Sun Java™ System

Identity Manager 7.1
管理ガイド

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820-2289

目 次

図目次 **19**

表目次 **25**

はじめに **27**

このガイドの対象読者 27
このガイドを読まれる前に 28
このガイドで使用する表記規則 28
　書体の表記規則 28
　記号 29
関連ドキュメント 29
　このマニュアルセットの内容 29
Sun リソースへのオンラインアクセス 30
Sun テクニカルサポートへの問い合わせ 31
関連他社 Web サイトの参照について 31
ご意見をお寄せください 31

第 1 章 Identity Manager の概要 **33**
全体像 33
　Identity Manager システムの目的 34
　ユーザーアクセスの定義 35
　ユーザータイプ 36
　管理の委任 37
Identity Manager オブジェクト 37
　ユーザーアカウント 38
　ロール 38
　リソースとリソースグループ 39
　組織と仮想組織 40
　ディレクトリジャンクション 41
　機能 41

管理者ロール 41
ポリシー 42
監査ポリシー 42
オブジェクトの関係 42

第 2 章 Identity Manager 入門 47
Identity Manager インタフェース 47
Identity Manager 管理者インタフェース 48
管理者インタフェースへのログオン 49
Identity Manager ユーザーインタフェース 49
ユーザーインタフェースのカスタマイズ 50
Identity Manager IDE 51
ヘルプとガイダンス 53
Identity Manager ヘルプ 53
情報の検索 53
検索の動作 54
高度なクエリー構文 54
Identity Manager ガイダンス 56
Identity Manager へのログイン 57
ユーザー ID を忘れた場合 57
Identity Manager タスク 58
以降の操作について 62

第 3 章 ユーザーとアカウントの管理 63
ユーザーアカウントデータについて 63
ID 64
割り当て 65
セキュリティー 65
委任 66
属性 66
コンプライアンス 66
インタフェースの「アカウント」エリア 68
「アカウント」エリアのアクションリスト 68
「アカウントリスト」エリアでの検索 69
ユーザーアカウントステータス 69
ユーザーアカウントの操作 70
ユーザー 70
表示 70
作成 (「新規作成アクション」リスト、「新規ユーザー」選択) 71
編集 72
ユーザーの移動 (「ユーザーアクション」) 73
名前の変更 (「ユーザーアクション」) 74

ユーザーの無効化 (「ユーザーアクション」、「組織アクション」) 75
ユーザーの有効化 (「ユーザーアクション」、「組織アクション」) 77
ユーザーの更新 (「ユーザーアクション」、「組織アクション」) 77
ユーザーのロック解除 (「ユーザーアクション」、「組織アクション」) 79
削除 (「ユーザーアクション」、「組織アクション」) 80
パスワード 82
アカウントの検索 82
一括アカウントアクション 84
一括アカウントアクションの起動 84
アクションリストの使用 85
一括アクションの表示属性 88
ユーザーアカウントパスワードの操作 89
ユーザーアカウントパスワードの変更 89
ユーザーアカウントパスワードのリセット 90
リセット時のパスワードの期限切れ 90
アカウントセキュリティーと特権の管理 91
パスワードポリシーの設定 91
ポリシーの作成 91
辞書ポリシーの選択 92
パスワード履歴ポリシー 92
使用禁止単語 93
使用禁止属性 93
パスワードポリシーの実装 94
ユーザー認証 94
ユーザー独自の秘密の質問 95
認証後のパスワード変更リクエストのバイパス 96
管理特権の割り当て 97
ユーザーの自己検索 97
自己検索の有効化 97
相関規則と確認規則 98
相関規則 99
確認規則 99
匿名登録 100
匿名登録の有効化 100
匿名登録の設定 100
ユーザー登録プロセス 101

第 4 章 設定 103
ロールとその管理について 104
ロールとは 104
ロールの作成 104
割り当てられているリソース属性値の編集 105
ロールの管理 106

ロール名の変更 107
ロールとリソースロールの同期 107
Identity Manager リソースの設定 107
リソースとは 107
インタフェースの「リソース」エリア 108
リソースリストの管理 109
リソースの作成 110
リソースの管理 115
アカウント属性の操作 115
リソースグループ 116
グローバルリソースポリシー 117
追加タイムアウト値の設定 117
一括リソースアクション 118
Identity Manager ChangeLog 119
ChangeLog とは 119
ChangeLog とセキュリティー 120
ChangeLog 機能の要件 120
ChangeLog の設定 121
ChangeLog ポリシーの概要 121
ChangeLog の概要 122
ChangeLog 設定変更の保存 122
ChangeLog ポリシーの作成と編集 122
ChangeLog の作成と編集 124
例 125
例 : アイデンティティー属性の定義 125
例 : ChangeLog の設定 126
ChangeLog の CSV ファイル形式 126
列 127
行 127
テキスト値 127
バイナリ値 128
複数テキスト値 128
複数バイナリ値 128
出力形式の例 128
ChangeLog のファイル名 129
ローテーションとシーケンスの設定 129
ChangeLog スクリプトの作成 130
アイデンティティー属性およびイベントの設定 131
アイデンティティー属性の操作 131
アプリケーションの選択 134
アイデンティティー属性の追加と編集 134
ターゲットリソースの追加 135
ターゲットリソースの削除 136

アイデンティティー属性のインポート 136
アイデンティティーイベントの設定 137
Identity Manager ポリシーの設定 138
ポリシーとは 138
ポリシーでの使用禁止属性 141
辞書ポリシー 141
辞書ポリシーの設定 141
辞書ポリシーの実装 142
電子メールテンプレートのカスタマイズ 143
電子メールテンプレートの編集 144
電子メールテンプレートでの HTML 形式とリンクの使用 146
電子メール本文で使用できる変数 146
監査グループおよび監査イベントの設定 147
監査設定グループ内のイベントの編集 147
監査設定グループへのイベントの追加 147
Remedy との統合 148
Identity Manager サーバーの設定 148
調整サーバーの設定 148
スケジューラの設定 149
電子メールテンプレートサーバーの設定 149
JMX 150
サーバーのデフォルト設定の編集 150

第 5 章 管理 151
Identity Manager の管理について 152
委任された管理 152
管理者の作成 153
管理者ビューのフィルタ 155
管理者パスワードの変更 156
管理者のアクションの認証 156
秘密の質問の回答の変更 158
管理者インタフェースでの管理者名の表示のカスタマイズ 158
Identity Manager 組織について 159
組織の作成 159
組織へのユーザーの割り当て 161
キーの定義と取り込み 162
管理する組織の割り当て 163
ディレクトリジャンクションおよび仮想組織について 164
ディレクトリジャンクションのセットアップ 165
仮想組織の更新 166
仮想組織の削除 166
機能とその管理について 166
機能のカテゴリ 167

機能の操作 167
機能の作成 167
機能の編集 167
機能の保存と名前の変更 167
機能の割り当て 168
機能の階層 168
機能の定義 174
管理者ロールとその管理について 189
管理者ロールの規則 190
ユーザー管理者ロール 190
管理者ロールの作成および編集 191
「General」タブ 192
Scope of Control 193
機能の割り当て 195
管理者ロールへのユーザーフォームの割り当て 195
作業項目の管理 196
作業項目のタイプ 196
作業項目リクエストの操作 197
作業項目履歴の表示 197
作業項目の委任 198
監査ログエントリ 198
現在の委任の表示 198
以前の委任の表示 198
委任の作成 198
委任の終了 200
アカウントの承認 200
承認者のセットアップ 201
承認の署名 203
その後の承認の署名 203
デジタル署名付き承認およびアクションの設定 204
署名付き承認のためのサーバー側の設定 204
署名付き承認のためのクライアント側の設定 206
前提条件 206
手順 206
トランザクション署名の表示 207

第 6 章 データの同期と読み込み 209
データ同期ツール : 最適なツールの選択 209
検索 210
ファイルへ抽出 210
ファイルから読み込み 211
CSV ファイル形式について 211
リソースから読み込み 214

調整 215
調整ポリシーについて 216
調整ポリシーの編集 216
調整の開始 219
調整のキャンセル 219
調整ステータスの表示 219
アカウントインデックスの操作 220
アカウントインデックスの検索 220
アカウントインデックスの検査 221
アカウントの操作 221
ユーザーの操作 221
ActiveSync アダプタ 222
同期の設定 222
同期ポリシーの編集 222
ActiveSync アダプタの編集 225
ActiveSync アダプタのパフォーマンスのチューニング 225
ポーリング間隔の変更 226
アダプタを実行するホストの指定 226
開始と停止 227
アダプタログ 227

第 7 章 レポート 229
レポートの操作 229
レポート 230
レポートの作成 231
レポートの複製 232
電子メールによるレポートの送信 232
レポートの実行 232
レポートのスケジュール 232
レポートデータのダウンロード 233
レポート出力のフォントの設定 233
レポートのタイプ 234
監査 235
監査ログ 235
リアルタイム 236
概要レポート 236
システムログ 238
使用状況レポート 238
使用状況レポートのグラフ 239
リスク分析 240
システムの監視 241
追跡イベント設定 241
グラフの操作 242

定義済みのグラフの表示 242
グラフの作成 243
グラフの編集 245
グラフの削除 246
ダッシュボードの操作 246
ダッシュボードの作成 247
ダッシュボードの編集 248
ダッシュボードの削除 249
トランザクションの検索 249

第 8 章 タスクテンプレート 253
タスクテンプレートの有効化 253
タスクテンプレートの設定 256
「一般」タブの設定 258
ユーザー作成テンプレートまたはユーザー更新テンプレートの場合 258
ユーザー削除テンプレートの場合 259
「通知」タブの設定 261
管理者通知の設定 261
ユーザー通知の設定 265
「承認」タブの設定 266
承認の有効化 267
追加の承認者の指定 267
承認フォームの設定 275
「監査」タブの設定 279
「プロビジョニング」タブの設定 280
「サンライズとサンセット」タブの設定 281
サンライズの設定 282
サンセットの設定 285
「データ変換」タブの設定 286

第 9 章 PasswordSync 289
PasswordSync の概要 290
インストールの前提条件 290
Microsoft .NET 1.1 のインストール 291
PasswordSync の以前のバージョンをアンインストールする 291
PasswordSync のインストール 292
PasswordSync の設定 293
PasswordSync のデバッグ 299
エラーログ 299
トレースログ 299
レジストリキー 300
PasswordSync のアンインストール 302

PasswordSync の配備 302
JMS リスナーアダプタの設定 302
ユーザーパスワード同期ワークフローの実装 303
通知の設定 304
Sun JMS サーバーを使用した PasswordSync の設定 304
概要 305
シナリオ例 305
ソリューションの概要 305
JMS の概要 308
JMS 設定パラメータ 311
JMS プロパティーのパラメータ 313
管理オブジェクトの作成と格納 314
LDAP ディレクトリでの管理オブジェクトの格納 314
ファイルでの管理オブジェクトの格納 316
このシナリオに対する JMS リスナーアダプタの設定 318
ActiveSync の設定 320
設定のデバッグ 325
PasswordSync のフェイルオーバー配備 326
PasswordSync についてのよくある質問 328
Java Messaging Service なしで PasswordSync を実装することはできますか。 328
PasswordSync は、カスタムパスワードポリシーを施行するために使われるほかの Windows パスワードフィルタと組み合わせて使用できますか。 328
PasswordSync サーブレットを、Identity Manager と異なるアプリケーションサーバー上にインストールできますか。 329
PasswordSync サービスは lh サーバーにクリアテキストでパスワードを送信しますか。 . . . 329
パスワード変更の結果、com.waveset.exception.ItemNotLocked が発生することがありますが、それはどうしてですか。 329

第 10 章 セキュリティー 331
セキュリティー機能 332
同時ログインセッションの制限 332
パスワード管理 333
パススルー認証 334
ログインアプリケーションについて 334
ログイン制約規則 334
ログインアプリケーションの編集 335
Identity Manager セッション制限の設定 336
アプリケーションへのアクセスの無効化 336
ログインモジュールグループの編集 336
ログインモジュールの編集 337
共通リソースの認証の設定 338
X509 証明書認証の設定 339
前提条件 339

Identity Manager での X509 証明書認証の設定 340
ログイン設定規則の作成とインポート 341
SSL 接続のテスト 342
問題の診断 342
暗号化の使用と管理 343
暗号化によって保護されるデータ 343
サーバー暗号化キーに関する質問と答え 344
サーバー暗号化キーとは何ですか？ 344
サーバー暗号化キーはどこで維持管理されますか？ 344
暗号化されたデータの復号化や再暗号化にどのキーを使用するかを、サーバーはどのようにして認識するのですか？ 345
サーバー暗号化キーはどのようにして更新しますか？ 345
現在のサーバーキーが変更された場合、既存の暗号化データはどうなりますか？ 345
暗号化キーを使用できない暗号化データをインポートした場合、どのようなことが起こりますか？ 345
サーバーキーはどのように保護されますか？ 346
サーバーキーを安全な外部記憶装置にエクスポートしてもよいですか？ 346
どのデータがサーバーとゲートウェイの間で暗号化されますか？ 346
ゲートウェイキーに関する質問と答え 347
データの暗号化または復号化に使用するゲートウェイキーとは何ですか？ 347
ゲートウェイキーはどのようにしてゲートウェイに配布されますか？ 347
サーバーゲートウェイ間ペイロードの暗号化や復号化に使用するゲートウェイキーを更新できますか？ 348
ゲートウェイキーはサーバー上とゲートウェイ上のどこに格納されますか？ 348
ゲートウェイキーはどのように保護されますか？ 348
ゲートウェイキーを安全な外部記憶装置にエクスポートしてもよいですか？ 348
サーバーキーやゲートウェイキーはどのようにして破棄されますか？ 349
サーバー暗号化の管理 349
セキュリティーの実装 351
セットアップ時 351
実行時 351

第 11 章 アイデンティティー監査 353
アイデンティティー監査について 353
アイデンティティー監査の目的 354
アイデンティティー監査について 355
ポリシーベースのコンプライアンス 355
継続的コンプライアンス 355
定期的コンプライアンス 356
ポリシーベースのコンプライアンスの論理タスクフロー 357
定期的アクセスレビュー 358
監査ログの有効化 358
電子メールテンプレート 358

管理者インタフェースの「コンプライアンス」エリア 359
ポリシーの管理 359
アクセススキャンの管理 359
アクセスレビュー 360
監査ポリシーについて 360
監査ポリシー規則 360
是正ワークフロー 361
是正者 361
監査ポリシーのシナリオ例 361
監査ポリシーの操作 362
監査ポリシーの作成 362
開始する前に 363
監査ポリシーの名前と説明の指定 364
規則のタイプの選択 364
既存の規則の選択 365
是正ワークフローの選択 366
是正者と是正タイムアウトの選択 367
このポリシーにアクセスできる組織の選択 368
規則ウィザードを使用した新しい規則の作成 368
監査ポリシーの編集 372
ポリシーの編集ページ 372
「是正者」エリア 373
是正ワークフローと組織のエリア 374
サンプルポリシー 375
監査ポリシーの削除 375
監査ポリシーのトラブルシューティング 376
規則のデバッグ 376
問題 376
解決方法 376
問題 376
解決方法 376
監査ポリシーの割り当て 377
監査ポリシーのスキャンとレポート 377
ユーザーおよび組織のスキャン 377
監査レポートの操作 380
監査レポートの作成 381
コンプライアンス違反の是正と受け入れ 383
是正について 383
是正者のエスカレーション 383
是正ワークフローのプロセス 384
是正応答 385
是正電子メールテンプレート 386
「是正」ページの操作 386

ポリシー違反の表示 386
保留中のリクエストの表示 386
完了したリクエストの表示 387
テーブルの更新 388
ポリシー違反の優先度の設定 388
ポリシー違反の受け入れ 389
「是正」ページでの操作 389
ポリシー違反の是正 390
是正リクエストの転送 391
是正作業項目のユーザーの編集 391
定期的アクセスレビューとアテステーション 392
定期的アクセスレビューについて 392
アクセスレビュースキャン 393
アテステーション 393
定期的アクセスレビューの計画 395
スキャンタスクのチューニング 396
アクセススキャンの作成 397
アクセススキャンの削除 402
アクセスレビューの管理 402
アクセスレビューの起動 403
アクセスレビュータスクのスケジュール 403
アクセスレビューの進行状況の管理 404
スキャン属性の変更 405
アクセスレビューのキャンセル 405
アクセスレビューの削除 406
アテステーション作業の管理 406
アクセスレビューの通知 406
保留中のリクエストの表示 407
エンタイトルメントレコードの操作 407
クローズループ是正 407
アテステーション作業項目の転送 409
アクセスレビューアクションのデジタル署名 409
アクセスレビューレポート 410
アクセスレビュー是正 412
アクセスレビュー是正について 412
是正者のエスカレーション 412
是正ワークフローのプロセス 412
是正応答 413
「是正」ページの操作 413
サポートされないアクセスレビュー是正アクション 413
アイデンティティー監査タスクのリファレンス 414

第 12 章 監査ログ 417

概要 418
Identity Manager 監査の機能 418
イベントの作成 419
ワークフローからの監査 419
例 420
監査設定 422
filterConfiguration 423
アカウント管理 425
コンプライアンス管理 425
設定管理 425
Identity Manager ログイン / ログオフ 426
パスワード管理 426
リソース管理 426
ロール管理 427
セキュリティー管理 427
タスク管理 427
Identity Manager 外部での変更 428
Service Provider Edition 428
extendedTypes 428
extendedActions 430
extendedResults 431
publishers 432
データベーススキーマ 432
waveset.log 432
waveset.logattr 434
ログデータベースキー 435
objectType、アクション、および結果 435
理由 436
監査ログの改ざんの防止 437
改ざん防止ログの設定 437
カスタムパブリッシャーの使用 440
パブリッシャーの開発 440
ライフサイクル 440
設定 441
フォーマッタの開発 441
パブリッシャー / フォーマッタの登録 442

第 13 章 サービスプロバイダの管理 443
Service Provider 機能の概要 443
拡張エンドユーザーページ 444
パスワードとアカウント ID のポリシー 444
Identity Manager と Service Provider の同期 444
Access Manager との統合 444

初期設定 445
メイン設定の編集 445
ディレクトリ設定 446
ユーザーフォームとポリシー 447
トランザクションデータベース 448
追跡イベント設定 450
同期アカウントインデックス 451
コールアウト設定 452
ユーザー検索設定の編集 453
トランザクション管理 454
デフォルトのトランザクション実行オプションの設定 454
トランザクション持続ストアの設定 457
トランザクション処理の詳細設定 458
トランザクションの監視 460
委任された管理 463
組織認証による委任 463
管理者ロール割り当てによる委任 464
サービスプロバイダ管理者ロール委任の有効化 464
サービスプロバイダユーザー管理者ロールの設定 465
サービスプロバイダユーザー管理者ロールの委任 467
サービスプロバイダユーザーの管理 468
ユーザー組織 468
ユーザーとアカウントの作成 469
サービスプロバイダユーザーの検索 471
詳細検索 471
検索結果 472
アカウントのリンク 473
アカウントの削除、割り当て解除、またはリンク解除 474
検索オプションの設定 475
エンドユーザーインタフェース 476
サンプル 476
登録 477
ホーム画面とプロファイル画面 478
同期 479
同期の設定 480
同期の監視 480
同期の開始と停止 480
ユーザーの移行 481
サービスプロバイダ監査イベントの設定 482

付録 A　lh リファレンス 483
使用法 483
使用上の注意 483

クラス 484
コマンド 484
例 485
export コマンド 485
使用法 485
オプション 485
license コマンド 486
使用法 486
オプション 486
例 486
syslog コマンド 487
使用法 487
オプション 487

付録 B　オンラインマニュアルの高度な検索 489
ワイルドカード文字 489
クエリー演算子 490
優先度の規則 490
デフォルト演算子 490

付録 C　監査ログデータベーススキーマ 493
Oracle 493
DB2 495
MySQL 496
Sybase 498
監査ログデータベースマッピング 499

付録 D　Active Sync ウィザード 501
概要 501
同期のセットアップ 501
同期モード 501
動作設定 503
一般の Active Sync 設定 506
イベントタイプ 508
プロセスの選択 508
ターゲットリソース 510
ターゲット属性マッピング 510

索引 517

図目次

図 1-1 Identity Manager ユーザーアカウント / リソースの関係 35
図 1-2 ユーザーアカウント、ロール、リソースの関係 39
図 1-3 リソースの割り当て 40
図 2-1 Identity Manager 管理者インタフェース 48
図 2-2 ユーザーインタフェース (「ホーム」タブ): 49
図 2-3 Sun Identity Manager IDE インタフェース 52
図 2-4 Identity Manager インタフェースの「ヘルプ」ボタン 53
図 2-5 検索結果のナビゲーション 54
図 2-6 Identity Manager ヘルプ 55
図 2-7 Identity Manager ガイダンス 56
図 3-1 「ユーザーの作成」-「ID」 64
図 3-2 「ユーザーの作成」ページ ― 「コンプライアンス」タブ 67
図 3-3 アカウントリスト 69
図 3-4 ユーザーの編集 (リソースアカウントの更新) 73
図 3-5 Rename User 74
図 3-6 無効化されたアカウント 76
図 3-7 リソースアカウントの更新 78
図 3-8 ユーザーアカウントとリソースアカウントの削除 81
図 3-9 ユーザーアカウントの検索結果 83
図 3-10 ユーザーパスワードの変更 89
図 3-11 パスワードポリシー (文字タイプ) 規則 92
図 3-12 ユーザーアカウント認証 95
図 3-13 回答の変更 ― ユーザー独自の秘密の質問 95
図 3-14 エンドユーザーリソースの設定オブジェクト 98
図 4-1 リソースウィザード: リソースパラメータ 112

図 4-2 リソースウィザード : アカウント属性 (スキーママップ) 113
図 4-3 リソースウィザード : アイデンティティーテンプレート 113
図 4-4 リソースウィザード : アイデンティティーシステムのパラメータ 114
図 4-5 「一括リソースアクションの起動」ページ 118
図 4-6 「ChangeLog 設定」 121
図 4-7 メタビューでのアイデンティティー属性の設定 132
図 4-8 「リソースが変更されています」警告メッセージ 133
図 4-9 Identity Manager ポリシー 139
図 4-10 パスワードポリシーの作成 / 編集 140
図 4-11 電子メールテンプレートの編集 145
図 5-1 ユーザーアカウントの「セキュリティー」ページ : 管理者特権の指定 154
図 5-2 「組織の作成」ページ 160
図 5-3 組織の作成 : ユーザーメンバー規則の選択 161
図 5-4 Identity Manager 仮想組織 164
図 5-5 「管理者ロールの作成」ページ : 「General」タブ 192
図 5-6 「管理者ロールの作成」: 「Scope of Control」 194
図 5-7 作業項目履歴の表示 197
図 5-8 アカウント作成ワークフロー 202
図 5-9 証明書 205
図 6-1 データの読み込みに適切な形式の CSV ファイルの例 211
図 6-2 ファイルから読み込み 214
図 7-1 「レポートの実行」の選択項目 231
図 7-2 レポートのダウンロード 233
図 7-3 管理者概要レポート 237
図 7-4 使用状況レポート (生成されたユーザーアカウント) 239
図 7-5 ダッシュボードの編集 248
図 7-6 トランザクションの検索 251
図 8-1 タスクの設定 254
図 8-2 プロセスマッピングの編集ページ 254
図 8-3 「必須のプロセスマッピング」セクション 255
図 8-4 更新された「タスクの編集」テーブル 255
図 8-5 「一般」タブ : ユーザー作成テンプレート 258
図 8-6 「通知」タブ : ユーザー作成テンプレート 261
図 8-7 管理者通知 : 属性 262
図 8-8 管理者通知 : 規則 263

図 8-9 管理者通知 : クエリー 264
図 8-10 管理者通知 : 管理者リスト 265
図 8-11 電子メールテンプレートの指定 265
図 8-12 「承認」タブ : ユーザー作成テンプレート 266
図 8-13 追加の承認者 : 属性 268
図 8-14 追加の承認者 : 規則 269
図 8-15 追加の承認者 : クエリー 270
図 8-16 追加の承認者 : 管理者リスト 271
図 8-17 承認のタイムアウトのオプション 272
図 8-18 「エスカレーション承認者を決定する方法」メニュー 273
図 8-19 「エスカレーション管理者属性」メニュー 274
図 8-20 「エスカレーション管理者規則」メニュー 274
図 8-21 「エスカレーション管理者クエリー」メニュー 274
図 8-22 「エスカレーション管理者」選択ツール 275
図 8-23 「承認のタイムアウト時のタスク」メニュー 275
図 8-24 承認フォームの設定 276
図 8-25 承認属性の追加 277
図 8-26 承認属性の削除 278
図 8-27 ユーザー作成テンプレートの監査設定 279
図 8-28 属性の追加 279
図 8-29 user.global.email 属性の削除 280
図 8-30 「プロビジョニング」タブ : ユーザー作成テンプレート 281
図 8-31 「サンライズとサンセット」タブ : ユーザー作成テンプレート 282
図 8-32 新しいユーザーを 2 時間後にプロビジョニングする設定 283
図 8-33 日付による新しいユーザーのプロビジョニング 284
図 8-34 属性による新しいユーザーのプロビジョニング 284
図 8-35 規則による新しいユーザーのプロビジョニング 285
図 8-36 「データ変換」タブ : ユーザー作成テンプレート 287
図 9-1 PasswordSync 設定ダイアログ 294
図 9-2 プロキシサーバーダイアログ 295
図 9-3 JMS 設定ダイアログ 296
図 9-4 JMS プロパティーダイアログ 297
図 9-5 電子メールダイアログ 298
図 9-6 「Trace」タブ 300
図 9-7 シナリオの構成 308

図 9-8 シナリオの通信フロー 309
図 9-9 「JMS Settings」タブ 310
図 9-10 「JMS Properties」タブ 310
図 9-11 「JMS リスナーリソースパラメータ」ページ 313
図 9-12 接続ファクトリおよびデスティネーションオブジェクトの検出 314
図 9-13 「JMS リスナーアダプタリソースパラメータ」ページ 319
図 9-14 IDMAccountID とパスワードアカウント属性のマッピング 320
図 9-15 ActiveSync 属性マッピング 320
図 9-16 「同期モード」画面 321
図 9-17 「ActiveSync の動作設定」パネル 322
図 9-18 「ターゲットリソース」画面 323
図 9-19 password と accountID の定義 324
図 9-20 Sun Directory のターゲット属性マッピングの定義 324
図 9-21 テスト接続ダイアログ 325
図 9-22 デバッグ情報ファイル 326
図 9-23 PasswordSync のフェイルオーバー配備 327
図 10-1 「サーバー暗号化の管理」タスク 349
図 11-1 監査ポリシーウィザード: 名前と説明の入力画面 364
図 11-2 監査ポリシーウィザード: 規則のタイプの選択画面 365
図 11-3 監査ポリシーウィザード: 是正ワークフローの選択画面 366
図 11-4 監査ポリシーウィザード: レベル 1 是正者の選択エリア 368
図 11-5 監査ポリシーウィザード: 閲覧を許可された組織の割り当て画面 368
図 11-6 監査ポリシーウィザード: 規則の説明の入力画面 369
図 11-7 監査ポリシーウィザード: リソースの選択画面 369
図 11-8 監査ポリシーウィザード: 規則式の選択画面 370
図 11-9 「監査ポリシーの編集」ページ: 識別と規則のエリア 372
図 11-10 「監査ポリシーの編集」ページ: 是正者の割り当て 373
図 11-11 「監査ポリシーの編集」ページ: 是正ワークフローと組織 374
図 11-12 タスクの起動ダイアログ 378
図 11-13 「レポートの実行」ページの選択項目 382
図 11-14 「ポリシー違反を受け入れる」ページ 389
図 11-15 「転送先の選択と確認」ページ 391
図 11-16 「アクセスレビュー概要レポート」ページ 405
図 11-17 ユーザーエンタイトルメントレコード 411
図 12-1 監査ログの改ざんレポートの設定 438

図 12-2 改ざん防止監査ログ設定 439
図 13-1 サービスプロバイダ (SPE) 設定 (ディレクトリ、ユーザーフォームとポリシー) 446
図 13-2 サービスプロバイダの設定 (トランザクションデータベース) 449
図 13-3 サービスプロバイダの設定 (追跡イベント、アカウントインデックス、および コールアウトの設定) 450
図 13-4 検索設定 453
図 13-5 トランザクションの設定 455
図 13-6 SPE トランザクション持続ストアの設定 457
図 13-7 トランザクション処理の詳細設定 458
図 13-8 トランザクションの検索 462
図 13-9 サービスプロバイダユーザーとアカウントの作成 470
図 13-10 ユーザーの検索 472
図 13-11 検索結果の例 473
図 13-12 アカウントの削除、割り当て解除、またはリンク解除 475
図 13-13 サービスプロバイダユーザーの検索オプションの設定 476
図 13-14「登録」ページ 478
図 13-15「自分のプロファイル」ページ 479
図 13-16「Service Provider Edition 監査設定グループの編集」ページ 482
図 D-1 Active Sync ウィザード :「同期モード」、「既存のフォーム」の選択 502
図 D-2 Active Sync ウィザード :「同期モード」、「ウィザード生成のフォーム」の選択 503
図 D-3 Active Sync ウィザード : 動作設定 505
図 D-4 Active Sync ウィザード : プロセスの選択 (規則) 509
図 D-5 Active Sync ウィザード : プロセスの選択 (イベントタイプ) 509
図 D-6 Active Sync ウィザード : ターゲットリソース 510
図 D-7 Active Sync ウィザード : ターゲット属性マッピング 511

表目次

表 1 書体の表記規則 28
表 2 記号の表記規則 29
表 1-1 Identity Manager オブジェクトの関係 43
表 2-1 Identity Manager インタフェースタスクリファレンス 58
表 3-1 ユーザーアカウントステータスアイコンの説明 69
表 3-2 バックグラウンドでの保存タスクのステータスインジケータの説明 71
表 4-1 カスタムリソースクラス 109
表 4-2 変更ログの使用例でのアイデンティティー属性 125
表 4-3 電子メールテンプレート変数 146
表 5-1 Identity Manager 機能の説明 174
表 5-2 管理者ロールのサンプル規則 190
表 6-1 データ同期ツールで使用するタスク 209
表 8-1 タスクテンプレートのタブ 257
表 8-2 「追加の承認者を決定する方法」メニューのオプション 267
表 9-1 ドメインコントローラのファイル 293
表 9-2 レジストリキー 301
表 10-1 暗号化によって保護されるデータの種類 343
表 11-1 アイデンティティー監査電子メールテンプレート 358
表 11-2 監査レポートの説明 380
表 11-3 アイデンティティー監査タスクのリファレンス 414
表 12-1 com.waveset.session.WorkflowServices の引数 419
表 12-2 filterConfiguration の属性 423
表 12-3 デフォルトのアカウント管理イベントグループ 425
表 12-4 デフォルトのコンプライアンス管理イベントグループ 425
表 12-5 デフォルトの設定管理イベントグループ 425
表 12-6 デフォルトの Identity Manager ログイン / ログオフイベントグループ 426
表 12-7 デフォルトのパスワード管理イベントグループとイベント 426

表 12-8 デフォルトのリソース管理イベントグループとイベント 426
表 12-9 デフォルトのロール管理イベントグループとイベント 427
表 12-10 デフォルトのセキュリティー管理イベントグループとイベント 427
表 12-11 タスク管理イベントグループとイベント 427
表 12-12 Identity Manager 外部での変更イベントグループとイベント 428
表 12-13 Service Provider Edition イベントグループとイベント 428
表 12-14 拡張されたオブジェクトの属性 429
表 12-15 extendedAction の属性 430
表 12-16 extendedResults の属性 431
表 12-17 publishers 属性 432
表 12-18 キーとして格納される objectType、アクション、結果 435
表 12-19 キーとして格納される理由 436
表 B-1 サポートされているワイルドカード文字 489
表 B-2 オンラインマニュアル検索でよく使われるクエリー演算子 491
表 C-1 Oracle データベースタイプのデータスキーマ値 493
表 C-2 DB2 データベースタイプのデータスキーマ値 495
表 C-3 MySQL データベースタイプのデータスキーマ値 496
表 C-4 Sybase データベースタイプのデータスキーマ値 498
表 C-5 オブジェクトキータイプ、アクション、およびアクションステータスのデータベースキー 499

はじめに

このガイドでは、Sun Java™ System Identity Manager ソフトウェアを使用して、ユーザーが企業情報システムおよびアプリケーションにセキュアにアクセスする方法について説明します。また、Identity Manager システムを使用して定期的な管理タスクを実行する際に役立つ手順とシナリオも示します。

このガイドの対象読者

この『Identity Manager 管理ガイド』の対象読者は、Sun Java System サーバーおよびソフトウェアを使用して統合アイデンティティー管理と Web アクセスプラットフォームを実装する管理者、ソフトウェア開発者、および IT サービスプロバイダです。

このガイドで説明する情報を適用する場合に、次の技術の知識が役立ちます。

- Lightweight Directory Access Protocol (LDAP)
- Java テクノロジ
- JavaServer Pages™ (JSP™) テクノロジ
- ハイパーテキストトランスポートプロトコル (HTTP)
- ハイパーテキストマークアップ言語 (HTML)
- XML (Extensible Markup Language)

このガイドを読まれる前に

Identity Manager は、ネットワークまたはインターネット環境に分散したエンタープライズアプリケーションをサポートするソフトウェアインフラストラクチャーである Sun Java Enterprise System のコンポーネントです。Sun Java Enterprise System に同梱のマニュアルをよく読んでください。http://docs.sun.com/app/docs/prod/entsys.05q4 からオンラインで入手できます。

Identity Manager の配備では Sun Java System Directory Server がデータストアとして使用されるので、この製品に同梱のマニュアルをよく読んでください。Directory Server のマニュアルは、http://docs.sun.com/coll/DirectoryServer_04q2 からオンラインで入手できます。

このガイドで使用する表記規則

この節の表では、このガイドで使用する表記規則について説明します。

書体の表記規則

次の表では、このガイドで使用する書体の違いについて説明します。

表 1 書体の表記規則

書体	意味	例
AaBbCc123 (等幅フォント)	API および言語要素、HTML タグ、Web サイトの URL、コマンド名、ファイル名、ディレクトリパス名、画面上のコンピュータ出力、サンプルコード。	.login ファイルを編集してください。 すべてのファイルを一覧表示するには、ls -a を使用してください。 % You have mail.
AaBbCc123 (等幅ボールドフォント)	画面上でのコンピュータ出力と対比させたユーザー入力。	% **su** Password:
AaBbCc123 (イタリック)	実際の名前や値に置き換える、コマンドまたはパス名でのプレースホルダ。	このファイルは、*install-dir*/bin ディレクトリに置かれています。

記号

次の表は、このガイドで使用する記号の表記規則について説明します。

表 2　記号の表記規則

記号	説明	例	意味
[ ]	オプションのコマンドオプションを囲みます。	ls [-l]	-l オプションは不要です。
{ | }	必須のコマンドオプションの選択肢を囲みます。	-d {y|n}	-d オプションでは、y か n のどちらかの引数を使用する必要があります。
-	同時に行う複数のキーストロークを結び付けます。	Control-A	コントロールキーを押しながら、A キーを押します。
+	連続した複数のキーストロークを結び付けます。	Ctrl+A+N	コントロールキーを押し、コントロールキーを離してから、その後のキーを押します。
>	グラフィカルユーザーインタフェースでのメニュー項目の選択を示します。	「ファイル」>「新規」>「テンプレート」	「ファイル」メニューから「新規」を選択します。「新規」サブメニューから「テンプレート」を選択します。

関連ドキュメント

http://docs.sun.comSM Web サイトから、オンラインで Sun テクニカルドキュメントを入手できます。アーカイブを参照することも、特定の書名または題目を検索することもできます。

このマニュアルセットの内容

Sun は、Identity Manager をインストール、使用、および設定する際に役立つ以下のマニュアルと情報を提供しています。

- 『Identity Manager インストールガイド』– Identity Manager とそれに関連するソフトウェアをインストールおよび設定する手順と参照情報が記載されています。

- 『Identity Manager Upgrade』－ Identity Manager とそれに関連するソフトウェアをアップグレードおよび設定する手順と参照情報が記載されています。
- 『Identity Manager 管理ガイド』－ ユーザーが企業情報システムにセキュアにアクセスし、ユーザーのコンプライアンスを管理できるようにするための Identity Manager の使用方法に関する手順、チュートリアル、および例が記載されています。
- 『Identity Manager の配備に関する技術情報』－ Identity Manager 製品の概念に関する概要 (オブジェクトアーキテクチャーを含む) および基本的な製品コンポーネントの紹介が記載されています。
- 『Identity Manager ワークフロー、フォーム、およびビュー』－ Identity Manager のワークフロー、フォーム、およびビューの使用方法に関する参照と手順情報が記載されています。これらのオブジェクトをカスタマイズするために必要なツールに関する情報も含まれています。
- 『Identity Manager 配備ツール』－ さまざまな Identity Manager 配備ツールの使用方法に関する参照と手順情報が記載されています。規則と規則ライブラリ、共通のタスクとプロセス、辞書サポート、Identity Manager サーバーによって提供される SOAP ベースの Web サービスインタフェースなどの情報が含まれます。
- 『Identity Manager リソースリファレンス』－ リソースから Identity Manager へのアカウント情報の読み込みおよび同期方法に関する参照と手順情報が記載されています。
- 『Identity Manager Tuning, Troubleshooting, and Error Messages』－ Identity Manager のエラーメッセージと例外に関する参照と手順情報、および作業中に発生する可能性のある問題の追跡とトラブルシューティングの手順が記載されています。
- 『Identity Manager Service Provider Edition Deployment』－ Sun Java™ System Identity Manager Service Provider Edition を計画し、実装する方法を説明する参照と手順情報が記載されています。
- Identity Manager ヘルプ － Identity Manager に関する完全な手順、参照、用語情報が記載されたオンラインのガイダンスと情報です。ヘルプにアクセスするには、Identity Manager メニューバーの「ヘルプ」リンクをクリックします。重要なフィールドではガイダンス (フィールド固有の情報) が利用可能です。

Sun リソースへのオンラインアクセス

製品のダウンロード、専門的なサービス、パッチおよびサポート、追加の開発者情報については、次のサイトにアクセスしてください。

- ダウンロードセンター
  http://wwws.sun.com/software/download/

- 専門的なサービス
  http://www.sun.com/service/sunps/sunone/index.html
- Sun エンタープライズサービス、Solaris パッチ、およびサポート
  http://sunsolve.sun.com/
- 開発者情報
  http://developers.sun.com/prodtech/index.html

Sun テクニカルサポートへの問い合わせ

この製品に関する技術的な質問があり、製品マニュアルでは解決できない場合は、http://www.sun.com/service/contacting にアクセスしてください。

関連他社 Web サイトの参照について

このマニュアルで取り上げる他社の Web サイトが使用可能かどうかについて、Sun は関知いたしません。これらのサイトまたはリソースで利用できるコンテンツ、広告、製品、その他の要素について、Sun は保証せず、責任も義務も負いません。Sun は、これらのサイトまたはリソースから利用できるこのようなコンテンツ、商品、またはサービスを使用または信用した結果、またはそれに関連して生じた、または生じたと主張する損害または損失に対して、実際のものか主張されたものかにかかわらず、責任も義務も負わないものとします。

ご意見をお寄せください

Sun はマニュアルの改善に取り組んでおり、皆様のご意見、ご提案をお待ちしております。

ご意見をお寄せいただくには、http://docs.sun.com にアクセスし、「コメントの送信」をクリックしてください。オンラインフォームには、マニュアルのタイトルとパーツ番号を記入してください。パーツ番号は、マニュアルのタイトルページまたはドキュメントの最上部に表示されている 7 桁の番号です。

たとえばこのマニュアルのタイトルは『Sun Java System Identity Manager 7.1 管理ガイド』であり、パーツ番号は 820-2289 です。

ご意見をお寄せください

第 1 章

Identity Manager の概要

Sun Java™ System Identity Manager システムを使用すると、アカウントおよびリソースへのアクセスをセキュアかつ効率的に管理し、監査することができます。Identity Manager は、定期的な日常のユーザープロビジョニングタスクおよび監査タスクを迅速に処理する機能とツールをユーザーに提供することで、内部および外部顧客に対して格別なサービスを容易に実行できるようにします。

この章では、概要について説明します。以下のトピックで構成されています。

- 全体像
- Identity Manager オブジェクト

全体像

今日のビジネスでは、IT サービスの柔軟性と機能性のさらなる向上がリクエストされます。これまで、ビジネス情報およびシステムへのアクセス管理には、限られた数のアカウントとの直接的な対話しか必要ありませんでした。ところが、アクセス管理は次第に、増大する内部顧客の処理のみならず、企業外のパートナーや顧客の処理も意味するようになってきました。

このようなアクセスニーズの増大によって生ずるオーバーヘッドは、膨大なものになる可能性があります。管理者は、ユーザー (企業内外の) が効果的かつセキュアに自分の任務を果たせるようにしなければなりません。さらに、最初のアクセスのあとには、パスワードの忘失、ロールやビジネス上の関係の変更、といった詳細な問題に次々に直面します。

さらに、今日のビジネスは重要なビジネス情報のセキュリティーと完全性を管理する厳しいリクエストに直面しています。米国企業改革 (SOX) 法、HIPAA 法 (医療保険の携行性と責任に関する法律)、GLB 法 (グラムリーチブライリー法) などコンプライアンスに関連する法律の影響を受ける環境では、活動の監視とレポートによって生み出されるオーバーヘッドは、膨大でコストがかかります。ビジネスの安全を確保するために、データ収集とレポートの要件を満たしながら、アクセス管理の変化にすばやく対応できるようにしておく必要があります。

Identity Manager は、動的な環境におけるこのような管理上の課題を解決する際に特に役立つように開発されました。Identity Manager を使用して、アクセス管理のオーバーヘッドを分散させ、コンプライアンスの負荷に対処することにより、アクセスをどのように定義するか、定義したあとに柔軟性と管理をどのようにして維持するか、という主要な課題が解決しやすくなります。

セキュアでありながら柔軟な設計の Identity Manager は、企業の構造に適応し、これらの課題に対処するようにセットアップできます。Identity Manager オブジェクトを管理対象のエンティティー (ユーザーおよびリソース) にマップすることにより、操作の効率は飛躍的に向上します。

サービスプロバイダ環境で、Identity Manager はこれらの機能をエクストラネットユーザーも管理するように拡張しました。

Identity Manager システムの目的

Identity Manager ソリューションでは次の目的を達成することができます。

- 多種多様なシステムおよびリソースに対するアカウントアクセスを管理する。
- 各ユーザーのアカウント配列に対する動的なアカウント情報をセキュアに管理する。
- ユーザーアカウントデータの作成および管理に対する委任された権限をセットアップする。
- 多数の企業リソースと、ますます増大するエクストラネット顧客およびパートナーを処理する。
- 企業情報システムへのユーザーアクセスをセキュアに承認する。Identity Manager では、組織内外でのアクセス特権の許可、管理、および失効の機能が完全に統合される。
- データを保持することなくデータの同期を維持する。Identity Manager ソリューションは、優れたシステム管理ツールで監視する必要のある 2 つの主要な原則をサポートする。
    - 管理対象システムへの製品の影響を最低限に抑える必要がある
    - 製品が別の管理リソースを追加することで、企業環境が複雑になってはならない

- ユーザーアクセス特権のコンプライアンスを管理し、自動是正措置と電子メール警告で違反を管理する監査ポリシーを定義する。
- 定期的アクセスレビューを行い、ユーザー特権を保証するプロセスを自動化するアテステーションレビューと承認手順を定義する。
- 主要な情報を監視し、ダッシュボードを使用して統計を監査し、レビューする。

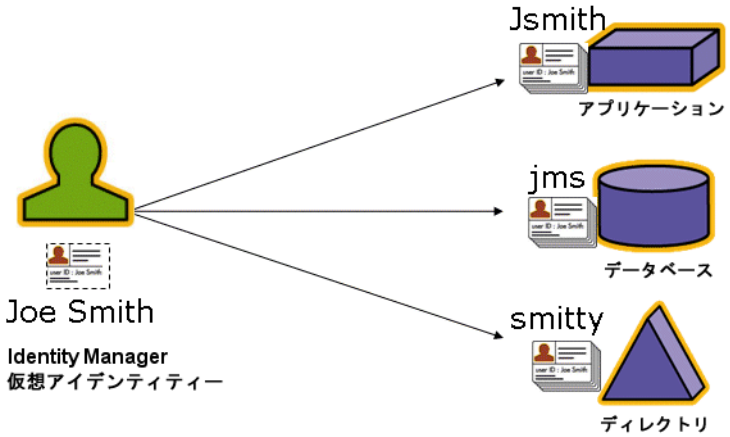
ユーザーアクセスの定義

拡張された企業内のユーザーとは、企業と関係を持つすべてのユーザーのことです。たとえば、従業員、顧客、パートナー、サプライヤ、買収者などです。Identity Manager システムでは、ユーザーはユーザーアカウントによって表されます。

ビジネスおよびほかのエンティティーとの関係に応じて、ユーザーは、コンピュータシステム、データベースに保存されたデータ、または特定のコンピュータアプリケーションなど、さまざまなものにアクセスする必要があります。Identity Manager では、これらをリソースと呼びます。

ユーザーは、アクセスするリソースごとに 1 つ以上の ID を持っていることが多くあるため、Identity Manager は、異種のリソースにマップされる単一の仮想 ID を作成します。これにより、ユーザーを単一のエンティティーとして管理できるようになります。図 1-1 を参照してください。

図 1-1 Identity Manager ユーザーアカウント / リソースの関係



多数のユーザーを効果的に管理するには、ユーザーをグループ化する論理的な方法が必要です。ほとんどの企業では、ユーザーは職務上の部署または地域的な部門にグループ化されています。通常、このような部署はそれぞれ、異なるリソースにアクセスする必要があります。Identity Manager では、このようなタイプのグループを組織と呼びます。

ユーザーをグループ化するもう 1 つの方法は、企業での関係または任務機能などの類似した特性でグループ化することです。Identity Manager ではこのようなグループ化をロールと呼びます。

Identity Manager システムでは、ユーザーアカウントにロールを割り当てて、リソースへのアクセスを効率的に有効化または無効化します。組織にアカウントを割り当てることにより、管理の役割の委任を効率的に行うことができます。

ポリシーを適用することによって、Identity Manager ユーザーを直接または間接的に管理することもできます。ポリシーは、規則およびパスワードと、ユーザー認証オプションをセットアップします。

ユーザータイプ

Identity Manager には、Identity Manager ユーザーと、Identity Manager システムをサービスプロバイダ実装用に設定する場合のサービスプロバイダユーザーという 2 つのユーザータイプが用意されています。これらのタイプを使用すると、ユーザーと企業との関係に基づきプロビジョニング要件が異なる可能性のあるユーザーを区別できます (たとえば、エクストラネットユーザーとイントラネットユーザーを区別)。

サービスプロバイダ実装の一般的なシナリオは、サービスプロバイダ企業が内部ユーザーと外部ユーザー (顧客) を Identity Manager で管理するケースです。サービスプロバイダを実装するための設定の詳細については、『Identity Manager SPE Deployment』を参照してください。

ユーザーアカウントを設定する場合は、Identity Manager ユーザータイプを指定します。サービスプロバイダユーザーの詳細については、第 13 章「サービスプロバイダの管理」を参照してください。

管理の委任

ユーザーアイデンティティーマネージメントの役割の分散を成功させるには、柔軟性と管理の適切なバランスを取る必要があります。選択した Identity Manager ユーザーに管理者特権を与えて管理タスクを委任することにより、管理者のオーバーヘッドが軽減します。さらに、人事部長など、ユーザーニーズを熟知したユーザーにアイデンティティー管理の役割を与えることにより、効率が向上します。このような拡張特権を持つユーザーを、Identity Manager 管理者と呼びます。

ただし、委任はセキュアなモデル内でのみ有効です。適切な管理レベルを維持するために、Identity Manager は管理者に異なるレベルの機能を割り当てることができます。機能は、システム内でのさまざまなレベルのアクセスおよび操作を承認します。

また、Identity Manager ワークフローモデルにも、特定の操作に承認が必要かどうかを確認する方法が含まれています。Identity Manager 管理者は、ワークフローを使用してタスクの管理権限を保有し、その進行状況を追跡できます。ワークフローの詳細については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

Identity Manager オブジェクト

Identity Manager オブジェクトとその操作の方法を明確に理解することは、システムの管理と導入を成功させるために不可欠です。オブジェクトには次のものがあります。

- ユーザーアカウント
- ロール
- リソースとリソースグループ
- 組織と仮想組織
- ディレクトリジャンクション
- 機能
- 管理者ロール
- ポリシー
- 監査ポリシー

ユーザーアカウント

Identity Manager ユーザーアカウント

- 1 つ以上のリソースにユーザーアクセスを提供し、それらのリソースのユーザーアカウントデータを管理する。
- ロールを割り当てる。これにより、さまざまなリソースへのユーザーアクセスが設定されます。
- 組織の一部を構成する。これにより、ユーザーアカウントの管理方法と管理者が決定されます。

ユーザーアカウントのセットアッププロセスは動的です。アカウントのセットアップで選択したロールに応じて、アカウントを作成するためのリソース固有の情報が増減する可能性があります。割り当てられたロールに関連付けられたリソースの数とタイプによって、アカウント作成時に必要な情報が決まります。

ユーザーに管理特権を与えて、ユーザーアカウント、リソース、およびほかの Identity Manager システムオブジェクトとタスクを管理できます。Identity Manager 管理者は組織を管理し、管理対象の各組織内のオブジェクトに適用する一連の機能を割り当てられます。

ロール

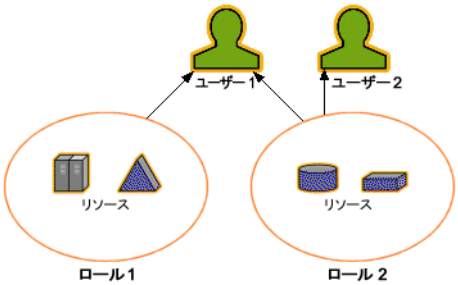
ロールは Identity Manager ユーザータイプを表す Identity Manager オブジェクトであり、リソースのグループ化とユーザーへの割り当てを許可します。通常、ロールはユーザーの任務機能を表します。たとえば金融機関では、ロールは出納係、融資担当者、支店長、窓口担当、経理担当者、管理補佐などに対応します。

ロールは、ユーザーに対するリソースおよびリソース属性の基本的なセットを定義します。また、ほかのロールとの関係、たとえばほかのロールを含むか除外するかなども定義できます。

同じロールを持つユーザーは、リソースに共通のベースグループへのアクセスを共有します。各ユーザーに 1 つ以上のロールを割り当てることも、ロールを割り当てないこともできます。

図 1-2 に示すように、ユーザー 1 とユーザー 2 は、ロール 2 の割り当てによって同じリソースセットへのアクセスを共有しています。ただし、ユーザー 1 はロール 1 の割り当てによってほかのリソースにもアクセスできます。

図 1-2　　ユーザーアカウント、ロール、リソースの関係



リソースとリソースグループ

Identity Manager リソースには、アカウントが作成されるリソースまたはシステムへの接続方法についての情報が格納されています。Identity Manager がアクセスを提供するリソースは、次のとおりです。

- メインフレームセキュリティーマネージャー
- データベース
- ディレクトリサービス (LDAP など)
- アプリケーション
- オペレーティングシステム
- ERP システム (SAP™ など)

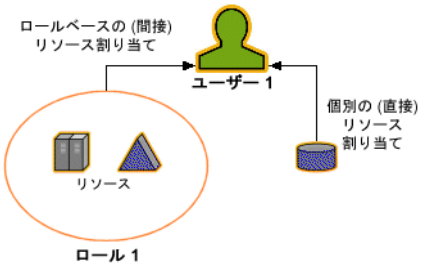
各 Identity Manager リソースに格納されている情報は、次の主要なグループに分類されます。

- リソースパラメータ
- アカウント情報 (アカウント属性とアイデンティティーテンプレートを含む)
- Identity Manager パラメータ

Identity Manager ユーザーアカウントは、図 1-3 に示すように次の割り当てによってリソースにアクセスできます。

- ロールベースの割り当て ― ユーザーにロールを割り当てることにより、そのロールに関連付けられた 1 つ以上のリソースが間接的にそのユーザーに割り当てられます。
- 個別の割り当て ― 個別のリソースを直接ユーザーアカウントに割り当てることができます。

図 1-3　　リソースの割り当て



関連する Identity Manager オブジェクトであるリソースグループを、リソースの割り当てと同じ方法でユーザーアカウントに割り当てることができます。リソースグループは、リソースを相互に関連付けて、アカウントを特定の順序でリソース上に作成できるようにします。また、複数のリソースのユーザーアカウントへの割り当てプロセスを簡素化します。リソースグループの詳細については、116 ページの「リソースグループ」を参照してください。

組織と仮想組織

組織とは、管理の委任を可能にするために使用される Identity Manager コンテナです。組織は、Identity Manager 管理者が管理するエンティティーの範囲を定義します。

また、組織は、ディレクトリベースのリソースへの直接のリンクも表します。これらは仮想組織と呼ばれます。仮想組織を使用すると、情報を Identity Manager リポジトリに読み込まずに、リソースデータを直接管理できます。Identity Manager では、仮想組織を使用して既存のディレクトリ構造とメンバーシップをミラー化することにより、セットアップタスクの重複と時間の浪費をなくします。

ほかの組織を含む組織は、親組織です。組織はフラットな構造に作成することも、階層構造として作成することもできます。階層構造は、ユーザーアカウントを管理するための部署、地域、またはその他の論理的な部門を表します。

ディレクトリジャンクション

ディレクトリジャンクションは、階層的に関係する組織のセットであり、ディレクトリリソースの実際の階層構造コンテナのセットをミラー化したものです。ディレクトリリソースは、階層構造コンテナを使用して、階層構造の名前空間を使用するリソースです。ディレクトリリソースの例には、LDAP サーバーおよび Windows Active Directory リソースがあります。

ディレクトリジャンクション内の各組織は、仮想組織です。ディレクトリジャンクションの最上位の仮想組織は、リソース内に定義されたベースコンテキストを表すコンテナをミラー化したものです。ディレクトリジャンクション内の残りの仮想組織は、最上位の仮想組織の直接または間接的な子であり、定義済みリソースのベースコンテキストコンテナの子であるディレクトリリソースコンテナのいずれかをミラー化しています。

Identity Manager ユーザーを、組織と同様の方法で仮想組織のメンバーにして、仮想組織から使用可能にすることができます。

機能

機能、つまり権限のグループが割り当てられたユーザーは、Identity Manager の管理操作を実行できるようになります。機能によって、管理ユーザーはシステム内で特定のタスクを実行したり、さまざまな Identity Manager オブジェクトを操作したりすることができます。

通常、機能は、パスワードのリセットまたはアカウントの承認など、特定のジョブの役割に従って割り当てられます。個別のユーザーに機能と権限を割り当てることにより、管理の階層構造が作成され、データの保護をおびやかすことなく、対象を絞ったアクセスと特権を提供することができます。

Identity Manager では、一般的な管理機能用のデフォルト機能のセットを提供しています。また、特定のニーズを満たす機能を作成して割り当てることもできます。

管理者ロール

管理者ロールを使用すると、管理ユーザーが管理している組織を組み合わせて、その組み合わせごとに一意の機能セットを定義できます。管理者ロールに機能および管理する組織を割り当ててから、その管理者ロールを管理ユーザーに割り当てることができます。

機能および管理する組織は、管理者ロールに直接割り当てることができます。また、管理ユーザーが Identity Manager にログインしたときに、間接的 (動的) に割り当てることもできます。Identity Manager 規則によって、動的に権限が割り当てられます。

ポリシー

アカウント ID、ログイン、およびパスワードの特性に関する制約をポリシーとして設定することによって、Identity Manager ユーザーに関する制限事項を設定します。アイデンティティーシステム アカウントポリシーは、ユーザー、パスワード、および認証ポリシーのオプションと制約を設定します。リソースパスワードとアカウント ID ポリシーは、長さ規則、文字タイプ規則、許容される単語や属性値を設定します。辞書ポリシーを使用すると、Identity Auditor は単語データベースと照合してパスワードをチェックすることができ、簡単な語句を使った辞書攻撃から保護することができます。

監査ポリシー

ほかのシステムポリシーとは異なり、監査ポリシーは特定のリソースのユーザーグループのポリシー違反を定義します。監査ポリシーは、1 つまたは複数の規則を設定し、これによってユーザーのコンプライアンス違反を評価します。これらの規則は、リソースによって定義された 1 つまたは複数の属性に基づく条件によって決まります。システムがユーザーをスキャンする場合、そのユーザーに割り当てられた監査ポリシーで定義された条件を使用し、コンプライアンス違反が発生しているかどうかを判断します。

オブジェクトの関係

以下の表は、Identity Manager オブジェクトおよびオブジェクト間の関係を示しています。

表 1-1 Identity Manager オブジェクトの関係

Identity Manager オブジェクト	説明	適用対象
ユーザーアカウント	Identity Manager および 1 つ以上のリソース上にあるアカウント。 ユーザーデータをリソースから Identity Manager に読み込むことができます。 特別なユーザークラスである Identity Manager 管理者は拡張特権を持ちます。	ロール 通常、各ユーザーアカウントには 1 つ以上のロールが割り当てられます。 組織 ユーザーアカウントは、組織の一部として階層構造に配置されます。Identity Manager 管理者は、さらに組織を管理します。 リソース 個別のリソースを、ユーザーアカウントに割り当てることができます。 機能 管理者には、自分が管理する組織に対する機能が割り当てられます。
ロール	ユーザークラスのプロファイルを作成し、アカウントが管理するリソースおよびリソース属性の集まりを定義します。	リソースとリソースグループ リソースとリソースグループにはロールが割り当てられます。 ユーザーアカウント ロールは、類似した特性を持つユーザーアカウントをグループ化します。 ロール ほかのロールとの間の関係 (含むまたは含まない) を定義します。

表 1-1　Identity Manager オブジェクトの関係 (続き)

Identity Manager オブジェクト	説明	適用対象
リソース	アカウントが管理するシステム、アプリケーション、またはほかのリソースについての情報を格納します。	ロール リソースにはロールが割り当てられます。ユーザーアカウントは、ロール割り当てのリソースアクセスを「継承」します。 ユーザーアカウント リソースをユーザーアカウントに個別に割り当てることができます。
リソースグループ	順序付けされたリソースのグループ。	ロール リソースグループにはロールが割り当てられます。ユーザーアカウントは、ロール割り当てのリソースアクセスを「継承」します。 ユーザーアカウント リソースグループをユーザーアカウントに直接割り当てることができます。
組織	管理者により管理されるエンティティーの範囲を階層構造で定義します。	リソース ある組織内の管理者は、すべてまたは一部のリソースにアクセスできる可能性があります。 管理者 組織は、管理特権を持つユーザーによって管理 (制御) されます。管理者は 1 つ以上の組織を管理できます。ある組織内の管理特権は、子の組織にも継承されます。 ユーザーアカウント 各ユーザーアカウントは、Identity Manager 組織および 1 つ以上のディレクトリ組織に割り当てることができます。
ディレクトリジャンクション		

表 1-1 Identity Manager オブジェクトの関係 (続き)

Identity Manager オブジェクト	説明	適用対象
管理者ロール	管理者に割り当てられた組織の組み合わせごとに、一意の機能セットを定義します。	管理者 管理者ロールは管理者に割り当てられます。 機能と組織 機能と組織は、直接的または間接的 (動的) に管理者ロールに割り当てられます。
機能	システム権限のグループを定義します。	管理者 機能は管理者に割り当てられます。
ポリシー	パスワードおよび認証の制限を設定します。	ユーザーアカウント ポリシーはユーザーアカウントに割り当てられます。 組織 ポリシーは組織に割り当てられるか、継承されます。
監査ポリシー	ユーザーのコンプライアンス違反を評価する規則を設定します。	ユーザーアカウント 監査ポリシーはユーザーアカウントに割り当てられます。 組織 監査ポリシーは組織に割り当てられます。

第 2 章

Identity Manager 入門

この章では、Identity Manager グラフィカルインタフェースと、Identity Manager をすぐに使用するための方法について説明します。この章は、次のトピックで構成されます。

- Identity Manager インタフェース
- ヘルプとガイダンス
- Identity Manager タスク
- 以降の操作について

Identity Manager インタフェース

Identity Manager システムには 3 つの主要なグラフィカルインタフェースがあり、ユーザーはそのインタフェースを通じてタスクを実行します。

- 管理者インタフェース
- ユーザーインタフェース
- Identity Manager IDE

Identity Manager 管理者インタフェース

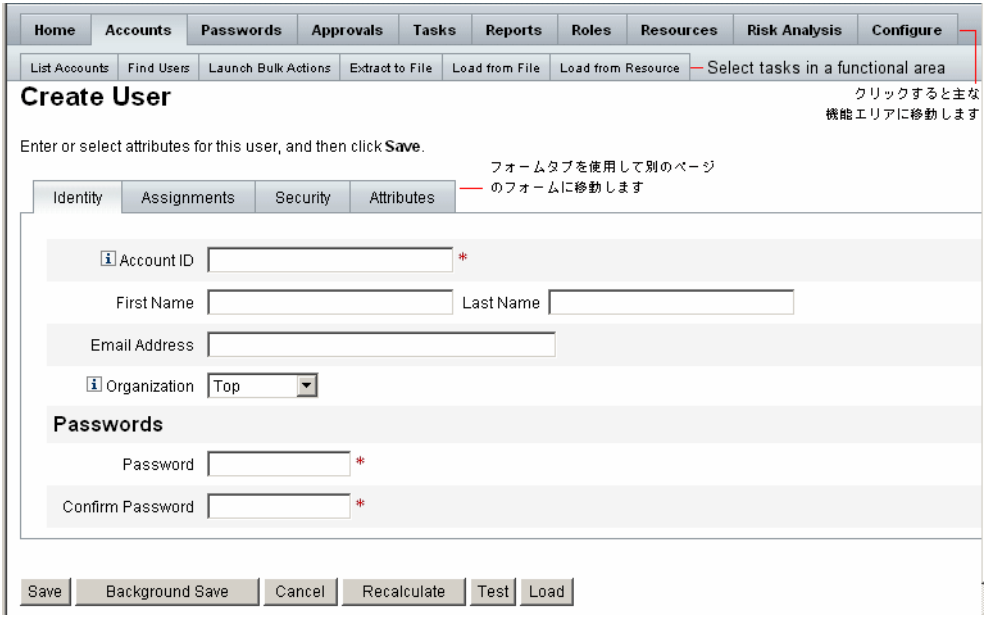
Identity Manager 管理者インタフェースは、製品の主要な管理ビューとして機能します。Identity Manager 管理者は、このインタフェースを通じてユーザーを管理し、リソースのセットアップおよび割り当てを行い、権限とアクセスレベルを定義し、Identity Manager システム内のコンプライアンスを監査します。

インタフェースは、次の要素から構成されます。

- **ナビゲーションバータブ** – 各インタフェースページの上部にあります。これらのタブを使用して、主な機能エリアに移動できます。
- **サブタブまたはメニュー** – ユーザーの実装方法に応じて、各ナビゲーションバータブの下に二次的なタブまたはメニューが表示されます。これらのサブタブまたはメニューを選択して、機能エリア内のタスクにアクセスできます。

「アカウント」など、一部のエリアでは、フォーム内をより簡単に移動できるように、長いフォームがタブ付きのフォームによって 1 ページ以上に分割されています。この画面を図 2-1 に示します。

図 2-1　　Identity Manager 管理者インタフェース



管理者インタフェースへのログオン

管理者インタフェースにログオンする場合、個々の実装に設定されたセッション制限に従ってログオンが維持されますが、例外が 1 つあります。Web ブラウザで Cookie が無効になっている場合、次の操作を行うとセッション中に再ログインするように求められます。

- 管理者、ロール、組織の名前変更のキャンセル
- 組織の削除のキャンセル
- ユーザーログインモジュールおよび管理者ログインモジュールの作成

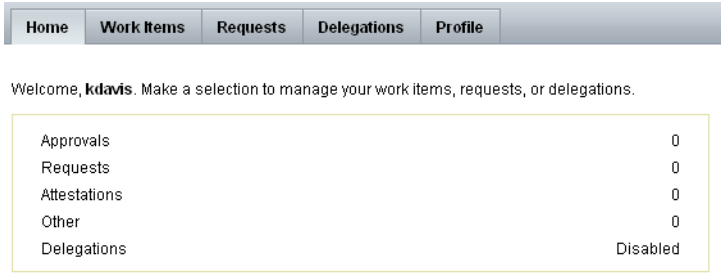
複数回ログインしなくて済むようにするには、Cookie を有効にします。

Identity Manager ユーザーインタフェース

Identity Manager ユーザーインタフェースには、Identity Manager システムの制限されたビューが表示されます。このビューは、管理機能を持たないユーザー用に調整されています。

ユーザーが Identity Manager ユーザーインタフェースにログインすると、次の図に示すように、そのユーザーの保留中の作業項目と委任が「ホーム」タブに表示されます。

図 2-2　ユーザーインタフェース (「ホーム」タブ):



「ホーム」タブを使用すると、保留中の項目にすばやくアクセスできます。作業項目リクエストに応答するか、ほかの可能な操作を実行するには、リスト内の項目をクリックします。操作が完了したあと、「メインメニューに戻る」をクリックして、「ホーム」ページに戻ります。

ユーザーは、パスワードの変更、セルフプロビジョニングタスクの実行、作業項目と委任の管理など、さまざまなアクティビティーをユーザーインタフェースから実行できます。

ユーザーは、次のオプションをユーザーインタフェースから使用できます。

- **「作業項目」** – 所有している、または操作権限を持っている保留中の作業項目を承認または却下します。

  作業項目には、承認、アテステーション、または Identity Manager から発生したその他のリクエストされたアクションアイテムを含めることができます。

- **「リクエスト」** – ユーザーアカウントへのリソースの割り当ておよびロールの割り当てに対する更新のリクエストを送信します。

  これらのリクエストは、ユーザーまたは従業員に対して実行できます。

  「リクエスト」タブの「表示」サブタブを使用して、リクエストのプロセスステータスの詳細を表示します。

- **「委任」** – 現在の委任を表示したり、委任を指定したりします。
- **「プロファイル」** – 次のサブタブを使用してユーザーパスワードやアカウント属性を変更したり、その他のセルフプロビジョニングタスクを実行したりします。
  - **「パスワードの変更」** – 選択したリソースまたはすべてのリソース上でパスワードを変更する場合にこのオプションを選択します。
  - **「アカウント属性」** – 自分のアカウントの電子メールアドレス (これは、Identity Manager がアカウントについての通知を送信するために使用する電子メールアドレス) など、ユーザーが編集可能な属性を変更する場合にこのオプションを選択します。
  - **「秘密の質問」** – 自分のユーザーアカウントの秘密の質問に対する回答を変更する場合にこのオプションを選択します。
  - **「アクセス特権」** – このアカウントの (直接または間接的な) リソース割り当てを表示する場合にこのオプションを選択します。

ユーザーインタフェースのカスタマイズ

ユーザーインタフェースは通常、企業固有のビューを表示し、カスタム選択を提供するようにカスタマイズされます。

ナビゲーションレイアウトのカスタマイズ

好みに応じて、ユーザーインタフェースのナビゲーションを水平タブ表示 (デフォルト) から垂直ツリー表示に変更できます。垂直ナビゲーション表示を設定するには、次の設定オブジェクトを設定します。

```
ui.web.user.menuLayout = 'vertical'
```

ユーザーインタフェースのカスタマイズおよびブランド設定の詳細については、『Identity Manager の配備に関する技術情報』を参照してください。

ダッシュボード表示オプションのカスタマイズ

管理者インタフェースから、ユーザーダッシュボードに表示するオプションを選択できます。表示オプションを設定するには、「設定」を選択し、「ユーザーインタフェース」を選択します。

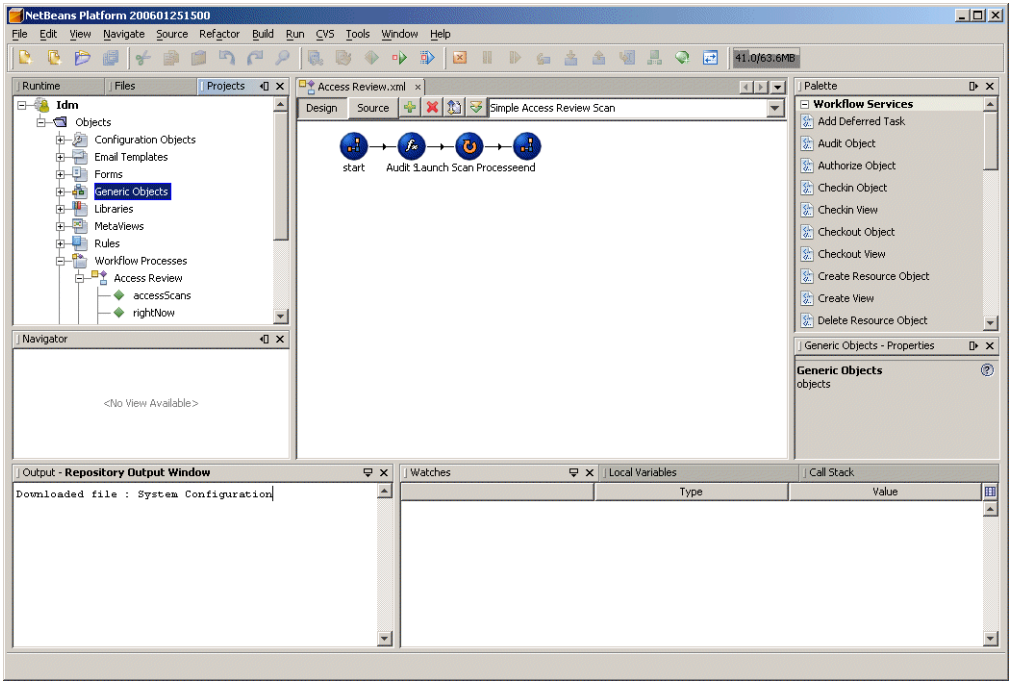
デフォルトでは、利用できる設定可能なすべての情報がユーザーダッシュボードに表示されます。次のオプションの 1 つまたは複数を選択解除し、情報を表示しないようにできます。

- displayPasswordExpirationWarning − パスワードポリシーをアカウントに適用するとき、パスワードの有効期限に関するメッセージを表示する場合に選択します。
- displayAttestationReviews − アテステーション作業項目数を表示する場合に選択します。
- displayOtherWorkItems − その他の作業項目の数を表示する場合に選択します。
- displayRemediations − 是正作業項目数を表示する場合に選択します。
- displayApprovals − 承認作業項目数を表示する場合に選択します。
- displayLoginFailures − パスワードまたは秘密の質問によるログイン試行の失敗回数を表示する場合に選択します。ユーザーのアカウントポリシーにログイン失敗の限度が設定されている場合にのみ、表示されます。
- displayDelegations − ユーザーが承認の委任を定義したことを示す文字列を表示する場合に選択します。
- displayRequests − アカウントのロール、グループ、またはリソースの更新に対する未処理の要求の数を表示する場合に選択します。

Identity Manager IDE

Sun Identity Manager Integrated Development Environment (IDE) は、Identity Manager のフォーム、規則、およびワークフローをグラフィカルに表示します。IDE を使用して、Identity Manager の各ページで使用可能な機能を設定するフォームを作成および編集することができます。また、Identity Manager ワークフローを修正することもできます。ワークフローには、Identity Manager ユーザーアカウントを使用するときに適用する一連の処理手順や実行するタスクを定義します。さらに、ワークフローの動作を定める、Identity Manager で定義した規則も変更できます。次の図に IDE インタフェースを示します。

図 2-3　　Sun Identity Manager IDE インタフェース



IDE の詳細と、Identity Manager のフォームとワークフローでの IDE の使用方法については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

以前のバージョンの Identity Manager でインストールしている場合は、Business Process Editor (BPE) を使用してカスタマイズを行うこともできます。

ヘルプとガイダンス

タスクを正常に実行するために、ヘルプおよび Identity Manager ガイダンス (フィールドレベルの情報および指示) を参照しなければならないことがあります。ヘルプとガイダンスは、Identity Manager 管理者インタフェースとユーザーインタフェースから使用可能です。

Identity Manager ヘルプ

タスクに関するヘルプと情報を表示するには、図 2-4 に示すように、管理者インタフェースおよびユーザーインタフェースの各ページの上部にある「ヘルプ」ボタンをクリックします。

図 2-4　　Identity Manager インタフェースの「ヘルプ」ボタン

各ヘルプウィンドウの下部には「目次」リンクがあり、ほかのヘルプトピックや Identity Manager 用語の用語集に移動できます。

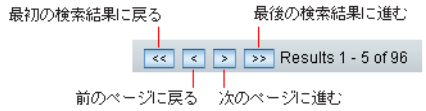
情報の検索

ヘルプウィンドウで検索機能を使用して、Identity Manager のヘルプおよびマニュアルに含まれるトピックと情報を検索できます。オンラインマニュアルを検索するには、次の手順に従います。

1. 検索エリアに、1 つ以上の単語を入力します。
2. 2 つのドキュメントタイプのどちらを検索するかを選択します。デフォルトでは、オンラインヘルプが検索されます。
   - **「オンラインヘルプ」** ― 一般的に、オンライン情報には、タスクの実行またはフォームの入力に役立つ手順が記載されています。
   - **「マニュアル」** (ガイド) ― Identity Manager ガイドには主に、概念やシステムオブジェクトを理解するために役立つ情報および完全なリファレンス情報が記載されています。
3. 「検索」をクリックします。

リンク付きの検索結果が表示されます。リストされた結果の間を移動するには、図 2-5 に示すように、「前へ」 / 「次へ」または「先頭」 / 「最後」ボタンを使用します。

図 2-5　検索結果のナビゲーション



「リセット」をクリックすると、ヘルプウィンドウの内容がクリアされます。

検索の動作

複数の単語を検索すると、各単語、すべての単語、および変化形を含む検索結果が返されます。

たとえば、次の語句を入力したとします。

```
resource adapter
```

この場合、検索結果では、次の語に一致するものが返されます。

- `resource` (およびその変化形)
- `adapter` (およびその変化形)
- `resource` および `adapter` (順不同で、間に 0 から *n* 個の単語を含む)

ただし、検索語句を引用符で囲んだ場合 ("resource adapter" など) は、その語句に完全に一致するもののみが返されます。

また、高度なクエリー構文を使用して、クエリー要素を明示的に含める、除外する、または並べ替えることもできます。

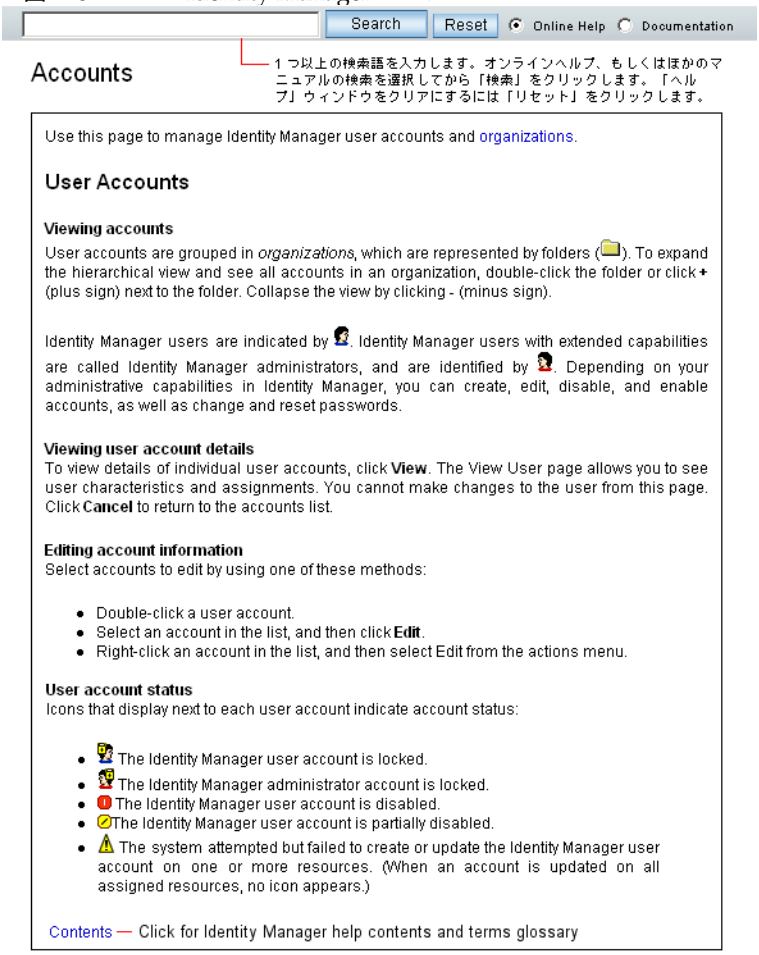
高度なクエリー構文

検索機能では、次を含む高度なクエリー構文がサポートされています。

- **ワイルドカード文字** (? と *)。完全な単語や語句ではなく、綴りのパターンを指定できます。
- **クエリー演算子** (AND または OR)。クエリー要素の結合方法を指定できます。

Identity Manager の高度なマニュアル検索機能の詳細については、このガイドの付録 B「オンラインマニュアルの高度な検索」を参照してください。

図 2-6 Identity Manager ヘルプ

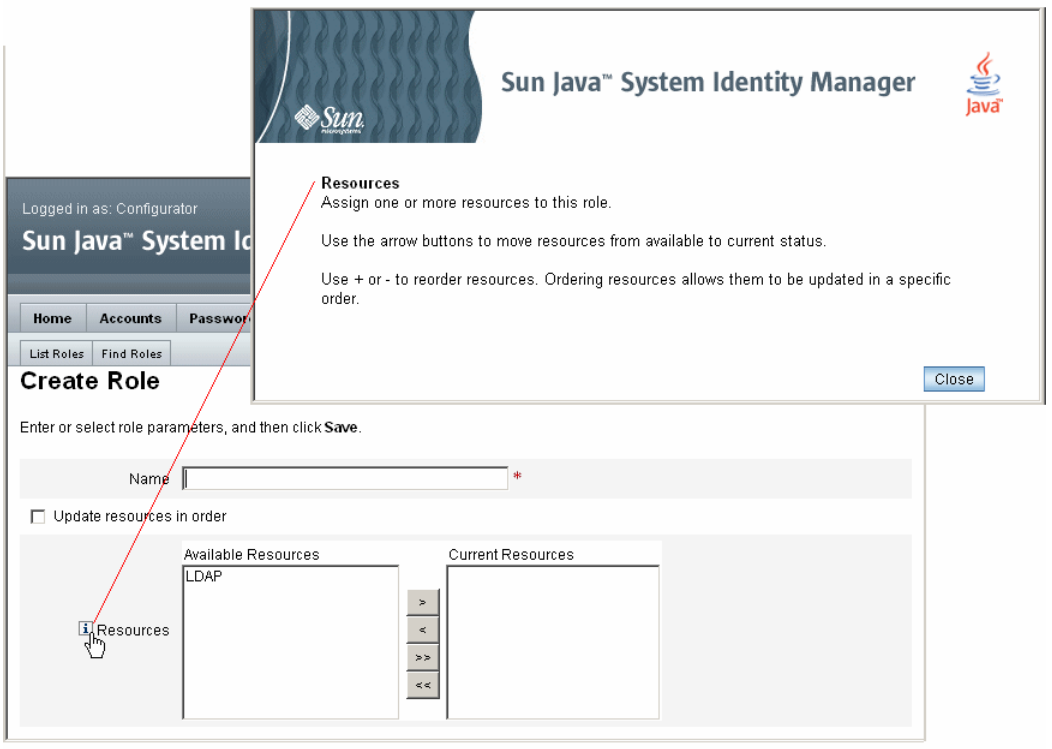


Identity Manager ガイダンス

Identity Manager ガイダンスは、簡潔で、対象を絞ったヘルプであり、多くのページでフィールドの横に表示されます。その目的は、タスクを実行するためにページで情報を入力および選択する際に、作業を容易にすることです。

ガイダンスのあるフィールドの横には、文字「i」で示された記号が表示されます。この記号をクリックすると、ウィンドウが開き、そのフィールドに関する情報が表示されます。

図 2-7　　Identity Manager ガイダンス



Identity Manager へのログイン

Identity Manager 管理者またはユーザーインタフェースにログインするには、ユーザー ID とパスワードを入力し、「ログイン」をクリックします。

ユーザー ID を忘れた場合

ユーザー ID を忘れた場合は、ログインページから「ユーザー ID をお忘れですか ?」をクリックすることで、ユーザー ID を取得できます。問い合わせページが表示され、姓と名、電子メールアドレス、電話番号など、アカウントに関連付けられたアイデンティティー属性情報を求められます。

Identity Manager は、入力された値に一致する 1 人のユーザーを見つけるクエリーを作成します。一致するユーザーが見つからない場合、または複数のユーザーが見つかった場合、「ユーザー ID の問い合わせ」ページにエラーメッセージが表示されます。

デフォルトで、問い合わせ機能は有効になっています。ただし、次のいずれかの操作によって無効にすることもできます。

- login.jsp の `forgotUserIdMode` の値を false に設定します。
- システム設定属性 `ui.web<admin|user>.disableForgotUserId` の値を true に設定します。

表示されるユーザー属性名は、システム設定属性 `security.authn.<Administrator Interface | User Interface>.lookupUserIdAttributes` を介して設定されます。指定できる属性は、`UserUIConfig` 設定オブジェクトの照会可能な属性として定義されているものです。

復元時に、「ユーザー ID の復元」電子メールテンプレートを使用して、復元されるユーザーの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

次のタスクマトリックスは、通常実行される Identity Manager タスクのクイックリファレンスです。このマトリックスでは、各タスクを開始するための主要な Identity Manager インタフェースの場所を示します。同じタスクを実行できる場所または方法がほかにもある場合には、それらも示します。

表 2-1 Identity Manager インタフェースタスクリファレンス

Identity Manager ユーザーの管理		
操作	**ナビゲーション**	**代替方法**
ユーザーの作成と編集	「アカウント」タブ、「アカウントのリスト」選択	「アカウント」タブ、「ユーザーの検索」選択 (「ユーザーアカウントの検索結果」ページ)
ユーザーアカウントの作成の承認	「作業項目」タブ、「承認」サブタブ	
ユーザー認証のセットアップ (ポリシー)	「セキュリティー」タブ、「ポリシー」選択	
ユーザーパスワードの変更	「パスワード」タブ、「ユーザーパスワードの変更」選択	「アカウント」タブ、「アカウントのリスト」選択 「アカウント」タブ、「ユーザーの検索」 選択 (「ユーザーアカウントの検索結果」ページ) Identity Manager ユーザーインタフェース
ユーザーパスワードのリセット	「パスワード」タブ、「ユーザーパスワードのリセット」選択	「アカウント」タブ、「アカウントのリスト」選択 「アカウント」タブ、「ユーザーの検索」 選択 (「ユーザーアカウントの検索結果」ページ)
ユーザーの検索	「アカウント」タブ、「ユーザーの検索」選択	「パスワード」タブ、「ユーザーパスワードの変更」選択
ユーザーの有効化または無効化	「アカウント」タブ、「アカウントのリスト」選択	「アカウント」タブ、「ユーザーの検索」 選択 (「ユーザーアカウントの検索結果」ページ)

表 2-1　Identity Manager インタフェースタスクリファレンス (続き)

ユーザーのロック解除	「アカウント」タブ、「アカウントのリスト」選択	「アカウント」タブ、「ユーザーの検索」 選択 (「ユーザーアカウントの検索結果」ページ)

Identity Manager 管理者の管理

操作	ナビゲーション
組織を通じて委任された管理のセットアップ	「アカウント」タブ、「アカウントのリスト」選択、「ユーザーの作成」ページ
機能の割り当て	「アカウント」タブ、「アカウントのリスト」選択、「ユーザーの作成」または「ユーザーの編集」ページ、「セキュリティー」サブタブ
機能の割り当て (管理者ロールを利用する場合)	「アカウント」タブ、「アカウントのリスト」選択、「ユーザーの作成」または「ユーザーの編集」ページ、「セキュリティー」サブタブ
承認者のセットアップ (アカウントの作成を検証するため)	「アカウント」タブ、「アカウントのリスト」選択、「組織の作成」ページ
	「ロール」タブ、「ロールの作成」ページ

Identity Manager の設定

操作	ナビゲーション
リソースの作成および管理 (リソースウィザード)	「リソース」タブ
リソースグループの管理	「リソース」タブ、「リソースグループのリスト」選択
ロールの作成および管理	「ロール」タブ
ロールの検索	「ロール」タブ、「ロールの検索」選択
機能の編集	「セキュリティー」タブ、「機能」選択
管理者ロールの作成および編集	「セキュリティー」タブ、「管理者ロール」選択、「管理者ロールの作成 / 編集」ページ
電子メールテンプレートのセットアップ	「設定」タブ、「電子メールテンプレート」選択
パスワード、アカウント、および名前ポリシーのセットアップ。組織へのポリシーの割り当て	「セキュリティー」タブ、「ポリシー」選択
アイデンティティー属性の設定	「メタビュー」タブ、「アイデンティティー属性」選択
アイデンティティーイベントの設定	「メタビュー」タブ、「アイデンティティーイベント」選択
ChangeLog の設定	「メタビュー」タブ、「ChangeLog」選択

表 2-1　Identity Manager インタフェースタスクリファレンス (続き)

アカウントおよびデータの読み込みと同期	
操作	**ナビゲーション**
データファイルのインポート (XML 形式のフォームなど)	「設定」タブ、「交換ファイルのインポート」選択
リソースアカウントの読み込み	「アカウント」タブ、「リソースから読み込み」選択
アカウントのファイルからの読み込み	「アカウント」タブ、「ファイルから読み込み」選択
Identity Manager ユーザーをリソースアカウントと比較	「リソース」タブ、「リソースの調整」選択
監査、リスク分析、およびレポート	
操作	**ナビゲーション**
イベント監査取得のセットアップと監査の有効化	「設定」タブ、「監査」選択
レポートの実行および管理	レポートの作成、実行、およびダウンロードを行うには「レポート」タブ、「レポートの実行」選択、レポート結果を表示するには「レポートの表示」
リスク分析レポートの定義および実行	「レポート」タブ、「リスク分析」選択
グラフ形式のレポートの表示	「レポート」タブ、「ダッシュボードの表示」選択
コンプライアンスの管理	
操作	**ナビゲーション**
監査ポリシーの定義	「コンプライアンス」タブ、「ポリシーの管理」選択
監査ポリシーの割り当て	「アカウント」タブ、「コンプライアンス」選択
コンプライアンス違反の管理	「自分の作業項目」タブ、「是正」選択
定期的アクセスレビューのセットアップ	「コンプライアンス」タブ、「アクセススキャンの管理」選択
定期的アクセスビューの監視	「コンプライアンス」タブ、「アクセスレビュー」選択
監査レポートの表示	「レポート」タブ、「監査レポート」タイプ選択

表 2-1　Identity Manager インタフェースタスクリファレンス (続き)

Identity Manager タスクの管理	
操作	**ナビゲーション**
定義されたタスク (またはプロセス) の実行	「サーバータスク」タブ、「タスクの実行」選択
タスクのスケジュール	「サーバータスク」タブ、「スケジュールの管理」選択
タスク結果の表示	「サーバータスク」タブ、「タスクの検索」または「すべてのタスク」選択
タスクの保留または中止	「サーバータスク」タブ、「すべてのタスク」選択
サービスプロバイダユーザーの管理	
操作	**ナビゲーション**
サービスプロバイダユーザーの管理	「アカウント」タブ、「サービスプロバイダユーザーの管理」選択
サービスプロバイダトランザクションの管理	「サーバータスク」タブ、「サービスプロバイダトランザクション」選択
サービスプロバイダ機能の設定	「サービスプロバイダ」タブ、「メイン設定の編集」選択
トランザクションのデフォルトの設定	「サービスプロバイダ」タブ、「トランザクション設定の編集」選択
サービスプロバイダポリシーの作成または編集	「セキュリティー」タブ、「ポリシー」選択

以降の操作について

Identity Manager のインタフェースおよび情報の検索方法について理解したあとは、次のリストを参照して、関心のあるトピックに進んでください。

章のトピック	説明
第 3 章「ユーザーとアカウントの管理」	インタフェースの「アカウント」エリアと、ユーザーアカウントの管理手順について説明します。
第 4 章「設定」	設定タスクと Identity Manager オブジェクトの設定方法について説明します。
第 5 章「管理」	Identity Manager 管理者と組織の作成および管理方法について説明します。
第 6 章「データの同期と読み込み」	Identity Manager での最新データの維持に使用できる機能およびツールについて説明します。
第 7 章「レポート」	レポートとその生成方法について説明します。
第 8 章「タスクテンプレート」	特定のワークフローの動作を設定するために使用できるタスクテンプレートについて説明します。
第 9 章「PasswordSync」	Windows Active Directory および Windows NT でのパスワード変更を Identity Manager と同期させる PasswordSync ユーティリティの設定方法について説明します。
第 10 章「セキュリティー」	セキュリティー機能とその使用方法について説明します。
第 11 章「アイデンティティー監査」	監査ポリシーの定義方法とコンプライアンスの管理方法について説明します。
第 12 章「監査ログ」	監査ログと監査システムの機能について説明します。
第 13 章「サービスプロバイダの管理」	サービスプロバイダユーザーを管理するための機能について説明します。
付録 A「lh リファレンス」	Identity Manager コマンド行から利用できるコマンドについて説明します。
付録 B「オンラインマニュアルの高度な検索」	オンラインヘルプで高度なクエリーを使用して Identity Manager ドキュメントを検索する手順について説明します。
付録 C「監査ログデータベーススキーマ」	サポートされるデータベースタイプと監査ログデータベースマッピングの監査データスキーマ値。
付録 D「Active Sync ウィザード」	7.0 以前のバージョンの Identity Manager のアクティブな同期の設定に使用します。

第 3 章

ユーザーとアカウントの管理

この章では、Identity Manager 管理者インタフェースを使用したユーザー管理の説明および手順を示します。次に示す Identity Manager ユーザーおよびアカウントの管理タスクについて説明します。

- ユーザーアカウントデータについて
- インタフェースの「アカウント」エリア
- ユーザーアカウントの操作
- アカウントの検索
- 一括アカウントアクション
- ユーザーアカウントパスワードの操作
- アカウントセキュリティーと特権の管理
- ユーザーの自己検索
- 相関規則と確認規則

ユーザーアカウントデータについて

ユーザーとは、Identity Manager システムアカウントを所持する個人のことです。Identity Manager には、各ユーザーについての一連のデータが格納されています。この情報が集まって、特定のユーザーの Identity Manager ID を形成します。

Identity Manager の管理者インタフェースの**「アカウント」**タブにある「ユーザーの作成」ページでは、ユーザーデータが次のエリアに分類されて表示されます。

- ID
- 割り当て
- セキュリティー

- 委任
- 属性
- コンプライアンス

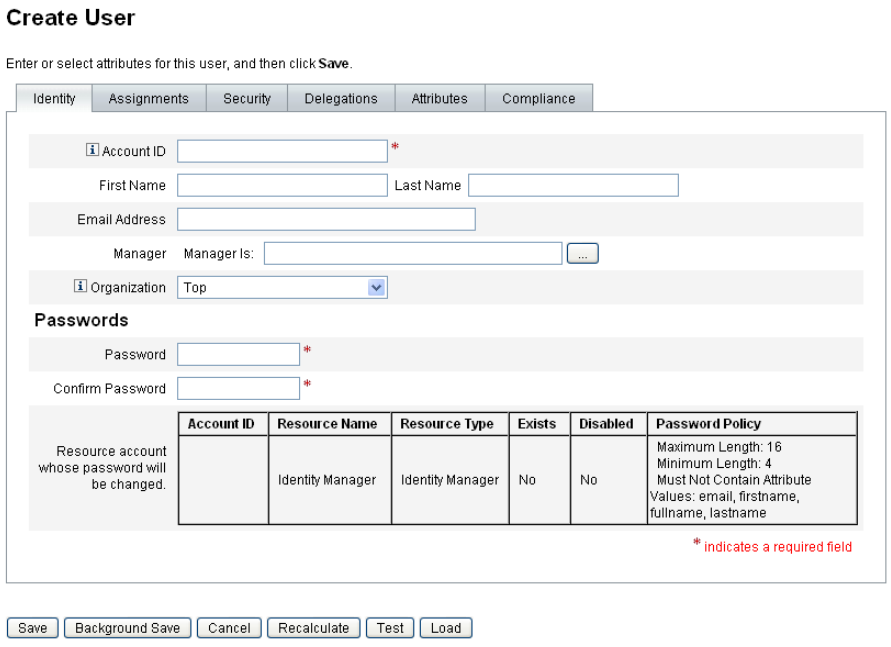
ID

「ID」エリアでは、ユーザーのアカウント ID、名前、連絡先情報、管理する組織、および Identity Manager アカウントパスワードを定義します。また、ユーザーがアクセスできるリソース、および各リソースアカウントに適用されているパスワードポリシーが示されます。

注 アカウントパスワードポリシーの設定の詳細については、この章の 89 ページの「ユーザーアカウントパスワードの操作」の節を参照してください。

次の図は、「ユーザーの作成」ページの「ID」エリアを示します。

図 3-1 「ユーザーの作成」- 「ID」



割り当て

「割り当て」エリアでは、リソースなどの Identity Manager オブジェクトに対するアクセスの制限を設定します。

「割り当て」フォームのタブをクリックして、次の割り当てを設定します。

- **Identity Manager アカウントポリシー**の割り当て – パスワードと認証の制限を設定します。
- **ロール**の割り当て – ユーザークラスのプロファイルを作成します。ロールは、間接的な割り当てによってリソースへのユーザーアクセスを定義します。
- **リソースとリソースグループ**の割り当て – ユーザーに直接割り当てることができる利用可能なリソースとリソースグループ、およびユーザーアクセスから除外できるリソースが表示されます。これらは、ロールの割り当てによってユーザーに間接的に割り当てられるリソースを補足します。

セキュリティー

Identity Manager では、拡張機能が割り当てられたユーザーを Identity Manager 管理者と呼びます。「セキュリティー」タブを使用して、次の割り当てを行うことにより、これらの拡張管理機能をユーザーに設定します。

- **管理者ロール** – 機能および管理する組織の一意のセットを組み合わせることによって、管理ユーザーに、調整済みの割り当てを簡単に設定できます。
- **機能** – Identity Manager システムでの権限を有効にします。各 Identity Manager 管理者には、多くの場合は職務に応じて、1 つ以上の機能が割り当てられます。
- **管理する組織** – ユーザーが管理者として管理する権限を持つ組織を割り当てます。管理者は、割り当てられた組織のオブジェクト、および階層内でその組織の下位にあるすべての組織のオブジェクトを管理できます。

注 ユーザーに管理者機能を与えるには、少なくとも 1 つの管理者ロールまたは 1 つ以上の機能および 1 つ以上の管理する組織を割り当てる必要があります。Identity Manager 管理者の詳細については、152 ページの「Identity Manager の管理について」を参照してください。

- **「ユーザーフォーム」** – ユーザーの作成および編集時に管理者が使用するユーザーフォームを指定します。「なし」を選択すると、管理者は自身の組織に割り当てられたユーザーフォームを継承します。
- **「ユーザー表示フォーム」** – ユーザーの表示時に管理者が使用するユーザーフォームを指定します。「なし」を選択すると、管理者は自身の組織に割り当てられたユーザーフォームを継承します。

委任

「ユーザーの作成」ページの「委任」タブを使用すると、作業項目をほかのユーザーに一定期間、委任できます。作業項目の委任の詳細については、198 ページの「作業項目の委任」を参照してください。

属性

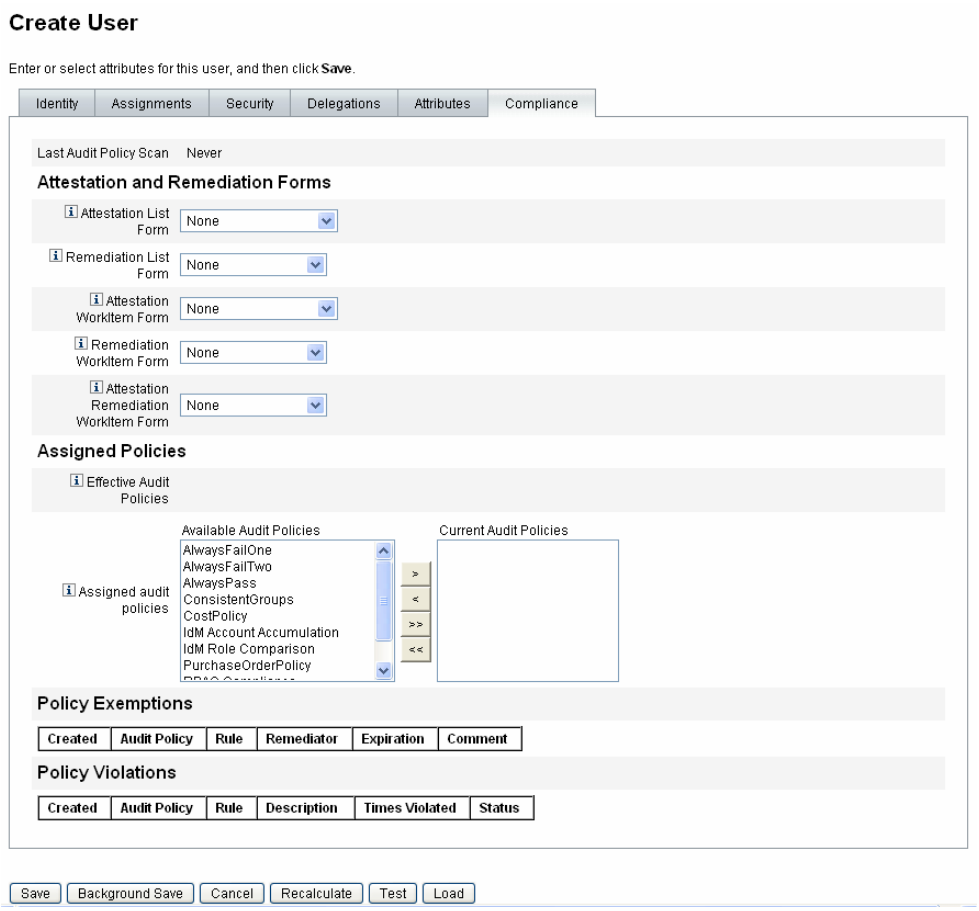
「ユーザーの作成」ページの「属性」エリアでは、割り当てられたリソースに関連付けられるアカウント属性を定義します。リストされる属性は、割り当てられたリソースごとに分類され、割り当てられたリソースによって異なります。

コンプライアンス

「コンプライアンス」タブ:

- ユーザーアカウントに対して、アテステーション用と是正用のフォームを選択できます。
- ユーザーの組織割り当てで有効になっているものを含め、ユーザーアカウントに対して割り当てられた監査ポリシーを指定します。これらのポリシーの割り当ては、ユーザーの現在の組織を編集するか、ユーザーを別の組織に移すことによってのみ変更できます。
- ユーザーアカウントに該当するデータがある場合は、次の図に示すように、ポリシーのスキャン、違反、および免除の現在のステータスも示されます。選択されたユーザーで最後に実行された監査ポリシースキャンの日時の情報も含まれます。

図 3-2　「ユーザーの作成」ページ ― 「コンプライアンス」タブ



監査ポリシーを割り当てるには、選択したポリシーを「利用可能な監査ポリシー」リストから「現在の監査ポリシー」リストへ移動します。

.

