

CA Identity Manager™

管理ガイド

12.6.4



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 Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 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 Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA CloudMinder™ Identity Management
- CA ディレクトリ
- CA Identity Manager™
- CA Identity Governance（旧 CA GovernanceMinder）
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder™

CA への連絡先

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

目次

第 1 章: ロールの計画	17
ロールの決定.....	17
ロールの目的.....	18
追加の管理者の作成.....	19
アイデンティティまたはアクセスを管理するロール.....	20
委任された管理.....	20
ロール管理者の指定.....	21
委任の手順.....	22
委任の例.....	23
ロールの特性.....	23
ロール プロファイル.....	24
ロールのタスク.....	24
アカウント テンプレート.....	25
メンバールール、管理ルール、および所有者ルール.....	25
スコープ ルール.....	27
ルールの一般的なガイドライン.....	30
アクションの追加および削除.....	32
メンバ ポリシー.....	33
管理ポリシー.....	33
ロールの計画のチェックリスト.....	34
 第 2 章: 管理ロール	 37
管理ロールと管理タスク.....	37
管理ロールと CA Identity Manager 環境.....	37
管理ロールとユーザ コンソール.....	38
管理ロールの作成.....	38
管理ロールの新規作成.....	39
管理ロールのプロファイルの定義.....	39
ロールの管理タスクの選択.....	40
管理ロールのメンバ ポリシーの定義.....	41
管理ロールの管理ポリシーの定義.....	42
管理ロールの所有者ルールの定義.....	43
管理ロールの確認.....	43
ユーザによるロールの自己割り当ての許可.....	44

第 3 章: 管理タスク 45

管理タスクの計画.....	45
管理タスクの例.....	47
管理タスクの使用法オプション	49
デフォルトの管理タスク	50
カスタム管理タスクの作成方法.....	50
タスクのプロファイルの定義.....	52
管理タスクの [プロファイル] タブ.....	52
タスク設定プロパティ.....	56
タスク スコープの定義.....	57
検索画面設定.....	58
タスクのタブの選択.....	68
[アカウント] タブ.....	69
[スケジュール] タブ.....	71
タスクのフィールドの表示	72
使用しているロールの表示	72
イベントへのワークフロー プロセスの割り当て	72
Active Directory ユーザ ストアの管理.....	73
sAMAccountName 属性	73
グループのタイプとスコープ.....	73
アプリケーション機能の外部タスク	75
[外部] タブ.....	75
[外部 URL] タブ	76
高度なタスク コンポーネント	77
ビジネス ロジック タスク ハンドラの作成	77
管理タスクおよびイベント.....	79
プライマリ イベントおよびセカンダリ イベント	80
タスクのイベントの表示.....	80
未変更のプロファイルに生成されるイベント	81
管理タスクの処理.....	81
同期段階の処理.....	82
非同期段階の処理.....	83
管理タスクの画像.....	85

第 4 章: ユーザ 87

ユーザの作成.....	87
ユーザ プロファイルの作成.....	89
ユーザへのグループの割り当て	90

ユーザへのロールの割り当て	90
ユーザへのサービスの割り当て	91
ユーザへの自己登録の許可	92
セルフサービス タスク	94
セルフサービス タスクへのアクセス	95
企業の Web サイトへのセルフサービス リンクの埋め込み	95
複数のセルフサービス タスクの設定	97
自己管理ロールへのアクセス制限	100

第 5 章: パスワード管理 101

CA Identity Manager のパスワード管理	101
パスワードポリシーの概要	102
パスワードポリシーの作成	103
追加パスワードポリシーの有効化	104
ユーザセットへのパスワードポリシーの適用	104
パスワードの有効期限の設定	106
パスワード構成の設定	110
正規表現の指定	112
パスワードの制限の設定	114
パスワードの詳細オプションの設定	118
パスワードポリシーの管理	119
パスワードポリシーとリレーショナルデータベース	119
CA Identity Manager と SiteMinder の統合パスワード基準	119
パスワードのリセットまたはアカウントのロック解除	120
クレデンシャルプロバイダのインストール	120
クレデンシャルプロバイダの設定	120
Credential Provider のレジストリ設定	123
Cube ブラウザのレジストリ設定	124
[Powered by] メッセージのカスタマイズ	126
Windows ログイン用パスワードのリセット	127
Credential Provider のサイレントインストール	127

第 6 章: エンドポイント上でのパスワードの同期 131

Windows 上のパスワードの同期	131
UNIX および Linux 上のパスワードの同期	141
OS400 でのパスワード同期	156

第 7 章: グループ 165

静的グループの作成.....	165
動的グループの作成.....	166
動的グループ クエリのパラメータ	167
ネスト グループの作成.....	169
静的グループ、動的グループ、ネスト グループの例	171
グループ管理者.....	172

第 8 章: 管理対象のエンドポイント アカウント 175

管理エンドポイントの統合	176
ロール定義ファイルのインポート	177
関連ルール作成.....	177
環境へのエンドポイントの追加.....	180
検索および関連付けの定義の作成.....	180
エンドポイントの検索および関連付け	182
ユーザ、アカウント、およびロールの同期	183
ユーザとロールの同期.....	185
ユーザとアカウント テンプレートの同期	186
エンドポイント アカウントとアカウント テンプレートの同期	187
エンドポイント アカウントとの逆同期	191
逆同期の仕組み.....	192
エンドポイント属性のマッピング	192
逆同期のポリシー.....	195
逆同期用の承認タスクの作成.....	199
逆同期の実行.....	201
エンドポイントのカスタム属性の拡張	202
アカウント タスク	204
エンドポイント アカウントの表示または変更	204
プロビジョニング済みアカウントの作成.....	205
例外アカウントの作成.....	206
孤立アカウントの割り当て	206
システム アカウントの割り当て	207
アカウントの移動タスク画面.....	208
エンドポイント アカウントの削除.....	208
エンドポイント アカウントのパスワード変更	209
複数のアカウントに対するアクションの実行	209
詳細なアカウント操作.....	210
アカウントに対するグローバル ユーザの変更	210

自動検索が機能するしくみ.....	211
アカウントを削除する.....	212
削除を保留中を使用する.....	213
削除されたアカウントの再作成.....	213

第 9 章: プロビジョニング ロール 215

プロビジョニング ロールとアカウント テンプレート	215
アカウント割り当て用のロールの作成	216
アカウント テンプレートの作成	218
プロビジョニング ロールの作成	219
ロールおよびテンプレート タスク	220
プロビジョニング ロールのインポート	220
プロビジョニング ロールへの新規所有者の割り当て	221
プロビジョニング ロールによって作成されたアカウントのパスワード	221
プロビジョニング ロール イベントの処理順序	222
環境での [ネストされたロール] の有効化	224
プロビジョニング ロール内へのロールの追加	225
アカウント テンプレートの属性	225
機能と初期属性.....	226
[アカウント テンプレート] 内のルール文字列	227
属性の値.....	229
詳細なルール式.....	229
ルールの文字列と値の組み合わせの使用	230
ルールのサブストリング	230
複数値のルール式.....	231
明示的なグローバル ユーザ属性ルール	233
組み込みルール関数.....	234
プロビジョニング ロールのパフォーマンス	236
JAM オブジェクト キャッシュ	236
セッションプーリング	237
既存環境用のプロビジョニング タスク	238

第 10 章: 管理されたサービス(基本的なアクセス リクエスト) 239

サービスの作成.....	240
サービスの作成の理解.....	242
サービスの作成の開始.....	243
サービス プロファイルの定義.....	243
サービスの管理ポリシーの定義.....	246

サービスの所有者ルールの定義.....	247
サービスの前提条件の定義.....	247
サービスの更新の電子メール通知の設定.....	248
履行と取り消しのアクションの理解.....	249
サービスの履行と取り消しのアクションの定義.....	249
ユーザへのサービスの割り当て.....	251
サービス割り当ての確認.....	252
サービスをユーザに利用可能にする.....	252
ユーザへのサービスの割り当て.....	254
サービス割り当ての確認.....	255
サービスの変更.....	255
[アクセスをリクエストおよび表示] への検索の追加.....	257
サービスの削除.....	258
サービス メンバの確認と削除.....	259
サービスの削除.....	259
サービスへのアクセスの更新.....	260

第 11 章: 同期 261

サーバ間のユーザの同期.....	261
インバウンド同期.....	261
インバウンド同期のフェールオーバ.....	261
アウトバウンド同期.....	261
パスワード同期の有効化.....	263
ユーザの作成または変更タスクにおけるユーザの同期.....	264
同期タスク.....	266
同期していないユーザが発生する理由.....	267
ユーザの同期.....	268
アカウント テンプレートの同期.....	271
アカウントの同期.....	275

第 12 章: ワークフロー 277

ワークフローの概要.....	277
WorkPoint プロセス図.....	278
ワークフローと電子メール通知.....	278
WorkPoint のマニュアル.....	279
Workflow の制御メソッド.....	279
ワークフロー コントロールの使用 - テンプレート メソッド.....	280
前提条件: ワークフローの有効化.....	281

ワークフロー制御-テンプレート メソッドの下に管理タスクを配置します。	281
タスク/イベント ベースのワークフロー	282
プロセス テンプレートのタイプ	289
参加者リゾルバのタイプ	293
[ワークフロー プロセス] に対して [電子メール ポリシー] を設定します	299
ワークフロー例： ユーザの作成	299
WorkPoint メソッドの使用方法	302
WorkPoint 管理ツールの設定	303
WorkPoint プロセス	308
ワークフロー アクティビティ	314
参加者リゾルバ： WorkPoint メソッド	317
WorkPoint Designer のプロセス	328
ジョブとプロセス インスタンス	331
ワークフロー アクティビティの実行	332
ワークフロー サーバによるアクティビティの完了	334
Workpoint ジョブの表示	335
既存の [承認] タブへの [ジョブの表示] タブの追加	335
承認タスクにおける [ジョブの表示] タブの表示	336
イベント レベル ワークフローのワークフロージョブの表示	337
タスク レベル ワークフローのワークフロー ジョブの表示	337
ポリシーベース ワークフロー	337
ワークフロー プロセス	338
ルールオブジェクト	339
ルールの評価	340
ポリシー順序	341
ポリシーの説明	343
承認画面での変更された属性の強調表示	344
承認ポリシーおよび複数值属性	345
ワークフロー承認画面で属性が変更済みとして強調表示される	346
ポリシーの例	346
ポリシーベースのイベント用ワークフローの設定方法	349
ポリシーベースのタスク用ワークフローの設定方法	350
承認ポリシーの設定方法	351
ポリシーベースのワークフロー ステータス	352
グローバル イベント レベルのポリシーベースのワークフロー マッピング	353
オンライン リクエスト	357
オンライン リクエスト タスク	357
オンライン リクエスト プロセス	359
オンライン リクエスト履歴	360
オンライン リクエストの使用	360

Workflow Action Buttons (ワークフロー アクション ボタン)	361
承認タスクのワークフロー ボタン	362
CA Identity Manager でのボタン設定	362
ワークフロー アクション ボタンの追加	363
ワーク リストと作業アイテム	366
ワーク リストの表示	367
作業アイテムの保留	368
作業アイテムの委任	369
作業アイテムの再割り当て	375
作業アイテムに対するバルク操作	378

第 13 章: 電子メール通知 379

CA Identity Manager の電子メール通知	380
電子メール通知方法を選択する方法	381
SMTP の設定	382
JBoss 上での SMTP の設定	383
WebLogic 上での SMTP の設定	384
WebSphere 上での SMTP の設定	384
電子メール通知ポリシーの作成方法	385
電子メール通知プロファイル タブ	386
[送信のタイミミング] タブ	388
受信者タブ	390
コンテンツ	391
電子メール通知ポリシーの変更	393
電子メール通知ポリシーの無効化	393
ユース ケース: ウェルカム メール の送信	394
電子メールテンプレートの使用方法	395
電子メール通知の有効化	396
電子メールを送信するためのイベントまたはタスクの設定	396
電子メールのコンテンツ	398
電子メールテンプレート	399
電子メールテンプレートの作成	402
電子メールのカスタム テンプレート	403
電子メールテンプレートの展開	423

第 14 章: レポート 427

設定の概要	427
レポート プロセス	429

スナップショット レポートの実行方法	430
レポート サーバ接続の設定	433
スナップショット データベース接続の作成	434
スナップショット 定義の作成	435
例： ユーザ権限データ用のスナップショット 定義の作成	437
スナップショット の管理	438
スナップショット データのキャプチャ	438
スナップショット 定義とレポート タスクの関連付け	440
エンドポイント アカウントとアカウント テンプレートの同期	442
管理タスクの例	442
レポートのリクエスト	445
レポートの表示	447
スナップショット 以外のレポートの実行方法	448
レポート サーバ接続の設定	449
レポート 用の接続の作成	450
接続のレポート タスクへの関連付け	450
レポートのリクエスト	451
レポートの表示	453
レポート オプションの設定	454
カスタム スナップショット レポートの作成および実行方法	455
Crystal Reports でのレポートの作成	457
レポート パラメータ XML ファイルの作成	457
レポートとレポート パラメータ XML ファイルのアップロード	462
レポート タスクの作成	464
レポートのリクエスト	467
レポートの表示	469
ユーザ、アカウント、およびロールの同期	470
ユーザとロールの同期	472
ユーザとアカウント テンプレートの同期	473
エンドポイント アカウントとアカウント テンプレートの同期	474
トラブルシューティング	478
レポートを表示すると Infoview のログイン ページにリダイレクトされる	478
20,000 を超えるレコードのユーザ アカウントの生成	478

第 15 章: アイデンティティ ポリシー 481

アイデンティティ ポリシー	481
アイデンティティ ポリシー セットの計画ワークシート	482
アイデンティティ ポリシー セットの作成	483
アイデンティティ ポリシー セットの管理	495

ユーザとアイデンティティ ポリシーとの同期の方法	496
CA Identity Manager 環境のアイデンティティ ポリシー セット	500
禁止アイデンティティ ポリシー	504
禁止アイデンティティ ポリシー違反のためのアクション	506
禁止アイデンティティ ポリシーの仕組み	507
禁止アイデンティティ ポリシーに関する重要な注意事項	507
禁止アイデンティティ ポリシーの作成	508
使用事例 - ユーザが競合するロールを持つのを防ぐ	509
ワークフローおよび禁止アイデンティティ ポリシー	510
アイデンティティ ポリシーおよび禁止アイデンティティ ポリシーの統合	515

第 16 章: Policy Xpress 517

Policy Xpress の概要	517
ポリシーの作成方法	518
プロファイル	519
イベント	524
データ エレメント	525
エントリ ルール	527
アクション ルール	529
詳細設定	534

第 17 章: CA Identity Manager モバイル アプリケーション 537

CA Identity Manager モバイル アプリケーション アーキテクチャ	538
実装プロセスのしくみ	542
アプリケーション設定の仕組み	543
ユーザ登録の仕組み	543
モバイル アプリケーションのサポート用に CA Identity Manager を設定する方法	544
必要な属性の設定	545
管理タスクのインポート	548
Web サービス設定の作成	550
登録電子メールの変更	552
モバイル アプリケーションのサポート用に SiteMinder を設定する方法	553
モバイル アプリケーションの設定	555
追加のプロパティの設定	558
モバイル アプリケーションのダウンロード	560
モバイル アプリケーションのトラブルシューティング	561

第 18 章: CA User Activity Reporting 563

CA UAR の機能	563
CA UAR コンポーネント	563
統合の制限	564
CA UAR と CA Identity Manager の統合方法	564
追加の CA UAR レポートまたはクエリと CA Identity Manager との統合	574
[Enterprise Log Manager ビューア] タブの設定	575

第 19 章: アクセス ロール 579

アクセスロールが権限を管理する方法	580
例: 間接的なプロファイル属性の変更	580
アクセス ロールの作成	581
アクセス ロールの作成の開始	581
アクセス ロールのプロファイルの定義	582
アクセス ロールのメンバ ポリシーの定義	582
アクセス ロールの管理ポリシーの定義	583
アクセス ロールの所有者ルールの定義	583

第 20 章: システム タスク 585

デフォルトのシステム タスク	585
フィーダ ファイルでユーザを追加する方法	586
Bulk Loader に関する注意事項	587
フィーダ ファイルの作成	590
[Loader レコード詳細] タブ	591
[Loader アクションマッピング] タブ	592
[Loader 通知詳細] タブ	593
Bulk Loader タスクの変更の認識	593
Bulk Loader タスク用電子メール通知の設定	594
[Bulk Loader] タスクのスケジュール	594
「Bulk Loader」の解析ファイルの変更	595
Bulk Loader の Web サービス サポート	595
JDBC 接続管理	596
JDBC 接続の作成	596
ロジカルアトリビュートハンドラ	596
ロジカルアトリビュートハンドラの作成	597
ロジカルアトリビュートハンドラのコピー	598
ロジカルアトリビュートハンドラ ForgottenPasswordHandler の作成	599
ロジカルアトリビュートハンドラの削除	599

ロジカルアトリビュートハンドラの変更	600
ロジカルアトリビュートハンドラの表示	600
セレクト ボックス データ	600
[相関属性の設定] タスク画面	601
グローバル ポリシー ベースのイベント用ワークフローの設定タスク画面	602
CA Identity Manager のタスク ステータス	603
CA Identity Manager がタスク ステータスを判別するしくみ	604
サブミット済みタスクの表示	605
[ユーザ履歴] タブ	616
サブミット済みタスクのクリーンアップ	622
[反復] タブ	623
[サブミット済みタスクのクリーンアップ] タブ	626
反復タスクの削除	627
Enterprise Log Manager 接続の設定	628
Enterprise Log Manager 接続の削除	629
秘密鍵の管理	630

第 21 章: タスク永続性 631

自動化されたタスクの永続ガベージ コレクションとアーカイブ	631
[反復] タブ	632
[サブミット済みタスクのクリーンアップ] タブ	634
ジョブの即時実行	635
新規ジョブのスケジュール	635
既存のジョブの変更	636
反復タスクの削除	636
タスク永続性データベースの移行方法	637
tpmigration125.properties ファイルの更新	638
JAVA_HOME 変数の設定	638
runmigration ツールの実行	639

第 1 章: ロールの計画

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

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

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

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

上記の質問の回答に基づいて、必要なロールの数と種類を決定します。

このセクションには、以下のトピックが含まれています。

[ロールの決定](#) (P. 17)

[ロールの目的](#) (P. 18)

[追加の管理者の作成](#) (P. 19)

[ロールの特性](#) (P. 23)

[ロールの計画のチェックリスト](#) (P. 34)

ロールの決定

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

ロールの目的

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

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

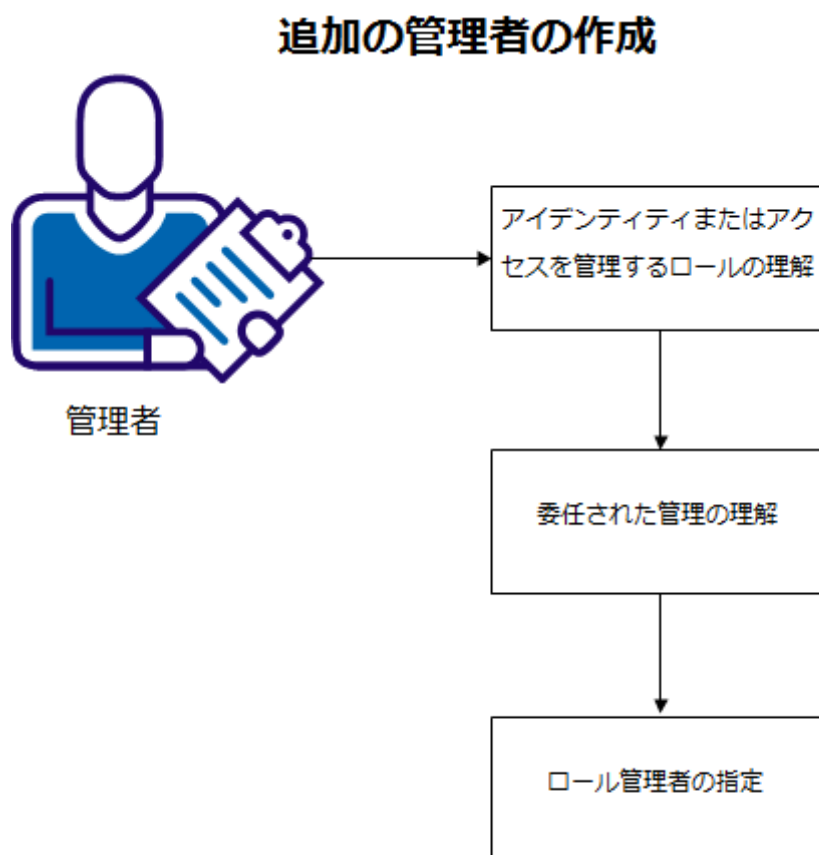
最後の質問は、ユーザの管理業務とアプリケーションへのアクセス付与業務の共有に関するものです。委任モデルの詳細については、「委任された管理」を参照してください。

上記の質問の回答に基づいて、必要なロールの数と種類を決定します。

追加の管理者の作成

システム内でユーザにロールを付与する権限を、1人のユーザが持つようにすることができます。また、追加の管理者を指定して、ユーザへのロール付与作業を分担することも可能です。この方法を、*委任された管理*といいます。

以下の図は、追加の管理者作成ために理解すべき情報、および実行する手順を示します。



以下のトピックでは、追加の管理者を作成する方法について説明します。

- [アイデンティティまたはアクセスを管理するロール](#) (P. 20)
- [委任された管理](#) (P. 20)
- [ロール管理者の指定](#) (P. 21)

アイデンティティまたはアクセスを管理するロール

ユーザアイデンティティおよびそれらの他のアカウントへのアクセスの管理を有効にするため、CA CloudMinder では 2 つのタイプのロールを提供します。管理者ロールを持つユーザは、ユーザ パスワードまたはグループ メンバシップの変更といったユーザ管理が可能です。管理ロールには、ユーザ コンソールに表示される任意のタスクを含めることができます。プロビジョニング ロールを持つユーザは、電子メール システムなどの他のビジネス アプリケーションにアクセスすることができます。

ロールの詳細については、以下のテーブルで概説されています。

ロールの種類	目的
管理ロール	このロールが付与されている場合、ユーザの管理タスクなど、ユーザが CA CloudMinder で実行できる管理タスクが含まれます。
プロビジョニング ロール	電子メール システムなど、管理対象エンドポイントに存在するアカウントを定義するアカウント テンプレートが含まれます。アカウント テンプレートでは、ユーザ属性とこれらのアカウントのマッピング方法も定義できます。
アクセス ロール	アクセス ロールは、CA Identity Manager または他のアプリケーションにおける権限付与の追加的な方法を提供します。たとえば、アクセス ロールを使用して以下の処理を実行できます。 ■ ユーザ属性に間接的なアクセス権を付与する。 ■ 複合式を作成する。 ■ 権限を決定するために別のアプリケーションが使用できる、プロファイル属性を設定する。

委任された管理

委任された管理とは、ロールを使用して、ユーザ管理とアプリケーションへのアクセス権付与の作業を共有することです。

システム内の各ロールについて、ユーザは以下の機能の 1 つ以上を実行することができます。

機能	定義
ロール所有者	ロールを変更します。

機能	定義
ロール管理者	ユーザおよび他のロール管理者へロールを割り当てます。
ロール メンバ	ロールを使用して、管理タスクまたはアクセス タスクを実行するか、エンドポイント アカウントを使用します。

これらの機能を複数のユーザに分配することによって、ロールの管理作業を共有することができます。たとえば、より低いレベルの管理者はロール メンバシップを管理でき、より高いレベルの管理者はロールを変更できるようにすることができます。

委任された管理は、以下の方法で実装できます。

- 該当するロールの管理者として、ユーザを直接指定します。
- ロール用の **管理ルール**を設定します。管理ルールでは、ロールの管理者になることができるユーザを定義します。ユーザがルールに指定された条件を満たす場合、システムは自動的に追加の管理者を作成します。

注: ロールを変更する権限を持つ管理者のみが、そのロール用の管理ルールを設定できます。通常、システム管理者がこの操作を実行します。ロール用の管理を自動的に委任する管理ルールを設定するには、オンライン ヘルプの参照情報内の「管理ロール」セクションを参照してください。

ロール管理者の指定

ロールの管理者としてユーザを指定できます。その後、管理者は他のユーザにロールを割り当てることができます。

次の手順に従ってください:

1. ロールの管理タスクを持つユーザとしてユーザ コンソールにログインします。
2. [タスク] - [ロールおよびタスク] を選択します。
3. 以下のいずれかのタスクを選択します。
 - 管理ロール、管理ロール メンバ/管理者の変更
 - プロビジョニング ロール、プロビジョニング ロール メンバ/管理者の変更
 - アクセス ロール、アクセス ロール メンバ/管理者の変更

検索画面が表示されます。

4. ユーザに割り当てるロールを選択します。

5. [管理者] タブをクリックします。

現在のロール管理者のリストが表示されます。

6. [ユーザの追加] をクリックします。

検索画面が表示されます。

7. 管理者として追加するユーザを検索し、[選択] をクリックします。

ロール管理者の更新されたリストが表示されます。

8. [サブミット] をクリックします。

ユーザはこのロールの管理者になります。これで、プロビジョニング ロールの管理を委任するプロセスが完了します。管理者は、関連するエンドポイント アカウントへのアクセスを付与して、他のユーザにロールを割り当てることができるようになります。

委任の手順

委任された管理が以下のように発生します。

1. 誰がロールの所有者、管理者、またはメンバであるか、というルールを使用して、管理者がロールを作成します。

2. ロールの所有者は、変更が必要になったときにロールを変更します。

3. ロール管理者

- 追加のロール管理者を割り当てます（オプション）。

- 追加のロール メンバを割り当てます（オプション）。

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

4. ロール メンバは次のロールを使用します。

- 管理ロールのメンバは、CA Identity Manager 環境において、ユーザおよび他のオブジェクトを管理します。

- アクセス ロールのメンバは、ビジネス アプリケーションの機能を実行します。

- プロビジョニング ロールのメンバは、そのロールのポリシーで定義されているアカウントを使用します。

委任の例

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

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

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

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

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

ロールの特性

ロールを作成すると、以下の表に示す特性を定義することができます。

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

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

ロール プロファイル

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

ロールのタスク

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

アカウント テンプレート

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

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

メンバ ルール、管理ルール、および所有者ルール

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

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

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

ロールの条件	例	ロールの構文
ユーザは特定のグループに所属する必要があります。	401K グループのメンバであるユーザ	who are members of group <グループ>
ユーザはロールのメンバである必要があります。	ヘルプ デスク ロールのメンバであるユーザ	以下のメンバである <ロール ルール>
ユーザはロール管理者である必要があります。	セールス マネージャ ロール管理者であるユーザ	以下の管理者である<ロール ルール>
ユーザはロールの所有者である必要があります。	ユーザ マネージャ ロールの所有者であるユーザ	以下の所有者である<ロール ルール>
ユーザは、グループの属性により指定される条件を満たすグループに所属している必要があります。	所有者が CIO のグループのメンバであるユーザ	who are members of group <グループ フィルタ>
ユーザは LDAP クエリに基づいた条件を満たす必要があります。	(CA Identity Manager ユーザ コンソールで作成されたクエリが不十分である場合は、LDAP ディレクトリを使用します)	クエリ ldap_query により返されたユーザ

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

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

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

スコープ ルール

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

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

スコープはタスクのプライマリ オブジェクトに適用されます。たとえば、ユーザは「ユーザの作成」タスクのプライマリ オブジェクトです。一方、グループはセカンダリ オブジェクトであるため、スコープはそのユーザのグループには適用されません。

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

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

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

<属性> <コンパレータ><値>

オブジェクトのプロファイルの属性は、指定された値と一致する必要があります。

<属性> <コンパレータ> 管理者の <ユーザ属性>

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

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

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

ルールの条件	例	ルールの構文
ユーザはいずれかの属性値と一致する必要があります。	販売グループのメンバ、または携帯電話が null ではないユーザ	条件 <ユーザ フィルタ>
ユーザは複数の属性値と一致する必要があります。	役職 = マネージャ、かつ地域 = USA であるユーザ	条件 <ユーザ フィルタ>
指定した組織にユーザが所属していなければなりません。	オーストラリアまたはニュージーランドの組織に所属しているユーザ 注: 組織スコープ ルールは、ルールに沿う組織の下位組織に適用されます。たとえば、組織ルールが「Organization1 内」の場合、スコープ ルールは Organization1.1 および Organization1.2 に適用されますが、Organization1 には適用されません。	内<組織ルール>

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

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

ロールの条件	例	ロールの構文
グループは、いずれかの属性値と一致する必要があります。	グループ名 = 401K であるグループ名	条件 <グループ フィルタ>
グループは、指定した組織に所属している必要があります。	会計およびその下位組織に所属しているグループ	内 <組織ルール>
グループは、いずれかの属性値に一致し、かつ指定した組織に所属する必要があります。	ビジネス タイプ = 財務部、および所属組織が販売以下であるグループ	条件 <グループ フィルタ> および所属組織 <組織ルール>

ロールの条件	例	ロールの構文
グループは、管理者の属性に記 載されている必要があります。	説明 = エンジニアリングである グループ	条件 <グループ属性><コン パレータ> 管理者の <ユー ザ属性> 注: 複数値属性では「等しく ない」コンパレータを使用 してください。

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

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

ロールの一般的なガイドライン

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

演算子の評価

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

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

CA Identity Manager は AND ステートメントの前に OR ステートメントを処理します。以下の例について考慮してください。

```
where(company=CA and city=Boston or city=Framingham)
```

この例では、CA Identity Manager はまず (`Boston or Framingham`) を処理し、次に、`company=CA` との論理 AND を実行します。

ルールにおける大文字/小文字の区別なし

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

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

アクションの追加および削除

管理者がロールを与えたり取り消したりしたときに **CA Identity Manager** でロールのメンバシップが正しく管理されるために、[追加アクション] および [削除アクション] を指定する必要があります。

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

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

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

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

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

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

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

メンバポリシー

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

- 最初のポリシーは、ロールメンバで Jones という Manager がいた場合、そのメンバは Sales Office におけるユーザのロールを使用すること、およびそれらのユーザを 401k グループのメンバとして管理できることを表しています。
- 2 番目のポリシーは、ロールメンバが Bend 市にいる場合、そのロールメンバは、Oregon 州のユーザに関するロールを使用すること、およびそれらのロールメンバを、Smith という Group Admin のグループのメンバとして管理できることを表しています。

メンバポリシー

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

管理ポリシー

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

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

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

管理ポリシー

	管理ルール	ユーザ スコープ ルール	メンバの管理	管理者の管理	
①	従業員タイプ = "IT Admin" の場合	市区町村 = "Boston" の場合	☒	☒	+
②	オフィス = "Sales" の場合	都道府県 = "Ohio" の場合	☒	☒	-

ロールの計画のチェックリスト

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

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

ロールの特性	詳細
管理ポリシー	各管理ポリシーを以下のように定義します。 ■ 管理ルール - ユーザをメンバまたは管理者として誰が管理するか ■ スコープルール - 管理者がどのユーザをメンバまたは管理者として管理できるか ■ アクションの追加 - 管理者になったユーザのプロファイルがどうなるか ■ アクションの削除 - 管理者として削除されたユーザのプロファイルがどうなるか
所有者ルール	ロールを変更できるユーザを定義します。

第 2 章：管理ロール

このセクションには、以下のトピックが含まれています。

[管理ロールと管理タスク](#) (P. 37)

[管理ロールの作成](#) (P. 38)

[管理ロールの確認](#) (P. 43)

[ユーザによるロールの自己割り当ての許可](#) (P. 44)

管理ロールと管理タスク

個々のビジネス要件に基づいて、オブジェクト管理のタスクを含むロールを作成します。たとえば、ユーザを管理するタスクを含むロールと、その作成したロールを管理するタスクを含む別のロールを作成します。

また、以下のようなタスクを含むロールを個別に作成します。

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

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

管理ロールと CA Identity Manager 環境

CA Identity Manager 環境にログインすると、ユーザ アカウントには 1 つ以上の管理ロールがあります。各管理ロールには、**CA Identity Manager** 環境で使用する [ユーザの作成] などのタスクが含まれます。

たとえば、中央の **CA Identity Manager** 環境で、管理ロールである **Help Desk**（ヘルプデスク）にパスワードをリセットするタスクが含まれます。ユーザは IT 担当の従業員である必要があるというメンバールールがロールにはあります。IT 担当の従業員が中央の **CA Identity Manager** 環境にログインすると、**Help Desk**（ヘルプデスク）ロールがあり、その **CA Identity Manager** 環境内のユーザのパスワードをリセットできます。

管理ロールとユーザ コンソール

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

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

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

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

管理ロールの作成

ロールの要件を確認したら、管理ロールを作成できます。これらの要件は以下の質問に関係があります。

- このロールを必要とするユーザ
- このロールが管理するオブジェクト
- 管理対象となるオブジェクトのある環境

管理ロールの新規作成

User Console から管理ロールを作成します。

管理ロールを作成する方法

1. 管理ロールを作成するタスクのロールを持つ CA Identity Manager アカウントにログインします。
たとえば、環境の最初のユーザは **System Manager** (システム マネージャ) ロールを持ちます。このロールには [管理ロールの作成] タスクが含まれます。
2. [ロールおよびタスク] - [管理ロール] および [管理ロールの作成] を選択します。
3. ロールを作成するかコピーするかどうかを決定します。
[プロファイル] タブが表示されるので、管理ロールの定義を開始します。
4. 管理ロールのプロファイルを定義します。

管理ロールのプロファイルの定義

[プロファイル] タブで、ロールの基本的な特性を定義します。

プロファイルを定義する方法

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

注: [プロファイル] タブに、管理ロールに関する追加情報を指定するカスタム属性を指定することができます。この追加情報は、多数のロールを含む環境におけるロール検索を簡易化できます。
2. 作成後、すぐにこのロールを使用できるようにする場合は、[有効] を選択します。
3. [ロールの管理タスクを選択します。](#) (P. 40)

ロールの管理タスクの選択

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

管理タスクを選択する方法

1. [カテゴリでフィルタ] フィールドで、カテゴリを選択します。
利用できるタスクのカテゴリを表示するには、下矢印のアイコンをクリックします。
2. [タスクの追加] フィールドでロールに含めるタスクを選択します。
CA Identity Manager により、ロールのタスクのリストにタスクが追加されます。
3. その他に追加するタスクがある場合は、手順 1 および 2 を繰り返します。
4. ロールからタスクを削除するにはそのタスクの [マイナス] アイコン () をクリックします。
5. [管理ロールのメンバ ポリシーを定義します](#) (P. 41)。

管理ロールのメンバポリシーの定義

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

メンバポリシーを定義する方法

1. [追加] をクリックして、メンバポリシーを定義します。メンバポリシーには以下のルールが含まれます。

- ユーザがロールメンバであるための要件を定義したメンバルール。

注: 以下の演算子は、メンバルールの中で数字を文字として扱います。

- より小さい (<)
- 以下 (<=)
- より大きい (>)
- 以上 (=>)

たとえば、「10」は「1」の後、「2」の前です。

- ロールのタスクに使用可能なプライマリオブジェクトとセカンダリオブジェクトを制限するスコープルール。

たとえば、ロールは、ユーザをグループに割り当てることによりユーザを変更するタスクを含みます。その結果、ユーザスコープルールは、検索可能なユーザ（プライマリオブジェクト）を制限し、グループスコープルールは割り当て可能なグループ（セカンダリオブジェクト）を制限します。

注: 1つ以上のスコープの質問に回答を入力してください。スコープルールは、ロールに含まれるタスクで使用できるプライマリおよびセカンダリオブジェクトを制限します。たとえば、ロールは、ユーザをグループに割り当てることによりユーザを変更するタスクを含みます。その結果、ユーザスコープルールは、検索可能なユーザ（プライマリオブジェクト）を制限し、グループスコープルールは割り当て可能なグループ（セカンダリオブジェクト）を制限します。

2. [メンバ] タブにメンバポリシーが表示されていることを確認します。

- ポリシーを編集するには、左側の右矢印記号をクリックします。
- 削除するには、マイナス符号アイコンをクリックします。

3. オプションで [メンバ] タブの [管理者は、このロールのメンバを追加および削除できます。] というチェックボックスをオンにします。これをオフにすると、ユーザはメンバルールに適合するメンバになります。

この機能を有効にすると、画面が拡張します。

4. 拡張された領域で [\[追加アクション\]](#) と [\[削除アクション\]](#) (P. 32) を定義します。これらは、ユーザをロールメンバとして追加または削除する条件を指定します。

重要: 追加アクションについては、定義対象のロールを参照するルールを設定しないでください。たとえば、あるメンバをロール A に含めることによって、ロール A のメンバを作成する追加アクションは定義しないでください。

5. [管理ロールの管理ポリシーを定義します](#) (P. 42)。

管理ロールの管理ポリシーの定義

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

管理ポリシーを定義する方法

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

この機能を有効にすると、画面が拡張します。

2. ロールの管理者権限を持つユーザを追加または削除した場合、拡張された領域で [\[追加アクション\]](#) と [\[削除アクション\]](#) を定義します。
3. 管理ポリシーを定義します。管理ポリシーには、管理ルール、スコープルール、および 1 つ以上の管理者権限が含まれます ([メンバの管理] または [管理者の管理])。

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

4. ポリシーを編集するには、左側にある矢印記号をクリックします。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. [管理ロールの所有者ルールを定義します](#) (P. 43)。

管理ロールの所有者ロールの定義

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

所有者ルールを定義する方法

1. ロールを変更できるユーザを決定する、所有者ルールを定義します。
2. 〔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します。

ロールは使用可能になります。メンバールールの条件に適合しているユーザは環境にログインでき、そのユーザはロールのタスクを使用できます。

管理ロールの確認

次の手順に従ってください：

1. 〔管理ロール〕を選択します。
2. 〔管理ロールの表示〕を選択します。
3. ロールの名前を選択します。

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

ユーザによるロールの自己割り当ての許可

ユーザは特定のロールを自身に割り当てることができます。たとえば、ユーザの作業アイテムを他のユーザに委任できるように、ユーザによる委任マネージャロールの登録を許可することができます。

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

次の手順に従ってください：

1. [ロールの自己管理マネージャ] タスクを以下のように変更します。
 - a. [ロールおよびタスク] - [管理タスクの変更] を選択し、[ロールの自己管理マネージャ] タスクを検索します。
 - b. [タブ] タブを選択します。
タスクに適用されるタブのリストが **CA Identity Manager** に表示されます。
 - c. 編集する [ロールの自己管理マネージャ] タブの横にある右矢印アイコンを選択します。
 - d. 以下のフィールドに値を入力します。

[以下のルールに適合する管理ロールのみ表示]

ユーザが自分に割り当てできるロールを決定するために **CA Identity Manager** で使用する基準を指定します。

新規ルールを追加するには、プラス (+) アイコンをクリックします。

[管理ロール管理者として使えるユーザ]

ユーザが自己割り当てできるロールの管理者を指定します。

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

リスト画面

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

- e. [OK] をクリックした後、[送信] をクリックします。
2. [ロールの自己管理マネージャ] タスクをロールに追加し、その機能を持たせるユーザにロールを割り当てます。

第 3 章：管理タスク

このセクションには、以下のトピックが含まれています。

- [管理タスクの計画](#) (P. 45)
- [管理タスクの使用法オプション](#) (P. 49)
- [デフォルトの管理タスク](#) (P. 50)
- [カスタム管理タスクの作成方法](#) (P. 50)
- [タスクのプロファイルの定義](#) (P. 52)
- [タスク スコープの定義](#) (P. 57)
- [タスクのタブの選択](#) (P. 68)
- [タスクのフィールドの表示](#) (P. 72)
- [使用しているロールの表示](#) (P. 72)
- [イベントへのワークフロー プロセスの割り当て](#) (P. 72)
- [Active Directory ユーザ ストアの管理](#) (P. 73)
- [アプリケーション機能の外部タスク](#) (P. 75)
- [高度なタスク コンポーネント](#) (P. 77)
- [管理タスクおよびイベント](#) (P. 79)
- [管理タスクの処理](#) (P. 81)
- [管理タスクの画像](#) (P. 85)

管理タスクの計画

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

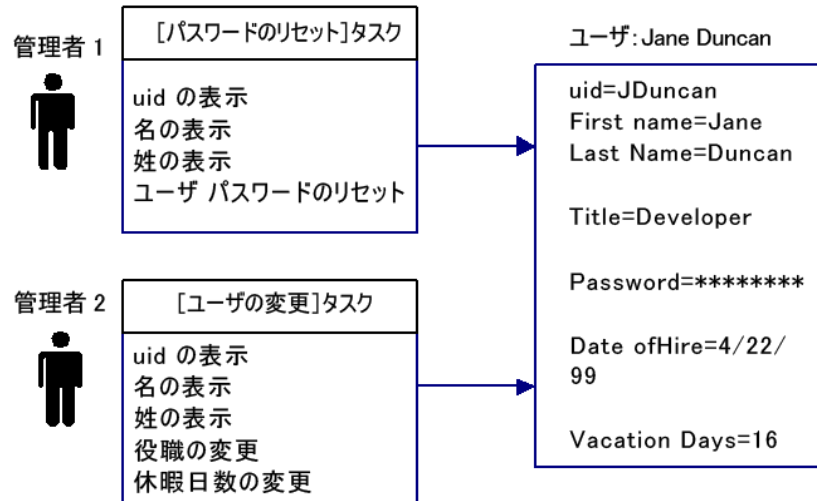
- ユーザの作成
- ユーザの表示
- ユーザの変更
- ユーザ パスワードのリセット

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

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

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

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



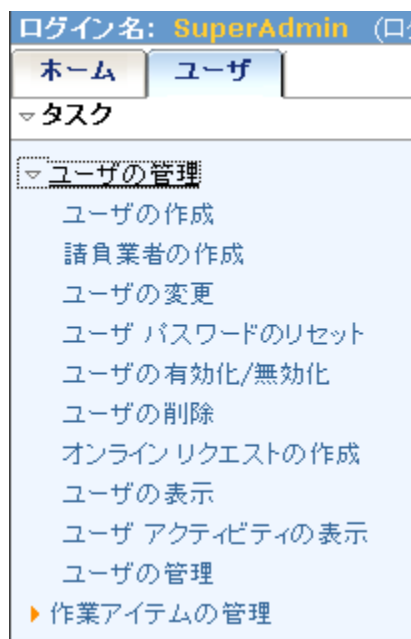
- 管理者 1 は [ユーザ パスワードのリセット] タスクを持っています。この管理者は、従業員のユーザ ID および名前の参照や、パスワードのリセットができます。
- 管理者 2 は [ユーザの変更] タスクを持っています。この管理者は、従業員のユーザ ID および名前の参照や、役職および休日の変更ができます。

管理タスクの例

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

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

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



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

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

作成するタスクについて、含めるタブと、タブの順序および内容を決めます。

ユーザの変更: liang

プロフィール アクセス ロール 管理ロール プロビジョニング ロール グループ

● = 必須項目

組織 Dealer

ユーザ ID liang

有効 ☒

●名 liang

●姓 liang

●フル ネーム liang

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

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

新しいカテゴリである「契約者」の下にこのタスクを作成できます。

ログイン名: SuperAdmin (ログアウト)

ホーム ユーザ 請負業者

▼ タスク

▼ 請負業者の管理
請負業者の変更

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

請負業者の変更: 販売管理者

プロフィール	グループ	請負業者ロール
ユーザ ID 販売管理者		
有効 ☒		
名	販売	
姓	管理者	
電子メール	jhansen@xyz.com	
開始日	2008/05/12	
会社		

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

管理タスクの使用法オプション

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

■ タスクの選択

カテゴリとタスクを選択してから、タスクを適用するオブジェクトを検索します。

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

■ オブジェクトの選択

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

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

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

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

デフォルトの管理タスク

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

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

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

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

カスタム管理タスクの作成方法

管理タスクとは、ユーザが CA Identity Manager で実行できる管理機能です。管理タスクの例には、ユーザの作成、グループの変更、ロール メンバシップの表示などがあります。

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

カスタム管理タスクを作成するときは、以下の手順に従います。

注: セクション「[Active Directory Prerequisites](#) (P. 73)」には、CA Identity Manager で Active Directory ユーザストアを管理する場合の、その他の考慮事項が記載されています。

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

CA Identity Manager によって、新しいタスクを作成するか、既存のタスクを元にしてタスクを作成するかどうかを確認されます。

たとえば、新しいタスクの基礎として [ユーザの変更] タスクを選択します。

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

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

3. [OK] を選択すると、次の 6 つのタブがある画面が表示されます。

タブ	目的	参照するトピック
プロファイル	作成するタスクのプロファイルを定義します	タスクのプロファイルの定義 (P. 52)
検索	タスクで管理するオブジェクトの範囲を制限します	タスク スコープの定義 (P. 57)
タブ	タスクのタブを選択および設計します	タスクのタブの選択 (P. 68)
フィールド	すべてのタブに使用するフィールドを表示します	タスクのフィールドの表示 (P. 72)
イベント	CA Identity Manager 環境でタスクがワークフローを使用する場合は、イベントごとにワークフロープロセスを選択します。	イベントへのワークフロープロセスの割り当て (P. 72)
使用しているロール	変更または表示しているタスクを含むロールが表示されます。	使用しているロールの表示 (P. 72)

注: カスタム管理タスクの作成の詳細については、「[ユーザ コンソール デザインガイド](#)」を参照してください。

タスクのプロファイルの定義

[プロファイル] タブには、タスクの全般的な設定が含まれます。

注: 管理タスク プロファイル設定の詳細については、「[ユーザ コンソール デザインガイド](#)」を参照してください。

タスクのプロファイルを定義する方法

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

注: 既存のタスクとプロファイル設定が似ているタスクを作成する場合、[別のタスクからのプロファイルのコピー] をクリックします。このオプションでは、選択した既存のタスクのプロファイル設定を使用して、作成するタスクのプロファイル設定を指定します。次に、新しいタスクのルールと説明を追加します。

3. （オプション）ビジネス ロジック タスク ハンドラをタスクに関連付けます。
4. このタブの設定が終了したら、次の手順「[タスク スコープの定義](#) (P. 57)」に進みます。

管理タスクの[プロファイル]タブ

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

このタブには以下のフィールドが含まれます。

■ 名前

タスクの名前を定義します。

■ タグ

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

■ 説明

タスクの目的に関するメモを指定できます。

- **タスク順**

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

- **カテゴリ**

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

- **カテゴリ順**

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

- **カテゴリ 2**

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

- **カテゴリ 2 順**

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

- **カテゴリ 3**

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

- **カテゴリ 3 順**

第 3 階層カテゴリの表示順を指定します。

- **プライマリ オブジェクト**

タスクの操作対象であるオブジェクトを指定します。

- **アクション**

オブジェクトで実行される操作を指定します。

■ ユーザの同期

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

- オフ (デフォルト)

このタスクでユーザの同期化はトリガされないことを指定します。

- タスク完了時

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

注: 複数のイベントを含むタスクに対して [タスク完了時] オプションを選択すると、CA Identity Manager では、そのタスク内のすべてのイベントが完了するまでユーザは同期されません。イベントの 1 つまたは複数がワークフローの承認を必要とする場合、その承認に数日かかることがあります。すべてのイベントが完了するまで CA Identity Manager がアイデンティティ ポリシーを適用しないであることを避けるには、[各イベント発生時] オプションを選択します。

- 各イベント発生時

タスク内の各イベントの完了時に、CA Identity Manager で [ユーザの同期化プロセス](#) (P. 496) を開始することを指定します。

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

■ アカウントの同期

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

- オフ (デフォルト)

このタスクでアカウントの同期化はトリガされないことを指定します。

- タスク完了時

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

- 各イベント発生時

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

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

■ メニューで非表示

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

■ パブリック タスク

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ようにします。デフォルトのパブリック タスクは [忘れたパスワード] と [自己登録] です。

■ 監査の有効化

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

■ ワークフローの有効化

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

■ Web サービスの有効化

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

■ ワークフロー プロセス

タスク レベル ワークフローの設定を有効化します。鉛筆のアイコンをクリックして、ポリシーベースまたは非ポリシーベースのワークフローを設定します。

■ タスク優先度

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

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

■ ビジネス ロジック タスク ハンドラ

[ビジネス ロジック タスク ハンドラ](#) (P. 77) をタスクと関連付けます。

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

カスタムのアクション ボタンをワークフローの承認タスクに追加します。

■ 別のタスクからのプロファイルのコピー

他のタスクの [プロファイル] タブからデータをコピーします。

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

タスク設定プロパティ

タスク設定プロパティでは、タスクの表示プロパティおよび特定の動作を制御します。

タスクアイコンパス

タスク リスト内でこのタスクのアイコンとして使用する画像の URL を指定します。

タスクアイコンプレビュー

タスク リスト内に表示される、タスクのアイコンを表示します。

タスク ナビゲーションの抑止

選択すると、ユーザがタスクを選択した後に、トップレベルのナビゲーションおよびタスク リストが非表示になります。これによって、必要なアクションを完了するかタスクをキャンセルするまで、ユーザが現在のタスクから離れてしまうのを防げます。

ターゲット ウィンドウ

このフィールドに値を入力すると、CA Identity Manager の新しいブラウザ ウィンドウにこのタスクが開きます。このフィールドは、ユーザを別の Web サイトにリダイレクトする外部タスク用に、新規ブラウザ ウィンドウを開くために使用します。

任意のウィンドウ名を指定できます。

注: このフィールドは、CA Identity Manager 管理タスクを別のブラウザ ウィンドウで開くためには使用しないでください。CA Identity Manager では、1 つの CA Identity Manager ユーザ セッションでの複数のブラウザ ウィンドウをサポートしていません。

タスク スコープの定義

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

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

[検索] タブで以下のように設定します。

検索画面

検索画面では、フィルタに基づいてタスクのスコープを制限します。

[参照] をクリックして、使用できる検索画面オプションを表示します。

注: [独自の検索画面](#) (P. 58)を作成できます。既存の検索画面の変更バージョンを作成するには、検索画面を選択し、[コピー] をクリックします。元の検索画面定義を変更することなく、検索画面を変更できます。検索画面を作成するには、[新規] をクリックします。

検索オプション

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

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

以下の点に注意してください。

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

変更されたオブジェクトは、管理者のスコープ内に残す必要があります。

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

検索画面設定

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

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

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

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

検索フィルタ

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

検索用に以下のフィールドを設定できます。

[以下のルールに適合するオブジェクトのみ表示]

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

このフィールドを使用するときは、以下の点に注意してください。

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

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

削除しない場合は、ユーザが入力した条件は無視されます。

[デフォルトの検索フィルタ]

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

[複数選択タスクで使用時にすべての検索結果を自動選択]

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

[自動的に検索を実行]

検索フィールドに検索結果が表示されるように指定します。

[単一の検索結果しかない場合、タスクの対象を自動的に設定]

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

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

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

[検索フィルタの保存]

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

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

[組織内の検索]

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

[組織検索の保存]

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

[組織検索]

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

[デフォルトの組織検索スコープ]

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

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

[単一式による検索]

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

[等号のみの検索]

管理者に「=」以外の検索演算子の使用を禁止します。

[結果の件数の表示]

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

[次に対しタスク ボタンを追加] `<task name>`

別のタスクへのリンクを検索画面に追加します。リンクはボタンとして表示されます。

通常、このフィールドは、オブジェクト タスク ナビゲーションに設定されている検索画面に [作成] タスクを追加するために使用されます。

[オプションのラベル]

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

[次に対し複数削除ボタンを追加] <task name>

管理者が複数オブジェクトを選択して削除できるタスクへのリンクを追加します。リンクはボタンとして表示されます。

通常、このフィールドは、オブジェクトタスク ナビゲーションと共に使用します。

検索フィールドと検索結果

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

[ユーザが検索可能なフィールドを選択]

管理者が検索クエリの作成に使用するフィールドを選択します。

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

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

注: 検索対象フィールドが指定されなかった場合、自動的に検索が開始されます。

検索結果に表示されるフィールドの選択

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

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

スタイル

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

■ 論理値の表示名

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

- **チェックマーク**

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

- **複数値文字列**

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

- **読み取り専用チェックボックス**

値を読み取り専用チェックボックスとして表示します。

- **文字列**

値をテキスト文字列として表示します。

■ タスク

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

この設定を使用して、属性値をタスクへのリンクとして表示することもできます。

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

■ タスク リスト

検索画面とリスト画面内のオブジェクトでユーザが実行できるタスクを追加します。たとえば、[ユーザの変更] タスクの検索画面で、検索によって返されたユーザ リストから、ユーザの無効化などのタスクをユーザが実行できるように設定できます。

このオプションを選択する際、ユーザのアクセス方法をアイコンのクリックにするかテキスト リンクにするかを決定します。

■ タスク メニュー

ポップアップ メニュー アイテムとしてタスク（タスク リストに似たスタイル）を追加します。

このオプションを選択すると、検索画面またはリスト画面の各オブジェクトの横に[アクション] ボタンが表示されます。ユーザは、[アクション] ボタンをクリックして、そのオブジェクトに対して実行できるタスクのリストを表示します。

注: [タスク リスト] および [タスク メニュー] スタイル オプションを表示するには、検索結果テーブルにフィールドを追加する際に [(セパレータ)] を選択します。検索画面およびリスト画面へのタスクの追加の詳細については、「ユーザ コンソール デザイン ガイド」を参照してください。

並べ替え可能

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

検索結果のデフォルトの並べ替え順の設定

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

[フィールドが変更されたオブジェクトの選択] の名前

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

返す数 N (各ページ)

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

検索画面のユーザ定義ヘルプ

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

- ページの先頭または末尾
- 作成の前または後
- 結果の前または後

検索画面のタイプ

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

アクセス ロール検索画面

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

アクセス タスク検索画面

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

管理ロール検索画面

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

管理タスク検索画面

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

承認検索画面

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

証明書開始ユーザ検索画面

証明書開始ユーザ検索画面を使用すると、証明書が必要と設定するユーザを見つける検索フィルタを設定できます。選択されたユーザは、証明書のステータスが*証明書が必要*に設定されます。

認証ユーザの検索画面

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

委任検索画面

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

ユーザの有効化/無効化の検索画面

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

証明書終了ユーザ検索画面

証明書終了ユーザ検索画面を使用すると、証明書のサイクルが完了したユーザを特定する検索フィルタを設定できます。

エンド ユーザ使用許諾契約の検索画面

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

検索および関連付け検索

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

フィーダ ファイル アップロード検索画面

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

忘れたパスワードの検索画面/忘れたユーザ ID の検索画面

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

グループ検索画面

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

アイデンティティ ポリシー セット検索画面

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

ロジカル アトリビュート ハンドラ検索画面

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

レポート管理検索画面

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

証明されていないユーザ検索画面

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

組織検索画面

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

プロビジョニング ロール検索画面

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

アカウントテンプレート検索画面

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

パスワードポリシー検索画面

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

スナップショット定義検索画面

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

標準検索画面

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

ユーザ検索画面

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

［検索］タブに入力してから、タスクのタブを選択します。

タスクのタブの選択

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

- プロファイル
- アクセス ロール
- 管理ロール
- グループ
- 作業アイテムの委任

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

[アカウント]タブ

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

アカウント詳細

今すぐアクションを実行するアカウント名をクリックします。

選択	名前	エンドポイント タイプ	エンドポイント	一時停止	ロック済み
☒	 ken	Windows NT	iam-fw-wl10		

アカウントの作成

選択したアカウントに対するアクション

アカウントのリフレッシュ	一時停止	再開	ロック解除	パスワードの変更	割り当て解除	割り当て	削除

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

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

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

[アカウント]タブを使用するための前提条件

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

注: 環境にプロビジョニング サポートを設定するには、「[設定ガイド](#)」を参照してください。

[アカウント]タブのフィールド

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

特に重要なテーブルは以下のとおりです。

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

[アカウント]タブのその他の機能

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

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

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

[スケジュール]タブ

スケジューリングで、今後の日付を指定してタスクの実行を自動化できます。ワークフローに関連付けられたタスクをスケジュールする場合は、**CA Identity Manager** はワークフローで定義されたタスクをすべて実行します。スケジュール済みタスクのステータスは、[サブミット済みタスクの表示] ページに表示できます。

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

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

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

管理タスクへの[スケジュール]タブの追加

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

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

[スケジュール]タブを管理タスクに追加する方法

1. [ロールおよびタスク] - [管理タスク] - [管理タスクの変更] をクリックします。
[管理タスクの選択] 画面が表示されます。
2. [条件] フィールドで [名前] または [カテゴリ] を選択し、検索文字列を入力して [検索] をクリックします。
検索基準を満たす管理タスクが表示されます。
3. 管理タスクを選択し、[選択] をクリックします。
選択した管理タスクのタスクの詳細が表示されます。
4. タブをクリックします。
選択した管理タスク用に設定されたタブが表示されます。

5. [このタスクで表示する必要があるのはどのタブですか] ドロップダウンからスケジュールを選択し、 をクリックします。
[スケジュール] タブは、選択した管理タスクに表示されるタブのリストに追加されます。
6. [サブミット] をクリックします。
[スケジュール] タブは、選択した管理タスクに追加されます。

タスクのフィールドの表示

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

このタブの設定が終了したら、次の手順「[イベントへのワークフロープロセスの割り当て \(P. 72\)](#)」に進みます。

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

使用しているロールの表示

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

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

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

イベントへのワークフロー プロセスの割り当て

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

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

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

Active Directory ユーザストアの管理

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

sAMAccountName 属性

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

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

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

詳細については、「[Java のプログラミングガイド](#)」のロジカル アトリビュートの章を参照してください。

グループのタイプとスコープ

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

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

各タイプのグループには、以下を決定するスコープがあります。

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

各タイプのグループは、以下のスコープのいずれかを持つことができます。

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

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

異なるタイプのグループを作成するために、カスタムのロジカルアトリビュートハンドラを作成できます。「*Java のプログラミングガイド*」のロジカルアトリビュートに関する章を参照してください。

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

アプリケーション機能の外部タスク

外部タスクでは以下が実行されます。

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

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

新規ブラウザ ウィンドウでアプリケーションを開くか、または **CA Identity Manager** 管理タスク内のタブとして、外部タスクを表示できます。

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

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

[外部]タブ

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

[外部] タブの場合

- 外部タスクに対して生成されるイベントはありません。
- オプションで管理オブジェクトを使用できます。

- [外部 URL] フィールドで、アプリケーションのアドレスを以下のように指定できます。
 - 完全なアドレス。完全修飾ドメイン名を含みます。たとえば以下のように指定します。
`http://server1.mycompany.org/report/viewUserReport`
 - 相対パス。たとえば以下のように指定します。
`/report/viewUserReport`
相対パスを指定すると、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が自動的に追加されます。
- [プロファイル] タブ上のアプリケーションに渡す属性を設定します。
- URL には管理者 DN またはタスク名を含めることも除外することもできます。

[外部 URL] タブ

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

[外部 URL] タブの場合

- [外部 URL] タブはタスクの唯一のタブである必要があります。 同じタスクに関連付けられた他のタブがある場合、外部タブはユーザを指定された URL にリダイレクトしません。
- タスクで、監査可能なイベントを生成できます。
- [外部 URL] フィールドで、アプリケーションのアドレスを以下のように指定できます。
 - 完全なアドレス。完全修飾ドメイン名を含みます。以下に例を示します。
`http://server1.mycompany.org/report/viewUserReport`
 - 相対パス。たとえば以下のように指定します。
`/report/viewUserReport`
相対パスを指定すると、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が自動的に追加されます。
- オプションで管理オブジェクトを使用できます。
- URL に渡す属性を設定できます。
開始するアプリケーションの URL を提供し、アプリケーションに渡す属性を含めます。
- URL には管理者 DN またはタスク名を含めることも除外することもできます。

高度なタスクコンポーネント

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

- 「タスクレベルの検証」で、タスクの他の属性に対して属性値を検証します。たとえば、ユーザ指定の電話番号のエリアコードが、ユーザの市区町村と都道府県に適切かどうか検証します。
- [ビジネスロジックタスクハンドラ](#) (P. 77) では、CA Identity Manager タスクのプロセスをサブミットする前に、カスタムのビジネスロジックが実行されます。通常、カスタムのビジネスロジックでデータが検証されます。たとえば、CA Identity Manager が新しいメンバをグループに追加する前に、ビジネスロジックタスクハンドラを使用して、グループメンバシップの限度を確認できます。グループメンバシップが限度に達している場合、ビジネスロジックタスクハンドラによって、新しいメンバを追加できなかったことをグループ管理者に知らせるメッセージが表示されます。

ビジネスロジックタスクハンドラの作成

ビジネスロジックタスクハンドラの完全修飾クラス名を以下のように定義します。

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

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

3. [追加] をクリックします。

[ビジネスロジックタスクハンドラの詳細] 画面が表示されます。

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

名前

ビジネスロジックタスクハンドラに割り当てる名前。

説明

オプションの、ビジネスロジックタスクハンドラの説明。

Java クラス

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

`com.mycompany.MyJavaBLTH`

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

JavaScript ファイル名

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

CA Identity Manager は、このファイルがカスタム **JavaScript** ファイル用のルート ディレクトリにあると想定します。**JavaScript** ファイルの展開の詳細については、「*Java のプログラミングガイド*」を参照してください。

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

`JavaScriptSubDir¥MyJavaScriptBLTH.js`

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

JavaScript

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

プロパティと値

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

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

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

管理タスクおよびイベント

管理タスクにはイベント (CA Identity Manager がタスクを完了するために実行するアクション) が含まれます。1つのタスクには、複数のイベントが含まれている場合があります。たとえば、[ユーザの作成] タスクには一般に、ユーザプロフィー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。

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

プライマリ イベントおよびセカンダリ イベント

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

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

タスクのイベントの表示

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

タスクのイベントの表示方法

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

現在のタスクに関連付けられたイベントが表示されます。

未変更のプロファイルに生成されるイベント

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

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

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

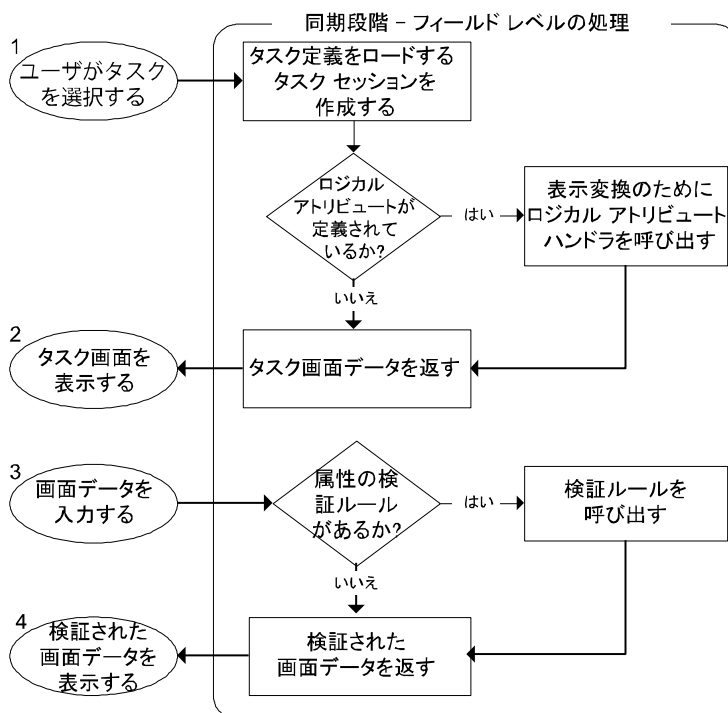
管理タスクの処理

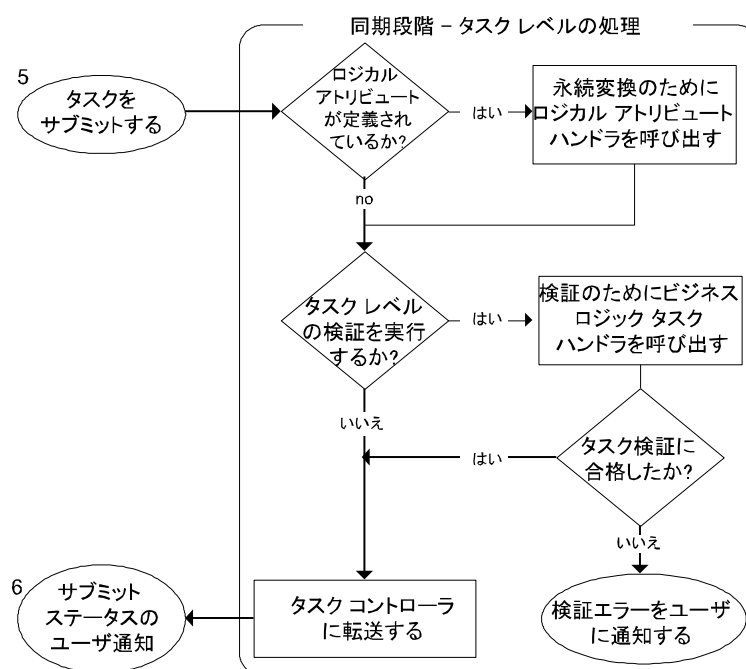
タスクの処理にかかる時間は、実行する手順によって変わります。タスクの処理がサブミットされると、CA Identity Manager では以下の手順が実行されます。

1. サブミットされたデータが検証されます。
これを *同期段階* と呼びます。
2. タスクに承認が必要な場合、CA Identity Manager からワークフロー エンジンにタスクが送信されます。
 - a. ワークフロー エンジンで承認者が決定され、承認者のワーク リストに承認タスクが設定されます。
 - b. オプションで、保留中の作業アイテムについて、CA Identity Manager から承認者に通知の電子メールが送信されます。
 - c. 承認者は作業アイテムを予約し（この項目は他の承認者のワーク リストから削除されます）、項目を承認または拒否します。
 - d. オプションで、タスクのステータスについて、関係するユーザに通知の電子メールが送信されます。
これを *非同期段階* と呼びます。
3. タスクが拒否されなかった場合、CA Identity Manager でタスクが実行されます。

同期段階の処理

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

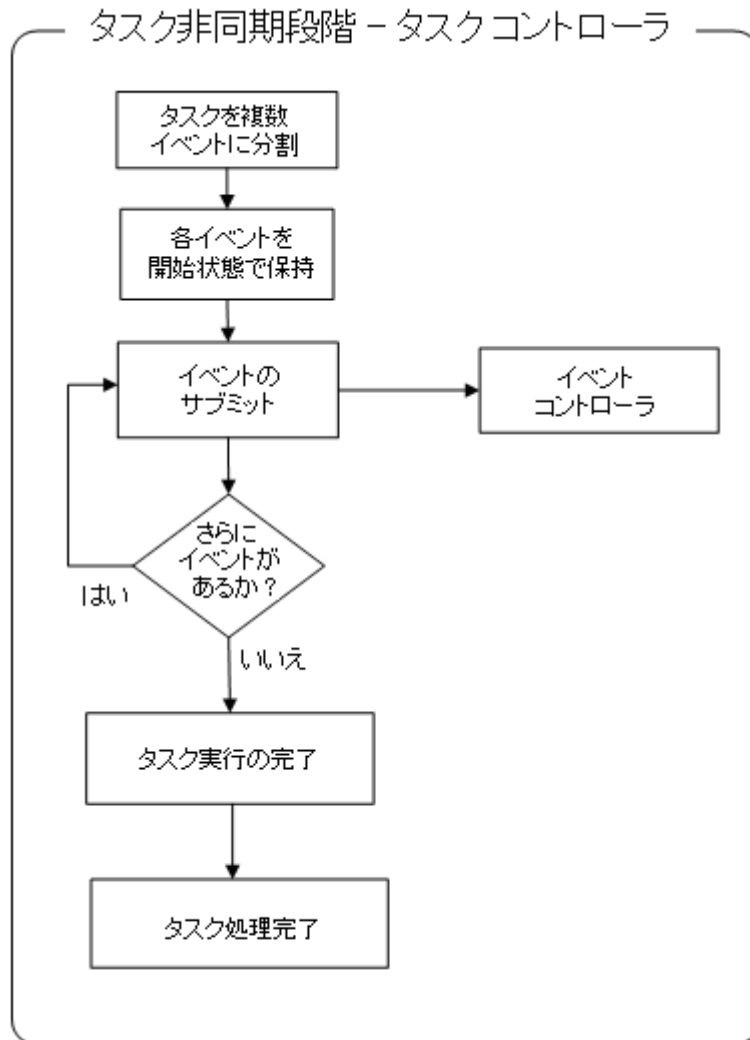




非同期段階の処理

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

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



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

通常、イベントは、次の段階を遷移します。

- 開始
- 保留中
- 承認済み
- 実行
- 完了
- ポスト

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

管理タスクの画像

ホーム ページに配置する管理タスク用の画像を作成できます。

第 4 章：ユーザ

このセクションには、以下のトピックが含まれています。

[ユーザの作成](#) (P. 87)

[ユーザへの自己登録の許可](#) (P. 92)

ユーザの作成

管理者は、ユーザ プロファイルでユーザ情報（権限、アプリケーション、およびサービスへのアクセス）を管理することができます。また、ユーザが自身のアカウントおよびサービスを自己管理する権限も付与できます。ユーザ プロファイルの作成は、システム管理者の共通タスクです。

ユーザを作成して設定する際は、ユーザ アカウントに関する以下の要素を考慮します。

セルフサービス タスク： ユーザ プロファイルは、デフォルトで、ユーザのパスワードやプロファイル情報の変更といった特定のセルフサービス タスクへのアクセス権が付与されるように設定されています。適切なタスクを持つシステム管理者は、ユーザにデフォルトで付与するセルフサービス タスクを変更できます。

グループ： グループはロール管理を簡略化します。たとえば、適切なタスクを持つシステム管理者は、グループのメンバとして追加されるユーザに複数のロールを自動的に割り当てるように、システムを設定できます。

管理ロール： 管理ロールは、ユーザがユーザ コンソールで実行できるタスクを定義します。たとえば、あるタスクでは、ユーザがアドレスや職位などのユーザ アカウント情報を変更できるようにします。また別のタスクでは、ユーザが、グループのユーザ メンバシップ付与のようなタスク管理をできるようにします。ユーザに管理ロールを割り当てると、そのユーザはそのロールに関連付けられたタスクを実行できます。

エンドポイント アカウントとプロビジョニング ロール：他のシステムに存在するアカウントはエンドポイント アカウントと呼ばれます。プロビジョニング ロールによって、CA CloudMinder エンドポイント内のアカウントをユーザに割り当てることができます。たとえば、電子メールの Exchange アカウント、データベース アクセスの Oracle アカウント、および Windows システムを使用する Active Directory アカウントが必要な場合を想定します。ユーザにプロビジョニング ロールを割り当てると、ユーザはプロビジョニング ロールが指定するエンドポイント アカウントを受信します。

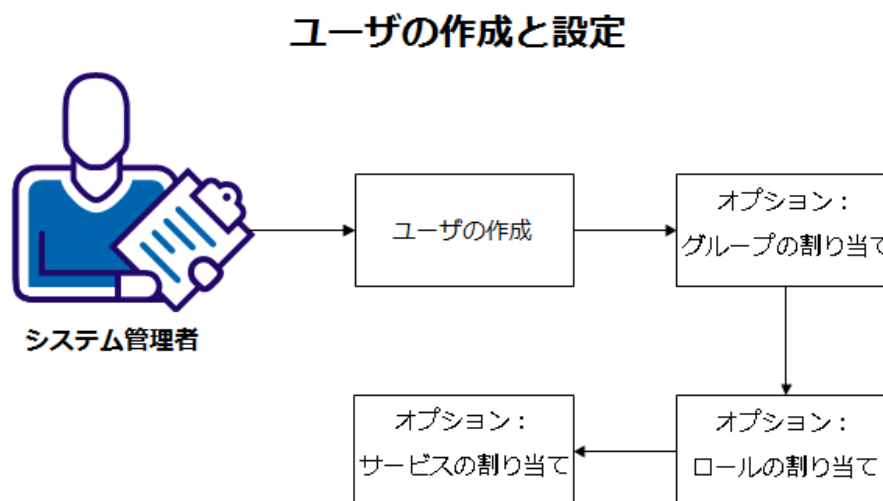
アクセス ロール：アクセス ロールは、CA Identity Manager または他のアプリケーションにおける権限付与の追加的な方法を提供します。たとえば、アクセス ロールを使用して以下の処理を実行できます。

- ユーザ属性に間接的なアクセス権を付与する
- 複合式を作成する
- 権限を決定するために他のアプリケーションで使われる、ユーザ プロファイルの属性を設定する

サービス：サービスを使用すると、ユーザが選択したユーザのタスク、ロール、グループ、および属性を1つのパッケージに統合することができます。この権限のパッケージは、セットとして管理できます。たとえば新しい販売担当者は全員、定義済みのタスク セット、特定のエンドポイント システム上のアカウント、およびユーザ アカウント プロファイルに追加された情報へのアクセスを必要とします。ユーザにサービスを割り当てると、そのユーザはサービスが指定するロール、タスク、グループ、およびアカウント属性のセット全体を受信します。

パスワード ポリシー：ポリシーでは、ルールと制限を適用し、パスワードの有効期限、構成、および使用方法を管理することで、ユーザ パスワードを管理します。システム管理者がユーザの環境のパスワード ポリシーを作成した場合、それらのポリシーは、1つ以上のパスワード ポリシー ルールに一致する新規ユーザに自動的に適用されます。適切なタスクを持つシステム管理者は、パスワード ポリシーを変更できます。

以下の図は、ユーザを作成して設定するために理解すべき情報、および実行する手順を示します。



以下のトピックでは、ユーザの作成と設定方法について詳細に説明します。

1. [ユーザの作成。](#) (P. 89)
2. [グループの割り当て。](#) (P. 90) (必要な場合)
3. [ユーザへのロールの割り当て。](#) (P. 90) (必要な場合)
4. [サービスの割り当て。](#) (P. 91) (必要な場合)

ユーザ プロファイルの作成

この手順を使用して、ユーザのプロファイルを作成します。[ユーザの作成] タスクの設定によっては、このタスクを使用して追加のプロファイルエレメントを定義することができます。ユーザをグループに追加したり、ユーザを管理ロールまたはプロビジョニング ロールのメンバにすることができます。

次の手順に従ってください：

1. ユーザの管理タスクを持つユーザとしてユーザ コンソールにログインします。
デフォルトの [ユーザ マネージャ] ロールは、適切なタスクを付与します。
2. [タスク] - [ユーザ] - [ユーザの管理] - [ユーザの作成] を選択します。
[ユーザの作成] タスクが開きます。

3. 必要に応じて、ユーザ プロファイル情報のフィールドに入力します。
4. [次へ] をクリックします。
5. 該当する場合は、タスク内のその他のタブのフィールドに入力します。
たとえば、ユーザをグループに追加したり、ユーザに対して管理ロール、プロビジョニング ロール、またはサービスを割り当てます（これらのオプションが利用可能な場合）。
6. [完了] をクリックします。
ユーザが作成されます。

ユーザへのグループの割り当て

ユーザをグループのメンバとすることができます。

次の手順に従ってください:

1. ユーザの管理タスクを持つユーザとしてユーザ コンソールにログインします。
2. [タスク] - [グループ] - [グループ メンバの変更] を選択します。
管理できるグループのリストが表示されます。
3. グループを選択し、[選択] をクリックします。
グループに割り当てられたユーザのリストが表示されます。
4. [ユーザの追加] をクリックします。
5. グループを割り当てるユーザを検索します。
自分が管理者権限を持つすべてのユーザのリストを表示するには、検索条件を変更せずに [検索] をクリックします。
6. ユーザを選択し、[選択] をクリックします。
グループに割り当てられたユーザの更新されたリストが表示されます。
7. [サブミット] をクリックします。
指定されたユーザがグループのメンバになります。

ユーザへのロールの割り当て

個々のユーザにプロビジョニング ロールを割り当てることができます。

次の手順に従ってください:

1. [プロビジョニング ロール メンバ/管理者の変更] タスクを持つユーザとしてユーザ コンソールにログインします。
2. [ロールおよびタスク] を選択します。
3. 以下のいずれかのタスクを選択します。
 - 管理ロール、管理ロール メンバ/管理者の変更
 - プロビジョニング ロール、プロビジョニング ロール メンバ/管理者の変更
 - アクセス ロール、アクセス ロール メンバ/管理者の変更

検索画面が表示されます。

4. ユーザに割り当てるロールを選択します。
[メンバシップ] タブが表示されます。
5. [ユーザの追加] をクリックします。
6. ロールを割り当てるユーザを検索します。
自分が管理者タスクを持つすべてのユーザのリストを表示するには、検索条件を変更せずに [検索] をクリックします。
7. ユーザを選択し、[選択] をクリックします。
8. [サブミット] をクリックします。
指定したロールがユーザに割り当てられます。

ユーザへのサービスの割り当て

個別のユーザにサービスを直接割り当てることができます。このユーザはサービスのメンバになります。

次の手順に従ってください:

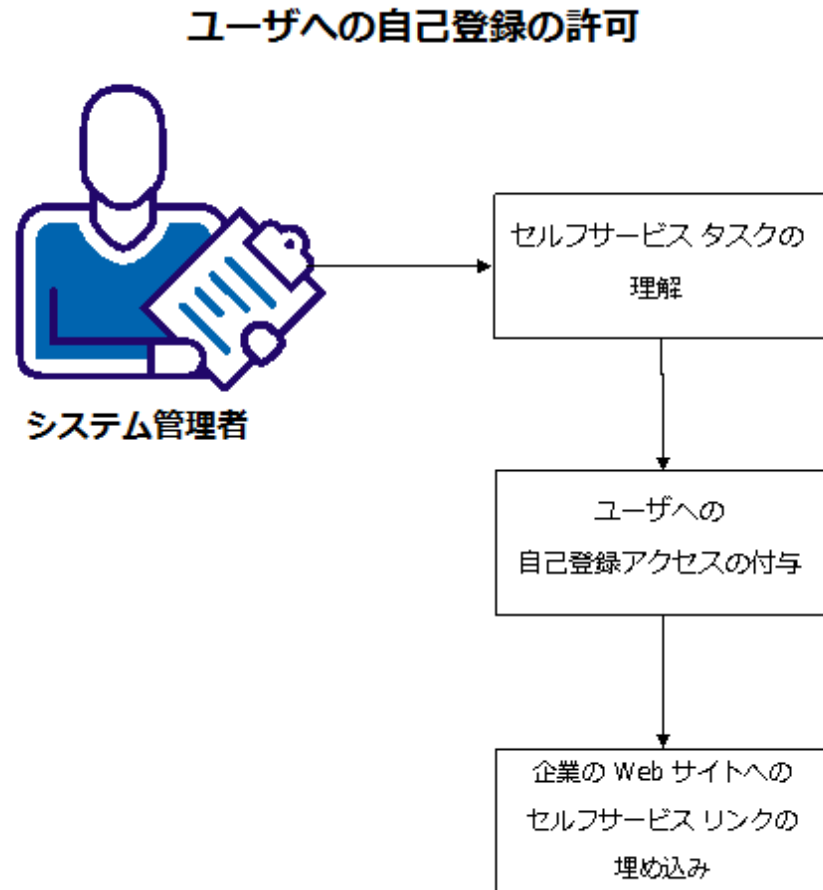
1. [サービス] - [アクセスをリクエスト/表示] に移動します。
管理できるサービスのリストが表示されます。
2. ユーザに割り当てるサービスを選択し、[選択] をクリックします。
サービスに割り当てられたユーザのリストが表示されます。
3. [アクセスをリクエスト] をクリックします。
4. サービスを割り当てるユーザを検索します。
自分が管理者権限を持つすべてのユーザのリストを表示するには、検索条件を変更せずに [検索] をクリックします。

5. ユーザを選択し、[選択] をクリックします。
サービスに割り当てられたユーザの更新されたリストが表示されます。
6. [変更の保存] をクリックします。
ユーザは指定されたサービスを受信します。ユーザは、サービスに含めたアプリケーション、ロール、グループおよび属性をすべて受信します。

ユーザへの自己登録の許可

セルフ サービス タスクは、ユーザが自分の環境を管理することを可能にします。
[自己登録] タスクを使用すると、ユーザは、一般に利用可能なユーザ コンソールから自身のユーザ アカウントおよびプロフィールを作成することができます。たとえば、**Bentley Cola** は、新入社員および顧客が **Bentley Cola** の企業 Web サイトの埋め込みリンクを使用して自身のユーザ アカウントとプロフィールを作成できるようにします。

以下の図は、ユーザによる自己登録を可能にするために理解すべき情報、および実行する手順を示します。



以下のトピックでは、ユーザに自己登録アクセスを付与する方法について説明します。

1. [セルフサービス タスクの理解。](#) (P. 94)
2. [ユーザへの自己登録アクセスの付与。](#) (P. 95)
3. [企業の Web サイトへのセルフサービス リンクの埋め込み。](#) (P. 95)

セルフサービス タスク

セルフ サービス タスクとは、自分のプロフィールを管理するために、（通常はユーザ コンソールを使用して）ユーザが実行できるアクションです。ユーザ アカウントは、デフォルトで、ユーザのパスワードやプロフィール情報の変更といった特定のセルフサービス タスクへのアクセス権が付与されるように設定されています。適切な権限を持つシステム管理者は、ユーザにデフォルトで付与するセルフサービス タスクを変更できます。

セルフサービス タスクには以下の 2 種類があります。

- パブリック タスク：ユーザがログイン認証情報を提供せずに使用できるタスクです。パブリック タスクの例は、自己登録、忘れたパスワード、忘れたユーザ ID のタスクです。
- 保護タスク：ユーザによる有効な認定情報の入力が必要なタスクです。例として、パスワードまたはプロフィール情報の変更タスクなどがあります。

以下の表では、デフォルトのセルフ サービス タスクのリストを示します。

タスク タイプ	タスク
パブリック タスク	■ 自己登録：ユーザが企業の Web サイトに登録することができます。 ■ 忘れたパスワードのリセット：ユーザが忘れたパスワードをリセットできます。 ■ 忘れたパスワード：CA Identity Manager にログインするときにユーザが使用できる一時パスワードを表示します。ユーザがログインすると、新しいパスワードの入力が求められます。 ■ 忘れたユーザ ID：忘れたユーザ ID を取得またはリセットします。
保護タスク	■ アクセスをリクエスト/表示：ユーザがサービスへのアクセスおよび削除をリクエストできます。 ■ マイパスワードの変更：ユーザがパスワードをリセットできます。 ■ マイプロフィールの変更：住所および電話番号などのプロフィール情報を保守します。 ■ マイグループの変更：ユーザがグループに参加することができます。 ■ マイロールの表示：ユーザのロールを表示します。 ■ サブミット済みタスクの表示：ユーザが開始した CA Identity Manager タスクを表示します。

セルフサービス タスクへのアクセス

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

セルフサービス タスクの URL は、以下のようなフォーマットになります。

`https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=task_tag`

各項目の説明：

- *domain* は、CA CloudMinder が実行されている環境内の Web サーバの完全修飾ドメイン名です。
- *public_alias* は、環境のパブリックエイリアスです。環境の作成時、システム管理者はパブリックエイリアスを定義します。
- *task_tag* は、タスクの一意の識別子

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

`https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=ForgottenPasswordReset`

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

`https://domain/iam/im/public_alias/ui7/index.jsp?task.tag=ForgottenUserID`

企業の Web サイトへのセルフサービス リンクの埋め込み

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

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

```
<A  
href="http://domain/iam/im/public_alias/ui7/index.jsp?task.tag=tasktag&task.RedirectURL=http://domain/redirect_URL">link text</A>
```

ドメイン

CA Identity Manager が実行されている環境内の Web サーバの完全修飾ドメイン名です。

public_alias

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文字列。

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

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

tasktag

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

redirect_URL

タスクをサブミットした後の移動先の URL。

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

link text

ターゲット URL にアクセスするためにユーザがクリックするテキスト。

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

以下の HTML は、リンク テキストの例です。

```
<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/welcome.html">Reset My Password</A>
```

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

```
<A href="http://domain/iam/im/public_alias/ui7/index.jsp?task.tag=tasktag&task.RedirectURL=RefererURL">
```

複数のセルフサービス タスクの設定

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

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

以下の図に、新しい従業員および顧客の個別の自己登録タスクを示します。

従業員の自己登録

● = 必須

へようこそ MyCompany.com！私たちのチームに参加いただきありがとうございます。

●名

●姓

●パスワードの入力

●パスワードの再入力

セキュリティの質問 1

回答 1

電子メール

送信

キャンセル

お客様の自己登録

● = 必須

に 関心をお寄せいただきありがとうございます MyCompany.Com！ 当社の 製品を受信する 情報 については、以下の 情報を提供してください:

●名

●姓

会社

タイトル

↓

↑

●パスワードの入力

●パスワードの再入力

セキュリティの質問 1

回答 1

電子メール

送信

キャンセル

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

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

たとえば、以下のように2つのタスクを作成できます。

タスク	タグ	URL
新しい従業員として登録	selfregistration_employee	http://domain/iam/im/alias/index.jsp?task.tag=SelfRegistration_employee
顧客として登録	selfregistration_customer	http://domain/iam/im/alias/index.jsp?task.tag=SelfRegistration_customer

自己管理ロールへのアクセス制限

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

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

第 5 章: パスワード管理

このセクションには、以下のトピックが含まれています。

[CA Identity Manager のパスワード管理](#) (P. 101)

[パスワードポリシーの概要](#) (P. 102)

[パスワードポリシーの作成](#) (P. 103)

[パスワードポリシーの管理](#) (P. 119)

[パスワードポリシーとリレーショナルデータベース](#) (P. 119)

[CA Identity Manager と SiteMinder の統合パスワード基準](#) (P. 119)

[パスワードのリセットまたはアカウントのロック解除](#) (P. 120)

[エンドポイント上でのパスワードの同期](#) (P. 131)

CA Identity Manager のパスワード管理

CA Identity Manager は、以下のようなユーザ パスワードを管理する機能を備えています。

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

- エンドポイント アカウントのパスワードの同期：パスワードの変更は **CA Identity Manager**、プロビジョニング サーバ、およびこのサーバのターゲット システムで同期されます。新しいパスワードは、**CA Identity Manager** パスワード ポリシーに対して検証されます。

パスワードポリシーの概要

パスワードポリシーは、複数のルールと制限のセットです。これらのルールにより、パスワードの作成および有効期限を指定します。**CA Identity Manager** 環境のパスワードポリシーを設定すると、このポリシーは、この環境に関連付けられたユーザストアに適用されます。ユーザディレクトリが、複数の環境に関連付けられている場合、ある環境で定義したパスワードポリシーを別の環境にも適用することができます。

パスワードポリシーでは、以下の設定を行うことができます。

注：これらの設定の一部では、特定の属性についてユーザディレクトリ マッピングを必要とします。「[追加パスワードポリシーの有効化 \(P. 104\)](#)」を参照してください。

- 特定のユーザセットへのパスワードの適用
- パスワードの有効期限：経過日数や失敗したログイン試行回数など、パスワードを期限切れにするイベントを定義します。パスワードが期限切れになると、ユーザアカウントが無効になります。
- パスワードの構成：新しいパスワードの内容の要件を指定します。たとえば、8 文字以上で数字と英字が含まれているパスワードを作成しなければならないように設定できます。
- 正規表現：有効なパスワードの形式を決定する式を提供します。パスワードがその形式に一致するかどうかを指定することができます。複数の正規表現を指定することもできます。
- パスワード制限：パスワードの再使用に関する制限を設定します。たとえば、90 日間経過しないと同一パスワードを再使用できないように設定できます。
- パスワードの詳細オプション：パスワードを処理する前にパスワードを小文字にするなど、**CA Identity Manager** が実行するアクションを指定します。複数のパスワードポリシーを適用する場合は、パスワードポリシーの優先順位を指定することもできます。

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

注: CA Identity Manager が SiteMinder と統合されると、SiteMinder がすべてのパスワード ポリシーを適用します。

パスワード ポリシーの作成

CA Identity Manager ユーザ コンソールを使用してパスワード ポリシーを作成します。

注: パスワード ポリシー オプションによっては、利用可能にするために特定の既知の属性のマッピングが必要になるものがあります。「[追加パスワード ポリシーの有効化](#) (P. 104)」を参照してください。

次の手順に従ってください:

1. ユーザ コンソールで、いずれかを選択します。
 - [ポリシー] - [パスワード ポリシーの管理] - [パスワード ポリシーの作成]。
 - [タスク] - [ポリシー] - [パスワード ポリシーの管理] - [パスワード ポリシーの作成]。
2. パスワード ポリシーの一意の名前とオプションの説明を入力します。
3. ご使用の実装に適するように、これらのパスワード ポリシー設定を行ってください。
 - [ユーザセットへのパスワード ポリシーの適用](#) (P. 104)
 - [パスワードの有効期限の設定](#) (P. 106)
 - [パスワード構成の設定](#) (P. 110)
 - [正規表現の指定](#) (P. 112)
 - [パスワードの制限の設定](#) (P. 114)
 - [パスワードの詳細オプションの設定](#) (P. 118)

追加パスワードポリシーの有効化

CA Identity Manager では、パスワードの有効期限、構成、および使用方法を適用することにより、ユーザパスワードを管理する基本的なパスワードポリシーを作成することができます。また、以下のような追加的なパスワードルールおよび制限も定義できます。

- パスワードの有効期限
 - 正常/失敗ログインの追跡
 - ログインの認証
 - 変更されない場合パスワードは失効
 - パスワードの未使用
 - 無効なパスワード
 - 複数の正規表現
- パスワードの制限
 - 再使用までの最短日数
 - 再使用までの最少パスワード世代数
 - 前のパスワードとの差異の割合 (%)
 - 差異をチェックする場合に順番を無視

次の手順に従ってください:

1. 管理コンソールで [Directories] - [<ディレクトリ名>] - [User] に移動します。
2. %PASSWORD DATA% および %ENABLED STATES% -> 'STATE' が物理属性にマップされていることを確認します。
3. これらの属性は、サンプル `directory.xml` ファイルで、デフォルトでマップされます。これらの属性がマップされていない場合、『*CA Identity Manager Configuration Guide*』を参照して詳細を確認してください。

ユーザセットへのパスワードポリシーの適用

パスワードポリシーが適用されるユーザセットを決定するルールを指定できます。この機能により、一般的な従業員用のパスワードポリシーと高レベルのマネージャ用のより厳しいポリシーを作成できるようになります。

次の手順に従ってください:

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

各フィルタ タイプの説明については以下の表を参照してください。

注: パスワードポリシーが適用されるユーザストアのタイプにより、[ディレクトリ フィルタ] リスト ボックスのオプションが決定されます。CA Identity Manager が SiteMinder と統合されている場合、いくつかのフィルタ タイプは、リレーショナル データベースおよび CA Directory ユーザ ストアについて利用できません。

3. 属性や演算子を選択し値を入力して、条件を指定します。
4. 条件をさらに追加するには、プラス記号をクリックします。

以下の表に、ディレクトリ フィルタ タイプのオプションおよび各フィルタ タイプの例を示します。以下の例における "=" の左側の属性は、ユーザディレクトリ定義領域で規定される通りです。作成-タイプ ユーザ タスクについて、ディレクトリ フィルタが設定されたパスワード ポリシーは、以下の条件が両方とも満たされる場合にのみ適用されます。

- CA Identity Manager が SiteMinder と統合されていない。
- ディレクトリ フィルタ タイプが [ユーザ]、[グループ]、[グループ フィルタ]、または [グループ検索] のいずれでもない。

フィルタ タイプ	このフィルタの用途	例
所属組織	組織を参照し、選択します。	
所属グループ	グループを参照し、選択します。	
ユーザ	単一のユーザを参照し、選択します。	
ユーザ フィルタ (SiteMinder と統合されている場合、リレーショナル データベースでは利用できません。)	ユーザに対するフィルタを指定します。	従業員タイプ = 契約者 部署 = セキュリティ

フィルタタイプ	このフィルタの用途	例
ユーザ検索式	ユーザの検索クエリを入力します。	uid=jsmith (LDAP 用) TBLUSERS.ID = jsmith (リレーショナルデータベース用)
グループフィルタ (SiteMinder と統合されている場合、リレーショナルデータベースでは利用できません。)	グループに対するフィルタを指定します。	自己登録 = *
グループ検索式	グループの検索クエリを入力します。	cn=販売 (LDAP 用) TBLGROUPS.NAME=GroupA (リレーショナルデータベース用)
組織フィルタ (SiteMinder と統合されている場合、リレーショナルデータベースでは利用できません。)	組織に対するフィルタを指定します。	組織名 = *マーケティング
組織検索式	組織の検索クエリを入力します。	ou=Boston (LDAP 用) TBLORGANIZATIONS.NAME=ボストン (リレーショナルデータベース用)
検索	フィルタタイプのオプションに含まれていないクエリを指定します。	(&(uid=*smith)(ou=ボストン))

パスワードの有効期限の設定

ユーザアクセスの管理のため、複数の失敗ログイン試行、またはアカウント非アクティブ状態などのイベントを定義することができます。これらのイベントが発生すると、CA Identity Manager は該当するユーザ アカウントを無効にします。CA Identity Manager が SiteMinder に統合されると、リダイレクトを指定できます。

注: これらには、追加の設定が必要です。「[追加パスワードポリシーの有効化](#) (P. 104)」を参照してください。

パスワードの有効期限では以下の設定が可能です。

- [失敗ログインの追跡] / [正常ログインの追跡] チェック ボックス
- [ログイン追跡失敗時の認証] チェックボックス
- [変更されない場合パスワードは失効] 設定
- [未使用の場合パスワードは失効] 設定
- [不正なパスワード] 設定

[失敗ログインの追跡]/[正常ログインの追跡]チェック ボックス

このチェック ボックスは、前回のログイン試行の時刻を含むユーザ ログイン試行の追跡を有効/無効にします。このチェック ボックスをオンにすると、CA Identity Manager は、ユーザストア内のパスワードデータ属性にログイン情報を書き込みます。

注: これには、追加の設定が必要です。「[追加パスワードポリシーの有効化 \(P. 104\)](#)」を参照してください。

[失敗ログインの追跡] チェック ボックスがオンの場合、[不正なパスワード] セクションおよび [ログイン追跡失敗時の認証] チェック ボックスが有効です。
[正常ログインの追跡] チェック ボックスがオンの場合、[未使用の場合パスワードは失効] セクションおよび [ログイン追跡失敗時の認証] チェック ボックスが有効です。

複数のパスワードポリシーがある場合は、該当するすべてのパスワードポリシーでログイン詳細を無効にしてください。そうでないと、ログイン詳細の追跡を有効にする 1 つのポリシーにより、複数のパスワードポリシーの動作が不正確になる場合があります。

[ログイン追跡失敗時の認証]チェックボックス

このチェック ボックスをオンにすると、ユーザの追跡が失敗したときにログインが可能になります。デフォルトでは、このチェック ボックスはオフになっています。ログイン追跡が無効なとき、ユーザはログインできません。

このチェック ボックスをオンにするときは、[失敗ログインの追跡] または [正常ログインの追跡] チェック ボックスも必ず選択してください。

注: これには、追加の設定が必要です。「[追加パスワードポリシーの有効化 \(P. 104\)](#)」を参照してください。

[変更されない場合パスワードは失効]設定

[変更されない場合パスワードは失効] フィールドでは、期限切れになったパスワードの動作を設定できます。必要に応じて、どの程度事前にパスワードの有効期限切れをユーザに警告するかを指定できます。

注: これには、追加の設定が必要です。「[追加パスワード ポリシーの有効化 \(P. 104\)](#)」を参照してください。

以下のフィールドを設定できます。

次以降: <数> 日

パスワードが期限切れになった後、ユーザの無効化またはパスワード変更の強制までに CA Identity Manager が待機する日数を指定します。

注: CA Identity Manager では、指定された日数が経過した後にユーザがログインを試行するまで、ユーザを無効にしません。

ユーザの無効化

このラジオ ボタンを選択すると、パスワードが期限切れになった場合にユーザを無効にします。無効になったユーザは、以下を使用して有効にすることができます。

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

注: 詳細については、「[CA SiteMinder ポリシー サーバ管理ガイド](#)」を参照してください。

パスワード変更の強制

このラジオ ボタンを選択すると、ユーザが次にログインを試行するときにパスワードの変更を強制します。

期限切れまでの日数の警告: <数> 日

パスワードが期限切れになる何日前にユーザに通知するかを指定します。

[未使用の場合パスワードは失効]設定

[未使用の場合パスワードは失効] 設定では、ユーザ ログイン試行の間隔を指定します。指定時間が経過した後、ユーザ アカウントは非アクティブとみなされます。また、このセクションを使用して、アカウントが非アクティブであるとみなされたユーザにログイン許可がある場合のアクションを指定することもできます。

[未使用の場合パスワードは失効] セクションの設定を行う場合は、[ログインの追跡] 詳細チェック ボックスを有効にする必要があります。

注: これには、追加の設定が必要です。 「[追加パスワードポリシーの有効化](#) (P. 104)」を参照してください。

[未使用の場合パスワードは失効] セクションには、以下の設定が含まれます。

- 次以降: <数> 日 -- パスワードが期限切れになるまでの未使用日数を指定します。
- ユーザの無効化 -- 未使用のためにパスワードが期限切れになった場合、ユーザを無効にし、ユーザ アカウントが無効になります。その後、無効になったユーザを有効にするには、[ユーザの有効化/無効化] を使用します。
- パスワード変更の強制 -- 未使用のためにパスワードが期限切れになった場合、パスワードの変更を強制します。ユーザは次のログイン試行でパスワードを変更します。

[不正なパスワード]設定

[不正なパスワード] 設定セクションでは、ユーザ アカウントを無効にする前に許可される失敗ログイン数を指定することができます。また、ユーザが再度ログインできるようになるまでのアカウント無効期間を指定することもできます。

[失敗ログインの追跡] チェック ボックスをオンにしたときに限り、この設定が適用されます。

注: これには、追加の設定が必要です。 「[追加パスワードポリシーの有効化](#) (P. 104)」を参照してください。

[不正なパスワード] には、以下のフィールドがあります。

アカウントが無効になる時点: <数> 回連続の無効なパスワード

この設定では、ユーザに許可されている連続した失敗ログイン試行の数を指定します。不正なログインの回数を制限することによって、正しいパスワードが見つかるまで繰り返しパスワードを入力してリソースにアクセスするプログラムからリソースを保護します。指定された回数を超えてもユーザが正常にログインできないと、**CA Identity Manager** はそのアカウントを無効にします。管理者は再度アカウントを有効にする必要があります。

次以降: <数> 分

この設定では、ユーザが次のログイン試行をし、アカウントが再度有効になるまでに待機する時間を指定します。ユーザが別の不正なパスワードを入力した場合、**CA Identity Manager** は再度アカウントを無効にします。このとき、ユーザは指定された時間だけ待機してから、ログインを再試行します。

1 回のログイン試行を許可

この設定では、ユーザが不正なパスワードを入力した後、次の 1 回のログイン試行を行うまでの分数を指定します。

アカウントの再有効化

この設定では、指定された分数の後に再度アカウントが有効化されます。

パスワード構成の設定

新しいパスワードの作成方法を決定するルールを指定できます。文字の要件に関する値を決定するときは、パスワードの最大長を必ず考慮してください。必要な文字および数値の合計数が最大パスワード長を超えると、すべてのパスワードが拒否されます。たとえば、[文字] と [数字] が共に「6」に設定された場合、すべてのパスワードには 12 文字（6 つの文字と 6 桁の数字）以上が含まれます。この例では、パスワードの最大長が 8 文字である場合、すべてのパスワードが拒否されます。

パスワード構成の設定には以下のものがあります。

パスワード最小長

ユーザパスワードの最小文字数を指定します。

パスワード最大長

ユーザパスワードの最大文字数を指定します。

繰り返し文字の最大数

パスワード内で連続して使用可能な反復文字の最大数を決定します。

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

英大文字

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

英小文字

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

文字

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

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

数字

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

文字または数字

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

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

記号

記号の使用を許可するかどうかを指定し、許可する場合はパスワードに含めることができる最小数を指定します。記号とは、ピリオド、カンマ、感嘆符、スラッシュ、ダッシュおよびハイフンです。

印刷不能

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

注: 一部のブラウザでは、印刷不能文字をサポートしていません。

英数字以外

記号およびその他のシンボル（「@」、「\$」、「*」など）のように、英数字でない文字の使用を許可するかどうかを指定し、許可する場合は、パスワードに含めることができる最小文字数を指定します。ここには、印刷不能文字も含まれます。また、英数字以外の文字は [記号] および [印刷不能] 文字の要件も満たします。

正規表現の指定

パスワードの正規表現では、各パスワードが一致すべき（または一致してはいけない）正規表現テキストパターンを有効にするように指定できます。このテストは、たとえば、最初の文字を数値とし、最後の文字は数値でないようにしたい場合などに役に立ちます。

1つのパスワードポリシーに対して、複数の表現を設定します。複数の表現を作成すると、指定されたすべての表現に一致するパスワードが許容されるパスワードとなります。

次の手順に従ってください：

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

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

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

Expression: [a-zA-Z].*

正規表現の構文

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

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

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

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

パスワードの制限の設定

パスワードの使用方法に制限を設定することができます。制限には、あるパスワードを再度使用する前に待機する必要がある時間や、過去に選択したパスワードとどの程度異なったパスワードを設定する必要があるかなどが含まれます。また、セキュリティリスクがあるか、個人情報が含まれると判断した用語を、ユーザが指定しないようにすることもできます。

注: これには、追加の設定が必要です。「[追加パスワードポリシーの有効化](#) (P. 104)」を参照してください。

[制限] セクションには以下のフィールドが含まれます。

再使用までの最短日数

ユーザがパスワードを再使用できるまでの待機日数を指定します。

再使用までの最少パスワード世代数

あるパスワードを再度使用できるまでに使用する必要があるパスワードの数を指定します。

注: 期間とパスワード数を指定した場合は、両方の条件を満たさないとパスワードを再使用できません。たとえば、パスワードポリシーで、以前のパスワードを再使用できるようになる条件として 365 日が経過していること、パスワードを 12 回指定していることを設定します。1 年後に 6 つのパスワードしか使用されていなかった場合、ユーザが最初のパスワードを再度使用できるようになるには、さらに 6 つのパスワードを使用することが必要です。

前のパスワードとの差異の割合 (%)

新しいパスワードに含める文字の割合を指定します。値は最大で 100 を設定できます。この場合、新しいパスワードには、以前のパスワードに含まれていた文字をまったく含めることができません。

差異をチェックする場合に順番を無視

文字の割合 (%) を判断する際、パスワード中での文字の位置を無視します。

たとえば、最初のパスワードが「BASEBALL12」である場合に「差異をチェックする場合に順番を無視」チェックボックスがオンになっていると、「12BASEBALL」は使用できないことになります。このチェックボックスをオフにした場合は、各文字の出現順序が異なっているため、12BASEBALL をパスワードに指定できます。

高い安全性を確保するには、[差異をチェックする場合に順番を無視] チェックボックスをオンにします。

パスワード	差異の割合 (%)	文字順を無視	承諾
BASEBALL12 (旧)	0	選択	Y
12BASEBALL		選択なし	Y
BASEBALL12 (旧)	100	選択	N
12BASEBALL		選択なし	Y

パスワード	差異の割合 (%)	文字順を無視	承諾
BASEBALL12 (旧)	0	選択	Y
12SOFTBALL		選択なし	Y
BASEBALL12 (旧)	90	選択	N
12SOFTBALL		選択なし	Y
BASEBALL12 (旧)	100	選択	N
12SOFTBALL		選択なし	N

プロフィール属性

「一致する長さ」フィールドを設定すると、ユーザがパスワードに個人情報を使用するのを防ぐことができます。「一致する長さ」フィールドは、パスワードポリシーがディレクトリエントリの属性と比較する最小のシーケンス長を指定します。たとえばこの値が4に設定された場合、CA Identity Managerでは、ユーザプロフィール属性（たとえば姓、電話番号など）の最後の4文字がパスワードに含まれないことを確認します。

辞書

パスワードで使用できない文字列のリストを指定します。

注: 辞書エントリの最後の行にはキャリッジリターンが続きます。

辞書の設定には、以下のフィールドがあります。

- パス -- 辞書ファイルのフルパスおよび名前を含みます。
- 一致する長さ -- 辞書ファイルの値と比較される文字列の長さを制御します。この比較では、大文字/小文字の区別は無視されます。[一致する長さ] フィールドは空白にするか、「0」に設定することができます。このような場合、CA Identity Manager は、辞書にある文字列に完全に一致するパスワードのみを拒否します。[一致する長さ] が 0 より大きい場合、CA Identity Manager は、以下の条件でエントリを拒否します。
 - パスワードに、辞書エントリと同じ文字の並びで開始する部分文字列が含まれている。
 - 連続して一致している文字数が、[一致文字数] フィールドで指定した数以上である。

たとえば、以下のエントリを含む辞書ファイルがあるとします。

- lion
- tiger
- bear

[一致する長さ] フィールドが 4 に設定されている場合、以下のような結果になります。

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

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

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

パスワードの詳細オプションの設定

パスワードの詳細ポリシー オプションでは、サブミットされたパスワードの検証および格納前に行う前処理を設定することができます。また、ポリシーに優先度を割り当てて、同じディレクトリまたはネームスペースに割り当てられる複数のパスワードポリシーの予測可能な評価を行うことができます。

大文字小文字の区別を強制しない | 大文字の強制 | 小文字の強制

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

重要: 文字変換オプションを指定する場合には、文字の使用に関連して定義されている構成オプションと矛盾がないことを確認してください。

先頭の空白の削除

処理の前にパスワードから先頭の空白を削除します。

末尾の空白の削除

処理の前にパスワードから末尾の空白を削除します。

埋め込み空白の削除

処理の前に埋め込み空白をすべて削除します。

注: いくつかのユーザ ディレクトリ実装では、属性値（この中にユーザパスワードが格納されている）を格納する前に先頭または末尾の空白を削除します。ユーザがパスワードポリシー内に指定する設定は影響を与えません。

評価優先度

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

優先度の低いパスワードポリシーの適用

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

パスワード ポリシーの管理

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

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

パスワード ポリシーとリレーショナル データベース

リレーショナル データベースに適用されるパスワード ポリシーを設定する場合、以下の形式を使用して、SiteMinder ユーザ ディレクトリのパスワード データ属性を設定する必要があります。

tablename.columnname

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

CA Identity Manager と SiteMinder の統合パスワード基準

CA Identity Manager が SiteMinder に統合され、SiteMinder のパスワード 処理機能を使用する場合は、パスワード ポリシーが SiteMinder ポリシー ストアから取得されます。この場合は、SiteMinder のパスワード 基準を満たすパスワードを作成します。SiteMinder のパスワード 基準を満たす記号は、以下の文字のみです。

'*', '(', '¥', '!', '@', '"', ':', '#', '_', '-', '|', '&', '?', ')', '{', '}', '*', '!', '/'

重要: CA Identity Manager では、パスワードに使用される記号に制限はありません。ただし、SiteMinder パスワード機能を使用する場合は、SiteMinder の制限に適合するパスワードを作成することをお勧めしています。

