスワードでアカウントへのログインを数回試みるとロックされます。 エンドポイントと通信できないために状態を取得できない場合、[利用不可]と表示されます。

[アカウント]タブのその他の機能

ユーザを変更するタスクに[アカウント]タブを含めると、管理者はそのタスクを使用して、ユーザのアカウントに対してさまざまな機能を実行できます。 使用できる機能は、タブ設定によって決まります。

使用できる機能を選択するには、[アカウント]タブが含められたタスクで[管理タスクの変更]を使用します。 [アカウント]タブを編集して、[アカウントの割り当て]や[アカウントのアサイン解除]などの機能を、タブで使用可能にするかどうかを指定します。

詳細については、[アカウントの設定]タブのオンライン ヘルプを参照してください。

[スケジュール]タブ

スケジューリングで、今後の日付を指定してタスクの実行を自動化できます。 ワークフローに関連付けられたタスクをスケジュールする場合、すべてのタスクはそのワークフローに定義されているとおりに実行されます。スケジュールされたタスクのステータスは、[サブミット済みタスクの表示]ページに表示できます。

CA Identity Manager でまだ実行されていないスケジュール済みタスクは、[サブミット済みタスクの表示]ページでキャンセルできます。

注: スケジュール済みのタスクがキャンセルされ、そのタスクを再サブミットした場合、そのタスクはスケジュールされた実行時間に関わらずただちに実行されます。

CA Identity Manager では、スケジューラが特殊なタブとして用意されています。 スケジューラにアクセスするには、[スケジュール]タブでタスクを設定する必要があります。

管理タスクへの[スケジュール]タブの追加

CA Identity Manager では、特定の日時にタスクが実行されるようにスケジュールすることができます。 タスクのスケジュールを立てるには、[スケジュール]タブを管理タスクに追加します。

注: CA Identity Manager の一部の管理タスクには[スケジュール]タブを追加できません。 タスクのスケジュールを立てることができない場合、スケジュール タブは[管理タスクの変更]画面で使用できません。

[スケジュール]タブを管理タスクに追加する方法

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]をクリックします。

   [管理タスクの選択]画面が表示されます。

2. [条件]フィールドで[名前]または[カテゴリ]を選択し、検索文字列を入力して[検索]をクリックします。

   検索基準を満たす管理タスクが表示されます。

3. 管理タスクを選択し、[選択]をクリックします。

   選択した管理タスクのタスクの詳細が表示されます。

4. タブをクリックします。

   選択した管理タスク用に設定されたタブが表示されます。

5. [このタスクで表示する必要があるのはどのタブですか]ドロップダウンからスケジュールを選択し、[ ]をクリックします。

   [スケジュール]タブは、選択した管理タスクに表示されるタブのリストに追加されます。

6. [送信]をクリックします。

   [スケジュール]タブは、選択した管理タスクに追加されます。

タスクのフィールドの表示

[フィールド]タブには、このタスクに適用されるフィールドが表示されます。 これらのフィールドは、このタスクのタブに作成されたフィールドです。 使用するフィールドを変更するには、[タブ]タブに戻り、変更が必要なタブを選択します。

このタブの設定が終了したら、次の手順「イベントへのワークフロー プロセスの割り当て (65 ページ)」に進みます。

ただし、Identity Manager 環境でワークフローを使用していない場合は、ここで[送信]をクリックできます。 タスクが成功したかどうかを示すメッセージが表示されます。 成功した場合、タスクをロールに追加でき、ロール メンバがタスクを使用できるようになります。

使用しているロールの表示

[使用しているロール]タブには、現在表示または変更しているタスクを含むロールが表示されます。

ロール所有者は、ロールにタスクを追加したり、ロールからタスクを削除することができます。

注: 「デフォルトの管理ロール (512 ページ)」には、デフォルトで CA Identity Manager と共にインストールされている管理ロールのタスク リストが表示されます。

イベントへのワークフロー プロセスの割り当て

この Identity Manager 環境でワークフローを有効にした場合、[イベント]タブを使用して、タスクが開始する各イベントについてワークフロー プロセスを選択します。 ユーザが選択したワークフロー プロセスは、Identity Manager 管理コンソールのデフォルトで選択される値よりも優先されます。

デフォルトのワークフロー マッピングの詳細については、「Configuration Guide」の高度な設定の章を参照してください。

このタスクの作成を完了するには、[送信]をクリックします。 タスクが成功したかどうかを示すメッセージが表示されます。 成功した場合、タスクをロールに追加でき、ロール メンバがタスクを使用できるようになります。

Active Directory の前提条件

Active Directory がユーザ ストアの場合、管理タスクを作成する前に、特定の Active Directory 機能の設定が必要になることがあります。

sAMAccountName 属性

sAMAccountName 属性はユーザとグループに適用されます。 この属性は必須で、ユーザとグループの作成に使用されるタスク画面に含める必要があります。

注: ユーザの作成時に、sAMAccountName 属性には 20 字を超える値を指定できません。 この制限はグループには適用されません。

ユーザまたはグループを作成するときに、一意の sAMAccountName を自動的に生成する、カスタムのロジカル アトリビュート ハンドラを作成できます。 この場合、[ユーザの作成]画面と[グループの作成]画面の非表示フィールドとして sAMAccountName 属性を含めることができます。

詳細については、「Programming Guide for Java」のロジカル アトリビュートの章を参照してください。

グループのタイプとスコープ

Active Directory には以下の 2 タイプのグループがあります。

- セキュリティ: リソースとオブジェクトのアクセス権を定義するアクセス制御リスト (ACL) に表示されます。
- 配布: ユーザやグループなど、グループ オブジェクトに使用されます。 配布グループは、Active Directory のアクセス権を付与するときに使用できません。

各タイプのグループには、以下を決定するスコープがあります。

- メンバのロケーション: 潜在的なメンバが存在する場所
- アクセス権: アクセス権管理のために、このグループを使用できる場所(グループがセキュリティ グループの場合)
- 他のグループのグループ メンバシップ: グループが所属するグループの場所

各タイプのグループは、以下のスコープのいずれかを持つことができます。

スコープ	メンバのロケーション	アクセス権	他のグループのグループ メンバシップ
ユニバーサル	グループ メンバは、フォレスト内の任意のドメインのユニバーサル グループ、グローバル グループ、およびユーザの可能性があります。	フォレスト内の任意のドメインでアクセス権を付与するために使用できます。	フォレスト内の任意のドメインのドメイン ローカル グループおよびユニバーサル グループのメンバの可能性があります。
グローバル	グループ メンバは、グローバル グループ、およびグループとして同じドメインに所属するユーザの可能性があります。	フォレスト内の任意のドメインでアクセス権を付与するために使用できます。	フォレスト内の任意のドメインのグローバル グループ、ドメイン ローカル グループ、およびユニバーサル グループのメンバの可能性があります。
ドメイン ローカル	グループ メンバは、フォレスト内の任意のドメインのユニバーサル グループ、グローバル グループ、およびユーザの可能性があります。 また、同じドメインのドメイン ローカル グループの可能性もあります。	グループが所属するドメインへのアクセス権を付与するときにのみ使用できます。	ドメイン内の他のドメイン ローカル グループのメンバのみです。

グループのタイプとスコープは必須の属性ではありませんが、グループのタイプとスコープを指定しない場合、Active Directory によってグローバル スコープでセキュリティ グループが作成されます。

異なるタイプのグループを作成するために、カスタムのロジカル アトリビュート ハンドラを作成できます。「Programming Guide for Java」のロジカル アトリビュートに関する章を参照してください。

これらの Active Directory 機能を設定したら、次のステップ「管理タスクの作成」に進みます。

アプリケーション機能の外部タスク

外部タスク

- Identity Manager ユーザ コンソール から Identity Manager 以外のアプリケーションで、管理者が機能を実行できるようになります。
- オプションで、ユーザ、グループ、または組織固有のタスクを生成するための情報をアプリケーションに渡します。

たとえば、外部タスクを使用して、発注書を生成するアプリケーションに組織に関する情報を渡す場合があります。 このタスクを実行する管理者は、Identity Manager ユーザ コンソール から、公開されている組織の発注書を表示できます。

[外部タスク]には 2 つのタブを使用できます。 これらのタブの設定方法は同じですが、機能は異なります。

- [外部]タブは表示タブです。つまり、タブ内に URL のコンテンツが表示されます。
- [外部 URL]は非表示のタブです。つまり、タスクは入力された URL にリダイレクトされます。

外部タブ

[外部]タブを任意の[作成]、[表示]、または[変更]タスクに追加して、そのタスクを外部タスクにすることができます。 たとえば、[ユーザの追加]タスクに[外部]タブを追加すると、そのタスクにタブが表示されます。

[外部]タブの場合

- 外部タスクに対してイベントが生成されません。
- オプションで管理オブジェクトを使用できます。

- ［外部 URL］フィールドでは、アプリケーションのアドレスを以下のように指定できます。
  - 完全なアドレス。完全修飾ドメイン名を含みます。以下に例を示します。

    http://server1.mycompany.org/report/viewUserReport
  - 相対パス。以下に例を示します。

    /report/viewUserReport

    相対パスを指定すると、Identity Manager をインストールしたサーバの完全修飾ドメイン名が自動的に付加されます。
- ［プロファイル］タブ上のアプリケーションに渡す属性を設定します。

［外部 URL］タブ

［外部 URL］タブを［ユーザの表示］などの表示タスクに追加できます。［ユーザの表示］タスクを使用すると、URL で指定された Web サイトにリダイレクトされます。 その他のタブは表示されません。

［外部 URL］タブの場合

- ［外部 URL］タブはタスク内の唯一のタブにする必要があります。 同じタスクと関連付けられている他のタブがある場合、外部タブは指定した URL にユーザをリダイレクトしません。
- タスクで、監査可能なイベントを生成できます。
- ［外部 URL］フィールドでは、アプリケーションのアドレスを以下のように指定できます。
  - 完全なアドレス。完全修飾ドメイン名を含みます。以下に例を示します。

    http://server1.mycompany.org/report/viewUserReport
  - 相対パス。以下に例を示します。

    /report/viewUserReport

    相対パスを指定すると、Identity Manager がインストールされているサーバの完全修飾ドメイン名が自動的に追加されます。
- オプションで管理オブジェクトを使用できます。
- URL に渡す属性を設定できます。

  起動するアプリケーションの URL を指定し、そのアプリケーションに渡す属性を含めます。

高度なタスク コンポーネント

高度なタスク コンポーネントを使用すると、タスクのカスタム プロセスを指定できます。

- [タスク レベルの検証]で、タスクの他の属性に対して属性値を検証します。 たとえば、ユーザ指定の電話番号のエリア コードが、ユーザの市区町村と都道府県に適切かどうか検証します。
- ビジネス ロジック タスク ハンドラ(70 ページ)では、Identity Manager タスクのプロセスをサブミットする前に、カスタムのビジネス ロジックが実行されます。 通常、カスタムのビジネス ロジックでデータが検証されます。 たとえば、Identity Manager が新しいメンバをグループに追加する前に、ビジネス ロジック タスク ハンドラを使用して、グループ メンバシップの限度を確認できます。 グループ メンバシップが限度に達している場合、ビジネス ロジック タスク ハンドラによって、新しいメンバを追加できなかったことをグループ管理者に知らせるメッセージが表示されます。

ビジネス ロジック タスク ハンドラの作成

ビジネス ロジック タスク ハンドラの完全修飾クラス名を以下のように定義します。

1. 管理タスクを作成または変更します。
2. [管理プロファイル]タブで、[ビジネス ロジック タスク ハンドラ]をクリックします。

   [ビジネス ロジック タスク ハンドラ]画面が表示されます。 この画面には、タスクに割り当てられている既存のビジネス ロジック タスク ハンドラが表示されます。 Identity Manager では、リストの表示順にハンドラが実行されます。
3. [追加]をクリックします。

   [ビジネス ロジック タスク ハンドラの詳細]画面が表示されます。

[ビジネス ロジック タスク ハンドラの詳細]画面を使用して、タスクに割り当てているビジネス ロジック タスク ハンドラに以下の情報を定義します。

名前

ビジネス ロジック タスク ハンドラに割り当てる名前。

説明

オプションの、ビジネス ロジック タスク ハンドラの説明。

Java クラス

ビジネス ロジック タスク ハンドラを Java で実装している場合、完全修飾ビジネス ロジック タスク ハンドラ クラス名。以下に例を示します。

com.mycompany.MyJavaBLTH

Identity Manager では、カスタム Java クラス ファイルに指定されたルート ディレクトリに、クラス ファイルが格納されていると判断します。 Java クラス ファイルの配置の詳細については、「Programming Guide for Java」を参照してください。

JavaScript ファイル名

ビジネス ロジック タスク ハンドラが JavaScript に実装されており、JavaScript コードがファイルに含まれている場合は、このフィールドにファイル名を指定してください。たとえば、ビジネス ロジック タスク ハンドラが複数のタスク画面で使用される場合は、ファイルに JavaScript を組み込むことができます。

Identity Manager は、このファイルがカスタム JavaScript ファイル用のルート ディレクトリにあると想定します。 JavaScript ファイルの展開の詳細については、「Programming Guide for Java」を参照してください。

ルートのサブディレクトリにファイルを保存する場合は、JavaScript ファイル名の指定時にサブディレクトリ名を含めてください。以下に例を示します。

JavaScriptSubDir¥yJavaScriptBLTH.js

JavaScript ファイルが展開されるプラットフォームに対応したスラッシュを使用する必要があります。

JavaScript

ファイルの代わりにフィールドに完全な JavaScript コードを入力して、JavaScript ビジネス ロジック タスク ハンドラを実装することもできます。 たとえば、スクリプトが非常に短い場合や他のタスク画面では使用されない場合は、フィールドに JavaScript を組み込むことができます。

プロパティおよび値

Java の実装では、これらのフィールドは、Java ビジネス ロジック タスク ハンドラの init() メソッドに渡されるデータのオプションの名前/値であり、このハンドラのビジネス ロジックが必要とするあらゆる方法で使用されます。

ユーザ定義のプロパティを追加するには、プロパティの名前と値を指定してから、[追加]をクリックします。

注: Java ビジネス ロジック タスク ハンドラを追加する場合は、アプリケーション サーバを再起動して、このハンドラがロードされるようにします。

管理タスクおよびイベント

管理タスクにはイベント(CA Identity Manager がタスクを完了するために実行するアクション)が含まれます。 1 つのタスクには、複数のイベントが含まれている場合があります。 たとえば、[ユーザの作成]タスクには一般に、ユーザ プロファイルを作成するイベント、ユーザをグループに追加するイベント、ロールを割り当てるイベントが含まれます。

Identity Manager はイベントを監査し、イベントに関連付けられた顧客固有のビジネス ルールを適用します。イベントがワークフロー プロセスにマッピングされると、そのイベントの承認が必要になります。

タスクに複数のイベントが生成され、それらのイベントがワークフロー プロセスにマッピングされた場合には、Identity Manager がタスクを完了させる前にすべてのワークフロー プロセスを完了させておく必要があります。

プライマリ イベントおよびセカンダリ イベント

一般的に、イベントは他のイベントから独立しています。 しかし、タスクの中には、プライマリ イベントおよび複数のセカンダリ イベントに関連付けられているタスクもあります。

- プライマリ イベントが失敗に終わると、そのセカンダリ イベントはすべて自動的に拒否されます。 たとえば、CreateUserEvent が失敗した場合、そのユーザのために、AddToGroupEvent を実施する必要はありません。 また、プライマリ イベントの失敗は、関連付けられているタスクのキャンセルにつながります。
- セカンダリ イベントが失敗しても、そのタスクで実施される他のどのイベントまたはそのタスク自体の成功にも影響は及ぼされません。 たとえば、[ユーザの作成]タスクで、AddToGroupEvent が拒否されることがあります。それは、新規ユーザを特定のグループに追加できないことを意味します。 ユーザの作成(CreateUserEvent)、プロビジョニング ロールへの割り当て(AssignProvisioningRoleEvent)、および他のグループへの追加は、依然として可能です。

タスクのイベントの表示

Identity Manager のユーザ コンソールで、タスクに関連付けられているイベントを表示できます。

タスクのイベントの表示方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスクの表示]を選択します。
2. 適切なタスクを検索して選択します。
3. [イベント]タブをクリックします。

   現在のタスクに関連付けられたイベントが表示されます。

未変更のプロファイルに生成されるイベント

ユーザ、グループ、および組織のオブジェクトにはそれぞれ、ユーザ ディレクトリに格納されている一連のフィジカル アトリビュートが含まれています。 これらのオブジェクトのいずれかのフィジカル アトリビュートが[プロファイル]タブ上で変更されると、Identity Manager はユーザがタスクをサブミットした後に Modify... イベントを生成します。 たとえば、Title 属性が[ユーザのプロファイル]タブ上で変更されると、Identity Manager は ModifyUserEvent イベントを生成します。

ユーザ、グループ、または組織のオブジェクトが[プロファイル]タブ上に表示されていても、ユーザが[送信]をクリックしたときにフィジカル アトリビュートを変更しなかった場合、Identity Manager は Modify... イベントを生成しません。 その代わり、これに対応する View... イベントが生成されます。以下に例を示します。

- ModifyUserEvent の代わりに ViewUserEvent が生成されます
- ModifyGroupEvent の代わりに ViewGroupEvent が生成されます
- ModifyOrganizationEvent の代わりに ViewOrganizationEvent が生成されます

管理タスクの処理

タスクの処理にかかる時間は、実行する手順によって変わります。 タスクの処理がサブミットされると、Identity Manager では以下の手順が実行されます。

1. サブミットされたデータが検証されます。

   これを同期段階と呼びます。

2. タスクに承認が必要な場合、Identity Manager からワークフロー エンジンにタスクが送信されます。

   a. ワークフロー エンジンで承認者が決定され、承認者のワーク リストに承認タスクが設定されます。

   b. オプションで、保留中の作業アイテムについて、Identity Manager から承認者に通知の電子メールが送信されます。

   c. 承認者は作業アイテムを予約し(この項目は他の承認者のワーク リストから削除されます)、項目を承認または拒否します。

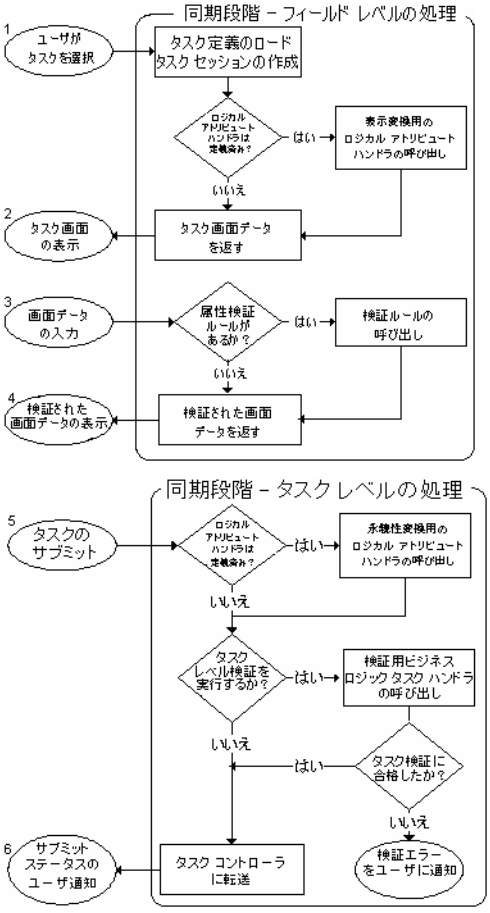
   d. オプションで、タスクのステータスについて、関係するユーザに通知の電子メールが送信されます。

   これを非同期段階と呼びます。

3. タスクが拒否されなかった場合、Identity Manager でタスクが実行されます。

同期段階の処理

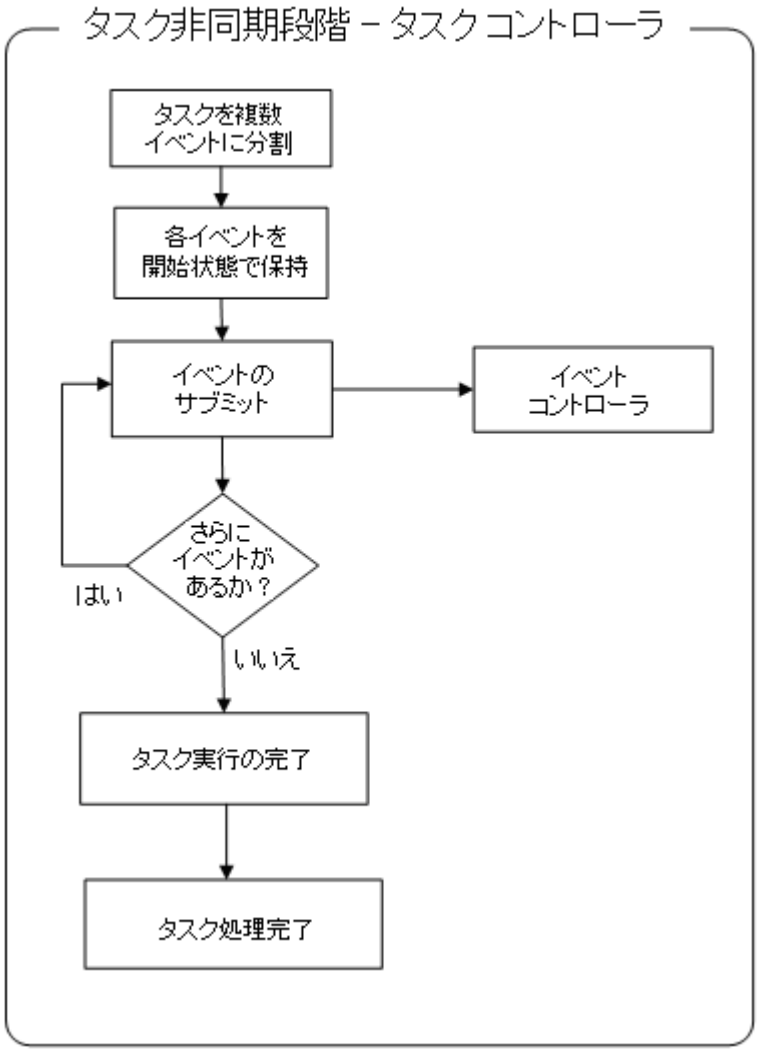
同期段階では、ユーザがタスク画面に入力したデータを Identity Manager が変換および検証できます。タスクが処理にサブミットする前に、データにビジネス ロジックを課することもできます。 同期段階で何が行われるかについての高度な説明を次の図に示します。



非同期段階の処理

同期段階が完了すると、タスクは非同期段階の実行に入ります。 非同期段階では、タスクによりイベントが生成されます。 イベントには、ユーザ プロファイルの作成やグループへのユーザの追加などのユーザ定義のイベントと、監査ログへの情報の書き込みなどのシステム生成のイベントがあります。

Identity Manager Server のコンポーネントであるタスク コントローラは、次の図に示すように、タスクとそのイベントのライフ サイクルを管理します。



大部分のイベントは、ライフ サイクル、実行、およびアクションについて、他のイベントから独立しています。 （作成タスクでは、セカンダリ イベントの前にプライマリ オブジェクトの作成イベントが実行される必要があります。）

通常、イベントは、次の段階を遷移します。

- 開始
- 保留
- 承認済み
- 実行
- 完了
- ポスト

注: Identity Manager には、EventListeners という名のフックが用意されています。このフックは、特定のイベントまたはイベントのグループを監視します。 イベントが発生すると、イベントと現在のイベントの状態に見合ったカスタム ビジネス ロジックがイベント リスナにより実行されます。 Event Listener API を使うと、カスタム イベント リスナを作成できます。（詳細については、「Programming Guide for Java」を参照してください）。

第 4 章: セルフサービス タスク

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 Identity Manager のセルフサービス タスク (79 ページ)
自己管理ロールへのアクセス制限 (80 ページ)
セルフサービス タスクへのアクセス (80 ページ)
企業の Web サイトへのセルフサービス リンクの埋め込み (81 ページ)
複数のセルフサービス タスクの設定 (82 ページ)

CA Identity Manager のセルフサービス タスク

セルフサービス タスクは、ユーザが自分のプロファイルを管理するために使用できる CA Identity Manager タスクです。 このタスクには以下の 2 つの種類があります。

- パブリック タスク: ユーザがログイン認証情報を提供せずに使用できるタスクです。 パブリック タスクの例は、自己登録、忘れたパスワード、忘れたユーザ ID のタスクです。
- 保護タスク: ユーザによる有効な認定情報の入力が必要なタスクです。 例として、パスワードまたはプロファイル情報の変更タスクなどがあります。 これらのタスクへのアクセスを取得するには、自己管理マネージャなどのロールをユーザに指定する必要があります。

以下の表に、CA Identity Manager をインストールすると使用できる、デフォルトのセルフサービス タスクを示します。

タスク タイプ	タスク
パブリック タスク	■ 自己登録: ユーザが企業の Web サイトに登録することができます。 ■ 忘れたパスワードのリセット: ユーザが忘れたパスワードをリセットできます。 ■ 忘れたパスワード: CA Identity Manager にログインするときにユーザが使用できる一時パスワードを表示します。 ユーザがログインすると、新しいパスワードの入力が求められます。 ■ 忘れたユーザ ID : 忘れたユーザ ID を取得またはリセットします。

タスク タイプ	タスク
保護タスク	■ マイ パスワードの変更：ユーザがパスワードをリセットできます。 ■ マイ プロファイルの変更：住所および電話番号などのプロファイル情報を保守します。 ■ マイ グループの変更：ユーザがグループに参加することができます。 ■ マイ ロールの表示：ユーザのロールを表示します。 ■ サブミット済みタスクの表示：ユーザが開始した CA Identity Manager タスクを表示します。

自己管理ロールへのアクセス制限

デフォルトでは、ユーザが自分のプロファイル情報を管理し、ロールとサブミット済みタスクを表示できる Self Manager（自己管理）ロールは、すべてのユーザに割り当てられます。

自己管理ロールをユーザのサブセットに付与するには、「管理ロールのメンバ ポリシーの定義」で説明したように、既存のメンバを削除して、新しいポリシーを作成します。

セルフサービス タスクへのアクセス

Identity Manager 環境にセルフサービス タスクを設定すると、これらのタスクの URL を企業 Web サイトに追加できます。

セルフサービス タスクの URL は、以下のようなフォーマットになります。

http://domain/idm/alias/index.jsp?task.tag=task_tag

各項目の説明：

- <domain> は、CA Identity Manager が稼動しているシステムの完全修飾ドメイン名
- alias は、Identity Manager 環境のパブリック エイリアス
- task_tag は、タスクの一意の識別子

  デフォルトの［忘れたパスワードのリセット］タスクでは、タスク タグは ForgottenPasswordReset になります。

  http://domain/idm/im/imcss/index.jsp?task.tag=ForgottenPasswordReset

  デフォルトの［忘れたユーザ ID］タスクでは、タグは ForgottenUserID になります。

  http://domain/idm/im/imcss/index.jsp?task.tag=ForgottenUserID

企業の Web サイトへのセルフサービス リンクの埋め込み

企業の Web サイトからパブリックのセルフサービス タスクへのアクセスを許可するには、Web ページのいずれかにリンクを追加します。 ユーザがリンクをクリックすると、Identity Manager タスク画面が開きます。 ユーザがタスクを完了すると、デフォルトで Identity Manager ユーザ コンソールにリダイレクトされます。

ユーザがリダイレクトされるページを変更するには、以下のように、リンクに関連付けられた Identity Manager URL に task.RedirectURL タグを追加します。

```
<A
href="http://domain/idm/public_alias/ca12/index.jsp?task.tag=tasktag&task.RedirectURL
=http://domain/redirect_URL">link text</A>
```

domain

Identity Manager がインストールされているシステムの完全修飾ドメイン名。

public_alias

Identity Manager のパブリック タスクにアクセスできるように、URL に追加された一意の文字列。

パブリック タスクはセルフサービス タスクです。たとえば、自己登録や、忘れたパスワードのタスクなどがあります。 パブリック タスクにアクセスするには、ユーザのログインは必要ありません。

注: パブリック タスクおよびエイリアスの詳細については、「Configuration Guide」を参照してください。

tasktag

タスクの一意な識別子。 タスク タグを決定するには、[管理タスクの変更]を使用してタスクのプロファイルを表示します。

redirect_URL

Identity Manager タスクをサブミットした後に、ユーザが送られる URL。

たとえば、ユーザが自己登録したら[Welcome]ページにリダイレクトできます。

link text

ターゲット URL にアクセスするためにユーザがクリックするテキスト。

たとえば、企業は、ユーザが忘れたパスワードをリセットし、そのユーザをようこそページに導くリンクを追加できます。

リンクは以下のようになります。

```
 <A href="http://myserver.mycompany.org/idm/Employees/ca12/ index.jsp?task.tag=
ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/
welcome.html">Reset My Password</A>
```

セルフサービス タスクにアクセスしたページにユーザを戻すには、以下のように RefererURL を task.RedirectURL タグの値として指定します。

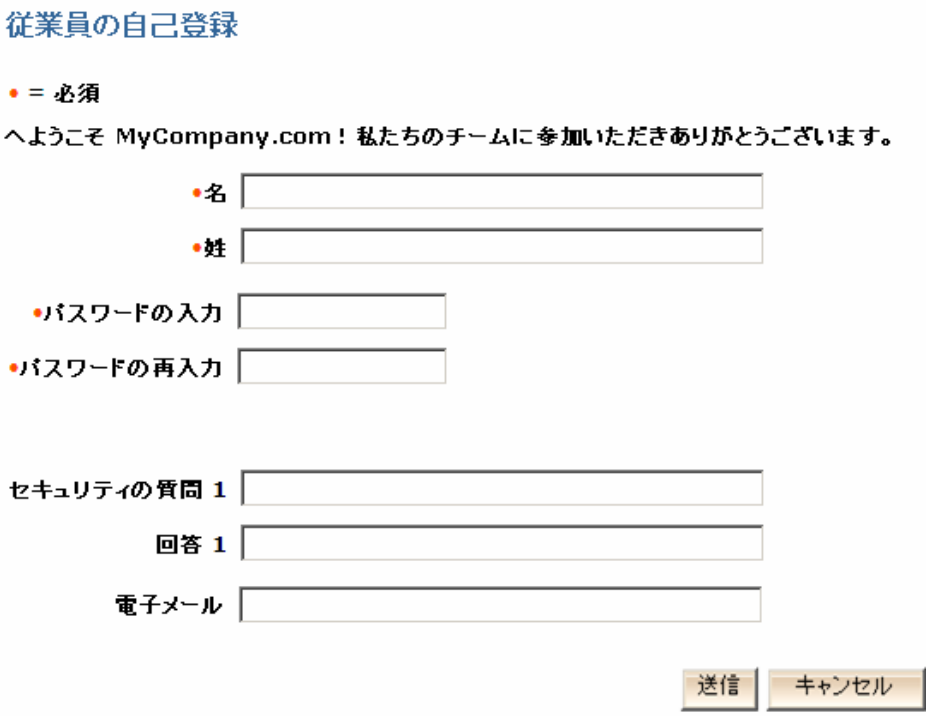
<A href="http://domain/idm/public_alias/ca12/index.jsp?task.tag=tasktag&task.RedirectURL=RefererURL</A>

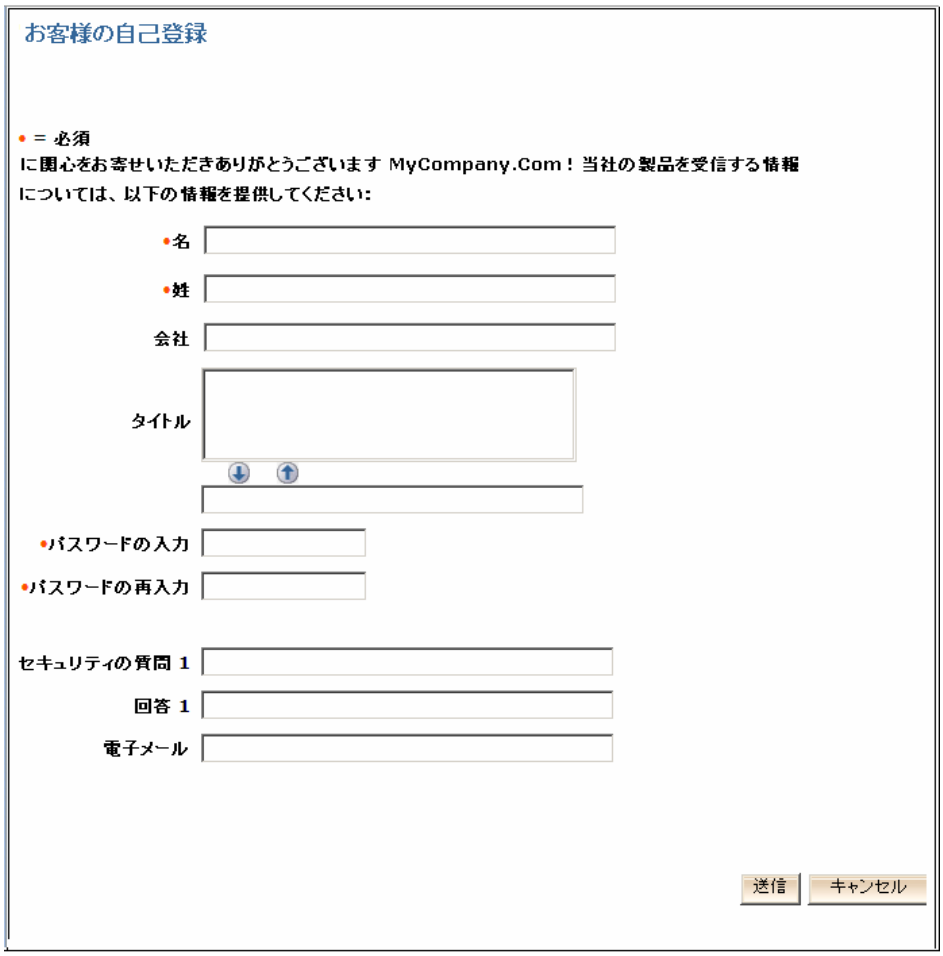
複数のセルフサービス タスクの設定

さまざまなタイプのユーザ用に複数のセルフサービス タスクを作成できます。 たとえば、新しい従業員を登録するタスクを作成し、顧客を登録する別のタスクを作成することができます。 異なるセルフ登録タスクを使用すると、以下のことを実行できます。

- さまざまな情報の収集
- さまざまな組織のユーザの登録
- 登録後、個別のログアウト ページへのユーザのリダイレクト
- さまざまなブランド設定の使用

以下の図に、新しい従業員および顧客の個別の自己登録タスクを示します。





同じ種類のセルフサービス タスクを複数設定するには、タスクの作成時に一意のタグを指定します。［タグ］フィールドは、タスクの［プロファイルの設定］画面上にあります。

タスクにアクセスするリンクを Web サイトに追加する場合は、タスク タグを追加して、一意の URL を作成します。

たとえば、以下のように 2 つのタスクを作成できます。

タスク	タグ	URL
新しい従業員として登録	selfregistration_employee	http://<domain>/idm/<im>/index.jsp?task.tag=SelfRegistration_employee

タスク	タグ	URL
顧客として登録	selfregistration_customer	http://<domain>/idm/<im>/index.jsp?task.tag=SelfRegistration_customer

第 5 章: ユーザ

このセクションには、以下のトピックが含まれています。

ユーザの作成 (85 ページ)
ユーザの管理 (86 ページ)
ユーザの変更 (86 ページ)
エンドポイント アカウントの表示または変更 (87 ページ)
ユーザへのロールの割り当て (88 ページ)

ユーザの作成

この手順を使用して、ユーザのプロファイルを作成します。 Identity Manager 環境での[ユーザの作成]タスクの設定内容に応じて、このタスクを使用してユーザをグループに追加したり、ユーザを管理ロールまたはプロビジョニング ロールのメンバにすることもできます。

ユーザの作成方法

1. ユーザの管理権限を持つユーザとしてユーザ コンソールにログインします。

   デフォルトのユーザ マネージャ ロールにより、ユーザに適切な権限が与えられます。

2. [ユーザ]-[ユーザの管理]-[ユーザの作成]を選択します。

   [ユーザの作成]タスクが開きます。

3. 必要に応じて、[プロファイル]タブのフィールドに入力します。

4. 該当する場合は、タスク内のその他のタブのフィールドに入力します。

5. [送信]をクリックします。

   CA Identity Manager によってユーザが作成されます。

ユーザの管理

[ユーザの管理]タスクを使用して、管理するユーザを検索できます。 ユーザを選択すると、CA Identity Manager に、ユーザの管理に使用できるタスクのリストが表示されます。

たとえば、この方法を使用してユーザを変更するには、[ユーザ]カテゴリを選択し、[ユーザの管理]タスクを選択します。 管理するユーザを検索して選択します。 検索結果の中からアイコンをクリックすると、その選択したユーザの管理に使用できるタスクのリストが表示されます。 このリストから[ユーザの変更]や他の適切なタスクを選択できます。

ユーザを管理するには、次の手順に従います。

1. [ユーザ]-[ユーザの管理]-[ユーザの管理]を選択します。

   ユーザを検索できる検索画面が開きます。

2. 検索条件を入力し、[検索]をクリックします。

   CA Identity Manager に、検索フィルタで条件に一致するユーザのリストが表示されます。

3. 管理するユーザの横にある右方向矢印アイコンをクリックします。

   CA Identity Manager に、そのユーザで実行できるタスクのリストが表示されます。

4. 使用するタスクを選択します。
5. タスクを完了して、[送信]をクリックします。

ユーザの変更

[ユーザの変更]タスクを使用して、ユーザのプロファイル情報を変更するか、環境での[ユーザの作成]タスクの設定内容に応じて、ユーザのグループおよびロール メンバシップを管理します。

ユーザを変更する方法

1. ユーザの管理権限を持つユーザとしてユーザ コンソールにログインします。

   デフォルトのユーザ マネージャ ロールにより、ユーザに適切な権限が与えられます。

2. [ユーザ]-[ユーザの管理]-[ユーザの変更]を選択します。

   [ユーザの変更]タスクが開きます。

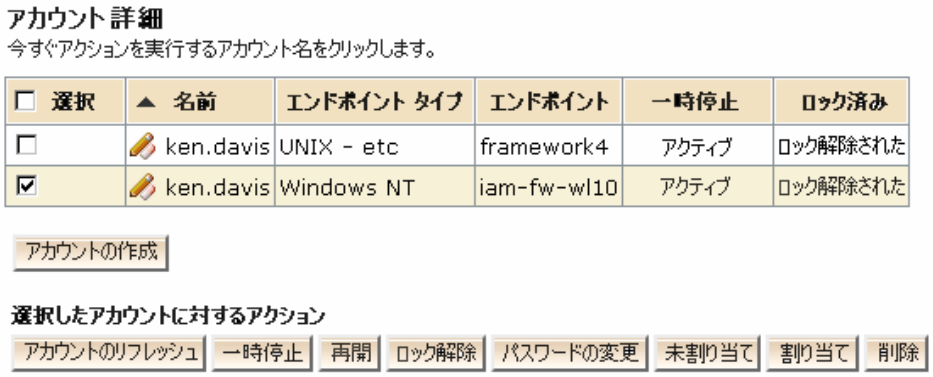
3. 必要に応じて、[プロファイル]タブのフィールドを変更します。

4. 該当する場合は、タスク内のその他のタブのフィールドを変更します。
5. [送信]をクリックします。

   CA Identity Manager で、ユーザのプロファイルが変更されます。

エンドポイント アカウントの表示または変更

ユーザの表示やマイ プロファイルの変更など、ユーザのプロファイルを表示することが許可されるタスクには、そのユーザのアカウントをエンドポイントにリストする[アカウント]タブが含まれています。



それぞれのアカウントについて、アカウント名、アカウントが存在するエンドポイント、アカウントのステータスなどの情報が表示されます。 変更のタスクには、ユーザ パスワードの変更、アカウントのロックまたは一時停止などで使用できるオプションがあります。

この例では、[アカウント]タブに[検索]ボタンが含まれていますが、これは検索画面で設定されるタブを表しています。 リスト画面、または検索画面、あるいはその両方を使用するよう、このタブを設定できます。

- 両方の画面を設定する場合は、検索画面で検索結果のフィールドを決定します。
- リスト画面のみを設定する場合は、リスト画面で検索結果のフィールドを決定します。
- 画面を両方とも設定しない場合、[アカウント]タブは静的なリスト表示を使用します。これは、列を表示するために[アカウント]タブをカスタマイズできないことを意味しています。

[アカウント]タブで設定可能な他のオプションの詳細については、[アカウントの設定]タブのユーザ コンソール ヘルプを参照してください。

ユーザへのロールの割り当て

以下のいずれかの方法で、ロールをユーザに割り当てることができます。

- [ロール メンバ/管理者の変更]タスクを使用して 1 つのロールから複数のユーザを追加または削除します。
- [ユーザの変更]タスクの[管理ロール]タブ、[プロビジョニング ロール]タブ、または[アクセス ロール]タブを使用して、管理ロール、プロビジョニング ロール、またはアクセス ロールを単一ユーザに割り当てます。
- ロールの[メンバ]タブでメンバ ポリシーを変更します。

  メンバ ポリシーの変更により、 Identity Manager で、ロールをユーザに自動的に割り当てるために使用する基準が変更されます。 たとえば、メンバ ポリシーには、マネージャの役職を持つすべてのユーザが、ユーザ マネージャ ロールを持つことを記載できます。

  注: メンバ ポリシーの詳細については、「メンバ ルール、管理ルール、および所有者ルール (22 ページ)」を参照してください。

[ロール メンバ/管理者の変更]タスクでのロールの割り当て

[ロール メンバ/管理者の変更]タスクによって、ロールのメンバまたは管理者としてユーザを追加または削除できます。

このタスクを使用すると、同時に複数ユーザを追加または削除できます。

ロール メンバまたは管理者を変更するには、以下の手順に従います。

1. ロールの管理権限を持つユーザとしてユーザ コンソールにログインします。
2. [ロールおよびタスク]-[管理タスク]-[管理メンバ/管理者の変更]を選択します。

   Identity Manager には、管理できるロールのリストが表示されます。 ロールをリストに表示するには、ロールの管理者である必要があります。必要に応じて、ロールは以下のオプションを選択する必要があります。

   管理者は、このロールのメンバを追加および削除できます。

   管理者は、このロールの管理者を追加および削除できます。
3. ロールのメンバまたは管理者を変更するかどうかに応じて、[メンバシップ]タブまたは[管理者]タブを選択します。

   Identity Manager には、既存のメンバまたは管理者のリストが表示されます。
4. ロールからメンバまたは管理者を削除するには 、ユーザ名の横にあるチェックボックスをオフにします。 次に、[送信]をクリックします。

5. 新しいユーザを追加するには、以下の手順に従います。
   a. [ユーザの追加]ボタンをクリックします。

      Identity Manager では、ユーザ検索画面が開きます。

   b. メンバまたは管理者として追加するユーザを検索して選択します。

      Identity Manager では、選択したユーザをメンバまたは管理者のリストに追加します。
6. [送信]をクリックします。

[ユーザの変更]タスクでのロールの割り当て

[ユーザの変更]タスクの[管理ロール]タブ、[プロビジョニング ロール]タブ、または[アクセス ロール]タブを使用して、追加の管理ロール、プロビジョニング ロール、またはアクセス ロールを単一ユーザに割り当てます。

注: [ユーザの作成]タスクでもこの 3 つのタブを使うことができます。

ユーザを変更する方法

1. ユーザの管理権限を持つユーザとしてユーザ コンソールにログインします。

   デフォルトのユーザ マネージャ ロールにより、ユーザに適切な権限が与えられます。
2. [ユーザ]-[ユーザの管理]-[ユーザの変更]を選択します。

   [ユーザの変更]タスクが開きます。

3. 必要に応じて、以下のタブのいずれかを選択します。
   - ［管理ロール］
   - ［プロビジョニング ロール］
   - ［アクセス ロール］

   CA Identity Manager に、選択したタブが表示されます。
4. 以下のいずれかのボタンをクリックします。
   - ロール タイプ ロールの追加

     ロール タイプは、管理ロール、プロビジョニング ロールまたはアクセス ロールを表します。

     このボタンをクリックすると、CA Identity Manager に、追加するロールを検索して選択できる検索画面が開きます。 CA Identity Manager に、管理できるロールのリストが表示されます。 ロールをリストに表示するには、ロールの管理者である必要があります。必要に応じて、ロールは以下のオプションを選択する必要があります。

     管理者は、このロールのメンバを追加および削除できます。

     管理者は、このロールの管理者を追加および削除できます。
   - ユーザからのコピー

     このボタンをクリックすると、CA Identity Manager に、現在のユーザが必要とするロールを持つユーザを検索して選択できる検索画面が開きます。
5. ［送信］をクリックします。

   CA Identity Manager で、指定されたロールのメンバまたは管理者としてユーザが追加されます。

第 6 章: パスワード管理

このセクションには、以下のトピックが含まれています。

CA Identity Manager のパスワード管理 (91 ページ)
パスワード ポリシー (92 ページ)
パスワードのリセットまたはアカウントのロック解除 (109 ページ)
パスワードの同期 (116 ページ)

CA Identity Manager のパスワード管理

CA Identity Manager は、ユーザ パスワードを管理する以下の機能を備えています。

- パスワード ポリシー: このポリシーでは、ルールと制限を適用し、パスワードの有効期限、構成、および使用方法を管理することで、ユーザ パスワードを管理します。
- パスワード マネージャ: パスワード マネージャ ロールを所有する管理者は、ユーザがヘルプ デスクに連絡したときにパスワードをリセットできます。
- セルフサービス パスワード管理: CA Identity Manager にはいくつかのセルフサービス タスクがあり、ユーザが自身のパスワードを管理することができます。 タスクには、以下のものがあります。
  - 自己登録: ユーザが企業の Web サイトに登録するときにパスワードを指定します。
  - マイ パスワードの変更:IT 担当者またはヘルプデスク担当者のサポートなしで、ユーザが自分のパスワードを変更できます。
  - 忘れたパスワード: CA Identity Manager がユーザの身元を確認した後で、ユーザが忘れたパスワードをリセットしたり、取得したりできます。
  - パスワードのリセットまたはアカウントのロック解除 (109 ページ): ユーザがパスワードを忘れた場合にパスワードをリセットまたは再取得したり、Identity Manager にアクセスする場合にシステムの Windows アカウントを解除できます。
  - 忘れたユーザ ID : CA Identity Manager がユーザの身元を確認した後で、忘れたユーザ ID を取得できます。
- エンドポイント アカウントのパスワードの同期: パスワードの変更は CA Identity Manager、プロビジョニング サーバ、およびこのサーバのターゲット システムで同期されます。 新しいパスワードは、Identity Manager パスワード ポリシーに対して検証されます。

パスワード ポリシー

パスワード ポリシーとは、パスワードの作成方法と、いつ期限が切れるかを決定する一連のルールおよび制限です。

パスワード ポリシーでは、以下の設定を行うことができます。

- パスワードの構成: 新しいパスワードの内容の要件を指定します。 たとえば、8 文字以上で数字と英字が含まれているパスワードを作成しなければならないように設定できます。
- 正規表現: 有効なパスワードの形式を決定する式を提供します。 パスワードがその形式に一致しなければならないか、一致してはならないかを指定することができます。
- 高度なパスワード オプション: パスワードを処理する前にパスワードを小文字にするなど、CA Identity Manager が実行しなければならないアクションを指定します。 複数のパスワード ポリシーを適用する場合は、パスワード ポリシーの優先順位を指定することもできます。

注: Identity Manager 環境のパスワード ポリシーを設定します。ただし、このポリシーは、この環境に関連付けられたユーザ ストアに適用されます。 ユーザ ディレクトリが、複数の環境に関連付けられている場合、ある環境で定義したパスワード ポリシーを別の環境にも適用することができます。

CA Identity Manager を SiteMinder と統合すると、パスワード管理のためにルールおよび規則を追加設定することができます。

- パスワードの有効期限: 経過日数や失敗したログイン試行回数など、パスワードを期限切れにするイベントを定義します。 パスワードが期限切れになると、ユーザ アカウントが無効になります。
- パスワード制限: パスワードの再使用に関する制限を設定します。 たとえば、90 日間経過しないと同じパスワードを再使用できないように設定できます。

SiteMinder ユーザは、SiteMinder 管理ユーザ インターフェースでパスワード ポリシーを設定することもできます。 これらのポリシーは、Identity Manager ユーザ コンソールに表示されます。

注: CA Identity Manager と SiteMinder を統合すると、パスワード構成ルール、正規表現、およびパスワードの詳細オプションを含むすべてのパスワード ポリシーが SiteMinder により実行されます。 SiteMinder が CA Identity Manager と異なるポリシーを実行する場合もあります。 SiteMinder パスワード ポリシーの詳細については、「CA SiteMinder Web Access Manager Policy Server Configuration Guide」を参照してください。

パスワード ポリシーの作成

パスワード ポリシーの作成方法

1. ユーザ コンソールで、[ポリシー]-[パスワード ポリシーの管理]-[パスワード ポリシーの作成]を選択します。
2. パスワード ポリシーの一意の名前とオプションの説明を入力します。
3. [有効]チェック ボックスをオンにして、Identity Manager 環境でパスワード ポリシーを使用します。
4. ユーザが自分のパスワードをリセットした場合のリダイレクト先のタスクを選択します(パスワードが期限切れになったり、パスワード ポリシーが変更されたりすると、強制的にパスワードをリセットされる可能性があります)。

   デフォルトでは、[マイ パスワードの変更]タスクにリダイレクトされます。

   指定するタスクはパブリック タスクまたは保護タスクです。 デフォルトの[パスワードサービス]タスクなどのパブリック タスクにはどのユーザもアクセスできます。 保護タスクにアクセスするには、ユーザが自己管理ロールなどのロールを所有する必要があります。
5. 以下のセクションの説明に従って、必要となるパスワード ポリシー設定を行います。
   - パスワード構成の設定(96 ページ)
   - 正規表現の指定(93 ページ)
   - パスワードの詳細オプションの設定(98 ページ)
6. CA Identity Manager を SiteMinder と統合する場合は、パスワード ポリシーの追加設定を行います。
   - パスワードの有効期限の設定(102 ページ)
   - パスワードの制限の設定(106 ページ)

正規表現の指定

パスワードに正規表現照合を使用すれば、正規表現(文字列照合を行うためのテキストパターン)を指定して、指定された正規表現に一致または不一致するかによってパスワードが有効であるかどうかを判断できます。 パスワードの先頭文字は数字とし、パスワードの最後の文字にはこの数字以外の文字を使用する、などのルールを設定する場合には、正規表現照合を使用すると便利です。

単独のパスワード ポリシーに対して複数の表現を設定するには、Identity Manager を SiteMinder と統合する必要があります。 複数の表現を作成する場合は、 許容可能なパスワードが、指定されたすべての表現に一致する必要があります。

新しい必須表現を追加する方法

1. [名前]フィールドに、表現の記述タグ(空白スペースなし)を入力します。
2. [Must Match(必須一致)]フィールドに、「正規表現の構文」(94 ページ) で説明されている構文を使用して正規表現を入力します。
3. パスワードが正規表現に一致してはいけない場合は、[一致してはいけない]列のチェック ボックスをオンにします。

注: CA Identity Manager を SiteMinder と統合すると、プラス(+)記号をクリックして表現を追加することで、複数の表現を指定できます。

例: すべてのパスワードの先頭を大文字または小文字に指定する場合には、次の正規表現定義を使用します。Name: MustStartAlpha

Expression: [a-zA-Z].*

正規表現の構文

ここでは、パスワードを照合するための正規表現の構文を説明します。 この構文は、レルムを指定する場合のリソース照合をサポートする正規表現構文で構成されています。

文字	結果
¥	メタキャラクタ(「*」など)を引用する場合に使用
¥¥	1 つの「¥」文字と一致
(A)	副次式のグループ化 (パターンの評価順序に影響)
[abc]	単純な文字クラス (文字 abc...の中の任意の 1 文字に一致)
[a-zA-Z]	範囲指定のある文字クラス(a から z、A から Z の範囲内にある 1 文字に一致)
[^abc]	文字 abc... 以外の任意の 1 文字に一致
.	改行以外の任意の 1 文字と一致
^	行の先頭に一致
$	行の末尾に一致

文字	結果
A*	A が 0 回または任意の回数現れるものに一致 (greedy)
A+	A が 1 回以上繰り返すものに一致(greedy)
A?	A が 1 回または 0 回現れるものに一致(greedy)
A*?	A が 0 回以上繰り返すものに一致(reluctant)
A+?	A が 1 回以上繰り返すものに一致(reluctant)
A??	A が 0 回または 1 回現れるものに一致(reluctant)
AB	A の後に B が続くものに一致
A|B	A または B のいずれかが現れるものに一致
¥1	1 番最初のかっこで囲まれた副次式への後方参照
¥n	n 番目のかっこで囲まれた副次式への後方参照

量指定子(+、*、?)はデフォルトで Greedy です。つまり、全体的な照合を中断することなく、文字列内で可能な限り多くの要素と一致します。 控えめ(Non-greedy)な照合を行うには、量指定子に「?」を追加します。 控えめな量指定子を使用すると、照合時に文字列のできるだけ少ない要素と一致します。

パスワード ポリシーの管理

適切な権限を所有する管理者は、パスワード ポリシーの表示、変更、削除のタスクを使用して、パスワード ポリシーを管理できます。 デフォルトでは、これらのタスクは[ポリシー]カテゴリに表示されます。

これらのタスクのいずれかにアクセスすると、CA Identity Manager には、現在の Identity Manager 環境に関連付けられたユーザ ストアに適用するパスワード ポリシーの一覧が表示されます。 CA Identity Manager を SiteMinder と統合すると、このリストには、パスワード サービスを使用して SiteMinder 管理ユーザ インターフェースで作成されたパスワード ポリシーも表示されます。 CA Identity Manager または SiteMinder で作成されたパスワード ポリシーを管理できます。

SiteMinder のパスワード サービスの詳細については、「CA SiteMinder Web Access Manager Policy Server Configuration Guide」を参照してください。

パスワード構成の設定

新しいパスワードの作成方法を決定するルールを指定できます。

注: パスワード構成を設定するときには、各文字要件の値を決定する際に最大パスワード長を考慮します。 必要な文字、数字、またはその両方の総数が最大パスワード長を超えると、すべてのパスワードが拒否されます。 たとえば、[文字] に 6 が設定されていて、[数字] にも 6 が設定されている場合、パスワードには 12 文字（6 文字 + 数字 6 桁）以上必要になります。 この例の場合、パスワードの最大文字数が 8 文字に設定されていると、すべてのパスワードが拒否されます。

パスワード構成の設定には以下のものがあります。

最小パスワード長

ユーザ パスワードの最小長を指定します。

パスワードの最大長

ユーザ パスワードの最大長を指定します。

最大繰り返し文字数

パスワード内で連続表示可能な反復文字の最大数を決定します。

たとえば、この値に「3」を設定すると、パスワードに「aaaa」のように指定することはできません。 ただし、「aaa」は指定できます。 この値を設定して、ユーザが 1 種類の文字で構成されるパスワードを入力できないようにします。

大文字

大文字の英字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小文字数を指定します。

小文字

小文字の英字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小文字数を指定します。

文字

文字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小文字数を指定します。

注: 大文字と小文字の使用を許可すると、[文字]チェック ボックスは自動的にオンになります。

桁

数字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小文字数を指定します。

文字と数字

文字と数字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小数を指定します。［数字］と共にこの設定を設定すると、文字はどちらの要件も満たすことができます。 たとえば、［数字］とこの設定が 4 の場合、パスワード「1234」は有効です。

注: 大文字、小文字、文字、または数字の使用を許可すると、［文字と数字］チェック ボックスは自動的にオンになります。

句読点

句読点の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小数を指定します。 ここでいう句読点とは、ピリオド（.）、カンマ（,）、感嘆符（!）、スラッシュ（/）、ダッシュ（-）、ハイフン（-）です。

印刷不能

印刷不可能文字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小数を指定します。印刷不可能文字は、コンピュータ画面には表示されません。

注: 一部のブラウザでは、印刷不可能文字をサポートしていません。

英数字以外

キーボードに表記されている句読点およびその他の記号（「@」、「$」、「*」など）のように、英数字でない文字の使用を許可するかどうかを指定し、許可する場合にはパスワードに含める必要がある最小文字数を指定します。 英数字でない文字には、印刷不可能文字も含まれます。 また、英数字でない文字は [句読点] および [印刷不可能文字] の文字要件も満たします。

高度なパスワード オプションの設定

パスワード ポリシーの詳細オプションでは、検証および格納する前にパスワードの前処理（すべての文字を大文字に強制的に変換するなど）を実行するように設定したり、ポリシーに優先順位を設定して、同じユーザ ディレクトリまたはネームスペースに適用される複数のパスワード ポリシーの評価順序を指定したりすることができます。

大文字/小文字を強制しない | 強制的に大文字に変換 | 強制的に小文字に変換

処理および格納する前にパスワードを大文字または小文字にする必要かあるかどうかを決定します。 大文字または小文字に強制的に変換する場合には、[大文字の使用を強制] ラジオボタンまたは [小文字の使用を強制] ラジオボタンをオンにします。 強制変換を行わない場合は、[大文字/小文字の使用の強制なし] ラジオボタンがオンになっていることを確認してください。

重要： 大文字または小文字に強制的に変換する場合には、定義されている大文字または小文字の変換の構成要件（96 ページ）と矛盾がないことを確認してください。

先頭の空白の削除

処理の前にパスワードから先頭の空白を削除します。

末尾の空白の削除

処理の前にパスワードから末尾の空白を削除します。

埋め込み空白の削除

処理の前に埋め込み空白をすべて削除します。

注： ユーザ ディレクトリによっては、パスワード ポリシーの設定に関係なく、格納される前に（ユーザ パスワードが保存される）属性値の先頭または末尾の空白が自動的に削除される場合があります。

評価優先度

パスワード ポリシーの評価優先度を指定します。 この値は、0（デフォルト）から 999 の間で設定します。 適用可能なポリシーは、降順（999 が最初、0 が最後）で評価されます。

優先度の低いパスワード ポリシーの適用

設定対象の後に、優先度の低いパスワード ポリシーを適用するかどうかを決定します。

注： CA Identity Manager を SiteMinder に統合した場合のみ、このフィールドを使用できます。

SiteMinder と組み合わせたパスワード ポリシー

CA Identity Manager では、ルールと制限を適用してパスワードの有効期限、構成、および使用方法を管理することで、ユーザ パスワードを管理する基本的なパスワード ポリシーを作成できます。

CA Identity Manager を SiteMinder と統合すると、以下のような追加ルールおよび制限を定義できる高度なパスワード ポリシーを作成できます。

- ディレクトリ フィルタ
- パスワードの有効期限
  - ログインの失敗または成功の追跡
  - ログインの認証
  - 変更されない場合パスワードは失効
  - パスワードの未使用
  - パスワードが正しくありません。
  - 複数の正規表現
- パスワードの制限
  - 再使用までの最短日数
  - 再使用までの最少パスワード数
  - 前のパスワードとの差異の割合(%)
  - 差異をチェックする場合に順番を無視
  - プロファイル属性のマッチング
  - 辞書のマッチング

パスワード ポリシーとリレーショナル データベース

リレーショナル データベースに適用されるパスワード ポリシーを設定する場合は、以下のフォーマットを使用して、SiteMinder User Directory のパスワード データ属性を設定する必要があります。

tablename.columnname

実行中の構文の問題発生を回避するために、プライマリ テーブルにこのフィールドを配置することをお勧めします。

ユーザ セットへのパスワード ポリシーの適用

高度なパスワード ポリシーの設定のために Identity Manager を SiteMinder と統合すると、パスワード ポリシーを適用するユーザ セットを決定するルールを指定することができます。 これにより、一般的な従業員用のパスワード ポリシーと高レベルのマネージャ用のより厳しいポリシーを作成できるようになります。

パスワード ポリシーのルールを指定する方法

1. ユーザ コンソールでパスワード ポリシーを作成または変更します。
2. [ディレクトリ フィルタ]フィールドで、設定するフィルタのタイプを選択します。

   各フィルタ タイプの説明については以下の表を参照してください。

   注: [ディレクトリ フィルタ]リスト ボックスに表示されるフィルタ タイプのオプションは、パスワード ポリシーが適用されるユーザ ストアのタイプによって決まります。フィルタ タイプによっては、リレーショナル データベースや CA Directory のユーザ ストアでは利用できないものがあります。
3. 属性や演算子を選択し値を入力して、条件を指定します。
4. 条件をさらに追加するには、プラス記号をクリックします。

以下の表に、ディレクトリ フィルタ タイプのオプションおよび各フィルタ タイプの例を示します。

フィルタ タイプ	このフィルタの用途	例
ディレクトリ全体	ユーザ ストアのすべてのユーザにパスワード ポリシーを適用します。	該当なし。
所属グループ	特定のグループを検索します。	名前 = 製品チーム
ユーザは、	単一のユーザを検索して選択します。	ユーザ ID = jsmith
ユーザ フィルタ (リレーショナル データベースでは使用できません)	ユーザに対するフィルタを指定します。	従業員タイプ = 受託業者
ユーザ検索式	ユーザの検索クエリを入力します。 **注**: LDAP 検索式の詳細については、「CA SiteMinder Web Access Manager Policy Server Configuration Guide」を参照してください。	uid=*smith

フィルタ タイプ	このフィルタの用途	例
グループ フィルタ (リレーショナル データベースおよびプロビジョニング サーバのユーザ ストアでは使用できません)	グループに対するフィルタを指定します。	自己購読 = *
グループ検索式 (プロビジョニング サーバのユーザ ストアでは使用できません)	グループの検索クエリを入力します。 **注**: LDAP 検索式の詳細については、「CA SiteMinder Web Access Manager Policy Server Configuration Guide」を参照してください。	cn= セールス*
組織フィルタ (リレーショナル データベースおよびプロビジョニング サーバのユーザ ストアでは使用できません)	組織に対するフィルタを指定します。 **注**: LDAP 検索式の詳細については、「CA SiteMinder Web Access Manager Policy Server Configuration Guide」を参照してください。	組織名 = *マーケティング
組織検索式 (リレーショナル データベースおよびプロビジョニング サーバのユーザ ストアでは使用できません)	組織の検索クエリを入力します。 **注**: LDAP 検索式の詳細については、「CA SiteMinder Web Access Manager Policy Server Configuration Guide」を参照してください。	ou=ボストン
検索	フィルタ タイプのオプションに含まれていないクエリを指定します。 **注**: LDAP 検索式の詳細については、「CA SiteMinder Web Access Manager Policy Server Configuration Guide」を参照してください。	(&(uid=*smith)(ou=ボストン))

パスワードの有効期限の設定

CA Identity Manager を SiteMinder と統合すると、管理者は、ユーザ アクセスを管理しやすいように、ログイン試行時の失敗が複数回にわたる場合やアカウントがアクティブでない場合をイベントとして定義できます。 このようなイベントが発生すると、イベントを引き起こしたユーザ アカウントを無効にし、必要に応じて新しい Web ページにユーザをリダイレクトします。

パスワードの有効期限では以下の設定が可能です。

- ［失敗/正常ログインの追跡］チェック ボックス
- ［ログイン追跡に失敗したときに認証を実施する］チェックボックス
- ［変更されない場合パスワードは失効］設定
- ［不正なパスワード］設定
- ［パスワードを使用しないので無効化］設定

［ 失敗/正常ログインの追跡］チェック ボックス

注: ログインの失敗または成功を追跡するには、Identity Manager を SiteMinder と統合する必要があります。 詳細については、「実装ガイド」を参照してください。

このチェック ボックスのオン/オフによって、ログイン最終時刻をはじめとするユーザが試行したログインを追跡する機能を有効/無効にします。 このチェック ボックスをオンにすると、ログイン情報がユーザ ストアの属性に書き込まれます。

［失敗ログインの追跡］チェック ボックスをオンにすると、［不正なパスワード］セクションおよび ［ログイン追跡失敗時の認証］チェック ボックスがアクティブになります。

［正常ログインの追跡］チェック ボックスをオンにすると、［パスワードを使用しないので無効化］セクションおよび ［ログイン追跡失敗時の認証］チェック ボックスがアクティブになります。

ログイン詳細の追跡を無効にするときにパスワード ポリシーが複数ある場合、使用できるすべてのパスワード ポリシーがログイン詳細を無効にしていることを確認してください。 そうでない場合、たとえば 1 つのポリシーがログイン詳細の追跡を有効にしていると、複数のパスワードポリシーが正しく機能しなくなります。

[ログイン追跡に失敗したときに認証を実施する] チェックボックス

注: ログインを無効にするには、Identity Manager を SiteMinder と統合する必要があります。 詳細については、「Implementation Guide」を参照してください。

このチェックボックスのオン/オフによって、ユーザ追跡が失敗したときのログインの可/不可を決定します。 デフォルトでは、このチェックボックスはオフです。したがって、ユーザアクティビティをユーザディレクトリに書き込めない場合、ユーザはログインできません。ただし、チェックボックスをオンにした場合は、パスワードデータをユーザディレクトリに書き込めなくても、ユーザはログインできます。

注: このチェック ボックスをオンにするには、[失敗ログインの追跡]または[正常ログインの追跡]チェック ボックスもオンにする必要があります。

[変更されない場合パスワードは失効]設定

注: パスワードの有効期限設定を行うには、Identity Manager を SiteMinder と統合する必要があります。 詳細については、「Implementation Guide」を参照してください。

[変更されない場合パスワードは失効]フィールドで、期限切れのパスワードを所有者が変更しなかった場合の動作を設定できます。 必要に応じて、どの程度事前にパスワードの有効期限切れをユーザに警告するかを指定できます。

以下のフィールドを設定できます。

期限切れまでの日数 <n> 日

パスワードが期限切れになるまでの日数を指定します。この間、ユーザの無効化やパスワード変更の強制は行われません。

注: 指定した日数が経過してからユーザがログインを試行するまで、ユーザ アカウントは無効になりません。

ユーザを無効にする

このラジオ ボタンをオンにすると、ユーザのパスワードが期限切れになったときに、このユーザは無効になります。 無効になったユーザは、以下の操作で有効にすることができます。

- ユーザ コンソールの[ユーザの有効化/無効化]タスク（デフォルトのシステム マネージャ、組織マネージャ、およびセキュリティ マネージャ ロールには[ユーザの有効化/無効化]タスクが含まれています）。
- SiteMinder 管理ユーザ インターフェース

  注: 詳細については、「CA SiteMinder Web Access Manager Policy Server Administration Guide」を参照してください。

パスワード変更の強制

このラジオ ボタンをオンにすると、ユーザのパスワードが期限切れになった場合、ユーザがログインを試みたときに、Identity Manager によりパスワードの変更が強制されます。

有効期限の警告の発行日数 <n> 日

パスワードの有効期限切れを何日前に(何日間)ユーザに通知するかを指定できます。

[パスワードを使用しないので無効化]設定

注: パスワードの非アクティブ設定を設定するには、Identity Manager を SiteMinder と統合する必要があります。 詳細については、「Implementation Guide」を参照してください。

[パスワードを使用しないので無効化]設定では、ユーザ アカウントがアクティブでないと判断するログインの間隔を指定できます。 また、アカウントがアクティブでないと判断されたユーザが正常にログインするための処理を、このセクションを使って指定することもできます。

注: [パスワードを使用しないので無効化]セクションの設定を行うには、[ログイン詳細を追跡する(ログインの試行、成功したログイン)]チェック ボックスをオンにします。

[パスワードを使用しないので無効化]セクションの内容は、以下のとおりです。

- 期限切れまでの日数 <数値> 日 - ユーザのパスワードが期限切れになるまでの非アクティブ日数を決定します。
- ユーザの無効化 - このラジオ ボタンをオンにすると、ユーザのパスワードがアクティブでないために期限切れになったときに、このユーザ アカウントが無効になります。 無効となったユーザは、[ユーザの有効化/無効化]タスクを使用して有効にすることができます。
- パスワードの変更の強制 - このラジオ ボタンをオンにすると、ユーザのパスワードがアクティブでないために期限切れになった場合、ユーザがログインを試みたときに、パスワードの変更が強制されます。

[不正なパスワード]設定

注: 不正なパスワード設定を設定するには、Identity Manager を SiteMinder と統合する必要があります。 詳細については、「Implementation Guide」を参照してください。

[不正なパスワード]設定では、ログインを何回失敗するとユーザ アカウントが無効になるかを指定できます。 また、ユーザが再度ログインできるようになるまでのアカウント無効期間を指定することもできます。

注: このセクションは、[失敗ログインの追跡]チェック ボックスがオンになっている場合のみ適用されます。

[不正なパスワード]セクションには、以下のフィールドがあります。

パスワードが無効になるまでの入力失敗回数 <n> 回

何回連続でログインに失敗するとユーザ アカウントが無効になるかを決定します。 不正なログインの回数を制限することによって、正しいパスワードが見つかるまで繰り返しパスワード入力してリソースにアクセスするプログラムからリソースを保護します。 指定された回数を超えてもユーザが正常にログインできないと、そのユーザのアカウントが無効になります。 管理者がこのアカウントを再度有効にする必要があります。

アカウントを再有効化するまでの時間 <n> 分

ユーザがログインを再度試行できるようになるか、アカウントが再び有効化(下記参照)されるまでに待機する時間(分)を指定します。 ユーザが別の不正なパスワードを入力した場合、アカウントは再度無効になります。 このとき、ユーザは指定された時間だけ待機してから、ログインを再試行しなければなりません。

1 回のログイン試行を許可

このラジオ ボタンをオンにすると、一度不正なパスワードを入力したユーザは、指定された分数が経過するまで再度ログインを試みることはできません。

再度有効にできるアカウント

このラジオ ボタンをオンにすると、不正なパスワードの入力によってユーザ アカウントが無効になった場合、指定された分数が経過した後にアカウントを再度有効にできます。

パスワードの制限の設定

注: パスワード制限を設定するには、Identity Manager を SiteMinder と統合する必要があります。 詳細については、「Implementation Guide」を参照してください。

パスワードポリシーを使って、パスワードの使用について制限を設けることができます。この制限は、パスワードを再使用できるまでにユーザが待機する期間、および以前に選択したパスワードとどの程度異なっている必要があるのかを決定します。 また、セキュリティ リスクがあるか、ユーザの個人情報が含まれると判断した用語を、ユーザに指定させないようにすることもできます。

[制限]セクションには、以下のフィールドがあります。

再使用までの最短日数

ユーザがパスワードを再使用できるまでの待機日数を指定します。

再使用までの最少パスワード数

ユーザがパスワードを再使用できるまでのパスワードの使用数を指定します。

注: 経過時間とパスワード数を指定した場合は、両方の条件を満たさないとパスワードを再使用できません。 たとえば、ユーザに対して以前のパスワードを再使用できるようになるまで、 365 日間の経過と、12 回のパスワードの指定を義務づけるパスワードポリシーを設定できます。 1 年経過した時点で使用したパスワード数が 6 の場合、さらに 6 つのパスワードを使用しないと、ユーザは最初のパスワードを再使用できません。

前のパスワードとの差異の割合 (%)

以前のパスワードに使用した文字と異なる文字をどれだけの割合(%)で新規パスワードに含める必要があるかを示します。 この値を 100 に設定した場合は、[差異をチェックする場合に順番を無視]チェック ボックスをオフにしていない限り、以前のパスワードで使用していた文字を、新規パスワードではすべて使用できないことになります。 このパラメータを[差異をチェックする場合に順番を無視]と共に使用した場合にどのように機能するかについては、以下の表を参照してください。

差異をチェックする場合に順番を無視

文字の割合(%)を判断する際、パスワード中での文字の位置を無視します。

たとえば、ユーザの最初のパスワードが BASEBALL12 で、[差異をチェックする場合に順番を無視]チェック ボックスがオンになっている場合、ユーザは新規パスワードに 12BASEBALL を選択できません。 このチェックボックスをオフにした場合は、各文字の出現順序が異なっているため、12BASEBALL をパスワードに指定できます。 このパラメータを[前のパスワードとの差異の割合(%)]と共に使用した場合にどのように機能するかについては、以下の表を参照してください。

高い安全性を確保するには、[相違点の確認時に順序を無視] チェックボックスをオンにするようにしてください。

パスワード	異なる割合 (%)	文字順を無視	使用可能
BASEBALL12 (旧)	0	選択済み	Y
12BASEBALL		選択解除済み	Y
BASEBALL12 (旧)	100	選択済み	N
12BASEBALL		選択解除済み	Y
BASEBALL12 (旧)	0	選択済み	Y
12SOFTBALL		選択解除済み	Y
BASEBALL12 (旧)	90	選択済み	N
12SOFTBALL		選択解除済み	Y
BASEBALL12 (旧)	100	選択済み	N
12SOFTBALL		選択解除済み	N

[プロファイル属性]

[一致する長さ]フィールドを設定すると、ユーザはパスワードに個人情報を使用できなくなります。 [一致する長さ]フィールドに、パスワード ポリシーがユーザ ディレクトリ エントリ内の属性と比較する最小連続文字数を指定します。 たとえば、値に 4 を設定した場合、パスワードがユーザの電話番号の下 4 桁で構成されていないことが確認されます。

辞書

パスワードに使用できない文字列の一覧を指定します。

注: 辞書ファイルの最後の行は、パスワード サービスによって使用される行で、この行の後には改行が必要です。改行がないと、この行はディクショナリ検索の対象から除外されます。

[辞書]設定には、以下のフィールドがあります。

- パス - 辞書ファイルの完全パスと名前を指定します。
- 一致する長さ - 辞書ファイルの値と比較される文字列の長さを制御します。 この比較では、文字列の(大文字/小文字)の区別は無視されます。 [一致する長さ]フィールドに何も指定しない場合、または 0 を指定した場合は、辞書内の文字列と完全一致したパスワードだけが拒否されます。 一致する長さが 0 より大きい場合は、以下の条件をすべて満たす場合にパスワード エントリが拒否されます。

  パスワードに、辞書エントリと同じ文字の並びで開始する部分文字列が含まれている。

  連続して一致している文字数が、[一致する長さ]フィールドで指定した数以上である。

  たとえば、以下を含む辞書ファイルがあるとします。

  lion

  tiger

  bear

  [一致する長さ]フィールドが 4 に設定されていると、結果は以下のようになります。

  「TeddyBear」は、辞書ファイルのエントリ「bear」に一致するため、拒否されます。

  「prestige」は、「tige」が辞書ファイルのエントリ「tiger」の最初の 4 文字と一致するため、拒否されます。

  「Geiger Counter」は、「iger」が辞書ファイルのエントリ「tiger」の最初の 4 文字に含まれていないので、受け入れられます。

パスワードのリセットまたはアカウントのロック解除

ユーザが Windows システムでパスワードを忘れた場合、Windows ログオン画面からユーザに入力を要求するようにセルフ サービスを設定できます。 以下のコンポーネントのいずれかをインストールして、この機能を使用できます。

- Windows 2000、2003、および XP システム用 GINA（Graphical Identification and Authorization）
- Windows VISTA および 2008 システム用 Credential Provider

この機能を使用すると、ユーザは、Cube Web ブラウザを使用して、[パスワード変更の要求]ページが表示されるセルフ サービスにログインできます。 このページへの入力後、[戻る]をクリックして、Windows ログオン画面に戻ります。

GINA または Credential Provider のインストール

GINA（Windows 2000、2003、および XP の場合）または Credential Provider（Windows Vista または 2008 の場合）は、ユーザが Identity Manager 環境へのアクセスに使用する Windows システムにインストールできます。

GINA または Credential Provider をインストールする方法

1. Identity Manager プロビジョニング コンポーネントのダウンロード、またはその他のインストール メディアを検索します。
2. Agent の下にあるインストーラを実行します。
3. ウィザードのプロンプトに従って、質問に回答します。
4. このコンポーネントをインストール後、適切な手順で設定します。
   - GINA の設定（110 ページ）
   - Credential Provider の設定（112 ページ）

GINA の設定

GINA 設定ツールを使用して、デフォルトの GINA 値を編集し、再パッケージ用にレジストリ(.reg)ファイルにエクスポートできます。 この設定は、現在のシステムにも適用することができます。

GINA を設定する方法

1. Windows Explorer で、GINA をインストールした場所に進みます。 次に、例を示します。

   C:\Program Files\CA\Identity Manager\Provisioning GINA

2. 次の実行可能ファイルをダブルクリックします。

   ginaconfig.exe

3. GINA の設定フィールドに以下の情報を入力します。

   [Link1 Command]

   ユーザが[Forgot Password]リンクをクリックしたときに実行される完全なコマンドラインです。 このリンクにより、パスワードの再設定用に、URL が Web インターフェースへロードされます。 たとえば、コマンドは次のようになります。

   http://eastern.local:8080/idm/pub/ca/index.jsp?task.tag=ForgottenPassword

   この URL の場合、実際の環境で自己登録が可能である必要があります。 また、Identity Manager 環境のセルフ サービス URL が、GINA をインストールしているシステムから機能することを確認してください。

   [Link2 Command]

   ユーザが[アカウントのロック解除]リンクをクリックしたときに実行される完全なコマンド ラインです。 このリンクにより、ユーザによるアカウントのロック解除が可能な Web インターフェースへ、URL がロードされます。

   [ドメイン]

   プロビジョニングのドメイン名です。

   [Section 508 Compliance](メニューで[戻る]を使用する)

   メニューで[戻る]の機能を有効にします。 選択されていない場合は、[戻る]ダイアログが使用されます。

4. [Secure Browser Settings]フィールドに以下のように入力します。

   [Default URL]

   link1_cmd または link2_cmd でコマンド ラインが指定されていない場合に移動するデフォルトのページです。

   [許可リスト]

   常にアクセスが許可される URL に一致する正規表現パターンです。

   [拒否リスト]

   常にアクセスが拒否される URL に一致する正規表現パターンです。

5. (オプション)[エクスポート]をクリックして、別のシステムに設定をエクスポートします。

6. [OK]をクリックして設定を保存します。

7. システムを再起動します。

クレデンシャル プロバイダの設定

設定ツールを使用して、クレデンシャル プロバイダをインストールしたシステムを設定します。

クレデンシャル プロバイダを設定する方法

1. Windows エクスプローラで、クレデンシャル プロバイダをインストールしたディレクトリに移動します。 以下に例を示します。

   C:¥Program Files¥CA¥Identity Manager¥Credential Provider

2. 次の実行可能ファイルをダブルクリックします。

   CAIMCredProvConfig.exe

3. [Credential Provider Settings]フィールドを以下のように入力します。

   [Link1 URL]

   ユーザが[Forgot Password]リンクをクリックするときに実行される完全なコマンドラインです。 このリンクは、パスワード リセット用の Web インターフェースへの URL である必要があります。

   たとえば、コマンドは次のようになります。

   http://eastern.local:8080/idm/pub/ca/index.jsp?task.tag=ForgottenPassword

   この URL の場合、実際の環境で自己登録が可能である必要があります。 さらに、IME 用のセルフ サービス URL がクレデンシャル プロバイダをインストールしているシステムから機能することを確認してください。

   [Link2 URL]

   ユーザが[アカウントのロック解除]リンクをクリックするときに実行される完全なコマンド ラインです。 このリンクは、ユーザがアカウントのロック解除を行うことができる Web インターフェースへの URL である必要があります。

   [ドメイン]

   プロビジョニングのドメイン名です。

4. [Secure Browser Settings]フィールドに以下のように入力します。

   [許可リスト]

   常にアクセスが許可される URL に一致する正規表現パターンです。

   [拒否リスト]

   常にアクセスが拒否される URL に一致する正規表現パターンです。

5. (オプション)[エクスポート]をクリックして、別のシステムに設定をエクスポートします。

6. [OK]をクリックして設定を保存します。

7. システムを再起動します。

レジストリの設定

GINA または Credential Provider を設定するための設定ツールがありますが、Windows レジストリを編集して同じ値を設定することができます。

GINA レジストリの設定

GINA 設定ツールを使用しない場合は、以下のキーで Windows レジストリ設定を編集できます。

[HKEY_LOCAL_MACHINE\FTWARE\ComputerAssociates\GINAUNLOCK]

gina

これは、現在チェーンしている GINA の値を保持しています。 通常、これは、Novell などの製品と統合している場合を除き、デフォルトの Microsoft Windows GINA である MSGINA.DLL になります。

link1_cmd

これは、[ログオン]ダイアログでリンク 1 を実行する完全なコマンド ラインです。

link2_cmd

これは、[ログオン]ダイアログでオプションのリンク 2 を実行する完全なコマンド ラインです。 たとえば、アカウントのロック解除を行うための Web サイトに移動するリンクを追加できます。

link2_cmd が空白の場合は、link1_cmd が[ログオン]ダイアログ ボックスに表示されます。

domain

プロビジョニングのドメイン名です。

langdir

ローカライズされた言語の DLL の場所です。

configdir

GINA がインストールされている場所のフル ディレクトリ パスです。

Credential Provider のレジストリ設定

Credential Provider 設定ツールを使用しない場合は、以下のキーで Windows レジストリ設定を編集できます。

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]

link1_cmd

これは、[ログオン]ダイアログでリンク 1 を実行する完全なコマンド ラインです。このリンクは、ユーザがリンク 1 をクリックすると移動できる URL として機能する必要があります。

link2_cmd

これは、[ログオン]ダイアログでオプションのリンク 2 を実行する完全なコマンド ラインです。 このリンクは、ユーザがリンク 2 をクリックすると移動できる URL として機能する必要があります。 たとえば、アカウントのロック解除を行うための Web サイトに移動するリンクを追加できます。

link2_cmd が空白の場合は、link1_cmd が[ログオン]ダイアログ ボックスに表示されます。

domain

プロビジョニングのドメイン名です。

langdir

ローカライズされた言語の DLL の場所です。

disablepwdcp

Microsoft Password Credential Provider 無効オプション。 1 は無効です。 0 は有効です。

CredentialProviderInstallPath

Credential Provider がインストールされている場所のフル ディレクトリ パスです。

configdir

Credential Provider がインストールされている場所のフル ディレクトリ パスです。

Cube ブラウザのレジストリ設定

Cube セキュア ブラウザのコンポーネントには、動作を制御するレジストリ値がいくつかあります。 以下のレジストリ キーに Cube 値が存在します。

[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Cube]

404

マシンが起動時にリモート プロビジョニング サーバに接続できない場合に表示される標準の HTML ドキュメントのパスです。

default

URL が Link1 Command または Link2 Command に含まれていない場合に移動するデフォルト ページです。

allow

明示的な許可 ACL。 常に許可される URL に一致する正規表現パターンです。 詳細については、「Cube アクセス制御リスト(115 ページ)」を参照してください。

拒否

明示的な拒否 ACL。 常にアクセスが拒否される URL に一致する正規表現パターンです。 詳細については、「Cube アクセス制御リスト(115 ページ)」を参照してください。

langdir

ローカライズされた言語の DLL の場所です。

Cube アクセス制御リスト

Cube ACL は、選択した URL への移動を明示的に許可または拒否する正規表現パターンです。 ACL は以下の順番で評価を行います。

1. 許可(最初にアクセス権が自動的に許可されます)
2. 拒否(拒否された URL が 2 番目に確認されます)

GINA アクセス制御リストの例

"allow"="(.pdf)"

すべての PDF ドキュメントの表示を許可します。

"deny"="(.doc|.xls)"

Microsoft Word および Excel のドキュメントへのアクセスを拒否します。

Windows ログイン用パスワードのリセット

GINA または Credential Provider が Windows システムにインストールされると、[忘れたパスワード]リンクが、標準 Microsoft Windows ログオン ダイアログに表示されます。 このリンクを使用して、パスワードをリセットするか、パスワードを思い出すためのヒントを表示します。

Windows ログイン用パスワードをリセットするには、以下の手順に従います。

1. [Windows Security(Windows セキュリティ)]ダイアログ ボックスから[ログイン]をクリックします。 [Windows ログイン]ダイアログ ボックスが表示されます。
2. 有効なユーザ名を入力します。
3. [忘れたパスワード]をクリックします。

   [Identity Manager パスワードのヒント]ページが表示されます。

   パスワードを思い出した場合、ログイン ダイアログに戻って続行します。 それ以外の場合は、手順 4 を実行して Identity Manager セルフ サービスへの認証を行います。
4. 認証の質問への回答を入力します。

   注: すべての質問への回答がわからない場合は、[リクエスト]をクリックして、管理者によるパスワードのリセットをリクエストしてください。
5. 質問への回答を行った場合は、[ログイン]をクリックします。

   システムによりログインが許可され、セルフ サービスが開きます。
6. ユーザ パスワードの変更
7. ログイン ダイアログに戻り、新しいパスワードでログインします。

パスワードの同期

CA Identity Manager は、ネイティブな Windows アカウントのパスワード変更をインターセプトし、新しいパスワードをユーザ、およびそのユーザに属しているすべてのアカウントに継承します。

この場合には、すべてのシステムで、あるユーザのパスワードを同じにできる、ということが基準である、と仮定しています。 ただし、アカウントで、一部のエンドポイントは、パスワード継承の対象外にするよう指定することもできます。 また、プロビジョニング ドメイン設定パラメータ(Password Synchronization/Update Only Global User)を使用して、パスワード同期エージェントからのリクエストにより、ユーザのみを更新し、そのユーザの他のアカウントは更新しないよう指定することも可能です。

ユーザがパスワードを変更しようとしていることをパスワード同期エージェントが検出すると、エージェントはそのリクエストをインターセプトし、プロビジョニング サーバへ送信します。プロビジョニング サーバは、新しいパスワードをユーザ、およびそのユーザに関連付けられている他のアカウントに継承します。

Identity Manager のパスワード同期の要件には以下が含まれます。

- パスワード変更をインターセプトするシステムには、Identity Manager パスワード同期エージェントがインストールされている必要があります。
- システムを取得されたエンドポイントとして管理する必要があります。
- 取得されたエンドポイントのプロパティにある[パスワード同期エージェントがインストールされています]チェック ボックスをオンにする必要があります。
- 管理対象システムのアカウントを検索し、CA Identity Manager グローバル ユーザに関連付けする必要があります。
- パスワードの同期を要求している各ユーザのグローバル ユーザプロパティ シートで、[Enable Password Synchronization Agent]フラグが選択されている必要があります。

重要: パスワード作成ルールを作成する際には、すべてのシステムで 1 つのパスワードが使用できるようにしてください。 たとえば、Windows のパスワードを 12 文字で指定する必要がある場合、10 文字のパスワードまでしか承認しないシステムは同期中に拒否されます。

Identity Manager サーバはエンドポイントでのパスワード制限を認識しません。 エンドポイント アカウントを操作する場合、Identity Manager のパスワード ポリシーは、エンドポイントのパスワード ポリシーよりも厳密にする必要があります。

パスワード同期エージェントのインストール

パスワード同期エージェントは、グローバル ユーザがログオンする管理対象の Windows コンピュータにインストールできます。 エージェントはこれらのマシンのバックグラウンドで動作します。

インストール プログラムの実行

以下の点に注意してください。

- エージェントをインストールするシステムは、プロビジョニング サーバで管理されている必要があります。
- パスワード変更を行うための管理者としてのユーザを作成する必要があります。このユーザの推奨名は etapwsad です。 このユーザには、PasswordAdministrator プロファイルを割り当てる必要があります。
- インストール メディアで使用できる Windows パスワード同期エージェントには、32 ビット Windows と 64 ビットの 2 つがあります。 32 ビット パスワード同期エージェントは、64 ビット Windows ではサポートされていません。 32 ビット パスワード同期エージェントでは、FIPS のみサポートされています。
- パスワード同期エージェントのインストールを始める前に、インストールを行うマシンがすべての前提条件を満たしていることを確認してください。 ハードウェアおよびソフトウェアの前提条件は、README ファイルで確認できます。
- パスワード同期エージェントのインストールでは、完了時に再起動する必要があります。

パスワード同期エージェントをインストールする方法

1. CA Identity Manager プロビジョニング コンポーネント インストール メディアを検索します。
2. ¥Agent¥PasswordSync または ¥Agent¥PasswordSync-x64 を参照します。
3. setup.exe を実行します。
4. インストール プロセスの途中で、設定ウィザードに次のように指示されます。
   a. [ホスト名]フィールドに、プロビジョニング サーバ システムの名前を入力します。
   b. プロビジョニング サーバへ接続するために、推奨される LDAP ポートは 20390 です。 プロビジョニング サーバのインストレーションでデフォルト以外のポートを使用する場合は、必要に応じてこのポートを変更してください。
   c. [Find domain]ボタンをクリックして、プロビジョニング サーバ ドメインを取得します。
   d. フェイルオーバに対してプロビジョニング サーバのインストールを設定する場合は、画面上の指示に従って、カンマで区切ったサーバのリストを追加します。
   e. [次へ]をクリックします。
   f. [管理者]フィールドに、パスワード同期エージェントのデフォルト グローバル ユーザ名として「etapwsad」と入力します。 このユーザは、PasswordAdministrator プロファイルで作成されている必要があります。 これはデフォルトでは存在しません。

g. [パスワード管理]フィールドで、管理者のパスワードを入力します。

h. [次へ]をクリックします。

i. [エンドポイント タイプ]ドロップダウン リストから、エージェントをインストールするホストのエンドポイントタイプを選択します。

j. [エンドポイント名]ドロップダウン リストから、エージェントをインストールするホストの名前を選択します。

k. [設定] をクリックします。

5. インストールを完了し、再起動するようプロンプトが表示されたら、[完了]をクリックします。

代替サーバに対するエージェントの設定

パスワード同期エージェントを設定して代替サーバを使用するには、Password Synchronization Agent Configuration ウィザードを使用します。

エージェントに対して代替サーバを設定する方法

1. password_sync_folder¥bin にある PwdSyncConfig.exe を実行します。
2. 以下の設定情報を入力します。

   ホスト

   プロビジョニング サーバ システムの名前を指定します。

   [Server URL]フィールドには、ここで指定するホスト名が表示されます。

   LDAP ポート

   プロビジョニング サーバへの接続で使用する LDAP ポートを「20390」と指定します。 プロビジョニング サーバのインストレーションでデフォルト以外のポートを使用する場合は、必要に応じてこのポートを変更してください。

3. [Find domain]ボタンをクリックして、プロビジョニング サーバ ドメインを取得します。
4. 次の形式で、[サーバ URL]フィールドに代替サーバのホスト名とポートを追加します。

   ldaps://primaryhost:20390,ldaps://alternatehost1:20390

5. [次へ]をクリックします。
6. 設定ウィザードの残りのフィールドを入力します。

パスワード同期エージェントが機能するしくみ

何らかの方法を使用して、Windows システム上でユーザのパスワードが変更されると、継承プロセスが開始されます。 パスワードを入力すると、以下の動作が行われます。

1. Windows オペレーティング システムによって、パスワードがパスワード ポリシーに一致するかどうかが確認されます。 Windows がパスワードを受け入れない場合、変更リクエストは拒否され、エラー メッセージが表示されます。同期化を含めて、これ以降の動作は行われません。
2. Windows システムがパスワード変更リクエストを Identity Manager のパスワードの同期エージェントに渡します。パスワード品質チェックが設定されている場合には、パスワードの同期エージェントがパスワードをプロビジョニング サーバにサブミットし、パスワード品質チェックが行われます。 パスワードが Identity Manager の品質ルールに一致しない場合、変更リクエストは拒否され、エラー メッセージが表示されます。 Windows パスワードは変更されず、同期も行われません。
3. Windows と CA Identity Manager の両方の品質ルールに一致するパスワードは、パスワードの同期エージェントによって継承のためにプロビジョニング サーバへサブミットされます。
4. CA Identity Manager はグローバル ユーザ パスワードを更新し、グローバル ユーザに関連する一部またはすべてのアカウントに新しいパスワードを継承します。

注: CA Identity Manager がリクエストを拒否した場合でも、表示されるエラー メッセージは Windows のパスワード ポリシーに基づくため、Windows と CA Identity Manager のパスワード ポリシーは同一であるか、一貫性を持たせる必要があります。

password_update_timeout 設定パラメータ(eta_pwdsync.conf)は、PSA が Identity Manager サーバからのパスワード変更継承の確認を待機する時間を秒単位で指定します。 その間に PSA が確認を受信しない場合は、継承が成功した場合と同じように動作が進行し、パスワード変更継承が確認されなかったという警告がログ(eta_pwdsync.log)に記録されます。 パラメータの最小値はゼロ(0)で、これは PSA が確認を待機しないことを意味します。 詳細については、プロビジョニング マネージャ ヘルプの「eta_pwdsync.conf--パスワードの同期エージェントの設定」を参照してください。

アカウントレベルのパスワード品質チェック

パスワード品質チェックは、管理エンドポイントでアカウントが作成または変更された場合や、Identity Manager ユーザのパスワードが設定された場合に実行されます。 アカウントに対するパスワード品質チェックは、パスワードの文字に基づいたチェックに制限されます。 Identity Manager はアカウント パスワードの変更すべてをインターセプトするわけではないため、最近の変更履歴(パスワード更新回数とパスワードの再使用回数)に基づいたグローバル ユーザのパスワード チェックは、アカウントでは実行されません。したがって、これらのチェックの実行対象となる正確なパスワード変更履歴はありません。

アカウント パスワードのチェックは、以下のドメイン設定パラメータで制御します。

- Endpoint/Check Account Passwords
- Endpoint/Check Empty Account Passwords

各パラメータの値は、各管理エンドポイントに対して実行すべきチェックのレベルを指定します。 エンドポイントは、以下のように指定できます。

ALL
-ALL
<NamespaceName>
-<NamespaceName>
<NamespaceName>:<DirectoryName>
-<NamespaceName>:<DirectoryName>

マイナス記号(-)を含む形式は、パラメータを無効にします。 この記号がない形式は、パラメータを有効にします。 [-]<NamespaceName> の形式の場合、指定されたエンドポイント タイプのすべてのエンドポイントが制御され、[-]<NamespaceName>:<DirectoryName> の形式の場合は各エンドポイントが制御されます。 [-]ALL の形式では、すべてのエンドポイント タイプのすべてのエンドポイントが制御されます。 両パラメータのデフォルト値は -ALL です。

各パラメータは何度でも指定できます。 同じエンドポイントに複数の値が指定された場合、最後の値が使用されます。 最初に全般的なルールを指定し、次に固有のルールを指定して全般的なルールを上書きすることができます。

Check Account Passwords パラメータによって、グローバル ユーザ パスワード品質チェックに相当するチェックを実行できます。 あるエンドポイントに対してこのパラメータを有効にすると、CA Identity Manager は、既存のアカウントに対して要求された変更におけるすべてのパスワードをチェックします。これは、空のパスワードを設定しようとした場合も含まれます。 アカウント作成時にパスワードを設定しないと、パスワード品質チェックは実行されません。

Check Empty Account Passwords により、アカウントの作成時に空のパスワードをチェックする機能も追加されます。 パスワード プロファイルが有効になっており、1 文字以上のパスワードが必要な場合に空のパスワードを設定すると、アカウントの作成が失敗します。 一部のエンドポイント タイプではパスワードなしでアカウントを作成することが可能なため、Check Account Passwords とは別にこのパラメータが設定されています。

注: 指定されたパスワードが現在のグローバル ユーザのパスワードと一致する場合、同期されたアカウント パスワードについては、アカウント パスワード品質チェックがスキップされます。

パスワード品質の実施

パスワード同期オプションはネイティブ システム(Windows NT/ADS など)のパスワード変更リクエストをインターセプトし、それらを Identity Manager サーバにサブミットします。サーバはグローバル ユーザ パスワードと、グローバル ユーザに関連するアカウント パスワードを同期させます。 パスワード品質制御を実施するには、Identity Manager のパスワード プロファイル用パスワード品質ルールと、ネイティブ システムのパスワード品質ルール(Windows NT/ADS)の両方を使用できます。

パスワード同期の設定

インストールのとき、パスワード同期エージェントが最初に設定されます。これは、パスワード同期設定ウィザードを使用して随時に再設定できます。 Identity Manager サーバでパスワード品質チェックを行う、タイムアウトを変更する、eta_pwdsync.conf ファイルを使用するなど、さらに設定を行うこともできます。 このファイルは、password_sync_folder¥data¥ フォルダ にあります。詳細については、プロビジョニング マネージャのヘルプの「eta_pwdsync.conf ファイル」のトピックを参照してください。

フェイルオーバ

プロビジョニング サーバが停止した、または高い負荷がかかった場合、パスワード同期エージェントは、元のサーバから別のサーバへフェイルオーバします。 このような場合のために、複数のプロビジョニング サーバが同じドメインを使用するように設定し、エージェントがこれらのサーバを使用するよう設定する必要があります。 フェイルオーバの詳細については、「Installation Guide」および「configuring the agent to use alternate servers (119 ページ)」を参照してください。

ログ メッセージの有効化

パスワードの変更が拒否された理由を知るには、パスワード同期エージェントのログを表示します。 記録されたすべてのメッセージは、eta_pwdsync.log ファイルに保存されています。 デフォルトでは、このファイルは password_sync_folder¥Logs フォルダにあります。

パスワード同期エージェントのロギングには、次の内容を含めることができます。

- エラー メッセージ。必ず記録されます。
- 診断(プロセス フロー、トレース)メッセージ。eta_pwdsync.conf ファイルの logging_enabled=yes|no パラメータの値によって、有効または無効に設定できます。

詳細は、同じ期間の eta_pwdsync.log およびプロビジョニング サーバのログを参照してください。

以前の log_level 設定パラメータは廃止になりましたが、下位互換のために残されています。「log_level=0」は logging_enabled=no に、「log_level=0 以外」は logging_enabled=yes に変換されます。 以前のパラメータと新しいパラメータの両方が設定ファイルに存在する場合、logging_enabled=yes|no パラメータの明示的な設定は、以前の「log_level=数値」によって実行される間接的な設定よりも優先されます。

インストールの確認

パスワード同期エージェントをインストールしたら、Windows システムのパスワードを変更して、アカウントに関連付けられているグローバル ユーザ パスワードも変更されていることを確認します。

第 7 章: グループ

複数のタイプのグループを作成することも、これらのタイプを組み合わせて作成することもできます。

- 静的グループ -- 対話式で追加されるユーザのリスト
- 動的グループ -- ユーザが LDAP クエリと一致する場合に、グループに属するユーザ(ユーザ ストアとして LDAP ディレクトリが必要)

  注: [動的グループ クエリ]フィールドは、グループの directory.xml に存在する場合でも、[グループの作成]タスクやその他のグループ タスクには含まれません。[動的グループ クエリ]フィールドをタスクに含めるには、関連付けられたプロファイル画面を編集します。
- ネスト グループ -- 他のグループを含むグループ(ユーザ ストアとして LDAP ディレクトリが必要)

注: ユーザが属する静的グループ、動的グループ、ネスト グループを表示するには、ユーザ オブジェクトの[グループ]タブを使用します。 デフォルトにより、このタブは[ユーザの表示]タスクと[ユーザの変更]タスクに表示されます。

このセクションには、以下のトピックが含まれています。

静的グループの作成(125 ページ)
動的グループの作成(126 ページ)
動的グループ クエリのパラメータ(127 ページ)
ネスト グループの作成(129 ページ)
静的グループ、動的グループ、ネスト グループの例(131 ページ)
グループ管理者(132 ページ)

静的グループの作成

複数のユーザを 1 つの静的グループに関連付けることができます。 静的グループのメンバシップ リストに各ユーザを追加したり、リストから各ユーザを削除することで、静的グループを管理できます。 グループのメンバ リストを表示するには、[メンバシップ]タブを使用します。デフォルトにより、このタブは[グループの表示]タスクと[グループの変更]タスクに組み込まれています。

注: [メンバシップ]タブは、グループに明示的に追加されたメンバしか表示されません。動的に追加されたメンバは表示されません。

静的グループを作成する方法

1. ユーザ コンソールで、[グループ]-[グループの作成]を選択します。
2. 新規グループの作成またはグループのコピーの作成を選択し、[OK]をクリックします。
3. [プロファイル]タブで、グループ名、グループの組織、説明、グループの管理者名を入力します。
4. [メンバシップ]タブをクリックします。
5. [ユーザの追加]をクリックします。
6. グループに含めるユーザを検索します。
7. 対象となるユーザの横にチェック マークを付け、[選択]をクリックします。
8. [送信]をクリックします。

動的グループの作成

動的グループを作成するには、ユーザ コンソールを使用して、ランタイムでグループ メンバを動的に決定する LDAP フィルタ クエリを定義します。こうすると、ユーザを個別に検索して追加する必要がなくなります。

たとえば、NeteAuto の米国の従業員全員をリストするグループを生成する場合は、ユーザ コンソールの[動的グループ クエリ]フィールドで、以下のような LDAP 検索フィルタを定義します。

ldap:///cn=Employees,o=NeteAuto,c=US??sub

また、このクエリを変更して、米国以外の従業員を検出することもできます。

静的グループ、動的グループ、ネスト グループの例(131 ページ)に、静的グループ、動的グループ、およびネスト グループによって作成されたグループの例を示します。

注: [動的グループ クエリ]フィールドをタスクに含めるには、関連付けられたプロファイル画面を編集します。 デフォルトにより、このフィールドは[グループの作成]タスクには組み込まれていません。

動的グループを作成する方法

1. ユーザ コンソールで、[グループ]-[グループの作成]を選択します。
2. 新規グループの作成またはグループのコピーの作成を選択し、[OK]をクリックします。
3. [プロファイル]タブで、グループ名、グループの組織、説明、グループの管理者名を入力します。

4. [動的グループ クエリ]フィールドに、以下の例のような LDAP 検索フィルタを入力します。

   ldap:///cn=Employees,o=NeteAuto,c=US??sub?