注　「ユーザーアクション」リストの**「コンプライアンスステータスの表示」**を選択することにより、「コンプライアンス」タブの情報にアクセスすることもできます。あるユーザーに対し特定の期間に記録されたコンプライアンス違反を表示するには、「ユーザーアクション」リストから**「コンプライアンス違反ログの表示」**を選択し、表示するエントリの範囲を指定します。

インタフェースの「アカウント」エリア

Identity Manager アカウントエリアを使用して、Identity Manager ユーザーを管理できます。このエリアにアクセスするには、管理者インタフェースメニューバーから「アカウント」を選択します。

アカウントリストには、Identity Manager ユーザーアカウントがすべて表示されます。アカウントは組織と仮想組織にグループ化され、階層構造のフォルダで表示されます。

アカウントリストは、フルネーム (「名前」)、ユーザーの姓 (「姓」)、またはユーザーの名 (「名」) で並べ替えることができます。列で並べ替えるには、ヘッダーバーをクリックします。同じヘッダーバーをクリックすると、昇順と降順が切り替わります。フルネーム (「名前」列) で並べ替えると、階層内のすべてのレベルのすべての項目がアルファベット順に並べ替えられます。

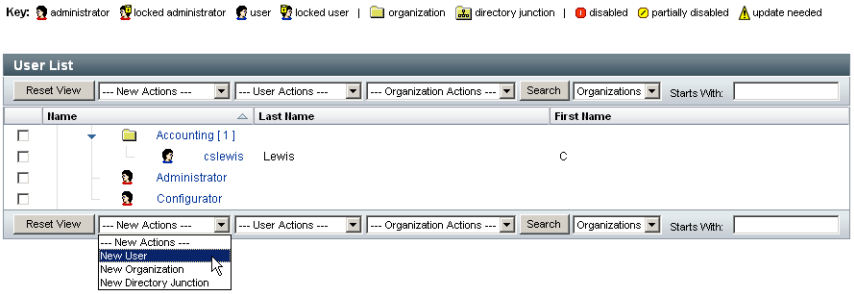
階層表示を展開して組織内のアカウントを表示するには、フォルダの隣にある三角形のマークをクリックします。表示を折りたたむには、マークをもう一度クリックします。

「アカウント」エリアのアクションリスト

各種アクションを実行するときは、図 3-3 に示すように、「アカウント」エリアの上部と下部にあるアクションリストを使用します。アクションリストの選択項目は、次のように分類されています。

- **「新規作成アクション」** – ユーザー、組織、およびディレクトリジャンクションを作成します。
- **「ユーザーアクション」** – ユーザーのステータスの編集、表示、および変更、パスワードの変更およびリセット、ユーザーの削除、有効化、無効化、ロック解除、移動、更新、および名前変更、ユーザー監査レポートの実行を行います。
- **「組織アクション」** – 組織と組織内のユーザーに対して各種アクションを実行します。

図 3-3　　アカウントリスト



「アカウントリスト」エリアでの検索

ユーザーと組織を検索するときは、「アカウント」エリアの検索機能を使用します。リストから「組織」または「ユーザー」を選択し、そのユーザーまたは組織の名前を先頭から 1 文字以上検索エリアに入力して、「検索」をクリックします。「アカウント」エリアでの検索の詳細については、82 ページの「アカウントの検索」を参照してください。

ユーザーアカウントステータス

各ユーザーアカウントの隣に表示されるアイコンは、現在割り当てられているアカウントステータスを示します。表 3-1 に、各アイコンの説明を示します。

表 3-1　　ユーザーアカウントステータスアイコンの説明

インジケータ	ステータス
	Identity Manager ユーザーアカウントはロックされています。これは、ログイン試行の失敗回数が、リソースに設定された制限を越えたために、ユーザーがリソースアカウントからロックアウトされていることを示します。
	Identity Manager 管理者アカウントはロックされています。
	アカウントは、割り当てられたすべてのリソースおよび Identity Manager で無効になっています。アカウントが有効なときは、アイコンは表示されません。

表 3-1　ユーザーアカウントステータスアイコンの説明 (続き)

インジケータ	ステータス
	アカウントは、一部無効になっています。これは、割り当てられた 1 つ以上のリソースで無効になっていることを示します。
	1 つ以上のリソースで Identity Manager ユーザーアカウントの作成または更新が試行されましたが、失敗しました。割り当てられたすべてのリソースでアカウントが更新されたときは、アイコンは表示されません。

ユーザーアカウントの操作

管理者インタフェースの「アカウント」エリアでは、次のシステムオブジェクトに対する一連の操作を実行できます。

- **ユーザー** ― 表示、作成、編集、移動、名前変更、プロビジョン解除、有効化、無効化、更新、ロック解除、削除、割り当て解除、リンク解除、および監査
- **パスワード** ― 変更およびリセット
- **組織** ― 組織のメンバーに対するユーザーアクションの作成、編集、更新、および実行
- **ディレクトリジャンクション** ― 作成

ユーザー

この節では、ユーザーアカウントの管理を中心に説明します。組織の管理など、管理レベルのその他のタスクの詳細については、第 5 章「管理」を参照してください。

表示

ユーザーアカウントの詳細を表示するには、リストでユーザーを選択し、「ユーザーアクション」リストから「表示」を選択します。

「ユーザーの表示」ページに、ユーザーの編集または作成時に設定された ID、割り当て、セキュリティー、および属性情報の選択項目のサブセットが表示されます。「ユーザーの表示」ページの情報は編集できません。アカウントリストに戻るには、「キャンセル」をクリックします。

作成 (「新規作成アクション」リスト、「新規ユーザー」選択)

ユーザーアカウントを作成するには、「新規作成アクション」リストから「新規ユーザー」を選択します。最上位 (Top) 以外の組織にユーザーを作成する場合は、組織フォルダを選択してから、「新規作成アクション」リストで「新規ユーザー」を選択します。

1 つのエリアで利用可能な選択項目は、別のエリアでの選択により異なります。

ユーザーフォームで定義した「ユーザーの作成」ページでは、ユーザーアカウントに関する次の項目を設定できます。

- **「ID」** – 名前、電子メール、組織、およびパスワードの詳細
- **「割り当て」** – アカウントポリシー、ロール、およびリソース
- **「セキュリティー」** – 組織と機能
- **「委任」** – 作業項目の委任
- **「属性」** – 割り当てられたリソースに対する特定の属性

ビジネスプロセスや特定の管理者機能をより適切に反映するように、環境に合わせたユーザーフォームを設定できます。ユーザーフォームのカスタマイズの詳細については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

ユーザーの作成設定を表示するには、「ユーザーの作成」ページのタブをクリックします。タブ間は任意の順序で移動できます。選択が完了したら、ユーザーアカウントを保存するための次の 2 つのオプションを選択できます。

- **「保存」** – ユーザーアカウントを保存します。アカウントに多数のリソースを割り当てた場合は、このプロセスにしばらく時間がかかります。
- **「バックグラウンドで保存」** – このプロセスではユーザーアカウントをバックグラウンドタスクとして保存します。この場合は、Identity Manager での作業を引き続き実行できます。「アカウント」ページ、「ユーザーの検索結果」ページ、および「ホーム」ページに、進行中の各保存処理に関するタスクステータスインジケータが表示されます。

ステータスインジケータでは、次の表で説明するように、保存プロセスの進捗を確認できます。

表 3-2 バックグラウンドでの保存タスクのステータスインジケータの説明

ステータスインジケータ	ステータス
	保存プロセスは進行中です。

表 3-2　バックグラウンドでの保存タスクのステータスインジケータの説明 (続き)

ステータスインジケータ	ステータス
	保存プロセスは保留されています。ほとんどの場合、これは、プロセスが承認を待っていることを意味します。
✓	プロセスは正常に完了しました。これは、ユーザーが正常に保存されたことを示すものではありません。プロセスがエラーなしで完了したことを示すものです。
?	プロセスはまだ開始されていません。
	プロセスは完了しましたが、1 つ以上のエラーが発生しました。

ステータスインジケータ内に表示されるユーザーアイコンの上にマウスを移動すると、バックグラウンドの保存プロセスについての詳細が表示されます。

注　サンライズが設定されている場合、ユーザーを作成すると、「承認」タブから表示できる作業項目が作成されます。この項目を承認すると、サンライズの日付が上書きされ、アカウントが作成されます。項目を却下すると、アカウントの作成がキャンセルされます。サンライズの設定の詳細については、281 ページの「「サンライズとサンセット」タブの設定」を参照してください。

複数のユーザーアカウント (アイデンティティー) の作成

1 つのリソースに複数のユーザーアカウントを作成できます。ユーザーを作成または編集して 1 つ以上のリソースを割り当てた場合、そのリソースに追加のアカウントをリクエストして定義することもできます。

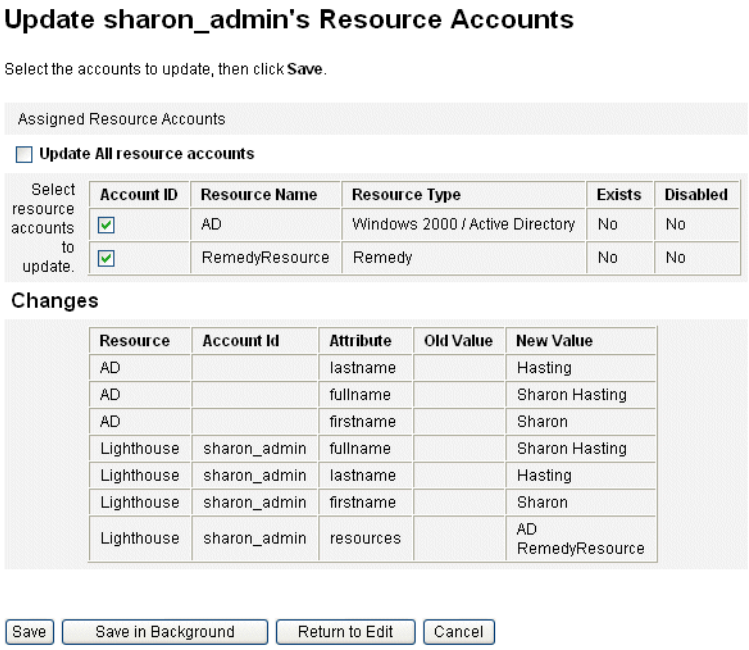
編集

アカウント情報を編集するには、次のいずれかの操作を行います。

- アカウントリストでユーザーアカウントをクリックします。
- リストでユーザーアカウントを選択し、「ユーザーアクション」リストから「編集」を選択します。

変更を加えて保存すると、Identity Manager により「リソースアカウントの更新」ページが表示されます。このページには、ユーザーに割り当てられたリソースアカウントと、そのアカウントに適用される変更が表示されます。割り当てられたすべてのリソースに変更を適用する場合は、「すべてのリソースアカウントの更新」を選択します。または、ユーザーに関連付けられた 0 または 1 つ以上のリソースアカウントを個別に選択して更新します。

図 3-4　　ユーザーの編集 (リソースアカウントの更新)



編集を完了する場合は「保存」をもう一度クリックします。さらに変更を加える場合は「編集に戻る」をクリックします。

ユーザーの移動 (「ユーザーアクション」)

「ユーザーの組織の変更」タスクでは、ユーザーを、現在割り当てられている組織から削除して、新しい組織に再割り当て、つまり移動できます。

ユーザーを別の組織に移動するには、リストで 1 つ以上のユーザーアカウントを選択し、「ユーザーアクション」リストから「移動」を選択します。

名前の変更 (「ユーザーアクション」)

通常、リソースのアカウント名の変更は複雑な操作です。このため、Identity Manager では、ユーザーの Identity Manager アカウントの名前を変更する機能、およびそのユーザーに関連付けられた 1 つ以上のリソースアカウントの名前を変更する機能を別個に用意しています。

名前の変更機能を使用するには、リストでユーザーアカウントを選択し、「ユーザーアクション」リストから「名前の変更」を選択します。

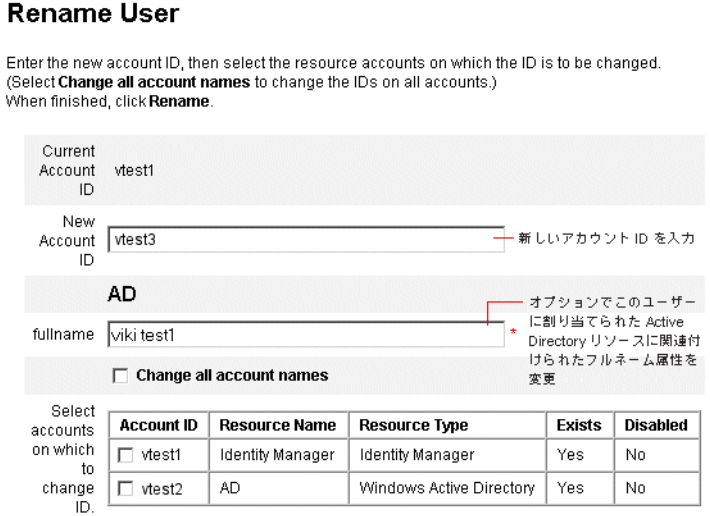
「ユーザーの名前変更」ページでは、ユーザーのアカウント名、関連付けられたリソースアカウント名、およびそのユーザーの Identity Manager アカウントに関連付けられたリソースアカウント属性を変更できます。

注 リソースタイプの一部では、アカウントの名前変更をサポートしません。

次の図に示すように、ユーザーには Active Directory リソースが割り当てられています。名前の変更プロセスでは、次を変更できます。

- Identity Manager ユーザーアカウント名
- Active Directory リソースアカウント名
- Active Directory リソース属性 (フルネーム)

図 3-5 Rename User



ユーザーの無効化 (「ユーザーアクション」、「組織アクション」)

ユーザーアカウントを無効化すると、そのアカウントは変更され、ユーザーは Identity Manager または割り当てられたリソースアカウントにログインできなくなります。

注 割り当てられたリソースがアカウントの無効化をサポートしない場合、ユーザーアカウントには新しくランダムに生成されたパスワードが割り当てられて、無効化されます。

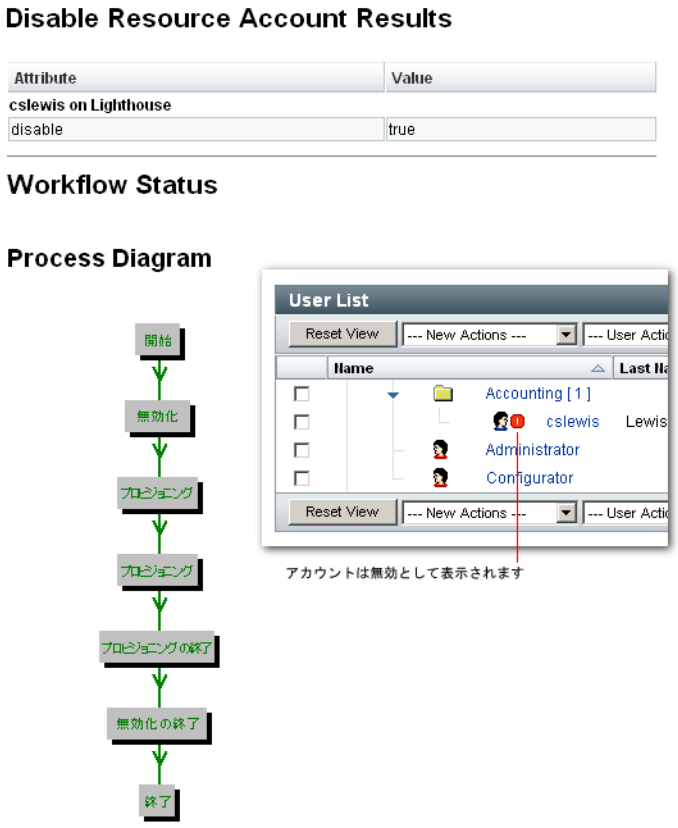
1 つのユーザーアカウントの無効化

1 つのユーザーアカウントを無効化するには、リストでユーザーアカウントを選択し、「ユーザーアクション」リストから「無効化」を選択します。

表示された「無効化」ページで、無効化するリソースアカウントを選択し、「OK」をクリックします。Identity Manager ユーザーアカウントと、それに関連付けられたすべてのリソースアカウントを無効化した結果が表示されます。ユーザーアカウントリストでは、そのユーザーアカウントが無効であることが示されます。

図 3-6 に、「無効化」ページでの無効化されたアカウントを示します。

図 3-6　　無効化されたアカウント



複数のユーザーアカウントの無効化

複数の Identity Manager ユーザーアカウントを同時に無効化できます。リストで複数のユーザーアカウントを選択し、「ユーザーアクション」リストから「無効化」を選択します。

注　　複数のユーザーアカウントを無効化する場合は、各ユーザーアカウントから、割り当てられたリソースアカウントを個別に選択することはできません。このプロセスでは、選択したすべてのユーザーアカウントのすべてのリソースが無効化されます。

ユーザーの有効化 (「ユーザーアクション」、「組織アクション」)

ユーザーアカウントの有効化は、無効化プロセスとは逆のプロセスです。アカウントの有効化をサポートしないリソースの場合は、ランダムなパスワードが新しく生成されます。選択した通知オプションによっては、管理者の結果ページにもそのパスワードが表示されることがあります。

ユーザーはそのパスワードをリセットできます (認証プロセスが必要)。または、管理特権を持つユーザーがこのパスワードをリセットできます。

1 つのユーザーアカウントの有効化

1 つのユーザーアカウントを有効化するには、リストでユーザーアカウントを選択し、「ユーザーアクション」リストから「有効化」を選択します。

表示された「有効化」ページで、有効化するリソースを選択し、「OK」をクリックします。Identity Manager アカウントと、それに関連付けられたすべてのリソースアカウントを有効化した結果が表示されます。

複数のユーザーアカウントの有効化

複数の Identity Manager ユーザーアカウントを同時に有効化できます。リストで複数のユーザーアカウントを選択し、「ユーザーアクション」リストから「有効化」を選択します。

注 複数のユーザーアカウントを有効化する場合は、各ユーザーアカウントから、割り当てられたリソースアカウントを個別に選択することはできません。このプロセスでは、選択したすべてのユーザーアカウントのすべてのリソースが有効化されます。

ユーザーの更新 (「ユーザーアクション」、「組織アクション」)

更新操作では、ユーザーアカウントに関連付けられたリソースが Identity Manager で更新されます。「アカウント」エリアから更新を実行した場合は、以前にユーザーに対して行われた保留中の変更が、選択されたリソースに送信されます。次の場合にこの状況が発生する可能性があります。

- 更新の実行時にリソースが利用不可能だった場合
- ロールまたはリソースグループに対して変更が行われたが、それに関連付けられたすべてのユーザーにその変更を送信する必要がある場合。この場合は、「ユーザーの検索」ページを使用してユーザーを検索し、更新操作の実行対象とする 1 人以上のユーザーを選択する必要があります。

ユーザーアカウントの更新時には、次のオプションを選択できます。

- 割り当てられたリソースアカウントが更新された情報を受け取るかどうか

- すべてのリソースアカウントを更新するか、リストから個別のアカウントを選択するか

1 つのユーザーアカウントの更新

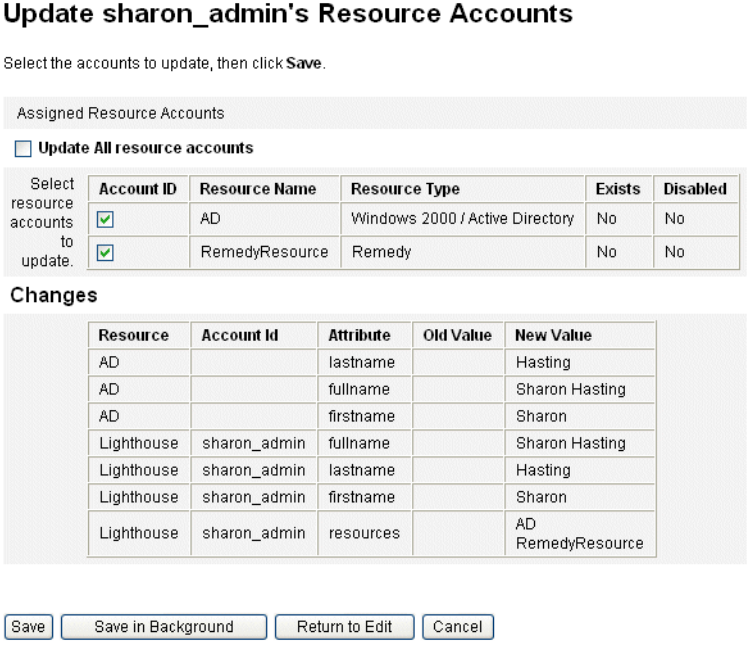
1 つのユーザーアカウントを更新するには、リストでユーザーアカウントを選択し、「ユーザーアクション」リストから「更新」を選択します。

「リソースアカウントの更新」ページで、更新するリソースを 1 つ以上選択するか、または割り当てられたリソースアカウントをすべて更新する場合は「すべてのリソースアカウントの更新」を選択します。選択し終えたら、「OK」をクリックして、更新プロセスを開始します。または、「バックグラウンドで保存」をクリックして、操作をバックグラウンドプロセスとして実行します。

確認ページで各リソースに送信されるデータを確認します。

図 3-7 に「リソースアカウントの更新」ページを示します。この図で、Lighthouse は Identity Manager を意味します。

図 3-7　　リソースアカウントの更新



複数のアカウントの更新

複数の Identity Manager ユーザーアカウントを同時に更新できます。リストで複数のユーザーアカウントを選択し、「ユーザーアクション」リストから「更新」を選択します。

注 複数のユーザーアカウントを更新する場合は、各ユーザーアカウントから、割り当てられたリソースアカウントを個別に選択することはできません。このプロセスでは、選択したすべてのユーザーアカウントのすべてのリソースが更新されます。

ユーザーのロック解除 (「ユーザーアクション」、「組織アクション」)

ログインの再試行回数が、リソースに設定された制限を越えたために、ユーザーが 1 つ以上のリソースアカウントからロックアウトされることがあります。パスワードまたは質問によるログイン試行で許容される最大失敗回数は、ユーザーの有効な Lighthouse アカウントポリシーによって設定されます。

パスワードによるログイン試行の最大失敗回数を超えたためにユーザーがロックされた場合、そのユーザーは、ユーザーインタフェース、管理者インタフェース、「Forgot My Password」、Identity Manager IDE、SOAP、およびコンソールを含むいずれの Identity Manager アプリケーションインタフェースにも認証されません。質問によるログイン試行の最大失敗回数を超えたためにロックされた場合は、「Forgot My Password」を除く任意の Identity Manager アプリケーションインターフェイスに認証できます。

パスワードによるログイン試行の失敗

パスワードによるログイン試行に失敗したためにロックされた場合、ユーザーアカウントは、次の期間ロックされたままになります。

- 管理ユーザーがそのユーザーアカウントをロック解除するまで。アカウントを正常にロック解除するには、管理者に「Unlock User」機能が割り当てられていて、管理者がそのユーザーのメンバー組織の管理コントロールを持っている必要があります。
- ロックの有効期限の日時が設定されている場合は、現在の日時がユーザーのロックの有効期限の日時を過ぎるまで。ロックの有効期限は、Lighthouse アカウントポリシーのロックタイムアウト値によって設定されます。

質問によるログイン試行の失敗

質問によるログイン試行の最大回数を超えたためにロックされた場合、ユーザーアカウントは、次のいずれかの操作が行われるまでロックされたままになります。

- 管理ユーザーがそのユーザーアカウントをロック解除するまで。アカウントを正常にロック解除するには、管理者に「Unlock User」機能が割り当てられていて、管理者がそのユーザーのメンバー組織の管理コントロールを持っている必要があります。
- ロックされたユーザー、または適切な機能を持つユーザーが、ユーザーのパスワードを変更またはリセットするまで。

適切な機能を持つ管理者は、ロックされた状態のユーザーに対して次の操作を実行できます。

- 更新 (リソースの再プロビジョンを含む)
- パスワードの変更またはリセット
- 無効化または有効化
- 名前の変更
- ロック解除

ロックされた状態のユーザーは、管理者インタフェース、ユーザーインタフェース、Identity Manager IDE を含むいずれの Identity Manager アプリケーションにもログインできません。この制限は、ユーザーが、ユーザー ID および秘密の質問への回答を提供するか、1 つ以上のリソースにパススルーするかのどちらにも関係なく、自分の Identity Manager ユーザー ID とパスワードでログインを試みる場合に適用されます。

アカウントをロック解除するには、リストで 1 つ以上のユーザーアカウントを選択し、「ユーザーアクション」または「組織アクション」リストから「ユーザーのロック解除」を選択します。

削除 (「ユーザーアクション」、「組織アクション」)

削除操作では、リソースから Identity Manager ユーザーアカウントアクセスを削除するためのオプションがいくつかあります。

- **「削除」** – 選択した各リソースについて、関連付けられたリソースアカウントが Identity Manager で削除されます。また、選択したリソースは、Identity Manager ユーザーからリンク解除されます。
- **「割り当て解除」** – 選択した各リソースについて、Identity Manager では関連付けられたリソースが、ユーザーに割り当てられたリソースのリストから削除されます。選択したリソースは、ユーザーからリンク解除されます。関連付けられたリソースアカウントは削除されません。

- **「リンク解除」** – 選択した各リソースについて、Identity Manager では付けられたリソースアカウント情報が Identity Manager ユーザーから削除されます。

注 ロールまたはリソースグループによってユーザーに間接的に割り当てられているアカウントをリンク解除する場合は、ユーザーを更新するとリンクが回復されることがあります。

削除操作を開始するには、ユーザーアカウントを選択し、「ユーザーアクション」または「組織アクション」リストから適切な削除操作を選択します。

Identity Manager では「リソースアカウントの削除」ページが表示されます。

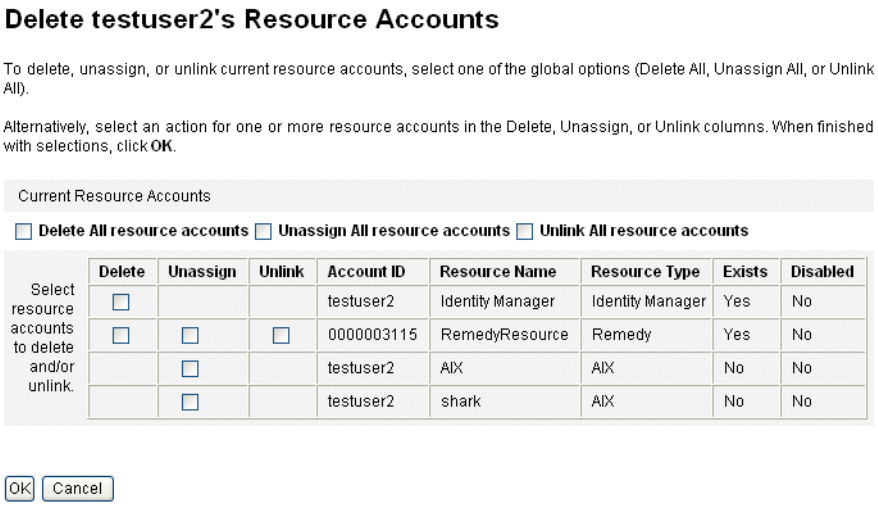
ユーザーアカウントとリソースアカウントの削除

Identity Manager ユーザーアカウントまたはリソースアカウントを削除するには、「削除」列でアカウントを選択して「OK」をクリックします。すべてのリソースアカウントを削除するには、「すべてのリソースアカウントの削除」オプションを選択して、「OK」をクリックします。

リソースアカウントの割り当て解除またはリンク解除

Identity Manager ユーザーアカウントからリソースアカウントを割り当て解除またはリンク解除するには、「割り当て解除」列または「リンク解除」列でアカウントを個別に選択して、「OK」をクリックします。すべてのリソースアカウントを割り当て解除するには、「すべてのリソースアカウントの割り当て解除」または「すべてのリソースアカウントのリンク解除」オプションを選択して、「OK」をクリックします。

図 3-8 ユーザーアカウントとリソースアカウントの削除



パスワード

「パスワードの変更」および「パスワードのリセット」のユーザーアクションを使用して、「ユーザーの編集」ページを呼び出し、選択したユーザーのユーザーパスワードを変更またはリセットできます。89 ページの「ユーザーアカウントパスワードの操作」も参照してください。

アカウントの検索

Identity Manager の検索機能を使用して、ユーザーアカウントを検索できます。検索パラメータを入力および選択すると、Identity Manager では選択した条件を満たすすべてのアカウントが検索されます。

アカウントを検索するには、メニューバーの「アカウント」を選択して、「ユーザーの検索」を選択します。次の 1 つ以上の検索の種類でアカウントを検索できます。

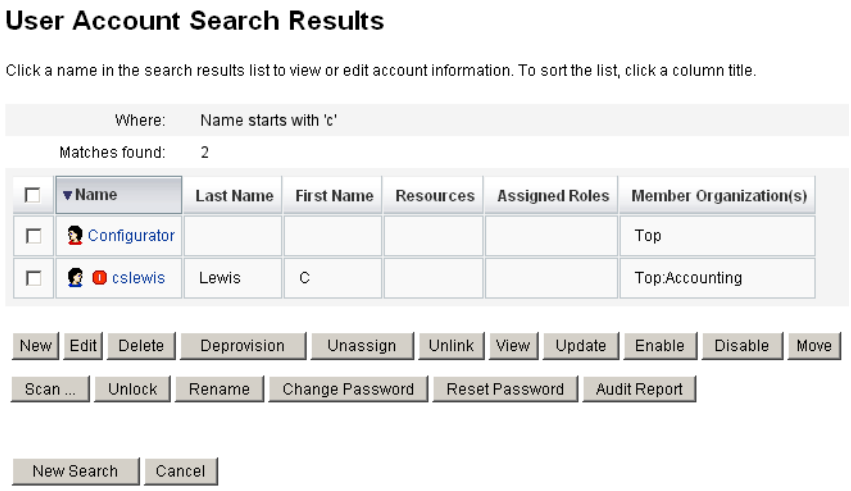
- ユーザー名、電子メールアドレス、姓、名などのアカウントの詳細。本人が所属する機関に固有の Identity Manager 実装によって選択は異なります。
- ユーザーの管理者。
- リソースアカウントステータス。次のものがあります。
  - **「無効」** – ユーザーは Identity Manager または割り当てられたリソースアカウントのどれにもアクセスできません。
  - **「一部無効」** – ユーザーは割り当てられたリソースアカウントの 1 つ以上にアクセスできません。
  - **「有効」** – ユーザーは割り当てられたリソースアカウントのすべてにアクセスできます。
- ユーザーアカウントステータス。次のものがあります。
  - **「ロックされている」** – パスワードまたは質問によるログイン試行の失敗回数が、許容される最大回数を超えたため、ユーザーアカウントがロックされています。
  - **「ロックされていない」** – ユーザーアカウントは制限されていません。
- 更新ステータス。次のものがあります。
  - **「0 個の」** – どのリソースでも更新されていないユーザーアカウント。
  - **「一部」** – 割り当てられたリソースの 1 つ以上 (ただし全部ではない) で更新されたユーザーアカウント。
  - **「すべて」** – 割り当てられたすべてのリソースで更新されたユーザーアカウント。
- 割り当てられたリソース
- ロール

- 所属している組織
- 管理する組織
- 機能
- 管理者ロール

検索結果リストには、検索に一致するすべてのアカウントが表示されます。結果ページで次の操作ができます。

- 編集するユーザーアカウントの選択。アカウントを編集するには、検索結果リストでそのアカウントをクリックするか、またはリストでそのアカウントを選択して「編集」をクリックします。
- 複数のアカウントに対する操作 (有効化、無効化、ロック解除、削除、更新、またはパスワードの変更 / リセットなど) の実行。操作を実行するには、検索結果リスト内でアカウントを 1 つ以上選択し、該当する操作をクリックします。
- ユーザーアカウントの作成。

図 3-9　　ユーザーアカウントの検索結果



一括アカウントアクション

Identity Manager アカウントに対していくつかの一括アクションを実行できます。これにより、複数のアカウントを同時に操作することができます。次の一括アクションを開始できます。

- **削除** ー 選択したリソースアカウントを削除、割り当て解除、またはリンク解除します。各ユーザーの Identity Manager アカウントを削除するには、「Identity Manager アカウントをターゲットにする」オプションを選択します。
- **削除とリンク解除** ー 選択したリソースアカウントを削除し、ユーザーからアカウントをリンク解除します。
- **無効化** ー 選択したリソースアカウントをすべて無効化します。各ユーザーの Identity Manager アカウントを無効化するには、「Identity Manager アカウントをターゲットにする」オプションを選択します。
- **有効化** ー 選択したリソースアカウントをすべて有効化します。各ユーザーの Identity Manager アカウントを有効にするには、「Identity Manager アカウントをターゲットにする」オプションを選択します。
- **割り当て解除、リンク解除** ー 選択したリソースアカウントをリンク解除し、それらのリソースに対する Identity Manager ユーザーアカウントの割り当てを削除します。割り当て解除によってリソースからアカウントが削除されることはありません。ロールまたはリソースグループによって Identity Manager ユーザーに間接的に割り当てられていたアカウントを割り当て解除することはできません。
- **リンク解除** ー リソースアカウントから、Identity Manager ユーザーアカウントとの関連付け (リンク) を削除します。リンク解除によってリソースからアカウントが削除されることはありません。ロールまたはリソースグループによって Identity Manager ユーザーに間接的に割り当てられていたアカウントをリンク解除した場合は、ユーザーを更新するとリンクを回復できます。

一括アクションは、ファイルか、電子メールクライアントやスプレッドシートプログラムなどのアプリケーションにユーザーのリストを保存している場合にもっとも役立ちます。ユーザーのリストをこのインタフェースページのフィールドにコピーして貼り付けることも、ファイルからユーザーのリストを読み込むこともできます。

これらの操作の大部分を、ユーザーの検索結果に対して実行できます。ユーザーの検索は、「ユーザーの検索」ページの「アカウント」タブで行います。

タスクの終了時にタスク結果が表示されたときに「CSV のダウンロード」をクリックすることにより、一括アカウントアクションの結果を CSV ファイルに保存できます。

一括アカウントアクションの起動

一括アカウントアクションを起動するには、値を選択または入力して、「起動」をクリックしてください。Identity Manager はバックグラウンドタスクを起動して一括アクションを実行します。

一括アクションタスクのステータスを監視するには、「タスク」タブに進んでタスクのリンクをクリックします。

アクションリストの使用

一括アクションのリストをカンマ区切り値 (comma-separated value; CSV) 形式で指定できます。これにより、各種操作を 1 つのアクションリストに混在させることができます。また、複雑な作成および更新の操作も指定できます。

CSV 形式は、2 行以上の入力行で構成されます。各行は、カンマで区切った値のリストで構成されます。1 行目にはフィールド名を指定します。以降の各行は、Identity Manager ユーザーまたはユーザーのリソースアカウント、あるいはその両方に対して実行する操作に対応します。各行に同じ数の値を指定する必要があります。空の値を指定すると、対応するフィールドの値は変更されないまま残ります。

どの一括アクション CSV にも必須のフィールドが 2 つあります。

- user − Identity Manager ユーザーの名前を指定します。
- command − Identity Manager ユーザーに対して実行する操作を指定します。有効なコマンドを次に示します。
    - Delete − リソースアカウントまたは Identity Manager アカウント、あるいはその両方を削除、割り当て解除、およびリンク解除します。
    - DeleteAndUnlink − リソースアカウントを削除してリンク解除します。
    - Disable − リソースアカウントまたは Identity Manager アカウント、あるいはその両方を無効化します。
    - Enable − リソースアカウントまたは Identity Manager アカウント、あるいはその両方を有効化します。
    - Unassign − リソースアカウントを割り当て解除してリンク解除します。
    - Unlink − リソースアカウントをリンク解除します。
    - Create − Identity Manager アカウントを作成します。オプションの作業として、リソースアカウントを作成します。
    - Update − Identity Manager アカウントを更新します。オプションの作業として、リソースアカウントを作成、更新、または削除します。
    - CreateOrUpdate − Identity Manager アカウントが存在しない場合は作成操作を実行します。存在する場合は更新操作を実行します。

Delete、DeleteAndUnlink、Disable、Enable、Unassign、および Unlink コマンド

Delete、DeleteAndUnlink、Disable、Enable、Unassign、または Unlink 操作を実行する場合、ほかに指定する必要のあるフィールドは resources のみです。resources フィールドは、どのリソースのどのアカウントに影響を与えるかを指定するために使用します。次の値を指定できます。

- all − Identity Manager アカウントを含むすべてのリソースアカウントを処理します。
- resonly − Identity Manager アカウントを除くすべてのリソースアカウントを処理します。
- *resource_name* [| *resource_name ...*] − 指定されたリソースアカウントを処理します。アカウントを処理するには、Identity Manager を指定します。

これらの操作のいくつかを、CSV 形式にした例を次に示します。

```
command,user,resources
Delete,John Doe,all
Disable,Jane Doe,resonly
Enable,Henry Smith,Identity Manager
Unlink,Jill Smith,Windows Active Directory|Solaris Server
```

Create、Update、および CreateOrUpdate コマンド

Create、Update、または CreateOrUpdate コマンドを実行する場合は、user フィールドと command フィールドのほかに、ユーザー画面のフィールドを指定できます。使用するフィールド名は、画面の属性のパス表現です。ユーザー画面で使用可能な属性については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。カスタマイズしたユーザーフォームを使用している場合は、フォームのフィールド名に、使用可能なパス表現がいくつか含まれています。

一括アクションで使用する一般的なパス表現のいくつかを次に示します。

- waveset.roles − Identity Manager アカウントに割り当てる 1 つ以上のロール名のリスト
- waveset.resources − Identity Manager アカウントに割り当てる 1 つ以上のリソース名のリスト
- waveset.applications − Identity Manager アカウントに割り当てる 1 つ以上のアプリケーション名のリスト
- waveset.organization − Identity Manager アカウントを配置する組織名
- accounts[*resource_name*].*attribute_name* − リソースアカウント属性。属性名はリソースのスキーマにリストします。

作成および更新操作を、CSV 形式にした例を次に示します。

```
command,user,waveset.resources,password.password,password.confirmPa
ssword,accounts[Windows Active
Directory].description,accounts[Corporate Directory].location
Create,John Doe,Windows Active Directory|Solaris
Server,changeit,changeit,John Doe - 888-555-5555,
Create,Jane Smith,Corporate Directory,changeit,changeit,,New York
CreateOrUpdate,Bill Jones,,,,,California
```

複数の値を持つフィールド

一部のフィールドには複数の値を指定できます。これらは複数値フィールドと呼ばれます。たとえば、waveset.resources フィールドでは、ユーザーに複数のリソースを割り当てることができます。1 つのフィールド内の複数の値を区切るには、縦棒 (|) 文字 (「パイプ」文字とも呼ばれる) を使用します。複数値の構文は、次のように指定できます。

```
value0 | value1 [ | value2 ... ] ] ]
```

既存のユーザーの複数値フィールドを更新する場合、現在のフィールドの値を 1 つ以上の新しい値で置き換えても、希望する指定にならないことがあります。値を一部削除したり、現在の値に追加する場合もあります。フィールド指示を使用すれば、既存のフィールドの値をどのように処理するかを指定できます。フィールド指示は、次のように、フィールド値の前に縦棒で囲んで指定します。

```
|directive [ ; directive ] | field values
```

選択できる指示は次のとおりです。

- Replace − 現在の値を指定した値で置き換えます。指示を指定しない場合 (または、List 指示のみを指定した場合) は、これがデフォルトになります。
- Merge − 指定した値を現在の値に追加します。重複する値はフィルタされます。
- Remove − 指定した値を現在の値から削除します。
- List − フィールドの値が 1 つしかない場合でも、複数の値があるかのように強制的に処理します。ほとんどのフィールドは値の数に関係なく適切に処理されるため、通常、この指示は必要ありません。別の指示とともに指定できるのはこの指示だけです。

注 フィールド値は大文字と小文字を区別します。Merge および Remove の指示を指定する場合はこれが重要です。値を正しく削除したり、マージで複数の類似した値ができないようにするには、値が正確に一致しなければなりません。

フィールド値の特殊文字

フィールド値にカンマ (,) または二重引用符 (") 文字を指定する場合、あるいは先行または後続するスペースを維持する場合は、フィールド値を二重引用符で囲む必要があります (" フィールド値 ")。さらに、フィールド値の二重引用符は 2 つの二重引用符 (") 文字で置き換える必要があります。たとえば、`"John ""Johnny"" Smith"` は、フィールド値で `John "Johnny" Smith` という結果になります。

縦棒 (|) または円記号 (¥) 文字をフィールド値に含める場合は、その前に円記号を指定する必要があります (¥| または ¥¥)。

一括アクションの表示属性

Create、Update、または CreateOrUpdate 操作を実行する場合は、ユーザー画面に、一括アクション処理でしか使用しない、または使用できない追加の属性があります。これらの属性はユーザーフォームで参照可能であり、一括アクションに固有の動作を可能にします。属性は次のとおりです。

- waveset.bulk.fields.*field_name* − この属性には、CSV の入力から読み込まれたフィールドの値が含まれます。*field_name* にはフィールド名を指定します。たとえば、command フィールドと user フィールドはそれぞれ、パス表現 `waveset.bulk.fields.command` および `waveset.bulk.fields.user` の属性内にあります。
- waveset.bulk.fieldDirectives.*field_name* − この属性は、指示を指定したフィールドに対してのみ定義されます。値は指示文字列です。
- waveset.bulk.abort − 現在の操作をアボートさせるには、このブール属性を true に設定します。
- waveset.bulk.abortMessage − waveset.bulk.abort が true に設定されているときに表示するメッセージ文字列を設定します。この属性を設定しない場合は、汎用的なアボートメッセージが表示されます。

ユーザーアカウントパスワードの操作

すべての Identity Manager ユーザーには、パスワードが割り当てられます。Identity Manager ユーザーパスワードが設定されると、ユーザーのリソースアカウントパスワードが同期されます。1 つ以上のリソースアカウントパスワードを同期させることができない場合 (たとえば、必須パスワードポリシーに従う場合) は、個別に設定できます。

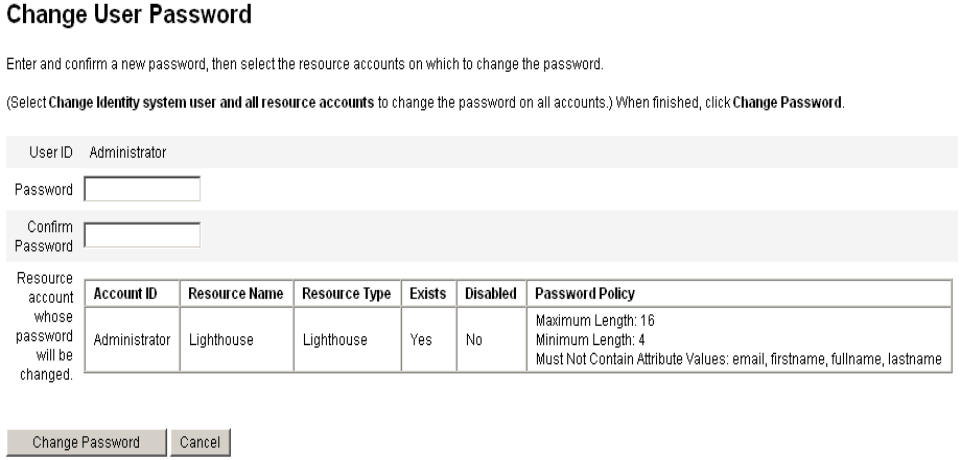
ユーザーアカウントパスワードの変更

ユーザーアカウントパスワードを変更するには、次を実行します。

1. メニューバーで、「パスワード」を選択します。

   次の図に示すように、「ユーザーパスワードの変更」ページがデフォルトで表示されます。

   図 3-10　　ユーザーパスワードの変更



2. 検索用語 (アカウント名、電子メールアドレス、名、姓など) を選択してから、検索タイプ (「が次の文字列で始まる」、「が次の文字列を含む」、または「が次の文字列と等しい」) を選択します。
3. 入力フィールドに検索語句の文字を 1 つ以上入力して、「検索」をクリックします。入力した文字が ID に含まれているすべてのユーザーのリストが返されます。ユーザーをクリックして選択すると、「ユーザーパスワードの変更」ページに戻ります。

4. 新しいパスワード情報を入力して確認し、「パスワードの変更」をクリックして、一覧表示されたリソースアカウントのユーザーパスワードを変更します。Identity Manager ではパスワードを変更するために実行した一連の操作を示すワークフロー図が表示されます。

ユーザーアカウントパスワードのリセット

Identity Manager ユーザーアカウントパスワードのリセットプロセスは、変更プロセスに類似しています。リセットプロセスがパスワードの変更と異なるのは、新しいパスワードを指定しない点です。代わりに、Identity Manager が、選択した項目とパスワードポリシーに応じて、ユーザーアカウント、リソースアカウント、またはその組み合わせの新しいパスワードをランダムに生成します。

直接の割り当てまたはユーザーの組織を通じた割り当てによってユーザーに割り当てられたポリシーは、次のようなリセットオプションを制御します。

- リセットが無効化されるまでにパスワードがリセットされる頻度
- 新しいパスワードを表示または送信する対象。ロールに対して選択した「リセット通知オプション」に応じて、Identity Manager は新しいパスワードを電子メールでユーザーに送信するか、リセットをリクエストした Identity Manager 管理者に結果ページで表示します。

リセット時のパスワードの期限切れ

デフォルトでは、ユーザーパスワードをリセットすると、そのパスワードはただちに期限切れになります。つまり、リセット後にユーザーがはじめてログインするとき、アクセスするためには新しいパスワードを選択する必要があります。このデフォルトの設定をフォームで無効にし、代わりに、ユーザーに関連付けられている Lighthouse アカウントポリシーで設定された期限切れパスワードポリシーに従ってユーザーのパスワードを期限切れにすることができます。

たとえば、「ユーザーパスワードのリセット」フォームで、`resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword` の値を `false` に設定します。

Lighthouse アカウントポリシーの「リセットオプション」フィールドを使用すると、次の 2 つの方法でパスワードを期限切れにすることができます。

- **「半永久」** – passwordExpiry ポリシー属性で指定された期間を使用して、パスワードがリセットされたときに現在の日付からの相対的な日付が計算され、その日付がユーザーに設定されます。値を指定しない場合、変更またはリセットされたパスワードは期限切れになりません。

- **「一時」** – tempPasswordExpiry ポリシー属性で指定された期間を使用して、パスワードがリセットされたときに現在の日付からの相対的な日付が計算され、その日付がユーザーに設定されます。値を指定しない場合、変更またはリセットされたパスワードは期限切れになりません。tempPasswordExpiry の値が 0 に設定されている場合、パスワードはただちに期限切れになります。

  `tempPasswordExpiry` 属性ポリシーは、パスワードがリセット (ランダムに変更) される場合にのみ適用され、パスワードの変更には適用されません。

アカウントセキュリティーと特権の管理

ここでは、セキュリティー保護されたアクセスをユーザーアカウントに与え、Identity Manager でユーザー特権を管理するために実行できる操作について説明します。

- パスワードポリシーの設定
- ユーザー認証
- 管理特権の割り当て

パスワードポリシーの設定

リソースパスワードポリシーは、パスワードの制限を設定します。強力なパスワードポリシーは、セキュリティーを高め、承認されていないログイン試行からリソースを保護する上で役立ちます。パスワードポリシーを編集して、一連の特性に対する値を設定または選択することができます。

パスワードポリシーの操作を開始するには、メニューバーの「セキュリティー」を選択し、「ポリシー」を選択します。

パスワードポリシーを編集するには、「ポリシー」リストから目的のポリシーを選択します。パスワードポリシーを作成するには、オプションの「新規」リストから「文字列の品質ポリシー」を選択します。

ポリシーの作成

パスワードポリシーは、文字列の品質ポリシーのデフォルトのタイプです。新しいポリシーの名前と任意で説明を指定したあとで、ポリシーを定義する規則のオプションとパラメータを選択します。

長さ規則

長さ規則は、パスワードの最小および最大必要文字数を設定します。このオプションを選択して規則を有効にし、規則の制限値を入力します。

文字タイプ規則

文字タイプ規則は、パスワードに指定できる特定のタイプの文字の最小および最大個数を設定します。次のものがあります。

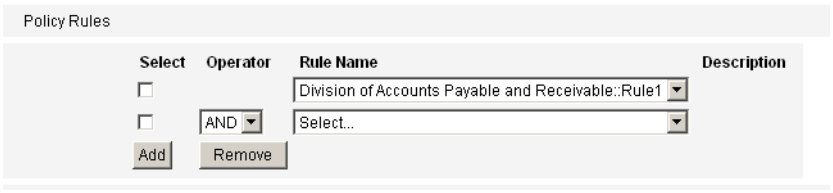
- 英字、数字、大文字、小文字、および特殊文字の最小および最大個数
- 挿入される数字の最小および最大個数
- 繰り返し文字および連続文字の最大個数
- 先頭の英字および数字の最小個数

各文字タイプ規則に制限数値を入力します。または、All を入力して、すべての文字がそのタイプになるように指定します。

文字タイプ規則の最小個数 : 図 3-11 に示すように、検証にパスする必要がある、文字タイプ規則の最小個数も設定できます。パスする必要のある最小個数は 1 です。最大個数は、有効にした文字タイプ規則の個数を越えることはできません。

注 パスする必要のある最小個数を最大値に設定するには、All と入力します。

図 3-11 パスワードポリシー (文字タイプ) 規則



辞書ポリシーの選択

辞書の単語と照合してパスワードをチェックすることもできます。このオプションを使用するには、次を実行する必要があります。

- 辞書の設定
- 辞書の単語の読み込み

辞書は「ポリシー」ページから設定します。辞書のセットアップの詳細については、『Identity Manager 配備ツール』の「辞書サポートの設定」の章を参照してください。

パスワード履歴ポリシー

新しく選択されたパスワードの直前に使用されていたパスワードの再利用を禁止することができます。

現在および直前のパスワードの再利用を禁止するには、「再使用してはいけない旧パスワードの個数」フィールドに 1 よりも大きい数値を入力します。たとえば、3 を入力した場合は、新しいパスワードを、現在のパスワードおよびその直前の 2 個のパスワードと同じにすることはできません。

以前に使用していたパスワードと類似した文字の再利用を禁止することもできます。「再使用できない旧パスワードに含まれる類似文字の最大個数」フィールドに、新しいパスワードで繰り返すことのできない、過去のパスワードからの連続文字の最大数を入力します。たとえば、7 を入力した場合、過去のパスワードが password1 であれば、新しいパスワードとして password2 や password3 を使用することはできません。

0 を指定した場合、連続性に関係なく、過去のパスワードに含まれるすべての文字を使用できません。たとえば、過去のパスワードが abcd の場合、新しいパスワードに a、b、c、d の各文字を使用することはできません。

この規則は、過去の 1 つ以上のパスワードに適用できます。チェックの対象となる過去のパスワードの数は、「再使用してはいけない旧パスワードの個数」フィールドに指定します。

使用禁止単語

パスワードに含むことのできない単語を 1 つ以上入力できます。入力ボックスで、1 行に 1 つずつ単語を入力してください。

また、辞書ポリシーを設定して実装することで、単語を除外することもできます。詳細については、141 ページの「辞書ポリシー」を参照してください。

使用禁止属性

パスワードに含むことのできない属性を 1 つ以上選択します。属性には次のものがあります。

- accountID
- email
- firstname
- fullname
- lastname

パスワードに含むことのできる「使用禁止」属性のセットを、`UserUIConfig` 設定オブジェクトで変更できます。`UserUIConfig` 内のパスワード属性は、`<PolicyPasswordAttributeNames>` に一覧表示されています。

パスワードポリシーの実装

パスワードポリシーは、リソースごとに設定します。パスワードポリシーを特定のリソースに割り当てるには、オプションの「パスワードポリシー」リストからポリシーを選択します。このリストは、「リソースの作成または編集ウィザード: Identity Manager パラメータ」ページの「ポリシー設定」エリアにあります。

ユーザー認証

パスワードを忘れたか、パスワードがリセットされた場合、ユーザーは、1 つ以上のアカウントの秘密の質問に答えることにより、Identity Manager へのアクセス権を取得できます。これらの質問とその管理規則を、Identity Manager アカウントポリシーの一部として設定します。パスワードポリシーとは異なり、Identity Manager アカウントポリシーはユーザーに直接割り当てられるか、「ユーザーの作成と編集」ページでユーザーに割り当てられた組織を通じて割り当てられます。

アカウントポリシーで認証を設定するには、次を実行します。

1. メニューバーの「セキュリティー」を選択し、「ポリシー」を選択します。
2. ポリシーのリストから「Default Identity Manager Account Policy」を選択します。

   ページの「二次認証ポリシーオプション」エリアで認証を選択できます。

重要！最初のセットアップ時に、ユーザーはユーザーインタフェースにログインして、秘密の質問に対する最初の回答を指定する必要があります。これらの回答を設定しない場合、ユーザーは自分のパスワードがなければログインできません。

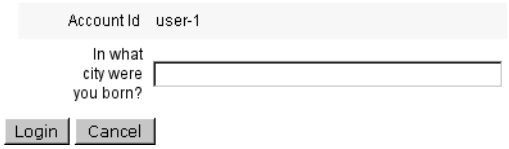
設定した認証規則に応じて、次に対して回答するようユーザーにリクエストすることができます。

- すべての秘密の質問
- 秘密の質問のいずれか 1 つ
- 質問セットからランダムに選択された質問。質問の数は、指定した値により決定します。
- 質問セットから連続して選択された 1 つ以上の質問

Identity Manager ユーザーインタフェースにログインして「パスワードをお忘れですか?」をクリックし、表示された質問に回答することで、認証の選択を確認することができます。

図 3-12 に「ユーザーアカウント認証」画面の例を示します。

図 3-12　　ユーザーアカウント認証

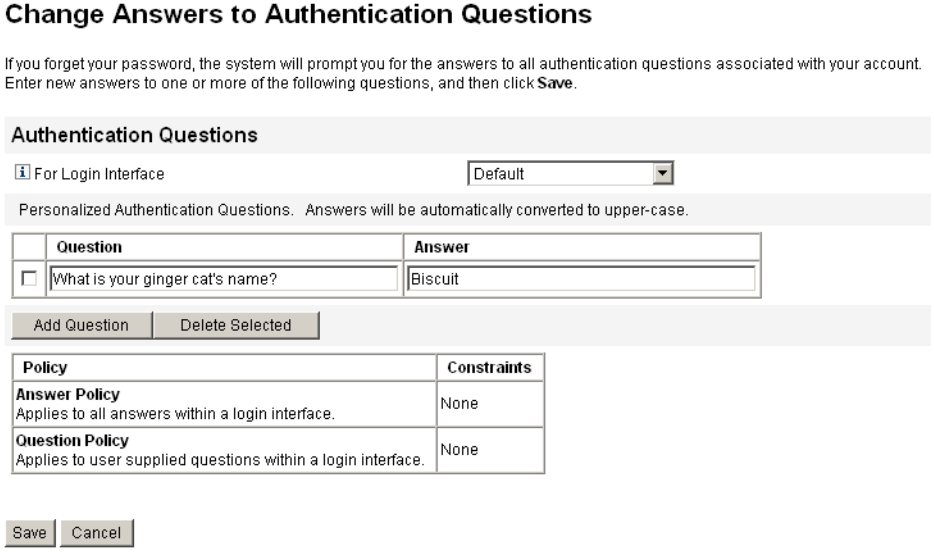


ユーザー独自の秘密の質問

Lighthouse アカウントポリシーでは、ユーザーがユーザーインタフェースおよび管理者インタフェースで独自の秘密の質問を入力できるようにするオプションを選択できます。また、ユーザー独自の秘密の質問を使用してログインに成功するためにユーザーが入力および回答する必要のある質問の最大数を設定することもできます。

設定後、ユーザーは、「秘密の質問の回答の変更」ページから質問を追加および変更できます。このページの例は、図 3-13 に示されています。

図 3-13　　回答の変更 ― ユーザー独自の秘密の質問



認証後のパスワード変更リクエストのバイパス

ユーザーが 1 つ以上の質問に回答して認証に成功すると、デフォルトでは、システムからユーザーに新しいパスワードの入力がリクエストされます。ただし、bypassChangePassword システム設定プロパティーを設定することによって、1 つ以上の Identity Manager アプリケーションでパスワードの変更リクエストをバイパスするように Identity Manager を設定できます。

認証に成功したあと、すべてのアプリケーションでパスワードの変更リクエストをバイパスするには、System Configuration オブジェクトで bypassChangePassword プロパティーを次のように設定します。

コード例 3-1 パスワード変更リクエストをバイパスするための属性の設定

```
<Attribute name="ui"
  <Object>
    <Attribute name="web">
      <Object>
        <Attribute name='questionLogin'>
          <Object>
            <Attribute name='bypassChangePassword'>
              <Boolean>true</Boolean>
            </Attribute>
          </Object>
        </Attribute>
        ...
      </Object>
    ...
```

特定のアプリケーションでこのパスワードリクエストを無効にするには、次のように設定します。

コード例 3-2 パスワード変更リクエストを無効にするための属性の設定

```
<Attribute name="ui">
  <Object>
    <Attribute name="web">
      <Object>
         <Attribute name='user'>
          <Object>
             <Attribute name='questionLogin'>
               <Object>
                  <Attribute name='bypassChangePassword'>
                   <Boolean>true</Boolean>
                  </Attribute>
               </Object>
             </Attribute>
               </Object>
        </Attribute>
        ...
      </Object>
    ...
```

管理特権の割り当て

次のような Identity Manager 管理特権または機能を、ユーザーに割り当てられます。

- 管理者ロール ー 管理者ロールを割り当てられたユーザーは、このロールで定義された機能および管理する組織を継承します。すべての Identity Manager ユーザーアカウントには、デフォルトでユーザー管理者ロールが作成時に割り当てられます。管理者ロールと管理者ロールの作成の詳細については、第 4 章の「Identity Manager リソースの設定」を参照してください。
- 機能 ー 機能は規則によって定義されます。Identity Manager では、機能は実用上の機能にグループ化され、このグループから選択することができます。機能の割り当てによって、より細かく管理特権を割り当てることができます。機能と機能の作成の詳細については、第 5 章の「機能とその管理について」を参照してください。
- 管理する組織 ー 管理する組織は、指定した組織に対する管理コントロール特権を与えます。詳細については、第 5 章の「Identity Manager 組織について」を参照してください。

Identity Manager 管理者と管理作業の詳細については、第 5 章「管理」を参照してください。

ユーザーの自己検索

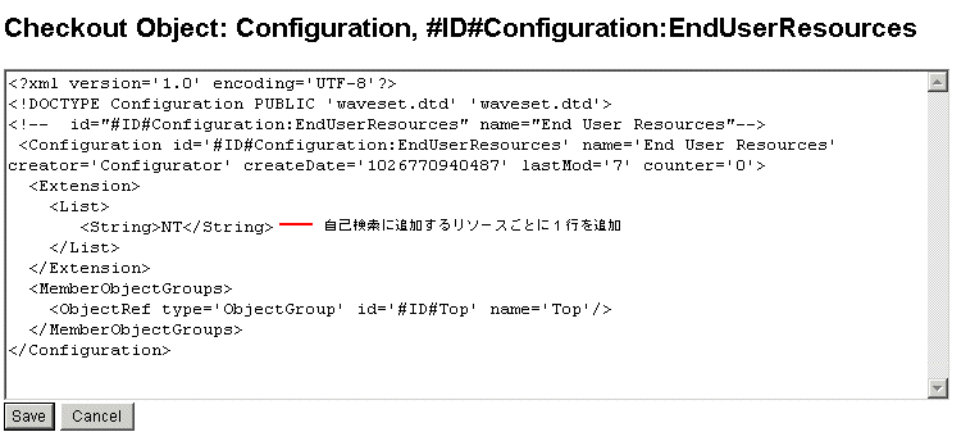
Identity Manager ユーザーインタフェースによって、ユーザーはリソースアカウントを検索できます。つまり、Identity Manager ID を持つユーザーは、存在するが、関連付けられていないリソースアカウントを ID に関連付けることができます。

自己検索の有効化

自己検索を有効にするには、特別な設定オブジェクト (エンドユーザーリソース) を編集して、アカウントの検索を許可される各リソースの名前を追加する必要があります。これを行うには、次の手順に従います。

1. Identity Manager システム設定ページを開きます (`idm/debug`)。
2. 「List Objects」ボタンの隣のリストから「Configuration」を選択し、「List Objects」ボタンをクリックします。
3. 「End User Resources」の隣の「Edit」をクリックすると、設定オブジェクトが表示されます。
4. `<String>`*Resource*`</String>` を追加します。ここで、図 3-14 に示すように、*Resource* はリポジトリ内のリソースオブジェクトの名前と一致します。

図 3-14　エンドユーザーリソースの設定オブジェクト



5. 「保存」をクリックします。

自己検索が有効になっている場合、Identity Manager ユーザーインタフェースの「プロファイル」メニュータブの下に新しい選択項目が表示されます (「自己検索」)。このエリアにより、ユーザーは、利用可能リストからリソースを選択し、リソースアカウント ID とパスワードを入力してアカウントを自分の Identity Manager ID にリンクすることができます。

相関規則と確認規則

操作の user フィールドに入力できる Identity Manager ユーザー名がわからない場合は、相関規則および確認規則を使用します。user フィールドの値を指定しない場合は、一括アクションを開始するときに相関規則を指定する必要があります。user フィールドの値を指定した場合、その操作の相関規則および確認規則は評価されません。

相関規則では、操作フィールドと一致する Identity Manager ユーザーを検索します。確認規則では、操作フィールドに対して Identity Manager ユーザーをテストし、ユーザーが一致するかどうかを確認します。この 2 段階のアプローチを使用すると、名前または属性を基にして可能性のあるユーザーをすばやく検出し、可能性のあるユーザーに対してのみ負荷が大きいチェックを実行することで、Identity Manager による相関を最適化することができます。

相関規則または確認規則を作成するには、サブタイプがそれぞれ SUBTYPE_ACCOUNT_CORRELATION_RULE または SUBTYPE_ACCOUNT_CONFIRMATION_RULE の規則オブジェクトを作成します。

相関規則と確認規則の詳細については、『Identity Manager の配備に関する技術情報』の「データ読み込みと同期」の章を参照してください。

相関規則

相関規則の入力は、操作フィールドのマップです。出力は次のいずれかである必要があります。

- 文字列 (ユーザー名または ID を含む)
- 文字列要素 (ユーザー名または ID) のリスト
- WSAttribute 要素のリスト
- AttributeCondition 要素のリスト

一般的な相関規則は、操作のフィールドの値に基づいてユーザー名のリストを生成します。相関規則は、ユーザーを選択するために使用される属性条件 (`Type.USER` のクエリー可能な属性を参照する) のリストを生成することもできます。

相関規則は、比較的低コストでかつできるかぎり選択能力を高くする必要があります。可能な場合は、コストのかかる処理は確認規則に回します。

属性条件は、`Type.USER` のクエリー可能な属性を参照する必要があります。これらは、Identity Manager `UserUIConfig` オブジェクト内に `QueryableAttrNames` として設定されます。

拡張属性の相関を行うには特別な設定が必要です。

- 拡張属性は、`UserUIConfig` 内でクエリー可能として指定する必要があります (`QueryableAttrNames` のリストに追加される)。
- `UserUIConfig` の変更を有効にするために、Identity Manager アプリケーション (またはアプリケーションサーバー) の再起動が必要な場合があります。

確認規則

確認規則の入力は次のとおりです。

- **`userview`** − Identity Manager ユーザーの完全表示。
- **`account`** − 操作フィールドのマップ。

確認規則は、ユーザーが操作フィールドに一致する場合は true、それ以外の場合は false という文字列形式のブール値を返します。

一般的な確認規則は、ユーザー表示の内部値と操作フィールドの値を比較します。相関処理のオプションの 第 2 段階として、確認規則は相関規則内に設定できないチェック (または相関規則内で評価するにはコストがかかりすぎるチェック) を実行します。一般に、次のような場合にのみ確認規則が必要です。

- 相関規則が複数の一致するユーザーを返す
- 比較する必要があるユーザー値がクエリー可能ではない

確認規則は、相関規則によって返される一致したユーザーごとに 1 回実行されます。

匿名登録

匿名登録機能を使用すると、Identity Manager アカウントを持っていないユーザーがアカウントをリクエストして取得することができます。

匿名登録の有効化

デフォルトで、匿名登録機能は無効になっています。有効にするには、次の手順に従います。

1. 管理者インタフェースにログインします。
2. **「設定」**を選択し、**「ユーザーインタフェース」**を選択します。
3. 「匿名登録」エリアで「有効化」オプションを選択し、**「保存」**をクリックします。

ユーザーがユーザーインタフェースにログインすると、**「アカウントのリクエスト」**ボタンがログインページに表示されるようになります。

匿名登録の設定

「ユーザーインタフェース」ページの「匿名登録」エリアから、匿名登録プロセスのオプションを設定できます。

- **「通知テンプレート」** – アカウントをリクエストしているユーザーへの通知メールの送信に使用される電子メールテンプレートの ID を指定します。
- **「プライバシーポリシーへの同意が必要」** – これを選択した場合、ユーザーはアカウントをリクエストする前に、プライバシーポリシーを受け入れる必要があります。これはデフォルトで有効になっています。
- **「検証の有効化」** – これを選択した場合、ユーザーはアカウントをリクエストする前に、その登録内容を検証する必要があります。これはデフォルトで有効になっています。

- **「プロセス開始 URL」**− URL を入力し、匿名登録プロセスでどのワークフローを使用するかを指定します。
- **「通知の有効化」**− これを選択すると、アカウントが作成されたときに、通知電子メールがユーザーに送信されます。
- **「電子メールドメイン」**− ユーザーの電子メールアドレスの構築に使用される電子メールドメインの名前を入力します。

完了したら、**「保存」**をクリックします。

ユーザー登録プロセス

ユーザーはユーザーインタフェースログインページで**「アカウントのリクエスト」**をクリックすることによってアカウントをリクエストできます。

2 ページの登録ページのうちの最初のページが表示され、姓、名、および従業員 ID を求められます。「検証の有効化」属性が選択されている場合 (デフォルト)、ユーザーは次のページに進む前にこの情報を検証する必要があります。

`EndUserLibrary` の `verifyFirstname`、`verifyLastname`、`verifyEmployeeId`、および `verifyEligibility` 規則がそれぞれの属性の情報を検証します。

注 これらの 1 つまたは複数の規則の変更が必要になる場合もあります。特に、従業員 ID を検証する規則を変更し、Web サービス呼び出しや Java クラスを使用して情報を検証するようにしてください。

「検証の有効化」属性が無効になっている場合、最初の登録ページは表示されません。この場合、「End User Anonymous Enrollment Completion」フォームを変更して、通常、最初の検証フォームによって取得される情報をユーザーが入力できるようにする必要があります。

登録ページで提供された情報から、Identity Manager は以下を生成します。

- ユーザー ID (名と姓の頭文字のあとに従業員 ID を繋げた文字列)。
- 次の形式の電子メールアドレス。

  FirstName.LastName@EmailDomain

  EmailDomain は、匿名登録設定の「電子メールドメイン」属性で設定されたドメインです。
- マネージャー属性 (`idmManager`)。`EndUserRuleLibrary:getIdmManager` 規則を変更することにより、この属性を設定できます。デフォルトでは、マネージャーは Configurator に設定されています。マネージャーとして指定された管理者は、ユーザーアカウントがプロビジョニングされる前にユーザーのリクエストを承認する必要があります。

- 組織属性。EndUserRuleLibrary:getOrganization 規則をカスタマイズすることによって、この属性を設定できます。デフォルトでは、ユーザーは組織階層の最上位 (「Top」) に割り当てられます。

登録ページでユーザーによって入力された情報が正しく検証された場合、2 ページ目の登録ページがユーザーに表示されます。ユーザーはこのページでパスワードおよびパスワード確認を入力する必要があります。また、「プライバシーポリシーへの同意が必要」属性が選択されている場合、ユーザーはプライバシーポリシーの条件に同意するオプションを選択する必要があります。

ユーザーが「登録」をクリックすると、確認ページが表示されます。「通知の有効化」属性が選択されている場合、アカウントの作成後、ユーザーに電子メールが送信されることがページに示されます。

ユーザー作成の標準プロセス (idmManager 属性およびポリシー設定が要求する承認を含む) の完了後、アカウントが作成されます。

第 4 章

設定

この章では、管理者インタフェースを使用した Identity Manager オブジェクトとサーバープロセスのセットアップの説明および手順を示します。Identity Manager オブジェクトの詳細については、「概要」の章の 37 ページの「Identity Manager オブジェクト」を参照してください。

注 Service Provider を実装するための Identity Manager の設定の詳細については、第 13 章「サービスプロバイダの管理」を参照してください。

この章は、次のトピックで構成されています。

- ロールとその管理について
- Identity Manager リソースの設定
- Identity Manager ChangeLog
- アイデンティティー属性およびイベントの設定
- Identity Manager ポリシーの設定
- 電子メールテンプレートのカスタマイズ
- 監査グループおよび監査イベントの設定
- Remedy との統合
- Identity Manager サーバーの設定

ロールとその管理について

この節では、Identity Manager でのロールのセットアップについて説明します。

ロールとは

Identity Manager ロールは、アカウントを管理するリソースの集まりを定義します。ロールを使用すると、ユーザークラスのプロファイルを作成し、類似した特性を持つ Identity Manager ユーザーをグループ化できます。

各ユーザーに 1 つ以上のロールを割り当てることも、ロールを割り当てないこともできます。ある 1 つのロールを割り当てられたすべてのユーザーは、同じベースグループのリソースへのアクセスを共有することになります。

1 つのロールに関連付けられたすべてのリソースは、ユーザーに間接的に割り当てられます。間接的な割り当ては、ユーザーに対して明確にリソースが選択される点で、直接的な割り当てとは異なります。

ロールを作成または編集すると、`ManageRole` ワークフローが開始されます。このワークフローでは、新しいロールまたは更新されたロールをリポジトリに保存し、ロールが作成または保存される前に承認などの操作を挿入することができます。

ロールは、管理者インタフェースの「ユーザーの作成と編集」ページでユーザーに割り当てます。

ロールの作成

次のいずれかの方法でロールを作成できます。

1. Identity Manager メニューバーで、「ロール」を選択します。
2. 「ロール」ページで、「新規」をクリックします。

   「ロールの作成」ページでは、次のことができます。

   - リソースとリソースグループをロールに割り当てる。
   - ロール承認者を選択して通知選択を行う。

ヒント 承認プロセスの詳細については、200 ページの「アカウントの承認」を参照してください。

   - ロールを除外する。つまり、このロールがユーザーに割り当てられているときに、除外されたロールを割り当てることはできません。

- このロールを割り当て可能にする組織を選択する。
- ロールに割り当てられているリソースの属性値を編集する。

割り当てられているリソース属性値の編集

「ロールの作成」ページの「割り当てられたリソース」エリアで「属性値の設定」をクリックして、ロールに割り当てられた各リソースの属性リストを表示します。この「属性の編集」ページで、各属性の新しい値を指定したり、属性値の設定方法を決定できます。Identity Manager の値は、直接設定するだけでなく、規則を使用して設定することもできます。また、既存の値を上書きしたり、既存の値にマージしたりすることもできます。

各リソースアカウント属性の値を設定するには、選択を行います。

- **「値の上書き」** – 次のいずれかのオプションを選択します。
  - **「なし」** – デフォルトの選択です。値は設定されません。
  - **「規則」** – 規則を使用して値を設定します。このオプションを選択した場合、リストから規則を選択する必要があります。
  - **「テキスト」** – 指定されたテキストを使用して値を設定します。このオプションを選択した場合、テキストを入力する必要があります。
- **「設定方法」** – 次のいずれかのオプションを選択します。
  - **「デフォルト値」** – 規則またはテキストをデフォルト属性値にします。この値はユーザーが変更または上書きできます。
  - **「値を設定」** – 規則またはテキストに指定されたように属性値を設定します。値が設定され、ユーザーの変更は上書きされます。
  - **「値とマージ」** – 規則またはテキストに指定された値に現在の属性値をマージします。
  - **「値とマージ、既存の値をクリア」** – 現在の属性値を消去し、このロールおよび割り当てられているその他のロールによって指定されるマージ値を値として設定します。
  - **「値から削除」** – 規則またはテキストに指定された値を属性値から削除します。
  - **「強制的に値を設定」** – 規則またはテキストに指定されたように属性値を設定します。値が設定され、ユーザーの変更は上書きされます。ロールを削除すると、新しい値が以前に属性上に存在していても NULL となります。
  - **「強制的に値とマージ」** – 規則またはテキストに指定された値に現在の属性値をマージします。ロールを削除すると、新しい属性値が以前に属性上に存在していても NULL となります。

複数値属性の場合、カンマ区切り値 (CSV) 文字列を使用することを示すためにリポジトリ内でロールオブジェクトを編集する必要があります。たとえば、次のようになります。

```
<RoleAttribute name='attrs role:Database Table:attrs' csv='true'>
```

- **「強制的に値とマージ、既存の値をクリア」** – 現在の属性値を消去し、このロールおよび割り当てられているその他のロールによって指定されるマージ値を値として設定します。ロールが削除されると、属性上に以前に存在していても、このロールによって指定された属性値はクリアされます。

- **「規則名」** – 「値の上書き」エリアで「規則」を選んだ場合、リストから規則を選択します。
- **「テキスト」** – 「値の上書き」エリアで「テキスト」を選んだ場合、追加するテキスト、削除するテキスト、または属性値として使用するテキストを入力します。

「OK」をクリックして変更を保存し、「ロールの作成」または「ロールの編集」ページに戻ります。

ロールの管理

「ロール」ページにあるロールのリストからロールに一連のアクションを実行できます。

- ロールの編集 – ロールのリストでロールを選択し、表示されるページでロールの属性を修正します。
- ロールの検索 – 「ロール」エリアで「ロールの検索」を選択します。ロールは、以下の 1 つ以上の検索の種類によって検索できます。
  - 名前
  - 可用性
  - 承認者
  - リソース
  - リソースグループ

検索の種類を複数選択した場合、指定されたすべての基準と一致しないと検索結果は返されません。検索は、大文字と小文字を区別しません。

- ロールのクローン作成または名前の変更 – 編集するロールを選択して、「名前」フィールドに新しい名前を入力して、「保存」をクリックします。新しいロールを作成するには、表示されるページで「作成」をクリックします。

ロール名の変更

ロール名を変更するには、次を実行します。

1. 編集するロールを選択します。
2. 「名前」フィールドに新しい名前を入力して、「保存」をクリックします。

   Identity Manager に「作成または名前変更」ページが表示されます。
3. ロール名を変更するには、「名前の変更」をクリックします。

ロールとリソースロールの同期

Identity Manager ロールをリソース上でネイティブに作成されたロールと同期することができます。同期すると、デフォルトでリソースはロールに割り当てられます。これには、タスクを使用して作成されたロール、およびいずれかのリソースロール名に一致する既存の Identity Manager ロールが該当します。

メニューバーで、「タスク」を選択してから「タスクの実行」タブを選択して、「アイデンティティーシステムのロールをリソースのロールと同期させる」タスクページを表示します。タスクを起動するには、同期タスクの名前、リソース、使用するリソースロール属性、ロールが適用される組織を指定して、「起動」をクリックします。

Identity Manager リソースの設定

この節では、Identity Manager リソースのセットアップの説明および手順を示します。

リソースとは

Identity Manager リソースには、アカウントが作成されるリソースまたはシステムへの接続方法についての情報が格納されています。Identity Manager リソースは、リソースに関連する属性を定義するものであり、Identity Manager でリソース情報を表示する方法を指定する際に役立ちます。

Identity Manager では、次のような広範囲なリソースタイプに対応したリソースを提供します。

- メインフレームセキュリティーマネージャー
- データベース
- ディレクトリサービス

- オペレーティングシステム
- Enterprise Resource Planning (ERP) システム
- メッセージプラットフォーム

インタフェースの「リソース」エリア

既存のリソースに関する情報は、「リソース」ページに表示されます。

リソースにアクセスするには、メニューバーの「リソース」をクリックします。

リソースはタイプごとにグループ化され、リスト内で名前付きのフォルダによって表されます。階層表示を展開して、現在定義されているリソースを表示させるには、フォルダの隣にあるインジケータをクリックします。表示を折りたたむには、マークをもう一度クリックします。

リソースタイプフォルダを展開すると、中に含まれるリソースオブジェクトの数が動的に更新されて表示されます (グループをサポートするリソースタイプの場合)。

リソースの一部には、次のような、管理可能な追加のオブジェクトを持つものがあります。

-  組織
-  組織単位
-  グループ
-  ロール

リソースリストからオブジェクトを選択し、次のオプションリストのいずれかから操作を選択して、管理タスクを開始します。

- **「リソースアクション」** ― 編集、アクティブな同期、名前変更、削除など各種のアクションを実行し、リソースオブジェクトの操作やリソース接続の管理も行います。
- **「リソースオブジェクトアクション」** ― リソースオブジェクトの編集、作成、削除、名前変更、別名保存、検索を行います。
- **「リソースタイプアクション」** ― リソースポリシーの編集、アカウントインデックスの操作、管理するリソースの設定を行います。

リソースを作成または編集すると、`ManageResource` ワークフローが開始されます。このワークフローでは、新しいリソースまたは更新されたリソースをリポジトリに保存し、リソースが作成または保存される前に承認などの操作を挿入することができます。

リソースリストの管理

リソースを作成するときのリソース選択リストは、管理者インタフェースの「リソース」タブで管理します。「リソースタイプアクション」オプションリストから「管理するリソースの設定」を選択して、リソースリストに表示するリソースを選択します。

「管理するリソース」ページでは、Identity Manager のリソースが次の 2 つのカテゴリに分類されています。

- **Identity Manager リソース** – このテーブルに含まれるリソースは、Identity Manager で頻繁に管理されるリソースです。このテーブルは、リソースのタイプとバージョンを示します。「管理しますか?」列でオプションを選択することによって、1 つ以上のリソースを選択し、「保存」をクリックしてそれらをリソースリストに追加します。
- **カスタムリソース** – このページエリアを使用して、カスタムリソースをリソースリストに追加します。

カスタムリソースを追加するには、次の手順を実行します。

1. 「カスタムリソースの追加」をクリックして、行をテーブルに追加します。
2. リソースのリソースクラスパスを入力するか、独自に開発したリソースを入力します。
3. 「保存」をクリックして、リソースをリソースリストに追加します。

表 4-1 に、カスタムリソースクラスを示します。

表 4-1 カスタムリソースクラス

カスタムリソース	リソースクラス
Access Manager	com.waveset.adapter.AccessManagerResourceAdapter
ACF2	com.waveset.adapter.ACF2ResourceAdapter
ActivCard	com.waveset.adapter.ActivCardResourceAdapter
Active Directory	com.waveset.adapter.ADSIResourceAdapter
Active Directory Active Sync	com.waveset.adapter.ActiveDirectoryActiveSyncAdapter
ClearTrust	com.waveset.adapter.ClearTrustResourceAdapter
DB2	com.waveset.adapter.DB2ResourceAdapter
INISafe Nexess	com.waveset.adapter.INISafeNexessResourceAdapter
Microsoft SQL Server	com.waveset.adapter.MSSQLServerResourceAdapter
MySQL	com.waveset.adapter.MySQLResourceAdapter
Natural	com.waveset.adapter.NaturalResourceAdapter

表 4-1　カスタムリソースクラス (続き)

カスタムリソース	リソースクラス
NDS SecretStore	com.waveset.adapter.NDSSecretStoreResourceAdapter
Oracle	com.waveset.adapter.OracleResourceAdapter
Oracle Financials	com.waveset.adapter.OracleERPResourceAdapter
OS400	com.waveset.adapter.OS400ResourceAdapter
PeopleSoft	com.waveset.adapter.PeopleSoftCompIntfcAdapter com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
RACF	com.waveset.adapter.RACFResourceAdapter
SAP	com.waveset.adapter.SAPResourceAdapter
SAP HR	com.waveset.adapter.SAPHRResourceAdapter
SAP Portal	com.waveset.adapter.SAPPortalResourceAdapter
Scripted Host	com.waveset.adapter.ScriptedHostResourceAdapter
SecurID	com.waveset.adapter.SecurIdResourceAdapter com.waveset.adapter.SecurIdUnixResourceAdapter
Siebel	com.waveset.adapter.SiebelResourceAdapter
SiteMinder	com.waveset.adapter.SiteminderAdminResourceAdapter com.waveset.adapter.SiteminderLDAPResourceAdapter com.waveset.adapter.SiteminderExampleTableResourceAdapter
Sun ONE Identity Server	com.waveset.adapter.SunISResourceAdapter
Sybase	com.waveset.adapter.SybaseResourceAdapter
Top Secret	com.waveset.adapter.TopSecretResourceAdapter

リソースの作成

リソースは、リソースウィザードを使用して作成します。リソースウィザードでは、リソース上のオブジェクトを管理するために、Identity Manager リソースアダプタを作成する手順を、順を追って実行します。

リソースウィザードを使用して、次の項目を設定します。

- **「リソース固有のパラメータ」**― これらの値は、このリソースタイプの特定のインスタンスを作成するときに Identity Manager インタフェースから修正できます。
- **「アカウント属性」**― リソースのスキーママップに定義されます。これらによって、Identity Manager ユーザー属性がリソースの属性にどのようにマップされるかが決まります。

- **「アカウントの DN またはアイデンティティーテンプレート」** – ユーザーに対するアカウント名の構文が含まれています。アカウント名の構文は、階層構造の名前空間で特に重要です。
- **「リソースの Identity Manager パラメータ」** – ポリシーをセットアップし、リソースの承認者を設定し、リソースに対する組織のアクセス権をセットアップします。

リソースを作成するには、次を実行します。

1. 「リソースタイプアクション」オプションリストから「新規リソース」を選択します。

   Identity Manager に「新規リソース」ページが表示されます。

2. リソースタイプを選択してから「新規」をクリックして、リソースウィザードの「ようこそ」ページを表示します。

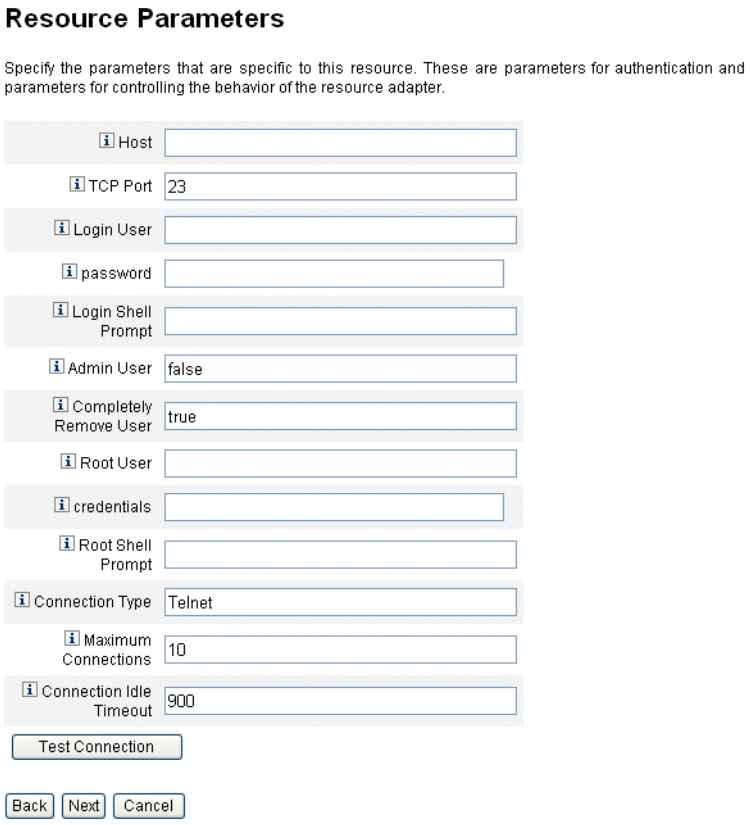
注 または、リソースリストでリソースタイプを選択してから、「リソースタイプアクション」リストで「新規リソース」を選択することもできます。この場合、Identity Manager に「新規リソース」ページは表示されませんが、リソースウィザードがただちに起動します。

---

3. 「次へ」をクリックして、リソースの定義を開始します。リソースウィザードの手順とページは、次の順序で表示されます。

   - **「リソースパラメータ」** – 認証とリソースアダプタの動作を管理するためのリソース固有のパラメータをセットアップします。パラメータを入力して「テスト接続」をクリックし、接続が有効であることを確認します。確認できたら、「次へ」をクリックして、アカウント属性をセットアップします。図 4-1 に「リソースパラメータ」ページを示します。

図 4-1　リソースウィザード : リソースパラメータ

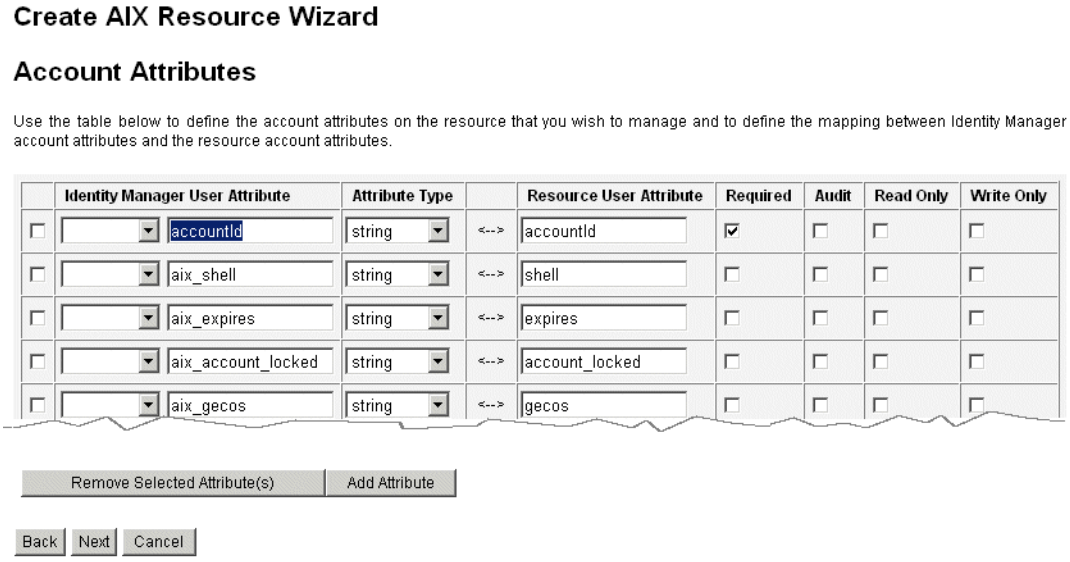


- **「アカウント属性」(スキーママップ)** – Identity Manager アカウント属性をリソースアカウント属性にマップします。

  属性を追加する場合は、「属性の追加」をクリックします。属性を 1 つ以上選択し、「選択した属性の削除」をクリックすると、スキーママップから属性が削除されます。削除が終了したら、「次へ」をクリックしてアイデンティティーテンプレートをセットアップします。

  図 4-2 に、リソースウィザードの「アカウント属性」ページを示します。

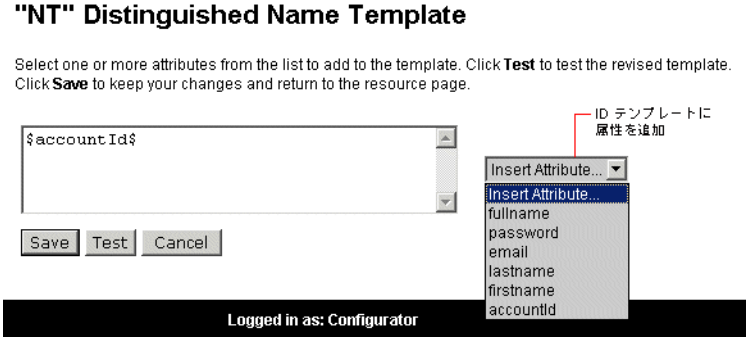
図 4-2　　リソースウィザード : アカウント属性 (スキーママップ)



- **「アイデンティティーテンプレート」** – ユーザーに対するアカウント名の構文を定義します。この機能は、階層構造の名前空間で特に重要です。

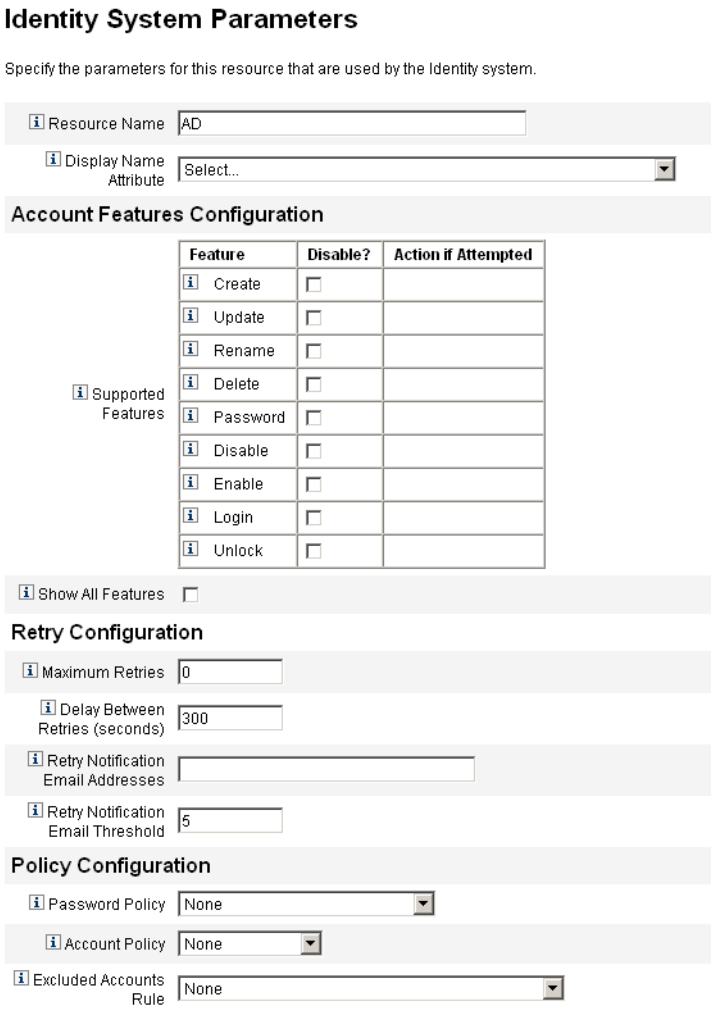
  「属性の挿入」リストから属性を選択します。テンプレートから属性を削除するには、リスト内をクリックし、文字列から 1 つ以上の項目を削除してください。属性名と前後の $ (ドル記号) の両方を削除してください。

図 4-3　　リソースウィザード : アイデンティティーテンプレート



- 「Identity System パラメータ」 – 図 4-4 に示すように、リソースに、再試行およびポリシー設定などの Identity Manager パラメータを設定します。

図 4-4　リソースウィザード : アイデンティティーシステムのパラメータ



ページ間を移動するには、「次へ」および「戻る」を使用します。選択がすべて終了したら、「保存」をクリックしてリソースを保存し、リストページに戻ります。

リソースの管理

リソースリストのリソースに対して一連の編集操作を実行できます。リソースウィザードの各ページの編集機能に加え、次の操作も実行できます。

- **リソースの削除**－1 つ以上のリソースを選択して、「リソースアクション」リストから「削除」を選択します。複数のリソースタイプを同時に選択することができます。ロールまたはリソースグループが関連付けられているリソースは削除できません。
- **リソースオブジェクトの検索** － リソースを選択して「リソースオブジェクトアクション」リストから「検索」を選択すると、オブジェクト特性によってリソースオブジェクト (組織、組織単位、グループ、または個人など) を検索できます。
- **リソースオブジェクトの管理** － リソースタイプによっては、新しいオブジェクトを作成できるものがあります。リソースを選択して、「リソースオブジェクトアクション」リストから「リソースオブジェクトの作成」を選択します。
- **リソース名の変更** －リソースを選択して、「リソースアクション」リストから「名前の変更」を選択します。表示される入力ボックスに新しい名前を入力して、「名前の変更」をクリックします。
- **リソースのクローン作成**－ リソースを選択して、「リソースアクション」リストから「名前を付けて保存」を選択します。表示される入力ボックスに新しい名前を入力します。クローンとして作成されたリソースが、選択した名前でリソースリストに表示されます。
- **リソース上での一括アクションの実行** － (CSV 形式の入力から) リスト内のすべてのリソースに適用するリソースおよびアクションのリストを指定します。続いて一括アクションを起動して、一括アクションバックグラウンドタスクを開始します。

アカウント属性の操作

Identity Manager リソースは、スキーママップを使用して、外部リソース (リソースアカウント属性) から取得した属性の名前とタイプを定義します。次に、それらの属性を標準の Identity Manager アカウント属性にマップします。スキーママップをセットアップする (リソースウィザードの「アカウント属性」ページで) ことにより、次を実行できます。

- リソース属性を、企業に必須のもののみに制限する。
- 複数のリソースで使用する一般的な Identity Manager 属性名を作成する。
- 必須のユーザー属性と属性タイプを識別する。

これらの値にアクセスするには、リソースリストからリソースを選択して、「リソースアクション」リストから「リソーススキーマの編集」を選択します。

スキーママップの左の列 (タイトルは「Identity System ユーザー属性」) には、Identity Manager 管理者インタフェースおよびユーザーインタフェースで使用されるフォームで参照される Identity Manager アカウント属性の名前が含まれています。スキーママップの右の列 (タイトルは「リソースユーザー属性」) には、外部ソースの属性名が含まれています。

Identity System 属性名を定義することにより、異なるリソースの属性を一般的な名前で定義できます。たとえば、Active Directory リソースの場合、Identity Manager の `lastname` 属性は Active Directory リソース属性の `sn` にマップされます。GroupWise の場合、`fullname` 属性は GroupWise 属性の `Surname` にマップできます。その結果、管理者は `lastname` に対して一度値を定義するだけで済み、ユーザーを保存するときには異なる名前のリソースにその値が渡されます。

リソースグループ

「リソース」エリアは、リソースグループを管理するためにも使用します。リソースグループは、リソースをグループ化して特定の順序で更新できるようにします。グループにリソースを入れて順序付けし、そのグループをユーザーに割り当てることで、そのユーザーのリソースが作成、更新、および削除される順序が決定します。

アクティビティーは、各リソースに対して順番に実行されます。あるリソースで操作が失敗した場合、残りのリソースは更新されません。このような関係は、関連するリソースがある場合に重要です。

たとえば、Exchange 5.5 のリソースは、既存の Windows NT または Windows Active Directory アカウントに依存します。つまり、Exchange アカウントを作成するには、その前にこれらのどちらかが存在している必要があります。Windows NT のリソースと Exchange 5.5 のリソースを持つリソースグループを (順番に) 作成することにより、正しいユーザー作成順序を保証できます。逆に、この順序により、ユーザーの削除時には正しい順序でリソースが削除されることが保証されます。

「リソース」を選択して「リソースグループのリスト」を選択すると、現在定義されているリソースグループのリストが表示されます。そのページで「新規」をクリックして、リソースグループを定義します。リソースグループの定義時には、選択エリアで選択を行い、選択したリソースを順序付けするほか、リソースグループを利用可能にする組織を選択することができます。

グローバルリソースポリシー

リソースのグローバルリソースポリシー内のプロパティーを編集できます。「グローバルリソースポリシー属性の編集」ページから、次のポリシー属性を編集できます。

- Default Capture Timeout − アダプタがタイムアウトになるまでに、アダプタがコマンド行プロンプトを待機する必要のある最大時間を指定する値を、ミリ秒単位で入力します。この値は、GenericScriptResourceAdapter または ShellScriptSourceBase アダプタにのみ適用されます。コマンドまたはスクリプトの結果が重要であり、アダプタによって解析されるときにこの設定を使用します。

  この設定のデフォルト値は 30000 (30 秒) です。

- Default Wait for Timeout − スクリプト化されたアダプタが、コマンドに文字 (または結果) が用意されているかどうかをチェックするまで、ポーリング間で待機する最大時間を指定する値を、ミリ秒単位で入力します。この値は、GenericScriptResourceAdapter または ShellScriptSourceBase アダプタにのみ適用されます。コマンドまたはスクリプトの結果をアダプタが調べない場合に、この設定を使用します。

- Wait For Ignore Case − タイムアウトするまでに、コマンド行プロンプトをアダプタが待機する必要のある最大時間を指定する値を、ミリ秒単位で入力します。この値は、GenericScriptResourceAdapter または ShellScriptSourceBase アダプタにのみ適用されます。大文字と小文字を区別しない場合に、この設定を使用します。

- Resource Account Password Policy − 該当する場合、選択したリソースに適用するリソースアカウントパスワードポリシーを選択します。「なし」がデフォルトの選択です。

- Excluded Resource Accounts Rule − 該当する場合、除外されるリソースアカウントを制御する規則を選択します。「なし」がデフォルトの選択です。

ポリシーに対する変更を保存するには、「保存」をクリックする必要があります。

追加タイムアウト値の設定

Waveset プロパティーファイルを編集することにより、`maxWaitMilliseconds` プロパティーを変更できます。`maxWaitMilliseconds` プロパティーは、操作のタイムアウトを監視する頻度を制御します。この値が指定されていない場合、システムは 50 のデフォルト値を使用します。

この値を設定するには、Waveset.properties ファイルに次の行を追加します。

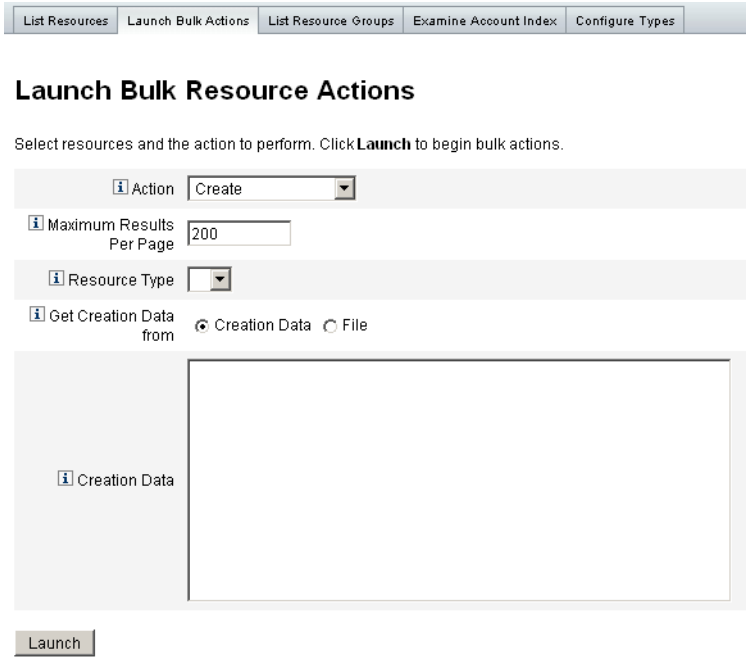
```
com.waveset.adapter.ScriptedConnection.ScriptedConnection.maxwaitMilliseconds.
```

一括リソースアクション

CSV 形式のファイルを使用するか、操作に適用するデータを作成または指定して、リソースに対して一括アクションを実行できます。

図 4-5 は、作成アクションを使用した一括アクションの起動ページを示しています。

図 4-5　「一括リソースアクションの起動」ページ



一括リソース操作に使用できるオプションは、操作に選択したアクションによって異なります。操作に適用するアクションを 1 つ指定するか、「アクションリストから」を選択して複数のアクションを指定できます。

- **「アクション」** – アクションを 1 つ指定するには、次のオプションの 1 つを選択します。作成、複製、更新、削除、パスワードの変更、パスワードのリセット。

  アクションを 1 つ選択すると、アクションに関連するリソースを指定するオプションが表示されます。作成アクションの場合は、リソースのタイプを指定します。

  「アクションリストから」を指定した場合は、「アクションリストの取得先」エリアを使用して、アクションを含んだ使用するファイル、または「入力」エリアで指定するアクションのいずれかを指定します。

注	ファイル内または入力エリアリストに入力したアクションは、カンマ区切り値 (CSV) 形式にする必要があります。

- **「ページあたりの最大結果数」** – このオプションを使用して、各タスク結果ページに表示される一括アクション結果の最大数を指定します。デフォルト値は 200 です。

操作を開始するには、「起動」をクリックします。これはバックグラウンドタスクとして実行されます。

Identity Manager ChangeLog

この節では、Identity Manager ChangeLog 機能の説明および ChangeLog の設定と使用の手順を示します。

ChangeLog とは

ChangeLog には、Identity Manager リソースに含まれるアイデンティティー属性情報が表示されます。それぞれの ChangeLog は、アイデンティティー属性のサブセットに加えられた変更を取得するように定義されています。

リソースの属性データに変更があると、Active Sync アダプタはその情報を取得して、変更を ChangeLog に書き込みます。次に、エンタープライズ内のリソースの操作専用に開発されたカスタムスクリプトが ChangeLog を読み取って、リソースを更新します。

ChangeLog 機能はプロビジョニングシステムからリソースへとカスタムスクリプトを介して間接的に通信するので、Identity Manager の標準的なリソースアクティブ同期機能や調整機能とは異なります。

ChangeLog とセキュリティー

Identity Manager の ChangeLog 機能を実行するには、ローカルファイルシステム内の指定されたディレクトリに対する書き込み権が必要です。Web コンテナによっては、Identity Manager のようなホストされる Web モジュールに対してローカルファイルシステムへのアクセスをデフォルトで許可していないものもあります。

その場合には、Java ポリシーファイルを編集してアクセス権を付与します。`/tmp/changelogs` を指定ディレクトリとして使用する場合には、ポリシーファイルに次の内容が含まれるようにします。

```
grant {
    permission java.io.FilePermission "/tmp/changelogs/*",
"read,write,delete";
};
```

指定したそれぞれの ChangeLog に対してファイルアクセス権を定義する必要があります。

Java 用のデフォルトのセキュリティーポリシーファイルは次の場所にあります。

```
$JAVA_HOME/jre/lib/security/java.policy
```

このファイルを編集すれば十分かもしれませんが、デフォルトファイルではない独自のファイルを使用している場合には、サーバーは次のようなオプションが指定された状態で稼働しています。

```
-Djava.security.manager
-Djava.security.policy=/path/to/your/java.policy
```

この場合は、`java.security.policy` システムプロパティーによって特定されるファイルを編集します。

注 セキュリティーポリシーファイルを編集したあとで、Web コンテナの再起動が必要になる場合があります。

ChangeLog 機能の要件

ChangeLog 機能の要件として、ChangeLog を設定する前にアイデンティティー属性を設定する必要があります。

注 131 ページの「アイデンティティー属性およびイベントの設定」の節で説明する手順を行なって、これらの要件を満たします。

ChangeLog の設定

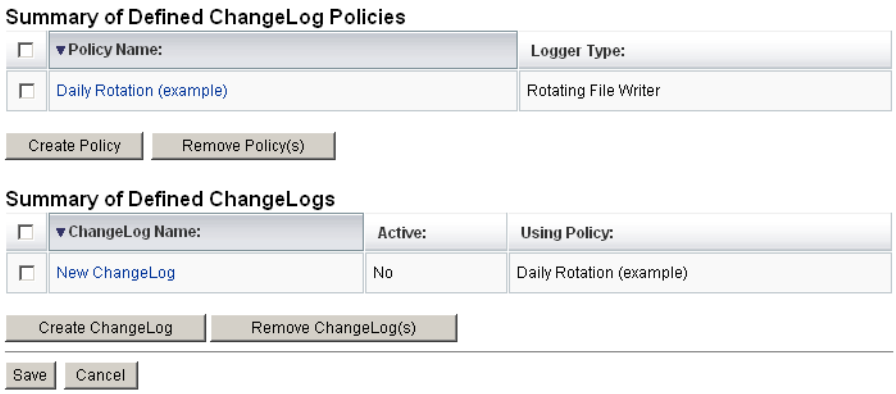
ChangeLog の設定は、ChangeLog ポリシーと ChangeLog を作成することによって行います。それぞれの ChangeLog には、関連付けられた ChangeLog ポリシーがなければなりません。ChangeLog は Active Sync によって検出されアイデンティティー属性に適用される変更のサブセットを定義したもので、ログ形式で書き込まれます。ChangeLog に関連付けられる ChangeLog ポリシーは、ChangeLog ファイルに書き込む方法を定義します。ChangeLog ファイルの内容はカスタムスクリプトによって使用されます。

ChangeLogs および ChangeLog ポリシーを設定するには、「メタビュー」を選択し、「ChangeLog」を選択します。

Identity Manager によって、次のような 2 つの概要エリアが含まれた「ChangeLog 設定」ページが表示されます。

注 アイデンティティー属性が設定されていない場合、「ChangeLog」タブは表示されません。

図 4-6 「ChangeLog 設定」



ChangeLog ポリシーの概要

「ChangeLog ポリシー」概要エリアには、現在定義されている ChangeLog ポリシーが表示されます。既存の ChangeLog ポリシーを編集するには、リスト内のポリシーの名前をクリックします。ChangeLog ポリシーを作成するには、「ポリシーの作成」をクリックします。

1 つ以上の ChangeLog ポリシーを削除するには、ChangeLog ポリシーを選択して、「ポリシーの削除」をクリックします。このアクションには確認は不要です。

ChangeLog の概要

ChangeLog の概要エリアには、現在定義されている ChangeLog が表示されます。既存の ChangeLog を編集するには、リスト内の名前をクリックします。ChangeLog を作成するには、「ChangeLog の作成」をクリックします。

1 つ以上の ChangeLog を削除するには、ChangeLog を選択して、「ChangeLog の削除」をクリックします。このアクションには確認は不要です。

ChangeLog 設定変更の保存

ChangeLog 設定に対して行う変更は、ChangeLog ポリシーと定義済み ChangeLog のどちらに対する変更であるとしても、「ChangeLog 設定」ページから保存する必要があります。「保存」をクリックすると変更が保存され、メタビューに戻ります。

ChangeLog ポリシーの作成と編集

「ChangeLog ポリシーの編集」ページで次の項目に入力および選択を行なって、ChangeLog ポリシーを作成または編集します。

- **「ポリシー名」** – 一意なポリシーの名前を入力します。
- **「毎日の開始時刻」** – ローテーションが開始または交替する時刻の算定に使用する時刻を設定します。このポリシーを使用する ChangeLog は、この時刻に、またこの時刻から計算した一定の間隔で新しいローテーションを開始します。たとえば、開始時刻を午前零時 (00:00) に、「1 日のローテーション数」を 3 に設定した場合、ログファイルのプレフィックスは 00:00、08:00、16:00 に変更になります。

  ファイル名の形式は `cl_User_yyyyMMddHHmmss.n.suffix` です。*HHmmss* はローテーションが開始した最近の時刻を表します (*n* はシーケンス番号で、*suffix* は ChangeLog 定義で指定されたサフィックス)。

  開始時刻を '00:00'、ローテーション回数を 3 にし、ChangeLog を午前 9:24 に起動することにした場合、朝の順番のローテーション名には最近のローテーション開始時刻 (08:00 など) が組み込まれます。この例の場合は、ファイル名が `cl_User_yyyyMMdd080000` で始まります。そして、新しいローテーション (ファイル名の新しいプレフィックス) が 16:00 に開始します。

- **「1 日のローテーション数」** – 1 日にログを切り替える回数を指定します。たとえば、4 時間ごとにローテーションを切り替える場合は、6 の値を入力します。

  この値には負でない整数のみ指定できます。値 0 は、このフィールドを無視することを意味します。このフィールドが 0 でないときは、「ローテーションの最大有効期間」設定が無視されます。

このローテーションの長さを秒数で指定し、かつ「1 日のローテーション回数」フィールドが 0 である場合は、「ローテーションの最大有効期間」の値を使用してローテーションの期間が決定されます。

「ローテーションの最大有効期間」には負ではない整数値のみ指定できます。「1 日のローテーション回数」にゼロではない数を指定した場合には、その値が使用されます (「ローテーションの最大有効期間」の値は使用されない)。これら両方のフィールドの値が 0 である場合は、シーケンス情報のみが適用されます。この場合は「毎日の開始時刻」も使用されません。

- **「保存するローテーション数」** − Identity Manager が削除するまでに蓄積できるローテーションの数を指定します。たとえば、1 日のローテーションが 3 回で、2 日間の変更をログに保存する場合は、6 の値を指定します。
- **「ファイルの最大サイズ (バイト単位)」** − 現在のファイルに変更を書き込むとこの制限を超える場合、同じローテーションプレフィックスで新しいシーケンス番号の付いた新しいログファイルが開始されます。値 0 は、この制限を使用しないことを示します。サイズ、行数、および有効期間の制限フィールドは、値が 0 でなければそれらすべてが使用されます。ただし、サイズの制限が 3 つの制限の中で最初にチェックされます。
- **「ファイルの最大サイズ (行単位)」** − 現在のファイルに変更を書き込むと行数がこの制限を超える場合には、新しいシーケンスのファイルが作成され、超過した行は新しいファイルに書き込まれます。値 0 は「制限なし」を表します。この制限は、サイズ制限の次、有効期間制限の前にチェックされます。
- **「ファイルの最大有効期間 (秒単位)」** − 変更を受け取ったときに、既存のシーケンスファイルがここに指定されている秒数以前のものである場合には、新しいシーケンスファイルが作成され、そこに変更が書き込まれます。値 0 は、この制限を使用しないことを示します。他の制限がゼロではない場合は、それらがこの制限より先に適用されます。

「OK」をクリックすると、「ChangeLog 設定」ページに戻ります。新しい ChangeLog ポリシーを保存する、または既存のポリシーへの変更を保存するために、必ず「ChangeLog 設定」ページから「OK」をクリックしてください。

ChangeLog の作成と編集

「ChangeLog の編集」ページで次の項目に入力および選択を行なって、ChangeLog を作成または編集します。

- **「ChangeLog 名」** – 一意な ChangeLog の名前を入力します。
- **「アクティブ」** – このオプションを選択した場合、ChangeLog は監視を行い、Active Sync リソースを通してアイデンティティー属性に変更が伝達されたときに、その変更を記録します (この処理が行われるためには、Active Sync がアイデンティティー属性アプリケーションであることが必要)。
- **「フィルタ」** – 使用する ChangeLog フィルタの名前を入力します。「Noop」はデフォルトフィルタを使用し、すべての変更を受け入れることを意味します。ほとんどの場合、この設定で十分です。この設定を使用しない場合は、`com.sun.idm.changelog.ChangeLogFilter` を実装する Java クラスを指定することになります。このクラスはサーバーのクラスパスに配置され、またパブリックなデフォルトコンストラクタが含まれている必要があります。
- **「次の操作をログに記録」** – 作成、更新、および削除など、選択したタイプのイベントのログを記録します。選択されていないイベントは無視されます。
- **「ChangeLog ビュー」** – このテーブルを使用して、ChangeLog の内容 (列) を定義します。テーブルの各行は ChangeLog の列を指定します。ChangeLog 列を追加するには「列の追加」をクリックします。それぞれの列には、名前、タイプ、アイデンティティー属性名があります。行の順序は列の順序を示します。列を定義したあとで列の順序を並び替えるには、「上へ」と「下へ」のボタンを使用します。

注 どの ChangeLog にも、テーブルの 1 列目に `'changeType'` という名前の暗黙の列があります。この 1 列目の暗黙の列は、変更のタイプを示します。この列のタイプは「テキスト」です。ログのデータは `'ADD'`、`'MOD'`、`'DEL'` のいずれかの値となります。

- **「使用するポリシー名」** – リストから定義済みの ChangeLog ポリシーを選択して、ロギングに使用します。
- **「出力パス」** – ファイルシステム上でログファイルを格納するディレクトリの名前を入力します。この格納先をネットワーク上にマウントされた場所にすることも可能ですが、サーバーと同じシステム内のディレクトリを使用することをお勧めします。ChangeLog ごとに一意な場所を使用するのもよい方法です。
- **「サフィックス」** – ChangeLog ファイルのサフィックスを入力します (`.csv` など)。選択したサフィックスを使用して、ChangeLog ファイル同士を区別することもできます。

「OK」をクリックすると、「ChangeLog 設定」ページに戻ります。新しい ChangeLog を保存する、または既存の ChangeLog への変更を保存するために、必ず「ChangeLog 設定」ページから「OK」をクリックしてください。

例

次の例には、アイデンティティー属性と ChangeLog をセットアップして特定の属性データのセットを取得する方法が詳しく示されています。

例 : アイデンティティー属性の定義

この例では、2 つの Identity Manager リソース (Resource 1 と Resource 2) が 3 つ目のリソース (Resource 3) にソースデータを提供します。Resource 3 は Identity Manager システムに直接には接続していません。Resource 1 と 2 からデータサブセットを取得し、それを Resource 3 に提供して保守するには、ChangeLog が必要です。

```
Resource 1: EmployeeInfo
employeeNumber*
givenname
mi
surname
phone

Resource2 : OrgInfo
employeeNum*
managerEmpNum
departmentNumber

Resource 3 : PhoneList
empId*
fullname
phone
department
```

注 * はレコードを相互に関連付けるキーを表します。

アイデンティティー属性の定義は次の表のようになります。

表 4-2 変更ログの使用例でのアイデンティティー属性

属性	<==	元になる Resource.Attribute
employee	<==	EmployeeInfo.employeeNumber
dept	<==	OrgInfo.departmentNumber

表 4-2　変更ログの使用例でのアイデンティティー属性 (続き)

属性	<==	元になる Resource.Attribute
reportsTo	<==	OrgInfo.managerEmpNum
firstName	<==	EmployeeInfo.givename
lastName	<==	EmployeeInfo.surname
middleInitial	<==	EmployeeInfo.mi
fullname	<==	firstName + " " + middleInitial + " " + lastName
phoneNumber	<==	EmployeeInfo.phone

例 : ChangeLog の設定

アイデンティティー属性を定義したら、次に PhoneList ChangeLog という名前の ChangeLog を定義します。この目的は、アイデンティティー属性のサブセットを ChangeLog ファイルに書き込むことです。

PhoneList ChangeLog の ChangeLogView

列名	種類	アイデンティティー属性
empId	テキスト	employee
fullname	テキスト	fullname
phone	テキスト	phoneNumber

Resource 1 または Resource 2 内のレコードが変更されると、変更された内容だけではなく、ChangeLog レコードのデータの完全セット、つまりアイデンティティー属性のすべてのデータが ChangeLog に書き込まれます。カスタムスクリプトはその情報を読み取り、それを使用して Resource 3 を設定します。

ChangeLog の CSV ファイル形式

この節では、ChangeLog によって作成されるカンマ区切り値 (CSV) ファイルの形式について説明します。

ChangeLog ファイルは、スプレッドシートやデータベーステーブルなどのように、「行」と「列」でできているものと考えてください。その「行」に当たるものが、ファイルの 1 行です。

ChangeLog 形式は、最初の 2 行を使用する自己記述型です。この 2 行が 1 組で「スキーマ」つまりテーブル内の各「セル」の論理名と論理タイプを定義します (「セル」とは、行上のカンマで区切られた 1 つ 1 つの値のこと)。

1 行目には、ファイル内の属性の名前が列挙されます。2 行目には、それらの属性の値のタイプが記述されます。それ以降の行は、すべて変更イベントのデータです。

ChangeLog ファイルは Java UTF-8 形式でエンコードされます。

列

ファイルの 1 列目は特に重要です。この列は操作タイプを定義し、変更イベントが作成、変更、または削除のアクションであったかどうかなどを示します。ここには常に `changeType` が入り、常にタイプ `T` (テキスト) です。その値は `ADD`、`MOD`、`DEL` のどれかです。

決まった 1 つの列にエントリの一意の識別子 (主キー) が保持されるようにしてください。通常、これはファイルの 2 列目です。

それ以外の列には、属性の名前が入ります。その名前は ChangeLog View テーブルの「列名」値から取られます。

行

ファイルの「スキーマ」を定義する最初の 2 つのヘッダー行に続いて、残りの行には属性の値が入ります。それらの値は 1 行目の列項目の順序に従って表示されます。ChangeLog はアイデンティティー属性から適用されるので、ChangeLog には変更が検出された時点でユーザーに関するすべてのデータが含まれます。

また、NULL (または設定されていないこと) を表す特別なセンチネル値はありません。変更が検出されているのに値がない場合、ChangeLog は空の文字列を書き込みます。

値は、ファイルの 2 行目に指定されている列のタイプにしたがってエンコードされます。サポートされているタイプは次のとおりです。

- `T`: テキスト
- `B`: バイナリ
- `MT`: 複数テキスト
- `MB`: 複数バイナリ

テキスト値

テキスト値は文字列として書き込まれますが、次の 2 つの例外があります。

- 値に , （ カンマ ）が含まれている場合、¥ (円記号) が挿入されて Identity Manager は値の中のカンマをエスケープします。たとえば、fullname の値が Doe, John である場合、Identity Manager は、Doe ¥,John を値として書き込みます。
- 値に ¥ (円記号) 文字が含まれる場合は、¥ がもう 1 つ付け足されて Identity Manager は円記号をエスケープします。たとえば、homedir の値に C:¥users¥home が含まれている場合、Identity Manager はログに C:¥¥users¥¥home を書き込みます。

テキスト値に復帰改行文字を含めることはできません。ファイルに復帰改行が必要な場合は、バイナリ値タイプを使用してください。

バイナリ値

バイナリ値は Base64 でエンコードされます。

複数テキスト値

複数テキスト値はテキスト値と同じように書き込まれますが、カンマで区切られ、[と] の括弧で囲まれます。

複数バイナリ値

複数バイナリ値はバイナリ値と同じように Base64 でエンコードされて書き込まれますが、カンマで区切られ、[と] の括弧で囲まれます。

出力形式の例

次に例を挙げて、さまざまな出力形式を示します。例の書式は次のとおりです。

```
column1, column2, column3, column4
```

各例の Column 3 にサンプルテキストが示されます。

- テキスト (T) データは、ファイル内で次のように文字列として表示されます。

  ```
  ADD,account0,some text data,column4
  ```