パスワードのリセットまたはアカウントのロック解除

ユーザが Windows システムでパスワードを忘れた場合、Windows ログオン画面からユーザに入力を要求するようにセルフ サービスを設定できます。この機能は、Windows VISTA および Windows 7 で、クレデンシャル プロバイダをインストールすることで使用できます。

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

クレデンシャル プロバイダのインストール

次の手順に従ってください：

1. CA Identity Manager プロビジョニング コンポーネントのダウンロード、またはその他のインストール メディアを検索します。
2. Agent の下にあるインストーラを実行します。
注：クレデンシャル プロバイダを 64 ビットのオペレーティング システムにインストールする場合、本ソフトウェアの 64 ビット版を選択してください。
3. ウィザードのプロンプトに従って、質問に回答します。
4. クレデンシャル プロバイダを 64 ビットのオペレーティング システムにインストールした場合、[Microsoft Visual C++ 2008 SP1 \(64 ビット\)](#) をダウンロードします。
5. インストールが完了したら、クレデンシャル プロバイダを設定します。

クレデンシャル プロバイダの設定

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

クレデンシャル プロバイダを設定する方法

1. Windows エクスプローラで、クレデンシャル プロバイダをインストールしたディレクトリに移動します。例：
`C:\Program Files\CA\Identity Manager\Credential Provider`
2. 次の実行可能ファイルをダブルクリックします。
`CAIMCredProvConfig.exe`

3. デフォルトとして最初のクレデンシャルプロバイダを選択します。

Microsoft パスワード資格情報プロバイダなどの 2 番目のクレデンシャルプロバイダが使用中の場合、ログオン画面にこの設定が反映されない可能性があります。両方のプロバイダがデフォルトプロバイダであることを試みると、ログオン画面はデフォルトプロバイダを選択します。

4. デフォルト クレデンシャルプロバイダを無効にします。
5. [クレデンシャルプロバイダ設定] フィールドを以下のように入力します。

[Link1 URL]

ユーザが [パスワードを忘れた場合] リンクをクリックすると使用される URL です。このリンクは、パスワードリセット用の Web インターフェースへの URL である必要があります。

以下はリンクの例です。

```
http://eastern.local:8080/iam/im/environment/ca12/index.jsp?
task.tag=forgottenpassword&facesViewId=/app/page/screen/
fp_identify_user.jsp&action.forgottenpassword.identify=1&USER_ID=%username%
```

この URL の場合、実際の環境で自己登録が可能である必要があります。さらに、CA Identity Manager 環境用のセルフ サービス URL が、クレデンシャルプロバイダをインストールしているシステムから機能することを確認してください。%username% は、[ログオン] ダイアログボックスの [ユーザ名] フィールドの値に置換されます。

[Link2 URL]

ユーザが [アカウントのロック解除] リンクをクリックすると使用される URL です。このリンクは、ユーザがアカウントのロック解除を行うことができる Web インターフェースへの URL である必要があります。%username% は、[ログオン] ダイアログボックスの [ユーザ名] フィールドの値に置換されます。

[Link3 URL]

ユーザが [新しいアカウント] リンクをクリックすると使用される URL です。このリンクは、ユーザがアカウントを作成するための Web インターフェースへの URL である必要があります。%username% タグは、URL の一部である必要はありません。

カスタム タイトルの使用

カスタマイズされた文字列により、クレデンシャル プロバイダの
[戻る] ダイアログ ボックスまたはタイトル バーに表示される
「Powered by ...」が置換されます。文字列の場所は、[Section 508
Compliance] 設定に基づきます。

ドメイン

プロビジョニングのドメイン名です。

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

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

[すべて無効] ダイアログ ボックス

ポップアップ、エラー、および印刷や保存のダイアログ ボックスなどの新しいダイアログ ボックス ウィンドウがセキュアブラウザで出力されないようにします。[すべて無効] ダイアログ ボックスによりシステム セキュリティを改善できますが、トラブルシューティングのために無効にできます。

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

許可リスト

常にアクセスが許可される URL に一致する正規表現パターンです。

拒否リスト

常にアクセスが拒否される URL に一致する正規表現パターンです。

7. (オプション) [エクスポート] をクリックして、別のシステムに設定をエクスポートします。
8. [OK] をクリックして設定を保存します。
9. システムを再起動します。

Credential Provider のレジストリ設定

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

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]

link1_cmd

このリンクは、ユーザがリンク 1 をクリックすると移動できる URL として機能する必要があります。

link2_cmd

このリンクは、ユーザがリンク 2 をクリックすると移動できる URL として機能する必要があります。たとえば、アカウントのロック解除を行うための Web サイトに移動するリンクを追加できます。

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

link3_cmd

このリンクにより、Web インターフェースへの URL がロードされ、ユーザがアカウントを作成できるようになります。

comp508

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

domain

プロビジョニングのドメイン名です。

langdir

ローカライズされた言語の DLL の場所です。

disablepwdcp

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

CredentialProviderInstallPath

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

configdir

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

selectdefaultcredential

デフォルト オプションとして最初のクレデンシャル プロバイダを選択します。Yes は有効です。No は無効です。

Cube ブラウザのレジストリ設定

Cube の安全なブラウザ コンポーネントには、その動作を制御するいくつかのレジストリ値があります。これらの設定は以下のレジストリ キーにあります。

[HKEY_LOCAL_MACHINE\SOFTWARE\CA\Cube]

Type

REG_SZ(文字列)

404

起動時にマシンが CA Identity Manager に接続できない場合に表示される、標準的な HTML ドキュメントのパス。

default

Link1 コマンドまたは Link2 コマンドに URL が含まれていない場合の、移動先のデフォルト ページ。

allow

明示的な許可 ACL。常に許可される URL に一致するパターンの正規表現です。詳細については、「[Cube アクセス制御リスト \(P. 125\)](#)」を参照してください。

close

セキュアブラウザを閉じて、クレデンシャルプロバイダの「忘れたパスワード」ダイアログボックスにユーザの制御を返します。

deny

明示的な拒否 ACL。常にアクセスが拒否される URL に一致するパターンの正規表現です。詳細については、「[Cube アクセス制御リスト](#) (P. 125)」を参照してください。

langdir

ローカライズされた言語の DLL の場所です。

rejectinvalidcerts

クレデンシャルプロバイダが有効な SSL 証明書のみを受け入れるかどうかをコントロールします。no に設定すると、このオプションで期限切れ、または無効な SSL 証明書が許可されます。

このキーの有効な値は *yes* と *no* です。

unreachable

Cube で接続性の問題が発生した場合に、URL にリダイレクトされます。

サンプル値：file:///C:¥unreachable.html

usecustomtitle

これで、クレデンシャルプロバイダのカスタムタイトルが有効になります。

customtitle

これは、クレデンシャルプロバイダに表示されるタイトルです。

Cube アクセス制御リスト

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

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

アクセス制御リストの例

"allow"=".pdf"

すべての PDF ドキュメントの表示を許可します。

"deny"=".doc|.xls"

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

[Powered by]メッセージのカスタマイズ

クレデンシャル プロバイダの [戻る] ダイアログ ボックスまたは [戻る] メニュー オプションで、[Powered by] メッセージの存在にお気づきかもしれません。このメッセージを編集するか削除できます。

[Powered by]メッセージのカスタマイズする方法

1. フリーウェアのリソース エディタである ResEdit を <http://www.resedit.net> からダウンロードします。
2. ResEdit を起動します。
3. 言語フォルダ内のファイル 1033.dll を編集します。
4. [String Table] をダブルクリックします。
5. リソース ID 135 (このメッセージのリソースの英語版) を削除または変更します。

Windows ログイン用パスワードのリセット

クレデンシャルプロバイダが Windows システムにインストールされると、[パスワードを忘れた場合]リンクが、標準 Microsoft Windows ログオン ダイアログ ボックスに表示されます。このリンクを使用して、パスワードをリセットするか、パスワードを思い出すためのヒントを表示します。

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

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

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

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

4. 認証の質問への回答を入力します。

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

次の画面で、パスワードの変更を促すメッセージが表示されます。

Credential Provider のサイレント インストール

Credential Provider は、サイレント モードのインストールをサポートしています。6 つのプロパティがサポートされています。

LINK1

レジストリ内の SOFTWARE¥CA¥CAIMCredentialProvider¥link1_cmd を参照します。

LINK2

レジストリ内の SOFTWARE¥CA¥CAIMCredentialProvider¥link2_cmd を参照します。

LINK3

レジストリ内の SOFTWARE¥CA¥CAIMCredentialProvider¥link3_cmd を参照します。

DOMAIN

レジストリ内の SOFTWARE¥CA¥CAIMCredentialProvider¥domain を参照します。

COMP508

レジストリ内の SOFTWARE¥CA¥CAIMCredentialProvider¥comp508 を参照します。

USECUSTOMTITLE

レジストリ内の SOFTWARE¥CA¥Cube¥usecustomtitle を参照します。

CUSTOMTITLE

レジストリ内の SOFTWARE¥CA¥Cube¥customtitle を参照します。

REJECTINVALIDCERTS

レジストリ内の SOFTWARE¥ComputerAssociates¥Cube¥rejectinvalidcerts を参照します。

UNREACHABLE

アクセスできないページの場所を参照します。

これらのプロパティの値を設定する構文を、以下に示します。

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=¥"C:¥Program Files¥CA¥Identity
Manager¥Credential Provider¥" LINK1=¥"<url>¥" LINK2=¥"<url>¥" LINK3=¥"<url>¥"
COMP508=¥"yes¥" REJECTINVALIDCERTS=¥"yes¥" USECUSTOMTITLE=¥"yes¥"
CUSTOMTITLE=¥"custom cp title¥"
```

または

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=¥"C:¥Program Files¥CA¥Identity
Manager¥Credential Provider¥" LINK1=¥"<url>¥" LINK2=¥"<url>¥" LINK3=¥"<url>¥"
COMP508=¥"yes¥" USECUSTOMTITLE=¥"yes¥" CUSTOMTITLE=¥"custom cp title¥"
SELECTDEFAULTCREDENTIAL=¥"yes¥" UNREACHABLE=¥"<url>¥"
```

または

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=¥"C:¥Program Files¥CA¥Identity
Manager¥Credential Provider¥"
LINK1=¥"<url>¥" LINK2=¥" <url>¥" LINK3=¥"<url>¥" COMP508=¥"yes¥"
USECUSTOMTITLE=¥"yes¥" CUSTOMTITLE=¥"custom cp title¥"
SELECTDEFAULTCREDENTIAL=¥"yes¥" UNREACHABLE=¥"file:/// [INSTALLDIR]<file
name>¥"CUBE_ALLOW=¥"¥"CUBE_DENY=¥"¥"
```

[INSTALLDIR]

INSTALLDIR プロパティの値を参照します。

<url>

アカウントのロック解除、またはパスワードを忘れた場合に使用する URL を指定します。

<file name>

接続できないファイルの名前を定義します。

CUBE_ALLOW

キューブからの URL 呼び出しの許可を指定します。

CUBE_DENY

キューブからの URL 呼び出しの制限を指定します。

第 6 章: エンドポイント上でのパスワードの同期

CA Identity Manager でサポートされているエンドポイントに、パスワード同期エージェントをインストールすることができます。このエージェントは、エンドポイント上のパスワード変更リクエストをインターセプトし、プロビジョニングサーバに変更をサブミットします。

このセクションには、以下のトピックが含まれています。

[Windows 上のパスワードの同期](#) (P. 131)

[UNIX および Linux 上のパスワードの同期](#) (P. 141)

[OS400 でのパスワード同期](#) (P. 156)

Windows 上のパスワードの同期

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

パスワード同期エージェントによってパスワード変更の試行が検出されると、エージェントはリクエストをインターセプトし、プロビジョニングサーバにそれを送信します。その後プロビジョニングサーバは、ユーザおよびそのユーザに関連付けられた他のアカウントに新しいパスワードを伝達します。

パスワード同期には以下の要件があります。

- パスワード変更をインターセプトするシステムには、パスワード同期エージェントがインストールされている必要があります。
- システムは、取得されたエンドポイントとして管理する必要があります。
- 取得された [エンドポイント設定] タブにある [パスワード同期エージェントのインストール] チェック ボックスがオンになっている必要があります。
- 管理対象システムのアカウントが検索され、CA Identity Manager ユーザに関連付けられている必要があります。
- 環境が、エンドポイントアカウントからのパスワード変更を受信できる必要があります。管理コンソールへのアクセスを持つ管理者が、この機能を有効にします。

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

CA Identity Manager サーバはエンドポイントでのパスワード制限を認識しません。エンドポイント アカウントの操作をする際、そのパスワード ポリシーはエンドポイントのパスワード ポリシーよりも厳しくする必要があります。

Windows パスワード同期エージェントのインストール

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

インストール プログラムの実行

以下の要件に注意してください。

- プロビジョニング サーバは、ユーザがエージェントをインストールしようとしているシステムを管理している必要があります。
- パスワード変更を行うための管理者としてのユーザを作成します。このユーザの推奨名は **etapwsad** です。このユーザには **PasswordAdministrator** プロファイルが必要です。
- インストール メディアには、2つの Windows パスワード同期エージェントがあります。32 ビット Windows 用と 64 ビット Windows 用です。32 ビット パスワード同期エージェントは、64 ビット Windows ではサポートされていません。32 ビット パスワード同期エージェントでは、FIPS のみサポートされています。

次の手順に従ってください:

1. CA Identity Manager インストール メディアを検索します。
2. ¥Agent¥PasswordSync または ¥Agent¥PasswordSync-x64 を参照します。
3. setup.exe を実行します。
4. 設定ウィザードで、以下を行います。
 - a. [ホスト名] フィールドに、プロビジョニング サーバシステムの名前を入力します。

- b. プロビジョニング サーバのインストールでデフォルト以外のポートを使用する場合は、必要に応じてポートを変更してください。
プロビジョニング サーバへの接続で推奨される LDAP ポートは 20390 です。
 - c. [ドメインの検索] ボタンをクリックして、プロビジョニング サーバ ドメインを取得します。
 - d. フェールオーバーに対してプロビジョニング サーバのインストールを設定する場合は、画面上の指示に従って、カンマで区切ったサーバのリストを追加します。
 - e. [次へ] をクリックします。
 - f. [管理者] フィールドに、パスワード同期エージェントのデフォルト グローバル ユーザ名として「etapwsad」と入力します。このユーザには PasswordAdministrator プロファイルが必要です。これはデフォルトでは存在しません。
 - g. [パスワード管理] フィールドで、管理者のパスワードを入力します。
 - h. [次へ] をクリックします。
 - i. [エンドポイント タイプ] ドロップダウン リストから、エージェントをインストールするホストのエンドポイントタイプを選択します。
 - j. [エンドポイント名] ドロップダウン リストから、ユーザ コンソールでエンドポイントを作成するとき使用されたエンドポイント名を選択します。
 - k. [設定] をクリックします。
5. インストールを完了し、再起動するようプロンプトが表示されたら、[完了] をクリックします。

ユーザ コンソールでのエンドポイントの更新

ユーザ コンソールで、エージェントがインストールされていることを示すためにエンドポイントを更新します。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. エージェントがインストールされているエンドポイントを検索します。
3. [エンドポイント設定] タブをクリックします。
4. [パスワード同期エージェントのインストール] チェック ボックスをオンにします。

環境でのパスワード同期の有効化

パスワード同期エージェントをインストールした後、エンドポイント上で行われたパスワード変更を環境が受信できるようにします。このタスクでは、環境が変更を受信できるようにするため、管理者は管理コンソールおよび CA Directory へのアクセスを持つ必要があります。

次の手順に従ってください：

1. 新規ユーザは、管理コンソールで以下を実行します。
 - a. 環境を選択します。
 - b. [詳細設定] - [プロビジョニング] を開きます。
 - c. [エンドポイントアカウント] チェック ボックスで [パスワード変更の有効化] を選択します。
2. 既存ユーザは、CA Directory で eTPropagatePassword 属性を 1 に設定します。

代替サーバに対するエージェントの設定

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

エージェントに対して代替サーバを設定する方法

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

Host

プロビジョニング サーバ システムの名前を指定します。

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

LDAP port

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

3. [ドメインの検索] ボタンをクリックして、プロビジョニング サーバ ドメインを取得します。

4. 次の形式で、[サーバ URL] フィールドに代替サーバのホスト名とポートを追加します。

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

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

パスワード同期エージェントが機能するしくみ

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

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

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

`password_update_timeout` 設定パラメータ (`eta_pwdsync.conf`) は、PSA が **CA Identity Manager** からのパスワード変更継承の確認を待機する時間を秒単位で指定します。その間に PSA が確認を受信しない場合は、継承が成功した場合と同じように動作が進行し、パスワード変更継承が確認されなかったという警告がログ (`eta_pwdsync.log`) に記録されます。パラメータの最小値はゼロ (0) で、これは PSA が確認を待機しないことを意味します。

アカウントレベルのパスワード品質チェック

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

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

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

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

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

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

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

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

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

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

パスワード品質の実施

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

パスワード同期の設定

パスワード同期エージェントは、インストール時に初期設定されます。これは、パスワード同期設定ウィザードを使用して随時再設定できます。さらに詳細に設定することもできます。たとえば、eta_pwdsync.conf ファイルを使用して、パスワード品質チェック用の設定変更や、タイムアウトの変更を行うことができます。

このファイルは、password_sync_folder¥data¥ フォルダにあります。この設定ファイル内のすべてのキーは、パスワード同期エージェントのインストール中に設定されます。そのため、これらのキーの変更は、必要な場合にのみ行ってください。詳細については、このファイル内のテキストを参照してください。

重要: 設定ファイルは、編集前に念のためバックアップを作成してください。

[Server] セクション

キー	説明	デフォルト値
host	パスワード伝達を管理するドメイン サーバを指定します。	なし
port	プロビジョニング サーバの LDAP リスニング ポートを指定します。	20411

キー	説明	デフォルト値
use_tls	パスワード同期エージェントとプロビジョニング サーバの間の通信を確保するために TLS/SSL を使用するかどうかを指定します。	Yes
admin_suffix	パスワード同期エージェントが CA Identity Manager にログインするために使用する管理者ユーザのドメイン サフィックスを指定します。	なし
admin	パスワード同期エージェントが CA Identity Manager にログインするために使用する管理者ユーザのアカウント名を指定します。	なし
password	admin キーで指定されたアカウント名用のパスワードを指定します。	なし

[eTaDomain] セクション

キー	説明	デフォルト値
Domain	パスワード同期エージェントをインストールしたプロビジョニング ドメインを指定します。	なし
etrust_suffix	CA Identity Manager 製品全体のサフィックスを指定します。	なし
domain_suffix	プロビジョニング ドメイン用のドメイン サフィックスを指定します。	なし
endpoint type	パスワード同期エージェントをインストールしたエンドポイント タイプを指定します。	なし
endpoint	パスワード同期エージェントがパスワードをインターセプトするエンドポイントを指定します。	なし
endpoint_dn	エンドポイントの識別名を指定します。	なし

キー	説明	デフォルト値
container_dn	パスワードを変更するアカウントが含まれるコンテナの識別名を指定します。	なし
acct_attribute_name	アカウントの属性名（たとえば Windows NT では eTN16AccountName）を指定します。	エンドポイントタイプによって異なる
acct_object_class	アカウントの objectClass を指定します。	エンドポイントタイプによって異なる

[PasswordProfile] セクション

キー	説明	デフォルト値
profile_enabled	パスワードプロファイルチェック機能が有効かどうかを指定します。	No
profile_dn	パスワード設定ウィザードがパスワードプロファイル用の DN を生成するかどうかを指定します。	eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

[Timeout] セクション

キー	説明	デフォルト値
search_acct_dn	アカウント DN を検索するときのタイムアウト値を指定します。	120 秒
pwd_update	パスワードを伝達するときのタイムアウト値を指定します。	400 秒
pwd_quality_check	パスワード品質チェックを実行するときのタイムアウト値（秒単位）を指定します。	1

[Logs] セクション

キー	説明	デフォルト値
log_file	パスワード同期エージェントからのログ記録されたメッセージが含まれるログファイルを指定します。	..¥Program files¥CA¥Identity Manager Password Sync Agent
log_level	ログ記録のレベルを指定します。有効な値は以下のとおりです。 1 -- Init ファイル 2 -- パスワード更新の成功または失敗 3 -- 接続デバッグ 4 -- 追跡	0、ログ記録なし

フェールオーバー

プロビジョニング サーバが停止した、または高い負荷がかかった場合、パスワード同期エージェントは別のサーバへフェールオーバーします。フェールオーバーには、複数のプロビジョニング サーバが同じドメインにサービスを提供し、エージェントがそれらのサーバを使用していることが必要です。

「代替サーバに対するエージェントの設定」に、設定手順が記載されています。

ログ メッセージの有効化

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

パスワード同期エージェントのロギングには、次の内容を含めることができます。

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

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

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

インストールの確認

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

UNIX および Linux 上のパスワードの同期

CA Identity Manager は、UNIX または Linux システム上でのアカウントのパスワード変更をインターセプトし、そのグローバル ユーザに関連付けられた他のすべてのアカウントにそれを伝達できます。外部のセキュリティ システムに対するパスワード認証に使用されるコンポーネントは **Pluggable Authentication Module (PAM)** と呼ばれます。PAM を使用すると、グローバル ユーザが既存のシステム パスワードを使用して CA Identity Manager にログオンできるように、CA Identity Manager が外部のセキュリティ システムに対してパスワードを認証します。

UNIX パスワード同期

UNIX PAM フレームワークを通じてパスワード変更イベントを検出する、パスワード同期モジュールが提供されています。UNIX パスワード同期モジュールは、パスワード変更をプロビジョニングサーバに通知します。プロビジョニングサーバは関連するグローバルユーザを検出し、他の関連するアカウントに変更を自動的に伝達します。

PAM フレームワークをサポートする UNIX オペレーティング システムには以下が含まれます。

- AIX v5.3 (Power プラットフォーム、PAM 有効)
- HP-UX v11.00 (PA-RISC プラットフォーム、および Itanium® 2 プラットフォーム上)
- Solaris v2.6 以降 (Sparc および Intel プラットフォーム上)
- 32 ビット Linux with glibc v2.2 以降 (s390 または Intel i386 プラットフォーム上)

注: Linux プラットフォームについては、`test_sync` バイナリはすべてのユーザの PATH 上に存在する必要がありますが、実行権限は `root` ユーザ (所有者) のみが持つ必要があります。

このライブラリをすべてのユーザのパスに追加するには、以下のコマンドを `global /etc/bashrc` ファイルに含めます。

```
export PATH=$PATH:/etc/pam_CA_eta
```

UNIX PAM の仕組み

以下プロセスでは、UNIX PAM 機能の仕組みについて説明します。

1. UNIX ユーザ パスワードは、以下のいずれかの理由によって変更されます。
 - ユーザによる決定。
 - システムの設定、または手動操作により、ユーザに対してパスワードの変更が強制された。
 - ユーザのパスワードが管理者によって変更された。
2. 新しいパスワードは、PAM フレームワーク パスワード サービスにサブミットされます。
3. PAM フレームワークのパスワード サービスは、ローカル UNIX セキュリティ ファイルを更新するために PAM ライブラリを呼び出します。
4. PAM フレームワークのパスワード サービスは、パスワード変更をプロビジョニング サーバに通知するために UNIX パスワード同期モジュール (pam_CA_eta) を呼び出します。
5. プロビジョニング サーバは、関連するグローバル ユーザおよびそのグローバル ユーザに関連付けられたすべてのアカウントのパスワードを更新します。

UNIX パスワード同期を使用する要件

UNIX パスワード同期機能を使用するための要件を以下に示します。

- パスワード変更を検出する UNIX システム上に UNIX パスワード同期エージェントがインストールされている必要があります。
- UNIX パスワード同期エージェントが存在する UNIX システム上に UNIX リモート エージェントおよび CAM がインストールされている必要があります。
- システムは、取得されたエンドポイントとして管理する必要があります。取得されたエンドポイントのプロパティにある [パスワード同期エージェントのインストール] チェック ボックスがオンになっている必要があります。
- 管理対象システムのアカウントが検索され、グローバル ユーザに関連付けられている必要があります。
- 環境が、エンドポイント アカウントからのパスワード変更を受信できる必要があります。管理コンソールへのアクセスを持つ管理者が、この機能を有効にします。

UNIX PAM 機能のインストール

UNIX PAM をインストールするには、以下の手順に従います。

UNIX PAM 機能をインストールする方法

1. お使いの UNIX プラットフォームに対応するパッケージ ファイルを選択します。

UNIX オペレーティング システム	パッケージ ファイル名
HP-UX v11 PA-RISC	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX Itanium2	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 Power	pam_CA_eta-1.1.AIX.tar.Z
Solaris Sparc	pam_CA_eta-1.1.Solaris.tar.Z
Solaris Intel	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux x86	pam_CA_eta-1.1.Linux.tar.gz
Linux s390	pam_CA_eta-1.1.LinuxS390.tar.gz

2. バイナリ モードで FTP を使用するか、バイナリ ファイルをサポートする他のファイル転送ツールを使用して、選択したパッケージ ファイルを UNIX サーバ上の一時フォルダ (/tmp) に転送します。以下は、サンプルの転送セッションの表示です。

```
W:¥Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01.company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1.1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1.1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```


3. UNIX サーバ上の root ユーザとしてログオンし、パッケージファイルを抽出します。

```
# cd /tmp
# zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
```

Linux では、以下のコマンドを使用します。

```
# tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
```

4. 設定ファイルと TLS ファイルをデフォルトの設定フォルダにコピーします。

```
# cd pam_CA_eta-1.1
# mv pam_CA_eta /etc
```

5. pam_CA_eta モジュールをセキュリティ ライブラリ フォルダにコピーします。

AIX では、以下のコマンドを使用します。

```
# cp -p pam_CA_eta.o /usr/lib/security/
```

HP-UX では、以下のコマンドを使用します。

```
# cp -p libpam_CA_eta.1 /usr/lib/security/
```

HP-UX Itanium2 では、以下のコマンドを使用します。

```
# cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
```

Linux i386 または s390 では、以下のコマンドを使用します。

```
# cp -p pam_CA_eta.so /lib/security/
```

Solaris Sparc または Intel では、以下のコマンドを使用します。

```
# cp -p pam_CA_eta.so /usr/lib/security/
```

6. (オプション) テスト プログラムをコピーします。

```
# cp -p test_* /etc/pam_CA_eta
# cp -p pam_test* (/usr)/lib/security/
```

詳細情報

[UNIX パスワード同期のトラブルシューティング \(P. 152\)](#)

ユーザ コンソールでのエンドポイントの更新

ユーザ コンソールで、エージェントがインストールされていることを示すためにエンドポイントを更新します。

次の手順に従ってください：

1. ユーザ コンソールにログインします。
2. エージェントがインストールされているエンドポイントを検索します。
3. [エンドポイント設定] タブをクリックします。
4. [パスワード同期エージェントのインストール] チェック ボックスをオンにします。

環境でのパスワード同期の有効化

パスワード同期エージェントをインストールした後、エンドポイント上で行われたパスワード変更を環境が受信できるようにします。このタスクでは、環境が変更を受信できるようにするため、管理者は管理コンソールおよび CA Directory へのアクセスを持つ必要があります。

次の手順に従ってください：

1. 新規ユーザは、管理コンソールで以下を実行します。
 - a. 環境を選択します。
 - b. [詳細設定] - [プロビジョニング] を開きます。
 - c. [エンドポイントアカウント] チェック ボックスで [パスワード変更の有効化] を選択します。
2. 既存ユーザは、CA Directory で eTPropagatePassword 属性を 1 に設定します。

UNIX パスワード同期機能の設定

UNIX パスワード同期機能では、以下のファイルでパラメータを設定します。

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

重要： 重要な権限を持つユーザのパスワードが pam_CA_eta.conf 設定ファイルに格納されているため、このファイルは root アカウントによってのみ読み取り可能である必要があります。パッケージファイル内のファイル設定には owner=root、mode=500 とあり、cp コマンドの -p スイッチによって、インストール中にこの設定が保存されます。

pam_CA_eta.conf ファイルの設定

pam_CA_eta.conf ファイルを設定するには、以下の手順に従います。

pam_CA_eta.conf ファイルの設定方法

1. /etc/pam_CA_eta フォルダに移動します。
2. pam_CA_eta.conf ファイルを編集します。この設定ファイルには、そのドキュメントが含まれます。

```
#
#  CA - CA Identity Manager
#
#  pam_CA_eta.conf
#
#  Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA Identity Manager LDAP server primary and optional alternate
server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA Identity Manager LDAP
server
# value: a valid TCP/IP port number
# default: 20390
# port 20390

# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#               server is used.
#               Cloud based server is accessed by proxying the requests
#               through the on-premise CS, requiring use of remote-server
#               set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA Identity Manager
#               server
# value: a numeric value
# default: 100
# size-limit 100

# keyword: root
# description: the root DN of the CA Identity Manager server
# value: a valid DN string
# default: dc=eta
# root dc=eta

# keyword: domain
# description: the name of the CA Identity Manager domain
# value: a string
# default: im
# domain im

# keyword: user
# description: the CA Identity Manager Global User name used to bind to the CA
#               Identity Manager server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin

# keyword: password
# description: the clear-text password of the "binding" CA Identity Manager Global
#               User
# value: the password of the above Global User
# default: no default
password SECRET
```

```
# keyword: directory-type
# description: the CA Identity Manager Unix Endpoint type of this Unix server
# value: ETC or NIS
# default: ETC
# endpoint-type ETC

# keyword: endpoint-name
# description: the CA Identity Manager Unix Endpoint name of this Unix server
# value: a valid Unix Endpoint name string
# default:
# ETC: the result of the "hostname" command (ie: gethostname() system call)
# NIS: "domain [hostname]" where "domain" is the result of the "domainname" command
# (ie: getdomainname() system call) and "hostname" the result of the "hostname"
# command (ie: gethostname() system call)
# endpoint-name dirname

# keyword: tls-cacert-file
# description: the name of the CA Identity Manager CA certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/et2_cacert.pem
# tls-cacert-file /etc/pam_CA_eta/et2_cacert.pem

# keyword: tls-cert-file
# description: the name of the CA Identity Manager client certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientcert.pem
# tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem

# keyword: tls-key-file
# description: the name of the CA Identity Manager client private key file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientkey.pem
# tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem

# keyword: tls-random-file
# description: the name of the "pseudo random number generator" seed file
# value: a valid full path file name
# default: /etc/pam_CA_eta/prng_seed
# tls-random-file /etc/pam_CA_eta/prng_seed

# keyword: use-status
# description: this module will exit with a non-zero status code in case of failure.
# value: yes or no
# default: no
# use-status no
```

```
# keyword: verbose
# description: this module will display informational or error messages to the
user.
# value: yes or no
# default: yes
# verbose yes
```

注: サーバ、ドメイン、およびパスワードパラメータはデフォルト値がなく、更新する必要はありません。

pam.conf ファイルの設定

/etc/pam.conf ファイルはメインの PAM 設定ファイルです。ファイルを編集して、パスワードサービススタックに行を挿入する必要があります。いくつかの Linux システムでは、pam.conf ファイルは /etc/pam.d と置換されるため、/etc/pam.d/system-auth ファイルを編集する必要があります。

pam.conf ファイルの設定方法

1. 適切な Linux システム上で PAM モジュールを設定している場合、/etc ディレクトリ、または /etc/pam.d ディレクトリに移動します。
2. pam.conf ファイルを編集して、パスワードサービススタックにパスワード同期の行を挿入します。プラットフォーム固有の設定については、以下の例を参照してください。

```
passwd password required /usr/lib/security/pam_unix.so
```

```
passwd password optional /usr/lib/security/pam_CA_eta.so
```

3. (オプション) `pam_CA_eta` モジュールの行に以下のオプションのパラメータを追加することができます。

`config=/path/file`

代替設定ファイルの場所を示します。

`syslog`

ローカル `syslog` サービスにエラーおよび情報メッセージを送信します。

`trace`

パスワード更新操作のそれぞれについて、トレース ファイルを生成します。トレース ファイルは `/tmp/pam_CA_eta-trace.<nnnn>` という名前になります。`<nnnn>` はパスワードプロセスの PID 番号です。

4. 以下のプラットフォーム固有の設定変更を実装します。

AIX システムについては、`/etc/pam.conf` ファイル最後に以下の行を追加します。

#

CA Identity Manager Unix Password Synchronization

#

```
login password optional /usr/lib/security/pam_CA_eta.so syslog
passwd password optional /usr/lib/security/pam_CA_eta.so syslog
rlogin password optional /usr/lib/security/pam_CA_eta.so syslog
su password optional /usr/lib/security/pam_CA_eta.so syslog
telnet password optional /usr/lib/security/pam_CA_eta.so syslog
sshd password optional /usr/lib/security/pam_CA_eta.so syslog
OTHER password optional /usr/lib/security/pam_CA_eta.so syslog
```

HP-UX システムについては、以下の行を `/etc/pam.conf` ファイルの最後に追加します。

#

CA Identity Manager Unix Password Synchronization

#

```
login password optional /usr/lib/security/libpam_CA_eta.1 syslog
passwd password optional /usr/lib/security/libpam_CA_eta.1 syslog
dtlogin password optional /usr/lib/security/libpam_CA_eta.1 syslog
dtaction password optional /usr/lib/security/libpam_CA_eta.1 syslog
OTHER password optional /usr/lib/security/libpam_CA_eta.1 syslog
```

HP-UX Itanium2 については、以下の行を `/etc/pam.conf` ファイルの最後に追加します。

#

```
# CA Identity Manager Unix Password Synchronization
```

```
#
```

```
login    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

Sun Solaris システムについては、既存の `pam_unix` の行の後に `pam_CA_eta` の行を追加します。

```
#
```

```
# Password management
```

```
#
```

```
other    password required    /usr/lib/security/pam_unix.so.1
other    password optional    /usr/lib/security/pam_CA_eta.so syslog
```

Linux システムについては、既存の `pam_cracklib` および `pam_unix` の行の間に `pam_CA_eta` の行を追加します。

```
password required    /lib/security/pam_cracklib.so retry=3 type=
password optional    /lib/security/pam_CA_eta.so syslog
password sufficient  /lib/security/pam_unix.so nullok use_authok md5 shadow
password required    /lib/security/pam_deny.so
```

5. AIX システムについては、`/etc/security/login.cfg` ファイルを編集して `auth_type = PAM_AUTH` を設定します。これにより、PAM フレームワークが有効になります（デフォルトでは有効になっていません）。これはランタイム設定であるため、設定を有効にするためにシステムを再起動する必要はありません。

UNIX パスワード同期のトラブルシューティング

UNIX PAM 機能のトラブルシューティングは、`syslog` とトレースメッセージを使用して実行できます。また、設定、LDAP/TLS 接続、パスワード同期、および PAM フレームワークをテストして行うこともできます。

詳細情報

[syslog メッセージのアクティブ化](#) (P. 153)

[トレース メッセージのアクティブ化](#) (P. 153)

syslog メッセージのアクティブ化

/etc/pam.conf ファイル内の `pam_CA_eta` の行に `syslog` パラメータを追加して、`pam_CA_eta` モジュールが情報およびエラー メッセージを生成できるようにします。ログ記録オプションが使用されている場合、UNIX アカウントがパスワードを変更するたびに、UNIX 管理者は `syslog` ファイルで情報メッセージを参照できます。これらのメッセージは、基本的な問題を診断するための十分な情報を提供します。

実稼働システム上でこのオプションを永続的に設定することが可能です。サイレント サービスで実行中の場合より多くのリソースを必要としないためです。

トレース メッセージのアクティブ化

`syslog` メッセージによって十分な情報が提供されない場合、トレース モードでより多くの詳細情報を取得することができます。パスワード更新操作のたびに、トレース モジュールは `/tmp/pam_CA_eta-trace.<nnnn>` という名前のファイルを作成します (<nnnn> はパスワードプロセスの PID です)。これには 1 つのエントリが含まれますが、それはモジュールによって使用されるほとんどのファンクションコール、およびそれらによって使用または返されるデータに対するものです。

トレース ファイルを読み取りできるのは `root` アカウントのみですが、これにはクリアテキストの新しいパスワードが含まれます。そのため、このパラメータは実稼働システム上で永続的に使用するべきではありません。

設定ファイルのテスト

/etc/pam_CA_eta ディレクトリにある test_config ツールを使用して、設定ファイルを検証することができます。まず、以下のようにフォルダ構造をセットアップします。

1. /etc 下の pam_CA_eta フォルダを移動します。
2. /etc/pam_CA_eta に pam_CA_eta-1.1 下のすべてをコピーします。

以下は、サンプルのコマンドライン エントリです。

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

セッションの例が続いて表示されます。

```
./test_config [config=/path/to/config_file]
# ./test_config
./test_config: succeeded
Trace file is /tmp/test_config-trace.1274
```

コマンド出力に表示されるように、設定ファイル解析の詳細をすべて含むトレース ファイルが生成されました。

CAM サービスの表示

サービスを起動したユーザを調べるために以下の手順に従うことができます。

CAM サービスを表示するには、以下の手順に従います。

1. Telnet または SSH クライアントの使用により root として UNIX マシンにログインします。
2. 以下の UNIX コマンドを発行します。

```
ps -ef | grep cam
```

以下のように表示されます。

```
root 13822      1 11 11:30:12 ?    0:00 cam
```

```
root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
```

注: システムの root ユーザがサービスを起動しない場合、起動されたように見えます。しかし、それらを使用できません。CA Identity Manager は「Permission denied: user must be root」のメッセージを発行します。

LDAP/TLS 接続のテスト

/etc/pam_CA_eta ディレクトリにある `test_ldap` ツールを使用して、プロビジョニングサーバへの接続を検証することができます（設定ファイルパラメータを使用）。以下は、サンプルのコマンドラインエントリです。

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

セッションの例が続いて表示されます。

```
./test_ldap [config=/path/to/config_file]
# ./test_ldap: succeeded
Trace file is /tmp/test_ldap-trace.1277
```

コマンド出力に表示されるように、設定ファイル解析、およびプロビジョニングサーバへの接続の詳細をすべて含むトレースファイルが生成されました。

パスワード同期のテスト

/etc/pam_CA_eta フォルダにある `test_sync` ツールを使用して、ローカルアカウントのパスワード更新がプロビジョニングサーバによって正常に伝達されたかどうかを検証することができます。以下は、サンプルのコマンドラインエントリです。

```
/etc/pam_CA_eta/test_sync <user> <password> [config=/path/to/config_file]
```

セッションの例が続いて表示されます。

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
CA Identity Manager password synchronization started.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
CA Identity Manager password synchronization succeeded.
/etc/pam_CA_eta/test_sync: succeeded
Trace file is /tmp/test_sync-trace.2244
```

コマンド出力に表示されるように、設定ファイル解析、プロビジョニングサーバへの接続、およびアカウントの更新の詳細をすべて含むトレースファイルが生成されました。

詳細モード（設定ファイルのデフォルトのパラメータ `verbose yes` を使用）を使用すると、コマンドにより、パスワード伝達に関する情報メッセージおよび潜在的なエラーのメッセージが提供されます。

PAM フレームワークのテスト

PAM テスト ライブラリを使用して、パスワード変更が PAM フレームワークによって正しく検出されたかどうかを検証できます。

PAM フレームワークのテスト方法

1. `pam_test` ファイルを `/usr/lib/security(/hpux32)` フォルダにコピーします。
2. `pam_test` ライブラリ用のパスワードクラスの行を、パラメータなしで追加します。

以下は Solaris の例です。

```
other password optional /usr/lib/security/pam_test
```

3. テスト ユーザに対してパスワード コマンドを発行し、その後、`syslog` ファイル内で `pam_test[<pid>]` というタグの行を探します。

コマンド出力には、以下の例のように、生成されたトレース ファイルの名前が表示されます。

```
pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
```

OS/400 でのパスワード同期

パスワード同期エージェントを使用すると、OS/400 エンドポイント システム上で行われたパスワード変更を、CA Identity Manager によって管理される他のアカウントに伝達することができます。パスワード同期エージェントは、以下のように作動します。

1. エージェントを OS/400 エンドポイント システムにインストールして実行します。

インストールの一部として、ユーザによるパスワード変更がエージェントによってプロビジョニング サーバに送信されるように、プログラムが OS/400 システムに登録されます。

2. プロビジョニング サーバは、このパスワード変更を関連アカウントに伝達します。

パスワード変更コマンド (CHGPWD) またはパスワード変更 API (QSYCHGPW) から開始されたパスワード変更は、エージェントによって受信されます。

3. エージェントは、操作の成功または失敗を PWDSYNCH/LOG にあるログ ファイルに記録します。

パスワード同期エージェントは、以下のプラットフォームでサポートされています。

- OS400 V5R2
- OS400 V5R3
- OS400 V5R4

パスワード同期エージェントをインストールする方法

1. プロビジョニング コンポーネントのインストール メディアの場所に移動します。
2. OS/400 上で、**¥Agent** 下のパスワード同期エージェント インストーラを実行します
3. 画面の指示に従って、インストールを完了してください。

注: エンドポイント エージェント ソフトウェア リンク内のインストール手順は、以降のセクションに含まれています。

OS400 パスワード同期エージェントのインストール

ユーザは ***ADDOBJ** の権限を持っている必要があり、またエージェントがパスワード変更通知を受信するには以下も必要です。

- システム値 **QPWDVLDPGM** が ***REGFAC** に設定されている必要があります。
- プログラムがコマンド **WRKREGINF EXITPNT (QIBM_QSY_VLD_PASSWRD)** で登録されている必要があります。
- 環境が、エンドポイント アカウントからのパスワード変更を受信できる必要があります。管理コンソールへのアクセスを持つ管理者が、この機能を有効にします。

エージェントは、パスワードが変更されたときに限り、開始されます。パスワードを変更するには、**CHGPWD** コマンドを発行します。

注: パスワード同期に関して、グローバル ユーザにフラグを立てる必要があります。

iSeries の場合

1. ***ALLOBJ** および ***SECADM** の権限（例： **QSECOFR**）を持つユーザとしてログオンします。
2. **PWDSYNCH** というユーザを作成します。

CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)

注: セキュリティ対策として、ユーザは期限切れのパスワードで作成されます。

3. savefile を作成し、任意のライブラリ（例： MYLIB）にインストールパッケージを格納します。

```
CRTSAVF MYLIB/PWDSYNCH
```

4. savefile を持つ Windows マシンでは、FTP を使用して iSeries に savefile を転送します。

```
ftp <hostname>  
binary  
cd MYLIB  
put PWDSYNCH.FILE
```

5. iSeries では、savefile からプログラムを抽出します。

```
RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
```

このコマンドは、同期エージェントを PWDSYNCH ライブラリに抽出してインストールします。

6. インストールを確認します。

```
DSPLIB PWDSYNCH
```

以下のオブジェクトが表示されます。

オブジェクト	タイプ	属性
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. iSeries をセットアップして、パスワード確認出口プログラムとして PWDSYNCH を使用するようにします。

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)  
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)  
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. iSeries 上で、CA IAM コネクタ サーバ用の接続パラメータを指定します。

```
EDTF FILE(PWDSYNCH/CONFIG)
```

OS400 パスワード同期エージェントのインストール

ユーザは *ADDOBJ の権限を持っている必要があり、またエージェントがパスワード変更通知を受信するには以下も必要です。

- システム値 QPWDVLDPGM が *REGFAC に設定されている必要があります。
- プログラムがコマンド WRKREGINF EXITPNT (QIBM_QSY_VLD_PASSWRD) で登録されている必要があります。
- 環境が、エンドポイント アカウントからのパスワード変更を受信できる必要があります。管理コンソールへのアクセスを持つ管理者が、この機能を有効にします。

エージェントは、パスワードが変更されたときに限り、開始されます。パスワードを変更するには、CHGPWD コマンドを発行します。

注: パスワード同期に関して、グローバル ユーザにフラグを立てる必要があります。

iSeries の場合

1. *ALLOBJ および *SECADM の権限（例：QSECOFR）を持つユーザとしてログオンします。
2. PWDSYNCH というユーザを作成します。

```
CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
```

注: セキュリティ対策として、ユーザは期限切れのパスワードで作成されます。

3. savefile を作成し、任意のライブラリ（例：MYLIB）にインストール パッケージを格納します。

```
CRTSAVF MYLIB/PWDSYNCH
```

4. savefile を持つ Windows マシンでは、FTP を使用して iSeries に savefile を転送します。

```
ftp <hostname>  
binary  
cd MYLIB  
put PWDSYNCH.FILE
```

5. iSeries では、savefile からプログラムを抽出します。

```
RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
```

このコマンドは、同期エージェントを PWDSYNCH ライブラリに抽出してインストールします。

6. インストールを確認します。

DSPLIB PWDSYNCH

以下のオブジェクトが表示されます。

オブジェクト	タイプ	属性
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. iSeries をセットアップして、パスワード確認出口プログラムとして PWDSYNCH を使用するようにします。

CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)

ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)

PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')

8. iSeries 上で、CA IAM コネクタ サーバ (CA IAM CS) 用の接続パラメータを指定します。

EDTF FILE(PWDSYNCH/CONFIG)

ユーザ コンソールでのエンドポイントの更新

ユーザ コンソールで、エージェントがインストールされていることを示すためにエンドポイントを更新します。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. エージェントがインストールされているエンドポイントを検索します。
3. [エンドポイント設定] タブをクリックします。
4. [パスワード同期エージェントのインストール] チェック ボックスをオンにします。

環境でのパスワード同期の有効化

パスワード同期エージェントをインストールした後、エンドポイント上で行われたパスワード変更を環境が受信できるようにします。このタスクでは、環境が変更を受信できるようにするため、管理者は管理コンソールおよび CA Directory へのアクセスを持つ必要があります。

次の手順に従ってください:

1. 新規ユーザは、管理コンソールで以下を実行します。
 - a. 環境を選択します。
 - b. [詳細設定] - [プロビジョニング] を開きます。
 - c. [エンドポイントアカウント] チェック ボックスで [パスワード変更の有効化] を選択します。
2. 既存ユーザは、CA Directory で eTPropagatePassword 属性を 1 に設定します。

SSL の設定

SSL は、同期エージェントとプロビジョニング サーバの間の通信を暗号化するために使用されます。SSL はネットワークを介してパスワードを送信するため、これは同期エージェントにとって重要です。SSL を常に使用することが推奨されます。

同期エージェントが SSL で接続するためには、プロビジョニング サーバの証明書を信頼する必要があります。そのため、iSeries マシンに証明書がインストールされ、証明書が同期エージェントによって信頼されるように設定する必要があります。これらのタスクは、Digital Certificate Manager (OS/400 のオプション コンポーネント) によって実行されます。Digital Certificate Manager のインストールおよびセットアップについては、OS/400 ドキュメントを参照してください。

プロビジョニング サーバ証明書のインストール

SSL を使用するには、iSeries マシンに以下のオペレーティング システム コンポーネントをインストールする必要があります。

- Cryptographic Access Provider ライセンス プログラム (5722-AC3)
- Digital Certificate Manager (OS/400 オプション 34)
- IBM HTTP Server for iSeries (5722 の DG1)

iSeries の場合

1. プロビジョニング サーバ証明書をプロビジョニング サーバマシンから iSeries にアップロードします。証明書は以下の場所にあります。

```
C:\Program Files\CA\Identity Manager\Provisioning  
Server\Data\Tls\server\et2_cacert.pem
```

2. DCM にログインします。

Web ブラウザを使用して `http://<hostname>:2001` に移動します。プロンプトに従って QSECOFR としてログオンし、Digital Certificate Manager リンクをクリックします。

3. [Select a Certificate Store] をクリックし、*SYSTEM 証明書ストアを選択します。このストアが存在しない場合は、「*SYSTEM」という新しいストアを作成し、次に、証明書ストア パスワードを入力します。
4. DCM を使用して、CA 証明書として証明書をインポートします。
[Manage Certificates] - [Import Certificate] をクリックします。[Certificate Authority (CA)] オプションを選択し、プロビジョニング サーバ証明書のファイル名を入力します。（これは、手順 1 で証明書をアップロードした場所です）。証明書のラベル「プロビジョニング サーバ」を入力します。
5. CA 証明書をエンドポイント *SYSTEM キーストアにインポートした後、IBM Directory クライアント QIBM_GLD_DIRSRV_CLIENT が *SYSTEM キーストアにアクセスできることを確認します。アクセスできない場合、PSA の SSL 初期化コールは失敗します。
6. [Manage Applications]-[Define CA Trust List]を開き、[Directory Services Client]を選択して、Directory Services クライアントアプリケーションがプロビジョニング サーバ証明書を信頼するように設定します。

手順 4 でプロビジョニング サーバ証明書が正しくインポートされている場合は、それらがここでリスト表示されます。

[Trusted for the Provisioning Server certificate] をクリックし、次に、[OK] をクリックします。

7. SSL ファイルに対して PUBLIC 読み取り権限を付与し、*SYSTEM 証明書ストアに読み取りアクセスを付与します。

(/QIBM/userdata/ICCS/Cert/Server/default.kdb)

親フォルダに対して読み取りおよび実行の権限を付与します。

(/QIBM/userdata/ICCS/Cert/Server)

注: ユーザ PWDSYNCH の権限は、/ファイル システムでは採用することができません。したがって、アクセス権はすべてのユーザに付与する必要があります。

パスワード同期エージェントのアンインストール

パスワード同期エージェントをアンインストールする必要がある場合は、以下の手順に従います。

パスワード確認出口点から

1. PWDSYNCH を削除します。

RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)

2. 同期エージェント ライブラリを削除します。

DLTLIB PWDSYNCH

3. PWDSYNCH ユーザを削除します。

DLTUSRPRF PWDSYNCH

4. SSL 手順に従って DCM にログオンし、*SYSTEM 証明書ストアで操作を行って、プロビジョニング サーバ証明書を削除します。

[Manage Certificates]-[Delete Certificate]をクリックして [Certificate Authority (CA)] を選択します。

[Provisioning Server] 証明書を選択して [Delete] をクリックします。

OS/400 パスワード エージェント パラメータには正しい設定が必要

「pwd_case_action」パラメータは、稼動するために、値を正しく設定する必要があります。正しい値には、以下のものが含まれます。

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

pwd_case_action = [無効な値] の場合、パスワードは強制的に大文字になります。

注: OS400 PSA 設定ファイルでフラグ pwd_case_action を pwd_to_uppercase または pwd_to_lowercase に設定するとき、提供されたパスワードがプロビジョニングサーバのパスワード ポリシー設定に準拠していない場合、パスワードはグローバルユーザに継承されない場合があります。たとえば、いくつかのパスワードポリシーでは、少なくとも 1 つの大文字または小文字の値がパスワード値に含まれることが必要です。

注: パスワード同期エージェントの設定時に QPWDLVL (パスワード レベル) システム値をメモしておいてください。

- AS400 システム上で QPWDLVL が 0 (デフォルト値) に設定されると、長さが 1 ～ 10 文字の大文字のパスワードがサポートされます。
- QPWDLVL が 2 または 3 に設定されると、長さが 1 ～ 128 文字の、大文字と小文字が混在したパスワードがサポートされます。

デフォルトでは、PSA は未変更のパスワードをプロビジョニングサーバに伝達します。しかし、QPWDLVL の値にかかわらず、"pwd_case_action" を "pwd_to_uppercase" または "pwd_to_lowercase" に設定することにより、それぞれ大文字または小文字のパスワードの伝達を PSA に強制することができます。

第 7 章: グループ

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

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

注: [動的グループ クエリ] フィールドは、グループの `directory.xml` にこのフィールドが存在する場合でも、「グループの作成」タスクやその他のグループ関連タスクには含まれません。[動的グループ クエリ] フィールドは、関連付けられたプロファイル画面を編集してタスクに含めます。

- ネスト グループ -- 他のグループを含むグループ（ユーザストアとして LDAP ディレクトリが必要）

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

このセクションには、以下のトピックが含まれています。

[静的グループの作成](#) (P. 165)

[動的グループの作成](#) (P. 166)

[動的グループ クエリのパラメータ](#) (P. 167)

[ネスト グループの作成](#) (P. 169)

[静的グループ、動的グループ、ネスト グループの例](#) (P. 171)

[グループ管理者](#) (P. 172)

静的グループの作成

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

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

静的グループを作成する方法

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

動的グループの作成

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

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

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

また、このクエリを変更して、米国以外の従業員を検出することもできます。

[静的グループ、動的グループ、ネスト グループの例 \(P. 171\)](#)に、静的グループ、動的グループ、およびネスト グループによって作成されたグループの例を示します。

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

注: 動的グループを有効にするには、システム管理者は、ディレクトリ設定ファイル (directory.xml) 内のサポートを設定します。

- [Directory Groups Behavior] セクションに GroupTypes エlementを以下のよう追加します。

<GroupTypes type=type>

type は [NESTED](#) (P. 169)、DYNAMIC または ALL にすることができます。

GroupTypes は大文字小文字が区別されます。

- 既知の属性である %DYNAMIC_GROUP_MEMBERSHIP% をユーザストアに存在する物理属性にマップします。

動的グループを作成する方法

1. ユーザ コンソールで、[グループ] - [グループの作成] を選択します。
2. 新規グループの作成またはグループのコピーの作成を選択し、[OK] をクリックします。
3. [プロファイル] タブで、グループ名、グループの組織、説明、グループの管理者名を入力します。
4. [動的グループ クエリ] フィールドに、以下の例のような LDAP 検索フィルタを入力します。

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

5. [サブミット] をクリックします。

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

動的グループ クエリのパラメータ

検索時には、以下の動的なクエリ パラメータを使用できます。

ldap:///<検索ベース DN>??<検索範囲>?<検索フィルタ>

- <検索ベース DN> には、LDAP ディレクトリ内の検索開始ポイントを指定します。クエリにベース DN を指定しない場合は、グループの組織がデフォルトのベース DN となります。

- <検索範囲>には、検索範囲を指定します。以下の値を使用できます。
 - sub -- ベース DN レベルとそれより下位にあるエントリを返します。
 - one -- URL で指定したベース DN よりも 1 レベル下にあるエントリを返します。（デフォルト）
 - base -- 検索オプションとして指定したベースを無視して、代わりに one を使用します。

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

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

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

(<論理演算子><比較><比較...>)

- <論理演算子>には、以下のいずれかを使用します。

論理 OR : |

論理 AND : &

論理 NOT : !

- <比較>には、<属性><演算子><値>を指定します。

以下に例を示します。

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

デフォルトの検索フィルタは (objectclass=*) です。

動的クエリを作成する場合、以下の点に注意が必要です。

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

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

- LDAP サーバホスト名またはポート番号は指定できません。すべての検索は、環境と関連付けられた LDAP ディレクトリ内で行われます。

以下の表にはサンプル LDAP クエリが含まれます。

説明	クエリ
マネージャになっているユーザ 全員	ldap:///o=MyCorporation??sub?(title=Manager)

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

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

ネストグループの作成

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

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

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

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

[静的グループ、動的グループ、ネストグループの例 \(P. 171\)](#)の図に、静的グループ、動的グループ、およびネストグループによって作成された親グループを示します。

ネストグループを作成する前に、以下の点に注意してください。

- ユーザコンソールで、グループの静的メンバリストからネストグループを追加または変更できるのは、[グループメンバの変更]タスクを持つ管理者のみです。

- グループからメンバの変更、追加、削除を実行できるのは、適切な管理権限を持つユーザのみです。

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

- ネストグループを有効にするには、システム管理者は、ディレクトリ設定ファイル (directory.xml) 内のネストグループのサポートを設定します。

- [Directory Groups Behavior] セクションに GroupTypes エレメントを以下のように追加します。

```
<GroupTypes type=type>
```

type は NESTED、[DYNAMIC](#) (P. 166)、または ALL にすることができます。

GroupTypes は大文字小文字が区別されます。

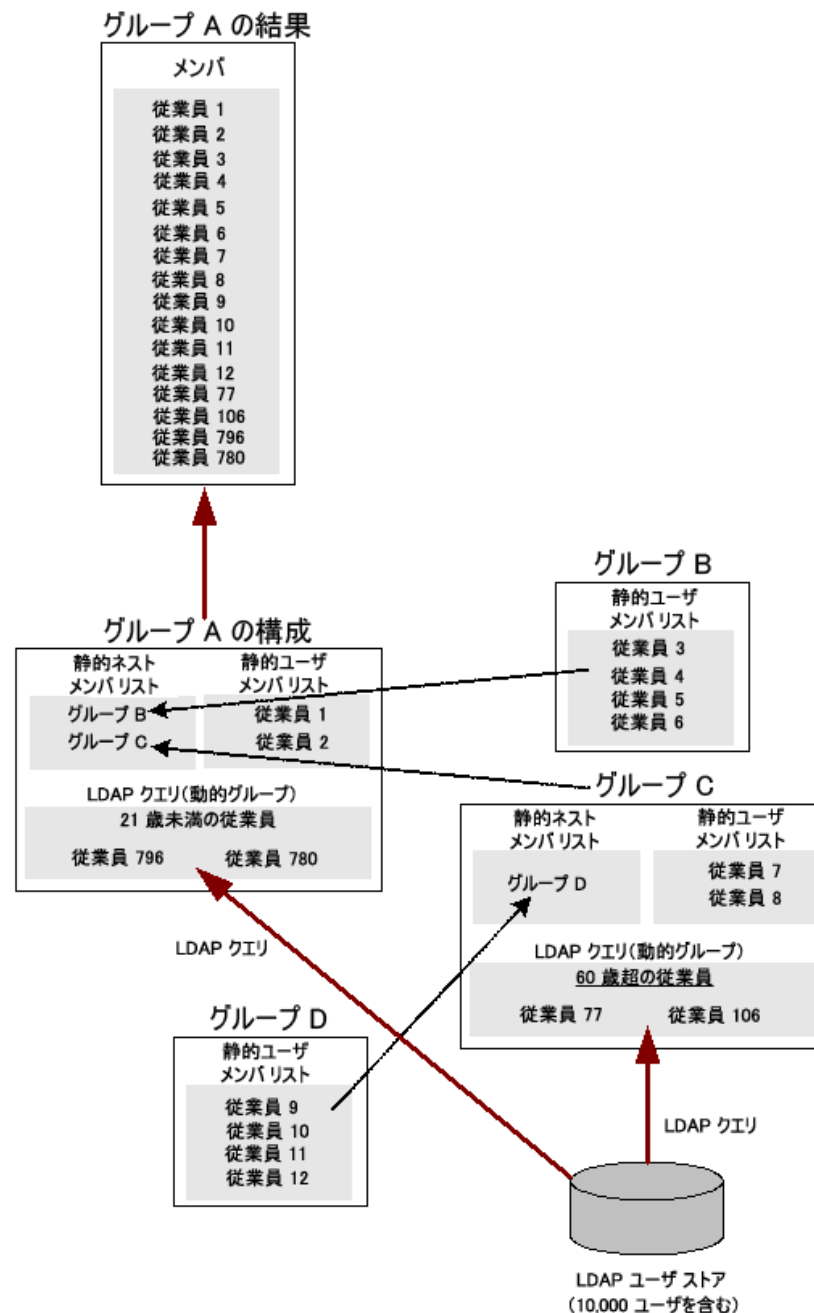
- 既知の属性である %NESTED_GROUP_MEMBERSHIP% をユーザストアに存在する物理属性にマップします。

ネストグループを作成する方法

1. ユーザコンソールで、[グループ] - [グループの作成] を選択します。
2. 新規グループの作成またはグループのコピーの作成を選択し、[OK] をクリックします。
3. [プロファイル] タブで、グループ名、グループの組織、説明、グループの管理者名を入力します。
4. [メンバシップ] タブで、以下の手順に従います。
 - a. [グループの追加] をクリックし、このグループにネストグループを追加します。
 - b. 既存のグループを検索します。
 - c. 対象となるグループの横にチェックマークを付け、[選択] をクリックします。
 - d. [サブミット] をクリックします。

静的グループ、動的グループ、ネストグループの例

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



以下に、上記の例について説明します

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

グループ管理者

〔作成〕または〔グループの変更〕のタスクの〔管理者〕タブでは、グループの管理者としてユーザおよびグループを指定できます。ユーザをグループ管理者として割り当てる場合は、その管理者がグループを管理できるだけの適切なスコープを持つロールが割り当てられていることを確認してください。例：

1. グループの管理者としてユーザを割り当てるには〔グループの変更〕を使用します。
2. そのユーザに〔グループ メンバの変更〕などのグループ管理タスクを持った管理ロールまたは〔グループ〕タブを持ったユーザ管理タスクを割り当てます。
3. ロールがグループ上に適切なスコープを持つことを確認します。
 - a. グループ管理タスクで割り当てたロール上で〔管理ロールの表示〕を使用します。
 - b. 〔メンバ〕タブで、以下を含むポリシーがあることを確認します。

グループ管理者が条件を満たすメンバルール

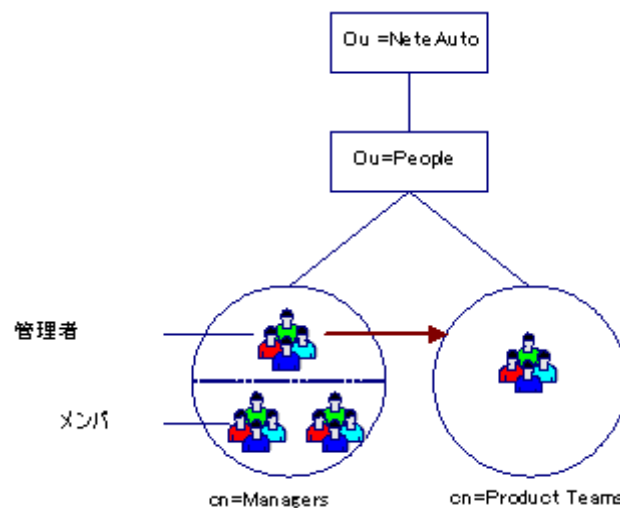
このグループを含むスコープ ルール

グループに追加されるユーザが含まれるスコープ ルール

注：グループをその他のグループの管理者として有効にするには、システム管理者は、ディレクトリ設定ファイル（`directory.xml`）にグループ管理者サポートを設定します。

- 〔Directory AdminGroups Behavior〕セクションで、`AdminGroupTypes type=ALL` を設定します。 `AdminGroupTypes` は大文字小文字が区別されます。
- 既知の属性である `%GROUP_ADMIN_GROUP%` をユーザストアに存在する物理属性にマップします。

管理者としてグループを割り当てるとき、そのグループの管理者のみが作成または変更しているグループの管理者になります。指定する管理者グループのメンバーは、グループを管理する権限がありません。以下の図に、あるグループが別のグループの管理者になる場合の例を示します。



この例の内容

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

第 8 章：管理対象のエンドポイント アカウ ント

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

このセクションには、以下のトピックが含まれています。

[管理エンドポイントの統合](#) (P. 176)

[ユーザ、アカウント、およびロールの同期](#) (P. 183)

[エンドポイント アカウントとの逆同期](#) (P. 191)

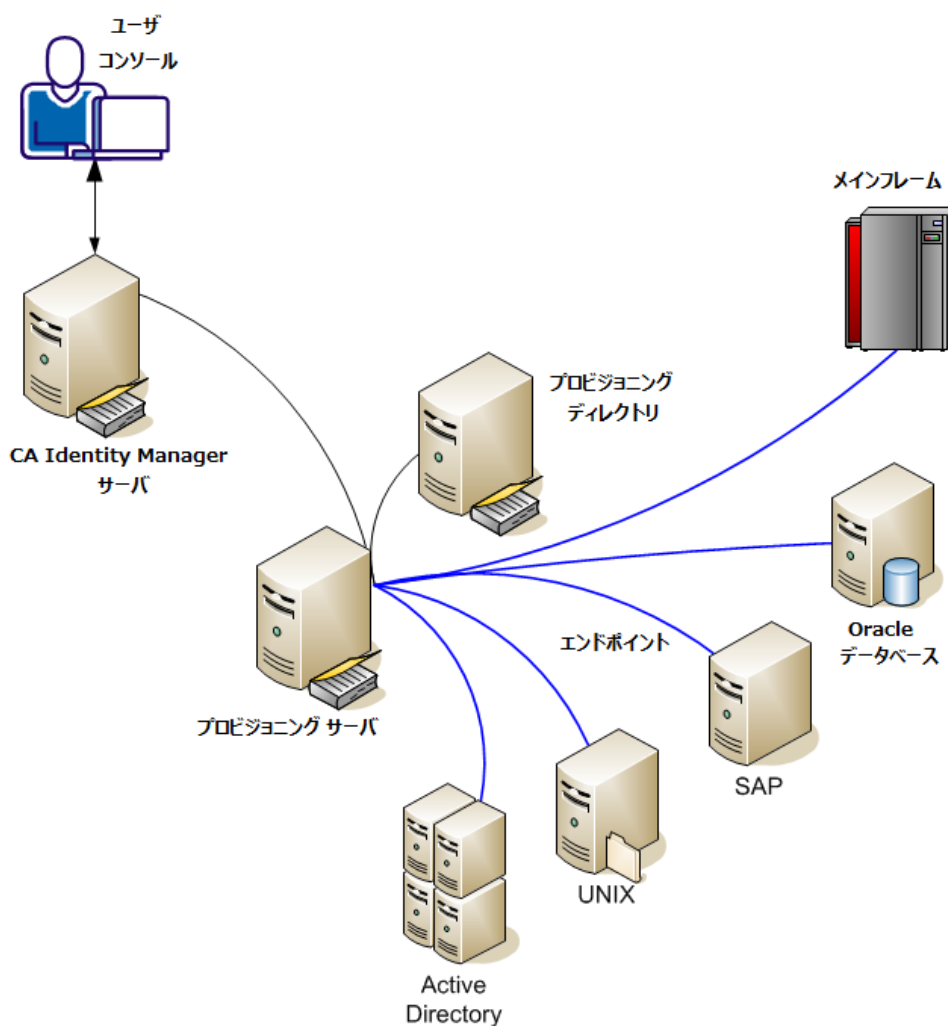
[エンドポイントのカスタム属性の拡張](#) (P. 202)

[アカウント タスク](#) (P. 204)

[詳細なアカウント操作](#) (P. 210)

管理エンドポイントの統合

CA Identity Manager では、複数のシステム上のアカウントを、単一のユーザ インターフェイスであるユーザ コンソールから管理できます。アカウントは、「管理 エンドポイント」(または単に「エンドポイント」)と呼ばれるシステム上に存在します。以下の例では、5つのエンドポイント上のユーザを管理します。



任意の組み合わせのエンドポイント上にあるアカウントをユーザに割り当てることができます。エンドポイントの統合を行うと、**CA Identity Manager**により各エンドポイント アカウントがプロビジョニング ディレクトリ内のユーザに関連付けされます。

以下の手順は、エンドポイントを統合する方法について説明します。その結果、エンドポイント アカウントをユーザ コンソールから管理できるようになります。

1. [ロール定義ファイルのインポート](#) (P. 177)
2. 関連ルールの作成
3. 環境へのエンドポイントの追加
4. 検索および関連付けの定義の作成
5. エンドポイントの検索および関連付け

ロール定義ファイルのインポート

新しいエンドポイントに適用されるファイルからロール定義をインポートします。この手順には、管理コンソールへのアクセスが必要です。

次の手順に従ってください:

1. 管理コンソールで、[Environments] をクリックします。
2. エンドポイントを追加する環境を選択します。
3. [Role and Task Settings] をクリックします。
4. [Import] をクリックします。
5. [Endpoint Type] の下のエンドポイントを選択します。
6. [Finish] をクリックします。

インポートのステータスが現在のウィンドウに表示されます。

7. [Continue] をクリックして終了します。
8. 環境を再起動すると、変更が有効になります。

関連ルールの作成

ホスティング管理者、または[関連属性の設定] タスクを持つ管理者は、ユーザがエンドポイントを検索するときに使用されるルールを作成できます。[検索および関連付けを実行] タスクは、タスクの関連についての部分でこれらのルールを使用します。

関連ルールは、エンドポイント アカウント属性がユーザ コンソール内のユーザ属性にどのようにマップされるかを決定します。たとえば、**Access Control** で、**AccountName** という属性が存在するとします。これをユーザ コンソール内の **FullName** にマップするルールを作成することができます。ルールが、1つのユーザ属性に対して2つのマッピングを適用するようになっている場合、最初のパラメータ値が使用されます。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. [システム] - [プロビジョニング設定] - [関連属性の設定] をクリックします。
3. [追加] をクリックします。
4. 以下のように関連ルールを定義します。
 - a. グローバルユーザ属性リストを選択します。

この値は、プロビジョニング ディレクトリにリスト表示されたユーザ属性を参照します。
 - b. [特定のアカウント属性の設定] チェック ボックスを有効にします。
 - c. エンドポイント タイプを選択します。
 - d. グローバルユーザ属性に適用されるアカウント属性を選択します。
 - e. 任意で、[サブストリング] フィールドに入力します。

[サブストリング開始] フィールドが空の場合、処理は文字列の最初から開始します。[サブストリング終了] フィールドが空の場合、処理は文字列の最後から開始します。
5. [OK] をクリックします。
6. [サブミット] をクリックします。