5. [送信]をクリックします。

注: グループの動的メンバシップを変更できるのは、[グループの変更]タスクを持つ管理者のみです。

動的グループ クエリのパラメータ

検索時には、以下の動的なクエリ パラメータを使用できます。

ldap:///<検索ベース DN>??<検索範囲>?<検索フィルタ>

- <検索ベース DN> には、LDAP ディレクトリ内の検索開始ポイントを指定します。クエリにベース DN を指定しない場合は、グループの組織がデフォルトのベース DN となります。
- <検索範囲> には、検索範囲を指定します。以下の値を使用できます。
  - sub -- ベース DN レベルとそれより下位にあるエントリを返します。
  - one -- URL で指定したベース DN よりも 1 レベル下にあるエントリを返します。 デフォルト値です。
  - base -- 検索オプションとして指定したベースを無視して、代わりに one を使用します。

  one または base を使用すると、ベース DN 組織内のユーザのみが取得されます。

  sub を使用すると、ベース DN 組織と、ツリー内のすべての下位組織にいるユーザ全員が取得されます。

- <検索フィルタ> には、検索範囲内のエントリに適用するフィルタを指定します。 検索フィルタの入力時には、以下のような標準の LDAP クエリ構文を使用します。

  (<論理演算子><比較><比較...>)

  - <論理演算子> には、以下のいずれかを使用します。

    論理 OR: |

    論理 AND: &

    論理 NOT: !

  - <比較> には、<属性><演算子><値> を指定します。

  以下に例を示します。

  (&(city=boston)(state=Massachusetts))

  デフォルトの検索フィルタは (objectclass=*) です。

動的クエリを作成する場合、以下の点に注意が必要です。

- 「LDAP」プレフィックスは小文字である必要があります。以下に例を示します。

  ldap:///o=MyCorporation??sub?(title=Manger)

- LDAP サーバ ホスト名またはポート番号は指定できません。 検索はすべて、Identity Manager 環境で設定した Identity Manager LDAP ディレクトリ内で行われます。

以下に、LDAP クエリの例を示します。

[説明]	クエリ
マネージャになっているユーザ全員	ldap:///o=MyCorporation??sub?(title=Manger)
ニューヨーク西支店のマネージャ全員	ldap:///o=MyCorporation??one?(&(title=Manager) (roomNumber=NYWest))
携帯電話を持っている技術者全員	ldap:///o=MyCorporation??one? (&(employeetype=technician) (mobile=*))
従業員番号が 1000 ～ 2000 の従業員全員	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
雇用期間が 6 か月を超えるヘルプデスク管理者全員	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **注**: このクエリの場合、ユーザの雇用日を示す DOH 属性を作成する必要があります。

注: 「> 」(より大きい)と「<」(より小さい)による比較は、算術式ではなく辞書式です。これらの使用法の詳細については、LDAP ディレクトリ サーバのマニュアルを参照してください。

ネスト グループの作成

ユーザ ストアが LDAP ディレクトリの場合は、あるグループを別のグループのメンバとして追加することができます。 このグループをネスト グループと呼びます。

ネスト グループが含まれるグループを親グループと呼びます。 ネスト グループのメンバは、親グループのメンバとなります。 ただし、親グループのメンバはネスト グループのメンバにはなりません。

電子メールの配信リストでは、あるリストを別のリストのメンバにすることができますが、ネスト グループもこれと似ています。 ネスト グループでは、グループ メンバとしてグループとユーザを追加できます。 あるグループを別のグループのメンバシップ リストにネストすると、ネスト グループのメンバがすべて組み込まれます。

たとえば、会社の製造部門、設計部門、配送部門、会計部門ごとに別個のグループを作成した場合、これらの各部門グループを会社の親グループのメンバとしてネストすると、会社全体を表す親グループを構成することができます。 こうすると、製造、設計、配送、会計の各ネスト グループに加えた変更内容が、会社全体のネスト グループに自動的に反映されるようになります。 別のグループ内にネストされたグループは、動的グループにすることができ、他のネスト グループを組み込むことができます。

静的グループ、動的グループ、ネスト グループの例 (131 ページ)の図に、静的グループ、動的グループ、およびネスト グループによって作成された親グループを示します。

ネスト グループを作成する前に、以下の点に注意してください。

- ユーザ コンソールで、グループの静的メンバ リストからネスト グループを追加または変更できるのは、[グループ メンバの変更]タスクを持つ管理者のみです。
- グループからメンバの変更、追加、削除を実行できるのは、適切な管理権限を持つユーザのみです。

  たとえば、親グループ A がネスト グループ B と C によって作成された場合、グループ A の管理者はグループ A のメンバのみ変更でき、B と C のメンバは変更できません。 グループ B と C は、適切な権限を持つ管理者のみ変更することができます。

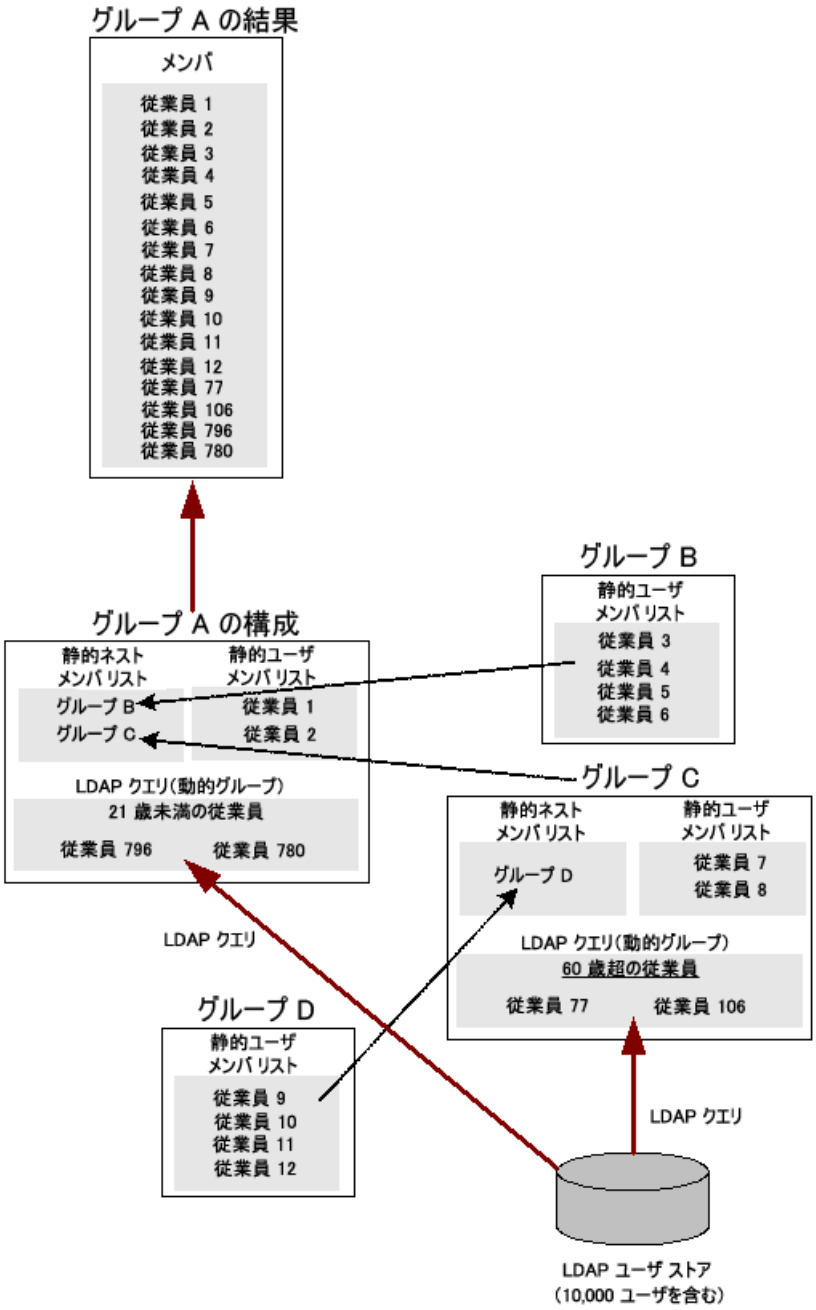
ネスト グループを作成する方法

1. ユーザ コンソールで、[グループ]-[グループの作成]を選択します。
2. 新規グループの作成またはグループのコピーの作成を選択し、[OK]をクリックします。

3. [プロファイル]タブで、グループ名、グループの組織、説明、グループの管理者名を入力します。
4. [メンバシップ]タブで、以下の手順に従います。
   a. [グループの追加]をクリックし、このグループにネスト グループを追加します。
   b. 既存のグループを検索します。
   c. 対象となるグループの横にチェック マークを付け、[選択]をクリックします。
   d. [送信]をクリックします。

静的グループ、動的グループ、ネスト グループの例

静的グループ、動的グループ、ネスト グループの組み合わせから成る複雑なグループを作成できます。 以下の図に、静的グループ、動的グループ、およびネスト グループによって作成された親グループを示します。



以下に、上記の例について説明します。

- 親グループ A には、ネスト グループ B と C、2 人の静的ユーザ、および 21 才未満の従業員をすべてリストする動的 LDAP クエリが含まれています。
- グループ B は 4 人の静的ユーザで構成されています。
- 親グループ C には、ネスト グループ D、2 人の静的ユーザ、および 60 才を超える従業員をすべてリストする動的 LDAP クエリが含まれています。
- グループ D には 4 人の静的ユーザが含まれています。
- 図の最上部には、グループ A のメンバがリストされています。これらのメンバは、ネスト グループ、動的クエリ、グループ B、C、D の静的ユーザ メンバ リストから取得されたものです。

グループ管理者

[グループの作成]または[グループの変更]タスクの[管理者]タブでは、グループの管理者としてユーザやグループを指定することができます。 ユーザをグループ管理者として割り当てる場合は、その管理者がグループを管理できるだけの適切なスコープを持つロールが割り当てられていることを確認してください。 以下に例を示します。

1. [グループの変更]を使用して、ユーザをグループの管理者として割り当てます。
2. このユーザに、[グループ メンバの変更]などのグループ管理タスクか、[グループ]タブでのユーザ管理タスクを持つ管理ロールを割り当てます。
3. このロールに、グループに対する適切なスコープがあることを確認します。
   a. グループ管理タスクと共に割り当てたロール上で、[管理ロールの表示]を使用します。
   b. [メンバ]タブで、以下のルールを使用したポリシーが存在することを確認します。

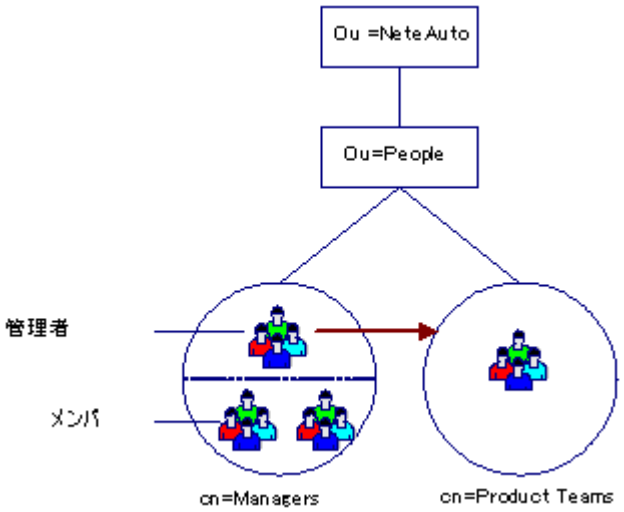
      グループ管理者が満たすメンバ ルール

      このグループを含むスコープ ルール

      このグループに追加されるユーザを含むスコープ ルール

注: IdentityMinder 環境で、グループを他のグループの管理者にするには、ディレクトリ設定ファイルでグループ管理者サポートを設定します。 詳細については、「Configuration Guide」を参照してください。

グループを管理者として割り当てる場合は、そのグループの管理者のみが、作成または変更するグループの管理者となります。 指定した管理者グループのメンバは、そのグループの管理権限を持ちません。 以下の図に、あるグループが別のグループの管理者になる場合の例を示します。



この例の内容

- Managers グループは、Product Teams グループの管理者です。
- Managers グループの管理者は、Product Teams グループを管理できます。
  Managers グループのメンバは、Product Teams グループを管理できません。

第 8 章: 管理対象のエンドポイント アカウント

CA Identity Manager では、CA Identity Manager のインストールにプロビジョニング サーバが含まれている場合、エンドポイント システムのアカウントを管理できます。 管理できるアカウントには、Exchange、Windows NT、または Oracle のアカウントに加え、現時点では CA Identity Manager に関連付けられていない孤立アカウントやシステム アカウントなどがあります。

このセクションには、以下のトピックが含まれています。

ユーザの複数アカウント (135 ページ)
ユーザへのエンドポイント アカウント付与 (137 ページ)
CA Identity Manager でエンドポイントを設定する方法 (137 ページ)
エンドポイントのカスタム属性の拡張 (142 ページ)
アカウント タスク (143 ページ)
詳細なアカウント操作 (148 ページ)

ユーザの複数アカウント

他のシステムに存在するアカウントを Identity Manager のユーザに割り当てることができます。 たとえば、電子メールの Exchange アカウント、データベース アクセスの Ingres アカウント、および Windows システムを使用する Active Directory アカウントが必要となる場合があります。 プロビジョニング ロールをユーザに割り当てると、このユーザは、プロビジョニング ロールのアカウント テンプレートによって定義されたアカウントを受信します。

アカウントテンプレートは、アカウントの固有の特性を定義します。 たとえば、Exchange アカウントのテンプレートでは、メールボックスのサイズを定義できます。

注: プロビジョニング サーバをインストールするには、「Installation Guide」を参照してください。

Identity Manager ユーザ

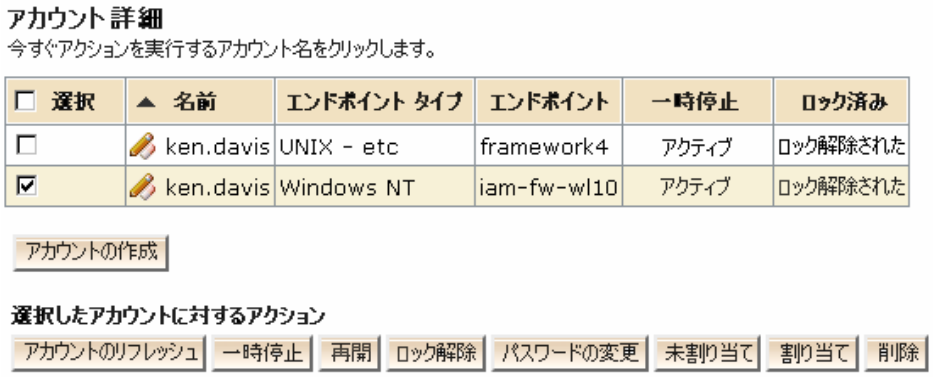
CA Identity Manager ユーザは、[ユーザの表示]または[ユーザの変更]などの管理タスクを通じて表示されるユーザです。 一部のユーザには関連するグローバル ユーザがある場合があります。これは、プロビジョニング サーバに存在する対応するアカウントです。

グローバル ユーザ

グローバル ユーザは、プロビジョニング サーバで保持されるオブジェクトです。 これは、プロビジョニング サーバまたはこのサーバを管理するエンドポイントにアクセスする必要がある個人または他のアイデンティティに対応します。 グローバル ユーザ オブジェクトには、個人の名前、パスワード設定、役職、電話番号、および住所などの情報が含まれます。 グローバル ユーザの主な目的は、エンドポイント システムの個人アカウントを結びつけることです。

エンドポイント システムのアカウント

ユーザのエンドポイント アカウントを表示または変更すると、そのユーザに対してエンドポイントのアカウント(UNIX、Microsoft Exchange、Active Directory など) が表示されます。 そこには、アカウント名、エンドポイント タイプ、エンドポイント、およびアカウントのステータスが表示されます。 変更タスクでは、ユーザ パスワードの変更、アカウントのロックまたは一時停止などのアクションを実行できる追加オプションがあります。



タスクにこれらのオプションを含めるには、[アカウントの設定]タブのユーザ コンソール ヘルプを参照してください。

以下のアカウント タイプがエンド ポイントにある場合がありますが、ユーザ コンソールには表示されません。

- 孤立アカウント — グローバル ユーザに関連付けられていないアカウント
- システム アカウント — グローバル ユーザに関連付けられておらず、エンドポイント システムの管理に使用されるアカウント

これらのアカウントをユーザに割り当てると、ユーザ コンソールで管理できるようになります。 [孤立アカウントの管理]と[システム アカウントの管理]タスクを使用します。

ユーザへのエンドポイント アカウント付与

CA Identity Manager で Identity Manager ユーザにエンドポイント アカウントを付与するには、以下の 3 つの手順を含む方法をお勧めします。

1. CA Identity Manager でエンドポイントを設定します(137 ページ)。
2. 上記のエンドポイントのアカウント テンプレートを使用して プロビジョニング ロールを作成します(154 ページ)。
3. 上記のエンドポイントにアカウントが必要なユーザに ロールを割り当てます(88 ページ)。

これらの手順が完了したら、ユーザにロールを割り当てることによって、アカウントをより多くのユーザに簡単に割り当てることができます。

CA Identity Manager でエンドポイントを設定する方法

ユーザ コンソールでエンドポイントを設定すると、エンドポイントで見つかったアカウントとオブジェクトがプロビジョニング ディレクトリに配置されます。 エンドポイントは、CA Identity Manager で管理されるアプリケーションまたはコンピュータであり、Microsoft Exchange Server や Oracle データベースなどです。

エンドポイントの設定の手順を次に示します。

1. ロール定義ファイルをインポートすることにより、エンドポイント タイプを定義します(138 ページ)。

   この操作により、エンドポイントが CA Identity Manager で管理できるようになります。
2. ユーザ コンソールでエンドポイントを作成します(139 ページ)。
3. エンドポイントの内容を参照し、アカウントどうしを関係付けます(139 ページ)。

エンドポイント タイプの定義

エンドポイント タイプの定義は、そのエンドポイント タイプ用の画面、タスク、ロールを含むロール定義ファイルをインポートすることで行います。

エンドポイント タイプを定義する方法

1. 管理コンソールで、[環境]をクリックします。
2. エンドポイント タイプを必要とする環境を選択します。
3. ロールおよびタスクの設定を選択します。
4. [インポート]をクリックします。
5. ProvisioningEndpointSupport フォルダからエンドポイント タイプ用のロール定義ファイルを選択します。

   このフォルダは管理ツール フォルダ内にあります。以下はデフォルトの場所です。

   - Windows: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools
6. [完了]をクリックします。
7. Identity Manager 環境を再起動します。

注: Connector Xpress におけるエンドポイントの定義については、「Connector Xpress ガイド」を参照してください。 次に、この手順を使用して、ロール定義ファイルをインポートします。

ユーザ コンソールでエンドポイントを作成します。

エンドポイント タイプを定義したら、管理する必要のある環境でエンドポイントを作成できます。

ユーザ コンソールでエンドポイントを作成する方法

1. [エンドポイント]-[エンドポイントの管理]-[エンドポイントの作成]を選択します。
2. エンドポイント タイプを選択します。
3. フィールドに入力してタブを完了します。

   必須フィールドは、赤丸で始まっています。 現在のタブにあるフィールドの定義の詳細については、[ヘルプ]をクリックしてください。

   注:エンドポイントの名前に、# 記号を使用しないようにしてください。この文字は検索できません。
4. [サブミット]をクリックします。

これで、エンドポイントを検索、関連付け(139 ページ)して、エンドポイントのアカウントを管理する準備ができました。

エンドポイントの検索および関連付け

ユーザ コンソールでは[検索および関連付けの定義]を決定できます。 そして、この定義を[検索および関連付けを実行]タスクで使用します。

この操作による結果は 3 種類あります。

- エンドポイントを検索すると、CA Identity Manager がエンドポイントのオブジェクトを検出し、そのインスタンスをプロビジョニング ディレクトリに保存します。
- エンドポイントのアカウントの関連付けを行うと、CA Identity Manager により各アカウントがプロビジョニング ディレクトリ内のユーザに関連付けされます。 関連付けの機能では、アカウントがデフォルトのユーザに関連付けされるのか、または新しいユーザが作成されるのかを決定することができます。
- また、選択したアカウントの属性値を使用して選択したユーザの属性を設定することもできます。

[検索および関連付けの定義]を作成する方法

1. Identity Manager 環境で、[エンドポイント]-[検索および関連付けの定義]-[検索および関連付けの定義の作成]をクリックします。
2. 新しい定義を開始するには[OK]をクリックします。

3. ［検索および関連付け］タブの入力を完了するには以下の手順に従います。

   a. ［検索および関連付けの名前］にわかりやすい名前を入力します。

      ［コンテナ/エンドポイント/検索メソッドの選択］をクリックして、検索するエンドポイントをクリックし、コンテナがある場合はコンテナを 1 つ以上クリックします。大きいエンドポイントのコンテナ検索には少々時間がかかります。 検索フィルタを使用して検索対象を絞り込みます。コンテナの検索メソッドをクリックします。［検索および関連付け］のプロセスには、選択したコンテナと、そのサブコンテナも含まれます。 ディレクトリ コンテナについては、そのサブツリーにあるコンテナもすべて含まれます。

   b. ［検索/関連付けアクション］をクリックして、以下を実行します。

      - ［管理オブジェクトをディレクトリで検索］ ーエンドポイントに保存されていて、プロビジョニング ディレクトリには保存されていないオブジェクトを検索します。
      - ［アカウントをユーザに関連付け］ - 検索機能で検出されたオブジェクトをプロビジョニング ディレクトリのユーザに関連付けます。 ユーザが検出されると、オブジェクトがそのユーザに関連付けられます。 代わりに、既存のユーザ（デフォルトのユーザ）にアカウントを割り当てるか、ユーザを作成してアカウントを割り当てるように選択することもできます。
      - ［ユーザ フィールドの更新］ - オブジェクト フィールドとユーザ フィールドの間にマッピングが存在する場合、ユーザ フィールドはオブジェクト フィールドからのデータを使用して更新されます。

4. タスクの実行をスケジュールしたい場合は、［反復］タブに必要な項目を入力します。

   a. ［スケジュール］をクリックします。

   b. 必要なフィールドに入力し、このタスクがいつ実行されるかを決定します。

      システムのルーチン アクセスをできるだけ妨げないよう、夜間にタスクを実行するようにスケジュールする場合があります。

注: この操作ではクライアント ブラウザがサーバと同じタイムゾーンにあることが必要です。 たとえば、サーバ時間が火曜日の 7:00 AM のときにクライアント時間が 10:00 PM であれば、[検索および関連付けの定義]は機能しません。

5. [送信]をクリックします。

[検索および関連付けの定義]を使用する方法

1. Identity Manager 環境で、[エンドポイント]-[検索および関連付けを実行]をクリックします。
2. [検索および関連付けの定義]をクリックして実行します。
3. [送信]をクリックします。

エンドポイントに存在するユーザ アカウントは、作成した[検索および関連付けの定義]に基づいて Identity Manager により作成または更新されます。

[検索および関連付け]が成功したかどうかを確認する方法

1. [システム]-[サブミット済みタスクの表示]を選択します。
2. [タスク名]フィールドに、「検索および関連付けを実行」と入力します。
3. [検索]をクリックします。

タスクが正常に完了したかどうかが結果に表示されます。

エンドポイントのカスタム属性の拡張

プロビジョニング サーバでは、カスタム エンドポイント属性を管理できます。 プロビジョニング ロールに関連付けられたカスタム エンドポイント属性を CA Identity Manager で読み取り可能にするには、追加の手順が必要です。

エンドポイントのカスタム属性を拡張する方法

1. CA Identity Manager r12.5 以前にこのコネクタを作成した場合は、パーサ テーブルからメタデータを生成します。

   「Programming Guide for Java Connector Server」を参照してください。

2. 以下の手順で、Connector Xpress を使用します。

   a. 名前空間ノードで、メタデータをインストールします。

   b. ロール定義ジェネレータを使用して、JAR ファイル、プロパティ ファイル、およびロール定義ファイルを生成します。

      詳細については、「Connector Xpress Guide」を参照してください。

3. JAR ファイルを次の場所にコピーします。

   - （Windows）app server home/IdentityMinder.ear/user_console.war/WEB-INF/lib
   - （UNIX）app server home¥IdentityMinder.ear¥user_console.war¥WEB-INF¥lib

     注： WebSphere の場合、JAR ファイルを次の場所にコピーします。
     WebSphere_home/AppServer/profiles/Profile_Name/config/cells/Cell_name/applications/IdentityMinder.ear/deployments/IdentityMinder/user_console.war/WEB-INF

4. プロパティ ファイルを次の場所にコピーします。

   - （Windows）app server
     home/IdentityMinder.ear/custom/provisioning/resourceBundles
   - （UNIX）app server
     home¥IdentityMinder.ear¥custom¥provisioning¥resourceBundles

     注： WebSphere の場合、プロパティ ファイルを次の場所にコピーします。
     WebSphere_home/AppServer/profiles/Profile_Name/config/cells/Cell_name/applications/IdentityMinder.ear/deployments/IdentityMinder/IdentityMinder.ear¥custom¥provisioning¥resourceBundles

5. クラスタがある場合は、ノードごとに上記 2 つの手順を繰り返します。

6. アプリケーション サーバを再起動します。

7. 以下の手順で、ロール定義ファイルをインポートします。

   a. 管理コンソールで、[環境]を選択します。

   b. ロールおよびタスク設定を選択します。

   c. [インポート]をクリックします。

d. エンドポイント タイプを選択し、[完了]をクリックします。

アカウント タスク

ユーザ コンソールでは、Identity Manager ユーザに関連付けられるエンドポイント アカウントを作成、変更、表示、および削除できます。 また、CA Identity Manager に関連付けられていない別のエンドポイント アカウントをユーザに割り当てることもできます。

エンドポイント アカウントには、以下の 4 つのタイプがあります。

プロビジョニング済み

ユーザにプロビジョニング ロールが割り当てられたときに作成されるアカウント

例外

ユーザにアカウント テンプレートが割り当てられたときに作成されるアカウント

孤立

エンドポイント システムに作成され、Identity Manager ユーザに関連付けられていないアカウント

システム

エンドポイント システムに作成され、Identity Manager ユーザに関連付けられておらず、エンドポイント システムの管理に使用されるアカウント

プロビジョニング済みアカウントの作成

Identity Manager ユーザのエンドポイント アカウントを作成するには、プロビジョニング ロールをユーザに割り当てる方法をお勧めします。 ユーザには、そのロールのアカウント テンプレートで定義された属性を持つアカウントが割り当てられます。 Exchange アカウントのメールボックスのサイズなど、必要に応じてそのアカウント テンプレートに変更を加えると、エンドポイント アカウントが更新されます。

プロビジョニング済みアカウントを作成する方法

1. ユーザ コンソールで、[ユーザの管理]-[ユーザの変更]を選択します。
2. 変更するユーザを選択します。
3. [プロビジョニング ロール]タブをクリックします。
4. [プロビジョニング ロールの追加]をクリックします。
5. ロールを選択します。
6. [送信]をクリックします。

例外アカウントの作成

ユーザに対して[ユーザの変更]を使用すると、[アカウント]タブで直接アカウントを作成できます。 このアカウントは、「例外アカウント」と呼ばれています。 ただし、このアカウントにはプロビジョニング ロールが関連付けられていないので、ロールとユーザの同期を行ってもこのアカウントは更新されません。

アカウント テンプレートを作成する方法

1. ユーザ コンソールで、[ユーザ]-[ユーザのエンドポイント アカウントの変更]を選択します。
2. 変更するユーザを選択します。
3. [作成]をクリックします。
4. エンドポイントを選択します。
5. このエンドポイント タイプにコンテナが必要な場合は、コンテナを選択します。
6. 各タブのフィールドを入力します。
7. [送信]をクリックします。

孤立アカウントの割り当て

ユーザ コンソールでは、孤立アカウントを管理できます。このアカウントは Identity Manager ユーザに関連付けられていないアカウントです。

孤立アカウントのデフォルト ユーザを作成する方法

プロビジョニング ディレクトリが Identity Manager ユーザ ストアとは別になっている場合、Identity Manager ユーザ ストアでプロビジョニング サーバのデフォルト ユーザを作成します。 デフォルト ユーザは、孤立アカウントに使用されます。

1. ユーザ コンソールで、[ユーザ]タブをクリックします。
2. [Manager Users]-[ユーザの作成]をクリックします。
3. 以下のように、かっこで囲んでユーザの名前を付けます。
   [デフォルト ユーザ]

   これで、孤立アカウントをユーザに割り当てることができます。

孤立アカウントを割り当てる方法

1. ユーザ コンソールで、[エンドポイント]をクリックします。
2. [孤立アカウントの管理]をクリックします。
3. ユーザを検索して選択します。
4. 孤立ユーザに割り当てるユーザをクリックします。

システム アカウントの割り当て

ユーザ コンソールでは、システム アカウントを管理できます。このアカウントはエンドポイント アカウントで、エンドポイント システムの管理に使用されます。

システム アカウントをユーザに割り当てるには、[システム アカウントの管理]タスクに基づいて管理タスクを作成します。 新規タスクには、特定のエンドポイントに適用される固有の Identity Manager ユーザが存在します。 エンドポイントのタイプごとにタスクを 1 つ作成することもできます。

タスクを設定して、システム アカウントを割り当てる方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの作成]をクリックします。
2. [システム アカウントの管理]に基づいて新規タスクを作成します。

   たとえば、「Oracle システム アカウントの管理」という名前のタスクを作成して、Oracle エンドポイント タイプのシステム アカウントを割り当てることができます。

3. [検索]タブで[参照]ボタンをクリックして、検索画面を編集します。 その検索画面で、ユーザの検索フィルタを追加して、このシステム アカウントに割り当てます。
4. タスクをサブミットします。
5. このタスクをロールに追加します。
6. ユーザにエンドポイントのシステム アカウントを割り当てる必要があるユーザに対してロールを割り当てます。

   このロールが設定されたユーザは新規タスクを実行して、システム ユーザを Identity Manager ユーザに割り当てることができます。

エンドポイント アカウントの削除

以下の 2 つの方法で、エンドポイント アカウントを削除できます。

1. [ユーザの変更]タスクを使用し、[プロビジョニング ロール]タブで、そのアカウントを作成したロールを削除する。
2. [ユーザのエンドポイント アカウントの変更]タスクを使用して、アカウントを削除する。

[ユーザのエンドポイント アカウントの変更]でアカウントを削除する方法

1. ユーザ コンソールで、[ユーザ]-[ユーザのエンドポイント アカウントの変更]を選択します。
2. 変更するユーザを選択します。
3. エンドポイント タイプに基づいてアカウントを検索します。
4. アカウントを選択します。
5. [削除]ボタンをクリックします。

削除したアカウントは、以下のようにプロビジョニング マネージャを使用すると、再作成されます。

- [Synchronize User with Roles]では、プロビジョニング済みアカウント(ユーザにプロビジョニング ロールが割り当てられたときに作成されたアカウント)が再作成されます。
- [Synchronize Accounts with Account Templates]では、例外(アカウントにアカウントテンプレートがある場合)とプロビジョニング済みアカウントが再作成されます。

エンドポイント アカウントのパスワード変更

現在のパスワードを知らなくてもエンドポイント アカウントのパスワードを変更できます。

エンドポイント アカウントのパスワードを変更する方法

1. ユーザ コンソールで、[ユーザ]-[ユーザのエンドポイント アカウントの変更]を選択します。
2. 変更するユーザを選択します。
3. エンドポイント タイプに基づいてアカウントを検索します。
4. アカウントを 1 つ以上選択します。
5. [パスワードの変更]ボタンをクリックします。
6. 新しいパスワードを入力します。

   CA Identity Manager パスワード ポリシーによって新しいパスワードが検証されます。
7. [送信]をクリックします。

複数のアカウントに対するアクションの実行

1 つまたは複数のアカウントに対してその他のアクションを複数実行できます。 たとえば、ユーザが間違ったパスワードを入力した場合やユーザにアカウントを割り当てたり、割り当て解除したりする場合、一時停止されていたアカウントを再開してアカウントのロックを解除することができます。 これらのアクションは選択されたすべてのアカウントに適用され、手順は同じです。

複数のアカウントに対してタスクを実行する方法

1. ユーザ コンソールで、[ユーザ]-[ユーザのエンドポイント アカウントの変更]を選択します。
2. 変更するユーザを選択します。
3. エンドポイント タイプに基づいてアカウントを検索します。
4. アカウントを 1 つ以上選択します。
5. [選択したアカウントに対するアクション]で、任意のボタンをクリックします。
6. 表示されるダイアログ ボックスに応答して、[送信]を送信します。

詳細なアカウント操作

プロビジョニング マネージャで、アカウントについて、次のような詳細な操作を実行することができます。

- アカウントを別のグローバル ユーザに関連付ける
- アカウントを自動検索する
- アカウントを削除する
- 削除を保留中を使用する
- 削除したアカウントを再作成する

アカウントに対するグローバル ユーザの変更

次のような場合には、アカウントを他のグローバル ユーザに関連付けたいと考えます。

- 同じ名前の 2 つのグローバル ユーザを持っており、CA Identity Manager がアカウントを間違った個人に関連付けている
- CA Identity Manager が、あるアカウントを[default user]オブジェクトに関連付けているが、自分ではこのアカウントを別のグローバル ユーザ オブジェクトに関連付けたい
- [New]を使用してアカウントを作成したが、次にそれをグローバル ユーザに関連付けたい

プロビジョニング マネージャで、アカウントを別のグローバル ユーザに関連付けるには、アカウントを、該当するグローバル ユーザへドラッグ アンド ドロップします。

自動検索が機能するしくみ

エンドポイントに対してネイティブなツールを使用して、アカウントまたは他のオブジェクトを追加または削除しても、エンドポイントを検索するまで CA Identity Manager には認識されません。 検索のプロセスでは、行われた追加および削除（および場合によっては変更）を認識し、それらの変更を、プロビジョニング ディレクトリにおけるオブジェクトの Identity Manager の表記に適用します。

ただし、この検索を行う前に、プロビジョニング マネージャを使用して、同じ名前を持つオブジェクトを作成しようとすると、CA Identity Manager は、この名前のオブジェクトがすでに存在していることに気が付き、このエラーをレポートします。 次に CA Identity Manager はこのオブジェクトを検索し、プロビジョニング ディレクトリ内で、このオブジェクトの表記を作成します。 このオブジェクトをすぐに使用することができます。 オブジェクトがプロビジョニング ディレクトリ内に存在していないくて、追加、移動、または名前変更の処理によって、エンドポイントにおいて「すでに存在している」エラーが生成された場合には必ず、1 オブジェクトの自動検索が行われます。

自動検索は、「Provisioning Reference Guide」に記載されている、Synchronization/Automatic Correlation ドメイン設定パラメータと組み合わせることができます。 これらの機能を組み合わせて有効にすると、最初にアカウント テンプレートから、新しいアカウントを作成するための試行として、アカウントを作成しようとします。 次に、以下の手順が行われます。

- 検索されていないアカウントに気が付く
- そのアカウントを自動的に検索する
- そのアカウントを、グローバル ユーザに自動的に関連付ける
- このグローバル ユーザに相互に関連付けられている既存のアカウントのように、アカウントに対してアカウント テンプレートを追加する

アカウントの削除

アカウントを削除しなければならない場合は、プロビジョニング マネージャで、次のいずれかの方法を使用します。

- アカウントを右クリックして[削除]を選択する
- グローバル ユーザを右クリックし、[Delete User and Accounts]を選択する
- アカウントの削除ウィザードを実行する
- グローバル ユーザとプロビジョニング ロールを同期させ、余分なアカウントを削除するよう指定する

プロビジョニング ロールからグローバル ユーザを削除する場合は、プロビジョニング マネージャによって、アカウントを削除するために次のオプションが提示されます。

- これらのアカウントを削除することが決まっている場合は、Identity Manager により、プロビジョニング ディレクトリからアカウントが削除されます。
- アカウントを削除することが決まっていない場合は、[Synchronize User with Roles]オプションを使用して、[アカウントの削除]を選択することができます。

アカウントを削除する前に、プロビジョニング ロールからグローバル ユーザを削除する場合は、そのグローバル ユーザに対するアカウントをリストすることができます。 グローバル ユーザを右クリックして、[List Accounts]を選択します。

- アカウントのリストには、各アカウントが属しているプロビジョニング ロールが表示されます。 あるアカウントがプロビジョニング ロールに属している場合、そのロールからユーザを削除し、ユーザの同期アクションを承認してアカウントを削除することによって削除されます。
- あるアカウントがプロビジョニング ロールに属していない場合は、それは余分なアカウントになり、ユーザの同期チェックでレポートされます。 グローバル ユーザで[Synchronize the User with Roles]メニュー項目を選択すると、アカウントが削除されます。

削除保留の使用

CA Identity Manager では、管理者が、通常はアカウントが削除されるような削除または同期のアクションを開始したときに、エンドポイントのアカウントが削除されないよう、エンドポイントごとの設定が可能です。 代わりに、アカウントは CA Identity Manager で「削除を保留中」の状態になり、管理エンドポイントでは「一時停止」の状態になります。

削除を保留中のアカウントは、プロビジョニング マネージャでは、アカウント プロパティの[統計]タブで確認できます。 一時停止のアカウントには、「削除を保留中」の一時停止理由があり、この状態になったときのタイムスタンプもあります。「削除を保留中」のステータスおよび「一時停止」のタイムスタンプを格納すると、これらの「削除を保留中」のアカウントを特定し、プロビジョニング サーバおよび管理エンドポイントから後で削除するユーティリティを記述することができます。

削除されたアカウントの再作成

Identity Manager 以外のツールを使用して、管理エンドポイントでアカウントを削除すると、アカウントの同期チェック機能で、そのアカウントが不明としてレポートされます。これは、対象のアカウントがプロビジョニング ディレクトリに存在しているのに、管理エンドポイントに存在していないためです。 このような場合には、Synchronize Account with Account Templates 関数を発行して、そのエンドポイントでアカウントを再作成します。この関数は、そのアカウントに関連付けられているアカウント テンプレートを使用して、アカウントを再作成します。

アカウントが再作成されると、Identity Manager は、アカウントが再作成されたものとして記録します。 これらのアカウントは、更新されたアカウントとは別のものと認識することができます。これは、管理者が、機能属性以外の属性(パスワードなど)が、最初のアカウント テンプレートの値にずっと設定されていることを認識している必要があるためです。

第 9 章: プロビジョニング ロール

このセクションには、以下のトピックが含まれています。

プロビジョニング ロールとアカウント テンプレート(153 ページ)
ロールおよびテンプレート タスク(154 ページ)
アカウント テンプレートの属性(161 ページ)
詳細なルール式(164 ページ)
プロビジョニング ロールのパフォーマンス(170 ページ)
既存環境用のプロビジョニング タスク(172 ページ)

プロビジョニング ロールとアカウント テンプレート

アカウント管理を単純にするために、アカウントの作成と保守にアカウント テンプレートを使用します。アカウント テンプレートは、プロビジョニング ロールで使用されます。プロビジョニング ロールには、1 つ以上のアカウント テンプレートが含まれます。 プロビジョニング ロールをユーザに適用すると、ユーザは、アカウント テンプレートで定義されたアカウントを受け取ります。

アカウント テンプレートには、特定のエンドポイント タイプのアカウントの基本設定が収められています。 アカウント テンプレートは、eTrust Admin のプロビジョニング ポリシー と同様の機能を実現します。

アカウント テンプレートを使用すると、次のことが実行できます。

- アカウントの作成時に、エンドポイントで CA Identity Manager ユーザが持つアカウント属性を制御する
- ルールの文字列や値を使用して属性を定義する
- 異なるプロビジョニング ロールのアカウント属性を組み合わせる(これにより、ユーザは特定のエンドポイントで 1 つのアカウントしか持たずに必要なアカウント属性をすべて持つことができる)
- グローバル ユーザがプロビジョニング ロールを変更するのに応じてアカウント属性を作成または変更する

ロールおよびテンプレート タスク

ユーザ コンソールで[ロールおよびタスク]を選択し、[プロビジョニング ロール]の下のタスクを選択して、プロビジョニング ロールを作成し管理することができます。 タスクは、ロールのメンバーであるユーザの作成、およびロールの変更や削除といった標準的な操作のために存在します。

プロビジョニング ロールを作成する前に、そのロールかインポートするプロビジョニング ロールにアカウント テンプレートが含まれるようにする必要があります。 インポートできるロールは、プロビジョニング マネージャか eTrust Admin で作成されたロールです。ただし、CA Identity Manager では、eTrust Admin で作成されたネストされたロールはサポートされません。

プロビジョニング ロールの作成

プロビジョニング ロールを作成するには、以下のロール要件を決定する必要があります。

- 別のアカウントを必要としているのはどのユーザか
- どのアカウントをロールに関連付けるか
- ロールのメンバ、管理者、および所有者となるのは誰か

プロビジョニング ロールを作成する方法

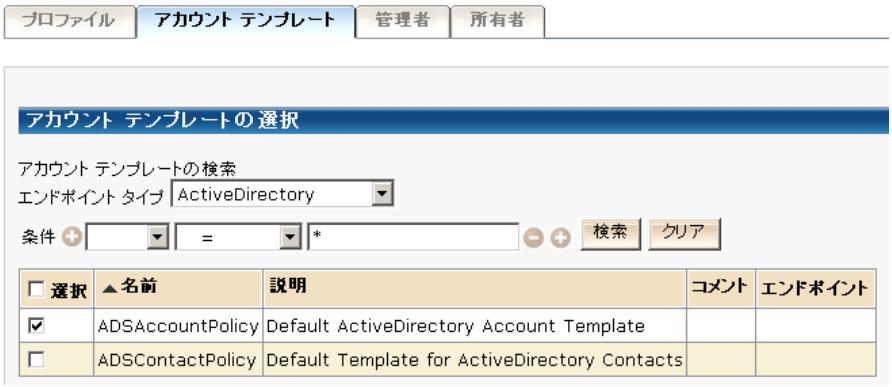
1. ユーザ コンソールで、[ロールおよびタスク]-[プロビジョニング ロール]-[プロビジョニング ロールの作成]をクリックします。

   各タブの詳細については、画面のヘルプのリンクをクリックしてください。

2. [プロファイル]タブを設定します。 必須となるのは[名前]フィールドのみです。

   注: [プロファイル]タブに、プロビジョニング ロールに関する追加情報を指定するカスタム属性を指定することができます。 この追加情報は、多数のロールを含む環境におけるロール検索を簡易化できます。

3. [アカウント テンプレート]タブを設定します。
   a. ActiveDirectory などの[エンドポイント タイプ]をクリックします。
   b. アカウント テンプレートをクリックします。
      [エンドポイント タイプ]によってクリックできるテンプレートが決められます。
   c. 必要に応じて異なるエンドポイント タイプのアカウント テンプレートを追加します。



4. 管理ルールを設定して、このロールのメンバおよび管理者に対する管理者を設定します。[管理者]タブの入力は完了です。
5. 誰がこのロールを変更できるかを制御する所有者ルールを追加して、[所有者]タブを設定します。
6. [送信]をクリックします。
7. ロールの作成を確認するには、[プロビジョニング ロール]-[プロビジョニング ロールの表示]をクリックします。

プロビジョニング ロールのインポート

プロビジョニング ロールはユーザ コンソールで管理しますが、プロビジョニング ロールによってプロビジョニング マネージャまたは外部アプリケーションで作成されたものもあります。 このようなプロビジョニング ロールの場合、ユーザ コンソールで管理できるようにロール所有者を「CA Identity Manager 管理者」にリセットすることができます。

プロビジョニング ロールをインポートする方法

1. システム マネージャ ロールを持つユーザとしてユーザ コンソールにログインします。 [ロールおよびタスク]をクリックします。
2. [プロビジョニング ロール]-[プロビジョニング ロール所有者のリセット]をクリックし、プロビジョニング マネージャで作成されたプロビジョニング ロールを選択します。

3. 誰がこのロールを変更できるかを制御する所有者ルールを追加して、[所有者]タブを設定します。
4. [送信]をクリックします。

これで、プロビジョニング ロール カテゴリのタスクを使用してロールの変更、割り当て、表示が可能になります。

プロビジョニング ロールへの新規所有者の割り当て

複数のプロビジョニング ロールを選択して、それらのロールを誰が変更できるかを制御する所有者ポリシーを割り当てることができます。

プロビジョニング ロールに新規所有者を割り当てる方法

1. システム マネージャ ロールを持つユーザとしてユーザ コンソールにログインします。
2. [ロールおよびタスク]をクリックします。
3. [プロビジョニング ロール]-[プロビジョニング ロールに割り当てる所有者ポリシーを作成]をクリックします。
4. プロビジョニング ロールを 1 つ以上選択します。
5. 誰がこのロールを変更できるかを制御する所有者ルールを追加して、[所有者]タブを設定します。
6. [送信]をクリックします。

新規所有者ポリシーを満たすユーザは、選択したプロビジョニング ロールを変更することができます。

アカウント テンプレートの作成

各エンドポイント タイプのデフォルトのアカウント テンプレートは、Identity Manager サーバにインストールされています。 プロビジョニング ロールでは、デフォルトのアカウント テンプレートを使用するか、または 設定した任意のエンドポイント(137 ページ)用に独自のアカウント テンプレートを作成することができます。

アカウント テンプレートを作成する方法

1. [エンドポイント]-[アカウント テンプレート]-[アカウント テンプレートの作成]を選択します。
2. そのテンプレートのエンドポイント タイプを選択します。
3. [エンドポイント名]をエンドポイントのシステム名、または該当する場合はローカルホストとして定義します。
4. タブのフィールドに入力するか、デフォルトの値を使用します。

   各エンドポイント タイプには、異なるタブ セットが使用されています。 フィールドの定義については、[ヘルプ]をクリックしてください。
5. [エンドポイント]タブで使用するエンドポイントを選択します。
6. [送信]をクリックします。

プロビジョニング ロールによって作成されたアカウントのパスワード

ユーザがプロビジョニング ロールに割り当てられると、Identity Manager ユーザのパスワードがエンドポイントのパスワード要件を満たさない場合、そのユーザのアカウント作成は失敗します。 一時パスワードを持つ新規ユーザの作成の場合も同様です。

したがって、Identity Manager パスワード ポリシーをエンドポイント パスワード ポリシーよりも厳しいものに設定します。 ユーザ コンソールへの次回のログイン時に、現在のパスワードをエンドポイントの要件を満たすパスワードに変更する必要があります。

プロビジョニング ロール イベントの処理順序

デフォルトの CA Identity Manager のタスクの中には、プロビジョニング ロール メンバシップを決定するイベント(タスクを完了するために CA Identity Manager によって実行されるアクション)があります。 たとえば、デフォルトの[ユーザの変更]タスクには、AssignProvisioningRoleEvent および RevokeProvisioningRoleEvent が含まれます。プロビジョニング ロールの割り当てまたは取り消しにより、エンドポイントでアカウントを追加または削除できます。 場合によっては、エンドポイントで、すべての[追加]アクションを[削除]アクションの前に行うことを要求されることがあります。

CA Identity Manager によって[追加]アクションが最初に処理されるようにするには、管理コンソールでプロビジョニング ロール メンバシップ イベントの累積の設定を有効にします。 この設定が有効になると、CA Identity Manager により、すべての[追加]および[削除]アクションを AccumulatedProvisioningRolesEvent と呼ばれる単一のイベントに累積します。 たとえば、[ユーザの変更]タスクにより、1 人のユーザに 3 つのプロビジョニング ロールが割り当てられ、そのユーザから 2 つの他のプロビジョニング ロールが削除される場合、3 つの [追加]アクションと 2 つの[削除]アクションを含む AccumulatedProvisioningRolesEvent が生成されます。

このイベントを実行すると、すべての[追加]アクションは、単一の操作に統合され、プロビジョニング サーバに送信され、処理されます。 [追加]アクションの処理が完了すると、CA Identity Manager により、[削除]アクションが単一の操作に統合され、その操作がプロビジョニング サーバに送信されます。

この設定を有効にすると、以下の CA Identity Manager の機能に影響を及ぼします。

- ユーザ タスクの[プロビジョニング ロール]タブ

  管理者が、[プロビジョニング ロール]タブを使用して、プロビジョニング ロールからユーザを追加または削除すると、CA Identity Manager によりこれらのアクションは単一のイベントに累積されます。

- アイデンティティ ポリシー

  アイデンティティ ポリシーの評価の結果、生成されるすべてのプロビジョニング ロール メンバシップ イベント(AssignProvisioningRoleEvent または RevokeProvisioningRoleEvent)は、単一の AccumulatedProvisioningRolesEvent に累積されます。 CA Identity Manager では、このイベントは他のセカンダリ イベントと同様に実行されます。 たとえば、2 つのアイデンティティ ポリシーを含むアイデンティティ ポリシー セットがあると考えてみてください。Policy A は、プロビジョニング ロール A でメンバシップを削除し、Policy B は、プロビジョニング ロール B でユーザ メンバを作成します。 CA Identity Manager により、あるユーザが Policy A は満たさなくなったが Policy B は満たすと判断されれば、2 つのアクション([削除]アクション 1 つと[追加]アクション 1 つ)を含む AccumulatedProvisioningRolesEvent が生成されます。 まず、[追加]アクションが実行され、次に[削除]アクションが実行されます。

- サブミット済みタスクの表示

  AccumulatedProvisioningRolesEvent のステータスおよび個々のアクションのステータスを確認するには、[サブミット済みタスクの表示]タスクを使用して、イベントの詳細を表示します。

  個々のアクションのいずれかが失敗すると、イベントのステータスは失敗となり、そのタスクは失敗状態に移行します。

- ワークフロー

  ワークフロー プロセスを、AccumulatedProvisioningRolesEvent に関連付けできます。 この場合、承認者は、そのイベント全体を承認または拒否できます。これにより、個々の各イベントも承認または拒否されることになります。

  AccumulatedProvisioningRolesEvent 内で個々のイベントのワークフローを有効にするには、追加設定（160 ページ）が必要となります。

- 監査

  CA Identity Manager では、AccumulatedProvisioningRolesEvent および個々の各イベントに関する情報の監査が行われます。

プロビジョニング ロール メンバシップ イベント累積の有効化

CA Identity Manager では、管理コンソールで設定を行うことができ、プロビジョニング ロール メンバシップ イベントのすべての[追加]および[削除]アクションを単一の操作に統合できます。 アクションが統合されると、CA Identity Manager により、[削除]アクションの処理の前に、[追加]アクションが単一の操作として処理されます。

これにより、一部のエンドポイント タイプで要求されるイベントの順序付けが可能になります。

注: この機能は、デフォルトで無効になっています。

プロビジョニング ロール メンバシップ イベントの累積を有効にする方法

1. Identity Manager の管理コンソールにアクセスします。
2. [環境]をクリックします。
3. 設定する環境を選択します。
4. [詳細設定]の[Provisioning]を開きます。
5. [Enable Accumulation of Provisioning Role Membership Events]チェック ボックスをオンにします。
6. アプリケーション サーバを再起動します。

AccumulatedProvisioningRolesEvent ワークフロー サポートの追加

AccumulatedProvisioningRolesEvent 内での個々の追加/削除アクションで承認が必要とされる場合、ロール、タスク、ワークフロー プロセスの定義を変更するには、追加設定が必要となります。

注: この追加設定は、展開において AccumulatedProvisioningRolesEvent 内の個々のアクションを承認する必要があり、CA Identity Manager 環境が CA Identity Manager r12 CR1 より前のリリースで作成された場合のみ必要となります。

AccummulatedProvisioningRolesEvent 内で個々のアクションを承認または拒否するには、承認者は、特定の承認画面で各アクションに対して[承認]または[拒否]ラジオ ボタンを選択する必要があります。 少なくとも 1 つのアクションが承認されると、そのイベントは承認状態に移行し、実行されます。 すべてのアクションが拒否された場合、イベントは拒否状態に移行した後にキャンセル状態に移行します。

注: 各アクションのステータスを表示するには、[サブミット済みタスクの表示]を使用して、AccumulatedProvisioningRolesEvent の詳細を表示します。

この手順には、CA Identity Manager 管理ツールのフォルダを表示する admin_tools への参照が含まれています。

管理ツールは、以下のデフォルトの場所に配置されます。

- Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

AccumulatedProvisioningRolesEvent のワークフローを有効にする方法

1. 既存の環境の場合、管理コンソールのロールとタスク設定で、該当するアップグレード ロール定義ファイル(Upgrade-8.1-to-12.5-RoleDefinitions.xml または Upgrade-12-to-12.5-RoleDefinitions.xml)をインポートします。

   詳細については、「Upgrade Guide」を参照してください。

   注: CA Identity Manager r12.0 CR1 以降を使用して構築した新規環境の場合、承認タスクは新規環境で利用できるので、AccumulatedProvisioningRolesUpdate.xml のインポートは必要ありません。
2. アプリケーション サーバを再起動します。
3. [管理タスクの表示]を使用して、[累積プロビジョニング ロールを承認]タスクが存在することを確認します。
4. Archive.bat プログラムを実行します。このプログラムは、admin_tools¥Workpoint¥bin フォルダ内にあります。

5. AccumulatedProvisioningRolesApproveProcess.zip をインポートします。このファイルは、admin_tools¥Workpoint¥bin フォルダ内にあります。
6. Designer.bat を開いて、このプロセスの定義が現在存在することを確認します。

   これで、ワークフローにより AccumulatedProvisioningRolesEvent がサポートされます。

アカウント テンプレートの属性

アカウント テンプレートの属性を使用して、アカウントの属性の定義方法を決定できます。

機能と初期属性

アカウント テンプレートには、2 種類の属性が収められます。

- 機能属性は、ディスク領域のサイズ、数量、頻度制限、グループ メンバシップなどのアカウント情報を表します。 プロビジョニング マネージャでは、機能属性は、簡単に見分けられるようにすべてのアカウント テンプレート画面で太字で表示されます。
- 初期属性は、アカウント名、パスワード、アカウント ステータス、個人情報（名前、住所、電話番号など）などアカウントに初期設定される情報すべてを表します。

アカウントは、機能属性すべてが同期されたときに、アカウント テンプレートと同期されたとみなされます。 機能属性は、グループ メンバシップ、権限、クォータ、ログイン制限などユーザがアカウントへのログイン中に何ができるかを制御する属性であり、エンドポイント タイプごとに異なります。

同期によって他のアカウントの属性が更新されることはありません。 他のアカウントの属性は、アカウント作成中にアカウント テンプレートから初期化されます。また、継承の実行時に更新される場合もあります。 プロビジョニング サーバには、2 つの伝達機能（アカウント テンプレート変更時のアカウントの即時更新とグローバル ユーザ属性の変更時のアカウント更新）が用意されています。

属性のルール文字列

アカウント属性の生成には、ルール文字列が用いられます。ルール文字列は、特定のアカウント用の値に置換される変数です。 ルール文字列は、アカウントごとに変更する属性を生成する場合に便利です。 ルールの評価時に、CA Identity Manager はアカウント テンプレートに入力されたルール文字列を、グローバル ユーザ オブジェクトに指定されたデータに置き換えます。

注:検索中に作成されたアカウントにもプロビジョニング ロールなしに作成されたアカウントにも、ルール評価は実行されません。

アカウント名は一意である必要があります。したがって、アカウント テンプレートのアカウント名フィールドに %AC% ルール文字列を入力する必要があります。 CA Identity Manager がこのアカウント テンプレートからのアカウントを作成する際には、ユーザのアカウント名が使用されます。

CA Identity Manager のルール文字列の一覧を次の表に示します。

ルール文字列	説明
%AC%	アカウント名
%D%	dd/mm/yyyy 形式での現在日(日付はグローバル ユーザ情報に含まれない計算値です)。 このルール文字列は、次のいずれとも同等です。 %$$DATE()% %$$DATE%
%EXCHAB%	Exchange アドレス帳に表示されないメールボックス
%EXCHS%	メールボックス ホーム サーバ名
%EXCMS%	メールボックス ストア名
%GENUID%	数値 UNIX/POSIX ユーザ識別子 このルール変数は、グローバル ユーザの UID 値が設定されている限り、%UID% と同じです。 ただし、グローバル ユーザに UID 値が割り当てられておらず、([システム タスク]の[グローバル プロパティ]で)UID 生成が有効にされている場合、次に利用可能な UID 値が予約され、グローバル ユーザに割り当てられ、このルール変数の値として使用されます。
%P%	パスワード
%U%	グローバル ユーザ名
%UA%	住所(郵便番号、都道府県、市区町村、番地から生成)
%UB%	建物

ルール文字列	説明
%UC%	市区町村
%UCOMP%	会社名
%UCOUNTRY%	国
%UCUxx% または %UCUxxx%	カスタム フィールド(xx または xxx は、[システム タスク]フレームの[カスタムユーザフィールド]タブに指定された 2 桁または 3 桁のフィールド ID を表します)。
%UD%	説明
%UDEPT%	部署
%UE%	電子メール アドレス
%UEP%	電子メール アドレス(メイン)
%UES%	電子メール アドレス(予備)
%UF%	名
%UFAX%	FAX 番号
%UHP%	ホーム ページ
%UI%	頭文字
%UID%	数値 UNIX/POSIX ユーザ識別子
%UL%	姓
%ULOC%	場所
%UMI%	ミドル ネームのイニシャル
%UMN%	ミドル ネーム
%UMP%	モバイル電話番号
%UN%	フルネーム
%UO%	オフィス名
%UP%	電話番号
%UPAGE%	ポケットベル番号
%UPC%	郵便番号
%UPE%	内線番号
%US%	都道府県
%USA%	番地

ルール文字列	説明
%UT%	職位
%XD%	固定長文字列形式の XML dateTimeValue 形式で現在のタイムスタンプが生成されます。 dateValue 属性または timeValue 属性に、dateTimeValue の日付部分や時刻部分を取り出すためのサブ文字列表現(:offset,length)を 1 つ記述できます。 たとえば、%XD:1,10% と指定すると、YYYY-MM-DD が生成されます。%XD:12,8% と指定すると、HH:MM:SS が生成されます。

属性の値

アカウント属性に特定の定数値を使用するには、ルール文字列内にではなくアカウント テンプレート フィールド内に値を入力します。 たとえば、頻度制限と数量サイズを指定する値を入力できます。

定数の属性値にパーセント記号を含める必要がある場合、パーセント記号 1 つごとに 2 回繰り返します(%%)。 CA Identity Manager は、繰り返されたパーセント記号(%%)を、アカウント属性値の構築時に 1 つのパーセント記号 (%)に変換します。 アカウント テンプレート値にパーセント記号が 1 つしかない場合、CA Identity Manager はエラーを生成しません。 つまりこの規則では、25% のリテラル値が必要な場合、25%% と指定する必要があるということです。 ただし、特殊な場合として 25% は使用できます。

詳細なルール式

単純なグローバル ユーザ属性を代入する場合よりも柔軟性を持たせるために、以下のような詳細なルール式を入力できます。

- オフセットと長さを使用したルール式のサブストリング
- ルールの文字列と値を組み合わせて使用
- 複数値アカウント属性に複数値を設定するためのルール式
- その他のグローバル ユーザ属性のルール変数
- 組み込み関数の呼び出し
- ユーザが記述したプログラム終了関数の呼び出し

ルールの文字列と値の組み合わせの使用

アカウント テンプレートの属性値に、ルール文字列と定数値を組み合わせて使用することができます。 たとえば、ルール文字列 %UI% がない場合、以下のように複数のルール式を連結することによって同じ効果を得ることができます。

```
%UF:,1%%UMI:,1%%UL:,1%
```

ルール文字列 %UA% は以下に相当します。

```
%USA%, %UC%, %US%, %UPC%
```

また、以下のようにルール文字列と定数値を組み合わせて、UNIX ホームのエンドポイント属性を作成できます。

```
/u/home/%AC%
```

ルールのサブストリング

ルール変数のサブストリング値を作成する構文を以下に示します。

```
%var[:offset,length]%
```

var

前に示した表に定義されている、定義済みのルール変数名を表します。

offset

(オプション)サブストリング サフィックスの開始オフセットを定義します。 数字の 1 は最初の文字を表します。

length

(オプション)サブストリング サフィックスの終了オフセットを定義します。 length の値としてアスタリスク(*)を指定すると、値の最後を表します。

たとえば、アカウント属性をグローバル ユーザの建物の属性の最初の 4 文字に設定するには、以下を使用して変数を定義します。

```
%UB:1,4%
```

建物の属性が空であるか、4 文字に満たない場合、アカウントの属性値は 4 文字未満になります。

複数値のルール式

大半のルール式は単一値を扱います。 1 つのユーザ属性値(空の場合もある)を使用して開始され、結果は 1 つのアカウント属性値(これも空の場合がある)となります。 ただし、空のユーザ属性を 0 の値として考える必要がある場合があります。 また、複数値を取るアカウント属性値のために複数の値を生成する必要がある場合もあります。

以下のルール構文では、ユーザ属性に含まれる 0 以上の値を操作できます。

%*var%

ルール式の % 記号の直後にオプションの複数値フラグであるアスタリスク(*)を指定すると、参照されているユーザ属性に含まれる値の数に応じて、このルール式は 0、1、または 1 よりも大きい値になります。

大半のユーザ属性値は単一値であるため、0、または 1 の値のみが含まれます。 ただし、カスタム属性(CustomField01 ～ CustomField99)は複数値属性であるため、これらの属性を参照するルール変数は 0 、1、または 1 以上の値を含む可能性があります。

ユーザ属性に複数の値が含まれている場合に、ルール式にアスタリスク(*)を含めないと、ルール評価の結果は最初の値の結果となります。 ただし、ほとんどの場合、複数の属性値は正式に順序付けられていないため、CA Identity Manager がどの値を最初の値とみなすのか予測できません。

ユーザ属性に複数の値があり、ルール式に * を含めると、そのアカウント属性には複数の値が生成されます。 アカウント テンプレート属性から設定されるアカウント属性自体が複数値をとらない場合は、そのアカウント テンプレートには複数値のルール式を定義しないでください。

ADS エンドポイント タイプの拡張アカウント属性を複数値として定義し、その複数値のルール式構文を使ってその属性を設定することができます。 たとえば、patents という名前の拡張 ADS アカウント属性と、同じ patents という名前の付いたカスタム ユーザ属性番号 3 を定義する環境を考えてみます。

ADS アカウント テンプレートは、patents 属性としてルール文字列 %*UCU03% を定義します。 次に、1 つまたは複数の値を追加して、ユーザの patents 属性を変更できます。 ユーザに変更を加える際に、ユーザのアカウントを更新するオプションを選択します。 これによってアカウントのアカウント テンプレートが確認され、ルール変数 %*UCU03% が検出されると、ユーザのすべての patents がアカウントの patents 属性にコピーされます。

同様に、アカウントの作成中にもルール文字列は評価されます。 さらに、アカウント テンプレートの変更時にルール文字列を変更した場合、そのアカウント テンプレートに関連するすべてのアカウントのルールの再計算を選択できます。

%*var% 構文は、単一値のユーザ属性を参照する変数 var にも有効です。 有効になるのは、連結が行われ、参照される属性がユーザに設定されていない場合のみです。

オプションの複数値フラグであるアスタリスク(*)は、ユーザ属性に値がない場合に、%*var% ルール変数を含むルールが値なしと評価することを示します。 これは、単一値のルール式 %var% とは異なります。単一値のルール式は、空の文字列であっても必ず単一の値と評価します。

この違いを理解するために、以下のルール文字列について考えてみます。

(310)%UP%
(310)%*UP%

これらのルール文字列は両方とも、電話番号にエリア コード 310 を追加します。 ただし、ユーザが電話番号の値を持っていない場合に、最初のルールはアカウントの値として(310)と評価してしまう点が異なります。 2 番目のルール文字列は値を生成せず、アカウント属性は未設定のままになります。

一方、電話番号に内線番号を追加する以下のルール文字列を考えてみます。

%UP%%UPE%
%UP%%*UPE%

すべての人が電話番号を持っているのに、一部の人が内線番号を持っていない場合、最初のルール文字列は各ユーザに内線番号のない電話番号を含む値を生成します。 2 番目のルール文字列は値を生成しません。 この場合は、%UPE% を使った最初のルールを使用します。

明示的なグローバル ユーザ属性ルール

以前のルール テーブルにリストされていた属性に比べ、より多くの属性を各ユーザが持つようになりました。 これらの他の属性を参照するルール式を作成する必要はない可能性があります。 しかし、必要に応じて、以下の構文を使用して特定のユーザ属性を参照することができます。

%#ldap-attribute%

たとえば、ユーザの[一時停止]フィールドの値を特定しなければならない場合、このフィールドの対応する LDAP 属性名(eTSuspended)を特定し、0 または 1 と評価されるルール式を作成します。eTSuspended の場合、以下のように指定します。

%#eTSuspended%

もう 1 つ例を挙げると、以下のルール式でユーザの割り当てられたプロビジョニング ロールを取得できます。

%*#eTRoleDN%

これらのプロビジョニング ロールは、完全な LDAP 識別名の値です。 組み込み関数 RDNVALUE(後に示される表を参照)と組み合わせると、この値はもう少し役立つようになります。 ユーザの割り当てられたプロビジョニング ロールをすべて取得するために、複数値を示すアスタリスク(*)を使用していることに注意してください。

サブストリング構文は、これらのルール式にも適用されます。したがって、%UP:6,* と同じ内容を示す %#eTTelephone:6,*% を使用することができます。 これによって、CA Identity Manager はユーザの電話フィールドの最初の 5 文字を除きます。

組み込みルール関数

値のさまざまな変換を実行するために、ルール式に組み込みルール関数を使用できます。 組み込みルール関数を呼び出すための一般的な形式は以下のとおりです。

%[*]$$function(arg[,…])[:offset,length]%

複数値を示すアスタリスク(*)と、オフセットと長さのサブストリングの指定はオプションです。

認識されている組み込み関数は、以下のとおりです。

組み込みルール関数	説明
ALLOF	すべてのパラメータを複数値属性にマージします。 順序は保持され、重複は削除されます。 たとえば、ユーザ属性が以下のように設定されたとします。 eTCustomField01: { A, B }

組み込みルール関数	説明
	eTCustomField02: { A, C } この場合、 %*ALLOF(%*UCU01%,%*UCU02%)% というルールは 3 つの値 { A, B, C } と評価されます。
DATE	dd/mm/yyyy 形式の現在の日付が評価されます。 ルール式 %D% は以下のいずれかに相当します。 %$$DATE()% %$$DATE%
FIRSTOF	パラメータの最初の値を返します。 属性が設定されていない場合に、デフォルト値を挿入するために使用されます。 %$$FIRSTOF(%UCU01%,'unknown')% %$$FIRSTOF(%LN%,%UCU01%,%U%)% 値が設定されていないと、結果に値が含まれません。 引数に定数の文字列を入力する場合は、一重引用符で囲む必要があります。
INDEX	複数値属性の値を 1 つ返します。 Index 1 は最初の値です。 実在する値の個数より大きな値をインデックスに指定すると、結果として未設定(空)の値が返されます。 以下の 1 行目のルールは 2 行目のルールに相当します。 %$$INDEX(%*UCU01%,1)% %$$FIRSTOF(%*UCU01%)%
NOTEMPTY	1 つの引数の値を 1 つ返しますが、この属性値が設定されていないとエラーがレポートされます。 事例 1 ユーザに UID 属性が割り当てられていない場合、アカウントの作成または更新が失敗します。 %$$NOTEMPTY(%UID%)% 事例 2 名を使用し、名前が設定されていない場合には姓を使用します。 両者が設定されていない場合は、アカウントの作成または更新が失敗します。 %$$NOTEMPTY(%$$FIRSTOF(%UF%, %UL%

組み込みルール関数	説明
	)%)%
PRIMARYEMAIL	複数の電子メール アドレスから抽出された、プライマリ電子メールアドレスを返します。 式 %UE% は以下の式に相当します。 %$$PRIMARYEMAIL(%UEP%)%
RDNVALUE	属性名を LDAP 識別名として扱い、その識別名からオブジェクトの共通名を抽出します。 %*$$RDNVALUE(%#eTRoleDN%)% これによって、すべての割り当てられたプロビジョニング ロールの共通名が返されます。 ユーザが同じ共通名を持つ 2 つのプロビジョニング ロールに属する場合、そのロール名は 1 つだけリストされます。
TOLOWER	大文字のテキストを小文字に変換します。 %$$TOLOWER(%AC%)%
TOUPPER	小文字のテキストを大文字に変換します。 %$$TOUPPER(%U%)%
TRIM	属性値の前後の空白を削除します。 たとえば、通常 “%UF %UL%” は空白文字によって区切られた名と姓を作成します。 しかし、ユーザが空の名の属性を持っている場合、このルールによって値の末尾に空白が追加されてしまいます。 この場合、 “%$$TRIM(%UF% %UL%)% を使用すると、名または姓が未設定の場合でも、アカウント属性値の前後に空白が残ることはありません。

プロビジョニング ロールのパフォーマンス

プロビジョニング サーバで Identity Manager を使用する場合、プロビジョニングのパフォーマンス機能強化についていくつかの検討事項があります。

JIAM オブジェクト キャッシュ

Identity Manager は、Java IAM（JIAM）API を使用してプロビジョニング サーバと通信します。 通信のパフォーマンスを改善するには、プロビジョニング サーバから取得されるオブジェクトのキャッシュを設定します。

JIAM キャッシュの有効化

JIAM キャッシュを有効化する方法

1. 管理コンソールから環境設定にアクセスします。［詳細設定］-［その他］を選択します。
2. JIAM キャッシュのユーザ定義プロパティを設定します。
   - プロパティ: JIAMCache
   - 値: true
3. ［追加］をクリックします。
4. ［保存］をクリックします。

   ユーザ定義プロパティが保存されます。

JIAM キャッシュの TTL の定義

JIAM キャッシュはデータが失効するまでの一定期間、情報を保存します。 この期間は TTL（time-to-live、存続期間）と呼ばれます。 JIAM キャッシュの TTL を秒単位で指定し、キャッシュにデータを存続させる期間を定義します。

ローカルにキャッシュされるデータを最大限利用するには、パフォーマンスへの影響を抑えつつ、適時にデータを利用できる期間を検討する必要があります。 TTL の値として、最小で 1 日、最大で 7 日の設定を推奨します。 使用する存続期間の値の表を以下に示します。

望ましい存続期間	TTL の設定値（秒）
24 時間（1 日）	86,400
72 時間（3 日）	259,200
120 時間（5 日）	432,000
168 時間（7 日）	604,800

JIAM キャッシュ TTL を定義する方法

1. 管理コンソールから[環境]にアクセスします。[詳細設定]-[その他]を選択します。
2. JIAM キャッシュ TTL のユーザ定義プロパティを設定します。
   - プロパティ: JIAMCacheTTL
   - 値: JIAM キャッシュにデータが存続する秒数

     デフォルト: 300
3. [追加]をクリックします。
4. [保存]をクリックします。

   ユーザ定義プロパティが保存されます。

セッション プーリング

パフォーマンスを改善するために、Identity Manager はプロビジョニング サーバと通信する際に使用する、多数のセッションがプールされるように事前に割り当てることができます。

セッション プーリングの詳細については、管理コンソールのオンライン ヘルプを参照してください。

既存環境用のプロビジョニング タスク

カスタム ロール定義をインポートして、ある環境でプロビジョニングを有効化する場合、管理コンソールでプロビジョニング専用のロール定義もインポートする必要があります。このようなロール定義は、以下のフォルダにあります。

IdentityMinder.ear\management_console.war\WEB-INF\Template\environment

注: ロール定義のインポートの詳細については、「Configuration Guide」を参照してください。

第 10 章: 同期

このセクションには、以下のトピックが含まれています。

サーバ間のユーザの同期 (173 ページ)
ユーザの作成または変更タスクにおけるユーザの同期 (176 ページ)
プロビジョニング マネージャでの同期 (177 ページ)

サーバ間のユーザの同期

Identity Manager の同期を設定して、企業ディレクトリとプロビジョニング ディレクトリのユーザのデータが一致していることを確認します。 各ディレクトリの変更を行うには、インバウンド同期とアウトバウンド同期を設定します。

インバウンド同期

インバウンド同期によって、プロビジョニング ディレクトリで変更が発生した場合も Identity Manager ユーザを最新の状態に保ちます。 プロビジョニング ディレクトリの変更には、プロビジョニング マネージャやプロビジョニング サーバへのコネクタを持つシステムによって行われた変更を含みます。 同期では、管理コンソールのプロビジョニング画面で定義されたマッピングが使用されます。

プロビジョニング マネージャ操作のステータス

プロビジョニング マネージャで実行された操作を[サブミット済みタスクの表示]を使用して表示する場合、操作の実際のステータスが表示されない場合があります。 たとえば、プロビジョニング マネージャを使用してエンドポイントの取得を試み、操作が失敗したとします。 それでも、ユーザ コンソールで[サブミット済みタスクの表示]を使用すると、タスクは完了したと表示されます。 この場合、イベントの詳細で、タスクの実際のステータスを確認します。

インバウンド同期のフェールオーバ

代替 Identity Manager Server URL へのフェールオーバは、URL で指定されたアプリケーション サーバが実行されていない場合にのみ発生します。 アプリケーション サーバが実行中で通知を受信したにもかかわらず、設定エラーが発生した場合（不明な環境がある場合、または環境が起動しない場合など）、これらのエラーによって通知の配信がブロックされます。 これらの問題は、インバウンド通知が適切に機能できるように解決する必要があります。

アウトバウンド同期

アウトバウンド同期では、Identity Manager を使用して、プロビジョニング ディレクトリにおいてユーザの作成および更新を行います。

Identity Manager からのグローバル ユーザの作成

プロビジョニング ディレクトリでのユーザ作成は、プロビジョニング関連のイベント（ユーザへのプロビジョニング ロールの割り当てなど）でのみ発生します。 管理タスクを使用してユーザを作成した場合、プロビジョニング ディレクトリでユーザは作成されません。ただし、タスクがロールを割り当てた場合、またはロールを割り当てたアイデンティティ ポリシーが含まれる場合は除きます。

Identity Manager でのユーザ作成によってプロビジョニング ディレクトリでユーザが作成された場合、Identity Manager は、新しいユーザの電子メール アドレスに、プロビジョニング ディレクトリで定義された一時パスワードを送信します。 ユーザは、そのパスワードを使用してユーザ コンソールにログインできます。ただし、ログインしたら、ユーザは新しいパスワードに変更する必要があります。 その結果、ユーザ ストアとプロビジョニング ディレクトリでパスワードが同期されます。

電子メール アドレスがないユーザの場合、ユーザ ストアでパスワードを変更してからユーザ コンソールにアクセスできます。または、Identity Manager 管理者がプロビジョニング マネージャでユーザのパスワードを変更できます。

注: 一時パスワードを電子メールで送信するには、[環境]で電子メール通知を有効にし、電子メール通知に CreateProvisioningUserNotificationEvent を設定する必要があります（詳細については、「Configuration Guide」を参照してください）。

Identity Manager を使用したグローバル ユーザの更新

ユーザを変更する管理タスクを使用すると、プロビジョニング ディレクトリでユーザに対する更新が発生します。 グローバル ユーザが存在しない場合は、同期は発生しません。

アウトバウンド マッピングは、Identity Manager のユーザ イベントを、プロビジョニング ディレクトリに影響を与えるアウトバウンド イベントに整合させます。

Identity Manager User Event	Outbound Event
DeleteUserEvent	POST_DELETE_GLOBAL_USER
DisableUserEvent	POST_DISABLE_GLOBAL_USER
EnableUserEvent	POST_ENABLE_GLOBAL_USER
ModifyUserEvent	POST_MODIFY_GLOBAL_USER
ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

あるユーザが、プロビジョニング ディレクトリ内に存在しているのに、Identity Manager に存在しない場合は、ユーザ コンソールでそのユーザを作成することができます。 作成タスクに対して属性をマップしており、ユーザが同じユーザ ID を持っている場合は、プロビジョニング ユーザの属性がプロビジョニング ディレクトリで更新されます。 これで、ユーザを Identity Manager から管理できるようになります。

注: あるイベントによってユーザ属性が更新されており、その値を CA Identity Manager と同期させたい場合は、イベントをアウトバウンド イベント POST_MODIFY_GLOBAL_USER にマップする必要があります。

Identity Manager を使用したグローバル ユーザの削除

デフォルトで、アウトバウンド同期にはユーザの削除イベントが設定されています。 Identity Manager でユーザを削除すると、そのユーザは、プロビジョニング ディレクトリおよびエンドポイントのすべてのアカウントからも削除されます。

CA Identity Manager が管理エンドポイントにおいて、あるユーザのアカウントを削除できない場合、残りのアカウントからこのユーザを削除しますが、プロビジョニング ディレクトリからはこのユーザを削除しません。

たとえば、ユーザ A が UNIX アカウントおよび Exchange アカウントを持っており、これらのアカウントは、プロビジョニング サーバで管理されているとします。 Identity Manager でユーザ A が削除されると、プロビジョニング サーバは、そのユーザのアカウントを削除しようとします。 通信エラーが原因で、プロビジョニング サーバが Exchange アカウントを削除できない場合、プロビジョニング サーバはユーザ A の UNIX アカウントを削除しますが、プロビジョニング ディレクトリからはそのユーザを削除しません。 ただし、ユーザ A はユーザ ストアにはリストアされません。

パスワード同期の有効化

プロビジョニング サーバでは、Identity Manager ユーザと、関連するエンドポイント ユーザ アカウント間のパスワード同期を行うことができます。 エンドポイントで生成された変更を有効にするには、次の 2 つの設定が必要です。

- エンドポイントで生成された変更を取得し、その変更をプロビジョニング サーバへ送信するよう、エンドポイントを設定する必要があります。
- グローバル ユーザに対して、パスワード同期エージェントの有効化属性を有効にしておく必要があります。

パスワード同期を有効にする方法

1. 管理コンソールで、[詳細設定]-[プロビジョニング]を選択します。
2. [エンドポイント アカウント]の[Enable Password Changes]をチェックします。
3. [保存]をクリックします。
4. アプリケーション サーバを再起動します。

詳細情報:

パスワードの同期(116 ページ)

ユーザの作成または変更タスクにおけるユーザの同期

ユーザを作成または変更するタスクのプロファイル タブにおいて、同期は、Identity Manager に対する変更がグローバル ユーザに対しても確実に行われるか、を制御します。 ユーザを作成または変更する管理タスクを作成するときに、アイデンティティ ポリシーが作成されている場合は、同期の制御を次のように設定します。

- ユーザ同期を[タスク完了時]に設定する
- アカウント同期を[タスク完了時]に設定する

注: パフォーマンスを最大にするには、[タスク完了時]オプションを選択します。 ただし、複数のイベントが含まれているタスクについて[タスク完了時]オプションを選択すると、Identity Manager は、そのタスク内のすべてのイベントが完了するまで同期しません。 イベントの 1 つまたは複数がワークフローの承認を必要とする場合、その承認に数日かかることがあります。 Identity Manager で、すべてのイベントが完了するまでアイデンティティ ポリシーが適用されない、またはアカウントが同期されないという事態を回避するには、[各イベント発生時]オプションを選択します。

ユーザを管理する管理タスクに属性を追加する場合は、管理コンソールのプロビジョニング画面で属性マッピングを更新する必要があります。 Identity Manager の各ユーザ属性に対しては、1 つのデフォルト プロビジョニング属性が存在します。

User Attribute	Provisioning Attribute
%ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
%EMAIL%	%EMAIL%
%ENABLED_STATE%	%ENABLED_STATE%
%FIRST_NAME%	%FIRST_NAME%
%FULL_NAME%	%FULL_NAME%
%IDENTITY_POLICY%	%IDENTITY_POLICY%
%LAST_NAME%	%LAST_NAME%
%PASSWORD%	%PASSWORD%
%PASSWORD_DATA%	%PASSWORD_DATA%
%USER_ID%	%USER_ID%

プロビジョニング マネージャでの同期

プロビジョニング マネージャで、次のタイプの同期を実行できます。

ユーザ同期

各グローバル ユーザが、適切な管理エンドポイント上に必要なアカウントを持っていること、およびグローバル ユーザのプロビジョニング ロールによってコール アウトされたときに、各アカウントが適切なアカウント テンプレートに割り当てられることを保証します。