- バイナリ (B) データは Base64 でエンコードされて表示されます。

  ```
  ADD,account0,FGResWE23WDE==,column4
  ```

- 複数テキスト (MT) は次のように表示されます。

  ```
  ADD,account0,[one,two,three],column4
  ```

- 複数バイナリ (MB) は次のように表示されます。

  ```
  ADD,account0,[FGResWE23WDE==,FGRCAFEBADE3sseGHSD],column4
  ```

注 Base64 のアルファベットには , (カンマ)、[(左括弧)、] (右括弧) の各文字、または復帰改行記号は含まれていません。

ChangeLog のファイル名

ファイル名の形式は次のとおりです。

```
servername_User_timestamp.sequenceNumber.suffix
```

各表記の意味は次のとおりです。

- *timestamp* は、このログが開始またはロールオーバーした時刻です。複数のファイルが同じタイムスタンプである場合は、「ローテーション」と見なされます。
- *sequenceNumber* は、バイト数、行数、秒数の最大値に従ってローテーションをファイルのサブセットに分割する際に使用する数値で、この数値は増え続けます。それらの各ファイルを「シーケンス」ファイルと呼びます。
- *suffix* は、ChangeLog 設定で定義されるファイル拡張子で、通常は `.csv` です。

ローテーションとシーケンスの設定

ローテーションとシーケンスは `ChangeLogPolicy` オブジェクトで定義され、ChangeLogs から参照されます。

例

あるポリシーが次の条件でローテーションを定義するとします。

- 午前 7:00 に開始する。
- 2 日間、毎日 3 回ローテーションする。

この条件の場合、ローテーションファイルには次のように名前が付けられることになります (ローテーションごとに 2 つのシーケンスファイルがある)。

```
myServer_User_20060101070000.1.csv
myServer_User_20060101070000.2.csv
myServer_User_20060101150000.1.csv
myServer_User_20060101150000.2.csv
myServer_User_20060101230000.1.csv
myServer_User_20060101230000.2.csv

myServer_User_20060102070000.1.csv
myServer_User_20060102070000.2.csv
myServer_User_20060102150000.1.csv
myServer_User_20060102150000.2.csv
myServer_User_20060102230000.1.csv
myServer_User_20060102230000.2.csv
```

1 月 1 日は 07:00:00 から始まって 8 時間ごとに 3 回ローテーションされており、ファイル名の日付部分が 20060102 となっていることを除けば、1 月 2 日も同様にローテーションされています。

ChangeLog スクリプトの作成

この節では、ChangeLog スクリプトを作成する上で役立つ情報を提供します。

- スクリプトは、新しいデータや新しいファイルを待ったり、あるいはアクティビティーの合間に休眠しながら、取得したファイルを読み取っては各行の変更内容をバックエンドリソースに適用するというように、継続的に実行されるものです。
- ChangeLog は削除操作をサポートしますが、その場合 `accountId` 値が `DEL` 行に書き込まれるだけです。
- ローテーションとシーケンスを使用することにより、スクリプトを実行する頻度を決めることができます。たとえば、次のように指定できます。
  - 午前零時にローテーションし、毎晩前回のローテーションに対してスクリプトを実行する。
  - 午前 8:00 から始めて 4 時間ごとにローテーションし、スクリプトを 4 時間ごとに (8 時、12 時、16 時、20 時、24 時、4 時、...) 実行する。
  - ローテーションはなしにして、シーケンス番号が増えるときにシーケンスファイルを読み取るかたちでスクリプトを実行する。シーケンス番号を増やす基準は、サイズベース、数値演算ベース、時間ベースで制御できます。
- 各 ChangeLog をバックエンドシステム内のレコードの表現と見ることができます。ログを読み取るスクリプトにとって処理しやすくするために、Identity Manager は特定のレコードに関しては、それが変更されているかどうかに関わりなく必ずそのすべてのデータを書き込みます。スクリプトはそのレコードのすべてのデータをそのまま適用します。

  ただし、スクリプトはバックエンドリソース (またはスクリプト) が、特に `ADD` と `DEL` に関して、次のいずれかの方法を取れるようにしておく必要があります。
  - べき等な操作を行える (べき等とは、データを複数回適用しても 1 回適用したときと変わらないこと意味する)。スクリプトが ChangeLog を最初から最後まで 2 回受け取って読み取る場合、受け取った後のリソース内のデータレコードの状態は 2 回とも厳密に一致しているべきです。
  - 操作を 1 回しか行えない。たとえば、追加および削除アクションに関してリソースをべき等にできない場合、ログエントリを一回だけ読み取るか、そうでなければ進捗を追跡するかして、スクリプトによる変更の適用が必ず一回だけになるようにする必要があります。

- 新しいシーケンスファイルが作成されたことを確認してから、その前のシーケンスファイルにあるデータを適用する方法がよいこともあります。.2 ファイルが作成されるまでは .1 ファイルを適用しないようにし、.3 ファイルが作成されたら .2 ファイルのデータを適用するという要領で行います。あるファイルのデータを適用したら、そのことをディスクに記録します。この方法により、`fstat` や `tail -f` などの呼び出しを使用しないで済みます。

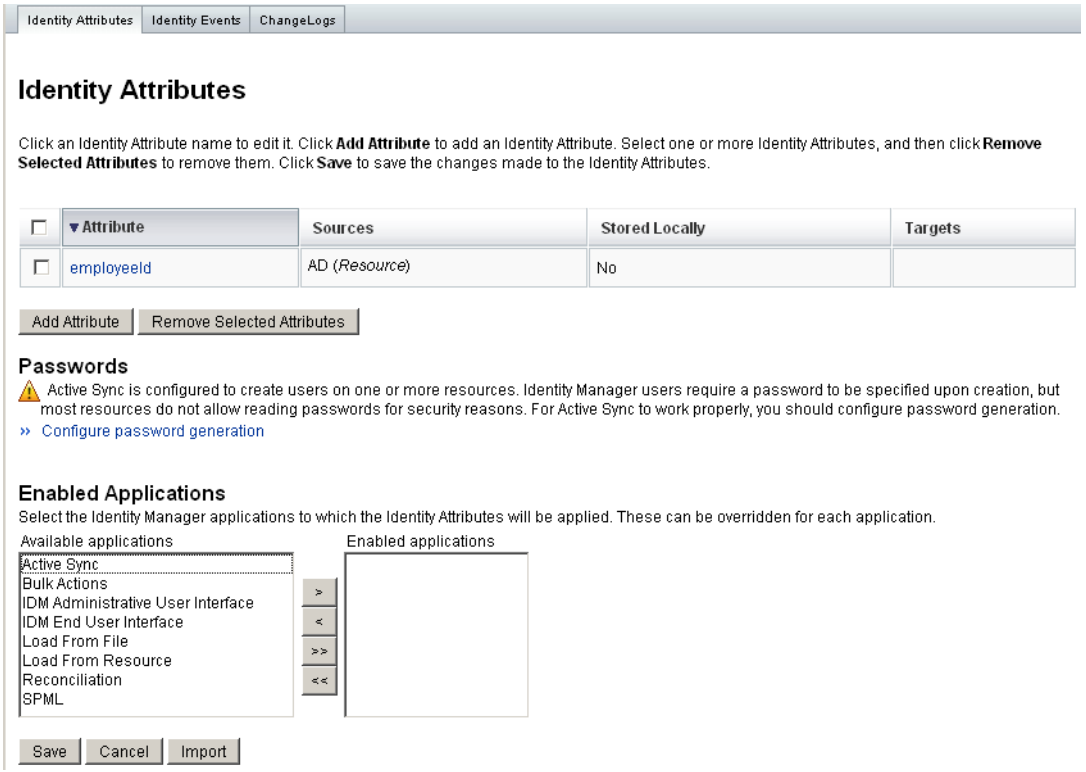
アイデンティティー属性およびイベントの設定

管理者インタフェースの「メタビュー」エリアを使用して、アイデンティティー属性およびイベントを設定します。次の節の情報と手順を使用して、Identity Manager アイデンティティー属性とアイデンティティーイベントを設定し、属性とイベントが適用される Identity Manager システムアプリケーションを選択してください。

アイデンティティー属性の操作

アイデンティティー属性を設定するには、「メタビュー」を選択して、「アイデンティティー属性」を選択します。「アイデンティティー属性」ページが表示されます。次の図は、このページの例を示しています。

図 4-7　メタビューでのアイデンティティー属性の設定



アイデンティティー属性を追加するには、「属性の追加」をクリックします。一度リストに追加されたアイデンティティー属性は、リスト内の名前をクリックすることによって編集できます。1 つ以上のアイデンティティー属性を削除するには、アイデンティティー属性を選択して、「選択した属性の削除」をクリックします。

属性に追加または属性から削除する応答を 1 つ以上選択できます。

アクションを実行する前に、必ず「保存」をクリックしてください。

アイデンティティー属性を最後に修正してからリソースを変更している場合は、「アイデンティティー属性」ページに次の警告メッセージが表示されます (図 4-8)。警告メッセージの「リソースの変更に基づいてアイデンティティー属性を設定」をクリックして、変更を同化させます。

図 4-8　「リソースが変更されています」警告メッセージ

パスワード

Active Sync は、1 つまたは複数のリソース上にユーザーを作成するよう設定されています。Identity Manager ユーザーは、作成時にパスワードを指定する必要がありますが、ほとんどのリソースがセキュリティー上の理由によりパスワードの読み取りを許可しません。パスワードの生成が設定されていない場合は、「パスワード生成の設定」をクリックします。

Active Sync によって作成されたアイデンティティーユーザーとその他のリソースアカウント上で、パスワードの設定方法を選択します。

- **「デフォルトパスワードを使用」** – このオプションを選択してからパスワードを入力します。password.password アイデンティティー属性がこの値からユーザーパスワードを設定します。
- **「規則を使用してパスワードを生成」** – パスワード生成に使用する規則を選択する場合は、このオプションを選択します。`password.password` アイデンティティー属性は、選択された規則を使用してパスワードを生成します。
- **「アイデンティティーシステムアカウントポリシーによるパスワード生成を使用」** – パスワード生成に使用するポリシーを選択する場合は、このオプションを選択します。このオプションを選択すると、`waveset.assignedLhPolicy` アイデンティティー属性が選択したポリシーに設定されます。選択したポリシーがパスワードを生成するよう設定されていない場合、ポリシーを作成および修正するのに必要な権限を持っていれば、ポリシーのコピーを作成したり、既存のポリシーを修正したりできる追加オプションがページに再表示されます。

  このオプションは、アイデンティティーシステムアカウントポリシーに設定されたパスワードポリシーに基づいてパスワードをランダムに生成します。ランダムなパスワード生成に依存しているため、これは、もっともセキュリティー保護されたパスワード生成オプションです。

アプリケーションの選択

「有効なアプリケーション」エリアを使用して、アイデンティティー属性を適用するアイデンティティーシステムアプリケーションを選択します。「利用可能なアプリケーション」エリアから 1 つ以上のアプリケーションを選択して、「有効なアプリケーション」エリアに移動します。アクションを実行する前に、必ず「保存」をクリックしてください。

注 ChangeLog 機能を使用するには、Active Sync アプリケーションを使用可能にする必要があります。詳細については、222 ページの「ActiveSync アダプタ」を参照してください。

アイデンティティー属性の追加と編集

「アイデンティティー属性の追加」または「アイデンティティー属性の編集」ページから、次の項目に関して選択して、アイデンティティー属性を追加または編集します。

- **「属性名」** – 属性名を選択または入力します。与えられているデフォルト値から (リソーススキーママップエントリ、オペレーショナルアイデンティティー属性、およびユーザー拡張属性から) 選択するか、またはテキストボックスに値を入力します。
- **「ソース」** – このアイデンティティー属性の値に利用する 1 つ以上のソースを選択します。ソースは順番に評価され、アイデンティティー属性は最初の null 以外の値に設定されます。
  - **「リソース」** – 値は、選択したリソース上の選択済み属性に由来します。
  - **「規則」** – 値は選択した規則の評価に由来します。
  - **「定数」** – 値は提供された定数値に設定されます。

  + (プラス記号) をクリックすると、新規行が追加され、別のソースを選択できます。ソースの横にある - (マイナス記号) をクリックすると、新規行は削除されます。ソースを並べ替え直すには、矢印をクリックしてリスト内でリソースを上下に移動させます。
- **「属性のプロパティー」** – このエリアを使用して、アイデンティティー属性のプロパティー設定を指定します。
  - **「アイデンティティー属性の設定方法」** – 次のいずれかのオプションを選択して、Identity Manager がリソース上の属性の値を設定する方法を指定します。
    - **「値を設定」** – アイデンティティー属性の値がすべてのターゲットに対して優先的に設定されます。このオプションを選択すると、ユーザーがフォームに入力したすべての値、および、ワークフロー、規則、ロールに設定された値よりも、ソースによって決められた値が優先されます。このオプションは一般的な実装に適した設定です。

アイデンティティー属性の追加情報については、『Identity Manager の配備に関する技術情報』を参照してください。

- **「デフォルト値」** – 値がない場合にのみターゲット上で属性値を設定します。
- **「値とマージ」** – 値を既存の値に追加します。重複する値はフィルタされます。

- **「IDM リポジトリに属性を保存」** – アイデンティティー属性をアイデンティティーシステムリポジトリにローカルに格納することを選択します。このオプションは、アイデンティティーシステムユーザーにアイデンティティー属性を保存する権限があるか、またはアイデンティティー属性がクエリーを処理できるようにする必要がある場合に選択します。
- **「割り当てられたすべてのリソースに値を設定」** – アイデンティティー属性をサポートするすべての割り当て済みリソースに対してアイデンティティー属性をグローバルに設定する場合に、このオプションを選択します。

- **「ターゲット」** – このアイデンティティー属性を設定するターゲットリソースを選択します。ターゲットが何も定義されていない場合は、「ターゲットの追加」をクリックします。リストからターゲットを削除するには、ターゲットを選択して、「選択したターゲットを削除」をクリックします。

  「OK」をクリックすると、アイデンティティー属性が追加され、「アイデンティティー属性」ページに戻ります。「アイデンティティー属性」ページで「保存」をクリックして、追加した内容を必ず保存してください。

ターゲットリソースの追加

アイデンティティー属性が ChangeLog のみに使用されている場合は、そのターゲットを設定する必要はありません。たとえば、ChangeLog を使用したいが、標準の「入力フォーム」を使用してデータを Active Sync に送信するようにもしたいという場合が、そのようなケースです。ターゲットがない場合には、メタビューはアイデンティティー属性の値の計算のみを行い、ほかのどのリソースにも値を設定しません。

次の項目の選択を行なって、アイデンティティー属性を設定するターゲットリソースを追加します。

- **「ターゲットリソース」** – 選択したアイデンティティー属性を設定するターゲットリソースを選択します。
- **「ターゲット属性」** – 値を受け取るターゲットリソースの属性の名前を選択します。
- **「条件」** – 選択したアイデンティティー属性の設定をこのターゲットリソースで行うかどうかを決めるときに実行する規則を選択します。この規則からは true または false の値が戻されるようにします。条件が設定されていない場合、ターゲット属性は常に選択されたイベントタイプに対して設定されます。

- **「適用イベント:」**－ このターゲットリソースで、選択したアイデンティティー属性を設定するイベントのタイプを選択します。この選択内容が「条件」と組み合わされて、ターゲット属性を設定するかどうかが判別されます。

  「OK」をクリックすると、ターゲットリソースが追加され、「アイデンティティー属性の追加」または「アイデンティティー属性の編集」ページに戻ります。

ターゲットリソースの削除

1 つ以上のターゲットリソースを削除するには、ターゲットリソースを選択して、「選択したターゲットを削除」をクリックします。

アイデンティティー属性のインポート

アイデンティティー属性のインポート機能を使用して、1 つ以上のフォームを選択し、アイデンティティー属性値をインポートして設定することができます。Identity Manager はインポートされたフォームの値を分析し、アイデンティティー属性に「最適な推定値」を見積もります。とはいえ、アイデンティティー属性値はインポート後に編集が必要になる場合があります。

次のインポート項目について選択を行います。

- **「既存のアイデンティティー属性とマージ」**－ このオプションを選択した場合、Identity Manager はインポートされた値を既存のアイデンティティー属性とマージします。このオプションを選択しない場合は、インポートを実行する前に既存のアイデンティティー属性がクリアされます。
- **「インポートするフォーム」**－ 「利用可能なフォーム」エリアから 1 つ以上のフォームを選択して、アイデンティティー属性を設定します。

  「インポート」をクリックして、フォームをインポートします。アイデンティティー属性ページには、新規またはマージされたアイデンティティー属性が一覧表示されます。

  「保存」をクリックして、アイデンティティー属性の変更を保存します。

注 アイデンティティー属性の条件に訂正の必要な箇所がある場合は、「警告」ページが表示されて、そこに 1 つ以上の警告が一覧表示されます。「OK」をクリックすると、「設定」エリアに戻ります。

アイデンティティーイベントの設定

Identity Manager が管理するリソースのアイデンティティーイベントを設定して、これらのリソース上で起きるイベントの動作を定義することもできます。アイデンティティーイベントで定義される動作は、Active Sync 中に、イベントが起きるタイミングを決定し、イベントに応答する適切なアクションを行うために使用されます。

たとえば、アイデンティティーユーザーとほかのすべてのリソースアカウントの削除をトリガーする、権威のある人事システム上での削除イベントを検出し応答するように、アイデンティティーイベントを設定できます。

アイデンティティーイベントを設定するには、「メタビュー」を選択し、「アイデンティティーイベント」タブを選択します。「アイデンティティーイベント」ページで、「イベントの追加」をクリックしてイベントタイプを指定します。「アイデンティティーイベント」ページでイベントを選択し、以下のオプションを指定することにより、アイデンティティーイベントを編集することもできます。

- **「イベントタイプ」** – 削除、有効化、または無効化を選択して、設定しているアイデンティティーイベントタイプを指定します。
- **「ソース」** – アイデンティティーイベントが適用されるリソースを選択します (Active Directory の AD など)。(ネイティブサポートがないため) イベントを検出し応答するためにリソースがイベント検出規則を必要とする場合は、「検出に使用する規則」フィールドで規則を選択します。リソースを追加または削除できます。
- **「応答」** – 応答リストから応答を選択するか、何も定義されていない場合は、「応答の追加」をクリックして応答を追加します。選択リストから応答を削除するには、その応答を選択して、「選択された応答の削除」をクリックします。

選択が終了したら、「OK」をクリックします。

Identity Manager ポリシーの設定

この節では、ユーザーポリシーの設定の説明および手順を示します。

ポリシーとは

Identity Manager ポリシーには、Identity Manager アカウント ID、ログイン、およびパスワードの特性に制約を設定することによって、Identity Manager ユーザーの制限を設定します。

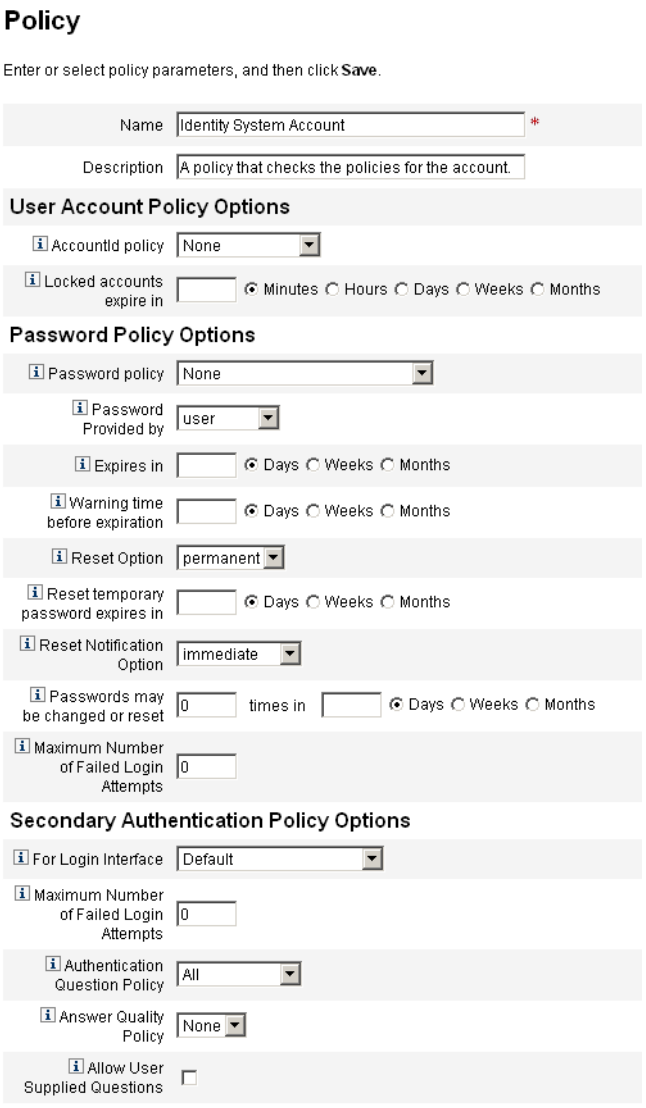
注	Identity Manager には、特にユーザーのコンプライアンスを監査するように設計された監査ポリシーも用意されています。監査ポリシーについては、第 11 章「アイデンティティー監査」を参照してください。

Identity Manager ユーザーポリシーの作成と編集は、「ポリシー」ページで行います。メニューバーの「セキュリティー」を選択してから、「ポリシー」を選択します。表示されたリストページで、既存のポリシーを編集したり、新規ポリシーを作成したりできます。

ポリシーは、以下のタイプに分類されています。

- **アイデンティティーシステムアカウントポリシー** – ユーザー、パスワード、および認証ポリシーのオプションと制約を設定します。アイデンティティーシステムアカウントポリシー (図 4-9 参照) は、「組織の作成」と「組織の編集」および「ユーザーの作成」と「ユーザーの編集」ページを使用して組織またはユーザーに割り当てます。

図 4-9　　Identity Manager ポリシー



設定または選択できるオプションは、次のとおりです。

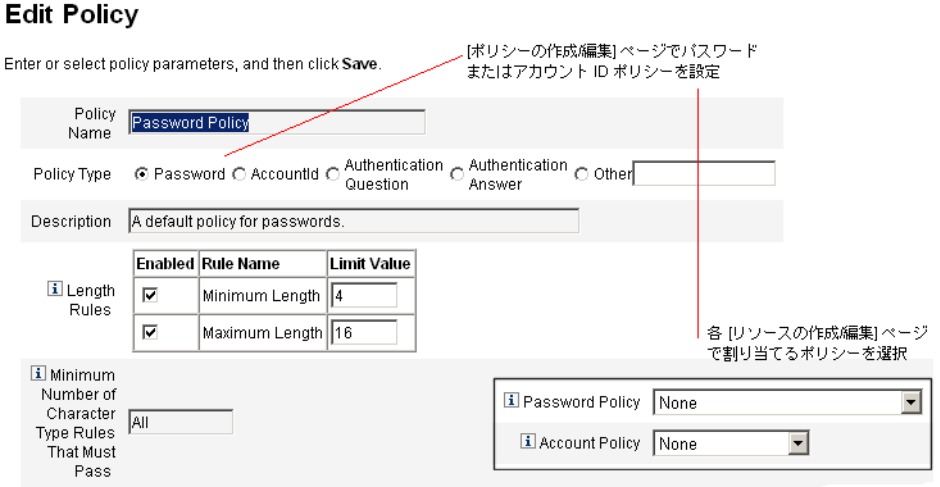
- **ユーザーポリシーオプション** – ユーザーが秘密の質問に正しく回答できない場合に、Identity Manager がユーザーアカウントをどのように処理するかを指定します。
- **パスワードポリシーオプション** – パスワードの有効期限、期限切れ前の警告時間、およびリセットオプションを設定します。

- **認証ポリシーオプション** – 秘密の質問をユーザーにどのように表示するか、およびユーザーが独自の秘密の質問を設定できるようにするかを決定し、ログイン時に認証を施行して、ユーザーに表示できる一まとまりの質問を設定します。

- **SPE システムアカウントポリシー** – このポリシータイプは、サービスプロバイダ用に実装されたもので、サービスプロバイダユーザーのユーザー、パスワード、認証ポリシーのオプションと制約を設定するために使用されます。このポリシーは、「組織の作成」と「組織の編集」および「ユーザーの作成」と「ユーザーの編集」ページを使用して組織またはユーザーに割り当てます。

- **文字列の品質ポリシー** – 文字列品質ポリシーにはパスワード、AccountID、認証などのポリシータイプが含まれており、長さ規則、文字タイプ規則、許容される単語や属性値を設定します。このタイプのポリシーは、各 Identity Manager リソースに関連付けられ、各リソースページに設定されます。図 4-10 に例を示します。

図 4-10　　パスワードポリシーの作成 / 編集



パスワードおよびアカウント ID に設定できるオプションと規則は、次のとおりです。

- **長さ規則** – 最大長および最小長を決定します。
- **文字タイプ規則** – 英字、数字、大文字、小文字、繰り返し、および連続文字に使用可能な最小値と最大値を設定します。

- **パスワードの再利用の制限** – 現在のパスワードより前に使用されていたパスワードのうち、再利用できないようにするパスワードの数を指定します。ユーザーがパスワードを変更しようとすると、新規パスワードがパスワードの履歴と比較され、一意のパスワードであることが確認されます。セキュリティーを確保する目的で以前のパスワードのデジタル署名が保存され、新規パスワードと比較されます。
- **禁止される単語および属性値** – ID またはパスワードとして使用できない単語および属性を指定します。

ポリシーでの使用禁止属性

`UserUIConfig` 設定オブジェクトでは「使用禁止」属性のセットを変更できます。`UserUIConfig` には次のような属性があります。

- `<PolicyPasswordAttributeNames>` – ポリシータイプ「Password」
- `<PolicyAccountAttributeNames>` – ポリシータイプ「AccountId」
- `<PolicyOtherAttributeNames>` – ポリシータイプ「Other」

辞書ポリシー

辞書ポリシーを使用すると、Identity Manager は単語データベースと照合してパスワードをチェックすることができ、単純な辞書攻撃から保護されることが保証されます。このポリシーをほかのポリシー設定と組み合わせて使用し、パスワードの長さと構成を強制することにより、Identity Manager がシステム内で生成または変更されたパスワードを、辞書を使用して推測することが困難になります。

辞書ポリシーは、ポリシーを使用して設定できるパスワード除外リストを拡張します。このリストは、管理者インタフェースに含まれるパスワードの「ポリシーの編集」ページの「使用禁止単語」オプションにより実装されます。

辞書ポリシーの設定

辞書ポリシーを設定するには、次を実行する必要があります。

- 辞書サーバーサポートの設定
- 辞書の読み込み

次の手順を実行します。

1. メニューバーの「設定」を選択してから、「ポリシー」を選択します。
2. 「辞書の設定」をクリックすると、「辞書の設定」ページが表示されます。
3. データベース情報を選択および入力します。

- **「データベースタイプ」** – 辞書の保存に使用するデータベースタイプ (Oracle、DB2、SQLServer、または MySQL) を選択します。
- **「ホスト」** – データベースが実行されているホストの名前を入力します。
- **「ユーザー」** – データベースに接続するときに使用するユーザー名を入力します。
- **「パスワード」** – データベースに接続するときに使用するパスワードを入力します。
- **「ポート」** – データベースがリスニング中のポートを入力します。
- **「接続 URL」** – 接続のときに使用する URL を入力します。次のテンプレート変数を使用することができます。
- `%h` - ホスト
- `%p` - ポート
- `%d` - データベース名

- **「ドライバクラス」** – データベースを操作する際に使用する JDBC ドライバクラスを入力します。
- **「データベース名」** – 辞書の読み込み先のデータベースの名前を入力します。
- **「辞書ファイル名」** – 辞書を読み込むときに使用するファイルの名前を入力します。

4. データベース接続をテストするには、「テスト」をクリックします。
5. 接続テストが成功したら、「単語の読み込み」をクリックして、辞書を読み込みます。読み込み作業が完了するまでに、数分かかる場合があります。
6. その辞書が正しく読み込まれたかどうかを確認するには、「テスト」をクリックします。

辞書ポリシーの実装

辞書ポリシーは、Identity Manager ポリシーエリアから実装します。「ポリシー」ページで、編集するパスワードポリシーをクリックします。「ポリシーの編集」ページで、「辞書の単語でパスワードをチェックする」オプションを選択します。実装すると、変更および生成されたパスワードはすべて、辞書と照合してチェックされます。

電子メールテンプレートのカスタマイズ

Identity Manager では、電子メールテンプレートを使用して、情報および操作のリクエストをユーザーと承認者に配信します。システムには次のためのテンプレートが用意されています。

- **アクセスレビュー通知** − ユーザーのアクセス権をレビューする必要があるという通知を送信します。アクセスポリシーの違反を是正するか受け入れる必要があるときに、システムはこの通知を送信します。
- **アカウントの作成の承認** − 新しいアカウントが承認待ちであるという通知を承認者に送信します。関連付けられているロールの「プロビジョン通知」オプションが「承認」に設定されている場合に、この通知が送信されます。
- **アカウントの作成の通知** − アカウントが作成され、特定のロールが割り当てられたという通知を送信します。「ロールの作成」または「ロールの編集」ページの「通知受信者」フィールドで、1 人以上の管理者が選択されている場合に、この通知が送信されます。
- **アカウントの削除の承認** − ユーザーアカウントの削除アクションが承認待ちであるという通知を承認者に送信します。「ロールの作成」または「ロールの編集」ページの「通知受信者」フィールドで、1 人以上の管理者が選択されている場合に、この通知が送信されます。
- **アカウントの削除の通知** − アカウントが削除されたという通知を送信します。
- **アカウントの更新の通知** − 指定の電子メールアドレスまたはユーザーアカウントへ、アカウントを更新したという通知を送信します。
- **パスワードリセット** − Identity Manager パスワードリセットの通知を送信します。関連付けられた Identity Manager ポリシーに対して選択されたリセット通知オプションの値に応じて、パスワードをリセットした管理者の Web ブラウザにただちに通知が表示されるか、パスワードがリセットされたユーザーに電子メールが送信されます。
- **パスワード同期通知** − パスワードの変更がすべてのリソースで正常に完了したことをユーザーに通知します。通知には、正常に更新されたリソースが一覧表示され、パスワード変更のリクエスト元が示されます。
- **パスワード同期エラー通知** − パスワードの変更がすべてのリソースでは成功しなかったことをユーザーに通知します。通知には、エラーが一覧表示され、パスワード変更のリクエスト元が示されます。
- **ポリシー違反通知** − アカウントポリシー違反が発生したという通知を送信します。
- **アカウントイベントの調整、リソースイベントの調整、調整の概要** − Notify Reconcile Response、Notify Reconcile Start、および Notify Reconcile Finish デフォルトワークフローからそれぞれ呼び出されます。通知は、各ワークフローの設定に基づいて送信されます。

- **レポート** − 生成されたレポートを指定されたリストの受信者に送信します。
- **リソースのリクエスト** − リソースがリクエストされたという通知をリソース管理者に送信します。管理者が「リソース」エリアからリソースをリクエストしたときに、この通知が送信されます。
- **再試行通知** − あるリソースに関する特定の操作の試行が指定回数失敗したという通知を管理者に送信します。
- **リスク分析** − リスク分析レポートを送信します。リソーススキャンの一部として、1 人以上の電子メール受信者が指定されている場合に、このレポートが送信されます。
- **一時パスワードリセット** − アカウントに暫定パスワードが提供されたという通知をユーザーまたはロール承認者に送信します。関連付けられた Identity Manager ポリシーに対して選択したパスワードリセット通知オプションの値に応じて、ユーザーの Web ブラウザにただちに通知が表示されるか、ユーザーまたはロール承認者に電子メールが送信されます。
- **ユーザー ID の復元** − 指定した電子メールアドレスに復元されたユーザー ID を送信します。

電子メールテンプレートの編集

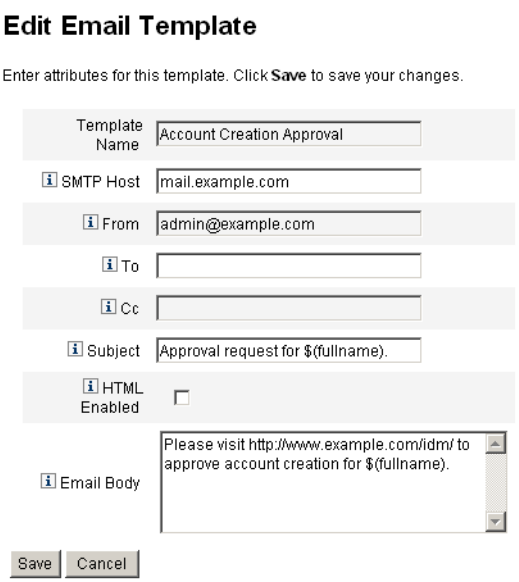
電子メールテンプレートをカスタマイズして、受信者に、タスクの実行方法や結果の表示方法などの特定の指示を通知することができます。たとえば、「アカウントの作成の承認」テンプレートをカスタマイズして、次のメッセージを追加することにより、承認者にアカウント承認ページを表示するとします。

`$(fullname)` 用アカウント作成を承認するには、`http://host.example.com:8080/idm/approval/approval.jsp` にアクセスしてください。

電子メールテンプレートをカスタマイズするには、例として「アカウントの作成の承認」テンプレートを使用した次の手順を実行します。

1. メニューバーで、「設定」を選択します。
2. 「設定」ページで「電子メールテンプレート」を選択します。
3. アカウント作成承認テンプレートをクリックして選択します。

図 4-11　　電子メールテンプレートの編集



4. テンプレートの詳細を入力します。
   - 「SMTP ホスト」フィールドに SMTP サーバー名を入力して、電子メール通知を送信できるようにします。
   - 「送信者」フィールドで、送信元の電子メールアドレスをカスタマイズします。
   - 「宛先」フィールドと「CC」フィールドに、電子メール通知の受信者になる 1 つ以上の電子メールアドレスまたは Identity Manager アカウントを入力します。
   - 「電子メール本文」フィールドで、Identity Manager の場所を指すように内容をカスタマイズします。
5. **「保存」**をクリックします。

Identity Manager IDE を使用して電子メールテンプレートを修正することもできます。IDE の詳細については、『Identity Manager 配備ツール』を参照してください。

電子メールテンプレートでの HTML 形式とリンクの使用

HTML 形式のコンテンツを電子メールテンプレートに挿入して、電子メールメッセージの本文に表示することができます。コンテンツには、テキスト、グラフィック、および情報への Web リンクを使用できます。HTML 形式のコンテンツを有効化するには、「HTML 有効」オプションを選択します。

電子メール本文で使用できる変数

電子メールテンプレートの本文には、変数の参照を $(*Name*) の形式で含めることもできます。例 : パスワード `$(password)` が復旧しました。

各テンプレートで使用できる変数を、次の表に定義します。

表 4-3 電子メールテンプレート変数

テンプレート	許容変数
パスワードリセット	$(password) − 新規に生成されたパスワード
承認の更新	$(fullname) − ユーザーのフルネーム
	$(role) − ユーザーのロール
通知の更新	$(fullname) − ユーザーのフルネーム
	$(role) − ユーザーのロール
レポート	$(report) − 生成されたレポート
	$(id) − タスクインスタンスのエンコード ID
	$(timestamp) − 電子メールの送信時刻
リソースのリクエスト	$(fullname) − ユーザーのフルネーム
	$(resource) − リソースタイプ
リスク分析	$(report) − リスク分析レポート
一時パスワードリセット	$(password) − 新規に生成されたパスワード
	$(expiry) − パスワードの有効期限

監査グループおよび監査イベントの設定

監査設定グループを設定すると、選択したシステムイベントを記録およびレポートすることができます。監査グループおよびイベントの設定には、Configure Audit 管理機能が必要になります。

監査設定グループを設定するには、メニューバーの「設定」を選択し、「監査」を選択します。

「監査設定」ページに監査グループのリストが表示されます。各グループに 1 つ以上のイベントが含まれています。各グループについて、成功したイベント、失敗したイベント、またはその両方を記録することができます。

リスト内の監査グループをクリックすると、「監査設定グループの編集」ページが表示されます。このページで、監査設定グループの一部としてシステム監査ログに記録する監査イベントのタイプを選択することができます。

「監査の有効化」チェックボックスが選択されていることを確認します。監査システムを無効にするには、チェックボックスを選択解除します。

監査設定グループ内のイベントの編集

グループ内のイベントを編集するために、特定のオブジェクトタイプの操作を追加または削除することができます。このためには、そのオブジェクトタイプの「アクション」列の項目を「利用可能」エリアから「選択」エリアに移動し、「OK」をクリックします。

監査設定グループへのイベントの追加

グループにイベントを追加するには、「新規」をクリックします。イベントはページの一番下に追加されます。「オブジェクトタイプ」列でリストからオブジェクトタイプを選択し、新しいオブジェクトタイプの「アクション」列で、1 つ以上の項目を「利用可能」エリアから「選択」エリアに移動します。「OK」をクリックしてイベントをグループに追加します。

Remedy との統合

Identity Manager を Remedy サーバーと統合すると、指定されたテンプレートに従って Remedy チケットを送信することができます。

Remedy との統合は、管理者インタフェースの次の 2 つのエリアでセットアップします。

- **「Remedy サーバーの設定」**－「リソース」エリアから Remedy リソースを作成することにより、Remedy を設定します。リソースのセットアップ後、接続をテストして統合が有効であることを確認します。
- **「Remedy テンプレート」**－ Remedy リソースのセットアップ後、Remedy テンプレートを定義します。そのためには、「設定」を選択して、「Remedy との統合」を選択します。次に、Remedy スキーマとリソースを選択します。

Remedy チケットの作成は、Identity Manager ワークフローを通じて設定されます。設定によっては、定義済みのテンプレートを使用して Remedy チケットを開く呼び出しを適切な時刻に行うこともできます。ワークフローの設定の詳細については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

Identity Manager サーバーの設定

Identity Manager サーバーが特定のタスクのみを実行するようにサーバー固有の設定を編集することができます。そのためには、「設定」を選択して、「サーバー」を選択します。

個別のサーバーの設定を編集するには、「サーバーの設定」ページでリスト内のサーバーを選択します。「サーバー設定の編集」ページが表示され、調整サーバー、スケジューラ、JMX などの設定を編集することができます。

調整サーバーの設定

デフォルトでは、調整サーバーの設定は、「サーバー設定の編集」ページに表示されます。デフォルト値を使用することも、「デフォルト値を使用する」オプションを選択解除して値を指定することもできます。

- **「並列リソースの制限」**－ 調整サーバーが同時に処理できるリソースの最大数を指定します。
- **「最小ワークスレッド」**－ 調整サーバーが常にライブ状態で維持する処理スレッドの最小数を指定します。

- **「最大ワークスレッド」** – 調整サーバーが使用できる処理スレッドの最大数を指定します。調整サーバーは、作業の負荷に応じて、スレッドを必要な数だけ開始します。ここで指定する最大数でその数が制限されます。

スケジューラの設定

「サーバー設定の編集」ページで「スケジューラ」をクリックすると、スケジューラオプションが表示されます。デフォルト値を使用することも、「デフォルト値を使用する」オプションを選択解除して値を指定することもできます。

- **「スケジューラの起動」** – スケジューラの起動モードを選択します。
  - **「自動」** – サーバーの起動時に起動します。これがデフォルトの起動モードです。
  - **「手動」** – サーバーの起動時に起動しますが、手動で起動するまで保留状態で維持されます。
  - **「無効」** – サーバーの起動時に起動しません。
- **「トレースの有効化」** – このオプションを選択すると、スケジューラのデバッグトレース結果が標準出力に表示されます。
- **「最大同時タスク数」** – スケジューラが一度に実行するデフォルト以外のタスクの最大数を指定するには、このオプションを選択します。この制限を超える追加タスクのリクエストは、延期されるか、別のサーバーで実行します。
- **「タスク指定」** – サーバーで実行できるタスクのセットを指定します。このためには、利用可能なタスクのリストから 1 つ以上のタスクを選択します。選択したタスクのリストは、選択したオプションに応じて、追加リストまたは除外リストになります。リストで選択したタスクを除くすべてのタスクを許可することも (デフォルトの動作)、選択したタスクのみを許可することもできます。

「保存」をクリックして、サーバー設定の変更を保存します。

電子メールテンプレートサーバーの設定

「サーバー」メニューの「電子メールテンプレート」をクリックして、デフォルトの SMTP サーバー設定を指定します。

デフォルト以外のメールサーバーを使用する場合は、このオプションを使用して、「デフォルト値を使用する」の選択を解除し、使用するメールサーバーを入力することにより、デフォルトの電子メールサーバーを指定します。入力するテキストは、電子メールテンプレートの *smtpHost* 変数の置換に使用されます。

JMX

この設定を使用して JMX クラスタポーリングを有効にし、ポーリングスレッドの間隔を設定します。収集された JMX データは、Identity Manager デバッグページにアクセスし、「Show MBean Info」ボタンをクリックすると表示できます。

JMX ポーリングを有効するには、「サーバー」タブの「JMX」をクリックして、次のオプションを選択します。

- **「JMX の有効化」** − このオプションを使用して、JMX クラスタ MBean のポーリングスレッドを有効または無効にします。JMX を有効にするにはデフォルト設定を選択解除します (デフォルト値 (false) を使用する)。

注	ポーリングサイクルにシステムリソースを使用するため、JMX の使用を計画している場合にのみこのオプションを有効にしてください。

- **「ポーリング間隔 (ms)」** − JMX を有効にしているときに、サーバーがレジストリをポーリングするデフォルトの間隔を変更するには、このオプションを使用します。間隔はミリ秒単位で指定します。

  デフォルトポーリング間隔は 60000 ミリ秒に設定されます。これを変更するには、このオプションのチェックボックスを選択解除し、表示される入力フィールドに新しい値を入力します。

「保存」をクリックして、サーバー設定の変更を保存します。

サーバーのデフォルト設定の編集

サーバーのデフォルト設定機能を使用して、すべての Identity Manager サーバーのデフォルト設定を設定することができます。個別のサーバー設定ページで異なる項目を選択しないかぎり、サーバーはこれらの設定を継承します。デフォルト設定を編集するには、「サーバーのデフォルト設定の編集」をクリックします。「サーバーのデフォルト設定の編集」ページには、個別のサーバー設定ページと同じオプションが表示されます。

各サーバーのデフォルト設定の変更は、その設定の「デフォルト値を使用する」オプションを選択解除しないかぎり、対応する個別のサーバー設定に伝播されます。

「保存」をクリックして、サーバー設定の変更を保存します。

第 5 章

管理

この章では、Identity Manager 管理者と組織の作成と管理など、Identity Manager システムで一連の管理レベルタスクを実行するための説明および手順を示します。また、Identity Manager でのロール、機能、管理者ロールの使用方法についても説明します。

この章は、次のトピックで構成されています。

- Identity Manager の管理について
- 管理者の作成
- Identity Manager 組織について
- 組織の作成
- ディレクトリジャンクションおよび仮想組織について
- 機能とその管理について
- 管理者ロールとその管理について
- 作業項目の管理
- アカウントの承認

Identity Manager の管理について

Identity Manager 管理者は、Identity Manager の拡張特権を持ったユーザーです。管理者を設定すると、次のものを管理できます。

- ユーザーアカウント
- ロールやリソースなどのシステムオブジェクト
- 組織

Identity Manager 管理者は、次のものが直接または間接的に割り当てられる点で、ユーザーと区別されます。

- **機能**。ユーザー、組織、ロール、およびリソースへのアクセス権を与えられる一連の権限。
- **管理する組織**。組織の管理を割り当てられると、管理者は、その組織内と、階層内でその組織の下にあるすべての組織のオブジェクトを管理できます。

委任された管理

ほとんどの企業では、実行すべき管理タスクを持つ従業員は、固有のさまざまな役割を持っています。多くの場合、管理者は、ほかのユーザーまたは管理者から「透過的な」アカウント管理タスクや、範囲の制限されたアカウント管理タスクを実行する必要があります。

たとえば、管理者が Identity Manager ユーザーアカウントの作成の役割しか持たない場合があります。このように役割の範囲が制限されている場合、管理者には、ユーザーアカウントを作成するリソースについての特定の情報や、システム内に存在するロールまたは組織についての情報は必要ないと思われます。

Identity Manager では、管理者が固有で定義済みの範囲内のオブジェクトのみを表示して管理できるようにすることで、役割を分離し、この委任された管理モデルをサポートしています。

Identity Manager では、次の手段によって、個別のシステムアクティビティーを管理者に委任する機能を実装しています。

- 固有の組織およびその組織内のオブジェクトに対する管理を制限する
- Identity Manager ユーザーの作成および編集ページの管理者ビューをフィルタする
- 管理者に固有のジョブの任務を機能の形式で与える

新しいユーザーアカウントを設定したり、ユーザーアカウントを編集したりする場合に、「ユーザーの作成」ページからユーザーの委任を指定できます。

また、「作業項目」タブから承認リクエストなどの作業項目を委任することもできます。詳細は、198 ページの「作業項目の委任」を参照してください。

管理者の作成

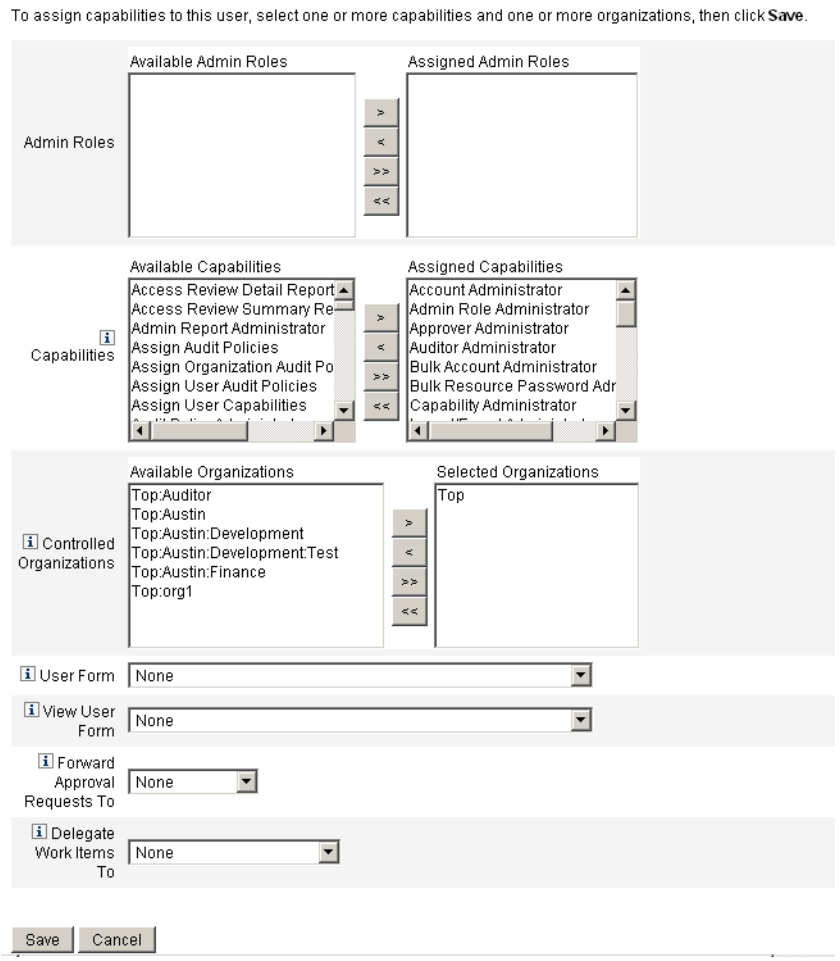
Identity Manager 管理者を作成するには、管理者にする Identity Manager ユーザーの機能を拡張します。ユーザーを作成または編集するときには、次を実行して管理コントロールを与えます。

- 管理できる組織を指定する
- 管理する組織内の機能を割り当てる
- Identity Manager ユーザーの作成および編集に使用するフォームを選択する (これらの操作の実行を許可する機能がユーザーに割り当てられている場合)
- 保留中承認リクエストを受け取る承認者を選択する (リクエストの承認を許可する機能がユーザーに割り当てられている場合)

ユーザーに管理特権を与えるには、メニューバーで「アカウント」を選択して「Identity Manager アカウント」エリアに移動します。新しいユーザーに対しては、「ユーザーの作成」ページで「セキュリティー」タブを選択し、管理者属性を割り当てます。

既存のユーザーに管理者属性を割り当てるには、「アカウント」リストでユーザーを選択して、「ユーザーアクション」リストで「ユーザー機能の編集」を選択して、ユーザーの機能を編集します。次の図のような「セキュリティー」フォームが表示されます。

図 5-1 ユーザーアカウントの「セキュリティー」ページ : 管理者特権の指定



1 つ以上の項目を選択して、管理コントロールを設定します。

- **「管理する組織」** – 組織を 1 つ以上選択します。管理者は、選択した組織内と、階層内でその組織の下にある任意の組織内のオブジェクトを管理できます。管理の範囲は、割り当てられた機能によってさらに定義されます。このエリアで項目を 1 つ選択する必要があります。
- **「機能」** – この管理者が管理する組織内でこの管理者が持つ機能を 1 つ以上選択します。Identity Manager 機能の詳細については、第 4 章「設定」を参照してください。

- **「ユーザーフォーム」** – Identity Manager ユーザーの作成および編集時にこの管理者が使用するユーザーフォームを選択します (その機能が割り当てられている場合)。ユーザーフォームを直接割り当てない場合、管理者は自分の所属する組織に割り当てられたユーザーフォームを継承します。ここで選択されたフォームは、この管理者の組織で選択されたどのフォームよりも優先されます。
- **「承認リクエスト転送先」** – 現在の保留中承認リクエストをすべて転送するユーザーを選択します。この管理者設定は、「承認」ページからも設定できます。
- **「作業項目の委任先」** – 使用できる場合は、このオプションを使用してユーザーアカウントへの委任を指定します。1 人または複数の選択したユーザーを IDM マネージャーに指定するか、承認委任先規則を使用します。

管理者ビューのフィルタ

組織と管理者にユーザーフォームを割り当てることにより、ユーザー情報についての特定の管理者ビューを設定できます。ユーザー情報へのアクセスは、次の 2 つのレベルで設定されます。

- **組織** – 組織を作成するときには、その組織内のすべての管理者が Identity Manager ユーザーの作成および編集時に使用するユーザーフォームを割り当てます。管理者レベルで設定されたフォームはすべて、ここで設定したフォームよりも優先されます。管理者または組織に対してフォームが選択されていない場合は、Identity Manager が親組織に対して選択されたフォームを継承します。親組織に対してフォームが設定されていない場合は、Identity Manager がシステム設定のデフォルトのフォームを使用します。
- **管理者** – ユーザー管理機能を割り当てるときには、管理者にユーザーフォームを直接割り当てることができます。フォームを割り当てない場合、管理者は自分の組織に割り当てられたフォームを継承します。組織にフォームが設定されていない場合は、システム設定のデフォルトのフォームになります。

第 4 章「設定」で、割り当て可能な Identity Manager 組み込み機能について説明します。

管理者パスワードの変更

管理者パスワードは、管理パスワード変更機能を割り当てられた管理者か、管理者所有者が変更できます。

管理者は、次の場所から別の管理者のパスワードを変更できます。

- **「アカウント」エリア** ー リストで管理者を選択し、「ユーザーアクション」リストから「パスワードの変更」を選択します。
- **「ユーザーの編集」ページ** ー 「ID」フォームタブを選択し、新しいパスワードを入力および確認します。
- **「パスワード」エリア** ー 管理者名を入力し、「パスワードの変更」をクリックします。

ヒント 1 文字以上入力して「検索」をクリックすると、一致するものがすべてリストされます。

管理者は、「パスワード」エリアから自分自身のパスワードを変更できます。「パスワード」を選択し、「自分のパスワードの変更」を選択すると、パスワードの自己管理フィールドにアクセスできます。

注 アカウントに適用された Identity Manager アカウントポリシーは、パスワードの有効期限、リセットオプション、および通知選択など、パスワードの制限を決定します。管理者のリソースにパスワードポリシーを設定することにより、パスワード制限を追加設定することができます。

管理者のアクションの認証

特定のアカウント変更を処理する前に Identity Manager ログインパスワードをアテストするように管理者にリクエストするオプションを設定することができます。パスワードの認証が失敗した場合、アカウントアクションは成功しません。

このオプションは、次の Identity Manager ページでサポートされます。

- 「ユーザーの編集」(`account/modify.jsp`)
- 「ユーザーパスワードの変更」(`admin/changeUserPassword.jsp`)
- 「ユーザーパスワードのリセット」(`admin/resetUserPassword.jsp`)

以降の節で説明するように、これらのオプションを設定します。

ユーザーリクエストの編集オプション

このオプションは、`account/modify.jsp` ページで次のように設定します。

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE,
"email, fullname, password");
```

ここでのオプションの値は、1 つ以上の次のユーザー表示属性名のカンマ区切りリストです。

- applications
- adminRoles
- assignedLhPolicy
- capabilities
- controlledOrganizations
- email
- firstname
- fullname
- lastname
- organization
- password
- resources
- roles

ユーザーパスワードの変更とユーザーパスワードリクエストのリセットオプション

このオプションは、admin/changeUserPassword.jsp ページおよび admin/resetUserPassword ページで次のように設定します。

```
requestState.setOption(UserViewConstants.OP_REQUIRES_CHALLENGE,
"true");
```

オプションの値として true または false を指定できます。

秘密の質問の回答の変更

「パスワード」エリアを使用して、アカウントの秘密の質問に設定した回答を変更することができます。メニューバーの「パスワード」を選択し、「自分の秘密の質問の回答の変更」を選択します。

認証の詳細については、94 ページの「ユーザー認証」を参照してください。

管理者インタフェースでの管理者名の表示のカスタマイズ

次のエリアのような、Identity Manager 管理者インタフェースのいくつかのページおよびエリアでは、accountId ではなく属性 (email や fullname など) に基づいて Identity Manager 管理者を表示することができます。

- 「ユーザーの編集」(承認選択リストを転送する)
- ロールテーブル
- 「ロールの作成」/「ロールの編集」
- 「リソースの作成」/「リソースの編集」
- 「組織の作成」/「組織の編集」/「ディレクトリジャンクション」
- 承認

表示名を使用するように Identity Manager を設定するには、次のように `UserUIConfig` オブジェクトに追加します。

```
<AdminDisplayAttribute>
  <String>attribute_name</String>
</AdminDisplayAttribute>
```

たとえば、email 属性を表示名として使用するには、次の属性名を `UserUIconfig` に追加します。

```
<AdminDisplayAttribute>
  <String>email</String>
</AdminDisplayAttribute>
```

Identity Manager 組織について

組織を使用して、次のことができます。

- ユーザーアカウントと管理者を論理的かつセキュアに管理する
- リソース、アプリケーション、ロール、およびその他の Identity Manager オブジェクトへのアクセスを制限する

組織を作成してユーザーを組織階層内のさまざまな場所に割り当てることで、委任された管理のステージが設定されます。1 つ以上の組織を含む組織は、親組織と呼ばれます。

すべての Identity Manager ユーザー (管理者を含む) は、1 つの組織に静的に割り当てられます。また、別の組織に動的に割り当てることもできます。

Identity Manager 管理者には、さらに組織の管理が割り当てられます。

組織の作成

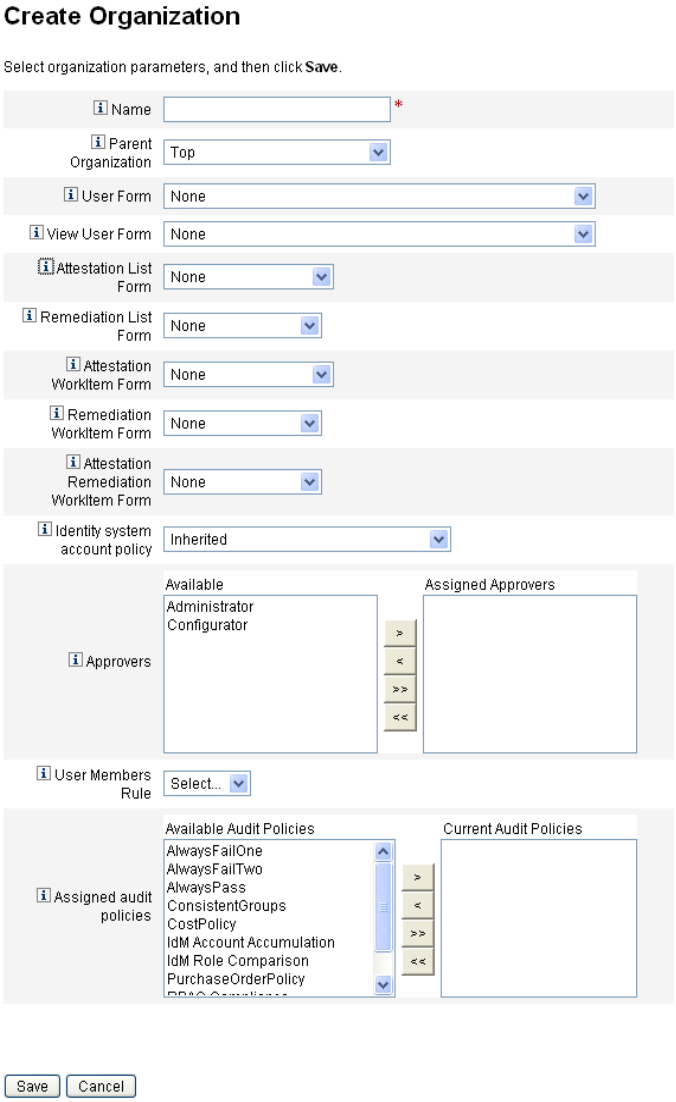
組織は、「Identity Manager アカウント」エリアで作成します。組織を作成するには、次の手順に従います。

1. メニューバーで、「アカウント」を選択します。
2. 「アカウント」ページの「新規作成アクション」リストから「新規組織」を選択します。

ヒント	組織階層内の特定の場所に組織を作成するには、リストで組織を選択してから、「新規作成アクション」リストで「新規組織」を選択します。

図 5-2 は、「組織の作成」ページを示しています。

図 5-2 「組織の作成」ページ



組織へのユーザーの割り当て

各ユーザーは 1 つの組織の静的なメンバーですが、複数の組織の動的なメンバーになることもできます。組織のメンバーシップは、次の方法で決定されます。

- **直接 (静的) 割り当て** – 「ユーザーの作成」または「ユーザーの編集」ページから、ユーザーを組織に直接割り当てます。「ID」フォームタブを選択して、「組織」フィールドを表示します。ユーザーは、1 つの組織に直接割り当てる必要があります。
- **規則に基づく (動的) 割り当て** – 組織に規則を割り当てることによって、ユーザーを動的に組織に割り当てます。割り当てた規則が評価されると、定義されているメンバーユーザーの一覧が返されます。Identity Manager は、次の場合にユーザーメンバー規則を評価します。
  - 組織内のユーザーの一覧を出力する
  - 「ユーザーの検索」ページでユーザーを検索するときに、ユーザーメンバー規則による組織内のユーザーの検索を含める
  - ユーザーへのアクセスをリクエストする (現在の管理者がユーザーメンバー規則を持つ組織を管理している場合)

ユーザーメンバー規則は、「組織の作成」ページの「ユーザーメンバー規則」フィールドで選択します。図 5-3 はユーザーメンバー規則の例を示しています。

図 5-3 組織の作成 : ユーザーメンバー規則の選択

次の例は、組織のユーザーメンバーシップを動的に管理できるユーザーメンバー規則をセットアップする方法を示しています。

注 Identity Manager の規則を作成および操作する方法については、『Identity Manager 配備ツール』を参照してください。

キーの定義と取り込み

- 「ユーザーメンバー規則」オプションボックスに規則を表示するには、authType を authType='UserMembersRule' と設定する必要があります。
- コンテキストは、現在認証されている Identity Manager ユーザーのセッションです。
- 定義された変数 (defvar) の「Team players」は、Windows Active Directory の「Pro Ball Team」組織単位 (OU) から、そのすべてのメンバーユーザーの識別名 (DN) を取得します。
- メンバーユーザーが検出されると、append ロジックは、「Pro Ball Team」OU のメンバーユーザーの DN に Identity Manager リソースの名前を連結し、先頭にコロンを付加します (「:smith-AD」など)。
- 結果は、Identity Manager リソース名が連結された DN (「*dn*:smith-AD」など) のリストとして返されます。

次は、サンプルのユーザーメンバー規則の構文例です。

コード例 5-1 ユーザーメンバー規則の例