注: 関連ルールを変更した場合は毎回、以前にエンドポイントの検索済みであったとしても、必ずエンドポイントの検索を行ってください。

関連ルールの例

以下の例は、**Active Directory** エンドポイント用のサンプル設定です。

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
CustomField01=ActiveDirectory:Telephone
```

以下のアクションは、以前は関連していなかったアカウントで、**Active Directory** コンテナ内でアカウントを関連する際に見つかったものについて発生します。

1. プロビジョニング サーバは最初のパラメータ値 (**GlobalUserName**) を **Active Directory** エンドポイント アカウント属性 (**NT_AccountID**) と比較します。サーバは、一意のグローバル ユーザで名前がアカウントの属性値 **NT_AccountID** に一致するものの検索を試行します。一意の一致が見つかった場合、プロビジョニング サーバはアカウントをグローバル ユーザに関連付けます。複数の一致が見つかった場合、プロビジョニング サーバは手順 5 を実行します。一致が見つからない場合、プロビジョニング サーバは次の手順を実行します。
2. プロビジョニング サーバは 2 番目のパラメータ値 (**FullName=LDAP Namespace:globalFullName**) を検証します。この値は別のエンドポイント タイプに固有であるためスキップされ、プロビジョニング サーバは次の手順を実行します。
3. プロビジョニング サーバは 3 番目のパラメータ値 (**FullName=ActiveDirectory:DisplayName**) を検証します。この値は **Active Directory** に固有であるので、これが使用されます。サーバは、一意のグローバル ユーザで、**FullName** がアカウントの属性値 **DisplayName** に一致するものの検索を試行します。一意の一致が見つかった場合、プロビジョニング サーバはアカウントをグローバル ユーザに関連付けます。複数の一致が見つかった場合、プロビジョニング サーバは手順 5 を実行します。一致が見つからない場合、プロビジョニング サーバは手順 4 を実行します。
4. プロビジョニング サーバは最後のパラメータ値 (**CustomField01=ActiveDirectory:Telephone**) を検証します。この値は **Active Directory** に固有であるので、これが使用されます。サーバは、一意のグローバル ユーザで、**Custom Field #01** 属性がアカウントの属性値 **Telephone** に一致するものの検索を試行します。システム タスクのグローバル プロパティを使用してカスタム グローバル ユーザ属性に与えた名前は、ここでは表示されません。一意の一致が見つかった場合、プロビジョニング サーバはアカウントをグローバル ユーザに関連付けます。複数の一致が見つかった場合、プロビジョニング サーバは手順 5 を実行します。一致が見つからない場合、プロビジョニング サーバは次の手順を実行します。
5. プロビジョニング サーバはアカウントを [デフォルト ユーザ] オブジェクトに関連付けます。[デフォルト ユーザ] オブジェクトが存在しない場合、サーバはそれを作成します。

環境へのエンドポイントの追加

管理対象の環境にエンドポイントを追加します。[エンドポイントの作成] タスクを持つ管理者が、この手順を実行できます。

次の手順に従ってください:

1. [エンドポイント] - [エンドポイントの管理] - [エンドポイントの作成] を選択します。
2. エンドポイント タイプを選択します。
3. フィールドに入力してタブを完了します。
必須フィールドは、赤丸で始まっています。

注: エンドポイントの名前に、# 記号を使用しないようにしてください。この文字は検索できません。

4. [サブミット] をクリックします。

これで、[検索および関連付けの定義](#) (P. 180)を作成して、エンドポイントのアカウントを管理する準備ができました。

検索および関連付けの定義の作成

エンドポイントに存在するユーザを追加するには、そのエンドポイント用の検索および関連付けの定義を作成します。[検索および関連付けの定義の作成] タスクを持つ管理者が、定義を作成できます。

次の手順に従ってください:

1. 環境内で、[エンドポイント] - [検索および関連付けの定義] - [検索および関連付けの定義の作成] をクリックします。
2. 新しい定義を開始するには [OK] をクリックします。
3. [検索および関連付けの名前] にわかりやすい名前を入力します。
4. [コンテナ/エンドポイント/検索メソッドの選択] をクリックして、エンドポイントとコンテナ（これらが存在する場合）を選択します。大きなエンドポイントについては、コンテナ検索に時間がかかる場合があります。検索フィルタを使用すると、検索を絞り込むことができます。
5. コンテナに対する検索メソッドをクリックします。[検索および関連付け]のプロセスには、選択したコンテナと、そのサブコンテナも含まれます。ディレクトリ コンテナについては、そのサブツリーにあるコンテナもすべて含まれます。

6. [検索/関連付けアクション] をクリックして、以下を実行します。

- **管理オブジェクトをディレクトリで検索** - エンドポイントに保存されていて、プロビジョニングディレクトリには保存されていないオブジェクトを検索します。
- **アカウントをユーザに関連付け** - 検索機能で検出されたオブジェクトをプロビジョニングディレクトリのユーザに関連付けます。2つの関連付けのいずれかを選択します。

- **既存のユーザを使用**

各アカウントを以前に作成したユーザと一致させる相関ルールの場合は、これを選択します。

ユーザが検出されると、アカウントがそのユーザに関連付けられます。複数のユーザが検出された場合は、アカウントはデフォルトユーザと関連付けられます。ユーザが検出されない場合は、このオプションによってユーザ(必須属性がすべてわかっている場合)が作成され、そのユーザとアカウントが関連付けられます。それ以外の場合は、アカウントがデフォルトユーザに関連付けられます。

- **必要に応じてユーザを作成**

プライマリ エンドポイントのアカウントを関連付ける場合は、これを選択します。このオプションは、エンドポイント上のアカウントがユーザと完全に同じ名前であることが前提です。このオプションでは、関連付け - 一致アルゴリズムを使用しません。代わりに、各アカウントが、同じ名前のユーザに関連付けられます。ユーザが存在しない場合は、作成されます。アカウントはデフォルトユーザには関連付けられません。

- **ユーザフィールドの更新** - オブジェクトフィールドとユーザフィールドの間にマッピングが存在する場合、ユーザフィールドはオブジェクトフィールドからのデータを使用して更新されます。

ユーザは、フルネーム、アドレス、電話番号などのオプションの属性を含めずに作成されます。エンドポイントを最初に取得するときに、このオプションを使用して、アカウント属性値でこれらのユーザ属性を設定します。その後続く検索および関連付けの間に、このオプションを使用してユーザ属性を更新し、CA Identity Manager 以外のツールなどによってアカウント属性に加えられた変更を適用します。

7. [サブミット] をクリックします。

これで、[検索および関連付け] タスクを持つ管理者によるエンドポイントの統合が完了しました。

エンドポイントの検索および関連付け

ホスティング管理者、または「検索および関連付けを実行」タスクを持つ別の管理者が、この手順を実行します。タスクの検索段階では、エンドポイント内のアカウントを特定します。関連付け段階では、アカウントを **CA Identity Manager** 内のユーザと一致させるか、またはアカウントを作成します。

次の手順に従ってください:

1. 環境内で、[エンドポイント] - [検索および関連付けを実行] をクリックします。
2. [今すぐ実行] を選択して検索および関連付けをすぐに実行するか、[\[新規ジョブのスケジュール \(P. 439\)\]](#) を選択して検索および関連付けを後ほど、または反復スケジュールで実行します。

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

3. [検索および関連付けの定義] をクリックして実行します。
4. [サブミット] をクリックします。

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

5. 以下の方法で、タスクが成功したかどうかを確認します。
 - a. [システム] - [サブミット済みタスクの表示] をクリックします。
 - b. [タスク名] フィールドに、「検索および関連付けを実行」と入力します。
 - c. [検索] をクリックします。

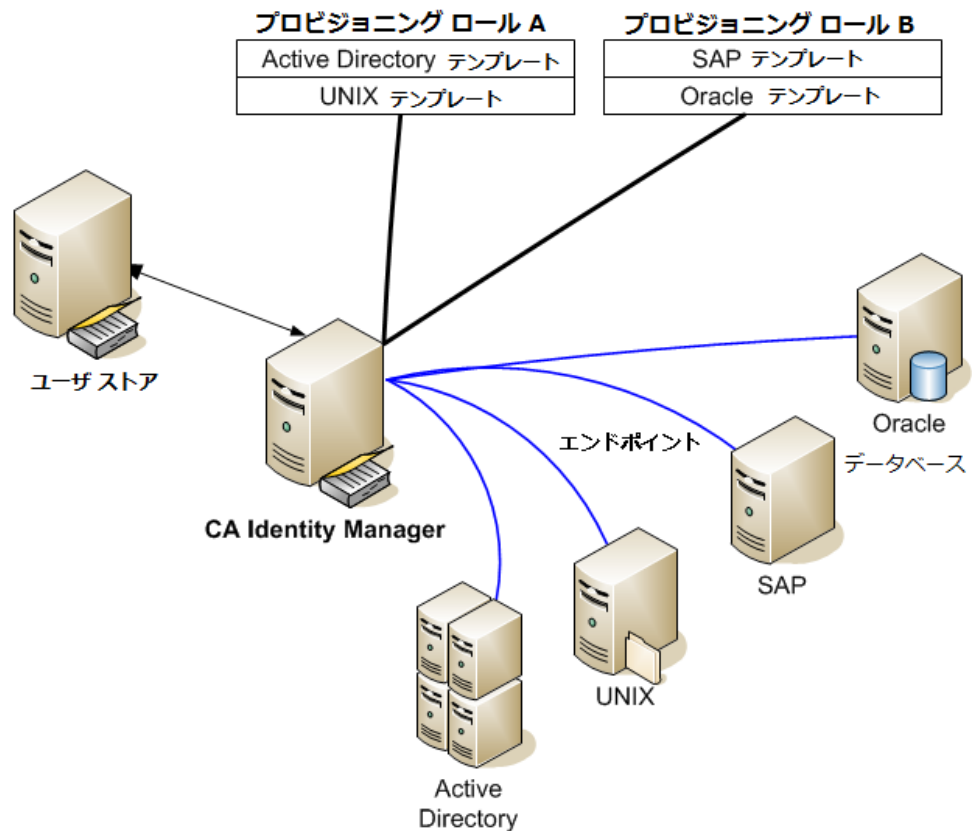
タスクが成功したかどうかの結果が表示されます。

注: [サブミット済みタスクの表示] (**VST**) でタスクステータスを表示し、[検索および関連付け] タスクを中止することができます。タスクを中止すると、タスクの処理が停止し、タスクのステータスは、中止した時点のステータスのままになります。通知が生成されて送信され、システム全体が同期されます。

ユーザ、アカウント、およびロールの同期

複数のエンドポイントおよびアカウントを単一のユーザ管理システムに統合すると、同期が失われる場合があります。ユーザに割り当てられたプロビジョニングロールまたはアカウントテンプレートは、そのユーザの実際のアカウントと異なることがあります。

たとえば、2つのプロビジョニングロール（Active Directory と UNIX のアカウントテンプレートを持つロールと、SAP および Oracle のテンプレートを持つロール）がある状況を考えてください。ユーザ `john_smith` にはプロビジョニングロール A（Active Directory と UNIX のアカウントテンプレートが含まれる）がありますが、このユーザは Active Directory アカウントしか持っていない。これは、このロールがユーザに割り当てられた後、ロールに UNIX アカウントテンプレートが追加されたためである可能性があります。そこで管理者は、ユーザを現在のロール定義と同期します。



ユーザがプロビジョニング ロールまたはアカウント テンプレートとの同期を失う他の理由には、以下のようなものがあります。

- ネットワークでハードウェアまたはソフトウェアの問題があるために、以前に必要なアカウントを作成しようとして失敗し、存在しないアカウントが生じています。
- プロビジョニング ロールおよびアカウント テンプレートが変更されたため、不要なアカウントまたは存在しないアカウントがあります。
- アカウント テンプレートが作成された後にアカウントが割り当てられたため、アカウントは存在しますがアカウント テンプレートと同期していません。
- アカウントを後で作成するよう指定されているため、新しいアカウントの作成が遅れています。
- 新しいエンドポイントが取得されました。検索および関連付けの際、プロビジョニング サーバは、プロビジョニング ロールを自動的にユーザに割り当てませんでした。ユーザはロールを更新し、このエンドポイント上のアカウントを必要とするユーザを示すようにします。ユーザに関連付けられているアカウントは、ユーザの同期時に、不要なアカウントとしてリストされます。
- 既存のアカウントをユーザにコピーする際、そのアカウントがユーザに割り当てられました。
- ユーザをロールに割り当てる以外の方法で、ユーザに対してアカウントが作成されました。たとえば、そのユーザのプロビジョニング ロールにないアカウント テンプレートにユーザをコピーしました。そのアカウントは、不要なアカウント、または不要なアカウント テンプレートを持つアカウントとしてリスト表示されます。ユーザをエンドポイントにコピーし、デフォルトアカウント テンプレートを使用してアカウントを作成すると、そのアカウントは不要なアカウントになることがあります。

以下のセクションでは、3つのタイプの同期を実行する方法について説明します。

1. [ユーザとロールの同期](#) (P. 185)。
2. [ユーザとアカウント テンプレートの同期](#) (P. 186)。
3. [エンドポイント アカウントとアカウント テンプレートの同期](#) (P. 187)。

ユーザとロールの同期

このタスクは、ユーザに割り当てられているプロビジョニングロールに対してアカウントが準拠するように、アカウントを作成、更新、または削除します。たとえば、管理者はエンドポイント上でネイティブツールを使用してアカウントを追加または削除しますが、ユーザはそのエンドポイントを再検索してプロビジョニングディレクトリを更新していません。そのため、ユーザには不要または存在しないアカウントがあります。このタスクにより、各アカウントが正しいアカウントテンプレートに属していることも保証されます。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. [タスク] - [ユーザ] - [同期] - [ロール同期のチェック] を選択します。
3. ユーザを選択します。

有効なアカウント、不要なアカウント、および存在しないアカウントが画面に表示されます。

4. アカウントをこのロールのテンプレートと一致させるために、[同期] をクリックします。
 - a. チェック ボックスを選択して、エンドポイント上でアカウントを作成することができます。ユーザの複数のアカウントテンプレートが同じアカウントを規定している場合、関連するすべてのアカウントテンプレートをマージすることによって、アカウントが作成されます。

このアカウントは、これらのアカウントテンプレートに割り当てられますが、これらのテンプレートは、現在のところアカウントと同期していません。
 - b. チェック ボックスを選択して、不要なアカウントを削除することができます。しかし、これらのアカウントを持つ正当な理由がある場合があります。その場合は、このオプションをオフにしておきます。

アカウント削除機能が無効になっているエンドポイントもあり、その場合はアカウントは削除されません。

ユーザとアカウント テンプレートの同期

このタスクは、エンドポイント アカウントの属性を、ユーザの関連するアカウント テンプレートと同期します。ただし、フル同期は以下の要因に依存します。

- アカウントのフル同期は 2 つの状況で発生します。アカウント テンプレートが[強い同期](#) (P. 189)を使用するか、2 つ以上のアカウント テンプレートがアカウントに追加されています。
- アカウント テンプレートが[弱い同期](#) (P. 188)を使用する場合、このタスクはこのテンプレートのみを含むアカウント同期を開始します。更新の前に、アカウントがすでに他のアカウント テンプレートとのアカウント同期とずれてしまっていた場合は、それ以降も、アカウント同期とずれることがあります。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. [タスク] - [ユーザ] - [同期] - [アカウント テンプレート同期のチェック] を選択します。
3. ユーザを選択します。

有効なアカウント、不要なアカウント、および存在しないアカウントが画面に表示されます。

4. [同期] をクリックして、アカウントをテンプレートと一致させます。
 - a. チェック ボックスを選択して、エンドポイント上でアカウントを作成することができます。ユーザの複数のアカウント テンプレートが同じアカウントを規定している場合、関連するアカウント テンプレートをマージすることによって、アカウントが作成されます。

このアカウントは、それと同期していないアカウント テンプレートに割り当てられています。新しく作成されたアカウントでは、アカウントの同期は必要ありません。

- b. チェック ボックスを選択して、不要なアカウントを削除することができます。しかし、これらのアカウントを持つ正当な理由がある場合があります。その場合は、このオプションをオフにしておきます。

アカウント削除機能が無効になっているエンドポイントもあり、その場合はアカウントは削除されません。

新しいアカウントだけの属性

アカウントテンプレートでは、一部の属性はアカウントの作成時のみに適用されます。たとえば、**Password** 属性は、新しいアカウントのパスワードを定義するルール表現です。このルール表現は、アカウントのパスワードを変更することはありません。パスワードルール表現への変更は、ルール表現が設定された後に作成されたアカウントだけに影響します。

同様に、読み取り専用アカウント属性のテンプレートルール表現は、ルール表現が設定された後に作成されたアカウントだけに影響します。変更は、既存のアカウントには何の影響ももたらしません。

エンドポイント アカウントとアカウント テンプレートの同期

このタスクは、関連するアカウントテンプレートの変更後にエンドポイントアカウントを同期します。たとえば、**Active Directory** アカウントにグループがありませんが、関連するアカウントテンプレートはグループを含むように定義されています。

次の手順に従ってください：

1. ユーザ コンソールにログインします。
2. [タスク] - [エンドポイント] - [エンドポイントの管理] - [エンドポイント アカウント同期のチェック] を選択します。
3. エンドポイントを選択します。

そのエンドポイント上のアカウント、関連するアカウントテンプレート、および同期されていない属性が画面に表示されます。

4. [同期] をクリックして、これらのアカウントの属性をアカウントテンプレートで定義されているものと一致させます。

アカウントテンプレートに対して行った変更は、既存のアカウントに次のように影響します。

- 機能属性の値を変更すると、対応するアカウント属性が更新され、アカウントテンプレートの属性値と同期されます。弱い同期と強い同期の説明を参照してください。
- 一部のアカウント属性は、コネクタにより、アカウントテンプレートの変更時には更新されないように指定されています。例としては、エンドポイントタイプがアカウント作成時にのみ設定できる属性や、パスワード属性があります。

更新対象となる属性

アカウントテンプレートで機能属性を変更すると、アカウント上の対応する属性が変更されます。この変更はアカウントの属性に影響を及ぼします。影響は以下の要因に基づきます。

- アカウントテンプレートが弱い同期で定義されているか強い同期で定義されているか
- アカウントが複数のアカウントテンプレートに属しているかどうか

弱い同期

*弱い同期*では、ユーザのアカウントに対する最小の機能属性だけをユーザが持つことが保証されます。大部分の種類のエンドポイントでは、弱い同期がデフォルトです。弱い同期を使用するテンプレートを更新する場合、CA Identity Manager は以下のように機能属性を更新します。

- アカウントテンプレートで数値フィールドが更新されていて、新しい数値がアカウントの数値より大きい場合、新しい数値に合うようにアカウントの値が変更されます。
- 選択されていなかったチェックボックスをアカウントテンプレートで選択すると、そのチェックボックスが選択されていないすべてのアカウントでチェックボックスが更新されます。
- アカウントテンプレートで一覧を変更すると、アカウントの値の一覧になかった新しい一覧の値が収まるようにすべてのアカウントが更新されます。

1つのアカウントが他の複数のアカウントテンプレートにも属している場合、強い同期であれ弱い同期であれ、変更のあるテンプレートだけが参照されます。この方がすべてのアカウントテンプレートを検証するより効率的です。弱い同期ではアカウントに機能が追加されるだけなので、これら他のアカウントテンプレートを参照する必要は通常はありません。

注: 弱い同期アカウントテンプレートから伝達された変更が機能の削除や低減を行うものであった場合、一部のアカウントが非同期のままになることがあります。弱い同期では機能の削除や低減は決して行われないことに注意してください。アカウントの他のテンプレートが参照されないので、弱い同期で十分かどうかがこの伝達では考慮されません。

この状況では、アカウントをそのアカウントテンプレートと同期するには [ユーザとアカウントテンプレートの同期] を使用します。

強い同期

強い同期により、アカウント テンプレートで指定されているものと同じアカウント属性をアカウントが持っていることが保証されます。

たとえば、既存の **UNIX** アカウント テンプレートにグループを追加するとします。最初に、アカウント テンプレートでは **Staff** グループのアカウント メンバを作成しました。次に、**Staff** グループと **System** グループの両方のアカウント メンバを作成します。このアカウント テンプレートに関連付けられているすべてのアカウントは、それぞれのアカウントが **Staff** グループおよび **System** グループのメンバである場合（および他のいずれのグループでもない場合）、同期されているとみなされます。**Staff** グループに含まれていないすべてのアカウントは、両方のグループに追加されます。

その他にも、以下の状況を考慮する必要があります。

- アカウント テンプレートで強い同期を使用している場合、**Staff** および **System** 以外のグループに属しているアカウントは、これらの追加グループから除外されます。
- アカウント テンプレートで弱い同期を使用している場合、アカウントは **Staff** グループおよび **System** グループに追加されます。他のグループが定義されているアカウントは、そのグループのメンバのままになります。

注: アカウントとアカウント テンプレートを定期的に同期することにより、アカウントおよびそのアカウント テンプレートの同期が確実に保たれます。

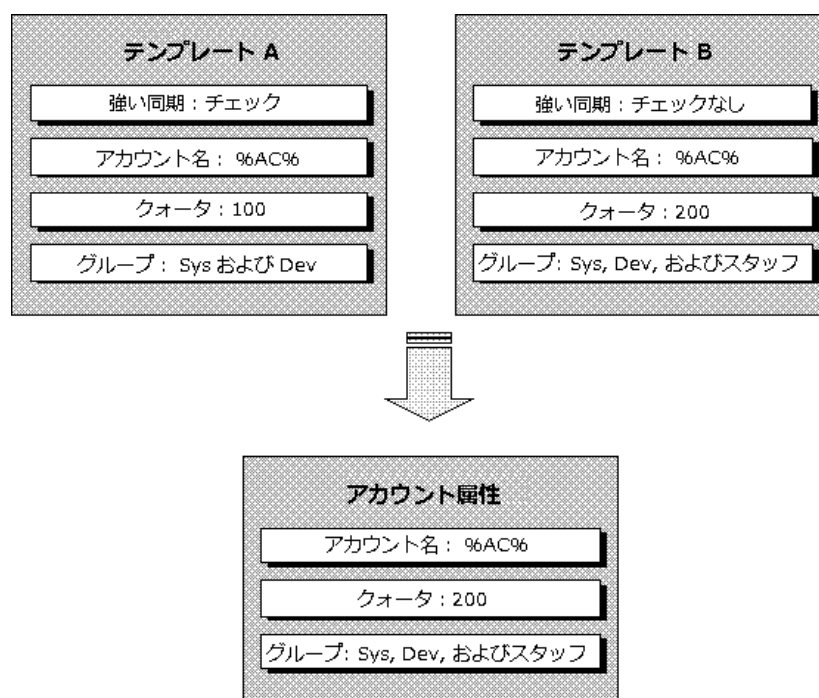
複数のテンプレートを持つアカウント

同期は、アカウントが複数のアカウント テンプレートに属しているかどうかによっても異なります。アカウントがアカウント テンプレートを 1 つのみ持ち、そのテンプレートの同期が強い場合、各属性は、アカウント テンプレート属性値の評価対象に正確に一致するように更新されます。その結果、属性は最初の属性と同じ値になります。

ユーザが複数のプロビジョニング ロールに属し、それぞれのロールが同じ管理対象エンドポイントに対して一定のレベルのアクセス権を持つ場合、アカウントは複数のアカウント テンプレートに属する場合があります。この状態になると、**CA Identity Manager** はこれらのアカウント テンプレートを 1 つの有効なアカウント テンプレートにまとめ、個々のアカウント テンプレートの機能を合わせた上位集合として規定します。個々のアカウント テンプレートすべての同期が弱い場合、アカウント テンプレート単体は弱い同期となりますが、アカウント テンプレートのうち強い同期を持つものが 1 つでもあると、強い同期となります。

注: アカウントテンプレートが1つのアカウントのみを制御している場合、弱い同期のみまたは強い同期のみを使用することが多いです。これは、ユーザに必要なアクセス権を企業のロールが完全に定義しているかどうかによって決まります。ユーザのロールが明確でなく、ユーザのアカウントに柔軟に対応する必要がある場合、弱い同期を使用します。ユーザに必要なアクセス権を明確に指定するロールを定義する場合、強い同期を使用します。

以下の例は、複数のアカウントテンプレートが1つの有効なアカウントテンプレートにまとめられる方法を示します。この例では、1つのアカウントテンプレートが弱い同期としてマークされ、もう一方のテンプレートが強い同期としてマークされています。したがって、2つのアカウントテンプレートをまとめて作成された有効なアカウントテンプレートは、強い同期を持つアカウントテンプレートになります。整数を持つ **Quota** 属性は、2つのアカウントテンプレートから大きい方の値を取り、複数値を持つ **Groups** 属性は、2つのポリシーの値を合わせたものになります。



エンドポイント アカウントとの逆同期

アカウントの作成、削除、および変更は **CA Identity Manager** の役目ですが、エンドポイントシステム ユーザ自らがこれらの操作を行わずにいることはできません。このような状況が発生する原因には、緊急事態、ハッカーなどの悪意によるものなどがあります。逆同期は、**CA Identity Manager** アカウントおよびエンドポイント上のアカウント間の相違を特定することにより、各エンドポイントにユーザが持つアカウントをコントロールできます。

たとえば、外部ツールを使用して **Active Directory** ドメインにアカウントが作成された場合、**CA Identity Manager** はこの潜在的なセキュリティ問題を認識する必要があります。さらに、**CA Identity Manager** をバイパスすることは、承認プロセスの不足および監査レポートの原因となります。

CA Identity Manager および管理対象エンドポイント間の 2 種類の相違を以下に示します。

- 新規アカウントの検出
- 既存アカウント内での変更

両方のケースとも、ポリシーを定義することで変更に対処できます。次に、検索および関連付けを使用して **CA Identity Manager** を更新し、ポリシーの実行をトリガします。

逆同期の仕組み

エンドポイント アカウントの逆同期は、以下のように発生します。

1. 管理者か悪意のあるユーザが、エンドポイント上のアカウントを作成または変更します。
2. このエンドポイントで検索および関連付けが実行されると、新規または変更されたアカウントが検出されます。
3. プロビジョニング サーバから通知が **CA Identity Manager** サーバに送られます。
4. **CA Identity Manager** サーバがエンドポイントの変更に一致する逆同期ポリシーを検索します。
5. 一致するポリシーが見つかり、実行されます。複数のポリシーがこのアカウントに一致し、これらのポリシーが同じスコープを持つ場合、最高優先度のポリシーが実行されます。
6. ポリシーによって、次のいずれかのアクションが発生します。
 - 新規アカウントに対して、ポリシーはアカウントの承諾、削除、または一時停、あるいはワークフロー承認への送信を行います。
 - 変更されたアカウントに対しては、ポリシーは値の承諾、最後の既知の値に戻す、またはワークフロー承認への送信を行います。
7. ワークフローが選択された場合、このワークフローの新規イベントが生成され、準備が完了します。次に、次のいずれかのアクションが発生します。
 - 新規アカウントに対して、承認者はアカウントの承諾、削除、または一時停止、あるいはユーザへの割り当てを行うことができます。
 - 変更されたアカウントでは、ワークフロー プロセスは値がユーザ コンソールで変更された場合と同じですが、拒否された値はエンドポイントで元に戻されます。

エンドポイント属性のマッピング

エンドポイント アカウントの属性に逆同期を使用するには、その属性をユーザ コンソールに表示される属性にマッピングする必要があります。アカウント名やパスワードなどの一部の属性は、デフォルトでマッピングされます。その他の属性はマッピングされません。たとえば、**Active Directory** 属性グループ メンバシップはマッピングされません。一部のエンドポイント タイプでは、属性はマッピングされません。

属性がマッピングできるかどうかを確認する方法

1. ユーザ コンソールで、[エンドポイント] をクリックするか、または [タスク] - [エンドポイント] をクリックします。
2. [変更の逆同期] - [変更済みアカウント逆同期ポリシーの作成]
3. 新規ポリシーまたはポリシーのコピーのどちらを作成するかを選択します。
4. [エンドポイント タイプ] をクリックして、[Active Directory] などのエンドポイントを選択します。
5. [属性名] をクリックして、マッピングできる属性のリストを表示します。
6. [キャンセル] をクリックします。

どの属性がマッピング可能かを確認することが目的なので、ここではポリシーの操作をキャンセルします。

重要: エンドポイントのネイティブ ツールだけで管理が可能な属性もあります。したがって、エンドポイントのユーザがこのタイプの属性を変更すると、逆同期ポリシーがトリガされたときに逆処理のイベントは失敗します。ただし、逆処理イベントでその他の属性に加えられた変更は逆処理されません。したがって、エンドポイントのみで管理可能な属性のマッピングは避けてください。

エンドポイント属性を逆同期用にマップする方法

1. [エンドポイント] - [エンドポイントの変更] をクリックします。
2. 逆同期が必要なエンドポイントを検索して選択します。
3. [属性マッピング] タブをクリックします。
4. [カスタム設定を使用] を選択します。
5. [追加] をクリックして、新しいカスタム属性を追加します。
6. 利用可能なカスタム属性を選択します。たとえば、CustomField 10 が環境で使用されていない場合、これを使用します。
7. カスタム属性を管理したいアカウント属性名にマッピングします。
8. ステップ 5 ~ 7 を繰り返し、すべての必要なアカウント属性と選択したカスタム属性の間にマッピングを追加します。

同じカスタム属性（例では CustomField 10）を、すべての管理したい属性に使用できます。

9. [サブミット] をクリックします。

このエンドポイントのベースラインの値を作成する方法

エンドポイントのすべての値をマッピングしたら、エンドポイントを検索します。この操作のために、インバウンド通知を無効にし、検索が完了したら有効にします。通知を無効にすることによって、不必要な通知が削除されます。無効にしないと、検索中に新しい属性の値を持つ各アカウントが通知を生成してしまいます。

1. プロビジョニング マネージャでは、次のようにインバウンド通知を無効化します。
 - a. [システム]-[Domain configuration]-[CA Identity Manager サーバ]-[Enable Notification] をクリックします。
 - b. [No] を選択します。
 - c. プロビジョニング サーバを再起動して、変更を有効にします。

2. ユーザ コンソールから [エンドポイント] - [検索および関連付けを実行] をクリックします。

関連付けが解除された検索および関連付け定義を選択します。

このアクションにより、ユーザ ストア属性に新しいエンドポイント属性データを投入します。エンドポイントが大きい場合、このタスクは時間がかかることがあります。

3. プロビジョニング マネージャでインバウンド通知を再有効化します。
4. プロビジョニング サーバを再起動します。

このエンドポイントの次の検索および関連付けの実行時に、アカウント変更通知が生成されます。通知が生成されるのは、グローバル ユーザ属性にマッピングされた属性に変更が発生し、その属性にポリシーが適用される場合です。

詳細情報:

[機能と初期属性](#) (P. 226)

逆同期のポリシー

エンドポイント上でアカウントが作成または変更されると、それに対して逆同期ポリシーは適切なアクションを起こします。たとえば、ユーザは企業ドメイン内の複数の OU でいくつかの **Active Directory** アカウントを作成します。また、ユーザは **Microsoft Exchange** アカウントもいくつか変更します。新規および変更されたアカウントを検出して、応答に逆同期アカウント ポリシーを使用して適切なアクションを提供できます。

逆同期を使用して、以下が可能です。

- ポリシーを設定して新規アカウントの承諾、拒否、またはワークフロー承認用に送信します。
- ポリシーを設定して属性への変更を承諾、元の属性に復元、またはワークフロー承認用に送信します。
- アカウントがワークフロー承認のために送信されると、承認者は以下のアクションのうちいずれかを実行します。
 - 拒否 (エンドポイントから削除/一時停止、または値を変更して **CA Identity Manager** ユーザ ストア値と一致させる)
 - 承諾し **CA Identity Manager** ユーザ ストアを更新し、アカウントに一致させる
 - ユーザ コンソールのユーザに割り当て (アカウント作成の場合)

新規アカウントのポリシー作成

新規アカウントがエンドポイント上で削除されたときのプロセスを定義したい場合、新規アカウントに適用されるアカウント ポリシーを作成します。新規アカウント ポリシーは、関連付けオプションが検索および関連付けの定義に含まれている場合にアカウントが検出されると実行されます。検索のみを実行時にアカウントが見つかった場合、次にそのエンドポイントの検索時に関連付けオプションが含まれていればポリシーが実行されます

新規アカウントのポリシー作成方法

1. ユーザ コンソールで、[エンドポイント] をクリックするか、または [タスク] - [エンドポイント] をクリックします。
2. [新規の逆同期]、[新規アカウント逆同期ポリシーの作成]。
3. ポリシーの名前および説明を入力します。
4. 以下のパラメータを入力します。
 - 優先度 — ポリシーの優先度。最高優先度のポリシーが、最小番号です。2つのポリシーの優先度およびスコープが同じ場合、どちらかのポリシーが実行されます。そのため、異なる優先度レベルが設定されていることを確認してください。
 - エンドポイントタイプ — すべてのエンドポイント、または特定のエンドポイントタイプ。
 - エンドポイント — 特定のエンドポイント名。エンドポイントタイプが「All」の場合、選択肢はすべてのエンドポイントのみです。
 - コンテナ — アカウントが存在するコンテナ。このフィールドは、階層エンドポイントのみに適用されます。コンテナを、エンドポイントで終わるノードのリストとして入力します。たとえば、パス「ou=child,ou=parent,ou=root,dc=domain,dc=name」の AD OU は、正しい形式は「child,parent,root」です。
 - 関連ユーザ — プロビジョニングディレクトリで関連付けされたユーザが見つかったかどうかに基づいて、ポリシーを実行するタイミングを制御します。

5. 以下のいずれかのアクションを選択します。
 - 承諾 — アカウント上でアクションを起こしません。この選択肢は、すべての新規アカウントを拒否するポリシーと、特定の OU のもとで作成されたアカウントを承認する、優先度の高いポリシーの 2 つのポリシーが存在する場合に役立ちます。そのため、アカウントがその OU で作成された場合は、承諾されます。拒否の優先度は、優先度が低いため実行されません。
 - 削除 — エンドポイントからアカウントを削除します。
 - 一時停止 — アカウントをエンドポイントに残したまま、一時停止にします。
 - 承認のため送信 — ワークフロー承認の変更をサブミットします。
6. [承認のため送信] にアクションを設定した場合、次のステップを実行します。
 - a. ワークフロー プロセスのとなりにあるアイコンをクリックします。
 - b. ワークフロー プロセスを選択します。
 - c. [OK] をクリックします。
7. [サブミット] をクリックします。

ワークフロー プロセスをポリシーに割り当てた場合、[承認タスクの作成](#) (P. 199) を行う必要があります。

変更されたアカウントのポリシー作成

エンドポイント アカウントのアカウント属性はいずれも、[属性マッピングで定義 \(P. 192\)](#)されている限り、逆同期で管理できます。

既存のエンドポイント アカウントと **CA Identity Manager** の既知の値の間に相違が見つかった場合のプロセスを定義するには、既存のアカウントに適用されるアカウント ポリシーを作成できます。属性が複数値の場合、複数の値が追加または削除された可能性があります。この場合、ポリシーを各値に別々に適用するか、異なる値用に別のポリシーを作成できます。

変更されたアカウントのポリシー作成方法

1. ユーザ コンソールで、[エンドポイント] をクリックするか、または [タスク] - [エンドポイント] をクリックします。
2. [変更の逆同期] - [変更済みアカウント逆同期ポリシーの作成]
3. ポリシーの名前および説明を入力します。
4. 以下のパラメータを入力します。
 - 優先度 — ポリシーの優先度。最高優先度のポリシーが、最小番号です。2つのポリシーの優先度およびスコープが同じ場合、どちらかのポリシーが実行されます。そのため、異なる優先度レベルが設定されていることを確認してください。
 - エンドポイント タイプ — すべてのエンドポイント、または特定のエンドポイント タイプ。
 - エンドポイント — 特定のエンドポイント名。エンドポイント タイプが「All」の場合、選択肢はすべてのエンドポイントのみです。
 - コンテナ — アカウントが存在するコンテナ。このフィールドは、階層エンドポイントのみに適用されます。コンテナを、エンドポイントで終わるノードのリストとして入力します。たとえば、パス「ou=child,ou=parent,ou=root,dc=domain,dc=name」の AD OU は、正しい形式は「child,parent,root」です。
 - 属性 — 物理名です。
 - 値 — 値の文字列表記であり、ワイルドカードとして*（アスタリスク）を含むことがあります。ワイルドカードは、変更のどの値も参照します。

5. 以下のいずれかのアクションを選択します。
 - 承諾 — CA Identity Manager ユーザストア内のアカウント値を更新し、エンドポイント アカウントの値を一致させます。
 - 拒否 — 属性を元に戻し、アカウント用の属性へのその他の変更に影響を与えずに元の値を回復させます。
 - 承認のため送信 — ワークフロー承認の変更をサブミットします。
6. [承認のため送信] にアクションを設定した場合、次のステップを実行します。
 - a. ワークフロー プロセスのとなりにあるアイコンをクリックします。
 - b. ワークフロー プロセスを選択します。
 - c. [OK] をクリックします。
7. [サブミット] をクリックします。

ワークフロー プロセスをポリシーに割り当てた場合、[承認タスクの作成](#) (P. 199) を行う必要があります。

逆同期用の承認タスクの作成

[Send to Workflow] アクションを持つポリシー用の逆処理の承認タスクを作成できます。タスクの作成には、以下のガイドラインを考慮します。

- 新規アカウントを承認するタスクには、2つの選択肢があります。
 - アカウントの汎用承認画面を作成します。タスクのプロファイル画面に、アカウントについての全般情報のみが表示されます。[逆の新規アカウントを承認] タスクは、この方法で作動します。
 - 承認者が新規アカウントの詳細を見る必要がある場合、画面はエンドポイント タイプに固有である必要があります。そのため、画面のある承認タスクは、そのエンドポイント タイプ固有のポリシーにのみ使用される必要があります。タスクには[逆処理の承認] タブが含まれる必要があります。
- アカウントの変更を承認するタスクでは、承認者が変更された値を見ることができるよう、承認画面はエンドポイント タイプ固有である必要があります。

逆処理の承認タスクは、アカウント変更に使用される承認タスクと同じです。特定のエンドポイント タイプの承認タスクがすでに存在する場合、そのタスクを使用できます。新規アカウントには、追加の逆処理の承認タブが必要です。エンドポイント タイプ用の既存の承認タスクが存在しない場合、以下の手順に従います。

逆同期用の承認タスクを作成する方法

1. ユーザ コンソールで、[タスク] - [ロールおよびタスク] または [ロールおよびタスク] をクリックします。
2. [管理タスク] - [管理タスクの作成] をクリックします。
3. エンドポイントの変更タスクを選択します。

名前が変更で終わり、エンドポイント タイプの名前を示します。例としては、[Active Directory アカウントの変更] などです。

4. [プロファイル] タブに、以下の変更を加えます。
 - 新しいタスクの名前を変更します。
 - タスク タグを変更します。
 - アクションを [イベントの承認] に変更します。
5. [タブ] タブに、以下の変更を加えます。
 - a. すべての [リレーションシップ] タブを削除します。
 - b. タスクが新規アカウントを承認する場合、[逆処理の承認] タブを追加します。このタブを移動させて、最初のタブにします。
 - c. 必要に応じて、タブの承認画面をコピーして編集します。

注: 承認タスクで一部のアカウント画面を使用すると、問題が発生する場合があります。その場合は、そのタブのデフォルトのアカウント画面をタスクで動作するように変更します。

6. [サブミット] をクリックします。
7. タスクが新規アカウント承認用の場合、タスクを承認者が属するロールに追加します。ロールはユーザ スコープを定義し、新規アカウントが割り当てられるユーザの検索に使用します。

逆同期の実行

逆同期は、[検索および関連付けを実行] タスクの使用時に発生します。このタスクの使用により、CA Identity Manager プロビジョニング ストアをエンドポイント上の新規または変更されたアカウントで更新します。

逆同期を実行する方法

1. 関連付けオプションを含む検索および関連付けの定義を作成します。関連付けは、新規アカウントの検出に必要です。
2. [タスク] - [エンドポイント] - [検索および関連付けを実行] をクリックします。
3. 新規または変更されたアカウントのあるエンドポイントに適用される定義を選択します。

注: 既存ユーザに関連付けする場合、ユーザがプロビジョニング ディレクトリ内に存在する必要があります。そうでないと、ユーザはそのディレクトリのデフォルトのユーザに関連付けられます。CA Identity Manager ユーザストアは、[検索および関連付け] タスクの範囲内にはありません。

4. [サブミット] をクリックします。

ポリシーにワークフロー プロセスがない場合、アカウントはすでにポリシーの定義に従って処理されています。

注: 逆同期ポリシーによって検出されたアカウント上で複数の属性が拒否された場合、すべてのアクションは1つのイベント内に配置されます。ただし、属性の問題が原因でそのイベントが失敗すると、属性は更新されません。

ワークフローがポリシーの一部である場合、逆同期により生成された承認はどれも、[ワークフロー] - 承認者用の [マイ ワーク リストの表示] のもとに表示されます。

新規アカウントでは、承認者には以下の選択肢があります。

- 承認者には、エンドポイントのアカウントの一時停止または削除のどちらかを行う選択肢があります。これには、[削除] または [一時停止] を選択してから [拒否] をクリックします。
- もしくは、承認者は [承諾] をクリックして新規アカウントを承諾します。

承認者が [関連ユーザ] フィールドのユーザを選択しない場合、アカウントはデフォルトのユーザに割り当てられます。[関連ユーザ] フィールドが承認タスク内に投入された場合、アカウントはこのユーザと関連付けられます。ユーザを見つけることができる場合、[関連ユーザ] フィールドには関連付けのメカニズムにより見つかった提示されたユーザが含まれます。

変更されたアカウントでは、承認者には以下の選択肢があります。

- 各アカウント用に、承認者はどの値が変更され、承認または拒否できるかを、変更がアカウント管理画面で開始されたかのように見ることができます。
- 承認者は機能属性（Active Directory グループなど）への変更を別々の承認イベントとして見ることができます。

逆同期が成功したかどうかを確認する方法

1. [システム] - [サブミット済みタスクの表示] を選択します。
2. 次のとおりにタスク名を完了させます: プロビジョニング アクティビティ
3. [検索] をクリックします。

逆同期イベントの完了が成功すると、結果が表示されます。

エンドポイントのカスタム属性の拡張

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

エンドポイントのカスタム属性を拡張する方法

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

「*Connector Programming Guide*」を参照してください。

2. 以下の手順で、Connector Xpress を使用します。
 - a. 名前空間ノードで、メタデータをインストールします。
 - b. ロール定義ジェネレータを使用して、JAR ファイル、プロパティ ファイル、およびロール定義ファイルを生成します。

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

3. JAR ファイルを次の場所にコピーします。
 - (Windows) *app server home/iam_im.ear/user_console.war/WEB-INF/lib*
 - (UNIX) *app server home¥iam_im.ear¥user_console.war¥WEB-INF¥lib*

注: WebSphere の場合、JAR ファイルを次の場所にコピーします。
WebSphere_home/AppServer/profiles/Profile_Name/config/cells/Cell_name/applications/iam_im.ear/user_console.war/WEB-INF
4. プロパティ ファイルを次の場所にコピーします。
 - (Windows) *app server home/iam_im.ear/custom/provisioning/resourceBundles*
 - (UNIX) *app server home¥iam_im.ear¥custom¥provisioning¥resourceBundles*

注: WebSphere の場合は、次の場所にプロパティ ファイルをコピーします。
WebSphere_home/AppServer/profiles/Profile_Name/config/cells/cell_name/applications/iam_im.ear¥custom¥provisioning¥resourceBundles
5. クラスタがある場合は、ノードごとに上記 2 つの手順を繰り返します。
6. アプリケーションサーバを再起動します。
7. 以下の手順で、ロール定義ファイルをインポートします。
 - a. 管理コンソールで、[環境] を選択します。
 - b. ロールおよびタスクの設定を選択します。
 - c. [インポート] をクリックします。
 - d. エンドポイント タイプを選択し、[完了] をクリックします。

アカウント タスク

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

エンドポイント アカウントには、以下の 4 つのタイプがあります。

プロビジョニング済み

ユーザにプロビジョニング ロールが割り当てられたときに作成されるアカウント

例外

ユーザにアカウント テンプレートが割り当てられたときに作成されるアカウント

孤立

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

システム

エンドポイント システムに作成され、CA Identity Manager ユーザに関連付けられておらず、エンドポイント システムの管理に使用されるアカウント

エンドポイント アカウントの表示または変更

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

アカウント 詳細
今すぐアクションを実行するアカウント名をクリックします。

選択	名前	エンドポイント タイプ	エンドポイント	一時停止	ロック済み
☒	 ken	Windows NT	iam-fw-wl10		

アカウントの作成

選択したアカウントに対するアクション

アカウントのリフレッシュ

一時停止

再開

ロック解除

パスワードの変更

割り当て解除

割り当て

削除

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

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

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

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

プロビジョニング済みアカウントの作成

CA Identity Manager ユーザのエンドポイント アカウントを作成するには、プロビジョニング ロールをユーザに割り当てる方法をお勧めします。ユーザには、そのロールのアカウント テンプレートで定義された属性を持つアカウントが割り当てられます。Exchange アカウントのメールボックスのサイズなど、必要に応じてそのアカウント テンプレートに変更を加えると、エンドポイント アカウントが更新されます。

プロビジョニング済みアカウントを作成する方法

1. ユーザ コンソールで、[ユーザの管理] - [ユーザの変更] を選択します。
2. 変更するユーザを選択します。
3. [プロビジョニング ロール] タブをクリックします。
4. [プロビジョニング ロールの追加] をクリックします。
5. ロールを選択します。
6. [サブミット] をクリックします。

例外アカウントの作成

ユーザに対して [ユーザの変更] を使用すると、[アカウント] タブで直接アカウントを作成できます。このアカウントは、「例外アカウント」と呼ばれています。ただし、このアカウントにはプロビジョニング ロールが関連付けられていないので、ロールとユーザの同期を行ってもこのアカウントは更新されません。

アカウント テンプレートを作成する方法

1. ユーザ コンソールで、[ユーザ] - [ユーザのエンドポイント アカウントの変更] を選択します。
2. 変更するユーザを選択します。
3. [作成] をクリックします。
4. エンドポイントを選択します。
5. このエンドポイント タイプにコンテナが必要な場合は、コンテナを選択します。
6. 各タブのフィールドを入力します。
7. [サブミット] をクリックします。

孤立アカウントの割り当て

ユーザ コンソールでは、孤立アカウントを管理できます。このアカウントは CA Identity Manager ユーザに関連付けられていないアカウントです。

孤立アカウントのデフォルト ユーザを作成する方法

プロビジョニング ディレクトリが CA Identity Manager ユーザ ストアとは別になっている場合、CA Identity Manager ユーザ ストアでプロビジョニング サーバのデフォルト ユーザを作成します。デフォルト ユーザは、孤立アカウントに使用されます。

1. ユーザ コンソールで、[ユーザ] をクリックします。
2. [ユーザの管理] - [ユーザの作成] をクリックします。
3. 以下のように、かっこで囲んでユーザの名前を付けます。
[デフォルト ユーザ]

これで、孤立アカウントをユーザに割り当てることができます。

孤立アカウントを割り当てる方法

1. ユーザ コンソールで、[エンドポイント] をクリックします。
2. [孤立アカウントの管理] をクリックします。
3. ユーザを検索して選択します。
4. 孤立ユーザに割り当てるユーザをクリックします。

システム アカウントの割り当て

ユーザ コンソールでは、システム アカウントを管理できます。このアカウントはエンドポイント アカウントで、エンドポイント システムの管理に使用されます。

システム アカウントをユーザに割り当てるには、[システム アカウントの管理] タスクに基づいて管理タスクを作成します。新規タスクには、特定のエンドポイントに適用される固有の **CA Identity Manager** ユーザが存在します。エンドポイントのタイプごとにタスクを 1 つ作成することもできます。

タスクを設定して、システム アカウントを割り当てる方法

1. ユーザ コンソールで、[ロールおよびタスク] - [管理タスク] - [管理タスクの作成] をクリックします。
2. [システム アカウントの管理] に基づいて新規タスクを作成します。
たとえば、「**Oracle** システム アカウントの管理」という名前のタスクを作成して、**Oracle** エンドポイント タイプのシステム アカウントを割り当てることができます。
3. [検索] タブで [参照] ボタンをクリックして、検索画面を編集します。その検索画面で、ユーザの検索フィルタを追加して、このシステム アカウントに割り当てます。
4. タスクをサブミットします。
5. このタスクをロールに追加します。
6. ユーザにエンドポイントのシステム アカウントを割り当てる必要があるユーザに対してロールを割り当てます。

このロールが設定されたユーザは新規タスクを実行して、システム ユーザを **CA Identity Manager** ユーザに割り当てることができます。

アカウントの移動タスク画面

このタスク画面を使用して、エンドポイント上のアカウントをコンテナから別のコンテナに移動させます。この画面のフィールドを以下に示します。

アカウント移動の詳細

移動させたいアカウント、親コンテナ、宛先コンテナ、エンドポイント、およびエンドポイント タイプを指定します。

[コンテナの選択]ボタン

クリックしてエンドポイントに属する利用可能なアカウント コンテナを検索します。

エンドポイント アカウントの削除

以下の 2 つの方法で、エンドポイント アカウントを削除できます。

1. [ユーザの変更] タスクを使用し、[プロビジョニング ロール] タブで、そのアカウントを作成したロールを削除する。
2. [ユーザのエンドポイント アカウントの変更] タスクを使用して、アカウントを削除する。

[ユーザのエンドポイント アカウントの変更]でアカウントを削除する方法

1. ユーザ コンソールで、[ユーザ] - [ユーザのエンドポイント アカウントの変更] を選択します。
2. 変更するユーザを選択します。
3. エンドポイント タイプに基づいてアカウントを検索します。
4. アカウントを選択します。
5. [削除] ボタンをクリックします。

削除したアカウントは、以下のようにプロビジョニング マネージャを使用すると、再作成されます。

- [ユーザとロールの同期] では、プロビジョニング済みアカウント（ユーザにプロビジョニング ロールが割り当てられたときに作成されたアカウント）が再作成されます。
- [アカウントとアカウント テンプレートの同期] では、例外（アカウントにアカウント テンプレートがある場合）とプロビジョニング済みアカウントが再作成されます。

エンドポイント アカウントのパスワード変更

現在のパスワードを知らなくてもエンドポイント アカウントのパスワードを変更できます。

エンドポイント アカウントのパスワードを変更する方法

1. ユーザ コンソールで、[ユーザ] - [ユーザのエンドポイント アカウントの変更] を選択します。
2. 変更するユーザを選択します。
3. エンドポイント タイプに基づいてアカウントを検索します。
4. アカウントを 1 つ以上選択します。
5. [パスワードの変更] ボタンをクリックします。
6. 新しいパスワードを入力します。

CA Identity Manager パスワード ポリシーによって新しいパスワードが検証されます。

7. [サブミット] をクリックします。

複数のアカウントに対するアクションの実行

1 つまたは複数のアカウントに対してその他のアクションを複数実行できます。たとえば、ユーザが間違ったパスワードを入力した場合やユーザにアカウントを割り当てたり、割り当て解除したりする場合、一時停止されていたアカウントを再開してアカウントのロックを解除することができます。これらのアクションは選択されたすべてのアカウントに適用され、手順は同じです。

複数のアカウントに対してタスクを実行する方法

1. ユーザ コンソールで、[ユーザ] - [ユーザのエンドポイント アカウントの変更] を選択します。
2. 変更するユーザを選択します。
3. エンドポイント タイプに基づいてアカウントを検索します。
4. アカウントを 1 つ以上選択します。
5. [選択したアカウントに対するアクション] で、任意のボタンをクリックします。
6. 表示されるダイアログ ボックスに応答して、[送信] を送信します。

詳細なアカウント操作

プロビジョニング マネージャで、アカウントについて、次のような詳細な操作を実行することができます。

- アカウントを別のグローバル ユーザに関連付ける
- アカウントを自動検索する
- アカウントを削除する
- 削除を保留中を使用する
- 削除したアカウントを再作成する

アカウントに対するグローバル ユーザの変更

次のような場合には、アカウントを他のグローバル ユーザに関連付けたいと考えます。

- 同じ名前の 2 つのグローバル ユーザを持っており、CA Identity Manager がアカウントを間違った個人に関連付けている
- CA Identity Manager が、あるアカウントを [default user] オブジェクトに関連付けているが、自分ではこのアカウントを別のグローバル ユーザ オブジェクトに関連付けたい
- [New] を使用してアカウントを作成したが、次にそれをグローバル ユーザに関連付けたい

プロビジョニング マネージャで、アカウントを別のグローバル ユーザに関連付けるには、アカウントを、該当するグローバル ユーザへドラッグ アンド ドロップします。

自動検索が機能するしくみ

エンドポイントに対してネイティブなツールを使用して、アカウントまたは他のオブジェクトを追加または削除しても、エンドポイントを検索するまで **CA Identity Manager** には認識されません。検索のプロセスでは、行われた追加および削除（および場合によっては変更）を認識し、それらの変更を、プロビジョニングディレクトリにおけるオブジェクトの **CA Identity Manager** の表記に適用します。

ただし、この検索を行う前に、プロビジョニング マネージャを使用して、同じ名前を持つオブジェクトを作成しようとするすると、**CA Identity Manager** は、この名前のオブジェクトがすでに存在していることに気が付き、このエラーをレポートします。次に **CA Identity Manager** はこのオブジェクトを検索し、プロビジョニングディレクトリ内で、このオブジェクトの表記を作成します。このオブジェクトをすぐに使用することができます。オブジェクトがプロビジョニングディレクトリ内に存在していないくて、追加、移動、または名前変更の処理によって、エンドポイントにおいて「すでに存在している」エラーが生成された場合には必ず、1 オブジェクトの自動検索が行われます。

自動検索は、「*Provisioning Reference Guide*」に記載されている、**Synchronization/Automatic Correlation** ドメイン設定パラメータと組み合わせることができます。これらの機能を組み合わせて有効にすると、最初にアカウント テンプレートから、新しいアカウントを作成するための試行として、アカウントを作成しようとします。次に、以下の手順が行われます。

- 検索されていないアカウントに気が付く
- そのアカウントを自動的に検索する
- そのアカウントを、グローバル ユーザに自動的に関連付ける
- このグローバル ユーザに相互に関連付けられている既存のアカウントのよう
に、アカウントに対してアカウント テンプレートを追加する

アカウントを削除する

アカウントを削除しなければならない場合は、プロビジョニング マネージャで、次のいずれかの方法を使用します。

- アカウントを右クリックして [削除] を選択する
- グローバル ユーザを右クリックし、[Delete User and Accounts] を選択する
- アカウントの削除ウィザードを実行する
- グローバル ユーザとプロビジョニング ロールを同期させ、余分なアカウントを削除するよう指定する

プロビジョニング ロールからグローバル ユーザを削除する場合は、プロビジョニング マネージャによって、アカウントを削除するために次のオプションが提示されます。

- これらのアカウントを削除することが決まっている場合は、**CA Identity Manager** により、プロビジョニング ディレクトリからアカウントが削除されます。
- アカウントを削除することが決まっていない場合は、[ユーザとロールの同期] オプションを使用して、[アカウントの削除] を選択することができます。

アカウントを削除する前に、プロビジョニング ロールからグローバル ユーザを削除する場合は、そのグローバル ユーザに対するアカウントをリストすることができます。グローバル ユーザを右クリックして、[List Accounts] を選択します。

- アカウントのリストには、各アカウントが属しているプロビジョニング ロールが表示されます。あるアカウントがプロビジョニング ロールに属している場合、そのロールからユーザを削除し、ユーザの同期アクションを承認してアカウントを削除することによって削除されます。
- あるアカウントがプロビジョニング ロールに属していない場合は、それは余分なアカウントになり、ユーザの同期チェックでレポートされます。グローバル ユーザで [ユーザとロールの同期] メニュー項目を選択すると、アカウントが削除されます。

削除を保留中を使用する

CA Identity Manager では、通常はアカウントが削除されるような削除または同期のアクションを管理者が開始したときに、エンドポイントのアカウントが削除されないよう、エンドポイントごとの設定が可能です。代わりに、アカウントはユーザ コンソールで「削除を保留中」の状態になり、管理エンドポイントでは「一時停止」の状態になります。CA Identity Manager はまた、一時停止されたアカウントからアカウント テンプレートをすべて削除し、一時停止されたアカウント上の多値属性もクリアします。

削除を保留中のアカウントは、プロビジョニング マネージャでは、アカウント プロパティの [統計] タブで確認できます。一時停止のアカウントには、「削除を保留中」の一時停止理由があり、この状態になったときのタイムスタンプもあります。「削除を保留中」のステータスおよび「一時停止」のタイムスタンプを格納すると、これらの「削除を保留中」のアカウントを特定し、プロビジョニング サーバおよび管理エンドポイントから後で削除するユーティリティを記述することができます。

削除されたアカウントの再作成

CA Identity Manager 以外のツールを使用して、管理エンドポイントでアカウントを削除すると、アカウントの同期チェック機能で、そのアカウントが不明としてレポートされます。これは、対象のアカウントがプロビジョニング ディレクトリに存在しているのに、管理エンドポイントに存在していないためです。このような場合には、**Synchronize Account with Account Templates** 関数を発行して、そのエンドポイントでアカウントを再作成します。この関数は、そのアカウントに関連付けられているアカウント テンプレートを使用して、アカウントを再作成します。

アカウントが再作成されると、CA Identity Manager は、アカウントが再作成されたものとして記録します。これらのアカウントは、更新されたアカウントとは別のものと認識することができます。これは、管理者が、機能属性以外の属性（パスワードなど）が、最初のアカウントテンプレートの値にずっと設定されていることを認識している必要があるためです。

第 9 章: プロビジョニング ロール

このセクションには、以下のトピックが含まれています。

[プロビジョニング ロールとアカウント テンプレート](#) (P. 215)

[アカウント割り当て用のロールの作成](#) (P. 216)

[ロールおよびテンプレート タスク](#) (P. 220)

[アカウント テンプレートの属性](#) (P. 225)

[詳細なルール式](#) (P. 229)

[プロビジョニング ロールのパフォーマンス](#) (P. 236)

[既存環境用のプロビジョニング タスク](#) (P. 238)

プロビジョニング ロールとアカウント テンプレート

アカウント管理を単純にするために、アカウントの作成と保守にアカウント テンプレートを使用します。アカウント テンプレートは、プロビジョニング ロールで使用されます。プロビジョニング ロールには、1 つ以上のアカウント テンプレートが含まれます。プロビジョニング ロールをユーザに適用すると、ユーザは、アカウント テンプレートで定義されたアカウントを受け取ります。

アカウント テンプレートには、特定のエンドポイント タイプのアカウントの基本設定が収められています。アカウント テンプレートは、eTrust Admin のプロビジョニング ポリシー と同様の機能を実現します。

アカウント テンプレートを使用すると、次のことが実行できます。

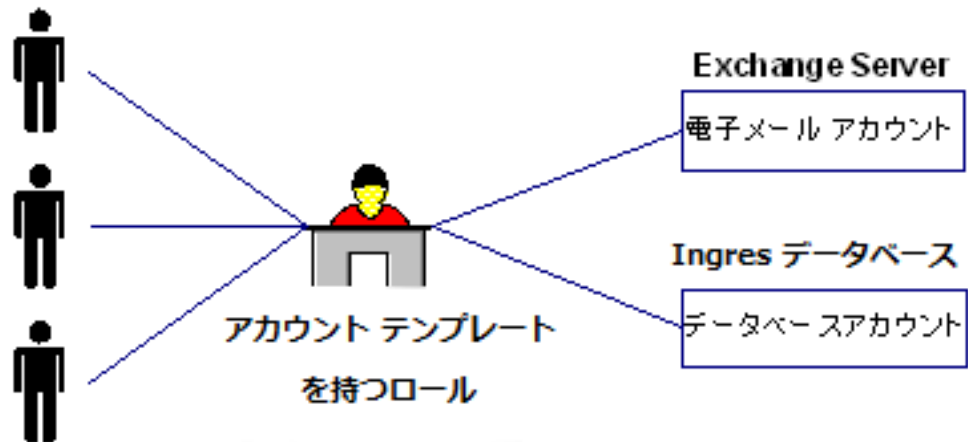
- アカウントの作成時に、エンドポイントで CA Identity Manager ユーザが持つアカウント属性を制御する
- ルールの文字列や値を使用して属性を定義する
- 異なるプロビジョニング ロールのアカウント属性を組み合わせる（これにより、ユーザは特定のエンドポイントで 1 つのアカウントしか持たずに必要なアカウント属性をすべて持つことができる）
- グローバル ユーザがプロビジョニング ロールを変更するのに応じてアカウント属性を作成または変更する

アカウント割り当て用のロールの作成

ほとんどの組織で、管理者は、さまざまなシステムおよびアプリケーション用のログインアカウントをユーザに提供するために多大な時間を費やします。この反復作業を簡略化するために、プロビジョニングロールを作成することができます。これは、アカウントテンプレートを含むロールです。このテンプレートでは、1つのタイプのアカウントに存在する属性を定義します。たとえば、Exchange アカウント用のアカウントテンプレートは、メールボックスのサイズなど属性を定義します。のアカウントテンプレートでは、ユーザ属性とアカウントのマッピング方法も定義できます。

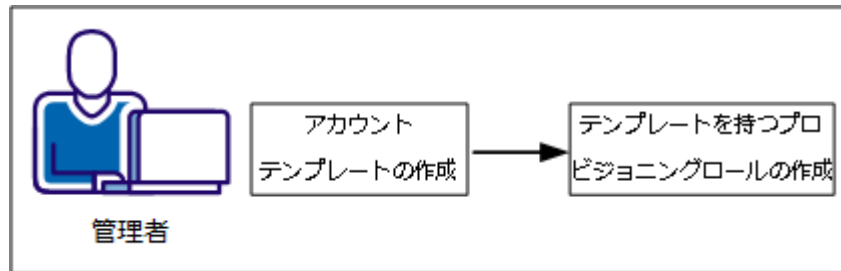
例として、Forward 社という会社で、すべての従業員がデータベースと電子メールへのアクセスを必要とする場合を考慮します。管理者は、各従業員のデータベースアカウントと電子メールアカウントを1つずつ作成することを避けたいと考えています。そこで管理者は、この会社のプロビジョニングロールを作成します。このロールには、電子メールアカウントを提供するための Microsoft Exchange Server 用アカウントテンプレートと、Oracle データベース用のテンプレートが含まれます。この例では、Exchange Server と Oracle のデータベースはエンドポイントと呼ばれます。これらは、アカウントが存在するシステムまたはアプリケーションです。

注: Forward 社とは架空の会社名であり、厳密に説明のみを目的として使用されています。現存する会社を参照するものではありません。



ロールが作成された後、管理者またはサポート担当者などの業務系管理者はこれらのロールをユーザに割り当て、エンドポイント内のアカウントを付与することができます。ユーザは、ロールを受信した後、エンドポイントにログインできます。

アカウントテンプレートを含むプロビジョニングロールの作成は、以下のような2段階のプロセスです。



以下のセクションでは、アカウントの割り当てに使用できるロールを作成する方法について説明します。

1. [アカウントテンプレートの作成](#) (P. 218)
2. [プロビジョニングロールの作成](#) (P. 219)

アカウント テンプレートの作成

アカウント管理を単純にするために、アカウントの作成と保守にアカウント テンプレートを使用します。アカウント テンプレートは、プロビジョニング ロールで使用されます。プロビジョニング ロールには、1 つ以上のアカウント テンプレートが含まれます。プロビジョニング ロールをユーザに適用すると、ユーザは、アカウント テンプレートで定義されたアカウントを受け取ります。

アカウント テンプレートには、特定のエンドポイント タイプのアカウントの基本設定が収められています。

アカウント テンプレートを使用すると、次のことが実行できます。

- アカウントの作成時に、エンドポイントでユーザが持つアカウント属性を制御する
- ルールの文字列や値を使用して属性を定義する
- 異なるプロビジョニング ロールのアカウント属性を組み合わせる（これにより、ユーザは特定のエンドポイントで1つのアカウントしか持たずに必要なアカウント属性をすべて持つことができる）
- グローバル ユーザがプロビジョニング ロールを変更するのに応じてアカウント属性を作成または変更する

各エンドポイント タイプのデフォルトのアカウント テンプレートは、CA Identity Manager サーバにインストールされています。プロビジョニング ロールでは、デフォルトのアカウント テンプレートを使用するか、または設定した任意のエンドポイント用に独自のアカウント テンプレートを作成することができます。

アカウント テンプレートを作成する方法

1. [タスク] にリスト表示される [エンドポイント] に移動し、[アカウント テンプレート] - [アカウント テンプレートの作成] をクリックします。
2. そのテンプレートのエンドポイント タイプを選択します。
3. [エンドポイント名] をエンドポイントのシステム名、または該当する場合はローカルホストとして定義します。
4. [エンドポイント] タブで使用するエンドポイントを選択します。
5. タブのフィールドに入力するか、デフォルトの値を使用します。
各エンドポイント タイプには、異なるタブ セットが使用されています。
フィールドの定義については、[ヘルプ] をクリックしてください。
6. [サブミット] をクリックします。

注: アカウントテンプレート内のエンドポイント オブジェクトを検索するとき、複数のエンドポイントが指定された場合、関連するオブジェクトの共通のサブセット（両方に含まれる）が返されます。たとえば、アカウントテンプレートに関連付けられている選択されたエンドポイントのそれぞれに存在する **Active Directory** グループなどです。検索結果にオブジェクト名以外の属性が表示される場合、最初のエンドポイントに関連付けられているオブジェクトの属性値が表示されます。たとえば、**PeopleSoft** コネクタ内の言語オブジェクトに対する説明属性などです。

プロビジョニング ロールの作成

プロビジョニング ロールを作成するには、以下のロール要件を決定する必要があります。

- 別のアカウントを必要としているのはどのユーザか
- どのアカウントをロールに関連付けるか
- ロールのメンバ、管理者、および所有者となるのは誰か

プロビジョニング ロールを作成する方法

1. ユーザ コンソールで、[ロールおよびタスク] - [プロビジョニング ロール] - [プロビジョニング ロールの作成] をクリックします。

各タブの詳細については、画面のヘルプのリンクをクリックしてください。

2. [プロファイル] タブを設定します。必須となるのは [名前] フィールドのみです。

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

3. [アカウントテンプレート] タブを設定します。
 - a. **ActiveDirectory** などの [エンドポイント タイプ] をクリックします。
 - b. アカウントテンプレートをクリックします。

[エンドポイント タイプ] によってクリックできるテンプレートが決まります。
 - c. 必要に応じて異なるエンドポイント タイプのアカウントテンプレートを追加します。
4. このタブ内でプロビジョニング ロールをネストする場合は、[プロビジョニング ロール] タブを設定します。

この手順を行うには、この環境で [ネストされたロール](#) (P. 224) が有効になっている必要があります。

5. 管理ルールを設定して、このロールのメンバおよび管理者に対する管理者を設定します。[管理者] タブの入力は完了です。
6. 誰がこのロールを変更できるかを制御する所有者ルールを追加して、[所有者] タブを設定します。
7. [サブミット] をクリックします。
8. ロールが作成されたことを確認するには、[プロビジョニング ロール] - [プロビジョニング ロールの表示] をクリックします。

ロールおよびテンプレート タスク

ユーザ コンソールで [ロールおよびタスク] を選択し、[プロビジョニング ロール] の下のタスクを選択して、プロビジョニング ロールを作成し管理することができます。タスクは、ロールのメンバーであるユーザの作成、およびロールの変更や削除といった標準的な操作のために存在します。

プロビジョニング ロールを作成する前に、そのロールがインポートするプロビジョニング ロールにアカウント テンプレートが含まれるようにする必要があります。インポートできるロールは、プロビジョニング マネージャか eTrust Admin で作成されたロールです。ただし、CA Identity Manager では、eTrust Admin で作成されたネストされたロールはサポートされません。

プロビジョニング ロールのインポート

プロビジョニング ロールはユーザ コンソールで管理しますが、プロビジョニング ロールによってプロビジョニング マネージャまたは外部アプリケーションで作成されたものもあります。このようなプロビジョニング ロールの場合、ユーザ コンソールで管理できるようにロール所有者を「CA Identity Manager 管理者」にリセットすることができます。

プロビジョニング ロールをインポートする方法

1. システム マネージャ ロールを持つユーザとしてユーザ コンソールにログインします。[タスク] - [ロールおよびタスク] をクリックします。
2. [プロビジョニング ロール] - [プロビジョニング ロール所有者のリセット] をクリックし、プロビジョニング マネージャで作成されたプロビジョニング ロールを選択します。
3. 誰がこのロールを変更できるかを制御する所有者ルールを追加して、[所有者] タブを設定します。

4. [サブミット] をクリックします。

これで、プロビジョニング ロール カテゴリのタスクを使用してロールの変更、割り当て、表示が可能になります。

プロビジョニング ロールへの新規所有者の割り当て

複数のプロビジョニング ロールを選択して、それらのロールを誰が変更できるかを制御する所有者ポリシーを割り当てることができます。

プロビジョニング ロールに新規所有者を割り当てる方法

1. システム マネージャ ロールを持つユーザとしてユーザ コンソールにログインします。
2. [タスク] - [ロール] をクリックするか、[ロール] - [タスク] をクリックします。
3. [プロビジョニング ロール] - [プロビジョニング ロールに割り当てる所有者ポリシーを作成] をクリックします。
4. プロビジョニング ロールを 1 つ以上選択します。
5. 誰がこのロールを変更できるかを制御する所有者ルールを追加して、[所有者] タブを設定します。
6. [サブミット] をクリックします。

新規所有者ポリシーを満たすユーザは、選択したプロビジョニング ロールを変更することができます。

プロビジョニング ロールによって作成されたアカウントのパスワード

ユーザがプロビジョニング ロールに割り当てられると、CA Identity Manager ユーザのパスワードがエンドポイントのパスワード要件を満たさない場合、そのユーザのアカウント作成は失敗します。一時パスワードを持つ新規ユーザの作成の場合も同様です。

したがって、照合するパスワードポリシーをエンドポイントパスワードポリシー要件と同等以上に厳しいものに設定します。CA Identity Manager パスワードポリシーまたはプロビジョニング パスワードプロファイルの使用により、パスワードポリシーを設定できます。両方のメソッドが使用される場合、ポリシーは一致する必要があります。

プロビジョニング ロール イベントの処理順序

デフォルトの **CA Identity Manager** タスクの中には、プロビジョニング ロール メンバシップを決定するイベント（タスクを完了するために **CA Identity Manager** が実行するアクション）があります。たとえば、デフォルトの [ユーザの変更] タスクには、**AssignProvisioningRoleEvent** および **RevokeProvisioningRoleEvent** が含まれます。プロビジョニング ロールの割り当てまたは取り消しにより、エンドポイントでアカウントを追加または削除できます。場合によっては、エンドポイントで、すべての [追加] アクションを [削除] アクションの前に行うことを要求されることがあります。

CA Identity Manager によって [追加] アクションが最初に処理されるようにするには、管理コンソールでプロビジョニング ロール メンバシップ イベントの累積の設定を有効にします。この設定が有効になると、**CA Identity Manager** により、すべての [追加] および [削除] アクションを **AccumulatedProvisioningRolesEvent** と呼ばれる単一のイベントに累積します。たとえば、[ユーザの変更] タスクにより、1 人のユーザに 3 つのプロビジョニング ロールが割り当てられ、そのユーザから 2 つの他のプロビジョニング ロールが削除される場合、3 つの [追加] アクションと 2 つの [削除] アクションを含む **AccumulatedProvisioningRolesEvent** が生成されます。

このイベントを実行すると、すべての [追加] アクションは、単一の操作に統合され、プロビジョニング サーバに送信され、処理されます。[追加] アクションの処理が完了すると、**CA Identity Manager** により、[削除] アクションが単一の操作に統合され、その操作がプロビジョニング サーバに送信されます。

この設定を有効にすると、以下の CA Identity Manager 機能に影響を及ぼします。

- ユーザ タスクの [プロビジョニング ロール] タブ

管理者が、[プロビジョニング ロール] タブを使用して、プロビジョニング ロールからユーザを追加または削除すると、CA Identity Manager によりこれらのアクションは単一のイベントに累積されます。

- アイデンティティ ポリシー

アイデンティティ ポリシーの評価の結果、生成されるすべてのプロビジョニング ロール メンバシップ イベント (AssignProvisioningRoleEvent または RevokeProvisioningRoleEvent) は、単一の AccumulatedProvisioningRolesEvent に累積されます。CA Identity Manager では、このイベントは他のセカンダリ イベントと同様に実行されます。たとえば、2 つのアイデンティティ ポリシーを含むアイデンティティ ポリシー セットがあると考えてみてください。

Policy A は、プロビジョニング ロール A でメンバシップを削除し、Policy B は、プロビジョニング ロール B でユーザ メンバを作成します。CA Identity Manager により、あるユーザが Policy A は満たさなくなったが Policy B は満たすと判断されれば、2 つのアクション ([削除] アクション 1 つと [追加] アクション 1 つ) を含む AccumulatedProvisioningRolesEvent が生成されます。まず、[追加] アクションが実行され、次に [削除] アクションが実行されます。

- サブミット済みタスクの表示

AccumulatedProvisioningRolesEvent のステータスおよび個々のアクションのステータスを確認するには、[サブミット済みタスクの表示] タスクを使用して、イベントの詳細を表示します。

個々のアクションのいずれかが失敗すると、イベントのステータスは失敗となり、そのタスクは失敗状態に移行します。

- ワークフロー

ワークフロー プロセスを、AccumulatedProvisioningRolesEvent に関連付けできます。この場合、承認者は、そのイベント全体を承認または拒否できます。これにより、個々の各イベントも承認または拒否されることになります。

AccumulatedProvisioningRolesEvent 内で個々のイベントのワークフローを有効にするには、追加設定 が必要となります。

- 監査

CA Identity Manager では、AccumulatedProvisioningRolesEvent および個々の各イベントに関する情報の監査が行われます。

プロビジョニング ロール メンバシップ イベント 累積の有効化

CA Identity Manager では、管理コンソールで設定を行うことができ、プロビジョニング ロール メンバシップ イベントのすべての [追加] および [削除] アクションを単一の操作に統合できます。アクションが統合されると、CA Identity Manager により、[削除] アクションの処理の前に、[追加] アクションが単一の操作として処理されます。

これにより、一部のエンドポイント タイプで要求されるイベントの順序付けが可能になります。

注: この機能は、デフォルトで無効になっています。

プロビジョニング ロール メンバシップ イベントの累積を有効にする方法

1. CA Identity Manager 管理コンソールのアクセス
2. [環境] をクリックします。
3. 設定する環境を選択します。
4. [詳細設定] の [プロビジョニング] を開きます。
5. [Enable Accumulation of Provisioning Role Membership Events] チェック ボックスをオンにします。
6. アプリケーション サーバを再起動します。

環境での[ネストされたロール]の有効化

プロビジョニング ロールを、別のプロビジョニング ロール内に含めることができます。含めたロールは、入れ子のロールと呼ばれます。

たとえば、従業員プロビジョニング ロールを作成したとします。この従業員ロールで、電子メール アカウントなど、すべての従業員が必要とするアカウントが提供されます。この従業員ロールを、部署に固有のプロビジョニング ロール (財務ロールや営業ロールなど) に含めます。部署ごとのプロビジョニング ロールでは、その部署にのみ関連するアカウントが提供されます。このようにロールを組み合わせることで、各ユーザに適切なアカウントが提供されます。

環境で[ネストされたロール]を有効にする方法

1. 管理コンソールで、[環境] を選択します。
2. [ロールおよびタスクの設定] - [インポート] をクリックします。
3. [ネストされたプロビジョニング ロールのサポート] を選択します。

4. [完了] をクリックします。
5. 環境を再起動します。

プロビジョニング ロール内へのロールの追加

プロビジョニング ロールにロールを含める方法

1. [ロールおよびタスク]-[プロビジョニング ロール]-[プロビジョニング ロールの変更] に移動します。
2. [ロールの追加] をクリックして、[プロビジョニング ロール] タブを設定し、プロビジョニング ロールを選択します。

パフォーマンス上の理由から、ロールのネストは、3 レベルまでに制限することをお勧めします。たとえば、現在のプロビジョニング ロール（第 1 レベルのロール）に別のロール（第 2 レベルのロール）を含めるとします。このロールに含まれるロールは第 3 レベルのロールとなります。ロールを含んでいるロールが第 3 レベルのロールにならないようにすることをお勧めします。

3. 所有者ルールを変更して所有者ポリシーを設定します。
スコープは、追加したロールと同等にするか、より広くする必要があります。
4. [サブミット] をクリックします。

アカウント テンプレートの属性

アカウント テンプレートの属性を使用して、アカウントの属性の定義方法を決定できます。

機能と初期属性

アカウントテンプレートには、2種類の属性が収められます。

- **機能属性**は、ディスク領域のサイズ、数量、頻度制限、グループメンバシップなどのアカウント情報を表します。プロビジョニングマネージャでは、機能属性は、簡単に見分けられるようにすべてのアカウントテンプレート画面で太字で表示されます。
- **初期属性**は、アカウント名、パスワード、アカウントステータス、個人情報（名前、住所、電話番号など）などアカウントに初期設定される情報すべてを表します。

アカウントは、機能属性すべてが同期されたときに、アカウントテンプレートと同期されたとみなされます。機能属性は、グループメンバシップ、権限、クォータ、ログイン制限などユーザがアカウントへのログイン中に何ができるかを制御する属性であり、エンドポイントタイプごとに異なります。

同期によって他のアカウントの属性が更新されることはありません。他のアカウントの属性は、アカウント作成中にアカウントテンプレートから初期化されます。また、継承の実行時に更新される場合もあります。プロビジョニングサーバには、2つの伝達機能（アカウントテンプレート変更時のアカウントの即時更新とグローバルユーザ属性の変更時のアカウント更新）が用意されています。

機能属性と初期属性の検出

どの属性が機能属性として定義され、どれが初期属性として定義されるかを検出するためには、**eTACapability.txt** ファイルを生成する必要があります。Windows コマンドプロンプトから、以下のコマンドを入力します。

```
PS_HOME¥dumpptt.exe -c > eTACapability.txt
```

```
PS_Home
```

Specifies C:¥Program Files¥CA¥Identity Manager¥Provisioning Server¥bin

インストールしたすべてのコネクタについて1つのファイルバージョンが生成されます。

[アカウントテンプレート]内のルール文字列

アカウントテンプレートを作成する場合、多くのアカウント属性の形式を定義するためにルール文字列を使用します。ルール文字列は実際の値の変数です。ルール文字列は、アカウントごとに変更しうる属性を生成する場合に便利です。ルールの評価時に、**CA Identity Manager** はアカウントテンプレートに入力されたルール文字列を、ユーザ オブジェクトに指定されたデータに置き換えます。

注: 検索中に作成されたアカウントにもプロビジョニング ロールなしに作成されたアカウントにも、ルール評価は実行されません。

CA Identity Manager のルール文字列の一覧を次の表に示します。

ルール文字列	説明
%AC%	アカウント名
%D%	<i>dd/mm/yyyy</i> 形式での現在日（日付はグローバル ユーザ情報に含まれない計算値です）。 このルール文字列は、次のいずれとも同等です。 %\$\$DATE()% %\$\$DATE%
%EXCHAB%	Exchange アドレス帳に表示されないメールボックス
%EXCHS%	メールボックス ホーム サーバ名
%EXCMS%	メールボックス ストア名
%GENUID%	数値 UNIX/POSIX ユーザ識別子 このルール変数は、グローバル ユーザの UID 値が設定されている限り、 %UID% と同じです。ただし、グローバル ユーザに割り当てられた UID 値がなく、 UID 生成が有効にされる（[システム タスク] の上の [グローバル プロパティ]）場合、いくつかのアクションが発生します。次の利用可能な UID 値はグローバル ユーザに割り当てられて、このルール変数の値として使用されます。
%P%	パスワード
%U%	グローバル ユーザ名
%UA%	住所（郵便番号、都道府県、市区町村、番地から生成）
%UB%	ビルド
%UC%	市区町村
%UCOMP%	会社名

ルール文字列	説明
%UCOUNTRY%	国
%UCUxx% または %UCUxxx%	カスタム フィールド (xx または xxx は、[システム タスク] フレームの [カスタムユーザフィールド] タブに指定された 2 桁または 3 桁のフィールド ID を表します)。
%UD%	説明
%UDEPT%	部門
%UE%	電子メール アドレス
%UEP%	電子メール アドレス (メイン)
%UES%	電子メール アドレス (予備)
%UF%	名
%UFAX%	FAX 番号
%UHP%	ホーム ページ
%UI%	頭文字
%UID%	数値 UNIX/POSIX ユーザ識別子
%UL%	姓
%ULOC%	場所
%UMI%	ミドル ネームのイニシャル
%UMN%	ミドル ネーム
%UMP%	モバイル電話番号
%UN%	フルネーム
%UO%	オフィス名
%UP%	電話番号
%UPAGE%	ポケットベル番号
%UPC%	郵便番号
%UPE%	内線番号
%US%	都道府県
%USA%	番地
%UT%	職位

ルール文字列	説明
%XD%	固定長文字列形式の XML dateTimeValue 形式で現在のタイムスタンプが生成されます。 dateValue 属性または timeValue 属性に、dateTimeValue の日付部分や時刻部分を取り出すためのサブ文字列表現 (:offset,length) を 1 つ記述できます。たとえば、%XD:1,10% と指定すると、YYYY-MM-DD が生成されます。%XD:12,8% と指定すると、HH:MM:SS が生成されます。

属性の値

アカウント属性に特定の定数値を使用するには、ルール文字列内ではなくアカウントテンプレートフィールド内に値を入力します。たとえば、頻度制限と数量サイズを指定する値を入力できます。

定数の属性値にパーセント記号を含める必要がある場合、パーセント記号 1 つごとに 2 回繰り返します (%%)。繰り返されたパーセント記号 (%%) は、アカウント属性値の構築時に 1 つのパーセント記号 (%) に変換されます。アカウントテンプレート値に、パーセント記号が 1 つしかない場合、エラーが生成されます。つまりこの規則では、25% のリテラル値が必要な場合、25%% と指定する必要があります。ただし、特殊な場合として 25% は使用できます。

詳細なルール式

単純なグローバルユーザ属性を代入する場合よりも柔軟性を持たせるために、以下のような詳細なルール式を入力できます。

- オフセットと長さを使用したルール式のサブストリング
- ルールの文字列と値を組み合わせて使用
- 複数値アカウント属性に複数値を設定するためのルール式
- その他のグローバルユーザ属性のルール変数
- 組み込み関数の呼び出し
- ユーザが記述したプログラム終了関数の呼び出し

ルールの文字列と値の組み合わせの使用

アカウントテンプレートの属性値に、ルール文字列と定数値を組み合わせて使用することができます。たとえば、ルール文字列 **%UI%** がない場合、以下のように複数のルール式を連結することによって同じ効果を得ることができます。

```
%UF:,1%%UMI:,1%%UL:,1%
```

ルール文字列 **%UA%** は以下に相当します。

```
%USA%, %UC%, %US%, %UPC%
```

また、以下のようにルール文字列と定数値を組み合わせて、UNIX ホームのエンドポイント属性を作成できます。

```
/u/home/%AC%
```

ルールのサブストリング

ルール変数のサブストリング値を作成する構文を以下に示します。

```
%var[:offset,length]%
```

var

前に示した表に定義されている、定義済みのルール変数名を表します。

offset

(オプション) サブストリングサフィックスの開始オフセットを定義します。数字の **1** は最初の文字を表します。

length

(オプション) サブストリングサフィックスの終了オフセットを定義します。**length** の値としてアスタリスク (*) を指定すると、値の最後を表します。

たとえば、アカウント属性をグローバル ユーザの建物の属性の最初の 4 文字に設定するには、以下を使用して変数を定義します。

```
%UB:1,4%
```

建物の属性が空であるか、4 文字に満たない場合、アカウントの属性値は 4 文字未満になります。

複数値のルール式

大半のルール式は単一値を扱います。1つのユーザ属性値（空の場合もある）を使用して開始され、結果は1つのアカウント属性値（これも空の場合がある）となります。ただし、空のユーザ属性を0の値として考える必要がある場合があります。また、複数値を取るアカウント属性値のために複数の値を生成する必要があります。

以下のルール構文では、ユーザ属性に含まれる0以上の値を操作できます。

`%*var%`

ルール式の%記号の直後にオプションの複数値フラグであるアスタリスク(*)を指定すると、参照されているユーザ属性に含まれる値の数に応じて、このルール式は0、1、または1よりも大きい値になります。

大半のユーザ属性値は単一値であるため、0、または1の値のみが含まれます。ただし、カスタム属性(CustomField01 ~ CustomField99)は複数値属性であるため、これらの属性を参照するルール変数は0、1、または1以上の値を含む可能性があります。

ユーザ属性に複数の値が含まれている場合に、ルール式にアスタリスク(*)を含めないと、ルール評価の結果は最初の値の結果となります。しかし、多くの場合、複数値は正式に順序付けられていないため、CA Identity Managerが最初の値とみなす値は予測できません。

ユーザ属性に複数の値があり、ルール式に*を含めると、そのアカウント属性には複数の値が生成されます。アカウントテンプレート属性から設定されるアカウント属性自体が複数値をとらない場合は、そのアカウントテンプレートには複数値のルール式を定義しないでください。

ADS エンドポイント タイプの拡張アカウント属性を複数値として定義し、その複数値のルール式構文を使ってその属性を設定することができます。たとえば、**patents** という名前の拡張 ADS アカウント属性と、同じ **patents** という名前の付いたカスタム ユーザ属性番号 3 を定義する環境を考えてみます。

ADS アカウントテンプレートは、**patents** 属性としてルール文字列 `%*UCU03%` を定義します。次に、1つまたは複数の値を追加して、ユーザの **patents** 属性を変更できます。ユーザに変更を加える際に、ユーザのアカウントを更新するオプションを選択します。これによってアカウントのアカウントテンプレートが確認され、ルール変数 `%*UCU03%` が検出されると、ユーザのすべての **patents** がアカウントの **patents** 属性にコピーされます。

同様に、アカウントの作成中にもルール文字列は評価されます。さらに、アカウントテンプレートの変更時にルール文字列を変更した場合、そのアカウントテンプレートに関連するすべてのアカウントのルールの再計算を選択できます。

`%*var%` 構文は、単一値のユーザ属性を参照する変数 `var` にも有効です。有効になるのは、連結が行われ、参照される属性がユーザに設定されていない場合のみです。

オプションの複数値フラグであるアスタリスク (*) は、ユーザ属性に値がない場合に、`%*var%` ルール変数を含むルールが値なしと評価することを示します。これは、単一値のルール式 `%var%` とは異なります。単一値のルール式は、空の文字列であっても必ず単一の値と評価します。

この違いを理解するために、以下のルール文字列について考えてみます。

```
(310)%UP%
(310)%*UP%
```

これらのルール文字列は両方とも、電話番号にエリアコード **310** を追加します。ただし、ユーザが電話番号の値を持っていない場合に、最初のルールはアカウントの値として **(310)** と評価してしまう点が異なります。**2** 番目のルール文字列は値を生成せず、アカウント属性は未設定のままになります。

一方、電話番号に内線番号を追加する以下のルール文字列を考えてみます。

```
%UP% %UPE%
%UP% %*UPE%
```

すべての人が電話番号を持っているのに、一部の人が内線番号を持っていない場合、最初のルール文字列は各ユーザに内線番号のない電話番号を含む値を生成します。**2** 番目のルール文字列は値を生成しません。この場合は、`%UPE%` を使った最初のルールを使用します。

明示的なグローバル ユーザ属性ルール

以前のルール テーブルにリストされていた属性に比べ、より多くの属性を各ユーザが持つようになりました。これらの他の属性を参照するルール式を作成する必要はない可能性があります。しかし、必要に応じて、以下の構文を使用して特定のユーザ属性を参照することができます。

`%#ldap-attribute%`

たとえば、ユーザの [一時停止] フィールドの値を特定しなければならない場合、このフィールドの対応する LDAP 属性名 (`eTSuspended`) を特定し、`0` または `1` と評価されるルール式を作成します。`eTSuspended` の場合、以下のように指定します。

`%#eTSuspended%`

もう 1 つ例を挙げると、以下のルール式でユーザの割り当てられたプロビジョニング ロールを取得できます。

`%%*#eTRoleDN%`

これらのプロビジョニング ロールは、完全な LDAP 識別名の値です。組み込み関数 `RDNVALUE` (後に示される表を参照) と組み合わせると、この値はもう少し役立つようになります。ユーザの割り当てられたプロビジョニング ロールをすべて取得するために、複数値を示すアスタリスク (*) を使用していることに注意してください。

サブストリング構文は、これらのルール式にも適用されます。したがって、`%UP:6,*` と同じ内容を示す `%#eTTelephone:6,*%` を使用することができます。これによって、CA Identity Manager はユーザの電話フィールドの最初の 5 文字を除きます。

組み込みルール関数

値のさまざまな変換を実行するために、ルール式に組み込みルール関数を使用できます。組み込みルール関数を呼び出すための一般的な形式は以下のとおりです。

