CA Identity Manager™

設定ガイド

12.6.4

ca technologies

このドキュメント（組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。 本ドキュメントは、CA が知的財産権を有する機密情報であり、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、変更、開示、修正、複製することはできません。

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

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

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

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

本書の制作者は 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 © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

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。

CA Technologies 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®
- CA ディレクトリ
- CA User Activity Reporting
- CA Identity Governance

目次

第 1 章: CA Identity Manager 環境の概要 15

CA Identity Manager 環境コンポーネント 15
複数の CA Identity Manager 環境 17
CA Identity Manager 管理コンソール 18
CA Identity Manager 管理コンソールにアクセスする方法 18
CA Identity Manager 環境を作成する方法 19

第 2 章: サンプル CA Identity Manager 環境 21

サンプル CA Identity Manager 環境の概要 21
組織サポートを使用して NeteAuto サンプルを設定する方法 21
- NeteAuto の LDAP ディレクトリ構造 22
- NeteAuto 用のリレーショナル データベース 23
- NeteAuto 用の前提条件のソフトウェア 23
- NeteAuto 環境用のインストール ファイル 24
- NeteAuto 環境のインストール 25
- LDAP ユーザ ディレクトリの設定 25
- リレーショナル データベースの設定 26
- CA Identity Manager ディレクトリの作成 27
- NeteAuto CA Identity Manager 環境の作成 29

組織サポートなしで NeteAuto サンプルを設定する方法 32
- サンプル CA Identity Manager 環境の説明 32
- Neteauto 環境用のインストール ファイル 33
- NeteAuto 環境をインストールする方法 -- 組織サポートなし 34
- 前提条件のソフトウェア 35
- リレーショナル データベースの設定 35
- CA Identity Manager ディレクトリの作成 36
- NeteAuto CA Identity Manager 環境の作成 38

NeteAuto CA Identity Manager 環境の使用方法 39
- セルフサービス タスク管理 40
- ユーザの管理 43

追加機能の設定方法 48
グローバル ユーザ名に対する SiteMinder のログイン名の制限 48

第 3 章: LDAP ユーザ ストアの管理 49

CA Identity Manager ディレクトリ 49
CA Identity Manager ディレクトリを作成する方法 50
ディレクトリ構造 50
ディレクトリ設定ファイル 52
ディレクトリ設定テンプレートを選択する方法 53
CA Identity Manager にユーザ ディレクトリを説明する方法 55
ディレクトリ構成ファイルを設定する方法 56
ユーザ ディレクトリへの接続 56
Provider エレメント 57
ディレクトリ検索パラメータ 61
ユーザ、グループ、および組織管理対象オブジェクトの説明 62
管理対象オブジェクトの説明 63
属性の説明 68
Sensitive 属性の管理 74
CA Directory に関する考慮事項 80
Microsoft Active Directory に関する考慮事項 81
IBM Directory Server に関する考慮事項 81
Oracle Internet Directory に関する考慮事項 82
LDAP ユーザ用の汎用属性 82
ユーザの既知の属性 83
グループ汎用属性 86
組織の汎用属性 88
%ADMIN_ROLE_CONSTRAINT% 属性 89
汎用属性 の設定 89
ユーザ ディレクトリ構造の説明 90
階層的ディレクトリ構造を説明する方法 90
フラット ユーザ ディレクトリ構造を説明する方法 90
フラット ディレクトリ構造を説明する方法 90
組織をサポートしないユーザ ディレクトリを説明する方法 91
グループの設定方法 91
自己登録グループの設定 91
動的およびネスト グループの設定 92
グループの管理者としてのグループに対するサポートの追加 94
検証ルール 94
追加の CA Identity Manager ディレクトリのプロパティ 95
並べ替え順序の設定 95
オブジェクト クラスの検索 96
レプリケーション待機時間の指定 97

LDAP 接続設定の指定 98
ディレクトリ検索のパフォーマンスを改善する方法 99
大規模な検索のパフォーマンスを改善する方法 100
Sun Java System Directory Server ページング サポートの設定 102
Active Directory ページング サポートの設定 103

第 4 章: リレーショナル データベース管理 107

CA Identity Manager ディレクトリ 107
リレーショナル データベース用に CA Identity Manager を設定する場合の重要な注意事項 109
WebSphere 用の Oracle データ ソースの作成 110
CA Identity Manager ディレクトリを作成する方法 111
JDBC データ ソースを作成する方法 111
JBoss アプリケーション サーバ用の JDBC データ ソースの作成 111
WebLogic 用 JDBC データ ソースの作成 114
WebSphere ODBC データ ソース 115
SiteMinder と併用するために ODBC データ ソースを作成する方法 117
ディレクトリ設定ファイルでデータベースを説明する方法 118
ディレクトリ設定ファイルの変更 120
管理対象オブジェクトの説明 120
属性の説明を変更する方法 126
ユーザ ディレクトリへの接続 141
データベース接続の説明 142
SQL クエリ方式 145
リレーショナル データベースの汎用属性 147
ユーザの既知の属性 148
グループ汎用属性 151
%Admin_Role_Constraint% 属性 152
汎用属性 の設定 152
自己登録グループを設定する方法 153
検証ルール 154
組織管理 154
組織サポートをセット アップする方法 155
データベース内の組織サポートの設定 155
ルート組織の指定 156
組織用の汎用属性 156
組織階層を定義する方法 157
ディレクトリ検索のパフォーマンスを改善する方法 158
大規模な検索のパフォーマンスを改善する方法 158

第 5 章: CA Identity Manager ディレクトリ 161

CA Identity Manager ディレクトリを作成するための前提条件 161
ディレクトリの作成方法 162
ディレクトリ設定ウィザードを使用したディレクトリの作成 162
ディレクトリ設定ウィザードの起動 163
［Select Directory Template］画面 165
［Connection Details］画面 165
［Configure Managed Objects］画面 169
［Confirmation］画面 176
XML 設定ファイルを含むディレクトリの作成 177
プロビジョニング サーバ アクセスの有効化 179
CA Identity Manager ディレクトリの表示 182
CA Identity Manager ディレクトリ プロパティ 183
CA Identity Manager ディレクトリ プロパティ ウィンドウ 184
管理対象オブジェクト プロパティおよび属性を表示する方法 186
検証ルールセット 190
CA Identity Manager ディレクトリの設定を更新する方法 192
CA Identity Manager ディレクトリのエクスポート 192
CA Identity Manager ディレクトリの更新 193
CA Identity Manager ディレクトリの削除 194

第 6 章: CA Identity Manager 環境 195

CA Identity Manager 環境 195
CA Identity Manager 環境を作成するための前提条件 196
CA Identity Manager 環境の作成 198
CA Identity Manager 環境にアクセスする方法 203
プロビジョニング用の環境を設定する方法 204
インバウンド管理者の設定 204
プロビジョニング サーバへの環境の接続 206
プロビジョニング マネージャでの同期の設定 206
カスタム プロビジョニング ロールのインポート 208
［ユーザ パスワードのリセット］タスクのアカウントの同期化 208
Connector Xpress を使用してコネクタを作成および展開する手順 209
環境の管理 217
CA Identity Manager 環境プロパティの変更 217
環境設定 220
CA Identity Manager 環境のエクスポート 221
CA Identity Manager 環境のインポート 222

CA Identity Manager 環境の再起動 222
CA Identity Manager 環境の削除 223
設定の管理 224
Config Xpress のセットアップ 225
Config Xpress への環境のロード 226
ある環境から別の環境へのコンポーネントの移動 228
PDF レポートの公開 229
XML 設定の表示 230
ポリシー ルール評価の最適化 231
ロールおよびタスクの設定 232
ロールおよびタスクの設定のエクスポート 232
ロールおよびタスクの設定のインポート 233
動的エンドポイント用のロールおよびタスクを作成する方法 234
システム マネージャ アカウントの変更 234
CA Identity Manager 環境のステータスへのアクセス 236
CA Identity Manager 環境のトラブルシューティング 237

第 7 章: 詳細設定 239

監査 239
ビジネス ロジック タスク ハンドラ 240
［ユーザ パスワードのリセット］タスクの［パスワード］フィールドの自動クリア 241
イベント リスト 241
電子メール通知 242
イベント リスナ 242
アイデンティティ ポリシー 243
ロジカル アトリビュート ハンドラ 243
その他 244
通知ルール 245
組織セレクタ 245
プロビジョニング 246
Provisioning Directory 247
Enable Session Pooling 248
パスワード同期の有効化 248
属性マッピング 249
Inbound Mappings 249
Outbound Mappings 249
ユーザ コンソール 249
Web サービス 252
ワークフロー プロパティ 253

作業アイテムの委任 253
ワークフロー参加者リゾルバ 254
カスタム設定のインポート/エクスポート 254
Java 仮想マシン メモリ不足エラー 255

第 8 章: 監査 257

監査データ レポートの設定および生成方法 257
前提条件の確認 259
監査設定ファイルの変更 259
タスクの監査の有効化 264
レポートのリクエスト 265
レポートの表示 268
監査データベースのクリーンアップ 269

第 9 章: 実稼働環境 271

管理ロールおよびタスク定義を移行する方法 271
管理ロールおよびタスク定義をエクスポートする方法 272
管理ロールおよびタスク定義のインポート方法 272
ロールおよびタスクのインポートを確認する方法 273
CA Identity Manager スキンを移行する方法 273
実稼働環境での CA Identity Manager の更新 273
CA Identity Manager 環境を移行する方法 274
CA Identity Manager 環境をエクスポートする方法 275
CA Identity Manager 環境をインポートする方法 275
CA Identity Manager 環境の移行を確認する方法 276
JBoss の iam_im.ear の移行 276
WebLogic の iam_im.ear の移行 277
WebSphere の iam_im.ear の移行 278
ワークフロー プロセス定義の移行 279
プロセス定義のエクスポート 280
プロセス定義のインポート 280

第 10 章: CA Identity Manager ログ 283

CA Identity Manager で問題を追跡する方法 283
コンポーネントおよびデータ フィールドを追跡する方法 285

第 11 章: CA Identity Manager 保護 289

ユーザ コンソール セキュリティ 289
管理コンソール セキュリティ 290
追加の管理コンソール管理者の追加 291
管理コンソールのネイティブ セキュリティの無効化 292
SiteMinder を使用して管理コンソールを保護する 292
アップグレードの後の既存環境の保護 294
CSRF 攻撃からの保護 295

第 12 章: CA SiteMinder の統合 297

SiteMinder および CA Identity Manager 298
リソースが保護される方法 299
SiteMinder と CA Identity Manager の統合の概要 300
CA Identity Manager の SiteMinder ポリシー ストアの設定 305
リレーショナル データベースの設定 305
Sun Java Systems Directory Server または IBM Directory Server の設定 306
Microsoft Active Directory の設定 307
Microsoft ADAM の設定 308
CA Directory Server の設定 309
Novell eDirectory Server の設定 310
Oracle Internet Directory （OID）の設定 311
ポリシー ストアの確認 311
ポリシー ストアへの CA Identity Manager スキーマのインポート 312
SiteMinder4.x エージェント オブジェクトの作成 312
CA Identity Manager ディレクトリおよび環境のエクスポート 314
すべてのディレクトリおよび環境定義の削除 315
SiteMinder ポリシー サーバ リソース アダプタの有効化 316
ネイティブ CA Identity Manager フレームワーク認証フィルタの無効化 317
アプリケーション サーバの再起動 318
SiteMinder 用のデータ ソースの設定 318
ディレクトリ定義のインポート 319
環境定義の更新およびインポート 320
Web プロキシ サーバ プラグインのインストール 320
WebSphere 上へのプロキシ プラグインのインストール 321
JBoss 用のプロキシ プラグインのインストール 329
WebLogic でのプロキシ プラグインのインストール 333
SiteMinder エージェントと CA Identity Manager ドメインの関連付け 341
SiteMinder LogOffUrl パラメータの設定 342

トラブルシューティング 342
Windows DLL がありません 343
正しくない SiteMinder ポリシー サーバの場所 343
正しくない管理者名 344
不正な管理者シークレット 345
不正なエージェント名 346
不正なエージェント シークレット 346
CA Identity Manager 内にユーザ コンテキストはありません 347
環境をロード中にエラーが発生しました 349
CA Identity Manager ディレクトリまたは環境を作成できません 350
ユーザがログインできない 350
CA Identity Manager エージェント設定を設定する方法 351
SiteMinder の高可用性の設定 352
ポリシー サーバ接続設定の変更 352
ポリシー サーバの追加 353
負荷分散またはフェイルオーバの選択 354
既存の CA Identity Manager 展開からの SiteMinder の削除 355
SiteMinder 操作 355
カスタム認証方式を使用したユーザ クレデンシャルの収集 356
ポリシー ストアへのデータ定義のインポート 357
アクセス ロールを設定する方法 358
LogOff URI の設定 374
SiteMinder レルムのエイリアス 375
SiteMinder パスワードまたは共有シークレットの編集 377
認証と認可用の別のディレクトリを使用できるように、CA Identity Manager 環境の設定 378
LDAP ディレクトリ操作のパフォーマンスを改善する方法 380

付録 A: FIPS 140-2 準拠 381

FIPS の概要 381
通信 382
インストール 382
SiteMinder への接続 383
キー ファイル ストレージ 383
パスワード ツール 384
FIPS モード検出 386
暗号文形式 387
暗号化される情報 387
FIPS モードのログ記録 388

付録 B: CA Identity Manager 証明書を SHA-2 署名付き SSL 証明書で置き換える 389
便利なコマンド.....392

第 1 章: CA Identity Manager 環境の概要

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 環境コンポーネント (P. 15)
複数の CA Identity Manager 環境 (P. 17)
CA Identity Manager 管理コンソール (P. 18)
CA Identity Manager 管理コンソールにアクセスする方法 (P. 18)
CA Identity Manager 環境を作成する方法 (P. 19)

CA Identity Manager 環境コンポーネント

CA Identity Manager *環境*は、CA Identity Manager 管理者がユーザ、グループ、組織などのオブジェクトを管理できる管理ネームスペースのビューです。これらのオブジェクトは、関連付けられたロールとタスクのセットで割り当てられます。CA Identity Manager 環境では、ディレクトリが視覚的に表され、ディレクトリの管理を制御します。

単一ユーザ ストアは、複数の CA Identity Manager 環境 (P. 17)を関連付けて、ディレクトリの異なるビューを定義することができます。ただし、CA Identity Manager 環境は、1 つのユーザ ストアのみと関連付けられます。

CA Identity Manager 環境には以下のエレメントが含まれます。

Directory

CA Identity Manager にユーザ ストアを説明します。ディレクトリ エレメントには以下のものが含まれます。

- ユーザ、グループ、および組織などの管理対象オブジェクトを格納する、ユーザ ストアへのポインタ。
- 管理対象オブジェクトがディレクトリにどのように格納され、CA Identity Manager で表示されるのかを説明するメタデータ。

プロビジョニング ディレクトリ (オプション)

管理エンドポイントで追加アカウントを管理するためにプロビジョニング サーバに関連するデータを格納します。1 つのプロビジョニング ディレクトリのみを 1 つの環境に関連付けることができます。

注: プロビジョニング サーバまたはプロビジョニング ディレクトリの詳細については、「インストール ガイド」を参照してください。

ユーザ コンソール

CA Identity Manager 管理者が CA Identity Manager 環境内のタスクを実行できます。

タスクおよびロール定義

CA Identity Manager および他のアプリケーションでのユーザ権限を決定します。 これらのタスクおよびロール定義は、それらがユーザに割り当てることができる CA Identity Manager 環境で最初に使用できます。

ユーザ コンソールを使用したデフォルトのロールおよびタスクをカスタマイズできます。

セルフサービス

ユーザがカスタマ Web サイトなどのリソースにアクセスするために自分のアカウントを作成し、管理できます。セルフサービスでは、ユーザが現在のパスワードを忘れた場合に一時パスワードをリクエストすることもできます。

ワークフロー定義

CA Identity Manager には、ユーザ プロファイルの作成、ロールまたはグループへのユーザの割り当てなど、ユーザ管理タスクの承認および通知を自動化するデフォルトのワークフロー定義が含まれます。 各企業の要件をサポートするために CA Identity Manager ではデフォルトのワークフロー プロセスを変更できます。

スキン

CA Identity Manager ユーザ インターフェースの外観を決定します。

カスタム機能

CA Identity Manager API を使用して、ビジネス要件に合うように CA Identity Manager を変更できます。 *「Java のプログラミング ガイド」*を参照してください。

各 CA Identity Manager 環境では、1 人以上のシステム マネージャがユーザ コンソールを使用して、最初のロールおよびタスクをカスタマイズする必要があります。システム マネージャが最初のロールおよびタスクを作成したら、そのマネージャはその環境内のユーザに管理者権限を付与できます。これらのユーザはユーザ、グループ、および組織を管理する管理者になります。「管理ガイド」を参照してください。

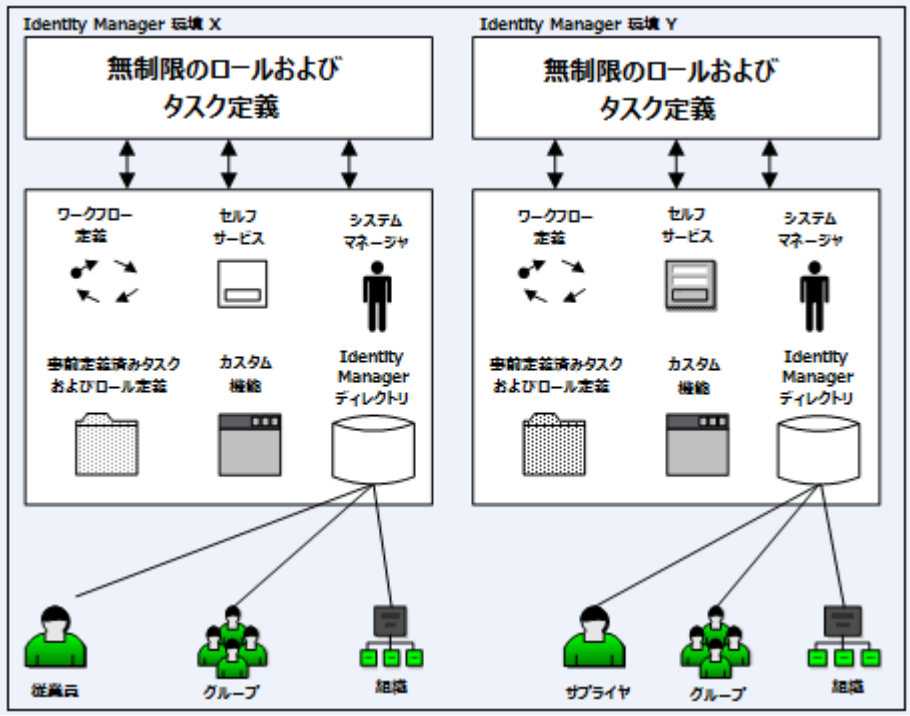
複数の CA Identity Manager 環境

ユーザが以下を行う場合は、複数の CA Identity Manager 環境を作成します。

追加のユーザ ストアの管理 -- 異なるタイプのユーザ ストアのユーザを管理できます。 たとえば、ユーザの会社が Sun Java System LDAP ディレクトリにユーザ プロファイルのすべてを格納します。 ユーザ情報を格納するために Oracle データベースを使用するパートナーと合弁事業を始めます。各ユーザのセットに異なる CA Identity Manager 環境を使用したい場合があります。

- 異なる LDAP オブジェクト クラスを使用したオブジェクトの管理 -- CA Identity Manager は LDAP ディレクトリを管理していることを考慮します。 同じディレクトリ内で、異なるオブジェクト クラスおよび属性と共に同じタイプのオブジェクトを管理できます。 たとえば、以下の図では、2 つのタイプのユーザが含まれるディレクトリを示しています。
  - 従業員（従業員 ID 番号を持つ）。
  - サプライヤ（サプライヤ番号で識別される）。

数式 1: 従業員とサプライヤが含まれるディレクトリがある 2 つの Identity Manager 環境の例を示す図



CA Identity Manager 管理コンソール

CA Identity Manager システム管理者として、ユーザの責任には以下のものが含まれます。

- CA Identity Manager ディレクトリの作成
- プロビジョニング ディレクトリの設定
- CA Identity Manager 環境の設定
- システム マネージャの割り当て
- 最初に使用するカスタム機能の有効化

CA Identity Manager 環境を設定するには、Web ベース アプリケーションである、管理コンソールを使用します。

管理コンソールは以下の 2 つのセクションに分かれています。

- ディレクトリ -- このセクションを使用して、CA Identity Manager にユーザ ストアを説明する、CA Identity Manager ディレクトリおよびプロビジョニング ディレクトリを作成し、管理します。
- 環境 -- このセクションを使用して、ディレクトリが視覚的に表され、ディレクトリの管理を制御する、CA Identity Manager 環境を作成し、管理します。

CA Identity Manager 管理コンソールにアクセスする方法

管理コンソールにアクセスするには、ブラウザで以下の URL を入力します。

http://*hostname:port*/iam/immanage

hostname

CA 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または IP アドレスを定義します。

注: ユーザが Internet Explorer 7 を使用して管理コンソールにアクセスしており、ホスト名に IPv6 アドレスが含まれる場合、管理コンソールの表示が正しくないことが想定されます。 この問題を防ぐには、完全修飾ホスト名または IPv4 アドレスを使用します。

ポート

アプリケーション サーバ ポートを定義します。

注: CA Identity Manager 用の高度な認証を提供するために Web エージェントを使用している場合は、ポート番号を指定する必要はありません。

注: 管理コンソールにアクセスするために使用するブラウザ内の Javascript を有効にします。

管理コンソールへのパス例：

- Geologic Weblogs の場合：

  http://myserver.mycompany.org:7001/iam/immanage

- JBoss の場合:

  http://myserver.mycompany.org:8080/iam/immanage

- WebSphere の場合:

  http://myserver.mycompany.org:9080/iam/immanage

CA Identity Manager 環境を作成する方法

CA Identity Manager 環境を作成するには、管理コンソールで以下の手順に従います。

1. ディレクトリ設定ウィザード (P. 162) を使用して、CA Identity Manager ディレクトリを作成します。
2. ご使用の環境にプロビジョニングが含まれる場合は、プロビジョニング ディレクトリを作成 (P. 179) するためにもう一度ディレクトリ設定ウィザードを使用します。
3. CA Identity Manager 環境を作成します。
4. 環境にアクセス (P. 203) して、環境が実行されていることを確認します。

第 2 章: サンプル CA Identity Manager 環境

このセクションには、以下のトピックが含まれています。

サンプル CA Identity Manager 環境の概要 (P. 21)
組織サポートを使用して NeteAuto サンプルを設定する方法 (P. 21)
組織サポートなしで NeteAuto サンプルを設定する方法 (P. 32)
NeteAuto CA Identity Manager 環境の使用方法 (P. 39)
追加機能の設定方法 (P. 48)
グローバル ユーザ名に対する SiteMinder のログイン名の制限 (P. 48)

サンプル CA Identity Manager 環境の概要

CA Identity Manager には、CA Identity Manager について学習し、テストするために使用できるサンプル環境が含まれています。

サンプル環境は NeteAuto という名前の自動車貿易会社に基づいています。NeteAuto 管理者は、CA Identity Manager を使用して、従業員、サプライヤ、および地域ディーラを管理します。

サンプル NeteAuto 環境を使用するユーザ ストア設定は以下のとおりです。

- 組織をサポートする LDAP ユーザ ストア
- 組織をサポートしない LDAP ユーザ ストア
- 組織をサポートするリレーショナル データベース ユーザ ストア
- 組織をサポートしないリレーショナル データベース ユーザ ストア

注: この環境にはプロビジョニング ディレクトリがないため、プロビジョニング機能は利用できません。

組織サポートを使用して NeteAuto サンプルを設定する方法

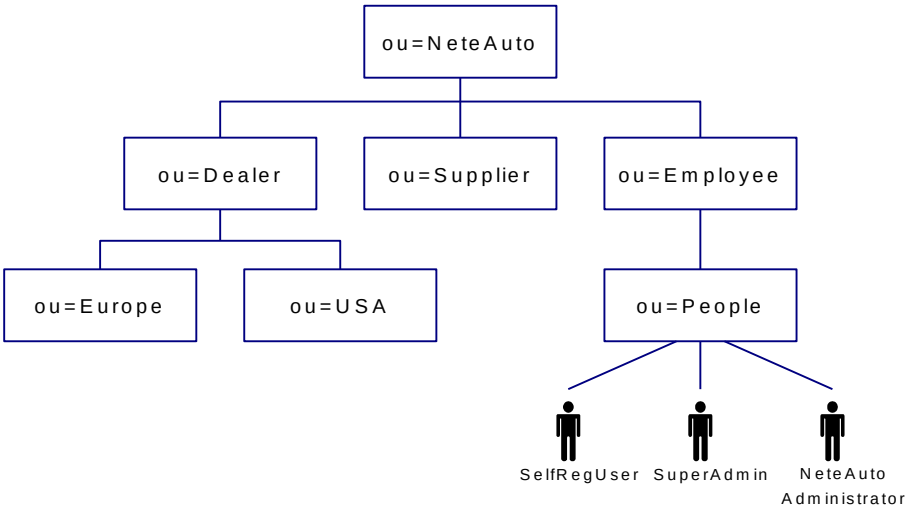
組織サポートを使用した NeteAuto サンプルの設定には、以下の手順が含まれます。

- 事前にインストールが必要なソフトウェアのインストール
- サンプル CA Identity Manager 環境のインストール
- LDAP ユーザ ディレクトリの設定
- リレーショナル データベースの設定

- CA Identity Manager ディレクトリの作成
- NeteAuto CA Identity Manager 環境の作成

NeteAuto の LDAP ディレクトリ構造

以下の図は、LDAP ディレクトリの NeteAuto サンプルについて説明します。



サンプル CA Identity Manager 環境には以下のユーザが含まれます。

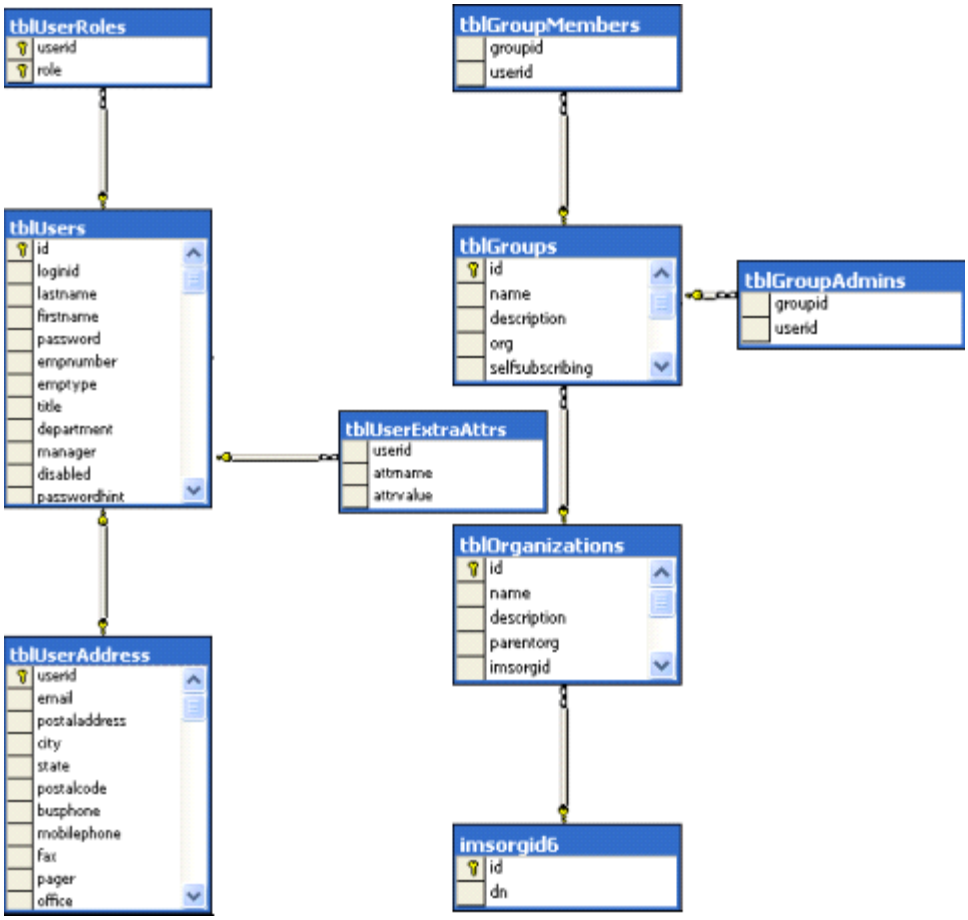
- Superadmin は、この CA Identity Manager 環境用のシステム マネージャ ロールを持つ管理者アカウントです。 superadmin として、デフォルト管理タスクをすべて実行できます。

  注: デフォルトの管理タスクについては、「管理ガイド」を参照してください。

- SelfRegUser は、この CA Identity Manager 環境用の自己登録を有効にするために CA Identity Manager が使用する管理者アカウントです。
- ユーザが NeteAuto 環境をインストールするときには、NeteAuto 管理者には権限がありません。ただし、「グループ マネージャ ロールの割り当て」で説明されるように、グループ マネージャをユーザ ロールとして割り当てることができます。

NeteAuto 用のリレーショナル データベース

以下の図は、組織テーブルを含む NeteAuto サンプルのリレーショナル データベースを示します。



NeteAuto 用の前提条件のソフトウェア

NeteAuto CA Identity Manager 環境には以下の前提条件があります。

- 「インストール ガイド」の説明に従って CA Identity Manager をインストールします。 必ず CA Identity Manager 管理ツールをインストールしてください。
- Sun Java システム（Sun ONE または iPlanet） ディレクトリ サーバまたは Microsoft SQL Server データベースへのアクセス権が必要です。

NeteAuto 環境用のインストール ファイル

CA Identity Manager には、サンプル CA Identity Manager 環境をセットアップするために使用できるファイルのセットが含まれています。CA Identity Manager 環境は、CA Identity Manager 管理者がユーザ、グループ、組織などのオブジェクトを管理できる管理ネームスペースのビューです。 これらのオブジェクトは、関連付けられたロールとタスクのセットと共に管理されます。CA Identity Manager 環境では、ディレクトリが視覚的に表され、ディレクトリの管理を制御します。

サンプル CA Identity Manager 環境には以下のものが含まれます。

- ユーザや組織などのサンプル オブジェクト
- ロール、タスク、および画面定義

  ユーザやグループなど、タブをクリックするときに、ユーザ コンソールに表示されるタスク。 割り当てられたロールに基づいて、ユーザがログインするときに関連タスクが表示されます。

  注: ロールおよびタスクの詳細については、「管理ガイド」を参照してください。
- NeteAuto ユーザ用のユーザ コンソールをカスタマイズするサンプル スキン。
- CA Identity Manager ディレクトリを作成するために使用するディレクトリ設定ファイル。

サンプル CA Identity Manager 環境を作成するためのファイルは以下の場所にインストールされます。

admin_tools¥samples¥NeteAuto

このパスで、*admin_tools* は管理ツールを示します。 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

NeteAuto 環境のインストール

NeteAuto 環境をインストールするには、以下のプロセスを実行します。

次の手順に従ってください:

1. 前提条件のソフトウェアがインストールされている (P. 23) ことを確認します。
2. ユーザ ストアを設定し、サンプルデータをインポートします。
   - LDAP ユーザの場合： LDAP ユーザ ディレクトリの設定 (P. 25)
   - リレーショナル データベース ユーザの場合： リレーショナル データベースの設定
3. NeteAuto CA Identity Manager ディレクトリを作成します。
4. NeteAuto CA Identity Manager 環境を作成します。
5. NeteAuto ユーザ用の CA Identity Manager ユーザ インターフェースのルック アンド フィールを設定します (P. 41)。

LDAP ユーザ ディレクトリの設定

LDAP ディレクトリはインストールに応じて使用できます。 以下の手順を使用して、ディレクトリが存在するかどうかを確認するか、またはディレクトリを作成することができます。

次の手順に従ってください:

1. ディレクトリ サーバ コンソールで、以下のルートを持つ LDAP のインスタンスを作成します。

   ```
   dc=security,dc=com
   ```

   後で参照するために、ポート番号を書き留めます。

2. 管理ツールの samples¥NeteAuto からディレクトリ サーバに NeteAuto.ldif ファイルをインポートします。

   管理ツールは、以下のデフォルトの場所にインストールされます。

   - **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

注: LDIF ファイルのインポートまたは CA Identity Manager ディレクトリの作成で問題が発生する場合は、LDIF ファイルの先頭に以下のテキストを追加します。

```
dn: dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

ファイルを保存し、手順 1 および 2 を繰り返します。

リレーショナル データベースの設定

リレーショナル データベースを設定するには、以下の手順に従います。

次の手順に従ってください:

1. NeteAuto という名前のデータベース インスタンスを作成します。
2. パスワードが「test」で、 neteautoadmin という名前のユーザを作成します。ユーザのプロパティを編集することにより NeteAuto に対して neteautoadmin 権限（パブリック権限や db_owner 権限など）を付与します。

   注: NeteAuto データベースを作成するには、neteautoadmin ロールには、sql スクリプトで作成されるすべてのテーブルに対する最低限の（選択、挿入、更新、および削除）権限がある必要があります。 また、neteautoadmin はこれらのスクリプトで定義されるストアド プロシージャ（ある場合）をすべて実行できる必要があります。
3. ユーザ プロパティを編集するときには、NeteAuto を neteautoadmin のデフォルト データベースにします。

4. リストに表示される順序で以下のスクリプトを実行します。

   - *db_type*-rdbuserdirectory.sql -- NeteAuto サンプル用のテーブルを設定し、ユーザ エントリを作成します。
   - ims_*db_type*_rdb.sql -- 組織のサポートを設定します

     db_type

     設定しているデータベースのタイプに応じて Microsoft SQL または Oracle を定義します。

   これらのスクリプト ファイルは *admin_tools*¥samples¥NeteAutoRDB¥Organization フォルダにあります。 この例では、*admin_tools* は以下のデフォルトの場所にインストールされる管理ツールを示します。

   - **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

5. NeteAuto データベースを指す neteautoDS という名前の JDBC データ ソースを定義します。

   データ ソースを設定する手順は、CA Identity Manager がインストールされているアプリケーション サーバのタイプによって異なります。 「JDBC データ ソースを作成する方法 (P. 111)」には、JDBC データ ソースを作成するためのアプリケーション サーバ固有の手順が説明されています。

CA Identity Manager ディレクトリの作成

CA Identity Manager ディレクトリを作成するには、以下の手順に従います。

次の手順に従ってください:

1. 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://*im_server*:*port*/iam/immanage

   im_server

   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。

   port

   アプリケーション サーバのポート番号を定義します。

2. ［ディレクトリ］をクリックします。
3. CA Identity Manager ディレクトリ ウィザードを開始するには、［ウィザードから作成］をクリックします。

4. 適切なディレクトリ設定 .xml ファイルを参照し、[次へ]をクリックします。

   ディレクトリ設定ファイルは以下のフォルダにあります。

   - Sun Java System Directory Server ユーザ ディレクトリの場合：

     admin_tools¥samples¥NeteAuto¥Organization¥directory.xml

   - リレーショナル データベースの場合：

     admin_tools¥samples¥NeteAutoRDB¥Organization¥*db_type* directory.xml

     admin_tools

     管理ツールのインストール場所を定義します。

     管理ツールは、以下のデフォルトの場所にインストールされます。

     Windows： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools

     UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

     db_type

     Microsoft SQL または Oracle を設定しているデータベースのタイプを指定します。

   ステータス情報は［ディレクトリ設定出力］画面に表示されます。

5. ウィザードの 2 番目のページで、以下の値を入力します。

   - Sun Java System Directory Server

     Name

     NeteAuto ディレクトリ

     Description

     サンプル NeteAuto ディレクトリ

     接続オブジェクト名

     NeteAuto ユーザ

     Host

     ユーザ ストアがインストールされているシステムのコンピュータ名または IP アドレス。

     Port

     ユーザ ストアのポート番号

     Search root

     dc=security, dc=com

Username

ユーザ ストアにアクセスできるアカウントのユーザ名。

Password and Confirm Password

ユーザ アカウントのパスワード

- Microsoft SQL Server および Oracle データベース

Name

NeteAutoRDB ディレクトリ

Description

サンプル NeteAuto ディレクトリ

Connection Object Name

NeteAutoRDB

JDBC Data Source

neteautoDS

Username

Neteautoadmin

Password

Test

6. ［次へ］をクリックします。
7. ［完了］をクリックするとウィザードが終了します。

NeteAuto CA Identity Manager 環境の作成

NeteAuto CA Identity Manager 環境を作成するには、以下の手順に従います。

次の手順に従ってください:

1. 管理コンソールで、［環境］をクリックします。
2. CA Identity Manager 環境画面で、［新規］をクリックします。

   CA Identity Manager 環境ウィザードが表示されます。
3. ウィザードの最初のページで、以下の値を入力します。

   環境名

   NeteAuto 環境

Description

サンプル環境

Alias

Neteauto

エイリアスは CA Identity Manager 環境にアクセスするために URL に追加されます。 たとえば、neteauto 環境にアクセスするための URL は以下のとおりです。

http://*server_name*/iam/im/neteauto

server_name

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。例：

http://myserver.mycompany.org/iam/im/neteauto

注: エイリアスは大文字と小文字が区別されます。

［次へ］をクリックします。

4. 作成している環境と関連付ける CA Identity Manager ディレクトリを選択します。
   - Sun Java System Directory Server の場合、NeteAuto Directory を使用します。
   - Microsoft SQL Server または Oracle データベースの場合は、NeteAutoRDB Directory を使用します。

   ［次へ］をクリックします。
5. 自己登録や忘れたパスワード タスクなどのパブリック タスクのサポートを以下のように設定します。
   a. パブリック タスクに以下のエイリアスを入力します。

      Neteautopublic

   b. 匿名のユーザ アカウントとして SelfRegUser を入力します。
   c. ユーザの固有な識別子を表示するには、［検証］をクリックします。

   注: ユーザはパブリック タスクを使用するためにログインする必要はありません。
6. NeteAuto 環境に対して作成するタスクおよびロールを選択します。
   a. ［ファイルからのロールのインポート］を選択します。
   b. 次のいずれかの場所を参照します。
      - Sun Java Systems Directory Server ユーザ ストアの場合：

        admin_tools¥samples¥NeteAuto¥RoleDefinitions.xml

- Microsoft SQL Server ユーザ ストアの場合：

  admin_tools¥samples¥NeteAutoRDB¥Organization¥mssqlRoleDefinitions.xml

- Oracle ユーザ ストアの場合：

  admin_tools¥samples¥NeteAutoRDB¥Organization¥oracleRoleDefinitions.xml

admin_tools はデフォルトで以下の場所にインストールされる管理ツールを示します。

Windows： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools

UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

7. この環境のシステム マネージャとしてユーザを指定し、［次へ］をクリックします。
   a. ［システム マネージャ］フィールドに SuperAdmin を入力します。
   b. ［追加］をクリックします。

      CA Identity Manager は、ユーザのリストに Superadmin ユーザの一意の識別子を追加します。
   c. ［次へ］をクリックします。
8. 環境用の設定を確認し、以下のタスクを実行します。
   - （オプション）変更するには［前へ］をクリックします。
   - 現在の設定で CA Identity Manager 環境を作成するには［完了］をクリックします。

     ［環境設定出力］画面に、環境作成の進捗状況が表示されます。
9. CA Identity Manager 環境ウィザードを終了するには、［続行］をクリックします。
10. CA Identity Manager 環境を起動します。

NeteAuto 環境を作成したら、以下を実行できます。

- この CA Identity Manager 環境用のスキンの作成（P. 41）
- 環境へのアクセス（P. 39）

組織サポートなしで NeteAuto サンプルを設定する方法

組織サポートなしで NeteAuto サンプルを設定するには、以下の手順が含まれます。

- 前庭条件のソフトウェア (P. 23) のインストール
- サンプル CA Identity Manager 環境のインストール
- データベースの設定
- JDBC データ ソースの作成
- CA Identity Manager ディレクトリの作成
- NeteAuto CA Identity Manager 環境の作成

サンプル CA Identity Manager 環境の説明

Microsoft SQL Server と Oracle データベースの場合、CA Identity Manager には、組織が含まれない NeteAuto 環境のバージョンが含まれます。 この CA Identity Manager 環境には以下の 3 人のユーザが含まれます。

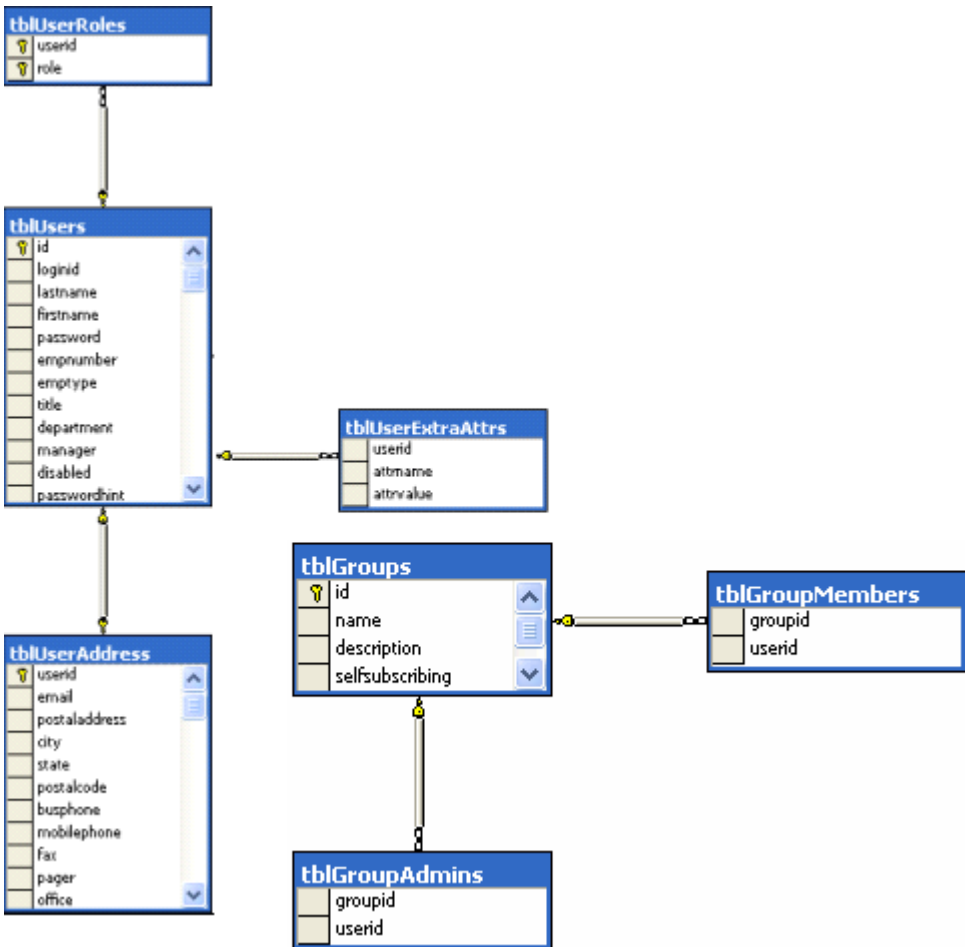
- Superadmin は、この CA Identity Manager 環境用のシステム マネージャ ロールを持つ管理者アカウントです。 Superadmin として、デフォルトの管理タスクをすべて実行できます。

  注: デフォルトの管理タスクについては、「管理ガイド」を参照してください。

- SelfRegUser は、この CA Identity Manager 環境用の自己登録を有効にするために、CA Identity Manager が使用する管理者アカウントです。
- ユーザが NeteAuto 環境をインストールするときには、NeteAuto 管理者には権限がありません。

  ただし、NeteAuto 管理者アカウントにグループ マネージャ ロールを割り当てることができます。

以下の図では、組織が含まれない、リレーショナル データベースの NeteAuto サンプルについて説明します。



Neteauto 環境用のインストール ファイル

CA Identity Manager には、サンプルの CA Identity Manager 環境をセットアップするためのファイル セットが 1 つ含まれています。 CA Identity Manager 環境は、CA Identity Manager 管理者がオブジェクトを管理できる CA Identity Manager 管理ネームスペースのビューです。 ユーザやグループなどのオブジェクトは、 1 セットのロールおよびタスクと関連付けられています。CA Identity Manager 環境では、ユーザ ストアが視覚的に表され、ユーザ ストアの管理を制御します。

サンプルの CA Identity Manager 環境には以下が含まれます。

- サンプル ユーザ
- ロール、タスクおよび画面定義

  ユーザやグループなどのカテゴリをクリックすると、ユーザ コンソールにタスクが表示されます。 表示されるタスクは、ユーザに割り当てられているロールに基づいています。

  注: ロールおよびタスクの詳細については、「*管理ガイド*」を参照してください。
- NeteAuto ユーザ用にユーザ コンソールをカスタマイズするためのサンプル スキン。
- CA Identity Manager ディレクトリの作成用に使用するディレクトリ設定ファイル。

サンプル CA Identity Manager 環境の作成用ファイルは以下の場所にインストールされます。

admin_tools¥samples¥NeteAutoRDB¥NoOrganization

このパスで、*admin_tools* は管理ツールを示します。

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

NeteAuto 環境をインストールする方法 -- 組織サポートなし

NeteAuto 環境をインストールするには、以下のプロセスを実行します。

次の手順に従ってください:

1. 前提条件のソフトウェア (P. 35) がインストールされていることを確認します。
2. データベースを設定します (P. 26)。
3. CA Identity Manager ディレクトリを作成します。 (P. 36)
4. NeteAuto CA Identity Manager 環境を作成します (P. 38)。
5. NeteAuto ユーザ用の CA Identity Manager ユーザ インターフェース (P. 41) のルック アンド フィールを設定します。

前提条件のソフトウェア

NeteAuto CA Identity Manager 環境には以下の前提条件があります。

- 「インストール ガイド」の説明に従って CA Identity Manager をインストールします。 必ず、CA Identity Manager 管理ツールをインストールします。
- Microsoft SQL Server または Oracle データベースへのアクセス権が必要です。

リレーショナル データベースの設定

リレーショナル データベースを設定するには、以下の手順に従います。

次の手順に従ってください:

1. NeteAuto という名前のデータベース インスタンスを作成します。
2. パスワードが「test」で、 neteautoadmin という名前のユーザを作成します。ユーザのプロパティを編集することにより NeteAuto に対して neteautoadmin 権限（パブリック権限や db_owner 権限など）を付与します。

   注: NeteAuto データベースを作成するには、neteautoadmin ロールには、sql スクリプトで作成されるすべてのテーブルに対する最低限の（選択、挿入、更新、および削除）権限がある必要があります。 また、neteautoadmin はこれらのスクリプトで定義されるストアド プロシージャ（ある場合）をすべて実行できる必要があります。
3. ユーザ プロパティを編集するときには、NeteAuto を neteautoadmin のデフォルト データベースにします。
4. リストに表示される順序で以下のスクリプトを実行します。
   - *db_type*-rdbuserdirectory.sql -- NeteAuto サンプル用のテーブルを設定し、ユーザ エントリを作成します。
   - ims_*db_type*_rdb.sql -- 組織のサポートを設定します

     db_type

     設定しているデータベースのタイプに応じて Microsoft SQL または Oracle を定義します。

   これらのスクリプト ファイルは *admin_tools*¥samples¥NeteAutoRDB¥Organization フォルダにあります。 この例では、*admin_tools* は以下のデフォルトの場所にインストールされる管理ツールを示します。
   - **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

5. NeteAuto データベースを指す neteautoDS という名前の JDBC データ ソースを定義します。

   データ ソースを設定する手順は、CA Identity Manager がインストールされているアプリケーション サーバのタイプによって異なります。 「JDBC データ ソースを作成する方法 (P. 111)」には、JDBC データ ソースを作成するためのアプリケーション サーバ固有の手順が説明されています。

CA Identity Manager ディレクトリの作成

CA Identity Manager ディレクトリを作成するには、以下の手順に従います。

次の手順に従ってください:

1. 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://*im_server*:*port*/iam/immanage

   im_server

   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。

   ポート

   アプリケーション サーバのポート番号を定義します。

2. ［ディレクトリ］をクリックします。

   CA Identity Manager ディレクトリ画面が表示されます。

3. CA Identity Manager ディレクトリ ウィザードを開始するには、［新規］をクリックします。

4. 以下のディレクトリ設定 XML ファイルのいずれかを参照し、［次へ］をクリックします。

   - Sun Java System：

     admin_tools¥samples¥NeteAuto¥NoOrganization¥directory.xml

   - SQL Server データベース：

     admin_tools¥samples¥NeteAuto¥NoOrganization¥mssql-directory.xml

   - Oracle データベース：

     admin_tools¥samples¥NeteAuto¥NoOrganization¥oracle-directory.xml

   admin_tools は以下の場所にデフォルトでインストールされる管理ツールを示します。

   - **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   ステータス情報は［ディレクトリ設定出力］画面に表示されます。

5. ウィザードの 2 番目のページで、以下の値を入力します。

   Name

   NeteAutoRDB ディレクトリ

   Description

   組織サポートなしのサンプル NeteAuto ディレクトリ

   接続オブジェクト名

   NeteAutoRDB

   JDBC **データ ソース**

   neteautoDS

   Username

   neteautoadmin

   Password

   test

6. ［次へ］をクリックします。
7. ［完了］をクリックするとウィザードが終了します。

NeteAuto CA Identity Manager 環境の作成

NeteAuto CA Identity Manager 環境を作成するには、以下の手順に従います。

次の手順に従ってください:

1. 管理コンソールで、［環境］をクリックします。
2. CA Identity Manager 環境画面で、［新規］をクリックします。

   CA Identity Manager 環境ウィザードが開きます。
3. ウィザードの最初のページで、以下の値を入力します。
   - 環境名 -- NeteAuto 環境
   - 説明 -- NeteAuto はサンプル環境です。
   - エイリアス -- neteautoRDB

     エイリアスは CA Identity Manager 環境にアクセスするための URL に追加されます。 たとえば、neteauto 環境にアクセスするための URL は以下のとおりです。

     `http://domain/iam/im/neteautoRDB`

     このパスで、*domain* は以下の例のように 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。

     `http://myserver.mycompany.org/iam/im/neteautoRDB`

     注: エイリアスは大文字と小文字が区別されます。

   ［次へ］をクリックします。
4. 作成している環境と関連付ける NeteAutoRDB Directory CA Identity Manager ディレクトリを選択し、［次へ］をクリックします。
5. 自己登録や忘れたパスワード タスクなどのパブリック タスクのサポートを設定します。

   注: ユーザはパブリック タスクにアクセスするためにログインする必要はありません。

   a. パブリック タスクに以下のエイリアスを入力します。

      neteautoRDBpublic

   b. 匿名のユーザ アカウントとして SelfRegUser を入力します。

   c. ユーザの固有な識別子（この場合は 2）を表示するには、［検証］をクリックします。
6. NeteAuto 環境に対して作成するタスクおよびロールを選択します。
   - ［ファイルからのロールのインポート］を選択します。

- 以下の場所を参照します。

  im_admin_tools_dir¥samples¥NeteAutoRDB¥NoOrganizations¥RoleDefinitions.xml

  このパスで、*im_admin_tools_dir* は、CA Identity Manager 管理ツールのインストール場所を定義します。

7. この環境のシステム マネージャとしてユーザを指定し、［次へ］をクリックします。
   a. ［システム マネージャ］フィールドに SuperAdmin を入力します。
   b. ［追加］をクリックします。
   c. ［次へ］をクリックします。
8. 環境用の設定を確認します。
   - 変更するには［前へ］をクリックします。
   - 現在の設定で CA Identity Manager 環境を作成するには［完了］をクリックします。

     ［環境設定出力］画面に、環境作成の進捗状況が表示されます。
9. CA Identity Manager 環境ウィザードを終了するには、［完了］をクリックします。
10. CA Identity Manager 環境を起動します。

NeteAuto 環境を作成したら、以下を実行できます。

- 「NeteAuto スキンのセットアップ (P. 41)」の説明に従って、この CA Identity Manager 環境用のスキンを作成します。
- 「NeteAuto CA Identity Manager 環境の使用」の説明に従って、環境にアクセスします。

NeteAuto CA Identity Manager 環境の使用方法

セルフサービスのタスクおよびユーザを管理するために NeteAuto CA Identity Manager 環境を使用できます。

セルフサービス タスク管理

セルフサービス タスクには以下のものが含まれます。

- 新規ユーザとして登録する
- 自己登録ユーザとしてログインする
- 忘れたパスワード機能の使用

新しいユーザとして登録

新規ユーザとして登録するには、以下の手順に従います。

次の手順に従ってください:

1. ブラウザで以下の URL を入力します。

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration`

   hostname

   CA Identity Manager が実行されているシステムの完全修飾ドメイン名を定義します。

   注: Neteauto スキンを設定 (P. 41)しなかった場合、URL から以下のように imcss を省略できます。

   http://*hostname*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   この URL により、デフォルトの ca コンソールにアクセスできます。

   自己登録の［エンドユーザ使用許諾契約］ページで、CA Identity Manager に CA Web サイトが表示されます。

   注: カスタムのエンドユーザ使用許諾契約を表示するためにデフォルトの自己登録タスクを設定できます。 詳細については、「管理ガイド」を参照してください。

2. ［承諾］をクリックして続行します。
3. ［プロファイル］タブで、以下の詳細を入力します。
   a. アスタリスク（*）で示された必須フィールドに値を入力します。
   b. パスワード ヒントと回答を入力します。

      パスワードを忘れた場合、CA Identity Manager ではパスワード ヒントを提供し、回答を要求します。 回答が正しい場合、CA Identity Manager は新しいパスワードを指定し、確認するようにユーザに促します。

4. ［グループ］タブはそのままにしておきます。
5. ［Submit］をクリックします。

自己登録ユーザとしてログインします。

自己登録ユーザとしてログインするには、以下の手順に従います。

次の手順に従ってください:

1. ブラウザで NeteAuto CA Identity Manager 環境用の以下の URL を入力します。

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   hostname

   CA Identity Manager が実行されているシステムの完全修飾ドメイン名を定義します。

2. 登録したときに指定したユーザ名およびパスワードを使用してログインします。

NeteAuto スキンのセットアップ

NeteAuto スキンをセットアップするには、SiteMinder ポリシー サーバで SiteMinder レスポンスを作成します。

次の手順に従ってください:

1. ドメイン権限を持つ管理者として以下のインターフェースのいずれかにログインします。
   - CASiteMinder Web Access Manager r12 の場合は、管理 UI にログインします。
   - CA eTrustSiteMinder6.0 SP5 の場合は、ポリシー サーバ ユーザ インターフェースにログインします。

   注: これらのインターフェースの使用の詳細については、使用している SiteMinder のバージョン用のマニュアルを参照してください。
2. neteautoDomain を開きます。
3. neteautoDomain の下では、［領域］を選択します。

   以下の領域が表示されます。

   neteauto_ims_realm

   CA Identity Manager 環境を保護します。

   neteauto_pub_realm

   自己登録や忘れたパスワード タスクなどのパブリック タスクのサポートを有効にします。

4. 各領域でルールを作成します。 以下の詳細を指定します。
   - Resource: *
   - アクション： GET、POST

   管理を簡略化するには、ルール名に NeteAuto スキンを含めてください。
5. 以下のレスポンス属性を持つドメインのレスポンスを作成します。
   - 属性： WebAgent-HTTP-Header-Variable

     この属性は、レスポンスに新しい HTTP ヘッダを追加します。
   - 属性の種類： 静的
   - 変数名： スキン

     変数値： neteauto
6. CA Identity Manager が neteautoDomain で作成したポリシーを変更します。 以下の詳細を指定します。
   - ユーザ
     - LDAP の場合： ［使用可能なメンバ］ で ou=People, ou=Employees, ou=NeteAuto を選択し、［現在のメンバ］にそれを追加します。［OK］をクリックします。
     - リレーショナル データベースの場合: ID 属性が等しい*ユーザを検索します。 ［使用可能なメンバ］のユーザをすべて選択し、［現在のメンバ］に追加します。 ［OK］をクリックします。
   - ルール
     - 手順 4 で作成したルールを追加します。
     - 各ルールについて、［レスポンスの設定］をクリックします。 手順 5 で作成したレスポンスと各ルールを関連付けます。

注: neteauto スキンは imcss コンソールに基づいています。 スキンを表示するには、NeteAuto CA Identity Manager 環境用の URL に以下のように /imcss/index.jsp を追加します。

http://*hostname*/iam/im/neteauto/imcss/index.jsp

「NeteAuto CA Identity Manager 環境へのアクセス (P. 44)」 では、Neteauto 環境にアクセスするための完全な手順が説明されています。

忘れたパスワード機能の使用

忘れたパスワード機能を使用するには、以下の手順に従います。

次の手順に従ってください:

1. ブラウザで以下の URL を入力します。

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset`

   hostname

   CA Identity Manager が実行されているシステムの完全修飾ドメイン名を定義します。

2. ［新規ユーザとして登録する (P. 40)］で作成した自己登録ユーザの一意の識別子を入力し、［次へ］をクリックします。
3. 確認を促すメッセージが表示されるたびに回答します。 回答は登録中に入力した内容です。

   注: 各質問に対して正確に回答する必要があります。 タスクをキャンセルするか、またはブラウザを閉じると、試行に失敗したと見なされます。
4. ［Submit］をクリックします。

   CA Identity Manager により新しいパスワードの入力を求められます。

ユーザの管理

ユーザ管理には以下の操作が含まれます。

- NeteAuto CA Identity Manager 環境へのアクセス
- ユーザの変更
- グループ マネージャ ロールの割り当て
- グループの作成
- 自己登録ユーザの管理

NeteAuto CA Identity Manager 環境へのアクセス

NeteAuto CA Identity Manager 環境にアクセスするには、以下の手順に従います。

次の手順に従ってください:

1. ブラウザで以下の URL を入力します。

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   hostname

   以下の例のように、完全修飾ドメイン名を定義します。

   http://myserver.mycompany.com/iam/im/neteauto/imcss/index.jsp.

   注: Neteauto スキンを設定しなかった場合に、Neteauto 環境にアクセスするには、以下の URL を使用できます。

   http://*hostname*/iam/im/neteauto

2. ログイン画面で、以下のクレデンシャルを入力します。

   User Name

   SuperAdmin

   Password

   test

ユーザの変更

ユーザを変更するには、以下の手順に従います。

次の手順に従ってください:

1. パスワード「test」を使用して、SuperAdmin として NeteAuto 環境にログインします。
2. ［ユーザ］-［ユーザの管理］-［ユーザの変更］を選択します。

   ［ユーザの選択］画面が表示されます。
3. ［検索］をクリックします。

   CA Identity Manager により、NeteAuto 環境のユーザのリストが表示されます。
4. 以下のように NeteAuto 管理者を選択します。
   - LDAP ディレクトリの場合： NeteAuto Administrator
   - リレーショナル データベースの場合： NeteAuto Admin

   ［選択］をクリックします。 CA Identity Manager により、NeteAuto 管理者のプロファイルが表示されます。

5. ［タイトル］フィールドで、「マネージャ」と入力します。 ［サブミット］をクリックします。

   CA Identity Manager によりタスク送信が確認されます。

6. ［OK］をクリックして、メイン画面に戻ります。

グループ マネージャ ロールの割り当て

グループ マネージャ ロールを割り当てる必要があります。 グループ マネージャを割り当てるには、以下の手順に従います。

次の手順に従ってください:

1. SuperAdmin として、［ロールおよびタスク］タブを選択し、［管理ロール］、［管理ロールの変更］を選択します、
2. グループ マネージャ ロールを選択し、［選択］をクリックします。

   グループ マネージャ ロールのプロファイルが表示されます。

3. ［メンバ］タブをクリックし、［メンバ ポリシー］の下の［追加］をクリックします。

   ［メンバ ポリシー］画面が表示されます。

4. ［メンバ ルール］の下で、［ユーザ］フィールドにある下矢印をクリックします。

   ドロップダウン リストから、where <user-filter> を選択します。

   ［ユーザ］フィールドはルールのフィルタを入力すると変更されます。

5. 以下のようにメンバシップ ルールを入力します。
   a. 最初のフィールドで、ドロップダウン リストから［タイトル］を選択します。
   b. 2 番目のフィールドで、等号（=）が選択されていることを確認します。
   c. 3 番目のフィールドで、「マネージャ」と入力します。
6. ［スコープ ルール］セクションで、ユーザ、グループ、および組織（サポート時）のルールを以下のように定義します。
   a. ［ユーザ］フィールドで、オプションのリストを参照するために下矢印をクリックします。 リストから［（すべて）］を選択します。
   b. ［グループ］および［組織］フィールド（サポート時）で手順「a」を繰り返します。
   c. ［アクセス タスク］フィールドは空のままにします。
7. ［OK］をクリックします。

   CA Identity Manager により、作成したメンバ ポリシーが表示されます。

8. ［サブミット］をクリックします。

   CA Identity Manager によりタスク送信が確認されます。

9. ［OK］をクリックして、メイン画面に戻ります。

10. CA Identity Manager を閉じます。

グループの作成

グループを作成するには、以下の手順に従います。

次の手順に従ってください:

1. NeteAuto 管理者として CA Identity Manager に以下のようにログインします。

   - LDAP ディレクトリの場合、ユーザ名「NeteAuto Administrator」およびパスワード「test」を入力します。
   - リレーショナル データベースの場合、ユーザ名「NeteAuto Admin」およびパスワード「test」を入力します。

   NeteAuto 管理者が実行できるタスクのリストが表示されます。NeteAuto 管理者は制限された数のタスクのみ実行できるので、CA Identity Manager では、カテゴリではなく、タスクをリスト表示します。

2. ［グループの作成］をクリックします。

3. ［新規グループの作成］が選択されていることを確認し、［OK］をクリックします。

4. 自分のケースに合った以下のいずれかの手順を実装します。

   - NeteAuto 環境が組織をサポートする場合：

     a. ［組織名］フィールドで、省略記号（...）をクリックして、CA Identity Manager でグループを作成する組織を選択します。

     b. ［組織の選択］画面下部で、NeteAuto を展開します。

     c. ディーラ組織を選択します。

   - NeteAuto 環境が組織をサポートしない場合は、次の手順に移動します。

5. グループの以下の情報を入力します。

   - グループ名： ディーラ管理者
   - グループの説明： NeteAuto ディーラの管理者

6. ［メンバシップ］タブをクリックし、［ユーザの追加］をクリックします。

   ［ユーザの選択］画面が表示されます。

7. ［検索］をクリックします。
8. NeteAuto 管理者を選択し、［選択］をクリックします。
9. ［サブミット］をクリックして、グループを作成します。

自己登録ユーザの管理

自己登録ユーザを管理するときには、以下の手順に従います。

次の手順に従ってください:

1. 以下のクレデンシャルを使用して、NeteAuto 管理者として CA Identity Manager にログインします。
   - LDAP ディレクトリの場合：

     Username

     NeteAuto 管理者

     Password

     test
   - リレーショナル データベースの場合：

     Username

     NeteAuto Admin

     Password

     test

   NeteAuto 管理者が実行できるタスクのリストがユーザ コンソールの左側に表示されます。NeteAuto 管理者は制限された数のタスクのみ実行できるので、CA Identity Manager では、カテゴリではなく、タスクのリストが表示されます。
2. ［グループの変更］をクリックします。
3. ［検索］をクリックします。

   CA Identity Manager では、グループのリストが表示されます。
4. ［ディーラ管理者］を選択し、［選択］をクリックします。
5. ［メンバシップ］タブをクリックし、［ユーザの追加］をクリックします。

   ［ユーザの選択］画面が表示されます。
6. ［検索］をクリックします。
7. ［ユーザ検索］画面で、［新規ユーザとして登録する (P. 40)］で入力したユーザを選択します。 ［選択］をクリックします。

8. ［サブミット］をクリックします。

   CA Identity Manager によりタスク送信が確認されます。

9. ［OK］をクリックして、メイン画面に戻ります。

ユーザが作成されたグループのメンバであることを確認するには、［グループの表示］タスクを使用します。

追加機能の設定方法

NeteAuto サンプルをインストールしており、基本的な CA Identity Manager 機能を実行したら、NeteAuto 環境を使用して、電子メール通知やワークフローを含む、追加の CA Identity Manager 機能を実行およびテストします。

注: これらの機能の詳細については、「管理ガイド」を参照してください。

グローバル ユーザ名に対する SiteMinder のログイン名の制限

ユーザが SiteMinder ポリシー サーバにログインする必要がある場合、以下の文字または文字列をグローバル ユーザ名の一部にすることはできません。

&
*
:
()

回避方法

グローバル ユーザ名でこれらの文字を使用しないようにします。

第 3 章: LDAP ユーザ ストアの管理

このセクションには、以下のトピックが含まれています。

CA Identity Manager ディレクトリ (P. 49)
CA Identity Manager ディレクトリを作成する方法 (P. 50)
ディレクトリ構造 (P. 50)
ディレクトリ設定ファイル (P. 52)
ディレクトリ設定テンプレートを選択する方法 (P. 53)
CA Identity Manager にユーザ ディレクトリを説明する方法 (P. 55)
ユーザ ディレクトリへの接続 (P. 56)
ディレクトリ検索パラメータ (P. 61)
ユーザ、グループ、および組織管理対象オブジェクトの説明 (P. 62)
LDAP ユーザ用の汎用属性 (P. 82)
ユーザ ディレクトリ構造の説明 (P. 90)
グループの設定方法 (P. 91)
検証ルール (P. 94)
追加の CA Identity Manager ディレクトリのプロパティ (P. 95)
ディレクトリ検索のパフォーマンスを改善する方法 (P. 99)

CA Identity Manager ディレクトリ

*CA Identity Manager ディレクトリ*は、ユーザ、グループ、組織などのオブジェクトがユーザ ディレクトリにどのように格納され、CA Identity Manager でどのように表示されるかを説明します。 CA Identity Manager ディレクトリは 1 つ以上の CA Identity Manager 環境と関連付けられます。

CA Identity Manager ディレクトリを作成する方法

LDAP ユーザ ストア用の CA Identity Manager ディレクトリの作成には、以下の手順が含まれます。

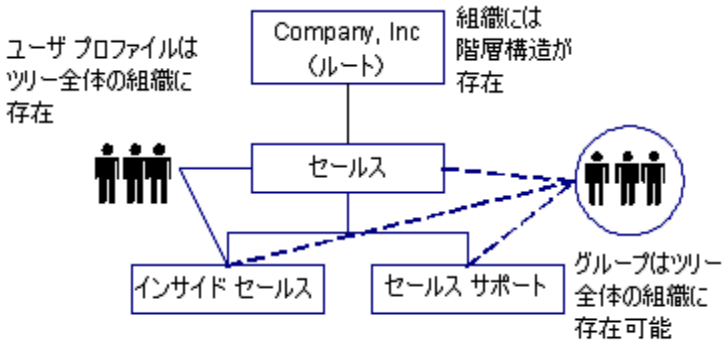
1. ディレクトリ構造を決定します。
2. ディレクトリ設定ファイル（directory.xml）（P. 55）を変更することによりユーザ ストアのオブジェクトについて説明します。
3. ディレクトリ設定ファイルをインストールし、ディレクトリを作成（P. 161）します。

注: SiteMinder を使用する場合は、CA Identity Manager ディレクトリを作成する前に、ポリシー ストア スキーマを適用していることを確認します。特定のポリシー ストア スキーマ、およびそれらの適用方法の詳細については、「インストール ガイド」を参照してください。

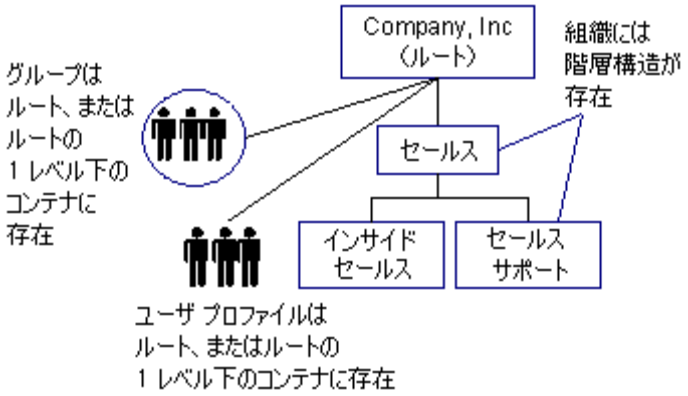
ディレクトリ構造

CA Identity Manager は、以下のディレクトリ構造をサポートします。

- 階層的 -- 親組織（ルート）およびサブ組織が含まれます。 サブ組織には、そのサブ組織もあります。以下の図に示すように、複数レベルの構造を作成します。

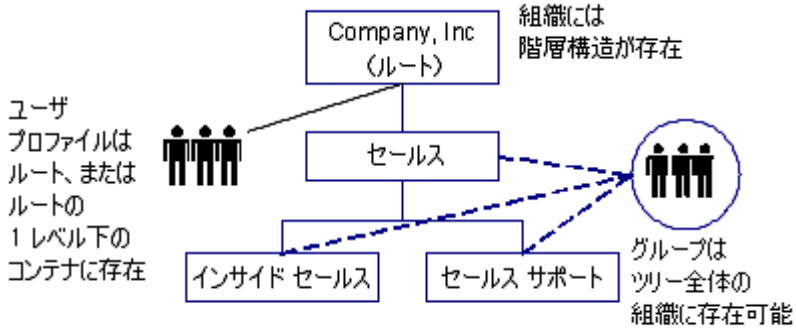


- フラット -- ユーザとグループは、検索ルート、または検索ルートの 1 レベル下のコンテナに格納されます。フラット ディレクトリ構造の以下の図に示すように、組織には階層構造があります。



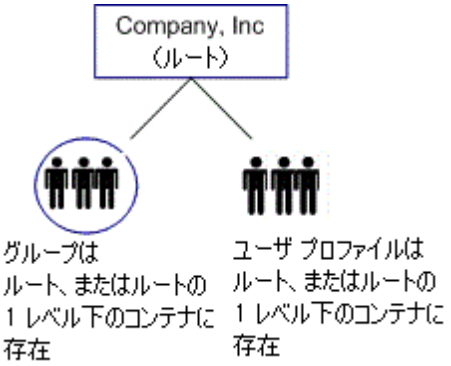
フラット ディレクトリ構造でユーザ管理および委任が容易に行えるように、ユーザとグループは論理的な組織に属します。 論理的な組織はユーザおよびグループ プロファイルの属性として格納されます。

- フラット ユーザ -- 組織とグループは階層的に格納されます。しかし、ユーザは、検索ルートまたは検索ルートの 1 レベル下のコンテナに格納されます。フラット ユーザ ディレクトリ構造の例は、以下の図に示されます。



フラット ユーザ ディレクトリ構造では、ユーザは論理的な組織に属します。ユーザの論理的な組織はユーザ プロファイルの属性として格納されます。

- 組織なし -- ディレクトリには組織が含まれません。 ユーザとグループは、検索ルート、または検索ルートの 1 レベル下のコンテナに格納されます。 組織なしのディレクトリは以下の図に示されます。



注: ディレクトリには複数のタイプの構造を含むことができます。たとえば、ユーザ プロファイルは、ディレクトリの一部ではフラットな構造で格納し、別の部分では階層的に格納できます。ハイブリッド ディレクトリ構造をサポートするには、複数の CA Identity Manager 環境を作成します。

ディレクトリ設定ファイル

CA Identity Manager にユーザ ディレクトリの構造を説明するには、ディレクトリ設定ファイルを作成します。

ディレクトリ設定ファイルには、以下のセクションの 1 つ以上が含まれます。

CA Identity Manager Directory Information

CA Identity Manager ディレクトリに関する情報が含まれます。

注: このセクション内の情報を変更しないでください。 管理コンソールで CA Identity Manager ディレクトリを作成するときに、CA Identity Manager により、この情報を提供するように促されます。

Attribute Validation

CA Identity Manager ディレクトリに適用される検証ルールを定義します。

Provider Information

CA Identity Manager が管理するユーザ ストアを説明します。

Directory Groups Behavior

CA Identity Manager でユーザ ストアが検索される方法を指定できます。

User Object

ユーザがユーザ ストアにどのように格納され、CA Identity Manager でどのように表示されるのかを説明します。

Group Object

グループがユーザ ストアにどのように格納され、CA Identity Manager でどのように表示されるのかを説明します。

Organization Object

組織がどのように格納され、CA Identity Manager でどのように表示されるのかを説明します。 ユーザ ストアに組織が含まれる場合にのみ、組織オブジェクトは詳細を提供します。

Self-Subscribing オブジェクト

セルフサービス ユーザが参加できるグループに対するサポートを設定します。

Directory Groups Behavior

CA Identity Manager ディレクトリが動的およびネスト グループをサポートするかどうかを指定します。

ディレクトリ設定ファイルを作成するには、設定テンプレートを変更します。

ディレクトリ設定テンプレートを選択する方法

CA Identity Manager では、別のディレクトリ タイプおよび構造をサポートするディレクトリ設定テンプレートを提供します。 CA Identity Manager ディレクトリを作成するには、ディレクトリ構造に最もマッチするテンプレートを変更します。

以下の表で説明されるテンプレートは、管理ツールでインストールされます。

admin_tools¥directoryTemplates¥*directory_type*¥

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

ディレクトリのタイプおよび対応する設定テンプレートは以下の表に示されます。

ディレクトリ タイプ	テンプレート
階層構造を持つ Active Directory （ADSI） LDAP ディレクトリ	ActiveDirectory¥directory.xml
階層構造を持つ Microsoft ADAM ディレクトリ	ADAM¥directory.xml
階層構造を持つ IBM Directory Server ディレクトリ	IBMDirectoryServer¥directory.xml
階層構造を持つ Novell eDirectory ユーザ ディレクトリ	eDirectory¥directory.xml
階層構造を持つ Oracle インターネット ディレクトリ	OracleInternetDirectory¥directory.xml
階層構造を持つ Sun Java System （SunOne または iPlanet） LDAP ディレクトリ	IPlanetHierarchical¥directory.xml
フラット構造を持つ Sun Java System （SunOne または iPlanet） LDAP ディレクトリ	IPlanetFlat¥directory.xml
組織が含まれない Sun Java System （SunOne または iPlanet） LDAP ディレクトリ	IPlanetNoOrganizations¥directory.xml
階層構造を持つ CA Directory ユーザ ストア	eTrustDirectory¥directory.xml

ディレクトリ タイプ	テンプレート
プロビジョニング ディレクトリ このテンプレートは、CA Identity Manager 環境用のプロビジョニング ディレクトリを設定します。 **注**: インストールに応じてこの設定テンプレートを使用できます。 このテンプレートを変更する必要はありません。	ProvisioningServer¥directory.xml
カスタム ディレクトリ	ディレクトリに最もマッチするテンプレートを使用します。

新規ディレクトリに設定テンプレートをコピーするか、またはそれを上書きされないように別の名前で保存します。

CA Identity Manager にユーザ ディレクトリを説明する方法

ディレクトリを管理するには、CA Identity Manager が、ディレクトリの構造およびコンテンツを理解している必要があります。 CA Identity Manager にディレクトリを説明するには、適切なテンプレート ディレクトリでディレクトリ設定ファイル（directory.xml）を変更します。

ディレクトリ設定ファイルには以下の重要な規則があります。

- ## -- 必要な値を示します。

  必要な情報をすべて提供するには、ダブル パウンド記号（##）をすべて検索し、それらを適切な値と置き換えます。たとえば、##DISABLED_STATE は、ユーザのアカウント ステータスを格納するためにユーザが属性を提供する必要があることを示します。

- @ -- CA Identity Manager が入力する値を示します。 ディレクトリ設定ファイルでこれらの値を変更しないでください。 CA Identity Manager は、ディレクトリ設定ファイルをインポートするときに、値を提供するようにユーザに促します。

ディレクトリ設定ファイルを変更する前に、以下の情報が必要です。

- ユーザ、グループ、および組織オブジェクトの LDAP オブジェクト クラス
- ユーザ、グループ、および組織プロファイルの属性のリスト

ディレクトリ構成ファイルを設定する方法

ディレクトリ設定ファイルを変更するには、以下の手順に従います。

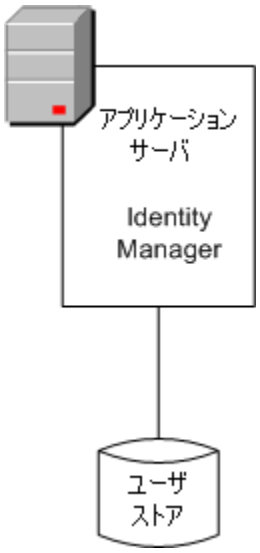
注: 必要な手順は順を追って明記されます。

1. 検索結果 (P. 61) のサイズを制限します。
2. デフォルト ユーザ、組織、またはグループ管理対象オブジェクトを変更します。
3. デフォルトの属性説明を変更します。
4. 汎用属性 (P. 82) を変更します。 （必須）

   汎用属性は、CA Identity Manager で、パスワード属性などの特別な属性を識別します。
5. CA Identity Manager のディレクトリ構造を設定します (P. 90)（必須）。
6. ユーザがグループに参加 (P. 91) できるようになります。

ユーザ ディレクトリへの接続

CA Identity Manager は、以下の図に示すように、ユーザ、グループ、組織情報などの情報を格納するためにユーザ ディレクトリに接続します。



新規ディレクトリまたはデータベースは必要ありません。ただし、既存のディレクトリまたはデータベースは、完全修飾ドメイン名（FQDN）を持つシステム上にある必要があります。

サポートされているディレクトリおよびデータベース タイプのリストについては、CA サポート サイト上の CA Identity Manager サポート マトリックスを参照してください。

管理コンソールで CA Identity Manager ディレクトリを作成するときに、ユーザ ストアへの接続を設定します。

ユーザが CA Identity Manager ディレクトリを作成した後にディレクトリ設定をエクスポートする場合、ユーザ ディレクトリ接続情報がディレクトリ設定ファイルの Provider エレメントに表示されます。

Provider エレメント

設定情報は、directory.xml ファイルの Provider エレメントおよびその従属エレメントに格納されます。

注: CA Identity Manager ディレクトリを作成する場合、directory.xml ファイル内のディレクトリ接続情報を提供する必要はありません。 管理コンソール内の CA Identity Manager ディレクトリ ウィザードの接続情報を提供します。 更新目的でのみ Provider エレメントを変更します。

Provider エレメントには以下の従属エレメントが含まれます。

LDAP

接続しているユーザ ディレクトリを説明します。

Credentials

LDAP ユーザ ストアにアクセスするためのユーザ名およびパスワードを提供します。

Connection

ユーザ ストアが格納されているコンピュータのホスト名およびポートを提供します。

Provisioning Domain

CA Identity Manager が管理する Provisioning Domain を定義します（プロビジョニング ユーザ専用）。

完了した Provider エレメントは以下のコードのようになります。

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

Provider エレメントには以下のパラメータが含まれます。

type

データベースのタイプを指定します。 すべての LDAP ユーザ ストアに対して、LDAP （デフォルト）を指定します。

userdirectory

ユーザ ディレクトリ接続の名前を指定します。

注: directory.xml ファイルにユーザ ディレクトリ接続の名前を指定しないでください。CA Identity Manager は、管理コンソールで CA Identity Manager ディレクトリを作成するときに、名前を提供するようにユーザに促します。

注: パラメータはオプションです。

LDAP 従属エレメント

LDAP 従属エレメントには以下のパラメータが含まれます。

searchroot

ディレクトリの開始ポイントとして機能する LDAP ディレクトリの場所を指定します。通常、組織（o）または組織単位（ou）です。

secure

LDAP ユーザ ディレクトリへの Secure Sockets Layer （SSL）接続を以下のように強制します。

- True -- CA Identity Manager は安全な接続を使用します。
- False -- CA Identity Manager は SSL なしでユーザ ディレクトリに接続します（デフォルト）。

注: パラメータはオプションです。

Credentials 従属エレメント

LDAP ディレクトリに接続するには、CA Identity Manager は有効なクレデンシャルを提供する必要があります。 クレデンシャルは、以下のコードのように、Credentials 従属エレメントで定義されます。

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

管理コンソールで CA Identity Manager ディレクトリを作成するときに、Credentials 従属エレメントでパスワードを指定しない場合、パスワードの入力を求められます。

注: 管理コンソールでパスワードを指定することをお勧めします。

ユーザが管理コンソールでパスワードを指定する場合、CA Identity Manager はユーザに代わってパスワードを暗号化します。そうでない場合に、クリア テキストでパスワードを表示しない場合、CA Identity Manager と共にインストールされているパスワード ツールを使用して、パスワードを暗号化します。

注: 1 セットのクレデンシャルのみ指定できます。 「Connection 従属エレメント」で説明されているように、ユーザが複数のディレクトリを定義する場合、指定するクレデンシャルはすべてのディレクトリに適用される必要があります。

Credentials 従属エレメントには以下のパラメータが含まれます。

user

ディレクトリにアクセスできるアカウントのログイン ID を指定します。

プロビジョニング ユーザ場合、指定するユーザ アカウントには、ドメイン管理者プロファイル、またはプロビジョニング サーバの同等の権限セットが必要です。

注: directory.xml ファイルのユーザ パラメータの値を指定しないでください。CA Identity Manager は、管理コンソールで CA Identity Manager ディレクトリを作成するときに、ログイン ID を提供するようにユーザに要求します。

cleartext

パスワードが directory.xml ファイル内のクリア テキストで表示されるかどうかを以下のように決定します。

- True -- パスワードはクリア テキストで表示されます。
- False -- パスワードは暗号化されます（デフォルト）。

注: パラメータはオプションです。

Connection 従属エレメント

Connection 従属エレメントでは、CA Identity Manager が管理するユーザ ストアの場所について説明します。 この従属エレメントには、以下のパラメータが含まれます。

host

ユーザ ディレクトリが格納されているシステムのホスト名または IP アドレスを指定します。

注: 接続するシステムに IPv6 アドレスがある場合は、IP アドレスを以下のように角かっこ（ [] ）で囲みます。

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"

failover="[2::9255:214:22ff:fe72:525a]:20389"/>

port

ユーザ ディレクトリのポート番号を指定します。

failover

プライマリ システムが利用できない場合に、重複するユーザ ストアが存在するシステムのホスト名および IP アドレスを指定します。プライマリ システムが再度利用できるようになる場合、フェイルオーバ システムが引き続き使用されます。プライマリ システムに戻る場合は、セカンダリ システムを再起動します。複数のサーバがリスト表示される場合、CA Identity Manager はリストに表示されている順序でシステムへの接続を試みます。

*スペース区切りリスト*でフェイルオーバ属性のホスト名と IP アドレスを以下のように指定します。

failover="IPaddress:port IPaddress:port"

例：

<Connection host="123.456.789.001" port="20389"

failover="123.456.789.002:20389 123.456.789.003:20389"/>

注: ポート 20389 はプロビジョニング サーバのデフォルト ポートです。

注: パラメータはオプションです。

Provisioning 従属エレメント

CA Identity Manager 環境にプロビジョニングが含まれる場合は、以下のようにプロビジョニング ドメインを定義します。

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

Provisioning 従属エレメントには以下のパラメータが含まれます。

ドメイン

CA Identity Manager が管理するプロビジョニング ドメインの名前が含まれます。

管理コンソールで CA Identity Manager ディレクトリを作成するときに、ドメイン名を求められます。 そのため、ディレクトリ設定ファイル（directory.xml）でドメイン パラメータの値が指定されていることを確認してください。

ディレクトリ検索パラメータ

DirectorySearch エレメントで以下の検索パラメータを設定できます。

maxrows

ユーザ ディレクトリを検索するときに CA Identity Manager が返すことができるオブジェクトの最大数を指定します。 オブジェクトの数が限度を超えると、エラーが表示されます。

maxrows パラメータに値の設定することにより、検索結果を制限する LDAP ディレクトリ内の設定を無効にすることができます。 矛盾する設定が適用される場合、LDAP サーバは優先度の最も低い設定を使用します。

注: maxrows パラメータは、CA Identity Manager タスク画面上に表示されるオブジェクトの数を制限しません。 表示設定を設定するには、CA Identity Manager ユーザ コンソール内のリスト画面定義を変更します。 手順については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

maxpagesize

単一の検索で返すことができるオブジェクトの数を指定します。 オブジェクトの数がページ サイズを超える場合、CA Identity Manager は複数の検索を実行します。

maxpagesize を指定するときは、以下の点に注意してください。

- maxpagesize オプションを使用するには、CA Identity Manager が管理するユーザ ストアがページングをサポートしている必要があります。 一部のユーザ ストア タイプは、ページングをサポートするために追加設定が必要です。 詳細については、「大規模な検索のパフォーマンスを改善する方法 (P. 100)」を参照してください。
- ユーザ ストアがページングをサポートせず、maxrows の値も指定される場合、CA Identity Manager は、検索サイズを制御するために maxrows 値のみを使用します。

timeout

CA Identity Manager がディレクトリの検索を終了するまでの最大秒数を決定します。

注: DirectorySearch エレメントはオプションです。 ただし、ディレクトリはページング (P. 100)をサポートします。DirectorySearch エレメントを指定することをお勧めします。

詳細情報:

ディレクトリ検索のパフォーマンスを改善する方法 (P. 99)
大規模な検索のパフォーマンスを改善する方法 (P. 100)

ユーザ、グループ、および組織管理対象オブジェクトの説明

CA Identity Manager では、ユーザ ディレクトリのエントリに対応する以下のタイプのオブジェクトを管理します。

ユーザ

企業のユーザを表します。 ユーザは単一の組織に属します。

グループ

何かを共有しているユーザの関連付けを表します。

組織

事業単位を表します。 組織には、ユーザ、グループ、他の組織などの詳細が含まれます。

オブジェクトの説明には以下の情報が含まれます。

- LDAP オブジェクト クラスやオブジェクトが格納されるコンテナなどのオブジェクト (P. 121)に関する情報。
- エントリに関する情報を格納する属性 (P. 126)。 たとえば、ポケットベル属性はポケットベル番号を格納します。

注: CA Identity Manager 環境は 1 つのタイプのユーザ、グループ、および組織オブジェクトのみをサポートします。たとえば、すべてのユーザ オブジェクトには同じオブジェクト クラスがあります。

管理対象オブジェクトの説明

管理対象オブジェクトは、ディレクトリ設定ファイルの User Object、Group Object、および Organization Object セクションのオブジェクト情報を指定することにより説明されます。

注: 設定テンプレート（directory.xml ファイル）を使用するときには、Organization Object セクションは、組織をサポートしないユーザ ディレクトリには使用できません。

これらの各セクションには、以下の例のように ImsManagedObject エレメントが含まれます。

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

オプションで、ImsManagedObject エレメントには、以下の例のように Container エレメントを含むことができます。

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people" />
```