```
<Rule name='Get Team Players'
     authType='UserMembersRule'>
    <defvar name='Team players'>
       <block>
          <defvar name='player names'>
             <list/>
          </defvar>
    <dolist name='users'>
       <invoke class='com.waveset.ui.FormUtil'
           name='getResourceObjects'>
          <ref>context</ref>
          <s>User</s>
          <s>singleton-AD</s>
          <map>
             <s>searchContext</s>
             <s>OU=Pro Ball Team,DC=dev-ad,DC=waveset,DC=com</s>
             <s>searchScope</s>
             <s>subtree</s>
             <s>searchAttrsToGet</s>
             <list>
                <s>distinguishedName</s>
             </list>
          </map>
       </invoke>
       <append name='player names'>
       <concat>
          <get>
             <ref>users</ref>
             <s>distinguishedName</s>
          </get>
             <s>:sampson-AD</s>
       </concat>
       </append>
    </dolist>
       <ref>player names</ref>
    </block>
    </defvar>
       <ref>Team players</ref>
</Rule>
```

管理する組織の割り当て

「ユーザーの作成」または「ユーザーの編集」ページから、1 つ以上の組織の管理を割り当てます。「セキュリティー」フォームタブを選択すると、「管理する組織」フィールドが表示されます。

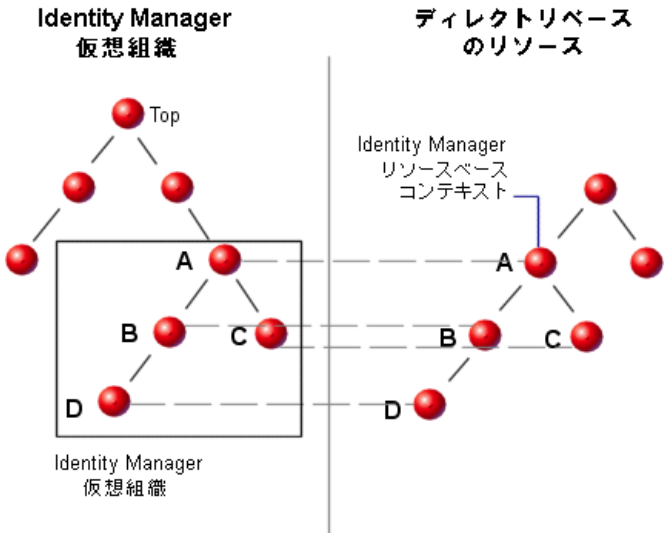
また、「管理者ロール」フィールドから 1 つ以上の管理者ロールを割り当てる方法で、管理する組織を割り当てることもできます。

ディレクトリジャンクションおよび仮想組織について

ディレクトリジャンクションは、階層的に関係する組織のセットであり、ディレクトリリソースの実際の階層構造コンテナのセットをミラー化したものです。ディレクトリリソースは、階層構造コンテナを使用して、階層構造の名前空間を使用するリソースです。ディレクトリリソースの例には、LDAP サーバーおよび Windows Active Directory リソースがあります。

ディレクトリジャンクション内の各組織は、仮想組織です。ディレクトリジャンクションの最上位の仮想組織は、リソース内に定義されたベースコンテキストを表すコンテナをミラー化したものです。ディレクトリジャンクション内の残りの仮想組織は、最上位の仮想組織の直接または間接的な子であり、定義済みリソースのベースコンテキストコンテナの子であるディレクトリリソースコンテナのいずれかをミラー化しています。この構造を図 5-4 に示します。

図 5-4　　Identity Manager 仮想組織



ディレクトリジャンクションは、既存の Identity Manager 組織構造を任意の場所で接合することができます。ただし、ディレクトリジャンクションは既存のディレクトリジャンクション内またはその下で接合することはできません。

ディレクトリジャンクションを Identity Manager 組織ツリーに追加すると、そのディレクトリジャンクションのコンテキスト内で仮想組織を作成または削除することができます。また、ディレクトリジャンクションを構成する仮想組織のセットを任意の時点で更新して、ディレクトリリソースコンテナと同期しているかどうかを確認できます。ディレクトリジャンクション内に非仮想組織を作成することはできません。

Identity Manager オブジェクト (ユーザー、リソース、およびロールなど) を、Identity Manager 組織と同様の方法で仮想組織のメンバーにして、仮想組織から使用可能にすることができます。

ディレクトリジャンクションのセットアップ

ディレクトリジャンクションは、「Identity Manager アカウント」エリアでセットアップします。

1. Identity Manager メニューバーで、「アカウント」を選択します。
2. 「アカウント」リストで Identity Manager 組織を選択し、「新規作成アクション」リストから「新規ディレクトリジャンクション」を選択します。

   選択した組織は、セットアップする仮想組織の親組織になります。

   Identity Manager に「ディレクトリジャンクションの作成」ページが表示されます。
3. 項目を選択して、仮想組織をセットアップします。
   - **「親組織」** — このフィールドには「アカウント」リストから選択した組織が含まれています。ただし、リストから異なる親組織を選択することもできます。
   - **「ディレクトリリソース」** — 構造を仮想組織にミラー化する既存のディレクトリを管理するディレクトリリソースを選択します。
   - **「ユーザーフォーム」** — この組織の管理者に適用するユーザーフォームを選択します。
   - **「Identity Manager アカウントポリシー」** — ポリシーを選択します。または、デフォルトのオプション (継承) を選択すると親組織からポリシーが継承されます。
   - **「承認者」** — この組織に関係するリクエストを承認できる管理者を選択します。

仮想組織の更新

このプロセスでは、選択した組織の下位にある、関連付けられたディレクトリリソースを持つ仮想組織を更新して同期し直します。リストで仮想組織を選択し、「組織アクション」リストから「組織の更新」を選択します。

仮想組織の削除

仮想組織を削除する場合は、次の 2 つの削除オプションから選択できます。

- Identity Manager 組織のみを削除」 − Identity Manager ディレクトリジャンクションのみを削除します。
- Identity Manager 組織とリソースコンテナを削除」 − Identity Manager ディレクトリジャンクションと、ネイティブリソース上にある対応する組織を削除します。

いずれかのオプションを選択して、「削除」をクリックします。

機能とその管理について

機能は、Identity Manager システム内の権限のグループです。機能は、パスワードのリセットやユーザーアカウントの管理などの管理ジョブの役割を表します。各 Identity Manager 管理ユーザーには、1 つ以上の機能が割り当てられ、データの保護をおびやかすことなく、特権のセットを提供します。

すべての Identity Manager ユーザーに機能を割り当てる必要はありません。機能を割り当てる必要があるのは、Identity Manager を使用して 1 つ以上の管理操作を実行するユーザーだけです。たとえば、ユーザーが自分のパスワードを変更する場合は、機能が割り当てられている必要はありませんが、別のユーザーのパスワードを変更する場合には、機能が必要になります。

割り当てられた機能により、Identity Manager 管理者インタフェースのどのエリアにアクセスできるかが決まります。すべての Identity Manager 管理ユーザーは、次の Identity Manager エリアにアクセスできます。

- 「**ホーム**」および「**ヘルプ**」タブ
- 「**パスワード**」タブ (「**自分のパスワードの変更**」および「**自分の秘密の質問の回答の変更**」サブタブのみ)
- 「**レポート**」(管理者の持つ役割に関連するレポートタイプのみ)

機能のカテゴリ

Identity Manager の機能は、次のように分類されています。

-  タスクベース。これらはもっとも単純なタスクレベルにある機能です。
-  機能。実用上の機能は、1 つ以上の実用上の機能またはタスクベース機能で構成されます。

組み込み機能 (Identity Manager システムに付属の機能) は保護されており、編集することができません。ただし、この機能を、自分で作成した機能の中で使用することはできます。

保護された (組み込み) 機能は、赤い鍵 (または赤い鍵とフォルダ) のアイコンとしてリストに示されます。ユーザーが作成し、編集できる機能は、緑色の鍵 (または緑色の鍵とフォルダ) アイコンとして機能リストに示されます。

機能の操作

1. メニューバーで、「セキュリティー」を選択します。
2. 「機能」タブを選択すると、Identity Manager 機能のリストが表示されます。

機能の作成

機能を作成するには、「新規」をクリックします。新しい機能に名前を付けて、機能、譲渡者、および、この機能を利用できる組織を選択します。少なくとも 1 つの組織を選択する必要があります。

注	譲渡者の選択元となる一連のユーザーには、機能の割り当て権限を割り当てられているユーザーが含まれます。

機能の編集

保護されていない機能を編集するには、リストでその機能を右クリックし、「編集」を選択します。

組み込み機能は編集できません。ただし、それを別の名前で保存して独自の機能を作成したり、自分で作成した機能の中で組み込み機能を使用したりすることはできます。

機能の保存と名前の変更

機能を「クローン作成」する (異なる名前で保存して、新しい機能を作成する) には、次を実行します。

- リスト内の機能を右クリックし、「名前を付けて保存」を選択します。
- 新しい名前を入力して、「OK」をクリックします。

コピー元の機能は保護されていますが、新しい機能は編集できます。

機能の割り当て

「ユーザーの作成」および「ユーザーの編集」ページから、ユーザーに機能を割り当てます。インタフェースの「セキュリティー」エリアでセットアップした管理者ロールを割り当てる方法で、ユーザーに機能を割り当てることもできます。詳細については、189 ページの「管理者ロールとその管理について」を参照してください。

機能の階層

タスクベースの機能は、次のような実用上の機能階層に分類されます。

Account Administrator

- Approver Administrator
  - Organization Approver
  - Resource Approver
  - Role Approver
- Assign User Capabilities
- SPML Access
- User Account Administrator
  - Create User
  - Delete User
    - Delete IDM User
    - Deprovision User
    - Unassign User
    - Unlink User
  - Disable User
  - Enable User
  - Password Administrator
    - Change Password Administrator
    - Reset Password Administrator

- Rename User
- Unlock User
- Update User
- View User
- Import User

Admin Role Administrator

- Connect Capabilities
- Connect Capabilities Rules
- Connect Controlled Organizations Rules
- Connect Organizations

Auditor Administrator

- Assign Audit Policies
  - Assign Organization Audit Policies
  - Assign User Audit Policies
- Audit Policy Administrator
  - Auditor View User
- Auditor Periodic Access Review Administrator
  - Auditor Access Scan Administrator
- Auditor Report Administrator
- Password Administrator
- User Account Administrator
- Assign User Capabilities

Auditor Report Administrator

- Access Review Detail Report Administrator
  - Run Access Review Detail Report
- Access Review Summary Report Administrator
  - Run Access Review Summary Report
- Audit Policy Scan Report Administrator
  - Run Audit Policy Scan Report
- Audited Attribute Report Administrator

- Run Audited Attribute Report
- AuditPolicy Violation History Administrator
  - Run Audit Policy Violation History Report
- Organization Violation History Administrator
  - Run Organization Violation History Report
- Policy Summary Report Administrator
- Resource Violation History Administrator
  - Run Resource Violation History Report
- Run Auditor Report
- Separation of Duties Report Administrator
  - Run Separation of Duties Report
- User Access Report Administrator
  - Run User Access Report
- Violation Summary Report Administrator

Bulk Account Administrator

- Approver Administrator
- Assign User Capabilities
- Bulk User Account Administrator
  - Bulk Create User
  - Bulk Delete IDM User
    - Bulk Delete IDM User
    - Bulk Deprovision User
    - Bulk Unassign User
    - Bulk Unlink User
  - Bulk Disable User
  - Bulk Enable User
  - Password Administrator
  - Rename User
  - Unlock User
  - View User

- Import User

Bulk Change Account Administrator

- Approver Administrator
- Assign User Capabilities
- Bulk Change User Account Administrator
  - Bulk Disable User
  - Bulk Enable User
  - Bulk Update User
  - Password Administrator
  - Rename User
  - Unlock User
  - View User

Bulk Resource Password Administrator

- Bulk Change Resource Password Administrator
- Bulk Reset Resource Password Administrator

Capability Administrator

Change Account Administrator

- Approver Administrator
- Assign User Capabilities
- Change User Account Administrator
  - Password Administrator
    - Change Password Administrator
    - Reset Password Administrator
  - Disable User
  - Enable User
  - Rename User
  - Unlock User
  - Update User
  - View User

Configure Certificates

Import/Export Administrator

License Administrator

Login Administrator

Meta View Administrator

Organization Administrator

Password Administrator (Verification Required)

- Change Password Administrator (Verification Required)
- Reset Password Administrator (Verification Required)

Policy Administrator

Reconcile Administrator

- Reconcile Request Administrator

Remedy Integration Administrator

Report Administrator

- Admin Report Administrator
  - Run Admin Report
- Audit Report Administrator
  - Run Audit Report
- Auditor Report Administrator
  -
- Reconcile Report Administrator
  - Run Reconcile Report
- Resource Report Administrator
  - Run Resource Report
- Risk Analysis Administrator
  - Run Risk Analysis
- Role Report Administrator

- Run Role Report
- Task Report Administrator
  - Run Task Report
- User Report Administrator
  - Run User Report
- Configure Audit

Resource Administrator

- Change Active Sync Resource Administrator
- Control Active Sync Resource Administrator
- Resource Group Administrator

Resource Object Administrator

Resource Password Administrator

- Change Resource Password Administrator
- Reset Resource Password Administrator

Role Administrator

Security Administrator

Service Provider Administrator

- Service Provider User Administrator
  - Service Provider Create User
  - Service Provider Delete User
  - Service Provider Update User
  - Service Provider View User

Service Provider Admin Role Administrator

User Account Administrator

- Delete User
- Password Administrator
- Create User
- Disable User

- Enable User
- Import User
- Rename User
- Unlock User
- Update User

View Organizations

- List Organizations

View Resources

- List Resources

Waveset Administrator

機能の定義

表 5-1 で、各タスクベースの機能と、各機能でアクセスできるタブおよびサブタブについて説明します。機能は、名前のアルファベット順に並べられています。

すべての機能で、ユーザーまたは管理者は、「パスワード」の「自分のパスワードの変更」および「自分の秘密の質問の回答の変更」タブにアクセスすることができます。

表 5-1 Identity Manager 機能の説明

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Access Review Detail Report Administrator	アクセスレビュー詳細レポートの作成、編集、削除、および実行	「レポート」>「レポートの実行」タブ、「レポートの表示」タブ - アクセスレビュー詳細レポートのみ 「レポート」>「ダッシュボードの表示」
Access Review Summary Report Administrator	アクセスレビュー概要レポートの作成、編集、削除、および実行	**「レポート」** - アクセスレビュー概要レポートのみ 「レポート」>「ダッシュボードの表示」
Account Administrator	機能の割り当てなど、ユーザーに対するすべての操作の実行 (一括アクションを除く)	**「アカウント」** -「アカウントのリスト」、「ユーザーの検索」、「ファイルへ抽出」、「ファイルから読み込み」、「リソースから読み込み」タブ **「パスワード」** - すべてのサブタブ **「作業項目」** -「承認」サブタブ **「タスク」** - すべてのサブタブ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Admin Report Administrator	管理者レポートの作成、編集、削除、および実行	**「レポート」**-「レポートの管理」、「レポートの実行」サブタブ (管理者レポートのみ)
Admin Role Administrator	管理者ロールの作成、編集、および削除	**「セキュリティー」**-「管理者ロール」サブタブ
Approver Administrator	ほかのユーザーにより発行されたリクエストの承認または却下	**デフォルトのみ**
Assign Audit Policies	ユーザーアカウントと組織への監査ポリシーの割り当て	**「アカウント」**-「ユーザーアクション」リストの「ユーザーの監査ポリシーの編集」 **「アカウント」**-「組織アクション」リストの「組織の監査ポリシーの編集」
Assign Organization Audit Policies	監査ポリシーを組織のみに割り当て	**「アカウント」**-「組織アクション」リストの「組織の監査ポリシーの編集」、「アカウントのリスト」タブ
Assign User Audit Policies	監査ポリシーをユーザーのみに割り当て	**「アカウント」**-「ユーザーアクション」リストの「ユーザーの監査ポリシーの編集」、「アカウントのリスト」タブ、「ユーザーの検索」タブ
Assign User Capabilities	ユーザー機能の割り当ての変更 (割り当て、割り当て解除)	**「アカウント」**-「アカウントのリスト」(編集のみ)、「ユーザーの検索」サブタブ。 別のユーザー管理者機能 (「ユーザーの作成」、「ユーザーの有効化」など) とともに割り当てる必要があります。
Audit Policy Administrator	監査ポリシーの作成、修正、および削除	**「コンプライアンス」**-「ポリシーの管理」
Audit Policy Scan Report Administrator	監査ポリシースキャンレポートの作成、修正、削除、および実行	**「レポート」**- 監査ポリシースキャンレポートのみ
Audit Report Administrator	監査レポートの作成、修正、削除、および実行	**「レポート」**- 監査レポートのみ
Audited Attribute Report Administrator	監査された属性のレポートの作成、修正、削除、および実行	**「レポート」**- 監査された属性のレポートのみ
AuditLog Report Administrator	監査ログレポートの作成、修正、削除、および実行	**「レポート」**- 監査ログレポートのみ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Auditor Access Scan Administrator	定期的アクセスレビュースキャンの作成、編集、および削除	**「コンプライアンス」- 「アクセススキャンの管理」**
Auditor Administrator	監査ポリシー、監査スキャン、ユーザーコンプライアンスの設定、管理、および監視	**「コンプライアンス」**- すべてのサブタブ
		「レポート」-「レポートの実行」、「レポートの表示」、「監査レポート」の管理
		「アカウント」-「ユーザーの監査ポリシーの編集」と「組織の監査ポリシーの編集」操作
Auditor Attestor	組織のセキュリティーを有効にしながら、ほかのユーザーをアテストする必要がある	**デフォルトのみ**
Auditor Periodic Access Review Administrator	定期的アクセスレビュー (PAR) の管理、アクセススキャンの管理、アテステーションの管理、PAR レポートの管理	**「コンプライアンス」**-「アクセススキャンの管理」、「アクセスレビュー」サブタブ
Auditor 是正者	監査ポリシー違反の是正、受け入れ、転送	**「是正」**- すべてのサブタブ
Auditor Report Administrator	任意の監査レポートの作成、修正、削除、および実行	**「レポート」**- 監査レポートのすべての操作
Auditor View User	ユーザーに関連するコンプライアンス情報の表示	**「アカウント」**-「アカウントのリスト」、「ユーザーの検索」タブ
AuditPolicy Violation History Administrator	監査ポリシー別違反履歴表示レポートの作成、修正、削除、および実行	**「レポート」**- 監査ポリシー別違反履歴表示レポートのみ
Bulk Account Administrator	機能の割り当てなど、ユーザーに対する通常操作および一括アクションの実行	**「アカウント」**- すべてのサブタブ
		「パスワード」- すべてのサブタブ
		「承認」- すべてのサブタブ
		「タスク」- すべてのサブタブ
Bulk Change Account Administrator	機能の割り当てなど、既存のユーザーに対する、既存のユーザーの削除以外の通常操作および一括アクションの実行	**「アカウント」**-「アカウントのリスト」、「ユーザーの検索」、「一括アクションの起動」サブタブ。ユーザーを作成または削除することはできません。
		「パスワード」- すべてのサブタブ
		「承認」- すべてのサブタブ
		「タスク」- すべてのサブタブ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Bulk Change User Account Administrator	既存のユーザーに対する、削除以外の通常操作および一括アクションの実行	**「アカウント」**- 「アカウントのリスト」、「ユーザーの検索」、「一括アクションの起動」サブタブ。機能の作成と削除、およびユーザーへの機能の割り当てを行うことはできません。 **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Bulk Create User	リソースの割り当てとユーザー作成リクエストの発行 (個別のユーザーに対する操作または一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(作成のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ **「タスク」**- すべてのサブタブ
Bulk Delete IDM User	Identity Manager ユーザーアカウントの削除、リソースアカウントのプロビジョン解除、割り当て解除、およびリンク解除 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(作成のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ **「タスク」**- すべてのサブタブ
Bulk Delete IDM User	既存の Identity Manager ユーザーアカウントの削除 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(削除のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ **「タスク」**- すべてのサブタブ
Bulk Deprovision User	既存のリソースアカウントの削除およびリンク解除 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(プロビジョン解除のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ **「タスク」**- すべてのサブタブ
Bulk Disable User	既存のユーザーとリソースアカウントの無効化 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(無効化のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ **「タスク」**- すべてのサブタブ
Bulk Enable User	既存のユーザーとリソースアカウントの有効化 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(有効化のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ **「タスク」**- すべてのサブタブ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Bulk Unassign User	既存のリソースアカウントの割り当て解除およびリンク解除 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(割り当て解除のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ
		「タスク」- すべてのサブタブ
Bulk Unlink User	既存のリソースアカウントのリンク解除 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(リンク解除のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ
		「タスク」- すべてのサブタブ
Bulk Update User	既存のユーザーとリソースアカウントの更新 (個別のユーザーに対する操作および一括アクションを使用した操作)	**「アカウント」**- 「アカウントのリスト」(更新のみ)、「ユーザーの検索」、「一括アクションの起動」サブタブ
		「タスク」- すべてのサブタブ
Bulk User Account Administrator	ユーザーに対するすべての通常操作および一括アクションの実行	**「アカウント」**- すべてのサブタブ
		「パスワード」- すべてのサブタブ
		「タスク」- すべてのサブタブ
Capability Administrator	機能の作成、修正、および削除	**「設定」**- 「機能」サブタブ
Change Account Administrator	機能の割り当てなど、既存のユーザーに対する削除以外のすべての操作の実行 (一括アクションを除く)	**「アカウント」**- すべてのサブタブ。ユーザーを削除することはできません。
		「パスワード」- すべてのサブタブ
		「承認」- すべてのサブタブ
		「タスク」- すべてのサブタブ
		「レポート」- 管理レポートおよびユーザーレポートの作成、管理レポートの実行と編集、および範囲内の監査ログレポートを実行します。範囲外の組織の管理レポートおよびユーザーレポートを実行することはできません。

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Change Active Sync Resource Administrator	Active Sync リソースパラメータの変更	**「タスク」**- 「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ **「リソース」**- Active Sync リソース : 「編集」アクションメニュー、「Active Sync パラメータの編集」
Change Password Administrator	ユーザーおよびリソースアカウントパスワードの変更	**「アカウント」**- 「アカウントのリスト」、「ユーザーの検索」サブタブ (パスワードの変更のみ) **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (「タスクの実行」サブタブから)
Change Password Administrator (Verification Required)	ユーザーの秘密の質問の回答が正しく検証されたあとの、ユーザーおよびリソースアカウントパスワードの変更	**「アカウント」**- 「アカウントのリスト」、「ユーザーの検索」サブタブ (パスワードの変更のみ、操作の前に検証が必要) **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (「タスクの実行」サブタブから)
Change Resource Password Administrator	リソース管理者のアカウントパスワードの変更	**「タスク」**- すべてのサブタブ **「リソース」**- **「リソースのリスト」**サブタブリソースパスワードの変更のみ (アクションメニューの**「接続の管理」-->「パスワードの変更」**から)
Change User Account Administrator	既存のユーザーに対する削除以外のすべての操作の実行 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」、「ユーザーの検索」サブタブ。機能の作成と削除、およびユーザーへの機能の割り当てを行うことはできません。 **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Configure Audit	システム内で監査されるイベントと設定グループの設定	**「設定」**- 「イベント監査」サブタブ
Configure Certificates	信頼できる証明書と CRL の設定	**「セキュリティー」**- 「証明書」サブタブ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Control Active Sync Resource Administrator	Active Sync リソースの状態 (開始、停止、更新など) の管理	**「タスク」**- 「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ
		「リソース」- Active Sync リソース : 「Active Sync」アクションメニュー (すべての選択肢)
Create User	リソースの割り当てとユーザー作成リクエストの開始 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(作成のみ)、「ユーザーの検索」サブタブ
		「タスク」- すべてのサブタブ
Delete User	Identity Manager ユーザーアカウントの削除、リソースアカウントのプロビジョン解除、割り当て解除、およびリンク解除 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(削除のみ)、「ユーザーの検索」サブタブ
		「タスク」- すべてのサブタブ
Delete IDM User	Identity Manager ユーザーアカウントの削除 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(削除のみ)、「ユーザーの検索」サブタブ
		「タスク」- すべてのサブタブ
Deprovision User	既存のリソースアカウントの削除およびリンク解除 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(プロビジョン解除のみ)、「ユーザーの検索」サブタブ
		「タスク」- すべてのサブタブ
Disable User	既存のユーザーアカウントとリソースアカウントの無効化 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(無効化のみ)、「ユーザーの検索」サブタブ
		「タスク」- すべてのサブタブ
Enable User	既存のユーザーアカウントとリソースアカウントの有効化 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(有効化のみ)、「ユーザーの検索」サブタブ
		「タスク」- すべてのサブタブ
Import User	定義済みリソースからのユーザーのインポート	**「アカウント」**- 「ファイルへ抽出」、「ファイルから読み込み」、「リソースから読み込み」サブタブ
Import/Export Administrator	全タイプのオブジェクトのインポートとエクスポート	**「設定」**- 「交換ファイルのインポート」サブタブ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
License Administrator	アイデンティティーシステム製品ライセンスの設定	`lh license` コマンドの実行権を提供します。この機能を割り当てただけでは「管理者インタフェース」にはアクセスできません。
Login Administrator	所定のログインインタフェースに対するログインモジュールセットの編集	**「設定」**- 「ログイン」サブタブ
Meta View Administrator	アイデンティティー属性の設定の変更	**「メタビュー」**- 「アイデンティティー属性」タブ
Organization Administrator	組織の作成、編集、および削除	**「アカウント」**- 「アカウントのリスト」サブタブ (組織およびディレクトリジャンクションの編集と作成、組織の削除のみ)
Organization Approver	新しい組織に対するリクエストの承認	**「作業項目」**- 「承認」サブタブ
Organization Violation History Administrator	組織別違反履歴表示レポートの作成、修正、削除、および実行	**「レポート」**- 組織別違反履歴表示レポートのみ
Password Administrator	ユーザーおよびリソースアカウントパスワードの変更とリセット	**「アカウント」**- 「アカウントのリスト」(パスワードのリスト、変更、およびリセットのみ)、「ユーザーの検索」サブタブ **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Password Administrator (Verification Required)	ユーザーの秘密の質問の回答が正しく検証されたあとの、ユーザーおよびリソースアカウントパスワードの変更とリセット	**「アカウント」**- 「アカウントのリスト」(パスワードのリスト、変更、およびリセットのみ、操作が成功するためには検証が必要)、「ユーザーの検索」サブタブ **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Policy Administrator	ポリシーの作成、編集、および削除	**「設定」**- 「ポリシー」サブタブ
Policy Summary Report Administrator	ポリシーの概要レポートの作成、修正、削除、および実行	**「レポート」**- ポリシーの概要レポートのみ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Reconcile Administrator	調整ポリシーの編集と調整タスクの管理	**「サーバータスク」**- すべてのサブタブ (調整タスクの表示)
		「リソース」-「リソースのリスト」サブタブ
Reconcile Report Administrator	調整レポートの作成、編集、削除、および実行	**「レポート」**-「レポートの実行」(アカウントインデックスレポートのみ)、「レポートの管理」サブタブ
Reconcile Request Administrator	調整リクエストの管理	**「タスク」**- すべてのサブタブ
		「リソース」-「リソースのリスト」サブタブ (リストおよび調整機能のみ)
Remedy Integration Administrator	Remedy との統合の設定の修正	**「タスク」**- すべてのサブタブ (タスクの表示、ロールの同期の実行)
		「設定」-「Remedy との統合」サブタブ
Rename User	既存のユーザーアカウントとリソースアカウントの名前の変更	**「アカウント」**-「アカウントのリスト」サブタブ (範囲内のすべてのアカウントのリスト、ユーザーの名前変更)
Report Administrator	監査の設定と全タイプのレポートの実行	**「タスク」**- すべてのサブタブ (タスクの表示、ロールの同期の実行)
		「レポート」- すべてのサブタブ
Reset Password Administrator	ユーザーおよびリソースアカウントパスワードのリセット	**「アカウント」**-「アカウントのリスト」、「ユーザーの検索」サブタブ (パスワードのリセットのみ)
		「パスワード」- すべてのサブタブ
		「タスク」- すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (「タスクの実行」サブタブから)
Reset Password Administrator (Verification Required)	ユーザーの秘密の質問の回答が正しく検証されたあとの、ユーザーおよびリソースアカウントパスワードのリセット	**「アカウント」**-「アカウントのリスト」、「ユーザーの検索」サブタブ (パスワードのリセットのみ、正しく操作するためには検証が必要)
		「パスワード」- すべてのサブタブ
		「タスク」- すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (「タスクの実行」サブタブから)

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Reset Resource Password Administrator	リソース管理者のアカウントパスワードのリセット	**「タスク」**- 「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ **「リソース」- 「リソースのリスト」**サブタブ。リソースパスワードのリセットのみ (アクションメニューの「接続の管理」 -->「パスワードのリセット」から)
Resource Administrator	リソースの作成、修正、および削除	**「レポート」**- リソースユーザーレポート、リソースグループレポートは範囲外のリソースに関するエラーを返します。 **「リソース」**-「リソースのリスト」サブタブ (グローバルポリシーの編集、パラメータの編集、リソースグループ。接続またはリソースオブジェクトを管理することはできない)。
Resource Group Administrator	リソースグループの作成、編集、および削除	**「リソース」**-「リソースグループのリスト」サブタブ
Resource Object Administrator	リソースオブジェクトの作成、修正、および削除	**「タスク」**-「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ (リソースオブジェクトを含むタスクの表示)。 **「リソース」**-「リソースのリスト」サブタブ (リソースオブジェクトのリストおよび管理のみ)
Resource Password Administrator	リソースプロキシアカウントパスワードの変更とリセット	**「タスク」**-「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ **「リソース」- 「リソースのリスト」**サブタブ。リソースパスワードの変更のみ (アクションメニューの**「接続の管理」 -->「パスワードの変更」**から)
Resource Report Administrator	リソースレポートの作成、編集、削除、および実行	**「レポート」**- すべてのサブタブ (リソースレポートのみ)
Resource Violation History Administrator	リソース別違反履歴表示レポートの作成、修正、削除、および実行	**「レポート」**- リソース別違反履歴表示レポートのみ
Risk Analysis Administrator	リスク分析の作成、編集、削除、および実行	**「リスク分析」**- すべてのサブタブ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Role Administrator	ロールの作成、修正、および削除	**「タスク」**- 「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ (ロールの同期)
		「ロール」- すべてのサブタブ
Role Report Administrator	リソースレポートの作成、編集、削除、および実行	**「レポート」**- ロールレポートのみ
Run Access Review Detail Report	アクセスレビュー詳細レポートの実行	**「レポート」**- アクセスレビュー詳細レポートのみ
Run Access Review Summary Report	アクセスレビュー概要レポートの実行	**「レポート」**- アクセスレビュー概要レポートのみ
Run Admin Report	管理者レポートの実行	**「レポート」**- 管理レポートのみ
Run Audit Policy Scan Administrator	監査ポリシースキャンレポートの実行と管理	「レポート」- 監査ポリシースキャンレポートのみ
Run Audit Policy Scan Report	監査ポリシースキャンレポートの実行	**「レポート」**- 監査ポリシースキャンレポートのみ
Run Audit Report	監査レポートの実行	**「レポート」**- 監査ログレポートおよび使用状況レポートのみ
Run Audited Attribute Report	監査された属性のレポートの実行	**「レポート」**- 監査された属性のレポートのみ
		「レポート」>「ダッシュボードの表示」
Run Auditor Report	任意の監査レポートの実行	**「レポート」**- 任意の監査レポート
		「レポート」>「ダッシュボードの表示」
Run AuditLog Report	監査ログレポートの実行	**「レポート」**- 監査ログレポートのみ
Run AuditPolicy Violation History	組織別違反履歴表示レポートの実行	**「レポート」**- 監査ポリシー別違反履歴表示レポートのみ
		「レポート」>「ダッシュボードの表示」
Run Policy Summary Report	ポリシーの概要レポートの実行	**「レポート」**- ポリシーの概要レポートのみ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Run Organization Violation History	組織別違反履歴表示レポートの実行	**「レポート」**- 組織別違反履歴表示レポートのみ 「レポート」>「ダッシュボードの表示」
Run Reconcile Report	調整レポートの実行	**「レポート」**- 監査ログレポートおよび使用状況レポートのみ
Run Resource Report	リソースレポートの実行	**「レポート」**- 監査ログレポートおよび使用状況レポートのみ
Run Resource Violation History	リソース別違反履歴表示レポートの実行	**「レポート」**- リソース別違反履歴表示レポートのみ
Run Risk Analysis	リスク分析の実行	**「レポート」**-「リスク分析の実行」、「リスク分析の表示」サブタブ
Run Role Report	ロールレポートの実行	**「レポート」**- ロールレポートのみ
Run Task Report	タスクレポートの実行	**「レポート」**- タスクレポートのみ
Run User Access Report	詳細なユーザーレポートの実行	**「レポート」**- ユーザーアクセスレポートのみ 「レポート」>「ダッシュボードの表示」
Run User Report	ユーザーレポートの実行	**「レポート」**- ユーザーレポートのみ
Run Violation Summary Report	違反の概要レポートの実行	**「レポート」**- 違反の概要レポートのみ 「レポート」>「ダッシュボードの表示」

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Security Administrator	暗号化鍵、ログイン設定、およびポリシーの管理などの機能を持つユーザーの作成	**「アカウント」** - 「アカウントのリスト」(パスワードの削除、作成、更新、編集、および変更)、「ユーザーの検索」サブタブ (監査レポート)
		「パスワード」 - すべてのサブタブ
		「タスク」 - 「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ
		「レポート」 - すべてのサブタブ
		「リソース」 - 「リソースのリスト」サブタブ (リソースオブジェクトのリストおよび管理)
		「セキュリティー」 - 「ポリシー」、「ログイン」サブタブ
Separation of Duties Report Administrator	職務分掌レポートの作成、編集、実行、および削除	**「レポート」** - 職務分掌レポートのすべての操作のみ
Run Separation of Duties Report	職務分掌レポートの実行	**「レポート」** - 職務分掌レポートのみ
		「レポート」>「ダッシュボードの表示」
Service Provider Admin Role	サービスプロバイダ管理者ロールと関連する規則の管理	**「セキュリティー」** - 「管理者ロール」タブ
Service Provider Administrator	サービスプロバイダユーザーとサービスプロバイダトランザクションの作成、編集、および管理。トランザクションデータベースと追跡イベントの設定。	**「アカウント」** - 「サービスプロバイダユーザーの管理」サブタブ
		「サーバータスク」>「サービスプロバイダトランザクション」タブ
		「レポート」>「ダッシュボードの表示」タブ
		「レポート」>「ダッシュボードの設定」タブ
		サービスプロバイダ - すべてのサブタブ
Service Provider Create User	サービスプロバイダ (エクストラネット) ユーザーのユーザーアカウントの作成	**「アカウント」** - 「サービスプロバイダユーザーの管理」サブタブ
Service Provider Delete User	サービスプロバイダユーザーアカウントの削除	**「アカウント」** - 「サービスプロバイダユーザーの管理」サブタブ

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
Service Provider Update User	サービスプロバイダユーザーアカウントの更新	**「アカウント」**- 「サービスプロバイダユーザーの管理」サブタブ
Service Provider User Administrator	サービスプロバイダ (エクストラネット) ユーザーの管理	**「アカウント」**>「サービスプロバイダユーザーの管理」- すべてのサブタブ
Service Provider View User	サービスプロバイダ (エクストラネット) ユーザーアカウント情報の表示	**「アカウント」**- 「サービスプロバイダユーザーの管理」サブタブ
SPML Access	Identity Manager の SPML (Service Provisioning Markup Language) 機能へのアクセスを許可	**「セキュリティー」**- 「機能」サブタブ
Task Report Administrator	タスクレポートの作成、編集、削除、および実行	**「レポート」**- タスクレポートのみ
Unassign User	既存のリソースアカウントの割り当て解除およびリンク解除 (一括アクションを除く)	**「アカウント」**- **「アカウントのリスト」**(割り当て解除のみ)、**「ユーザーの検索」**サブタブ
		「タスク」- すべてのサブタブ
Unlink User	既存のリソースアカウントのリンク解除 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(リンク解除のみ)、「ユーザーの検索」サブタブ
		「タスク」- すべてのサブタブ
Unlock User	ロック解除をサポートする既存のユーザーリソースアカウントのロック解除 (一括アクションを除く)	**「アカウント」**- 「アカウントのリスト」(ロック解除のみ)、「ユーザーの検索」サブタブ
		「タスク」- 「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ
Update User	既存のユーザーの編集と、ユーザー更新リクエストの発行	**「アカウント」**- ユーザーの編集および更新
		「タスク」- 既存のタスクの管理 (「すべてのタスク」サブタブから)
User Access Report Administrator	ユーザーアクセスレポートの作成、実行、編集、および削除	**「レポート」**- ユーザーアクセスレポートのみ
		「レポート」>「ダッシュボードの表示」

表 5-1　Identity Manager 機能の説明 (続き)

機能	管理者 / ユーザーに許可する操作	アクセス可能なタブとサブタブ
User Account Administrator	ユーザーに対するすべての操作	**「アカウント」**- 「アカウントのリスト」、「ユーザーの検索」、「ファイルへ抽出」、「ファイルから読み込み」、「リソースから読み込み」サブタブ。ユーザー機能を割り当てることはできません (「アカウントのリスト」サブタブの「セキュリティー」フォームタブ)。 **「タスク」**- 「タスクの検索」、「すべてのタスク」、「タスクの実行」サブタブ
User Report Administrator	ユーザーレポートの作成、編集、削除、および実行	**「レポート」**- ユーザーレポートの実行
View User	個別のユーザーの詳細の表示	**「アカウント」**- リストからユーザーを選択して、個別のユーザーアカウント情報を表示します。変更操作は許可されません。
Violation Summary Report Administrator	違反の概要レポートの作成、修正、削除、および実行	**「レポート」**- 違反の概要レポートのみ 「レポート」>「ダッシュボードの表示」
Waveset Administrator	System Configuration オブジェクトの修正など、システム全体にわたるタスクの実行	**「サーバータスク」**- すべてのサブタブ。ロールの同期、ソースアダプタテンプレートの編集、およびレポートのスケジュール **「レポート」**- すべてのサブタブ **「リソース」**-「リソースのリスト」(リストのみ、変更操作は許可されない) **「設定」**-「監査」、「電子メールテンプレート」、「フォームおよびプロセスマッピング」、および「サーバー」サブタブ

管理者ロールとその管理について

管理者ロールを使用すると、1 人または複数の管理者に、機能と管理の範囲の一意の組み合わせや管理する組織を割り当てることができます。1 人の管理者に複数の管理者ロールを割り当てられます。これによって、管理者は 1 つの管理の範囲内ではある一連の機能を持ち、別の管理の範囲内では別の一連の機能を持つことができます。

たとえば、管理者にある管理者ロールを割り当てて、その管理者ロールで指定された管理対象組織のユーザーの作成および編集の権限を与えます。同じ管理者に別の管理者ロールを割り当てて、その管理者ロールで指定された管理対象組織では、ユーザーのパスワード変更の権限のみを与えることもできます。

ユーザーに直接機能や管理する組織を割り当てるのではなく、管理者ロールを使用して管理特権を与えることをお勧めします。管理者ロールでは機能と範囲または管理の組み合わせを再使用し、同時に多数のユーザーに対する管理者特権の管理を簡素化できます。

機能または組織 (またはその両方) の管理者ロールへの割り当ては、直接または間接的 (動的) に行うことができます。

- **直接** ー この方法を使用して、機能および / または管理する組織を明示的に管理者ロールに割り当てます。たとえば、管理者ロールには管理する組織として最上位と User Report Administrator 機能が割り当てられている場合があります。
- **動的** (間接) ー この方法は、機能および管理する組織の規則の割り当てを使用します。規則は管理者ロールを割り当てられた管理者がログインするたびに評価され、管理者の認証に基づいて機能および / または管理する組織の明示的なセットを動的に決定します。

  たとえば、ユーザーがログインする場合、次のようになります。

  - ユーザーの Active Directory (AD) ユーザータイトルが 'manager' (マネージャー) である場合には、機能規則は割り当てられる機能としてアカウント管理者を返します。
  - ユーザーの Active Directory (AD) ユーザー部署が 'marketing' (マーケティング) である場合には、管理する組織規則は割り当てられる管理組織としてマーケティングを返します。

管理者への管理者ロールの割り当ては直接または間接的 (動的) に行うことができます。

- **直接** ー 管理者ロールを管理者 (ユーザーアカウント) に明示的に割り当てます。
- **間接 (動的)** ー 管理者ロール規則を使用して管理者ロールを割り当てます。Identity Manager は管理者がログインするたびに規則を評価して、管理者ロールが認証中の管理者に割り当てられるかどうかを判断します。

たとえば、ユーザーがログインし、その Active Directory (AD) ユーザー都市が `Austin` で州が `Texas` の場合、規則は `true` を返します。このため、管理者ロールが割り当てられます。

注 管理者ロールのユーザーへの動的割り当ては、各ログインインタフェース (たとえば、ユーザーインタフェースまたは管理者インタフェース) でシステム設定属性 `security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.`*loginterface* を `true` または `false` に設定して有効または無効にできます。デフォルトはすべてのインタフェースで false です。

管理者ロールの規則

Identity Manager には、管理者ロールの規則の作成に使用できるサンプル規則があります。これらの規則は、`sample/adminRoleRules.xml` 内の Identity Manager インストールディレクトリにあります。表 5-2 は規則名と規則に指定する必要のある `authType` を示しています。

表 5-2 管理者ロールのサンプル規則

規則名	authType
管理する組織の規則	ControlledOrganizationsRule
機能規則	CapabilitiesRule
ユーザーへの管理者ロール割り当て規則	UserIsAssignedAdminRoleRule

注 サービスプロバイダユーザー管理者ロールのサンプル規則については、「サービスプロバイダの管理」の章の 463 ページの「委任された管理」を参照してください。

ユーザー管理者ロール

Identity Manager にはユーザー管理者ロールという組み込み管理者ロールがあります。デフォルトでは、割り当てられた機能や管理する組織の割り当てはありません。また、このロールを削除することはできません。この管理者ロールは、ログインするインタフェース (たとえば、ユーザー、管理者、コンソール、または IDE) に関らず、ログイン時に暗黙的にすべてのユーザー、つまりエンドユーザーと管理者に割り当てられます。

注 サービスプロバイダユーザーの管理者ロールの作成については、「サービスプロバイダの管理」の章の 463 ページの「委任された管理」を参照してください。

ユーザー管理者ロールは、管理者インタフェースで「セキュリティー」を選択してから「管理者ロール」を選択することによって編集できます。

この管理者ロールによって静的に割り当てられる機能または管理する組織はすべてのユーザーに割り当てられるので、機能および管理する組織の割り当ては規則を通して行うことをお勧めします。そうすることで、異なるユーザーが異なる機能を持つまたは機能を持たないようにすることができ、ユーザーがだれか、ユーザーがどの部署に所属するか、またはユーザーが管理者であるかなど、規則のコンテキスト内で問い合わせ可能な要素に基づいて割り当ての範囲が設定されます。

ユーザー管理者ロールによって、ワークフローで使用される `authorized=true` フラグの有用性が低下したり、そのフラグが完全に取って代わられるわけではありません。ワークフローが実行中である場合を除き、ワークフローがアクセスするオブジェクトに対してユーザーがアクセス権を持っていないときには、依然としてこのフラグのほうが適しています。基本的には、このときユーザーは「スーパーユーザーとして実行」モードに入ります。

しかし、ユーザーがワークフロー外にあるまたはワークフロー内にある可能性のある 1 つ以上のオブジェクトに対して特定のアクセス権を持っている場合は、ユーザー管理者ロールを使用して機能および管理する組織を動的に割り当てることにより、それらのオブジェクトに対して動的で緻密な承認を行えます。

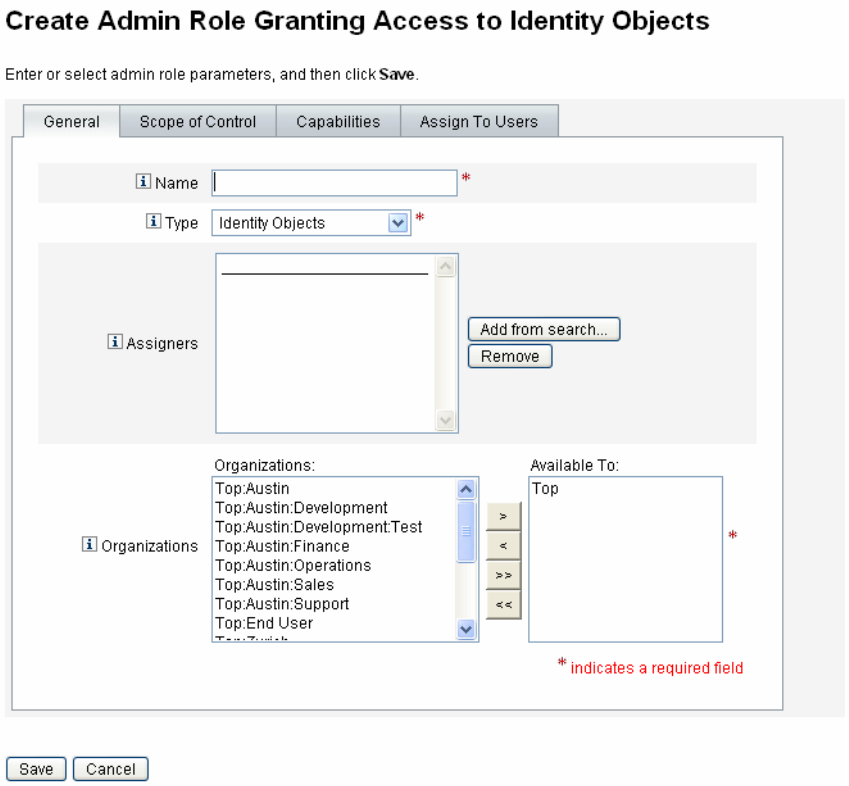
管理者ロールの作成および編集

管理者ロールを作成または編集するには、Admin Role Administrator 機能が必要です。

管理者ロールにアクセスするには、管理者インタフェースで「セキュリティー」をクリックしてから「管理者ロール」タブをクリックします。「管理者ロール」リストページでは、Identity Manager ユーザーとサービスプロバイダユーザーの管理者ロールを作成、編集、および削除できます。

既存の管理者ロールを編集するには、リスト内の名前をクリックします。管理者ロールを作成するには、「新規」をクリックします。Identity Manager の「管理者ロールの作成」オプションが表示されます (図 5-5 参照)。「管理者ロールの作成」画面には 4 つのタブが表示されます。これらを使用して一般的な属性、機能、新しい管理者ロールの範囲、ユーザーへのロールの割り当てを指定します。

図 5-5 「管理者ロールの作成」ページ：「General」タブ



「General」タブ

「管理者ロールの作成」または「管理者ロールの編集」画面の「General」タブを使用して、管理者ロールの次の一般的な特性を指定します。

- **「名前」** – この管理者ロールの一意の名前。

  たとえば、財務部門 (または組織) のユーザーの管理機能を持つユーザーに対して財務管理者ロールを作成できます。

- **「タイプ」** – タイプには「アイデンティティーオブジェクト」または「サービスプロバイダユーザー」を選択します。このフィールドは必須です。

Identity Manager ユーザー (またはオブジェクト) の管理者ロールを作成している場合は、「アイデンティティーオブジェクト」を選択します。サービスプロバイダユーザーにアクセス権限を与える管理者ロールを作成している場合は、「サービスプロバイダユーザー」を選択します。

注 サービスプロバイダユーザーにアクセス権限を与える管理者ロールの作成については、「サービスプロバイダの管理」の章の 463 ページの「委任された管理」を参照してください。

- **「譲渡者」** – ほかのユーザーにこの管理者ロールを割り当てることのできるユーザーを選択または検索します。選択できる一連のユーザーには、機能の割り当て権限を割り当てられているユーザーが含まれます。

  ユーザーを選択しなかった場合、管理者ロールを割り当てることのできるユーザーは、それを作成したユーザーのみになります。管理者ロールを作成したユーザーに「ユーザーへの機能の割り当て」機能が割り当てられていない場合、少なくとも 1 人のユーザーが管理者ロールをほかのユーザーに割り当てることができるように、1 人または複数のユーザーを「譲渡者」として選択します。

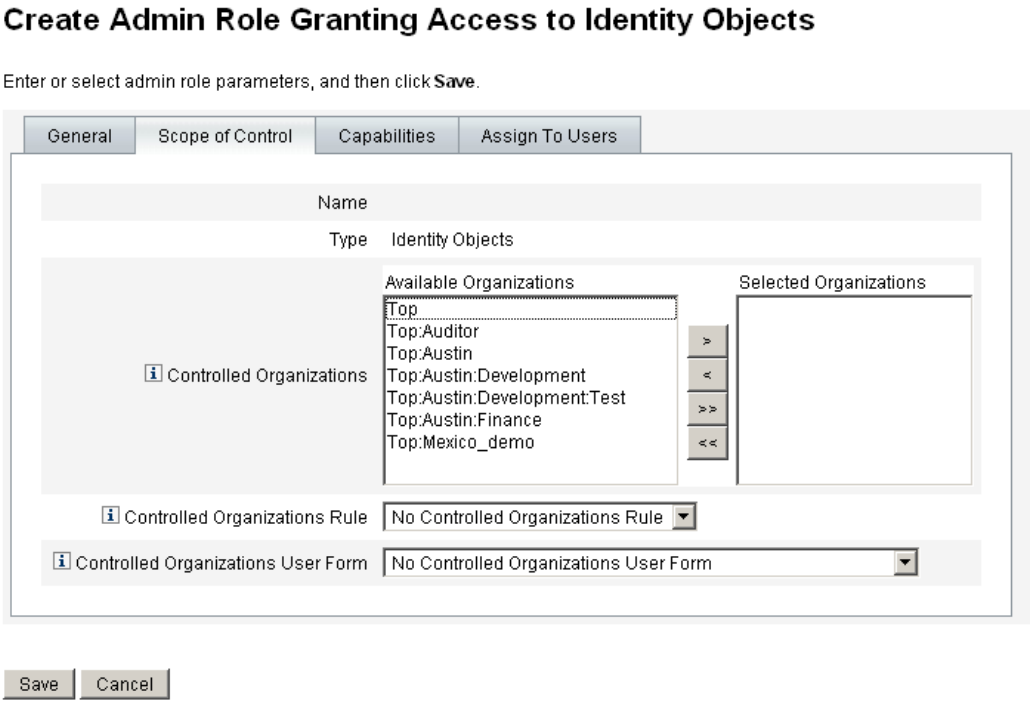
- **「組織」** – この管理者ロールが使用できる組織を 1 つまたは複数選択します。このフィールドは必須です。

  管理者は、割り当てられた組織のオブジェクト、および階層内でその組織の下位にあるすべての組織のオブジェクトを管理できます。

Scope of Control

このタブ (図 5-6 を参照) を使用して、この組織のメンバーが管理できる組織を指定するか、または管理者ロールのユーザーによって管理される組織を決定する規則を指定し、管理者ロールのユーザーフォームを選択します。

図 5-6　「管理者ロールの作成」：「Scope of Control」



- **「管理する組織」**－「利用可能な組織」リストから、この管理者ロールが管理する権利をもつ組織を選択します。
- **「管理する組織の規則」**－ ユーザーログイン時に評価の対象となる、この管理者ロールが割り当てられたユーザーによって管理される組織に対する規則を選択します。選択する規則は、`ControlledOrganizationsRule` authType を持つ必要があります。デフォルトで、管理する組織の規則は選択されていません。
- **「管理する組織のユーザーフォーム」**－ この管理者ロールが割り当てられたユーザーが、この管理者ロールの管理する組織のメンバーであるユーザーを作成または編集する場合に使用するユーザーフォームを選択します。デフォルトで、「管理する組織のユーザーフォーム」は選択されていません。

  管理者ロールを介して割り当てられたユーザーフォームは、管理者がメンバーになっている組織から継承したすべてのユーザーフォームよりも優先されます。ただし、管理者に直接割り当てられたユーザーフォームよりも優先されることはありません。

機能の割り当て

管理者ロールに割り当てられる機能によって、この管理者ロールが割り当てられたユーザーの管理権限が決まります。たとえば、この管理者ロールが管理者ロールの管理する組織のユーザーの作成のみに制限される場合があります。この場合、「ユーザーの作成」機能を割り当てます。

「Capabilities」タブで次のオプションを選択します。

- **「機能」**― これらは、管理者ロールのユーザーが管理する組織に対して持つ特定の機能 (管理権限) です。利用可能な機能のリストから 1 つ以上の機能を選択して、「割り当てられた機能」リストに移動します。
- **「機能規則」**― ユーザーログインの評価時に、管理者ロールが割り当てられたユーザーに与えられる機能のリストを決定する規則を選択します。選択する規則は、`CapabilitiesRule` authType を持つ必要があります。

管理者ロールへのユーザーフォームの割り当て

管理者ロールのメンバーにユーザーフォームを指定することができます。「管理者ロールの作成」または「管理者ロールの編集」画面の「Assign To Users」タブを使用して、割り当てを指定します。

管理者ロールを割り当てられた管理者は、その管理者ロールによって管理されている組織内のユーザーを作成または編集するときにこのユーザーフォームを使用します。管理者ロールを介して割り当てられたユーザーフォームは、管理者がメンバーになっている組織から継承したすべてのユーザーフォームよりも優先されます。ただし、管理者に直接割り当てられたユーザーフォームよりも優先されることはありません。

ユーザーを編集するときに使用されるユーザーフォームは、次の優先順位で決定されます。

- ユーザーフォームが管理者に直接割り当てられている場合は、そのユーザーフォームが使用されます。
- 管理者に直接割り当てられているユーザーフォームがなくても、次のような管理者ロールが管理者に割り当てられる場合があります。
  - 作成または編集するユーザーがメンバーになっている組織を管理する
  - その組織に対して、ユーザーフォームが指定されている

  この場合は、そのユーザーフォームが使用されます。
- 管理者に直接割り当てられているかまたは管理者ロールを介して間接的に割り当てられているユーザーフォームがない場合は、管理者のメンバー組織 (管理者のメンバー組織から最上位組織のすぐ下の組織まで) に割り当てられているユーザーフォームが使用されます。

- 管理者のメンバー組織に割り当てられているユーザーフォームがない場合は、デフォルトのユーザーフォームが使用されます。

管理者に、同じ組織を管理しながら異なるユーザーフォームを指定している複数の管理者ロールが割り当てられている場合、その組織内のユーザーを作成または編集しようとするとエラーが表示されます。管理者が、同じ組織を管理しながら異なるユーザーフォームを指定している複数の管理者ロールを割り当てようとすると、エラーが表示されます。この相反する状況を解決するまで変更は保存できません。

作業項目の管理

Identity Manager のタスクによって発生した一部のワークフロープロセスでは、アクションアイテムまたは作業項目が作成されます。これらの作業項目は、承認のリクエストや Identity Manager アカウントに割り当てられたその他の操作リクエストである場合があります。

Identity Manager は、1 か所に保留中のリクエストをすべて表示し、応答できるように、作業項目をすべてインタフェースの「作業項目」エリアにグループ化します。

作業項目のタイプ

作業項目は次のいずれかのタイプである場合があります。

- **「承認」** – 新しいアカウントまたはアカウントへの変更の承認リクエスト。
- **「アテステーション」** – ユーザーのエンタイトルメントのレビューおよび承認リクエスト。
- **「是正」** – ユーザーアカウントポリシー違反の是正または受け入れリクエスト。
- **「その他」** – 標準タイプ以外のアクションアイテムリクエスト。これは、カスタマイズされたワークフローから発生した操作リクエストである場合があります。

各作業項目タイプの保留中の作業項目を表示するには、メニューバーの「作業項目」タブをクリックします。作業項目にアクセスし、このタブからリクエストを管理したり、作業項目タイプの 1 つを選んでそのタイプのリクエストを一覧表示したりできます。

注	保留中の作業項目 (または委任された作業項目) を持つ作業項目の所有者である場合は、Identity Manager ユーザーインタフェースにログインすると、作業項目リストが表示されます。

作業項目リクエストの操作

作業項目リクエストに応答するには、インタフェースの「作業項目」の作業項目タイプのうち 1 つをクリックします。リクエストのリストから項目を選択して、使用できるボタンの 1 つをクリックして、実行する操作を示します。作業項目オプションは、作業項目タイプによって異なります。

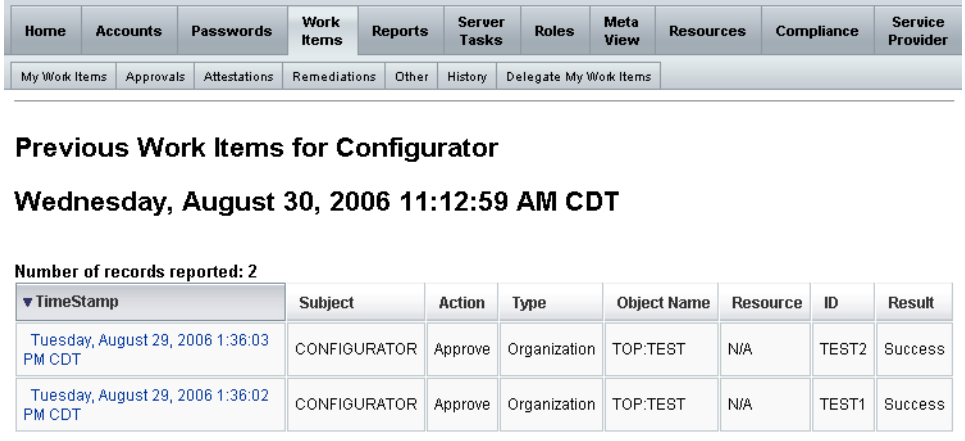
リクエストへの応答の詳細については、次のトピックを参照してください。

- 200 ページの「アカウントの承認」
- 406 ページの「アテステーション作業の管理」
- 383 ページの「コンプライアンス違反の是正と受け入れ」

作業項目履歴の表示

「作業項目」エリアの「履歴」タブを使用して、以前の作業項目操作の結果を表示できます。図 5-7 は、作業項目履歴の表示例です。

図 5-7　作業項目履歴の表示



作業項目の委任

作業項目の所有者は、作業項目を他のユーザーに一定期間委任して作業負荷を管理できます。「作業項目」>「自分の作業項目の委任」ページを使用して、承認のリクエストなど、将来の作業項目を 1 人以上のユーザー (被委任者) に委任できます。委任されるユーザーに Approver 機能は必要ありません。

注	委任機能は、将来の作業項目にのみ適用されます。既存の作業項目 (「自分の作業項目」の下に一覧表示される項目) は転送機能で選択的に転送されます。

「ユーザーの作成 / 編集」ページの「委任」フォームタブとユーザーインタフェースメインメニューからも作業項目を委任できます。

被委任者は有効な委任期間中、承認者の代わりに作業項目を承認できます。委任された作業項目には、被委任者の名前が記されます。

すべてのユーザーは自分の将来の作業項目に対する委任を設定できます。また、ユーザーを編集できる管理者も、ユーザーに代わって委任を設定できます。

監査ログエントリ

承認および却下された作業項目の監査ログエントリには、リクエストが委任された場合、委任者の名前が記されます。ユーザーが作成または修正されると、ユーザーの委任承認者情報の変更が監査ログエントリの詳細変更セクションにログ記録されます。

現在の委任の表示

「作業項目」タブから**「自分の作業項目の委任」**を選択すると、「現在の委任」ページが表示され、現在の有効な委任を表示および編集できます。

以前の委任の表示

「作業項目」タブから「自分の作業項目の委任」を選択し、「委任履歴 (Previous)」を選択すると、以前に委任された作業項目が表示され、新しい委任を設定するために使用できます。

委任の作成

委任を作成するには、「自分の作業項目の委任」を選択し、「新規」を選択します。次の選択を行います。

- **「委任する作業項目タイプの選択」** — 選択リストから作業項目タイプを選択します。

  デフォルトの作業項目タイプは、次のとおりです。

- 承認
- 組織の承認
- リソースの承認
- ロールの承認
- アテステーション
- レビュー
- アクセスレビュー是正

注 少なくとも 1 つのロールに対して承認者でない場合、「ロールの承認」タイプの作業項目を委任できません。同様に、少なくとも 1 つのリソースに対して承認者でない場合、「リソースの承認」作業項目を委任できません。また、少なくとも 1 つの組織に対して承認者でない場合、「組織の承認」作業項目を委任できません。

「組織の承認」、「リソースの承認」、または「ロールの承認」を選択すると、関連するオブジェクトタイプに関する選択エリアがページに表示されます。選択リストに一覧表示されるロール、リソース、組織には、自分が承認者であるもののみが含まれます。

このため、たとえば、自分が承認者であるリソースのうち 1 つのリソースのみに対する承認を委任できます。

- **「作業項目の委任先」** − 次のいずれかを選択します。
  - **「選択されたユーザー」** − 自分の管理範囲内で、委任するユーザーを名前で検索して選択します。また、選択した被委任者のうちのだれかがこの作業項目をさらにほかの人に委任した場合、今後リクエストされる作業項目は被委任者の被委任者に委任されることになります。

    「選択されたユーザー」エリアで 1 人以上のユーザーを選択します。または、**「検索して追加」**をクリックし、検索機能を開いてユーザーを検索します。見つけたユーザーをリストに追加するには、**「追加」**をクリックします。リストから被委任者を削除するには、そのユーザーを選択し、**「削除」**をクリックします。
  - **「自分のマネージャー」** − 作業項目リクエストを自分のマネージャーに委任する場合は、これを選択します (マネージャーが割り当てられている場合)。
  - DelegateWorkItemRule − 選択された作業項目タイプを委任できる Identity Manager ユーザー名のリストを返す規則を選択します。
- **開始日** − 作業項目の委任を開始する日付を選択します。デフォルトでは、選択した日の午前 12:01 に開始します。

- **終了日** ― 作業項目の委任が終了する日付を選択します。デフォルトでは、選択した日付の午後 11:59 に終了します。

注	1 日間だけ作業項目を委任するために、開始日と終了日を同じにすることもできます。

「**OK**」をクリックして選択を保存し、承認待ち作業項目のリストに戻ります。

委任の終了

1 つまたは複数の委任を終了するには、次の手順に従います。

1. 「委任」を選択し、「現在」を選択します。
2. 終了する 1 つまたは複数の委任を選択し、「**終了**」をクリックします。

   選択した委任設定が削除され、選択した委任された作業項目タイプが保留中の作業項目リストに戻ります。

アカウントの承認

ユーザーが Identity Manager システムに追加された場合、新しいアカウントに対する承認者として割り当てられている管理者は、アカウント作成を検証する必要があります。Identity Manager は、これらの Identity Manager オブジェクトに適用される次の 3 つの承認カテゴリをサポートします。

- **組織** ― 組織に追加されるユーザーアカウントに承認が必要です。
- **ロール** ― ロールに割り当てられるユーザーアカウントに承認が必要です。
- **リソース** ― リソースに対するアクセス権を与えられるユーザーアカウントに承認が必要です。

注	Identity Manager では、デジタル署名された承認を設定できます。詳細については、204 ページの「デジタル署名付き承認およびアクションの設定」を参照してください。

承認者のセットアップ

これらの各カテゴリに対する承認者のセットアップは必須の作業ではありませんが、セットアップすることを推奨します。アカウントの作成では、承認者をセットアップするカテゴリごとに、少なくとも 1 つの承認が必要です。1 人の承認者がリクエストの承認を却下した場合、アカウントは作成されません。

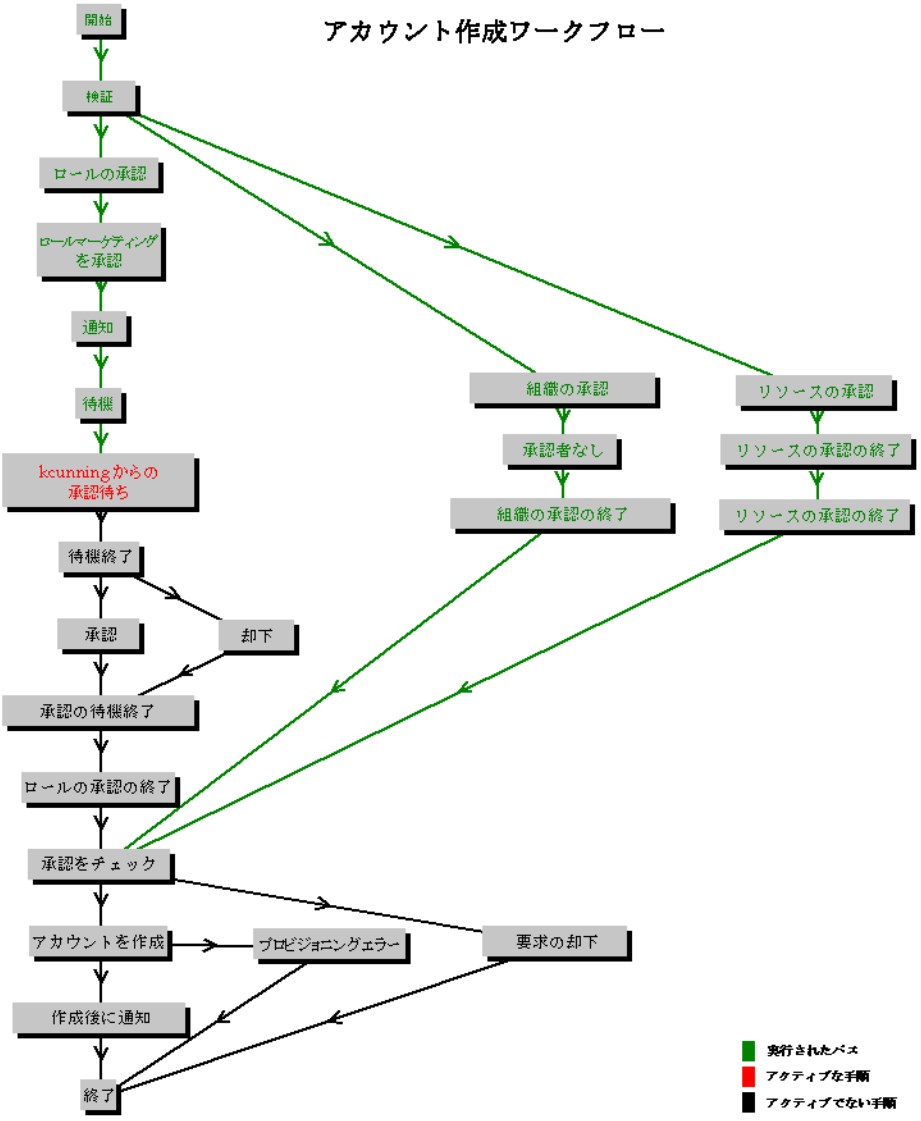
各カテゴリに複数の承認者を割り当てることができます。1 つのカテゴリ内で必要な承認は 1 つのみであるため、複数の承認者をセットアップして、ワークフローが遅延または停止していないかどうかを確認できます。1 人の承認者が利用不可能な場合は、ほかの承認者を利用してリクエストを処理できます。承認は、アカウント作成にのみ適用されます。デフォルトでは、アカウントの更新と削除に承認は必要ありません。ただし、承認を必要とするように、このプロセスをカスタマイズできます。

Identity Manager は、承認プロセスとアカウント作成リクエストのステータスをワークフロー図として図示します。Identity Manager IDE を使用すると、承認の流れを変更したり、アカウントの削除を取得したり、更新を取得したりして、ワークフローをカスタマイズすることができます。

IDE、ワークフローの詳細、承認ワークフローの変更を図示した例については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

図 5-8 はアカウント作成ワークフローとワークフロープロセスでの承認のタイミングを示しています。

図 5-8　アカウント作成ワークフロー



Identity Manager 承認者は承認リクエストを承認または却下できます。デジタル署名を使用してアカウントを承認するには、204 ページの「デジタル署名付き承認およびアクションの設定」の説明に従ってまずデジタル署名を設定する必要があります。

Identity Manager インタフェースの「作業項目」エリアで保留中の承認を表示したり、承認を管理したりできます。保留中の承認を表示するには、「作業項目」ページで「自分の作業項目」をクリックします。承認を管理するには、「承認」タブををクリックします。

承認の署名

次の手順を実行して、承認に署名します。

1. Identity Manager の管理者インタフェースから、「作業項目」を選択します。
2. 「承認」タブをクリックします。
3. リストから承認を 1 つまたは複数選択します。
4. 承認のコメントを入力して、「承認」をクリックします。

   Identity Manager はアプレットを信頼するかどうかを確認するようにリクエストします。
5. 「常時」をクリックします。

   Identity Manager は承認の日付入りの概要を表示します。
6. キーストアの場所 (署名付き承認の設定中に設定した場所。206 ページの「署名付き承認のためのクライアント側の設定」の手順 10m で説明) を、入力するかまたは**「参照」**をクリックして特定します。
7. キーストアパスワード (署名付き承認の設定中に設定したパスワード。206 ページの「署名付き承認のためのクライアント側の設定」の手順 10l で説明) を入力します。
8. 「署名」をクリックして、リクエストを承認します。

その後の承認の署名

承認に署名すると、それ以後の承認アクションでは、キーストアパスワードを入力して**「署名」**をクリックするだけで済みます。Identity Manager は、前回の承認で使用したキーストアの場所を記憶しています。

デジタル署名付き承認およびアクションの設定

次の情報と手順を使用して、デジタル署名を設定します。次のものにデジタル署名できます。

- ユーザーの承認
- アクセスレビューアクション
- コンプライアンス違反の是正

この節では、署名付き承認のために証明書と CRL を Identity Manager に追加するために必要なサーバー側とクライアント側の設定について説明します。

署名付き承認のためのサーバー側の設定

サーバー側の設定を有効にするには、次のようにします。

1. システム設定に `security.nonrepudiation.signedApprovals=true` を設定します。
2. 自分の認証局 (CA) の証明書を信頼できる証明書として追加します。そのためには、まず証明書のコピーを取得する必要があります。

   たとえば、Microsoft CA を使用している場合には、行う手順は次のようになります。

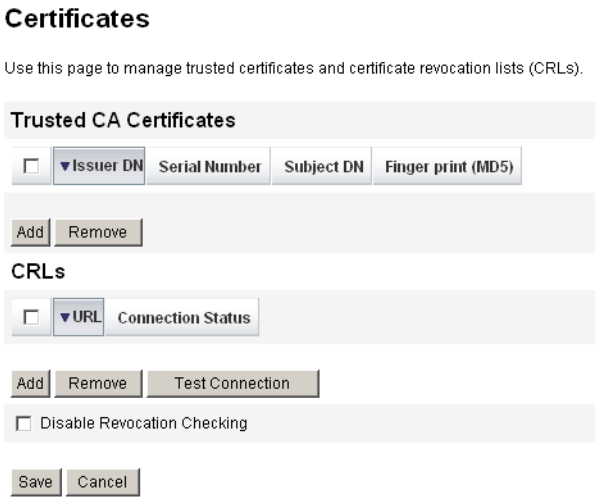
   a. http://*IPAddress*/certsrv にアクセスして、管理特権でログインします。

   b. 「CA 証明書または証明書失効リストの取得」を選択して、「次へ」をクリックします。

   c. CA 証明書をダウンロードして保存します。
3. この証明書を Identity Manager に信頼できる証明書として追加します。

   a. 管理者インタフェースから、「設定」を選択し、「証明書」を選択すると、Identity Manager は「証明書」ページを表示します。

図 5-9　　証明書



b. 「信頼できる認証局証明書」エリアで、「追加」をクリックします。Identity Manager は「証明書のインポート」ページを表示します。

c. 信頼できる証明書を参照および選択して、「インポート」をクリックします。

これで、証明書が信頼できる証明書のリストに表示されます。

4. 次のようにして、CA の証明書失効リスト (CRL) を追加します。

a. 「証明書」ページの「CRL」エリアで、「追加」をクリックします。

b. CA の CRL の URL を入力します。

注

- 証明書失効リスト (CRL) は、失効したか有効ではない証明書シリアル番号のリストです。
- CA の CRL の URL は http または LDAP にすることができます。
- CRL 配布先の URL は CA ごとに異なりますが、CA 証明書の「CRL 配布点」拡張を参照して決めることができます。

---

5. 「テスト接続」をクリックして、URL を確認します。

6. 「保存」をクリックします。

7. jarsigner を使用して applets/ts1.jar に署名します。

注	詳細については、http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/jarsigner.html を参照してください。Identity Manager とともに提供されている ts1.jar ファイルは、自己署名付き証明書を使用して署名されているため、本稼働システムには使用しないでください。本稼働では、信頼できる CA によって発行されたコード署名証明書を使用して、このファイルを署名し直すことをお勧めします。

署名付き承認のためのクライアント側の設定

クライアント側の設定を有効にするには、次のようにします。

前提条件

クライアントシステムで、JRE 1.4 以上が動作する Web ブラウザが実行されている必要があります。

手順

証明書と非公開鍵を取得して、PKCS#12 キーストアにエクスポートします。

たとえば、Microsoft CA を使用している場合には、行う手順は次のようになります。

1. Internet Explorer を使用して、http://*IPAddress*/certsrv を参照し、管理特権でログインします。
2. 「証明書のリクエスト」を選択して、「次へ」をクリックします。
3. 「リクエストの詳細設定」を選択して、「次へ」をクリックします。
4. 「次へ」をクリックします。
5. 「証明書テンプレート」で「ユーザー」を選択します。
6. 次のオプションを選択します。
   a. エクスポート可能なキーとして指定する
   b. 秘密キーの強力な保護を有効にする
   c. ローカルコンピュータストアを使用する
7. 「送信」をクリックして、「OK」をクリックします。
8. 「この証明書のインストール」をクリックします。
9. 「ファイル名を指定して実行」—> mmc を実行して、mmc を起動します。
10. 証明書スナップインを追加します。

a. 「コンソール」—>「スナップインの追加と削除」を選択します。

b. 「追加 ...」をクリックします。

c. 「コンピュータアカウント」を選択します。

d. 「次へ」をクリックして、「完了」をクリックします。

e. 「閉じる」をクリックします。

f. 「OK」をクリックします。

g. 「証明書」—>「個人」—>「証明書」の順に進みます。

h. 「管理者」を右クリックして、「すべてのタスク」—>「エクスポート」を選択します。

i. 「次へ」をクリックします。

j. 「次へ」をクリックして、非公開鍵がエクスポートされていることを確認します。

k. 「次へ」をクリックします。

l. パスワードを設定して、「次へ」をクリックします。

m. ファイル *CertificateLocation*。

n. 「次へ」をクリックして、「完了」をクリックします。「OK」をクリックして確認します。

注 クライアント側の設定の手順 10l (パスワード) と 10m (証明書の場所) で使用した情報をメモしておいてください。この情報は、承認の署名のために必要です。

トランザクション署名の表示

次の手順を実行して、Identity Manager の監査ログレポートにトランザクション署名を表示します。

1. Identity Manager の管理インタフェースから、「レポート」を選択します。
2. 「レポートの実行」ページで、オプションの「新規 ... リストから「監査ログレポート」を選択します。
3. 「レポートタイトル」フィールドに、「承認」などのタイトルを入力します。
4. 「組織」選択エリアで、すべての組織を選択します。
5. 「アクション」オプションを選択して、「承認」を選択します。
6. 「保存」をクリックしてレポートを保存し、「レポートの実行」ページに戻ります。

7. 「実行」をクリックして、「承認」レポートを実行します。
8. 詳細リンクをクリックして、次に示すトランザクション署名情報を表示します。
   - 発行者
   - 主体
   - 証明書シリアル番号
   - 署名されたメッセージ
   - 署名
   - 署名アルゴリズム

第 6 章

データの同期と読み込み

この章では、Identity Manager でのデータの同期と読み込み機能の説明および手順を示します。データの同期ツール (検索、調整、および同期) と、これらのツールを使用してデータを最新に保つ方法について説明します。

- データ同期ツール : 最適なツールの選択
- 検索
- 調整
- ActiveSync アダプタ

データ同期ツール : 最適なツールの選択

Identity Manager データ同期ツールを選択してタスクを実行する場合は、次のガイドラインに従います。

表 6-1　データ同期ツールで使用するタスク

実行するタスク	使用する機能
読み込みの前に表示確認など行わずに、最初からリソースアカウントを Identity Manager に読み込ませる	リソースから読み込み
最初からリソースアカウントを Identity Manager に読み込ませる。オプションの作業として、読み込みの前にデータを表示および編集する	ファイルへ抽出、ファイルから読み込み
定期的にリソースアカウントを Identity Manager に読み込ませる。設定されたポリシーに従って各アカウントを操作する	リソースの調整
リソースアカウントの変更を Identity Manager に適用する、または読み込ませる	Active Sync アダプタを使用した同期 (複数リソースの実装)

検索

Identity Manager アカウント検索機能を使用すると、導入とアカウント作成タスクの速度が向上します。これらの機能には次のものがあります。

- **ファイルへ抽出** − リソースアダプタによって返されたリソースアカウントをファイル (CSV または XML 形式) に抽出します。データを Identity Manager にインポートする前に、このファイルを処理することができます。
- **ファイルから読み込み** − ファイル (CSV または XML 形式) のアカウントを読み取り、Identity Manager に読み込みます。
- **リソースから読み込み** − ほかの 2 つの検索機能を組み合わせたもので、リソースからアカウントを抽出し、それを Identity Manager に直接読み込みます。

これらのツールを使用して、新しい Identity Manager ユーザーを作成したり、リソースのアカウントを既存の Identity Manager ユーザーアカウントに相互に関連付けたりすることができます。

ファイルへ抽出

この機能は、リソースアカウントをリソースから XML または CSV テキストファイルに抽出するために使用します。これにより、抽出したデータを表示して変更したあとに、Identity Manager にインポートすることができます。

アカウントを抽出するには、次を実行します。

1. メニューバーで「アカウント」を選択し、「ファイルへ抽出」を選択します。
2. アカウントの抽出元となるリソースを選択します。
3. 出力のアカウント情報のファイル形式を選択します。データを XML ファイルまたはテキストファイルに抽出することができます。アカウント属性はカンマ区切り値 (CSV) 形式で表示されます。
4. 「ダウンロード」をクリックします。Identity Manager は「ファイルのダウンロード」ダイアログを表示し、そこで、抽出したファイルを保存するか表示するかを選択できます。

ファイルを開く場合は、そのファイルを表示するプログラムを選択しなければならない場合があります。

ファイルから読み込み

この機能は、リソースアカウント、つまり Identity Manager を通じてリソースから抽出されたリソースアカウントか、別のファイルソースから抽出されたリソースアカウントを Identity Manager に読み込むために使用します。Identity Manager のファイルへ抽出機能で作成されたファイルは XML 形式です。新しいユーザーのリストを読み込んだ場合、通常、データファイルは CSV 形式です。

CSV ファイル形式について

ほとんどの場合、読み込まれるアカウントはスプレッドシートにリストされ、値をカンマで区切った CSV 形式で保存されて、Identity Manager に読み込まれます。CSV ファイルの内容は、次のフォーマットガイドラインに従っている必要があります。

- **1 行目** − 各フィールドの列見出しまたはスキーマ属性を、カンマで区切ってリストします。
- **2 行目から最後まで** − 1 行目で定義した各属性の値を、カンマで区切ってリストします。フィールド値のデータが存在しない場合は、連続するカンマでそのフィールドを表します。

  たとえば、ファイルの最初の 3 行が次の図のファイルエントリのようになることがあります。

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID
,Department,Phone
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

図 6-1 データの読み込みに適切な形式の CSV ファイルの例

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Ph
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

この例では、2 番目のユーザーである Jane Doe には部署がありません。値がない場合は、連続するカンマ (,,) で表します。

注 読み込み操作中にアイデンティティー属性を適用する機能を有効にするには、「メタビュー」を使用し、「ファイルから読み込み」をアイデンティティー属性の有効なアプリケーションのリストに追加します。

有効にした場合、読み込み操作で次のオプションは表示されなくなります。

- 「ユーザーフォーム」
- 「属性の更新」
- 「属性値のマージ」

「アカウントの更新」オプションを選択した場合、すべてのアイデンティティー属性が完全に処理され、アカウントが再プロビジョニングされます。これを選択しない場合、読み込みファイルから取り込まれた属性のみが、アイデンティティーユーザーに対して処理されます。

アカウントをロードするには、次を実行します。

1. メニューバーで「アカウント」を選択し、「ファイルから読み込み」を選択します。

   Identity Manager は「ファイルから読み込み」ページを表示します。

   - **「ユーザーフォーム」** – 読み込み結果により Identity Manager ユーザーが作成される場合、ユーザーフォームは、ロール、リソース、およびその他の属性と同様に組織を割り当てます。各リソースアカウントに割り当てるユーザーフォームを選択してください。
   - **「アカウント相関規則」** – アカウント相関規則は、所有者のいない各リソースアカウントの所有者候補となる Identity Manager ユーザーを選択します。所有者のいないリソースアカウントの属性が与えられると、相関規則は、所有者候補のユーザーを選択するために使用される名前のリストまたは属性条件のリストを返します。所有者のいない各アカウントを所有している可能性のある Identity Manager ユーザーを検索するための規則を選択してください。
   - **「アカウント確認規則」** – アカウント確認規則は、相関規則が選択した所有者の候補から所有者でないものを除外します。ユーザーの完全なビューと所有されていないリソースアカウントの属性が与えられた場合、確認規則はユーザーがアカウントを所有していれば true を、そうでない場合は false を返します。リソースアカウントの各所有者候補をテストするための規則を選択します。「確認規則なし」を選択した場合、Identity Manager はすべての所有者候補を確認なしで受け入れます。

     注 お使いの環境で、相関規則が各アカウントに対して多くとも 1 つの所有者しか選択しない場合、確認規則は必要ありません。

- **「一致のみ読み込み」** – 既存の Identity Manager ユーザーと一致するアカウントのみを読み込むことを選択します。このオプションが選択されている場合、不一致のリソースアカウントはすべて読み込みから破棄されます。
- **「属性の更新」** – 現在の Identity Manager ユーザー属性値を、読み込まれたアカウントの属性値で置き換えることを選択します。
- **「属性値のマージ」** – その属性値が上書きではなく (重複を除いて) 結合されるような、1 つ以上の属性名をカンマで区切って入力します。このオプションは、グループやメーリングリストなどの、リストタイプの属性にのみ使用できます。また、「属性値の更新」オプションも選択する必要があります。
- **「結果レベル」** – 読み込みプロセスがアカウントの個々の結果を記録するしきい値を選択します。
  - **「エラーのみ」** – アカウントの読み込みでエラーメッセージが生成されたときにのみ個々の結果を記録します。
  - **「警告およびエラー」** – アカウントの読み込みで警告またはエラーメッセージが生成されたときに個々の結果を記録します。
  - **「情報以上」** – すべてのアカウントの個々の結果を記録します。これを選択すると、読み込みの速度が低下します。

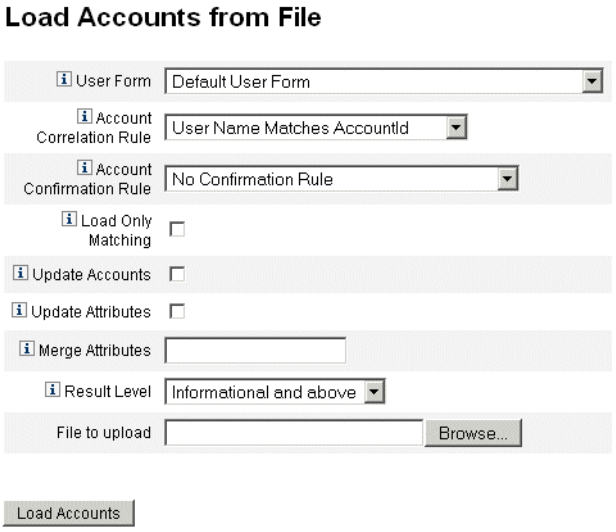
2. 「アップロードするファイル」フィールドで、読み込むファイルを指定して「アカウントの読み込み」をクリックします。

注

- 入力ファイルにユーザー列が含まれていない場合は、読み込みを正常に続行するために確認規則を選択する必要があります。
- 読み込みプロセスに関連付けられているタスクインスタンス名は、入力ファイル名に基づいています。そのため、ファイル名を再利用すると、最後の読み込みプロセスに関連付けられているタスクインスタンスによって以前のすべてのタスクインスタンスが上書きされます。

図 6-2 に、「ファイルから読み込み」画面で使用できるフィールドとオプションを示します。

図 6-2　ファイルから読み込み



アカウントが既存のユーザーと一致する (または相互に関連する) 場合、読み込みプロセスではアカウントがユーザーにマージされます。また、相互に関連しない入力アカウントから新しい Identity Manager ユーザーも作成されます (「相関は必須」が指定されていない場合)。

`bulkAction.maxParseErrors` 設定変数は、ファイルの読み込み時に発生するエラーの数の制限を設定します。デフォルトでは、エラー数の制限は 10 です。`maxParseErrors` の数のエラーが発生した場合、解析が停止します。

リソースから読み込み

この機能は、指定した読み込みオプションに従ってアカウントを Identity Manager に直接抽出してインポートするために使用します。

アカウントをインポートするには、メニューバーで「アカウント」を選択し、「リソースから読み込み」を選択します。

Identity Manager では、処理を続行する前に、読み込みオプションを指定できます。「リソースから読み込み」ページで利用可能な読み込みオプションと、その結果の操作は、「ファイルから読み込み」ページと同じです。

注 読み込み操作中にアイデンティティー属性を適用する機能を有効にするには、「リソースから読み込み」をアイデンティティー属性の有効なアプリケーションのリストに追加します。

有効にした場合、読み込み操作で次のオプションは表示されなくなります。

- 「ユーザーフォーム」
- 「属性の更新」
- 「属性値のマージ」

「アカウントの更新」オプションを選択した場合、すべてのアイデンティティー属性が完全に処理され、アカウントが再プロビジョニングされます。これを選択しない場合、リソースから取り込み、アイデンティティーユーザーに含める属性のみが処理されます。

調整

調整機能は、Identity Manager のリソースアカウントと実際にリソースに存在するアカウントの不整合をハイライト表示し、アカウントデータを定期的に相互に関連付けるために使用します。

調整は処理の進行中に比較するために設計されており、次の特徴があります。

- 検索プロセスよりも具体的なアカウント状況の診断と、より広範囲な応答のサポート
- スケジュール可能 (検索では不可能)
- 差分モードの提供 (検索では常に完全モード)
- ネイティブ変更の検出 (検索では不可能)

また、リソース処理の次の各時点で任意のワークフローを起動するように調整を設定できます。

- アカウントの調整前
- アカウントごと
- すべてのアカウントの調整後

Identity Manager 調整機能には、「リソース」エリアからアクセスします。リソースリストには、各リソースが最後に調整された日時および現在の調整ステータスが表示されます。

調整ポリシーについて

調整ポリシーを使用して、調整タスクごとに各リソースに対して一連の応答を設定できます。ポリシーでは、調整を実行するサーバーを選択し、どのような場合にどのような頻度で調整を実行するかを指定して、調整中に発生した各状況に対する応答を設定します。また、アカウント属性に対して (Identity Manager を経由せずに) ネイティブに行われた変更を検出するように調整を設定することもできます。

調整ポリシーの編集

調整ポリシーを編集するには、次の手順を実行します。

1. メニューバーで「リソース」を選択します。
2. 「リソース」リスト階層内のリソースを選択します。
3. 「リソースアクション」オプションリストから「調整ポリシーの編集」を選択します。

Identity Manager は「調整ポリシーの編集」ページを表示し、ここで、次のようなポリシーの項目を選択できます。

- **「調整サーバー」** – クラスタ環境では、各サーバーが調整を実行できます。ポリシーで、どの Identity Manager サーバーがリソースに対して調整を実行するのかを指定します。
- **「調整モード」** – 調整は、いくつかの異なるモードで実行でき、これにより品質を最適化できます。
  - **「完全調整」** – スピードを犠牲にして徹底的に最適化します。
  - **「差分調整」** – ある程度の妥協により速度を最適化します。

ポリシー内で、Identity Manager がリソースに対して調整を実行するモードを選択します。目的のリソースの調整を無効化する場合は、「調整しない」を選択します。

- **「完全調整スケジュール」** – 完全調整モードが有効になっている場合、調整は固定されたスケジュールで自動的に実行されます。ポリシー中で、完全調整がリソースに対してどのような頻度で実行されるかを指定します。より高いレベルのポリシーから指示されたスケジュールを継承する場合は、「継承」オプションを選択します。スケジュールまたはタスクスケジュール繰り返し規則を指定する場合は、「継承」オプションの選択を解除します。

- **「差分調整スケジュール」** – 差分調整モードが有効になっている場合、調整は固定されたスケジュールで自動的に実行されます。**「デフォルトポリシーを継承」**オプションを選択した場合、より高いレベルのポリシーからスケジュールは継承されます。ポリシーで差分調整がリソースに対してどのような頻度で実行されるかを指定する場合、またはタスクスケジュール繰り返し規則を選択する場合は、**「継承」**オプションの選択を解除します。

  注 差分調整をサポートしないリソースもあります。

- **「属性レベル調整」** – 調整は、アカウント属性に対してネイティブな (つまり、Identity Manager を介さない) 変更が加えられたことを検出するように設定できます。「調整アカウント属性」で、指定された属性へのネイティブな変更を検出するかどうかを指定します。
- **「アカウント相関規則」** – アカウント相関規則は、所有者のいない各リソースアカウントの所有者候補となる Identity Manager ユーザーを選択します。所有者のいないリソースアカウントの属性が与えられると、相関規則は、所有者候補のユーザーを選択するために使用される名前のリストまたは属性条件のリストを返します。所有者のいない各アカウントを所有している可能性のある Identity Manager ユーザーを検索するための規則を選択してください。
- **「アカウント確認規則」** – アカウント確認規則は、相関規則が選択した所有者の候補から所有者でないものを除外します。Identity Manager ユーザーの完全なビューと所有されていないリソースアカウントの属性が与えられた場合、確認規則はユーザーがアカウントを所有していれば true を、そうでない場合は false を返します。リソースアカウントの各所有者候補をテストするための規則を選択します。「確認規則なし」を選択した場合、Identity Manager はすべての所有者候補を確認なしで受け入れます。

  注 お使いの環境で、相関規則が各アカウントに対して多くとも 1 つの所有者しか選択しない場合、確認規則は必要ありません。

- **「プロキシ管理者」** – 調整応答の実行時に使用される管理者を指定します。調整では、指定されたプロキシ管理者が実行を許可されている操作のみを実行できます。応答は、(必要な場合) この管理者と関連付けられたユーザーフォームを使用します。

  「プロキシ管理者なし」オプションを選択することもできます。このオプションを選択した場合、調整の結果を表示できますが、応答の操作またはワークフローは実行されません。

- **「状況オプション」** (および「応答」) – 調整では、数種類の状況が認識されます。「応答」列で、調整が実行する操作を指定します。
  - 「CONFIRMED」 – 予想されるアカウントは存在します。
  - 「DELETED」 – 予想されるアカウントは存在しません。

- 「FOUND」 – 調整プロセスは、割り当てられたリソースに対して、一致するアカウントを発見しました。
- 「MISSING」 – ユーザーに割り当てられたリソースに一致するアカウントが存在しません。
- 「COLLISION」 – 2 人以上の Identity Manager ユーザーが、単一のリソースに対して同じアカウントを割り当てられています。
- 「UNASSIGNED」 – 調整プロセスは、このユーザーに割り当てられていないリソースに対して、一致するアカウントを発見しました。
- 「UNMATCHED」 – アカウントはどのユーザーとも一致しません。
- 「DISPUTED」 – アカウントは 1 人以上のユーザーと一致します。

次のいずれかの応答オプションを選択します (状況により、選択できるオプションは異なる)。

- **「リソースアカウントに基づく新規 Identity Manager ユーザーの作成」** – リソースアカウント属性に基づいてユーザーフォームが実行され、新規ユーザーが作成されます。リソースアカウントは、どのような変更が行われても更新されません。
- **「Identity Manager ユーザーのリソースアカウントの作成」** – ユーザーフォームを使用してリソースアカウント属性を再生成し、存在しないリソースアカウントを再作成します。
- **「リソースアカウントの削除」および「リソースアカウントの無効化」** – リソースのアカウントを削除 / 無効化します。
- **「Identity Manager ユーザーへリソースアカウントをリンク」および「Identity Manager ユーザーからリソースアカウントへのリンク解除」** – リソースアカウント割り当てをユーザーに追加するか、ユーザーから削除します。フォーム処理は実行されません。

- **「調整前ワークフロー」** – 調整は、リソースを調整する前にユーザー指定のワークフローを実行するように設定できます。調整が実行するワークフローを選択してください。どのワークフローも実行しない場合は、「ワークフローを実行しない」を選択してください。
- **「アカウント単位ワークフロー」** – 調整がリソースアカウントの状況に応答したあと、ユーザー指定のワークフローを実行するように設定できます。調整が実行するワークフローを選択してください。どのワークフローも実行しない場合は、「ワークフローを実行しない」を選択してください。
- **「調整後ワークフロー」** – リソースの調整が完了したあとに、ユーザー指定のワークフローを実行するように設定できます。調整が実行するワークフローを選択してください。どのワークフローも実行しない場合は、「ワークフローを実行しない」を選択してください。

ポリシーの変更を保存するには、「保存」をクリックしてください。

調整の開始

調整タスクを開始する場合は、次の 2 つのオプションが利用可能です。

- **調整のスケジュール** ― 「調整ポリシーの編集」ページで、調整スケジュールを設定できます。これにより、調整が定期的に実行されます。
- **即座に調整** ― 調整をただちに実行します。このためには、リソースリスト内のリソースを選択し、「リソースアクション」リストから次のオプションのどちらかを選択します。
  - ただちに完全調整
  - ただちに差分調整

調整は、ポリシーに設定されたパラメータに従って実行されます。定期的に調整を実行するようにポリシーを設定すると、指定どおりに調整が実行されます。

調整のキャンセル

調整をキャンセルするには、リソースを選択し、「リソースアクション」リストから「調整のキャンセル」を選択します。

調整ステータスの表示

リソースリストの「ステータス」列には、次のような調整ステータスの状態が表示されます。

- **「不明」**― ステータスは不明です。最後に実行された調整の結果はわかりません。
- **「無効」**― 調整は無効化されています。
- **「失敗」**― 直前の調整は正常に完了していません。
- **「成功」**― 直前の調整は正常に完了しています。
- **「エラーありで完了」**― 直前の調整は完了しましたが、エラーがありました。

注	ステータスの変更を確認するには、このページを更新する必要があります (情報は自動更新されない)。

リソースの各アカウントの詳細なステータス情報を表示できます。リスト内のリソースを選択し、「リソースアクション」リストから「調整ステータスの表示」を選択してください。

アカウントインデックスの操作

アカウントインデックスは、Identity Manager に認識される各リソースアカウントの最後の既知の状態を記録します。アカウントインデックスは主に調整によって保守されますが、ほかの Identity Manager 機能も、必要に応じてアカウントインデックスを更新します。

検索ツールはアカウントインデックスを更新しません。

アカウントインデックスの検索

アカウントインデックスを検索するには、「リソースアクション」リストから「アカウントインデックスの検索」を選択します。

検索タイプを選択してから、検索属性を入力または選択します。「検索」をクリックすると、検索条件と一致するアカウントを検索します。

- **リソースアカウント名** – このオプションを選択した場合は、「が次の文字列で始まる」、「が次の文字列を含む」、「が次の文字列と等しい」のいずれかの修飾子を選択してから、アカウント名の一部または全部を入力します。
- **検索対象リソース** – このオプションを選択した場合は、リストから 1 つ以上のリソースを選択して、指定したリソース上にある調整済みアカウントを検索します。
- **所有者** – このオプションを選択した場合は、「が次の文字列で始まる」、「が次の文字列を含む」、「が次の文字列と等しい」のいずれかの修飾子を選択してから、所有者名の一部または全部を入力します。所有者のいないアカウントを検索するには、UNMATCHED または DISPUTED 状況のアカウントを検索します。
- **調整状況** – このオプションを選択した場合、リストから 1 つ以上の状況を選択して、指定した状況と一致する調整済みアカウントを検索します。

「検索」をクリックすると、検索パラメータに従ってアカウントを検索します。検索結果の数を制限するために、「結果表示を次の件数に限定」フィールドに数を指定することもできます。デフォルトの制限数は、検出されたアカウントの最初から 1000 件目までです。

「クエリーのリセット」をクリックすると、ページがクリアされ、新たに選択を行えます。

アカウントインデックスの検査

すべての Identity Manager ユーザーアカウントを表示することができます。また、オプションとして、それらをユーザーベースで調整することができます。このためには、「リソース」を選択してから、「アカウントインデックスの検査」を選択します。

Identity Manager が認識するすべてのリソースアカウントが表形式で表示されます (Identity Manager ユーザーに所有されるアカウントかどうかに関係なく)。この情報は、リソース別、または Identity Manager の組織別にまとめられます。この表示を変更するには、「インデックス表示の変更」リストから選択を行います。

アカウントの操作

リソースのアカウントを操作するには、「リソースごとのグループ」インデックス表示を選択します。リソースタイプごとにフォルダが表示されます。フォルダを展開して特定のリソースに移動します。リソースの隣の + または - をクリックすると、Identity Manager が認識するリソースアカウントがすべて表示されます。

リソースに対する最後の調整後に、そのリソースに直接追加されたアカウントは、表示されません。

アカウントの現在の状況に応じて、いくつかの操作を実行できます。また、アカウントの詳細を表示したり、その 1 つのアカウントを調整したりすることを選択できます。

ユーザーの操作

Identity Manager ユーザーを操作するには、「ユーザーごとのグループ」インデックス表示を選択します。この表示では、「アカウントのリスト」ページのように、Identity Manager ユーザーおよび組織が階層構造で表示されます。Identity Manager で現在ユーザーに割り当てられているアカウントを表示するには、ユーザーに移動してユーザー名の隣のインジケータをクリックします。ユーザーのアカウントと、Identity Manager が認識するそのアカウントの現在のステータスがユーザー名の下に表示されます。

アカウントの現在の状況に応じて、いくつかの操作を実行できます。また、アカウントの詳細を表示したり、その 1 つのアカウントを調整したりすることを選択できます。

ActiveSync アダプタ

Identity Manager の ActiveSync 機能を使用すると、アイデンティティー情報の源泉として信頼性の高い外部リソース (アプリケーションやデータベースなど) に格納された情報を、Identity Manager のユーザーデータと同期させることができます。Identity Manager リソースに対して同期を設定することで、アイデンティティー情報の源泉として信頼性の高いリソースへの変更をリスニングまたはポールすることができます。

メタビューを使用するか、(適切なターゲットオブジェクトタイプに対して) リソース同期ポリシーの入力フォームを指定することにより、リソース属性変更の Identity Manager への伝達方法を設定することができます。

メタビューを使用してデータの更新方法を指定する場合、Active Sync アプリケーションで有効にするアイデンティティー属性を指定します。アイデンティティー属性の設定の詳細については、131 ページの「アイデンティティー属性およびイベントの設定」を参照してください。

同期の設定については、次の節を参照してください。

同期の設定

Identity Manager は、同期ポリシーを使用してリソースの同期を有効にします。同期を設定するには、「リソース」タブで同期を設定するリソースを選択したあと、「リソースアクション」リストから「同期ポリシーの編集」を選択します。

同期ポリシーの編集

「同期ポリシーの編集」ページの次のオプションを指定して同期を設定します。

- **「ターゲットオブジェクトタイプ」** – ポリシーを適用するユーザーのタイプとして、Identity Manager ユーザーまたは Service Provider Edition ユーザーのいずれかを選択します。

  注 これらのユーザーに対してデータの同期を有効にするには、サービスプロバイダ実装で同期ポリシー (オブジェクトタイプとして Service Provider Edition ユーザーを指定) を設定する必要があります。サービスプロバイダユーザーの詳細については、第 13 章「サービスプロバイダの管理」を参照してください。

- **「スケジューリングの設定」** – 起動方法とポーリングスケジュールを指定するには、このセクションを使用します。

起動タイプには、「手動」、「自動」、「フェイルオーバー付自動」、または「無効」を指定できます。

- **「自動」または「フェイルオーバー付自動」** – アイデンティティーシステムの起動時に、このソースも起動されます。
- **「手動」** – 管理者がこのソースを起動する必要があります。
- **「無効」** – リソースを無効にします。

いつポーリングを開始するかを指定するには、「開始日」および「開始時刻」オプションを使用します。間隔を選択し、その間隔の値を入力することにより、ポーリング周期を指定します (秒、分、時間、日、週、月)。

ポーリング開始日と時刻を将来の日時に設定すると、指定した日時にポーリングが開始します。ポーリング開始日と時刻を過去の日時に設定すると、Identity Manager はこの情報とポーリング間隔に基づいて、いつポーリングを開始するかを決定します。次に例を示します。

- リソースのアクティブな同期を 2005 年 7 月 18 日 (火曜) に設定
- リソースのポールを週単位で、開始日を 2005 年 7 月 4 日 (月曜)、時刻を午前 9 時に設定

この場合、リソースのポーリングは 2005 年 7 月 25 日 (次の月曜) に開始されます。

開始日または開始時刻を指定しない場合、ただちにリソースのポーリングが開始されます。この場合、アプリケーションサーバーを再起動するたびに、アクティブな同期を行うよう設定されたリソースすべてのポーリングが、ただちに開始されます。一般的には、開始日と開始時刻を設定します。

- **「同期サーバー」** – クラスタ環境では、各サーバーが同期を実行できます。いずれかのオプションを選択して、リソースの同期を実行するために使用するサーバーを指定します。
  - どこで同期が実行されてもかまわない場合は、**「使用可能なサーバーを任意に使用」**を選択します。同期開始時に使用可能なサーバーのうち 1 台のサーバーが選ばれます。
  - 同期の実行に waveset.properties で指定されているサーバーを使用する場合は、**「waveset.properties での設定を使用します」**を選択します (この機能は非推奨)。
  - 特定のサーバーを選択して同期を実行する場合は、**「指定されたサーバーを使用」**を選択し、「同期サーバー」リストから 1 台以上の使用可能なサーバーを選択します。
- **「リソース固有の設定」** – 同期で処理すべきリソースのデータを決定する方法を指定するには、このセクションを使用します。
- **「共通設定」** – データ同期アクティビティーの次の一般設定を指定します。

- **「プロキシ管理者」** – 更新を処理する管理者を選択します。すべての操作は、この管理者に割り当てられた機能を通して承認されます。ユーザーフォームが空のプロキシ管理者を選択する必要があります。
- **「入力フォーム」** – データ更新を処理する入力フォームを選択します。このオプション設定項目を使用すると、属性を変換してからアカウントに保存することができます。
- **「規則」** – データ同期プロセス中に使用する規則を指定できる次のオプションがあります。
  - **「処理規則」** – 対象となる各アカウントに対して実行する処理規則を指定するには、この規則を選択します。この選択は、ほかのすべての選択よりも優先されます。処理規則を指定した場合、このリソースに関するほかの設定に関係なく、すべての行に対して処理が実行されます。これは、プロセス名か、またはプロセス名として評価される規則です。
  - **「相関規則」** – リソースの調整ポリシーに指定されている相関規則に優先して適用される相関規則を選択します。相関規則は、リソースアカウントをアイデンティティーシステムアカウントに相互に関連付けます。
  - **「確認規則」** – リソースの調整ポリシーに指定されている確認規則に優先して適用される確認規則を選択します。
  - **「解決プロセス規則」** – データフィード内の複数のレコードと一致した場合に実行するタスク定義の名前を指定するには、この規則を選択します。これは、管理者に手動アクションを求めるプロセスである必要があります。これは、プロセス名か、またはプロセス名として評価される規則です。
  - **「削除規則」** – 削除操作を行うかどうかを決定するために、対象となるユーザー更新ごとに評価される、true または false を返す規則を選択します。

- **「一致しないアカウントの作成」** – このオプションを有効 (true) にすると、アダプタは Identity Manager システム上に存在しないアカウントの作成を試みます。有効にしない場合、アダプタは解決プロセス規則が返すプロセスを使用してアカウントを実行します。
- **「ログ設定」** – 次のログオプションの値を指定します。
  - **「ログアーカイブの最大数」** – 値が 0 (ゼロ) より大きい場合、最新の N 個のログファイルが保持されます。0 (ゼロ) の場合は 1 つのログファイルが繰り返し利用されます。-1 の場合、ログファイルは破棄されません。
  - **「アクティブログの最大有効期間」** – この期間を経過すると、アクティブログはアーカイブされます。期間が 0 (ゼロ) の場合、期間ベースのアーカイブは行われません。ログアーカイブの最大数が 0 (ゼロ) に設定されている場合、この期間が経過してもアーカイブは行われず、アクティブログは切り捨てられ、再使用されます。この有効期間条件は、「ログファイルの最大サイズ」に指定される条件とは別に評価されます。

    数値を入力し、次に時間の単位 (日、時間、分、月、秒、または週) を選択します。デフォルトの単位は日です。

- **「ログファイルパス」** – アクティブログとアーカイブされたログのファイルが作成されるディレクトリへのパスを入力します。ログファイル名はリソース名から開始します。
- **「ログファイルの最大サイズ」** – アクティブログファイルの最大サイズをバイト数で入力します。指定した最大サイズに達すると、アクティブログファイルはアーカイブされます。ログアーカイブの最大数が 0 (ゼロ) に設定されている場合、この期間が経過してもアーカイブは行われず、アクティブログは切り捨てられ、再使用されます。このサイズ条件は、「アクティブログの最大有効期間」に指定される条件とは別に評価されます。
- **「ログレベル」** – ログのレベルを入力します。
  - 0 – ログなし
  - 1 – エラー
  - 2 – 情報
  - 3 – 詳細
  - 4 – デバッグ

「保存」をクリックして、リソースのポリシー設定を保存します。

ActiveSync アダプタの編集

Active Sync アダプタを編集する前に、同期を停止します。「同期ポリシーの編集」ページで、Identity Manager ユーザーの「起動タイプ」として「無効」を選択します。サービスプロバイダユーザーの場合は、「同期の有効化」オプションの選択を解除します。アクティブな同期が無効にされたことを示す警告メッセージが表示されます。

リソースに対して同期を無効にすると、変更の保存時に同期タスクが停止されます。

ActiveSync アダプタのパフォーマンスのチューニング

同期はバックグラウンドタスクであるため、ActiveSync アダプタ設定によってはサーバーのパフォーマンスが影響を受ける可能性があります。次のタスクを実行して、ActiveSync アダプタのパフォーマンスをチューニングします。

- ポーリング間隔の変更
- アダプタを実行するホストの指定
- 開始と停止

- アダプタログ

ActiveSync アダプタは、リソースリストを通じて管理します。ActiveSync アダプタを選択し、「リソースアクション」リストの「同期」セクションから処理を制御する実行、停止、ステータス更新を利用してください。

ポーリング間隔の変更

ポーリング間隔は、ActiveSync アダプタが新しい情報の処理を開始する時期を決定します。ポーリング間隔は、実行するアクティビティーのタイプに基づいて決定する必要があります。たとえば、アダプタがデータベースから多数のユーザーのリストを読み込むたびに、Identity Manager の全ユーザーを更新する場合、この処理を毎日早朝に実行するとします。アダプタによっては処理する新しい項目を即座に検索するため、毎分実行するよう設定できるかもしれません。

アダプタを実行するホストの指定

アダプタを実行するホストを指定するには、`waveset.properties` ファイルを編集します。`sources.hosts` プロパティーを次のいずれかのオプションに編集します。

- `sources.hosts=`*`hostname1,hostname2,hostname3`* と設定します。これにより、ActiveSync アダプタを実行するマシンのホスト名がリストされます。アダプタは、このフィールドに最初にリストされた利用可能なホスト上で実行されます。

注 入力する *hostname* は、サーバーの Identity Manager リスト内のエントリと一致する必要があります。「設定」タブからサーバーのリストを表示します。

または

- `sources.hosts=localhost` と設定します。この設定では、アダプタは、そのリソースに対して ActiveSync を開始しようとする最初の Identity Manager サーバー上で実行します。

注 クラスタで特定のサーバーを指定する必要がある場合は、最初のオプションを使用する必要があります。

このプロパティー設定は、Identity Manager ユーザーの同期にのみ適用されます。サービスプロバイダユーザーの同期におけるホスト設定は、同期ポリシーによって決定されます。

メモリと CPU サイクルを多く必要とする ActiveSync アダプタは、専用のサーバー上で実行するように設定して、システムの負荷を分散することができます。

開始と停止

ActiveSync アダプタは、無効化したり、手動で開始したり、自動で開始したりすることができます。ActiveSync アダプタを起動または停止するには、ActiveSync リソースを変更できる適切な管理者機能が必要です。管理者機能の詳細については、167 ページの「機能のカテゴリ」を参照してください。

自動に設定すると、アプリケーションサーバーが再起動したときにアダプタが再起動されます。アダプタを開始すると、アダプタは指定したポーリング間隔で即座に実行します。アダプタを停止すると、アダプタは次回に停止フラグを検出したときに停止します。

アダプタログ

アダプタログは、現在処理中のアダプタの情報を取得します。ログが取得する詳細の量は、設定したログレベルに応じて異なります。アダプタログは、問題のデバッグとアダプタプロセスの進行状況の監視に役立ちます。

各アダプタには独自のログファイル、パス、およびログレベルがあります。適切なユーザータイプ (Identity Manager またはサービスプロバイダ) の同期ポリシーの「ログ」セクションでこれらの値を指定します。

アダプタログの削除

アダプタログは、アダプタが停止されたときにのみ削除しなければなりません。ほとんどの場合は、ログを削除する前に、ログをコピーしてアーカイブしておきます。

第 7 章

レポート

Identity Manager は、自動化されたシステムアクティビティーと手動によるシステムアクティビティーについてのレポートを作成します。一連の強力なレポート機能により、重要なアクセス情報や Identity Manager ユーザーに関する統計をいつでも取得して表示できます。

この章では、Identity Manager レポートタイプ、レポートの作成、実行、および電子メールによる送信の方法、レポート情報のダウンロード手順について説明します。

この章は、次の節で構成されています。

- レポートの操作
- レポートのタイプ
- リスク分析
- システムの監視
- ダッシュボードの操作

レポートの操作

Identity Manager では、レポートは特別なタスクカテゴリとみなされます。そのため、Identity Manager 管理者インタフェースの次の 2 つのエリアでレポートを操作します。

- **「レポート」**— レポートを定義、実行、削除、およびダウンロードできます。また、スケジュールされたレポートの管理もできます。
- **「タスク」**— レポートを定義したあとに、「タスク」エリアに移動して、レポートタスクをスケジュールおよび処理します。

レポート

レポート関連のアクティビティーのほとんどは、「レポートの実行」ページから実行できます。このページでは、次のレポートアクティビティーを実行できます。

- レポートの作成、修正、および削除
- レポートの実行
- StarOffice などの別のアプリケーションで使用するためのレポート情報のダウンロード

このページを表示するには、メニューバーから「レポート」を選択します。「レポートの実行」ページに使用可能なレポートのリストが表示されます。

デフォルトでは、次のレポートはログイン管理者が管理する組織セットに対して実行されます。ただし、レポートの実行対象となる組織を 1 つ以上選択した場合は、その選択が優先されます。

- 管理者ロールの概要
- 管理者概要
- ロールの概要
- ユーザー質問の概要
- ユーザー概要

図 7-1 は、「レポートの実行」ページの例を示します。

図 7-1 「レポートの実行」の選択項目

レポートの定義を開始するには、次のいずれかの方法を使用します。

- レポートを作成する。
- レポートを選択して修正し、新しい名前で保存する (レポートのクローン作成とも呼ばれる)。

レポートの作成

レポートを作成するには、次の手順に従います。

1. メニューバーで「レポート」を選択します。
2. レポートのカテゴリを「Identity Manager レポート」と「監査レポート」から選択し、「新規」オプションリストからレポートタイプを選択します。

Identity Manager の「レポートの定義」ページが表示されます。ここでオプションを選択して保存すると、レポートが作成されます。

レポートの複製

レポートを複製するには、リストからレポートを選択します。新しいレポート名を入力し、オプションの作業としてレポートパラメータを調整して「保存」をクリックします。レポートは新しい名前で保存されます。

電子メールによるレポートの送信

レポートを作成または編集するときには、レポートの結果を 1 人または複数の電子メール受信者に送信するオプションを選択できます。このオプションを選択すると、ページが更新され、電子メール受信者を指定するようにリクエストされます。アドレスをカンマで区切り、1 人以上の受信者を入力します。

電子メールに添付するレポートの形式を選択することもできます。

- **「CSV 形式のレポートの添付」** − カンマ区切り値 (CSV) 形式でレポートの結果を添付します。
- **「PDF 形式のレポートの添付」** − PDF (Portable Document Format) 形式でレポートの結果を添付します。

レポートの実行

レポートの条件を入力および選択したら、次を実行できます。

- 保存せずにレポートを実行する − 「実行」をクリックしてレポートを実行します。レポート (新しいレポートを定義した場合) または変更したレポートの条件 (既存のレポートを編集した場合) は保存されません。
- レポートを保存する − 「保存」をクリックしてレポートを保存します。保存後は、「レポートの実行」ページ (レポートのリスト) からこのレポートを実行できます。

レポートのスケジュール

レポートをただちに実行するのか、定期的に実行するようスケジュールするのかによって、選択は異なります。

- **「レポート」>「レポートの実行」** − 保存されたレポートをただちに実行できます。レポートのリストから「実行」をクリックします。Identity Manager によりレポートが実行され、結果が要約および詳細形式で表示されます。

- **「タスク」>「タスクのスケジュール」**－ 実行するレポートタスクをスケジュールします。レポートタスクの選択後、レポートの頻度とオプションを設定できます。また、レポートの特定の詳細を調整することもできます (「レポートの定義」ページの「レポート」エリアで)。

レポートデータのダウンロード

「レポートの実行」ページで、次のいずれかの行の「ダウンロード」をクリックします。

- **「CSV レポートのダウンロード」**－ レポートの出力を CSV 形式でダウンロードします。保存したら、StarOffice などの別のアプリケーションでレポートを開いて操作できます。
- **「PDF レポートのダウンロード」**－ Adobe Reader で表示できる PDF (Portable Document Format) 形式でレポート出力をダウンロードします。

図 7-2　　レポートのダウンロード

レポート出力のフォントの設定

PDF (Portable Document Format) で生成されるレポートについて、レポートで使用するフォントを決定するための選択を行うことができます。

レポートのフォント選択を設定するには、「レポート」をクリックして「設定」を選択します。次のオプションを選択できます。

- **PDF レポートオプション**
  - **「PDF フォント名」**－ PDF レポートを生成するときに使用するフォントを選択します。デフォルトでは、すべての PDF ビューアで使用可能なフォントだけが示されます。ただし、フォント定義ファイルを製品の fonts/ ディレクトリにコピーしてサーバーを再起動することにより、アジア言語をサポートするために必要なフォントなどの追加フォントをシステムに追加できます (手順の詳細については、リリースノートの「ID-10641/14376」の項目を参照)。

追加できるフォント定義形式には .ttf、.ttc、.otf、および .afm があります。これらのフォントのいずれかを選択する場合、レポートが表示されるコンピュータシステムでそのフォントが使用可能である必要があります。フォントが使用できない場合、代わりに「PDF ドキュメントにフォントを埋め込む」オプションを選択してください。

- **「PDF ドキュメントにフォントを埋め込む」** – 生成される PDF レポートにフォント定義を埋め込むには、このオプションを選択します。これにより、レポートがどの PDF ビューアでも表示できることが保証されます。

注 フォントを埋め込むと、ドキュメントのサイズが非常に大きくなる可能性があります。

- **「CSV レポートオプション」** – レポートを生成するときに使用する文字セットを選択します。

「保存」をクリックしてレポート設定オプションを保存します。

レポートのタイプ

Identity Manager では次の複数のレポートタイプが用意されています。

- 監査
- 監査ログ
- リアルタイム
- 概要
- システムログ
- 使用状況

これらのレポートは、次のレポートカテゴリの一方または両方からアクセスできます。

- Identity Manager レポート
- 監査レポート

監査

監査レポートは、監査ポリシーで定義された基準に基づいて、ユーザーのコンプライアンスを管理するための情報を提供します。監査ポリシーと監査レポートの詳細については、第 11 章「アイデンティティー監査」を参照してください。

Identity Manager では次の監査レポートが用意されています。

- アクセスレビューレポート
- 監査ポリシーのスキャン
- 監査ポリシーの概要レポート
- 監査属性レポート
- 監査ポリシー別違反履歴
- ユーザーアクセスレポート
- 組織別違反履歴
- リソース別違反履歴
- 違反の概要レポート
- 職務分掌レポート

監査レポートを定義するには、「レポートの実行」ページの「監査レポート」オプションを選択し、「監査レポート」のリストからレポートを選択します。監査レポートの詳細については、第 11 章「アイデンティティー監査」を参照してください。

監査ログ

監査レポートは、システム監査ログに取得されたイベントに基づいています。これらのレポートには、生成されたアカウント、承認されたリクエスト、失敗したアクセス試行、パスワードの変更とリセット、セルフプロビジョニングアクティビティー、ポリシー違反、およびサービスプロバイダ (エクストラネット) ユーザーなどについての情報が表示されます。

注　監査ログを実行する前に、取得する Identity Manager イベントのタイプを指定する必要があります。それには、メニューバーの「設定」を選択し、「監査」を選択します。グループごとに成功したイベントと失敗したイベントを記録するために、監査グループ名を 1 つ以上選択します。監査設定グループの設定の詳細については、147 ページの「監査グループおよび監査イベントの設定」を参照してください。

「レポートの実行」ページのレポートオプションのリストから選択することにより、監査ログレポートを実行することができます。このレポートは、Identity Manager レポートと監査レポートの両方のカテゴリから利用できます。

レポートパラメータを設定して保存したら、「レポートの実行」リストページからレポートを実行します。「実行」をクリックすると、保存した条件を満たすすべての結果を含んだレポートが作成されます。レポートには、イベントの発生日、実行された操作、および操作の結果が表示されます。

リアルタイム

リアルタイムレポートは、リソースを直接ポーリングしてリアルタイム情報をレポートします。リアルタイムレポートには次の情報が含まれます。

- **リソースグループ** − ユーザーメンバーシップを含むグループ属性の概要を表示します。
- **リソースステータス** − 各リソースに対して testConnection メソッドを実行することにより、1 つ以上の指定されたリソースの接続ステータスをテストします。
- **リソースユーザー** − ユーザーリソースアカウントとアカウント属性を一覧表示します。

リアルタイムレポートを定義するには、「レポートの実行」ページの「Identity Manager レポート」リストからいずれかのレポートオプションを選択します。

レポートパラメータを設定して保存したら、「レポートの実行」リストページからレポートを実行します。「実行」をクリックすると、保存した条件を満たすすべての結果を含んだレポートが作成されます。

概要レポート

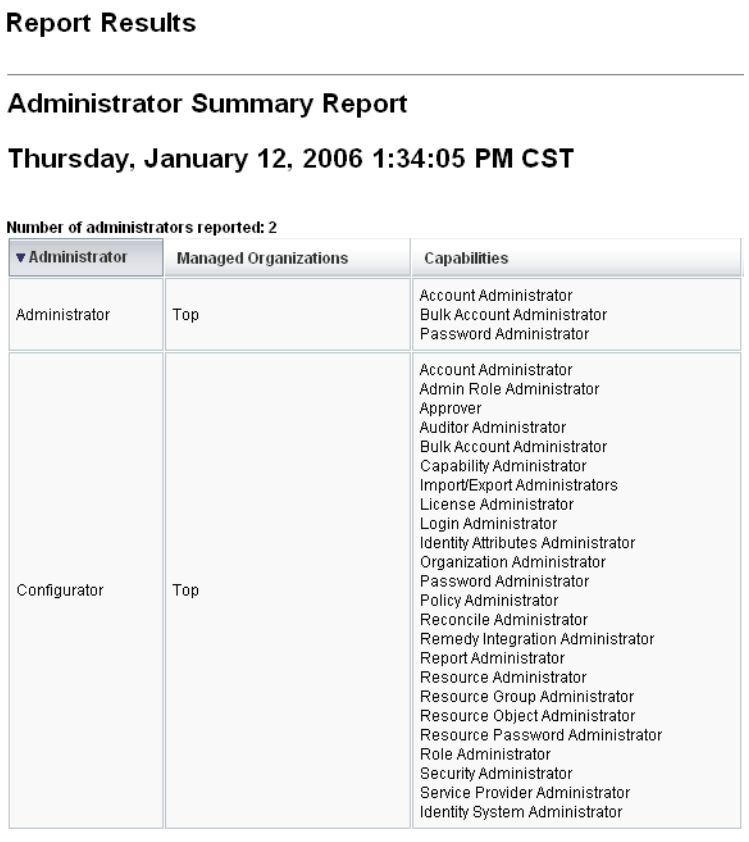
概要レポートタイプには、「Identity Manager レポート」リストから使用できる、次のレポートが含まれます。

- **アカウントインデックス** − 調整状況に従って選択したリソースアカウントについてレポートします。
- **管理者** − Identity Manager 管理者、管理者が管理する組織、および管理者に割り当てられている機能が表示されます。管理者レポートを定義するときには、レポートに含める管理者を組織によって選択できます。
- **管理者ロール** − 管理者ロールに割り当てられているユーザーを一覧表示します。
- **ロール** − Identity Manager ロールとそれに関連付けられたリソースが要約されます。ロールレポートを定義するときには、レポートに含めるロールを、関連付けられた組織によって選択できます。

- **タスク** – 保留中または終了済みのタスクをレポートします。含める情報の詳細さは、承認者、説明、有効期限、所有者、開始日、状態などの属性のリストから選択することによって決まります。
- **ユーザー** – ユーザー、ユーザーに割り当てられたロール、およびユーザーがアクセスできるリソースが表示されます。ユーザーレポートを定義するときには、レポートに含めるユーザーを名前、割り当てられた管理者、ロール、組織、またはリソース割り当てによって選択できます。
- **ユーザー質問** – アカウントポリシー要件で指定した秘密の質問の最小個数を回答していないユーザーを、管理者が検索できるようにします。結果には、ユーザー名、アカウントポリシー、ポリシーに関連付けられたインタフェース、および回答が必要な質問の最小個数が示されます。

次の図に示すように、管理者レポートには、Identity Manager 管理者、管理者が管理する組織、および管理者に割り当てられている機能と管理者ロールが一覧表示されます。

図 7-3　　管理者概要レポート



Report Results

Administrator Summary Report

Thursday, January 12, 2006 1:34:05 PM CST

Number of administrators reported: 2

▼Administrator	Managed Organizations	Capabilities
Administrator	Top	Account Administrator Bulk Account Administrator Password Administrator
Configurator	Top	Account Administrator Admin Role Administrator Approver Auditor Administrator Bulk Account Administrator Capability Administrator Import/Export Administrators License Administrator Login Administrator Identity Attributes Administrator Organization Administrator Password Administrator Policy Administrator Reconcile Administrator Remedy Integration Administrator Report Administrator Resource Administrator Resource Group Administrator Resource Object Administrator Resource Password Administrator Role Administrator Security Administrator Service Provider Administrator Identity System Administrator

システムログ

システムログレポートは、リポジトリに記録されるシステムメッセージおよびエラーを示します。このレポートを設定するとき、次の情報を含めるか除外するかを指定できます。

- システムコンポーネント (プロビジョニングツール、スケジューラ、サーバーなど)
- エラーコード
- 重要度レベル (エラー、致命的、または警告)

表示するレコードの最大数 (デフォルトは 3000) や、表示可能なレコード数が指定された最大値を超えた場合に古いレコードと新しいレコードのどちらを優先して表示するかも設定できます。

システムログレポートを実行する場合、ターゲットエントリの Syslog ID を指定することにより、特定の Syslog エントリを取得することができます。たとえば、「Recent Systems Messages」レポートの特定のエントリを表示するには、レポートを編集し、「イベント」フィールドを選択してから、リクエストされる Syslog ID を入力して「実行」をクリックします。

注 `lh syslog` コマンドを実行して、システムログからレコードを抽出することもできます。コマンドオプションの詳細については、付録 A 「lh リファレンス」の「syslog コマンド」を参照してください。

システムログレポートを定義するには、「レポートの実行」ページのレポートオプションのリストから「システムログレポート」を選択します。

使用状況レポート

使用状況レポートを作成して実行すると、管理者、ユーザー、ロール、またはリソースなどの Identity Manager オブジェクトに関連するシステムイベントの要約をグラフ形式または表形式で表示できます。出力を円グラフ、棒グラフ、または表形式で表示することができます。

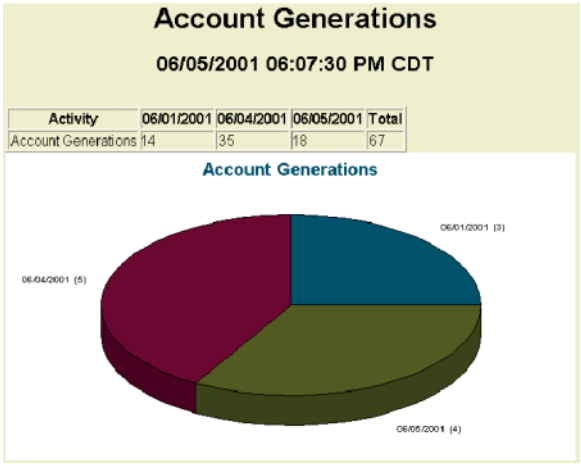
使用状況レポートを定義するには、「レポートの実行」リストページのレポートオプションのリストから「使用状況レポート」を選択します。

レポートパラメータを設定して保存したら、「レポートの実行」リストページからレポートを実行します。

使用状況レポートのグラフ

次の図では、最上部の表にレポートを構成するイベントが表示されます。その下にあるグラフは、この表の情報をグラフ化したものです。マウスポインタをグラフの各部に移動すると、その部分の値が表示されます。

図 7-4　　使用状況レポート (生成されたユーザーアカウント)



円グラフの一部をハイライト表示処理することができます。データスライスの一部を右クリックしたまま、ほかのデータスライスから離れて見えるように中央からドラッグします。この処理は、グラフ内の複数の部分で実行できます。ほとんどの管理の場合、スライスの中央に近い部分をクリックすると、ほかのスライスとの間隔がさらに広くなるようドラッグすることができます。

表示したい方向に円グラフを回転させることもできます。グラフの端の部分をクリックしたまま、表示したい方向へマウスを右または左に移動して回転します。

リスク分析

Identity Manager リスク分析機能を使用すると、プロファイルが特定のセキュリティー制限の外部にあるユーザーアカウントについてレポートを作成できます。リスク分析レポートは、物理的なリソースをスキャンしてデータを収集し、無効化されたアカウント、ロックされたアカウント、および所有者のいないアカウントについての詳細をリソースごとに表示します。また、リスク分析では期限切れパスワードについての詳細も表示されます。レポートの詳細は、リソースタイプによって異なります。

注 標準のレポートは、AIX、HP、Solaris、NetWare NDS、Windows NT、および Windows Active Directory リソースに対して実行可能です。

リスク分析ページは、フォームによって制御され、環境に合わせて設定できます。フォームのリストは、`idm¥debug` ページの RiskReportTask オブジェクトの下に表示され、Business Process Editor を使って修正できます。Identity Manager フォームの設定の詳細については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

リスク分析レポートを作成するには、メニューバーの「リスク分析」をクリックして、オプションの「新規」リストからレポートを選択します。

選択したリソースをスキャンするようにレポートを制限できます。また、リソースタイプによっては、次のアカウントをスキャンすることができます。

- 無効化されているか、期限が切れているか、非アクティブか、ロックされている
- まったく使用されたことがない
- フルネームまたはパスワードがない
- パスワードを必要としない
- パスワードの期限が切れているか、指定された日数の間変更されていない

定義したあとは、リスク分析レポートを指定した間隔で実行するようにスケジュールすることができます。

1. 「タスクのスケジュール」をクリックして、実行するレポートを選択します。
2. 「タスクスケジュールの作成」ページで、名前とスケジュール情報を入力し、オプションの作業としてその他のリスク分析の選択を調整します。
3. 「保存」をクリックして、スケジュールを保存します。

システムの監視

ダッシュボードグラフにイベントを表示してリアルタイムに追跡および監視するように Identity Manager をセットアップできます。ダッシュボードを使用することで、システムリソースをすばやく検査して異常を発見し、日付、曜日などに基づいた履歴上のパフォーマンス傾向を把握し、監査ログを見る前に問題を対話的に特定することができます。これらには監査ログほど多くの詳細は含まれませんが、問題を特定するためにログのどこを見ればよいかについてのヒントが得られます。

自動化されたアクティビティーと手動によるアクティビティーを高レベルで追跡する、グラフィカルなダッシュボード表示を作成することができます。Identity Manager は、サンプルのリソース操作ダッシュボードグラフを用意しています。リソース操作ダッシュボードグラフを使用することにより、システムリソースをすばやく監視し、許容レベルのサービスを維持できるようになります。

リソース操作ダッシュボードのこれらのグラフにはサンプルデータを表示できます。ダッシュボードの使用の詳細については、246 ページの「ダッシュボードの操作」を参照してください。

統計はさまざまなレベルで収集および集約され、指定内容に基づいたリアルタイムビューが提示されます。

追跡イベント設定

「レポートの設定」ページの「追跡イベント設定」エリアから、追跡イベントの統計収集が現在有効かどうかを判定したり、有効にしたりできます。追跡イベント設定を有効にするには、「イベント収集の有効化」をクリックします。

イベント収集の次のオプションを指定します。

- **「タイムゾーン」** – 追跡イベントの記録に使用するタイムゾーンを設定します。これは主に日付の境界を決定します。

  または、タイムゾーンを、サーバーに設定されているデフォルトタイムゾーンに設定できます。

- **「収集するタイムスケール」** – データ収集の時間間隔 (つまり、データを収集し保管する間隔) を指定します。たとえば、間隔が 1 分に選択された場合、データは毎分収集され保管されます。

システムは追跡されたイベントデータを格納し、期間を変更しながらシステムの詳細かつ最新の概覧を表示し、履歴上での傾向を把握できるようにします。

次のタイムスケールを使用できます。デフォルトではすべてが選択されています。収集しない間隔に対する選択は解除してください。

- 10 秒間隔

- 1 分間隔
- 1 時間間隔
- 1 日間隔
- 1 週間間隔
- 1 か月間隔

追跡イベントを設定したあと、ダッシュボードを使用して追跡イベントを監視します。

グラフの操作

グラフに関する次のアクティビティーを実行することができます。

- 定義済みのグラフの表示
- グラフの作成
- グラフの編集
- グラフの削除

定義済みのグラフの表示

Identity Manager は、いくつかのサンプルグラフを用意しています。サンプルデータを使用するものとしないものがあります。それぞれの配備に適したグラフを追加作成することをお勧めします。

配備を本稼働に移行する前に、サンプルグラフとサンプルダッシュボードを削除してください。サンプルデータを使用しないサンプルグラフの一部は、該当データが収集されていない場合に空白として表示される可能性があります。

1. メニューバーで「レポート」をクリックします。
2. 「ダッシュボードグラフ」をクリックします。
3. 「ダッシュボードグラフの種類の選択」オプションリストから、ダッシュボードグラフのカテゴリを選択します。

   選択されたカテゴリのすべてのグラフがグラフリストに表示されます。
4. グラフ名をクリックします。
5. 必要に応じて、「更新を一時停止」をクリックしてダッシュボードの更新を一時停止します。表示を更新するには、「再開」をクリックします。

注	多数のグラフを含むダッシュボードでは、すべてのグラフが最初に読み込まれるまで更新を停止するとよい場合があります。

6. 必要に応じて、「今すぐ更新」をクリックして即座に更新を適用します。
7. 「ダッシュボードグラフ」リストページに戻るには、**「完了」**をクリックします。

注	エラーメッセージがいずれかのグラフで表示される場合、デバッグページを使用して「システム設定」設定オブジェクトに `dashboard.debug=true` を設定します。このプロパティーを設定したら、エラーを生成したグラフに戻り、「問題をレポートする場合は、このテキストスクリプトを含めてください。」リンクを使用してグラフスクリプトを取得します。問題をレポートする場合は、このグラフスクリプトを含めてください。

グラフの作成

ダッシュボードグラフを作成するには、次の手順に従います。

1. メニューバーで**「レポート」**を選択します。
2. **「ダッシュボードグラフ」**を選択します。
3. 「ダッシュボードグラフの種類の選択」オプションリストから、ダッシュボードグラフのカテゴリを選択します。

   選択されたカテゴリのすべてのグラフがグラフリストに表示されます。
4. **「新規」**をクリックすると、「ダッシュボードグラフの作成」ページが表示されます。
5. **グラフ名**を入力します。グラフは名前でダッシュボードに追加されるため、一意のわかりやすい名前を選択します。
6. **レジストリ**を選択します (IDM または SAMPLE)。

   サンプルデータオプションは、システムをはじめて利用する管理者のために用意されています。追跡するすべてのイベントでサンプルデータが利用できるとは限らないため、この選択はデモンストレーションやさまざまなグラフオプションを指定した実験に最適です。本稼働環境への移行前にサンプルデータは削除してください。

注	サンプルデータを使用した追跡イベントセットは、実際に追跡されるイベントとは異なります。

7. リストから「追跡するイベント」の適切なタイプを選択します。

   イベントは、メモリー使用状況などのシステムの特性、または履歴値が追跡され、グラフまたはチャートで視覚的に表示されるリソース操作などのイベントの集まりです。

   IDM レジストリの追跡イベントは、次のとおりです。

   - **プロビジョニングツールの実行回数** − プロビジョニングツール操作の実行回数を追跡します (操作タイプごと)。
   - **プロビジョニングツールの実行時間** − 各プロビジョニングツール操作の実行時間を追跡します (操作タイプごと)。
   - **リソース操作の回数** − リソース操作の回数を追跡します。
   - **リソース操作期間** − リソース操作の期間を追跡します。
   - **ワークフロー時間** − ワークフローの実行時間を追跡します。
   - **ワークフロー実行回数** − 各ワークフローの実行回数を追跡します。

8. リストからタイムスケールを選択します。

   これは、データ収集の間隔 (1 時間など)、収集データの保管期間 (1 か月など) を制御します。システムは追跡されたイベントデータを保存し、期間を変更しながらシステムの詳細かつ最新の概覧を表示し、履歴上での傾向を把握できるようにします。

9. リストから測定基準を選択します。選択している追跡イベントに応じて、デフォルトの測定基準 (カウントまたは平均) が選択されます。

   グラフごとに測定基準が 1 つ表示されます。使用できる測定基準は、選択した追跡イベントにより異なります。可能な測定基準は次のとおりです。

   - カウント − 期間内に発生したイベントの合計回数
   - 平均 − 期間中のイベント値の算術平均
   - 最大 − 期間中のイベントの最大値
   - 最小 − 期間中のイベントの最小値
   - ヒストグラム − 期間中の各範囲のイベント値に対する個別のカウント

10. リストから「カウントの表示様式」を選択します。

    グラフカウントは、生の合計値として、またはさまざまなタイムスケールによってスケールされた値として表示されます。

11. リストからグラフの種類を選択します。

    これは、追跡されたイベントデータの表示様式を制御します。使用可能なグラフの種類は、選択した追跡イベントにより異なり、線グラフ、棒グラフ、円グラフなどがあります。

ベース次元

12. 必要に応じ、リストから次を選択します。
    - **「リソース名」**。選択した場合、すべての次元値がグラフで使用されます。個々の次元の値をグラフに含める場合は、このオプションの選択を解除します。
    - **「サーバーインスタンス」**。選択した場合、すべての次元値がグラフで使用されます。個々の次元の値をグラフに含める場合は、このオプションの選択を解除します。
    - **「操作のタイプ」**。選択した場合、すべての次元値がグラフで使用されます。個々の次元の値をグラフに含める場合は、このオプションの選択を解除します。

    次元を選択すると、ページが更新されグラフが表示されます。

グラフオプション

13. 必要に応じ、グラフのサブタイトルを入力します。

    これにより、グラフのメインタイトルの下にサブタイトルが生成されます。

詳細なグラフオプション

14. 必要に応じ、「詳細なグラフオプション」を選択します。次を設定したい場合に選択します。
    - **グリッドライン**
    - **フォント**
    - **カラーパレット**
15. グラフを作成するには、「保存」をクリックします。

グラフの編集

グラフを編集するには、**「レポート」**タブを選択し、「ダッシュボードグラフの種類の選択」オプションリストからダッシュボードグラフのカテゴリを選択し、リストからグラフ名を選択します。

選択したグラフにより、編集できるグラフ属性は異なります。次の 1 つ以上の特性を編集に使用できます。

- **グラフ名** − グラフは名前でダッシュボードに追加されます。
- **レジストリ** − レジストリに定義される追跡されたイベントの説明を指定します。現在は SAMPLE、SPE (サービスプロバイダ)、および IDM が選択されています。
- **追跡するイベント** − メモリ使用状況などのシステムの特性、または履歴値が追跡され、グラフまたはチャートで視覚的に表示されるリソース操作などのイベントの集まりです。

- **タイムスケール** – データ収集の間隔および収集データの保管期間を制御します。
- **測定基準** – グラフごとに測定基準が 1 つ表示されます。使用できる測定基準は、選択した追跡イベントにより異なります。選択した測定基準によってその他のオプションが使用できることもあります。
- **グラフの種類** – 追跡されたイベントの表示様式を制御します (線グラフ、棒グラフなど)。
- **次元値を含める** – 選択した場合、すべての次元値がグラフで使用されます。
- **グラフのサブタイトル** – 必要に応じて、グラフのメインタイトルの下にサブタイトルを入力します。
- **詳細なグラフオプション** – 次を設定したい場合に選択します。
  - **グリッドライン**
  - **フォント**
  - **カラーパレット**

16. **「保存」**をクリックします。

グラフの削除

グラフを削除するには、リストからグラフを選択し、**「削除」**をクリックします。

注	グラフを削除した場合、警告なしに、そのグラフを含むすべてのダッシュボードからグラフが自動的に削除されます。

ダッシュボードの操作

ダッシュボードは、1 つのページ上に表示される関連グラフの集まりです。グラフと同様、Identity Manager にはサンプルダッシュボードセットが用意されており、それぞれの配備に合わせてこれらをカスタマイズすることをお勧めします。手順については、247 ページの「ダッシュボードの作成」を参照してください。

「レポート」メニューの次のエリアで、ダッシュボードを操作することができます。

Identity Manager インタフェースの「レポート」エリアから、既存のダッシュボードを表示することができます。現在定義済みのダッシュボードを一覧表示するには、「ダッシュボードの表示」>「ダッシュボードグラフ」をクリックしてから、表示したいダッシュボードの横の「表示」をクリックします。

注	多数のグラフを含むダッシュボードでは、すべてのグラフが最初に読み込まれるまで更新を停止することが役立つ場合があります。 ダッシュボードの更新を停止するには、「更新を一時停止」をクリックし、表示を更新するには、「今すぐ更新」をクリックします。

続く節では、ダッシュボードの操作手順について説明します。

- ダッシュボードの作成
- ダッシュボードの編集
- ダッシュボードの削除

ダッシュボードの作成

ダッシュボードを作成するには、次の手順に従います。

1. メニューバーで「レポート」をクリックします。
2. 「ダッシュボードの表示」をクリックします。
3. 「新規」をクリックします。
4. 新しいダッシュボードの名前を入力します。
5. 新しいダッシュボードを説明する概要を入力します。
6. リストから、秒、分、時間単位の更新レートを選択します。

注	30 秒未満の更新レートを設定した場合、複数のグラフを含むダッシュボードで問題が発生する可能性があります。

7. ダッシュボードにグラフスタイルを関連付けるには、リストから適切なエントリを選択します。

注	1 つのグラフを複数のダッシュボードで使用することができます。

8. ダッシュボードグラフを削除するには、リストから適切なエントリを選択し、**「グラフの削除」**をクリックします。
9. **「保存」**をクリックします。

ダッシュボードの編集

ダッシュボードを編集するには、「ダッシュボードの作成」で説明した手順に従います。ただし、「新規」を選択する代わりに、修正するダッシュボードを選択し、次の属性を編集します。

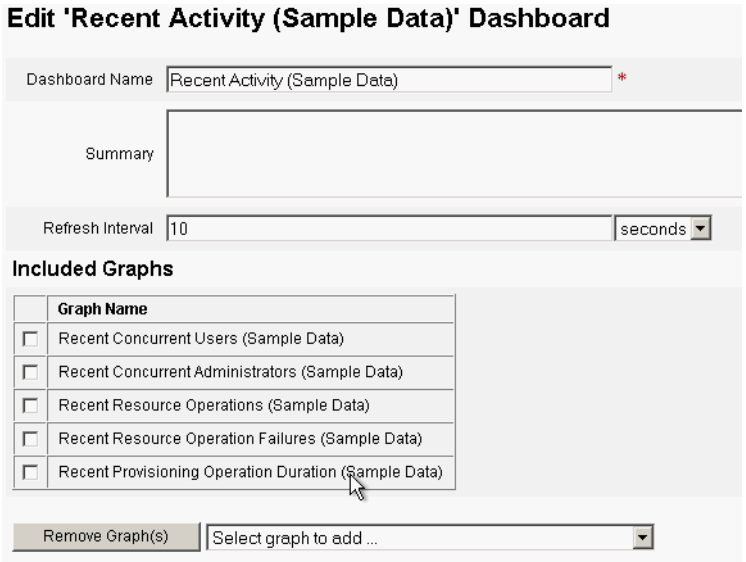
- ダッシュボードの名前。
- 新しいダッシュボードを説明する概要。
- リストからの、秒、分、時間単位の更新レート。
- ダッシュボードに関連付けられたグラフの追加または削除。

注 ダッシュボードからグラフを削除してもグラフは削除されません。そのグラフは、ほかのダッシュボードで引き続き使用可能です。

1 つのグラフを複数のダッシュボードで使用することができます。

図 7-5 に、ダッシュボード編集ページの例を示します。

図 7-5 ダッシュボードの編集



ダッシュボードの削除

サービスプロバイダダッシュボードを削除するには、「サービスプロバイダ」エリアから「ダッシュボードの管理」をクリックし、適切なダッシュボードを選択してから「削除」をクリックします。

注 ダッシュボードに含まれるグラフは、この手順では削除されません。「ダッシュボードグラフの管理」ページを使用してグラフを削除してください (「グラフの削除」を参照)。

トランザクションの検索

トランザクションは、新しいユーザーの作成や新しいリソースの割り当てなど、単一のプロビジョニング操作をカプセル化します。リソースを使用できないときにこれらのトランザクションを終了させるため、トランザクションがトランザクション持続ストアに書き込まれます。

注 「トランザクション設定の編集」ページを使用すると (「トランザクション管理」を参照)、管理者はいつトランザクションを保管するかを制御できます。たとえば、トランザクションをただちに保管できます (最初の試行前であっても)。

「トランザクションの検索」ページを使用すると、トランザクション持続ストア内のトランザクションを検索することができます。ここには、すでに完了しているトランザクションとともに再試行中のトランザクションが含まれます。完了していないトランザクションは、それ以上試行されないようにキャンセルできます。

トランザクションを検索するには、次を実行します。

1. Identity Manager にログインします。
2. メニューバーの「サービスプロバイダ」をクリックします。
3. 「トランザクションの検索」をクリックします。

   「検索条件」ページが表示されます。

注 検索では、下で選択したすべての条件に一致するトランザクションのみが返されます。これは、「アカウント」>「ユーザーの検索」ページと類似しています。

4. 必要に応じ、「ユーザー名」を選択します。

入力した **accountId** を持つユーザーのみに適用されるトランザクションを検索できます。

注	Service Provider Edition トランザクション設定ページで「照会可能なユーザー属性のカスタマイズ」を設定している場合は、それらがここに表示されます。たとえば、照会可能なユーザー属性のカスタマイズとして姓またはフルネームが設定されている場合、これらに基づいて検索することを選択できます。

5. 必要に応じて、「タイプ」の検索を選択します。

   選択したタイプのトランザクションを検索できます。

6. 必要に応じて、「状態」の検索を選択します。

   選択した次の状態のトランザクションを検索できます。

   - 「未試行」トランザクションは、まだ試行されていません。
   - 「再試行保留中」トランザクションは、1 回以上試行されましたが、1 つ以上のエラーが見つかり、個々のリソースに設定された再試行制限まで再試行がスケジュールされています。
   - 「成功」トランザクションは、正常に完了しました。
   - 「失敗」トランザクションは、1 つ以上失敗して完了しました。

7. 必要に応じ、「試行」での検索を選択します。

   試行された回数に基づいて、トランザクションを検索できます。失敗したトランザクションは、個々のリソースに設定された再試行制限まで再試行されます。

8. 必要に応じ、「送信時間」での検索を選択します。

   時間、分、日の単位でトランザクションが最初に送信された時間に基づいて、トランザクションを検索できます。

9. 必要に応じ、「終了時間」での検索を選択します。

   時間、分、日の単位でトランザクションが完了した時間に基づいて、トランザクションを検索できます。

10. 必要に応じ、「キャンセルステータス」での検索を選択します。

    トランザクションがキャンセルされているかどうかに基づいて、トランザクションを検索できます。

11. 必要に応じ、「トランザクション ID」での検索を選択します。

    一意のトランザクション ID に基づいてトランザクションを検索できます。このオプションを使用すると、入力した ID 値に基づいてトランザクションが検索されます。この ID は、すべての監査ログレコードに表示されます。

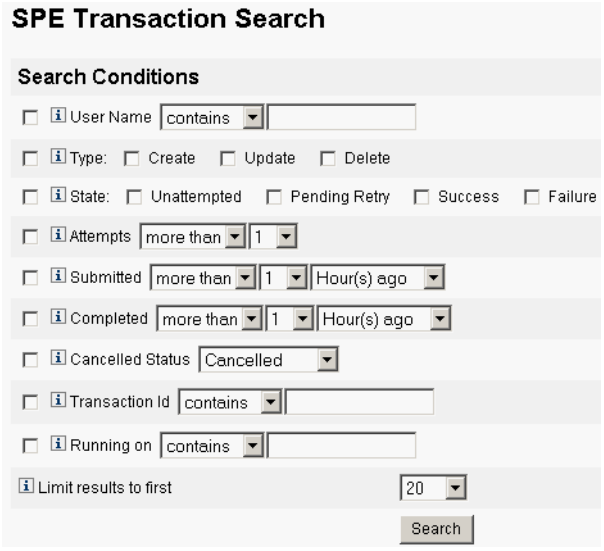
12. 必要に応じ、「SPE サーバー名」での検索を選択します。

    実行中の Service Provider Edition サーバーに基づいてトランザクションを検索できます。サーバーの ID は、`Waveset.properties` ファイルで上書きされている場合を除き、マシン名に基づきます。

13. 検索結果をリストから選択したエントリ数までに制限します。

    指定された制限までの結果のみ返されます。制限数以上の結果が存在するかどうかについては示されません。

図 7-6　　トランザクションの検索



14. 「検索」をクリックします。

    検索結果が表示されます。

15. 必要に応じ、結果ページの最下部にある「一致したすべてのトランザクションをダウンロードします」をクリックします。結果は XML 形式のファイルに保存されます。

注　　検索結果に返されたトランザクションをキャンセルすることができます。結果テーブルのトランザクションを選択し、「選択内容のキャンセル」をクリックします。完了している、またはすでにキャンセルされているトランザクションはキャンセルできません。

第 8 章

タスクテンプレート

Identity Manager のタスクテンプレートを使用すると、カスタマイズしたワークフローを記述する代わりに、管理者インタフェースを使用して特定のワークフローの動作を設定することができます。

この章では以下のトピックで、タスクテンプレートをシステムで使用できるようにする方法と、タスクテンプレートを使用してワークフローの動作を設定する方法について説明します。

- タスクテンプレートの有効化
- タスクテンプレートの設定

タスクテンプレートの有効化

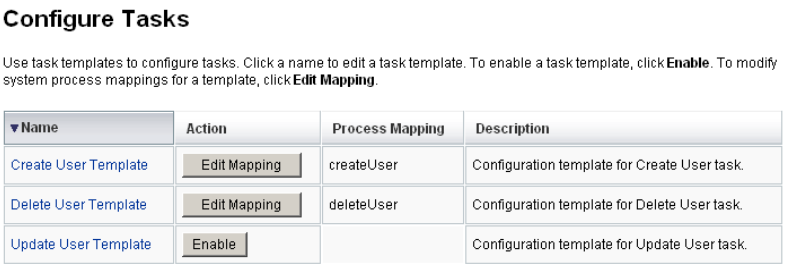
Identity Manager には、ユーザーによる設定が可能な次のタスクテンプレートが用意されています。

- **ユーザー作成テンプレート** – ユーザー作成タスクのプロパティーを設定します。
- **ユーザー削除テンプレート** – ユーザー削除タスクのプロパティーを設定します。
- **ユーザー更新テンプレート** – ユーザー更新タスクのプロパティーを設定します。

タスクテンプレートを使用する前に、タスクテンプレートのプロセスをマップする必要があります。プロセスタイプをマップするには、次の手順に従います。

1. Identity Manager 管理者インタフェースから「タスク」を選択し、「タスクの設定」を選択します。図 8-1 に「タスクの設定」ページを示します。

図 8-1　タスクの設定



「タスクの設定」ページには、次の列を持つテーブルがあります。

- **「名前」** – ユーザー作成、ユーザー削除、およびユーザー更新の各テンプレートへのリンクがあります。
- **「アクション」** – 次のいずれかのボタンがあります。
  - **「有効化」** – テンプレートをまだ有効にしていない場合に表示されます。
  - **「マッピングの編集」** – テンプレートを有効にしたあとで表示されます。

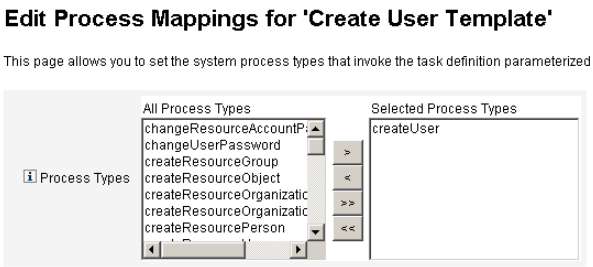
プロセスマッピングを有効化する手順と編集する手順は同じです。

- **「プロセスマッピング」** – 各テンプレートにマップされたプロセスタイプが一覧表示されます。
- **「説明」** – 各テンプレートの簡単な説明です。

2. **「有効化」**をクリックして、テンプレートのプロセスマッピングの編集ページを開きます。

   たとえば、ユーザー作成テンプレートに対して次のページ (図 8-2) が表示されます。

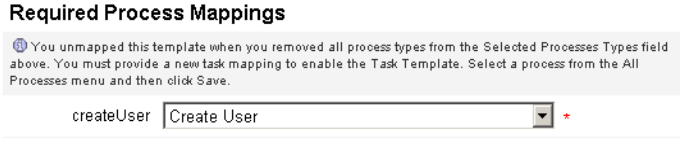
図 8-2　プロセスマッピングの編集ページ



注 「選択したプロセスタイプ」リストには、デフォルトのプロセスタイプ (この場合 `createUser`) が自動的に表示されます。必要に応じて、メニューから別のプロセスタイプを選択できます。

- 一般に、各テンプレートに複数のプロセスタイプをマップすることはありません。
- 「選択したプロセスタイプ」リストからプロセスタイプを削除し、代わりのプロセスタイプを選択しない場合、「必須のプロセスマッピング」セクションに、新しいタスクマッピングを選択するように指示が表示されます。

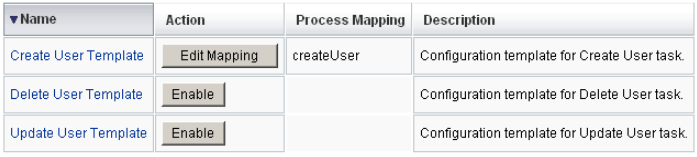
図 8-3 「必須のプロセスマッピング」セクション



3. 「保存」をクリックして、選択したプロセスタイプをマップし、「タスクの設定」ページに戻ります。

注 「タスクの設定」ページが再表示されると、「有効化」ボタンが「マッピングの編集」ボタンに変化し、「プロセスマッピング」列にプロセス名が表示されます。

図 8-4 更新された「タスクの編集」テーブル



4. 残りの各テンプレートに対して、マッピングプロセスを繰り返します。

注

- 「設定」>「フォームおよびマッピングプロセス」を選択することにより、マッピングを検証することができます。「フォームおよびプロセスマッピングの設定」ページが表示されたら、下にスクロールして「プロセスマッピング」テーブルを表示し、テーブル内に示される「マップされるプロセス名」エントリに次のプロセスタイプがマップされていることを確認します。

プロセスタイプ	マップされるプロセス名
createUser	Create User Template
deleteUser	Delete User Template
updateUser	Update User Template

  テンプレートが正しく有効化されていれば、すべての「マップされるプロセス名」エントリに「Template」という文字列が含まれています。

- テーブルに示すように「マップされるプロセス名」列に「**Template**」と入力することで、「フォームおよびプロセスマッピング」ページから直接、これらのプロセスタイプをマップすることもできます。

テンプレートのプロセスタイプを正しくマップしたら、タスクテンプレートの設定に進むことができます。

タスクテンプレートの設定

各種のタスクテンプレートを設定するには、次の手順に従います。

1. タスクテンプレートテーブル内の「名前」リンクを選択します。次のいずれかのページが表示されます。
   - **「タスクテンプレート「Create User Template」の編集 :」** ― 新しいユーザーアカウントの作成に使用するテンプレートを編集するには、このページを開きます。
   - **「タスクテンプレート「Delete User Template」の編集 :」** ― ユーザーアカウントの削除またはプロビジョニング解除に使用するテンプレートを編集するには、このページを開きます。
   - **「タスクテンプレート「Update User Template」の編集 :」** ― 既存ユーザーの情報の更新に使用するテンプレートを編集するには、このページを開きます。

それぞれのタスクテンプレートの編集ページには、ユーザーワークフローの主な設定領域に対応する一連のタブがあります。

次の表は、それぞれのタブの名前、目的、そのタブを使用するテンプレートについて説明したものです。

表 8-1 タスクテンプレートのタブ

タブ名	目的	テンプレート
一般 (デフォルトタブ)	「ホーム」および「アカウント」の各ページのタスクバー内と、「タスク」ページ上のタスクインスタンステーブル内でのタスク名の表示形式を定義します。	ユーザー作成タスクテンプレートとユーザー更新タスクテンプレートのみ
	ユーザーアカウントの削除 / プロビジョニング解除形式を指定できます。	ユーザー削除テンプレートのみ
通知	Identity Manager がプロセスを起動したときに管理者およびユーザーに送信される電子メール通知を設定できます。	すべてのテンプレート
承認	タイプ別に承認を有効または無効にする、追加の承認者を指定する、Identity Manager が特定のタスクを実行する前にアカウントデータの属性を指定するなどの作業を行うことができます。	すべてのテンプレート
監査	ワークフローの監査を有効化および設定できます。	すべてのテンプレート
プロビジョニング	バックグラウンドでタスクを実行できるようにします。また、タスクが失敗した場合に Identity Manager がタスクを再試行できるようにします。	ユーザー作成タスクテンプレートとユーザー更新タスクテンプレートのみ
サンライズとサンセット	指定された日時までの作成タスクの保留 (サンライズ) または指定された日時までの削除タスクの保留 (サンセット) についての設定を行うことができます。	ユーザー作成タスクテンプレートのみ
データ変換	プロビジョニング中にユーザーデータがどのように変換されるかを設定することができます。	ユーザー作成タスクテンプレートとユーザー更新タスクテンプレートのみ

2. いずれかのタブを選択して、テンプレートのワークフロー機能を設定します。

   これらのタブでの設定方法については、次の各節を参照してください。

   - 258 ページの「「一般」タブの設定」
   - 261 ページの「「通知」タブの設定」
   - 266 ページの「「承認」タブの設定」

- 279 ページの「「監査」タブの設定」
- 280 ページの「「プロビジョニング」タブの設定」
- 281 ページの「「サンライズとサンセット」タブの設定」
- 286 ページの「「データ変換」タブの設定」

3. テンプレートの設定を完了したら、「保存」ボタンをクリックして変更を保存します。

「一般」タブの設定

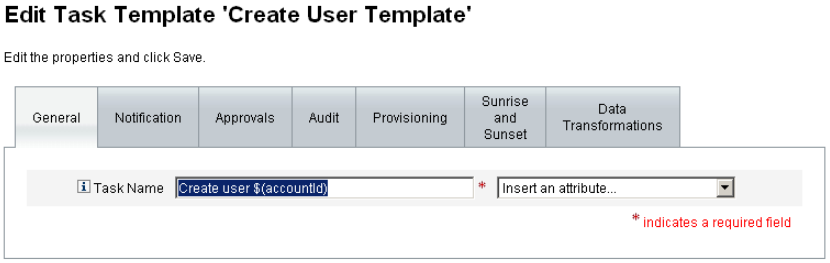
この節では、「一般」タブでの設定手順を説明します。

注	ユーザー作成テンプレートとユーザー更新テンプレートのタスクテンプレートの編集ページは共通なため、タブの設定手順は 1 つの節にまとめられています。

ユーザー作成テンプレートまたはユーザー更新テンプレートの場合

「タスクテンプレート「Create User Template」の編集 :」または「タスクテンプレート「Update User Template」の編集 :」ページを開くと、「一般」タブページがデフォルトで表示されます。次の図に示すように、このページは「タスク名」テキストフィールドおよびメニューで構成されます。

図 8-5　「一般」タブ : ユーザー作成テンプレート



タスク名はリテラルテキストまたはタスク実行時に解決される属性参照、あるいはその両方で指定できます。

デフォルトのタスク名を変更するには、次の手順に従います。

1. 「タスク名」フィールドに名前を入力します。

   デフォルトのタスク名を編集することも、完全に別の名前にすることもできます。

2. 「タスク名」メニューには、このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されている属性のリストが表示されます。メニューから属性を選択します (省略可能)。

   Identity Manager によって、「タスク名」フィールド内のエントリに属性名が追加されます。次に例を示します。

   ```
   Create user $(accountId) $(user.global.email)
   ```

3. 終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - 新しいタスク名が Identity Manager のタスクバーに表示されます。タスクバーは「ホーム」タブおよび「アカウント」タブの最下部にあります。
   - 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

ユーザー削除テンプレートの場合

「タスクテンプレート「Delete User Template」の編集 :」ページを開くと、「一般」タブページがデフォルトで表示されます。

ユーザーアカウントの削除 / プロビジョニング解除形式を指定するには、次の手順に従います。

1. Identity Manager アカウントの削除」ボタンを使用して、削除操作の間に Identity Manager アカウントを削除できるかどうかを指定します。
   - **「なし」** – アカウントが削除されるのを防ぐには、このボタンを有効にします。
   - **「プロビジョニング解除後にユーザーがリンクされたアカウントを持っていない場合のみ」** – プロビジョニング解除後にリンクされたリソースアカウントがない場合にのみユーザーアカウントの削除を許可するには、このボタンを有効にします。
   - **「常時」** – 割り当てられたリソースアカウントがまだ存在する場合も含めてユーザーアカウントの削除を常に許可するには、このボタンを有効にします。
2. 「リソースアカウントのプロビジョニング解除」ボックスを使用して、すべてのリソースアカウントを対象にリソースアカウントのプロビジョニング解除を制御します。
   - **「すべて削除」** – すべての割り当て済みリソース上の、ユーザーを表すすべてのアカウントを削除するには、このボックスを有効にします。
   - **「すべて割り当て解除」** – すべてのリソースアカウントをユーザーから割り当て解除するには、このボックスを有効にします。リソースアカウントは削除されません。

- **「すべてをリンク解除」**－ Identity Manager システムからリソースアカウントへのすべてのリンクを解除するには、このボックスを有効にします。割り当てられているがリンクされていないアカウントを持つユーザーは、更新が必要なことを示すバッジのマークとともに表示されます。

注 これらの制御設定は、「個々のリソースアカウントのプロビジョニング解除」テーブルでの動作よりも優先されます。

---

3. **「個々のリソースアカウントのプロビジョニング解除」**ボックスを使用すると、次のように、(「リソースアカウントのプロビジョニング解除」と比較して) ユーザーのプロビジョニング解除についてより詳細な設定を行うことができます。
   - **「削除」**－ リソース上のユーザーを表すアカウントを削除するには、このボックスを有効にします。
   - **「割り当て解除」**－ このボックスを有効にすると、ユーザーはリソースに直接割り当てられなくなります。リソースアカウントは削除されません。
   - **「リンク解除」**－ Identity Manager システムからリソースアカウントへのリンクを解除するには、このボックスを有効にします。割り当てられているがリンクされていないアカウントを持つユーザーは、更新が必要なことを示すバッジのマークとともに表示されます。

注 「個々のリソースアカウントのプロビジョニング解除」オプションは、複数の異なるリソースに対してプロビジョニング解除ポリシーを個別に指定したい場合に便利です。たとえば、個々の Active Directory ユーザーは削除後に再生成できないグローバル ID を持つため、ほとんどの顧客は Active Directory ユーザーを削除したくないと考えます。

一方、プロビジョニング解除設定は新しいリソースを追加するたびに更新しなければならないため、新しいリソースが追加される環境ではこのオプションを使用しないほうが適している場合もあります。

---

4. 終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

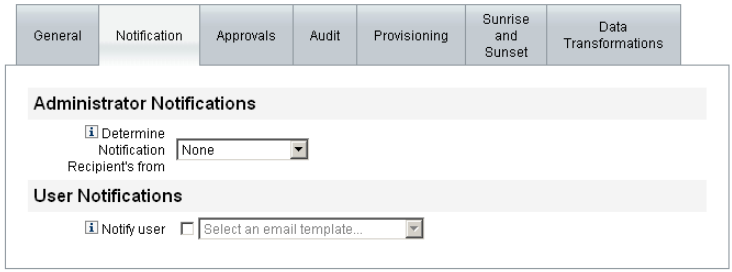
「通知」タブの設定

すべてのタスクテンプレートは、Identity Manager がプロセスを起動したとき (通常はプロセスの完了後) に、管理者およびユーザーに電子メールで通知を送信する動作をサポートします。「通知」タブを使用してこれらの通知を設定できます。

注 Identity Manager では、電子メールテンプレートを使用して、情報および操作のリクエストを管理者、承認者、およびユーザーに配信します。Identity Manager の電子メールテンプレートの詳細については、このガイドの「電子メールテンプレートの理解」の節を参照してください。

次の図は、ユーザー作成テンプレートの「通知」ページを示したものです。

図 8-6 「通知」タブ : ユーザー作成テンプレート



Identity Manager が通知の受信者を決定する方法を指定するには、次の手順に従います。

1. 「管理者通知」セクションの設定を完了します。
2. 「ユーザー通知」セクションの設定を完了します。
3. 終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

管理者通知の設定

管理者である受信者に通知するための方法を決定するには、「通知の受信者を決定する方法」メニューからオプションを選択します。

- **「なし」**(デフォルト) ― 管理者への通知を行いません。

- **「属性」** ― 通知の受信者のアカウント ID を、ユーザービューで指定された属性から取得する場合に選択します。262 ページの「属性による受信者の指定」に進みます。
- **「規則」** ― 指定された規則を評価することによって通知の受信者のアカウント ID を取得する場合に選択します。263 ページの「規則による受信者の指定」に進みます。
- **「クエリー」** ― 特定のリソースへのクエリーを作成することによって通知の受信者のアカウント ID を取得する場合に選択します。263 ページの「クエリーによる受信者の指定」に進みます。
- **「管理者リスト」** ― 通知の受信者をリストから直接選ぶ場合に選択します。264 ページの「管理者リストからの受信者の指定」に進みます。

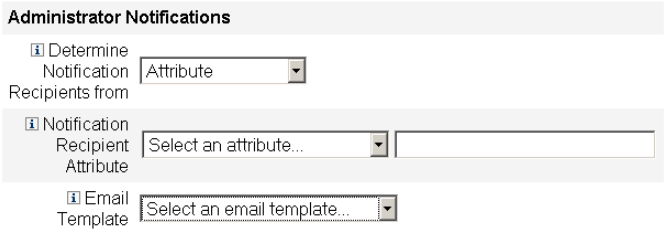
属性による受信者の指定

指定された属性から通知の受信者のアカウント ID を取得するには、次の手順に従います。

注	属性は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストに解決する必要があります。

1. 「通知の受信者を決定する方法」メニューから「属性」を選択します。次の新しいオプションが表示されます。

   図 8-7　　管理者通知 : 属性

   - **「通知の受信者の属性」** ― 受信者のアカウント ID を決定するために使われる属性 (このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されている) のリストが提示されます。
   - **「電子メールテンプレート」** ― 電子メールテンプレートのリストが提示されます。
2. **「通知の受信者の属性」**メニューから属性を選択します。

   メニューの隣にあるテキストフィールドに属性名が表示されます。

3. 「電子メールテンプレート」メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

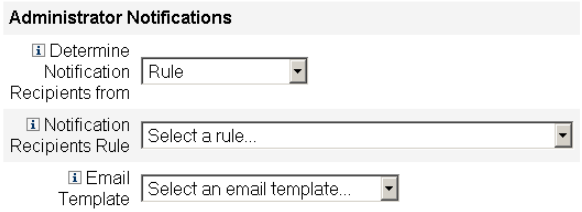
規則による受信者の指定

指定された規則から通知の受信者のアカウント ID を取得するには、次の手順に従います。

注	評価されたとき、規則は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストを返す必要があります。

1. 「通知の受信者を決定する方法」メニューから「規則」を選択します。「通知」フォームに次の新しいオプションが表示されます。

図 8-8　管理者通知 : 規則



   - **「通知の受信者の規則」** – 評価されたときに受信者のアカウント ID を返す規則 (システムに対して現在定義されているもの) のリストが提示されます。
   - **「電子メールテンプレート」** – 電子メールテンプレートのリストが提示されます。
2. 「通知の受信者の規則」メニューから規則を選択します。
3. 「電子メールテンプレート」メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

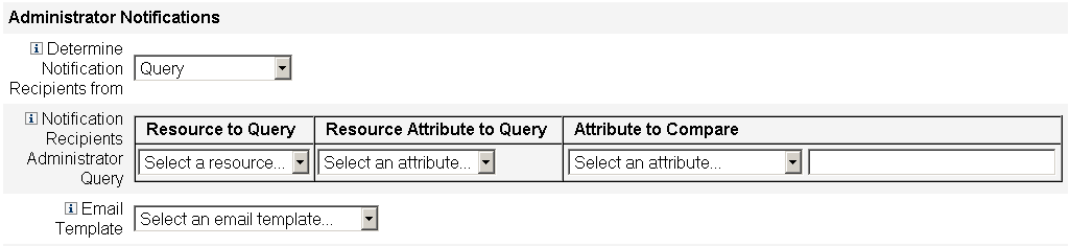
クエリーによる受信者の指定

注	現時点では、LDAP および Active Directory リソースのクエリーのみがサポートされています。

指定されたリソースを問い合わせることで通知の受信者のアカウント ID を取得するには、次の手順に従います。

1. 「通知の受信者を決定する方法」メニューから「クエリー」を選択します。図 8-9 に示すように、「通知」フォームに次の新しいオプションが表示されます。

図 8-9　　管理者通知 : クエリー



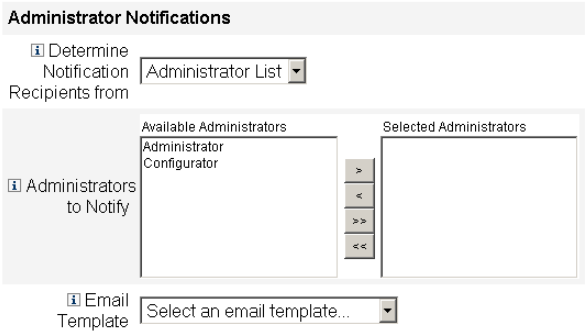
- **「通知受信者の管理者クエリー」** – 次のメニューで構成されるテーブルが提示されます。このテーブルを使用してクエリーを作成できます。
- **「問い合わせ先のリソース」** – システムに対して現在定義されているリソースのリストが提示されます。
- **「問い合わせ先のリソース属性」** – システムに対して現在定義されているリソース属性のリストが提示されます。
- **「比較対象の属性」** – システムに対して現在定義されている属性のリストが提示されます。
- **「電子メールテンプレート」** – 電子メールテンプレートのリストが提示されます。

2. これらのメニューからリソース、リソース属性、および比較対象の属性を選択し、クエリーを作成します。
3. 「電子メールテンプレート」メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

管理者リストからの受信者の指定

「通知の受信者を決定する方法」メニューから「管理者リスト」を選択します。「通知」フォームに次の新しいオプションが表示されます。

図 8-10　　管理者通知 : 管理者リスト



- **「通知する管理者」** – 通知可能な管理者のリストと選択ツールが提示されます。
- **「電子メールテンプレート」** – 電子メールテンプレートのリストが提示されます。

4. 「利用可能な管理者」リストから 1 人以上の管理者を選択し、「選択された管理者」リストに移動します。
5. 「電子メールテンプレート」メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

ユーザー通知の設定

通知を受けるユーザーを指定するとき、通知のための電子メールを生成するために使われる電子メールテンプレートの名前も指定する必要があります。

作成、更新、または削除中のユーザーに通知するには、図 8-11 に示すように、「ユーザーへの通知」チェックボックスをオンにし、リストから電子メールテンプレートを選択します。

図 8-11　　電子メールテンプレートの指定

「承認」タブの設定

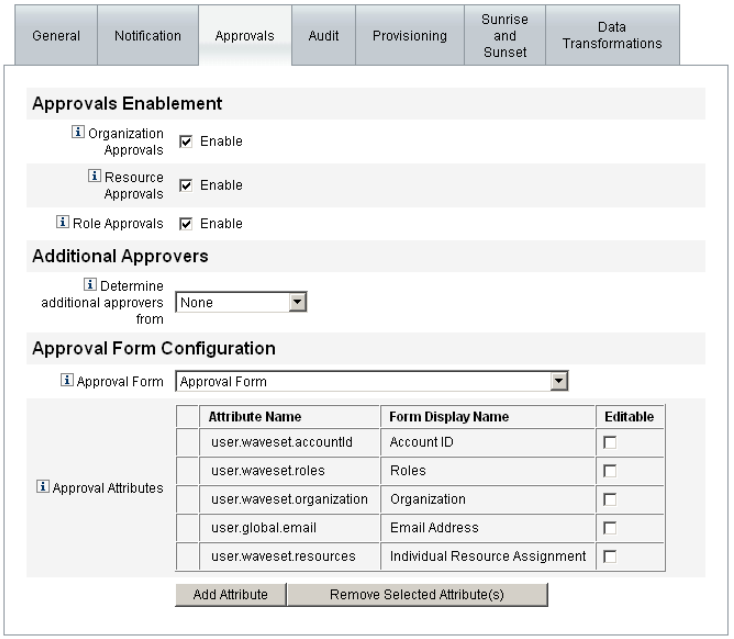
Identity Manager がユーザーの作成、削除、または更新の各タスクを実行する前に、「承認」タブを使用して、追加の承認者やタスク承認フォームの属性を指定することができます。

従来の方式では、特定の組織、リソース、またはロールと関連付けられた管理者は、実行前に特定のタスクを承認する必要があります。Identity Manager では、追加の承認者 (タスクを承認する必要がある追加の管理者) を指定することもできます。

注 ワークフローに対して追加の承認者を設定する場合、従来からの承認者による承認に加えて、テンプレートで指定された追加の承認者による承認もリクエストすることになります。

次の図は、初期状態の「承認」ページの管理ユーザーインタフェースの例です。

図 8-12 「承認」タブ : ユーザー作成テンプレート



承認を設定するには、次の手順に従います。

1. 「承認の有効化」の節の手順を完了します (267 ページの「承認の有効化」を参照)。

2. 「追加の承認者」の節の手順を完了します (267 ページの「追加の承認者の指定」を参照)。
3. ユーザー作成テンプレートおよびユーザー更新テンプレートのみを対象に、「承認フォームの設定」の節の手順を完了します (275 ページの「承認フォームの設定」を参照)。
4. 「承認」タブの設定を完了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

承認の有効化

次のそれぞれの「承認の有効化」チェックボックスを使用して、ユーザー作成、ユーザー削除、またはユーザー更新の各タスクの実行前に承認をリクエストするように設定します。

注	デフォルトでは、これらのチェックボックスはユーザー作成テンプレートおよびユーザー更新テンプレートに対しては有効になっていますが、ユーザー削除テンプレートに対しては「無効」になっています。

- **「組織の承認」** – 設定済みの任意の組織承認者による承認を必須とするには、このチェックボックスをオンにします。
- **「リソースの承認」** – 設定済みの任意のリソース承認者による承認を必須とするには、このチェックボックスをオンにします。
- **「ロールの承認」** – 設定済みの任意のロール承認者による承認を必須とするには、このチェックボックスをオンにします。

追加の承認者の指定

「追加の承認者を決定する方法」メニューを使用して、Identity Manager がユーザー作成、ユーザー削除、またはユーザー更新の各タスクに対して追加の承認者を決定する方法を指定します。このメニューのオプションには、次のものがあります。

表 8-2 「追加の承認者を決定する方法」メニューのオプション

オプション	説明
なし (デフォルト)	タスク実行のために追加の承認者は必要ありません。
属性	承認者のアカウント ID は、ユーザーのビューで指定された属性の内部から取得されます。

表 8-2　「追加の承認者を決定する方法」メニューのオプション (続き)

オプション	説明
規則	承認者のアカウント ID は、指定された規則を評価することで取得されます。
クエリー	承認者のアカウント ID は、特定のリソースを問い合わせることで取得されます。
管理者リスト	承認者はリストから明示的に選択されます。

(「なし」を除く) これらのオプションのいずれかを選択すると、管理ユーザーインタフェースに追加のオプションが表示されます。これらのオプションを設定するための手順は、267 ページ以降で説明します。

以下の各節の指示に従って、追加の承認者を決定する方法を指定します。

- 属性から (268 ページ)
- 規則から (269 ページ)
- クエリーから (270 ページ)
- 管理者リストから (271 ページ)

属性から

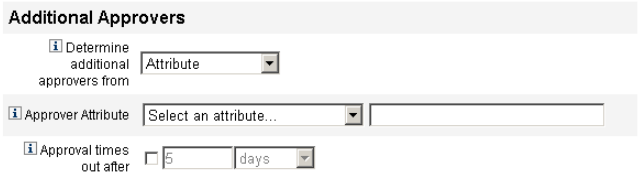
属性から追加の承認者を決定するには、次の手順に従います。

1. 「追加の承認者を決定する方法」メニューから「属性」を選択します。

注	属性は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストに解決する必要があります。

次の新しいオプションが表示されます。

図 8-13　追加の承認者 : 属性



- **「承認者の属性」** ― 承認者のアカウント ID を決定するために使われる属性 (このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されているもの) のリストが提示されます。

- **「承認がタイムアウトになるまでの時間」** ― 承認がいつタイムアウトするかを指定できます。

注	「承認がタイムアウトになるまでの時間」の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

2. 「承認者の属性」メニューを使用して属性を選択します。

   選択した属性が隣のテキストフィールドに表示されます。

3. 指定された時間が経過したら承認リクエストをタイムアウトさせるかどうかを決定します。
   - タイムアウト時間を指定する場合は、272 ページの「承認のタイムアウトの設定」の手順に進みます。
   - タイムアウト時間を指定しない場合、275 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

規則から

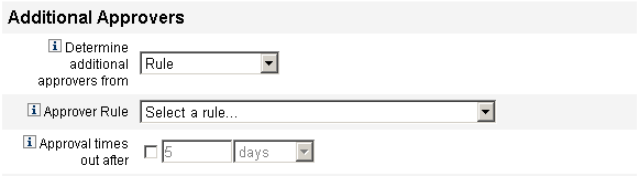
承認者のアカウント ID を指定された規則から取得するには、次の手順に従います。

1. 「追加の承認者を決定する方法」メニューから「規則」を選択します。

注	評価されたとき、規則は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストを返す必要があります。

次の新しいオプションが表示されます。

図 8-14 追加の承認者 : 規則



- **「承認者の規則」** ― 評価されたときに受信者のアカウント ID を返す規則 (システムに対して現在定義されているもの) のリストが提示されます。
- **「承認がタイムアウトになるまでの時間」** ― 承認がいつタイムアウトするかを指定できます。

注	「承認がタイムアウトになるまでの時間」の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

2. 「承認者の規則」メニューから規則を選択します。
3. 指定された時間が経過したら承認リクエストをタイムアウトさせるかどうかを決定します。
   - タイムアウト時間を指定する場合は、272 ページの「承認のタイムアウトの設定」の手順に進みます。
   - タイムアウト時間を指定しない場合、275 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

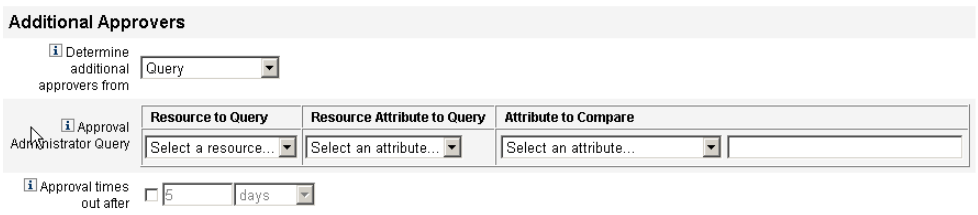
クエリーから

注	現時点では、LDAP および Active Directory リソースのクエリーのみがサポートされています。

指定されたリソースを問い合わせることで承認者のアカウント ID を取得するには、次の手順に従います。

1. 「追加の承認者を決定する方法」メニューから「クエリー」を選択します。次の新しいオプションが表示されます。

図 8-15 追加の承認者 : クエリー



- **「承認の管理者のクエリー」** – 次のメニューで構成されるテーブルが提示されます。このテーブルを使用してクエリーを作成できます。
  - **「問い合わせ先のリソース」** – システムに対して現在定義されているリソースのリストが提示されます。
  - **「問い合わせ先のリソース属性」** – システムに対して現在定義されているリソース属性のリストが提示されます。

- ❍ **「比較対象の属性」** – システムに対して現在定義されている属性のリストが提示されます。

- **「承認がタイムアウトになるまでの時間」** – 承認がいつタイムアウトするかを指定できます。

注	「承認がタイムアウトになるまでの時間」の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

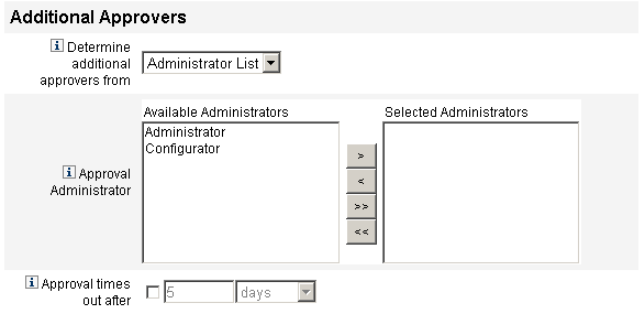
2. 次のようにしてクエリーを作成します。
   a. 「問い合わせ先のリソース」メニューからリソースを選択します。
   b. 「問い合わせ先のリソース属性」メニューおよび「比較対象の属性」メニューから属性を選択します。
3. 指定された時間が経過したら承認リクエストをタイムアウトさせるかどうかを決定します。
   - ❍ タイムアウト時間を指定する場合は、272 ページの「承認のタイムアウトの設定」の手順に進みます。
   - ❍ タイムアウト時間を指定しない場合、275 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

管理者リストから

追加の承認者を管理者リストから明示的に選択するには、次の手順に従います。

1. 「追加の承認者を決定する方法」メニューから「管理者リスト」を選択します。次の新しいオプションが表示されます。

図 8-16 追加の承認者 : 管理者リスト



- ❍ **「通知する管理者」** – 通知可能な管理者のリストと選択ツールが提示されます。

- **「承認フォーム」** – 追加の承認者が承認リクエストを承認または却下するために使用できるユーザーフォームのリストが提示されます。
- **「承認がタイムアウトになるまでの時間」** – 承認がいつタイムアウトするかを指定できます。

注 「承認がタイムアウトになるまでの時間」の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

2. 「利用可能な管理者」リストから 1 人以上の管理者を選択し、選択した名前を「選択された管理者」リストに移動します。
3. 指定された時間が経過したら承認リクエストをタイムアウトさせるかどうかを決定します。
   - タイムアウト時間を指定する場合は、272 ページの「承認のタイムアウトの設定」の手順に進みます。
   - タイムアウト時間を指定しない場合、275 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

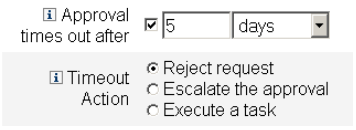
承認のタイムアウトの設定

承認のタイムアウトを設定するには、次の手順に従います。

1. チェックボックスをオンにします。

   次の図に示すように、隣接するテキストフィールドとメニューがアクティブになり、「タイムアウトのアクション」ボタンが表示されます。

図 8-17 承認のタイムアウトのオプション



2. 次のように、「承認がタイムアウトになるまでの時間」のテキストフィールドとメニューを使用してタイムアウト時間を指定します。
   a. メニューから秒、分、時間、または日を選択します。
   b. テキストフィールドに数値を入力して、タイムアウトの秒数、分数、時間数、または日数を指定します。

注 「承認がタイムアウトになるまでの時間」の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

3. 「タイムアウトのアクション」のいずれかのラジオボタンを選択して、承認リクエストがタイムアウトしたときの動作を指定します。

   - **「リクエストの却下」**— 指定されたタイムアウト時間までにリクエストが承認されない場合、Identity Manager は自動的にそのリクエストを却下します。
   - **「承認のエスカレーション」**— 指定されたタイムアウト時間までにリクエストが承認されない場合、Identity Manager はそのリクエストを別の承認者に自動的にエスカレーションします。

     このラジオボタンを選択すると、エスカレーションされた承認の承認者を Identity Manager が決定する方法を指定する必要があるため、新しいオプションが表示されます。続きの手順については、273 ページの「承認のエスカレーション」を参照してください。
   - **「タスクの実行」**— 指定されたタイムアウト時間までに承認リクエストが承認されない場合、Identity Manager は自動的に代替のタスクを実行します。

     このラジオボタンを選択すると、承認リクエストがタイムアウトした場合に実行するタスクを指定するための「承認のタイムアウト時のタスク」メニューが表示されます。続きの手順については、275 ページの「タスクの実行」を参照してください。

承認のエスカレーション

「タイムアウトアクション」で「承認のエスカレーション」ラジオボタンを選択すると、次のような「エスカレーション承認者を決定する方法」メニューが表示されます。

図 8-18 「エスカレーション承認者を決定する方法」メニュー

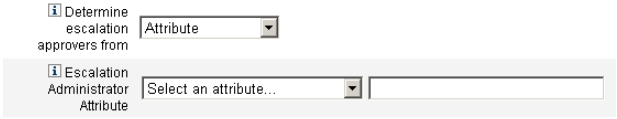
このメニューから次のいずれかのオプションを選択して、エスカレーションされた承認の承認者を決定する方法を指定します。

- **「属性」**— 新しいユーザーのビューで指定された属性の内部から承認者のアカウント ID を決定します。

注	属性は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストに解決する必要があります。

「エスカレーション管理者属性」メニューが表示されたら、リストから属性を選択します。選択した属性が隣のテキストフィールドに表示されます。

図 8-19　「エスカレーション管理者属性」メニュー

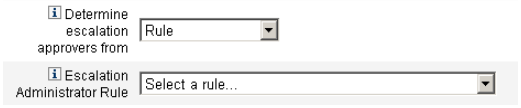


- **「規則」** ― 指定された規則を評価することによって承認者のアカウント ID を決定します。

注	評価されたとき、規則は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストを返す必要があります。

「エスカレーション管理者規則」メニューが表示されたら、リストから規則を選択します。

図 8-20　「エスカレーション管理者規則」メニュー



- **「クエリー」** ― 特定のリソースを問い合わせることで承認者のアカウント ID を決定します。

  「エスカレーション管理者クエリー」メニューが表示されたら、次のようにしてクエリーを作成します。

  a. 「問い合わせ先のリソース」メニューからリソースを選択します。

  b. 「問い合わせ先のリソース属性」メニューから属性を選択します。

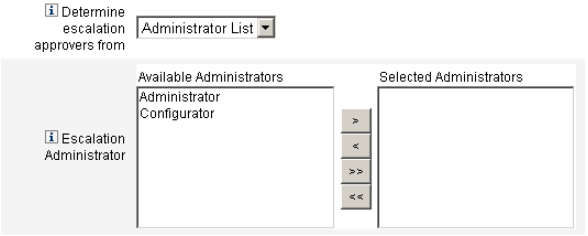
  c. 「比較対象の属性」メニューから属性を選択します。

図 8-21　「エスカレーション管理者クエリー」メニュー

- **管理者リスト」** (デフォルト) ― リストから承認者を明示的に選択します。

「エスカレーション管理者」選択ツールが表示されたら、次のようにして承認者を選択します。

図 8-22　「エスカレーション管理者」選択ツール



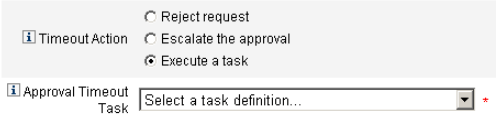
a. **「利用可能な管理者」**リストから、1 人または複数の管理者の名前を選択します。

b. 選択した名前を**「選択された管理者」**リストに移動します。

タスクの実行

「タイムアウトアクション」で「タスクの実行」ラジオボタンを選択すると、次のような「承認のタイムアウト時のタスク」メニューが表示されます。

図 8-23　「承認のタイムアウト時のタスク」メニュー



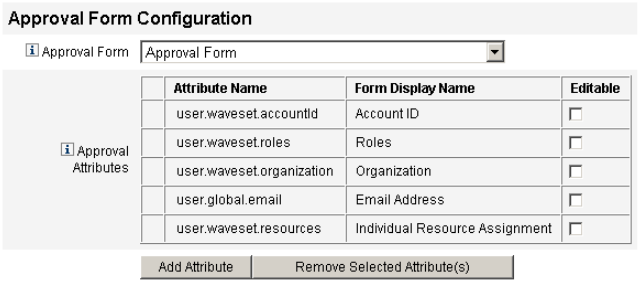
承認リクエストがタイムアウトした場合に実行するタスクを指定します。たとえば、リクエスト者がヘルプデスクリクエストを送信したり、レポートを管理者に送信したりすることを許可できます。

承認フォームの設定

注	ユーザー削除テンプレートには「承認フォーム設定」セクションは含まれません。このセクションはユーザー作成テンプレートおよびユーザー更新テンプレートに対してのみ設定できます。

「承認フォーム設定」セクションの機能を使用して、承認フォームの選択や、属性の承認フォームへの追加 (または承認フォームからの削除) を行うことができます。

図 8-24　承認フォームの設定



デフォルトでは、「承認の属性」テーブルには次の標準属性が含まれます。

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`
- `user.waveset.resources`

注　デフォルトの承認フォームは、承認属性の表示を許可するように設定されています。デフォルトフォーム以外の承認フォームを使用する場合、「承認の属性」テーブルで指定された承認属性を表示するようにフォームを設定する必要があります。

追加の承認者のための承認フォームを設定するには、次の手順に従います。

1. 「承認フォーム」メニューからフォームを選択します。

   承認者はこのフォームを使用して承認リクエストを承認または却下します。

2. 承認者による属性値の編集を許可する場合、「承認の属性」テーブルで、各属性の「編集可能」列のチェックボックスをオンにします。

   たとえば、`user.waveset.accountId` 属性のチェックボックスをオンにすると、承認者はユーザーのアカウント ID を変更できます。

注 承認フォーム内でアカウント固有の属性値を変更すると、ユーザーが実際にプロビジョニングされるときに、同じ名前のグローバル属性値もすべてオーバーライドされます。

たとえば、スキーマ属性 description を持つリソース R1 がシステムに存在し、user.accounts[R1].description 属性を編集可能な属性として承認フォームに追加する場合、承認フォーム内で description 属性の値を変更すると、リソース R1 のみを対象に、global.description から伝播された値がオーバーライドされます。

3. **「属性の追加」または「選択している属性の削除」**ボタンをクリックして、新しいユーザーのアカウントデータ内の属性のうち承認フォームに表示するものを指定します。
   - 属性をフォームに追加する方法については、277 ページの「属性の追加」を参照してください。
   - 属性をフォームから削除する方法については、278 ページの「属性の削除」を参照してください。

注 XML ファイルを変更しない限り、デフォルトの属性を承認フォームから削除することはできません。

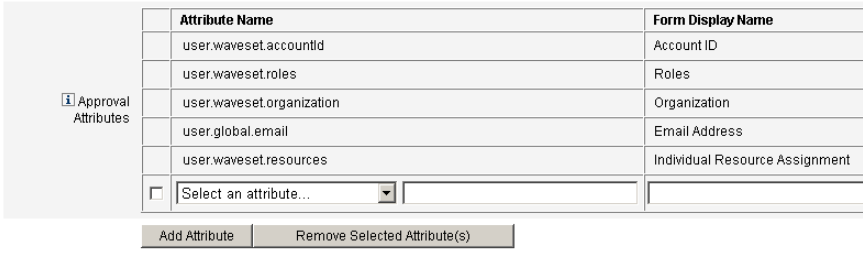
属性の追加

属性を承認フォームに追加するには、次の手順に従います。

1. 「承認の属性」テーブルの下にある「属性の追加」ボタンをクリックします。

   次の図に示すように、「承認の属性」テーブルの「属性名」列内で選択メニューがアクティブになります。

図 8-25 承認属性の追加



2. メニューから属性を選択します。

   選択された属性名が隣のテキストフィールドに表示され、属性のデフォルトの表示名が「フォーム表示名」列に表示されます。

   たとえば、`user.waveset.organization` 属性を選択した場合、表には次の情報が含まれます。

   - 必要に応じて、それぞれのテキストフィールドに新しい名前を入力することによって、デフォルトの属性名またはデフォルトのフォーム表示名を変更できます。
   - 承認者による属性値の変更を許可する場合、「編集可能」チェックボックスをオンにします。

     たとえば、あらかじめ定義されているユーザーの電子メールアドレスなどの情報を承認者が変更したい場合があります。

3. これらの手順を繰り返して、必要な属性を指定します。

属性の削除

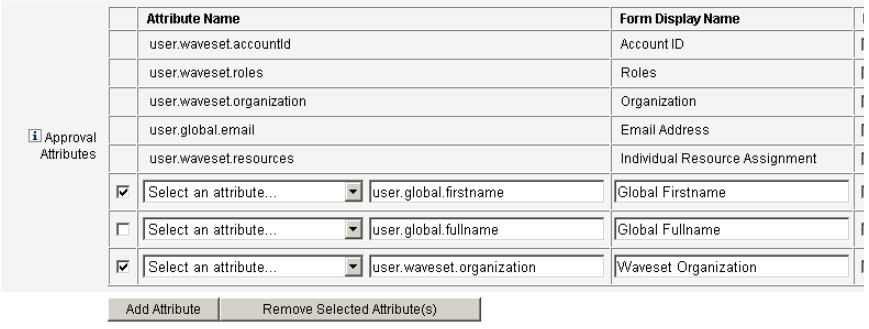
注 XML ファイルを変更しない限り、デフォルトの属性を承認フォームから削除することはできません。

承認フォームから属性を削除するには、次の手順に従います。

1. 「承認の属性」テーブルの左端の列で、1 つ以上のチェックボックスをオンにします。
2. **「選択している属性の削除」**ボタンをクリックすると、選択した属性が「承認の属性」テーブルからただちに削除されます。

   たとえば、次の状態のテーブルで**「選択している属性の削除」**ボタンをクリックすると、`user.global.firstname` および `user.waveset.organization` がテーブルから削除されます。

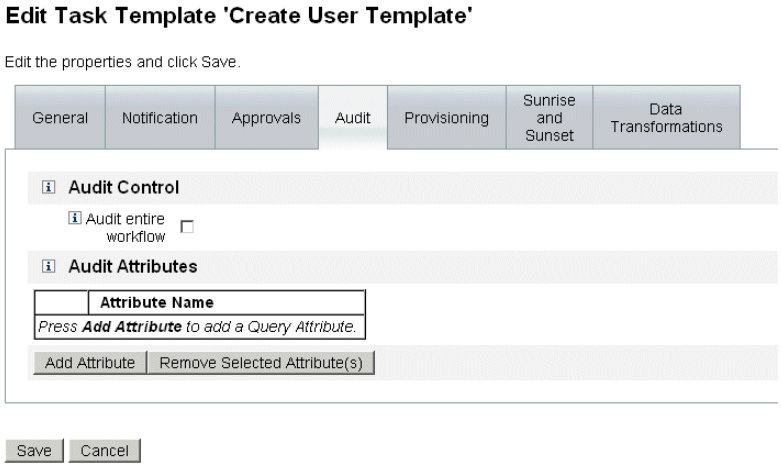
図 8-26 承認属性の削除



「監査」タブの設定

設定可能なすべてのタスクテンプレートで、特定のタスクを監査するためのワークフローを設定することができます。特に、「監査」タブを設定することにより、ワークフローイベントの監査の有無や、レポート対象として記録する属性を指定することができます。

図 8-27　　ユーザー作成テンプレートの監査設定



ユーザーテンプレートの「監査」タブから監査を設定するには、次の手順に従います。

1. 「ワークフロー全体の監査」チェックボックスをオンにして、ワークフローの監査機能を有効にします。
2. 「属性の監査」セクションの「属性の追加」ボタンをクリックして、レポート対象として記録する属性を選択します。
3. 「属性の監査」テーブルに「属性の選択」メニューが表示されたら、リストから属性を選択します。

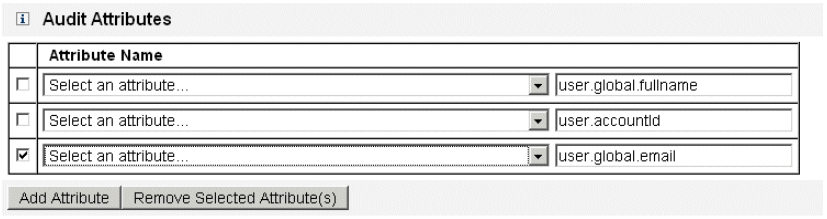
   属性名が隣のテキストフィールドに表示されます。

図 8-28　　属性の追加

「属性の監査」テーブルから属性を削除するには、次の手順に従います。

1. 削除する属性の隣にあるチェックボックスを有効にします。

図 8-29　user.global.email 属性の削除



2. **「選択している属性の削除」**ボタンをクリックします。

このタブの設定を終了したら、次の処理を実行できます。

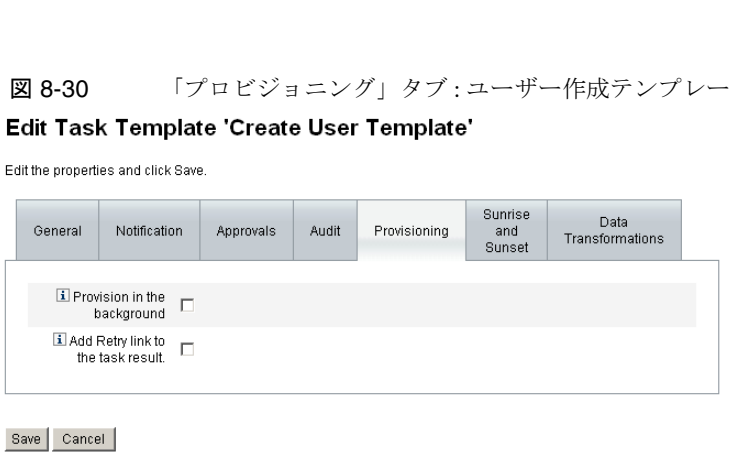
- 別のタブを選択して、テンプレートの編集を続けます。
- 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
- 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

「プロビジョニング」タブの設定

注　このタブはユーザー作成テンプレートおよびユーザー更新テンプレートに対してのみ使用できます。

「プロビジョニング」タブでは、プロビジョニングに関連する次のオプションを設定できます。

図 8-30　「プロビジョニング」タブ : ユーザー作成テンプレート



- **「バックグラウンドでプロビジョニング」** – 作成、削除、または更新タスクを同期的に実行するのではなくバックグラウンドで実行するには、このチェックボックスをオンにします。

  バックグラウンドでプロビジョニングを行うことにより、タスクの実行中も Identity Manager での作業を継続できます。

- **「再試行リンクをタスク結果に追加します」** – タスク実行の結果としてプロビジョニングエラーが発生したときに再試行リンクをユーザーインタフェースに追加する場合は、このチェックボックスをオンにします。再試行リンクにより、ユーザーは最初の試行でタスクが失敗した場合にタスクを再試行できます。

「プロビジョニング」タブの設定を終了したら、次の処理を実行できます。

- 別のタブを選択して、テンプレートの編集を続けます。
- 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
- 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

「サンライズとサンセット」タブの設定

注　このタブはユーザー作成テンプレートのみに対して使用できます。

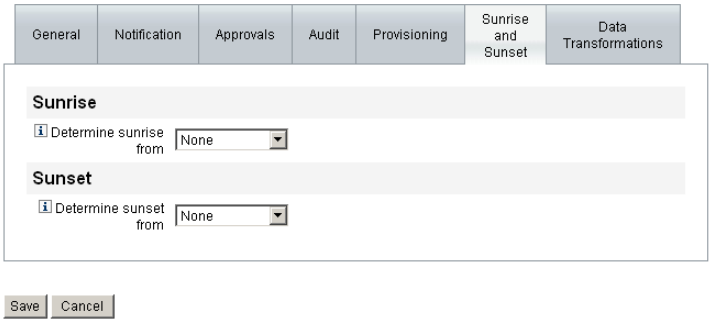
「サンライズとサンセット」タブでは、次のアクションが行われる日時を決定するための方法を選択できます。

- 新しいユーザーのプロビジョニングが行われる (サンライズ)。
- 新しいユーザーのプロビジョニング解除が行われる (サンセット)。

たとえば、6 ヶ月後に契約が終了する派遣社員に対してサンセット日付を指定できます。

図 8-31 に「サンライズとサンセット」タブでの設定を示します。

図 8-31 「サンライズとサンセット」タブ : ユーザー作成テンプレート



以下のトピックでは、「サンライズとサンセット」タブの設定手順を説明します。

サンライズの設定

新しいユーザーのプロビジョニングを行う日時を指定し、サンライズの作業項目を所有するユーザーを指定して、サンライズの設定を行います。

サンライズを設定するには、次の手順に従います。

1. 「サンライズを決定する方法」メニューから次のいずれかのオプションを選択して、Identity Manager がプロビジョニングの日時を決定する方法を指定します。
   - **指定された経過時間** – 指定された時間が経過するまでプロビジョニングを保留します。続きの手順については、283 ページを参照してください。
   - **指定された日** – 将来の指定された日付までプロビジョニングを保留します。続きの手順については、283 ページを参照してください。
   - **属性の指定** – ユーザーのビューでの属性値に基づいて、指定された日時までプロビジョニングを保留します。属性には日付 / 時刻文字列が含まれている必要があります。日付 / 時刻文字列を含むように属性を指定するとき、データが従うべきデータ形式を指定できます。

     続きの手順については、284 ページを参照してください。
   - **規則の指定** – 評価されたときに日付 / 時刻文字列を生成する規則に基づいてプロビジョニングを保留します。属性を指定するとき、データが従うべきデータ形式を指定できます。

     続きの手順については、284 ページを参照してください。

注 「サンライズを決定する方法」メニューのデフォルトでは、プロビジョニングをただちに行うようにする「なし」が選択されています。

2. 「作業項目の所有者」メニューからユーザーを選択して、サンライズの作業項目を所有する人物を指定します。

注 サンライズ作業項目は「承認」タブから利用可能です。

3. サンライズの設定が終了したら、次の処理を実行できます。
   - 別のタブを選択して、ユーザー作成テンプレートの編集を続けます。
   - 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

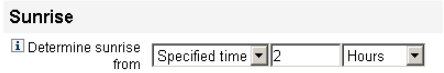
指定された経過時間

指定された時間が経過するまでプロビジョニングを保留するには、次の手順に従います。

1. 「サンライズを決定する方法」メニューから「指定された経過時間」を選択します。
2. 「サンライズを決定する方法」メニューの右側に新しいテキストフィールドとメニューが表示されたら、空のテキストフィールドに数値を入力し、メニューから時間の単位を選択します。

   たとえば、新しいユーザーを 2 時間後にプロビジョニングしたい場合、次のように指定します。

図 8-32 新しいユーザーを 2 時間後にプロビジョニングする設定



日付の指定

指定された日付までプロビジョニングを保留するには、次の手順に従います。

1. 「サンライズを決定する方法」メニューから「指定された日」を選択します。
2. 表示されるメニューオプションを使用して、プロビジョニングを実行する週、曜日、および月を指定します。

   たとえば、新しいユーザーを 9 月の第 2 月曜日にプロビジョニングしたい場合、次のように指定します。

図 8-33　日付による新しいユーザーのプロビジョニング

属性の指定

ユーザーアカウントデータ内の属性値に基づいてプロビジョニング日時を決定するには、次の手順に従います。

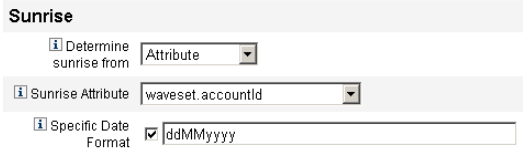
1. 「サンライズを決定する方法」メニューから「属性」を選択します。次のオプションがアクティブになります。
   - 「サンライズの属性」メニュー ー このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されている属性のリストが提示されます。
   - 「特定の日付形式」チェックボックスおよびメニュー ー 必要に応じて、属性値の日付形式文字列を指定できます。

注	「特定の日付形式」チェックボックスをオンにしない場合、日付文字列は `FormUtil` メソッドの `convertDateToString` に対して使用できる形式に従う必要があります。サポートされている日付形式の完全な一覧については、製品ドキュメントを参照してください。

2. 「サンライズの属性」メニューから属性を選択します。
3. 必要な場合、「特定の日付形式」チェックボックスをオンにし、アクティブになった「特定の日付形式」フィールドに日付形式文字列を入力します。

   たとえば、ユーザーの `waveset.accountId` 属性値に基づき、日、月、および年の形式を使用して新しいユーザーをプロビジョニングするには、次のように指定します。

図 8-34　属性による新しいユーザーのプロビジョニング



規則の指定

指定された規則を評価することでプロビジョニング日時を決定するには、次の手順に従います。

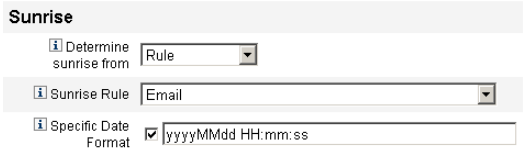
1. 「サンライズを決定する方法」メニューから「規則」を選択します。次のオプションがアクティブになります。
   - **「サンライズの規則」**メニュー ー システムに対して現在定義されている規則の一覧が提示されます。
   - 「特定の日付形式」チェックボックスおよびメニュー ー 必要に応じて、規則の戻り値の日付形式文字列を指定できます。

注 「特定の日付形式」チェックボックスをオンにしない場合、日付文字列は FormUtil メソッドの convertDateToString に対して使用できる形式に従う必要があります。サポートされている日付形式の完全な一覧については、製品ドキュメントを参照してください。

2. 「サンライズの規則」メニューから規則を選択します。
3. 必要な場合、「特定の日付形式」チェックボックスをオンにし、アクティブになった「特定の日付形式」フィールドに日付形式文字列を入力します。

たとえば、「電子メール」規則に基づき、年、月、日、時、分、および秒の形式を使用して新しいユーザーをプロビジョニングするには、次の手順に従います。

図 8-35 規則による新しいユーザーのプロビジョニング



サンセットの設定

サンセット (プロビジョニング解除) を設定するためのオプションおよび手順は基本的に、「サンライズの設定」で説明した、サンライズ (プロビジョニング) の設定に使用するものと同じです。

唯一の違いは、「サンセット」セクションには「サンセットタスク」メニューがある点です。このメニューを使用して、指定された日時にユーザーをプロビジョニング解除するためのタスクを指定する必要があります。

サンセットを設定するには、次の手順に従います。

1. 「サンセットを決定する方法」メニューを使用して、プロビジョニング解除がいつ行われるかを決定するための方法を指定します。

注 「サンセットを決定する方法」メニューでは、プロビジョニング解除をただちに行える「なし」オプションがデフォルトによって選択されます。

- **「指定された経過時間」** – 指定された時間が経過するまでプロビジョニング解除を保留します。手順については、283 ページの「指定された経過時間」を参照してください。
- **「指定された日」** – 将来の指定された日付までプロビジョニング解除を遅らせます。手順については、283 ページの「日付の指定」を参照してください。
- **「属性」** – ユーザーのアカウントデータ内の属性の値に基づいて、指定された日時までプロビジョニング解除を保留します。属性には日付 / 時刻文字列が含まれている必要があります。日付 / 時刻文字列を含むように属性を指定するとき、データが従うべき日付形式を指定できます。

  手順については、284 ページの「属性の指定」を参照してください。
- **「規則」** – 評価されたときに日付 / 時刻文字列を生成する規則に基づいてプロビジョニング解除を保留します。属性を指定するとき、データが従うべき日付形式を指定できます。

  手順については、284 ページの「規則の指定」を参照してください。

2. 「サンセットタスク」メニューを使用して、指定された日時にユーザーをプロビジョニング解除するためのタスクを指定します。
3. このタブの設定を終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

「データ変換」タブの設定

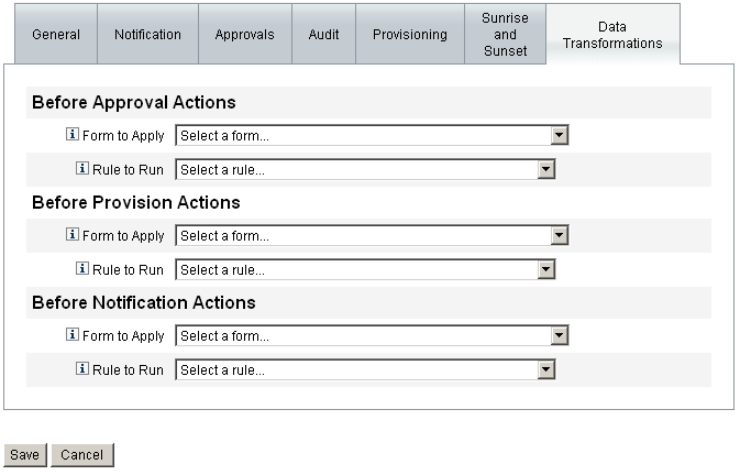
注	このタブはユーザー作成テンプレートおよびユーザー更新テンプレートに対してのみ使用できます。

ワークフローの実行時にユーザーアカウントデータを変更したい場合、「データ変換」タブを使用して、Identity Manager がプロビジョニング中にデータを変換する方法を指定できます。

例としては、企業のポリシーに準拠した電子メールアドレスをフォームまたは規則に生成させたい場合や、サンライズまたはサンセット日付を生成したい場合があります。

「データ変換」タブを選択すると、次のページが表示されます。

図 8-36　「データ変換」タブ : ユーザー作成テンプレート



このページは次のセクションで構成されます。

- **「承認アクション前」**― 指定された承認者に承認リクエストを送信する前にユーザーアカウントデータを変換したい場合、このセクションのオプションを設定します。
- **「プロビジョニングアクション前」**― プロビジョニングアクションの前にユーザーアカウントデータを変換したい場合、このセクションのオプションを設定します。
- **「通知アクション前」**― 指定された受信者に通知が送信される前にユーザーアカウントデータを変換したい場合、このセクションのオプションを設定します。

各セクションで、次のオプションを設定できます。

- **「適用するフォーム」**メニュー ― システムに対して現在設定されているフォームのリストが提示されます。これらのメニューを使用して、ユーザーアカウントからのデータを変換するために使われるフォームを指定します。
- **「実行する規則」**メニュー ― システムに対して現在設定されている規則のリストが提示されます。これらのメニューを使用して、ユーザーアカウントからのデータを変換するために使われる規則を指定します。

このタブの設定を終了したら、次の処理を実行できます。

- 別のタブを選択して、テンプレートの編集を続けます。
- 「保存」をクリックして変更を保存し、「タスクの設定」ページに戻ります。
- 「キャンセル」をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

第 9 章

PasswordSync

この章では、Sun Java™ System Identity Manager の PasswordSync 機能について説明します。この機能を使用すると、Windows クライアントが Windows Active Directory または Windows NT ドメイン内でパスワードを変更し、Identity Manager と変更を同期できるようになります。

説明する内容は次のとおりです。

- PasswordSync の概要
- インストールの前提条件
- PasswordSync のインストール
- PasswordSync の設定
- PasswordSync のデバッグ
- PasswordSync のアンインストール
- PasswordSync の配備
- Sun JMS サーバーを使用した PasswordSync の設定
- PasswordSync のフェイルオーバー配備
- PasswordSync についてのよくある質問

PasswordSync の概要

PasswordSync 機能は、Windows Active Directory および Windows NT ドメイン上で行われたユーザーパスワードの変更を、Identity Manager で定義されているほかのリソースと同期された状態に保ちます。PasswordSync は、Identity Manager と同期されるドメイン内の各ドメインコントローラにインストールする必要があります。PasswordSync は Identity Manager とは別にインストールする必要があります。

PasswordSync をドメインコントローラにインストールすると、コントローラは、Java Messaging Service (JMS) クライアントのプロキシとして機能するサーブレットと通信します。その後、サーブレットが JMS 対応のメッセージキューと通信します。JMS リスナーリソースアダプタはキューからメッセージを削除し、ワークフロータスクを使用してパスワード変更を処理します。ユーザーに割り当てられたすべてのリソース上でパスワードが更新され、SMTP サーバーがユーザーに電子メールを送信し、パスワード変更の状態をユーザーに通知します。

注 パスワード変更は、同期のために Identity Manager サーバーに転送される変更リクエストに対するネイティブのパスワードポリシーと符合する必要があります。提案されたパスワード変更がネイティブのパスワードポリシーと符合しない場合、ADSI はエラーダイアログを表示し、同期データは Identity Manager に送信されません。

インストールの前提条件

PasswordSync 機能は、Windows 2000、Windows 2003、および Windows NT のドメインコントローラ上でのみセットアップできます。Identity Manager と同期されるドメイン内の各ドメインコントローラに PasswordSync をインストールする必要があります。

PasswordSync は JMS サーバーと接続できる必要があります。JMS システムの要件の詳細については、『Sun Java™ System Identity Manager リソースリファレンス』の JMS リスナーリソースアダプタに関する節を参照してください。

加えて、PasswordSync には次の要件があります。

- 各ドメインコントローラに Microsoft .NET 1.1 以降がインストールされている
- 以前のバージョンの PasswordSync は削除する

これらの要件については、以降の各節で詳しく説明します。

Microsoft .NET 1.1 のインストール

PasswordSync を使用するには、Microsoft .NET Framework 1.1 以降をインストールする必要があります。このフレームワークは、Windows 2003 ドメインコントローラを使用している場合にはデフォルトでインストールされています。Windows 2000 または Windows NT ドメインコントローラを使用している場合、次の場所の Microsoft Download Center からツールキットをダウンロードできます。

http://www.microsoft.com/downloads

注

- Microsoft .NET Framework 1.1 の動作には Internet Explorer 5.01 以降を必要とします。(Windows 2000 SP4 に付属の) Internet Explorer 5.0 は使用できません。
- フレームワークツールキットをすばやく見つけるには、「キーワード」検索フィールドに「**`NET Framework 1.1 Redistributable`**」と入力してください。
- ツールキットにより . NET Framework 1.1 がインストールされます。

PasswordSync の以前のバージョンをアンインストールする

新しいバージョンをインストールする前に、以前にインストールした PasswordSync のインスタンスをすべて削除する必要があります。

- 以前にインストールしたバージョンの PasswordSync が `IdmPwSync.msi` インストーラをサポートする場合、Windows の「プログラムの追加と削除」標準ユーティリティーを使用してプログラムを削除できます。
- 以前にインストールしたバージョンの PasswordSync が `IdmPwSync.msi` インストーラをサポートしない場合、InstallAnywhere アンインストーラを使用してプログラムを削除します。

PasswordSync のインストール

ここでは、PasswordSync 設定アプリケーションをインストールする手順について説明します。

注	Identity Manager と同期されるドメイン内の各ドメインコントローラに PasswordSync をインストールする必要があります。

1. Identity Manager のインストールメディアから、`pwsync¥IdmPwSync.msi` アイコンをクリックします。「Welcome」ウィンドウが表示されます。

   インストールウィザードには、次のナビゲーションボタンがあります。

   - 「Cancel」: このボタンをクリックすると、変更を保存せずにいつでもウィザードを終了できます。
   - 「Back」: 1 つ前のダイアログボックスに戻る場合にクリックします。
   - 「Next」: 次のダイアログボックスに進む場合にクリックします。

2. 「Welcome」画面の情報を読み、「Next」をクリックして「Setup Type PasswordSync Configuration」ウィンドウを表示します。
PasswordSync のセットアップ

3. PasswordSync のフルパッケージをインストールする場合は「Typical」または「Complete」をクリックします。インストールするパッケージ内容を変更する場合は「Custom」をクリックします。

4. 「Install」をクリックして製品をインストールします。

   PasswordSync が正常にインストールされたかどうかを示すメッセージが表示されます。

5. 「Finish」をクリックしてインストールプロセスを終了します。

   PasswordSync の設定を開始できるように、「Launch Configuration Application」を必ず選択してください。このプロセスの詳細については、293 ページの「PasswordSync の設定」を参照してください。

注	変更を有効にするにはシステムを再起動する必要がある、というメッセージがダイアログボックスに表示されます。PasswordSync の設定を完了するまでは再起動の必要はありませんが、PasswordSync を実装する前にドメインコントローラを再起動する必要があります。

表 9-1 に、各ドメインコントローラにインストールされるファイルを示します。

表 9-1　ドメインコントローラのファイル

インストールされるコンポーネント	説明
%$INSTALL_DIR$%¥configure.exe	PasswordSync 設定プログラム
%$INSTALL_DIR$%¥configure.exe.manifest	設定プログラムのデータファイル
%$INSTALL_DIR$%¥DotNetWrapper.dll	.NET SOAP 通信を処理する DLL
%$INSTALL_DIR$%¥passwordsyncmsgs.dll	PasswordSync メッセージを処理する DLL
%SYSTEMROOT%¥SYSTEM32¥lhpwic.dll	パスワード通知 DLL。この DLL は Windows の PasswordChangeNotify() 関数を実装する

PasswordSync の設定

インストーラから設定アプリケーションを実行する場合、ウィザード形式の設定画面が表示されます。ウィザードを終了し、以後 PasswordSync 設定アプリケーションを実行するときは、タブの選択によって設定画面を切り替えることができます。

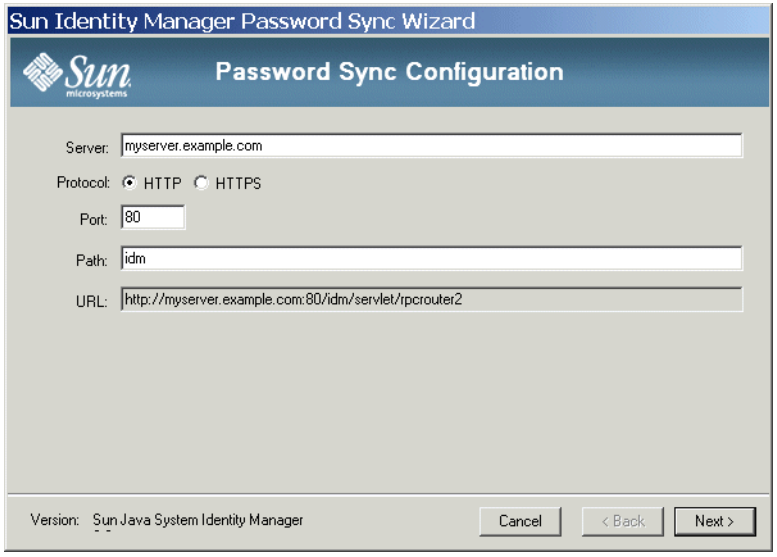
PasswordSync を設定するには、次の手順に従います。

1. まだ実行されていない場合、PasswordSync 設定アプリケーションを開始します。

   デフォルトでは、設定アプリケーションは「すべてのプログラム」> Sun Java System Identity Manager PasswordSync >「設定」でインストールされます。

   PasswordSync 設定ダイアログが表示されます (PasswordSync 参照)。

図 9-1　　PasswordSync 設定ダイアログ

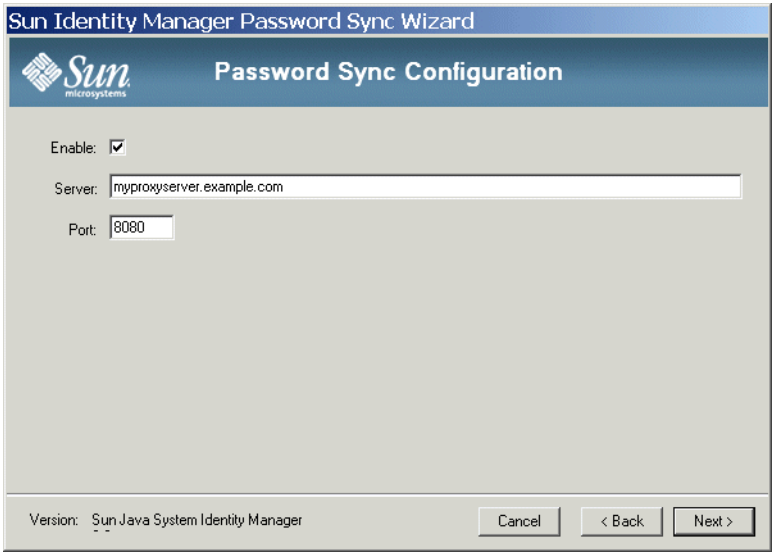


必要に応じてフィールドを編集します。

- 「**Server**」は、Identity Manager がインストールされた完全修飾ホスト名または IP アドレスと置き換える必要があります。
- 「**Protocol**」では、Identity Manager へのセキュア接続を行うかどうかを指定します。「HTTP」を選択した場合、デフォルトのポートは 80 です。「HTTPS」を選択した場合、デフォルトのポートは 443 です。
- 「**Path**」には、アプリケーションサーバー上の Identity Manager へのパスを指定します。
- 「**URL**」の値はほかのフィールドの値を基に生成されます。「URL」フィールドの値は編集できません。

2. 「Next」をクリックして、プロキシサーバーの設定ページを表示します (図 9-2)。

図 9-2　　プロキシサーバーダイアログ

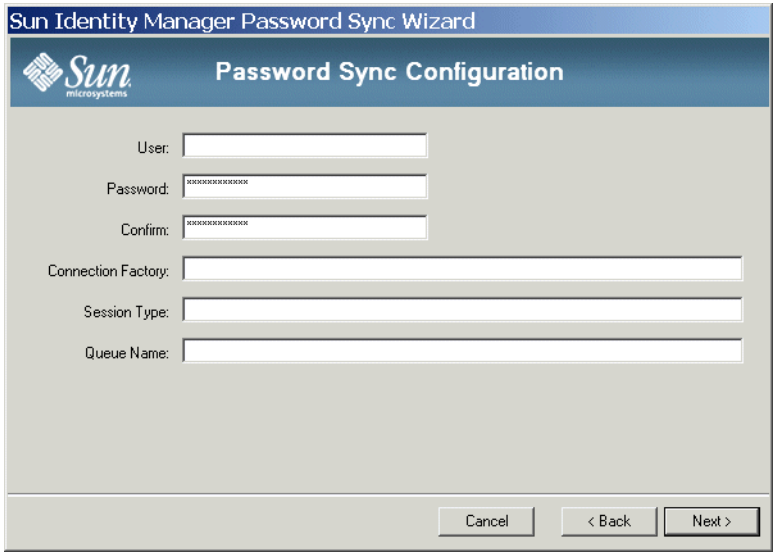


必要に応じてフィールドを編集します。

- プロキシサーバーが必要な場合は「Enable」をクリックします。
- 「Server」は、プロキシサーバーの完全修飾ホスト名または IP アドレスと置き換える必要があります。
- 「Port」：サーバーに対して使用可能なポート番号を指定します。
  (デフォルトのプロキシポートは 8080、デフォルトの HTTPS ポートは 443)。

3. 「Next」をクリックして、JMS 設定ダイアログ (図 9-3) を表示します。

図 9-3　　JMS 設定ダイアログ

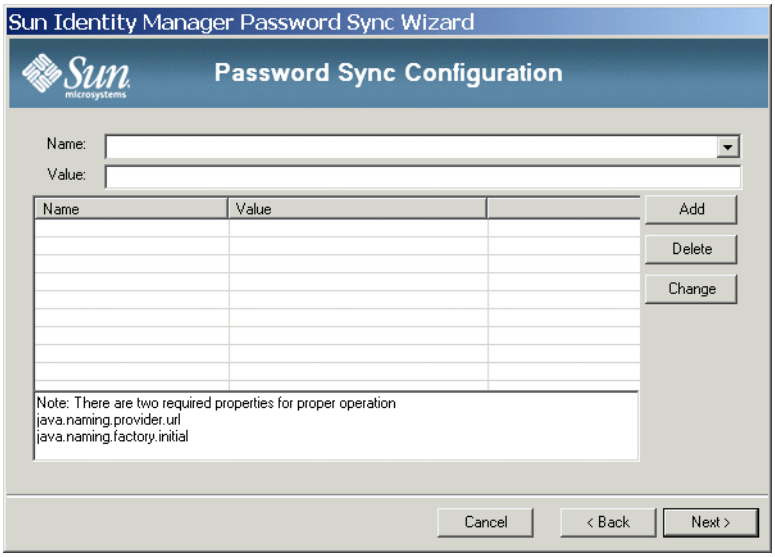


必要に応じてフィールドを編集します。

- 「User」には、新しいメッセージをキューに送る JMS ユーザー名を指定します。
- 「Password」と「Confirm」では、JMS ユーザーのパスワードを指定します。
- 「Connection Factory」には、使用する JMS 接続ファクトリの名前を指定します。JMS システム上にすでに存在しているファクトリを指定する必要があります。
- 「Session Type」はほとんどの場合、ローカルセッショントランザクションが使われることを表す LOCAL に設定することが推奨されます。セッションは各メッセージの受信後にコミットされます。指定できるその他の値は AUTO、CLIENT、および DUPS_OK です。
- 「Queue Name」には、パスワード同期イベントのデスティネーションルックアップ名を指定します。

4. 「Next」をクリックして、JMS プロパティーダイアログ (図 9-4) を表示します。

図 9-4　　JMS プロパティーダイアログ



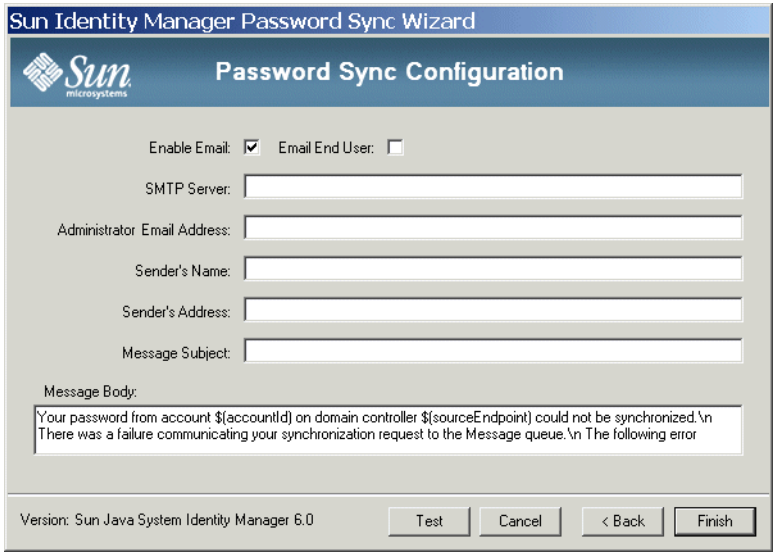
JMS プロパティーダイアログでは、初期 JNDI コンテキストの構築に使われる一連のプロパティーを定義します。次の名前と値のペアを定義する必要があります。

- `java.naming.provider.url` ― 値は JNDI サービスを実行しているマシンの URL に設定する必要があります。
- `java.naming.factory.initial` ― 値は JNDI サービスプロバイダの初期コンテキストファクトリのクラス名 (パッケージを含む) に設定する必要があります。

「名前」プルダウンメニューの内容は、`java.naming` パッケージのクラスの一覧です。クラス名としてクラスまたは型を選択し、「Value」フィールドにその対応する値を入力します。

5. 「Next」をクリックして、電子メールダイアログ (図 9-5) を表示します。

図 9-5　　電子メールダイアログ



電子メールダイアログでは、通信エラーや Identity Manager の外部で発生したその他のエラーが原因でユーザーのパスワード変更が正しく同期されない場合に、電子メール通知を送信するかどうかを設定できます。

必要に応じてフィールドを編集します。

- この機能を有効にするには「Enable Email」を選択します。ユーザーが通知を受け取る場合は「Email End User」を選択します。このオプションを選択しない場合、管理者だけが通知を受け取ります。
- 「SMTP Server」は、障害通知の送信時に使われる SMTP サーバーの完全修飾名または IP アドレスです。
- 「Administrator Email Address」は、通知の送信に使われる電子メールアドレスです。
- 「Sender's Name」は送信者の「フレンドリーネーム」です。
- 「Sender's Address」は送信者の電子メールアドレスです。
- 「Message Subject」には、すべての通知に共通する件名行を指定します。
- 「Message Body」には通知のテキストを指定します。

  メッセージの本文には次の変数を含めることができます。

  - `$(accountId)` ー パスワードを変更しようとしているユーザーのアカウント ID。

- `$(sourceEndpoint)` ― パスワード通知ツールがインストールされたドメインコントローラのホスト名。この情報は、トラブルが発生したマシンの特定に役立ちます。
- `$(errorMessage)` ― エラーが発生したことを説明するエラーメッセージ。

6. 「Finish」をクリックして変更を保存します。

設定アプリケーションの 2 回目以降の実行時には、ウィザードではなく一連のタブで構成される画面が表示されます。設定アプリケーションをウィザード形式で表示したい場合、コマンド行から次のコマンドを入力します。