```
%[*]$$function(arg[,...])[:offset,length]%
```

複数值を示すアスタリスク（*）と、オフセットと長さのサブストリングの指定はオプションです。

認識されている組み込み関数は、以下のとおりです。

組み込みルール関数	説明
ALLOF	すべてのパラメータを複数值属性にマージします。順序は保持され、重複は削除されます。たとえば、ユーザ属性が以下のように設定されたとします。 eTCustomField01: { A, B } eTCustomField02: { A, C } この場合、 %*ALLOF(%*UCU01%,%*UCU02%)% というルールは 3 つの値 { A, B, C } と評価されます。
DATE	dd/mm/yyyy 形式の現在の日付が評価されます。ルール式 %D% は以下のいずれかに相当します。 \$\$\$DATE()% \$\$\$DATE%
FIRSTOF	パラメータの最初の値を返します。属性が設定されていない場合に、デフォルト値を挿入するために使用されます。 \$\$\$FIRSTOF(%UCU01%, 'unknown')% \$\$\$FIRSTOF(%LN%, %UCU01%, %U%)% 値が設定されていないと、結果に値が含まれません。引数に定数の文字列を入力する場合は、一重引用符で囲む必要があります。
INDEX	複数值属性の値を 1 つ返します。Index 1 は最初の値です。実在する値の個数より大きな値をインデックスに指定すると、結果として未設定（空）の値が返されます。以下の 1 行目のルールは 2 行目のルールに相当します。 \$\$\$INDEX(%*UCU01%, 1)% \$\$\$FIRSTOF(%*UCU01%)%

組み込みルール関数	説明
NOTEEMPTY	1つの引数の値を1つ返しますが、この属性値が設定されていないとエラーがレポートされます。 事例 1 ユーザに UID 属性が割り当てられていない場合、アカウントの作成または更新が失敗します。 %%\$NOTEEMPTY(%UID%)% 事例 2 名を使用し、名前が設定されていない場合には姓を使用します。両者が設定されていない場合は、アカウントの作成または更新が失敗します。 %%\$NOTEEMPTY(%%\$FIRSTOF(%UF%, %UL%)%)%
PRIMARYEMAIL	複数の電子メールアドレスから抽出された、プライマリ電子メールアドレスを返します。式 %UE% は以下の式に相当します。 %%\$PRIMARYEMAIL(%UEP%)%
RDNVALUE	属性名を LDAP 識別名として扱い、その識別名からオブジェクトの共通名を抽出します。 %%*\$RDNVALUE(%#eTRoleDN%)% これによって、すべての割り当てられたプロビジョニングロールの共通名が返されます。ユーザが同じ共通名を持つ2つのプロビジョニングロールに属する場合、そのロール名は1つだけリストされます。
TOLOWER	大文字のテキストを小文字に変換します。 %%\$TOLOWER(%AC%)%
TOUPPER	小文字のテキストを大文字に変換します。 %%\$TOUPPER(%U%)%

組み込みルール関数	説明
TRIM	属性値の前後の空白を削除します。 たとえば、通常 “%UF %UL%” は空白文字によって区切られた名と姓を作成します。しかし、ユーザが空の名の属性を持っている場合、このルールによって値の末尾に空白が追加されてしまいます。この場合、 “%\$\$TRIM(%UF% %UL%)%” を使用すると、名または姓が未設定の場合でも、アカウント属性値の前後に空白が残ることはありません。

プロビジョニング ロールのパフォーマンス

プロビジョニング サーバで CA Identity Manager を使用する場合、プロビジョニングのパフォーマンス機能強化についていくつかの検討事項があります。

JIAM オブジェクト キャッシュ

CA Identity Manager は、Java IAM (JIAM) API を使用してプロビジョニング サーバと通信します。通信のパフォーマンスを改善するには、プロビジョニング サーバから取得されるオブジェクトのキャッシュを設定します。

JIAM キャッシュの有効化

JIAM キャッシュを有効化する方法

1. 管理コンソールから環境設定にアクセスします。[詳細設定] - [その他] を選択します。
2. JIAM キャッシュのユーザ定義プロパティを設定します。
 - プロパティ : JIAMCache
 - 値 : true
3. [追加] をクリックします。
4. [保存] をクリックします。
ユーザ定義プロパティが保存されます。

JIAM キャッシュの TTL の定義

JIAM キャッシュはデータが失効するまでの一定期間、情報を保存します。この期間は TTL (time-to-live、存続期間) と呼ばれます。JIAM キャッシュの TTL を秒単位で指定し、キャッシュにデータを存続させる期間を定義します。

ローカルにキャッシュされるデータを最大限利用するには、パフォーマンスへの影響を抑えつつ、適時にデータを利用できる期間を検討する必要があります。TTL の値として、最小で 1 日、最大で 7 日の設定を推奨します。使用する存続期間の値の表を以下に示します。

望ましい存続期間	TTL の設定値(秒)
24 時間 (1 日)	86,400
72 時間 (3 日)	259,200
120 時間 (5 日)	432,000
168 時間 (7 日)	604,800

JIAM キャッシュ TTL を定義する方法

1. 管理コンソールから [環境] にアクセスします。[詳細設定] - [その他] を選択します。
2. JIAM キャッシュ TTL のユーザ定義プロパティを設定します。
 - プロパティ : JIAMCacheTTL
 - 値 : JIAM キャッシュにデータが存続する秒数
デフォルト : 300
3. [追加] をクリックします。
4. [保存] をクリックします。
ユーザ定義プロパティが保存されます。

セッション プーリング

パフォーマンスを改善するために、CA Identity Manager はプロビジョニング サーバと通信する際に使用する、多数のセッションがプールされるように事前に割り当てることができます。

セッション プーリングの詳細については、*管理コンソールのオンライン ヘルプ*を参照してください。

既存環境用のプロビジョニング タスク

カスタム ロール定義をインポートして、ある環境でプロビジョニングを有効化する場合、管理コンソールでプロビジョニング専用のロール定義もインポートする必要があります。このようなロール定義は、以下のフォルダにあります。

`iam_im.ear¥management_console.war¥WEB-INF¥Template¥environment`

注: ロール定義のインポートの詳細については、「*Configuration Guide*」を参照してください。

第 10 章：管理されたサービス（基本的なアクセス リクエスト）

このセクションには、以下のトピックが含まれています。

[サービスの作成](#) (P. 240)

[サービスをユーザに利用可能にする](#) (P. 252)

[サービスの変更](#) (P. 255)

[「アクセスをリクエストおよび表示」への検索の追加](#) (P. 257)

[サービスの削除](#) (P. 258)

[サービスへのアクセスの更新](#) (P. 260)

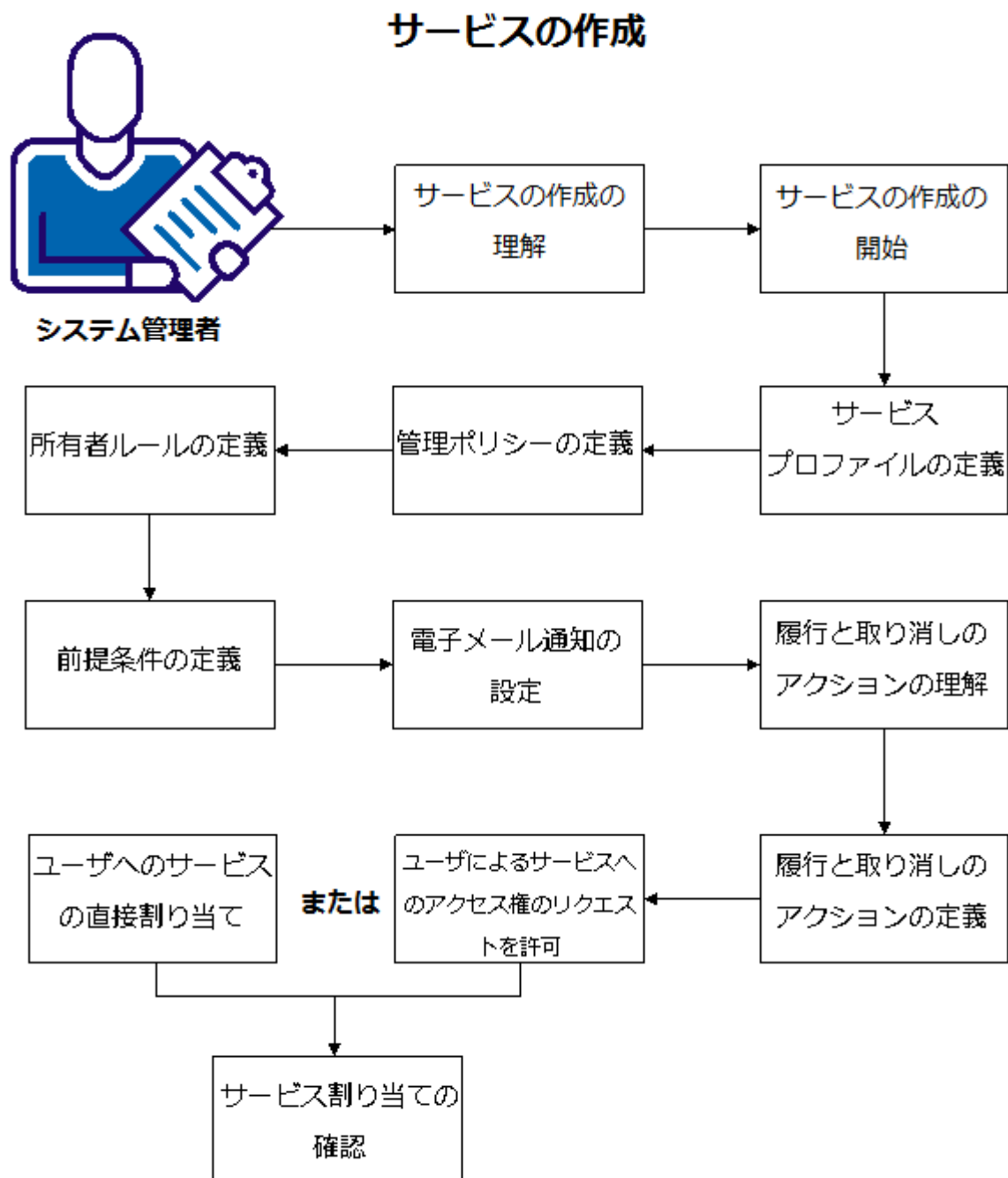
サービスの作成

サービスは権限管理を簡略化します。サービスにより、ユーザが指定ビジネスロールに必要なすべての権限（タスク、ロール、グループ、および属性）をまとめます。ユーザは、**CA CloudMinder ユーザ コンソール**の「アクセス リクエスト」タスクからサービスにアクセスできます。「アクセス リクエスト」タスクでは、ユーザまたは管理者がサービスのリクエスト、割り当て、取り消し、更新を実行できます。

サービスを使用すると、管理者はユーザ権限を 1 つのパッケージに統合することができ、それはセットとして管理されます。たとえば新しい販売担当者は全員、定義済みのタスク セットおよび特定のエンドポイント システム上のアカウントを必要とします。また、ユーザ アカウント プロファイルに特定の情報を追加することも必要です。管理者は、新しい販売担当者のためのすべての必要なタスク、ロール、グループ、およびプロファイル属性情報を含む「**Sales Administration**」という名前のサービスを作成します。管理者がユーザに「**Sales Administration**」サービスを割り当てると、ユーザは、このサービスによって定義されたロール、タスク、グループ、およびアカウント属性のセットを受け取ります。

また、ユーザ自身がサービスへのアクセスをリクエストすることもできます。ユーザ コンソール には、各ユーザがリクエスト可能なサービスのリストがあります。このリストは、サービスの作成時などに管理者によって「自己登録」としてマークされ、適切な権限が付与されたサービスが自動入力されています。ユーザは、サービスのリストから必要なサービスへのアクセス権をリクエストすることができます。ユーザがサービスへのアクセス権をリクエストすると、リクエストは自動的に履行され、関連する権限は、すぐにユーザに割り当てられます。適切な権限を持つ管理者は、サービス履行の設定を行って、ワークフロー承認の要求や電子メール通知の生成を指定することができます。

以下の図は、サービスを作成するために理解すべき情報、および実行する手順を示します。



以下のトピックでは、サービスを作成し、ユーザから利用可能にする方法について説明します。

1. [サービスの作成の理解。](#) (P. 242)
2. [サービスの作成の開始。](#) (P. 243)
3. [サービス プロファイルの定義。](#) (P. 243)
4. [サービスの管理ポリシーの定義。](#) (P. 246)
5. [サービスの所有者ルールの定義。](#) (P. 247)
6. [サービスの前提条件の定義。](#) (P. 247)
7. [サービスの更新の電子メール通知の設定。](#) (P. 248)
8. [履行と取り消しのアクションの理解。](#) (P. 249)
9. [サービスの履行と取り消しのアクションの定義。](#) (P. 249)
10. ユーザのサービスへのアクセス リクエストの許可。
ユーザ コンソールで [マイ アクセス] をクリックしてから [アクセスをリクエスト/表示] をクリックすると、そのユーザがリクエスト可能なサービスのリストが表示されます。このリストに表示されるサービスは、サービスの作成時などに管理者によって「自己登録」としてマークされ、適切な権限が付与されたサービスです。
11. [ユーザへのサービスの直接割り当て。](#) (P. 91)
12. サービス割り当ての確認。

サービスの作成の理解

サービスを作成する前に、サービスの作成と履行に必要な前提条件となる情報および権限を考慮します。

以下の質問について考慮します。

1. このサービスが対応するビジネス ニーズは何ですか。たとえば、Salesforce.com 上のアカウントをすべての新入社員に利用可能にするサービスを作成できます。
2. サービスのメンバは特定の管理ロールを必要としますか。そうであれば、それらの管理ロールを作成または特定します。

3. サービスのメンバは、1つ以上のエンドポイントへのアクセスを受信する必要がありますか。そうであれば、それらのエンドポイントを作成または特定します。
4. サービスのメンバがエンドポイントへのアクセスを必要とする場合は、関連するプロビジョニング ロールおよびアカウント テンプレートを作成または特定します。
5. サービスのメンバはあるグループのメンバである必要がありますか。そうであれば、それらのグループを作成または特定します。
6. ユーザがサービスのメンバになるとき、特定のユーザ属性が参照または変更される必要がありますか。たとえば、ユーザが **Salesforce.com** サービスを受けるとき、そのユーザの部署属性を **Sales** に設定するかどうかを確認することが必要ですか。そうであれば、それらのユーザ属性を作成または特定します。

これらの前提条件を作成または特定すると、[サービスの作成を開始](#) (P. 243) できます。

サービスの作成の開始

ユーザ コンソール からサービスを作成します。

次の手順に従ってください:

1. サービス管理権限があるアカウントにログインします。
たとえば、環境の最初のユーザはシステム マネージャ ロールを持ちます。このロールには [サービスの作成] タスクが含まれます。
2. ナビゲーション メニューから [サービス] （ [タスク] に表示されます）を選択します。
3. [サービスの管理] - [サービスの作成] をクリックします。
4. サービス プロファイルを定義します。

サービス プロファイルの定義

[プロファイル] タブで、サービスの基本的な特性を定義します。

次の手順に従ってください:

1. 名前およびタグを入力します。タグは、サービスの一意の識別子です。
注: タグには英数字とアンダースコアの文字のみを含めることができ、数字で開始することはできません。タグ名は、一度作成されると、後でサービスが削除されても変更または再利用ができません。

2. 作成後、すぐにこのサービスをユーザが使用できるようにする場合は、[有効]を選択します。
3. このサービスを、ユーザがリクエストできるサービスのリストに表示したい場合は、[自己登録]を選択します。[自己登録]が有効になっていると、ユーザはユーザ コンソールを使用してこのサービスへのアクセスをリクエストすることができます。
4. (オプション) 1つ以上のカテゴリを追加します。カテゴリ名を入力し、上向き矢印をクリックしてサービスに追加します。

カテゴリは、サービスの情報を追加します。この追加情報により、多数のサービスを含む環境におけるサービス検索を簡易化できます。

5. ユーザがサービスをリクエストするときに追加のユーザ データを収集する場合は、[サービス ランタイム ユーザ データ画面]を指定します。

[サービス ランタイム ユーザ データ画面]は、サービスの履行に必要なすべてのユーザ データがシステムに存在することを保証するために使用します。たとえば、Google Apps でアカウントを作成するサービスを履行する場合は、有効な電子メールアドレスが必要です。ユーザの電子メールアドレスが CA CloudMinder ユーザ ストアに存在しない場合、サービスのリクエスト時にそれを入力する必要があります。

- a. [参照] をクリックします。

利用可能なプロフィール画面のリストが表示されます。これらの画面は通常、ユーザデータを収集するために使用されます。

- b. 収集するユーザデータが含まれるプロフィール画面を選択します。以下のいずれかのオプションを選択します。

- 画面に含まれるユーザデータをすべて収集するには、[選択] をクリックします。

OR

- 収集するユーザデータをカスタマイズするには、[コピー] をクリックします。新しい画面用の名前および一意のタグを指定します。ユーザデータエレメントの追加、編集、または削除を行って、[OK] をクリックします。

OR

- 画面に含まれるユーザデータを変更するには、[編集] をクリックします。ユーザデータエレメントの追加、編集、または削除を行って、[OK] をクリックします。

重要: ユーザデータ画面を編集すると、この変更は、ユーザコンソール内でこの画面が使用されるすべての個所に適用されます。代わりに、プロフィール画面をコピーしてカスタマイズすることを考慮してください。

- c. [選択] をクリックします。

選択したユーザデータエレメントが、ユーザによるサービスのリクエスト時に収集されます。

注: ユーザがサービスをリクエストするときに、必要なデータがシステムに存在する場合は、そのデータがプロフィール画面に自動入力されます。

6. [サービスの管理ポリシーの定義。](#) (P. 246)

サービスの管理ポリシーの定義

「管理者」タブで、サービスのメンバおよび管理者としてユーザを追加または削除するユーザを定義します。管理ポリシーには、管理ルールとスコープルール、および少なくとも1つの管理者権限（「メンバの管理」または「管理者の管理」）が含まれます。

管理ルールは、誰がこのサービスを管理できるかを定義します。スコープルールは、管理者になることができるユーザを制限します。たとえば、管理ルールは、Sales グループの全メンバがサービスを管理することを可能にできます。その後、スコープルールで、ボストンにいる Sales グループのメンバのみにユーザを制限することができます。

次の手順に従ってください：

1. 「管理者」タブで「追加」をクリックします。
「管理ポリシー」画面が表示されます。
2. ユーザがこのサービスを管理するための管理ルールを定義します。たとえば、Sales グループのメンバであるユーザ、または職位のプロファイル属性が「営業マネージャ」であるユーザを指定することができます。

ルールのうち、以前に指定された個所を編集するには、左矢印をクリックします。
3. このサービスを管理できるユーザを制限するための、スコープルールを定義します。たとえば、管理ルールで、Sales グループのメンバであるユーザを指定していた場合、そのルールのスコープを制限して、市区町村名が「ボストン」であるユーザのみとすることができます。

注：各サービスについて、異なるルールと権限を持つ複数の管理ポリシーを追加することができます。
4. 管理者にこのサービスのメンバの追加または削除を許可する場合は、「このサービスのメンバを管理できます」をクリックします。
5. 「OK」をクリックします。
6. ポリシーをさらに編集するには、「編集」アイコンをクリックします。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。
7. [サービスの所有者ルールを定義します。](#)（P. 247）

サービスの所有者ルールの定義

「所有者」タブで、サービスの所有者となることができるユーザに関するルールを定義します。所有者は、サービスを変更できるユーザです。

次の手順に従ってください:

1. 「所有者」タブで「追加」をクリックします。
「所有者ルール」画面が表示されます。
2. ユーザがこのサービスを所有するための所有者ルールを定義します。たとえば、Sales グループのメンバであるユーザ、または職位のプロファイル属性が「営業マネージャ」であるユーザを指定することができます。
ルールのうち、以前に指定された個所を編集するには、左矢印をクリックします。
3. 「OK」をクリックします。
4. [サービスの前提条件を定義します。](#) (P. 247)

サービスの前提条件の定義

「前提条件」タブで、サービスをリクエストする前にユーザが必要とするサービスを定義します。ユーザがすべての前提条件サービスのメンバである場合のみ、そのユーザの利用可能なサービス リストに表示されます。

前提条件サービスに対して期間が設定されていると、定義するサービスにその期間が適用されます。たとえば、サービス A がサービス B の前提条件であるとしします。サービス A の期間は 1 週間です。サービス B もまた、1 週間で期限切れになります。

次の手順に従ってください:

1. 「前提条件」タブで「サービスの追加」をクリックします。
検索画面が表示されます。
2. このサービスの前提条件として指定するサービスを検索します。
自分が管理者権限を持つすべてのサービスのリストを表示するには、検索条件を変更せずに「検索」をクリックします。
3. サービスを選択し、「選択」をクリックします。
このサービスの前提条件の更新されたリストが表示されます。

サービスの更新の電子メール通知の設定

いくつかのサービスは、一定期間の後に期限切れになります。

[電子メール] タブで、メンバシップが期限切れになる前にサービスメンバにその更新を促す電子メール通知を設定することができます。メンバは、サービスの更新タスクを使用してアクセスを更新します。

CA CloudMinder では、動的コンテンツを含むデフォルト電子メールテンプレートが提供されています。電子メールの送信時に、このコンテンツが自動入力されます。動的コンテンツ（電子メール通知エディタで中括弧（{}）内に表示されます）は、特定のユーザ名、サービス名、および有効期限を電子メールに追加します。

エディタ内の電子メール通知のコンテンツは、変更することができます。たとえば、本文または件名の変更、フォントの変更、または動的コンテンツの削除などがあります。

電子メール通知を設定するときは、以下に注意してください。

- 電子メール通知に動的コンテンツを含める場合は、中括弧（{}）内のテキストを変更しないでください。
- サービスに、期限切れになる前提条件サービスがある場合、電子メール通知が両方のサービスについて設定されていた場合でも、電子メール通知は前提条件サービスについてのみ送信されます。

次の手順に従ってください：

1. [電子メール] タブで、[サービスの有効期限が切れる前にユーザへ電子メール通知を送信] チェックボックスを選択して通知を有効にします。
2. （オプション）エディタのコントロールを使用して、電子メール通知をカスタマイズします。

電子メール通知エディタは HTML をサポートします。ツールバーで [HTML ソースの切り替え] ボタン (<>) をクリックすると、電子メール通知の本文に HTML コンテンツを追加できます。

3. [履行と取り消しのアクションを理解します。](#) (P. 249)

履行と取り消しのアクションの理解

［アクション］タブで、サービスの割り当てまたは取り消し時に追加、変更、または削除される権限と情報（タスク、ロール、グループ、および属性）を定義します。つまり、サービスアクションは、サービスが実行するアクションを定義します。

CA CloudMinder では、Policy Xpress ポリシーを使用して、履行と取り消しが発生する状況を定義します。CA CloudMinder は、ユーザがサービスをリクエストしたとき、常に適切な条件とデータが存在するように、このポリシーを事前設定します。サービスは自動的に履行または取り消されます。

管理者は、サービスの履行または取り消し時にシステムが実行するアクションを定義する必要があります。たとえば、サービスを作成するとき、管理者は、サービスメンバが［営業マネージャ］管理ロール、［Salesforce.com］プロビジョニングロール、および［Sales］グループを受信するように指定することができます。同様に管理者は、サービスの取り消し時これらの権限が削除されるように指定することができます。

サービスの履行と取り消しのアクションの定義

［アクション］タブで、ユーザへのサービスの割り当て、またはユーザからのサービスの削除時に、追加、変更、または削除される権限と情報を定義します。

次の手順に従ってください：

1. ［アクション］タブをクリックします。

履行と取り消しのアクションの画面が表示されます。

2. [履行アクションの管理] または [取り消しアクションの管理] ボタンをクリックします。

[Policy Xpress ポリシーの作成] 画面が表示されます。

以下のフィールドがアクションルールの作成用に事前定義されています。

名前

アクションルールについて、わかりやすい名前を定義します。一意の名前を指定する必要があります。

説明

アクションルールの意味を定義します。

優先度

いくつかのアクションルールが一致した場合に、どのアクションルールを実行するかを定義します。このフィールドは、デフォルトのアクションを定義する場合に有用です。たとえば複数のルール（1つの部門ごとに1つのルール）がある場合は、条件がなく、優先度の低い（他のルールが5の場合は10など）ルールを追加することによって、デフォルトを設定できます。部門のルールがいずれも一致しない場合は、デフォルトのルールが使用されます。

3. [アクションルール条件] に一致条件を指定します。
4. [追加アクション] の下にある [一致した場合の追加アクション] ボタンをクリックします

[一致した場合の追加アクション] 画面が表示されます。この画面で、ルールに一致した場合にシステムが実行するアクションを定義します。

5. アクションの目的を定義するフレンドリ名を入力します。
たとえば、「営業マネージャ管理ロールの追加」と入力します。
6. システムに実行させるアクションのカテゴリを選択します。
たとえば、ロールを追加するには [ロール] カテゴリを選択します。
7. システムに実行させるアクションのタイプを選択します。
たとえば、管理ロールを追加するまたは削除するには、[管理ロールの設定] タイプを選択します。
8. システムに実行させる機能を選択します。
たとえば、管理ロールを追加するには、[追加] 機能を選択します。

注: 機能を選択すると、その機能の説明が表示されます。この説明で、選択した機能によってシステムが希望する動作を行うかどうかを確認することができます。

9. システムに実行させるアクションを定義します。

たとえば、「販売マネージャ」という名前の管理ロールを追加するには、ロール名を入力するか、[参照] ボタンをクリックして利用可能な管理ロールのリストから「販売マネージャ」を選択します。

10. [OK] をクリックします。

このサービスに必要なすべてのアクションを追加するまで、この手順を繰り返します。

11. [OK] をクリックします。

システムは、指定の履行アクションおよび取り消しアクションをサービスに関連付けます。ユーザがサービスを受信すると、関連する権限および情報は追加、変更、または削除されます。

12. [ユーザにサービスを割り当てる](#) (P. 91) ができるようになりました。

ユーザへのサービスの割り当て

個別のユーザにサービスを直接割り当てることができます。このユーザはサービスのメンバになります。

次の手順に従ってください:

1. [サービス] - [アクセスをリクエスト/表示] に移動します。

管理できるサービスのリストが表示されます。

2. ユーザに割り当てるサービスを選択し、[選択] をクリックします。

サービスに割り当てられたユーザのリストが表示されます。

3. [アクセスをリクエスト] をクリックします。

4. サービスを割り当てるユーザを検索します。

自分が管理者権限を持つすべてのユーザのリストを表示するには、検索条件を変更せずに [検索] をクリックします。

5. ユーザを選択し、[選択] をクリックします。

サービスに割り当てられたユーザの更新されたリストが表示されます。

6. [変更の保存] をクリックします。

ユーザは指定されたサービスを受信します。ユーザは、サービスに含めたアプリケーション、ロール、グループおよび属性をすべて受信します。

サービス割り当ての確認

ユーザにサービスを割り当てたら、そのサービスと関連付けられたタスクがすべて正常に完了したことを確認します。

次の手順に従ってください：

1. [サービス] - [サービス アクセス リクエスト履歴の表示] に移動します。
検索画面が表示されます。
2. ユーザに割り当てたサービスを検索します。
自分が管理者権限を持つすべてのサービスのリストを表示するには、検索条件を変更せずに [検索] をクリックします。
管理できるサービスのリストが表示されます。
3. 割り当てたサービスを選択し、[選択] をクリックします。
サービスと関連付けられたアクションの履歴が表示されます。
4. 先に最新のアクションを参照するために [前回変更] をクリックします。
5. 該当するユーザがサービスを正常に受信したことを確認します。
6. [閉じる] をクリックします。

サービスをユーザに利用可能にする

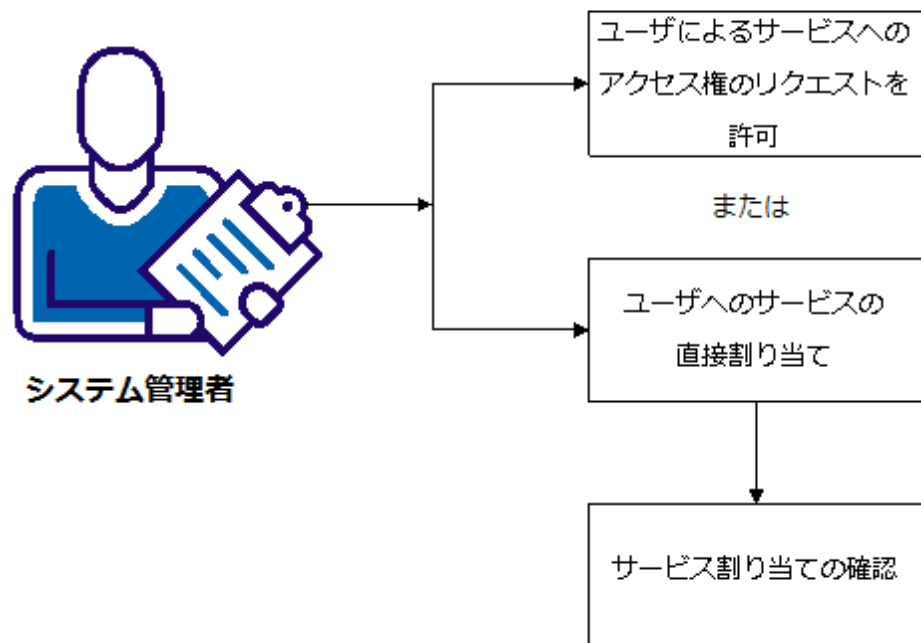
サービスは権限管理を簡略化します。サービスは、指定されたビジネス ロールに対してユーザが必要とする権限をすべてバンドルします。ユーザは、ユーザ コンソールの [アクセス リクエスト] タスクからサービスにアクセスできます。[アクセス リクエスト] タスクでは、ユーザまたは管理者が、ユーザ インターフェースを使用してサービスのリクエスト、割り当て、取り消し、更新ができます。

サービスを使用すると、システム管理者は、ユーザ アクティビティおよび情報（タスク、ロール、グループ、および属性）を 1 つのパッケージに統合することができ、それはセットとして管理されます。たとえば新しい販売担当者は全員、定義済みのタスク セット、特定のエンドポイント システム上のアカウント、およびユーザ アカウント プロファイルに追加された特定の情報へのアクセスを必要とします。システム管理者は、新しい販売担当者のためのすべての必要なタスク、ロール、グループ、およびプロファイル属性情報を含む「Sales Administration」という名前のサービスを作成します。管理者がユーザに「Sales Administration」サービスを割り当てると、ユーザは、このサービスによって定義されたロール、タスク、グループ、およびアカウント属性のセットを受け取ります。

また、ユーザー自身がサービスへのアクセスをリクエストすることもできます。ユーザーコンソールには、各ユーザーがリクエスト可能なサービスのリストがあります。このリストは、サービスの作成時などにシステム管理者によって「自己登録」としてマークされ、適切な権限が付与されたサービスが自動入力されています。ユーザーは、サービスのリストから必要なサービスへのアクセス権をリクエストすることができます。ユーザーがサービスへのアクセス権をリクエストすると、リクエストは自動的に履行されます。関連するタスク、ロール、グループ、および属性は、すぐにユーザーに割り当てられます。適切な権限を持つ CA CloudMinder 管理者は、サービス履行の設定を行って、ワークフロー承認の要求や電子メール通知の生成を指定することができます。

以下の図は、ユーザーに対してサービスを利用可能にするために理解すべき情報、および実行する手順を示します。

サービスを利用可能なユーザーにする



以下の方法で、ユーザに対してサービスを利用可能にすることができます。

1. ユーザ自身によるアクセス権のリクエストを許可します。

CA CloudMinder ユーザ コンソールで[マイ アクセス]をクリックしてから[アクセスをリクエスト/表示]をクリックすると、そのユーザがリクエスト可能なサービスのリストが表示されます。このリストに表示されるサービスは、サービスの作成時などに CA CloudMinder 管理者によって「自己登録」としてマークされ、適切な権限が付与されたサービスです。

アクセスをリクエストすると、ユーザにサービスが割り当てられます。ユーザは、サービスに関連付けられたアプリケーション、ロール、グループおよび属性をすべて受信します。サービスにアプリケーションの起動ロールが含まれる場合、アイコンおよびアプリケーションのリンクがユーザ コンソールのホーム ページに表示されます。

2. [ユーザへのサービスの直接割り当て。](#) (P. 91)
3. ユーザにサービスを直接割り当てる場合、[サービス割り当てを確認](#) (P. 255) します。

ユーザへのサービスの割り当て

個別のユーザにサービスを直接割り当てることができます。このユーザはサービスのメンバになります。

次の手順に従ってください:

1. [サービス] - [アクセスをリクエスト/表示] に移動します。
管理できるサービスのリストが表示されます。
2. ユーザに割り当てるサービスを選択し、[選択] をクリックします。
サービスに割り当てられたユーザのリストが表示されます。
3. [アクセスをリクエスト] をクリックします。
4. サービスを割り当てるユーザを検索します。
自分が管理者権限を持つすべてのユーザのリストを表示するには、検索条件を変更せずに [検索] をクリックします。
5. ユーザを選択し、[選択] をクリックします。
サービスに割り当てられたユーザの更新されたリストが表示されます。
6. [変更の保存] をクリックします。
ユーザは指定されたサービスを受信します。ユーザは、サービスに含めたアプリケーション、ロール、グループおよび属性をすべて受信します。

サービス割り当ての確認

ユーザにサービスを割り当てたら、そのサービスと関連付けられたタスクがすべて正常に完了したことを確認します。

次の手順に従ってください:

1. [サービス] - [サービス アクセス リクエスト履歴の表示] に移動します。
検索画面が表示されます。
2. ユーザに割り当てたサービスを検索します。
自分が管理者権限を持つすべてのサービスのリストを表示するには、検索条件を変更せずに [検索] をクリックします。
管理できるサービスのリストが表示されます。
3. 割り当てたサービスを選択し、[選択] をクリックします。
サービスと関連付けられたアクションの履歴が表示されます。
4. 先に最新のアクションを参照するために [前回変更] をクリックします。
5. 該当するユーザがサービスを正常に受信したことを確認します。
6. [閉じる] をクリックします。

サービスの変更

システム管理者は、以前に作成したサービスを変更できます。たとえば、サービスにロールを追加することにより、サービスがサービス メンバに付与する権限を変更できます。また、サービスに対する管理者および所有者のルール、サービス的前提条件、およびその他の管理上の詳細を変更できます。

指定されたユーザのサービスを **CA CloudMinder** が履行済みの場合、そのサービスへの変更はユーザに伝達されません。サービスの変更を決定した場合、変更前にサービスを受信したユーザに元の権限があります。変更後にサービスを受信するユーザは、変更されたサービスによって付与される権限を持ちます。例として次の場合を考えてみましょう。

システム管理者は、サービス メンバに「販売マネージャ」ロールと「販売」グループを付与する「販売マネージャ」サービスを作成します。ユーザは「販売マネージャ」サービスをリクエストし、**CA CloudMinder** はユーザに適切なロールとグループを付与することにより、サービスを履行します。「従業員マネージャ」ロールを含めるために「販売マネージャ」サービスを変更することにします。こうすると、このサービスの既存メンバは「従業員マネージャ」ロールを受信しません。「営業マネージャ」サービスの新メンバーのみが、「販売マネージャ」ロールおよび「販売」グループに加えて「従業員マネージャ」ロールを受信します。

したがって、サービスの変更を考慮するのは、サービスがメンバを持たない場合のみにしてください。すなわち、どのユーザもサービスのリクエストおよび受信をしておらず、どの管理者もユーザにサービスを割り当てていない場合にのみ、サービスを変更するようにしてください。

サービスについては、管理情報、管理者および所有者のルール、サービスの前提条件、および権限（タスク、ロール、グループ、および属性）を変更できます。

次の手順に従ってください：

1. サービス管理権限がある **CA CloudMinder** アカウントにログインします。
たとえば、環境の最初のユーザはシステム マネージャ ロールを持ちます。このロールには [サービスの変更] タスクが含まれます。
2. ナビゲーション メニューから [タスク] - [サービス] を選択します。
3. [サービスの管理] - [サービスの変更] をクリックします。
検索画面が表示されます。
4. 変更するサービスを検索します。
自分が管理者権限を持つすべてのサービスのリストを表示するには、検索条件を変更せずに [検索] をクリックします。
5. サービスを選択し、[選択] をクリックします。
確認メッセージが表示されます。
6. [はい] をクリックします。
7. [サブミット] をクリックします。
CA CloudMinder は、変更をサービスに適用します。

[アクセスをリクエストおよび表示]への検索の追加

[アクセスをリクエストおよび表示] タスクにはサービスのリストが表示されますが、追加のサービスを検索するフィールドはありません。検索フィールドを追加するには、以下の手順に従います。

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの変更]を選択します。
2. [アクセスをリクエストおよび表示]を検索します。
3. サービス カテゴリのタスクを選択します。
4. [タブ] をクリックします。
5. [タブ] の下で、[アクセスの管理] の左側の編集アイコンをクリックします。
6. [リスト画面] 行の上の[参照] をクリックします。
7. 正しい検索を追加するために適用されるオプションを設定します。
8. 必要な画面を選択し、[編集] ボタンをクリックして画面を編集します。
9. [標準リスト画面の設定] で、[ユーザが検索可能なフィールドの選択] セクションに移動します。
10. 検索フィールドを選択し、検索フィールド名を設定します。
11. [OK] をクリックして変更内容を保存します。

サービス リクエスト期間、ユーザ データなどのサービス リクエストに関する情報が、[サービス リクエスト] 承認ワークフロー アイテムに表示されます。また、[アクセスをリクエストおよび表示] タスクに **AddServiceToUserEvent** ポリシーベースのワークフローを割り当ててる場合、この情報が電子メールで送信されます。

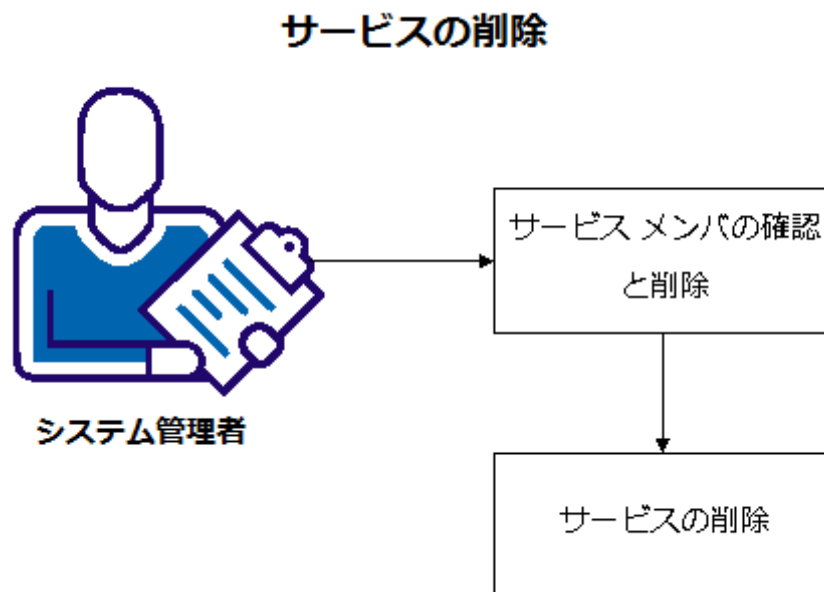
サービスの削除

システム管理者は、サービスを削除できます。削除されたサービスは、完全にシステムから削除されます。

サービスにユーザが割り当てられている場合は、サービスを削除できません。サービスを削除する前に、割り当てられているすべてのユーザ、つまりメンバを確認して削除します。

注: 同様に、あるユーザがサービスのメンバである場合、そのユーザは削除できません。先にサービスのメンバからユーザを削除してから、ユーザを削除します。

以下の図は、サービスを削除するために理解すべき情報、および実行する手順を示します。



以下のトピックでは、サービスを削除する方法について説明します。

1. [サービス メンバの確認と削除](#) (P. 259)
2. [サービスの削除](#) (P. 259)

サービス メンバの確認と削除

サービスを削除する前に、まず既存のメンバを確認して削除します。

次の手順に従ってください：

1. サービス管理権限がある **CA CloudMinder** アカウントにログインします。
たとえば、環境の最初のユーザはシステム マネージャ ロールを持ちます。このロールには [サービスの変更] タスクが含まれます。
2. [タスク] - [サービス] - [アクセスをリクエスト/表示] を選択します。
管理できるサービスのリストが表示されます。
3. 削除するサービスを選択し、[選択] をクリックします。
サービスに割り当てられたユーザのリストが表示されます。
4. サービスがメンバを持つ場合は、すべてのユーザの横のチェック ボックスをオフにします。
5. [変更の保存] をクリックします。
確認メッセージが表示されます。
6. [はい] をクリックします。
CA CloudMinder はサービスからメンバを削除します。

サービスの削除

サービス メンバを持たないサービスを削除できます。

サービスを削除する方法

1. サービス管理権限があるアカウントで **CA CloudMinder** にログインします。
たとえば、環境の最初のユーザはシステム マネージャ ロールを持ちます。このロールには [サービスの削除] タスクが含まれます。
2. 左ペインから、または [タスク] を選択し、[サービス] に移動します。
3. [サービスの管理] - [サービスの削除] をクリックします。
検索画面が表示されます。

4. 削除するサービスを検索します。

自分が管理者権限を持つすべてのサービスのリストを表示するには、検索条件を変更せずに「検索」をクリックします。

5. サービスを選択し、「選択」をクリックします。

確認メッセージが表示されます。

6. 「はい」をクリックします。

サービスは削除されます。

サービスへのアクセスの更新

いくつかのサービスは、一定期間の後に期限切れになります。管理者は、ユーザーが継続してアクセス可能になるようにサービスを更新できます。

サービスは、以下のいずれかの方法で更新できます。

- サービスを選択し、更新するユーザアクセスを選択します
- ユーザを選択し、更新するサービスを選択します

注: 環境が設定によっては、エンドユーザも「アクセスの更新」タスクを使用してアクセスを更新することができます。

以下手順では、サービスを先に選択してアクセスを更新する方法について説明します。ユーザを先に選択する場合は、「ユーザ」カテゴリの「ユーザアクセス リクエスト」 - 「ユーザ更新リクエストの管理」タスクを使用します。

次の手順に従ってください：

1. ユーザ コンソールで「サービス」 - 「アクセスの更新」をクリックします。
2. 更新するサービスを検索し、選択します。

ユーザ コンソールは、選択したサービスに対して現在アクセス権があるユーザのリスト、およびそれらのアクセスが期限切れになる日付を表示します。

3. 「アクセス リクエスト」列の更新の期間を選択し、「OK」をクリックします。
「期間」フィールド内のオプションは、サービスが作成されるときに決定されます。
4. 「変更の保存」をクリックします。

ユーザ コンソールで「サービス アクセス リクエスト履歴の表示」を使用して、サービス更新のステータスを表示できます。

第 11 章：同期

このセクションには、以下のトピックが含まれています。

[サーバ間のユーザの同期](#) (P. 261)

[ユーザの作成または変更タスクにおけるユーザの同期](#) (P. 264)

[同期タスク](#) (P. 266)

サーバ間のユーザの同期

CA Identity Manager の同期を設定して、CA Identity Manager ユーザストアとプロビジョニングディレクトリのユーザのデータが一致していることを確認します。各ディレクトリまたはユーザストアの変更を行うには、インバウンド同期とアウトバウンド同期を設定します。

インバウンド同期

インバウンド同期によって、プロビジョニングディレクトリでの変更についての最新情報が CA Identity Manager ユーザに通知されます。プロビジョニングディレクトリでの変更には、プロビジョニングサーバへのコネクタを持つシステムによって行われた変更が含まれます。同期では、管理コンソールのプロビジョニング画面で定義されたマッピングが使用されます。

インバウンド同期のフェールオーバー

代替 CA Identity Manager Server URL へのフェールオーバーは、URL で指定されたアプリケーションサーバが実行されていない場合にのみ発生します。アプリケーションサーバが実行中で通知を受信したにもかかわらず、設定エラーが発生した場合（不明な環境がある場合、または環境が起動しない場合など）、これらのエラーによって通知の配信がブロックされます。これらの問題は、インバウンド通知が適切に機能できるように解決する必要があります。

アウトバウンド同期

アウトバウンド同期では、CA Identity Manager を使用して、プロビジョニングディレクトリにおいてユーザの作成および更新を行います。

プロビジョニング ディレクトリ ユーザの作成

プロビジョニング ディレクトリでのユーザ作成は、プロビジョニング関連のイベント（ユーザへのプロビジョニング ロールの割り当てなど）でのみ発生します。ユーザがプロビジョニング ディレクトリに作成されるのは、ユーザを作成するルールを割り当てる管理タスクを使用するときに限ります。

注: プロビジョニング ディレクトリ ユーザもグローバル ユーザと呼ばれます。グローバル ユーザとは、エンドポイント アカウントを接続する単一のユーザです。

CA Identity Manager でのユーザ作成によってプロビジョニング ディレクトリでのユーザ作成がトリガされた場合、CA Identity Manager は、新しいユーザの電子メールアドレスに、プロビジョニング ディレクトリで定義された一時パスワードを送信します。ユーザはこのパスワードでユーザ コンソールにログインできますが、パスワードを変更する必要があります。その結果、ユーザ ストアとプロビジョニング ディレクトリでパスワードが同期されます。

ユーザに電子メールアドレスがない場合、ユーザ ストアのパスワードを変更するまでユーザ コンソールにアクセスできません。

注: 一時パスワードを電子メールで送信するには、[環境] で電子メール通知を有効にし、電子メール通知に `CreateProvisioningUserNotificationEvent` を設定する必要があります（詳細については、「*Configuration Guide*」を参照してください）。

CA Identity Manager を使用したグローバル ユーザの更新

ユーザを変更する管理タスクを使用すると、プロビジョニング ディレクトリでユーザに対する更新が発生します。グローバル ユーザが存在しない場合は、同期は発生しません。

アウトバウンドマッピングは、CA Identity Manager のユーザ イベントを、プロビジョニング ディレクトリに影響を与えるアウトバウンド イベントに整合させます。

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

あるユーザが、プロビジョニングディレクトリ内に存在しているのに、CA Identity Manager に存在しない場合は、ユーザ コンソールでそのユーザを作成することができます。作成タスクに対して属性をマップしており、ユーザが同じユーザ ID を持っている場合は、プロビジョニングユーザの属性がプロビジョニングディレクトリで更新されます。これで、ユーザをユーザ コンソールから管理できます。

注: あるイベントによってユーザ属性が更新されており、その値を CA Identity Manager と同期させたい場合は、イベントをアウトバウンドイベント POST_MODIFY_GLOBAL_USER にマップする必要があります。

CA Identity Manager を使用したグローバル ユーザの削除

デフォルトで、アウトバウンド同期にはユーザの削除イベントが設定されています。CA Identity Manager でユーザを削除すると、そのユーザは、プロビジョニングディレクトリおよびエンドポイントのすべてのアカウントからも削除されます。

CA Identity Manager が管理エンドポイントにおいて、あるユーザのアカウントを削除できない場合、残りのアカウントからこのユーザを削除しますが、プロビジョニングディレクトリからはこのユーザを削除しません。

たとえば、ユーザ A が UNIX アカウントおよび Exchange アカウントを持っており、これらのアカウントは、プロビジョニングサーバで管理されているとします。CA Identity Manager でユーザ A が削除されると、プロビジョニングサーバは、そのユーザのアカウントを削除しようとします。通信エラーが原因で、プロビジョニングサーバが Exchange アカウントを削除できない場合、プロビジョニングサーバはユーザ A の UNIX アカウントを削除しますが、プロビジョニングディレクトリからはそのユーザを削除しません。ただし、ユーザ A はユーザ ストアにはリストアされません。

パスワード同期の有効化

プロビジョニングサーバでは、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のパスワード同期を行うことができます。エンドポイントで生成された変更を有効にするには、次の 2 つの設定が必要です。

- エンドポイントで生成された変更を取得し、その変更をプロビジョニングサーバへ送信するよう、エンドポイントを設定する必要があります。
- グローバルユーザに対して、パスワード同期エージェントの有効化属性を有効にしておく必要があります。

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。

ユーザの作成または変更タスクにおけるユーザの同期

ユーザを作成または変更するタスクのプロファイルタブにおいて、同期は、CA Identity Manager に対する変更がグローバル ユーザに対しても確実に行われるかを制御します。ユーザを作成または変更する管理タスクを作成するときに、アイデンティティ ポリシーが作成されている場合は、同期の制御を次のように設定します。

- ユーザ同期を [タスク完了時] に設定する
- アカウント同期を [タスク完了時] に設定する

注: パフォーマンスを最大にするには、[タスク完了時] オプションを選択します。ただし、複数のイベントが含まれているタスクについて [タスク完了時] オプションを選択すると、CA Identity Manager は、そのタスク内のすべてのイベントが完了するまで同期しません。イベントの 1 つまたは複数がワークフローの承認を必要とする場合、その承認に数日かかることがあります。すべてのイベントが完了するまで CA Identity Manager がアイデンティティ ポリシーを適用したりアカウントを同期しないであることを避けるには、[各イベント発生時] オプションを選択します。

ユーザを管理する管理タスクに属性を追加する場合は、管理コンソールのプロビジョニング画面で属性マッピングを更新する必要があります。 **CA Identity Manager** の各ユーザ属性に対しては、1つのデフォルトプロビジョニング属性が存在します。

User Attribute	Provisioning Attribute
☐ %ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
☐ %EMAIL%	%EMAIL%
☐ %ENABLED_STATE%	%ENABLED_STATE%
☐ %FIRST_NAME%	%FIRST_NAME%
☐ %FULL_NAME%	%FULL_NAME%
☐ %IDENTITY_POLICY%	%IDENTITY_POLICY%
☐ %LAST_NAME%	%LAST_NAME%
☐ %PASSWORD%	%PASSWORD%
☐ %PASSWORD_DATA%	%PASSWORD_DATA%
☐ %USER_ID%	%USER_ID%

同期タスク

以下のタイプの同期を実行できます。

ユーザの同期

各ユーザが、適切な管理エンドポイント上に必要なアカウントを持っていること、およびユーザのプロビジョニングロールによってコールアウトされたときに、各アカウントが適切なアカウントテンプレートに割り当てられることを保証します。

アカウントの同期

アカウント上の機能属性が、アカウントテンプレートに割り当てられているアカウントで示されている適切な値であることが保証されます。アカウントの同期は、強い同期にすることも、弱い同期にすることもできます。弱い同期の場合は、アカウントの機能属性が、少なくとも、そのアカウントテンプレートで必要な最小限の機能を持つことが保証されます。強い同期の場合は、アカウントの機能属性が、そのアカウントテンプレートで必要なものと同じ機能を持つことが保証されます。アカウントが、[強い同期] チェックボックスが選択されている1つ以上のアカウントテンプレートに属している場合は、アカウントの同期は強い同期になります。

ユーザ同期を制御するような[強い同期] チェックボックスはありませんが、類似の概念があります。[ユーザとロールの同期] メニュー項目を選択すると、次の2つの同期オプションが表示されます。

- 存在しないアカウントおよびアカウントテンプレートの割り当てを追加する。
- 不要なアカウントおよびアカウントテンプレートの割り当てを削除する。
- これは弱いアカウント同期に類似していますが、[追加]チェックボックスのみを選択して、グローバルユーザが、割り当てられているプロビジョニングロールで必要な最小限のアカウントを持つようにします。ただし、ユーザが、そのプロビジョニングロールで指示されていない他のアカウントを持つことも可能です。

[追加]と[削除]の両方のチェックボックスを選択して、ユーザがどのアカウントを持つのかをプロビジョニングロールが定義します（これは強いアカウントの同期に類似しています）。その他のすべてのアカウントは削除されます。

プロビジョニングロールがどのくらい詳細に定義されるかに基づいて、弱い/強いアカウント同期、または弱い/強いユーザ同期を選択します。ユーザが、明確に定義されているプロビジョニングロールに適合しており、アカウントアクセスがそれらのロールに関連している場合には、強い同期を使用します。

注: いくつかのエンドポイント タイプでは、デフォルトで強い同期を設定します。詳細については、「コネクタガイド」を参照してください。

ユーザ同期とアカウントの同期は、個別に実行しなければならない別のタスクです。通常は、ユーザ同期を最初に実行して必要なアカウントをすべて作成した後で、アカウントの同期を実行し、プロビジョニング サーバがアカウント属性の値を割り当てまたは変更できるようにします。

プロビジョニング サーバは、オブジェクトに対して次の 2 つの同期メニュー オプションのセットを用意しています。

- 同期のチェック メニュー オプションは、同期を確認し、プロビジョニング ロールに準拠していないアカウントまたはアカウント テンプレートのリストを返します。
- 同期メニュー オプションは、グローバル ユーザとそのプロビジョニング ロール、またはアカウントとそのアカウント テンプレートを同期させます。

同期のチェック機能を最初に実行すると、プロビジョニング サーバは、同期機能でどの修正を行うかを通知します。同期のチェック機能で問題が見つからなかった場合は、同期の機能を実行しません。

同期していないユーザが発生する理由

ユーザが、プロビジョニング ロールまたはアカウント テンプレートと同期しなくなっている理由として、以下が考えられます。

- 以前に必要なアカウントを作成しようとした際、ネットワークでのハードウェアまたはソフトウェアの問題が原因で失敗し、存在しないアカウントが生じています。
- プロビジョニング ロールおよびアカウント テンプレートが変更され、不要なアカウントまたは存在しないアカウントが生成されている可能性があります。
- アカウント テンプレートが作成された後にアカウントが割り当てられたため、アカウント テンプレートと同期していないアカウントが存在しています。
- アカウントを後で作成するよう指定されているため、新しいアカウントの作成が遅れています。
- 新しいエンドポイントが取得されました。検索および関係付けの際、プロビジョニング サーバはプロビジョニング ロールをユーザに自動的に割り当てません。したがって、ロールを更新して、新しいエンドポイント上でどのユーザがアカウントを持つかを指定する必要があります。ユーザに関連付けられているアカウントは、ユーザの同期時に、不要なアカウントとしてリストされます。

- 既存のアカウントがユーザにコピーされることによってそのアカウントがユーザに割り当てられ、それによって手動での関連付けが行われ、不要なアカウントが生じています。
- ユーザをロールに割り当てる以外の方法で、ユーザに対してアカウントが作成されました。たとえば、あるユーザのどのプロビジョニングロールにもないアカウントテンプレートにそのユーザをコピーすると、そのアカウントは、不要なアカウント、または不要なアカウントテンプレートを持つアカウントとしてリストされます。このユーザをあるエンドポイントにコピーし、そのエンドポイントのデフォルトアカウントテンプレートを使用してアカウントを作成すると、そのアカウントは不要なアカウントになることがあります。

ユーザの同期

ユーザの同期は、ユーザに割り当てられているプロビジョニングロールに対してアカウントが準拠するように、アカウントを作成、更新、または削除します。したがって、管理者はネイティブツールを使用して管理エンドポイントでアカウントを追加または削除しているが、ユーザはプロビジョニングディレクトリを更新するためのエンドポイント再検索を行っていない場合には、実際には不要なアカウントまたは存在しないアカウントがあるにもかかわらず、ユーザ同期時には問題が検出されない場合があります。

ユーザとロールの同期

ユーザに対する同期チェックを行って、不要なアカウントまたはアカウントテンプレート、および存在しないアカウントをリスト表示させることができます。ユーザとロールとの同期をリクエストすると、プロビジョニングサーバは、そのユーザのプロビジョニングロールに必要とされるすべてのアカウントをユーザが持っていること、および、各アカウントが正しいアカウントテンプレートに属していることを確認します。

- このタスクでは、チェックボックスを選択してエンドポイント上にアカウントを作成することができます。ユーザのプロビジョニングロールで複数のアカウントテンプレートが同じアカウントを規定している場合、関連するすべてのアカウントテンプレートをマージすることによって、アカウントが作成されます。
- ユーザとロール同期時に、不要なアカウントを削除することもできます。ただし、自身のプロビジョニングロールでは必要ないアカウントを所有しているユーザには正当な理由があると判断される場合もあります。そのような場合は、この削除オプションを選択してはいけません。

削除されるアカウントが管理エンドポイント内にあり、そのエンドポイントに対してはアカウントの削除が無効になっている場合は、アカウントは実際には削除されません。

アカウントの作成

プロビジョニング ロールにはアカウント テンプレートが含まれており、アカウント テンプレートはエンドポイントに関連付けられているため、ユーザは、正しいアカウント属性を持つ各エンドポイントについてリストされているアカウントを持っていなければなりません。

このタスクでは、チェック ボックスを選択してエンドポイント上にアカウントを作成することができます。ユーザのプロビジョニング ロールで複数のアカウント テンプレートが同じアカウントを規定している場合、関連するすべてのアカウント テンプレートをマージすることによって、アカウントが作成されます。

このアカウントは、これらのアカウント テンプレートに割り当てられますが、これらのテンプレートは、現在のところアカウントと同期していません。新しく作成されたアカウントでは、アカウントの同期は必要ありません。

アカウントの削除

ユーザとロール同期時に、不要なアカウントを削除することもできます。ただし、自身のプロビジョニング ロールでは必要ないアカウントを所有しているユーザには正当な理由があると判断される場合もあります。そのような場合は、この削除オプションを選択してはいけません。

削除されるアカウントが管理エンドポイント内にあり、そのエンドポイントに対してはアカウントの削除が無効になっている場合は、アカウントは実際には削除されません。

アカウントに対するアカウント テンプレートの追加

あるアカウントに、割り当てられていないアカウント テンプレートが 1 つ以上ある場合は、ユーザとアカウント テンプレートの同期により、既存のアカウントがこれらのアカウント テンプレートに割り当てられます。1 つのアカウントが、1 つ以上の新しいアカウント テンプレートに割り当てられると、アカウント同期が自動的に実行され、アカウントの機能属性が、アカウント テンプレートで指定されている機能に更新されます。

ユーザとアカウントテンプレートの同期によってアカウントが更新された後、そのアカウントはアカウントテンプレートと同期している場合もそうでない場合もあります。追加されたアカウントテンプレートの1つが強い同期のアカウントテンプレートであるか、または1つのアカウントに対して複数のアカウントテンプレートが追加されている場合、ユーザとロールの同期は、そのアカウントに対してフルアカウント同期を開始します。しかし、弱い同期のアカウントテンプレートが1つだけ追加された場合は、ユーザとアカウントテンプレートの同期は、この1つのアカウントテンプレートのみを含むアカウント同期を開始します。更新の前に、アカウントがすでに他のアカウントテンプレートとのアカウント同期とずれてしまった場合は、それ以降も、アカウント同期とずれることがあります。

アカウントからのアカウントテンプレートの削除

ユーザとロールの同期は、アカウントから不要なアカウントテンプレートを削除するために使用することもできます。これは、削除オプションを選択した場合のみ行われます。ユーザ同期で、あるアカウントを更新して1つ以上の不要なアカウントテンプレートを削除する必要があると判断した場合は、そのアカウントでアカウント同期が自動的に実行され、機能属性と、対象のアカウント上の残りのアカウントテンプレートが同期されます。

このアカウント同期は、アカウントからアカウントテンプレートを削除するときに発生します。残りのアカウントテンプレートのいずれかが強い同期に対してマークされている場合は強い同期を使用し、残りのアカウントテンプレートのすべてが弱い同期に対してマークされている場合は弱い同期を使用します。

弱い同期と強い同期のどちらが使用されているかによって、アカウントテンプレートがアカウントに割り当てられたときに以前に付与されたアカウント属性が、そのアカウントテンプレートが後で削除されたときに消去されるかどうか異なります。強い同期を使用している場合、アカウントテンプレートによって付与された機能（グループメンバシップや、より多くのクォータなど）は、対象のアカウント上の残りのアカウントテンプレートでこの機能を指示していなければ、消去されます（グループメンバシップが削除されるか、またはクォータが低減されます）。ただし、弱い同期の場合、通常はアカウントは変更されません。これは、プロビジョニングサーバでオンデマンドの特別な機能と、アカウントテンプレートによって付与された機能を区別しないからです。

`SyncRemoveValues` 属性として指定されている、いくつかの複数値の機能属性は、このルールが当てはまりません。アカウントに割り当てられた値のコレクションを表記している、単一の複数値属性（グループメンバシップのリストなど）は通常、`SyncRemoveValues` 属性としてリストされます。これらの属性では、アカウントからアカウントテンプレートを削除するときに発生する弱い同期アクションによって、削除中のアカウントテンプレートで指示されていた値が（残りのアカウントテンプレートのいずれかによって指示されていないければ）削除されます。

たとえば、複数のアカウントテンプレートを作成し、各アカウントテンプレートがアカウントに対して一意のグループメンバシップを割り当てている場合には、この **SyncRemoveValues** 機能は、「特別なアカウントテンプレートが不要になるよう、グローバルユーザのプロビジョニングロールを変更した場合、そのアカウントテンプレートで指示されたグループに属さないようアカウントも更新される」ことを意味します。アカウントテンプレートに規定されている内容に優先して、アカウントに対して指示されたグループメンバシップが保持されるため、これは強い同期とまったく同じではないことがわかるでしょう。

単一値のすべての属性、および **SyncRemoveValues** 属性として指定されていないいくつかの複数值属性では、アカウントからアカウントテンプレートを削除するときの、弱い同期アクションは、通常の弱い同期アクションと同じになり、機能は削除されません。

弱い同期によって機能を削除したくない場合は、ドメイン設定パラメータ **Synchronize/Remove Account Template Values from Accounts** を [いいえ] に設定して、**SyncRemoveValues** 機能を無効にします。

アカウントテンプレートの同期

アカウントテンプレートに対して行った変更は、既存のアカウントに次のように影響します。

- 機能属性の値を変更すると、対応するアカウント属性が更新され、必要に応じてアカウントテンプレートの属性値と同期されます。弱い同期と強い同期の説明を参照してください。
- 一部のアカウント属性は、コネクタにより、アカウントテンプレートの変更時には更新されないように指定されています。例としては、エンドポイントタイプがアカウント作成時にのみ設定することができる属性や、パスワード属性があります。

更新対象となる属性

アカウントテンプレートで機能属性を変更すると、アカウント上の対応する属性が変更されます。この変更はアカウントの属性に影響を及ぼします。影響は以下の要因に基づきます。

- アカウントテンプレートが弱い同期で定義されているか強い同期で定義されているか
- アカウントが複数のアカウントテンプレートに属しているかどうか

弱い同期

*弱い同期*では、ユーザのアカウントに対する最小の機能属性だけをユーザが持つことが保証されます。大部分の種類のエンドポイントでは、弱い同期がデフォルトです。弱い同期を使用するテンプレートを更新する場合、CA Identity Manager は以下のように機能属性を更新します。

- アカウント テンプレートで数値フィールドが更新されていて、新しい数値がアカウントの数値より大きい場合、新しい数値に合うようにアカウントの値が変更されます。
- 選択されていなかったチェックボックスをアカウント テンプレートで選択すると、そのチェックボックスが選択されていないすべてのアカウントでチェックボックスが更新されます。
- アカウント テンプレートで一覧を変更すると、アカウントの値の一覧になかった新しい一覧の値が収まるようにすべてのアカウントが更新されます。

1つのアカウントが他の複数のアカウント テンプレートにも属している場合、強い同期であれ弱い同期であれ、変更のあるテンプレートだけが参照されます。この方がすべてのアカウント テンプレートを検証するより効率的です。弱い同期ではアカウントに機能が追加されるだけなので、これら他のアカウント テンプレートを参照する必要は通常はありません。

注: 弱い同期アカウント テンプレートから伝達された変更が機能の削除や低減を行うものであった場合、一部のアカウントが非同期のままになることがあります。弱い同期では機能の削除や低減は決して行われなことに注意してください。アカウントの他のテンプレートが参照されないので、弱い同期で十分かどうかがこの伝達では考慮されません。

この状況では、アカウントをそのアカウント テンプレートと同期するには [ユーザとアカウント テンプレートの同期] を使用します。

強い同期

強い同期により、アカウント テンプレートで指定されているものと同じアカウント属性をアカウントが持っていることが保証されます。

たとえば、既存の **UNIX** アカウント テンプレートにグループを追加するとします。最初に、アカウント テンプレートでは **Staff** グループのアカウント メンバを作成しました。次に、**Staff** グループと **System** グループの両方のアカウント メンバを作成します。このアカウント テンプレートに関連付けられているすべてのアカウントは、それぞれのアカウントが **Staff** グループおよび **System** グループのメンバである場合（および他のいずれのグループでもない場合）、同期されているとみなされます。 **Staff** グループに含まれていないすべてのアカウントは、両方のグループに追加されます。

その他にも、以下の状況を考慮する必要があります。

- アカウント テンプレートで強い同期を使用している場合、**Staff** および **System** 以外のグループに属しているアカウントは、これらの追加グループから除外されます。
- アカウント テンプレートで弱い同期を使用している場合、アカウントは **Staff** グループおよび **System** グループに追加されます。他のグループが定義されているアカウントは、そのグループのメンバのままになります。

注: アカウントとアカウント テンプレートを定期的に同期することにより、アカウントおよびそのアカウント テンプレートの同期が確実に保たれます。

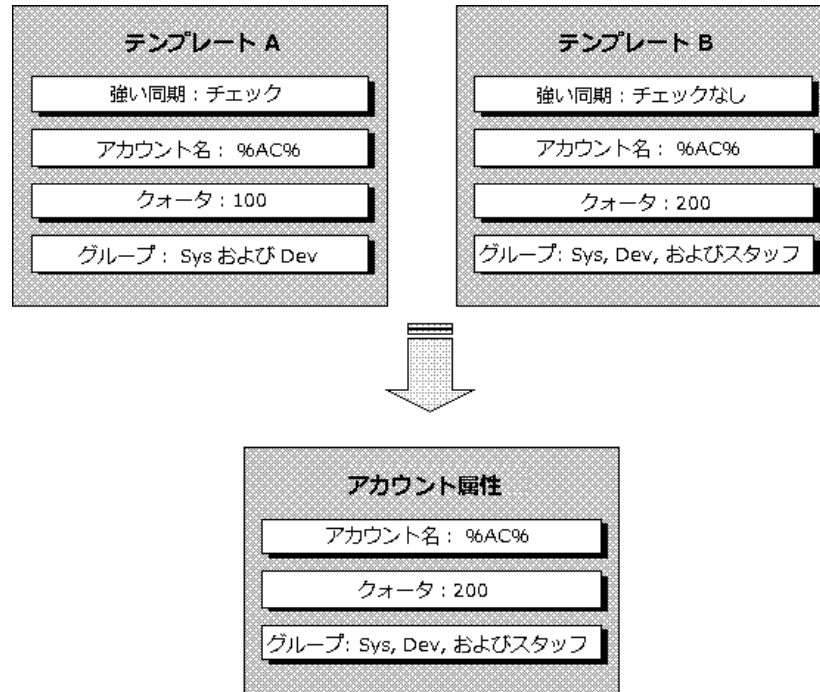
複数のテンプレートを持つアカウント

同期は、アカウントが複数のアカウント テンプレートに属しているかどうかによっても異なります。 アカウントがアカウント テンプレートを 1 つのみ持ち、そのテンプレートの同期が強い場合、各属性は、アカウント テンプレート属性値の評価対象に正確に一致するように更新されます。その結果、属性は最初の属性と同じ値になります。

ユーザが複数のプロビジョニング ロールに属し、それぞれのロールが同じ管理対象エンドポイントに対して一定のレベルのアクセス権を持つ場合、アカウントは複数のアカウント テンプレートに属する場合があります。この状態になると、**CA Identity Manager** はこれらのアカウント テンプレートを 1 つの有効なアカウント テンプレートにまとめ、個々のアカウント テンプレートの機能を合わせた上位集合として規定します。個々のアカウント テンプレートすべての同期が弱い場合、アカウント テンプレート単体は弱い同期となりますが、アカウント テンプレートのうち強い同期を持つものが 1 つでもあると、強い同期となります。

注: アカウント テンプレートが 1 つのアカウントのみを制御している場合、弱い同期のみまたは強い同期のみを使用することが多いです。これは、ユーザに必要なアクセス権を企業のロールが完全に定義しているかどうかによって決まります。ユーザのロールが明確でなく、ユーザのアカウントに柔軟に対応する必要がある場合、弱い同期を使用します。ユーザに必要なアクセス権を明確に指定するロールを定義する場合、強い同期を使用します。

以下の例は、複数のアカウントテンプレートが1つの有効なアカウントテンプレートにまとめられる方法を示します。この例では、1つのアカウントテンプレートが弱い同期としてマークされ、もう一方のテンプレートが強い同期としてマークされています。したがって、2つのアカウントテンプレートをまとめて作成された有効なアカウントテンプレートは、強い同期を持つアカウントテンプレートになります。整数を持つ **Quota** 属性は、2つのアカウントテンプレートから大きい方の値をとり、複数値を持つ **Groups** 属性は、2つのポリシーの値を合わせたものになります。



新しいアカウントだけの属性

アカウントテンプレートでは、一部の属性はアカウントの作成時のみに適用されます。たとえば、**Password** 属性は、新しいアカウントのパスワードを定義するルール表現です。このルール表現は、アカウントのパスワードを変更することはありません。パスワードルール表現への変更は、ルール表現が設定された後に作成されたアカウントだけに影響します。

同様に、読み取り専用アカウント属性のテンプレートルール表現は、ルール表現が設定された後に作成されたアカウントだけに影響します。変更は、既存のアカウントには何の影響ももたらしません。

アカウントの同期

アカウントの同期により、機能属性が更新され、アカウント テンプレートによって指定された機能をアカウントが確実に持つようになります。この同期は、アカウントの初期属性に影響しません。

アカウント テンプレートでの機能属性の変更をアカウントと同期するには、このセクションで説明した同期メニュー オプションの 1 つを使用します。

アカウント同期のチェック

エンドポイントとユーザのアカウント同期を確認することができます。この処理では、アカウント テンプレートに準拠していないアカウントのリストが返されます。次の表は、各オブジェクトでアカウントの同期をチェックしたときに、どのようなになるかを表しています。

オブジェクト	同期
エンドポイント	エンドポイント内の各アカウントに対するアカウント属性を同期し、関連付けられているアカウント テンプレートに確実に準拠するようにします。
グローバル ユーザ	各ユーザのアカウントに対するアカウント属性を同期し、関連付けられているアカウント テンプレートに確実に準拠するようにします。

アカウントの同期

エンドポイント、ユーザ、およびアカウント テンプレートに対してアカウント同期を実行できます。次の表に、各オブジェクトにおけるアカウントの同期の影響を示します。

オブジェクト	同期
エンドポイント	エンドポイントの各アカウントを、関連付けられているアカウント テンプレートと同期する。
グローバル ユーザ	グローバル ユーザの各アカウントを、関連付けられているアカウント テンプレートと同期する。

第 12 章: ワークフロー

このセクションには、以下のトピックが含まれています。

[ワークフローの概要](#) (P. 277)

[ワークフロー コントロールの使用 - テンプレート メソッド](#) (P. 280)

[WorkPoint メソッドの使用法](#) (P. 302)

[Workpoint ジョブの表示](#) (P. 335)

[ポリシーベース ワークフロー](#) (P. 337)

[オンラインリクエスト](#) (P. 357)

[Workflow Action Buttons \(ワークフロー アクション ボタン\)](#) (P. 361)

[ワーク リストと作業アイテム](#) (P. 366)

ワークフローの概要

CA Identity Manager ワークフロー機能では、ワークフロー プロセスで CA Identity Manager タスクを制御することができます。ワークフロー プロセスは、CA Identity Manager がワークフロー制御下のタスクを完了するまでに実行する必要のある 1 つ以上の手順です。ジョブとは、ワークフロー プロセスのランタイム インスタンスを指します。

WorkPoint Designer は、Planet Group, Inc の一部門である Workpoint LLC 製作のソフトウェアで、CA Identity Manager に統合されています。WorkPoint Designer では、ワークフロー プロセスおよびワークフロー ジョブを管理できます。

ワークフロー プロセスは、アクティビティと呼ばれる 1 つ以上のプロセスで構成されており、従業員ユーザ アカウントの作成や変更といったビジネス タスクを遂行するために実行する必要があります。通常、ワークフロー プロセスには、タスクの承認または拒否を行うために、権限を持つユーザまたは参加者が必要となる手動アクティビティが 1 つ以上含まれています。

参加者は、ワークフロー アクティビティを実行する権限を持つ個人です。CA Identity Manager では、ワークフロー制御下のタスクを承認または拒否する必要があります。参加者は承認者と呼ばれることもあります。参加者リゾルバは、参加者を決定するルールまたは基準のセットです。

ワークフローの個別の手動アクティビティは、CA Identity Manager では作業アイテムと呼ばれます。

ワーク リストは、ワークフローが生成する許可タスク (作業アイテム) のリストであり、このタスクを承認する権限を持つ参加者のユーザ コンソールに表示されます。

WorkPoint プロセス図

通常、CA Identity Manager タスクは CA Identity Manager イベントをトリガします。たとえば、ユーザを作成するために、管理者が「ユーザの作成」タスクを選択します。このタスクが開始されると、イベント **CreateUserEvent** がトリガされます。

以下の図は、WorkPoint Designer に表示される、単純なワークフロー プロセス（事前定義済みのプロセス **CreateUserApproveProcess**）の例です。「ユーザの作成」タスクがワークフロー制御下にある場合、このプロセスは **CreateUserEvent** により起動されます。

このプロセスには、手動アクティビティ「ユーザ作成を承認」が含まれています。これは、同じ名前である CA Identity Manager ワークフロー承認タスクに対応します。参加者は、ワークフロー制御下のタスクの実行が完了するまでに、通常、ユーザ コンソールのボタンをクリックして承認タスクを承認または拒否する必要があります。

ワークフローと電子メール通知

タスクを開始すると、CA Identity Manager は処理のためにタスクをサブミットします。タスクが終了すると、以下のように確認メッセージが表示されます。

確認： タスクが完了しました。

ただし、このタスクがワークフロー制御下にあり、承認が必要な場合は、このメッセージは以下のようになります。

アラート： タスクはペンディングです。

画面上のメッセージに加えて、以下の場合に CA Identity Manager により電子メール通知が自動的に生成されます。

- ワークフロー承認者による承認または拒否が必要なイベントまたはタスクが保留中である場合
- 承認者がイベントまたはタスクを承認する場合
- 承認者がイベントまたはタスクを拒否する場合
- イベントまたはタスクが完了した場合

詳細情報：

[電子メール通知](#) (P. 379)

WorkPoint のマニュアル

ワークフローの概念の一般的な情報、および **WorkPoint Designer** でのワークフロープロセス、アクティビティ、およびジョブの詳細については、**WorkPoint** のマニュアルを参照してください。このマニュアルを参照するには、以下の HTML ページを開きます。

`admin_tools¥WorkPoint¥docs¥designer¥default.htm`

admin_tools

CA Identity Manager 管理ツールのインストールディレクトリを決定します。デフォルトのインストールディレクトリは以下のとおりです。

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

注: Workpoint は、**CA Identity Manager** でインストールされるサードパーティ製品です。**CA Identity Manager** は、**WorkPoint** の機能のサブセットをサポートしています。たとえば、**CA Identity Manager** は **WpConsole** をサポートしていません。ただし、**WorkPoint** ドキュメントでは、この製品の機能がすべて説明されます。**Workpoint** ドキュメントの一部は、**CA Identity Manager** ユーザには適用されません。

Workflow の制御メソッド

CA Identity Manager には、ワークフロー制御下でタスクを配置するのに 2 つのメソッドがあります。

テンプレート メソッド

CA Identity Manager には、ワークフロー制御下にタスクを配置するのに使用できるワークフロープロセス テンプレートがあります。テンプレートメソッドでは、テンプレートを使用して、ユーザ コンソール内のワークフローをすべて設定および管理できます。**CA Identity Manager r12** に導入された、こうした一般的なプロセス テンプレートを設定すると、ほとんどの **CA Identity Manager** のタスクとイベントを制御できます。

テンプレートメソッドは以下のような新しい機能を有効にします。

- タスク レベルとイベント レベル両方のワークフロー制御
- ワークフロー承認者の参加者リゾルバ設定の簡略化

- 作業アイテムの委任。これにより、ユーザが別のユーザに作業アイテムの承認を委任することが可能となり、「外出中」のシナリオに対応できます。
- 作業アイテムの再割り当て。これにより、実行中のタスクを承認のため別のユーザに再度割り当てることができます。

WorkPoint メソッド

CA Identity Manager には、特定の CA Identity Manager タスクに対応するデフォルトのイベント マッピングを含む事前定義済みのワークフロー プロセスのセットがあります。WorkPoint メソッドでは、WorkPoint Designer 内でこれらのプロセスの設定およびカスタマイズを行う必要があります。これらの事前定義済みのプロセスは、CA Identity Manager r12 より前のリリースと互換性があります。

WorkPoint メソッドは以下のような新しい機能も有効にします。

- タスク レベルとイベント レベル両方のワークフロー制御
- 作業アイテムの委任。これにより、ユーザが別のユーザに作業アイテムの承認を委任することが可能となり、「外出中」のシナリオに対応できます。
- 作業アイテムの再割り当て。これにより、実行中のタスクを承認のため別のユーザに再度割り当てることができます。

注: 柔軟性と使い勝手の向上のため、できるだけテンプレート メソッドを使用することをお勧めします。

詳細情報:

[ワークフロー コントロールの使用 - テンプレート メソッド \(P. 280\)](#)

ワークフロー コントロールの使用 - テンプレート メソッド

CA Identity Manager r12 に導入されたテンプレート メソッドでは、WorkPoint Designer を開かずに、ユーザ コンソールでワークフロー プロセス テンプレートを設定できます。

テンプレート メソッドの利点は以下のとおりです。

- 複数の段階のプロセス テンプレートにより、ほとんどのワークフロー ニーズに対応できます。WorkPoint Designer 内でのカスタマイズは不要です。
- テンプレートでは、タスク レベルとイベント レベル両方のワークフロー制御をサポートします。

- 同じワークフロー プロセス テンプレートは、プロセス デザイン自体は変更することなく、多くのさまざまなタスクに使用できるように設定できます。
- 参加者リゾルバは、ユーザ コンソールで簡単に指定できます。
- 作業アイテムの委任をユーザ コンソールで実行できます。

前提条件: ワークフローの有効化

ワークフローを使用して **CA Identity Manager** タスクを制御する前に、ワークフローを有効にする必要があります。デフォルトでは、ワークフローは無効になっています。

次の手順に従ってください:

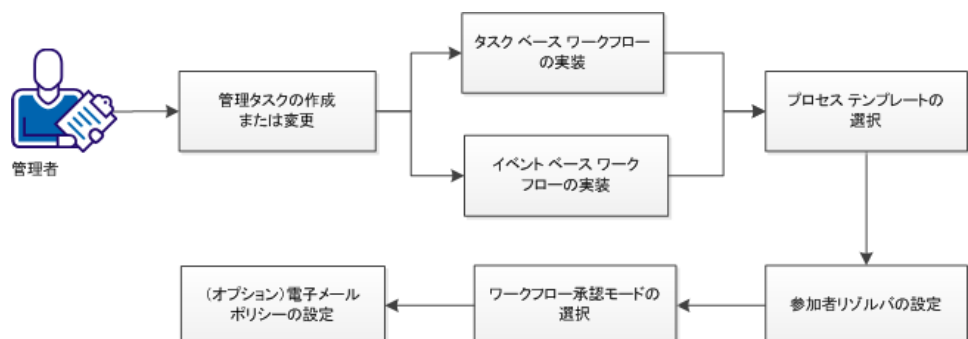
1. 管理コンソールで [環境] を選択します。
2. [詳細設定] - [ワークフロー] の順に進みます。
3. [有効] チェック ボックスをオンにし、[保存] をクリックします。

注: この画面のイベント マッピングは、**WorkPoint** メソッドを使用してワークフローを設定している場合のみ適用されます。テンプレート メソッド (推奨) を使用する場合は、この管理コンソールを使用してイベントをマッピングして処理しないでください。

4. アプリケーション サーバを再起動します。
5. (オプション) [WorkPoint 管理ツールを設定](#) (P. 303) します。

ワークフロー制御 - テンプレート メソッドの下に管理タスクを配置します。

管理者は、テンプレート メソッドを使用したワークフロー制御下に管理タスクを配置できます。



次の手順に従ってください:

1. ユーザ コンソールで、[ロールおよびタスク] - [管理タスク] - [管理タスクの変更] または [管理タスクの作成] を選択します。
2. ワークフロー制御下で実行するタスクを検索して、[選択] をクリックします。
3. 以下のいずれかの操作を行います。
 - [タスク レベルのワークフローを実装します \(P. 283\)](#)。そのためには、[プロファイル] タブ上で [ワークフロー プロセス] 編集ボタンをクリックします。
 - [イベント レベルのワークフローを実装します \(P. 286\)](#)。そのためには、[イベント] タブで 1 つ以上のイベントを選択します。
4. [プロセス テンプレートを選択します \(P. 289\)](#)。
5. [参加者リゾルバを設定します \(P. 293\)](#)。
6. ワークフロー承認モードを選択します。
7. (オプション) [ワークフロー プロセスに対して電子メール ポリシーを設定します \(P. 299\)](#)。

注: EscalationApproval プロセスを選択した場合、[承認のタイムアウト (分)] という名前のフィールドが表示されます。このフィールドは分数で特定され、入力必須です。デフォルトでは、時間は 60 分に設定されています。

ワークフロー制御が設定されたら、適切なロールを持つユーザが管理タスクを実行した場合、指定のワークフロー参加者がタスク/イベントを承認または拒否します。

タスク/イベント ベースのワークフロー

CA Identity Manager では、ワークフロー プロセスをタスクまたはイベントのいずれかに関連付けることができます。これは、参加者が CA Identity Manager のタスク全体またはタスク内の特定のイベントのいずれかを承認または拒否できることを意味します。

たとえば、CA Identity Manager のタスクが複数のイベントを生成するため、承認者がリクエストの承認または拒否を決定する前にすべてのイベントを確認する必要がある場合があります。これは、タスク レベルのワークフローで実行可能です。ワークフロー プロセスが特定のイベントに関連付けられている場合、承認者は、リクエストが行われたタスク全体の状況を確認できません。

タスクレベルのワークフロー

タスク レベルのワークフローでは、承認者がリクエストの承認または拒否を決定する前にすべてのイベントを確認できます。タスク レベルのワークフローは、タスク アクティビティが処理される前に発生します。ワークフロー プロセス ジョブが開始するまで、イベントまたはネストされたタスクは実行されません。

タスク レベルのワークフローが拒否されると、タスクのいずれの部分も実行されません。

注: タスク レベルのワークフロー制御で設定されたタスクは、イベント レベルのワークフロー制御にも同時に設定することができます。同時に設定可能なイベント レベルのワークフローは、全体に適用することも、特定のタスクに適用することもできます。

タスクレベルのプロセス属性

タスク レベルのワークフローと互換性があるワークフロー プロセスはすべて、**WorkPoint Designer** 内で定義された特別な属性があります。TASK_LEVEL と呼ばれるこのプロセス レベルのユーザ データ属性は、以下のプロセス テンプレートではデフォルトで **true** に設定されます。

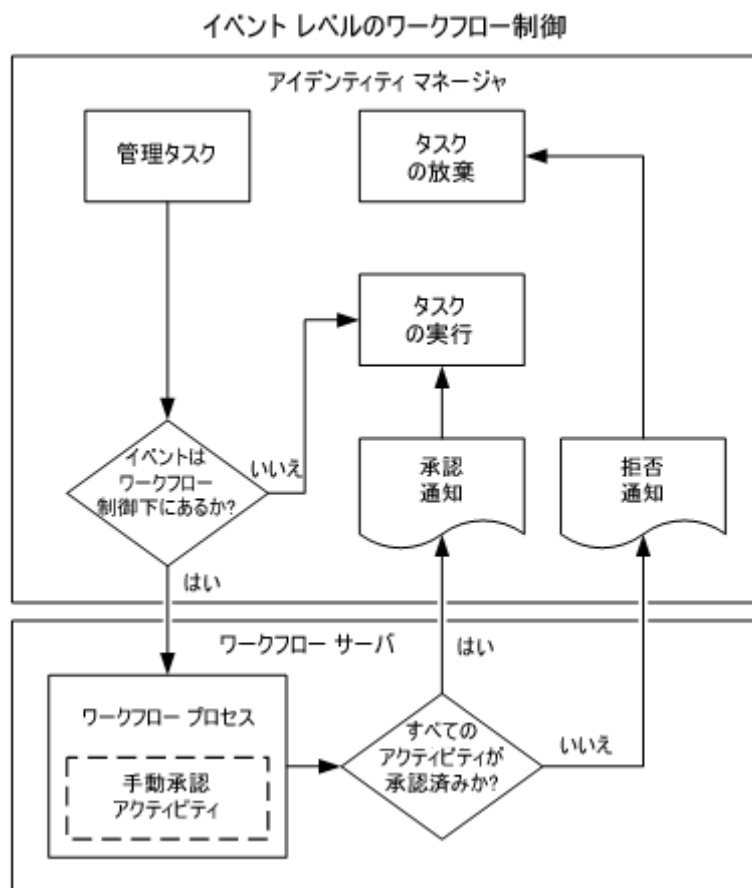
- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

タスク レベルのワークフローの管理タスクを選択すると、上記のプロセス テンプレートのみが使用できます。

注: TASK_LEVEL が **true** に設定されている場合でも、イベント レベルのワークフローでプロセス テンプレートを使用できます。この TASK_LEVEL の属性値を変更しないでください。

タスクレベル制御の図

以下の図は、一般的なタスク レベルのワークフロー プロセスが開始されたときの CA Identity Manager とワークフロー サーバの間の対話を示しています。



詳細情報:

[イベント レベル制御の図](#) (P. 287)

タスクレベルのワークフローの設定方法

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

非ポリシー ベースのタスクレベル ワークフローを設定する方法

1. ユーザ コンソールで、[ロールおよびタスク] - [管理タスク] - [管理タスクの変更] または [管理タスクの作成] を選択します。
[管理タスクの選択] 画面が表示されます。
2. ワークフロー制御下で実行するタスクを検索して、[選択] をクリックします。
[管理タスクの変更] または [管理タスクの作成] 画面が表示されます。
3. [プロファイル] タブで、[ワークフローの有効化] がチェックされているかどうかを確認します。
4. [プロファイル] タブで、[ワークフロー プロセス] ボタンをクリックします。
[タスク レベル ワークフロー設定] タブが表示されます。
5. [ワークフロー プロセス] リストから、以下のプロセス テンプレートのいずれかを選択します。
 - SingleStepApprovalProcess
 - TwoStageApprovalProcess
 - EscalationApprovalProcess
[タスク レベル ワークフロー設定] タブが展開されます。
6. プロセス テンプレートで必要に応じて参加者リゾルバを設定します。
参加者のリクエストがプロセスに追加されます。
7. [OK] をクリックします。
CA Identity Manager によってタスク レベルのワークフロー設定が保存されます。
8. [サブミット] をクリックします。
CA Identity Manager によってタスクの変更が処理されます。

注: ポリシー ベースのタスク レベル ワークフローを設定するには、[「ポリシー ベース ワークフロー」](#) (P. 337)を参照してください。

イベントレベルのワークフロー

イベントは、ワークフロー プロセスにマッピングすることができます。ワークフロー プロセスにマッピングしたイベントがトリガされると、ワークフロー プロセスが開始します。イベントをトリガしたタスクは保留状態になり、ワークフローの制御下に置かれます。

ワークフロー プロセスでは、プロセスが完了する前に参加者がイベントやタスクを承認または拒否する必要がある場合があります。参加者による手動のワークフロー承認が必要なタスクは、ワークフロー制御下のタスクよりも完了するまでに時間がかかります。

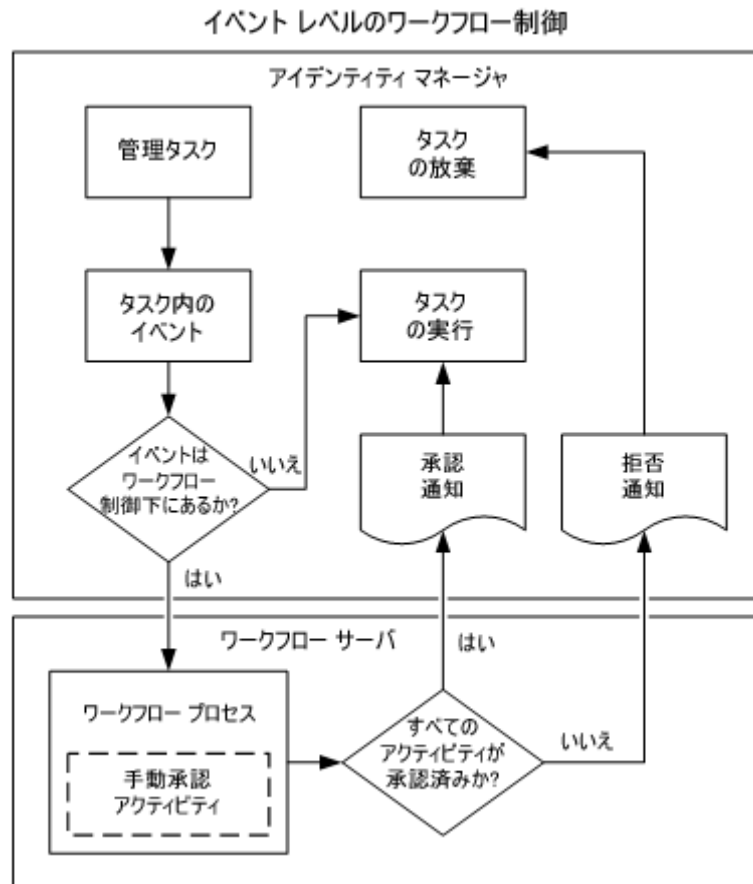
ワークフロー プロセスのすべてのアクティビティが実行されると、そのワークフロー プロセスにマッピングされたイベントはワークフロー制御から解放されます。特定のタスクでトリガされたすべてのイベントがワークフロー制御から解放されると、ワークフローで制御されているタスクが完了します。

タスクがワークフロー制御下にある場合は、タスク画面の内容はタスクの持続的なデータベースに保存されます。ワークフロー ジョブの状態（ワークフロー関連のデータ）は **WorkPoint** データベースに保存されます。

注： [イベント] タブでは、タスクの各タブで生成されたイベントを一覧で表示します。タスクに新しいタブを追加した後、[イベント] タブに新しいイベントが表示される前に、[管理タスクの変更] を使用してタスクをサブミットし再開する必要があります。

イベント レベル制御の図

以下の図は、一般的なイベント レベルのワークフロー プロセスが開始されたときの CA Identity Manager とワークフロー サーバの間の対話を示しています。



詳細情報:

[タスク レベル制御の図](#) (P. 284)

イベントレベルのワークフローの設定方法

ワークフロー プロセスにマッピングされるイベントがトリガされると、イベントレベルのワークフローが開始します。イベントをトリガしたタスクは、参加者がタスクを承認または拒否するまで保留状態に置かれます。

非ポリシー ベースのイベントレベル ワークフローを設定する方法

1. ユーザ コンソールで、[ルールおよびタスク] - [管理タスク] - [管理タスクの変更] または [管理タスクの作成] を選択します。
[管理タスクの選択] 画面が表示されます。
2. ワークフロー制御下で実行するタスクを検索して、[選択] をクリックします。
[管理タスクの変更] または [管理タスクの作成] 画面が表示されます。
3. [プロファイル] タブで、[ワークフローの有効化] がチェックされているかどうかを確認します。
4. [イベント] タブで、イベントを選択して、プロセス テンプレートにマッピングします。
ワークフローのマッピングの画面が表示されます。
5. [ワークフロー プロセス] リストから、以下のプロセス テンプレートのいずれかを選択します。
 - SingleStepApproval
 - TwoStageApprovalProcess
 - EscalationApprovalProcessワークフローのマッピングの画面が展開されます。
6. プロセス テンプレートで必要に応じて参加者リゾルバを設定します。
参加者のリクエストがプロセスに追加されます。
7. [OK] をクリックします。
CA Identity Manager によってイベント レベルのワークフロー設定が保存されます。
8. ワークフロー制御下に置くイベントごとに手順 3 から 6 を繰り返します。
9. [サブミット] をクリックします。
CA Identity Manager によってタスクの変更が処理されます。

ポリシー ベースのイベント レベル ワークフローを設定するには、[「ポリシー ベース ワークフロー」](#) (P. 337)を参照してください。

注: ワークフロー プロセス リストには、テンプレート メソッドと **WorkPoint** メソッドの両方で使用するプロセスが含まれています。

- テンプレート メソッド プロセス (**SingleStepApproval**、**TwoStageApprovalProcess** または **EscalationApproval** のいずれか) が選択されると、ページが展開されて、参加者リゾルバの設定が有効になります。
- **WorkPoint** メソッド プロセスが選択されているとき、ページは展開しません。参加者リゾルバは **WorkPoint Designer** で設定されます。

プロセス テンプレートのタイプ

ワークフロー プロセス テンプレートには以下の特徴があります。

- **WorkPoint Designer** で定義される。
- 手動アクティビティであり、**CA Identity Manager** の承認タスクに対応する。
- 参加者 (承認者とも呼ばれる) を識別する情報を含む特別な属性が含まれている。

ワークフロー プロセス テンプレートには、特定の参加者を選択する情報は含まれていません。これは、ユーザがワークフローおよびワークフローの参加者リゾルバを設定した後に **CA Identity Manager** によって提供されます。この情報は、イベント レベルのワークフロー制御のイベント、およびタスク レベルのワークフロー制御のタスクにマッピングされます。

テンプレート メソッドを使用すると、ワークフローおよび参加者の設定はすべてユーザ コンソール内で行われます。

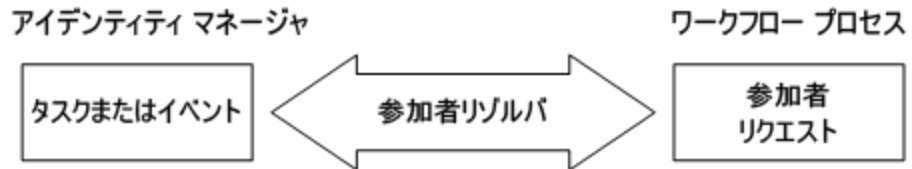
テンプレート メソッドを使用するプロセス テンプレートは以下の 3 つがあります。

- **SingleStepApprovalProcess**
- **TwoStageApprovalProcess**
- **EscalationApprovalProcess**

プロセス テンプレートの動作方法

ワークフロー プロセス テンプレートには、参加者リストが必要となる場所が多く含まれています。テンプレートが **CA Identity Manager** のタスクまたはイベントにマッピングされると、これらのリストの参加者リゾルバを設定します。

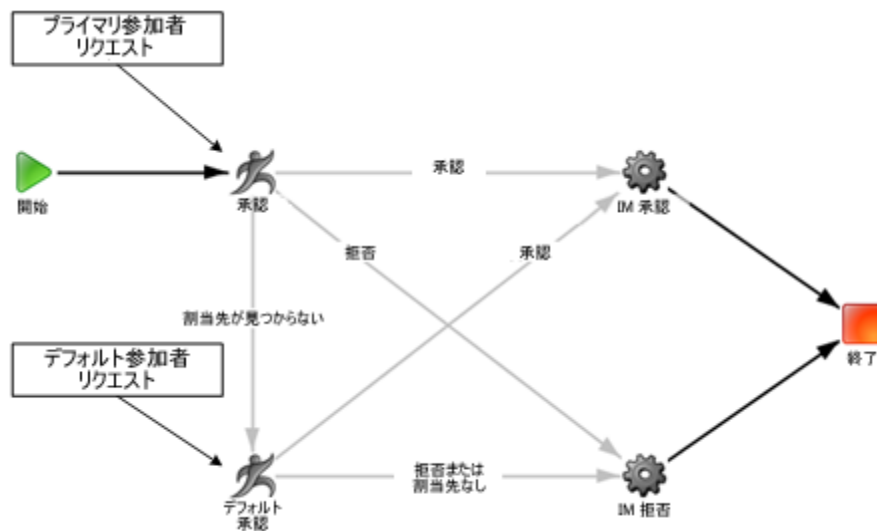
実行時には、以下の図に示すように、設定情報に基づく参加者リストが CA Identity Manager によりワークフロー プロセスに表示されます。



1 つの段階のテンプレートの図

以下の図は、WorkPoint Designer に表示される、SingleStageApproval プロセス テンプレートを示しています。プロセス テンプレートには、以下の 2 つの手動アクティビティがあります。

- プライマリ参加者の承認ノード。このユーザがリクエストを承認または拒否すると、プロセスを実行して完了します。
- デフォルト参加者の承認ノード。プライマリ参加者が見つからない場合に、このユーザはリクエストを承認または拒否できます。

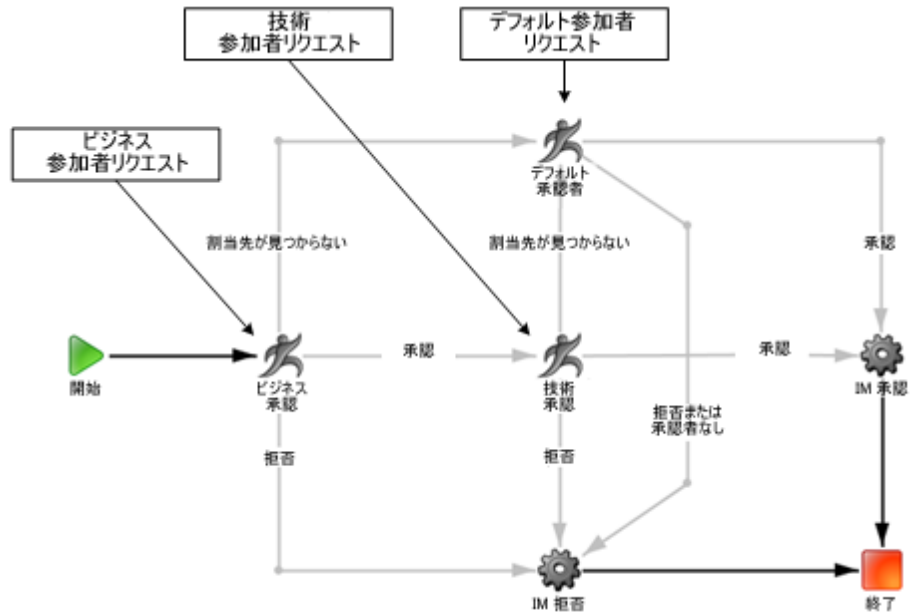


2 つの段階のテンプレートの図

以下の図は、WorkPoint Designer に表示される、TwoStageApproval プロセス テンプレートを示しています。TwoStageApproval プロセス テンプレートには、以下の 3 つの手動アクティビティがあります。

- ビジネス参加者の承認ノード。このユーザがリクエストを承認すると、技術系承認者によるプロセスに進みます。このユーザがリクエストを拒否すると、プロセスは完了します。

- 技術参加者の承認ノード。このユーザがリクエストを承認または拒否すると、プロセスを実行して完了します。
- デフォルト参加者の承認ノード。ビジネス参加者または技術参加者が見つからない場合に、このユーザはリクエストを承認または拒否できます。

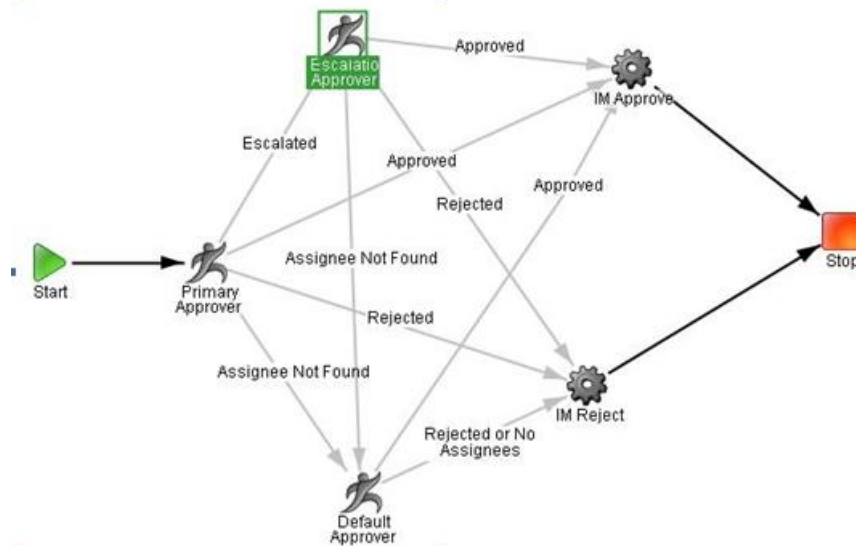


エスカレーション承認のテンプレート図

以下の図は、WorkPoint Designer に表示される、EscalationApproval プロセス テンプレートを示しています。プロセス テンプレートには、以下の手動アクティビティがあります。

- プライマリ参加者の承認ノード。このユーザがリクエストを承認または拒否すると、プロセスを実行して完了します。
- デフォルト参加者の承認ノード。プライマリ参加者が見つからない場合に、このユーザはリクエストを承認または拒否できます。

- プライマリ承認者からエスカレーション承認者への、時間制トランジション承認ノード。このユーザは、プライマリ参加者が見つかったものの、設定されたタイムアウト期間に応答しない場合、リクエストを承認または拒否できます。



注: 既存のプロセスにタイムアウト オプションを追加するには、アクティビティ ノードにユーザ データ フィールド [PARTICIPANT_TIMEOUT] を追加し、作業アイテムをエスカレーションする必要があるノードに「エスカレーション」 トランジションを追加します。

エスカレーション承認テンプレートの使用

エスカレーション承認テンプレートを使用するには、r12.5 から 12.6.4 へのアップグレード時に以下の zip ファイルをインポートします。

12.5to12.5SPUpgradeWFScripts.zip

ZIP ファイルはデフォルトでは以下のディレクトリにあります。

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

参加者リゾルバのタイプ

テンプレート メソッドでは、以下の 7 つのタイプの参加者リゾルバがあります。

承認タスク ロール メンバ

参加者は、承認タスクへのアクセス権が付与されるロールのメンバであることを指定します。

ユーザ リスト

参加者は、指定したユーザのリストであることを指定します。

グループ メンバ

参加者は、指定したグループのリストのメンバであることを指定します。

管理ロール メンバ

参加者は、指定した管理ロールのリストのメンバであることを指定します。

管理タスク メンバ

参加者は、指定した管理タスクのリストに関連付けられた管理ロールのメンバであることを指定します。

動的リゾルバ

参加者は、承認されるタスクまたはイベントに応じて動的に選択されることを指定します。

NULL リゾルバ

ユーザのいない null リストに解決します。

カスタム

カスタム参加者リゾルバによって、参加者が決定されることを指定します。

ビジネス所有者リゾルバ

カタログ ルールに設定された参加者のリストをエンティティのビジネス所有者として指定します。

管理者所有者リゾルバ

カタログ ルールに設定された参加者のリストをエンティティの管理者所有者として指定します。

マネージャリゾルバ

ユーザ オブジェクトのマネージャとして設定された参加者を指定します。

承認タスク ロール メンバ

このリゾルバは、承認タスクへのアクセス権が付与されるすべての **CA Identity Manager** ロールのすべてのメンバにアクティビティを割り当てます。このリゾルバには追加設定はありません。

ユーザ リスト

このリゾルバは、指定したユーザのリストに作業アイテムを割り当てます。

スコープは実施されません。ワークフロー設定画面へのアクセス権があれば、リストへのユーザの追加、またはリストからのユーザの削除を行うことができます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つのユーザ名を指定する必要があります。
- ユーザ名は、現在存在するユーザである必要があります。

グループ メンバ

このリゾルバは、グループ リスト内で指定したすべてのグループのすべてのメンバに作業アイテムを割り当てます。

グループ メンバの評価は、参加者リゾルバが指定されるときではなく、作業アイテムが作成されるときに実行されます。

スコープは実施されません。ワークフロー設定画面へのアクセス権があれば、リストへのグループの追加、またはリストからのグループの削除を行うことができます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つのグループ名を指定する必要があります。
- グループ名は、現在存在するグループである必要があります。

管理ロール メンバ

このリゾルバは、管理ロール リストで指定した管理ロールのメンバ全員に作業アイテムを割り当てます。

ロール メンバの評価は、参加者リゾルバの指定時ではなく、作業アイテムの作成時に実行されます。

スコープは実施されません。ワークフロー設定画面にアクセスできるユーザであれば、任意のロールをリストに追加したり、リストから任意のロールを削除することができます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つの管理ロールを指定する必要があります。
- 管理ロール名は、現存する管理ロールと同じにする必要があります。

管理タスク メンバ

このリゾルバは、管理タスク リストで指定した管理タスクに関連付けられた、すべての管理ロールのメンバ全員に作業アイテムを割り当てます。

スコープは実施されません。ワークフロー設定画面にアクセスできるユーザであれば、任意のタスクをリストに追加したり、リストから任意のタスクを削除することができます。

ロール メンバの評価とタスク上に存在するロールの評価は、参加者リゾルバの指定時ではなく、作業アイテムの作成時に実行されます。

このリゾルバには、以下の検証ルールがあります。

- 最低 1 つの管理タスクを指定する必要があります。
- 管理タスク名は、現存する管理タスクと同じにする必要があります。

動的リゾルバ

このリゾルバは、実行時に解決された動的ルールに従ってユーザ リストを返します。動的ルールの制約を設定するには、以下の選択内容を使用します。

承認者

このタスクを承認するユーザのタイプを指定します。

注: ここにはユーザ（または承認者）を含めることのできるオブジェクトのみが表示されます。

ユーザまたはオブジェクト

承認者が含まれているユーザまたはオブジェクトを指定します。

- このイベントに関連付けられるオブジェクト - ワークフロー制御下にあるイベント
- このタスクの開始ソース - 管理タスクを開始したユーザ
- このタスクのプライマリ オブジェクト - このタスクによって作成または変更されるユーザ
- このタスクの前の承認者 - このタスクの前の承認者

このアカウントに関連付けられているユーザ

「ユーザまたはオブジェクト属性」フィールドを更新して、エンドポイント アカウント属性の代わりに **CA Identity Manager** ユーザ属性をリストします。リゾルバは **CA Identity Manager** ユーザ レベルで属性をオフラインで作業します。**Active Directory** アカウントなどエンドポイント アカウント オブジェクトを選択すると、このチェックボックスが適用されます。

属性

承認者が含まれている属性を指定します。

注: 「属性」リストはアルファベット順に並べ替えられ、一意の表示名が含まれます。拡張された属性はリストから除外されています。

イベントオブジェクト タイプ

このイベントのオブジェクト タイプを指定します。

注: これは「このイベントに関連付けられるオブジェクト」を選択した場合にのみ表示されます。

注: 「グループの作成」で「動的リゾルバ」を使用するには、オブジェクトが存在する必要があります。グループ メンバシップや管理者の情報を動的リゾルバや一致属性リゾルバと共に使用できるのは、既存のグループの場合だけです。

動的リゾルバの機能が強化され、前の承認者をサポート対象オブジェクト リストに追加できるようになりました。マネージャ情報をホストしているフィジカル アトリビュートが選択された場合、設定は承認をマネージャに回覧します。

マネージャ承認リゾルバ用のリゾルバを設定するには、以下の手順に従います。

- 承認者をユーザに設定します
- [ユーザまたはオブジェクト] ドロップダウン リストから [このタスクの前の承認者] を選択します
- 属性をマネージャ情報を含むフィジカル アトリビュートに設定します

一致属性リゾルバ

このリゾルバは、タイプが「ユーザ」であるオブジェクトに対してのみ機能します。利用可能なオブジェクトからの値は、ユーザ オブジェクトのフィールドに対して一致します。一致する属性ルールの制約を設定するには、以下の選択内容を使用します。

承認者

このタスクを承認するユーザのタイプを指定します。

ユーザまたはオブジェクト

承認者が以下で選択された属性で持つ値を指定します。

注: ユーザまたはオブジェクトから取得された値は、ユーザの選択された属性の検索で許容できる値である必要があります。

- このイベントに関連付けられるオブジェクト - ワークフロー制御下にあるイベント
- このタスクの開始ソース - 管理タスクを開始したユーザ
- このタスクのプライマリ オブジェクト - タスクによって作成/変更されているタスク (タスク レベルのイベント マッピングにのみ利用できます)
- このタスクの前の承認者 - このタスクの前の承認者

このアカウントに関連付けられているユーザ

[ユーザまたはオブジェクト属性] フィールドを更新して、エンドポイント アカウント属性の代わりに **CA Identity Manager** ユーザ属性をリストします。リゾルバは **CA Identity Manager** ユーザ レベルで属性をオフラインで作業します。 **Active Directory** アカウントなどエンドポイント アカウント オブジェクトを選択すると、このチェック ボックスは適用されます。

ユーザまたはオブジェクト属性

承認者の検索で使用する値を含む属性を指定します。

承認者検索属性

上記で識別された値の検索に使用される属性を指定します。

注: [ユーザの作成を承認] タスクを、ユーザ、参加者リゾルバを操作する一致属性リゾルバとして設定する場合、**WorkPoint Designer** 上の **imApprovers** スクリプトのメソッド **シグネチャ** を、 **TwoStageProcessDefinition** の一意名をポイントするように変更する必要があります。

NULL リゾルバ

NULL リゾルバはユーザを返しません。ワークフロー プロセスの設計方法によっては、これによりプロセスで承認全体がスキップされる可能性があります。**NULL** リゾルバに関する詳しい設定は必要ありません。

カスタム参加者リゾルバ

カスタム参加者リゾルバは、ワークフロー アクティビティの参加者を決定し、リストを **CA Identity Manager** に返す **Java** オブジェクトです。**CA Identity Manager** は、このリゾルバから返されたリストをワークフロー エンジンに渡します。一般に、カスタム参加者リゾルバを作成するのは、標準の参加者ポリシーではアクティビティに必要な参加者のリストを提供できない場合のみです。

注: カスタム参加者リゾルバの作成には、参加者リゾルバ **API** を使用します。詳細については、「*Programming Guide for Java*」を参照してください。

[ワークフロー プロセス]に対して[電子メール ポリシー]を設定します

ワークフロー プロセスの各手順の電子メール ポリシーを指定できます。定義された電子メール ポリシーに基づき、プロセスが対応する手順またはアクティビティに到達すると、電子メールが送信されます。ワークフロー プロセスに関連する電子メール通知については、[送信のタイミング] タイプとして [ワークフロー 待ち電子メール] のみを選択できます。

注: 電子メール ポリシーの詳細については、「電子メール通知ポリシーの作成方法」を参照してください。

ワークフロー例: ユーザの作成

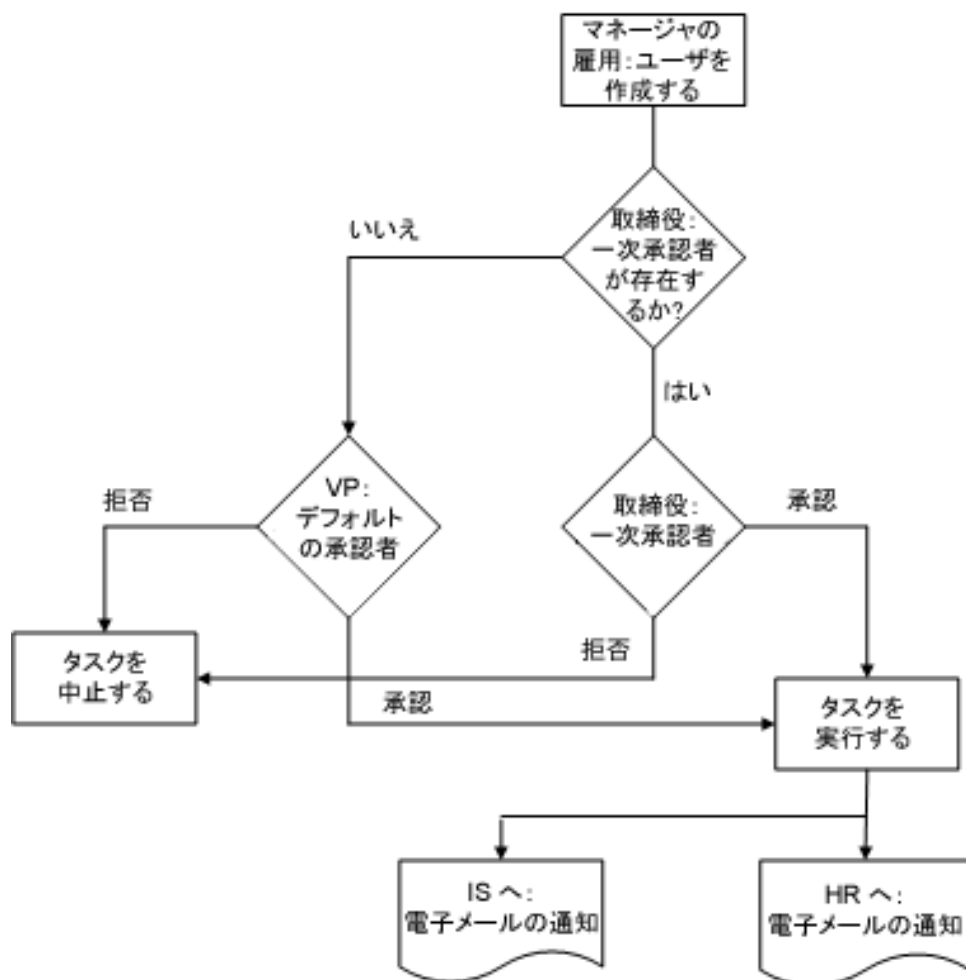
ある会社の CA Identity Manager 管理者が、以下のシナリオを処理するためのワークフローとユーザ ロールを定義することになりました。

- この会社の営業マネージャは、新しい営業担当者を雇うことにしました。営業マネージャは、この新規雇用に対する CA Identity Manager ユーザを作成する必要があります。
- 雇用プロセスを合理化するために、参加者が 1 つの作業アイテムを実行するだけで、タスクの承認（または拒否）を行えるようにします。
- 営業部長は、すべての新規雇用に対する第 1 承認者です。営業部長が見つからない場合は、営業の VP はデフォルトの承認者になります。
- 新規雇用が承認されると、CA Identity Manager は新規ユーザの電子メール通知を人事（HR）部と情報サービス（IS）部に送信します。

ユーザ制御図の作成

以下の図に、ユーザの作成シナリオの論理フローを示します。

タスク レベル ワークフローの例: ユーザを作成する



ワークフロー例の実装

この例のシナリオを実装するには、管理者が以下のタスクを実行する必要があります。

- タスクの開始者が必要な管理ロールのメンバであることを確認します。

営業マネージャは、[ユーザ マネージャ] 管理ロールのメンバである必要があります。このロールは、営業担当者の新規雇用に際して、[ユーザの作成] 管理タスクを開始するのに必要な権限を営業マネージャに与えます。

- [ユーザの作成] 管理タスクに対してタスク レベルのワークフローを有効にします。

タスク レベルのワークフローを使用すると、[ユーザの作成] タスクを完了するための作業アイテムが確実に 1 つだけ生成されるようになります。

[ユーザの作成] タスクには複数の個別イベントが関連付けられているため、イベント レベルのワークフローでは複数の作業アイテムが生成され、イベント レベルのワークフローが設定ハンドラにもなります。

- 参加者リゾルバを設定します。

使用可能な参加者リゾルバの数は、選択したワークフロー プロセス テンプレートによって決まります。SingleStageApproval テンプレートには、第 1 承認者とデフォルトの承認者が含まれます。その他のテンプレートはそれ以上の許可を行います。

このシナリオでは 2 人の個人承認者しか必要としないので、[ユーザ リスト] 参加者リゾルバは最も単純なソリューションを提供します。このリゾルバは、ロールやグループで複数のユーザを選択するのではなく、名前で個人承認者を選択できるようにします。

- 電子メール通知を設定します。

管理コンソールでは、特定のタスクやイベントに関する電子メール通知を作成できます。このシナリオでは、タスクの電子メールが有効になっており、[ユーザの作成] タスクの完了時に電子メール通知が送信されます。

適切な件名行とメッセージテキストを付けて、電子メールを人事部と情報サービス部に送信するには、カスタム電子メール テンプレートが必要です。

WorkPoint メソッドの使用法

WorkPoint メソッドは、R12 より前の CA Identity Manager リリースに適用されました。事前定義された WorkPoint ワークフロー プロセスは 14 個あり、これらはデフォルトにより特定の CA Identity Manager イベントとマッピングされています。参加者リゾルバを設定し、必要に応じてワークフロー プロセスを変更するには、WorkPoint Designer を使用する必要があります。

WorkPoint メソッドでは、管理コンソールを使用して、ワークフロー プロセスと承認イベントをマッピングし、対応するタスクを使用環境のグローバル レベルでワークフロー制御下に置く必要もあります。

このセクションでは、WorkPoint メソッドを使用して管理タスクをワークフロー制御下に置くための概要手順を示します。

注: 柔軟性と使い勝手の向上のため、できるだけテンプレート メソッドを使用することをお勧めします。

WorkPoint メソッドを使用する方法

1. [WorkPoint 管理ツールの設定](#) (P. 303)
2. 管理コンソールで以下の手順を実行します。
 - a. お使いの環境に対してワークフローを有効にするには、[詳細設定] - [ワークフロー] で [有効] チェックボックスを選択します。

注: この画面のイベント マッピングは、WorkPoint メソッドを使用してワークフローを設定している場合のみ適用されます。テンプレート メソッド（推奨）を使用する場合は、この管理コンソールを使用してイベントをマッピングして処理しないでください。
 - b. （オプション）グローバル イベントのマッピングで、イベント（複数可）を適切な事前定義ワークフロー プロセスと関連付けます。
 - c. 必要に応じて、CA Identity Manager 環境を再起動します。
3. ユーザ コンソールで以下の手順を実行します。
 - a. タスク固有イベントのマッピングで、イベント（複数可）を適切な事前定義ワークフロー プロセスと関連付けます。（オプション）
4. WorkPoint Designer で以下の手順を実行します。
 - a. 承認タスクをワークフロー プロセスと関連付けます（オプション）。
 - b. ワークフロー プロセスを使用して参加者リゾルバを設定します（オプション）。

5. ユーザ コンソールで以下の手順を実行します。
 - a. ワークフロー制御が設定されたら、適切なロールを持つユーザが管理タスクを実行します。
 - b. 指定されたワークフロー参加者は、イベントの承認または拒否を行います。

WorkPoint 管理ツールの設定

WorkPoint Designer は、Planet Group, Inc の一部門である Workpoint LLC 製作のソフトウェアで、CA Identity Manager に統合されています。WorkPoint Designer では、ワークフロープロセスおよびワークフロー ジョブを管理できます。WorkPoint 管理ツールには、WorkPoint Designer と WorkPoint Archive が含まれています。WorkPoint 管理ツールを設定するには、CA Identity Manager 管理ツールをインストールします。CA Identity Manager 管理ツールをインストールしない場合、インストーラを実行して、[CA Identity Manager 管理ツール] オプションを選択します。

注:管理ツールをワークフローに使用するには、管理ツールがインストールされているシステムにサポート対象 JDK がインストールされている必要があります。サポート対象のプラットフォームとバージョンの詳細な一覧については、[CA Identity Manager のサポート サイト](#)で「CA Identity Manager サポート マトリックス」を参照してください。

ワークフロー クライアント ツールは、CA Identity Manager 管理ツールの WorkPoint ディレクトリにあります。管理ツールは、以下のデフォルトの場所に配置されています。

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

このディレクトリのツールにより、次のことが行えます。

- ワークフロー データベース スキーマの作成
- デフォルト ワークフロー スクリプトのロード
- ワークフロープロセスとジョブの設計と監視

JBoss における WorkPoint Administrative Tool の設定

JBoss で WorkPoint 管理ツールを設定するには、`init.bat/sh` ファイルおよび `workpoint-client.properties` ファイルを編集します。

init.bat/init.sh の編集

init.bat/init.sh を編集する方法

1. テキスト エディタで、次のファイルのいずれかを編集します。

- **Windows の場合 :**

`admin_tools¥Workpoint¥bin¥init.bat`

- **UNIX の場合 :**

`admin_tools/Workpoint/bin/init.sh`

2. ファイルの JBoss セクションにある EJB_CLASSPATH 行のコメントを解除します。

注:他のアプリケーション サーバのセクションはすべてコメントになっていることを確認します。

3. `admin_tools¥Workpoint¥lib` 下で JBoss という名前のディレクトリを作成します。
4. `admin_tools¥Workpoint¥lib¥JBoss` ディレクトリに `jboss_home¥client` ディレクトリのコンテンツをコピーします。

workpoint-client.properties の編集

CA Identity Manager インストール中に選択したアプリケーション サーバの種類に応じて `workpoint-client.properties` ファイルを編集します。

workpoint-client.properties ファイルを設定する方法

1. `admin_tools¥Workpoint¥conf¥workpoint-client.properties` をテキスト エディタで開きます。

`admin_tools` は管理ツールがインストールされている場所を示します。管理ツールは、以下のデフォルトの場所に配置されています。

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

- **UNIX :** `/opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools`

2. JBOSS SETTINGS というタイトルのセクションを探します。

3. そのセクションのすべてのプロパティ値をコメント解除します。

以下に例を示します。

```
java.naming.provider.url=localhost
java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
java.naming.factory.url.pkgs=org.jboss.naming
```

注: java.naming.provider.url property 値を編集しなければならない場合があります。たとえば、localhost を `jnp://server_name` または `ip:port` に置き換えます。jnp ポート番号 1099 を使用していることを確認します。

4. ファイルを保存します。

WebLogic における WorkPoint 管理ツールの設定

WebLogic で WorkPoint 管理ツールを設定するには、`init.bat/sh` ファイルおよび `workpoint-client.properties` ファイルを編集します。

init.bat/init.sh の編集

init.bat/init.sh を編集する方法

1. テキスト エディタで、次のファイルのいずれかを編集します。

- Windows の場合 :

```
admin_tools¥Workpoint¥bin¥init.bat
```

- UNIX の場合 :

```
admin_tools/Workpoint/bin/init.sh
```

2. ファイルの WebLogic セクションにある `EJB_CLASSPATH` 行のコメントを解除します。

注:他のアプリケーション サーバのセクションはすべてコメントになっていることを確認します。

3. `weblogic_home¥server¥lib` から次の場所に `wlclient.jar` ファイルをコピーします。

```
admin_tools¥Workpoint¥lib¥
```

workpoint-client.properties の編集

CA Identity Manager インストール中に選択したアプリケーション サーバの種類に応じて `workpoint-client.properties` ファイルを編集します。

workpoint-client.properties ファイルを設定する方法

1. `admin_tools¥Workpoint¥conf¥workpoint-client.properties` をテキスト エディタで開きます。
2. ファイルの WebLogic セクションを見つけます。

3. そのセクションのすべてのプロパティ値をコメント解除します。
4. ファイルを保存します。

注: `java.naming.provider.url` プロパティは、CA Identity Manager Server をインストールしたシステムの完全修飾ドメイン名および WebLogic ポート番号を参照する必要があります。

WebSphere における WorkPoint 管理ツールの設定

WebSphere で WorkPoint 管理ツールを設定するには、`init.bat/sh` ファイルおよび `workpoint-client.properties` ファイルを編集します。

`init.bat/init.sh` の編集

`init.bat/init.sh` を編集する方法

1. テキスト エディタで、次のファイルのいずれかを編集します。

- **Windows の場合 :**

`admin_tools\Workpoint\bin\init.bat`

- **UNIX の場合 :**

`admin_tools/Workpoint/bin/init.sh`

2. IBM WebSphere セクションのコメントを解除します。

注: COMMON WP_CLASSPATH セクションの WP_CLASSPATH エントリをコメントにしないでください。

3. 他のアプリケーション サーバのセクションがすべて、コメントになっていることを確認します。
4. 必要に応じて、ご使用の環境での適切なパス `JAVA_HOME` と `WAS_HOME` の値を置き換えてください。

`workpoint-client.properties` の編集

CA Identity Manager インストール中に選択したアプリケーション サーバの種類に応じて `workpoint-client.properties` ファイルを編集します。

workpoint-client.properties ファイルを設定する方法

1. `admin_tools¥Workpoint¥conf¥`

`workpoint-client.properties` をテキスト エディタで開きます。

`admin_tools` は管理ツールがインストールされている場所を示します。 管理ツールは、以下のデフォルトの場所に配置されています。

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

2. IBM WEBSPPHERE SETTINGS というタイトルのセクションを探します。

3. そのセクションのすべてのプロパティ値をコメント解除します。

以下に例を示します。