オブジェクト情報の指定

オブジェクト情報はさまざまなパラメータの値を提供することにより指定されます。

次の手順に従ってください:

1. User Object、Organization Object、または Group Object セクションで ImsManagedObject エレメントを検索します。

2. 以下のパラメータの値を提供します。

name

管理対象オブジェクトの一意の名前を指定します。

注: このパラメータは必須です。

description

管理対象オブジェクトの説明が含まれています。

objectclass

オブジェクト タイプ（ユーザ、グループ、または組織）の LDAP オブジェクト クラスの名前を指定します。 オブジェクト クラスは、オブジェクトに使用可能な属性のリストを決定します。

複数のオブジェクト クラスの属性がオブジェクト タイプに適用される場合は、カンマ区切りのリストでオブジェクト クラスを表示します。 たとえば、オブジェクトに person、organizationalperson および inetorgperson オブジェクト クラスの属性が含まれる場合は、以下のようにこれらのオブジェクト クラスを追加します。

objectclass="top,person,organizationalperson,inetorgperson"

各 LDAP ディレクトリには、事前定義済みオブジェクト クラスのセットが含まれます。 事前定義済みオブジェクト クラスの詳細については、ディレクトリ サーバのドキュメントを参照してください。

注: このパラメータは必須です。

objecttype

管理対象オブジェクトのタイプを指定します。 有効な値は以下のとおりです。

- User
- Organization
- Group

注: このパラメータは必須です。

maxrows

ユーザ ディレクトリを検索するときに CA Identity Manager が返すことができるオブジェクトの最大数を指定します。 オブジェクトの数が限度を超えると、エラーが表示されます。

maxrows パラメータに値の設定することにより、検索結果を制限する LDAP ディレクトリ内の設定を無効にすることができます。矛盾する設定が適用される場合、LDAP サーバは優先度の最も低い設定を使用します。

注: maxrows パラメータは、CA Identity Manager タスク画面上に表示されるオブジェクトの数を制限しません。 表示設定を設定するには、CA Identity Manager ユーザ コンソール内のリスト画面定義を変更します。手順については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

maxpagesize

単一の検索で返すことができるオブジェクトの数を指定します。オブジェクトの数がページ サイズを超える場合、CA Identity Manager は複数の検索を実行します。

［Search Page Size］を指定するときは、以下の点に注意してください。

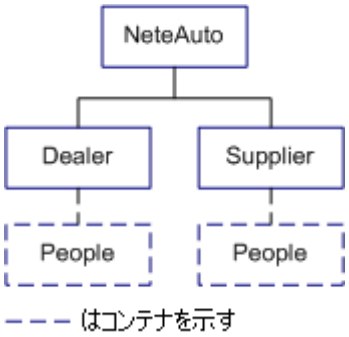
- ［Search Page Size］オプションを使用するには、CA Identity Manager が管理するユーザ ストアでページングがサポートされる必要があります。 一部のユーザ ストア タイプは、ページングをサポートするために追加設定が必要です。詳細については、「大規模な検索のパフォーマンスを改善する方法 (P. 100)」を参照してください。
- ユーザ ストアがページングをサポートせず、maxrows の値も指定される場合、CA Identity Manager は、検索サイズを制御するために maxrows 値のみを使用します。

3. オプションで、コンテナ情報を提供します。

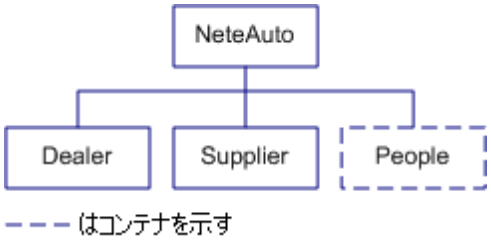
コンテナ

管理を容易に行うために、コンテナ内の特定のタイプのオブジェクトをグループ化できます。ユーザがディレクトリ設定ファイルのコンテナを指定する場合、CA Identity Manager はコンテナ内のエントリのみを管理します。たとえば、以下の図に示すように、ユーザが People という名前のユーザ コンテナを指定する場合、CA Identity Manager は People コンテナ内のユーザを管理します。

- 階層的ディレクトリ



- フラット ディレクトリ



これらの例では、すべてのユーザが People コンテナに存在します。

コンテナを指定する場合は、以下の点に注意してください。

- コンテナが組織に存在しない場合、CA Identity Manager は最初のエントリが追加されるとすぐにコンテナを作成します。 階層的ディレクトリの場合、CA Identity Manager は、エントリが追加される組織にコンテナを作成します。 フラット ディレクトリおよび組織をサポートしない階層的ディレクトリの場合、CA Identity Manager は、検索ルートの下にコンテナを作成します。これは CA Identity Manager ディレクトリの作成時に指定します。
- CA Identity Manager は、指定されたコンテナに存在しないエントリを無視します。 たとえば、People コンテナを指定する場合、People コンテナ以外に存在するユーザを管理することはできません。

  注: 指定されたコンテナに存在しないユーザを管理するには、別の CA Identity Manager 環境を作成します。

コンテナおよび汎用属性

汎用属性は CA Identity Manager で特別な意味を持つ属性です。CA Identity Manager がコンテナを含むユーザ ストアを管理するときに、以下の汎用属性がコンテナに関する情報を識別します。

%ORG_MEMBERSHIP%

コンテナのフル ネーム（DN）を格納する属性を識別します。

たとえば、フル ネームは以下のように示します。

ou=People、ou=Employee、ou=NeteAuto、dc=security、dc=com

%ORG_MEMBERSHIP_NAME%

属性のユーザ フレンドリな名前を格納する属性を識別します。

たとえば、前の例に示すコンテナのユーザ フレンドリな名前は、People です。

これらの汎用属性は、directory.xml ファイルの User Object および Group Object セクションの属性の説明で以下のように表示されます。

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

階層的ユーザ ストア構造の場合、physicalname および wellknown パラメータは、汎用属性に以下のようにマップされます。

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

この例では、directory.xml ファイル内の他の情報から CA Identity Manager がコンテナ DN およびユーザ フレンドリな名前を自動的に引き出すことを示します。

フラット ユーザ ストア構造の場合、物理属性名を提供します。

注: 詳細については、「フラット ユーザ ディレクトリ構造を説明する方法 (P. 90)」を参照してください。

ユーザまたはグループ コンテナの指定

ユーザまたはグループ コンテナを指定するには、以下の手順に従います。

次の手順に従ってください:

1. User Object または Group Object セクションのコンテナ エレメントを検索します。
2. 以下のパラメータの値を提供します。

   objectclass

   特定のタイプのオブジェクトが作成されるコンテナの LDAP オブジェクト クラスを決定します。 たとえば、ユーザ コンテナのデフォルト値は "top,organizationalUnit," で、ユーザが LDAP 組織単位（ou）で作成されることを示します。

   動的またはネスト グループを管理している場合は、必ずこれらのグループ タイプ (P. 92)をサポートするオブジェクト クラスを指定します。

   注: このパラメータは必須です。

   attribute

   コンテナ名（たとえば ou）を格納する属性を指定します。

   この属性は、以下の例のように、コンテナの相対 DN を形成する値とペアになります。

   ou=People

   注: このパラメータは必須です。

   value

   コンテナの名前を指定します。

   注: このパラメータは必須です。

注: 組織のコンテナを指定できません。

属性の説明

属性は、電話番号や住所などのエントリに関する情報を格納します。 エントリ属性はそのプロファイルを決定します。

ディレクトリ設定ファイルで、属性は ImsManagedObjectAttr エレメントで説明されます。 ディレクトリ設定ファイルの User Object、Group Object および Organization Object セクションで、以下のアクションを実行できます。

- ユーザ ストアの属性について説明するには、デフォルトの属性の説明を変更します。
- 既存の説明をコピーし、必要に応じて値を変更することにより、新しい属性の説明を作成します。

ユーザ、グループ、および組織プロファイルの属性ごとに、1 つの ImsManagedObjectAttr エレメントがあります。たとえば、ImsManagedObjectAttr エレメントはユーザ ID として説明されます。

ImsManagedObjectAttr エレメントは以下のコードのようになります。

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%" maxlength="0" />
```

ImsManagedObjectAttr には以下のパラメータがあります。

physicalname

このパラメータには以下のアイテムのいずれかが含まれる必要があります。

- プロファイル値が格納される LDAP 属性の名前。 たとえば、ユーザ ID はユーザ ディレクトリの uid 属性に格納されます。

  注: パフォーマンスを改善するには、ユーザ コンソールの検索クエリで使用される LDAP 属性に対してインデックスを作成します。

- 汎用属性 (P. 82)。 ユーザが汎用属性を提供するときに、CA Identity Manager は値を自動的に計算します。 たとえば、汎用属性 %ORG_MEMBERSHIP% を指定するとすぐに、CA Identity Manager はエントリの DN に基づいてエントリが属している組織を決定します。

description

属性の説明が含まれます。

displayname

属性の一意の名前を指定します。

ユーザ コンソールで、表示名がタスク画面に追加可能な属性のリストに表示されます。 このパラメータは必須です。

注: ディレクトリ設定ファイル（directory.xml）の属性の表示名は変更しないでください。 タスク画面で属性の名前を変更するには、タスク画面定義で属性のラベルを指定することができます。 詳細については、「管理ガイド」を参照してください。

valuetype

属性のデータ型を指定します。 有効な値は以下のとおりです。

String

値は任意の文字列を指定できます。

デフォルト値です。

Integer

値は整数である必要があります。

注: 整数は 10 進数をサポートしません。

Number

値は整数である必要があります。 数値オプションは 10 進数をサポートします。

Date

値は以下のパターンを使用して有効な日付であることを解析する必要があります。

MM/dd/yyyy

ISODate

値はパターン yyyy-MM-dd を使用して、有効な日付であることを解析する必要があります。

UnicenterDate

値はパターン YYYYYYYDDD を使用して、有効な日付であることを解析する必要があります。ここで：

YYYYYYY は、3 つのゼロで始まり、年を示す 7 つの数値表現です。 例： 0002008

DDD は必要に応じて、ゼロで始まり、日付を示す 3 つの数値表現です。 有効な数値範囲は、001 ～ 366 です。

Structured

この種の属性は、単一の属性値が複数の関連する値を格納できるようにする構造化データからなります。 たとえば、構造化属性には、名、姓、電子メール アドレスなどの値が含まれます。

特定のエンドポイント タイプはこれらの属性を使用しますが、CA Identity Manager によって管理されます。

注: CA Identity Manager は、ユーザ コンソールのテーブルに構造化属性を表示できます。 ユーザがテーブルで値を編集する場合、値はユーザ ストアに格納され、エンドポイントに伝搬されます。 multivalued 属性の表示の詳細については、「管理ガイド」を参照してください。

required

属性が必要かどうかを以下のように示します。

- True -- 属性は必要です。
- False -- 属性はオプションです（デフォルト）。

注: 属性が LDAP ディレクトリ サーバに必要な場合は、必要なパラメータを true に設定します。

multivalued

属性が複数値を持つことができるかどうかを示します。 たとえば、グループ メンバシップ属性は各グループ メンバのユーザ DN を格納できるように複数値を設定されます。 有効な値は以下のとおりです。

- True -- 属性は複数値を持つことができます。
- False -- 属性は単一値しか持つことができません（デフォルト）。

重要: ユーザ オブジェクト定義のグループ メンバシップおよび管理ロール属性は複数値である必要があります。

wellknown

汎用属性の名前を定義します。

汎用属性は CA Identity Manager で特別な意味を持ちます (P. 82)。 これらの属性は以下の構文で識別されます。

%ATTRIBUTENAME%

maxlength

属性値が持つことができる最大長を定義します。 無制限の長さを指定するには maxlength パラメータを 0 に設定します。

注: このパラメータは必須です。

permission

属性の値をタスク画面で変更できるかどうかを示します。 有効な値は以下のとおりです。

READONLY

値が表示されますが変更できません。

WRITEONCE

オブジェクトが作成されたら、値は変更できません。 たとえば、ユーザが作成された後で、ユーザ ID を変更できません。

READWRITE

値は変更できます（デフォルト）。

hidden

属性が CA Identity Manager タスク形式で表示されるかどうかを示します。 有効な値は以下のとおりです。

- True -- 属性はユーザに表示されません。
- False -- 属性はユーザに表示されます（デフォルト）。

論理属性は hidden 属性を使用します。

注: 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。

system

CA Identity Manager のみが属性を使用したことを示します。 ユーザ コンソールのユーザは属性を変更できません。 有効な値は以下のとおりです。

- True -- ユーザは属性を変更できません。 属性は CA Identity Manager ユーザ インターフェース内で非表示です。
- False -- ユーザはこの属性を変更できます。 属性は CA Identity Manager ユーザ インターフェースのタスク画面に追加できます。 （デフォルト）

validationruleset

属性と検証ルール セットを関連付けます。

指定する検証ルール セットがディレクトリ設定ファイルの ValidationRuleSet エレメントで定義されていることを確認します。

objectclass

属性が ImsManagedObject エレメントで指定されたプライマリ オブジェクト クラスの一部でない場合に、ユーザ、グループ、または組織属性の LDAP 補助クラスであることを示します。

たとえば、ユーザのプライマリ オブジェクト クラスが、top、person、organizationalperson であると仮定します。これらは以下のユーザ属性を定義します。

- 共通名（cn）
- 姓（sn）
- ユーザ ID （uid）
- パスワード（userPassword）

従業員の補助クラスで定義されている属性 employeeID を含むには、以下の属性の説明を追加します。

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true" multivalued="false"
maxlength="0" objectclass="Employee"/>
```

属性の説明の指定

属性の説明には以下の手順が含まれます。

1. 以下のトピックの関連するセクションを参照します。
   - CA Directory に関する考慮事項 (P. 80)
   - Microsoft Active Directory に関する考慮事項 (P. 81)
   - IBM Directory Server に関する考慮事項 (P. 81)
   - Oracle Internet Directory に関する考慮事項 (P. 82)
2. ディレクトリ設定ファイルの User Object、User Object および Organization Object セクションで、以下のアクションを実行します。
   - ユーザのディレクトリ属性を説明するためにデフォルトの属性の説明を変更します。
   - 既存の説明をコピーし、必要に応じて値を変更することにより、新しい属性の説明を作成します。

   注: 新規の属性の説明が作成され、物理属性が指定されていると仮定します。物理属性は必ず、オブジェクト タイプに対して指定したオブジェクト クラスに存在する必要があります。
3. （オプション）ユーザ コンソールで、パスワードまたは給料などの機密情報を表示しないようにするために属性の表示設定を変更 (P. 77) します。
4. （オプション）デフォルトの並べ替え順を設定します。
5. フラット ユーザ構造のディレクトリ、あるいは組織を含まないディレクトリを管理する場合は、「ユーザ ディレクトリ構造の説明 (P. 90)」に移動します。

Sensitive 属性の管理

CA Identity Manager では、sensitive 属性を管理するための以下の方法を提供します。

- 属性のデータ分類

  データ分類により、ディレクトリ設定ファイル（directory.xml）でユーザが属性の表示および暗号化のプロパティを指定できます。

  以下のように sensitive 属性を管理するデータ分類を定義できます。

  - CA Identity Manager タスク画面で、一連のアスタリスクとして属性の値を表示します。

    たとえば、パスワードをクリア テキストで表示する代わりにアスタリスクとして表示できます。

  - ［サブミット済みタスクの表示］画面で、属性値を非表示にします。

    このオプションにより、属性を管理者に表示しないようにすることができます。 たとえば、CA Identity Manager 内でタスク ステータスを表示するが、給与詳細を表示する必要のない管理者に給与などの詳細を見せないようにすることなどです。

  - 既存のオブジェクトのコピーを作成するときには、特定の属性を無視します。

  - 属性を暗号化します

- タスク プロファイル画面のフィールド スタイル

  directory.xml ファイル内の属性を変更しない場合は、sensitive 属性が表示される画面定義で属性の表示プロパティを設定します。

  フィールド スタイルにより、クリア テキストの代わりに一連のアスタリスクとして、パスワードなどの属性を表示できます。

  注: sensitive 属性のフィールド スタイルの詳細については、ユーザ コンソール ヘルプでフィールド スタイルを検索してください。

データ分類属性

データ分類エレメントは、属性の説明と追加のプロパティを関連付ける方法を提供します。 このエレメントの値は、CA Identity Manager が属性を処理する方法を決定します。 このエレメントは以下のパラメータをサポートします。

- sensitive

  CA Identity Manager は、［サブミット済みタスクの表示］画面で一連のアスタリスク（*）として属性を表示できます。 このパラメータは、属性の古い値と新しい値が［サブミット済みタスクの表示］画面にクリア テキストで表示されないようにします。

  また、ユーザ コンソールで既存のユーザのコピーを作成する場合、このパラメータは属性が新規ユーザにコピーされないようにします。

- vst_hide

  ［サブミット済みタスクの表示］タブの［イベント詳細］画面の属性を非表示にします。 sensitive 属性（アスタリスクとして表示される）とは異なり、vst_hidden 属性は表示されません。

  このパラメータを使用して、給料などの属性への変更が［サブミット済みタスクの表示］で表示されないようにすることができます。

- ignore_on_copy

  管理者がユーザ コンソールでオブジェクトのコピーを作成するときに、CA Identity Manager は属性を無視します。 たとえば、ユーザ オブジェクト上のパスワード属性に対して ignore_on_copy を指定したと仮定します。ユーザ プロファイルをコピーするときに、CA Identity Manager は新規ユーザ プロファイルに現在のユーザのパスワードを適用しません。

- AttributeLevelEncrypt

  属性値をユーザ ストアに格納すると、それらを暗号化します。 CA Identity Manager で FIPS 140-2 が有効になっている場合、CA Identity Manager は RC2 暗号化または FIPS 140-2 暗号化を使用します。

  CA Identity Manager での FIPS 140-2 サポートの詳細については、「*設定ガイド*」を参照してください。

  属性はランタイム中にクリア テキストで表示されます。

  注: 属性がクリア テキストで画面に表示されないようにするために、機密データ分類エレメントを暗号化された属性に追加することもできます。 詳細については、「属性レベルの暗号化の追加方法 (P. 78)」を参照してください。

- PreviouslyEncrypted

  CA Identity Manager がユーザ ストアのオブジェクトにアクセスするときに、暗号化された値を検出し、復号化します。

  このデータ分類を使用して、以前に暗号化された値を復号化します。

  オブジェクトを保存するときに、クリア テキスト値がストアに保存されます。

データ分類属性の設定

次の手順に従ってください:

1. ディレクトリ設定ファイルの属性を検索します。
2. 属性の説明の後で、以下の属性を追加します。

   <DataClassification name="*parameter*">

   parameter

   以下のいずれかのパラメータを示します。

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   たとえば、vst_hide データ分類属性が含まれる属性の説明は以下のコードのようになります。

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Attribute-Level 暗号化

ユーザ ストアの属性を暗号化するには、ディレクトリ設定ファイル（directory.xml）でその属性用の AttributeLevelEncypt データ分類を指定することにより行います。属性レベルの暗号化が有効な場合、CA Identity Manager では、ユーザ ストアにその属性の値を格納する前にそれを暗号化します。 属性はユーザ コンソールでクリア テキストとして表示されます。

注: 属性がクリア テキストで画面に表示されないようにするために、機密データ分類エレメントを暗号化された属性に追加することもできます。詳細については、「属性レベルの暗号化を削除する方法 (P. 78)」を参照してください。

FIPS 140-2 サポートが有効な場合、属性は RC2 暗号化または FIPS 140-2 暗号化を使用して暗号化されます。

属性レベルの暗号化を実装する前に、以下の点に注意してください。

- CA Identity Manager では、検索で暗号化された属性を検出できません。

  暗号化された属性は、メンバ、管理者、所有者のポリシーまたはアイデンティティ ポリシーに追加されたものとみなされます。 CA Identity Manager では属性を検索できないため、ポリシーを正しく解決できません。

  directory.xml ファイルで属性を searchable="false" に設定することを検討してください。例：

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- CA Identity Manager が共有されたユーザ ストアおよびプロビジョニング ディレクトリを使用する場合は、プロビジョニング サーバ属性を暗号化しないでください。
- 以下の条件を満たす環境のユーザ パスワード用の AttributeLevelEncrypt を有効化しないでください。
  - CA SiteMinder の統合を含み、かつ、
  - リレーショナル データベースにユーザが格納されている

  CA Identity Manager が CA SiteMinder と統合されている場合、新規ユーザがログインを試行して、クリア テキストでパスワードを入力すると、暗号化されたパスワードによって問題が発生します。
- CA Identity Manager 以外のアプリケーションによって使用されるユーザ ストアの属性レベルの暗号化を有効にする場合、他のアプリケーションは暗号化された属性を使用できません。

属性レベルの暗号化の追加方法

CA Identity Manager ディレクトリへの属性レベルの暗号化を追加したと仮定します。 属性と関連付けられるオブジェクトを保存する場合、CA Identity Manager は既存のクリア テキスト属性値を自動的に暗号化します。たとえば、ユーザのプロファイルを保存する場合、パスワード属性を暗号化することによって、パスワードが暗号化されます。

注: 属性値を暗号化するには、オブジェクトを保存するために使用するタスクに属性が含まれている必要があります。前の例のパスワード属性を暗号化するには、オブジェクトを保存するために使用するタスク（［ユーザの変更］タスクなど）にパスワード フィールドが追加されていることを確認します。

新規オブジェクトはすべてユーザ ストアに暗号化された値で作成されます。

次の手順に従ってください:

1. 以下のいずれかのタスクを実行します。
   - CA Identity Manager ディレクトリの作成
   - ディレクトリ設定をエクスポートすることによる既存のディレクトリの更新
2. directory.xml ファイルで暗号化する属性に以下のデータ分類属性を追加します。

   AttributeLevelEncrypt

   ユーザ ストア内で暗号化された形式で属性を保持します。

   sensitive（**オプション**）

   CA Identity Manager 画面で属性値を非表示にします。 たとえば、パスワードはアスタリスク （*） として表示されます。

   例：

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false"
   multivalued="false" maxlength="0" searchable="false">
   <DataClassification name="AttributeLevelEncrypt"/>
   <DataClassification name="sensitive"/>
   ```
3. CA Identity Manager ディレクトリを作成している場合は、環境とディレクトリを関連付けます。
4. CA Identity Manager ですべての値を直ちに暗号化するには、Bulk Loader を使用して、すべてのオブジェクトを変更します。

   注: Bulk Loader の詳細については、「管理ガイド」を参照してください。

属性レベルの暗号化を削除する方法

CA Identity Manager ディレクトリに暗号化された属性があり、それがクリア テキストとしてその属性の値と共に保存される場合、AttributeLevelEncrypt データ分類を削除できます。

データ分類が削除されたら、CA Identity Manager では、新規属性値を暗号化しなくなります。 ユーザが属性と関連付けられるオブジェクトを保存する場合には、既存の値が復号化されます。

注: 属性値を復号化するには、オブジェクトの保存に使用するタスクに属性が含まれている必要があります。 たとえば、既存ユーザに対してパスワードを復号化するには、パスワード フィールドが含まれるタスク（［ユーザの変更］タスクなど）と共にユーザ オブジェクトを保存します。

CA Identity Manager で属性用のユーザ ストアに残るすべての暗号化された値を検出し、復号化するようにするには、別のデータ分類、PreviouslyEncrypted を指定できます。ユーザがオブジェクトを保存するときには、クリア テキスト値がユーザ ストアに保存されます。

注: PreviouslyEncrypted データ分類を追加すると、すべてのオブジェクト ロードにおいて余分な処理が追加されます。パフォーマンス上の問題が発生するのを防ぐため、PreviouslyEncrypted データ分類を追加し、その属性に関連付けられる各オブジェクトをロードおよび保存してから、そのデータ分類を削除することを検討します。この方法により、すべての暗号化されて格納されている値を格納されているクリア テキストに自動的に変換されます。

次の手順に従ってください:

1. 適切な CA Identity Manager ディレクトリ用のディレクトリ設定をエクスポートします。
2. directory.xml ファイルで、復号化する属性から、データ分類 AttributeLevelEncrypt を削除します。
3. CA Identity Manager に以前に暗号化された値を強制的に削除させる場合は、PreviouslyEncrypted データ分類属性を追加します。

   例 :

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. CA Identity Manager に強制的にすべての値を直ちに復号化させるには、Bulk Loader を使用して、オブジェクトをすべて変更します。

   注: Bulk Loader の詳細については、「管理ガイド」を参照してください。

CA Directory に関する考慮事項

CA Directory ユーザ ストア用の属性を説明する場合は、以下の点に注意してください。

- 属性名は大文字と小文字を区別します。
- 管理者がグループを作成するときに、自己登録グループを示す属性として seeAlso 属性を使用するとエラーが発生する場合があります。

管理者がユーザを作成するときに、ユーザ アカウントのステータス（有効または無効）を示す属性として photo 属性を使用するとエラーが発生する場合があります。

注: CA Directory 要件の詳細については、CA Directory のマニュアルを参照してください。

Microsoft Active Directory に関する考慮事項

Active Directory の属性を説明する場合は、以下の点に注意してください。

- 属性の説明で指定された属性の大文字と小文字は、Active Directory で属性の大文字と小文字と一致する必要があります。 たとえば、ユーザ パスワードを格納する属性として unicodePwd 属性を選択する場合、ディレクトリ設定ファイルで unicodePwd （大文字の P を持つ）を指定します。
- ユーザおよびグループ オブジェクトの場合、sAMAccountName 属性が含まれていることを確認します。

IBM Directory Server に関する考慮事項

IBM Directory Server ユーザ ディレクトリの属性を説明する場合は、以下のセクションを参照してください。

- Directory Server ディレクトリのグループ (P. 81)
- 組織オブジェクトの説明の「トップ」オブジェクト クラス (P. 82)

Directory Server ディレクトリのグループ

IBM Directory Server には、グループに少なくとも 1 つのメンバが含まれる必要があります。 この要件に対応するため、グループを作成するときに、CA Identity Manager は新規グループのメンバとしてダミーのユーザを追加します。

ダミー ユーザの設定

次の手順に従ってください:

1. ディレクトリ設定ファイルの Group Object セクションで、以下のエレメントを検索します。

```
<PropertyDict name="DUMMY_USER">
    <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
</PropertyDict>
```

注: これらのエレメントがディレクトリ設定ファイルに存在しない場合は、ここで表示されるとおりに追加します。

2. ##DUMMY_USER_DN をユーザ DN と置き換えます。CA Identity Manager はすべての新規グループのメンバとしてこの DN を追加します。

   注: 既存ユーザの DN を指定する場合、そのユーザは CA Identity Manager のすべてのグループのメンバとして表示されます。ダミーのユーザがグループ メンバとして表示されないようにするには、ディレクトリに存在しない DN を指定します。

3. ディレクトリ設定ファイルを保存します。

組織オブジェクトの説明のトップ オブジェクト クラス

重要: ディレクトリ設定ファイルの組織オブジェクトの説明には、top オブジェクト クラスを含めないでください。

たとえば、組織オブジェクトのオブジェクト クラスが top, organizationalUnit である場合、以下のようにオブジェクト クラスを指定します。

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

top が含まれると、予期しない検索結果が生じる可能性があります。

Oracle Internet Directory に関する考慮事項

Oracle Internet Directory （OID）ユーザ ストアの属性を説明する場合は、小文字のみを使用して、LDAP 属性を指定します。

LDAP ユーザ用の汎用属性

汎用属性は CA Identity Manager で特別な意味があります。 これらの属性は、以下の構文で示されるように識別されます。

%ATTRIBUTENAME%

この構文で、*ATTRIBUTENAME* は大文字である必要があります。

汎用属性は属性の説明 (P. 126)を使用して、1 つの物理属性にマップされます。

以下の属性の説明では、属性 userpassword は、CA Identity Manager がパスワードとして userpassword の値を処理できるように、汎用属性 %PASSWORD% にマップされます。

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

汎用属性は必須のものもあれば、オプションのものもあります。

ユーザの既知の属性

ユーザの既知の属性と、属性がマップされる項目を以下に示します。

%ADMIN_ROLE_CONSTRAINT%

管理者の管理ロールのリストにマップされます。

%ADMIN_ROLE_CONSTRAINT% にマップされた物理属性は、複数のロールを持てるよう、複数値に対応している必要があります。

%ADMIN_ROLE_CONSTRAINT% にマップされる LDAP 属性にインデックスを付けることをお勧めします。

%CERTIFICATION_STATUS%

ユーザの認証ステータスにマップされます。

この属性はユーザの認証機能を使用するために必要です。

注: ユーザ認証の詳細については、「管理ガイド」を参照してください。

%DELEGATORS%

現在のユーザに作業アイテムを委任したユーザのリストにマップします。

この属性は委任を使用するのに必要です。%DELEGATORS% にマップした物理属性は複数値で、文字列を保持できる必要があります。

重要: CA Identity Manager タスクまたは外部ツールを使用してこのフィールドを直接編集すると、重大なセキュリティ上の影響が生じる場合があります。

%EMAIL%

ユーザの電子メール アドレスにマップされます。

電子メール通知機能を使用するために必要です。

%ENABLED_STATE%

（必須）

ユーザのステータスにマップされます。

注: この属性は SiteMinder ユーザ ディレクトリ接続内の無効フラグ ユーザ ディレクトリ属性と一致する必要があります。

%FIRST_NAME%

ユーザの名にマップされます。

%FULL_NAME%

ユーザの姓と名にマップされます。

%IDENTITY_POLICY%

ユーザ アカウントに適用されたアイデンティティ ポリシーのリスト、および、そのユーザ オブジェクトに対して追加または削除アクションを行った一意の Policy Xpress ポリシー ID のリストを指定します。

CA Identity Manager は、この属性を使用して、ユーザに対するアイデンティティ ポリシーの適用が必要かどうか決定します。このポリシーには、一回のみ適用設定が有効化され、また、ポリシーは、%IDENTITY_POLICY% 属性にリストされていることが前提されています。 CA Identity Manager では、ポリシーの変更はユーザに適用されません。

注: アイデンティティ ポリシーの詳細については、「*管理ガイド*」を参照してください。

%LAST_CERTIFIED_DATE%

ユーザに対してロールが認証される日付にマップされます。

ユーザの認定機能を使用するために必要です。

注: ユーザ認証の詳細については、「*管理ガイド*」を参照してください。

%LAST_NAME%

ユーザの姓にマップされます。

%MEMBER_OF%

ユーザがメンバであるグループのリストにマップされます。

%MEMBER_OF% にマップされた物理属性は、複数のグループを持てるように、複数値に対応している必要があります。

この属性を使用すると、ユーザのグループを検索する際の応答時間が短縮されます。

この属性は、Active Directory、またはユーザ オブジェクトのユーザ グループ メンバシップを管理するあらゆるディレクトリ スキーマで使用できます。

%ORG_MEMBERSHIP%

（必須）

ユーザが所属する組織の DN にマップされます。

CA Identity Manager は、この既知の属性を使用して、ディレクトリの構造 (P. 90)を決定します。

ユーザ ディレクトリに組織が含まれていない場合、この属性は必要ではありません。

%ORG_MEMBERSHIP_NAME%

（必須）

ユーザのプロファイルが存在する組織の、ユーザ フレンドリな名前にマップされます。

ユーザ ディレクトリに組織が含まれていない場合、この属性は必要ではありません。

%PASSWORD%

ユーザのパスワードにマップされます。

この属性は SiteMinder ユーザ ディレクトリ接続のパスワード属性と一致する必要があります。

注: CA Identity Manager 画面内では、%PASSWORD% 属性の値は、常にアスタリスク（*）文字の連続として表示されます。パスワードの非表示設定が属性やフィールドに対して指定されていない場合も同様です。

%PASSWORD_DATA%

（パスワード ポリシーのサポートに必須）

パスワード ポリシー情報を追跡する属性を指定します。

注: CA Identity Manager 画面内では、%PASSWORD_DATA% 属性の値は、常にアスタリスク（*）文字の連続として表示されます。パスワードの非表示設定が属性やフィールドに対して指定されていない場合も同様です。

%PASSWORD_HINT%

（必須）

ユーザが指定した質問と回答のペアにマップされます。 質問と回答のペアは、ユーザがパスワードを忘れた場合に使用されます。

複数の質問と回答のペアをサポートするには、%PASSWORD_HINT% 属性が複数の値を持てるように指定してください。

パスワードの管理用に SiteMinder のパスワード サービス機能を使用している場合、パスワード のヒント属性は、SiteMinder ユーザ ディレクトリの チャレンジ/レスポンス属性と一致している必要があります。

注: CA Identity Manager 画面内では、%PASSWORD% 属性の値は、常にアスタリスク（*）文字の連続として表示されます。パスワードの非表示設定が属性やフィールドに対して指定されていない場合も同様です。

%USER_ID%

（必須）

ユーザの ID にマップされます。

グループ汎用属性

以下のアイテムはグループ汎用属性のリストです。

%GROUP_ADMIN_GROUP%

どの属性がグループの管理者であるグループのリストを格納するかを示します。 たとえば、グループ 1 がグループ A の管理者である場合、グループ 1 は %GROUP_ADMIN_GROUP% 属性に格納されます。

注: ユーザが %GROUP_ADMIN_GROUP% 属性を指定しない場合、CA Identity Manager は %GROUP_ADMIN% 属性に管理者グループを格納します。

注: 別のグループの管理者としてグループを追加するには、「管理ガイド」を参照してください。

%GROUP_ADMIN%

どの属性にグループの管理者の DN が含まれるかを示します。

%GROUP_ADMIN% にマップされる物理属性は複数値である必要があります。

%GROUP_DESC%

どの属性にグループの説明が含まれるかを示します。

%GROUP_MEMBERSHIP%

（必須）

どの属性にグループのメンバのリストが含まれるかを示します。

%GROUP_MEMBERSHIP% にマップされる物理属性は複数値である必要があります。

%GROUP_MEMBERSHIP% 汎用属性はプロビジョニング ユーザ ディレクトリには必要ありません。

%GROUP_NAME%

（必須）

どの属性がグループ名を格納するかを示します。

%ORG_MEMBERSHIP%

（必須）

どの属性にグループが属している組織の DN が含まれるかを示します。

CA Identity Manager は、この汎用属性を使用して、ディレクトリの構造 (P. 90)を決定します。

ユーザ ディレクトリに組織が含まれない場合、この属性は必要ではありません。

%ORG_MEMBERSHIP_NAME%

どの属性にグループが存在する組織のユーザ フレンドリな名前が含まれるかを示します。

この属性は、組織が含まれないユーザ ディレクトリには無効です。

%SELF_SUBSCRIBING%

ユーザがグループ (P. 89)に参加できるかどうかをどの属性が決定するかを示します。

%NESTED_GROUP_MEMBERSHIP%

どの属性がグループのメンバであるグループのリストを格納するかを示します。 たとえば、グループ 1 がグループ A のメンバである場合、グループ 1 は %NESTED_GROUP_MEMBERSHIP% 属性に格納されます。

ユーザが %NESTED_GROUP_MEMBERSHIP% 属性を指定しない場合、CA Identity Manager は %GROUP_MEMBERSHIP% 属性にネスト グループを格納します。

他のグループのメンバとしてグループを含めるには、「動的およびネスト グループの設定」の説明に従って、ネスト グループに対するサポートを設定します。

%DYNAMIC_GROUP_MEMBERSHIP%

どの属性が動的グループ (P. 153)を生成する LDAP クエリを格納するかを示します。

注: %NESTED_GROUP_MEMBERSHIP% および %DYNAMIC_GROUP_MEMBERSHIP% 属性を含めるように、グループ オブジェクトで使用可能な属性を拡張するには、補助オブジェクト クラスを使用できます。

組織の汎用属性

以下の汎用属性は、組織をサポートする環境にのみ適用されます。

%ORG_DESCR%

どの属性に組織の説明が含まれるかを示します。

%ORG_MEMBERSHIP%

（必須）

どの属性に組織の親組織の DN が含まれるかを示します。

%ORG_MEMBERSHIP_NAME%

どの属性に組織の親組織のユーザ フレンドリな名前が含まれるかを示します。

%ORG_NAME%

（必須）

どの属性に組織の名前が含まれるか示します。

%ADMIN_ROLE_CONSTRAINT% 属性

管理ロールを作成するときに、ロール メンバシップの 1 つ以上のルールを指定します。メンバシップ ルールを満たすユーザはロールを付与されます。たとえば、ユーザ マネージャ ロールのメンバシップ ルールが title=User Manager である場合、「ユーザ マネージャ」というタイトル持つユーザがユーザ マネージャ ロールを所有します。

注: ルールの詳細については、「管理ガイド」を参照してください。

%ADMIN_ROLE_CONSTRAINT% により、管理者の管理ロールを格納するにプロファイル属性を指定できます。

%ADMIN_ROLE_CONSTRAINT% 属性を使用する方法

すべての管理ロールの制約として %ADMIN_ROLE_CONSTRAINT% を使用するには、以下のタスクを実行します。

- 複数のロールに対応できるように、%ADMIN_ROLE_CONSTRAINT% 汎用属性を複数値プロファイル属性とペアにします。
- ユーザ コンソールで管理ロールを設定する場合は、以下の制約について確認してください。

  管理ロールは*ロール名*と等しい

  ロール名

  以下の例のように、制約を提供しているロールの名前を定義します。

  管理ロールはユーザ マネージャと等しい

注: 管理ロールは %ADMIN_ROLE_CONSTRAINT% 属性のデフォルトの表示名です。

汎用属性 の設定

汎用属性を設定するには、以下の手順に従います。

次の手順に従ってください:

1. ディレクトリ設定ファイルで、以下の記号を検索します。

   ##
2. ## から始まる値を適切な LDAP 属性で置き換えます。
3. 必要な値をすべて置き換えるまで、手順 1 および 2 を繰り返します。

4. 必要に応じて、オプションの汎用属性を物理属性にマップします。
5. ディレクトリ設定ファイルを保存します。

ユーザ ディレクトリ構造の説明

CA Identity Manager は %ORG_MEMBERSHIP% 汎用属性を使用して、ユーザ ディレクトリの構造を決定します。

ユーザ ディレクトリ構造を説明する手順は、ディレクトリ構造のタイプによって異なります。

階層的ディレクトリ構造を説明する方法

ディレクトリ設定ファイルは、階層的ディレクトリ構造用にすでに設定されています。その結果、%ORG_MEMBERSHIP% 属性の説明を変更する必要はありません。

フラット ユーザ ディレクトリ構造を説明する方法

次の手順に従ってください:

1. directory.xml ファイルの User Object セクションにある %ORG_MEMBERSHIP% 属性説明を検索します。
2. physicalname パラメータで、%ORG_MEMBERSHIP% をユーザが属する組織を格納する属性の名前で置き換えます。

フラット ディレクトリ構造を説明する方法

次の手順に従ってください:

1. directory.xml ファイルの User Object セクションにある %ORG_MEMBERSHIP% 属性説明を検索します。
2. physicalname パラメータで、%ORG_MEMBERSHIP% をユーザが属する組織を格納する属性の名前で置き換えます。
3. グループ オブジェクト セクションの手順 1 を繰り返します。
4. physicalname パラメータで、%ORG_MEMBERSHIP% をグループが属する組織を格納する属性の名前で置き換えます。

組織をサポートしないユーザ ディレクトリを説明する方法

オブジェクトの説明または汎用属性が directory.xml の組織に対して定義されていないことを確認します。

グループの設定方法

設定するために、グループを以下のように分割できます。

- 自己登録グループ
- 動的およびネスト グループ

自己登録グループの設定

ディレクトリ設定ファイルで自己登録グループのサポートを設定することにより、セルフサービス ユーザがグループに参加できるようになります。

ユーザが自己登録する場合、CA Identity Manager は指定された組織のグループを検索し、ユーザに自己登録グループを表示します。

次の手順に従ってください:

1. 自己登録グループ セクションで、以下のように SelfSubscribingGroups エレメントを追加します。

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. 以下のパラメータの値を追加します。

   type

   CA Identity Manager が自己登録グループをどこで検索するかを以下のように示します。

   - NONE -- CA Identity Manager はグループを検索しません。 グループにユーザが自己登録できないようにするには NONE を指定します。
   - ALL -- CA Identity Manager はルートでグループの検索を始めます。 ユーザが階層ディレクトリ全体のグループに参加できる場合は、ALL を指定します。

- INDICATEDORG -- CA Identity Manager はユーザの組織およびそのサブ組織内の自己登録グループを検索します。 たとえば、ユーザのプロファイルがマーケティング組織にある場合、CA Identity Manager は、マーケティング組織、およびそのすべてのサブ組織内の自己登録グループを検索します。
- SPECIFICORG -- CA Identity Manager は特定の組織を検索します。org パラメータの特定の組織の識別名（DN）を提供します。

org

CA Identity Manager が自己登録グループを検索する組織の一意の識別子を指定します。

注: type=SPECIFICORG の場合、必ず org パラメータを指定してください。

自己登録グループのサポートが CA Identity Manager ディレクトリで設定されれば、CA Identity Manager 管理者はどのグループがユーザ コンソールで自己登録しているかを指定できます。

注: グループの管理の詳細については、「管理ガイド」を参照してください。

動的およびネスト グループの設定

LDAP ユーザ ストアを管理する場合は、ディレクトリ設定ファイルで以下のタイプのグループに対するサポートを設定できます。

ダイナミック グループ

ユーザ コンソールで LDAP フィルタ クエリを動的に指定することにより、グループ メンバシップを定義できます。動的グループの場合、管理者は、グループ メンバを個別に検索したり、追加したりする必要はありません。

ネスト グループ

他のグループのメンバとしてグループを追加できます。

ディレクトリ設定ファイルを使用して、動的およびネスト グループを有効にできます。

次の手順に従ってください:

1. 必要に応じて、以下の汎用属性 (P. 86)をグループ管理対象オブジェクトの物理属性にマップします。
   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   注: 選択する物理属性は複数値をサポートする必要があります。
2. ［ディレクトリ グループ動作］セクションで、以下の GroupTypes エレメントを追加します。

   <GroupTypes type=*group*>

   注: GroupTypes では、大文字と小文字が区別されます。
3. 以下のパラメータの値を入力します。

   group

   動的およびネスト グループのサポートを有効にします。 有効な値は以下のとおりです。
   - NONE -- CA Identity Manager は動的およびネスト グループをサポートしません。
   - ALL -- CA Identity Manager は動的およびネスト グループをサポートします。
   - DYNAMIC -- CA Identity Manager は動的グループのみをサポートします。
   - NESTED -- CA Identity Manager はネスト グループのみをサポートします。

動的およびネスト グループのサポートが CA Identity Manager ディレクトリで設定されれば、CA Identity Manager 管理者は、ユーザ コンソールでどのグループが動的で、ネストされているかを指定できます。

注: %NESTED_GROUP_MEMBERSHIP% 汎用パラメータを設定しないで、グループ タイプを NESTED または ALL に設定していることを検討します。 そのような場合、CA Identity Manager は、%GROUP_MEMBERSHIP% 汎用パラメータに、ネストされたグループとユーザの両方を格納します。そのため、グループ メンバシップの処理がわずかに低速になる場合があります。

グループの管理者としてのグループに対するサポートの追加

LDAP ユーザ ストアを管理している場合、グループを他のグループの管理者とすることができます。 管理者としてグループを割り当てる場合、そのグループの管理者のみが指定されたグループの管理者となります。指定する管理者グループのメンバは、グループを管理する権限がありません。

次の手順に従ってください:

1. %GROUP_ADMIN_GROUP% 汎用属性を管理者となるグループのリストを格納する物理属性にマップします。

   注: 選択する物理属性は複数値をサポートする必要があります。

   グループ汎用属性 (P. 86)は、%GROUP_ADMIN_GROUP% 属性に関する詳細情報を提供します。

   注: %GROUP_ADMIN_GROUP% 汎用属性を設定しないで、管理グループ タイプを ALL に設定した場合、CA Identity Manager は %GROUP_ADMIN% 属性に管理者グループを格納します。

2. Directory AdminGroups Behavior セクションで、以下のように AdminGroupTypes エレメントを設定します。

   <AdminGroupTypes type="ALL">

   デフォルトの AdminGroupTypes は NONE です。

   注: AdminGroupTypes では、大文字と小文字が区別されます。

管理者としてのグループのサポートが CA Identity Manager ディレクトリで設定されれば、CA Identity Manager 管理者はユーザ コンソールでグループを他のグループの管理者として指定できます。

検証ルール

検証ルールは、ユーザがタスク画面フィールドに入力するデータに関する要件を適用します。要件にはデータ型または形式を適用することができます。 したがって、データがタスク画面上の他のデータのコンテキストで有効であるかどうかを確認します。

検証ルールはプロファイル属性と関連付けられます。 CA Identity Manager は、タスクを処理する前に、プロファイル属性に入力されたデータが関連する検証ルールを満たしていることを確認します。

検証ルールを定義し、それらをディレクトリ設定ファイルのプロファイル属性と関連付けることができます。

追加の CA Identity Manager ディレクトリのプロパティ

以下の追加のプロパティを設定できます。

- 検索結果の順序を並べ替える。
- オブジェクト クラスを検索し、新規ユーザが存在しないことを確認する。
- マスタ LDAP ディレクトリからスレーブ LDAP ディレクトリへのデータのレプリケーションを完了するまでに CA Identity Manager がタイムアウトにならないように待機する。

並べ替え順序の設定

ユーザ、グループ、組織など、各管理対象オブジェクトの並べ替え属性を指定できます。 CA Identity Manager は、この属性を使用して、CA Identity Manager API を使用して作成するカスタム ビジネス ロジックで検索結果を並べ替えます。

注: 並べ替え属性は、検索結果がユーザ コンソールで表示される方法に影響しません。

たとえば、ユーザ オブジェクトに対して cn 属性を指定する場合、CA Identity Manager はユーザの検索結果を cn 属性のアルファベット順に並べ替えます。

次の手順に従ってください:

1. 並べ替え順序が適用される管理対象オブジェクトのセクションの最後の IMSManagedObjectAttr エレメントの後に、以下のステートメントを追加します。

```
<PropertyDict name="SORT_ORDER">
    <Property name="ATTR">your_sort_attribute
    </Property>
</PropertyDict>
```

2. *your_sort_attribute* を CA Identity Manager が検索結果を並べ替える属性と置き換えます。

注: 1 つの物理属性をのみを指定します。 汎用属性を指定しないでください。

たとえば、cn 属性の値に基づいてユーザの検索結果を並べ替える必要があると仮定します。 ディレクトリ設定ファイルの User Object セクションの最後の IMSManagedObjectAttr エレメントの後に以下のエレメントを追加します。

```
<!-- ******************* User Object ******************* -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

オブジェクト クラスの検索

CA Identity Manager は、ユーザの作成時に、ユーザを検索し、ユーザが存在するかどうかを確認します。 この検索は、ディレクトリ設定ファイル（directory.xml）内のユーザ オブジェクト定義でオブジェクト クラスを指定しているユーザに制限されます。既存ユーザがそれらのオブジェクト クラスで見つからない場合、CA Identity Manager はユーザを作成しようとします。

ユーザが同じ一意の識別子（ユーザ ID）を持つがオブジェクト クラスが異なる場合、LDAP サーバはユーザを作成できません。 エラーは LDAP サーバでレポートされますが、CA Identity Manager はエラーを認識できません。 CA Identity Manager にはユーザが正常に作成されているように見えます。

この問題を防ぐために、既存のユーザを確認するときに CA Identity Manager がオブジェクト クラス定義全体にわたってユーザを検索できるように SEARCH_ACROSS_CLASSES プロパティを設定できます。

注: ユーザを作成するなどのタスクを実行する場合、このプロパティは、重複ユーザの検索にのみ影響を及ぼします。他のすべての検索に対して、オブジェクト クラスの制約が適用されます。

次の手順に従ってください:

1. ディレクトリ設定ファイル（directory.xml）で、ユーザ オブジェクトについて説明する ImsManagedObject エレメントを検索します。

2. 以下の PropertyDict エレメントを追加します。

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

注: 以下の例のように、PropertyDict エレメントは ImsManagedObject エレメントの最後のエレメントである必要があります。

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
description="Department" valuetype="String" required="true"
multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

レプリケーション待機時間の指定

マスタおよびスレーブ LDAP ディレクトリ間のレプリケーションが含まれる展開では、SiteMinder ポリシー サーバがスレーブ ディレクトリと通信できるように設定できます。 この設定で、ポリシー サーバは、LDAP ディレクトリにデータを書き込む操作中にマスタ ディレクトリを指す参照を自動的に検出します。データはマスタ LDAP ディレクトリに格納され、ユーザのネットワーク リソースのレプリケーション スキームに従ってスレーブ LDAP ディレクトリに複製されます。

この設定で、ユーザが CA Identity Manager でオブジェクトを作成するときに、オブジェクトはマスタ ディレクトリで作成され、また、スレーブ ディレクトリにも複製されます。 レプリケーション プロセス中に遅延が発生すると、CA Identity Manager で作成アクションが失敗する可能性があります。

この問題が発生するのを防ぐために、REPLICATION_WAIT_TIME プロパティで CA Identity Manager が「タイムアウトする」まで待機する時間（秒単位）を指定できます。

次の手順に従ってください:

1. ディレクトリ設定ファイル（directory.xml）で、ユーザ オブジェクトについて説明する ImsManagedObject エレメントを検索します。
2. 以下の PropertyDict エレメントを追加します。

```
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME><time in seconds></Property>
</PropertyDict>
```