```
C:¥InstallDir¥Configure.exe -wizard
```

PasswordSync のデバッグ

この節では、PasswordSync で発生する問題の診断に必要な情報の見つけ方と、設定ツールを使用してトレースを有効にする方法について説明します。また、PasswordSync をデバッグしたり、設定ツールからは実装できない機能を有効にしたりするために必要なレジストリキーの一覧を示します。

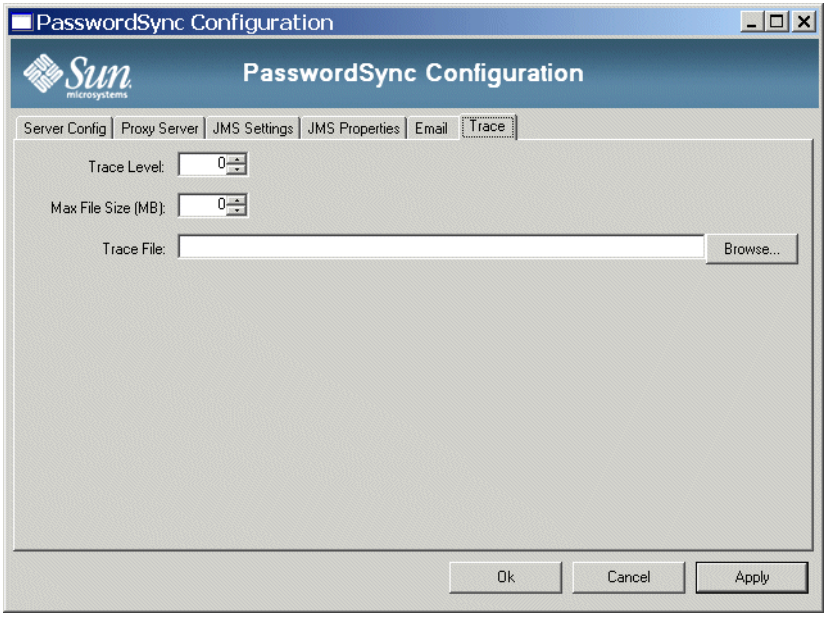
エラーログ

PasswordSync はすべての障害情報を Windows イベントビューアに書き込みます。エラーログエントリのソース名は *PasswordSync* です。

トレースログ

設定ツールを最初に実行するとき、ウィザードにはトレースを設定するためのパネルがありません。ただし、設定ツールの 2 回目以降の実行では、「Trace」タブ (図 9-6) が常に表示されます。

図 9-6　「Trace」タブ



「Trace Level」フィールドでは、PasswordSync がトレースログに書き込む情報の詳細度を指定します。値 0 はトレースが無効であることを表し、値 4 は最も詳細な情報を出力することを表します。

トレースファイルが「Max File Size (MB)」フィールドで指定されたサイズを超えると、PasswordSync はベース名に .bk を追加したファイルにそれまでのログを移動します。たとえば、トレースファイルを C:¥logs¥pwicsvc.log に、トレースファイルの最大サイズを 100M バイトに設定した場合、トレースファイルが 100M バイトを超えると、PasswordSync はそれまでのファイルの名前を C:¥logs¥pwicsvc.log.bk に変更し、以降のデータを新しい C:¥logs¥pwicsvc.log file ファイルに書き込みます。

レジストリキー

表 9-2 に示すレジストリキーは、Windows レジストリエディタを使用して編集できます。これらのキーは次の場所に置かれています。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Waveset¥Lighthouse¥PasswordSync
```

この場所にはその他のキーもありますが、それらのキーは設定ツールを使用して編集できます。

表 9-2　レジストリキー

キー名	種類	説明
allowInvalidCerts	REG_DWORD	1 に設定すると、このキーは .NET クライアント上で次のフラグを設定します。 • SECURITY_FLAG_IGNORE_UNKNOWN_CA • INTERNET_FLAG_IGNORE_CERT_CN_INVALID • INTERNET_FLAG_IGNORE_CERT_DATE_INVALID その結果、期限が切れた証明書や CN またはホスト名が無効な証明書をクライアントが受け入れるようになります。この設定は SSL 使用時にのみ適用されます。 この設定は、ほとんどの証明書が無効な認証局 (CA) から発行されるテスト環境でデバッグを行なっているときに役立ちます。 デフォルトは 0 です。
clientConnectionFlags	REG_DWORD	.NET SOAP クライアントに渡されるオプションの接続フラグ。 デフォルトは 0 です。
clientSecurityFlags	REG_DWORD	.NET SOAP クライアントに渡すことができるオプションのセキュリティーフラグ。 デフォルトは 0 です。
installdir	REG_SZ	PasswordSync アプリケーションがインストールされたディレクトリ。
soapClientTimeout	REG_DWORD	SOAP クライアントが Identity Manager サーバーと通信してエラーが発生するまでのタイムアウト時間 (ミリ秒)。

PasswordSync のアンインストール

PasswordSync アプリケーションをアンインストールするには、Windows のコントロールパネルから「アプリケーションの追加と削除」を選択します。次に、「Sun Java System Identity Manager PasswordSync」を選択して「削除」をクリックします。

注	PasswordSync は、Identity Manager のインストールメディアをロードし、`pwsync¥IdmPwSync.msi` アイコンをクリックしてアンインストール (または再インストール) することもできます。

アンインストールを完了するにはシステムを再起動する必要があります。

PasswordSync の配備

PasswordSync を配備するには、Identity Manager で次の作業を行う必要があります。

- JMS リスナーアダプタを設定する
- ユーザーパスワード同期ワークフローを実装する
- 通知を設定する

JMS リスナーアダプタの設定

メッセージがドメインコントローラによって間接的にキューに配置されたら、それらのメッセージを受け入れるためにリソースアダプタを設定する必要があります。JMS リスナーリソースアダプタを作成し、キューと通信するようにそのアダプタを設定する必要があります。このアダプタの設定の詳細については、『Sun Java™ System Identity Manager リソースリファレンス』を参照してください。

次のリソースパラメータを設定する必要があります。

- **「宛先タイプ」** ― 通常、この値はキューに設定されます。1 人の加入者が存在し、また複数の発行者が存在する可能性があるため、トピックは通常は関係しません。
- **「初期コンテキスト JNDI のプロパティー」** ― このテキストボックスでは、初期 JNDI コンテキストの構築に使われる一連のプロパティーを定義します。次の名前と値のペアを定義する必要があります。
  - `java.naming.provider.url` ― 値は JNDI サービスを実行しているマシンの URI に設定する必要があります。

- java.naming.factory.initial − 値は JNDI サービスプロバイダの初期コンテキストファクトリのクラス名 (パッケージを含む) に設定する必要があります。

追加のプロパティーの定義が必要な場合があります。プロパティーと値のリストは、設定アプリケーションの JMS 設定ページで指定するものと一致することが推奨されます。

- **「接続ファクトリの JNDI 名」** − 接続ファクトリの名前 (JMS サーバー上で定義されたもの)。
- **「ユーザー」**および**「パスワード」** − キューから新しいイベントをリクエストする管理者のアカウント名とパスワード。
- **「Reliable Messaging サポート」** − LOCAL (ローカルトランザクション) を選択します。それ以外のオプションはパスワード同期には使用しません。
- **「メッセージマッピング」** − 「java:com.waveset.adapter.jms.PasswordSyncMessageMapper」を入力します。このクラスは、JMS サーバーからのメッセージを、ユーザーパスワード同期ワークフローで使用できる形式に変換します。

ユーザーパスワード同期ワークフローの実装

デフォルトのユーザーパスワード同期ワークフローは、JMS リスナーアダプタから送られてくる個々のリクエストを受け取ってチェックアウトし、ChangeUserPassword ビューアに戻します。チェックインが完了したあと、ワークフローはすべてのリソースアカウントに対して処理を繰り返し、ソースリソースを除くすべてのリソースを選択します。Identity Manager は、すべてのリソースに対してパスワード変更が成功したかどうかを電子メールでユーザーに通知します。

ユーザーパスワード同期ワークフローのデフォルト実装を使用する場合、JMS リスナーアダプタインスタンスの処理規則にその実装を割り当てます。処理規則はアダプタの ActiveSync ウィザードで割り当てることができます。

デフォルトのユーザー同期パスワードワークフローを変更したい場合、$WSHOME/sample/wfpwsync.xml ファイルをコピーして変更を行います。その後、変更したワークフローを Identity Manager にインポートします。

デフォルトのワークフローに対して行うことが考えられる変更には、次のようなものがあります。

- パスワードが変更されたときに通知を受けるエントリ
- Identity Manager アカウントが見つからない場合に行う処理
- ワークフロー内でリソースを選択する方法
- Identity Manager からのパスワード変更を許可するかどうか

ワークフローの使用方法の詳細については、『Sun Java™ System Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

通知の設定

Identity Manager には、パスワード同期通知およびパスワード同期失敗通知の電子メールテンプレートが用意されています。これらのテンプレートは、複数のリソースに対するパスワード変更の試みが成功したかどうかをユーザーに知らせます。

さらに補助が必要な場合にユーザーが従うべき手順について、企業ごとに異なる情報を提供するために、どちらのテンプレートも更新することが推奨されます。143 ページの「電子メールテンプレートのカスタマイズ」を参照してください。

Sun JMS サーバーを使用した PasswordSync の設定

Identity Manager では、信頼性を高め配信を保証するために、パスワードの変更イベントを JMS メッセージサーバーのキューに入れる JMS リスナーアダプタが用意されています。

注	このアダプタの詳細については、『Sun Java™ System Identity Manager リソースリファレンス』を参照してください。

この節では、シナリオ例を使用しながら、Sun JMS サーバーを使用した PasswordSync の設定手順について説明します。説明する内容は次のとおりです。

- 概要
- 管理オブジェクトの作成と格納
- 設定のデバッグ

概要

ここでは、シナリオ例、Windows PasswordSync ソリューション、および JMS ソリューションについて説明します。

シナリオ例

JMS サーバーを使用して PasswordSync を設定する一般的な (単純な) 方法は、ユーザーが Windows 上で自身のパスワードを変更して、Identity Manager で新しいパスワードを発行し、Sun Directory Server 上で新しいパスワードを使用してユーザーアカウントを更新するというものです。

このシナリオで構成された環境は次のとおりです。

- Windows Server 2003 Enterprise Edition − Active Directory
- Sun Java™ System Identity Manager 6.0 2005Q4M3
- Suse Linux 10.0 上で稼働する MySQL 4.1.13
- Suse Linux 10.0 上で稼働する Tomcat 5.0.28
- Suse Linux 10.0 上で稼働する Sun Java™ System Message Queue 3.6 SP3 2005Q4
- Suse Linux 10.0 上で稼働する Sun Java™ System Directory Server 5.2 SP4
- Java 1.4.2

JMS と JNDI を有効にするために、次のファイルが Tomcat の `common/lib` ディレクトリにコピーされました。

- `jms.jar` (Sun Message Queue から)
- `fscontext.jar` (Sun Message Queue から)
- `imq.jar` (Sun Message Queue から)
- `jndi.jar` (Java JDK から)

ソリューションの概要

Windows PasswordSync ソリューションで動作するすべてのコンポーネントを分析するときには、次の処理が行われます。

1. ユーザーがワークステーション上で自身のパスワードを変更すると、PasswordSync はパスワードの変更を現在の Active Directory ドメインコントローラに送信し、Identity Manager パスワードキャプチャー `dll` (ドメインコントローラ上に常駐) がクリアテキストのパスワードを取得します。
2. このパスワードキャプチャー `dll` は、Identity Manager SOAP リクエストハンドラへ SOAP リクエストを発行します。

ユーザー ID、暗号化パスワード、必要な JMS 設定情報が、この SOAP リクエストにカプセル化されます。次に例を示します。

コード例 9-1 SOAP リクエスト例

```
POST /idm/servlet/rpcrouter2 HTTP/1.0
Accept: text/*
SOAPAction: "urn:lighthouse"
Content-Type: text/xml; charset=utf-8
User-Agent: VCSoapClient
Host: 192.168.1.4:8080
Content-Length: 1154
Connection: Keep-Alive
Pragma: no-cache
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
<soap:Body soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<snp:queuePasswordUpdate xmlns:snp="urn:lighthouse">
<userEmailAddress xsi:nil="1"/>
<resourceAccountId>CN=John Smith,OU=people,DC=org,DC=local</resourceAccountId>
<resourceAccountGUID>b4e1c14b79d3a949a618a607dde7784d</resourceAccountGUID>
<password>zkpS8qcIJkVBWa/Frp+JqA==</password>
<accounts xsi:nil="1"/>
<resourcename xsi:nil="1"/>
<resourcetype>Windows Active Directory</resourcetype>
<clientEndpoint>W2003EE</clientEndpoint>
<jmsUser>guest</jmsUser>
<jmsPassword>guest</jmsPassword>
<queueName>cn=pwsyncDestination</queueName>
<connectionFactory>cn=pwsyncFactory</connectionFactory>
<sessionType>LOCAL</sessionType>
<JNDIProperties>java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;java.naming.
   provider.url=ldap://gwenig.coopsrccom:389/ou=sunmq,dc=coopsrc,dc=com</JNDIProperties>
<singleResult>true</singleResult>
</snp:queuePasswordUpdate>
</soap:Body>
</soap:Envelope>
```

3. SOAP ハンドラはリクエストを受信し、リクエストに含まれる JMS パラメータを使用して JMS Message Queue Broker への接続を開始します。続いて SOAP ハンドラは、ユーザー ID と暗号化パスワード (および後述するその他のパラメータ) を含んだメッセージを送信します。

   たとえば、Message Queue Broker 上の SOAP ハンドラは、次のような (タイプ *MapMessage* の) メッセージを送信します。

コード例 9-2 SOAP ハンドラのメッセージ

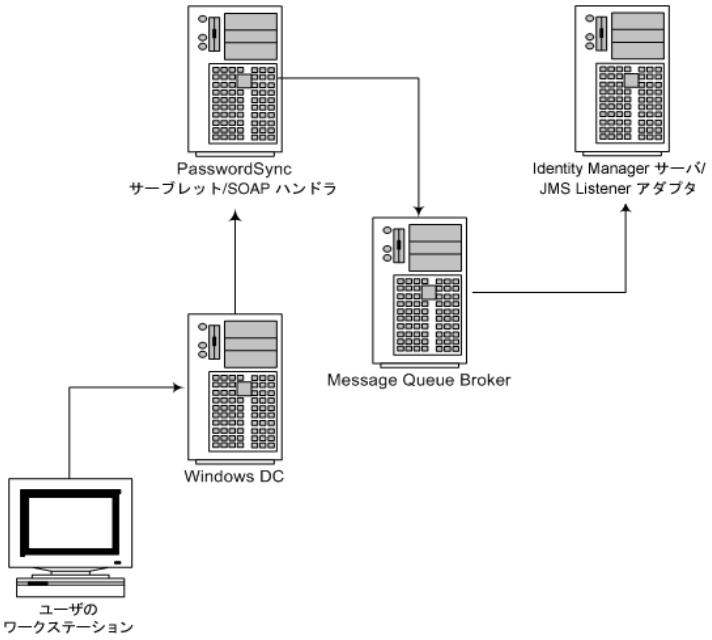
```
password: zkpS8qcIJkVBWa/Frp+JqA==
accounts: null
resourceAccountGUID: 8f245d1490de7a4192a8821c569c9ac4
requestTimestamp: 1143639284325
queueName: cn=pwsyncDestination
jmsUser: guest
resourcetype: Windows Active Directory
resourcename: null
JNDIProperties:
java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;
java.naming.provider.url=ldap://gwenig.coopsrc.com:389/
ou=sunmq,dc=coopsrc,dc=com
connectionFactory: cn=pwsyncFactory
clientEndpoint: W2003EE
userEmailAddress: null
sessionType: LOCAL
jmsPassword: guest
resourceAccountId: CN=John Smith,OU=people,DC=org,DC=local
```

4. Message Queue Broker がメッセージをキューに入れ、JMS リスナーアダプタがメッセージを受信します。これで Identity Manager はワークフローを開始できます。

   図 9-7 に、このシナリオ例で使用した構成を示します。

注	この図では、SOAP ハンドラと Identity Manager が別々のサーバーに配置されていますが、同一のサーバーで両方を実行することもできます。

図 9-7　　シナリオの構成



JMS の概要

Java Message Service (JMS) API は、(Java 2 Platform, Enterprise Edition (J2EE) に基づいた) アプリケーションコンポーネントでメッセージの作成、送信、受信、および読み込みを行えるようにするメッセージング標準です。この API により、疎結合され、信頼性が高く、非同期の分散型通信が可能になります。

メッセージを送信または受信するには、JMS クライアントはまず JMS プロバイダに接続する必要があります。JMS プロバイダは多くの場合メッセージブローカとして実装されます。この接続により、クライアントとブローカ間の通信チャネルが開きます。次にクライアントは、メッセージを作成、生成、および消費するためにセッションをセットアップする必要があります。

JMS では、次のメッセージ要素を完全には定義していません。

- **接続ファクトリ** – 接続ファクトリ管理対象オブジェクトは、ブローカへのクライアント接続を生成します。これらのオブジェクトは、接続処理、クライアント識別、メッセージヘッダーの上書き、信頼性、フローコントロールなど、メッセージング動作の特定の側面を制御するプロバイダ固有の情報をカプセル化します。特定の接続ファクトリから派生するすべての接続は、そのファクトリに設定された動作を行います。

- **デスティネーション** – デスティネーション管理のオブジェクトは、ブローカ上の物理的なデスティネーションを参照します。これらのオブジェクトは、プロバイダ固有の命名 (アドレス構文) 規則をカプセル化し、この規則によって、使用されるデスティネーションのメッセージングドメインがキューかトピックに指定されます。

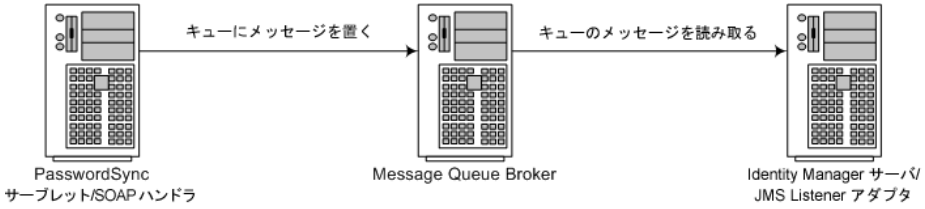
これら 2 つのオブジェクトは、プログラムによって作成されるのではなく、通常は管理ツールを使用して作成および設定されます。続いて、これらのオブジェクトはオブジェクトストアに格納され、標準 JNDI ルックアップを介して JMS クライアントからアクセスされます。

注 接続ファクトリとデスティネーションの詳細については、次のサイトにアクセスして『Sun Java™ System Message Queue 技術の概要』を参照してください。

http://docs.sun.com/source/819-3564/intro.html

図 9-8 に、このシナリオ例の通信フローを示します。

図 9-8 シナリオの通信フロー



SOAP ハンドラは、Windows パスワードキャプチャー dll からリクエストを受信すると、プロキシとして動作して、SOAP リクエストを JMS メッセージに変換します。次に JMS リスナーアダプタがメッセージを受信して、適切なワークフローをトリガーします。

JMS ブローカを操作するには、Identity Manager SOAP ハンドラと Identity Manager JMS リスナーアダプタの両方に、接続ファクトリとデスティネーション (JNDI を使用してルックアップ) が必要になります。

Identity Manager SOAP ハンドラは、必要な詳細を SOAP メッセージに組み込みます (前図参照)。

コード例 9-3 SOAP メッセージ

```
<jmsUser>guest</jmsUser>
<jmsPassword>guest</jmsPassword>
<queueName>cn=pwsyncDestination</queueName>
```

コード例 9-3　　SOAP メッセージ (続き)

```
<connectionFactory>cn=pwsyncFactory</connectionFactory>
<sessionType>LOCAL</sessionType>
<JNDIProperties>java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory;java.naming.
  provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com</JNDIProperties>
```

次のパラメータ (図 9-9 および図 9-10 参照) はすべて、Windows に PasswordSync をインストールおよび設定するときに用意されます。

図 9-9　　「JMS Settings」タブ

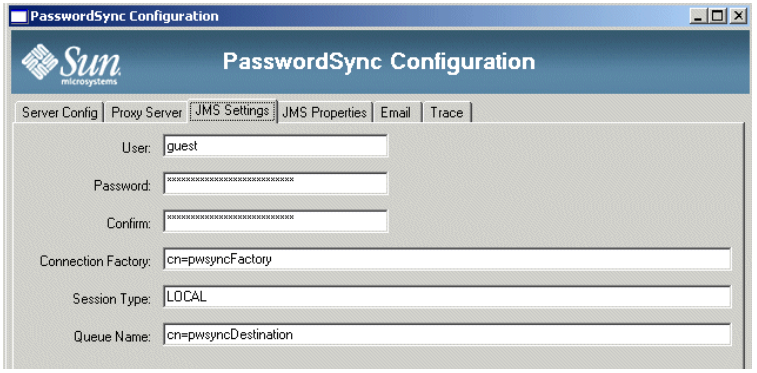
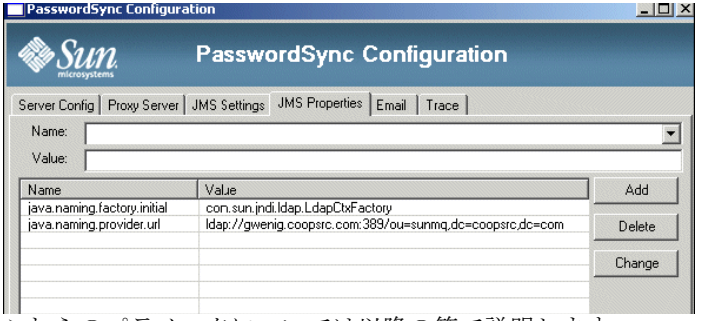


図 9-10　　「JMS Properties」タブ



これらのパラメータについては以降の節で説明します。

- JMS 設定パラメータ
- JMS プロパティーのパラメータ

JMS 設定パラメータ

「JMS Settings」タブには次のパラメータが含まれます。

- 「User」および「Password」フィールド : JMS ブローカへの接続時に使用する資格を定義します。
- 「Connection Factory」フィールド : 接続ファクトリオブジェクトの JNDI ルックアップ名を指定します。
- 「Session Type」フィールド : 指定します。
- 「Queue Name」フィールド : デスティネーションオブジェクトの JNDI ルックアップ名を指定します。

コード例 9-4 では、「Connection Factory」および「Queue Name」は LDAP RDN です。これは (`java.naming.provider.url` と組み合わされると) 完全な DN になります。単純な `ldapsearch` は、管理オブジェクトエントリを示します。

コード例 9-4 接続ファクトリとキュー名の例

```
Connection Factory:
#> ldapsearch -h gwenig.coopsrc.com -b 'dc=coopsrc,dc=com' 'cn=pwsyncfactory'
dn: cn=pwsyncFactory,ou=sunmq,dc=coopsrc,dc=com
objectClass: top
objectClass: javaContainer
objectClass: javaObject
objectClass: javaNamingReference
javaClassName: com.sun.messaging.QueueConnectionFactory
javaFactory: com.sun.messaging.naming.AdministeredObjectFactory
javaReferenceAddress: #0#version#3.0
javaReferenceAddress: #1#readOnly#false
javaReferenceAddress: #2#imqOverrideJMSPriority#false
javaReferenceAddress: #3#imqConsumerFlowLimit#1000
javaReferenceAddress: #4#imqAddressListIterations#1
javaReferenceAddress: #5#imqOverrideJMSExpiration#false
javaReferenceAddress: #6#imqConnectionType#TCP
javaReferenceAddress: #7#imqLoadMaxToServerSession#true
javaReferenceAddress: #8#imqPingInterval#30
javaReferenceAddress: #9#imqSetJMSXUserID#false
javaReferenceAddress: #10#imqConfiguredClientID#
javaReferenceAddress: #11#imqSSLProviderClassname#com.sun.net.ssl.internal.ssl.Provider
javaReferenceAddress: #12#imqJMSDeliveryMode#PERSISTENT
javaReferenceAddress: #13#imqConnectionFlowLimit#1000
javaReferenceAddress: #14#imqConnectionURL#http://localhost/imq/tunnel
javaReferenceAddress: #15#imqBrokerServiceName#
javaReferenceAddress: #16#imqJMSPriority#4
javaReferenceAddress: #17#imqBrokerHostName#localhost
javaReferenceAddress: #18#imqJMSExpiration#0
javaReferenceAddress: #19#imqAckOnProduce#
javaReferenceAddress: #20#imqEnableSharedClientID#false
javaReferenceAddress: #21#imqAckTimeout#0
javaReferenceAddress: #22#imqAckOnAcknowledge#
```

コード例 9-4 接続ファクトリとキュー名の例 (続き)

```
javaReferenceAddress: #23#imqConsumerFlowThreshold#50
javaReferenceAddress: #24#imqDefaultPassword#guest
javaReferenceAddress: #25#imqQueueBrowserMaxMessagesPerRetrieve#1000
javaReferenceAddress: #26#imqDefaultUsername#guest
javaReferenceAddress: #27#imqReconnectEnabled#false
javaReferenceAddress: #28#imqConnectionFlowCount#100
javaReferenceAddress: #29#imqAddressListBehavior#PRIORITY
javaReferenceAddress: #30#imqReconnectAttempts#0
javaReferenceAddress: #31#imqSetJMSXAppID#false javaReferenceAddress:
#32#imqConnectionHandler#com.sun.messaging.jmq.jmsclient.protocol.
tcp.TCPStreamHandler
javaReferenceAddress: #33#imqSetJMSXRcvTimestamp#false
javaReferenceAddress: #34#imqBrokerServicePort#0
javaReferenceAddress: #35#imqDisableSetClientID#false
javaReferenceAddress: #36#imqSetJMSXConsumerTXID#false
javaReferenceAddress: #37#imqOverrideJMSDeliveryMode#false
javaReferenceAddress: #38#imqBrokerHostPort#7676
javaReferenceAddress: #39#imqQueueBrowserRetrieveTimeout#60000
javaReferenceAddress: #40#imqSSLIsHostTrusted#true
javaReferenceAddress: #41#imqSetJMSXProducerTXID#false
javaReferenceAddress: #42#imqConnectionFlowLimitEnabled#false
javaReferenceAddress: #43#imqReconnectInterval#3000
javaReferenceAddress: #44#imqAddressList#mq://gwenig:7676/jms
javaReferenceAddress: #45#imqOverrideJMSHeadersToTemporaryDestinations#false
cn: pwsyncFactory
```

デスティネーションは次のようになります。

コード例 9-5 デスティネーションの例

```
#> ldapsearch -h gwenig.coopsrc.com -b 'dc=coopsrc,dc=com' 'cn=pwsyncdestination'
dn: cn=pwsyncDestination,ou=sunmq,dc=coopsrc,dc=com
objectClass: top
objectClass: javaContainer
objectClass: javaObject
objectClass: javaNamingReference
javaClassName: com.sun.messaging.Queue
javaFactory: com.sun.messaging.naming.AdministeredObjectFactory
javaReferenceAddress: #0#version#3.0
javaReferenceAddress: #1#readOnly#false
javaReferenceAddress: #2#imqDestinationName#pwsyncQueue
javaReferenceAddress: #3#imqDestinationDescription#A Description for the Destination Object
cn: pwsyncDestination
```

JMS プロパティーのパラメータ

シナリオ例では、接続ファクトリおよびデスティネーションオブジェクトは LDAP ディレクトリに置かれています。`java.naming.factory.initial` は、初期 JNDI コンテキストの作成に使用されるファクトリクラス値です。`java.naming.provider.url` は、使用されているサービスプロバイダの設定情報の指定に使用される環境プロパティーの名前を保持します。詳細を指定しない場合は、PasswordSync は匿名 LDAP セッションを使用して、接続ファクトリおよびデスティネーションオブジェクトを検出します。

資格およびバインドメソッドを提供するには、次のプロパティーを指定します。

- `java.naming.security.principal`: Bind DN (例 : cn=Directory manager)
- `java.naming.security.authentication`: Bind method (例 : simple)
- `java.naming.security.credentials`: Password

注 JMS リスナーアダプタに対してこれらと同じ設定を定義する必要があります。

図 9-11 「JMS リスナーリソースパラメータ」ページ

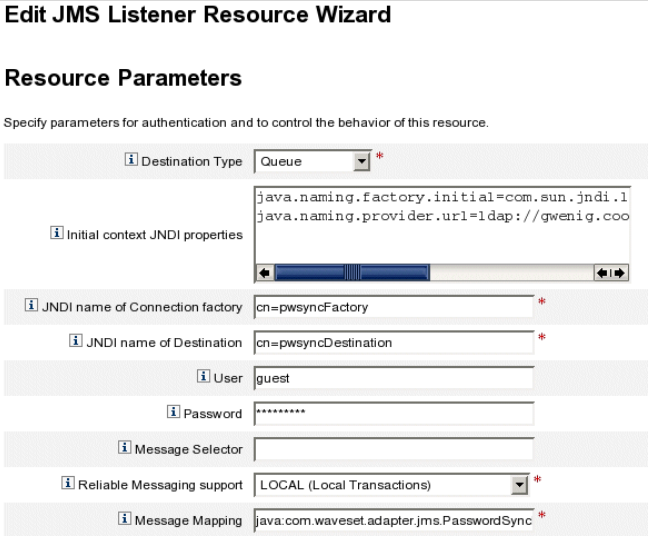
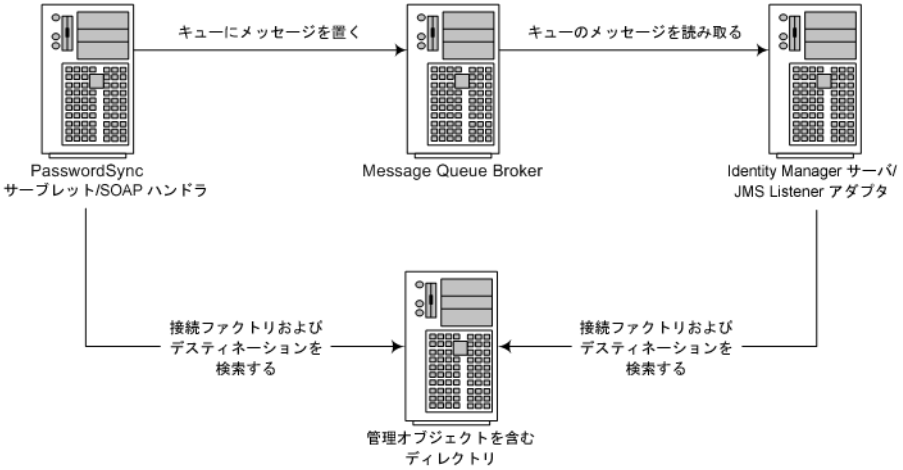


図 9-12 に詳細なプロセスを示します。

図 9-12　接続ファクトリおよびデスティネーションオブジェクトの検出



SOAP ハンドラと JMS リスナーアダプタは、メッセージの送受信を行うために、接続ファクトリおよびデスティネーションを検索する必要があります。

管理オブジェクトの作成と格納

ここでは、次の管理オブジェクトの作成および格納手順について説明します。この手順はシナリオ例が正しく機能するために必要です。

- 接続ファクトリオブジェクト
- デスティネーションオブジェクト

注

- ここでの手順では、Sun Java™ System Message Queue がインストールされていることを前提にしています。必要なツールは、Message Queue インストールメディアの `bin/` ディレクトリにあります。
- これらの管理オブジェクトの作成には、Message Queue 管理 GUI (`imqadmin`) かコマンド行ツール (`imqobjmgr`) のどちらかを使用できます。以下の手順ではコマンド行ツールを使用します。

LDAP ディレクトリでの管理オブジェクトの格納

ここでは、LDAP ディレクトリに接続ファクトリオブジェクトを格納するために必要なコマンドを示します。

接続ファクトリオブジェクトの格納

接続ファクトリオブジェクトを格納するには、コード例 9-6 のコマンドを使用します。

コード例 9-6 接続ファクトリオブジェクトの格納

```
#> ./imqobjmgr add -l "cn=mytestFactory"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t qf
-o "imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false

Using the following lookup name:
cn=mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager
Object successfully added.
```

ただし、`imqAddressList` は、JMS サーバー / ブローカのホスト名 (`gwenig.coopsrc.com`)、ポート (`7676`)、およびアクセスメソッド (`jms`) を定義します。

デスティネーションオブジェクトの格納

デスティネーションオブジェクトを格納するには、コード例 9-7 のコマンドを使用します。

コード例 9-7 デスティネーションオブジェクトの格納

```
#> ./imqobjmgr add -l "cn=mytestDestination"
-j "java.naming.factory.initial=com.sun.jndi.ldap.LdapCtxFactory"
-j "java.naming.provider.url=ldap://gwenig.coopsrc.com:389/ou=sunmq,dc=coopsrc,dc=com"
-j "java.naming.security.principal=cn=directory manager"
-j "java.naming.security.credentials=password"
-j "java.naming.security.authentication=simple"
-t q
-o "imqDestinationName=mytestDestination"
```

コード例 9-7 デスティネーションオブジェクトの格納 (続き)

```
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] mytestDestination
Using the following lookup name:
cn=mytestDestination
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.ldap.LdapCtxFactory
java.naming.provider.url ldap://gwenig.coopsrc.com:389/
    ou=sunmq,dc=coopsrc,dc=com
java.naming.security.authentication simple
java.naming.security.credentials netscape
java.naming.security.principal cn=directory manager
Object successfully added.
```

注 ldapsearch または LDAP ブラウザを使用して、新たに作成したオブジェクトをチェックできます。

ファイルでの管理オブジェクトの格納

ここでは、コマンド行ツールを使用して、ファイルに管理オブジェクトを格納する方法について説明します。

接続ファクトリオブジェクトの格納

コード例 9-8 に、接続ファクトリオブジェクトを格納し、ルックアップ名を指定するために必要なコマンドを示します。

コード例 9-8 接続ファクトリオブジェクトの格納とルックアップ名の指定

```
#> ./imqobjmgr add -l "mytestFactory" -j "java.naming.factory.initial=
com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t qf -o
"imqAddressList=mq://gwenig.coopsrc.com:7676/jms"
Adding a Queue Connection Factory object with the following attributes:
imqAckOnAcknowledge [Message Service Acknowledgement of    Client Acknowledgements]
...
imqSetJMSXUserID [Enable JMSXUserID Message Property] false
Using the following lookup name:
mytestFactory
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
```

コード例 9-8 接続ファクトリオブジェクトの格納とルックアップ名の指定 (続き)

```
Object successfully added.
To specify a destination:
#> ./imqobjmgr add -l "mytestQueue" -j
"java.naming.factory.initial=com.sun.jndi.fscontext.RefFSContextFactory"
-j "java.naming.provider.url=file:///home/gael/tmp" -t q -o
   "imqDestinationName=myTestQueue"
Adding a Queue object with the following attributes:
imqDestinationDescription [Destination Description] A Description for the Destination
Object imqDestinationName [Destination Name] myTestQueue
Using the following lookup name:
mytestQueue
The object's read-only state: false
To the object store specified by:
java.naming.factory.initial com.sun.jndi.fscontext.RefFSContextFactory
java.naming.provider.url file:///home/gael/tmp
Object successfully added.
```

ブローカでのデスティネーションの作成

Sun Java System Message Queue ブローカでは、デフォルトでキューデスティネーションの自動作成が有効になっています (`config.properties` を参照。ただし、`imq.autocreate.queue` のデフォルト値は `true`)。

キューデスティネーションが自動的に作成されない場合、コード例 9-9 に示すコマンドを使用して、ブローカ上でデスティネーションオブジェクトを作成する必要があります (ただし、*myTestQueue* はデスティネーション)。

コード例 9-9 ブローカでのデスティネーションオブジェクトの作成

```
name (Queue name):
#> cd /opt/sun/mq/bin
#>./imqcmd create dst -t q -n mytestQueue
Username: <admin>
Password: <admin>
Creating a destination with the following attributes:
Destination Name mytestQueue
Destination Type Queue
On the broker specified by:
-------------------------
Host Primary Port
-------------------------
localhost 7676
Successfully created the destination.
```

ディレクトリまたはファイルに管理オブジェクトを格納できます。

- **ディレクトリの場合** : Identity Manager SOAP ハンドラと Identity Manager サーバーを同一のサーバーで実行していない Identity Manager 配備の場合は、ディレクトリを使用した方法により、接続ファクトリオブジェクトとデスティネーションオブジェクトを一元的に格納することができます。

  ディレクトリを使用する場合、これらの管理オブジェクトはディレクトリエントリとして格納されます。

注	Identity Manager SOAP ハンドラと Identity Manager サーバーが同一のマシンに置かれていない場合は、それぞれから `.bindings` ファイルにアクセスできる必要があります。管理オブジェクトの作成をマシンごとに繰り返すことも、`.bindings` ファイルを各マシンの適切な場所にコピーすることもできます。

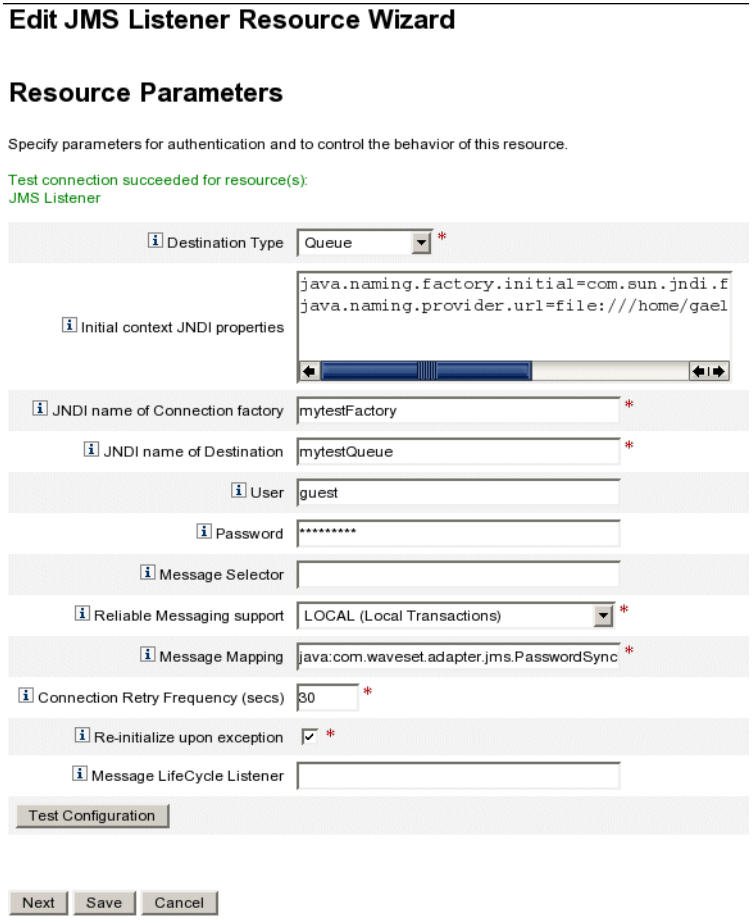
- **ファイルの場合** : Identity Manager SOAP ハンドラと Identity Manager サーバーの両方が同一のサーバー上で実行しているか、ディレクトリが使用可能でない場合は、ファイルに管理オブジェクトを格納できます。