アカウントの同期

アカウント上の機能属性が、アカウント テンプレートに割り当てられているアカウントで示されている適切な値であることが保証されます。 アカウントの同期は、強い同期にすることも、弱い同期にすることもできます。 弱い同期の場合は、アカウントの機能属性が、少なくとも、そのアカウント テンプレートで必要な最小限の機能を持つことが保証されます。 強い同期の場合は、アカウントの機能属性が、そのアカウント テンプレートで必要なものと同じ機能を持つことが保証されます。［Strong Synchronization］チェックボックスが選択されている、1 つ以上のアカウント テンプレートにアカウントが属している場合は、アカウントの同期は強い同期になります。

ユーザ同期を制御するような、[Strong Synchronization]チェックボックスはありませんが、類似の概念があります。 グローバル ユーザで[Synchronize User with Roles]メニュー項目を選択すると、次の 2 つの同期オプションが表示されます。

- 不明なアカウントおよびアカウント テンプレートの割り当てを追加する。
- 余分なアカウントおよびアカウント テンプレートの割り当てを削除する。
- これは弱いアカウント同期に類似していますが、[追加]チェックボックスのみを選択して、グローバル ユーザが、割り当てられているプロビジョニング ロールで必要な最小限のアカウントを持つようにします。ただし、グローバル ユーザが、そのプロビジョニング ロールで指示されていない他のアカウントを持つことも可能です。

[追加]と[削除]の両方のチェックボックスを選択して、グローバル ユーザがどのアカウントを持つのかをプロビジョニング ロールが定義します(これは強いアカウントの同期に類似しています)。 その他のすべてのアカウントは削除されます。

プロビジョニング ロールがどのくらい正確に定義されるかに基づいて、[Weak/Strong Account Synchronization]または[Weak/Strong User Synchronization]を選択します。ユーザが、明確に定義されているプロビジョニング ロールに適合しており、アカウントアクセスがそれらのロールに関連している場合には、強い同期を使用します。

注: いくつかのエンドポイント タイプでは、デフォルトで強い同期を設定します。 詳細は、エンドポイント タイプ特有の「Connector Guide」を参照してください。

ユーザ同期とアカウントの同期は、個別に実行しなければならない別のタスクです。 通常は、ユーザ同期を最初に実行して必要なアカウントをすべて作成した後で、アカウントの同期を実行し、プロビジョニング サーバがアカウント属性の値を割り当てまたは変更できるようにします。

プロビジョニング サーバは、オブジェクトに対して次の 2 つの同期メニュー オプションのセットを用意しています。

- 同期のチェック メニュー オプションは、同期を確認し、プロビジョニング ロールに準拠していないアカウントまたはアカウント テンプレートのリストを返します。
- 同期メニュー オプションは、グローバル ユーザとそのプロビジョニング ロール、またはアカウントとそのアカウント テンプレートを同期させます。

同期のチェック機能を最初に実行すると、プロビジョニング サーバは、同期機能でどの修正を行うかを通知します。 同期のチェック機能で問題が見つからなかった場合は、同期の機能を実行しません。

注: 同期のチェック機能は、最初に実行しなくてもかまいません。 ただし、プロビジョニング マネージャに慣れてきたら、これらのコマンドを実行して、同期機能で何が行われるかを学習することをお勧めします。

グローバル ユーザで同期がずれる理由

グローバル ユーザが、プロビジョニング ロールまたはアカウント テンプレートと同期がずれている理由として、次のことが考えられます。

- ネットワークでハードウェアまたはソフトウェアの問題があるために、以前に必要なアカウントを作成しようとして失敗し、不明なアカウントが生じています。
- プロビジョニング ロールおよびアカウント テンプレートが変更されているため、余分なアカウントまたは不明なアカウントが生成されている可能性があります。
- アカウント テンプレートが作成された後にアカウントが割り当てられたため、アカウント テンプレートと同期していないアカウントが存在しています。
- アカウントを後で作成するよう指定されているため、新しいアカウントの作成が遅れています。
- 新しいエンドポイントが取得されました。 検索および相互関係付けのときに、プロビジョニング サーバは、プロビジョニング ロールをグローバル ユーザに自動的に割り当てません。したがって、新しいエンドポイント上でユーザがどのアカウントを持つのかを示すよう、ロールを更新する必要があります。 グローバル ユーザに相互関連付けられているすべてのアカウントは、グローバル ユーザが同期するときに、余分なアカウントとしてリストされます。
- アカウントをグローバル ユーザにコピーすることによって、つまり、手動で相互関連付けを行い、余分なアカウントを設定することによって、既存のアカウントがグローバル ユーザに割り当てられています。
- ユーザをロールに割り当てる以外の方法で、グローバル ユーザに対してアカウントが作成されました。 たとえば、対象ユーザのプロビジョニング ロールにないアカウント テンプレートに対して、グローバル ユーザをコピーすると、そのアカウントは、余分なアカウントとしてリストされるか、または余分なアカウント テンプレートを持つアカウントとしてリストされます。 グローバル ユーザをエンドポイントにコピーし、エンドポイントのデフォルト アカウント テンプレートを使用してアカウントを作成すると、そのアカウントは余分なアカウントになることがあります。

グローバル ユーザ同期

ユーザ同期は、グローバル ユーザに割り当てられているプロビジョニング ロールに対してアカウントが準拠するように、アカウントを作成、更新、または削除します。 したがって、管理者が、ネイティブ ツールを使用して管理エンドポイントでアカウントを追加または削除しており、ユーザは自身のエンドポイントの再検索を行って、プロビジョニング ディレクトリを更新していない場合には、実際には余分なアカウントまたは不明なアカウントがあるのに、ユーザ同期で問題がない、と示されることがあります。

アカウントの作成

プロビジョニング ロールにはアカウント テンプレートが含まれており、アカウント テンプレートはエンドポイントに関連付けられているため、グローバル ユーザは、正しいアカウント属性を持つ各エンドポイントについてリストされているアカウントを持っていなければなりません。

ユーザ同期のプロセス中に、CA Identity Manager が、必要なアカウントがエンドポイント上にないことを検出した場合は、エンドポイント上にアカウントを作成します。 グローバル ユーザのプロビジョニング ロールで複数のアカウント テンプレートが同じアカウントを規定している場合、関連するすべてのアカウント テンプレートをマージすることによって、アカウントが作成されます。 このアカウントは、これらのアカウント テンプレートに割り当てられますが、これらのテンプレートは、現在のところアカウントと同期していません。 新しく作成されたアカウントでは、アカウントの同期は必要ありません。

アカウントに対するアカウント テンプレートの追加

既存のアカウントで、1 つ以上のアカウント テンプレートの割り当てが不明である場合は、ユーザ同期により、既存のアカウントがこれらのアカウント テンプレートに割り当てられます。 1 つのアカウントが、1 つ以上の新しいアカウント テンプレートに割り当てられると、アカウント同期が自動的に実行され、アカウントの機能属性が、アカウント テンプレートで指定されている機能に更新されます。

ユーザ同期からアカウントが更新された後で、アカウントをアカウント テンプレートと同期させることも、同期させないことも可能です。 追加されたアカウント テンプレートの 1 つが強力な同期アカウント テンプレートであるか、または 1 つのアカウントに対して複数のアカウント テンプレートが追加された場合、ユーザ同期は、そのアカウントでフル アカウント同期を開始します。 ただし、弱い同期アカウント テンプレートが 1 つだけ追加された場合は、ユーザ同期は、このアカウント テンプレートのみが含まれている 1 つのアカウント同期を開始します。 更新の前に、アカウントがすでに他のアカウント テンプレートとのアカウント同期とずれてしまった場合は、それ以降も、アカウント同期とずれることがあります。

アカウントの削除

ユーザ同期のときに、余分なアカウントを削除するオプションがあります。 ただし、自身のプロビジョニング ロールでは必要ないアカウントを所有しているユーザには正当な理由があると判断される場合もあります。 そのような場合は、この削除オプションを選択してはいけません。

削除されるアカウントが管理エンドポイント内にあり、そのエンドポイントに対してはアカウントの削除が無効になっている場合は、アカウントは実際には削除されません。「削除の保留中を使用する」のセクションを参照してください。

アカウントからのアカウント テンプレートの削除

ユーザ同期を使用して、アカウントから余分なアカウント テンプレートを削除することもできます。 これは、削除オプションを選択した場合のみ行われます。 ユーザ同期で、あるアカウントを更新して 1 つ以上の余分なアカウントを削除する必要があると判断した場合は、そのアカウントでアカウント同期が自動的に実行され、機能属性と、対象のアカウント上の残りのアカウント テンプレートが同期されます。

このアカウント同期は、アカウントからアカウント テンプレートを削除するときに発生します。残りのアカウント テンプレートのいずれかが強い同期に対してマークされている場合は強い同期を使用し、残りのアカウント テンプレートのすべてが弱い同期に対してマークされている場合は弱い同期を使用します。

弱い同期と強い同期のどちらが使用されているかによって、アカウント テンプレートがアカウントに割り当てられたときに以前に付与されたアカウント属性が、そのアカウント テンプレートが後で削除されたときに消去されるかどうかが異なります。 強い同期を使用している場合、アカウント テンプレートによって付与された機能(グループ メンバシップや、より多くのクォータなど)は、対象のアカウント上の残りのアカウント テンプレートでこの機能を指示していなければ、消去されます(グループ メンバシップが削除されるか、またはクォータが低減されます)。 ただし、弱い同期の場合、通常はアカウントは変更されません。これは、プロビジョニング サーバでオンデマンドの特別な機能と、アカウント テンプレートによって付与された機能を区別しないからです。

SyncRemoveValues 属性としてとして指定されている、いくつかの複数値の機能属性は、このルールが当てはまりません。 アカウントに割り当てられた値のコレクションを表記している、単一の複数値属性(グループ メンバシップのリストなど)は通常、SyncRemoveValues 属性としてリストされます。 これらの属性では、アカウントからアカウント テンプレートを削除するときに発生する弱い同期アクションによって、削除中のアカウント テンプレートで指示されていた値が(残りのアカウント テンプレートのいずれかによって指示されていなければ)削除されます。

たとえば、複数のアカウント テンプレートを作成し、各アカウント テンプレートがアカウントに対して一意のグループ メンバシップを割り当てている場合には、この SyncRemoveValues 機能は、「特別なアカウント テンプレートが不要になるよう、グローバル ユーザのプロビジョニング ロールを変更した場合、そのアカウント テンプレートで指示されたグループに属さないようアカウントも更新される」ことを意味します。 アカウント テンプレートに規定されている内容に優先して、アカウントに対して指示されたグループ メンバシップが保持されるため、これは強い同期とまったく同じではないことがわかるでしょう。

単一値のすべての属性、および SyncRemoveValues 属性として指定されていないいくつかの複数値属性では、アカウントからアカウント テンプレートを削除するときの、弱い同期アクションは、通常の弱い同期アクションと同じになり、機能は削除されません。

弱い同期によって機能を削除したくない場合は、ドメイン設定パラメータ Synchronize/Remove Account Template Values from Accounts を[いいえ]に設定して、SyncRemoveValues 機能を無効にします。

ユーザ同期のチェック

グローバル ユーザ、またはプロビジョニング ロールにおける同期をチェックし、不明なアカウントをリストすることができます。 グローバル ユーザの場合は、リストに、余分なアカウントまたはアカウント テンプレートが含まれていてもかまいません。 グローバル ユーザまたはプロビジョニング ロールに対して同期のチェックを選択できます。

次の表は、ユーザ同期をチェックする場合に、プロビジョニング サーバが何を調べるか、について説明しています。

オブジェクト	処理
グローバル ユーザ	グローバル ユーザが、個人のプロビジョニング ロールで必要なすべてのアカウントを持っていること、および各アカウントが正しいアカウント テンプレートに属していることを確認します。
プロビジョニング ロール	プロビジョニング ロールに割り当てられている各グローバル ユーザが、必要なすべてのアカウントを持っていることを確認します。 また、各アカウントが、ロールに関連付けられているアカウント テンプレートに属していることを確認します。

グローバル ユーザまたはロールの同期

グローバル ユーザまたはロールでユーザ同期を実行できます。 グローバル ユーザまたはロールで右クリックすると、ポップアップ メニューで同期を選択することができます。次の表は、グローバル ユーザまたはロールを同期するときにプロビジョニング マネージャが行う処理について説明しています。

オブジェクト	処理
グローバル ユーザ	グローバル ユーザと、そのユーザに関連付けられている各ロールを同期します。
ロール	ロールと、そのロールに関連付けられている各グローバル ユーザを同期します。

アカウント テンプレート同期

プロビジョニング マネージャでは、アカウント テンプレートに対して行った変更は、既存のアカウントに次のように影響します。

- プロビジョニング マネージャで機能属性の値を変更すると、対応するアカウント属性が更新され、必要に応じてアカウント テンプレートの属性値と同期されます。 弱い同期と強い同期の説明を参照してください。
- 一部のアカウント属性は、コネクタにより、アカウント テンプレートの変更時には更新されないように指定されています。 たとえば、アカウントの作成時のみに設定可能なエンドポイント タイプの属性や、Password 属性があります。Password 属性では、不注意に[はい]と応答してすべてのユーザのパスワードを誤ってリセットしてしまうことを避けるためです。

プロビジョニング マネージャでアカウント テンプレートを変更すると、[アカウント テンプレートの属性変更]ダイアログ ボックスが表示されます。 このダイアログ ボックスには、変更されたアカウント属性、およびアカウント属性をすぐ更新するかという質問に[はい]と答えるた場合に更新されるアカウント属性が一覧表示されます。 ダイアログ ボックスでは、アカウントへの影響の仕方の観点から、前に説明した 3 種類の属性(初期属性、機能属性、テンプレート専用属性)が区別されます。

注:アカウント テンプレートだけに影響する属性を更新した場合、このダイアログ ボックスは表示されません。 さらに、エンドポイントの種類によっては、プロパティ シートのフィールドは、アカウント属性と 1 対 1 には対応しません。したがって、1 つの属性に複数のフィールドが影響している場合もあります。

機能属性の同期方法

アカウント テンプレートで機能属性を変更すると、アカウント上の対応する属性が変更されることがあります。 特定のアカウントの属性の影響は、次の 2 つの要因により左右されます。

- アカウント テンプレートが弱い同期で定義されているか強い同期で定義されているか
- アカウントが複数のアカウント テンプレートに属しているかどうか

弱い同期

強い同期および弱い同期を指定するには、プロパティ シートで[アカウント テンプレート]タブをクリックしてから、[強い同期の使用]チェックボックスをオンまたはオフにします。

弱い同期では、グローバル ユーザのアカウントが、持つべき最小の機能の属性だけを持つことが保証されます。 大部分の種類のエンドポイントでは、弱い同期がデフォルトです。 弱い同期を使用しているテンプレートを更新して、関連するアカウントを更新するオプションをそのままにすると、CA Identity Manager は、次のように機能属性を更新します。

- アカウント テンプレートで数値フィールドが更新されており、新しい数値がアカウントの数値より大きい場合、CA Identity Manager は、新しい数値に合うようにアカウントの値を変更します。
- 選択されていなかったチェックボックスをアカウント テンプレートで選択すると、CA Identity Manager は、チェックボックスが選択されていないすべてのアカウントにおいて、そのチェックボックスを更新します。
- アカウント テンプレートでリストを変更すると、CA Identity Manager は、アカウントの値リストになかった新しいリストの値が収まるようにすべてのアカウントを更新します。

あるアカウントが他の複数のアカウント テンプレートにも属している場合(それらのテンプレートが使用しているのが弱い同期であっても、強い同期であっても)、CA Identity Manager は変更のあるテンプレートのみを参照します。 この方がすべてのアカウント テンプレートを検証するより効率的です。 弱い同期ではアカウントに機能が追加されるだけなので、これら他のアカウント テンプレートを参照する必要は通常はありません。

注: 弱い同期アカウント テンプレートから伝達された変更が機能の削除や低減を行うものであった場合、一部のアカウントが非同期のままになることがあります。 弱い同期では機能の削除や低減は決して行われないことに注意してください。 アカウントの他のテンプレートが参照されないので、弱い同期で十分かどうかがこの伝達では考慮されません。

アカウントとアカウント テンプレートを正しく同期するために、続いて[テンプレートとのアカウント同期]を実行しなければならない場合があります。 この操作には、プロビジョニング マネージャ を使用します。

強い同期

強い同期により、アカウントが、アカウント テンプレートで指定されているものと同じアカウント属性を持っていることが保証されます。

たとえば、既存の UNIX アカウント テンプレートにグループを追加するとします。 最初に、アカウント テンプレートで、Staff グループのアカウント メンバを作成します。 次に、Staff グループと System グループの両方のアカウント メンバを作成したいとします。このアカウント テンプレートに関連付けられているすべてのアカウントは、それぞれのアカウントが Staff グループおよび System グループのメンバである場合（および他のいずれのグループでもない場合）、同期されているとみなされます。 Staff グループではないすべてのアカウントは、両方のグループに追加されます。

その他にも、以下の要素を考慮する必要があります。

- アカウント テンプレートで強い同期を使用している場合、Staff および System 以外のグループに属しているアカウントは、これらの特別なグループから除外されます。
- アカウント テンプレートで弱い同期を使用している場合、アカウントは Staff グループおよび System グループに追加されます。 自身に、その他のグループが定義されているアカウントは、それらのグループのメンバをそのまま保持します。

注: アカウント テンプレートの機能属性が更新されるたびに、その変更をアカウントに適用しない場合は、アカウントとアカウント テンプレートを定期的に同期させて、アカウントとアカウント テンプレートの同期を保持する必要があります。

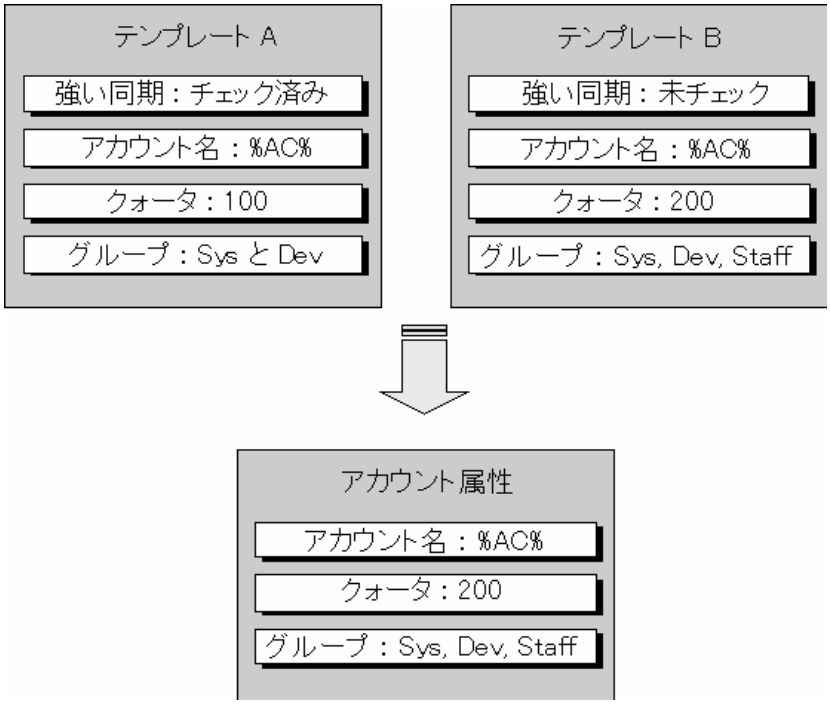
複数のテンプレートを持つアカウント

同期は、アカウントが複数のアカウント テンプレートに属しているかどうかによっても異なります。 アカウントがアカウント テンプレートを 1 つのみ持ち、そのテンプレートの同期が強い場合、各属性は、アカウント テンプレート属性値の評価対象に正確に一致するように更新されます。 その結果、属性は最初の属性と同じ値になります。

グローバル ユーザが複数のプロビジョニング ロールに属し、それぞれのロールが同じ管理対象エンドポイントに対して一定のレベルのアクセス権を持つ場合、アカウントは複数のアカウント テンプレートに属する場合があります。 この状態になると、CA Identity Manager はこれらのアカウント テンプレートを 1 つの有効なアカウント テンプレートにまとめ、個々のアカウント テンプレートの機能を合わせた上位集合として規定します。 個々のアカウント テンプレートすべての同期が弱い場合、アカウント テンプレート単体は弱い同期となりますが、アカウント テンプレートのうち強い同期を持つものが 1 つでもあると、強い同期となります。

注: アカウント テンプレートが 1 つのアカウントのみを制御している場合、弱い同期のみまたは強い同期のみを使用するのが一般的です。これは、ユーザに必要なアクセス権を企業が完全に定義しているかどうかによって決まります。 ユーザのロールが明確でなく、ユーザのアカウントに柔軟に対応する必要がある場合、弱い同期を使用します。ユーザに必要なアクセス権を明確に指定するロールを定義する場合、強い同期を使用します。

以下の例は、複数のアカウント テンプレートが 1 つの有効なアカウント テンプレートにまとめられる方法を示します。 この例では、1 つのアカウント テンプレートが弱い同期としてマークされ、もう一方のテンプレートが強い同期としてマークされています。 したがって、2 つのアカウント テンプレートをまとめて作成された有効なアカウント テンプレートは、強い同期を持つアカウント テンプレートになります。 整数を持つ Quota 属性は、2 つのアカウント テンプレートから大きい方の値をとり、複数値を持つ Groups 属性は、2 つのポリシーの値を合わせたものになります。



新しいアカウントだけの属性

アカウント テンプレートでは、一部の属性はアカウントの作成時のみに適用されます。たとえば、Password 属性は、新しいアカウントのパスワードを定義するルール表現です。このルール表現は、アカウントのパスワードを変更することはありません。 パスワード ルール表現への変更は、ルール表現が設定された後に作成されたアカウントだけに影響します。

同様に、読み取り専用アカウント属性のテンプレート ルール表現は、ルール表現が設定された後に作成されたアカウントだけに影響します。 変更は、既存のアカウントには何の影響ももたらしません。

テンプレート ルールの再計算

初期属性のテンプレート ルール表現を変更する場合、アカウントに変更を適用する機会が 1 つあります。 このオプションを拒否すると、新しいアカウントがテンプレートから作成されるときに使用するために値がテンプレートに保存されます。 その後にプロビジョニング マネージャでテンプレートに[テンプレートとのアカウント同期]操作を使用すると、アカウント上の属性ではなく機能属性だけが更新されます。

定数のテンプレート アカウント属性値などのルール表現を強制して、すべてのテンプレートのアカウントの属性を更新させるには、以下の手順に従います。

- (属性値の削除など)テンプレートに変更を行ってから、すべてのアカウントの更新を拒否します。
- 元の値に戻し、すべてのアカウントを更新することを承諾することにより、テンプレートを再び変更します。

Global-User-to-Account 伝達にもこの方法を使用できます。 グローバル ユーザ属性の変更時にアカウントに変更を伝達しない場合、後に再び行うことができます。それには、2 つの変更を行ってから、2 番目の変更でアカウントを更新することを承諾します。

アカウントの同期

アカウントの同期により機能属性が更新され、アカウントが、アカウント テンプレートで指定された機能を持つことが保証されます。

注: 同期では、アカウントの機能属性を更新しますが、アカウントの初期属性には影響を与えません。

初期属性および機能属性は、アカウント テンプレートの[Attribute Changes]ダイアログで更新されます。 アカウント テンプレートで機能属性を更新し、変更をアカウントに適用すると、属性が自動的に更新されます。

アカウント テンプレートで、機能属性の変更をそのアカウントと同期するには、アカウント テンプレートの[Attribute Changes]ダイアログを使用するか、またはこのセクションで説明した同期メニューのいずれかのオプションを使用します。

アカウント同期のチェック

アカウント、コンテナ、エンドポイント、グローバル ユーザ、アカウント テンプレート、およびロールに対してアカウントの同期をチェックできます。 この処理では、アカウント テンプレートに準拠していないアカウントのリストが返されます。 次の表は、各オブジェクトでアカウントの同期をチェックしたときに、どのようになるかを表しています。

オブジェクト	同期
アカウント	アカウント属性を同期し、関連付けられているアカウント テンプレートに確実に準拠するようにします。
コンテナ	コンテナ内の各アカウントに対するアカウント属性を同期し、関連付けられているアカウント テンプレートに確実に準拠するようにします。
エンドポイント	エンドポイント内の各アカウントに対するアカウント属性を同期し、関連付けられているアカウント テンプレートに確実に準拠するようにします。
グローバル ユーザ	各グローバル ユーザのアカウントに対するアカウント属性を同期し、関連付けられているアカウント テンプレートに確実に準拠するようにします。
アカウント テンプレート	このアカウント テンプレートに関連付けられている各アカウントのアカウント属性を同期し、アカウント テンプレートに確実に準拠するようにします。 アカウント テンプレートで強力な同期を使用している場合は、これらのアカウント属性が関連付けられているすべてのアカウント テンプレートに準拠するように、各アカウントのアカウント属性がチェックされます。
ロール	このロールに含まれているアカウント テンプレートに関連付けられている各アカウントのアカウント属性を同期し、ロール内のアカウント テンプレートに確実に準拠するようにします。

アカウントの同期

アカウント、コンテナ、エンドポイント、グローバル ユーザ、アカウント テンプレート、およびロールにおいてアカウントの同期を実行できます。 次の表に、各オブジェクトにおけるアカウントの同期の影響を示します。

オブジェクト	同期
アカウント	アカウントを、関連付けられているアカウント テンプレートと同期する。
コンテナ	コンテナ内の各アカウントを、関連付けられているアカウント テンプレートと同期する。

オブジェクト	同期
エンドポイント	エンドポイントの各アカウントを、関連付けられているアカウント テンプレートと同期する。
グローバル ユーザ	グローバル ユーザの各アカウントを、関連付けられているアカウント テンプレートと同期する。
アカウント テンプレート	関連付けられている各アカウントを、アカウント テンプレートと同期する。
ロール	各アカウントを、ロールの各カウント テンプレートと同期する。

第 11 章: アイデンティティ ポリシー

このセクションには、以下のトピックが含まれています。

アイデンティティ ポリシー (191 ページ)
アイデンティティ ポリシー セットの計画ワークシート (192 ページ)
アイデンティティ ポリシー セットの作成 (193 ページ)
アイデンティティ ポリシー セットの管理 (203 ページ)
ユーザとアイデンティティ ポリシーとの同期の方法 (204 ページ)
Identity Manager 環境のアイデンティティ ポリシー セット (208 ページ)

アイデンティティ ポリシー

アイデンティティ ポリシーは、ユーザが特定の条件やルールを満たした場合に発生する一連のビジネス変化です。 アイデンティティ ポリシー セットを使用して以下の処理を実行できます。

- ロールやグループ メンバシップの割り当て、リソースの割り当て、ユーザ プロファイル属性の変更といった、特定のアイデンティティ管理タスクを自動化する。
- 職務の分離を実行する。 たとえば、アイデンティティ ポリシーを作成し、Check Signer ロールのメンバが Check Approver ロールを所有することを禁止して社内の人間が $10,000 を超える小切手を書くことを制限することができます。
- コンプライアンスを適用する。 たとえば、特定の役職に就いており給与が $100,000 を超えるユーザを監査できます。

  コンプライアンスを適用するアイデンティティ ポリシーは、コンプライアンス ポリシーと呼ばれます。

アイデンティティ ポリシーに関連付けられるビジネス変化には以下のものがあります。

- プロビジョニング ロールをはじめとするロールの割り当てまたは取り消し (プロビジョニング ディレクトリのみを使用している場合)
- グループ メンバシップの割り当てまたは取り消し
- ユーザ プロファイルの属性の更新

たとえば、ある企業では、副社長は全員カントリー クラブ メンバー グループに所属しており、給与承認者ロールを所有していることを記述するアイデンティティ ポリシーを作成する場合があります。 ユーザの役職を副社長に変更して、このユーザをアイデンティティ ポリシーと同期すると、適切なグループとロールにユーザが追加されます。 副社長が CEO に昇進すると、副社長アイデンティティ ポリシーの条件を満たさなくなります。 よって、このポリシーで適用されていた変更は取り消され、CEO ポリシーに基づいた新しい変更が適用されます。

アイデンティティ ポリシーに基づいて発生するこの変更アクションには、ワークフロー制御下に置かれて監査されるイベントが含まれます。 前の例では、給与承認者ロールによって、所属するメンバに重要な権限が付与されます。 給与承認者ロールを保護するために、企業は、ロールの割り当ての前に一連の承認を必要とするワークフロー プロセスを作成し、Identity Manager を設定してロールの割り当てを監査できます。

アイデンティティ ポリシー管理を簡略化するため、アイデンティティ ポリシーはアイデンティティ ポリシー セットとしてグループ化されています。 たとえば、副社長ポリシーと CEO ポリシーを、幹部権限アイデンティティ ポリシー セットの一部とすることができます。

アイデンティティ ポリシー セットの計画ワークシート

アイデンティティ ポリシー セットには、アイデンティティ ポリシーが 1 つ以上含まれています。 アイデンティティ ポリシー セットを作成する前に、以下のワークシートを使用してこのセット内の各アイデンティティ ポリシーを計画してください。

質問	回答
アイデンティティ ポリシーにどのような名前を付けますか。	
どのユーザにアイデンティティ ポリシーを適用しますか。	
アイデンティティ ポリシーをユーザに適用すると、CA Identity Manager はどのようなアクションを実行しますか。	
ユーザに適用されているアイデンティティ ポリシーの適用を取り消すと、CA Identity Manager はどのようなアクションを実行しますか。	
CA Identity Manager はアイデンティティ ポリシーの変更を複数回適用しますか。それとも、ポリシーの条件を最初に満たしたときに 1 回のみ適しますか。	

ポリシー セットの各アイデンティティ ポリシーについてこのワークシートを記入したら、ポリシーが他のポリシーと競合しないことを確認してください。 たとえば、あるポリシーが取り消している権限を別のポリシーが付与しないようにします。

アイデンティティ ポリシー セットの作成

アイデンティティ ポリシー セットを作成するには、システム マネージャ ロールまたは[アイデンティティ ポリシー セットの作成]タスクを含むロールを所有している必要があります。

アイデンティティ ポリシー セットを作成するには、以下の手順に従います。

1. アイデンティティ ポリシー セットのプロファイルの定義(193 ページ)
2. ポリシー セット メンバ ルールの作成(194 ページ)
3. アイデンティティ ポリシーの作成(194 ページ)
4. アイデンティティ ポリシー セットの所有者の指定(203 ページ)

注:Identity Manager 環境のポリシーを使用するには、Identity Manager 管理コンソールでアイデンティティ ポリシーを有効にする必要があります。 詳細については、「Configuration Guide」を参照してください。

アイデンティティ ポリシー セットのプロファイルの定義

1. ユーザ コンソールから[ポリシー]-[アイデンティティ ポリシー セットの作成]を選択します。
2. アイデンティティ ポリシー セットの名前を入力します。
3. アイデンティティ ポリシー セットのカテゴリを入力します。

   カテゴリでは、アイデンティティ ポリシー セットがレポートの目的別にグループ化されます。 [カテゴリ]フィールドは必須です。
4. アイデンティティ ポリシー セットの説明を入力することもできます。

詳細情報:

ポリシー セット メンバ ルールの作成(194 ページ)
アイデンティティ ポリシーの作成(194 ページ)

ポリシー セット メンバ ルールの作成

ポリシー セットが特定のユーザのみに適用されるように、ポリシー セットのメンバ ルールを作成できます。 セットにおけるアイデンティティ ポリシーが評価される前にルールが評価され、大幅に時間を短縮できます。 たとえば、メンバ ルールによりアイデンティティ ポリシーの評価がユーザの 10 % に制限されている場合、そのルールは評価時間を 90 % 短縮できます。

ポリシー セット メンバ ルールを作成する方法

1. [ポリシー]タブを選択します。
2. [ポリシー セット メンバ ルール]で、[編集]記号をクリックします。
3. 特定のユーザのみに適用されるルールを入力します。
4. [OK]をクリックします。

詳細情報:

アイデンティティ ポリシーの作成(194 ページ)

アイデンティティ ポリシーの作成

アイデンティティ ポリシー セットのプロファイルとメンバ ルールを定義すると、このポリシー セットでアイデンティティ ポリシーを定義できます。

注: 大規模な実装環境では、アイデンティティ ポリシー ルールを評価するのにかなりの時間を要することがあります。 ユーザ属性を含むルールに対する評価時間を短縮するには、メモリ内評価オプションを有効にします。 詳細については、「Configuration Guide」を参照してください。

アイデンティティ ポリシーを作成する方法

1. [ポリシー]タブを選択します。
2. [追加]をクリックします。
3. アイデンティティ ポリシーの名前を入力します。
4. ユーザが最初にポリシーを満たしたときのみこのポリシーを適用する場合は、[1 回のみ適用]チェック ボックスをオンにします。

5. [Compliance]チェック ボックスをオンにして、コンプライアンス ポリシーとしてこのポリシーをフラグ設定します。

   このチェック ボックスをオンにした場合の処理は以下のとおりです。

   - CA Identity Manager は、コンプライアンス ポリシーと同期していないユーザに対してレポートを生成することができます。
   - [コンプライアンス違反]アクションが、[ポリシー適用/削除時のアクション]リストボックスに表示されます。

6. ポリシー条件セクション内でポリシーを適用するユーザを特定します。
7. [ポリシー適用時のアクション]セクションで、アイデンティティ ポリシーをユーザに適用したときに CA Identity Manager が実行するアクションを定義します。
8. [ポリシー削除時のアクション]セクションで、ユーザがアイデンティティ ポリシーの条件を満たさなくなったときに CA Identity Manager によって実行されるアクションを定義します。
9. [OK]をクリックします。

注: 作成したアイデンティティ ポリシー セットを使用する前に、管理コンソールでアイデンティティ ポリシーを有効にする必要があります。 詳細については、「Configuration Guide」を参照してください。

1 回のみ適用の設定

1 回のみ適用の設定によって、CA Identity Manager はアイデンティティ ポリシーの適用方法を変えることができます。

1 回のみ適用の設定を有効にする

[1 回のみ適用]設定を有効にすると、アイデンティティ ポリシーで定義された条件をユーザが最初に満たしたとき、CA Identity Manager はこのポリシーに関連付けられた変更を適用します。 ポリシーに関連付けられた変更アクションが発生するのは 1 回のみです。 このため、ポリシーが以前に適用されている場合には、CA Identity Manager はポリシーの更新をユーザに適用しません。

ユーザがポリシーで定義された条件を満たさなくなると、CA Identity Manager はポリシーの削除アクションを実行します。

[1 回のみ適用]設定は、通常、リソースのプロビジョニング時に使用されます。 たとえば、携帯電話をマネージャに割り当てるポリシーがあるとします。 ユーザが最初にマネージャになったときに、このユーザに携帯電話が割り当てられます。 CA Identity Manager はポリシーを評価するたびにではなく、1 回のみ携帯電話を発行します。 携帯電話ポリシーを更新して、新しい携帯電話モデルを追加した場合、CA Identity Manager は既存のマネージャに新しい携帯電話を発行しません。

注: CA Identity Manager をプロビジョニング サーバに統合すると、リソース プロビジョニングが使用できます。

1 回のみ適用の設定を無効にする

[1 回のみ適用]の設定を有効にしない場合、アイデンティティ ポリシーに関連付けられる変更アクションは、アイデンティティ ポリシーが評価されるたびに適用されます。 これは、変更アクションが以前に適用されたかどうかに関係なく、CA Identity Manager はポリシーの条件を満たすすべてのユーザに変更アクションを適用することを意味します。

通常、コンプライアンスを適用するアイデンティティ ポリシーでは[1 回のみ適用]設定を無効にします。 たとえば、マネージャの支出権限を $5,000 に制限するアイデンティティ ポリシーを作成できます。 CA Identity Manager でマネージャの支出権限を $10,000 に設定すると、支出権限は $5,000 にリセットされます。 マネージャをアイデンティティ ポリシーと同期するたびに、CA Identity Manager は支出権限が正しく設定されていることを確認します。

変更アクションと競合する変更を手動でユーザ プロファイルに加えると、CA Identity Manager はユーザをポリシーと同期する際にこの変更を上書きします。

上記の例では、誰かがマネージャの支出権限を手動で $10,000 に増やすと、CA Identity Manager はマネージャをポリシーと同期する際に支出権限が $5,000 にリセットします。

以下の表は、[1 回のみ適用]設定を有効または無効にしたときの影響についてまとめています。

[1 回のみ適用]の設定	動作
有効	■ アイデンティティ ポリシーに関連付けられた変更アクションが 1 回のみ適用されます。 ■ アイデンティティ ポリシー適用後に手動で加えられた変更は保持されます。 ■ CA Identity Manager が以前にアイデンティティ ポリシーを適用している場合は、このポリシーの条件を満たしているユーザに更新が適用されません。 ■ ユーザがアイデンティティ ポリシーで定義された条件を満たさなくなると、CA Identity Manager は削除アクションを実行します。
無効	■ アイデンティティ ポリシーに関連付けられた変更アクションは、ユーザをポリシーと同期するたびに適用されます。 ■ 手動で加えた変更は、アイデンティティ ポリシーの適用時に上書きされます。 ■ ポリシーの更新は、ユーザの同期時に適用されます。 ■ ユーザがアイデンティティ ポリシーで定義された条件を満たさなくなると、CA Identity Manager は削除アクションを実行します。

ポリシー条件

ポリシー条件とは、アイデンティティ ポリシーを適用するユーザを決定するルールです。

以下の表に、使用できるオプションの説明をまとめます。

構文	条件	例
(すべて)	アイデンティティ ポリシーはすべてのユーザに適用されます。	
条件 <ユーザ フィルタ>	ユーザは、1 つ以上の属性値に一致する必要があります。	役職がマネージャ、地域が東部のユーザ

構文	条件	例
内<組織ルール>	指定した組織にユーザが所属している必要があります。 **注**: このオプションを選択すると、CA Identity Manager には、以下のオプションを選択できる新しいリスト ボックスが表示されます。 ■ 組織 <組織> [かつ次より低い] - 組織検索画面を使用して、組織を選択します。組織の子組織を指定することもできます。 ■ <組織フィルタ> [かつ次より低い] 組織 - 1 つ以上の組織を選択するフィルタを指定します。	販売部門以下の組織内のユーザ
条件 <ユーザ フィルタ> および所属組織 <組織ルール>	ユーザは、特定のユーザ属性に一致しており、特定の組織に所属している必要があります。	役職 = マネージャおよび組織 = セールス*
以下のメンバである <グループ メンバ ルール>	ユーザは、グループの属性により指定される条件を満たすグループに所属している必要があります。 **注**: このオプションを選択すると、CA Identity Manager には、以下のオプションを選択できる新しいリスト ボックスが表示されます。 ■ グループ <グループ> - グループ検索画面を使用してグループを選択します。 ■ <グループ フィルタ> のグループ - 1 つ以上のグループを選択するフィルタを指定します。	所有者が CIO のグループのメンバであるユーザ

構文	条件	例
以下のメンバである <ロール ルール>	ユーザはロールのメンバである必要があります。 ロールは以下のいずれかにすることができます。 ■ アクセス ロール ■ 管理ロール ■ プロビジョニング ロール **注**: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。 詳細については、「Installation Guide」を参照してください。	ヘルプ デスク ロールのメンバであるユーザ
以下の管理者である<ロール ルール>	ユーザはロールの管理者である必要があります。 ロールは以下のいずれかにすることができます。 ■ アクセス ロール ■ 管理ロール ■ プロビジョニング ロール **注**: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。 詳細については、「Installation Guide」を参照してください。	セールス マネージャ ロールの管理者であるユーザ
以下の所有者である<ロール ルール>	ユーザはロールの所有者である必要があります。 ロールは以下のいずれかにすることができます。 ■ アクセス ロール ■ 管理ロール ■ プロビジョニング ロール **注**: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。 詳細については、「Installation Guide」を参照してください。	ユーザ マネージャ ロールの所有者であるユーザ
このクエリで返される値 <LDAP クエリ>	ユーザは LDAP クエリに基づいた条件を満たす必要があります。	LDAP クエリの条件に一致するユーザ 例: (departmentNumber=Accounts)

構文	条件	例
<管理 OR 演算制約>	ユーザは、条件のリストの中の少なくとも 1 つの条件を満たしている必要があります。管理 AND 演算制約では、以下の種類のフィルタを指定できます。 ■ アクセス/管理/プロビジョニング ロールのメンバ ■ アクセス/管理/プロビジョニング ロールの管理者 ■ アクセス/管理/プロビジョニング ロールの所有者 ■ グループのメンバ	Certify Manager ロールのメンバであるか、Certify Manager ロールの所有者であるユーザ
<管理 AND 演算制約>	ユーザは、条件のリスト内の条件をすべて満たしている必要があります。 管理 AND 演算制約では、以下の種類のフィルタを指定できます。 ■ アクセス/管理/プロビジョニング ロールのメンバ ■ アクセス/管理/プロビジョニング ロールの管理者 ■ アクセス/管理/プロビジョニング ロールの所有者 ■ グループのメンバ	Contract Initiator ロールのメンバであり、かつ Contract Approver ロールのメンバであるユーザ

ポリシー適用/削除時のアクション

アイデンティティ ポリシーの評価時に CA Identity Manager が実行する変更アクションを定義できます。 定義できるアクションには以下のものがあります。

- ポリシー適用時のアクション - ユーザがポリシー条件の条件を満たしているときに CA Identity Manager が実行する一連のアクション。
- ポリシー削除時のアクション - ユーザがポリシー条件の条件を満たさなくなったときに CA Identity Manager が実行する一連のアクション。

アイデンティティ ポリシーを適用または削除するときに CA Identity Manager が実行できるアクションは同じです。 詳細については以下の表を参照してください。

変更アクション	説明
グループ <グループ名> への追加 [...]	グループにユーザを追加します。 このオプションを選択すると、CA Identity Manager には、対象となるグループを検索できる画面が表示されます。
ユーザの組織の <グループ名> への追加	ローカル グループにユーザを追加します。 このオプションを選択すると、CA Identity Manager には、追加するグループ名を入力できるテキスト ボックスが表示されます。
<単一値ユーザ属性> の値の設定	ユーザ プロファイルの属性値を設定します。 既存の値がある場合は、CA Identity Manager によって、変更アクションで指定した値に上書きされます。
<値> の <複数値ユーザ属性> への追加	複数値のユーザ属性に値を追加します。 このオプションは既存の値を上書きしません。
アクセス ロールのメンバの作成	アクセス ロールにユーザを割り当てます。
アクセス ロールの管理者の作成	アクセス ロールのユーザ管理者の作成
管理ロールのメンバの作成	管理ロールのユーザ メンバの作成
管理ロールの管理者の作成	管理ロールのユーザ管理者の作成
プロビジョニング ロールのメンバの作成	関連するエンドポイント アカウントを作成する、プロビジョニング ロールのユーザ メンバを作成します。 **注**: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。 お使いのアプリケーション サーバの「Installation Guide」を参照してください。
プロビジョニング ロールの管理者の作成	プロビジョニング ロールのユーザ管理者を作成します。 **注**: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。 お使いのアプリケーション サーバの「Installation Guide」を参照してください。

変更アクション	説明
グループ <グループ名> からの削除 [...]	グループからユーザを削除します。 このオプションを選択すると、CA Identity Manager には、対象となるグループを検索できる画面が表示されます。
ユーザの組織の <グループ名> からの削除	ローカル グループからユーザを削除します。 このオプションを選択すると、CA Identity Manager には、追加するグループ名を入力できるテキスト ボックスが表示されます。
<値> の <複数値ユーザ属性> からの削除	複数値のユーザ属性から値を削除します。
メンバのアクセス ロールからの削除	アクセス ロールの取り消し
管理者のアクセス ロールからの削除	特定のアクセス ロールの管理者権限を取り消します。
メンバの管理ロールからの削除	管理ロールを取り消します。
管理者の管理ロールからの削除	特定の管理ロールの管理者権限を取り消します。
メンバのプロビジョニング ロールからの削除	プロビジョニング ロールを取り消します。
管理者のプロビジョニング ロールからの削除	特定のプロビジョニング ロールの管理者権限を取り消します。
監査メッセージの送信	作成したメッセージを監査データベースに送信します。 このメッセージは、作成したレポートに表示される場合があります。
コンプライアンス違反	作成したメッセージを監査データベースに送信します。 コンプライアンス レポートを作成すると、アイデンティティ ポリシーがユーザに対して適用または削除されるたびに、このメッセージが表示されます。 監査の詳細については、「Configuration Guide」を参照してください。 **注**: コンプライアンス違反オプションを使用するには、アイデンティティ ポリシー セットの[プロファイル]タブの[コンプライアンス]チェック ボックスをオンにする必要があります。

アイデンティティ ポリシー セットの所有者の指定

[所有者]タブで、アイデンティティ ポリシー セットの所有者にすることができるルールを定義します。 アイデンティティ ポリシー セットの所有者は、ポリシーセットの基本情報を変更したり、セット内のアイデンティティ ポリシーを追加、変更、または削除することができます。

[所有者]タブで以下の手順を実行します。

1. アイデンティティ ポリシー セットを変更できるユーザを決定する、所有者ルールを定義します。
2. [送信]をクリックします。

アイデンティティ ポリシー セットの管理

CA Identity Manager には、アイデンティティ ポリシー セットを管理する以下のタスクがあります。

- アイデンティティ ポリシー セットの表示
- アイデンティティ ポリシー セットの変更
- アイデンティティ ポリシー セットの削除

デフォルトでは、管理者が上記のいずれかのタスクを使用すると、CA Identity Manager には、この管理者が所有者であるアイデンティティ ポリシー セットのリストが表示されます。 管理者は、リストから必要なポリシー セットを選択できます。

アイデンティティ ポリシー セットが多く含まれている Identity Manager 環境では、アイデンティティ ポリシー セットの表示、変更、および削除タスクをカスタマイズすると、リストに表示する代わりに、管理者がアイデンティティ ポリシー セットを検索できるように設定できます。

上記のタスクをカスタマイズする方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理ロール]-[管理タスクの変更]を選択します。

   [管理タスクの変更]画面が開きます。
2. カスタマイズするタスクを検索し、選択します。
3. [スコープ]タブで、[すべてのアイデンティティ ポリシー セット]を選択します。

   このオプションを選択すると、CA Identity Manager は[デフォルトのアイデンティティ ポリシー セット検索]画面の定義を使用します。
4. [送信]をクリックします。

ユーザとアイデンティティ ポリシーとの同期の方法

アイデンティティ ポリシーを使用する際には、CA Identity Manager でのポリシー評価方法とユーザへの適用方法を理解することが重要です。 ユーザの同期プロセスを十分に理解していない場合、予期しない結果を引き起こすアイデンティティ ポリシーを設定してしまう場合があります。

CA Identity Manager でアイデンティティ ポリシーが評価および適用される方法を以下の手順に示します。

1. ユーザ同期プロセスは以下の方法で開始されます。
   - 自動 — 自動的にユーザ同期をトリガするように CA Identity Manager のタスクを設定できます。
   - 手動 — ユーザ コンソールの[ユーザの同期]タスクを使用して、ユーザを同期します。
2. CA Identity Manager は、任意のユーザに適用するアイデンティティ ポリシーの組み合わせを判断します。
3. CA Identity Manager は、そのユーザに適用しようとするアイデンティティ ポリシー一式を、そのユーザに対して適用済みのポリシー一覧と比較します。

   注: ユーザに適用されたポリシーの一覧は、ユーザ プロファイルの %IDENTITY_POLICY% 汎用属性に格納されています。 属性の設定の詳細については、「Configuration Guide」を参照してください。
   - 適用可能なポリシー一覧に含まれるいずれかのアイデンティティ ポリシーが、以前にそのユーザに適用されていない場合、そのポリシーは割り当て一覧に追加されます。
   - 適用可能なポリシー一覧に含まれるいずれかのアイデンティティ ポリシーが、以前にそのユーザに適用されていて、さらに、そのポリシーで[1 回のみ適用]が無効になっている場合、そのポリシーは再割り当て一覧に追加されます。
   - アイデンティティ ポリシーが適用可能なポリシーの一覧になく、かつ、そのポリシーがユーザに適用されている場合は、ユーザはそのポリシー条件に一致しなくなります。 CA Identity Manager はそれらのポリシーは割り当て解除一覧に追加します。
4. ユーザに対するすべてのポリシーを CA Identity Manager が評価後、以下の順序でポリシーが適用されます。
   a. 割り当て解除一覧のアイデンティティ ポリシー
   b. 割り当て一覧のアイデンティティ ポリシー
   c. 再割り当て一覧のアイデンティティ ポリシー

5. 各アイデンティティ ポリシーの適用後、CA Identity Manager はポリシーを再評価し、最初の同期化プロセス(手順 2 から 4)で発生した変更に基づいて、新たな変更が必要かどうか確認します。

   この手順は、アイデンティティ ポリシーの適用によって加えられた変更が、他のアイデンティティ ポリシーをトリガしていないことを確認するためのものです。

6. ユーザが適用可能なすべてのポリシーと同期するまで、または管理コンソールで定義された最大再帰レベルに達するまで、CA Identity Manager は引き続きアイデンティティ ポリシーの再評価と適用を実施します。

   たとえば、ユーザがロールに割り当てられると、アイデンティティ ポリシーはユーザの部署を変更します。 新しい部署は、別のアイデンティティ ポリシーをトリガします。ただし、再帰レベルが 1 に設定されている場合は、ユーザが再同期されるまで後続の変更は行われません。

   再帰レベルの設定の詳細については、管理コンソールのオンライン ヘルプを参照してください。

自動的なユーザ同期の設定

CA Identity Manager では、タスクのライフサイクル中のさまざまな時点でアイデンティティ ポリシーとユーザ アカウントを自動的に同期できます。

CA Identity Manager のタスクは、タスク処理中に発生する検出可能なアクティビティであるイベントを生成します。 たとえば、デフォルトの[ユーザの作成]タスクは、CreateUserEvent、AddUserToGroupEvent、および AssignAccessRoleEvent を生成します。 タスクの完了後、または各イベントの完了時にユーザを同期するように、CA Identity Manager を設定できます。

注: 「アイデンティティ ポリシーとユーザの同期化」(204 ページ) のセクションではユーザ同期化プロセスについて詳しく説明しています。

ユーザ同期化をトリガするタスクを設定する方法

1. 管理タスクを変更可能なユーザとして CA Identity Manager にログインします。
2. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。

   CA Identity Manager の検索画面が表示されます。

3. ユーザ同期化をトリガする管理タスクを検索して、選択します。

4. この管理タスクの[プロファイル]タブの[ユーザの同期]フィールドで以下のいずれかのオプションを選択します。

   - オフ — このタスクはユーザ同期化をトリガしません。
   - タスク完了時 —CA Identity Manager は、イベントがすべて完了した後にユーザ同期化プロセスが開始されます。 この設定は、[ユーザの作成]、[ユーザの変更]、および[ユーザの削除]タスクのデフォルト同期化オプションです。 それ以外の他のタスクのデフォルト設定は、[オフ]です。

     注: 複数のイベントを含むタスクに対して[タスク完了時]オプションを選択すると、CA Identity Manager は、そのタスク内のすべてのイベントが完了するまでユーザは同期されません。 イベントの 1 つまたは複数がワークフローの承認を必要とする場合、その承認に数日かかることがあります。 すべてのイベントが完了するまで CA Identity Manager がアイデンティティ ポリシーを適用しないでいることを避けるには、[各イベント発生時]オプションを選択します。
   - 各イベント発生時 — CA Identity Manager は、タスク内の各イベントが完了したときにユーザ同期化プロセスが開始されます。

     同一のユーザにプライマリ イベントとセカンダリ イベントがあるタスクの場合は、ユーザ同期化を[各イベント発生時]に設定すると、[タスク完了時]オプションを選択した場合よりも、ユーザに適用されるポリシーを評価する回数が多くなります。

手動によるユーザの同期化

ユーザ アカウントが正しい権限を有しているか、またはコンプライアンス ポリシーに従っているかどうかを確認する場合、ユーザとアイデンティティ ポリシー セットを手動で同期できます。

Identity Manager ユーザ コンソールで[ユーザの同期]タスクを使用することで、ユーザを手動で同期できます。

注: [ユーザの同期]タスクが適切に動作するには、[ユーザの同期]オプションを[オフ]に設定し、[アカウントの同期化]オプションを[タスク完了時]または[各イベント発生時]に設定する必要があります。 パフォーマンスを高めるには、[タスク完了時]オプションを選択します。 これらのオプションは、ユーザ同期の[プロファイル]タブで設定します。

[ユーザの同期]タスクには、以下のタブが含まれます。

- 現在一致しているポリシー — [ユーザの同期]タスクをサブミットしたときにユーザに適用されるアイデンティティ ポリシーの一覧を表示します。

  注: [現在一致しているポリシー]タブには、[ユーザの同期]タスクにアクセスした時点でユーザに適用されるアイデンティティ ポリシーのみが表示されます。 ユーザをこれらのポリシーと同期すると、他のアイデンティティ ポリシーがトリガされる変更が発生する場合があります。 これらのポリシーを確認するまで CA Identity Manager で新しいポリシーが適用されないようにするには、Identity Manager 管理コンソールでアイデンティティ ポリシーの再帰レベルを 1 に設定します。 [ユーザの同期]タスクをサブミットした後に、再度このタスクにアクセスして、ポリシーを確認します。

- すでに適用されているポリシー — すでにユーザに適用されているアイデンティティ ポリシーの一覧を表示します。

- 同期化サマリ — ユーザに適用するアイデンティティ ポリシーおよびこのポリシーの変更アクションをすべて表示します。

ユーザ アカウントを同期する方法

1. [ユーザの同期]タスクを使用可能なユーザとして Identity Manager にログインします（デフォルトでは、システム マネージャ ロールを所有するユーザはこのタスクを使用できます）。
2. [ポリシー]-[ユーザの同期]を選択します。

   [ユーザの同期]タスクが開きます。
3. [同期化サマリ]タブを選択します。
4. ユーザに適用されるポリシーおよび関連するアクションを確認して、[サブミット]をクリックします。

ユーザ同期化の確認

ユーザがアイデンティティ ポリシーと同期化されるときに適切な変更が行われることを確認するには、[ユーザの同期]タスクで[すでに適用されているポリシー]タブを確認します。

1. [ユーザの同期]タスクを使用可能なユーザとして CA Identity Manager にログインします（デフォルトでは、システム マネージャ ロールを所有するユーザはこのタスクを使用できます）。
2. [ポリシー]-[ユーザの同期]を選択します。

   [ユーザの同期]タスクが開きます。

3. [すでに適用されているポリシー]タブを選択します。
4. CA Identity Manager が、ユーザに適用されるポリシーおよび関連するアクションを確認します。

Identity Manager 環境のアイデンティティ ポリシー セット

以下のセクションでは、アイデンティティ ポリシーを使用するさまざまな方法について説明しています。

- 例: ユーザ属性を自動的に追加する(208 ページ)
- 例: リソースおよび権限付与の割り当て(209 ページ)
- 例: コンプライアンス の適用(210 ページ)
- 例: 職務の分離の実行(211 ページ)

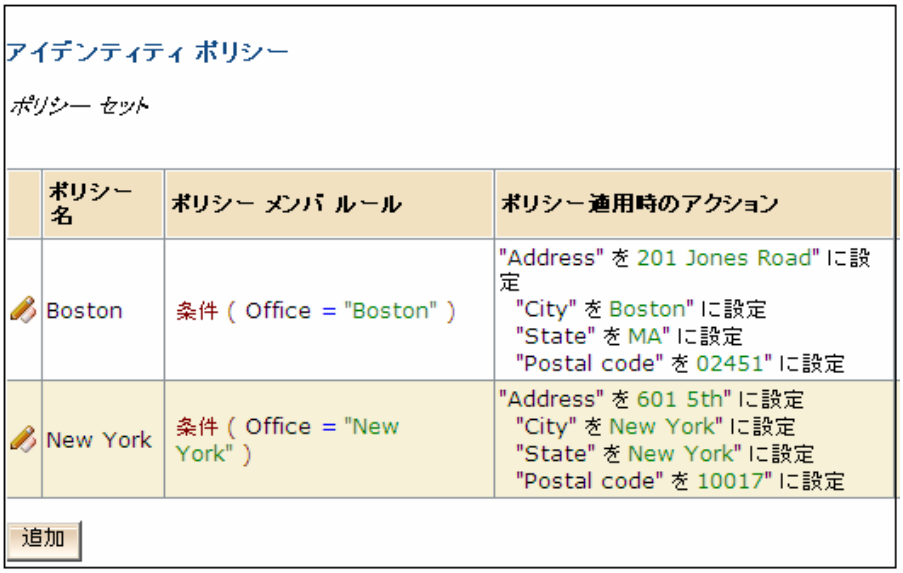
例: ユーザ属性を自動的に追加する

アイデンティティ ポリシー セットを使用して、別の属性値やユーザ権限に基づいてユーザ属性値を自動的に割り当てることができます。 たとえば、ユーザのホーム オフィスに基づいてユーザの送付先住所を自動的に入力するアイデンティティ ポリシー セットを作成することができます。

従業員の住所のアイデンティティ ポリシーを設定するには、オフィスの場所ごとに以下の設定でアイデンティティ ポリシーを作成します。

設定	値
ポリシー条件	オフィス =<オフィスの場所>
ポリシー適用時のアクション	番地の設定 =<番地の住所> 市区町村の設定 =<市区町村> 都道府県の設定 =<都道府県> 郵便番号の設定 =<郵便番号>

以下の図は、従業員の住所のアイデンティティ ポリシー セットのサンプル ポリシーを示しています。



例: リソースおよび権限付与の割り当て

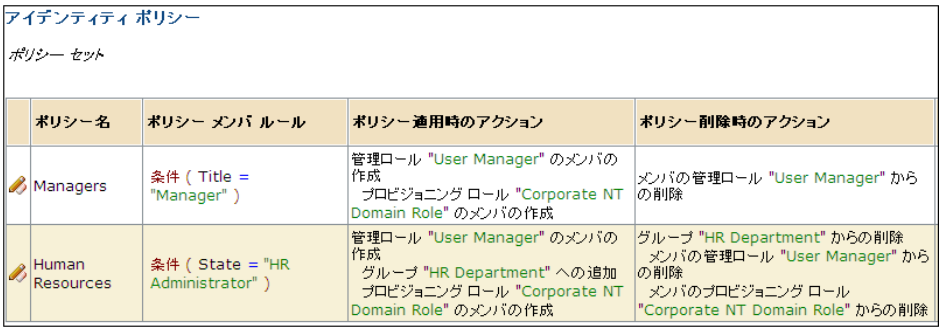
アイデンティティ ポリシーでは、ユーザがポリシー条件を満たしたときに、ドメイン アカウントなどのリソースの割り当て、ユーザをロールのメンバにするといった権限の付与を自動的に行うことができます。 たとえば、ユーザの役職に基づいてリソースとロールを割り当てる一連のアイデンティティ ポリシーを作成できます。

リソースおよびロールを割り当てるアイデンティティ ポリシーを作成するには、組織の役職ごとに以下の設定でアイデンティティ ポリシーを作成します。

設定	値
ポリシー条件	役職 =<役職>
ポリシー適用時のアクション	ポリシー条件を満たすユーザにリソースまたは権限を割り当てるアクションです。以下に例を示します。 ■ <グループ> のメンバの作成 ■ 管理ロール <管理ロール> のメンバの作成 ■ プロビジョニング ロール <プロビジョニング ロール> のメンバの作成

設定	値
ポリシー削除時のアクション	ユーザがポリシー条件を満たさなくなったときにリソースまたは権限を削除するアクションです。 たとえば、アイデンティティ ポリシーを適用されたときにユーザがロールのメンバになった場合、ユーザがポリシー条件を満たさなくなるときにロールが取り消されるように Identity Manager を設定することができます。

以下の図は、従業員のリソースのアイデンティティ ポリシー セットのサンプル ポリシーを示しています。



アイデンティティ ポリシー

ポリシー セット

	ポリシー名	ポリシー メンバ ルール	ポリシー適用時のアクション	ポリシー削除時のアクション
	Managers	条件 (Title = "Manager")	管理ロール "User Manager" のメンバの作成 プロビジョニング ロール "Corporate NT Domain Role" のメンバの作成	メンバの管理ロール "User Manager" からの削除
	Human Resources	条件 (State = "HR Administrator")	管理ロール "User Manager" のメンバの作成 グループ "HR Department" への追加 プロビジョニング ロール "Corporate NT Domain Role" のメンバの作成	グループ "HR Department" からの削除 メンバの管理ロール "User Manager" からの削除 メンバのプロビジョニング ロール "Corporate NT Domain Role" からの削除

例: コンプライアンスの適用

アイデンティティ ポリシーを設定して、存在しなければならない条件、または存在してはいけない条件を定義したり、これらの条件の評価に基づいて特定のアクションを実行したりできます。 たとえば、マネージャの支出上限を $5,000 に制限することを記述するコンプライアンス ポリシーを定義できます。 あるマネージャの支出上限が $10,000 である場合は、CA Identity Manager では、このマネージャの支出上限をリセットして、監査目的のためコンプライアンス違反を記録することができます。

支出上限を適用するコンプライアンス ポリシー セットを作成するには、以下の手順に従ってアイデンティティ ポリシーを作成します。

設定	値
1 回のみ適用	無効
コンプライアンス	[有効]

設定	値
ポリシー条件	コンプライアンスまたはコンプライアンス違反を定義する条件。以下に例を示します。 役職 =<役職> AND 支出上限 =<支出上限>
ポリシー適用時のアクション	ポリシー条件の適用時に CA Identity Manager によって実行されるアクション。以下に例を示します。 ■ コンプライアンス違反メッセージ: 支出上限を超えています ■ 支出上限を <値> に設定

以下の図に、この例で説明したコンプライアンス ポリシーの例を示します。

例: 職務の分離の実行

アイデンティティ ポリシーで同じユーザに同時にロールを許可できない相互排他的なロールを定義できます。 たとえば、昇給を許可できるユーザ マネージャが給与承認担当者にならないようにすることができます。

職務の分離を適用するアイデンティティ ポリシー セットを作成するには、以下の手順に従ってアイデンティティ ポリシーを作成します。

設定	値
1 回のみ適用	無効
コンプライアンス	[有効]

設定	値
ポリシー条件	<管理 AND 演算制約> オプションを使用して、ビジネス ポリシーに違反する一連の条件を定義します。 ユーザがすべての条件を満たす場合は、[ポリシー適用時のアクション]フィールドのアクションが実行されます。 たとえば、以下のようにポリシー条件を設定します。 AND 演算(<ロール>のメンバである)かつ(<他のロール>のメンバである)
ポリシー適用時のアクション	ポリシー条件の適用時に実行されるアクション。以下に例を示します。 ■ コンプライアンス違反メッセージ: ユーザが相互に排他的なロールを所有しています ■ <ロール> からメンバを削除します

以下の図に、この例のアイデンティティ ポリシーを示します。

第 12 章: CA Role & Compliance Manager 統合

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 Role & Compliance Manager の統合 (213 ページ)
Smart Provisioning (214 ページ)
CA Identity Manager および CA RCM の通信方法 (214 ページ)
共有情報 (217 ページ)
動的通知 (218 ページ)
CA RCM ロール モデル (218 ページ)
CA RCM との統合を設定する方法 (219 ページ)
CA RCM 内の CA Identity Manager データ分析 (243 ページ)
サジェストされたプロビジョニング ロール (247 ページ)
コンプライアンス メッセージおよびパターン メッセージ (258 ページ)

CA Role & Compliance Manager の統合

CA Role & Compliance Manager (CA RCM) は、ロール モデルを迅速かつ正確に開発、保守、および分析できる、アイデンティティ ライフサイクル管理製品です。 また、集中管理されたアイデンティティ コンプライアンス ポリシー制御と、コンプライアンスとセキュリティの要求を満たすプロセスの自動化を可能にします。 CA RCM を使用すると、以下を実行できるようになります。

- ユーザが適切な権限を持っているかどうかの検証
- 権限がセキュリティ ポリシーに従って付与されているかどうかの確認
- アイデンティティ管理制御の効果の監視
- 組織に存在するロールの理解、および組織に適したロール モデルの作成
- ビジネスの成長に合わせたロール モデルの分析と保守

CA Identity Manager は、以下の 2 つの方法で CA RCM に統合されます。

- CA Identity Manager コネクタ

  CA Identity Manager のコネクタは、CA Identity Manager と CA RCM のロールベースの権限データを自動的に同期させます。 コネクタを使用することによって、CA Identity Manager から CA RCM にデータをインポートしたり、CA RCM から CA Identity Manager にデータをエクスポートしたりできます。

  注: CA Identity Manager コネクタの詳細については、「CA RCM Connector for CA Identity Manager Guide」を参照してください。

- スマート プロビジョニング

  CA Identity Manager が CA RCM と統合されている場合、日常のアイデンティティ管理操作をサポートするためにロール モデルで使用可能な、ロールとコンプライアンス情報を使用できるようにする追加機能を設定できます。 CA Identity Manager への変更によって、CA RCM のロール モデルが動的に更新されます。

Smart Provisioning

Smart Provisioning は、日々のアイデンティティ管理作業を簡略化する機能の集まりです。CA Identity Manager が、CA RCM と統合されている場合に利用できます。 この機能には、以下が含まれます。

- サジェスト プロビジョニング ロール
- パターン外メッセージ
- コンプライアンス外メッセージ

Smart Provisioning は、CA RCM に Identity Manager データに基づいて確立されたロール モデルがあれば、Identity Manager 環境に実装できます。

CA Identity Manager および CA RCM の通信方法

CA Identity Manager と CA RCM が統合されると、以下の通信が発生します。

1. CA RCM 管理者が CA Identity Manager コネクタを設定し、プロビジョニング サーバからデータを取得します。
2. CA RCM は CA Identity Manager からのデータを使用して CA RCM でロール モデルを作成し、ロール エンジニアが必要に応じてこれを調整します。

3. ロール モデルが完了すると、ロール エンジニアは結果をエクスポートしてロール モデルを Identity Manager データに直接適用します。

   データは Java Identity and Access Management (JIAM) API を使用して CA Identity Manager に送信されます。

   この結果、CA RCM が CA Identity Manager の以下のアクションを 完了させる可能性があります。

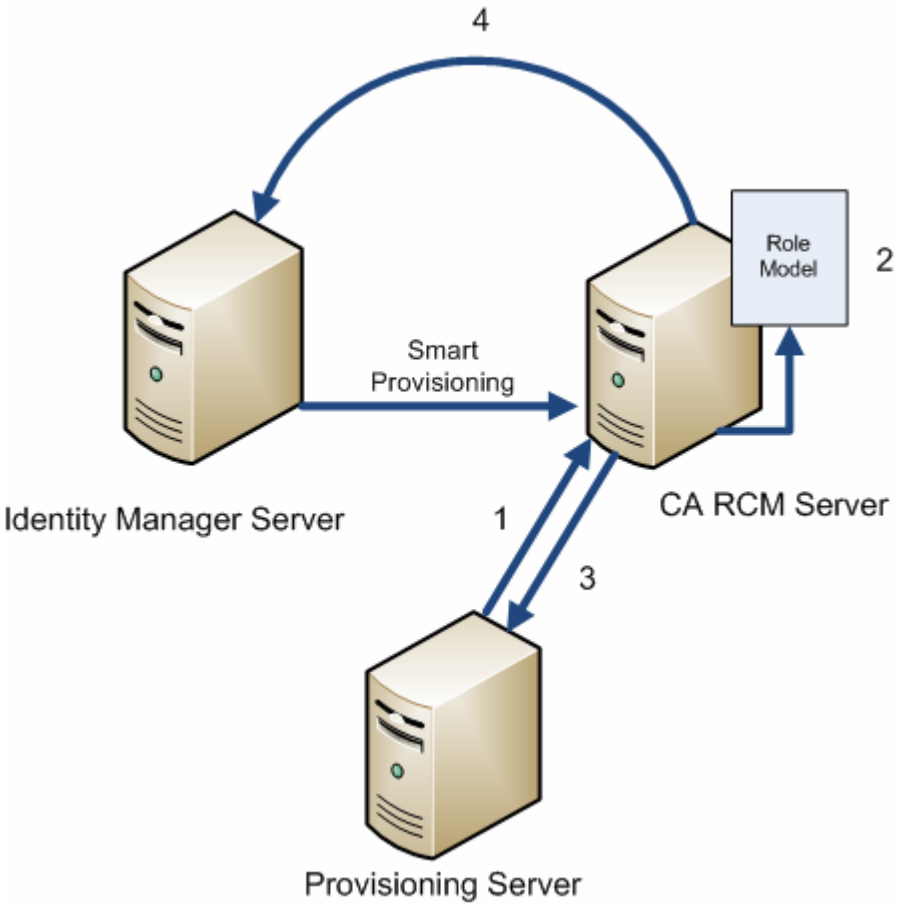
   - プロビジョン ロールおよびアカウント テンプレートの作成、変更、または作成
   - プロビジョニング ロールからのアカウント テンプレートの追加または削除
   - プロビジョニング ロールからのユーザの追加または削除

   たとえば、CA RCM は Identity Manager ロール モデルを分析し、エンドポイントにすべてのユーザが同じ権限を持つユーザの新しいグループがあることに着目します。 CA RCM は新しいアカウント テンプレートを CA Identity Manager 内の当該エンドポイント用に作成し、このアカウント プレートをプロビジョニング ロールと関連付けてユーザにプロビジョニング ロールを割り当てます。

   CA Identity Manager は、[サブミット済みタスクの表示]タスクで表示できるよう、これらの変更をタスク永続性データベースに記録します。

4. CA RCM は Task Execution Web Service (TEWS) を使用して、新しいプロビジョニング ロールのロール オーナーをリセットします。

以下の図は、通信のフローの実例を示します。



スマート プロビジョニングが有効化されていると、さまざまなプロセスが(上記のプロセスに加えて)発生します。

1. Identity Manager 管理者がユーザの作成または変更やプロビジョニング ロールの割り当てを行う場合、管理者はサジェストされたロールのリストを要求するか、変更がコンプライアンスまたはパターンに違反していないか検証します。
2. CA Identity Manager は CA RCM サーバに要求を送ります。
3. CA RCM サーバは既存のモデル ロールに対して要求を評価し、サジェストされたロールのリスト、あるいはコンプライアンスまたは検証メッセージを CA Identity Manager に返します。

共有情報

CA Identity Manager および CA RCM の統合に際し、以下の情報が 2 つのシステム間で共有されます。

- ユーザ情報
- ロール情報
- リソース情報

以下の表では、システム内の情報が、もう一方のシステムにどのようにマッピングされるかを説明します。

CA RCM オブジェクト	Identity Manager オブジェクト
[ユーザ]	[ユーザ]
ロール	プロビジョニング ロール アカウント テンプレート
リソース	エンドポイント機能。たとえば、 ■ Active Directory グループ ■ SAP プロファイル ■ Oracle テーブル所有権
ユーザ-ロール リンク	プロビジョニング ロール内のユーザ メンバシップ
ロール-ロール リンク	プロビジョニング ロール アカウント テンプレート **注**: CA RCM のロール-ロール リンクは、ネストされたプロビジョニング ロールを表す場合があります。 これらのオブジェクトは、プロビジョニング ディレクトリ内に格納されます。ただし、Identity Manager ユーザ コンソールでは非表示です。ネストされたプロビジョニング ロールを表示するには、プロビジョニング マネージャを使用します。 プロビジョニング マネージャの詳細については、「Provisioning Reference Guide」を参照してください。
ロール-リソース リンク	特定のエンドポイントでのロールおよび機能間の関係。 CA Identity Manager では、特定のエンドポイントで機能を付与するアカウント テンプレートと関連付けられているプロビジョニング ロールが、これに含まれます。
ユーザ-リソース リンク	ユーザおよび機能間の関係

動的通知

スマート プロビジョニング機能をサポートするには、CA Identity Manager で加えられた特定の変更がただちに CA RCM に渡される必要があります。 これにより、CA RCM はプロビジョニング ロール サジェストを行い、CA Identity Manager からの別のインポートを待って情報を更新する代わりに現在の Identity Manager 情報に基づきコンプライアンス ポリシーおよびパターンに対して変更を検証できます。

以下のイベントが発生した場合、CA Identity Manager は CA RCM に動的な通知を行います。

- プロビジョン ロールの作成、変更、または作成

  重要: CA Identity Manager がプロビジョニング ロールの作成または変更に関する情報を渡すと、CA RCM 内に「プレースホルダ」ロールが作成されます。 このプレースホルダ ロールは CA RCM を有効にして、どのユーザがこれらのロールを持っているかを追跡します。 ただし CA Identity Manager は、プロビジョニング ロールに関連するアカウント テンプレートへの変更、またはロールのアカウント テンプレートの詳細への変更は渡しません。

- ユーザの作成または削除
- プロビジョニング ロール メンバシップの割り当てまたは削除

これらの動的通知は、Identity Manager 環境に CA RCM へのアクティブな接続がある場合に自動的に発生します。 追加設定は必要ありません。

詳細情報:

動的通知の間隔の調整 (240 ページ)

CA RCM ロール モデル

CA RCM ロール モデルは、ロール エンジニアによる CA RCM 分析とその他の入力の結果である組織のロールのセットです。 ロール モデルが完成すると、組織のロールに適用され、ロール構造の保守に使用されます。

CA RCM との統合を設定する方法

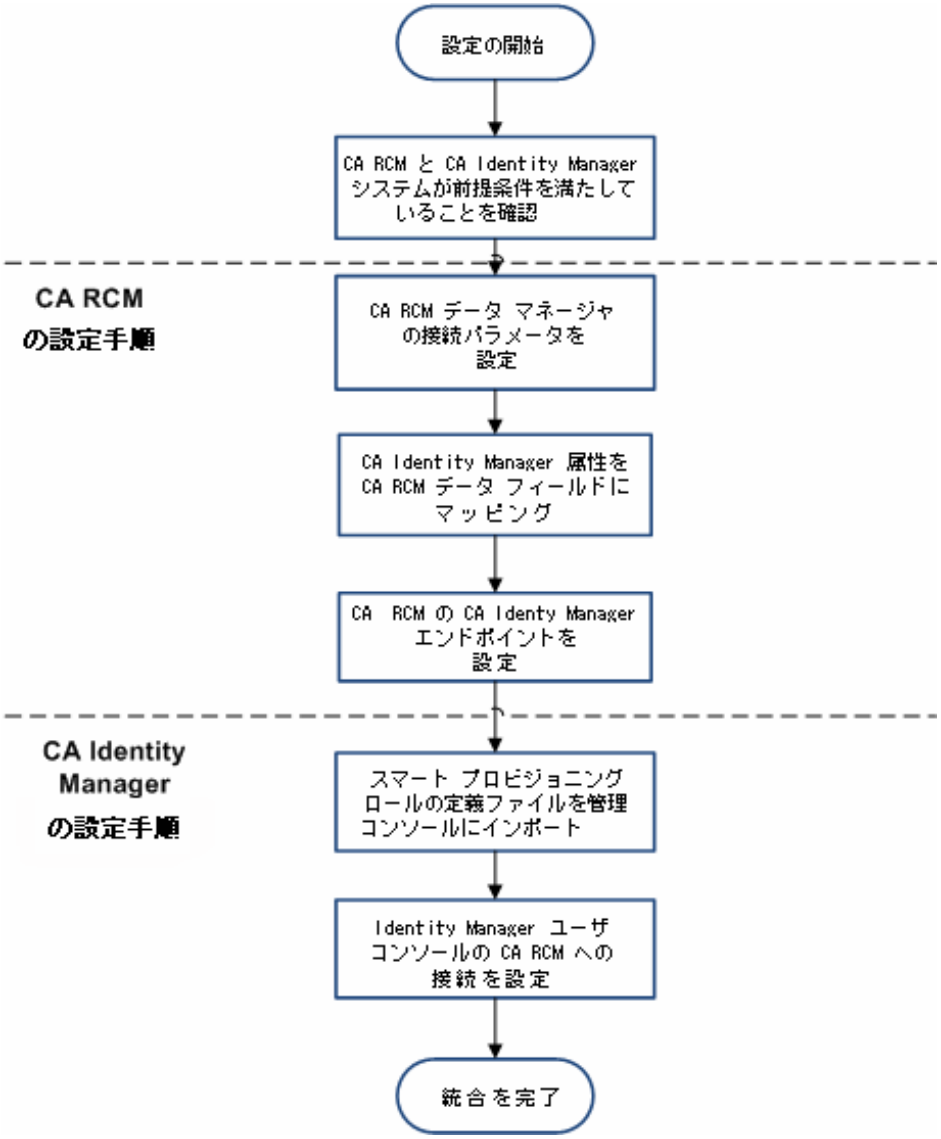
以下の高度な手順は、CA RCM との統合を設定する場合に実行する必要があります。

1. CA RCM と CA Identity Manager をホストするシステムが 設定の要件 (221 ページ) を満たしていることを確認します。
2. CA RCM で、以下の手順を実行します。
   a. CA RCM Data Manager の接続パラメータを設定します。
   b. クライアント ツールにインストールされている defaultMapping.xml ファイル内の CA RCM のデータ フィールドに、CA Identity Manager 属性をマッピングします。
   c. CA RCM にインポートされている Identity Manager エンドポイントと、それらのエンドポイントのリソースの処理方法を定義します。
3. CA Identity Manager で、以下の手順を実行します。
   a. スマート プロビジョニング ロールの定義を管理コンソールにインポートして、Identity Manager 環境への CA RCM 統合に対するサポートを追加します。

      注: スマート プロビジョニング ロールの定義には、ユーザ コンソールの CA RCM への接続を設定するために使用するタスクが含まれます。 スマート プロビジョニングの機能を使用する予定がない場合でも、これらのロール定義をインポートしておきます。
   b. CA RCM への接続を設定し、Identity Manager ユーザ コンソールで CA Identity Manager 属性を CA RCM 属性にマッピングします。
   c. (オプション) サジェストされたプロビジョニング ロール、コンプライアンスとパターンのメッセージなどのスマート プロビジョニング機能を設定します。

CA Identity Manager と CA RCM の統合を設定すると、Identity Manager データを CA RCM にインポートしてロール モデルを作成できます。 ロール エンジニアは、モデルを変更し望ましいロール構造を反映させ、そのモデルを CA Identity Manager にエクスポートします。 モデルが適用された CA Identity Manager は、必要に応じてロール定義とメンバシップを変更します。

以下のフローチャートでは、CA Identity Manager と CA RCM の統合を設定するために必要な手順を示します。



詳細情報:

CA RCM で接続を設定する方法 (221 ページ)
CA Identity Manager で接続を設定する方法 (236 ページ)
[サジェストされたプロビジョニング ロール]のデフォルト設定 (254 ページ)
コンプライアンスおよびパターン メッセージ サポートの設定方法 (263 ページ)

CA RCM 統合の前提条件

CA RCM への接続を設定するには、以下の前提条件が満たされていることを確認します。

- CA RCM が、CA Identity Manager と通信できるシステムにインストールされている必要があります。
- CA Identity Manager のコネクタが、CA RCM クライアント ツール インストーラを使用してインストールされている必要があります。

  注: 詳細については、CA RCM ブックシェルフの CA RCM Connector for CA Identity Manager のマニュアルを参照してください。
- CA Identity Manager と CA RCM の間の接続を保護する場合、両方のシステムで SSL がサポートされるように設定します。

CA RCM で接続を設定する方法

CA RCM は CA Identity Manager 用のコネクタを使用して CA Identity Manager と通信します。 コネクタを使用する前に、ユーザは接続情報を提供し、Identity Manager 属性を CA RCM データ フィールドにマッピングし、管理対象とするエンドポイントを設定します。

CA Identity Manager 用の接続パラメータの設定

コネクタは CA Identity Manager と通信してデータを交換します。 CA RCM がこの接続を確立するのに必要なネットワーク アドレスおよびログイン情報を含むファイルを作成します。

CA Identity Manager 用の接続パラメータを設定する方法

4. CA RCM Data Management を実行します。
5. [インポート]をクリックして、Identity Manager からインポートします。

   接続ウィンドウが表示されます。
6. [接続詳細]セクションで[開く]をクリックし、接続設定ファイルを選択します。

   注: defaultSettings.xml ファイルには標準的なデフォルト設定が含まれます。 defaultSettings.xml をコピーして名前を変更し、これらのデフォルトをカスタマイズ済みファイルのベースとして使用します。
7. [接続詳細]セクションで[編集]をクリックします。

   [CA Connection Settings]ウィンドウが表示されます。

8. ダイアログ ボックスで以下のフィールドを完了します。

サーバ アドレス

プロビジョニング サーバの IP アドレスまたはホスト名を定義します。

サーバ ポート

プロビジョニング サーバがセキュリティ保護されていない通信を待機するポートを定義します。

サーバ セキュア ポート

プロビジョニング サーバがセキュリティ保護されていない通信を待機するポートを定義します。［Use Secure Connection］チェックボックスを選択して、このフィールドを有効にします。

ドメイン名

プロビジョニング サーバのドメイン名を定義します。

ユーザ名

コネクタがプロビジョニング サーバへのログインに使用するユーザの名前を定義します。

パスワード

コネクタがプロビジョニング サーバへのログインに使用するパスワードを定義します。パスワードは設定 XML ファイルに保存されないため、コネクタ ジョブの実行またはスケジュールのたびに入力する必要があります。

セキュア接続を使用

サーバ ポートの代わりにサーバ セキュア ポートを使用するよう指定します。

TEWS 接続を使用

CA Identity Manager の使用を指定し、TEWS 接続詳細を設定します。

注: TEWS 接続は、エクスポート設定の CA Identity Manager への変更のみに使用されます。

Identity Manager サーバ アドレス

Identity Manager サーバ IP アドレスまたはホスト名を指定します。

Identity Manager サーバ ポート

Identity Manager サーバが待機するポート番号を指定します。

Identity Manager ユーザ名

Identity Manager パブリック ユーザの識別名を指定します。

Identity Manager ユーザ環境

接続先である Identity Manager 内の環境の名前を指定します。

9. [保存]をクリックします。

   ファイルに変更が保存されました。

10. 接続設定をテストするには、[Initiate Connection to the server]をクリックします。

    [Test Connection succeeded]ラベルが緑色にハイライトされると、ターゲットの Identity Manager 動作環境への接続に成功したことを示します。

フィールド マッピングの設定

この手順に従って、コネクタが CA Identity Manager および CA RCM データ構造間のデータ フィールドをどのようにマッピングするかを定義します。

フィールド マッピングを設定する方法

1. CA RCM クライアント ツールをホストしているコンピュータ上で、以下のディレクトリを表示します。

   RCM_install\Client Tools\Software\Converters\CA\conf

   注: RCM_install は、CA RCM のインストール ディレクトリにあります。

2. 編集するマッピング設定ファイルを開きます。

   注: defaultMapping.xml ファイルには標準的なデフォルト設定が含まれます。defaultMapping.xml ファイルをコピーして名前を変更し、これらのデフォルトをカスタマイズ済みファイルのベースとして使用します。あるいは、カスタマイズ済みファイルがすでに作成されている場合は、そのファイルを開きます。

   ファイルは、CA RCM ユーザ、ロール、およびリソース データ レコード内のフィールドを Identity Manager フィールドにマッピングします。 以下のエレメントおよび属性がファイル内で使用されます。

   KEYn

   CA RCM データ レコードの必須フィールドを示します。 このフィールドに Identity Manager フィールドをマッピングする必要があります。

   FIELDn

   CA RCM データ レコードのオプション フィールドを示します。 場合によっては、このフィールドのマッピングは行いません。 たとえば、コネクタのスコープ内のすべてのエンドポイントに共通するパラレル Identity Manager フィールドが存在しない場合は、フィールドをマッピングできない可能性があります。

   host

   コネクタの動作に使用される CA RCM ユニバース設定内のフィールドを定義します。

   guest

   Identity Manager 動作環境のフィールドを定義します。

3. デフォルトのマッピングを編集します。

   注: ファイルの <USERS_MAPPING> エレメントのみを編集します。 ファイル内の他のエレメントは編集しないでください。

   - フィールドのマッピングを変更するには、KEY または FIELD エレメントのゲスト属性用に新しい値を入力します。
   - 新しいフィールド マッピングを追加するには、新しい FIELD エレメントを作成して番号を付け、ホスト および ゲスト 属性を割り当てます。
   - フィールド マッピングを削除するには、対応する FIELD エレメントを削除します。

4. ファイルに加えた変更を保存します。

エンドポイントとリソースの選択

CA Identity Manager は、エンタープライズ環境で多くのプロビジョニング エンドポイントと相互作用します。 コネクタの範囲に含めるエンドポイント、および各エンドポイント内の関連するユーザ、ロール、およびリソース情報を定義します。

エンドポイントの選択は、コネクタのインストール ルート ディレクトリの下にある xml ファイルに保存されます。

エンドポイントとリソースの選択方法

1. CA RCM クライアント ツールをホストするコンピュータで、ディレクトリを参照します。

   RCM_install\Client Tools\Software\Converters\CA\conf

   注: RCM_install は、CA RCM のインストール ディレクトリにあります。

2. endpointTypeMapping.xml ファイルを編集します。

   カスタマイズ可能なコネクタを使用してエンドポイントを定義する方法

   a. <!-- and --> で示される xml コメントを削除して、含めたいエンドポイントに対応する endpointtype エレメントをアクティブ化します。

      注: 完全に新規の endpointtype エレメントを作成するには、既存のエレメントをコピーします。

   b. xml 属性と子エレメントを編集して、コネクタに含めるエンドポイント タイプ、エンドポイント、およびリソースを反映させます。

   c. コネクタに含める各エンドポイント タイプで、このプロセスを繰り返します。

   事前定義済みの従来のエンドポイントを使用するには、<!-- and --> で示される xml コメントを削除して、含めたいエンドポイント タイプに対応する endpointtype エレメントをアクティブ化します。

3. ファイルに変更を加えます。

例: 2 つの種類のエンドポイント ハンドラ

デフォルトの endpointTypeMapping.xml ファイルの以下のコード スニペットは、ファイルに含まれる 2 つの種類の endpointtype エレメントを示します。

- カスタマイズ可能なコネクタ テンプレート - 最初の endpointtype エレメントは設定可能です。 xml エレメントを編集し、ターゲットの Identity Manager データ ツリーから属性値を割り当てて、コネクタに含まれるエンドポイントとリソースを定義します。
- 事前定義済みの従来のエンドポイント指定 - 2 つ目の endpointtype エレメントは、ハードコードされた Java ベースのエンドポイント ハンドラを参照します。 コネクタに含まれるエンドポイントとリソースは変更できません。 この xml エレメントは、カスタマイズできるエレメントより短くなります。

```
<endpointtype name="Windows NT"
    handler="com.eurekify.connectors.ca.subconnectors.cst.CustomizableNsHandler"
    abbreviation="N16" default-policy-name="N16DefaultPolicy"
    policy-class="eTN16Policy" policy-name-attribute="eTN16PolicyName"
    policy-container-name-attribute="eTN16PolicyContainerName"
    policy-container-name="Windows NT Policies"
    >
    <endpoint name="*" fetch-policy="TRYFETCH"
        directory-class="eTN16Directory"
        directory-name-attribute="eTN16DirectoryName"
        account-class="eTN16Account"
        account-name-attribute="eTN16AccountName"
        default-policy-name="N16DefaultPolicy"
        ignore-problematic-policies="true"
        ignore-problematic-accounts="true"
        ignore-problematic-resource-types="true"
        >
        <resource description="NT Group"
        resource-class="eTN16Group"
        resource-name-attribute="eTN16GroupName"
        resource-referenced-attribute="eTN16GroupName"
        resource-appears-in-attribute="eTN16GroupMembers"
        ignore-problematic-resources="true">
        </resource>
    </endpoint>
</endpointtype>
<endpointtype name="Windows NT"
    handler="com.eurekify.connectors.ca.subconnectors.n16.NtNsHandler">
    <endpoint name="*" fetch-policy="TRYFETCH"/>
</endpointtype>
```

詳細情報:

カスタマイズ可能なコネクタ テンプレート(226 ページ)

カスタマイズ可能なコネクタ テンプレート

カスタマイズ可能なコネクタ テンプレートは xml データ構造を使用して、コネクタのスコープに含めるエンドポイント、および各エンドポイントの関連ユーザ、ロール、リソース情報を指定します。 ターゲットの Identity Manager データ ツリーの値をこのテンプレートに入力することにより、コネクタがどのエンドポイントおよびリソースのポーリングまたは更新を行うかを定義できます。

例: 含まれるエンドポイントの定義

endopintTypeMapping.xml ファイルの以下のコード スニペットは、タイプ OS400 のエンドポイント用に含まれるリソースを定義します。 エンドポイント マッピング ファイルには通常、コネクタのスコープ内で指定するエンドポイント タイプごとに 1 つずつ、この例のように複数の <endpointtype> 宣言が含まれます。

<endpoint> 子エレメントで含めることができるのは、一部のタイプの特定のエンドポイント インスタンスのみです。 同様に、<resource> 子エレメントで含めることができるのは、特定のアカウントおよび親エンドポイントからのリソース データのみです。

```
<endpointtype
        name="OS400"
        handler="com.eurekify.connectors.ca.subconnectors.cst.CustomizableNsHandler"
        abbreviation="AS4" default-policy-name="OS400DefaultPolicy"
        policy-class="eTAS4Policy" policy-name-attribute="eTAS4PolicyName"
        policy-container-name-attribute="eTAS4PolicyContainerName"
        policy-container-name="OS400 Policies"
        >
        <endpoint
                name="*"
                fetch-policy="TRYFETCH"
                directory-class="eTAS4Directory"
                directory-name-attribute="eTAS4DirectoryName"
                account-class="eTAS4Account"
                account-name-attribute="eTAS4UserProfileName"
                default-policy-name="OS400DefaultPolicy"
                ignore-problematic-policies="true"
                ignore-problematic-accounts="true"
                ignore-problematic-resource-types="true"
                >
                <resource
                 description="OS400 Group"
                 resource-class="eTAS4Group"
                 resource-name-attribute="eTAS4GroupName"
                 resource-referenced-attribute="eTAS4AccountMembers"
                 resource-appears-in-attribute="eTAS4GroupMembers"
                 ignore-problematic-resources="true">
                </resource>
        </endpoint>
</endpointtype>
```

EndpointType エレメント—コネクタ内の Identity Manager エンドポイント タイプを含める

EndpointType エレメントは、コネクタ ジョブに含まれる Identity Manager データ ツリーのエンドポイント タイプを定義します。 このエレメントには子エレメントが含まれ、指定されたエンドポイント タイプ内のエンドポイントおよびリソースの詳細な選択ができます。

CA RCM から CA Identity Manager にエクスポートされたデータには、Identity Manager エンドポイント上での新しいアカウント テンプレート作成を含めることができます。 このエレメントは、新しいアカウント テンプレートが基づいているポリシー クラスも定義します。Identity Manager データ構造がこれらのポリシーをエンドポイントタイプ レベルで格納するためです。

このエレメントの構文は、以下のようになります。

```
<endpointtype
    name="name"
    handler="com.eurekify.connectors.ca.subconnectors.cst.CustomizableNsHandler"
    abbreviation="abbreviation"
    default-policy-name="default-policy-name"
    policy-class="policy-class"
    policy-name-attribute="policy-name-attribute"
    policy-container-name-attribute="policy-container-name-attribute"
    policy-container-name="policy-container-name"
    >
    <endpoint>
    ...
    <endpoint>
</endpointtype>
```