注: 以下の例のように、PropertyDict エレメントは ImsManagedObject エレメントの最後のエレメントである必要があります。

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
description="Department" valuetype="String" required="true"
multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME>800</Property>
</PropertyDict>
```

レプリケーション待機時間が定義されない場合は、デフォルト値 0 が使用されます。

LDAP 接続設定の指定

パフォーマンスを改善するには、ディレクトリ設定ファイル（directory.xml）で以下のパラメータを指定できます。

Connection Timeout

CA Identity Manager がディレクトリの検索を終了するまで最大時間（ミリ秒）を指定します。

このプロパティは、ディレクトリ設定ファイルで以下のように指定されます。

com.sun.jndi.ldap.connect.timeout

Connection Pool Max Size

CA Identity Manager が LDAP ディレクトリで行うことができる接続の最大数を指定します。

このプロパティは、ディレクトリ設定ファイルで以下のように指定されます。

com.sun.jndi.ldap.connect.pool.maxsize

Connection Pool Default Size

CA Identity Manager と LDAP ディレクトリ間のデフォルトの接続数を指定します。

このプロパティは、ディレクトリ設定ファイルで以下のように指定されます。

com.sun.jndi.ldap.connect.pool.prefsize

次の手順に従ってください:

1. ディレクトリ設定ファイル（directory.xml）で、ユーザ オブジェクトについて説明する ImsManagedObject エレメントを検索します。
2. 以下の PropertyDict エレメントを追加します。

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection
Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. directory.xml ファイルを保存します。

   このファイルで CA Identity Manager ディレクトリを作成するときに、CA Identity Manager はこれらの設定を設定します。

ディレクトリ検索のパフォーマンスを改善する方法

ユーザ、組織、およびグループのディレクトリ検索のパフォーマンスを改善するには、以下を行ってください。

- 管理者が検索クエリで指定できる属性にインデックスを作成します。

  注: Oracle Internet Directory の場合、検索クエリの属性にインデックスが作成されていないと、検索が失敗する場合があります。

- CA Identity Manager が大規模な検索を処理する方法を決定するために、ページサイズと最大行設定を設定します (P. 100)。

- ユーザ ディレクトリを調整します。使用しているユーザ ディレクトリ用のドキュメントを参照してください。

大規模な検索のパフォーマンスを改善する方法

CA Identity Manager が非常に大規模なユーザ ストアを管理する場合、多数の結果を返す検索により、システムがメモリ不足に陥る可能性があります。 メモリの問題を防ぐため、大規模な検索に対して制限を定義できます。

以下の 2 つの設定は、CA Identity Manager がどのように大規模な検索を処理するか決定します。

- Maximum number of rows

  ユーザ ディレクトリの検索時に CA Identity Manager が返す結果の最大数を指定します。 結果数が限度を超えると、エラーが表示されます。

- Page size

  単一の検索で返すことができるオブジェクトの数を指定します。 オブジェクトの数がページ サイズを超える場合、CA Identity Manager は複数の検索を実行します。

  ページ サイズを指定する場合は、以下の点に注意します。

  - ［Search Page Size］オプションを使用するには、CA Identity Manager が管理するユーザ ストアでページングがサポートされる必要があります。 一部のユーザ ストア タイプは、ページングをサポートするために追加設定が必要です。 詳細については、以下のトピックを参照してください。

    Sun Java System Directory Server ページング サポートの設定 (P. 102)

    Active Directory ページング サポートの設定

  - ユーザ ストアがページングをサポートせず、maxrows の値が指定される場合、CA Identity Manager は、maxrows 値のみを使用して検索サイズを制御します。

以下の場所で最大行数の制限とページ サイズを設定できます。

- ユーザ ストア

  ほとんどのユーザ ストアおよびデータベースで、検索制限を設定できます。

  注: 詳細については、使用しているユーザ ストアまたはデータベースのドキュメントを参照してください。

- CA Identity Manager ディレクトリ

  CA Identity Manager ディレクトリを作成するために使用するディレクトリ設定ファイル（directory.xml）内に DirectorySearch エレメントを設定 (P. 61)できます。

  デフォルトでは、既存のディレクトリの最大行数とページ サイズの値が無制限に設定されます。新規ディレクトリに対しては、最大行数の値が無制限に、ページ サイズの値が 2000 に設定されます。

- 管理対象オブジェクト定義

  ディレクトリ全体ではなく、オブジェクトの特定のタイプに適用される最大行数の制限とページ サイズを設定するには、CA Identity Manager ディレクトリの作成に使用する directory.xml ファイル内で *管理対象オブジェクト定義*を設定 (P. 63)します。

  管理対象オブジェクト タイプに制限を設定することで、自社のビジネス要件に合わせた調整を行うことができます。 たとえば、ほとんどの会社ではグループ数よりユーザ数のほうが多くあります。 そのような会社では、ユーザ オブジェクト検索だけに制限を設定できます。

- タスク検索画面

  ユーザ コンソールの検索およびリスト画面でユーザが参照する検索結果の数を制御できます。 結果数がタスクに対して定義されている 1 ページ当たりの結果数を超える場合、ユーザは結果の追加のページへのリンクを参照します。

  この設定は、検索によって返される結果数に影響しません。

  注: 検索およびリスト画面でのページ サイズ設定の詳細については、「管理ガイド」を参照してください。

最大行数の制限とページ サイズが複数の場所で定義されている場合、最も詳細な設定が適用されます。たとえば、管理対象オブジェクト設定はディレクトリ レベルの設定より優先されます。

Sun Java System Directory Server ページング サポートの設定

Sun Java System Directory Servers は、特定の順序または特定のサブセットで検索結果を提供する方法である、Virtual List View （VLV） をサポートします。 この方法は CA Identity Manager が使用する Simple Paged Results と異なります。

VLV を使用するには、権限を設定し、インデックスを作成します。 CA Identity Manager には、ページング サポートを設定する必要がある以下のファイルが含まれます。

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

これらのファイルは管理ツールの samples¥NeteAuto に NeteAuto サンプルの一部として含まれています。

管理ツールは、以下のデフォルトの場所にインストールされます。

Windows: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

次の手順に従ってください:

1. CA Identity Manager ディレクトリの directory.xml ファイル内の DirectorySearch エレメント (P. 61)に以下のパラメータを追加します。

   ```
   minsortrules="1"
   ```

   注: 既存の CA Identity Manager ディレクトリを変更する場合は、「CA Identity Manager ディレクトリの設定を更新する方法 (P. 192)」を参照してください。

2. 以下のように vlvcntrl.ldif ファイルに権限を設定します。
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```
3. 以下のように VLV 検索およびインデックス定義をインポートします。
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```
4. 以下のようにディレクトリを停止します。
   ```
   stop-slapd
   ```
5. runvlvindex を使用して、インデックスを構築します。
6. 以下のようにディレクトリを開始します。
   ```
   start-slapd
   ```

Active Directory ページング サポートの設定

Active Directory でページング サポートを設定するには、以下の高度な手順に従います。

- Virtual List View のサポートの設定 (P. 103)。
- Active Directory の MaxPageSize の設定 (P. 104)。(**CA Identity Manager r12.5 SP7 より前に作成されたディレクトリの場合のみ**)

Virtual List Views (VLV)のサポートの設定

Active Directory は、特定の順序または特定のサブセットで検索結果を提供する方法である、Virtual List View (VLV) をサポートします。 この方法は CA Identity Manager が使用する Simple Paged Results と異なります。

VLV を使用するには、権限を設定し、インデックスを作成します。 CA Identity Manager には、ページング サポートを設定する必要がある以下のファイルが含まれます。

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

これらのファイルは管理ツールの samples¥NeteAuto に NeteAuto サンプルの一部として含まれています。

管理ツールは、以下のデフォルトの場所にインストールされます。

Windows: C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

次の手順に従ってください:

1. CA Identity Manager ディレクトリの directory.xml ファイル内の DirectorySearch エレメント (P. 61) に以下のパラメータを追加します。

   ```
   minsortrules="1"
   ```

   注: 既存の CA Identity Manager ディレクトリを変更する場合は、「CA Identity Manager ディレクトリの設定を更新する方法 (P. 192)」を参照してください。

2. 以下のように vlvcntrl.ldif ファイルに権限を設定します。
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. 以下のように VLV 検索およびインデックス定義をインポートします。
   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. 以下のようにディレクトリを停止します。
   ```
   stop-slapd
   ```

5. runvlvindex を使用して、インデックスを構築します。

6. 以下のようにディレクトリを開始します。
   ```
   start-slapd
   ```

Active Directory の MaxPageSize の設定

Active Directory はデフォルトの MaxPageSize として 1000 を使用します。 directory.xml の maxpagesize 属性値が 1000 以上であると仮定します。 このような場合に、検索結果数が directory.xml の maxrows 値を超えたときに、CA Identity Manager は警告を表示できません。 この場合、検索を実行する管理者は、一部の検索結果が省略されていることに気付きません。

この問題を防ぐには、ディレクトリおよび各管理対象オブジェクトの maxpagesize 属性値が Active Directory MaxPageSize よりも小さいことを確認します。

CA Identity Manager12.5 SP7 以上と共にインストールされるテンプレート directory.xml ファイルを使用して、CA Identity Manager ディレクトリを作成していると仮定します。 この場合、ページング サポート用の追加の手順を実行する必要はありません。 directory.xml の maxpagesize 属性はデフォルトで設定されています。

ユーザが既存の CA Identity Manager ディレクトリにページング サポートを追加する場合、directory.xml の maxpagesize 属性は 1000 より小さい必要があります。

また、Active Directory MaxPageSize が 1000 である場合は、必ず CA Identity Manager ディレクトリおよびすべての管理対象オブジェクトに対して適切に maxpagesize 属性を設定してください。

第 4 章: リレーショナル データベース管理

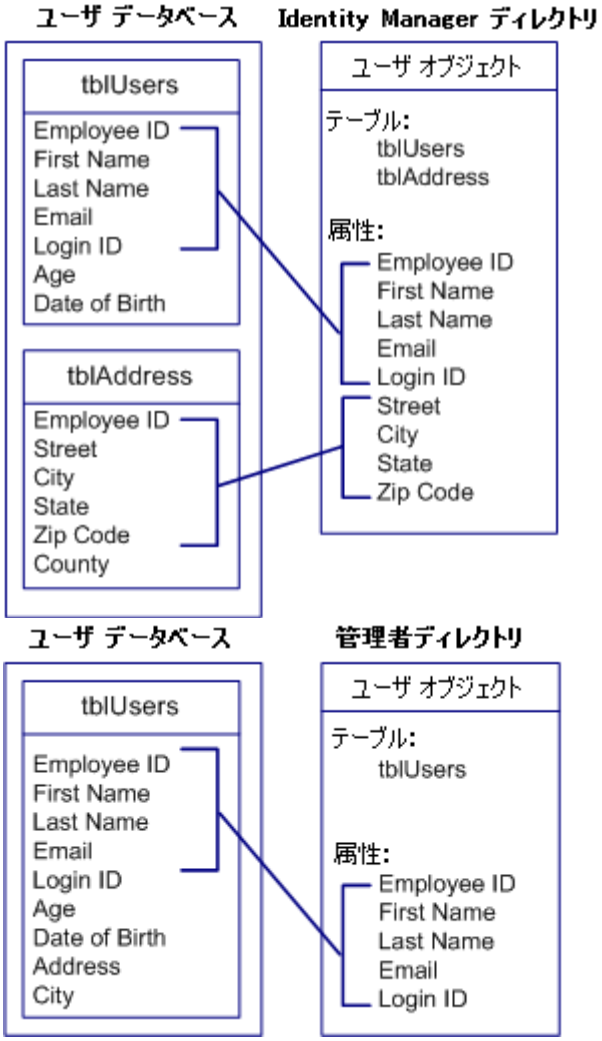
このセクションには、以下のトピックが含まれています。

CA Identity Manager ディレクトリ (P. 107)
リレーショナル データベース用に CA Identity Manager を設定する場合の重要な注意事項 (P. 109)
WebSphere 用の Oracle データ ソースの作成 (P. 110)
CA Identity Manager ディレクトリを作成する方法 (P. 111)
JDBC データ ソースを作成する方法 (P. 111)
SiteMinder と併用するために ODBC データ ソースを作成する方法 (P. 117)
ディレクトリ設定ファイルでデータベースを説明する方法 (P. 118)
ユーザ ディレクトリへの接続 (P. 141)
リレーショナル データベースの汎用属性 (P. 147)
自己登録グループを設定する方法 (P. 153)
検証ルール (P. 154)
組織管理 (P. 154)
ディレクトリ検索のパフォーマンスを改善する方法 (P. 158)

CA Identity Manager ディレクトリ

*CA Identity Manager ディレクトリ*では、ユーザ、グループ、（オプションで）組織などのオブジェクトがユーザ ストアにどのように格納され、 CA Identity Manager でどのように表示されるのかを説明します。 CA Identity Manager ディレクトリは 1 つ以上の CA Identity Manager 環境と関連付けられます。

以下の図では、CA Identity Manager ディレクトリがユーザ ストアにどのように関連するかを説明します。



注: データベース内のいくつかのユーザ属性は CA Identity Manager ディレクトリの一部ではありません。そのため、CA Identity Manager はそれらを管理しません。

リレーショナル データベース用に CA Identity Manager を設定する場合の重要な注意事項

CA Identity Manager がリレーショナル データベースを管理できるように設定する前に、データベースが以下の要件を満たしていることを確認します。

- データベースは、JDBC ドライバまたは Open Database Connectivity （ODBC）ドライバ（CA Identity Manager が SiteMinder と統合される場合）によってアクセスできる必要があります。 ドライバは外部結合をサポートする必要があります。 2 つを超えるテーブルが管理対象オブジェクトを表すために使用される場合、ドライバはネストされた外部結合もサポートする必要があります。

  注: ドライバが外部結合をサポートしない場合、データベースを照会するときに、CA Identity Manager は内部結合を使用します。 これにより、予期しないクエリ結果が生じる可能性があります。

- ユーザ、グループ、組織（サポートされる場合）のように、CA Identity Manager が管理する各オブジェクトを一意に識別します。 たとえば、ユーザの一意の識別子をログイン ID にすることができます。

  注: 一意の識別子が単一の列に格納されることを確認します。

- CA Identity Manager はいくつかの複数値属性を必要とします。これらの属性は個別テーブルの単一のセルまたは複数行で区切りリストとして格納できます。たとえば、以下の tblGroupMembers テーブルは、グループのメンバを格納します。

ID	メンバ
Research	dmason
Research	rsavory
Marketing	dmason
Marketing	awelch

［ID］列には、グループの一意の識別子が含まれます。また、［メンバ］列には、グループのメンバの一意の識別子が含まれます。たとえば、dmason と rsavory は Research グループのメンバです。新メンバがそのグループに追加されるとき、別の行が tblGroupMembers に追加されます。

- ユーザの環境には組織が含まれる場合は、以下タスクを実行します。
  - 組織のサポートの設定 (P. 155)を行うデータベースに対して、CA Identity Manager に付属の SQL スクリプトを編集しおよび実行します。
  - CA Identity Manager は、ルートという名前のトップレベルの組織が必要です。 他のすべての組織はルート組織と関連します。

    組織要件の詳細については、「組織管理 (P. 154)」を参照してください。

WebSphere 用の Oracle データ ソースの作成

次の手順に従ってください:

1. WebSphere 管理コンソールで、JDBC ドライバの設定時に作成した JDBC プロバイダに移動します。
2. 以下のプロパティでデータ ソースを作成し、［適用］をクリックします。

   名前： ユーザ ストア データ ソース

   JNDI 名： userstore

   URL： jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*
3. ユーザ ストア データ ソース用の新しい J2C Authentication Data Entry を設定します。
   a. 以下のプロパティを入力します。

      エイリアス： ユーザ ストア

      ユーザ ID： *username*

      パスワード： *password*

      username と *password* は、データベースの作成時に指定したアカウント用のユーザ名およびパスワードです。

   b. ［OK］をクリックし、画面の一番上にあるナビゲーション リンクを使用して、作成しているデータ ソースに戻ります。
4. 以下のフィールドのリスト ボックスから作成した［ユーザ ストア J2C 認証データ エントリ］を選択します。
   - コンポーネント管理の認証エイリアス
   - コンテナ管理の認証エイリアス
5. ［OK］をクリックして設定内容を保存します。

   注: データ ソースが正しく設定されることを確認するには、データ ソースの設定画面で［テスト接続］をクリックします。テスト接続が失敗する場合は、WebSphere を再起動し、再度接続をテストします。

CA Identity Manager ディレクトリを作成する方法

次の手順に従ってください:

1. SiteMinder を使用している場合は、CA Identity Manager ディレクトリを作成する前にポリシー ストア スキーマを適用します。

   注: 特定のポリシー ストア スキーマ、およびそれらの適用方法の詳細については、「インストール ガイド」を参照してください。

2. SiteMinder を使用している場合は、SiteMinder と共に使用するために ODBC データ ソースを作成 (P. 117) します。

3. CA Identity Manager が管理するユーザ データベース用のデータ ソースを作成します。

4. ディレクトリ設定ファイル（directory.xml）を変更することにより CA Identity Manager にデータベースについて説明します。 詳細については、「ディレクトリ設定ファイルでデータベースを説明する方法」を参照してください。

5. 管理コンソールで、ディレクトリ設定ファイルをインポートし、ディレクトリを作成します。

JDBC データ ソースを作成する方法

CA Identity Manager は、ユーザ ストアに接続するために CA Identity Manager がインストールされているアプリケーション サーバで JDBC データ ソースが必要です。データ ソースを作成するための手順はアプリケーション サーバごとに異なります。

JBoss アプリケーション サーバ用の JDBC データ ソースの作成

次の手順に従ってください:

1. 以下のファイルのコピーを作成します。

   jboss_home¥server¥default¥deploy¥objectstore-ds.xml

   jboss home

   CA Identity Manager がインストールされている Jboss アプリケーション サーバのインストール場所。

   新規ファイルは同じ場所に存在する必要があります。

2. userstore-ds.xml にファイルの名前を変更します。

3. userstore-ds.xml を以下のように編集します。
   a. <jndi-name> エレメントを検索します。
   b. <jndi-name> エレメントの値を jdbc/objectstore から userstore に以下のように変更します。

      <jndi-name>userstore</jndi-name>

   c. <connection-url> エレメントで、DatabaseName パラメータを以下のようにユーザ ストアとして役立つデータベースの名前に変更します。

      <connection-url>

      jdbc:sqlserver://*ipaddress:port*;selectMethod=cursor;DatabaseName=*userstore_name*

      </connection-url>

      ipaddress

      ユーザ ストアがインストールされているマシンの IP アドレスを指定します。

      port

      データベースのポート番号を指定します

      userstore_name

      ユーザ ストアとして機能するデータベースの名前を指定します。

4. FIPS をサポートするために必要な JBoss セキュリティ レルムを作成する予定である場合は、以下の手順に従います。
   a. security-domain を <security-domain>imuserstoredb</security-domain> に名前を変更します。
   b. ファイルを保存します。
   c. 残りの手順は省略します。 代わりに、「JDBC データ ソース用の JBoss セキュリティ レルムの作成 (P. 113)」の手順に従ってください。
5. userstore-ds.xml に以下の追加の変更を加えます。
   a. <user-name> エレメントの値を、ユーザ ストアへの読み取りおよび書き込みのアクセス権を持つアカウントのユーザ名に変更します。
   b. <user-name> エレメントの値を <user-name> エレメントで指定したアカウントのパスワードに変更します。

   注: ユーザ名とパスワードはこのファイル内のクリア テキストで表示されます。 そのため、userstore-ds.xml を編集するのではなく JBoss セキュリティ レルムを作成することを決定できます。
6. ファイルを保存します。

JDBC データ ソース用の JBoss セキュリティ レルムの使用

JBoss アプリケーション サーバで JDBC データ ソースを作成していると仮定します。ユーザ名とパスワードを使用するようにデータ ソースを設定するか、またはセキュリティ レルムを使用するようにそれを設定できます。

重要: FIPS が使用されている場合は、[JBoss セキュリティ レルム] オプションが使用されることを確認します。

次の手順に従ってください:

1. 「JBoss アプリケーション サーバ用の JDBC データ ソースの作成 (P. 111)」の手順を完了します。

   手順 4 で説明されているように userstore-ds.xml でユーザ名とパスワードを指定しないでください。

2. login-cfg.xml in *jboss_home*¥server¥default¥conf を開きます。
3. ファイル内で次のエントリを確認します。

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option
name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=N
oTxCM</module-option>
       </login-module>
  </authentication>
</application-policy>
```

4. 完全なエントリをコピーし、それを login-cfg.xml ファイルの <policy> と </policy> タグ内に貼り付けます。
5. ファイルに貼り付けたエントリに、以下の変更を行います。
   a. 名前属性値を imobjectstoredb から imuserstoredb に以下のように変更します。

      ```
      <application-policy name="imuserstoredb">
      ```

   b. ユーザ ストアに対する認証に使用したユーザの名前を以下のように指定します。

      ```
      <module-option name="userName">user_store_user</module-option>
      ```

   c. 前の手順のユーザのパスワードを以下のように指定します。

      ```
      <module-option name="password">user_store_user_password</module-option>
      ```

注: ユーザ ストア パスワードを暗号化するには、CA Identity Manager と共にインストールされるパスワード ツール（pwdtools）を使用します。

d. <module-option name="managedConnectionFactoryName"> エレメントで、正しい jdbc.jca:name を以下のように入力します。

```
<module-option name="managedConnectionFactoryName">
   jboss.jca:name=userstore,service=NoTxCM
</module-option>
```

6. ファイルを保存します。
7. アプリケーション サーバを再起動します。

WebLogic 用 JDBC データ ソースの作成

WebLogic 管理コンソールでデータ ソースを作成します。

注: Weblogic 接続プールの詳細については、Oracle WebLogic 11 のマニュアルを参照してください。

次の手順に従ってください:

1. WebLogic 管理コンソールで以下のパラメータを指定して JDBC データ ソースを作成します。

   名前： ユーザ ストア データ ソース

   JNDI 名： userstore

2. 以下の情報を使用して、データ ソースの接続プールを作成します。

   - SQL Server 2005 データベースの場合は、以下の値を使用します。

     URL： jdbc:sqlserver://*db_systemName*:1433

     ドライバ クラス名： com.microsoft.sqlserver.jdbc.SQLServerDriver

     プロパティ： user=*username*

     databaseName=*user store name*

     selectMethod=cursor

     パスワード：（*password*）

   - Oracle データベースの場合、以下の値を使用してください。

     URL： jdbc:oracle:thin:@*tp_db_systemname*:1521:*oracle_SID*

     ドライバ クラス名： oracle.jdbc.driver.OracleDriver

     プロパティ： user=*username*

     パスワード：（*password*）

3. 設定の後で、サーバ インスタンス *wl_server_name* にプールのターゲットを設定します。

   プールを展開した後で、いずれかのエラーが発生したかどうか確認するためにコンソールを確認します。

   注: 存在しないプールでデータ ソースを作成できないというエラーが表示される場合があります。このエラーを解決するには、WebLogic を再起動します。

WebSphere ODBC データ ソース

以下のセクションでは、WebSphere アプリケーション サーバ用の SQL または Oracle のデータ ソースを作成する方法について説明します。

WebSphere 用の SQL Server データ ソースの作成

次の手順に従ってください:

1. WebSphere 管理コンソールで、JDBC ドライバの設定時に作成した JDBC プロバイダに移動します。
2. ［追加のプロパティ］セクションの［データ ソース］を選択します。
3. 以下のプロパティでデータ ソースを作成し、［適用］をクリックします。

   名前： ユーザ ストア データ ソース

   JNDI 名： userstore

   databaseName： *userstore_name*

   serverName： *db_systemname*

4. 以下のように selectMethod プロパティを設定します。
   a. ［追加のプロパティ］セクションの［カスタム プロパティ］を選択します。
   b. selectMethod カスタム プロパティをクリックします。
   c. ［値］フィールドに以下のテキストを入力します。

      cursor

   d. ［OK］をクリックし、画面の一番上にあるナビゲーション リンクを使用して、作成しているデータ ソースに戻ります。

5. ユーザ ストア データ ソース用の新しい J2C Authentication Data Entry を設定します。
   a. ［関連項目］セクションから J2EE Connector Architecture （J2C）認証データ エントリを選択します。
   b. ［新規作成］をクリックします。
   c. 以下のプロパティを入力します。

      エイリアス： ユーザ ストア

      ユーザ ID： *username*

      パスワード： *password*

      username と *password* は、データベースの作成時に指定したアカウント用のユーザ名およびパスワードです。
   d. ［OK］をクリックし、画面の一番上にあるナビゲーション リンクを使用して、作成しているデータ ソースに戻ります。
6. ［コンポーネント管理の認証エイリアス］フィールドでリスト ボックスから作成したユーザ ストア J2C Authentication Data Entry を選択します。
7. ［OK］をクリックして設定内容を保存します。

   注: データ ソースが正しく設定されることを確認するには、データ ソースの設定画面で［テスト接続］をクリックします。テスト接続が失敗する場合は、WebSphere を再起動し、再度接続をテストします。

WebSphere 用の Oracle データ ソースの作成

次の手順に従ってください:

1. WebSphere 管理コンソールで、JDBC ドライバの設定時に作成した JDBC プロバイダに移動します。
2. 以下のプロパティでデータ ソースを作成し、［適用］をクリックします。

   名前： ユーザ ストア データ ソース

   JNDI 名： userstore

   URL： jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. ユーザ ストア データ ソース用の新しい J2C Authentication Data Entry を設定します。

   a. 以下のプロパティを入力します。

      エイリアス： ユーザ ストア

      ユーザ ID： *username*

      パスワード： *password*

      username と *password* は、データベースの作成時に指定したアカウント用のユーザ名およびパスワードです。

   b. ［OK］をクリックし、画面の一番上にあるナビゲーション リンクを使用して、作成しているデータ ソースに戻ります。

4. 以下のフィールドのリスト ボックスから作成した［ユーザ ストア J2C 認証データ エントリ］を選択します。

   - コンポーネント管理の認証エイリアス
   - コンテナ管理の認証エイリアス

5. ［OK］をクリックして設定内容を保存します。

   注: データ ソースが正しく設定されることを確認するには、データ ソースの設定画面で［テスト接続］をクリックします。テスト接続が失敗する場合は、WebSphere を再起動し、再度接続をテストします。

SiteMinder と併用するために ODBC データ ソースを作成する方法

CA Identity Manager が SiteMinder と統合される場合は、データベースを指している SiteMinder マシン上の ODBC データ ソースを定義します。後で使用するためにデータ ソースの名前を書き留めます。 以下の手順に従います。

- **Windows：** ODBC データ ソースを「System DN」として設定します。 手順については、Windows オペレーティング システムのマニュアルを参照してください。
- **UNIX：** *policy_server_installation*/db にある system_odbc.ini ファイルに ODBC データ ソースのパラメータを指定するエントリを追加します。

ディレクトリ設定ファイルでデータベースを説明する方法

データベースを管理するには、CA Identity Manager がデータベース構造とコンテンツを理解している必要があります。 CA Identity Manager にデータベースを説明するには、ディレクトリ設定ファイル（directory.xml）を作成します。

ディレクトリ設定ファイルには、以下のセクションの 1 つ以上が含まれます。

CA Identity Manager Directory Information

CA Identity Manager が使用する CA Identity Manager ディレクトリに関する情報が含まれます。

Attribute Validation

CA Identity Manager ディレクトリに適用される検証ルールを定義します。

Provider Information

CA Identity Manager が管理するユーザ ストアを説明します。

Directory Groups Behavior

CA Identity Manager でユーザ ストアが検索される方法を指定できます。

User Object (P. 120)

ユーザがユーザ ストアにどのように格納され、CA Identity Manager でどのように表示されるのかを説明します。

Group Object (P. 120)

グループがユーザ ストアにどのように格納され、CA Identity Manager でどのように表示されるのかを説明します。

Organization Object (P. 120)

組織がどのように格納されるか、どのように CA Identity Manager で表示されるかを説明します。

Self-Subscribing Groups

セルフサービス ユーザが参加できるグループに対するサポートを設定します。

CA Identity Manager 用の管理ツールをインストールしたディレクトリには、リレーショナル データベース用の以下のディレクトリ設定ファイル テンプレートが含まれます。

admin_tools¥directoryTemplates¥RelationalDatabase¥directory.xml

admin_tools

以下の例のように、CA Identity Manager 管理ツールのインストールされた場所を定義します。

- **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
- **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

注: directoryTemplates¥RelationalDatabase のディレクトリ設定ファイル テンプレートは、組織をサポートする環境に対して設定されます。 組織が含まれない環境用のディレクトリ設定ファイルを表示するには、*admin_tools*¥samples¥NeteAutoRDB¥NoOrganization にある NeteAuto サンプル用の directory.xml ファイルを参照できます。

新規ディレクトリに設定テンプレートをコピーするか、またはそれを上書きされないように別の名前で保存します。 その後、データベース構造を反映させてテンプレートを変更できます。

ディレクトリ設定ファイルには以下の 2 つの重要な規則があります。

- ## -- 必要な値を示します。

  必要な情報をすべて提供するには、ダブル パウンド記号（##）をすべて検索し、それらを適切な値と置き換えます。 たとえば、##PASSWORD_HINT は、パスワードを忘れた場合に、一時パスワード受け取るためにユーザが答える質問を格納する属性を提供する必要があることを示します。

- @ -- CA Identity Manager が入力する値を示します。 ディレクトリ設定ファイルでこれらの値を変更しないでください。 CA Identity Manager は、ディレクトリ設定ファイルをインポートするときに、値を提供するようにユーザに促します。

ディレクトリ設定ファイルを変更する前に、以下の情報が必要です。

- ユーザ、グループ、および組織オブジェクト（ユーザの構造に組織が含まれる場合）のテーブル名。
- ユーザ、グループ、および組織プロファイル（ユーザの構造に組織が含まれる場合）の属性のリスト。

ディレクトリ設定ファイルの変更

ディレクトリ設定ファイルを変更するには、以下の手順に従います。

次の手順に従ってください:

1. データベースへの接続を設定します。
2. 検索を終了する前に、CA Identity Manager がディレクトリの検索を終了するまでの時間を指定します。
3. CA Identity Manager が管理するユーザおよびグループの管理対象オブジェクト (P. 120) を定義します。
4. 汎用属性を変更します。

   汎用属性は、CA Identity Manager で、パスワード属性などの特別な属性を識別します。
5. 自己登録グループのサポートを設定します。
6. ユーザの環境に組織が含まれる場合は、組織サポートを設定します。

詳細情報:

管理対象オブジェクトの説明 (P. 120)
組織管理 (P. 154)
自己登録グループを設定する方法 (P. 153)
リレーショナル データベースの汎用属性 (P. 147)

管理対象オブジェクトの説明

CA Identity Manager で、ユーザ ストアのエントリに対応する、以下のタイプのオブジェクトを管理します。

- ユーザ -- 企業のユーザを表します。
- グループ -- 何かを共有しているユーザの関連付けを表します。
- （オプション）組織 -- 事業単位を表します。 組織にはユーザ、グループ、および他の組織が含まれる場合があります。

  注: 組織管理 (P. 154)では組織の設定に関する情報を提供します。

オブジェクトの説明には以下の情報が含まれます。

- オブジェクトが格納されるテーブルなどの、オブジェクトに関する情報 (P. 121)。
- エントリに関する情報を格納する属性 (P. 126)。 たとえば、ポケットベル属性はポケットベル番号を格納します。

重要: CA Identity Manager 環境は 1 つのタイプのユーザ、グループ、および組織オブジェクトのみをサポートします。

管理対象オブジェクトを説明する方法

管理対象オブジェクトは、ディレクトリ設定ファイルの User Object、Group Object、および Organization Object （データベースに組織が含まれる場合）の各セクションのオブジェクト情報を指定することにより説明されます。

これらの各セクションには、以下のコードのような ImsManagedObject エレメントが含まれます。

```
<ImsManagedObject name="User" description="My Users">
```

ImsManagedObject エレメントには以下のエレメントが含まれます。

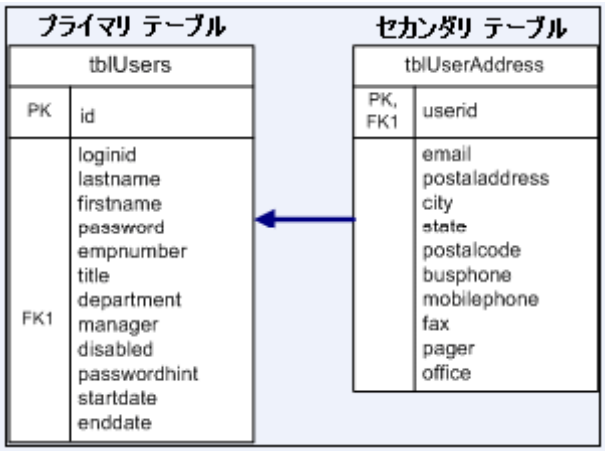
- Table （必須）
- UniqueIdentifier （必須）
- ImsManagedObjectAttr （必須）
- RootOrg （組織オブジェクトの場合のみ）

データベース テーブル

ディレクトリ設定ファイルでは Table エレメントを使用して、管理対象オブジェクトに関する情報を格納するテーブルを定義します。

各管理対象オブジェクトにはオブジェクトの一意の識別子が含まれる、1 つのプライマリ テーブルが必要です。 追加の情報はセカンダリ テーブルに格納できます。

以下の図は、プライマリおよびセカンダリ テーブルにユーザ情報を格納するデータベースを示します。



オブジェクトの情報が複数のテーブルに格納される場合は、各テーブルの Table エレメントを作成します。 セカンダリ テーブルがプライマリ テーブルとの関係を定義するために Table エレメントで Reference エレメントを使用します。

たとえば、ユーザに関する基本情報が tblUsers に格納され、アドレス情報が tblUserAddress に格納される場合、ユーザ管理対象オブジェクトのテーブル定義は以下のエントリのようになります。

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

Table エレメント

Table エレメントのパラメータを以下に示します。

name

（必須）

オブジェクトの管理プロファイルに属性の一部またはすべてを格納するテーブルの名前を指定します。

primary

テーブルが管理対象オブジェクトのプライマリ テーブルであるかどうかを示します。プライマリ テーブルには、オブジェクトの一意の識別子が以下のように含まれます。

- True -- テーブルはプライマリ テーブルです。
- False -- テーブルはセカンダリ テーブルです（デフォルト）。

ユーザがプライマリ パラメータを指定しない場合、CA Identity Manager はテーブルをセカンダリ テーブルと見なします。

注: 1 つのテーブルのみプライマリ テーブルに指定できます。

filter

管理対象オブジェクトに適用されるテーブル エントリのサブセットを識別します。

オプションのフィルタ パラメータは以下の例のようになります。

```
filter="ORG=2"
```

注: フィルタは、CA Identity Manager が生成するクエリにのみ適用されます。カスタム クエリで生成されたクエリを上書きする場合は、カスタム クエリでフィルタを指定します。

fullouterjoin

外部結合が完全な外部結合かどうかを示します。

- True -- 外部結合は完全な外部結合です。 この場合、有効な行を返すのに必要な条件は、返される行の結合で両方のテーブルで検出されます。
- False -- 外部結合はプライマリ テーブルに関連のある左外部結合です。この場合、クエリの 1 つのテーブル内の行のみが条件を満たす必要があります（デフォルト）。

注: パラメータは特に指定されていない限りオプションです。

Table パラメータには、プライマリ テーブルをセカンダリ テーブルにリンクするために 1 つ以上の Reference エレメントを含めることができます。

Reference エレメント

Reference エレメントのパラメータを以下に示します。

childcol

プライマリ テーブル内の列にマップする、セカンダリ テーブル（対応する Table エレメントで指定された）内の列を示します。

primarycol

セカンダリ テーブル内の列にマップするプライマリ テーブル内の列を示します。

注: パラメータは特に指定されていない限りオプションです。

オブジェクト情報の指定

オブジェクト情報はさまざまなパラメータの値を提供することにより指定されます。

次の手順に従ってください:

1. User Object、Group Object、または Organization Object セクションで ImsManagedObject エレメントを検索します。
2. 以下のパラメータの値を提供します。

   name

   （必須）

   管理対象オブジェクトの一意の名前を提供します。

   description

   管理対象オブジェクトの説明を提供します。

   objecttype

   （必須）

   管理対象オブジェクトのタイプを指定します。 有効な値は以下のとおりです。

   - USER
   - GROUP
   - ORGANIZATION

   ImsManagedObject エレメントは以下のコードのようである必要があります。

   ```
   <ImsManagedObject name="User" description="My  Users" objecttype="USER">
   ```

3. 「データベース テーブル (P. 121)」で述べられているように、Table 情報を提供します。
4. オブジェクトの一意の識別子 (P. 125)が含まれる列を指定します。
5. オブジェクトのプロファイルを構成する属性 (P. 126)を説明します。
6. 組織オブジェクトを設定している場合は、「組織管理 (P. 154)」移動します。

管理対象オブジェクトの一意の識別子を指定する方法

CA Identity Manager が管理する各オブジェクトには一意の識別子が必要です。 一意の識別子が管理対象オブジェクトのプライマリ テーブルの単一の列に格納されていることを確認します。 プライマリ テーブルは「データベース テーブル (P. 121)」で説明されています。

以下のように一意の識別子を定義するために UniqueIdentifier と UniqueIdentifierAttr エレメントを使用します。

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="tablename.columnname" />
</UniqueIdentifier>
```

UniqueIdentifierAttr エレメントには name パラメータが必要です。 name パラメータの値は一意の識別子が格納される属性です。値には物理属性または汎用属性 (P. 82)を指定できます。

物理属性を指定する場合は、以下の点に注意してください。

- 「属性の説明を変更する方法 (P. 126)」で説明されているように、指定された属性がデータベースに存在し、ディレクトリ設定ファイルで定義されていることを確認します。 属性の説明で、読み取り専用または再書き込み不可の権限を必ず指定し、セッション中に一意の識別子が変更されないようにしてください。
- 物理属性を指定するには、以下の構文を使用します。

  tablename.columnname

  tablename

  属性が格納されるテーブルの名前を定義します。 指定するテーブルはプライマリ テーブルである必要があります。

  columnname

  属性を格納する列の名前を定義します。
- データベースが一意の識別子を生成する場合は、属性のカスタム操作 (P. 137)を指定します。 たとえば、データベースから最後に生成した識別子を抽出する操作を指定する必要がある場合があります。

属性の説明を変更する方法

属性は、電話番号や住所など、ユーザ、グループ、または組織エンティティに関する情報を格納します。 エンティティの属性はそのプロファイルを決定します。

ディレクトリ設定ファイルで、属性は ImsManagedObjectAttr エレメントで説明されます。 ディレクトリ設定ファイルの User Object、Group Object、および Organization Object セクションで、以下を実行します。

- データベース属性を説明するには、デフォルトの属性の説明を変更します。
- 既存の説明をコピーし、必要に応じて値を変更することにより、新しい属性の説明を作成します。

ユーザ、グループ、および組織プロファイル内の各属性には、ImsManagedObjectAttr エレメントが 1 つのみあります。 たとえば、ImsManagedObjectAttr エレメントは、ユーザ ID を説明できます。

ImsManagedObjectAttr エレメントは以下のコードのようになります。

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

注: Oracle データベースを使用している場合、管理対象オブジェクト属性を設定する際には、以下の点に注意してください。

- Oracle データベースはデフォルトでは大文字と小文字を区別します。 ディレクトリ設定ファイルの属性およびテーブル名の大文字小文字は、Oracle の属性の大文字小文字と一致する必要があります。

  切り捨てを防ぐために String データ タイプの最大長を必ず指定します。 文字列の長さを制限するには、ユーザが最大長を超える文字列を入力するときにエラーが表示されるように、検証ルールを作成できます。

ImsManagedObjectAttr パラメータは以下のとおりです。

注: パラメータは特に指定されていない限りオプションです。

physicalname

（必須）

属性の物理名およびそれを指定し、それには以下の詳細のいずれかが含まれている必要があります。

- 値が格納される名前および場所。

  形式： *tablename.columnname*

  たとえば、属性が tblUsers テーブルの ID 列に格納される場合は、その属性の物理名は以下のとおりです。

  tblUsers.id

  Table エレメント (P. 121)に属性が含まれる各テーブルを定義する必要があります。

- 汎用属性。

  汎用属性は計算された値を表すことができます。 たとえば、カスタム操作 (P. 137)を使用して計算された属性を参照するために汎用属性を使用できます。

displayname

（必須）

属性の一意の名前を指定します。

ユーザ コンソールで、表示名がタスク画面に追加可能な属性のリストに表示されます。

注: ディレクトリ設定ファイル（directory.xml）の属性の表示名は変更しないでください。 タスク画面で属性の名前を変更するには、タスク画面定義で属性のラベルを指定することができます。 詳細については、「*管理者ガイド*」を参照してください。

description

属性の説明を提供します。

valuetype

属性のデータ型を指定します。 有効な値は以下のとおりです。

String

値は任意の文字列を指定できます。

デフォルト値です。

Integer

値は整数である必要があります。

注: 整数は 10 進数をサポートしません。

Number

値は整数である必要があります。 数値オプションは 10 進数をサポートします。

Date

値は以下のパターンを使用して有効な日付であることを解析する必要があります。

MM/dd/yyyy

ISODate

値はパターン yyyy-MM-dd を使用して、有効な日付であることを解析する必要があります。

UnicenterDate

値はパターン YYYYYYYDDD を使用して、有効な日付であることを解析する必要があります。ここで：

YYYYYYY は 3 つのゼロで始まる、年の 7 つの数値表現です。 例：0002008

DDD は必要に応じて、ゼロで始まる日付の数値表現です。 有効な値の範囲は、001 ～ 366 です。

属性の valuetype が正しくない場合、CA Identity Manager クエリは失敗する場合があります。

属性がデータベースに正しく格納されていることを確認するために、それを検証ルールと関連付けることができます。

required

以下のように、値が属性に対して指定される必要があるかどうかを示します。

- True -- 必須
- False -- オプション（デフォルト）

multi-valued

属性が以下のように複数値を持つことができるかどうかを示します。

- True -- 属性は複数値を持つことができます。
- False -- 属性は単一値のみを持つことできます（デフォルト）。

たとえば、ユーザ プロファイル内のグループ メンバシップ属性はユーザが属するグループを格納するために multi-valued です。

複数行テーブルではなく、区切りリストで multi-valued 属性を格納するには、区切り文字パラメータで区切り文字を定義する必要があります。

可能な値の数、および列で可能な各値の長さが十分であることを確認します。

重要: ユーザ オブジェクト定義のグループ メンバシップ属性が multi-valued であることを確認してください。

wellknown

汎用属性の名前を提供します。

汎用属性は CA Identity Manager で特別な意味を持ちます。

形式： *%ATTRIBUTENAME%*

注: カスタム操作が属性と関連付けられる場合に、汎用属性 (P. 82)を指定する必要があります。

maxlength

列の最大サイズを決定します。

permission

属性の値がタスク画面で以下のように変更できるかどうかを示します。

READONLY

値が表示されますが変更できません。

WRITEONCE

オブジェクトが作成されたら、値は変更できません。 たとえば、ユーザが作成された後で、ユーザ ID を変更できません。

READWRITE

値は変更できます（デフォルト）。

hidden

属性が CA Identity Manager タスク画面に表示されるかどうかを以下のように示します。

- True -- 属性はユーザに表示されません。
- False -- 属性はユーザに表示されます（デフォルト）。

論理属性は hidden 属性を使用します。

注: 論理属性の詳細については、「Java のプログラミング ガイド」を参照してください。

system

CA Identity Manager のみが属性を使用したことを示します。 以下のように、ユーザは、ユーザ コンソールで属性を変更することはできません。

- True -- ユーザは属性を変更できません。 属性はユーザ コンソールに表示されません。
- False -- ユーザはこの属性を変更することができ、ユーザ コンソールのタスク画面に追加できます（デフォルト）。

validationruleset

属性と検証ルール セットを関連付けます。

指定する検証ルール セットがディレクトリ設定ファイルの ValidationRuleSet エレメントで定義されていることを確認します。

delimiter

複数の値が単一の列に格納されるときに値を区切る文字を定義します。

重要: multivalued パラメータは delimiter パラメータを適用するために true に設定されていることを確認してください。

注: ユーザ コンソールで、パスワードまたは給料などの機密情報が表示されないようにするために、DataClassification (P. 77) パラメータを指定できます。

Sensitive 属性の管理

CA Identity Manager では、sensitive 属性を管理するための以下の方法を提供します。

- 属性のデータ分類

  データ分類により、ディレクトリ設定ファイル（directory.xml）でユーザが属性の表示および暗号化のプロパティを指定できます。

  以下のように sensitive 属性を管理するデータ分類を定義できます。

  - CA Identity Manager タスク画面で、一連のアスタリスクとして属性の値を表示します。

    たとえば、パスワードをクリア テキストで表示する代わりにアスタリスクとして表示できます。

  - ［サブミット済みタスクの表示］画面で、属性値を非表示にします。

    このオプションにより、属性を管理者に表示しないようにすることができます。 たとえば、CA Identity Manager 内でタスク ステータスを表示するが、給与詳細を表示する必要のない管理者に給与などの詳細を見せないようにすることなどです。

  - 既存のオブジェクトのコピーを作成するときには、特定の属性を無視します。

  - 属性を暗号化します

- タスク プロファイル画面のフィールド スタイル

  directory.xml ファイル内の属性を変更しない場合は、sensitive 属性が表示される画面定義で属性の表示プロパティを設定します。

  フィールド スタイルにより、クリア テキストの代わりに一連のアスタリスクとして、パスワードなどの属性を表示できます。

  注: sensitive 属性のフィールド スタイルの詳細については、ユーザ コンソール ヘルプでフィールド スタイルを検索してください。

データ分類属性

データ分類エレメントは、属性の説明と追加のプロパティを関連付ける方法を提供します。 このエレメントの値は、CA Identity Manager が属性を処理する方法を決定します。 このエレメントは以下のパラメータをサポートします。

- sensitive

  CA Identity Manager は、［サブミット済みタスクの表示］画面で一連のアスタリスク（*）として属性を表示できます。 このパラメータは、属性の古い値と新しい値が［サブミット済みタスクの表示］画面にクリア テキストで表示されないようにします。

  また、ユーザ コンソールで既存のユーザのコピーを作成する場合、このパラメータは属性が新規ユーザにコピーされないようにします。

- vst_hide

  ［サブミット済みタスクの表示］タブの［イベント詳細］画面の属性を非表示にします。 sensitive 属性（アスタリスクとして表示される）とは異なり、vst_hidden 属性は表示されません。

  このパラメータを使用して、給料などの属性への変更が［サブミット済みタスクの表示］で表示されないようにすることができます。

- ignore_on_copy

  管理者がユーザ コンソールでオブジェクトのコピーを作成するときに、CA Identity Manager は属性を無視します。 たとえば、ユーザ オブジェクト上のパスワード属性に対して ignore_on_copy を指定したと仮定します。ユーザ プロファイルをコピーするときに、CA Identity Manager は新規ユーザ プロファイルに現在のユーザのパスワードを適用しません。

- AttributeLevelEncrypt

  属性値をユーザ ストアに格納すると、それらを暗号化します。 CA Identity Manager で FIPS 140-2 が有効になっている場合、CA Identity Manager は RC2 暗号化または FIPS 140-2 暗号化を使用します。

  CA Identity Manager での FIPS 140-2 サポートの詳細については、「*設定ガイド*」を参照してください。

  属性はランタイム中にクリア テキストで表示されます。

  注: 属性がクリア テキストで画面に表示されないようにするために、機密データ分類エレメントを暗号化された属性に追加することもできます。 詳細については、「属性レベルの暗号化の追加方法 (P. 78)」を参照してください。

- PreviouslyEncrypted

  CA Identity Manager がユーザ ストアのオブジェクトにアクセスするときに、暗号化された値を検出し、復号化します。

  このデータ分類を使用して、以前に暗号化された値を復号化します。

  オブジェクトを保存するときに、クリア テキスト値がストアに保存されます。

データ分類属性の設定

次の手順に従ってください:

1. ディレクトリ設定ファイルの属性を検索します。
2. 属性の説明の後で、以下の属性を追加します。

   <DataClassification name="*parameter*">

   parameter

   以下のいずれかのパラメータを示します。

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   たとえば、vst_hide データ分類属性が含まれる属性の説明は以下のコードのようになります。

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Attribute-Level 暗号化

ユーザ ストアの属性を暗号化するには、ディレクトリ設定ファイル（directory.xml）でその属性用の AttributeLevelEncypt データ分類を指定することにより行います。属性レベルの暗号化が有効な場合、CA Identity Manager では、ユーザ ストアにその属性の値を格納する前にそれを暗号化します。 属性はユーザ コンソールでクリア テキストとして表示されます。

注: 属性がクリア テキストで画面に表示されないようにするために、機密データ分類エレメントを暗号化された属性に追加することもできます。詳細については、「属性レベルの暗号化を削除する方法 (P. 78)」を参照してください。

FIPS 140-2 サポートが有効な場合、属性は RC2 暗号化または FIPS 140-2 暗号化を使用して暗号化されます。

属性レベルの暗号化を実装する前に、以下の点に注意してください。

- CA Identity Manager では、検索で暗号化された属性を検出できません。

  暗号化された属性は、メンバ、管理者、所有者のポリシーまたはアイデンティティ ポリシーに追加されたものとみなされます。 CA Identity Manager では属性を検索できないため、ポリシーを正しく解決できません。

  directory.xml ファイルで属性を searchable="false" に設定することを検討してください。例：

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- CA Identity Manager が共有されたユーザ ストアおよびプロビジョニング ディレクトリを使用する場合は、プロビジョニング サーバ属性を暗号化しないでください。
- 以下の条件を満たす環境のユーザ パスワード用の AttributeLevelEncrypt を有効化しないでください。
  - CA SiteMinder の統合を含み、かつ、
  - リレーショナル データベースにユーザが格納されている

  CA Identity Manager が CA SiteMinder と統合されている場合、新規ユーザがログインを試行して、クリア テキストでパスワードを入力すると、暗号化されたパスワードによって問題が発生します。
- CA Identity Manager 以外のアプリケーションによって使用されるユーザ ストアの属性レベルの暗号化を有効にする場合、他のアプリケーションは暗号化された属性を使用できません。

属性レベルの暗号化の追加方法

CA Identity Manager ディレクトリへの属性レベルの暗号化を追加したと仮定します。 属性と関連付けられるオブジェクトを保存する場合、CA Identity Manager は既存のクリア テキスト属性値を自動的に暗号化します。たとえば、ユーザのプロファイルを保存する場合、パスワード属性を暗号化することによって、パスワードが暗号化されます。

注: 属性値を暗号化するには、オブジェクトを保存するために使用するタスクに属性が含まれている必要があります。前の例のパスワード属性を暗号化するには、オブジェクトを保存するために使用するタスク（［ユーザの変更］タスクなど）にパスワード フィールドが追加されていることを確認します。

新規オブジェクトはすべてユーザ ストアに暗号化された値で作成されます。

次の手順に従ってください:

1. 以下のいずれかのタスクを実行します。
   - CA Identity Manager ディレクトリの作成
   - ディレクトリ設定をエクスポートすることによる既存のディレクトリの更新
2. directory.xml ファイルで暗号化する属性に以下のデータ分類属性を追加します。

   AttributeLevelEncrypt

   ユーザ ストア内で暗号化された形式で属性を保持します。

   sensitive（**オプション**）

   CA Identity Manager 画面で属性値を非表示にします。たとえば、パスワードはアスタリスク（*）として表示されます。

   例：

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false"
multivalued="false" maxlength="0" searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. CA Identity Manager ディレクトリを作成している場合は、環境とディレクトリを関連付けます。
4. CA Identity Manager ですべての値を直ちに暗号化するには、Bulk Loader を使用して、すべてのオブジェクトを変更します。

   注: Bulk Loader の詳細については、「管理ガイド」を参照してください。

属性レベルの暗号化を削除する方法

CA Identity Manager ディレクトリに暗号化された属性があり、それがクリア テキストとしてその属性の値と共に保存される場合、AttributeLevelEncrypt データ分類を削除できます。

データ分類が削除されたら、CA Identity Manager では、新規属性値を暗号化しなくなります。 ユーザが属性と関連付けられるオブジェクトを保存する場合には、既存の値が復号化されます。

注: 属性値を復号化するには、オブジェクトの保存に使用するタスクに属性が含まれている必要があります。 たとえば、既存ユーザに対してパスワードを復号化するには、パスワード フィールドが含まれるタスク（［ユーザの変更］タスクなど）と共にユーザ オブジェクトを保存します。

CA Identity Manager で属性用のユーザ ストアに残るすべての暗号化された値を検出し、復号化するようにするには、別のデータ分類、PreviouslyEncrypted を指定できます。ユーザがオブジェクトを保存するときには、クリア テキスト値がユーザ ストアに保存されます。

注: PreviouslyEncrypted データ分類を追加すると、すべてのオブジェクト ロードにおいて余分な処理が追加されます。パフォーマンス上の問題が発生するのを防ぐため、PreviouslyEncrypted データ分類を追加し、その属性に関連付けられる各オブジェクトをロードおよび保存してから、そのデータ分類を削除することを検討します。この方法により、すべての暗号化されて格納されている値を格納されているクリア テキストに自動的に変換されます。

次の手順に従ってください:

1. 適切な CA Identity Manager ディレクトリ用のディレクトリ設定をエクスポートします。
2. directory.xml ファイルで、復号化する属性から、データ分類 AttributeLevelEncrypt を削除します。
3. CA Identity Manager に以前に暗号化された値を強制的に削除させる場合は、PreviouslyEncrypted データ分類属性を追加します。

   例 :

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. CA Identity Manager に強制的にすべての値を直ちに復号化させるには、Bulk Loader を使用して、オブジェクトをすべて変更します。

   注: Bulk Loader の詳細については、「管理ガイド」を参照してください。

カスタム操作

特定の管理対象オブジェクトのカスタム操作を定義すると、以下の操作を行うことができます。

- ストアド プロシージャの使用
- データベース構造に対するクエリの最適化
- データベースに生成された一意の識別子の取得

カスタム操作は属性にのみ適用されます。

カスタム操作を指定する場合は、以下の点に注意してください。

- カスタム操作を指定するユーザは SQL に精通している必要があります。
- CA Identity Manager はカスタム操作を検証しません。 ランタイムまで、構文エラーおよび無効なクエリはレポートされません。
- 属性に対してカスタム操作を指定する場合は、CA Identity Manager タスクの検索フィルタでその属性を使用することはできません。
- カスタム操作は XML 標準に従う必要があります。XML 構文を使用して特殊文字を表します。 たとえば、' として一重引用符（'）を指定します。

カスタム操作を指定するには、Operation エレメントを使用します。

Operation エレメント

Operation エレメントは、カスタム クエリを実行できる SQL ステートメントを定義したり、属性の作成、取得、変更、または削除を行うストアド プロシージャを呼び出したりします。 Operation エレメントは以下の例のように、IMSManagedObjectAttr エレメントの従属エレメントです。

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

Operation エレメントのパラメータを以下に示します。

name

操作の事前定義済みの名前を指定します。 有効な操作は以下のとおりです。

- Create
- Get
- Set
- Delete
- GetDB

  GetDB 操作は、一意の識別子がデータベースまたはストアド プロシージャから生成されるときに、作成タスク中にデータベースから一意の識別子を取得します。

value

実行する SQL ステートメントまたはストアド プロシージャを定義します。有効な値は以下のとおりです。

- INSERT
- SELECT

- UPDATE
- DELETE
- CALL （ストアド プロシージャの場合）

注: パラメータは特に指定されていない限りオプションです。

Operation エレメントには 1 つ以上の Parameter エレメントを含めることができます。

Parameter エレメント

Parameter エレメントは、クエリに渡される値を指定します。複数の Parameter エレメントが定義される場合、値は指定されたリスト順にクエリに渡されます。

Parameter エレメントは name パラメータを必要とします。 name パラメータの値には物理属性または汎用属性 (P. 82)を指定できます。

注: CA Identity Manager は、Parameter エレメント内のクエリに渡される値を理解している必要があります。 たとえば、値には、ImsManagedObjectAttr 属性で定義されている物理名または汎用属性を指定できます。

物理属性を指定する場合は、以下の点に注意してください。

- 物理属性を指定するには、以下の構文を使用します。

  tablename.columnname

  - *tablename*

    属性が格納されるテーブルの名前を提供します。 指定するテーブルはプライマリ テーブルである必要があります。

  - *columnname*

    属性を格納する列の名前を提供します。

- 指定する属性はデータベースに存在する必要があります。また、「属性の説明を変更する方法 (P. 126)」で説明されているように、ディレクトリ設定ファイルで定義されています。

例 : Business Number 属性のカスタム操作

以下の例で、Business Number 属性はストアドプロシージャをコールすることにより生成されます。データベースの物理属性ではありません。

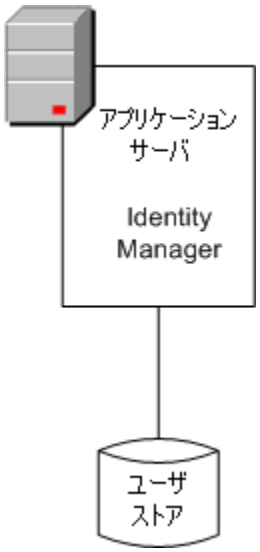
```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

以下の点に注意してください。

- sp_getbusinessnumber、sp_setbusinessnumber、および sp_deletebusinessnumber はユーザ定義のストアドプロシージャです。
- Get 操作から返される値は %BUSINESS_NUMBER% 属性にマップされます。
- 疑問符（?）は、クエリが実行される前に、ランタイムに作成される代用を示します。たとえば、Get 操作で、汎用属性である %USER_ID% はストアドプロシージャ sp_getbusinessnumber に渡されます。

ユーザ ディレクトリへの接続

CA Identity Manager は、以下の図に示すように、ユーザ、グループ、組織情報などの情報を格納するためにユーザ ディレクトリに接続します。



新規ディレクトリまたはデータベースは必要ありません。ただし、既存のディレクトリまたはデータベースは、完全修飾ドメイン名（FQDN）を持つシステム上にある必要があります。

サポートされているディレクトリおよびデータベース タイプのリストについては、CA サポート サイト上の CA Identity Manager サポート マトリックスを参照してください。

管理コンソールで CA Identity Manager ディレクトリを作成するときに、ユーザ ストアへの接続を設定します。

ユーザが CA Identity Manager ディレクトリを作成した後にディレクトリ設定をエクスポートする場合、ユーザ ディレクトリ接続情報がディレクトリ設定ファイルの Provider エレメントに表示されます。

データベース接続の説明

データベース接続を説明するには、directory.xml ファイルの Provider エレメントおよびその従属エレメントを使用します。

注: CA Identity Manager ディレクトリを作成する場合、directory.xml ファイル内のディレクトリ接続情報を提供する必要はありません。 管理コンソール内の CA Identity Manager ディレクトリ ウィザードの接続情報を提供します。

更新目的でのみ Provider エレメントを変更します。

Provider エレメント

Provider エレメントには以下の従属エレメントが含まれます。

JDBC（**必須**）

ユーザ ストアに接続するときに使用する JDBC データ ソースを識別します。 JDBC データ ソースを作成 (P. 111)するときに提供している JNDI 名を指定します。

Credentials（**必須**）

データベースにアクセスするためのユーザ名およびパスワードを提供します。

DSN

ユーザ ストアに接続するときに使用する ODBC データ ソースを識別します。

注: CA Identity Manager が SiteMinder と統合される場合にのみ、この従属エレメントは適用されます。 SiteMinder が含まれない CA Identity Manager 環境では、この従属エレメントは無視されます。

SiteMinderQuery

リレーショナル データベース内のユーザ情報を検索するためのカスタム クエリ スキームを指定します。

注: CA Identity Manager が SiteMinder と統合される場合にのみ、この従属エレメントは適用されます。 SiteMinder が含まれない CA Identity Manager 環境では、この従属エレメントは無視されます。

完了したデータベース接続は以下のようになります。

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Provider エレメントの属性を以下に示します。

type

データベースのタイプを指定します。 Microsoft SQL Server と Oracle データベースの場合、RDB を指定します（デフォルト）。

userdirectory

ユーザ ディレクトリ接続の名前を指定します。 このパラメータは、ディレクトリ作成中に提供する接続オブジェクト名に対応します。

CA Identity Manager が認証用に SiteMinder と統合される場合、インストール中に接続オブジェクトに対して指定する名前を使用して SiteMinder でユーザ ディレクトリ接続を作成します。既存の SiteMinder ユーザ ディレクトリに接続する場合は、接続オブジェクトに対して入力を促された場合に、そのユーザ ディレクトリの名前を入力します。 CA Identity Manager は、ユーザが指定する名前で userdirectory パラメータを入力します。

CA Identity Manager が SiteMinder と統合されない場合、userdirectory パラメータの値は、ユーザ ストアに JDBC 接続を提供する任意の名前です。

注: directory.xml ファイルにユーザ ディレクトリ接続の名前を指定しないでください。 CA Identity Manager は、ディレクトリ作成中に名前を提供するようにユーザに促します。

データベース クレデンシャル

データベースに接続するには、CA Identity Manager はデータ ソースに有効なクレデンシャルを提供する必要があります。 クレデンシャルは、以下の例のように、Credentials エレメントで定義されています。

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

ユーザが Credentials エレメントでパスワードを指定せず、管理コンソールで CA Identity Manager ディレクトリを作成しようとすると、パスワード クレデンシャルを促されます。

注: 管理コンソールでパスワードを指定することをお勧めします。

ユーザが管理コンソールでパスワードを指定する場合、CA Identity Manager はユーザに代わってパスワードを暗号化します。 そうでない場合に、パスワードをクリア テキストで表示しない場合は、CA Identity Manager と共にインストールされるパスワード ツールを使用して、パスワードを暗号化します。 SiteMinder パスワードには、パスワード ツールの使用に関する説明が含まれています。

注: 1 セットのクレデンシャルのみ指定できます。 ユーザが複数のデータ ソースを定義するとき場合、指定するクレデンシャルはすべてのデータ ソースに適用される必要があります。

クレデンシャル パラメータは以下のとおりです。

user

データ ソースにアクセスできるアカウント用のログイン ID を定義します。

directory.xml ファイルで user パラメータに対する値を指定しないでください。 CA Identity Manager は、管理コンソールで CA Identity Manager ディレクトリを作成するときに、ログイン ID を提供するようにユーザに促します。

cleartext

パスワードが directory.xml ファイルのクリア テキストで表示されるかどうかを決定します。

- True -- パスワードはクリア テキストで表示されます。
- False -- パスワードは暗号化されます（デフォルト）。

注: これらのパラメータはオプションです。

Data Source Name (DSN)

directory.xml ファイル内の DSN エレメントには 1 つのパラメータ（データベースに接続するために CA Identity Manager が使用する ODBC データ ソースの名前）があります。 name パラメータの値は、既存のデータ ソースの名前に一致する必要があります。

注: CA Identity Manager が SiteMinder と統合される場合にのみ、このエレメントは適用されます。 CA Identity Manager が SiteMinder と統合されない場合、このエレメントは無視されます。

name パラメータの値が @SmDirDSN の場合、directory.xml ファイルで DSN 名を指定する必要はありません。 CA Identity Manager は、directory.xml ファイルをインポートするときに、DSN 名を提供するようにユーザに促します。

フェイルオーバを設定するには、複数の DSN エレメントを定義します。プライマリ データ ソースがリクエストに応答しない場合、定義される次のデータ ソースがリクエストに応答します。

たとえば、以下の方法でフェイルオーバが設定されていると仮定します。

```
<DSN name="DSN1">
<DSN name="DSN2">
```

CA Identity Manager は、データベースに接続するためにデータ ソース DSN1 を使用します。DSN1 に問題がある場合、CA Identity Manager は DSN2 を使用して、データベースに接続しようとします。

注: Credentials エレメント (P. 143)で指定するクレデンシャルは、定義するすべての DSN に適用される必要があります。

SQL クエリ方式

CA Identity Manager は、リレーショナル データベースでユーザとグループ情報を検索するために、クエリ スキームを使用します。

注: CA Identity Manager が SiteMinder と統合される場合にのみ、このエレメントは適用されます。 SiteMinder が含まれない環境では、このパラメータは無視されます。

ユーザが管理コンソールで CA Identity Manager ディレクトリを作成するときに、CA Identity Manager は SiteMinder 内の必要なクエリ スキームに基づいて一連のクエリ スキームを生成します（SiteMinder クエリ スキームの詳細については、「*CA SiteMinder Web Access Manager Policy Server Configuration Guide*」を参照）。SiteMinder クエリ スキームのテーブルおよび列名は、ディレクトリ設定ファイルで指定するデータで置き換えられます。

カスタム クエリ スキームを定義する方法

クエリ スキームはディレクトリ設定ファイルの SiteMinderQuery エレメントで定義されています。 SiteMinderQuery エレメントは以下のようになります。

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

注: サンプル クエリで、' は一重引用符（'）の XML 構文です。

CA Identity Manager が SiteMinder と統合される場合にのみ、SiteMinderQuery エレメントが適用されます。

クエリ スキーム パラメータを以下に示します。

name

SiteMinder クエリ スキームの再定義された名前を指定します。

この値を変更しないでください。

query

実行する SQL ステートメントまたはストアド プロシージャを指定します。有効な値は以下のとおりです。

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL （ストアド プロシージャの場合）

注: これらのパラメータは SiteMinderQuery エレメントに必要です。

クエリ スキームをカスタマイズする前に、以下を実行してください。

- デフォルトのクエリ スキームに精通します。

  注: SQL クエリ スキームの詳細については、「*CA SiteMinder Web Access Manager Policy Server Configuration Guide*」を参照してください。

- SQL クエリを開発して幅広い経験を積みます。

デフォルト クエリ スキームの変更

デフォルト クエリ スキームを変更するには、以下の手順に従います。

次の手順に従ってください:

1. ディレクトリ設定ファイルをエクスポートします。

   CA Identity Manager は、生成されたクエリ スキームを含む、CA Identity Manager ディレクトリ用の現在の設定をすべて含むディレクトリ設定ファイルを生成します。

2. ディレクトリ設定ファイルを保存します。

   注: 元のディレクトリ設定ファイルのバックアップを作成する場合は、エクスポートされたファイルを保存する前に別の名前で、または別の場所にファイルを保存します。

3. 変更する CA Identity Manager で生成されたクエリ スキームを見つけます。
4. クエリ パラメータで実行するクエリ スキームまたはストアド プロシージャを入力します。

   注: クエリ名は変更しないでください。

5. 必要な変更が行われた後で、ディレクトリ設定ファイルを保存します。

   ファイルをインポートして、CA Identity Manager ディレクトリを更新 (P. 193)します。

リレーショナル データベースの汎用属性

汎用属性は CA Identity Manager で特別な意味があります。 汎用属性は以下の構文によって識別されます。

%ATTRIBUTENAME%

この構文で、*ATTRIBUTENAME* は大文字である必要があります。

汎用属性は属性説明 (P. 126)を使用して、1 つの物理属性にマップされます。

以下の属性説明では、属性 tblUsers.password は、汎用属性 %PASSWORD% にマップされ、CA Identity Manager は tblUsers.password の値をパスワードとして処理できるようになります。

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

汎用属性は必須のものもあれば、オプションのものもあります。

ユーザの既知の属性

既知のユーザ属性を以下に示します。

%ADMIN_ROLE_CONSTRAINT%

管理者 (P. 152)に割り当てられる管理ロール (P. 152)のリストが含まれています。

%ADMIN_ROLE_CONSTRAINT% にマップされた物理属性は、複数のロールを持てるよう、複数値に対応している必要があります。

%ADMIN_ROLE_CONSTRAINT% にマップされる属性にインデックスを付けることをお勧めします。

%CERTIFICATION_STATUS%

（ユーザ認証機能の使用で必須）

ユーザの認証ステータスに含まれています。

注: ユーザ認証の詳細については、「管理ガイド」を参照してください。

%DELEGATORS%

現在のユーザに作業アイテムを委任したユーザのリストにマップします。

この属性は委任を使用するのに必要です。%DELEGATORS% にマップした物理属性は複数値で、文字列を保持できる必要があります。

重要: CA Identity Manager タスクまたは外部ツールを使用してこのフィールドを直接編集すると、重大なセキュリティ上の影響が生じる場合があります。

%EMAIL%

（電子メール通知機能の有効化に必須）

ユーザの電子メール アドレスが格納されています。

%ENABLED_STATE%

（必須）

ユーザのステータスを追跡します。

注: %ENABLED_STATE% にマップされる物理属性のデータ型は、文字列である必要があります。

%FIRST_NAME%

ユーザの名が含まれています。

%FULL_NAME%

（必須）

ユーザの名および姓が含まれています。

%IDENTITY_POLICY%

ユーザ アカウントに適用されたアイデンティティ ポリシーのリストが含まれています。

CA Identity Manager は、アイデンティティ ポリシーをユーザに適用する必要があるかどうか決定するためにこの属性を使用します。 ポリシーで 1 回のみ適用設定が有効化されており、ポリシーが %IDENTITY_POLICY% 属性にリストされている場合、CA Identity Manager はポリシーの変更をユーザに適用しません。

注: アイデンティティ ポリシーの詳細については、「*管理ガイド*」を参照してください。

%LAST_CERTIFIED_DATE%

（ユーザ認証機能の使用で必須）

ユーザのロールが認証された日付が含まれています。

注: ユーザ認証の詳細については、「管理ガイド」を参照してください。

%LAST_NAME%

ユーザの姓が含まれています。

%ORG_MEMBERSHIP%

（組織がサポートされている場合に必須）

ユーザが所属する組織の一意の識別子が含まれています。

%ORG_MEMBERSHIP_NAME%

（組織がサポートされている場合に必須）

ユーザが所属する組織のユーザ フレンドリな名前が含まれています。

%PASSWORD%

ユーザ パスワードが含まれています。

注: CA Identity Manager 画面内では、%PASSWORD% 属性の値は、常にアスタリスク（*）文字の連続として表示されます。パスワードの非表示設定が属性やフィールドに対して指定されていない場合も同様です。