  ファイルを使用する場合、両方の管理オブジェクトは、java.naming.provider.url に対して指定したディレクトリ (たとえば Windows では `file:///c:/temp`、Unix では `file:///tmp`) の下の、単一のファイル (Windows と Unix の両方で `.bindings` と呼ばれる) に格納されます。

このシナリオに対する JMS リスナーアダプタの設定

JMS リスナーアダプタ設定の最初のページは図 9-13 と同じように表示されます。

図 9-13 「JMS リスナーアダプタリソースパラメータ」ページ

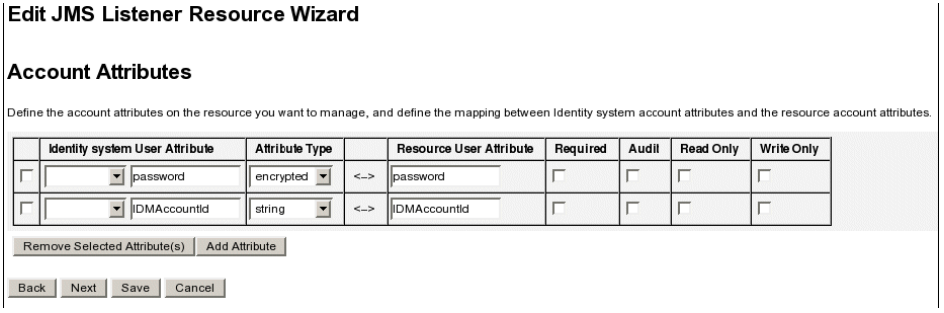


JMS リスナーアダプタを設定するには、次の手順に従います。

1. 「メッセージマッピング」フィールドで、**`java:com.waveset.adapter.jms.PasswordSyncMessageMapper`** を指定して、ユーザーパスワード同期ワークフローで使用できるフォーマットに着信 JMS メッセージを変換します。
2. このシナリオの場合、次の属性 (`PasswordSyncMessageMapper` によって JMS Lister アダプタで使用可能になる) をマップします。
   - IDMAccountId: この属性は、JMS メッセージで渡される `resourceAccountId` 属性と `resourceAccountGUID` 属性に基づいて、PasswordSyncMessageMapper によって解釈処理されます。

- password: 暗号化パスワードは、SOAP リクエストで受信され、JMS メッセージで転送されます。

図 9-14　IDMAccountID とパスワードアカウント属性のマッピング



スキーママップでこれらの属性フィールドを設定すると、ActiveSync ウィザードの「属性マッピング」セクションのリソースで属性を使用できるようになります (図 9-15)。

注　ここではアイデンティティーテンプレートは提供されません。

図 9-15　ActiveSync 属性マッピング

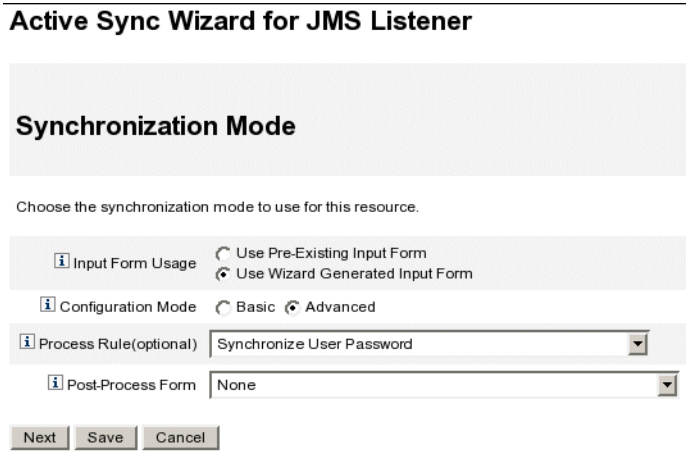
ActiveSync の設定

詳細設定モードで JMS リスナー用の ActiveSync ウィザードを使用して、このシナリオに合わせて ActiveSync を設定します。

1. 「同期モード」画面が表示されたら (図 9-16)、パラメータをデフォルト値の設定のままにし、「次へ」をクリックして続行できます。

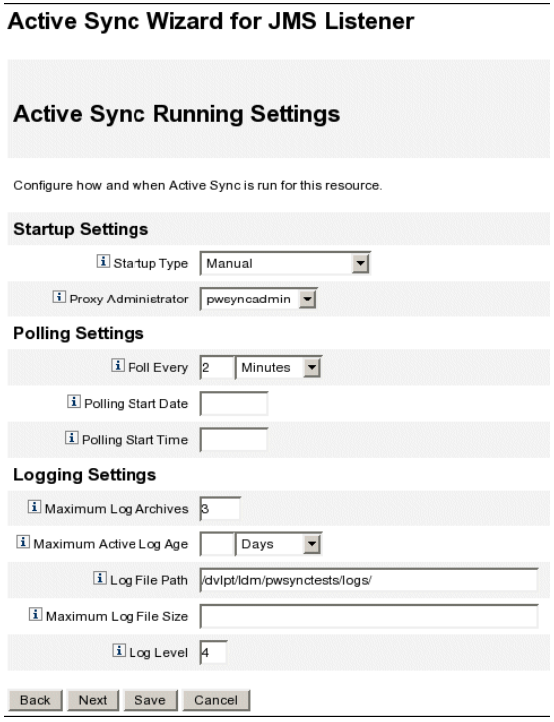
デフォルトのユーザーパスワード同期ワークフローは、JMS リスナーアダプタから送られてくる個々のリクエストを受け取って、ChangeUserPassword ビューアをチェックアウトしてから、ChangeUserPassword ビューアに再度チェックインします。

図 9-16　「同期モード」画面



2. 「ActiveSync の動作設定」パネルが表示されたら、空のフォームに関連付けられたプロキシ管理者 (pwsyncadmin) を定義する必要があります。

図 9-17 「ActiveSync の動作設定」パネル



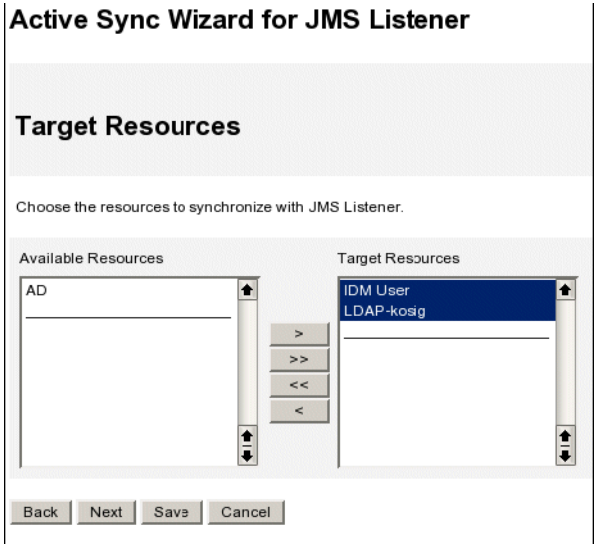
3. デバッグのために、ログレベルを **4** に設定し、ログファイルパスを指定して、特定のディレクトリに詳細ログファイルを生成します。

   たとえば、図 9-17 に示したログファイルは、`/dvlpt/Idm/pwsynctests/logs/` ディレクトリに保存されます。

4. 終了したら、「次へ」をクリックして続行します。

5. 次の 2 つの ActiveSync ウィザードパネルではデフォルト値を変更しないでください。「ターゲットリソース」画面が表示されるまで (図 9-18)、「次へ」をクリックするだけです。

図 9-18　「ターゲットリソース」画面



6. 「ターゲットリソース」選択ツールを使用して、ターゲットリソースを指定します。「利用可能なリソース」リストからリソースを選択し > 、ボタンをクリックして、リソースを「ターゲットリソース」リストに移動します。

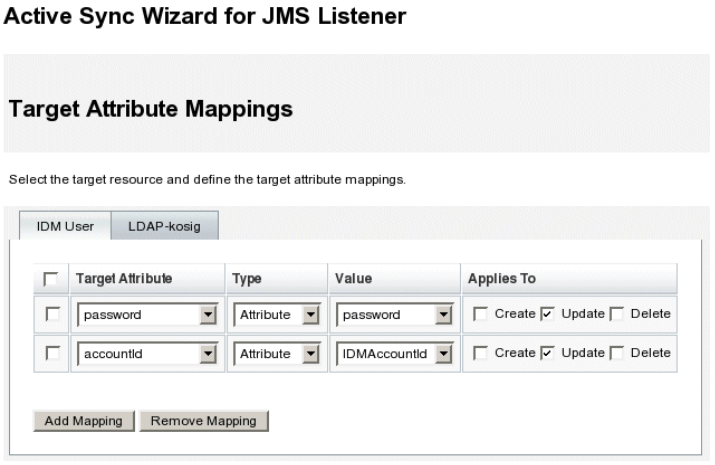
   たとえば、このシナリオでは、Windows パスワードを Sun Directory Server と同期させ、Identity Manager パスワードを同期させたいとします。

7. 「次へ」をクリックし、「ターゲット属性マッピング」パネルが表示されたら、「IDM ユーザー」タブを選択します (まだ選択されていない場合)。

8. 「IDM ユーザー」タブで、テーブルを使用して、Identity Manager ユーザーのターゲット属性マッピングを指定します。

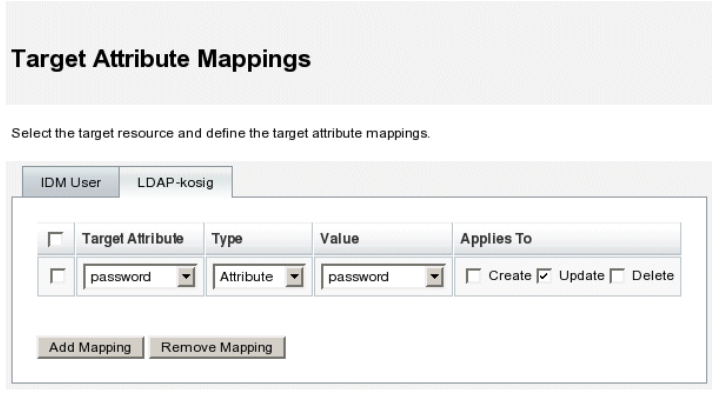
   たとえば、図 9-19 では、`password` と `accountID` が定義されています。

図 9-19　password と accountID の定義



9. 終了したら、「マッピングの追加」をクリックします。
10. 「LDAP-kosig」タブを選択して、Sun Directory のターゲット属性マッピングを定義します (図 9-20)。

図 9-20　Sun Directory のターゲット属性マッピングの定義



11. 終了したら、「マッピングの追加」をクリックして、変更を保存します。

設定のデバッグ

Windows 側の設定のデバッグに、Windows PasswordSync 設定アプリケーションを使用できます。

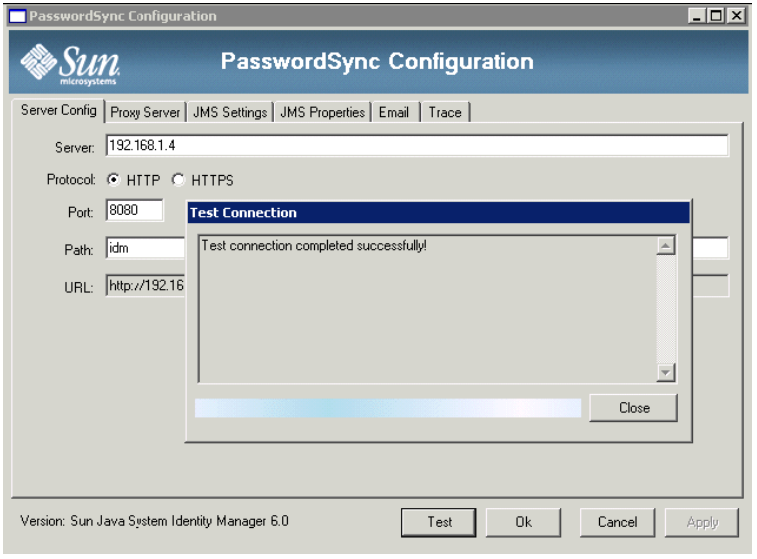
1. まだ実行されていない場合、PasswordSync 設定アプリケーションを開始します。

   デフォルトでは、設定アプリケーションは、「すべてのプログラム」>「Sun Java System Identity Manager PasswordSync」>「設定」でインストールされます。

2. PasswordSync 設定ダイアログが表示されたら、「テスト」ボタンをクリックします。

3. テスト接続ダイアログ (図 9-21) が表示され、テスト接続が正しく行われたかどうかを示すメッセージが示されます。

図 9-21　　テスト接続ダイアログ

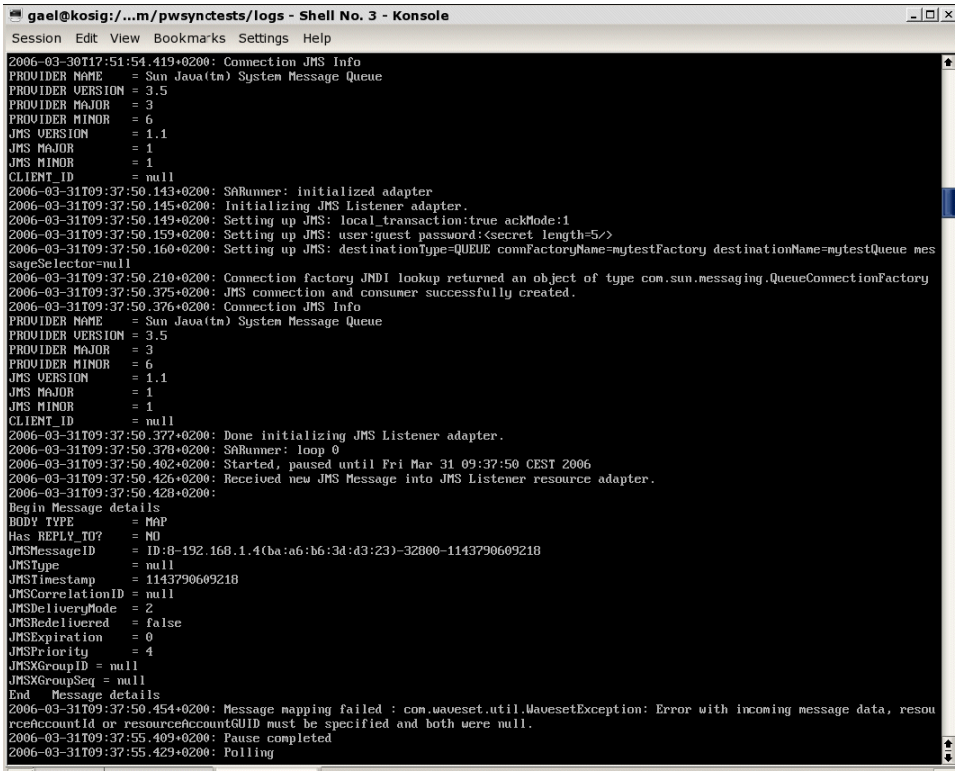


4. 「閉じる」をクリックしてテスト接続ダイアログを閉じます。

5. 「OK」をクリックして、PasswordSync 設定ダイアログを閉じます。

   続いて、JMS リスナーアダプタがデバッグモードで実行し、図 9-22 と同様のデバッグ情報をファイルに生成します。

図 9-22　　デバッグ情報ファイル

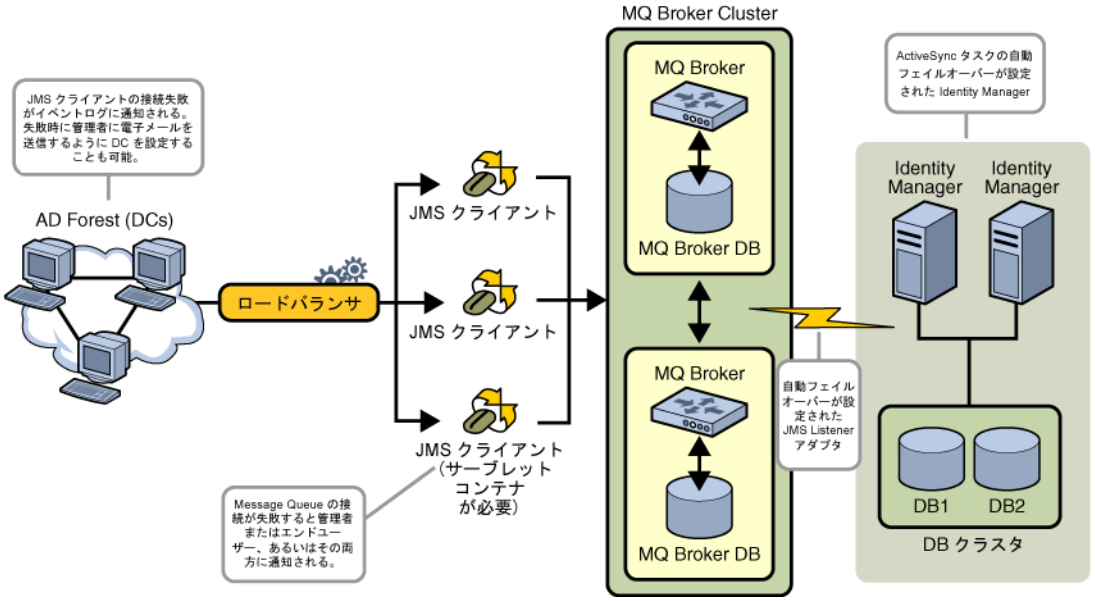


PasswordSync のフェイルオーバー配備

PasswordSync のアーキテクチャーにより、Identity Manager の Windows パスワード同期配備におけるシングルポイント障害が解消されます。

ロードバランサ (図 9-23 参照) を介して一連の JMS クライアント内のいずれかに接続するように各 Active Directory Domain Controller (ADC) を設定した場合、JMS クライアントは Message Queue Broker クラスタにメッセージを送信できます。このため、Message Queue に障害が発生した場合でもメッセージの損失を防止できます。

図 9-23　PasswordSync のフェイルオーバー配備



注　Message Queue クラスタではおそらく、メッセージを存続させるためにデータベースが必要になります。Message Queue Broker クラスタの設定手順については、ベンダーの製品マニュアルを参照してください。

自動フェイルオーバーが設定された JMS リスナーアダプタを実行している Identity Manager サーバーは、Message Queue Broker クラスタと通信します。アダプタは、1 度に 1 つの Identity Manager でのみ実行しますが、第 1 ActiveSync サーバーに障害が発生した場合、第 2 Identity Manager サーバー上でのパスワード関連のメッセージのポーリングと、ダウンストリームへのパスワード変更の伝達を開始します。

PasswordSync についてのよくある質問

Java Messaging Service なしで PasswordSync を実装することはできますか。

はい。ただし、この場合、JMS を使用したパスワード変更イベントの追跡を行えなくなります。

JMS なしで PasswordSync を実装するには、次のフラグを指定して設定アプリケーションを実行します。

```
Configure.exe -direct
```

`-direct` フラグを指定すると、設定アプリケーションは「User」タブを表示します。次にあげる 2 つの点を除き、293 ページの「PasswordSync の設定」で説明した手順に従って PasswordSync を設定します。

- 「JMS Settings」および「JMS Properties」タブを設定しないでください。
- 「User」タブに、Identity Manager への接続に使用するアカウント ID とパスワードを指定します。

JMS なしで PasswordSync を実装する場合、JMS リスナーアダプタを作成する必要はありません。したがって、302 ページの「PasswordSync の配備」で説明した手順を省くようにしてください。通知を設定したい場合、ユーザーパスワード変更ワークフローを変更する必要がある場合があります。

注 `-direct` フラグを指定せずに、引き続き設定アプリケーションを実行する場合は、PasswordSync で JMS が設定されている必要があります。`-direct` フラグを指定してアプリケーションを再実行すると、ふたたび、JMS を使わずに Passwordsync を使用できます。

PasswordSync は、カスタムパスワードポリシーを施行するために使われるほかの Windows パスワードフィルタと組み合わせて使用できますか。

はい。PasswordSync はほかの _WINDOWS_ パスワードフィルタと組み合わせて使用できます。ただし PasswordSync は、レジストリの「Notification Package」エントリの値で列挙されるパスワードフィルタのうち最後のフィルタである必要があります。

次のレジストリパスを使用する必要があります。

`HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Lsa¥Notification Packages`（種類 `REG_MULTI_SZ` の値）

デフォルトでは、インストーラは Identity Manager のパスワードインターセプトをリストの最後に置きますが、インストール後にカスタムのパスワードフィルタをインストールした場合、`lhpwic` を「Notification Packages」リストの最後に移動する必要があります。

PasswordSync はほかの Identity Manager パスワードポリシーと組み合わせて使用できます。Identity Manager サーバーの側でポリシーがチェックされるとき、パスワード同期をほかのリソースにプッシュするために、すべてのリソースのパスワードポリシーが基準を満たす必要があります。結果として、Windows のネイティブパスワードポリシーの制約度を、Identity Manager で定義される最も制約的なパスワードポリシーと同じくらいにすることが推奨されます。

注 パスワードインターセプト DLL はパスワードポリシーを一切施行しません。

PasswordSync サーブレットを、Identity Manager と異なるアプリケーションサーバー上にインストールできますか。

はい。サーブレットは、JMS アプリケーションが必要とするすべての JAR ファイルに加えて、`spml.jar` および `idmcommon.jar` の各 JAR ファイルを必要とします。

PasswordSync サービスは lh サーバーにクリアテキストでパスワードを送信しますか。

Sun では PasswordSync を SSL 上で実行することを推奨しますが、すべての重要なデータは Identity Manager サーバーに送信される前に暗号化されます。

パスワード変更の結果、com.waveset.exception.ItemNotLocked が発生することがありますが、それはどうしてですか。

PasswordSync を有効にすると、(ユーザーインタフェースから開始されたものも含めた) パスワード変更の結果としてリソース上でパスワード変更が発生し、それによってリソースが Identity Manager と通信するからです。

`passwordSyncThreshold` ワークフロー変数が正しく設定されている場合、Identity Manager はユーザーオブジェクトを検証し、パスワード変更が処理済みかどうかを判定します。しかしながら、ユーザーまたは管理者が同じユーザーに対して同時に別のパスワード変更を行う場合、ユーザーオブジェクトがロックされている可能性があります。

第 10 章

セキュリティー

この章では、Identity Manager セキュリティー機能と、セキュリティー上のリスクを軽減するための手順について詳しく説明します。

以下のトピックで、Identity Manager でのシステムセキュリティーの管理について詳細に説明します。

- セキュリティー機能
- 同時ログインセッションの制限
- パスワード管理
- パススルー認証
- 共通リソースの認証の設定
- X509 証明書認証の設定
- 暗号化の使用と管理
- サーバー暗号化の管理
- セキュリティーの実装

セキュリティー機能

Identity Manager では、次の機能によってセキュリティー上のリスクを軽減します。

- アカウントアクセスの即時無効化 ー Identity Manager では、1 回の操作で組織または個々のアクセス権限を無効にすることができます。
- ログインセッションの制限 ー 並行して行われるログインセッション数に制限を設定できます。
- アクティブリスク分析 ー Identity Manager では、非アクティブなアカウントや疑わしいパスワードのアクティビティーなどのセキュリティー上のリスクを絶えずスキャンします。
- 包括的なパスワード管理 ー 完全で柔軟性に富んだパスワード管理機能によって、完全なアクセス管理が保証されます。
- 監査およびレポートによるアクセスのアクティビティーの監視 ー 一連のレポートを実行して、アクセスのアクティビティーについての対象を絞った情報を提供します。レポート機能の詳細については、第 7 章「レポート」を参照してください。
- 管理特権の詳細な制御 ー ユーザーに、または管理者ロールで定義された一定範囲の管理作業に単一の機能を割り当てることにより、Identity Manager での管理コントロールを付与し管理できます。
- サーバーキーの暗号化 ー Identity Manager では、「タスク」エリアでサーバー暗号化キーを作成および管理できます。

また、システムアーキテクチャによってセキュリティー上のリスクを可能な限り軽減するようにしています。たとえば、一度ログアウトすると、ブラウザの「戻る」機能を使用しても、以前にアクセスしたページにアクセスすることはできません。

同時ログインセッションの制限

デフォルトでは、Identity Manager ユーザーは同時ログインセッションを行えます。ただし、System Configuration オブジェクトの `security.authn.singleLoginSessionPerApp` 設定属性の値を変更すれば、並行セッションをログインアプリケーションごとに 1 つに制限できます。この属性は、管理者インタフェース、ユーザーインタフェース、Identity Manager IDE などのそれぞれのログインアプリケーション名に対応した 1 つの属性を含んだオブジェクトです。この属性の値を `true` に変更すると、強制的に各ユーザーのログインセッションが 1 つに制限されます。

制限された場合、ユーザーは複数のセッションにログインできますが、最後にログインしたセッションだけがアクティブで有効になります。無効なセッションでアクションを実行すると、ユーザーは自動的にセッションから強制的にログオフされ、セッションが終了します。

パスワード管理

Identity Manager は、複数のレベルでパスワード管理を実行します。

- **変更の管理**
  - ユーザーのパスワードを複数の場所から変更する (「ユーザーの編集」、「ユーザーの検索」、または「パスワードの変更」ページ)
  - リソースを細分化して選択することにより、ユーザーの任意のリソースでパスワードを変更する
- **パスワードリセットの管理**
  - ランダムなパスワードを生成する
  - パスワードをエンドユーザーまたは管理者に表示する
- **ユーザーによるパスワードの変更**
  - 次のサイトで、エンドユーザーは自己管理機能によりパスワードを変更できる

    http://localhost:8080/idm/user
  - オプションとして、エンドユーザーの環境に適するように自己管理ページをカスタマイズする
- **ユーザーによるデータの更新**
  - エンドユーザーが管理するユーザーのスキーマ属性をセットアップする
- **ユーザーによるアクセスの復旧**
  - 秘密の質問を使用して、自分のパスワードを変更するアクセス権をユーザーに与える
  - パススルー認証を使用して、いくつかのパスワードのうちの 1 つを使ってアクセス権をユーザーに与える
- **パスワードポリシー**
  - パスワードパラメータを定義する規則を使用する

パススルー認証

パススルー認証を使用して、1 つ以上の異なるパスワードによるアクセス権をユーザーと管理者に与えます。Identity Manager は、次のものを実装することによって認証を管理します。

- ログインアプリケーション (ログインモジュールグループの集まり)
- ログインモジュールグループ (順序づけされたログインモジュールのセット)
- ログインモジュール (割り当てられたリソースごとに認証を設定し、認証の成功条件を複数ある中から 1 つ指定する)

ログインアプリケーションについて

ログインアプリケーションはログインモジュールグループの集まりを定義し、さらにログインモジュールグループはユーザーが Identity Manager にログインするときに使用するログインモジュールのセットと順序を定義します。各ログインアプリケーションは 1 つ以上のログインモジュールグループで構成されます。

ログインアプリケーションは、ログイン時にログインモジュールグループのセットをチェックします。設定されているログインモジュールグループが 1 つだけの場合は、そのログインモジュールグループが使用され、それに含まれるログインモジュールがグループ内で定義された順序で処理されます。ログインアプリケーションに複数のログインモジュールグループが定義されている場合には、Identity Manager が各ログインモジュールに適用されるログイン制約規則をチェックして、処理するグループを決定します。

ログイン制約規則

ログイン制約規則は、ログインアプリケーションに定義されているログインモジュールグループに対して適用されます。ログインアプリケーションのログインモジュールグループの各セットの中で、1 つのログインモジュールグループだけは適用されるログイン制約を持つことができません。

セットの中のどのログインモジュールグループを処理するかを決めるにあたって、Identity Manager は最初のログインモジュールグループの制約規則を評価します。評価が成功した場合は、そのログインモジュールグループが処理されます。評価に失敗すると、制約規則が成功するかまたは制約規則を持たないログインモジュールグループが評価された後に使用されるまで、各ログインモジュールグループが次々に評価されます。

注 ログインアプリケーションに複数のログインモジュールグループが含まれる場合には、ログイン制約規則を持たないログインモジュールグループをセットの最後の位置に置くようにしてください。

ログイン制約規則の例

次に示す場所に基づいたログイン制約規則の例では、規則がヘッダーからリクエスト側の IP アドレスを取得し、そのアドレスが 192.168 ネットワーク上にあるかどうかをチェックします。ＩＰ アドレスに 192.168. が検出されると、規則は true の値を返し、そのログインモジュールグループが選択されます。

コード例 10-1　　場所に基づいたログイン制約規則

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
  <match>
    <ref>remoteAddr</ref>
    <s>192.168.</s>
  </match>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='All'/>
  </MemberObjectGroups>
</Rule>
```

ログインアプリケーションの編集

メニューバーで、「設定」を選択してから「ログイン」を選択して、「ログイン」ページにアクセスします。

ログインアプリケーションリストには次の内容が表示されます。

- 定義済みの各 Identity Manager ログインアプリケーション (インタフェース)
- ログインアプリケーションを構成するログインモジュールグループ
- 各ログインアプリケーションに設定された Identity Manager セッションのタイムアウト制限

「ログイン」ページから次の操作を行えます。

- カスタムログインアプリケーションの作成
- カスタムログインアプリケーションの削除
- ログインモジュールグループの管理

ログインアプリケーションを編集するには、リストからログインアプリケーションを選択します。

Identity Manager セッション制限の設定

「ログインアプリケーションの修正」ページから、Identity Manager ログインセッションごとのタイムアウト値 (制限) を設定できます。時間、分、および秒を選択して、「保存」をクリックします。設定した制限が、ログインアプリケーションリストに表示されます。

各 Identity Manager ログインアプリケーションにセッションタイムアウトを設定できます。ユーザーが Identity Manager アプリケーションにログインすると、現在のタイムアウト設定値を使用し、ユーザーセッションが未使用時にタイムアウトされる将来の日時が計算されます。こうして計算された日付はユーザーの Identity Manager セッションとともに格納されるため、リクエストが実行されるたびにチェックできます。

ログイン管理者がログインアプリケーションのセッションタイムアウト値を変更した場合、その値は将来のすべてのログインに影響します。既存のセッションは、ユーザーがログインしたときに適用されていた値に基づいてタイムアウトします。

http タイムアウトの設定値はすべての Identity Manager アプリケーションに影響し、ログインアプリケーションのセッションタイムアウト値よりも優先されます。

アプリケーションへのアクセスの無効化

「ログインアプリケーションの作成」ページと「ログインアプリケーションの修正」ページで、「無効化」オプションを選択してログインアプリケーションを無効化し、ユーザーがログインできないようにすることができます。ユーザーが無効化されたアプリケーションにログインしようとすると、インタフェースによって、アプリケーションが現在無効にされていることを示す代替ページにリダイレクトされます。カスタムカタログを編集することで、このページに表示されるメッセージを編集することができます。

このオプションの選択を解除するまで、ログインアプリケーションは無効にされたままになります。安全措置として、管理者ログインは無効化できません。

ログインモジュールグループの編集

ログインモジュールグループリストには次の内容が表示されます。

- 定義済みの各 Identity Manager ログインモジュールグループ
- 各ログインモジュールグループに含まれるログインモジュール
- ログインモジュールグループに制約規則が含まれるかどうか

「ログインモジュールグループ」ページから、ログインモジュールグループを作成、編集、削除できます。リストからログインモジュールグループを 1 つ選択して、それを編集します。

ログインモジュールの編集

詳細を入力するか、ログインモジュールに関して次のように選択します。すべてのオプションがどのログインモジュールにも選択できるとは限りません。

- **「ログイン成功条件」** − このモジュールに適用する条件を選択します。次の中から選択できます。
  - **「必須」** − 成功するにはそのログインモジュールが必要です。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。ログインモジュールが 1 つしかない場合、管理者は正常にログインします。
  - **「必要条件」** − 成功するにはそのログインモジュールが必要です。成功すると、認証はリスト内の次のログインモジュールに進みます。失敗した場合、認証は続行しません。
  - **「十分条件」** − 成功するためにそのログインモジュールが必要ではありません。成功すると、認証は次のログインモジュールに進まず、管理者は正常にログインします。失敗した場合、認証はリスト内の次のログインモジュールに進みます。
  - **「オプション」** − 成功するためにそのログインモジュールが必要ではありません。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。
- **「ログイン検索属性」** − (LDAP のみ) 関連する LDAP サーバーへのバインド (ログイン) 試行時に使用する、LDAP ユーザー属性名の順序付けられたリストを指定します。指定したユーザーのログイン名とともに、指定された LDAP ユーザー属性を使用して、一致する LDAP ユーザーを順番に検索します。これにより、LDAP へのパススルーが設定されている場合、LDAP の cn 属性または電子メールアドレス属性により、ユーザーは Identity Manager にログインできます。

  たとえば、次のように指定するとします。

  ```
  cn
  mail
  ```

  そして、ユーザーは `gwilson` としてログインしようとするとします。このとき LDAP リソースはまず `cn=gwilson` という条件で LDAP ユーザーの検索を試行します。これに成功すると、そのユーザーによって指定されたパスワードでバインドを試みます。成功しない場合、LDAP リソースは `mail=gwilson` という条件で LDAP ユーザーを検索します。これにも失敗すると、ログインが失敗します。

  値を指定しない場合のデフォルト LDAP 検索属性は次のとおりです。

  ```
  uid
  cn
  ```

- **「ログイン相関規則」** – ユーザーが提供したログイン情報と Identity Manager ユーザーのマッピングに使用されるログイン相関規則を選択します。この規則では、規則で指定されたロジックを使用して Identity Manager ユーザーが検索されます。この規則は 1 つ以上の AttributeConditions を含むリストを返します。このリストは、一致する Identity Manager ユーザーを検索するために使用されます。選択する規則は、LoginCorrelationRule authType を持つ必要があります。
- **「新規ユーザー命名規則」** – ログインの一環として新規 Identity Manager ユーザーを自動的に作成する場合に使用される、新規ユーザー命名規則を選択します。

「保存」をクリックして、ログインモジュールを保存します。一度保存すると、このモジュールをログインモジュールグループ内のほかのすべてのモジュールと関連づけて配置できます。

警告 Identity Manager ログインが複数のシステムから認証を受けるよう設定する場合は、Identity Manager の認証のターゲットとなるすべてのシステムで、アカウントのユーザー ID とパスワードを同じにします。

ユーザー ID とパスワードの組み合わせが異なる場合、ユーザー ID およびパスワードが「Identity Manager ユーザーログイン」フォームに入力されたユーザー ID およびパスワードと一致しないシステムで、ログインが失敗します。これらのシステムの中には、ログイン試行回数が一定数を超えるとアカウントを強制的にロックするロックアウトポリシーを持つものもあります。このようなシステムでは、Identity Manager によるユーザーのログインが成功し続けた場合でも、ユーザーアカウントは最終的にロックされます。

共通リソースの認証の設定

物理的または論理的に同一の複数のリソースがある場合 (たとえば、同一の物理ホストに対して定義された 2 つのリソース、NT または AD ドメイン環境内の信頼できるドメインを表す複数のリソース)、System Configuration オブジェクト内でそれらのリソースのセットを「共通リソース」として指定することができます。

リソースを共通リソースとして設定することで、あるユーザーを共通リソースの 1 つのリソースに対して認証しながら、共通リソースの別のリソースを使用してそのユーザーの関連付けられた Identity Manager ユーザーにマップすることができます。たとえば、あるユーザーのリソース AD-1 に対するリソースアカウントが、自分の Identity Manager ユーザーにリンクされているとします。ログインモジュールグループでは、ユーザーがリソース AD-2 を認証する必要があることが定義されているとし

ます。AD-1 と AD-2 が、共通リソースとして定義されている場合 (この場合、同じ信頼できるドメイン内にある)、ユーザーが AD-2 に対して正常に認証されると、Identity Manager はリソース AD-1 で同じ accountId を持つユーザーを見つけることによって、関連付けられた Identity Manager ユーザーにマップすることができます。

この System Configuration オブジェクトの属性の形式は次の例で示します。

コード例 10-2 共通リソースの認証の設定

```
<Attribute name='common resources'>
    <Attribute name='Common Resource Group Name'>
        <List>
            <String>Common Resource Name</String>
            <String>Common Resource Name</String>
        </List
    </Attribute>
</Attribute>
```

X509 証明書認証の設定

次の情報と手順を使用して、Identity Manager の X509 証明書認証を設定します。

前提条件

Identity Manager で X509 証明書ベースの認証をサポートするには、クライアントとサーバーの 2 方向の SSL 認証が正しく設定されているかを確認します。クライアントの観点では、これは、X509 準拠のユーザー証明書がブラウザにインポートされ (またはスマートカードリーダーで利用可能で)、ユーザー証明書に署名するために使用された信頼できる証明書が、Web アプリケーションサーバーの信頼できる証明書のキーストアにインポートされている必要があることを意味します。

さらに、使用したクライアント証明書がクライアント認証のために選択されている必要があります。これを確認するには、次を実行します。

1. Internet Explorer を使用して、「ツール」を選択し、「インターネットオプション」を選択します。
2. 「コンテンツ」タブを選択します。
3. 「証明書」エリアで、「証明書」をクリックします。
4. クライアント証明書を選択し、「詳細」をクリックします。

5. 「証明書の目的」エリアで、「クライアント認証」オプションが選択されていることを確認します。

Identity Manager での X509 証明書認証の設定

Identity Manager で X509 証明書認証を設定するには、次を実行します。

1. 管理者インタフェースに Configurator (または同等の権限を持つユーザー) としてログインします。
2. 「設定」を選択し、「ログイン」を選択して、「ログイン」ページを表示します。
3. 「ログインモジュールグループの管理」をクリックし、「ログインモジュールグループ」ページを表示します。
4. リストからログインモジュールグループを選択します。
5. 「ログインモジュールの割り当て」リストから「Identity Manager X509 証明書ログインモジュール」を選択します。「ログインモジュールグループの修正」ページが表示されます。
6. ログインの成功条件を設定します。使用可能な値は次のとおりです。
   - **「必須」** – 成功するにはそのログインモジュールが必要です。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。ログインモジュールが 1 つしかない場合、管理者は正常にログインします。
   - **「必要条件」** – 成功するにはそのログインモジュールが必要です。成功すると、認証はリスト内の次のログインモジュールに進みます。失敗した場合、認証は続行しません。
   - **「十分条件」** – 成功するためにそのログインモジュールが必要ではありません。成功すると、認証は次のログインモジュールに進まず、管理者は正常にログインします。失敗した場合、認証はリスト内の次のログインモジュールに進みます。
   - **「オプション」** – 成功するためにそのログインモジュールが必要ではありません。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。
7. ログイン相関規則を選択します。組み込み規則またはカスタム相関規則を選択できます。カスタム相関規則の作成については、次の節を参照してください。
8. 「保存」をクリックして、「ログインモジュールグループの修正」ページに戻ります。
9. オプションの作業として、ログインモジュールの順序を変更し (複数のログインモジュールがログインモジュールグループに割り当てられている場合)、「保存」をクリックします。

10. ログインモジュールグループがログインアプリケーションに割り当てられていない場合はここで割り当てます。「ログインモジュールグループ」ページで、「ログインアプリケーションに戻る」をクリックし、ログインアプリケーションを選択します。ログインモジュールグループをログインアプリケーションに割り当てたら、「保存」をクリックします。

注

waveset.properties ファイルで `allowLoginWithNoPreexistingUser` オプションの値が `true` に設定されている場合、「Identity Manager X509 証明書ログインモジュール」を設定するときに、新規ユーザー命名規則を選択するようにリクエストされます。この規則は、関連付けられたログイン相関規則によってユーザーが検出されないときに作成される新しいユーザーの命名方法を決定するために使用されます。

新規ユーザー命名規則では、ログイン相関規則と同じ入力引数を使用できます。この規則は、1 つの文字列を返し、これが新しい Identity Manager ユーザーアカウントを作成するためのユーザー名として使用されます。

サンプルの新規ユーザー命名規則が、NewUserNameRules.xml という名前で idm/sample/rules にあります。

ログイン設定規則の作成とインポート

ログイン相関規則は、Identity Manager X509 証明書ログインモジュールによって、証明書データを適切な Identity Manager ユーザーにマップする方法を決定するために使用されます。Identity Manager には、「X509 証明書 subjectDN を使用した相関」という名前の組み込み相関規則が 1 つ用意されています。

独自の相関規則を追加することもできます。各相関規則は、次のガイドラインに従っている必要があります。

- `authType` 属性は `LoginCorrelationRule` に設定する必要があります (`<LoginCorrelationRule>` 要素で `authType='LoginCorrelationRule'` を設定する)。
- 相関規則は、関連付けられた Identity Manager ユーザーを検出するためにログインモジュールが使用する `AttributeConditions` のリストのインスタンスを返す必要があります。たとえば、ログイン相関規則は、関連付けられた Identity Manager ユーザーを電子メールアドレスによって検索する `AttributeCondition` を返す場合があります。

次の引数がログイン設定規則に渡されます。

- 標準の X509 証明書フィールド (`subjectDN`、`issuerDN`、有効な日付など)
- 重要な拡張プロパティーと重要ではない拡張プロパティー

次の証明書引数の命名規則がログイン相関規則に渡されます。

```
cert.field name.subfield name
```

次の例のような引数名を規則で使用できます。

- `cert.subjectDN`
- `cert.issuerDN`
- `cert.notValidAfter`
- `cert.notValidBefore`
- `cert.serialNumber`

ログイン設定規則は、渡された引数を使用して、1 つ以上の `AttributeConditions` のリストを返します。Identity Manager X509 証明書ログインモジュールは、これらを使用して関連付けられた Identity Manager ユーザーを検出します。

サンプルのログイン相関規則が、`LoginCorrelationRules.xml` という名前で、`idm/sample/rules` にあります。

カスタム相関規則を作成したら、その規則を Identity Manager にインポートする必要があります。管理者インタフェースで、「設定」を選択し、「交換ファイルのインポート」を選択して、ファイルインポート機能を使用します。

SSL 接続のテスト

SSL 接続をテストするには、SSL を介して、設定済みのアプリケーションインタフェースの URL (例 : https//idm007:7002/idm/user/login.jsp) にアクセスします。セキュアなサイトに入ったことを知らせるメッセージが表示され、Web サーバーに送信する個人用証明書を指定するようにリクエストされます。

問題の診断

X509 証明書を使用した認証に関する問題は、ログインフォーム上でエラーメッセージとして報告されます。詳しい診断情報を得るには、Identity Manager サーバーで次のクラスとレベルのトレースを有効にします。

- `com.waveset.session.SessionFactory 1`
- `com.waveset.security.authn.WSX509CertLoginModule 1`
- `com.waveset.security.authn.LoginModule 1`

http リクエスト内のクライアント証明書の属性が `javaxservlet.request.X509Certificate` 以外である場合、この属性が http リクエスト内に見つからないことを知らせるメッセージが表示されます。これを解決するには、次を実行します。

1. `SessionFactory` のトレースを有効にして、http 属性の完全なリストを表示し、X509Certificate の名前を特定します。
2. Identity Manager デバッグ機能を使用して、`LoginConfig` オブジェクトを編集します。
3. Identity Manager X509 証明書ログインモジュールの `<LoginConfigEntry>` 内の `<AuthnProperty>` の名前を正しい名前に変更します。
4. 保存して、もう一度試します。

さらに、Identity Manager X509 証明書ログインモジュールをログインアプリケーションから削除して、もう一度追加することが必要な場合があります。

暗号化の使用と管理

暗号化は、メモリーおよびリポジトリ内のサーバーデータだけでなく、サーバーとゲートウェイの間で送信されるすべてのデータの機密性と完全性を保証するために使用されます。

続く節では、Identity Manager サーバーとゲートウェイで暗号化が使用および管理される方法を詳しく説明し、サーバーとゲートウェイの暗号化キーに関する質問を検討します。

暗号化によって保護されるデータ

次の表は、Identity Manager 製品で暗号化によって保護されるデータの種類と、各データの種類を保護するために使用される暗号を示したものです。

表 10-1 暗号化によって保護されるデータの種類

データの種類	RSA MD5	NIST トリプル DES 168 ビットキー (DESede/ECB/NoPadding)	PKCS#5 パスワードベースの暗号化 56 ビットキー (PBEwithMD5andDES)
サーバー暗号化キー		デフォルト	設定オプション[1]
ゲートウェイ暗号化キー		デフォルト	設定オプション[1]
ポリシー辞書単語	はい		

表 10-1　暗号化によって保護されるデータの種類 (続き)

データの種類	RSA MD5	NIST トリプル DES 168 ビットキー (DESede/ECB/NoPadding)	PKCS#5 パスワードベースの暗号化 56 ビットキー (PBEwithMD5andDES)
ユーザーパスワード		はい	
ユーザーパスワード履歴		はい	
ユーザーの回答		はい	
リソースパスワード		はい	
リソースパスワード履歴	はい		
サーバーゲートウェイ間のすべてのペイロード		はい	

1. pbeEncrypt 属性または「サーバー暗号化の管理」タスクにより System Configuration オブジェクト経由で設定します。

サーバー暗号化キーに関する質問と答え

続く節では、サーバー暗号化キーのソース、場所、保守、使用についてよく尋ねられる質問に答えていますのでご覧ください。

サーバー暗号化キーとは何ですか？

サーバー暗号化キーはトリプル DES 168 ビットの対称キーです。サーバーでサポートされるキーには 2 つのタイプがあります。

- **デフォルトキー** – このキーはコンパイル時にサーバーコードに組み込まれます。
- **ランダムに生成されるキー** – このキーは、サーバーの最初の起動時、または現在のキーのセキュリティーに不安がある場合にいつでも生成することができます。

サーバー暗号化キーはどこで維持管理されますか？

サーバー暗号化キーはリポジトリで維持管理されるオブジェクトです。どのリポジトリにも多数のデータ暗号化キーがある可能性があります。

暗号化されたデータの復号化や再暗号化にどのキーを使用するかを、サーバーはどのようにして認識するのですか？

リポジトリに格納された各暗号化データの先頭には、そのデータを暗号化する際に使用したサーバー暗号化キーの ID が付加されます。暗号化データを含むオブジェクトがメモリーに読み込まれると、Identity Manager はその暗号化データ の ID プレフィックスに関連づけられたサーバー暗号化キーを使用して復号化し、データが変更されている場合には同じキーで再暗号化します。

サーバー暗号化キーはどのようにして更新しますか？

Identity Manager には「サーバー暗号化の管理」というタスクが用意されています。このタスクを使用することにより、承認されたセキュリティー管理者は次のようなキー管理タスクを実行することができます。

- 新しい現在のサーバーキーの生成
- 現在のサーバーキーを使用して暗号化したデータを含む既存オブジェクトに対する、タイプ別の再暗号化

このタスクの使用法の詳細については、この章の「サーバー暗号化の管理」を参照してください。

現在のサーバーキーが変更された場合、既存の暗号化データはどうなりますか？

何も問題はありません。既存の暗号化データは、引き続き、暗号化データの ID プレフィックスで参照されているキーを使用して復号化や再暗号化されます。新しいサーバー暗号化キーが生成され、そのキーが現在のキーに設定された場合、新たに暗号化されるデータには新しいサーバーキーが使用されます。

複数のキーがあることによる問題を回避するため、またデータの完全性のレベルを高い状態に保つために、「サーバー暗号化の管理」タスクを使用して、現在のサーバー暗号化キーで既存の暗号化データをすべて再暗号化してください。

暗号化キーを使用できない暗号化データをインポートした場合、どのようなことが起こりますか？

暗号化データを含むオブジェクトをインポートする際、読み込み先となるリポジトリにないキーでデータが暗号化されている場合、データはインポートされますが、復号化されません。

サーバーキーはどのように保護されますか？

サーバーがパスワードベースの暗号化 (PBE) - PKCS#5 暗号化を使用するよう `pbeEncrypt` 属性または「サーバー暗号化の管理」タスクによって System Configuration オブジェクトで設定されていない場合には、デフォルトキーを使用してサーバーキーが暗号化されます。デフォルトキーはすべての Identity Manager インストールで同じです。

サーバーが PBE 暗号化を使用するよう設定されている場合は、サーバーを起動するたびに PBE キーが生成されます。PBE キーは、サーバー固有の秘密キーから生成されるパスワードを PBEwithMD5andDES 暗号に渡すことによって生成されます。PBE キーはメモリー内にのみ保持され、それが持続させられることは決してありません。また、共通リポジトリを共有するすべてのサーバーの PBE キーは同じです。

サーバーキーの PBE 暗号化を有効化するには、暗号 PBEwithMD5andDES が使用できなければなりません。この暗号は Identity Manager にはデフォルトでパッケージされていませんが、Sun や IBM が提供する実装をはじめ、多くの JCE プロバイダ実装で使用可能な PKCS#5 標準です。

サーバーキーを安全な外部記憶装置にエクスポートしてもよいですか？

はい。サーバーキーが PBE 暗号化されている場合、エクスポートの前に、サーバーキーは復号化されてデフォルトキーで再暗号化されます。これにより、それ以後ローカルサーバー PBE キーに依存することなく、同じサーバーまたは別のサーバーにサーバーキーをインポートできるようになります。サーバーキーがデフォルトキーで暗号化されている場合は、エクスポート前の事前処理は行われません。

サーバーキーをサーバーにインポートするときには、サーバーが PBE キー用に設定されていればキーが復号化され、次いで、そのサーバーが PBE キー暗号化用に設定されていればローカルサーバーの PBE キーで再暗号化されます。

どのデータがサーバーとゲートウェイの間で暗号化されますか？

サーバーとゲートウェイの間で送信されるすべてのデータ (ペイロード) が、ランダムに生成されたサーバーゲートウェイセッション対称 168 ビットキーを使用してトリプル DES で暗号化されます。

ゲートウェイキーに関する質問と答え

続く節では、ゲートウェイのソース、記憶装置、配布、保護についてよく尋ねられる質問に答えていますのでご覧ください。

データの暗号化または復号化に使用するゲートウェイキーとは何ですか？

Identity Manager サーバーがゲートウェイに接続するたびに、初期ハンドシェークによって新規のランダム 168 ビットのトリプル DES セッションキーが生成されます。それ以降サーバーとゲートウェイの間で送信されるすべてのデータは、このキーを使用して暗号化または復号化されます。サーバー / ゲートウェイのペアごとに一意のセッションキーが生成されます。

ゲートウェイキーはどのようにしてゲートウェイに配布されますか？

セッションキーはサーバーによってランダムに生成された後、初期サーバーゲートウェイ間ハンドシェークの一環として共有秘密マスターキーによって暗号化されることにより、サーバーとゲートウェイの間でセキュアに交換されます。

初期ハンドシェーク時に、サーバーはゲートウェイに問い合わせて、ゲートウェイがサポートするモードを判別します。ゲートウェイは次の 2 つのモードで作動します。

- **「デフォルト」モード** − サーバーゲートウェイ間の初期プロトコルハンドシェークは、コンパイル時にサーバーコードに組み込まれている、デフォルトの 168 ビットトリプル DES キーで暗号化されます。
- **「セキュア」モード** − 共有リポジトリを使用する、ランダムな 168 ビットキーであるトリプル DES ゲートウェイキーが生成され、初期ハンドシェークプロトコルの一環としてサーバーからゲートウェイに送信されます。このゲートウェイキーは他の暗号化キーと同様にサーバーリポジトリに格納され、ゲートウェイによりゲートウェイ自身のローカルレジストリにも格納されます。

  セキュアモードでかつサーバーがゲートウェイに接続している場合、サーバーはテストデータをゲートウェイキーで暗号化してゲートウェイに送信します。ゲートウェイはテストデータの復号化を試み、テストデータにゲートウェイ固有のデータを追加してから、元のデータと追加したデータの両方を再暗号化してサーバーに送り返します。サーバーがテストデータとゲートウェイ固有のデータを正常に復号化できた場合、サーバーはサーバーゲートウェイ間用に一意のセッションキーを生成し、それをゲートウェイキーで暗号化してゲートウェイに送信します。ゲートウェイはセッションキーを受け取ると、すぐに復号化し、サーバーゲートウェイ間のセッションが持続する間そのキーを保持して使用します。サーバーがテストデータとゲートウェイ固有のデータを正常に復号化できない場合、サーバーはデフォルトキーを使用してゲートウェイキーを暗号化し、ゲートウェイに送信します。ゲートウェイはコンパイル時に組み込まれたデフォルトキーを使用してゲートウェイキーを復号化し、そのゲートウェイキーをレジストリに格

納します。その後、サーバーはそのゲートウェイキーを使ってサーバーゲートウェイ間で一意のセッションキーを暗号化し、セッションキーをゲートウェイに送信して、サーバーゲートウェイ間のセッションが持続する間そのセッションキーを使用します。

それ以後、ゲートウェイは自身のゲートウェイキーでセッションキーを暗号化したサーバーからのリクエストのみを受け入れます。ゲートウェイは、起動時にキーのレジストリをチェックします。キーのレジストリがあれば、そのキーを使用します。ない場合は、デフォルトキーを使用します。いったんゲートウェイがレジストリにキーを設定してしまうと、デフォルトキーを使用してセッションを確立することはできなくなります。それにより、だれかが不正なサーバーをセットアップしてゲートウェイに接続することを防げます。

サーバーゲートウェイ間ペイロードの暗号化や復号化に使用するゲートウェイキーを更新できますか？

Identity Manager には「サーバー暗号化の管理」というタスクが用意されており、承認されたセキュリティー管理者はいろいろなキー管理タスクを実行することができます。そのタスクには、新しい現在のゲートウェイキーの生成や生成された現在のゲートウェイキーによるすべてのゲートウェイの更新などが含まれます。このキーはサーバーゲートウェイ間で送信されるすべてのペイロードを保護する、セッション単位のキーを暗号化するために使用されます。新たに生成されるゲートウェイキーは、システム設定の `pbeEncrypt` 属性の値に基づいて、デフォルトキーまたは PBE キーで暗号化されます。

ゲートウェイキーはサーバー上とゲートウェイ上のどこに格納されますか？

サーバー上では、ゲートウェイキーはサーバーキーとまったく同じようにリポジトリに格納されます。ゲートウェイ上では、ローカルレジストリキー内に格納されます。

ゲートウェイキーはどのように保護されますか？

ゲートウェイキーはサーバーキーの場合と同じように保護されます。サーバーが PBE 暗号化を使用するように設定されている場合、ゲートウェイキーは PBE が生成するキーで暗号化されます。このオプションが false に設定されている場合には、ゲートウェイキーはデフォルトキーで暗号化されます。詳細については、前述の「サーバーキーはどのように保護されますか？」の節を参照してください。

ゲートウェイキーを安全な外部記憶装置にエクスポートしてもよいですか？

ゲートウェイキーは、サーバーキーの場合と同じく、「サーバー暗号化の管理」タスクを使用してエクスポートできます。詳細については、前述の「サーバーキーを安全な外部記憶装置にエクスポートしてもよいですか？」の節を参照してください。

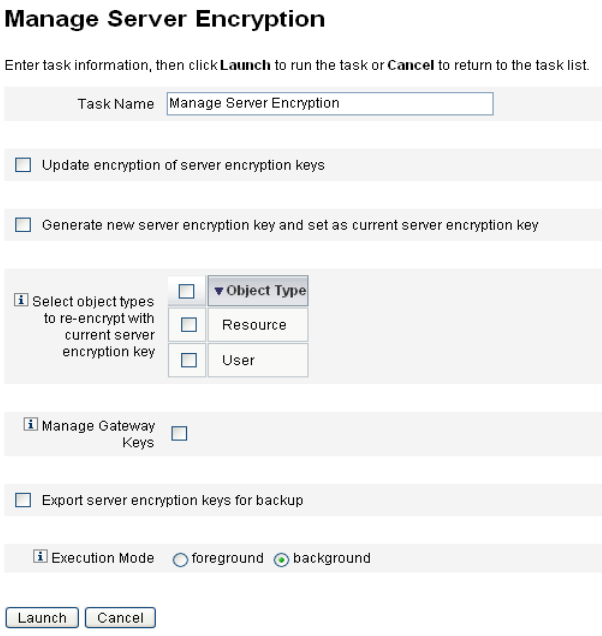
サーバーキーやゲートウェイキーはどのようにして破棄されますか？

サーバーキーとゲートウェイキーは、サーバーリポジトリからそれらを削除することによって破棄されます。あるキーを使用して暗号化されたサーバーデータがある間や、そのキーに依存するゲートウェイがある間は、そのキーを削除しないように注意してください。「サーバー暗号化の管理」タスクを使用して、現在のサーバーキーですべてのサーバーデータを再暗号化し、現在のゲートウェイキーをすべてのゲートウェイで同期することによって、古いキーを削除する前に、確実にどの古いキーも使用されていない状態になるようにしてください。

サーバー暗号化の管理

次の図に示すように、Identity Manager のサーバー暗号化機能を使用して、新しい 3DES サーバー暗号化キーを作成してから、3DES または PKCS#5 暗号化を使ってこれらのキーを暗号化できます。サーバー暗号化の管理タスクは、Security Administrator 機能を持つユーザーだけが実行でき、「サーバータスク」タブからアクセスします。

図 10-1　「サーバー暗号化の管理」タスク



「タスクの実行」を選択し、リストから「サーバー暗号化の管理」を選択して、タスクに関する次の情報を設定します。

- **「サーバー暗号化キーの暗号化の更新」** − サーバー暗号化キーの暗号化を、デフォルトの 3DES 方式または PKCS#5 方式のどちらを使用して行うかを選択します。このオプションを選択すると、2 つの暗号化方式 (「デフォルト」と「PKCS#5」) が表示されるので、どちらかを選択します。
- **「新しいサーバー暗号化キーを生成し、現在のサーバー暗号化キーとして設定する」** − 新しいサーバー暗号化キーを生成する場合に選択します。このオプションを選択した場合は、それ以降に生成される暗号化データでは、このキーが使用されます。新しいサーバー暗号化キーを生成しても、既存の暗号化データに適用されているキーはそのまま使用できます。
- **「現在のサーバー暗号化キーを使用して再暗号化するオブジェクトタイプを選択」** − 1 つ以上の Identity Manager オブジェクトタイプ (リソースやユーザーなど) を選択し、現在の暗号化キーを使用して再度暗号化します。
- **「ゲートウェイ鍵の管理」** − 選択すると、ページに次のゲートウェイキーオプションが表示されます。
  - **「新しい鍵を生成し、すべてのゲートウェイを同期させる」**
    最初からセキュリティー保護されたゲートウェイ環境を有効にする場合は、このオプションを選択します。このオプションは、新しいゲートウェイキーを生成し、それをすべてのゲートウェイに送信します。
  - **「現在のゲートウェイ鍵を使用して、すべてのゲートウェイを同期させる」**
    新しいゲートウェイ、または新しいゲートウェイキーが送信されていないゲートウェイを同期させる場合に選択します。すべてのゲートウェイが現在のゲートウェイキーを使用して同期されている状況で 1 つのゲートウェイが停止した場合、または新規ゲートウェイにキーを更新させる場合は、このオプションを選択します。
- **「バックアップ用にサーバー暗号化キーをエクスポート」** − 既存のサーバー暗号化キーを XML 形式のファイルにエクスポートする場合に選択します。このオプションを選択すると、追加フィールドが表示され、キーをエクスポートするためのパスおよびファイル名を指定できます。

注 PKCS#5 暗号化を使用しているときに、新しいサーバー暗号化キーを生成および設定することを選択した場合には、このオプションも選択する必要があります。さらに、エクスポートしたキーは、リムーバブルメディアに保存した上で、ネットワークに接続されていない安全な場所に保管する必要があります。

- **「実行モード」** − このタスクをバックグラウンド (デフォルトオプション) またはフォアグラウンドのどちらで実行するかを選択します。新しく生成したキーを使用して 1 つ以上のオブジェクトタイプを再暗号化する場合には、時間がかかることがあるため、バックグラウンドで実行することをお勧めします。

セキュリティーの実装

Identity Manager 管理者は、セットアップ時とそれ以降に以下の推奨事項に従うことで、保護されたアカウントおよびデータに対するセキュリティー上のリスクをさらに軽減できます。

セットアップ時

以下の操作を実行する必要があります。

- https を使用するセキュアな Web サーバーを通じて Identity Manager にアクセスする。
- デフォルトの Identity Manager 管理者アカウント (Administrator と Configurator) 用のパスワードをリセットする。これらのアカウントのセキュリティーをさらに向上させるには、アカウント名を変更します。
- Configurator のアカウントへのアクセス権を制限する。
- 管理者の機能セットをその職務権限に必要な操作のみに制限し、組織階層をセットアップして管理者の機能を制限する。
- Identity Manager インデックスリポジトリのデフォルトパスワードを変更する。
- Identity Manager アプリケーションでのアクティビティーの追跡の監査をオンにする。
- Identity Manager ディレクトリのファイルに対する権限を編集する。
- 承認またはほかのチェックポイントを挿入してワークフローをカスタマイズする。
- 復旧手順を作成して、緊急の際に Identity Manager 環境を復旧する方法を記述しておく。

実行時

以下の操作を実行する必要があります。

- デフォルトの Identity Manager 管理者アカウント (Administrator と Configurator) 用のパスワードを定期的に変更する。
- システムをあまり使用していないときには Identity Manager からログアウトする。
- Identity Manager セッションのデフォルトのタイムアウト期間を設定する、あるいは既存の設定値を知っておく。セッションタイムアウト値は各ログインアプリケーションに別々に設定できるため、異なる可能性があります。

アプリケーションサーバーが Servlet 2.2 準拠の場合、Identity Manager のインストールプロセスでは、http セッションのタイムアウトをデフォルトの 30 分に設定します。この値はプロパティーを編集して変更できますが、セキュリティーを向上させるため、この値を低く設定する必要があります。30 分を超える値を設定しないでください。

セッションのタイムアウト値を変更するには、次を実行します。

1. `web.xml` ファイルを変更します。
   このファイルは、アプリケーションサーバーのディレクトリツリーの `idm/WEB-INF` ディレクトリにあります。
2. 次の行の数値を変更します。

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

第 11 章

アイデンティティー監査

この章では、監査の管理を設定して企業情報システムおよびアプリケーションの監査とコンプライアンスを監視および管理するための Identity Manager 機能について説明します。

アイデンティティー監査について

Identity Manager では、社内外のポリシーと規制に対するコンプライアンスを確保するために、企業全体のアイデンティティーデータを体系的に捉えて、分析し、必要な処理を行う (応答する) ことを監査と定義します。

アカウンティングおよびデータプライバシーの法律へのコンプライアンスは簡単な作業ではありません。Identity Manager の監査機能は柔軟な方法で、各企業に有効なコンプライアンスソリューションを実装できます。

大半の環境で、内部および外部の監査チーム (監査が最も重要と考える) と監査以外のスタッフ (監査を迷惑と考えていることもある) のさまざまなグループがコンプライアンスにかかわっています。IT もコンプライアンスにかかわることが多く、内部監査チームの要件を、選択されたソリューションの実装に移行する支援を行います。監査ソリューションの実装の成功に重要なのが、監査以外のスタッフの知識、コントロール、プロセスを正確に把握し、その情報の利用を自動化することです。

この章では、監査レビューの実施方法や、セキュリティー制御を継続的に行い、法規制のコンプライアンスを管理する上で役立つ手法の実装方法を中心に、監査機能について説明します。

この章では、次の概念およびタスクについて説明します。

- アイデンティティー監査の目的
- アイデンティティー監査について
- 監査ログの有効化
- 管理者インタフェースの「コンプライアンス」エリア

- 監査ポリシーについて
- 監査ポリシーの操作
- 監査ポリシーの割り当て
- 監査ポリシーのスキャンとレポート
- コンプライアンス違反の是正と受け入れ
- 定期的アクセスレビューとアテステーション
- アイデンティティー監査タスクのリファレンス

アイデンティティー監査の目的

アイデンティティー監査ソリューションでは、以下の方法により、監査のパフォーマンスを容易に向上させることができます。

- *コンプライアンス違反を自動的に検出し、即時に通知することで、迅速な是正を促進する*

  Identity Manager の監査ポリシー機能で、違反の「規則」(条件) を定義できます。定義後は、承認されていないアクセス変更や誤ったアクセス特権など、設定されたポリシーに違反する条件がシステムによってスキャンされます。違反が検出されると、定義されたエスカレーションチェーンに従って適切な人物に通知されます。その後、ユーザーが呼び出したタスク、またはポリシー違反によって自動的に呼び出されたワークフローで、その違反を是正 (訂正) できます。

- *内部監査管理の効果に関する主要な情報をオンデマンドで提供する*

  監査レポートに、違反や例外に関するステータス情報の概要が表示され、危険なステータスをすばやく分析できます。「レポート」タブにも、違反に関するグラフ形式のレポートが表示されます。定義したレポート特性に従って各グラフをカスタマイズし、リソース別、組織別、またはポリシー別に違反を表示できます。

- *アイデンティティー管理のアテステーションレビューを自動化することで操作上のリスクを減らす*

  ワークフロー機能で、選択したレビューアにポリシー違反およびアクセス違反を自動通知できます。

- *ユーザーアクティビティーの詳細を示し、法的要件を満たす包括的なレポートを作成する*

  「レポート」エリアで、アクセスの履歴、特権およびその他のポリシー違反に関する情報を表示する詳細レポートおよびグラフを定義できます。セキュリティー保護された包括的なアイデンティティー監査証跡がシステムに維持され、レポート機能を使用してアクセスデータやユーザープロファイルの更新について調べることができます。

- *セキュリティーおよび法規制のコンプライアンスを維持するための定期的なレビューのプロセスを簡素化する*

  定期的アクセスレビューを実施することで、ユーザーエンタイトルメントレコードを収集し、レビューが必要なエンタイトルメントを判断できます。さらに、このプロセスは指定されたアテスターに保留中のリクエストを通知し、アテスターがリクエストに対する操作を完了した場合はそのステータスまたは保留中のリクエストを更新します。

- *利益相反する可能性があるユーザーアカウントの機能を特定する*

  Identity Manager では、職務分掌レポートを使用して、利益相反する可能性がある特定の機能または特権を持つユーザーを特定することができます。

アイデンティティー監査について

Identity Manager では、ユーザーアカウントの特権とアクセス権を監査し、コンプライアンスを維持および保証するため、2 つの異なる機能を提供しています。それらの機能は、ポリシーベースのコンプライアンスと、定期的アクセスレビューです。

ポリシーベースのコンプライアンス

Identity Manager の監査ポリシー機能を用いることで、管理者はすべてのユーザーアカウントについて、会社が設定した要件に対するコンプライアンスを維持できます。

監査ポリシーを使用して、継続的コンプライアンスと定期的コンプライアンスという 2 とおりの相補的な方法でコンプライアンスを確保できます。

この 2 つの方法を相補的に使用することは、Identity Manager 以外でプロビジョニング操作が実行される可能性がある環境では特に有用です。既存の監査ポリシーを実行または遵守しないプロセスによってアカウントが変更される可能性がある場合は、定期的コンプライアンスが必要です。

継続的コンプライアンス

継続的コンプライアンスでは、現在のポリシーに準拠しない方法でアカウントを修正できないように、すべてのプロビジョニング操作にポリシーが適用されます。

継続的コンプライアンスを有効にするには、組織またはユーザー、あるいはその両方に監査ポリシーを割り当てます。ユーザーに対して実行されるプロビジョニング操作では、ユーザーに割り当てられたポリシーと組織に割り当てられたポリシーの両方が評価されます。ポリシー評価の結果、違反が検出されると、プロビジョニング操作が中断されます。

組織ベースのポリシーセットは階層構造で定義されます。各ユーザーに有効な組織ポリシーセットは 1 つだけです。もっとも下位レベルにある組織に対して割り当てられたポリシーセットが、実際に適用されます。次に例を示します。

所属している組織	直接割り当てられたポリシーセット	有効なポリシー
Austin	ポリシー A1、A2	ポリシー A1、A2
マーケティング		ポリシー A1、A2
開発	ポリシー B、C2	ポリシー B、C2
サポート		ポリシー B、C2
テスト	ポリシー D、E5	ポリシー D、E5
財務		ポリシー A1、A2
Houston		< なし >

定期的コンプライアンス

定期的コンプライアンスでは、リクエストがあったときに Identity Manager によってポリシーが評価されます。準拠しない状況があればコンプライアンス違反として取得されます。

定期的コンプライアンスのスキャンを実行するときに、スキャンに使用するポリシーを選択できます。スキャンプロセスでは、直接割り当てられたポリシー (ユーザーに割り当てられたポリシーと組織に割り当てられたポリシー) と、任意に選択したポリシーセットが併用されます。

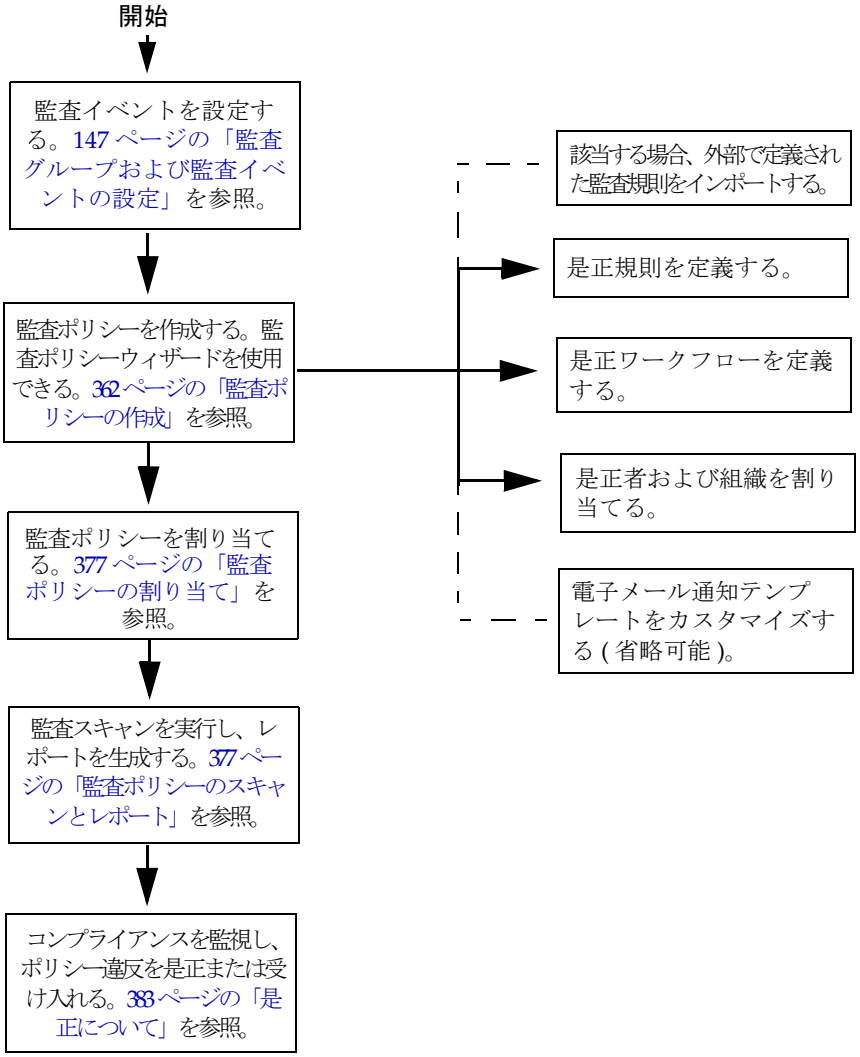
Auditor Administrator 機能を持つ Identity Manager ユーザーは、監査ポリシーを作成し、定期的なポリシースキャンとポリシー違反のレビューによってそれらのポリシーのコンプライアンスを監視することができます。違反は、是正手順と受け入れ手順によって管理できます。

Auditor Administrator 機能の詳細については、166 ページの「機能とその管理について」を参照してください。

Identity Manager による監査では、ユーザーの定期的なスキャンが可能であり、監査ポリシーの実行によって、設定されているアカウント制限からの逸脱が検出されます。違反が検出されると、是正のアクティビティーが開始されます。規則には、Identity Manager に付属する標準の監査ポリシー規則、またはカスタマイズされたユーザー定義の規則を使用できます。

ポリシーベースのコンプライアンスの論理タスクフロー

次の図は、この節で説明する監査タスクを完了するための論理タスクフローを示しています。



定期的アクセスレビュー

Identity Manager の定期的アクセスレビューを使用すると、マネージャーおよびその他の責任者は、そのつど、または定期的に、ユーザーアクセス特権のレビューと検証を行うことができます。この機能の詳細については、392 ページの「定期的アクセスレビューとアテステーション」を参照してください。

監査ログの有効化

コンプライアンス管理およびアクセスレビューを開始するには、Identity Manager 監査ログシステムを有効にし、監査イベントを収集するように設定する必要があります。デフォルトで、監査システムは有効になっています。Configure Audit 機能を持つ Identity Manager 管理者が監査を設定できます。

Identity Manager には、Compliance Management 監査設定グループが用意されています。Compliance Management グループに格納されたイベントを表示または修正するには、メニューバーの**「設定」**を選択し、**「監査」**をクリックします。「監査設定」ページで、**「Compliance Management」**という監査グループ名を選択します。

監査設定グループの設定の詳細については、「設定」の章の147 ページの「監査グループおよび監査イベントの設定」を参照してください。

監査システムでのイベントの記録方法については、第 12 章「監査ログ」を参照してください。

電子メールテンプレート

アイデンティティー監査では、多くの操作で電子メールベースの通知が使われます。これらの各通知には、電子メールテンプレートオブジェクトが使われます。電子メールテンプレートでは、電子メールメッセージのヘッダーと本文をカスタマイズできます。

表 11-1 アイデンティティー監査電子メールテンプレート

テンプレート名	目的
Access Review Remediation Notice	ユーザーエンタイトルメントが最初に是正状態で作成された場合に、アクセスレビューによって是正者に送信されます。
Bulk Attestation Notice	保留中のアテステーションがある場合に、アクセスレビューによってアテスターに送信されます。
Policy Violation Notice	違反が発生した場合に、監査ポリシースキャンによって是正者に送信されます。

表 11-1　アイデンティティー監査電子メールテンプレート (続き)

テンプレート名	目的
Access Scan Begin Notice	アクセスレビューのスキャンが開始されると、アクセススキャン所有者に送信されます。
Access Scan End Notice	アクセススキャンが完了すると、アクセススキャン所有者に送信されます。

管理者インタフェースの「コンプライアンス」エリア

監査ポリシーは、Identity Manager 管理者インタフェースの「コンプライアンス」エリアで作成および管理します。メニューバーの**「コンプライアンス」**を選択して、「ポリシーの管理」ページにアクセスします。このページには、自分が表示と編集の権限を持っているポリシーが一覧表示されます。また、アクセススキャンもこのエリアで管理できます。

ポリシーの管理

「ポリシーの管理」ページでは、監査ポリシーを操作して次のタスクを実行できます。

- 監査ポリシーの作成
- 表示または編集するポリシーの選択
- ポリシーの削除

これらのタスクの詳細については、「監査ポリシーの操作」を参照してください。

アクセススキャンの管理

アクセススキャンを作成、変更、および削除するには、「コンプライアンス」エリアの**「アクセススキャンの管理」**タブを使用します。ここから、定期的アクセスレビューで実行またはスケジュールするスキャンを定義できます。この機能の詳細については、392 ページの「定期的アクセスレビューとアテステーション」を参照してください。

アクセスレビュー

「コンプライアンス」エリアの「アクセスレビュー」タブで、アクセスレビューの起動、終了、削除、進行状況の監視を実行できます。このタブには、スキャン結果の概要レポートと情報リンクが表示され、情報リンクからレビューのステータスおよび保留中のアクティビティーに関するさらに詳細な情報にアクセスできます。

この機能の詳細については、402 ページの「アクセスレビューの管理」を参照してください。

監査ポリシーについて

監査ポリシーは、1 つ以上のリソースのユーザーのセットに対するアカウント制限を定義します。監査ポリシーは、ポリシーの制限を定義する「規則」と、発生した違反を処理する「ワークフロー」から構成されます。監査スキャンでは、監査ポリシーに定義された条件を使用して、組織内で違反が発生しているかどうかを評価します。

監査ポリシーは次のコンポーネントで構成されます。

- **ポリシー規則**。特定の違反を定義します。XPRESS、XML オブジェクト、または JavaScript 言語で作成された関数を含めることができます。
- **是正ワークフロー**。監査スキャンでポリシー規則違反が検出されたときに、オプションとして起動されます。
- **是正者**。ポリシー違反に応答することが許可されている、指定されたユーザー。是正者は、個別のユーザーでもユーザーグループでもかまいません。

監査ポリシー規則

監査ポリシー内では、規則によって、属性に基づいた競合の可能性を定義します。1 つの監査ポリシーに、広範囲のリソースを参照する多数の規則を含めることができます。規則の評価時に、規則は 1 つ以上のリソースからのユーザーアカウントデータにアクセスします。監査ポリシーで、規則に使用できるリソースを制限できます。

1 つのリソースの 1 つの属性のみをチェックする規則、または複数のリソースの複数の属性をチェックする規則を設定できます。

規則の subType は、`SUBTYPE_AUDIT_POLICY_RULE` または `SUBTYPE_AUDIT_POLICY_SOD_RULE` である必要があります。監査ポリシーウィザードで生成される規則、または監査ポリシーウィザードによって参照される規則には、自動的にこの subType が割り当てられます。

規則の authType は AuditPolicyRule である必要があります。監査ポリシーウィザードで生成される規則には、自動的にこの authType が割り当てられます。

規則のロジックの説明については、『Identity Manager 配備ツール』の「規則の操作」を参照してください。

是正ワークフロー

ポリシー違反を定義する規則を作成したあとは、監査スキャンで違反が検出されたときに起動するワークフローを選択します。Identity Manager には、監査ポリシースキャンのデフォルトの是正処理を提供するデフォルトの標準是正ワークフローが用意されています。たとえば、このデフォルトの是正ワークフローでは、レベル 1 是正者として指定された各是正者に対して通知電子メールが生成され、必要な場合はそれ以下のレベルの是正者にも生成されます。

注 Identity Manager ワークフロープロセスとは異なり、是正ワークフローには AuthType=AuditorAdminTask および SUBTYPE_REMEDIATION_WORKFLOW のサブタイプを割り当てる必要があります。監査スキャンで使用するワークフローをインポートする場合は、この属性を手動で追加する必要があります。詳細については、363 ページの「(省略可能) ワークフローを Identity Manager にインポートする」を参照してください。

是正者

是正ワークフローを割り当てる場合は、1 人以上の是正者を指定する必要があります。3 レベルまでの監査ポリシーの是正者を指定できます。是正に関する詳細については、この章の「コンプライアンス違反の是正と受け入れ」を参照してください。

是正者を割り当てるには、その前に是正ワークフローを割り当てる必要があります。

監査ポリシーのシナリオ例

買掛金と売掛金の責任者は、経理部で働く従業員が担当する金額の総計が危険な額に達しないようにするための措置を講じる必要があります。このポリシーでは、買掛金の担当者が売掛金の担当も兼ねていないかどうかを確認する必要があります。

監査ポリシーには、次のものが含まれます。

- 4 つの規則のセット。それぞれ、ポリシー違反となる条件を指定します。
- 是正タスクを起動するワークフロー

- 前述の規則で作成されたポリシー違反を参照し、それに応答する権限を持つ、指定された管理者 (是正者) のグループ

規則によってポリシー違反 (この例では、過剰な権限を持つユーザー) が検出されると、関連付けられたワークフローで特定の是正関連タスク (指定された是正者への自動通知など) を起動することができます。

レベル 1 是正者は、監査スキャンでポリシー違反が検出されたときに連絡される最初の是正者です。監査ポリシーで 2 レベル以上の是正者が指定されている場合、このエリアで指定されたエスカレーション期間を過ぎると、Identity Manager は次のレベルの是正者に通知します。

監査ポリシーの操作

Identity Manager の監査ポリシーウィザードを使用すると、監査ポリシーを設定できます。監査ポリシーの定義後、そのポリシーに対して、変更や削除など、さまざまなアクションを実行できます。この節のトピックでは、監査ポリシーおよび監査ポリシー規則を作成および管理する方法を説明します。

さらに、監査ポリシーウィザードでは規則を作成できますが、作成できる規則のタイプが限られます。より厳密な規則を作成してウィザードで使用する場合は、Identity Manager IDE を使用してください。

デフォルトで、ウィザードで作成される規則の authType は `AuditPolicyRule` です。ウィザードまたは Identity Manager IDE を使用して作成する監査ポリシー規則では、この authType を指定するようにしてください。

規則の subType は `SUBTYPE_AUDIT_POLICY_RULE` である必要があります。監査ポリシーウィザードで生成される規則には、自動的にこの subType が割り当てられます。

監査ポリシーの作成

監査ポリシーウィザードでは、監査ポリシーの作成手順を、順を追って説明します。監査ポリシーウィザードにアクセスするには、インタフェースの**「コンプライアンス」**エリアで**「ポリシーの管理」**をクリックして、新しい監査ポリシーを作成します。

ウィザードでは、次のタスクを実行して監査ポリシーを作成します。

- ポリシー制限の定義に使用する規則の選択または作成
- 承認者の割り当てとエスカレーション制限の設定
- 是正ワークフローの割り当て

各ウィザード画面に表示されたタスクを完了したら、「**次へ**」をクリックして次の手順に進みます。

開始する前に

監査ポリシーを作成する前に、以下の作業も含めて十分に計画を練ります。

- 監査ポリシーウィザードでポリシーの作成に使用する規則を特定する。選択する規則は、作成するポリシーのタイプと、定義する特定の制限によって決まります。
- 新しいポリシーに含める是正ワークフローまたは規則をインポートする。
- 監査ポリシーの作成に必要な機能を持っていることを確認する。必要な機能については、166 ページの「機能とその管理について」を参照してください。

必要な規則の特定

ポリシーで指定する制限は、作成またはインポートする規則セットに実装されます。監査ポリシーウィザードを使用して規則を作成する場合、次の操作を行います。

1. 操作する特定のリソースを指定します。
2. リソースで有効な属性のリストからアカウント属性を選択します。
3. その属性に課す条件を選択します。
4. 比較用の値を入力します。

(省略可能) 職務分掌規則を Identity Manager にインポートする

監査ポリシーウィザードでは、職務分掌規則を作成できません。それらの規則は、Identity Manager 以外で作成し、「**設定**」タブの「**交換ファイルのインポート**」を使用してインポートする必要があります。

(省略可能) ワークフローを Identity Manager にインポートする

現在 Identity Manager から利用できない是正ワークフローを使用するには、次のタスクを完了して外部ワークフローをインポートします。

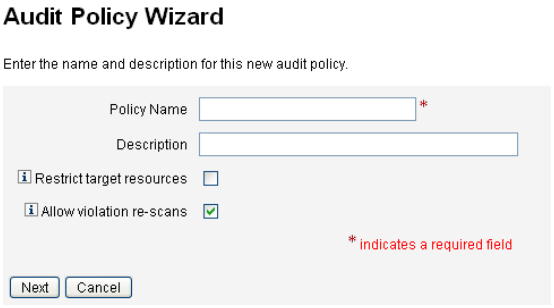
1. `authType='AuditorAdminTask'` を設定し、`subtype='SUBTYPE_REMEDIATION_WORKFLOW'` を追加します。これらの設定オブジェクトを設定するには、Identity Manager IDE または任意の XML エディタを使用します。
2. 「交換ファイルのインポート」オプションを使用してワークフローをインポートします。この機能には「**設定**」タブからアクセスできます。

ワークフローが正常にインポートされると、監査ポリシーウィザードの「是正ワークフロー」のオプションリストに、そのワークフローが表示されます。

監査ポリシーの名前と説明の指定

監査ポリシーウィザード (図 11-1 を参照) で、新しいポリシーの名前と簡単な説明を入力します。

図 11-1　監査ポリシーウィザード : 名前と説明の入力画面



注　監査ポリシー名には、次の文字を含めることはできません。' (アポストロフィー)、. (ピリオド)、| (パイプ)、[(左角括弧)、] (右角括弧)、, (カンマ)、: (コロン)、$ (ドル記号)、" (二重引用符)、= (等号)。

スキャンの実行時のアクセス対象を、選択したリソースだけに制限する場合は、**「ターゲットリソースを制限」**オプションを有効にします。

違反の是正として、ただちにユーザーを再スキャンさせる場合は、**「違反の再スキャンを許可」**オプションを有効にします。

注　監査ポリシーでリソースを制限しない場合、スキャンでは、ユーザーがアカウントを持つすべてのリソースがアクセスされます。規則で使用するリソースが少ない場合は、ポリシーの適用をそれらのリソースに限定するほうが効率的です。

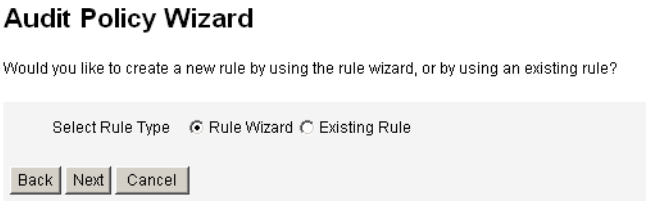
「次へ」をクリックして次のページに進みます。

規則のタイプの選択

このページで、ポリシーの規則を定義または追加するプロセスを開始します。ポリシー作成時の作業の大部分は、規則の定義と作成です。

図 11-2 に示すように、Identity Manager の規則ウィザードを使用して独自の規則を作成するか、または既存の規則を組み込むことができます。デフォルトでは、「規則ウィザード」オプションが選択されています。**「次へ」**をクリックして規則ウィザードを起動し、規則の作成手順を説明する 368 ページの「規則ウィザードを使用した新しい規則の作成」に進みます。

図 11-2 監査ポリシーウィザード : 規則のタイプの選択画面



既存の規則の選択

新しいポリシーに既存の規則を含める場合は、規則のオプションを選択するときに**「既存の規則」**をクリックします。次に、**「次へ」**をクリックし、アクセスできる既存の監査ポリシー規則を表示して選択します。

「規則」オプションリストから追加する規則を選択し、**「次へ」**をクリックします。

注 以前に Identity Manager にインポートした規則の名前が表示されない場合は、360 ページの「監査ポリシー規則」で説明した追加属性をその規則に追加したことを確認してください。

規則の追加

ウィザードで追加の規則を作成したり、規則をインポートしたりすることができます。規則ウィザードでは、1 つの規則で使用できるリソースは 1 つだけです。インポートした規則では、必要なだけの数のリソースを参照できます。

必要な場合は、**「AND」**または**「OR」**をクリックして、規則の追加を続行します。規則を削除するには、規則を選択して**「削除」**をクリックします。

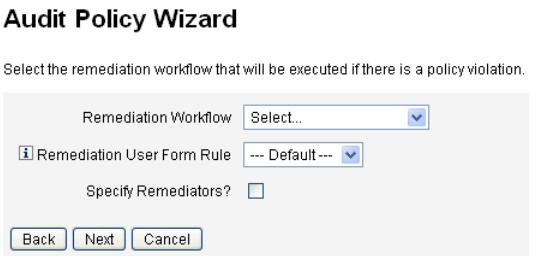
ポリシー違反が発生するのは、すべての規則のブール式が true と評価した場合だけです。AND/OR 演算子で規則をグループ化すると、すべての規則が true でなくても、ポリシーが true と評価される可能性があります。Identity Manager では、true と評価された規則についてのみ、およびポリシー式が true と評価された場合にのみ違反が発生します。監査ポリシーウィザードでは、入れ子になったブール式を明示的に制御しないため、深い式を作成しないことをお勧めします。

是正ワークフローの選択

この画面で、このポリシーに関連付ける是正ワークフローを選択します。ここで割り当てたワークフローによって、監査ポリシー違反が検出されたときに Identity Manager で実行されるアクションが決まります。

注 違反が検知された監査ポリシーごとに 1 つのワークフローが起動します。各ワークフローには、特定のポリシーのポリシースキャンによって作成されたコンプライアンス違反ごとに、1 つまたは複数の作業項目が含まれます。

図 11-3 監査ポリシーウィザード : 是正ワークフローの選択画面



注 XML エディタまたは Identity Manager Integrated Development Environment (IDE) を使用して作成したワークフローのインポートについては、363 ページの「(省略可能) ワークフローを Identity Manager にインポートする」を参照してください。

「是正ユーザーフォーム規則」を選択して、是正によってユーザーを編集する際に適用されるユーザーフォームの生成に使用する規則を選択します。デフォルトでは、是正作業項目に対応してユーザーを編集する是正者は、是正者に割り当てられたユーザーフォームを使用します。監査ポリシーで是正ユーザーフォームを指定すると、このフォームが代わりに使用されます。これにより、監査ポリシーで対応する特定の問題を示す場合に、厳密に限定されたフォームを使うことができます。

この是正ワークフローに関連付ける是正者を指定する場合は、**「是正者の指定」**を選択します。このオプションを有効にして**「次へ」**をクリックすると、是正者の割り当てページが表示されます。このオプションを有効にしなかった場合は、組織の割り当て画面が次に表示されます。

是正者と是正タイムアウトの選択

是正者を指定した場合、この監査ポリシーの違反が検出されると、このポリシーに割り当てられた是正者に通知されます。さらに、デフォルトのワークフローで是正作業項目が是正者に割り当てられます。すべての Identity Manager ユーザーが是正者になることができます。

1 人以上のレベル 1 是正者、すなわち、指定されたユーザーを割り当てることができます。レベル 1 是正者は、ポリシー違反が検出されたときに、是正ワークフローによって送信される電子メールで最初に連絡を受けます。指定されたエスカレーションタイムアウト時間に達するまでにレベル 1 是正者が応答しなかった場合、Identity Manager は次に、ここに指定されたレベル 2 是正者に連絡します。エスカレーション期間が経過するまでにレベル 1 是正者もレベル 2 是正者も応答しなかった場合にのみ、Identity Manager がレベル 3 是正者に連絡します。

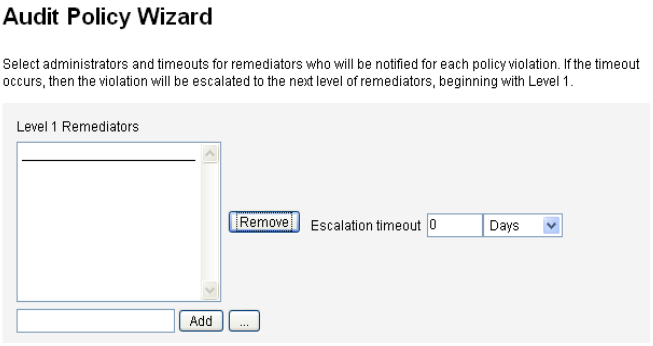
注	選択した最高レベルの是正者に対してエスカレーションタイムアウト値を指定した場合、エスカレーションがタイムアウトすると、リストから作業項目が削除されます。デフォルトでは、エスカレーションタイムアウトは 0 の値に設定されています。この場合、作業項目は期限切れにならず、是正者リストに残ります。

是正者の割り当ては省略可能です。このオプションを選択する場合は、「是正者の指定」チェックボックスを有効にして、次の画面に進みます。

是正者の利用可能リストにユーザーを追加するには、ユーザー ID を入力して、**「追加」**をクリックします。または、**「...」**ボタンをクリックして、ユーザー ID を検索します。「が次の文字列で始まる」フィールドに 1 文字以上入力して、**「検索」**をクリックします。検索リストからユーザーを選択したら、**「追加」**をクリックして、是正者のリストに追加します。**「閉じる」**をクリックして、検索エリアを閉じます。

是正者のリストからユーザー ID を削除するには、リストのユーザー ID を選択して、**「削除」**をクリックします。

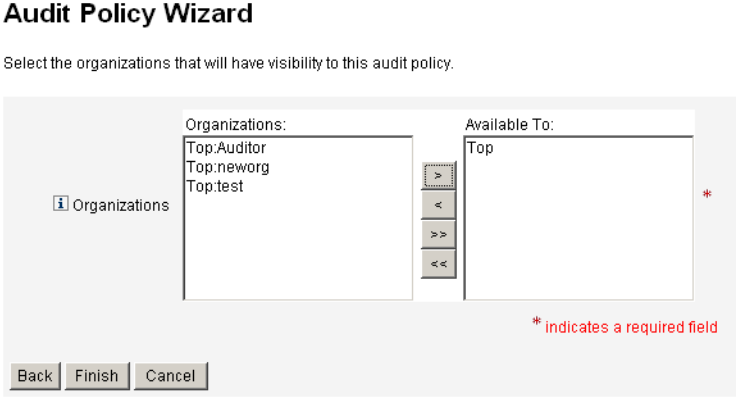
図 11-4　監査ポリシーウィザード : レベル 1 是正者の選択エリア



このポリシーにアクセスできる組織の選択

図 11-5 に示すように、この画面では、このポリシーを表示および編集できる組織を選択します。

図 11-5　監査ポリシーウィザード : 閲覧を許可された組織の割り当て画面



組織を選択したら、「**完了**」をクリックして監査ポリシーを作成し、「ポリシーの管理」ページに戻ります。新しく作成したポリシーがこのリストに表示されます。

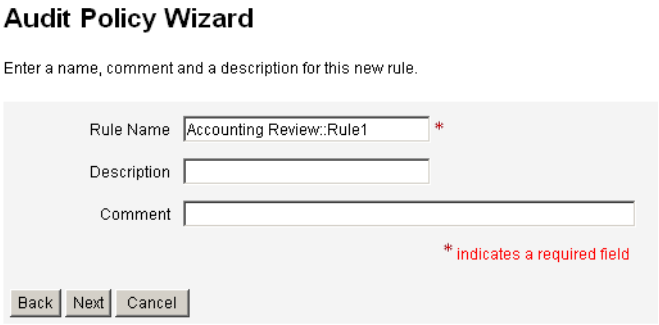
規則ウィザードを使用した新しい規則の作成

監査ポリシーウィザードで「規則ウィザード」を選択して規則を作成する場合は、次の節で説明するページに情報を入力していきます。

新しい規則の名前と説明の指定

オプションの作業として新しい規則に名前を付けて説明します。このページでは、Identity Manager で規則が表示されるときに規則名の横に表示される説明テキストを入力します。規則の内容を示す簡潔でわかりやすい説明を入力します。この説明は、Identity Manager の「ポリシー違反のレビュー」ページ内に表示されます。

図 11-6　監査ポリシーウィザード : 規則の説明の入力画面



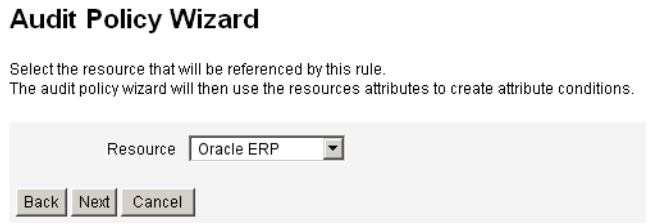
たとえば、Oracle ERP responsibilityKey の `Payable User` 属性値と `Receivable User` 属性値の両方を持つユーザーを検出する規則を作成する場合であれば、「説明」フィールドに「**`Payable User と Receivable User の両方の役割を持つユーザーを検出する`**」のようにテキストを入力します。

規則に関する追加情報を入力する場合は、「コメント」フィールドを使用します。

規則で参照するリソースの選択

このページでは、規則で参照するリソースを選択します。各規則変数は、このリソースの属性に対応している必要があります。このオプションリストには、表示アクセス権を持つすべてのリソースが表示されます。この例では、「Oracle ERP」が選択されています。

図 11-7　監査ポリシーウィザード : リソースの選択画面



注	使用可能な各リソースアダプタのほとんどの属性 (ただし全部ではない) がサポートされています。使用可能な個々の属性については、『Identity Manager リソースリファレンス』を参照してください。

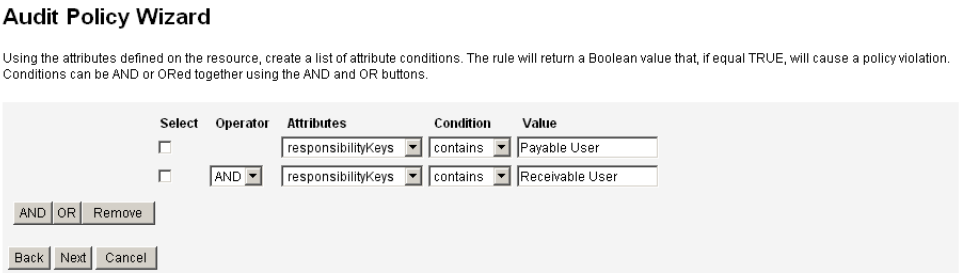
「次へ」をクリックして次のページに進みます。

規則式の作成

この画面では、新しい規則の規則式を入力します。この例では、Oracle ERP responsibilityKey の `Payable User` 属性値を持つユーザーは `Receivable User` 属性値を同時に持つことができないという規則を作成します。

1. 使用可能な属性のリストからユーザー属性を選択します。この属性は、規則変数に直接対応します。
2. リストから論理条件を選択します。有効な条件には、「=」(等しい)、「!=」(等しくない)、「<」(より小さい)、「<=」(より小さいまたは等しい)、「>」(より大きい)、「>=」(より大きいまたは等しい)、「が true である」、「が null である」、「が null でない」、「が空の文字列である」、および「が右の文字列を含む」があります。この例では、使用できる属性条件のリストから「`contains`」を選択します。
3. 式の値を入力します。たとえば、「`Payable user`」と入力した場合は、responsibilityKeys の `Payable user` 属性値を持つ Oracle ERP ユーザーを指定したことになります。
4. (省略可能)「**AND**」または「**OR**」演算子をクリックし、行を追加して、別の式を作成します。

図 11-8　監査ポリシーウィザード : 規則式の選択画面



この規則はブール値を返します。両方のステートメントが true の場合、ポリシー規則は、ポリシー違反となる TRUE の値を返します。

注 Identity Manager では、入れ子になった規則の制御はサポートされません。複数の規則が指定されている場合は常に、最初は AND 演算子、次に OR に従ってポリシーが評価されます。たとえば、R1 AND R2 AND R3 or R4 AND R5 は、(R1 + R2 + R3) | (R4 + R5) と解釈されます。

次のコード例は、この画面で作成した規則の XML を示しています。

コード例 11-1 新しく作成した規則の XML 構文の例

```
<Description>Payable User/Receivable User</Description>
  <RuleArgument name='resource' value='Oracle ERP'>
    <Comments>Resource specified when  audit policy was created.</Comments>
    <String>Oracle ERP</String>
  </RuleArgument>
    <and>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Receivable User</s>
      </contains>
      <contains>
        <ref>accounts[Oracle ERP].responsibilityKeys</ref>
        <s>Payables User</s>
      </contains>
    </and>
    <MemberObjectGroups>
      <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
    </MemberObjectGroups>
</Rule>
```

規則から式を削除するには、属性条件を選択して**「削除」**をクリックします。

「次へ」をクリックして監査ポリシーウィザードを続行します。さらに、ウィザードを使用して新しい規則を作成するか、既存の規則を追加するかのいずれかの方法で規則を追加することもできます。

監査ポリシーの編集

監査ポリシーに関する一般的な編集タスクは次のとおりです。

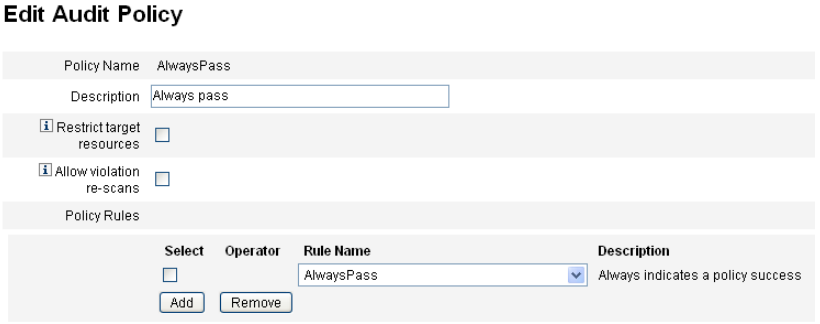
- 規則を追加または削除する
- ターゲットリソースを変更する
- ポリシーにアクセスできる組織のリストを調整する
- 各レベルの是正に関連付けられたエスカレーションタイムアウトを変更する
- ポリシーに関連付けられた是正ワークフローを変更する

ポリシーの編集ページ

監査ポリシー名の列でポリシーの名前をクリックして「監査ポリシーの編集」ページを開きます。このページでは、監査ポリシーに関する情報が次のエリアに分類されています。

- 識別と規則のエリア
- 是正者とエスカレーションタイムアウトのエリア
- ワークフローと組織のエリア

図 11-9　「監査ポリシーの編集」ページ : 識別と規則のエリア



ページのこのエリアでは、次の操作を行うことができます。

- ポリシーの説明の編集
- 規則の追加または削除

注　この製品で既存の規則を直接編集することはできません。Identity Manager IDE または XML エディタを使用して規則を編集してから、Identity Manager にインポートします。その後、以前のバージョンの規則を削除して、改訂バージョンの規則を追加します。

監査ポリシーの説明の編集

監査ポリシーの説明を編集するには、「説明」フィールド内のテキストを選択し、新しいテキストを入力します。

オプションの編集

オプションの作業として、**「ターゲットリソースを制限」**オプションまたは**「違反の再スキャンを許可」**オプションを選択するか、選択解除します。

ポリシーの規則の削除

ポリシーの規則を削除するには、規則名の前にある**「選択」**ボタンをクリックし、**「削除」**をクリックします。

ポリシーへの規則の追加

「追加」をクリックして新しいフィールドを追加し、そのフィールドで、追加する規則を選択します。

ポリシーで使用する規則の変更

「規則名」列で、選択リストから別の規則を選択します。

「是正者」エリア

図 11-10 に、レベル 1、レベル 2、レベル 3 のポリシーの是正者を割り当てるための「是正者」エリアの一部を示します。

図 11-10　「監査ポリシーの編集」ページ : 是正者の割り当て

ページのこのエリアでは、次の操作を行うことができます。

- ポリシーの是正者の削除または割り当て
- エスカレーションタイムアウトの調整

是正者の削除または割り当て

1 つまたは複数の是正レベルの是正者を選択するには、ユーザー ID を入力して、**「追加」**をクリックします。ユーザー ID を検索するには、**「...」**ボタンをクリックします。少なくとも 1 人の是正者を選択する必要があります。

是正者を削除するには、リストのユーザー ID を選択して、「**削除**」をクリックします。

エスカレーションタイムアウトの調整

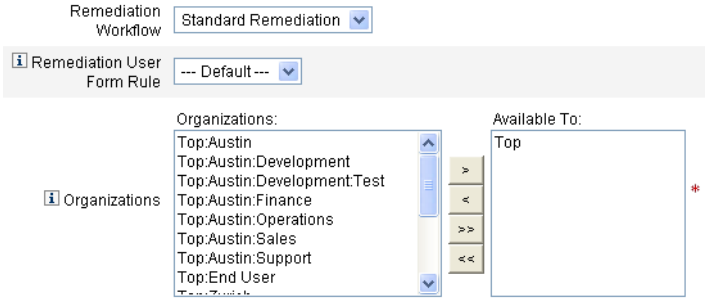
タイムアウト値を選択し、新しい値を入力します。デフォルトでは、タイムアウト値は設定されていません。

注	選択した最高レベルの是正者に対してエスカレーションタイムアウト値を指定した場合、エスカレーションがタイムアウトすると、リストから作業項目が削除されます。

是正ワークフローと組織のエリア

図 11-11 に、監査ポリシーの是正ワークフローと組織を指定するエリアを示します。

図 11-11 「監査ポリシーの編集」ページ : 是正ワークフローと組織



ページのこのエリアでは、次の操作を行うことができます。

- ポリシー違反の発生時に起動する是正ワークフローを変更する
- 是正ユーザーフォーム規則を選択する
- このポリシーにアクセスできる組織を調整する

是正ワークフローの変更

ポリシーに割り当てられたワークフローを変更するには、オプションリストから別のワークフローを選択します。デフォルトでは、ワークフローは監査ポリシーに割り当てられません。

注	監査ポリシーにワークフローが割り当てられていない場合、違反はどの是正者にも割り当てられません。

リストから是正ワークフローを選択し、**「保存」**をクリックします。

是正ユーザーフォーム規則の選択

オプションの作業として、是正によってユーザーを編集する際に適用されるユーザーフォームを生成する規則を選択します。

組織の閲覧許可の割り当てまたは削除

この監査ポリシーを使用できる組織を調整し、**「保存」**をクリックします。

サンプルポリシー

Identity Manager には、「監査ポリシー」リストからアクセス可能な次のサンプルポリシーが用意されています。

- IDM Role Comparison Policy
- IDM Account Accumulation Policy

IDM Role Comparison Policy

このサンプルポリシーを使用して、Identity Manager ロールで指定されている属性と、ユーザーの現在の属性を比較できます。このポリシーは、ロールに指定されたすべてのリソース属性がユーザーに設定されていることを確認するためのものです。

このポリシーは次の場合に違反を検知します。

- ロールに指定されたリソース属性がユーザーに含まれていない
- ユーザーのリソース属性が、ロールに指定されているものと異なる

IDM Account Accumulation Policy

このサンプルポリシーでは、ユーザーが保有するすべてのアカウントが、そのユーザーによって保有されている少なくとも 1 つのロールによって参照されていることを確認します。

ユーザーに割り当てられているリソースアカウントのうち、いずれか 1 つでも現在ユーザーに割り当てられているどのロールからも明示的に参照されていない場合、このポリシーに違反します。

監査ポリシーの削除

監査ポリシーを Identity Manager から削除すると、そのポリシーを参照する違反もすべて削除されます。

「ポリシーの管理」をクリックしてポリシーを表示した時に、インタフェースの「コンプライアンス」エリアからポリシーを削除できます。監査ポリシーを削除するには、ポリシーのリストからポリシー名を選択し、**「削除」**をクリックします。

監査ポリシーのトラブルシューティング

通常、監査ポリシーに関する問題に対処するにはポリシー規則のデバッグが最善の方法です。

規則のデバッグ

規則をデバッグするには、規則コードに次のトレース要素を追加します。