このエレメントには、以下の属性および子エレメントが含まれます。

name

CA Identity Manager で定義されている通り、含めたいエンドポイント タイプを定義します。

handler

エンドポイント タイプ定義の処理を行う java ハンドラを定義します。 この値は変更しないでください。

abbreviation

CA Identity Manager 内にあるこのエンドポイント タイプに割り当てられる 3 文字の略記を定義します。

default-policy-name

新しいアカウント テンプレートが作成される際にデフォルト設定が使用される、アカウント テンプレート名を定義します。

policy-class

［default-policy-name］フィールドで定義されたデフォルトのアカウント テンプレートのオブジェクト クラスを定義します。

policy-container-name-attribute

DN 名を示すポリシー コンテナの属性を定義します。

policy-container-name

このエンドポイント タイプのポリシー コンテナの名前を定義します。

endpoint

EndpointType エレメントには、endpoint エレメントを子エレメントとして、いくつでも含めることができます。 これらのエレメントにより、含まれるエンドポイントおよびリソース ノードの詳細な指定が可能です。

Endpoint エレメント—コネクタに Identity Manager エンドポイントを含める

Endpoint エレメントは、コネクタ ジョブに含まれる Identity Manager データ ツリーのエンドポイントを定義します。

エンドポイント タイプを指定してから、エンドポイントをコネクタに割り当てる必要があります。 これは xml 構造に反映されており、endpoint エレメントは endpointtype エレメントの子エレメントとしてのみ表示されます。

Endpoint エレメントには子エレメントが含まれ、指定されたエンドポイント内のデータ リソースを詳細に定義できます。

このエレメントの構文は、以下のようになります。

```
<endpoint
    name="name"
    fetch-policy="fetch-policy"
    directory-class="directory-class"
    directory-name-attribute="directory-name-attribute"
    account-class="account-class"
    account-name-attribute="account-name-attribute"
    default-policy-name="default-policy-name"
    ignore-problematic-policies="ignore-problematic-policies"
    ignore-problematic-accounts="ignore-problematic-accounts"
    ignore-problematic-resource-types="ignore-problematic-resource-types"
    >
    <Resource>
    ...
    <Resource>
</endpoint>
```

このエレメントには、以下の属性および子エレメントが含まれます。

name

CA Identity Manager で定義されている通り、含めたいエンドポイントを定義します。 ワイルドカード * を使用して、エンドポイント タイプのすべてのエンドポイントを含めます。

fetch-policy

エンドポイント データを取得できなかった場合の、コネクタの動作を指定します。 有効な値は以下のとおりです。

- TRYFETCH–このエンド ポイントが失敗した場合、コネクタ ジョブを継続します。
- FORCEFETCH–このエンドポイントが失敗した場合、すべてのコネクタ ジョブを中止します。

directory-class

プロビジョニング ディレクトリ内でエンドポイントのオブジェクト クラスを定義します。

directory-name-attribute

エンドポイントの DN 名を示す属性の名前を定義します。

account-class

プロビジョニング ディレクトリ内で、このエンドポイントのアカウントのオブジェクト クラスを定義します。

account-name-attribute

アカウントの DN 名を示す属性の名前を定義します。

default-policy-name

ユーザアカウントの作成に使用されるアカウント テンプレートの名前を定義します。

ignore-problematic-policies

含まれるアカウント テンプレートを取得できなかった場合の、データ ポーリングの行動を指定します。 有効な値は以下のとおりです。

- true—コネクタ ジョブは継続されます
- false—コネクタ ジョブは中止されます

ignore-problematic-accounts

含まれるアカウントを取得できなかった場合の、データ ポーリングの行動を指定します。有効な値は以下の通りです。

- true—コネクタ ジョブは継続されます
- false—コネクタ ジョブは中止されます

ignore-problematic-resource-types

含まれるリソース タイプを取得できなかった場合の、データ ポーリングの行動を指定します。有効な値は以下の通りです。

- true—コネクタ ジョブは継続されます
- false—コネクタ ジョブは中止されます

resource

Endpoint エレメントには、resource エレメントを子エレメントとして、いくつでも含めることができます。 これらのエレメントにより、含まれるリソース ノードの詳細な指定が可能です。

resource エレメント—コネクタに Identity Manager を含める

Resource エレメントは、コネクタ ジョブに含まれるエンドポイント情報のタイプを定義します。 リソースの定義は、Identity Manager データ ツリー内で明示的に宣言されるエンドポイント特有です。 エンドポイントを指定してから、リソースをコネクタに割り当てる必要があります。 これは xml 構造に反映されており、resource エレメントは endpoint エレメントの子エレメントとしてのみ表示されます。

CA RCM がエンドポイントのポーリングを行うと、通常はコネクタ定義内の単一の resource エレメントが CA RCM で一連の新しいリソース エンティティを生成します。

CA RCM がエンドポイントを更新すると、コネクタのフィールド マッピングは、更新されたリソース データがエンドポイント上のユーザ アカウントをどのように変更するかを決定します。

このエレメントの構文は、以下のようになります。

```
<resource
    description="description"
    resource-class="resource-class"
    resource-name-attribute="resource-name-attribute"
    resource-referenced-attribute="resource-referenced-attribute"
    resource-appears-in-attribute="resource-appears-in-attribute"
    ignore-problematic-resources="ignore-problematic-resources"
    >
    <value name="name" />
    ...
    <value />
    <constant-link value="value" />
    <replace-in-links pattern="pattern" new-value="new-value" />
</resource>
```

このエレメントには、以下の属性および子エレメントが含まれます。

説明

このリソース定義に基づく新しい CA RCM リソース レコードの[res_name_3]フィールドにマッピングされるテキストを定義します。

resource-class

プロビジョニング ディレクトリ内で、このリソース タイプを表すオブジェクト クラスを定義します。

resource-name-attribute

リソースの DN を示すオブジェクト クラスの属性を定義します。

resource-referenced-attribute

リソース オブジェクトのタイプを参照するのに使用されるアカウント オブジェクトの属性を定義します。この属性は、リソースがどのようにユーザ アカウントに割り当てられるかを定義します。

resource-appears-in-attribute

このオブジェクトへの参照を含むアカウント オブジェクトの属性を定義します。 この属性は、リソースがどのようにユーザ アカウントに割り当てられるかを定義します。

ignore-problematic-resources

含まれるデータ リソースを取得できなかった場合の、データ ポーリングの行動を指定します。有効な値は以下の通りです。

- true—コネクタ ジョブは継続されます
- false—コネクタ ジョブは中止されます

重要: 以下の詳細パラメータについては、お客様による変更はしないでください。 テクニカル サポートの詳細については、当社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

resource-type

リソースのタイプを指定します。 有効な値は以下のとおりです。

- LDAP_OBJECT
- CONSTANT_LIST–value エレメントのリストを要求します。

value

コネクタに含める特定の名前のリソースを定義します。 この子エレメントはリソースタイプ属性と共に使用され、リソースの固定リストを定義します。

constant-link

各アカウントに自動的に追加された特定のリソースへの参照を定義します。

replace-in-links

アカウントに書き込まれたリソース DN 参照内の文字列の自動置換を定義します。

resource-reference-level

リソース参照に含めるプロビジョニング ツリー内のレベル数を定義します。

Active Directory 用のコネクタ

以下の問題は、Active Directory へのコネクタの使用に当てはまります。

- CA RCM アカウント テンプレートの処理は、AD アカウント ポリシーあるいは AD コントラクト ポリシーに基づく必要があります。

  コネクタがポーリングおよび更新できるのは、これらのポリシー タイプのうち 1 つのみです。

- アカウント テンプレートの参照先エンドポイントは 1 つのみである必要があります。

- データのエクスポート中、監査カード内において、変更エントリによってはコネクタによるパーサが正しく行われません。
- コネクタを設定する際、エクスポートされるデータ タイプそれぞれに DN フィールドを割り当てる必要があります。
- データ取得中、コネクタが非標準 CSV ファイルを生成する場合があります。 この状況を正すには、エンドポイント マッピング xml ファイルを編集します。

  1. CA RCM クライアント ツールをホストしているコンピュータ上で、以下のディレクトリを表示します。

     RCM_install¥Client Tools¥Software¥Converters¥CA¥conf

     注: RCM_install は CA RCM インストール ディレクトリです。

  2. endpointTypeMapping.xml ファイルを以下のように編集します。

     a. Active Directory エンドポイント タイプで、Active Directory Group と言う名前の resource エレメントを検索します。

     b. 以下の例に示されるように、constant-link および replace-in-links エレメントの値を変更します。

例: Active Directory コネクタ用に更新された EndpointTypeMapping.xml

以下の例では、エンドポイント マッピング ファイルを更新して、Active Directory コネクタがデータ取得中に非標準 CSV ファイルを生成しないようにする方法を示します。

```
<resource description="Active Directory Group"
        resource-class="eTADSGroup"
        resource-name-attribute="eTADSGroupName"
        resource-referenced-attribute="eTADSdistinguishedName"
        resource-appears-in-attribute="eTADSmemberOf"
        friendly-name-transformation="FIRST_DN_PART"
        ignore-problematic-resources="true">
        <constant-link
        value="CN=Cert Publishers,CN=Users,DC=eurekify,DC=corp"/>
        <replace-in-links
        pattern="DC=\?"
        new-value="DC=eurekify,DC=corp"/>
</resource>
```

コネクタ設定の CA RCM サーバへのコピー

コネクタ設定ファイルを CA RCM サーバ インストール ディレクトリにコピーして、CA RCM ポータルからのコネクタ ジョブを実行します。 これにより、ユーザはポータルの詳細なスケジュール ツールを使用し、取得したデータ ディレクトリをアクティブな設定に統合できます。

- CA RCM サーバをインストール済みでクライアント アプリケーションが別のコンピュータ上にある場合、ファイルをクライアント コンピュータからサーバ コンピュータにコピーします。
- すべての CA RCM アプリケーションを単一のコンピュータにインストールした場合、ファイルをこのコンピュータ上のディレクトリ間でコピーします。

コネクタ設定の CA RCM サーバへのコピー方法

1. CA RCM サーバ上で、以下のディレクトリに移動します。

   RCM install/Server

   注: RCM_install は、CA RCM のインストール ディレクトリにあります。

   CA RCM サーバが WebSphere/AIX 環境にある場合、このディレクトリを CA RCM クラスタ内のすべてのサービスにアクセスできる共有リソースとして作成します。

2. Connectors という名前のサブディレクトリを作成します。

   注: 他のコネクタを設定済みの場合、このディレクトリはすでに存在します。

3. クライアント ツールをホストしているコンピュータ上で、以下のディレクトリに移動します。

   RCM_install\Client Tools\Software\Converters\

4. ¥CA サブフォルダ全体を、このディレクトリから CA RCM サーバ上で作成した ¥Connectors ディレクトリにコピーします。

5. (オプション) 以下のタスクの 1 つを動作環境で実行します。

   - (JBoss クラスタ) この手順を、クラスタ内のすべてのサーバで繰り返します。
   - (WebSphere/AIX) 管理者として CA RCM ポータルにログインし、以下のシステム プロパティを編集します。
     - sage.v32.connecters.workingDirectory—コネクタ処理中にテンポラリ ファイル用に使用されるディレクトリを定義します。 すべてのサーバが、このディレクトリを読み取り/書き込みできる必要があります。
     - sage.v32.connecters.CAConnectorHomeDir—ユーザにより作成された ¥Connectors¥CA¥bin ディレクトリのパス名を定義します。

CA Identity Manager で接続を設定する方法

CA RCM で接続情報を設定した後、CA Identity Manager で追加設定情報を設定します。

CA Identity Manager から CA RCM への接続を設定するための高度なレベルの手順を以下に説明します。

1. 統合サポートを Identity Manager 環境に追加します。
2. Identity Manager ユーザ コンソールで接続情報を設定します。
3. CA Identity Manager 属性を CA RCM データ フィールドにマッピングします。

統合サポートの Identity Manager 環境への追加

CA Identity Manager を設定して CA RCM と合わせて作動させるには、Identity Manager 環境に一連のロールおよびタスク定義を追加します。

ロールおよびタスク定義のインポート方法

1. 管理コンソールで、[環境]をクリックします。

   Identity Manager 環境のリストが表示されます。

2. ロールおよびタスク設定のインポート先となる Identity Manager 環境の名前をクリックします。

   この環境のプロパティ画面が表示されます。

3. [ロールおよびタスクの設定]をクリックし、[インポート]をクリックします。

4. スマート プロビジョニング ロール定義ファイルを選択して、環境用にデフォルトのロールおよびタスクを作成します。

   注: スマート プロビジョニング ロール定義ファイルには、ユーザ コンソール内の CA RCM への接続設定に使用するタスクが含まれます。 スマート プロビジョニング機能を使用しない場合でも、このファイルをインポートしてください。

5. [完了]をクリックします。

   [Role Configuration Output]ウィンドウにステータスが表示されます。

6. [続行]をクリックして終了します。

CA Identity Manager の接続の設定

CA RCM への接続を設定して、以下のスマート プロビジョニング機能を有効にします。

- サジェスト ロールのサポート
- パターン外メッセージ
- コンプライアンス外メッセージ
- CA RCM ロール モデルへの動的アップデート

注: スマート プロビジョニング機能とユーザ コンソールの設定オプションを表示するには、CA RCM への接続を設定する必要があります。

接続を設定する手順の中で、CA RCM 属性を CA Identity Manager 属性にマッピングします。 マッピングにより、CA RCM と CA Identity Manager は情報を共有できるようになります。

CA RCM への接続を設定する方法

1. システム管理権限を持つユーザとしてユーザ コンソールにログインします。
2. [システム]タブを選択します。
3. [CA RCM 接続管理]-[Configure an RCM Connection]を選択します。

   注: CA RCM への接続の作成に、ユーザ コンソール内の他の接続タスクは使用しないでください。

   接続情報を入力できる画面が開きます。
4. CA RCM が実行されているシステムに関する以下の情報を入力します。

   ホスト

   CA RCM がインストールされているシステムの完全修飾名または IP アドレス。

   ポート

   CA RCM のポート番号。

［ユーザ ID］

CA RCM へのアクセス権を持つアカウントの名前。

［パスワード］

［ユーザ ID］フィールドに指定されたアカウントのパスワード。

セキュア接続（HTTPS）

CA Identity Manager と CA RCM の間の HTTPS 接続を有効にします。

注： CA Identity Manager と CA RCM の間の接続をセキュリティ保護するには、SSL を設定する必要があります。

5. CA RCM に関する以下の情報を入力します。

設定

CA Identity Manager の通信対象である CA RCM における設定の名前。

ユニバース

CA Identity Manager の通信対象である CA RCM におけるユニバースの名前。

ユニバースは、CA Identity Manager から収集されたデータを含む、CA RCM における仮想の場所です。

注： CA RCM ポータルで、ユニバースと設定を作成します。 詳細については、「CA Role & Compliance Manager Portal User Guide」を参照してください。

6. ［テスト接続］をクリックして、CA Identity Manager から CA RCM に接続できることを確認します。

CA Identity Manager の画面上部に、接続ステータスが表示されます。

7. 以下のように CA RCM 属性を CA Identity Manager 属性にマッピングします。

   a. [属性マッピング ファイルのアップロード]フィールドで、CA RCM ホスト システムの user-mapping.properties ファイルを参照します。

      注: user-mapping.properties ファイルは、ユーザ コンソールが実行されているブラウザからアクセスできるシステムに配置する必要があります。 ブラウザが CA RCM とは異なるシステムで実行されている場合、CA RCM を参照する共有を作成するか、ブラウザが動作しているシステムにマッピング ファイルをコピーします。

      user-mapping.properties ファイルは、CA RCM クライアント ツールがインストールされているサーバ上の C:¥Program Files¥CA¥RCM¥Client Tools¥Software¥Converters¥Identity Manager¥conf に配置されています。

   b. [アップロード]をクリックします。

      CA Identity Manager に、プロパティ ファイルで定義されたマッピングが含まれる[CA RCM 属性マッピング]テーブルが読み込まれます。

8. [完了]をクリックします。

   これで、CA Identity Manager は CA RCM と正常に通信できます。

CA RCM 属性マッピングの変更

CA RCM への接続を設定する際に、CA RCM の属性を CA Identity Manager の属性にマップします。 CA Identity Manager にあるこれらのマッピングを定義するには、user-mapping.properties ファイルを CA RCM からアップロードします。

初期設定の後は、必要に応じてマッピングを変更できます。

属性マッピングの追加方法

1. システム管理権限を持つユーザとしてユーザ コンソールにログインします。
2. [システム]タブを選択します。
3. [CA RCM 接続管理]-[Configure an RCM Connection]を選択します。

   接続情報を入力できる画面が開きます。

4. [Add Attribute Mapping]フィールドに追加する RCM 属性の名前を入力し、[追加]アイコンをクリックします。

   CA Identity Manager により、[CA RCM 属性マッピング]テーブルに属性が追加されます。

5. テーブルに追加した RCM 属性の横のテキスト ボックスで、対応する Identity Manager 属性の名前を入力します。

   属性の表示名を指定します。 表示名は、環境が作成されたときにディレクトリ設定ファイル(directory.xml)で設定されます。

6. 追加する属性マッピングごとに 4 と 5 の手順を繰り返します。
7. [送信]をクリックします。

   CA Identity Manager で、接続情報が新しい属性で更新されます。

属性マッピングの削除方法

1. システム管理権限を持つユーザとしてユーザ コンソールにログインします。
2. [システム]タブを選択します。
3. [CA RCM 接続管理]-[Configure an RCM Connection]を選択します。

   接続情報を入力できる画面が開きます。
4. 削除する属性マッピングの横にある[削除]アイコンをクリックします。

   CA Identity Manager により、[CA RCM 属性マッピング]テーブルから属性が削除されます。
5. [送信]をクリックします。

動的通知の間隔の調整

スマート プロビジョニング機能が有効化されると、CA Identity Manager から CA RCM へのインポートを待つ代わりに、CA Identity Manager はプロビジョニング ロールの変更を CA RCM に頻繁に通知します。 これらの動的通知は Web サービスを使用して送信され、CA RCM に最新の Identity Manager 情報があることを確認するのに役立ちます。

プロビジョニング ロールに変更が発生すると、CA Identity Manager は通知を生成してキューに追加します。 指定された間隔で、CA Identity Manager はキュー内のすべての情報から集約通知を作成して CA RCM に送信します。

パフォーマンスを改善するため、環境の「queue notification delay」パラメータを定義することで、CA Identity Manager が CA RCM に情報を送信する頻度を設定できます。 デフォルトでは、このパラメータは 60 秒に設定されます。

動的通知の間隔を調整する方法

1. 管理コンソールで[環境]、[Environment Name]、[詳細設定]、[その他]を開きます。

   [ユーザ定義プロパティ]ページが開きます。
2. [プロパティ]フィールドに「QueueNotificationDelay」と入力します。

3. [値]フィールドに、間隔を秒数で指定します。

   CA Identity Manager は指定された数毎に CA RCM に情報を送信します。

   注: 通知をただちに送信するには、値を 0 に設定します。 この場合、CA Identity Manager は通知がキューに入ると送信し、通知は集約通知に追加されません。

4. [追加]をクリックします。
5. 環境を再起動します。

TEWS Jar の作成方法

CA RCM は Task Execution Web Service (TEWS) を使用して、CA Identity Manager 内に作成する新しいプロビジョニング ロールのロール所有者をリセットします。

CA RCM クライアント ツールには、ほとんどの展開で利用できる TEWS jar が含まれます。 ただし、以下の Identity Manager タスクをカスタマイズした場合、WSDL に基く Java プロキシ ソース コード(.java ファイル)を以下のタスク用に作成する必要があります。

- プロビジョニング ロール所有者のリセット
- アイデンティティ ポリシー セットの作成
- アイデンティティ ポリシー セットの変更

TEWS jar の生成に関与する高度なレベルの手順を以下に説明します。

1. Web サービスのための環境を準備します(241 ページ)。
2. Apache Axis Java プロキシ クラスを作成します(242 ページ)。
3. コンパイルされたプロキシ クラスのための Java jar ファイルを作成します(242 ページ)。

Web サービスのための環境の準備

Web サービスのための環境を準備する方法

1. 管理コンソールで、Web サービスの実行および環境用 WSDL の生成を有効化します。
2. ユーザ コンソールで、以下のタスク用の Web サービスを有効化します。
   - プロビジョニング ロール所有者のリセット
   - アイデンティティ ポリシー セットの作成
   - アイデンティティ ポリシー セットの変更

注: Web サービス設定およびクライアント アプリケーション開発の詳細については、「Java のプログラミング ガイド」の Task Execution Web Service の章を参照してください。

Apache Axis Java プロキシ クラスの作成

Apache Axis フレームワークには、WSDL に基づく Java プロキシ ソース コード(.java ファイル)を生成するユーティリティ WSDL2JAVA が含まれます。 Java ファイルが生成されると、Java クラスにコンパイルされる必要があります。

WSDL2JAVA の起動時に、Identity Manager 環境用の Identity Manager WSDL URL の名前を渡します。 以下の例では、MyCorp が環境の名前です。

```
wsdl2java --timeout -1 –output genoutput http://localhost:8080/idm/TEWS6/MyCorp?wsdl
```

プロキシ Java ファイルが生成されたら、.java ファイルを .class ファイルにコンパイルします。 ンパイラ クラス パスに、必ず完全な Axis jar ファイルのセットを含めてください。

注: CA Identity Manager には AXIS 用のビルド スクリプトの Web サービス サンプルが含まれており、Java プロキシ クラスの生成およびコンパイル方法の例として使用できます。 管理ツールの samples¥WebService¥AXIS¥build.xml を参照してください。 管理ツールは、以下のデフォルトの場所に配置されます。

- Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

コンパイルされたプロキシ クラスのための Java jar ファイルの作成

CA Identity Manager のための CA RCM 接続には、Web サービスで Identity Manager タスクを起動する際に、Axis Java プロキシ クラスを使用する必要があります。 プロキシ クラスを提供するには、クラスを Java jar ファイルにコンパイルし、この jar を CA RCM サーバにコピーします。

以下は、Java jar ファイルの作成に使用できるコマンドの例です。

```
jar –c RCMTews.jar build
```

Jar ファイルの作成後、CA RCM クライアント ツールがインストールされているシステム上の以下のフォルダにコピーします。

RCM_install¥Client Tools¥Software¥Converters¥CA¥lib

CA RCM 内の CA Identity Manager データ分析

CA Identity Manager と CA RCM 間の接続が確立されると、プロビジョニング ロールに関する情報を CA RCM にインポートできます。 これで、ロール エンジニアは CA RCM のさまざまなツールを使用してデータを分析することができます。 ロール エンジニアがプロビジョニング ロール構造を決定すると、その構造に基づいて、CA Identity Manager に変更を適用することが可能です。

CA Identity Manager により管理されているエンドポイントのポーリング(インポート)および更新(エクスポート)を行うには、CA RCM ポータル内のコネクタ ジョブを定義します。これでジョブを実行するか、指定された間隔で自動的にジョブを実行するスケジュールを定義することができます。 データ強化やスケジュールのような、さまざまなオプションを適用するコネクタに基づく、複数のジョブを定義することができます。

コネクタ ジョブの定義

コネクタ ジョブを定義すると、このジョブをポータルとは個別に実行できます。または、ポータルのスケジュール機能を使用してジョブが自動的に実行されるようにできます。

CA RCM ポータルでコネクタ ジョブを定義する方法

1. 管理者として CA RCM ポータルにログインします。
2. [管理]-[設定]-[Connector Settings]をクリックします。

   [Connector Settings]画面が表示されます。
3. 以下のいずれかの操作を行います。
   - エンドポイントをポーリングするジョブを作成するには、画面の[インポート]領域の[作成]をクリックします。
   - エンドポイントを更新するジョブを作成するには、画面の[エクスポート]領域の[作成]をクリックします。

   [Create New Import]または[Create New Export]ページが表示されます。
4. ページのフィールドに入力して、新しいジョブを定義します。 以下のフィールドには、説明が必要です。

   ユニバース

   CA RCM サーバのユニバースを指定します。 取得されたエンドポイント データはこのユニバースに追加され、エンドポイントの更新はこのユニバースに基づきます。

   注: コネクタ ジョブを実行できるようにするには、ユニバースに対して明示的にログイン フィールドを指定し、このフィールドで コネクタがエンドポイント データにマッピングすることを確認(246 ページ)します。

   Enrichment Users Database

   (オプション)CA RCM で使用される既存のユーザ データベース(.udb)ファイルを定義し、データのポーリングの際に新規ユーザ レコードを準備します。

   注: ファイル名を入力しますが、.udb サフィックスは入力しないでください。 たとえば、enrich.udb ファイルを参照するには enrich と入力します。

   Ticket Type

   チケット キューのジョブの追跡に使用するチケット形式を指定します。
   - ポーリング ジョブの場合、FlowTicketforImport_V0.8 を選択します。
   - 更新ジョブの場合、FlowTicketforExport_V0.4 を選択します。

   Workflow process name

   CA RCM がコネクタ ジョブの実装に使用する Workpoint のビジネス プロセスを指定します。

- ポーリング ジョブの場合、[Import Configuration]を選択します。
- 更新ジョブの場合、[Export Master Model Deltas]を選択します。

Max duration time（秒）

ジョブの推定処理時間を定義します。 ジョブの処理時間がこの制限値を超える場合、CA RCM では、チケット キューにジョブが延滞として表示されますが、処理は継続されます。

優先度

チケット キューの他のタスクと比較した、ジョブの重要度を指定します。

重大度

チケット キューの他のタスクと比較した、ジョブの処理中に生成されたエラーの重要度を指定します。

Connector Type

CA RCM ポータルがジョブの実行に使用するアルゴリズムを指定します。

- ポーリング ジョブの場合、[External Process Import Connector]オプションを選択します。
- 更新ジョブの場合、[External Process Connector Export]オプションがデフォルトで選択されています。

Connector Java Class

コネクタで使用する Java 環境を定義します。
[CARemortSystemExternalProcessConnector]オプションを選択します。

Settings XML file

コネクタの接続設定ファイルのサーバ側コピーへのパス名を定義します。 通常、コネクタの設定時にサーバに作成した /Connectors/CA/conf ディレクトリになります。

XML ファイルのマッピング

コネクタのフィールド マッピング ファイルのサーバ側コピーへのパス名を定義します。 通常、コネクタの設定時にサーバに作成した /Connectors/CA/conf ディレクトリになります。

Remote system login password

CA RCM で使用される、ターゲットの Identity Manager インスタンスにログインするためのパスワードを定義します。 この値は暗号化され、コネクタ ジョブに保存されます。

5. [保存]をクリックします。

このジョブが保存され、[Connector Settings]ページにリストされます。

ログイン フィールドのマッピング検証

CA RCM がエンドポイント データに基づいて新規ユーザ レコードを作成する際、CA RCM ポータルのこれらのユーザのためのアカウントを自動的に作成します。 これをサポートするには、コネクタ ジョブがターゲット ユニバースのログイン フィールドに有効な値をマッピングする必要があります。

ログイン フィールドのマッピングを検証する方法

1. ターゲット ユニバースに定義済みログイン フィールドがあることを検証します。
   a. CA RCM ポータル上で[管理]、[設定]、[Universe Settings]をクリックします。

      [Universe settings]画面が表示されます。

   b. コネクタ ジョブ用に指定したユニバースを検索し、該当行の[編集]をクリックします。

      検索画面が表示されます。

   c. [設定]ログイン フィールドが、ユニバースの既存のフィールドを参照していることを検証します。 [設定]ログイン フィールドが空白の場合、フィールドまたはユニバースを選択して定義します。

   d. [設定]ログイン フィールドの名前を確認してください。
2. コネクタがログイン フィールドにデータをマッピングしていることを検証します。
   a. コネクタ ジョブ用に指定したマッピング xml ファイルを開きます。

   b. 以下の条件が含まれる、[ログイン]フィールドをマッピングする行を検索します。

      host='Login'

   c. エンドポイント データが guest= 条件内のこのフィールドにマッピングされていることを検証します。 マッピングが空白である場合、エンドポイント データ フィールドを指定して定義します。

詳細情報:

フィールド マッピングの設定 (223 ページ)

コネクタ ジョブの実行とスケジュール

事前定義済みのコネクタ ジョブを実行して、外部プロビジョニング プラットフォームとデータを交換できます。

コネクタ ジョブを実行およびスケジュールする方法

1. 管理者として CA RCM ポータルにログインします。
2. [管理]-[設定]-[Connector Settings]をクリックします。

   [Connector Settings]画面が表示されます。
3. 以下のいずれかのオプションを選択します。
   - 実行するジョブ プロファイルの横にある[実行]をクリックします。

     ジョブがただちに開始されます。
   - 今後のジョブをスケジュールするには、[スケジュール]をクリックします。

     [New Connector Scheduled Task]ダイアログ ボックスが表示されます。

     以下のフィールドに値を入力します。
     - First execution—ジョブが最初に実行される日時を指定します。
     - Number of additional repeats—ジョブを実行させる回数。 無限のシリーズを定義するには、値 -1 を入力します。
     - Repeat interval—シリーズにおける実行の間隔

     [OK]ボタンをクリックします。

     スケジュールが保存されました。 スケジュールされた時間にコネクタ ジョブが実行されます。

コネクタ ジョブを監視する方法

以下の 2 つの方法で、アクティブ コネクタ ジョブを監視できます。

- チケット キューからジョブの進行状況を追跡する。
- CA RCM サーバ ログ内でジョブ関連のメッセージを確認する。

サジェストされたプロビジョニング ロール

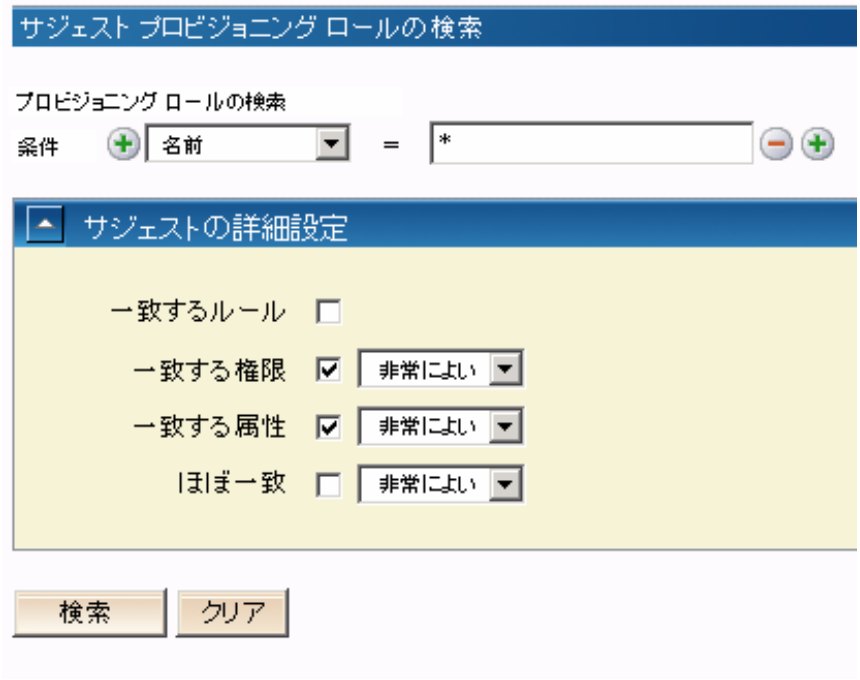
CA Identity Manager が CA RCM と統合されている場合は、管理者は、CA Identity Manager でユーザへの割り当てに適切なプロビジョニング ロールのリストを利用できます。 プロビジョニング ロールのリストは、管理者が入力した基準に基づいて、CA RCM により決定されます。

Identity Manager 環境に、CA RCM へのアクティブな接続がある場合は、[プロビジョニング ロール]タブには、以下の例に示す[サジェストされたプロビジョニング ロール]ボタンが表示されます。

管理者は、そのボタンをクリックして、ユーザに割り当て可能なロールのリストを表示できます。 また、CA Identity Manager の[プロビジョニング ロール検索画面]には、デフォルトの条件を満たすロールのリストが表示されます。 このデフォルトの条件は、管理者が最初に検索画面を設定するときに定義されます。

管理者がその他のプロビジョニング ロールを確認する場合、サジェスト機能を使用せずにこれらのロールを検索することができます。 一部の実装では、管理者は以下の画面に示す[サジェストの詳細設定]セクションを展開して、新しいサジェスト条件を指定することもできます。

注: 一部の実装では、[サジェストの詳細設定]セクションが使用できない場合があります。 システム管理者は サジェスト ロールへのサポートを設定(254 ページ)する際に、[Hide Advanced Configuration]オプションを選択して、このセクションを表示または非表示にすることができます。



新規条件を作成すると、その条件に基づいて追加のプロビジョニング ロールが返されます。管理者は、[追加]をクリックすることで、それらのロールを割り当てできます。 検索により返されたロールは、以下の条件を満たしています。

- 管理者は、選択されたユーザに対してプロビジョニング ロールを割り当てることのできる適正な権限を有している。
- それらのプロビジョニング ロールは、管理者が[検索]フィールドに入力した検索条件(ある場合)に合致している。
- プロビジョニング ロールは、少なくとも選択されたサジェストの条件のいずれかを満たしている。

サジェスト ロールの条件

CA RCM は以下の 1 つまたは複数の条件に基づき、ユーザにプロビジョニング ロールをサジェストします。

- ［一致するルール］

  現在のユーザが、CA RCM のルール ベース ロールにおけるメンバシップを決定するルールに一致する場合、CA RCM はプロビジョニング ロールをサジェストします。

  たとえば、Sales Manager ロールには「役職 = Sales Manager」という適合ルールがあるとします。 ユーザが「役職 = Sales manager」を持っているものの、Sales Manager ロールのメンバではない場合、CA RCM はこのロールをユーザにサジェストします。

- ［一致する権限］

  CA RCM は、現在のユーザが持っている権限と類似した権限を持つユーザに対し、プロビジョニング ロールをサジェストします。 権限には、アカウント、ロール、グループ メンバシップ、およびその他の権限が含まれます。

  たとえば、UNIX アカウントを持ち、企業の IT サポート データベースへアクセス可能な多くのユーザは、IT ヘルプ デスク ロールを所有しています。 CA RCM は、UNIX アカウントを持ち、IT サポート データベースへアクセス可能なすべてのユーザに対して IT ヘルプ デスク ロールをサジェストします。

  この場合、CA RCM では、以下の基準を使用して、サジェスト ロールが適切なものである可能性を決定することができます。

  - 他のユーザが持つ権限が、現在のユーザが持つ権限にどの程度一致するか
  - 一致する権限を持ち、そのロールを所有するユーザが何人いるか

- ［一致する属性］

  CA RCM は、現在のユーザが持っている属性と類似した属性を持つユーザに対し、プロビジョニング ロールをサジェストします。

  たとえば、プロファイルに以下の属性を持つ従業員に対して、管理者がロールを割り当てるとします。

  - 役職: 販売員
  - マネージャ: Bob Folchart
  - オフィス: 北東

  同じ役職、マネージャ、およびオフィスを持つユーザは、Employee ロールと Northeast Sales Associate ロールを所有しています。 CA RCM はこれらのロールの割り当てをサジェストします。

CA RCM は以下の条件を使用して、サジェスト ロールがユーザに適切かどうかを計算します。

- 他のユーザが持つ属性が、現在のユーザが持つ属性にどの程度一致するか
- 一致する属性を持ち、そのロールを所有するユーザが何人いるか

一致する属性の数が最も多く、同じロールを所有するユーザ数が最も多いロールが最適です。 たとえば、役職が店員で、マネージャが Bob Folchart である 10 人のユーザが、Remote Employee ロールを所有しているとします。 北東オフィスにいる 5 人のユーザが Quota-based Salary ロールを所有しています。 この場合、Remote Employee ロールは Quota-based Salary ロールよりも一致の評価が高くなります。

- ［ほぼ一致］

  CA RCM は、ユーザが持つ権限を既存のプロビジョニング ロールと比較します。ユーザがロールによって定義された権限の多くを持っている場合、CA RCM はそのロールをサジェストします。 このタイプのサジェスト ロールは、ユーザが持つ個別の権限数とシステム内のロール数を最小限に押さえるのに役立ちます。

  この場合にサジェスト ロールがユーザに適切かどうかを計算するために、CA RCM は以下の条件を検討します。

  - プロビジョニング ロールに含まれている権限の数
  - その権限のうち、ユーザがすでに持っている権限の数

  たとえば、ユーザが Exchange アカウントと UNIX アカウントを持っており、Product Team グループのメンバであるとします。 これらの権限に基づいて、CA RCM は以下の 2 つのプロビジョニング ロールをサジェストします。

  - Employee ロール。ユーザに Exchange アカウントと Unix アカウントを与え、Product Team グループのメンバにします。
  - UNIX Administrator ロール。ユーザに UNIX アカウントを与えます。

  この例では、Employee ロールの方が UNIX administrator ロールよりも適していると考えられます。

サジェスト ロールの表示

CA Identity Manager に CA RCM を統合すると、CA RCM が特定のユーザにサジェストするプロビジョニング ロールのリストを表示できます。 CA RCM がサジェストするプロビジョニング ロールは、以下の条件を満たしています。

- 選択したユーザにそのプロビジョニング ロールを割り当てる権限を、割り当て担当者が持っている。
- プロビジョニング ロールが[検索]フィールドに入力された検索基準(ある場合)に一致している。
- プロビジョニング ロールが 1 つ以上の選択されたサジェスト方法に一致している。

サジェスト ロールを表示する方法

1. ユーザ コンソールで[プロビジョニング ロール]タブを持つタスクを開きます。

   デフォルトでは、[プロビジョニング ロール]タブは[ユーザの作成]タスクと[ユーザの変更]タスクに表示されます。

   CA Identity Manager は、現在のユーザがすでに所有しているプロビジョニング ロールをすべて表示します。

2. [サジェストされたプロビジョニング ロール]をクリックします。

   検索画面が表示され、サジェストするプロビジョニング ロールのタイプの基準を指定できます。

   CA Identity Manager は、最初にサジェスト ロール機能を設定(254 ページ)したときに定義された、デフォルトの検索基準を満たすプロビジョニング ロールのリストを表示します。

   各プロビジョニング ロールにはスコア(253 ページ)が表示されます。これは、サジェスト ロールが、指定された条件にどの程度一致するかを示すものです。

3. その他のプロビジョニング ロールを確認するには、以下のいずれかの検索方法を使用します。

   - 名前などのロールの属性に基づいてプロビジョニング ロールを検索するには、[検索]フィールドに基準を入力します。

     アスタリスク(*)を使用して値のすべてまたは一部を表すと、全体または一部分にワイルドカード検索を指定できます。

   - サジェスト ロールに新しい一致基準を指定するには、[サジェストの詳細設定]セクションを展開します。 検索に使用する 基準(250 ページ)を選択してから、必要に応じて 一致レベル(253 ページ)を選択します。

     CA Identity Manager は、指定した基準を満たすプロビジョニング ロールのリストを返します。

   注: [サジェストの詳細設定]セクションはすべての実装において使用できない場合があります。 管理者はサジェスト ロールへのサポートを設定する際に、このセクションの表示または非表示を選択できます。

4. ユーザに割り当てるロールを選択し、[送信]をクリックします。

   CA Identity Manager は指定されたロールをユーザに割り当てます。

プロビジョニング ロールのスコア

CA Identity Manager でサジェストされたプロビジョニング ロールが表示される場合、各ロールには、指定された基準をサジェストされたロールがどの程度満たしているかについてのスコアが付されています。 通常、スコアが高ければ高いほど、そのプロビジョニング ロールは割り当てられるユーザに適合していることを示しています。

サジェスト ロールのスコアは、0% から 100% の範囲で表示され、100% は一致レベルが最高水準であることを示しています。 このスコアは、CA RCM によるサジェスト ロールの基準の評価時に生成されます。 スコアの範囲は、次のいずれかの合致レベルに関連付けられます。

- 非常に良い
- 良い
- 普通
- 悪い

各一致レベルに対応するスコアを、業務上のニーズに合わせて設定できます。 たとえば、90 以上のスコアを「非常によい」の一致レベルとして指定することができます。

[プロビジョニング ロール]検索画面の設定方法に応じて、CA Identity Manager ではロール スコアを複数列で表示することができます。 複数のサジェスト条件がある場合、CA Identity Manager では条件ごとにスコアを表示し、すべての条件でプロビジョニングロールが取得した最も高いスコアが[ロール スコア]に表示されます。

注: 設定オプションは、サジェスト ロール機能を設定(254 ページ)するときに使用できます。このオプションの設定によって列の表示結果が決まります。

[サジェストされたプロビジョニング ロール]のデフォルト設定

管理者が、[プロビジョニング ロール]タブの[サジェストされたプロビジョニング ロール]ボタンをクリックすると、選択したユーザに適用できるロールのリストが CA Identity Manager に表示されます。

CA Identity Manager により、最初に表示されるサジェストされたプロビジョニング ロールのリストは、デフォルトの基準に照らして決定されます。 管理者は、以下に示すデフォルトの基準を設定できます。

- [一致するルール]
- [一致する権限]
- [一致する属性]
- [ほぼ一致]

ユーザは、検索時にこれらのフィールドに新しい値を入力することにより、デフォルトの設定を無効にできます。

[サジェストされたプロビジョニング ロール]検索のデフォルト値を設定する方法

1. ユーザ コンソールに、[プロビジョニング ロール]タブを変更できる権限を持つユーザとしてログインします。
2. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。

   [管理タスクの選択]画面が開きます。
3. [プロビジョニング ロール]タブを含むタスクを検索して選択します。

   選択したタスクの[管理タスクの変更]画面が表示されます。
4. [タブ]タブを選択し、次に[プロビジョニング ロール]タブの横にある[編集]アイコンをクリックします。

   [プロビジョニング ロールの設定]画面が表示されます。

5. 必要に応じて、以下のフィールドに入力します。

[Hide Advanced Configuration]

[サジェストの詳細設定]セクションが[サジェストされたプロビジョニング ロール]検索画面に表示されるかどうかを指定します。

[サジェストの詳細設定]セクションでは、管理者はサジェスト ロール検索に対して新しい基準を入力できます。 管理者はいずれかの基準のタイプ([一致するルール]、[一致する権限]、[一致する属性]、[ほぼ一致])を選択して、結果の一致レベルを選択できます。

[Show Best Score Only]

[サジェストされたプロビジョニング ロール]のリストに列を表示するように指定します。 このオプションを選択すると、[ロール スコア]列のみが CA Identity Manager に表示されます。この列には、検索のすべての条件でサジェストされたプロビジョニング ロールが取得した最も高いスコアが表示されます。

このオプションをクリアすると、検索のすべての条件のスコアが CA Identity Manager に表示されます。

[Check 'Matched Rule' by Default]

このチェック ボックスをオンにすると、[プロビジョニング ロール]タブの[一致するルール]フィールドがデフォルトで有効になります。

[一致するルール]フィールドを有効にすると、現在のユーザが CA RCM ロールのメンバシップを定めたルールに一致する場合、CA Identity Manager によりプロビジョニング ロールがサジェストされます。

[Check 'Matched Privileges' by Default]

このチェック ボックスをオンにすると、[プロビジョニング ロール]タブの[一致する権限]フィールドがデフォルトで有効になります。

[一致する権限]フィールドを選択する場合、現在のユーザと類似した権限を持つ複数のユーザにも割り当てられているプロビジョニング ロールが CA Identity Manager によりサジェストされます。

このフィールドを選択する場合は、[一致する権限]フィールドのデフォルト値を入力します。

[Default Setting for 'Matched Privileges']

デフォルトの一致レベルを設定して、サジェストされたプロビジョニング ロールを[一致する権限]の一致条件にどの程度一致させるかを指定します。

しきい値の設定で定義された一致レベルを満たすロールのみが、CA Identity Manager によりサジェストされます(手順 6 を参照)。

[Check 'Matched Attributes' by Default]

このチェック ボックスをオンにすると、[プロビジョニング ロール]タブの[一致する属性]フィールドがデフォルトで有効になります。

[一致する属性]フィールドを有効にすると、類似したプロファイル属性を持つ他のユーザにも割り当てられているプロビジョニング ロールが CA Identity Manager によりサジェストされます。

このフィールドを選択する場合は、[一致する属性]フィールドのデフォルト値を入力してください。

[Default Setting for 'Matched Attributes']

デフォルトの一致レベルを設定して、サジェストされたプロビジョニング ロールを[一致する属性]の一致条件にどの程度一致させるかを指定します。

しきい値の設定で定義された一致レベルを満たすロールのみが、CA Identity Manager によりサジェストされます(手順 6 を参照)。

[Check 'Almost Has' by Default]

このチェック ボックスをオンにすると、[プロビジョニング ロール]タブの[ほぼ一致]フィールドがデフォルトで有効になります。

[ほぼ一致]フィールドを有効にすると、類似の権限も含まれているプロビジョニング ロールが CA Identity Manager によりサジェストされます。 管理者は、類似する権限を使用してロールを作成する代わりに、既存のロールを割り当てることができます。

このフィールドをオンにする場合は、[ほぼ一致]フィールドのデフォルト値を入力してください。

[Default Setting for 'Almost Has']

[ほぼ一致]フィールドのデフォルト値を指定します。

デフォルトの一致レベルを設定して、サジェストされたプロビジョニング ロールを[ほぼ一致]の一致条件にどの程度一致させるかを指定します。

しきい値の設定で定義された一致レベルを満たすロールのみが、CA Identity Manager によりサジェストされます(手順 6 を参照)。

6. 以下に示すフィールドで各一致レベルに関連付ける値を指定します。

指定する値は、指定した基準をサジェストされたプロビジョニング ロールが満たす程度を示す CA RCM のスコアに対応しています。 たとえば、[「非常によい」のしきい値]を「90」に設定し、[一致する属性]および[ほぼ一致]フィールドのデフォルト値を「非常によい」に設定すると、CA RCM で 90 以上のスコアの[一致する属性]と[ほぼ一致]の基準を満たすプロビジョニング ロールのみが CA Identity Manager に表示されます。

スコアを高い値に設定するほど、ロールに求められる基準が厳しくなるので、サジェスト ロールは少なくなります。

[「非常によい」のしきい値]

サジェスト ロールが「非常によい」に一致するとみなされる CA RCM のスコアを指定します。

[「良い」のしきい値]

サジェスト ロールが「良い」に一致するとみなされる CA RCM のスコアを指定します。

[「普通」のしきい値]

サジェスト ロールが「普通」に一致するとみなされる CA RCM のスコアを指定します。

[「悪い」のしきい値]

サジェスト ロールが「悪い」に一致するとみなされる CA RCM のスコアを指定します。

7. [OK]をクリックして[タブ]タブに戻り、次に[送信]をクリックします。

［プロビジョニング ロール］タブに行った変更が CA Identity Manager に保存されます。

コンプライアンス メッセージおよびパターン メッセージ

CA Identity Manager が、CA RCM と統合されている場合は、Identity Manager の管理者は、変更をコミットする前に提案済みの変更を CA RCM のロール モデルと照合できます。 コミットする前に変更を検証することにより、企業が各業務に定義したロール モデルを維持できます。

ユーザは、プロビジョニング ロールに対する提案済みの変更（ロールの割り当てまたは削除）の検証 およびユーザ属性に対する変更の検証を行うことができます。

CA Identity Manager では、以下の 2 つの種類の検証を実行します。

- コンプライアンス

  提案済みの変更は、それらの変更が CA RCM のビジネス ポリシー ルールに違反していないかどうかを確認するため、CA RCM のロール モデルと照合されます。

- パターン

  提案済みの変更は、変更対象が「パターン外」とならないかどうかを確認するため、CA RCM ロール モデルと比較されます。また、各変更がロール モデルで定められているパターンを大きく変えることのないよう、CA Identity Manager による検証が行われます。

ユーザが特定のタスクを遂行する場合に、このような検証を自動で実行するか、ユーザが手動で開始できるようにするかを CA Identity Manager で設定できます。

コンプライアンス メッセージ

ある環境で、コンプライアンスメッセージが有効化されると、管理者がタスクのサブミットや作業アイテムの承認を行う前に CA Identity Manager により、プロビジョニング ロールおよびユーザ属性に対する提案済みの変更の検証が実行されます。 提案済みの変更は、Business Process Rule（BPR）と照合されます。BPR は、CA RCM で定義され、権限に対するさまざまな制約が定められています。 たとえば、ある BPR では、メンバの下請け会社への備品の発注を許可する調達部門のロールをもつユーザが、下請け会社に支払いを行うロールをもつことを禁じています。 BPR は、CA RCM 内のシステム管理者、業務マネージャ、監査人、ロール エンジニアによって作成されます。

注: BPR エージェントの詳細については、「CA RCMSage DNA User Guide」を参照してください。

例: コンプライアンス警告

コンプライアンス メッセージのサポートが、Identity Manager 環境で有効化されると、CA Identity Manager により、提案済みの変更が、CA RCM のコンプライアンス ポリシーに違反するかどうかを示すメッセージが表示されます。

この例の企業は、管理者が従業員にプロビジョニング ロールを割り振るときに行う自動のコンプライアンス チェックを設定しています。

ある従業員、Nancy McDonald は、財務グループから営業グループに異動します。Identity Manager のユーザ コンソールで、管理者は、Sales Representative プロビジョニング ロールを Nancy に割り当てます。 このロールにより、注文書を生成する販売アプリケーションへのロール メンバ アクセス権が付与されます。

また、Nancy は、注文書を承認するメンバを許可する財務のプロビジョニング ロールを保持しています。 このロールは、入社時に Nancy に割り当てられたものですが、彼女の新しい職務にはもはや適用されません。

会社には、CA RCM で定義されている、ある業務ポリシーがあります。そのポリシーにより、ユーザは、Sales Representative と Finance のロールを同時に持つことを制限されます。 管理者が、Nancy に Sales Representative のロールを割り当てるタスクをサブミットしようとすると、エラーメッセージが表示されます。

管理者は、Nancy に Sales Representative のロールを割り振る前に、Finance ロールを削除する必要があります。 違反を削除すると、管理者は正常にタスクをサブミットすることができるようになります。

パターン メッセージ

パターン メッセージを使用すると、CA RCM ロール モデルのパターンに違反しているプロビジョニング ロールまたはユーザ属性に対する提案済みの変更を特定できます。CA Identity Manager では、以下のタイプのパターン チェックが実行されます。

- [ユーザが事前定義済みルールと一致しません]

  提案済みの変更と CA RCM のロールの明示的なルール間の不一致を示します。

- [ユーザの権限に対するロールの割り当てがパターン外です]

  類似した権限を持つ複数のユーザは、通常このロールを有しません。

- [累積した権限が多すぎます]

  そのユーザには、もはや必要なくなったロールやリソースに対するアクセス権限が長期間のうちに累積されている可能性があります。

- [ユーザが割り当てられたロールが多すぎます]

  そのユーザは、ほとんどのユーザより多くのロールを有しています。

- ［ロールが割り当てられたユーザが多すぎます］

  そのロールは、ほとんどのロールより多くのユーザを有しています。
- ［重複したユーザおよびロール定義のリンクが検出されました］

  ユーザは、メッセージに記載されているロールに複数の方法でリンクされています。

例：パターン警告

CA Identity Manager が、CA RCM と統合されている場合は、提案済みの変更が、その CA RCM ロール モデルのパターンに照らして検証されるように CA Identity Manager を設定できます。

この例では、管理者は、CA Identity Manager の［ユーザの変更］タスクを使用して、社内で 3 ヵ月間勤務する予定のある契約者に HR ロールを割り当てます。

［ユーザの変更］タスクは、管理者が［コンプライアンスのチェック］ボタンをクリックすることで、新しいロールを割り当てる前に、会社の既存のロール モデルの違反がないかどうかをチェックできるように設定されています。

管理者が、HR プロビジョニング ロールをチェックすると、2 つのメッセージが表示されます。 最初のメッセージは、契約者に HR ロールを割り当てることは、ロール モデルのパターンに違反することを通知する警告です。その契約者は、CA RCM に定義されているこのロールのルールを満たしていないからです。 2 番目のメッセージは、HR ロールに登録されているユーザが多過ぎることを通知するアラートです。

管理者は、たとえ 2 つのパターン違反があってもタスクをサブミットすることはできますが、その警告メッセージを無視する正当な理由を入力する必要があります。 管理者は、そのユーザが臨時の契約者であることを述べた注意書きをその取引に追加して、タスクをサブミットします。

その注意書きは、そのタスクの履歴に記録され、［サブミット済みタスクの表示］タスクに表示されます。

メッセージの種類

コンプライアンス チェックまたはパターン チェックを実行すると、次の例に示すようにユーザ コンソールの現在のタスクの上に違反メッセージが表示されます。

違反メッセージには、以下の情報が含まれています。

- メッセージのカテゴリ

  以下のいずれかのカテゴリを示します。

  - クリティカル

    重度のコンプライアンス違反またはパターン違反を示します。 管理者は、エラーが解消されるまでタスクをサブミットできません。

  - 警告

    重要なコンプライアンス違反またはパターン違反を示します。 管理者は、1 つ以上の警告のあるタスクをサブミットできますが、警告を無効にすることを確認するプロンプトが表示されます。 このような無効化についての情報は、永久に保管されるタスクの記録です。 管理者は、オプションでその無効化を正当化する理由を記録できますが、この理由もタスクの履歴に記録されます。

  - アラート

    その他のすべてのレベルのコンプライアンス違反またはパターン違反を示します。 また、現在の取引に関与していない他のユーザのパターン違反を引き起こす違反を示す場合もあります。

    管理者は、アラートを無効にできます。 確認や正当化を行う必要はありません。

  注: コンプライアンス警告およびパターン警告を表示するタスクの設定時には、各カテゴリの基準を設定します。

- 違反の種類

  設定できる違反の種類には、[コンプライアンス]または[パターン]があります。

- 重大度のスコア

  違反の重大度を、1 から 100 の数値で指定します。100 は、最も重大度の高い違反です。

- 詳細

  提案された変更が違反する業務ポリシーまたはパターンの種類を示します。

注: コンプライアンス メッセージの場合には、ビジネス ポリシー ルールが CA RCM に作成されると、メッセージの詳細についてのテキストおよび重大度のスコアが設定されます。

承認タスク内のコンプライアンスおよびパターン メッセージ

Identity Manager 管理者は、ユーザ プロファイルの変更やプロビジョニング ロールの割り当てなどのタスクの実行中に変更を検証するだけではなく、承認の変更を検証することもできます。 その場合、管理者は承認タスク画面の[コンプライアンスのチェック]ボタンをクリックし、提示された変更が CA RCM でコンプライアンス ポリシーまたはパターンに違反していないか検証します。

注: コンプライアンスおよびパターンの検証をサポートする他のタスクと同様に、エラーの重大度を持つメッセージが発生した場合、管理者はエラーが解消されるまで承認をサブミットできません。

コンプライアンスおよびパターン メッセージのサポートは、以下のタスクにおいて利用可能です。

- プロビジョニング ロール メンバシップ変更を承認
- 累積プロビジョニング ロールを承認

  CA Identity Manager が累積プロビジョニング ロールをサポートするように設定されると、プロビジョニング ロールに関連するタスク内の[追加]および[削除]アクションは AccumulatedProvisioningRolesEvent という名前の 1 つのイベントに累積されます。 たとえば、[ユーザの変更]タスクにより、ユーザに 3 つのプロビジョニング ロールが割り当てられ、そのユーザから 2 つの他のプロビジョニング ロールが削除される場合、3 つの[追加]アクションと 2 つの[削除]アクションを含む AccumulatedProvisioningRolesEvent が生成されます。

  累積プロビジョニング ロールを承認タスクでは、管理者がこれらの[追加]または[削除]アクションを個別に承認または拒否することができます。 前の例では、管理者は[削除]アクションを承認し、[追加]アクションを拒否できます。

  コンプライアンスおよびパターン メッセージのサポートが累積プロビジョニング ロールを承認タスクで有効化されている場合、管理者はタスクをサブミットする前に、各アクションの承認または拒否の結果を見ることができます。

詳細情報:

プロビジョニング ロール イベントの処理順序 (158 ページ)

コンプライアンス メッセージとパターン メッセージの履歴

CA Identity Manager が、コンプライアンス メッセージおよびパターン メッセージをサポートする場合、すべてのコンプライアンスおよびパターンチェックの履歴がタスク永続性データベースに記録されます。 ユーザは、この履歴をユーザ コンソールの[サブミット済みタスクの表示]タスクで閲覧できます。

また、その環境に監査を設定した場合は、CA Identity Manager により、監査データベースにもコンプライアンス メッセージおよびパターン メッセージが記録されます。

CA Identity Manager では、以下のような情報もコンプライアンスおよびパターン メッセージの履歴に記録されます。

- コンプライアンス チェックまたはパターン チェックをいつ行うか
- チェックは手動または自動のどちらで行うか
- そのコンプライアンス チェックまたはパターン チェックの結果
- 表示されるエラーまたは警告
- ユーザが、エラーをクリアするために提案済みの変更を修正した回数
- 無視された警告があるか、ある場合はその正当な理由があるか
- 無視されたアラートはあるか

コンプライアンスおよびパターン メッセージ サポートの設定方法

コンプライアンスおよびパターン メッセージ サポートの設定は、2 段階で行います。まず、タスクがコンプライアンスおよびパターン メッセージをサポートするかどうか、そしてそのメッセージをどのように取り扱うかを指定します。 次に、そのタスクのどのタブの情報が、RCM に送信された提案済みの変更の説明に使用されるかを決定します。

コンプライアンスおよびパターン メッセージのサポートを設定するには、次の設定を行います。

- タブの設定 (266 ページ)
- タスクの設定 (264 ページ)

詳細情報:

タスクの設定 (264 ページ)

タブの設定 (266 ページ)

タスクの設定

タスクの設定で、以下を指定します。

- そのタスクがサポートする妥当性チェックの種類 (コンプライアンスおよびパターン メッセージ)
- メッセージのレベル (エラー、警告、アラート)
- CA Identity Manager でのメッセージ表示に必要となる最小の重大度スコア

コンプライアンスおよびパターン メッセージをサポートするタスクを設定する方法

1. 管理タスクを変更できる管理者の権限で、CA Identity Manager にログインします。
2. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。

   CA Identity Manager に、変更対象の管理タスクを検索できる画面が表示されます。
3. 変更するタスクを検索し、選択します。
4. [タブ]タブをクリックします。
5. タブ コントローラ選択フィールドの横にある[編集]アイコンをクリックします。

   CA Identity Manager に、[タブ コントローラの設定]画面が表示されます。

6. 必要に応じて、以下のフィールドに入力します。

[コンプライアンス外アナリティクス レベル]

CA Identity Manager に表示する CA RCM コンプライアンス分析の情報レベルを決定します。

以下のレベルを設定できます。

- [アナリティクスなし]
- [情報メッセージの発行]
- [警告メッセージの発行]
- [エラー メッセージの発行]

[コンプライアンス外重大度カットオフ]

コンプライアンス メッセージを表示する最小の重大度のスコアを指定します。たとえば、75 を指定すると、75 以上の重大度のスコアを持つコンプライアンス メッセージのみが、CA Identity Manager に表示されます。

この設定では、タスクに表示するコンプライアンス メッセージの数を制限します。

[エラー メッセージの発行]を選択する場合、この設定によりサブミットできるタスクにも影響します。 たとえば、低いスコアを持つエラーが省略されるようにカットオフを設定すると、ユーザはエラーが含まれているタスクをサブミットできます。

[パターン外アナリティクス レベル]

CA Identity Manager に表示する CA RCM パターン分析の情報レベルを決定します。

このフィールドには、[コンプライアンス外アナリティクス レベル]と同じレベルが含まれています。

[パターン外重大度カットオフ]

パターン メッセージを表示する最小の重大度のスコアを指定します。 たとえば、75 を指定すると、75 以上の重大度のスコアを持つパターン メッセージのみが、CA Identity Manager に表示されます。

この設定では、タスクに表示するパターン メッセージの数を制限します。

[サブミット時に強制的にアナリティクスを実行]

このレベルを選択すると、自動的な妥当性チェックが有効になります。 ユーザがタスクをサブミットすると、CA Identity Manager により自動的にコンプライアンス チェックおよびパターン チェックが実行されます。 ユーザは[コンプライアンスのチェック]ボタンを手動でクリックして、コンプライアンス メッセージおよびパターン メッセージを確認する必要はありません。

7. [OK]をクリックして[タブ]タブに戻り、次に[送信]をクリックしてタスクを保存します。

タブの設定

Identity Manager が CA RCM と統合されている場合は、管理者は、提案済みの変更が CA RCM のコンプライアンス ポリシーまたはパターンに違反したときに警告を表示するように次のタブを設定できます。

- [プロビジョニング ロール]タブ
- [プロビジョニング ロール メンバシップ]タブ
- [ユーザのプロファイル]タブ
- [リレーションシップを承認]タブ(単一のプロビジョニング ロールの割り当てまたは削除に使用)などの承認用のタブ、[累積プロビジョニング ロールの関係を承認]タブ(累積プロビジョニング ロール イベントの承認に使用)

コンプライアンス メッセージおよびパターン メッセージを有効にする方法

1. 管理タスクを変更する権限をもつユーザとして、ユーザ コンソールにログインします。
2. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。

   [管理タスクの選択]画面が開きます。
3. 変更するタスクを検索し、選択します。

   選択したタスクの[管理タスクの変更]画面が表示されます。
4. [タブ]タブを選択して、設定するタブの横にある矢印アイコンをクリックします。

5. 必要に応じて、以下のフィールドに入力します。

   [タブを[コンプライアンス外アナリティクス]に含める]

   そのタブのコンプライアンス チェックを有効にします。

   [タブを[パターン外アナリティクス]に含める]

   タブのパターンチェックを有効にします。

   注:CA RCM へのアクティブな接続が、表示するこれらのフィールドの環境に存在している必要があります。

6. [OK]をクリックして[タブ]タブに戻り、次に[サブミット]をクリックします。

   タブに対して行った変更が保存されます。

手動検証の設定方法

コンプライアンス チェックまたはパターン チェックが含まれているタブで手動検証を設定すると、タスク画面に[コンプライアンスのチェック]ボタンが表示されます。 管理者は、そのボタンをクリックすることで、タスクをサブミットする前にコンプライアンス チェックまたは妥当性チェックを開始できます。 妥当性チェックでエラー メッセージが返された場合には、管理者はタスクをサブミットする前に違反をクリアする必要があります。

手動検証は、コンプライアンス チェックおよびパターン チェックのデフォルトの方法です。 管理者がコンプライアンス チェックまたはパターン チェックの開始を選択できるため、システム パフォーマンスへの影響を最小限に抑えることができます。

妥当性チェックを手動で行うには、コンプライアンス メッセージまたはパターン メッセージあるいはその両方をサポートするよう、タブを設定(266 ページ)します。 追加設定は必要ありません。

自動検証の設定方法

自動検証を有効化することにより、常にコンプライアンス チェックまたはパターン チェックを実行するように重要なタスクを設定できます。 この場合、CA Identity Manager により、自動的に妥当性チェックが実行され、管理者が検証プロセスを開始する必要はありません。

注: 自動検証の実行により、パフォーマンスに影響が及ぼされることがあります。 自動検証は、重要なタスクに対して設定することをお勧めします。

自動検証の設定方法

1. コンプライアンス チェックまたはパターン チェックあるいはその両方をサポートするように、タブを設定します。(266 ページ)
2. タブ コントローラ設定の[サブミット時に強制的にアナリティクスを実行]を選択し、自動検証をサポートするタブが含まれているタスクを設定します。(264 ページ)

第 13 章: CA Enterprise Log Manager 統合

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 Enterprise Log Manager の機能 (269 ページ)
追加の CA Enterprise Log Manager リポートまたはクエリの CA Identity Manager への統合 (280 ページ)

CA Enterprise Log Manager の機能

CA Enterprise Log Manager と CA Identity Manager が統合されると、以下の機能が利用可能になります。

- CA Enterprise Log Manager エージェントが CA Identity Manager 監査情報を収集し、CA Enterprise Log Manager に送信して Event Grammar (CEG) に変換します。
- Identity Manager ユーザ コンソールは、返された情報をフィルタするために使用される CA Identity Manager コンテキスト情報を利用して、CA Enterprise Log Manager レポートとクエリをシームレスに取得できます。
- CA Identity Manager には多数のデフォルトのレポートが付属しており、CA Enterprise Log Manager レポートおよびクエリを既存タスクまたは新しいタスクに追加するための基盤を備えています。
- CA Enterprise Log Manager エージェントは CA Identity Manager [監査データベース] マシン上にインストールされます。
- CA Identity Manager コネクタは CA Enterprise Log Manager エージェント上で設定されます。
- Identity Manager 環境のための CA Enterprise Log Manager の製品登録が作成されます。
- 製品登録のオプションとして CA Enterprise Log Manager データ アクセス フィルタが作成されます。

CA Enterprise Log Manager コンポーネント

CA Identity Manager が CA Enterprise Log Manager と統合されると、以下のコンポーネントが Identity Manager アーキテクチャに追加されます。

- [CA Elm Viewer]タブ では、CA Enterprise Log Manager オブジェクトを任意の新しいタスクまたは既存タスクに埋め込むことができます。

  注: 設定済みの CA Enterprise Log Manager サーバに接続する必要があります。

- インポート可能なロール定義

統合の制限

以下は、CA Enterprise Log Managers サーバでのフレームワーク統合の制限事項として知られています。

- ランタイム時のタスク設定用のクエリおよびレポート リスト取得は、実行速度が遅くなる場合がある。
- CA Enterprise および Log Manager の API が、Java により指定されたデフォルトのタイム ゾーンのみを認識する。
- 複合フィルタで使用されている場合、EQUAL の操作で大文字小文字が区別される。
- CA Enterprise Log Manager サーバの最低バージョンは、表示順にサブスクリプション更新が適用された以下の GA ELM サーバ (45.10) です。

  1. SP-1 サブスクリプション パッチ
  2. M5 コンテンツ パッチ
  3. Open API 更新

- CA Enterprise Log Manager サーバへの接続は、同時に 1 つのみサポートされている。

CA Enterprise Log Manager を CA Identity Manager に統合する方法

CA Enterprise Log Manager レポートおよびクエリを表示および管理する前に、管理者が以下を行う必要があります。

1. CA Enterprise Log Manager エージェントのインストール
2. 新しいコネクタを作成します。
3. CA Identity Manager での監査の有効化。
4. CA Enterprise Log Manager サーバの設定

CA Enterprise Log Manager エージェントのインストール前提条件

CA Enterprise Log Manager エージェントのインストール前に、以下を行う必要があります。

- CA Enterprise Log Manager サーバ マシンに、CA Identity Manager を実行している、または Identity Manager 監査データベースをホストしているマシンから接続できることを確認します。
- エージェント マシンにサーバ マシンから接続できることを確認します。
- エージェント マシン上のデータ ソースを設定します。 手順をご覧になるには ここ (271 ページ)をクリックしてください
- Adobe Flash Player のバージョンが 9.0.28 またはそれ以上であることを確認します。プレーヤはここからダウンロードできます。

  http://www.adobe.com/go/getflash
- エージェント バイナリのダウンロード。 手順をご覧になるには ここ (272 ページ)をクリックしてください
- エージェント認証キーの取得。 手順をご覧になるには ここ (272 ページ)をクリックしてください
- サーバ名/IP にただちにアクセスできることを確認します。
- アカウント情報には迅速にアクセスできるようにしても、セキュリティを脅かさないようにしてください。 これはエージェントがサービスとして実行されるアイデンティティ アカウントです(Windows)。
- コネクタがすでに存在する場合、デフォルトのコネクタ情報をエクスポートし、すぐに使用できるようにします。
- マシンに 4 GB の RAM が実装されていることを確認してください。

エージェント マシン上のデータ ソースの設定

以下の手順に従って、エージェント マシン上でデータ ソースを設定します。

データ ソースの設定方法

1. [コントロール パネル]、[管理ツール]、[データ ソース(ODBC)]の順に移動します。
2. [System DSN]タブから、以下を追加します。

   監査データベースを参照する imsauditevent12 データ ソース(ODBC)。
3. [適用/OK]をクリックします。

   データ ソースが設定されました。

エージェント バイナリのダウンロード

以下の手順に従って、エージェント バイナリをダウンロードします。

エージェント バイナリをダウンロードする方法

1. 以下の URL から CA Enterprise Log Manager サーバにログインします。

   https://<host>:5250/spin/calm/CALMSpindle.csp

2. [管理]、[Log Collection]、[Agent Explorer]、[エージェント バイナリのダウンロード]、<OS> <version> の順に移動します。
3. ファイルに保存します。

エージェント認証キーの取得

この手順を使用して、エージェント認証キーを取得します。

エージェント認証キーを取得する方法

1. CA Enterprise Log Manager サーバから[管理]、[Log Collection]、[Agent Explorer]、[エージェント認証キー]に移動します。
2. キーには迅速にアクセスできるようにしても、セキュリティを脅かさないようにしてください。

CA Enterprise Log Manager エージェントのインストール

CA Enterprise Log Manager エージェントは、イベントの収集および情報の CA Enterprise Log Manager サーバへの送信を担当します。 Identity Manager データベース サーバあるいはエンドポイント マシン上にエージェントをインストールし、ロギングを有効にします。

注: CA Enterprise Log Manager エージェントは Windows および Linux でサポートされています。

CA Enterprise Log Manager エージェントのインストール方法

1. データベース サーバ上で ca-elmagent-<version>.exe インストールを実行し、以下を指定します。

   CA Enterprise Log Manager サーバ名/IP アドレスおよび認証コード。

   サービス/デーモンとしてエージェントを実行するために使用される、エージェント サーバのアカウント情報。

2. デフォルトのコネクタ リスト ファイルが利用可能であれば指定します。
3. 以下の URL から CA Enterprise Log Manager サーバにログインします。

   https://<host> :5250/spin/calm/CALMSpindle.csp

4. [管理]、[Log Collection]、[Agent Explorer]、[Default Agent Group]の順に移動します。
5. エージェント マシンを選択し、[Status and Command]ビューを起動します。

   ステータスが実行されています。

ロール定義のインポート

ユーザ コンソールで Enterprise Log Manager 接続を設定する前に、CA Enterprise ロール定義をインポートする必要があります。

ロール定義をインポートする方法

1. 以下の URL から Management コンソールにログオンします。

   http://host:port/idmmanage

2. [環境]、[ロールおよびタスクの設定]の順に移動し、[インポート]ボタンをクリックして Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml を選択します。
3. [保存して閉じる]をクリックします。
4. ユニット コンソールの[システム]タブから、[Enterprise Log Manager 接続の設定]をクリックし、必要な情報を入力してから[送信]をクリックします。

新しいコネクタの作成

以下の手順に従って、新しいコネクタを作成します。

新しいコネクタを作成する方法

1. 以下の URL から CA Enterprise Log Manager サーバにログインします。

   https://<host> :5250/spin/calm/CALMSpindle.csp

2. [管理]、[Log Collection]、[Agent Explorer]、[Default Agent Group]の順に移動します。
3. エージェント マシンを選択します。
4. コネクタ表示に切り替えます。
5. [Create a new Connector]ボタンをクリックして、以下の情報を入力します。

   コネクタの詳細

   統合タイプに[CAIdentityManager]を選択し、必要に応じてコネクタ名を変更します。

   コネクタの設定

   接続文字列

   - Driver={SQL Server} ; Server=<Auditing DB Server> ; Database=<Auditing DB>
   - Driver={Microsoft ODBC for Oracle} ; Dbq=<Auditing DB TNSname>

   ユーザ名: <Auditing DB User>

   パスワード: <Auditing DB User Password>

6. r12.5 で使用できるよう、以下の接続設定の変更を CA Identity Manager コネクタに適用します。

   - SourceName: エージェント マシン上のデータ ソースの名前 - imsauditevent12
   - AnchorSQL: select max(id) from imsauditevent12
   - AnchorField: IMS_EVENTID
   - EventSQL:

     select imsauditevent12.id as IMS_EVENTid ,imsauditevent12.audit_time as IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME ,imsauditevent12.admin_name as ADMINUNIQUENAME ,imsauditevent12.admin_dn as ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID ,imsauditevent12.event_description as EVENTINFO ,imsauditevent12.event_state as EVENTSTATE ,imsauditevent12.tasksession_oid as TASKOID ,imsaudittasksession12.task_name as TASKNAME ,imsauditeventobject12.object_type as OBJECTTYPE , imsauditeventobject12.object_name as

```
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as
ATTRNAME ,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE
,imsauditobjectattributes12.attribute_newvalue as
ATTRNEWVALUE ,imsauditobjectattributes12.attribute_newvalue as ATTRVALUE from
imsauditasksession12, imsauditevent12, imsauditeventobject12, imsauditobjectattributes12 where
imsauditevent12.id >? and
imsauditevent12.tasksession_id = imsauditasksession12.id and imsauditevent12.tasksession_oid =
imsauditasksession12.tasksession_oid and
imsauditeventobject12.parent_event_id = imsauditevent12.id and imsauditobjectattributes12.parent_object_id =
imsauditeventobject12.id ORDER BY
imsauditevent12.id ASC;
```

7. 保存して閉じます。

コネクタが動作していることを検証する方法

1. ［管理］、［Log Collection］、［Agent Explorer］、［Default Agent Group］の順に移動します。
2. エージェント マシンを選択します。
3. コネクタ表示に切り替え、［Launch Status and Command View］ボタンをクリックします。

   ステータスが実行されています。

CA Identity Manager での監査の有効化

CA Identity Manager で監査を有効化する方法

1. 管理コンソールを開きます。

   http://host:port/idmmanage

2. [環境]、<Environment>、[詳細設定]、[監査中]の順に移動します。
3. 既存の設定をエクスポートし、ファイルを保存します。
4. 保存したファイルに以下の変更を加え、変更を保存します。
   - <Audit enabled="true" auditlevel="BOTH" datasource="auditDbDataSource"
   - 最後の定義済み監査プロファイルの下に、パスワード ポリシー用の監査プロファイルを追加します。

     <AuditProfile objecttype="FWPASSWORDPOLICY" auditlevel="BOTHCHANGED"/>
5. ファイルを管理コンソールにインポートして戻し、以下のいずれかを実行して監査情報の集約をトリガします。
   - ユーザ管理対象オブジェクト上で実行されるタスク
   - グループ管理対象オブジェクト上で実行されるタスク
   - パスワード ポリシー管理対象オブジェクト上で実行されるタスク
6. 以下の URL から CA Enterprise Log Manager サーバにログインします。

   https://<host> : 5250/spin/calm/CALMSpindle.csp
7. 既存のレポートを使用するには、[Queries and Reports]、[クエリ]、[CA Identity Manager]の順に移動します。

   注: 設定済みの Enterprise Log Manager サーバが必要です。
8. 実行したタスクによっては、以下のデフォルトのレポートを開いてイベントが予定されていることを検証します。
   - ユーザ ID でフィルタされた「CA Identity Manager - システム全体のイベント」を呼び出す、[システム全体のイベント (ユーザ別)]タスク
   - 「アカウント管理 (ホスト別) 」をそのまま起呼び出す、[アカウント管理 (ホスト別)]タスク
   - 「アカウント作成 (アカウント別) 」をそのまま呼び出す、[アカウント作成 (アカウント別)]タスク
   - 「アカウント削除 (アカウント別) 」をそのまま呼び出す、[アカウント削除 (アカウント別)]タスク
   - 「アカウントのロックアウト (アカウント別) 」をそのまま呼び出す、[アカウントのロックアウト (アカウント別)]タスク

- 「CA Identity Manager - プロセス アクティビティ (ホスト別) 」をそのまま呼び出す、[認証プロセス アクティビティ (ホスト別)]タスク
- 「CA Identity Manager - ポリシーの変更アクティビティ 」タスクをそのまま呼び出す、[パスワード ポリシーの変更アクティビティ]タスク

CA Enterprise Log Manager サーバの設定

CA Enterprise Log Manager サーバの設定および管理を行う前に、以下を確認する必要があります。

- EiamAdmin クレデンシャルを取得していること
- Adobe Flash Player 9.0.28 またはそれ以降のバージョンがインストールされていること

CA Enterprise Log Manager サーバが設定されると、以下の機能が使用可能になります。

- 監査イベントを作成する複数の環境は、単一の CA Enterprise Log Manager サーバまたはフェデレーション階層によって消費されます。
- リモート システムのデータ認証は、CA Enterprise Log Manager のデータ アクセス フィルタを使用して実装可能です。

CA Enterprise Log Manager サーバの設定方法

1. 以下の URL から、CA Enterprise Log Manager Administrator クレデンシャルを使用して CA Enterprise Log Manager サーバの製品登録ページにログインします。

   https://host:port/spin/calmapi/products.csp

2. [Register]ボタンをクリックし、証明書名およびパスワードを入力して、Identity Manager 環境を登録します。

   注: 各環境にはそれぞれ別の登録ペア(証明書名/パスワード)が必要です。

3. [管理]、[User and Access Management]、[New Data Access Filter]の順に移動し、作成するフィルタ名を入力します。
4. 次の手順に進みます。
5. [Selected Identities]を[All Identities]のままにして、次の手順に進みます。
6. [New Event Filter]ボタンをクリックして、アクセス フィルタを作成します。

   CA Identity Manager から収集されたログでは作成された証明書をマシン/環境名のみに制限して、Data Access Filter を設定します。 また、証明書を管理エンドポイントではネイティブ エンドポイント情報へのアクセスのみに制限することもできます。

7. 保存して閉じます。
8. [Open Access Policies]ボタンをクリックして、[Access Policies]を開きます。
9. [Obligation Policies]を選択して、利用可能な単一のポリシーをクリックします。
10. 「All Identities」を削除し、証明書名を追加します。
11. ポリシーを保存します。
12. Identity Manager ユーザ コンソールにログインし、Enterprise Log Management 接続を設定します。

Enterprise Log Manager 接続の設定

この画面を使用して、新規に追加された CA Enterprise Log Manager 接続タスクを管理します。

この画面のフィールドを以下に示します。

[接続名]

単一の CA ELM 接続管理オブジェクトに使用する一意の名前を指定します。

このフィールドは、読み取り専用です。

[説明]

その CA ELM 接続について説明します。

[ホスト名]

CA Enterprise Log Manager サーバのホスト名または IP アドレスを指定します。

これは必須フィールドです。

[ポート #]

CA Enterprise Log Manager サーバの接続ポートを指定します。

デフォルト: 52520

これは必須フィールドです。

[認証機関によって署名された SSL 証明書]

チェックがオンになっている場合には、CA Enterprise Log Manager サーバへの接続時に、厳格な SSL 証明書チェックを指定します。

たとえば、デフォルトで CA Enterprise Log Manager にインストールされている SSL 証明書のような自己署名 SSL 証明書を有する場合は、ルート認証局へのトラステッド パスが存在しないので、このチェック ボックスをオフにする必要があります。

[証明書名]

認証に使用する CA Enterprise Log Manager 証明書の名前を指定します。

これは必須フィールドです。

[Certificate Password]

CA Enterprise Log Manager のパスワードを指定します。

これは必須フィールドです。

[属性]

サポート対象外です。 バージョンは、接続情報をテストとして保存するために取得します。

Enterprise Log Manager 接続の削除

リストから接続を選択して、[削除]をクリックします。 CA Enterprise Log Manager 接続タスクが削除されます。

追加の CA Enterprise Log Manager リポートまたはクエリの CA Identity Manager への統合

[Enterprise Log Manager ビューア]タブを使用して、追加の CA Enterprise Log Manager レポートまたはクエリを CA Identity Manager に統合することができます。 これらの新しいレポートまたはクエリは、(ウィザードも含む)既存のタスクおよび新規タスクと組み合わせることができます。 CA Enterprise Log Manager フェデレーション データを必要に応じて含めることもできます。 [Enterprise Log Manager ビューア]タブを使用して、取得した情報にフィルタを適用できます。 フィルタでは以下を使用できます。

- 固定値
- 管理対象オブジェクトの属性
  - たとえば、physical - ::MyPhysicalAttribute::

    logical - ::|MyLogicalAttribute|::
- CA Enterprise Log Manager Common Event Grammar (CEG) により記述されている、すべてのフィールド
  - dest_username
  - dest_objectname
  - dest_uid
  - source_username
  - source_objectname
  - source_uid
  - …

[Enterprise Log Manager ビューア]タブの設定

[CA Enterprise Log Manager ビューア]タブに、以下のいずれかまたはすべてのフィールドを表示するように設定します。

名前

タブに割り当てる名前。

タグ

タスク内で一意なタブの識別子。 文字またはアンダースコアで始まり、文字、数字、アンダースコアのみで構成される必要があります。 タグは主として、XML ドキュメントまたは HTTP パラメータを通じてデータ値を設定するために使用されます。

タブの非表示

タスク中にタブを非表示にします。 このオプションは、タブを非表示にする必要があるが、タブのアトリビュートにはアクセスするアプリケーションで役に立ちます。

Enterprise Log Manager クエリ

CA Enterprise Log Manager クエリが表示されるように指定します。

注: [CA Enterprise Log Manager クエリ]または[CA Enterprise Log Manager レポート]のいずれかを指定できますが、両方は指定できません。

Enterprise Log Manager レポート

CA Enterprise Log Manager レポートが表示されるように指定します。

注: [CA Enterprise Log Manager クエリ]または[CA Enterprise Log Manager レポート]のいずれかを指定できますが、両方は指定できません。

Enterprise Log Manager ID

クエリまたはレポートのいずれかに ID を指定します。

フェデレーション データを含める

結果に CA Enterprise Log Manager のフェデレーション データを含めるか、除外します。 デフォルトでは、このフィールドはチェック マークがオフになっています。

プロンプトの表示

CA Enterprise Log Manager のプロンプト クエリのみを表示するように指定します。 デフォルトでは、このフィールドはチェック マークがオフになっています。

フィルタ

CA Enterprise Log Manager のクエリまたはレポートによって返された結果を絞り込むために使用する、SQL ベースの詳細条件を指定します。 定数値や変動値を含めることができます。 以下は式のサンプルです。

((source_uid EQUAL ::logical.attribute.X::) AND (source_username EQUAL ::logical.attribute.Y::))

サポートされている演算子は以下のとおりです。

- equals (EQUAL)
- not equals (NEQ)
- less (LESS)
- greater (GREATER)
- less or equals (LEQ)
- greater or equals (GREATEQ)
- like (LIKE)
- not like (NOTLIKE)
- in set (INSET)
- not in set (NOTINSET)

サポートされている論理演算子は以下のとおりです。

- AND
- OR

かっこは必ず使用する必要があります。 条件式の左側の値の両端にマーカ「::」がないと、その値は定数と見なされ、定数として CA Enterprise Log Manager に送信されます。

Parameter/Value TABLE

スコーピングに使用するフィールドと値を指定します。

スコーピングのタグおよびタグのロジックに一致するクエリまたはレポートだけが選択されます。

パラメータ

開始、終了、および制限のパラメータの値を指定します。 以下のパラメータがサポートされます。

- 時間粒度（トレンドのみ）
- 開始時刻
- 終了時刻
- 最も古いグループ化イベント日付が後にある（グループ化クエリのみ）
- 最新のグループ化イベント日付が後にある（グループ化クエリのみ）
- 最新のグループ化イベント日付が前にある（グループ化クエリのみ）
- グループ化での最小イベント数（グループ化クエリのみ）
- グループ化での最大イベント数（グループ化クエリのみ）

第 14 章: タスク永続性

このセクションには、以下のトピックが含まれています。

自動化されたタスクの永続ガベージ コレクションとアーカイブ (283 ページ)
[反復]タブ (284 ページ)
[サブミット済みタスクのクリーンアップ]タブ (285 ページ)
ジョブの即時実行 (286 ページ)
[新規ジョブのスケジュール] (286 ページ)
既存のジョブの変更 (287 ページ)
[反復タスクの削除] (287 ページ)
タスク永続性データベースの移行方法 (288 ページ)

自動化されたタスクの永続ガベージ コレクションとアーカイブ

このリリースでは、管理者は[サブミット済みタスクのクリーンアップ]タスクを使用して、特定のパラメータのジョブをスケジュールまたは変更し、タスク永続性データベースのタスク情報とイベント情報をクリーンアップおよびアーカイブします。また、必要に応じてこれらの反復タスクを削除します。

[システム]タブでは、[サブミット済みタスクのクリーンアップ]を選択してウィザードを起動できます。 このウィザードから、ジョブの設定とスケジュールができ、さらにデータをアーカイブするかどうかも設定できます。 また、[システム]タブから[反復タスクの削除]を選択して、必要に応じて反復ジョブが削除されるようにすることもできます。

タスク データがクリーンアップおよびアーカイブされるようにタスクをスケジュールすると、パフォーマンスの問題とシステム停止が発生する可能性は大幅に減少します。 このアーカイブ機能によって、実行中のデータベースからタスクを削除する前に、これらのタスクをアーカイブ データベースにバックアップできます。 前の手順に戻り、削除されたタスクを表示する必要がある場合、[サブミット済みタスクの表示]のアーカイブの[Search the archive]チェック ボックスをオンにして、削除およびアーカイブされたすべてのタスクのリストを検索または表示できます。

[反復]タブ

このタブを使用して、ジョブをスケジュールします。 このタブ内のフィールドは以下のとおりです。

[今すぐ実行]

クエリを今すぐ実行します

[新規ジョブのスケジュール]

新規ジョブをスケジュールします。

[既存ジョブの変更]

すでに存在するジョブで変更するジョブを指定します。

注: このタスクにジョブがすでにスケジュールされている場合には、このフィールドのみが表示されます。

[ジョブ名]

作成または変更するジョブの名前を指定します。

[タイムゾーン]

サーバーの時間帯を指定します。

注: 新しいジョブのスケジュール時に、使用しているタイムゾーンがサーバーのタイムゾーンと異なる場合には、ドロップダウンボックスが表示されますので、使用中のタイムゾーンまたはサーバーのタイムゾーンのいずれを使用するかを選択できます。既存のジョブを修正する場合には、タイムゾーンは変更できません。

[毎週のスケジュール]

ある週の特定の日または期間でのジョブの実行を指定します。

[詳細なスケジュール]

その他のスケジュール情報を指定します。

[曜日]

ジョブを実行する曜日を指定します。

[実行時間]

ジョブを実行する時刻を、24 時間形式で指定します。 例: 14:15

[Cron 式]

このフィールドの入力の詳細については、以下の Web サイトを参照してください。

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

注:[詳細なスケジュール]が選択されている場合には、このフィールドが表示されます。

詳細情報

ジョブの即時実行 (286 ページ)
[新規ジョブのスケジュール] (286 ページ)
既存のジョブの変更 (287 ページ)
[反復タスクの削除] (287 ページ)

[サブミット済みタスクのクリーンアップ]タブ

このタブを使用して、タスクの最小期間、アーカイブ、監査タイムアウト、制限時間、タスク制限を指定します。 すべての必須フィールドに入力したら[完了]をクリックします。 このタブ内のフィールドは以下のとおりです。

[最小期間]

最終状態(完了、失敗、拒否、キャンセル、または中止)にあるタスクがクリーンアップされるまでの最小期間を指定します。 たとえば、最小期間に 1 か月を指定した場合、最後の月に最終状態に到達した任意のタスクは保持されます。 1 か月以上前に、最終状態に到達したタスクは、クリーンアップおよびアーカイブ対象となります。

これは必須フィールドです。

[アーカイブ]

実行中のデータベースからタスクを削除する前に、アーカイブデータベースにタスクをバックアップします。

ジョブが実行されたら、アーカイブが選択されている場合、データはアーカイブ データベースにコミットされ、実行時のタスク永続性データベースから削除されます。 データはアーカイブ データベースに正常にコミットされるまで削除されません。

[監査タイムアウト]

監査状態にあるタスクがクリーンアップされるまでの時間の長さを指定します。 監査状態のタスクは、この期間が経過するまで最終状態とはみなされません。 監査状態のタスクは、サブミットされていません。

[時間制限]

クリーンアップを特定の時間内に制限します。

[タスク制限]

クリーアップを特定のタスク回数に制限します。

ジョブの即時実行

ジョブを即時に実行するには、[サブミット済みタスクのクリーンアップ]ウィザードを使用します。

[システム]タブで、以下の操作を実行します。

1. 左ペインから、[サブミット済みタスクのクリーンアップ]を選択します。

   [反復]手順のウィザードが表示されます。

2. [今すぐ実行]-[次へ]を選択します。

   [サブミット済みタスクのクリーンアップ]手順のウィザードが表示されます。

3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了]をクリックします。

   ジョブが即時にサブミットされます。

[新規ジョブのスケジュール]

新規ジョブをスケジュールするには、[サブミット済みタスクのクリーンアップ]ウィザードを使用します。

[システム]タブをクリックします。

1. 左ペインから、[サブミット済みタスクのクリーンアップ]を選択します。

   [反復]手順が表示されます。

2. [新規ジョブのスケジュール]を選択し、ジョブ名とそのジョブのスケジュール設定情報を入力し、[次へ]をクリックします。

   [サブミット済みタスクのクリーンアップ]手順が表示されます。

3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了]をクリックします。

   新規ジョブがスケジュール化されます。

既存のジョブの変更

既存のジョブを変更するには、[サブミット済みタスクのクリーンアップ]ウィザードを使用します。

[システム]タブで、以下の操作を実行します。

1. 左ペインから、[サブミット済みタスクのクリーンアップ]を選択します。

   [反復]手順が表示されます。

2. [既存ジョブの変更]を選択し、既存のジョブを選び、スケジュール情報を変更してから、[次へ]をクリックします。

   [サブミット済みタスクのクリーンアップ]手順が表示されます。

3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を変更してから、[完了]をクリックします。

   既存のジョブが変更されます。

[反復タスクの削除]

反復するタスクの削除方法

[サブミット済みタスクの表示]をクリックします。

1. [反復タスクの削除]を選択します。
2. 削除するタスクを選択します。
3. [サブミット]をクリックします。

タスク永続性データベースの移行方法

これまでのリリースでは、移行は管理コンソールを使用して「オン ザ フライ」で行われていました。 コマンド ライン移行ツールが提供されたことにより、大量のタスクの移行時に発生するパフォーマンスのボトルネックを解消できます。 また、特定の環境、タスクの状態、および特定の日付範囲内で作成および実行されたタスクに合わせて微調整することもできます。 r8.1 SP2 および r12.0 から r12.5 への移行は、どちらもコマンド ライン ツールによって実行されます。

コマンド ライン ツールである runmigration は、管理ツール キットの一部であり、以下のフォルダに置かれています。

<IAM suite folder>/tools/tpmigration

タスク永続性データベースの移行には、以下を実行する必要があります。

1. tpmigration125.properties ファイルの更新。
2. JAVA_HOME 変数の設定。
3. Runmigration ツールの実行。

tpmigration125.properties ファイルの更新

タスク永続性データベースの移行を設定するには、保存されている値を含むオブジェクト ストアおよびタスク永続性情報を使用して tpmigration.properties ファイルを更新する必要があります。 tpmigration125.properties ファイルは、以下の場所に置かれています。