%PASSWORD_DATA%

（パスワード ポリシーのサポートに必須）

パスワード ポリシー情報を追跡する属性を指定します。

注: CA Identity Manager 画面内では、%PASSWORD_DATA% 属性の値は、常にアスタリスク（*）文字の連続として表示されます。パスワードの非表示設定が属性やフィールドに対して指定されていない場合も同様です。

%PASSWORD_HINT%

（必須）

ユーザ指定の質問と回答のペアが含まれています。 質問と回答のペアは、パスワードを忘れた場合に使用されます。

注: CA Identity Manager 画面内では、%PASSWORD_HINT% 属性の値は、常にアスタリスク（*）文字の連続として表示されます。パスワードの非表示設定が属性やフィールドに対して指定されていない場合も同様です。

%USER_ID%

（必須）

ユーザのログイン ID が格納されています。

グループ汎用属性

グループ汎用属性のリストは以下のとおりです。

%GROUP_ADMIN%

グループの管理者が含まれます。

注: %GROUP_ADMIN% 属性は複数値である必要があります。

%GROUP_DESC%

グループの説明が含まれます。

%GROUP_ID%

グループの一意の識別子が含まれます。

%GROUP_MEMBERSHIP%

（必須）

グループのメンバのリストが含まれます。

注: %GROUP_MEMBERSHIP% 属性は複数値である必要があります。

%GROUP_NAME%

（必須）

グループの名前を格納します。

%ORG_MEMBERSHIP%

（組織がサポートされている場合に必要）。

グループが所属している組織の一意の識別子が含まれます。

%ORG_MEMBERSHIP_NAME%

（組織がサポートされている場合に必要）。

グループが所属している組織のユーザ フレンドリな名前が含まれます。

%SELF_SUBSCRIBING%

ユーザがグループに参加できるかどうかを決定します。

%Admin_Role_Constraint% 属性

管理ロールを作成するときに、ロール メンバシップの 1 つ以上のルールを指定します。メンバシップ ルールを満たすユーザはロールを持ちます。たとえば、ユーザ マネージャ ロールのメンバシップ ルールが title=User Manager である場合、タイトルが「ユーザ マネージャ」のユーザがユーザ マネージャ ロールを持ちます。

注: ルールの詳細については、「管理ガイド」を参照してください。

%ADMIN_ROLE_CONSTRAINT% では、1 つのプロファイル属性を指定して、管理者の管理ロールをすべて格納できるようにします。

%ADMIN_ROLE_CONSTRAINT% 属性を使用する方法

すべての管理ロールの制約として %ADMIN_ROLE_CONSTRAINT% を使用するには、以下のタスクを実行します。

- 複数のロールに対応できるように、%ADMIN_ROLE_CONSTRAINT% 汎用属性を複数値プロファイル属性とペアにします。
- ユーザが CA Identity Manager ユーザ インターフェースで管理ロールを設定するときに、以下のシナリオを制約に指定できます。

  管理ロールは*ロール名*と等しい

  ロール名

  制約を提供しているロールの名前を定義します。

  たとえば、管理ロールはユーザ マネージャと等しい

注: 管理ロールは %ADMIN_ROLE_CONSTRAINT% 属性のデフォルトの表示名です。

汎用属性 の設定

汎用属性を設定するには、以下の手順に従います。

次の手順に従ってください:

1. ディレクトリ設定ファイルで、以下の記号を検索します。

   ##

   必要な値は 2 つのパウンド記号（##）によって識別されます。

2. ## から始まる値を、データベースに存在するように、必要な属性の物理名で置き換えます。 以下の形式を使用して、属性名を提供します。

   tablename.columnname

   たとえば、パスワード属性を tblUsers テーブルのパスワード列に格納する場合は、以下の方法でそれを指定します。

   tblUsers.password

3. 必要な値がすべて置き換えられ、希望するオプションの値が含まれるまで、手順 1 および 2 を繰り返します。
4. 必要に応じて、オプションの汎用属性を物理属性にマップします。
5. ディレクトリ設定ファイルを保存します。

自己登録グループを設定する方法

ディレクトリ設定ファイルで自己登録グループのサポートを設定することにより、セルフサービス ユーザがグループに参加できるようになります。

次の手順に従ってください:

1. 自己登録グループ セクションで、以下のように SelfSubscribingGroups エレメントを追加します。

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. 以下のパラメータの値を入力します。

   type

   CA Identity Manager が自己登録グループを検索するタイプを指定します。 有効な値は以下のとおりです。

   - NONE -- CA Identity Manager はグループを検索しません。 ユーザがグループに登録できないようにするには NONE を指定します。
   - ALL -- CA Identity Manager は、ユーザ ストアのグループをすべて検索します。 ユーザがすべてのグループに登録できる場合は、ALL を指定します。
   - INDICATEDORG （*組織をサポートする環境の場合のみ*） -- CA Identity Manager は、ユーザの組織およびそのサブ組織内の自己登録グループを検索します。 たとえば、ユーザのプロファイルがマーケティング組織にある場合、CA Identity Manager は、マーケティング組織、およびそのすべてのサブ組織内の自己登録グループを検索します。
   - SPECIFICORG （*組織をサポートする環境の場合のみ*） -- CA Identity Manager は特定の組織で検索します。 org パラメータで、特定の組織の一意の識別子を提供します。

org

CA Identity Manager が自己登録グループを検索する組織の一意の識別子を定義します。

注: type=SPECIFICORG の場合は、必ず org パラメータを指定してください。

3. 以下のアイテムのいずれかを変更した場合は、SiteMinder ポリシー サーバを再起動します。
   - SPECIFICORG への type パラメータの変更、または type パラメータ の SPECIFICORG への変更
   - org パラメータの値

自己登録グループのサポートが CA Identity Manager ディレクトリで設定されれば、CA Identity Manager 管理者はどのグループがユーザ コンソールで自己登録しているかを指定できます。

ユーザが自己登録する場合、CA Identity Manager は指定された組織のグループを検索し、ユーザに自己登録グループを表示します。

検証ルール

検証ルールは、ユーザがタスク画面フィールドに入力するデータに関する要件を適用します。要件にはデータ型または形式を適用することができます。また、データがタスク画面上の他のデータのコンテキストで有効であるかどうかを確認することができます。

検証ルールはプロファイル属性と関連付けられます。 タスクが処理される前に、CA Identity Manager はプロファイル属性に入力されたデータがすべての関連する検証ルールを満たしていることを確認します。

ディレクトリ設定ファイルで検証ルールを定義し、それらをプロファイル属性と関連付けることができます。

組織管理

リレーショナル データベースの場合、CA Identity Manager には、組織を管理するオプションがあります。 データベースが組織をサポートする場合には、以下の点が当てはまります。

- 組織には階層構造があります。
- ユーザ、グループ、および他の組織などすべての管理対象オブジェクトは、1 つの組織に属します。

- ユーザがある組織を削除する場合は、その組織に属しているオブジェクトも削除されます。

ユーザやグループ オブジェクトを設定した方法と同様に組織オブジェクトを設定しますが、いくつかの手順が追加されています。

組織サポートをセット アップする方法

組織サポートをセット アップする以下の手順を実装します。

1. データベース内の組織サポートを設定します (P. 155)。
2. ImsManagedObject (P. 121) で組織オブジェクトを説明します。

   必ず Table および UniqueIdentifier 従属エレメントを設定します。
3. トップレベルの組織 (P. 155) を設定します。
4. 組織を構成する属性を説明 (P. 126) します。
5. 組織オブジェクト (P. 156) の有汎用属性を定義します。

データベース内の組織サポートの設定

次の手順に従ってください:

1. エディタで以下のいずれかの SQL スクリプトを開きます。
   - Microsoft SQL Server データベース：

     ims_mssql_rdb.sql
   - Oracle データベース：

     ims_oracle_rdb.sql

     これらファイルは、以下の場所にあります。

     admin_tools¥directoryTemplates¥RelationalDatabase

     admin_tools は、管理ツールがインストールされた場所を示します。以下の場所のいずれかにデフォルトでインストールされます。

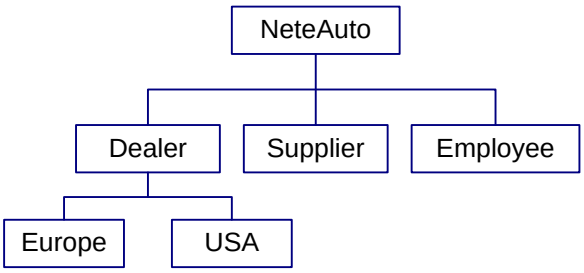
     Windows： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools

     UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
2. SQL スクリプトで、<@primary organization table@> を検索し、それを組織オブジェクトのプライマリ テーブルの名前で置き換えます。 SQL スクリプトを保存します。
3. データベースに対して SQL スクリプトを実行します。

ルート組織の指定

ルート組織はディレクトリのトップレベルまたは親組織として機能します。すべての組織はルート組織と関連します。

以下の図で、NeteAuto はルート組織です。他の組織は NeteAuto のサブ組織です。



完全なルート組織定義は以下のサンプルのようになります。

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
        <Result name="%ORG_ID%" />
    </RootOrg>
```

組織プロファイルおよび組織オブジェクトの一意の識別子を構成するテーブルを含む組織オブジェクトの基本情報を定義した後で、directory.xml ファイルのルート組織を指定します。

- RootOrg エレメントの value パラメータで、以下の例のように、ルート組織を取得するために CA Identity Manager が使用するクエリを定義します。

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- Result エレメントの name パラメータで、以下の例のように、組織の一意の識別子を入力します。

  ```
  <Result name="%ORG_ID%" />
  ```

  注: name パラメータの値は組織オブジェクトの一意の識別子である必要があります。

組織用の汎用属性

「汎用属性 (P. 82)」で説明されるように、組織プロファイルのプロファイルの属性の汎用属性を定義します。

必須およびオプションの組織の汎用属性は、以下のとおりです。

%ORG_DESCR%

組織の説明が含まれています。

%ORG_MEMBERSHIP%

（必須）

組織の親組織が含まれています。

注: %ORG_MEMBERSHIP% 属性の詳細については、「組織階層の定義」を参照してください。

%ORG_MEMBERSHIP_NAME%

（必須）

組織の親組織 (P. 157)のユーザ フレンドリな名前が含まれています。

%ORG_NAME%

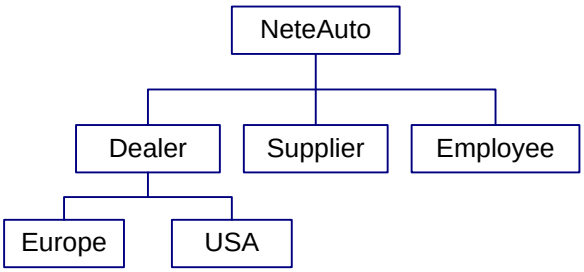
（必須）

組織の名前が含まれています。

組織階層を定義する方法

CA Identity Manager において、組織には、ルート組織およびサブ組織を含む階層構造があります。 サブ組織には、そのサブ組織もある場合があります。

ルート組織を除いて、組織にはそれぞれ親組織があります。 たとえば、以下の図で、ディーラは米国とヨーロッパ組織の親組織です。



親組織の一意の識別子は組織のプロファイルの属性に格納されます。この属性の情報を使用して、CA Identity Manager は組織階層を構築できます。

親組織を格納する属性を指定するには、%ORG_MEMBERSHIP% および %ORG_MEMBERSHIP_NAME% 汎用属性を、以下のように属性の説明で親組織の名前を格納する物理属性と共に使用します。

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0" />
```

ディレクトリ検索のパフォーマンスを改善する方法

ユーザ、組織、およびグループのディレクトリ検索のパフォーマンスを改善するには、以下のタスクを実行します。

- 管理者が検索クエリで指定できる属性にインデックスを作成します。
- デフォルトのディレクトリ タイムアウト設定を、ディレクトリ設定ファイル（directory.xml）内のタイムアウト検索パラメータの値を指定することにより無効にします。
- ユーザ ディレクトリを調整します。使用しているデータベースのマニュアルを参照してください。

ODBC データ ソースではデータベース固有のオプションを設定します。 詳細については、データ ソースのドキュメントを参照してください。

大規模な検索のパフォーマンスを改善する方法

CA Identity Manager が非常に大規模なユーザ ストアを管理する場合、多数の結果を返す検索により、システムがメモリ不足に陥る可能性があります。

以下の 2 つの設定は、CA Identity Manager がどのように大規模な検索を処理するか決定します。

- Maximum number of rows

  ユーザ ディレクトリの検索時に CA Identity Manager が返す結果の最大数を指定します。 結果数が限度を超えると、エラーが表示されます。

- Page size

  単一の検索で返すことができるオブジェクトの数を指定します。 オブジェクトの数がページ サイズを超える場合、CA Identity Manager は複数の検索を実行します。

  注: ユーザ ストアがページングをサポートせず、maxrows に対する値が指定される場合、CA Identity Manager は、検索サイズを制御するために maxrows 値のみを使用します。

以下の場所で最大行数の制限とページ サイズを設定できます。

- ユーザ ストア

  ほとんどのユーザ ストアおよびデータベースで、検索制限を設定できます。

  注: 詳細については、使用しているユーザ ストアまたはデータベースのドキュメントを参照してください。

- CA Identity Manager ディレクトリ

  CA Identity Manager ディレクトリを作成するために使用するディレクトリ設定ファイル（directory.xml）内に DirectorySearch エレメントを設定 (P. 61)できます。

  デフォルトでは、既存のディレクトリの最大行数とページ サイズの値が無制限に設定されます。新規ディレクトリに対しては、最大行数の値が無制限に、ページ サイズの値が 2000 に設定されます。

- 管理対象オブジェクト定義

  ディレクトリ全体ではなく、オブジェクトの特定のタイプに適用される最大行数の制限とページ サイズを設定するには、CA Identity Manager ディレクトリの作成に使用する directory.xml ファイル内で *管理対象オブジェクト定義*を設定 (P. 63)します。

  管理対象オブジェクト タイプに制限を設定することで、自社のビジネス要件に合わせた調整を行うことができます。 たとえば、ほとんどの会社ではグループ数よりユーザ数のほうが多くあります。 そのような会社では、ユーザ オブジェクトの検索だけに制限を設定できます。

- タスク検索画面

  ユーザ コンソールの検索およびリスト画面でユーザが参照する検索結果の数を制御できます。 結果数がタスクに対して定義されているページ当たりの結果数を超える場合、ユーザは結果の追加ページへのリンクを参照します。

  この設定は、検索によって返される結果数に影響しません。

  注: 検索およびリスト画面でのページ サイズ設定の詳細については、「管理ガイド」を参照してください。

最大行数の制限とページ サイズが複数の場所で定義されている場合、最も詳細な設定が適用されます。たとえば、管理対象オブジェクト設定はディレクトリ レベルの設定より優先されます。

第 5 章: CA Identity Manager ディレクトリ

CA Identity Manager ディレクトリによって、CA Identity Manager が管理するユーザ ディレクトリに関する情報が提供されます。 この情報は、ユーザ、グループ、組織などオブジェクトがユーザ ストアにどのように格納され、CA Identity Manager で表示されるかを説明します。

管理コンソールの CA Identity Manager ディレクトリ セクションで CA Identity Manager ディレクトリを作成、表示、エクスポート、更新し、および削除します。

注: CA Identity Manager が、SiteMinder ポリシー サーバのクラスタを使用する場合は、CA Identity Manager ディレクトリを作成または更新する前に 1 つのポリシー サーバ以外のすべてを終了します。

このセクションには、以下のトピックが含まれています。

CA Identity Manager ディレクトリを作成するための前提条件 (P. 161)
ディレクトリの作成方法 (P. 162)
ディレクトリ設定ウィザードを使用したディレクトリの作成 (P. 162)
XML 設定ファイルを含むディレクトリの作成 (P. 177)
プロビジョニング サーバ アクセスの有効化 (P. 179)
CA Identity Manager ディレクトリの表示 (P. 182)
CA Identity Manager ディレクトリ プロパティ (P. 183)
CA Identity Manager ディレクトリの設定を更新する方法 (P. 192)

CA Identity Manager ディレクトリを作成するための前提条件

CA Identity Manager ディレクトリを作成する前に、以下を行う必要があります。

- CA Identity Manager ディレクトリ を作成するか変更する前に、1 つの CA Identity Manager ノード以外のすべてを停止します。

  注: CA Identity Manager ノードのクラスタがある場合、管理コンソールに変更を加えるときには、1 つの CA Identity Manager ノードのみは有効にできます。

- CA Identity Manager ディレクトリを作成するか更新する前に 1 つのポリシー サーバ以外のすべてを停止します。

  注: SiteMinder ポリシー サーバのクラスタがある場合、管理コンソールに変更を加えるときには、1 つの SiteMinder ポリシー サーバのみは有効にできます。

ディレクトリの作成方法

管理コンソールで、CA Identity Manager ディレクトリ （ユーザ ストアの構造およびコンテンツを示す）およびプロビジョニング ディレクトリ（プロビジョニング サーバに必要な情報を格納する）を作成します。 これらのディレクトリは CA Identity Manager 環境と関連付けられます。

これらのディレクトリを作成するには、以下の方法のいずれかを使用します。

- ディレクトリ設定ウィザードの使用

  管理者にユーザ ストア用のディレクトリを作成するプロセスが順を追って示されます。 この方法を使用すると、起こりえる設定エラーを削減するのを支援します。

  注: ディレクトリ設定ウィザードを使用して、LDAP ユーザ ストア専用の新規ディレクトリを作成します。リレーショナル データベース用のディレクトリを作成するか、または既存のディレクトリを更新するには、directory.xml ファイルを直接インポートします。

- XML 構成ファイルの使用

  管理者がユーザ ストアまたはプロビジョニング サーバを作成するか変更するために、完全に設定された XML ファイルを選択できます。

  リレーショナル データベース用のディレクトリを作成している場合、または既存のディレクトリを更新している場合は、この方法を選択します。

詳細情報:

XML 設定ファイルを含むディレクトリの作成 (P. 177)
ディレクトリ設定ウィザードを使用したディレクトリの作成 (P. 162)

ディレクトリ設定ウィザードを使用したディレクトリの作成

ディレクトリ設定ウィザードにより、管理者はユーザ ストア用ディレクトリの作成プロセスを順を追って実行し、設定エラーを減らすことができます。 ウィザードを起動する前に、まず CA Identity Manager LDAP ディレクトリ設定テンプレートをアップロードする必要があります。 これらのテンプレートは、既知の必須属性であらかじめ設定されます。 LDAP ユーザストアまたはプロビジョニング ディレクトリの接続詳細を入力した後で、LDAP 属性の選択、汎用属性のマッピング、属性のメタデータの入力を行うことができます。 属性のマッピングが終了したら、［完了］をクリックしてディレクトリを作成します。

ディレクトリ設定ウィザードの起動

ディレクトリ設定ウィザードにより、管理者は CA Identity Manager テンプレートを選択し、ユーザの環境で使用するためにそのテンプレートを変更することができます。

次の手順に従ってください:

1. 管理コンソールから、［Directories］をクリックし、ウィザードから［Create］を選択します。

   ユーザ ストアを設定するディレクトリ設定ファイルを選択するように促されます。

2. ［Browse］をクリックして、以下のデフォルトの場所からユーザ ストアまたはプロビジョニング サーバを設定する設定ファイルを選択し、［Next］をクリックします。

   `admin_tools¥directoryTemplates¥directory¥`

   注: admin_tools は管理ツールがインストールされているディレクトリを指定し、directory は LDAP ベンダーの名前を指定します。

   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

3. ［Connection Details］画面で、LDAP ディレクトリまたはプロビジョニング サーバの接続情報、ディレクトリ検索パラメータ、およびフェイルオーバ接続情報を指定し、［Next］をクリックします。

4. ［Configure Managed Object］画面で、設定するオブジェクトを指定し、［Next］をクリックします。 以下のオブジェクトから選択できます。

   - Configure User Managed Object
   - Configure Group Managed Object
   - Configure Organization Object
   - Show summary and deploy directory

     注: ディレクトリを設定し終えた場合にのみ、［summary and deploy directory］を選択してください。

   a. ［Select Attribute］画面で、必要に応じて構造および補助クラスを表示および編集し、［Next］をクリックします。

   b. ［Select Attributes］の［Mapping Well-Knowns］画面で、CA Identity Manager の既知のエイリアスを 選択した LDAP 属性にマップし、［Next］をクリックします。

   c. （オプション）［Describe User Attributes］画面で、属性定義を表示、および変更し、［Next］をクリックします。表示名と説明を変更できます。

   d. （オプション）［User Attribute Details］画面で、管理するために選択した属性ごとにメタデータを定義し、［Next］をクリックします。

      ［Managed Object Selection］画面が表示されます。

      グループまたは組織を設定するには、管理対象オブジェクトを選択し、［Next］をクリックして、これらのオブジェクトに対する［Attributes］画面を参照します。

5. リストから［Show summary and deploy directory］を選択し、［Next］をクリックします。

   ［Confirmation］画面が表示されます。

6. ディレクトリの詳細を参照します。

   エラーがある場合は、［Back］ボタンをクリックして、適切な画面で変更します。 ［Finish］をクリックして変更を適用します。

   CA Identity Manager で設定が検証され、ディレクトリが作成されます。 新規ディレクトリを表示可能な［Directories listing］画面に戻ります。

[Select Directory Template]画面

この画面を使用して、LDAP がユーザ ストアまたはプロビジョニング サーバを設定するディレクトリ XML ファイルを選択します。

［参照］ボタンをクリックして、以下のデフォルトの場所からユーザ ストアまたはプロビジョニング サーバを設定する設定ファイルを選択します。

```
admin_tools¥directoryTemplates¥directory¥
```

注: admin_tools は管理ツールがインストールされているディレクトリを指定し、directory は LDAP ベンダーの名前を指定します。

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

ディレクトリ XML ファイルを選択した後で、［Next］をクリックして［Connection Details］画面に進みます。

[Connection Details]画面

この画面を使用して、ユーザのユーザ ストア用の設定クレデンシャルを入力します。 また、ディレクトリ検索パラメータを入力したり、フェイルオーバ接続を追加したりできます。 接続情報を入力した後で、［Next］をクリックして管理対象オブジェクトを選択します。

注: この画面に表示されるフィールドは、ユーザ ストアのタイプ、およびディレクトリ設定ウィザードを使用して接続を作成するか、XML ファイルを直接インポートして接続を作成するかによって異なります。

この画面には、以下のフィールドがあります。

Name

接続しているユーザ ディレクトリの名前を指定します。

Description

ユーザ ディレクトリの説明を指定します。

Host

ユーザ ストアが格納されているコンピュータのホスト名を指定します。

Port

ユーザ ストアが格納されているコンピュータのポートを指定します。

User DN

LDAP ユーザ ストアにアクセスするためのユーザ ドメイン名を指定します。

JDBC Data Source JNDI Name

CA Identity Manager がデータベースに接続するために使用する既存の JDBC データ ソースの名前を指定します。

Username

プロビジョニング サーバにアクセスするためのユーザ名を指定します。

注: プロビジョニング サーバの場合のみ。

Domain

プロビジョニング サーバにアクセスするためのドメイン名を指定します。

注: プロビジョニング サーバの場合のみ。

Password

LDAP ユーザ ストア/プロビジョニング サーバにアクセスするためのパスワードを指定します。

Confirm Password

LDAP ユーザ ストア/プロビジョニング サーバにアクセスするためのパスワードを確認します。

Secure Connection

これを選択した場合、LDAP ユーザ ディレクトリへの Secure Sockets Layer （SSL）接続を強制します。

Search Root

ディレクトリの開始ポイントとして機能する LDAP ディレクトリの場所を指定します。通常、組織（o）または組織単位（ou）です。

注: LDAP ユーザ ストアの場合のみ。

Search Maximum Rows

ユーザ ディレクトリの検索時に CA Identity Manager が返す結果の最大数を指定します。 結果数が限度を超えると、エラーが表示されます。

最大行数を設定することにより、検索結果を制限する LDAP ディレクトリ内の設定を無効にすることができます。矛盾する設定が適用される場合、LDAP サーバは優先度の最も低い設定を使用します。

Search Page Size

単一の検索で返すことができるオブジェクトの数を指定します。 オブジェクトの数がページ サイズを超える場合、CA Identity Manager は複数の検索を実行します。

［Search Page Size］を指定するときは、以下の点に注意してください。

- ［Search Page Size］オプションを使用するには、CA Identity Manager が管理するユーザ ストアでページングがサポートされる必要があります。 ユーザ ストアのタイプによっては、ページングをサポートするために追加の設定が必要な場合があります。 詳細については、「*設定ガイド*」を参照してください。
- ユーザ ストアがページングをサポートせず、［Search Maximum Rows］の値が指定される場合、CA Identity Manager は、［Search Maximum Rows］の値のみを使用して検索サイズを制御します。

Search Timeout

CA Identity Manager がディレクトリの検索を終了するまでの最大秒数を指定します。

Failover Host

プライマリ システムが利用できない場合に、重複するユーザ ストアまたは別のプロビジョニング サーバが存在するシステムのホスト名を指定します。 複数のサーバがリストに表示される場合、CA Identity Manager はリストされているのと同じ順序でシステムへの接続を試みます。

Failover Port

プライマリ システムが利用できない場合に、重複するユーザ ストアまたは別のプロビジョニング サーバが存在するシステムのポートを指定します。 複数のサーバがリストに表示される場合、CA Identity Manager はリストされているのと同じ順序でシステムへの接続を試みます。

[Add]ボタン

追加のファイルオーバ ホスト名およびポート番号を追加する場合にクリックします。

[Configure Managed Objects]画面

この画面を使用して、設定するオブジェクトを選択します。

以下はこの画面のフィールドのリストです。

Configure User Managed Object

ユーザがユーザ ストアにどのように格納され、CA Identity Manager でどのように表示されるのかを説明します。

Configure Group Managed Object

グループがユーザ ストアにどのように格納され、CA Identity Manager でどのように表示されるのかを説明します。

Configure Organization Managed Object

ユーザ ストアに組織が含まれる場合、組織がどのように格納され、CA Identity Manager で表示されるのかを説明します。

Show Summary and Deploy Directory

管理対象オブジェクトがすべて定義されており、ディレクトリを配備することを示します。 ［Show summary and the deploy directory］を選択した後で、［次へ］をクリックすると、サマリ ページが表示されます。

[Save]ボタン

XML ファイルを保存する場合にクリックします。

[Back]ボタン

［Connection Details］画面に戻って変更する場合にクリックします。

[Next]ボタン

［Select Attributes］画面に進んで、設定するユーザ、グループ、または組織属性を選択する場合にクリックします。

[Select Attributes]画面

この画面を使用して、ユーザ、グループ、または組織オブジェクト用の構造および補助クラスを変更または追加します。 この画面は、使用しているディレクトリのタイプに共通のディレクトリ スキーマおよびベスト プラクティスに基づいた値であらかじめ設定されます。管理者はドロップダウン メニューから新しいクラスを選択することにより、構造クラスを変更できます。 クラスを選択すると、新しい構造クラスに属する属性でテーブルが更新されます。

補助クラスはドロップダウン メニューから 1 つ選択することにより追加できます。 補助クラスを選択すると、新しい補助クラスに属する属性でテーブルが更新されます。

以下はこの画面に表示されるフィールドのリストです。

Structural Class Name

設定する属性の構造クラスを指定します。

[Change]ボタン

構造クラスを変更する場合にクリックします。

Auxiliary Class Name

設定する属性の補助クラスを指定します。

[Add]ボタン

設定する補助クラスを追加する場合にクリックします。

Object Class

コンテナ オブジェクト クラスを指定します。

ID

コンテナ ID を指定します。

Name

コンテナ名を指定します。

Attributes Table

物理名、オブジェクト クラス、属性が複数値であるかどうか、および選択した属性のデータ型を指定します。 このテーブル内の属性は Selected、Object Class、Multi-Valued、および Data Type によって並べ替えることができます。

[Back]ボタン

［Configured Managed Objects］画面に戻る場合にクリックします。

Next

必須およびオプションの既知のエイリアスをマップする［Well-Known Mapping］画面に進む場合にクリックします。

[Well-Known Mapping]画面

この画面を使用して、CA Identity Manager の汎用属性を、選択した LDAP 属性にマップします。 管理者は、テキスト フィールドに新しい汎用属性を入力し、［Add］ボタンをクリックすることにより、汎用属性のリストに追加できます（カスタム コードに対して要求される場合）。 画面がリフレッシュされるので、必要に応じて、汎用属性を追加し続けることができます。

以下はこの画面に表示されるフィールドのリストです。

Required Well-Knowns

LDAP 属性にマップされる必要があるユーザ、グループ、または組織（該当する場合）の汎用属性を指定します。

Optional Well-Knowns

オプションでマップできるユーザ、グループ、または組織（該当する場合）の汎用属性を指定します。

New Well-Known

カスタム コードによって参照される汎用属性を指定します。

[Add]ボタン

［Optional Well-Knowns］テーブルに新しい汎用属性を追加する場合にクリックします。

[Back]ボタン

［Select User Attributes］画面に戻ってさらに属性を選択する場合にクリックします。 この画面に戻ると、すでに行ったマッピングは保存され利用できるようになります。

[Next]ボタン

［Basic Object Attribute Definition］画面に進んで基本的な属性定義を指定する場合にクリックします。

詳細情報

LDAP ユーザ用の汎用属性 (P. 82)
グループ汎用属性 (P. 86)
ユーザの既知の属性 (P. 83)
組織の汎用属性 (P. 88)

[Basic Object Attribute Definition]定義画面

この画面を使用して、一般的に定義される定義（表示名や説明）を表示および変更します。

以下はこの画面に表示されるフィールドのリストです。

Managed Object Table

管理対象オブジェクトの表示名、物理名、汎用名、および説明を指定します。 必要に応じて、説明を変更する場合は、ドロップダウン メニューを使用します。 変更したら、［Next］をクリックして続行します。

[Back]ボタン

［Well-Known Mapping］画面に戻ってマッピングの詳細を変更する場合にクリックします。

[Next]ボタン

追加の属性定義を指定できる［Detailed Object Attribute Definition］画面に進む場合にクリックします。

[Detailed Object Attribute Definition]画面

この画面を使用して、他の属性定義を指定します。 管理者は、表示名を変更し、ユーザ コンソール画面の属性、値のデータ型、最大長、および検証ルール セットを管理することにより、選択した属性ごとのメタデータを定義できます。 属性定義を指定したら、［次へ］をクリックして続行します。

この画面のフィールドを以下に示します。

Display Name

管理対象オブジェクト属性の一意の名前を指定します。 これはユーザ コンソールに表示される名前です。

Tags

管理対象オブジェクト属性値のデータ分類タグを指定します。 タグはすべてオプションで、searchable を除いて、すべてデフォルトで false に設定されています。 以下のタグが選択できます。

Required

オブジェクトを作成するときに属性が必須であることを示します。

Multiple Values

属性が複数値として表示されることを示します。

Hidden

属性が非表示であることを示します。

System

属性がシステム属性であり、タスク画面に追加されないことを示します。

Searchable

属性が検索フィルタに追加されることを示します。 デフォルトで true です。

Sensitive Encrypt

属性が sensitive で、一連のアスタリスク（*）として表示されることを示します。

Hide in VST

属性が［View Submitted Tasks］の［Event Details］画面で非表示であることを示します。

Do not copy

管理者がオブジェクトのコピーを作成するときに属性が無視される必要があることを示します。

Previously encrypted

ユーザ ストアでアクセスされている属性が以前に暗号化され、復号化を必要とすることを示します。 オブジェクトが保存されるときに、クリア テキスト値はユーザ ストアに保存されます。

Untagged encrypted

属性が以前にユーザ ストアで暗号化され、暗号文の先頭に暗号化アルゴリズム タグ名がないことを示します。

Data Type

ユーザ コンソールで管理対象オブジェクト属性の値のデータ型を指定します。 以下のリストから選択できます。

- READONLY
- WRITEONCE
- READWRITE

Maximum Length

管理対象オブジェクト属性の値の最大長を指定します

デフォルト： 0

Validation Rule Set

管理対象オブジェクト属性の値を検証する検証ルール セットを指定します。 以下のリストから選択できます。

- User Validation
- Phone Format
- International Phone Format

[Back]ボタン

［Basic Object Attribute Definition］画面に戻って変更するにはこのボタンをクリックします。

[Next]ボタン

［Configure Managed Objects］画面に進むには、このボタンをクリックします。 この画面で、設定する次の管理対象オブジェクトを選択できます。 管理対象オブジェクトを設定したら、［Show summary and the deploy directory］を選択して、ディレクトリ情報を表示して、ディレクトリを配備します。

詳細情報

Sensitive 属性の管理 (P. 74)

[Confirmation]画面

この画面は、ディレクトリ詳細のサマリを表示します。

以下のリストはこの画面に表示されるフィールドです。

Connection Details

ユーザ ディレクトリの接続詳細を指定します。

User/Group/Organization Details

directory.xml に行われる変更を指定します。

[Back]ボタン

ウィザードで詳細を変更する場合にクリックします。

[Save]ボタン

［OK］をクリックして選択内容を保存します。

[Finish]ボタン

ディレクトリ詳細のすべてが正しく、ウィザードを終了する場合にクリックします。

設定が検証され、ディレクトリが作成されます。 新規ディレクトリがリスト表示される、[Directories listing]画面が表示されます。新規ディレクトリを編集またはエクスポートするには、ディレクトリ リストからそれを選択します。

XML 設定ファイルを含むディレクトリの作成

管理コンソール内の完了した directory.xml ファイルのインポートにより、CA Identity Manager ディレクトリを作成するか更新できます。

注: ディレクトリ設定ウィザードを使用する代わりに directory.xml ファイルを使用して、ディレクトリを作成する場合は、デフォルトの設定テンプレートを変更していることを確認します。詳細については、「*設定ガイド*」を参照してください。

次の手順に従ってください:

1. 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*:*port*/iam/immanage

   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。

   port

   アプリケーション サーバのポート番号を定義します。

2. ［ディレクトリ］をクリックします。

   CA Identity Manager ディレクトリ ウィンドウが表示されます。

3. XML から［作成］または［更新］をクリックします。

4. CA Identity Manager ディレクトリを更新するためのディレクトリ設定 XML ファイルのパスとファイル名を入力するか、ファイルを参照します。［次へ］をクリックします。

5. このウィンドウ内のフィールドに対する値を以下のように提供します。

   注: このウィンドウに表示されるフィールドはユーザ ストア タイプ、および手順 4 のディレクトリ設定ファイルで提供した情報によって異なります。ディレクトリ設定ファイルの以下のフィールドのいずれかに対する値を提供した場合、CA Identity Manager はユーザに再度これらの値を提供するように促しません。

   Name

   作成する CA Identity Manager ディレクトリの名前を決定します。

   Description

   （オプション） CA Identity Manager ディレクトリを説明します。

接続オブジェクト名

CA Identity Manager ディレクトリが説明するユーザ ディレクトリの名前を指定します。 以下の詳細の*いずれか*を入力します。

- CA Identity Manager が SiteMinder と統合されない場合は、ユーザ ストアに接続するために CA Identity Manager が使用するオブジェクトに任意の意味のある名前を指定します。
- CA Identity Manager が SiteMinder と統合され、SiteMinder でユーザ ディレクトリ接続オブジェクトを作成する場合は、任意の意味のある名前を指定します。 CA Identity Manager は指定する名前を使用して SiteMinder でユーザ ディレクトリ接続オブジェクトを作成します。
- CA Identity Manager が SiteMinder と統合され、既存の SiteMinder ユーザ ディレクトリに接続する場合は、ポリシー サーバ ユーザ インターフェースに表示される通りに、SiteMinder ユーザ ディレクトリ接続オブジェクトの名前を正確に指定します。

JDBC Data Source JNDI Name（**リレーショナル ディレクトリの場合のみ**）

CA Identity Manager がデータベースに接続するために使用する既存の JDBC データ ソースの名前を指定します。

ホスト（LDAP **ディレクトリの場合のみ**）

ユーザ ディレクトリがインストールされているシステムのホスト名または IP アドレスを指定します。

CA Directory ユーザ ストアの場合、ホスト システムの完全なドメイン名を使用します。 localhost は使用しないでください。

Active Directory ユーザ ストアの場合、IP アドレスではなくドメイン名を指定します。

ポート（LDAP **ディレクトリの場合のみ**）

ユーザ ディレクトリのポート番号を指定します。

Provisioning Domain

CA Identity Manager が管理するプロビジョニング ドメイン。

注: プロビジョニング ドメイン名では大文字と小文字が区別されます。

Username/User DN

ユーザ ストアにアクセスできるアカウントのユーザ名を指定します。

プロビジョニング ユーザ ストアの場合、指定するユーザ アカウントにはドメイン管理者 プロファイル、またはプロビジョニング ドメインの同等の権限セットが必要です。

Password

［ユーザ名］（リレーショナル データベース用）または［ユーザ DN］フィールド（LDAP ディレクトリ用）で指定したユーザ アカウントのパスワードを指定します。

Confirm Password

確認するために［パスワード］フィールドで入力したパスワードを再度入力します。

セキュア接続（LDAP ディレクトリの場合のみ）

CA Identity Manager が安全な接続を使用するかどうかを示します。

必ず Active Directory ユーザ ストア用のこのオプションを選択します。

［次へ］をクリックします。

6. CA Identity Manager ディレクトリの設定を確認します。 現在の設定で CA Identity Manager ディレクトリ を作成するには［完了］をクリックし、変更するには［前へ］をクリックします。

   ステータス情報が［ディレクトリ設定出力］ウィンドウに表示されます。

7. ［続行］をクリックして終了します。

   CA Identity Manager によってディレクトリが作成されます。

プロビジョニング サーバ アクセスの有効化

管理コンソールで［ディレクトリ］リンクを使用することによりプロビジョニング サーバへのアクセスを有効にします。

注: この手順への前提条件は、CA Directory でプロビジョニング ディレクトリをインストールすることです。詳細については、「インストール ガイド」を参照してください。

次の手順に従ってください:

1. 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:port/iam/immanage`

   hostname

   CA Identity Manager サーバがインストールされているシステムの完全修飾ホスト名を定義します。

   ポート

   アプリケーション サーバのポート番号を定義します。

2. ［ディレクトリ］をクリックします。

   CA Identity Manager ディレクトリ ウィンドウが表示されます。

3. ウィザードから［作成］をクリックします。

4. プロビジョニング ディレクトリ用のディレクトリ XML ファイルのパスとファイル名を入力します。 管理ツール フォルダの directoryTemplates¥ProvisioningServer に格納されます。このフォルダのデフォルトの場所は、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

   注: 変更せずに、インストールに応じて、このディレクトリ設定ファイルを使用できます。

5. ［次へ］をクリックします。

6. このウィンドウのフィールドに対する値を以下のように提供します。

   名前

   設定しているプロビジョニング サーバと関連付けられるプロビジョニング ディレクトリの名前です。

   - CA Identity Manager が SiteMinder と統合されない場合は、ユーザ ディレクトリに接続するために CA Identity Manager が使用するオブジェクトの意味のある名前を指定します。
   - CA Identity Manager が SiteMinder と統合される場合、2 つの選択肢があります。

     SiteMinder でユーザ ディレクトリ接続オブジェクトを作成する場合は、任意の意味のある名前を指定します。 CA Identity Manager は指定した名前で SiteMinder でこのオブジェクトを作成します。

     既存の SiteMinder ユーザ ディレクトリに接続する場合は、ポリシー サーバ ユーザ インターフェースに表示される通りに、SiteMinder ユーザ ディレクトリ接続オブジェクトの名前を正確に指定します。

   説明

   （オプション） CA Identity Manager ディレクトリを説明します。

   Host

   ユーザ ディレクトリがインストールされているシステムのホスト名または IP アドレスを指定します。

   Port

   ユーザ ディレクトリのポート番号を指定します。

ドメイン

CA Identity Manager が管理するプロビジョニング ドメインの名前を指定します。

重要: ドメイン名として外国語の文字を持つプロビジョニング ディレクトリを管理コンソールで作成しようとすると失敗します。

名前は、インストール中に指定したプロビジョニング ドメインの名前に一致する必要があります。

注: ドメイン名では大文字と小文字が区別されます。

Username

プロビジョニング マネージャにログインできるユーザを指定します。

ユーザはドメイン管理者プロファイル、またはプロビジョニング ドメイン用の権限の同等のセットが必要です。

パスワード

［ユーザ名］フィールドで指定したグローバル ユーザのパスワードを指定します。

Confirm Password

確認するために［パスワード］フィールドで入力したパスワードを再度入力します。

Secure Connection

CA Identity Manager が安全な接続を使用するかどうかを示します。

必ず Active Directory ユーザ ストア用のこのオプションを選択します。

ディレクトリ検索パラメータ

maxrows は、ユーザ ディレクトリを検索するときに CA Identity Manager が返すことができる結果の最大数を定義します。 この値は、LDAP ディレクトリで設定された制限よりも優先されます。 設定の競合が発生した場合、LDAP サーバは最小の設定を使用します。

注: maxrows パラメータは、CA Identity Manager タスク画面上に表示される結果の数を制限しません。 表示設定を指定するには、CA Identity Manager ユーザ コンソールでリスト画面定義を変更します。 手順については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

タイムアウトは、CA Identity Manager がディレクトリの検索を終了するまでの最大秒数を決定します。

フェイルオーバ接続

代替プロビジョニング サーバである 1 つ以上のオプションのシステムのホスト名およびポート番号。 複数のサーバがリスト表示される場合、CA Identity Manager はリスト順にシステムに接続しようとします。

プライマリ プロビジョニング サーバが失敗する場合、代替プロビジョニング サーバが使用されます。 プライマリ プロビジョニング サーバが再び利用できるようになる場合、別のプロビジョニング サーバが使用され続けます。 プロビジョニング サーバの使用に戻る場合は、代替プロビジョニング サーバを再起動します。

7. ［次へ］をクリックします。
8. ユーザやグループなどの、管理するオブジェクトを選択します。
9. 必要に応じてオブジェクトを設定した後で、［サマリの表示および配備ディレクトリの表示］をクリックし、プロビジョニング ディレクトリの設定を確認します。
10. これらのアクションのいずれかをクリックします。
    a. 変更するには［戻る］をクリックします。
    b. 展開するために後で戻る場合は、［保存］をクリックして、ディレクトリ情報を保存します。
    c. この手順を完了するには、［完了］をクリックし、プロビジョニングで環境の設定 (P. 204)を開始します。

CA Identity Manager ディレクトリの表示

CA Identity Manager ディレクトリを表示するには、以下の手順に従います。

次の手順に従ってください:

1. CA Identity ManagerManagement Console で、［ディレクトリ］をクリックします。
2. 表示する CA Identity Manager ディレクトリの名前をクリックします。 ［ディレクトリのプロパティ］ウィンドウが表示され、CA Identity Manager ディレクトリ プロパティが表示されます。

CA Identity Manager ディレクトリ プロパティ

CA Identity Manager ディレクトリ プロパティを以下に示します。

注: 表示されるプロパティは、CA Identity Manager ディレクトリと関連付けられるデータベースまたはディレクトリのタイプによって異なります。

Name

CA Identity Manager ディレクトリの一意の名前を定義します。

Description

CA Identity Manager ディレクトリの説明を入力します。

Type

ディレクトリ プロバイダのタイプを定義します。

Connection Object Name

CA Identity Manager ディレクトリが説明するユーザ ディレクトリの名前を表示します。

CA Identity Manager が SiteMinder と統合される場合、接続オブジェクト名は SiteMinder ユーザ ディレクトリ接続の名前に一致します。

ルート組織(組織が含まれるユーザ ストアの場合)

ユーザ ストアへエントリ ポイントを指定します。

LDAP ディレクトリの場合、ルート組織は DN として指定されます。 リレーショナル データベースの場合、ルート組織の一意の識別子が表示されます。

JDBC Data Source

CA Identity Manager がデータベースへの接続に使用する JDBC データソースの名前を指定します。

URL

ユーザ ストアの URL または IP アドレスを提供します。

Username

ユーザ ストアにアクセスできるアカウントのユーザ名を指定します。

Search Maximum Rows

検索の結果として返された行の最大数を示します。

Search Page Size

単一の検索で返すことができるオブジェクトの数を指定します。 オブジェクトの数がページ サイズを超える場合、CA Identity Manager は複数の検索を実行します。

注: CA Identity Manager が管理するユーザ ストアはページングをサポートする必要があります。ユーザ ストアのタイプによっては、ページングをサポートするために追加の設定が必要な場合があります。 詳細については、「*設定ガイド*」を参照してください。

ページングのサポート

ディレクトリがページングをサポートすることを示します。

Search Timeout（LDAP **ディレクトリの場合のみ**）

CA Identity Manager が検索を終了する前までに、ユーザ ストアを検索する最大秒数を指定します。

Provisioning Domain（[**プロビジョニング サーバ**]**ディレクトリの場合のみ**）

CA Identity Manager が管理するプロビジョニング ドメイン。

CA Identity Manager ディレクトリ プロパティ ウィンドウ

CA Identity Manager ディレクトリに関する一般情報は、選択するディレクトリのプロパティ ウィンドウで示されます。［ディレクトリのプロパティ］ウィンドウは以下のセクションに分割されます。

Directory Properties

プロビジョニングが環境に対して有効になっている場合、関連したプロビジョニング ドメインを含む CA Identity Manager ディレクトリの基本的なプロパティを表示します。

管理対象オブジェクト (P. 186)

CA Identity Manager が管理するユーザ ストア オブジェクトのタイプの説明を提供します。

検証ルールセット (P. 190)

CA Identity Manager ディレクトリに適用されるリスト検証ルール セットをリスト表示します。

環境

CA Identity Manager ディレクトリと関連付けられる環境をリスト表示します。 ディレクトリは複数の CA Identity Manager 環境と関連付けることができます。

CA Identity Manager 環境に関する情報を表示するには、環境の名前をクリックします。

CA Identity Manager ディレクトリのプロパティを変更するには、「CA Identity Manager ディレクトリの更新 (P. 193)」の説明に従って、ディレクトリ設定ファイルをインポートします。

プロパティを表示することのほか、以下のアクションを行うこともできます。

Update Authentication

管理者は、管理コンソールを認証するために CA Identity Manager で使用するディレクトリを変更できます。また、管理者は、既存の認証ディレクトリに追加の管理コンソール管理者を追加できます。

注: [認証の更新]オプションは、ネイティブ CA Identity Manager セキュリティが管理コンソールを保護する場合にのみ適用されます。ネイティブ セキュリティの有効化または異なるセキュリティ方法の使用の詳細については、「*設定ガイド*」を参照してください。

Export (P. 192)

XML ファイルとしてディレクトリ定義をエクスポートします。ディレクトリ設定をエクスポートした後で、XML ファイルを変更し、ディレクトリを更新するために再度インポートできます。 また、そのディレクトリ用の同じ設定を設定するために別のディレクトリへの XML ファイルをインポートできます。

Update (P. 193)

管理者がオブジェクトの属性など管理対象オブジェクト定義の追加または変更、検索パラメータの設定、ディレクトリ プロパティの変更を行えます。

管理対象オブジェクト プロパティおよび属性を表示する方法

管理対象オブジェクトは、ユーザ、グループ、組織などのユーザ ストアの一連のエントリについて説明します。管理対象オブジェクトに適用されるプロパティおよび属性はそのタイプのすべてのエントリに適用されます。たとえば、ユーザ プロファイルは、ユーザ管理対象オブジェクトのプロパティおよび属性からすべて構成されます。

管理対象オブジェクトの詳細を表示するには、オブジェクトの名前をクリックして、［Managed Object Properties］ウィンドウを開きます。

Managed Object Properties

［Managed Object Properties］ウィンドウは、管理対象オブジェクト タイプのプロパティおよび属性について説明します。

［Managed Object Properties］ウィンドウに関する情報は、管理しているユーザ ストアのタイプによって異なります。オブジェクトの管理対象プロパティは以下のとおりです。

Description

管理対象オブジェクトの説明を提供します。

Type

管理対象オブジェクトが表すエントリのタイプを示します。 オブジェクト タイプは以下のいずれかを指定できます。

- User
- Group
- Organization

オブジェクト クラス（LDAP ディレクトリの場合のみ）

管理対象オブジェクトのオブジェクト クラスを指定します。管理対象オブジェクトには複数のオブジェクト クラスがある場合があります。

並べ替え順（LDAP ディレクトリの場合のみ）

カスタム ビジネス ロジック内の検索結果を並べ替えるために、CA Identity Manager が使用する属性を指定します。並べ替え順は、ユーザ コンソール内の検索結果の順序には影響しません。

たとえば、ユーザ オブジェクトに対して cn 属性を指定する場合、CA Identity Manager はユーザの検索結果を cn 属性のアルファベット順に並べ替えます。

プライマリ テーブル（リレーショナル データベースの場合のみ）

管理対象オブジェクトの一意の識別子が含まれるテーブルを指定します。

最大行数

このタイプのオブジェクトを検索する場合に CA Identity Manager が返すことができる結果の最大数を指定します。 結果数が限度を超えると、エラーが表示されます。

最大行数を設定することにより、検索結果を制限する LDAP ディレクトリ内の設定を無効にすることができます。 矛盾する設定が適用される場合、LDAP サーバは優先度の最も低い設定を使用します。

ページ サイズ

単一の検索で返すことができるオブジェクトの数を指定します。 オブジェクトの数がページ サイズを超える場合、CA Identity Manager は複数の検索を実行します。

注: CA Identity Manager が管理するユーザ ストアはページングをサポートする必要があります。 ユーザ ストアのタイプによっては、ページングをサポートするために追加の設定が必要な場合があります。 詳細については、「*設定ガイド*」を参照してください。

コンテナのプロパティ（LDAP ディレクトリの場合のみ）

LDAP ディレクトリで、*コンテナ*グループには特定のタイプのオブジェクトが含まれます。 コンテナが指定されるときに、CA Identity Manager はコンテナ内のエントリのみを処理します。 たとえば、コンテナ ou=People を指定するときに、CA Identity Manager は People コンテナに存在するユーザを処理します。

注: 定義されたコンテナではなく LDAP ディレクトリに存在するユーザおよびグループが、ユーザ コンソールに表示される場合があります。 このようなユーザとグループを管理する場合に問題が発生する場合があります。

コンテナは、ユーザおよびグループのみをグループ化します。 組織のコンテナは指定できません。

コンテナのプロパティを以下に示します。

objectclass

特定のタイプのオブジェクトが作成されるコンテナの LDAP オブジェクト クラスを指定します。 たとえば、ユーザ コンテナのデフォルト値は "top,organizationalUnit," で、ユーザが LDAP 組織単位（ou）で作成されることを示します。

ID

コンテナ名（たとえば ou）を格納する属性を指定します。以下の例のように、属性と名前の値がペアになって、コンテナの相対 DN を構成します。

ou=People

Name

コンテナ名を指定します。

セカンダリ テーブルのプロパティ（リレーショナル データベースの場合のみ）

セカンダリ テーブルには、管理対象オブジェクトの追加の属性が含まれます。たとえば、tblUserAddress という名前のセカンダリ テーブルには、ユーザ管理対象オブジェクトの通り、都市、状態、および郵便番号属性が含まれる場合があります。

以下のプロパティがセカンダリ テーブルに表示されます。

テーブル

テーブルの名前を指定します。

リファレンス

プライマリ テーブルとセカンダリ テーブルの間のマッピングを説明します。

参照は以下の形式を使用して表示されます。

primarytable.attribute=secondarytable.attribute

たとえば、tblUsers.id= tblUserAddress.userid は、プライマリ テーブル（tblUsers）の ID 属性が tblUserAddress テーブルの userid 属性にマップすることを示します。

管理対象オブジェクト プロパティ ウィンドウ内の属性プロパティ

以下のプロパティが［Managed Object Properties］ウィンドウの属性に対して表示されます。

表示名

属性のユーザフレンドリな名前。この名前は、ユーザがユーザ コンソール内の特定のタスクのタスク ウィンドウを設計する場合に利用可能な属性のリストに表示されます。

物理名

ユーザ ストアの属性の名前。

Well-Known 名

汎用名は、ユーザ パスワードを格納するために使用される属性など、CA Identity Manager において特別な意味がある属性であることを示します。

[属性プロパティ]ウィンドウの属性プロパティ

［属性プロパティ］を開くためにその名前をクリックすることにより、属性に関する追加の詳細を表示できます。

以下の属性プロパティが［属性プロパティ］ウィンドウに表示されます。

説明

属性の説明を入力します。

物理名

ユーザ ストアで属性の名前を指定します。

オブジェクト クラス（LDAP ディレクトリのユーザ、グループ、および組織の属性の場合のみ）

属性がユーザ オブジェクトに対して指定されているプライマリ オブジェクト クラスの一部ではない場合に、ユーザ属性の LDAP 補助クラスを示します。

ユーザおよびグループのオブジェクトに対してのみ補助オブジェクト クラスを指定できます。

Well-Known 名

ユーザ パスワードを格納するために使用される属性など、CA Identity Manager において特別な意味がある属性を示します。

必須

属性に対して値が必要であるかどうかを以下のように示します。

- True は、属性に値が必要なことを示します。
- False は、値がオプションであることを示します。

読み取り専用

属性の権限レベルを以下のように示します。

- True は、属性を変更できないことを示します。
- False は、属性を変更できることを示します。

非表示

属性が特定のタスクに対してタスク ウィンドウで表示できるかどうかを示します。

非表示属性は、論理属性スキームで頻繁に使用されます。

注: 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。

複数値のサポート

属性が以下のように複数の値があるかどうかを示します（たとえば、グループのメンバを格納するために使用される属性は複数値です）。

- True は、属性が複数の値をサポートできることを示します。
- False は、属性が単一値のみ持つことができることを示します。

複数値区切り文字（リレーショナル データベースの場合のみ）

複数の値が単一の列に格納されるときに、値を区切る文字。

システム属性

属性が CA Identity Manager によってのみ使用されるかどうかを以下のように示します。

- True は、属性がシステム属性であることを示します。 属性はタスク ウィンドウに追加するのには利用できません。
- False は、ユーザがこの属性を使用できることを示します。 属性はタスク ウィンドウに表示される場合があります。

データのタイプ

属性のデータ型を指定します。 デフォルト値は文字列です。

最大文字数

属性値に指定できる最大長を指定します。 0 に設定されれば、値の長さに制限はありません。

Validation Rule Set

属性が 1 つと関連付けられる場合に、検証ルール セットの名前を指定します。

検証ルールセット

検証ルールはユーザがタスク ウィンドウ フィールドに入力するというデータの要件を設定します。 要件はデータ型または形式を実施できるか、またはデータがタスク ウィンドウの他のデータのコンテキストで有効であることを確認できます。

1 つ以上の検証ルールは検証ルール セットでグループ化されます。 その後、検証ルール セットはプロファイル属性と関連付けられます。 たとえば、ユーザは、mm-dd-yyyy の日付表示形式を実施する、Format Date 検証ルールを含む検証ルール セットを作成できます。その後、従業員の開始日を格納する属性と検証ルール セットを関連付けることができます。

注: ディレクトリ設定ファイルまたはユーザ コンソールで検証ルールおよび検証ルール セットを作成します。

［Managed Object Properties］ウィンドウは、CA Identity Manager ディレクトリに適用される検証ルール セットのリストを表示します。 検証ルール セットの詳細を表示するには、ルール セットの名前をクリックして、［Validation Rule Set Properties］ウィンドウを開きます。

Validation Rule Properties

以下の情報が［Validation Rule Properties］ウィンドウに表示されます。

Name

検証ルールの名前を提供します。

Description

ルールの説明を提供します。

Class

検証ルールを実装する Java クラスの名前を提供します。

検証ルールが Java クラスで定義されていない場合、このフィールドは表示されません。

Filename

検証ルールの JavaScript 実装が含まれるファイルの名前を提供します。

検証ルールがファイルで定義されていない場合、このフィールドは表示されません。

Regular Expression

検証ルールを実装する正規表現を提供します。

検証ルールが正規表現として定義されていない場合、このフィールドは表示されません。

Validation Rule Set Properties

以下の情報が［Validation Rule Set Properties］ウィンドウに表示されます。

Name

検証ルール セットの名前を指定します。

Description

検証ルール セットの説明を提供します。

［Validation Rule Set Properties］ページには、セットでの検証ルールのリストも含まれます。検証ルールの名前をクリックすると、［Validation Rule Properties］ウィンドウが開きます。

CA Identity Manager ディレクトリの設定を更新する方法

CA Identity Manager ディレクトリの現在の設定を表示するには、ディレクトリ設定をエクスポートし XML ファイルとしてそれを保存します。

ディレクトリ設定をエクスポートした後で、XML ファイルを変更し、ディレクトリを更新するために再度インポートできます。 また、そのディレクトリ用の同じ設定を設定するために別のディレクトリへの XML ファイルをインポートできます。

CA Identity Manager ディレクトリのエクスポート

CA Identity Manager ディレクトリをエクスポートするには、以下の手順に従います。

次の手順に従ってください:

1. ［ディレクトリ］をクリックします。

   CA Identity Manager ディレクトリのリストが表示されます。

2. エクスポートするディレクトリの名前をクリックします。

   CA Identity Manager ディレクトリ ウィンドウのプロパティが表示されます。

3. プロパティ ウィンドウの一番下で、［エクスポート］をクリックします。
4. プロンプトが表示されたら、XML ファイルを保存します。

CA Identity Manager ディレクトリの更新

CA Identity Manager ディレクトリを更新する目的は、以下のとおりです。

- オブジェクトの属性を含め、管理対象オブジェクト定義の追加または変更
- 検索パラメータの設定
- ディレクトリ プロパティの変更

注: CA Identity Manager はオブジェクトまたは属性定義を削除しません。

ディレクトリ設定ファイルには、加える変更のみ含めることができます。すでに定義されているプロパティまたは属性を含める必要はありません。

注: CA Identity Manager ノードのクラスタがある場合、管理コンソールに変更を加えるときには、1 つの CA Identity Manager ノードのみは有効にできます。 CA Identity Manager ディレクトリを作成または変更する前に、1 つの CA Identity Manager ノード以外のすべてを停止します。

次の手順に従ってください:

1. XML ファイルに現在の CA Identity Manager ディレクトリ設定をエクスポートします。
2. ユーザの変更を反映させるために XML ファイルを変更します。
3. ［ディレクトリ］をクリックします。

   CA Identity Manager ディレクトリのリストが表示されます。
4. 更新するディレクトリの名前をクリックします。

   CA Identity Manager ディレクトリのプロパティが表示されます。
5. プロパティ ウィンドウの下部にある［エクスポート］をクリックします。
6. CA Identity Manager ディレクトリを更新するために XML ファイルのパスとファイル名を入力するか、ファイルを参照します。 ［完了］をクリックします。

   ディレクトリ設定出力フィールドにステータス情報が表示されます。
7. ［続行］をクリックします。

CA Identity Manager ディレクトリの削除

CA Identity Manager ディレクトリを削除する前に、それと関連付けられるすべての CA Identity Manager 環境を削除します。

次の手順に従ってください:

1. 管理コンソールで、［ディレクトリ］をクリックします。

   CA Identity Manager ディレクトリのリストが表示されます。

2. 削除するディレクトリの左側のチェック ボックスをオンにします（複数可）。
3. ［削除］をクリックします。

   確認メッセージが表示されます。

4. ［OK］をクリックし、削除を確定します。

第 6 章: CA Identity Manager 環境

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 環境 (P. 195)
CA Identity Manager 環境を作成するための前提条件 (P. 196)
CA Identity Manager 環境の作成 (P. 198)
CA Identity Manager 環境にアクセスする方法 (P. 203)
プロビジョニング用の環境を設定する方法 (P. 204)
環境の管理 (P. 217)
設定の管理 (P. 224)
ポリシー ルール評価の最適化 (P. 231)
ロールおよびタスクの設定 (P. 232)
システム マネージャ アカウントの変更 (P. 234)
CA Identity Manager 環境のステータスへのアクセス (P. 236)

CA Identity Manager 環境

CA Identity Manager 環境はユーザ ストアのビューです。 CA Identity Manager 環境では、ユーザ、グループ、組織、タスク、およびロールを管理できます。 また、ユーザに電子メール アカウントや他のアプリケーションなど管理対象エンドポイントのアカウントを与えることもできます。

管理コンソールを使用すると、以下のタスクを実行できます。

- CA Identity Manager 環境を作成、変更、または削除します。
- CA Identity Manager 環境をエクスポートおよびインポートします。
- 詳細設定を設定します。
- ロールおよびタスクをインポートします。
- システム マネージャ アカウントをリセットします。

CA Identity Manager 環境を作成するための前提条件

始める前に、以下の表を使用して、必要な情報を収集します。

CA Identity Manager 環境設定ワークシート	
必要な情報	**値**
選択対象の CA Identity Manager 環境のわかりやすい名前。 例： MyEnvironment。	
環境用のデフォルト パスワード ポリシーの［リダイレクト URL］を形成するために CA Identity Manager が使用するベース URL。 例： http://server.yourcompany.org	
環境内の保護タスクにアクセスするために URL に追加されるエイリアス。 例： http://server.yourcompany.org/iam/im/alias	
自己登録や忘れたパスワード タスクなどのパブリック タスクにアクセスするために URL に追加されるエイリアス。 例： http://server.yourcompany.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration **注**: ユーザの環境にパブリック タスクが含まれない場合は、パブリック エイリアスを指定する必要はありません。	
パブリック エイリアスを提供した場合に、パブリック ユーザとなる既存のユーザの名前。 CA Identity Manager は、パブリック タスクにアクセスする際、ユーザから提供されたクレデンシャルの代わりに、パブリック ユーザのクレデンシャルを使用します。	

CA Identity Manager 環境設定ワークシート	
必要な情報	**値**
CA Identity Manager (P. 107) の名前	
CA Identity Manager 環境がプロビジョニングをサポートする場合は、プロビジョニング ディレクトリの名前。	
CA Identity Manager 環境を管理する既存ユーザのための一意の識別子。 例： myadmin	
CA Identity Manager が SiteMinder と統合される場合に、CA Identity Manager 環境を保護する SiteMinder エージェントまたはエージェント グループの名前。	

CA Identity Manager 環境の作成

CA Identity Manager 環境では、一連のロールやタスクでディレクトリ内のオブジェクトを管理できます。 CA Identity Manager 環境ウィザードを使用して、CA Identity Manager 環境を作成する手順を説明します。

CA Identity Manager 環境を作成する前に、以下の点に注意します。

- LDAP ユーザ ストアを使用しており、CA Identity Manager ディレクトリ用のディレクトリ設定ファイル（directory.xml）内の ou=People などユーザ コンテナを設定していることを前提としています。 CA Identity Manager 環境を作成する場合に選択するユーザ`がそのコンテナに存在することを確認します。ユーザ コンテナに存在しないユーザ アカウントを選択すると障害が発生する場合があります。
- ユーザがフラットなユーザ構造を持つ LDAP ユーザ ディレクトリを管理するように CA Identity Manager 環境を設定する場合は、選択したユーザのプロファイルにはユーザの組織が含まれる必要があります。 ユーザのプロファイルが正しく設定されるようにするには、directory.xml ファイル (P. 90)の汎用属性 %ORG_MEMBERSHIP% に対応する物理属性にユーザの組織の名前を追加します。 たとえば、物理属性の説明が directory.xml ファイルの汎用属性 %ORG_MEMBERSHIP% にマップされ、ユーザが「従業員」組織に属する場合、ユーザのプロファイルには「属性/値ペアの説明 = 従業員」が含まれる必要があります。

次の手順に従ってください:

1. CA Identity Manager がポリシー サーバのクラスタを使用する場合は、1 つのポリシー サーバ以外のすべてを停止します。
2. CA Identity Manager ノードのクラスタがある場合は、1 つの CA Identity Manager ノード以外のすべてを停止します。
3. 管理コンソールで、［環境］をクリックします。
4. ［新規作成］をクリックします。

   CA Identity Manager 環境ウィザードが開きます。
5. 以下の情報を入力します。
   - **環境名**

     環境の一意の名前を指定します
   - **説明**

     環境を説明します

- **保護されたエイリアス**

  従業員などの一意の名前を指定します。 このエイリアスは、CA Identity Manager 環境の保護タスクにアクセスするために URL に追加されます。 たとえば、エイリアスが従業員である場合、従業員環境にアクセスするための URL は http://my*server.mycompany.com*/iam/im/employees です

  注: エイリアスは大文字と小文字を区別し、スペースを含めることはできません。 エイリアスを指定する場合は、句読点またはスペースのない小文字を使用することを推奨します。

- **ベース URL**

  CA Identity Manager 用の URL を指定します。URL にはホスト名が必要です。localhost を含めることはできません。 また、エイリアスを含めないでください。例： http://*myserver.mycompany.com*/iam/im。

  Web エージェントを使用している場合は、Web エージェントの URL を反映するためにベース URL が変更されていることを確認します。

  注: CA Identity Manager リソースを保護するために Web エージェントを使用している場合は、ベース URL フィールドでポート番号を指定しないでください。 ユーザが Web エージェントを使用しており、ベース URL にポート番号が含まれる場合は、CA Identity Manager タスクへのリンクが正しく動作しません。

  CA Identity Manager リソースの保護の詳細については、お使いのアプリケーション サーバの「インストール ガイド」を参照してください。

  ［次へ］をクリックします。

6. 作成している環境と関連付ける CA Identity Manager ディレクトリを選択し、［次へ］をクリックします。

7. CA Identity Manager 環境がプロビジョニングをサポートする場合は、使用する適切なプロビジョニング サーバを選択します。

   注: CA Identity Manager ディレクトリとしてプロビジョニング ディレクトリを選択している場合は、プロビジョニング サーバを選択するよう指示するメッセージが表示されません。

8. パブリック タスクのサポートを設定します。 通常、これらのタスクは、自己登録や忘れたパスワードのタスクなどのセルフサービス タスクです。 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: ユーザがセルフサービスのタスクを使用できるようにするには、パブリック タスク サポートを設定します。

   a. パブリック タスクにアクセスできるように、URL に追加される一意の名前を指定します。

      例： デフォルトの自己登録タスクにアクセスするには以下の URL を使用します。

      http://*myserver.mycompany.com*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration

      この URL で、*alias* は提供する一意の名前です。

   b. パブリック ユーザ アカウントとして機能する以下の既存のユーザ アカウントのいずれかを指定します。CA Identity Manager は、このアカウントを使用して、不明なユーザがクレデンシャルを提供する必要なしに、パブリック タスクにアクセスできるようにします。

      - LDAP ユーザは、パブリック ユーザ アカウントの一意の識別子または相対 DN を入力します。 この値が %USER_ID% well-known (P. 82) にマップされていることを確認します。 たとえば、ユーザ DN の DN が uid=Admin1、ou=People、ou= Employees、ou=NeteAuto の場合は、「Admin1」を入力します。
      - リレーショナル データベース ユーザは、ディレクトリ設定ファイルの汎用属性 %USER_ID% にマップされる値、またはユーザの一意の識別子を入力します。

   ユーザの完全な識別子を表示するには、［検証］をクリックします。

9. この環境に対して作成するタスクおよびロールを選択します。 以下のタスクを実行できます。

   - **デフォルト ロールの作成**

     環境内で最初に利用可能なデフォルトのタスクおよびロールのセットを作成します。 管理者は、ユーザ コンソールで新しいタスクおよびロールを作成するためのテンプレートとして、これらのタスクおよびロールを使用できます。

   - **システム マネージャ ロールのみの作成**

     システム マネージャ ロール、およびそれと関連付けられるタスクのみを作成します。

     システム マネージャ ロールは環境にアクセスするために必要です。

     システム マネージャは、ユーザ コンソールで新しいタスクおよびロールを作成できます。

- **ファイルからのロールのインポート**

  別の CA Identity Manager 環境からエクスポートしたロール定義ファイルをインポートします。

  注: CA Identity Manager 環境を使用するには、ロール定義ファイルには、少なくともシステム マネージャ ロール、または同様のタスクを含むロールが含まれる必要があります。