```
java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory
java.naming.provider.url=iiop://localhost:bootstrap_port
```

注:ブートストラップ ポート番号は、WebSphere 管理コンソールに指定したポート番号に合致する必要があります。正しいポート番号を知るには、[サーバ] - [エンドポイント] - [ブートストラップ サーバのアドレス] をクリックします。

4. 以下の手順に従い、WebSphere プロファイルの BOOTSTRAP_ADDRESS ポートを更新します。
 - a. WebSphere 管理コンソールで、[アプリケーション サーバ] - [server_name] - [通信] をクリックします。
 - b. [ポート] を展開します。
 - c. `iam_im.ear/config` にある `workpoint-client.properties` ファイルを編集します。
 - d. WebSphere セクションのデフォルト ポート 2809 をプロファイルの BOOTSTRAP_ADDRESS のポートに変更します。
5. ファイルを保存します。

WorkPoint Designer の開始

WorkPoint Designer を開始するには、以下のファイルを実行します。

- **Windows** : `admin_tools¥WorkPoint¥bin¥Designer.bat`
- **UNIX** : `admin_tools/WorkPoint/bin/Designer.sh`

admin_tools は、CA Identity Manager 管理ツールのインストールディレクトリです。管理ツールは、以下のデフォルトの場所に配置されています。

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

注: WorkPoint Designer を実行する前に、ワークフロー コンポーネントをインストールして設定しておく必要があります。詳細については、お使いのアプリケーション サーバの「WorkPoint 管理ツールの設定」を参照してください。

詳細情報:

[JBoss における WorkPoint Administrative Tool の設定](#) (P. 303)

[WebLogic における WorkPoint 管理ツールの設定](#) (P. 305)

[WebSphere における WorkPoint 管理ツールの設定](#) (P. 306)

WorkPoint プロセス

CA Identity Manager には、WorkPoint Designer で事前定義された多数のワークフロー プロセスが組み込まれています。事前定義されたプロセスとデフォルトのイベント マッピングの使用、ワークフロー プロセスと他のイベントとのマッピング、アクティビティの追加または削除によるワークフロー プロセスの変更、ワークフロー プロセスの新規作成などを行うことができます。

プロセスとイベントのグローバル マッピング

ワークフロー プロセスは、非ポリシーベースとポリシーベースのどちらでもグローバル レベルのイベントにマッピングできます。

ポリシーベース ワークフローを使用してイベントをワークフロー プロセスにマッピングする方法の詳細については、「[Global Event Policy-Based Workflow Mapping](#)」を参照してください。

以下の表に、ワークフロー プロセスとイベントのデフォルトのグローバル マッピングを示します。それらのマッピングは、管理コンソールで指定されています。

重要: これらはグローバル マッピングです。マッピングされたワークフロー プロセスは、使用環境内の任意のタスクによって、対応するイベントが生成されたときに実行されます。

ワークフロー プロセス	マッピングされるイベント
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	AssignAdminRoleEvent RevokeAdminRoleEvent
ModifyGroupMembershipApproveProcess*	AddToGroupEvent RemoveFromGroupEvent
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
ModifyObjectApproveProcess	ModifyObjectEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

注: アスタリスク (*) の付いたワークフロー プロセスは、デフォルトではイベントとマッピングされません。

プロセスとイベントのマッピング

ワークフロー プロセスの作成と変更には、**WorkPoint Designer** を使用します。CA Identity Manager 用のワークフロー プロセスを作成する場合は、特定の CA Identity Manager タスクを念頭に置いて作成してください。このタスクの実行は、ワークフロー プロセスによって制御されます。

ワークフロー プロセスの作成に加え、以下のことも実行する必要があります。

- 「管理タスクおよびイベント」の説明に従って、CA Identity Manager タスクによって生成されるイベントを特定します。イベントを生成する任意の CA Identity Manager タスクに対し、ワークフロー プロセスを作成 できます。
- ワークフロー プロセスとイベントをマッピングするには、以下の操作のいずれかを実行します。
 - グローバル レベルでワークフロー プロセスをイベントに割り当てます。
このグローバル マッピングでは、イベントを生成するタスクに関係なく、使用環境内でこのイベントが生成されると必ずワークフロー プロセスが実行されます。
 - 特定のタスクによって生成されるイベントにワークフロー プロセスを割り当てます。

このタスク固有のマッピングでは、指定したタスクによってこのイベントが生成された場合にのみ、ワークフロー プロセスが実行されます。

注: グローバル レベルと特定のタスクの両方でイベントとワークフロー プロセスをマッピングすると、特定のタスクに関連付けられたワークフロー プロセスが優先されます。

- ワークフロー プロセス内のワークフロー アクティビティに対し、参加者リゾルバを指定します。
- ワークフロー アクティビティを承認タスクと関連付けます。

グローバル レベルでのプロセスとイベントのマッピング

グローバル レベルでワークフロー プロセスとイベントをマッピングすると、使用環境内の任意のタスクによってそのイベントが生成されたときに、ワークフロー プロセスが実行されます。

注: 以下の手順は動作しますが、グローバル イベント [レベルのポリシー ベースの \(P. 354\)](#) 手順は、イベントにプロセスをマップする推奨方法です。

グローバル レベルで非ポリシー ベースのワークフロー プロセスとイベントをマッピングする方法

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

`http://hostname/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。たとえば、`myserver.mycompany.com:port` です。

2. [環境] をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. [詳細設定] をクリックし、次に [ワークフロー] をクリックします。
4. イベントとワークフロー プロセスをマッピングする方法
 - a. [イベント] リスト ボックスからイベントを選択します。
 - b. 承認プロセスのリスト ボックスからワークフロー プロセスを選択します。
 - c. [追加] をクリックします。
5. イベントとワークフロー プロセスのマッピングが完了したら、[保存] をクリックします。
6. CA Identity Manager 環境を再起動して、変更内容を有効にします。

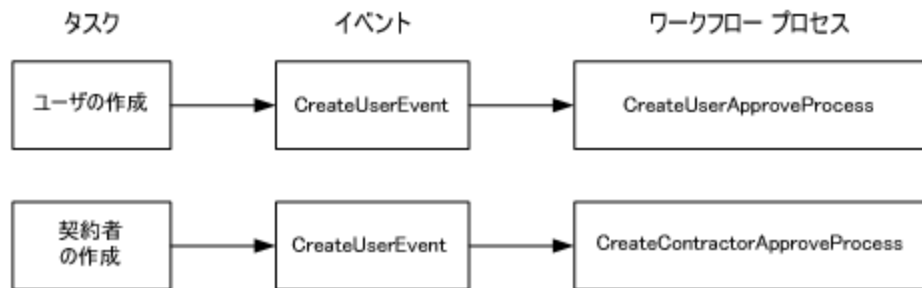
詳細情報:

[プロセスとイベントのグローバル マッピング \(P. 309\)](#)

特定のタスクでのプロセスとイベントのマッピング

特定のタスクによって生成されるイベントに、ワークフロー プロセスを割り当てるができます。この場合は、指定したタスクによってマッピングしたイベントが生成されたときにのみ、ワークフロー プロセスが実行されます。

タスク固有のマッピングは、同じイベントに対して実行可能なワークフロー プロセスを可変的に制御します。たとえば、以下の図に示す 2 種類のタスクは同じイベントを生成しますが、トリガされるワークフロー プロセスはそれぞれ異なります。



この図では、各タスクが異なるワークフロー プロセスを使用しています。

ユーザの作成

CreateUserEvent をトリガするデフォルトの管理タスクを指定します。このイベントは、デフォルトのワークフロー プロセスである CreateUserApproveProcess にマッピングされています。

契約業者の作成

「ユーザの作成」をベースにした カスタム タスクを指定します。この場合は、CreateUserEvent が CreateContractorApproveProcess とマッピングされます。これは、新規契約業者アカウントの承認用に作成されたカスタム ワークフロー プロセスです。

既存のタスク内の非ポリシー ベースのワークフロー プロセスとイベントをマッピングする方法

1. ユーザ コンソールで、[ルールおよびタスク] - [管理タスク] - [管理タスクの変更] を選択します。
2. 管理タスクを検索します。
3. タスク（「ユーザの変更」、「ユーザの作成」など）を選択し、[選択] をクリックします。

4. [イベント] タブで、タスク内のイベントに対するワークフロー プロセスを選択します。

注: イベント名と [ワークフロー プロセス] ドロップダウン メニューをこのタブに表示するには、ワークフローを有効化する必要があります。

5. [編集] ボタンをクリックし、[Workflow mapping] 画面を表示します。
6. [ワークフロー プロセス] ドロップダウン メニューを使用して、ワークフロー プロセスをイベント名に割り当て、[OK] をクリックします。
7. [サブミット] をクリックします。

新規タスク内の非ポリシー ベースのワークフロー プロセスとイベントをマッピングする方法

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

注: 新しいワークフロー承認タスクのテンプレートとして、既存のワークフロー承認タスク ([グループ作成を承認]、[ユーザ作成を承認] など) を選択してください。

2. [プロファイル] タブで、適切なフィールドに情報を入力します。
3. [イベント] タブで、タスク内のイベントに対するワークフロー プロセスを選択します。

注: イベント名と [ワークフロー プロセス] ドロップダウン メニューをこのタブに表示するには、ワークフローを有効化する必要があります。

4. [ワークフロー プロセス] ドロップダウン メニューを使用して、ワークフロー プロセスをイベント名に割り当て、[OK] をクリックします。
5. [サブミット] をクリックします。

注: ポリシー ベースのワークフロー プロセスとイベントをマッピングするには、[「ポリシー ベース ワークフロー」](#) (P. 337)を参照してください。

注: ワークフロー プロセス リストには、テンプレート メソッドと WorkPoint メソッドの両方で使用するプロセスが含まれています。

- テンプレート メソッドプロセス (SingleStepApproval、TwoStageApprovalProcess または EscalationApproval のいずれか) が選択されると、ページが展開されて、参加者リゾルバの設定が有効になります。
- WorkPoint メソッドプロセスが選択されているとき、ページは展開しません。参加者リゾルバは WorkPoint Designer で設定されます。

詳細情報:

[プロセスとイベントのグローバル マッピング \(P. 309\)](#)

ワークフロー アクティビティ

CA Identity Manager には、WorkPoint Designer で事前定義された多数のワークフロー アクティビティが組み込まれています。これらのアクティビティは、事前定義ワークフロー プロセスに割り当てられます。

事前定義ワークフロー プロセスは、1 ステップのみのプロセスです。したがって、各プロセスには事前定義アクティビティが 1 つだけ含まれます。

それぞれの事前定義アクティビティは、CA Identity Manager で事前定義された同じ名前のワークフロー承認タスクと対応しています。事前定義アクティビティは他のワークフロー プロセスにも使用できます。また、新しいアクティビティを作成することもできます。

事前定義ワークフロー プロセスは、変更せずにそのまま使用できますが、さらにアクティビティを追加することもできます。ワークフロー プロセスにアクティビティを追加する方法の詳細については、WorkPoint のマニュアルを参照してください。

プロセス、タスク、アクティビティ

以下の表に、事前定義ワークフロー アクティビティと、各アクティビティがデフォルトで割り当てられる事前定義ワークフロー プロセスを示します。

注: 事前定義ワークフロー アクティビティと、それに対応するワークフロー承認タスクは同じ名前になります。

ワークフロー プロセス	ワークフロー タスク/アクティビティ
CertifyRoleApprovalProcess**	ロール認証を承認
Consultation Process*	
CreateGroupApproveProcess	グループ作成を承認
CreateOrganizationApproveProcess	組織作成を承認
CreateUserApproveProcess	ユーザ作成を承認
DeleteGroupApproveProcess	グループ削除を承認

ワークフロー プロセス	ワークフロー タスク/アクティビティ
DeleteOrganizationApproveProcess	組織削除を承認
DeleteUserApproveProcess	ユーザ削除を承認
ModifyAccessRoleMembershipApproveProcess	アクセス ロール メンバシップ変更を承認
ModifyAdminRoleMembershipApproveProcess	管理ロール メンバシップ変更を承認
ModifyGroupMembershipApproveProcess	グループ メンバシップ変更を承認
ModifyIdentityPolicySetApproveProcess	アイデンティティ ポリシー セット変更を承認
ModifyOrganizationApproveProcess	組織変更を承認
ModifyUserApproveProcess	ユーザ変更を承認
SelfRegistrationApproveProcess	自己登録の承認
SingleStepApproval*	
TwoStageApprovalProcess*	

注: 1 つのアスタリスク (*) が付いたワークフロー プロセスは、テンプレート メソッドと共に使用します。これらはユーザ コンソールで設定するため、デフォルトのタスクやアクティビティは関連付けられていません。

CertifyRoleApprovalProcess (**) は、カスタム参加者リゾルバのデモンストレーションを行うサンプルプロセスです。

ワークフロー アクティビティと承認タスクの関連付け

ワークフロー アクティビティとワークフロー承認タスクを関連付けるには、WorkPoint Designer で名前と値のペアを定義します。

注: ワークフロー アクティビティに対して名前と値のペアが定義されていない場合、CA Identity Manager のデフォルトでは、承認タスクと名前が一致するタスクが使用されます。

ワークフロー アクティビティと承認タスクを関連付けるには

1. WorkPoint Designer を起動します。
2. [ファイル] - [開く] - [プロセス] をクリックします。
3. ワークフロー プロセスを選択し、[開く] をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、[プロパティ] を選択します。

5. [タイプ] ドロップダウン メニューから [テキスト] を選択します。
6. [ユーザ データ] タブに、以下の情報を入力します。
 - 名前 — TASK_TAG
 - 値 — 承認タスクのタグ名
7. [追加] をクリックします。
8. [OK] をクリックして、変更を保存します。

エンドポイントの承認タスクの作成

アカウント管理画面に承認タスクを作成できます。アカウントの変更を承認するタスクでは、承認者が変更された値を見ることができるよう、承認画面はエンドポイント タイプ固有である必要があります。作成または変更タスクに承認タスクを作成するには、以下の手順に従います。

エンドポイントに承認タスクを作成する方法

1. ユーザ コンソールで、[ロールおよびタスク] - [管理タスク] - [管理タスクの作成] をクリックします。
2. エンドポイントでのアカウントの管理に使用するために、[管理タスクのコピーの作成] を選択します。

名前が「作成」で終わり、エンドポイント タイプの名前を示します。例としては、[Active Directory アカウントの作成] などです。
3. [プロファイル] タブに、以下の変更を加えます。
4. 新しいタスクの名前を変更します。
 - タスク タグを変更します。
 - アクションを [イベントの承認] に変更します。
5. [タブ] タブに、以下の変更を加えます。
 - a. すべての [リレーションシップ] タブを削除します。
 - b. 必要に応じて、タブの承認画面をコピーしてから編集します。

注: 承認タスクでアカウント画面を使用しているときに、問題が発生する場合があります。承認タスクでアカウント画面を動作させるためには、デフォルトのアカウント画面を変更する必要がある可能性があります。
6. [サブミット] をクリックします。

参加者リゾルバ: WorkPoint メソッド

WorkPoint メソッドを使用して参加者を指定するには、WorkPoint Designer で以下のアクティビティ プロパティを定義します。

- CA Identity Manager とワークフロー サーバ間の通信を有効化する、事前定義された CA Identity Manager スクリプトの名前。このスクリプトは、アクティビティの参加者に対するリクエストを CA Identity Manager に発行し、そのリストをワークフロー サーバに渡します。
- 参加者リゾルバ（複数可）の参照

参加者リゾルバのタイプ

ワークフロー アクティビティのプロパティに特定の参加者リストを入力するのではなく、参加者リゾルバとマッピングされた任意の名前によって参加者が参照されます。

事前定義されたプロセス モデルの場合、以下の 4 種類の参加者リゾルバがあります。

ロール参加者リゾルバ

特定のロールのメンバが参加者であることを指定します。

グループ参加者リゾルバ

特定のグループのメンバが参加者であることを指定します。

カスタム参加者リゾルバ

カスタム参加者リゾルバによって、参加者が決定されることを指定します。

フィルタ参加者リゾルバ

検索フィルタを使用して参加者が選択されることを指定します。

ロール参加者リゾルバ

ロール タイプの参加者リゾルバでは、CA Identity Manager が該当するロールのメンバをすべて取得し、それらのメンバを参加者として返します。

[アクティビティ] ダイアログ ボックスの UserData パラメータでリゾルバ タイプが指定されていない場合は、デフォルトによりロール タイプのリゾルバが使用されます。

[WorkPoint アクティビティのプロパティ] ダイアログ ボックスの [ユーザ データ] タブで参加者リゾルバが指定されていない場合は、CA Identity Manager のデフォルトにより、この承認タスクが含まれた使用可能なロールがすべて検出され、それらのロール メンバが参加者として返されます。

ロール参加者リゾルバの設定方法

1. WorkPoint Designer を起動します。
2. [ファイル] - [開く] - [プロセス] をクリックします。
3. ワークフロー プロセスを選択し、[開く] をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、[プロパティ] を選択します。
5. [タイプ] ドロップダウン メニューから [テキスト] を選択します。
6. [ユーザ データ] タブに、以下の情報を入力します。

- 名前 — APPROVER_ROLE_NAME

- 値 — CA Identity Manager ロールの名前 (例: セキュリティ マネージャ)

7. [追加] をクリックします。
- 注: このロールには、承認タスクを含める必要はありません。
8. [タイプ] ドロップダウン メニューから [テキスト] を選択します。
9. [ユーザ データ] タブで、以下の名前と値のペアを入力します (オプション)。

- 名前 — APPROVERS_REQUIRED

- 値 — YES

10. [追加] をクリックします。

注: デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。

11. [OK] をクリックして、変更を保存します。

グループ参加者リゾルバ

グループタイプの参加者リゾルバでは、CA Identity Manager が該当するグループのメンバをすべて取得し、それらのメンバを参加者として返します。

グループ参加者リゾルバの設定方法

1. WorkPoint Designer を起動します。
2. [ファイル] - [開く] - [プロセス] をクリックします。
3. ワークフロー プロセスを選択し、[開く] をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、[プロパティ] を選択します。
5. [タイプ] ドロップダウン メニューから [テキスト] を選択します。
6. [ユーザ データ] タブに、以下の情報を入力します。
 - 名前—APPROVER_GROUP_UNIQUENAME
 - 値—CA Identity Manager グループの名前
7. [追加] をクリックします。
8. [タイプ] ドロップダウン メニューから [テキスト] を選択します。
9. [ユーザ データ] タブで、以下の名前と値のペアを入力します (オプション)。
 - 名前—APPROVERS_REQUIRED
 - 値—YES
10. [追加] をクリックします。

注: デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。
11. [OK] をクリックして、変更を保存します。

カスタム参加者リゾルバ

カスタム参加者リゾルバは、ワークフロー アクティビティの参加者を決定し、リストを CA Identity Manager に返す Java オブジェクトです。CA Identity Manager は、このリゾルバから返されたリストをワークフロー エンジンに渡します。一般に、カスタム参加者リゾルバを作成するのは、標準の参加者ポリシーではアクティビティに必要な参加者のリストを提供できない場合のみです。

注: カスタム参加者リゾルバの作成には、参加者リゾルバ API を使用します。詳細については、「Java のプログラミングガイド」を参照してください。

カスタム参加者リゾルバを設定する方法

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

`http://hostname/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。たとえば、`myserver.mycompany.com:port` です。

2. [環境] をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. [詳細設定] をクリックし、次に [ワークフロー参加者リゾルバ] をクリックします。
4. [ワークフロー参加者リゾルバ] 画面で [新規] をクリックし、以下の情報を入力します。

名前

カスタム参加者リゾルバ名を指定します。たとえば、`GroupFinder` です。

説明

カスタム参加者リゾルバの説明を指定します。

クラス

Java クラス名を指定します。たとえば、`com.netegrity.samples.GroupFinder` です。

5. [保存] をクリックします。
6. WorkPoint Designer を起動します。
7. [ファイル] - [開く] - [プロセス] をクリックします。
8. ワークフロー プロセスを選択し、[開く] をクリックします。
9. プロセス内のアクティビティ ノードを右クリックし、[プロパティ] を選択します。
10. [タイプ] ドロップダウン メニューから [テキスト] を選択します。

11. [ユーザ データ] タブに、以下の情報を入力します。

名前

APPROVER_CUSTOMRESOLVER_NAME

値

カスタム リゾルバの名前を一意に指定します。これは、管理コンソールの [カスタム タイプの参加者リゾルバ] 画面に入力した名前と一致している必要があります。たとえば、GroupFinder です。

12. [追加] をクリックします。

注: デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。

13. [OK] をクリックして、変更を保存します。

フィルタ参加者リゾルバ

フィルタ参加者リゾルバを使用すると、CA Identity Manager がフィルタ基準と一致するユーザまたはグループを検索できるようになります。WorkPoint Designer で検索フィルタを指定すると、CA Identity Manager によって対応するワークフローアクティビティと一致する承認者が返されます。

フィルタ参加者リゾルバを作成するには、[WorkPoint アクティビティのプロパティ] ダイアログ ボックスの [ユーザ データ] タブを使用します。

参加者リゾルバのフィルタ構文

検索フィルタを作成するために組み合わせる必要がある 3 つの属性は、以下の通りです。

- 承認者属性 (例: タイトル)
- 承認者属性演算子 (例: equals)
- 承認者属性値 (例: マネージャ)

検索フィルタの必須属性は、以下の順序で組み合わせます。

属性 演算子 値

以下に例を示します。

「タイトル equals マネージャ」または「部署 contains 給与」

参加者リゾルバの必須フィルタ属性

参加者リゾルバの必須フィルタ属性は以下のとおりです。

注: 各フィルタの「n」は、検索フィルタ番号を示す正の整数です。デフォルトは 1 です。

APPROVER_FILTER_n_ATTRIBUTE

承認者属性を指定します。（例：Title、Department、User ID）。承認者属性名の文字列は、CA Identity Manager のユーザ属性名の文字列と一致している必要があります。

APPROVER_FILTER_n_OP

承認者属性と関連付けられる演算子を指定します。（例：equals、not_equals、contains）。演算キーワードの大文字小文字は区別されません。

このフィルタへの有効な入力を以下に示します。

- EQUALS
- STARTSWITH
- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

承認者と関連付けられる値を指定します。（例：manager、payroll、engineering）

参加者リゾルバのオプション フィルタ属性

参加者リゾルバのオプションフィルタ属性は以下のとおりです。

APPROVER_OBJECTTYPE

USER または GROUP（大文字小文字の区別なし）

デフォルトは USER です。

APPROVER_ORG_UNIQUENAME

承認者の組織を示す一意の名前。組織名の文字列は、CA Identity Manager の組織名の文字列と一致する必要があります。

デフォルトは **root** です。

APPROVER_ORG_AND_LOWER

承認者の組織または下位組織です。

- 0 は、承認者の組織内で検索することを意味します。
- 1 は、承認者の組織のすべての下位組織内で検索することを意味します。

デフォルトは **1** です。

APPROVER_FILTER_NO

使用する検索フィルタの番号。フィルタが **2** つある場合、この数値は **2** になります。

デフォルトは **1** です。

注: フィルタの数が **2** 以上の場合、このフィルタは必須です。

APPROVER_FILTER_n_CONJ_TYPE

OR または **AND** 連結タイプを使用して、検索フィルタを組み合わせることができます。

注: **OR** 連結タイプで区切られたフィルタは、**AND** で区切られたフィルタよりも優先されます。

たとえば、**"title equals manager"** および **"department equals development"** の両方を検索する場合は、**AND** 連結タイプを指定します。

注: 「n」は、検索フィルタ番号を示す **2** 以上の正の整数です。

参加者リゾルバフィルタの追加

参加者リゾルバフィルタの追加方法

1. **WorkPoint Designer** を起動します。
2. **［ファイル］** - **［開く］** - **［プロセス］** をクリックします。
3. ワークフロー プロセスを選択し、**［開く］** をクリックします。
4. プロセス内のアクティビティ ノードを右クリックし、**［プロパティ］** を選択します。
5. **［タイプ］** ドロップダウン メニューから **［テキスト］** を選択します。

6. [ユーザ データ] タブに、以下の情報を入力します。

- 名前 — APPROVER_FILTER_1_ATTRIBUTE
- 値 — 一意のロール識別子（例：title）

7. [追加] をクリックします。

8. 検索フィルタの属性ごとに、手順 6 ～ 7 を繰り返します。

注：デフォルトの承認者の設定は、APPROVERS_REQUIRED=NO です。この場合は、参加者が検出されなくてもアクティビティが自動的に承認されます。

APPROVERS_REQUIRED=YES で、CA Identity Manager が参加者を検出できない場合は、アクティビティを正常に完了できません。

9. [OK] をクリックして、変更を保存します。

例：フィルタ参加者リゾルバ

以下の表のユーザストアには、4 人のユーザ（Holly、Sarah、John、Dave）と、ユーザ ID、役職、部署の各属性が含まれています。

ユーザ	ID	タイトル	部署
Holly	admin1	sysadmin	管理
Sarah	test1	sysadmin	development
John	admin2	manager	development
Dave	admin3	sysadmin	accounting

CA Identity Manager は、上記のユーザストアに対し、以下の表で定義される 3 つのフィルタを適用します。

名前	値
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	=
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	department
APPROVER_FILTER_2_OP	=

名前	値
APPROVER_FILTER_2_VALUE	administration
APPROVER_FILTER_3_CONJ_TYPE	OR
APPROVER_FILTER_3_ATTRIBUTE	title
APPROVER_FILTER_3_OP	=
APPROVER_FILTER_3_VALUE	sysadmin

CA Identity Manager は、これらのフィルタを以下の順序で適用します。

1. OR 連結で接続された 2 番目と 3 番目のフィルタを評価します。
"department equals administration" OR "title equals sysadmin"
これにより John が除外され、Holly、Sarah、Dave が返されます。
2. AND 連結で接続された 1 番目と 2 番目のフィルタを評価します(ここで、「*」はワイルドカード文字となります)。
"uid equals admin*" AND "department equals administration"
これにより Sarah が除外され、Holly と Dave が返されます。

このユーザストアから最終的に返されるユーザは Holly と Dave です。

参加者リゾルバの優先順位

参加者リゾルバが指定されていない場合は、CA Identity Manager のデフォルトにより、この承認タスクが含まれた使用可能なロールがすべて識別され、それらのロールメンバが参加者として返されます。

複数の参加者リゾルバを指定した場合、CA Identity Manager は以下の優先順でそれら进行评估します。

1. カスタム
2. ロール
3. フィルタ
4. グループ

CA Identity Manager は、この優先順で最初のリゾルバを識別および適用し、残っている後続のリゾルバはすべて無視します。

使用できるリゾルバは一度に 1 つのみです。また、CA Identity Manager が参加者を正しく識別できるように、リゾルバが正しく設定されていることを確認してください。

ワークフロー リソース スクリプトの指定

CA Identity Manager には、CA Identity Manager とワークフロー サーバ間で情報を渡すスクリプト（名前は IM Approvers）が用意されています。

ワークフロー アクティビティに参加者リストが必要な場合は、このスクリプトによって、アクティビティ名、[WorkPoint アクティビティのプロパティ] ダイアログボックスの [ユーザ データ] タブで指定された参加者識別子、および [ユーザ データ] タブで指定されたその他の情報が CA Identity Manager に渡されます。CA Identity Manager は参加者を検索し、このスクリプトにリストを返します。次に、このスクリプトからワークフロー サーバにリストが渡されます。

新しいワークフロー プロセス定義があり、そのワークフロー プロセスのアクティビティが CA Identity Manager のワークフロー承認タスクの場合、IM Approvers スクリプトを [WorkPoint アクティビティのプロパティ] ダイアログボックスの [リソース] タブに指定する必要があります。

WorkPoint Designer で IM Approvers スクリプトを指定するには、以下の手順に従います。

1. [Resources] タブで、[Select] をクリックします。
2. [Select Resources] ダイアログボックスで、ドロップダウンリストから [Rule] を選択します。このアクションによって、アクティビティと関連付けできるルール（スクリプト）がリストされます。
3. スクリプト名 IM Approvers を選択し、[Add] をクリックします。
4. [OK] をクリックし、[Activity Properties] ダイアログボックスで [適用] をクリックします。

注：IM Approvers スクリプトは変更しないでください。

ユーザ認証タスクの参加者の指定

ユーザ認証タスクはイベント CertifyRoleEvent を生成します。このイベントは、事前定義プロセス CertifyRoleApproveProcess を通してワークフロー承認を受けることができます。

CA Identity Manager には、事前定義の参加者リゾルバ CertifyRoleParticipantResolver も組み込まれています。このリゾルバはデフォルトで使用環境内に表示されます。CertifyRoleApprovalProcess のアクティビティに対する参加者は、CertifyRoleParticipantResolver によって指定されます。

参加者の設定情報を指定する方法

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

`http://hostname/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。たとえば、`myserver.mycompany.com:port` です。

2. [環境] をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. [詳細設定] をクリックし、次に [その他] をクリックします。
4. 名前と値のペアを定義して、認証される各ロールの承認者を指定します。
 - [プロパティ] フィールドで、*role-type.role-name* の形式を使用します。
role-type には、`admin`、`access`、`provisioning` のいずれかのロールを指定します。
role-name には、既存の任意のロール名を指定します。
ロール名とロールタイプはピリオド (.) で区切る必要があります。
 - [値] フィールドに、承認者の ID を指定します。各 ID はセミコロン (;) で区切ります。

以下の例では、以下のロールに対するユーザ認証が以下の参加者によって承認されます。

- `jsmith01` と `ajones19` は、[ユーザ マネージャ] ロールに対する認証を承認できます。
- `plewis12` は、[System Manager] ロールに対する唯一の承認者です。
- `rtrevor8` と `pkitt3` は、[My Access] ロールに対する認証を承認できます。

プロパティ	値
<code>admin.User Manager</code>	<code>jsmith01;ajones19</code>
<code>admin.System Manager</code>	<code>plewis12</code>
<code>access.My Access Role</code>	<code>rtrevor8;pkitt3</code>

注: 指定されていないロールは、`CertifyRoleEvent` に対する承認者を持ちません。

WorkPoint Designer のプロセス

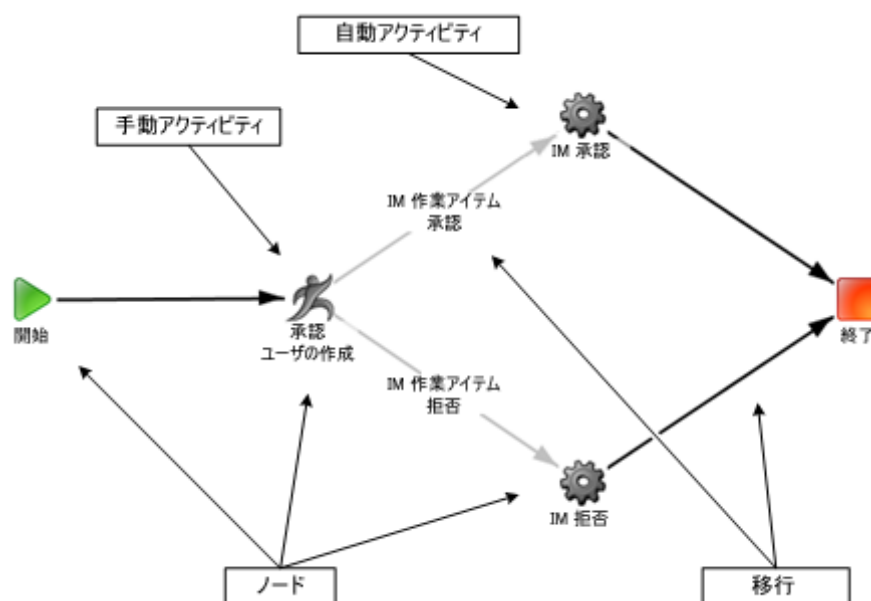
WorkPoint Designer では、CA Identity Manager に用意されているデフォルトのワークフロープロセスとアクティビティをカスタマイズして、新しいワークフロープロセスとアクティビティを作成することができます。

このマニュアルでは、CA Identity Manager に固有の WorkPoint ワークフロー情報について説明します。詳細については、WorkPoint Directory のマニュアルを参照してください。

注: ワークフロープロセスの作成時には、既存の CA Identity Manager プロセスのコピーを作成し、新しいプロセスを必要に応じて変更してください。この方法で作成されたワークフロープロセスには、移行スクリプトや自動アクティビティなど CA Identity Manager 固有のデフォルトの要素とノードが組み込まれます。

WorkPoint プロセス図

以下の図に、一般的なワークフロープロセスを示します。ここでは、CA Identity Manager のタスクを制御するプロセスに関する最小限のコンポーネントセットが使用されています。この図は、ユーザ作成タスクの実行を制御する事前定義プロセス CreateUserApproveProcess を示しています。



WorkPoint プロセスのコンポーネント

このワークフロー プロセスには、以下のノードと移行が含まれています。

開始

各ワークフロー プロセスは、このノードから始まります。

停止

各ワークフロー プロセスは、このノードで終わります。

手動アクティビティ

手動アクティビティでは、参加者による **CA Identity Manager** タスクの承認または拒否が必要です。このアクティビティの名前は、**CA Identity Manager** のワークフロー承認タスクと同じにする必要があります。

CA Identity Manager のタスクを制御するワークフロー プロセスには、そのタスクの承認を求める手動アクティビティが少なくとも 1 つ含まれている必要があります。

自動アクティビティ

自動アクティビティには、以下のいずれかのスクリプトが割り当てられます。

- **INotify IM Approve** — **CA Identity Manager** に、ワークフロー制御下にある **CA Identity Manager** タスクを実行するよう通知します。
- **Notify IM Reject** — **CA Identity Manager** に、**CA Identity Manager** タスクの実行をキャンセルするよう通知します。

一般に、**Notify IM Approve** スクリプトはすべての手動アクティビティが承認された場合に有効化され、**Notify IM Reject** スクリプトは手動アクティビティが 1 つでも拒否された場合に有効化されます。

無条件移行

無条件移行は、ワークフロー プロセス内のあるノードから別のノードまでのパスであり、条件スクリプトとは関連付けられません。

条件移行

条件移行は、ワークフロー プロセス内のあるノードから別のノードまでの代替パスであり、条件スクリプトと関連付けられます。

条件スクリプトは、関連付けられたアクティビティの結果を評価して、移行するかどうかを決定します。このスクリプトが **true** を返した場合は、移行が実行され、プロセスが次に指令されたノードに移ります。

2 つ以上の条件スクリプトが **true** を返す可能性もあります。各スクリプトは別の移行と関連付けられているため、この場合はアクティビティを並列実行することができます。

注: 条件移行では、カスタム スクリプトを使用できます。詳細については、「*Programming Guide for Java*」を参照してください。

手動アクティビティのプロパティ

以下の表に、CA Identity Manager に固有のプロパティ設定を示します。これらの設定は、WorkPoint Designer の [Activity Properties] ダイアログ ボックスの各タブで定義します。

[プロパティ]タブ	プロパティの説明
リソース	IM Approvers — Include リストで指定されます。このスクリプトは CA Identity Manager とワークフロー サーバ間で情報を渡します。
エージェント	Nobody Auto Complete — Asynchronous リストで指定され、Available 状態と関連付けられます。このスクリプトは、アクティビティ参加者が存在しない場合に、アクティビティを承認済みと見なすかどうかを決定します。
ユーザ データ	CA Identity Manager がアクティビティ参加者を取得するために使用する名前と値のペアを定義します。オプションで、カスタム参加者リゾルバに渡すデータを定義することもできます。

条件移行のプロパティ

以下のデフォルト スクリプトは、[移行のプロパティ] ダイアログ ボックスの [条件] タブに表示されます。

IM WorkItem Approved

関連付けられたアクティビティが承認された場合に **true** を返します。ワークフロー プロセスは、移行によって示された次のノードに移ります。

IM WorkItem Rejected

関連付けられたアクティビティが拒否された場合に **true** を返します。ワークフロー プロセスは、移行によって示された次のノードに移ります。

ジョブとプロセス インスタンス

ワークフロー プロセスは、CA Identity Manager が特定のタスクを完了できる前に実行する必要があるステップを定義します。ジョブとは、ワークフロー プロセスのランタイム インスタンスを指します。

たとえば、デフォルトのワークフロー プロセス `CreateUserApproveProcess` は、新規ユーザを承認するために実行する必要があるステップを定義します。CA Identity Manager で新規ユーザが実際に作成され、承認のためにそのタスクがサブミットされると、`CreateUserApproveProcess` のジョブ インスタンスが WorkPoint Designer で作成されます。

WorkPoint Designer でジョブを開いたり、表示や変更を行うためのインターフェースは、ワークフロー プロセスの編集用インターフェースと良く似ています。

同一のプロセスをベースにして、複数のジョブを共存させることができます。

ジョブのフィルタリング

WorkPoint Designer には、さまざまな基準に基づいてジョブを検索できるフィルタリング機能が組み込まれています。たとえば、以下のようなジョブを検索できます。

- 選択したワークフロー プロセス（複数可）をベースにしたジョブ
- ユーザ定義のジョブ参照または固有のジョブ ID を持つジョブ
- 特定の状態（アクティブ、完了、一時停止など）にあるジョブ
- 指定した日付範囲内に作成または開始されたジョブ

注: ジョブ フィルタリングの説明および参照情報については、WorkPoint Designer のマニュアルを参照してください。

ジョブ ステータスとプロパティ

ジョブを開くと、そのジョブのワークフロー図が表示されます。ワークフロー アクティビティのノードと移行は、実行されたかどうかを示す色付きで描画されます。

以下のものを表示し、必要に応じて変更することができます。

- ジョブのプロパティ（参加者、ジョブ履歴情報など）
- 開いているジョブの状態（完了しているかどうかなど）
- ジョブに含まれる各ノードと移行のプロパティ

アクティビティと作業アイテムのプロパティ

以下のようなジョブ アクティビティのプロパティやプロセス アクティビティのプロパティを表示し、必要に応じて変更することができます。

- アクティビティの状態情報
- アクティビティの承認情報
- 承認タスク（WorkPoint Designer では作業アイテムと呼ぶ）情報。以下に例を示します。
 - どの参加者も作業アイテムを保留していない場合は（他の承認者のワーク リストからそのアイテムが削除されます）、状態が **Available** になり、どの参加者のユーザ ID も表示されません。
 - ある参加者が作業アイテムを保留しているが、まだ完了していない場合は、状態が **Open** になり、その参加者のユーザ ID と予約時間が表示されます。
 - 作業アイテムが完了している場合は、状態が **Complete** になります。ワークフロー制御下でそのタスクを承認または拒否した参加者のユーザ ID と、完了時間が表示されます。

各作業アイテムのプロパティには、以下の情報が含まれます。

- 作業アイテムの名前と現在の状態
- 状態履歴情報（所定の状態に対して責任を持つ参加者のユーザ ID など）
- 権限が付与された作業アイテム参加者の情報

注: ジョブ、アクティビティ、作業アイテムのプロパティの詳細については、WorkPoint Designer のマニュアルを参照してください。

ワークフロー アクティビティの実行

ワークフロー プロセスでは、アクティビティ参加者として指定されたユーザによって、手動アクティビティが実行されます。アクティビティ参加者は、承認タスクと関連付けられたイベントを承認または拒否します。参加者は CA Identity Manager でこのアクティビティを実行します。

CA Identity Manager の承認タスクと関連付けられたアクティビティが実行されると、以下の処理が行われます。

1. CA Identity Manager が参加者に通知をします。
2. 参加者はタスクを承認または拒否します。
3. ワークフロー サーバがアクティビティを完了します。

参加者の検出と通知

CA Identity Manager の承認タスクと関連付けられたワークフロー アクティビティが開始されると、ワークフロー サーバからアクティビティ参加者に関する情報が CA Identity Manager に渡されます。この情報は、アクティビティ プロパティで定義されます。CA Identity Manager はこの情報を使用してアクティビティ参加者を取得し、承認タスクが保留中である旨の警告を出します。

参加者を識別すると、CA Identity Manager は各参加者のワーク リストに新しい作業アイテム（承認タスク）を追加します。オプションで、CA Identity Manager から各参加者に新しい作業アイテムに関する電子メール通知を送信することもできます。

注: APPROVERS_REQUIRED アクティビティ プロパティが **false** に設定され、参加者が検出されない場合は、デフォルトによりそのタスクは承認済みと見なされます。

注: [ステータス] 列の丸マークは、その承認タスクを任意の参加者が要求できることを示します。チェック マークは、ワーク リストの所有者が承認タスクを受け入れたが、まだタスクを完了していないことを示します。

承認タスクの受け入れと実行

参加者が検出されると、1 人の参加者が承認タスクを受け入れて、ワークフロー 制御下でそのタスクを承認または拒否するまで、アクティビティを完了することはできません。

参加者が承認タスクを受け入れるには、ワークフロー アクティビティ コンソールで作業アイテム名をクリックし、次に [アイテムの保留] をクリックします。アイテムを保留すると、他の承認者のワーク リストから削除されます。

承認タスクを受け入れた参加者は、ワークフロー制御下でそのタスクを承認するか拒否するかを決定します。また、複数の参加者が同じ承認タスクを受け入れることはできないため、その承認タスクは他の参加者のワーク リストから削除されます。

参加者が承認タスクを受け入れると、承認画面が表示されます。この画面で、参加者は以下のいずれかのアクションを実行できます。

- ワークフロー制御下でただちにタスクを承認または拒否します。
- 承認タスクを解放して、他の参加者が受け入れられるようにします。
- ダイアログ ボックスを閉じて、アクティビティを後で完了します。上記の [ユーザの作成を承認] ダイアログ ボックスを再度開くには、参加者がワーク リストで承認タスクの名前をクリックします。

また、参加者はこの承認画面で、変更可能フィールド（複数可）を必要に応じて更新できます。タスクの作成時には、この画面上のフィールドを変更可能にすることができます。

参加者がワークフロー制御下でタスクを承認または拒否すると、アクティビティが完了し、アクティビティの結果によって決定されるパスに従ってワークフロープロセスを続行できるようになります（次のセクションを参照）。

ワークフロー サーバによるアクティビティの完了

手動アクティビティは、そこから導かれる 2 つ以上の条件移行と共に、**Designer** ウィンドウに表示されます。

それぞれの条件移行には、スクリプトが関連付けられています。参加者がアクティビティを完了すると、各スクリプトがアクティビティ結果を評価します。これらの評価の結果によって、プロセス フローの方向が決まります。

以下の図に、**Designer** の「ユーザの作成を承認」アクティビティと、**CA Identity Manager** でそれに対応する同一名の承認タスクを示します。

アクティビティ参加者（または承認者）が **CA Identity Manager** で「承認」または「拒否」ボタンをクリックすると、以下のことが行われます。

1. プロセス ジョブ インスタンスの「ユーザ作成を承認」アクティビティが終了します。条件移行と関連付けられた各スクリプトは、アクティビティの結果を評価します。
2. どの条件移行の評価が **true** かに基づいて、ジョブ インスタンスを続行します。
 - アクティビティが承認された場合は、**IM WorkItem Approved** スクリプトから **true** が返されます。ワークフローは **IM WorkItem Approved** 移行を次のノードに渡します。この自動アクティビティ **IM Approve** は、**CA Identity Manager** にユーザ作成タスクを実行するよう通知します。
 - アクティビティが拒否された場合は、**IM WorkItem Rejected** スクリプトから **true** が返されます。ワークフローは **IM WorkItem Rejected** 移行を次のノードに渡します。この自動アクティビティ **IM Reject** は、**CA Identity Manager** にユーザ作成タスクをキャンセルするよう通知します。

Workpoint ジョブの表示

以下のタスクから **Workpoint** ジョブの実行時のステータスをユーザ コンソールに表示できます。

- 承認タスク
- サブミット済みタスクの表示

新規環境では、すべての承認タスクにはデフォルトで [ジョブの表示] タブが含まれています。このリリースで作成されるイベントのみが、[サブミット済みタスクの表示] で選択されたイベントまたはタスクのために呼び出されたすべてのプロセス定義に対し、ジョブ イメージの表示をサポートしています。旧リリースで作成されるイベントでは、ワークフローのジョブ ビュー機能はサポートしていません。

既存の [承認] タブへの [ジョブの表示] タブの追加

承認タスクの場合、作業アイテムのジョブ イメージを表示するには、すべての既存のタスクに新規の [ジョブの表示] タブを追加する必要があります。

注: 新規環境には、すべての承認タスクについてこのタブが含まれています。

既存のタスクに [ジョブの表示] タブを追加する方法

1. [管理タスク] および [ロール] カテゴリから、[管理タスク] - [管理タスクの変更] を選択して、**ModifyAdminTask** を実行します。
2. [検索] をクリックし、承認タスク（たとえば、[ユーザの作成を承認]）を選択してから、[選択] をクリックします。

[管理タスクの変更: ユーザの作成を承認] ダイアログ ボックスが表示されます。

3. ドロップダウン メニューから [タブ] タブをクリックし、[ジョブの表示] (JobView) を選択し、[サブミット] をクリックします。

承認タスクに、[ジョブの表示] タブが追加されます。

すべての既存の承認タスクに対して、同じ作業を繰り返します。

[Configure View Job (ジョブの表示設定)] タブ

以下を使用して、このタブを設定します。

名前

タブに割り当てる名前。

タグ

タスク内で一意なタブの識別子。文字またはアンダースコアで始まり、文字、数字、アンダースコアのみで構成される必要があります。タグは主として、XML ドキュメントまたは HTTP パラメータを通じてデータ値を設定するために使用されます。

タブの非表示

タスク中にタブを非表示にします。このオプションは、タブを非表示にする必要があるが、タブの属性にはアクセスするアプリケーションで役に立ちます。

ジョブ ビュー

このタブでは、指定された作業アイテムのジョブ イメージが表示されます。

承認タスクにおける[ジョブの表示]タブの表示

承認タスクで [ジョブの表示] タブを表示するには、以下の手順に従います。

[ジョブの表示] タブを表示する方法

1. [ワーク リスト] ダイアログ ボックスから、承認タスクを選択して表示します。
2. [ジョブの表示] タブをクリックして、タスクの実行時のステータスを表示します。

この画面から、[承認]、[拒否]、[保留] を実行するか、またはタブを閉じることができます。

あるいは、[ホーム] タブおよび [View my Worklist (マイ ワーク リストの表示)] をクリックして、[ワーク リスト] ダイアログ ボックスに戻ることができます。

イベントレベル ワークフローのワークフロージョブの表示

「サブミット済みのタスク」で、イベント レベル ワークフローのワークフロー ジョブを表示する方法

ワークフロー ジョブを表示する方法

1. 「システム」タブから、「サブミット済みタスクの表示」を選択し、検索条件を入力し、「検索」を選択します。
2. タスクを選択し、イベントを選択してからペンシルをクリックすると、イベントの詳細が表示されます。
3. 「イベント ワークフローのジョブ ビュー」下で、プロセスを選択し、ペンシルをクリックしてから、このイベントのジョブイメージを表示します。

タスクレベル ワークフローのワークフロー ジョブの表示

「サブミット済みタスクの表示」で、タスク レベル ワークフローのワークフロー ジョブを表示する方法

ワークフロー ジョブを表示する方法

1. 「システム」タブから、「サブミット済みタスクの表示」を選択し、検索条件を入力し、「検索」を選択します。
2. タスクを選択し、ペンシルをクリックしてから、タスクの詳細を表示します。
3. 「タスク ワークフローのジョブ ビュー」下で、プロセスを選択し、ペンシルを選択してから、このタスクのジョブ イメージを表示します。

ポリシーベース ワークフロー

ポリシーベース ワークフローを使用すると、ルールの評価に基づいて、ワークフロー コントロールのもとにイベントまたは管理タスクを配置できます。これにより、常にイベントや管理タスクによりワークフロー プロセスが開始されるのではなく、イベントまたは管理タスクに関連付けられたルールが **True** である場合にワークフロー プロセスにより作業アイテムが実行および生成されます。

承認ルールは、ワークフロー プロセスを開始するかどうかを決定する条件です。ワークフロー プロセスが開始されると、イベントまたは管理タスクはワークフロー コントロールのもとに配置され、承認者の作業リストに作業アイテムが追加されます。

承認ポリシーは、承認ルール、ルールの評価タイプ、ポリシー順序、ポリシーの説明、およびワークフロー プロセスを組み合わせたものです。

たとえば、新規のグループを作成する場合、新しいグループが、指定された親組織の一部門である場合のみ、**CreateGroupEvent** をワークフロー コントロールの下に配置し、作業アイテムを作成するように承認ポリシーを定義できます。新規グループがその組織の一部門でない場合は、ワークフロー プロセスは実行されず、作業アイテムは作成されません。

イベントに複数のルールがある場合、そのイベントを承認するには、イベントに関連付けられたすべてのワークフロー プロセスを承認する必要があります。同様に管理タスクでも、ワークフロー制御のもとに **CreateGroupTask** を配置する承認ポリシーを定義し、新しいグループの名前が「セールス」で始まる場合にのみ作業アイテムを作成できます。新しいグループの名前が「セールス」で始まらない場合、ワークフロー プロセスは実行されず、作業アイテムも作成されません。

常時評価を行うか、または管理対象オブジェクトの指定された属性が変化した場合（従業員の給与の値が変化した場合など）のみに評価を行うかのポリシー ルールを作成できます。

注: 以前のバージョンのポリシー ベース ワークフローでは、承認者が属性を変更すると再承認のためにサブミットされました。属性レベルの承認および拒否により、どの段階の変更も 1 回のみ承認されます。ルールに含まれる属性が変更された場合でも、作業アイテムが再承認のためにサブミットされることはありません。承認者が変更を承認すると、新しい変更がサブミットされるか、タスクが再サブミットされるまでは、その作業アイテムを見ることはありません。

ワークフロー プロセス

すべてのワークフロー テンプレートおよびあらかじめ定義されたワークフロー プロセスにより、以下に示すようにワークフロー ルールがサポートされます。

- **プロセス テンプレート** – これらのテンプレートを使用することで、承認者（または参加者リゾルバ）をユーザ コンソールに設定できます。
- **あらかじめ定義されたワークフロー プロセス** – これには、WorkPoint Designer での、参加者リゾルバの設定が必要となります。

また、ワークフロー ルール用のカスタム ワークフロー プロセスを作成することも可能です。

ルールのオブジェクト

CA Identity Manager 管理者は、次のオブジェクトに基づいて、イベントまたは管理タスク用の承認ポリシーを作成できます。指定されたイベントに適用されイベント実行中でも存在する場合の、イベント用のオブジェクトを以下に示します。

- **タスクの開始ソース** – タスクを実行する CA Identity Manager 管理者。
- **イベントのプライマリ オブジェクト** – イベントと関連付けられるプライマリ オブジェクト。
- **イベントのセカンダリ オブジェクト** – プライマリ オブジェクトに対応する、イベントと関連付けられているセカンダリ オブジェクト。

管理タスク用のオブジェクトを以下に示します。

- **このタスクのプライマリ オブジェクト** – タスクと関連付けられるプライマリ オブジェクト。
- **タスクの開始ソース** – タスクを実行する CA Identity Manager 管理者。
- **アイデンティティ ポリシー違反** – アイデンティティ ポリシー違反の場合、ルールは、違反したアイデンティティ ポリシーのポリシー名に基づきます（例：Policy Name EQUALS TitlePolicy）。違反メッセージは [承認] 画面の [タスク詳細] タブに表示されます。これは [サブミット済みタスクの表示] の [タスク詳細] と同じです。SOD 違反メッセージは [アイデンティティ ポリシー違反] という見出し名の新しいセクションの下に表示されます。承認者はこれらのメッセージを確認して、タスクを承認するか拒否するかを決定できます。

注：ルールがアイデンティティ ポリシー違反に基づいている場合、評価は通常の評価とは異なるものになります。一度承認された SOD 違反は、その SOD 違反を真と評価する可能性のある他のルールが存在する場合でも、他のワークフロープロセスを呼び出しません。通常の評価では、同じ変更が他の承認者によって承認されている場合でも、すべてのワークフロー プロセスが 1 つずつ呼び出されます。

ルールの評価

ポリシー ルールは、1つのイベントに対して以下の2つの方法で評価することができます。

■ 常時

評価タイプが「Always」のポリシーは、ポリシーに含まれる属性が変更されたかどうかに関わらず、そのポリシーが「True」と評価されると開始されます。評価タイプが「Always」のポリシーの結果として生成された作業アイテムの承認画面で、承認者は編集可能な属性を変更できます。

注: 承認者が[拒否] ボタンをクリックすると、イベントは拒否されます。

「Always」の場合、評価タイプの動作はタスクおよびイベントの場合と同じです。

■ 承認条件に指定した属性が変更された場合のみ

評価タイプが「OnChange」のポリシーは、ポリシーが「True」と評価され、ポリシーに含まれるいずれかの属性が変更された場合にのみ開始されます。評価タイプが「OnChange」のポリシーの結果として生成された作業アイテムの承認画面で、承認者がポリシーに含まれるこれらの属性の値を変更できるのは、これらの属性に承認画面の読み書き許可がある場合のみです。承認画面上のその他のすべての属性は、読み取り専用の許可を与えられています。

注: イベント レベル ワークフローでは、承認者が[拒否] ボタンをクリックすると、承認ポリシーに含まれる属性への変更のみが拒否され、次の承認ポリシーが評価されます。

タスク レベル ワークフローでは、承認者が[拒否] ボタンをクリックすると、イベントは拒否されます。

注: 「OnChange」および「Always」の両方のタイプで、承認者がすべての変更を取り消して[承認]をクリックすると、変更は拒否または監査されます。

ルールの評価の例

たとえば、以下のポリシーについて考えてみます。これらはすべて、[ユーザーの変更] 管理タスクの ModifyUserEvent 用のポリシーです。

ポリシー	ルール	評価
Policy1	User where (User ID = Smith01)	常時
Policy2	User where (Title = Manager)	Title 属性が変更された場合
Policy3	User where (Salary >= 80000)	Salary 属性が変更された場合

Policy1 は、管理者がユーザ **Smith01** の [ユーザの変更] タスクを呼び出した場合に評価されます。どの属性が変更されたかは関係ありません。

Policy2 は、管理者が [ユーザの変更] タスクを呼び出して、任意のユーザ オブジェクトの **Title** 属性を変更した場合に評価されます。 **Policy2** は **Title** 属性が **Manager** に変更された場合に真になります。

Policy3 は、管理者が [ユーザの変更] タスクを呼び出して、任意のユーザ オブジェクトの **Salary** 属性を変更した場合に評価されます。 **Policy3** は **Salary** 属性が **80000** 以上に変更された場合に真になります。

この例では、管理者が [ユーザの変更] タスクを使用してユーザ **Smith01** の **Title** 属性を **Manager** に変更すると、**Policy1** と **Policy2** の両方が真に評価され、それぞれのワークフロー プロセスが開始されます。この場合、標準的な優先度が適用されます。

条件付きルールの評価により、イベントの保留中に、ある作業項目の承認者が、同じイベントの他の作業項目に影響を与える属性を変更できるようになります。これが可能なのは、評価タイプが「**Always**」の承認ポリシーのみです。前述の例では、管理者がユーザ **Smith01** の属性を変更すると、**Policy1** が真となり、作業項目が生成されます。承認者は、**Policy1** によって生成された作業項目を承認する一方で、同じ承認画面で **Smith01** の **Salary** 属性を変更することが可能です。この場合、**Smith01** の新しい **Salary** の値によって、**Policy3** が同じ **ModifyUserEvent** のインスタンスの作業項目を生成するかどうかが決まります。承認者が **Salary** 属性を **90000** に変更すると、**Policy3** は新しい作業項目を生成します。この作業項目は、イベント自体が承認される前に承認されている必要があります。標準的な優先度が適用されます。

ポリシー順序

すべての承認ポリシーには、ポリシー順序フィールドが含まれています。このフィールドでは、昇順の正の整数値により優先度を指定します。各ポリシーの優先度により、以下が決まります。

- 承認ルールを評価する順序
- ルールが **True** である場合には、ワークフロー プロセスが開始される順序

ポリシー順序の整数値が小さいポリシーほど優先度は高くなり、そのルールは、整数値の大きいポリシーより先に評価されます。あるイベントまたは管理タスクに対して **True** であるすべてのポリシーにおいては、優先度が最も高いポリシーのワークフロー プロセスが最初に開始されます。

ポリシー順序の例

この簡単な例では、ポリシーの順番付けがどのように機能するかを示しています。この例では、ポリシールールが常に評価されていることを前提としています。

あるイベントに、常に評価される複数のポリシーがある場合に、そのイベントそのものを承認するためには、すべてのポリシーを承認する必要があります。ただし、イベントに関連付けられているポリシー評価タイプ「ALWAYS」のポリシーが1つ拒否されると、イベント自体も拒否されます。

注: イベントに関連付けられているポリシーの評価タイプが「Onchange」の場合、そのポリシーに含まれる属性に関連付けられた変更のみが拒否されます。イベント自体は拒否されず、次のポリシーが評価されます。

この例では、Policy1、Policy2、および Policy3 すべてのポリシー評価タイプは「ALWAYS」です。Policy1 は False と評価され、Process1 と名付けられたワークフロープロセスは実行されず、User1 の作業アイテムは生成されません。イベント制御は、即座に Policy2 に渡されます。Policy2 および Policy3 は、両方とも True と評価されました。優先度が高いため、ワークフロー Process2 が最初に実行され、User2 の作業アイテムが生成されます。

User2 がその作業アイテムを承認すれば、ワークフロー Process3 が実行され、User3 の作業アイテムが生成されます。次に、User3 がその作業アイテムを承認することで、イベントそのものが承認されます。これらのアクションを、以下のテーブルに示します。

優先度	ポリシー	結果	ワークフロー	承認者	アクション
1	Policy1	False	Process1	User1	—
2	Policy2	True	Process2	User2	承認済み
3	Policy3	True	Process3	User3	承認済み

しかし、User2 がその作業アイテムを拒否する場合には、イベントそのものが拒否され、次の表に示すように、User3 には作業アイテムは生成されません。

優先度	ポリシー	結果	ワークフロー	承認者	アクション
1	Policy1	False	Process1	User1	—
2	Policy2	True	Process2	User2	拒否

優先度	ポリシー	結果	ワークフロー	承認者	アクション
3	Policy3	True	Process3	User3	—

次に、Policy1、Policy2、および Policy3 すべてのポリシー評価タイプは「ONCHANGE」です。User2 が作業アイテムを拒否した場合、Policy2 に含まれる属性に関連した変更のみが拒否されます。次に Policy3 が評価され、Workflow Process3 の実行および作業アイテムまたは User3 の生成が行われます。User3 が作業アイテムを拒否した場合、このイベントへのすべての変更が拒否されるため、イベントは拒否されます。User3 が作業アイテムを承認した場合、イベントは承認され、Policy3 に含まれる属性の変更は永続化されます。

優先度	ポリシー	結果	ワークフロー	承認者	アクション
1	Policy1	False	Process1	User1	—
2	Policy2	True	Process2	User2	拒否
3	Policy3	True	Process3	User3	承認済み

ポリシーの説明

オプションの検索不能な文字列の説明属性が承認ポリシーの管理対象オブジェクトに追加され、結果である作業アイテム上に表示されます。

サポートされる最大文字数：255 文字

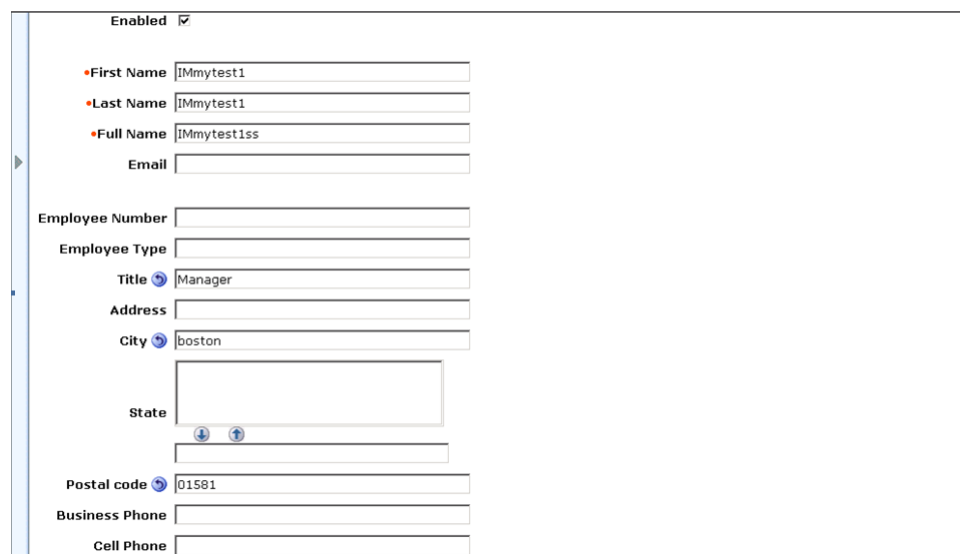
説明には以下の形式でバンドル/キー情報を入力できます。

\$ (bundle=<完全修飾リソース バンドル名> : key=<キー>)

承認画面での変更された属性の強調表示

承認者がどの属性が変更されたかを知り、必要に応じてこれらの属性への変更を元に戻せるようにするため、承認者のプロフィール画面に取り消しアイコンが追加されました。これで承認者に、この属性が変更されたことを知らせます。

承認者は取り消しボタンをクリックして元の値を見ることができ、属性の値をほかの値に変更することもできます。



The screenshot shows a user profile form with the following fields and values:

- Enabled:** ☒
- First Name:** IMmytest1 (highlighted with a red dot)
- Last Name:** IMmytest1 (highlighted with a red dot)
- Full Name:** IMmytest1ss (highlighted with a red dot)
- Email:** (empty)
- Employee Number:** (empty)
- Employee Type:** (empty)
- Title:** Manager (with a blue circular icon containing a white 'X' for cancel)
- Address:** (empty)
- City:** boston (with a blue circular icon containing a white 'X' for cancel)
- State:** (empty)
- Postal code:** 01581 (with a blue circular icon containing a white 'X' for cancel)
- Business Phone:** (empty)
- Cell Phone:** (empty)

承認ポリシーおよび複数値属性

ルールが複数値属性用に設定されている場合、このルールを新しく追加または削除された複数属性の値にのみ適用させる方法はありませんでした。複数値属性に基づくポリシーの評価タイプを見ることで、これを行うことができるようになりました。ルール評価タイプが **Onchange** の場合、このルールは複数値属性の新規追加または削除された値にのみ適用され、複数値属性のすべての値に適用されるわけではありません。

ルールが複数値属性のすべての値に基づく必要がある場合（新規追加または削除されたかどうかに関わらず）、そのルールの評価タイプは「常に」とします。

複数値属性に加えられた変更は、プロフィール画面上で「元に戻す」アイコンと共に強調表示されます。複数値属性に新しい値が追加または削除されたためにルールが「TRUE」と評価された場合、この変更を承認する承認者には、複数値属性に含まれるすべての値が表示されます。「元に戻す」アイコンをクリックすると、属性の値が元の値に戻ります。承認者が削除された値を確認したい場合、「元に戻す」アイコンをクリックして元の値を表示させます。

「やり直し」アイコンをクリックすると新しい値が表示され、承認者はどの値が削除され、どの値が追加されたかを区別できます。「承認」ボタンをクリックして、この複数値属性のすべての変更を承認します。「拒否」ボタンをクリックして、この複数値属性のすべての変更を拒否します。この複数値属性に関連するすべての後続のポリシーは、複数値属性の新しい差分値がない限り評価されません。

注: 複数値属性に基づくルールでは、複数値属性に含まれる値は実行値であり、表示値ではありません。たとえば、州（都道府県）「MA」の表示値は「マサチューセッツ」です。州属性に基づく承認ポリシーを作成する場合、ルールは `state=MA` のようになる必要があります。

たとえば、以下のポリシーについて考えてみます。これらはすべて、「ユーザーの変更」管理タスクの `ModifyUserEvent` 用のポリシーです。

ポリシー	ルール	評価
Policy1	次の条件を満たすユーザー (State = OnChange MA)	
Policy2	次の条件を満たすユーザー (State = 常時 DC)	

管理者が [ユーザの変更] タスクを開始して州属性を変更し、州属性において MA が追加または削除した場合に true であるか評価するたびに Policy1 が評価されます。

Policy 2 は、管理者が州に値 DC を含むユーザのための [ユーザの変更] タスクを開始するたびに評価されます。

ワークフロー承認画面で属性が変更済みとして強調表示される

承認画面で、管理者が元のタスクで変更していなくても、追加属性が変更済みとして強調表示される場合があります。これは、この画面に含まれる様々な属性の値を変更できるスクリプトがこの画面に含まれているためです。これは、画面の初期化、または他の一部の属性の画面検証の一環として行われます。

ポリシーの例

以下のビジネスでの使用事例は、イベントのワークフロー承認ポリシーの適用方法を示しています。

事例 1

使用事例 – 管理者は、ある従業員のリレーショナルデータベース用のアカウントを変更します。

管理タスク – ModifyMSSQLAccount

イベント – ModifyMSSQLAccountEvent

承認ルール – 次の条件を満たすユーザ (Title = RDBAcctManager)

ワークフロー プロセス – ModAcctApproval (カスタム ワークフロー プロセス)

オブジェクト – タスクの開始ソース

評価 – 常時ルールを評価

事例 2

使用事例 – 管理者は、新たな昇給制度を反映するため、従業員の給与を変更します。

管理タスク – [ユーザの変更]

イベント – ModifyUserEvent

承認ルール- 次の条件を満たすユーザ (Salary >= 100000)

ワークフロー プロセス - SalaryChangeApproval (カスタム ワークフロー プロセス)

オブジェクト- イベントのプライマリ オブジェクト (ユーザ)

評価- [Salary] 属性が変化した場合のみ評価

事例 3

使用事例- 管理者は、あるユーザの肩書が契約社員に変わったときに、契約社員グループに 1 人のユーザを追加します。この事例は、以下の 2 つの承認ポリシーに分割することができます。

ポリシー 1 :

管理タスク - [ユーザの変更]

イベント- ModifyUserEvent

承認ルール- 次の条件を満たすユーザ (Title = Contractor)

ワークフロー プロセス - SingleStepApproval (デフォルトのプロセス テンプレート)

オブジェクト- イベントのプライマリ オブジェクト (ユーザ)

評価- [役職] 属性が変化した場合のみ評価

ポリシー 2 :

管理タスク - [グループの変更] (または [グループメンバシップの変更])

イベント- AddToGroup

承認ルール- 以下の条件を満たすグループ (Group Name = Contractors)

ワークフロー プロセス - SingleStepApproval (デフォルトのプロセス テンプレート)

オブジェクト- イベントのセカンダリ オブジェクト (グループ)

評価 - 常時ルールを評価

以下のビジネスでの使用事例は、タスクのワークフロー承認ポリシーの適用方法を示しています。

事例 1

使用事例 – 管理者は、ある従業員の Active Directory アカウントを変更します。

管理タスク – ModifyActiveDirectoryAccount

オブジェクト – タスクの開始ソース

承認ルール – 次の条件を満たすユーザ (Title = ActiveDirectoryManager)

ワークフロー プロセス – シングル ステップ承認

評価 – 常時ルールを評価

事例 2

使用事例 – 管理者は、従業員コードが HighSecurity のユーザを変更します。

管理タスク – [ユーザの変更]

オブジェクト – このタスクのプライマリ オブジェクト

承認ルール – 次の条件を満たすユーザ (employeenumber = HighSecurity)

ワークフロー プロセス – シングル ステップ承認

評価 – 常時ルールを評価

事例 3

使用事例 – 管理者は、ユーザを変更して管理ロール「CheckApprover」および「CheckSigner」を割り当てます。

管理タスク – [ユーザの変更]

オブジェクト – アイデンティティ ポリシー違反

承認ルール – 次の条件を満たすアイデンティティ ポリシー (Name = CheckRoles)

ワークフロー プロセス – シングル ステップ承認

評価 – 常時ルールを評価

ポリシーベースのイベント用ワークフローの設定方法

ポリシーベース ワークフローを設定する手順は、イベント レベル ワークフローを設定する手順に類似していますが、ワークフローを実行するかどうかを決定する承認ポリシーの定義ステップがあります。

ポリシーベース ワークフローの設定方法

1. ユーザ コンソールで、[ルールおよびタスク] - [管理タスク] - [管理タスクの変更] または [管理タスクの作成] を選択します。
[管理タスクの選択] 画面が表示されます。
2. ワークフロー制御下で実行するタスクを検索して、[選択] をクリックします。
[管理タスクの変更] または [管理タスクの作成] 画面が表示されます。
3. [プロファイル] タブで、[ワークフローの有効化] がチェックされているかどうかを確認します。
4. [イベント] タブで、イベントを選択して、プロセス テンプレートにマッピングします。
ワークフローのマッピングの画面が表示されます。
5. [ポリシー ベース] ラジオ ボタンを選択し、[追加] をクリックします。
[承認ポリシー] 画面が表示されます。
6. [承認ポリシーを設定します。](#) (P. 351)
7. 選択したワークフロー プロセスに必要な参加者リゾルバを設定します。
参加者のリクエストがプロセスに追加されます。
8. [OK] をクリックします。
CA Identity Manager によってイベント レベルのワークフロー設定が保存されます。
9. [サブミット] をクリックします。
CA Identity Manager によってタスクの変更が処理されます。

注: ワークフロー プロセス リストには、テンプレート メソッドと WorkPoint メソッドの両方で使用するプロセスが含まれています。

- テンプレート メソッド プロセス (SingleStepApproval、TwoStageApprovalProcess または EscalationApproval のいずれか) が選択されると、ページが展開されて、参加者リゾルバの設定が有効になります。
- WorkPoint メソッド プロセスが選択されているとき、ページは展開しません。参加者リゾルバは WorkPoint Designer で設定されます。

ポリシーベースのタスク用ワークフローの設定方法

ポリシーベースのタスク用ワークフローを設定する手順は、タスク レベル ワークフローを設定する手順に類似していますが、ワークフローを実行するかどうかを決定する承認ポリシーの定義ステップがあります。

ポリシーベース ワークフローの設定方法

1. ユーザ コンソールで、[ルールおよびタスク] - [管理タスク] - [管理タスクの変更] または [管理タスクの作成] を選択します。
[管理タスクの選択] 画面が表示されます。
2. ワークフロー制御下で実行するタスクを検索して、[選択] をクリックします。
[管理タスクの変更] または [管理タスクの作成] 画面が表示されます。
3. [プロファイル] タブで、[ワークフローの有効化] がチェックされているかどうかを確認します。
4. [プロファイル] タブで、[ワークフロー プロセス] フィールドのとなりにある鉛筆のアイコンをクリックします。
ワークフローのマッピングの画面が表示されます。
5. [ポリシー ベース] ラジオ ボタンを選択し、[追加] をクリックします。
[承認ポリシー] 画面が表示されます。
6. [承認ポリシーを設定します。](#) (P. 351)
7. 選択したワークフロー プロセスに必要な参加者リゾルバを設定します。
参加者のリクエストがプロセスに追加されます。
8. [OK] をクリックします。

CA Identity Manager によってタスク レベルのワークフロー設定が保存されます。

9. [サブミット] をクリックします。

CA Identity Manager によってタスクの変更が処理されます。

注: ワークフロー プロセス リストには、タスクレベルのポリシーベース ワークフロー用のテンプレート メソッドと共に使用するプロセスが含まれます。

- テンプレート メソッド (SingleStepApproval または TwoStageApprovalProcess のいずれか) が選択されると、ページが展開されて、参加者リゾルバの設定が有効になります。

詳細情報

[承認ポリシーの設定方法](#) (P. 351)

承認ポリシーの設定方法

イベントまたはタスクの承認ポリシーを設定するには、以下の手順が必要です。

1. テスト対象のオブジェクトを選択します。
2. そのオブジェクトの承認ルールを定義します。
3. プライマリ オブジェクトの場合、これが条件付きの評価であるかどうかを判断します。
4. ポリシー評価の順序を入力します。
5. そのルールが **True** である場合に実行するワークフロー プロセスを設定します。

承認ポリシーを設定する方法

1. [承認ポリシー] 画面で、テストするルールの対象オブジェクトをドロップダウン リストから選択します。
行った選択を反映して、画面が変化します。
2. オブジェクト名の横にある新しいドロップダウン メニューから、条件式テンプレートを選択します。
行った選択を反映して、画面が変化します。
3. 必要に応じて条件式を作成および編集します。
4. [ルールの評価] オプション ボタンを選択して、ルールの評価を常時行うか、承認条件の属性が変更された場合にのみ行うかを示します。
5. 正の整数値を入力して、ポリシーの評価順序（そのイベントに対して複数のポリシーが存在する場合）を指定します。
6. そのルールが **True** と評価された場合に実行するワークフロー プロセスの選択および設定を行います。
7. [OK] をクリックして、承認ポリシーを保存します。

ポリシーベースのワークフロー ステータス

CA Identity Manager 管理者は、以下に示す標準的なシステム ツールを使用して、ワークフロー承認ポリシーを含むタスクのステータスを表示できます。

- [サブミット済みタスクの表示] タブ
- [ユーザ履歴] タブ
- レポートとログ

サブミットされたタスクおよびタスク履歴情報には、以下のようなものがあります。

- タスクおよびイベント情報
- ワークフローおよび承認ルール情報
- 承認ルールの評価結果

サブミット済みタスクの履歴の説明については、[システム] タブ関連文書を参照してください。

グローバル イベントレベルのポリシーベースのワークフロー マッピング

現在、イベントは管理コンソールからのワークフロー プロセスにマッピングするか、特定のタスク内でポリシーベースのワークフロー承認ポリシーと関連付けることができます。新しい「グローバル ポリシーベースのイベント用ワークフローの設定」タスクにより、管理者はポリシーベースのワークフロー マッピングを環境レベルで設定できます。管理者タスクにおけるイベント用のポリシーベースのワークフローの設定とは異なり、設定済みポリシーベースのワークフロー マッピングはイベントを生成するすべてのタスクに適用されます。

注: 「グローバル ポリシーベースのイベント用ワークフローの設定」タスクは、ワークフローが有効化されている場合にのみ作動します。ワークフローが無効化されているときにこのタスクを実行すると、エラーが発生します。

このタスクは [システム] タブに追加されています。タスクがサブミットされると、このタスク内の各イベントのワークフロー プロセスが次の方法で取得されます。

管理タスクのイベント用に設定されたワークフローが優先されます。イベントはポリシーベースと非ポリシーベースのワークフローどちらにも設定できます。ポリシーベースのワークフローが管理タスクのイベント用に設定された場合、このワークフロー プロセスが開始されます。ルールが一致しない場合、イベント用のワークフローは開始されません。同じように、非ポリシーベースのワークフローが管理タスクのイベント用に設定された場合、このワークフロー プロセスが開始されます。管理タスクのイベント用にワークフローが設定されていない場合、そのイベントのグローバル ワークフロー設定が優先されます。

グローバル ポリシー ベースのイベント用ワークフローの設定タスク画面

「グローバル ポリシー ベースのイベント用ワークフローの設定」タスクでは、管理者は現在の環境におけるすべてのイベントのポリシーまたは非ポリシー ベースのワークフローを設定できます。タスクをクリックすると、ワークフロー プロセス定義へのデフォルトのイベント マッピングが表示されます。各イベント マッピングは変更または削除でき、設定されていないイベント用に新しいイベント マッピングを追加できます。

ホーム ユーザ 組織 グループ **ルールおよびタスク** エンドポイント ポリシー 電子メール レポート システム

タスク

グローバル ポリシー ベースのイベント用ワークフローの設定

この環境のイベントに関連するワークフロー プロセス。

イベント名	ワークフロー プロセス
AssignAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
編集 CertifyRoleEvent	CertifyRoleApproveProcess
CreateGroupEvent	CreateGroupApproveProcess
CreateOrganizationEvent	CreateOrganizationApproveProcess
CreateUserEvent	CreateUserApproveProcess
DeleteGroupEvent	DeleteGroupApproveProcess
DeleteOrganizationEvent	DeleteOrganizationApproveProcess
DeleteUserEvent	DeleteUserApproveProcess
ModifyOrganizationEvent	ModifyOrganizationApproveProcess
RevokeAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess
SelfRegisterUserEvent	SelfRegistrationApproveProcess

マッピングの新規追加

イベント AccountChangePasswordEvent

追加

この画面のフィールドを以下に示します。

この環境のイベントに関連するワークフロー プロセス。

承認ポリシーに関連付けられたワークフロー プロセスを指定します。

マッピングの新規追加

ワークフロー プロセスにマッピングする承認ポリシーを指定します。

[追加]ボタン

新しいマッピングを追加します。

マッピングを追加または変更することにより、プロセス マッピングおよび承認ポリシーを選択できる「ワークフロー マッピング」画面が開きます。動作はイベント レベルのワークフロー設定と同じです。「ワークフロー マッピング」ページの「追加」ボタンをクリックすると、承認ポリシーを設定できる別のページが開きます。

詳細情報

[ポリシーベースのイベント用ワークフローの設定方法](#) (P. 349)

[承認ポリシーの設定方法](#) (P. 351)

グローバル ポリシー ベースのイベント用ワークフローの設定

グローバル ポリシー ベースのイベント用ワークフローを設定するタブです。

Name

タブに割り当てる名前。

タグ

タスク内で一意なタブの識別子。文字またはアンダースコアで始まり、文字、数字、アンダースコアのみで構成される必要があります。タグは主として、XML ドキュメントまたは HTTP パラメータを通じてデータ値を設定するために使用されます。

タブの非表示

タスク中にタブを非表示にします。このオプションは、タブを非表示にする必要があるが、タブの属性にはアクセスするアプリケーションで役に立ちます。

ユーザ検索画面

ユーザの表示用に用いる検索画面を定義します。

ユーザリスト画面

このタブで列と並べ替えを決定する画面を制御します。

グループ検索画面

グループの表示用に用いる検索画面を定義します。

グループリスト画面

このタブで列と並べ替えを決定する画面を制御します。

管理ロール検索画面

管理ロールの表示に使用する検索画面を定義します。

管理ロールリスト画面

このタブで列と並べ替えを決定する画面を制御します。

管理タスク検索画面

管理タスクの表示に使用する検索画面を定義します。

管理タスクリスト画面

このタブで列と並べ替えを決定する画面を制御します。

オンライン リクエスト

CA Identity Manager では、汎用のオンライン リクエスト タスクを作成できます。デフォルトのオンライン リクエストの実装は、自己変更リクエストと管理ユーザ変更リクエストの両方の関連タスク セットで構成されます。ただし、オンライン リクエスト機能は、他の CA Identity Manager リクエスト タスクに対しても簡単に実装できます。

ユーザ変更リクエストによって、作業アイテムを生成するワークフロー プロセスがトリガされます。ワークフロー参加者は、作業アイテムを承認して実装するか、拒否することができます。タスクを開始するユーザは、履歴エディタ（リクエストの履歴を保守するために CA Identity Manager が使用するテキスト領域）にリクエストの説明を入力します。この履歴エディタは、参加者が作業アイテムに対して実行したアクションについてコメントを残せるように設定することができます。これらのコメントは、累積的な作業アイテム履歴の一部になります。

標準の承認アクションと拒否アクションのほかに（あるいはその代わりに）新しいアクションを実行することもできます。たとえば、ビジネス参加者がリクエストの明確化やコメント作成をしたり、技術参加者がリクエストを実装することができます。これらの新しいアクティビティは、[明確化] や [実装] などの新しいワークフロー アクション ボタンで表現できます。これらのボタンは、承認タスク上の標準の [承認] ボタンと [拒否] ボタンに加えることができます。

オンライン リクエスト タスク

デフォルトのオンライン リクエストの実装内容を構成する連携タスクは 5 つあります。これらのタスクは、カスタム リクエスト、履歴、ワークフロー アクション ボタンの使用法を示します。

注: 管理タスク（[マイ アカウントの変更]、[オンライン リクエストの作成]）は、デフォルトによりコンサルテーション プロセス テンプレートを使用するイベント レベルのワークフロー用に設定されます。

マイ アカウントの変更

ユーザ アカウントの変更リクエストを作成する自己変更管理タスクです。このタスクの [リクエスト] タブには、リクエストについて記述するための履歴エディタがあり、[プロファイル] タブには読み取り専用のユーザ詳細が表示されます。

オンライン リクエストの作成

特定のユーザに対するアカウント変更リクエストを作成するユーザ変更管理タスクです。[リクエスト] タブには、リクエストについて記述するための履歴エディタがあり、[対象プロファイル] タブには読み取り専用のユーザ詳細が表示されます。

オンライン リクエストの承認

ビジネス参加者がタスクの承認または拒否、あるいはタスクの明確化リクエストを行うことを許可する承認タスクです。このタスクの[リクエスト]タブには、履歴表示とクエリまたはコメント用の履歴エディタ、読み取り専用の[対象プロファイル] タブ、および[担当者] タブがあります。

オンライン リクエストの明確化

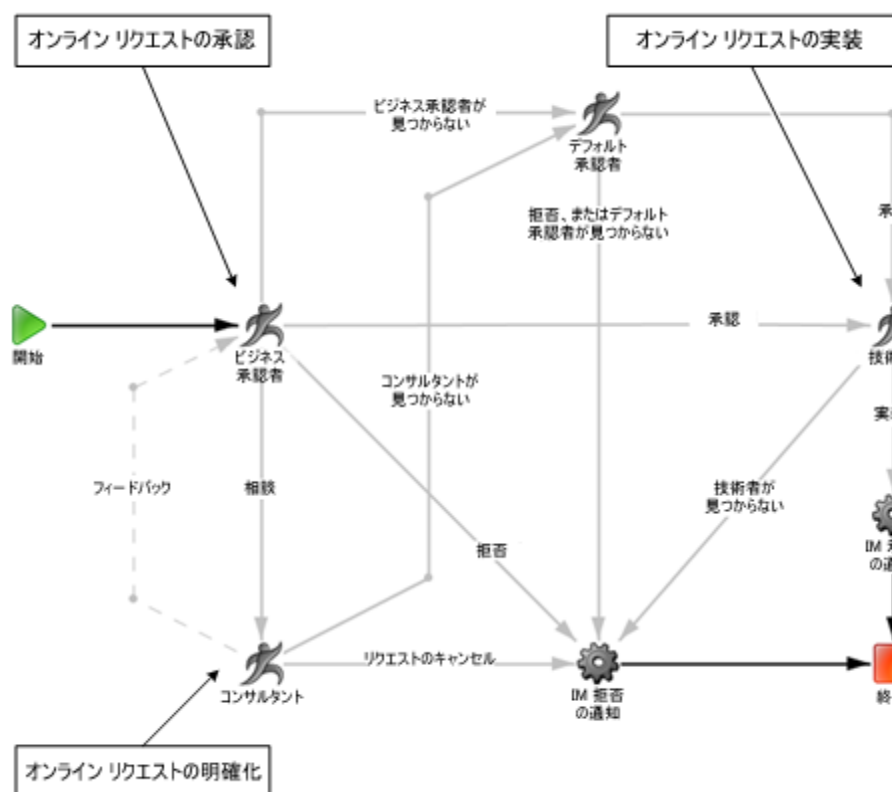
明確化の参加者が明確化リクエストに応答し、承認のためにビジネス参加者にタスクを返送することを許可する承認タスクです。[リクエスト] タブには、履歴表示とコメント用の履歴エディタ、および読み取り専用の[対象プロファイル] タブがあります。

オンライン リクエストの実装

技術参加者がタスクを実装し、タスク履歴にコメントを追加することを許可する承認タスクです。[実装リクエスト] タブには、履歴表示とコメント用の履歴エディタ、読み取り専用の[対象プロファイル] タブ、および[担当者] タブがあります。

オンライン リクエスト プロセス

オンライン リクエスト タスクは、コンサルティング プロセスと呼ばれるワークフロー プロセス テンプレートによって制御されます。このテンプレートは、WorkPoint Designer では以下のように示されます。



コンサルティング プロセスには、以下の 4 つの手動アクティビティが含まれます。これらは、オンライン リクエスト実装の承認タスクに対応しています。

- 作業アイテムを拒否するか、作業アイテムを承認して技術者に渡すか、コンサルタントからさらに明確化をリクエストするビジネス承認者のアクティビティ。
- 作業アイテムを明確化し、ビジネス承認者に返送するコンサルタントのアクティビティ。
- ビジネス承認者またはコンサルタントと連絡が取れない場合に引き継ぐデフォルト承認者のアクティビティ。
- リクエストを実装し、作業アイテムを完了する技術者のアクティビティ。

オンライン リクエスト履歴

オンライン リクエスト履歴機能を使用すると、参加者は作業アイテムに対するアクションの記録を作成できます。作業アイテムは、ある参加者から別の参加者に渡す必要があるため、新しい参加者はアクションを実行する前に、作業アイテム履歴を確認することができます。

オンライン リクエスト履歴の実装には、以下の 2 つのコントロールが使用されます。

- 履歴表示は、以前の履歴エントリの詳細情報が時系列順に含まれた読み取り専用テーブルです。
- 履歴エディタは、新しい履歴エントリを作成するためのテキストボックスです。また、作業アイテムをサブミットせずに、複数のエントリを追加できるオプションボタンもあります。

デフォルトにより、履歴エディタと履歴表示は、オンライン リクエスト実装と関連付けられたすべてのタスクの「リクエスト」タブに表示されます。以下の画面に、「オンライン リクエストの明確化」タスクの履歴コントロールを示します。

オンライン リクエストの明確化

リクエストの明確化 対象プロフィール

あなたのリクエストの承認権限を持つユーザが、プロセスを進める前に追加情報をリクエストしています。彼らのコメントは、リクエスト履歴上で明白になっていなければなりません。追加情報を提供の上、「戻る」をクリックしてリクエストを承認者に返送してください。または、「キャンセル」をクリックしてリクエストを取り消します。

リクエスト、および履歴:

ソース	説明	時刻
"リクエスタ"として行動している "SuperAdmin (SuperAdmin)" によるユーザ コメント	オーストラリアの販売担当者に変更。	2008-05-13 15:36:45.937
"承認者"として行動している "SelfRegUser (SelfReg)" によるユーザ コメント	私達はオーストラリアの担当者が必要なため、彼女はシドニーに移転します。	2008-05-13 15:38:35.267
"リクエスタ"として行動している "SuperAdmin (SuperAdmin)" によるユーザ コメント	彼女はニュージーランドも担当しますか？	2008-05-13 15:45:45.937

追加情報

履歴エディタ

履歴を表示

歴史イベントを追加

リターン キャンセルのリクエスト 準備アイテム 閉じる

オンライン リクエストの使用

以下に、オンライン リクエストのワークフロー プロセスのステップを示します。各手順のかつこ内に、生成される IM タスクを示します。プロセスの各ステップでは、参加者が履歴エディタでコメントを追加することができます。このコメントは履歴表示に示され、ワークフロー プロセスの次の参加者が見ることができます。

1. タスク開始者が **CA Identity Manager** ユーザの変更をリクエストします（[オンライン リクエストの作成]）。
2. 業務系承認者が作業アイテムを受け取り、以下のいずれかを行います。
 - 作業アイテムを承認します（[オンライン リクエストの承認]）。
 - 作業アイテムを拒否し、ワークフロー プロセスを終了します。新しいタスクは生成されません。
 - コンサルタントからの明確化をリクエストします（[オンライン リクエストの明確化]）。
3. コンサルタントが作業アイテムを受け取り、以下のいずれかを行います。
 - 明確化を追加し、作業アイテムを業務系承認者に返します。新しいタスクは生成されません。
 - 作業アイテムをキャンセルし、ワークフロー プロセスを終了します。新しいタスクは生成されません。
4. 技術者が作業アイテムを受け取り、リクエストを実装します（[オンライン リクエストの実装]）。

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

CA Identity Manager の承認タスクには、始めから [承認] ボタンと [拒否] ボタンが用意されています。これらのボタンは、対応する作業アイテム画面に表示されます。ワークフロー アクション ボタンでは、管理者が承認タスクにアクション ボタンを追加したり、既存のボタンを削除または変更して、**CA Identity Manager** のタスクとワークフローの機能を拡張することができます。（標準の [承認] ボタンと [拒否] ボタンは、カスタム ワークフロー アクション ボタンと同じ方法で実装されます。）

たとえば、あるワークフロー プロセスで、中級レベルの参加者が一部のケースを上級レベルの参加者にエスカレーションして、最終的な承認または拒否を求めるためのアクションが必要だとします。この場合、中級レベルの参加者は、履歴エディタを使用してコメントまたは推奨事項を追加し、確認と承認または拒否を行う上級レベルの参加者にその作業アイテムを送信できます。

ワークフロー アクション ボタンを追加または削除する際には、これらの新しいアクションを処理するために、ビジネス ロジックを提供する **WorkPoint** ワークフロー プロセスに適切な変更を加える必要があります。

承認タスクのワークフロー ボタン

ワークフロー アクション ボタンは、WorkPoint プロセス図の手動アクティビティ ノードから外に向いている移行ノードに対応します。たとえば、コンサルテーションプロセスの技術者のアクティビティ ノードには、「実装済み」と呼ばれる移行が 1 つあります。以下の図に示すように、これはオンライン リクエストの実装の承認タスクの「実装済み」ボタンに対応しています。

実装リクエスト	対象プロフィール	担当者

ここで説明しているリクエストはプロフィールの提供されているユーザに対する変更に関するもので、承認されているので実施が必要です。提供されたボタンを使ってタスクを起動し、リクエストを実装してください。終了したら、[実装済み]をクリックしてリクエストを閉じてください。

リクエスト、および履歴:

ソース	説明	▲時刻
リクエストとして行動している "SuperAdmin (SuperAdmin)" によるユーザ コメント	オーストラリアの変更を販売担当者。	2008-05-13 15:36:45.937
承認者として行動している "SelfRegUser (SelfReg)" によるユーザ コメント	私たちはオーストラリアの担当者が必要だったので、彼女の動きがシドニーです	2008-05-13 15:38:35.267
リクエストとして行動している "SuperAdmin (SuperAdmin)" によるユーザ コメント	彼女はあまりにもカバーがニュージーランドですか？	2008-05-13 15:45:45.937

コメント

ユーザアカウントの SalesRepAsia として実装され要求されています。

追加

このリクエストを使用し、これらのタスクを実装する:

ワークフローのアクションボタンをクリック

実装済み

アイテムの保留

閉じる

注: [アイテムの保留] ボタンと [閉じる] ボタンは、ワークフロー制御下ではなく、CA Identity Manager のプログラミング ロジックによって制御されます。

CA Identity Manager でのボタン設定

ワークフロー アクション ボタンを設定するには、承認タスクの [プロフィール] タブで、[ワークフロー アクション ボタン] というボタンをクリックします。

ボタンの [プロフィール] タブにはテーブルがあり、各行が 1 つのワークフロー アクション ボタンを示しています。各ボタンの行には、以下の 4 つのプロパティがあります。これらはテーブル内の列に対応します。

表示名

承認画面内のボタンに表示される名前。この名前は条件付きでローカライズされる値です。値には、リソース ファイル内の文字列か、ローカライズされた文字列を示すキーを使用できます。

アクション

オプションの選択時にワークフロー プロセスに返される値。この値は、WorkPoint プロセス図内で対応する移行ノードの属性を示します。値はローカライズされていない文字列です。デフォルト設定は「approved」と「rejected」です。

ツール ヒント

ユーザがボタン上にマウス カーソルを合わせたときに表示される、ボタン アクションについての簡単な説明（ツール ヒント）。このツール ヒントは条件付きでローカライズされる値です。値には、リソース ファイル内の文字列か、ローカライズされた文字列を示すキーを使用できます。

詳細説明

ボタン アクションについての詳細説明。これにより、[サブミット済みタスクの表示] 画面上のアクションについて説明するメッセージが追加されます。説明が空の場合、[サブミット済みタスクの表示] 画面上に表示されるメッセージは、ボタン名になります。この名前は条件付きでローカライズされる値です。値には、リソース ファイル内の文字列か、ローカライズされた文字列を示すキーを使用できます。

詳細情報:

[WorkPoint Designer でのボタン設定 \(P. 365\)](#)

ワークフロー アクション ボタンの追加

既存のワークフロー プロセスに新しいボタンを追加するための概要手順は以下のとおりです。

1. CA Identity Manager で、ワークフロー ボタンを追加します。

手順については、「[ワークフロー アクション ボタンの追加方法 \(P. 364\)](#)」を参照してください。

2. 必要に応じて、ローカライズ キーを追加します。

詳細については、「[設定ガイド](#)」を参照してください。

3. WorkPoint Designer で、新しい必須ノードを追加します。

詳細については、WorkPoint Designer のオンライン ヘルプを参照してください。

4. WorkPoint Designer の移行ノードで、スクリプトを定義します。

詳細については、「[WorkPoint Designer でのボタン設定 \(P. 365\)](#)」を参照してください。

ワークフロー アクション ボタンの追加方法

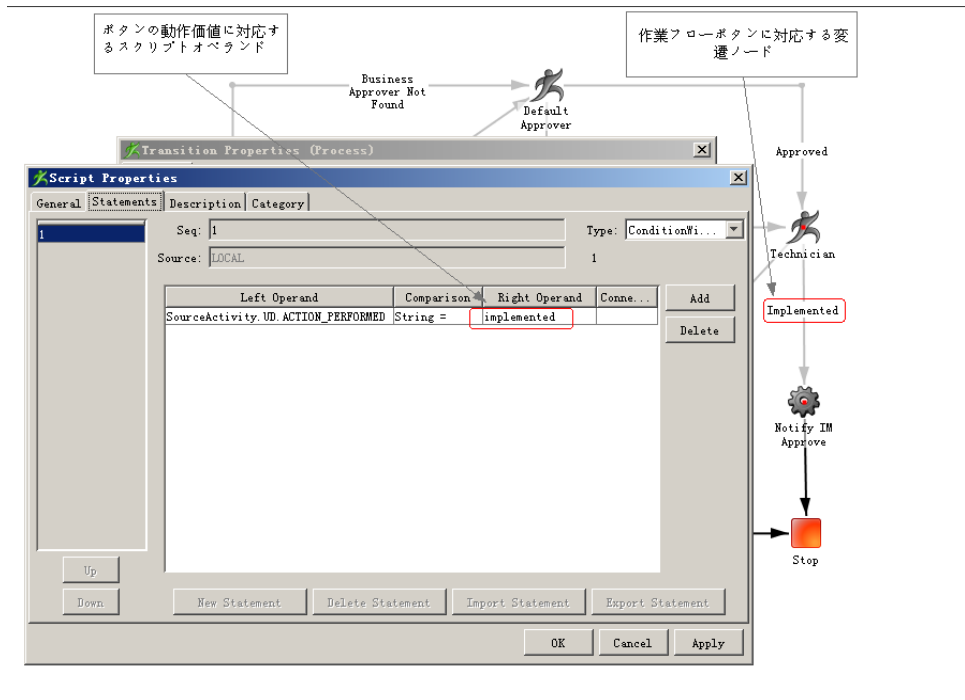
CA Identity Manager で、承認タスクにワークフロー アクション ボタンを追加することができます。

管理タスクにワークフロー アクション ボタンを追加する方法

1. ユーザ コンソールで、[ルールおよびタスク] - [管理タスク] - [管理タスクの変更] を選択します。
[管理タスクの選択] 画面が表示されます。
2. 承認タスクを検索し、[選択] をクリックします。
[管理タスクの変更] 画面が表示されます。
3. [プロファイル] タブで、[ワークフロー アクション ボタン] という名前のボタンをクリックします。
ワークフロー アクション ボタン プロファイル タブが表示されます。
4. [ボタンの追加] をクリックし、承認タスクに新しいボタンを追加します。
5. ボタンのプロパティ情報を入力します。
6. [OK] をクリックします。
CA Identity Manager に新しいボタンの情報が保存されます。
7. [サブミット] をクリックします。
CA Identity Manager によってタスクの変更が処理されます。

WorkPoint Designer でのボタン設定

以下の図に示すように、WorkPoint Designer では、移行ノードのスクリプト プロパティを使用してワークフロー アクション ボタンが設定されます。



デフォルトにより、ワークフロー アクション ボタンは以下のスクリプト プロパティを使用して、文字列の比較を行います。

- [Left Operand] -- 前の手動アクティビティ ノードの [ユーザ データ] プロパティで定義された ACTION_PERFORMED
- [Right Operand] -- ユーザ コンソールの ボタン プロファイル タブで定義された、ボタンのアクション値

注: アクティビティ ノードと移行ノードのスクリプトおよびプロパティの詳細については、WorkPoint Designer のオンラインヘルプを参照してください。

詳細情報:

[CA Identity Manager でのボタン設定](#) (P. 362)

ワークリストと作業アイテム

ワーク リストは、タスクの承認権限が与えられた参加者のユーザ コンソールに表示される作業アイテム（または承認タスク）のリストです。作業アイテムは、ワークフロー プロセスの手動のアクティビティに相当します。作業アイテムは、ワーク リストの行に表示されます。

作業アイテムは、以下の方法でワーク リストに追加できます。

- 参加者リゾルバが承認のリストを決定します。
- 別のユーザから委任された作業アイテムを受け取ります。
- その作業アイテムを別のユーザに再度割り当てます。

作業アイテムは、以下の方法でワーク リストから削除できます。

- 作業アイテムを完了（承認または拒否）します。
- その作業アイテムを別のユーザに再度割り当てます。
- 作業アイテムを保留します。これで、他のすべての参加者のワーク リストから作業アイテムが削除されます。

注: 作業アイテムを承諾または拒否すると、変更はすぐに反映されません。たとえば、作業アイテムを拒否すると、ワークフロー プロセスが情報を記録して次のノードにプロセスを進めるまで、そのアイテムはリスト内に表示されたままです。

作業アイテム上に表示される情報タブは、ワークフローによって生成された作業アイテムが、タスク レベルとイベント レベルのどちらの制御下にあるのかによって異なります。

- **プロフィール** -- イベントの影響を受けるオブジェクトに関するプロフィール情報が表示されます（イベント レベルのみ）。
- **タスク詳細** -- タスク内のすべてのイベントに関する詳細情報が表示されます（タスク レベルのみ）。
- **承認者** -- タスクまたはイベントに関するすべての個人承認者と委任者をリストします（タスク レベルおよびイベント レベル）

ワークリストの表示

他のユーザが開始したタスク（または作業アイテム）を承認する参加者として割り当てられている場合は、ユーザ コンソールにログインすると、ワーク リストが自動的に表示されます。

ワークリストを手動で表示する方法

1. ユーザ コンソールで、[ホーム] - [マイ ワーク リストの表示] を選択します。

ワーク リストが表示されます。

2. 表示する作業アイテムの名前をクリックします。

選択した作業アイテムが表示されます。

管理者は、スコープの対象となるユーザの作業アイテムを管理することができます。

注: ユーザの作業アイテムを管理する際には、管理者が作業アイテムを保留できます。ユーザのワーク リストを表示しても、作業アイテムに変更を加えることはできません。

他のユーザのワークリストを表示する方法

1. ユーザ コンソールで、[ユーザ] - [作業アイテムの管理] - [ユーザのワーク リストの表示] を選択します。

ユーザ選択画面が表示されます。

2. 表示するワーク リストを所有するユーザを検索し、[選択] をクリックします。

そのユーザのワーク リスト画面が表示されます。

他のユーザの作業アイテムを管理する方法

1. ユーザ コンソールで、[ユーザ] - [作業アイテムの管理] - [ユーザのワーク リストの表示] を選択します。

ユーザ選択画面が表示されます。

2. 管理する作業アイテムを所有するユーザを検索し、[選択] をクリックします。

そのユーザのワーク リスト画面が表示されます。

3. 表示する作業アイテムの名前をクリックします。

選択した作業アイテムが表示されます。

作業アイテムの保留

「要確認」の作業アイテムを保留し、その作業アイテムを他の参加者のワーク リストから削除することができます。作業アイテムを保留すると、保留を実行したユーザのみがその作業アイテムを扱えるようになります。

保留したユーザが作業アイテムを解放すると、他の参加者のワーク リストに再びその作業アイテムが表示されるようになります。保留したユーザが作業アイテムを承認または拒否すると、その作業アイテムは完了となり、他の参加者には表示されなくなります。

再割り当てと保留済み作業アイテム

作業アイテムが再割り当てされている最中に、ユーザが作業アイテムを保留した場合は、そのユーザの保留が継続されます。ただし、その後このユーザが作業アイテムを解放すると、このユーザはその作業アイテムにアクセスできなくなります。

管理者は、他のユーザの作業アイテムを再割り当て、保留、または解放できますが、他のユーザの作業アイテムを承認または拒否することはできません。これを実行できるのは、割り当てられた作業アイテムの参加者のみです。

詳細情報:

[作業アイテムの再割り当て](#) (P. 375)

委任と保留済み作業アイテム

委任がアクティブになっている場合は、代行者または委任者が作業アイテムを保留することができます。あるユーザが保留した作業アイテムを、別のユーザのワーク リストに表示することはできません。

たとえば、委任が撤回されている最中に、代行者が作業アイテムを保留した場合は、代行者がその作業アイテムの保留を続けることができます。ただし、その後この代行者が作業アイテムを解放すると、このユーザはその作業アイテムにアクセスできなくなります。

代行者になっているユーザが作業アイテムを保留している最中に、その代行者が削除された場合でも、代行者がその作業アイテムを保持し続けることができます。その後、代行者がこの作業アイテムを承認した場合は、監査を行っても元の委任者を判別できなくなります。

委任が撤回されている最中に、代行者が作業アイテムを保留した場合は、その作業アイテムが完了または解放されるまで、代行者のアクセス権は保持されます。

作業アイテムの保留または解放方法

「要確認」の作業アイテムを保留し、その作業アイテムを他の参加者のワーク リストから削除することができます。

保留した作業アイテムが他の参加者のワーク リストに表示されるようにするには、その作業アイテムを解放します。

注: 保留した作業アイテムを他の参加者が使用できるようにするには、作業アイテムを明示的に解放する必要があります。

作業アイテムを保留または解放する方法

1. ユーザ コンソールで、[ホーム] - [マイ ワーク リストの表示] を選択します。
ワーク リストが表示されます。
2. 保留または解放する作業アイテムを選択します。
作業アイテムの拡張画面が表示されます。
3. [アイテムの保留] または [アイテムの解放] をクリックします。
CA Identity Manager によってアクションが確認されます。

作業アイテムの委任

作業アイテムの委任では、ユーザ（委任者）が別のユーザ（代行者）を指定して、代行者が委任者のワーク リスト内のタスクを承認できるようにします。委任者が「外出」する際には、その期間だけ別の承認者に作業アイテムを割り当てることができます。委任者は、委任期間中でも自分の作業アイテムに完全にアクセスすることができます。

委任された作業アイテムは何も変わらない状態で示されます。ログインを行うと、作業アイテムが委任されたかがわかります。

委任は、代行者が委任者に「なりすまし」、委任者のワーク リスト上のアイテムを表示できるようにすることで機能します。代行者がワーク リストを表示すると、自分の作業アイテムのほかに委任者の作業アイテムも表示されます。

委任は移行型ではありません。代行者は、委任者が直接割り当てた作業アイテムしか見ることはできません。たとえば、ユーザ A がユーザ B に作業アイテムを委任し、ユーザ B がユーザ C に作業アイテムを委任した場合、ユーザ C はユーザ B に属する作業アイテムしか見ることはできず、ユーザ A がユーザ B に委任した可能性のある作業アイテムは見ることができません。

詳細情報:

[委任と保留済み作業アイテム](#) (P. 368)

委任の汎用属性

委任では、以下の汎用属性が使用されます。

%DELEGATORS%

この汎用属性には、この属性を持つユーザに委任しているユーザの名前と、委任が作成された時刻が格納されます。

委任の有効化方法

他のユーザに作業アイテムを委任するには、ワークフロー承認の委任を有効化しておく必要があります。デフォルトでは、委任は無効になっています。

ワークフロー承認の委任を有効化するには、以下の手順に従います。

1. ブラウザに以下の URL を入力して、管理コンソールを開きます。

`http://hostname/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。たとえば、`myserver.mycompany.com:port` です。

2. [環境] をクリックしてから、適切な CA Identity Manager 環境の名前を選択します。
3. [詳細設定] をクリックし、次に [ワークフロー承認の委任] をクリックします。
4. [有効] チェック ボックスをオンにし、[保存] をクリックします。

自分の作業アイテムを委任する方法

「外出」する際には、その期間だけ別のユーザに作業アイテムを委任することができます。委任者は、委任期間中でも自分の作業アイテムに完全にアクセスすることができます。

自分の作業アイテムを委任する方法

1. ユーザ コンソールで、[ホーム] - [不在時のアシスタント] を選択します。
[不在時のアシスタント] 画面が表示されます。
2. [ユーザの追加] をクリックします。
ユーザ選択画面が表示されます。
3. 代行者にするユーザ（複数可）を検索し、選択します。
選択したユーザが代行者リストに追加されます。
4. [サブミット] をクリックします。
タスクがサブミットされ、委任内容が保存されます。

注:すでに代行者になっているユーザは、代行者の追加時に検索結果に表示されません。

詳細情報:

[委任の有効化方法](#) (P. 370)

時間単位の作業アイテム委任

前回のリリースでは開始時刻を指定することはできましたが、委任の終了時刻の指定はできませんでした。新しく作成された委任は、委任の日付が **true** に、デフォルトの開始時刻は **now** に設定されています。

変更時間において、開始および終了日を変更できます。デフォルトの終了時刻は、開始日から一週間です。

開始または終了の日付を変更するには、以下の手順に従います。

1. ユーザ コンソールの [ホーム] タブから、[不在時のアシスタント] を選択します。
2. 委任情報を変更したいユーザ ID のとりにある鉛筆のアイコンをクリックします。

[委任の詳細の編集] 画面が表示されます。

3. [開始日] のとりにあるカレンダーをクリックし、委任の開始日を変更します。

注: 選択した委任開始日が現在の日付より以前の場合、エラー メッセージが表示されます。

4. 終了日を選択したい場合は、[終了日指定] チェックボックスをチェックします。

これで [終了日] フィールドが利用可能になり、終了日を設定できます。

5. [終了日] のとりにあるカレンダーをクリックし、委任の終了日を設定します。

6. 日付を設定したら、[OK] をクリックします。

あるいはユーザの作成または変更時に、同じ作業を [作業アイテムの委任] タブから行えます。

時間単位の作業アイテム委任の有効化

アップグレードにあたり既存の環境で時間単位の作業アイテム委任を有効化するには、以下の手順に従います。

管理コンソールから

1. [環境] ページに移動します。
2. 選択した [環境] - [詳細設定] - [Work Item Delegation] にドリル ダウンします。
3. [有効] チェック ボックスをオフにします。
4. 変更を保存して、環境を再起動します。
5. [詳細設定] - [Work Item Delegation] にドリルダウンします。
6. [有効] チェックボックスをチェックします。
7. 変更を保存して、環境を再起動します。

注: このプロシージャは、既存の環境に対してのみ有効です。 時間単位のワークフロー アイテム委任は、新しい環境に対して有効です。

[不在時のアシスタント]画面

自分の代行者を追加および削除するには、以下の [不在時のアシスタント] 画面を使用します。

[不在時のアシスタント] 画面には、現在の代行者のリストが表示されます。 リストには、委任を識別する列のほかに以下の 3 つの列があります。

開始日

委任が作成された日付が表示されます。

終了日

委任が終了する日付けが表示されます。

委任の有無

代行者が他のユーザに作業アイテムを委任したかどうかを示されます。

選択されたユーザ ID のとりにある鉛筆のアイコンをクリックすると、[委任の詳細の編集] 画面が表示され、委任の [開始日] を変更して [終了日] を指定できます。

他のユーザの作業アイテムを委任する方法

管理者は、あるユーザ（委任者）の作業アイテムを別のユーザに委任することができます。たとえば、あるユーザが予定外に外出してしまった場合や、管理者が大きな作業負荷を複数のユーザに割り当てる必要がある場合があります。

管理者は、スコープの対象となるユーザの作業アイテムしか委任できません。同様に、管理者が代行者リストに追加または削除できるのは、自分が管理しているユーザのみです。

他のユーザの作業アイテムを委任する方法

1. ユーザ コンソールで、[ユーザ] - [作業アイテムの管理] - [作業アイテムの委任] を選択します。

ユーザ選択画面が表示されます。

2. 委任する作業アイテムを所有するユーザ（委任者）を検索し、[選択] をクリックします。

作業アイテムの委任画面が表示されます。

3. [ユーザの追加] をクリックします。

ユーザ選択画面が表示されます。

4. 代行者にするユーザ（複数可）を検索し、選択します。

選択したユーザが代行者リストに追加されます。

5. [サブミット] をクリックします。

タスクがサブミットされ、委任内容が保存されます。

注:すでに代行者になっているユーザは、代行者の追加時に検索結果に表示されません。

詳細情報:

[委任の有効化方法](#) (P. 370)

委任を削除する方法

委任が設定されている場合にユーザが CA Identity Manager にログインすると、CA Identity Manager に以下のメッセージが表示されます。

委任が設定されました。 それらがまだ必要であることを確認してください。

自分の委任を削除する方法

1. ユーザ コンソールで、[ホーム] - [不在時のアシスタント] を選択します。
[不在時のアシスタント] 画面が表示されます。
2. 削除する代行者のマイナス記号 (-) をクリックします。
選択した代行者がリストから削除されます。
3. [サブミット] をクリックします。
タスクがサブミットされ、委任内容が削除されます。

他のユーザの委任を削除する方法

1. ユーザ コンソールで、[ユーザ] - [作業アイテムの管理] - [作業アイテムの委任] を選択します。
ユーザ検索画面が表示されます。
2. 削除する委任を所有するユーザを検索し、選択します。
代行者リストが表示されます。
3. 削除する代行者のマイナス記号 (-) をクリックします。
選択した代行者がリストから削除されます。
4. [サブミット] をクリックします。
タスクがサブミットされ、委任内容が削除されます。

注: 代行者を削除できるのは、そのユーザに対するスコープがある場合のみです。

作業アイテムの再割り当て

再割り当てによって、ユーザおよび管理者は作業アイテムを作成後、その担当者を変更できます。管理者は以下のことを実行できます。

- 別のユーザのワーク リストの表示
- 作業アイテムの担当者の追加および削除
- 作業アイテムの予約ステータスの変更

たとえば、管理者は作業アイテムを再割り当てするか、または予約された作業アイテムに対してユーザが作業していない場合はそのアイテムを解放できます。

再割り当て中に予約された作業アイテムがある場合は、そのユーザの予約が継続されます。ただし、その後このユーザが作業アイテムを解放すると、このユーザはその作業アイテムにアクセスできなくなります。

委任の取り消し中に予約された作業アイテムがある場合、作業アイテムが完了するか解放されるまで、委任先はアクセス権を保持します。

詳細情報:

[再割り当てと保留済み作業アイテム](#) (P. 368)

[承認者]タブ

現在の作業アイテムの承認者（または担当者）のリストを表示する作業アイテム承認者タブ上で、再割り当てを実行します。再割り当ての実行時、開いている作業アイテムをリスト内のすべての承認者に割り当てます。そのため、作業アイテムを新しい担当者に再割り当てするには、現在の担当者を削除する必要があります。

作業アイテムの再割り当て方法

作業アイテムをあるユーザから別のユーザに再度割り当てるプロセスには、次の2段階があります。

- 新しい承認者を選択します。
- 現在の承認者を削除します。

注: 再割り当ての対象ユーザに対するスコープが必要です。

自分の作業アイテムを再割り当てする方法

1. [ホーム] - [マイ ワーク リストの表示] を選択します。
ワーク リストが表示されます。
2. 作業アイテムを選択し、拡張します。
3. [承認者] タブを選択します。

現在管理中のワーク リストを所有するユーザを含め、現在の承認者全員のリストが表示されます。

4. [担当者の追加] をクリックします。
ユーザ選択画面が表示されます。

5. 再割り当てする対象のユーザを検索して選択します（複数可）。

注: ALL および SUBSET の承認モードの場合、作業アイテムは1人のユーザにのみ再割り当てできます。

6. 自分を担当者として削除するには、マイナス記号のボタン (-) をクリックします。

7. [再割り当ての実行] をクリックします。

再割り当てされたユーザのワーク リストに、その作業アイテムが表示されます。

注: 管理者は、他のユーザの作業アイテムを再割り当て、保留、または解放できますが、他のユーザの作業アイテムを承認または拒否することはできません。それをできるのは作業アイテムの所有者のみです。

別のユーザの作業アイテムを再割り当てする方法

1. [ユーザ]、[作業アイテムの管理]、[ユーザの作業アイテムの管理] を選択します。

ユーザ選択画面が表示されます。

2. 再割り当てする作業アイテムを所有するユーザを検索し、[選択] をクリックします。

[ユーザの作業アイテムの管理] 画面が表示されます。

3. 作業アイテムを選択し、拡張します。

4. [承認者] タブを選択します。

現在管理中のワーク リストを所有するユーザを含め、現在の承認者全員のリストが表示されます。

5. [担当者の追加] をクリックします。

ユーザ選択画面が表示されます。

6. 再割り当てする対象のユーザを検索して選択します（複数可）。

7. 現在の担当者を削除するには、マイナス記号のボタン (-) をクリックします。

8. [再割り当ての実行] をクリックします。

再割り当てされたユーザのワーク リストに、その作業アイテムが表示されます。

作業アイテムに対するバルク操作

CA Identity Manager の本リリースでは、選択された作業アイテム上で、以下のバルク操作を実行できます。

- 承認
- 拒否
- 保留
- 解放

ユーザ コンソールの [Configure Work List] タブが拡張され、新たに [バルク ワークフロー操作をサポートする] チェック ボックスが含まれています。このチェック ボックスが有効化されている場合、ユーザは所有する作業アイテム、または委任された作業アイテムをバルクで承認、拒否、解放、保留できます。管理者はこれらのバルク操作を、[ユーザの作業アイテムの管理] タスクを使用してのみ、作業アイテムに実行できます。

注: バルク操作は、[マイ ワーク リストの表示] などの表示タイプのタスクでは有効化できません。

バルク操作用の[ワークリスト]タブの設定

[ワーク リスト] タブを設定して作業アイテムに対するバルク操作をサポートするには、この手順に従います。

ユーザ コンソールの [ロールおよびタスク] タブから

1. 次のいずれかを選択します。
 - [ロールおよびタスク]。
 - [タスク] - [ロールおよびタスク]。
2. [管理タスク] - [管理タスクの管理] を選択します。
3. [検索] をクリックします。
4. [ユーザの作業アイテムの管理] を選択します。
5. [タブ] タブから、ワーク リストのとなりにある鉛筆のアイコンをクリックします。

[ワーク リストの設定] 画面が表示されます。
6. [バルク ワークフロー操作をサポート] を選択します。
7. 変更を保存してタスクを送信します。

これで作業アイテムに対するバルク操作が有効になります。

第 13 章：電子メール通知

このセクションには、以下のトピックが含まれています。

[CA Identity Manager の電子メール通知](#) (P. 380)

[電子メール通知方法を選択する方法](#) (P. 381)

[SMTP の設定](#) (P. 382)

[電子メール通知ポリシーの作成方法](#) (P. 385)

[電子メールテンプレートの使用方法](#) (P. 395)

CA Identity Manager の電子メール通知

電子メール通知は、CA Identity Manager ユーザに、システムのタスクとイベントに関する情報を提供します。たとえば、イベントタスクが承認をリクエストすると CA Identity Manager が承認者に電子メールを送信します。

CA Identity Manager では以下の電子メール通知の設定方法を提供します。

■ 電子メール通知ポリシー

電子メール通知ポリシーでは、業務系管理者はユーザ コンソールのタスクを使用して電子メールの作成、表示、変更、および削除を行うことができます。電子メール通知の作成にコーディングは必要ありません。

管理者は電子メールのコンテンツ、送信するタイミング、送信者を定義できます。HTML エディタで定義される電子メールのコンテンツには、現在の日付やイベント情報などの動的情報が含まれます。これらの情報は、電子メールの送信時に CA Identity Manager に読み込まれます。たとえば、新しいユーザが作成されると承認者に送信される電子メール通知を設定できます。電子メールにはユーザのログイン情報、雇用日、およびマネージャを含めることができます。

注: 電子メール通知ポリシーは、別のタスクのセットによって作成および管理される [Policy Xpress ポリシー](#) (P. 517) です。

■ 電子メールテンプレート

この方法では、電子メール通知は電子メールテンプレートから作成されます。CA Identity Manager に用意されているデフォルトの電子メールテンプレートは、インストール時の状態でそのまま使用することも、システム管理者がカスタマイズすることもできます。これらの管理者は電子メールテンプレート API を使用して、受信者のリストなどの動的コンテンツや、電子メールをトリガするイベントに関する情報を指定します。

CA Identity Manager は、以下のいずれかが発生した場合に電子メール通知を生成できます。

- ワークフロー承認者による承認または拒否が必要なイベントが保留中である場合。

注: 複数の承認アクティビティが存在する Workpoint 承認プロセスがある場合、「ユーザ コンソール」タスクで設定されている電子メール通知は各アクティビティの通知を送信します。電子メールテンプレートを同じ通知に使う場合、承認者に送信される電子メールは（イベントが保留状態になった際の）1 件のみです。

- 承認者がイベントまたはタスクを承認する場合。
- 承認者がイベントまたはタスクを拒否する場合。

- イベントまたはタスクが開始、失敗、または完了した場合。
- ユーザが作成または変更された場合。

CA Identity Manager 電子メール通知を使用するには、[SMTP 設定](#) (P. 382)を行います。電子メール テンプレート方式を使用している場合、CA Identity Manager の電子メール通知も有効化します。

電子メール通知方法を選択する方法

以下の表では、電子メール通知ポリシーと電子メール テンプレートの違いをまとめています。

アクティビティ	電子メール管理タスク	電子メール テンプレート
電子メール通知の設定	管理者はユーザ コンソールの管理タスクを使用して、電子メール通知を作成、変更、表示、および削除します。	管理者は CA Identity Manager 管理ツールのデフォルト テンプレートを変更します。
電子メールの送信時間の設定	CA Identity Manager は、所定のイベントやタスクが発生した場合に、電子メール通知を生成できます。電子メール管理タスクと電子メール テンプレートは同じイベントとタスクをサポートしますが、電子メール管理タスクのほうがより詳細な管理が可能である場合があります。 電子メール通知は以下のタスクとイベントでサポートされています。 ■ ワークフロー承認者による承認または拒否が必要なイベントが保留中である場合。 ■ 注: 複数の承認アクティビティが存在する Workpoint 承認プロセスがある場合、電子メール管理タスクを使用して設定されている電子メール通知は各アクティビティの通知を送信します。電子メール テンプレートを同じ通知に使う場合、承認者に送信される電子メールは（イベントが保留状態になった際の）1 件のみです。 ■ 承認者がイベントまたはタスクを承認する場合。 ■ 承認者がイベントまたはタスクを拒否する場合。 ■ イベントまたはタスクが開始、失敗、または完了した場合。 ■ ユーザが作成または変更された場合。	

アクティビティ	電子メール管理タスク	電子メール テンプレート
動的コンテンツの電子メールへの追加	管理者は [電子メールの作成] または [電子メールの変更] タスクの [コンテンツ] タブにあるオプションのリストを選択することにより、動的コンテンツを電子メール メッセージの本体に追加できます。 CA Identity Manager は、通知をトリガするイベントまたはタスクの情報に基づき、動的コンテンツを自動的に読み込みます。	管理者は電子メール テンプレート API を使用して、電子メール通知を生成するために使用されるデフォルトの電子メール テンプレートをカスタマイズします。
既存の電子メール通知のサポート	電子メール管理タスクを使用して設定される電子メール通知は、 Policy Xpress ポリシーに基づいています。 CA Identity Manager Option Pack 1 から CA Identity Manager 12.6.4 へアップグレードした場合、 Policy Xpress で設定した電子メール通知は引き続き動作します。ただし、電子メール通知の管理は Policy Xpress ではなく、電子メール管理タスクを使用しています。	以前のバージョンの CA Identity Manager の電子メール テンプレート メソッドを使用して作成した電子メール通知は、 CA Identity Manager 12.6.4 でも引き続き動作します。

SMTP の設定

電子メール通知を有効にする前に、SMTP を設定します。お使いのアプリケーション サーバの SMTP を設定するには、以下のセクションを参照してください。

JBoss 上での SMTP の設定

1. テキスト エディタで、次のようにしてメール サービスの配備記述子を開きます。

単一ノード : `jboss_home¥server¥default¥deploy¥mail-service.xml`

クラスタ : `jboss_home¥server¥all¥deploy¥mail-service.xml`

2. `mail.smtp.host` プロパティを、次のようにして、SMTP サーバの名前に修正します。

`<-- Change to the SMTP gateway server -->`

`<property name="mail.smtp.host" value="your_smtp_server" />`

以下に例を示します。

`<property name="mail.smtp.host" value="smtp.mailserver.company.com" />`

3. `mail-service.xml` ファイルを保存します。
4. テキスト エディタで、次の電子メール プロパティ ファイルを開きます。

単一ノード :

`jboss_home¥server¥default¥deploy¥iam_im.ear¥config¥com¥netegrity¥config¥email.properties`

クラスタ :

`jboss_home¥server¥all¥deploy¥iam_im.ear¥config¥com¥netegrity¥config¥email.properties`

5. ワークフロー生成電子メールが使用する返信用電子メールアドレスを設定するには、`admin.email.address` プロパティを見つけて、その値に該当する電子メールアドレスを設定します。以下に例を示します。

`admin.email.address=admin@company.com`

6. 電子メール テンプレート方式を使用している場合、管理コンソールで電子メール通知を有効にします。

電子メール通知ポリシーを使用している場合は、管理コンソールで電子メール通知を有効にする必要はありません。

WebLogic 上での SMTP の設定

WebLogic サーバの管理者コンソール、および `email.properties` ファイルで電子メールを設定します。

WebLogic に対して電子メールを設定する方法

1. WebLogic サーバの管理者コンソールで、次のプロパティを持つメールセッションを作成します。
 - **mail.smtp.host** プロパティ：この値を対象の SMTP サーバに設定します。
例：mail.smtp.host=mymailserver.company.com
 - **mail.transport.protocol** プロパティ：この値を SMTP に設定します。例：
mail.transport.protocol=smtp
 - **JNDI Name**：nete/Mail
 - **Target**：WebLogic のサーバ名
2. テキストエディタで、CA Identity Manager に対する以下の電子メールプロパティファイルを開きます。

`weblogic_domain¥applications¥iam.ear¥config¥com¥netegrity¥config¥email.properties`
3. `admin.email.address` プロパティを見つけて、その値を該当する電子メールアドレスに設定し、ワークフローで生成した電子メールで使用する電子メールの復帰アドレスを設定します。以下に例を示します。
`admin.email.address=admin@company.com`
4. 管理コンソールでの電子メール通知の有効化

注：電子メール通知ポリシーを使用している場合は、管理コンソールの電子メール通知を有効化する必要はありません。

WebSphere 上での SMTP の設定

CA Identity Manager コンポーネントをインストールした後で実行する `imsSetup` ユーティリティは、`mailMail` という名前の新しいメールセッションオブジェクトを設定します。

電子メールの通知機能を正しく作動させるには、`mailMail` セッションの [Mail Transport Host] フィールドで電子メールを送信するときに、WebSphere が接続するサーバを指定します。

mailMail セッションは、WebSphere 管理コンソールの [リソース]、[Mail Providers]、[Built-in Mail Provider]、[Mail Sessions]、[mailMail] にあります。

注: mailMail オブジェクトを参照するには、[Mail Session] 画面で [スコープ] を [サーバ] へ変更します。スコープを [サーバ] へ変更しないと、mailMail オブジェクトは表示されません。

WebSphere メールプロバイダを設定する詳細については、WebSphere のマニュアルを参照してください。

電子メールテンプレート方式を使用している場合、SMTP 設定を行った後、管理コンソールで電子メール通知を有効にします。

注: 電子メール通知ポリシーを使用している場合は、管理コンソールの電子メール通知を有効化する必要はありません。

電子メール通知ポリシーの作成方法

ユーザ コンソールを使用して、特定のアクションが発生すると電子メールを送信して承認者に知らせる電子メール通知ポリシーを作成できます。たとえば、ユーザが作成されると電子メールを送信して承認者に通知する電子メール通知ポリシーを作成できます。

次の手順に従ってください:

1. [システム] - [電子メール] - [電子メールの作成] 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。
 - オブジェクトタイプ: "管理電子メール" の作成
 - オブジェクトタイプ: "管理電子メール" のコピーの作成既存の電子メール通知ポリシーをテンプレートに使用して、ポリシーを作成します。
3. [プロファイル] タブで、電子メール通知ポリシーに関する基本情報を入力します。

4. [送信のタイミング] タブで、CA Identity Manager から電子メールを送信するタイミングを指定します。
[送信のタイミング] タブでは、電子メール通知のトリガとなるアクションを複数のオプションから指定できます。
5. [受信者] タブで、電子メールの受信者を指定します。
6. [コンテンツ] タブで、電子メールの件名およびコンテンツを定義します。
電子メールのコンテンツ内の動的コンテンツ（日付、タスクまたはイベント名、ユーザ属性など）を指定できます。

電子メール通知プロフィール タブ

電子メール管理タスクの [プロフィール] タブでは、電子メール通知ポリシーに関する基本情報を指定できます。このタブには以下のフィールドが含まれます。

電子メール名

ユーザ コンソールの電子メール通知ポリシーを識別します。

注: 電子メール名は、電子メールの送信時には表示されません。名前はユーザ コンソール内で電子メール通知ポリシーを管理する目的のみに使用されます。

カテゴリ

電子メール通知ポリシーをグループ化して管理を容易にします。

ドロップダウン リストから選択して既存のカテゴリを指定するか、2 つめのオプション ボタンを選択して新しいカテゴリの名前を入力します。

説明

管理者に対する電子メール通知ポリシーの説明です。

説明は電子メールの送信時には表示されません。

有効

[送信のタイミング] タブで定義された基準を満たす場合に CA Identity Manager が電子メールを送信するよう指定します。

カスタム データ

カスタム受信者やカスタム コンテンツの設定に使用できるカスタム データ エlementを **Policy Xpress** に作成します。

カスタム データ エlementは、その他のデータ エlementのパラメータとしても使用できます。

注: データ エlementの詳細情報は「[データ \(P. 525\)](#)」を参照してください。

[カスタム データ] をクリックすると、新しいデータ エlementを追加できる画面が **CA Identity Manager** によって開かれます。

エントリ ルール

[送信のタイミング] タブのデフォルト ルールが十分に細かく設定されていない場合に **CA Identity Manager** が電子メール通知を送信する際のルールを定義します。

たとえば、[送信のタイミング] タブは、ユーザ プロファイルの属性が変更されたときに電子メールを送信するデフォルト ルールを提供します。**CA Identity Manager** による電子メールの送信をユーザの部署が変更されたときのみに限定したい場合は、カスタム エントリ ルールを作成します。（この場合、部署の変更を識別するカスタム データ エlementを作成してから、このカスタム データ エlementを使用するエントリ ルールを作成します）。

注: 詳細については「[エントリ ルール \(P. 527\)](#)」を参照してください。

詳細情報:

[データ エlement \(P. 525\)](#)

[エントリ ルール \(P. 527\)](#)

[送信のタイミング]タブ

CA Identity Manager では、電子メールの送信タイミングを決定する複数のオプションがデフォルトで用意されています。一部のオプションでは、タスクやイベント名などの追加情報が必要になります。たとえば、タスクの開始時に電子メールを送信するには、電子メールをトリガするタスクを選択する必要があります。

[送信のタイミング] オプションでは、以下のオプションから 1 つ以上を選択できます。

ユーザ作成時

ユーザが作成されると電子メールを送信します。CreateUserEvent が完了すると電子メールが送信されます。

ユーザ変更時

ユーザが変更されると電子メールを送信します。ModifyUserEvent が完了すると電子メールが送信されます。

ワークフロー待ち時

ワークフロープロセスによって承認者が割り当てられると電子メールが送信されます。このオプションを選択する場合、適用可能なワークフロープロセスを指定してください。このポリシーで定義される電子メールは、選択したワークフロープロセスの各ステップで、承認者に個別に電子メールを送信します。

ワークフロー待ち電子メール

ワークフロープロセスが指定したアクティビティに到達すると、電子メールを送信します。このオプションを選択する場合、適用可能なワークフロープロセスを指定してください。このポリシーで定義される電子メールは、各承認ステップで電子メール通知を個別に送信します。

イベント開始時

イベントが [以前] 状態になると電子メールを送信します。このオプションを選択する場合、イベントを指定してください。

注: [イベント開始時] を指定し、電子メールの送信が失敗した場合、通知に関連付けられたイベントは実行されません。

イベント終了時

イベントが [以降] 状態になると電子メールを送信します。このオプションを選択する場合、イベントを指定してください。

イベント承認時

イベントが「承認」状態になると電子メールを送信します。このオプションを選択する場合、イベントを指定してください。

イベント拒否時

イベントが「拒否」状態になると電子メールを送信します。このオプションを選択する場合、イベントを指定してください。

イベント失敗時

イベントが失敗すると電子メールを送信します。このオプションを選択する場合、イベントを指定してください。

タスクのサブミット時

タスクの処理が開始されると電子メールを送信します。このオプションを選択する場合、タスクを指定してください。

タスク完了時

タスクが完了すると電子メールを送信します。このオプションを選択する場合、タスクを指定してください。

タスク失敗時

タスクが失敗すると電子メールを送信します。このオプションを選択する場合、タスクを指定してください。

受信者タブ

電子メールの [TO]、[CC]、または [BCC] フィールドには複数の受信者を設定できます。受信者リストとして、固定リストを指定することもできますし、電子メールをトリガするアクションのタイプや関連ユーザに応じて異なるリストを指定することもできます。

受信者を指定するには、[受信者] タブで [TO]、[CC]、または [BCC] フィールドのとなりにある [編集] アイコンを選択します。続けて次のオプションのいずれかを選択すると、受信者リストの設定が可能になります。

ワークフロー承認者

ワークフロー プロセス内のすべての承認者に電子メールを送信します。このオプションは、ワークフロー待ち時イベントにより電子メールが送信された場合にのみ適用されます。

マネージャ

タスクの実行対象となるユーザのマネージャに電子メールを送信します。

注: [マネージャ] 受信者オプションを使用するには、使用環境においてマネージャ属性を設定します。マネージャ属性を設定するには、管理コンソールで [Environments] - [*EnvironmentName*] - [Advanced Settings] - [Miscellaneous] を選択します。managerattribute には、ユーザのマネージャの一意な名前を保存するフィジカルアトリビュート名を設定します。

リレーショナル データベースには、次の形式を使用して属性を指定します。

テーブル名.属性

グループ メンバ

グループのすべてのメンバに電子メールを送信します。このオプションを選択すると、利用可能なグループ名のドロップダウン リストが開きます。

ロール メンバ

管理ロールのすべてのメンバに電子メールを送ります。このオプションを選択すると、利用可能なロール名のドロップダウン リストが開きます。

静的アドレス

選択したアドレス宛てに電子メールを送信します。テキスト領域で、追加の電子メールアドレスを指定できます。

注: テキスト領域では複数のアドレスを指定しないでください。

ユーザ

タスクの実行対象となるユーザに電子メールを送信します。

開始者

リクエストを行った個人に電子メールを送信します。

カスタム

カスタム データ エlementを選択して受信者を定義します。

カスタム オプションを選択すると、利用可能なカスタム データ エlementのドロップダウン リストが表示されます。

注: データ エlementの詳細情報は「[データ \(P. 525\)](#)」を参照してください。

コンテンツ

電子メールの件名および本文は、テキスト形式を使用して定義するか、電子メールを送信するタイミングが計算された動的コンテンツを追加できます。

件名行は、メッセージを記入できるテキスト形式のフィールドです。これが電子メールの件名になります。

本文は HTML エディタで表示されます。テキストの挿入および書式設定を行って電子メールの本文を作成します。

動的コンテンツを追加するには、ドロップダウン リストから対応するオプションを選択します。カーソルのある位置には、次に示す形式の動的コンテンツ インジケータが追加されます。

{<type>}

<type> は、サポート対象である動的コンテンツのタイプを表します。

たとえば、動的コンテンツのタイプとして「属性」を選択して **FirstName** 属性を指定した場合、HTML エディタの [コンテンツ] タブには次の項目が表示されます。

{'Attribute: FirstName'}

注: 件名行に動的コンテンツを追加するには、件名行の下にあるドロップダウン リストを使用します。電子メール本文に動的コンテンツを追加するには、コンテンツ ボックスの下にあるドロップダウン リストを使用します。

電子メールメッセージが送信されると、CA Identity Manager は動的コンテンツを適切なテキストで置き換えます。テキストは HTML エディタで指定された太字などの書式設定を保持します。

動的コンテンツのタイプには以下の項目が含まれます。

[Date]

ユーザが指定する書式設定で今日の日付を指定します。

タスク

電子メールの送信対象となるタスクを指定します。

オブジェクト名

電子メールをトリガするイベント内のオブジェクト名を指定します。イベントがユーザ イベントの場合、このフィールドはユーザ ログイン名です。

オブジェクトはユーザ以外の可能性もあります。たとえば、グループや管理ロールなどの、管理オブジェクトの場合があります。

属性

ユーザ属性のうち 1 つの値を指定します。ユーザがタスクの対象です。このオプションでは、ドロップダウン リストから属性を選択する必要があります。

マネージャ属性

ユーザのマネージャの属性のうち 1 つの値を指定します。ユーザがタスクの対象です。このオプションでは、ドロップダウン リストから属性を選択する必要があります。

注: [マネージャ] 受信者オプションを使用するには、使用環境においてマネージャ属性を設定します。マネージャ属性を設定するには、管理コンソールで [Environments] - [*EnvironmentName*] - [Advanced Settings] - [Miscellaneous] を選択します。managerattribute には、ユーザのマネージャの一意な名前を保存するフィジカル アトリビュート名を設定します。

リレーショナル データベースには、次の形式を使用して属性を指定します。

テーブル名.属性

カスタム

カスタム データ エlement を選択して受信者を定義します。

カスタム オプションを選択すると、利用可能なカスタム データ エlement のドロップダウン リストが表示されます。

注: データ エlement の詳細情報は「[データ](#) (P. 525)」を参照してください。

電子メール通知ポリシーの変更

ビジネス要件に合わせて既存の電子メール通知ポリシーを変更できます。

電子メール通知ポリシーを変更する方法

1. [システム] - [電子メール] - [電子メールの作成] を選択します。
CA Identity Manager の検索画面が表示されます。
2. 変更する電子メール通知ポリシーを検索して選択します。
3. [プロファイル]、[送信のタイミング]、[受信者]、および[コンテンツ] タブの設定を必要に応じて変更します。

電子メール通知ポリシーの無効化

電子メール通知ポリシーを有効化/無効化するには、電子メール通知ポリシーの作成時または変更時に、[プロファイル] タブの [有効] チェックボックスを使用します。電子メール通知ポリシーが無効化されている場合、選択された電子メールは非アクティブであり、電子メールは送信されません。

注: デフォルトでは、電子メール通知ポリシーは有効です。

ユース ケース: ウェルカム メールを送信

新しい従業員が雇用されると、Forward, Inc はそのユーザに電子メールを送信して入社を歓迎します。電子メールは、従業員ホームページへのリンクやマネージャおよび部署に関する情報など、重要な情報を新しい従業員に提供する必要があります。

電子メールを作成するには、人事管理者はユーザ コンソールの「電子メールの作成」タスクを使用して次を設定します。

- [送信のタイミング] タブで、[ユーザ作成時] を選択します。
- [受信者] タブで、以下の手順を実行します。
 - [TO] フィールドのとなりにある [編集] アイコンをクリックします。
ユーザを選択してから、プラス (+) 記号をクリックします。同じ手順でマネージャを選択し、[OK] をクリックします。
 - [CC] フィールドのとなりにある [編集] アイコンをクリックします。
開始者を選択し、プラス (+) 記号をクリックしてから [OK] をクリックし、CA Identity Manager で従業員を作成したユーザに電子メールのコピーを送信します。
- [コンテンツ] タブで、以下の手順を実行します。
 - [件名] フィールドに、「Welcome,」と入力します。
入力した文字の末尾にあるカーソルで、ドロップダウン リストから [属性] を選択します。次に、2 つめのドロップダウン リストから [フルネーム] を選択し、プラス (+) 記号をクリックします。
件名は次のようになります。
Welcome, {'Attribute: eTFullName'}
注: 属性名は、ユーザ ストアおよび使用している属性に依存します。
 - [コンテンツ] ボックスに、歓迎のメッセージを入力します。従業員ポータルへのリンクを含め、コンテンツ ボックスの下に動的コンテンツ オプションを使用して、次のようにユーザの部署、マネージャおよびマネージャの電話番号を表示します。

プロファイル 送信のタイミング 受信者 コンテンツ

件名 Welcome, {'Attribute: cn'}

マネージャ属性 Business Phone (telephoneNumber)

一書式 フォント サイズ A A A * A A

Hello, {'Attribute: givenName'},

Welcome to Forward, Inc. We are so glad that you joined our team!

Here are some helpful links to get you started in your new role:

[Employee home page](#)

[Intranet](#)

You may also need the following information about your department and manager:

Department: {'Attribute: departmentNumber'}

Manager: {'Manager Attribute: cn'}

Manager Phone: {'Manager Attribute: telephoneNumber'}

電子メール テンプレート の 使用方法

CA Identity Manager には、電子メール メッセージの生成に使用できるデフォルトの電子メール テンプレートが含まれています。インストールされたままのデフォルト テンプレートを使用することも、ニーズに合わせてカスタマイズすることもできます。

電子メール テンプレート の 使用方法

1. CA Identity Manager が電子メール通知を送信できるように SMTP を設定します。
2. [管理コンソールでの電子メール通知の有効化](#) (P. 396)
3. [電子メールを送信するためのイベントまたはタスクを設定します。](#) (P. 396)
4. (オプション) 必要に応じて、[デフォルトのテンプレートをカスタマイズ](#) (P. 402) します。

電子メール通知の有効化

CA Identity Manager 環境に対して、電子メール通知を有効にしたり、無効にしたりできます。電子メール通知を有効にすると、CA Identity Manager は、指定したイベントおよびタスクに対して電子メール通知を送信します。

注: 忘れたパスワードの機能を使用するには、電子メール通知を有効にします。

CA Identity Manager で電子メール通知を有効にする前に、アプリケーション サーバに対して [SMTP を設定](#) (P. 382) してください。

電子メール通知を有効にする方法

1. 管理コンソールで、[環境] をクリックします。
CA Identity Manager 環境の一覧が表示されます。
2. 該当する CA Identity Manager 環境をクリックします。
3. [詳細設定]- [電子メール]の順に進みます。
4. [有効] チェックボックスをオンにします。
5. [電子メールをトリガするイベントおよびタスクを設定します](#) (P. 396)。
6. [保存] をクリックします。
7. CA Identity Manager がインストールされているアプリケーション サーバのインスタンスを再起動します。

電子メールを送信するためのイベントまたはタスクの設定

電子メールの通知が有効になっていると、電子メール通知をトリガするイベントまたはタスクのリストを指定することができます。たとえば、以下の場合に電子メールを送信したいとします。

- [ユーザ パスワードのリセット] タスクの完了時にシステム管理者に対して送信する場合。
- [ユーザの作成]タスクの完了時に、新しい従業員のマネージャに対して送信する場合。また、[ユーザの作成]タスクで生成された AddToGroupEvent が承認された場合に、新しいユーザが追加されるグループのすべてのメンバに対して、別の電子メールを送信することもできます。

電子メール通知をトリガするイベントおよびタスクを指定する方法

1. 管理コンソールで、[環境] をクリックします。
CA Identity Manager 環境の一覧が表示されます。
2. 該当する CA Identity Manager 環境をクリックします。

3. [詳細設定]- [電子メール]の順に進みます。

電子メール プロパティ画面が表示されます。

4. 以下の有効化のチェックボックスで、適切なものを選択します。

- イベント電子メール有効化

CA Identity Manager のイベントに対する電子メール通知を有効化します

- タスク電子メール有効化

CA Identity Manager のタスクに対する電子メール通知を有効化します

5. CA Identity Manager が電子メール メッセージの作成に使用する、電子メール テンプレートの場所を入力します。

電子メール テンプレートは、以下の場所のサブディレクトリに格納されています。

`iam_im.ear¥custom¥emailTemplates`

注: 別の言語を使用しているファイル名の電子メール テンプレート ファイルを作成する場合は、オペレーティング システムのセッションで、文字セットをサポートしている言語を操作する必要があります。

6. 電子メールの通知を送信するイベントを、次のように指定します。

- イベントを追加するには、[イベント]リスト ボックスでイベントを選択し、[追加]をクリックします。

CA Identity Manager により、電子メール通知を送信するイベントのリストに対して、選択したイベントが追加されます。

注: ワークフロー プロセスに関連付けられていないイベントを選択すると、CA Identity Manager は、イベントの完了時に電子メール通知を送信します。

- イベントを削除するには、そのイベントのチェックボックスをオンにして [削除]をクリックします。

7. 電子メールの通知を送信するタスクを、次のように指定します。

- タスクを追加するには、最初のフィールドで条件を選択してタスクを検索し、2 番目のフィールドにタスク名を入力します。 [検索] をクリックします。

ワイルドカード (*) 文字を使用して、タスク名の一部を入力することができます。たとえば、作成のタスクを検索するには、「作成*」と入力します。

検索結果から、1 つ以上のタスクを選択します。 [追加] をクリックします。

注: アクションタイプが [表示] または [自己表示] のタスクでは、タスクレベルの電子メール通知は使用できません。 タスクのアクションタイプを参照するには、[管理タスクの変更] - [Select a Task] を選択し、タスク プロファイルのアクションフィールドを確認します。

- タスクを削除するには、そのタスクのチェックボックスをオンにして [削除] をクリックします。

タスクを削除すると、タスク テーブルからタスクが削除されます。 この処理で、タスクが削除されるわけではありません。

8. 電子メール通知をトリガするタスクおよびイベントの設定が終わったら、[保存] をクリックします。

9. CA Identity Manager がインストールされているアプリケーション サーバを再起動します。

電子メールのコンテンツ

電子メールの通知は、汎用的なテンプレート、および電子メール API によって電子メールに追加された、タスク特有の詳細によって構成されています。たとえば、[ユーザの作成] タスクの場合は、電子メールに次の情報を挿入することができます。

- タスクを実行する管理者の名前
- 新しいユーザの名前
- ユーザの電子メール アドレス、部門名、およびその他の属性データ
- ユーザが作成された組織
- ワークフローの承認ステータスおよび承認時間
- タスク名、およびそのタスクのイベント名

電子メール テンプレート

電子メール通知は、電子メール テンプレートから生成されます。CA Identity Manager に用意されているデフォルトの電子メール テンプレートは、インストール時の状態でそのまま使用することも、独自の電子メール テンプレートを作成するために使用することもできます。

各電子メール テンプレートには、次の情報が含まれています。

- **配信情報**：電子メールの受信者リスト。CA Identity Manager は、このタスクに含まれているユーザに基づいて、受信者のリストを自動的に生成します。たとえば、承認の電子メールは、このタスクに対するすべての承認者へ送信されます。
- **件名**：メッセージの件名の行で使用されているテキスト。
- **内容**：メッセージの本文。本文には通常、静的なテキストと変数の両方が含まれています。CA Identity Manager は、電子メールをトリガするタスクまたはイベントに基づいてこれらを解決します。

デフォルトの電子メール テンプレートは、CA Identity Manager の管理ツールがインストールされている、**emailTemplates** ディレクトリに格納されています。管理ツールのデフォルトのインストール場所は次のとおりです。

- Windows の場合：C:\Program Files\CA\IAM Suite\Identity Manager\tools\emailtemplates
- UNIX の場合：<home_directory>/CA/IAM Suite/Identity Manager/tools/emailtemplates

emailTemplates ディレクトリには、次の 5 つのフォルダが含まれています。各フォルダは、1 つのタスクまたはイベントのステートに関連付けられています。

ディレクトリ	内容
承認済み	defaultEvent.tmpl：イベントが承認されたことを受信者に知らせます。

ディレクトリ	内容
完了	■ CertificationNonCertifiedActionCompletedNotification.tmpl: 非準拠のアクションが従業員に適用されたことを、マネージャに知らせます。 ■ CertificationNonCertifiedActionPendingNotification.tmpl: 非準拠のアクションが従業員に適用されそうであることを、マネージャに知らせます。 ■ CertificationRequiredFinalNotification.tmpl: ある従業員に対して [ユーザの認証] タスクを完了しなければならないことをマネージャに知らせる最終確認。 ■ CertificationRequiredNotification.tmpl: ある従業員に対して認証プロセスが開始されたことをマネージャに知らせます。マネージャは、この従業員に対して、[ユーザの認証] タスクを完了する必要があります。 ■ CertificationRequiredReminderNotification.tmpl: ある従業員に対して [ユーザの認証] タスクを完了しなければならないことを、マネージャに指摘します。 ■ Certify Employee.tmpl: ある従業員に対する認証プロセスが完了したことを管理者に知らせます。 ■ CreateProvisioningUserNotificationEvent.tmpl: プロビジョニング ディレクトリでユーザのアカウントが作成されたときに、そのユーザに一時的なパスワードを送信します。 ■ defaultTask.tmpl: CA Identity Manager がタスクを完了したことを受信者に知らせます。 ■ ForgottenPassword.tmpl: 忘れたパスワードの機能を使用したユーザに対して、一時的なパスワードを送信します。 ■ ForgottenUserID.tmpl: 忘れたユーザ ID の機能を使用したユーザに対して、ユーザ ID を送信します。 ■ Self Registration.tmpl: 自己登録タスクが正常に完了したことをユーザに通知します。
無効	■ AssignProvisioningRoleEvent.tmpl: ユーザをプロビジョニング ロールへ追加する要求が失敗したことを受信者に知らせます。 ■ DefaultEvent.tmpl: イベントが失敗したことを受信者に知らせます。 ■ DefaultTask.tmpl: CA Identity Manager のタスクが失敗したことを受信者に知らせます。

ディレクトリ	内容
保留中	■ defaultEvent.tmpl : ワーク リスト アイテムで注意が必要であることを承認者に知らせます。 ■ ModifyUserEvent.tmpl : デフォルトのテンプレートと同じですが、ユーザ管理オブジェクトの属性を取得するためのメソッドが含まれています。
拒否	defaultEvent.tmpl : イベントが拒否されたことを受信者に知らせます。

<im_admin_tools_dir>%Identity Manager%tools% にインストールされている、CA Identity Manager のテンプレートおよびテンプレート ディレクトリ構造を使用します。
電子メールのカスタム テンプレートを作成するためのベースとしての emailTemplates ディレクトリ。

テンプレート ディレクトリ

「[電子メール テンプレート \(P. 399\)](#)」で説明されている、各テンプレート ディレクトリは、特定のタスクまたはイベントのステートに関連付けられています。たとえば、ワークフロー プロセスで拒否されたイベントに対して電子メールを送信すると、CA Identity Manager は、配置されている拒否ディレクトリの中で、使用するテンプレートを検索します。CA Identity Manager は、ディレクトリ内の適切な電子メール テンプレートから電子メールを生成します。

ディレクトリ内の電子メール テンプレート

配置されている各テンプレート ディレクトリには、1 つ以上の電子メール テンプレートが含まれています。電子メールが有効になっているタスクまたはイベントが発生すると、CA Identity Manager は、該当するテンプレート ディレクトリで、タスクまたはイベントの名前と同じテンプレート名を検索します。このようなテンプレートが見つからない場合、CA Identity Manager はディレクトリ内のデフォルトのテンプレートを使用します。デフォルトのテンプレート名は「[電子メール テンプレート \(P. 399\)](#)」に記載されています。たとえば、CA Identity Manager は Pending ディレクトリ内の defaultEvent.tmpl を使用して、新しいワーク リスト項目があることを承認者に知らせます。

テンプレート ディレクトリのセット

テンプレート ディレクトリのセットには、承認済みディレクトリ、完了済みディレクトリ、保留中ディレクトリ、および拒否されたディレクトリが含まれています。テンプレート ディレクトリの複数のセットを配置して、特定の **CA Identity Manager** 環境に対して使用する 1 つのセットを指定することができます。

「[電子メール テンプレートの配置](#) (P. 423)」には、テンプレート ディレクトリのセットを配置するための情報が記載されています。

電子メールテンプレートディレクトリを設定し、**CA Identity Manager** で特定の環境に対して正しいセットを使用できるようにするための詳細については、「**CA Identity Manager 設定ガイド**」を参照してください。

電子メール テンプレートの作成

電子メールのカスタム メッセージの作成方法

1. 修正するテンプレートを開きます。

たとえば、保留中の「ユーザの作成」イベントに対して電子メール メッセージを作成したい場合は、**Pending** ディレクトリの **defaultEvent.tmpl** を開きます。

2. このテンプレートに別の名前を付けて、同じディレクトリに保存します。テンプレート名は、電子メールを適用するイベント名と一致していること、および拡張子 **.tmpl** を持っていることが必要です。

たとえば、保留中の「ユーザの作成」イベントに対するメッセージには、次のように名前を付けます。

CreateUserEvent.tmpl

注: 別の言語を使用しているファイル名の電子メールテンプレートファイルを作成する場合は、オペレーティングシステムのセッションで、文字セットをサポートしている言語を操作する必要があります。

3. 次のセクションの「[電子メールのカスタム テンプレート](#) (P. 403)」に記載されているように、必要に応じてメッセージ テンプレートを修正します。

電子メールのカスタム テンプレート

電子メールテンプレートは、HTML および埋め込み型サーバサイド JavaScript の両方をサポートするダイナミック ファイルです。テンプレートによって静的テキストに変数値を挿入することができるため、単一のテンプレートによる大文字と小文字を区別したメッセージの生成が可能になります。

同じテンプレートを何度も使用して、定型的な静的テキスト（承認されているフレーズなど）と、所定のコンテキストに特有の可変的なテキスト（承認中のイベント名など）を合わせて印刷することができます。

たとえば、イベントの承認をレポートするテンプレートは次のようになります。