<IAM suite folder>/tools/tpmigration/com/ca/tp/migratetpto125

移行を設定するには、プロパティ ファイル内の以下の情報を完了させます。

```
############################################################
# 環境の詳細を入手するには、オブジェクト ストアが必要です。
############################################################
os.db.hostname=<ホスト名>
os.db.dbname=<データベース名または SID>
os.db.username=<db ユーザ名>
os.db.password=<db ユーザのパスワード>
os.db.port=<db ポート番号>
os.db.dbType=<データベースのタイプ。 例: SQL サーバの場合は sql2005、Oracle の場合は「oracle」>

############################################################
# 以前のテーブルおよび新しいテーブルが置かれているタスク永続性データ
############################################################
tp.db.hostname=<ホスト名>
tp.db.dbname=<データベース名または SID>
tp.db.username=<db ユーザ名>
tp.db.password=<db ユーザのパスワード>
tp.db.port=<db ポート番号>
tp.db.dbType=<データベースのタイプ。 例: SQL サーバの場合は sql2005、Oracle の場合は「oracle」>
```

JAVA_HOME 変数の設定

Runmigration ツールを正しく実行するには、環境変数 JAVA_HOME が設定されていることを確認します。

runmigration ツールの実行

マイグレーションを開始する方法

コマンド ラインから以下を実行してください

1. Runmigration ツールを実行します。

   Windows の場合:

   runmigration.bat

   UNIX の場合:

   runmigration.sh

2. 以下の情報を入力します。
   - エイリアスの保護環境(すべての環境を入力するには、「all」とします)。

     注: すべてを指定しない場合、入力可能な環境は 1 つのみです。
   - タスク状態。
     注: すべてを指定しない場合、入力可能なタスク状態は 1 つのみです。
   - (1-8.x, 2-12.0) から移行する CA Identity Manager のバージョン。
   - タスクを移行する日付の範囲を指定するかどうか(y/n)。

     注:「y」を選択する場合、以下を入力する必要があります。
     - 開始日(mm/dd/yy)
     - 終了日(mm/dd/yy)

   移行が開始されます。

移行が完了すると、移行されたタスクの数がステータスに表示されます。

第 15 章: コンプライアンスのサポート

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 Identity Manager でのコンプライアンスのサポート (291 ページ)
ユーザ資格の認証 (291 ページ)

CA Identity Manager でのコンプライアンスのサポート

コンプライアンスとは、企業とその従業員がビジネス ポリシーに準拠していることを確認する広範な手順を含んだコーポレート ガバナンスです。 これらのコンプライアンス手順には通常、アプリケーションやシステムへの資格の割り当てに対する監査、自動化、および文書化が含まれます。

CA Identity Manager には、このようなコンプライアンス管理をサポートする以下の機能が含まれます。

- アイデンティティ ポリシー -- ユーザが他の権限を持っている場合に特定の権限を持つことを禁止するコンプライアンス ポリシーを作成できます。このポリシーはアイデンティティ ポリシーの 1 種です。 たとえば、小切手を承認できるユーザが、小切手を発行することを禁止できます。

  コンプライアンス ポリシーでは、使用環境における義務を分離する必要があります。

- コンプライアンス レポート -- CA Identity Manager には、使用環境におけるユーザのコンプライアンス ステータスを表示するサンプル レポートが組み込まれています。このレポートを使用すれば、ビジネス ポリシーに準拠していないユーザを確認できます。

- ユーザ資格認証 -- マネージャなどのユーザが管理対象ユーザのロールを確認し、認証する必要があります。

ユーザ資格の認証

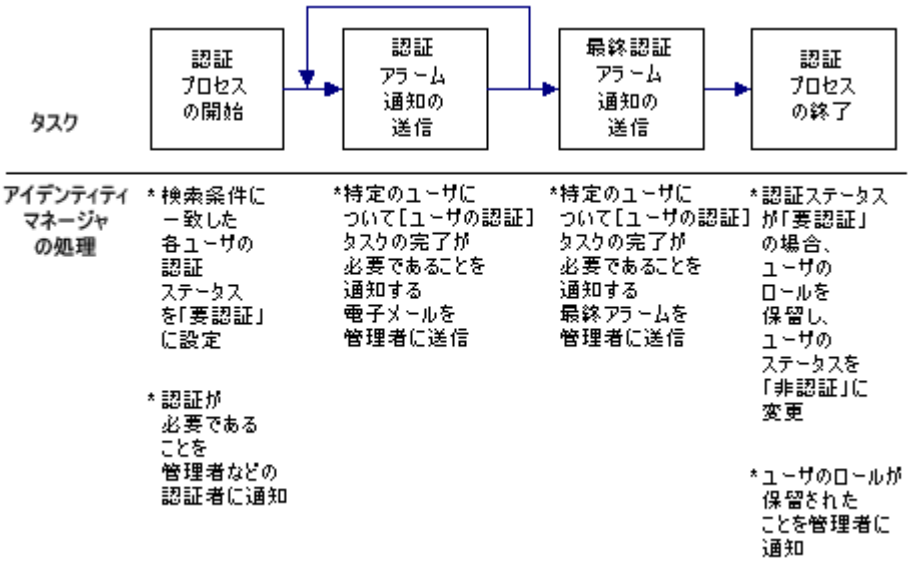
ユーザ認証では、ビジネス マネージャが管理対象ユーザのロールを定期的に確認し、承認する必要があります。 管理者は、認証タスクを使用して以下のことを実行できます。

- 認証を必要とするユーザを識別します。
- 四半期などの認証期間を指定します。この期間内に、すべてのユーザを認証する必要があります。

- マネージャなどのユーザに、保留中の認証があることを通知します。
- マネージャなどの特権ユーザに権限の認証または削除を許可します。
- 一定の期間が過ぎても認証されないユーザの権限を無効にします。

認証プロセスのしくみ

以下の図に、ユーザ認証プロセスのステップと、各ステップで Identity Manager が実行するアクションを示します。



ユーザ認証の設定方法

Identity Manager のインストール時には、デフォルトによりユーザ認証機能が設定されます。 ユーザ認証機能に関する前提条件に記載される前提条件が満たされていれば、それ以上の設定は必要ありません。

ビジネス要件に合わせてデフォルトの実装内容をカスタマイズするには、以下のセクションを参照してください。

- 検索画面の設定(293 ページ)
- 認証者の決定(294 ページ)
- 電子メール通知の設定
- 非認証ユーザに対する Identity Manager アクションの設定(296 ページ)

- 承認の要求(296 ページ)
- 認証タスクのスケジュール(297 ページ)

ユーザ認証機能の前提条件

ユーザ認証機能を設定する前に、以下のことを確認してください。

- 電子メール通知が正しく有効化され、設定されていること(421 ページ)
- %CERTIFICATION_STATUS% および %LAST_CERTIFIED_DATE% というよく知られているこれらの属性は、ディレクトリ設定ファイル(directory.xml)で設定します。

  詳細については、「CA Identity Manager Configuration Guide」を参照してください。

検索画面の設定

ユーザ認証プロセス内の各タスクでは、タスクの実行対象となるユーザまたはユーザ グループを検索できます。 ユーザの氏名や ID に基づいてユーザを検索できるように、デフォルトの検索画面が設定されています。

検索画面で利用可能なオプションを変更する方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。

   検索画面が開きます。
2. 変更するタスクを検索し、選択します。
3. [検索]タブを選択します。
4. [検索画面]フィールドで[参照]をクリックします。

   [画面定義の選択]フィールドで、タスクの検索画面が選択されます。
5. 以下のいずれかの操作を実行します。
   - デフォルトの検索画面(推奨)のコピーを変更するには、[コピー]をクリックします(推奨)。

     注: デフォルトの画面定義のコピーを作成した場合は、画面の名前とタグを変更する必要があります。
   - デフォルトの検索画面を編集するには、[編集]をクリックします。
6. ユーザが検索できるフィールドを選択するセクションで、必要に応じてフィールドを追加または削除します。

   フィールドを追加するには、既存のフィールドの下にあるリスト ボックスからフィールドを選択し、プラス記号のアイコンをクリックします。

フィールドを削除するには、削除するフィールドの横の削除ボタン( )をクリックします。

注: [最終の確認通知の送信]タスク、[ユーザの認証]タスク、[認証終了プロセス]タスクの場合は、[以下のルールに適合するオブジェクトのみ表示]セクションの認証ステータス ルールを変更しないでください。

7. [OK]をクリックし、次に[選択]をクリックしてタスク画面に戻ります。

認証者の決定

認証者とは、[ユーザの認証]タスクを使用してユーザ ロールを認証または拒否するユーザを言います。 一般にはマネージャが認証者となります。

認証者を指定する方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理ロールの変更]を選択します。

   CA Identity Manager にロールのリストが表示されます。

   注: デフォルトの[認証マネージャ]ロールが上書きされるのを防ぐには、ロールのコピーを作成し、それを変更します。

2. [認証マネージャ]ロールを選択します。
3. [メンバ]タブを選択します。
4. 認証者となるユーザを選択するメンバ ポリシーを追加します。
5. 認証者が担当するユーザを指定するスコープ ルールを定義します。
6. [OK]をクリックします。

電子メール通知の設定

認証タスクを使用する際には、Identity Manager から認証者に対し、認証者が実行すべきアクションや Identity Manager が実行したアクションに関する電子メールが送信されます。 たとえば、[確認通知の送信]タスクの実行時には、Identity Manager からマネージャに対し、特定の従業員について[ユーザの認証]タスクを完了する必要がある旨の確認通知が送信されます。

以下の内容を設定できます。

- Identity Manager が電子メール通知を送信するタイミング
- Identity Manager が電子メール メッセージを送信するユーザ
- 電子メール メッセージの内容

電子メール通知を送信するタイミングの設定

Identity Manager のデフォルトでは、以下のイベントに対して電子メール通知を送信するように設定されています。

- CertificationRequiredNotification
- CertificationRequiredReminderNotification
- CertificationRequiredFinalReminderNotification
- CertificationNonCertifiedActionPendingNotification
- CertificationNonCertifiedActionCompletedNotification

Identity Manager がこれらのイベントに対して電子メール通知を送信しないようにするには、Identity Manager の管理コンソールで電子メール通知設定を変更します。

1. Identity Manager の管理で、変更する Identity Manager 環境を選択します。
2. [詳細設定]をクリックし、次に[電子メール]をクリックします。
3. [イベント]セクションで、電子メール通知をトリガさせないイベントを選択し、[削除]をクリックします。

電子メール通知の受信者の決定

Identity Manager のデフォルトでは、認証を必要とするユーザのマネージャに電子メールが送信されます。

Identity Manager は、ユーザ認証用の電子メール テンプレートに USER_MANAGER 通知ルールを使用して、該当するユーザのマネージャを特定します。

電子メール メッセージの変更

Identity Manager が送信する電子メール メッセージの内容は、電子メール テンプレートで決定されます。これには、静的テキスト(「認証要求」などのフレーズ)と、所定のコンテキスト特有の可変テキスト(認証が必要なユーザの名前など)が含まれます。

インストールされたままのデフォルト テンプレートを使用することも、ニーズに合わせてカスタマイズすることもできます。

非認証ユーザに対する Identity Manager アクションの設定

CA Identity Manager のデフォルトでは、[認証終了プロセス]タスクの実行時に認証されていないユーザのユーザ アカウントは無効になります。 [認証終了プロセス]タスクを変更することで、CA Identity Manager の実行アクションを変更できます。 CA Identity Manager を設定して実行できる処理は、以下のとおりです。

- 何もしない
- ユーザの無効化(デフォルト)
- メンバシップ/管理ロール権限の取り消し
- メンバシップ/管理ロール権限の取り消しとプロビジョニング アカウントの削除

[認証終了プロセス]タスクを設定する方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。

   CA Identity Manager にタスクの検索画面が表示されます。
2. [認証終了プロセス]タスクを検索し、選択します。
3. [タブ]タブを選択します。

   CA Identity Manager に[認証終了プロセス]タスクに表示されるタブが表示されます。
4. [アクション タイプ]タブの横の右矢印をクリックします。

   CA Identity Manager に[未認証ユーザ アクションの設定]画面が表示されます。
5. 以下のいずれかのオプションを選択します。
   - 何もしない: CA Identity Manager はアクションを取りません。
   - ユーザの無効化(デフォルト): Identity Manager は、認証されないユーザのアカウントを無効にします。
   - メンバシップ/管理ロール権限の取り消し: 認証されないユーザのロールは CA Identity Manager により取り消されます。
   - メンバシップ/管理ロール権限の取り消しとユーザ アカウントの削除: CA Identity Manager は認証されていないユーザのロールを取り消し、プロビジョニング アカウントを削除します。
6. [OK]をクリックして、[タブ]タブに戻ります。 次に、[送信]をクリックします。

承認の要求

セキュリティ強化のために、承認者にすべての認証済みロールを承認するよう要求できます。 承認を要求するには、CertifyRole イベントとワークフロー承認プロセスを関連付けます。

認証タスクのスケジュール

サードパーティのスケジューラを使用して、認証タスクのスケジュールを設定できます。スケジューラからタスクを呼び出すには、TEWS（Identity Manager Task Execution Web Service）を使用します。

TEWS の詳細については、「Programming Guide for Java」を参照してください。

ユーザ認証プロセスの開始

認証が必要なユーザを選択するには、[認証プロセスの開始]タスクを使用します。ユーザを選択すると、そのユーザの認証ステータスが REQUIRES CERTIFICATION に設定され、保留中の認証があることを知らせる電子メールが適切な認証者に送信されます。

認証プロセスを開始するには、以下の手順に従います。

1. 認証プロセスの設定タスクを持つロール（[認証プロセス マネージャ]など）が割り当てられた Identity Manager アカウントにログインします。
2. [認証]-[認証プロセスの開始]を選択します。
3. 認証を必要とするユーザを検索します。

   検索基準と一致するユーザがすべて返されます。

   デフォルトでは、すべてのユーザが選択されています。 すべてのユーザを選択解除するには、ヘッダの[選択]チェック ボックスをオンにします。
4. 認証対象のユーザのリストを確認し、[はい]をクリックして認証プロセスを開始します。

確認通知の送信

保留中の認証があることを知らせる電子メールを認証者に送信するには、[確認通知の送信]タスクと[最終の確認通知の送信]タスクを使用します。

これらのタスクを設定するには、以下の手順に従います。

1. 認証プロセスの設定タスクを持つロール（[認証プロセス マネージャ]など）が割り当てられた Identity Manager アカウントにログインします。
2. [認証]カテゴリで、以下のいずれかのタスクを選択します。
   - 認証アラーム通知の送信
   - 最終認証アラーム通知の送信

3. 認証を必要とするユーザを検索します。

   検索基準と一致するユーザと、認証ステータスが CERTIFIE でないユーザがすべて返されます。

   デフォルトでは、すべてのユーザが選択されています。 すべてのユーザを選択解除するには、ヘッダの[選択]チェック ボックスをオンにします。

4. 認証対象のユーザのリストを確認し、[はい]をクリックして確認通知を送信します。

[ユーザの認証]タスクの使用

[ユーザの認証]タスクでは、マネージャなどのユーザが、ユーザの管理ロール、アクセス ロール プロビジョニング ロールを認証することができます。 このユーザは、ロールメンバまたは管理者のいずれかです。

1. ユーザの認証タスクを持つロールが割り当てられている Identity Manager アカウントにログインします。

   たとえば、デフォルトの[認証マネージャ]ロールには[ユーザの認証]タスクが含まれています。

2. [ユーザ]-[ユーザの認証]を選択します。
3. 認証するユーザを検索します。
4. [ロールの認証]タブを選択します。

   このユーザがメンバまたは管理者になっているロールのリストが表示されます。

   注: 管理者がメンバまたは管理者を追加/削除できるロールのみが表示されます。

5. ロールごとに、以下のオプションのいずれかを選択します。
   - [認証] -- このユーザは引き続きロールのメンバ/管理者となります。
   - [削除] -- このユーザはロールのメンバ/管理者ではなくなります。
6. [送信]をクリックします。

認証プロセスの終了

[認証終了プロセス]タスクを使用して、以下のことを実行できます。

- 認証ステータスが REQUIRES CERTIFICATION のユーザ アカウントを無効化します。
- ユーザ アカウントが無効化されたことを知らせる通知を認証者に送信します。

第 16 章: レポート

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 (299 ページ)
スナップショット レポートを実行する方法 (300 ページ)
スナップショット以外のレポートの実行方法 (314 ページ)
レポート オプションの設定 (320 ページ)
カスタム レポートの作成および実行方法 (321 ページ)
デフォルトのレポート (331 ページ)

概要

CA Identity Manager 内では、2 つの異なる種類のレポートを実行できます。

- スナップショット レポート - Identity Manager オブジェクト ストアおよび Identity Manager ユーザストアからの情報を含むスナップショット データベースからのデータが含まれています。 スナップショット レポートの例は、ユーザ プロファイル レポートです。 スナップショット データベースに追加するデータの定義は、追加する情報を指定するスナップショット定義を使用して行います。
- スナップショット以外のレポート - 監査データベースなど、他のデータ ソースからのデータが含まれています。 たとえば、Identity Manager には、デフォルトの監査レポートが含まれています。 (これらのレポートには、ユーザ コンソール内で、レポートの名前に、「Audit-」のプレフィックスが付けられています。 デフォルトでは、CA Identity Manager のみに、監査レポートを格納できますが、ユーザは、ワークフローまたはタスク永続性データベースなどあらゆるデータ ソースからのデータを含む独自のカスタム レポートを作成できます。

CA Identity Manager 内の各レポートには、実行する前に初期設定を行う必要があります。 設定手順は、実行するレポートの種類によって異なります。

スナップショット レポート (300 ページ) の設定方法

1. スナップショット定義ファイルを作成し、スナップショット データベースに追加するデータを定義します。
2. レポート用のスナップショット データを取り込みます。
3. CA Identity Manager でレポート タスクを変更し、以下の操作を実行します。
   a. スナップショット定義をタスクに関連付けます。
   b. rptParamConn 接続オブジェクトをそのタスクに追加します。

4. 以下のいずれかの方法でレポートを要求します。
   - レポートを即時に実行
   - レポートをスケジュール
5. ユーザ コンソールでレポートを表示します。

スナップショット以外のレポート(314 ページ)の設定方法

1. レポートのデータ ソース情報を使用して接続オブジェクトを作成します。
2. CA Identity Manager でレポート タスクを修正し、接続オブジェクトをそのタスクに追加します。
3. 以下のいずれかの方法でレポートを要求します。
   - レポートを即時に実行
   - レポートをスケジュール
4. レポートをユーザ コンソールで表示します。

レポートの初期設定が完了したら、CA Identity Manager 内でレポートを要求できます。レポートを即座に実行することも、後日実行するためにスケジュールすることも可能です。また、CA Identity Manager 内で、レポート用の反復スケジュールを作成することもできます。

さらに、ユーザ コンソール内でレポートを表示したり、さまざまな形式にレポートをエクスポートできます。

スナップショット レポートを実行する方法

以下の表では、CA Identity Manager でスナップショット データベース レポートを実行する手順について説明しています。

手順	参照先
1. 管理コンソールでレポートを設定します。	レポートの設定(301 ページ)
2. スナップショット データベース接続を作成します。	スナップショット データベース接続の作成(302 ページ)
3. スナップショット定義を作成します。	スナップショット定義の作成(302 ページ)
4. (オプション)スナップショット データをキャプチャします。	スナップショット データのキャプチャ(310 ページ)
5. スナップショット定義とスナップショット接続	スナップショット定義とスナップショット接続のレポート タスク

手順	参照先
をレポート タスクに関連付けます。	への関連付け(311 ページ)
6. レポートをリクエストします。	レポートのリクエスト(312 ページ)
7. レポートを表示します。	レポートの表示(313 ページ)

レポートの設定

CA Identity Manager のレポートを設定して、CA Identity Manager とレポート サーバの接続を追加します。 これによって、CA Identity Manager にデフォルトのレポート タスクも追加されます。

レポートの設定は、Identity Manager レポートを使用するすべての環境で行う必要があります。

注: レポートに関係するすべてのシステムのタイムゾーンと時刻を同じに設定することをお勧めします。

レポートを設定する方法

1. 管理コンソールで[環境]をクリックし、[詳細設定]をクリックします。
2. [レポート]をクリックします。
3. レポート サーバ(ビジネス オブジェクト)の設定を入力します。

   以下の点に注意してください。

   - 必ずサーバの完全修飾ホスト名を使用してください。
   - [Business Objects Port]フィールドには Tomcat のポート番号を入力します。

   注: レポート サーバの設定の詳細については、管理コンソール オンライン ヘルプを参照してください。
4. [保存]をクリックします。

   レポートの接続が確立され、レポート タスクとデフォルトのレポートがインストールされます。

注: レポートの設定後、環境を再起動する必要はありません。

スナップショット データベース接続の作成

CA Identity Manager で、スナップショット データのエクスポート先を指定する必要があります。 CA Identity Manager からスナップショット データベースへのデータベース接続を作成します。

スナップショットデータベース接続の作成方法

1. ユーザ コンソールで、[レポート]-[スナップショット タスク]-[スナップショット データベースの管理]-[スナップショット データベース接続の作成]を選択します。
2. すべての必要なフィールドに入力して、新規のスナップショットデータベース接続を作成します。
3. [サブミット]をクリックします。

   新規のスナップショット データベース接続が作成されます。

スナップショット定義の作成

スナップショットは、所与の時刻の CA Identity Manager 内のオブジェクトの状態を反映し、このデータを抽出して、1 つまたは複数のレポートで使用できるようにします。 スナップショット データベースにデータをエクスポートする前に、スナップショット定義を作成する必要があります。

スナップショット定義を作成する方法

1. ユーザ コンソールで、[レポート]、[スナップショット タスク]、[スナップショット定義の管理]、[スナップショット定義の作成]を選択します。
2. スナップショットを作成するか、既存のスナップショットをコピーします。
3. [プロファイル]タブで、以下の詳細を入力します。

   [スナップショット定義名]

   スナップショット定義に一意の名前を指定します。

   [スナップショット定義の説明]

   スナップショットについて説明する追加情報を表示します。

   [有効]

   このオプションを指定すると、スケジュール設定された時刻に現在のスナップショット定義に基づいて、CA Identity Manager によりスナップショットが作成されます。

   注: このオプションを選択しないと、スケジュール設定した時刻にスナップショットがキャプチャされません。 また、スナップショット定義も[スナップショット データのキャプチャ]画面にリストされません。

スナップショット パラメータ XML ファイル

オブジェクトとその属性を定義するスナップショット パラメータ XML ファイル (304 ページ)を指定します。このファイルはスナップショット データベースにエクスポートされます。

サンプルのスナップショット パラメータ XML ファイルは、以下のディレクトリにあります。

IdentityMinder.ear¥config¥com¥netegrity¥config¥imrexport¥sample

注: 以前、これらのファイルはエクスポート コマンド ファイルと呼ばれ、imrexport ツールで使用されていました。 CA Identity Manager の前のバージョンでレポートを使用し、既存のエクスポート コマンド ファイルがある場合は、ユーザ コンソール内の管理用のサンプルのスナップショット パラメータ XML ファイル ディレクトリにそれらのファイルを移動してください。

重要: ExportAll.xml はデフォルトの XML ファイルですが、サンプル XML ファイルとしてのみ使用することを目的としています。 ExportAll.xml ファイルを使用する場合、レポート用のデータすべてがエクスポートされ、完了までに時間がかかることがあります。 そのため、レポート実行に必要なデータのみをエクスポートするカスタム XML ファイルを作成することをお勧めします。

[過去の保存件数]

スナップショット データベースに格納される正常なスナップショットの数を指定します。

注: スナップショットの数は 0 より大きい数値にする必要があります。 このフィールドの値を指定しない場合、CA Identity Manager により無制限にスナップショットが格納されます。

4. 特定の日時にスナップショット データのエクスポート スケジュールを設定する場合は、[反復]タブをクリックします。

   スナップショット定義のスケジュールに関する詳細が表示されます。

   注: データが大量にある場合は、スナップショット データのエクスポートに時間がかかることがあります。 エクスポートするデータが大量にある場合は、スナップショットのスケジュールを行うことをお勧めします。 スナップショットのスケジュールを行わない場合は、[スナップショット データのキャプチャ (310 ページ)]画面を使用してスナップショット データを手動でエクスポートします。

5. [送信]をクリックします。

   スナップショット パラメータ XML ファイルで指定したオブジェクトのスナップショットを作成するように、CA Identity Manager が設定されます。

スナップショット パラメータ XML ファイル

CA Identity Manager レポートでは、Identity Manager 環境の現在の状態を確認できます。 この情報を使って、内部のビジネス ポリシーや外部規制とのコンプライアンスを確保できます。

Identity Manager のレポートは、Identity Manager 環境におけるオブジェクト間の関連性を記述する管理データから作成します。 管理データの例には以下のものが含まれます。

- ユーザのプロファイル属性
- 特定のタスクに含まれるロールの一覧
- ロールまたはグループのメンバ
- ロールを構成するルール

レポートで使用する管理データを定義するには、スナップショット パラメータ XML ファイルを使用します。

スナップショット パラメータ XML ファイルの設定

CA Identity Manager がエクスポートするデータを管理するには、スナップショット パラメータ XML ファイルを作成します。 このファイルにはエクスポートするオブジェクトをリストし、必要に応じてエクスポート基準を追加します。 基準を満たすオブジェクトのみがエクスポートされます。 たとえば、ある属性値を持つユーザに関する情報をエクスポートするなどが可能です。

スナップショット パラメータ XML ファイルには以下の形式を使用します。

```
<IMRExport>
    <export object="user">
        <where attr="%USER_ID%" satisfy="ANY">
            <value op="EQUALS">abc*</value>
        </where>
        <exportattr attr="%USER_ID%"/>
        <exportattr attr="title"/>
        <exportattr attr="|groups|" />
        <exportattr attr="|roles|" />
        <exportattr attr="|identitypolicystatus|" />
    </export>
</IMRExport>
```

スナップショット パラメータ XML ファイルには以下のエレメントが含まれます。

<export>

エクスポートするオブジェクトを示します。 たとえば、<export> エレメントによってユーザ データのエクスポートを示すことができます。

<export> エレメントには 1 つまたは複数の <exportattr> や <where> のエレメントを含めることができます。これによって、一定の基準を満たすデータだけをエクスポートすることが可能になります。 <exportattr> や <where> のエレメントを指定しないと、オブジェクトに関するすべてのデータがエクスポートされます。

<export> エレメントには object パラメータしかありません。

<where>

<value> エレメントで定義される固有の基準に基づき、エクスポートされるデータをフィルタリングします。 <where> エレメントには 1 つ以上の <value> エレメントが必要です。 また、複数の <where> エレメントを指定して、フィルタを絞り込むことができます（OR エレメントとして機能します）。

たとえば、<where> エレメントと <value> エレメントを以下のように使用すると、有効にされたロールのタスクをエクスポートできます。

```
<export object="role">
<where attr="enabled" satisfy="ALL">
<value op="EQUALS">Yes</value>
</where>
<exportattr attr="|tasks|">
</export>
```

以下の表では、<where> エレメントのパラメータについて説明します。

パラメータ	［説明］
attr	フィルタに使用する属性を示します。 たとえば、enabled 属性を指定すると、CA Identity Manager は enabled 属性の値を確認して、ロールをエクスポートするかどうかを判断します。
satisfy	エクスポートされるオブジェクトまたは属性が、一部またはすべての値の評価を満たす必要があるかどうかを示します。 ■ ALL - 属性またはオブジェクトは値の評価のすべてを満たす必要があります。 ■ ANY - 属性またはオブジェクトは 1 つ以上の値の評価を満たす必要があります。

<value>

<where> エレメント内で、属性またはオブジェクトをエクスポートするために満たす必要がある条件を定義します。 <value> エレメントには operator(op)パラメータが必要です。 op には、EQUALS または CONTAINS を指定します。

<exportattr>

エクスポートする特定の属性を示します。 <exportattr> エレメントを使用するのは、エクスポート対象オブジェクトの属性のサブセットをエクスポートする場合です。 たとえば、ユーザの ID だけをエクスポートする場合に、<exportattr> エレメントを使用できます。

また、エンドポイント オブジェクトをエクスポートする場合、<exportattr> エレメントを使用して、次のように特定のエンドポイント タイプでエクスポートされるように account 属性を定義できます。

```
<exportattr objecttype="endpoint_type">
<objattr name="description"/>
<objattr name="fullName"/>
<objattr name="lastLogin"/>
</exportattr>
```

<exportattr> エレメントには attr パラメータまたは objecttype パラメータがあります。

<objattr>

エクスポートする endpoint 属性を指定します。 objecttype がパラメータの場合、<exportattr> エレメント内で使用します。

以下の表は、<where> エレメントまたは <exportattr> エレメントで使用できる属性を、オブジェクトごとに示しています。

オブジェクト	<where> エレメントで使用できる属性	<exportattr> エレメントで使用できる属性
role	name 属性を使ってフィルタリングできます。 name - フィルタ基準を満たす名前が付けられたロール roletype - アクセス ロール、管理ロール、プロビジョニング ロールなど、フィルタ基準を満たすロールのタイプ	以下の属性のいずれかをエクスポートできます。 ■ |tasks| - ロールに関連付けられているすべてのタスク ■ |rules| - ロールに適用されるすべてのメンバ、管理、所有者、およびスコープ ルール ■ |users| - ロールのすべてのメンバ、管理者、および所有者 ■ |rolemembers| - すべてのロール メンバ ■ |roleadmins| - すべてのロール管理者 ■ |roleowners| - すべてのロール所有者
user	汎用属性またはフィジカル アトリビュート、および以下の属性のいずれか。	以下の属性のいずれかをエクスポートできます。

オブジェクト	<where> エレメントで使用できる属性	<exportattr> エレメントで使用できる属性
	■ |groups| - グループのメンバ ■ |roles| - ロールのメンバ ■ |orgs| - フィルタ基準を満たす組織にプロファイルが存在するユーザ	■ |all_attributes| - すべての使用可能なユーザ属性 ■ |groups| - ユーザがメンバまたは管理者であるすべてのグループ ■ |roles| - ユーザがメンバ、管理者、または所有者であるすべてのロール ■ |identitypolicystatus| - 特定のユーザまたはユーザ セットに適用される、すべてのアイデンティティ ポリシー ■ |allocations| - ユーザに初めて適用されるすべてのポリシー ■ |reallocations| - ユーザに再適用されるすべてのポリシー ■ |deallocations| - ユーザがポリシー条件に一致しなくなったために、ユーザに適用されないすべてのポリシー
group	汎用属性またはフィジカル アトリビュート、あるいは以下の属性。 |groups| - フィルタ基準を満たすグループ内の、ネストされたグループのリスト	汎用属性またはフィジカル アトリビュート、あるいは以下の属性のいずれかをエクスポートできます。 ■ |all_attributes| - ディレクトリ設定ファイル（directory.xml）で Group オブジェクトに定義されたすべての属性 ■ |groups| - グループ内のすべてのネストされたグループ ■ |users| - グループのすべてのメンバ ■ |groupadmins| - 指定したグループの管理者であるすべてのユーザ ■ |groupmembers| - 指定したグループのメンバであるすべてのユーザ ■ |users| - すべてのグループ管理者とグループメンバ
organization	汎用属性またはフィジカル アトリビュート	汎用属性またはフィジカル アトリビュート、あるいは以下の属性のいずれかをエクスポートできます。 ■ |all_attributes| - ディレクトリ設定ファイル（directory.xml）で Organization オブジェクトに定義されたすべての属性 ■ |orgs| - 組織内のすべてのネストされた組織

オブジェクト	<where> エレメントで使用できる属性	<exportattr> エレメントで使用できる属性
		■ |groups| - 組織内のすべてのグループ ■ |users| - 組織内のすべてのユーザ
useraccount	汎用属性またはフィジカル アトリビュート、あるいは以下の属性のいずれか。 ■ name - フィルタ基準を満たすアカウント ■ |groups| - グループのメンバ ■ |roles| - ロールのメンバ ■ |orgs| - フィルタ基準を満たす組織にプロファイルが存在するユーザ ■ |endpoints| - フィルタ基準を満たすエンドポイント ■ |endpoint_types| - フィルタ基準を満たすエンドポイントのタイプ **注**: endpoints および endpoint_types のフィルタについては、<where> エレメントでは EQUALS だけがサポートされています。	エンドポイント タイプのマッピング ファイルの属性名の指定(imname の使用)または以下の属性の使用により、アカウント固有の属性をエクスポートできます。 ■ |all_attributes| - すべての使用可能なユーザ属性 ■ |accountdata| - アカウント名、エンドポイント、コンテナ、ドメイン、およびタイプ ■ |statistics| - アカウントの作成時や変更時 ■ |assignmentinfo| - アカウントの作成者と承認者、およびその理由 ■ |syncwithroles| - ユーザ プロビジョニング ロールに対してアカウントが重複しているかどうか ■ |entitlementattributes| - マッピング ファイルに存在するすべての権限付与属性 ■ |users| - フィルタ基準を満たすユーザ ■ |groups| - グループのわかりやすい名前。 この検索を実行するとグループ メンバが返されます。 ■ |roles| - ロールのわかりやすい名前。 この検索を実行するとロール メンバが返されます。 ■ |orgs| - 組織のわかりやすい名前。 この検索を実行すると組織メンバが返されます。 ■ |allocations| - ユーザに初めて割り当てられる必要があるポリシー名が含まれます。 ■ |reallocations| - ユーザに再割り当てされる必要があるポリシー名が含まれます。 ■ |deallocations| - ユーザから割り当て解除される必要があるポリシー名が含まれます。 ■ |identitypolicystatus| - ユーザに対する割り当て、再割り当て、および割り当て解除の包含をトリガします。
endpoint	汎用属性またはフィジカル アトリビュート、あるいは以下の属性。	以下の属性のいずれかをエクスポートできます。

オブジェクト	<where> エレメントで使用できる属性	<exportattr> エレメントで使用できる属性
	■ name - フィルタ基準を満たすエンドポイント ■ |accounts| - エンドポイントで検索されたアカウント **注**: ユーザ オブジェクトもエクスポートされます。 ■ |endpoint_types| - エンドポイント タイプの情報	■ |all_attributes| - すべての使用可能なエンドポイント属性 ■ |endpoint_groups| - エンドポイントのグループ（該当する場合） ■ |accounts| - すべてのエンドポイント アカウント ■ |accounttemplates| - エンドポイントに関連付けられるアカウント テンプレート
identityPolicySet	name 属性を使ってフィルタリングできます。 name - フィルタ基準を満たすアイデンティティ ポリシー セット	以下の属性のいずれかをエクスポートできます。 ■ |all_attributes| - すべてのポリシー セット、ポリシー、およびアクション ■ |identitypolicystatus| - 特定のユーザまたはユーザ セットに適用される、すべてのアイデンティティ ポリシー

スナップショットの管理

CA Identity Manager では、スナップショット定義を表示、変更、および削除できます。スナップショット定義を表示または変更する際、[プロファイル]、[反復]、および[メンテナンス]タブが表示されます。 [メンテナンス]タブが表示されるのは、スナップショットがいったんキャプチャされた後です。 [メンテナンス]タブからは、スナップショットを削除することが可能です(スナップショットのステータスが失敗である場合でも削除可能)。

スナップショット定義を表示、変更、および削除するには、[レポート] - [スナップショット タスク] - [スナップショット定義の管理]を選択し、実行するタスクをクリックします。

注: スナップショット定義は、スナップショット データベースにデータをエクスポートするのに使用されている場合は、削除できません。 使用されているスナップショット定義を削除すると、スナップショット データベースへのデータのエクスポートは停止されますが、スナップショット定義は引き続き使用できます。

スナップショット データのキャプチャ

スナップショット定義のスケジュールを設定せずに、スナップショット データをオンデマンドでキャプチャする場合は、[スナップショット データのキャプチャ]タスクを実行して(スナップショット定義で定義された)データを即座にスナップショット データベースにエクスポートします。

重要: エクスポートするデータが大きい場合、スナップショット データのエクスポートは、処理に時間を要することがあります。 大量のデータをエクスポートする際は、スナップショットを スケジュール(302 ページ)することをお勧めします。

スナップショット データをキャプチャする方法

1. ユーザ コンソールで、[レポート] - [スナップショット タスク] - [スナップショット データのキャプチャ]を選択します。
2. スナップショット定義を選択します。
3. [サブミット]をクリックします。

   スナップショット データがスナップショット データベースにエクスポートされます。

注: [スナップショット データのキャプチャ]タスクの処理に長時間かかっている場合、[システム]タブの[サブミット済みタスクの表示]をクリックして、タスクの進捗を確認できます。

スナップショット定義とレポート タスクの関連付け

スナップショット定義をレポート タスクに割り当てると、CA Identity Manager に、どのスナップショット定義がレポートの実行に使用されるかを認識させることができます。 また、Identity Manager レポートに関する情報は、複数のソースから得ることができます。各レポートは、レポートで表示させたい情報に基づき、特定のデータ ソースに関連付けられている必要があります。

スナップショット定義とスナップショット接続をレポート タスクに関連付ける方法

1. Identity Manager のユーザ コンソールで[ロールおよびタスク]-[管理タスク]-[管理タスクの作成]を選択します。
2. スナップショット定義と関連付けるレポート タスクを検索します。
3. [タブ]タブをクリックし、[スナップショット定義の関連付け]の隣にある をクリックします。
4. [追加]をクリックします。
5. レポート タスクと関連付けるスナップショット定義を検索し、[選択]をクリックします。

   スナップショット定義とレポート タスクを関連付ける際は、以下の点に注意してください。

   - レポートは、1 つ以上のスナップショット定義と関連付けることができます。
   - スナップショット定義は、1 つ以上のレポートと関連付けることができます。
   - 1 つのレポート タスクに関する複数のスナップショットで同じ繰り返し時間を使用しないでください。
6. [OK]をクリックします。
7. [検索]タブをクリックし、[参照]をクリックして検索画面を探します。
8. 該当するレポート タスクの検索画面を編集して、[レポート用接続オブジェクト]の下の rptParamConn を選択します。
9. [OK]をクリックします。
10. [選択]をクリックします。
11. [サブミット]をクリックします。

接続のレポート タスクへの関連付け

Identity Manager レポートに関する情報は、複数のソースから得ることができます。各レポートは、レポートで表示させたい情報に基づき、特定のデータ ソースに関連付けられている必要があります。

接続をレポート タスクに関連付ける方法

1. Identity Manager のユーザ コンソールで[ロールおよびタスク]-[管理タスク]-[管理タスクの作成]を選択します。
2. 関連付け先のレポート タスクを検索します。
3. [検索]タブに移動し、[参照]をクリックして検索画面を表示します。
4. レポート タスクの検索画面を編集し、スナップショット データベース接続オブジェクトを選択します。
5. [OK]をクリックします。

レポートのリクエスト

CA Identity Manager 内でレポートを生成することができます。

レポートを生成する方法

1. レポート タスクに対するアクセス権を持つユーザとしてユーザ コンソールにログインします。
2. [レポート]-[タスクのレポート中]-[レポートのリクエスト]を選択します。

   左側のフレームにレポート リストが表示されます。
3. 生成するレポートを選択します。

   [パラメータ]画面が表示されます。
4. 必要なパラメータ情報を入力します。

   注: スナップショット レポートを実行中で、このレポート用のスナップショットがない場合は、まずスナップショットをキャプチャしてください。
5. [レポートのスケジュール]をクリックします。
6. レポートのスケジュールを選択し、[OK]をクリックします。

   レポートがレポート サーバにサブミットされます。

詳細情報

レポート スケジューラ(318 ページ)

レポート スケジューラ

レポートによっては、実行に時間を要するものがあります。同じレポートを参照する場合は、そのたびにレポートを再実行しなくても複数回参照することができます。 レポート スケジューラにより、レポートを後で自動的に生成するようにスケジュールを設定できます。 レポートが生成されると、再実行しなくてもレポートを複数回参照できます。

以下のオプションを使用して、レポートのスケジュールを設定できます。 選択したスケジュール オプションに基づいて、より多くのオプションが CA Identity Manager によって表示されます。

[今すぐ]

このオプションを指定すると、レポートがただちに実行されます。

[1 回]

このオプションを指定すると、レポートが 1 回のみ実行されます。 レポート生成時の開始日、終了日、開始時刻、終了時刻を選択する必要があります。

レポート反復スケジュールの管理

CA Identity Manager を使用すると、レポート反復スケジュールの表示、変更、削除を行うことができます。

レポート反復スケジュールの表示、変更、削除を行うには、[レポート] - [タスクのレポート中] - [レポート反復スケジュールの管理]をクリックして、実行するタスクをクリックします。

注: レポート反復スケジュールを変更する場合には、[次回実行時]フィールドは、最後に予定されているレポート インスタンスが完了するまで変更されません。 たとえば、レポートを日次で実行するようにスケジュールしている場合に、レポート反復スケジュールにより、次のインスタンスが何時実行されるかについての詳細が表示されます(例: 明日の 10:00 AM)。 今、レポート反復スケジュールを日次から月次に変更した場合、レポート サーバでは、[次回実行時]は即座には変更されません。 レポート反復スケジュールには依然として、次のインスタンスは、明日の 10:00 に実行されると表示されています。 この最後の日次のレポート インスタンスが完了すると、[次回実行時]は、新しい月次スケジュールを反映して変更されます。

レポートの表示

レポートを表示する方法

1. ユーザ コンソールで[レポート] -[レポート タスク]へ進み、[マイ レポートの表示]をクリックします。

2. 表示するレポートを検索します。

   反復レポートとオンデマンド レポートのインスタンスが表示されます。

3. 表示するレポートを選択します。

   注: CA Identity Manager で[マイ レポートの表示]タスクを使用してレポートを表示するには、ブラウザでサードパーティ セッションの Cookie を有効にします。

4. (オプション)[Export this report](左上隅)をクリックし、レポートを以下の形式にエクスポートします。

   - Crystal Report
   - Excel
   - PDF

スナップショット以外のレポートの実行方法

以下のテーブルに、CA Identity Manager でスナップショット以外のレポート(監査レポートなど)を実行する手順を示します。

手順	参照先
1. 管理コンソールでレポートを設定します。	レポートの設定(301 ページ)
2. レポート タスク用に、JDBC 接続を作成します。	レポート用の接続の作成(316 ページ)
3. 接続をレポート タスクに関連付けます。	接続のレポート タスクへの関連付け (以下のページで定義参照: 312)
4. レポートをリクエストします。	レポートのリクエスト(312 ページ)
5. レポートを表示します。	レポートの表示(313 ページ)

レポートの設定

CA Identity Manager のレポートを設定して、CA Identity Manager とレポート サーバの接続を追加します。 これによって、CA Identity Manager にデフォルトのレポート タスクも追加されます。

レポートの設定は、Identity Manager レポートを使用するすべての環境で行う必要があります。

注: レポートに関係するすべてのシステムのタイムゾーンと時刻を同じに設定することをお勧めします。

レポートを設定する方法

1. 管理コンソールで[環境]をクリックし、[詳細設定]をクリックします。
2. [レポート]をクリックします。
3. レポート サーバ(ビジネス オブジェクト)の設定を入力します。

   以下の点に注意してください。

   - 必ずサーバの完全修飾ホスト名を使用してください。
   - [Business Objects Port]フィールドには Tomcat のポート番号を入力します。

   注: レポート サーバの設定の詳細については、管理コンソール オンライン ヘルプを参照してください。
4. [保存]をクリックします。

   レポートの接続が確立され、レポート タスクとデフォルトのレポートがインストールされます。

注: レポートの設定後、環境を再起動する必要はありません。

レポート用の接続の作成

Identity Manager レポートの情報は、複数のソースから収集できます。 レポート用に他のデータ ソースへ接続する際にその詳細を指定するには、CA Identity Manager 内に JDBC 接続を作成します。

JDBC 接続を作成する方法

1. ユーザ コンソールで[システム] - [JDBC 接続管理] - [JDBC 接続の作成]をクリックします。
2. 新しい接続オブジェクトを作成するか、特定の JNDI データ ソースに基づいて接続オブジェクトを選択します。
3. 必要なすべてのフィールドに入力して、[サブミット]をクリックします。

   新しい JDBC 接続が作成されます。

重要: レポートの生成には Identity Manager オブジェクト ストア データベースを使用しないことをお勧めします。

接続のレポート タスクへの関連付け

Identity Manager レポートに関する情報は、複数のソースから得ることができます。各レポートは、レポートで表示させたい情報に基づき、特定のデータ ソースに関連付けられている必要があります。

接続をレポート タスクに関連付ける方法

1. Identity Manager のユーザ コンソールで[ロールおよびタスク]-[管理タスク]-[管理タスクの作成]を選択します。
2. 関連付け先のレポート タスクを検索します。
3. [検索]タブに移動し、[参照]をクリックして検索画面を表示します。
4. 検索画面をレポート タスク用に編集し、[レポート用接続オブジェクト]の下にある接続を選択します。
5. [OK]をクリックします。
6. [選択]をクリックします。
7. [サブミット]をクリックします。

レポートのリクエスト

CA Identity Manager 内でレポートを生成することができます。

レポートを生成する方法

1. レポート タスクに対するアクセス権を持つユーザとしてユーザ コンソールにログインします。
2. [レポート]-[タスクのレポート中]-[レポートのリクエスト]を選択します。

   左側のフレームにレポート リストが表示されます。
3. 生成するレポートを選択します。

   [パラメータ]画面が表示されます。
4. 必要なパラメータ情報を入力します。

   注: スナップショット レポートを実行中で、このレポート用のスナップショットがない場合は、まずスナップショットをキャプチャしてください。
5. [レポートのスケジュール]をクリックします。
6. レポートのスケジュールを選択し、[OK]をクリックします。

   レポートがレポート サーバにサブミットされます。

詳細情報

レポート スケジューラ(318 ページ)

レポート スケジューラ

レポートによっては、実行に時間を要するものがあります。同じレポートを参照する場合は、そのたびにレポートを再実行しなくても複数回参照することができます。 レポート スケジューラにより、レポートを後で自動的に生成するようにスケジュールを設定できます。 レポートが生成されると、再実行しなくてもレポートを複数回参照できます。

以下のオプションを使用して、レポートのスケジュールを設定できます。 選択したスケジュール オプションに基づいて、より多くのオプションが CA Identity Manager によって表示されます。

[今すぐ]

このオプションを指定すると、レポートがただちに実行されます。

[1 回]

このオプションを指定すると、レポートが 1 回のみ実行されます。 レポート生成時の開始日、終了日、開始時刻、終了時刻を選択する必要があります。

注: レポートで使用する次の反復オプションにアクセスするには、[レポート サーバ スケジューラ]タブの[反復オプションの有効化]を選択します。

(監査レポートのみ)毎時間

このオプションを指定すると、開始時刻とその後「n」時間ごとにレポートが生成されます。「n」は後続のレポートの生成間隔を示します。 開始日、終了日、開始時刻、終了時刻、後続のレポート間隔を選択する必要があります。

(監査レポートのみ)毎日

このオプションを指定すると、開始時刻とその後「n」日ごとにレポートが生成されます。「n」は後続のレポートの生成間隔を示します。 開始日、終了日、開始時刻、終了時刻、後続のレポート間隔を選択する必要があります。

(監査レポートのみ)毎週

このオプションを指定すると、開始日から毎週指定した曜日にレポートが生成されます。 レポート生成時の開始日、終了日、開始時刻、終了時刻を選択する必要があります。

(監査レポートのみ)毎月

このオプションを指定すると、開始日からその後「n」か月ごとにレポートが生成されます。「n」か月とは、一連のレポートの間の月数を示しています。 開始日、終了日、開始時刻、終了時刻、後続のレポート間隔を選択する必要があります。

(監査レポートのみ)指定した月の特定の日にレポートを実行

このオプションを指定すると、指定した月の特定の日にレポートが生成されます。 レポート生成時の開始日、終了日、開始時刻、終了時刻を選択する必要があります。

(監査レポートのみ)最初の月曜日

このオプションを指定すると、毎月最初の月曜日にレポートが生成されます。 レポート生成時の開始日、終了日、開始時刻、終了時刻を選択する必要があります。

(監査レポートのみ)月末日

このオプションを指定すると、月末日にレポートが生成されます。 レポート生成時の開始日、終了日、開始時刻、終了時刻を選択する必要があります。

(監査レポートのみ)毎月特定の週の特定の曜日

このオプションを指定すると、毎月特定の週の特定の曜日にレポートが生成されます。 レポート生成時の開始日、終了日、開始時刻、終了時刻を選択する必要があります。 たとえば、毎月第 3 週目の金曜日にレポートを生成することができます。

レポート反復スケジュールの管理

CA Identity Manager を使用すると、レポート反復スケジュールの表示、変更、削除を行うことができます。

レポート反復スケジュールの表示、変更、削除を行うには、[レポート] - [タスクのレポート中] - [レポート反復スケジュールの管理]をクリックして、実行するタスクをクリックします。

注: レポート反復スケジュールを変更する場合には、[次回実行時]フィールドは、最後に予定されているレポート インスタンスが完了するまで変更されません。 たとえば、レポートを日次で実行するようにスケジュールしている場合に、レポート反復スケジュールにより、次のインスタンスが何時実行されるかについての詳細が表示されます(例: 明日の 10:00 AM)。 今、レポート反復スケジュールを日次から月次に変更した場合、レポート サーバでは、[次回実行時]は即座には変更されません。 レポート反復スケジュールには依然として、次のインスタンスは、明日の 10:00 に実行されると表示されています。 この最後の日次のレポート インスタンスが完了すると、[次回実行時]は、新しい月次スケジュールを反映して変更されます。

レポートの表示

レポートを表示する方法

1. ユーザ コンソールで[レポート] -[レポート タスク]へ進み、[マイ レポートの表示]をクリックします。

2. 表示するレポートを検索します。

   反復レポートとオンデマンド レポートのインスタンスが表示されます。

3. 表示するレポートを選択します。

   注: CA Identity Manager で[マイ レポートの表示]タスクを使用してレポートを表示するには、ブラウザでサードパーティ セッションの Cookie を有効にします。

4. (オプション)[Export this report](左上隅)をクリックし、レポートを以下の形式にエクスポートします。

   - Crystal Report
   - Excel
   - PDF

レポート オプションの設定

ユーザが特定のレポートについて生成できるレポート インスタンスの数を設定します。

レポート オプションを変更する方法

1. [レポート]-[タスクのレポート中]-[レポート オプションの設定]を選択します。

   CA Identity Manager から IAM レポート サーバに接続され、すべてのレポートのリストが取得されます。

2. レポートを選択し、[変更]をクリックします。

   レポートの属性ペインが表示されます。

3. 以下のフィールドを編集します。

   名前

   選択したレポートの表示名を指定します。

   インスタンス数

   指定したレポートに対して生成可能なインスタンスの数を指定します。

4. [OK]をクリックします。

   レポート属性が変更されます。

カスタム レポートの作成および実行方法

CA Identity Manager では、ビジネスのニーズに適したレポートを作成およびカスタマイズできます。

以下の表では、CA Identity Manager でカスタム レポートを作成する手順について説明しています。

手順	参照先
1. Crystal Reports Developer でレポートを作成する。	Crystal Reports でのレポートの作成 (321 ページ)
2. レポート パラメータ XML ファイルを作成する。	レポート パラメータ XML ファイルの作成 (322 ページ)
3. レポート サーバにレポートとレポート パラメータ XML ファイルをアップロードする。	レポートとレポート パラメータ XML ファイルのアップロード (326 ページ)
4. レポート タスクを作成する。	レポート タスクの作成 (327 ページ)
5. レポートを実行する。	スナップショット レポートの実行方法 (300 ページ) スナップショット以外のレポートの実行方法 (314 ページ)

Crystal Reports でのレポートの作成

CA Identity Manager では、ビジネスのニーズに適した独自のカスタム レポートを作成できます。 CA Identity Manager でカスタム レポートを使用するには、まず Crystal Reports Developer でレポート (RPT ファイル) を作成します。 Crystal Reports でレポートを作成する方法の詳細については、Crystal Reports のマニュアルを参照してください。

重要: カスタム レポートを作成するために Identity Manager スキーマを参照する必要がある場合は、Identity Manager データベース スキーマを以下の場所に配置します。

C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥db¥objectstore

レポート パラメータ XML ファイルの作成

CA Identity Manager では、それぞれのレポートに独自の検索画面が表示されます。その画面で、ユーザはレポートの生成時に必要なデータを入力または選択できます。 パラメータは、レポートのフィルタに使用されるレポート フィールドの 1 つです。 パラメータを使用してデータをフィルタすることで、レポートを生成できます。 レポートの検索画面をカスタマイズできるようにするには、各レポート(RPT ファイル)をレポート パラメータ XML ファイルに関連付けます。

重要: レポート パラメータ XML ファイルはレポート(RPT ファイル)と同じ名前にし、.xml 拡張子を持つ必要があります。 たとえば、test1.rpt というレポートをレポート サーバにアップロードする場合、XML ファイルは test1.xml という名前になります。

レポート パラメータ XML ファイルには以下のエレメントが含まれます。

<product>

パラメータが使用される製品を識別します。 同じパラメータ XML ファイルを使用して、複数の製品に異なるパラメータを作成できます。

<screen>

画面に表示されるパラメータを定義します。 パラメータを特定の画面にバインドするには、画面エレメントを使用できます。 画面 ID は一意の英数字で、画面と画面のパラメータを識別するために使用されます。

<parameters>

画面のパラメータの集合を指定します。

<param>

指定されたデータをレポートに転送するパラメータ エレメントを定義します。 <param> エレメントでは、以下の属性が使用されます。

id

レポートの、どのパラメータに関連付けるかを定義します。

注: これは、Crystal Report のパラメータと同じ名前である必要があります。

name

このフィールドは CA Identity Manager では現在使用されていません。 この属性は、id と同じ値に設定します。

displaytext

パラメータの画面に表示する、分かりやすいテキストを指定します。

タイプ

パラメータのタイプを定義します。 この画面は、属性によって変わります。 サポートされるパラメータ タイプは、以下のとおりです。

- テキスト ボックス

  例: <param id="param1" displaytext="First Name" name="param1" type="string"/>

- 日時

  例: <param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>

  <param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>

  <param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>

- ドロップダウン リスト

  例: <param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>

- リスト ボックス

  例: <param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>

- ラジオ ボックス

  例: <param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>

  <param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>

  <param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>

- チェック ボックス

  例: <param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>

行

リスト ボックスに表示する行の数を定義します。

デフォルト: 5

default

指定のパラメータの画面に表示するデフォルト値を定義します。 この属性は、文字列、リスト ボックス、およびドロップダウン リストの各タイプで使用できます。

SQL

SQL クエリは、レポート パラメータ XML ファイルのリスト ボックスまたはドロップダウン ボックスの一部として定義できます。 ドロップダウン ボックスまたはリスト ボックス パラメータで SQL を使用するには、sql 属性に有効な SQL 文を用意します。

例:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr" multiselect="true" sql="select lastname, lastname from tblusers where firstname like 'S%/>
```

上記の例では、「S」で始まる名を持つユーザの姓はすべて、レポートに表示されます。

ただし、「S」で始まる名の条件は、静的なものです。 これは、以前の画面(同じレポート パラメータ グループで使用される)のいずれかに入力されるパラメータ値に基づく値をロードするユーザにとって、充分な柔軟性を持つものではありません。 以前に別の画面に入力された値を使用するには、「##<parameter id>##」を使用して SQL 文を拡張します。

たとえば、id=User、タイプが String のパラメータの場合、以下のようになります。

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

そして、SQL のそのパラメータに入力値を使用する場合、SQL 文は以下のようになります。

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr" multiselect="true" sql="select lastname, lastname from tblusers where firstname like '##User##'/>
```

CA Identity Manager は、##User## を、id=User のパラメータに入力された値と置き換えます。

注: 置換されるパラメータ値は、SQL パラメータと同じ画面には入力できません。 たとえば、「lstlastname2」が画面 3 にある場合、User パラメータは以前の画面にいずれかに入力する必要があります。

Java Beans

SQL の使用が望ましくない場合、Java Beans を使用して値を計算し、<key,value> のペアのリストを CA Identity Manager に提供できます。 Java Beans は、CA Identity Manager の classpath にあります。

例:

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2" type="dropdown"
class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

上記の例では、TestDataCollector は独自の方法で値を取得し、ドロップダウン リストのデータをレポートに送信します。 <key, value> ペアは %1F で分割されます。

Java Bean が IdentityMinder.ear¥custom ディレクトリにあることを確認します。

注: Java Beans の実装の詳細については、ビジネス オブジェクトのマニュアルを参照してください。

文字列リテラル

パラメータ値をリストまたはドロップダウン ボックスに表す最も単純な方法は、文字列リテラルを使用する方法です。 キー値は %1F で区切られ、<key, value> ペアはそれぞれ %1E で分割されます。

例:

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown" default="key1%1FMy
Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

非表示パラメータ

非表示パラメータは、レポートのコンテキスト内でパスワードなどの機密データを渡すために使用されます。 非表示データは、レポート、SQL、または Java Bean で使用され、ユーザが知識を持たなくてもビジネス ロジックを処理できます。

例:

```
<param id="city" displaytext="User1" name="city" hidden="true" type="string"
class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

上記の例では、city パラメータの値は TestDataCollector Java Bean によって処理されますが、ユーザはそれを見ることはできません。

Java Bean が IdentityMinder.ear¥custom ディレクトリにあることを確認します。

レポート パラメータ XML ファイルの例

XML ファイルというレポート パラメータの設定例を以下に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<product xmlns="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsi="http://www.example.org/Parameters"
xsi:schemaLocation="http://www.example.org/Parameters ../../../reporting/src/com/ca/ims/reporting/utils/Parameters.xsd ">
<screen id="1">
<parameters>
<param id="param1" displaytext="User" name="User" type="string"/>
</parameters>
</screen>
<screen id="Test">
<parameters>
<param id="Test" displaytext="Test" name="Test" type="sqlstr" conn_id="rptParamConn"
multiselect="true" rows="3" sql="select CUSTOMERID, CONTACTNAME from customers where customerid like
'##param1##"' />
</parameters>
</screen>
</product>
```

レポートとレポート パラメータ XML ファイルのアップロード

レポート(RPT)および対応するレポート パラメータ XML ファイルを作成したら、レポート サーバ(ビジネス オブジェクト)に両方のファイルをアップロードします。

レポートとレポート パラメータ XML ファイルをアップロードする方法

1. ビジネス オブジェクトの中央管理コンソールにログインします。
2. [Folders]をクリックします。
3. [IM Reports]フォルダを選択します。
4. [New Object]をクリックして、オブジェクトが Crystal Reports のタイプであることを確認します。
5. 作成した新しいレポート(RPT)を参照します。
6. レポートの保存先として[IM Reports]フォルダが選択されていることを確認します。
7. [送信]をクリックします。
8. 左上隅の[IM Reports]をクリックします。
9. [New Object]をクリックして、オブジェクトがテキスト タイプであることを確認します。
10. 作成した新しいレポート パラメータ XML を参照します。
11. レポートの保存先として[IM Reports]フォルダが選択されていることを確認します。

12. [送信]をクリックします。
13. [IM Reports]フォルダを開いて、新しいファイルが両方とも使用可能になっていることを確認します。

レポート タスクの作成

レポート タスクは、ユーザ コンソールで生成されるレポートにテンプレートを作成、管理、表示、削除するために使用されます。 レポート タスクを作成するプロセスは、CA Identity Manager に管理タスクを作成するプロセスに類似しています。

レポートにタスクを作成する方法

1. ユーザ コンソールで[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。
2. [管理タスクの作成]を選択し、[OK]をクリックします。
3. [プロファイル]タブ(327 ページ)を設定します。
4. [検索]タブ(328 ページ)を設定します。
5. [タブ]タブ(330 ページ)を設定します。

注: レポート(RPT ファイル)は、1 つのレポート タスクにのみ関連付けることができます。

詳細情報:

レポート タスクの[プロファイル]タブ(327 ページ)
レポート タスクの[検索]タブ(328 ページ)
レポート タスクの[タブ]タブ(330 ページ)

レポート タスクの[プロファイル]タブ

レポート タスクにプロファイル情報を入力するには、[プロファイル]タブをクリックして、以下のフィールドを設定します。

名前

レポートの名前を定義します。 各レポート タスクには、一意の名前を使用する必要があります。

タグ

タスクの一意な識別子を定義します。 これは URL、Web サービス、またはプロパティ ファイルで使用されます。 識別子は、アルファベット文字、数字、または下線文字で構成し、先頭をアルファベット文字または下線文字にする必要があります。

カテゴリ

現在のタスクが所属するカテゴリを指定します。

注: [レポート]カテゴリを選択します。

カテゴリ 2

現在のタスクが所属するサブカテゴリを指定します。 フィールドに文字列を入力します。

[プライマリ オブジェクト]

タスクを操作するオブジェクトを指定します。

注: プライマリ オブジェクトとして[レポート インスタンス]を選択します。

[アクション]

プライマリ オブジェクトで操作するアクションを指定します。

注: アクションとして[作成]を選択します。

レポート タスクの[検索]タブ

検索画面を使用して、タスクの範囲を制限し、ユーザが検索できるフィールドを制御します。 パラメータをレポートに動的に渡すかどうかに基づいて、レポートの検索画面を設定できます。

レポートごとに個別の検索画面を作成する必要があります。 検索画面では、レポート データのフィルタに使用できるパラメータを定義できます。 レポートの生成時には、検索画面の設定に基づき、CA Identity Manager によってレポート データのフィルタに使用されるパラメータの入力が求められます。 入力した内容によっては、CA Identity Manager からレポート データベースに接続して、条件を満たすデータを取得します。

レポート タスクに検索情報を入力するには、[検索]タブをクリックして、検索画面を選択します。

注: すべてのレポートには、関連付けられた検索画面があります。 レポートに適した検索画面が見つからない場合、新しい検索画面を作成します。 レポートの検索画面の新規作成の詳細については、「レポートの検索画面の作成 (329 ページ)」を参照してください。

レポート タスク用の検索画面の新規作成

レポート検索画面は、デフォルトの[Report Type Selection]画面をベースにしています。

レポート用の検索画面を作成する方法

1. [参照]をクリックして検索画面を検索します。

   利用可能な検索画面のリストが表示されます。

2. [新規]をクリックします。

   [画面の作成]ペインが表示されます。

3. リストから[レポート テンプレート選択画面]を選択し、[OK]をクリックします。

   CA Identity Manager がレポート サーバに接続され、すべてのレポートが表示されます。

4. 以下のフィールドに値を入力します。

   名前

   レポートの名前を定義します。 各レポート タスクには、一意の名前を使用する必要があります。

   タグ

   タスク内で一意の識別子です。 タグには、ASCII 文字(a ～ z、A ～ Z)、数字(0 ～ 9)、またはアンダースコアを含めることが可能で、1 字目には文字かアンダースコアを使用します。

   [役職]

   新しい検索画面のタイトルを定義します。 一意のタイトルを使用する必要があります。

   レポート テンプレート

   検索画面に関連付けるレポートを識別します。

   注: レポート サーバに追加したレポートのうちの 1 つを選択します。

   レポート用接続オブジェクト

   レポートで使用するデータ ソースの接続の詳細を定義します。

   レポート用の新しい検索画面が作成されます。

5. [OK]をクリックします。

レポート タスクの[タブ]タブ

タスクの実行に必要なフィールドを整理するためのタブです。 レポートの[タブ]タブでは、レポートをスナップショット定義と関連付けて、レポート スケジューラを利用可能にします。

レポート タスクの[タブ]タブを設定する方法

1. タブをクリックします。

   ユーザに対して表示されるタブが表示されます。

2. [標準タブ コントローラ]を選択します。

3. 以下のいずれかの操作を行います。

   - レポートでスナップショット定義を使用する場合、以下の手順を実行します。

     a. [このタスクで表示する必要があるのはどのタブですか?]から[スナップショット定義の関連付け]を選択します。

        タブのリストに[スナップショット定義の関連付け]タブが追加されます。

     b. をクリックして、[スナップショット定義の関連付け]タブを編集します。

        [Configure Associate Snapshot Definitions]画面が表示されます。

     c. [追加]をクリックして、レポート タスクをスナップショット定義に関連付けます。

        利用可能な スナップショット定義(304 ページ)が表示されます。

     d. [スナップショット定義]を選択して、[OK]をクリックします。

        レポート タスクがスナップショット定義と関連付けられます。

   - レポートでスナップショット定義を使用しない場合、以下の手順を実行します。

     [このタスクで表示する必要があるのはどのタブですか?]から[レポート サーバ スケジューラ]を選択します。

     タブのリストに［スケジューラ］タブが追加されます。

4. [送信]をクリックします。

   レポート タスクが作成されます。

5. 管理ロールに、新規作成されたレポート タスクを割り当てます。

   管理ロールの一部として指定された Identity Manager ユーザは、新規作成されたレポート タスクを使用できます。

デフォルトのレポート

CA Identity Manager には、ニーズに合わせてカスタマイズできるデフォルトのレポートがインストールされています。 デフォルトのレポートは、以下のディレクトリにあります。

MSSQL

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexport\ReportDefinitions\CR11\Ms-SQL Reports

Oracle

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\imrexport\ReportDefinitions\CR11\Oracle Reports

以下の表では、デフォルトのレポートについて説明します。

レポート	[説明]
アカウント詳細	関連付けられたプロビジョニング ロール、エンドポイント タイプ、エンドポイント、およびアカウントのアカウント テンプレートのリストが表示されます。
Administration	管理者とそれに対応する管理者権限のリストが表示されます。
監査 - プロビジョニング ロールの割り当て/取り消し	プロビジョニング ロールのイベントのリストが表示されます。
監査-プロビジョニング取り消し	プロビジョニングが取り消されたユーザとそのアカウントのリストが表示されます。
監査詳細	タスクとイベントが、関連するステータス詳細とともに表示されます。
監査-承認待ちタスク	承認待ちのタスクのリストが表示されます。
監査-パスワードのリセット	指定の期間リセットされていたユーザのパスワードのリストが表示されます。
エンドポイント アカウント	各エンドポイントのアカウントが表示されます(表示するエンドポイントを選択できます)。
エンドポイント詳細	エンドポイント タイプ、エンドポイント、およびエンドポイント属性のリストが表示されます。
非標準アカウント	孤立アカウント、システム アカウント、および例外アカウントがすべて表示されます。

レポート	[説明]
非標準アカウントの傾向	孤立アカウント、システム アカウント、および例外アカウントなどの非標準アカウントの傾向が表示されます。
孤立アカウント	プロビジョニング サーバにグローバル ユーザがないエンドポイント アカウントがすべて表示されます。
ポリシー	アイデンティティ ポリシーがすべて表示されます。
ロール管理者	ロールとロールの管理者が表示されます。
ロール メンバ	レポート データベースのロールと、それらのロールのメンバ リストが表示されます。
ロール所有者	ロールとロールの所有者が表示されます。
ロール	レポート データベースの各ロールに関する以下の情報が表示されます。 ■ ロールに関連付けられているタスク ■ メンバ ポリシーとロール メンバ ■ 管理者ポリシーとロールの管理者 ■ 所有者ポリシーとロールの所有者
スナップショット	エクスポートされたスナップショットがすべて表示されます。
タスク ロール	レポート データベースのタスクと、それらが関連付けられているロールが表示されます。
ユーザ アカウント	ユーザとそのアカウントのリストが表示されます。 **注**: このレポートに表示されるアカウント属性のリストは、エクスポートされる属性ごとに異なります。
ユーザ権限	ユーザのロール、グループ、およびアカウントが表示されます。 **注**: このレポートに表示されるアカウント属性のリストは、エクスポートされる属性ごとに異なります。
ユーザ ポリシー同期ステータス	ポリシー(割り当てられるポリシー、割り当て解除されるポリシー、または再割り当てされるポリシー)ごとのユーザのステータスが表示されます。

レポート	［説明］
ユーザのプロファイル	ユーザに関する以下の情報が表示されます。 ■ 名前 ■ ［ユーザ ID］ ■ ユーザがメンバまたは管理者であるグループ ■ ユーザがメンバ、管理者、または所有者であるロール
ユーザ ロール	ユーザに割り当てられたロールが表示されます。

第 17 章: ワークフロー

このセクションには、以下のトピックが含まれています。

ワークフローの概要 (335 ページ)
ワークフローを有効にする方法 (339 ページ)
WorkPoint 管理ツールの設定 (339 ページ)
WorkPoint Designer の開始 (344 ページ)
テンプレート メソッド (345 ページ)
WorkPoint メソッド (364 ページ)
Workpoint ジョブの表示 (389 ページ)
ポリシーベース ワークフロー (392 ページ)
オンライン リクエスト (400 ページ)
ワークフロー アクション ボタン (404 ページ)
ワーク リストと作業アイテム (409 ページ)

ワークフローの概要

CA Identity Manager ワークフロー機能では、ワークフロー プロセスで Identity Manager タスクを制御することができます。 ワークフロー プロセスは、CA Identity Manager がワークフロー制御下のタスクを完了するまでに実行する必要のある 1 つ以上の手順です。 ジョブとは、ワークフロー プロセスのランタイム インスタンスを指します。

WorkPoint Designer は、Planet Group, Inc の一部門である Workpoint LLC 製作のソフトウェアで、Identity Manager に統合されています。 WorkPoint Designer では、ワークフロー プロセスおよびワークフロー ジョブを管理できます。

ワークフロー プロセスは、アクティビティと呼ばれる 1 つ以上のプロセスで構成されており、従業員ユーザ アカウントの作成や変更といったビジネス タスクを遂行するために実行する必要があります。 通常、ワークフロー プロセスには、タスクの承認または拒否を行うために、権限を持つユーザまたは参加者が必要となる手動アクティビティが 1 つ以上含まれています。

参加者は、ワークフロー アクティビティを実行する権限を持つ個人です。 CA Identity Manager では、ワークフロー制御下のタスクを承認または拒否する必要があるため、参加者は承認者と呼ばれることもあります。 参加者リゾルバは、参加者を決定するルールまた基準のセットです。

ワークフローの個別の手動アクティビティは、CA Identity Manager では作業アイテムと呼ばれます。

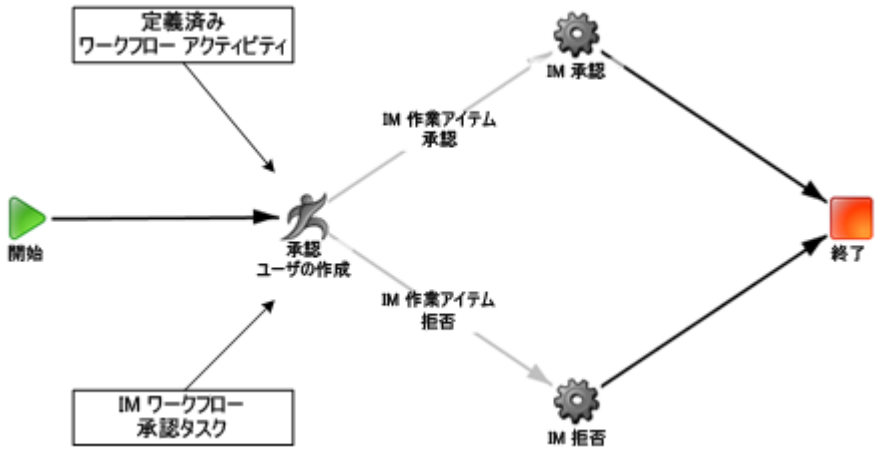
ワーク リストは、ワークフローが生成する許可タスク(作業アイテム)のリストであり、このタスクを承認する権限を持つ参加者のユーザ コンソールに表示されます。

WorkPoint プロセス図

通常、Identity Manager タスクは Identity Manager イベントをトリガします。 たとえば、ユーザを作成するために、管理者が[ユーザの作成]タスクを選択します。 このタスクが開始されると、イベント CreateUserEvent がトリガされます。

以下の図は、WorkPoint Designer に表示される、単純なワークフロー プロセス(事前定義済みのプロセス CreateUserApproveProcess)の例です。 [ユーザの作成]タスクがワークフロー制御下にある場合、このプロセスは CreateUserEvent により起動されます。

このプロセスには、手動アクティビティ [ユーザ作成を承認] が含まれています。これは、同じ名前である Identity Manager ワークフロー承認タスクに対応します。 参加者は、ワークフロー制御下のタスクの実行が完了するまでに、通常、ユーザ コンソールのボタンをクリックして承認タスクを承認または拒否する必要があります。



ワークフローと電子メール通知

タスクを開始すると、CA Identity Manager によりタスクがサブミットされ、以下のような確認メッセージが処理および表示されます。

確認: タスクが完了しました。

ただし、このタスクがワークフロー制御下にあり、承認が必要な場合は、このメッセージは以下のようになります。

アラート: タスクはペンディングです。

画面上のメッセージに加えて、以下の場合に CA Identity Manager により電子メール通知が自動的に生成されます。

- ワークフロー承認者による承認または拒否が必要なイベントまたはタスクが保留中である場合
- 承認者がイベントまたはタスクを承認する場合
- 承認者がイベントまたはタスクを拒否する場合
- イベントまたはタスクが完了した場合

詳細情報:

電子メール通知(421 ページ)

WorkPoint のマニュアル

ワークフローの概念の一般的な情報、および WorkPoint Designer でのワークフロープロセス、アクティビティ、およびジョブの詳細については、WorkPoint のマニュアルを参照してください。 このマニュアルを参照するには、以下の HTML ページを開きます。

admin_tools\WorkPoint\docs\designer\default.htm

admin_tools

Identity Manager 管理ツールのインストール ディレクトリを決定します。 デフォルトのインストール ディレクトリは以下のとおりです。

- Windows: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

Workflow の制御メソッド

CA Identity Manager には、ワークフロー制御下でタスクを配置するための 2 つのメソッドがあります。

テンプレート メソッド

CA Identity Manager には、ワークフロー制御下にタスクを配置するために使用できるワークフロー プロセス テンプレートがあります。 テンプレート メソッドでは、テンプレートを使用して、ユーザ コンソール内のワークフローをすべて設定および管理できます。 CA Identity Manager r12 に導入された、こうした一般的なプロセス テンプレートを設定すると、ほとんどの Identity Manager のタスクとイベントを制御できます。

テンプレート メソッドは以下のような新しい機能を有効にします。

- タスク レベルとイベント レベル両方のワークフロー制御
- ワークフロー承認者の参加者リゾルバ設定の簡略化
- 作業アイテムの委任。これにより、ユーザが別のユーザに作業アイテムの承認を委任することが可能となり、「外出中」のシナリオに対応できます。
- 作業アイテムの再割り当て。これにより、実行中のタスクを承認のため別のユーザに再度割り当てることができます。

WorkPoint メソッド

CA Identity Manager には、特定の Identity Manager タスクに対応するデフォルトのイベント マッピングを含む事前定義済みのワークフロー プロセスのセットがあります。 WorkPoint メソッドでは、WorkPoint Designer 内でこれらのプロセスの設定およびカスタマイズを行う必要があります。 これらの事前定義済みのプロセスは、CA Identity Manager r12 より前のリリースと互換性があります。

WorkPoint メソッドは以下のような新しい機能も有効にします。

- タスク レベルとイベント レベル両方のワークフロー制御
- 作業アイテムの委任。これにより、ユーザが別のユーザに作業アイテムの承認を委任することが可能となり、「外出中」のシナリオに対応できます。
- 作業アイテムの再割り当て。これにより、実行中のタスクを承認のため別のユーザに再度割り当てることができます。

注: 柔軟性と使い勝手の向上のため、できるだけテンプレート メソッドを使用することをお勧めします。

詳細情報:

テンプレート メソッド (345 ページ)
WorkPoint メソッド (364 ページ)

ワークフローを有効にする方法

ワークフローを使用して Identity Manager タスクを制御する前に、ワークフローを有効にする必要があります。 デフォルトでは、ワークフローは無効になっています。

ワークフローを有効化する方法

1. 管理コンソールで[環境]を選択します。
2. [詳細設定]-[ワークフロー]の順に進みます。
3. [有効]チェック ボックスをオンにし、[保存]をクリックします。

   注: この画面のイベント マッピングは、WorkPoint メソッドを使用してワークフローを設定している場合のみ適用されます。 テンプレート メソッド(推奨)を使用する場合は、この管理コンソールを使用してイベントをマッピングして処理しないでください。
4. アプリケーション サーバを再起動します。
5. (オプション)WorkPoint 管理ツールを設定(339 ページ)します。

詳細情報:

Workflow の制御メソッド(338 ページ)
グローバル レベルでのプロセスとイベントのマッピング(367 ページ)

WorkPoint 管理ツールの設定

WorkPoint Designer は、Planet Group, Inc の一部門である Workpoint LLC 製作のソフトウェアで、Identity Manager に統合されています。 WorkPoint Designer では、ワークフロー プロセスおよびワークフロー ジョブを管理できます。 WorkPoint 管理ツールには、WorkPoint Designer と WorkPoint Archive が含まれています。 WorkPoint 管理ツールを設定するには、Identity Manager 管理ツールをインストールします。 Identity Manager 管理ツールをインストールしない場合、インストーラを実行して、[Identity Manager 管理ツール]オプションを選択します。

注: 管理ツールをワークフローに使用するには、管理ツールがインストールされているシステムにサポート対象 JDK がインストールされている必要があります。 サポート対象のプラットフォームとバージョンの詳細な一覧については、CA Identity Manager のサポート サイトで「CA Identity Manager サポート マトリックス」を参照してください。

ワークフロー クライアント ツールは、Identity Manager 管理ツールの WorkPoint ディレクトリにあります。 管理ツールは、以下のデフォルトの場所に配置されます。

- Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

このディレクトリのツールにより、次のことが行えます。

- ワークフロー データベース スキーマの作成
- デフォルト ワークフロー スクリプトのロード
- ワークフロープロセスとジョブの設計と監視

JBoss における WorkPoint Administrative Tool の設定

JBoss で WorkPoint 管理ツールを設定するには、init.bat/sh ファイルおよび workpoint-client.properties ファイルを編集します。

init.bat/init.sh の編集

init.bat/init.sh を編集する方法

1. テキスト エディタで、次のファイルのいずれかを編集します。
   - Windows の場合

     admin_tools¥Workpoint¥bin¥init.bat
   - UNIX の場合

     admin_tools/Workpoint/bin/init.sh
2. JBoss 4.2.2 アプリケーション サーバのセクションの次の行のコメント記号を削除します。
   - Windows の場合

     SET EJB_CLASSPATH=..¥lib¥jbossall-client.jar;..¥lib
   - UNIX の場合

     EJB_CLASSPATH=../lib/jbossall-client.jar;../lib

   注: 他のアプリケーション サーバのセクションはすべてコメントになっていることを確認します。
3. jbossall-client.jar を jboss_home¥client¥ から次の場所にコピーします。

   admin_tools¥Workpoint¥lib

workpoint-client.properties の編集

CA Identity Manager インストール中に選択したアプリケーション サーバの種類に応じて workpoint-client.properties ファイルを編集します。

workpoint-client.properties ファイルを設定する方法

1. admin_tools¥Workpoint¥conf¥
   workpoint-client.properties をテキスト エディタで開きます。

   admin_tools は管理ツールがインストールされている場所を示します。 管理ツールが配置されるデフォルトの場所は以下の通りです。

   - Windows: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

2. JBOSS SETTINGS というタイトルのセクションを探します。
3. そのセクションのプロパティ値すべてのコメント記号を削除します。

   以下に例を示します。

   java.naming.provider.url=localhost
   java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
   java.naming.factory.url.pkgs=org.jboss.naming

   注: java.naming.provider.url property 値を編集しなければならない場合があります。 たとえば、localhost を jnp://server_name または ip:port に置き換えます。 jnp ポート番号 1099 を使用していることを確認します。
4. ファイルを保存します。

WebLogic における WorkPoint 管理ツールの設定

WebLogic で WorkPoint 管理ツールを設定するには、init.bat/sh ファイルおよび workpoint-client.properties ファイルを編集します。

init.bat/init.sh の編集

init.bat/init.sh を編集する方法

1. テキスト エディタで、次のファイルのいずれかを編集します。
   - Windows の場合

     admin_tools¥Workpoint¥bin¥init.bat
   - UNIX の場合

     admin_tools/Workpoint/bin/init.sh
2. WebLogic アプリケーション サーバのセクションで、次の行のコメント記号を削除します。
   - Windows の場合

     SET EJB_CLASSPATH=.¥lib¥wlclient.jar
   - UNIX の場合

     EJB_CLASSPATH=./lib/wlclient.jar

   注: 他のアプリケーション サーバのセクションはすべてコメントになっていることを確認します。
3. weblogic_home¥server¥lib から次の場所に wlclient.jar ファイルをコピーします。

   admin_tools¥Workpoint¥lib¥

workpoint-client.properties の編集

CA Identity Manager のインストール時に選択したアプリケーション サーバの種類に応じて workpoint-client.properties ファイルを編集する必要があります。

workpoint-client.properties ファイルを設定する方法

1. admin_tools¥Workpoint¥conf¥
   workpoint-client.properties をテキスト エディタで開きます。
2. BEA WEBLOGIC というタイトルのセクションを探します。
3. そのセクションのプロパティ値すべてのコメント記号を削除します。

   以下に例を示します。

   java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory
   java.naming.provider.url=t3://im_server:port
   java.naming.security.principal=IDM
   java.naming.security.credentials=password
4. ファイルを保存します。

   注: java.naming.provider.url プロパティは、Identity Manager Server をインストールしたシステムの完全修飾ドメイン名および WebLogic ポート番号を参照する必要があります。

WebSphere における WorkPoint 管理ツールの設定

WebSphere で WorkPoint 管理ツールを設定するには、init.bat/sh ファイルおよび workpoint-client.properties ファイルを編集します。

init.bat/init.sh の編集

init.bat/init.sh を編集する方法

1. テキスト エディタで、次のファイルのいずれかを編集します。
   - Windows の場合

     admin_tools¥Workpoint¥bin¥init.bat
   - UNIX の場合

     admin_tools/Workpoint/bin/init.sh
2. IBM WebSphere 6.1.0.7 アプリケーション サーバのセクションで、以下の行をコメント解除します。

   注:以下の行は init.bat にあります。 init.sh でこれに対応する行は、多少異なっています。

   ```
   SET JAVA_HOME=C:\WebSphere\AppServer\java\jre
   SET WAS_HOME=C:\WebSphere\AppServer
   SET
   WAS_EXT_DIRS=%JAVA_HOME%\lib;%JAVA_HOME%\lib\ext;%WAS_HOME%\classes;%WAS_HOME%\lib;%WAS_HOME%\lib\ext;%WAS_HOME%\properties
   SET WAS_BOOTCLASSPATH=%JAVA_HOME%\lib\ext\ibmorb.jar;%WAS_HOME%\properties
   SET PATH=%JAVA_HOME%\bin
   SET JAVAXPARMS=-Xbootclasspath/p:%WAS_BOOTCLASSPATH%
   SET JAVADPARMS=-Djava.ext.dirs=%WAS_EXT_DIRS%
   SET WP_CLASSPATH=./lib/wpClient_ibm.jar;%WP_CLASSPATH%
   ```

   注: COMMON WP_CLASSPATH セクションの WP_CLASSPATH エントリをコメントにしないでください。
3. 必要に応じて、ご使用の環境での適切なパス JAVA_HOME と WAS_HOME の値を置き換えてください。

workpoint-client.properties の編集

CA Identity Manager のインストール時に選択したアプリケーション サーバの種類に応じて workpoint-client.properties ファイルを編集する必要があります。

workpoint-client.properties ファイルを設定する方法

1. admin_tools¥Workpoint¥conf¥
   workpoint-client.properties をテキスト エディタで開きます。

   admin_tools は管理ツールがインストールされている場所を示します。 管理ツールは、以下のデフォルトの場所に配置されています。

   - Windows: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

2. IBM WEBSPHERE SETTINGS というタイトルのセクションを探します。
3. そのセクションのすべてのプロパティ値をコメント解除します。

   たとえば、次のようにします。

   java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory
   java.naming.provider.url=iiop://localhost:bootstrap_port

   注:ブートストラップ ポート番号は、WebSphere 管理コンソールに指定したポート番号に合致する必要があります。 正しいポート番号を知るには、[サーバ]-[エンドポイント]-[ブートストラップ サーバのアドレス]をクリックします。
4. 以下の手順に従い、WebSphere プロファイルの BOOTSTRAP_ADDRESS ポートを更新します。
   a. WebSphere 管理コンソールで、[アプリケーション サーバ]-[server_name]-[通信]をクリックします。
   b. [ポート]を展開します。
   c. IdentityMinder.ear/config にある workpoint-client.properties ファイルを編集します。
   d. WebSphere セクションのデフォルト ポート 2809 をプロファイルの BOOTSTRAP_ADDRESS のポートに変更します。
5. ファイルを保存します。

WorkPoint Designer の開始

WorkPoint Designer を開始するには、以下のファイルを実行します。

- Windows: admin_tools\WorkPoint\bin\Designer.bat
- UNIX: admin_tools/WorkPoint/bin/Designer.sh

admin_tools は、Identity Manager 管理ツールのインストール ディレクトリです。 管理ツールは、以下のデフォルトの場所に配置されます。

- Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools

注: WorkPoint Designer を実行する前に、ワークフロー コンポーネントをインストールして設定しておく必要があります。 詳細については、お使いのアプリケーション サーバの「WorkPoint 管理ツールの設定」を参照してください。

詳細情報:

JBoss における WorkPoint Administrative Tool の設定 (340 ページ)
WebLogic における WorkPoint 管理ツールの設定 (341 ページ)
WebSphere における WorkPoint 管理ツールの設定 (343 ページ)

テンプレート メソッド

CA Identity Manager r12 に導入されたテンプレート メソッドでは、WorkPoint Designer を開かずに、ユーザ コンソールでワークフロー プロセス テンプレートを設定できます。

テンプレート メソッドの利点は以下のとおりです。

- 複数の段階のプロセス テンプレートにより、ほとんどのワークフロー ニーズに対応できます。WorkPoint Designer 内でのカスタマイズは不要です。
- テンプレートでは、タスク レベルとイベント レベル両方のワークフロー制御をサポートします。
- 同じワークフロー プロセス テンプレートは、プロセス デザイン自体は変更することなく、多くのさまざまなタスクに使用できるように設定できます。
- 参加者リゾルバは、ユーザ コンソールで簡単に指定できます。
- 作業アイテムの委任をユーザ コンソールで実行できます。

プロセス テンプレート

ワークフロー プロセス テンプレートには以下の特徴があります。

- WorkPoint Designer で定義される。
- 手動アクティビティであり、Identity Manager の承認タスクに対応する。
- 参加者(承認者とも呼ばれる)を識別する情報を含む特別な属性が含まれている。

ワークフロー プロセス テンプレートには、特定の参加者を選択する情報は含まれていません。 これは、ユーザがワークフローおよびワークフローの参加者リゾルバを設定した後に CA Identity Manager によって提供されます。 この情報は、イベント レベルのワークフロー制御のイベント、およびタスク レベルのワークフロー制御のタスクにマッピングされます。

テンプレート メソッドを使用すると、ワークフローおよび参加者の設定はすべてユーザ コンソール内で行われます。

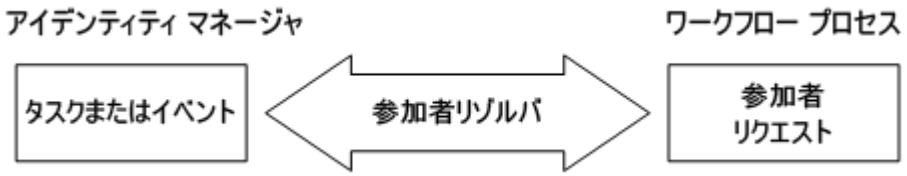
テンプレート メソッドを使用するプロセス テンプレートは以下の 2 種類です。

- SingleStepApproval
- TwoStageApprovalProcess

プロセス テンプレートの動作方法

ワークフロー プロセス テンプレートには、参加者リストが必要となる場所が多く含まれています。 テンプレートが Identity Manager のタスクまたはイベントにマッピングされると、これらのリストの参加者リゾルバを設定する必要があります。

実行時には、以下の図に示すように、設定情報に基づく参加者リストが CA Identity Manager によりワークフロー プロセスに表示されます。

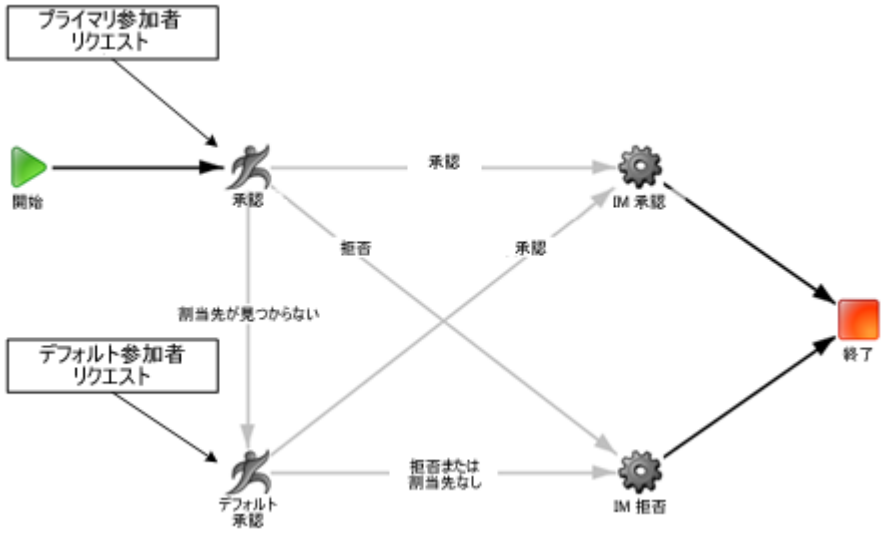


1 つの段階のテンプレートの図

以下の図は、WorkPoint Designer に表示される、SingleStageApproval プロセス テンプレートを示しています。 プロセス テンプレートには、以下の 2 つの手動アクティビティがあります。

- プライマリ参加者の承認ノード。 このユーザがリクエストを承認または拒否すると、プロセスを実行して完了します。

- デフォルト参加者の承認ノード。 プライマリ参加者が見つからない場合に、このユーザはリクエストを承認または拒否できます。

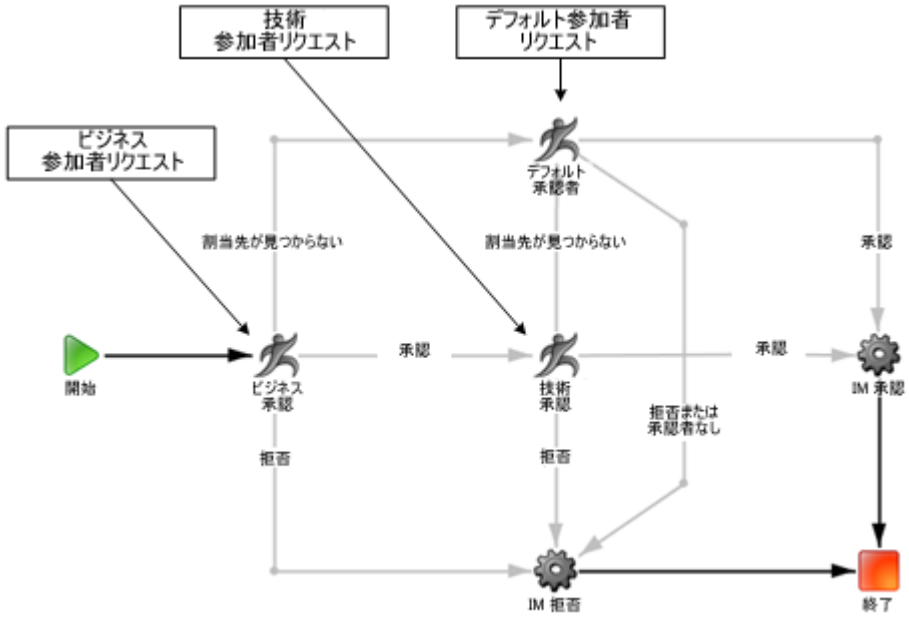


2 つの段階のテンプレートの図

以下の図は、WorkPoint Designer に表示される、TwoStageApproval プロセス テンプレートを示しています。 TwoStageApproval プロセス テンプレートには、以下の 3 つの手動アクティビティがあります。