  ［ファイルからのロールのインポート］オプション ボタンを選択し、ロール定義ファイルのパスとファイル名を入力するか、インポートするファイルを参照します。

10. ユーザの環境用のデフォルト タスクのセットを作成するためのロール定義ファイルを選択し、［次へ］をクリックします。

    ロール定義ファイルは、特定の機能をサポートするのに必要なタスクおよびロールのセットを定義する XML ファイルです。 たとえば、Active Directory と UNIX の NIS エンドポイントを管理する場合は、それらのロール定義ファイルを選択します。

    注: この手順はオプションです。 新しい機能をサポートするための追加のデフォルト タスクを作成しない場合は、この画面をスキップします。

11. この環境のシステム マネージャとしてユーザを以下のように定義します。

    a. ［システム マネージャ］フィールドで、ディレクトリ設定ファイル内の %USER_ID% well-known 属性にマップされる値を入力するか、または以下のユーザ アカウントのいずれかを指定します。

       - LDAP ユーザは、ユーザの一意の識別子または相対 DN を入力します。たとえば、ユーザ DN の DN が uid=Admin1、ou=People、ou= Employees、ou=NeteAuto の場合は、「Admin1」を入力します。
       - リレーショナル データベース ユーザは、ユーザの一意の識別子を入力します。

    b. ［追加］をクリックします。

       CA Identity Manager は、ユーザのリストにユーザの完全な識別子を追加します。

    c. ［次へ］をクリックします。

    システム マネージャを指定するときは、以下の点に注意してください。

    - システム マネージャはユーザ ストアの管理者と同じユーザであっては *なりません*。
    - 環境に対して複数のシステム マネージャを指定できます。 ただし、管理コンソールで最初のシステム マネージャのみ指定できます。 追加のシステム マネージャを指定するには、ユーザ コンソールで適切なユーザにシステム マネージャ ロールを割り当てます。

12. ［インバウンド管理者］フィールドで、インバウンド マッピングにマップされる管理タスクを実行できる CA Identity Manager 管理者アカウントを指定します。

    ユーザは、任意のユーザ上でそれらのタスクをすべて実行できる必要があります。 ［プロビジョニング同期マネージャ］ロールには、デフォルトのインバウンド マッピングに含まれているプロビジョニング タスクが含まれます。

13. キーストア用のパスワード（データを暗号化し復号化するキーのデータベース）を入力します。

    このパスワードを定義することは、動的なキーを定義するための前提条件です。 System （［秘密鍵］タスク）を使用して、環境を作成した後にパスワードを変更できます。

    環境用の設定の概要について説明するページが表示されます。

14. 環境用の設定を確認します。 変更するには［前へ］をクリックし、現在の設定で CA Identity Manager 環境を作成するには［完了］をクリックします。

    ［環境設定の出力］画面には、環境作成の進捗状況が表示されます。

15. CA Identity Manager 環境ウィザードを終了するには、［続行］をクリックします。

16. 環境を起動します。

    環境名をクリックし、［開始］をクリックします。

17. 手順 1 でポリシー サーバを停止している場合は、再起動します。

CA Identity Manager 環境にアクセスする方法

CA Identity Manager 環境を作成した後で、ブラウザで URL を入力することによりそれにアクセスできます。

注: 管理コンソールにアクセスするために使用するブラウザ内の Javascript を有効にします。

URL の形式は、ユーザが環境、およびアクセスするタスクのタイプをどのように設定したかによって異なります。

- ユーザ コンソールから保護されているタスクにアクセスするには、以下の URL を使用します。

  `http://`*`hostname`*`/iam/im/`*`alias`*

  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

  alias

  環境エイリアス（たとえば従業員）のエイリアスを定義します。

  CA Identity Manager 環境に対して作成したシステム マネージャ アカウントなど、権限のある管理者アカウントを備えた CA Identity Manager 環境にログインします。

  注: ユーザがパブリック タスクを設定しない場合、CA Identity Manager タスクはすべて保護されます。

- パブリック タスク（クレデンシャルを提供することをユーザに要求しない）にアクセスするには、以下の形式の URL を使用します。

  `http://`*`hostname`*`/iam/im/`*`alias`*`/index.jsp?task.tag=`*`tasktag`*

  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。

alias

パブリック タスクのエイリアスを定義します。たとえば、セルフサービス。

task_tag

タスクが呼び出すためのタグを定義します。

ユーザ コンソールでタスクを設定する場合は、タスク タグを指定します。

デフォルトの自己登録および忘れたパスワード リセット タスク用のタスク タグは、SelfRegistration と ForgottenPasswordReset です。

注: 詳細については、「管理ガイド」を参照してください。

プロビジョニング用の環境を設定する方法

プロビジョニング サーバへのアクセスを有効 (P. 179)にした後で、プロビジョニング用の環境を設定できます。

その後、「インバウンド管理者」と呼ばれる特別の CA Identity Manager ユーザを作成し、プロビジョニング サーバへの接続を作成し、プロビジョニング マネージャでインバウンド同期を設定します。

注: 環境のプロビジョニング プロパティを変更する場合は常に、変更が有効になるためにアプリケーション サーバを再起動することを確認します。

インバウンド管理者の設定

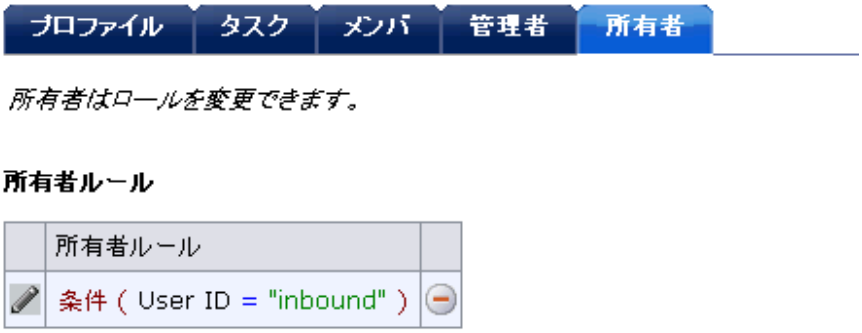
インバウンド同期が動作するには、*インバウンド管理者*と呼ばれる特別な CA Identity Manager ユーザを作成します。 CA Identity Manager の前のリリースでは、インバウンド管理者は*企業*ユーザと呼ばれました。ユーザはこのユーザ アカウントにログインしません。代わりに、CA Identity Manager がそれを内部的に使用します。ただし、このユーザ アカウントを作成し、それに適切なタスクを与えます。

次の手順に従ってください:

1. システム マネージャ ロールを所有するユーザとして CA Identity Manager 環境にログインします。
2. ユーザを作成します。 このことを示すため、ユーザを**インバウンド**と指定する場合があります。

3. ［管理ロール］（［管理ロールの変更］）を選択し、同期に使用するタスクが含まれるロールを選択します。
   - プロビジョニングによるユーザの作成
   - 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の変更

   注: デフォルトの同期タスクを変更していない場合は、［プロビジョニング同期マネージャ］ロールを使用します。
4. ［メンバ］タブで、以下を含むメンバ ポリシーを追加します。
   - 新規ユーザが満たすメンバ ルール。
   - インバウンド同期をトリガするプロビジョニング ディレクトリの変更によって影響を受けるすべてのユーザへのアクセスを提供するスコープ ルール。

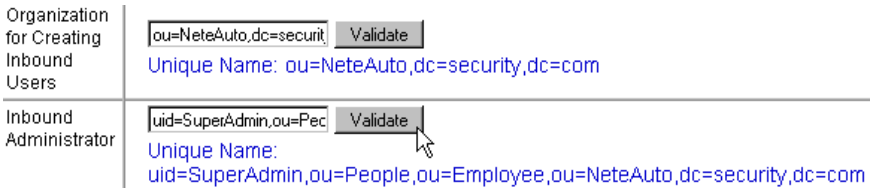


5. 管理コンソールで以下の手順を実行します。
   a. 環境を選択します。
   b. ［詳細設定］-［プロビジョニング］を選択します。
   c. CA Identity Manager ディレクトリに組織が含まれる場合は、［インバウンド ユーザを作成する組織］フィールドに入力します。

      この組織は、インバウンド同期が発生する場合に、ユーザが作成される場所です。 たとえば、ユーザがプロビジョニング ディレクトリに追加される場合、CA Identity Manager はこの組織にユーザを追加します。

d. 手順 2 で作成したユーザのユーザ ID を使用して［インバウンド管理者］フィールドに入力します。

e. 完全なユーザ ID が入力されたユーザ ID の下に表示される場合は、以下の例のように、ユーザ ID 受理されたことを確認するために［検証］をクリックします。



f. この画面上の他のフィールドを変更します。変更は必要ではありません。

変更する際には、フィールドがどのように連携するのかを理解しておく必要があります。 各フィールドの詳細については、画面のヘルプのリンクをクリックしてください。

プロビジョニング サーバへの環境の接続

次の手順に従ってください:

1. 管理コンソールで、［環境］をクリックします。

   既存の環境のリストが表示されます。

2. プロビジョニング サーバと関連付ける環境の名前をクリックします。
3. ［プロビジョニング サーバ］フィールドの右矢印アイコンをクリックします。

   ［プロビジョニング プロパティ］画面が表示されます。

4. プロビジョニング サーバを選択します。
5. 画面下部の［保存］をクリックします。
6. プロビジョニング マネージャで同期を設定します。（P. 206）

プロビジョニング マネージャでの同期の設定

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 CA Identity Manager を最新の状態に保ちます。 変更には、プロビジョニング マネージャを使用した変更と、プロビジョニング サーバがコネクタを持つエンドポイントでの変更が含まれます。プロビジョニング サーバはそれぞれ単一の環境をサポートします。 ただし、現在の環境が利用不可能な場合は、クラスタ内の別のシステム上にバックアップ環境を設定できます。

次の手順に従ってください:

1. ［開始］-［CA Identity Manager］-［プロビジョニング マネージャ］を選択します。
2. ［システム］（CA Identity Manager セットアップ）をクリックします。
3. CA Identity Manager Server がインストールされているシステムの名前で［ホスト名］フィールドに入力します。
4. アプリケーション サーバ ポート番号で［ポート］フィールドに入力します。
5. 環境用のエイリアスで［環境名］フィールドに入力します。
6. CA Identity Manager サーバとの通信に HTTP を使用して個別の通知を暗号化するのではなく、HTTPS プロトコルを使用する場合は、［セキュア接続］を選択します。
7. ［追加］をクリックします。
8. 環境のバックアップ バージョンごとに手順 3 ～ 6 を繰り返します。

   現在の環境用のアプリケーション サーバが利用不可能な場合は、CA Identity Manager はバックアップ環境にフェイルオーバします。 フェイルオーバ順序を設定するために現在の環境とバックアップ環境を並べ替えることができます。
9. これが最初の環境である場合は、埋め込みコンポーネントのユーザに対して CA Identity Manager インストール中に入力されたパスワードを使用して、［共有秘密キー］フィールドに入力します。

   注: FIPS がこのインストールで有効な場合、これらのフィールドは当てはまりません。
10. ログ レベルを以下のように設定します。
    - ログなし -- 情報はログ ファイルに書き込まれていません。
    - エラー -- エラー メッセージのみがログに記録されます。
    - 情報 -- エラーと情報メッセージがログに記録されます（デフォルト）。
    - 警告 -- エラー、警告および情報メッセージがログに記録されます。
    - デバッグ -- 情報がすべてログに記録されます。
11. 環境にログインする前に、アプリケーション サーバを再起動します。

注: インバウンド同期操作、および同期中に遭遇したあらゆる問題のログについては、以下のファイルを参照します。

PSHOME¥logs¥etanotify<date>.log

カスタム プロビジョニング ロールのインポート

環境を作成する場合、デフォルト ロールを使用するか、または作成するカスタム ロール定義ファイルを使用するかを選択します。カスタム ロール定義をインポートする場合は、プロビジョニングのみのロール定義もインポートします。環境を作成したら、以下のフォルダのいずれかにある ProvisioningOnly-RoleDefinitions.xml ファイルからロール定義をインポートします。

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

admin_tools のデフォルトの場所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

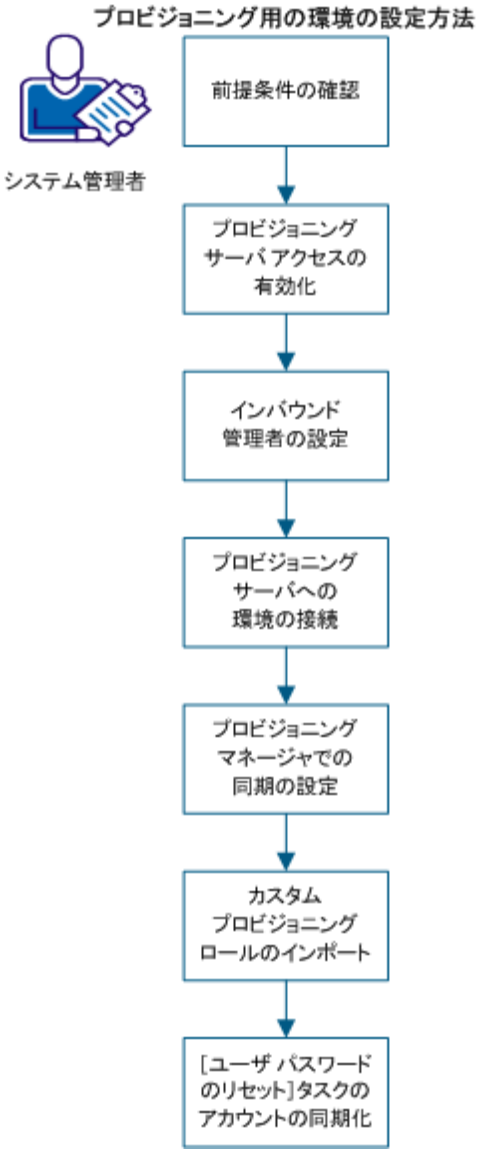
[ユーザ パスワードのリセット]タスクのアカウントの同期化

ユーザが CA Identity Manager 環境用のプロビジョニングを有効にする前に、［ユーザ パスワードのリセット］タスクに対するアカウントの同期化設定は、［タスク完了時］に設定されます。ただし、ユーザがユーザ プロビジョニング用のロールおよびタスクを作成する ProvisioningOnly-RoleDefinitions.xml 設定ファイルをインポートする場合、アカウント同期は無効です。

［ユーザ パスワードのリセット］を使用して、アカウントの同期化をトリガするには、このタスクのアカウント同期を［タスク完了時］に戻します。

Connector Xpress を使用してコネクタを作成および展開する手順

CA Identity Manager によって管理されるユーザに別のシステムのアカウントを提供するように環境のプロビジョニングを設定できます。 アカウントは、電子メール アカウントなど、追加リソースへのアクセスをユーザに提供します。CA Identity Manager によって作成するプロビジョニング ロールを割り当てることによって、これらの追加アカウントを提供します。



管理者として、以下の手順を実行します。

1. 前提条件の確認 (P. 210)

2. プロビジョニング サーバ アクセスの有効化 (P. 179)
3. インバウンド管理者の設定 (P. 204)
4. プロビジョニング サーバへの環境の接続 (P. 206)
5. プロビジョニング マネージャでの同期の設定 (P. 206)
6. カスタム プロビジョニング ロールのインポート (P. 208)
7. ［ユーザ パスワードのリセット］タスクのアカウントの同期化 (P. 208)

前提条件の確認

プロビジョニング用の環境を設定する前に、プロビジョニング ディレクトリが CA Directory にインストールされていることを確認します。詳細については、「インストール ガイド」を参照してください。

プロビジョニング サーバ アクセスの有効化

管理コンソールで［ディレクトリ］リンクを使用することによりプロビジョニング サーバへのアクセスを有効にします。

注: この手順への前提条件は、CA Directory でプロビジョニング ディレクトリをインストールすることです。詳細については、「インストール ガイド」を参照してください。

次の手順に従ってください:

1. 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:port/iam/immanage`

   hostname

   CA Identity Manager サーバがインストールされているシステムの完全修飾ホスト名を定義します。

   ポート

   アプリケーション サーバのポート番号を定義します。

2. ［ディレクトリ］をクリックします。

   CA Identity Manager ディレクトリ ウィンドウが表示されます。

3. ウィザードから［作成］をクリックします。

4. プロビジョニング ディレクトリ用のディレクトリ XML ファイルのパスとファイル名を入力します。 管理ツール フォルダの directoryTemplates¥ProvisioningServer に格納されます。このフォルダのデフォルトの場所は、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

   注: 変更せずに、インストールに応じて、このディレクトリ設定ファイルを使用できます。

5. ［次へ］をクリックします。

6. このウィンドウのフィールドに対する値を以下のように提供します。

   名前

   設定しているプロビジョニング サーバと関連付けられるプロビジョニング ディレクトリの名前です。

   - CA Identity Manager が SiteMinder と統合されない場合は、ユーザ ディレクトリに接続するために CA Identity Manager が使用するオブジェクトの意味のある名前を指定します。
   - CA Identity Manager が SiteMinder と統合される場合、2 つの選択肢があります。

     SiteMinder でユーザ ディレクトリ接続オブジェクトを作成する場合は、任意の意味のある名前を指定します。 CA Identity Manager は指定した名前で SiteMinder でこのオブジェクトを作成します。

     既存の SiteMinder ユーザ ディレクトリに接続する場合は、ポリシー サーバ ユーザ インターフェースに表示される通りに、SiteMinder ユーザ ディレクトリ接続オブジェクトの名前を正確に指定します。

   説明

   （オプション） CA Identity Manager ディレクトリを説明します。

   Host

   ユーザ ディレクトリがインストールされているシステムのホスト名または IP アドレスを指定します。

   Port

   ユーザ ディレクトリのポート番号を指定します。

ドメイン

CA Identity Manager が管理するプロビジョニング ドメインの名前を指定します。

重要: ドメイン名として外国語の文字を持つプロビジョニング ディレクトリを管理コンソールで作成しようとすると失敗します。

名前は、インストール中に指定したプロビジョニング ドメインの名前に一致する必要があります。

注: ドメイン名では大文字と小文字が区別されます。

Username

プロビジョニング マネージャにログインできるユーザを指定します。

ユーザはドメイン管理者プロファイル、またはプロビジョニング ドメイン用の権限の同等のセットが必要です。

パスワード

［ユーザ名］フィールドで指定したグローバル ユーザのパスワードを指定します。

Confirm Password

確認するために［パスワード］フィールドで入力したパスワードを再度入力します。

Secure Connection

CA Identity Manager が安全な接続を使用するかどうかを示します。

必ず Active Directory ユーザ ストア用のこのオプションを選択します。

ディレクトリ検索パラメータ

maxrows は、ユーザ ディレクトリを検索するときに CA Identity Manager が返すことができる結果の最大数を定義します。 この値は、LDAP ディレクトリで設定された制限よりも優先されます。 設定の競合が発生した場合、LDAP サーバは最小の設定を使用します。

注: maxrows パラメータは、CA Identity Manager タスク画面上に表示される結果の数を制限しません。 表示設定を指定するには、CA Identity Manager ユーザ コンソールでリスト画面定義を変更します。 手順については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

タイムアウトは、CA Identity Manager がディレクトリの検索を終了するまでの最大秒数を決定します。

フェイルオーバ接続

代替プロビジョニング サーバである 1 つ以上のオプションのシステムのホスト名およびポート番号。 複数のサーバがリスト表示される場合、CA Identity Manager はリスト順にシステムに接続しようとします。

プライマリ プロビジョニング サーバが失敗する場合、代替プロビジョニング サーバが使用されます。 プライマリ プロビジョニング サーバが再び利用できるようになる場合、別のプロビジョニング サーバが使用され続けます。 プロビジョニング サーバの使用に戻る場合は、代替プロビジョニング サーバを再起動します。

7. ［次へ］をクリックします。
8. ユーザやグループなどの、管理するオブジェクトを選択します。
9. 必要に応じてオブジェクトを設定した後で、［サマリの表示および配備ディレクトリの表示］をクリックし、プロビジョニング ディレクトリの設定を確認します。
10. これらのアクションのいずれかをクリックします。
    a. 変更するには［戻る］をクリックします。
    b. 展開するために後で戻る場合は、［保存］をクリックして、ディレクトリ情報を保存します。
    c. この手順を完了するには、［完了］をクリックし、プロビジョニングで環境の設定 (P. 204)を開始します。

インバウンド管理者の設定

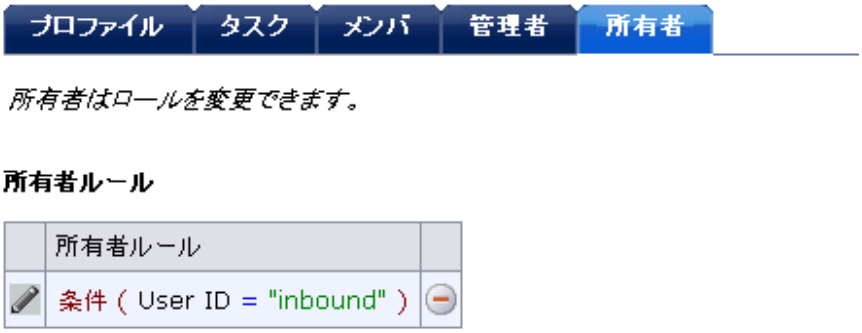
インバウンド同期が動作するには、*インバウンド管理者*と呼ばれる特別な CA Identity Manager ユーザを作成します。 CA Identity Manager の前のリリースでは、インバウンド管理者は*企業ユーザ*と呼ばれました。ユーザはこのユーザ アカウントにログインしません。代わりに、CA Identity Manager がそれを内部的に使用します。ただし、このユーザ アカウントを作成し、それに適切なタスクを与えます。

次の手順に従ってください:

1. システム マネージャ ロールを所有するユーザとして CA Identity Manager 環境にログインします。
2. ユーザを作成します。 このことを示すため、ユーザを**インバウンド**と指定する場合があります。

3. ［管理ロール］（［管理ロールの変更］）を選択し、同期に使用するタスクが含まれるロールを選択します。
   - プロビジョニングによるユーザの作成
   - 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の変更

   注: デフォルトの同期タスクを変更していない場合は、［プロビジョニング同期マネージャ］ロールを使用します。
4. ［メンバ］タブで、以下を含むメンバ ポリシーを追加します。
   - 新規ユーザが満たすメンバ ルール。
   - インバウンド同期をトリガするプロビジョニング ディレクトリの変更によって影響を受けるすべてのユーザへのアクセスを提供するスコープ ルール。

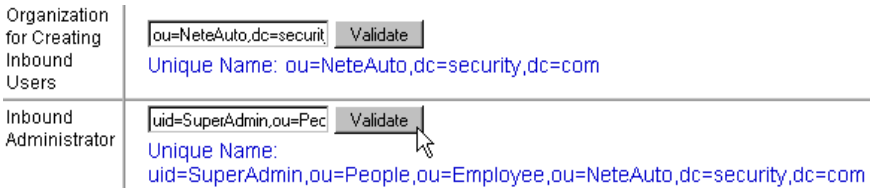


5. 管理コンソールで以下の手順を実行します。
   a. 環境を選択します。
   b. ［詳細設定］-［プロビジョニング］を選択します。
   c. CA Identity Manager ディレクトリに組織が含まれる場合は、［インバウンド ユーザを作成する組織］フィールドに入力します。

      この組織は、インバウンド同期が発生する場合に、ユーザが作成される場所です。 たとえば、ユーザがプロビジョニング ディレクトリに追加される場合、CA Identity Manager はこの組織にユーザを追加します。

d. 手順 2 で作成したユーザのユーザ ID を使用して［インバウンド管理者］フィールドに入力します。

e. 完全なユーザ ID が入力されたユーザ ID の下に表示される場合は、以下の例のように、ユーザ ID 受理されたことを確認するために［検証］をクリックします。



f. この画面上の他のフィールドを変更します。変更は必要ではありません。

変更する際には、フィールドがどのように連携するのかを理解しておく必要があります。 各フィールドの詳細については、画面のヘルプのリンクをクリックしてください。

プロビジョニング サーバへの環境の接続

次の手順に従ってください:

1. 管理コンソールで、［環境］をクリックします。

   既存の環境のリストが表示されます。

2. プロビジョニング サーバと関連付ける環境の名前をクリックします。
3. ［プロビジョニング サーバ］フィールドの右矢印アイコンをクリックします。

   ［プロビジョニング プロパティ］画面が表示されます。

4. プロビジョニング サーバを選択します。
5. 画面下部の［保存］をクリックします。
6. プロビジョニング マネージャで同期を設定します。 (P. 206)

プロビジョニング マネージャでの同期の設定

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 CA Identity Manager を最新の状態に保ちます。 変更には、プロビジョニング マネージャを使用した変更と、プロビジョニング サーバがコネクタを持つエンドポイントでの変更が含まれます。プロビジョニング サーバはそれぞれ単一の環境をサポートします。 ただし、現在の環境が利用不可能な場合は、クラスタ内の別のシステム上にバックアップ環境を設定できます。

次の手順に従ってください:

1. ［開始］-［CA Identity Manager］-［プロビジョニング マネージャ］を選択します。
2. ［システム］（CA Identity Manager セットアップ）をクリックします。
3. CA Identity Manager Server がインストールされているシステムの名前で［ホスト名］フィールドに入力します。
4. アプリケーション サーバ ポート番号で［ポート］フィールドに入力します。
5. 環境用のエイリアスで［環境名］フィールドに入力します。
6. CA Identity Manager サーバとの通信に HTTP を使用して個別の通知を暗号化するのではなく、HTTPS プロトコルを使用する場合は、［セキュア接続］を選択します。
7. ［追加］をクリックします。
8. 環境のバックアップ バージョンごとに手順 3 ～ 6 を繰り返します。

   現在の環境用のアプリケーション サーバが利用不可能な場合は、CA Identity Manager はバックアップ環境にフェイルオーバします。 フェイルオーバ順序を設定するために現在の環境とバックアップ環境を並べ替えることができます。
9. これが最初の環境である場合は、埋め込みコンポーネントのユーザに対して CA Identity Manager インストール中に入力されたパスワードを使用して、［共有秘密キー］フィールドに入力します。

   注: FIPS がこのインストールで有効な場合、これらのフィールドは当てはまりません。
10. ログ レベルを以下のように設定します。
    - ログなし -- 情報はログ ファイルに書き込まれていません。
    - エラー -- エラー メッセージのみがログに記録されます。
    - 情報 -- エラーと情報メッセージがログに記録されます（デフォルト）。
    - 警告 -- エラー、警告および情報メッセージがログに記録されます。
    - デバッグ -- 情報がすべてログに記録されます。
11. 環境にログインする前に、アプリケーション サーバを再起動します。

注: インバウンド同期操作、および同期中に遭遇したあらゆる問題のログについては、以下のファイルを参照します。

PSHOME¥logs¥etanotify<date>.log

カスタム プロビジョニング ロールのインポート

環境を作成する場合、デフォルト ロールを使用するか、または作成するカスタム ロール定義ファイルを使用するかを選択します。カスタム ロール定義をインポートする場合は、プロビジョニングのみのロール定義もインポートします。環境を作成したら、以下のフォルダのいずれかにある ProvisioningOnly-RoleDefinitions.xml ファイルからロール定義をインポートします。

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

admin_tools のデフォルトの場所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

[ユーザ パスワードのリセット]タスクのアカウントの同期化

ユーザが CA Identity Manager 環境用のプロビジョニングを有効にする前に、［ユーザ パスワードのリセット］タスクに対するアカウントの同期化設定は、［タスク完了時］に設定されます。ただし、ユーザがユーザ プロビジョニング用のロールおよびタスクを作成する ProvisioningOnly-RoleDefinitions.xml 設定ファイルをインポートする場合、アカウント同期は無効です。

［ユーザ パスワードのリセット］を使用して、アカウントの同期化をトリガするには、このタスクのアカウント同期を［タスク完了時］に戻します。

環境の管理

このセクションでは、環境を管理する方法について説明します。

CA Identity Manager 環境プロパティの変更

管理コンソールの［CA Identity Manager 環境プロパティ］画面では、以下のタスクを実行できます。

- 環境用の現在の設定を表示します。
- 説明、ベース URL、および保護されたエイリアスやパブリック エイリアスを変更します。

- アップグレードの後に既存の CA Identity Manager 環境をインポートします。

  注: 既存の CA Identity Manager 環境のインポートの詳細については、「インストール ガイド」のアップグレード セクションを参照してください。
- 環境を開始するおよび停止します
- 以下のタスクを設定するためのアクセス ページ :
  - **詳細設定**

    CA Identity Manager API を使用して構築される機能など、拡張機能を設定します。
  - **ロールおよびタスクの設定**

    別の CA Identity Manager 環境からエクスポートしたロール定義ファイルをインポートします。
  - **システム マネージャ**

    システム マネージャ ロールを割り当てます。

次の手順に従ってください:

1. CA Identity Manager が SiteMinder ポリシー サーバのクラスタを使用する場合は、1 つのポリシー サーバ以外のすべてを停止します。
2. CA Identity Manager ノードのクラスタがある場合は、1 つの CA Identity Manager ノード以外のすべてを停止します。
3. ［環境］をクリックします。

   CA Identity Manager 環境 画面が CA Identity Manager 環境のリストと共に表示されます。
4. 変更する CA Identity Manager 環境の名前をクリックします。

   ［CA Identity Manager プロパティ］画面が表示されて、以下のプロパティが表示されます。

   OID

   環境の一意な識別子を定義します。 ユーザが CA Identity Manager 環境を作成する場合、CA Identity Manager はこの識別子を生成します。

   タスク永続性データベースからのタスク削除を設定する場合は、OID を使用します。 詳細については、「インストール ガイド」を参照してください。

   名前

   CA Identity Manager 環境の一意の名前を指定します。

   説明

   CA Identity Manager 環境の説明を示します。

CA Identity Manager ディレクトリ

環境が関連付けられる CA Identity Manager ディレクトリを指定します。

詳細ログ出力の有効化

CA Identity Manager が記録する情報量を制御し、環境をインポートするときに環境ログを表示します。 ユーザが 環境またはファイルから他のオブジェクト定義をインポートする場合に、環境ログが管理コンソールのステータス ウィンドウに表示されます。

注: このチェック ボックスをオンにすると、パフォーマンスに著しく影響を与える場合があります。

詳細ログには、環境での各オブジェクト（タスク、画面、ロールおよびポリシー）およびその属性の検証と展開のメッセージが含まれます。

詳細ログを参照するには、このチェック ボックスをオンにし 環境プロパティを保存します。 ユーザがファイルからのロールまたは他の設定をインポートする場合、追加の情報がログに表示されます。

プロビジョニング サーバ

プロビジョニング ユーザ ストアとして使用されるプロビジョンング ディレクトリを指定します。

［プロビジョニング プロパティ］ページでプロビジョニング ディレクトリを設定するには、右矢印ボタンをクリックします。

バージョン

CA Identity Manager のバージョン番号を定義します。

ベース URL

環境用の保護されたエイリアスまたはパブリック エイリアスを含まない CA Identity Manager URL の部分を指定します。

CA Identity Manager は、環境用のデフォルト パスワード ポリシーで［パスワード サービス］タスクを指す［リダイレクト URL］を形成します。

保護されたエイリアス

CA Identity Manager 環境用のユーザ コンソールで 保護されているタスクにアクセスするためのベースの URL 名を定義します。

パブリック エイリアス

自己登録と忘れたパスワード タスクなどパブリック タスクにアクセスするためのベース URL 名を定義します。

パブリック ユーザ

パブリック タスクにアクセスするためにユーザに提供されたクレデンシャルの代わりに CA Identity Manager が使用するユーザ アカウントを定義します。

ジョブ タイムアウト

タスクがサブミットされてからステータス メッセージが表示されるまでに CA Identity Manager が待機する時間を決定します。

この値は［詳細設定］の［ユーザ コンソール］ページで設定されます。

ステータス

CA Identity Manager 環境を停止または再起動します。

CA Identity Manager 8.1 からのタスク永続性データの移行

CA Identity Manager 8.1 タスク永続性データベースから CA Identity Manager 12.6.4 タスク永続性データベースにデータを移行します。

詳細については、「インストール ガイド」を参照してください。

注:［CA Identity Manager 8.1 からのタスク永続性データの移行］ボタンは、CA Identity Manager の旧バージョンで作成され、CA Identity Manager 12.6.4 に移行した環境でのみ表示できます。

5. 必要に応じて、説明、ベース URL または保護されたエイリアスやパブリック エイリアスを変更します。
6. 環境プロパティを変更した場合は、CA Identity Manager 環境を再起動します。
7. 手順 1 でポリシー サーバを停止している場合は、再起動します。

環境設定

環境に固有の情報は、以下の 3 つの環境設定ファイルに格納されます。

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

注: *alias* は環境のエイリアスを示します。 環境作成時に、alias を指定します。

ユーザは、これらのファイルを含む ZIP ファイルを生成します。これは、ユーザが環境設定をエクスポートする際に、現在の設定を反映します。

環境設定をエクスポートした後で、以下のいずれかのタスクを実行する設定をインポートします。

- 同様の設定で複数の環境を管理します。 この場合、必要とする設定で 1 つの環境を作成し、他の環境へのそれらの設定をインポートし、次に、必要に応じて、各環境の設定をカスタマイズします。
- 開発システムから実稼働システムに環境を移行します。
- CA Identity Manager の新バージョンにアップグレードした後に既存の環境を更新します。

CA Identity Manager 環境のエクスポート

実稼働システム上の CA Identity Manager 環境を展開するには、開発またはステージング システムから環境をエクスポートし、実稼働システムへその環境をインポートします。

注: ユーザが以前にエクスポートされた環境をインポートする場合、CA Identity Manager に管理コンソール内のステータス ウィンドウ内のログが表示されます。このログで各管理対象オブジェクトおよびその属性の検証および展開情報を参照するには、環境をエクスポートする*前に*、［環境プロパティ］ページ上で［詳細ログ出力の有効化］フィールドを選択します。［詳細ログ出力の有効化］フィールドを選択するとインポート中に重大なパフォーマンスの問題を引き起こす場合があることを確認します。

次の手順に従ってください:

1. 管理コンソールの［環境］をクリックします。

   CA Identity Manager 環境画面が CA Identity Manager 環境のリストと共に表示されます。
2. エクスポートする環境を選択します。
3. [エクスポート]ボタンをクリックします。

   ［ファイルのダウンロード］画面が表示されます。
4. 実稼働システムにアクセス可能な場所に ZIP ファイルを保存します。
5. ［完了］をクリックします。

環境情報は、別の環境にインポート可能な ZIP ファイルにエクスポートされます。

CA Identity Manager 環境のインポート

以下のいずれかのタスクを実行するために CA Identity Manager 環境設定をインポートできます。

- 同様の設定で複数の環境を管理します。 この場合、必要とする設定で 1 つの環境を作成し、他の環境へのそれらの設定をインポートし、次に、必要に応じて、各環境の設定をカスタマイズします。
- 開発システムから実稼働システムに環境を移行します。
- CA Identity Manager の新バージョンにアップグレードした後に既存の環境を更新します。

次の手順に従ってください:

1. 管理コンソールの［環境］をクリックします。

   CA Identity Manager 環境画面が CA Identity Manager 環境のリストと共に表示されます。

2. ［インポート］ボタンをクリックします。

   ［環境のインポート］画面が表示されます。

3. 環境をインポートするのに必要な ZIP ファイルを参照します。
4. ［完了］をクリックします。

環境は CA Identity Manager へインポートされます。

CA Identity Manager 環境の再起動

次の手順に従ってください:

1. 管理コンソールの［環境］をクリックします。

   CA Identity Manager 環境画面が CA Identity Manager 環境のリストと共に表示されます。

2. 開始する CA Identity Manager 環境の名前をクリックします。

   ［CA Identity Manager 環境プロパティ］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。

環境の再起動

環境を停止および開始します。

停止

現在実行されている環境を停止します。

開始

現在実行されていない環境を開始します。

CA Identity Manager 環境の削除

CA Identity Manager 環境を削除するには、以下の手順に従います。

注: CA Identity Manager が高度な認証用の SiteMinder と統合する場合、CA Identity Manager は環境、および環境に対して作成されるデフォルト認証方式を保護する SiteMinder ポリシー ドメインを削除します。

次の手順に従ってください:

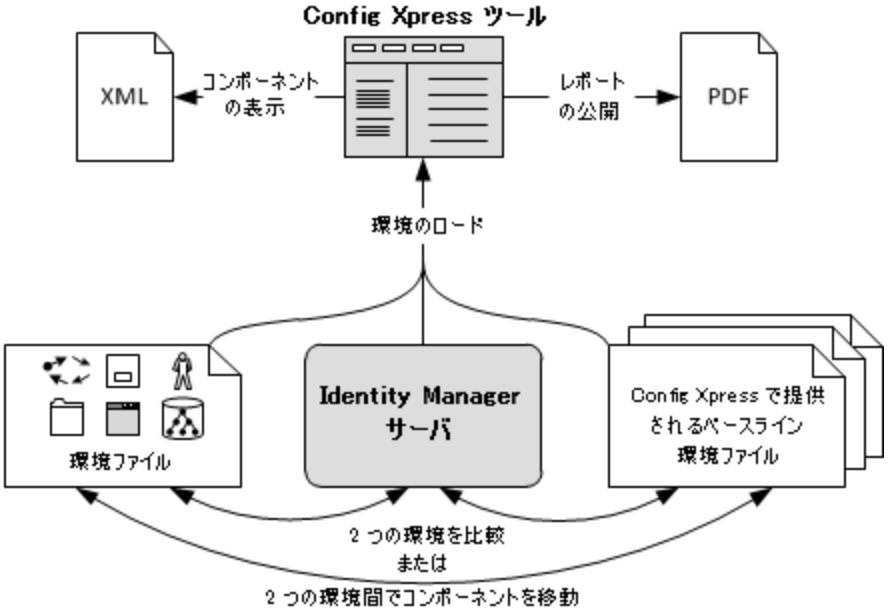
1. ［環境］画面で、CA Identity Manager 環境が削除するチェック ボックスをオンにします。
2. ［削除］をクリックします。

   CA Identity Manager に確認メッセージが表示されます。
3. ［OK］をクリックし、削除を確定します。

設定の管理

Config Xpress は CA Identity Manager に含まれているツールです。 このツールを使用して、ユーザの CA Identity Manager 環境の設定を分析し、処理することができます。

最も重要なのは、このツールにより、環境間のコンポーネントの移動ができるということです。 Config Xpress は、他の必要なコンポーネントを自動的に検出し、それらも移動するように要求します。 この支援により、ユーザの作業を省き、問題のリスクを減らすことができます。



次の手順に従ってください:

1. Config Xpress をセットアップします (P. 225)。
2. ツールを使用する前に、分析用の Config Xpress に CA Identity Manager 環境をロードします (P. 226)。
3. Config Xpress を使用して、ロードした環境で以下のタスクを実行します。
   - 環境間でコンポーネントを移動します (P. 228)。
   - システム コンポーネントの PDF レポートを発行します (P. 229)。
   - 特定のコンポーネントの XML 設定を表示します (P. 230)。

Config Xpress のセットアップ

Config Xpress 用のインストール ファイルはインストール ドライブに含まれています。しかし、ツールはインストールされません。

Config Xpress には以下のソフトウェア要件があります。

- CA Identity Manager r12.0 以降
- Windows オペレーティング システム
- Adobe Air ランタイム
- レポートを表示するための PDF リーダ

次の手順に従ってください:

1. http://get.adobe.com/air から Adobe Air ランタイムをダウンロードし、次に、それをインストールします。
2. 管理ツールがインストールされていることを確認します。
3. Config Xpress のインストール ファイル用の以下の場所の中を検索します。

   ```
   C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥ConfigXpress
   ```

4. Config Xpress.air を実行して、Config Xpress をインストールします。
5. インストールが完了したら、Config Xpress が起動します。

Config Xpress への環境のロード

Config Xpress を使用する前に、ツールに 1 つ以上の環境をロードします。 このタスクは、Config Xpress の環境で動作できます。

実際の CA Identity Manager サーバから Config Xpress に環境を直接ロードするか、または環境ファイルからロードできます。 Config Xpress でインストールされるベースライン環境ファイルのいずれかを使用する場合は、環境を既定の設定と比較できます。

環境をロードする処理には数分かかる場合があります。

次の手順に従ってください:

1. Config Xpress を開きます。
2. CA Identity Manager サーバから**ライブ環境**を直接ロードするには、以下の手順に従います。
   a. ［サーバ］（［ネットワーク］）タブをクリックします。
   b. CA Identity Manager サーバの名前およびポートを入力します。 例：

      `servername.ca.com:8080`

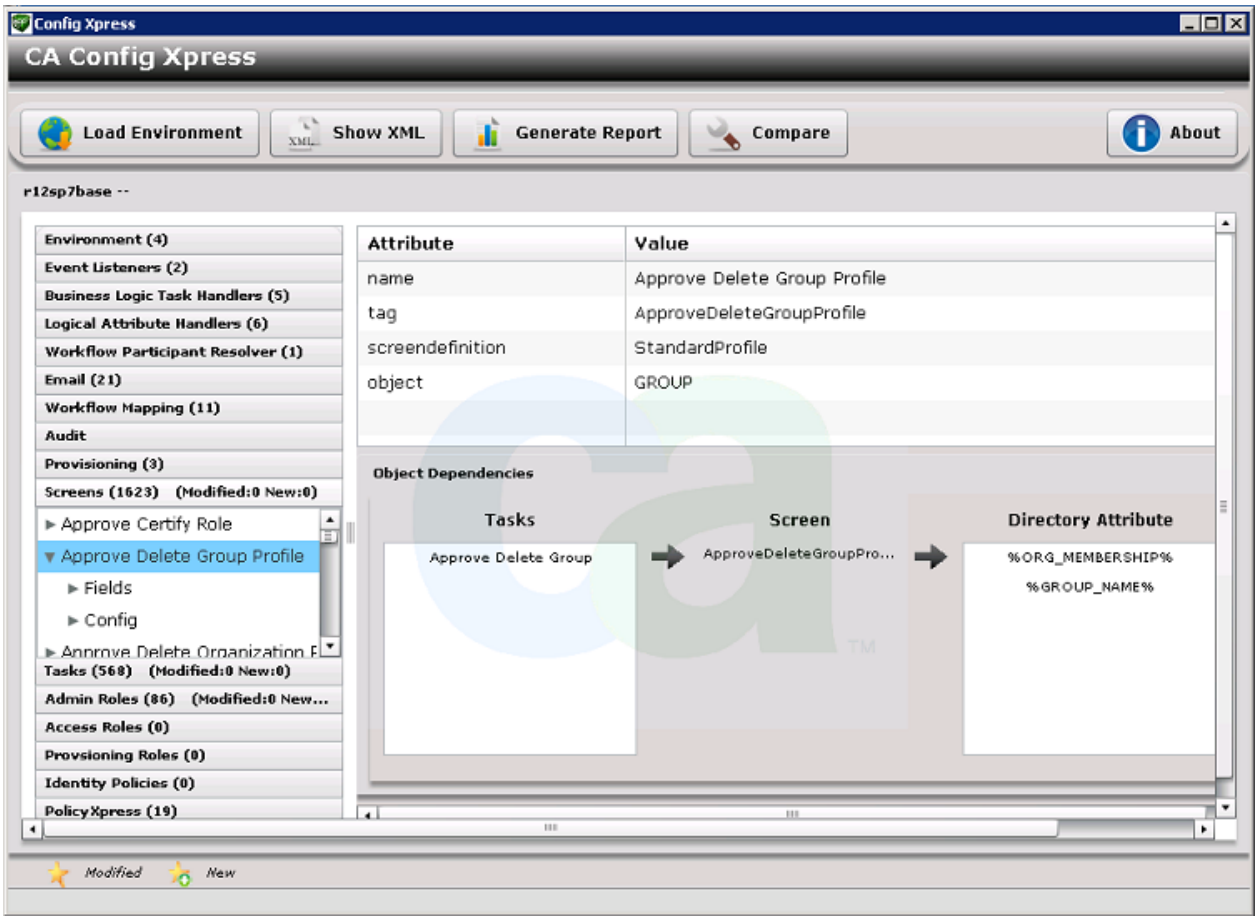
   c. サーバが HTTPS のみを許可するようにセットアップする場合は、［HTTPS を使用］を選択します。
   d. サーバのバージョンが r12.5 SP6 より新しい場合は、［12.5 SP7］を選択します。
   e. ［接続］をクリックします。
   f. ［*ロードする環境の選択*］リストから環境を選択し、［ロード］をクリックします。
3. ユーザの CA Identity Manager 環境からエクスポートされた**環境ファイル**をロードするには、以下の手順に従います。
   a. CA Identity Manager 環境をエクスポートします。
   b. Config Xpress で、［ファイル システム］タブをクリックします。
   c. バージョンを選択してから、環境ファイルを参照し、次に、［ロード］をクリックします。
4. Config Xpress でインストールされた**ベースライン環境ファイル**をロードするには、以下の手順に従います。
   a. ［ベース バージョン］タブをクリックします。
   b. 必要なバージョンを選択し、［選択］をクリックします。

Config Xpress は、環境を分析し、環境の詳細を表示します。

これで、PDF (P. 229) または XML (P. 230) として環境の一部またはすべてを公開できます。 2 番目の環境をロードする場合、これらの環境を比較し、環境間でコンポーネントを移動 (P. 228)させることができます。

例: ベースライン設定ファイルをロードした後の Config Xpress

このスクリーンショットは、Config Xpress が従属オブジェクトを表示する方法を示しています。



ある環境から別の環境へのコンポーネントの移動

Config Xpress がインストールされていない場合は、ステージング エリア間でコンポーネントを移動させるタスクは複雑で、失敗する可能性があります。

Config Xpress を使用してコンポーネントを移動させる場合は、ツールによって必要なオブジェクトもすべて移動させます。 たとえば、画面を必要とするタスクを移動させる場合、Config Xpress により、必要なコンポーネントも選択するかどうか確認するメッセージが表示されます。 Config Xpress は、タスクがこの画面を使用し、ターゲット環境に移動される必要があることも認識しています。

ライブ環境にコンポーネントを移動させる場合、Config Xpress では、それをすぐにアップロードします。 環境ファイルにコンポーネントを移動させる場合は、XML ファイルとしてコンポーネントを保存し、次に、環境にそのファイルをインポートします。

次の手順に従ってください:

1. 移動させるコンポーネントが含まれる環境をロードします。
2. この環境を別の環境と比較するには：
   a. ［比較］をクリックします。
   b. ターゲット環境をロードします。

   Config Xpress により、2 つの環境間の違いを示すリストが表示されます。
3. 違いのリストで、移動させるコンポーネントを検索します。 リストを並べ替えるには、［名前］列をクリックします。
4. コンポーネントごとに、以下の手順に従います。
   a. ［アクション］列のアイテムを選択します。

   Config Xpress によりコンポーネントが分析されます。この処理には時間かかる場合があります。

   b. コンポーネントに依存コンポーネントがある場合は、［変更された依存コンポーネントの追加］画面が表示されます。 ［はい］または［いいえ］をクリックして続行します。

   移動させるコンポーネントをすべて選択したら、更新されたコンポーネントを移動させる準備が整います。
5. ライブ サーバにコンポーネントを移動させる場合は、［アップロード先］をクリックします。

   コンポーネントはすぐに移動されます。
6. 環境ファイルにコンポーネントを移動させる場合：
   a. ［保存］をクリックします。

b. ファイル名を入力し、もう一度［保存］をクリックします。

Config Xpress により、XML ファイルで選択したコンポーネントがすべて保存されます。 これで、実際のターゲット環境へこの XML ファイルをインポートできるようになります。

PDF レポートの公開

Config Xpress では、CA Identity Manager 環境の現在の状態を文書化するレポートを生成できます。 このレポートを使用して、実稼働環境のスナップショットを作成できます。レポートを生成するときに、完全な設定を含めるか、またはインストール後の変更のみを含めるかを選択します。

このレポートは、後で参照する場合に、またはシステムのリカバリ計画の一環として役立ちます。

次の手順に従ってください:

1. Config Xpress に環境をロードします。
2. ［レポートの生成］をクリックします。

   ［PDF レポートの生成］ダイアログ ボックスで、フォント サイズを変更したり、タイトルまたはカバー ページのテキストを入力したりすることもできます。 また、構成アイテムをすべて含めるか、新しいアイテムまたは変更されたアイテムのみを含めるかどうかも選択できます。

   重要: ［*新規または変更されたタスク、画面、ロールの詳細のみを含める*］ボックスをオンにしない場合、レポートには環境全体が含まれます。PDF ファイルは、約 2000 ページで、40 MB を超えます。
3. ［OK］をクリックします。
4. ファイル名を入力し、レポートを保存します。 保存は数分かかる場合があります。または環境全体を公開することを選択する場合は、それよりも時間がかかる可能性があります。

   レポートは PDF リーダで開きます。

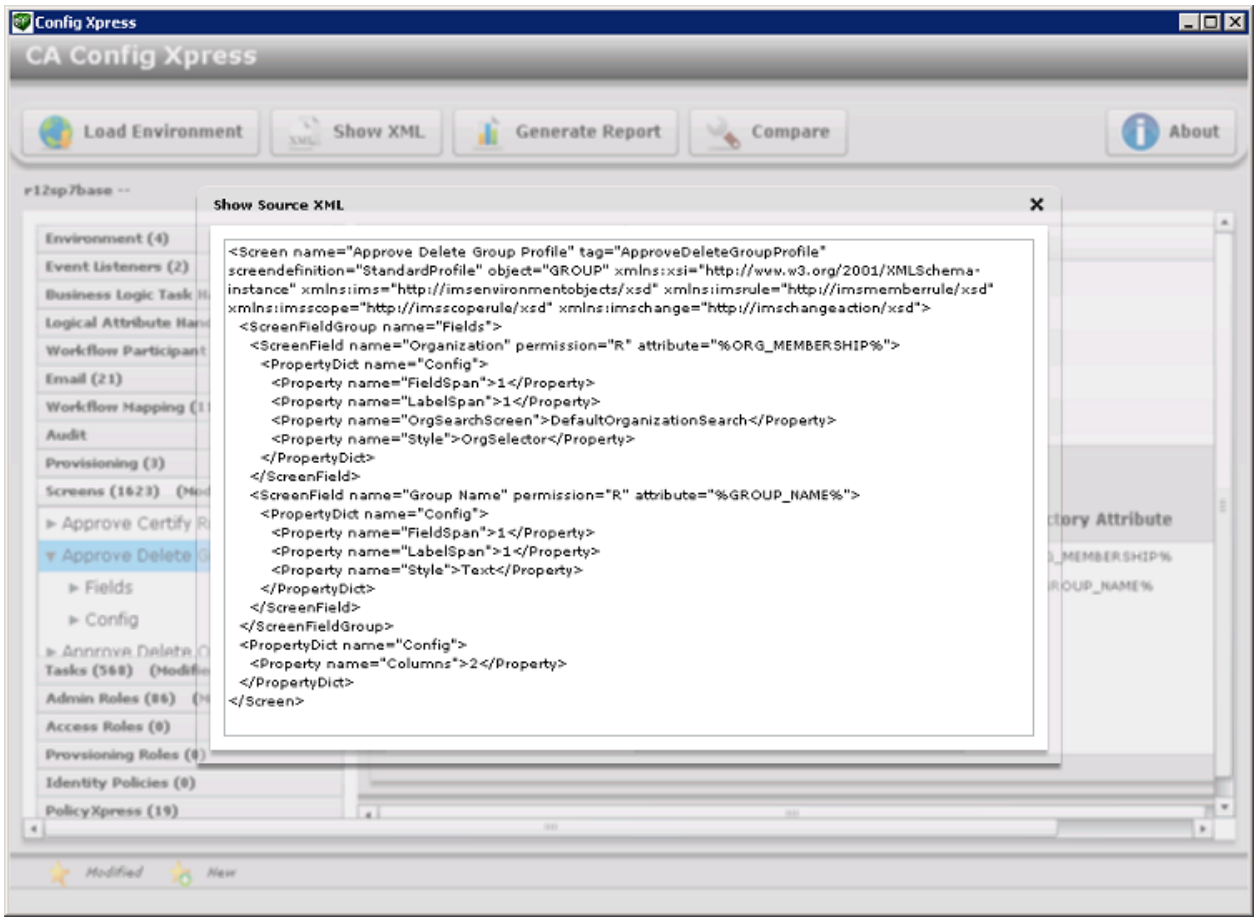
XML 設定の表示

Config Xpress では、特定のコンポーネント用の XML 設定を表示できます。 この XML ファイルを学習すると、システムを理解するのに役立ちます。

次の手順に従ってください:

1. Config Xpress に環境をロードします。
2. ［Config Xpress］画面でコンポーネントをクリックします。
3. ［Show XML］をクリックします。

   ［XML 設定］が表示されます。



ポリシー ルール評価の最適化

ユーザ セットを動的に識別するポリシー ルールは、ロール メンバ、管理者、所有者ポリシー、およびアイデンティティ ポリシーの評価で使用されます。これらのルールの評価は大規模な CA Identity Manager の実装において、かなり時間がかかる場合があります。

注: メンバ、管理者、所有者、およびアイデンティティ ポリシーに関する詳細については、「管理ガイド」を参照してください。

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。 メモリ内評価オプションが有効な場合、CA Identity Manager はユーザ ストアから評価されるユーザに関する情報を取得し、メモリにそのユーザを表示したものを格納します。 CA Identity Manager では、このメモリ内表示を使用して、ポリシー ルールに対する属性値を比較します。 これにより、CA Identity Manager がユーザ ストアに直接行うコール数が制限されます。

管理コンソールで、環境用のメモリ内評価オプションを有効にします。

次の手順に従ってください:

1. 管理コンソールを開きます。
2. ［環境］-［*環境名*］-［詳細設定］-［その他］を選択します。

   ［ユーザ定義プロパティ］ページが開きます。
3. ［プロパティ］フィールドに以下のテキストを入力します。

   UseInMemoryEvaluation
4. ［値］フィールドに以下の*いずれか*の数を入力します。

   0

   メモリ内評価は無効です。

   1

   メモリ内評価は有効です。 このオプションが指定される場合、属性比較は大文字と小文字を区別します。

   3

   メモリ内評価は有効です。 このオプションが指定される場合、属性比較は大文字と小文字を区別しません。
5. ［追加］をクリックします。

   CA Identity Manager は、環境の既存のプロパティのリストに新規プロパティを追加します。
6. ［保存］をクリックします。

ロールおよびタスクの設定

管理コンソールの［ロールおよびタスクの設定］画面から、ロール定義ファイルと呼ばれる XML ファイルで画面、タブ、ロールおよびタスクの設定をインポートまたはエクスポートできます。 CA Identity Manager では、特定の機能セット用の画面、タブ、ロール、およびタスクを作成する事前定義済みロール定義ファイルを提供します。たとえば、スマート プロビジョニングをサポートするロール定義ファイルや、エンドポイント管理画面をサポートする他のロール定義ファイルがあります。

また、ロール定義ファイルを使用して、1 つの環境から複数の環境に設定を適用することもできます。 以下のタスクを実行します。

- 1 つの環境で画面、タブ、タスクおよびロール設定を設定します。
- これらの設定を XML ファイルにエクスポートします。
- 必要な環境に XML ファイルをインポートします。

ロールおよびタスクの設定のエクスポート

ロールおよびタスクの設定をエクスポートするには、以下の手順に従います。

次の手順に従ってください:

1. 管理コンソールで、［環境］をクリックします。

   CA Identity Manager 環境のリストが表示されます。

2. 適切な CA 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］-［エクスポート］をクリックします。
4. ブラウザ ウィンドウでファイルを表示するには［開く］をクリックし、XML ファイルに設定を保存するには［保存］をクリックします。

ロールおよびタスクの設定のインポート

ロールおよびタスクの設定は、ロール定義ファイルと呼ばれる XML ファイルで定義されます。 CA Identity Manager の特定の機能セット（スマート プロビジョニングなど）をサポートするように、事前定義済みロール定義ファイルをインポートできます。または、ある環境から別の環境にロール定義ファイルをインポートすることもできます。

注: Connector Xpress で作成されるカスタム コネクタ用のロール定義をインポートすることもできます。 これらのロール定義ファイルは、ロール定義生成プログラムで作成します。 詳細については、「*Connector Xpress Guide*」を参照してください。

ロールおよびタスクの設定をインポートするには、以下の手順に従います。

次の手順に従ってください:

1. 管理コンソールで、［環境］をクリックします。

   CA 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 CA 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. 以下のいずれかのアクションを実行します。

   - 環境用にデフォルトのロールおよびタスクを作成するには、1 つ以上のロール定義ファイルを選択します。

     利用可能なロール定義ファイルをすべて選択するには、［すべて選択/選択解除］をクリックします。

   - ファイルをインポートするか参照するには、ロール定義ファイルのパスおよびファイル名を入力します。 次に［完了］をクリックします。

5. ［完了］をクリックします。

   ［ロール設定出力］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。

動的エンドポイント用のロールおよびタスクを作成する方法

Connector Xpress を使用すると、SQL データベースおよび LDAP ディレクトリのプロビジョニングおよび管理を行えるように動的コネクタを設定できます。各動的コネクタごとに、ロール定義生成プログラムを使用して、ユーザ コンソールに表示されるアカウント管理画面用のタスクおよび画面の定義を作成できます。

ロール定義生成プログラムを実行した後で、結果として生成されたロール定義ファイルを管理コンソールにインポートします (P. 233)。

注: ロール定義生成プログラムの詳細については、「*Connector Xpress Guide*」を参照してください。

システム マネージャ アカウントの変更

システム マネージャは CA Identity Manager 環境セットアップおよび保守を担当します。 通常、システム マネージャのタスクには次のものが含まれます。

- 初期環境の作成および管理
- 管理ロールの作成および変更
- 他の管理者アカウントの作成および変更

CA Identity Manager 環境を作成するときに、システム マネージャ アカウントを作成します。システム マネージャがパスワードを忘れた場合などにこのアカウントが「ロックアウト」された場合は、システム マネージャ ウィザードを使用してアカウントを再作成できます。

システム 、マネージャ ウィザードの手順に従ってユーザにシステム管理ロールを割り当てます。

システム マネージャ アカウントを変更する前に、以下の点に注意してください。

- LDAP ユーザ ストアを使用しており、CA Identity Manager ディレクトリ用のディレクトリ設定ファイル（directory.xml）で ou=People などのユーザ コンテナを設定していることを確認します。 選択したユーザは、システム マネージャを設定するコンテナと同じコンテナに存在する必要があります。 ユーザ コンテナに存在しないユーザ アカウントを選択すると障害が発生する場合があります。
- CA Identity Manager 環境がフラットなユーザ構造を持つユーザ ディレクトリを管理する場合は、選択したユーザのプロファイルには組織も含まれている必要があります。 ユーザのプロファイルが正しく設定されていることを確認するには、directory.xml ファイル (P. 90) の汎用属性 %ORG_MEMBERSHIP% に対応する物理属性にユーザの組織の名前を追加します。 たとえば、物理属性の説明が directory.xml ファイルの汎用属性 %ORG_MEMBERSHIP% にマップされ、ユーザが「従業員」組織に属する場合、ユーザのプロファイルには「属性/値ペアの説明 = 従業員」が含まれる必要があります。

次の手順に従ってください:

1. CA Identity Manager 環境画面で、適切な CA Identity Manager 環境の名前をクリックします。

   特定の環境画面のプロパティが表示されます。

2. ［システム マネージャ］をクリックします。

   システム マネージャ ウィザードが表示されます。

3. システム マネージャ ロールを持つユーザの一意の名前を以下のように入力します。

   - リレーショナル データベース ユーザの場合、ユーザの一意の識別子、またはディレクトリ設定ファイル内の汎用属性 %USER_ID にマップされる値を入力します。
   - LDAP ユーザの場合、ユーザの相対 DN を入力します。 たとえば、ユーザの DN が uid=Admin1、ou=People、ou= Employees、ou=NeteAuto の場合は、「Admin1」を入力します。

   注: システム マネージャはユーザ ストアの管理者と同じユーザ でないことを確認します。

4. ユーザの完全な識別子を表示するには、［検証］をクリックします。

5. ［次へ］をクリックします。

6. ウィザードの 2 番目のページで、以下のようにユーザに割り当てるロールを選択します。
   - システム マネージャ ロールを割り当てる場合は、以下のタスクを実行します。
     a. システム マネージャ ロールの横にあるラジオ ボタンを選択します。
     b. ［完了］をクリックします。
   - システム マネージャ ロール以外のロールを割り当てる場合は、以下のタスクを実行します。
     a. 最初のリストで条件を選択します。
     b. 2 番目のリスト ボックスで部分的または完全なロール名またはアスタリスク（*）を入力します。［検索］をクリックします。
     c. 検索結果リストから割り当てるロールを選択します。
     d. ［完了］をクリックします。

   ［システム マネージャ設定出力］画面にはステータス情報が表示されます。
7. システム マネージャ ウィザードを閉じるには、［続行］をクリックします。

CA Identity Manager 環境のステータスへのアクセス

CA Identity Manager には、以下のステータスを確認するために使用可能なステータス ページが含まれています。

- CA Identity Manager ディレクトリは正しくロードされます。
- CA Identity Manager はユーザ ストアに接続できます。
- CA Identity Manager 環境は正しくロードされます。

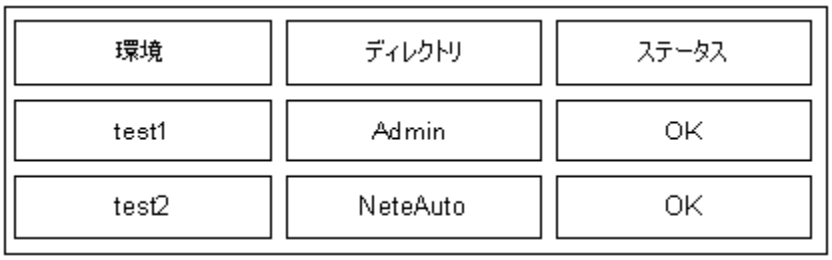
ステータス ページにアクセスするには、ブラウザで以下の URL を入力します。

`http://hostname/iam/im/status.jsp`

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決定します。たとえば、myserver.mycompany.com。

CA Identity Manager 環境が正しく開始され、接続がすべて正常に実行されている場合、ステータス ページは以下の図のようになります。



また、ステータス ページには、環境が FIPS 140-2 準拠であるかどうかも示されます。

CA Identity Manager 環境のトラブルシューティング

以下の表は、予想されるエラー メッセージおよびトラブルシューティング プロセスについて説明します。

メッセージ	説明	トラブルシューティング
ロードされていない	CA Identity Manager が開始されるときに、環境と関連付けられる CA Identity Manager ディレクトリがロードされませんでした。	1. ユーザ ストアが実行されていることを確認します。 CA Identity Manager が SiteMinder と統合される場合は、SiteMinder がユーザ ストアに接続できることを確認します。
OK でない	CA Identity Manager は CA Identity Manager ディレクトリに接続できません。	ポリシー サーバ ユーザ インターフェースで、ユーザ ストアと関連付けられる SiteMinder ユーザ ディレクトリ接続用のプロパティ ページを開き、［コンテンツの表示］ボタンをクリックすることにより、接続を確認できます。 ユーザ ストアのコンテンツを表示できる場合、SiteMinder は正常に接続できます。 ポリシー サーバの詳細については、「*CA SiteMinder Web Access Manager Policy Server Configuration Guide*」を参照してください。 2. CA Identity Manager とポリシー サーバを再起動します。

メッセージ	説明	トラブルシューティング
SM 接続は OK でない	CA Identity Manager は SiteMinder ポリシー サーバに接続できません(SiteMinder が含まれる実装の場合)	1. 以下の状態を確認します。 ■ ポリシー サーバが実行されている。 ■ Web エージェントはリソースを保護している。 ポリシー サーバ ユーザ インターフェースにアクセスすることにより、Web エージェントが正しく実行されているかどうかを確認できます。 ユーザがクレデンシャルを要求される場合、Web エージェントは正しく機能しています。 2. CA Identity Manager とポリシー サーバを再起動します。
IMS は現在利用できない	CA Identity Manager でエラーが発生しました。	アプリケーション サーバ ログでエラーの詳細を確認します。
Windows 500 エラー メッセージ	LDAP ユーザ ディレクトリとの接続を解除する間にアクセスされる場合、ステータス ページは表示されません。	ステータス ページを表示するには、インターネット ブラウザ オプションの［エラー メッセージを簡易表示する］をオフに設定します。

第 7 章: 詳細設定

管理コンソールの［詳細設定］ウィンドウで以下の設定を実行できます。

- 詳細設定を設定するための画面へのアクセス
- 「カスタム設定のインポート/エクスポート (P. 254)」の説明に従って詳細設定をインポートおよびエクスポートします。

このセクションには、以下のトピックが含まれています。

監査 (P. 239)
ビジネス ロジック タスク ハンドラ (P. 240)
イベント リスト (P. 241)
電子メール通知 (P. 242)
イベント リスナ (P. 242)
アイデンティティ ポリシー (P. 243)
ロジカル アトリビュート ハンドラ (P. 243)
その他 (P. 244)
通知ルール (P. 245)
組織セレクタ (P. 245)
プロビジョニング (P. 246)
ユーザ コンソール (P. 249)
Web サービス (P. 252)
ワークフロー プロパティ (P. 253)
作業アイテムの委任 (P. 253)
ワークフロー参加者リゾルバ (P. 254)
カスタム設定のインポート/エクスポート (P. 254)
Java 仮想マシン メモリ不足エラー (P. 255)

監査

監査ログは、CA Identity Manager 環境で実行された操作の記録を保持します。 システム アクティビティを監視するために監査ログのデータを使用できます。

CA Identity Manager は*イベント*を監査します。 イベントは CA Identity Manager タスクによって生成される操作です。 1 つのタスクで複数のイベントを生成できます。たとえば、CreateUser タスクは CreateUserEvent および AddToGroupEvent のイベントを生成することができます。

デフォルトでは、CA Identity Manager は監査データベースにすべてのイベント情報をエクスポートします。 CA Identity Manager が記録するイベント情報のタイプおよび量を制御するには、以下のタスクを実行できます。

- CA Identity Manager 管理タスクの監査を有効にします。
- 管理タスクによって生成された CA Identity Manager のイベントの一部またはすべての監査を有効にします。
- イベント完了時やイベントがキャンセルされたときなど、特定の状態のイベント情報を記録します。
- イベントに含まれる属性に関する情報をログに記録します。 たとえば、ModifyUserEvent の実行中に変更される属性をログに記録できます。
- イベントと属性の監査レベルを設定します。

ビジネス ロジック タスク ハンドラ

CA Identity Manager タスクが処理のためにサブミットされる前に、ビジネス ロジック タスク ハンドラはカスタム ビジネス ロジックを実行します。 通常、カスタム ビジネス ロジックはデータを検証します。 たとえば、CA Identity Manager がグループにメンバを追加する前に、ビジネス ロジック タスク ハンドラは、グループ ンバシップの制限を確認できます。 グループ メンバシップの制限に達すると、ビジネス ロジック タスク ハンドラは新メンバが追加できなかったことをグループ管理者に伝えるメッセージを表示します。

事前定義済みビジネス ロジック タスク ハンドラを使用するか、または Business Logic Task Handler API を使用してカスタム ハンドラを作成できます。

注: カスタム ビジネス ロジックの作成の詳細については、「Java のプログラミング ガイド」を参照してください。

［ビジネス ロジック タスク ハンドラ］画面には、既存のグローバル ビジネス ロジック タスク ハンドラのリストが含まれます。 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。 CA Identity Manager は、このリストで表示される順にハンドラを実行します。

グローバル ビジネス ロジック タスク ハンドラは Java でのみ実装できます。

[ユーザ パスワードのリセット]タスクの[パスワード]フィールドの自動クリア

以前に入力した値がパスワード ポリシーに違反している場合や、［パスワード］と[パスワードの確認]フィールドの値が一致しない場合に CA Identity Manager が［パスワード］フィールドを自動的にクリアするように設定できます。

次の手順に従ってください:

1. 管理コンソールの起動
2. 管理する環境を選択し、［詳細設定］をクリックします。

   ［Advanced Settings （詳細設定）］ページが表示されます。
3. ビジネス ロジック タスク ハンドラ、BlthPasswordServices.をクリックします。

   ［ビジネス ロジック タスク ハンドラ プロパティ］ページが表示されます。
4. 以下のプロパティを作成します。

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|
5. ConfirmPasswordHandler 設定が以下のようであることを確認します。
   - Object type – User
   - Class – ConfirmPasswordHandler
   - ConfirmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   ユーザは、これで［ユーザ パスワードのリセット］タスクの［パスワード］フィールドをクリアできるようになります。

イベント リスト

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。

CA 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。

このページを使用して、CA Identity Manager で利用可能なイベントのリストを表示します。

電子メール通知

タスクまたはイベントが完了するとき、またはワークフロー管理下のイベントが特定の状態に到達するときに、CA Identity Manager は電子メール通知を送信できます。 たとえば、電子メールは、イベントが承認を必要とすることを承認者に伝えることができます。