```
<!-- Define the E-mail Properties --->
<%
_to = _util.getNotifiers("ADMIN");
_cc = "";
_bcc = "";
_subject = _eventContextInformation.getEventName() + " approved";
%>
<!-- Start of Body --->
<html>
<body text="Navy">

Event: <b> <%= _eventContextInformation.getEventName() %> </b><br>
<%= _eventContextInformation.getPrimaryObjectTypeName() %>:
<b><%= _eventContextInformation.getPrimaryObjectName() %></b><br>
In <%= _eventContextInformation.getSecondaryObjectTypeName() %>:
<b><%= _eventContextInformation.getSecondaryObjectName() %></b><br>
Status: <b>Approved</b>
</body>
</html>
```

注：上記の例で使用されている、CA Identity Manager のオブジェクトの `_util` および `_eventContextInformation` については、「[電子メール テンプレート API \(P. 406\)](#)」で説明しています。

イベント `CreateUserEvent` に対して承認が生成され、HR の組織で John Jones というユーザが作成された場合、この承認テンプレートから生成される電子メール通知は次のようになります。

イベント: **CreateUserEvent**

USER: **John Jones**

In ORGANIZATION: **HR**

Status: **Approved**

以降のセクションでは、動的な電子メール メッセージを可能にする構文および CA Identity Manager のオブジェクトについて説明します。

テンプレートのエレメント

CA Identity Manager の電子メール テンプレートは以下のものをサポートしています。

- 標準の HTML タグ
- サーバーサイド JavaScript
- 1 つ以上の暗黙的なオブジェクト（CA Identity Manager がテンプレートの 1 つのインスタンス、つまり電子メール メッセージを利用できるようにするもの）
- CA Identity Manager のタグ。このタグを使用して JavaScript をテンプレートに埋め込む、CA Identity Manager の暗黙的なオブジェクトでメソッドをコールする、変数値をテンプレートの静的テキストに挿入する、といったことが可能。

CA Identity Manager タグの拡張

電子メール テンプレートは以下のタグをサポートしています。

`<% %>`

電子メール テンプレートに JavaScript を埋め込みます。

`<%= %>`

静的なテキストに可変的な値を挿入します。

以降のセクションでこれらのタグについて説明します。

`<% %>`

このタグを使用して、インライン実行のための JavaScript を電子メール テンプレートに埋め込むことができます。

埋め込まれた JavaScript では、任意の JavaScript オブジェクトを使用できます。埋め込まれた JavaScript では、CA Identity Manager の暗黙的なオブジェクト メソッドをコールすることもできます。

たとえば、次のコードは、「[電子メールのカスタム テンプレート \(P. 403\)](#)」で示した承認テンプレートの本文を変更します。ここでは JavaScript を使用して、セカンダリ オブジェクトがイベントに含まれているかどうかを決定します (USER プライマリ オブジェクトが追加された場合の ORGANIZATION オブジェクトなど)。セカンダリ オブジェクトがない場合は、セカンダリ オブジェクトに関連するテキストがメッセージから削除されます。

```
Event: <b> <%= _eventContextInformation.getEventName() %> </b><br>
<%= _eventContextInformation.getPrimaryObjectTypeName() %>:
<b><%= _eventContextInformation.getPrimaryObjectTypeName() %></b><br>
<%
vvar secondaryType =      _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
    template.add("In " + secondaryType + ": ");
    template.add("<b> "+_eventContextInformation.getSecondary
                                ObjectName()+" </b><br>");
    }
%>
Status: <b>Approved</b>
```

<%= %>

このタグを使用して、可変的な値を静的なテキストに挿入することができます。値として、次のものを使用できます。

- テンプレート内で以前に実行された JavaScript で定義されている変数。例：

```
<%
vvar secondaryType
=      _eventContextInformation.getSecondaryObjectTypeName();
...      // More JavaScript processing
%>
...      // More HTML
The primary object was created in <%=secondaryType%>.
```

- CA Identity Manager の暗黙的なオブジェクトにおいてメソッドから返された値。例：

```
Event <%= _eventContextInformation.getEventName() %> is approved.
```

電子メール テンプレート API

テンプレートからメッセージが生成されると、CA Identity Manager は、以下の暗黙的なオブジェクトをメッセージで使用できるようにします。これらのオブジェクトを使用すると、電子メールテンプレート API でメソッドをコールすることによって、インスタンス特有の情報をメッセージに挿入できます。

テンプレートは、次のいずれかのオブジェクトでメソッドをコールできます。

- `_contentType` : 電子メールの `contentType` を指定します。
- `_priority` : 電子メールの優先度を指定します。
- `_to` : メッセージの `[To]` フィールドに受信者を追加します。
- `_cc` : メッセージの `[cc]` (コピーを送信) フィールドに受信者を追加します。
- `_bcc` : メッセージの `[bcc]` (ブラインドコピーを送信) フィールドに受信者を追加します。
- `_subject` : 電子メールの件名を指定します。
- `_encoding` : 電子メールのエンコーディングを指定します。
- `_additionalHeaders` : 電子メール テンプレートで余分な電子メール ヘッダ属性を指定することを可能にします。
- `template` : JavaScript コードの行からメッセージヘテキスト文字列を追加できるようにします。
- `_util` : ユーティリティ オブジェクト。
- `_eventContextInformation` : イベント名や承認ステータスなど、現在のタスクにより生成されたイベントに関する情報を含みます。
- `_taskContextInformation` : タスク名、組織名、および構成イベントなどの現在のタスクに関する情報を含みます。

以降のセクションで、これらのオブジェクトについて説明します。

contentType

電子メールの `contentType` を指定します。

`contentType` が specified through `_contentType` 変数の場合、デフォルトの `contentType` である「text/html」が適用されます。

メソッド: なし。

例 :

```
<% _contentType = "text/html"; %>
```

priority

電子メールの優先度を指定します。優先度なし（デフォルト）には `0`、高優先度には `1` を指定します。

メソッド: なし。

例 :

```
<% _priority = "1"; %>
```

to

メッセージの `[To]` フィールドに受信者を追加します。

`_to variable` の値は JavaScript 文字列です。複数の受信者が許可されていますが、以下の例のに示されるように文字列は JavaScript 構文に準拠する必要があります。

メソッド: なし。

例：

```
<%
_to =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "" ;
_bcc = "" ;
_subject = "Your new password ";
%>
```

注: 電子メールが参加者にワークフロー コントロールに保留状態のタスクがあることを警告する場合、`_to` オブジェクトに受信者のアドレスが事前入力されます。Pending テンプレートに `_to` オブジェクトを使用することはできません。

cc

メッセージの [cc]（コピーを送信）フィールドに受信者を追加します。

`_to variable` の値は JavaScript 文字列です。複数の受信者が許可されていますが、以下の例のに示されるように文字列は JavaScript 構文に準拠する必要があります。

メソッド: なし。

例：

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

bcc

メッセージの [bcc]（ブラインド コピーを送信）フィールドに受信者を追加します。

このフィールドで指定された電子メール アドレスは、電子メールには表示されません。

`_to variable` の値は JavaScript 文字列です。複数の受信者が許可されていますが、以下の例のに示されるように文字列は JavaScript 構文に準拠する必要があります。

メソッド: なし。

例 :

```
<%  
_bcc =  
_util.getNotifiers("USER") + ',' +  
_util.getNotifiers("USER_MANAGER", "ManagerLookup=managerattribute");  
%>
```

subject

電子メールの件名を指定します。

メソッド: なし。

例 :

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

encoding

電子メールのエンコーディングを指定します。

エンコーディングが `_encoding` または `LANG` 変数のどちらかで指定されている場合、電子メールの文字が正しく表示されない可能性があります。必ず `set _encoding` または `LANG` を設定し、適切なローケルを設定してください。

メソッド: なし。

例 :

```
<% _encoding = "UTF-8"; %>
```

additionalHeaders

`_additionalHeaders`

電子メール テンプレート内のその他の電子メール ヘッダ属性を指定します。

この属性には、`HashMap()` を割り当てる必要があります。 `HashMap` に格納された名前と値は文字列である必要があります。

例: カスタム ヘッダ属性の追加

以下の例は、2つのカスタム ヘッダ属性、「X-TCCCSWD」および「myheader」を追加する方法を示しています。

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```

template

JavaScript コードの行（<% %> タグ内の行）からメッセージにテキストの文字列を追加できます。文字列には HTML タグ、静的テキスト、および CA Identity Manager の implicit オブジェクトでメソッドにより返される変数値を含めることができます。

注: template オブジェクトは最初の下線（_）文字はつきません。

メソッド:

- add(String)

引数は、CA Identity Manager の implicit オブジェクトのメソッドに対するすべてのコールも含めて、文字列に数値を求める必要があります。以下の例にある `_eventContextInformation.getSecondaryObjectName()` を参照してください。

例 :

```
<%
vvar secondaryType = _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
    template.add("In " + secondaryType + ": ");
    template.add("<b> "+_eventContextInformation.getSecondary
                                   ObjectName()+" </b><br>");
}
%>
```

util

ユーティリティ オブジェクト。

メソッド:

- getNotifiers(String [,String])

通知ルールに基づいて電子メール ID を返します。

最初の引数は、以下の引用符で囲まれた定義済み通知ルールをサポートします。

- "ADMIN"。タスクを開始した管理者に電子メールを送信します。
- "USER"。現在のコンテキストのユーザに電子メールを送信します。
- "USER_MANAGER"。現在のコンテキストのユーザの管理者に電子メールを送信します。

Notification Rule API で作成するカスタム通知ルールを参照することもできます。詳細については、「*Java のプログラミングガイド*」を参照してください。

秒の引数はオプションです。引数を使用して、ユーザ定義された名前/値の 1 つ以上のペアをカスタム通知ルールに渡すことができます。名前/値のペアは、以下の形式でコンマ区切りとします。

`"name1=value1,name2=value2,..."`

例 :

```
<%
_to = _util.getNotifiers("ADMIN");
_cc = "";
%>
<%
_to = _util.getNotifiers("MYRULE","type=loan,district=3");
_cc = "";
%>
```

ユーザのマネージャへの通知

USER_MANAGER 通知ルールを使用して、ユーザのマネージャに電子メールを送信できます。CA Identity Manager はこのルールを電子メール テンプレートで使用し、ユーザ資格認証をサポートします。

注: The USER_MANAGER 通知ルールは、単一のユーザを作成または管理するイベントまたはタスクにのみ適用されます。

ユーザからマネージャへの関係をユーザ ディレクトリ内で指定する方法が数多くあるため、デフォルトのユーザ マネージャ通知アダプタは、`getNotifiers()` メソッドの第 2 パラメータ内で指定された属性式に基づいてこの関係を解決します。

例 :

```
<%
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "";
%>
```

ユーザ マネージャ通知アダプタは、2 つの検索オプションをサポートしています。

- `managerattribute = <Manager AttributeName>` - User オブジェクトがユーザのマネージャの DN またはユーザ ID を示す属性を維持する場合
- `commonattribute = <AttributeName>` - ユーザおよびユーザのマネージャが「部署」などの共通属性値を共有する場合

これらの検索オプションは、CA Identity Manager の管理コンソール内にある環境の [その他] 属性で設定します。

USER_MANAGER 通知ルールを設定する方法

1. CA Identity Manager 管理コンソールで、CA Identity Manager 環境を選択します。次に、電子メール通知を設定する環境を選択します。
2. [詳細設定] - [Miscellaneous Properties] を選択します。
3. [Miscellaneous Properties] ページで、使用する検索オプション用の設定手順を完了させます。
 - managerattribute=<Manager AttributeName> 検索オプションを使用する方法
 - a. [プロパティ] フィールドに managerattribute を入力します。
 - b. [値] フィールドでマネージャの DN または ユーザ ID を格納する属性を入力します。
 - c. [追加] をクリックします。
 - d. [保存] をクリックします。
 - commonattribute=<AttributeName> 検索オプションを使用する方法
 - a. [プロパティ] フィールドに commonattribute を入力します。
 - b. [値] フィールドでユーザおよびユーザのマネージャが共有する属性を入力します。
 - c. [追加] をクリックします。
 - d. [プロパティ] フィールドに ismanagerfilter を入力します。
 - e. [値] フィールドで以下の構文を使用した検索式を入力します。
`<attribute> <operator> <filter>`
たとえば、役職 EQUALS マネージャ
 - f. [追加] をクリックします。
 - g. [保存] をクリックします。

カスタム アダプタを記述して、ユーザのマネージャへの通知に関する独自のルールを作成することもできます。「Java のプログラミングガイド」を参照してください。

eventContextInformation

イベント名や承認ステータスなど、現在のタスクにより生成されたイベントに関する情報を含みます。この情報は、イベントのコンテキスト情報と呼ばれます。

`_eventContextInformation` オブジェクトは、パッケージ `com.netegrity.imapi` の `ExposedEventContextInformation` クラスから作成されます。

このオブジェクトは **Approved**、**Pending**、および **Rejected** テンプレートに基づく電子メール メッセージに利用できます。これらのテンプレートの詳細については、「[電子メール テンプレート](#) (P. 399)」を参照してください。

メソッド：以下のすべてのメソッドは文字列を返します。

メソッド	説明
<code>getAdminName()</code>	イベントを生成したタスクをサブミットした人の名前を返します。 CA Identity Manager 5.6 では廃止されています。以下のいずれかのメソッドを使用します。 ■ <code>getAdministrator()</code> ■ <code>getAdminFriendlyName()</code>
<code>getApprovalStatus()</code>	イベントの承認ステータスを返します。次のいずれかの値を取ります。 <code>APPROVAL_STATUS_APPROVED</code> <code>APPROVAL_STATUS_REJECTED</code>
<code>getApprovalTime()</code>	イベントが承認された時間を返します。
<code>getEventName()</code>	イベントの名前を返します。 イベント名のリストについては、「CA Identity Manager イベント」を参照してください。
<code>getOrgName()</code>	タスクが実行されている組織のわかりやすい名前を返します。 CA Identity Manager 5.6 では廃止されています。継承されたメソッド <code>getObjectOrganizationFriendlyName()</code> を使用します。
<code>getPassword()</code>	プライマリ オブジェクトがタイプ USER の場合、ユーザのパスワードを返します。

メソッド	説明
<code>getPrimaryObjectName()</code>	プライマリ オブジェクトのタイプを返します。 返されるプライマリ オブジェクト: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
<code>getPrimaryObjectTypeName()</code>	イベントに影響されるプライマリ オブジェクトの名前を返します。 プライマリ オブジェクトは、イベントから直接影響を受けるオブジェクトです。セカンダリ オブジェクトは、プライマリ オブジェクトに関連があるオブジェクトです。 以下に例を示します。 ■ <code>CreateUserEvent</code> のプライマリ オブジェクトタイプは <code>USER</code> です。セカンダリ オブジェクトはユーザが作成されるオブジェクト、すなわち <code>ORGANIZATION</code> です。 ■ <code>CreateAdminRoleEvent</code> のプライマリ オブジェクトタイプは <code>ADMINROLE</code> です。このオブジェクトは他のオブジェクトと関連しないため、セカンダリ オブジェクトは存在しません。 タイプ <code>USER</code> のプライマリ オブジェクトでは、<code>getPrimaryObjectName()</code> は <code>John Jones</code> を返す場合があります。

メソッド	説明
<code>getSecondaryObjectTypeName()</code>	セカンダリ オブジェクトがイベントの影響を受けた場合、オブジェクト タイプを返します。 返されるセカンダリ オブジェクト タイプ: ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
<code>getSecondaryObjectName()</code>	セカンダリ オブジェクトがイベントの影響を受けた場合、オブジェクト名を返します。 プライマリおよびセカンダリ オブジェクトの情報については、 <code>getPrimaryObjectName()</code> を参照してください。 タイプ ORGANIZATION のセカンダリ オブジェクトでは、 <code>getSecondaryObjectName()</code> は HR を返す場合があります。

注: methods in `_eventContextInformation` は、インターフェース `ExposedEventContextInformation` から提供されます。
`ExposedEventContextInformation` はコア CA Identity Manager API のメソッドを継承するため、`_eventContextInformation` は上記の表に記載されたメソッドに加えて、これらのメソッドも電子メール テンプレートからコールできます。これらの継承されたメソッドの詳細については、「[追加のメソッド](#) (P. 420)」を参照してください。

例-- [Pending] イベントに関する電子メール通知:

```
<%
_cc = "" ;
_bcc = "";
_subject = _eventContextInformation.getEventName() +
           " 承認リクエスト";
%>
<!-- Start of Body --->
<html>
<body text="Navy">
```

以下のアイテムがワーク リストに追加され、承認待ちです:

```
<br><br><br>
イベント: <b><%= _eventContextInformation.getEventName()%></b> <br>
<%= _eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%= _eventContextInformation.getPrimaryObjectName()%></b><br>
所属 <%= _eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%= _eventContextInformation.getSecondaryObjectName()%></b><br>
</body>
</html>
```

電子メールの本文はこのようになります:

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent 承認リクエスト

以下のアイテムがワーク リストに追加され、承認待ちです:

イベント: **CreateUserEvent**
 USER: **Richard Ferrigamo**
 所属 ORGANIZATION: **Mortgages & Loans**

注: [From] フィールドの値は、email.properties ファイルから派生します。値を変更するには、以下のファイルを編集します。

```
<iam_im.ear>%config%com%netegrity%config%email.properties
```

<iam_im.ear> は、アプリケーション サーバドメイン内の CA Identity Manager がインストールされた場所です。以下に例を示します。

WebLogic の場合:

```
<WebLogic_home>%user_projects%<domain>%applications%iam_im.ear
```

JBoss の場合:

```
<Identity Manager_home>%jboss-3.2.2%server%default%deploy%iam_im.ear
```

WebSphere の場合:

```
<im_admin_tools_dir >%WebSphere-ear%iam_im.ear
```

イベントにより影響されたユーザに関する追加情報を前述の例にある電子メールに追加するには、以下のようなテキストを追加します。

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>ユーザ情報:</b><br>
ラスト ネーム: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
ファースト ネーム: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
フル ネーム: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
電子メール: <b><%=user.getAttribute("%EMAIL%")%></b><br>
組織メンバシップ: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

電子メールの本文はこのようになります:

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent 承認リクエスト

以下のアイテムがワーク リストに追加され、承認待ちです:

イベント: **CreateUserEvent**
USER: **Richard Ferrigamo**
所属 ORGANIZATION: **Mortgages & Loans**
ユーザ情報:
ラスト ネーム: Ferrigamo
ファースト ネーム: Richard
フル ネーム: Richard Ferrigamo
電子メール: rferrigamo@mybank.org
組織メンバシップ: **Mortgages & Loans**

taskContextInformation

タスク名、組織名、および構成イベントなどの現在のタスクに関する情報を含みます。この情報は、タスクのコンテキスト情報と呼ばれます。

このオブジェクトは、および **Completed** テンプレートに基づく電子メールメッセージに利用できます。このテンプレートの詳細については、「[電子メール テンプレート](#) (P. 399)」を参照してください。

メソッド: 以下の全てのメソッドは、**Java Vector** を返すメソッド
getExposedEventContexts() を除いて、文字列を返します。

メソッド	説明
getAdminName()	タスクをサブミットしている人の名前を返します。 CA Identity Manager 5.6 では廃止されています。以下のいずれかのメソッドを使用します。 ■ getAdministrator() ■ getAdminFriendlyName()
getExposedEventContexts()	タスクに関連付けられているすべてのイベントの Java Vector を返します。 Vector 内の各イベントは、イベント コンテキストオブジェクトです。 _eventContextInformation にリストされているメソッドを使用して、任意のイベントオブジェクト用にコンテキスト情報を取得できます。 return オブジェクトは標準の Java Vector オブジェクトです。 Vector のエレメント管理には、たとえば Vector の get() および size() など、 Vector オブジェクトのメソッドをどれでも使用できます。
getOrgName()	タスクが実行されている組織の名前を返します。 CA Identity Manager 5.6 では廃止されています。継承されたメソッド getObjectOrganizationFriendlyName() を使用します。
getTaskName()	実行されているタスクの名前を返します。 CA Identity Manager 5.6 では廃止されています。以下のいずれかのメソッドを使用します。 ■ getAdminTask() ■ getTaskFriendlyName()

注: methods in **_taskContextInformation** は、インターフェース **ExposedTaskContextInformation** から提供されます。 **ExposedTaskContextInformation** はコア **CA Identity Manager API** にメソッドを継承するため、**_taskContextInformation** はこれらのメソッドを上記の表にあるメソッドのみならず電子メール テンプレートからもコールできます。これらの継承されたメソッドの詳細については、「[追加のメソッド](#) (P. 420)」を参照してください。

例--パスワード変更用の電子メール 通知テンプレートの本文:

```
<%  
var imsEventContexts  
=      _taskContextInformation.getExposedEventContexts();  
if(imsEventContexts != null)  
{  
    for(var i=0;i<imsEventContexts.size();i++)  
    {  
        var eventContext = imsEventContexts.get(i);  
        template.add("Hi "+  
eventContext.getPrimaryObjectName()  
            + ",");  
        template.add("<br>新しいパスワード: <b>" +  
            eventContext.getPassword());<br>  
        template.add("<hr>");  
    }  
}  
%>
```

電子メールの本文はこのようになります:

Hi Victor Imperioso,
新しいパスワード: LFH7F1226

追加のメソッド

`_taskContextInformation` および `_eventContextInformation` のメソッドは、それぞれ CA Identity Manager オブジェクトの `ExposedTaskContextInformation` と `ExposedEventContextInformation` を使用して提供されます。

これらのオブジェクトは、コア CA Identity Manager API のメソッドを継承します。その結果、`_taskContextInformation` および `_eventContextInformation` も継承されたメソッドを使用できます。

`TaskInfo` オブジェクトから継承された以下のメソッドは、特に電子メール テンプレートに役立ちます。

- `getAdministrator()`. 現在のタスクを実行している管理者の `User` オブジェクトを取得します。
- `getAdminTask()`. 現在のタスクの `AdminTask` オブジェクトを取得します。

これらの取得されたオブジェクトにより、管理者固有およびタスク固有の情報を電子メールに挿入できます。以下に例を示します。

```
<!-- Define the E-mail Properties --->
```

```
<%
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +
" 承認リクエスト";
%>
```

```
<!-- Start of Body --->
```

```
<html>
```

```
<body text="Navy">
```

以下のアイテムがワーク リストに追加され、承認待ちです:


```
<br>
```

```
User <b><%= _eventContextInformation.getAdministrator().
getAttribute(Packages.com.netegrity.llsdk6.imsapi.
managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
from department <b><%= _eventContextInformation.
getAdministrator().getOrg(null).getFriendlyName()
%></b> initiated task <b><%= _eventContextInformation.
getAdminTask().getFriendlyName() %></b>at
<b><%=
_eventContextInformation.getSessionCreateTime() %></b>
```

```
<br><br>
```

```
<font color="green">詳細: </font><b><%= _eventContextInformation.
getEventName()%></b><br>
```

```
<font color="green"><%= _eventContextInformation.
getPrimaryObjectTypeName()%>:</font>
```

```
<b><%= _eventContextInformation.getPrimaryObjectName()%></b>
が変更されました
```

```
<br>
```

```
<font color="green">更新された属性:</font>
```

```
<table border="1">
```

```
<tr>
```

```
<td> <b> 名前 </b></td>
```

```
<td> <b> 値 </b></td>
```

```
</tr>
```

```
<%
    var event = _eventContextInformation.getEvent();
    if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
        var user = event.getUser();
        var attributes = user.getAttributes().keys();
        while(attributes.hasMoreElements()) {
            var attr = attributes.nextElement();
            var value = user.getAttribute(attr);
            if(user.hasAttributeChanged(attr)) {
                template.add("<tr><td>" + attr + "</td>");
                template.add("<td>" + value + "</td></tr>");
            }
        }
    }
    %>
</table>
<br>
</body>
</html>
```

電子メールの本文はこのようになります:

以下の項目が、承認のためにワークリストに追加されました。

人事部のロバート・ジェンキンスが、「ユーザの変更」タスクを 3:17 pm に開始しました。

詳細: [ModifyUser Event](#)

ユーザ: ジョン・ジョーンズが変更されました。

更新された属性:

名前	値
電子メール	jjones@mycorp.com
電話番号	781 555 1234

電子メール テンプレート API で利用可能な継承されたメソッドの詳細については、「CA Identity Manager Javadoc」のオブジェクト `ExposedTaskContextInformation` および `ExposedEventContextInformation` を参照してください。

Java 標準出力ストリーム

電子メール メッセージは、JavaScript タグ (`<%>`) から Java 標準出力ストリームにコールすることも可能です。たとえば、以下のコールはメッセージ「Done」をサーバ コンソールに送信します。

```
<%
...// JavaScript processing
out.println("Done.");
%>
```

Javadoc リファレンス

コア CA Identity Manager API から継承するメソッドを含む
ExposedTaskContextInformation および ExposedEventContextInformation オブジェクトの詳細については、「CA Identity Manager Javadoc」を参照してください。

Javadoc のページは、CA Identity Manager Bookshelf で利用可能な「Programming Guide for Java」の HTML バージョンと統合されています。

電子メール テンプレートの展開

CA Identity Manager は電子メールの送信前に、アプリケーション サーバ内の以下のルート ロケーションで、電子メールの生成に使用するテンプレートを検索します。

```
iam_im.ear¥custom¥emailTemplates
```

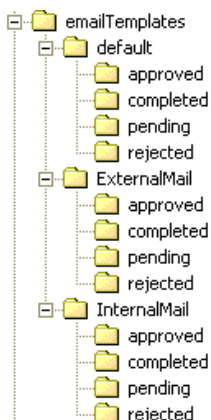
このルートに展開された電子メール テンプレートは同じディレクトリ構造を持つテンプレートセットに含まれ、承認済み、完了、保留、および拒否ディレクトリが各セットに存在します。

テンプレート セット

emailTemplates で、電子メール テンプレートの複数のセットを展開できます。たとえば、インストール中に、以下の電子メール テンプレートのセットが iam_im.ear¥custom¥emailTemplates の下に作成されます。

```
default¥approved  
default¥completed  
default¥pending  
default¥rejected
```

デフォルトの電子メールテンプレートのセットには、[電子メールテンプレート \(P. 399\)](#)で説明されているインストール済みのテンプレートが含まれます。デフォルトのセット内にカスタムテンプレートを追加できます。電子メールテンプレートの他のセットを、デフォルトのセットと同じレベルで定義したディレクトリ構造で展開することもできます。たとえば、iam_im.ear¥custom に、以下の展開された電子メールテンプレートを含めることもできます。



注: CA Identity Manager がテンプレートセット内の特定の電子メールテンプレートを選択する方法の詳細については、「[テンプレートのディレクトリ \(P. 401\)](#)」を参照してください。

環境用のテンプレートセットを指定する方法

CA Identity Manager 環境用に電子メールを設定する場合、この環境に使用する電子メールテンプレートを指定します。CA Identity Manager 環境用の電子メールの設定の詳細については、「*CA Identity Manager 設定ガイド*」を参照してください。

テンプレート名

カスタムテンプレートセット内のディレクトリには、デフォルトテンプレートセットにインストールされたものと同じ名前を持つデフォルトテンプレートが含まれる必要があります。デフォルト名は「[Email Templates \(P. 399\)](#)」に記載されています。CA Identity Manager は、実行中のタスクまたはイベントと一致する名前を持つ他のテンプレートを検出できない場合、デフォルトのテンプレートを使用します。

必要に応じて、特定のテンプレートから電子メールを生成させたい場合、追加テンプレートを 1 つ以上のテンプレート セット内のディレクトリに追加できます。以下の手順を実行します。

- 電子メールが作成されるタスクまたはイベントと同じ名前を、テンプレートに割り当てます。
- 電子メールが作成されるタスクまたはイベントに関連付けられたディレクトリに、テンプレートを配置します。

たとえば、`CreateUserEvent` が拒否されたときに 特定のテンプレートから電子メールを生成させたい場合、`CreateUserEvent.tmpl` という名前のテンプレートを環境のテンプレート セットの `[rejected]` ディレクトリ内に置きます。

第 14 章: レポート

このセクションには、以下のトピックが含まれています。

[設定の概要 \(P. 427\)](#)

[レポートプロセス \(P. 429\)](#)

[スナップショット レポートの実行方法 \(P. 430\)](#)

[スナップショット以外のレポートの実行方法 \(P. 448\)](#)

[レポート オブションの設定 \(P. 454\)](#)

[カスタム スナップショット レポートの作成および実行方法 \(P. 455\)](#)

[ユーザ、アカウント、およびロールの同期 \(P. 470\)](#)

[トラブルシューティング \(P. 478\)](#)

設定の概要

CA Identity Manager 内では、2 つの異なる種類のレポートを実行できます。

スナップショット レポート

スナップショット レポートには、CA Identity Manager オブジェクトストアおよび CA Identity Manager ユーザストアからの情報を含むスナップショット データベースからのデータが含まれています。スナップショット レポートの例は、ユーザ プロファイル レポートです。スナップショット データベースに追加するデータの定義は、追加する情報を指定するスナップショット定義を使用して行います。

スナップショット以外のレポート

監査データベースなど、他のデータ ソースからのデータが含まれています。たとえば、CA Identity Manager には、デフォルトの監査レポートが含まれています。（これらのレポートには、ユーザ コンソール内で、レポートの名前に、「Audit-」のプレフィックスが付けられています。デフォルトでは、CA Identity Manager は監査レポートのみを格納しますが、ユーザは、ワークフローまたはタスク永続性データベースなどあらゆるデータ ソースからのデータを含む独自のカスタム レポートを作成できます。

CA Identity Manager 内の各レポートには、実行する前に初期設定を行う必要があります。設定手順は、実行するレポートの種類によって異なります。

以下の手順は、この章に含まれる手順の概要について説明します。

スナップショットレポートについて

1. スナップショット定義ファイルを作成し、スナップショット データベースに追加するデータを定義します。
2. レポート用のスナップショット データを取り込みます。
3. ユーザ コンソールのレポート タスクを変更し、以下の手順を実行します。
 - a. スナップショット定義をタスクに関連付けます。
 - b. rptParamConn 接続オブジェクトをそのタスクに追加します。
4. 以下のいずれかの方法でレポートを要求します。
 - レポートを即時に実行
 - レポートをスケジュール
5. レポートをユーザ コンソールで表示します。

スナップショット以外のレポートについて

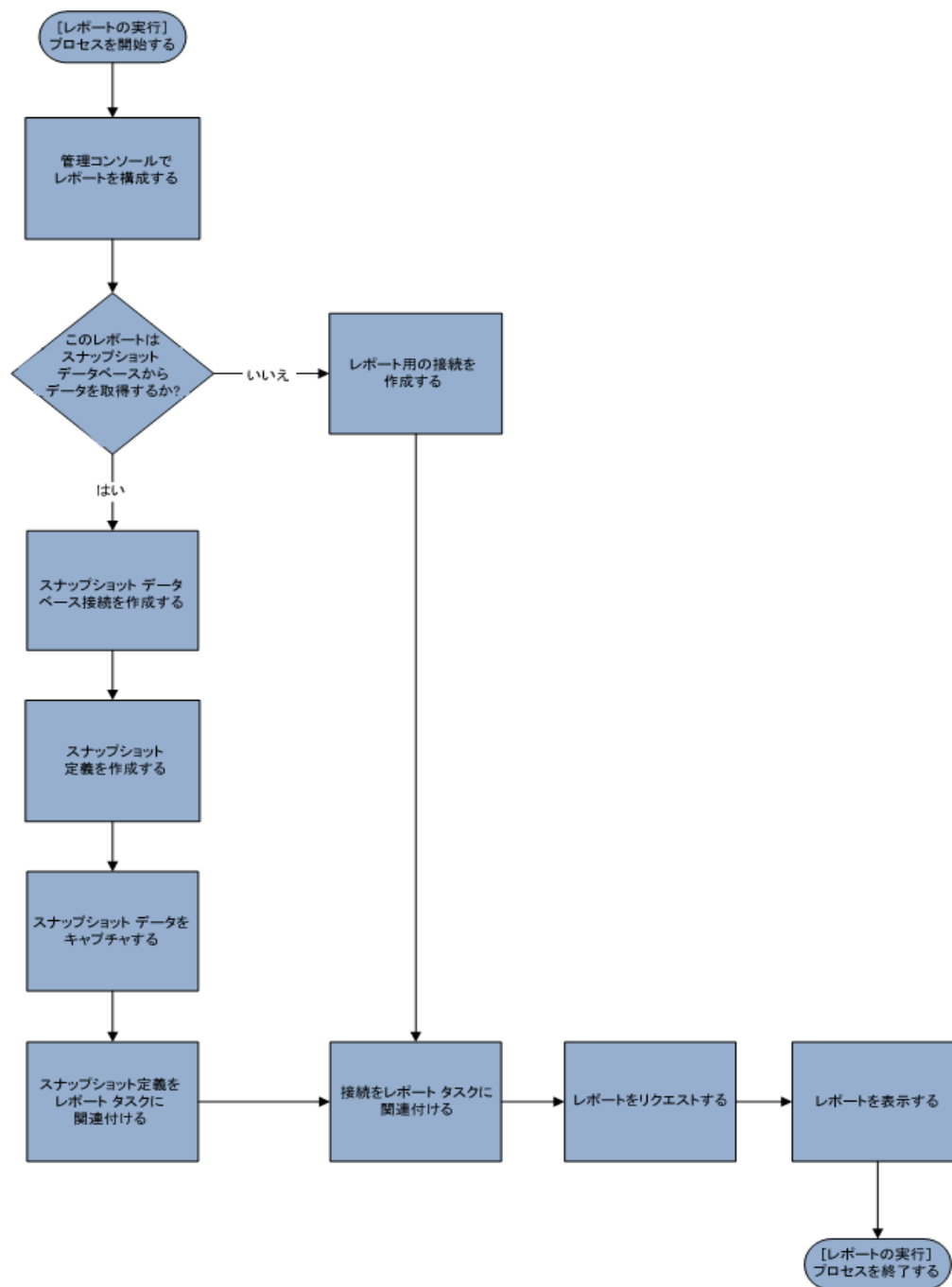
1. レポートのデータ ソース情報を使用して接続オブジェクトを作成します。
2. CA Identity Manager でレポート タスクを修正し、接続オブジェクトをそのタスクに追加します。
3. 以下のいずれかの方法でレポートを要求します。
 - レポートを即時に実行
 - レポートをスケジュール
4. レポートをユーザ コンソールで表示します。

レポートの初期設定が完了したら、CA Identity Manager 内でレポートを要求できます。レポートを即座に実行することも、後日実行するためにスケジュールすることも可能です。また、CA Identity Manager 内で、レポート用の反復スケジュールを作成することもできます。

さらに、ユーザ コンソール内でレポートを表示したり、さまざまな形式にレポートをエクスポートできます。

レポート プロセス

次の図は、レポートの実行と表示に必要なプロセスを詳しく説明しています。



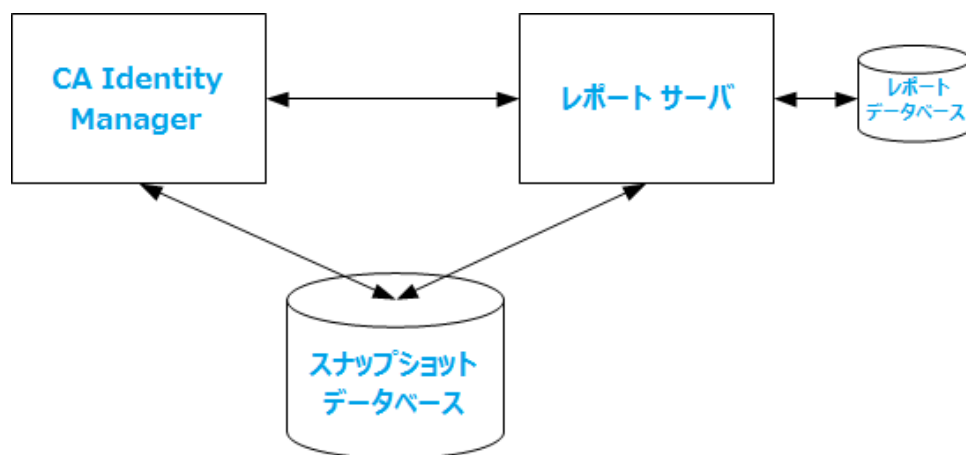
スナップショットレポートの実行方法

CA Identity Manager レポートでは、CA Identity Manager 環境の現在の状態を確認できます。この情報を使って、内部のビジネス ポリシーや外部規制とのコンプライアンスを確保できます。

CA Identity Manager のレポートは、CA Identity Manager 環境 における オブジェクト間の関連性を記述する管理データから作成します。管理データの例には以下のものが含まれます。

- ユーザのプロファイル属性
- 特定のタスクに含まれるロールの一覧
- ロールまたはグループのメンバ
- ロールを構成するルール

CA Identity Manager では、レポートのセットアップに、以下の 3 つの主要コンポーネントが必要です。



注: この図のスナップショット データベースは、監査データベースまたはワークフロー データベースである場合もあります。

レポート サーバ

別名 CA Business Intelligence のこのサーバは、CA Identity Manager およびスナップショット データベースと直接通信して、レポートを生成します。

レポート データベース

CA レポート サーバ (Business Objects) が独自データを格納するデータベース。

CA Identity Manager

CA Identity Manager により、レポート データベースに CA Identity Manager オブジェクト データをエクスポートできるようになります。

スナップショット データベース

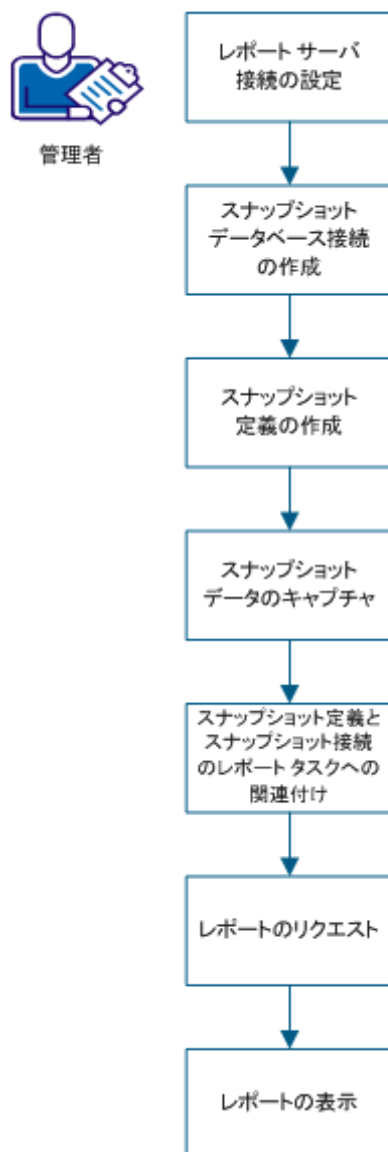
CA Identity Manager 内のオブジェクトのスナップショット データを含む別個のデータベース

重要: レポート サーバは Business Objects Enterprise を使用します。ユーザ環境にすでにレポート サーバがあり、CA Identity Manager と共にそれを使用する場合、CA Identity Manager が必要とする最小バージョンは CA Business Intelligence 3.2 SP5 です。

スナップショット レポートには、CA Identity Manager オブジェクト ストアおよびユーザストアからの情報を含むスナップショット データベースからのデータが含まれています。スナップショット レポートの例は、ユーザ プロファイル レポートです。スナップショット データベースに追加するスナップショット データを定義し、スナップショット 定義を使用して、追加する情報を指定します。

以下の図は、スナップショット レポートを実行するプロセスを示しています。

スナップショットレポートの実行方法



スナップショット レポートを実行するには、以下の手順に従います。

1. [レポートサーバ接続を設定します](#) (P. 449)。
2. スナップショット データベース接続を作成します。
3. スナップショット定義を作成します。
4. スナップショットデータをキャプチャします。
5. スナップショット定義とスナップショット接続をレポート タスクに関連付けます。

6. レポートをリクエストします。
7. [レポートを表示します](#) (P. 453)。

レポート サーバ接続の設定

CA Identity Manager とレポート サーバの間の接続を設定します。

注: レポートに関係するすべてのシステムのタイムゾーンと時刻を同じ設定にすることをお勧めします。

レポートを設定する方法

1. ユーザ コンソールで、[タスク] - [システム] - [レポート] - [レポート サーバ接続] をクリックします。
2. レポート サーバの設定を入力します。以下の点に注意してください。
 - [ホスト名] と [ポート] -- レポート サーバがインストールされているシステムのホスト名および HTTP URL ポート番号。
 - [レポート フォルダ名] -- デフォルト CA Identity Manager レポートの場所。
 - [ユーザ ID] -- レポート サーバ用に作成されたユーザ。
 - [パスワード] -- レポート サーバで作成されたユーザのパスワード。
 - [セキュア接続] -- CA Identity Manager とレポート サーバの間の Secure Sockets Layer (SSL) 接続を有効にするには、このチェック ボックスを選択します。

注: [セキュア接続] チェック ボックスを選択する前に、BOServer から証明書をインストール済みであることを確認してください。SSL の設定方法の詳細については、「インストールガイド」の「レポート サーバのインストール」の章を参照してください。
 - [Web サーバ] -- Tomcat の場合は IIS 以外に設定します。
3. [テスト接続] をクリックして、データベース接続を検証します。
4. [サブミット] をクリックします。

レポート接続が確立されます。

スナップショット データベース接続の作成

CA Identity Manager で、スナップショットデータのエクスポート先を指定する必要があります。CA Identity Manager からスナップショット データベースへのデータベース接続を作成します。

スナップショットデータベース接続の作成方法

1. ユーザ コンソールで、[タスク] - [レポート] - [スナップショット タスク] - [スナップショット データベース接続の管理] - [スナップショット データベース接続の作成] をクリックします。
2. すべての必要なフィールドに入力して、新規のスナップショットデータベース接続を作成します。
3. [サブミット] をクリックします。

新規のスナップショット データベース接続が作成されます。

スナップショット定義の作成

スナップショットは、指定された時間の CA Identity Manager 内のオブジェクトの状態を反映します。このスナップショットデータを使用して、レポートを構築します。CA Identity Manager オブジェクトデータをキャプチャするには、スナップショットデータベースにデータをエクスポートするスナップショット定義を作成します。スナップショット定義を使用して、ユーザ、エンドポイント、管理ロール、プロビジョニングロール、グループ、および組織をロードするルールを定義します。

次の手順に従ってください:

1. ユーザ コンソールで、[タスク] - [レポート]、[スナップショットタスク]、[スナップショット定義の管理]、[スナップショット定義の作成] に移動します。
2. [スナップショットタイプ] タイプのオブジェクトを作成またはコピーします。
3. [OK] をクリックします。
4. [プロファイル] タブの下に以下のフィールドを入力して、スナップショット定義プロファイルを作成します。

スナップショット定義名

スナップショット定義の一意の名前を指定します。

スナップショット定義の説明

スナップショットを説明するのに必要な追加情報を表示します。

Enabled

このオプションを指定すると、スケジュール設定された時刻に現在のスナップショット定義に基づいて、CA CA Identity Manager によりスナップショットが作成されます。

注: このオプションを選択しないと、スケジュール設定した時刻にスナップショット定義がキャプチャされません。また、スナップショット定義も [スナップショットデータのキャプチャ] 画面にリストされません。

保持されるスナップショット数

スナップショットデータベースに保持される正常なスナップショットの数を指定します。

注: このフィールドの値を指定しない場合、CA Identity Manager により無制限にスナップショットが格納されます。

5. [スナップショットポリシー] タブで、エクスポートするポリシーに関連するオブジェクトを選択します。

6. [ロール設定] タブで、スナップショットがエクスポートする 1 つ以上のロール コンポーネントおよび利用可能な属性を選択します。

注: [スナップショット ポリシー] タブで、[アクセス ロール]、[管理ロール]、または [プロビジョニング ロール] のいずれかのオブジェクトを選択している場合は、[ロール設定] タブで属性を選択します。

7. [ユーザ属性詳細] タブで、スナップショットがエクスポートする 1 つ以上のユーザ属性を選択します。

注: [スナップショット ポリシー] タブで、ユーザ属性を 1 のみ選択した場合、デフォルトでは、すべてのユーザ属性に関連するデータがエクスポートされます。

8. [エンドポイントアカウント属性] タブで、エンドポイント タイプの 1 つ以上のアカウント属性を選択します。

注: 選択されたエンドポイント タイプについては、デフォルトでは、エンドポイント アカウント属性に関連するデータはすべてエクスポートされます。特定の属性に関連するデータをキャプチャするには、適切な属性を選択します。エンドポイント タイプに対するエクスポートが必要な属性の選択の詳細については、「[設定ガイド](#)」で「デフォルトのレポート」セクションを参照してください。

9. (オプション) [孤立アカウントのエクスポート] チェック ボックスをオンにして、プロビジョニング サーバにグローバル ユーザを持たないエンドポイントアカウントを含めます。

注: 非標準、非標準トレンド、および孤立アカウント レポートのレポート データをエクスポートするには、**exceptionAccount** 属性および [孤立アカウントのエクスポート] チェック ボックスを選択します。

10. [サブミット] をクリックします。

CA Identity Manager は、スナップショット定義に含まれるオブジェクトのスナップショットを作成するように設定されています。

スナップショット定義を作成したら、スナップショット データをすぐにキャプチャするか、後でスナップショット データをエクスポートするようにスケジュールできます。詳細については、「[スナップショット データのキャプチャ](#)」を参照してください。

詳細情報:

[\[反復\] タブ](#) (P. 439)

例：ユーザ権限データ用のスナップショット定義の作成

以下の例では、ユーザ権限レポート用のスナップショット定義を作成するプロセスを示します。

- 1. ユーザ コンソールで、[タスク] - [レポート]、[スナップショット タスク]、[スナップショット定義の管理]、[スナップショット定義の作成] に移動します。
- 2. [オブジェクト タイプ:"スナップショット タイプ" の作成] を選択します。
- 3. スナップショット定義の名前と説明、および保持されるスナップショット数を入力します。
- 4. [スナップショット ポリシー定義] タブで [追加] をクリックします。

ドロップダウンからユーザを選択し、[すべて] を選択します。同様に、以下の画面のように、エンドポイント、プロビジョニング ロール、管理ロール、アクセス ロール、組織、およびグループを追加します。

エクスポート 対象オブジェクト	
アクセス ロール	
(すべて)	
管理ロール	
(すべて)	
エンドポイント	
(すべて)	
グループ	
(すべて)	
組織	
(すべて)	
プロビジョニング ロール	
(すべて)	
ユーザ	
(すべて)	

- 5. [ロール設定] タブで、すべてのユーザ ロール チェック ボックスをオンにします。
- 6. [ユーザ属性] タブで、[使用可能な値] リストから必要な属性を選択し、[現在の値] リストにそれらを移動させます。
- 7. [サブミット] をクリックします。

スナップショットの管理

CA Identity Manager では、スナップショット定義を表示、変更、および削除できます。スナップショット定義を表示または変更する際、[プロファイル] および [メンテナンス] タブが表示されます。[メンテナンス] タブが表示されるのは、スナップショットがいったんキャプチャされた後です。[メンテナンス] タブからは、スナップショットを削除することが可能です（スナップショットのステータスが失敗である場合でも削除可能）。

スナップショット定義を表示、変更、および削除するには、[レポート] - [スナップショット タスク] - [スナップショット定義の管理] を選択し、実行するタスクをクリックします。

注: スナップショット定義は、スナップショット データベースにデータをエクスポートするのに使用されている場合は、削除できません。使用されているスナップショット定義を削除すると、スナップショット データベースへのデータのエクスポートは停止されますが、スナップショット定義は引き続き使用できます。

スナップショット データのキャプチャ

ただちにスナップショットデータをキャプチャする場合、あるいはスナップショットデータを後で、または反復スケジュールでエクスポートするようスケジュールする場合、[スナップショット データのキャプチャ] タスクを実行します。このタスクでは、データはただちに（スナップショット定義の定義による）スナップショット データベースにエクスポートされます。

重要: エクスポートするデータが大きい場合、スナップショット データのエクスポートは、処理に時間を要することがあります。大量のデータをエクスポートする際は、スナップショットをスケジュールすることをお勧めします。

スナップショット データをキャプチャする方法

1. ユーザ コンソールで、[タスク] - [レポート] - [スナップショット タスク] - [スナップショット データのキャプチャ] に移動します。
2. [今すぐ実行] を選択してデータのエクスポートをすぐに実行するか、[\[新規ジョブのスケジュール \(P. 439\)\]](#) を選択してデータのエクスポートを後ほど、または反復スケジュールで実行します。
3. [次へ] をクリックします。
4. スナップショット定義を選択します。

5. [サブミット] をクリックします。

スナップショット データがスナップショット データベースにエクスポートされます。

注: [スナップショット データのキャプチャ] タスクの処理に長時間かかっている場合、[システム] タブの [サブミット済みタスクの表示] をクリックして、タスクの進捗を確認できます。

[反復]タブ

このタブを使用して、ジョブをスケジュールします。このタブ内のフィールドは以下のとおりです。

今すぐ実行

ジョブを今すぐ実行します。

新規ジョブのスケジュール

新規ジョブをスケジュールします。

既存ジョブの変更

すでに存在するジョブで変更するジョブを指定します。

注: このフィールドが表示されるのは、このタスクのジョブがすでにスケジュールされている場合のみです。

ジョブ名

作成または変更するジョブの名前を指定します。

タイムゾーン

サーバのタイムゾーンを指定します。

注: 新しいジョブのスケジュール時に、使用しているタイムゾーンがサーバのタイムゾーンと異なる場合には、ドロップダウンボックスが表示されるので、使用中のタイムゾーンまたはサーバのタイムゾーンのいずれを使用するかを選択できます。既存のジョブを修正する場合には、タイムゾーンは変更できません。

日単位のスケジュール

特定の日数だけ毎日ジョブが実行されるよう指定します。

毎(日数)

ジョブを実行する間隔(日数)を定義します。

週単位のスケジュール

1 週間のうち特定の日または期間でのジョブの実行を指定します。

曜日

ジョブを実行する曜日を指定します。

月単位のスケジュール

月単位で実行されるジョブの曜日または日付を指定します。

年単位のスケジュール

年単位で実行されるジョブの曜日または日付を指定します。

詳細なスケジュール

その他のスケジュール情報を指定します。

Cron 式

このフィールドの入力の詳細については、以下の Web サイトを参照してください。

<http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html>

実行時間

ジョブを実行する時刻を、24 時間形式で指定します。例：14:15

スナップショット定義とレポート タスクの関連付け

スナップショット定義をレポート タスクに割り当てると、CA Identity Manager に、どのスナップショット定義がレポートの実行に使用されるかを認識させることができます。また、CA Identity Manager レポートに関する情報は、複数のソースから得ることができます。各レポートは、レポートで表示させたい情報に基づき、特定のデータ ソースに関連付けられている必要があります。

スナップショット定義とスナップショット接続をレポート タスクに関連付ける方法

1. ユーザ コンソールで、[タスク] - [ロールおよびタスク] - [管理タスク] - [管理タスクの変更] に移動します。
2. スナップショット定義と関連付けるレポート タスクを検索します。
3. [タブ] タブをクリックし、[スナップショット定義の関連付け] タブの隣にある [編集] ボタンをクリックします。
4. [追加] をクリックします。

5. レポート タスクと関連付けるスナップショット定義を検索し、[選択] をクリックします。

スナップショット定義とレポート タスクを関連付ける際は、以下の点に注意してください。

- レポートは、1 つ以上のスナップショット定義と関連付けることができます。
- スナップショット定義は、1 つ以上のレポートと関連付けることができます。
- 1 つのレポート タスクに関する複数のスナップショットで同じ繰り返し時間を使用しないでください。

6. [OK] をクリックします。
7. [検索] タブに移動し、[参照] をクリックして検索画面を表示します。
8. 該当するレポート タスクの検索画面を編集して、[レポート用接続オブジェクト] の下の **rptParamConn** を選択します。
9. [OK] をクリックします。
10. [選択] をクリックします。
11. [サブミット] をクリックします。

エンドポイント アカウントとアカウント テンプレートの同期

このタスクは、関連するアカウント テンプレートの変更後にエンドポイント アカウントを同期します。たとえば、**Active Directory** アカウントにグループがありませんが、関連するアカウント テンプレートはグループを含むように定義されています。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. [タスク] - [エンドポイント] - [エンドポイントの管理] - [エンドポイント アカウント同期のチェック] を選択します。
3. エンドポイントを選択します。

そのエンドポイント上のアカウント、関連するアカウント テンプレート、および同期されていない属性が画面に表示されます。

4. [同期] をクリックして、これらのアカウントの属性をアカウント テンプレートで定義されているものと一致させます。

アカウント テンプレートに対して行った変更は、既存のアカウントに次のように影響します。

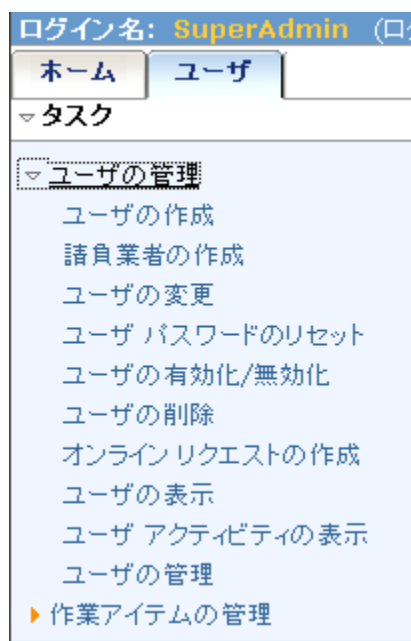
- 機能属性の値を変更すると、対応するアカウント属性が更新され、アカウント テンプレートの属性値と同期されます。弱い同期と強い同期の説明を参照してください。
- 一部のアカウント属性は、コネクタにより、アカウント テンプレートの変更時には更新されないように指定されています。例としては、エンドポイント タイプがアカウント作成時にのみ設定できる属性や、パスワード属性があります。

管理タスクの例

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

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

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



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

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

作成するタスクについて、含めるタブと、タブの順序および内容を決めます。

ユーザの変更: liang

プロフィール アクセス ロール 管理ロール プロビジョニング ロール グループ

● = 必須項目

組織 Dealer

ユーザ ID liang

有効 ☒

●名 liang

●姓 liang

●フル ネーム liang

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

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

新しいカテゴリである「契約者」の下にこのタスクを作成できます。

ログイン名: SuperAdmin (ログアウト)

ホーム ユーザ 請負業者

▼ タスク

▼ 請負業者の管理
請負業者の変更

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

請負業者の変更: 販売管理者

プロフィール	グループ	請負業者ロール
ユーザ ID 販売管理者		
有効 ☒		
● 名 販売		
● 姓 管理者		
電子メール jhansen@wxyz.com		
開始日 2008/05/12		
会社		

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

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。承認が必要となるのは、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な場合があるためです。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。

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. 「タスク」 - 「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. リクエストするレポートを選択します。
「パラメータ」画面が表示されます。

必要なパラメータ情報を入力します。

注: スナップショットレポートを実行中で、このレポート用のスナップショットがない場合は、まずスナップショットをキャプチャしてください。

- レポートには、特定の時点のシステムステータスを表示するレポートがあります。このタイプのレポートをリクエストする場合は、レポートデータを参照する時点を選択します。この時点のことをスナップショットといいます。

注: 選択できるスナップショットの日時は、事前定義されています。通常は、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、スナップショットを設定します。リクエストするレポートのために利用可能なスナップショットがない場合は、システム管理者に問い合わせてください。

- レポートには、特定の期間のアクティビティを表示するレポートがあります。これらのレポートのタイトルは、通常「監査」という語で始まります。このタイプのレポートをリクエストする場合は、レポートデータを参照する期間を指定します。たとえば、過去 30 日間の監査-パスワードのリセットレポートを実行できます。

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。

注: リクエストするレポートが大量のデータを必要とする場合に、このオプションの選択を考慮してください。システムリソースを節約するには、システムアクティビティが少ない時間を選択します。

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。

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 [タスク] - [レポート] - [レポート タスク] へ移動し、[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。

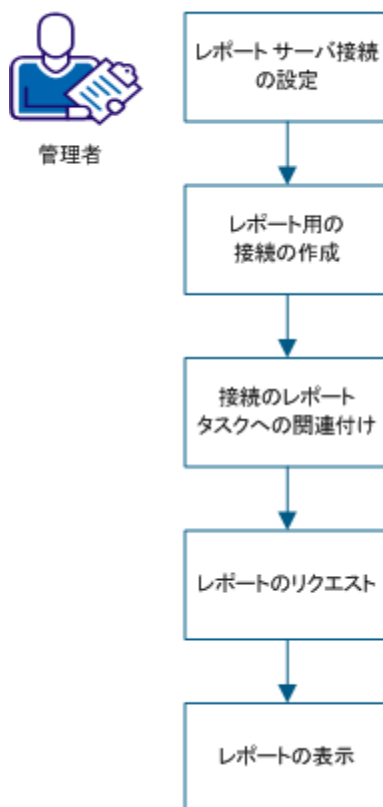
- Crystal Report
- PDF
- Microsoft Excel (97-2003)
- Microsoft Excel (97-2003) データのみ
- Microsoft Excel (97-2003) - 編集可能
- Rich Text Format (RTF)
- カンマ区切り (CSB)
- XML

スナップショット以外のレポートの実行方法

スナップショット以外のレポートには、他のデータ ソース（監査、ワークフロー、またはタスク永続性データベースなど）からのデータが含まれています。CA Identity Manager には、デフォルトの監査レポートが含まれています（これらのレポートには、ユーザ コンソール内で、レポートの名前に「Audit-」のプレフィックスが付けられています）。デフォルトでは、CA Identity Manager には監査レポートのみが含まれますが、任意のデータ ソースからのデータを含む独自のカスタムレポートを作成できます。

このシナリオでは、スーパー管理者によるレポート データベース接続の設定方法およびスナップショット以外のレポートの実行方法について説明します。

スナップショット以外のレポートの実行方法



以下の図は、スナップショット レポートを実行するプロセスを示しています。

スナップショット以外のレポートを実行するには、以下の手順に従います。

1. [レポートサーバ接続を設定します。](#) (P. 449)
2. レポート用の接続を作成します。

3. 接続をレポート タスクに関連付けます。
4. レポートをリクエストします。
5. [レポートを表示します。](#) (P. 453)

レポート サーバ接続の設定

レポート サーバからデータを収集するには、レポート サーバへの接続を設定する必要があります。手順を開始する前に、レポート サーバに関する以下の情報を収集します。

名前	説明
ホスト名	レポート サーバがインストールされているマシンのホスト名。
ポート	レポート サーバがインストールされているマシンのポート名。
レポート フォルダ名	デフォルトの CA Identity Manager レポートの場所。
ユーザ ID	レポート サーバ用に作成されたユーザを指定します。
パスワード	レポート サーバ用に作成されたユーザのパスワードを指定します。
セキュア接続	レポート サーバ用のセキュリティ接続を指定します。 CA Identity Manager とレポート サーバの間の Secure Sockets Layer (SSL) 接続を有効にするには、このチェック ボックスを選択します。 注: [セキュア接続] チェック ボックスを選択する前に、BOServer から証明書をインストール済みであることを確認してください。 SSL の設定方法の詳細については、「インストールガイド」の「レポート サーバのインストール」の章を参照してください。
Web サーバ	Web サーバを指定します。 Tomcat の場合は IIS 以外に設定してください。

注: レポートに関係するすべてのシステムのタイムゾーンと時刻を同じ設定にすることをお勧めします。

次の手順に従ってください:

1. ユーザ コンソールで、[システム] - [レポート] - [レポート サーバ接続] をクリックします。
2. レポート サーバの設定を入力します。

3. [テスト接続] をクリックして、データベース接続を検証します。
4. [サブミット] をクリックします。

レポート接続が確立されます。

レポート用の接続の作成

CA Identity Manager レポートの情報は、複数のソースから収集できます。 レポート用に追加のデータ ソースへ接続する際にその詳細を指定するには、CA Identity Manager 内に JDBC 接続を作成します。

次の手順に従ってください:

1. ユーザ コンソールで [タスク] - [システム] - [JDBC 接続管理] - [JDBC 接続の作成] に移動します。
 2. 新しい接続オブジェクトを作成するか、特定の JNDI データ ソースに基づいて接続オブジェクトを選択します。
 3. 必要なすべてのフィールドに入力して、[送信] をクリックします。
- 新しい JDBC 接続が作成されます。

重要: レポートの作成には CA Identity Manager オブジェクトストア データベースを使用しないことをお勧めします。

接続のレポート タスクへの関連付け

CA Identity Manager レポートに関する情報は、複数のソースから取得されます。各レポートは、レポートで表示させたい情報に基づき、特定のデータ ソースに関連付けられる必要があります。

接続をレポート タスクに関連付ける方法

1. ユーザ コンソールで、[タスク] - [ロールおよびタスク] - [管理タスク] - [管理タスクの変更] に移動します。
2. 関連付け先のレポート タスクを検索します。
3. [検索] タブに移動し、[参照] をクリックして検索画面を表示します。
4. 検索画面をレポート タスク用に編集し、[レポート用接続オブジェクト] の下にある接続を選択します。
5. [OK] をクリックします。

6. [選択] をクリックします。
7. [サブミット] をクリックします。

レポートのリクエスト

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。承認が必要となるのは、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な場合があるためです。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。

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. [タスク] - [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. リクエストするレポートを選択します。

[パラメータ] 画面が表示されます。

必要なパラメータ情報を入力します。

注: スナップショットレポートを実行中で、このレポート用のスナップショットがない場合は、まずスナップショットをキャプチャしてください。

- レポートには、特定の時点のシステムステータスを表示するレポートがあります。このタイプのレポートをリクエストする場合は、レポートデータを参照する時点を選択します。この時点のことをスナップショットといいます。

注: 選択できるスナップショットの日時は、事前定義されています。通常は、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、スナップショットを設定します。リクエストするレポートのために利用可能なスナップショットがない場合は、システム管理者に問い合わせてください。

- レポートには、特定の期間のアクティビティを表示するレポートがあります。これらのレポートのタイトルは、通常「監査」という語で始まります。このタイプのレポートをリクエストする場合は、レポートデータを参照する期間を指定します。たとえば、過去 30 日間の監査-パスワードのリセットレポートを実行できます。

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。

注: リクエストするレポートが大量のデータを必要とする場合に、このオプションの選択を考慮してください。システム リソースを節約するには、システム アクティビティが少ない時間を選択します。

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。

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

レポート オプションの設定

ユーザが特定のレポートについて生成できるレポート インスタンスの数を設定します。

レポート オプションを変更する方法

1. [タスク] - [レポート] - [レポート タスク] - [レポート オプションの設定] を選択します。

CA Identity Manager から IAM レポート サーバに接続され、すべてのレポートのリストが取得されます。

2. レポートを選択し、[変更] をクリックします。

レポートの属性ペインが表示されます。

3. 以下のフィールドを編集します。

名前

選択したレポートの表示名を指定します。

インスタンス数

指定したレポートに対して生成可能なインスタンスの数を指定します。

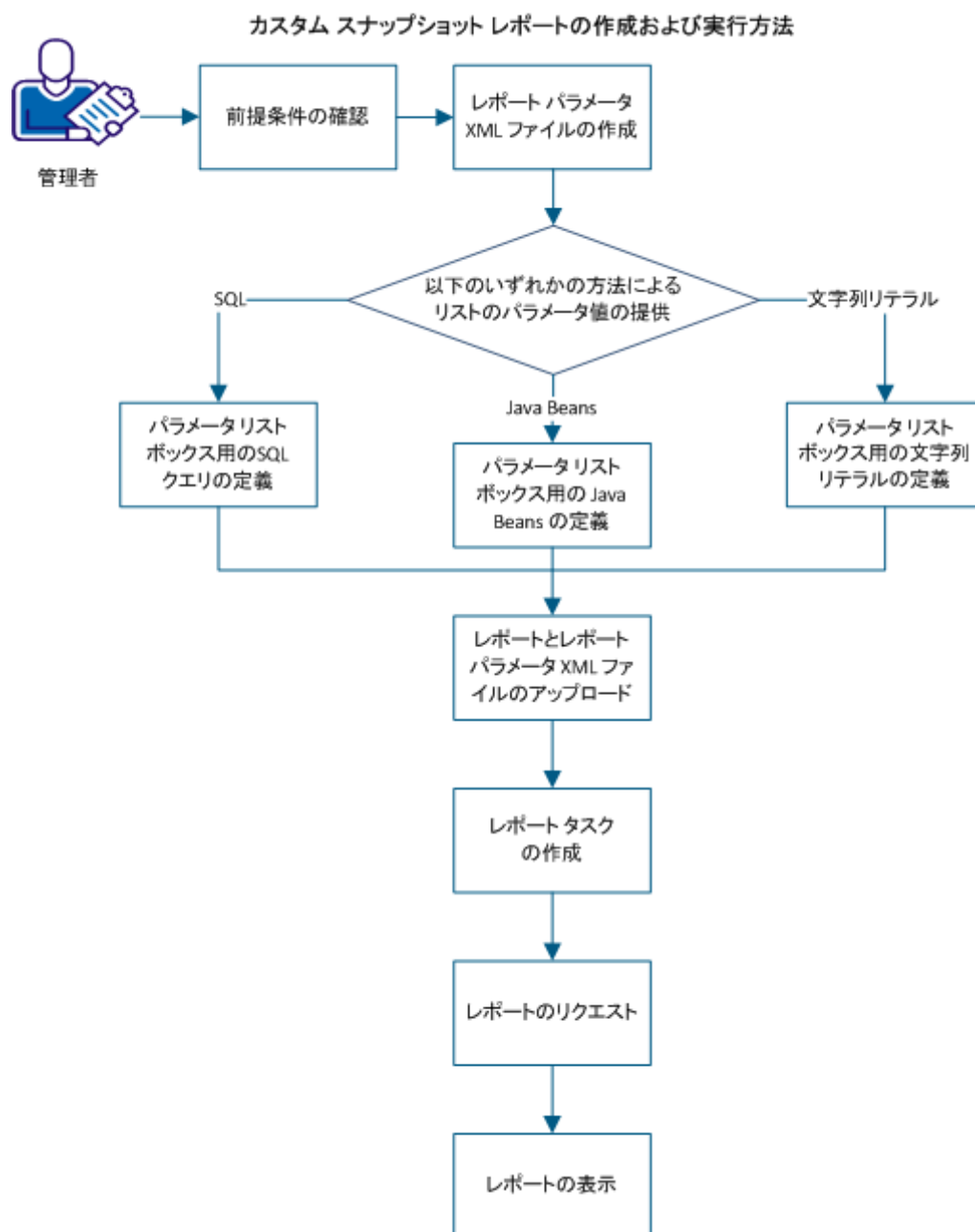
4. [OK] をクリックします。

レポート属性が変更されます。

カスタム スナップショット レポートの作成および実行方法

CA Identity Manager では、ビジネスのニーズに適したレポートを作成およびカスタマイズできます。CA Identity Manager は、レポート属性に関連するすべてのパラメータを含むレポート パラメータ XML ファイルを提供します。ビジネス ニーズに従って、スナップショット データ ソースからのレポート データに入力するために、必要な属性を選択できます。

以下の図は、カスタム スナップショット レポートを作成して実行するプロセスを示しています。



システム管理者として、以下の手順を実行します。

1. [前提条件の確認](#) (P. 457)
2. [レポートパラメータ XML ファイルの作成](#) (P. 457)
3. 以下のいずれかの方法によるリストのパラメータ値の提供
 - [パラメータ リスト ボックス用の SQL クエリの定義](#) (P. 461)

- [パラメータ リスト ボックス用の Java Beans の定義](#) (P. 462)
- [パラメータ リスト ボックス用の文字列リテラルの定義](#) (P. 462)
- 4. [レポートとレポート パラメータ XML ファイルのアップロード](#) (P. 462)
- 5. レポート タスクの作成
- 6. レポートのリクエスト
- 7. [レポートの表示](#) (P. 453)

Crystal Reports でのレポートの作成

CA Identity Manager でカスタム レポートを使用するには、まず Crystal Reports Developer でレポート (RPT ファイル) を作成します。Crystal Reports でレポートを作成する方法の詳細については、Crystal Reports のマニュアルを参照してください。

注: カスタム レポートを作成するために CA Identity Manager スキーマを参照するには、CA Identity Manager データベース スキーマを以下の場所に配置します。

C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\db\objectstore

レポート パラメータ XML ファイルの作成

パラメータは、レポートのフィルタに使用されるレポート フィールドの 1 つです。パラメータを使用してデータをフィルタすることで、レポートを生成できます。レポートの検索画面をカスタマイズできるようにするには、各レポート (RPT ファイル) をレポート パラメータ XML ファイルに関連付けます。CA Identity Manager では、ユーザがレポートの生成時に必要なデータを入力または選択できるように、レポート タスクを作成し、検索画面を作成できます。

注: レポートがオブジェクトの属性にクエリを実行する場合にのみ、レポート パラメータ XML ファイルが必要です。

レポート パラメータ XML ファイルはレポート (RPT ファイル) と同じ名前にし、.xml 拡張子を持つ必要があります。たとえば、test1.rpt というレポートをレポート サーバにアップロードする場合、XML ファイルは test1.xml という名前になります。

レポート パラメータ XML ファイルには以下のエレメントが含まれます。

<product>

パラメータが使用される製品を識別します。同じパラメータ XML ファイルを使用して、複数の製品に異なるパラメータを作成できます。

<screen>

画面に表示されるパラメータを定義します。パラメータを特定の画面にバインドするには、画面エレメントを使用できます。画面 ID は一意の英数字で、画面と画面のパラメータを識別するために使用されます。

<parameters>

画面のパラメータの集合を指定します。

<param>

指定されたデータをレポートに転送するパラメータ エレメントを定義します。<param> エレメントでは、以下の属性が使用されます。

id

レポートの、どのパラメータに関連付けるかを定義します。

注: ID は、Crystal Report のパラメータと同じ名前を持つ必要があります。

name

このフィールドは CA Identity Manager では現在使用されていません。この属性は、id と同じ値に設定します。

displaytext

パラメータの画面に表示する、分かりやすいテキストを指定します。

type

パラメータのタイプを定義します。この属性に基づいて画面が変わります。サポートされるパラメータタイプは、以下のとおりです。

– テキスト ボックス

例 : `<param id="param1" displaytext="First Name" name="param1" type="string"/>`

– 日時

例 : `<param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>`

`<param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>`

`<param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>`

– ドロップダウン リスト

例 : `<param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>`

– リスト ボックス

例 : `<param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>`

– ラジオ ボックス

例 : `<param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>`

`<param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>`

`<param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>`

– チェック ボックス

例 : `<param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>`

row

リスト ボックスに表示する行の数を定義します。

デフォルト : 5

default

指定されたパラメータの画面に表示されるデフォルト値を定義します。この属性は、文字列、リスト ボックス、およびドロップダウン リストの各タイプで使用できます。

パラメータ リスト ボックス用の SQL クエリの定義

SQL クエリは、レポート パラメータ XML ファイルのリスト ボックスまたはドロップダウン ボックスの一部として定義できます。パラメータをレポートに関連付け、レポート タスクを作成すると、パラメータが、リスト ボックスまたはドロップダウン ボックスによってユーザに表示されます。ドロップダウン ボックスまたはリスト ボックス パラメータで SQL を使用するには、`sql` 属性に有効な SQL 文を用意します。

例:

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'S%"/>
```

上記の例では、「S」で始まる名を持つユーザの姓はすべて、レポートに表示されます。

ただし、「S」で始まる名の条件は、静的なものです。このクエリは、以前の画面（同じレポート パラメータ グループで使用される）のいずれかに入力されるパラメータ値に基づく値をロードするユーザにとって、十分な柔軟性を持つものではありません。別の画面に入力された以前の値を使用するには、「`##<parameter id>##`」を使用して SQL 文を拡張します。

たとえば、`id=User`、タイプが `String` のパラメータの場合、以下のようになります。

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

SQL のそのパラメータに入力値を使用する場合、SQL 文は以下のようになります。

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'##User##' />
```

CA Identity Manager は、`##User##` を、`id=User` のパラメータに入力された値と置き換えます。

注: 置換されるパラメータ値は、SQL パラメータと同じ画面には入力できません。たとえば、「`lstlastname2`」が画面 3 にある場合、`User` パラメータは以前の画面にいずれかに入力する必要があります。

パラメータ リスト ボックス用の Java Beans の定義

SQL の使用が望ましくない場合は、Java Beans を使用して値を計算し、<キー, 値> ペアのリストを CA Identity Manager に提供できます。Java Beans は、CA Identity Manager の classpath にあります。

例:

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2" type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

上記の例では、`TestDataCollector` は独自の方法で値を取得し、ドロップダウン リストのデータをレポートに送信します。<key, value> ペアは %1F で分割されます。

Java Bean が `iam_im.ear¥custom` ディレクトリにあることを確認します。

注: Java Beans の実装の詳細については、[Business Objects のマニュアル](#)を参照してください。

パラメータ リスト ボックス用の文字列リテラルの定義

パラメータ値をリストまたはドロップダウン ボックスに表す最も単純な方法は、文字列リテラルを使用する方法です。キー値は %1F で区切られ、<key, value> ペアはそれぞれ %1E で分割されます。

例:

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

レポートとレポート パラメータ XML ファイルのアップロード

レポート (RPT) および対応するレポート パラメータ XML ファイルを作成したら、レポート サーバ (Business Objects) に両方のファイルをアップロードします。

次の手順に従ってください:

1. Business Objects の中央管理コンソールにログインします。
2. [Folders] をクリックします。
3. [IM Reports] フォルダを選択します。
4. オブジェクト パッケージを作成します。
5. 新しいオブジェクト パッケージで、Crystal Report を参照して追加します。

6. 作成した新しいレポート（RPT）を参照します。

注: レポートの保存先として [IM Reports] フォルダが選択されていることを確認します。

7. [OK] をクリックします。

Crystal Report ファイルが追加されます。

8. 新しいオブジェクトパッケージで、新しいローカル ドキュメントを追加し、新しいレポート パラメータ XML ファイルを参照します。

9. ファイルタイプとして [テキスト] を選択します。

10. [OK] をクリックします。

レポートとレポート パラメータ XML ファイルがアップロードされました。確認のために [IM Reports] フォルダに移動して、新しいファイルが両方とも使用可能になっていることを確認します。

レポート タスクの作成

レポート タスクは、ユーザ コンソールで生成されるレポートにテンプレートを作成、管理、表示、削除するために使用されます。

次の手順に従ってください:

1. ユーザ コンソールで、[タスク] - [ロールおよびタスク] - [管理タスク] - [管理タスクの変更] に移動します。
2. [管理タスクの作成] を選択し、[OK] をクリックします。
3. [プロファイル] タブで、以下のフィールドに入力します。

名前

レポートの名前を定義します。各レポート タスクには、一意の名前を使用する必要があります。

タグ

タスクの一意な識別子を定義します。これは URL、Web サービス、またはプロパティ ファイルで使用されます。識別子は、アルファベット文字、数字、または下線文字で構成し、先頭をアルファベット文字または下線文字にする必要があります。

[Category]

現在のタスクが所属するカテゴリを指定します。

注: [レポート] カテゴリを選択します。

カテゴリ 2

現在のタスクが所属するサブカテゴリを指定します。フィールドに文字列を入力します。

プライマリ オブジェクト

タスクを操作するオブジェクトを指定します。

注: プライマリ オブジェクトとして [レポート インスタンス] を選択します。

アクション

プライマリ オブジェクトで操作するアクションを指定します。

注: アクションとして [作成] を選択します。

4. レポート タスク用の新しい検索画面を作成するには、以下の手順に従います。
 - a. [検索] タブで、[参照] をクリックして検索画面を表示します。
利用可能な検索画面のリストが表示されます。

- b. [新規] をクリックします。
[画面の作成] ペインが表示されます。
- c. リストから [レポート テンプレート 選択画面] を選択し、[OK] をクリックします。

CA Identity Manager がレポート サーバに接続され、すべてのレポートが表示されます。

- d. 以下のフィールドに値を入力します。

名前

レポートの名前を定義します。各レポート タスクには、一意の名前を使用する必要があります。

タグ

タスク内で一意の識別子です。タグには、ASCII 文字 (a ~ z、A ~ Z)、数字 (0 ~ 9)、またはアンダースコアを含めることが可能で、1 字目には文字かアンダースコアを使用します。

タイトル

新しい検索画面のタイトルを定義します。一意のタイトルを使用する必要があります。

レポート テンプレート

検索画面に関連付けるレポートを識別します。

注: レポート サーバに追加したレポートのうちの 1 つを選択します。

レポート用接続オブジェクト

レポートで使用するデータ ソースの接続の詳細を定義します。

- 5. [OK] をクリックします。
レポート用の新しい検索画面が作成されました。
- 6. レポート タスクの [タブ] タブの作成で、以下の手順を実行します。
 - a. [タブ] をクリックします。
ユーザに対して表示されるタブが表示されます。
 - b. [標準タブ コントローラ] を選択します。
 - c. レポートでスナップショット定義を使用する場合、以下の手順を実行します。
 - a. [このタスクで表示する必要があるのはどのタブですか?] から [スナップショット定義の関連付け] を選択します。

タブのリストに [スナップショット定義の関連付け] タブが追加されます。

- b.  をクリックして、[スナップショット定義の関連付け] タブを編集します。
- c. [追加] をクリックして、レポート タスクをスナップショット定義に関連付けます。

利用可能なスナップショット定義が表示されます。

- d. [スナップショット定義] を選択して、[OK] をクリックします。

レポート タスクがスナップショット定義と関連付けられます。

- d. [サブミット] をクリックします。

レポート タスクが作成されます。

- e. 管理ロールに新しいレポート タスクを割り当てます。

CA Identity Manager の管理ロール ユーザは、新しいレポート タスクを使用できます。

管理ロール ユーザがレポート タスクを使用するための準備が完了しました。

注: レポート (RPT ファイル) は、1 つのレポート タスクにのみ関連付けることができます。

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。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。承認が必要となるのは、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 リソースが必要な場合があるためです。 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。

次の手順に従ってください:

1. レポート タスクに対するアクセス権を持つユーザとしてユーザ コンソールにログインします。
2. ナビゲーションメニューから、[タスク] - [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. リクエストするレポートを選択します。
[パラメータ] 画面が表示されます。
4. 必要なパラメータ情報を入力します。

注: スナップショット レポートを実行中で、このレポート用のスナップショットがない場合は、まずスナップショットをキャプチャしてください。

- レポートには、特定の時点のシステム ステータスを表示するレポートがあります。このタイプのレポートをリクエストする場合は、レポートデータを参照する時点を選択します。この時点のことをスナップショットといいます。

注: 選択できるスナップショットの日時は、事前定義されています。通常は、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、スナップショットを設定します。リクエストするレポートのために利用可能なスナップショットがない場合は、システム管理者に問い合わせてください。

- レポートには、特定の期間のアクティビティを表示するレポートがあります。これらのレポートのタイトルは、通常「監査」という語で始まります。このタイプのレポートをリクエストする場合は、レポートデータを参照する期間を指定します。たとえば、過去 30 日間の監査-パスワードのリセットレポートを実行できます。

5. [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。

注: リクエストするレポートが大量のデータを必要とする場合に、このオプションの選択を考慮してください。システム リソースを節約するには、システム アクティビティが少ない時間を選択します。

6. [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。

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 [タスク] - [レポート] - [レポート タスク] へ移動し、[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。

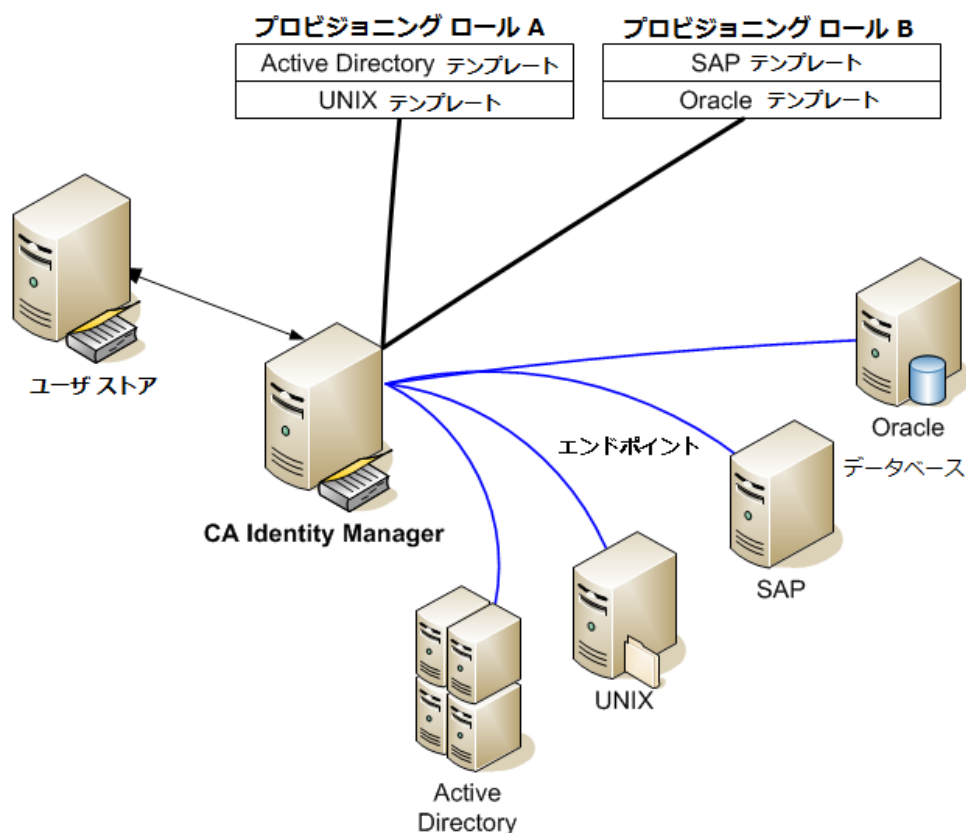
3. 表示するレポートを選択します。
4. (オプション) [このレポートをエクスポート] (左上隅) をクリックし、レポートを以下の形式でエクスポートします。

- 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)
- 区切り値 (CSV)
- XML

ユーザ、アカウント、およびロールの同期

複数のエンドポイントおよびアカウントを単一のユーザ管理システムに統合すると、同期が失われる場合があります。ユーザに割り当てられたプロビジョニングロールまたはアカウントテンプレートは、そのユーザの実際のアカウントと異なることがあります。

たとえば、2つのプロビジョニングロール（Active Directory と UNIX のアカウントテンプレートを持つロールと、SAP および Oracle のテンプレートを持つロール）がある状況を考えてください。ユーザ `john_smith` にはプロビジョニングロール A（Active Directory と UNIX のアカウントテンプレートが含まれる）がありますが、このユーザは Active Directory アカウントしか持っていません。これは、このロールがユーザに割り当てられた後、ロールに UNIX アカウントテンプレートが追加されたためである可能性があります。そこで管理者は、ユーザを現在のロール定義と同期します。



ユーザがプロビジョニング ロールまたはアカウント テンプレートとの同期を失う他の理由には、以下のようなものがあります。

- ネットワークでハードウェアまたはソフトウェアの問題があるために、以前に必要なアカウントを作成しようとして失敗し、存在しないアカウントが生じています。
- プロビジョニング ロールおよびアカウント テンプレートが変更されたため、不要なアカウントまたは存在しないアカウントがあります。
- アカウント テンプレートが作成された後にアカウントが割り当てられたため、アカウントは存在しますがアカウント テンプレートと同期していません。
- アカウントを後で作成するよう指定されているため、新しいアカウントの作成が遅れています。
- 新しいエンドポイントが取得されました。検索および関連付けの際、プロビジョニング サーバは、プロビジョニング ロールを自動的にユーザに割り当てませんでした。ユーザはロールを更新し、このエンドポイント上のアカウントを必要とするユーザを示すようにします。ユーザに関連付けられているアカウントは、ユーザの同期時に、不要なアカウントとしてリストされます。
- 既存のアカウントをユーザにコピーする際、そのアカウントがユーザに割り当てられました。
- ユーザをロールに割り当てる以外の方法で、ユーザに対してアカウントが作成されました。たとえば、そのユーザのプロビジョニング ロールにないアカウント テンプレートにユーザをコピーしました。そのアカウントは、不要なアカウント、または不要なアカウント テンプレートを持つアカウントとしてリスト表示されます。ユーザをエンドポイントにコピーし、デフォルトアカウント テンプレートを使用してアカウントを作成すると、そのアカウントは不要なアカウントになることがあります。

以下のセクションでは、3 つのタイプの同期を実行する方法について説明します。

1. [ユーザとロールの同期](#) (P. 185)。
2. [ユーザとアカウント テンプレートの同期](#) (P. 186)。
3. [エンドポイント アカウントとアカウント テンプレートの同期](#) (P. 187)。

ユーザとロールの同期

このタスクは、ユーザに割り当てられているプロビジョニングロールに対してアカウントが準拠するように、アカウントを作成、更新、または削除します。たとえば、管理者はエンドポイント上でネイティブツールを使用してアカウントを追加または削除しますが、ユーザはそのエンドポイントを再検索してプロビジョニングディレクトリを更新していません。そのため、ユーザには不要または存在しないアカウントがあります。このタスクにより、各アカウントが正しいアカウントテンプレートに属していることも保証されます。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. [ユーザ] - [同期] - [ロール同期のチェック] を選択します。
3. ユーザを選択します。

有効なアカウント、不要なアカウント、および存在しないアカウントが画面に表示されます。

4. アカウントをこのロールのテンプレートと一致させるために、[同期] をクリックします。
 - a. チェック ボックスを選択して、エンドポイント上でアカウントを作成することができます。ユーザの複数のアカウントテンプレートが同じアカウントを規定している場合、関連するすべてのアカウントテンプレートをマージすることによって、アカウントが作成されます。

このアカウントは、これらのアカウントテンプレートに割り当てられますが、これらのテンプレートは、現在のところアカウントと同期していません。

- b. チェック ボックスを選択して、不要なアカウントを削除することができます。しかし、これらのアカウントを持つ正当な理由がある場合があります。その場合は、このオプションをオフにしておきます。

アカウント削除機能が無効になっているエンドポイントもあり、その場合はアカウントは削除されません。

ユーザとアカウント テンプレートの同期

このタスクは、エンドポイント アカウントの属性を、ユーザの関連するアカウント テンプレートと同期します。ただし、フル同期は以下の要因に依存します。

- アカウントのフル同期は 2 つの状況で発生します。アカウント テンプレートが[強い同期](#) (P. 189)を使用するか、2 つ以上のアカウント テンプレートがアカウントに追加されています。
- アカウント テンプレートが[弱い同期](#) (P. 188)を使用する場合、このタスクはこのテンプレートのみを含むアカウント同期を開始します。更新の前に、アカウントがすでに他のアカウント テンプレートとのアカウント同期とずれてしまっていた場合は、それ以降も、アカウント同期とずれることがあります。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. [ユーザ] - [同期] - [アカウント テンプレート同期のチェック] を選択します。
3. ユーザを選択します。

有効なアカウント、不要なアカウント、および存在しないアカウントが画面に表示されます。

4. [同期] をクリックして、アカウントをテンプレートと一致させます。
 - a. チェック ボックスを選択して、エンドポイント上でアカウントを作成することができます。ユーザの複数のアカウント テンプレートが同じアカウントを規定している場合、関連するアカウント テンプレートをマージすることによって、アカウントが作成されます。

このアカウントは、それと同期していないアカウント テンプレートに割り当てられています。新しく作成されたアカウントでは、アカウントの同期は必要ありません。

- b. チェック ボックスを選択して、不要なアカウントを削除することができます。しかし、これらのアカウントを持つ正当な理由がある場合があります。その場合は、このオプションをオフにしておきます。

アカウント削除機能が無効になっているエンドポイントもあり、その場合はアカウントは削除されません。

エンドポイント アカウントとアカウント テンプレートの同期

このタスクは、関連するアカウント テンプレートの変更後にエンドポイント アカウントを同期します。たとえば、**Active Directory** アカウントにグループがありませんが、関連するアカウント テンプレートはグループを含むように定義されています。

次の手順に従ってください:

1. ユーザ コンソールにログインします。
2. [エンドポイント] - [エンドポイントの管理] - [エンドポイント アカウント同期のチェック] を選択します。
3. エンドポイントを選択します。

そのエンドポイント上のアカウント、関連するアカウント テンプレート、および同期されていない属性が画面に表示されます。

4. [同期] をクリックして、これらのアカウントの属性をアカウント テンプレートで定義されているものと一致させます。

アカウント テンプレートに対して行った変更は、既存のアカウントに次のように影響します。

- 機能属性の値を変更すると、対応するアカウント属性が更新され、アカウント テンプレートの属性値と同期されます。弱い同期と強い同期の説明を参照してください。
- 一部のアカウント属性は、コネクタにより、アカウント テンプレートの変更時には更新されないように指定されています。例としては、エンドポイント タイプがアカウント作成時にのみ設定できる属性や、パスワード属性があります。

更新対象となる属性

アカウント テンプレートで機能属性を変更すると、アカウント上の対応する属性が変更されます。この変更はアカウントの属性に影響を及ぼします。影響は以下の要因に基づきます。

- アカウント テンプレートが弱い同期で定義されているか強い同期で定義されているか
- アカウントが複数のアカウント テンプレートに属しているかどうか

弱い同期

弱い同期では、ユーザのアカウントに対する最小の機能属性だけをユーザが持つことが保証されます。大部分の種類のエンドポイントでは、弱い同期がデフォルトです。弱い同期を使用するテンプレートを更新する場合、CA Identity Manager は以下のように機能属性を更新します。

- アカウント テンプレートで数値フィールドが更新されていて、新しい数値がアカウントの数値より大きい場合、新しい数値に合うようにアカウントの値が変更されます。
- 選択されていなかったチェックボックスをアカウント テンプレートで選択すると、そのチェックボックスが選択されていないすべてのアカウントでチェックボックスが更新されます。
- アカウント テンプレートで一覧を変更すると、アカウントの値の一覧になかった新しい一覧の値が収まるようにすべてのアカウントが更新されます。

1つのアカウントが他の複数のアカウント テンプレートにも属している場合、強い同期であれ弱い同期であれ、変更のあるテンプレートだけが参照されます。この方がすべてのアカウント テンプレートを検証するより効率的です。弱い同期ではアカウントに機能が追加されるだけなので、これら他のアカウント テンプレートを参照する必要は通常はありません。

注: 弱い同期アカウント テンプレートから伝達された変更が機能の削除や低減を行うものであった場合、一部のアカウントが非同期のままになることがあります。弱い同期では機能の削除や低減は決して行われなことに注意してください。アカウントの他のテンプレートが参照されないので、弱い同期で十分かどうかがこの伝達では考慮されません。

この状況では、アカウントをそのアカウント テンプレートと同期するには [ユーザとアカウント テンプレートの同期] を使用します。

強い同期

強い同期により、アカウント テンプレートで指定されているものと同じアカウント属性をアカウントが持っていることが保証されます。

たとえば、既存の **UNIX** アカウント テンプレートにグループを追加するとします。最初に、アカウント テンプレートでは **Staff** グループのアカウント メンバを作成しました。次に、**Staff** グループと **System** グループの両方のアカウント メンバを作成します。このアカウント テンプレートに関連付けられているすべてのアカウントは、それぞれのアカウントが **Staff** グループおよび **System** グループのメンバである場合（および他のいずれのグループでもない場合）、同期されているとみなされます。**Staff** グループに含まれていないすべてのアカウントは、両方のグループに追加されます。

その他にも、以下の状況を考慮する必要があります。

- アカウント テンプレートで強い同期を使用している場合、**Staff** および **System** 以外のグループに属しているアカウントは、これらの追加グループから除外されます。
- アカウント テンプレートで弱い同期を使用している場合、アカウントは **Staff** グループおよび **System** グループに追加されます。他のグループが定義されているアカウントは、そのグループのメンバのままになります。

注: アカウントとアカウント テンプレートを定期的に同期することにより、アカウントおよびそのアカウント テンプレートの同期が確実に保たれます。

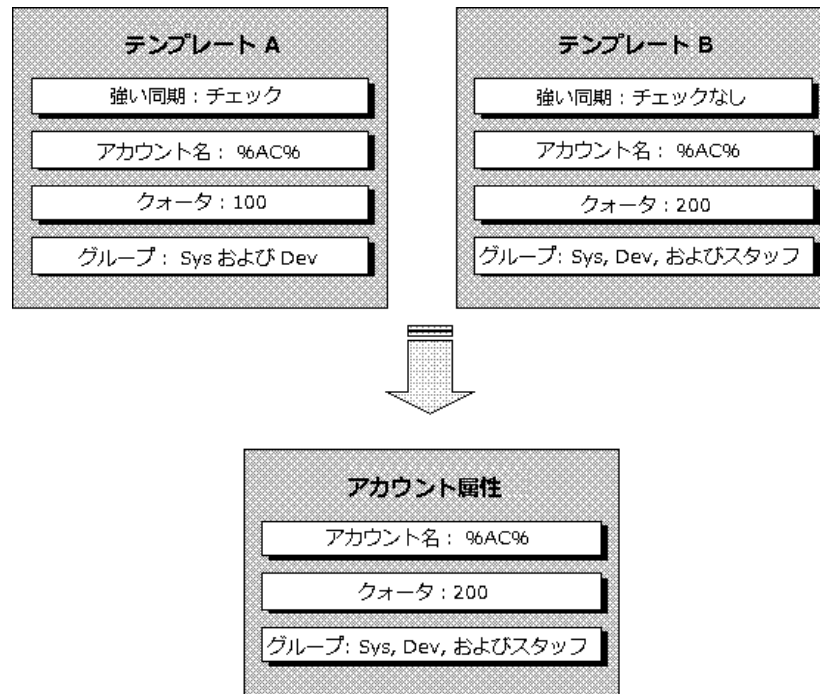
複数のテンプレートを持つアカウント

同期は、アカウントが複数のアカウント テンプレートに属しているかどうかによっても異なります。 アカウントがアカウント テンプレートを **1** つのみ持ち、そのテンプレートの同期が強い場合、各属性は、アカウント テンプレート属性値の評価対象に正確に一致するように更新されます。その結果、属性は最初の属性と同じ値になります。

ユーザが複数のプロビジョニング ロールに属し、それぞれのロールが同じ管理対象エンドポイントに対して一定のレベルのアクセス権を持つ場合、アカウントは複数のアカウント テンプレートに属する場合があります。この状態になると、**CA Identity Manager** はこれらのアカウント テンプレートを **1** つの有効なアカウント テンプレートにまとめ、個々のアカウント テンプレートの機能を合わせた上位集合として規定します。個々のアカウント テンプレートすべての同期が弱い場合、アカウント テンプレート単体は弱い同期となりますが、アカウント テンプレートのうち強い同期を持つものが **1** つでもあると、強い同期となります。

注: アカウント テンプレートが **1** つのアカウントのみを制御している場合、弱い同期のみまたは強い同期のみを使用することが多いです。これは、ユーザに必要なアクセス権を企業のロールが完全に定義しているかどうかによって決まります。ユーザのロールが明確でなく、ユーザのアカウントに柔軟に対応する必要がある場合、弱い同期を使用します。ユーザに必要なアクセス権を明確に指定するロールを定義する場合、強い同期を使用します。

以下の例は、複数のアカウントテンプレートが1つの有効なアカウントテンプレートにまとめられる方法を示します。この例では、1つのアカウントテンプレートが弱い同期としてマークされ、もう一方のテンプレートが強い同期としてマークされています。したがって、2つのアカウントテンプレートをまとめて作成された有効なアカウントテンプレートは、強い同期を持つアカウントテンプレートになります。整数を持つ **Quota** 属性は、2つのアカウントテンプレートから大きい方の値をとり、複数值を持つ **Groups** 属性は、2つのポリシーの値を合わせたものになります。



新しいアカウントだけの属性

アカウントテンプレートでは、一部の属性はアカウントの作成時のみに適用されます。たとえば、**Password** 属性は、新しいアカウントのパスワードを定義するルール表現です。このルール表現は、アカウントのパスワードを変更することはありません。パスワードルール表現への変更は、ルール表現が設定された後に作成されたアカウントだけに影響します。

同様に、読み取り専用アカウント属性のテンプレートルール表現は、ルール表現が設定された後に作成されたアカウントだけに影響します。変更は、既存のアカウントには何の影響ももたらしません。

トラブルシューティング

以下のセクションでは、レポートに関連するトラブルシューティングのトピックを詳しく説明します。

レポートを表示すると Infoview のログイン ページにリダイレクトされる

CA Identity Manager でレポートを表示すると、Business Objects Infoview のログイン ページにリダイレクトされる場合があります。

リダイレクトされた場合のレポートの表示

1. CA レポート サーバ (Business Objects) の完全修飾ドメイン名を使用していることを確認します。
2. Infoview の Web ログイン ページで右クリックして、[View Source] を選択します。
3. レポートの URL を見つけます。
4. その URL をブラウザの新規ウィンドウへコピーして貼り付けます。
5. レポートが表示されない場合は、HTTP トレース ツールを使用して、詳細情報を入力します。
6. レポートを表示する場合は、以下の操作を実行して、ブラウザの設定を修正します。
 - サードパーティの Cookie を受け入れます。
 - セッション Cookie を許可します。
 - 高度なセキュリティ設定を削除します。

20,000 を超えるレコードのユーザ アカウントの生成

20,000 を超えるレコードが存在する場合は、ユーザ アカウント レポートを生成するために、さらにいくつかの手順が必要です。

20,000 を超えるレコードのユーザ アカウントレポートを生成する方法

1. Business Objects Central Management コンソールを開きます。
2. [Servers] をクリックし、[servername.pageserver] を選択します。
3. レポートのプレビューまたはリフレッシュ時に、エントリ [Database Records To Read] に対して [Unlimited records] を選択します。
4. Crystal Reports designer を使用して、ユーザ アカウント レポートを開きます。

5. [Database]、[Datasource Location] を使用して、データベースの場所をスナップショット データベースに設定します。
6. 変更を保存します。
7. [Database]、[Datasource Expert] を使用して、右側のウィンドウで [コマンド] を右クリックします。
左側に SQL 構文、およびパラメータ リストが表示されます。
8. レポート テンプレートのパラメータ フィールドに表示されているパラメータ名を入力します。
9. 左側のクエリを変更し、クエリにパラメータを追加します。
たとえば、**reportid** パラメータがあるとすれば、クエリは以下のようになります。