- ビジネス参加者の承認ノード。 このユーザがリクエストを承認すると、技術系承認者によるプロセスに進みます。このユーザがリクエストを拒否すると、プロセスは完了します。
- 技術参加者の承認ノード。 このユーザがリクエストを承認または拒否すると、プロセスを実行して完了します。

- デフォルト参加者の承認ノード。 ビジネス参加者または技術参加者が見つからない場合に、このユーザはリクエストを承認または拒否できます。



プロセス テンプレートの属性

テンプレート メソッドをサポートするワークフロー プロセスには、以下の特別なユーザ データ属性があります。

PARTICIPANT_ID

参加者リクエストの一意のキーを指定します。 設定がない場合、ノードは参加者リクエストと見なされません。

PARTICIPANT_NAME

リクエストのわかりやすい名前を指定します。 この属性には、テキスト文字列またはローカライゼーション キーを指定できます。 設定がない場合、WorkPoint ノードが代わりに使用されます。

PARTICIPANT_DESCRIPTION

リクエストの詳細な説明を指定します。 この属性には、テキスト文字列またはローカライゼーション キーを指定できます。 設定がない場合、WorkPoint ノードの説明が代わりに使用されます。

注: これらの属性は、WorkPoint Designer の手動アクティビティ プロパティで定義されます。 参加者リゾルバがユーザ コンソールで設定されると、属性値が作成されます。

テンプレート メソッドの使用方法

このセクションでは、テンプレート メソッドを使用してワークフロー制御下に管理タスクを配置する高レベルの手順を説明しています。

テンプレート メソッドの使用

1. ユーザ コンソールで、ワークフロー制御下で行うタスクの[管理タスクの変更]または[管理タスクの作成]を開きます。
2. タスク レベルのワークフローを実装するには、以下の手順に従います。
   a. [プロファイル]タブで、[ワークフロー プロセス]ボタンをクリックします。
   b. タスク レベルのワークフローの設定タブから、プロセス テンプレートを選択して参加者リゾルバを設定します。
3. イベント レベルのワークフローを実装するには、以下の手順に従います。
   a. [イベント]タブから、イベントを 1 つ以上選択します。
   b. イベント レベルのワークフローの設定タブから、プロセス テンプレートを選択して参加者リゾルバを設定します。
4. ワークフロー制御が設定されたら、適切なロールを持つユーザが管理タスクを実行します。
5. 指定されたワークフロー参加者が、タスクまたはイベントを承認または拒否します。

詳細情報:

イベント レベルのワークフロー (352 ページ)
タスク レベルのワークフロー (350 ページ)
参加者リゾルバ: テンプレート メソッド (356 ページ)

タスクおよびイベント

CA Identity Manager では、ワークフロー プロセスをタスクまたはイベントのいずれかに関連付けることができます。 これは、参加者が Identity Manager のタスク全体またはタスク内の特定のイベントのいずれかを承認または拒否できることを意味します。

たとえば、Identity Manager のタスクが複数のイベントを生成するため、承認者がリクエストの承認または拒否を決定する前にすべてのイベントを確認する必要がある場合があります。 これは、タスク レベルのワークフローで実行可能です。 ワークフロー プロセスが特定のイベントに関連付けられている場合、承認者は、リクエストが行われたタスク全体の状況を確認できません。

タスク レベルのワークフロー

タスク レベルのワークフローでは、承認者がリクエストの承認または拒否を決定する前にすべてのイベントを確認できます。

タスク レベルのワークフローは、タスク アクティビティが処理される前に発生します。ワークフロー プロセス ジョブが開始するまで、イベントまたはネストされたタスクは実行されません。

タスク レベルのワークフローが拒否されると、タスクのいずれの部分も実行されません。

[管理タスクの変更]または[管理タスクの作成]の[プロファイル]タブで、タスク レベルのワークフロー マッピングと参加者リゾルバを設定します。

注: タスク レベルのワークフロー制御で設定されたタスクは、イベント レベルのワークフロー コントロールでも同時に設定することができます。 同時に設定可能なイベント レベルのワークフローは、全体に適用することも、特定のタスクに適用することもできます。

詳細情報

イベント レベルのワークフロー (352 ページ)
プロセスとイベントのグローバル マッピング (366 ページ)

タスク レベルのプロセス属性

タスク レベルのワークフローと互換性があるワークフロー プロセスはすべて、WorkPoint Designer 内で定義された特別な属性があります。 TASK_LEVEL と呼ばれるこのプロセス レベルのユーザ データ属性は、以下のプロセス テンプレートではデフォルトで true に設定されます。

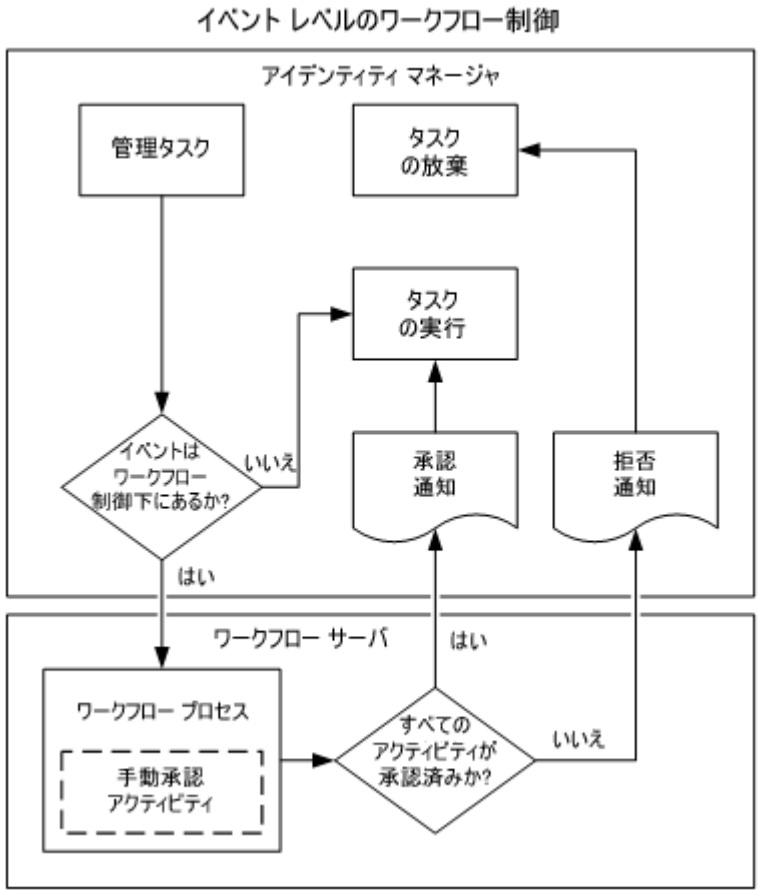
- SingleStepApproval
- TwoStageApprovalProcess

タスク レベルのワークフローの管理タスクを選択すると、 上記のプロセス テンプレートのみが使用できます。

注: TASK_LEVEL が true に設定されている場合も、イベント レベルのワークフローでプロセス テンプレートを使用できます。 この TASK_LEVEL の属性値を変更しないでください。

タスク レベル制御の図

以下の図は、一般的なタスク レベルのワークフロー プロセスが開始されたときの CA Identity Manager とワークフロー サーバの間の対話を示しています。



詳細情報:

イベント レベル制御の図 (354 ページ)

タスク レベルのワークフローの設定方法

タスク レベルのワークフローは、タスク アクティビティが処理される前に発生します。ワークフロー プロセス ジョブが開始するまで、イベントまたはネストされたタスクは実行されません。

タスク レベルのワークフローの設定方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]または[管理タスクの作成]を選択します。

   [管理タスクの選択]画面が表示されます。

2. ワークフロー制御下で実行するタスクを検索して、[選択]をクリックします。

   [管理タスクの変更]または[管理タスクの作成]画面が表示されます。

3. [プロファイル]タブで、[ワークフローの有効化]がチェックされているかどうかを確認します。

4. [プロファイル]タブで、[ワークフロー プロセス]ボタンをクリックします。

   [タスク レベル ワークフロー設定]タブが表示されます。

5. [ワークフロー プロセス]リストから、以下のプロセス テンプレートのいずれかを選択します。

   - SingleStepApproval
   - TwoStageApprovalProcess

   [タスク レベル ワークフロー設定]タブが展開されます。

6. プロセス テンプレートで必要に応じて参加者リゾルバを設定します。

   参加者のリクエストがプロセスに追加されます。

7. [OK]をクリックします。

   CA Identity Manager によってタスク レベルのワークフロー設定が保存されます。

8. [送信]をクリックします。

   CA Identity Manager によってタスクの変更が処理されます。

詳細情報:

参加者リゾルバ: テンプレート メソッド (356 ページ)

イベント レベルのワークフロー

Identity Manager のイベントは、ワークフロー プロセスにマッピングすることができます。ワークフロー プロセスにマッピングしたイベントがトリガされると、ワークフロー プロセスが開始します。 イベントをトリガしたタスクは保留状態になり、ワークフローの制御下に置かれます。

ワークフロー プロセスでは、プロセスが完了する前に Identity Manager 参加者がイベントまたはタスクを承認または拒否することが必要なことがあります。 参加者による手動のワークフロー承認が必要なタスクは、ワークフロー制御下のタスクよりも完了するまでに時間がかかります。

ワークフロー プロセスのすべてのアクティビティが実行されると、そのワークフロー プロセスにマッピングされたイベントはワークフロー制御から解放されます。 特定のタスクでトリガされたすべてのイベントがワークフロー制御から解放されると、ワークフローで制御されているタスクが完了します。

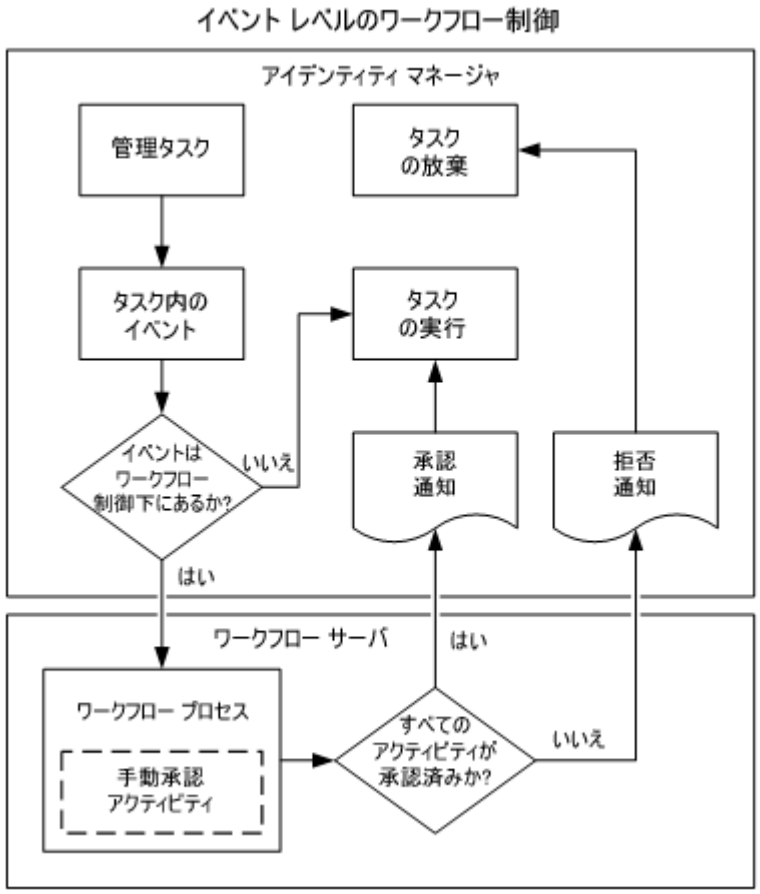
タスクがワークフロー制御下にある場合は、タスク画面の内容はタスクの持続的なデータベースに保存されます。 ワークフロー ジョブの状態(ワークフロー関連のデータ)は WorkPoint データベースに保存されます。

[管理タスクの変更]または[管理タスクの作成]の[イベント]タブで、イベント レベルのワークフロー マッピングと参加者リゾルバを設定します。

注: [イベント]タブでは、タスクの各タブで生成されたイベントを一覧で表示します。 タスクに新しいタブを追加した後、[イベント]タブに新しいイベントが表示される前に、[管理タスクの変更]を使用してタスクをサブミットし再開する必要があります。

イベント レベル制御の図

以下の図は、一般的なイベント レベルのワークフロー プロセスが開始されたときの CA Identity Manager とワークフロー サーバの間の対話を示しています。



詳細情報:

タスク レベル制御の図 (351 ページ)

イベント レベルのワークフローの設定方法

ワークフロー プロセスにマッピングされるイベントがトリガされると、イベント レベルのワークフローが開始します。 イベントをトリガしたタスクは、参加者がタスクを承認または拒否するまで保留状態に置かれます。

イベント レベルのワークフローの設定方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]または[管理タスクの作成]を選択します。

   [管理タスクの選択]画面が表示されます。

2. ワークフロー制御下で実行するタスクを検索して、[選択]をクリックします。

   [管理タスクの変更]または[管理タスクの作成]画面が表示されます。

3. [プロファイル]タブで、[ワークフローの有効化]がチェックされているかどうかを確認します。

4. [イベント]タブで、イベントを選択して、プロセス テンプレートにマッピングします。

   ワークフローのマッピングの画面が表示されます。

5. [ワークフロー プロセス]リストから、以下のプロセス テンプレートのいずれかを選択します。

   - SingleStepApproval
   - TwoStageApprovalProcess

   ワークフローのマッピングの画面が展開されます。

6. プロセス テンプレートで必要に応じて参加者リゾルバを設定します。

   参加者のリクエストがプロセスに追加されます。

7. [OK]をクリックします。

   CA Identity Manager によってイベント レベルのワークフロー設定が保存されます。

8. ワークフロー制御下に置くイベントごとに手順 3 から 6 を繰り返します。

9. [送信]をクリックします。

   CA Identity Manager によってタスクの変更が処理されます。

注: ワークフロー プロセス リストには、テンプレート メソッドと WorkPoint メソッドの両方で使用するプロセスが含まれています。

- テンプレート メソッド(SingleStepApproval または TwoStageApprovalProcess のいずれか)が選択されると、ページが展開されて、参加者リゾルバの設定が有効になります。
- WorkPoint method が選択されると、このページは展開されません。 参加者リゾルバは WorkPoint Designer で設定されます。

詳細情報:

参加者リゾルバ: テンプレート メソッド(356 ページ)

参加者リゾルバ: テンプレート メソッド

プロセス テンプレート メソッドを使用して参加者を指定するには、ユーザ コンソールで以下のアクティビティ プロパティを定義します。

- 承認タスクの名前
- 参加者リゾルバのタイプ
- 参加者リゾルバにより必要となる追加情報

参加者リゾルバは、以下のユーザ コンソール画面で設定されます。

タスク レベル ワークフロー

ワークフロー設定画面。[管理タスクの変更]または[管理タスクの作成]の[プロファイル]タブから選択します。

イベント レベル ワークフロー

ワークフローのマッピング画面。[管理タスクの変更]または[管理タスクの作成]の[イベント]タブから選択します。

参加者リゾルバのタイプ

テンプレート メソッドでは、以下の 7 つのタイプの参加者リゾルバがあります。

Approval Task Role Members(承認タスクのロール メンバ)

参加者は、承認タスクへのアクセス権が付与されるロールのメンバであることを指定します。

ユーザ リスト

参加者は、指定したユーザのリストであることを指定します。

グループ メンバ

参加者は、指定したグループのリストのメンバであることを指定します。

管理ロール メンバ

参加者は、指定した管理ロールのリストのメンバであることを指定します。

Admin Task Members（承認タスク メンバ）

参加者は、指定した管理タスクのリストに関連付けられた管理ロールのメンバであることを指定します。

動的リゾルバ

参加者は、承認されるタスクまたはイベントに応じて動的に選択されることを指定します。

NULL リゾルバ

ユーザのいない null リストに解決します。

カスタム

カスタム参加者リゾルバによって、参加者が決定されることを指定します。

Approval Task Role Members（承認タスクのロール メンバ）

このリゾルバは、承認タスクへのアクセス権が付与されるすべての Identity Manager ロールのすべてのメンバにアクティビティを割り当てます。 このリゾルバには追加設定は必要ありません。

承認タスク ロール メンバのリゾルバを設定する方法

1. ユーザ コンソールのワークフロー設定画面で、[参加者リゾルバ]リストから [Approval Task Role Members（承認タスクのロール メンバ）]を選択します。

   ワークフロー設定画面は、参加者リゾルバの選択によって変わります。

2. [OK]をクリックして、参加者リゾルバの設定を保存します。

   管理タスク プロファイルのタブが再度表示されます。

3. [サブミット]をクリックし、管理タスク ワークフローの変更内容を保存します。

ユーザ リスト

このリゾルバは、指定したユーザのリストに作業アイテムを割り当てます。

スコープは実施されません。 ワークフロー設定画面へのアクセス権があれば、リストへのユーザの追加、またはリストからのユーザの削除を行うことができます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つのユーザ名を指定する必要があります。
- ユーザ名は、現在存在するユーザである必要があります。

ユーザ リスト リゾルバを設定する方法

1. ユーザ コンソールのワークフロー設定画面で、[参加者リゾルバ]リストから[ユーザ リスト]を選択します。

   ワークフロー設定画面は、参加者リゾルバの選択によって変わります。

2. [ユーザの追加]をクリックして、リストに参加者を追加します。

   ユーザ選択画面が表示されます。

3. 参加者を検索して、選択します。

   参加者がユーザ リストに追加されます。

4. [OK]をクリックして、参加者リゾルバの設定を保存します。

   管理タスク プロファイルのタブが再度表示されます。

5. [サブミット]をクリックし、管理タスク ワークフローの変更内容を保存します。

グループ メンバ

このリゾルバは、グループ リスト内で指定したすべてのグループのすべてのメンバに作業アイテムを割り当てます。

グループ メンバの評価は、参加者リゾルバが指定されるときではなく、作業アイテムが作成されるときに実行されます。

スコープは実施されません。 ワークフロー設定画面へのアクセス権があれば、リストへのグループの追加、またはリストからのグループの削除を行うことができます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つのグループ名を指定する必要があります。
- グループ名は、現在存在するグループである必要があります。

グループ メンバ リゾルバの設定

1. ユーザ コンソールのワークフロー設定画面で、[参加者リゾルバ]リストから[グループ メンバ]を選択します。

   ワークフロー設定画面は、参加者リゾルバの選択によって変わります。

2. [グループの追加]をクリックして、リストにグループを追加します。

   選択グループ画面が表示されます。

3. グループ(複数可)を検索し、選択します。

   選択したグループがグループ リストに追加されます。

4. [OK]をクリックして、参加者リゾルバの設定を保存します。

   管理タスク プロファイルのタブが再度表示されます。

5. [サブミット]をクリックし、管理タスク ワークフローの変更内容を保存します。

管理ロール メンバ

このリゾルバは、管理ロール リストで指定した管理ロールのメンバ全員に作業アイテムを割り当てます。

ロール メンバの評価は、参加者リゾルバの指定時ではなく、作業アイテムの作成時に実行されます。

スコープは実施されません。 ワークフロー設定画面にアクセスできるユーザであれば、任意のロールをリストに追加したり、リストから任意のロールを削除することができます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つの管理ロールを指定する必要があります。
- 管理ロール名は、現存する管理ロールと同じにする必要があります。

管理ロール メンバのリゾルバを設定するには

1. [User Console]ワークフロー設定画面で、[参加者リゾルバ]リストから[管理ロール メンバ]を選択します。

   ワークフロー設定画面は、参加者リゾルバの選択によって変わります。

2. [Add Admin Roles]をクリックし、リストにロールを追加します。

   ロールの選択画面が表示されます。

3. ロール(複数可)を検索し、選択します。

   選択したロールがロール リストに追加されます。

4. [OK]をクリックして、参加者リゾルバの設定を保存します。

   管理タスク プロファイルのタブが再度表示されます。

5. [サブミット]をクリックし、管理タスク ワークフローの変更内容を保存します。

管理タスク メンバ

このリゾルバは、管理タスク リストで指定した管理タスクに関連付けられた、すべての管理ロールのメンバ全員に作業アイテムを割り当てます。

スコープは実施されません。 ワークフロー設定画面にアクセスできるユーザであれば、任意のタスクをリストに追加したり、リストから任意のタスクを削除することができます。

ロール メンバの評価とタスク上に存在するロールの評価は、参加者リゾルバの指定時ではなく、作業アイテムの作成時に実行されます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つの管理タスクを指定する必要があります。
- 管理タスク名は、現存する管理タスクと同じにする必要があります。

管理タスク メンバのリゾルバを設定する方法

1. [User Console]ワークフロー設定画面で、[参加者リゾルバ]リストから[Admin Task Members(承認タスク メンバ)]を選択します。

   ワークフロー設定画面は、参加者リゾルバの選択によって変わります。

2. [管理タスクの追加]をクリックし、リストにタスクを追加します。

   タスクの選択画面が表示されます。

3. タスク(複数可)を検索し、選択します。

   選択したタスクがタスク リストに追加されます。

4. [OK]をクリックして、参加者リゾルバの設定を保存します。

   管理タスク プロファイルのタブが再度表示されます。

5. [サブミット]をクリックし、管理タスク ワークフローの変更内容を保存します。

動的リゾルバ

このリゾルバは、実行時に解決された動的ルールに従ってユーザ リストを返します。 動的ルールの制約を設定するには、以下の選択内容を使用します。

[承認者]

このタスクを承認するユーザのタイプを指定します。

注: ここにはユーザ(または承認者)を含めることのできるオブジェクトのみが表示されます。

[ユーザまたはオブジェクト]

承認者が含まれているユーザまたはオブジェクトを指定します。

- イベント関連のオブジェクト — ワークフロー制御下にあるイベント
- このタスクの開始者 — 管理タスクを開始したユーザ
- このタスクのプライマリ オブジェクト - このタスクによって作成または変更されるユーザ

［属性］

承認者が含まれている属性を指定します。

［イベント オブジェクト タイプ］

このイベントのオブジェクト タイプを指定します。

注: これは［このイベントに関連付けられるオブジェクト］を選択した場合にのみ表示されます。

NULL リゾルバ

NULL リゾルバはユーザを返しません。 ワークフロー プロセスの設計方法によっては、これによりプロセスで承認全体がスキップされる可能性があります。 NULL リゾルバに関する詳しい設定は必要ありません。

NULL リゾルバを設定するには、以下の手順に従います。

1. ［ユーザ コンソール］ワークフロー設定画面で、［参加者リゾルバ］リストから［NULL リゾルバ］を選択します。

   ワークフロー設定画面は、参加者リゾルバの選択によって変わります。

2. ［OK］をクリックして、参加者リゾルバの設定を保存します。

   管理タスク プロファイルのタブが再度表示されます。

3. ［送信］をクリックし、管理タスク ワークフローの変更内容を保存します。

カスタム参加者リゾルバ

カスタム参加者リゾルバは、ワークフロー アクティビティの参加者を決定し、リストを CA Identity Manager に返す Java オブジェクトです。CA Identity Manager は、このリゾルバから返されたリストをワークフロー エンジンに渡します。 一般に、カスタム参加者リゾルバを作成するのは、標準の参加者ポリシーではアクティビティに必要な参加者のリストを提供できない場合のみです。

注: カスタム参加者リゾルバの作成には、参加者リゾルバ API を使用します。 詳細については、「Programming Guide for Java」を参照してください。

カスタム参加者リゾルバを設定する方法

1. ［User Console］ワークフロー設定画面で、［参加者リゾルバ］リストから<リゾルバ名>を選択します。

   ワークフロー設定画面は、参加者リゾルバの選択によって変わります。

2. カスタム参加者リゾルバに必要な入力パラメータを追加します。

3. ［OK］をクリックして、参加者リゾルバの設定を保存します。

   管理タスク プロファイルのタブが再度表示されます。

4. ［サブミット］をクリックし、管理タスク ワークフローの変更内容を保存します。

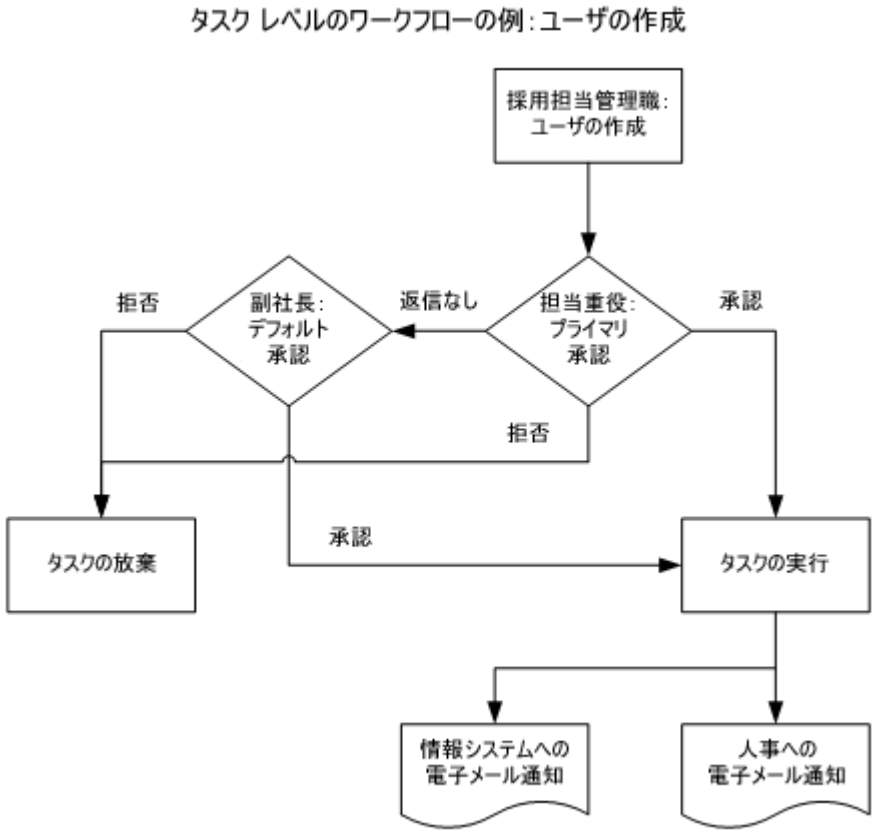
ワークフロー例：ユーザの作成

ある会社の Identity Manager 管理者が、以下のシナリオを処理するためのワークフローとユーザ ロールを定義することになりました。

- この会社の営業マネージャは、新しい営業担当者を雇うことにしました。 営業マネージャは、この新規雇用に対する Identity Manager ユーザを作成できる必要があります。
- 雇用プロセスを合理化するために、参加者が 1 つの作業アイテムを実行するだけで、タスクの承認（または拒否）を行えるようにします。
- 営業部長は、すべての新規雇用に対する第 1 承認者です。 営業部長が見つからない場合は、営業の VP はデフォルトの承認者になります。
- 新規雇用が承認されると、CA Identity Manager は新規ユーザに関する電子メール通知を人事（HR）部と情報サービス（IS）部に送信します。

ユーザ制御の作成図

以下の図に、ユーザの作成シナリオの論理フローを示します。



ワークフロー例の実装

この例のシナリオを実装するには、管理者が以下のタスクを実行する必要があります。

- タスクの開始者が必要な管理ロールのメンバであることを確認します。

  営業マネージャは、[ユーザ マネージャ]管理ロールのメンバである必要があります。このロールは、営業担当者の新規雇用に際して、[ユーザの作成]管理タスクを開始するのに必要な権限を営業マネージャに与えます。

- [ユーザの作成]管理タスクに対してタスク レベルのワークフローを有効にします。

  タスク レベルのワークフローを使用すると、[ユーザの作成]タスクを完了するための作業アイテムが確実に 1 つだけ生成されるようになります。 [ユーザの作成]タスクには複数の個別イベントが関連付けられているため、イベント レベルのワークフローでは複数の作業アイテムが生成され、イベント レベルのワークフローが設定ハンドラにもなります。

- 参加者リゾルバを設定します。

  使用可能な参加者リゾルバの数は、選択したワークフロー プロセス テンプレートによって決まります。 SingleStageApproval テンプレートには、第 1 承認者とデフォルトの承認者が含まれます。その他のテンプレートはそれ以上の許可を行います。

  このシナリオでは 2 人の個人承認者しか必要としないので、[ユーザ リスト]参加者リゾルバは最も単純なソリューションを提供します。 このリゾルバは、ロールやグループで複数のユーザを選択するのではなく、名前で個人承認者を選択できるようにします。

- 電子メール通知を設定します。

  管理コンソールでは、特定のタスクやイベントに関する電子メール通知を作成できます。 このシナリオでは、タスクの電子メールが有効になっており、[ユーザの作成]タスクの完了時に電子メール通知が送信されます。

  適切な件名行とメッセージ テキストを付けて、電子メールを人事部と情報サービス部に送信するには、カスタム電子メール テンプレートが必要です。

詳細情報

テンプレート メソッドの使用方法 (349 ページ)
タスク レベルのワークフローの設定方法 (352 ページ)
参加者リゾルバ: テンプレート メソッド (356 ページ)
電子メール通知 (421 ページ)

WorkPoint メソッド

WorkPoint メソッドは、R12 より前の CA Identity Manager リリースに適用されました。事前定義された WorkPoint ワークフロー プロセスは 14 個あり、これらはデフォルトにより特定の Identity Manager イベントとマッピングされています。 参加者リゾルバを設定し、必要に応じてワークフロー プロセスを変更するには、WorkPoint Designer を使用する必要があります。

WorkPoint メソッドでは、管理コンソールを使用して、ワークフロー プロセスと承認イベントをマッピングし、対応するタスクを使用環境のグローバル レベルでワークフロー制御下に置く必要もあります。

WorkPoint メソッドの使用方法

このセクションでは、WorkPoint メソッドを使用して管理タスクをワークフロー制御下に置くための概要手順を示します。

注: 柔軟性と使い勝手の向上のため、できるだけテンプレート メソッドを使用することをお勧めします。

WorkPoint メソッドを使用するには

1. 管理コンソールで以下の手順を実行します。
   a. ワークフローが有効になっていることを確認します。
   b. (オプション)グローバル イベントのマッピングで、イベント(複数可)を適切な事前定義ワークフロー プロセスと関連付けます。
   c. 必要に応じて、Identity Manager 環境を再起動します。
2. ユーザ コンソールで以下の手順を実行します。
   a. タスク固有イベントのマッピングで、イベント(複数可)を適切な事前定義ワークフロー プロセスと関連付けます。(オプション)
3. WorkPoint Designer で以下の手順を実行します。
   a. 承認タスクをワークフロー プロセスと関連付けます(オプション)。
   b. ワークフロー プロセスを使用して参加者リゾルバを設定します(オプション)。
4. ユーザ コンソールで以下の手順を実行します。
   a. ワークフロー制御が設定されたら、適切なロールを持つユーザが管理タスクを実行します。
   b. 指定されたワークフロー参加者は、イベントの承認または拒否を行います。

詳細情報:

プロセスとイベントのマッピング(366 ページ)
ワークフロー アクティビティと承認タスクの関連付け(371 ページ)
参加者リゾルバ: WorkPoint メソッド(372 ページ)

WorkPoint プロセス

CA Identity Manager には、WorkPoint Designer で事前に定義されている多数のワークフロー プロセスがあります。 事前定義されたプロセスとデフォルトのイベント マッピングの使用、ワークフロー プロセスと他のイベントとのマッピング、アクティビティの追加または削除によるワークフロー プロセスの変更、ワークフロー プロセスの新規作成などを行うことができます。

プロセスとイベントのグローバル マッピング

以下の表に、管理コンソールで指定されている、ワークフロー プロセスとイベントのデフォルトのグローバル マッピングを示します。

重要: これらはグローバル マッピングです。 マッピングされたワークフロー プロセスは、使用環境内の任意のタスクによって、対応するイベントが生成されたときに実行されます。

ワークフロー プロセス	マッピングされるイベント
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	
ModifyGroupMembershipApproveProcess*	
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

注: アスタリスク(*)の付いたワークフロー プロセスは、デフォルトではイベントとマッピングされません。

詳細情報:

グローバル レベルでのプロセスとイベントのマッピング (367 ページ)
特定のタスクでのプロセスとイベントのマッピング (368 ページ)

プロセスとイベントのマッピング

ワークフロー プロセスの作成と変更には、WorkPoint Designer を使用します。 CA Identity Manager 用のワークフロー プロセスを作成する場合は、特定の Identity Manager タスクを念頭に置いて作成してください。 このタスクの実行は、ワークフロープロセスによって制御されます。

ワークフロー プロセスの作成に加え、以下のことも実行する必要があります。

- 「管理タスクおよびイベント」の説明に従って、Identity Manager タスクによって生成されるイベントを特定します。 イベントを生成する任意の Identity Manager タスクに対し、ワークフロー プロセスを作成できます。
- ワークフロー プロセスとイベントをマッピングするには、以下の操作のいずれかを実行します。
  - グローバル レベルでワークフロー プロセスをイベントに割り当てます。

    このグローバル マッピングでは、イベントを生成するタスクに関係なく、使用環境内でこのイベントが生成されると必ずワークフロー プロセスが実行されます。
  - 特定のタスクによって生成されるイベントにワークフロー プロセスを割り当てます。

    このタスク固有のマッピングでは、指定したタスクによってこのイベントが生成された場合にのみ、ワークフロー プロセスが実行されます。

  注: グローバル レベルと特定のタスクの両方でイベントとワークフロー プロセスをマッピングすると、特定のタスクに関連付けられたワークフロー プロセスが優先されます。
- ワークフロー プロセス内のワークフロー アクティビティに対し、参加者リゾルバを指定します。
- ワークフロー アクティビティを承認タスクと関連付けます。

詳細情報:

グローバル レベルでのプロセスとイベントのマッピング (367 ページ)
特定のタスクでのプロセスとイベントのマッピング (368 ページ)
ワークフロー アクティビティ (370 ページ)
参加者リゾルバ: WorkPoint メソッド (372 ページ)

グローバル レベルでのプロセスとイベントのマッピング

グローバル レベルでワークフロー プロセスとイベントをマッピングすると、使用環境内の任意のタスクによってそのイベントが生成されたときに、ワークフロー プロセスが実行されます。

グローバル レベルでワークフロー プロセスとイベントをマッピングする方法

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

   http://hostname/idmmanage

   hostname

   CA Identity Manager がインストールされているサーバの完全修飾ドメイン名を定義します。 たとえば、myserver.mycompany.com:port です。

2. ［環境］をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. ［詳細設定］をクリックし、次に［ワークフロー］をクリックします。
4. イベントとワークフロー プロセスをマッピングする方法
   a. ［イベント］リスト ボックスからイベントを選択します。
   b. ［Approve Process］リスト ボックスからワークフロー プロセスを選択します。
   c. ［追加］をクリックします。
5. イベントとワークフロー プロセスのマッピングが完了したら、［保存］をクリックします。
6. Identity Manager 環境を再起動して、変更内容を有効にします。

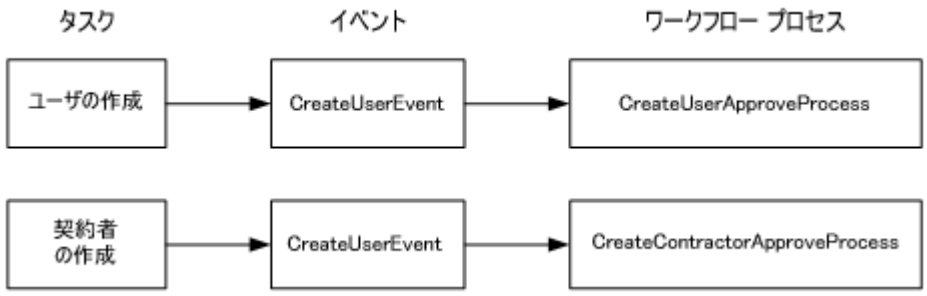
詳細情報:

プロセスとイベントのグローバル マッピング (366 ページ)

特定のタスクでのプロセスとイベントのマッピング

特定のタスクによって生成されるイベントに、ワークフロー プロセスを割り当てることができます。 この場合は、指定したタスクによってマッピングしたイベントが生成されたときにのみ、ワークフロー プロセスが実行されます。

タスク固有のマッピングは、同じイベントに対して実行可能なワークフロー プロセスを可変的に制御します。 たとえば、以下の図に示す 2 種類のタスクは同じイベントを生成しますが、トリガされるワークフロー プロセスはそれぞれ異なります。



この図では、各タスクが異なるワークフロー プロセスを使用しています。

ユーザの作成

CreateUserEvent をトリガするデフォルトの管理タスクを指定します。このイベントは、デフォルトのワークフロー プロセスである CreateUserApproveProcess にマッピングされています。

契約業者の作成

[ユーザの作成]をベースにした カスタム タスクを指定します。 この場合は、CreateUserEvent が CreateContractorApproveProcess とマッピングされます。これは、新規契約業者アカウントの承認用に作成されたカスタム ワークフロー プロセスです。

既存のタスク内のイベントとワークフロー プロセスをマッピングする方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。
2. 管理タスクを検索します。
3. タスク([ユーザの変更]、[ユーザの作成]など)を選択し、[選択]をクリックします。
4. [イベント]タブで、タスク内のイベントに対するワークフロー プロセスを選択します。

   注: イベント名と[ワークフロー プロセス]ドロップダウン メニューをこのタブに表示するには、ワークフローを有効化する必要があります。
5. [編集]ボタンをクリックし、[Workflow mapping]画面を表示します。
6. [ワークフロー プロセス]ドロップダウン メニューを使用して、ワークフロー プロセスをイベント名に割り当て、[OK]をクリックします。
7. [送信]をクリックします。

新規タスク内のイベントとワークフロー プロセスをマッピングする方法

1. ユーザ コンソールで、[ロールおよびタスク]、[管理タスク]、[管理タスクの作成]を選択します。

   注: 新しいワークフロー承認タスクのテンプレートとして、既存のワークフロー承認タスク([グループ作成を承認]、[ユーザ作成を承認]など)を選択してください。
2. [プロファイル]タブで、適切なフィールドに情報を入力します。
3. [イベント]タブで、タスク内のイベントに対するワークフロー プロセスを選択します。

   注: イベント名と[ワークフロー プロセス]ドロップダウン メニューをこのタブに表示するには、ワークフローを有効化する必要があります。
4. [ワークフロー プロセス]ドロップダウン メニューを使用して、ワークフロー プロセスをイベント名に割り当て、[OK]をクリックします。
5. [送信]をクリックします。

注: ワークフロー プロセス リストには、テンプレート メソッドと WorkPoint メソッドの両方で使用するプロセスが含まれています。

- テンプレート メソッド(SingleStepApproval または TwoStageApprovalProcess のいずれか)が選択されると、ページが展開されて、参加者リゾルバの設定が有効になります。
- WorkPoint method が選択されると、このページは展開されません。 参加者リゾルバは WorkPoint Designer で設定されます。

詳細情報:

プロセスとイベントのグローバル マッピング(366 ページ)

ワークフロー アクティビティ

CA Identity Manager には、WorkPoint Designer で事前定義された多数のワークフロー アクティビティが組み込まれています。 これらのアクティビティは、事前定義ワークフロー プロセスに割り当てられます。

事前定義ワークフロー プロセスは、1 ステップのみのプロセスです。したがって、各プロセスには事前定義アクティビティが 1 つだけ含まれます。

それぞれの事前定義アクティビティは、CA Identity Manager で事前定義された同じ名前のワークフロー承認タスクと対応しています。 事前定義アクティビティは他のワークフロー プロセスにも使用できます。また、新しいアクティビティを作成することもできます。

事前定義ワークフロー プロセスは、変更せずにそのまま使用できますが、さらにアクティビティを追加することもできます。 ワークフロー プロセスにアクティビティを追加する方法の詳細については、WorkPoint のマニュアルを参照してください。

プロセス、タスク、アクティビティ

以下の表に、事前定義ワークフロー アクティビティと、各アクティビティがデフォルトで割り当てられる事前定義ワークフロー プロセスを示します。

注: 事前定義ワークフロー アクティビティと、それに対応するワークフロー承認タスクは同じ名前になります。

ワークフロー プロセス	ワークフロー タスク/アクティビティ
CertifyRoleApprovalProcess**	ロール認証を承認
Consultation Process*	
CreateGroupApproveProcess	グループ作成を承認

ワークフロー プロセス	ワークフロー タスク/アクティビティ
CreateOrganizationApproveProcess	組織作成を承認
CreateUserApproveProcess	ユーザ作成を承認
DeleteGroupApproveProcess	グループ削除を承認
DeleteOrganizationApproveProcess	組織削除を承認
DeleteUserApproveProcess	ユーザ削除を承認
ModifyAccessRoleMembershipApproveProcess	アクセス ロール メンバシップ変更を承認
ModifyAdminRoleMembershipApproveProcess	管理ロール メンバシップ変更を承認
ModifyGroupMembershipApproveProcess	グループ メンバシップ変更を承認
ModifyIdentityPolicySetApproveProcess	アイデンティティ ポリシー セット変更を承認
ModifyOrganizationApproveProcess	組織変更を承認
ModifyUserApproveProcess	ユーザ変更を承認
SelfRegistrationApproveProcess	自己登録の承認
SingleStepApproval*	
TwoStageApprovalProcess*	

注: アスタリスク(*)の付いたワークフロー プロセスは、テンプレート メソッドと共に使用します。 これらはユーザ コンソールで設定するため、デフォルトのタスクやアクティビティは関連付けられていません。 CertifyRoleApprovalProcess(**)は、カスタム参加者リゾルバのデモンストレーションを行うサンプル プロセスです。

ワークフロー アクティビティと承認タスクの関連付け

ワークフロー アクティビティとワークフロー承認タスクを関連付けるには、WorkPoint Designer で名前と値のペアを定義します。

注: ワークフロー アクティビティに対して名前と値のペアが定義されていない場合、CA Identity Manager のデフォルトでは、承認タスクと名前が一致するタスクが使用されます。

ワークフロー アクティビティと承認タスクを関連付けるには

1. WorkPoint Designer を起動します。
2. [ファイル]-[開く]-[プロセス]をクリックします。
3. ワークフロー プロセスを選択し、[開く]をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、[プロパティ]を選択します。

5. [タイプ]ドロップダウン メニューから[テキスト]を選択します。
6. [ユーザ データ]タブに、以下の情報を入力します。
   - 名前 — TASK_TAG
   - 値 — 承認タスクのタグ名
7. [追加]をクリックします。
8. [OK]をクリックして、変更を保存します。

参加者リゾルバ: WorkPoint メソッド

WorkPoint メソッドを使用して参加者を指定するには、WorkPoint Designer で以下のアクティビティ プロパティを定義します。

- CA Identity Manager とワークフロー サーバ間の通信を有効化する、事前定義された CA Identity Manager スクリプトの名前。 このスクリプトは、アクティビティの参加者に対するリクエストを CA Identity Manager に発行し、そのリストをワークフローサーバに渡します。
- 参加者リゾルバ(複数可)の参照

参加者リゾルバのタイプ

ワークフロー アクティビティのプロパティに特定の参加者リストを入力するのではなく、参加者リゾルバとマッピングされた任意の名前によって参加者が参照されます。

事前定義されたプロセス モデルの場合、以下の 4 種類の参加者リゾルバがあります。

ロール参加者リゾルバ

特定のロールのメンバが参加者であることを指定します。

グループ参加者リゾルバ

特定のグループのメンバが参加者であることを指定します。

カスタム参加者リゾルバ

カスタム参加者リゾルバによって、参加者が決定されることを指定します。

フィルタ参加者リゾルバ

検索フィルタを使用して参加者が選択されることを指定します。

ロール参加者リゾルバ

ロール タイプの参加者リゾルバでは、CA Identity Manager が該当するロールのメンバをすべて取得し、それらのメンバを参加者として返します。

[アクティビティ]ダイアログ ボックスの UserData パラメータでリゾルバ タイプが指定されていない場合は、デフォルトによりロール タイプのリゾルバが使用されます。

[WorkPoint アクティビティのプロパティ]ダイアログ ボックスの[ユーザ データ]タブで参加者リゾルバが指定されていない場合は、CA Identity Manager のデフォルトにより、この承認タスクが含まれた使用可能なロールがすべて検出され、それらのロール メンバが参加者として返されます。

ロール参加者リゾルバの設定方法

1. WorkPoint Designer を起動します。
2. [ファイル]-[開く]-[プロセス]をクリックします。
3. ワークフロー プロセスを選択し、[開く]をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、[プロパティ]を選択します。
5. [タイプ]ドロップダウン メニューから[テキスト]を選択します。
6. [ユーザ データ]タブに、以下の情報を入力します。
   - 名前 — APPROVER_ROLE_NAME
   - 値 — Identity Manager ロールの名前(例: セキュリティ マネージャ)
7. [追加]をクリックします。

   注: このロールには、承認タスクを含める必要はありません。
8. [タイプ]ドロップダウン メニューから[テキスト]を選択します。
9. [ユーザ データ]タブで、以下の名前と値のペアを入力します(オプション)。

   名前 — APPROVERS_REQUIRED

   値 — YES
10. [追加]をクリックします。

    注: デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

    APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。
11. [OK]をクリックして、変更を保存します。

グループ参加者リゾルバ

グループ タイプの参加者リゾルバでは、CA Identity Manager が該当するグループのメンバをすべて取得し、それらのメンバを参加者として返します。

グループ参加者リゾルバの設定方法

1. WorkPoint Designer を起動します。
2. [ファイル]-[開く]-[プロセス]をクリックします。
3. ワークフロー プロセスを選択し、[開く]をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、[プロパティ]を選択します。
5. [タイプ]ドロップダウン メニューから[テキスト]を選択します。
6. [ユーザ データ]タブに、以下の情報を入力します。
   - 名前—APPROVER_GROUP_UNIQUENAME
   - 値—Identity Manager グループの名前
7. [追加]をクリックします。
8. [タイプ]ドロップダウン メニューから[テキスト]を選択します。
9. [ユーザ データ]タブで、以下の名前と値のペアを入力します(オプション)。
   - 名前—APPROVERS_REQUIRED
   - 値 — YES
10. [追加]をクリックします。

    注: デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

    APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。
11. [OK]をクリックして、変更を保存します。

カスタム参加者リゾルバ

カスタム参加者リゾルバは、ワークフロー アクティビティの参加者を決定し、リストを CA Identity Manager に返す Java オブジェクトです。CA Identity Manager は、このリゾルバから返されたリストをワークフロー エンジンに渡します。 一般に、カスタム参加者リゾルバを作成するのは、標準の参加者ポリシーではアクティビティに必要な参加者のリストを提供できない場合のみです。

注: カスタム参加者リゾルバの作成には、参加者リゾルバ API を使用します。 詳細については、「Programming Guide for Java」を参照してください。

カスタム参加者リゾルバを設定する方法

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

   http://hostname/idmmanage

   hostname

   CA Identity Manager がインストールされているサーバの完全修飾ドメイン名を定義します。 たとえば、myserver.mycompany.com:port です。

2. [環境]をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. [詳細設定]をクリックし、次に[ワークフロー参加者リゾルバ]をクリックします。
4. [ワークフロー参加者リゾルバ]画面で[新規]をクリックし、以下の情報を入力します。

   名前

   カスタム参加者リゾルバ名を指定します。たとえば、GroupFinder です。

   [説明]

   カスタム参加者リゾルバの説明を指定します。

   クラス

   Java クラス名を指定します。たとえば、com.netegrity.samples.GroupFinder です。

5. [保存]をクリックします。
6. WorkPoint Designer を起動します。
7. [ファイル]-[開く]-[プロセス]をクリックします。
8. ワークフロー プロセスを選択し、[開く]をクリックします。
9. プロセス内のアクティビティ ノードを右クリックし、[プロパティ]を選択します。
10. [タイプ]ドロップダウン メニューから[テキスト]を選択します。
11. [ユーザ データ]タブに、以下の情報を入力します。

    名前

    APPROVER_CUSTOMRESOLVER_NAME

    値

    カスタム リゾルバの名前を一意に指定します。 これは、管理コンソールの[カスタム タイプの参加者リゾルバ]画面に入力した名前と一致している必要があります。たとえば、GroupFinder です。

12. [追加]をクリックします。

注: デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。

13. [OK]をクリックして、変更を保存します。

フィルタ参加者リゾルバ

フィルタ参加者リゾルバを使用すると、CA Identity Manager がフィルタ基準と一致するユーザまたはグループを検索できるようになります。 WorkPoint Designer で検索フィルタを指定すると、CA Identity Manager によって対応するワークフロー アクティビティと一致する承認者が返されます。

フィルタ参加者リゾルバを作成するには、[WorkPoint アクティビティのプロパティ]ダイアログ ボックスの[ユーザ データ]タブを使用します。

参加者リゾルバのフィルタ構文

検索フィルタを作成するために組み合わせる必要がある 3 つの属性は、以下の通りです。

- 承認者属性(例: タイトル)
- 承認者属性演算子(例: equals)
- 承認者属性値(例: マネージャ)

検索フィルタの必須属性は、以下の順序で組み合わせます。

属性 演算子 値

以下に例を示します。

「タイトル equals マネージャ」または「部署 contains 給与」

参加者リゾルバの必須フィルタ属性

参加者リゾルバの必須フィルタ属性は以下のとおりです。

注: 各フィルタの「n」は、検索フィルタ番号を示す正の整数です。 デフォルトは 1 です。

APPROVER_FILTER_n_ATTRIBUTE

承認者属性を指定します。(例: Title、Department、User ID)。 承認者属性名の文字列は、Identity Manager のユーザ属性名の文字列と一致している必要があります。

APPROVER_FILTER_n_OP

承認者属性と関連付けられる演算子を指定します。（例： equals、not_equals、contains）。 演算キーワードの大文字小文字は区別されません。

このフィルタへの有効な入力を以下に示します。

- EQUALS
- STARTSWITH
- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

承認者と関連付けられる値を指定します。（例： manager、payroll、engineering）

参加者リゾルバのオプション フィルタ属性

参加者リゾルバのオプション フィルタ属性は以下のとおりです。

APPROVER_OBJECTTYPE

USER または GROUP（大文字小文字の区別なし）

デフォルトは USER です。

APPROVER_ORG_UNIQUENAME

承認者の組織を示す一意の名前。 組織名の文字列は、Identity Manager の組織名の文字列と一致している必要があります。

デフォルトは root です。

APPROVER_ORG_AND_LOWER

承認者の組織または下位組織です。

- 0 は、承認者の組織内で検索することを意味します。
- 1 は、承認者の組織のすべての下位組織内で検索することを意味します。

デフォルトは 1 です。

APPROVER_FILTER_NO

使用する検索フィルタの番号。 フィルタが 2 つある場合、この数値は 2 になります。

デフォルトは 1 です。

注: フィルタの数が 2 以上の場合、このフィルタは必須です。

APPROVER_FILTER_n_CONJ_TYPE

OR または AND 連結タイプを使用して、検索フィルタを組み合わせることができます。

注: OR 連結タイプで区切られたフィルタは、AND で区切られたフィルタよりも優先されます。

たとえば、"title equals manager" および "department equals development" の両方を検索する場合は、AND 連結タイプを指定します。

注: 「n」は、検索フィルタ番号を示す 2 以上の正の整数です。

参加者リゾルバ フィルタの追加

参加者リゾルバ フィルタの追加方法

1. WorkPoint Designer を起動します。
2. [ファイル]-[開く]-[プロセス]をクリックします。
3. ワークフロー プロセスを選択し、[開く]をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、[プロパティ]を選択します。
5. [タイプ]ドロップダウン メニューから[テキスト]を選択します。
6. [ユーザ データ]タブに、以下の情報を入力します。
   - 名前 — APPROVER_FILTER_1_ATTRIBUTE
   - 値 — 一意のロール識別子（例: title）
7. [追加]をクリックします。
8. 検索フィルタの属性ごとに、手順 6 ～ 7 を繰り返します。

   注: デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

   APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。
9. [OK]をクリックして、変更を保存します。

例: フィルタ参加者リゾルバ

以下の表のユーザ ストアには、4 人のユーザ(Holly、Sarah、John、Dave)と、ユーザ ID、役職、部署の各属性が含まれています。

[ユーザ]	ID	[役職]	[部署]
Holly	admin1	sysadmin	管理
Sarah	test1	sysadmin	development
John	admin2	マネージャ	development
Dave	admin3	sysadmin	監査

CA Identity Manager は、上記のユーザ ストアに対し、以下の表で定義される 3 つのフィルタを適用します。

名前	値
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	=
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	デパートメント
APPROVER_FILTER_2_OP	=
APPROVER_FILTER_2_VALUE	管理
APPROVER_FILTER_3_CONJ_TYPE	OR
APPROVER_FILTER_3_ATTRIBUTE	title
APPROVER_FILTER_3_OP	=
APPROVER_FILTER_3_VALUE	sysadmin

CA Identity Manager は、これらのフィルタを以下の順序で適用します。

1. OR 連結で接続された 2 番目と 3 番目のフィルタを評価します。

   "department equals administration" OR "title equals sysadmin"

   これにより John が除外され、Holly、Sarah、Dave が返されます。

2. AND 連結で接続された 1 番目と 2 番目のフィルタを評価します(ここで、「*」はワイルドカード文字となります)。

   "uid equals admin*" AND "department equals administration"

   これにより Sarah が除外され、Holly と Dave が返されます。

このユーザ ストアから最終的に返されるユーザは Holly と Dave です。

参加者リゾルバの優先順位

参加者リゾルバが指定されていない場合は、Identity Manager のデフォルトにより、この承認タスクが含まれた使用可能なロールがすべて識別され、それらのロール メンバが参加者として返されます。

複数の参加者リゾルバを指定した場合、Identity Manager は以下の優先順でそれらを評価します。

1. カスタム
2. ロール
3. フィルタ
4. グループ

Identity Manager は、この優先順で最初のリゾルバを識別および適用し、残っている後続のリゾルバはすべて無視します。

使用できるリゾルバは一度に 1 つのみです。 また、Identity Manager が参加者を正しく識別できるように、リゾルバが正しく設定されていることを確認してください。

ワークフロー リソース スクリプトの指定

Identity Manager には、Identity Manager とワークフロー サーバ間で情報を渡すスクリプトとして、名前指定された IM Approvers が用意されています。

ワークフロー アクティビティに参加者リストが必要な場合は、このスクリプトによって、アクティビティ名、[WorkPoint Activity Properties]ダイアログ ボックスの[User Data]タブで指定された参加者識別子、および[User Data]タブで指定されたその他の情報が Identity Manager に渡されます。 Identity Manager は参加者を検索し、このスクリプトにリストを返します。 次に、このスクリプトからワークフロー サーバにリストが渡されます。

新しいワークフロー プロセス定義があり、そのワークフロー プロセスのアクティビティが Identity Manager のワークフロー承認タスクの場合、IM Approvers スクリプトを［WorkPoint Activity Properties］ダイアログ ボックスの［Resources］タブに指定する必要があります。

WorkPoint Designer で IM Approvers スクリプトを指定するには、以下の手順に従います。

1. ［Resources］タブで、［Select］をクリックします。
2. ［Select Resources］ダイアログ ボックスで、ドロップダウン リストから［Rule］を選択します。 このアクションによって、アクティビティと関連付けできるルール（スクリプト）がリストされます。
3. スクリプト名 IM Approvers を選択し、［Add］をクリックします。
4. ［OK］をクリックし、［Activity Properties］ダイアログ ボックスで［Apply］をクリックします。

注: IM Approvers スクリプトは変更しないでください。

ユーザ認証タスクの参加者の指定

ユーザ認証タスクはイベント CertifyRoleEvent を生成します。 このイベントは、事前定義プロセス CertifyRoleApproveProcess を通してワークフロー承認を受けることができます。

Identity Manager には、事前定義の参加者リゾルバ CertifyRoleParticipantResolver も組み込まれています。このリゾルバはデフォルトで使用環境内に表示されます。CertifyRoleApprovalProcess のアクティビティに対する参加者は、CertifyRoleParticipantResolver によって指定されます。

参加者の設定情報を指定する方法

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

   http://hostname/idmmanage

   hostname

   CA Identity Manager がインストールされているサーバの完全修飾ドメイン名を定義します。 たとえば、myserver.mycompany.com:port です。

2. ［環境］をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. ［詳細設定］をクリックし、次に［その他］をクリックします。

4. 名前と値のペアを定義して、認証される各ロールの承認者を指定します。
   - [プロパティ]フィールドで、role-type.role-name の形式を使用します。

     role-type には、admin、access、provisioning のいずれかのロールを指定します。

     role-name には、既存の任意のロール名を指定します。

     ロール名とロール タイプはピリオド(.)で区切る必要があります。
   - [値]フィールドに、承認者の ID を指定します。各 ID はセミコロン(;)で区切ります。

以下の例では、以下のロールに対するユーザ認証が以下の参加者によって承認されます。

- jsmith01 と ajones19 は、[ユーザ マネージャ]ロールに対する認証を承認できます。
- plewis12 は、[System Manager]ロールに対する唯一の承認者です。
- rtrevor8 と pkitt3 は、[My Access]ロールに対する認証を承認できます。

プロパティ	値
admin.User Manager	jsmith01;ajones19
admin.System Manager	plewis12
access.My Access Role	rtrevor8;pkitt3

注: 指定されていないロールは、CertifyRoleEvent に対する承認者を持ちません。

WorkPoint Designer のプロセス

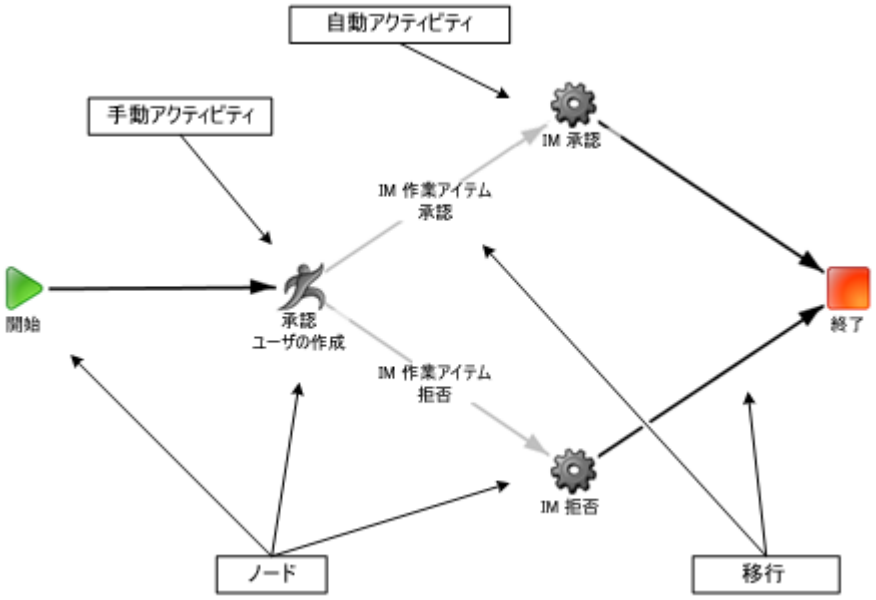
WorkPoint Designer では、Identity Manager に用意されているデフォルトのワークフロー プロセスとアクティビティをカスタマイズして、新しいワークフロー プロセスとアクティビティを作成することができます。

このマニュアルでは、Identity Manager に固有の WorkPoint ワークフローについて説明します。 詳細については、WorkPoint Designer のマニュアルを参照してください。

注: ワークフロー プロセスの作成時には、既存の Identity Manager プロセスのコピーを作成し、新しいプロセスを必要に応じて変更してください。 この方法で作成されたワークフロー プロセスには、移行スクリプトや自動アクティビティなど Identity Manager 固有のデフォルトのエレメントとノードが組み込まれます。

WorkPoint プロセス図

以下の図に、一般的なワークフロー プロセスを示します。ここでは、Identity Manager のタスクを制御するプロセスに関する最小限のコンポーネント セットが使用されています。この図は、ユーザ作成タスクの実行を制御する事前定義プロセス CreateUserApproveProcess を示しています。



WorkPoint プロセスのコンポーネント

このワークフロー プロセスには、以下のノードと移行が含まれています。

開始

各ワークフロー プロセスは、このノードから始まります。

終了

各ワークフロー プロセスは、このノードで終わります。

手動アクティビティ

手動アクティビティでは、参加者による Identity Manager タスクの承認または拒否が必要です。このアクティビティの名前は、Identity Manager のワークフロー承認タスクと同じでなければなりません。

Identity Manager のタスクを制御するワークフロー プロセスには、そのタスクの承認を求める手動アクティビティが少なくとも 1 つ含まれている必要があります。

自動アクティビティ

自動アクティビティには、以下のいずれかのスクリプトが割り当てられます。

- Notify IM Approve - Identity Manager に、ワークフロー制御下にある Identity Manager タスクを実行するよう通知します。
- Notify IM Reject - Identity Manager に、Identity Manager タスクの実行をキャンセルするよう通知します。

一般に、Notify IM Approve スクリプトはすべての手動アクティビティが承認された場合に有効化され、Notify IM Reject スクリプトは手動アクティビティが 1 つでも拒否された場合に有効化されます。

無条件移行

無条件移行は、ワークフロー プロセス内のあるノードから別のノードまでのパスであり、条件スクリプトとは関連付けられません。

条件移行

条件移行は、ワークフロー プロセス内のあるノードから別のノードまでの代替パスであり、条件スクリプトと関連付けられます。

条件スクリプトは、関連付けられたアクティビティの結果を評価して、移行するかどうかを決定します。 このスクリプトが true を返した場合は、移行が実行され、プロセスが次に指令されたノードに移ります。

2 つ以上の条件スクリプトが true を返す可能性もあります。 各スクリプトは別の移行と関連付けられているため、この場合はアクティビティを並列実行することができます。

注: 条件移行では、カスタム スクリプトを使用できます。 詳細については、「Programming Guide for Java」を参照してください。

手動アクティビティのプロパティ

以下の表に、Identity Manager に固有のプロパティ設定を示します。 これらの設定は、WorkPoint Designer の[Activity Properties]ダイアログ ボックスの各タブで定義します。

[プロパティ]タブ	プロパティの説明
リソース	IM Approvers — Include リストで指定されます。 このスクリプトは Identity Manager とワークフロー サーバ間で情報を渡します。
Agents	Nobody Auto Complete — Asynchronous リストで指定され、Available 状態と関連付けられます。 このスクリプトは、アクティビティ参加者が存在しない場合に、アクティビティを承認済みと見なすかどうかを決定します。
ユーザ データ	Identity Manager がアクティビティ参加者を取得するために使用する名前と値のペアを定義します。 オプションで、カスタム参加者リゾルバに渡すデータを定義することも

[プロパティ]タブ	プロパティの説明
	できます。

条件移行のプロパティ

以下のデフォルト スクリプトは、[移行のプロパティ]ダイアログ ボックスの[条件]タブに表示されます。

IM WorkItem Approved

関連付けられたアクティビティが承認された場合に true を返します。 ワークフロー プロセスは、移行によって示された次のノードに移ります。

IM WorkItem Rejected

関連付けられたアクティビティが拒否された場合に true を返します。 ワークフロー プロセスは、移行によって示された次のノードに移ります。

ジョブとプロセス インスタンス

ワークフロー プロセスは、Identity Manager が特定のタスクを完了するために実行すべきステップを定義します。 ジョブとは、ワークフロー プロセスのランタイム インスタンスを指します。

たとえば、デフォルトのワークフロー プロセス CreateUserApproveProcess は、新規ユーザを承認するために実行すべきステップを定義します。 Identity Manager で新規ユーザが実際に作成され、承認のためにそのタスクがサブミットされると、CreateUserApproveProcess のジョブ インスタンスが WorkPoint Designer で作成されます。

WorkPoint Designer でジョブを開いたり、表示や変更を行うためのインターフェースは、ワークフロー プロセスの編集用インターフェースと良く似ています。

同一のプロセスをベースにして、複数のジョブを共存させることができます。

フィルタの基礎

WorkPoint Designer には、さまざまな基準に基づいてジョブを検索できるフィルタリング機能が組み込まれています。 たとえば、以下のようなジョブを検索できます。

- 選択したワークフロー プロセス(複数可)をベースにしたジョブ
- ユーザ定義のジョブ参照または固有のジョブ ID を持つジョブ

- 特定の状態(アクティブ、完了、一時停止など)にあるジョブ
- 指定した日付範囲内に作成または開始されたジョブ

注: ジョブ フィルタリングの説明および参照情報については、WorkPoint Designer のマニュアルを参照してください。

ジョブ ステータスとプロパティ

ジョブを開くと、そのジョブのワークフロー図が表示されます。 ワークフロー アクティビティのノードと移行は、実行されたかどうかを示す色付きで描画されます。

以下のものを表示し、必要に応じて変更することができます。

- ジョブのプロパティ(参加者、ジョブ履歴情報など)
- 開いているジョブの状態(完了しているかどうかなど)
- ジョブに含まれる各ノードと移行のプロパティ

アクティビティと作業アイテムのプロパティ

以下のようなジョブ アクティビティのプロパティやプロセス アクティビティのプロパティを表示し、必要に応じて変更することができます。

- アクティビティの状態情報
- アクティビティの承認情報
- 承認タスク(WorkPoint Designer では作業アイテムと呼ぶ)情報。以下に例を示します。
  - どの参加者も作業アイテムを保留していない場合は(他の承認者のワーク リストからそのアイテムが削除されます)、状態が Available になり、どの参加者のユーザ ID も表示されません。
  - ある参加者が作業アイテムを保留しているが、まだ完了していない場合は、状態が Open になり、その参加者のユーザ ID と予約時間が表示されます。
  - 作業アイテムが完了している場合は、状態が Complete になります。 ワークフロー制御下でそのタスクを承認または拒否した参加者のユーザ ID と、完了時間が表示されます。

各作業アイテムのプロパティには、以下の情報が含まれます。

- 作業アイテムの名前と現在の状態
- 状態履歴情報(所定の状態に対して責任を持つ参加者のユーザ ID など)
- 権限が付与された作業アイテム参加者の情報

注: ジョブ、アクティビティ、作業アイテムのプロパティの詳細については、WorkPoint Designer のマニュアルを参照してください。

ワークフロー アクティビティの実行

ワークフロー プロセスでは、アクティビティ参加者として指定されたユーザによって、手動アクティビティが実行されます。アクティビティ参加者は、承認タスクと関連付けられたイベントを承認または拒否します。 参加者は Identity Manager でこのアクティビティを実行します。

Identity Manager の承認タスクと関連付けられたアクティビティが実行されると、以下の処理が行われます。

1. Identity Manager が参加者に通知をします。
2. 参加者はタスクを承認または拒否します。
3. ワークフロー サーバがアクティビティを完了します。

参加者の検出と通知

Identity Manager の承認タスクと関連付けられたワークフロー アクティビティが開始されると、ワークフロー サーバからアクティビティ参加者に関する情報が Identity Manager に渡されます。 この情報は、アクティビティ プロパティで定義されます。 Identity Manager はこの情報を使用してアクティビティ参加者を取得し、承認タスクが保留中である旨の警告を出します。

参加者を識別すると、Identity Manager は各参加者のワーク リストに新しい作業アイテム(承認タスク)を追加します。 オプションにより、Identity Manager から各参加者に新しい作業アイテムに関する電子メール通知を送信することもできます。

注: APPROVERS_REQUIRED アクティビティ プロパティが false に設定され、参加者が検出されない場合は、デフォルトによりそのタスクは承認済みと見なされます。

注: [ステータス]列の丸マークは、その承認タスクを任意の参加者が要求できることを示します。 チェック マークは、ワーク リストの所有者が承認タスクを受け入れたが、まだタスクを完了していないことを示します。

承認タスクの受け入れと実行

参加者が検出されると、1 人の参加者が承認タスクを受け入れて、ワークフロー制御下でそのタスクを承認または拒否するまで、アクティビティを完了することはできません。

参加者が承認タスクを受け入れるには、ワークフロー アクティビティ コンソールで作業アイテム名をクリックし、次に[アイテムの保留]をクリックします。 アイテムを保留すると、他の承認者のワーク リストから削除されます。

承認タスクを受け入れた参加者は、ワークフロー制御下でそのタスクを承認するか拒否するかを決定します。 また、複数の参加者が同じ承認タスクを受け入れることはできないため、その承認タスクは他の参加者のワーク リストから削除されます。

参加者が承認タスクを受け入れると、承認画面が表示されます。この画面で、参加者は以下のいずれかのアクションを実行できます。

- ワークフロー制御下でただちにタスクを承認または拒否します。
- 承認タスクを解放して、他の参加者が受け入れられるようにします。
- ダイアログ ボックスを閉じて、アクティビティを後で完了します。 上記の[ユーザの作成を承認]ダイアログ ボックスを再度開くには、参加者がワーク リストで承認タスクの名前をクリックします。

また、参加者はこの承認画面で、変更可能フィールド(複数可)を必要に応じて更新できます。 タスクの作成時には、この画面上のフィールドを変更可能にすることができます。

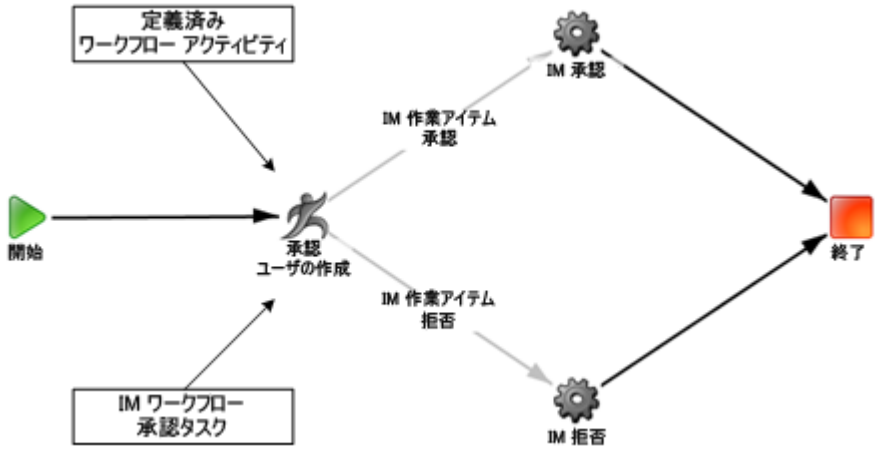
参加者がワークフロー制御下でタスクを承認または拒否すると、アクティビティが完了し、アクティビティの結果によって決定されるパスに従ってワークフロー プロセスを続行できるようになります(次のセクションを参照)。

ワークフロー サーバによるアクティビティの完了

手動アクティビティは、そこから導かれる 2 つ以上の条件移行と共に、Designer ウィンドウに表示されます。

それぞれの条件移行には、スクリプトが関連付けられています。 参加者がアクティビティを完了すると、各スクリプトがアクティビティ結果を評価します。 これらの評価の結果によって、プロセス フローの方向が決まります。

以下の図に、Designer の[ユーザ作成を承認]アクティビティと、Identity Manager でそれに対応する同一名の承認タスクを示します。



アクティビティ参加者（または承認者）が Identity Manager で[承認]または[拒否]ボタンをクリックすると、以下のことが行われます。

1. プロセス ジョブ インスタンスの[ユーザ作成を承認]アクティビティが終了します。条件移行と関連付けられた各スクリプトは、アクティビティの結果を評価します。
2. どの条件移行の評価が true かに基づいて、ジョブ インスタンスを続行します。
   - アクティビティが承認された場合は、IM WorkItem Approved スクリプトから true が返されます。 ワークフローは IM WorkItem Approved 移行を次のノードに渡します。 この自動アクティビティ IM Approve は、Identity Manager にユーザ作成タスクを実行するよう通知します。
   - アクティビティが拒否された場合は、IM WorkItem Rejected スクリプトから true が返されます。 ワークフローは IM WorkItem Rejected 移行を次のノードに渡します。 この自動アクティビティ IM Reject は、Identity Manager にユーザ作成タスクをキャンセルするよう通知します。

Workpoint ジョブの表示

以下のタスクから Workpoint ジョブの実行時のステータスをユーザ コンソールに表示できます。

- 承認タスク
- サブミット済みタスクの表示

新規環境では、すべての承認タスクにはデフォルトで[ジョブの表示]タブが含まれています。 このリリースで作成されるイベントのみが、[サブミット済みタスクの表示]で選択されたイベントまたはタスクのために呼び出されたすべてのプロセス定義に対し、ジョブイメージの表示をサポートしています。 旧リリースで作成されるイベントでは、ワークフローのジョブ ビュー機能はサポートしていません。

既存の[承認]タブへの[ジョブの表示]タブの追加

承認タスクの場合、作業アイテムのジョブ イメージを表示するには、すべての既存のタスクに新規の[ジョブの表示]タブを追加する必要があります。

注:新規環境には、すべての承認タスクについてこのタブが含まれています。

既存のタスクに[ジョブの表示]タブを追加する方法

1. [管理タスク]および[ロール]カテゴリから、[管理タスク]-[管理タスクの変更]を選択して、ModifyAdminTask を実行します。
2. [検索]をクリックし、承認タスク(たとえば、[ユーザの作成を承認])を選択してから、[選択]をクリックします。

   [管理タスクの変更: ユーザの作成を承認]ダイアログ ボックスが表示されます。
3. ドロップダウン メニューから[タブ]タブをクリックし、[ジョブの表示](JobView) を選択し、[サブミット]をクリックします。

   承認タスクに、[ジョブの表示]タブが追加されます。

   すべての既存の承認タスクに対して、同じ作業を繰り返します。

[Configure View Job(ジョブの表示設定)]タブ

以下を使用して、このタブを設定します。

名前

タブに割り当てる名前。

タグ

タスク内で一意なタブの識別子。 文字またはアンダースコアで始まり、文字、数字、アンダースコアのみで構成される必要があります。 タグは主として、XML ドキュメントまたは HTTP パラメータを通じてデータ値を設定するために使用されます。

タブの非表示

タスク中にタブを非表示にします。 このオプションは、タブを非表示にする必要があるが、タブのアトリビュートにはアクセスするアプリケーションで役に立ちます。

承認タスクにおける[ジョブの表示]タブの表示

承認タスクで[ジョブの表示]タブを表示するには、以下の手順に従います。

[ジョブの表示]タブの表示方法

1. [ワーク リスト]ダイアログ ボックスから、承認タスクを選択して表示します。
2. [ジョブの表示]タブをクリックして、タスクの実行時のステータスを表示します。

   この画面から、[承認]、[拒否]、[保留]を実行するか、またはタブを閉じることができます。

あるいは、[ホーム]タブおよび[View my Worklist(マイ ワーク リストの表示)]をクリックして、[ワーク リスト]ダイアログ ボックスに戻ることができます。

イベント レベル ワークフローのワークフロージョブの表示

[サブミット済みのタスク]で、イベント レベル ワークフローのワークフロー ジョブを表示する方法

ワークフロージョブの表示方法

1. [システム]タブから、[サブミット済みタスクの表示]を選択し、検索条件を入力し、[検索]を選択します。
2. タスクを選択し、イベントを選択してからペンシルをクリックすると、イベントの詳細が表示されます。
3. [イベント ワークフローのジョブ ビュー]下で、プロセスを選択し、ペンシルをクリックしてから、このイベントのジョブイメージを表示します。

タスク レベル ワークフローのワークフロー ジョブの表示

[サブミット済みタスクの表示]で、タスク レベル ワークフローのワークフロー ジョブを表示する方法

ワークフロージョブの表示方法

1. [システム]タブから、[サブミット済みタスクの表示]を選択し、検索条件を入力し、[検索]を選択します。
2. タスクを選択し、ペンシルをクリックしてから、タスクの詳細を表示します。
3. [タスク ワークフローのジョブ ビュー]下で、プロセスを選択し、ペンシルを選択してから、このタスクのジョブ イメージを表示します。

ポリシーベース ワークフロー

ポリシーベース ワークフローを使用すると、ルールの評価に基づいて、ワークフロー コントロールの下にイベントを配置できます。 これにより、常にイベントによりワークフロー プロセスが開始されるのではなく、イベントに関連付けられたルールが True である場合にワークフロー プロセスにより作業アイテムが実行および生成されます。

承認ルールは、ワークフロー プロセスを開始するかどうかを決定する条件です。 ワークフロープロセスが開始されると、イベントはワークフロー コントロールの下に配置され、承認者の作業リストに作業アイテムが追加されます。

承認ポリシーは、承認ルール、ワークフロー プロセス、関連情報を組み合わせたものです。

たとえば、新規のグループを作成する場合、新しいグループが、指定された親組織の一部門である場合のみ、CreateGroupEvent をワークフロー コントロールの下に配置し、作業アイテムを作成するように承認ポリシーを定義できます。 新規グループがその組織の一部門でない場合は、ワークフロー プロセスは実行されず、作業アイテムは作成されません。

常時評価を行うか、または管理対象オブジェクトの指定された属性が変化した場合（従業員の給与の値が変化した場合など）のみに評価を行うかのポリシー ルールを作成できます。

注：ポリシーベース ワークフローは、イベントレベルのワークフローにおいてのみ設定できます。 ポリシーベース ワークフローは、タスクレベルのワークフローと共に使用することはできません

詳細情報：

ポリシー順序（393 ページ）
ルールの評価（395 ページ）
イベント レベルのワークフロー（352 ページ）
タスク レベルのワークフロー（350 ページ）

デフォルトのワークフロー プロセス

すべてのデフォルトのワークフロー テンプレートおよびあらかじめ定義されたワークフロー プロセスにより、以下に示すようにワークフロー ルールがサポートされます。

- プロセス テンプレート – これらのテンプレートを使用することで、承認者（または参加者リソルバ）をユーザ コンソールに設定できます。
- あらかじめ定義されたワークフロー プロセス – これには、WorkPoint Designer での、参加者リゾルバの設定が必要となります。

また、ワークフロー ルール用のカスタム ワークフロー プロセスを作成することも可能です。

詳細情報:

プロセス テンプレート(345 ページ)
WorkPoint プロセス(365 ページ)

ポリシー順序

すべての承認ポリシーには、ポリシー 順序フィールドが含まれています。このフィールドでは、昇順の正の整数値により優先度を指定します。 各ポリシーの優先度により、以下が決まります。

- 承認ルールが評価される順序
- ルールが True である場合には、ワークフロー プロセスが開始される順序

ポリシー順序の整数値が小さいポリシーほど優先度は高くなり、そのルールは、整数値の大きいポリシーより先に評価されます。 あるイベントに対して True であるすべてのポリシーにおいては、優先度が最も高いポリシーのワークフロー プロセスが最初に開始されます。

ポリシー順序の例

この簡単な例では、ポリシーの順番付けがどのように機能するかを示しています。 この例では、ポリシールールが常に評価されていることを前提としてます。

あるイベントに、常に評価される複数のポリシーがある場合に、そのイベントそのものを承認するためには、すべてのポリシーを承認する必要があります。 しかし、そのイベントに関連付けられた 1 つのポリシーが拒否された場合、そのイベントそのものも拒否されます。

この例では、Policy1 は、False と評価され、Process1 と名付けられたワークフロー プロセスは実行されず、User1 の作業アイテムは生成されません。 イベント制御は、即座に Policy2 に渡されます。 Policy2 および Policy3 は、両方とも True と評価されました。優先度が高いため、ワークフロー Process2 が最初に実行され、User2 の作業アイテムが生成されます。

User2 がその作業アイテムを承認すれば、ワークフロー Process3 が実行され、User3 の作業アイテムが生成されます。次に、User3 がその作業アイテムを承認することで、イベントそのものが承認されます。 これらのアクションを、以下のテーブルに示します。

優先度	ポリシー	Result	ワークフロー	承認者	アクション
1	Policy1	False	Process1	User1	—
2	Policy2	True	Process2	User2	承認済み
3	Policy3	True	Process3	User3	承認済み

しかし、User2 がその作業アイテムを拒否する場合には、イベントそのものが拒否され、次の表に示すように、User3 には作業アイテムは生成されません。

優先度	ポリシー	Result	ワークフロー	承認者	アクション
1	Policy1	False	Process1	User1	—
2	Policy2	True	Process2	User2	拒否
3	Policy3	True	Process3	User3	—

ルールのオブジェクト

Identity Manager 管理者は、以下の 3 つのオブジェクトに基づいてイベントの承認ポリシーを作成できます。ただし、これらのオブジェクトが所定のイベントに適用され、イベント実行中に存在している場合に限ります。

- タスクの開始ソース – タスクを実行する Identity Manager 管理者。
- イベントのプライマリ オブジェクト – イベントと関連付けされているプライマリ オブジェクト。
- イベントのセカンダリ オブジェクト – プライマリ オブジェクトに対応する、イベントと関連付けされているセカンダリ オブジェクト。

ルールの評価

ポリシー ルールは、1 つのイベントに対して以下の 2 つの方法で評価することができます。

- 常時
- 承認条件に指定した属性が変更された場合のみ

注: この評価方法は、イベントのプライマリ オブジェクトだけに適用できます。

たとえば、以下のポリシーについて考えてみます。これらはすべて、[ユーザの変更]管理タスクの ModifyUserEvent 用のポリシーです。

ポリシー	ルール	評価
Policy1	User where (User ID = Smith01)	常時
Policy2	User where (Title = Manager)	Title 属性が変更された場合
Policy3	User where (Salary >= 80000)	Salary 属性が変更された場合

Policy1 は、管理者がユーザ Smith01 の[ユーザの変更]タスクを呼び出した場合に評価されます。どの属性が変更されたかは関係ありません。

Policy2 は、管理者が[ユーザの変更]タスクを呼び出して、任意のユーザ オブジェクトの Title 属性を変更した場合に評価されます。 Policy2 は Title 属性が Manager に変更された場合に真になります。

Policy3 は、管理者が[ユーザの変更]タスクを呼び出して、任意のユーザ オブジェクトの Salary 属性を変更した場合に評価されます。 Policy3 は Salary 属性が 80000 以上に変更された場合に真になります。

この例では、管理者が[ユーザの変更]タスクを使用してユーザ Smith01 の Title 属性を Manager に変更すると、Policy1 と Policy2 の両方が真に評価され、それぞれのワークフロー プロセスが開始されます。 この場合、標準的な優先度が適用されます。

条件付きルールの評価により、イベントの保留中に、ある作業項目の承認者が、同じイベントの他の作業項目に影響を与える属性を変更できるようになります。 前述の例では、管理者がユーザ Smith01 の属性を変更すると、Policy1 が真となり、作業項目が生成されます。 承認者は、Policy1 によって生成された作業項目を承認する一方で、同じ承認画面で Smith01 の Salary 属性を変更することが可能です。 この場合、Smith01 の新しい Salary の値によって、Policy3 が同じ ModifyUserEvent のインスタンスの作業項目を生成するかどうかが決まります。 承認者が Salary 属性を 90000 に変更すると、Policy3 は新しい作業項目を生成します。この作業項目は、イベント自体が承認される前に承認されている必要があります。 標準的な優先度が適用されます。

詳細情報:

ポリシー順序 (393 ページ)
ルールのオブジェクト (394 ページ)

ポリシーの例

以下のビジネスでの使用事例は、ワークフロー承認ポリシーの適用方法を示しています。

事例 1

使用事例 – 管理者は、ある従業員のリレーショナル データベース用のアカウントを変更します。

管理タスク –[ユーザの変更]

イベント– ModifyMSSQLAccountEvent

承認ルール– 次の条件を満たすユーザ (Title = RDBAcctManager)

ワークフロー プロセス – ModAcctApproval (カスタム ワークフロー プロセス)

オブジェクト– タスクの開始ソース

評価– 常時ルールを評価

事例 2

使用事例 – 管理者は、新たな昇給制度を反映するため、従業員の給与を変更します。

管理タスク –[ユーザの変更]

イベント– ModifyUserEvent

承認ルール – 次の条件を満たすユーザ (Salary >= 100000)

ワークフロー プロセス – SalaryChangeApproval (カスタム ワークフロー プロセス)

オブジェクト– イベントのプライマリ オブジェクト (ユーザ)

評価–[Salary]属性が変化した場合のみ評価

事例 3

使用事例 – 管理者は、あるユーザの肩書が契約社員に変わったときに、契約社員グループに 1 人のユーザを追加します。 この事例は、以下の 2 つの承認ポリシーに分割することができます。

ポリシー 1:

管理タスク –[ユーザの変更]

イベント– ModifyUserEvent

承認ルール – 次の条件を満たすユーザ（Title = Contractor）

ワークフロー プロセス – SingleStepApproval（デフォルトのプロセス テンプレート）

オブジェクト– イベントのプライマリ オブジェクト(ユーザ)

評価–[役職]属性が変化した場合のみ評価

ポリシー 2:

管理タスク –[グループの変更](または[グループメンバの変更])

イベント– AddToGroup

承認ルール – 以下の条件を満たすグループ(Group Name = Contractors)

ワークフロー プロセス – SingleStepApproval（デフォルトのプロセス テンプレート）

オブジェクト– イベントのセカンダリ オブジェクト(グループ)

評価– 常時ルールを評価

ポリシーベース ワークフローの設定方法

ポリシーベース ワークフローを設定する手順は、イベント レベル ワークフローを設定する手順に類似していますが、ワークフローを実行するかどうかを決定する承認ポリシーの定義ステップがあります。

ポリシーベース ワークフローの設定方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]または[管理タスクの作成]を選択します。

   [管理タスクの選択]画面が表示されます。

2. ワークフロー制御下で実行するタスクを検索して、[選択]をクリックします。

   [管理タスクの変更]または[管理タスクの作成]画面が表示されます。

3. [プロファイル]タブで、[ワークフローの有効化]がチェックされているかどうかを確認します。

4. [イベント]タブで、イベントを選択して、プロセス テンプレートにマッピングします。

   ワークフローのマッピングの画面が表示されます。

5. [ポリシー ベース]ラジオ ボタンを選択し、[追加]をクリックします。

   [承認ポリシー]画面が表示されます。

6. 承認ポリシーを設定します。(398 ページ)

7. 選択したワークフロー プロセスに必要となる参加者リゾルバを設定します。

   参加者のリクエストがプロセスに追加されます。

8. [OK]をクリックします。

   CA Identity Manager によってイベント レベルのワークフロー設定が保存されます。

9. [送信]をクリックします。

   CA Identity Manager によってタスクの変更が処理されます。

注: ワークフロー プロセス リストには、テンプレート メソッドと WorkPoint メソッドの両方で使用するプロセスが含まれています。

- テンプレート メソッド(SingleStepApproval または TwoStageApprovalProcess のいずれか)が選択されると、ページが展開されて、参加者リゾルバの設定が有効になります。
- WorkPoint method が選択されると、このページは展開されません。 参加者リゾルバは WorkPoint Designer で設定されます。

詳細情報:

承認ポリシーの設定方法(398 ページ)
参加者リゾルバ: テンプレート メソッド(356 ページ)
参加者リゾルバ: WorkPoint メソッド(372 ページ)

承認ポリシーの設定方法

あるイベントの承認ポリシーを設定するには、以下に示す最上位レベルの手順が必要となります。

1. テスト対象のオブジェクトを選択します。
2. そのオブジェクトの承認ルールを定義します。
3. プライマリ オブジェクトの場合、これが条件付きの評価であるかどうかを判断します。

4. ポリシー評価の順序を入力します。
5. そのルールが True である場合に実行するワークフロー プロセスを設定します。

承認ポリシーを設定する方法

1. [承認ポリシー]画面で、テストするルールの対象オブジェクトをドロップダウンボックスから選択します。

   行った選択を反映して、画面が変化します。
2. オブジェクト名の横にある新しいドロップダウン メニューから、条件式テンプレートを選択します。

   行った選択を反映して、画面が変化します。
3. 必要に応じて条件式を作成および編集します。
4. [ルールの評価]ラジオ ボタンを選択して、ルールの評価を常時行うか、承認条件の属性が変更された場合のみ行うかを示します。
5. 正の整数値を入力して、ポリシーの評価順序(そのイベントに対して複数のポリシーが存在する場合)を指定します。
6. そのルールが True と評価された場合に実行するワークフロープロセスの選択および設定を行います。
7. [OK]をクリックして、承認ポリシーを保存します。

詳細情報:

ポリシーベース ワークフローの設定方法(397 ページ)
イベント レベルのワークフローの設定方法(355 ページ)

ポリシーベースのワークフロー ステータス

Identity Manager 管理者は、以下に示す標準的なシステム ツールを使用して、ワークフロー承認ポリシーを含むタスクのステータスを表示できます。

- [サブミット済みタスクの表示]タブ
- [ユーザ履歴]タブ
- レポートとログ

サブミットされたタスクおよびタスク履歴情報には、以下のようなものがあります。

- タスクおよびイベント情報
- ワークフローおよび承認ルール情報
- 承認ルールの評価結果

サブミット済みタスクの履歴の説明については、[システム]タブ関連文書を参照してください。

詳細情報:

Identity Manager のタスク ステータス(458 ページ)
イベント ステータスの説明(466 ページ)

オンライン リクエスト

Identity Manager では、汎用のオンライン リクエスト タスクを作成できます。 デフォルトのオンライン リクエストの実装は、自己変更リクエストと管理ユーザ変更リクエストの両方の関連タスク セットで構成されます。 ただし、オンライン リクエスト機能は、他の Identity Manager リクエスト タスクに対しても簡単に実装できます。

ユーザ変更リクエストによって、作業アイテムを生成するワークフロー プロセスがトリガされます。 ワークフロー参加者は、作業アイテムを承認して実装するか、拒否することができます。 タスクを開始するユーザは、履歴エディタ(リクエストの履歴を保守するために Identity Manager が使用するテキスト領域)にリクエストの説明を入力します。 この履歴エディタは、参加者が作業アイテムに対して実行したアクションについてコメントを残せるように設定することができます。 これらのコメントは、累積的な作業アイテム履歴の一部になります。

標準の承認アクションと拒否アクションのほかに(あるいはその代わりに)新しいアクションを実行することもできます。 たとえば、ビジネス参加者がリクエストの明確化やコメント作成をしたり、技術参加者がリクエストを実装することができます。 これらの新しいアクティビティは、[明確化]や[実装]などの新しいワークフロー アクション ボタンで表現できます。これらのボタンは、承認タスク上の標準の[承認]ボタンと[拒否]ボタンに加えることができます。