電子メール通知のコンテンツを指定するには、事前定義済み電子メール テンプレートを使用するか、またはユーザのニーズに適するようにテンプレートをカスタマイズできます。

管理コンソールを使用すると、以下のタスクを実行できます。

- CA Identity Manager 環境の電子メール通知を有効にします。
- 電子メール メッセージを作成するためのテンプレート セットを指定します。
- 電子メール通知が送信されるイベントおよびタスクを示します。

イベント リスナ

CA Identity Manager タスクは、CA Identity Manager がタスクの実行中に実行するイベントという名前の、1 つ以上のアクションで構成されます。 たとえば、「ユーザの作成」タスクには以下のイベントが含まれる場合があります。

- CreateUserEvent -- 組織内のユーザ プロファイルを作成します
- AddToGroupEvent --（オプション）グループのメンバとしてユーザを追加します
- AssignAccessRole --（オプション）ユーザにアクセス ロールを割り当てます

*イベント リスナ*は特定のイベントを「リスン」し、イベントのライフサイクルの特定の時点でカスタム ビジネス ロジックを実行します。 たとえば、新規ユーザが CA Identity Manager で作成された後で、イベント リスナは別のアプリケーションのデータベースにユーザの情報を追加できます。

注: イベント リスナの設定の詳細については、「Java のプログラミング ガイド」を参照してください。

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、特定のルールまたは条件に適合するユーザにビジネス変更のセットを適用します。アイデンティティ ポリシーを使用して、以下のタスクを実行できます。

- 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、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するアイデンティティ ポリシーを作成できます。
- 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。

ユーザ コンソールでアイデンティティ ポリシー セットを作成し管理します。 アイデンティティ ポリシーの詳細については、「管理ガイド」を参照してください。

アイデンティティ ポリシーを使用する前に、管理コンソールを使用して以下のタスクを実行します。

- CA Identity Manager 環境用のアイデンティティ ポリシーを有効にします。
- 再帰レベルを設定します（オプション）。

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 ストアの属性（*フィジカル アトリビュート*と呼びます）をタスク画面上に分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 アトリビュートによって処理されます。ロジカル アトリビュートは、ロジカル アトリビュート API を使用して作成された Java オブジェクトです。 たとえば、タスク画面が表示されるときに、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。

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: 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。

その他

この画面上で定義されるユーザ定義のプロパティは CA Identity Manager 環境全体に適用されます。 それらは、CA Identity Manager API で作成するすべてのカスタム Java オブジェクトの init （） メソッドに名前/値のペアとして渡されます。 カスタム オブジェクトは、オブジェクトのビジネス ロジックが要求する任意の方法で、このデータを使用できます。

ユーザ定義のプロパティも特定のカスタム オブジェクトに対して定義されます。 たとえば、MyListener という名前のイベント リスナのための［プロパティ］画面でユーザ定義のプロパティが定義されていると仮定します。 ［その他］画面で定義されたオブジェクトに固有のユーザ定義のプロパティおよび環境全体にわたるプロパティは、MyListener.init （） に単一のコールで渡されます。

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

1 つ以上のユーザ定義のプロパティを削除するには、削除する各名前/値のペアの隣のチェック ボックスをオンにし、［削除］をクリックします。

変更が行われれば、［保存］をクリックします。 変更を有効にするために、アプリケーション サーバを再起動します。

注: ［その他］のプロパティはすべて大文字と小文字を区別します。 そのため、ユーザが SelfRegistrationLogoutUrl という名前のプロパティおよび selfregistrationlogouturl という名前の別のプロパティを定義する場合、両方のプロパティが追加されます。

通知ルール

通知ルールはユーザが電子メール通知を受信することを決定します。タスクが完了するか、タスクのイベントが、承認待ち、承認済み、または拒否済みなどの特定の状態に達する場合、ユーザは通知ルールに従って電子メール通知を受信します。

注: 電子メール通知機能の詳細については、「管理ガイド」を参照してください。

CA Identity Manager には以下の事前定義済み通知ルールが含まれています。

ADMIN_ADAPTER

タスクを開始する管理者に電子メール メッセージを送信します

USER_ADAPTER

タスクによって影響を受けたユーザに電子メール メッセージを送信します

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

カスタム通知ルールを作成するには、Notification Rule API を使用します。

注: 通知ルールの詳細については、「Java のプログラミング ガイド」を参照してください。

組織セレクタ

組織セレクタは、CA Identity Manager が自己登録ユーザのプロファイルを作成する場所を決定するカスタム ロジカル アトリビュート ハンドラです。このハンドラは、登録中にユーザが提供する情報に基づきます。たとえば、登録するときに、宣伝用のコードを提供するユーザのプロファイルは、Promotional Users 組織に追加することができます。

プロビジョニング

プロビジョニングを含む CA Identity Manager を使用する場合に、この画面を使用します。

注:「CA Identity Manager 環境のプロビジョニングをセットアップ (P. 204)」では、段階的な詳細な手順が記載されています。

［Provisioning Properties］オプションを以下に示します。

Enabled

2 つのユーザ ストア、CA Identity Manager 用に 1 つ、およびプロビジョニング アカウント用に別のユーザ ストア（プロビジョニング ディレクトリと呼ばれます）の使用を指定します。 このオプションが無効な場合、CA Identity Manager ユーザ ストアのみが使用されます。

Use Session Pool

セッション プールの使用を有効にします。

Session Pool Initial Sessions

起動時に利用可能なセッションの最小数を定義します。

デフォルト： 8

Session Pool Maximum Sessions

プールでセッションの最大数を定義します。

デフォルト： 32

Enable Password Changes from Endpoint Accounts

プロビジョニング サーバで各ユーザの［Enable Password Synchronization Agent］の設定を定義します。 このオプションは、CA Identity Manager ユーザと関連するエンドポイント アカウント間のパスワード同期を有効にできます。

Enable Accumulation of Provisioning Role Membership Events

有効な場合、このチェック ボックスは CA Identity Manager が特定の順序でプロビジョニング ロール メンバシップに関連するイベントを実行することを確認します。 すべての［Add］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。［Add］アクションの処理が完了すると、CA Identity Manager により、［Remove］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。 AccumulatedProvisioningRoleEvent と呼ばれる単一のイベントがこの順にイベントを実行するために生成されます。

注: AccumulatedProvisioningRoleEvent の詳細については、「管理ガイド」を参照してください。

Organization for Creating Inbound Users

CA Identity Manager が使用するユーザ ストアへの完全修飾パスを定義します。ユーザ ストアに組織が含まれる場合にのみ、このフィールドが表示されます。

Inbound Administrator

着信マッピングにマップされるタスクを実行できる CA Identity Manager 管理者アカウントを定義します。 これらのタスクは、プロビジョニング同期マネージャ ロールに含まれています。管理者は、任意の CA Identity Manager ユーザ上で各タスクを実行できる必要があります。

Provisioning Directory

プロビジョニング ディレクトリは、ドメイン、グローバル ユーザ、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 テンプレートを含むプロビジョニング情報のリポジトリです。 ユーザが選択する場合、他のオプションが、プロビジョニング ディレクトリに CA Identity Manager ユーザ ストアをマップするために表示されます。

Enable Session Pooling

パフォーマンスを改善するために、CA Identity Manager は、プロビジョニング サーバと通信する際に、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。

［Session Pools］オプションが無効な場合、CA Identity Manager は必要に応じてセッションを破棄します。

新しい環境の場合、［Session Pools］はデフォルトで有効になっています。 既存の環境の場合、［Session Pools］を有効にできます。

次の手順に従ってください:

1. 管理コンソールで、［Advanced Settings］-［Provisioning］を選択します。
2. ［Use Session Pool］を選択します。
3. 起動時にプールで利用可能なセッションの最小数を定義します。
4. プールで利用可能なセッションの最大数を定義します。
5. ［Save］をクリックします。
6. アプリケーション サーバを再起動します。

   ［Session Pool］は定義された設定ごとに有効になります。

パスワード同期の有効化

プロビジョニング サーバでは、CA Identity Manager ユーザと、関連するエンドポイント ユーザ アカウント間でパスワードを同期できます。 つまり、プロビジョニング ロールを持つユーザが CA Identity Manager で作成されるか変更される場合に、プロビジョニング ユーザはエンドポイント アカウントからのパスワード変更を許可するように設定されます。

注: 管理コンソールでこの機能を有効にする場合は、環境内の すべてのユーザがエンドポイント アカウントからのパスワード変更を許可するように設定されます。

次の手順に従ってください:

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。

属性マッピング

属性マッピングは Provision Create User などのプロビジョニング関連の管理タスクのユーザ属性をプロビジョニング サーバの対応する属性と関連付けます。単一のプロビジョニング属性は、CA Identity Manager ユーザ ストアの複数の属性にマップできます。

デフォルト マッピングは、「インバウンド マッピング」セクションでリスト表示されている、デフォルト タスクの属性に対して存在します。別の属性を使用するために、これらの管理タスクのいずれかを変更する場合は、必要に応じて属性マッピングを更新します。

Inbound Mappings

着信マッピングはプロビジョニング サーバによって生成されるイベントを管理タスクにマップします。 これらのマッピングはあらかじめ設定され、変更できません。

Outbound Mappings

送信マッピングは、管理タスクによって生成されるイベントをプロビジョニング ディレクトリに適用されるイベントと関連付けます。 デフォルト マッピングは、ユーザ属性に影響を与えるイベントに対して存在します。

ユーザ コンソール

管理タスクをユーザが実行できる Web アプリケーションである、ユーザ コンソールを使用して CA Identity Manager 環境にアクセスします。 管理コンソールの［ユーザ コンソール］ページで、管理者が環境にアクセスするために使用するユーザ コンソールの特定のプロパティを定義します。

［ユーザ コンソール］ページには、以下のフィールドが含まれます。

General Properties

環境に適用されるプロパティを定義します。

Show Recently Completed Tasks

タスクが完了するときに CA Identity Manager がステータス メッセージを表示するかどうかを決定します。

このオプションが選択されている場合、ユーザは CA Identity Manager が表示するステータス メッセージをクリアするために［OK］をクリックする必要があります。

メッセージを無効にし、ステータス メッセージが表示されるたびにユーザが［OK］をクリックする必要がないようにするには、このオプションをクリアします。

Show About Link

ユーザ コンソールの右下隅に［バージョン情報］リンクが表示されるかどうかを決定します。 このオプションが選択されている場合、CA Identity Manager ユーザは CA Identity Manager コンポーネントのバージョン情報への［バージョン情報］リンクをクリックできます。

Enable Language Switching

ログイン画面およびユーザ コンソールで CA Identity Manager に［言語の選択］ドロップダウン リストが含まれるかどうか決定します。 このフィールドが選択されている場合、CA Identity Manager ユーザはリストから新しい言語を選択することによりユーザ コンソールで言語を変更できます。

注:［言語の選択］フィールドを表示するには、［言語切り替えの有効化］フィールドを選択し、複数の言語をサポートするように CA Identity Manager を設定していることを確認してください。

詳細については「*ユーザ コンソール デザイン ガイド*」を参照してください。

Job Timeout

タスクがサブミットされてからステータス メッセージが表示されるまでに CA Identity Manager が待機する時間を決定します。

タスクが指定された時間内で完了する場合、CA Identity Manager は以下のメッセージを表示します。

「タスク完了」

タスクが完了するのに時間がかかるか、ワークフロー管理の下にある場合、CA Identity Manager は以下のメッセージを表示します。

「*現在の日付*の処理に関して、タスクがサブミットされました」

注: 変更はすぐに有効にならない場合があります。

Theme Properties

ユーザは環境内のユーザ コンソールのアイコンおよびタイトルをカスタマイズできます。たとえば、［ユーザ コンソール］画面に会社ロゴおよび会社名を追加できます。

テーマ プロパティには以下の設定が含まれます。

Icon（URI）

アプリケーション サーバに利用可能なイメージへの URI を使用して、アイコンを定義します。

例： http://myserver.mycompany.com/images/front/logo.gif

Icon Link（URI）

URI を使用して、イメージへのナビゲーション リンクを定義します。

Icon Title

アイコンにマウスオーバー テキストとして表示されるツールヒントを定義します。

Title

カスタム テキストを指定します。カスタム テキストは、ユーザ コンソールの一番上のアイコンの隣に表示されます。

注: カスタム スキンを定義した場合、スキン用のプロパティ ファイルを参照することによりアイコンまたはタイトルを指定できます。 たとえば、カスタム スキン用のプロパティ ファイル内のアイコン イメージのエントリが、image/logo.gif である場合、アイコン フィールドにその同じ文字列を入力できます。

Login Properties

環境にアクセスするときにユーザに表示されるログイン ページの認証方式および場所を指定します。

Authentication Provider module class name

認証プロバイダ モジュールのクラス名を指定します。

Login Page

環境にアクセスするときにユーザに表示されるページを指定します。

Web サービス

CA Identity Manager Task Execution Web Service （TEWS）は、実行用の CA Identity Manager への CA Identity Manager タスクをリモートでサブミットするためにサードパーティ クライアント アプリケーションを有効にします。

［Web サービス］プロパティ 画面では、環境用の TEWS を設定できます。 この画面から、以下のタスクを実行できます。

- CA Identity Manager 環境の TEWS を有効にします。
- タスクに固有の Web サービス定義言語（WSDL）ドキュメントを生成します。
- ［代理］を許可します。
- 管理者パスワードが認証に必要であることを指定します。
- SiteMinder 認証を設定します。
- CA Identity Manager が SiteMinder と統合する場合に、Web サービス URL を保護する SiteMinder を設定します。
- Web Security Services Username トークン認証を指定します。
- 3 つの可能な認証タイプの少なくとも 1 つを指定します。

Task Execution Web Service による CA Identity Manager へのリモート リクエストの発行に関する詳細については、「Java のプログラミング ガイド」を参照してください。

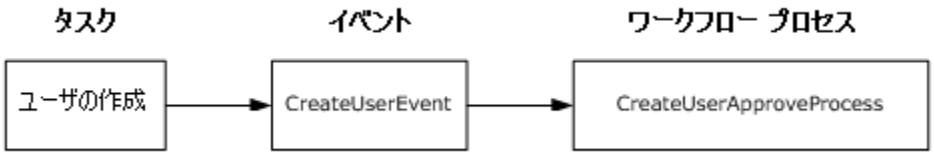
ワークフロー プロパティ

有効な場合、ワークフロー機能はワークフロー プロセスと関連付けられる CA Identity Manager タスクの実行を制御します。

ワークフロー プロセスは、ユーザ アカウントの作成などのビジネス目標を達成するために実行される手順セットです。 通常、これらの手順の 1 つにはタスクの承認または却下が含まれます。

管理タスクは 1 つ以上のイベントと関連付けられます。1 つ以上のワークフロー プロセスをトリガされる場合があります。ワークフロー プロセスが完了した後で、CA Identity Manager はワークフロー プロセスの結果に基づくタスクを実行するか、または拒否します。

以下の図は、CA Identity Manager タスク、関連するイベント、およびワークフロー プロセスの関係について示しています。



ワークフロー プロパティ

CA Identity Manager 環境のワークフローを有効にするか無効にするにはチェック ボックスを使用します。

作業アイテムの委任

有効な場合、作業アイテムの委任では、参加者（委任者）が別のユーザ（代行者）を指定して、代行者が委任者の作業リスト内のタスクを承認できるようにします。参加者が「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。

注: 作業アイテムの詳細については、「管理ガイド」を参照してください。

ワークフロー参加者リゾルバ

タスクの承認や拒否などのワークフロー プロセスのアクティビティは、*参加者*によって実行されます。

完全修飾参加者リゾルバ Java クラスにカスタム参加者リゾルバをマップするには、［ワークフロー参加者リゾルバ］画面を使用します。

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、CA Identity Manager にリストを返す Java オブジェクトです。 その後、CA Identity Manager はリストをワークフロー エンジンへ渡します。

一般に、カスタム参加者リゾルバを作成するのは、標準の参加者リゾルバ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を開発する詳細については、「Java のプログラミング ガイド」を参照してください。標準的な参加者リゾルバの詳細については、「管理ガイド」を参照してください。

カスタム設定のインポート/エクスポート

管理コンソールの［詳細設定］画面から、以下のように複数の環境に詳細設定を適用できます。

- 1 つの環境で詳細設定を設定します。
- XML ファイルに詳細設定をエクスポートします。
- 必要な環境に XML ファイルをインポートします。

Java 仮想マシン メモリ不足エラー

症状:

CA Identity Manager Server の機能に影響を及ぼすストレスまたは高負荷期間中に JVM メモリ不足エラーが発生します。

解決方法:

メモリ不足エラーが発生したら警告するように JVM デバッグ オプションを設定することをお勧めします。

注: JVM デバッグ オプションの設定の詳細については、Java HotSpot VM Options の「Debugging Options」（http://www.oracle.com）を参照してください。

第 8 章: 監査

このセクションには、以下のトピックが含まれています。

監査データ レポートの設定および生成方法 (P. 257)
監査データベースのクリーンアップ (P. 269)

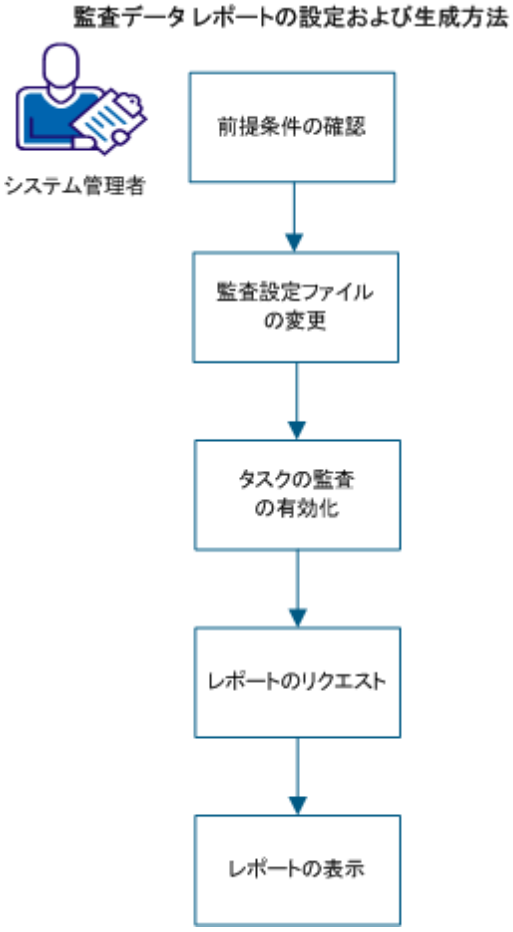
監査データレポートの設定および生成方法

監査データによって、環境で実行される操作の履歴レコードが提供されます。監査を設定して有効にすると、タスクに関する情報が監査データベースに記録されます。監査情報はレポートの生成に使用できます。管理データには、以下のようなものがあります。

- 特定期間のシステム アクティビティ。
- 特定の環境にアクセスしている間のユーザ ログインとログアウトのイベント。
- 特定のユーザが実行するタスク
- 特定期間内に変更されたオブジェクトのリスト
- ユーザが割り当てたロール
- 特定のユーザアカウントで実行される操作

監査データは、CA Identity Manager イベントに対して生成されます。 イベントは CA Identity Manager タスクによって生成される操作です。 たとえば、「ユーザの作成」タスクに「AssignAccessRoleEvent」イベントを含めることができます。

以下の図は、システム管理者が監査を設定し、監査データに関するレポートを生成する方法を示しています。



管理者として、以下の手順を実行します。

1. 前提条件の確認 (P. 259)
2. 監査設定ファイルの変更 (P. 259)
3. タスクの監査の有効化 (P. 264)
4. レポートのリクエスト (P. 265)
5. レポートの表示 (P. 268)

前提条件の確認

監査設定を設定するには、事前に以下の前提条件を満たしておく必要があります。

- 監査に関するデータを格納するために、個別のデータベース インスタンスが作成されます。 デフォルトでは、CA Identity Manager データベース スキーマ ファイルは以下の場所にあります。
  - **Windows**： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥Identity Manager¥tools¥db
- 監査レポートをリクエストして表示するためのレポート サーバ接続を設定します。
- 監査レポート用の接続オブジェクトを追加します。 以下の手順に従います。
  a. 管理者権限でユーザ コンソールにログインします。
  b. ［ロールおよびタスク］-［管理タスク］に移動し、変更する監査レポートを検索します。
  c. ［レポート用接続オブジェクト］フィールドに以下の接続名を入力します。
  `rptParamConn`

監査設定ファイルの変更

CA Identity Manager が監査する情報のタイプを定義するには、監査設定ファイルの監査設定を設定します。 監査設定ファイルを設定することによって、以下のタスクを実行できます。

- 管理タスクによって生成されるイベントの一部またはすべてを監査します。
- イベント完了時やイベントがキャンセルされるときなど、特定の状態のイベント情報を記録します。
- イベントに含まれる属性に関する情報をログ記録します。 たとえば、ModifyUserEvent イベント時に変更された属性をログ記録できます。

- 属性ログ記録の監査レベルを設定します。

監査設定ファイルは監査設定をエクスポートすることにより作成する XML ファイルです。 ファイルには以下のスキーマがあります。

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

Audit エレメントおよびスキーマの詳細については、監査設定ファイルのコメントを参照してください。

AuditProfileAttribute エレメントは、CA Identity Manager が監査する属性を示します。属性は AuditProfile エレメントで指定されたオブジェクトに適用されます。

注: 監査プロファイル属性が指定されていない場合、AuditProfile エレメントで指定されたオブジェクトの属性がすべてログに記録されます。

以下のテーブルでは、CA Identity Manager オブジェクト タイプの有効な属性について説明します。

CA Identity Manager オブジェクト タイプの有効な属性

オブジェクト タイプ	有効な属性
ACCESS ROLE	■ name -- ロールに対するユーザの表示名 ■ description -- ロールの目的に関するオプションのコメント。 ■ members -- ロールを使用できるユーザ。 ■ administrators -- ロール メンバまたは管理者を割り当てることができるユーザ。 ■ owners -- ロールを変更できるユーザ。 ■ enabled -- ロールが有効かどうかを示します。 ■ assignable -- 管理者によって割り当て可能かどうかを示します。 ■ tasks -- ロールと関連付けられるアクセス タスク。

CA Identity Manager オブジェクト タイプの有効な属性	
オブジェクト タイプ	**有効な属性**
ACCESS TASK	■ name -- タスクのユーザ表示名 ■ description -- タスクの目的に関するオプションのコメント ■ application -- タスクと関連付けられるアプリケーション。 ■ tag -- タスクの一意な識別子。 ■ reserved1、reserved2、reserved3、reserved4 — タスクの予約済みフィールドの値。
ADMINISTRATIVE ROLE	■ name -- ロールに対するユーザの表示名 ■ description -- ロールの目的に関するオプションのコメント ■ members -- ロールを使用できるユーザ。 ■ administrators -- ロール メンバまたは管理者を割り当てることができるユーザ。 ■ owners -- ロールを変更できるユーザ。 ■ enabled -- ロールが有効かどうかを示します。 ■ assignable -- 管理者によって割り当て可能かどうかを示します。 ■ tasks -- ロールと関連付けられるタスク。

CA Identity Manager オブジェクト タイプの有効な属性

オブジェクト タイプ	有効な属性
ADMINISTRATIVE TASK	■ name -- タスクのユーザ表示名 ■ description -- タスクの目的に関するオプションのコメント ■ tag -- タスクの一意な識別子。 ■ category -- タスクが表示される、CA Identity Manager ユーザ インターフェース内のカテゴリ ■ primary_objec -- タスクが操作するオブジェクト。 ■ action -- オブジェクト上で実行される操作。 ■ hidden -- タスクがメニューに表示されないかどうかを示します。 ■ public -- CA 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かどうかを示します。 ■ auditing -- タスクが監査情報の記録を有効にするかどうかを示します。 ■ external -- タスクが外部タスクかどうかを示します。 ■ url -- 外部タスクが実行されるときに、CA Identity Manager がユーザをリダイレクトする URL。 ■ workflow -- CA Identity Manager のイベントがタスク トリガ ワークフローと関連付けられているかどうかを示します ■ webservice -- タスクが CA Identity Manager 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であるかどうかを示します。
GROUP	ディレクトリ設定ファイル（directory.xml）で GROUP オブジェクトに対して定義されている任意の有効な属性。
ORGANIZATION PARENTORG	ディレクトリ設定ファイル（directory.xml）で Organization オブジェクトに対して定義されている任意の有効な属性。

CA Identity Manager オブジェクト タイプの有効な属性	
オブジェクト タイプ	**有効な属性**
RELATIONSHIP	■ %CONTAINER% -- 親オブジェクトの一意の識別子。 たとえば、RELATIONSHIP オブジェクトがロール メンバシップを説明する場合、コンテナはロールになります。 ■ %CONTAINER_NAME% -- 親グループのユーザ表示名。 ■ %ITEM% -- 親オブジェクトに含まれているオブジェクトの一意の識別子。 たとえば、RELATIONSHIP オブジェクトがロール メンバシップを説明する場合、アイテムはロール メンバになります。 ■ %ITEM_NAME% -- ネスト グループのユーザ表示名
USER	ディレクトリ設定ファイル（directory.xml）で USER オブジェクトに対して定義されている任意の有効な属性
NONE	属性なし

注: 以下の点が前のテーブルに適用されます。

- Enabled、assignable、auditable、workflow、hidden、webservice、および public は、true または false としてログに記録されます。
- ロールのタスクを監査するときには、ユーザ表示名がログに記録されます。
- データベースはコンパイルされた XML 形式でメンバ、管理者、および所有者ポリシーを格納します。 この形式は、各ポリシーが式として表示されるユーザ インターフェースとは異なります。

次の手順に従ってください:

1. 管理コンソールにログインして、環境を選択し、［Advanced Settings］を選択して、［Auditing］をクリックします。
2. ［Export］をクリックします。

   現在の監査設定が監査設定 XML ファイルにエクスポートされます。

3. 前の手順でエクスポートした XML ファイルの監査設定を変更します。以下のタスクを実行します。
   a. 「Audit enabled =」の値を「true」に設定し、データ ソース エレメントに「iam_im_<auditdb>.xml」の JNDI Name 値を指定します。
   b. 以下の JNDI 名を指定します。
      `java:/auditDbDataSource`

      注: このデータ ソースは、以下の場所にあります。
      `iam/im/jdbc/auditDbDataSource`
   c. ファイルのエレメントを追加、変更、または削除します。
   d. 各イベントに対して記録される情報のレベルを変更します。
4. 手順 1 ～ 2 を繰り返します。［Import］をクリックし、変更した監査設定 XML ファイルをアップロードします。
5. 環境を再起動します。

監査設定ファイルが更新されました。

タスクの監査の有効化

監査設定ファイルで監査を設定したタスクの監査を有効にします。

次の手順に従ってください:

1. 管理者権限でユーザ コンソールにログインします。
2. 監査を有効にするタスクを作成または変更します。
3. ［プロファイル］タブで、［監査の有効化］チェック ボックスがオンになっていることを確認します。
4. ［サブミット］をクリックします。

タスクに対して監査が有効になりました。

レポートのリクエスト

レポートを表示するには、レポートの管理権限を持つユーザにレポートをリクエストします。 監査データを追跡する適切なレポートを選択します。 レポート リクエストが承認を必要とする場合、システムはユーザに電子メール アラートを送ります。

レポートをスケジュールする前に、以下の手順を実行します。

1. 管理者権限でユーザ 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］に移動し、変更する監査レポートを検索します。
3. ［タブ］タブを選択し、編集する IAM ReportServerScheduler をクリックします。
4. ［反復オプションの有効化］チェック ボックスをオンにします。
5. ［OK］-［サブミット］をクリックします。

次の手順に従ってください:

1. レポート タスクのユーザ権限でユーザ コンソールにログインします。
2. ［レポート］-［レポート タスク］-［レポートのリクエスト］を選択します。

   レポートのリストが表示されます。
3. 監査ベースの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. ［レポートのスケジュール］をクリックし、レポートのスケジュールを選択します。

   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、特定の期間内にレポートが 1 回実行されます。 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。

   （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隔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。

5. ［サブミット］をクリックします。

   レポート リクエストがサブミットされます。ユーザの環境設定に応じて、リクエストはすぐに実行されるか、管理者による承認の後に実行されます。

   通常、システムによるリクエスト完了前に、システム管理者またはレポート管理権限を持つ別のユーザがレポート リクエストを承認する必要があります。承認が必要な理由は、レポートによっては実行に長い時間がかかったり、多大なシステム リソースが必要とされるためです。レポート リクエストが承認を必要とする場合、システムはユーザに電子メール アラートを送ります。

   注: 承認が必要な場合は、環境の［ワークフローの有効化］を設定します。

レポートの表示

ユーザの環境設定によっては、管理者がレポートのリクエストを承認するまでレポートを表示できません。レポート リクエストが承認待ちである場合、システムはユーザに電子メール アラートを送ります。表示しようとするレポートは、承認されるまで検索リストに表示されません。

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。

次の手順に従ってください:

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. 生成されたレポートで表示したものを検索します。

   反復レポートとオンデマンド レポートの両方のインスタンスが表示されます。

   注: レポートのステータスが保留中/反復である場合、レポートは生成されず、完了するのに時間がかかる可能性があります。
3. 表示するレポートを選択します。
4. （オプション）［このレポートをエクスポート］（左上隅）をクリックし、レポートを以下の形式でエクスポートします。
   - Crystal Report
   - PDF
   - Microsoft Excel （97-2003）
   - Microsoft Excel （97-2003）データのみ
   - Microsoft Excel （97-2003） - 編集可能
   - Rich Text Format （RTF）
   - カンマ区切り （CSB）
   - XML

監査データベースのクリーンアップ

必要でなくなったレコードが最終的に監査データベースによって累積される場合があります。これらのレコードを削除するには、db¥auditing ディレクトリの以下のデータベース手順を実行します。

`garbageCollectAuditing12 environment-ID MM/DD/YYYY`

environment-ID

CA Identity Manager 環境の ID を定義します。

MM/DD/YYYY

監査レコードを削除する必要がある日付を定義します。

第 9 章: 実稼働環境

このセクションは、特定の機能を移行するための段階的な機能の説明を提供します。制限のある変更が開発環境で行われ、それらの変更が適切に理解される場合にのみ使用してください。

このセクションには、以下のトピックが含まれています。

管理ロールおよびタスク定義を移行する方法 (P. 271)
CA Identity Manager スキンを移行する方法 (P. 273)
実稼働環境での CA Identity Manager の更新 (P. 273)
JBoss の iam_im.ear の移行 (P. 276)
WebLogic の iam_im.ear の移行 (P. 277)
WebSphere の iam_im.ear の移行 (P. 278)
ワークフロー プロセス定義の移行 (P. 279)

管理ロールおよびタスク定義を移行する方法

ユーザの会社の特定のニーズを満たすために、CA Identity Manager ロールおよびタスクをカスタマイズできます。カスタマイズには、管理ロールおよびタスクの作成または変更、管理ロールまたはタスクの作成または変更タスクの使用が含まれます。

代替方法は、*推奨されません*が、roledefinition.xml ファイルのロールおよびタスクを変更することです。編集にはエラーのリスクがあるため、非常に限定された変更に対してこの方法を使用します。

このプロセスでは管理ロールおよびタスク定義のみを移行します。ロールが組織にバインドされた場合は、CA Identity Manager 環境全体を移行することを検討します。

重要: ユーザが実稼働環境のロールまたはタスク定義を変更した場合、ユーザが開発環境からロールまたはタスク定義をインポートするときに、それらの変更が失われます。ロールおよびタスク定義をインポートすると、同じ名前を持つ既存のロールおよびタスク定義が上書きされます。

管理ロールおよびタスク定義をエクスポートする方法

変更が roledefinition.xml ファイルに直接行われた場合、このファイルは、直接実稼働環境にインポートできます。 それ以外の方法で、ロールおよびタスクの定義をエクスポートする方法

1. ポリシー サーバ クラスタがある場合は、1 つのポリシー サーバのみが実行されていることを確認します。
2. 1 つの CA Identity Manager ノード以外のすべてを停止します。
3. 管理コンソールにログインします。
4. CA Identity Manager 環境をクリックします。
5. ロールおよびタスク定義をエクスポートする、CA Identity Manager 環境を選択します。
6. ［ロール］をクリックし、［エクスポート］をクリックして、ファイルの名前を提供します。
7. このファイルをインポートするには、次の手順の指示に従います。

管理ロールおよびタスク定義のインポート方法

次の手順に従ってください:

1. 実稼働環境に前の手順で作成したファイルをコピーします。
2. 実稼働環境で管理コンソールにログインします。
3. CA Identity Manager 環境をクリックします。
4. 該当する CA Identity Manager 環境をクリックします。
5. ［ロール］をクリックします。
6. ［インポート］をクリックし、エクスポートが生成する XML ファイルの名前を指定します。
7. これらの手順が正常に行われた場合、停止しているすべてのポリシー サーバおよび CA Identity Manager ノードを開始します。

   注: CA Identity Manager 環境でまだ変更を行う場合は、手順 6 を繰り返します。

ロールおよびタスクのインポートを確認する方法

ロールおよびタスクが正常にインポートされたことを確認するには、以下のタスクを使用できる管理者アカウントとして CA Identity Manager にログインします。

- 管理ロールの変更
- 管理タスクの変更

これらのタスクを実行し、ロールおよびタスクが新しくインポートされたロール定義を反映していることを確認します。

CA Identity Manager スキンを移行する方法

CA Identity Manager スキンはアプリケーションに特定のルック アンド フィールを与えるようにカスタマイズできます。ユーザの集合に新しいスキンを変更または作成した場合、開発環境から実稼働環境にスキンを移行するには、以下の手順に従います。

スキンを変更している場合は、変更されたファイルをコピーします。

次の手順に従ってください:

1. イメージ ファイル、スタイル シート、プロパティ ファイル、コンソール ページ（index.jsp）など開発サーバから実稼働サーバに新規の変更されたファイルをコピーします。
2. 複数のスキンが使用されている場合は、SiteMinder レスポンスを設定します。

   注: 複数のスキンの使用方法の詳細については、「*設定ガイド*」を参照してください。

スキンの移行を確認するには、［ユーザ コンソール］にログインして、スキンが正しく表示されることを確認します。

実稼働環境での CA Identity Manager の更新

開発から実稼働に CA Identity Manager を移行した後に、増分更新を実行する必要がある場合があります。 ユーザの開発環境からユーザの実稼働環境に新しい CA Identity Manager 機能を移行するには、以下の手順に従います。

1. CA Identity Manager 環境を移行します。
2. iam_im.ear をコピーします。
3. ワークフロー プロセス定義を移行します。

CA Identity Manager 環境を移行する方法

CA Identity Manager 環境は管理コンソールから作成されます。CA Identity Manager 環境には 1 セットのロールおよびタスク定義、ワークフロー定義、CA Identity Manager API で作成されるカスタム機能、および CA Identity Manager ディレクトリが含まれます。

次の手順に従ってください:

1. CA Identity Manager が SiteMinder と統合され、ポリシー サーバ クラスタがある場合は、1 つのポリシー サーバのみが実行されていることを確認します。
2. 1 つの CA Identity Manager ノード以外のすべてを停止します。
3. 開発環境で管理コンソールから CA Identity Manager 環境をエクスポートします。
4. 実稼働環境の管理コンソールでエクスポートされた環境をインポートします。
5. CA Identity Manager が SiteMinder と統合される場合は、ポリシー サーバ ユーザ インターフェースの CA Identity Manager レルムを再保護します。

   ユーザが CA Identity Manager 環境をエクスポートするときに、ポリシー ドメインはポリシー ストアからエクスポートされません。
6. 停止したポリシー サーバおよび CA Identity Manager ノードを再起動します。

CA Identity Manager 環境 を移行するときには、以下のアクティビティが発生します。

- 同じオブジェクトが両方の場所に存在する場合、開発サーバ上の変更は実稼働サーバ上の変更を上書きします。
- 新規オブジェクトが開発環境で作成される場合、それらは実稼働サーバに追加されます。
- 新規オブジェクトが実稼働サーバで作成される場合、それらは保持されます。

CA Identity Manager 環境をエクスポートする方法

実稼働システム上の CA Identity Manager 環境を展開するには、開発またはステージング システムから環境をエクスポートし、実稼働システムへその環境をインポートします。

注: ユーザが以前にエクスポートされた環境をインポートする場合、CA Identity Manager に管理コンソール内のステータス ウィンドウ内のログが表示されます。このログで各管理対象オブジェクトおよびその属性の検証および展開情報を参照するには、環境をエクスポートする*前に*、［環境プロパティ］ページ上で［詳細ログ出力の有効化］フィールドを選択します。［詳細ログ出力の有効化］フィールドを選択するとインポート中に重大なパフォーマンスの問題を引き起こす場合があることを確認します。

次の手順に従ってください:

1. 管理コンソールの［環境］をクリックします。

   CA Identity Manager 環境画面が CA Identity Manager 環境のリストと共に表示されます。
2. エクスポートする環境を選択します。
3. [エクスポート]ボタンをクリックします。

   ［ファイルのダウンロード］画面が表示されます。
4. 実稼働システムにアクセス可能な場所に ZIP ファイルを保存します。
5. ［完了］をクリックします。

   環境情報は、別の環境にインポート可能な ZIP ファイルにエクスポートされます。

CA Identity Manager 環境をインポートする方法

開発システムから CA Identity Manager 環境をエクスポートした後で、実稼働システムにインポートできます。

次の手順に従ってください:

1. 管理コンソールの［環境］をクリックします。

   CA Identity Manager 環境画面が CA Identity Manager 環境のリストと共に表示されます。
2. ［インポート］ボタンをクリックします。

   ［環境のインポート］画面が表示されます。

3. 環境をインポートするのに必要な ZIP ファイルを参照します。
4. ［完了］をクリックします。

環境は CA Identity Manager へインポートされます。

CA Identity Manager 環境の移行を確認する方法

CA Identity Manager 環境の適切な移行を確認するには、CA Identity Manager 環境が実稼働環境のポリシー サーバのポリシー サーバ ユーザ インターフェースに表示されることを確認します。

ポリシー サーバ ユーザ インターフェースで、以下の点を確認します。

- CA Identity Manager ユーザ ディレクトリ設定が正確である
- 新しい CA Identity Manager ドメインが存在する
- 正しい認証スキームは CA Identity Manager レルムを保護する

また、管理コンソールにログインする際に、ユーザが環境を選択するときに CA Identity Manager 環境が表示されることを確認します。

JBoss の iam_im.ear の移行

機能が開発環境から実稼働環境に移行されるたびに、iam_im.ear を再展開します。EAR 全体を移行することにより、実稼働環境が開発環境と同一であることを確認します。

次の手順に従ってください:

1. 開発環境からユーザの実稼働環境にアクセス可能な場所に iam_im.ear をコピーします。
2. iam_im.ear のコピーで、ポリシー サーバ接続情報を編集し、実稼働環境を反映されるようにします。

   この変更を行うには、実稼働環境の *jboss_home*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml を iam_im.ear にコピーします。

3. インストールされた iam_im.ear を以下のような手順で、開発環境の iam_im.ear のコピーと置き換えます。
   a. 実稼働サーバで、iam_im.ear を削除します。

      cluster_node_jboss_home¥server¥default¥deploy¥iam_im.ear

   b. 削除されたファイルを開発環境の iam_im.ear の編集されたコピーと置き換えます。
4. クラスタの各ノードでこの手順を繰り返します。

WebLogic の iam_im.ear の移行

機能が開発環境から実稼働環境に移行されるたびに、iam_im.ear を再展開します。EAR 全体を移行することにより、実稼働環境が開発環境と同一であることを確認します。

次の手順に従ってください:

1. ポリシー サーバ接続情報を維持します。

   ポリシー サーバ接続情報は、policyserver_rar/WEB-INF ディレクトリの ra.xml ファイルに格納されます。 このファイルを別の場所にコピーし、それを再展開する前に iam_im.ear で置き換えられるようにします。
2. WebLogic 管理サーバに利用可能な場所に iam_im.ear をコピーします。
3. ポリシー サーバ接続情報を置き換えます。

   iam_im.ear で、policyserver_rar/WEB-INF/ra.xml ファイルを手順 1 で保持しているファイルに置き換えます。
4. iam_im.ear を再展開します
   a. WebLogic コンソールにログインします。
   b. ［展開］-［アプリケーション］-［Identity Manager］に移動します。

［展開］ タブで、［アプリケーションの展開（再展開）］を選択します。

WebSphere の iam_im.ear の移行

次の手順に従ってください:

1. *was_im_tools_dir*¥*WebSphere-tools* から *deployment_manager_dir* ¥*bin* ディレクトリに *imsInstall.jacl* スクリプトをコピーします。各項目の説明：
   - *was_im_tools_dir* は、WebSphere 用の CA Identity Manager Tools がインストールされている開発システム上のディレクトリです。
   - *deployment_manager_dir* は展開マネージャがインストールされている場所です。
2. CA Identity Manager アプリケーションを設定した開発システムで、*was_im_tools_dir* ¥*WebSphere-tools*¥*imsExport.bat* または *imsExport.sh* を *was_home*¥*bin* にコピーします。
3. コマンド ラインで、*was_home*¥*bin* に移動します。
4. WebSphere アプリケーションが実行されていることを確認します。
5. 展開した CA Identity Manager アプリケーションを以下のようにエクスポートします。

   Windows の場合、以下のコマンドを入力します。

   ```
   imsExport.bat "path-to-exported-ear"
   ```

   ここで *path-to-exported-ear* は、imsExport ユーティリティが作成するフルパスおよびファイル名です。

   Windows システムの場合、path to was_im.ear を指定するときに、バックスラッシュ（¥）の代わりにスラッシュ（/）を使用します。 例：

   ```
   imsExport.bat "c:/program files/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   UNIX の場合、以下のコマンドを入力します。

   ```
   ./wsadmin -f imsExport.jacl -conntype RMI -port 2809 path to exported ear
   ```

   ここで *path-to-exported-ear* は、エクスポートされた EAR ファイルのファイル名を含むフル パスです。
6. エクスポートした EAR ファイルを、エクスポートした開発環境の場所から、展開マネージャがインストールされているシステム上の場所にコピーします。
7. *was_im_tools_dir*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml を実稼働環境のものと置き換えます。

   ra.xml ファイルにはポリシー サーバ接続情報が含まれます。

8. 展開マネージャがインストールされているシステムで、Identity Manager EAR を展開します。

   a. コマンドラインで、次のディレクトリに移動します。

      deployment_manager_dir ¥bin.

   b. WebSphere アプリケーション サーバが実行されていることを確認します。

   c. 以下のように imsInstall.jacl スクリプトを実行します。

   注: imsInstall.jacl スクリプトは、実行するのに数分かかる場合があります。

   Windows の場合：

      wsadmin -f imsInstall.jacl *"path-to-copied-ear" cluster_name*

      ここで *path-to-copied-ear* は展開マネージャ システムにコピーした Identity Manager EAR のファイル名を含むフル パスです。

      例：

      wsadmin -f imsInstall.jacl "c:¥Program Files¥CA¥Identity Manager¥WebSphere-tools¥was_im.ear" im_cluster

   UNIX の場合：

      ./wsadmin -f imsInstall.jacl *path-to-copied-ear cluster_name*

      ここで *path-to-copied-ear* は展開マネージャ システムにコピーした Identity Manager EAR のファイル名を含むフル パスです。

      例：

      ./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. CA Identity Manager が SiteMinder と統合される場合は、以下の点を確認します。

   - SiteMinder エージェントはユーザのポリシー ストアに接続できます。
   - ポリシー サーバはユーザ ストアに接続できます。
   - CA Identity Manager ドメインが作成されています。

ワークフロー プロセス定義の移行

開発環境でワークフローを使用した場合は、ワークフロー定義をエクスポートし、それを実稼働環境にインポートします。次に、各サーバ ノードのワークフローを設定します。

プロセス定義のエクスポート

開発環境システムで、ワークフロー プロセス定義をエクスポートします。

次の手順に従ってください:

1. アプリケーション サーバが実行されていることを確認します。
2. *admin_tools*¥Workpoint¥bin¥ に移動し、Archive.bat （Windows 用）または Archive.sh （UNIX 用）を以下のように実行します。
   a. ［インポート］ダイアログ ボックスで、ルート オブジェクトを選択します。
   b. ［追加］をクリックします。
   c. 生成するファイルの名前を指定します。
   d. ［エクスポート］をクリックします。
   e. ［実行］をクリックします。

   admin_tools は、以下のいずれかの場所にデフォルトでインストールされる管理ツールを参照します。

   - **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
3. 手順については、次のセクションの「プロセス定義のインポート (P. 280)」に従ってください。

プロセス定義のインポート

実稼働環境システムで、ワークフロー プロセス定義をインポートします。

次の手順に従ってください:

1. アプリケーション サーバを再起動します。
2. オプションで、前の手順を使用して定義をエクスポートすることにより現在の定義のバックアップ コピーを作成します。

3. *admin_tools*¥Workpoint¥bin¥ に移動し、以下のように Archive スクリプトを実行します。

   a. ［インポート］ダイアログ ボックスで、インポートするアイテムをすべて選択します。

   b. 新しい形式を使用するか、または古い形式を使用するかについて促される場合は、古い形式を保持します。

      新しい形式は CA Identity Manager をサポートしていません。

   c. エクスポートが生成するファイルの名前を提供します。

   d. ［実行］をクリックします。

   admin_tools は、以下のいずれかの場所にデフォルトでインストールされる管理ツールを参照します。

   - **Windows：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools
   - **UNIX：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

第 10 章: CA Identity Manager ログ

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 で問題を追跡する方法 (P. 283)
コンポーネントおよびデータ フィールドを追跡する方法 (P. 285)

CA Identity Manager で問題を追跡する方法

CA Identity Manager には、ステータスとトラッキングの問題を記録するための以下の方法が含まれます。

[サブミット済みタスクの表示]タスク

CA Identity Manager 環境のすべてのイベントおよびタスクのステータスを表示します。管理者はユーザ コンソールでこのタスクを使用します。

［サブミット済みタスクの表示］では、以下のタイプの情報を提供します。

- 環境で発生するイベントおよびタスクのリスト。
- イベントと関連付けられる属性のリスト。
- 成功および失敗したイベント
- 保留中かストール状態のイベント。
- 拒否されたイベント（拒否された理由を含む）
- アカウント同期ステータス
- アイデンティティ ポリシー同期ステータス
- プロビジョニング情報（プロビジョニングが有効な場合）。

アプリケーション サーバ 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。

ログ ファイルの場所およびタイプは、ユーザが以下のタイプのアプリケーション サーバのどれを使用しているかによって異なります。

- WebLogic -- CA Identity Manager 情報は標準出力に書き込まれます。デフォルトでは、標準出力はサーバ インスタンスが実行されているコンソール ウィンドウです。
- JBoss -- CA Identity Manager 情報は、サーバ インスタンスが実行されているコンソール ウィンドウ、および *jboss_home*¥server¥log¥server.log に書き込まれます。
- WebSphere -- CA Identity Manager 情報は、サーバ インスタンスが実行されているコンソール ウィンドウ、および *was_home*¥AppServer¥logs¥*server_name*¥SystemOut に書き込まれます。

詳細については、アプリケーション サーバのマニュアルを参照してください。

ディレクトリ サーバ ログ ファイル

ユーザ ディレクトリで発生するアクティビティに関する情報を含みます。

記録される情報のタイプおよびログ ファイルの場所は、使用しているディレクトリ サーバのタイプにより異なります。 詳細については、ディレクトリのサーバ マニュアルを参照してください。

ポリシー サーバ ログ ファイル

CA Identity Manager が SiteMinder と統合されるときに、以下の情報を表示します。

- SiteMinder 接続問題
- SiteMinder 認証問題
- SiteMinder ポリシー ストアの CA Identity Manager 管理対象オブジェクトに関する情報。
- パスワード ポリシー評価

SiteMinder ログの設定の詳細については、「*CA SiteMinder Web Access Manager Policy Server Administration Guide*」を参照してください。

ポリシー サーバ プロファイラ

CA Identity Manager が SiteMinder と統合する場合、CA Identity Manager に関連する機能を含む、内部ポリシー サーバ診断および処理機能を追跡できます。

詳細については、「コンポーネントおよびデータ フィールドを追跡する方法 (P. 285)」 を参照してください。

Web エージェント ログ ファイル

CA Identity Manager が SiteMinder と統合される場合、Web エージェントは以下の 2 つのログに情報を書き込みます。

- エラー ログ ファイル -- プログラムおよび操作レベルのエラー（たとえば、Web エージェントがポリシー サーバと通信できないなど）が含まれます。
- トレース ログ ファイル -- 警告、およびトレース メッセージやフロー状態メッセージなどの情報メッセージが含まれます。 また、このファイルには、ヘッダの詳細や cookie 変数などのデータも含まれます。

注: Web エージェント ログ ファイルの詳細については、「*CA SiteMinder Web Access Manager Web Agent Configuration Guide*」を参照してください。

コンポーネントおよびデータ フィールドを追跡する方法

CA Identity Manager が SiteMinder と統合される場合、ポリシー サーバ用の CA Identity Manager 拡張でトレース コンポーネントおよびデータ フィールドを追跡するには、SiteMinder ポリシー サーバ プロファイラを使用できます。プロファイラでは、コンポーネントまたはデータ フィールドに対する特定の値のみがキャプチャされるように、追跡出力のフィルタを設定できます。

注: ポリシー サーバ プロファイラの使用方法の詳細については、「*CA SiteMinder Web Access Manager Policy Server Administration Guide*」を参照してください。

以下のコンポーネントに対してトレースを有効にできます。

Function_Begin_End

ポリシー サーバ用の CA Identity Manager 拡張で特定の方法が実行される場合に、低レベルのトレース ステートメントを提供します。

IM_Error

SiteMinder ポリシー サーバ用の CA Identity Manager 拡張でランタイム エラーを追跡します。

IM_Info

CA Identity Manager 拡張の一般的なトレース情報を提供します。

IM_Internal

内部 CA Identity Manager 操作に関する一般的な情報をトレースします。

IM_MetaData

CA Identity Manager がディレクトリ メタデータを処理するときにトレース情報を提供します。

IM_RDB_Sql

リレーショナル データベースのトレース情報を提供します。

IM_LDAP_Provider

LDAP ディレクトリのトレース情報を提供します。

IM_RuleParser

ランタイムに解釈される XML ファイルで定義されている、メンバ、所有者、および管理ポリシーを解析および評価するプロセスをトレースします。

IM_RuleEvaluation

メンバ、管理者、所有者、およびスコープ ルールの評価をトレースします。

IM_MemberPolicy

メンバシップおよびスコープを含む、メンバ ポリシーの評価をトレースします。

IM_AdminPolicy

管理ポリシーの評価をトレースします。

IM_OwnerPolicy

所有者ポリシーの評価をトレースします。

IM_RoleMembership

ユーザが持つロールのリストや特定のロールのメンバのリストなどロール メンバシップに関係する情報をトレースします。

IM_RoleAdmins

ユーザが管理できるロールのリストや特定のロールの管理者のリストなどロール管理に関係する情報をトレースします。

IM_RoleOwners

ユーザが所有するロールのリストや特定のロールの所有者のリストなどロール所有者に関係する情報をトレースします。

IM_PolicyServerRules

RoleMember、RoleAdmin、ポリシー サーバが解決した RoleOwner、AccessTasks の All や AccessTaskFilter ルールなどのスコール ルールなど、メンバ ルールの評価をトレースします。

IM_LLSDK_Command

内部 CA Identity Manager SDK とポリシー サーバの間の通信をトレースします。テクニカル サポートはこのトレース コンポーネントを使用します。

IM_LLSDK_Message

トレース メッセージは、内部 CA Identity Manager SDK からポリシー サーバに Java コードによって明示的に送信されます。 テクニカル サポートはこのトレース コンポーネントを使用します。

IM_IdentityPolicy

アイデンティティ ポリシーの評価およびアプリケーションをトレースします。

IM_PasswordPolicy

パスワード ポリシーの評価をトレースします。

IM_Version

CA Identity Manager バージョンに関する情報を提供します。

IM_CertificationPolicy

認証ポリシーの評価をトレースします。

IM_InMemoryEval

メンバ、管理者、所有者、アイデンティティ ポリシーを含む、CA Identity Manager ポリシーの処理をトレースします。 テクニカル サポートはこのトレース コンポーネントを使用します。

IM_InMemoryEvalDetail

メンバ、管理者、所有者、アイデンティティ ポリシーを含む、CA Identity Manager ポリシーの処理に関する追加の詳細を提供します。 テクニカル サポートはこのトレース コンポーネントを使用します。

トレースを設定できるデータ フィールドは、「*CA SiteMinder Web Access Manager Policy Server Administration Guide*」でリスト表示されます。

第 11 章: CA Identity Manager 保護

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 コンソール セキュリティ (P. 289)
管理コンソール セキュリティ (P. 290)
CSRF 攻撃からの保護 (P. 295)

ユーザ コンソール セキュリティ

ユーザ コンソールは、管理者が CA Identity Manager 環でユーザ、グループ、組織のようなオブジェクトを管理できるユーザ インターフェースです。これらのオブジェクトは、関連付けられたロールとタスクのセットで割り当てられます。 管理者がユーザ コンソールにログインするときに、管理者に関連するタスクがその環境に表示されます。

デフォルトで、CA Identity Manager は、ネイティブ認証を使用したユーザ コンソールへのアクセスを保護します。 CA Identity Manager 管理者は、CA Identity Manager 環境にログインするために、有効なユーザ名およびパスワードを入力します。 CA Identity Manager は、CA Identity Manager が管理するユーザ ストアに対する名前およびパスワードを認証します。

CA Identity Manager が SiteMinder と統合される場合、CA Identity Manager は、環境を保護するために*自動的に* SiteMinder 基本認証を使用します。 基本認証を使用するために追加の設定を行う必要ではありません。 SiteMinder 管理ユーザ インターフェースを使用して、高度な認証方式を設定できます。

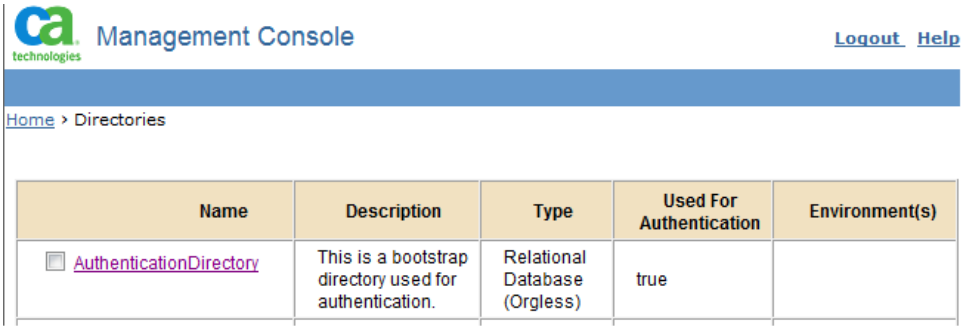
注: 詳細については、「*CA SiteMinder Web Access Manager Policy Server Configuration Guide*」を参照してください。

管理コンソール セキュリティ

管理コンソールにより、管理者が CA Identity Manager ディレクトリおよび環境を作成し管理できます。 管理者は、管理コンソールを使用して、環境用のカスタム機能を設定することもできます。

CA Identity Manager インストールには、管理コンソールを保護するオプションが含まれます。デフォルトでは、このオプションが選択されています。インストール中に、管理コンソールにアクセスできる管理者を認証するには、CA Identity Manager が使用するクレデンシャルを指定します。 CA Identity Manager は、AuthenticationDirectory という名前のブートストラップ ディレクトリで提供するクレデンシャルを使用してユーザを作成します。管理コンソールでこのディレクトリを表示できます。

注: CA Identity Manager が CASiteMinder と統合するときに、管理コンソールを保護するためにネイティブ セキュリティを使用することはできません。



追加の管理コンソール管理者の追加

デフォルトでは、ネイティブ CA Identity Manager セキュリティによって保護される管理コンソールは、インストール中に新しい CA Identity Manager ディレクトリで作成される 1 つの管理者アカウントがあります。

追加の管理者を追加するには、管理コンソールへのアクセスを必要とするユーザを含む CA Identity Manager ディレクトリを指定します。 新規アカウントを作成する必要なしに、既存のディレクトリを使用することにより、組織のユーザへの管理コンソール アクセスを付与できます。

認証のために 1 つのディレクトリのみを指定できます。ディレクトリが認証用に設定されている限り、そのディレクトリを削除することはできません。

次の手順に従ってください:

1. インストール中に提供したユーザ クレデンシャルを使用して管理コンソールにログインします。
2. ディレクトリを開き、管理コンソールへのアクセスを必要とするユーザを含むディレクトリをクリックします。
3. ［Update Authentication］をクリックします。
4. ［Used for Authentication］を選択します。
5. 最初のユーザのログイン名を入力し、［追加］をクリックします。
6. すべてのユーザが追加されるまで管理コンソールへのアクセスを必要とするユーザの追加を続行します。 次に、［保存］をクリックします。

   これで、指定したユーザは、ユーザ名とパスワードを使用して、管理コンソールにアクセスできるようになります。

管理コンソールのネイティブ セキュリティの無効化

管理コンソールのネイティブ セキュリティを有効にし、それを保護するために別のアプリケーションを使用する場合は、別のセキュリティ方法を実装する前にネイティブ セキュリティを無効にします。

次の手順に従ってください：

1. web.xml ファイルの管理コンソールのネイティブ セキュリティを以下のように無効にします。
   a. テキスト エディタで *CA Identity Manager_installation*¥iam_im.ear¥management_console.war¥WEB-INF¥web.xml を開きます。
   b. ManagementConsoleAuthFilter の Enable パラメータの値を以下のように設定します。

```
<filter>
<filter-name>ManagementConsoleAuthFilter</filter-name>
<filter-class>com.netegrity.ims.manage.filter.ManagementConsoleAuthFilter</filter-class>
<init-param>
<param-name>Enable</param-name>
<param-value>false</param-value>
</init-param>
</filter>
```

   c. web.xml ファイルを保存します。
2. WebLogic サーバを再起動します。

   管理コンソールは、ネイティブ セキュリティによって保護されなくなります。

SiteMinder を使用して管理コンソールを保護する

管理コンソールを最初に保護するために、SiteMinder ポリシーを作成できます。

SiteMinder ポリシーは、管理コンソールなど、保護するリソースを特定し、そのリソースへのユーザ アクセスのセットを付与します。

次の手順に従ってください：

1. 管理コンソールのネイティブ セキュリティを無効 (P. 292)にします。
2. ドメイン権限を持つ管理者として以下のインターフェースのいずれかにログインします。
   - CASiteMinder r12 以降の場合は、管理 UI にログインします。
   - CASiteMinder6.0 SP*x* の場合は、ポリシー サーバ ユーザ インターフェースにログインします。

   注: これらのインターフェースの使用の詳細については、使用している SiteMinder のバージョン用のマニュアルを参照してください。
3. 適切な CA Identity Manager 環境のポリシー ドメインを見つけます。

   CA Identity Manager が SiteMinder と統合するときに、このドメインは自動的に作成されます。 ドメイン名の形式は、以下のとおりです。

   *Identity Manager-environment*Domain

   この形式では、*Identity Manager-environment* は、変更している環境の名前を指定します。 たとえば、名前が *従業員* であるときには、ドメイン名は *employees*Domain です。
4. 以下のリソース フィルタでレルムを作成します。

   /iam/immanage/
5. レルムにルールを作成します。 管理コンソールのページをすべて保護するためのフィルタとしてアスタリスク（*）を指定します。
6. 新しいポリシーを作成し、前の手順で作成したルールと関連付けます。

   必ず管理コンソールにアクセスできるユーザとポリシーを関連付けます。
7. アプリケーション サーバを再起動します。

アップグレードの後の既存環境の保護

CA Identity Manager12.6 以降にアップグレードした後で、ネイティブ セキュリティを使用して、管理コンソールを保護できます。

注: CA Identity Manager が CASiteMinder と統合される場合は、管理コンソールを保護するためにネイティブ CA Identity Manager セキュリティを使用することはできません。

次の手順に従ってください：

1. web.xml ファイルの管理コンソールのネイティブ セキュリティを以下のように有効にします。
   a. テキスト エディタで *CA Identity Manager_installation*¥iam_im.ear¥management_console.war¥WEB-INF¥web.xml を開きます。
   b. ManagementConsoleAuthFilter の Enable パラメータの値を 以下のように true に設定します。