```
Select * from endPointAttributes, endpointview, imreport6
```


ここで、`endPointAttributes.imr_endpointid = endpointview.imr_endpointid` および
`endPointAttributes.imr_reportid = endpointview.imr_reportid`
`endpointview.imr_reportid = imreport6.imr_reportid and imreport6.imr_reportid = {?reportid}` です。
10. レポートを保存します。

第 15 章: アイデンティティ ポリシー

このセクションには、以下のトピックが含まれています。

[アイデンティティ ポリシー \(P. 481\)](#)

[禁止アイデンティティ ポリシー \(P. 504\)](#)

[アイデンティティ ポリシーおよび禁止アイデンティティ ポリシーの統合 \(P. 515\)](#)

アイデンティティ ポリシー

アイデンティティ ポリシーとは、ユーザが特定の条件やルールを満たした場合に発生する一連の業務変更です。アイデンティティ ポリシー セットを使用して以下の処理を実行できます。

- ロールやグループ メンバシップの割り当て、リソースの割り当て、ユーザ プロファイル属性の変更といった、特定のアイデンティティ管理タスクを自動化する。
- 職務分掌を適用する。たとえば、アイデンティティ ポリシー セットを作成し、**Check Signer** ロールのメンバが **Check Approver** ロールを所有することを禁止して社内の人間が \$10,000 を超える小切手を書くことを制限することができます。
- コンプライアンスを適用する。たとえば、特定の役職に就いており給与が \$100,000 を超えるユーザを監査できます。

コンプライアンスを適用するアイデンティティ ポリシーは、**コンプライアンス ポリシー**と呼ばれます。

アイデンティティ ポリシーに関連付けられる業務変更には以下のものがあります。

- プロビジョニング ロールをはじめとするロールの割り当てまたは取り消し（プロビジョニング ディレクトリのみを使用している場合）
- グループ メンバシップの割り当てまたは取り消し
- ユーザ プロファイルの属性の更新

たとえば、ある企業では、副社長は全員カントリー クラブ メンバー グループに所属しており、給与承認者ロールを所有していることを記述するアイデンティティポリシーを作成する場合があります。ユーザの役職が副社長に変わり、そのユーザがアイデンティティポリシーに同期されると、CA Identity Manager は、そのユーザを適切なグループおよびロールに追加します。副社長が CEO に昇進すると、副社長アイデンティティポリシーの条件を満たさなくなります。よって、このポリシーで適用されていた変更は取り消され、CEO ポリシーに基づいた新しい変更が適用されます。

アイデンティティポリシーに基づいて発生するこの変更アクションには、ワークフロー制御下に置かれて監査されるイベントが含まれます。前の例では、給与承認者ロールによって、所属するメンバに重要な権限が付与されます。給与承認者ロールを保護するために、企業は、ロールの割り当て前に一連の承認を必要とするワークフロープロセスを作成し、さらにロールの割り当てを監査するように CA Identity Manager を設定できます。

アイデンティティポリシー管理を簡略化するため、アイデンティティポリシーはアイデンティティポリシーセットとしてグループ化されています。たとえば、副社長ポリシーと CEO ポリシーを、幹部権限アイデンティティポリシーセットの一部とすることができます。

注: CA Identity Manager には「禁止アイデンティティポリシー (504P.)」と呼ばれる追加のタイプのアイデンティティポリシーが含まれます。タスクがサブミットされる前に実行されるこれらのポリシーにより、管理者は権限の割り当てやプロファイル属性の変更を行う前にポリシー違反を確認することができます。違反がある場合、管理者はタスクをサブミットする前に違反をクリアできます。

アイデンティティポリシー セットの計画ワークシート

アイデンティティポリシーセットには、アイデンティティポリシーが 1 つ以上含まれています。アイデンティティポリシーセットを作成する前に、以下のワークシートを使用してこのセット内の各アイデンティティポリシーを計画してください。

質問	回答
アイデンティティポリシーにどのような名前を付けますか。	
どのユーザにアイデンティティポリシーを適用しますか。	

質問	回答
アイデンティティポリシーをユーザに適用すると、CA Identity Manager はどのようなアクションを実行しますか。	
ユーザに適用されているアイデンティティポリシーの適用を取り消すと、CA Identity Manager はどのようなアクションを実行しますか。	
CA Identity Manager はアイデンティティポリシーの変更を複数回適用しますか。それとも、ポリシーの条件を最初に満たしたときに1回のみ適用しますか。	

ポリシーセットの各アイデンティティポリシーについてこのワークシートを記入したら、ポリシーが他のポリシーと競合しないことを確認してください。たとえば、あるポリシーが取り消している権限を別のポリシーが付与しないようにします。

アイデンティティポリシーセットの作成

アイデンティティポリシーセットを作成するには、システム マネージャ ロールまたは [アイデンティティポリシーセットの作成] タスクを含むロールを所有している必要があります。

アイデンティティポリシーセットを作成するには、以下の手順に従います。

1. [アイデンティティポリシーセットのプロファイルの定義](#) (P. 484)
2. [ポリシーセットメンバールールの作成](#) (P. 484)
3. [アイデンティティポリシーの作成](#) (P. 485)
4. [アイデンティティポリシーセットの所有者の指定](#) (P. 495)

注: CA Identity Manager 環境のポリシーを使用するには、CA Identity Manager 管理コンソールでアイデンティティポリシーを有効にします。詳細については、「[設定ガイド](#)」を参照してください。

アイデンティティ ポリシー セットのプロファイルの定義

[プロファイル] タブでは、アイデンティティ ポリシー セットの基本プロパティを定義できます。

アイデンティティ ポリシー セットのプロファイルを定義する方法

1. ユーザ コンソールから [ポリシー] - [アイデンティティ ポリシーの管理] - [アイデンティティ ポリシー セットの作成] を選択します。

アイデンティティ ポリシーの管理権限を持つユーザとして **CA Identity Manager** にログインしている必要があります。これらの権限は、デフォルトのシステム マネージャ ロールに含まれます。

2. アイデンティティ ポリシー セットの新規作成、または既存のアイデンティティ ポリシー セットのコピーの作成を選択します。
3. アイデンティティ ポリシー セットの名前を入力します。
4. アイデンティティ ポリシー セットのカテゴリを入力します。
カテゴリでは、アイデンティティ ポリシー セットがレポートの目的別にグループ化されます。[カテゴリ] フィールドは必須です。
5. アイデンティティ ポリシー セットの説明を入力することもできます。
6. アイデンティティ ポリシー セットを利用可能に設定したくない場合、[有効] チェック ボックスをクリアします。
7. [プロファイル] タブが完了したら、[ポリシー] タブを選択して、アイデンティティ ポリシー セット用のアイデンティティ ポリシーを作成します。

ポリシー セット メンバールールの作成

ポリシー セットが特定のユーザのみに適用されるように、ポリシー セットのメンバールールを作成できます。セットにおけるアイデンティティ ポリシーが評価される前にルールが評価され、大幅に時間を短縮できます。たとえば、メンバールールによりアイデンティティ ポリシーの評価がユーザの **10 %** に制限されている場合、そのルールは評価時間を **90 %** 短縮できます。

ポリシー セット メンバールールを作成する方法

1. [ポリシー] タブを選択します。
2. [ポリシー セット メンバールール] で、[編集] 記号をクリックします。
3. 特定のユーザのみに適用されるルールを入力します。
4. [OK] をクリックします。

詳細情報:

[アイデンティティ ポリシーの作成](#) (P. 485)

アイデンティティポリシーの作成

アイデンティティ ポリシー セットのプロファイルとメンバールールを定義すると、このポリシー セットでアイデンティティ ポリシーを定義できます。

注: 大規模な実装環境では、アイデンティティ ポリシー ルールを評価するのにかなりの時間を要することがあります。ユーザ属性を含むルールに対する評価時間を短縮するには、メモリ内評価オプションを有効にします。詳細については、「[設定ガイド](#)」を参照してください。

アイデンティティポリシーを作成する方法

1. [ポリシー] タブを選択します。
2. [追加] をクリックします。
3. アイデンティティ ポリシーの名前を入力します。
4. ユーザが最初にポリシーを満たしたときのみこのポリシーを適用する場合は、[1回のみ適用] チェック ボックスをオンにします。
5. [コンプライアンス] チェック ボックスをオンにして、コンプライアンス ポリシーとしてこのポリシーをフラグ設定します。

このチェック ボックスをオンにした場合の処理は以下のとおりです。

- CA Identity Manager は、コンプライアンス ポリシーと同期していないユーザに対してレポートを生成することができます。
 - [コンプライアンス違反] アクションが、[ポリシー適用/削除時のアクション] リスト ボックスに表示されます。
6. ポリシー条件セクション内でポリシーを適用するユーザを特定します。
 7. [ポリシー適用時のアクション] セクションで、アイデンティティ ポリシーをユーザに適用したときに CA Identity Manager が実行するアクションを定義します。
 8. [ポリシー削除時のアクション] セクションで、ユーザがアイデンティティ ポリシーの条件を満たさなくなったときに CA Identity Manager によって実行されるアクションを定義します。
 9. [OK] をクリックします。

注: 作成したアイデンティティ ポリシー セットを使用する前に、管理コンソールでアイデンティティ ポリシーを有効にする必要があります。詳細については、「[設定ガイド](#)」を参照してください。

1 回のみ適用の設定

1 回のみ適用の設定によって、CA Identity Manager はアイデンティティ ポリシーの適用方法を変えることができます。

1 回のみ適用の設定を有効にする

「1 回のみ適用」設定を有効にすると、アイデンティティ ポリシーで定義された条件をユーザが最初に満たしたとき、CA Identity Manager はこのポリシーに関連付けられた変更を適用します。ポリシーに関連付けられた変更アクションが発生するのは 1 回のみです。このため、ポリシーが以前に適用されている場合には、CA Identity Manager はポリシーの更新をユーザに適用しません。

ユーザがポリシーで定義された条件を満たさなくなると、CA Identity Manager はポリシーの削除アクションを実行します。

「1 回のみ適用」設定は、通常、リソースのプロビジョニング時に使用されます。たとえば、携帯電話をマネージャに割り当てるポリシーがあるとします。ユーザが最初にマネージャになったときに、このユーザに携帯電話が割り当てられます。CA Identity Manager はポリシーを評価するたびにではなく、1 回のみ携帯電話を発行します。携帯電話ポリシーを更新して、新しい携帯電話モデルを追加した場合、CA Identity Manager は既存のマネージャに新しい携帯電話を発行しません。

注: CA Identity Manager をプロビジョニングサーバに統合すると、リソース プロビジョニングが使用できます。

1 回のみ適用の設定を無効にする

「1 回のみ適用」の設定を有効にしない場合、アイデンティティ ポリシーに関連付けられる変更アクションは、アイデンティティ ポリシーが評価されるたびに適用されます。これは、変更アクションが以前に適用されたかどうかに関係なく、CA Identity Manager はポリシーの条件を満たすすべてのユーザに変更アクションを適用することを意味します。

通常、コンプライアンスを適用するアイデンティティ ポリシーでは「1 回のみ適用」設定を無効にします。たとえば、マネージャの支出権限を \$5,000 に制限するアイデンティティ ポリシーを作成できます。CA Identity Manager でマネージャの支出権限を \$10,000 に設定すると、支出権限は \$5,000 にリセットされます。マネージャをアイデンティティ ポリシーと同期するたびに、CA Identity Manager は支出権限が正しく設定されていることを確認します。

変更アクションと競合する変更を手動でユーザ プロファイルに加えると、CA Identity Manager はユーザをポリシーと同期する際にこの変更を上書きします。

上記の例では、誰かがマネージャの支出権限を手動で \$10,000 に増やすと、CA Identity Manager はマネージャをポリシーと同期する際に支出権限が \$5,000 にリセットされます。

以下の表は、[1 回のみ適用] 設定を有効または無効にしたときの影響についてまとめています。

[1 回のみ適用]の設定	結果
有効	■ アイデンティティ ポリシーに関連付けられた変更アクションが 1 回のみ適用されます。 ■ アイデンティティ ポリシー適用後に手動で加えられた変更は保持されます。 ■ CA Identity Manager が以前にアイデンティティ ポリシーを適用している場合は、このポリシーの条件を満たしているユーザーに更新が適用されません。 ■ ユーザーがアイデンティティ ポリシーで定義された条件を満たさなくなると、CA Identity Manager は削除アクションを実行します。
無効	■ アイデンティティ ポリシーに関連付けられた変更アクションは、ユーザーをポリシーと同期するたびに適用されます。 ■ 手動で加えた変更は、アイデンティティ ポリシーの適用時に上書きされます。 ■ ポリシーの更新は、ユーザーの同期時に適用されます。 ■ ユーザーがアイデンティティ ポリシーで定義された条件を満たさなくなると、CA Identity Manager は削除アクションを実行します。

ポリシー条件

ポリシー条件とは、アイデンティティ ポリシーを適用するユーザを決定するルールです。

以下の表に、使用できるオプションの説明をまとめます。

構文	条件	例
(すべて)	アイデンティティ ポリシーはすべてのユーザに適用されます。	
条件 <ユーザ フィルタ>	ユーザは、1 つ以上の属性値に一致する必要があります。	役職がマネージャ、地域が東部のユーザ
内<組織ルール>	指定した組織にユーザが所属していなければなりません。 注: このオプションを選択すると、CA Identity Manager には、以下のオプションを選択できる新しいリスト ボックスが表示されます。 ■ 組織 <組織> [かつ次より低い] - 組織検索画面を使用して、組織を選択します。組織の子組織を指定することもできます。 ■ <組織フィルタ> [かつ次より低い] 組織 - 1 つ以上の組織を選択するフィルタを指定します。	販売部門以下の組織内のユーザ
条件 <ユーザ フィルタ> および所属組織 <組織ルール>	ユーザは、特定のユーザ属性に一致しており、特定の組織に所属している必要があります。	役職 = マネージャおよび組織 = セールス*

構文	条件	例
以下のメンバである<グループメンバルール>	ユーザは、グループの属性により指定される条件を満たすグループに所属している必要があります。 注: このオプションを選択すると、CA Identity Manager には、以下のオプションを選択できる新しいリストボックスが表示されます。 ■ グループ<グループ>-グループ検索画面を使用してグループを選択します。 ■ <グループ フィルタ>のグループ-1つ以上のグループを選択するフィルタを指定します。	所有者が CIO のグループのメンバであるユーザ
以下のメンバである<ロールルール>	ユーザはロールのメンバである必要があります。ロールは以下のいずれかにすることができます。 ■ アクセス ロール ■ 管理ロール ■ プロビジョニング ロール 注: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。詳細については、<i>「Installation Guide」</i>を参照してください。	ヘルプ デスク ロールのメンバであるユーザ

構文	条件	例
以下の管理者である<ロール ルール>	ユーザはロール管理者である必要があります。ロールは以下のいずれかにすることができます。 ■ アクセス ロール ■ 管理ロール ■ プロビジョニング ロール 注: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。詳細については、<i>「Installation Guide」</i>を参照してください。	セールス マネージャ ロール管理者であるユーザ
以下の所有者である<ロール ルール>	ユーザはロールの所有者である必要があります。ロールは以下のいずれかにすることができます。 ■ アクセス ロール ■ 管理ロール ■ プロビジョニング ロール 注: プロビジョニング ロールを使用するには、CA Identity Manager をプロビジョニング サーバと統合する必要があります。詳細については、<i>「Installation Guide」</i>を参照してください。	ユーザ マネージャ ロー ルの所有者であるユーザ
このクエリで返される値 <LDAP クエリ>	ユーザは LDAP クエリに基づいた条件を満たす必要があります。	LDAP クエリの条件に一致するユーザ 例 : (departmentNumber=Accounts)

構文	条件	例
<管理 OR 演算制約>	ユーザは、条件のリストの中の少なくとも 1 つの条件を満たしている必要があります。管理 AND 演算制約では、以下の種類のフィルタを指定できます。 ■ アクセス/管理/プロビジョニング ロールのメンバ ■ アクセス/管理/プロビジョニング ロールの管理者 ■ アクセス/管理/プロビジョニング ロールの所有者 ■ グループのメンバ	認証マネージャ ロールのメンバであるか、認証マネージャ ロールの所有者であるユーザ
<管理 AND 演算制約>	ユーザは、条件のリスト内の条件をすべて満たしている必要があります。管理 AND 演算制約では、以下の種類のフィルタを指定できます。 ■ アクセス/管理/プロビジョニング ロールのメンバ ■ アクセス/管理/プロビジョニング ロールの管理者 ■ アクセス/管理/プロビジョニング ロールの所有者 ■ グループのメンバ	Contract Initiator ロールのメンバであり、かつ Contract Approver ロールのメンバであるユーザ

ポリシー適用/削除時のアクション

アイデンティティポリシーの評価時に CA Identity Manager が実行する変更アクションを定義できます。定義できるアクションには以下のものがあります。

ポリシー適用時のアクション

ユーザがポリシー条件内の条件を満たす場合に CA Identity Manager により実行される一連のアクションです。

ポリシー削除時のアクション

ユーザがポリシー条件内の条件を満たさなくなった場合に CA Identity Manager により実行される一連のアクションです。

アイデンティティ ポリシーを適用または削除するときに **CA Identity Manager** が実行できるアクションは同じです。詳細については以下の表を参照してください。

変更アクション	説明
グループ <グループ名> への追加 [...]	グループにユーザを追加します。 このオプションを選択すると、 CA Identity Manager には、対象となるグループを検索できる画面が表示されます。
ユーザの組織の <グループ名> への追加	ローカル グループにユーザを追加します。 このオプションを選択すると、 CA Identity Manager には、追加するグループ名を入力できるテキスト ボックスが表示されます。
<単一値ユーザ属性> の値の設定	ユーザ プロファイルの属性値を設定します。 既存の値がある場合は、 CA Identity Manager によって、変更アクションで指定した値に上書きされます。
<値> の <複数値ユーザ属性> への追加	複数値のユーザ属性に値を追加します。 このオプションは既存の値を上書きしません。
アクセス ロールのメンバの作成	アクセス ロールにユーザを割り当てます。
アクセス ロール管理者の作成	アクセス ロールのユーザ管理者の作成
管理ロールのメンバの作成	管理ロールのユーザ メンバの作成
管理ロール管理者の作成	管理ロールのユーザ管理者の作成
プロビジョニング ロールのメンバの作成	関連するエンドポイントアカウントを作成する、プロビジョニング ロールのユーザ メンバを作成します。 注: プロビジョニング ロールを使用するには、 CA Identity Manager をプロビジョニング サーバと統合する必要があります。お使いのアプリケーション サーバの <i>「Installation Guide」</i> を参照してください。
プロビジョニング ロール管理者の作成	プロビジョニング ロールのユーザ管理者を作成します。 注: プロビジョニング ロールを使用するには、 CA Identity Manager をプロビジョニング サーバと統合する必要があります。お使いのアプリケーション サーバの <i>「Installation Guide」</i> を参照してください。

変更アクション	説明
グループ<グループ名>からの削除 [...]	グループからユーザを削除します。 このオプションを選択すると、CA Identity Manager には、対象となるグループを検索できる画面が表示されます。
ユーザの組織の<グループ名>からの削除	ローカル グループからユーザを削除します。 このオプションを選択すると、CA Identity Manager には、追加するグループ名を入力できるテキスト ボックスが表示されます。
<値> の<複数値ユーザ属性>からの削除	複数値のユーザ属性から値を削除します。
メンバのアクセス ロールからの削除	アクセス ロールの取り消し
管理者のアクセス ロールからの削除	特定のアクセス ロールの管理者権限を取り消します。
メンバの管理ロールからの削除	管理ロールを取り消します。
管理者の管理ロールからの削除	特定の管理ロールの管理者権限を取り消します。
メンバのプロビジョニング ロールからの削除	プロビジョニング ロールを取り消します。
管理者のプロビジョニング ロールからの削除	特定のプロビジョニング ロールの管理者権限を取り消します。
監査メッセージの送信	作成したメッセージを監査データベースに送信します。 このメッセージは、作成したレポートに表示される場合があります。
コンプライアンス違反	作成したメッセージを監査データベースに送信します。 コンプライアンス レポートを作成すると、アイデンティティ ポリシーがユーザに対して適用または削除されるたびに、このメッセージが表示されます。監査の詳細については、「設定ガイド」を参照してください。 注: コンプライアンス違反オプションを使用するには、アイデンティティ ポリシーセットの [プロファイル] タブの [コンプライアンス] チェック ボックスをオンにする必要があります。

変更アクション	説明
承諾 (ポリシー適用のアクションのみ)	禁止アイデンティティポリシー違反が発生した場合にタスクをサブミットできます。 このアクションを選択した場合、CA Identity Manager が監査データベース内に書き込み、違反の発生時に [サブミット済みタスクの表示] に表示するメッセージを入力します。
拒否 (ポリシー適用のアクションのみ)	アイデンティティポリシー違反が発生した場合のタスクによるサブミットを禁止します。 このアクションは禁止アイデンティティポリシーと共に使用され、ユーザが利害の衝突や不正の原因となりうる権限を得ることを禁止します。 このアクションを選択した場合、違反の発生時に CA Identity Manager によって表示されるメッセージの入力も行います。このメッセージは監査データベースに格納され、ユーザコンソールに表示されます。
警告 (ポリシー適用のアクションのみ)	違反がワークフロー承認ポリシーと関連付けられている場合、禁止アイデンティティポリシー違反の発生時にワークフロープロセスをトリガします。 ワークフローが設定されているかどうかに関わらず、CA Identity Manager はタスクのサブミットを許可します。 注: ワークフロープロセスの禁止アイデンティティポリシーへの関連付けの詳細については、「ワークフローおよび禁止アイデンティティポリシー」を参照してください。(P. 510) このアクションを選択した場合、違反の発生時に CA Identity Manager によって表示されるメッセージの入力も行います。このメッセージは監査データベースに格納され、[サブミット済みタスクの表示] に表示されます。

詳細情報:

[禁止アイデンティティポリシー](#) (P. 504)

[ワークフローおよび禁止アイデンティティポリシー](#) (P. 510)

アイデンティティポリシー セットの所有者の指定

[所有者] タブで、アイデンティティポリシー セットの所有者にすることができるルールを定義します。アイデンティティポリシー セットの所有者は、ポリシー セットの基本情報を変更したり、セット内のアイデンティティポリシーを追加、変更、または削除することができます。

[所有者] タブで以下の手順を実行します。

1. アイデンティティポリシー セットを変更できるユーザを決定する、所有者ルールを定義します。
2. [サブミット] をクリックします。

アイデンティティポリシー セットの管理

CA Identity Manager には、アイデンティティポリシー セットを管理する以下のタスクがあります。

- アイデンティティポリシー セットの表示
- アイデンティティポリシー セットの変更
- アイデンティティポリシー セットの削除

デフォルトでは、管理者が上記のいずれかのタスクを使用すると、CA Identity Manager には、この管理者が所有者であるアイデンティティポリシー セットのリストが表示されます。管理者は、リストから必要なポリシー セットを選択できます。

アイデンティティポリシー セットが多く含まれている CA Identity Manager 環境では、アイデンティティポリシー セットの表示、変更、および削除タスクをカスタマイズすると、リストに表示する代わりに、管理者がアイデンティティポリシー セットを検索できるように設定できます。

上記のタスクをカスタマイズする方法

1. ユーザ コンソールで、[ルールおよびタスク] - [管理ロール] - [管理タスクの変更] を選択します。
[管理タスクの変更] 画面が開きます。
2. カスタマイズするタスクを検索し、選択します。

3. [スコープ] タブで、[すべてのアイデンティティポリシーセット] を選択します。

このオプションを選択すると、CA Identity Manager は [デフォルトのアイデンティティポリシーセット検索] 画面の定義を使用します。

4. [サブミット] をクリックします。

ユーザとアイデンティティポリシーとの同期の方法

アイデンティティポリシーを使用する際には、CA Identity Manager でのポリシー評価方法とユーザへの適用方法を理解することが重要です。ユーザの同期プロセスを十分に理解していない場合、予期しない結果を引き起こすアイデンティティポリシーを設定してしまう場合があります。

CA Identity Manager でアイデンティティポリシーが評価および適用される方法を以下の手順に示します。

1. ユーザ同期プロセスは以下の方法で開始されます。
 - **自動** — 自動的にユーザ同期をトリガするように CA Identity Manager のタスクを設定できます。
 - **手動** — ユーザ コンソールの [ユーザの同期] タスクを使用して、ユーザを同期します。
2. CA Identity Manager は、ユーザに適用するアイデンティティポリシーの組み合わせを判別します。
3. CA Identity Manager は、そのユーザに適用するアイデンティティポリシーの一式を、そのユーザに対して適用済みのポリシーの一覧と比較します。

注: ユーザに適用されたポリシーの一覧は、ユーザプロファイルの %IDENTITY_POLICY% 汎用属性に格納されています。属性の設定の詳細については、「[設定ガイド](#)」を参照してください。

- 適用可能なポリシーの一覧に含まれるアイデンティティポリシーが、以前にそのユーザに適用されていない場合、そのポリシーは CA Identity Manager で割り当て一覧に追加されます。
- 適用可能なポリシーの一覧に含まれるアイデンティティポリシーが、以前にそのユーザに適用されていて、さらにそのポリシーで [1 回のみ適用] 設定が無効になっている場合、そのポリシーは CA Identity Manager で再割り当て一覧に追加されます。
- アイデンティティポリシーが適用可能なポリシーの一覧になく、かつ、そのポリシーがユーザに適用されている場合は、ユーザはそのポリシー条件に一致なくなります。CA Identity Manager ではそれらのポリシーは割り当て解除一覧に追加されます。

4. ユーザに対するすべてのポリシーを CA Identity Manager が評価後、以下の順序でポリシーが適用されます。
 - a. 割り当て解除一覧のアイデンティティ ポリシー
 - b. 割り当て一覧のアイデンティティ ポリシー
 - c. 再割り当て一覧のアイデンティティ ポリシー

5. 各アイデンティティ ポリシーの適用後、CA Identity Manager はポリシーを再評価し、最初の同期化プロセス（手順 2 から 4）で発生した変更に基づいて、新たな変更が必要かどうか確認します。

この手順は、アイデンティティ ポリシーの適用によって加えられた変更が、他のアイデンティティ ポリシーをトリガしていないことを確認するためのものです。

6. 適用可能なすべてのポリシーとユーザが同期するまで、または管理コンソールで定義された最大再帰レベルに CA Identity Manager で達するまで、CA Identity Manager は引き続きアイデンティティ ポリシーの再評価と適用を実施します。

たとえば、ユーザがロールに割り当てられると、アイデンティティ ポリシーはユーザの部署を変更します。新しい部署は、別のアイデンティティ ポリシーをトリガします。ただし、再帰レベルが 1 に設定されている場合は、ユーザが再同期されるまで後続の変更は行われません。

再帰レベルの設定の詳細については、管理コンソールのオンライン ヘルプを参照してください。

自動的なユーザ同期の設定

CA Identity Manager では、タスクのライフサイクル中のさまざまな時点でアイデンティティ ポリシーとユーザ アカウントを自動的に同期できます。

CA Identity Manager のタスクは、タスク処理中に発生する検出可能なアクティビティであるイベントを生成します。たとえば、デフォルトの [ユーザの作成] タスクは、CreateUserEvent、AddUserToGroupEvent、および AssignAccessRoleEvent を生成します。タスクの完了後、または各イベントの完了時にユーザを同期するように、CA Identity Manager を設定できます。

注: [「アイデンティティ ポリシーとユーザの同期化」](#) (P. 496) のセクションではユーザ同期化プロセスについて詳しく説明しています。

ユーザ同期化をトリガするタスクを設定する方法

1. 管理タスクを変更可能なユーザとして CA Identity Manager にログインします。
2. [ロールおよびタスク] - [管理タスク] - [管理タスクの変更] を選択します。

CA Identity Manager の検索画面が表示されます。

3. ユーザ同期化をトリガする管理タスクを検索して、選択します。
4. この管理タスクの [プロファイル] タブの [ユーザの同期] フィールドで以下のいずれかのオプションを選択します。

- **オフ** — このタスクはユーザ同期化をトリガしません。
- **タスク完了時** — CA Identity Manager は、イベントがすべて完了した後にユーザ同期化プロセスが開始されます。この設定は、[ユーザの作成]、[ユーザの変更]、および [ユーザの削除] タスクのデフォルト同期化オプションです。それ以外の他のタスクのデフォルト設定は、[オフ] です。

注: 複数のイベントを含むタスクに対して [タスク完了時] オプションを選択すると、CA Identity Manager では、そのタスク内のすべてのイベントが完了するまでユーザは同期されません。イベントの 1 つまたは複数があるワークフローの承認を必要とする場合、その承認に数日かかることがあります。すべてのイベントが完了するまで CA Identity Manager がアイデンティティポリシーを適用しないであることを避けるには、[各イベント発生時] オプションを選択します。

- **各イベント発生時** — CA Identity Manager は、タスク内の各イベントが完了したときにユーザ同期化プロセスが開始されます。

同一のユーザにプライマリ イベントとセカンダリ イベントがあるタスクの場合は、ユーザ同期化を [各イベント発生時] に設定すると、[タスク完了時] オプションを選択した場合よりも、ユーザに適用されるポリシーを評価する回数が多くなります。

手動によるユーザの同期化

ユーザアカウントが正しい権限を有しているか、またはコンプライアンスポリシーに従っているかどうかを確認する場合、ユーザとアイデンティティポリシーセットを手動で同期できます。

CA Identity Manager ユーザ コンソールで [ユーザの同期] タスクを使用することで、ユーザを手動で同期できます。

注: [ユーザの同期] タスクが適切に動作するには、[ユーザの同期] オプションを [オフ] に設定し、[アカウントの同期化] オプションを [タスク完了時] または [各イベント発生時] に設定する必要があります。パフォーマンスを高めるには、[タスク完了時] オプションを選択します。これらのオプションは、ユーザ同期の [プロファイル] タブで設定します。

「ユーザの同期」タスクには、以下のタブが含まれます。

- **現在一致しているポリシー** — 「ユーザの同期」タスクをサブミットしたときに CA Identity Manager でユーザに適用されるアイデンティティ ポリシーの一覧を表示します。

注: 「現在一致しているポリシー」タブには、「ユーザの同期」タスクにアクセスした時点でユーザに適用されるアイデンティティ ポリシーのみが表示されます。ユーザをこれらのポリシーと同期すると、他のアイデンティティ ポリシーがトリガされる変更が発生する場合があります。これらのポリシーを確認するまで CA Identity Manager で新しいポリシーが適用されないようにするには、CA Identity Manager 管理コンソールでアイデンティティ ポリシーセットの再帰レベルを 1 に設定します。「ユーザの同期」タスクをサブミットした後に、再度このタスクにアクセスして、ポリシーを確認します。

- **すでに適用されているポリシー** —すでにユーザに適用されているアイデンティティ ポリシーの一覧を表示します。
- **同期化サマリ** —ユーザに適用するアイデンティティ ポリシーおよびこのポリシーの変更アクションをすべて表示します。

ユーザ アカウントを同期する方法

1. 「ユーザの同期」タスクを使用可能なユーザとして CA Identity Manager にログインします。(デフォルトでは、システム マネージャ ロールを所有するユーザはこのタスクを使用できます)。
2. 「ポリシー」 - 「ユーザの同期」を選択します。
「ユーザの同期」タスクが開きます。
3. 「同期化サマリ」タブを選択します。
4. CA Identity Manager でユーザに適用されるポリシーおよび関連するアクションを確認して、「サブミット」をクリックします。

ユーザ同期化の確認

ユーザがアイデンティティ ポリシーと同期化されるときに適切な変更が行われることを確認するには、「ユーザの同期」タスクで「すでに適用されているポリシー」タブを確認します。

1. 「ユーザの同期」タスクを使用可能なユーザとして CA Identity Manager にログインします。(デフォルトでは、システム マネージャ ロールを所有するユーザはこのタスクを使用できます)。
2. 「ポリシー」 - 「ユーザの同期」を選択します。
「ユーザの同期」タスクが開きます。

3. [すでに適用されているポリシー] タブを選択します。
4. CA Identity Manager でユーザに適用されるポリシーおよび関連するアクションを確認します。

CA Identity Manager 環境のアイデンティティ ポリシー セット

以下のセクションでは、アイデンティティ ポリシーを使用するさまざまな方法について説明しています。

- [例：ユーザ属性を自動的に追加する](#) (P. 500)
- [例：リソースおよび権限付与の割り当て](#) (P. 501)
- [例：コンプライアンスの適用](#) (P. 502)
- [例：職務の分離の実行](#) (P. 503)

例：ユーザ属性を自動的に追加する

アイデンティティ ポリシー セットを使用して、別の属性値やユーザ権限に基づいてユーザ属性値を自動的に割り当てることができます。たとえば、ユーザのホーム オフィスに基づいてユーザの送付先住所を自動的に入力するアイデンティティ ポリシー セットを作成することができます。

従業員の住所のアイデンティティ ポリシーを設定するには、オフィスの場所ごとに以下の設定でアイデンティティ ポリシーを作成します。

設定	値
ポリシー条件	オフィス = <オフィスの場所>
ポリシー適用時のアクション	番地の設定 = <番地の住所> 市区町村の設定 = <市区町村> 都道府県の設定 = <都道府県> 郵便番号の設定 = <郵便番号>

以下の図は、従業員の住所のアイデンティティポリシーセットのサンプルポリシーを示しています。

アイデンティティポリシー

ポリシー セット

	ポリシー名	ポリシー メンバ ルール	ポリシー適用時のアクション
	BT	条件 (Office = "BT")	"Address" を 601 ストリート" に設定 "City" を BT" に設定 "State" を MA" に設定 "Postal code" を 02451" に設定
	NY	条件 (Office = "NY")	"Address" を 201 ストリート" に設定 "City" を NY" に設定 "State" を NY" に設定 "Postal code" を 10017" に設定

例: リソースおよび権限付与の割り当て

アイデンティティポリシーでは、ユーザがポリシー条件を満たしたときに、ドメインアカウントなどのリソースの割り当て、ユーザをロールのメンバにするといった権限の付与を自動的に行うことができます。たとえば、ユーザの役職に基づいてリソースとロールを割り当てる一連のアイデンティティポリシーを作成できます。

リソースおよびロールを割り当てるアイデンティティポリシーを作成するには、組織の役職ごとに以下の設定でアイデンティティポリシーを作成します。

設定	値
ポリシー条件	役職 = <役職>
ポリシー適用時のアクション	ポリシー条件を満たすユーザにリソースまたは権限を割り当てるアクションです。以下に例を示します。 ■ <グループ> のメンバの作成 ■ 管理ロール <管理ロール> のメンバの作成 ■ プロビジョニング ロール <プロビジョニング ロール> のメンバの作成

設定	値
ポリシー削除時のアクション	ユーザがポリシー条件を満たさなくなったときにリソースまたは権限を削除するアクションです。たとえば、アイデンティティ ポリシーを適用されたときに CA Identity Manager でユーザがロールのメンバになった場合、ユーザがポリシー条件を満たさなくなるとロールが取り消されるように CA Identity Manager を設定することができます。

以下の図は、従業員のリソースのアイデンティティ ポリシー セットのサンプルポリシーを示しています。

アイデンティティ ポリシー

ポリシー セット

ポリシー名	ポリシー メンバ ルール	ポリシー適用時のアクション	ポリシー削除時のアクション
マネージャ	条件 (Title = "マネージャ")	管理ロール "UM" のメンバの作成 プロビジョニング ロール "UP" の メンバの作成	メンバの管理ロール "UM" からの削除
HR	条件 (Title = "HR")	管理ロール "UM" のメンバの作成 グループ "UG" への追加 プロビジョニング ロール "UP" の メンバの作成	グループ "UG" からの削除 メンバの管理ロール "UM" からの 削除 メンバのプロビジョニング ロール "UP" からの削除

例: コンプライアンスの適用

アイデンティティ ポリシーを設定して、存在しなければならない条件、または存在してはいけない条件を定義したり、これらの条件の評価に基づいて特定のアクションを実行したりできます。たとえば、マネージャの支出上限を \$5,000 に制限することを記述するコンプライアンス ポリシーを定義できます。あるマネージャの支出上限が \$10,000 である場合は、**CA Identity Manager** では、このマネージャの支出上限をリセットして、監査目的のためコンプライアンス違反を記録することができます。

支出上限を適用するコンプライアンス ポリシー セットを作成するには、以下の手順に従ってアイデンティティ ポリシーを作成します。

設定	値
1 回のみ適用	無効
コンプライアンス	有効

設定	値
ポリシー条件	コンプライアンスまたはコンプライアンス違反を定義する条件。以下に例を示します。 役職 = <役職> AND 支出上限 = <支出上限>
ポリシー適用時のアクション	ポリシー条件の適用時に CA Identity Manager によって実行されるアクション。以下に例を示します。 ■ コンプライアンス違反メッセージ: 支出上限を超えています ■ 支出上限を <値> に設定

以下の図に、この例で説明したコンプライアンス ポリシーの例を示します。

アイデンティティポリシー

ポリシー セット

ポリシー名	ポリシー ゼンバルール	ポリシー適用時のアクション
マネージャ	条件 (Title = "マネージャ" ~ Spending limit > "5000")	コンプライアンス違反メッセージ: 限度額は5000を超えました

例: 職務の分離の実行

アイデンティティ ポリシーで同じユーザーに同時にロールを許可できない相互排他的なロールを定義できます。たとえば、昇給を許可できるユーザー マネージャが給与承認担当者にならないようにすることができます。

職務の分離を適用するアイデンティティ ポリシー セットを作成するには、以下の手順に従ってアイデンティティ ポリシーを作成します。

設定	値
1 回のみ適用	無効
コンプライアンス	有効

設定	値
ポリシー条件	<管理 AND 演算制約> オプションを使用して、ビジネスポリシーに違反する一連の条件を定義します。ユーザがすべての条件を満たす場合は、[ポリシー適用時のアクション] フィールドのアクションが CA Identity Manager によって実行されます。 たとえば、以下のようにポリシー条件を設定します。 AND 演算 (<ロール>のメンバである) かつ (<他のロール>のメンバである)
ポリシー適用時のアクション	ポリシー条件の適用時に CA Identity Manager によって実行されるアクション。以下に例を示します。 ■ コンプライアンス違反メッセージ: ユーザが相互に排他的なロールを所有しています ■ <ロール> からメンバを削除します

以下の図に、この例のアイデンティティ ポリシーを示します。

アイデンティティ ポリシー

ポリシー セット

ポリシー名	ポリシー メンバ ルール	ポリシー適用時のアクション
制限	AND 演算 (以下のメンバである (管理 ロール "ユーザ マネージャ") ~ 以下のメンバである (管 理ロール "ユーザ 承認者"))	コンプライアンス違反メッセージ: ユー ザーは相互に排他的権利を有する メンバの管理ロール "ユーザ承認者" からの削除

禁止アイデンティティ ポリシー

禁止アイデンティティ ポリシーは、ユーザが利害の衝突や不正の原因となりうる権限を得ることを防止するタイプのアイデンティティ ポリシーです。これらのポリシーは、企業に要求される職務分掌 (SOD) をサポートします。

タスクがサブミットされる前に禁止のアイデンティティ ポリシーを実行することにより、管理者は権限の割り当てやプロファイル属性の変更を行う前にポリシー違反を確認することができます。違反がある場合、管理者はタスクをサブミットする前に違反をクリアできます。

たとえば企業は、ユーザ マネージャ ロールを持つユーザが同時にユーザ承認者ロールも持つことを禁止する禁止アイデンティティ ポリシーを作成できます。管理者が [ユーザの変更] タスクを使用してユーザ マネージャにユーザ承認者ロールを与えた場合、CA Identity Manager は違反についてのメッセージを表示します。管理者はロールの割り当てを変更し、タスクをサブミットする前に違反をクリアできます。

次の変更に対して、禁止アイデンティティ ポリシーを作成できます。

■ **ロール メンバシップ**

ユーザが特定のロールを同時に持つことを防ぎます。

たとえば、ユーザは、ユーザ マネージャとユーザ承認者ロールを同時に持つことはできません。

■ **ロール管理者**

ユーザがほかのロールの管理者である場合、特定のロール管理者になるのを防ぎます。

たとえば、ユーザは、ユーザ マネージャとユーザ承認者ロールの管理者には同時になることはできません。

■ **ユーザ属性**

ユーザが特定のプロファイル属性を同時に持つことを防ぎます。

たとえば、ユーザはシニア アカウンタントの役職を持ちながら、IT 部門に属することはできません。

■ **組織属性**

ユーザ プロファイルが特定の組織内で作成されるのを防ぎます。

たとえば、管理者は従業員プロファイルをサプライヤの組織に作成することはできません。

■ **グループ属性**

ユーザが特定のグループのメンバになるのを防ぎます。

たとえば、ユーザはプロジェクト チーム グループとアカウントिंग グループのメンバになることはできません。

詳細情報:

[禁止アイデンティティ ポリシー違反のためのアクション](#) (P. 506)

禁止アイデンティティポリシー違反のためのアクション

禁止アイデンティティポリシーがビジネスの変更に適用される場合、CA は特定のアクションを実行して違反に対処します。

アイデンティティポリシーでこれらのアクションのいずれかを特定する場合、違反を説明するメッセージを指定します。このメッセージは、監査データベースに記録されます。アクションのタイプによって、ユーザ コンソールおよび[サブミット済みタスクの表示] のレコードにもメッセージが表示れることもあります。

禁止アイデンティティポリシー用の以下のアクションを設定できます。

承諾

CA Identity Manager は違反を説明する [サブミット済みタスクの表示] にメッセージを表示しますが、タスクによるサブミットは可能です。

拒否

CA Identity Manager はユーザ コンソールにメッセージを表示し、タスクによるサブミットを禁止します。

警告

CA Identity Manager はユーザ コンソールおよび [サブミット済みタスクの表示] にメッセージを表示します。このアクションはオプションで、適切なユーザからの承認が要求されるワークフロープロセスを CA Identity Manager がタスクを実行する前にトリガできます。

ワークフロープロセスをトリガするには、違反の原因となる可能性のあるタスクの[ポリシーベースのワークフロープロセスに禁止アイデンティティポリシーの関連付け \(P. 512\)](#)を行います。

たとえば、ユーザが特定のロールを同時に受信したときに違反が発生した場合、これらのロールをユーザに割り当てるすべてのタスクのワークフロープロセスを設定します。

注: ポリシーベースのタスク用ワークフロープロセスを設定する場合、承認ルールの名前は禁止アイデンティティポリシーを参照する必要があります。

禁止アイデンティティポリシーの仕組み

以下のプロセスの例は、禁止アイデンティティポリシーの仕組みを解説しています。

1. アイデンティティポリシー管理者は、シニア アカウンタントの役職を持つユーザが IT 部門に属することを禁止する禁止アイデンティティポリシーを作成します。

このアイデンティティポリシーの定義時、管理者は **CA Identity Manager** がこのポリシーに違反するいかなる変更も拒否するように指定します。

2. 人事管理者が [ユーザの作成] タスクを使用して、シニア アカウンタントの新規ユーザプロフィールを作成します。人事管理者はユーザの役職は正しいものを選ぶものの、間違えて IT 部門を選択してしまいます。
3. 人事管理者は [ユーザの作成] タスクの残りのフィールドを完了させ、[送信] をクリックします。
4. **CA Identity Manager** はアイデンティティポリシーで定義された変更に関連するタスクを検出し、変更違反がないか評価します。
5. **CA Identity Manager** が違反を検出し、メッセージを人事管理者に表示して、タスクのサブミットを防ぎます。

また、**CA Identity Manager** は監査データベースにメッセージを記録します。

6. 人事管理者はメッセージ内にある違反の詳細を確認し、ユーザの部門を財務に変更します。その後、管理者はタスクを再サブミットします。
7. **CA Identity Manager** はすべての適用されるアイデンティティポリシーに対する提示された変更を評価してから、[ユーザの作成] タスクのサブミットを許可します。

禁止アイデンティティポリシーに関する重要な注意事項

禁止アイデンティティポリシーを実装する前に、以下に注意してください。

- 禁止アイデンティティポリシーは、現在のタスクで提示された変更のために発生した違反のみを防ぎます。既存の違反の禁止は行いません。

たとえば企業は、ユーザがユーザ マネージャおよびユーザ承認者ロールを同時に持つことを禁じる禁止アイデンティティポリシーを作成します。管理者は、すでにユーザ マネージャとユーザ承認者ロールを持つユーザに、グループ マネージャ ロールを割り当てます。**CA Identity Manager** が新規割り当ての成功を許したのは、この変更はポリシー違反の直接の原因ではないためです。

- 複数の禁止アイデンティティポリシーが一連の提示された変更に応用される場合、**CA Identity Manager** は拒否アクションを持つポリシーを最初に適用します。

- 禁止アイデンティティ ポリシー条件で動的グループを特定しないでください（ポリシー条件は、禁止アイデンティティ ポリシーが適用される一連のユーザを決定します）。

たとえば、企業に、マネージャの役職を持つすべてのユーザを含む動的グループがあります。この企業は、マネージャ グループのメンバが契約社員ロールを持つことを禁止する禁止アイデンティティ ポリシーも作成します。

管理者は契約社員ロールを持つユーザの役職を、マネージャに変更します。この変更により、タスクのサブミットが成功した後に、ユーザはマネージャグループのメンバとなります。ただし、ユーザの役職は **CA Identity Manager** によるポリシーの評価時点ではマネージャではないため、違反は検出されません。

- ロール所有者フィルタおよび **LDAP** クエリ フィルタは、禁止アイデンティティ ポリシー用のポリシー条件内ではサポートされていません。

禁止アイデンティティ ポリシーの作成

禁止アイデンティティ ポリシーを作成する前に、一連のアイデンティティ ポリシーを論理的にグループ化するアイデンティティ ポリシー セットを作成します。

注: 作業を始める前に、「[禁止アイデンティティ ポリシーに関する重要な注意事項 \(P. 507\)](#)」を参照してください。

禁止アイデンティティ ポリシー セットを作成する方法

1. ユーザ コンソールから [ポリシー] - [アイデンティティ ポリシー セットの作成] を選択します。

新規のアイデンティティ ポリシー セットを作成するか、既存のアイデンティティ ポリシー セットをテンプレートとして使用します。
2. [アイデンティティ ポリシー セットのプロファイルの定義 \(P. 484\)](#) を [プロファイル] タブで行います。
3. [ポリシー セット メンバールールの作成 \(P. 484\)](#) を [ポリシー] タブで行います。
4. 以下のように禁止アイデンティティ ポリシーを作成します。
 - a. [追加] をクリックします。
 - b. アイデンティティ ポリシーの名前を入力します。

注: [1 回のみ適用] および [コンプライアンス] 設定は、禁止アイデンティティ ポリシーには適用されません。

- c. ポリシー条件セクション内でポリシーを適用するユーザを特定します。

注: ロール所有者フィルタおよび **LDAP** クエリ フィルタは、禁止アイデンティティ ポリシーではサポートされていません。

- d. [ポリシー適用時のアクション] フィールドでは、CA Identity Manager によるポリシー違反の検出時に CA Identity Manager によって行われるアクションを定義します。

承諾

CA Identity Manager は違反を説明する [サブミット済みタスクの表示] にメッセージを表示しますが、タスクによるサブミットは可能です。

拒否

CA Identity Manager はユーザ コンソールにメッセージを表示し、タスクによるサブミットを禁止します。

警告

CA Identity Manager はユーザ コンソールおよび [サブミット済みタスクの表示] にメッセージを表示します。このアクションは、オプションで[ワークフロープロセスのトリガ](#) (P. 510)を行います。

これらのアクションのいずれかを選択する場合、違反の発生時に表示されるメッセージを指定できるテキスト ボックスを CA Identity Manager は表示します。

- e. テキスト ボックス内にメッセージを指定します。

注: ユーザ コンソールのローカライズを行っている場合、メッセージ フィールドではテキストの代わりにリソース キーを指定できます。リソース キーの詳細については「ユーザ コンソール デザイン ガイド」を参照してください。

- f. 必要に応じて追加のアクションを追加し、[OK] をクリックします。

5. [アイデンティティ ポリシー セット用の所有者の指定](#) (P. 495)。

注: 作成したアイデンティティ ポリシー セットを使用する前に、管理コンソールでアイデンティティ ポリシーを有効にする必要があります。詳細については、「[設定ガイド](#)」を参照してください。

使用事例 - ユーザが競合するロールを持つのを防ぐ

Forward, Inc. では従業員がユーザ マネージャ ロールとユーザ承認者ロールを同時に持つことを防止したいと考えています。これら両方のロールを持つ従業員は、給与などのユーザ属性を変更して不正に承認できます。

この状況を防止するため、Forward, Inc. はユーザ マネージャおよびユーザ承認者ロールを持つ従業員に適用される禁止アイデンティティ ポリシーを作成します。管理者がこれらのロールをユーザに与えようとすると、CA Identity Manager はタスクのサブミットを拒否して違反を説明するメッセージを表示します。

禁止アイデンティティ ポリシーを設定して、この使用事例を以下のようにサポートします。

- 作成したいアイデンティティ ポリシーのためのアイデンティティ ポリシー セットを作成します。
- 次の設定を使用して禁止アイデンティティ ポリシーを作成します。
 - ポリシー条件:

このポリシーを次のユーザに適用します:

ユーザ  AND 演算 ()

 以下のメンバである ()

 管理ロール   ) )

かつ  以下のメンバである ()

 管理ロール   ) )

- ポリシー適用時のアクション:
 - 拒否メッセージ: ユーザは、ユーザ承認者とユーザ マネージャ ロールのメンバになることはできません。

ワークフローおよび禁止アイデンティティ ポリシー

禁止アイデンティティ ポリシーが警告を発行するよう設定された場合、違反をトリガする可能性のあるタスク用に、アイデンティティ ポリシーに関連付けられているタスク レベルのポリシーベースのワークフロー プロセスを定義することができます。たとえば、アイデンティティ ポリシーによってシニア アカウンタントが IT 部門のメンバになることを禁止されている場合、[ユーザの作成] および [ユーザの変更] タスク上でタスク レベルのポリシーベースのワークフロー プロセスを定義できます。

タスク レベルのポリシーベースのワークフローの結果として生成されたすべての作業アイテムは、CA Identity Manager がタスクを実行する前に承認される必要があります。承認者は、ユーザ コンソールへのログイン時にワーク リスト アイテムを確認します。承認者がワーク リスト アイテムをクリックすると、違反を説明する警告メッセージを含む承認タスクが表示されます。承認者は、違反に基づいてタスクの承認または拒否を選択できます。

ポリシーベースのワークフロー プロセスは、禁止アイデンティティ ポリシーとポリシー名によって関連付けられています。

詳細情報:

[ポリシーベース ワークフロー \(P. 337\)](#)

承認タスクにおけるアイデンティティポリシー違反

禁止アイデンティティポリシーがタスク用のワークフロー プロセスに関連付けられている場合、CA Identity Manager は適切な承認者のためのワーク リスト アイテムを生成します。これらの承認者は承認タスクを使用して、ポリシー違反をトリガした変更を承認または拒否します。

デフォルトの承認タスクにはアイデンティティポリシー違反をリスト表示するセクションが含まれます。提示された変化が複数の禁止アイデンティティポリシーをトリガする場合、複数の違反がある可能性があります。

各違反には以下のステータスがあります。

- **保留中の評価**

CA Identity Manager はタスクの承認ルールの評価を開始していません。これが初期ステータスです。

- **承認待ち**

CA Identity Manager が承認ルールで定義されているアイデンティティポリシーとの一致を見つけ、関連付けられたワークフロー プロセスをトリガしました。

- **承認済み**

承認者が、提示された変更を承認しました。CA Identity Manager は禁止アイデンティティポリシー違反をトリガした変更を行います。

- **拒否**

承認者が、提示された変更を拒否しました。タスクが拒否されました。

- **ワークフローが設定されていません**

この違反用に設定されたワークフロー プロセスがありません。タスクは承認リクエストなしに実行されます。

禁止アイデンティティ ポリシー用のワークフローを設定する方法

禁止アイデンティティ ポリシー用のワークフローを、禁止アイデンティティ ポリシー違反をトリガする可能性のある変更を含む管理タスクに設定します。

たとえば、禁止アイデンティティ ポリシーによりユーザが特定の管理ロールを同時に持つことが禁止されている場合、管理ロールを割り当てるタスクを設定して、禁止アイデンティティ ポリシー用のワークフローをサポートします。

注: ワークフローを設定する前に、以下の設定で禁止アイデンティティ ポリシーを作成します。

- 一意なポリシー名

ポリシー名は、すべてのアイデンティティ ポリシー セットにわたり一意である必要があります。これは、ワークフロー プロセスがポリシー名により禁止アイデンティティ ポリシーに関連付けられているためです。

複数の禁止アイデンティティ ポリシーが同じ名前を持っている場合、複数のプロセスが適用される可能性があります。

- ポリシー適用時のアクションの警告

警告は、ワークフロー プロセスをトリガできる唯一のアクションです。

禁止アイデンティティ ポリシーの設定後、ポリシー違反をトリガする可能性のあるタスクを決定します。次に、これらのタスク用に[ワークフロー承認ポリシーの作成](#) (P. 513)を行います。

禁止アイデンティティポリシー用のワークフロー承認ポリシーの作成

タスク レベルでポリシーベースの管理タスク用ワークフロー プロセスを設定できます。このワークフロー プロセスには、禁止アイデンティティ ポリシーをワークフローに関連付けできる 1 つかそれ以上の承認ポリシーを含みます。CA Identity Manager は、関連付けされた禁止アイデンティティ ポリシーの違反発生時にワークフローを実行します。

注: タスク レベルのポリシーベースのワークフロー プロセスの詳細については、「[ポリシーベースのワークフロー \(P. 337\)](#)」を参照してください。

禁止アイデンティティポリシー用のワークフロー承認ポリシーを作成する方法

1. 禁止アイデンティティ ポリシーの違反をトリガする可能性のある変更を許可する管理タスクを変更します。

たとえば、ユーザがユーザ マネージャおよびユーザ承認ロースを持っているためにアイデンティティ ポリシー違反が発生する場合、[ユーザの作成] や [ユーザの変更]、[管理ロール メンバ/管理者の変更] といったロールの割り当てを管理者に許可する管理タスクを変更します。

2. [プロファイル] タブの [ワークフロー プロセス] フィールドのとなりにある [編集] アイコンをクリックし、ワークフロー プロセスを追加します。

CA Identity Manager は [タスク レベル ワークフロー設定] 画面を表示します。

3. [ポリシーベース] を選択してから、[追加] をクリックします。
4. [承認ルール] セクションで、[アイデンティティ ポリシー違反] オブジェクトを選択します。
5. [アイデンティティ ポリシー] フィールドで、どのアイデンティティ ポリシーが承認ポリシーに関連付けられているワークフローをトリガするかどうかを決定するフィルタを選択します。

フィルタには、アイデンティティ ポリシー セット名ではなく、アイデンティティ ポリシー名を含めます。

6. 必要に応じて [ルールの評価]、[ポリシー順序]、および [ポリシーの説明] フィールドを設定します。
7. ワークフロー プロセスを選択して、[OK] をクリックします。

ワークフロー プロセスの選択時に、CA Identity Manager は追加のフィールドを表示します。

8. 必要に応じて、承認タスクおよび承認者を特定します。

CA Identity Manager はワークフロー プロセスを禁止アイデンティティ ポリシーに関連付けます。

使用事例: 役職の承認

Forward, Inc には、すべてのマネージャは正規従業員でなければならないというポリシーがあります。しかしながら、Forward, Inc は最近、特別プロジェクトのために多くの契約社員を雇用しました。これらの特別プロジェクトを能率的に運営するために、数人の契約社員にはマネージャの役職が与えられます。Forward, Inc は、管理者が契約社員にマネージャの役職を割り当てる前に、人事担当者からの承認要求を行いたいと考えています。

このような状況で承認プロセスを自動化するため、Forward, Inc は「契約社員のためのマネージャの役職」という名前の禁止アイデンティティ ポリシーを作成します。これは、ユーザの役職がマネージャで、ユーザの組織が「契約社員」の場合に検出を行います。また、Forward, Inc は「ユーザの変更」タスク上でポリシーベースの承認プロセスを設定します。この承認プロセスは、従業員ポリシー用のマネージャの役職に違反した場合にトリガされます。

管理者が契約社員の役職をマネージャに変更する場合、CA Identity Manager は警告メッセージを表示し、作業アイテムを人事担当者へ送信して承認を求めます。CA Identity Manager は、作業アイテムが承認されるまで、契約社員の役職を変更しません。

この使用事例をサポートする設定を行うには、CA Identity Manager で以下の手順を完了させます。

- 以下が設定されている従業員用に、「マネージャの役職」と名づけられた禁止アイデンティティ ポリシーを作成します。
 - ポリシー条件: 次の条件を満たすユーザ (Title = "Manager" and Organization = "Contractor")
 - ポリシー適用時のアクション: 「マネージャは正規従業員でなければいけません」というメッセージによる警告。
- 「ユーザの変更」タスクを変更し、以下に設定されたワークフロー プロセスを含めます。
 - ワークフロー プロセス: ポリシー ベース
 - 承認ルール オブジェクト: アイデンティティ ポリシー違反
 - アイデンティティ ポリシー: 次の条件を満たす (Name = "Manager Title for Contractors")
 - ワークフロー プロセス: SingleStepApproval

アイデンティティ ポリシーおよび禁止アイデンティティ ポリシーの統合

アイデンティティ ポリシーおよび禁止アイデンティティ ポリシーを統合して、職務分掌 (SOD) 要件に対応できます。この場合、アイデンティティ ポリシーは既存の SOD 違反に対処し、禁止アイデンティティ ポリシーは新しい違反を禁じます。

この使用事例をサポートするため、2 種類のアクションを持つアイデンティティ ポリシー セットを設定します。

- ユーザの同期中に発生するアクション

これらのアクションの結果、ユーザ属性、グループおよびロール メンバ、管理者、または所有者が変更されます。たとえば、このタイプのアクションは、違反が検出されるとユーザをロールから削除する可能性があります。

これらのアクションは、禁止アクションとは異なり、タスクのサブミット時に適用されません。適用されるのは、[ユーザの同期](#) (P. 496) 中のみです。

- 禁止アクション

これらのアクションは、タスクがサブミットされる *前* の禁止アイデンティティ ポリシー違反の発生時に、CA Identity Manager が何をするかを決定します。CA Identity Manager はタスクによるサブミットの許可、警告発行およびワークフロー プロセスのトリガ、またはタスクによるサブミットの防止などができます。

これらの各事例では、違反は監査データベースに記録されます。

ユーザが人事管理者と給与承認者のロールを同時に持つことを防ぎたい企業について考えてみます。この企業は 2 つの [ポリシー適用時のアクション] アクションを持つアイデンティティ ポリシーを作成します。

- 給与承認者のロールからのユーザの削除

このアクションは、CA Identity Manager がアイデンティティ ポリシーを持つユーザと同期すると発生します。

この事例では、企業は [ユーザの変更] タスク用のユーザの同期を設定しています。管理者がユーザを変更する場合、CA Identity Manager はすべての適用可能なアイデンティティ ポリシーを評価してアクションを適用します。この例では、CA Identity Manager は人事管理者ロールおよび給与承認者ロールを持つユーザを、給与承認者ロールから削除します。

- タスクの拒否

この禁止アクションは、管理者にタスクのサブミットを許可しないことによって、管理者がこれら 2 つのロールを個人に割り当てることを禁止します。

注: 両方のタイプのアクションを持つアイデンティティ ポリシーを設定する場合、アクションが競合しないことを確認してください。たとえば、ユーザがマネージャおよび契約社員ロールを持つことを防止するアイデンティティ ポリシーを設定します。ポリシーで2つのアクションを特定します。

- ロールを割り当てる前に承認を要求する、ワークフロー プロセスをトリガする警告、および
- ユーザをマネージャ ロールから削除するアクション

承認者はマネージャおよび契約社員ロールのロール割り当てを承認しますが、2つめのアクションでは、ユーザの同期が発生するとマネージャ ロールからユーザを削除します。

第 16 章: Policy Xpress

このセクションには、以下のトピックが含まれています。

[Policy Xpress の概要](#) (P. 517)

[ポリシーの作成方法](#) (P. 518)

Policy Xpress の概要

Policy Xpress を使用すると、カスタム コードを開発しなくても、CA Identity Manager に複雑なビジネス ロジック（ポリシー）を作成することができます。ただし、Policy Xpress ポリシーの作成に関する概念は複雑で、注意深く計画する必要があります。CA Identity Manager ポータル画面を使用する管理者は、Policy Xpress でポリシーを設定して、非常に高度なビジネス ロジックが必要な場合でも実装することができます。ビジネス ポリシーが変更された場合、管理者は CA Identity Manager の設定画面を使用してポリシーを変更することが可能なため、開発者によるコード変更の必要がなく、さらに、適切な変更管理手順に従っていれば CA Identity Manager サービスの再起動も必要ありません。

注: Policy Xpress の詳細については、[Policy Xpress Wiki](#) を参照してください。

ポリシーの作成方法

Policy Xpress を使用してポリシーを作成するには、ポリシーについて次の基本要素を定義します。

プロファイル

ポリシーのタイプと優先度を定義します。管理を簡単にするために、類似のポリシーをグループ化することができます。

イベント

ポリシーを実行するタイミングを定義します。

注: イベント パラメータは注意して設定してください。ビジネス ロジックは、データが破損しないよう、またパフォーマンスが向上するように、特定の時間に実行する必要があります。たとえば、ユーザを有効に設定するのは、ユーザを作成したタイミングで行います。このロジックを任意のタイミングで実行すると、無効にしなければならないユーザアカウントがもう一度有効になってしまう可能性があります。別の例として、ユーザにプロビジョニング ロールを定義し、これによって、あるシステムに対するアクセス権をユーザに付与する場合があります。このロールを割り当てる場合は 対象のユーザに別のロールが割り当てられ承認された後で行う必要があります。Policy Xpress では、カスタム アダプタとほとんど同じように、イベントおよびビジネス ロジック タスク ハンドラの処理中に、ビジネス ロジックを有効にすることができます。つまり、アイデンティティ ポリシーとは異なり、ロジックは、タスクの最初だけでなく任意のタイミングでトリガすることができます。

データ(データ エlement)

ポリシーで使用するデータを指定します。すべてのタイプのビジネス ロジックでは、対象となるいくつかのデータが必要です。このデータを使用して意思決定を行ったり、より複雑なデータを作成したりします。Policy Xpress には、データを収集するための個別のコンポーネントが多数用意されています。これらのコンポーネントはデータ エlement と呼ばれます。データ エlement の例として、ユーザの属性値があります。たとえば、Policy Xpress はユーザの名前を収集して、それを後で使用するためにデータ エlement として格納できます。

エントリ ルール

実行する前に、満たさなければならない要件を定義します。エントリ ルールを定義すると、Policy Xpress がポリシーを評価するタイミングを指定できますが、これによってポリシーが簡潔になり、パフォーマンスが向上します。エントリ ルールの例として、名前または姓が変わった場合のみ、「Set Full Name」ポリシーを実行する、というものがあります。

アクション ルール

収集した情報に基づいて行うアクションを定義します。たとえば Policy Xpress は、ユーザの部門名に基づいて、ユーザをさまざまなロールに割り当てたり、さまざまなアカウント値を割り当てたりすることができます。

アクション

実行するアクションを指定します。Policy Xpress はプロセスの最後に、ビジネス ロジックで必要なアクションを実行します。Policy Xpress は、アクション ルールを複数のアクションに割り当てることによって動作します。つまり、ルールの条件が満たされた場合にアクションが実行されます。アクションには、属性値をユーザまたはアカウントに割り当てる、コマンド ラインを実行する、SQL コマンドを実行する、新しいイベントを生成する、などがあります。

プロファイル

Policy Xpress ポリシーの [プロファイル] タブには、ポリシーを管理し、ポリシーの機能を定義するためのフィールドがあります。

注: ポリシーは、自身が作成された環境にのみ適用されます。たとえば、netauto 環境にログインしている間にポリシーを作成した場合、そのポリシーは netauto 環境でのみ作用します。

ポリシーを作成する場合には、次のプロファイル情報を提供します。

ポリシー名

ポリシーについて一意の名前を定義します。

ポリシー タイプ

ポリシーをトリガする [リスナ](#) (P. 521) を定義します。各ポリシー タイプには、それぞれ異なる設定が 1 つあります。

注: 一度ポリシーを保存すると、このフィールドは変更できません。

カテゴリ

関連するポリシーのグループを定義します。このフィールドでは、管理を簡単にするために複数のポリシーをグループ化することができます。

説明

ポリシーの説明を指定します。

優先度

1 つのイベントで実行するポリシーが複数ある場合には、このフィールドで、ポリシーを実行するタイミングを指定します。ポリシーは、自身の優先度に基づいて実行されます。番号が小さいほど、優先度が高くなります（優先度 1 が最初に実行され、優先度 10 が 2 番目、50 が 3 番目、というふうになります）。

優先度を設定することは、互いに依存しているポリシーに有用です。また、複雑な 1 つのポリシーを 2 つのシンプルなポリシーに分けて順次実行させる場合にも役立ちます。

たとえば、データベース内に特定の値があった場合に実行する 3 つのポリシーがあります。各ポリシーが、データベースの値を確認するのではなく、他の 3 つのポリシーの前に実行する 1 つのポリシーを作成して、この値をチェックできます。新しいポリシーが、要求された値を満たしている場合、Policy Xpress は変数を設定できます。他の 3 つのポリシーは、この変数が設定されている場合にのみ実行され、これによってデータベースへの冗長なアクセスが回避されます。

Enabled

CA Identity Manager 内でポリシーが有効かどうかを表します。ポリシーを削除せずに無効にしたい場合は、このチェック ボックスをオフにすることができます。

一度実行

ポリシーを一度だけ実行するかどうかを指定します。ポリシーには、基準を満たすたびに実行する必要があるものと、一度だけ実行すればよいものがあります。この値によって、すでに実行されたアクションルールをもう一度実行する必要があるかどうかが決まります。

たとえば、部門に基づいてユーザに SAP のロールを追加することは、ユーザがその部門に初めて一致したときのみ実行するアクションです。また、役職に基づいてユーザに給与レベルを設定するポリシーは、不正な変更が生じないように、「一度実行」するようには設定しません。

注：[一度実行] オプションはオブジェクトに適用されるもので、グローバルには適用されません。

リスナ

Policy Xpress のポリシーは、システム内で発生した事象によってトリガされます。この機能を実現するために、イベントが発生すると、システムを統合しているリスナが Policy Xpress に通知し、発生したイベントの詳細情報を提供します。

次のリスナを使用できます。

イベント

システム内のすべてのイベント、およびそのイベントに関連付けられているすべての状態（以前、承認、拒否、など）についてリスンします。このリスナは、Policy Xpress に対してイベントの名前もレポートします。イベントリスナでは、次の状態を使用できます。

- 以前
- 拒否
- 承認済み

- 以降
- 失敗

UI

同期されている状態では、ユーザがタスクに対してユーザ インターフェイスをオープンにしている間、システム内で実行中のさまざまなタスクをリスンします。UI リスナについては、次の状態を使用できます。

- 開始 - タスクを開始するとき
- 対象の設定 - プライマリ オブジェクトが見つかったとき
- [変更時に検証](#) (P. 523) - [変更時に検証] フラグが設定されている属性が変わったとき
- サブミット時に検証 - サブミット ボタンをクリックしたとき
- サブミット - タスクをサブミットしたとき

ワークフロー

承認者が見つかったワークフロー プロセスをリスンします。このリスナは、承認者に電子メールを送信するなど、承認者に基づいてロジックを実行する場合に便利です。

サブミットされたタスク

サブミットされたけれども、バックグラウンドで実行されていないタスクをリスンします。このリスナは、イベント リスナに似ていますが、タスクのイベントではなく、タスク全体で考えます。サブミットされたタスクのリスナでは、次の状態を使用できます。

- タスク開始
- タスク完了
- タスク失敗時

逆同期

CA Identity Manager の検索機能に関連する通知をリスンします。

画面上の属性検証

定義されているトリガ（ポリシー タイプ）の他に、Policy Xpress では属性についての検証をリスンすることもできます。これにより、「変更時に検証」としてフラグが設定されている画面上の属性が更新されたときに実行されるポリシーを作成することができます。

この機能を使用して、従属するドロップダウン リストを作成できます。たとえば、画面上に 2 つのドロップダウン リストがあった場合、最初のドロップダウン オプションが選択されたときに Policy Xpress が実行され、最初に選択されたオプションに基づいて、2 番目のドロップダウン リストの値が設定されます。表示数に制限のないドロップダウン リスト、および他の画面も更新することができます。これは「セレクト ボックス データ」とは異なり、静的オプションを含む XML ファイルをインポートする代わりに、何らかのロジックを使用してドロップダウン オプションに値を挿入できます。

他の使用方法として、1 つの属性の値に基づいて他の属性に値を読み込む場合があります。たとえば、管理者がある部門を選択したときに、Policy Xpress が、部門のマネージャ、部門番号、HR Dept Code などの他の属性の値を自動的に読み込むことができます。これにより、ロジカル アトリビュート ハンドラのカスタム コードを記述する必要がなくなります。

Policy Xpress ポリシーを使用して検証を設定する方法

1. ユーザ コンソールで、タスクのプロファイル画面を変更し、リスンしたいフィールドを選択します。
2. フィールドのプロパティにアクセスし、「変更時に検証」のドロップダウン リストで「はい」を選択します。
3. Policy Xpress で、タイプが「[UI](#) (P. 521)」のポリシーを作成します。
4. 「実行開始イベント」タブで、「状態」として「変更時に検証」を選択し、ステップ 1 で変更したタスクを選択します。

ユース ケース: 有害な名前についてチェックする

新しいユーザを作成したときに、その名前が有害でないかチェックしたい場合があります。次のプロセスは、Policy Xpress のポリシーを使用して、有害な名前についてチェックする方法を概説しています。

1. 「ユーザの作成」タスクのプロファイル画面で、該当するフィールドの「変更時に検証」が「はい」に設定されていることを確認してください。
2. Policy Xpress で、タイプが「UI」のポリシーを作成します。
3. 「実行開始イベント」タブで、「状態」として「変更時に検証」を選択し、「ユーザの作成」タスクを選択します。

4. 名前をチェックするために、次のデータ エLEMENTを作成します。
 - 名前の属性を取得する（[属性]、[ユーザ属性]、[取得]）。
 - 名前をすべて小文字にして解析する（[全般]、[文字列パーサ]、[小文字へ]）
 - データベース テーブル内の有害な言葉に対して名前をチェックする（[データ ソース]、[SQL クエリ データ]）
5. 姓をチェックするために、ステップ 4 と類似したデータ エLEMENTを作成します。
6. 次のようにアクション ルールを作成します。
 - 条件 - 名前が "" と等しくない（クエリで、名前が有害であるというメッセージを返す場合に、この条件が当てはまる）
 - アクション - 有害な名前であることを示す（メッセージ、画面メッセージ）を表示する。

このルールにより、ユーザはユーザの作成タスクをもう一度サブミットする前に、名前を強制的に変更させられます。
7. 姓をチェックするために、ステップ 6 と類似したアクション ルールを作成します。

イベント

[プロファイル] タブで選択したポリシー タイプによって、有効化時間を設定して、ポリシーを評価するタイミングを確立することができます。たとえば、タイプが [イベント] のポリシーについて、**CreateUserEvent** の「前」に評価するよう設定することができます。タイプが [タスク] のポリシーについて、**DisableUserEvent** の「対象の設定」で評価するよう設定できます。

有効化時間を設定するには、次のフィールドを選択します。

State

ポリシーを有効にするイベントに関連する期間またはアクションを指定します。たとえば、ポリシーに、イベントが発生する「前」に実行するよう設定することができます。

イベント名

ポリシーを有効にするイベントを指定します（**CreateUserEvent** など）。

1つのポリシーは、1つ以上の有効化時間を持つことが可能です。システム内で、指定された有効化時間（状態およびイベント）が生じるたびに、Policy Xpress は、その有効化時間を持つすべてのポリシーを検索し、順序に基づいて各ポリシーを評価します。

注: あるポリシーが、システム内で発生した有効化時間に一致しても、そのポリシーが自動的に実行されるわけではありません。プロセスにおいて後で評価されるルール基準によって、ポリシーが完了しているかどうか判断されます。

データ エレメント

データ エレメントは、ポリシー データを作成するために使用します。1つのポリシーには、ポリシーで使用する情報を表す複数のデータ エレメントを含めることが可能です。

Policy Xpress は、データ エレメント情報を収集するために柔軟なプラグインを使用します。各プラグインは、専用の小さいタスクを実行できます。ただし、いくつかのプラグインをまとめて使用して、より複雑なポリシーを作成することができます。データ エレメントのプラグインの例として、ユーザの属性エレメントがあります。エレメントの目的は、ユーザのプロファイルの一部である、特定の属性に関する情報を収集することです。

データ エレメントは、コールされたときに計算されます。つまり、ルールがそのデータ エレメントを使用している場合、または計算が必要な他のエレメントがパラメータとしてそのデータ エレメントを使用している場合です。たとえば、SQL クエリのデータ エレメントはテーブルから値を取得できますが、クエリを作成するにはユーザの部門が必要です。このような場合には、SQL クエリのデータ エレメントの前に部門のデータ エレメントを実行する必要があります。次に、[その値をパラメータとして使用することができます](#) (P. 527)。

次のフィールドがデータ エレメントを定義します。

Name

データ エレメントを説明する、わかりやすい名前を定義します。データ エレメントには複雑なものもあります（変数を取得する、データベースから情報を取得するなど）。データ エレメントの管理を簡潔にするために、意味のある名前を選択してください。

[Category]

データ エレメントのグループ化を提供します。このフィールドはデータ エレメントを並べ替えて、簡単に選択できるようにします。

Type

データ エLEMENTのタイプを指定します。それぞれについて、専用の用途があります。このフィールドは、選択したカテゴリをベースにしています。

機能

同じデータについて、考えられるバリエーションを定義します。大半のデータ エLEMENTは、**Get** 関数のみサポートしています。

たとえば、ユーザ属性のデータ エLEMENTには次の関数があります。

- **Get** - 属性の値を返します。
- **is multi valued** - 値が複数值の場合に **true** を返します。
- **is logical** - 値がロジカルの場合は **true** を返します。

関数の説明

関数の説明を、事前に定義します。選択された各関数について、使用方法、およびどのような値が返されるかをわかりやすくするために、個別の説明を提供します。

パラメータ

データ エLEMENTへ渡すパラメータを定義します。データ エLEMENTは動的なもので、パラメータに基づいてさまざまな処理を行うことができます。ユーザ属性のデータ エLEMENTは、選択された属性に基づいてさまざまな結果を返します。サブタイプ オプションも、パラメータの数、パラメータの名前、および使用できる場合のオプションの値を定義します。

必要に応じてパラメータを追加できます。**SQL** クエリの例では、必要な2つのパラメータとして、データ ソースとクエリ自身を受け取ります。クエリでは、「?」を使用して実際の値と置き換えることができます (**prepared statement** と非常に似ています)。パラメータを追加すると、これらの値を設定できます。

注: Policy Xpress でデータ エLEMENTを表示すると、「使用中」というタイトルの列があります。この列のチェックマークは、データ エLEMENTが、ルール、アクションパラメータ、または他のデータ エLEMENTのパラメータとして使用されていることを意味します。

データまたはアクションのエLEMENTにおける動的な値の使用

動的な値は、計算されたデータ ELEMENTの結果として生じるもので、これらの値は実行時に初めて決定されます。これらの値を、他の（優先度に基づいて、それ以降に計算される）データ ELEMENTのパラメータとして使用することができます。

データ ELEMENTのパラメータとして動的な値を使用する方法

1. [ポリシー データ] タブで、動的な値を設定したいパラメータを見つけます。
2. 空のテキスト フィールドで、通常の何らかのテキストを入力するか、右側のドロップダウン リストから動的な値を選択します。
3. [OK] をクリックします。

変数

Policy Xpress には、アクションに設定される変数が用意されています。この変数はデータ ELEMENT（カテゴリは変数）として保存されます。変数は、同時に実行するすべてのポリシーで共有されるため、設定されている 1 つの変数を、優先度の低い他のポリシーで使用することができます。

たとえば、変数には、あるポリシーでいったん計算された値を含めることが可能で、この変数を他のポリシーで共有することにより、他のポリシーで値を再計算する必要がなくなります。最初のポリシーは値に変数を設定し、後で実行するポリシーは、この変数名を持つデータ ELEMENTをパラメータとして使用して、値を読み込みます。

変数は、他のポリシーに対するトリガとして使用することもできます。このような場合には、前のポリシーが実行されるまで、対象のポリシーを実行できません。

エン트리 ルール

エン트리 ルールは、ポリシーを実行するタイミングについての条件を定義します。これらの条件では、ポリシー内でデータ ELEMENTが収集した値を使用します。

1 つのポリシーには複数のエン트리 ルールを含めることが可能で、1 つのエン트리 ルールに複数の条件を定義することも可能です。少なくとも 1 つのエン트리 ルールが一致する必要があります。つまり、ポリシーがアクション ルールに進むためには、エン트리 ルール内のすべての条件が一致する必要があります。

次のフィールドで、エントリ ルールを定義します。

名前

エントリ ルールについて、わかりやすい名前を定義します。

説明

エントリ ルールの意味を定義します。

条件

一致する基準を指定します。

注: エントリ ルールの複数の条件には、必ず条件の間に **AND** 演算子があります。

詳細情報:

[条件](#) (P. 528)

条件

条件はエントリ ルールとアクションルールで使用されるもので、以下のコンポーネントから構成されています。

- ポリシー データ
- オペレータ
- 値

たとえば、ユーザの部門が変わったかどうかをチェックする条件を作成するとします。最初に、**Department Changed** というデータ エレメントを定義し、次に条件で、「**Department Changed** (変更された部署)」というデータ エレメントを選択し、演算子として [等しい] を選択して値に [TRUE] を設定します。

詳細情報:

[エントリ ルール](#) (P. 527)

[アクションルール](#) (P. 529)

アクション ルール

アクションルールの構造はエントリ ルールに似ていますが、機能の点では異なります。アクションルールは、アクションを実行するタイミングを定義します。たとえば、あるユーザの部門が「販売」に変ったときにポリシーでアクションを実行する場合には、「**Department = Sales**」の場合を定義するアクションルールを作成します。

また、1つのエントリ ルールを一致させる代わりに、いくつかのアクションルールの一致させることもできます。最も高い優先度（0が最高）を持つアクションルールのみが使用されます。

アクションルールには、1つ以上のアクションが含まれており、それらのアクションは「追加アクション」と「削除アクション」に分けられます。

次のフィールドでアクション ルールを定義します。

名前

アクションルールについて、わかりやすい名前を定義します。一意の名前を指定する必要があります。

説明

アクション ルールの意味を定義します。

条件

一致する基準を指定します。

優先度

いくつかのアクションルールが一致した場合に、どのアクションルールを実行するかを定義します。このフィールドは、デフォルトのアクションを定義する場合に有用です。たとえば複数のルール（1つの部門ごとに1つのルール）がある場合は、条件がなく、優先度の低い（他のルールが5の場合は10など）ルールを追加することによって、デフォルトを設定できます。部門のルールがいずれも一致しない場合は、デフォルトのルールが使用されます。

追加アクション

ルールが一致したときに、実行するアクションのリストを定義します。たとえば、ユーザの部門が、条件で設定された部門と一致した場合に特定の **Active Directory** グループを追加する、というルールを設定できます。アクションルールの動作は、[一度実行] の設定に基づいて変わります。一度実行するようにポリシーを設定すると、ルールが初めて一致したときに、関連するアクションが実行されます。それ以降のルールが一致しても、アクションが再度実行されることはありません。前述の例では、**Active Directory** グループがユーザに一度だけ追加されます。[一度実行] が設定されていない場合は、ルールが一致するたびにアクションが実行されます。このフィールドは、値を強制的に設定する場合に重要です。

削除アクション

ルールが一致しない場合に実行するアクションのリストを定義します。たとえば、前述の例では、部門に基づいて、**Active Directory** グループをユーザに追加しました。部門が変わると、削除アクションによって、**Active Directory** グループが削除されます。

詳細情報:

[条件](#) (P. 528)

アクション

アクションは、すべての意思決定が終了した後で、ビジネス ロジックを実行します。アクションは、最後を除いて、データ エlement と同等の方法で機能します。アクションを実行すると、値を返す代わりにタスクが実行されます。

注: アクションは、ユーザ コンソールに表示される順序で実行されます。

次のフィールドでアクションを定義します。

アクション名

アクションの目的を定義します。

カテゴリ

アクションのグループ化を提供します。このフィールドによりアクションが並べ替えられ、選択が簡単になります。

タイプと関数

実行するアクションのタイプと関数を定義します。

注: タイプと関数の詳細については、「データ」を参照してください。

関数の説明

関数の説明を、事前に定義します。選択された各関数について、使用方法、およびどのような値が返されるかをわかりやすくするために、個別の説明を提供します。

パラメータ

アクションへ渡すパラメータを定義します。

フロー制御

デフォルトでは、ポリシーは優先度の順に並べ替えられて、1 つずつ評価されます。このフローはほとんどの場合に適用されますが、必要に応じて変更することができます。

このフロー変更の機能は、すべてのアクション ルールに割り当てることが可能な 1 つのアクションとして表現されます。フロー変更の機能は、アクションの [システム] カテゴリにあります。

重要: プロセス フローを変更する場合には注意してください。これらのアクションを使用すると、無限ループが生じることがあります。たとえば、あるアクション ルールについて「現在のポリシーのやり直し」を条件なしで設定すると、このルールは常に **true** になり、ポリシーは常に再実行されて終わることがありません。

フロー制御の機能として、次の 4 つを使用することができます。

処理の停止

現在のポリシーの後、すべてのポリシーを無効にして、Policy Xpress を終了します。

注: 終了するのは Policy Xpress だけです。CA Identity Manager も強制的に終了させる場合は、例外タイプのアクション プラグインを使用することができます。

すべてのポリシーの再実行

残りのポリシーの処理を停止し、リストの最初に戻ります。このオプションは、あるポリシーのアクションによって、そのポリシーの前にチェックされ実行されなかった別のポリシーがエントリ基準を満たすようになった場合に有効です。このポリシーは、再評価されます。

現在のポリシーのやり直し

ポリシーを再実行します。このオプションは、反復して使用すると便利です。たとえば、一意のユーザ名を作成する場合には、一意の名前を見つけるまでポリシーを何度も実行する必要があります。

特定のポリシーに移動

このアクションでは、現存するポリシーを 1 つ選択する必要があります。このポリシーが現行のポリシーと一緒に（順番は前でも後でも可）実行されている場合、**Policy Xpress** は、選択されたポリシーへジャンプします。新しいポリシーの優先度が低い場合は、現行のポリシーと選択されたポリシーとの間にあるすべてのポリシーが無視されます。新しいポリシーの優先度が高い場合は、プロセスが前に戻ります。

注: アクションによって、**Policy Xpress** が特定のポリシーをスキップすることもあるため、このアクションタイプを使用する場合は注意してください。

アカウントに関連付けられたオブジェクトの設定

追加アクションを作成して、[次のメンバ] のようにアカウントに関連付けられたオブジェクトを設定する場合、特定のリレーションシップ形式を使用してオブジェクトが表示されます。次の 2 つのタイプの形式で、CA Identity Manager のオブジェクトを表すことができます。

- **Active Directory** グループなどのオブジェクトとアカウント間のシンプル リレーションシップを表すには、以下の手順に従います。
NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server

- **SAP** ロールなどのオブジェクトとアカウント間のバインディング リレーションシップを表すには、以下の手順に従います。
{ "validFromDate": "2009¥/12¥/01", "roleName": "SAPRole=SAP_AUDITOR_ADMIN, EndPoint=sap_endpoint, Namespace=SAPR3, Domain=im, Server=Server", "validToDate": "2009¥/12¥/31" }

シンプル リレーションシップとは違い、バインディング リレーションシップではオブジェクトとアカウント間の関連付けに追加データがあります。前の例では、パラメータ **validFromDate** および **validToDate** はアカウントと SAP ロール間の関連付けに関するデータのみを含んでいます。**validFromDate** および **validToDate** データはアカウント、またはロール オブジェクトには存在しません。

リレーションシップの形式を識別するには、オブジェクトの値を取得するデータエレメントを作成します。返される値は、その機能属性を設定するために、追加アクションで使用する形式です。

例: Active Directory グループ

1. 次の設定を使用して Policy Xpress のポリシーを作成します。
 - ポリシー タイプ： イベント
 - イベント： 以降 - ユーザの変更
2. アクションルールで、次の追加アクションを設定します。
 - カテゴリ： 属性
 - タイプ： アカウント データの設定
 - 関数： 設定
 - エンドポイント タイプ： Active Directory
 - エンドポイント： *endpoint_name*
 - アカウント名： *account*

- 属性：次のメンバ（groupMembership）
- 値：
NativeGroup=Administrators,Container=BuiltIn,Endpoint=*endpoint_name*,Namespace=ActiveDirectory,Domain=im,Server=Server

詳細設定

Policy Xpress では、設定について多くのバリエーションを持つこと、および外部のコンポーネントとやりとりすることが可能です。この柔軟性によって、データソースが正しく設定されていない、動的なデータエレメントから不明な値が返された、他方のエンドポイントが応答しない、などの必ずしもバグではないエラーが生じることがあります。

通常はエラーが発生すると、システムが現行のステップについてポリシーの計算を停止します。ただし、エラーのカテゴリに基づいて、エラー時のデフォルトの応答を変更することができます。たとえば、あまり重要ではないポリシーについては、エラーの場合に処理を続行するよう定義できます。

「詳細設定」タブでは、必要に応じてエラー時のデフォルトの応答を変更できます。

注：これらのエラーの応答はデフォルトのままにしておくことを推奨していますが、高度なユースケースの場合には、ポリシーごとにこれら設定を変更することができます。たとえば、あまり重要ではないポリシーについては、ポリシーでエラーが発生した場合に処理を続行するよう定義できます。

以下のエラーカテゴリをそれぞれのタブで設定できます。

- 検証 - プラグインに対して不正な情報が提供されたときに、発生します。このタイプのエラーは、アクションが試行される前にレポートされます。
- 環境 - SQL プラグインに対してデータベース サーバで障害が発生したなど、環境の問題が生じた場合に発生します。
- 許可 - あまり重要でないエラー。このタイプのエラーのデフォルトの動作として、電子メールの送信に失敗した場合など、要求の処理を続行します。

これらの各エラーについて、次のオプションを設定できます。

- イベントの失敗 - 現行のアクションを停止する。これは、ほとんどのタイプのエラーのデフォルトです。
- ポリシーの失敗 - 現行のポリシー、およびそれに関連するすべてのアクションを停止する。残りのポリシーは処理を続行します。
- 無視 - すべての障害が記録されるが、アクションまたはポリシーは停止しない。

第 17 章: CA Identity Manager モバイル アプリケーション

CA Identity Manager モバイル アプリケーションでは、既存の CA Identity Manager インフラストラクチャを活用して、スマートフォンやタブレットなどのモバイルデバイスで以下のタスクを行うことができます。

- 忘れたパスワードのリセット
- パスワードの変更
- 承諾または拒否することで、承認リクエストに応答します。リクエストの保留または解放のいずれかに、ユーザ コンソールを使用します。
- ユーザ情報の表示

この機能を使用すると、ユーザが組織内の他のユーザに関する情報を表示できます。たとえば、作業アイテムの承認者は、承認決定を下す前に、名前やアドレスなどのユーザのマネージャに関する基本情報を参照できます。さらに詳しい情報が必要な場合、承認者は、リンクをクリックして完全なプロフィールを参照できます。

このセクションには、以下のトピックが含まれています。

[CA Identity Manager モバイル アプリケーション アーキテクチャ](#) (P. 538)

[実装プロセスのしくみ](#) (P. 542)

[アプリケーション設定の仕組み](#) (P. 543)

[ユーザ登録の仕組み](#) (P. 543)

[モバイル アプリケーションのサポート用に CA Identity Manager を設定する方法](#) (P. 544)

[モバイル アプリケーションの設定](#) (P. 555)

[追加のプロパティの設定](#) (P. 558)

[モバイル アプリケーションのダウンロード](#) (P. 560)

[モバイル アプリケーションのトラブルシューティング](#) (P. 561)

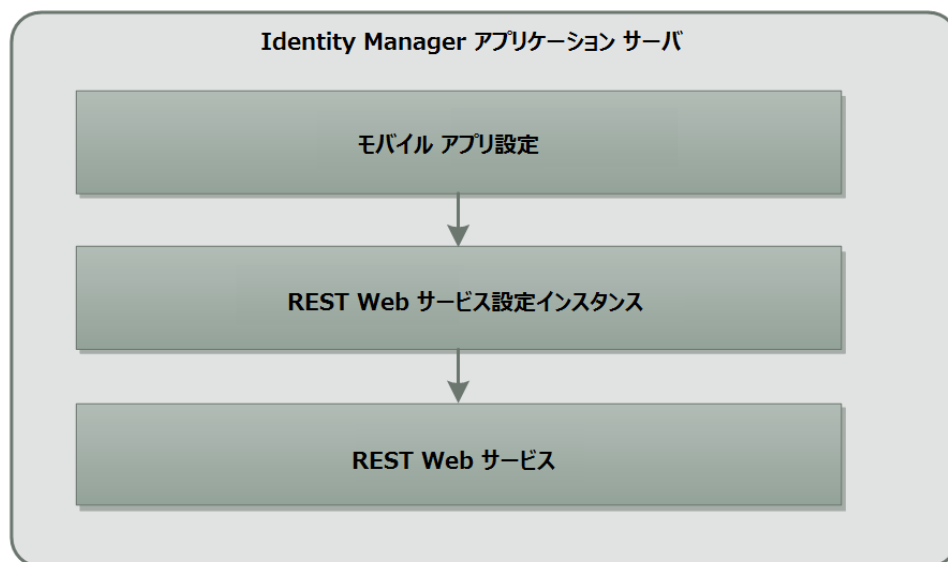
CA Identity Manager モバイル アプリケーション アーキテクチャ

CA Identity Manager モバイル アプリケーション アーキテクチャは、スマートフォンやタブレットなど様々なモバイルデバイスに対して CA Identity Manager の機能セットを提供するように設計されています。モバイルアプリケーション用に選択された機能は、クリティカルなビジネス ニーズおよび、それらの機能がユーザが小型デバイスで操作するのに適切かどうかに基づいています。

そのアーキテクチャは、CA Identity Manager のサーバ機能を使用するアプリケーションおよび RESTful Web サービス固有の設定コンポーネントの使用にフォーカスしています。CA Identity Manager サーバは、指定された環境のモバイルアプリケーション設定を管理する機能、およびアプリケーションによって使用される REST Web サービスの設定をサポートします。

注：REST Web サービスは CA Identity Manager モバイル アプリケーション固有で、SOAP ベースのタスク実行 Web サービス（TEWS）とは異なり、パブリック API として使用することを意図したものではありません。

REST Web サービスは、CA Identity Manager 環境（IME）ごとに複数の設定をサポートできます。ここで、各設定は通常、モバイルアプリケーションなどの特定の REST クライアントと関連付けられます。高レベル アーキテクチャ、およびモバイルアプリケーション設定と Web サービス設定の関係を以下に示します。



REST Web サービス設定では、モバイルアプリケーションが機能するために選択された特定のオプションのセットが必要です。 Web Service 設定を、モバイルアプリケーション設定（管理タスクでも使用可能）を作成する前に、Web サービス設定タスクを介して定義する必要があります。

モバイルアプリケーション Web サービス設定の詳細

REST Web サービス設定は、以下の要素で構成されています。

- 一意の設定名、識別子および有効なフラグを定義するプロファイル
- SSL、ペイロード暗号化および暗号化鍵の使用を定義するセキュリティ設定。
- REST を介して各タイプに対してサポートされる、管理対象オブジェクトタイプ、操作、および属性のセット。
- パスワードのリセットや許可されているユーザセルフサービス属性にセットなどの、サポートされているセルフサービス操作。
- 設定された REST 操作の呼び出しをユーザが許可されているメンバポリシー。

以下のテーブルは、Web サービス設定の詳細、およびモバイルアプリケーションで必要な設定を示しています。

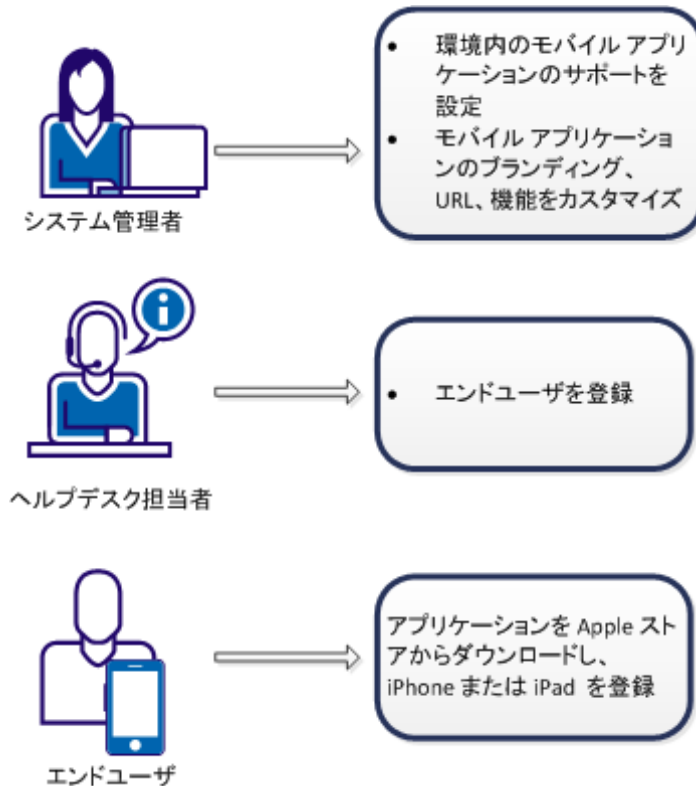
設定セクション	アイテム	説明	モバイルアプリケーション設定
プロファイル	名前	設定の名前	展開の選択
	識別子	各 CA Identity Manager サーバリクエストの "設定 -Id" http ヘッダで指定されたクライアントが設定する必要がある一意の識別子。	展開の選択。 モバイルアプリケーション設定サービスは、以降のすべての REST リクエストで使用する必要がある識別子を返します。
	Enabled （有効）	設定を有効/無効にします	True
セキュリティ	安全な通信が必須	https が必要かどうか	展開の選択。 モバイルアプリケーション設定サービスによってダウンロードされる値。

	暗号化の有効化	SSL を使用しない場合のペイロードを暗号化に使用されます。クライアントサイドの暗号ライブラリ、暗号化キーに関する知識、および明示的なクライアントサイドの暗号化/復号化サポートが必要です	使用されません。チェック マークはオフのままにします。
	設定の秘密情報	サーバ信頼モデルへの REST クライアントの一部として必要な共有される秘密情報。	指定される必要があります。設定インスタンスを定義する際に、展開によって秘密情報が生成される必要があります。
オブジェクト タイプ	オブジェクト タイプ	REST リソースとして表示されるオブジェクトタイプ。	ユーザオブジェクトタイプ
	メソッドおよび属性	選択されたオブジェクトタイプに対してサポートされているリソースメソッド (CRUD)、およびそれらのメソッドに対して許可されている属性のセット。	展開固有のユーザスキーマに示されているような、以下の属性に対する表示アクセス権限があるユーザオブジェクトタイプ。 ■ 職場電話 ■ 部門 ■ 電子メール ■ 名 ■ 姓 ■ マネージャ ■ オフィス ■ タイトル

自己管理	メンバールール	どのユーザが自己管理を実行できるか示すルール。	モバイルアプリケーション設定のメンバールールと一致する必要があります。 変更用の属性のセットは空である必要があります。
	パスワードリセットを有効化	ユーザが自分のパスワードをリセットできるようにします	有効
	属性	ユーザが自分で管理できる属性のセット	空のリスト
メンバ	メンバ	この設定に対して定義されている REST 操作を呼び出す権限がユーザに与えられるルールを定義します	モバイルアプリケーションユーザのセットに一致するメンバールール

実装プロセスのしくみ

モバイルアプリケーションのセットアップには、3種類のユーザが関係しています。以下の図は、これらのユーザの種類と、実行するタスクを示しています。



エンドユーザがモバイルアプリケーションで **CA Identity Manager** を使用できるようにするには、以下を行います。

1. システム管理者は、環境内のモバイルアプリケーション用サポートを以下のように設定します。

設定には、以下のアクティビティが含まれます。

- アクティベーションの設定とコード属性のリセット
- モバイル ユーザ登録用のタスク、Policy Xpress ポリシーおよび電子メールテンプレートの追加
- Web サービス定義の作成
- 登録電子メールの変更。

また、システム管理者は、モバイル ユーザがアクセスできる、ブランド、URL、および機能も設定します。

- ヘルプデスク技術者などの管理者は該当するエンドユーザをユーザコンソールで登録します。

登録処理を行うと、ユーザのアクティベーションコードがトリガされ、コードと登録方法を指示する電子メールが各ユーザに自動的に送信されます。

- エンドユーザは、電子メールに示された指示とコードを使用して、モバイルアプリケーションを Apple ストアからダウンロードし、スマートフォンやタブレットなどのデバイスを登録します。

エンドユーザは、モバイルアプリケーションを使用して CA Identity Manager の機能にアクセスできます。

注: [パスワードの変更が必要] オプションがユーザ作成中に選択された場合、モバイルアプリケーションユーザはアクティベーションを完了できません。

アプリケーション設定の仕組み

モバイルアプリケーションは CA Identity Manager サーバ設定 API からその設定を取得します。モバイルアプリケーションがまずインストールされ、設定がダウンロードされていない場合、アプリケーションはユーザにユーザ名とパスワードの入力を促し、それらの認証情報を使用して、ユーザ登録電子メールで提供されるリンクから定義された設定をダウンロードします。

設定の初回ダウンロード後、アプリケーションが起動されるたびに、その設定バージョンが CA Identity Manager サーバで利用可能な最新バージョンと比較されます。設定バージョン確認 API は、新しいバージョンが利用可能かどうか検出するために使用されます。

ユーザ登録の仕組み

モバイルアプリケーションへアクセスするユーザはそれぞれ、CA Identity Manager 内でアクセスをリクエストする必要があります。アクセスが承認されると、ユーザはアクセスが許可されたことを示すアクティベーションコードで更新されます。モバイルアプリケーション設定メンバポリシーおよびその基礎となる Web サービスメンバポリシーは、アクセスをリクエストするモバイルユーザに対して定義されるいかなる基準でも満たす必要があります。最低でも、[登録済み] の %ACTCODE% 値または「0」より大きな値を定義する必要があります。

ユーザのモバイルアクセスが削除されると、CA Identity Manager サーバはアクティベーション属性をリセットし、モバイルアプリケーションへのユーザアクセスを阻止します。

モバイル アプリケーションのサポート用に CA Identity Manager を設定する方法

モバイル アプリケーションは、パスワードと承認を管理するために **CA Identity Manager** と通信します (REST Web サービスを使用して)。通信を有効にするには、システム管理者が以下の手順を完了する必要があります。

1. [必要な属性を設定します](#) (P. 545)。
2. [管理タスクをインポートします。](#) (P. 548)
3. [Web サービスを作成します](#) (P. 550)。
4. [登録電子メールを変更します](#) (P. 552)。
5. 必要に応じて、モバイル アプリケーションに対して **SiteMinder** サポートを設定します。

必要な属性の設定

モバイルアプリケーションを介したユーザの登録およびアクセスを有効にするために、CA Identity Manager ユーザストアに以下の既知の属性を含める必要があります。

- **%ACTCODE%** -- ランダムに生成されたアクティベーション番号を格納する属性を特定します。ユーザの登録後は、この属性には「Registered」という語が入ります。
- **%ACTCODEVAL%** -- 登録時にクライアントが設定するアクティベーションコードを格納する属性を特定します。CA Identity Manager は、この値を %ACTCODE% の値と比較します。
- **%CURRENT_AUTH_QUESTIONS%** -- 一時的にチャレンジ質問値を格納する属性を識別します。この値は、ユーザ応答の後に正しくクリアされます。
- **%MOBILE_PIN%** -- 暗証番号または文字列値を格納する属性を識別します。これは、システムに対するユーザの認証に使用できる、ユーザとシステムの間で共有される英数字のパスワードを指定します。
- **%PWRESETCODE%** -- 暗号化されたコードを格納する属性を特定します（パスワードリセット時に 1 要素認証を指定します）

これらの既知の属性は、ディレクトリ設定ファイル（**directory.xml**）で利用可能なユーザストア属性にマップします。利用可能な属性がない場合は、ユーザストアスキーマを拡張します。スキーマを拡張する詳細については、お使いのユーザストア用のドキュメントを参照してください。

属性の説明に以下のデータ分類を含めます。

<DataClassification name="sensitive"/>

タスク画面、監査レコード、システムログでリセットコード値をワイルドカード文字に置換します。

重要: %ACTCODE% 属性定義に機密データ分類を含めないでください。機密属性を含めた場合、モバイルアプリケーションは正しく動作しません。

<DataClassification name="AttributeLevelEncrypt"/>

定義された暗号化キーを使用して、ユーザストアから書き込まれたり読み取られたリセットコード値を暗号化および復号化します。

<DataClassification name="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。

注: これらの既知の属性のサンプルについては、このトピックの終わりを参照してください。

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ます。
2. ディレクトリを選択し、モバイル ユーザを含むディレクトリをクリックします。
3. ディレクトリをエクスポートします。
4. 既知の属性 `%ACTCODE%` を含めるように属性の説明を追加または変更します。
利用可能な任意の属性を既知の `%ACTCODE%` にマップできます。
5. 手順 4 を繰り返して、既知の属性 `%ACTCODE%` を定義します。以下のデータ分類を含めます。
`<DataClassification name="sensitive"/>`
`<DataClassification name="ignore_on_copy"/>`
`<DataClassification name=" AttributeLevelEncrypt"/>`
6. 以下のデータ分類を含め、既知の属性 `%CURRENT_AUTH_QUESTIONS%` に対して属性の説明を追加します。
`<DataClassification name="ignore_on_copy"/>`
7. 既知の属性 `%MOBILE_PIN%` の属性説明を追加します。以下のデータ分類を含めます。
`<DataClassification name="sensitive"/>`
`<DataClassification name="ignore_on_copy"/>`
`<DataClassification name=" AttributeLevelEncrypt"/>`
8. 既知の属性 `%PWRESETCODE%` の属性説明を追加します。以下のデータ分類を含めます。
`<DataClassification name="sensitive"/>`
`<DataClassification name="ignore_on_copy"/>`
`<DataClassification name=" AttributeLevelEncrypt"/>`
9. `directory.xml` ファイルを保存します。
10. 管理コンソールのディレクトリのプロパティページで[更新]をクリックし、保存された `directory.xml` ファイルをロードします。

サンプル

注: 利用可能な任意の属性を、これらの既知の属性にマップできます。

%ACTCODE%

```
<ImManagedObjectAttr
  physicalname="attribute_name"
  displayname="your_attribute_display_name"
  description="your_attribute_description"
  valuetype="String"
  required="false"
```

```
multivalued="false"
wellknown="%ACTCODE%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

%ACTCODEVAL%

```
ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%ACTCODEVAL%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

%CURRENT_AUTH_QUESTIONS%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%CURRENT_AUTH_QUESTIONS%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
```

%MOBILE_PIN%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
```

```
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%MOBILE_PIN%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

%PWRESETCODE%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%PWRESETCODE%"
maxlength="0"
hidden="true"
system="true">
  <DataClassification name="ignore_on_copy"/>
  <DataClassification name=" AttributeLevelEncrypt"/>
</ImsManagedObjectAttr>
```

管理タスクのインポート

モバイル ユーザが **CA Identity Manager** にログインできるようになるには、管理者がユーザ コンソールで登録する必要があります。登録処理はアクティベーションコードを生成し、モバイル ユーザに電子メールを送信します。

これらのアクティビティをサポートするには、以下の機能を環境に追加するローカル定義ファイルをインポートします。

- モバイル設定タスク
- モバイル アプリケーションへのユーザの追加および削除タスク
- アクティベーションコードを生成し、ユーザ アカウントからモバイル クライアントの登録を解除する **Policy Xpress** ポリシー。
- モバイル ユーザに電子メールを送信するための電子メール テンプレート

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ます。
2. 環境を選択し、モバイル アプリケーションをサポートさせる環境をクリックします。
3. ロールとタスクの設定を選択し、次の画面で [インポート] をクリックします。
4. [MobileApp-RoleDefinitions] を選択し、[完了] をクリックします。
5. 環境を再起動します。
6. システム管理者ロールに以下のタスクを追加します。
 - モバイル設定の作成
 - モバイル設定の変更
 - モバイル設定の表示
 - モバイル設定の削除
 - モバイル アプリケーションへのユーザの追加
 - モバイル アプリケーションからのユーザの削除

新しいタスクは [ユーザ] および [システム] のカテゴリにあります。

Web サービス設定の作成

モバイル アプリケーションは、REST Web サービスを使用して、CA Identity Manager と通信します。モバイル アプリケーションをサポートするには、システム管理者がユーザ コンソールを使用して Web サービス定義を作成します。

注: Web サービス設定で暗号化が有効な場合、REST コールは動作しません。

次の手順に従ってください:

1. システム管理者権限を持つユーザとしてユーザ コンソールにログインします。
2. 以下のように Web サービス定義を作成します。
 - a. [システム] - [Web サービス] - [Web サービス設定の作成] に移動します。
 - b. [プロファイル] タブで、以下のフィールドに入力します。
 - 名前: 任意の名前。例: RestMobile。
 - 識別子: 一意の識別子。デフォルト値は RestMobile です。
[識別子] フィールドの値は、モバイルアプリケーション設定の **restid** の値と一致する必要があります。
セキュリティを向上するため、識別子と **restid** の値を変更することを検討してください。
 - 属性の有効化: このチェック ボックスをオンにします。

c. [セキュリティ] タブで、以下のフィールドに入力します。

- [安全な通信が必須] オプションを選択する必要があるかどうか判断します。

注: モバイル アプリケーションの http トラフィックをすべて暗号化することを検討してください。通常、このトラフィックの設定には 2 通りの方法があります。

- プロキシ サーバの使用: このユース ケースでは、CA Identity Manager サーバはファイアウォールの後ろに置かれます。プロキシ サーバから CA Identity Manager サーバへの通信をセキュリティ保護しないことを選択できます。ただし、モバイル アプリケーションとプロキシ サーバ間の http 通信を確実にする必要があります。このユース ケースについては、[安全な通信が必須] を選択しないでください。

注: CA Identity Manager と SiteMinder を統合しない場合は、[安全な通信が必須] オプションを選択して、Web サービス コールに対する SSL 通信が残るようにしてください。

- CA Identity Manager サーバを直接使用: このユース ケースでは、モバイル クライアントは CA Identity Manager サーバと直接通信します。この場合の http 通信は暗号化する必要があります。この要件を適用するには、[安全な通信が必須] オプションを選択します。
- [暗号化の有効化] が選択されていないことを確認します。

注: 暗号化が有効な場合、ユーザ詳細はモバイル アプリケーションに表示されません。

d. [オブジェクト タイプ] タブで、ユーザを参照し、[ユーザ] を選択して [編集] ボタンをクリックします。

e. [表示アクセスを許可] のみを選択します。

[変更アクセスを許可]、[作成アクセスを許可]、[削除アクセスを許可] オプションをオフにすることにより、その他のアクセス権限を削除します。

- f. [自己管理] タブで、以下の手順を実行します。
 - [メンバールール] の下の [追加] ボタンを選択し、メンバールールを作成して [すべて] を指定します。

注: 1つのメンバールールのみを作成できます。
 - パスワードリセットを有効にし、モバイル アプリケーションでのパスワード変更機能をサポートします。
- g. [メンバ] タブで、以下の条件のメンバールールを作成します。
 - アクティベーション コード = 登録済み、または
 - アクティベーション コード > 0
- h. Web サービスをサブミットして保存します。

登録電子メールの変更

モバイル設定オブジェクトの URL を含めるように、デフォルトの登録電子メールを編集します。

次の手順に従ってください：

1. ユーザ コンソールで、[システム] - [電子メール] - [電子メールの変更] を選択します。
2. モバイル アプリケーション電子メール用に登録されたユーザを検索し、選択します。
3. [コンテンツ] タブで、HTML ソースを切り替えるボタンをクリックします。
4. mobileregservidm の href エントリにモバイル設定オブジェクトの URL を以下のように指定します。