オンライン リクエスト タスク

デフォルトのオンライン リクエストの実装内容を構成する連携タスクは 5 つあります。 これらのタスクは、カスタム リクエスト、履歴、ワークフロー アクション ボタンの使用法を示します。

注: 管理タスク([マイ アカウントの変更]、[オンライン リクエストの作成])は、デフォルトによりコンサルテーション プロセス テンプレートを使用するイベント レベルのワークフロー用に設定されます。

[マイ アカウントの変更]

ユーザ アカウントの変更リクエストを作成する自己変更管理タスクです。 このタスクの[リクエスト]タブには、リクエストについて記述するための履歴エディタがあり、[プロファイル]タブには読み取り専用のユーザ詳細が表示されます。

[オンライン リクエストの作成]

特定のユーザに対するアカウント変更リクエストを作成するユーザ変更管理タスクです。 このタスクの[リクエスト]タブには、リクエストについて記述するための履歴エディタがあり、[対象プロファイル]タブには読み取り専用のユーザ詳細が表示されます。

[オンライン リクエストの承認]

ビジネス参加者がタスクの承認または拒否、あるいはタスクの明確化リクエストを行うことを許可する承認タスクです。 このタスクの[リクエスト]タブには、履歴表示とクエリまたはコメント用の履歴エディタ、読み取り専用の[対象プロファイル]タブ、および[担当者]タブがあります。

[オンライン リクエストの明確化]

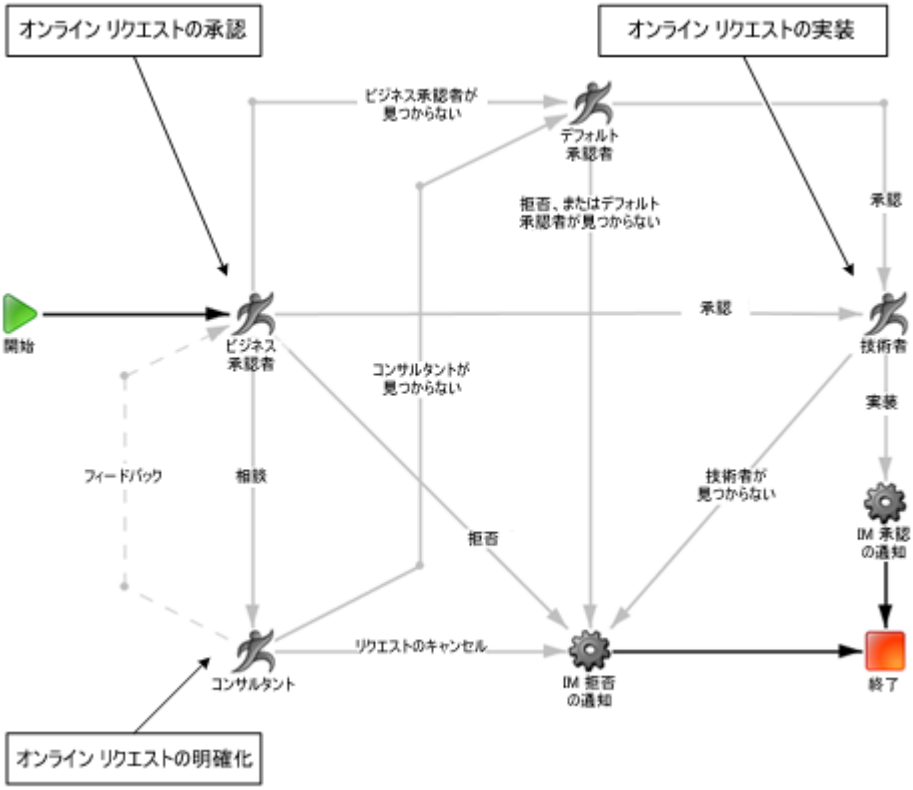
明確化の参加者が明確化リクエストに応答し、承認のためにビジネス参加者にタスクを返送することを許可する承認タスクです。 このタスクの[リクエスト]タブには、履歴表示とコメント用の履歴エディタ、および読み取り専用の[対象プロファイル]タブがあります。

[オンライン リクエストの実装]

技術参加者がタスクを実装し、タスク履歴にコメントを追加することを許可する承認タスクです。 このタスクの[実装リクエスト]タブには、履歴表示とコメント用の履歴エディタ、読み取り専用の[対象プロファイル]タブ、および[担当者]タブがあります。

オンライン リクエスト プロセス

オンライン リクエスト タスクは、コンサルテーション プロセスと呼ばれるワークフロー プロセス テンプレートによって制御されます。このテンプレートは、WorkPoint Designer では以下のように示されます。



コンサルテーション プロセスには、以下の 4 つの手動アクティビティが含まれます。これらは、オンライン リクエスト実装の承認タスクに対応しています。

- 作業アイテムを拒否するか、作業アイテムを承認して技術者に渡すか、コンサルタントからさらに明確化をリクエストするビジネス承認者のアクティビティ
- 作業アイテムを明確化し、ビジネス承認者に返送するコンサルタントのアクティビティ
- ビジネス承認者またはコンサルタントと連絡が取れない場合に引き継ぐデフォルトの承認者のアクティビティ
- リクエストを実装し、作業アイテムを完了する技術者のアクティビティ

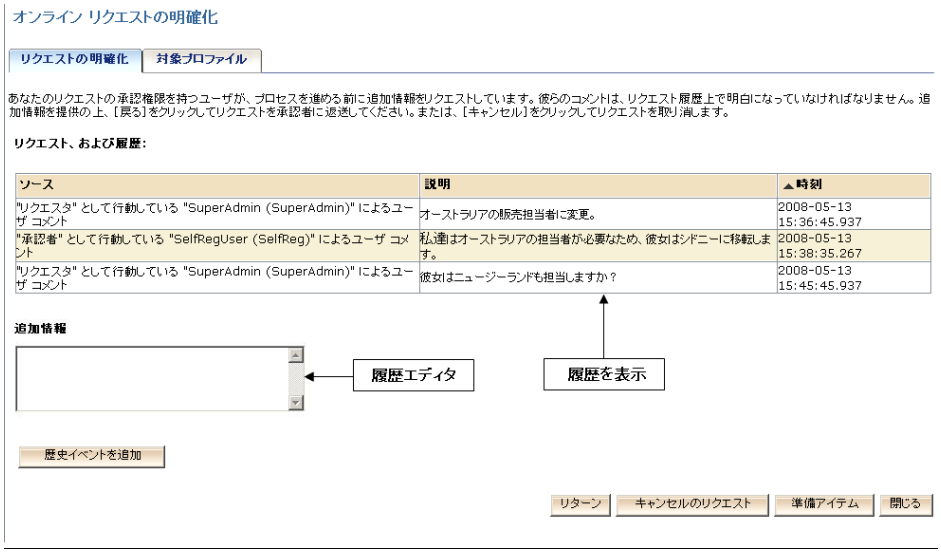
オンライン リクエスト履歴

オンライン リクエスト履歴機能を使用すると、参加者は作業アイテムに対するアクションの記録を作成できます。 作業アイテムは、ある参加者から別の参加者に渡す必要があるので、新しい参加者はアクションを実行する前に、作業アイテム履歴を確認することができます。

オンライン リクエスト履歴の実装には、以下の 2 つのコントロールが使用されます。

- 履歴表示は、以前の履歴エントリの詳細情報が時系列順に含まれた読み取り専用テーブルです。
- 履歴エディタは、新しい履歴エントリを作成するためのテキスト ボックスです。 また、作業アイテムをサブミットせずに、複数のエントリを追加できるオプション ボタンもあります。

デフォルトにより、履歴エディタと履歴表示は、オンライン リクエスト実装と関連付けられたすべてのタスクの[リクエスト]タブに表示されます。 以下の画面に、[オンライン リクエストの明確化]タスクの履歴コントロールを示します。



オンライン リクエストの使用

以下に、オンライン リクエストのワークフロー プロセスのステップを示します。 各手順のかっこ内に、生成される IM タスクを示します。 プロセスの各ステップでは、参加者が履歴エディタでコメントを追加することができます。 このコメントは履歴表示に示され、ワークフロー プロセスの次の参加者が見ることができます。

1. タスク開始者が IM ユーザの変更をリクエストします([オンライン リクエストの作成])。
2. 業務系承認者が作業アイテムを受け取り、以下のいずれかを行います。
   - 作業アイテムを承認します([オンライン リクエストの承認])。
   - 作業アイテムを拒否し、ワークフロー プロセスを終了します。 新しいタスクは生成されません。
   - コンサルタントからの明確化をリクエストします([オンライン リクエストの明確化])。
3. コンサルタントが作業アイテムを受け取り、以下のいずれかを行います。
   - 明確化を追加し、作業アイテムを業務系承認者に返します。 新しいタスクは生成されません。
   - 作業アイテムをキャンセルし、ワークフロー プロセスを終了します。 新しいタスクは生成されません。
4. 技術者が作業アイテムを受け取り、リクエストを実装します([オンライン リクエストの実装])。

ワークフロー アクション ボタン

Identity Manager の承認タスクには、始めから[承認]ボタンと[拒否]ボタンが用意されています。これらのボタンは、対応する作業アイテム画面に表示されます。 ワークフロー アクション ボタンでは、管理者が承認タスクにアクション ボタンを追加したり、既存のボタンを削除または変更して、Identity Manager のタスクとワークフローの機能を拡張することができます。 (標準の[承認]ボタンと[拒否]ボタンは、カスタム ワークフロー アクション ボタンと同じ方法で実装されます。)

たとえば、あるワークフロー プロセスで、中級レベルの参加者が一部のケースを上級レベルの参加者にエスカレーションして、最終的な承認または拒否を求めるためのアクションが必要だとします。 この場合、中級レベルの参加者は、履歴エディタを使用してコメントまたは推奨事項を追加し、確認と承認または拒否を行う上級レベルの参加者にその作業アイテムを送信できます。

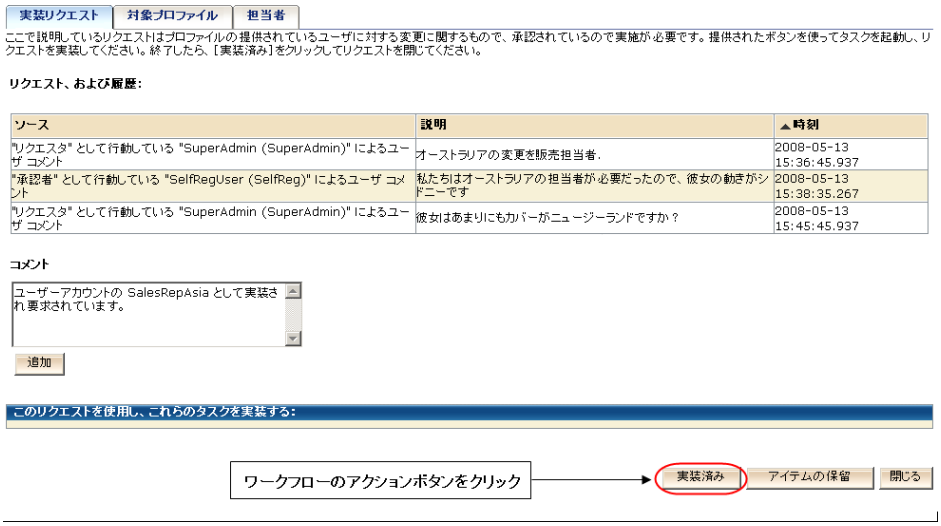
ワークフロー アクション ボタンを追加または削除する際には、これらの新しいアクションを処理するために、ビジネス ロジックを提供する WorkPoint ワークフロー プロセスに適切な変更を加える必要があります。

詳細情報

承認タスクのワークフロー ボタン(405 ページ)
Identity Manager でのボタン設定(406 ページ)
WorkPoint Designer でのボタン設定(408 ページ)

承認タスクのワークフロー ボタン

ワークフロー アクション ボタンは、WorkPoint プロセス図の手動アクティビティ ノードから外に向いている移行ノードに対応します。 たとえば、コンサルテーション プロセスの技術者のアクティビティ ノードには、「実装済み」と呼ばれる移行が 1 つあります。以下の図に示すように、これはオンライン リクエストの実装の承認タスクの[実装済み]ボタンに対応しています。



注: [アイテムの保留]ボタンと[閉じる]ボタンは、ワークフロー制御下ではなく、Identity Manager のプログラミング ロジックによって制御されます。

詳細情報:

ワークフロー アクション ボタン (404 ページ)
Identity Manager でのボタン設定 (406 ページ)

Identity Manager でのボタン設定

ワークフロー アクション ボタンを設定するには、承認タスクの[プロファイル]タブで、[Workflow Action Buttons(ワークフロー アクション ボタン)]という名前のボタンをクリックします。 以下のようなボタンの[プロファイル]タブが表示されます。

ボタンの[プロファイル]タブにはテーブルがあり、各行が 1 つのワークフロー アクション ボタンを示しています。 各ボタンの行には、以下の 4 つのプロパティがあります。これらはテーブル内の列に対応します。

表示名

承認画面内のボタンに表示される名前。 これは条件付きでローカライズされる値です。値には、リソース ファイル内の文字列か、ローカライズされた文字列を示すキーを使用できます。

アクション

オプションの選択時にワークフロー プロセスに返される値。 この値は、WorkPoint プロセス図内で対応する移行ノードの属性を示します。 これはローカライズされない文字列です。 デフォルト設定は「approved」と「rejected」です。

ツール ヒント

ユーザがボタン上にマウス カーソルを合わせたときに表示される、ボタン アクションについての簡単な説明(ツール ヒント)。 これは条件付きでローカライズされる値です。値には、リソース ファイル内の文字列か、ローカライズされた文字列を示すキーを使用できます。

Long Description(詳細説明)

ボタン アクションについての詳細説明。これにより、[サブミット済みタスクの表示]画面上のアクションについて説明するメッセージが追加されます。 これが空白の場合は、[サブミット済みタスクの表示]画面上に表示されるメッセージがボタン名となります。 これは条件付きでローカライズされる値です。値には、リソース ファイル内の文字列か、ローカライズされた文字列を示すキーを使用できます。

詳細情報:

WorkPoint Designer でのボタン設定(408 ページ)

ワークフロー アクション ボタンの追加

既存のワークフロー プロセスに新しいボタンを追加するための概要手順は以下のとおりです。

1. Identity Manager で、ワークフロー ボタンを追加します。

   詳細については、ワークフロー アクション ボタンの追加方法(407 ページ)を参照してください。

2. 必要に応じて、ローカライズ キーを追加します。

   詳細については、「Configuration Guide」を参照してください。

3. WorkPoint Designer で、新しい必須ノードを追加します。

   詳細については、WorkPoint Designer のオンライン ヘルプを参照してください。

4. WorkPoint Designer の移行ノードで、スクリプトを定義します。

   詳細については、WorkPoint Designer でのボタン設定(408 ページ)を参照してください。

詳細情報

ワークフロー アクション ボタンの追加方法(407 ページ)
WorkPoint Designer でのボタン設定(408 ページ)

ワークフロー アクション ボタンの追加方法

CA Identity Manager で、承認タスクに[ワークフロー アクション ボタン]を追加することができます。

管理タスクにワークフロー アクション ボタンを追加する方法

1. ユーザ コンソールで、[ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。

   [Select Admin Task]画面が表示されます。

2. 承認タスクを検索し、[選択]をクリックします。

   [管理タスクの変更]画面が表示されます。

3. [プロファイル]タブで、[Workflow Action Buttons(ワークフロー アクション ボタン)]という名前のボタンをクリックします。

   [Workflow Action Button Profile]タブが表示されます。

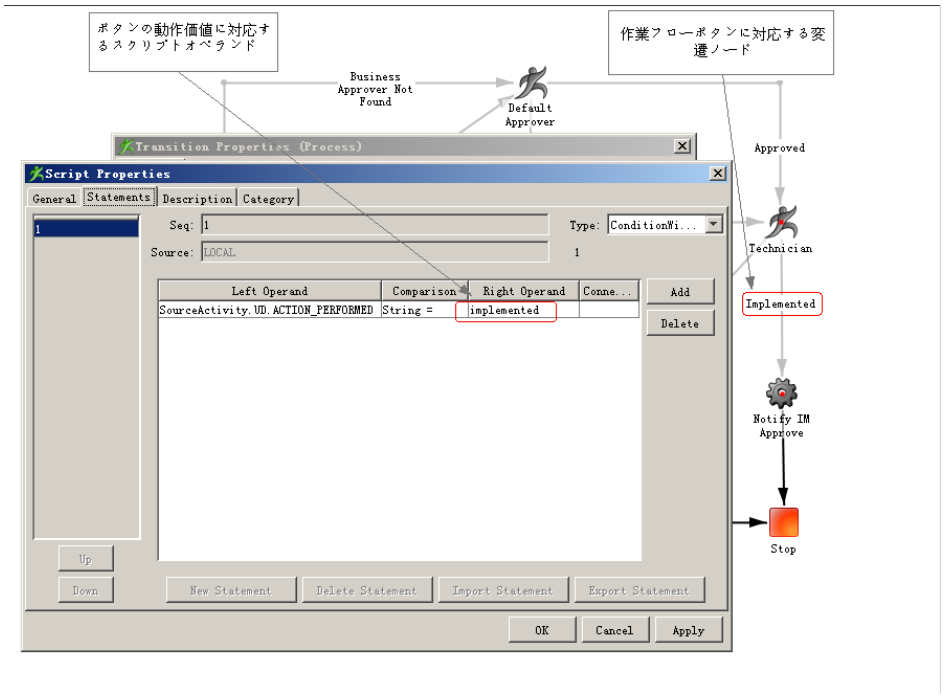
4. ［ボタンの追加］をクリックし、承認タスクに新しいボタンを追加します。
5. ボタンのプロパティ情報を入力します。
6. ［OK］をクリックします。

   CA Identity Manager に新しいボタンの情報が保存されます。
7. ［送信］をクリックします。

   CA Identity Manager によってタスクの変更が処理されます。

WorkPoint Designer でのボタン設定

以下の図に示すように、WorkPoint Designer では、移行ノードのスクリプト プロパティを使用してワークフロー アクション ボタンが設定されます。



デフォルトにより、ワークフロー アクション ボタンは以下のスクリプト プロパティを使用して、文字列の比較を行います。

- ［Left Operand］-- 前の手動アクティビティ ノードの［ユーザ データ］プロパティで定義された ACTION_PEFORMED
- ［Right Operand］-- ユーザ コンソールのボタン プロファイル タブで定義された、ボタンのアクション値

注: アクティビティ ノードと移行ノードのスクリプトおよびプロパティの詳細については、WorkPoint Designer のオンライン ヘルプを参照してください。

詳細情報:

Identity Manager でのボタン設定 (406 ページ)

ワーク リストと作業アイテム

ワーク リストは、タスクの承認権限が与えられた参加者のユーザ コンソールに表示される作業アイテム(または承認タスク)のリストです。 作業アイテムは、ワークフロー プロセス内の手動アクティビティと対応します。 作業アイテムは、ワーク リスト内の行で表されます。

ワーク リストに作業アイテムを追加する方法は以下のとおりです。

- 参加者リゾルバが承認者のリストを決定します。
- 別のユーザから、委任された作業アイテムを受け取ります。
- 作業アイテムを別のユーザに再度割り当てます。

ワーク リストから作業アイテムを削除する方法は以下のとおりです。

- 作業アイテムを完了(承認または拒否)します。
- 作業アイテムを別のユーザに再度割り当てます。
- 作業アイテムを保留します。 これにより、他のすべての承認者のワーク リストから、その作業アイテムが削除されます。

作業アイテム上に表示される情報タブは、ワークフローによって生成された作業アイテムが、タスク レベルとイベント レベルのどちらの制御下にあるのかによって異なります。

- [プロファイル]- イベントの影響を受けるオブジェクトに関するプロファイル情報が表示されます(イベント レベルのみ)。
- [タスクの詳細]- タスク内のすべてのイベントに関する詳細情報が表示されます(タスク レベルのみ)。
- [承認者]- タスクまたはイベントに関するすべての個人承認者と委任者をリストします(タスク レベルおよびイベント レベル)

ワーク リストの表示

他のユーザが開始したタスク(または作業アイテム)を承認する参加者として割り当てられている場合は、ユーザ コンソールにログインすると、ワーク リストが自動的に表示されます。

ワーク リストを手動で表示する方法

1. ユーザ コンソールで、[ホーム]-[マイ ワーク リストの表示]を選択します。

   ワーク リストが表示されます。

2. 表示する作業アイテムの名前をクリックします。

   選択した作業アイテムが表示されます。

管理者は、スコープの対象となるユーザの作業アイテムを管理することができます。

注: ユーザの作業アイテムを管理する際には、管理者が作業アイテムを保留できます。ユーザのワーク リストを表示しても、作業アイテムに変更を加えることはできません。

他のユーザのワーク リストを表示する方法

1. ユーザ コンソールで、[ユーザ]-[作業アイテムの管理]-[ユーザのワーク リストの表示]を選択します。

   ユーザ選択画面が表示されます。

2. 表示するワーク リストを所有するユーザを検索し、[選択]をクリックします。

   そのユーザのワーク リスト画面が表示されます。

他のユーザの作業アイテムを管理する方法

1. ユーザ コンソールで、[ユーザ]-[作業アイテムの管理]-[ユーザのワーク リストの表示]を選択します。

   ユーザ選択画面が表示されます。

2. 管理する作業アイテムを所有するユーザを検索し、[選択]をクリックします。

   そのユーザのワーク リスト画面が表示されます。

3. 表示する作業アイテムの名前をクリックします。

   選択した作業アイテムが表示されます。

作業アイテムの保留

「要確認」の作業アイテムを保留し、その作業アイテムを他の参加者のワーク リストから削除することができます。 作業アイテムを保留すると、保留を実行したユーザのみがその作業アイテムを扱えるようになります。

保留したユーザが作業アイテムを解放すると、他の参加者のワーク リストに再びその作業アイテムが表示されるようになります。 保留したユーザが作業アイテムを承認または拒否すると、その作業アイテムは完了となり、他の参加者には表示されなくなります。

詳細情報

委任と保留済み作業アイテム(411 ページ)
再割り当てと保留済み作業アイテム(411 ページ)

再割り当てと保留済み作業アイテム

作業アイテムが再割り当てされている最中に、ユーザが作業アイテムを保留した場合は、そのユーザの保留が継続されます。 ただし、その後このユーザが作業アイテムを解放すると、このユーザはその作業アイテムにアクセスできなくなります。

管理者は、他のユーザの作業アイテムを再割り当て、保留、または解放できますが、他のユーザの作業アイテムを承認または拒否することはできません。 これを実行できるのは、割り当てられた作業アイテムの参加者のみです。

詳細情報

作業アイテムの再割り当て(416 ページ)

委任と保留済み作業アイテム

委任がアクティブになっている場合は、代行者または委任者が作業アイテムを保留することができます。 あるユーザが保留した作業アイテムを、別のユーザのワーク リストに表示することはできません。

たとえば、委任が撤回されている最中に、代行者が作業アイテムを保留した場合は、代行者がその作業アイテムの保留を続けることができます。 ただし、その後この代行者が作業アイテムを解放すると、このユーザはその作業アイテムにアクセスできなくなります。

代行者になっているユーザが作業アイテムを保留している最中に、その代行者が削除された場合でも、代行者がその作業アイテムを保持し続けることができます。 その後、代行者がこの作業アイテムを承認した場合は、監査を行っても元の委任者を判別できなくなります。

委任が撤回されている最中に、代行者が作業アイテムを保留した場合は、その作業アイテムが完了または解放されるまで、代行者のアクセス権は保持されます。

詳細情報

作業アイテムの保留 (411 ページ)
作業アイテムの委任 (412 ページ)

作業アイテムの保留または解放方法

「要確認」の作業アイテムを保留し、その作業アイテムを他の参加者のワーク リストから削除することができます。

保留した作業アイテムが他の参加者のワーク リストに表示されるようにするには、その作業アイテムを解放します。

注: 保留した作業アイテムを他の参加者が使用できるようにするには、作業アイテムを明示的に解放する必要があります。

作業アイテムを保留または解放する方法

1. ユーザ コンソールで、[ホーム]-[マイ ワーク リストの表示]を選択します。

   ワーク リストが表示されます。

2. 保留または解放する作業アイテムを選択します。

   作業アイテムの拡張画面が表示されます。

3. [アイテムの保留]または[アイテムの解放]をクリックします。

   CA Identity Manager によってアクションが確認されます。

作業アイテムの委任

作業アイテムの委任では、ユーザ(委任者)が別のユーザ(代行者)を指定して、代行者が委任者のワーク リスト内のタスクを承認できるようにします。 委任者が「外出」する際には、その期間だけ別の承認者に作業アイテムを割り当てることができます。委任者は、委任期間中でも自分の作業アイテムに完全にアクセスすることができます。

委任された作業アイテムは何も変わらない状態で示されます。 ロギングを行うと、作業アイテムが委任されたかどうかがわかります。

委任は、代行者が委任者に「なりすまし」、委任者のワーク リスト上のアイテムを表示できるようにすることで機能します。 代行者がワーク リストを表示すると、自分の作業アイテムのほかに委任者の作業アイテムも表示されます。

委任は移行型ではありません。 代行者は、委任者が直接割り当てた作業アイテムしか見ることができません。 たとえば、ユーザ A がユーザ B に作業アイテムを委任し、ユーザ B がユーザ C に作業アイテムを委任した場合、ユーザ C はユーザ B に属する作業アイテムしか見ることができず、ユーザ A がユーザ B に委任した可能性のある作業アイテムは見ることができません。

詳細情報

委任と保留済み作業アイテム(411 ページ)

委任の汎用属性

委任では、以下の汎用属性が使用されます。

%DELEGATORS%

この汎用属性には、この属性を持つユーザに委任しているユーザの名前と、委任が作成された時刻が格納されます。

委任の有効化方法

他のユーザに作業アイテムを委任するには、ワークフロー承認の委任を有効化しておく必要があります。 デフォルトでは、委任は無効になっています。

ワークフロー承認の委任を有効化するには、以下の手順に従います。

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

   http://hostname/idmmanage

   hostname

   CA Identity Manager がインストールされているサーバの完全修飾ドメイン名を定義します。 たとえば、myserver.mycompany.com:port です。

2. [環境]をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. [Advanced Settings]をクリックし、次に[Work Item Delegation]をクリックします。
4. [Enabled]チェック ボックスをオンにし、[Save]をクリックします。

詳細情報

自分の作業アイテムを委任する方法(414 ページ)
他のユーザの作業アイテムを委任する方法(415 ページ)

自分の作業アイテムを委任する方法

「外出」する際には、その期間だけ別のユーザに作業アイテムを委任することができます。委任者は、委任期間中でも自分の作業アイテムに完全にアクセスすることができます。

自分の作業アイテムを委任する方法

1. ユーザ コンソールで、[ホーム]-[不在時のアシスタント]を選択します。

   [不在時のアシスタント]画面が表示されます。

2. [ユーザの追加]をクリックします。

   ユーザ選択画面が表示されます。

3. 代行者にするユーザ(複数可)を検索し、選択します。

   選択したユーザが代行者リストに追加されます。

4. [サブミット]をクリックします。

   タスクがサブミットされ、委任内容が保存されます。

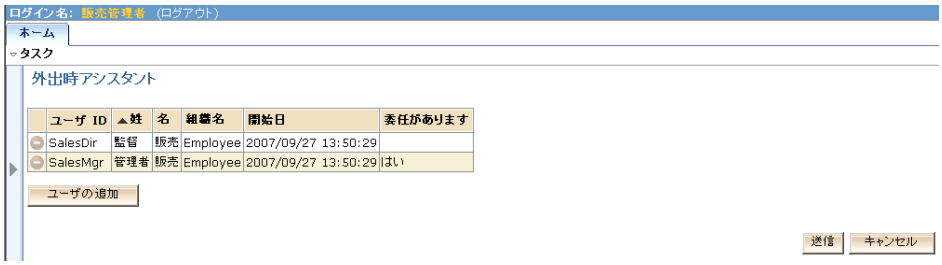
注: すでに代行者になっているユーザは、代行者の追加時に検索結果に表示されません。

詳細情報:

委任の有効化方法(413 ページ)

[外出時アシスタント]画面

自分の代行者を追加および削除するには、以下の[外出時アシスタント]画面を使用します。



[外出時アシスタント]画面には、現在の代行者のリストが表示されます。 リストには、代行者を識別する列のほかに以下の 2 つの列があります。

開始日

委任が作成された日付が表示されます。

委任があります

代行者が他のユーザに作業アイテムを委任したかどうかが示されます。

他のユーザの作業アイテムを委任する方法

管理者は、あるユーザ(委任者)の作業アイテムを別のユーザに委任することができます。たとえば、あるユーザが予定外に外出してしまった場合や、管理者が大きな作業負荷を複数のユーザに割り当てる必要がある場合があります。

管理者は、スコープの対象となるユーザの作業アイテムしか委任できません。 同様に、管理者が代行者リストに追加または削除できるのは、自分が管理しているユーザのみです。

他のユーザの作業アイテムを委任する方法

1. ユーザ コンソールで、[ユーザ]-[作業アイテムの管理]-[作業アイテムの委任]を選択します。

   ユーザ選択画面が表示されます。

2. 委任する作業アイテムを所有するユーザ(委任者)を検索し、[選択]をクリックします。

   作業アイテムの委任画面が表示されます。

3. [ユーザの追加]をクリックします。

   ユーザ選択画面が表示されます。

4. 代行者にするユーザ(複数可)を検索し、選択します。

   選択したユーザが代行者リストに追加されます。

5. [サブミット]をクリックします。

   タスクがサブミットされ、委任内容が保存されます。

注: すでに代行者になっているユーザは、代行者の追加時に検索結果に表示されません。

詳細情報:

委任の有効化方法(413 ページ)

委任を削除する方法

委任が設定されている場合にユーザが CA Identity Manager にログインすると、CA Identity Manager に以下のメッセージが表示されます。

委任が設定されました。それらがまだ必要であることを確認してください。

自分の委任を削除する方法

1. ユーザ コンソールで、[ホーム]-[不在時のアシスタント]を選択します。

   [不在時のアシスタント]画面が表示されます。

2. 削除する代行者のマイナス記号(-)をクリックします。

   選択した代行者がリストから削除されます。

3. [送信]をクリックします。

   タスクがサブミットされ、委任内容が削除されます。

他のユーザの委任を削除する方法

1. ユーザ コンソールで、[ユーザ]-[作業アイテムの管理]-[作業アイテムの委任]を選択します。

   ユーザ検索画面が表示されます。

2. 削除する委任を所有するユーザを検索し、選択します。

   代行者リストが表示されます。

3. 削除する代行者のマイナス記号(-)をクリックします。

   選択した代行者がリストから削除されます。

4. [送信]をクリックします。

   タスクがサブミットされ、委任内容が削除されます。

注: 代行者を削除できるのは、そのユーザに対するスコープがある場合のみです。

作業アイテムの再割り当て

再割り当てを行うと、ユーザと管理者が作成済みの作業アイテムの担当者を変更できます。 管理者は以下のことを実行できます。

- 他のユーザのワーク リストの表示
- 作業アイテムの担当者の追加および削除
- 作業アイテムの保留ステータスの変更

たとえば、管理者は作業アイテムを再度割り当てたり、アクションを実行しないユーザから保留中の作業アイテムを解放することができます。

作業アイテムが再割り当てされている最中に、ユーザが作業アイテムを保留した場合は、そのユーザの保留が継続されます。 ただし、その後このユーザが作業アイテムを解放すると、このユーザはその作業アイテムにアクセスできなくなります。

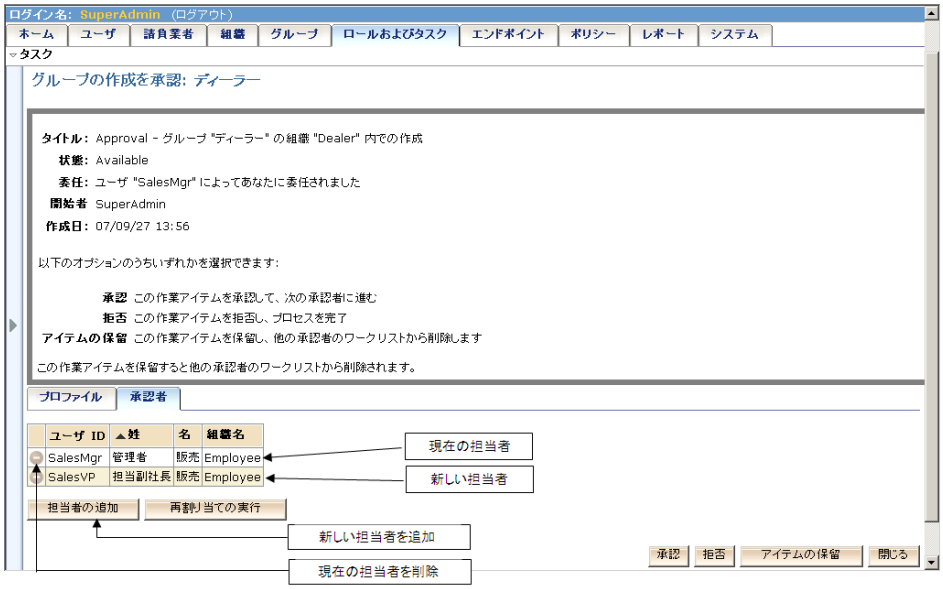
委任が撤回されている最中に、代行者が作業アイテムを保留した場合は、その作業アイテムが完了または解放されるまで、代行者のアクセス権は保持されます。

詳細情報

再割り当てと保留済み作業アイテム(411 ページ)

[承認者]タブ

再割り当てを実行するには、[ワークアイテム承認者]タブを使用します。このタブには、現在の作業アイテムの承認者(担当者)のリストが表示されます。 再割り当ての実行時には、開いている作業アイテムがリスト内のすべての承認者に割り当てられます。 したがって、新しい担当者に作業アイテムを再割り当てするには、以下の図に示すように、現在の担当者を明示的に削除する必要もあります。



作業アイテムの再割り当て方法

あるユーザから別のユーザに作業アイテムを再割り当てする手順は以下の 2 つです。

- 新しい承認者を選択します。
- 現在の承認者を削除します。

注: 再割り当て先のユーザに対してスコープが必要です。

自分の作業アイテムを再割り当てするには、以下の手順に従います。

1. [ホーム]-[マイ ワーク リストの表示]を選択します。

   ワーク リストが表示されます。

2. 作業アイテムを選択し、拡張します。
3. [承認者]タブを選択します。

   現在管理中のワーク リストを所有するユーザを含め、現在の承認者全員のリストが表示されます。

4. [担当者の追加]をクリックします。

   ユーザ選択画面が表示されます。

5. 再割り当て先のユーザ(複数可)を検索し、選択します。
6. 自分を担当者として削除するには、マイナス記号のボタン(-)をクリックします。
7. [再割り当ての実行]をクリックします。

   再割り当てされたユーザのワーク リストに、その作業アイテムが表示されます。

注: 管理者は、他のユーザの作業アイテムを再割り当て、保留、または解放できますが、他のユーザの作業アイテムを承認または拒否することはできません。 これを実行できるのは、作業アイテムの所有者のみです。

他のユーザの作業アイテムを再割り当てするには、以下の手順に従います。

1. [ユーザ]-[作業アイテムの管理]-[ユーザの作業アイテムの管理]を選択します。

   ユーザ選択画面が表示されます。

2. 再割り当てする作業アイテムを所有するユーザを検索し、[選択]をクリックします。

   [ユーザの作業アイテムの管理]画面が表示されます。

3. 作業アイテムを選択し、拡張します。
4. [承認者]タブを選択します。

   現在管理中のワーク リストを所有するユーザを含め、現在の承認者全員のリストが表示されます。

5. [担当者の追加]をクリックします。

   ユーザ選択画面が表示されます。

6. 再割り当て先のユーザ(複数可)を検索し、選択します。
7. 現在の担当者を削除するには、マイナス記号のボタン(-)をクリックします。

8. ［再割り当ての実行］をクリックします。

   再割り当てされたユーザのワーク リストに、その作業アイテムが表示されます。

第 18 章: 電子メール通知

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 Identity Manager の電子メール通知 (421 ページ)
SMTP の設定 (421 ページ)
電子メール通知の有効化 (424 ページ)
電子メールを送信するためのイベントまたはタスクの設定 (425 ページ)
電子メールのコンテンツ (426 ページ)
電子メール テンプレート (427 ページ)
電子メール テンプレートの作成 (430 ページ)
電子メールのカスタム テンプレート (430 ページ)
電子メール テンプレートの展開 (448 ページ)

CA Identity Manager の電子メール通知

電子メール通知は、CA Identity Manager ユーザに、システムのタスクとイベントに関する情報を提供します。 CA Identity Manager は、以下のいずれかが発生した場合に電子メール通知を生成します。

- ワークフロー承認者による承認または拒否が必要なイベントが保留中である。
- 承認者がイベントを承認する。
- 承認者がイベントを拒否する。
- イベントまたはタスクが完了する。
- ユーザが、忘れたパスワード機能を使用して一時パスワードをリクエストする。

CA Identity Manager 電子メール通知を使用するには、SMTP を設定して、CA Identity Manager で電子メール通知を有効にします。

SMTP の設定

電子メール通知を有効にする前に、SMTP を設定します。 お使いのアプリケーションサーバの SMTP を設定するには、以下のセクションを参照してください。

JBoss 上での SMTP の設定

SMTP を設定する方法

1. テキスト エディタで、次のようにしてメール サービスの配備記述子を開きます。
   jboss_home\server\default\deploy\mail-service.xml
2. mail.smtp.host プロパティを、次のようにして、SMTP サーバの名前に修正します。
   <-- Change to the SMTP gateway server -->
   <property name="mail.smtp.host" value="your_smtp_server "/>
   たとえば、次のようにします。
   <property name="mail.smtp.host" value="smtp.mailserver.company.com"/>
3. mail-service.xml ファイルを保存します。
4. テキスト エディタで、次の電子メール プロパティ ファイルを開きます。
   jboss_home¥server¥default¥deploy¥Identity Manager.ear¥config¥com¥netegrity¥config¥email.properties
5. 電子メールを生成したワークフローで使用される、電子メールの復帰アドレスを設定するには、admin.email.address プロパティを見つけて、その値に該当する電子メール アドレスを設定します。 たとえば、次のようにします。
   admin.email.address=admin@company.com
6. 管理コンソールで、電子メールの通知を有効にします。

注: JBoss の同じインスタンスに複数の ear をインストールする場合は、application_id_mail-service.xml という名前の jboss_home¥server¥default¥deploy¥mail-service.xml のコピーを作成し、mbean の名前を application_id-Mail に変更し、<attribute name="JNDIName">java:/Mail</attribute> を <attribute name="JNDIName">java:iam/application_id/mail/Mail</attribute> へ変更します。

WebLogic 9.2 での SMTP の設定

WebLogic サーバの管理者コンソール、および email.properties ファイルで電子メールを設定します。

WebLogic に対して電子メールを設定する方法

1. WebLogic サーバの管理者コンソールで、次のプロパティを持つ新しいメール セッションを作成します。
   - mail.smtp.host プロパティ: この値を対象の SMTP サーバに設定します。 例: mail.smtp.host=mymailserver.company.com
   - mail.transport.protocol プロパティ: この値を SMTP に設定します。 例: mail.transport.protocol=smtp
   - JNDI Name: nete/Mail
   - Target: WebLogic のサーバ名
2. テキスト エディタで、CA Identity Manager に対する以下の電子メール プロパティ ファイルを開きます。

   weblogic_domain¥applications¥IdentityMinder.ear¥config¥com¥netegrity¥config¥email.properties
3. admin.email.address プロパティを見つけて、その値を該当する電子メール アドレスに設定し、ワークフローで生成した電子メールで使用される電子メールの復帰アドレスを設定します。 以下に例を示します。

   admin.email.address=admin@company.com
4. 管理コンソールでの電子メール通知の有効化

WebSphere 上での SMTP の設定

CA Identity Manager コンポーネントをインストールした後で実行する imsSetup ユーティリティは、mailMail という名前の新しいメール セッション オブジェクトを設定します。

電子メールの通知機能を正しく作動させるには、mailMail セッションの[Mail Transport Host]フィールドで電子メールを送信するときに、WebSphere が接続するサーバを指定します。

mailMail セッションは、WebSphere 管理コンソールの[リソース]、[Mail Providers]、「Built-in Mail Provider]、[Mail Sessions]、[mailMail]にあります。

注: mailMail オブジェクトを参照するには、[Mail Session]画面で[スコープ]を[サーバ]へ変更します。 スコープを[サーバ]へ変更しないと、mailMail オブジェクトは表示されません。

WebSphere メール プロバイダを設定する詳細については、WebSphere のマニュアルを参照してください。

電子メール通知の有効化

Identity Manager 環境に対して、電子メール通知を有効にしたり、無効にしたりできます。電子メール通知を有効にすると、CA Identity Manager は、指定したイベントおよびタスクに対して電子メール通知を送信します。

注: 忘れたパスワードの機能を使用するには、電子メール通知を有効にします。¥

CA Identity Manager で電子メール通知を有効にする前に、アプリケーション サーバに対して SMTP を設定(421 ページ)してください。

電子メール通知を有効にする方法

1. 管理コンソールで、[環境]をクリックします。

   Identity Manager 環境の一覧が表示されます。
2. 該当する Identity Manager 環境をクリックします。
3. [詳細設定]-[電子メール]の順に進みます。
4. [有効]チェックボックスをオンにします。
5. 電子メールをトリガするイベントおよびタスクを設定します(425 ページ)。
6. [保存]をクリックします。
7. CA Identity Manager がインストールされているアプリケーション サーバのインスタンスを再起動します。

電子メールを送信するためのイベントまたはタスクの設定

電子メールの通知が有効になっていると、電子メール通知をトリガするイベントまたはタスクのリストを指定することができます。 たとえば、以下の場合に電子メールを送信したいとします。

- ［ユーザ パスワードのリセット］タスクの完了時にシステム管理者に対して送信する場合。
- ［ユーザの作成]タスクの完了時に、新しい従業員のマネージャに対して送信する場合。 また、［ユーザの作成]タスクで生成された AddToGroupEvent が承認された場合に、新しいユーザが追加されるグループのすべてのメンバに対して、別の電子メールを送信することもできます。

電子メール通知をトリガするイベントおよびタスクを指定する方法

1. 管理コンソールで、［環境］をクリックします。

   Identity Manager 環境の一覧が表示されます。

2. 該当する Identity Manager 環境をクリックします。
3. ［詳細設定]-［電子メール]の順に進みます。

   ［Email Properties］画面が表示されます。

4. 以下の有効化のチェックボックスで、適切なものを選択します。
   - ［イベント電子メール有効化］

     Identity Manager のイベントに対する電子メール通知を有効化します
   - ［Tasks Email Enabled］

     Identity Manager のタスクに対する電子メール通知を有効化します
5. CA Identity Manager が電子メール メッセージの作成で使用する電子メール テンプレートの場所を指定します。

   電子メール テンプレートは、以下の場所のサブディレクトリに格納されています。

   IdentityMinder.ear¥custom¥emailTemplates

   注: 別の言語を使用しているファイル名の電子メール テンプレート ファイルを作成する場合は、オペレーティング システムのセッションで、文字セットをサポートしている言語を操作する必要があります。

6. 電子メールの通知を送信するイベントを、次のように指定します。
   - イベントを追加するには、[イベント]リスト ボックスでイベントを選択し、[追加]をクリックします。

     CA Identity Manager により、電子メール通知を送信するイベントのリストに対して、選択したイベントが追加されます。

     注: ワークフロー プロセスに関連付けられていないイベントを選択すると、CA Identity Manager は、イベントの完了時に電子メール通知を送信します。
   - イベントを削除するには、そのイベントのチェックボックスをオンにして[削除]をクリックします。
7. 電子メールの通知を送信するタスクを、次のように指定します。
   - タスクを追加するには、最初のフィールドで条件を選択してタスクを検索し、2 番目のフィールドにタスク名を入力します。 [検索]をクリックします。

     ワイルドカード(*)文字を使用して、タスク名の一部を入力することができます。 たとえば、作成のタスクを検索するには、「作成*」と入力します。

     検索結果から、1 つ以上のタスクを選択します。 [追加]をクリックします。

     注: アクション タイプが[表示]または[自己表示]のタスクでは、タスクレベルの電子メール通知は使用できません。 タスクのアクション タイプを参照するには、[管理タスクの変更]-[Select a Task]を選択し、タスク プロファイルのアクション フィールドを確認します。
   - タスクを削除するには、そのタスクのチェックボックスをオンにして[削除]をクリックします。

     タスクを削除すると、タスク テーブルからタスクが削除されます。 この処理で、タスクが削除されるわけではありません。
8. 電子メール通知をトリガするタスクおよびイベントの設定が終わったら、[保存]をクリックします。
9. CA Identity Manager がインストールされているアプリケーション サーバを再起動します。

電子メールのコンテンツ

電子メールの通知は、汎用的なテンプレート、および電子メール API によって電子メールに追加された、タスク特有の詳細によって構成されています。 たとえば、[ユーザの作成]タスクの場合は、電子メールに次の情報を挿入することができます。

- タスクを実行する管理者の名前
- 新しいユーザの名前
- ユーザの電子メール アドレス、部門名、およびその他の属性データ

- ユーザが作成された組織
- ワークフローの承認ステータスおよび承認時間
- タスク名、およびそのタスクのイベント名

電子メール テンプレート

電子メール通知は、電子メール テンプレートから生成されます。 CA Identity Manager にはデフォルトの電子メール テンプレートが用意されています。これらのテンプレートは、インストールされた状態のまま使用したり、テンプレートを使用して独自の電子メール テンプレートを作成したりできます。

各電子メール テンプレートには、次の情報が含まれています。

- 配信情報: 電子メールの受信者リスト。 CA Identity Manager は、このタスクに含まれているユーザに基づいて、受信者のリストを自動的に生成します。 たとえば、承認の電子メールは、このタスクに対するすべての承認者へ送信されます。
- 件名: メッセージの件名の行で使用されているテキスト。
- 内容: メッセージの本文。 メッセージには通常、静的なテキストと変数の両方が含まれています。CA Identity Manager は、電子メールをトリガするタスクまたはイベントに基づいてこれらのものを解決します。

デフォルトの電子メール テンプレートは、Identity Manager の管理ツールがインストールされている、emailTemplates ディレクトリに格納されています。 管理ツールのデフォルトのインストール場所は次のとおりです。

- Windows の場合: C:\Program Files\CA\IAM Suite\Identity Manager\tools\emailtemplates
- UNIX の場合: <home_directory>/CA/IAM Suite/Identity Manager/tools/emailtemplates

emailTemplates ディレクトリには、次の 4 つのフォルダが含まれています。 各フォルダは、1 つのタスクまたはイベントのステートに関連付けられています。

ディレクトリ	内容
Approved	defaultEvent.tmpl: イベントが承認されたことを受信者に知らせます。

ディレクトリ	内容
Completed	■ CertificationNonCertifiedActionCompletedNotification.tmpl：非準拠のアクションが従業員に適用されたことを、マネージャに知らせます。 ■ CertificationNonCertifiedActionPendingNotification.tmpl：非準拠のアクションが従業員に適用されそうであることを、マネージャに知らせます。 ■ CertificationRequiredFinalNotification.tmpl：ある従業員に対して[ユーザの認証]タスクを完了しなければならないことをマネージャに知らせる最終確認。 ■ CertificationRequiredNotification.tmpl：ある従業員に対して認証プロセスが開始されたことをマネージャに知らせます。 マネージャは、この従業員に対して、[ユーザの認証]タスクを完了する必要があります。 ■ CertificationRequiredReminderNotification.tmpl：ある従業員に対して[ユーザの認証]タスクを完了しなければならないことを、マネージャに指摘します。 ■ Certify Employee.tmpl：ある従業員に対する認証プロセスが完了したことを管理者に知らせます。 ■ CreateProvisioningUserNotificationEvent.tmpl：プロビジョニング ディレクトリでユーザのアカウントが作成されたときに、そのユーザに一時的なパスワードを送信します。 ■ defaultTask.tmpl：Identity Manager がタスクを完了したことを受信者に知らせます。 ■ ForgottenPassword.tmpl：忘れたパスワードの機能を使用したユーザに対して、一時的なパスワードを送信します。 ■ ForgottenUserID.tmpl：忘れたユーザ ID の機能を使用したユーザに対して、ユーザ ID を送信します。 ■ Self Registration.tmpl：自己登録タスクが正常に完了したことをユーザに通知します。
Invalid	■ AssignProvisioningRoleEvent.tmpl：ユーザをプロビジョニング ロールへ追加する要求が失敗したことを受信者に知らせます。 ■ DefaultEvent.tmpl：イベントが失敗したことを受信者に知らせます。 ■ DefaultTask.tmpl：Identity Manager のタスクが失敗したことを受信者に知らせます。
Pending	■ defaultEvent.tmpl：ワーク リスト アイテムで注意が必要であることを承認者に知らせます。 ■ ModifyUserEvent.tmpl：デフォルトのテンプレートと同じですが、ユーザ管理オブジェクトの属性を取得するためのメソッドが含まれています。
Rejected	defaultEvent.tmpl：イベントが拒否されたことを受信者に知らせます。

電子メールのカスタム テンプレートを作成するためのベースとして、<im_admin_tools_dir>¥Identity Manager¥tools¥emailTemplates ディレクトリにインストールされている、Identity Manager のテンプレートおよびテンプレート ディレクトリ構造を使用します。

テンプレート ディレクトリ

「電子メール テンプレート(427 ページ)」で説明されている、各テンプレート ディレクトリは、特定のタスクまたはイベントのステートに関連付けられています。 たとえば、ワークフロー プロセスで拒否されたイベントに対して電子メールを送信すると、Identity Manager は、配置されている拒否ディレクトリの中で、使用するテンプレートを検索します。 Identity Manager は、ディレクトリ内の適切な電子メール テンプレートから電子メールを生成します。

ディレクトリ内の電子メール テンプレート

配置されている各テンプレート ディレクトリには、1 つ以上の電子メール テンプレートが含まれています。 電子メールが有効になっているタスクまたはイベントが発生すると、Identity Manager は、該当するテンプレート ディレクトリで、タスクまたはイベントの名前と同じテンプレート名を検索します。 このようなテンプレートが見つからない場合、Identity Manager はディレクトリ内のデフォルトのテンプレートを使用します。 デフォルトのテンプレート名は「電子メール テンプレート(427 ページ)」に記載されています。 たとえば、Identity Manager は Pending ディレクトリ内の defaultEvent.tmpl を使用して、新しいワーク リスト リストがあることを承認者に知らせます。

テンプレート ディレクトリのセット

テンプレート ディレクトリのセットには、承認済みディレクトリ、完了済みディレクトリ、保留中ディレクトリ、および拒否されたディレクトリが含まれています。 複数のテンプレート ディレクトリのセットを配置して、特定の Identity Manager 環境に対して使用する 1 つのセットを指定することができます。

「電子メール テンプレートの配置(448 ページ)」には、テンプレート ディレクトリのセットを配置するための情報が記載されています。

電子メール テンプレート ディレクトリを設定し、Identity Manager で特定の環境に対して正しいセットを使用できるようにするための詳細については、「CA Identity Manager Configuration Guide」を参照してください。

電子メール テンプレートの作成

電子メールのカスタム メッセージの作成方法

1. 修正するテンプレートを開きます。

   たとえば、保留中の「ユーザの作成」イベントに対して電子メール メッセージを作成したい場合は、Pending ディレクトリの defaultEvent.tmpl を開きます。

2. このテンプレートに別の名前を付けて、同じディレクトリに保存します。 テンプレート名は、電子メールを適用するイベント名と一致していること、および拡張子 .tmpl を持っていることが必要です。

   たとえば、保留中の「ユーザの作成」イベントに対するメッセージには、次のように名前を付けます。

   CreateUserEvent.tmpl

   イベントの一覧については、Identity Manager のイベントを参照してください。

   注: 別の言語を使用しているファイル名の電子メール テンプレート ファイルを作成する場合は、オペレーティング システムのセッションで、文字セットをサポートしている言語を操作する必要があります。

3. 次のセクションの「電子メールのカスタム テンプレート(430 ページ)」に記載されているように、必要に応じてメッセージ テンプレートを修正します。

電子メールのカスタム テンプレート

電子メール テンプレートは、HTML および埋め込み型サーバ サイド JavaScript の両方をサポートするダイナミック ファイルです。 テンプレートによって静的テキストに変数値を挿入することができるため、単一のテンプレートによる大文字と小文字を区別したメッセージの生成が可能になります。

同じテンプレートを何度も使用して、定型的な静的テキスト(承認されているフレーズなど)と、所定のコンテキストに特有の可変的なテキスト(承認中のイベント名など)を合わせて印刷することができます。

たとえば、イベントの承認をレポートするテンプレートは次のようになります。

```
<!-- Define the E-mail Properties --->
<%
_to = _util.getNotifiers("ADMIN");
_cc = "";
_bcc = "";
_subject = _eventContextInformation.getEventName() + " approved";
%>
<!--- Start of Body --->
<html>
<body text="Navy">
```

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
Status: <b>Approved</b>
</body>
</html>
```

注: 上記の例で使用されている、Identity Manager のオブジェクトの _util および _eventContextInformation については、「電子メール テンプレート API」で説明しています。

イベント CreateUserEvent に対して承認が生成され、HR の組織で John Jones というユーザが作成された場合、この承認テンプレートから生成される電子メール通知は次のようになります。

Event: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Approved

以降のセクションでは、動的な電子メール メッセージを可能にする構文および Identity Manager のオブジェクトについて説明します。

テンプレートのエレメント

Identity Manager の電子メール テンプレートは以下のものをサポートしています。

- 標準の HTML タグ
- サーバーサイド JavaScript
- 1 つ以上の暗黙的なオブジェクト(Identity Manager がテンプレートの 1 つのインスタンス、つまり電子メール メッセージを利用できるようにするもの)
- Identity Manager のタグ。このタグを使用して JavaScript をテンプレートに埋め込む、Identity Manager の暗黙的なオブジェクトでメソッドをコールする、変数値をテンプレートの静的テキストに挿入する、といったことが可能になる

Identity Manager タグの拡張

電子メール テンプレートは以下のタグをサポートしています。

<% %>

電子メール テンプレートに JavaScript を埋め込みます。

<%= %>

静的なテキストに可変的な値を挿入します。

以降のセクションでこれらのタグについて説明します。

<% %>

このタグを使用して、インライン実行のための JavaScript を電子メール テンプレートに埋め込むことができます。

埋め込まれた JavaScript では、任意の JavaScript オブジェクトを使用できます。 埋め込まれた JavaScript では、Identity Manager の暗黙的なオブジェクト メソッドをコールすることもできます。

たとえば、次のコードは、「電子メールのカスタム テンプレート(430 ページ)」で示した承認テンプレートの本文を変更します。 ここでは JavaScript を使用して、セカンダリ オブジェクトがイベントに含まれているかどうかを決定します(USER プライマリ オブジェクトが追加された場合の ORGANIZATION オブジェクトなど)。 セカンダリ オブジェクトがない場合は、セカンダリ オブジェクトに関連するテキストがメッセージから削除されます。

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
template.add("In " + secondaryType + ":");
template.add("<b> "+_eventContextInformation.getSecondary
ObjectName()+" </b><br>");
}
%>
Status: <b>Approved</b>
```

<%= %>

このタグを使用して、可変的な値を静的なテキストに挿入することができます。 値として、次のものを使用できます。

- テンプレート内で以前に実行された JavaScript で定義されている変数。例:

```
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
..// More JavaScript processing
%>
..// More HTML
The primary object was created in <%=secondaryType%>.
```

- Identity Manager の暗黙的なオブジェクトにおいてメソッドから返された値。例:

```
Event <%=_eventContextInformation.getEventName()%> is approved.
```

電子メール テンプレート API

テンプレートからメッセージが生成されると、Identity Manager は、以下の暗黙的なオブジェクトをメッセージで使用できるようにします。 これらのオブジェクトを使用すると、電子メール テンプレート API でメソッドをコールすることによって、インスタンス特有の情報をメッセージに挿入できます。

テンプレートは、次のいずれかのオブジェクトでメソッドをコールできます。

- _contentType: 電子メールの contentType を指定します。
- _priority: 電子メールの優先度を指定します。
- _to: メッセージの[To]フィールドに受信者を追加します。
- _cc: メッセージの[CC](コピーを送信)フィールドに受信者を追加します。
- _bcc: メッセージの[BCC](ブラインド コピーへ送信)フィールドへ受信者を追加します。
- _subject: 電子メールの件名を指定します。
- _encoding: 電子メールの円コーディングを指定します。
- template: JavaScript コードの行からメッセージへテキスト文字列を追加できるようにします。
- _util: ユーティリティ オブジェクト。

- _eventContextInformation: 現行のタスクで生成されたイベントに関する情報(イベント名、承認ステータスなど)が含まれます。
- _taskContextInformation: 現行のタスクに関する情報のコレクション(タスク名、組織名、構成イベントなど)が含まれます。

以降のセクションで、これらのオブジェクトについて説明します。

_contentType

電子メールの contentType を指定します。

contentType が specified through _contentType 変数の場合、デフォルトの contentType である「text/html」が適用されます。

メソッド: なし。

例:

```
<% _contentType = "text/html"; %>
```

_priority

電子メールの優先度を指定します。 優先度なし(デフォルト)には 0、高優先度には 1 を指定します。

メソッド: なし。

例:

```
<% _priority = "1"; %>
```

_to

メッセージの[To]フィールドに受信者を追加します。

_to variable の値は JavaScript 文字列です。 複数の受信者が許可されていますが、以下の例のに示されるように文字列は JavaScript 構文に準拠する必要があります。

メソッド: なし。

例:

```
<%
_to =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER""ManagerLookup=managerattribute");
_cc = "";
_bcc = "";
_subject = "Your new password ";
%>
```

注: 電子メールが参加者にワークフロー コントロールに保留状態のタスクがあることを警告する場合、_to オブジェクトに受信者のアドレスが事前入力されます。 Pending テンプレートに _to オブジェクトを使用することはできません。

_cc

メッセージの[cc](コピーを送信)フィールドに受信者を追加します。

_to variable の値は JavaScript 文字列です。 複数の受信者が許可されていますが、以下の例のに示されるように文字列は JavaScript 構文に準拠する必要があります。

メソッド: なし。

例:

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER""ManagerLookup=managerattribute");
%>
```

_bcc

メッセージの[bcc](ブラインド コピーを送信)フィールドに受信者を追加します。

このフィールドで指定された電子メール アドレスは、電子メールには表示されません。

_to variable の値は JavaScript 文字列です。 複数の受信者が許可されていますが、以下の例のに示されるように文字列は JavaScript 構文に準拠する必要があります。

メソッド: なし。

例:

```
<%
_bcc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER"",""ManagerLookup=managerattribute");
%>
```

_subject

電子メールの件名を指定します。

メソッド: なし。

例:

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

_encoding

電子メールのエンコーディングを指定します。

エンコーディングが _encoding または LANG 変数のどちらかで指定されている場合、電子メールの文字が正しく表示されない可能性があります。 必ず set _encoding または LANG を設定し、適切なローケルを設定してください。

メソッド: なし。

例:

```
<% _encoding = "UTF-8"; %>
```

template

JavaScript コードの行（<% %> タグ内の行）からメッセージにテキストの文字列を追加できます。 文字列には HTML タグ、静的テキスト、および Identity Manager の implicit オブジェクトでメソッドにより返される変数値を含めることができます。

注: template オブジェクトは最初に下線 (_) 文字はつきません。

メソッド:

- add(String)

  引数は、Identity Manager の implicit オブジェクトのメソッドに対するすべてのコールも含めて、文字列に数値を求める必要があります。 以下の例にある _eventContextInformation.getSecondaryObjectName() を参照してください。

例:

```
<%
var secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
template.add("In " + secondaryType + ":");
template.add("<b> "+_eventContextInformation.getSecondary
ObjectName()+" </b><br>");
}
%>
```

_util

ユーティリティ オブジェクト。

メソッド:

- getNotifiers(String [,String])

  通知ルールに基づいて電子メール ID を返します。

  最初の引数は、以下の引用符で囲まれた定義済み通知ルールをサポートします。

  - "ADMIN"。 タスクを開始した管理者に電子メールを送信します。
  - "USER"。 現在のコンテキストのユーザに電子メールを送信します。
  - "USER_MANAGER"。 現在のコンテキストのユーザの管理者に電子メールを送信します。

  theNotification Rule API で作成するカスタム通知ルールを参照することもできます。詳細については、「Java のプログラミング ガイド」を参照してください。

  秒の引数はオプションです。 引数を使用して、ユーザ定義された名前/値の 1 つ以上のペアをカスタム通知ルールに渡すことができます。 名前/値のペアは、以下の形式でコンマ区切りとします。

  "name1=value1,name2=value2,..."

例:

```
<%
_to = _util.getNotifiers("ADMIN");
_cc = "";
%>
<%
_to = _util.getNotifiers("MYRULE","type=loan,district=3");
_cc = "";
%>
```

ユーザのマネージャへの通知

USER_MANAGER 通知ルールを使用して、ユーザのマネージャに電子メールを送信できます。 Identity Manager はこのルールを電子メール テンプレートで使用し、ユーザ資格認証をサポートします。

注: The USER_MANAGER 通知ルールは、単一のユーザを作成または管理するイベントまたはタスクにのみ適用されます。

ユーザからマネージャへの関係をユーザ ディレクトリ内で指定する方法が数多くあるため、デフォルトのユーザ マネージャ通知アダプタは、getNotifiers() メソッドの第 2 パラメータ内で指定された属性式に基づいてこの関係を解決します。

例:

```
<%
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "";
%>
```

ユーザ マネージャ通知アダプタは、2 つの検索オプションをサポートしています。

- managerattribute = <Manager AttributeName>- User オブジェクトがユーザのマネージャの DN またはユーザ ID を示す属性を維持する場合
- commonattribute = <AttributeName> - ユーザおよびユーザのマネージャが「部署」などの共通属性値を共有する場合

これらの検索オプションは、Identity Manager の管理コンソール内にある環境の[その他]属性で設定します。

USER_MANAGER 通知ルールを設定する方法

1. Identity Manager 管理コンソールで、Identity Manager 環境を選択します。 次に、電子メール通知を設定する環境を選択します。
2. [詳細設定]-[Miscellaneous Properties]を選択します。

3. ［Miscellaneous Properties］ページで、使用する検索オプション用の設定手順を完了させます。

   - managerattribute=<Manager AttributeName> 検索オプションを使用する方法
     a. ［プロパティ］フィールドに managerattribute を入力します。
     b. ［値］フィールドでマネージャの DN または ユーザ ID を格納する属性を入力します。
     c. ［追加］をクリックします。
     d. ［保存］をクリックします。
   - commonattribute=<AttributeName> 検索オプションを使用する方法
     a. ［プロパティ］フィールドに commonattribute を入力します。
     b. ［値］フィールドでユーザおよびユーザのマネージャが共有する属性を入力します。
     c. ［追加］をクリックします。
     d. ［プロパティ］フィールドに ismanagerfilter を入力します。
     e. ［値］フィールドで以下の構文を使用した検索式を入力します。

        <attribute> <operator> <filter>

        たとえば、役職 EQUALS マネージャ
     f. ［追加］をクリックします。
     g. ［保存］をクリックします。

カスタム アダプタを記述して、ユーザのマネージャへの通知に関する独自のルールを作成することもできます。「Java のプログラミング ガイド」を参照してください。

_eventContextInformation

イベント名や承認ステータスなど、現在のタスクにより生成されたイベントに関する情報を含みます。 この情報は、イベントのコンテキスト情報と呼ばれます。

_eventContextInformation オブジェクトは、パッケージ com.netegrity.imapi の ExposedEventContextInformation クラスから作成されます。

このオブジェクトは Approved、Pending、および Rejected テンプレートに基づく電子メール メッセージに利用できます。 これらのテンプレートの詳細については、「電子メール テンプレート(427 ページ)」を参照してください。

メソッド: 以下の全てのメソッドは文字列を返します。

メソッド	説明
getAdminName()	イベントを生成したタスクをサブミットした人の名前を返します。 Identity Manager 5.6 では使用されません。 以下のいずれかのメソッドを使用します。 ■ getAdministrator() ■ getAdminFriendlyName()
getApprovalStatus()	イベントの承認ステータスを返します。 次のいずれかの値を取ります。 APPROVAL_STATUS_APPROVED APPROVAL_STATUS_REJECTED
getApprovalTime()	イベントが承認された時間を返します。
getEventName()	イベントの名前を返します。 イベント名の一覧は、Identity Manager のイベントを参照してください。
getOrgName()	タスクが実行されている組織のわかりやすい名前を返します。 Identity Manager 5.6 では使用されません。 継承されたメソッド getObjectOrganizationFriendlyName() を使用します。
getPassword()	プライマリ オブジェクトがタイプ USER の場合、ユーザのパスワードを返します。
getPrimaryObjectTypeName()	プライマリ オブジェクトのタイプを返します。 返されるプライマリ オブジェクト: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER

メソッド	説明
getPrimaryObjectName()	イベントに影響されるプライマリ オブジェクトの名前を返します。 プライマリ オブジェクトは、イベントから直接影響を受けるオブジェクトです。 セカンダリ オブジェクトは、プライマリ オブジェクトに関連があるオブジェクトです。 以下に例を示します。 ■ CreateUserEvent のプライマリ オブジェクト タイプは USER です。 セカンダリ オブジェクトはユーザが作成されるオブジェクト、すなわち ORGANIZATION です。 ■ CreateAdminRoleEvent のプライマリ オブジェクト タイプは ADMINROLE です。 このオブジェクトは他のオブジェクトと関連しないため、セカンダリ オブジェクトは存在しません。 タイプ USER のプライマリ オブジェクトでは、getPrimaryObjectName() は John Jones を返す場合があります。
getSecondaryObjectTypeName()	セカンダリ オブジェクトがイベントの影響を受けた場合、オブジェクト タイプを返します。 返されるセカンダリ オブジェクト タイプ: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getSecondaryObjectName()	セカンダリ オブジェクトがイベントの影響を受けた場合、オブジェクト名を返します。 プライマリおよびセカンダリ オブジェクトの情報については、getPrimaryObjectName() を参照してください。 タイプ ORGANIZATION のセカンダリ オブジェクトでは、getSecondaryObjectName() は HR を返す場合があります。

注: methods in _eventContextInformation は、インターフェース ExposedEventContextInformation から提供されます。 ExposedEventContextInformation はコア Identity Manager API にメソッドを継承するため、_eventContextInformation はこれらのメソッドを上記の表にあるメソッドのみならず電子メール テンプレートからもコールできます。 これらの継承されたメソッドの詳細については、「追加のメソッド (445 ページ)」を参照してください。

例--[Pending]イベントに関する電子メール通知:

```
<%
_cc = "" ;
_bcc = "";
_subject = _eventContextInformation.getEventName() +
"  承認リクエスト";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

以下のアイテムがワーク リストに追加され、承認待ちです:
<br><br><br>
イベント: <b><%=_eventContextInformation.getEventName()%></b> <br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
所属 <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
</body>
</html>
```

電子メールの本文はこのようになります:

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent 承認リクエスト

以下のアイテムがワーク リストに追加され、承認待ちです:

イベント: CreateUserEvent
USER: Richard Ferrigamo
所属 ORGANIZATION: Mortgages & Loans

注: [From]フィールドの値は、email.properties ファイルから派生します。 値を変更するには、以下のファイルを編集します。
<IdentityMinder.ear>\config\com\netegrity\config\email.properties

<IdentityMinder.ear> はアプリケーション サーバ ドメイン内の Identity Manager がインストールされた場所です。以下に例を示します。

WebLogic の場合:
<WebLogic_home>\user_projects\<domain>\applications\IdentityMinder.ear

JBoss の場合:
<Identity Manager_home>\jboss-3.2.2\server\default\deploy\IdentityMinder.ear

WebSphere の場合:
< im_admin_tools_dir >\WebSphere-ear\IdentityMinder.ear

イベントにより影響されたユーザに関する追加情報を前述の例にある電子メールに追加するには、以下のようなテキストを追加します。

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>ユーザ情報:</b><br>
ラスト ネーム: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
ファースト ネーム: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
フル ネーム: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
電子メール: <b><%=user.getAttribute("%EMAIL%")%></b><br>
組織メンバシップ: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

電子メールの本文はこのようになります:
From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent 承認リクエスト

以下のアイテムがワーク リストに追加され、承認待ちです:

イベント: CreateUserEvent
USER: Richard Ferrigamo
所属 ORGANIZATION: Mortgages & Loans
ユーザ情報:
ラスト ネーム: Ferrigamo
ファースト ネーム: Richard
フル ネーム: Richard Ferrigamo
電子メール: rferrigamo@mybank.org
組織メンバシップ: Mortgages & Loans

_taskContextInformation

タスク名、組織名、および構成イベントなどの現在のタスクに関する情報を含みます。 この情報は、タスクのコンテキスト情報と呼ばれます。

このオブジェクトは、および Completed テンプレートに基づく電子メール メッセージに利用できます。 このテンプレートの詳細については、「電子メール テンプレート(427 ページ)」を参照してください。

メソッド: 以下の全てのメソッドは、Java Vector を返すメソッド getExposedEventContexts() を除いて、文字列を返します。

メソッド	説明
getAdminName()	タスクをサブミットしている人の名前を返します。 Identity Manager 5.6 では使用されません。 以下のいずれかのメソッドを使用します。 ■ getAdministrator() ■ getAdminFriendlyName()
getExposedEventContexts()	タスクに関連付けられているすべてのイベントの Java Vector を返します。 Vector 内の各イベントは、イベント コンテキスト オブジェクトです。 _eventContextInformation にリストされているメソッドを使用して、任意のイベント オブジェクト用にコンテキスト情報を取得できます。 return オブジェクトは標準の Java Vector オブジェクトです。 Vector のエレメント管理には、たとえば Vector の get() および size() など、Vector オブジェクトのメソッドをどれでも使用できます。
getOrgName()	タスクが実行されている組織の名前を返します。 Identity Manager 5.6 では使用されません。 継承されたメソッド getObjectOrganizationFriendlyName() を使用します。
getTaskName()	実行されているタスクの名前を返します。 Identity Manager 5.6 では使用されません。 以下のいずれかのメソッドを使用します。 ■ getAdminTask() ■ getTaskFriendlyName()

注: methods in _taskContextInformation は、インターフェース ExposedTaskContextInformation から提供されます。 ExposedTaskContextInformation はコア Identity Manager API にメソッドを継承するため、_taskContextInformation はこれらのメソッドを上記の表にあるメソッドのみならず電子メール テンプレートからもコールできます。 これらの継承されたメソッドの詳細については、「追加のメソッド (445 ページ)」を参照してください。

例--パスワード変更用の電子メール 通知テンプレートの本文:

```
<%
var imsEventContexts = _taskContextInformation.getExposedEventContexts();
if(imsEventContexts != null)
{
for(var i=0;i<imsEventContexts.size();i++)
{
var eventContext = imsEventContexts.get(i);
template.add("Hi "+ eventContext.getPrimaryObjectName() +",");
template.add("<br>新しいパスワード: <b>"+
eventContext.getPassword());</br>
template.add("<hr>");
}
}
%>
```

電子メールの本文はこのようになります:

Hi Victor Imperioso,
新しいパスワード: LFH7F1226

追加のメソッド

_taskContextInformation および _eventContextInformation のメソッドは、それぞれ Identity Manager オブジェクトの ExposedTaskContextInformation と ExposedEventContextInformation を使用して提供されます。

これらのオブジェクトは、コア Identity Manager API にメソッドを継承します。 その結果、_taskContextInformation および _eventContextInformation も継承されたメソッドを使用できます。

TaskInfo オブジェクトから継承された以下のメソッドは、特に電子メール テンプレートに役立ちます。

- getAdministrator(). 現在のタスクを実行している管理者の User オブジェクトを取得します。
- getAdminTask(). 現在のタスクの AdminTask オブジェクトを取得します。

これらの取得されたオブジェクトにより、管理者固有およびタスク固有の情報を電子メールに挿入できます。 以下に例を示します。

```
<!-- Define the E-mail Properties --->

<%
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +
"  承認リクエスト";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

以下のアイテムがワーク リストに追加され、承認待ちです:<br>
<br>
User <b><%= _eventContextInformation.getAdministrator().
getAttribute(Packages.com.netegrity.llsdk6.imsapi.
managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
from department <b><%= _eventContextInformation.
getAdministrator().getOrg(null).getFriendlyName()
%></b> initiated task <b><%= _eventContextInformation.
getAdminTask().getFriendlyName() %></b>at <b><%= _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
<font color="green">詳細: </font><b><%=_eventContextInformation.
getEventName()%></b><br>
<font color="green"><%=_eventContextInformation.
getPrimaryObjectTypeName()%>:</font>
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>
が変更されました
<br>
<font color="green">更新された属性:</font>
<table border="1">
<tr>
[assign the value for TD in your book]<b>名前</b></td>
[assign the value for TD in your book]<b>値</b></td>
</tr>
```

```
<%
var event = _eventContextInformation.getEvent();
if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
var user = event.getUser();
var attributes = user.getAttributes().keys();
while(attributes.hasMoreElements()) {
var attr = attributes.nextElement();
var value = user.getAttribute(attr);
if(user.hasAttributeChanged(attr)) {
template.add("<tr>[assign the value for TD in your book]" + attr +"</td>");
template.add("[assign the value for TD in your book]" + value +"</td></tr>");
}
}
}
%>
</table>
<br>
</body>
</html>
```

電子メールの本文はこのようになります:

Email Template API で利用可能な継承されたメソッドの詳細については、「Identity Manager Javadoc」のオブジェクト ExposedTaskContextInformation および ExposedEventContextInformation を参照してください。

Java 標準出力ストリーム

電子メール メッセージは、JavaScript タグ (<%%>) から Java 標準出力ストリームにコールすることも可能です。 たとえば、以下のコールはメッセージ「Done」をサーバ コンソールに送信します。