```
<filter>
<filter-name>ManagementConsoleAuthFilter</filter-name>
<filter-class>com.netegrity.ims.manage.filter.ManagementConsoleAuthFilter</filter-class>
<init-param>
<param-name>Enable</param-name>
<param-value>true</param-value>
</init-param>
</filter>
```

   c. web.xml ファイルを保存します。
2. CA Identity Manager オブジェクト ストアで IM_AUTH_USER テーブルを作成します。

   IM_AUTH_USER テーブルは、管理コンソール管理者に関する情報を格納します。
   a. CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥db¥objectstore に移動します
   b. オブジェクト ストアに対して、以下のいずれかのスクリプトを実行します。
      - sql_objectstore.sql
      - oracle_objectstore.sql

   注: 既存のデータベースに対してスクリプトを実行する方法の詳細については、そのデータベース用のベンダー マニュアルを参照してください。

3. パスワード ツールを使用して、ユーザー パスワードを暗号化します。

   パスワード ツールは、CA Identity Manager ツールとともに以下の場所にインストールされます。

Windows： C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥PasswordTool

UNIX： /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   PasswordTool

   以下のコマンドを使用して、パスワード ツールを実行します。
   `pwdtools -JSAFE -p anypassword`

   JSAFE オプションにより、PBE アルゴリズムを使用してプレーン テキスト値が暗号化されます。

1. IM_AUTH_USER テーブルにブートストラップ ユーザ情報を挿入します。
   IM_AUTH_USER テーブルですべての列に対する値を指定します。

   例：

   USER_NAME: admin1

   PASSWORD: *anypassword*

   DISABLED: 0

   ID:1

2. CA Identity Manager サーバを再起動します。

   管理コンソールはネイティブ セキュリティによって保護されます。

CSRF 攻撃からの保護

CA Identity Manager は強化され、Cross-Site Request Forgery （CSRF）攻撃に対する抵抗が向上しました。 この強化機能は CA Identity Manager ではデフォルトで無効になっています。

強化機能を有効化する方法

1. 以下の場所にある web.xml ファイルを開きます。

   application-server/iam_im.ear/user_console.war/WEB-INF

2. <param-name> csrf-prevention-on を持つ <context-param> エレメントを検索します。

3. <param-value> を true に設定します。

4. アプリケーション サーバを再起動します。

第 12 章: CA SiteMinder の統合

このセクションには、以下のトピックが含まれています。

SiteMinder および CA Identity Manager (P. 298)
リソースが保護される方法 (P. 299)
SiteMinder と CA Identity Manager の統合の概要 (P. 300)
CA Identity Manager の SiteMinder ポリシー ストアの設定 (P. 305)
ポリシー ストアへの CA Identity Manager スキーマのインポート (P. 312)
SiteMinder4.x エージェント オブジェクトの作成 (P. 312)
CA Identity Manager ディレクトリおよび環境のエクスポート (P. 314)
すべてのディレクトリおよび環境定義の削除 (P. 315)
SiteMinder ポリシー サーバ リソース アダプタの有効化 (P. 316)
ネイティブ CA Identity Manager フレームワーク認証フィルタの無効化 (P. 317)
アプリケーション サーバの再起動 (P. 318)
SiteMinder 用のデータ ソースの設定 (P. 318)
ディレクトリ定義のインポート (P. 319)
環境定義の更新およびインポート (P. 320)
Web プロキシ サーバ プラグインのインストール (P. 320)
SiteMinder エージェントと CA Identity Manager ドメインの関連付け (P. 341)
SiteMinder LogOffUrl パラメータの設定 (P. 342)
トラブルシューティング (P. 342)
CA Identity Manager エージェント設定を設定する方法 (P. 351)
SiteMinder の高可用性の設定 (P. 352)
既存の CA Identity Manager 展開からの SiteMinder の削除 (P. 355)
SiteMinder 操作 (P. 355)

SiteMinder および CA Identity Manager

CA Identity Manager が CASiteMinder と統合される場合、CA SiteMinder は CA Identity Manager 環境に以下の機能を追加できます。

高度な認証

CA Identity Manager には、デフォルトで CA Identity Manager 環境用のネイティブ認証が含まれます。 CA Identity Manager 管理者は、CA Identity Manager 環境にログインするために、有効なユーザ名およびパスワードを入力します。 CA Identity Manager は、CA Identity Manager が管理するユーザ ストアに対する名前およびパスワードを認証します。

CA Identity Manager が CASiteMinder と統合される場合、CA Identity Manager は、環境を保護するために CA SiteMinder 基本認証を使用します。 ユーザが CA Identity Manager 環境を作成する場合、ポリシー ドメインおよび認証方式がその環境を保護するために CA SiteMinder で作成されます。

CA Identity Manager が CASiteMinder と統合される場合は、管理コンソールを保護するために SiteMinder 認証も使用できます。

アクセス ロールおよびタスク

アクセス ロールにより、CA Identity Manager 管理者が CA SiteMinder が保護するアプリケーションで権限を割り当てることができます。 これらのアクセス ロールは、財務アプリケーションでの発注書の生成など、ビジネス アプリケーションでユーザが実行できる単一のアクションを表します。

ディレクトリマッピング

管理者は、管理者の認証に対して使用されるものとは別のユーザ ストアにそのプロファイルが存在するユーザを管理する必要がある場合があります。CA Identity Manager 環境にログインするときに、管理者は、あるディレクトリと使用して認証され、管理者にユーザを管理する権限を与えるために別のディレクトリを使用して認証されます。

CA Identity Manager が CA SiteMinder と統合される場合、認証と認可用に別のディレクトリを使用するように CA Identity Manager 環境を設定できます。

異なるユーザ セットのスキン

スキンにより、ユーザ コンソールの外観が変更されます。 CA Identity Manager が CASiteMinder と統合される場合、異なるユーザ セットが異なるスキンを参照できるようになります。 この変更を実行するには、スキンをユーザのセットと関連付けるために SiteMinder レスポンスを使用します。 レスポンスは、ユーザのセットに関連付けられる、ポリシーのルールと組み合わされます。 ルールが実行される場合、ユーザ コンソールを構築するために、スキンに関する情報を CA Identity Manager に渡すようにレスポンスをトリガします。

注: 詳細については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

ローカライズされた環境のロケール基本設定

CA Identity Manager が CASiteMinder と統合される場合、imlanguage HTTP ヘッダを使用して、ユーザにロケール基本設定を定義できます。SiteMinder ポリシー サーバで、SiteMinder レスポンス内でこのヘッダを設定し、ヘッダの値としてユーザ属性を指定します。 この imlanguage ヘッダはユーザに対する優先度が最も高いロケール基本設定として機能します。

注: 詳細については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

詳細情報:

カスタム認証方式を使用したユーザ クレデンシャルの収集 (P. 356)

リソースが保護される方法

高度な認証では、ユーザの実装で SiteMinder ポリシー サーバを使用する必要があります。CA Identity Manager Server をホストするアプリケーション サーバは、Web Server とは別のオペレーティング環境上にあります。 サービスを転送するには、Web Server には以下が必要です。

- アプリケーション サーバ ベンダーが提供したプラグイン。
- ユーザ コンソール、自己登録、および忘れたパスワード機能など CA Identity Manager リソースを保護する SiteMinder エージェント。

Web エージェントは、CA Identity Manager リソースをリクエストする ユーザのアクセスを制御します。ユーザが認証され認可されたら、Web エージェントは Web Server がリクエストを処理できるようにします。

Web Server がリクエストを受信するときに、アプリケーション サーバ プラグインは CA Identity Manager Server をホストするアプリケーション サーバにそれを転送します。

Web エージェントは、ユーザと管理者に提供される CA Identity Manager リソースを保護します。

SiteMinder と CA Identity Manager の統合の概要

ポリシー管理者およびアイデンティティ管理者が連携して、 SiteMinder を既存の CA Identity Manager インストールに統合する場合、CA Identity Manager アーキテクチャは拡張され、以下のコンポーネントが含まれます。

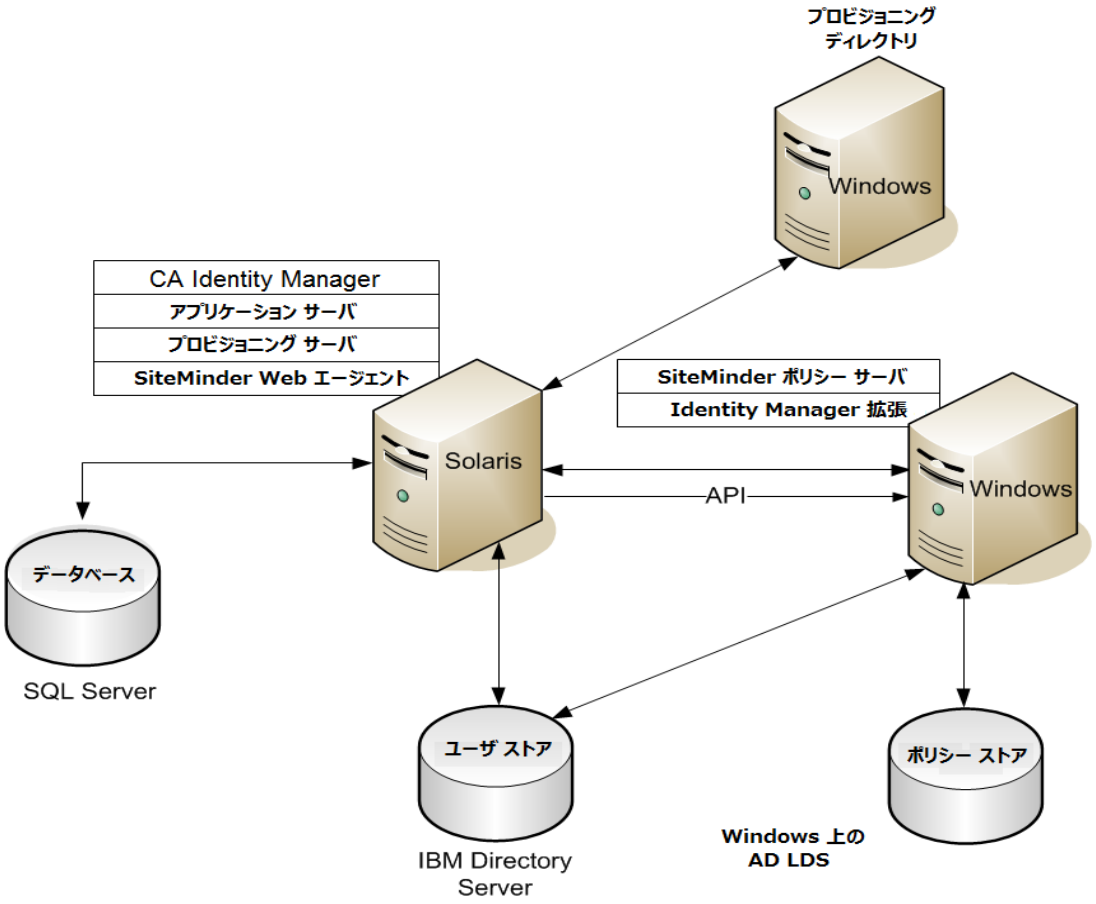
SiteMinder Web エージェント

CA Identity Manager Server を保護します。 この Web エージェントは、CA Identity Manager サーバと共にシステムにインストールされます。

SiteMinder ポリシー サーバ

CA Identity Manager 用の高度な認証および認可を提供します。

以下の図は、SiteMinder ポリシー サーバおよび Web エージェントを含む CA Identity Manager インストールの例です。

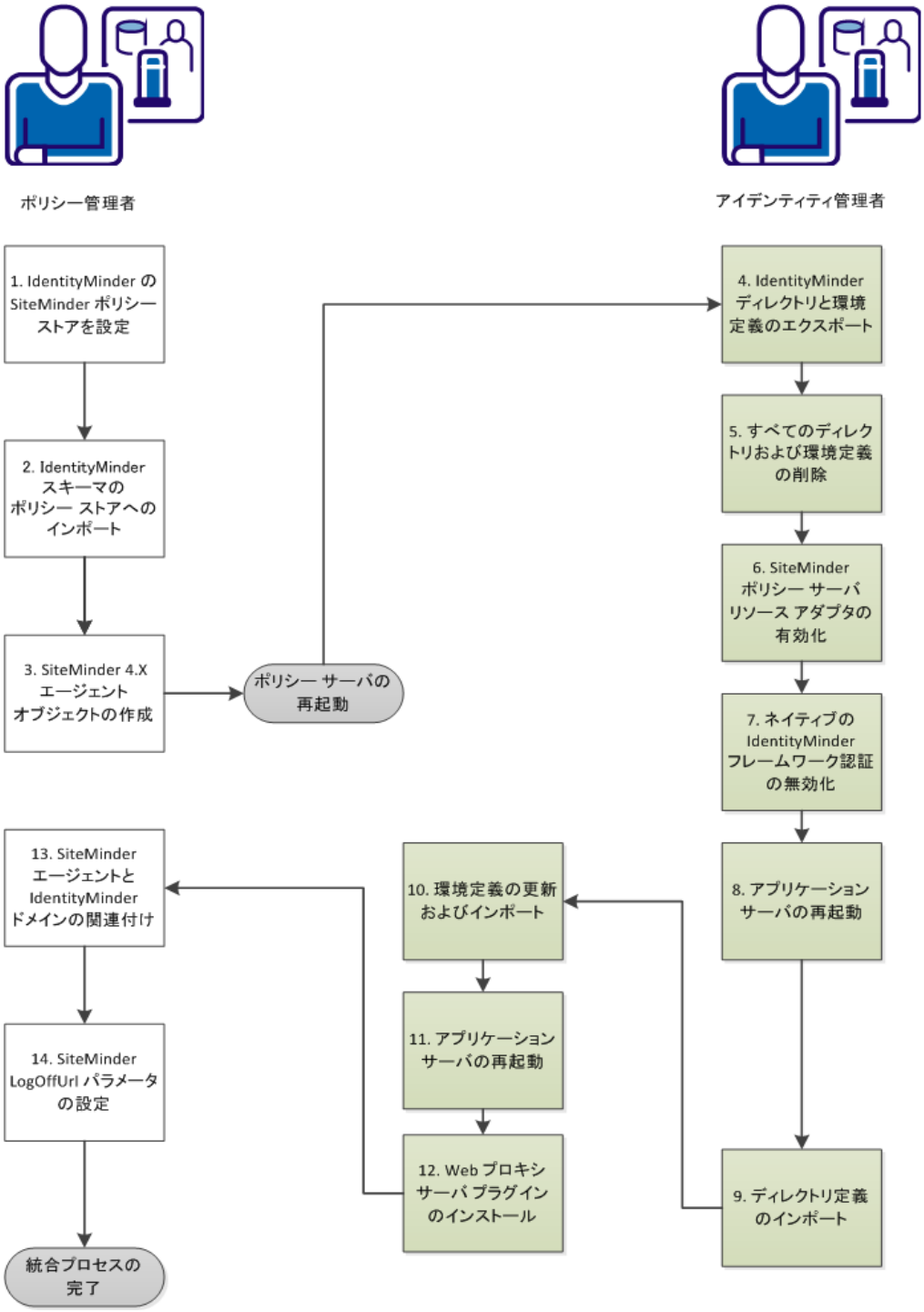


注: これらのコンポーネントは、例のように、さまざまなプラットフォームにインストールされます。ただし、他のプラットフォームを選択することもできます。CA Identity Manager データベースは、Microsoft SQL Server 上にあり、ユーザ ストアは IBM Directory Server 上にあります。SiteMinder ポリシー ストアは Windows 上の AD LDS にあります。

このプロセスを完了するには 2 つのロール（CA Identity Manager アイデンティティ管理者および SiteMinder ポリシー管理者）が必要です。一部の組織では、1 人で両方のロールを割り当てられる場合があります。 2 人で行う場合は、緊密な連携をとって、このシナリオの手順を完了する必要があります。 ポリシー管理者はこのプロセスを開始して終了し、アイデンティティ管理者は、中間のすべての手順を実行します。

重要: リリース 12.5 SP7 を使用して開始する CA Identity Manager のインストールの場合、Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files（JCE ライブラリ）が必要です。 Oracle の Web サイトからこれらのライブラリをダウンロードします。 それらを次のフォルダにロードします：
<Java_path>¥<jdk_version>¥jre¥lib¥security¥.

以下の図は、SiteMinder を CA Identity Manager に統合する完全なプロセスを示しています。



次の手順に従ってください：

1. CA Identity Manager の SiteMinder ポリシー ストアを設定します。（P. 305）
2. ポリシー サーバに CA Identity Manager スキーマをインポートします。（P. 312）
3. SiteMinder 4.X エージェント オブジェクトを作成します。（P. 312）
4. CA Identity Manager ディレクトリおよび環境をエクスポートします。（P. 314）
5. ディレクトリおよび環境定義をすべて削除します。（P. 315）
6. SiteMinder ポリシー サーバ リソース アダプタを有効にします。（P. 316）
7. ネイティブ CA Identity Manager フレームワーク認証フィルタを無効にします。（P. 317）
8. アプリケーション サーバを再起動します。（P. 318）
9. SiteMinder データ ソースを設定します。（P. 318）
10. ディレクトリ定義をインポートします。（P. 319）
11. 環境定義を更新およびインポートします。（P. 320）
12. アプリケーション サーバを再起動します。（P. 318）
13. Web プロキシ サーバ プラグインをインストールします。（P. 320）
14. CA Identity Manager ドメインと SiteMinder エージェントを関連付けます。（P. 341）
15. SiteMinder LogOffUrl パラメータを設定します。（P. 342）

CA Identity Manager の SiteMinder ポリシー ストアの設定

ポリシー管理者として、ポリシー ストアに IMS スキーマを追加する SQL スクリプトまたは LDAP スキーマ テキストにアクセスするため、CA Identity Manager 管理ツールを使用します。アイデンティティ管理者はこれらのツールを［管理ツール］フォルダにインストールしています。ポリシー ストアを設定するには、以下の*いずれか*の手順に従います。

リレーショナル データベースの設定 (P. 305)

Sun Java Systems Directory Server または IBM Directory Server の設定 (P. 306)

Microsoft Active Directory の設定 (P. 307)

Microsoft ADAM の設定 (P. 308)

CA Directory Server の設定 (P. 309)

Novell eDirectory Server の設定 (P. 310)

Oracle Internet Directory （OID） の設定 (P. 311)

リレーショナル データベースの設定

設定の後に、SiteMinder ポリシー ストアとしてリレーショナル データベースを使用できます。

次の手順に従ってください:

1. サポートされている SiteMinder ポリシー ストアとしてデータベースを設定します。

   注: 設定手順については、SiteMinder の「ポリシー サーバ インストール ガイド」を参照してください。

2. データベース用の適切なスクリプトを実行します。

   - **SQL：** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas¥MicrosoftSQLServer¥ims8_mssql_ps.sql
   - **Oracle：** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   上記のパスはデフォルトのインストール場所です。 ユーザのインストールの場所は異なる場合があります。

Sun Java Systems Directory Server または IBM Directory Server の設定

Java または IBM のディレクトリ サーバを設定するには、適切なスキーマ ファイルを適用します。

次の手順に従ってください:

1. サポートされている SiteMinder ポリシー ストアとしてディレクトリを設定します。

   注: 設定の詳細については、「*CA SiteMinder Policy Server Installation Guide*」を参照してください。

2. ディレクトリに適切な LDIF スキーマ ファイルを追加します。 Windows のデフォルトの LDIF ファイルの場所は C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas です。

   ユーザのディレクトリに以下のスキーマ ファイルを追加：

   - **IBM Directory Server：**

     IBMDirectoryServer¥V3.identityminder8

   - **Sun Java Systems Directory Server （iPlanet） ：**

     SunJavaSystemDirectoryServer¥sundirectory_ims8.ldif

Microsoft Active Directory の設定

Microsoft Active Directory ポリシー ストアを設定するには、activedirectory_ims8.ldif スクリプトを適用します。

次の手順に従ってください:

1. サポートされている SiteMinder ポリシー ストアとしてディレクトリを設定します。

   注: 設定の詳細については、「*CA SiteMinder Policy Server Installation Guide*」を参照してください。

2. 以下のように activedirectory_ims8.ldif スキーマ ファイルを変更します。

   a. テキスト エディタで、activedirectory_ims8.ldif ファイルを開きます。Windows のデフォルトの場所は以下のとおりです。

      C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas¥MicrosoftActiveDirectory

   b. {root} のすべてのインスタンスをディレクトリのルート組織で置き換えます。

      ルート組織は、ポリシー サーバ管理コンソールでポリシー ストアを設定したときに指定したルート組織に一致する必要があります。

      たとえば、root が dc=myorg,dc=com である場合、以下のように置き換えます。
      dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root} を dn: CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com で置き換えます。

   c. ファイルを保存します。

3. ユーザのディレクトリに対してマニュアルで説明されるように、スキーマ ファイルを追加します。

Microsoft ADAM の設定

Microsoft ADAM ポリシー ストアを設定するには、adam_ims8.ldif スクリプトを適用します。

次の手順に従ってください:

1. サポートされている SiteMinder ポリシー ストアとしてディレクトリを設定します。

   注: 設定の詳細については、「*CA SiteMinder Policy Server Installation Guide*」を参照してください。

   CN 値（guid）をメモしてください。

2. 以下のように adam_ims8.ldif スキーマ ファイルを変更します。

   a. テキスト エディタで adam_ims8.ldif¥.ldif ファイルを開きます。 Windows のデフォルトの場所は以下のとおりです。

      C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas¥MicrosoftActiveDirectory

   b. すべての cn={guid} 参照を手順 1 で SiteMinder ポリシー ストアを設定したときに検出した文字列で置き換えます。

      たとえば、guid 文字列が CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8} である場合、すべての cn={guid} 参照を CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8} で置き換えます。

   c. ファイルを保存します。

3. ユーザのディレクトリに対してマニュアルで説明されるように、スキーマ ファイルを追加します。

CA Directory Server の設定

CA Directory Server を設定するには、カスタム スキーマ ファイルを作成します。以下の手順で、*dxserver_home* は CA Directory がインストールされているディレクトリです。 Windows 上のデフォルトのこのファイルのソースの場所は C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas¥eTrustDirectory です。

次の手順に従ってください:

1. サポートされている SiteMinder ポリシー ストアとしてディレクトリを設定します。

   注: 設定の詳細については、「*CA SiteMinder Policy Server Installation Guide*」を参照してください。

2. etrust_ims8.dxc to *dxserver_home*¥config¥schema をコピーします。

3. 以下のようにカスタム スキーマ設定ファイルを作成します。

   a. *dxserver_home*¥config¥schema¥default.dxg を *dxserver_home*¥config¥schema¥*company_name*-schema.dxg へコピーします。

   b. ファイルの下部に以下の行を追加することにより、*dxserver_home*¥config¥schema¥*company_name*-schema.dxg ファイルを編集します。

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. ファイルの末尾に etrust_ims_schema.txt のコンテンツを追加することにより、*dxserver_home*¥bin¥schema.txt ファイルを編集します。Windows 上のデフォルトのこのファイルのソースの場所は C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas¥eTrustDirectory です。

5. 以下のようにカスタム制限設定ファイルを作成します。

   a. *dxserver_home*¥config¥limits¥default.dxc を *dxserver_home*¥config¥limits¥*company_name*-limits.dxc にコピーします。

   b. *dxserver_home*¥config¥limits¥*company_name*-limits.dxc ファイルでデフォルト サイズ制限を以下のように 5000 に増やします。

   ```
   set max-op-size=5000
   ```

   注: CA Directory のアップグレードにより、limits.dxc ファイルが上書きされます。 そのため、アップグレードが完了した後で、max-op-size を 5000 にリセットしてください。

6. *dxserver_home*¥config¥servers¥*dsa_name*.dxi を以下のように編集します。

```
# schema
source "company_name-schema.dxg";

#service limits
source "company_name-limits.dxc";
```

ここで *dsa_name* はカスタマイズされた設定ファイルを使用した、DSA の名前です。

7. dxsyntax ユーティリティを実行します。
8. スキーマの変更を有効にするために、dsa ユーザとして以下のように DSA を停止および再起動します。

```
dxserver stop dsa_name
dxserver start dsa_name
```

Novell eDirectory Server の設定

Novell eDirectory Server ポリシー ストアを設定するには、novell_ims8.ldif スクリプトを適用します。

次の手順に従ってください:

1. サポートされている SiteMinder ポリシー ストアとしてディレクトリを設定します。

注: 設定の詳細については、「*CA SiteMinder Policy Server Installation Guide*」を参照してください。

2. ポリシー サーバがインストールされているシステム上のコマンド ウィンドウに以下の情報を入力することにより、Novell eDirectory Server 用の NCPServer の識別名（DN）を検索します。

```
ldapsearch -h hostname -p port -b container -s sub
-D admin_login -w password objectClass=ncpServer dn
```

例：

```
ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D
"cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn
```

3. novell_ims8.ldif ファイルを開きます。
4. 手順 2 で検索した値ですべての NCPServer 変数を置き換えます。

Windows 上の novell_ims8.ldif のデフォルトの場所は次のとおりです。

C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥policystore-schemas¥NovelleDirectory

たとえば、DN 値が cn=servername、cn=servername の場合、*NCPServer* のすべてのインスタンスを cn=servername、o=servercontainer で置き換えます。

5. eDirectory Server を novell_ims8.ldif ファイルで更新します。

   手順については、Novell eDirectory のマニュアルを参照してください。

Oracle Internet Directory（OID）の設定

Oracle Internet Directory を設定するには、oracleoid ldif ファイルを更新します。

次の手順に従ってください:

1. サポートされている SiteMinder ポリシー ストアとしてディレクトリを設定します。

   注: 設定の詳細については、「*CA SiteMinder Policy Server Installation Guide*」を参照してください。

2. oracleoid_ims8.ldif ファイルで Oracle Internet Directory Server を更新します。Window 上のこのファイルのデフォルトのインストール場所は以下のとおりです。

   install_path¥policystore-schemas¥OracleOID¥

   手順については、 Oracle Internet Directory のマニュアルを参照してください。

ポリシー ストアの確認

ポリシー ストアを確認するには、以下の点を確認します。

- ユーザのポリシー サーバ ログには、以下のコードから始まる警告のセクションが含まれません。

  `*** IMS NO SCHEMA BEGIN`

  ユーザが SiteMinder ポリシー サーバの拡張機能をインストールしているが、ポリシー ストア スキーマを拡張していない場合にのみ、この警告が表示されます。

- CA Identity Manager オブジェクトはポリシー ストア データベースまたはディレクトリに存在します。 CA Identity Manager オブジェクトは ims プレフィックスから始まります。

ポリシー ストアへの CA Identity Manager スキーマのインポート

ポリシー管理者はポリシー ストアに CA Identity Manager スキーマをインポートします。 このタスクにより CA Identity Manager はポリシー オブジェクトを作成、更新、および削除できます。 例にはディレクトリ オブジェクト、ドメイン、レルム、ルール、ポリシー、およびアクセス ロールとタスクを有効にするポリシー オブジェクトが含まれます。

次の手順に従ってください:

1. SiteMinder ポリシー サーバで、ポリシー サーバ サービスをシャットダウンします。
2. 使用しているバージョンの CA Identity Manager インストーラを実行します。
3. どのコンポーネントをインストールするかを尋ねるメッセージが表示されたら、インストールするコンポーネントをインストールするかを尋ねられたとき、SiteMinder 用の拡張機能を選択します（SiteMinder がローカルにインストールされている場合）。
4. 続行する前に、必ずポリシー サーバ サービスを再起動してください。

SiteMinder4.x エージェント オブジェクトの作成

ポリシー管理者は SiteMinder 4.x Web エージェントを作成します。このタスクは、SiteMinder と CA Identity Manager の間の通信を有効にします。 アイデンティティ管理者は CA Identity Manager 設定中にこのエージェントを参照します。

次の手順に従ってください:

1. SiteMinder 管理 UI にログオンします。

   管理者権限に関連するタブが表示されます。
2. ［インフラストラクチャ］-［エージェント］-［エージェント］-［エージェントの作成］をクリックします。

   ［エージェントの作成］ダイアログ ボックスが表示されます。
3. ［エージェント タイプの新しいオブジェクトの作成］を選択して、［OK］をクリックします。

   ［エージェントの作成］ダイアログ ボックスが表示されます。
4. 名前および説明（オプション）を入力します。

   注: 対応する SharePoint 接続ウィザードと容易に関連付けることができる名前を使用します。

5. ［SiteMinder］を選択します。
6. ドロップダウン リストから［Web エージェント］を選択します。
7. 以下の手順で 4.x 機能を有効にします。
   a. ［4.x エージェントをサポートする］チェック ボックスをオンにします。

      信頼設定フィールドが表示されます。
   b. 以下のフィールドを入力することにより信頼設定を追加します。

      IP アドレス

      ポリシー サーバの IP アドレスを指定します。

      共有秘密キー

      4.x Agent オブジェクトと関連付けられるパスワードを指定します。 SharePoint 接続ウィザードもこのパスワードが必要です。

      秘密キーの確認入力

      4.x Agent オブジェクトと関連付けられるパスワードを確認します。 SharePoint 接続ウィザードもこのパスワードの確認が必要です。
8. ［サブミット］をクリックします。

   エージェント オブジェクトの作成タスクが処理に対してサブミットされ、確認メッセージが表示されます。

CA Identity Manager ディレクトリおよび環境のエクスポート

統合プロセスにより、現在の環境およびディレクトリ定義のすべてが削除されます。 この情報が保持されることを確認するため、アイデンティティ管理者は CA Identity Manager 管理コンソールを使用して、環境をエクスポートします。ユーザが統合を完了した後で、これらの定義はディレクトリと環境をリストアします。

次の手順に従ってください:

1. CA Identity Manager 管理コンソールを開きます。
2. ［Directories］をクリックします。
3. リストの最初のディレクトリをクリックし、［Export］をクリックします。
4. directory xml ファイルを保存してアーカイブします。
5. 残りのディレクトリにこのプロセスを繰り返します。
6. ［Home］をクリックし、［Environments］をクリックします。
7. 最初の環境を選択します。
8. ［Export］をクリックします。
9. 残りの環境にこのプロセスを繰り返します。

   注: このプロセスは、各環境に対して数分かかる場合があります。

すべてのディレクトリおよび環境定義の削除

SiteMinder で CA Identity Manager を保護するように準備するために、アイデンティティ管理者は CA Identity Manager 管理コンソールを使用して、ディレクトリおよび環境定義を削除します。

次の手順に従ってください:

1. CA Identity Manager 管理コンソールを開きます。
2. ［Environments］をクリックします。
3. 最初の環境を選択します。
4. ［Delete］をクリックします。
5. 残りの環境のそれぞれにこのプロセスを繰り返します。

   注: 環境がディレクトリを参照するため、ユーザのディレクトリを削除する前に環境を削除します。
6. ［Directories］セクションに移動します。
7. リスト表示されたディレクトリをすべて選択します。
8. ［Delete］をクリックします。

SiteMinder ポリシー サーバ リソース アダプタの有効化

アイデンティティ管理者は SiteMinder ポリシー サーバ リソース アダプタを有効にします。 アダプタの目的は SMSESSION cookie を検証することです。 検証の後で、SiteMinder はユーザ コンテキストを作成します。

次の手順に従ってください:

1. CA Identity Manager を実行しているアプリケーション サーバ上の iam_im.ear m.ear の内にある ¥policysever.rar¥META-INF フォルダに移動します。
2. エディタで ra.xml ファイルを開きます。
3. Enabled config-property を検索し、以下の例のように config-property-value を true に変更します。

```
        <config-property-name>validateSMHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. ConnectionURL プロパティを探し、SiteMinder ポリシー サーバのホスト名を提供します。 完全修飾ドメイン名（FQDN）を使用します。
5. UserName プロパティを探し、SiteMinder との通信に使用するアカウントを指定します。 SiteMinder はこのアカウントのデフォルト値です。
6. AdminSecret プロパティを探します。 暗号化されたパスワードを提供します。エクスポートした directory.xml ファイルからパスワードをコピーし、それを ra.xml に貼り付けます。共通のパスワードがあるかどうか分からない場合は、CA Identity Manager パスワード ツールを使用して、パスワードを暗号化します。
7. ra.xml ファイルに暗号化されたパスワードを貼り付けます。
8. ポリシー管理者が SiteMinder 設定中に作成した 4.x エージェント名を指定します。
9. 暗号化されたパスワードを指定します。 必要な場合は、パスワード ツールを使用して、パスワードを暗号化します。
10. ra.xml ファイルへの変更を保存します。

SiteMinder ポリシー サーバ リソース アダプタが有効になります。

詳細情報:

SiteMinder パスワードまたは共有シークレットの編集 (P. 377)

ネイティブ CA Identity Manager フレームワーク認証フィルタの無効化

SiteMinder アダプタを設定すると、フレームワーク認証フィルタは必要なくなります。 アイデンティティ管理者はフィルタを無効にすることができます。

次の手順に従ってください:

1. iam_im.ear 下の ¥user_console.war¥WEB-INF フォルダに web.xml ファイルを置いて、編集します。
2. FrameworkAuthFilter を探し、Enable init-param の値を false に切り替えます。

   CA Identity Manager r12.5 SP7 以降を使用している場合は、Java Cryptographic Extension Unlimited Strength Jurisdiction Policy Files（JCE）が CA Identity Manager 環境の ¥<Java_path>¥<jdk_version>¥jre¥lib¥security にダウンロードされていることを確認します。 これらのファイルにより、CA Identity Manager は SiteMinder に接続できるようになります。

   JCE ライブラリがインストールされている場合、CA Identity Manager のアプリケーションの起動中に以下のメッセージを参照します。

   ```
   2012-07-06 11:23:56,079 WARN  [ims.default] (main) * Startup Step 2 : Attempting to start PolicyServerService
   2012-07-06 11:23:56,081 WARN  [ims.default] (main) Unlimited Strength Java Crypto Extensions enabled: TRUE
   ```

   Otherwise, the value is false for the "Unlimited Strength Java Crypto Extensions enabled" entry. CA Identity Manager はポリシー サーバに接続できません。

アプリケーション サーバの再起動

再起動により、アプリケーション サーバがリフレッシュされます。アイデンティティ管理者は、スイッチが成功し、SiteMinder ポリシー サーバへの適切な接続が存在することを検証します。

次の手順に従ってください:

1. アプリケーション サーバがサービスとして実行されているときに、サービス パネルを使用して CA Identity Manager を再起動します。
2. 接続を検証するには server.log を参照します

SiteMinder 用のデータ ソースの設定

ユーザの CA Identity Manager 環境がそのアイデンティティ ストアに対してリレーショナル データベースを使用する場合、アイデンティティ管理者は SiteMinder ポリシー サーバ上の追加のプロセスを完了する必要があります。SiteMinder は、データベースと通信するためにローカルデータ ソースが必要です。

次の手順に従ってください:

1. Windows サーバの場合、管理ツールの下にある ODBC データ ソース管理コンソールを開きます。
2. ［システム DSN］タブをクリックします。
3. ［追加］をクリックし、ご使用のデータベースに対応する SiteMinder ドライバを選択します。
4. リレーショナル データベース ユーザ ストアを参照するために必要な情報を提供します。
5. 続行する前に、接続性をテストします。

ディレクトリ定義のインポート

環境をインポートする準備をするには、アイデンティティ管理者は、環境が参照するディレクトリをインポートします。 CA Identity Manager にディレクトリ定義をインポートすると、ディレクトリ情報も SiteMinder ポリシー ストアに追加されます。

次の手順に従ってください:

1. CA Identity Manager が実行されていて SiteMinder に接続されていることを確認します。
2. CA Identity Manager 管理コンソールに移動します。
3. ［Directories］をクリックし、次に、［Create or Update from XML］をクリックします。
4. ディレクトリ設定ファイル（directory.xml）を指定します。このファイルは「CA Identity Manager ディレクトリおよび環境のエクスポート（P. 314）」でエクスポートしたファイルです。
5. ［Next］をクリックします。
6. ［Finish］をクリックし、ロード出力を確認します。ディレクトリが CA Identity Manager および SiteMinder にあることを確認します。
7. プロビジョニング ストアおよび残りのディレクトリに対してこれらの手順を繰り返します。
8. ユーザ ディレクトリの作成を検証するために SiteMinder 管理 UI にログインします。

環境定義の更新およびインポート

アイデンティティ管理者は、更新された環境を CA Identity Manager にインポートします。

次の手順に従ってください:

1. ディレクトリのエクスポートと異なり、環境のエクスポートは、zip ファイルの形式です。zip ファイルから *name*.xml ファイルのコピーをドラッグします。
2. *name*.xml ファイルをコピーします。 ImsEnvironment エレメントの最後で、enclosing /> bracket: *agent="idmadmin"* の前に、保護するエージェント（SM 4.x エージェントではない）への参照を挿入します。
3. ファイルを保存して、zip ファイルに貼り付けます。
4. CA Identity Manager 管理コンソールを開き、［Environments］-［Import］をクリックします。
5. 更新された環境 zip ファイルの名前を入力します。
6. ［Finish］をクリックし、インポート出力を確認します。
7. 残りのすべての環境にこのプロセスを繰り返します。
8. アプリケーション サーバを再起動します。

Web プロキシ サーバ プラグインのインストール

どのアプリケーションがインストールされるかに基づいて、アイデンティティ管理者は、Web サーバがアプリケーション サーバへのリクエストを転送するために使用する以下のプラグインのいずれかをインストールします。

- WebSphere（P. 321）
- JBoss（P. 329）
- WebLogic（P. 333）

WebSphere 上へのプロキシ プラグインのインストール

Web エージェントをインストールした Web サーバは、CA Identity Manager サーバをホストするアプリケーション サーバへリクエストを転送します。 ベンダーが提供する Web サーバ プロキシ プラグインはこのサービスを提供します。

ユーザの展開に適用可能な手順を使用して、以下を実行します。

1. IBM HTTP サーバの設定 (P. 321)（すべての Web サーバ）
2. プロキシ プラグインの設定 (P. 322)（すべての Web サーバ）
3. 以下のいずれか：
   - IIS 上の設定の完了 (P. 326)
   - iPlanet または Apache 上の設定の完了 (P. 328)

IBM HTTP サーバの環境設定

すべての Web サーバについて、プロキシ プラグインをインストールし、configurewebserver コマンドを使用します。

次の手順に従ってください:

1. WebSphere Launch Pad からプロキシ プラグインをインストールします。
2. 以下のように、configurewebserver1.bat command コマンドを実行することによって、WebSphere セルに Web サーバを追加します。
   a. テキスト エディタで *websphere_home*¥Plugins¥bin¥configurewebserver1.bat/,sh を編集します。
   b. 以下のように wsadmin.bat/.sh の後にユーザ名とパスワードを追加します。
   ```
   wsadmin.bat -user wsadmin -password password -f
   configureWebserverDefinition.jacl
   ```
   c. configurewebserver1.bat/.sh を実行します。

   注: configurewebserver コマンドの詳細については、IBM WebSphere のマニュアルを参照してください。
3. 「プロキシ プラグインの設定 (P. 322)」の手順に進みます。

プロキシ プラグインの設定

すべての Web サーバについて、WebSphere の GenPluginCfg コマンドを使用して、プラグインを更新します。

次の手順に従ってください:

1. WebSphere がインストールされているシステムにログインします。
2. コマンド ラインから、*websphere_home¥bin* に移動します。ここで、*websphere_home* は WebSphere のインストール場所です。

   例：

   - **Windows の場合：**

     C:¥Program Files¥WebSphere¥AppServer¥profile¥AppSrv01¥bin

   - **UNIX の場合：**

     /*home_dir*/WebSphere/AppServer/profile/AppSrv01/bin

3. GenPluginCfg.bat または GenPluginCfg.sh コマンドを実行します。

   このコマンドを実行すると、以下の場所に plugin-cfg.xml ファイルが生成されます。

   websphere_home¥AppServer¥profiles¥AppSrv01¥config¥cells

4. 以下のいずれかの手順を続行します。

   - IIS 上の設定の完了 (P. 326)
   - iPlanet または Apache 上の設定の完了 (P. 328)

IIS (7.x) 上の設定の完了

この手順を開始する前に、Web サーバ プラグインのバージョン 6.1.0.9 以降を使用していることを確認します。プラグインの以前のバージョンは Windows Server 2008 オペレーティング システムをサポートしません。

次の手順に従ってください：

1. IIS Version 6.0 Management Compatibility コンポーネントを持つ IIS Version 7.x をインストールします。IIS Version 6.0 Management Compatibility コンポーネントはデフォルトではインストールされません。
2. Windows Server 2008 上で Server Manager ウィンドウを表示するには、以下の手順に従います。
   1. ［スタート］-［管理ツール］-［サーバー マネージャ］をクリックします。
   2. ［アクション］-［役割の追加］をクリックし、［次へ］をクリックします。
   3. ［サーバーの役割の選択］ページ上で［Web サーバー (IIS) の役割］を選択し、［次へ］をクリックします。
   4. Windows プロセス起動サービス機能の入力を求めるメッセージが表示されたら、［フィーチャーの追加］-［次へ］をクリックします。
   5. IIS の概要ページで、［次へ］をクリックします。
3. ［役割サービス］ウィンドウが表示されたら、既に選択されているデフォルトのオプションのほかに、以下のオプションが選択されていることを確認します。
   - インターネット インフォメーション サービス： 管理ツール
   - IIS Version 6.0 Management Compatibility： IIS Version 6.0 管理コンソール、IIS Version 6.0 Scripting Tools、IIS Version 6.0 WMI Compatibility、および IIS Metabase compatibility
   - アプリケーション開発： ISAPI Extensions、ISAPI フィルタ
4. 選択したオプションを有効にするには［次へ］をクリックし、インストールを実行するには次のウィンドウで［インストール］をクリックします。
5. インストールが完了したら、［インストールの結果］ウィンドウで［閉じる］をクリックします。
6. コマンド プロンプトを開き、¥Program Files¥IBM¥WebSphere¥AppServer¥profiles¥Dmgr01¥bin に移動します。
7. このコマンドを実行します： GenPluginCfg.bat

   plugin-cfg.xml ファイルが次の場所に生成されます： C:¥Program Files¥IBM¥WebSphere¥AppServer¥profiles¥Dmgr01¥config¥cells

8. たとえば、c:¥ 下に c:¥plugin などのディレクトリを作成します。
9. c:¥plugin ディレクトリに plugin-cfg.xml ファイルをコピーします。
10. c:¥plugin ディレクトリに iiisWASPlugin_http.dll ファイルをコピーします。
11. Windows Server 2008 オペレーティング システムで、［スタート］-［すべてのプログラム］-［管理ツール］-［インターネット インフォメーション サービス (IIS) マネージャ］を選択します。このアクションは IIS アプリケーションを開始し、Web サイト インスタンス用の新しい仮想ディレクトリを作成します。これらの手順は、ユーザが既定の Web サイトを使用していることを前提としています。
12. 既定の Web サイトが参照されるまで、左側のツリーを展開します。
13. 既定のインストールが設定されたディレクトリを作成するには、［既定の Web サイト］-［仮想ディレクトリの追加］ を右クリックします。
14. 仮想ディレクトリの作成ウィザードの［仮想ディレクトリ エイリアス］ウィンドウの ［エイリアス］ フィールドに setPlugins を入力します。
15. ウィザードの［Web サイトのコンテンツのディレクトリ］ウィンドウの ［物理パス］ フィールドの c:¥plugin directory を参照し、 ［OK］をクリックします。
16. ［テストの設定］ボタンをクリックします。 設定テストが失敗する場合、物理ディレクトリの許可を変更できます。 または、［ユーザー名を指定して接続］を選択し、その物理パスのファイルに権限のある Windows ユーザ アカウントとして IIS 接続を可能にします。
17. Web サイトに SsetPlugins 仮想ディレクトリを追加するには ［OK］ をクリックします。
18. ナビゲーション ツリーに作成した setPlugins 仮想ディレクトリを選択します。
19. ［ハンドラ マッピング］-［ハンドラ マッピング］をクリックし、［アクション］パネル上の ［機能のアクセス許可の編集］をクリックします。
20. 選択していない場合は、 ［スクリプト］ および ［実行］を選択します。
21. ［OK］をクリックします。
22. ［IIS マネージャ］ウィンドウに戻り、そのウィンドウの左側のナビゲーション ツリーの［Web サイト］フォルダを展開します。
23. ナビゲーション ツリーの ［既定の Web サイト］を選択します。

24. ISAPI フィルタを追加するには、［既定の Web サイト］プロパティの以下の手順を実行します。
    1. ［SAPI フィルタ］タグをダブルクリックします。
    2. クリックして［フィルタのプロパティの追加と編集］ダイアログ ボックスを開きます。
    3. ［フィルタ名］フィールドに「iisWASPlugin」と入力します。
    4. c:¥plugin¥iisWASPlugin_http.dl ディレクトリにあるプラグイン ファイルを選択するには［参照］をクリックします。
    5. ［フィルタのプロパティの追加と編集］ダイアログ ボックスを閉じるには ［OK］ をクリックします。
25. ナビゲーション ツリーのトップ レベルのサーバ ノードを選択します。
26. ［機能］パネル上 ［ISAPI および CGI の制限］をダブルクリックします。

    ［ISAPI または CGI パス］プロパティに対して指定する値を決定するには、前の手順で選択したのと同じプラグイン ファイルを参照して選択します。 例：c:¥plugin¥iisWASPlugin_http.dll。
27. ［アクション］パネルで ［追加］をクリックします。
28. ［説明］ フィールドに「WASPlugin」と入力して、 ［拡張パスの実行を許可する］を選択し、 ［OK］ をクリックして、 ［ISAPI および CGI の制限］ ダイアログ ボックスを閉じます。
29. 場所 c:¥plugin で新規ファイル plugin-cfg.loc を作成します。 plugin-cfg.loc ファイルで値を設定ファイルの場所に設定します。 デフォルトの場所は C:¥plugin¥plugin-cfg.xml. です。

Web エージェントの更新

IIS 7.x を設定したら、Web エージェントに以下の変更を加えます。

1. アプリケーション プールをクリックし、Classic モードに Default App Pool を変更します。
2. ［サブミット］をクリックします。
3. ISAPI フィルタの優先度リストで、エージェントが、CA Identity Manager によって使用されるアプリケーション サーバ用のプラグインよりも上位になっていることを確認します。
4. IIS Version 7.x および WebSphere Application Server プロファイルを再起動します。

IIS 上の設定の完了

IBM HTTP サーバおよびプロキシ プラグインを設定した後で、プロキシ plugin-cfg.xml が正しい場所にあることを確認し、追加のプラグイン ファイルを設定する手順を実行します。

次の手順に従ってください:

1. 以下のように plugin-cfg.xml をコピーします。
   a. Web エージェントがインストールされているシステムにログインします。
   b. C ドライブの下にスペースなしでフォルダを作成します。例 : C:¥plugin。
   c. C:¥plugin フォルダに plugin-cfg.xml ファイルをコピーします。
2. C:¥plugin フォルダで plugin-cfg.loc という名前のファイルを作成し、そのファイルに以下の行を追加します。

   C:¥plugin¥plugin-cfg.xml
3. www.ibm.com から WebSphere がインストールされているシステムに Websphere Plugin インストーラをダウンロードします。
4. WebSphere Plugin インストーラの場所に移動します。
5. このコマンドを使用することにより iisWASPlugin_http.dll ファイルが生成されます。

   ```
   install is:javahome "c:¥IBM¥WebSphere¥AppServer¥Java
   ```

   ユーザの設定に基づいて表示された質問に答えます。

   ウィザードが終了する場合、iisWASPlugin_http.dll ファイルは C:¥IBM¥WebSphere¥Plugs¥bin フォルダに保存されます。64 ビット サブフォルダの 32 ビットを探します。
6. Web エージェントを持つシステム上の C:¥plugin フォルダに iisWASPlugin_http.dll ファイルをコピーします。
7. 以下のように仮想ディレクトリを作成します。
   a. IIS マネージャを開きます。
   b. ［既定の Web サイト］を右クリックします。
   c. ［新規仮想ディレクトリ］をクリックし、以下の値を提供します。

      エイリアス： sePlugins （大文字と小文字を区別します。）

      パス： c:¥plugin

      アクセス許可： 読み取り + 実行（ISAPI または CGI）

8. 以下の要領で、ISAPI フィルタを追加します。
   a. ［既定の Web サイト］を右クリックします。
   b. ［プロパティ］をクリックします。
   c. ［ISAPI フィルタ］タブで［追加］をクリックします。
   d. 以下の値を提供します。

      フィルタ名： sePlugins

      実行可能ファイル： c:¥plugin¥iisWASPlugin_http.dll
9. 以下のように Web サービス拡張を作成します。
   a. IIS6 Manager で、コンピュータ名を展開します。
   b. Web サービス拡張を作成し、それを［許可］に設定します。

      拡張機能の名前： WASPlugin

      パス： C:¥plugin¥iisWASPlugin_http.dll
   c. それぞれの Web サービス拡張機能を右クリックし、それを許可ステータスに変更します。
10. IIS Web サーバを再起動します。

    マスタ WWW サービスで、WebSphere プラグイン（sePlugin）が SiteMinder Web Agent プラグインの後に表示され、WebSphere プラグインが正常に開始されたことを確認します。

iPlanet または Apache 上の設定の完了

IBM HTTP サーバおよびプロキシ プラグインを設定した後で、proxy plugin-cfg.xml が正しい場所にあることを確認し、Web サーバを再起動します。

次の手順に従ってください:

1. 以下のようにプロキシ プラグインをインストールしたシステムに plugin-cfg.xml をコピーします。

   websphere_home¥AppServer¥profiles¥*server_name*¥config¥cells¥*websphere_cell*¥nodes¥webserver1_node¥servers¥webserver1¥

2. すべての iPlanet Web Servers 上で、WebSphere プラグイン（libns41_http.so）が SiteMinderWeb エージェント プラグイン（NSAPIWebAgent.so）の後にロードされていることを確認します。

3. IPlanet 6.0 Web Servers の *iplanet_home*/https-*instance*/config/magnus.conf で、プラグインの順序を確認します。

4. *iplanet_home*/https-*instance*/config/magnus.conf から *iplanet_home*/https-*instance*/config/obj.conf （IPlanet 5.x Web Serverse）に以下の行をコピーします。

   ```
   Init fn="load-modules" funcs="as_init,as_handler,as_term"
   shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init"
   bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg.xml"
   ```

   AuthTrans fn="SiteMinderAgent" in the obj.conf の後に以下のコードを追加します。

   ```
   Service fn="as_handler"
   ```

5. Apache Web Server 上で、SiteMinder Web エージェント プラグイン（mod2_sm.so）は、WebSphere プラグイン（mod_ibm_app_server_http.so）の前にロードされていることを確認します。 このコマンドは、*apache_home*/config/httpd.conf の Dynamic Shared Object （DSO） Support セクションにあります。

6. Web サーバを再起動します。

JBoss 用のプロキシ プラグインのインストール

SiteMinder Web エージェントが CA Identity Manager リソースのリクエスト認証および認可した後で、Web サーバは CA Identity Manager サーバをホストするアプリケーション サーバへのリクエストを転送します。これらのリクエストを転送するには、SiteMinderWeb エージェントがインストールされたシステムに JK Connector をインストールして設定します。 JK Connector の詳細については、以下の Jakarta Project Web サイトを参照してください。

http://community.jboss.org/wiki/usingmodjk12withjboss

CA Identity Manager 管理ツールには、JK Connector を設定するために使用可能なサンプル設定ファイルが含まれます。 手順については、以下のテーブルに示すディレクトリの readme.txt ファイルを参照してください。

プラットフォーム	場所
Windows システム上の IIS Web サーバ	C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥samples¥ConnectorConfiguration¥windows¥IIS_JBoss*
Solaris システム上の Sun Java System Web サーバ	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss*
Solaris システム上の Apache Web サーバ	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/apache_JBoss*

JBoss アプリケーション プラグイン(IIS 7.x)をインストールおよび設定します。

この手順では、IIS 7.0 で始まる JBoss Apache プラグインの設定について説明します

次の手順に従ってください:

1. ファイル システム上で ISAPI フィルタを展開および更新します。

   C ドライブのルートに ISAPI フォルダを展開します。

2. 解凍されたフォルダにある jakarta.reg ファイルを編集します。

   C:¥ のルートに ISAPI フォルダを配置した場合は、このファイルを変更しないでください。 別のフォルダにそれを配置した場合は、9、11 および 12 行目にそのフォルダを指定します。

3. 変更を保存し、ダブルクリックしてレジストリを更新します。

4. JBoss アプリケーション サーバの場所を指定することにより、workers.properties ファイルを編集します。 ポートとタイプは変更する必要はありません。
5. Windows 2008 上への IIS7 または IIS7.5 のインストール
6. ［システム マネージャ］を開き、IIS ISAPI フィルタおよび ISAPI 拡張機能 がインストールされていることを確認します。
7. ［実行］ウィンドウで inetmgr を開始します。
8. m/c 名を選択し、［ISAPI または CGI の制限］をダブルクリックします。
9. 右側のパネルで［追加］をクリックします。
10. ［ISAPI または CGI 制限の追加］ウィンドウが表示されます。
11. isapi_redirect.dll を選択し、説明として「ISAPI」と入力します。
12. ［拡張パスの実行を許可する］を選択します。
13. ［ISAPI または CGI 制限の追加］ウィンドウで、［OK］をクリックします。
14. ［接続］セクションの［サイト］を展開し、［既定の Web サイト］を選択して、［仮想ディレクトリの追加］を右クリックします。
15. エイリアスに「jakarta」と入力し、物理パスで isap_redirect.dll ファイル（c:¥ajp）の場所を入力します。
16. ［テストの設定］ボタンをクリックします
    - 認証および認可がパスしたら、［OK］をクリックします。
    - 認証が失敗した場合、［ユーザー名を指定して接続］ボタンをクリックします。
17. 特定のユーザを選択し、管理ユーザ名とパスワードを提供します。
18. 再度［テストの設定］ボタンをクリックします。 今回は、その認証がパスします。
19. 左側の［既定の Web サイト］をクリックして、ISAP フィルタをクリックします。
20. 右側のパネルで［追加］をクリックします。
21. 名前を入力し、isapi_redirect.dll ファイルの場所を提供します。
22. ［OK］をクリックします。
23. ［既定の Web サイト］を展開し、jakarta 仮想ディレクトリをクリックします。
24. ハンドラ マッピングをダブルクリックします。
25. ［ISAPI-dll］を選択して［機能のアクセス許可の編集］をクリックします。

26. 権限（読み取り、スクリプト、実行）がすべて選択されていることを確認します。
27. ［OK］をクリックします。

Web エージェントの更新

IIS 7.x を設定したら、Web エージェントに以下の変更を加えます。

1. アプリケーション プールをクリックし、Classic モードに Default App Pool を変更します。
2. ［サブミット］をクリックします。
3. ISAPI フィルタの優先度リストで、エージェントが、CA Identity Manager によって使用されるアプリケーション サーバ用のプラグインよりも上位になっていることを確認します。

JBoss プラグインが設定されます。

JBoss アプリケーション プラグイン（IIS 6.0）をインストールおよび設定します。

この統合は、CA Identity Manager に到達する前に、SiteMinder がユーザを認証および認可していることを前提とします。 ユーザは CA Identity Manager に到達する前に SMSESSION クッキーがある必要があります。 SiteMinder Web エージェントによって保護されたアプリケーション プラグイン（プロキシ リダイレクト）を使用します。 この設定によって、ユーザは SiteMinder によって認証され、SMSESSION クッキーが作成された後で、CA Identity Manager にリダイレクトされます。

この手順は、IIS 6.0 用の JBoss Apache プラグインの展開および設定向けです。

次の手順に従ってください:

1. File System 上で ISAPI フィルタを展開および更新します。

   必ず C ドライブのルートに ISAPI フォルダを展開します。
2. 解凍されたフォルダにある jakarta.reg ファイルを編集します。

   C:¥ のルートに ISAPI フォルダを配置した場合は、このファイルを変更しないでください。 別のフォルダにそれを配置する場合は、9、11 および 12 行名にそのフォルダを指定します。
3. 変更を保存し、ダブルクリックしてレジストリを更新します。
4. JBoss アプリケーション サーバの場所を指定することにより、workers.properties ファイルを編集します。 ポートとタイプは変更する必要はありません。
5. IIS 上に ISAPI フィルタを展開します。
6. 管理ツールからのインターネット Information Services Manager を開きます。

7. ［既定の Web サイト］が表示されるまでレベルを拡張します。右クリックし、［新規］（仮想ディレクトリ）を選択します。
8. エイリアスとして *jakarta* を入力します。
9. ISAPI プラグインをインストールしているパスを参照します。
10. 読み取り、実行スクリプト（ASP など）および 実行 （ISAPI アプリケーションまたは CGI など）を選択します。
11. ウィザードを続行し完了するには、［次へ］をクリックします。
12. ［既定の Web サイト］を右クリックし、選択したプロパティを右クリックして、［ISAPI フィルタ］タブを選択し、［追加］をクリックします。
13. フィルタ名用の *jakarta* を入力し、次に、isapi_redirect.dll を選択するために参照をクリックします。 ［OK］を 2 回クリックします。
14. IIS 6.0 については、Web Service Extensions 下でこのフィルタを有効にします。
15. ［Web サービス拡張］フォルダを選択します。 ［新しい Web サービス拡張を追加］の左側の青いリンクをクリックします。
16. 名前には「Jakarta-Tomcat」と入力します。 上記と同じ dl に対して［追加］および［参照］をクリックします。 ［OK］をクリックします。 ［拡張の状態を許可済みに設定する］をクリックし、［OK］をクリックします。
17. IIS サーバを再起動します。

プロキシが所定の場所で設定されていれば、IIS によって CA Identity Manager にアクセスできます。 たとえば、ここに、プロキシ設定前後に CA Identity Manager にアクセスするためのリンクがあります。

以前

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

以降

http://smserver.forwardinc/idmmanage http://smserver.forwardinc/idmmanage

注: スラッシュ「/」はプロキシが作動するためにこの URL の最後に必要になる場合があります。 ユーザが管理コンソールに転送されない場合は、プロキシ ログを参照します。

WebLogic でのプロキシ プラグインのインストール

Web エージェントが CA Identity Manager リソースのリクエスト認証および認可した後で、Web サーバは CA Identity Manager サーバをホストするアプリケーション サーバにリクエストを転送します。

1. WebLogic のマニュアルに記載されている手順に従って、WebLogic プロキシ プラグインをインストールします。

   注: IIS ユーザの場合、プロキシ プラグインをインストールするときに、必ずファイル拡張子、およびパス別に proxying を設定してください。 ファイル拡張子による proxying を設定する場合、以下のプロパティを持つ［App Mapping］タブでアプリケーション マッピングを追加します。

   Executable： IISProxy.dll

   Extension： .wlforward

2. 以下のいずれかのセクションの説明に従って CA Identity Manager 用のプロキシ プラグインを設定します。

   - IIS Proxy プラグイン (P. 336)
   - iPlanet Proxy プラグイン (P. 337)
   - Apache Proxy プラグイン (P. 340)

IIS（7.x）用のプロキシ プラグインの設定

以下の手順は、IIS 7.x の WebLogic プロキシ プラグインの展開および設定を示しています。

注: これらの手順は 32 ビット オペレーティング環境向けです。 同じ手順は 64 ビット オペレーティング環境に適用されます。 installation .dll ファイルの場所は異なります。

- %WL_HOME%server¥plugin¥win¥32¥
- %WL_HOME%server¥plugin¥win¥64¥

次の手順に従ってください:

1. IIS7 に Web エージェントをインストールして設定します。
2. 'C' ドライブで「プラグイン」という名前でフォルダを作成します。
3. プラグイン フォルダに以下のファイルをコピーします。
   - lisforward.dll
   - lisproxy.dll
   - iisproxy.ini

   ¥¥lodimmaple.ca.com¥RegressionHarness¥thirdparty¥weblogic¥Weblogic_Proxy_Files_IIS7 でこれらのファイルを検索できます。

4. IIS7 上にアプリケーション開発および管理ツール ロール サービスをインストールします。
5. Inet Manager を開き、［既定の Web サイト］を選択します。
6. ［ハンドラ マッピング］をクリックします。
7. ［静的ファイル］をダブルクリックし、要求パスを *.* に変更します。
8. ［要求の制限］ボタンをクリックします。
9. ［マップ］タブの［要求のマップ先が次の場合のみハンドラーを呼び出す:］で［ファイルまたはフォルダー］を選択します。
10. ［ハンドラ マッピング］ダイアログ ボックスで、右側のサイド メニュー オプションで［スクリプト マップの追加］をクリックします。 以下の値を入力します。
    - 要求パス： *.cgi
    - Executable： iisProxy.dll
    - 名前： プロキシ
11. ［要求の制限］ボタンをクリックします。
12. リクエストがマップされる場合にのみ、Invoke ハンドラ をクリアします。
13. この IASPI 拡張の許可に関するプロンプトに［はい］をクリックします。
14. IIS Manager ツリーの ルート ノード（マシン名）をクリックし、ISAPI と CGI の Restrictions をクリックします。
15. ［アクション］ペインで［追加］をクリックし、以下の値を入力します。
    - ISAPI または CGI パス： C:¥plugin¥iisproxy.dll。
    - 説明： Weblogic
    - ［拡張パスの実行を許可する］を選択します。
16. IIS Manager ツリーの ルート ノード（マシン名）をクリックし、［ISAPI と CGI 制限］をクリックします。 オプション［Weblogic］を選択し、右側のペインで［機能設定の編集］をクリックします。
17. ［特定できない ISAPI モジュールを許可する］を選択します。
18. Webagent に対して同じ操作を実行します。
19. ［機能ビュー］の［既定の Web サイト］で、Handler Mappings をダブルクリックします。

20. ［アクション］ペインの［ハンドラ マッピング］で、［スクリプト マップの追加］および以下の値をクリックします。
    - 要求パス： .jsp
    - Executable： iisproxy.dll
    - 名前： JSP 1
21. ［要求の制限］をクリックします。
22. リクエストがファイルにマップされる場合にのみ、［マッピング］タブで、要求がファイルにマップされる場合にのみ起動ハンドラを選択します。
23. ［OK］をクリックします。
24. ［スクリプト マップの追加］および以下の値をクリックします。
    - 要求パス： .do
    - 実行可能ファイル： C:¥plugin¥iisproxy.dll
25. ［要求の制限］をクリックします。 設定は同じ .jsp. です。
26. ［OK］をクリックします。
27. ［スクリプト マップの追加］をクリックし、以下の値を入力します。
    - 要求パス： .wlforward
    - 実行可能ファイル： C:¥plugin¥iisproxy.dll
28. ［要求の制限］をクリックします。 設定は .jsp. と同じものです。
29. ［既定の Web サイト］をクリックし、［既定の Web フィルタ］をクリックし、ISAPI ファイルをダブルクリックします。
30. 右側のペインで［View Order List］をクリックします。
31. リストの 2 番目の場所に実行可能ファイル SiteMinder Agent を配置します。このエントリの後で、Weblogic 実行可能ファイルのみがリストに記載されます。

    注: SiteMinder Agent 実行可能ファイルが Weblogic 実行可能ファイルの後に表示される場合は、MOVE UP アクションを使用して、SiteMinder Agent を移動させます。
32. アプリケーション プールをクリックし、Classic モードに Default App Pool を変更します。

WebLogic プラグインが設定されます。

(WL) IIS 6.0 プロキシ プラグインの設定

この手順は、IIS 6.0.x 用の WebLogic プロキシ プラグインの設定に適用されます。

次の手順に従ってください:

1. Web エージェントがインストールされているシステム上でフォルダを作成します。 例： c:¥weblogic_proxy。
2. CA Identity Manager サーバが実行されているシステムにログインします。
3. このフォルダに移動します： *Weblogic_Home*¥wlserver_11¥server¥plugin
4. 手順 1 で作成された weblogic のプロキシ フォルダに以下のファイルをコピーします。
   - iisforward.dll
   - iisproxy.dll
5. 同じ フォルダで iisproxy という名前のファイルを作成し、以下のコンテンツを含めます。

   ```
   # This file contains initialization name/value pairs
   # for the IIS/WebLogic plug-in.
   WebLogicHost=host-name
   WebLogicPort=7001
   ConnectTimeoutSecs=20
   ConnectRetrySecs=2
   WlForwardPath=/castylesr5.1.1,/iam,/im , /ca/Odata/
   WLLogFile= c:¥weblogic_proxy ¥proxy.log
   DebugConfigInfo=ON
   ```

   host-name を実際のホスト名に置き換えます。
6. IIS マネージャを開始します。
7. Web サイトを展開します。
8. ［既定の Web サイト］を右クリックします。
9. ［プロパティ］を選択します。
10. 以下のようにフィルタを追加します。
    a. ［ISAPI フィルター］をクリックします。
    b. ［追加］をクリックし、以下のようにダイアログ ボックスを完了します。

       フィルタ名： WebLogic

       実行可能ファイル： iisforward.dll のパス

11. iisproxy.dll ファイルの場所を以下のように提供します。
    a. ［ホーム ディレクトリ］をクリックします。
    b. ［設定］をクリックします。
    c. ［追加］をクリックします。
    d. iisproxy.dll ファイルのパスを入力します。
    e. ［拡張子］フィールドに「.jsp」を入力します。
    f. ［ファイルの存在を確認する］オプションをクリアします。
12. .do と .wlforward 拡張子について手順 11 を繰り返します。
13. iisforward.dll の場所に指している wlforward（すべての小文字）用の Web サービス拡張を追加します。

    拡張の状態を許可済みに設定します。
14. それぞれの Web サービス拡張機能を右クリックし、それを許可ステータスに変更します。
15. IIS Web サーバを再起動します。

iPlanet Proxy プラグインの設定

プラグインを設定するには、以下の iPlanet 設定ファイルを変更します。

- magnus.conf
- obj.conf

iPlanet 設定ファイルにはテキストの配置に関する厳しいルールがあります。問題を回避するために、以下の点に注意してください。

- 余分な前後の余白を削除します。余分な余白により iPlanet サーバを起動できない場合があります。
- 1 行に調整可能な文字以上の文字を入力する必要がある場合は、その行の最後に円記号（¥）を配置し、次の行に残りを入力します。 円記号は、以下の行の先頭に最初の行の末尾を直接追加します。 最初の行を終了し、2 番目の行を開始する単語間でスペースが必要な場合は、必ず最初の行の最後（円記号の前）、または 2 番目の行の初めにスペースを 1 つ使用してください。
- 複数行にわたって属性を分割しないでください。

ユーザの iPlanet インスタンス用の iPlanet 設定ファイルは以下の場所にあります。

iplanet_home/https-*instance_name*/config/

ここで、*iplanet_home* は、iPlanet インストールのルート ディレクトリで、*instance_name* は、特定のサーバ設定です。

次の手順に従ってください:

1. *weblogic_home*/server/lib directory から、iPlanet をインストールしたファイル システムに iPlanet Web Server のバージョンに対応する libproxy.so ファイルをコピーします。
2. テキスト エディタで、iPlanet magnus.conf ファイルを変更します。

   iPlanet モジュールとして libproxy.so ファイルをロードするように iPlanet に指示するには、magnus.conf ファイルの先頭に以下の行を追加します。

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"¥
   shlib=path in file system from step 1/libproxy.so
   Init fn="wl_init"
   ```

   例：

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"¥
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   iPlanet が起動するときに、関数 load-modules はロード用の共有ライブラリにタグ付けします。値 wl_proxy および wl_init は、プラグインが実行する機能を識別します。

3. テキスト エディタで、以下のように iPlanet obj.conf ファイルを変更します。

   a. 以下のテキストから始まる最後の行の後で：

      NameTrans fn=....

      以下のサービス ディレクティブを Object name="default" セクションに追加します。

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      注: 既存の サービス ディレクティブに従う行にこのディレクティブを追加できます。

   b. 以下のコードをファイルの終わりに追加します。

      ```
      <Object name="idm" ppath="*/iam/*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      ```

      ここで、*hostname* は、WebLogic をインストールしたシステムのサーバ名とドメインで、*portnumber* は、WebLogic ポート（デフォルトは 7001）です。

      複数の Object エントリを持つ場合があります。

      例：

      ```
      <Object name="idm" ppath="*/iam/*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```

4. iPlanet 設定ファイルを保存します。
5. Web サーバ インスタンスを再起動します。

IM_12.8--Apache プロキシ プラグインの設定

Apache プロキシ プラグインの設定には http.conf ファイルを編集する必要があります。

次の手順に従ってください:

1. Web エージェントを Solaris にインストールした後で Apache の Web サーバを停止し、 mod_wl_20.so ファイルをコピーします。コピー元：

   weblogic_home/server/lib/solaris

   コピー先：

   apache_home/modules

2. http.conf ファイル（*apache_home*/conf にある）を編集し、以下の変更を加えます。

   a. ロード モジュール セクションの下で、以下のコードを追加します。

   ```
   LoadModule weblogic_module     modules/mod_wl_20.so
   ```

   b. Apache サーバ システムの名前でサーバ名を編集します。

   c. ファイルの最後で以下のように If ブロックを追加します。

   ```
   <IfModule mod_weblogic.c>
     WebLogicHost weblogic_server.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
     MatchExpression /ca/Odata
   </IfModule>
   ```

3. http.conf ファイルを保存します。
4. Apache Web サーバを再起動します。

SiteMinder エージェントと CA Identity Manager ドメインの関連付け

ポリシー管理者は CA Identity Manager タスクを完了した後にこのタスクを実行します。 CA Identity Manager に環境をロードしているときに、4.X エージェントを参照します。 SiteMinder ポリシー サーバでドメイン/レルムの作成時にそのエージェントを使用します。このエージェントは SMSESSION Cookie を検証します。ドメイン/レルムを更新し、CA Identity Manager へのアクセスに使用される Web サーバ上にある正常に動作しているエージェントを参照します。 この Web サーバは CA Identity Manager へのアクセス ポイントとして機能し、SMSESSION Cookie を作成します。

次の手順に従ってください:

1. SiteMinder 管理 UI にログインします。
2. ［ポリシー］-［ドメイン］の順に移動します。
3. 使用する環境に合わせてドメインを変更します。
4. ［レルム］タブで、最初にリスト表示されるレルム（XXX_ims_realm）を編集します。
5. プロキシ上のエージェントを検索および選択します。

   注: プロキシ エージェント（Web サーバ エージェント）がない場合は、1 つ作成します。前面の CA Identity Manager に対して Web サーバとプロキシを設定していることを確認します。
6. ［OK］を 2 回クリックし、Public realm XXX_pub_realm に対してこのプロセスを繰り返します。
7. 両方のレルムを更新した後で、［サブミット］をクリックします。
8. エージェントがリフレッシュするのを待機するか、またはプロキシ エージェントが存在する Web サーバを再起動します。

SiteMinder LogOffUrI パラメータの設定

環境に SiteMinder を追加した後で、CA Identity Manager でのログオフは実際に何も機能しません。 再度この機能を有効にするには、プロキシ上のエージェントの Agent Configuration Object （ACO）を更新します。

次の手順に従ってください:

1. SiteMinder 管理 UI にログインします。[インフラストラクチャ]タブをクリックし、[エージェント] - [エージェント設定の展開]をクリックして、[エージェント設定の変更]をクリックします。
2. ACO を探します。 #LogoffUri パラメータを探します。 そのパラメータの左側にある再生ボタン（右に指している矢印）をクリックします。
3. [値]フィールドでの名前からパウンド記号（#）を削除し、/idm/logout.jsp を入力します。
4. [OK]をクリックしてから[サブミット]をクリックし、エージェント設定オブジェクトを更新します。

   次回エージェントがポリシー サーバからその設定を取得したときに、新しい設定が適用されます。

トラブルシューティング

以下のトピックでは、発生する可能性のある共通のエラーについて説明します。可能な場合は、解決策はエラーとペアリングされ、統合して支援することができます。

Windows DLL がありません

症状:

Windows DLL （MSVCP71.dll）がありません

SiteMinder 接続が有効にされた後で、DLL （MSVCP71.dll）が見つからないという Java エラーが JBoss で検出されたことを確認しました。

注: JBoss がサービスとして実行されている場合は、このエラーが表示されない場合があります。 可能な場合は、JBoss をサービスとして実行せずに、ユーザの設定をテストします。

解決方法:

次の手順に従ってください:

1. Windows 上で実行されている場合は、SiteMinder ポリシー サーバに MSVCP71.dll を置きます。
2. ¥Windows¥system32 フォルダにこの DLL （MSVCP71.dll）をコピーします。
3. 正しい場所にこのファイルを配置した後で、OS にそれを登録します。
4. コマンド ウィンドウから、regsvr32 コマンドを実行します。 ファイルがロードされる限り、ok であるはずです。
5. アプリケーション サーバを再起動します。

正しくない SiteMinder ポリシー サーバの場所

症状:

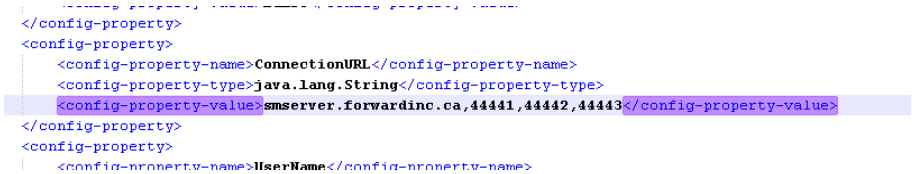
正しくない SiteMinder ポリシー サーバの場所。

解決方法:

ra.xml で正しくない場所が参照され、「ポリシー サーバに接続できません： xxx」というエラーが表示されます。

次の手順に従ってください:

1. ra.xml で提供されるホスト名を確認します。



2. ConnectionURL プロパティで、SiteMinder ポリシー サーバ ホスト名を指定します。 FQN （完全修飾名）を使用します。

正しくない管理者名

症状:

正しくない管理者名

解決方法:

ra.xml で正しくない管理者が参照され、「不明な管理者」というエラーが表示されます。

次の手順に従ってください:

1. ra.xml で UserName プロパティを確認します。

```
    <config-property-value>smserver.forwardinc.ca,44441,44442,44443</co
</config-property>
<config-property>
    <config-property-name>UserName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>SiteMinder</config-property-value>
</config-property>
<!--The property 'password' has been removed.  'AdminSecret' is used in
This is due to the fact that we have added algorithm name padding in th
the algorithm name (for ex, PBES) with its own handlers.  This crashes
```

2. UserName プロパティで、CASiteMinder と通信するために使用されるアカウントを指定します。 たとえば、SiteMinder アカウント（デフォルト値）を使用します。

不正な管理者シークレット

症状:

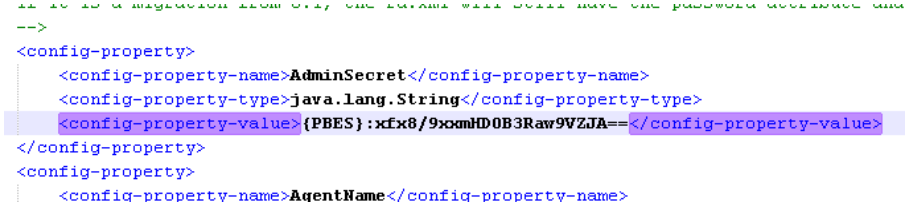
不正な管理者シークレット

解決方法:

ra.xml で不正な管理者シークレットが使用され、「ポリシー サーバに接続できません： 無効な認証情報」というエラーが表示されます。

次の手順に従ってください:

1. ra.xml で AdminSecret プロパティを確認します。



2. AdminSecret プロパティで、UserName プロパティで参照されるユーザ名の暗号化されたパスワードを指定します。

詳細情報:

SiteMinder パスワードまたは共有シークレットの編集 (P. 377)

不正なエージェント名

症状:

不正なエージェント名

解決方法:

ra.xml で不正なエージェント名が使用され、「ポリシー サーバに接続できません： エージェント API の初期化に失敗しました： -1」というエラーが表示されます。

次の手順に従ってください:

1. ra.xml で AgentName プロパティを確認します。

```
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>idmagent</config-property-value>
</config-property>
<config-property>
```

2. SiteMinder 設定の 3 番目の手順中に作成した 4.X エージェント名を指定します。

不正なエージェント シークレット

症状:

不正なエージェント シークレット

解決方法:

ra.xml で不正なエージェント シークレットが使用され、「ポリシー サーバに接続できません： エージェント API の初期化に失敗しました： -1」というエラーと、その前の暗号化ハンドラ エラーが表示されます。

次の手順に従ってください:

1. ra.xml で AgentSecret プロパティを確認します。