```
<a  
href="mobileregservidm://{Attribute:%ACTCODE%}'&https://FQN/iam/im/ws  
/Alias/mobile/ConfigName">
```

FQN

CA Identity Manager サーバの名前または IP アドレスを指定します。

Alias

環境の名前を指定します。

ConfigName

設定オブジェクトの名前を指定します。

5. [サブミット] をクリックします。

モバイルアプリケーションのサポート用に SiteMinder を設定する方法

モバイルアプリケーションによって使用される Web サービスは、HTTP AUTHORIZATION ヘッダまたは SiteMinder 認証を介してモバイルアプリケーションによって渡されるユーザ名/パスワード認証情報を使用して、ネイティブ認証をサポートできます。Web サービス設定は、以前説明したように、REST リソースおよびメソッドリクエストのそれぞれに対する許可ポリシーを定義します。

IM REST Web サービス URL

IM REST Web サービスは、以下のベース URL に依存します。

`http[s]://[FQN]/iam/im/ws/[エイリアス]`

- FQN - ユーザの CA Identity Manager サーバアクセス ポイントの完全修飾名およびポート
- エイリアス - 接続先の CA Identity Manager 環境のパブリック エイリアス。

モバイルアプリケーション設定 URL

モバイルアプリケーション設定には、モバイルアプリケーション設定のダウンロードに必要なブートストラップ設定情報の取得を許可する特定の URL が含まれています。この設定 URL は以下のとおりです。

`http[s]://[FQN]/iam/im/ws/[エイリアス]/mobile/[設定名]`

設定名 - モバイルアプリケーション ユーザの指定されたセットの CA Identity Manager 環境用のモバイルアプリケーション設定の名前。設定名は、ユーザのモバイルアプリケーションアクセス リクエストの承認次第送信される登録電子メールに記載されている設定 URL へのリンクを介して、アプリケーションに通知されます。

認証されていない REST API

設定 API

以下の設定 API は認証を必要としません。

`http[s]://[FQN]/iam/im/ws/[エイリアス]/mobile/[設定名]/image`

`http[s]://[FQN]/iam/im/ws/[エイリアス]/mobile/[設定名]/ver`

パスワードのリセット API

`https://[FQN]/iam/im/ws/[エイリアス]`

`/myself/resetpasswordWithResetCodeAndToken`

注: `resetPasswordWithResetCodeAndToken` API には、モバイルアプリケーションから http ヘッダで渡されるセキュリティ トークンが含まれています。CA Identity Manager サーバは、これらのトークンの存在および妥当性を確認します。

CA Identity Manager アクセスを保護するために SiteMinder と統合する場合、これらの URLS は、保護されていないか、匿名の認証方式で保護されているレلمで定義できます。

認証された REST API

以下の URLS はモバイル アプリケーションによって使用され、認証が必要で、Web サービス設定ポリシーを許可に使用します。

Configuration

`http[s]://[FQN]/iam/im/ws/[エイリアス]/mobile/[設定名]/conf`

セルフ サービス ユーザ

`http[s]://[FQN]/iam/im/ws/[エイリアス]/myself`

ワークリスト

`http[s]://[FQN]/iam/im/ws/[エイリアス]/worklist`

ユーザ

`http[s]://[FQN]/iam/im/ws/[エイリアス]/mo/User`

モバイル アプリケーションの設定

システム管理者は、ユーザ コンソールで **CA Identity Manager** のモバイル アプリケーションを設定します。

環境には複数のモバイル アプリケーション設定を含めることができます。別々の設定を作成すると、異なるタイプのモバイル ユーザに対して異なるブランドまたは機能をサポートできます。たとえば、パスワードを変更できる従業員用の設定と、作業アイテムを承認できる管理者用の設定を別々に作成できます。

管理者は、モバイル アプリケーションの以下のプロパティを設定できます。

- ブランド

モバイル アプリケーションの会社ロゴを指定します。

- 機能

以下の機能を有効にします。

- パスワードを忘れた場合のサポート
- パスワード変更のサポート
- ワークフロー承認キュー
- マネージャ リンクの表示

- サポート情報

- 属性マッピング

ユーザ ストアの属性と、モバイル アプリケーションに表示される属性をマップします。

次の手順に従ってください：

1. モバイル設定タスクを使用できるユーザとしてユーザ コンソールにログインします。
2. [システム] - [モバイル設定] - [モバイル設定の作成] をクリックします。
3. デフォルトのオブションを受け入れ、[モバイル設定] タイプの新しいオブジェクトを作成します。
4. [全般] タブで、必須フィールドに入力します。モバイルアプリケーション用の画像を指定できます。

ベース URL

現在の環境のベース URL を確認します。モバイル設定を作成する場合、ベース URL は自動的に入力されます。

CA Identity Manager は、ベース URL を使用して、サーバ名、ポート、およびプロトコルを取得します。モバイル アプリケーションは、これらを使用して、REST コール用の URL を構築します。

設定

設定を参照するか、一意の設定名を入力します。

バージョン

設定を変更または保存するたびに、バージョン番号が増加します。

モバイル アプリケーションはバージョン番号を使用して、新しい設定バージョンをダウンロードするタイミングを決定します。モバイル アプリケーションは、起動すると、サーバにある設定のバージョン番号とロード済みの設定のバージョン番号を比較します。新しいバージョンが使用可能な場合、モバイル アプリケーションは設定を更新します。

注： ファイルを最初に変更した際は、バージョン番号をインクリメントしないでください。

ブランド画像

背景が透明色の PNG イメージの完全な URL を指定します。画像がモバイル アプリケーションの画面の上部に表示されます。

5. [機能] タブで、モバイル アプリケーションの機能を選択します。

パスワードリセットの動作

必須属性の設定時に決定される、動作に使用する方法を選択します。

- デフォルト
- PIN チャレンジ
- QnA チャレンジ

注: [QnA チャレンジ] を選択する場合、[タスク] - [環境管理者] にいってから、[質問と回答の設定] を選択します。[有効化] ボックスがオンになっていることを確認してから、認証用の質問数 (1 ~ 5) を入力し、[サブミット] をクリックします。デフォルト設定に変更を加えなくても、設定が有効になるには [サブミット] ボタンをクリックする必要があります。

6. [サポート] タブで、モバイル ユーザのサポート情報を指定します。
7. [属性マッピング] タブで、モバイル アプリケーション属性を **CA Identity Manager** ユーザストア内の属性にマップします。属性は、物理属性または既知の属性にマップできます。
8. [追加のプロパティ] タブで、モバイル アプリケーションの新しい機能またはフィールドをサポートするための追加のプロパティ値ペアを指定します。
以下の形式を使用します。
Key1=value1
Key2=value2
Key3=value3
注: 管理者が追加のプロパティを追加する必要がある場合は、手順が表示されます。このリリースで、追加のプロパティを指定する必要はありません。
9. [メンバ] タブで、この設定がモバイル アプリケーションに表示されるユーザを決定するルールを指定します。
10. [サブミット] をクリックします。

追加のプロパティの設定

モバイルアプリケーションの設定後、モバイルアプリケーションで新しい機能をサポートするために、必要に応じて追加のプロパティ キー-値ペアを指定できます。これは、[追加のプロパティ] タブを使用して行います。

以下の形式を使用します。

- demoMode="Disable/Enable"
- maxPinRetries=<any positive numerical value>
- multiAccount="Disable/Enable"
- managerTraversal="Disable/Enable"
- startupWithBrandLogo="true/false"

注: 管理者が追加のプロパティを追加する必要がある場合は、手順が表示されます。

ただし、これらの 5 つの機能はモバイル設定でデフォルトで有効になっています。

- **demoMode** : ユーザにモバイルアプリケーションのデモ バージョンの表示を許可します。このオプションはモバイルアプリケーションの[設定]セクションで使用できます。
- **maxPinRetries** : 管理者にモバイル ユーザの間違ったまたは失敗した PIN エントリー試行数の設定を許可します。失敗した試行のデフォルト数は 5 です。
- **multiAccount** : 特にそのアクティベーション コードで複数のモバイル ユーザを追加して、ユーザに複数アカウントの追加を許可します。
- **managerTraversal** : 作業アイテム詳細に承認者およびリクエストのマネージャ詳細を表示します。
- **startupWithBrandLogo** : デフォルトの CA ロゴの代わりに表示されるカスタムアカウント ロゴ (アカウントのブランドイメージ) の指定をユーザに許可します。このキー値が「true」に設定されているが、何らかの理由で、ブランドロゴフィールドが空か URL が無効な場合、起動画面はスタートアップ時に空白のままになります。インストール後にアプリケーションが最初に起動される際に、CA ロゴが常に表示されます。この追加のプロパティはアカウントのデータの部分です。また、初回起動時に利用できるアカウントデータはありません。

注: これらの変更が以降の起動に反映されるのは、CA Identity Manager サーバと正常に通信が行われた後になります。

モバイルクライアントでこれらの機能を無効にするには、[追加のプロパティ] タブの CA Identity Manager モバイル設定で以下のキー-値ペアを追加する必要があります。

- デモ モード機能を有効または無効にする方法
=Enable または =Disable となるように demoMode を設定します
 - demoMode="Disable/Enable"
- maxPinRetries 機能を有効または無効にする方法
任意の正の数値と等しくなるように maxPinRetries を設定します
 - maxPinRetries=<equal any positive numerical value> 失敗試行のデフォルト数が 5 であることに注意してください。
- マルチアカウント機能を有効または無効にする方法
=Enable または =Disable となるように multiAccount を設定します
 - multiAccount="Disable/Enable"
- Manager Traversal 機能を有効または無効にする方法
=Enable または =Disable となるように ManagerTraversal を設定します
 - managerTraversal="Disable/Enable"
- startupWithBrandLogo 機能を有効または無効にする方法
startupWithBrandLogo を [true] または [false] に設定します。
 - startupWithBrandLogo="true/false"

次の手順に従ってください：

1. 管理者（スーパーユーザ）として CA Identity Manager ユーザ コンソールにログオンします。
2. [システム] - [モバイル設定] - [モバイル設定の作成] をクリックします。
3. モバイルアプリケーションの新しい機能をサポートするために、[追加のプロパティ] タブで追加のプロパティ キー-ペアを指定します。
 - demoMode="Disable/Enable"
 - maxPinRetries=<any positive numerical value> 失敗試行のデフォルト数が 5 であることに注意してください。
 - multiAccount="Disable/Enable"
 - managerTraversal="Disable/Enable"
 - startupWithBrandLogo="true/false"

モバイル アプリケーションのダウンロード

モバイル アプリケーションの設定が完了すると、エンド ユーザは、Apple ストアからアプリケーションをダウンロードできます。Apple ストアでモバイル アプリを見つけるには、「CA Identity Manager」を検索します。

その後、エンド ユーザは、電子メールで受信した手順およびコードを使用して、デバイス（スマートフォン、タブレットなど）を登録できます。

モバイル アプリケーションのトラブルシューティング

サポートにログ ファイルを提供します

モバイル アプリケーションで問題が発生した場合、サポート エンジニアはトラブルシューティングに役立てるためにログ ファイルをリクエストする場合があります。

モバイル ユーザは、iPhone または iPad からデバッグを有効化します。デバッグが有効になると、モバイル ユーザは、モバイル アプリケーションを使用してサポートの電子メールアドレス宛にログを送信できます。

モバイル アプリケーションによるログ生成をモバイル ユーザが有効化するには、以下の手順に従います。

1. iPhone または iPad で、[設定] - [Identity Manager] - [デバッグ] に移動します。
2. [有効] をタップします。
3. アプリケーションを再起動し、ログに表示させるアクションを実行します。
4. CA Identity Manager モバイル アプリケーションの [設定] タブで、電子メール ログをクリックします。

モバイル アプリケーションは、ログ ファイルが添付された電子メールを作成します。ユーザ コンソールでサポート用に設定した電子メールアドレスに電子メールが送信されます。

Identity Manager タスクの環境管理者が、[質問と回答の設定]設定を使用して、[パスワードのリセット動作]としての[QnA]に失敗する。

問題の状況

デフォルトの [質問と回答の設定] 設定で [パスワードのリセット動作] として [QnA] を選択すると、パスワードのリセットが失敗し、以下のエラー メッセージが表示されます。

```
"ERROR [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) Failed to process get user credential questions. Message:java.lang.NullPointerException in the server log file"
```

解決方法:

パスワードのリセット動作として QnA を使用してパスワードのリセット作業を行うには、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 CA Identity Manager にログインします。
2. [タスク] - [環境管理者] に移動してから、[質問と回答の設定] を選択します。
3. [サブミット] ボタンをクリックします。

注：[有効化] オプションおよび [認証用の質問数] のデフォルト値が適用されるのは、この手順の実行後です。

第 18 章: CA User Activity Reporting

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 UAR の機能 \(P. 563\)](#)

[追加の CA UAR レポートまたはクエリと CA Identity Manager との統合 \(P. 574\)](#)

CA UAR の機能

CA User Activity Reporting (CA UAR) が CA Identity Manager と統合されると、以下の機能が有効になります。

- CA UAR エージェントは CA Identity Manager 監査情報を収集し、それを CA Common Event Grammar (CEG) に変換します。
- ユーザ コンソールは CA UAR レポートを取得し、返された情報をフィルタするために使用される CA Identity Manager コンテキスト情報でクエリすることができます。
- CA Identity Manager のリリースには、多くのデフォルト レポート、および、CA UAR のレポートとクエリを既存または新規タスクに追加するためのインフラストラクチャが含まれます。

注: CA UAR は、以前は CA Enterprise Log Manager と呼ばれていました。ユーザ コンソールでは、CA Enterprise Log Manager という名前がまだ使用されている個所があります。

CA UAR コンポーネント

CA Identity Manager が CA UAR と統合されると、以下のコンポーネントが CA Identity Manager アーキテクチャに追加されます。

- [CA ELM ビューア] タブ で、CA UAR オブジェクトを任意の新しいタスクまたは既存タスクに埋め込むことができます。

注: CA UAR サーバ接続が必要です。

- インポート可能なロール定義。

統合の制限

CA UAR との統合の既知の制限を以下に示します。

- タスク設定のためのランタイムでのクエリおよびレポート リスト取得に時間がかかる場合がある。
- CA UAR の API は、Java により指定されたデフォルトのタイム ゾーンのみを認識する。
- 複合フィルタで使用されている場合、EQUAL の操作で大文字小文字が区別される。
- CA UAR サーバへの接続は、同時に 1 つのみサポートされる。

CA UAR と CA Identity Manager の統合方法

CA UAR のレポートおよびクエリを表示し管理できるようにするには、管理者は以下の手順に従う必要があります。

1. CA UAR エージェントをインストールします。
2. コネクタを作成します。
3. CA Identity Manager での監査を有効化します。
4. CA UAR サーバを設定します。

CA Enterprise Log Manager エージェントのインストール前提条件

CA UAR エージェントをインストールする前に、以下の手順に従います。

- CA UAR サーバマシンに、CA Identity Manager を実行している、または CA Identity Manager 監査データベースをホストしているマシンから接続できることを確認します。
- エージェントマシンにサーバマシンから接続できることを確認します。
- エージェントマシン上のデータソースを設定します。
- Adobe Flash Player のバージョンが 9.0.28 またはそれ以上であることを確認します。プレーヤはここからダウンロードできます。
<http://www.adobe.com/go/getflash>
- [エージェントバイナリをダウンロードします。](#) (P. 566)
- [エージェント認証キーを取得します。](#) (P. 566)
- サーバ名/IP にアクセスできるようにします。
- アカウント情報にアクセスできるようにします。ただし、セキュリティが不十分にならないようにします。エージェントは、サービス (Windows) として実行するときこのアカウントを使用します。
- コネクタが存在する場合、デフォルトのコネクタ情報をエクスポートし、すぐに使用できるようにします。
- マシンに 4 GB の RAM が実装されていることを確認します。

エージェントマシン上のデータソースの設定

以下の手順に従って、エージェントマシン上でデータソースを設定します。

データソースの設定方法

1. [コントロールパネル]、[管理ツール]、[データソース (ODBC)] の順に移動します。
2. [System DSN] タブから、以下を追加します。
監査データベースを参照する imsauditevent12 データソース (ODBC)。
3. [適用/OK] をクリックします。
データソースが設定されました。

エージェント バイナリのダウンロード

以下の手順に従って、エージェント バイナリをダウンロードします。

次の手順に従ってください：

1. 以下の URL で CA UAR サーバにログインします。
`https://<host>:5250/spin/calm/CALMSpindle.csp`
2. [管理] - [ログ収集] - [エージェント エクスプローラ] - [エージェント バイナリのダウンロード] - [<OS> バージョン] に移動します。
3. ファイルに保存します。

エージェント認証キーの取得

この手順を使用して、エージェント認証キーを取得します。

次の手順に従ってください：

1. CA UAR サーバで、[管理] - [ログ収集] - [エージェント エクスプローラ] - [エージェント認証キー] に移動します。
2. キーにアクセスできるようにします。ただし、セキュリティが不十分にならないようにします

CA UAR エージェントのインストール

CA UAR エージェントは、イベントの収集と、その情報の CA UAR サーバへの送信を行います。CA Identity Manager データベース サーバあるいはエンドポイントマシン上にエージェントをインストールし、ログ記録を有効にします。

注: CA UAR エージェントは、Windows および Linux でサポートされています。

次の手順に従ってください:

1. データベース サーバ上で `ca-elmagent-<version>.exe` インストールを実行し、以下の情報を指定します。
 - サーバ名または IP アドレス
 - 認証コード
 - エージェント サーバのアカウント情報 (エージェントをサービス/デーモンとして実行するために使用される)
2. デフォルトのコネクタ リスト ファイルが利用可能であれば指定します。
3. 以下の URL で CA UAR サーバにログインします。
`https://host:5250/spin/calm/CALMSpindle.csp`
4. [管理] - [ログ収集] - [エージェント エクスプローラ] - [デフォルト エージェント グループ] に移動します。
5. エージェント マシンを選択し、[ステータスとコマンド] ビューを起動します。

ロール定義のインポート

ユーザ コンソールで Enterprise Log Manager 接続を設定する前に、CA Enterprise ロール定義をインポートする必要があります。

ロール定義をインポートする方法

1. 以下の URL から Management コンソールにログインします。
`http://host:port/iam/immanage`
2. [環境]、[ロールおよびタスクの設定] の順に移動し、[インポート] ボタンをクリックして Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml を選択します。
3. [保存して閉じる] をクリックします。
4. ユニット コンソールの [システム] タブから、[Enterprise Log Manager 接続の設定] をクリックし、必要な情報を入力してから [送信] をクリックします。

新しいコネクタの作成

以下の手順に従って、コネクタを作成します。

次の手順に従ってください：

1. 以下の URL で CA UAR サーバにログインします。
`https://host:5250/spin/calm/CALMSpindle.csp`
2. [管理] - [ログ収集] - [エージェント エクスプローラ] - [デフォルト エージェント グループ] に移動します。
3. エージェント マシンを選択します。
4. コネクタ表示に切り替えます。
5. [コネクタの新規作成] ボタンをクリックして、以下の情報を入力します。

コネクタの詳細

統合タイプに [CAIdentityManager] を選択し、必要に応じてコネクタ名を変更します。

コネクタの設定

接続文字列

- Driver={SQL Server} ; Server=<Auditing DB Server> ; Database=<Auditing DB>
- Driver={Microsoft ODBC for Oracle} ; Dbq=<Auditing DB TNSname>

ユーザ名: **監査するDB ユーザ**

パスワード: **監査するDB ユーザのパスワード**

6. 12.6.4 で使用するために、CA Identity Manager コネクタに対する以下の接続設定変更を適用します。

- ソース名: エージェント マシン上のデータ ソースの名前 -
imsauditevent12
- アンカー SQL: select max(id) from imsauditevent12
- アンカー フィールド: IMS_EVENTID
- イベント SQL:

```
select imsauditevent12.id as IMS_EVENTid ,imsauditevent12.audit_time as  
IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME  
,imsauditevent12.admin_name as ADMINUNIQUENAME ,imsauditevent12.admin_dn as  
ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID  
,imsauditevent12.event_description as  
EVENTINFO ,imsauditevent12.event_state as  
EVENTSTATE ,imsauditevent12.tasksession_oid as TASKOID
```



```
,imsaudittasksession12.task_name as  
TASKNAME ,imsauditeventobject12.object_type as OBJECTTYPE ,  
imsauditeventobject12.object_name as  
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as  
ATTRNAME ,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE  
,imsauditobjectattributes12.attribute_newvalue as  
ATTRNEWVALUE ,imsauditobjectattributes12.attribute_newvalue as ATTRVALUE  
from  
imsaudittasksession12, imsauditevent12, imsauditeventobject12,  
imsauditobjectattributes12 where imsauditevent12.id >? and  
imsauditevent12.tasksession_id = imsaudittasksession12.id and  
imsauditevent12.tasksession_oid = imsaudittasksession12.tasksession_oid  
and  
imsauditeventobject12.parent_event_id = imsauditevent12.id and  
imsauditobjectattributes12.parent_object_id = imsauditeventobject12.id  
ORDER BY  
imsauditevent12.id ASC;
```

7. 保存して閉じます。

コネクタが動作していることを検証する方法

1. [管理] - [ログ収集] - [エージェント エクスプローラ] - [デフォルト エージェント グループ] に移動します。
2. エージェント マシンを選択します。
3. コネクタ表示に切り替え、[ステータスとコマンド ビューの起動] ボタンをクリックします。

ステータスが実行されています。

CA Identity Manager での監査の有効化

CA Identity Manager で監査を有効にする方法

1. 管理コンソールを開きます。

`http://host:port//iam/immanage`

2. [環境] - [<環境>] - [詳細設定] - [監査中] に移動します。

3. 既存の設定をエクスポートし、ファイルを保存します。

4. 保存したファイルに以下の変更を加え、変更を保存します。

- `<Audit enabled="true" auditlevel="BOTH" datasource="java:/auditDbDataSource"`

- 最後の定義済み監査プロファイルの下に、パスワード ポリシー用の監査プロファイルを追加します。

- `<AuditProfile objecttype="FWPASSWORDPOLICY" auditlevel="BOTHCHANGED"/>`

5. ファイルを管理コンソールにインポートして戻し、以下のいずれかを実行して監査情報の集約をトリガします。

- ユーザ管理対象オブジェクト上で実行されるタスク
- グループ管理対象オブジェクト上で実行されるタスク
- パスワード ポリシー管理対象オブジェクト上で実行されるタスク

6. 以下の URL で CA UAR サーバにログインします。

`https://host:5250/spin/calm/CALMSpindle.csp`

7. 既存のレポートを使用するには、[クエリおよびレポート] - [クエリ] - [CA Identity Manager] に移動します。

注: 設定済みの CA UAR サーバが必要です。

8. 実行したタスクによっては、以下のデフォルトのレポートを開いてイベントが予定されていることを検証します。

- ユーザ ID でフィルタされた「CA Identity Manager - システム全イベント」を呼び出す、[システム全イベント (ユーザ別)] タスク
- 「アカウント管理 (ホスト別)」をそのまま呼び出す、[アカウント管理 (ホスト別)] タスク
- 「アカウント作成 (アカウント別)」をそのまま呼び出す、[アカウント作成 (アカウント別)] タスク
- 「アカウント削除 (アカウント別)」をそのまま呼び出す、[アカウント削除 (アカウント別)] タスク
- 「アカウントロックアウト (アカウント別)」をそのまま呼び出す、[アカウントのロックアウト (アカウント別)] タスク

- 「CA Identity Manager - プロセス アクティビティ (ホスト別)」をそのまま呼び出す、[認証プロセス アクティビティ (ホスト別)] タスク
- 「CA Identity Manager - ポリシー変更アクティビティ」タスクをそのまま呼び出す、[パスワードのポリシー変更アクティビティ] タスク

CA UAR サーバの設定

管理する CA UAR サーバを設定する前に、以下の要件を確認します。

- EiamAdmin クレデンシャルを取得していること
- Adobe Flash Player 9.0.28 またはそれ以降のバージョンがインストールされていること

CA UAR サーバが設定されると、以下の機能が使用可能になります。

- 単一の CA UAR サーバまたはフェデレーション階層は、監査イベントを作成する複数の環境を消費できます。
- リモート システムのデータ認証は、CA UAR のデータ アクセス フィルタを使用して実装可能です。

次の手順に従ってください：

1. 以下の URL を使用して、Administrator クレデンシャルで CA UAR サーバの製品登録ページにログインします。

`https://host:port/spin/calmap/products.csp`

2. [Register] ボタンをクリックし、証明書名およびパスワードを入力して、CA Identity Manager 環境を登録します。

注: 各環境にはそれぞれ別の登録ペア（証明書名/パスワード）が必要です。

3. [Administration]、[User and Access Management]、[New Data Access Filter] の順に移動し、フィルタ名を入力します。
4. 次の手順に進みます。
5. [Selected Identities] を [All Identities] のままにして、次の手順に進みます。
6. [New Event Filter] をクリックして、アクセス フィルタを作成します。

CA Identity Manager から収集されたログでは作成された証明書をマシンまたは環境名だけに制限して、Data Access Filter を設定します。また、証明書を管理エンドポイントではネイティブ エンドポイント情報へのアクセスのみに制限することもできます。

7. 保存して閉じます。
8. [Open Access Policies] をクリックして、[アクセス ポリシー] を開きます。
9. [Obligation Policies] を選択して、利用可能な単一のポリシーをクリックします。
10. 「All Identities」を削除し、証明書名を追加します。
11. ポリシーを保存します。
12. CA Identity Manager ユーザ コンソールにログインし、Enterprise Log Management 接続を設定します。

Enterprise Log Manager 接続の設定

この画面を使用して、新しく追加された **CA UAR** 接続タスクを管理します。

この画面には以下のフィールドが含まれます。

接続名

単一の **CA UAR** 接続管理オブジェクトに使用する一意の名前を指定します。

このフィールドは読み取り専用です。

ホスト名(必須)

CA UAR のサーバホスト名または IP アドレスを指定します。

ポート番号(必須)

CA UAR のサーバ接続ポートを指定します。

デフォルト：52520

認証機関によって署名された SSL 証明書

チェックがオンになっている場合には、**CA UAR** サーバへの接続時に、厳格な **SSL** 証明書チェックを指定します。

たとえば、デフォルトで **CA UAR** にインストールされている **SSL** 証明書のような自己署名 **SSL** 証明書がある場合は、このチェックボックスをオフにします。ルート認証局へのトラステッドパスは存在しません。

証明書名(必須)

認証に使用する **CA UAR** 証明書の名前を指定します。

証明書パスワード(必須)

CA UAR パスワードを指定します。

属性

サポート対象外です。バージョンは、接続情報をテストとして保存するために取得します。

Enterprise Log Manager 接続の削除

リストから接続を選択して、[削除]をクリックします。**CA Enterprise Log Manager** 接続タスクが削除されます。

追加の CA UAR レポートまたはクエリと CA Identity Manager との統合

「Enterprise Log Manager ビューア」タブを使用して、追加のレポートまたはクエリを CA Identity Manager に統合することができます。これらの新しいレポートまたはクエリは、（ウィザードも含む）既存のタスクおよび新規タスクと組み合わせることができます。CA UAR フェデレーション データを必要に応じて含めることもできます。「Enterprise Log Manager ビューア」タブを使用して、取得した情報にフィルタを適用できます。フィルタでは以下を使用できます。

- 固定値
- 管理対象オブジェクトの属性
 - たとえば、physical - ::MyPhysicalAttribute::
logical - ::|MyLogicalAttribute|::
- Common Event Grammar（CEG）により記述されている、すべてのフィールド
 - dest_username
 - dest_objectname
 - dest_uid
 - source_username
 - source_objectname
 - source_uid

[Enterprise Log Manager ビューア] タブの設定

以下の 1 つ以上のフィールドを入力して [Enterprise Log Manager ビューア] タブを設定します。

名前

タブに割り当てる名前。

タグ

タスク内で一意なタブの識別子。文字またはアンダースコアで始まり、文字、数字、アンダースコアのみで構成される必要があります。タグは主として、XML ドキュメントまたは HTTP パラメータを通じてデータ値を設定するために使用されます。

タブの非表示

タスク中にタブを非表示にします。このオプションは、タブを非表示にする必要があるが、タブの属性にはアクセスするアプリケーションで役に立ちます。

Enterprise Log Manager クエリ

CA UAR クエリの表示を指定します。

注: [CA Enterprise Log Manager クエリ] または [CA Enterprise Log Manager レポート] のいずれかを指定できますが、両方は指定できません。

Enterprise Log Manager レポート

CA UAR レポートの表示を指定します。

Enterprise Log Manager ID

クエリまたはレポートのいずれかに ID を指定します。

フェデレーション データを含める

フェデレーション データを結果に含めるかどうかを指定します。デフォルトでは、このフィールドはチェック マークがオフになっています。

プロンプトの表示

CA UAR のプロンプト クエリのみを指定します。デフォルトでは、このフィールドはチェック マークがオフになっています。

フィルタ

CA UAR のクエリまたはレポートによって返された結果を絞り込むために使用する、SQL ベースの詳細条件を指定します。定数値や変動値を含めることができます。以下のコードは式のサンプルです。

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username  
EQUAL ::logical.attribute.Y:: ))
```

サポートされている演算子は以下のとおりです。

- equals (EQUAL)
- not equals (NEQ)
- less (LESS)
- greater (GREATER)
- less or equals (LEQ)
- greater or equals (GREATEQ)
- like (LIKE)
- not like (NOTLIKE)
- in set (INSET)
- not in set (NOTINSET)

サポートされている論理演算子は以下のとおりです。

- AND
- OR

丸かっこは必須です。条件式の左側の値の両端にマーカ「::」がないと、その値は定数と見なされ、定数として値が CA UAR に送信されます。

パラメータ/値の表

スコープ用のフィールドおよび値を指定します。

スコーピングのタグおよびタグのロジックに一致するクエリまたはレポートだけが選択されます。

パラメータ

開始、終了、および制限のパラメータの値を指定します。以下のパラメータがサポートされます。

- 時間粒度（トレンドのみ）
- 開始時刻
- 終了時刻
- 最も古いグループ化イベント日付がある（グループ化クエリのみ）
- 最新のグループ化イベント日付がある（グループ化クエリのみ）

- 最新のグループ化イベント日付が前にある（グループ化クエリのみ）
- グループ化での最小イベント数（グループ化クエリのみ）
- グループ化での最大イベント数（グループ化クエリのみ）

第 19 章: アクセス ロール

アクセス ロールは、CA Identity Manager または他のアプリケーションにおける権限付与の追加的な方法を提供します。たとえば、アクセス ロールを使用して以下の処理を実行できます。

- ユーザ属性に間接的なアクセス権を付与する
- 複合式を作成する
- 権限を決定するために他のアプリケーションで使用される、ユーザ プロファイルの属性を設定する

アクセス ロールは、ユーザまたはユーザのグループに一連のビジネス変化を適用するという点でアイデンティティ ポリシーに似ています。ただし、アクセス ロールを使用してビジネス変化を適用すると、アクセス ロールのメンバを表示して、この変化の適用先のユーザを確認できます。

ほとんどの場合、アクセス ロールはタスクと関連付けられていません。

注: CA Identity Manager が CA SiteMinder と統合されると、アクセス ロールは CA SiteMinder によって保護されるアプリケーションへのアクセスも提供できます。この場合、アクセス ロールにはアクセス タスクが含まれます。詳細については、「[設定ガイド](#)」の SiteMinder 統合についての章を参照してください。

このセクションには、以下のトピックが含まれています。

[アクセスロールが権限を管理する方法](#) (P. 580)

[例: 間接的なプロファイル属性の変更](#) (P. 580)

[アクセス ロールの作成](#) (P. 581)

アクセスロールが権限を管理する方法

変化アクションを指定することで、アクセス ロールを使用して権限を管理できます。このアクションは、ユーザーがロールのメンバまたは管理者として追加または削除されたときに発生します。

アクセス ロールを使用する方法

1. 管理者がアクセス ロールを作成します。
2. [メンバ] タブで、管理者は追加または削除アクションを指定します。これにより、ユーザにアクセス ロールが割り当てられるときに **CA Identity Manager** によって実行されるアクションが決定されます。
3. 管理者は必要に応じて管理者ポリシーと所有者ポリシーを指定し、アクセス ロールを作成するタスクを送信します。
4. アクセス ロールの管理者がユーザにアクセス ロールを割り当てます。
5. **CA Identity Manager** が、ロールで指定されたアクション追加を完了します。

例：間接的なプロファイル属性の変更

アクセス ロールを使用して、ユーザ プロファイルの属性を間接的に変更できます。たとえば、企業では自分以外のユーザの役職を直接変更できない場合があります。こうした企業では、管理者がユーザにロールを割り当てたときに役職を変更できるアクセス ロールを作成できます。

属性を間接的に変更するには、アクセス ロールに変更アクションを設定します。管理者がロールを割り当てると、この変更アクションにより、ユーザ プロファイルの属性に 1 つ以上の変更を加えることができます。

アクセス ロールを使用して属性を間接的に変更する方法

1. アクセス ロールを作成します。
2. [メンバ] タブで、[管理者はこのロールのメンバの追加、削除が可能] チェック ボックスをオンにして、矢印アイコンをクリックします。
CA Identity Manager には、[追加アクション] および [削除アクション] フィールドが表示されます。
3. [追加アクション] または [アクションの削除] フィールドで、リスト ボックスからアクションを選択します。
CA Identity Manager には、選択したオプションに基づいた追加フィールドが表示されます。
4. 必要に応じて、[追加] または [削除] アクションを設定します。

5. [管理者] タブを選択して、作成中のアクセス ロールにメンバを追加できる管理者を指定します。
6. [所有者] タブを選択して、アクセス ロールの定義を変更できる管理者を指定します。
7. [送信] をクリックしてアクセス ロールの作成を完了します。
8. 必要に応じてユーザにアクセス ロールを割り当てます。

アクセス ロールの作成

アクセス ロールを作成するには、以下の手順に従います。

- [アクセス ロールの作成の開始](#) (P. 581)
- [アクセス ロールのプロファイルの定義](#) (P. 582)
- [アクセス ロールのメンバ ポリシーの定義](#) (P. 582)
- [アクセス ロールの管理ポリシーの定義](#) (P. 583)
- [アクセス ロールの所有者ルールの定義](#) (P. 583)

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 ロールのプロフィールの定義

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: [プロフィール] 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」](#) (P. 582) 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] タブで以下の手順を実行します。

1. [追加] を選択してメンバ ポリシーを定義します。
2. (オプション) [メンバ ポリシー] ページでは、このロールの使用を許可するメンバルールを定義できます。
これにより、メンバ ポリシーの条件に一致するユーザにこのロールが自動的に割り当てられます。
3. [メンバ] タブにメンバ ポリシーが表示されていることを確認します。
ポリシーを編集するには、左側にある矢印記号をクリックします。削除するには、マイナス符号アイコンをクリックします。
4. [メンバ] タブで、[管理者は、このロールのメンバを追加および削除できます。] チェック ボックスをオンにします。
この機能を有効にすると、[追加アクション] と [削除アクション] を定義します。これらのアクションでは、ロールのメンバとしてユーザが追加または削除されたときに行われる処理が定義されます。
5. 次のセクション [「アクセス ロールの管理ポリシーの定義」](#) (P. 583) に進んでください。

アクセス ロールの管理ポリシーの定義

[管理者] タブで以下の手順を実行します。

1. [管理者の管理] オプションを使用可能にする場合は、[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します。
2. [管理者] タブで、管理ルールとスコープ ルール、管理者権限を含む管理ポリシーを追加します。各ポリシーでは少なくとも 1 つの権限（メンバの管理または管理者の管理）が必要です。
このルールを満たす管理者用に個別のルールや権限を所有する複数の管理ポリシーを追加できます。
3. ポリシーを編集するには、左側にある矢印記号をクリックします。削除するには、マイナス符号アイコンをクリックします。
4. 次のセクション [「アクセス ロールの所有者ルールの定義」](#) (P. 583) に進んでください。

アクセス ロールの所有者ルールの定義

[所有者] タブで以下の手順を実行します。

1. ロールを変更できるユーザを決定する、所有者ルールを定義します。
2. [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。

第 20 章：システム タスク

このセクションには、以下のトピックが含まれています。

[デフォルトのシステム タスク](#) (P. 585)
[フィーダ ファイルでユーザを追加する方法](#) (P. 586)
[「Loader レコード詳細」 タブ](#) (P. 591)
[「Loader アクションマッピング」 タブ](#) (P. 592)
[「Loader 通知詳細」 タブ](#) (P. 593)
[Bulk Loader タスクの変更の認識](#) (P. 593)
[Bulk Loader タスク用電子メール通知の設定](#) (P. 594)
[「Bulk Loader」 タスクのスケジュール](#) (P. 594)
[「Bulk Loader」の解析ファイルの変更](#) (P. 595)
[Bulk Loader の Web サービス サポート](#) (P. 595)
[JDBC 接続管理](#) (P. 596)
[ロジカルアトリビュートハンドラ](#) (P. 596)
[セレクト ボックス データ](#) (P. 600)
[「相関属性の設定」 タスク画面](#) (P. 601)
[グローバル ポリシー ベースのイベント用ワークフローの設定タスク画面](#) (P. 602)
[CA Identity Manager のタスク ステータス](#) (P. 603)
[サブミット済みタスクのクリーンアップ](#) (P. 622)
[反復タスクの削除](#) (P. 627)
[Enterprise Log Manager 接続の設定](#) (P. 628)
[Enterprise Log Manager 接続の削除](#) (P. 629)
[秘密鍵の管理](#) (P. 630)

デフォルトのシステム タスク

CA Identity Manager には、管理者が CA Identity Manager 環境を管理する際に役立つ以下のタスクが組み込まれています。

- 「サブミット済みタスクの表示」 タスク

管理者が使用環境内のタスクのステータスを表示できます。また、古いタスクの削除も「サブミット済みタスクの表示」画面で行います。

- 「Bulk Loader」 タスク

フィーダ ファイルをアップロードします。このファイルは、多数の管理対象オブジェクトを同時に操作する際に使用します。

■ [バルク] タスク

「ユーザ」などのオブジェクトに対して、部署、市区町村、終了日といったオブジェクトの属性に基づいてタスクを実行します。このタスクは、毎週土曜日などに定期的に実行します。

バルク ユーザに変更を加える場合にもこのタスクを使用します。

■ [セレクト ボックス データ] タスク

管理者が、フィールドにオプションを設定するためのファイル（セレクト ボックスなど）を管理タスクにアップロードできます。

■ [ロジカルアトリビュート ハンドラ] タスク

管理者がロジカルアトリビュートを管理できます。ロジカルアトリビュートは、タスク画面で属性（フィジカルアトリビュートと呼ばれる）をユーザにわかりやすい形式で表示する際に使用します。

■ [JDBC 接続管理] タスク

CA Identity Manager にデータベース サーバ接続の詳細情報を設定します。

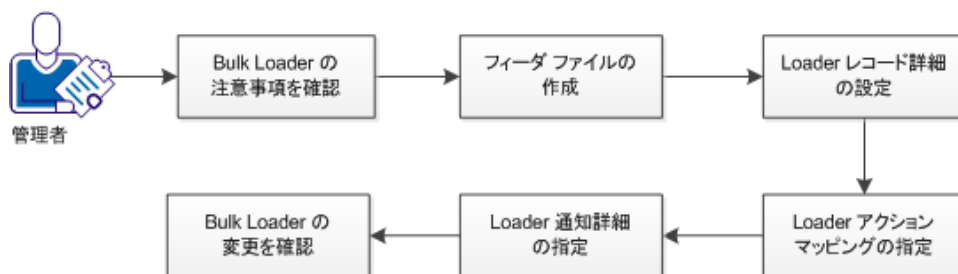
■ [電子メール] タスク

電子メール通知ポリシーを管理します。

フィーダ ファイルでユーザを追加する方法

[Bulk Loader] タブを使用して、同時に多数の管理対象オブジェクトを操作するために使用するフィーダ ファイルをアップロードできます。たとえば、1000 人のユーザをシステム内で手動で作成することもできますが、Bulk Loader を使用して作成することもできます。Bulk Loader タスクは、ワークフロープロセスにマッピングすることもできます。

Bulk Load クライアントはバッチ処理用に存在するコマンドラインユーティリティです。環境が（負荷分散目的で）クラスタ内に存在する場合は、Bulk Load クライアントの使用をお勧めします。Bulk Load クライアントは、プロビジョニングコンポーネント メディア上にあります。



次の手順に従ってください:

1. [Bulk Loader の注意事項を確認します](#) (P. 587)。
2. [CSV または XLS 形式のフィード ファイルを作成](#) (P. 590) し、アップロードします。
3. [Loader レコード詳細を設定します](#) (P. 591)。
このタブでは、フィード ファイルのアクションおよび識別子フィールドを指定することができます。
4. [Loader アクションマッピングを指定します](#) (P. 592)。
このタブでは、プライマリ オブジェクトを選択し、そのオブジェクトのアクションに実行するタスクを指定することができます。
5. [Loader 通知詳細を指定します](#) (P. 593)。
このタブでは、Bulk Loader タスク変更を認証するユーザを選択することができます。
6. [Bulk Loader タスク変更の進捗状況を確認し、変更します](#) (P. 593)。

Bulk Loader に関する注意事項

「Bulk Loader」タブを使用して、同時に多数の管理対象オブジェクトを操作するために使用するフィード ファイルをアップロードできます。Bulk Loader を使用する際は以下の点に注意してください。

- 大量のバルク ロードは、ピーク時以外（夜中など）にスケジュールすることを考慮してください。大量のバルク ロードはパフォーマンスに影響します。多くのサブ タスクが含まれるバルク ロードを実行すると、そのバルク ロードが終了するまで、ユーザがサブミットしたタスクが完了できない場合があります。
- 多数のオブジェクトのアップロードなど、時間のかかるタスクの実行中にサーバがダウンした場合は、「サブミット済みタスクの表示」でタスクを再開できます。タスクが再開される場合、最後に正常に実行されたレコードから開始されます。
- Solaris のユーザ ストアとして LDAP を使用している場合は、インポート中に Bulk Loader が停止する場合があります。この問題を修正するには、「*Configuration Guide*」の「Specify LDAP Connection Settings」トピックを参照し、そこに説明されている設定を適用してください。

- **Bulk Loader** を使用して、多数のユーザをインポートすると、メモリ不足の例外が発生する場合があります。この問題に対処するには、以下のヒープ サイズ メモリ パラメータを調整します。

- `-Xmx`
- `-XX:maxPermSize`

注: メモリ パラメータを調整する方法の詳細については、アプリケーション サーバのドキュメントを参照してください。

- **Bulk Loader** を使用した多数の管理対象オブジェクトの操作（多くのユーザを作成するなど）は、パフォーマンスに影響する場合があります。パフォーマンスを改善するには、以下の推奨事項を考慮します。

- ユーザ コンソール を使用してバルク ロードを行うときは、1つの大きな CSV ファイルを複数の小さなファイルに分割します。たとえば、10,000 ユーザの 10 のバルク ロードの実行は 100,000 ユーザの 1 つのバルク ロードの実行より高速です。

注: 50,000 を超えるエントリを持つ CSV ファイルは、システムの問題を引き起こす可能性があります。

- バルク ロードを実行しているユーザのタスクの数を制限します。たとえば、バルク ロードを開始する管理者が持つタスク数が少なければ、パフォーマンスは改善します。管理者が多くのタスクを持つ場合、**CA Identity Manager** はより広範な権限チェックを実行する必要があり、パフォーマンスに影響します。
- バルク変更に関連付けられている **Policy Xpress** ポリシーの数を制限します。また、複雑なポリシーのようにバルク ロード中時のパフォーマンスに影響しない、シンプルな **Policy Xpress** ポリシーの作成を考慮します。
- 十分なシステム リソースがあることを確認します。

データ検証の制限によるバルク ロードのパフォーマンスの改善

管理タスクには、通常、複数のタブが含まれます。デフォルトでは、バルク操作により、タスクの各タブでデータが検証されます。

この検証により、バルク操作のパフォーマンスが低下する場合があります。検証が不要な場合は、パフォーマンスを改善するために、タスク タブのデータ検証を無効にできます。

次の手順に従ってください：

1. 管理タスクを変更できるユーザとして、ユーザ コンソールにログインします。
2. [タスク] - [ロールおよびタスク] - [管理タスク] - [管理タスクの変更] を選択します。
3. バルク操作で適用されるタスクを検索して、選択します。

4. [タブ] を選択し、変更するタブを選択します。
 5. [バルク操作で検証を実行しない] を選択し、[OK] をクリックします。
 6. データ検証が不要な各タブについて、手順 4 ～ 5 を繰り返します。
 7. [サブミット] をクリックします。
- 変更したタブではデータ検証が無効になります。

カスタム ビジネス ロジックの制限

ビジネス ロジック タスク ハンドラやイベント リスナなどのカスタム ビジネス ロジックをバルク操作で使用するタスクに含めると、パフォーマンスが低下する場合があります。

パフォーマンスを改善するには、バルク ロード操作のカスタム ビジネス ロジックを無効にします。

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. イベント リスナまたはビジネス ロジック タスク ハンドラが含まれる変更対象の環境を選択します。
3. [詳細設定] - [ビジネス ロジック タスク ハンドラ]（該当する場合）を選択します。
4. `UseInBulkOperation` プロパティの値を「false」に設定し、[保存] をクリックします。
5. イベント リスナについて、手順 4 を繰り返します。
6. ビジネス ロジック タスク ハンドラおよびイベント リスナに関する変更を完了したら、環境を再起動します。

フィーダ ファイルの作成

Bulk Loader ファイルの使用により、多数の管理対象オブジェクトに対してアクションが繰り返し自動実行されます。ユーザがフィーダ ファイルをアップロードすると、システムはフィーダ ファイルを解析し、読み取ります。

フィーダ ファイルは拡張子が CSV または XLS で、プロパティが以下のとおりである必要があります。

- このファイルには、管理対象オブジェクトのフィジカル アトリビュート、ロジカル アトリビュートまたは既知の属性の名前を指定するヘッダ行が含まれている必要があります。
- ヘッダ行には、レコードに対して実行されるアクションを示す列が含まれている必要があります。
- フィーダ ファイルの各行を「レコード」と呼びます。レコードには、ヘッダ行によって指定された各属性の値が含まれます。属性に対して使用できる値として以下のオプションがあります。
 - 値 — 属性は指定した値に設定されます。
 - Value;Value;Value;... — 属性は指定した複数值属性に設定されます。
 - '' (空白) — 属性は変更されません。
 - NULL — 属性は削除されます。削除の順序はデフォルトで「NULL」に設定されていますが、[Bulk Loader ファイル アップロード検索] 画面で編集できます。

注: フィーダ ファイルでハッシュ (#) を使用するには、ハッシュ記号を二重引用符で囲みます。たとえば、user#1 は "user#1" と指定します。

重要: フィーダ ファイルは、UTF-8 エンコーディングで保存する必要があります。

ユーザを作成するためのサンプル フィーダ ファイル

このサンプル フィーダ ファイルは、特定の必要な属性を持つユーザを作成します。

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

上記のコードで、フィーダ ファイルのプロパティは以下のとおりです。

ヘッダ

コードの最初の行はヘッダ行です。ヘッダ行には、管理対象オブジェクト「ユーザ」のフィジカルアトリビュートまたは既知の属性が含まれます。

アクション

アクション列では、各レコードに対して実行されるタスクを識別します。たとえば、上記のファイルでは、名「John」に対して「作成」アクションを実行するように指定しています。

ユーザを有効化するためのサンプル フィーダ ファイル

このサンプル フィーダ ファイルは論理属性 `|enabled|` の値を変更します。ヘッダ内の論理属性、およびファイル内の各ユーザ エントリの値（この場合 `true` または `false`）を指定します。

```
action,%USER_ID%,|enable|
```

```
MODIFY,user1,false
```

```
MODIFY,user2,true
```

[Loader レコード詳細] タブ

この [Loader レコード詳細] タブでは、フィーダ ファイルに存在するレコードの簡易プレビューが表示されます。プレビュー テーブルには最大 5 レコードが表示されます。プレビュー テーブルは、正しいファイルをアップロードしているかどうかを確認するのに役立ちます。また、このタブでは、フィーダ ファイルで指定した管理対象オブジェクトに実行するアクションを指定することもできます。以下のフィールドを洗い出し、それらのフィールドに入力する必要があります。

[このオブジェクトに対して実行されるアクションを表しているのは、どのフィールドですか?]

管理対象オブジェクトに実行するアクションを示すフィールドを、フィーダ ファイルから洗い出します。たとえば、`Create`、`Modify`、`Delete` という値を取る 'action' というフィールドがあるフィーダ ファイルを使用できます。これらの各アクションを [\[Loader アクション マッピング \(P. 592\)\]](#) の管理タスクにマップする必要があります。

[オブジェクトの一意な識別に使用されるのはどのフィールドですか?]

プライマリ オブジェクトを一意に識別できるフィールドを、フィーダ ファイルから洗い出します。

注: 無効なヘッダ行がフィーダ ファイルにあると、フィーダ ファイル レコードは [Loader レコード詳細] タブに表示されません。ヘッダー行が無効の場合は、別のフィーダ ファイルを選択してください。フィーダ ファイルに無効なレコードが含まれていると、[システム] タブの下に [サブミット済みタスクの表示] にアップロードの詳細ステータスが表示されます。

[Loader アクション マッピング]タブ

[Loader アクション マッピング] タブでは、フィーダ ファイルで指定されたアクションの実行対象となるプライマリ オブジェクトを選択することができます。また、選択したプライマリ オブジェクトに対するフィーダ ファイル内アクションを管理タスクにマップする必要があります。

プライマリ オブジェクトとは何でしょうか。

フィーダ ファイルを使用して CA Identity Manager によって操作されるプライマリ オブジェクトのことを表します。以下のいずれかのプライマリ オブジェクトを選択できます。

- User
- グループ
- 組織

'action' 用に実行するタスクの選択

フィーダ ファイルが指定した各アクション用に実行する必要がある管理タスク、たとえば [削除] や [変更] タスクを指定します。

注: フィーダ ファイルに記述したすべてのアクションを管理タスクにマップする必要があります。また、このフィールドに表示される管理タスクは、選択したプライマリ オブジェクトに従属します。たとえば、プライマリ オブジェクトとして「ユーザ」を選択していると、「ユーザ」に関連する管理タスクのみが表示されます。

'action' 用の存在しないオブジェクトに対するタスクの選択

管理対象オブジェクトが CA Identity Manager 内にまだ存在しない場合には、フィーダ ファイルが指定したアクション用に実行する必要がある代替管理タスク、たとえば [作成] タスクを指定します。

[Loader 通知詳細]タブ

重要: デフォルトでは、このタブは **Bulk Loader** ウィザードに含まれません。 **Bulk Loader** タスクを変更して **[Loader 通知詳細]** タブを手動で追加する必要があります。また、このタブを使用するには、ワークフローが環境内で有効であることが必要です。

[Loader 通知詳細] タブを使用すると、**Bulk Loader** タスクの認証管理者を選択できます。 **Bulk Loader** タスクが完了したとき、**CA Identity Manager** によって、そのタスク用に設定されたすべての認証管理者向けに **Bulk Loader** 通知が作成されます。この通知は、**[Bulk Loader 通知]** の下の **[ホーム]** タブ内に表示されます。通知をクリックすると、バルク ロード操作で開始されるタスクの詳細が表示されます。認証管理者は、通知に記載された変更点を確認できます。

注: 認証管理者のリストを表示するには、ドロップダウン リストに表示される参加者リゾルバのいずれかを使用します。参加者リゾルバの詳細については、このガイドの「ワークフロー」セクションを参照してください。

Bulk Loader タスクの変更の認識

Bulk Loader 通知には、**Bulk Loader** タスクが開始したすべての変更に関する詳細が含まれます。認証管理者は、**Bulk Loader** タスクによって開始されたすべての変更を確認できます。

Bulk Loader タスク変更を確認して認識する方法

1. **Bulk Loader** タスクの認証管理者としてリストされたユーザとして、ユーザ コンソールにログインします。
2. **[ホーム]** に移動し、**[マイ Bulk Loader 通知の表示]** に移動します。
3. 確認する **Bulk Loader** 通知を選択します。

[Bulk Loader 通知の管理] 画面が表示され、開始された **Bulk Loader** タスク変更をすべてリストした表が表示されます。

この画面から、以下を実行できます。

- 作成または変更オブジェクトの特定のタスク詳細を確認するには、**[説明]** 列の下ハイパーリンクをクリックします。
- コンプライアンス違反がある場合、またはユーザに追加されたロールを削除する場合は、**[ユーザ ID]** の隣にある **[編集]** アイコンをクリックすると、通知画面からユーザを直接編集できます。
- ユーザに追加されたロールを確認するには、**[ユーザ ID]** に関連付けられた **[リクエストされたロールの割り当て]** 列の下ハイパーリンクをクリックします。

4. 特定のオブジェクトの変更をすべて確認したら、そのオブジェクトの [確認] チェック ボックスをオンにします。
5. 変更を確認し終わったら、[確認] をクリックして、選択された変更通知をすべて、リストから削除します。

注: [すべてを確認] を選択すると、Bulk Loader 通知内の変更をすべて確認できます。これにより、[ホーム] タブから Bulk Loader 通知が削除されます。また、[確認] 列の一番上のチェック ボックスをオンにすると、その時点で画面にある変更通知がすべて選択され、変更を画面単位で確認できます。

Bulk Loader タスクに関連付けられたユーザの変更がすべて確認されると、Bulk Loader 通知は [ホーム] タブに表示されなくなります。

Bulk Loader タスク用電子メール通知の設定

環境によっては、バルク操作の電子メール通知がデフォルトで設定されています。バルク操作の電子メール通知がユーザのシステムで設定されているかどうかを確認するには、[システム] - [電子メール] - [電子メールの表示] に移動し、「バルク」という語で検索します。

ユーザの環境で電子メール通知が設定されていない場合は、バルク操作の完了時に送信される電子メールを設定します。

次の手順に従ってください:

1. ユーザ コンソールで [システム] - [電子メール] - [電子メールの作成] をクリックします。
2. [プロファイル] タブの必須フィールドに入力します。
3. [送信のタイミング] タブで、以下の手順に従います。
 - a. 最初のフィールドで [タスク完了時] を選択します。
 - b. 2 番目のフィールドで [Bulk Loader] を選択します。
4. [受信者] と [コンテンツ] タブを入力し、[サブミット] をクリックします。

Bulk Loader タスク用に電子メール通知が設定されます。

[Bulk Loader] タスクのスケジュール

[Bulk Loader] タスクは、システム内でスケジュール設定することができます。
[Bulk Loader] タスクをスケジュールするには、そのタスクに[スケジュールのタブを追加](#) (P. 71) します。

「Bulk Loader」の解析ファイルの変更

フィーダ ファイルの解析に使用するパーサを変更するには、該当する管理タスクを設定します。

Bulk Loader の管理タスクを変更する方法

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの管理] に移動します。
2. [Bulk Loader] タスクを検索します。
3. [Bulk Loader] タスクを選択し、[選択] をクリックします。
4. [Bulk Loader] タスクの [検索] タブを選択します。
5. [参照] をクリックして検索画面を検索します。

利用可能な検索画面のリストが表示されます。

6. 検索画面を選択して [編集] をクリックします。

[検索] 画面の詳細が表示されます。

7. (オプション) [パーサの完全修飾名] を編集します。

[パーサの完全修飾名] は、パーサ ファイル名と一致する必要があります。

注: カスタム CSV パーサの作成の詳細については、FeederParser クラス用の Javadoc を参照してください。アプリケーション サーバとして JBoss を使用し、カスタム パーサを作成する場合は、カスタム パーサ ファイルが `iam_im.ear/user_console_war/WEB-INF/classes` ディレクトリにある必要があります。

8. [OK] をクリックします。

Bulk Loader の Web サービス サポート

Bulk Loader には、CA Identity Manager の Task Execution Web Service (TEWS) インターフェースを使用して呼び出すことができる Web サービス API があります。TEWS では、クライアント アプリケーションがリモート タスクを CA Identity Manager にサブミットして実行できます。このインターフェースは、WSDL および SOAP のオープン標準を実装して、CA Identity Manager へのリモート アクセスを提供します。

CA Identity Manager には、Web サービスとして Bulk Loader への呼び出しの実例を示す Java クライアント サンプルが含まれています。Java サンプルは、以下のソース ファイルにあります。

`admin_tools\samples\WebService\Axis\Optional\ObjectsFeeder.java`

Web サービスとして Bulk Loader を呼び出す方法が記載されたデータ サンプルおよびマニュアルは、以下のディレクトリにあります。

`admin_tools¥samples¥Feeder¥`

注: 詳細については、「Java のプログラミング ガイド」を参照してください。

JDBC 接続管理

CA Identity Manager レポートに関する情報は、複数のソースから得ることができます。各レポートは、レポートで表示させたい情報に基づき、特定のデータ ソースに関連付けられている必要があります。

レポートで使用する他のデータ ソース（監査データベース、またはタスク永続性データベースなど）を確立するには、CA Identity Manager で接続管理オブジェクトを作成します。接続を作成すると、レポートタスクの [検索] タブで、レポートタスクを変更し、[レポート用接続オブジェクト] を設定して、レポートを特定の接続管理オブジェクトに関連付けることができます。

JDBC 接続の作成

CA Identity Manager に接続に関する詳細を設定するには、以下の手順に従います。

JDBC 接続を作成する方法

1. [システム] - [JDBC 接続管理] - [JDBC 接続の作成] をクリックします。
2. 新しい接続オブジェクトを作成するか、特定の JNDI データ ソースに基づいて接続オブジェクトを選択します。
3. 必要なすべてのフィールドに入力して、[送信] をクリックします。

新しい JDBC 接続が作成されます。

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、ユーザーが保存した属性（フィジカル アトリビュートと呼びます）をタスク画面上にわかりやすい形式で表示できます。CA Identity Manager 管理者はタスク画面を使用して CA Identity Manager の機能を実行します。ロジカル アトリビュートはユーザ ストアには存在しません。通常、ロジカル アトリビュートは 1 つ以上のフィジカル アトリビュートを表して表示を簡略化します。たとえば、ロジカル アトリビュートの日付は、月、日、および年のフィジカル アトリビュートを表すことができます。

ロジカルアトリビュートはロジカルアトリビュートハンドラによって処理されます。ロジカルアトリビュートハンドラは、ロジカルアトリビュートAPIを使用して作成されたJavaオブジェクトです（「Javaのプログラミングガイド」を参照してください）。たとえば、タスク画面の場合、ロジカルアトリビュートハンドラによってユーザストアのフィジカルアトリビュートデータがロジカルアトリビュートデータに変換されます。このデータがタスク画面に表示されます。CA Identity Managerにある事前定義されたロジカルアトリビュートとロジカルアトリビュートハンドラを使用することも、ロジカルアトリビュートAPIを使用して新たにロジカルアトリビュートハンドラを作成することもできます。

注: ロジカルアトリビュートの詳細については、「Javaのプログラミングガイド」を参照してください。

ユーザコンソールの[環境]カテゴリには、ロジカルアトリビュートハンドラを管理するためのタスクが含まれています。リストには、CA Identity Managerに付属している事前定義されたハンドラと、組織で定義したすべてのカスタムハンドラが表示されます。

[環境] タスク カテゴリから以下を実行できます。

- CA Identity Managerを使用した新規のロジカルアトリビュートハンドラの作成
- ハンドラのコピー
- ハンドラの削除
- 既存のハンドラ設定の変更

注: ロジカルアトリビュートハンドラの実行順序を変更するには、管理コンソールを使用します。

ロジカルアトリビュートハンドラの作成

ロジカルアトリビュートハンドラの作成方法

1. [システム] - [ロジカルアトリビュート] - [ロジカルアトリビュートハンドラの作成] に移動します。
2. [ロジカルアトリビュートハンドラの作成] 画面で[標準ロジカルアトリビュートハンドラの作成]を選択し、[OK]をクリックします。

3. [ロジカルアトリビュート ハンドラの作成] 画面で、ロジカルアトリビュート ハンドラの設定を行います。

各フィールドの説明については、この画面のヘルプリンクをクリックして参照してください。

4. [サブミット] をクリックします。

このハンドラが[ロジカルアトリビュート ハンドラ] 画面のハンドラ リストに表示されます。

注: ユーザ コンソールを使用してロジカルアトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラのコピー

ロジカル アトリビュート ハンドラをコピーする方法

1. [システム] - [ロジカルアトリビュート] - [ロジカルアトリビュート ハンドラの作成] に移動します。

2. [ロジカルアトリビュート ハンドラの作成] 画面で、[ロジカルアトリビュート ハンドラ定義のコピーの作成] を選択して[検索] をクリックします。

3. ロジカルアトリビュート ハンドラ (ConfirmPasswordHandler など) を選択して、[OK] をクリックします。

4. [ロジカルアトリビュート ハンドラの作成] 画面で、ロジカルアトリビュート ハンドラの設定を行います。

各フィールドの説明については、この画面のヘルプリンクをクリックして参照してください。

5. [サブミット] をクリックします。

このハンドラが[ロジカルアトリビュート ハンドラ] 画面のハンドラ リストに表示されます。

注: ユーザ コンソールを使用してロジカルアトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラ ForgottenPasswordHandler の作成

ロジカル アトリビュート ハンドラ **ForgottenPasswordHandler** では、以下の操作に対して個別のロジカル アトリビュートを使用します。

- 設定
- 実行時の質問と回答

ロジカル アトリビュート ハンドラ ForgottenPasswordHandler の作成方法

1. [システム] - [ロジカル アトリビュート] - [ロジカル アトリビュート ハンドラの作成] に移動します。
2. [ロジカル アトリビュート ハンドラの作成] 画面で [標準ロジカル アトリビュート ハンドラの作成] を選択し、[検索] をクリックします。
3. **ForgottenPasswordHandler** を選択し、[OK] をクリックします。
4. **ForgottenPasswordHandler** の [ロジカル アトリビュート ハンドラの作成] 画面で、ロジカル アトリビュート ハンドラの設定を行います。
各フィールドの説明については、この画面のヘルプリンクをクリックして参照してください。
5. [サブミット] をクリックします。

このハンドラが [ロジカル アトリビュート ハンドラ] 画面のハンドラ リストに表示されます。

注: ユーザ コンソールを使用してロジカル アトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラの削除

ロジカル アトリビュート ハンドラを削除する方法

1. [システム] - [ロジカル アトリビュート] - [ロジカル アトリビュート ハンドラの作成] に移動します。
2. [ロジカル アトリビュート ハンドラの削除] 画面で、削除する各ロジカル アトリビュートの横にあるチェック ボックスをオンにします。
3. [選択] をクリックします。
CA Identity Manager に確認メッセージが表示されます。
4. [はい] をクリックして、削除を確定します。

ロジカル アトリビュート ハンドラの変更

ロジカル アトリビュート ハンドラの変更方法

1. [システム] - [ロジカル アトリビュート] - [ロジカル アトリビュート ハンドラの作成] に移動します。
2. [ロジカル アトリビュート ハンドラの変更] 画面で、変更するハンドラを選択して、[選択] をクリックします。
3. ロジカル アトリビュート ハンドラ (ConfirmPasswordHandler など) を選択して、[OK] をクリックします。
4. [ロジカル アトリビュート ハンドラの変更] 画面で、ロジカル アトリビュート ハンドラの設定を行います。

各フィールドの説明については、この画面のヘルプ リンクをクリックして参照してください。

5. [サブミット] をクリックします。

注: ユーザ コンソールを使用してロジカル アトリビュート ハンドラを設定した後、アプリケーション サーバを再起動する必要はありません。

ロジカル アトリビュート ハンドラの表示

ロジカル アトリビュート ハンドラの表示方法

1. [システム] - [ロジカル アトリビュート] - [ロジカル アトリビュート ハンドラの作成] に移動します。
2. [View Logical Attribute Handler (ロジカル アトリビュート ハンドラの表示)] 画面で、表示するハンドラを選択して、[選択] をクリックします。
3. ロジカル アトリビュート ハンドラのプロパティを参照して、[閉じる] をクリックします。

セレクト ボックス データ

以下のフィールドに使用するオプションを作成できます。

- チェック ボックスの複数選択
- ドロップダウン
- ドロップダウン コンボ
- 複数選択

- オプションセレクト
- オプションセレクト コンボ
- ラジオ ボタン 1つ選択
- 単一選択

これらのオプションはセレクト ボックス データの XML ファイルに格納されます。たとえば、セレクト ボックス データ XML ファイルを使用して、[ユーザの作成] タスクの [プロファイル] タブにある市区町村または都道府県ドロップダウン ボックスのオプションを入力できます。

また、セレクト ボックス データの XML ファイルを使用して、管理タスクの 2 つのフィールド間に依存関係を設定することもできます。たとえば、[市区町村] フィールドに入力可能なオプションを、[都道府県] フィールドでユーザが選択したオプションに依存させることができます。

注: セレクト ボックス データの詳細については、「ユーザ コンソール デザイン ガイド」を参照してください。

[関連属性の設定]タスク画面

このトピックは、CA CloudMinder にのみ該当します。

環境に対する関連ルールを設定するには、[関連属性の設定] タスク画面を使用します。

CA Identity Manager はメモリに設定パラメータを読み込み、定期的にメモリ バージョンを共通 DSA のデータベース バージョンと同期します。関連属性はテナント固有であるため、プロビジョニング サーバは検索および関連付けの操作中に対応するテナント DSA から関連属性を読み取ります。更新された関連ルールは、パラメータの更新時刻を待つことなくすぐに有効になります。

グローバル ポリシー ベースのイベント用ワークフローの設定タスク画面

「グローバル ポリシー ベースのイベント用ワークフローの設定」タスクでは、管理者は現在の環境におけるすべてのイベントのポリシーまたは非ポリシー ベースのワークフローを設定できます。タスクをクリックすると、ワークフロー プロセス定義へのデフォルトのイベント マッピングが表示されます。各イベント マッピングは変更または削除でき、設定されていないイベント用に新しいイベント マッピングを追加できます。

ホーム	ユーザ	組織	グループ	ロールおよびタスク	エンドポイント	ポリシー	電子メール	レポート	システム
タスク									
グローバル ポリシー ベースのイベント用ワークフローの設定									
この環境のイベントに関連するワークフロー プロセス。									
イベント名	ワークフロー プロセス								
AssignAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess								
CertifyRoleEvent	CertifyRoleApproveProcess								
CreateGroupEvent	CreateGroupApproveProcess								
CreateOrganizationEvent	CreateOrganizationApproveProcess								
CreateUserEvent	CreateUserApproveProcess								
DeleteGroupEvent	DeleteGroupApproveProcess								
DeleteOrganizationEvent	DeleteOrganizationApproveProcess								
DeleteUserEvent	DeleteUserApproveProcess								
ModifyOrganizationEvent	ModifyOrganizationApproveProcess								
RevokeAccessRoleEvent	ModifyAccessRoleMembershipApproveProcess								
SelfRegisterUserEvent	SelfRegistrationApproveProcess								
マッピングの新規追加									
イベント AccountChangePasswordEvent									
追加									

この画面のフィールドを以下に示します。

この環境のイベントに関連するワークフロー プロセス。

承認ポリシーに関連付けられたワークフロー プロセスを指定します。

マッピングの新規追加

ワークフロー プロセスにマッピングする承認ポリシーを指定します。

[追加]ボタン

新しいマッピングを追加します。

マッピングを追加または変更することにより、プロセス マッピングおよび承認ポリシーを選択できる「ワークフロー マッピング」画面が開きます。動作はイベント レベルのワークフロー設定と同じです。「ワークフロー マッピング」ページの「追加」ボタンをクリックすると、承認ポリシーを設定できる別のページが開きます。

詳細情報

[ポリシーベースのイベント用ワークフローの設定方法](#) (P. 349)

[承認ポリシーの設定方法](#) (P. 351)

CA Identity Manager のタスク ステータス

CA Identity Manager タスクを処理のためにサブミットした後で、管理者がタスクのステータスを追跡したい場合があります。CA Identity Manager でタスク ステータスを表示する方法を以下に示します。

■ [サブミット済みタスクの表示] タブ

このタブでは、処理用にサブミット済みの CA Identity Manager タスクを検索および表示できます。

管理者は、タスクの詳細を概要レベルで表示することも、さらに詳しいレベルで表示することもできます。

[サブミット済みタスクの表示] タブは、以下の 2 つのデフォルト タスクに組み込まれています。

– マイ サブミット済みタスクの表示

管理者は、処理用にサブミット済みのタスクに関する情報を検索および表示できます。

– サブミット済みタスクの表示

管理者は、他の管理者が処理用にサブミットしたタスクに関する情報を検索および表示できます。

■ [ユーザ履歴] タブ

このタブは、[ユーザの表示] や [ユーザの変更] などのユーザ タスクに追加できます。管理者は、選択したユーザに関する以下の情報を表示できます。

– ユーザに対して実行されるタスク

– ユーザによって実行されるタスク

– ユーザが承認したワークフロー

- レポート

CA Identity Manager レポートでは、CA Identity Manager 環境の現在の状態を確認できます。この情報を使って、内部のビジネス ポリシーや外部規制とのコンプライアンスを確保できます。

[レポート機能](#) (P. 427)を使用すると、レポートの設定と使用に関する追加情報を確認できます。

- ログ

CA Identity Manager のインストールに含まれるすべてのコンポーネントに関する情報、および CA Identity Manager のすべての操作に関する詳細情報が表示されます。

CA Identity Manager のログの詳細については、「[設定ガイド](#)」を参照してください。

CA Identity Manager がタスク ステータスを判別するしくみ

タスクとは、CA Identity Manager でユーザが実行できる管理機能を言います。タスクにはイベントが含まれます。イベントとは、CA Identity Manager がタスクを完了するために実行するアクションを言います。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、ユーザプロフィールを作成するイベント、ユーザをグループに追加するイベント、ロールを割り当てるイベントが含まれます。

CA Identity Manager のタスクとイベントはワークフロー プロセスに関連付けることが可能で、これによって、必要とされるアクションやその他のカスタムのビジネス ロジックを CA Identity Manager が実行する方法が決まります。また、タスクは「ネスト タスク」と呼ばれる別のタスクと関連付けられる場合もあります。この場合、CA Identity Manager は元のタスクを使用してネスト タスクを処理します。

タスクのステータスは、関連付けられたイベント、ワークフロー プロセス、ネスト タスク、およびカスタム ビジネス ロジックのステータスによって決まります。

サブミット済みタスクの表示

CA Identity Manager には「サブミット済みタスクの表示」機能が組み込まれています。この機能では、CA Identity Manager 環境のタスクに関する情報が提供されます。この機能を使用して、CA Identity Manager が実行するアクションに関する高レベルの詳細情報を検索し、表示することができます。詳細画面によって、各タスクおよびイベントに関する追加情報が提供されます。

タスクのステータスに応じて、「サブミット済みタスクの表示」を使用してタスクの中止または再サブミットを実行できます。

「サブミット済みタスクの表示」では、タスクの処理を始めから終わりまで追跡することができます。たとえば、CA Identity Manager タスクにプロビジョニングロールの割り当てが含まれていて、その割り当てによって別のシステムでアカウントが作成される場合、「サブミット済みタスクの表示」タブには元のタスクの全詳細と、アカウント作成に関する詳細が表示されます。

「サブミット済みタスクの表示」には、システム内で実行された処理の詳細が表示されます。これらの処理は、EnableUserEvent などの CA Identity Manager イベントに起因する場合があります。システムから送信された通知は、このイベントの下にグループ化されます。「サブミット済みタスクの表示」には、最後の詳細通知が送信されるまで、通知が進行中であることを示すメッセージが表示されます。その後、メッセージは「完了」に変わります。

CA Identity Manager のデフォルトでは、「サブミット済みタスクの表示」タブは以下の 2 つのタスクに組み込まれています。

- サブミット済みタスクの表示
- マイ サブミット済みタスクの表示

サブミット済みタスクの検索

サブミット済みタスクを検索するには、以下の手順に従います。

サブミット済みタスクの検索方法

1. 「システム」 - 「サブミット済みタスクの表示」をクリックします。
「サブミット済みタスクの表示」ページが表示されます。
2. 検索基準を指定し、表示される行の数を入力し、「検索」をクリックします。
検索条件に適合するタスクが表示されます。

注: 検索基準に属性を指定する方法の詳細については、「[サブミット済みタスクの表示に関する検索属性 \(P. 606\)](#)」を参照してください。

サブミット済みタスクの表示に関する検索属性

処理用にサブミットされたタスクを確認するには、[サブミット済みタスクの表示] で検索機能を使用します。以下の条件に基づいて、タスクを検索できます。

開始者

検索条件となるタスクを開始したユーザの名前を識別します。このユーザ名に基づいて検索が実行されます。有効なユーザ名を入力したことを確認するには、[検証] ボタンを使用します。

承認タスクの実行者

検索条件としてタスク承認者の名前を識別します。このユーザ名に基づいて検索が実行されます。有効なユーザ名を入力したことを確認するには、[検証] ボタンを使用します。

注: タスクのフィルタとして [承認タスク実行者] 条件を選択した場合は、デフォルトにより [承認タスクの表示] 条件も有効になります。

タスク名

検索条件としてタスク名を識別します。[タスク名の条件] フィールドの値として「=」、「以下を含む」、「以下で開始」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。たとえば、「=」条件を指定し、テキストフィールドに「ユーザの作成」と入力すると、「タスク名 = ユーザの作成」という検索基準を指定できます。

タスクのステータス

検索条件となるタスク ステータスを識別します。タスクのステータスを選択するには、「タスク ステータス =」を有効にし、条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

- 完了
- 実行中
- 失敗
- 拒否
- 一部完了
- 中止
- スケジュール済み

注: 詳細については、「[タスク ステータスの説明](#) (P. 608)」を参照してください。

タスク優先度

検索条件としてタスクの優先度を識別します。タスク優先度を選択するには、[タスク優先度の条件]を有効にして条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

低

このオプションを指定すると、低優先度のタスクを検索できます。

中

このオプションを指定すると、中優先度のタスクを検索できます。

高

このオプションを指定すると、高優先度のタスクを検索できます。

実行対象

選択したオブジェクト インスタンスに対して実行されるタスクを識別します。オブジェクト インスタンスを選択しない場合は、そのオブジェクトの全インスタンスに対して実行されたタスクがすべて表示されます。

注: このフィールドは、[サブミット済みタスクの設定] 画面で [次に対し設定を実行] フィールドを指定した場合にのみ表示されます。[サブミット済みタスク] タブを設定するには、この画面を使用します。詳細については、この画面に関するオンライン ヘルプを参照してください。

日付範囲

サブミット済みタスクの検索範囲を識別します。開始日と終了日を指定する必要があります。

サブミットされていないタスクの表示

監査済み状態のタスクを識別します。他のタスクを開始したタスクや、サブミットされていないタスクが識別されます。このタブを選択した場合は、そのようなタブがすべて監査され、表示されます。

承認タスクの表示

ワークフローの一部として承認すべきタスクを識別します。

サブミット済みタスクのアーカイブを検索

アーカイブされたサブミット済みタスクを識別します。

タスク ステータスの説明

サブミット済みタスクのステータスは、以下のいずれかになります。タスクのステータスに基づいて、タスクのキャンセルや再サブミットなどのアクションを実行できます。

注: タスクをキャンセルまたは再サブミットするには、タスク ステータスに基づいてキャンセル ボタンと再サブミット ボタンが表示されるように[サブミット済みタスクの表示]を設定する必要があります。タスクのキャンセルと再サブミットの詳細については、[\[サブミット済みタスクの表示\] タブのカスタマイズ](#) (P. 611) を参照してください。

実行中

以下のいずれかが発生した場合に表示されます。

- ワークフローが開始されたが、まだ完了していない場合
- 現在のタスクの前に開始されたタスクが実行中の場合
- ネスト タスクが開始されたが、まだ完了していない場合
- プライマリ イベントが開始されたが、まだ完了していない場合
- セカンダリ イベントが開始されたが、まだ完了していない場合

この状態のタスクはキャンセルすることができます。

注: タスクをキャンセルすると、現在のタスクに関する未完了のネスト イベントとタスクがすべてキャンセルされます。

キャンセル済み

実行中のタスクまたはイベントのいずれかをキャンセルした場合に表示されます。

拒否

ワークフロー プロセスの一部となるイベントまたはタスクが **CA Identity Manager** によって拒否された場合に表示されます。拒否されたタスクは再サブミットすることができます。

注: タスクを再サブミットすると、失敗または拒否されたネスト タスクとイベントがすべて再サブミットされます。

一部完了

一部のイベントまたはネスト タスクをキャンセルした場合に表示されます。一部完了したイベントまたはネスト タスクは再サブミットすることができます。

完了

タスクが完了した場合に表示されます。現在のタスクのネスト タスクとネスト イベントがすべて完了すると、タスクが完了します。

失敗

現在のタスクに含まれるタスク、ネスト タスク、またはネスト イベントが無効の場合に表示されます。このステータスは、タスクが失敗した場合に表示されます。失敗したタスクは再サブミットすることができます。

スケジュール済み

タスクを後で実行するようスケジュール設定されている場合に表示されます。この状態のタスクはキャンセルすることができます。

監査済み

現在のタスクが監査済みの場合に表示されます。

タスクの詳細の表示

CA Identity Manager では、サブミット済みタスクのステータス、ネスト タスク、タスクに関連付けられたイベントなどのタスク詳細を確認できます。

サブミット済みタスクの詳細を表示する方法

1. [サブミット済みタスクの表示] タブで、選択されたタスクの横にある右矢印アイコンをクリックします。

タスクの詳細が表示されます。

注: イベントとネスト タスク (ある場合) は、[タスク詳細] ページに表示されます。タスクおよびイベントごとのタスク詳細を表示できます。

2. [閉じる] をクリックします。

[タスクの詳細] タブが閉じ、CA Identity Manager の [サブミット済みタスクの表示] タブにタスク リストが表示されます。

イベントの詳細の表示

CA Identity Manager では、サブミット済みイベントのステータス、イベント属性、イベントに関する追加情報などのイベント詳細を確認できます。

サブミット済みイベントの詳細を表示する方法

1. [タスクの詳細の表示] ページで、イベントの横にある右矢印アイコンをクリックします。
イベントの詳細が表示されます。
2. [閉じる] をクリックします。
[イベントの詳細] ページが閉じます。

イベント ステータスの説明

CA Identity Manager のイベントのステータスは、以下のいずれかになります。 イベントのステータスに基づいて、実行対象イベントをキャンセルまたは再サブミットできます。

注: 管理者がイベントをキャンセルまたは再サブミットできるようにするには、[イベントのキャンセル] ボタンと [Resubmit Events] ボタンが表示されるように [サブミット済みタスクの表示] を設定する必要があります。 タスクの設定時には、イベントをキャンセルおよび再サブミットできる管理者を指定できます。 イベントのキャンセルと再サブミットの詳細については、「[\[サブミット済みタスクの表示\] タブのカスタマイズ \(P. 611\)](#)」を参照してください。

実行中

以下のいずれかが発生した場合に表示されます。

- ワークフローまたは事前イベントが開始済み、実行中、または承認済みの場合
- CA Identity Manager がイベントを実行中の場合
- CA Identity Manager が事後イベントを実行する場合

この状態のイベントはキャンセルすることができます。

拒否

ワークフローの一部となるイベントが CA Identity Manager によって拒否された場合に表示されます。拒否されたイベントは再サブミットすることができます。

キャンセル済み

実行中のイベントのいずれかをキャンセルした場合に表示されます。キャンセルされたイベントは再サブミットすることができます。

完了

イベントが完了した場合に表示されます。

失敗

イベントの実行中に CA Identity Manager が例外を検出した場合に表示されます。キャンセルされたイベントは再サブミットすることができません。

注: セカンダリ イベントは、プライマリ イベントが完了状態になるまで再サブミットできません。

スケジュール済み

イベントを後で実行するようスケジュール設定されている場合に表示されます。この状態のイベントはキャンセルすることができます。

監査済み

現在のイベントが監査済みの場合に表示されます。

[サブミット済みタスクの表示] タブのカスタマイズ

以下のようにして、[サブミット済みタスクの表示] タブをカスタマイズできます。

- 別のタスク名とタグを指定します。
- デフォルトの表示プロパティを変更します。ユーザがインストールすると、このタブに表示されるタスクを決定するための基準を入力できる検索画面が表示されます。ユーザが検索基準を入力せずに済むように、その日のサブミット済みタスクを自動的に表示するようにタブを設定できます。
- [タスク詳細] ページに監査イベントが表示されるかどうかを決定します。
- タスク表示に列を追加します。
- タスクやイベントをキャンセルまたは再サブミットするための基準を指定します。

注: 一部のタスクとイベントの詳細には、給与やパスワードといった [サブミット済みタスクの表示] タブにクリア テキスト形式で表示すべきではないデータが含まれます。このようなデータは、**directory.xml** ファイルで属性を定義する際に、データ分類のパラメータを指定して非表示にすることができます。 **directory.xml** ファイルの詳細については、「[設定ガイド](#)」を参照してください。

対応する管理タスクを変更して、[サブミット済みタスクの表示] タブを設定することができます。

[サブミット済みタスクの表示]タブを設定する方法

1. [ロールおよびタスク] - [管理タスク] - [管理タスクの変更] をクリックします。
[管理タスクの選択] 画面が表示されます。
2. [管理タスクの検索] の [条件] フィールドで [名前] または [カテゴリ] を選択し、検索文字列を入力して [検索] をクリックします。
検索基準を満たす管理タスクが表示されます。
3. [サブミット済みタスクの表示] を選択し、[選択] をクリックします。
[サブミット済みタスクの表示] 管理タスクの詳細が表示されます。
4. [タブ] タブをクリックします。
[サブミット済みタスクの表示] タブに使用されるタブが表示されます。
5. 右矢印アイコンをクリックし、[サブミット済みタスク] タブを編集します。
タブの詳細が表示されます。
6. 各フィールドを編集して、必要に応じて [サブミット済みタスクの表示] タブをカスタマイズします。詳細については、「[\[サブミット済みタスク\] タブの設定 \(P. 613\)](#)」を参照してください。

[サブミット済みタスクの表示]タブの設定

[サブミット済みタスクの表示] タブの外観と機能を変更するには、以下のフィールドを使用します。

名前

タスクの名前を定義します。

タグ

タスクの一意な識別子を定義します。これは URL、Web サービス、またはプロパティ ファイルで使用されます。アルファベット文字、数字、または下線文字で構成し、先頭をアルファベット文字または下線文字にする必要があります。

タブの非表示

ユーザに対してタブが表示されるが、実行はされないことを示します。このオプションを選択すると、ユーザに対してエラーが表示されます。

ロード中のタスクリストを表示

その日のサブミット済みタスクが表示されます。

注: このオプションを有効にすると、[サブミット済みタスクの表示] をクリックしたユーザに対し、その日にサブミットされたタスクが直接表示されます。

監査イベントの表示

監査対象のイベントを [サブミット済みタスクの表示] ページのタスクに含めるかどうかを指定します。

カスタム列を許可

タスク テーブルにカスタム列を追加できることを指定します。タスク テーブルは、[サブミット済みタスクの表示] タブと [ユーザ履歴] タブから表示できます。たとえば、[ユーザ履歴] タブから表示されるタスク テーブルに [ユーザ ID] 列を追加することができます。

カスタム列見出し

カスタム列の表示名を指定します。

カスタム列属性

タスク テーブルのカスタム列入力に用いるアトリビュートを指定します。たとえば、ある組織の従業員に対して実施するタスクを検索する場合、各従業員の組織を表示する組織列を追加することができます。

タスクおよびイベントのキャンセル

タスクやイベントをキャンセルするための基準を指定します。このフィールドのスコップを設定するには、以下のオプションのいずれかを選択します。

タスク作成者は現在のユーザである必要があります

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

タスク作成者はスコップに入っている必要があります

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコップが含まれたメンバシップルール内の基準と自分が一致するため、[サブミット済みタスクの表示] が含まれた [ユーザ マネージャ] ロールを受け取ったとします。この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

不可

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

タスクおよびイベントの再サブミット

タスクやイベントを再サブミットするための基準を指定します。以下のいずれかのオプションを選択して、このフィールドの範囲を設定できます。

タスク作成者は現在のユーザである必要があります

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

タスク作成者はスコープに入っている必要があります

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコープが含まれたメンバシップルール内の基準と自分が一致するため、[サブミット済みタスクの表示] が含まれた [ユーザ マネージャ] ロールを受け取ったとします。この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

不可

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

[ユーザ履歴]タブ

[ユーザ履歴] タブでは、特定のユーザに関連するタスクを表示できます。このタブに表示されるタスク詳細は、[サブミット済みタスクの表示] タブでも表示できます。

注: このタブを追加しても、[ユーザの作成] などのタスクを作成することはできません。

このタブを使用して、以下のタスクの履歴を表示できます。

- ユーザに対して実行されるタスク

選択したユーザに対して実行されるすべてのタスクを表示します。

- ユーザによって実行されるタスク

選択したユーザによって実行されるすべてのタスクを表示します。

- ユーザが承認したワークフロー

ワークフローの一部としてユーザが承認したすべてのタスクを表示します。

注: このタブに表示できるタスクのタイプは、タブの設定によって異なります。詳細については、「[\[ユーザ履歴\] タブのカスタマイズ \(P. 618\)](#)」を参照してください。

ユーザ履歴の表示に関する検索属性

処理用にサブミットされたタスクを確認するには、[サブミット済みタスクの表示] で検索機能を使用します。以下の条件に基づいて、タスクを検索できます。

タスク名

検索条件としてタスク名を識別します。[タスク名の条件] フィールドの値として「=」、「以下を含む」、「以下で開始」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。たとえば、「=」条件を指定し、テキストフィールドに「ユーザの作成」と入力すると、「タスク名 = ユーザの作成」という検索基準を指定できます。

タスクのステータス

検索条件となるタスク ステータスを識別します。タスクのステータスを選択するには、「タスク ステータス=」を有効にし、条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

- 完了
- 実行中
- 失敗
- 拒否
- 一部完了
- キャンセル済み
- スケジュール済み

注: 詳細については、「[タスク ステータスの説明 \(P. 608\)](#)」を参照してください。

タスク優先度

検索条件としてタスクの優先度を識別します。タスク優先度を選択するには、[タスク優先度の条件]を有効にして条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

低

このオプションを指定すると、低優先度のタスクを検索できます。

中

このオプションを指定すると、中優先度のタスクを検索できます。

高

このオプションを指定すると、高優先度のタスクを検索できます。

日付範囲

サブミット済みタスクの検索範囲を識別します。開始日と終了日を指定する必要があります。

[ユーザ履歴]タブのカスタマイズ

管理者は以下のようにして、[ユーザ履歴] タブをカスタマイズできます。

- 別のタスク名とタグを指定します。
- デフォルトの表示プロパティを変更します。デフォルトでは、ユーザはタブに表示するタスクを決定する条件を入力できます。管理者は、ユーザが検索条件を入力せずに済むように、その日のタスクを自動的に表示するようにタブを設定できます。
- [タスク詳細] ページに監査イベントが表示されるかどうかを決定します。
- タスク表示に列を追加します。
- タスクやイベントをキャンセルまたは再サブミットするための基準を指定します。

次の手順に従ってください:

1. [ロールおよびタスク]-[管理タスク]-[管理タスクの管理] に移動します。
[管理タスクの選択] 画面が表示されます。
2. [管理タスクの検索] の [条件] フィールドで [名前] または [カテゴリ] を選択し、検索文字列を入力して [検索] をクリックします。
検索基準を満たす管理タスクが表示されます。
3. [ユーザ履歴] タブが含まれたタスクを選択し、[選択] をクリックします。
その管理タスクの詳細が表示されます。
4. [タブ] タブをクリックします。
5. [ユーザ履歴] タブの横の編集アイコンをクリックします。
タブの詳細が表示されます。
6. フィールドを編集して [ユーザ履歴] タブをカスタマイズします。

[ユーザ履歴]タブ用の設定

以下のフィールドを使用して、[ユーザ履歴] タブの表示および機能を変更します。

名前

タスクの名前を定義します。

タグ

タスクの一意な識別子を定義します。これは URL、Web サービス、またはプロパティ ファイルで使用されます。アルファベット文字、数字、または下線文字で構成し、先頭をアルファベット文字または下線文字にする必要があります。

タブの非表示

ユーザに対してタブが表示されるが、実行はされないことを示します。このオプションを選択すると、ユーザに対してエラーが表示されます。

ロード中のタスクリストを表示

その日のサブミット済みタスクが表示されます。

注: このオプションを有効にすると、[サブミット済みタスクの表示] をクリックしたユーザに対し、その日にサブミットされたタスクが直接表示されます。

監査イベントの表示

監査対象のイベントを [サブミット済みタスクの表示] ページのタスクに含めるかどうかを指定します。

カスタム列を許可

タスク テーブルにカスタム列を追加できることを指定します。タスク テーブルは、[サブミット済みタスクの表示] タブと [ユーザ履歴] タブから表示できます。たとえば、[ユーザ履歴] タブから表示されるタスク テーブルに [ユーザ ID] 列を追加することができます。

カスタム列見出し

カスタム列の表示名を指定します。

カスタム列属性

タスク テーブルのカスタム列入力に用いるアトリビュートを指定します。たとえば、ある組織の従業員に対して実施するタスクを検索する場合、各従業員の組織を表示する組織列を追加することができます。

タスクおよびイベントのキャンセル

タスクやイベントをキャンセルするための基準を指定します。このフィールドのスコップを設定するには、以下のオプションのいずれかを選択します。

タスク作成者は現在のユーザである必要があります

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

タスク作成者はスコップに入っている必要があります

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコップが含まれたメンバシップルール内の基準と自分が一致するため、[サブミット済みタスクの表示] が含まれた [ユーザ マネージャ] ロールを受け取ったとします。この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

不可

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

タスクおよびイベントの再サブミット

タスクやイベントを再サブミットするための基準を指定します。以下のいずれかのオプションを選択して、このフィールドの範囲を設定できます。

タスク作成者は現在のユーザである必要があります

作成したタスクやイベントをキャンセルまたは再サブミットできることを示します。

タスク作成者はスコープに入っている必要があります

このタブにアクセスできる管理ロールのユーザ スコープ ルールと一致する他のユーザが開始したタスクをキャンセルまたは再サブミットできることを示します。

たとえば、「従業員」という組織のユーザ全員に対するスコープが含まれたメンバシップルール内の基準と自分が一致するため、[サブミット済みタスクの表示] が含まれた [ユーザ マネージャ] ロールを受け取ったとします。この場合は、「従業員」という組織のすべてのユーザがサブミットしたタスクをキャンセルまたは再サブミットできます。

制限なし

任意のユーザがタスクやイベントをキャンセルまたは再サブミットできることを示します。

不可

タスクやイベントをキャンセルまたは再サブミットできないことを示します。

タスクの表示

[ユーザ履歴] タブに表示されるタスクを決定します。

ユーザに対して実行されるタスク

選択したユーザに対して実行されるすべてのタスクを表示します。

ユーザによって実行されるタスク

選択したユーザによって実行されるすべてのタスクを表示します。

ユーザが承認したワークフロー

ワークフローの一部としてユーザが承認したすべてのタスクを表示します。

ユーザ アクティビティの表示タスク

ユーザ アクティビティとは、ある特定のユーザに関するタスクの履歴です。管理者は「ユーザ アクティビティの表示」タスクを使用して、以下のユーザ情報を追跡できます。

- ユーザに対して実行されるタスク
- ユーザによって実行されるタスク
- ユーザが実行するワークフローの承認

ユーザ アクティビティを表示する方法

1. 「ユーザ」 - 「ユーザの管理」 - 「ユーザ アクティビティの表示」に移動します。

「ユーザの選択」画面が表示されます。

2. ユーザを検索して「選択」をクリックします。

「ユーザ アクティビティの表示」画面が表示されます。

注: 表示されたユーザ アクティビティの詳細については、ユーザ コンソールのオンライン ヘルプを参照してください。

サブミット済みタスクのクリーンアップ

各タスクをサブミットして、タスク永続性データベースが拡大するにつれ、タスクおよびイベントの実行時のパフォーマンスが低下します。ストアドプロシージャのガーベッジコレクションを行うと、タスク永続性データベースの記憶領域が不足することが原因のパフォーマンス上の問題やシステムの機能停止のリスクを低減することができます。タスクのアーカイブ機能を使用することで、管理者は、削除されたタスクやイベントと共に現在のタスクおよびイベント情報の両方を表示できます。

ユーザ コンソールで、CA Identity Manager の管理者は、ガーベッジ コレクションおよびアーカイブが反復ベースで自動的に実行されるように、ジョブをスケジュールすることができます。

[反復]タブ

このタブを使用して、ジョブをスケジュールします。このタブ内のフィールドは以下のとおりです。

今すぐ実行

ジョブを今すぐ実行します。

新規ジョブのスケジュール

新規ジョブをスケジュールします。

既存ジョブの変更

すでに存在するジョブで変更するジョブを指定します。

注: このフィールドが表示されるのは、このタスクのジョブがすでにスケジュールされている場合のみです。

ジョブ名

作成または変更するジョブの名前を指定します。

タイムゾーン

サーバのタイムゾーンを指定します。

注: 新しいジョブのスケジュール時に、使用しているタイムゾーンがサーバのタイムゾーンと異なる場合には、ドロップダウンボックスが表示されるので、使用中のタイムゾーンまたはサーバのタイムゾーンのいずれを使用するかを選択できます。既存のジョブを修正する場合には、タイムゾーンは変更できません。

日単位のスケジュール

特定の日数だけ毎日ジョブが実行されるよう指定します。

毎(日数)

ジョブを実行する間隔(日数)を定義します。

週単位のスケジュール

1 週間のうち特定の日または期間でのジョブの実行を指定します。

曜日

ジョブを実行する曜日を指定します。

月単位のスケジュール

月単位で実行されるジョブの曜日または日付を指定します。

年単位のスケジュール

年単位で実行されるジョブの曜日または日付を指定します。

詳細なスケジュール

その他のスケジュール情報を指定します。

Cron 式

このフィールドの入力の詳細については、以下の Web サイトを参照してください。

<http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html>

実行時間

ジョブを実行する時刻を、24 時間形式で指定します。 例： 14:15

ジョブの即時実行

ジョブを即時に実行するには、[サブミット済みタスクのクリーンアップ] ウィザードを使用します。

次の手順に従ってください：

1. [システム] - [サブミット済みタスクのクリーンアップ] に移動します。
[反復] 手順のウィザードが表示されます。
2. [今すぐ実行] - [次へ] を選択します。
[サブミット済みタスクのクリーンアップ] 手順のウィザードが表示されます。
3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了] をクリックします。
ジョブが即時にサブミットされます。

新規ジョブのスケジュール

新規ジョブをスケジュールするには、[サブミット済みタスクのクリーンアップ] ウィザードを使用します。

次の手順に従ってください：

1. [システム] - [サブミット済みタスクのクリーンアップ] に移動します。
[反復] 手順が表示されます。
2. [新規ジョブのスケジュール] を選択し、ジョブ名とそのジョブのスケジュール設定情報を入力し、[次へ] をクリックします。
[サブミット済みタスクのクリーンアップ] 手順が表示されます。
3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了] をクリックします。
新規ジョブがスケジュール化されます。

既存のジョブの変更

既存のジョブを変更するには、[サブミット済みタスクのクリーンアップ] ウィザードを使用します。

次の手順に従ってください：

1. [システム] - [サブミット済みタスクのクリーンアップ] に移動します。
[反復] 手順が表示されます。
2. [既存ジョブの変更] を選択し、既存のジョブを選び、スケジュール情報を変更してから、[次へ] をクリックします。
[サブミット済みタスクのクリーンアップ] 手順が表示されます。
3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を変更してから、[完了] をクリックします。
既存のジョブが変更されます。

反復タスクの削除

反復するタスクの削除方法

次の手順に従ってください：

1. [システム] - [反復タスクの削除] に移動します。
2. 削除するタスクを選択します。
3. [サブミット] をクリックします。

[サブミット済みタスクのクリーンアップ]タブ

このタブを使用して、タスクの最小期間、アーカイブ、監査タイムアウト、制限時間、タスク制限を指定します。すべての必須フィールドに入力したら [完了] をクリックします。このタブ内のフィールドは以下のとおりです。

最短期間

最終状態（完了、失敗、拒否、キャンセル、または中止）にあるタスクがクリーンアップされるまでの最小期間を指定します。たとえば、最小期間に 1 か月を指定した場合、最後の月に最終状態に到達した任意のタスクは保持されます。1 か月以上前に、最終状態に到達したタスクは、クリーンアップおよびアーカイブ対象となります。

これは必須フィールドです。

アーカイブ

実行中のデータベースからタスクを削除する前に、アーカイブデータベースにタスクをバックアップします。

ジョブが実行されたら、アーカイブが選択されている場合、データはアーカイブデータベースにコミットされ、実行時のタスク永続性データベースから削除されます。データはアーカイブデータベースに正常にコミットされるまで削除されません。

監査タイムアウト

監査状態にあるタスクがクリーンアップされるまでの時間の長さを指定します。監査状態のタスクは、この期間が経過するまで最終状態とはみなされません。監査状態のタスクは、サブミットされていません。

時間制限

クリーンアップを特定の時間内に制限します。

タスク制限

クリーンアップを特定のタスク回数に制限します。

反復タスクの削除

タスクを反復ベースで実行する必要性がなくなった場合に、**CA Identity Manager** の管理者はタスクを削除できます。タスクが削除されると、ガーベッジコレクションおよびアーカイブは、そのタスクに対しては実行されません。

[サブミット済みタスクのクリーンアップ] を使用してスケジュールしたすべてのタスク：反復ウィザードは、このページにリストされており、**CA Identity Manager** の管理者は、どのタスクを削除するかを選択できます。

注: そのタスクは、依然としてデータベースには存在しており、反復のスケジュールのみが削除されます。

Enterprise Log Manager 接続の設定

新しく追加された **CA User Activity Reporting (CA UAR)** 接続タスクを管理するために、この画面を使用します。

注: CA Enterprise Log Manager は名前が変更されました。現在は **CA UAR** と呼ばれます。

この画面のフィールドを以下に示します。

接続名

単一の **CA UAR** 接続管理オブジェクトに使用する一意の名前を指定します。

このフィールドは、読み取り専用です。

説明

CA UAR 接続について説明します。

ホスト名

CA UAR サーバのホスト名または IP アドレスを指定します。

これは必須フィールドです。

ポート番号

CA UAR サーバの接続ポートを指定します。

デフォルト: **52520**

これは必須フィールドです。

認証機関によって署名された SSL 証明書

チェックがオンになっている場合には、**CA UAR** サーバへの接続時に、厳格な **SSL** 証明書チェックを指定します。

たとえば、デフォルトで **CA UAR** にインストールされている **SSL** 証明書のような自己署名 **SSL** 証明書を有する場合は、ルート認証局へのトラステッドパスが存在しないので、このチェック ボックスをオフにする必要があります。

証明書名

認証に使用する **CA UAR** 証明書の名前を指定します。

これは必須フィールドです。

証明書パスワード

CA UAR パスワードを指定します。

これは必須フィールドです。

属性

サポート対象外です。バージョンは、接続情報をテストとして保存するために取得します。

Enterprise Log Manager 接続の削除

リストから接続を選択して、[削除] をクリックします。CA UAR 接続が削除されます。

秘密鍵の管理

データを暗号化または復号化する動的キーを管理するために、秘密鍵を使用します。あるユーザがキーへの不正アクセスを取得したことが疑われる場合、キーストア用のパスワードを変更することができます。キーストアは、秘密鍵を格納するデータベースです。このパスワードを変更すると、**CA Identity Manager** はキーの値を再度暗号化します。

各環境には、動的キーおよびキーストアパスワードのセットがあります。環境がユーザディレクトリを共有している場合は、各環境で同じ動的キーおよびキーストアパスワードを使用します。

キーストアパスワードは、**CA Identity Manager** サーバのインストール中に入力された暗号化コードまたはパラメータに埋め込まれたキーを使用して暗号化されます。クラスタ内では、動的キーおよびキーストアパスワードの値がすべてのノードによって共有されています。

暗号化操作では、対応するアルゴリズムおよび環境用の最新の動的キーが使用されます。復号化操作では、正しいキーが使用されるように、暗号化されたデータにキー ID が存在するかどうか確認します。詳細は「*Configuration Guide*」の「*Encrypted Text Formats*」セクションに提供されています。

次の手順に従ってください：

1. キーストアへのパスワードを入力するか変更します。
2. 別のキーが必要な場合は [キーの追加] をクリックします。
3. アルゴリズムを選択します。
4. キー用のパスワードを入力します。

PBE と RC2 については、キーの最大長は 128 バイトです。
AES については、有効なキー サイズは 16、24 および 32 バイトです。
5. [サブミット] をクリックします。
6. キーストアパスワードを変更した場合は、[サブミット] をクリックします。

CA Identity Manager は、再度キーの値を暗号化します。

第 21 章：タスク永続性

このセクションには、以下のトピックが含まれています。

[自動化されたタスクの永続ガベージコレクションとアーカイブ](#) (P. 631)

[\[反復\] タブ](#) (P. 632)

[\[サブミット済みタスクのクリーンアップ\] タブ](#) (P. 634)

[ジョブの即時実行](#) (P. 635)

[新規ジョブのスケジュール](#) (P. 635)

[既存のジョブの変更](#) (P. 636)

[反復タスクの削除](#) (P. 636)

[タスク永続性データベースの移行方法](#) (P. 637)

自動化されたタスクの永続ガベージコレクションとアーカイブ

このリリースでは、管理者は [サブミット済みタスクのクリーンアップ] タスクを使用して、特定のパラメータのジョブをスケジュールまたは変更し、タスク永続性データベースのタスク情報とイベント情報をクリーンアップおよびアーカイブします。また、必要に応じてこれらの反復タスクを削除します。

[システム] タブでは、[サブミット済みタスクのクリーンアップ] を選択してウィザードを起動できます。このウィザードから、ジョブの設定とスケジュールができ、さらにデータをアーカイブするかどうかも設定できます。また、[システム] タブから [反復タスクの削除] を選択して、必要に応じて反復ジョブが削除されるようにすることもできます。

タスク データがクリーンアップおよびアーカイブされるようにタスクをスケジュールすると、パフォーマンスの問題とシステム停止が発生する可能性は大幅に減少します。このアーカイブ機能によって、実行中のデータベースからタスクを削除する前に、これらのタスクをアーカイブ データベースにバックアップできます。前の手順に戻り、削除されたタスクを表示する必要がある場合、[サブミット済みタスクの表示] のアーカイブの [Search the archive] チェック ボックスをオンにして、削除およびアーカイブされたすべてのタスクのリストを検索または表示できます。

[反復]タブ

このタブを使用して、ジョブをスケジュールします。このタブ内のフィールドは以下のとおりです。

今すぐ実行

ジョブを今すぐ実行します。

新規ジョブのスケジュール

新規ジョブをスケジュールします。

既存ジョブの変更

すでに存在するジョブで変更するジョブを指定します。

注: このタスクにジョブがすでにスケジュールされている場合には、このフィールドのみが表示されます。

ジョブ名

作成または変更するジョブの名前を指定します。

タイムゾーン

サーバのタイムゾーンを指定します。

注: 新しいジョブのスケジュール時に、使用しているタイムゾーンがサーバのタイムゾーンと異なる場合には、ドロップダウンボックスが表示されるので、使用中のタイムゾーンまたはサーバーのタイムゾーンのいずれを使用するかを選択できます。既存のジョブを修正する場合には、タイムゾーンは変更できません。

週単位のスケジュール

ある週の特定の日または期間でのジョブの実行を指定します。

詳細なスケジュール

その他のスケジュール情報を指定します。

曜日

ジョブを実行する曜日を指定します。

実行時間

ジョブを実行する時刻を、24 時間形式で指定します。例: 14:15

Cron 式

このフィールドの入力の詳細については、以下の Web サイトを参照してください。

<http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html>

注: [詳細なスケジュール] が選択されている場合には、このフィールドが表示されます。

詳細情報

[反復タスクの削除](#) (P. 625)

[新規ジョブのスケジュール](#) (P. 625)

[既存のジョブの変更](#) (P. 625)

[ジョブの即時実行](#) (P. 624)

[サブミット済みタスクのクリーンアップ]タブ

このタブを使用して、タスクの最小期間、アーカイブ、監査タイムアウト、制限時間、タスク制限を指定します。すべての必須フィールドに入力したら [完了] をクリックします。このタブ内のフィールドは以下のとおりです。

最短期間

最終状態（完了、失敗、拒否、キャンセル、または中止）にあるタスクがクリーンアップされるまでの最小期間を指定します。たとえば、最小期間に 1 か月を指定した場合、最後の月に最終状態に到達した任意のタスクは保持されます。1 か月以上前に、最終状態に到達したタスクは、クリーンアップおよびアーカイブ対象となります。

これは必須フィールドです。

アーカイブ

実行中のデータベースからタスクを削除する前に、アーカイブデータベースにタスクをバックアップします。

ジョブが実行されたら、アーカイブが選択されている場合、データはアーカイブデータベースにコミットされ、実行時のタスク永続性データベースから削除されます。データはアーカイブデータベースに正常にコミットされるまで削除されません。

監査タイムアウト

監査状態にあるタスクがクリーンアップされるまでの時間の長さを指定します。監査状態のタスクは、この期間が経過するまで最終状態とはみなされません。監査状態のタスクは、サブミットされていません。

時間制限

クリーンアップを特定の時間内に制限します。

タスク制限

クリーンアップを特定のタスク回数に制限します。

ジョブの即時実行

ジョブを即時に実行するには、[サブミット済みタスクのクリーンアップ] ウィザードを使用します。

次の手順に従ってください：

1. [システム] - [サブミット済みタスクのクリーンアップ] に移動します。
[反復] 手順のウィザードが表示されます。
2. [今すぐ実行] - [次へ] を選択します。
[サブミット済みタスクのクリーンアップ] 手順のウィザードが表示されます。
3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了] をクリックします。

ジョブが即時にサブミットされます。

新規ジョブのスケジュール

新規ジョブをスケジュールするには、[サブミット済みタスクのクリーンアップ] ウィザードを使用します。

次の手順に従ってください：

1. [システム] - [サブミット済みタスクのクリーンアップ] に移動します。
[反復] 手順が表示されます。
2. [新規ジョブのスケジュール] を選択し、ジョブ名とそのジョブのスケジュール設定情報を入力し、[次へ] をクリックします。
[サブミット済みタスクのクリーンアップ] 手順が表示されます。
3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を入力してから、[完了] をクリックします。

新規ジョブがスケジュール化されます。

既存のジョブの変更

既存のジョブを変更するには、[サブミット済みタスクのクリーンアップ] ウィザードを使用します。

次の手順に従ってください：

1. [システム] - [サブミット済みタスクのクリーンアップ] に移動します。
[反復] 手順が表示されます。
2. [既存ジョブの変更] を選択し、既存のジョブを選び、スケジュール情報を変更してから、[次へ] をクリックします。
[サブミット済みタスクのクリーンアップ] 手順が表示されます。
3. 最小期間、アーカイブ、監査タイムアウト、時間制限、タスク制限情報を変更してから、[完了] をクリックします。
既存のジョブが変更されます。

反復タスクの削除

反復するタスクの削除方法

次の手順に従ってください：

1. [システム] - [反復タスクの削除] に移動します。
2. 削除するタスクを選択します。
3. [サブミット] をクリックします。

タスク永続性データベースの移行方法

これまでのリリースでは、移行は管理コンソールを使用して「オンザフライ」で行われていました。コマンドライン移行ツールが提供されたことにより、大量のタスクの移行時に発生するパフォーマンスのボトルネックを解消できます。また、特定の環境、タスクの状態、および特定の日付範囲内で作成および実行されたタスクに合わせて微調整することもできます。`runmigration` コマンドラインツールは以下のフォルダに格納されています。

`admin_tools/tools/tpmigration`

タスク永続性データベースの移行には、以下を実行する必要があります。

1. `tpmigration125.properties` ファイルの更新。
2. `JAVA_HOME` 変数の設定。
3. `Runmigration` ツールの実行。

tpmigration125.properties ファイルの更新

タスク永続性データベースの移行を設定するには、保存されている値を含むオブジェクトストアおよびタスク永続性情報を使用して `tpmigration.properties` ファイルを更新する必要があります。`tpmigration125.properties` ファイルは、以下の場所に置かれています。

<IAM suite folder>/tools/tpmigration/com/ca/tp/migratetp125

移行を設定するには、プロパティ ファイル内の以下の情報を完了させます。

```
#####
# 環境の詳細を入手するには、オブジェクト ストアが必要です。
#####
os.db.hostname=<ホスト名>
os.db.dbname=<データベース名または SID>
os.db.username=<db ユーザ名>
os.db.password=<db ユーザのパスワード>
os.db.port=<db ポート番号>
os.db.dbType=<データベースのタイプ。例: SQL サーバの場合は sql2005,Oracle の場合は「oracle」>

#####
# 以前のテーブルおよび新しいテーブルが置かれているタスク永続性データ
#####
tp.db.hostname=<ホスト名>
tp.db.dbname=<データベース名または SID>
tp.db.username=<db ユーザ名>
tp.db.password=<db ユーザのパスワード>
tp.db.port=<db ポート番号>
tp.db.dbType=<データベースのタイプ。例: SQL サーバの場合は sql2005,Oracle の場合は「oracle」>
>
```

JAVA_HOME 変数の設定

Runmigration ツールを正しく実行するには、環境変数 `JAVA_HOME` が設定されていることを確認します。

runmigration ツールの実行

マイグレーションを開始する方法

コマンドラインから以下を実行してください

1. Runmigration ツールの実行。

Windows の場合:

`runmigration.bat`

UNIX の場合:

`runmigration.sh`

2. 以下の情報を入力します。

- エイリアスの保護環境 (すべての環境を入力するには、「all」とします)。

注: すべての環境を指定しない場合、入力可能な環境は 1 つのみです。

- タスク状態。

注: すべての状態を指定しない場合、入力可能なタスク状態は 1 つのみです。

- (1-8.x, 2-12.0) から移行する CA Identity Manager のバージョン。

- タスクを移行する日付の範囲を指定するかどうか (y/n)。

注: 「y」を選択する場合、以下を入力する必要があります。

- 開始日 (mm/dd/yy)

- 終了日 (mm/dd/yy)

移行が開始されます。

移行が完了すると、移行されたタスクの数がステータスに表示されます。