```
<%
...// JavaScript processing
out.println("Done.");
%>
```

Javadoc リファレンス

コア Identity Manager API から継承するメソッドを含む ExposedTaskContextInformation および ExposedEventContextInformation オブジェクトの詳細については、「Identity Manager Javadoc」を参照してください。

Javadoc のページは、Identity Manager Bookshelf で利用可能な「Java のプログラミング ガイド」の HTML バージョンと統合されています。

電子メール テンプレートの展開

Identity Manager は電子メールの送信前に、アプリケーション サーバ内の以下のルート ロケーションのうち電子メールを生成するテンプレートを検索します。

<IdentityMinder.ear>\custom\emailTemplates

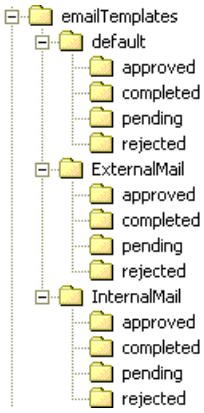
このルートに展開された電子メール テンプレートは同じディレクトリ構造を持つテンプレート セットに含まれ、承認済み、完了、保留、および拒否ディレクトリが各セットに存在します。

テンプレート セット

emailTemplates で、電子メール テンプレートの複数のセットを展開できます。 たとえば、インストール中に、以下の電子メール テンプレートのセットが IdentityMinder.ear¥custom¥emailTemplates の下に作成されます。

default\approved
default\completed
default\pending
default\rejected

デフォルトの電子メール テンプレートのセットには、電子メール テンプレート(427 ページ)で説明されているインストール済みのテンプレートが含まれます。 デフォルトのセット内にカスタム テンプレートを追加できます。 電子メール テンプレートの他のセットを、デフォルトのセットと同じレベルで定義したディレクトリ構造で展開することもできます。 たとえば、IdentityMinder.ear¥custom に以下の展開された電子メール テンプレートを含めることもできます。



Identity Manager がどのようにテンプレート セット内の特定の電子メール テンプレートを選択するかの詳細については、「テンプレートのディレクトリ(429 ページ)」を参照してください。

環境用のテンプレート セットを指定する方法

Identity Manager 環境用に電子メールを設定する場合、この環境に使用する電子メール テンプレートを指定します。 Identity Manager 環境用の電子メールの設定の詳細については、「CA Identity Manager Configuration Guide」を参照してください。

テンプレート名

カスタム テンプレート セット内のディレクトリには、デフォルト テンプレート セットにインストールされたものと同じ名前を持つデフォルト テンプレートが含まれる必要があります。 デフォルト名は「Email Templates(427 ページ)」に記載されています。 Identity Manager は、実行中のタスクまたはイベントと一致する名前を持つ他のテンプレートを検出できない場合、デフォルトのテンプレートを使用します。

必要に応じて、特定のテンプレートから電子メールを生成させたい場合、追加テンプレートを 1 つ以上のテンプレート セット内のディレクトリに追加できます。 以下の手順に従ってください。

- 電子メールが作成されるタスクまたはイベントと同じ名前を、テンプレートに割り当てます。
- 電子メールが作成されるタスクまたはイベントに関連付けられたディレクトリに、テンプレートを配置します。

たとえば、CreateUserEvent が拒否されたときに特定のテンプレートから電子メールを生成させたい場合、CreateUserEvent.tmpl という名前のテンプレートを環境のテンプレートセットの［rejected］ディレクトリ内に置きます。

第 19 章: アクセス ロール

このセクションには、以下のトピックが含まれています。

CA Identity Manager のアクセスロール (451 ページ)
アクセス ロールの作成 (453 ページ)

CA Identity Manager のアクセスロール

アクセス ロールを使用すると、CA Identity Manager または他のアプリケーションの権限を付与することができます。 たとえば、アクセス ロールを使用して以下の処理を実行できます。

- ユーザ属性に間接的なアクセス権を付与する
- 複合式を作成する
- 権限を決定するために他のアプリケーションで使用される、ユーザ プロファイルの属性を設定する

アクセス ロールは、ユーザまたはユーザのグループに一連のビジネス変化を適用するという点でアイデンティティ ポリシーに似ています。 ただし、アクセス ロールを使用してビジネス変化を適用すると、アクセス ロールのメンバを表示して、この変化の適用先のユーザを確認できます。

アクセス ロールはタスクに関連付けられません。

アクセスロールが権限を管理する方法

変化アクションを指定することで、アクセス ロールを使用して権限を管理できます。このアクションは、ユーザーがロールのメンバまたは管理者として追加または削除されたときに発生します。

アクセス ロールを使用する方法

1. 管理者がアクセス ロールを作成します。
2. [メンバ]タブで、管理者は追加または削除アクションを指定します。これにより、ユーザにアクセス ロールが割り当てられるときに CA Identity Manager によって実行されるアクションが決定されます。
3. 管理者は必要に応じて管理者ポリシーと所有者ポリシーを指定し、アクセス ロールを作成するタスクを送信します。

4. アクセス ロールの管理者がユーザにアクセス ロールを割り当てます。
5. CA Identity Manager が、ロールで指定されたアクション追加を完了します。

例: 間接的なプロファイル属性の変更

アクセス ロールを使用して、ユーザ プロファイルの属性を間接的に変更できます。 たとえば、企業では自分以外のユーザの役職を直接変更できない場合があります。 こうした企業では、管理者がユーザにロールを割り当てたときに役職を変更できるアクセス ロールを作成できます。

属性を間接的に変更するには、アクセス ロールに変更アクションを設定します。 管理者がロールを割り当てると、この変更アクションにより、ユーザ プロファイルの属性に 1 つ以上の変更を加えることができます。

アクセス ロールを使用して属性を間接的に変更する方法

1. アクセス ロールを作成します。
2. [メンバ]タブで、[管理者はこのロールのメンバの追加、削除が可能]チェック ボックスをオンにして、矢印アイコンをクリックします。

   CA Identity Manager には、[追加アクション]および[アクションの削除]フィールドが表示されます。
3. [追加アクション]または[アクションの削除]フィールドで、リスト ボックスからアクションを選択します。

   Identity Manager には、選択したオプションに基づいた追加フィールドが表示されます。
4. 必要に応じて、[追加]または[削除]アクションを設定します。
5. [管理者]タブを選択して、作成中のアクセス ロールにメンバを追加できる管理者を指定します。
6. [所有者]タブを選択して、アクセス ロールの定義を変更できる管理者を指定します。
7. [送信]をクリックしてアクセス ロールの作成を完了します。
8. 必要に応じてユーザにアクセス ロールを割り当てます。

アクセス ロールの作成

アクセス ロールを作成するには、以下の手順に従います。

- アクセス ロールの作成の開始 (453 ページ)
- アクセス ロールのプロファイルの定義 (453 ページ)
- アクセス ロールのメンバ ポリシーの定義 (454 ページ)
- アクセス ロールの管理ポリシーの定義 (454 ページ)
- アクセス ロールの所有者ルールの定義 (455 ページ)

アクセス ロールの作成の開始

1. アクセス ロールの作成タスクが含まれているロールで Identity Manager アカウントにログインします。
2. [アクセス ロール]-[アクセス ロールの作成]をクリックします。

   オプションを選択して、新しいロールまたはロールのコピーを作成します。 [コピー]を選択した場合は、ロールを検索してください。
3. セクション「アクセス ロールのプロファイルの定義」に進んでください。

アクセス ロールのプロファイルの定義

アクセス ロールのプロファイルを定義する方法

1. 名前、説明を入力し、このロールのカスタム属性をすべて設定します。

   注: [プロファイル]タブに、アクセス ロールに関する追加情報を指定するカスタム属性を指定することができます。 この追加情報は、多数のロールを含む環境におけるロール検索を簡易化できます。
2. 作成後、すぐにこのロールを使用できるようにする場合は、[有効]を選択します。
3. 次のセクション「アクセス ロールのメンバ ポリシーの定義」(454 ページ)に進んでください。

詳細情報:

ロールのユーザ定義のカスタム属性 (50 ページ)

アクセス ロールのメンバ ポリシーの定義

[メンバ]タブで以下の手順を実行します。

1. [追加]を選択してメンバ ポリシーを定義します。
2. (オプション)[メンバ ポリシー]ページでは、このロールの使用を許可するメンバ ルールを定義できます。

   このルールにより、メンバ ポリシーの条件に一致するユーザにこのロールが自動的に割り当てられます。
3. [メンバ]タブにメンバ ポリシーが表示されていることを確認します。

   ポリシーを編集するには、左側にある矢印記号をクリックします。 ポリシーを削除するには、マイナス記号のアイコンをクリックします。
4. [メンバ]タブで、[管理者は、このロールのメンバを追加および削除できます]チェック ボックスをオンにします。

   この機能を有効にすると、[アクションの追加]および[アクションの削除]を定義できます。 これらのアクションでは、ロールのメンバとしてユーザが追加または削除されたときに行われる処理が定義されます。
5. 次のセクション「アクセス ロールの管理ポリシーの定義」(454 ページ)に進んでください。

アクセス ロールの管理ポリシーの定義

[管理者]タブで以下の手順を実行します。

1. [管理者の管理]オプションを使用する場合は、[管理者はこのロールのメンバの追加、削除が可能] チェック ボックスをオンにします。

   この機能を有効にすると、ロールの管理者としてユーザが追加または削除されたときのアクションを定義できます。
2. [管理者]タブで、管理ルールとスコープ ルール、管理者権限を含む管理ポリシーを追加します。 少なくとも 1 つの権限(メンバの管理または管理者の管理)に各ポリシーが必要です。

   このルールを満たす管理者用に個別のルールや権限を所有する複数の管理ポリシーを追加できます。
3. ポリシーを編集するには、左側にある矢印記号をクリックします。 ポリシーを削除するには、マイナス記号のアイコンをクリックします。
4. 次のセクション「アクセス ロールの所有者ポリシーの定義」(455 ページ)に進んでください。

アクセス ロールの所有者ルールの定義

［所有者］タブで以下の手順を実行します。

1. ロールを変更できるユーザを決定する、所有者ルールを定義します。
2. ［送信］をクリックします。

   タスクが送信されたことを示すメッセージが表示されます。 ユーザがロールを使用可能になるまでに一時的な遅延が発生する場合があります。

第 20 章: システム タスク

このセクションには、以下のトピックが含まれています。

デフォルトのシステム タスク (458 ページ)
Identity Manager のタスク ステータス (458 ページ)
Identity Manager がタスク ステータスを判別するしくみ (460 ページ)
[サブミット済みタスクの表示]タブ (461 ページ)
[ユーザ履歴]タブ (470 ページ)
Bulk Loader (476 ページ)
セレクト ボックス データ (482 ページ)
ロジカル アトリビュート ハンドラ (483 ページ)
JDBC 接続管理 (487 ページ)
サブミット済みタスクのクリーンアップ (487 ページ)
反復タスクの削除 (491 ページ)
Enterprise Log Manager 接続の設定 (492 ページ)
Enterprise Log Manager 接続の削除 (493 ページ)

デフォルトのシステム タスク

CA Identity Manager には、管理者が Identity Manager 環境を管理する際に役立つ以下のタスクが組み込まれています。

- ［サブミット済みタスクの表示］タスク

  管理者が使用環境内のタスクのステータスを表示できます。

- ［Bulk Loader］タスク

  フィーダ ファイルをアップロードします。このファイルは、多数の管理対象オブジェクトを同時に操作する際に使用します。

- ［セレクト ボックス データ］タスク

  管理者が、フィールドにオプションを設定するためのファイル（セレクト ボックスなど）を管理タスクにアップロードできます。

- ［ロジカル アトリビュート ハンドラ］タスク

  管理者がロジカル アトリビュートを管理できます。ロジカル アトリビュートは、タスク画面で属性（フィジカル アトリビュートと呼ばれる）をユーザにわかりやすい形式で表示する際に使用します。

- ［JDBC 接続管理］タスク

  CA Identity Manager でデータベース サーバ接続の詳細情報を設定します。

Identity Manager のタスク ステータス

CA Identity Manager タスクの処理用にサブミットした後で、管理者がそのタスクのステータスを追跡する必要が生じる場合があります。 CA Identity Manager でタスク ステータスを表示する方法を以下に示します。

- ［サブミット済みタスクの表示］タブ

  このタブでは、処理用にサブミット済みの CA Identity Manager タスクを検索および表示できます。

  管理者は、タスクの詳細を概要レベルで表示することも、さらに詳しいレベルで表示することもできます。

［サブミット済みタスクの表示］タブは、以下の 2 つのデフォルト タスクに組み込まれています。

- ［マイ サブミット済みタスクの表示］

  管理者は、処理用にサブミット済みのタスクに関する情報を検索および表示できます。

- ［サブミット済みタスクの表示］

  管理者は、他の管理者が処理用にサブミットしたタスクに関する情報を検索および表示できます。

- ［ユーザ履歴］タブ

  このタブは、［ユーザの表示］や［ユーザの変更］などのユーザ タスクに追加できます。管理者は、選択したユーザに関する以下の情報を表示できます。

  - ユーザに対して実行されるタスク
  - ユーザによって実行されるタスク
  - ユーザが承認したワークフロー

- レポート

  CA Identity Manager レポートでは、Identity Manager 環境の現在の状態を確認できます。 この情報を使って、内部のビジネス ポリシーや外部規制とのコンプライアンスを確保できます。

  レポート機能を使用すると、レポートの設定と使用に関する追加情報を確認できます。

- ログ

  CA Identity Manager のインストールに含まれるすべてのコンポーネントに関する情報、および CA Identity Manager のすべての操作に関する詳細情報が表示されます。

  CA Identity Manager のログの詳細については、「Configuration Guide」を参照してください。

Identity Manager がタスク ステータスを判別するしくみ

タスクとは、CA Identity Manager でユーザが実行できる管理機能を言います。 タスクには、CA Identity Manager がタスクを完了するために実行するアクションであるイベントが含まれます。 1 つのタスクには、複数のイベントが含まれている場合があります。 たとえば、[ユーザの作成]タスクには一般に、ユーザ プロファイルを作成するイベント、ユーザをグループに追加するイベント、ロールを割り当てるイベントが含まれます。

CA Identity Manager のタスクとイベントはワークフロー プロセスに関連付けることができます。これにより、CA Identity Manager は必要なアクションやその他のカスタムのビジネス ロジックを実行する方法について判断します。 また、タスクは「ネスト タスク」と呼ばれる別のタスクと関連付けられる場合もあります。 この場合、CA Identity Manager は元のタスクを使用してネスト タスクを処理します。

タスクのステータスは、関連付けられたイベント、ワークフロー プロセス、ネスト タスク、およびカスタム ビジネス ロジックのステータスによって決まります。

[サブミット済みタスクの表示]タブ

CA Identity Manager には[サブミット済みタスクの表示]タブが組み込まれています。このタブには、Identity Manager 環境のタスクに関する情報が表示されます。 このタブを使用して、Identity Manager が実行するアクションに関する高度な詳細情報を検索し、表示することができます。 詳細画面によって、各タスクおよびイベントに関する追加情報が提供されます。

タスクのステータスに応じて、[サブミット済みタスクの表示]を使用してタスクのキャンセルまたは再サブミットを実行できます。

[サブミット済みタスクの表示]タブでは、タスクの処理を始めから終わりまで追跡することができます。 たとえば、CA Identity Manager タスクにプロビジョニング ロールの割り当てが含まれていて、その割り当てによって別のシステムでアカウントが作成される場合、[サブミット済みタスクの表示]タブには元のタスクの全詳細と、アカウント作成に関する詳細が表示されます。

[サブミット済みタスクの表示]には、プロビジョニング サーバで実行される処理の詳細が表示されます。 これらの処理は、EnableUserEvent などの CA Identity Manager イベントに起因する場合があります。 プロビジョニング サーバから送信された通知は、このイベントの下にグループ化されます。 [サブミット済みタスクの表示]には、最後の詳細通知が送信されるまで、通知が進行中であることを示すメッセージが表示されます。その後、メッセージは[完了]に変わります。

プロビジョニング マネージャから発生した処理については、処理の詳細に関する通知はグループ化されません。 [サブミット済みタスクの表示]に、その他のタスクと共に表示されます。 処理によってエンドポイント アカウントが変更されない場合、プロビジョニング サーバは Identity Manager サーバに通知を送信しません。

Identity Manager のデフォルトでは、[サブミット済みタスクの表示]タブは以下の 2 つのタスクに組み込まれています。

- サブミット済みタスクの表示
- マイ サブミット済みタスクの表示

サブミット済みタスクの検索

サブミット済みタスクを検索するには、以下の手順に従います。

サブミット済みタスクを検索するには

1. [システム]-[サブミット済みタスクの表示]をクリックします。

   [サブミット済みタスクの表示]ページが表示されます。

2. 検索基準を指定し、表示される行の数を入力し、[検索]をクリックします。

   検索基準を満たすタスクが表示されます。

   注: 検索基準に属性を指定する方法の詳細については、サブミット済みタスクの表示に関する検索属性(462 ページ)を参照してください。

サブミット済みタスクの表示に関する検索属性

処理用にサブミットされたタスクを確認するには、[サブミット済みタスクの表示]で検索機能を使用します。 以下の条件に基づいて、タスクを検索できます。

[開始者]

検索条件となるタスクを開始したユーザの名前を識別します。 ユーザ名に基づいて検索が実行されます。 有効なユーザ名を入力したことを確認するには、[検証]ボタンを使用します。

[承認タスクの実行者:]

検索条件としてタスク承認者の名前を識別します。 ユーザ名に基づいて検索が実行されます。 有効なユーザ名を入力したことを確認するには、[検証]ボタンを使用します。

注: タスクのフィルタとして[承認タスク実行者]条件を選択した場合は、デフォルトにより[承認タスクの表示]条件も有効になります。

[タスク名]

検索条件としてタスク名を識別します。 [タスク名の条件]フィールドの値として「=」、「以下を含む」、「以下で開始:」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。 たとえば、「=」条件を指定し、テキスト フィールドに「ユーザの作成」と入力すると、「タスク名 = ユーザの作成」という検索基準を指定できます。

[タスクのステータス]

検索条件としてタスクのステータスを識別します。 タスクのステータスを選択するには、[Where task status equals]を有効にし、条件を選択します。 以下の条件に基づいて、タスクをさらに絞り込むことができます。

- 完了
- 実行中
- 失敗
- 拒否
- 一部完了
- キャンセル済み
- スケジュール済み

注: 詳細については、「タスク ステータスの説明(464 ページ)」を参照してください。

[タスク優先度]

検索条件としてタスクの優先度を識別します。 タスク優先度を選択するには、[タスク優先度の条件]を有効にして条件を選択します。 以下の条件に基づいて、タスクをさらに絞り込むことができます。

低

このオプションを指定すると、低優先度のタスクを検索できます。

中

このオプションを指定すると、中優先度のタスクを検索できます。

高

このオプションを指定すると、高優先度のタスクを検索できます。

[実行対象]

選択したオブジェクト インスタンスに対して実行されるタスクを識別します。 オブジェクト インスタンスを選択しない場合は、そのオブジェクトの全インスタンスに対して実行されたタスクがすべて表示されます。

注: このフィールドは、[サブミット済みタスクの設定]画面で[次に対し設定を実行]フィールドを指定した場合にのみ表示されます。 [サブミット済みタスク]タブを設定するには、この画面を使用します。 詳細については、この画面に関するオンラインヘルプを参照してください。

[日付範囲]

サブミット済みタスクの検索範囲を識別します。 開始日と終了日を指定する必要があります。

[サブミット解除されたタスクの表示]

監査済み状態のタスクを識別します。 他のタスクを開始したタスクや、サブミットされていないタスクが識別されます。 このタブを選択した場合は、そのようなタブがすべて監査され、表示されます。

[承認タスクの表示]

ワークフローの一部として承認すべきタスクを識別します。

[サブミット済みタスクのアーカイブを検索]

アーカイブされたサブミット済みタスクを識別します。

詳細情報:

タスク ステータスの説明 (464 ページ)

タスク ステータスの説明

サブミット済みタスクのステータスは、以下のいずれかになります。 タスクのステータスに基づいて、タスクのキャンセルや再サブミットなどのアクションを実行できます。

注: タスクをキャンセルまたは再サブミットするには、タスク ステータスに基づいてキャンセル ボタンと再サブミット ボタンが表示されるように[サブミット済みタスクの表示]を設定する必要があります。 タスクのキャンセルと再サブミットの詳細については、[サブミット済みタスクの表示]タブのカスタマイズ (467 ページ)を参照してください。

[実行中]

以下のいずれかが発生した場合に表示されます。

- ワークフローが開始されたが、まだ完了していない場合
- 現在のタスクの前に開始されたタスクが実行中の場合
- ネスト タスクが開始されたが、まだ完了していない場合
- プライマリ イベントが開始されたが、まだ完了していない場合
- セカンダリ イベントが開始されたが、まだ完了していない場合

この状態のタスクはキャンセルすることができます。

注: タスクをキャンセルすると、現在のタスクに関する未完了のネスト イベントとタスクがすべてキャンセルされます。

キャンセル済み

実行中のタスクまたはイベントのいずれかをキャンセルした場合に表示されます。

拒否

ワークフロー プロセスの一部となるイベントまたはタスクが Identity Manager によって拒否された場合に表示されます。 拒否されたタスクは再サブミットすることができます。

注: タスクを再サブミットすると、失敗または拒否されたネスト タスクとイベントがすべて再サブミットされます。

一部完了

一部のイベントまたはネスト タスクをキャンセルした場合に表示されます。 一部完了したイベントまたはネスト タスクは再サブミットすることができます。

完了

タスクが完了した場合に表示されます。 現在のタスクのネスト タスクとネスト イベントがすべて完了すると、タスクが完了します。

失敗

現在のタスクに含まれるタスク、ネスト タスク、またはネスト イベントが無効の場合に表示されます。 このステータスは、タスクが失敗した場合に表示されます。 失敗したタスクは再サブミットすることができます。

スケジュール済み

タスクを後で実行するようスケジュール設定されている場合に表示されます。 この状態のタスクはキャンセルすることができます。

監査済み

現在のタスクが監査済みの場合に表示されます。

[タスクの詳細の表示]

CA Identity Manager では、サブミット済みタスクのステータス、ネスト タスク、タスクに関連付けられたイベントなどのタスク詳細を確認できます。

サブミット済みタスクの詳細を表示する方法

1. [サブミット済みタスクの表示]タブで、選択されたタスクの横にある右矢印アイコンをクリックします。

   タスクの詳細が表示されます。

   注: イベントとネスト タスク(ある場合)は、[Task Details]ページに表示されます。タスクおよびイベントごとのタスク詳細を表示できます。

2. [閉じる]をクリックします。

   [Task Details]タブが閉じ、CA Identity Manager の[サブミット済みタスクの表示]タブにタスク リストが表示されます。

イベントの詳細の表示

CA Identity Manager では、サブミット済みイベントのステータス、イベント属性、イベントに関する追加情報などのイベント詳細を確認できます。

サブミット済みイベントの詳細を表示する方法

1. [タスクの詳細の表示]ページで、イベントの横にある右矢印アイコンをクリックします。

   イベントの詳細が表示されます。

2. [閉じる]をクリックします。

   [イベントの詳細]ページが閉じます。

イベント ステータスの説明

CA Identity Manager のイベントの状態は、以下の説明のいずれかになります。 イベントのステータスに基づいて、実行対象イベントをキャンセルまたは再サブミットできます。

注: 管理者がイベントをキャンセルまたは再サブミットできるようにするには、[イベントのキャンセル]ボタンと[Resubmit Events]ボタンが表示されるように[サブミット済みタスクの表示]を設定する必要があります。 タスクの設定時には、イベントをキャンセルおよび再サブミットできる管理者を指定できます。 イベントのキャンセルと再サブミットの詳細については、「[サブミット済みタスクの表示]タブのカスタマイズ(467 ページ)」を参照してください。

[実行中]

以下のいずれかが発生した場合に表示されます。

- ワークフローまたは事前イベントが開始済み、実行中、または承認済みの場合
- CA Identity Manager がイベントを実行中の場合
- CA Identity Manager が事後イベントを実行する場合

この状態のイベントはキャンセルすることができます。

[拒否]

ワークフローの一部となるイベントが CA Identity Manager によって拒否された場合に表示されます。 拒否されたイベントは再サブミットすることができます。

[キャンセル済み]

実行中のイベントのいずれかをキャンセルした場合に表示されます。 キャンセルされたイベントは再サブミットすることができます。

[完了]

イベントが完了した場合に表示されます。

[失敗]

イベントの実行中に CA Identity Manager が例外を検出した場合に表示されます。キャンセルされたイベントは再サブミットすることができます。

注: セカンダリ イベントは、プライマリ イベントが完了状態になるまで再サブミットできません。

[スケジュール済み]

イベントを後で実行するようスケジュール設定されている場合に表示されます。 この状態のイベントはキャンセルすることができます。

[監査済み]

現在のイベントが監査済みの場合に表示されます。

[サブミット済みタスクの表示]タブのカスタマイズ

以下のようにして、[サブミット済みタスクの表示]タブをカスタマイズできます。

- 別のタスク名とタグを指定します。
- デフォルトの表示プロパティを変更します。 ユーザがインストールすると、このタブに表示されるタスクを決定するための基準を入力できる検索画面が表示されます。ユーザが検索基準を入力せずに済むように、その日のサブミット済みタスクを自動的に表示するようにタブを設定できます。
- [Task Details]ページに監査イベントが表示されるかどうかを決定します。
- タスク表示に列を追加します。
- タスクやイベントをキャンセルまたは再サブミットするための基準を指定します。

注: 一部のタスクとイベントの詳細には、給与やパスワードといった[サブミット済みタスクの表示]タブにクリア テキスト形式で表示すべきではないデータが含まれます。 このようなデータは、directory.xml ファイルで属性を定義する際に、データ分類のパラメータを指定して非表示にすることができます。 directory.xml ファイルの詳細については、「Configuration Guide」を参照してください。

対応する管理タスクを変更して、[サブミット済みタスクの表示]タブを設定することができます。

[サブミット済みタスクの表示]タブを設定する方法

1. [ロールおよびタスク]-[管理タスク]-[管理ロールの変更]をクリックします。

   [管理タスクの選択]画面が表示されます。

2. [Search Admin Task where]フィールドで[名前]または[カテゴリ]を選択し、検索文字列を入力して[検索]をクリックします。

   CA Identity Manager には、検索基準を満たす管理タスクが表示されます。

3. [サブミット済みタスクの表示]を選択し、[選択]をクリックします。

   CA Identity Manager には、[サブミット済みタスクの表示]管理タスクのタスク詳細が表示されます。

4. [タブ]タブをクリックします。

   [サブミット済みタスクの表示]タブに使用されるタブが表示されます。

5. 右矢印アイコンをクリックし、[サブミット済みタスク]タブを編集します。

   タブの詳細が表示されます。

6. 各フィールドを編集して、必要に応じて[サブミット済みタスクの表示]タブをカスタマイズします。 詳細については、「[サブミット済みタスク]タブの設定(468 ページ)」を参照してください。

[サブミット済みタスクの表示]タブの設定

[サブミット済みタスクの表示]タブの外観と機能を変更するには、以下のフィールドを使用します。

名前

タスクの名前を定義します。

タグ

タスクの一意な識別子を定義します。 これは URL、Web サービス、またはプロパティ ファイルで使用されます。 識別子は、アルファベット文字、数字、または下線文字で構成し、先頭をアルファベット文字または下線文字にする必要があります。

タブの非表示

ユーザに対してタブが表示されるが、実行はされないことを示します。 このオプションを選択すると、ユーザに対してエラーが表示されます。

[ロード中のタスク リストを表示]

その日のサブミット済みタスクが表示されます。

注: このオプションを有効にすると、[サブミット済みタスクの表示]をクリックしたユーザに対し、その日にサブミットされたタスクが直接表示されます。

[監査イベントの表示]

[サブミット済みタスクの表示]ページ内のタスクに監査済みイベントが含まれるかどうかを指定します。

[カスタム列を許可]

タスク テーブルにカスタム列を追加できることを指定します。タスク テーブルは、[サブミット済みタスクの表示]タブと[ユーザ履歴]タブから表示できます。 たとえば、[ユーザ履歴]タブから表示されるタスク テーブルに[ユーザ ID]列を追加することができます。

カスタム列見出し

カスタム列の表示名を指定します。

[カスタム列属性]

タスク テーブル内のカスタム列に設定するための属性を指定します。 たとえば、組織の従業員に対して実行されるタスクを検索する場合は、各従業員の組織を表示する組織列を追加します。

タスクおよびイベントのキャンセル

タスクやイベントをキャンセルするための基準を指定します。 以下のいずれかのオプションを選択して、このフィールドの範囲を設定できます。

[タスク作成者は現在のユーザでなければなりません]

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

[タスク作成者はスコープに入っている必要があります]

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する、他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコープが含まれたメンバシップ ルール内の基準と自分が一致するため、[サブミット済みタスクの表示]が含まれた[ユーザ マネージャ]ロールを受け取ったとします。 この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

[許可されません]

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

タスクおよびイベントの再サブミット

タスクやイベントを再サブミットするための基準を指定します。 以下のいずれかのオプションを選択して、このフィールドの範囲を設定できます。

[タスク作成者は現在のユーザでなければなりません]

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

[タスク作成者はスコープに入っている必要があります]

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する、他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコープが含まれたメンバシップ ルール内の基準と自分が一致するため、[サブミット済みタスクの表示]が含まれた[ユーザ マネージャ]ロールを受け取ったとします。 この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

[許可されません]

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

[ユーザ履歴]タブ

[ユーザ履歴]タブでは、特定のユーザに関連するタスクを表示できます。 このタブに表示されるタスク詳細は、[サブミット済みタスクの表示]タブでも表示できます。

注: このタブを追加しても、[ユーザの作成]などのタスクを作成することはできません。

このタブを使用して、以下のタスクの履歴を表示できます。

- ユーザに対して実行されたタスク

  選択したユーザに対して実行されたタスクがすべて表示されます。

- ユーザによって実行されたタスク

  選択したユーザが実行したタスクがすべて表示されます。

- ユーザによるワークフロー承認

  ワークフローの一部としてユーザが承認したタスクがすべて表示されます。

注: このタブに表示できるタスクのタイプは、タブの設定によって異なります。 詳細については、[ユーザ履歴]タブのカスタマイズ(472 ページ)を参照してください。

ユーザ履歴の表示に関する検索属性

処理用にサブミットされたタスクを確認するには、[サブミット済みタスクの表示]で検索機能を使用します。 以下の基準に基づいて、タスクを検索できます。

タスク名

検索基準となるタスク名を識別します。 [タスク名の条件]フィールドの値として「=」、「含む」、「以下で開始:」、「終了文字列」などの条件を指定すると、検索を絞り込むことができます。 たとえば、equals 条件を指定し、テキスト フィールドに「ユーザの作成」と入力すると、「タスク名= ユーザの作成」という検索基準を指定できます。

タスク ステータス

検索基準となるタスク ステータスを識別します。 タスク ステータスを選択するには、[タスク ステータスの条件 =]を有効にし、条件を選択します。 以下の基準に基づいて、タスクをさらに絞り込むことができます。

- 完了
- 実行中
- 失敗
- 拒否
- [一部完了]
- キャンセル済み
- スケジュール済み

注: 詳細については、タスク ステータスの定義(464 ページ)を参照してください。

[タスク優先度]

検索基準となるタスクの優先度を識別します。 タスク ステータスを選択するには、[タスク ステータスの条件 =]を有効にし、条件を選択します。 以下の基準に基づいて、タスクをさらに絞り込むことができます。

低

このオプションを指定すると、低優先度のタスクを検索できます。

中

このオプションを指定すると、中優先度のタスクを検索できます。

高

このオプションを指定すると、高優先度のタスクを検索できます。

[日付範囲]

サブミット済みタスクの検索範囲を識別します。 開始日と終了日を指定する必要があります。

[ユーザ履歴]タブのカスタマイズ

管理者は以下のようにして、[ユーザ履歴]タブをカスタマイズできます。

- 別のタスク名とタグを指定します。
- デフォルトの表示プロパティを変更します。 ユーザがインストールすると、このタブに表示されるタスクを決定するための基準を入力できる検索画面が表示されます。管理者は、ユーザが検索基準を入力せずに済むように、その日のタスクを自動的に表示するようにタブを設定できます。
- [タスク詳細]ページに監査イベントが表示されるかどうかを決定します。
- タスク表示に列を追加します。
- タスクやイベントをキャンセルまたは再サブミットするための基準を指定します。

[ユーザ履歴]タブを設定する方法

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]をクリックします。

   [管理タスクの選択]画面が表示されます。

2. [Search Admin Task where]フィールドで[名前]または[カテゴリ]を選択し、検索文字列を入力して[検索]をクリックします。

   検索基準を満たす管理タスクが表示されます。

3. [ユーザ履歴]タブが含まれたタスクを選択し、[選択]をクリックします。

   その管理タスクのタスク詳細が CA Identity Manager に表示されます。

4. [タブ]タブをクリックします。
5. [ユーザ履歴]タブの横の編集アイコン( )をクリックします。

   タブの詳細が表示されます。
6. フィールドを編集して[ユーザ履歴]タブをカスタマイズします。

   参照

[ユーザ履歴]タブの設定

以下のフィールドを使用して、[ユーザ履歴]タブの表示および機能を変更します。

名前

タスクの名前を定義します。

タグ

タスクの一意な識別子を定義します。 これは URL、Web サービス、またはプロパティ ファイルで使用されます。 識別子は、アルファベット文字、数字、または下線文字で構成し、先頭をアルファベット文字または下線文字にする必要があります。

タブの非表示

ユーザに対してタブが表示されるが、実行はされないことを示します。 このオプションを選択すると、ユーザに対してエラーが表示されます。

[ロード中のタスク リストを表示]

その日のサブミット済みタスクが表示されます。

注: このオプションを有効にすると、[サブミット済みタスクの表示]をクリックしたユーザに対し、その日にサブミットされたタスクが直接表示されます。

[監査イベントの表示]

[サブミット済みタスクの表示]ページ内のタスクに監査済みイベントが含まれるかどうかを指定します。

[カスタム列を許可]

タスク テーブルにカスタム列を追加できることを指定します。タスク テーブルは、[サブミット済みタスクの表示]タブと[ユーザ履歴]タブから表示できます。 たとえば、[ユーザ履歴]タブから表示されるタスク テーブルに[ユーザ ID]列を追加することができます。

カスタム列見出し

カスタム列の表示名を指定します。

[カスタム列属性]

タスク テーブル内のカスタム列に設定するための属性を指定します。 たとえば、組織の従業員に対して実行されるタスクを検索する場合は、各従業員の組織を表示する組織列を追加します。

タスクおよびイベントのキャンセル

タスクやイベントをキャンセルするための基準を指定します。 以下のいずれかのオプションを選択して、このフィールドの範囲を設定できます。

[タスク作成者は現在のユーザでなければなりません]

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

[タスク作成者はスコープに入っている必要があります]

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する、他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコープが含まれたメンバシップ ルール内の基準と自分が一致するため、[サブミット済みタスクの表示]が含まれた[ユーザ マネージャ]ロールを受け取ったとします。 この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

[許可されません]

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

タスクおよびイベントの再サブミット

タスクやイベントを再サブミットするための基準を指定します。 以下のいずれかのオプションを選択して、このフィールドの範囲を設定できます。

[タスク作成者は現在のユーザでなければなりません]

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

[タスク作成者はスコープに入っている必要があります]

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する、他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコープが含まれたメンバシップ ルール内の基準と自分が一致するため、[サブミット済みタスクの表示]が含まれた[ユーザ マネージャ]ロールを受け取ったとします。 この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

[許可されません]

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

タスクの表示

[ユーザ履歴]タブに表示されるタスクを決定します。

ユーザに対して実行されるタスク

選択したユーザに対して実行されるすべてのタスクを表示します。

ユーザによって実行されるタスク

選択したユーザによって実行されるすべてのタスクを表示します。

ユーザが承認したワークフロー

ワークフローの一部としてユーザが承認したすべてのタスクを表示します。

ユーザ アクティビティの表示タスク

ユーザ アクティビティとは、ある特定のユーザに関するタスクの履歴です。 管理者は[ユーザ アクティビティの表示]タスクを使用して、以下のユーザ情報を追跡できます。

- ユーザに対して実行されるタスク
- ユーザによって実行されるタスク
- ユーザが実行するワークフローの承認

ユーザ アクティビティを表示する方法

1. [ユーザ]-[ユーザの管理]-[ユーザ アクティビティの表示]をクリックします。

   [ユーザの選択]画面が表示されます。

2. ユーザを検索して[選択]をクリックします。

   [ユーザ アクティビティの表示]画面が表示されます。

注: 表示されたユーザ アクティビティの詳細については、ユーザ コンソールのオンライン ヘルプを参照してください。

Bulk Loader

[Bulk Loader]タブを使用して、同時に多数の管理対象オブジェクトを操作するために使用するフィーダ ファイルをアップロードできます。 たとえば、1000 人のユーザを手動で CA Identity Manager に作成することも、Bulk Loader を使用して作成することもできます。 Bulk Loader 操作の利点は、多数の管理対象オブジェクトの操作の処理を 1 つの情報(フィーダ)ファイルを使用して自動化できることです。 [Bulk Loader]タスクをワークフロー プロセスにマッピングすることもできます。

注: [Bulk Loader]タスクのワークフローへのマッピング方法の詳細については、「ワークフローの概要(335 ページ)」を参照してください。

Bulk Loader クライアントは、バッチ処理用として存在します。 CA Identity Manager 環境が(負荷分散目的で)クラスタ内に存在する場合は、Bulk Load クライアントの使用をお勧めします。 Bulk Loader クライアントは、プロビジョニング コンポーネント メディア上にあります。

Bulk Loader タスクの管理ロールへの追加

多数のプライマリ オブジェクトを操作するには、[Bulk Loader]タスクを使用します。 システム マネージャとしてログインし、[Bulk Loader]タスクを使用するように管理ロールを設定します。

Bulk Loader タスクを管理ロールへ追加する方法

1. システム マネージャとしてログインします。
2. [ロールおよびタスク]をクリックします。

   [ロールおよびタスク]のタスクが表示されます。
3. [管理ロール]-[管理ロールの変更]をクリックします。

   [管理ロール検索]画面が表示されます。
4. [Bulk Loader]タスクを追加する管理ロールを検索し、[選択]をクリックします。

   管理ロールの詳細が表示されます。
5. [タスク]タブで、以下のオプションを選択して新しいタスクを追加します。
   - カテゴリでフィルタ: システム
   - タスクの追加: Bulk Loader
6. [送信]をクリックします。

   管理ロールが[Bulk Loader]タスクを使用するように設定されます。

Bulk Loader の使用法

多数のユーザ、グループまたは組織を操作するには、以下の手順を実行します。

1. CSV または XLS フィーダ ファイルを作成します。
2. フィーダ ファイルをアップロードします。
3. [Loader レコード詳細]を設定します。

   このタブでは、フィーダ ファイルのアクションおよび識別子フィールドを指定することができます。
4. [Loader アクション マッピング]を選択します。

   このタブでは、プライマリ オブジェクトを選択し、そのオブジェクトのアクションに実行するタスクを指定することができます。
5. [システム]タブの下の[サブミット済みタスクの表示]タブで[Bulk Loader]タスクの進行状況を参照し、変更します。

以下の点に注意してください。

- 多数のオブジェクトのアップロードなど、時間のかかるタスクの実行中に Identity Manager サーバがダウンした場合は、[サブミット済みタスクの表示]タブでタスクを再開できます。 タスクが再開される場合、最後に正常に実行されたレコードから開始されます。
- Solaris のユーザ ストアとして LDAP を使用している場合は、インポート中に Bulk Loader が停止する場合があります。 この問題を修正するには、「Configuration Guide」の「Specify LDAP Connection Settings」トピックを参照し、そこに説明されている設定を適用してください。

フィーダ ファイルの作成

各フィーダ ファイルには、多数のプライマリ オブジェクトを自動管理するために使用できるデータが含まれます。

フィーダ ファイルを作成する方法

1. テキスト エディタを使用して、CSV または XLS ファイルを作成します。 適切なファイル 形式(478 ページ)を使用します。
2. ファイルを保存します。

   多数のプライマリ オブジェクトを操作する環境に、このファイルをアップロードします。

フィーダ ファイル形式

Bulk Loader ファイルの使用により、多数の管理対象オブジェクトに対してアクションが繰り返し自動実行されます。 フィーダ ファイルをアップロードすると、CA Identity Manager によってフィーダ ファイルが解析され、読み込まれます。

フィーダ ファイルは拡張子が CSV または XLS で、プロパティが以下のとおりである必要があります。

- このファイルには、管理対象オブジェクトのフィジカル アトリビュート、ロジカル アトリビュートまたは既知の属性の名前を指定するヘッダ行が含まれている必要があります。
- ヘッダ行には、レコードに対して実行されるアクションを示す列が含まれている必要があります。
- フィーダ ファイルの各行を「レコード」と呼びます。 レコードには、ヘッダ行によって指定された各属性の値が含まれます。 属性に対して使用できる値として以下のオプションがあります。
  - 値 — 属性は指定した値に設定されます。
  - 値;値;値;... — 属性は指定した複数値属性に設定されます。
  - ''(空白) — 属性は変更されません。
  - NULL — 属性は削除されます。 削除の順序はデフォルトで「NULL」に設定されていますが、[Bulk Loader ファイル アップロード検索]画面で編集できます。

重要: Bulk Loader ファイルは、UTF-8 エンコーディングで保存する必要があります。

フィーダ ファイルのサンプル

CSV フィーダ ファイルのサンプル

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,test,Johndoe@a.com
Modify,MD,Jane,Doe,Jane Doe,test,Marydoe@a.com
create,BD,Baby,Doe,Baby Doe,test,Babydoe@a.com
```

上記のコードで、フィーダ ファイルのプロパティは以下のとおりです。

[ヘッダ]

コードの最初の行はヘッダ行です。 ヘッダ行には、管理対象オブジェクト「ユーザ」のフィジカル アトリビュートまたは既知の属性が含まれます。

[アクション]

アクション列では、各レコードに対して実行されるタスクを識別します。 たとえば、上記のファイルでは、名「John」に対して「作成」アクションを実行するように指定しています。

[Loader レコード詳細]タブ

この[Loader レコード詳細]タブでは、フィーダ ファイルに存在するレコードの簡易プレビューが表示されます。 プレビュー テーブルには最大 5 レコードが表示されます。 プレビュー テーブルは、正しいファイルをアップロードしているかどうかを確認するのに役立ちます。 また、このタブでは、フィーダ ファイルで指定した管理対象オブジェクトに実行するアクションを指定することもできます。 以下のフィールドを洗い出し、それらのフィールドに入力する必要があります。

このオブジェクトに対して実行されるアクションを表しているのは、どのフィールドですか?

管理対象オブジェクトに実行するアクションを示すフィールドを、フィーダ ファイルから洗い出します。 たとえば、Create、Modify、Delete という値を取る 'action'というフィールドがあるフィーダ ファイルを使用できます。 これらの各アクションを[Loader アクション マッピング(480 ページ)]の管理タスクにマップする必要があります。

そのオブジェクトを一意に識別するにはどのフィールドを使用しますか。

プライマリ オブジェクトを一意に識別できるフィールドを、フィーダ ファイルから洗い出します。

注: 無効なヘッダ行がフィーダ ファイルにあると、フィーダ ファイル レコードは[Loader レコード詳細]タブに表示されません。 ヘッダー行が無効の場合は、別のフィーダ ファイルを選択してください。 フィーダ ファイルに無効なレコードが含まれていると、[システム]タブの下の[サブミット済みタスクの表示]にアップロードの詳細ステータスが表示されます。

[Loader アクション マッピング]タブ

[Loader アクション マッピング]タブでは、フィーダ ファイルで指定されたアクションの実行対象となるプライマリ オブジェクトを選択することができます。 また、選択したプライマリ オブジェクトに対するフィーダ ファイル内アクションを管理タスクにマップする必要があります。

プライマリ オブジェクトとは何でしょうか。

フィーダ ファイルを使用して CA Identity Manager によって操作されるプライマリ オブジェクトのことを表します。 以下のいずれかのプライマリ オブジェクトを選択できます。

- ユーザ
- グループ
- 組織

'action' 用に実行するタスクの選択

フィーダ ファイルが指定した各アクション用に実行する必要のある管理タスク、たとえば[削除]や[変更]タスクを指定します。

注: フィーダ ファイルに記述したすべてのアクションを管理タスクにマップする必要があります。 また、このフィールドに表示される管理タスクは、選択したプライマリ オブジェクトに従属します。 たとえば、プライマリ オブジェクトとして「ユーザ」を選択していると、「ユーザ」に関連する管理タスクのみが表示されます。

'action' 用の存在しないオブジェクトに対するタスクの選択

管理対象オブジェクトが CA Identity Manager 内にまだ存在しない場合には、フィーダ ファイルが指定したアクション用に実行する必要のある代替管理タスク、たとえば作成タスクを指定します。

フィーダ タスクに関する電子メール通知の有効化

ワークフロー プロセスの一部として[Bulk Loader]タスクに電子メール通知を設定するには、[Bulk Loader イベント]または[Bulk Loader]タスクの管理コンソールで電子メール通知を有効にします。

注: 電子メール通知の詳細については、管理コンソールのオンライン ヘルプを参照してください。

[Bulk Loader]タスクのスケジュール

[Bulk Loader]タスクは、CA Identity Manager でスケジュール設定することができます。[Bulk Loader]タスクをスケジュールするには、そのタスクに スケジューラのタブを追加 (64 ページ)します。

「Bulk Loader」の解析ファイルの変更

パーサ CA Identity Manager の用途をフィーダ ファイルの解析に変更するには、該当する管理タスクを設定します。

Bulk Loader の管理タスクを変更する方法

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]をクリックします。
2. [Bulk Loader]タスクを検索します。
3. [Bulk Loader]タスクを選択し、[選択]をクリックします。
4. [Bulk Loader]タスクの[検索]タブを選択します。
5. [参照]をクリックして検索画面を検索します。

   利用可能な検索画面のリストが表示されます。
6. 検索画面を選択して[編集]をクリックします。

   [検索]画面の詳細が表示されます。
7. (オプション)[パーサの完全修飾名]を編集します。

   [パーサの完全修飾名]は、パーサ ファイル名と一致する必要があります。

   注: CA Identity Manager で提供されるパーサのサンプルがデフォルト値として表示されます。 サンプルのパーサ ファイルを使用して、CSV ファイルと XLS ファイルを解析します。 CA Identity Manager で提供されるサンプルのパーサ ファイルは以下の場所にあります。

   admin_tools¥samples¥feeder
8. [OK]をクリックします。

Bulk Loader の Web サービス サポート

Bulk Loader には、CA Identity Manager の Task Execution Web Service(TEWS)インターフェースを使用して呼び出すことができる Web サービス API があります。 TEWS では、クライアント アプリケーションがリモート タスクを CA Identity Manager にサブミットして実行できます。 このインターフェースは、WSDL および SOAP のオープン標準を実装して、CA Identity Manager へのリモート アクセスを提供します。

CA Identity Manager には、Web サービスとして Bulk Loader への呼び出しの実例を示す Java クライアント サンプルが含まれています。 Java サンプルは、以下のソースファイルにあります。

admin_tools¥samples¥WebService¥Axis¥optional¥ObjectFeeder.java

Web サービスとして Bulk Loader を呼び出す方法が記載されたデータ サンプルおよびマニュアルは、以下のディレクトリにあります。

admin_tools¥samples¥Feeder¥

注: 詳細については、「Programming Guide for Java」を参照してください。

Bulk Loader のメモリに関する注意事項

Bulk Loader を使用して、多数のユーザをインポートすると、メモリ不足の例外が発生する場合があります。 また、Bulk Loader が多数のユーザをインポートするときに、膨大なリソースを必要とするタスクを実行すると、タスクによっては失敗する場合があります。

このような問題の対処方法として、以下について検討します。

- バッチ サーバを Identity Manager 実装で追加して、大量のインポートを処理する

  注: バッチ サーバの追加の詳細については、「実装ガイド」を参照してください。
- JVM メモリの設定を増やす

セレクト ボックス データ

以下のフィールドに使用するオプションを作成できます。

- チェック ボックスの複数選択
- ドロップダウン
- ドロップダウン コンボ
- 複数選択
- オプション セレクタ
- オプション セレクタ コンボ

- ラジオ ボタンとしての単一選択
- 単一選択

これらのオプションはセレクト ボックス データの XML ファイルに格納されます。 たとえば、セレクト ボックス データ XML ファイルを使用して、[ユーザの作成]タスクの[プロファイル]タブにある市区町村または都道府県ドロップダウン ボックスのオプションを入力できます。

また、セレクト ボックス データの XML ファイルを使用して、管理タスクの 2 つのフィールド間に依存関係を設定することもできます。 たとえば、[市区町村]フィールドに入力可能なオプションを、[都道府県]フィールドでユーザが選択したオプションに依存させることができます。

注: セレクト ボックス データの詳細については、「User Console Design Guide」を参照してください。

ロジカル アトリビュート ハンドラ

CA Identity Manager ロジカル アトリビュートでは、ユーザが保存した属性(フィジカル アトリビュートと呼びます)をタスク画面上にわかりやすい形式で表示できます。 CA Identity Manager 管理者はタスク画面を使用して CA Identity Manager の機能を実行します。 ロジカル アトリビュートはユーザ ストアには存在しません。 通常、ロジカル アトリビュートは 1 つ以上のフィジカル アトリビュートを表して表示を簡略化します。 たとえば、ロジカル アトリビュートの日付は、月、日、および年のフィジカル アトリビュートを表すことができます。

ロジカル アトリビュートはロジカル アトリビュート ハンドラによって処理されます。ロジカル アトリビュート ハンドラは、ロジカル アトリビュート API を使用して作成された Java オブジェクトです (「Java のプログラミング ガイド」を参照してください)。たとえば、タスク画面の場合、ロジカル アトリビュート ハンドラによってユーザ ストアのフィジカル アトリビュート データがロジカル アトリビュート データに変換されます。このデータがタスク画面に表示されます。 CA Identity Manager にある事前定義されたロジカル アトリビュートとロジカル アトリビュート ハンドラを使用することも、ロジカル アトリビュート API を使用して新たにロジカル アトリビュート ハンドラを作成することもできます。

注: ロジカル アトリビュートの詳細については、「Java のプログラミング ガイド」を参照してください。

ユーザ コンソールの[環境]カテゴリには、ロジカル アトリビュート ハンドラを管理するためのタスクが含まれています。 リストには、CA Identity Manager に付属している事前定義されたハンドラと、組織で定義したすべてのカスタム ハンドラが表示されます。

[環境]タスク カテゴリから以下を実行できます。

- CA Identity Manager を使用した新規のロジカル アトリビュート ハンドラの作成
- ハンドラのコピー
- ハンドラの削除
- 既存のハンドラ設定の変更

注: ロジカル アトリビュート ハンドラの実行順序を変更するには、管理コンソールを使用します。

ロジカル アトリビュート ハンドラの作成

ロジカル アトリビュート ハンドラの作成方法

1. [システム]-[ロジカル アトリビュート ハンドラの作成]を選択します。
2. [ロジカル アトリビュート ハンドラの作成]画面で[標準ロジカル アトリビュート ハンドラの作成]を選択し、[OK]をクリックします。
3. [ロジカル アトリビュート ハンドラの作成]画面で、ロジカル アトリビュート ハンドラの設定を行います。

   各フィールドの説明については、この画面のヘルプ リンクをクリックして参照してください。
4. [サブミット]をクリックします。

   このハンドラが[ロジカル アトリビュート ハンドラ]画面のハンドラ リストに表示されます。

注: ユーザ コンソールを使用してロジカル アトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラのコピー

ロジカル アトリビュート ハンドラをコピーする方法

1. [システム]-[ロジカル アトリビュート ハンドラの作成]を選択します。
2. [ロジカル アトリビュート ハンドラの作成]画面で、[ロジカル アトリビュート ハンドラ定義のコピーの作成]を選択して[検索]をクリックします。
3. ロジカル アトリビュート ハンドラ(ConfirmPasswordHandler など)を選択して、[OK]をクリックします。

4. [ロジカル アトリビュート ハンドラの作成]画面で、ロジカル アトリビュート ハンドラの設定を行います。

   各フィールドの説明については、この画面のヘルプ リンクをクリックして参照してください。

5. [送信]をクリックします。

   このハンドラが[ロジカル アトリビュート ハンドラ]画面のハンドラ リストに表示されます。

注: ユーザ コンソールを使用してロジカル アトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラ ForgottenPasswordHandler の作成

ロジカル アトリビュート ハンドラ ForgottenPasswordHandler では、以下の操作に対して個別のロジカル アトリビュートを使用します。

- 設定
- 実行時の質問と回答

ロジカル アトリビュート ハンドラ ForgottenPasswordHandler の作成方法

1. [システム]-[ロジカル アトリビュート ハンドラの作成]を選択します。
2. [ロジカル アトリビュート ハンドラの作成]画面で[標準ロジカル アトリビュート ハンドラの作成]を選択し、[検索]をクリックします。
3. ForgottenPasswordHandler を選択し、[OK]をクリックします。
4. ForgottenPasswordHandler の[ロジカル アトリビュート ハンドラの作成]画面で、ロジカル アトリビュート ハンドラの設定を行います。

   各フィールドの説明については、この画面のヘルプ リンクをクリックして参照してください。

5. [サブミット]をクリックします。

   このハンドラが[ロジカル アトリビュート ハンドラ]画面のハンドラ リストに表示されます。

注: ユーザ コンソールを使用してロジカル アトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラの削除

ロジカル アトリビュート ハンドラを削除する方法

1. [システム]-[ロジカル アトリビュート ハンドラの削除]を選択します。
2. [ロジカル アトリビュート ハンドラの削除]画面で、削除する各ロジカル アトリビュートの横にあるチェック ボックスをオンにします。
3. [選択]をクリックします。

   CA Identity Manager に確認メッセージが表示されます。
4. [はい]をクリックして、削除を確定します。

ロジカル アトリビュート ハンドラの変更

ロジカル アトリビュート ハンドラの変更方法

1. [システム]-[ロジカル アトリビュート ハンドラの変更]を選択します。
2. [ロジカル アトリビュート ハンドラの変更]画面で、変更するハンドラを選択して、[選択]をクリックします。
3. ロジカル アトリビュート ハンドラ(ConfirmPasswordHandler など)を選択して、[OK]をクリックします。
4. [ロジカル アトリビュート ハンドラの変更]画面で、ロジカル アトリビュート ハンドラの設定を行います。

   各フィールドの説明については、この画面のヘルプ リンクをクリックして参照してください。
5. [サブミット]をクリックします。

注: ユーザ コンソールを使用してロジカル アトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラの表示

ロジカル アトリビュート ハンドラの表示方法

1. [システム]-[ロジカル アトリビュート ハンドラの表示]を選択します。
2. [View Logical Attribute Handler(ロジカル アトリビュート ハンドラの表示)]画面で、表示するハンドラを選択して、[選択]をクリックします。
3. ロジカル アトリビュート ハンドラのプロパティを参照して、[閉じる]をクリックします。

JDBC 接続管理

CA Identity Manager レポートに関する情報は複数のソースから取得できます。各レポートは、レポートに表示する情報に応じて特定のデータ ソースに関連付けられている必要があります。

レポートに使用する他のデータ ソース(監査データベース、またはタスク永続性データベースなど)を確立するには、CA Identity Manager で接続管理オブジェクトを作成します。 接続を作成すると、レポート タスクの[検索]タブで、レポート タスクを変更し、[レポート用接続オブジェクト]を設定して、レポートを特定の接続管理オブジェクトに関連付けることができます。

JDBC 接続の作成

CA Identity Manager に接続に関する詳細を設定するには、以下の手順に従います。

JDBC 接続を作成する方法

1. [システム]-[JDBC 接続管理]-[JDBC 接続の作成]をクリックします。
2. 新しい接続オブジェクトを作成するか、特定の JNDI データ ソースに基づいて接続オブジェクトを選択します。
3. 必要なすべてのフィールドに入力して、[送信]をクリックします。

   新しい JDBC 接続が作成されます。

サブミット済みタスクのクリーンアップ

各タスクをサブミットして、タスク永続性データベースが拡大するにつれ、タスクおよびイベントの実行時のパフォーマンスが低下します。 ストアド プロシージャのガーベッジ コレクションを行うと、タスク永続性データベースの記憶領域が不足することが原因のパフォーマンス上の問題やシステムの機能停止のリスクを低減することができます。 タスクのアーカイブ機能を使用することで、管理者は、削除されたタスクやイベントと共に現在のタスクおよびイベント情報の両方を表示できます。

ユーザ コンソールで、CA Identity Manager の管理者は、ガーベッジ コレクションおよびアーカイブが反復ベースで自動的に実行されるように、ジョブをスケジュールすることができます。

[反復]タブ

このタブを使用して、ジョブをスケジュールします。 このタブ内のフィールドは以下のとおりです。

[今すぐ実行]

クエリを今すぐ実行します

[新規ジョブのスケジュール]

新規ジョブをスケジュールします。

[既存ジョブの変更]

すでに存在するジョブで変更するジョブを指定します。

注: このタスクにジョブがすでにスケジュールされている場合には、このフィールドのみが表示されます。

[ジョブ名]

作成または変更するジョブの名前を指定します。

[タイムゾーン]

サーバーの時間帯を指定します。

注: 新しいジョブのスケジュール時に、使用しているタイムゾーンがサーバーのタイムゾーンと異なる場合には、ドロップダウンボックスが表示されますので、使用中のタイムゾーンまたはサーバーのタイムゾーンのいずれを使用するかを選択できます。既存のジョブを修正する場合には、タイムゾーンは変更できません。

[毎週のスケジュール]

ある週の特定の日または期間でのジョブの実行を指定します。

[詳細なスケジュール]

その他のスケジュール情報を指定します。

[曜日]

ジョブを実行する曜日を指定します。

[実行時間]

ジョブを実行する時刻を、24 時間形式で指定します。 例: 14:15

[Cron 式]

このフィールドの入力の詳細については、以下の Web サイトを参照してください。

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

注:[詳細なスケジュール]が選択されている場合には、このフィールドが表示されます。

詳細情報

ジョブの即時実行 (286 ページ)
[新規ジョブのスケジュール] (286 ページ)
既存のジョブの変更 (287 ページ)
[反復タスクの削除] (287 ページ)

ジョブの即時実行

ジョブを即時に実行するには、[サブミット済みタスクのクリーンアップ]ウィザードを使用します。

[システム]タブで、以下の操作を実行します。

1. 左ペインから、[サブミット済みタスクのクリーンアップ]を選択します。

   [反復]手順のウィザードが表示されます。

2. [今すぐ実行]-[次へ]を選択します。

   [サブミット済みタスクのクリーンアップ]手順のウィザードが表示されます。

3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了]をクリックします。

   ジョブが即時にサブミットされます。

[新規ジョブのスケジュール]

新規ジョブをスケジュールするには、[サブミット済みタスクのクリーンアップ]ウィザードを使用します。

[システム]タブをクリックします。

1. 左ペインから、[サブミット済みタスクのクリーンアップ]を選択します。

   [反復]手順が表示されます。

2. [新規ジョブのスケジュール]を選択し、ジョブ名とそのジョブのスケジュール設定情報を入力し、[次へ]をクリックします。

   [サブミット済みタスクのクリーンアップ]手順が表示されます。

3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了]をクリックします。

   新規ジョブがスケジュール化されます。

既存のジョブの変更

既存のジョブを変更するには、[サブミット済みタスクのクリーンアップ]ウィザードを使用します。

[システム]タブで、以下の操作を実行します。

1. 左ペインから、[サブミット済みタスクのクリーンアップ]を選択します。

   [反復]手順が表示されます。

2. [既存ジョブの変更]を選択し、既存のジョブを選び、スケジュール情報を変更してから、[次へ]をクリックします。

   [サブミット済みタスクのクリーンアップ]手順が表示されます。

3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を変更してから、[完了]をクリックします。

   既存のジョブが変更されます。

[反復タスクの削除]

反復するタスクの削除方法

[サブミット済みタスクの表示]をクリックします。

1. [反復タスクの削除]を選択します。
2. 削除するタスクを選択します。
3. [サブミット]をクリックします。

[サブミット済みタスクのクリーンアップ]タブ

このタブを使用して、タスクの最小期間、アーカイブ、監査タイムアウト、制限時間、タスク制限を指定します。 すべての必須フィールドに入力したら[完了]をクリックします。 このタブ内のフィールドは以下のとおりです。

[最小期間]

最終状態(完了、失敗、拒否、キャンセル、または中止)にあるタスクがクリーンアップされるまでの最小期間を指定します。 たとえば、最小期間に 1 か月を指定した場合、最後の月に最終状態に到達した任意のタスクは保持されます。 1 か月以上前に、最終状態に到達したタスクは、クリーンアップおよびアーカイブ対象となります。

これは必須フィールドです。

[アーカイブ]

実行中のデータベースからタスクを削除する前に、アーカイブデータベースにタスクをバックアップします。

ジョブが実行されたら、アーカイブが選択されている場合、データはアーカイブ データベースにコミットされ、実行時のタスク永続性データベースから削除されます。 データはアーカイブ データベースに正常にコミットされるまで削除されません。

[監査タイムアウト]

監査状態にあるタスクがクリーンアップされるまでの時間の長さを指定します。 監査状態のタスクは、この期間が経過するまで最終状態とはみなされません。 監査状態のタスクは、サブミットされていません。

[時間制限]

クリーンアップを特定の時間内に制限します。

[タスク制限]

クリーアップを特定のタスク回数に制限します。

反復タスクの削除

タスクを反復ベースで実行する必要性がなくなった場合に、CA Identity Manager の管理者はタスクを削除できます。 タスクが削除されると、ガーベッジ コレクションおよびアーカイブは、そのタスクに対しては実行されません。

[サブミット済みタスクのクリーンアップ]を使用してスケジュールしたすべてのタスク: 反復ウィザードは、このページにリストされており、CA Identity Manager の管理者は、どのタスクを削除するかを選択できます。

注: そのタスクは、依然としてデータベースには存在しており、反復のスケジュールのみが削除されます。

Enterprise Log Manager 接続の設定

この画面を使用して、新規に追加された CA Enterprise Log Manager 接続タスクを管理します。

この画面のフィールドを以下に示します。

[接続名]

単一の CA ELM 接続管理オブジェクトに使用する一意の名前を指定します。

このフィールドは、読み取り専用です。

[説明]

その CA ELM 接続について説明します。

[ホスト名]

CA Enterprise Log Manager サーバのホスト名または IP アドレスを指定します。

これは必須フィールドです。

[ポート #]

CA Enterprise Log Manager サーバの接続ポートを指定します。

デフォルト: 52520

これは必須フィールドです。

[認証機関によって署名された SSL 証明書]

チェックがオンになっている場合には、CA Enterprise Log Manager サーバへの接続時に、厳格な SSL 証明書チェックを指定します。

たとえば、デフォルトで CA Enterprise Log Manager にインストールされている SSL 証明書のような自己署名 SSL 証明書を有する場合は、ルート認証局へのトラステッド パスが存在しないので、このチェック ボックスをオフにする必要があります。

[証明書名]

認証に使用する CA Enterprise Log Manager 証明書の名前を指定します。

これは必須フィールドです。

[Certificate Password]

CA Enterprise Log Manager のパスワードを指定します。

これは必須フィールドです。

[属性]

サポート対象外です。 バージョンは、接続情報をテストとして保存するために取得します。

Enterprise Log Manager 接続の削除

リストから接続を選択して、[削除]をクリックします。 CA Enterprise Log Manager 接続タスクが削除されます。

付録 A: デフォルトのタスクとロール

Identity Manager 環境には、ある環境で使用または変更できるデフォルトのタスクとロールのセットが存在します。

このセクションには、以下のトピックが含まれています。

デフォルトのセルフサービス タスク (495 ページ)
デフォルトの管理タスク (496 ページ)
デフォルトの管理ロール (512 ページ)
デフォルトのワークフロー承認ロール (519 ページ)

デフォルトのセルフサービス タスク

CA Identity Manager には以下のセルフサービス タスクがあります。

- 自己登録 (495 ページ)
- 忘れたパスワード (495 ページ)
- 忘れたパスワードのリセット (496 ページ)
- 忘れたユーザ ID (496 ページ)
- パスワード サービス (496 ページ)

これらのタスクは、ユーザがログイン認証情報を提供せずに使用できる、パブリック タスクです。

自己登録

「自己登録」タスクでは、ユーザは管理者の関与なしに企業 Web サイトに登録できます。ユーザはプロファイル情報を入力してパスワードを設定し、グループにサブスクライブすることができます。

忘れたパスワード

「忘れたパスワード」タスクでは、一時パスワードが提供され、ユーザはこのパスワードを使用して Identity Manager にログインできます。 ユーザがログインすると、ただちに新しいパスワードを入力するように求められます。

忘れたパスワードのリセット

[忘れたパスワードのリセット]タスクを使用すると、ユーザの身元が確認された後に、ユーザがパスワードをリセットできます。

デフォルトの「忘れたパスワードのリセット」タスクでは、ユーザはユーザ ID を入力して 3 つの確認の質問に回答する必要があります。 Identity Manager によってユーザ ID が確認されると、新しいパスワードを入力する画面が表示されます。

忘れたユーザ ID

「忘れたユーザ ID」タスクでは、忘れたユーザ ID を取得できます。 デフォルトのタスクでは、ユーザ ID が記載された電子メールを受信するために電子メール アドレスを入力し、1 つの確認の質問に回答する必要があります。

パスワードサービス

「パスワード サービス」タスクでは、ユーザが現在のパスワードを入力した後で、そのパスワードが変更されます。 パスワード ポリシーまたは SiteMinder 認証エラーなどにより、強制的にパスワードの変更を求められる場合、ユーザは自動的に「パスワード サービス」タスクに移動します。

このタスクは、ユーザ コンソールのタスクとして表示されません。

デフォルトの管理タスク

管理ロールを作成する場合、以下のカテゴリのユーザ インターフェースに表示される任意のデフォルトの管理タスクを含めることができます。

- ホーム
- アクセス ロール (453 ページ)
- 管理ロール (499 ページ)
- 認証 (501 ページ)
- グループ (502 ページ)
- 組織 (504 ページ)
- ポリシー (505 ページ)
- プロビジョニング ロール (507 ページ)

- ［レポート］
- システム（508 ページ）
- ユーザ

注： Identity Manager に表示されるタスクのうち、ここで定義されたタスク以外ものは、Identity Manager 管理者によって作成されたタスクです。

割り当てられた管理ロールに応じて、特定の管理タスクのみを参照できます。 たとえば、デフォルトの「グループ マネージャ」ロールを割り当てられた場合は、［グループ］にある 5 つのタスクを参照できます。

注： タスクを使用した後、処理のためにタスクがサブミットされたというメッセージが表示された場合は、変更が有効になっていない可能性があることを示しています。 この処理の詳細については、「管理タスクの処理」（74 ページ）を参照してください。

ホーム

［マイ アカウント］タブには、現在のユーザのプロファイル、ロール、グループ、およびパスワードを参照または変更するための以下のタスクがあります。

- マイ アカウントの変更（497 ページ）
- マイ パスワードの変更（497 ページ）
- マイ グループの変更（498 ページ）
- マイ プロファイルの変更（498 ページ）
- 不在時（498 ページ）
- マイ ロールの表示（499 ページ）
- マイ サブミット済みタスクの表示（499 ページ）
- マイ ワーク リストの表示（499 ページ）

マイ アカウントの変更

マイ アカウントの変更では、ユーザの詳細の変更を要求できます。

マイ パスワードの変更

「マイ パスワードの変更」タスクでは、ユーザが現在のパスワードを入力した後で、そのパスワードが変更されます。 このタスクはユーザ パスワードのリセットとは異なり、現在のパスワードを必要とせずに別のユーザのパスワードを変更します。

[マイ エンドポイント アカウントの変更]

[マイ エンドポイント アカウントの変更]は、選択したアカウントに対して以下のアクションを実行します。

- アカウントの現在のステータスの取得
- ユーザへのアカウントの割り当て
- ユーザのアカウントの割り当て解除
- アカウントの一時停止
- 一時停止されたアカウントの再開
- アカウントのロック解除
- アカウントのパスワードを変更
- アカウントの削除

マイ グループの変更

「マイ グループの変更」タスクでは、任意の自己登録グループへの追加や削除を行えます。 [グループ]タブには、ユーザに割り当てられたグループおよびメンバとなった自己登録グループが表示されます。

他の自己登録グループのメンバとして追加するには、[さらに追加]をクリックします。 グループから削除するには、各自己登録グループの横の[削除]チェック ボックスをクリックします。

マイ プロファイルの変更

「マイ プロファイルの変更」タスクでは、名前、電話番号、および役職などの個人情報を変更できます。

不在時

不在時では、ユーザ(委任者)が別のユーザ(代行者)を指定して、代行者が委任者のワーク リスト内のタスクを承認できるようにします。 委任者の「不在時」に、委任者は作業アイテムを他の承認者に割り当てることができます。

マイ エンドポイント アカウントの変更

[マイ エンドポイント アカウントの変更]には、エンドポイント システム上の各アカウントのステータスが表示されます。

マイ ロールの表示

「マイ ロールの表示」タスクでは、自分がロール メンバまたはロール管理者であるロールのリストを表示できます。

マイ サブミット済みタスクの表示

「マイ サブミット済みタスクの表示」タスクでは、処理のためにサブミットしたタスクのステータスを表示できます。 このタスクを実行すると、以下のことを行えます。

- 開始したすべてのタスクを表示できます。または、一定期間にサブミットしたタスクを検索して表示するなど、ある特定の基準を満たすタスクのみを表示できます。
- タスクによって生成されたイベントに関する詳細を表示できます。

注: このタスクは TEWS(Task Execution Web Service)では使用できません。

マイ ワーク リストの表示

「マイ ワーク リストの表示」タスクでは、ワークフロー プロセスにより受信したすべてのタスクを参照できます。 通常、これらのタスクではワークフロー プロセスを続行するための承認アクションが必要です。

管理ロール

「管理ロールの管理」カテゴリを使用して、管理ロールおよび 管理タスク(31 ページ)を作成または管理します。

このカテゴリには、以下のタスクがあります。

- 管理ロールの作成(500 ページ)
- 管理タスクの作成(500 ページ)
- 管理ロールの削除(500 ページ)
- 管理タスクの削除(500 ページ)
- 管理ロールの変更(500 ページ)
- 管理ロール メンバ/管理者の変更(500 ページ)
- 管理タスクの変更(501 ページ)
- 管理ロール所有者のリセット(501 ページ)
- 管理ロールの表示(501 ページ)
- 管理ロール メンバ/管理者の表示(501 ページ)
- 管理タスクの表示(501 ページ)

管理ロールの作成

「管理ロールの作成」タスクでは、管理タスクを含むロールを作成します。

管理タスクの作成

「管理タスクの作成」タスクでは、管理ロールに含めることができるタスクを作成します。

管理ロールの削除

「管理ロールの削除」タスクでは、選択した管理ロールを環境から削除します。 このロールは現在使用されていません。

ロールを削除する前に、ロールからメンバを削除することを考慮してください。 管理ロールが削除された場合でも、ロール メンバは、その時点で使用中のロールのタスクを完了できます。 タスクが完了した後、そのタスクをもう一度実行することはできません。

管理タスクの削除

「管理タスクの削除」タスクでは、選択した管理タスクを削除します。

注: ユーザがタスクを実行している間にタスクが削除された場合でも、ユーザはそのタスクを完了できます。

管理ロールの変更

[管理ロールの変更]タスクでは、選択した管理ロールの有効または無効ステータスなどのプロパティを変更します。

ロールはすぐに使用できるように有効にしたり、まだロールを使用できない場合は無効にすることができます。 無効にしたロールは、管理者に割り当てることができますが、ユーザが所有するロールのリストには表示されません。

管理ロールを変更する場合は以下の点に注意してください。

- ロール メンバがロールのタスクを実行している間にロールが変更された場合でも、ロール メンバはタスクを完了できます。
- CA Identity Manager は、[管理ロールの変更]タスクを使用したロール所有者権限の変更について、別個のイベントは生成されません。

管理ロール メンバ/管理者の変更

「管理ロール メンバ/管理者の変更」タスクでは、選択した管理ロールのメンバまたは管理者を追加または削除します。 このタスクを実行する場合、メンバの管理または管理者の管理の権限を持つ任意の管理ロールを選択できます。

管理タスクの変更

「管理タスクの変更」タスクでは、選択した管理タスクを変更します。

管理ロール所有者のリセット

「管理ロール所有者のリセット」タスクでは、選択した管理ロールの所有者が誰かを制御する所有者ルールを再定義します。 所有者はロールを変更できます。

管理ロールの表示

「管理ロールの表示」タスクでは、選択した管理ロールの特性を表示します。

管理ロール メンバ/管理者の表示

「管理ロール メンバ/管理者の表示」タスクでは、選択した管理ロールのすべてのメンバまたは管理者のリストを表示します。

メンバの管理または管理者の管理の権限を持つ任意のロールを選択できます。

管理タスクの表示

「管理タスクの表示」タスクでは、選択した管理タスクの特性を表示します。

注: 「マイ サブミット済みタスクの表示」タスクを使用するには、タスクの永続性データベースを有効にする必要があります。 サポートが必要な場合は、Identity Manager システム管理者にご相談ください。

認証

「認証」カテゴリを使用して、ユーザ認証プロセスを管理します。 このカテゴリには、以下のタスクがあります。

- 認証プロセスの開始 (501 ページ)
- 認証プロセスの終了 (502 ページ)
- 認証アラーム通知の送信 (502 ページ)
- 最終認証アラーム通知の送信 (502 ページ)

認証プロセスの開始

「認証プロセスの開始」タスクでは、認証が必要なユーザを選択できます。 ユーザを選択すると、Identity Manager によってユーザの認証が「要認証」に設定され、該当する認証者に認証を保留していることを通知する電子メールが送信されます。

認証プロセスの終了

「認証プロセスの終了」タスクでは、認証されていないユーザを無効にし、該当する認証者に通知します。

認証アラーム通知の送信

「認証アラーム通知の送信」タスクでは、認証者に認証を保留していることを通知する電子メールを送信します。

最終認証アラーム通知の送信

「最終認証アラーム通知の送信」タスクは、「認証アラーム通知の送信」(502 ページ)タスクに類似しますが、今後は認証者にアラーム通知が送信されないことを通知する電子メールを送信します。

グループ

「グループ」カテゴリを使用して、グループを作成または管理します。 このカテゴリには、以下のタスクがあります。

- グループの作成(502 ページ)
- グループの削除(503 ページ)
- グループの変更(503 ページ)
- グループ メンバの変更(503 ページ)
- グループの表示(504 ページ)

グループの作成

「グループの作成」タスクでは、現在の組織内にグループを作成します。 このタスクを実行すると、以下のことを行えます。

- プロファイル情報の提供
- グループを作成する対象組織の指定
- 現在の組織に存在するユーザのリストからの選択による、管理者および静的メンバの割り当て

このタスクを実行すると、以下のタブが表示されます。

- ［メンバ］-- 静的メンバをグループに追加します。「グループの変更」タスクのある組織にプロファイルが存在するメンバを選択します。
- ［管理者］-- グループの管理者を追加します。「グループの変更」タスクのある組織にプロファイルが存在するグループ管理者を選択します。

  ［管理者］タブで、ユーザおよびグループを管理者として指定できます。 グループを指定すると、そのグループの管理者が、変更対象のグループの管理者になります。指定するグループのメンバには、作成対象のグループを管理する権限がありません。

注: ［動的グループ クエリ］フィールドは、グループの directory.xml ファイルにこのフィールドが存在する場合でも、「グループの作成」タスクやその他のグループ関連タスクには含まれません。［動的グループ クエリ］フィールドは、関連付けられたプロファイル画面を編集してタスクに含めます。

グループの削除

「グループの削除」タスクでは、現在の組織から選択したグループを削除します。

グループの変更

「グループの変更」タスクでは、選択したグループのプロファイル、グループ管理者のリスト、または静的メンバのリストを変更します。

注: グループを管理者として指定した場合は、そのグループの管理者のみが変更対象のグループを管理できます。 管理者グループのメンバには、変更対象のグループを管理する権限がありません。

グループ メンバの変更

「グループ メンバの変更」タスクでは、静的メンバをグループに追加、またはグループから削除します。 グループ管理者を追加または削除するには、「グループの変更」タスクを使用します。

グループの表示

「グループの表示」タスクでは、グループのプロファイル、管理者およびメンバを表示します。

このタスクを実行すると、以下のタブが表示されます。

- [メンバ]-- グループのすべての静的メンバ(ユーザおよびグループ)のリストを表示します。
- [管理者]-- グループ管理者のリストを表示します。

  グループが管理者として表示された場合は、そのグループの管理者であるユーザのみが表示対象のグループを管理できます。 管理者グループのメンバには、表示対象のグループを管理する権限がありません。

組織

「組織」カテゴリは、組織を含む LDAP ディレクトリまたはリレーショナル データベースであるユーザ ストアとして使用します。 このカテゴリには、組織の作成または管理に使用する以下のタスクがあります。

- 組織の作成(504 ページ)
- 組織の削除(504 ページ)
- 組織の変更(504 ページ)
- 組織の表示(504 ページ)

組織の作成

「組織の作成」タスクでは、選択した組織に下位組織を作成します。

組織の削除

「組織の削除」タスクでは、選択した組織を削除します。 組織内のすべてのユーザおよびグループも削除されます。

組織の変更

「組織の変更」タスクでは、選択した組織を変更します。

組織の表示

「組織の表示」タスクでは、選択した組織の特性を表示します。

ポリシー

「ポリシー」カテゴリを使用して、アイデンティティ ポリシー セットおよびパスワード ポリシーを管理します。 このカテゴリには、以下のタスクがあります。

- アイデンティティ ポリシー セットの作成 (505 ページ)
- アイデンティティ ポリシー セットの削除 (505 ページ)
- アイデンティティ ポリシー セットの変更 (505 ページ)
- アイデンティティ ポリシー セットの表示 (506 ページ)
- ユーザの同期化 (506 ページ)
- パスワード ポリシーの作成 (506 ページ)
- パスワード ポリシーの削除 (506 ページ)
- パスワード ポリシーの変更 (506 ページ)
- パスワード ポリシーの表示 (506 ページ)

アイデンティティ ポリシー セットの作成

「アイデンティティ ポリシー セットの作成」タスクでは、ユーザが特定の条件やルールを満たした場合に発生する、一連のビジネス変化を設定できます。 ビジネス変化には、以下のものがあります。

- プロビジョニング ロールなどのロールの割り当ておよび取り消し
- グループ メンバシップの割り当てまたは取り消し
- ユーザ プロファイルの属性の更新

アイデンティティ ポリシー セットの削除

「アイデンティティ ポリシー セットの削除」タスクでは、選択したポリシー セットを削除します。 アイデンティティ ポリシー セットを削除すると、関連付けられたアイデンティティ ポリシーが削除されます。

アイデンティティ ポリシー セットの変更

「アイデンティティ ポリシー セットの変更」タスクでは、選択したポリシー セットを変更します。

アイデンティティ ポリシー セットの表示

「アイデンティティ ポリシー セットの表示」タスクでは、選択したポリシー セットの以下に示す特性を表示します。

- アイデンティティ ポリシー セットの名前、カテゴリ、および説明などの基本情報
- セットに含まれるアイデンティティ ポリシー
- セットの所有者ポリシー

ユーザの同期化

「ユーザの同期化」タスクでは、アイデンティティ ポリシーと共に選択したユーザを同期化します。

[ユーザの同期化]タスクには、以下のタブが含まれます。

- [現在一致しているポリシー]-- 同期化の実行時にユーザに適用されるアイデンティティ ポリシーのリストを表示します。
- [すでに適用されているポリシー]-- すでにユーザに適用されているアイデンティティ ポリシーのリストを表示します。
- [同期化サマリ]-- ユーザに適用されているすべてのアイデンティティ ポリシーおよびそれらのポリシーに対する変更アクションを表示します。

パスワード ポリシーの作成

「パスワード ポリシーの作成」では、パスワードの作成方法、およびその有効期限を決定する一連のルールおよび制限を設定できます。

パスワード ポリシーの削除

「パスワード ポリシーの削除」タスクでは、選択したパスワード ポリシーを削除します。

パスワード ポリシーの変更

「パスワード ポリシーの変更」タスクでは、選択したパスワード ポリシーを変更します。

パスワード ポリシーの表示

「パスワード ポリシーの表示」タスクでは、選択したパスワード ポリシーの特性を表示します。

プロビジョニング ロール

「プロビジョニング ロール」カテゴリを使用して、ユーザに関連付けることができるプロビジョニング ロールを作成し、管理します。 このカテゴリには、以下のタスクがあります。

- プロビジョニング ロールの作成(507 ページ)
- プロビジョニング ロールの削除(507 ページ)
- プロビジョニング ロールの変更(507 ページ)
- プロビジョニング ロール メンバ/管理者の変更(507 ページ)
- プロビジョニング ロール所有者のリセット(508 ページ)
- プロビジョニング ロールの表示(508 ページ)
- プロビジョニング ロール メンバ/管理者の表示(508 ページ)

プロビジョニング ロールに割り当てる所有者ポリシーを作成

[プロビジョニング ロールに割り当てる所有者ポリシーを作成]では、誰がロールを変更できるかを制御する所有者ルールを定義します。 複数のプロビジョニング ロールを選択して、すべてのロールに適用される所有者ルールを定義することができます。

プロビジョニング ロールの作成

「プロビジョニング ロールの作成」タスクでは、ユーザがそのメンバまたは管理者になることができるプロビジョニング ロールを作成します。

プロビジョニング ロールの削除

「プロビジョニング ロールの削除」タスクでは、環境からロールを削除します。

プロビジョニング ロールの変更

[プロビジョニング ロールの変更]では、選択したプロビジョニング ロールを変更します。

注: CA Identity Manager では、[プロビジョニング ロールの変更]タスクを使用して行われたロールの所有者権限の変更について、別個のイベントは生成されません。

プロビジョニング ロール メンバ/管理者の変更

「プロビジョニング ロール メンバ/管理者の変更」タスクでは、選択したプロビジョニング ロールのメンバまたは管理者を追加または削除します。

プロビジョニング ロール所有者のリセット

「プロビジョニング ロール所有者のリセット」タスクでは、選択したプロビジョニング ロールの所有者が誰かを制御する所有者ルールを再定義します。 所有者はロールを変更できます。

プロビジョニング ロールの表示

「プロビジョニング ロールの表示」タスクでは、選択したプロビジョニング ロールの特性を表示します。

プロビジョニング ロール メンバ/管理者の表示

「プロビジョニング ロール メンバ/管理者の表示」タスクでは、選択したプロビジョニング ロールのメンバおよび管理者のリストを表示します。

レポート

[レポート]カテゴを使用して、レポートを表示および管理できます。 このカテゴリには、以下のタスクがあります。

タスク	説明
レポート反復スケジュールの管理	このタスクでは、レポート反復スケジュールを表示、変更、または削除できます。
レポートのリクエスト	このタスクでは、レポートのインスタンスを作成できます。
マイ レポートの表示	このタスクでは、生成したレポートを表示できます。
マイ レポートの削除	このタスクでは、生成したレポートをどれでも削除できます。
レポート オプションの設定	このタスクでは、レポート生成のオプションを管理できます。 たとえば、各レポート タイプで生成できるレポートの数を制限することが可能です。

システム

「システム」カテゴリを使用して、処理のためにサブミットされたタスクおよびイベントのステータスを監視します。 このカテゴリには、以下のタスクがあります。

タスク	説明
JDBC 接続管理	このタスクは、Identity Manager 内で、データベース

タスク	説明
	サーバ接続の詳細設定に使用されます。
［ロジカル アトリビュート］	このタスクを使用して、以下のものを作成できます。 ■ ロジカル アトリビュート -- タスク画面上でユーザに表示されるデータですが、データ ストアには書き込まれません。 ■ ロジカル アトリビュート ハンドラ -- ロジカル アトリビュート データを処理する Java オブジェクト
セレクト ボックス データ	このタスクでは、ユーザ コンソールの選択式コントロールのオプションを XML ファイルから入力できます。
Bulk Loader	［Bulk Loader］を使用して、同時に多数の管理対象オブジェクトを操作するために使用するフィーダ ファイルをアップロードできます。
サブミット済みタスクの表示	このタスクでは、現在の環境で処理のためにサブミットされたタスクのステータスを表示します。 **注**: このタスクは TEWS（Task Execution Web Service）では使用できません。

論理属性ハンドラの作成

「論理属性ハンドラの作成」タスクでは、論理属性ハンドラを作成します。これは、論理属性データを処理する Java オブジェクトで、論理属性 API を使用して作成します。 たとえば、このタスクを実行して、ユーザ ストアにある物理属性データを論理属性データに変換してタスク画面に表示できるようにするための論理属性ハンドラを作成できます。

ロジカル アトリビュート ハンドラの削除

「論理属性ハンドラの削除」タスクでは、既存の論理属性ハンドラを削除できます。 論理属性ハンドラを削除すると、論理属性データを処理する Java オブジェクトが削除されますが、データ ストアは影響を受けません。

ロジカル アトリビュート ハンドラの変更

「ロジカル アトリビュート ハンドラの変更」タスクでは、既存のロジカル アトリビュート ハンドラを変更し、更新できます。

論理属性ハンドラの表示

「論理属性ハンドラの表示」タスクでは、既存の論理属性ハンドラのプロパティを表示できます。

ユーザ

「ユーザ」カテゴリを使用して、ユーザ アカウントを作成または管理します。 このカテゴリには、以下のタスクがあります。

- ユーザの作成(510 ページ)
- 作業アイテムの委任(510 ページ)
- ユーザの削除(510 ページ)
- ユーザの有効化/無効化(511 ページ)
- ユーザの変更(511 ページ)
- ユーザ パスワードのリセット(511 ページ)
- ユーザの表示(512 ページ)

ユーザの作成

「ユーザの作成」タスクでは、Identity Manager アカウントを作成します。 ユーザを作成する場合、以下の操作を実行できます。

- ユーザのプロファイルを作成する組織の選択
- 割り当てるロールの管理者である場合、アクセス ロールまたは管理ロールの割り当て
- グループの管理者である場合、そのグループへのユーザの割り当て

注: 変更を行えない特定のタブは表示されません。 たとえば、グループ管理者でない場合は、[グループ]タブは表示されません。

作業アイテムの委任

作業アイテムの委任では、ユーザが委任マネージャ ロールを使用して他のユーザ(委任者)の代理として役割を果たし、作業アイテムの承認タスクをもう 1 人のユーザ(委任先)に委任できます。

ユーザの削除

「ユーザの削除」タスクでは、選択したユーザ アカウントを Identity Manager から削除します。 ユーザが管理者であるか、エンド ユーザであるかを問いません。

ユーザの有効化/無効化

「ユーザの有効化/無効化」タスクでは、ユーザ アカウントが有効かどうかを制御します。

ユーザの変更

「ユーザの変更」タスクでは、ユーザ アカウントを変更します。 変更を行うと、自分が管理者であるロールおよびグループのユーザのプロファイルとメンバシップが変更されます。

ユーザに割り当てられた他のロールや、ユーザがロール制約を満たし、受信した他のロールも参照できます。

ユーザのエンドポイント アカウントの変更

[ユーザのエンドポイント アカウントの変更]フィールドを使用すると、選択したアカウントに対して以下のアクションを実行します。

- アカウントの現在のステータスの取得
- ユーザへのアカウントの割り当て
- ユーザのアカウントの割り当て解除
- アカウントの一時停止
- 一時停止されたアカウントの再開
- アカウントのロック解除
- アカウントのパスワードを変更
- アカウントの削除

この変更は、タスクのサブミット時に有効になります。 タスクで実行するアクションを参照するには、[リクエストされたアクションのプレビュー]をクリックします。

ユーザ パスワードのリセット

「ユーザ パスワードのリセット」タスクでは、現在のパスワードを入力することなく、ユーザアカウントのパスワードを変更できます。

ユーザの表示

「ユーザの表示」タスクでは、ユーザのプロファイル、ロール、およびグループを表示します。 ユーザが管理者であるか、エンド ユーザであるかを問いません。 このタスクでは、ユーザに割り当てられたロールや、ユーザがロールの制約に適合することにより受信したロールをすべて表示できます。

注: 「システム マネージャ」ロールを使用すると、環境内の任意のユーザを表示できます。

ユーザのエンドポイント アカウントの表示

[ユーザのエンドポイント アカウントの表示]を使用すると、選択したユーザの各エンドポイント アカウントのステータスを表示できます。

デフォルトの管理ロール

以下のセクションは、Identity Manager でインストールされたデフォルトのロールを定義します。

- アクセス ロール マネージャ(513 ページ)
- 管理ロール マネージャ(513 ページ)
- 認証マネージャ(514 ページ)
- 認証プロセス マネージャ(514 ページ)
- 委任マネージャ(514 ページ)
- グループ マネージャ(515 ページ)
- 組織マネージャ(515 ページ)
- パスワード マネージャ(516 ページ)
- プロビジョニング ロール マネージャ(516 ページ)
- プロビジョニング同期マネージャ(516 ページ)
- セキュリティ マネージャ(517 ページ)
- 自己委任(517 ページ)
- 自己マネージャ(517 ページ)
- システム マネージャ(518 ページ)
- ユーザ マネージャ(518 ページ)

注: デフォルトのロールを変更した場合は、[管理ロールの表示]タスクを使用してロールに含まれるタスクを参照できます。

アクセス ロール マネージャ

アクセス タスクとロールを作成、変更、および削除し、ロールのメンバまたは管理者を決定します。 このロールには、以下のタスクがあります。

アクセス ロール管理	
■ アクセス ロールの作成	■ アクセス タスクの変更
■ アクセス タスクの作成	■ アクセス ロールの表示
■ アクセス ロールの削除	■ アクセス ロール メンバ/管理者の表示
■ アクセス タスクの削除	■ アクセス タスクの表示
■ アクセス ロールの変更	
■ アクセス ロールの変更 メンバ/管理者	

注: このロールでは重要な権限が与えられます。 このロールを割り当てる管理者の人数を制限できます。

管理ロール マネージャ

管理タスクとロールを作成、変更、および削除し、ロールのメンバまたは管理者を決定します。 このロールには、以下のタスクがあります。

管理ロールの管理	
■ 管理ロールの作成	■ 管理ロール メンバ/管理者の変更
■ 管理タスクの作成	■ 管理タスクの変更
■ 管理ロールの削除	■ 管理ロールの表示
■ 管理タスクの削除	■ 管理ロール メンバ/管理者の表示
■ 管理ロールの変更	■ 管理タスクの表示

注: このロールでは重要な権限が与えられます。 このロールを割り当てる管理者の人数を制限できます。

認証プロセス マネージャ

認証対象のユーザを選択し、認証者に認証を保留していることを通知するアラーム通知を送信し、認証プロセスを終了して認証されていないユーザのアカウントを無効にします。

このロールには、以下のタスクがあります。

認証
■ 認証プロセスの開始
■ 認証プロセスの終了
■ 認証アラーム通知の送信
■ 最終認証アラーム通知の送信

認証マネージャ

ユーザのロールを認証または拒否することにより、ユーザ権限の認証を行います。

このロールには、以下のタスクがあります。

ユーザ管理
■ ユーザの認証

委任マネージャ

委任マネージャは他のユーザ(委任者)の代理として役割を果たし、作業アイテムの承認タスクをもう 1 人のユーザ(委任先)に委任できます。

このロールにはすべてのユーザにわたるスコープがあります。

このロールには以下のタスクが含まれます。

作業アイテムの委任(510 ページ)

グループ マネージャ

管理者が管理権限を持つ組織内でグループを作成、変更、および削除し、グループ管理者を割り当てます。 このロールには、以下のタスクがあります。

グループ管理

- グループの作成
- グループの削除
- グループの変更
- グループの表示

組織マネージャ

グループ、ユーザ、管理者、および組織の作成、変更、削除 このロールには、以下のタスクがあります。

組織管理

- 組織の作成
- 組織の削除
- 組織の変更
- 組織の表示

グループ管理

- グループの作成
- グループの削除
- グループの変更
- グループの表示

ユーザ管理

- ユーザの作成
- ユーザの削除
- ユーザの有効化/無効化
- ユーザの変更
- ユーザ パスワードのリセット
- ユーザの表示

管理ロールの管理

- 管理ロール メンバ/管理者の変更
- 管理ロールの表示
- 管理ロール メンバ/管理者の表示

アクセス ロール管理

- アクセス ロール メンバ/管理者の変更
- アクセス ロールの表示
- アクセス ロール メンバ/管理者の表示

パスワード マネージャ

ユーザ パスワードをリセットします。 このロールは、ヘルプ デスクの担当者にとって便利です。 このロールには、以下のタスクがあります。

ユーザ管理

- ユーザ パスワードのリセット
- ユーザの表示

プロビジョニング ロール マネージャ

管理タスクとロールを作成、変更、および削除し、ロールのメンバまたは管理者を決定します。 このロールには、以下のタスクがあります。

プロビジョニング ロール

- プロビジョニング ロールの作成
- プロビジョニング ロールの削除
- プロビジョニング ロールの変更
- プロビジョニング ロール メンバ/管理者の変更
- プロビジョニング ロールの表示
- プロビジョニング ロール メンバ/管理者の表示

プロビジョニング同期マネージャ

Identity Manager で使用されるユーザ ストアを更新し、プロビジョニング サーバで行われたユーザ変更を反映します。 このロールは Identity Manager によって内部で使用されます。 このロールには、以下のタスクがあります。

プロビジョニング同期

- プロビジョニングによるユーザ作成
- プロビジョニングによるユーザの有効化/無効化
- プロビジョニングによるユーザ変更

セキュリティ マネージャ

ユーザのアカウントを有効または無効にし、ユーザ パスワードをリセットします。 このロールには、以下のタスクがあります。

ユーザ管理

- ユーザの有効化/無効化
- ユーザ パスワードのリセット
- ユーザの表示

自己委任

自己委任(委任者)は、別のユーザ(代行者)が委任者の作業リスト内のタスクを承認できるよう指定できます。

このロールにはすべてのユーザにわたるスコープがあります。

このロールには以下のタスクが含まれます。

不在時(498 ページ)

自己マネージャ

パスワードなど自分のプロファイルの変更、自己登録グループへのメンバシップ要求、および自分のロールの表示を行います。 このロールには、以下のタスクがあります。

マイ アカウント

- マイ パスワードの変更
- マイ グループの変更
- マイ プロファイルの変更
- マイ ロールの表示
- マイ サブミット済みタスクの表示
- マイ ワーク リストの表示

System Manager

環境内で初期の最上位管理者、タスク、およびロールを設定します。 ロールには、以下のデフォルトの管理タスクのすべてが含まれます。

組織管理

- 組織の作成
- 組織の削除
- 組織の変更
- 組織の表示

ユーザ管理

- ユーザの作成
- ユーザの削除
- ユーザの変更
- ユーザの表示

システム管理

- サブミット済みタスクの表示

アクセス ロール管理

- アクセス ロール所有者のリセット

管理ロールの管理

- 管理ロールの作成
- 管理タスクの作成
- 管理ロールの削除
- 管理タスクの削除
- 管理ロールの変更
- 管理タスクの変更
- 管理ロール所有者のリセット
- 管理ロールの表示
- 管理タスクの表示

ユーザ マネージャ

組織内でユーザを作成、変更、および削除し、ロールおよびグループのメンバシップを制御します。 このロールには、以下のタスクがあります。

ユーザ管理

- ユーザの作成
- ユーザの削除
- ユーザの変更
- ユーザの表示

グループ管理

- グループ メンバの変更

アクセス ロール管理

- アクセス ロール メンバ/管理者の変更
- アクセス ロール メンバ/管理者の表示

デフォルトのワークフロー承認ロール

各ロールが承認権限を持つワークフロー承認ロールおよびタスクを、以下の表に示します。

注: ロールやグループ メンバシップの承認タスクでは、ロールまたはグループのメンバや管理者の変更を承認します。

承認ロール名	承認のタスク
アクセス ロール メンバシップ承認者	■ アクセス ロール メンバシップ変更を承認
管理ロール メンバシップ承認者	■ 管理ロール メンバシップ変更を承認
グループ承認者	■ グループ作成を承認 ■ グループ削除を承認
グループ メンバシップ承認者	■ グループ メンバシップ変更を承認
組織承認者	■ 組織作成を承認 ■ 組織削除を承認 ■ 組織変更を承認
プロビジョニング ロール メンバシップ承認者	■ プロビジョニング ロール メンバシップ変更を承認
自己登録承認者	■ 自己登録の承認
ユーザ承認者	■ ユーザ作成を承認 ■ ユーザ削除を承認 ■ ユーザ変更を承認

索引

_

_bcc 電子メール テンプレート オブジェクト - 435
_cc 電子メール テンプレート オブジェクト - 435
_encoding 電子メール テンプレート オブジェクト - 435
_eventContextInformation 電子メール テンプレート オブジェクト - 435
_subject 電子メール テンプレート オブジェクト - 435
_taskContextInformation 電子メール テンプレート オブジェクト - 435
_template 電子メール テンプレート オブジェクト - 435
_to 電子メール テンプレート オブジェクト - 435
_util 電子メール テンプレート オブジェクト - 435

<

<% %> HTML タグの拡張 - 434
<%= %> HTML タグの拡張 - 434

1

1 回のみ適用の設定 - 197

A

access roles
    アクセス ロールの表示 - 503, 510
ACCESSROLE オブジェクト タイプ - 435
ACCESSTASK オブジェクト タイプ - 435
account synchronization
    説明 - 178
Active Directory
    sAMAccountName の要件 - 68
    タスク画面の作成 - 68
Active Directory のグループ タイプとスコープ - 68
add() - 435
admin roles
    管理ロールの削除 - 502
    管理ロールの作成 - 502
    管理ロールの変更 - 502
    管理ロール メンバ/管理者の表示 - 503
    管理ロール メンバ/管理者の変更 - 502
Admin Roles category
    説明 - 501
admin tasks
    Active Directory の注意事項 - 68
    アクセス ロールの表示 - 503, 510
    管理タスクの削除 - 502
    管理タスクの作成 - 502
    管理タスクの表示 - 503
    管理タスクの変更 - 503
    管理ロールのカテゴリ - 501
    管理ロールの削除 - 502
    管理ロールの作成 - 502
    管理ロールの変更 - 502
    管理ロール メンバ/管理者の変更 - 502
    グループ カテゴリ - 504
    グループの削除 - 505
    グループの作成 - 504
    グループの表示 - 506
    グループの変更 - 505
    グループ メンバの変更 - 505
    サブミット済みタスクの表示 - 510
    システムのカテゴリ - 510
    組織のカテゴリ - 506
    組織の削除 - 506
    組織の作成 - 506
    組織の表示 - 506
    組織の変更 - 506
    電子メールへの挿入 - 447
    マイ グループの変更 - 500
    マイ サブミット済みタスクの表示 - 501
    マイ パスワードの変更 - 499
    マイ プロファイルの変更 - 500
    マイ ロールの表示 - 501
    ユーザの削除 - 512
    ユーザの作成 - 512
    ユーザの表示 - 514
    ユーザの変更 - 513
    ユーザの有効化/無効化 - 513
    ユーザ パスワードのリセット - 513
administrators
    電子メールへの挿入 - 435, 447
ADMINROLE オブジェクト タイプ - 435

ADMINTASK オブジェクト タイプ - 435
ADMIN 通知ルール - 435
API
  Identity Manager API からのメソッド継承 - 447
  電子メール テンプレート - 435
APPROVAL_STATUS_APPROVED - 435
APPROVAL_STATUS_REJECTED - 435

C

categories
  管理ロール - 501
  システム - 510
  組織 - 506
  デフォルト - 498
certification
  設定 - 294
  説明 - 293
  前提条件 - 295
  認証者の決定 - 296
  認証プロセスの開始 - 299
CertificationNonCertifiedActionCompletedNotification.tmpl - 429
CertificationNonCertifiedActionPendingNotification.tmpl - 429
CertificationRequiredFinalNotification.tmpl - 429
CertificationRequiredNotification.tmpl - 429
CertificationRequiredReminderNotification.tmpl - 429
certifiers
  指定 - 296
commonattribute
  User Manager Notification Adapter - 435
compliance
  ユーザ権限の認証 - 293
compliance check box
  アイデンティティ ポリシー セット - 196
configuring
  パスワードの構成要件 - 98
  ユーザ認証 - 294
context information
  イベント - 435
  タスク - 435
CreateProvisioningUserNotificationEvent.tmpl - 429
customizing Identity Manager
  電子メール テンプレート - 432
  電子メールの生成 - 427

D

defaultEvent.tmpl - 429
defaultTask.tmpl - 429
delegation
  ワークリスト - 501
description
  親グループ - 131
  静的グループ - 127
  動的グループ - 128
  ネスト グループ - 131
dynamic groups
  説明 - 128
  例 - 133

E

email notifications
  イベントに対する有効化 - 427
  環境に対する有効化 - 426
  生成されるタイミング - 423
  説明 - 423
  タスクの有効化 - 427
  電子メール テンプレート API - 435
  テンプレートからの生成 - 429
  ユーザ認証の設定 - 296
email templates
  From 値の変更 - 435
  JavaScript - 434
  Java 出力ストリーム - 449
  一連の - 450
  イベントの状態 - 429
  エレメント - 433
  オブジェクト - 435
  カスタマイズ - 432
  環境用の指定 - 451
  完了テンプレート - 429
  拒否テンプレート - 429
  承認済みのテンプレート - 429
  説明 - 432
  タグの拡張 - 434
  通知ルール - 435
  デフォルト - 429, 450
  展開 - 450
  電子メール テンプレート API - 435
  内容 - 429
  名前 - 451

場所 - 429
変数 - 434
保留中テンプレート - 429
email.properties - 435
emailTemplates ディレクトリ - 429, 450
Employee.tmpl の認証 - 429
events
状態, 電子メール テンプレート - 429
電子メール通知のトリガ - 427
電子メールのコンテキスト情報 - 435
電子メールへの挿入 - 435
ExposedEventContextInformation インターフェース - 435
ExposedEventContextInformation クラス - 435
ExposedTaskContextInformation インターフェース - 435

F

ForgottenPassword.tmpl - 429

G

getAdminFriendlyName() - 435
getAdministrator() - 435, 447
getAdminName() - 435
getAdminTask() - 435, 447
getApprovalStatus() - 435
getApprovalTime() - 435
getEventName() - 435
getExposedEventContexts() - 435
getNotifiers() - 435
getObjectOrganizationFriendlyName() - 435
getOrgName() - 435
getPassword() - 435
getPrimaryObjectName() - 435
getPrimaryObjectTypeName() - 435
getSecondaryObjectName() - 435
getSecondaryObjectTypeName() - 435
getTaskFriendlyName() - 435
getTaskName() - 435
GROUP オブジェクト タイプ - 435

I

Identity Manager
電子メール テンプレートのオブジェクト - 435
identity policies
作成 - 196
説明 - 193
ポリシー適用時のアクション - 202
ユーザの同期 - 206
identity policy sets
1 回のみ適用の設定について - 197
管理 - 205
計画 - 194
作成 - 195
説明 - 194
変更アクションの定義 - 202
ポリシー条件の定義 - 199
ポリシー適用/削除時のアクションの設定 - 199
例 - 210

J

Javadoc リファレンス - 450
Java 標準出力ストリーム - 449
JIAM
キャッシュ - 173
存続期間 - 173

M

managerattribute
User Manager Notification Adapter - 435
ModifyUserEvent.tmpl - 429

N

nested groups
作成 - 131
説明 - 131
例 - 133
notification templates
電子メール テンプレートを参照 - 432

O

organizations
組織の削除 - 506
組織の作成 - 506
組織の表示 - 506
組織の変更 - 506
電子メールへの追加 - 435
ORGANIZATION オブジェクト タイプ - 435
owner rules
アクセス ロール - 457
管理ロール - 39

P

password policies
　構成 - 98
　説明 - 94
　有効期限 - 104
passwords
　電子メールへの挿入 - 435
policy conditions
　アイデンティティ ポリシー セット - 199
protected tasks
　リスト - 81
public tasks
　リスト - 81

R

remote task submission
　Task Execution Web Service も参照 - 299

S

Self Registration.tmp - 429
self-service tasks
　概要 - 81
static groups
　作成 - 127
　説明 - 127
　例 - 133
System category
　説明 - 510

T

task execution
　リモート タスクのサブミット - 299
Task Execution Web Service
　説明 - 299
task screens
　Active Directory の注意事項 - 68
　sAMAccountName の追加 - 68
templates for email messages
　電子メール テンプレートを参照 - 432

U

user interface
　デフォルト カテゴリ - 498
User Manager Notification Adapter - 435
user synchronization
　アイデンティティ ポリシー - 206
　確認 - 208
　自動同期 - 207
　手動同期 - 208
USER_MANAGER 通知ルール - 296, 435
users
　アイデンティティ ポリシーとの同期 - 206
　権限の認証 - 293
　ユーザの削除 - 512
　ユーザの作成 - 512
　ユーザの表示 - 514
　ユーザの変更 - 513
　ユーザの有効化/無効化 - 513
　ユーザ パスワードのリセット - 513
USER オブジェクト タイプ - 435
USER 通知ルール - 435

W

Web サービス Task Execution Web Service を参照 - 299

あ

アクションの追加/削除 - 28
アクセス ロールの表示 - 503, 510
アプリケーション機能と外部タスク - 70
暗黙的なメッセージ オブジェクト - 435

か

管理タスクの削除 - 502
管理タスクの作成 - 502
管理タスクの変更 - 503
完了テンプレート - 429
　情報の取得 - 435
管理ロールの削除 - 502
管理ロールの作成 - 502
管理ロールの変更 - 502
管理ロール メンバ/管理者の表示 - 503
管理ロール メンバ/管理者の変更 - 502
拒否テンプレート - 429
　情報の取得 - 435
groups
　グループの削除 - 505
　グループの作成 - 504
　グループの表示 - 506
　グループの変更 - 505
　グループ メンバの変更 - 505
グループの削除 - 505

グループの作成 - 504
グループの表示 - 506
グループの変更 - 505
グループ メンバの変更 - 505

さ

サブミット済みタスクの表示 - 510
承認済みのテンプレート - 429
    情報の取得 - 435
親グループ - 131
    説明 - 131
セッション プーリング - 174
組織のカテゴリ - 506
組織の削除 - 506
組織の作成 - 506
組織の表示 - 506
組織の変更 - 506

た

タスク
    デフォルト カテゴリ - 498
    電子メール通知のトリガ - 427
    電子メールへの挿入 - 435
    電子メール用のコンテキスト情報 - 435
    リモート タスクのサブミット - 299
通知ルール - 435
デフォルト タスク - 498
電子メール テンプレート API - 435
    Identity Manager API メソッドの継承 - 447
電子メール テンプレートの JavaScript - 434
電子メール テンプレートのオブジェクト - 435
電子メール テンプレートのタグ - 434
電子メール テンプレートの展開 - 450
電子メール テンプレートの変数 - 434
電子メールの承認ステータス - 435
電子メールのセカンダリ オブジェクト - 435
電子メールのプライマリ オブジェクト - 435
動的な電子メール メッセージ - 432

な

認証に対する電子メール通知の設定 - 296

は

パスワード同期 - 178
標準出力ストリーム - 449
ポリシー適用/削除時のアクション - 199, 202
保留中テンプレート - 429
    情報の取得 - 435

ま

マイ グループの変更 - 500
マイ サブミット済みタスクの表示 - 501
マイ パスワードの変更 - 499
マイ ロールの表示 - 501

や

ユーザ タスクの同期 - 208
ユーザの削除 - 512
ユーザの作成 - 512
[ユーザの認証]タスク - 300
ユーザの表示 - 514
ユーザの有効化/無効化 - 513
ユーザ パスワードのリセット - 513

ら

例
    アイデンティティ ポリシー セット - 210