```
<block trace='true'>
<and>
    <contains>
        <ref>accounts[AD].firstname</ref>
        <s>Sam</s>
    </contains>
    <contains>
        <ref>accounts[AD].lastname</ref>
        <s>Smith</s>
    </contains>
</and>
</block>
```

問題

自分のワークフローが Identity Manager インタフェースに表示されない

解決方法

次のことを確認します。

- ワークフローに `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` 属性を追加した。このサブタイプが指定されていないワークフローは Identity Manager 管理者インタフェースに表示されません。
- authType `AuditorAdminTask` に対する権限が設定されている機能を持っている。
- ワークフローが含まれる組織を管理している。

問題

規則をインポートしましたが、監査ポリシーウィザードに表示されません。

解決方法

次のことを確認します。

- 各規則が `subtype='SUBTYPE_AUDIT_POLICY_RULE'` または `subtype='SUBTYPE_AUDIT_POLICY_SOD_RULE'` である。

- authType `AuditPolicyRule` に対する権限が設定されている機能を持っている。
- ワークフローが含まれる組織を管理している。

監査ポリシーの割り当て

組織に監査ポリシーを割り当てるには、少なくとも「Assign Organization Audit Policies」機能を持っている必要があります。ユーザーに監査ポリシーを割り当てるには、「Assign User Audit Policies」機能を持っている必要があります。「Assign Audit Policies」機能を持つユーザーは、これらの両方の機能を持ちます。

組織レベルのポリシーを割り当てるには、「アカウント」タブで「組織」を選択し、「割り当てられた監査ポリシー」リストでポリシーを選択します。

ユーザーレベルのポリシーを割り当てるには、次の手順に従います。

1. 「アカウント」エリアでユーザーをクリックします。
2. ユーザーフォームで**「コンプライアンス」**を選択します。
3. 「割り当てられた監査ポリシー」リストでポリシーを選択します。

注 ユーザーに直接割り当てられている (ユーザーアカウントや組織の割り当てによって割り当てられている) 監査ポリシーは、そのユーザーの違反の是正時に常に再評価されます。

監査ポリシーのスキャンとレポート

この節では、監査ポリシースキャンについて、および監査スキャンの実行と管理の手順について説明します。

ユーザーおよび組織のスキャン

スキャンは、選択した監査ポリシーを個々のユーザーまたは組織に対して実行します。特定の違反についてユーザーまたは組織をスキャンしたり、ユーザーまたは組織に割り当てられていないポリシーを実行したりできます。インタフェースの**「アカウント」**エリアからスキャンを起動します。

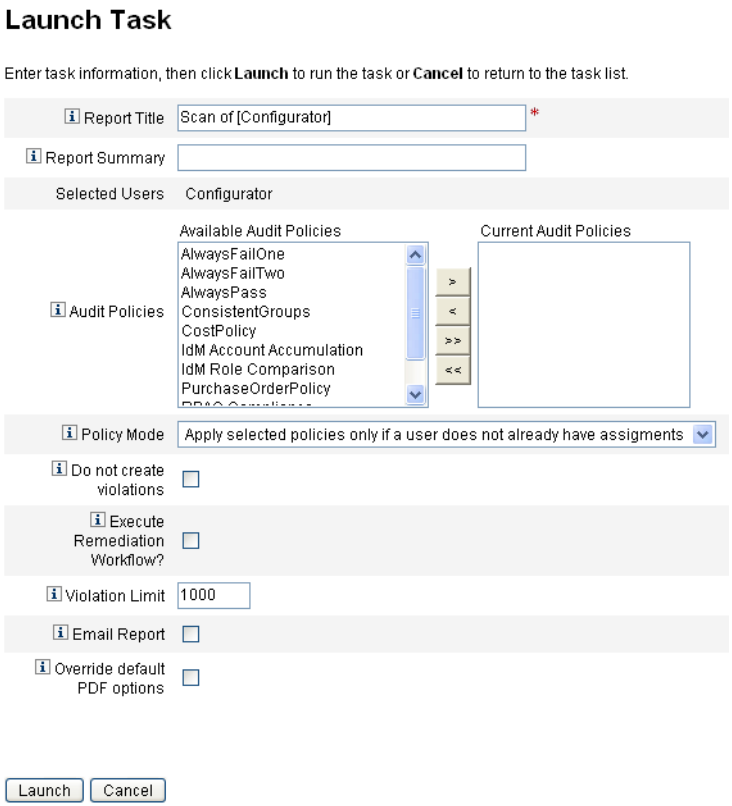
注 「サーバータスク」タブから監査ポリシースキャンを起動またはスケジュールすることもできます。

「アカウント」エリアからユーザーアカウントまたは組織のスキャンを開始するには、次の手順に従います。

1. **「アカウント」**を選択します。
2. 「アカウント」リストで、次のいずれかの操作を行います。
   a. 1 人以上のユーザーを選択し、「ユーザーアクション」オプションリストから**「スキャン」**を選択します。
   b. 1 つ以上の組織を選択し、「組織アクション」オプションリストから**「スキャン」**を選択します。

タスクの起動ダイアログが表示されます。表 11-3 は、監査ポリシーユーザースキャンの「タスクの起動」ページの例です。

図 11-12　タスクの起動ダイアログ



3. 「レポートタイトル」フィールドにスキャンのタイトルを指定します。このフィールドは必須です。任意で、「レポートの概要」フィールドにスキャンの説明を指定できます。
4. 実行する監査ポリシーを 1 つ以上選択します。少なくとも 1 つのポリシーを選択する必要があります。
5. **「ポリシーモード」**を選択します。これにより、ポリシーが割り当てられているユーザーに対して、選択したポリシーをどのように適用するかが決まります。ここで、ユーザーに割り当てられているポリシーとは、ユーザーに直接割り当てられたポリシーと、ユーザーが所属している組織に割り当てられたポリシーの両方が該当します。
6. オプションの作業として**「違反を作成しない」**オプションを選択します。このオプションを有効にすると、監査ポリシーが評価され、違反が報告されますが、コンプライアンス違反の作成または更新が行われないため、是正ワークフローも実行されません。ただし、スキャンによるタスク結果で、違反が発生したことが示されるため、監査ポリシーのテスト時にこのオプションが役立ちます。
7. 監査ポリシーに割り当てられた是正ワークフローを実行する場合は、**「是正ワークフローを実行しますか ?」**を選択します。監査ポリシーに是正ワークフローが定義されていない場合は、是正ワークフローは実行されません。
8. **「違反数の最大値」**の値を編集して、スキャンが強制終了する前にスキャンが発行できるコンプライアンス違反の最大数を設定します。この値は、チェックが厳しすぎる可能性のある監査ポリシーを実行する場合に、リスクを制限するための安全措置です。空の値は制限を設定しないことを意味します。
9. レポートの受信者を指定する場合は、**「レポート結果を送信」**を選択します。また、Identity Manager が CSV (カンマ区切り値) 形式のレポートを格納したファイルを添付するように設定することもできます。
10. デフォルトの PDF オプションに優先して適用する場合は、**「デフォルトの PDF オプションを上書き」**オプションを有効にします。
11. **「起動」**をクリックしてスキャンを開始します。

    監査スキャンの結果のレポートを見るには、「監査レポート」を表示します。

監査レポートの操作

Identity Manager には、さまざまな監査レポートが用意されています。次の表で、それらのレポートについて説明します。

表 11-2 監査レポートの説明

監査レポートのタイプ	説明
アクセスレビュー範囲	選択したアクセスレビューによって示されたユーザーのオーバーラップと差異を表示します。ほとんどのアクセスレビューでは、ユーザークエリーまたは何らかのメンバーシップの操作によって、ユーザーの範囲が指定されるため、厳密なユーザーセットは時間の経過とともに変化すると予想されます。このレポートには、2 つの異なるアクセスレビューによって指定されたユーザー間 (操作でレビューが効率的に行われるかどうかを確認するため)、2 つの異なるアクセスレビューによって生成されたエンタイトルメント間 (時間の経過とともに範囲が変化するかどうかを確認できる)、またはユーザーとエンタイトルメント間 (レビューの対象とされているすべてのユーザーに対して、エンタイトルメントが生成されたかどうかを確認できる) のオーバーラップまたは差異、あるいはその両方を表示することができます。
アクセスレビュー詳細	すべてのユーザーエンタイトルメントレコードの現在のステータスが表示されます。このレポートは、ユーザーの組織、アクセスレビューとアクセスレビューインスタンス、エンタイトルメントレコードの状態、およびアテスターによってフィルタリングできます。
アクセスレビュー概要	すべてのアクセスレビューに関する概要情報が表示されます。一覧表示されたアクセスレビュースキャンごとに、スキャンしたユーザー、スキャンしたポリシー、およびアテステーションアクティビティーのステータスの概要が表示されます。
アクセススキャンユーザー範囲	選択されたスキャンを比較して、スキャン範囲に含まれるユーザーを判断します。オーバーラップ (すべてのスキャンに含まれるユーザー) または差異 (すべてのスキャンに含まれないが、複数のスキャンに含まれるユーザー) が表示されます。このレポートは、同一または異なるユーザーを範囲とする複数のアクセススキャンをスキャンのニーズに従って編成しようとする場合に便利です。
監査ポリシーの概要	各ポリシーの規則、是正者、ワークフローなど、すべての監査ポリシーの主要な要素の概要が表示されます。
監査属性	指定されたリソースアカウント属性の変更を示すすべての監査レコードが表示されます。 このレポートでは、格納されているすべての監査可能属性に関する監査データが調べられます。すべての拡張属性に基づいてデータが調べられます。拡張属性は、WorkflowServices または監査可能としてマークされたリソース属性から指定できます。

表 11-2　監査レポートの説明 (続き)

監査レポートのタイプ	説明
監査ポリシー別違反履歴	指定された期間中に作成されたすべてのコンプライアンス違反がポリシー別にグラフ形式で表示されます。このレポートは、ポリシーでフィルタリングしたり、日、週、月、または四半期ごとにグループ化したりできます。
ユーザーアクセス	指定されたユーザーの監査レコードとユーザー属性が表示されます。
組織別違反履歴	一定期間中に作成されたすべてのコンプライアンス違反が組織別にグラフ形式で表示されます。組織でフィルタリングしたり、日、週、月、または四半期ごとにグループ化したりできます。
リソース別違反履歴	指定された期間中に作成されたすべてのコンプライアンス違反がリソース別にグラフ形式で表示されます。
職務分掌	競合テーブルに配置された職務分掌違反が表示されます。Web ベースインタフェースでは、リンクをクリックすると追加情報にアクセスできます。 このレポートは、組織でフィルタリングしたり、日、週、月、または四半期ごとにグループ化したりできます。
違反の概要	現在のコンプライアンス違反がすべて表示されます。このレポートは、是正者、リソース、規則、ユーザー、またはポリシーによってフィルタリングできます。

これらのレポートは、Identity Manager インタフェースの「レポート」タブから利用できます。

監査レポートの作成

レポートを実行するには、まず、レポートテンプレートを作成する必要があります。レポートでは、レポート結果を受け取る電子メール受信者など、さまざまな条件を指定できます。レポートテンプレートを作成して保存すると、「レポートの実行」ページからそのレポートを使用できるようになります。

図 11-13 に、定義済み監査レポートのリストが表示された「レポートの実行」ページの例を示します。

図 11-13 「レポートの実行」ページの選択項目

監査レポートを作成するには、次の手順に従います。

1. メニューバーで**「レポート」**を選択します。
2. レポートタイプとして**「監査レポート」**を選択します。
3. レポートの**「新規」**リストからレポートを選択します。

「レポートの定義」ページが表示されます。レポートダイアログに表示されるフィールドやレイアウトは、レポートのタイプによって異なります。レポートの条件の指定については、Identity Manager ヘルプを参照してください。

レポートの条件を入力および選択したら、次を実行できます。

- 保存せずにレポートを実行する - **「実行」**をクリックしてレポートの実行を開始します。Identity Manager はレポート (新しいレポートを定義した場合) または変更したレポート条件 (既存のレポートを編集した場合) を保存しません。
- レポートを保存する ー **「保存」**をクリックしてレポートを保存します。保存後は、「レポートの実行」ページ (レポートのリスト) からそのレポートを実行できます。

「レポートの実行」ページからレポートを実行したあとは、「レポートの表示」タブで、ただちにまたはあとで出力を表示することができます。

- レポートのスケジュールについては、232 ページの「レポートのスケジュール」を参照してください。

コンプライアンス違反の是正と受け入れ

この節では、Identity Manager の是正機能を使用して重要な資産を保護する方法について説明します。以下のトピックで、Identity Manager 是正プロセスの要素について説明します。

- 是正について
- 是正電子メールテンプレート
- 「是正」ページの操作
- ポリシー違反の表示
- ポリシー違反の受け入れ
- ポリシー違反の是正
- 是正リクエストの転送

是正について

Identity Manager は、未解決の (受け入れられていない) 監査ポリシーコンプライアンス違反を検出すると、是正リクエストを作成します。このリクエストは「是正者」によって処理される必要があります。是正者とは、監査ポリシー違反の評価と応答を許可されている、指定されたユーザーです。

是正者のエスカレーション

Identity Manager では、3 レベルの是正者のエスカレーションを定義できます。是正リクエストは、まず、レベル 1 是正者に送信されます。タイムアウト時間が経過するまでにレベル 1 是正者が是正リクエストに応答しなかった場合、Identity Manager はその違反をレベル 2 是正者にエスカレーションし、新しいタイムアウト時間を開始します。タイムアウト時間が経過するまでにレベル 2 是正者が応答しなかった場合、そのリクエストはさらにレベル 3 是正者にエスカレーションされます。

是正を実行するには、そのシステムで少なくとも 1 人の是正者を指定する必要があります。任意設定ですが、各レベルに 2 人以上の是正者を指定することをお勧めします。複数の是正者を指定すると、ワークフローの遅延や停止を防ぐことができます。

是正セキュリティーアクセス

これらの権限付与オプションは、authType `RemediationWorkItem` の作業項目用のものです。

- 是正作業項目の所有者
- 是正作業項目の所有者の直属または直属以外のマネージャー

- 是正作業項目の所有者が所属する組織を管理する管理者

デフォルトでは、権限付与に関するチェックは次のようにして行い、いずれかの条件を満たす作業項目に対して、ユーザーに是正権限が付与されます。

- 作業項目は、アクションを実行しようとしているユーザー自身が所有者となっている
- 作業項目は、アクションを実行しようとしているユーザーが管理する組織に属すユーザーが所有している
- 作業項目は、アクションを実行しようとしているユーザーの部下が所有している

2 番目および 3 番目のチェックを別個に設定するには、次のオプションを変更します。

- controlOrg - 有効な値は true または false
- subordinate - 有効な値は true または false
- lastLevel - 結果に含める最後の従属レベル。-1 はすべてのレベルを意味する。lastLevel の整数値は、デフォルトでは -1 に設定され、これは直属の部下と直属ではない部下を含むことを意味します。

これらのオプションは、次のファイルで追加または変更できます。

```
UserForm: Remediation List
```

是正ワークフローのプロセス

Identity Manager では、監査ポリシースキャンの是正処理を行う標準是正ワークフローが提供されます。

標準是正ワークフローでは、コンプライアンス違反に関する情報を含む是正リクエスト (レビュータイプの作業項目) が生成され、監査ポリシーで指定された各レベル 1 是正者に電子メール通知が送信されます。是正者が違反を受け入れると、ワークフローによって既存のコンプライアンス違反オブジェクトの状態が変更され、有効期限が割り当てられます。

コンプライアンス違反は、ユーザー、ポリシー名、および規則名の組み合わせによって一意に識別されます。監査ポリシーで true と評価されたときに、このユーザー / ポリシー / 規則の組み合わせによる既存の違反が存在していなければ、その組み合わせによる新しいコンプライアンス違反が作成されます。その組み合わせでの違反が存在し、その違反が受け入れられた状態になっている場合は、ワークフロープロセスによる処理は行われません。既存の違反が受け入れられていない場合、その再発回数が加算されます。

是正ワークフローの詳細については、360 ページの「監査ポリシーについて」を参照してください。

是正応答

デフォルトでは、各是正者は次の 3 つの応答オプションから選択できます。

- **「是正」**- 是正者は、何らかの処理を行なってリソースの問題を修正したことを示します。

  コンプライアンス違反が修正されると、Identity Manager は監査イベントを作成して是正をログに記録します。さらに、Identity Manager は、是正者の名前および入力されたコメントを保存します。

注 是正後、違反は、次の監査スキャンまで削除されません。監査ポリシーが再スキャンを許可するように設定されている場合、違反が是正されるとただちにユーザーが再スキャンされます。

- **「受け入れる」**- 是正者は、ユーザーが一定期間その違反を免除されるように違反の内容を受け入れます。

  違反が意図的なものである場合 (たとえば、業務上 2 つのグループに所属する必要がある場合など) は、長期間にわたって違反を受け入れることができます。また、リソースのシステム管理者が休暇中で問題の修正方法がわからない場合などには、短期間だけ違反を受け入れることもできます。

  Identity Manager は、違反を受け入れた是正者の名前を、免除に割り当てた有効期限および入力したコメントとともに保存します。

注 Identity Manager は、期限切れになった免除を検出すると、違反を受け入れた状態から保留中の状態に戻します。

- **「転送」**- 是正者は、違反を解決する役割を別の人物に再割り当てします。

是正の例

ユーザーが買掛金と売掛金の両方を担当できないようにする規則を設定した企業で、あるユーザーがこの規則に違反しているという通知を受け取ったとします。

- 会社がその職位に別の従業員を雇用するまでの間、そのユーザーがスーパーバイザとして両方の役割を受け持つ場合は、その違反を受け入れ、最長で 6 か月間の免除を与えることができます。
- ユーザーが規則に違反している場合、競合を修正し、そのリソースで問題が解決されたときに違反を是正するように Oracle ERP 管理者に依頼することもできます。または、是正リクエストを Oracle ERP 管理者に転送することができます。

是正電子メールテンプレート

Identity Manager には、「ポリシー違反通知」電子メールテンプレートが用意されています。これを利用するには、**「設定」**タブを選択し、次に**「電子メールテンプレート」**サブタブを選択します。このテンプレートを、保留中の違反を是正者に通知するように設定できます。詳細については、143 ページの「電子メールテンプレートのカスタマイズ」を参照してください。

「是正」ページの操作

「是正」ページにアクセスするには、**「作業項目」**を選択し、**「是正」**タブを選択します。

このページでは、次の操作を行うことができます。

- 保留中の違反を表示する
- ポリシー違反の優先度を設定する
- 1 つ以上のポリシー違反を受け入れる
- 1 つ以上のポリシー違反を是正する
- 1 つ以上の違反を転送する
- 是正作業項目のユーザーを編集する

ポリシー違反の表示

「是正」ページでは、違反に対するアクションを実行する前に、違反に関する詳細を表示できます。

割り当てられている機能または Identity Manager 機能の階層の位置によっては、ほかの是正者の違反を表示してアクションを実行できる場合もあります。

以下のトピックは、違反の表示に関するものです。

- 386 ページの「保留中のリクエストの表示」
- 387 ページの「完了したリクエストの表示」
- 388 ページの「テーブルの更新」

保留中のリクエストの表示

デフォルトでは、割り当てられている保留中のリクエストは「是正」テーブルに表示されます。**「右の者に対する是正リクエスト一覧」**オプションを使用すると、別の是正者に対する保留中の是正リクエストを表示できます。

- 直接報告された組織内のユーザーの保留中のリクエストを表示するには、**「自分の直属の部下」**を選択します。
- 保留中のリクエストを表示したい 1 人以上のユーザーを入力するか、検索するには、**「ユーザーの検索」**を選択します。ユーザー ID を入力して、**「適用」**をクリックすると、そのユーザーの保留中のリクエストが表示されます。または、**「...」**ボタンをクリックして、ユーザーを検索します。ユーザーを見つけて選択したら、**「閉じる」**をクリックして、「検索」エリアを閉じます。

結果のテーブルには、リクエストごとに次の情報が表示されます。

- **「是正者」**- 割り当てられた是正者の名前。この列は、ほかの是正者の是正リクエストを表示する場合にのみ表示されます。
- **「ユーザー」**― リクエストが作成されたユーザー。
- **「監査ポリシー / リクエスト」**― 是正者にリクエストされるアクション。
- **「監査ポリシー / 説明」**― リクエストの是正コメント。
- **「違反の状態」**― 違反の現在の状態。
- **「重要度」**― リクエストに割り当てられた重要度 (なし、低、中、高、クリティカル)。
- **「優先度」**― リクエストに割り当てられた優先度 (なし、低、中、高、緊急)。
- **「リクエスト日」**― 是正リクエストが発行された日時。

注 各ユーザーは、その特定の是正者に関連する是正データを表示するカスタムフォームを選択できます。カスタムフォームを割り当てるには、ユーザーフォームの**「コンプライアンス」**タブを選択します。

完了したリクエストの表示

完了した是正リクエストを表示するには、**「自分の作業項目」**タブをクリックし、次に**「履歴」**タブをクリックします。以前に是正した作業項目のリストが表示されます。

結果のテーブル (`AuditLog` レポートで生成される) には、是正リクエストごとに次の情報が表示されます。

- **「タイムスタンプ」**― リクエストが是正された日時
- **「主体」**― リクエストを処理した是正者の名前
- **「アクション」**― 是正者がリクエストを受け入れたのか是正したのかを示す
- **「タイプ」**― `ComplianceViolation` やユーザーエンタイトルメントなど
- **「オブジェクト名」**― 違反した監査ポリシーの名前
- **「リソース」**― 是正者のアカウント ID (「なし」と表示されることもある)

- 「ID」 – 作業項目に関連するアカウント ID (たとえばポリシー違反の場合は、違反したアカウントの ID) が表示されます。
- **「結果」** – 常に「成功」と表示される

テーブルのタイムスタンプをクリックすると、「監査イベントの詳細」ページが開きます。

「監査イベントの詳細」ページには、完了したリクエストに関する情報が表示されます。この情報には、是正または受け入れに関する情報、イベントパラメータ (該当する場合)、監査可能属性などが含まれます。

テーブルの更新

「是正」テーブルに表示された情報を更新するには、**「更新」**をクリックします。新しい是正リクエストがあれば、「是正」ページのテーブルが更新されます。

ポリシー違反の優先度の設定

ポリシー違反に優先度、重要度、またはその両方を割り当てて、ポリシー違反の優先度を設定することができます。「是正」ページから違反の優先度を設定します。

違反の優先度または重要度を編集するには、次の手順に従います。

1. リストの違反を 1 つまたは複数選択します。
2. **「優先度の設定」**をクリックします。

   「ポリシー違反の優先度設定」ページが表示されます。
3. オプションの作業として違反の重要度を設定します。選択項目は、「なし」、「低」、「中」、「高」、「クリティカル」です。
4. オプションの作業として違反の優先度を設定します。選択項目は、「なし」、「低」、「中」、「高」、「緊急」です。
5. 選択が完了したら、「OK」をクリックします。Identity Manager は是正者のリストに戻ります。

注	重要度と優先度の値は、タイプ CV (コンプライアンス違反) の是正項目にのみ設定できます。

ポリシー違反の受け入れ

「是正」ページまたは「ポリシー違反のレビュー」ページで、ポリシー違反を受け入れることができます。

「是正」ページでの操作

「是正」ページで保留中のポリシー違反を受け入れるには、次の手順に従います。

1. テーブルの行を選択して、受け入れるリクエストを指定します。
   - 1 つまたは複数のリクエストを受け入れ対象に指定するには、それぞれのオプションを有効にします。
   - テーブルに一覧表示されたすべてのリクエストを受け入れるには、テーブルヘッダーのオプションを有効にします。

注

Identity Manager では、受け入れアクションを説明するコメントは 1 セットしか入力できません。関連する違反であるためコメントが 1 つで十分な場合を除いては、一括受け入れを実行しないでください。

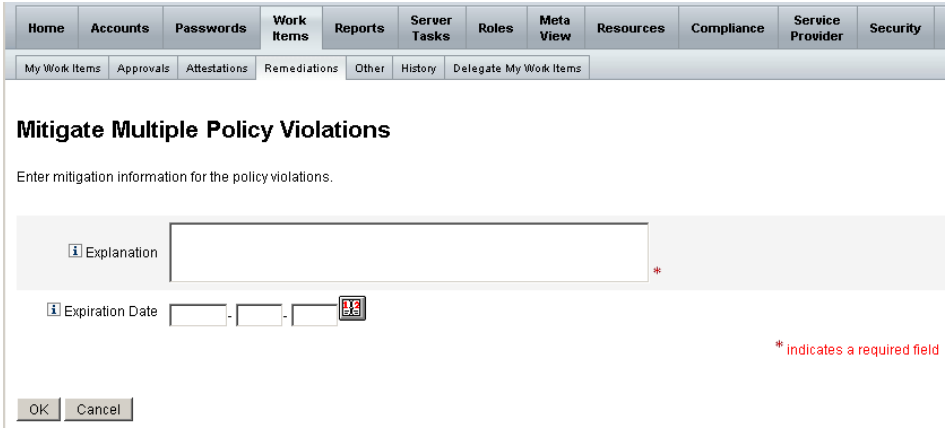
受け入れ可能なリクエストは、コンプライアンス違反を含むリクエストのみです。ほかの是正リクエストは受け入れることができません。

---

2. **「受け入れる」**をクリックします。

   次のような「ポリシー違反を受け入れる」ページ (または「複数のポリシー違反を受け入れる」ページ) が表示されます。

図 11-14　「ポリシー違反を受け入れる」ページ



3. 「説明」フィールドに、受け入れに関するコメントを入力します。このフィールドは必須です。

   コメントは、このアクションの監査証跡として利用されるので、ひととおりの有用な情報を入力する必要があります。たとえば、ポリシー違反を受け入れる理由、日付、免除期間の選択理由などを説明します。

4. 免除の有効期限を指定します。「有効期限」フィールドに日付 (**YYYY-MM-DD** 形式) を直接入力するか、または  ボタンをクリックしてカレンダから日付を選択します。

注 日付を入力しない場合、免除期間は無期限となります。

5. **「OK」**をクリックして変更を保存し、「是正」ページに戻ります。

ポリシー違反の是正

1 つ以上のポリシー違反を是正するには、次の手順に従います。

1. テーブル内のチェックボックスを使用して、是正するリクエストを指定します。
   - 1 つまたは複数のリクエストを是正対象に指定するには、それぞれのチェックボックスを有効にします。
   - テーブルに一覧表示されたすべてのリクエストを是正するには、テーブルヘッダーのチェックボックスを有効にします。

     複数のリクエストを選択した場合、Identity Manager では、是正アクションを説明するコメントは 1 セットしか入力できません。関連する違反であるためコメントが 1 つで十分な場合を除いては、一括是正を実行しないでください。
2. **「是正」**をクリックします。
3. 「ポリシー違反の是正」ページ (または「複数のポリシー違反の是正」ページ) が表示されます。
4. 「コメント」フィールドに、是正に関するコメントを入力します。
5. **「OK」**をクリックして変更を保存し、「是正」ページに戻ります。

注 ユーザーに直接割り当てられている (ユーザーアカウントや組織の割り当てによって割り当てられている) 監査ポリシーは、そのユーザーの違反の是正時に常に再評価されます。

是正リクエストの転送

1 つ以上の是正リクエストをほかの是正者に転送できます。その場合は次の手順に従います。

1. テーブル内のチェックボックスを使用して、転送するリクエストを指定します。
   - テーブルに一覧表示されたすべてのリクエストを転送するには、テーブルヘッダーのチェックボックスを有効にします。
   - 1 つまたは複数のリクエストを転送するには、それぞれのチェックボックスを有効にします。
2. **「転送」**をクリックします。

   「転送先の選択と確認」ページが表示されます。

   図 11-15　「転送先の選択と確認」ページ

3. 「転送先」フィールドに是正者の名前を入力して、**「OK」**をクリックします。または、**「...」**ボタンをクリックして、是正者の名前を検索します。検索リストから名前を選択して、**「設定」**をクリックして、「転送先」フィールドにその名前を入力します。**「閉じる」**をクリックして、検索エリアを閉じます。

「是正」ページが再表示され、テーブルの「是正者」列に新しい是正者の名前が表示されます。

是正作業項目のユーザーの編集

適切なユーザー編集機能を持つ場合、関連付けられたエンタイトルメント履歴に説明されているとおり、是正作業項目から、ユーザーを編集して問題を是正できます。

ユーザーを編集するには、「是正リクエストのレビュー」ページから、**「ユーザーの編集」**をクリックします。表示される「ユーザーの編集」ページには、次の項目が表示されます。

- この作業項目について、ユーザーに関連付けられているエンタイトルメント履歴
- ユーザーの属性。ここに表示されるオプションは、「アカウント」エリアから使用できる「ユーザーの編集」フォームのオプションと同じです。

ユーザーを変更したら、「**保存**」をクリックします。

注	ユーザーを編集し、保存すると、ユーザーの更新ワークフローが実行されます。このワークフローに承認プロセスが含まれている場合があるため、ユーザーアカウントを変更し、保存してもしばらくの間、有効にならない可能性があります。監査ポリシーで再スキャンが許可されており、ユーザーの更新ワークフローが完了していない場合、後続のポリシースキャンで同じ違反が検出されることがあります。

定期的アクセスレビューとアテステーション

Identity Manager では、アクセスレビューを実行するプロセスによって、マネージャーなどの責任者がユーザーアクセス特権のレビューと検証を行うことができます。このプロセスは、時間の経過とともに蓄積されたユーザー特権を識別および管理し、米国企業改革 (SOX) 法、GLBA、および米国で義務付けられているその他の規制に対するコンプライアンスを維持するのに役立ちます。

アクセスレビューは、必要に応じて実行できます。また、四半期ごとなど、定期的に実行されるようにスケジュールすることもできます。定期的アクセスレビューを実行することで、正しいレベルのユーザー特権を維持できます。アクセスレビューにオプションの作業として監査ポリシースキャンを含めることもできます。

定期的アクセスレビューについて

定期的アクセスレビューは、従業員セットが特定の時点で適切なリソースに対する適切な特権を持っていることをアテストする定期的プロセスです。

定期的アクセスレビューでは次のアクティビティーを行います。

- アクセスレビュースキャン - 自分が定義して実行または実行をスケジュールしたスキャンです。このスキャンでは、指定したユーザーセットの「ユーザーエンタイトルメント」を評価し、規則ベースの評価を実行してアテステーションが必要かどうかを決定します。
- アテステーション - ユーザーエンタイトルメントを承認または却下することによってアテステーションリクエストに応答するプロセスです。

「ユーザーエンタイトルメント」は、特定のリソースセットについてのユーザーのアカウントの詳細のレコードです。

アクセスレビュースキャン

定期的アクセスレビューを開始するには、まず、1 つ以上のアクセススキャンを定義する必要があります。

アクセススキャンには、スキャン対象のユーザー、スキャンに含めるリソース、スキャンで評価するオプションの監査ポリシー、および手動でアテストするエンタイトルメントレコードを決定する規則とその実行者を定義します。

アクセスレビューのワークフロープロセス

一般に、Identity Manager のアクセスレビューワークフローは次のようになります。

- ユーザーのリストを作成し、各ユーザーのアカウント情報を取得し、オプションの監査ポリシーを評価する
- ユーザーエンタイトルメントレコードを作成する
- 各ユーザーエンタイトルメントレコードについて、アテステーションが必要かどうかを判断する
- 作業項目を各アテスターに割り当てる
- すべてのアテスターによる承認または最初の却下を待つ
- 指定された時間内にリクエストへの応答を受け取らなかった場合は、次のアテスターにエスカレーションする
- 解決したユーザーエンタイトルメントレコードを更新する

是正機能については、412 ページの「アクセスレビュー是正」を参照してください。

必要な管理者機能

定期的アクセスレビューを実行してレビュープロセスを管理するユーザーは、「Auditor Periodic Access Review Administrator」機能を持っている必要があります。「アクセススキャン監査管理者」機能を持つユーザーは、アクセススキャンの作成と管理を行うことができます。

これらの機能を割り当てるには、ユーザーアカウントを編集してセキュリティー属性を変更します。これらの機能およびその他の機能の詳細については、166 ページの「機能とその管理について」を参照してください。

アテステーション

アテステーションは、特定の日付に存在しているユーザーエンタイトルメントを確認するために、1 人以上の指定されたアテスターが実行するアテステーションプロセスです。アクセスレビュー中に、アテスターは電子メール通知によってアクセスレビューアテステーションリクエストの通知を受け取ります。アテスターは、Identity Manager ユーザーである必要がありますが、Identity Manager 管理者である必要はありません。

アテステーションワークフロー

Identity Manager は、レビューを必要とするエンタイトルメントレコードがアクセススキャンで検出されたときに起動されるアテステーションワークフローを使用します。アクセススキャンは、アクセススキャンで定義された規則に基づいてこの判断を行います。

アクセススキャンで評価される規則によって、ユーザーエンタイトルメントレコードを手動でアテストする必要があるか、あるいは自動的に承認または却下できるか決まります。ユーザーエンタイトルメントレコードを手動でアテストする必要がある場合は、2 番目の規則を使用して適切なアテスターが決定されます。

手動でアテストする各ユーザーエンタイトルメントレコードは、1 人のアテスターにつき 1 つの作業項目でワークフローに割り当てられます。これらの作業項目のアテスターへの通知を、アテスターごと、スキャンごとに項目を 1 つの通知にまとめる ScanNotification ワークフローを使用して送信できます。ScanNotification ワークフローが選択されていない場合は、ユーザーエンタイトルメントごとの通知になります。この場合、1 人のアテスターが同じスキャンで複数の通知を受け取ることになり、スキャンするユーザー数によっては多数の通知になる可能性があります。

アテステーションセキュリティーアクセス

これらの権限付与オプションは、authType `AttestationWorkItem` の作業項目用のものです。

- 作業項目の所有者
- 作業項目の所有者の直属または直属以外のマネージャー
- 作業項目の所有者が所属する組織を管理する管理者
- 認証チェックで検証済みのユーザー

デフォルトでは、権限付与に関するチェックは次のようにして行い、いずれかの条件を満たす作業項目に対して、ユーザーにアテステーション権限が付与されます。

- 作業項目は、アクションを実行しようとしているユーザー自身が所有者となっている
- 作業項目は、アクションを実行しようとしているユーザーが管理する組織に属すユーザーが所有している
- 作業項目は、アクションを実行しようとしているユーザーの部下が所有している

2 番目および 3 番目のチェックを別個に設定するには、次のフォームプロパティーを変更します。

- `controlOrg` - 有効な値は「true」または「false」
- `subordinate` - 有効な値は「true」または「false」
- `lastLevel` - 結果に含める最後の従属レベル。-1 はすべてのレベルを意味する

lastLevel の整数値は、デフォルトでは -1 に設定され、これは直属の部下と直属ではない部下を含むことを意味します。

これらのオプションは、次のファイルで追加または変更できます。

```
UserForm: AccessApprovalList
```

注	アテステーションのセキュリティーが組織管理に設定されている場合 (controlOrg が true)、ほかのユーザーが所有しているアテステーションを変更するには Auditor Attestor 機能も必要です。

委任されたアテステーション

デフォルトの動作として、アクセススキャンワークフローは、アクセスレビューアテステーション作業項目およびアクセスレビュー是正作業項目に対して、アテステーション作業項目およびその通知用にユーザーが作成した委任設定に従います。しかし、アクセススキャンの管理者が、「委任に従う」オプションを選択解除して委任設定を無視する場合があります。アテスターがすべての作業項目を別のユーザーに委任している場合でも、アクセスレビュースキャンで「委任に従う」オプションが設定されていなければ、委任を割り当てたユーザーではなく、そのアテスターがアテステーションリクエスト通知と作業項目を受け取ることになります。

定期的アクセスレビューの計画

アクセスレビューは、どの企業でも多くの労働力と時間を要するプロセスです。Identity Manager 定期的アクセスレビュープロセスを使用すると、プロセスの多くの部分が自動化されるため、必要なコストと時間を最小限にできます。ただし、それでも時間のかかるプロセスがいくつかあります。たとえば、いくつもの場所から多数のユーザーのユーザーアカウントデータを取得するプロセスには、かなりの時間を要する場合があります。レコードを手動でアテストする作業も、時間がかかる場合があります。適切な計画を行えば、プロセスの効率を高め、必要な手間を大幅に減らすことができます。

定期的アクセスレビューの計画では、次のことを考慮する必要があります。

- スキャン時間は、ユーザー数および関連するリソースの数によって大きく異なる場合があります。

  大規模な組織で 1 回の定期的アクセスレビューを行う場合、スキャンに 1 日以上かかることがあり、手動アテステーションを完了するのに 1 週間以上かかることもあります。

  たとえば、50,000 人のユーザーと 10 のリソースを持つ組織では、次の計算によると、アクセススキャンの完了にほぼ 1 日かかる可能性があります。

  1 秒 / リソース * 50000 ユーザー * 10 リソース / 5 同時スレッド = 28 時間

リソースが各地域に散在している場合は、ネットワークの待ち時間が処理時間に加わることがあります。

- 複数の Identity Manager サーバーを使用して並行処理を行うと、アクセスレビュープロセスをスピードアップできます。

  各スキャンでリソースが共通していない場合は、並列スキャンの実行がもっとも効果的です。アクセスレビューを定義するときに、複数のスキャンを作成し、リソースを特定のリソースセットに制限して、スキャンごとに異なるリソースを使用するようにします。そして、タスクの起動時に、複数のスキャンを選択し、ただちに実行するようにスケジュールします。

- アテステーションワークフローおよび規則をカスタマイズすることにより、管理を強化して効率を高めることができます。

  たとえば、アテスター規則を、複数のアテスターにアテステーション作業を分散させるようにカスタマイズします。そうすれば、アテステーションプロセスで、その規則に従って作業項目が割り当てられ通知が送信されます。

- アテスターエスカレーション規則を使用すると、アテステーションリクエストに対する応答時間を短くできます。

  デフォルトのエスカレーションアテスター規則を設定するか、またはカスタマイズした規則を使用して、アテスターのエスカレーションチェーンを設定します。エスカレーションタイムアウト値も指定します。

- レビュー決定規則の使用方法を理解し、手動レビューが必要なエンタイトルメントレコードの判別を自動化することで時間を節約します。

- スキャンレベルの通知ワークフローを指定して、スキャンごとにアテステーションリクエストの通知をまとめます。

スキャンタスクのチューニング

スキャンプロセス時に、複数のスレッドがユーザーのビューにアクセスし、ユーザーがアカウントを持つリソースにアクセスする可能性があります。ビューへのアクセス後、複数の監査ポリシーと規則が評価され、コンプライアンス違反が生成されることがあります。

2 つのスレッドが同じユーザービューを同時に更新することを避けるため、プロセスはユーザー名にメモリー内ロックを設定します。このロックがデフォルトで 5 秒以内に設定できない場合、スキャンタスクにエラーが書き込まれ、ユーザーはスキップされるため、同じユーザーセットを処理する同時スキャンが防止されます。

スキャンタスクへのタスク引数として提供されるいくつかの「チューニング可能パラメータ」の値を編集できます。

- `clearUserLocks` (ブール型) - true の場合、スキャンの開始前に、現在のすべてのユーザーロックが解除されます。

- `userLock` (整数) - ユーザーをロックしようとして待つ時間 (ミリ秒)。デフォルト値は 5 秒です。負の値を設定すると、スキャン中にユーザーのロックは行いません。
- `scanDelay` (整数) - スキャンスレッドのディスパッチ間でスリープする時間 (ミリ秒)。デフォルト値は 0 (遅延なし) です。この引数の値を指定すると、スキャンは遅くなりますが、システムのほかの操作の応答が速くなります。
- `maxThreads` (整数) - スキャンの処理に使用する同時スレッド数。デフォルト値は 5 です。リソースの応答が極めて遅い場合は、この数値を大きくすると、スキャンのスループットが向上する可能性があります。

これらのパラメータの値を変更するには、対応する「タスク定義」フォームを編集します。このタスクの詳細については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

アクセススキャンの作成

アクセスレビュースキャンを定義するには、次の手順に従います。

1. **「コンプライアンス」**を選択し、**「アクセススキャンの管理」**を選択します。
2. **「新規」**をクリックして、「新規アクセススキャンの作成」ページを表示します。
3. アクセススキャンに名前を割り当てます。

注	アクセススキャン名には、次の文字を含めることはできません。' (アポストロフィー)、. (ピリオド)、| (パイプ)、[(左角括弧)、] (右角括弧)、, (カンマ)、: (コロン)、$ (ドル記号)、" (二重引用符)、= (等号)。

4. 必要に応じて、そのスキャンを特定する説明を追加します。
5. オプションの作業として**「動的エンタイトルメント」**オプションを有効にします。有効にした場合、アテスターは、次の追加オプションから選択できます。
   - 保留中のアテステーションをすぐに再スキャンして、エンタイトルメントデータを更新し、アテステーションの必要性を再評価できます。
   - 保留中のアテステーションを別のユーザーに配信して是正を求めることができます。是正後、エンタイトルメントデータは更新および再評価され、アテステーションの必要性が判断されます。
6. **「ユーザー範囲タイプ」**で、次のいずれかのオプションを選択します。このフィールドは必須です。
   - **「属性条件規則に従う」** - 選択したユーザー範囲規則に従って、ユーザーをスキャンする場合は、このオプションを選択します。Identity Manager では次の規則を使用できます。

- 「All Administrators」
- 「All Non-Administrators」
- 「Users without a Manager」

注	ユーザーの範囲を指定する規則を追加するには、Identity Manager Integrated Development Environment (IDE) を使用します。詳細については、『Identity Manager 配備ツール』を参照してください。

- **「リソースに割り当て」** ー 選択した 1 つ以上のリソースにアカウントを持つすべてのユーザーをスキャンする場合は、このオプションを選択します。このオプションを選択した場合、ページにユーザー範囲リソースが表示され、リソースを指定できます。
- **「組織のメンバー」**- 選択した 1 つ以上の組織のすべてのメンバーをスキャンする場合は、このオプションを選択します。
- **「特定のマネージャーの部下」** ー 選択したマネージャーに直属するすべてのユーザーをスキャンする場合は、このオプションを選択します。マネージャーの階層は、ユーザーの Lighthouse アカウントの Identity Manager 属性によって決まります。

ユーザー範囲タイプが「組織のメンバー」または「特定のマネージャーの部下」の場合は、「範囲を再帰的に計算 ?」オプションを使用できます。このオプションを使用すると、管理する一連のメンバーを通して再帰的にユーザー選択が行われるようにできます。

7. アクセスレビュースキャンで監査ポリシーもスキャンして違反を検出する場合は、このスキャンに適用する監査ポリシーを「利用可能な監査ポリシー」リストから選択し、「現在の監査ポリシー」リストに移動させます。

   アクセススキャンに監査ポリシーを追加した場合の動作は、同じユーザーセットに対して監査スキャンを実行するのと同じ結果になります。ただし、それに加えて、監査ポリシーによって検出された違反がユーザーエンタイトルメントレコードに格納されます。この情報により、ユーザーエンタイトルメントレコード内に違反が存在するかどうかを規則のロジックの一部として使用できるので、自動承認または自動却下が容易になります。

8. 前の手順でスキャンする監査ポリシーを選択した場合は、**「ポリシーモード」**オプションを使用して、アクセススキャンされる各ユーザーに対してどの監査ポリシーを実行するかを指定することができます。ユーザーレベルまたは組織レベル、あるいはその両方でユーザーにポリシーを割り当てることができます。デフォルトのアクセススキャンでは、ユーザーにまだポリシーが割り当てられていない場合にのみ、アクセススキャンで指定されたポリシーが適用されます。

   a. 選択されたポリシーを適用し、それ以外の割り当ては無視する

b. ユーザーにまだ割り当てられていない場合にのみ、選択されたポリシーを適用する

c. ユーザーの割り当てに加えて、選択されたポリシーを適用する

9. (省略可能)**「レビュープロセスの所有者」**を指定します。定義しているアクセスレビュータスクの所有者を指定する場合は、このオプションを使用します。レビュープロセスの所有者を指定すると、アテステーションリクエストへの応答で競合が起こる可能性があるアテスターは、ユーザーエンタイトルメントを承認または却下する代わりに「拒否」できます。その場合、アテステーションリクエストはレビュープロセスの所有者に転送されます。選択 (省略記号) ボックスをクリックして、ユーザーアカウントを検索し、選択を行います。

10. **「委任に従う」**- アクセススキャンの委任を有効にする場合は、このオプションを選択します。このオプションを選択した場合、アクセススキャンでは委任設定のみが遵守されます。「委任に従う」は、デフォルトで有効になっています。

11. **「ターゲットリソースを制限」**- ターゲットのリソースのみにスキャンを制限する場合は、このオプションを選択します。

    この設定は、アクセススキャンの効率に直接関係します。ターゲットリソースを制限しない場合、各ユーザーエンタイトルメントレコードには、そのユーザーが関連付けられているすべてのリソースのアカウント情報が含まれます。つまり、そのスキャンでは、各ユーザーに割り当てられたすべてのリソースが問い合わせを受けます。このオプションを使用してリソースのサブセットを指定すると、Identity Manager がユーザーエンタイトルメントレコードを作成するために必要な処理時間を大幅に減らすことができます。

12. **「違反の是正を実行する」**- 違反が検出された場合に監査ポリシーの是正ワークフローを有効にする場合は、このオプションを選択します。

    このオプションを選択すると、割り当てられた監査ポリシーのいずれかに対する違反が検出されると、その監査ポリシーの是正ワークフローが実行されます。

    特別に必要な場合を除いて、このオプションは選択しないようにしてください。

13. **「アクセス承認ワークフロー」**- デフォルトの Standard Attestation ワークフローを選択するか、またはカスタマイズしたワークフロー (使用可能な場合) を選択します。

    このワークフローは、レビュー用のユーザーエンタイトルメントレコードを適切なアテスター (アテスター規則によって決まる) に提示するために使用されます。デフォルトの Standard Attestation ワークフローでは、1 人のアテスターに対して 1 つの作業項目が作成されます。アクセススキャンにエスカレーションが指定されている場合、このワークフローでは、保留状態の時間が長すぎる作業項目のエスカレーションが行われます。ワークフローが指定されていない場合、ユーザーアテステーションは無期限に保留状態のままになります。

14. **「アテスター規則」**- 「Default Attestor」規則を選択するか、またはカスタマイズしたアテスター規則 (使用可能な場合) を選択します。

アテスター規則は、ユーザーエンタイトルメントレコードを入力として受け取り、アテスター名のリストを返します。「委任に従う」が選択されている場合、アクセススキャンでは、元の名前リストにある各ユーザーが設定した委任情報に従って、名前リストが適切なユーザー名のリストに変換されます。Identity Manager ユーザーの委任がルーティングサイクルになった場合、その委任情報は破棄され、作業項目は最初のアテスターに配信されます。「Default Attestor」規則では、エンタイトルメントレコードに示されたユーザーのマネージャー (idmManager) がアテスターとなり、そのユーザーの idmManager が null の場合は Configurator アカウントがアテスターとなります。マネージャーだけでなくリソースの所有者もアテステーションに携わる必要がある場合は、カスタム規則を使用する必要があります。規則のカスタマイズについては、『Identity Manager 配備ツール』を参照してください。

15. **「アテスターエスカレーション規則」** - 「Default Escalation Attestor」規則を指定する場合、またはカスタマイズした規則 (使用可能な場合) を選択する場合は、このオプションを使用します。また、規則のエスカレーションタイムアウト値を指定することもできます。デフォルトのエスカレーションタイムアウト値は 0 日です。

    この規則は、エスカレーションタイムアウト時間が経過した作業項目のエスカレーションチェーンを指定します。「Default Escalation Attestor」規則では、割り当てられたアテスターのマネージャー (idmManager) にエスカレーションされるか、または、アテスターの idmManager の値が null の場合は Configurator にエスカレーションされます。

    エスカレーションタイムアウト値は、分単位、時間単位、または日単位で指定できます。

16. **「レビュー決定規則」** - スキャンプロセスがエンタイトルメントレコードの処置を決定する方法を指定する場合は、次のいずれかの規則を選択します。このフィールドは必須です。

    - 「Reject Changed Users」 - 同じアクセススキャン定義による最後のユーザーエンタイトルメントと異なっていて、最後のユーザーエンタイトルメントが承認されているユーザーエンタイトルメントレコードを自動的に却下します。これを選択しない場合は、以前に承認されたユーザーエンタイトルメントから変更されたすべてのユーザーエンタイトルメントを手動でアテステーションおよび承認する必要があります。デフォルトでは、この規則に対して、ユーザービューの「アカウント」部分のみが比較されます。
    - 「Review Changed Users」 - 同じアクセススキャン定義による最後のユーザーエンタイトルメントと異なっていて、最後のユーザーエンタイトルメントが承認されているすべてのユーザーエンタイトルメントレコードの手動アテステーションを強制します。以前に承認されたユーザーエンタイトルメントから変更されていないユーザーエンタイトルメントはすべて承認します。デフォルトでは、この規則に対して、ユーザービューの「アカウント」部分のみが比較されます。
    - 「Review Everyone」 - すべてのユーザーエンタイトルメントレコードの手動アテステーションを強制します。

注 「Reject Changed Users」規則と「Review Changed Users」規則では、ユーザーエンタイトルメントを、そのエンタイトルメントレコードが承認されたアクセススキャンの最後のインスタンスと比較します。

この動作を変更するには、規則をコピーし、ユーザーデータの特定の部分のみを比較するように修正します。規則のカスタマイズについては、『Identity Manager 配備ツール』を参照してください。

この規則は次の値を返します。

- -1 ー アテステーションを必要としない
- 0 ー アテステーションを自動的に却下する
- 1 ー 手動のアテステーションが必要
- 2 ー アテステーションを自動的に承認する
- 3 ー アテステーションを自動的に是正する (自動是正)

17. **「是正者規則」ー** 自動是正の場合に、特定のユーザーエンタイトルメントを是正するユーザーを特定するときに使用する規則を選択します。この規則により、ユーザーの現在のユーザーエンタイトルメントと違反を調査できます。規則は是正すべきユーザーのリストを返す必要があります。規則を指定しない場合、是正は行われません。この規則は一般的に、エンタイトルメントにコンプライアンス違反がある場合に使用します。

18. **「是正ユーザーフォーム規則」ー** ユーザーの編集時に、アテステーション是正者に適切なフォームを選択する場合に使用する規則を選択します。是正者は独自のフォームを設定でき、このフォームより優先されます。このフォーム規則は、スキャンでカスタムフォームに一致する厳密に限定されたデータを収集する場合に設定します。

19. **「通知ワークフロー」**- 作業項目ごとに通知動作を指定する場合は、次のオプションのいずれかを選択します。

    - **「なし」**- これがデフォルトの選択です。これを選択すると、アテスターは、アテステーションの必要があるユーザーエンタイトルメントごとに電子メール通知を受け取ります。
    - 「ScanNotification」- これを選択すると、アテステーションリクエストが 1 つの通知にまとめられます。通知には、その受信者に何件のアテステーションリクエストが割り当てられたかが示されます。

      アクセススキャンで「レビュープロセスの所有者」が指定されている場合、ScanNotification ワークフローでは、スキャンの開始時と終了時に、レビュープロセスの所有者にも通知が送信されます。手順 9 を参照してください。

      ScanNotification ワークフローでは、次の電子メールテンプレートを使用します。

- Access Scan Begin Notice
- Access Scan End Notice
- Bulk Attestation Notice

ScanNotification ワークフローはカスタマイズできます。

20. **「違反の最大値」**- このオプションを使用すると、コンプライアンス違反の数がここで設定した数値に達した時点で、スキャンを強制終了します。デフォルトの制限は 1000 です。フィールドの値を空にした場合は、制限なしと同じです。

    通常、監査スキャンまたはアクセススキャンでは、ポリシー違反の数はユーザー数に比べると少ないですが、この値を設定すると、欠陥のあるポリシーによって違反数が大幅に増えた場合の保護対策になります。たとえば、次のようなシナリオを考えてみます。

    50,000 ユーザーのアクセススキャンで、ユーザーあたり 2 ～ 3 個の違反が発生すると、各コンプライアンス違反の是正にかかるコストは Identity Manager システムに有害な影響を及ぼす可能性があります。

21. **「組織」**- このアクセススキャンオブジェクトで使用可能な組織を選択します。これは必須フィールドです。

「保存」をクリックしてスキャン定義を保存します。

アクセススキャンの削除

1 つ以上のアクセススキャンを削除できます。アクセススキャンを削除するには、**「コンプライアンス」**タブで**「アクセススキャンの管理」**を選択し、スキャンの名前を選択して**「削除」**をクリックします。

アクセスレビューの管理

アクセススキャンを定義したあと、そのスキャンをアクセスレビューの一部として使用またはスケジュールすることができます。アクセスレビューの開始後、いくつかのオプションを使用してレビュープロセスを管理できます。詳細については、次のセクションを参照してください。

- アクセスレビューの起動
- アクセスレビュータスクのスケジュール
- アクセスレビューの進行状況の管理
- スキャン属性の変更
- アクセスレビューのキャンセル

アクセスレビューの起動

管理者インタフェースからアクセスレビューを起動するには、次のいずれかの方法を使用します。

- **「コンプライアンス」>「アクセスレビュー」**ページから、**「レビューの起動」**をクリックします。
- **「サーバータスク」>「タスクの実行」**ページでアクセスレビュータスクを選択します。

表示された「タスクの起動」ページで、アクセスレビューの名前を指定します。「利用可能なアクセススキャン」リストでスキャンを選択し、「選択されたアクセススキャン」リストに移動させます。複数のスキャンを選択した場合は、次のいずれかの起動オプションを選択できます。

- **「すぐに起動」-**「起動」ボタンをクリックすると、ただちにスキャンの実行が開始されます。起動タスクで複数のスキャンに対してこのオプションを選択した場合は、各スキャンが並行して実行されます。
- **「起動までの (待機時間)」-** アクセスレビュータスクを起動した時間を基準として、スキャンを起動するまでの待機時間を指定することができます。

注 1 つのアクセスレビューセッションで複数のスキャンを開始できます。ただし、各スキャンのユーザー数が多いと、スキャンプロセスの完了に長時間かかる可能性があることを考慮してください。それぞれの状況に応じた方法でスキャンを管理することをお勧めします。たとえば、1 つのスキャンをただちに実行し、その他のスキャンは時間をずらしてスケジュールすることもできます。

アクセスレビュープロセスを開始するには、**「起動」**をクリックします。

注 アクセスレビューに割り当てる名前は重要です。同じ名前で定期的に実行されたアクセスレビューを、いくつかのレポートで比較できます。

アクセスレビューを起動すると、プロセスの手順を示すワークフロープロセス図が表示されます。

アクセスレビュータスクのスケジュール

アクセスレビュータスクは、「サーバータスク」エリアでスケジュールできます。たとえば、定期的にアクセスレビューを行う場合は、**「スケジュールの管理」**を選択し、スケジュールを定義します。毎月、または四半期ごとにタスクを実行するようにスケジュールできます。

スケジュールを定義するには、「タスクのスケジュール」ページでアクセスレビュータスクを選択し、タスクスケジュールの作成ページに情報を入力します。

「保存」をクリックして、スケジュールしたタスクを保存します。

注	Identity Manager では、アクセスレビュータスクの結果は、デフォルトで 1 週間維持されます。1 週間に 1 回よりも短い間隔でレビューをスケジュールする場合は、「結果オプション」を「削除」に設定します。「結果オプション」が「削除」に設定されていない場合は、前のタスク結果がまだ存在しているため新しいレビューは実行されません。

アクセスレビューの進行状況の管理

アクセスレビューの進行状況を監視するには、**「アクセスレビュー」**タブを使用します。この機能には**「コンプライアンス」**タブからアクセスします。

「アクセスレビュー」タブから、すべてのアクティブなアクセスレビューおよび以前に処理されたアクセスレビューの概要をレビューできます。一覧表示されるアクセスレビューごとに、次の情報が表示されます。

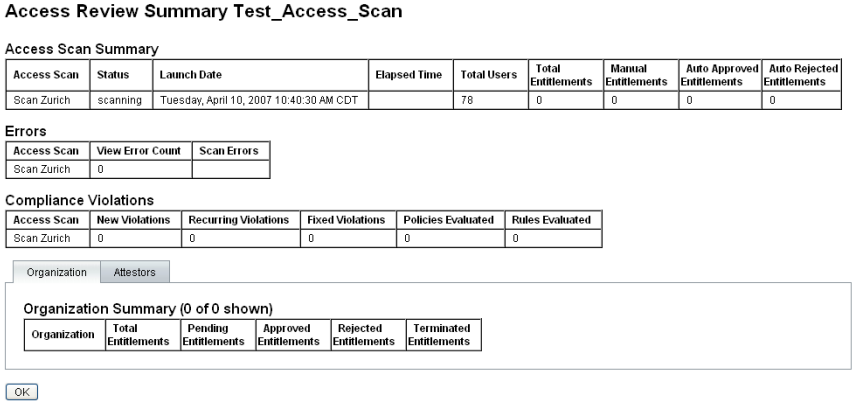
- **「ステータス」**- レビュープロセスの現在のステータス。初期化中、終了中、終了、進行中のスキャンの数、スケジュールされているスキャンの数、アテステーションを待機中、完了のいずれかになります。
- **「起動日」**- アクセスレビュータスクが開始された日付 (タイムスタンプ)。
- **「全ユーザー数」**- スキャン対象のユーザーの総数。
- **「エンタイトルメントの詳細」**- テーブルの追加の列に、ステータス別のエンタイトルメントの総数を表示します。これには、保留中、承認済み、却下済み、終了、是正済みのエンタイトルメントの詳細と、エンタイトルメント総数が含まれます。

  是正済みの列は、現在 REMEDIATING 状態のエンタイトルメント数が示されます。エンタイトルメントの是正後、PENDING 状態に移行するため、アクセスレビューの終了時、この列の値はゼロになります。

レビューの詳細情報を表示するには、そのレビューを選択して概要レポートを開きます。

図 11-16 に、アクセスレビュー概要レポートの例を示します。

図 11-16　「アクセスレビュー概要レポート」ページ



「組織 (Organization)」または**「アテスター (Attestors)」**フォームタブをクリックして、それらのオブジェクト別に分類されたスキャン情報を表示します。

「アクセスレビュー概要レポート」を実行することにより、レポートのこの情報をレビューおよびダウンロードすることもできます。

スキャン属性の変更

アクセススキャンの設定後、スキャンを編集して新しいオプションを指定できます。たとえば、スキャンするターゲットリソースの指定、アクセススキャンの実行中に違反をスキャンする監査ポリシーの指定などを行うことができます。

スキャン定義を編集するには、「アクセススキャン」リストから目的のスキャンを選択し、「アクセスレビュースキャンの編集」ページで属性を変更します。

スキャン定義の変更を保存するには、**「保存」**をクリックする必要があります。

注　アクセススキャンの範囲を変更すると、レビュー決定規則でユーザーエンタイトルメントを以前のユーザーエンタイトルメントレコードと比較している場合、その規則に影響する可能性があるため、新しく獲得されるユーザーエンタイトルメントレコードの情報が変わることがあります。

アクセスレビューのキャンセル

「アクセスレビュー」ページで**「終了」**をクリックすると、選択された進行中のレビューを停止します。レビューを終了すると、次のアクションが発生します。

- スケジュールされたスキャンがすべてスケジュール解除される
- アクティブなスキャンがすべて停止される

- 保留中のすべてのワークフローと作業項目が削除される
- 保留中のすべてのアテステーションにキャンセルのマークが付けられる
- ユーザーが完了したすべてのアテステーションが変更されないままになる

アクセスレビューの削除

「アクセスレビュー」ページで**「削除」**をクリックして、選択されたレビューを削除します。

アクセスレビューのタスクのステータスが「TERMINATED」または「COMPLETED」の場合、そのアクセスレビューを削除できます。進行中のアクセスレビュータスクは、終了させなければ削除できません。

アクセスレビューを削除すると、そのレビューで生成されたすべてのユーザーエンタイトルメントレコードも削除されます。削除アクションは監査ログに記録されます。

アクセスレビューを削除するには、「アクセスレビュー」ページから、**「削除」**をクリックします。

注 アクセスレビューをキャンセルし、削除すると、大量の Identity Manager オブジェクトやタスクを更新する可能性があるため、完了するまでに数分かかることがあります。処理の進行状況は、**「サーバータスク」>「すべてのタスク」**でタスクの結果を表示して確認できます。

アテステーション作業の管理

アテステーションリクエストの管理は、Identity Manager の管理者インタフェースまたはユーザーインタフェースで行うことができます。この節では、アテステーションリクエストへの応答、およびアテステーションに必要な作業について説明します。

アクセスレビューの通知

スキャン中、アテステーションリクエストの承認が必要になると、Identity Manager からアテスターに通知が送信されます。アテスターの役割が委任されている場合、そのリクエストは委任者に送信されます。複数のアテスターが定義されている場合は、それぞれのアテスターが電子メール通知を受け取ります。

Identity Manager インタフェースでは、リクエストは**「アテステーション」**作業項目として表示されます。保留中のアテステーション作業項目は、割り当てられたアテスターが Identity Manager にログインしたときに表示されます。

保留中のリクエストの表示

インタフェースの「作業項目」エリアからアテステーション作業項目を表示します。「作業項目」エリアの**「アテステーション」**タブを選択すると、承認を必要としているすべてのエンタイトルメントレコードが一覧表示されます。「アテステーション」ページでは、すべての直属の部下のエンタイトルメントレコードや、直接または間接的に管理している特定のユーザーのエンタイトルメントレコードも表示できます。

エンタイトルメントレコードの操作

アテステーション作業項目には、レビューを必要とするユーザーエンタイトルメントレコードが含まれます。エンタイトルメントレコードは、ユーザーアクセス特権、割り当てられたリソース、およびポリシー違反に関する情報を提供します。

アテステーションリクエストに想定される応答を次に示します。

- **「承認」**- エンタイトルメントレコードに記録された日付において適切なエンタイトルメントであることを認証します。
- **「却下」**- エンタイトルメントレコードに現時点では検証または是正できない矛盾がある可能性があることを示します。
- **「再スキャン」**ー 再スキャンをリクエストし、ユーザーのエンタイトルメントを再評価します。
- **「転送」**- 別の受信者がレビューするように指定できます。
- **「拒否」**- このレコードのアテステーションを適切に行えない場合、あるいは、より適切なアテスターがわからない場合にこのオプションを選びます。アテステーション作業項目は、レビュープロセスの所有者に転送されます。このオプションは、アクセスレビュータスクにレビュープロセスの所有者が定義されている場合にのみ使用できます。

指定されたエスカレーションタイムアウト時間までにアテスターがこれらのアクションのいずれかを実行することでリクエストに応答しなかった場合は、エスカレーションチェーン内の次のアテスターに通知が送信されます。通知プロセスは、応答がログに記録されるまで続行されます。

「コンプライアンス」>「アクセスレビュー」タブで、アテステーションステータスを監視できます。

クローズループ是正

ユーザーエンタイトルメントを却下する前に、次の手順を実行できます。

- 修正が必要なエンタイトルメントに対して、ほかのユーザーに修正をリクエストすること (是正のリクエスト) ができます。この場合、新しい是正作業項目が作成されるので、その作業項目に対して 1 人以上の是正者を割り当てます。

新しい是正者は、Identity Manager を使用して、または別の方法でユーザーを編集し、違反している箇所を是正できた場合には作業項目を是正済みとしてマークします。その時点で、ユーザーエンタイトルメントは再スキャンされ、再評価されます。

- エンタイトルメントの再評価 (再スキャン) をリクエストします。この場合、ユーザーエンタイトルメントは再スキャンされ、再評価されます。元のアテステーション作業項目はクローズされます。アクセススキャンに定義された規則によりエンタイトルメントにまだアテステーションが必要と判断された場合は、新しいアテステーション作業項目が作成されます。

是正のリクエスト

アクセススキャンで定義されている場合、保留中のアテステーションを別のユーザーに配信して是正してもらうことができます。

注	「アクセススキャンの作成」ページまたは「アクセススキャンの編集」ページの「動的エンタイトルメント」オプションで、この機能を有効にします。

別のユーザーから是正をリクエストするには、次の手順を実行します。

1. アテステーションのリストから 1 つ以上のエンタイトルメントを選択し、**「是正のリクエスト」**をクリックします。

   「是正のリクエストの選択と確認」ページが表示されます。

2. ユーザー名を入力して、**「追加」**をクリックし、そのユーザーを「転送先」フィールドに追加します。または、**「...」**ボタンをクリックして、ユーザーを検索します。検索リストのユーザーを選択して、**「追加」**をクリックし、そのユーザーを「転送先」リストに追加します。**「閉じる」**をクリックして、検索エリアを閉じます。

3. 「コメント」フィールドにコメントを入力して、**「続行」**をクリックします。

   Identity Manager はアテステーションのリストを返します。

注	各ユーザーエンタイトルメントの「履歴」エリアに是正リクエストの詳細が表示されます。

アテステーションの再スキャン

アクセススキャンで定義されている場合、保留中のアテステーションを再スキャンし、再評価することができます。

注	「アクセススキャンの作成」ページまたは「アクセススキャンの編集」ページの「動的エンタイトルメント」オプションで、この機能を有効にします。

保留中のアテステーションを再スキャンするには、次を実行します。

1. アテステーションのリストから 1 つ以上のエンタイトルメントを選択し、**「再スキャン」**をクリックします。

   「ユーザーエンタイトルメントの再スキャン」ページが表示されます。

2. 「コメント」エリアに再スキャンアクションに関するコメントを入力して、**「続行」**をクリックします。

アテステーション作業項目の転送

1 つ以上のアテステーション作業項目をほかのユーザーに転送できます。アテステーションを転送するには、次の手順を実行します。

1. アテステーションのリストから 1 つ以上の作業項目を選択し、**「転送」**をクリックします。

   「転送先の選択と確認」ページが表示されます。

2. 「転送先」フィールドにユーザー名を入力します。または、**「...」**ボタンをクリックして、ユーザー名を検索します。
3. 「コメント」フィールドに、転送アクションに関するコメントを入力します。
4. **「続行」**をクリックします。

   Identity Manager はアテステーションのリストを返します。

注	各ユーザーエンタイトルメントの「履歴」エリアに転送アクションの詳細が表示されます。

アクセスレビューアクションのデジタル署名

アクセスレビューアクションを処理するデジタル署名を設定できます。デジタル署名の設定については、203 ページの「承認の署名」を参照してください。その節では、署名付き承認のために証明書と CRL を Identity Manager に追加するために必要なサーバー側とクライアント側の設定について説明しています。

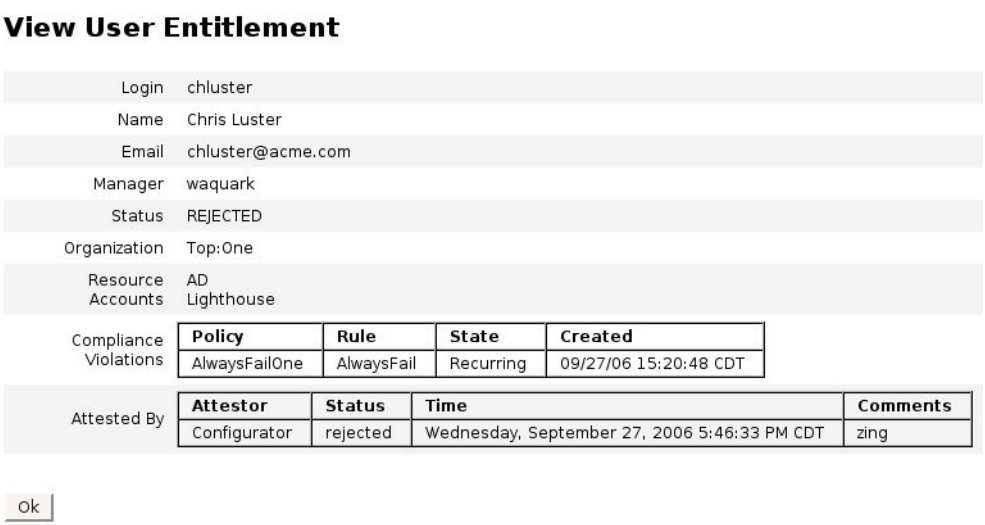
アクセスレビューレポート

Identity Manager では、次のレポートでアクセスレビューの結果を評価できます。

- **「アクセスレビュー範囲レポート」** - このレポートは、選択したアクセスレビューによって示されたユーザー間のオーバーラップまたは差異を特定します。ほとんどのアクセスレビューでは、ユーザークエリーまたは何らかのメンバーシップの操作によって、ユーザーの範囲が指定されるため、厳密なユーザーセットは時間の経過とともに変化すると予想されます。
- **「アクセスレビュー詳細レポート」** - このレポートには、以下の情報が表形式で表示されます。
  - **「名前」** - ユーザーエンタイトルメントレコードの名前
  - **「ステータス」** - レビュープロセスの現在のステータス。初期化中、終了中、終了、進行中のスキャンの数、スケジュールされているスキャンの数、アテステーションを待機中、完了のいずれかになります。
  - **「アテスター」** - そのレコードのアテスターとして割り当てられた Identity Manager ユーザー
  - **「スキャン日」** - スキャンが行われた日付として記録されたタイムスタンプ
  - **「処理日」** - エンタイトルメントレコードがアテストされた日付 (タイムスタンプ)
  - **「組織」** - エンタイトルメントレコード内のユーザーの組織
  - **「マネージャー」** - スキャンされたユーザーのマネージャー
  - **「リソース」** - このユーザーエンタイトルメントに取得された、ユーザーがアカウントを持つリソース
  - **「違反」** - レビューで検出された違反の数

ユーザーエンタイトルメントレコードを開くには、レポート内で名前をクリックします。図 11-17 は、ユーザーエンタイトルメントレコードの情報の表示例を示します。

図 11-17　ユーザーエンタイトルメントレコード



- **「アクセスレビュー概要レポート」** - このレポートは、404 ページの「アクセスレビューの進行状況の管理」でも説明されており、図 11-16 にも示されています。このレポートには、レポート用に選択したアクセススキャンに関する以下の概要情報が表示されます。
  - **「名前」** - アクセススキャンの名前
  - **「日付」** - レビューが起動された時のタイムスタンプ
  - **「ユーザー数」** - レビューでスキャンされたユーザーの数
  - **「エンタイトルメント数」** - 生成されたエンタイトルメントレコードの数
  - **「承認済み」** - 承認されたエンタイトルメントレコードの数
  - **「却下済み」** - 却下されたエンタイトルメントレコードの数
  - **「保留中」** - まだ保留中のエンタイトルメントレコードの数
  - **「キャンセル済み」** - キャンセルされたエンタイトルメントレコードの数

これらのレポートは、「レポートの実行」ページから PDF (Portable Document Format) 形式または CSV (カンマ区切り値) 形式でダウンロードできます。

アクセスレビュー是正

コンプライアンス違反の是正と受け入れ、およびアクセスレビューの是正は、「作業項目」タブの「是正」エリアから管理します。ただし、この 2 つの是正タイプには違いがあります。この節では、アクセスレビューの是正の一意の動作、383 ページの「コンプライアンス違反の是正と受け入れ」で説明している是正タスクおよび情報との違いを説明します。

アクセスレビュー是正について

アテスターがユーザーエンタイトルメントを是正するように要求する場合、Standard Attestation ワークフローによって、是正リクエストを作成します。このリクエストは「是正者」によって処理される必要があります。是正者とは、是正リクエストの評価と応答を許可されている、指定されたユーザーです。

問題は是正のみ可能で、受け入れることはできません。問題が解決されるまで、アテステーションを続行できません。

アクセスレビューによって是正者が指定された場合、アクセスレビューダッシュボードで、レビューにかかわるすべてのアテスターと是正者が追跡されます。

是正者のエスカレーション

アクセスレビューの是正リクエストは、最初の是正者より上にエスカレーションされません。

是正ワークフローのプロセス

アクセスレビューの是正のロジックは、Standard Attestation ワークフローに定義します。

アテスターがユーザーエンタイトルメントの是正をリクエストした場合、Standard Attestation ワークフローは次のようになります。

- 是正が必要なユーザーエンタイトルメントに関する情報を含む是正リクエスト (タイプ `accessReviewRemediation`) を生成します。
- リクエストされた是正者に電子メールを送信します。

新しい是正者は、Identity Manager を使用して、または別の方法でユーザーを編集し、違反している箇所を是正できた場合には作業項目を是正済みとしてマークします。その時点で、ユーザーエンタイトルメントは再スキャンされ、再評価されます。

是正応答

デフォルトでは、アクセスレビュー是正者は次の 3 つの応答オプションから選択できます。

- **「是正」**– 是正者は、何らかの処理を行なって問題を修正したことを示します。

  ユーザーエンタイトルメントは再スキャンされ、再評価されます。ユーザーエンタイトルメントに是正が必要であると再度マークされると、そのユーザーエンタイトルメントが元のアテスターのアテステーション作業項目リストに再表示されます。

  各ユーザーエンタイトルメントの「履歴」エリアに是正リクエストアクションの詳細が表示されます。

- **「転送」**– 是正者は、是正リクエストを解決するために別の人物に再割り当てします。

  各ユーザーエンタイトルメントの「履歴」エリアに転送アクションの詳細が表示されます。

- **「ユーザーの編集」**– 是正者は、問題を是正するためにユーザーを直接編集します。

  このボタンは、是正者がユーザーを変更する権限を持つ場合にのみ表示されます。ユーザーを変更し、**「保存」**をクリックすると、是正者は是正の確認ページに移動し、ユーザーの変更について説明するコメントを入力します。

  ユーザーエンタイトルメントは再スキャンされ、再評価されます。ユーザーエンタイトルメントに是正が必要であると再度マークされると、そのユーザーエンタイトルメントが元のアテスターのアテステーション作業項目リストに再表示されます。

  各ユーザーエンタイトルメントの「履歴」エリアに是正リクエストアクションとして編集の詳細が表示されます。

「是正」ページの操作

アクセスレビュー是正作業項目であるすべての是正作業項目の「タイプ」列に、UE (ユーザーエンタイトルメント) と表示されます。

サポートされないアクセスレビュー是正アクション

アクセスレビュー是正では、優先度と受け入れ機能がサポートされません。

アイデンティティー監査タスクのリファレンス

表 11-3 は、通常実行されるアイデンティティー監査タスクのクイックリファレンスです。この表では、各タスクを開始するための主要な Identity Manager インタフェースの場所を示します。そのタスクを実行できる場所または方法がほかにもある場合には、それらも示します。

表 11-3 アイデンティティー監査タスクのリファレンス

操作	ナビゲーション
監査ポリシーの作成、編集、または削除	**「コンプライアンス」**タブ、**「ポリシーの管理」**サブタブ
監査ポリシーの是正者の定義および是正ワークフローの割り当て	**「コンプライアンス」**タブ、**「ポリシーの管理」**サブタブ
1 人以上のユーザーまたは 1 つ以上の組織に対する監査スキャンの実行	**「アカウント」**タブ、「ユーザーアクション」リストまたは「組織アクション」リストから**「スキャン」**を選択
ポリシー違反是正リクエストに対する応答	**「作業項目」**タブ、**「是正」**サブタブ
ポリシー違反の受け入れ	**「作業項目」**タブ、**「是正」**サブタブ
是正されたポリシー違反のレビュー	**「作業項目」**タブ、**「是正」**サブタブ
監査ポリシーレポートの生成	**「レポート」**タブ、**「レポートの実行」**サブタブ
監査の無効化または有効化	**「設定」**タブ、**「監査」**サブタブ
イベント監査取得のセットアップ	**「設定」**タブ、**「監査」**サブタブ
管理者監査機能の編集	**「セキュリティー」**タブ、**「機能」**サブタブ
監査通知用の電子メールテンプレートのセットアップ	**「設定」**タブ、**「電子メールテンプレート」**サブタブ
データファイル / 規則のインポート (XML 形式のフォームなど)	**「設定」**タブ、**「交換ファイルのインポート」**サブタブ
アクセスレビュースキャンの定義	**「コンプライアンス」**タブ、**「スキャンの管理」**サブタブ
アクセスレビューの実行	**「コンプライアンス」**タブ、**「アクセスレビュー」**サブタブ
アクセスレビューの終了	**「コンプライアンス」**タブ、**「アクセスレビュー」**サブタブ
アクセスレビューのスケジュール	**「サーバータスク」**タブ、**「スケジュールの管理」**サブタブ
定期的アクセスレビューのセットアップ	**「コンプライアンス」**タブ、**「アクセススキャンの管理」**サブタブ
アクセスレビューステータスの監視	**「コンプライアンス」**タブ、**「アクセスレビュー」**サブタブ
アテスターの設定	**「コンプライアンス」**タブ、**「アクセススキャンの管理」**サブタブ

表 11-3 アイデンティティー監査タスクのリファレンス (続き)

操作	ナビゲーション
アテスターの作業の実行 (ユーザーエンタイトルメントのレビューと保証)	**「作業項目」**タブ、**「自分の作業項目」**タブ、**「アテステーション」**サブタブ
職務分掌レポートのレビュー	**「レポート」**タブ、**「レポートの実行」**サブタブ

第 12 章

監査ログ

この章では、Sun Java™ System Identity Manager 監査システムでのイベントの記録方法について説明します。説明する内容は次のとおりです。

- 概要
- Identity Manager 監査の機能
- イベントの作成
- 監査設定
- データベーススキーマ
- ログデータベースキー
- 監査ログの改ざんの防止
- カスタムパブリッシャーの使用

概要

Identity Manager 監査の目的は、誰が何をいつどの Identity Manager オブジェクトに対して行なったかを記録することです。

監査イベントは、1 つ以上のパブリッシャーによって処理されます。デフォルトでは、Identity Manager はリポジトリパブリッシャーを使用してリポジトリに監査イベントを記録します。管理者は、監査グループを使用してフィルタすることにより、記録する監査イベントのサブセットを選択できます。各パブリッシャーには、最初に有効にされた 1 つ以上の監査グループを割り当てることができます。

注	ユーザーの違反の監視および管理の詳細については、第 11 章「アイデンティティー監査」を参照してください。

Identity Manager 監査の機能

ほとんどのデフォルトの監査は、内部 Identity Manager コンポーネントにより実行されます。ただし、ワークフローまたは Java コードからイベントを生成できるようにしているインタフェースもあります。

デフォルトの Identity Manager 監査インストゥルメンテーションでは、次の 4 つの主要領域に焦点が当てられます。

- **プロビジョニングツール** – プロビジョニングツールと呼ばれる内部コンポーネントは監査イベントを生成します。
- **ビューハンドラ** – ビューアーキテクチャーでは、ビューハンドラが監査レコードを生成する必要があります。ビューハンドラは常に、オブジェクトの作成または変更時に監査を行います。
- **セッション** – セッションメソッド (`checkinObject`、`createObject`、`runTask`、`login`、`logout` など) は、監査処理の終了後に監査レコードを作成します。ほとんどのインストゥルメンテーションはビューハンドラにプッシュされます。
- **ワークフロー** – デフォルトでは、承認ワークフローだけが監査レコードを生成するように設定されています。これらは、リクエストが承認または却下されたときに、監査イベントを生成します。ワークフロー機能は、com.waveset.session.WorkflowServices アプリケーションを介して、監査ロガーとやり取りします。

イベントの作成

Identity Manager は内部監査を扱いますが、場合によっては、カスタムワークフローから監査イベントをログする必要があります。

ワークフローからの監査

com.waveset.session.WorkflowServices アプリケーションを使用して、ワークフロープロセスから監査イベントを生成します。表 12-1 では、このアプリケーションで利用できる引数について説明しています。

表 12-1 com.waveset.session.WorkflowServices の引数

引数	種類	説明
op	String	WorkflowServices の操作。audit に設定する必要があります。
type	String	監査対象のオブジェクトタイプの名前。
action	String	実行されたアクションの名前。
status	String	指定されたアクションのステータスの名前。
name	String	指定されたアクションの影響を受けるオブジェクトの名前。
resource	String	(オプション) 変更されるオブジェクトが置かれているリソースの名前。
accountId	String	(オプション) 変更されるアカウント ID。 これはネイティブなリソースアカウント名にします。
error	String	(オプション) 障害の発生時に付けられるローカライズされたエラー文字列。
reason	String	(オプション) ReasonDenied オブジェクトの名前。これは一般的な障害の原因を説明する、国際化されたメッセージにマップされています。
attributes	Map	(オプション) 追加または変更された属性の名前および値のマップ。
parameters	Map	(オプション) イベントに関連する追加の名前または値を最高 5 つまでマップします。
organizations	List	このイベントが配置される組織の名前または ID のリスト。これは、組織での監査ログの範囲設定に使用されます。このリストが存在しない場合、ハンドラは、種類と名前に基づいて組織を解決しようと試みます。組織を解決できない場合、イベントは最上位 (組織階層の最高レベル) に置かれます。

表 12-1　com.waveset.session.WorkflowServices の引数 (続き)

引数	種類	説明
originalAttributes	Map	(オプション) 古い属性値のマップ。この名前は、attributes 引数でリストされた名前に一致している必要があります。値は、監査ログに保存したいと考える任意の以前の値になります。

デフォルトのオブジェクト、アクション、ステータスの名前のリストについては、表 12-18 を参照してください。

例

コード例 12-1 は単純なワークフローアクティビティーを示します。ここでは、ResourceAdministrator が実行した ADSIResource1 という名前のリソース削除アクティビティーのログを記録するイベントが生成されます。

コード例 12-1　単純なワークフローアクティビティー

```
<Activity name='createEvent'>
   <Action class='com.waveset.session.WorkflowServices'>
   <Argument name='op' value='audit'/>
   <Argument name='type' value='Resource'/>
   <Argument name='action' value='Delete'/>
   <Argument name='status' value='Success'/>
   <Argument name='subject' value='ResourceAdministrator'/>
   <Argument name='name' value='ADSIResource1'/>
   </Action>
   <Transition to='end'/>
</Activity>
```

コード例 12-2 では、承認プロセスで各ユーザーが適用した変更を詳細なレベルまで追跡するワークフローに、特定の属性を追加する方法を示しています。この追加は通常、ユーザーからの入力をリクエストする ManualAction のあとに行われます。

ACTUAL_APPROVER は、実際に承認を実行した人物に基づいて、フォームおよびワークフロー (承認テーブルから承認する場合) で設定されます。APPROVER は、それが割り当てられた人物を識別します。

コード例 12-2 承認プロセスでの変更追跡への属性の追加

```
<Action name='Audit the Approval'
   application='com.waveset.session.WorkflowServices'>
     <Argument name='op' value='audit'/>
     <Argument name='type' value='User'/>
     <Argument name='name' value='$(CUSTOM_DESCRIPTION)'/>
     <Argument name='action' value='approve'/>
     <Argument name='accountId' value='$(accountId)'/>
     <Argument name='status' value='success'/>
     <Argument name='resource' value='$(RESOURCE_IF_APPLICABLE)'/>
     <Argument name='loginApplication' value='$(loginApplication)'/>
     <Argument name='attributes'>
       <map>
          <s>fullname</s><ref>user.accounts[Lighthouse].fullname</ref>
          <s>jobTitle</s><ref>user.accounts[Lighthouse].jobTitle</ref>
          <s>location</s><ref>user.accounts[Lighthouse].location</ref>
          <s>team</s><ref>user.waveset.organization</ref>
          <s>agency</s><ref>user.accounts[Lighthouse].agency</ref>
      </map>
    </Argument>
    <Argument name='originalAttributes'>
      <map>
<s>fullname</s>
        <s>User's previous fullname</s>
        <s>jobTitle</s>
        <s>User's previous job title</s>
        <s>location</s>
        <s>User's previous location</s>
        <s>team</s>
        <s>User's previous team</s>
        <s>agency</s>
        <s>User's previous agency</s>      </map>
    </Argument>
    <Argument name='attributes'>
      <map>
         <s>firstname</s>
         <s>Joe</s>
         <s>lastname</s>
         <s>New</s>
```

コード例 12-2　　承認プロセスでの変更追跡への属性の追加 (続き)

```
<Action name='Audit the Approval'
   application='com.waveset.session.WorkflowServices'>
      </map>
    </Argument>
    <Argument name='subject'>
       <or>
          <ref>ACTUAL_APPROVER</ref>
          <ref>APPROVER</ref>
      </or>
    </Argument>
    <Argument name='approver' value='$(APPROVER)'/>
</Action>
```

監査設定

監査設定は、1 つ以上のパブリッシャーと定義済みの複数のグループから構成されます。

監査グループは、オブジェクトタイプ、アクション、アクションの結果に基づいて、すべての監査イベントのサブセットを定義します。各パブリッシャーには 1 つ以上の監査グループが割り当てられます。デフォルトで、すべての監査グループにリポジトリパブリッシャーが割り当てられます。

監査パブリッシャーは、特定の監査出力先に監査イベントを配信します。デフォルトのリポジトリパブリッシャーは、監査レコードをリポジトリに書き込みます。それぞれの監査パブリッシャーには、実装専用のオプションを指定できます。監査パブリッシャーには、テキストフォーマッタを割り当てることができます。テキストフォーマッタは監査イベントのテキスト表現を提供します。

監査設定 (`#ID#Configuration:AuditConfiguration`) オブジェクトは、`sample/auditconfig.xml` ファイルで定義されます。この設定オブジェクトには、汎用オブジェクトである拡張機能があります。その最上位には次の属性があります。

- filterConfiguration
- extendedTypes
- extendedActions
- extendedResults
- publishers

filterConfiguration

filterConfiguration 属性は、1 つ以上のイベントがイベントフィルタを通過できるようにするために使用されるイベントグループをリストします。filterConfiguration 属性にリストされたそれぞれのグループには、表 12-2 にリストした属性が含まれます。

表 12-2　filterConfiguration の属性

属性	種類	説明
groupName	String	イベントグループ名
displayName	String	グループ名を示すメッセージカタログキー
enabled	String	グループ全体が有効か無効かを示すブール型のフラグ。この属性は、フィルタリングを行うオブジェクトを最適化します。
enabledEvents	List	グループがどのイベントを有効にするかを示す汎用オブジェクトのリスト。ログを有効にするには、イベントをリストする必要があります。リストされた各オブジェクトには次の属性が必要になります。 • objectType (文字列) − objectType の名前。 • actions (リスト) − 1 つ以上のアクションのリスト。 • results (リスト) − 1 つ以上の結果のリスト。

コード例 12-3 に、デフォルトのリソース管理グループを示します。

コード例 12-3　　デフォルトのリソース管理グループ

```
<Object name='Resource Management'>
  <Attribute name='enabled' value='true'/>
  <Attribute name='displayName'
             value='UI_RESOURCE_MGMT_GROUP_DISPLAYNAME'/>
  <Attribute name='enabledEvents'>
    <List>
      <Object>
        <Attribute name='objectType' value='Resource'/>
        <Attribute name='actions' value='ALL'/>
        <Attribute name='results' value='ALL'/>
      </Object>
      <Object>
        <Attribute name='objectType' value='ResourceObject'/>
        <Attribute name='actions' value='ALL'/>
        <Attribute name='results' value='ALL'/>
      </Object>
    </List>
  </Attribute>
</Object>
```

Identity Manager には、次のデフォルトのイベントグループが用意されています。

- アカウント管理
- コンプライアンス管理
- 設定管理
- Identity Manager ログイン / ログオフ
- パスワード管理
- リソース管理
- ロール管理
- セキュリティー管理
- タスク管理
- Identity Manager 外部での変更
- Service Provider Edition

Identity Manager 管理インタフェースの「イベント監査」ページ (`configure/auditeventconfig.jsp`) から、それぞれのグループを設定できます。このページでは、成功のイベントや失敗のイベントをグループごとに設定できます。グループの enabledEvents の追加や変更は、このインタフェースではサポートされていませんが、Identity Manager デバッグページを使用して行うことができます。

デフォルトのイベントグループと、それによって有効にされるイベントについては、以降の節で説明します。

アカウント管理

このグループはデフォルトで有効になっています。

表 12-3 デフォルトのアカウント管理イベントグループ

種類	アクション
Resource Account	作成、更新、削除、有効化、無効化、却下、承認、名前の変更
Identity Manager Account	作成、更新、削除、有効化、無効化、名前の変更

コンプライアンス管理

このグループはデフォルトで有効になっています。

表 12-4 デフォルトのコンプライアンス管理イベントグループ

種類	アクション
AuditPolicy	すべてのアクション
ComplianceViolation	すべてのアクション
Remediation Workflow	すべてのアクション

設定管理

このグループはデフォルトで有効になっています。

表 12-5 デフォルトの設定管理イベントグループ

種類	アクション
Configuration	すべてのアクション
UserForm	すべてのアクション

表 12-5　デフォルトの設定管理イベントグループ (続き)

種類	アクション
Rule	すべてのアクション
EmailTemplate	すべてのアクション
LoginConfig	すべてのアクション
Policy	すべてのアクション
XMLData	Import
Log	すべてのアクション

Identity Manager ログイン / ログオフ

このグループはデフォルトで有効になっています。

表 12-6　デフォルトの Identity Manager ログイン / ログオフイベントグループ

種類	アクション
User	ログイン、ログオフ、クレデンシャル有効期限
Administrator	ログイン、ログオフ、クレデンシャル有効期限

パスワード管理

このグループはデフォルトで有効になっています。

表 12-7　デフォルトのパスワード管理イベントグループとイベント

種類	アクション
Resource Account	パスワードの変更 / リセット

リソース管理

このグループはデフォルトで有効になっています。

表 12-8　デフォルトのリソース管理イベントグループとイベント

種類	アクション
Resource	すべてのアクション

表 12-8　デフォルトのリソース管理イベントグループとイベント (続き)

種類	アクション
Resource Object	すべてのアクション
ResourceForm	すべてのアクション
ResourceAction	すべてのアクション
AttrParse	すべてのアクション

ロール管理

このグループはデフォルトで無効になっています。

表 12-9　デフォルトのロール管理イベントグループとイベント

種類	アクション
Role	すべてのアクション

セキュリティー管理

このグループはデフォルトで有効になっています。

表 12-10　デフォルトのセキュリティー管理イベントグループとイベント

種類	アクション
ObjectGroup	すべてのアクション
AdminGroup	すべてのアクション
Administrator	すべてのアクション
EncryptionKey	すべてのアクション

タスク管理

このグループはデフォルトで無効になっています。

表 12-11　タスク管理イベントグループとイベント

種類	アクション
TaskInstance	すべてのアクション

表 12-11　タスク管理イベントグループとイベント (続き)

種類	アクション
TaskDefinition	すべてのアクション
TaskSchedule	すべてのアクション
TaskResult	すべてのアクション
ProvisioningTask	すべてのアクション

Identity Manager 外部での変更

このグループはデフォルトで無効になっています。

表 12-12　Identity Manager 外部での変更イベントグループとイベント

種類	アクション
ResourceAccount	NativeChange

Service Provider Edition

このグループはデフォルトで有効になっています。

表 12-13　Service Provider Edition イベントグループとイベント

種類	アクション
IDMXUser	作成、変更、削除、ユーザー名の復旧、チャレンジ応答、認証回答の更新、操作前と操作後のコールアウト

extendedTypes

`com.waveset.object.Type` クラスに追加する新しいタイプをそれぞれ監査できます。新しいタイプには一意の 2 文字のデータベースキーが割り当てられ、このキーはデータベースに格納されます。新しいタイプはすべて、さまざまな監査レポートインタフェースに追加されます。フィルタされずにデータベースにログされる新しいタイプは、監査イベントグループの `enabledEvents` 属性にそれぞれ追加する必要があります (`enabledEvents` 属性の説明を参照)。

関連付けられた `com.waveset.objectType` を持たない対象を監査したり、既存のタイプをさらに細かく表したりする必要が生じる場合があります。

たとえば、WSUser オブジェクトは、ユーザーのアカウント情報をすべてリポジトリに格納します。監査プロセスは、各イベントを USER タイプとしてマークを付けるのではなく、WSUser オブジェクトを 2 つの異なる監査タイプ (Resource Account および Identity Manager Account) に分割します。このようにオブジェクトを分割することにより、監査ログでの特定のアカウント情報が検索しやすくなります。

extendedObjects 属性に追加することによって、拡張された監査タイプを追加します。それぞれの拡張されたオブジェクトには、次の表にリストした属性が必要になります。

表 12-14 拡張されたオブジェクトの属性

引数	種類	説明
name	String	タイプの名前。これは AuditEvents の作成時とイベントフィルタリング中に使用されます。
displayName	String	タイプの名前を表すメッセージカタログキー。
logDbKey	String	ログテーブルにこのオブジェクトを格納するときに使用する 2 文字のデータベースキー。詳細については、「ログデータベースキー」を参照してください。
supportedActions	List	オブジェクトタイプがサポートするアクション。この属性は、ユーザーインタフェースから監査クエリーを作成するときに使用されます。この値が NULL である場合、すべてのアクションが、このオブジェクトタイプのクエリーで取り得る値として表示されます。
mapsToType	String	(オプション) 該当する場合、このタイプにマップされる com.waveset.object.Type の名前。この属性は、イベントでまだ指定されていない場合、オブジェクトの組織のメンバーシップを解決しようとするときに使用されます。
organizationalMembership	List	(オプション) このタイプのイベントにまだ組織のメンバーシップが割り当てられていない場合、このイベントを配置する組織 ID のデフォルトのリスト。

すべての顧客固有のキーには # の記号を先頭に付け、新しい内部キーが追加されたときにキーが重複するのを防止します。

コード例 12-4 に、拡張タイプの Identity Manager アカウントを示します。

コード例 12-4　拡張タイプの Identity Manager アカウント

```
<Object name='LighthouseAccount'>
   <Attribute name='displayName' value='LG_LIGHTHOUSE_ACCOUNT'/>
   <Attribute name='logDbKey' value='LA'/>
   <Attribute name='mapsToType' value='User'/>
   <Attribute name='supportedActions'>
      <List>
         <String>Disable</String>
         <String>Enable</String>
         <String>Create</String>
         <String>Modify</String>
         <String>Delete</String>
         <String>Rename</String>
      </List>
   </Attribute>
</Object>
```

extendedActions

監査アクションは通常、com.waveset.security.Right オブジェクトにマップします。新しい Right オブジェクトを追加するときに、一意の 2 文字の logDbKey を指定する必要があります。これはデータベースに格納されます。監査する必要のある特定のアクションに対応する権利がない状況に遭遇することがあります。extendedActions 属性のオブジェクトのリストに追加することにより、アクションを拡張できます。

それぞれの extendedActions オブジェクトは、表 12-15 で示した属性を含んでいる必要があります。

表 12-15　extendedAction の属性

属性	種類	説明
name	String	アクションの名前。これは AuditEvents の作成時とイベントのフィルタ中に使用されます。
displayName	String	アクションの名前を表すメッセージカタログキー。

表 12-15　extendedAction の属性 (続き)

属性	種類	説明
logDbKey	String	ログテーブルにこのアクションを格納するときに使用する 2 文字のデータベースキー。 詳細については、「ログデータベースキー」を参照してください。

すべての顧客固有のキーには # の記号を先頭に付け、新しい内部キーが追加されたときにキーが重複するのを防止します。

コード例 12-5 に、ログアウトのアクションを追加する例を示します。

コード例 12-5　ログアウトのアクションの追加

```
<Object name='Logout'>
  <Attribute name='displayName' value='LG_LOGOUT'/>
  <Attribute name='logDbKey' value='LO'/>
</Object>
```

extendedResults

監査のタイプおよびアクションを拡張する以外に、結果を追加できます。デフォルトで、成功と失敗の 2 つの結果があります。extendedResults 属性のオブジェクトのリストに追加することにより、結果を拡張できます。

それぞれの extendedResults オブジェクトは、表 12-16 で示した属性を含んでいる必要があります。

表 12-16　extendedResults の属性

属性	種類	説明
name	String	結果の名前。これは AuditEvents でのステータスの設定時とイベントのフィルタ中に使用されます。
displayName	String	結果の名前を表すメッセージカタログキー。
logDbKey	String	ログテーブルにこの結果を格納するときに使用する 1 文字のデータベースキー。予約済みの値については、「データベースキー」のタイトルの節を参照してください。

すべての顧客固有のキーには 0 ～ 9 の範囲を使用して、新しい内部キーを追加するときにキーの重複を防止します。

publishers

パブリッシャーリストの各項目は汎用オブジェクトです。各パブリッシャーには次の属性があります。

表 12-17　publishers 属性

属性	種類	説明
class	String	パブリッシャークラスの名前。
displayName	String	パブリッシャーの名前を表すメッセージカタログキー。
description	String	パブリッシャーの説明。
filters	List	このパブリッシャーに割り当てられた監査グループのリスト。
formatter	String	テキストフォーマッタの名前 (存在する場合)。
options	List	パブリッシャーオプションのリスト。これらのオプションはパブリッシャーに固有のものです。このリストの各項目は、PublisherOption のマップ表現です。例については、sample/auditconfig.xml を参照してください。

データベーススキーマ

監査データの格納に使用する Identity Manager データベースには次の 2 つのテーブルがあります。

- waveset.log － イベントのほとんどの詳細を格納します。
- waveset.logattr － 各イベントが所属する組織の ID を格納します。

waveset.log

ここでは、waveset.log テーブルで使用されるさまざまな列名とデータ型をリストします。データ型は、Oracle データベース定義から取得され、データベースごとに若干異なります。サポートされるすべてのデータベースのデータスキーマ値のリストについては、付録 C 「監査ログデータベーススキーマ」を参照してください。

いくつかの列値は、領域を最適化するために、キーとしてデータベースに格納されます。キー定義については、「ログデータベースキー」の節を参照してください。

- objectType CHAR(2) ― 監査されているオブジェクトタイプを表す 2 文字のキー。
- action CHAR(2) ― 実行されたアクションを表す 2 文字のキー。
- actionStatus CHAR(1) ― 実行されたアクションの結果を表す 1 文字のキー。
- reason CHAR(2) ― 障害が発生した場合に、`ReasonDenied` オブジェクトを記述するための 2 文字のデータベースキー。`ReasonDenied` は、メッセージカタログエントリをラップするクラスで、無効な資格や不十分な特権などの一般的なエラーに使用されます。
- actionDateTime VARCHAR(21) ― 上記のアクションが行われる日時。この値はグリニッジ標準時で格納されます。
- objectName VARCHAR(128) ― 操作中に影響を受けたオブジェクトの名前。
- resourceName VARCHAR(128) ― 該当する場合、操作中に使用されたリソース名。リソースを参照しないイベントもありますが、多くの場合、操作の実行で使用したリソースをログすると、より詳しい詳細が得られます。
- accountName VARCHAR(255) ― 該当する場合、影響を受けているアカウント ID。
- server VARCHAR(128) ― アクションが実行されるサーバー (イベントトロガーにより自動的に割り当て)。
- message VARCHAR(255) ― エラーメッセージなど、アクションに関連するローカライズされたメッセージ。テキストはローカライズして格納されます。したがって国際化されません。
- interface VARCHAR(50) ― 操作が実行された Identity Manager インタフェース (管理者、ユーザー、IVR、SOAP インタフェースなど)。
- acctAttrChanges VARCHAR(4000) ― 作成および更新中に変更されたアカウント属性を格納します。属性変更フィールドは常に、リソースアカウントまたは Identity Manager アカウントオブジェクトの作成または更新中に設定されます。アクション中に変更されたすべての属性は、文字列としてこのフィールドに格納されます。データは `NAME=VALUE NAME2=VALUE2` の形式です。このフィールドは、名前または値に対して `"contains"` SQL 文を実行して問い合わせることができます。

  コード例 12-6 に `acctAttrChanges` 列の値を示します。

コード例 12-6　　acctAttrChanges 列の値

```
COMPANY="COMPANY" DEPARTMENT="DEPT" DESCRIPTION="DSMITH
DESCRIPTION" FAX NUMBER="5122222222" HOME ADDRESS="12282
MOCKINGBIRD LANE" HOME CITY="AUSTIN" HOME PHONE="5122495555"
HOME STATE="TX" HOME ZIP="78729" JOB TITLE="DEVELOPER"
MOBILE PHONE="5125551212" WORK PHONE="5126855555"
EMAIL="someone@somecompany.COM" EXPIREPASSWORD="TRUE"
FIRSTNAME="DANIEL" FULLNAME="DANIEL SMITH" LASTNAME="SMITH"
```

- acctAttr01label-acctAttr05label VARCHAR(50) − これらの 5 つの追加 NAME スロットは、最高 5 つの属性を、大きな塊 (ブロブ) ではなく独立した列に格納されるように格上げできる列です。属性の格上げを行うには、リソーススキーマ設定ページの 「監査」列のチェックを有効にします。これにより、属性がデータマイニングに使用できるようになります。
- acctAttr01value-acctAttr05value VARCHAR(128) − ブロブ列ではなく、個別の列に格納されるように最高 5 つの属性を格上げできる 5 つの追加 VALUE スロット。
- parm01label-parm05label VARCHAR(50) − イベントに関連するパラメータの格納に使用される 5 つのスロット。これらの例は、Client IP と Session ID です。
- parm01value-parm05value VARCHAR(128) − イベントに関連するパラメータの格納に使用される 5 つのスロット。これらの例は、Client IP と Session ID です。
- id VARCHAR(50) − waveset.logattr テーブルで参照されるリポジトリによって各レコードに割り当てられた一意の ID。
- name VARCHAR(128) − 各レコードに割り当てられた生成名。

waveset.logattr

waveset.logattr テーブルは、イベントごとに組織のメンバーシップの ID を格納するために使用されます。このテーブルを使用して、組織別に監査ログの範囲が設定されます。

- id VARCHAR(50) − waveset.log レコードの ID。
- attrname VARCHAR(50) − 現在は常に MEMBEROBJECTGROUPS です。
- attrval VARCHAR(255) − イベントが所属する MemberObject グループの ID。

ログデータベースキー

objectType、アクション、actionStatus、および理由の列は、領域を節約するために、キーとしてデータベースに格納されています。

objectType、アクション、および結果

表 12-18 に、キーとしてデータベースに格納される objectType、アクション、および結果を示します。

表 12-18　キーとして格納される objectType、アクション、結果

objectType 名	DbKey	アクション名	DbKey	結果名	DbKey
Account	AN	Approve	AP	Success	S
Administrator	AD	Bypass Verify	BV	Failure	F
AdminGroup	AG	Cancel Reconcile	CR		
Attribute Definition	AF	challengeResponse	CD		
Application	AP	Change Password	CP		
Capability	US	Create	CT		
Configuration	CN	Connect	CO		
Discovery	DS	Delete	DL		
EmailTemplate	ET	Deprovision	DP		
Extract	ER	Disable	DS		
ExtractTask	EX	Disconnect	DC		
Identity Manager Account	LA	Enable	EN		
IDMXUser	UX	Execute	LN		
LoadConfig	LD	Export	EP		
LoadTask	LT	Import	IM		
LoginConfig	LC	List	LI		
Policy	PO	Load	LD		
Provisioning Task	PT	Login	LG		
Resource	RS	Update	MO		
Resource Account	RA	Logout	LO		
Resource Form	RF	Native Changes	NC		
Resource Object	RE	Post Operation	PT		
RiskReportTask	RR	Pre Operation	PE		

表 12-18　キーとして格納される objectType、アクション、結果 (続き)

objectType 名	DbKey	アクション名	DbKey	結果名	DbKey
Role	RL	Provision	PV		
Rule	RU	Reset Password	RP		
User	US	Reprovision	RV		
TaskDefinition	TD	Reject	RJ		
TaskInstance	TI	Terminate	TR		
TaskSchedule	TS	usernameRecovery	UR		
TaskTemplate	TT				
TaskResult	TR				
UserForm	UF				
WorkItem	WI				
XMLDATA	XD				

理由

表 12-19 に、キーとしてデータベースに格納される理由を示します。

表 12-19　　キーとして格納される理由

理由名	説明	DbKey
PolicyViolation	ポリシー {0} の違反 : {1}	PV
InvalidCredentials	無効な資格	CR
InsufficientPrivileges	不十分な特権	IP
DatabaseAccessFailed	データベースアクセスの失敗	DA
AccountDisabled	アカウントの無効	DI

監査ログの改ざんの防止

Identity Manager を設定して、次の形式の監査ログの改ざんを防止できます。

- 監査ログレコードの追加または挿入
- 既存の監査ログレコードの変更
- 監査ログレコードまたは監査ログ全体の削除
- 監査ログの切り捨て

すべての Identity Manager 監査ログレコードには、サーバー単位の一意のシーケンス番号と、レコードおよびシーケンス番号の暗号化ハッシュが記録されています。改ざん検出レポートを作成するときに、サーバーごとに監査ログが走査され、次の点が調べられます。

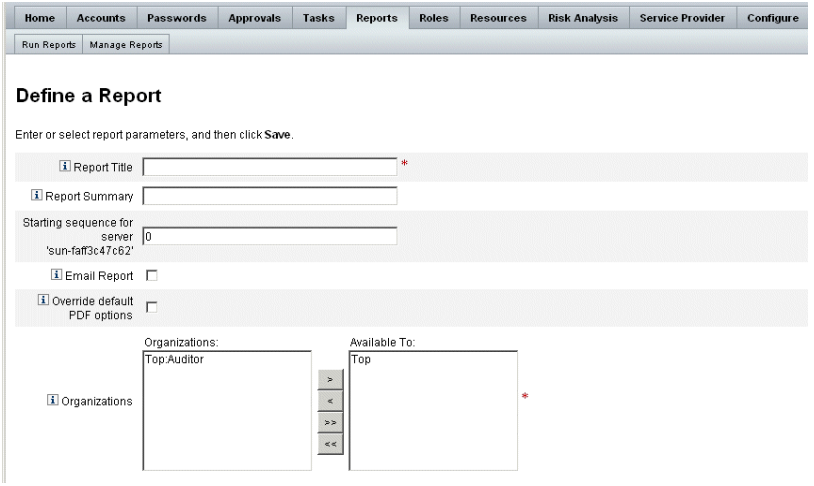
- シーケンス番号の欠如 (削除されたレコードを示す)
- ハッシュの不一致 (変更されたレコードを示す)
- 重複したシーケンス番号 (コピーされたレコードを示す)
- 予想より小さな最後のシーケンス番号 (切り捨てられたログを示す)

改ざん防止ログの設定

改ざん防止ログを設定するには、次の手順に従います。

1. **「レポート」>「新規」>「監査ログの改ざんレポート」**を選択して、改ざんレポートを作成します。
2. 改ざんレポート用の定義ページが表示されたら (図 12-1 参照)、レポートのタイトルを入力し、**「保存」**をクリックします。

図 12-1　監査ログの改ざんレポートの設定

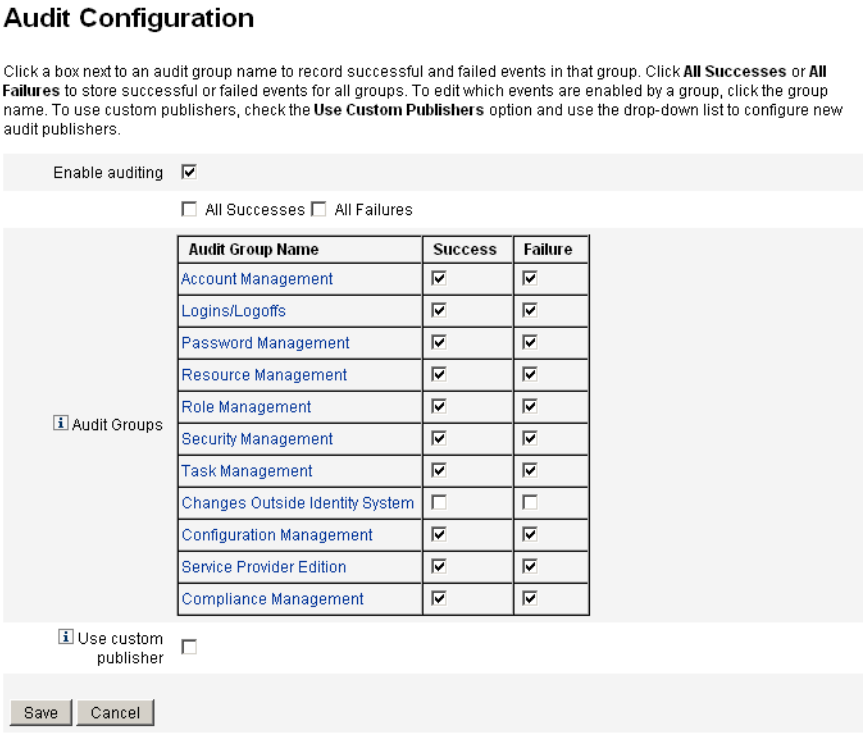


次のオプションパラメータも指定できます。

- **「レポートの概要」**― レポートの概要をわかりやすく記述します。
- **「サーバー「<*server_name*>」の開始シーケンス」**― サーバーの開始シーケンス番号を入力します。
- このオプションを使用すると、改ざんのフラグを付けることなく古いログエントリを削除でき、パフォーマンスが低下しないようにレポートの範囲を制限できます。
- **「レポート結果を送信」**― 指定した電子メールアドレスへレポート結果を電子メールで送信できるようにします。
- このオプションを選択すると、ページが更新され、電子メールアドレスを指定するようにリクエストされます。ただし、電子メールはテキストコンテンツにとって安全ではないことに留意してください。機密情報 (アカウント ID やアカウント履歴など) が漏洩する可能性があります。
- **「デフォルトの PDF オプションを上書き」**― このレポートのデフォルトの PDF オプションを上書きします。
- **「組織」**― このレポートにアクセスできる組織を選択します。

3. 次に、**「設定」>「監査」**を選択して、「監査設定」ページを開きます (図 12-2 参照)。

図 12-2 改ざん防止監査ログ設定



4. **「カスタムパブリッシャーの使用」**を選択し、「リポジトリ」パブリッシャーリンクをクリックします。
5. **「改ざん防止監査ログ」**のチェックボックスを選択し、**「OK」**をクリックします。
6. **「保存」**をクリックして、設定を保存します。

   このオプションをもう一度選択解除できますが、解除したエントリには、監査ログの改ざんレポートで、解除されていることを示すフラグが付けられます。これらのエントリを無視するようにレポートを再設定する必要があります。

カスタムパブリッシャーの使用

Identity Manager では、カスタム監査パブリッシャーへ監査イベントを送信できます。次のカスタムパブリッシャーを使用できます。

- コンソール − 標準出力または標準エラーに監査イベントを印刷します。
- ファイル − フラットファイルへ監査イベントを書き込みます。
- JDBC − JDBC データストアに監査イベントを記録します。
- JMS − JMS キューかトピックに監査イベントを記録します。
- スクリプト − カスタムスクリプトで監査イベントを保存できるようにします。

これらのパブリッシャーのソースコードはリファレンスキットにあります。リファレンスキットでは、Javadoc 形式で記されたインタフェースのマニュアルも用意されています。

パブリッシャーの開発

すべてのパブリッシャーは AuditLogPublisher インタフェースを実装します。インタフェースの詳細については、Javadoc を参照してください。開発者には、`AbstractAuditLogPublisher` クラスを拡張するようにお勧めします。このクラスは設定を解析し、すべての必要なオプションがパブリッシャーに用意されていることを確認します。リファレンスキットのパブリッシャーの例を参照してください。

パブリッシャーには引数なしコンストラクタが必要になります。

ライフサイクル

パブリッシャーのライフサイクルを、次の手順で説明します。

1. オブジェクトがインスタンス化されます。
2. `setFormatter()` メソッドを使用して、フォーマッタ (存在する場合) が設定されます。
3. `configure(`*Map*`)` メソッドを使用して、オプションが指定されます。
4. `publish(`*Map*、*LoggingErrorHandler*`)` メソッドを使用して、イベントが発行されます。
5. `shutdown()` メソッドを使用して、パブリッシャーが終了します。

手順 1 ～ 3 は、Identity Manager の起動時と監査設定の更新ごとに実行されます。シャットダウンが呼び出される前に監査イベントが生成されていない場合には、手順 4 は行われません。

`configure(`*Map*`)` は、同一のパブリッシャーオブジェクトでは 1 度だけ呼び出されます。パブリッシャーは、実行時の設定変更に備える必要はありません。監査設定が更新されると、まず現在のパブリッシャーが停止され、新しいパブリッシャーが作成されます。

手順 3 の `configure()` メソッドは WavesetException をスローする場合があります。この場合、パブリッシャーは無視され、パブリッシャーに対してほかの呼び出しは行われません。

設定

パブリッシャーにはオプションを付けないことも、1 つ以上のオプションを付けることもできます。`getConfigurationOptions()` メソッドは、パブリッシャーがサポートするオプションのリストを返します。オプションは、PublisherOption クラス (このクラスの詳細については Javadoc を参照) を使用してカプセル化されます。監査設定ビューアは、パブリッシャー用の設定インタフェースを構築するときに、このメソッドを呼び出します。

Identity Manager は、サーバーの起動時および監査設定の変更後に、configure(Map) メソッドを使用してパブリッシャーを設定します。

フォーマッタの開発

リファレンスキットには、次のフォーマッタのソースコードが収められています。

- XmlFormatter － 監査イベントを XML 文字列としてフォーマットします。
- UlfFormatter - 汎用ログ形式 (ULF) に従って、監査イベントをフォーマットします。Sun Java System Application Server はこの形式を使用します。

フォーマッタは、`AuditRecordFormatter` インタフェースを実装する必要があります。さらに、フォーマッタには引数なしコンストラクタが必要になります。詳細については、リファレンスキットに収録された Javadoc を参照してください。

パブリッシャー / フォーマッタの登録

#ID#Configuration:SystemConfiguration オブジェクトの監査属性は、登録済みのパブリッシャーとフォーマッタをすべて一覧表示します。これらのパブリッシャーとフォーマッタだけが、監査設定ユーザーインタフェースで使用できます。

第 13 章

サービスプロバイダの管理

この章では、Sun Java™ System Identity Manager のサービスプロバイダ (SPE) 機能を管理するために知っておく必要がある情報を提供します。この情報を利用するには、Lightweight Directory Access Protocol (LDAP) ディレクトリおよび連携管理についての知識が役に立ちます。Service Provider 実装に関するより広範な解説については、『Identity Manager SPE Deployment』を参照してください。

この章は次のトピックで構成されています。

- Service Provider 機能の概要
- 初期設定
- トランザクション管理
- 委任された管理
- サービスプロバイダユーザーの管理
- 同期
- サービスプロバイダ監査イベントの設定

Service Provider 機能の概要

サービスプロバイダ環境では、イントラネットユーザーだけでなくエクストラネットユーザーも含むすべてのエンドユーザーのユーザープロビジョニングを管理できる必要があります。Identity Manager Service Provider Edition 機能を利用すると、企業の管理者は、ID アカウントを Identity Manager ユーザーとサービスプロバイダユーザーの 2 種類に分類することができます。Identity Manager のサービスプロバイダユーザーは、タイプに「サービスプロバイダユーザー」が設定されているユーザーアカウントです。

Identity Manager のユーザープロビジョニング機能と監査機能は、次の機能を提供することにより、サービスプロバイダ実装にも拡張されます。

拡張エンドユーザーページ

サービスプロバイダ実装用にカスタマイズ可能な拡張エンドユーザーページが用意されています。

パスワードとアカウント ID のポリシー

ほかの Identity Manager ユーザーと同じように、サービスプロバイダユーザーとリソースアカウントについても、アカウント ID ポリシーとパスワードポリシーを定義できます。

ポリシーテーブルに追加されている**「SPE システムアカウントポリシー」**により、サービスプロバイダユーザーに対するポリシーチェックコードが作動します。

Identity Manager と Service Provider の同期

Identity Manager アカウントとサービスプロバイダアカウントの同期は、すべての Identity Manager サーバーで実行するか、または選択したサーバーだけで実行するように設定できます。

Service Provider 同期は、Identity Manager 同期と同様に、「リソース」ページの「リソースアクション」オプションで簡単に停止および開始できます。480 ページの「同期の開始と停止」を参照してください。

Identity Manager ユーザー同期と Service Provider ユーザー同期では、入力フォームが異なります。476 ページの「エンドユーザーインタフェース」を参照してください。

Access Manager との統合

Service Provider のエンドユーザーページでの認証に Sun Java System Access Manager 7 2005Q4 を使用できます。Access Manager との統合を設定すると、Access Manager は、認証されたユーザーだけがエンドユーザーページにアクセスできるようにします。

Service Provider は、監査のためのユーザー名を必要とします。`AMAgent.properties` ファイルを更新して、ユーザーの ID を HTTP ヘッダーに追加します。その例を次に示します。