```
<config-property>
    <config-property-name>AgentSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
```

2. そのエージェントを作成するときに使用された暗号化されたパスワードを指定します。

詳細情報:

SiteMinder パスワードまたは共有シークレットの編集 (P. 377)

CA Identity Manager 内にユーザ コンテキストはありません

症状:

CA Identity Manager 内にユーザ コンテキストはありません。

ユーザが SMSESSION Cookie のない CA Identity Manager にアクセスしようとする場合、CA Identity Manager はユーザを認証できません。この場合、空の CA Identity Manager UI を表示することを予想できます。

ユーザの環境にワークフローが有効になっている場合、このような問題が発生する可能性があります。

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

解決方法:

少数のものがこれを引き起こす場合があります。しかし、それは通常以下のいずれかです。

- 直接 CA Identity Manager にアクセスしました。
- プロキシの SiteMinder エージェントが無効になります（すなわち、保護されるものが何もない - SMSESSION Cookie が作成されていません）。
- CA Identity Manager 環境の SiteMinder ドメインが誤って設定されています。

最初の 2 つの原因はかなり単純です。 完全に機能的な Web エージェントが有効になっている Web サーバからルーティングしていることを確認します。 ただし、Web サーバを通り抜け、エージェントが有効な場合、ドメインを変更する必要があります。

次の手順に従ってください:

1. SiteMinder 管理 UI にログインします。
2. CA Identity Manager ドメインを探して、それを変更するレイヤをクリックします。 リストの［レルム］タブおよび最初のレルムをクリックします。
3. スラッシュのデフォルトの場所はレルムの下にあります。 それを削除します。
4. このレルムの下のルールをクリックします。

   ルールのデフォルトの効果的なリソースはアスタリスク「*」です。
5. アスタリスクの前にスラッシュ「/」を追加します。

   レルムからルールにスラッシュを移動させました。 この保護は同じですが SiteMinder はそれを別の方法で処理します。

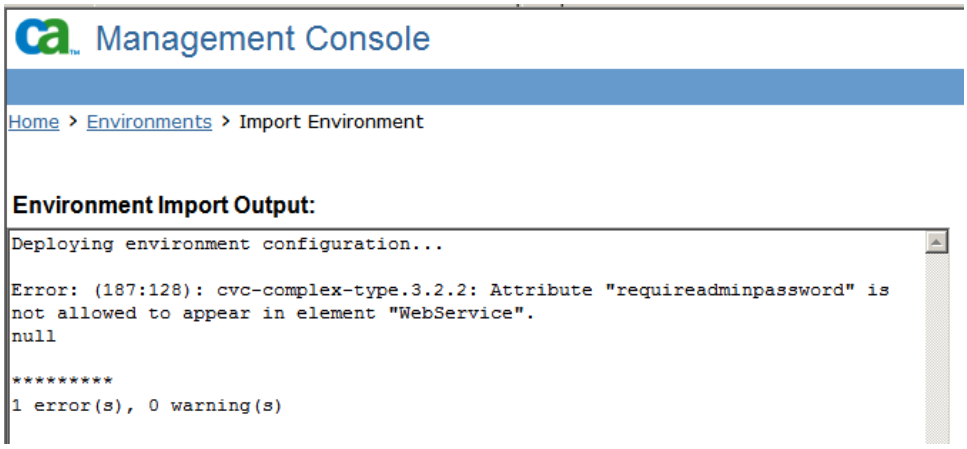
   SiteMinder から CA Identity Manager に正常にログインできます。 適切な保護を検証するには、SiteMinder エージェント ログを確認します。

環境をロード中にエラーが発生しました

症状:

SiteMinder と統合した後で、環境を CA Identity Manager にインポートする場合に、属性 "requireadminpassword" およびエレメント "WebService" に関するエラーが表示されます。

注: この問題は、SiteMinder が展開の一部ではない場合にも発生する場合があります。



解決方法:

このエラーは、環境の部分的な展開を許可します。部分的な展開により CA Identity Manager オブジェクト ストアに空のエレメントを作成できます。 環境 XML のいずれかを訂正して、再インポートします。

次の手順に従ってください:

1. アーカイブされた ZIP ファイルを探して、それを調査します。
2. XXX_environment_settings.xml のコピーを作成します。
3. このファイルを編集し、"WebService" エレメントを探します。
4. タグ "requireadminpassword="false." を削除します。

   注: タグと値を削除します。 値のみを削除しないでください。
5. 変更を保存して、ファイルを ZIP ファイルに戻します。
6. アーカイブされた環境 zip ファイルを再インポートします。

   失敗した試行から作成された環境を削除する必要はありません。 訂正されたファイルを再インポートすると、失敗した試行から作成されたエラーが修正されます。

CA Identity Manager ディレクトリまたは環境を作成できません

症状：

SiteMinder の統合が有効なときに、CA Identity Manager ディレクトリまたは環境を作成できません。

解決方法：

この問題はレジストリにエントリがないことにより発生する場合があります。

以下のレジストリ設定が SiteMinder ポリシー サーバ マシンに存在することを確認します。

- Solaris または Linux の場合：

  以下のエントリが sm.registry に存在することを確認します。
  ImsInstalled=8.0; REG_SZ

- Windows の場合：

  "ImsInstalled=8.0; REG_SZ" の設定が以下の場所に存在することを確認します。
  HKLM¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion

  注: レジストリ パス ¥Netegrity¥SiteMinder¥CurrentVersion が存在しない場合は、それを手動で作成します。

レジストリを変更する場合は、変更を有効にするために必ずポリシー サーバを再起動してください。

重要: レジストリを変更する前に、完全なシステム バックアップを実行します。

ユーザがログインできない

症状:

新規ユーザがクリア テキスト パスワードで環境にログインできません。

解決方法:

以下のデータ分類が、ディレクトリ設定ファイル（directory.xml）のパスワード属性定義に含まれていないことを確認します。

<DataClassification name="AttributeLevelEncrypt"/>

以下のコンポーネントが含まれる環境で、属性レベルの暗号化が有効化されていると、ユーザはログインできません。

- CA SiteMinder および
- リレーショナル データベース

CA Identity Manager エージェント設定を設定する方法

CA Identity Manager が SiteMinder と統合される場合、CA Identity Manager は、SiteMinder ポリシー サーバと通信するためにビルトイン CA Identity Manager エージェントを使用します。パフォーマンスを調整するには、CA Identity Manager エージェント用の以下の接続設定を設定します。

1. 以下のいずれかの操作を実行します。
   - CA Identity Manager が WebLogic または WebSphere のアプリケーション サーバ上で実行されている場合は、アプリケーション サーバのコンソール内の policyserver_rar コネクタ記述子のリソース アダプタを編集します。
   - CA Identity Manager が JBoss アプリケーション サーバ上で実行されている場合、<JBoss_home>¥server¥default¥deploy¥iam_im.ear¥policyserver_rar¥META-INF から policyserver-service.xml を開きます。
2. 以下のように設定します。

   ConnectionMax

   ポリシー サーバへの接続の最大数（たとえば 20）を設定します。

   ConnectionMin

   ポリシー サーバへの接続の最小数（たとえば 2）を設定します。

   ConnectionStep

   エージェント接続がすべて使用中のときに開始する追加の接続数を設定します。

   ConnectionTimeout

   エージェントがタイムアウトになる前に SiteMinder に接続するのを待機するために必要な秒数を指定します。
3. アプリケーション サーバを再起動します。

SiteMinder の高可用性の設定

SiteMinder ポリシー サーバ クラスタを作成している場合、それを負荷分散とフェイルオーバに使用するためにアプリケーション サーバ クラスタを設定できます。

次の手順に従ってください:

1. 以下の場所の ra.xml ファイルを編集します。
   WebSphere:
   WAS_PROFILE/config/cells/*CELL_NAME*/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF
   Jboss:*jboss_home*/server/all/deploy/iam_im.ear/policyserver_rar/META-INF
   WebLogic: *wl_domain*/applications/iam_im.ear/policyserver_rar/META-INF
2. 以下の項目を変更します（後続のセクションで説明されます）。
   - ポリシー サーバの接続設定
   - ポリシー サーバの数
   - クラスタ用の負荷分散またはフェイルオーバの選択内容。
3. クラスタ内の各 CA Identity Manager サーバに対してこれらの手順を繰り返します。
4. 変更を有効にするために、アプリケーション サーバを再起動します。

注: CA Identity Manager ディレクトリまたは環境を作成しているか、ディレクトリまたは環境の設定を変更している場合は、SiteMinder Failover および FailoverServers を false に設定します。そうでないと、ディレクトリ オブジェクトは作成できるが、使用されるときまでにレプリケートできない場合があります。たとえば、Server 1 でディレクトリを作成するとします。その後、Server 2 上でそのディレクトリのオブジェクト ID を使用して、属性を作成します。しかし、2 番目のディレクトリはまだ存在しません。[オブジェクトが見つかりません]エラーを受信します。

ポリシー サーバ接続設定の変更

ポリシー サーバ接続情報は、実稼働環境のプライマリ サーバを反映する必要があります。 この情報は ConnectionURL、SiteMinder 管理者 アカウントのユーザ名とパスワード、およびエージェントの名前および共有シークレットで構成されます。

以下の例では、編集可能な値が大文字で表示されます。

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</co
nfig-
                property-value>
</config-property>

<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

注: 暗号文を必要とする値については、CA Identity Manager パスワード ツールを使用します。 詳細については、「*設定ガイド*」を参照してください。

ポリシー サーバの追加

CA Identity Manager インストール インスタンスにポリシー サーバをさらに追加するには、ra.xml ファイル内の FailoverServers エントリを編集します。

注: FailoverServers エントリにプライマリ ポリシー サーバおよびすべてのフェイルオーバ サーバを含めます。

各ポリシー サーバについては、IP アドレス、および認証、認可、およびアカウント サービス用のポート番号を入力します。以下のように、個別のエントリにはセミコロンを使用します。

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

負荷分散またはフェイルオーバの選択

CA Identity Manager のデフォルト動作は、ConnectionURL と FailoverServers によって識別されるサーバを使用して、ラウンド ロビン負荷分散を使用することです。FailOver を false に設定しておく場合、負荷分散が発生します。

フェイルオーバを選択するには、FailOver を true に設定します。

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

既存の CA Identity Manager 展開からの SiteMinder の削除

このセクションは、既存の CA Identity Manager 環境から CASiteMinder を削除するための詳細な手順を説明します。

次の手順に従ってください:

重要: ［パスワード履歴］情報には移行後にアクセスできません。

1. アプリケーション サーバを停止します。
2. Enabled config-property 値を false に設定することにより ¥iam_im.ear¥policyserver.rar¥META-INF にある ra.xml ファイル内のポリシー サーバを無効にします。
3. ¥iam_im.ear¥User_console.war/WEB-INF にある web.xml ファイルを編集し、FrameworkAuthFilter プロパティを Enabled = true に設定します。

   注: WebSphere については、web.xml ファイルは、*WebSphere_home*/AppServer/profiles/*Profile_name*/config/cells/*Cell_name*/applications/iam_im.ear/deployments/IdentityMinder/user_console.war/WEB-INF にあります。
4. アプリケーション サーバを起動します。
5. （WebSphere のみ） ra.xml ファイルで同じ値を持つ管理コンソール内の policyServer オブジェクトを更新します。

SiteMinder 操作

以下のセクションでは、CA Identity Manager をサポートするためにポリシー ドメインおよび認証方式を含む、SiteMinder 機能を変更する方法について説明します。

カスタム認証方式を使用したユーザ クレデンシャルの収集 (P. 356)

CA Identity Manager 環境にアクセスしようとするユーザのためのクレデンシャルを収集するために、CA Identity Manager が使用するメソッドを変更します。

アクセス ロールの設定 (P. 358)

アプリケーションの機能へのアクセスを提供します。

LogOff URL の設定 (P. 374)

完全なログアウトを実施することにより CA Identity Manager 環境への不正なアクセスを防ぎます。

SiteMinder レルムのエイリアスの更新 (P. 375)

ユーザが環境のエイリアスを変更するときに CA Identity Manager 環境を保護するレルムを更新します。

SiteMinder パスワード (P. 377)

SiteMinder と通信するために CA Identity Manager が使用する管理者アカウントのパスワード、および CA Identity Manager 環境を保護する SiteMinder エージェントの共有シークレットを変更します

CA Identity Manager エージェント設定の設定 (P. 351)

SiteMinder ポリシー サーバと通信する CA Identity Manager エージェントのパフォーマンスを調整します。

認証と認可用の別のディレクトリの使用 (P. 378)

あるディレクトリにプロファイルを持つ管理者が別のディレクトリのユーザを管理できるようにします。

LDAP ディレクトリ操作のパフォーマンスの改善 (P. 380)

同じディレクトリへの複数の接続を開始できるように SiteMinder を設定することにより、ユーザ ストアへの CA Identity Manager リクエストのスループットを向上させます。

カスタム認証方式を使用したユーザ クレデンシャルの収集

SiteMinder は、ユーザ クレデンシャルを収集し、ログイン時にユーザのアイデンティティを決定するために認証方式を使用します。 ユーザが識別されれば、CA Identity Manager はユーザの権限に基づいてあるパーソナライズされたユーザ コンソールを生成します。

CA Identity Manager 環境を保護するために任意の SiteMinder 認証方式も実装できます。

たとえば、ユーザは HTML 形式でクレデンシャルを収集する、Forms Authentication Scheme を実装できます。 HTML フォームを使用すると、会社ロゴ、自己登録や忘れたパスワード ページへのリンクなど、ブランド要素を含むログイン ページを作成できます。

注: 高度な認証方式に関する詳細については、「*CA SiteMinder Policy Server Configuration Guide*」を参照してください。

次の手順に従ってください:

1. 以下のいずれかのインターフェースにログインします。
   - CASiteMinder Web Access Manager r12 の場合は、管理 UI にログインします。
   - CA eTrustSiteMinder6.0 SP5 の場合は、ポリシー サーバ ユーザ インターフェースにログインします。

   注: これらのインターフェースの使用の詳細については、使用している SiteMinder のバージョン用のドキュメントを参照してください。
2. 「*CA SiteMinder Policy Server Configuration Guide*」の説明に従って、認証スキームを作成します。
3. 手順 1 で作成した認証スキームを使用するのに適切な CA Identity Manager 環境を保護するレルムを変更します。

   レルム名の形式は、以下のとおりです。

   *Identity Manager-environment*_ims_realm

   注: パブリック タスクのサポートを設定している場合は、追加のレルム、*Identity Manager-environment*_pub_realm を参照します。 このレルムは、クレデンシャルを提供せずに、不明のユーザが自己登録と忘れたパスワード機能を使用可能な匿名の認証スキームを使用します。 これらのレルムの認証スキームを変更しないでください。

ポリシー ストアへのデータ定義のインポート

SiteMinder ポリシーを使用して、アプリケーション機能へのユーザのアクセスを制御できます。 ポリシー サーバ インストールには、このコントロールを許可するために必要なデータ定義が含まれます。 この場所からの IdmSmObjects.xdd ファイルをインポートします。

siteminder_home¥xps¥dd

siteminder_home はポリシー サーバ インストール パスです。

アクセス ロールを設定する方法

アクセス ロールは、SiteMinder が保護している外部アプリケーション内のユーザ権限の集中的管理を有効にします。 CA Identity Manager 管理者は、CA Identity Manager の外側のアプリケーションへのユーザ アクセスを決定する、CA Identity Manager ユーザ コンソールのロールを作成し割り当てることができます。たとえば、ロール管理者は、財務部アプリケーションへのアクセスを制御するロールをユーザ コンソールに作成し、ヘルプデスク管理者にロールを割り当てる機能を付与することができます。ヘルプデスク管理者は、ユーザ コンソールを通じてロールの割り当てや取り消しを行うことができます。

アクセス ロールは SiteMinder との統合を通じて使用が可能になります。SiteMinder は、ロールをポリシーに関連付けて、どのユーザが保護されたリソースへのアクセスが許可されているかを確認し、保護されたリソースにユーザ固有のロール情報とタスク情報を送信します。

アクセス ロールは、CA Identity Manager および SiteMinder で設定する必要があります。 2 人の管理者が以下のように関係します。

- CA Identity Manager 管理者は CA Identity Manager でアクセス ロールとタスクを作成します。 デフォルトのシステム マネージャおよびアクセス ロール マネージャ ロールには、以下のタスクが含まれます。
- SiteMinder 管理者は、CA SiteMinder 内の System オブジェクトと Domain のオブジェクトを管理します。 SiteMinder 管理者には System スコープが必要です。

  注: 詳細については、「ポリシー サーバ管理ガイド」を参照してください。

以下の手順では、アクセス ロールを作成する手順の概要について説明します。SiteMinder との併用については、アクセス ロールを設定する *前に*、以下の手順を確認してください。

1. CA Identity Manager 管理者は以下のタスクを完了します。
   a. SiteMinder と併用するために、アクセス ロールおよびタスクを有効にします。
   b. アクセス タスクを作成します。
   c. アクセス ロールを作成します。
   d. SiteMinder ロールベースのアクセス制御ポリシーを作成する目的で、SiteMinder 管理者にロールおよびタスク情報を伝達します。

2. SiteMinder 管理者は以下の手順に従うことによりロール ベースのアクセス制御ポリシーを作成します。

   a. ポリシー ドメインへの 1 つ以上の CA Identity Manager 環境と関連付けられるユーザ ディレクトリの割り当て。

   b. 手順 1 でポリシー ドメインとの 1 つ以上の CA Identity Manager 環境の関連付け。

   c. ポリシー ドメイン（それらが存在しない場合）でのレルムとルールの作成。 レルムとルールはアクセス ロール許可がアクセスを付与するリソースに対応している必要があります。

   d. ポリシーの作成とそれらの CA Identity Manager 環境からのロールへのバインド。

   e. （オプション）保護されているリソースに資格情報を提供するレスポンスの指定。

   注: これらの手順中の詳細な手順については、「ポリシー サーバ設定ガイド」を参照します。

詳細情報:

SiteMinder で併用するためのアクセス ロールの有効化 (P. 359)

SiteMinder で併用するためのアクセス ロールの有効化

CASiteMinder を持つアクセス ロールを使用するには、CA Identity Manager は、SiteMinder ポリシー ストアのそれらのアクセス ロールに関連する、CA Identity Manager オブジェクト ストアのオブジェクトをすべてミラーリングします。 SiteMinder とアクセス ロールが併用できるようにするには、CA Identity Manager 管理コンソールでプロパティを設定します。

次の手順に従ってください:

1. 管理コンソールを開きます。
2. ［環境］-［*ユーザ環境*］-［詳細設定］-［その他］を選択します。
3. 以下の情報を提供することによりプロパティを追加します。
   - ［プロパティ］フィールドに、以下のテキストを入力します。

     EnableSMRBAC
   - ［値］フィールドに、以下のテキストを入力します。

     true

4. ［追加］をクリックします。 次に、［保存］をクリックします。

   環境を再起動するよう指示するメッセージが表示されます。

5. ［環境の再起動］をクリックします。

   CA Identity Manager は現在、CA SiteMinder と併用するためにアクセス ロールとタスクをサポートします。

アクセス ロールが CA SiteMinder と併用できない場合、以下の点に注意します：

- CA Identity Manager r8x でアクセス ロールを使用した場合は、CA Identity Manager の現在のバージョンのそれらのアクセス ロールを管理する追加の移行手順を実行します。 詳細については、「アップグレード ガイド」を参照してください。
- SiteMinder のアクセス ロールのサポートを無効にするには、SiteMinder ポリシー ストアから CA Identity Manager アクセス ロールおよびタスク オブジェクトを削除します。次に、［その他のプロパティ］リストから "EnableSMRBAC" プロパティを削除し、環境を再起動します。

管理ロールへのアクセス タスクの追加

デフォルトでは、アクセス タスクは［ロールおよびタスク］タブに表示されません。ログイン ユーザの管理ロールにアクセス タスクを追加する必要があります。

次の手順に従ってください：

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 CA Identity Manager アカウントにログインします。
2. ［ロールおよびタスク］-［管理ロールの変更］をクリックします。
3. ログイン ユーザの管理ロールを選択します。
4. ［タスク］タブ、［カテゴリでフィルタ］フィールドをクリックし、ドロップ ダウンから［ロールおよびタスク］を選択します。
5. ［タスクの追加］ドロップダウンから［アクセス タスクの作成］を選択します。
6. ［サブミット］をクリックします。

アクセス タスクの作成

アクセス タスクは、財務アプリケーションでの発注書の生成など、ビジネス アプリケーションでユーザが実行できる単一のアクションを表します。ユーザがそのアクションを実行するのは、それらがアクセス タスクが含まれるアクセス ロールを割り当てられる場合です。

重要: アクセス タスクを作成するには、ログイン ユーザの管理ロールにアクセス タスクを追加 (P. 360)する必要があります。

次の手順に従ってください:

1. ［ロールおよびタスク］-［アクセス タスク］-［アクセス タスクの作成］を選択します。
2. 以下のいずれかのオプションを選択します。
   - アクセス タスクを作成します。
   - アクセス タスクのコピーを作成します。
3. これらのフィールドに入力します

   名前

   Generate Purchase Order などタスクに割り当てることができる一意の名前。

   タグ

   タスクの一意のタグ。タグは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。

   説明

   タスクの目的に関するオプションのメモ。

   アプリケーション ID

   タスクに関連付けられたアプリケーション名などのアプリケーションの識別子。 アプリケーション ID にはスペースまたは英数字以外の文字を含むことはできません。

   この ID をメモしておいてください。SiteMinder でロールを有効にするときに必要です。
4. アクセス タスクを完了するには、［サブミット］をクリックします。

[アクセス ロール]を作成する方法

アクセス ロールには、アプリケーションで関数へのアクセスを提供するアクセス タスクが含まれます。たとえば、ロールに、ロール メンバが購入アプリケーションで発注し、在庫管理アプリケーションで数量を更新可能なタスクが含まれる場合があります。

アクセス ロールを作成するには、以下の手順に従います。

1. アクセス ロールの作成を開始します。 (P. 362)
2. ［プロファイル］タブでアクセス ロールの基本的なプロパティを定義します。 (P. 362)
3. ロールのアクセス タスクを選択します。 (P. 363)
4. ロールのメンバ ポリシーを定義します。 (P. 364)
5. ロールの管理ポリシーを定義します。 (P. 364)
6. ロールの所有者ルールを定義します。 (P. 365)

アクセス ロールの作成の開始

次の手順に従ってください:

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 CA 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、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

次の手順に従ってください:

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」に進んでください。

ロールのアクセス タスクの選択

［タスク］タブで：

1. このロールに含めるタスクを選択します。 まず、アプリケーション、次にタスクを選択します。 各種アプリケーションからタスクを含むことができます。

   注: 別のロールに必要なタスクがある場合は、別のロールから［コピー タスク］をクリックします。 表示されるリストを編集できます。

   ロールまたはタスクを作成することで、アイテムを追加、編集、削除するアイコンが表示されます。

   現在のアイテムに移動するか、アイテムを選択すると、表示または編集できます。

   JavaScript が無効な場合は、進むボタンを押してドロップダウン リストから選択します。

   前の画面に戻るか、前の選択を元に戻します。

   タスクやロールなどのエレメントを挿入します。

   現在のタスク、またはルールで後続の式を削除します。

   現在のアイテムをリストの上に移動します。

   現在のアイテムをリストの下に移動します。

2. 次のセクション「アクセス ロールの管理ポリシーの定義」に進んでください。

アクセス ロールのメンバ ポリシーの定義

メンバ ポリシーは、ロールのメンバ ルールとスコープ ルールを定義します。1 つのロールに対して複数のポリシーを定義できます。 各ポリシーに対して、メンバ ルールで条件を満たすユーザは、ポリシーで定義されているロールを使用するためのスコープを持ちます。

次の手順に従ってください:

1. ［メンバ］タブを選択します。
2. ［追加］を選択してメンバ ポリシーを定義します。
3. （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。

   メンバ ルールを定義することにより、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。

   注: たとえば、ディレクトリ属性のみを使用するメンバ ポリシーを定義します。例： title=Manager。 ユーザが管理ロールなどユーザ ディレクトリに格納されないオブジェクトを参照するメンバ ポリシーを定義する場合、SiteMinder はその参照を解決できません。
4. ［メンバ ポリシー］が［メンバ］タブに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、マイナス符号アイコンをクリックします。
5. ［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 ボックスを有効にします。

   この機能を有効にすると、［追加アクション］と［削除アクション］を定義できます。 これらのアクションでは、ユーザがロールのメンバとして追加されるか削除されるときに行われる処理が定義されます。

アクセス ロールの管理ポリシーの定義

管理ポリシーは、管理ルール、スコープ ルール、およびロールの管理者権限を定義します。 1 つのロールに対して複数の管理ポリシーを定義できます。 各ポリシーは、管理ルールにスコープおよびそのポリシーに対して定義されている管理者権限があるという条件を満たすかどうか示しています。

次の手順に従ってください:

1. アクセス ロールの［管理者］タブを選択します。
2. ［管理者の管理］オプションを使用する場合は、［管理者は、このロールの管理者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、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。

3. ［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。

   注: ディレクトリ属性のみを使用する管理ポリシーを定義します： 例： title=Manager。 ユーザが管理ロールなどユーザ ディレクトリに格納されないオブジェクトを参照するメンバ ポリシーを定義する場合、SiteMinder はその参照を解決できません。

4. 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、マイナス符号アイコンをクリックします。

5. 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」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

所有者ルールにより、ロールを変更可能なユーザを定義します。 1 つのロールに対して複数の所有者ルールを定義できます。

次の手順に従ってください:

1. アクセス ロールの［所有者］タブを選択します。

2. 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。

   注: ディレクトリ属性のみを使用する所有者ルールを定義します。例： title=Manager。ユーザが管理ロールなどユーザ ディレクトリに格納されないオブジェクトを参照する所有者ポリシーを定義する場合、SiteMinder はその参照を解決できません。

3. ［サブミット］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。

SiteMinder のアクセスロール

SiteMinder の管理者は、ポリシー サーバ ユーザ インターフェースで CA Identity Manager 環境とポリシー ドメインを関連付けて、保護されたリソースへのロールベースのアクセス制御を設定します。管理者はアプリケーションを保護するポリシーを作成し、そのポリシーに 1 つまたは複数のロールを関連付けます。 ロールが関連付けられているユーザは、保護されたアプリケーションへのアクセスが許可されます。

SiteMinder 管理者はユーザがどのようにリソースと対話するか定義するセキュリティ ポリシーにバインドします。 以下のオブジェクトを持つポリシー リンク。

- ユーザおよびグループ

  1 セットのポリシーの影響を受けたユーザを識別します。

- ロール

  CA Identity Manager で権限セットを割り当てられているユーザを識別します。

- ルール

  リソースと、そのリソースに対して許可するか、拒否するリソースおよびアクションを識別します。 リソースは通常 URL、アプリケーション、またはスクリプトです。

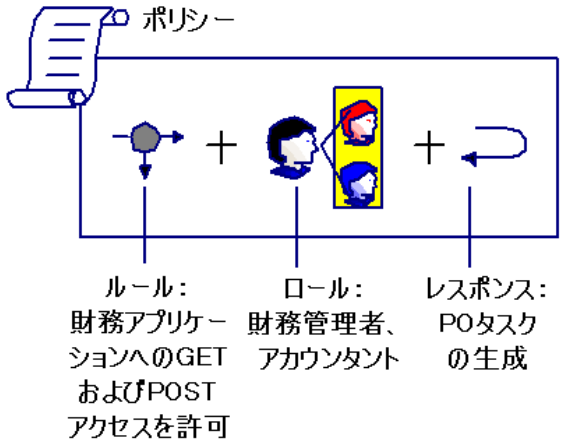
- 応答

  ルールに対する反応を定義します。 ルールが起動されると、SiteMinder エージェントにレスポンスが返されます。

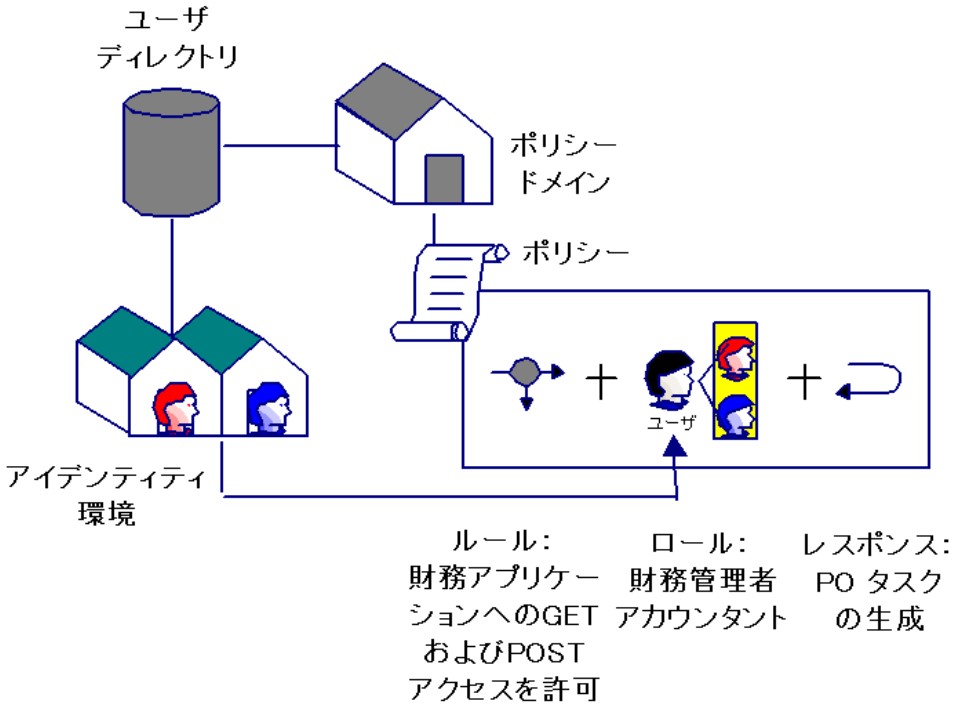
  CA Identity Manager は、SiteMinder レスポンスを使用して、保護されているリソースに特定のタスクおよびロール情報を配信します。

SiteMinder ポリシーをユーザ、またはロールにバインドできます、またはユーザとロールにバインドできます。ユーザまたはロールのメンバが保護されているリソースへのアクセスを試みたとします。SiteMinder はポリシーの情報を使用して、アクセスを付与しレスポンスのトリガになるかどうかを決定します。

以下の図は、ロール ベースのポリシーでのポリシー オブジェクトの関係を示します。



SiteMinder ポリシーはポリシー ドメインで作成されます。それは論理上保護されているリソースにユーザ ディレクトリを結び付けます。以下の図は、ロール ベースのポリシーでのポリシー オブジェクトの関係を示します。



保護されているアプリケーションに対するユーザ権限を付与するには、SiteMinder 管理者はレスポンスを持つアプリケーションのポリシーでルールをペアリングします。 レスポンスには、CA Identity Manager から資格情報を取得する stmndr で 生成されたレスポンス属性が含まれます。

SiteMinder で、保護されているリソースへのアクセスがロール メンバに許可されると、以下のイベントが発生します。

1. ポリシーのルールはペアになったレスポンスのトリガになって、SiteMinder で実行します。
2. ポリシー サーバは、CA Identity Manager からレスポンスに含める資格情報を取得します。
3. ポリシー サーバは Web エージェントにレスポンス属性を渡します。
4. Web エージェントは、資格情報を HTTP ヘッダ変数または cookie としてアプリケーションに提供します。

SiteMinder で生成されるレスポンス属性

CA Identity Manager はアプリケーションに SiteMinder Web エージェント レスポンスを通して資格情報を渡します。 これらのレスポンスにはレスポンス属性に HTTP ヘッダ変数が含まれます。それを使用して、アプリケーションで、ユーザのアクセス権限を決定します。 レスポンスは、ユーザが保護されたリソースと SiteMinder ポリシーに含まれています。それは、ユーザがどのように保護されているリソースとやり取りするのかを決定します。

SiteMinder 管理者は、情報をアプリケーションへ渡す以下の 2 種類のレスポンス属性が含まれるレスポンスを設定できます。

- SM_USER_APPLICATION_ROLES ［: *アプリケーション ID*］ -- ユーザに割り当てられるロールのリストを返します。
- SM_USER_APPLICATION_TASKS ［: *アプリケーション ID*］ -- ユーザが割り当てられるロールに基づいて実行できるタスクのリストを返します。

アプリケーション ID は、ロールとタスクのリクエストされたセットを特定のアプリケーションに制限します。 たとえば、以下のレスポンス属性を作成したとします。

SM_USER_APPLICATION_ROLES:Finance_application

SiteMinder は、Web エージェントへの財務アプリケーションにタスクを含むロールを返し、その後、財務アプリケーションにその情報を返します。

注: 指定する *アプリケーション ID* は、CA Identity Manager の［アクセス タスクの作成］を使用したときに入力した *アプリケーション ID* と一致する必要があります。 タスクがまだ作成されていない場合、ユーザはアプリケーション ID に対してどの名前も選択できますが、それにはスペースまたは数字以外の文字を含むことはできません。

単一のレスポンス属性の複数のアプリケーションからロールとタスクのセットを返すために、カンマ区切りのリストで複数のアプリケーション ID を指定できます。 たとえば、ユーザが財務アプリケーションと購買アプリケーションに含むロールのリストを返すには、以下の方法で指定します。

SM_USER_APPLICATION_ROLES:Finance, Purchasing

SiteMinder でのアクセス ロールを有効にする方法

以下の手順は、SiteMinder がアクセス ロールがアクセスを付与するアプリケーションをすでに保護していると仮定します。 たとえば、SiteMinder がまだ保護していないアプリケーション用のアクセス ロールを作成していると仮定します。そのような場合、SiteMinder マニュアル選択メニューにある以下のいずれかのマニュアルを参照してください。

- SiteMinder6.0 SP5 の場合、「*Policy Design Guide*」を参照してください。
- SiteMinder12.0 SP2 の場合、「ポリシー サーバ設定ガイド」を参照してください。

注: SiteMinder でアクセス ロールを設定するには、SiteMinder 管理 UI の代わりに、ポリシー サーバ ユーザ インターフェース（アプレット ベースのアプリケーション）を使用します。 SiteMinder12 で、このアプレットは SiteMinder Federation Security Services Administrative UI （FSS Administrative UI）という名前が付けられています。 ポリシー サーバ インストーラを使用して、FSS Administrative UI をインストールできます。

SiteMinder でアクセス ロールを有効にするには、以下の概要手順に従います。

1. ポリシー サーバ ユーザ インターフェースで、ユーザ ディレクトリと CA Identity Manager 環境をポリシー ドメインと関連付けます (P. 370)。
2. ポリシー ドメインで、アクセス ロールがアクセスを付与するリソースに対応するレルムおよびルール（それらが存在しない場合）を作成します。

   注: レルムとルールの作成の詳細については、SiteMinder マニュアル選択メニューで以下のいずれかのマニュアルを参照してください。

   - SiteMinder6.0 SP5 の場合、*「Policy Design Guide」*を参照してください。
   - SiteMinder12.0 SP2 の場合、「ポリシー サーバ設定ガイド」を参照してください。
3. 資格情報をリソースへ渡すレスポンスを作成 (P. 371)します。
4. ポリシーを作成し、それを以下のオブジェクトと関連付けます。

   - アクセス ロール (P. 372)
   - 手順 2 で作成したレルムおよびルール。
   - 手順 3 で作成したレスポンス。

   注: ポリシーの作成の詳細については、*「Policy Design Guide」*（SiteMinder6.0 SP5 用の）または「ポリシー サーバ *設定ガイド*」（SiteMinder12.0 SP2 ）を参照してください。

ポリシー ドメインへの CA Identity Manager 環境の追加

SiteMinder でアクセス ロールをサポートできるようにするために、CA Identity Manager 環境を SiteMinder のユーザ ディレクトリおよびポリシー ドメインと関連付けます。

注: ユーザがポリシー ドメインに CA Identity Manager 環境を追加する*前に*、CA Identity Manager 環境と関連付けられているユーザ ストアをポリシー ドメインに追加します。

次の手順に従ってください:

1. ポリシー サーバ ユーザ インターフェースの［ポリシー ドメイン］ダイアログ ボックスで、ポリシー ドメインを持つ CA Identity Manager 環境と関連付けられるユーザ ストアを以下のように追加します。
   a. ［ユーザ ディレクトリ］タブを選択します。
   b. タブの最下部にあるドロップダウン リスト ボックスから、ポリシー ドメインに含めるユーザ ディレクトリを選択します。

c. ［追加］ボタンをクリックします。

ポリシー サーバ ユーザ インターフェースは、［ユーザ ディレクトリ］タブに表示されるリストにディレクトリを追加します。

d. ［適用］をクリックします。

2. CA Identity Manager 環境をポリシー サーバに以下のように追加します。

a. CA Identity Manager 環境タブを選択します。

b. タブの下部にあるドロップダウンリストから、ポリシードメインに関連付ける CA Identity Manager 環境を選択します。

c. ［追加］をクリックします。

ポリシー サーバ ユーザ インターフェースは、タブの一番上の CA Identity Manager 環境のリストにユーザの選択内容を追加します。

3. ［OK］をクリックして変更内容を保存し、ダイアログ ボックスを閉じます。

選択した CA Identity Manager 環境は、ポリシーを作成すると利用できるようになります。

SiteMinder レスポンスを作成

次の手順に従ってください:

1. ポリシー サーバ ホスト ユーザ インターフェースにログインします。
2. ユーザの管理者権限に応じて、以下のいずれかのタスクを実行します。
   - Manage System および Domain Objects 権限がある場合：
     a. オブジェクトペインで、［ドメイン］タブをクリックします。
     b. 値を追加する ポリシー ドメインを選択します。
   - ドメイン オブジェクトの管理権限がある場合は、ポリシー ドメインを選択して、［オブジェクト］ペイン内のレスポンスを追加します。
3. メニュー バーから、［編集］-［<ドメイン名>］-［レスポンスの作成］の順に選択します。

［SiteMinder レスポンス］ ダイアログ ボックスが表示されます（［レスポンス］ダイアログ ボックスを参照）。

4. 新しいレスポンスの名前と説明を入力します。
5. ［エージェント タイプ］グループ ボックスで、［SiteMinder］ラジオ ボタンを選択します。
6. ［エージェント タイプ］グループ ボックス内のドロップダウン リストから［Web エージェント］オプションを選択し［適用］をクリックして変更内容を保存します。

7. ［作成］をクリックします。

   ［SiteMinder レスポンス属性エディタ］ダイアログ ボックスが表示されます。

8. ［属性］ドロップダウン リストから、WebAgent-HTTP-Header-Variable レスポンス属性を選択します。

9. ［属性のセットアップ］タブで、［ユーザ属性］ラジオ ボタンを選択します。

10. ［変数］フィールドで、アプリケーションに渡す変数の名前を入力します。

    たとえば、変数 TASKS を指定する場合、以下のヘッダがアプリケーションに返されます。

    HTTP_TASKS

11. ［属性名］フィールドで、以下のようにレスポンス属性を指定します。

    - SM_USER_APPLICATION_ROLES[:*application id1, application_id2, ...application_idn*] -- ユーザに割り当てられるロールのリストを返します。
    - SM_USER_APPLICATION_TASKS[:*application id1, application_id2, ...application_idn*]

    SiteMinder-Generated レスポンス属性 (P. 368)はより多くの情報を提供します。

12. ［OK］をクリックして変更を保存し、［SiteMinder 管理］ページに戻ります。

SiteMinder ポリシーへのロールの追加

ユーザが保護されているリソースにアクセスする適切なアクセス ロールに割り当てられる場合、SiteMinder ポリシー サーバはユーザへのアクセス ロール割り当てを確認します。検証に際して、ポリシーに含まれているルールを起動して、ユーザがリソースへのアクセスを許可されているかどうかを判断します。

次の手順に従ってください:

1. ［SiteMinder ポリシー］ダイアログ ボックスで、［ユーザ］タブをクリックします。

   ［ユーザ］タブには、ポリシー ドメインに含まれた各ユーザ ディレクトリおよび CA Identity Manager 環境のタブが含まれます。

2. ポリシーに追加するロールが含まれている CA Identity Manager 環境を選択します。

3. ［追加］または［削除］タンをクリックします。

   ［SiteMinder ポリシー CA Identity Manager ロール］ダイアログ ボックスが表示されます。

4. ポリシーにロールを追加するには、［使用可能なメンバ］リストからエントリを選択し、［現在のメンバ］リストに移動します。
5. ［OK］をクリックして変更内容を保存し、［SiteMinder ポリシー］ダイアログ ボックスに戻ります。

ポリシーからロールの除外

アクセス ロールを使用してアプリケーションにアクセスを付与することのほかに、アクセス ロールを使用して、アクセス ロールのメンバがアプリケーションにアクセスできないようにすることもできます。アクセス ロールのメンバがアプリケーションにアクセスできないようするには、SiteMinder ポリシーからのロールを除外します。 CA Identity Manager で除外されているアクセスロールが割り当てられているユーザが保護されたリソースにアクセスしようとすると、ポリシー サーバは、割り当てられたユーザに対する CA Identity Manager ロールの除外を検証します。 検証時には、リソースへのアクセスを阻止します。

次の手順に従ってください:

1. ［SiteMinder ポリシー］ダイアログ ボックスで、［ユーザ］タブをクリックします。

   ［ユーザ］タブには、ポリシー ドメインに含まれた各ユーザ ディレクトリおよび CA Identity Manager 環境のタブが含まれます。
2. ポリシーから除外するロールが含まれている CA Identity Manager 環境をクリックします。
3. ［追加］または［削除］タンをクリックします。

   ［SiteMinder ポリシー CA Identity Manager ロール］ダイアログ ボックスが表示されます。
4. ポリシーにロールを追加するには、［使用可能なメンバ］リストからエントリを選択し、［現在のメンバ］リストの方向を指している左矢印ボタンをクリックします。

   逆の操作を行うと、［現在のメンバ］リストからロールを削除します。
5. ［現在のメンバ］リストで、除外するロールを選択し、リストの下にある［除外］ボタンをクリックます。

   ロールの左には、赤丸に斜線が入ったアイコンが表示されます。このアイコンは、そのロールが除外されていることを示します。
6. ［OK］をクリックして変更内容を保存し、［SiteMinder ポリシー］ダイアログ ボックスに戻ります。

LogOff URI の設定

CA Identity Manager 環境を保護するには、ユーザが CA Identity Manager からログオフした後でユーザ セッションを終了するために環境を保護する SiteMinderWeb エージェントを設定します。

Web エージェントは、Web ブラウザから SiteMinder セッションおよび認証 Cookie を削除し、ポリシー サーバにセッション情報を削除するよう指示することにより、ユーザ セッションを終了します。

SiteMinder セッションを終了するには、CA Identity Manager 環境を保護する SiteMinder エージェント用の［エージェント設定オブジェクト］の［LogOffURI］フィールドでログアウト機能を設定します。

注:

- SiteMinder エージェントには 1 つの LogOff URI があります。 エージェントによって保護されたアプリケーションはすべて同じログアウト ページを使用します。
- 「カスタム ログアウト ページの設定」の説明に従って管理コンソールでカスタム ログアウト ページを設定する場合、CA Identity Manager はカスタム ログアウト ページおよびLogOff URI にログアウト リクエストを送信します。ただし、CA Identity Manager は、ユーザへのカスタム ログアウト ページのみを表示します。

次の手順に従ってください:

1. 以下のいずれかのインターフェースにログインします。
   - CASiteMinder r12 以降の場合は、管理 UI にログインします。
   - CA eTrustSiteMinder6.0 SP5 の場合は、ポリシー サーバ ユーザ インターフェースにログインします。

   注: これらのインターフェースの使用の詳細については、使用している SiteMinder のバージョン用のマニュアルを参照してください。

2. 以下のように、CA Identity Manager 環境を保護するエージェント用の［Agent Configuration Object］内の #LogOffUri プロパティを変更します。
   - パウンド記号（#）の削除
   - ［値］フィールドに、以下のように入力します。

     /iam/im/logout.jsp

   注: Web エージェントをインストールするときに、［エージェント設定オブジェクト］を選択します。詳細については、*「CA SiteMinder Web Access Manager Policy Server Installation Guide」*を参照してください。
3. 変更内容を保存します。
4. Web サーバを再起動します。

SiteMinder レルムのエイリアス

*エイリアス*は、CA Identity Manager 環境にアクセスできるように URL に追加される一意の文字列です。 たとえば、環境のエイリアスが*従業員*である場合、その環境にアクセスするための URL は以下のとおりです。

`http://myserver.mycompany.org/iam/im/employees`

myserver.mycompany.org

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。

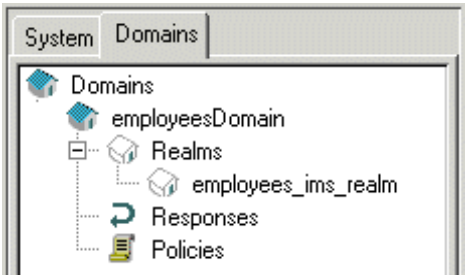
管理コンソールで CA Identity Manager 環境を作成するときに、少なくとも 1 つのエイリアスを指定します （パブリック エイリアスも指定できます）。

SiteMinder は、環境名を使用して、環境を保護するオブジェクトを指定します。たとえば、名前*従業員*を指定するときに、SiteMinder は *employeesobject_type* という名前のオブジェクトを作成します。

object_type

employees_ims_realm などの SiteMinder オブジェクトを定義します。

以下の図では、SiteMinder が作成するオブジェクトの 2 つを示しています。



SiteMinder レルムのエイリアスの更新

管理コンソール内の保護されたエイリアス、またはパブリック エイリアスを変更する場合、CA Identity Manager はポリシー サーバのエイリアス名を更新しようとします。 CA Identity Manager が名前を更新できない場合、以下のいずれかのインターフェースでそれらを手動で更新できます。

- CA SiteMinder Web Access Manager r12 以降の場合は、管理 UI を使用します。
- CA eTrust SiteMinder 6.0 SP5 の場合は、ポリシー サーバ ユーザ インターフェースにログインします。

次の手順に従ってください:

1. CA Identity Manager 環境のレルムを探します。

   CA Identity Manager が SiteMinder と統合される場合、これらのレルムは、（他の必要な SiteMinder オブジェクトと共に）自動的に作成されます。

   レルムは以下の命名規則を使用します。

   - *Identity Manager-environment*_ims_realm-- ユーザ コンソールを保護します。
   - *Identity Manager-environment*_pub_realm-- 自己登録と忘れたパスワード タスクなどパブリック タスクのサポートを有効にします。パブリック エイリアスを設定している場合にのみ、このレルムが表示されます。

     注: レルムを変更するために、まず、ポリシー サーバ ユーザ インターフェースを使用している場合は、CA Identity Manager 環境用のポリシー ドメイン（*Identity Manager-environmentDomain*）をまず探します。 レルムはドメインの下の場所にあります。

2. 以下のようにレルムのリソースを変更します。

   /iam/im/*new_alias*

   リソース フィルタのエイリアスに先行する /iam/im/ を削除しないでください。

3. 変更内容を保存します。

注: ［CA Identity Manager プロパティの変更］では、管理コンソール内のエイリアスの変更についての指示に従います。

SiteMinder パスワードまたは共有シークレットの編集

ポリシー サーバに CA Identity Manager 拡張をインストールするときに、ポリシー サーバと通信するために CA Identity Manager が使用する SiteMinder 管理者アカウント用のパスワードを提供します。

パスワードは変更できます。ただし、パスワードは暗号化される必要があります。パスワードを暗号化するには、CA Identity Manager と共に提供されるパスワード ツールを使用します。

注: ユーザが SiteMinder パスワードを変更する前に、JAVA_HOME 変数がユーザの環境に対して定義されることを確認します。

次の手順に従ってください:

1. 以下のようにパスワードを暗号化します。
   a. コマンド ラインから、以下の例のように、*admin_tools* が管理ツールのインストールされた場所である場合、*admin_tools*¥PasswordTool に移動します。
      - **Windows:** C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity Manager¥tools¥PasswordTool
      - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/PasswordTool
   b. 以下のコマンドを入力します。

      pwdtools *new_password*

      このコマンドで、*new_password* は暗号化するパスワードです。

      注: pwdtools ユーティリティのオプションの詳細については、以下のコマンドを入力します。

      pwdtools ヘルプ
   c. 暗号化されたパスワードをコピーします。
2. 以下のとおりに、関連する手順を完了します。
   - CA Identity Manager が WebLogic アプリケーション サーバで実行されている場合は、以下タスクを実行します。
     a. WebLogic コンソールで、policyserver_rar コネクタ記述子内の WebLogic リソース アダプタを編集します。
     b. パスワード プロパティの値として暗号化されたパスワードを追加します。

- CA Identity Manager が JBoss アプリケーション サーバで実行されている場合は、以下のタスクを実行します。

  a. Open ra.xml from *JBoss_home*¥server¥default¥deploy¥iam_im.ear¥policyserve から ra.xml を開きます。

  b. パスワード設定プロパティの値として暗号化されたパスワードを追加します。

- CA Identity Manager が WebSphere アプリケーション サーバで実行されている場合は、以下のタスクを完了します。

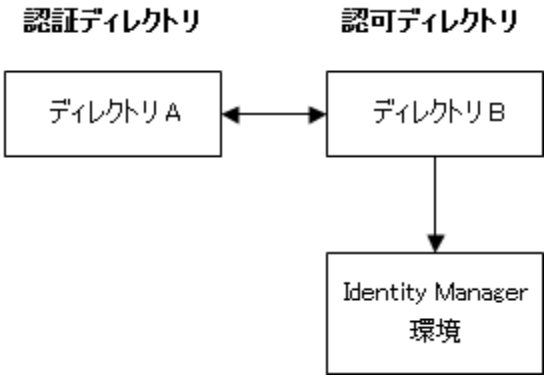
  a. WebSphere コンソールで、ra.xml を開きます。

  b. パスワード設定プロパティの値として暗号化されたパスワードを追加します。

3. アプリケーション サーバを再起動します。

認証と認可用の別のディレクトリを使用できるように、CA Identity Manager 環境の設定

管理者は、管理者の認証に対して使用されるものとは別のユーザ ストアにそのプロファイルが存在するユーザを管理する必要がある場合があります。つまり、CA Identity Manager 環境にログインするときに、管理者は、1 つのディレクトリを使用して認証される必要があり、以下の図で示すように、別のディレクトリ内のユーザを管理する権限が必要です。



次の手順に従ってください:

1. 以下のいずれかのインターフェースにログインします。
   - CASiteMinder Web Access Manager r12 の場合は、管理 UI にログインします。
   - CA eTrustSiteMinder6.0 SP5 の場合は、ポリシー サーバ ユーザ インターフェースにログインします。

   注: これらのインターフェースの使用の詳細については、使用している SiteMinder のバージョンのマニュアルを参照してください。
2. 2 つのユーザ ディレクトリを作成します。

   1 つのディレクトリは認証データ（管理者プロファイル）を参照し、別のディレクトリは認可データ（ユーザ プロファイル）を参照します。
3. 管理コンソールで、CA Identity Manager 環境 を作成します。

   CA Identity Manager ディレクトリとして認可ディレクトリを選択します。
4. 使用される SiteMinder のバージョンのインターフェースで、前の手順で作成した CA Identity Manager 環境用のドメインへの認証ディレクトリを追加します。

   ユーザが環境を作成し、SiteMinder が CA Identity Manager と統合される場合、SiteMinder に必要なドメインおよび他のオブジェクトは自動的に作成されます。

   ドメインは以下の命名規則を使用します。

   *Identity Manager-environment*Domain
5. ドメインと関連付けられるディレクトリのリストにこのディレクトリが最初に表示されることを確認します。
6. *Identity Manager-environment*_ims_realm を探します。
7. レルム定義の［詳細］セクション内の認証ディレクトリに認可ディレクトリをマップします。
8. 以下の *Identity Manager-environment*response_ims レスポンスを探します。
9. 以下のようにレスポンスにレスポンス属性を追加します。

フィールド	値
属性	Web-Agent-HTTP-Header-Variable
属性の種類	ユーザ属性
変数名	sm_userdn
属性名	SM_USERNAME

10. 変更内容を保存します。

    CA Identity Manager はこれで、認証と認可用の個別のディレクトリを使用するようになりました。

LDAP ディレクトリ操作のパフォーマンスを改善する方法

LDAP ユーザ ディレクトリに対して CA Identity Manager が要求するすべてが一定の接続セットからルーティングされるため、ディレクトリ操作は処理に時間がかかる場合があります。

ユーザ ディレクトリへの CA Identity Manager リクエストのスループットを向上させるため、SiteMinder が同じディレクトリへの複数の接続を開けるように設定します。 この手順を実行するには、ポリシー サーバ ユーザ インターフェース内の［LDAP ディレクトリのフェイルオーバ］および［ロード バランシングのセットアップ］ダイアログ ボックスを追加します。

LDAP サーバ（および作成する接続数）を入力する回数は、CA Identity Manager 上の負荷により異なります。

付録 A: FIPS 140-2 準拠

このセクションには、以下のトピックが含まれています。

FIPS の概要 (P. 381)
通信 (P. 382)
インストール (P. 382)
SiteMinder への接続 (P. 383)
キー ファイル ストレージ (P. 383)
パスワード ツール (P. 384)
FIPS モード検出 (P. 386)
暗号文形式 (P. 387)
暗号化される情報 (P. 387)
FIPS モードのログ記録 (P. 388)

FIPS の概要

FIPS（Federal Information Processing Standards： 連邦情報処理標準） 140-2 は、製品が暗号化に使用すべき暗号のライブラリおよびアルゴリズムのセキュリティ標準です。 FIPS 140-2 暗号化は、CA 製品のコンポーネント間、および CA 製品とサードパーティ製品間におけるすべての機密データの通信に影響を与えます。 FIPS 140-2 では、機密性の高い未分類のデータを保護するセキュリティ システム内で暗号アルゴリズムを使用するための要件が指定されています。

CA Identity Manager は、米国政府によって適用される Advanced Encryption Standard（AES）を使用します。CA Identity Manager には RSA CryptoJ v3.5 および CryptoC ME v2.0 暗号化ライブラリが組み込まれています。 これは、FIPS 140-2 の暗号化モジュールのセキュリティ要件を満たしていることが確認されています。

通信

FIPS 暗号化は、CA Identity Manager と以下のコンポーネントの間のデータ通信をすべて網羅します。

- CA Identity Manager Server
- プロビジョニング サーバ
- プロビジョニング マネージャおよびクライアント
- C++ コネクタ サーバ
- C++ コネクタ サーバ エンドポイント（エンドポイントによってサポートされている場合）
- CA IAM コネクタ サーバ（CA IAM CS）
- CA IAM CS エンドポイント（エンドポイントによってサポートされている場合）
- Connector Xpress （エンドポイントによってサポートされている場合）
- Windows パスワード同期エージェント
- Java アイデンティティおよびアクセス管理（JIAM）

インストール

CA Identity Manager インストーラにより、FIPS 140-2 に準拠するように CA Identity Manager を設定できます。

CA Identity Manager 環境内のコンポーネントはすべて CA Identity Manager が FIPS 140-2 をサポートするように、FIPS 140-2 が有効である必要があります。 インストール中に FIPS 140-2 を有効にするには FIPS 暗号化キーが必要です。 FIPS 暗号化キーを生成するには、インストール パッケージをアンパックした場所からパスワード ツール（pwdtools.bat/pwdtools.sh）を実行します。パスワード ツールは以下の場所で利用可能です。

- Windows: *package root*¥PasswordTool¥bin¥pwdtools.bat
- UNIX: *package root*/PasswordTool/bin/pwdtools.sh

注: パスワード ツールも以下の場所にインストールされます。

```
C:¥Program Files¥CA¥Identity Manager¥IAM Suite¥Identity
Manager¥PasswordTool¥pwdtools.bat
```

重要: すべてのインストールで同じ FIPS 140-2 暗号化キーを使用し、パスワード ツールで生成されたキー ファイルを保護してください。

SiteMinder への接続

CA Identity Manager インストール中に CA SiteMinder に接続する場合は、以下の表にリスト表示されているように、FIPS モードおよび製品バージョン設定のみがサポートされることに注意してください。

CA Identity Manager r12	SiteMinder	SiteMinder バージョン
FIPS-only モード	FIPS-only モード	r12
FIPS-only モード	FIPS-compatible モード	r12
Non-FIPS モード	FIPS-compatible モード	r12
Non-FIPS モード	Non-FIPS モード	r6

キー ファイル ストレージ

CA Identity Manager は、FIPS 暗号化キー ストレージに対してファイル システムを使用します。 CA Identity Manager 管理者は不正なアクセスからファイルを保護する責任を担っています。CA Identity Manager 管理者は、CA Identity Manager を実行する権限が与えられているユーザなど、特定のグループまたはユーザ タイプに対してディレクトリ アクセス許可を設定することにより、ファイルを保護することができます。

以下の表に、各 CA Identity Manager コンポーネントの FIPS キー ファイルの場所をリストします。

コンポーネント	インストール場所
CA Identity Manager Server	*iam_im.ear*¥config¥com¥netegrity¥config¥keys¥FIPSkey.dat *iam_im.ear* は、アプリケーション サーバ上の CA Identity Manager のインストール場所です。
プロビジョニング サーバ	*Provisioning Server install*¥data¥tls¥keymgmt¥imps_datakey
C++ コネクタ サーバ	*Provisioning Server install*¥data¥tls¥keymgmt¥imps_datakey
パスワード同期エージェント	*Provisioning Server install*¥data¥tls¥keymgmt¥imps_datakey

パスワード ツール

FIPS 準拠のパスワード ツール ユーティリティ（pwdtools.bat （または pwdtools.sh））はコマンド ラインから、CA Identity Manager インストール中に暗号化鍵を生成できます。

パスワード ツールを使用する前に pwdtools.bat/pwdtools.sh ファイルを編集し、JAVA_HOME 変数を設定します。

重要: CA Identity Manager はデータ マイグレーションまたは再暗号化をサポートしません。そのため、暗号化鍵がインストールの後に変更されないことを確認します。

このコマンドの構文は、以下のようになります。

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <key file location>] [-f
<encrypting parameters file>]
```

JSAFE

PBE アルゴリズムを使用して、プレーン テキスト値を暗号化します。

例：

```
pwdtools -JSAFE –p mypassword
```

注: 以前のバージョンでは、ブートストラップ管理者のパスワードはクリア テキストで格納されます。 CA Identity Manager r12.6 SP1 以降にアップグレードまたは移行する場合は、クリア テキストのパスワードを手動で暗号化する必要があります。 ツールを使用する場合は、JSAFE オプションが指定されることを確認し、以下の手順に従います。

1. CA Identity Manager r12.6 SP1 にアップグレードまたは移行した後、CA Identity Manager オブジェクト ストア データベースに移動し、以下のテーブルを検索します。
   IM_AUTH_USER
2. パスワード ツールを使用し、JSAFE によって、クリア テキストのパスワードを暗号化します。
3. テーブル内のクリア テキストを暗号化されたパスワードと置き換えます。

FIPSKEY

インストーラに対して、FIPS キー ファイルを作成します。 CA Identity Manager をインストールする前にキーを生成します。

例：

```
pwdtools -FIPSKEY –k C:¥keypath¥FIPSkey.dat
```

ここで *keypath* は、FIPS キーを格納する場所へのフル パスです。

パスワード ツールは指定された場所で FIPS キーを作成します。 インストール中に、インストーラに FIPS キー ファイルの場所を提供します。

注: 必ず CA Identity Manager を実行する権限が与えられているユーザなど、特定のグループまたはユーザ タイプに対してディレクトリ アクセス許可を設定することにより、キーを保護してください。

FIPS

FIPS キー ファイルを使用して、プレーン テキスト値を暗号化します。 FIPS は既存の FIPS キー ファイルを使用します。

例：

```
pwdtools -FIPS –p firewall -k C:¥keypath¥FIPSkey.dat
```

ここで *keypath* は FIPS キー ディレクトリへのフル パスです。

注: インストール中に指定したのと同じ FIPS キー ファイルを使用します。

RC2

RC2 アルゴリズムを使用して、プレーン テキスト値を暗号化します。

重要: CA Identity Manager は、FIPS キー ファイルを使用して、アプリケーションが FIPS モードまたは非 FIPS モードで開始することかどうかを確認します。そのため、キー ファイルが以下のアプリケーション サーバ展開パスを持つ FIPSKey.dat という名前であることを確認します。

```
iam_im.ear¥config¥com¥netegrity¥config¥keys¥FIPSkey.dat
```

ここで、iam_im.ear はアプリケーション サーバ展開ディレクトリです。

```
jboss_home¥server¥default¥deploy
```

FIPS モード検出

CA Identity Manager が FIPS モード、または非 FIPS モードで動作しているかどうかを判断するには、CA Identity Manager 環境ステータス ページを使用します。

ステータス ページを表示するには、ブラウザで以下の URL を入力します。

`http://server_name/iam/im/status.jsp`

server_name

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決定します。たとえば、myserver.mycompany.com。 この例では、完全な URL は次のとおりです。

http://myserver.mycompany.com/iam/im/status.jsp

FIPS ステータスはページの下部に表示されます。

注: また、以下のキー ファイルを見つけることにより、FIPS モードで CA Identity Manager が動作しているかどうかも確認できます。

`/config/com/netegrity/config/keys/FIPSkey.dat`

このファイルが存在する場合、CA Identity Manager は FIPS モードで動作しています。

パスワード ツール ユーティリティ、pwdtools.bat （または pwdtools.sh）は CA Identity Manager インストール中に FIPSkey.dat キー ファイルを作成します。

暗号文形式

アルゴリズム名はプレフィックスとして暗号文に追加されます。また、どのアルゴリズムが暗号化に使用されたかを CA Identity Manager に伝えます。

FIPS モードでは、プレフィックスは {AES} です。 たとえば、テキスト「パスワード」を暗号化する場合、暗号文は以下のようになります。

{AES}:eolQCTq1CGPyg6qe++0asg==

非 FIPS モード（または JSAFE モード）では、アルゴリズムに応じて、プレフィックス（アルゴリズム タグ）は {PBES} または {RC2} です。 たとえば、テキスト「パスワード」を暗号化する場合、暗号文は以下のようになります。

{PBES}:gSex2/BhDGzEKWvFmzca4w==

［システム］の下の「秘密鍵」タスクを使用して、動的なキーを作成できます。 ユーザが動的なキーを定義する場合、キー ID がアルゴリズム タグとタグ区切り文字（':'）の間に挿入されます。 暗号化されたデータにキー ID がない場合は、ハードコードされたキーが暗号化に使用されたことを示します。これは後方互換性、または、動的なキーが指定のアルゴリズムに対して定義されていない場合に使用できます。

暗号化される情報

以下の CA Identity Manager 情報が暗号化されます。

- Jboss 用のデータ ソース設定のパスワード
- 忘れたパスワード回復情報
- プロビジョニング サーバ コールバック シークレット

- ワークフロー セッション情報
- ポリシー サーバ接続情報

CA Identity Manager は、JSafe ライブラリを使用して、データを暗号化および復号化します。 ライブラリが改ざんされていないことを確認するために、CA Identity Manager では起動時に CryptoJ セルフテスト コードを使用します。

セルフテストが実行された後で、そのテストのステータスをレポートする CryptoJ メッセージがアプリケーション サーバ ログに表示されます。 ログには以下のいずれかのメッセージが含まれます。

```
[ims.default] * CryptoJ was initialized properly.

[ims.default] !!! CryptoJ was not initialized properly. !!!
```

FIPS モードのログ記録

以下の CA Identity Manager コンポーネントは、FIPS モードが有効であるかどうかをログ ファイルに示します。

- CA Identity Manager Server
- プロビジョニング サーバ
- C++ コネクタ サーバ
- CA IAM CS
- プロビジョニング マネージャ
- パスワード同期エージェント

すべての場合に、FIPS モードが有効であることを示すログ エントリの最後は以下の文字列になります。

FIPS 140-2 MODE: ON

付録 B: CA Identity Manager 証明書を SHA-2 署名付き SSL 証明書で置き換える

SHA-2 SSL 証明書ハッシュは、全米標準技術研究所（NIST）および国家安全保障局（NSA）によって開発された暗号のアルゴリズムです。SHA2 証明書は以前のすべてアルゴリズムより安全です。 CA Identity Manager で、SHA-1 ハッシュ関数で署名される証明書の代わりの SHA-2 署名付き SSL 証明書を設定できます。

注: SSL 証明書の設定の詳細については、「インストール ガイド」を参照してください。

以下のテーブルでは、SHA-2 署名付き証明書を配置できる CA Identity Manager サーバ上のパスの場所について説明します。

証明書	インストール場所	説明
プロビジョニング サーバ証明書	[Provisioning Server install dir]/data/tls/server/eta2_servercert.pem [Provisioning Server install dir]/data/tls/server/eta2_serverkey.pem *cs_install*/ccs/data/tls/server/eta2_servercert.pem *cs_install*/ccs/data/tls/server/eta2_serverkey.pem *cs_install*/jcs/conf/eta2_server.p12	.pem 形式および .p12 形式（署名付き証明書、秘密鍵およびルート CA 証明書を含む）で CA IAM CS によって使用されます。 **注**: alias eta2_server の下の *cs_install*/jcs/conf/ssl.keystore に eta2_server.p12 をインポートします。ssl.keystore パスワードはインストール中に提供されるコネクタ サーバのパスワードです。

証明書	インストール場所	説明
プロビジョニング クライアント証明書	[Provisioning Server install dir]/data/tls/client/eta2_clientcert.pem [Provisioning Server install dir]/data/tls/client/eta2_clientkey.pem [Provisioning Manager install dir]/data/tls/client/eta2_clientcert.pem [Provisioning Manager install dir]/data/tls/client/eta2_clientkey.pem *cs_install*/ccs/data/tls/client/eta2_clientcert.pem *cs_install*/ccs/data/tls/client/eta2_clientkey.pem *cs_install*/jcs/conf/eta2_client.p12	.pem 形式および .p12 形式（署名付き証明書、秘密鍵およびルート CA 証明書を含む）で CA IAM CS によって使用されます。
プロビジョニング ディレクトリ Trusted 証明書	*cadir_install*/config/ssld/impd_trusted.pem	.pem 形式で CA Directory によって使用されます。以下の構造で証明書コンテンツが含まれる必要があります。 -----証明書の開始----- 証明書の内容 -----証明書の終了-----
プロビジョニング ディレクトリ使用者証明書	*cadir_install*/config/ssld/personalities/impd-co.pem *cadir_install*/config/ssld/personalities/impd-inc.pem *cadir_install*/config/ssld/personalities/impd-main.pem *cadir_install*/config/ssld/personalities/impd-notify.pem *cadir_install*/config/ssld/personalities/impd-router.pem	.pem 形式で CA Directory によって使用されます。

証明書	インストール場所	説明
ルート CA 証明書	[Provisioning Server install dir]/data/tls/et2_cacert.pem [Provisioning Manager install dir]/data/tls/et2_cacert.pem *cs_install*/ccs/data/tls/ et2_cacert.pem *conxp_install*/lib/jiam.jar [Application Server install dir]/iam_im.ear/library/jiam.jar	証明書は、Connector Xpress keystore located at [Connector Xpress install dir]/conf/ssl.keystore にインスールされます。 証明書は jiam.jar キーストアにもインポートされる必要があります。 インポートするには、jar を抽出し、証明書を certificate into admincacerts.jks にインポートしてから、jar のコンテンツを再パッケージします。admincacerts.jks のキーストア パスワードは "changeit" です。 jiam.jar のコピーがすべて置き換えられていることを確認します。

便利なコマンド

OpenSSL プログラムは、OpenSSL のライブラリのさまざまな暗号化機能を使用するためのコマンド ライン ツールです。 このツールは [Provisioning Server install dir]/bin にある IMPS に同梱されています。

以下のテーブルでは、証明書の管理に関連するさまざまなコマンドを実行する、OpenSSL プログラムの便利なコマンドについて説明しています。

コマンド	説明
`openssl x509 –in cert.pem –text –noout`	.pem 証明書のコンテンツを印刷します。
`openssl.exe pkcs12 -in my.pkcs12 –info`	.p12 ファイルのコンテンツを印刷します。
`openssl.exe pkcs12 -export -chain –inkey key.pem –in cert.pem -CAfile cacert.pem -out my.p12`	.pem 証明書/keypair を .p12. に変換します。
`keytool –list –v -keystore my.keystore`	Java キーストアのコンテンツを印刷します。
`keytool –list –v –alias myalias –keystore my.keystore`	Java キーストアの特定のエイリアスのコンテンツを印刷します。

コマンド		説明
	keytool –delete –alias myalias –keystore my.keystore	Java キーストアからエイリアスを削除します。
	keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias	Java キーストアに .p12 ファイルをインポートします。
	keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore	Java キーストアに pem root ca 証明書をインポートします。