```
com.sun.identity.agents.config.response.attribute.mapping[uid] =
HEADER_speuid
```

エンドユーザーページ認証フィルタによって、残りのコード部分で想定されている HTTP ヘッダー値が HTTP セッションに割り当てられます。

初期設定

Service Provider 機能を設定するには、次の手順に従って、ディレクトリサーバーの Identity Manager 設定オブジェクトを編集します。

- メイン設定の編集
- ユーザー検索設定の編集

注　続行する前に、次のことを確認してください。

- LDAP リソースが定義されている。デフォルトで、SPE End-User Directory という名前のサンプルリソースがインポートされます。ユーザー情報と設定情報を異なるディレクトリに格納する場合は、複数のリソースを設定できます。
  - スキーマを XML オブジェクトのマッピングに含める必要があります。
  - ディレクトリリソース用に設定されたベースコンテキストは、そのディレクトリに格納されたユーザーのみに適用されます。
- 必要に応じて、Service Provider アカウントポリシーを設定します。

メイン設定の編集

Service Provider 実装の設定オブジェクトを編集するには、次の手順に従います。

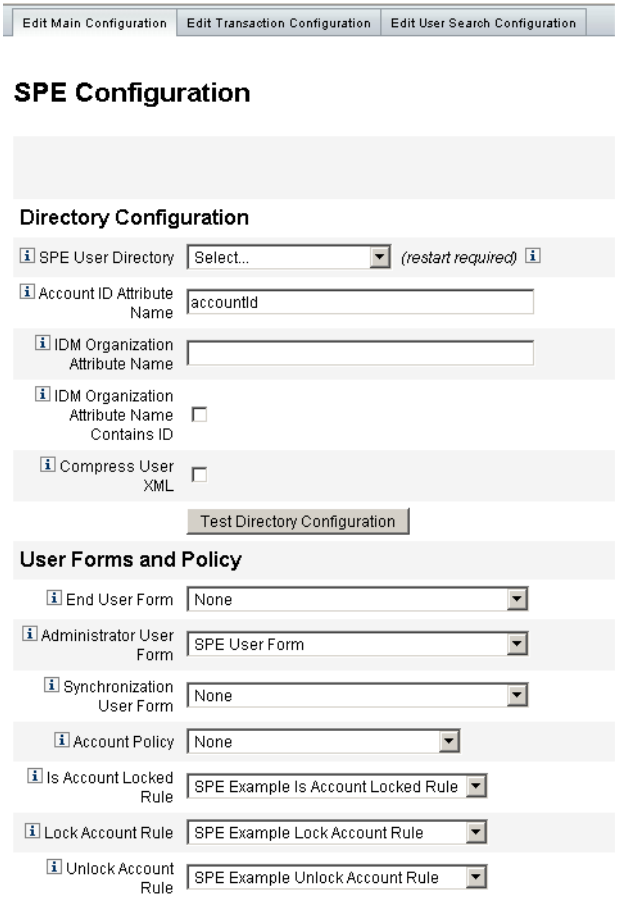
1. Configurator 特権で Identity Manager にログインします。
2. メニューバーの**「サービスプロバイダ」**をクリックします。
3. **「メイン設定の編集」**をクリックします。**「SPE 設定」**ページが表示されます。「SPE 設定」ページ内の次の各エリアで、必要に応じて情報を入力または選択します。
   - ディレクトリ設定
   - ユーザーフォームとポリシー
   - トランザクションデータベース
   - 追跡イベント設定
   - 同期アカウントインデックス
   - コールアウト設定

ディレクトリ設定

「ディレクトリ設定」エリアでは、LDAP ディレクトリの設定情報を入力し、サービスプロバイダユーザーの Identity Manager 属性を指定します。

図 13-1 に、「SPE 設定」ページのこのエリアと、次の節で説明する「ユーザーフォームとポリシー」エリアを示します。

図 13-1　サービスプロバイダ (SPE) 設定 (ディレクトリ、ユーザーフォームとポリシー)



1. **「SPE ユーザーディレクトリ」**をリストから選択します。

   すべての Service Provider ユーザーデータが格納されている LDAP ディレクトリリソースを選択します。

2. **「アカウントアイデンティティー属性名」**を入力します。

これは、一意の短い識別子を含む LDAP アカウント属性の名前です。これは API を通じた認証およびアカウントアクセスのためのユーザー名と見なされます。属性名をスキーママップで定義する必要があります。

3. **「IDM 組織の属性名」**を指定します。

   このオプションには、Identity Manager 内で LDAP アカウントが所属する組織の名前または ID を含む LDAP アカウント属性の名前を指定します。LDAP アカウントの委任管理に使用します。属性名は LDAP リソーススキーママップ内に存在する必要があり、Identity Manager システムの属性名 (スキーママップの左側の名前) になります。

注 組織認証による委任管理を有効にする場合は、「Identity Manager 組織の属性名」を指定し、さらに、必要に応じて「IDM 組織の属性名が ID を含む」を指定してください。

4. **「IDM 組織の属性名が ID を含む」**を選択する場合は、このオプションを有効にします。

   LDAP アカウントが所属する Identity Manager 組織を参照する LDAP リソース属性に、Identity Manager 組織の名前ではなく ID が含まれている場合、このオプションを選択します。

5. **「ユーザー XML の圧縮」**を選択する場合は、このオプションを有効にします。

   このオプションは、ユーザー XML を圧縮してディレクトリに保存する場合に選択します。

6. **「ディレクトリ設定のテスト」**をクリックして、設定の入力を検証します。

注 必要に応じて、**「ディレクトリ設定」**、**「トランザクション設定」**、および **「監査設定」**をテストできます。3 つの設定をすべてテストするには、3 つのテスト設定ボタンをすべてクリックします。

ユーザーフォームとポリシー

「ユーザーフォームとポリシー」エリアでは、前の図 13-1 に示されているように、サービスプロバイダユーザー管理に使用するフォームとポリシーを指定します。

1. **「エンドユーザーフォーム」**をリストから選択します。

   このフォームは、Delegated Administrator ページ以外のすべての場所で、同期中に使用されます。**「なし」**を選択した場合、デフォルトのユーザーフォームは使用されません。

2. **「管理者ユーザーフォーム」**をリストから選択します。

これは、管理者コンテキストで使用されるデフォルトのユーザーフォームです。これには、Service Provider アカウント編集ページが含まれます。**「なし」**を選択した場合、デフォルトのユーザーフォームは使用されません。

注　「管理者ユーザーフォーム」を選択しなかった場合、管理者は Identity Manager で Service Provider ユーザーを作成または編集できません。

---

3. **「同期ユーザーフォーム」**をリストから選択します。

   Service Provider の同期を実行するリソースにフォームが指定されていない場合、「同期ユーザーフォーム」で指定したフォームがデフォルトのフォームとして使用されます。リソースの同期ポリシーに入力フォームが指定されている場合は、そのフォームが代わりに使用されます。リソースは通常さまざまな同期入力フォームを必要とします。この場合、リストからフォームを選択する代わりに、リソースごとに同期ユーザーフォームを設定するようにしてください。

4. **「アカウントポリシー」**をリストから選択します。

   選択肢には、「設定」>「ポリシー」で定義されたアイデンティティーシステムのアカウントポリシーが含まれます。

5. **「アカウントのロックを判断する規則」**をリストから選択します。

   アカウントがロックされているかどうかを判断するために、Service Provider ユーザービューで実行する規則を選択します。

6. **「アカウントをロックする規則」**を選択します。

   属性を設定する Service Provider ユーザービューでアカウントのロックを実行する規則を選択します。

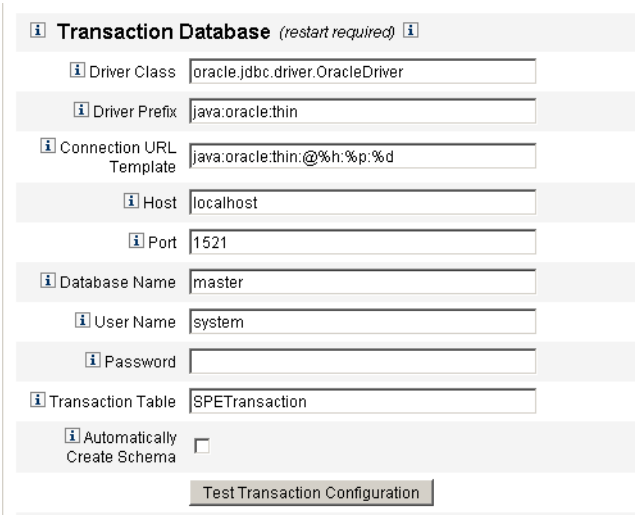
7. **「アカウントをロック解除する規則」**を選択します。

   属性を設定する Service Provider ユーザービューでアカウントのロック解除を実行する規則を選択します。

トランザクションデータベース

「SPE 設定」ページのこのエリアでは、図 13-2 に示すように、トランザクションデータベースの設定を行います。これらのオプションは、JDBC トランザクション持続ストアを使用する場合にのみ必要です。いずれかの値を変更した場合、変更を適用するにはサーバーを再起動する必要があります。

図 13-2　サービスプロバイダの設定 (トランザクションデータベース)



1. 次のデータベース情報を入力します。
   - **「ドライバクラス」** - JDBC ドライバクラス名を指定します。
   - **「ドライバプレフィックス」** - このフィールドは省略可能です。指定した場合、新しいドライバを登録する前に JDBC DriverManager に問い合わせが行われます。
   - **「接続 URL テンプレート」** - このフィールドは省略可能です。指定した場合、新しいドライバを登録する前に JDBC DriverManager に問い合わせが行われます。
   - **「ホスト」** ― データベースが実行されているホストの名前を入力します。
   - **「ポート」** ― データベースサーバーがリスニング中のポート番号を入力します。
   - **「データベース名」** - 使用するデータベースの名前を入力します。
   - **「ユーザー名」** - 選択したデータベースのトランザクションテーブルおよび監査テーブルの行を読み取り、更新、および削除する権限を持ったデータベースユーザーの ID を入力します。
   - **「パスワード」** - データベースユーザーパスワードを入力します。
   - **「トランザクションテーブル」** - 選択したデータベースで、保留中のトランザクションの保存に使用するテーブルの名前を入力します。
2. テーブルのスキーマを Identity Manager サーバーで自動的に作成する場合は、**「スキーマの自動作成」** オプションを有効にします。

   本稼働システムではこのオプションを無効にします。本稼働システムでは、`web/samples` にあるサンプルデータベース初期化スクリプトをカスタマイズします。

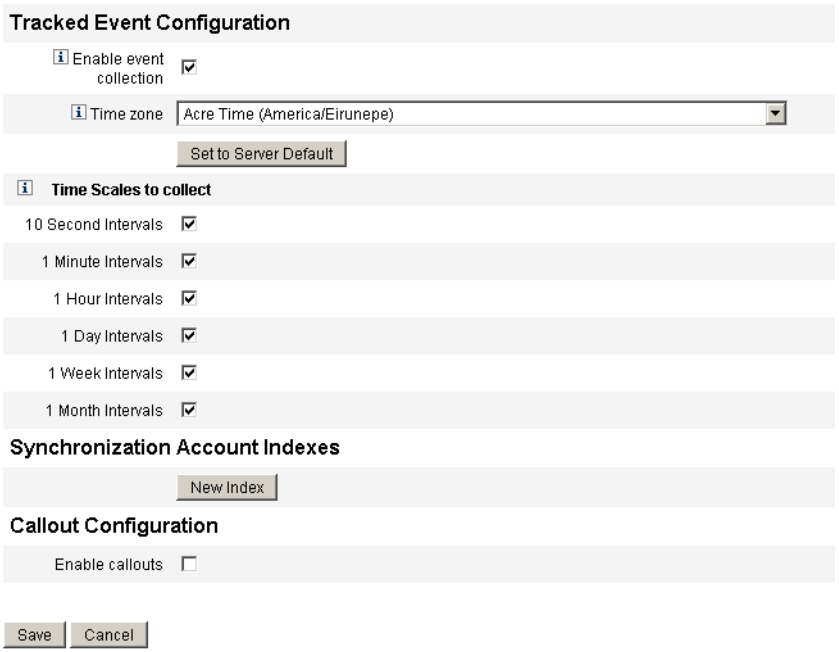
3. 必要に応じて、「**トランザクション設定のテスト**」をクリックしてエントリを検証します。

サービスプロバイダの設定ページの次のエリアに進み、追跡するイベントを設定します。

追跡イベント設定

イベント収集を有効にすると、リアルタイムで統計を追跡して、期待されるレベルまたは合意を得たレベルのサービスの維持に役立てることができます。図 13-3 に示すように、イベント収集はデフォルトで有効になっています。「**イベント収集の有効化**」チェックボックスの選択を解除すると、収集は無効になります。

図 13-3 サービスプロバイダの設定 (追跡イベント、アカウントインデックス、およびコールアウトの設定)



次の手順に従って、タイムゾーンを設定し、サービスプロバイダの追跡イベントの収集間隔を指定します。

1. 「**タイムゾーン**」をリストから選択します。

   追跡イベントの記録時に使用するタイムゾーンを選択します。サーバーで設定されているタイムゾーンを使用する場合は、「**サーバーのデフォルトに設定**」を選択します。

2. **「収集するタイムスケール」**のオプションを選択します。

   10 秒ごと、1 分ごと、1 時間ごと、1 日ごと、1 週間ごと、および 1 か月ごとの間隔で収集が行われます。収集を行いたくない間隔があれば、その間隔を無効にします。

同期アカウントインデックス

Service Provider 実装で ActiveSync リソースを使用する場合、リソースが送信するイベントが Service Provider ディレクトリ内のユーザーに正しく関連付けられるように、**「アカウントインデックス」**を定義する必要がある場合があります。

デフォルトでは、ディレクトリ内の accountId 属性と一致する accountId 属性の値をリソースイベントに含める必要があります。一部のリソースでは、常に accountId が送信されるわけではありません。たとえば、Active Directory からの削除イベントには、Active Directory が生成したアカウント GUID のみが含まれます。

accountId 属性が含まれないリソースには、次のいずれかの属性の値が含まれている必要があります。

- guid - 通常、この属性にはシステムが生成する一意の識別子が含まれます。
- identity - 通常、この属性は LDAP リソース以外のすべてのリソースの accountId と同じです。identity にはオブジェクトの完全 DN が含まれます。

guid または identity を使用して関連付ける必要がある場合は、これらの属性のアカウントインデックスを定義する必要があります。インデックスは、リソース固有のアイデンティティーの保存に使用される可能性のある 1 つ以上のディレクトリユーザー属性を抜粋したものです。identity がディレクトリに保存されると、検索フィルタでそれらを使用して、同期イベントと関連付けることができます。

アカウントインデックスを定義するには、まず、同期に使用するリソースと、そのうちどれにインデックスが必要かを判断します。次に、Service Provider ディレクトリのリソース定義を編集し、各 ActiveSync リソースの GUID または identity 属性のスキーママップに属性を追加します。たとえば、Active Directory から同期する場合は、manager などの未使用のディレクトリ属性にマップされた AD-GUID という名前の属性を定義します。

Service Provider リソースのすべてのインデックス属性を定義したら、次の操作を行います。

1. 設定ページの「同期アカウントインデックス」エリアで、**「新しいインデックス」**ボタンをクリックします。

   フォームが展開され、リソース選択フィールドと 2 つの属性選択フィールドが表示されます。属性選択フィールドは、リソースが選択されるまでは空のままです。

2. **「リソース」**をリストから選択します。

これで、選択したリソースのスキーママップに定義された値が属性フィールドに表示されます。

3. **「GUID 属性」**または**「完全アイデンティティー属性」**のどちらかで、適切なインデックス属性を選択します。

   通常は両方を設定する必要はありません。両方を設定すると、最初に GUID、次に完全 ID を使用して関連付けが行われます。

4. ほかのリソースのインデックス属性を定義する場合は、**「新しいインデックス」**を再度クリックします。

5. インデックスを削除する場合は、**「リソース」**選択フィールドの右にある**「削除」**ボタンをクリックします。

インデックスを削除すると、設定からインデックスが削除されるだけあり、現在インデックス属性に保存されている値を持つ既存のディレクトリユーザーは一切変更されません。

注 インデックスを削除すると、設定からインデックスが削除されるだけあり、現在インデックス属性に保存されている値を持つ既存のディレクトリユーザーは一切変更されません。

コールアウト設定

コールアウトを有効にする場合は、「コールアウト設定」エリアでこのオプションを選択します。コールアウトを有効にすると、コールアウトマッピングが表示され、一覧表示されたトランザクションタイプごとに操作前および操作後のオプションを選択できるようになります。

デフォルトでは、操作前と操作後のオプションは「なし」に設定されます。

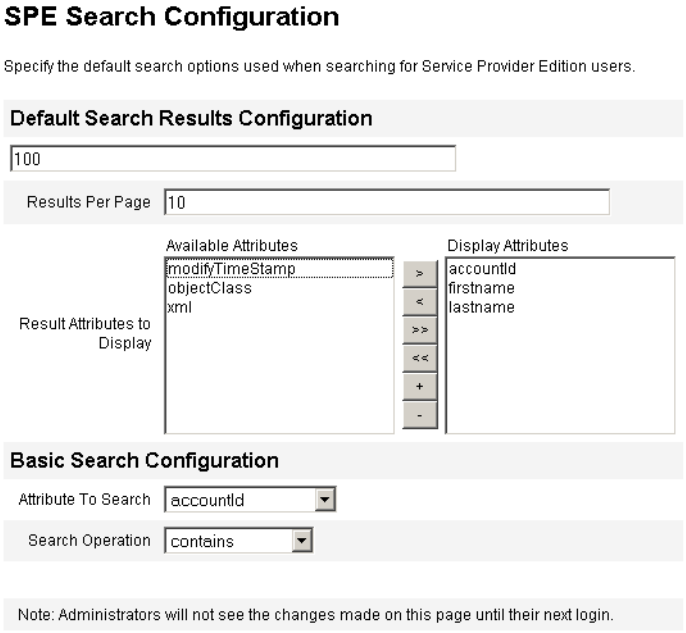
操作後のコールアウトを指定する場合、操作後のコールアウト処理が完了するまでトランザクションが待機するように指定するには、**「操作後コールアウトを待機」**オプションを指定します。この設定により、操作後のコールアウトが正常に完了したあとにのみ従属トランザクションが実行されます。

注 「SPE 設定」ページですべてのエリアの選択が完了したら、**「保存」**をクリックして設定を完了します。

ユーザー検索設定の編集

このページでは、図 13-4 に示すように、委任された管理者が「サービスプロバイダユーザーの管理」ページで実行する検索に関するデフォルトの検索設定を指定します。このデフォルト設定は、「サービスプロバイダユーザーの管理」ページのすべてのユーザーに適用されますが、セッションごとに別の設定を適用することもできます。

図 13-4　検索設定



サービスプロバイダユーザーを検索するためのデフォルトの検索設定を指定するには、次の手順に従います。

1. メニューバーの「**サービスプロバイダ**」をクリックします。
2. 「**ユーザー検索設定の編集**」をクリックします。
3. 「**返される結果の最大数**」に数値を入力します (デフォルトは 100)。
4. 「**ページあたりの結果数**」に数値を入力します (デフォルトは 10)。
5. 「**表示する結果属性**」の横にある「**利用可能な属性**」を、矢印キーを使用して選択します。
6. 「**検索する属性**」をリストから選択します。
7. 「**検索操作**」をリストから選択します。
8. 「**保存**」をクリックします。

注	検索設定に加えた変更は、ログオフして再度ログオンするまで有効になりません。 SPE ディレクトリが設定されていない場合、これらの設定オブジェクトは使用できません。

トランザクション管理

トランザクションは、新しいユーザーの作成や新しいリソースの割り当てなど、単一のプロビジョニング操作をカプセル化します。リソースを使用できないときにこれらのトランザクションを終了させるため、トランザクションがトランザクション持続ストアに書き込まれます。

この節の以下のトピックでは、サービスプロバイダトランザクションの管理手順について説明します。

- デフォルトのトランザクション実行オプションの設定
- トランザクション持続ストアの設定
- トランザクション処理の詳細設定
- トランザクションの監視

デフォルトのトランザクション実行オプションの設定

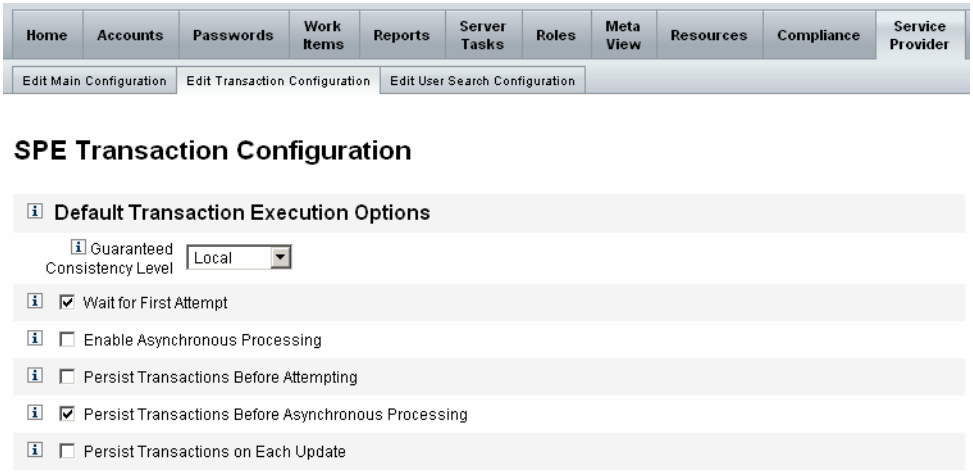
これらのオプションは、同期 / 非同期処理などのトランザクションの実行方式や、トランザクション持続ストアでの持続期間を制御します。オプションは IDMXUser ビューで、または IDMXUser の処理に使用されるフォームを通じて上書きできます。詳細については、『Identity Manager SPE Deployment』を参照してください。

サービスプロバイダトランザクションを設定するには、次の手順に従います。

1. **「サービスプロバイダ」>「トランザクション設定の編集」をクリックします。**
   「SPE トランザクションの設定」ページが表示されます。

   図 13-5 に、「デフォルトのトランザクション実行オプション」エリアを示します。

図 13-5　　トランザクションの設定



2. **「保証される整合性レベル」**で次のオプションのいずれかを選択して、ユーザー更新のトランザクション整合性レベルを指定します。
   - **「なし」**- ユーザーのリソース更新の整合性は保証されません。
   - **「ローカル」**- 同じサーバーで処理されているユーザーのリソース更新の整合性が保証されます。
   - **「完全」**- すべてのサーバーにわたって、ユーザーのすべてのリソース更新の整合性が保証されます。このオプションは、すべてのトランザクションがトランザクションの試行まで、または非同期処理まで持続していることを必要とします。
3. 次のデフォルトのトランザクション実行オプションのうち、有効にするものを選択します。
   - **「最初の試行を待機」**- IDMXUser ビューオブジェクトのチェックイン時に、コントロールを呼び出し側に返す方式を指示します。このオプションを有効にした場合、プロビジョニングトランザクションで 1 回の試行が終了するまでチェックイン操作はブロックされます。非同期処理を無効にした場合、トランザクションは成功するか、コントロールが返される場合は失敗します。非同期処理を有効にした場合、トランザクションはバックグラウンドで継続的に再試行されます。オプションを無効にした場合、チェックイン操作から呼び出し側にコントロールが返されたあとで、プロビジョニングトランザクションが試行されます。このオプションを有効にすることを検討してください。
   - **「非同期処理の有効化」**- このオプションは、チェックイン呼び出しにより結果が返されたあともプロビジョニングトランザクションの処理を続けるかどうかを制御します。

非同期処理を有効にすると、システムはトランザクションを再試行できるようになります。さらに、「トランザクション処理の詳細設定」で設定したワークスレッドを非同期で実行できるようになることで、スループットも向上します。このオプションを選択する場合、プロビジョニングされるか、または同期入力フォームによって更新されるリソースの再試行間隔と試行を設定するようにしてください。

「非同期処理の有効化」を選択した場合は、**「再試行タイムアウト」**の値を入力します。これは、失敗したプロビジョニングトランザクションがサーバーで再試行される期間の上限をミリ秒で表した値です。この設定により、サービスプロバイダユーザー LDAP ディレクトリなど、個々のリソースの再試行設定が補足されます。たとえば、リソースの再試行制限に達する前にこの制限に達した場合、トランザクションは終了します。負の値の場合、再試行の回数は個々のリソースの設定のみにより制限されます。

- **「試行前の持続的トランザクション」-** 有効にした場合、プロビジョニングトランザクションは試行される前に、トランザクション持続ストアに書き込まれます。このオプションを有効にすると、ほとんどのプロビジョニングトランザクションは最初の試行で成功するため、不要なオーバーヘッドが生じる場合があります。**「最初の試行を待機」**オプションを無効にしている場合を除き、このオプションは無効にすることを検討してください。「完全」整合性レベルが選択されている場合は、このオプションを使用できません。
- **「非同期処理の前の持続的トランザクション」(** デフォルト **) -** 有効にした場合、プロビジョニングトランザクションは非同期に処理される前に、トランザクション持続ストアに書き込まれます。「最初の試行を待機」オプションを有効にしている場合、再試行が必要なトランザクションは、呼び出し側にコントロールが返されるまで持続します。「最初の試行を待機」オプションを無効にした場合、トランザクションは常に、試行されるまで持続します。このオプションは有効にすることを推奨します。「完全」整合性レベルが選択されている場合は、このオプションを使用できません。
- **「各更新時の持続的トランザクション」-** 有効にした場合、再試行のあともプロビジョニングトランザクションが持続します。これにより、**「トランザクションの検索」**ページから検索できるトランザクション持続ストアは常に最新になるため、問題の分離に役に立つ場合があります。

トランザクション持続ストアの設定

「SPE トランザクションの設定」ページのこれらのオプションは、トランザクション持続ストアに適用されます。ストア内で表示する問い合わせ可能な追加属性以外に、ストアのタイプも設定できます。次の図を参照してください。

図 13-6　SPE トランザクション持続ストアの設定

これらのオプションを設定するには、次の手順に従います。

1. 目的の**「トランザクション持続ストアタイプ」**をリストから選択します。

   「データベース」オプションを選択した場合、Service Provider 設定のメインページで設定された RDBMS がプロビジョニングトランザクションの持続に使用されます。これによって、サーバーを再起動した後も、再試行の必要なトランザクションが破棄されません。このオプションを選択する場合、サービスプロバイダ設定のメインページで RDBMS を設定する必要があります。**「メモリーベースのシミュレート」**オプションを選択した場合、再試行の必要なトランザクションはメモリー内にのみ格納され、サーバーを再起動すると破棄されます。本稼働環境では、**「データベース」**オプションを有効にします。

注　メモリーベースのトランザクション持続ストアは、クラスタ環境での使用には適しません。

「トランザクション持続ストアタイプ」を変更した場合、変更を適用するには、実行中のすべての Identity Manager インスタンスを再起動する必要があります。

2. 必要に応じて、**「照会可能なユーザー属性のカスタマイズ」**を入力します。

トランザクション概要内で表示される IDMXUser オブジェクトの追加属性を選択します。これらの属性は、検索トランザクションページから問い合わせ可能であり、検索結果に表示されます。次のフィールドがあります。

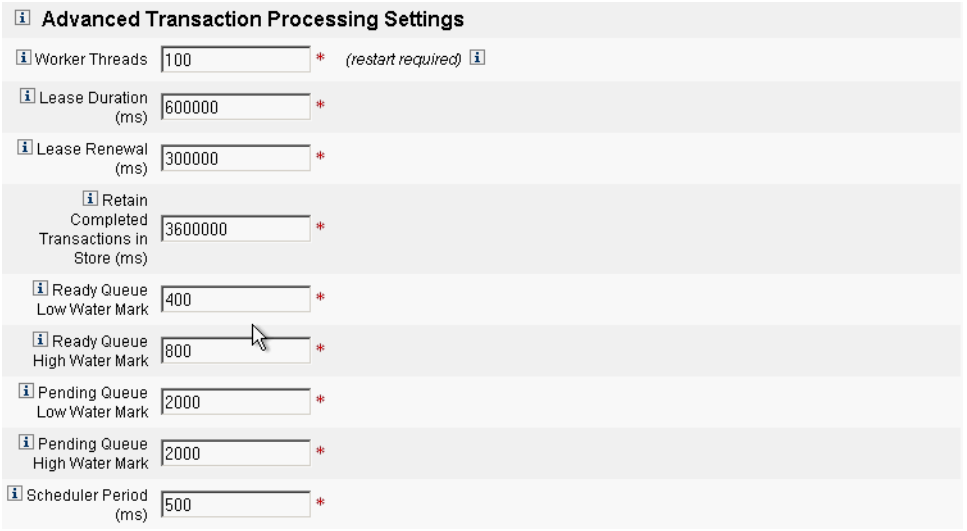
- **「ユーザーパス表現」** - IDMXUser オブジェクトのパス表現を入力します。
- **「表示名」** - パス表現に対応する表示名を選択します。この表示名はトランザクション検索ページに表示されます。

トランザクション処理の詳細設定

これらの詳細なオプションは、トランザクションマネージャーの内部動作を制御します。パフォーマンス分析で最適ではないと示されない限り、指定されたデフォルトを変更できません。すべての入力が必要です。

図 13-5 に、「トランザクション設定の編集」ページの「トランザクション処理の詳細設定」エリアを示します。

図 13-7 トランザクション処理の詳細設定



1. **「ワークスレッド」に、必要な数値を入力します (デフォルトは 100)。**

   これはトランザクションの処理に使用されるスレッド数です。この値は同時に処理されるトランザクション数を制限します。これらのスレッドは起動時に静的に割り当てられます。

注 「ワークスレッド」を変更した場合、変更を適用するには、実行中のすべての Identity Manager インスタンスを再起動する必要があります。

2. 「リース時間 (ms)」に、必要な時間を入力します (デフォルトは 600000)。

   これは、再試行中のトランザクションをサーバーでロックする時間を制御します。リースは必要に応じて更新されます。ただし、サーバーが完全にシャットダウンしていない場合、オリジナルサーバーのリース時間が終了するまで、ほかのサーバーはトランザクションをロックできません。最低値は 1 分です。小さい値を設定すると、トランザクション持続ストアの負荷に影響する場合があります。

3. 「リース更新 (ms)」に、必要な時間を入力します (デフォルトは 300000)。

   これは、ロックされたトランザクションのリースの更新時期を制御します。リース期間の残りがこのミリ秒数になった時点で更新されます。

4. 「終了トランザクションのストア内での保持時間 (ms)」に、必要な時間を入力します (デフォルトは 360000)。

   トランザクション持続ストアから終了トランザクションを削除するまでの待機時間 (ミリ秒) です。トランザクションの直後に持続を設定している場合を除き、トランザクション持続ストアには終了したトランザクションは格納されません。

5. 「実行可能キュー最低水準点」に、必要な数値を入力します (デフォルトは 400)。

   トランザクションスケジューラの実行可能なトランザクションキューがこの制限を下回ると、最高水準制限までキューに実行可能なトランザクションが補充されます。

6. 「実行可能キュー最高水準点」に、必要な数値を入力します (デフォルトは 800)。

   トランザクションスケジューラの実行可能なトランザクションキューが最低水準点よりも下回ると、この制限まで、キューに実行可能なトランザクションが補充されます。

7. 「保留キュー最低水準点」に、必要な数値を入力します (デフォルトは 2000)。

   トランザクションスケジューラの保留中のキューが、失敗し再試行を保留しているトランザクションを保持しています。キューのサイズが最高水準点を超える場合、最低水準点を超えるすべてのトランザクションはトランザクション持続ストアにフラッシュされます。

8. 「保留キュー最高水準点」に、必要な数値を入力します (デフォルトは 2000)。

   トランザクションスケジューラの保留中のキューが、失敗し再試行を保留しているトランザクションを保持しています。キューのサイズが最高水準点を超える場合、最低水準点を超えるすべてのトランザクションはトランザクション持続ストアにフラッシュされます。

9. 「スケジューラ間隔 (ms)」に、必要な数値を入力します (デフォルトは 500)。

これは、トランザクションスケジューラの実行間隔です。トランザクションスケジューラは実行されると、実行可能なトランザクションを保留中のキューから実行可能キューに移動し、トランザクション持続ストアに対して、トランザクションの持続などの別の定期的な作業を実行します。

10. **「保存」**をクリックして、設定を受け入れます。

トランザクションの監視

サービスプロバイダトランザクションは、トランザクション持続ストアに書き込まれます。トランザクション持続ストアのトランザクションを検索して、トランザクションのステータスを表示できます。

注 「トランザクション設定の編集」ページを使用すると (「トランザクション管理」を参照)、管理者はいつトランザクションを保管するかを制御できます。たとえば、トランザクションをただちに保管できます (最初の試行前であっても)。

「トランザクションの検索」ページで、検索条件を指定してトランザクションをフィルタリングし、ユーザー、タイプ、ステータス、トランザクション ID、現在の状態、成功か失敗かなど、トランザクションイベントに関する特定の条件に基づいて表示できます。ここには、すでに完了しているトランザクションとともに再試行中のトランザクションが含まれます。完了していないトランザクションは、それ以上試行されないようにキャンセルできます。

トランザクションを検索するには、次を実行します。

1. Identity Manager にログインします。
2. メニューバーの**「サーバータスク」**をクリックします。
3. **「サービスプロバイダトランザクション」**をクリックします。

   「SPE トランザクション検索」ページが表示され、そこで検索条件を指定できます。

注 検索では、下で選択したすべての条件に一致するトランザクションのみが返されます。これは、**「アカウント」>「ユーザーの検索」**ページと類似しています。

---

4. 必要に応じ、**「ユーザー名」**を選択します。

   入力した **accountId** を持つユーザーのみに適用されるトランザクションを検索できます。

注	Service Provider トランザクション設定ページで「照会可能なユーザー属性のカスタマイズ」を設定している場合は、それらがここに表示されます。たとえば、照会可能なユーザー属性のカスタマイズとして姓またはフルネームが設定されている場合、これらに基づいて検索することを選択できます。

5. 必要に応じて、**「タイプ」**の検索を選択します。

   選択したタイプのトランザクションを検索できます。

6. 必要に応じて、**「状態」**の検索を選択します。

   選択した次の状態のトランザクションを検索できます。

   - **「未試行」**トランザクションは、まだ試行されていません。
   - **「再試行保留中」**トランザクションは、1 回以上試行されましたが、1 つ以上のエラーが見つかり、個々のリソースに設定された再試行制限まで再試行がスケジュールされています。
   - **「成功」**トランザクションは、正常に完了しました。
   - **「失敗」**トランザクションは、1 つ以上失敗して完了しました。

7. 必要に応じ、**「試行」**での検索を選択します。

   試行された回数に基づいて、トランザクションを検索できます。失敗したトランザクションは、個々のリソースに設定された再試行制限まで再試行されます。

8. 必要に応じ、**「送信時間」**での検索を選択します。

   時間、分、日の単位でトランザクションが最初に送信された時間に基づいて、トランザクションを検索できます。

9. 必要に応じ、**「終了時間」**での検索を選択します。

   時間、分、日の単位でトランザクションが完了した時間に基づいて、トランザクションを検索できます。

10. 必要に応じ、**「キャンセルステータス」**での検索を選択します。

    トランザクションがキャンセルされているかどうかに基づいて、トランザクションを検索できます。

11. 必要に応じ、**「トランザクション ID」**での検索を選択します。

    一意のトランザクション ID に基づいてトランザクションを検索できます。このオプションを使用すると、入力した ID 値に基づいてトランザクションが検索されます。この ID は、すべての監査ログレコードに表示されます。

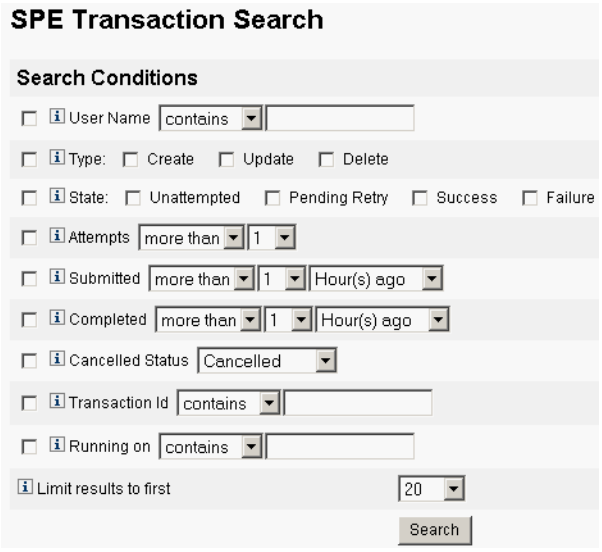
12. 必要に応じ、**「SPE サーバー名」**での検索を選択します。

実行中の Service Provider サーバーに基づいてトランザクションを検索できます。サーバーの ID は、`Waveset.properties` ファイルで上書きされている場合を除き、マシン名に基づきます。

13. 検索結果をリストから選択したエントリ数までに制限します。

    指定された制限までの結果のみ返されます。制限数以上の結果が存在するかどうかについては示されません。

図 13-8　　トランザクションの検索



14. **「検索」**をクリックします。

    検索結果が表示されます。

15. 必要に応じ、結果ページの最下部にある**「一致したすべてのトランザクションをダウンロードします」**をクリックします。結果は XML 形式のファイルに保存されます。

注　　検索結果に返されたトランザクションをキャンセルすることができます。結果テーブルのトランザクションを選択し、**「選択内容のキャンセル」**をクリックします。完了している、またはすでにキャンセルされているトランザクションはキャンセルできません。

委任された管理

サービスプロバイダユーザーの委任された管理を有効にするには、Identity Manager 管理者ロールまたは組織ベース認証モデルを使用します。

組織認証による委任

Identity Manager では、デフォルトで、組織ベース認証モデルを使用して管理作業を委任できます。組織ベース認証モデルで委任される管理者を作成するときは、次のことに留意してください。

- サービスプロバイダ管理者は、特定の機能および管理する組織を持つ Identity Manager ユーザーです。
- ユーザーの組織属性の値は、Identity Manager 組織名かオブジェクト ID のどちらかになります。どちらにするかは、Identity Manager メイン設定画面の **Identity Manager「IDM 組織の属性名が ID を含む」**フィールドの設定によって決まります。
- Identity Manager 階層を作成し、その階層に組織を配置して、それらの組織の管理を委任することができます。組織の単純名ではなく、組織に固有の識別情報を使用します。
- サービスプロバイダユーザーの組織はディレクトリサーバーのユーザー属性から取得されます。
    - ディレクトリサーバーリソースのスキーママップに属性を設定する必要があります。
    - 属性の比較は、管理者が管理する組織リストとの「完全一致」によって行われます。ディレクトリに格納される値は、階層全体ではなく、組織名と一致する必要があります。管理者が `Top:orgA:sub1` を管理する場合、`sub1` は Service Provider ユーザーの組織属性に格納されている値でなければなりません。
    - 属性が設定されていない場合、または Identity Manager 組織と一致しない場合、その Service Provider ユーザーは最上位 (Top) 組織のメンバーとみなされます。このため、Service Provider Edition 管理者は、それらのユーザーを管理するために、`Top` 内で Service Provider ユーザー機能を持っていることが必要です。
- 属性の設定によって、Service Provider 管理者による検索の範囲が決まります。
- 委任される管理者のアカウントを作成するには、まず Identity Manager 管理者を作成し、次に Service Provider Administrator 機能を追加します。ユーザーに割り当てることができる Service Provider Edition タスクに固有の機能があります (**「ユーザーの編集」**ページの**「セキュリティー」**タブ)。管理する組織は、管理者が変更できる Service Provider ユーザーを指定します。Service Provider ユーザーが使用できるリソースは、すべての Identity Manager 管理者も使用できます。

注 Identity Manager の委任された管理の詳細については、第 5 章「管理」の「委任された管理」を参照してください。

管理者ロール割り当てによる委任

サービスプロバイダユーザーに細かい機能や管理範囲を付与する場合は、サービスプロバイダユーザー管理者ロールを使用します。1 人以上の Identity Manager ユーザーまたはサービスプロバイダユーザーへの管理者ロールの割り当てを、ログイン時に動的に行うように設定できます。

管理者ロールを割り当てられたユーザーに与える機能 (「サービスプロバイダのユーザーの作成」など) を指定する規則を定義して管理者ロールに割り当てることができます。

サービスプロバイダユーザーの管理者ロール委任を使用するには、Identity Manager システム設定でそれを有効にする必要があります。

管理者ロール割り当てによる委任を有効にする場合、「SPE 設定」の「IDM 組織の属性名」は必要ありません。

サービスプロバイダ管理者ロール委任の有効化

サービスプロバイダ管理者ロール委任 (SPE 委任管理) を有効にするには、Identity Manager デバッグページを使用して、System Configuration オブジェクトで次のプロパティーを `true` に設定します。

`security.authz.external.`*app name*`.`*object type*

app name は Identity Manager アプリケーション (管理者インタフェースなど)、*object type* は `Service Provider Users` です。

このプロパティーは、Identity Manager アプリケーション (管理者インタフェースやユーザーインタフェースなど) 単位およびオブジェクトタイプ単位で有効にすることができます。現在サポートされているオブジェクトタイプは `Service Provider Users` のみです。デフォルト値は `false` です。

たとえば、Identity Manager 管理者の SPE 委任管理を有効にするには、System Configuration オブジェクトで次の属性を "true" に設定します。

```
security.authz.external.Administrator Interface.Service Provider
Users
```

特定の Identity Manager またはサービスプロバイダアプリケーションで SPE 委任管理を無効に (false に設定) した場合は、組織ベース認証モデルが使用されます。

SPE 委任管理を有効にした場合は、実行された認証規則の数および時間に関する情報が追跡イベントによって取得されます。それらの統計情報はダッシュボードで表示できます。

サービスプロバイダユーザー管理者ロールの設定

サービスプロバイダユーザー管理者ロールを設定するには、次の手順に従って、管理者ロールを作成し、管理範囲、機能、および割り当てるユーザーを指定します。

注 サービスプロバイダユーザー管理者ロールを作成する前に、その管理者ロールの検索コンテキスト、検索フィルタ、検索後のフィルタ、機能、およびユーザー割り当てに関する規則を定義します。これらの規則 (SPEUsersSearchContextRule、SPEUsersSearchFilterRule、SPEUsersAfterSearchFilterRule、CapabilitiesOnSPEUserRule、UserIsAssignedAdminRoleRule、および SPEUserIsAssignedAdminRoleRule) を使用するように、規則の `authType` を指定する必要があります。

サービスプロバイダユーザー管理者ロールのこれらの規則を作成するには、Identity Manager に付属するサンプル規則を使用できます。サンプル規則は Identity Manager インストールディレクトリの `sample/adminRoleRules.xml` にあります。

各環境での規則の作成の詳細については、『Identity Manager SPE Deployment』を参照してください。

1. 「セキュリティー」タブで「管理者ロール」を選択し、**「新規」**をクリックして「管理者ロールの作成」ページを開きます。
2. 管理者ロールの名前を指定し、タイプとして**「サービスプロバイダユーザー」**を選択します。
3. 次の節の説明に従って、「Scope of Control」、「Capabilities」、および「Assign to Service Provider Users」オプションを指定します。

管理範囲の指定

サービスプロバイダユーザー管理者ロールの管理範囲は、特定の Identity Manager 管理者、Identity Manager エンドユーザー、または Identity Mananger サービスプロバイダエンドユーザーが表示できるサービスプロバイダユーザーを指定します。この範囲は、ディレクトリのサービスプロバイダユーザーを一覧表示するようにリクエストされたときに適用されます。

サービスプロバイダユーザー管理者ロールの管理範囲では、以下の設定を 1 つ以上指定できます。

- **「ユーザー検索コンテキスト」**- 検索の開始に規則を使用するかテキスト文字列を使用するかを指定します。

  「なし」を指定した場合、デフォルトの検索コンテキストは、サービスプロバイダユーザーディレクトリとして設定された Identity Mananger リソースで指定されたベースコンテキストになります。

- **「ユーザー検索フィルタ」**- 検索フィルタに規則を適用するかテキスト文字列を適用するかを指定します。

  指定したテキスト文字列、または選択した規則から返されるテキスト文字列は、検索コンテキスト内で、この管理者ロールに割り当てられたユーザーが管理するユーザーセットを表す LDAP 準拠の検索フィルタ文字列になります。指定したフィルタは、ユーザーが指定した検索フィルタと結合されます。検索結果として返されるユーザーには、この管理者ロールに割り当てられたユーザーが一覧表示する権限を与えられていないユーザーが含まれないようにします。

- **「ユーザー検索後に適用されるフィルタ規則」**- ユーザー検索フィルタの適用後に適用する規則を選択します。

  この規則は、サービスプロバイダユーザーディレクトリに対して最初の LDAP 検索が実行されたあとに実行され、検索結果を評価して、リクエスト元のユーザーがアクセスを許可されている識別名 (dn) を決定します。

  このタイプの規則を使用できるのは、あるユーザーをリクエスト元ユーザーの管理範囲に含めるかどうかを LDAP 以外のユーザー属性 (グループメンバーシップなど) を使用して判断する場合や、フィルタでの判断をサービスプロバイダユーザーディレクトリ以外のリポジトリ (Oracle データベースや RACF など) を使用して行う必要がある場合などです。

機能の指定

サービスプロバイダユーザー管理者ロールの機能では、アクセスをリクエストされているサービスプロバイダユーザーに対してリクエスト元のユーザーが持つ機能と権利を指定します。これは、サービスプロバイダユーザーの表示、作成、変更、または削除のリクエストが作成されたときに適用されます。

「Capabilities」タブで、この管理者ロールに適用する「ユーザーごとの機能規則」を選択します。

サービスプロバイダユーザーへの管理者ロールの割り当て

ログイン時の評価で認証ユーザーに管理者ロールを割り当てるかどうかを判断する規則を指定することにより、サービスプロバイダユーザー管理者ロールをサービスプロバイダユーザーに動的に割り当てることができます。

「Assign to Service Provider Users」タブをクリックし、割り当てに適用する規則を選択します。

注

ユーザーへの管理者ロールの動的割り当ては、ログインインタフェース (ユーザーインタフェースや管理者インタフェースなど) ごとに有効にする必要があります。そのためには、次の System Configuration オブジェクトを `true` に設定します。

`security.authz.checkDynamicallyAssignedAdminRolesAtLoginTo.`*`logininterface`*

すべてのインタフェースのデフォルトは `false` です。

サービスプロバイダユーザー管理者ロールの委任

デフォルトで、サービスプロバイダユーザーは、自分に割り当てられたサービスプロバイダユーザー管理者ロールを、自分の管理範囲内のほかのサービスプロバイダユーザーに割り当てる (委任する) ことができます。

実際に、サービスプロバイダユーザーを編集する機能を持つ Identity Manager ユーザーは、自分に割り当てられたサービスプロバイダユーザー管理者ロールを、自分の管理範囲内のサービスプロバイダユーザーに割り当てることができます。

サービスプロバイダユーザー譲渡者ロールに、管理範囲に関係なく譲渡者ロールを割り当てることができる「譲渡者」のリストを含めることもできます。このような直接の割り当てにより、1 人以上の既知のユーザーアカウントが管理者ロールを割り当てることができるようにします。

サービスプロバイダユーザーの管理

この節では、Identity Manager で サービスプロバイダ ユーザーを管理するための手順および説明を示します。この節は次のトピックで構成されています。

- ユーザー組織
- ユーザーとアカウントの作成
- サービスプロバイダユーザーの検索
- アカウントのリンク
- アカウントの削除、割り当て解除、またはリンク解除

ユーザー組織

Service Provider では、ユーザーの属性値によって、そのユーザーが割り当てられる組織が決まります。これは、Service Provider メイン設定の**「Identity Manager 組織の属性名」**フィールドで指定されます (「初期設定」を参照)。ただし、それらの組織名は、ディレクトリサーバーで割り当てられたユーザー属性の値と一致する必要があります。

「Identity Manager 組織の属性名」が定義されている場合は、「ユーザーの作成」または「ユーザーの編集」ページに、使用できる組織の複数選択リストが表示されます。デフォルトでは短い組織名が表示されます。組織の完全なパスが表示されるように SPE ユーザーフォームを変更できます。

どの属性が組織名属性になるかを選択できます。組織名属性は、そのユーザーを検索および管理できる管理者を制約するために Service Provider ユーザー管理ページで使用されます。

注

現在、Service Provider アカウントおよびリソースアカウント用のアカウント ID ポリシーとパスワードポリシーがあります。

「SPE システムアカウントポリシー」は、主要ポリシーテーブルから使用できます。

ユーザーとアカウントの作成

すべてのサービスプロバイダユーザーは、Service Provider ディレクトリ内にアカウントを持つ必要があります。ユーザーがほかのリソースのアカウントを持つ場合、それらのアカウントへのリンクがユーザーのディレクトリエントリに保存されるので、そのユーザーを表示するときに、それらのアカウントに関する情報を表示できます。

注 ユーザーを作成および編集するための Service Provider ユーザーフォームのサンプルが用意されています。このフォームを、実際のサービスプロバイダ環境でのユーザー管理の要件に合わせてカスタマイズしてください。詳細については、『Identity Manager ワークフロー、フォーム、およびビュー』を参照してください。

Service Provider アカウントを作成するには、次の手順に従います。

1. メニューバーの「**アカウント**」をクリックします。
2. 「**サービスプロバイダユーザーの管理**」タブをクリックします。
3. 「**アカウントの作成**」をクリックします。

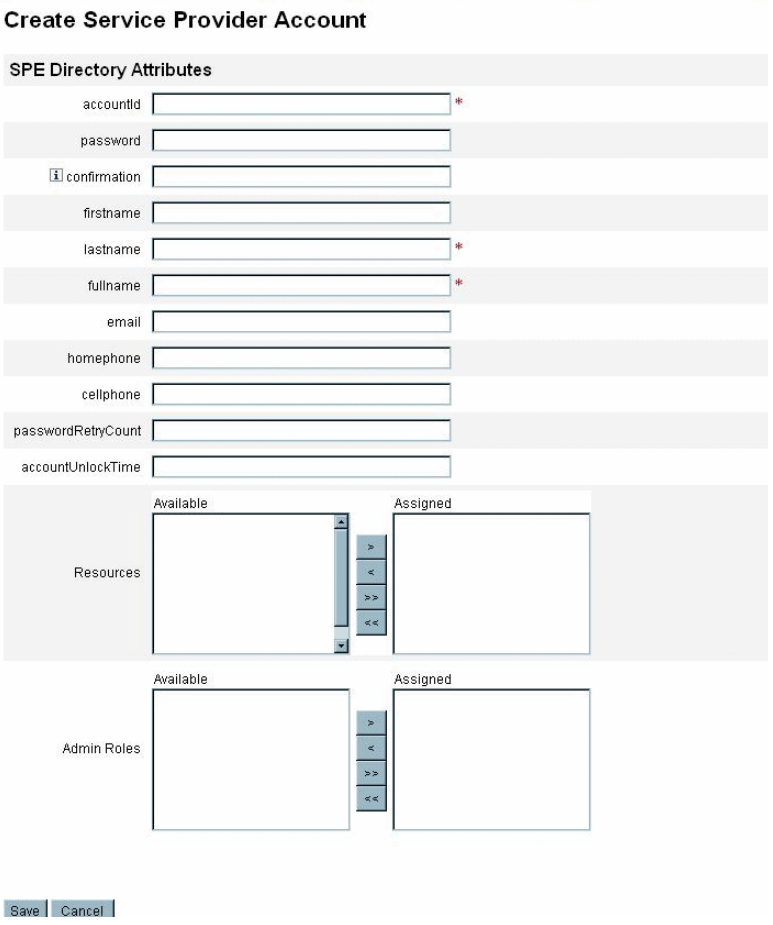
注 デフォルトの Service Provider ユーザーフォームの使用時に表示される実際のフィールドは、Service Provider ディレクトリリソースのアカウント属性テーブル (スキーママップ) に設定された属性によって異なります。また、ユーザー (委任された管理者など) にリソースを割り当てた場合は、そのリソースの属性値を指定するための新しいエリアが追加表示されます。フィールドをカスタマイズすることもできます。

4. 以下の値を必要に応じて入力します。
   - 「**accountid**」(このフィールドは必須)
   - 「**password**」
   - 「**confirmation**」(パスワード確認用)
   - 「**firstname**」(このフィールドは必須)
   - 「**lastname**」(このフィールドは必須)
   - 「**fullname**」
   - 「**email**」
   - 「**home phone**」
   - 「**cell phone**」
   - 「**password retry count**」

- 「**account unlock time**」

5. 矢印キーを使用して「利用可能」リストから目的のリソースを割り当てます。
6. 「**アカウントステータス**」に、アカウントがロックされているかロック解除されているかが表示されます。アカウントをロックまたはロック解除する場合は、このオプションをクリックします。

図 13-9　サービスプロバイダユーザーとアカウントの作成



注 このフォームでは、ディレクトリアカウント (最上位) で定義された属性に基づいて、リソースアカウント属性の値が自動的に設定されます。たとえば、リソースに `firstName` を定義した場合、ディレクトリアカウントの `firstName` の値が設定されます。ただし、この初期設定後、それらの属性の変更はリソースアカウントに伝達されません。必要に応じて、付属のサンプル Service Provider ユーザーフォームをカスタマイズしてください。

7. **「保存」**をクリックしてユーザーアカウントを作成します。

サービスプロバイダユーザーの検索

Service Provider には、ユーザーアカウントの管理に役立つ設定可能な検索機能が含まれています。検索では、組織やその他の要素で定義された範囲内のユーザーのみが返されます。

サービスプロバイダユーザーの基本検索を実行するには、Identity Manager インタフェースの**「アカウント」**エリアで、**「サービスプロバイダユーザーの管理」**をクリックし、検索値を入力して**「検索」**をクリックします。

次のトピックで、サービスプロバイダの検索機能について説明します。

- 詳細検索
- 検索結果
- アカウントの削除、割り当て解除、またはリンク解除
- 検索オプションの設定

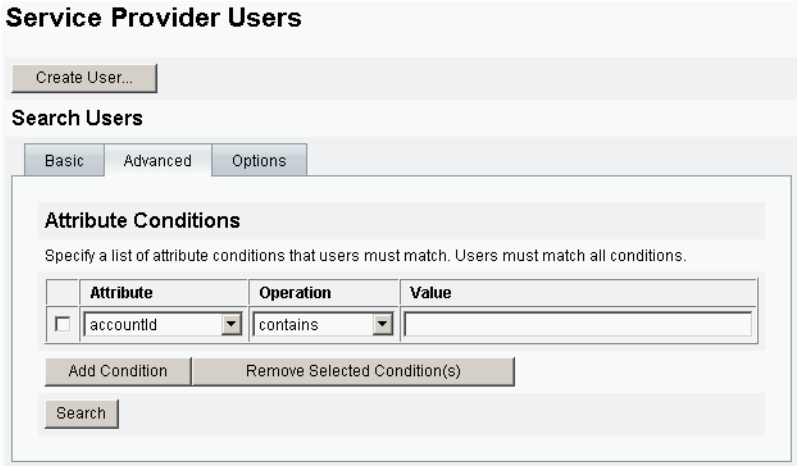
詳細検索

サービスプロバイダユーザーの詳細検索を実行するには、サービスプロバイダユーザーの検索ページで**「詳細」**をクリックし、次のアクションを実行します。

1. 目的の**「属性」**をリストから選択します。
2. 目的の**「操作」**をリストから選択します。

   検索で返されるユーザーをフィルタリングして、指定したすべての条件を満たすユーザーのみが返されるようにするための条件セットを指定しています。
3. 目的の検索値を入力し、**「検索」**をクリックします。

図 13-10　ユーザーの検索



属性条件を追加または削除するには、次のいずれかの操作を行います。

- **「条件の追加」**をクリックし、新しい属性を指定します。
- 項目を選択して、**「選択した条件の削除」**をクリックします。

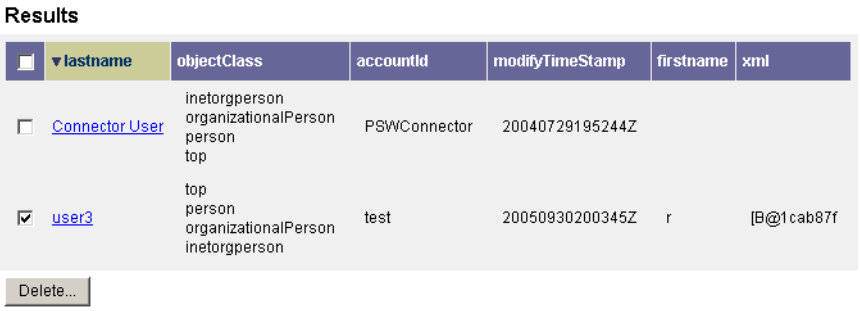
検索結果

図 13-11 に示すように、Service Provider の検索結果はテーブル形式で表示されます。属性の列ヘッダーをクリックすると、結果をその属性で並べ替えることができます。表示される結果は選択した属性によって異なります。

結果の最初のページ、前ページ、次ページ、および最終ページを表示するには、矢印ボタンを使用します。特定のページに移動するには、テキストボックスにページ番号を入力して Enter キーを押します。

ユーザーを編集するには、テーブル内のユーザー名をクリックします。

図 13-11　検索結果の例



検索結果ページで、ユーザーの削除またはリソースアカウントのリンク解除を行うには、1 人以上のユーザーを選択して、**「削除」**ボタンをクリックします。このアクションにより、ユーザーの削除ページが開き、追加のオプションが表示されます (「アカウントの削除、割り当て解除、またはリンク解除」を参照)。

アカウントのリンク

Service Provider は、ユーザーが複数のリソースにアカウントを持つ環境にインストールする場合があります。Service Provider のアカウントリンク機能によって、既存のリソースアカウントを差分方式で Service Provider ユーザーに追加できます。アカウントリンクプロセスは、リンク相関規則、リンク確認規則、リンク検証オプションを定義する Service Provider のリンクポリシーで管理します。

ユーザーアカウントをリンクするには、次の手順に従います。

1. メニューバーで**「リソース」**を選択します。
2. 目的のリソースを選択します。
3. 「リソースアクション」メニューから**「サービスプロバイダリンクポリシーの編集」**を選択します。
4. リンク相関規則を選択します。この規則は、ユーザーが所有する可能性のあるリソースのアカウントを検索します。
5. リンク確認則を選択します。この規則は、リンク相関規則で選択されるアカウントの候補のリストから、リソースアカウントを除外します。

注　リンク相関規則で 1 つだけのアカウントを選択する場合、リンク確認規則は必要ありません。

6. **「リンク検証が必要」**を選択して、ターゲットリソースアカウントを Service Provider ユーザーにリンクします。

アカウントの削除、割り当て解除、またはリンク解除

ユーザーアカウントの削除、割り当て解除、またはリンク解除を行うには、次の手順に従います。

1. メニューバーの**「アカウント」**をクリックします。
2. **「サービスプロバイダユーザーの管理」**をクリックします。
3. 基本検索または詳細検索を実行します。
4. 目的のユーザーを選択します。
5. **「削除」**ボタンをクリックします。
6. 必要に応じて、次のいずれかのグローバルオプションを選択します。
   - **「すべてのリソースアカウントの削除」**

注	リソースを削除した場合、アカウントは削除されますが、リソース割り当てはまだ存在しています。その後ユーザーを更新すると、アカウントが再作成されます。リソースアカウントのリンクは、リソースの削除時に常に解除されます。

   - **「すべてのリソースアカウントの割り当て解除」**

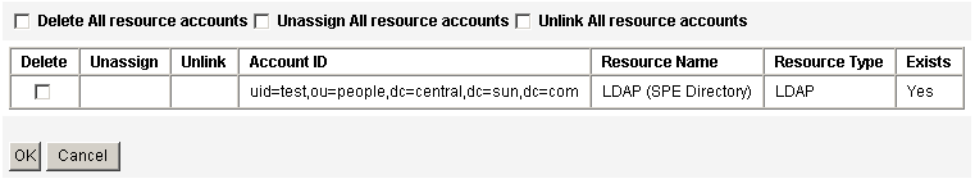
注	リソースを割り当て解除すると、そのリソース割り当てが削除されます。割り当て解除すると、そのリソースアカウントのリンクも解除されます。リソースを割り当て解除しても、リソースアカウントは削除されません。

   - **「すべてのリソースアカウントのリンク解除」**

注	リンクを解除すると、ユーザーとリソースアカウント間のリンクが削除されますが、アカウントは削除されません。リソース割り当ても削除されませんので、その後ユーザーを更新すると、アカウントと再リンクされるか、またはそのリソースの新しいアカウントが作成されます。

7. または、「**削除**」列、「**割り当て解除**」列、または「**リンク解除**」列で、1 つ以上のリソースアカウントに対するアクションを選択します。
8. 目的のユーザーアカウントを選択したら、「**OK**」をクリックします。

図 13-12　　アカウントの削除、割り当て解除、またはリンク解除



検索オプションの設定

サービスプロバイダユーザーの検索オプションを設定するには、次の手順に従います。

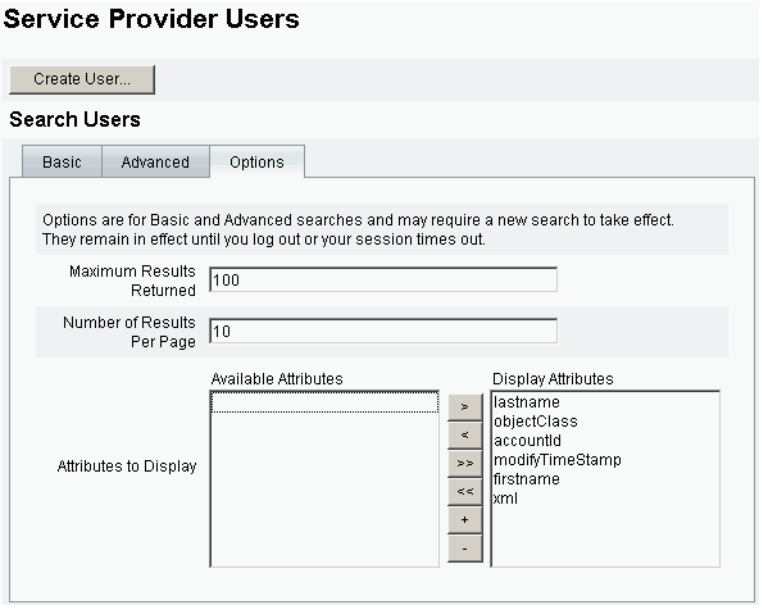
1. メニューバーの「**アカウント**」をクリックします。
2. 「**サービスプロバイダ**」をクリックします。
3. 「**オプション**」をクリックします。

注　　これらのオプションは、現在のログインセッションでのみ有効です。これらのオプションでは、検索結果の表示方法を設定します。この設定は、基本検索と詳細検索の両方の結果に適用され、一部の設定は新しい検索でのみ有効になります。

---

4. 「**返される結果の最大数**」を入力します。
5. 「**ページあたりの結果数**」を入力します。
6. 矢印キーを使用して、「**利用可能な属性**」から目的の「**表示属性**」を選択します。

図 13-13　サービスプロバイダユーザーの検索オプションの設定



エンドユーザーインタフェース

付属のサンプルエンドユーザーページは、xSP 環境での一般的な登録とセルフサービスの例を示しています。サンプルは拡張可能であり、カスタマイズ可能です。実際の配備用に、外観や使い勝手を変更したり、ページ間の移動方法を変更したり、ロケール固有のメッセージを表示したりできます。エンドユーザーページのカスタマイズの詳細については、『Identity Manager SPE Deployment』を参照してください。

セルフサービスイベントや登録イベントの監査に加えて、影響を受けるユーザーに、電子メールテンプレートを使用して通知を送信することができます。アカウント ID ポリシーとパスワードポリシー、およびアカウントロックアウトの例も用意されています。アプリケーション開発者は Identity Manager フォームも活用できます。サーブレットフィルタとして実装されている認証サービスモジュールを、必要に応じて拡張したり置き換えたりできます。これにより、Sun Java System Access Manager のようなアクセス管理システムとの統合が可能になります。

サンプル

付属のサンプルエンドユーザーページを使用すると、ユーザーは、操作しやすい一連の画面で基本的なユーザー情報の登録と管理を行い、自分のアクションに関する電子メール通知を受け取ることができます。サンプルページには次の機能が含まれています。

- チャレンジ質問による認証を含むログイン (およびログアウト)
- 登録および自己登録
- パスワードの変更
- ユーザー名の変更
- チャレンジ質問の変更
- 通知アドレスの変更
- ユーザー名を忘れた場合の処理
- パスワードを忘れた場合の処理
- 電子メール通知
- 監査

注 Identity Manager は登録に検証テーブルを使用します。そのテーブル内のユーザーだけが登録を許可されます。たとえば、Betty Childs というユーザーを登録する場合、bchilds@example.com という電子メールアドレスを持つ Betty Childs のエントリが検証テーブル内で検索され、登録が受け入れられます。

ページは、配備に合わせて簡単にカスタマイズできます。次のカスタマイズが可能です。

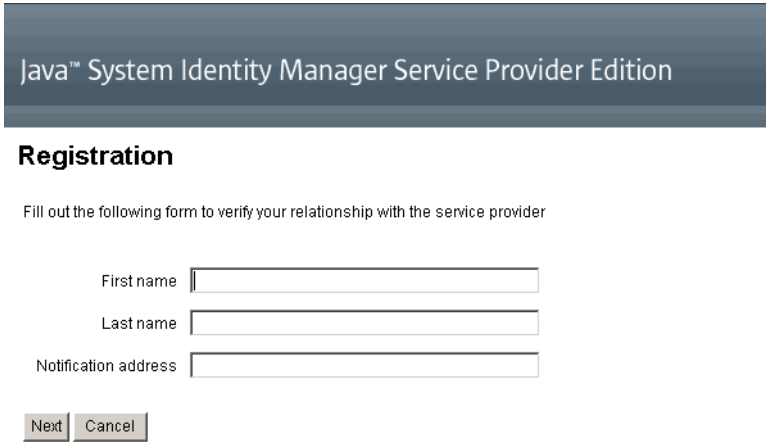
- ブランド設定
- 設定オプション (たとえば、ログイン試行エラー回数など)
- ページの追加 / 削除

ページのカスタマイズの詳細については、『Identity Manager SPE Deployment』を参照してください。

登録

新しいユーザーは登録を求められます。登録時に、ユーザーは自分のログイン、チャレンジ質問、および通知に関する情報を設定できます。

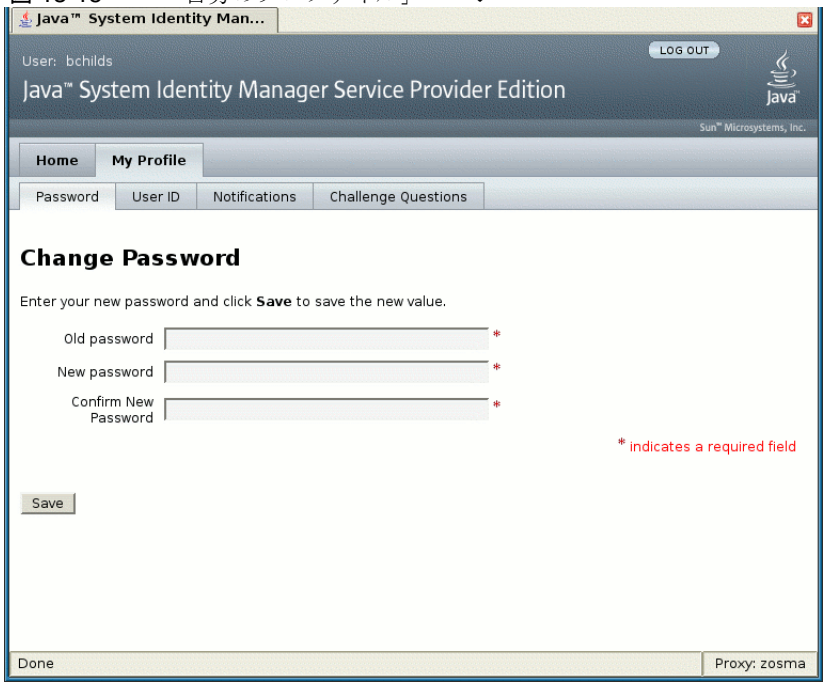
図 13-14　「登録」ページ



ホーム画面とプロファイル画面

図 13-15 に、エンドユーザーのホームタブとプロファイルページを示します。ユーザーは、自分のログイン ID とパスワードの変更、通知の管理、およびチャレンジ質問の作成を行うことができます。

図 13-15　「自分のプロファイル」ページ



同期

サービスプロバイダユーザーの同期は、同期ポリシーによって有効にできます。Identity Manager でリソースの属性に加えた変更をサービスプロバイダユーザーと同期させるには、サービスプロバイダ同期を設定する必要があります。次のトピックでは、サービスプロバイダ実装で同期を有効にする方法を説明します。

- 同期の設定
- 同期の監視
- 同期の開始と停止
- ユーザーの移行

注　サービスプロバイダ同期は、Identity Manager の「**リソース**」エリアのリソースリストから設定します。

同期の設定

Service Provider 同期を設定するには、222 ページの「同期の設定」で説明されているように、リソースの同期ポリシーを編集します。同期ポリシーを編集するときに、次のオプションを指定して、サービスプロバイダユーザーの同期プロセスを有効にする必要があります。

- 「ターゲットオブジェクトタイプ」として**「Service Provider Edition ユーザー」**を選択します。
- 「スケジューリングの設定」エリアで、**「同期の有効化」**を選択します。

222 ページの「同期の設定」の手順に従って、環境に応じてその他のオプションを指定します。

注	確認の規則とフォームでは、Identity Manager のユーザー入力ビューではなく、IDMXUser ビューを使用する必要があります (詳細については『Identity Manager SPE Deployment』を参照)。 その理由は、確認規則は相関規則で識別されるユーザーごとにユーザービューにアクセスするので、同期パフォーマンスに影響するためです。

「保存」をクリックしてポリシー定義を保存します。ポリシーで同期を無効にしなかった場合、同期は指定されたとおりにスケジュールされます。同期の無効を指定した場合、現在実行されている同期サービスは停止されます。有効にすると、Identity Manager サーバーを再起動したとき、または同期リソースアクションの下の**「サービスプロバイダに対して開始」**を選択したときに、同期が開始されます。

同期の監視

Identity Manager では、次の方法で Service Provider 同期を監視します。

- 「リソース」リストの説明フィールドに同期ステータスを表示する。
- JMX インタフェースを使用して同期の測定基準を監視する。

同期の開始と停止

Identity Manager をサービスプロバイダ実装用に設定する場合、サービスプロバイダ同期はデフォルトで有効になります。Service Provider Active Sync を無効にするには、次の手順に従います。

1. 「**リソース**」エリアでリソースを選択し、「**同期ポリシーの編集**」をクリックしてポリシーを編集します。
2. 「**同期の有効化**」チェックボックスを選択解除します。
3. 「**保存**」をクリックします。

   ポリシーが保存されると、同期は停止します。

同期を無効にせずに停止するには、同期リソースアクションの「**サービスプロバイダに対して停止**」を選択します。

注	同期を無効にせずにリソースアクションを使用して同期を停止した場合、いずれかの Identity Manager サーバーを起動すると、同期がふたたび開始されます。

ユーザーの移行

Service Provider 機能には、サンプルのユーザー移行タスクと関連スクリプトが含まれています。このタスクは、既存の Identity Manager ユーザーを Service Provider ユーザーディレクトリに移行します。この節では、サンプルの移行タスクの使用方法を説明します。使用状況に応じて、このサンプルを変更することをお勧めします。

既存の Identity Manager ユーザーを移行するには、次の手順に従います。

1. メニューバーの「**タスク**」をクリックします。
2. 「**タスクの実行**」をクリックします。
3. 「**SPE Migration**」をクリックします。
4. 一意の「**タスク名**」を入力します。
5. 「**リソース**」をリストから選択します。

   これは、Service Provider ディレクトリサーバーを表す、Identity Manager 内のリソースです。Identity Manager ユーザーで見つかったこのリソースへのリンクは移行されません。
6. 「**アイデンティティー属性**」を入力します。

   これは、ディレクトリユーザーの短い一意の ID を含む Identity Manager ユーザー属性です。
7. 「**ID 規則**」をリストから選択します。

これは、Identity Manager ユーザーの属性からディレクトリユーザーの名前を生成できるオプションの規則です。ID 規則は単純名 (通常は uid) を生成することができます。その後、この名前はリソースのアイデンティティーテンプレートで処理され、ディレクトリサーバーの識別名 (DN) を形成します。また、この規則は、アイデンティティーテンプレートを使用しない完全指定 DN を返すこともあります。

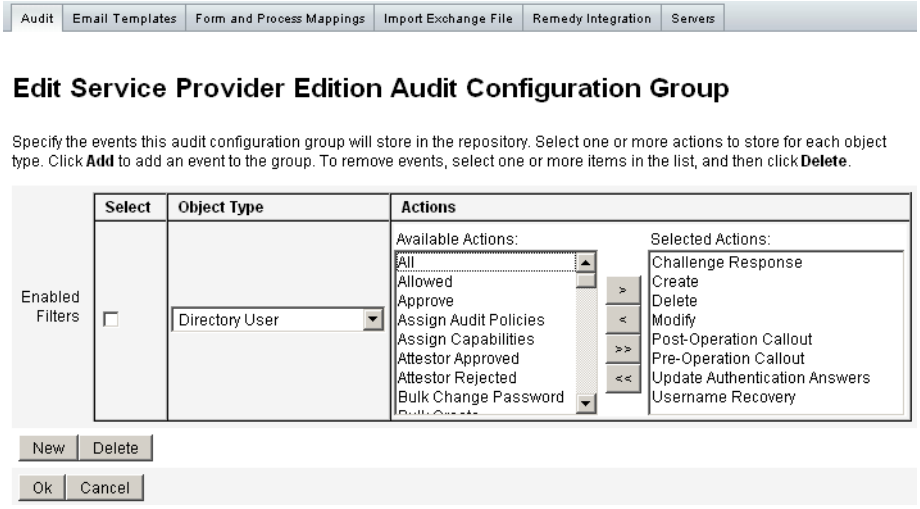
8. **「起動」**をクリックして、バックグラウンドでの移行タスクを開始します。

サービスプロバイダ監査イベントの設定

サービスプロバイダ実装で、Identity Manager の監査ログシステムは、エクストラネットユーザーのアクティビティーに関連するイベントを監査します。Identity Manager では、Service Provider Edition 監査設定グループ (デフォルトで有効) を使用して、サービスプロバイダユーザーのログを記録する監査イベントを指定することができます。図 13-16 を参照してください。

監査ログ、および Service Provider Edition 監査設定グループのイベントの変更の詳細については、第 12 章「監査ログ」を参照してください。

図 13-16　「Service Provider Edition 監査設定グループの編集」ページ



付録 A

lh リファレンス

使用法

次の構文を使用して、Identity Manager コマンド行インタフェースを呼び出し、Identity Manager コマンドを実行します。

```
lh { $class | $command } [ $arg [$arg... ] ]
```

使用上の注意

コマンドの使用法についてのヘルプを表示するには、lh と入力します (引数は指定しない)。

パス環境変数の設定

- lh コマンドの使用時には、JAVA_HOME を、Java 実行可能ファイルを保存した bin ディレクトリが含まれている JRE ディレクトリに設定する必要があります。この場所は、インストールごとに異なります。

  Sun から標準的な (JDK なしの) JRE を取得している場合、通常のディレクトリの場所は C:¥Program Files¥Java¥j2re1.4.1_01 です。このディレクトリには、Java 実行可能ファイルを保存した bin ディレクトリが含まれています。この場合は、JAVA_HOME を C:¥Program Files¥Java¥j2re1.4.1_01 に設定します。

  JDK のフルインストールには複数の Java 実行可能ファイルがあります。この場合は、JAVA_HOME を、内蔵の jre ディレクトリに設定します。このディレクトリには、正しい bin/java.exe ファイルが含まれています。通常のインストールでは、JAVA_HOME を D:¥¥java¥jdk1.3.1_02.jre に設定します。

- 次のように、WSHOME 変数を Identity Manager インストールディレクトリに設定します。

  ```
  set WSHOME=<path_to_identity_manager_directory>
  ```

たとえば、この変数をデフォルトのインストールディレクトリに設定するには、次のように指定します。

```
set WSHOME=C:¥Program Files¥tomcat¥webapps¥idm
```

注 WSHOME 変数の値に次の文字が含まれていないことを確認してください。

- 引用符 (" ")
- パスの末尾の円記号 (¥)

アプリケーションの配備ディレクトリのパスにスペースが含まれる場合でも、引用符を使用しないでください。

UNIX システム上では、次のようにしてパス変数をエクスポートする必要もあります。

```
export WSHOME
export JAVA_HOME
```

クラス

`com.waveset.session.WavesetConsole` などの完全修飾クラス名でなければなりません。

コマンド

次のコマンドのいずれかでなければなりません。

- `config` ー Business Process Editor を起動します。
- `console` ー Identity Manager コンソールを起動します。
- `export` ー 交換ファイルをエクスポートします。
- `js` ー JavaScript プログラムを起動します。
- `javascript` ー js と同じです。
- `import` ー Identity Manager オブジェクトをインポートします。
- `license [options] {status | set {parameters }}` ー Identity Manager ライセンスキーを設定します。
- `setRepo` ー Identity Manager インデックスリポジトリを設定します。

- `setup` ー Identity Manager セットアッププロセスを開始します。これにより、ライセンスキーの設定、Identity Manager インデックスリポジトリの定義、および設定ファイルのインポートができるようになります。
- `syslog [options]` ー システムログからレコードを抽出します。
- `xmlparse` ー Identity Manager オブジェクトに対し XML の妥当性検査を行います。
- `xpress [options]` ファイル名 ー 式を評価します。有効なオプションは次のとおりです。
  `-trace` (トレース出力を有効にする)

例

- `lh com.waveset.session.WavesetConsole`
- `lh console`
- `lh console -u $user -p` *`PathtoPassword`*`.txt`
- `lh setup -U` 管理者名 `-P` *`PathtoPassword`*`.txt`
- `lh setRepo -c -A` 管理者名 `-C` *`PathtoPassword`*`.txt`
- `lh setRepo -t` ローカルファイル `-f $WSHOME`

export コマンド

使用法

`export [-v]` *`Outfile`* `[ typeSet | typeName... ]`

オプション

- `-v` ー 詳細モードを有効にします。
- `typeName` オプション : `all`、`default`、または `users`。`all` オプションは次を除くすべてのオブジェクトタイプをエクスポートします。
  - Log
  - Syslog
  - TestItem

- Server
- Administrator

一般に、別の環境にログファイルをエクスポートすることはあまりありません。

license コマンド

使用法

```
license [options] { status | set {parameters} }
```

オプション

- `-U` *username* (Configurator のアカウント名が変更されている場合)
- `-P` *PathtoPassword*`.txt` (Configurator のパスワードが変更されている場合)

`set` オプションのパラメータは、「`-f` ファイル」の形式でなければなりません。

例

- `lh license status`
- `lh license set -f` ファイル

syslog コマンド

使用法

```
syslog [options]
```

オプション

- `-d` 日数 ー 指定された直近の日数分のレコードを表示します (デフォルト =1)
- `-F` ー 重要度レベルが「fatal」のレコードのみを表示します
- `-E` ー 重要度レベルが「error」以上のレコードのみを表示します
- `-W` ー 重要度レベルが「warning」以上のレコードのみを表示します (デフォルト)
- `-X` ー エラーの原因がレポートされている場合、出力に含めます

オンラインマニュアルの高度な検索

Identity Manager のオンラインマニュアルを検索するとき、複雑なクエリーを作成するための高度な構文を使用できます。オブジェクトには次のものがあります。

- ワイルドカード文字 ― 完全な語句の代わりにスペルのパターンを指定できます。
- クエリー演算子 ― クエリー要素がどのように結合または変更されるかを指定します。

注 同じ検索の中でワイルドカード文字とクエリー演算子を併用できます。

ワイルドカード文字

ワイルドカードは、検索においてほかの文字または文字のグループを表す特殊文字です。

Identity Manager のオンラインマニュアルの検索では、次のワイルドカード文字を使用できます。

表 B-1 サポートされているワイルドカード文字

ワイルドカード文字	説明
疑問符 (?)	任意の 1 文字と一致します。 たとえば、「t?p」を検索すると tap、tip、top などの語と一致します。「ball????」を検索すると ballpark、ballroom、ballyhoo などの語と一致しますが、「ball」に続く文字数が 4 文字ではない ballet や balloon などの語は検索されません。
アスタリスク (*)	任意の文字のグループと一致します。 たとえば、「comp*」を検索すると、computer、company、comptroller など、「comp」で始まるすべての語が検索されます。

クエリー演算子

クエリー演算子を使用して、検索の要素を結合、変更、または除外することができます。クエリー演算子は大文字、小文字、または両者の混合で入力できます。通常、クエリー演算子は <CONTAINS> のように山括弧で囲みます。

注	基本的なブール演算子 (AND、OR、および NOT) と特殊文字演算子 (<、=、!= など) には山括弧は必要ありません。

優先度の規則

1 つのクエリーの中で複数のタイプの演算子を使用するとき、優先度の規則と括弧の使い方によって演算子の有効範囲が決まります。AND 演算子は OR 演算子より優先されます。たとえば、次のようなクエリーがあるとします。

```
resource AND adapter OR attribute
```

これは次のクエリーと同じ働きです。

```
(resource AND adapter) OR attribute
```

「adapter」と「attribute」が、「resource」とともに検索される二者択一の用語として解釈されるようにするには、次のように括弧を使う必要があります。

```
resource AND (adapter OR attribute)
```

デフォルト演算子

演算子を指定せずにクエリー用語またはクエリー要素を連続して入力すると、標準のデフォルト演算子 <AND> を使ってクエリー要素が結合されます。

<EXACT>、<MORPH>、<EXPAND> などの明示的な単項用語演算子が付かない 1 つの単語でクエリーが構成される場合、その単語にはデフォルトの用語演算子 <MORPH> が適用されるとみなされます。

次の表は、オンラインマニュアル検索で最もよく使われるクエリー演算子の一覧です。

表 B-2　オンラインマニュアル検索でよく使われるクエリー演算子

演算子	説明	例
<AND> または AND	必須の基準を検索に追加します。	「apples AND oranges」を検索すると、順序を問わず「apples」および「oranges」の両方を含む一致結果が返されます。どちらか 1 つの単語しか含まれないドキュメントは無視されます。
<CASE>	後続の 1 つ以上の用語の一致を、大文字と小文字を区別して検索します。 注意 : Identity Manager では、大文字を含むクエリー用語は自動的に大文字と小文字を区別する検索とみなされるため、<CASE> を付ける必要は必要ありません。すべて小文字の用語は大文字と小文字を区別しない検索として扱われるため、すべて小文字の一致結果だけを得るには <CASE> を使う必要があります。	「<CASE> bill」を検索すると「bill」に一致しますが「Bill」には一致しません。
<EXACT>	指定された単語と完全に一致する単語を含むドキュメントを検索します。	「<EXACT> soft」を検索すると、単語「soft」を含むドキュメントが検索されますが、「softest」や「softer」を含むドキュメントは検索されません。
<MORPH>	指定された単語に加えて、その単語が形態変化した単語を含むドキュメントも検索します。これには複数形や過去形に加えて、接頭辞、接尾辞、複合語を含む複合形が含まれます。	不規則な形式を正しく扱うために、語彙データベースの情報も利用します。<MORPH> surf」を検索すると、「surfs」、「surfed」、「surfing」のような単語「surf」の単純な変化形に加えて、接頭辞付き (「resurf」) や複合語 (「surfboard」) などの変化形も対象としてドキュメントを検索します。
<NEAR>	指定された単語どうしが 1000 語以内の近さにあるドキュメントを検索します。単語どうしが近いドキュメントほど検索結果の上位に表示されます。	「resource <NEAR> configuration」を検索すると、両方の単語を含み、単語間の距離が 1000 語以内であるドキュメントが検索されます。
<NEAR/n>	指定された単語間の距離が n 語以下であるドキュメントを検索します。 注意 : *n* の値は 1 ～ 1024 の範囲で指定する必要があります。	「buy <NEAR/3> sell」を検索すると、「buy」と「sell」の間が 3 語以下である「buy low and sell high」のような表現を含むドキュメントが検索されます。
<NOT> または NOT	特定の単語または語句を含まないドキュメントを検索します。	「surf <AND> <NOT> channel」を検索すると、「surf」を含み「channel」を含まないドキュメントが検索されます。

監査ログデータベーススキーマ

この付録では、サポートされるデータベースタイプと監査ログデータベースマッピングの監査データスキーマ値について説明します。

- Oracle
- DB2
- MySQL
- Sybase
- 監査ログデータベースマッピング

Oracle

表 C-4 に、Oracle データベースタイプのデータスキーマ値を示します。

表 C-1　Oracle データベースタイプのデータスキーマ値

データベースの列	値
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)

表 C-1　Oracle データベースタイプのデータスキーマ値 (続き)

データベースの列	値
acctAttrChanges	VARCHAR(4000)
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

DB2

表 C-2 に、DB2 データベースタイプのデータスキーマ値を示します。

表 C-2　DB2 データベースタイプのデータスキーマ値

データベースの列	値
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
acctAttrChanges	CLOB(16M)
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)

表 C-2　DB2 データベースタイプのデータスキーマ値 (続き)

データベースの列	値
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

MySQL

表 C-3 に、MySQL データベースタイプのデータスキーマ値を示します。

表 C-3　MySQL データベースタイプのデータスキーマ値

データベースの列	値
id	VARCHAR(50) BINARY NOT NULL
name	VARCHAR(128) BINARY NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)

表 C-3　MySQL データベースタイプのデータスキーマ値 (続き)

データベースの列	値
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
acctAttrChanges	BLOB
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

Sybase

表 C-4 に、Sybase データベースタイプのデータスキーマ値を示します。

表 C-4　Sybase データベースタイプのデータスキーマ値

データベースの列	値
id	VARCHAR(50) NOT NULL
name	VARCHAR(128) NOT NULL
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDate	CHAR(8)
actionTime	CHAR(12)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255)
acctAttrChanges	TEXT
acctAttr01label	VARCHAR(50)
acctAttr01value	VARCHAR(128)
acctAttr02label	VARCHAR(50)
acctAttr02value	VARCHAR(128)
acctAttr03label	VARCHAR(50)
acctAttr03value	VARCHAR(128)
acctAttr04label	VARCHAR(50)
acctAttr04value	VARCHAR(128)
acctAttr05label	VARCHAR(50)

表 C-4　Sybase データベースタイプのデータスキーマ値 (続き)

データベースの列	値
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128)

監査ログデータベースマッピング

表 C-5 には、格納された監査ログデータベースキーと、監査レポート出力でそれらのキーと対応している表示文字列との間のマッピングが示されています。Identity Manager では、リポジトリ内の領域を節約するために、定数として使用されるアイテムを短いデータベースキーとして格納します。製品のインタフェースにはこれらのマッピングは表示されません。代わりに、監査レポート結果のダンプの出力を調べるときにのみこれらのマッピングが表示されます。

表 C-5　オブジェクトキータイプ、アクション、およびアクションステータスのデータベースキー

監査オブジェクトタイプ	DB キー	アクション	DB キー	アクションステータス	DB キー
Administrator	AD	Approve	AP	Failure	F
Admin Group	AG	Change Password	CP	Success	S
Application	AP	Change Resource Password	CR		
Audit Config	AC	Configure	CG		
Audit Log	AL	Connect	CN		
Email Template	ET	Create	CT		
Lighthouse Account	LA	Credentials Expired	CE		

表 C-5　オブジェクトキータイプ、アクション、およびアクションステータスのデータベースキー (続き)

監査オブジェクトタイプ	DB キー	アクション	DB キー	アクションステータス	DB キー
Login Config	LC	Delete	DL		
Notify	NT	Delete Account	DA		
Object Group	OG	Deprovision	DP		
Policy	PO	Disable	DS		
Remedy Config	RC	Disconnect	DC		
Resource Account	RA	Enable	EN		
Resource	RS	Launch	LN		
Resource Object	RE	Load	LD		
Role	RL	Login	LG		
Role Attribute	RT	Logout	LO		
Task Definition	TD	Native Change	NC		
Task Instance	TI	Protect Resource Password	PT		
Task Schedule	TS	Provision	PV		
User	US	Reject	RJ		
Workflow Case	WC	Reprovision	RV		
Workflow Process	WP	Reset Password	RP		
Workflow Task	WT	Terminate	TR		
		Update	MO		
		View	VW		

Active Sync ウィザード

概要

7.0 より前のバージョンの Identity Manager では、アクティブな同期の作成および管理に Active Sync ウィザードを使用します。この付録では、サポートされているバージョンの Identity Manager での Active Sync ウィザードによるアクティブな同期のセットアップおよび管理について説明します。バージョン 7.0 以降では、同期の設定には同期ポリシーを使用します。

同期のセットアップ

Identity Manager リソースエリアにある「Active Sync ウィザード」を使用して、アクティブな同期をセットアップします。このウィザードは手順のさまざまなセットを示し、このセットによりリソース用のアクティブな同期が設定されます (手順は選択によって異なる)。

Active Sync ウィザードを起動するには、リソースリスト内のリソースを選択し、「リソースアクション」オプションリストから**「Active Sync ウィザード」**を選択します。

同期モード

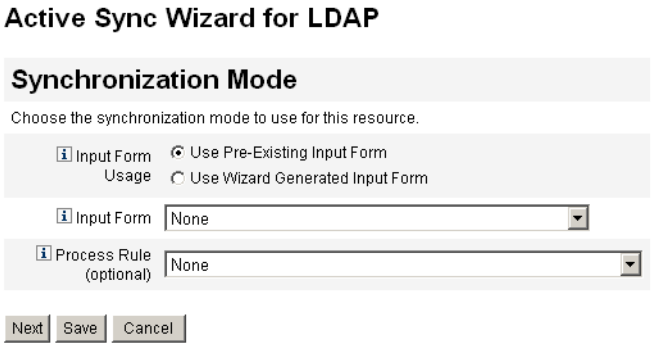
「同期モード」ページでは、アクティブな同期の設定中に選択可能な設定オプションの範囲を指定できます。

次のいずれかのオプションを選択します。

「入力フォームの使用」 – アクティブな同期のセットアップ時に使用するモードを選択します。既存のフォームを使用するよう選択できますが、その場合このリソースの設定の選択が制限されます。代わりに、Active Sync ウィザードで生成したフォームを使用すると、設定の選択の完全なセットが提供されます。

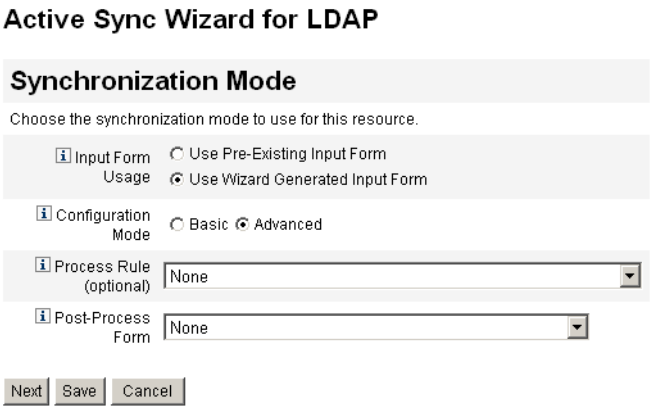
- 「既存の入力フォーム」(デフォルト) を選択した場合、次のオプションの選択を行います。
  - **「入力フォーム」** – データ更新を処理する入力フォームを選択します。このオプション設定項目を使用すると、属性を変換してからアカウントに保存することができます。
  - **「処理規則」** – 対象となる各アカウントに対して実行する処理規則をオプションの作業として選択します。この選択は、ほかのすべての選択よりも優先されます。処理規則を指定した場合、このリソースに関するほかの設定に関係なく、すべての行に対して処理が実行されます。これは、プロセス名か、またはプロセス名として評価される規則です。

図 D-1　Active Sync ウィザード : 「同期モード」、「既存のフォーム」の選択



- **「ウィザードで生成した入力フォームを使用」** を選択した場合、次のオプションの選択を行います。
  - **「設定モード」** – Active Sync ウィザードに基本モードを使用するか詳細モードを使用するかを選択します。基本モードがデフォルトのオプションです。詳細モードを選択した場合、イベントタイプを定義し処理規則を設定できます。
  - **「処理規則」** – (詳細設定モードでのみ表示) 対象となる各アカウントに対して実行する処理規則をオプションの作業として選択します。この選択は、ほかのすべての選択よりも優先されます。処理規則を指定した場合、このリソースに関するほかの設定に関係なく、すべての行に対して処理が実行されます。これは、プロセス名か、またはプロセス名として評価される規則です。
  - **「処理後のフォーム」** – (詳細設定モードでのみ表示) Active Sync ウィザードで生成されるフォームに追加して実行するフォームをオプションの作業として選択します。このフォームは、Active Sync ウィザードによる設定に優先して適用されます。

図 D-2　Active Sync ウィザード：「同期モード」、「ウィザード生成のフォーム」の選択



「次へ」をクリックしてウィザードを続行します。「Active Sync の動作設定」ページが表示されます。

動作設定

このページでは、アクティブな同期の以下の項目を設定できます。

- スタートアップ
- ポーリング
- ログ

スタートアップ設定

次のオプションから Active Sync スタートアップの選択を行います。

- **「起動タイプ」**― 次のいずれかのオプションを選択します。
  - **「自動」または「フェイルオーバー付自動」**― アイデンティティーシステムの起動時に、このソースも起動されます。
  - **「手動」**― 管理者がこのソースを起動する必要があります。
  - **「無効」**― リソースを無効にします。
- **「プロキシ管理者」**― 更新を処理する管理者を選択します。すべての操作は、この管理者に割り当てられた機能を通して承認されます。ユーザーフォームが空のプロキシ管理者を選択する必要があります。

ポーリング設定

ポーリング開始日と時刻を将来の日時に設定すると、指定した日時にポーリングが開始します。ポーリング開始日と時刻を過去の日時に設定すると、Identity Manager はこの情報とポーリング間隔に基づいて、いつポーリングを開始するかを決定します。次に例を示します。

- リソースのアクティブな同期を 2005 年 7 月 18 日 (火曜) に設定
- リソースのポールを週単位で、開始日を 2005 年 7 月 4 日 (月曜)、時刻を午前 9 時に設定

この場合、リソースのポーリングは 2005 年 7 月 25 日 (次の月曜) に開始されます。

開始日または開始時刻を指定しない場合、ただちにリソースのポーリングが開始されます。この場合、アプリケーションサーバーを再起動するたびに、アクティブな同期を行うよう設定されたリソースすべてのポーリングが、ただちに開始されます。一般的には、開始日と開始時刻を設定します。

ポーリングの設定の選択を行います。

- **「ポール間隔」** − ポールを行う頻度を指定します。数値を入力し、次に時間の単位 (日、時間、分、月、秒、または週) を選択します。デフォルトの単位は分です。
- **「ポーリング開始日」** − 最初にスケジューリング間隔を開始する日付を yyyyMMdd 形式で入力します。
- **「ポーリング開始時刻」** − 最初にスケジューリング間隔を開始する時刻を `HH:mm:ss` 形式で入力します。

ログ設定

次のオプションから、ログ情報およびログレベルの設定の選択を行います。

- **「ログアーカイブの最大数」** − 値が 0 (ゼロ) より大きい場合、最新の N 個のログファイルが保持されます。0 (ゼロ) の場合は 1 つのログファイルが繰り返し利用されます。-1 の場合、ログファイルは破棄されません。
- **「アクティブログの最大有効期間」** − この期間を経過すると、アクティブログはアーカイブされます。期間が 0 (ゼロ) の場合、期間ベースのアーカイブは行われません。ログアーカイブの最大数が 0 (ゼロ) に設定されている場合、この期間が経過してもアーカイブは行われず、アクティブログは切り捨てられ、再使用されます。この有効期間条件は、「ログファイルの最大サイズ」に指定される条件とは別に評価されます。

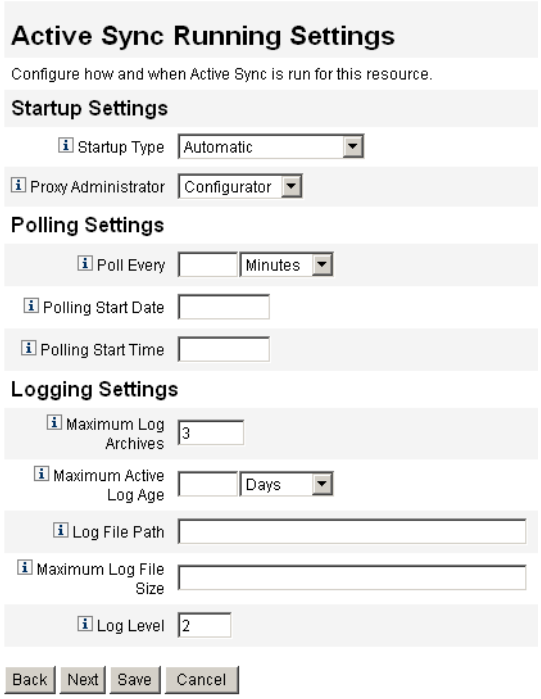
数値を入力し、次に時間の単位 (日、時間、分、月、秒、または週) を選択します。デフォルトの単位は日です。

- **「ログファイルパス」** − アクティブログとアーカイブされたログのファイルが作成されるディレクトリへのパスを入力します。ログファイル名はリソース名から開始します。

- **「ログファイルの最大サイズ」** ― アクティブログファイルの最大サイズをバイト数で入力します。指定した最大サイズに達すると、アクティブログファイルはアーカイブされます。ログアーカイブの最大数が 0 (ゼロ) に設定されている場合、この期間が経過してもアーカイブは行われず、アクティブログは切り捨てられ、再使用されます。このサイズ条件は、「アクティブログの最大有効期間」に指定される条件とは別に評価されます。
- **「ログレベル」** ― ログのレベルを入力します。
  - 0 ― ログなし
  - 1 ― エラー
  - 2 ― 情報
  - 3 ― 詳細
  - 4 ― デバッグ

図 D-3 は「動作設定」ページの表示例です。

図 D-3　　Active Sync ウィザード : 動作設定



「次へ」をクリックしてウィザードを続行します。「Active Sync の一般設定」ページが表示されます。

一般の Active Sync 設定

このページを使用して、一般的なアクティブな同期の設定パラメータを指定します。

リソース固有の設定

利用可能なリソース固有の設定は、リソースタイプによって異なります。たとえば LDAP リソースの場合、次の設定を適用できます。

- **「同期するオブジェクトクラス」** – 同期させるオブジェクトクラスを入力します。変更ログはすべてのオブジェクトに対してですが、このフィルタは、ここでリストされたオブジェクトクラスのみを更新します。
- **「同期させるアカウントの LDAP フィルタ」** – 同期させるオブジェクトの LDAP フィルタをオプションとして指定します。変更ログはすべてのオブジェクトに対してですが、このフィルタは、指定されたフィルタと一致するオブジェクトのみを更新します。フィルタを指定した場合、フィルタと一致し、同期されるオブジェクトクラスを含むオブジェクトだけが同期されます。
- **「同期する属性」** – 同期する属性名を指定します。変更ログファイルからの更新のうち、指定属性以外の更新は無視されます。たとえば、部署属性のみを指定した場合、部署属性に影響する変更のみが処理されます。それ以外の更新は無視されます。空欄 (デフォルト) の場合、すべての変更が処理されます。
- **「変更ログブロックサイズ」** – クエリーをフェッチする変更ログエントリ数を入力します。デフォルトの数は 100 です。
- **「変更番号属性名」** – 変更ログエントリ中の変更番号属性の名前を入力します。
- **「変更者フィルタ」** – 変更からフィルタするディレクトリ管理者の名前 (RDN) を入力します。このリストのエントリに属性 `modifiersname` が一致する変更がフィルタされます。

標準値は、ループを防ぐため、このアダプタにより使用される管理者名です。エントリは、`cn=Directory Manager` の形式です。

共通の設定

- **「相関規則」** – リソースの調整ポリシーに指定されている相関規則に優先して適用される相関規則をオプションの作業として指定します。相関規則は、リソースアカウントをアイデンティティーシステムアカウントに相互に関連付けます。
- **「確認規則」** – リソースの調整ポリシーに指定されている確認規則に優先して適用される確認規則をオプションの作業として指定します。

- **「解決プロセス規則」** – フィード内の複数のレコードと一致した場合に実行するタスク定義の名前をオプションの作業として指定します。これは、管理者に手動アクションを求めるプロセスである必要があります。これは、プロセス名か、またはプロセス名として評価される規則です。
- **「削除規則」** – 削除操作を行うかどうかを決定するために、対象となるユーザー更新ごとに評価される、true または false を返す規則をオプションの作業として指定します。
- **「一致しないアカウントの作成」** – true に設定すると、アダプタはアイデンティティーシステム上に存在しないアカウントの作成を試みます。false に設定した場合、アダプタは解決プロセス規則が返すプロセスを使用してアカウントを実行します。
- **「作成イベントで Active Sync リソースを割り当てる」** – このオプションを選択した場合、Active Sync ソースリソースは作成イベントが検出されたときに作成されるユーザーに割り当てられます。
- **「グローバルで利用」** – ActiveSync ネームスペースの下のフォームは、対象となる各アカウント内のすべての属性を常に利用できます。このオプションを選択した場合、グローバルネームスペースでもすべての属性 (accountId を除く) を利用できます。
- **「リセット時に過去の変更を無視する」** – アダプタの最初の開始時またはリセット時に、過去の変更を無視するよう選択します。アダプタをリセットするには、XmlData オブジェクト SYNC_resourceName を編集し、適切な同期プロセス (ActiveSync など) の MapEntry を削除します。このオプションは、すべてのアダプタで利用可能ではありません。
- **「ポール前のワークフロー」** – 各ポールの直前にオプションとして実行するワークフローを選択します。
- **「ポール後のワークフロー」** – 各ポールの直後にオプションとして実行するワークフローを選択します。

「保存」または**「次へ」**をクリックして、リソースの一般設定の変更を保存します。

- 既存の入力フォームを使用している場合、**「保存」**をクリックしてウィザードの選択を終了し、リソースリストに戻ります。
- ウィザードで生成した入力フォームを使用している場合、**「次へ」**をクリックして続行します。
  - 「基本」設定モードを使用している場合、「ターゲットリソース」ページが表示されます。この章の 510 ページの「ターゲットリソース」に進んでください。
  - 「詳細」設定モードを使用している場合、「イベントタイプ」ページが表示されます。

イベントタイプ

このページを使用して、Active Sync リソースに特定のタイプのイベントの変更が発生したかどうかを確認するメカニズムを設定します。

イベントについて

アクティブな同期イベントは、Active Sync リソースで発生した変更として定義されます。リソースごとにリストされたイベントタイプは、リソースのタイプおよび変更イベントに影響を受けるオブジェクトに応じて異なります。イベントタイプには、作成、削除、更新、無効化、有効化、および名前の変更があります。

イベントの無視

Active Sync イベントを無視するかどうかを決定するメカニズムを選択できます。次のオプションがあります。

- **「なし」**― どの Active Sync イベントも無視されません。
- **「規則」**― 規則を使用して Active Sync イベントを無視するかどうかを決定します。このオプションを選択した場合、オプションリストからさらに規則を選択する必要があります。
- **「条件」**― 条件を使用して Active Sync イベントを無視するかどうかを決定します。このオプションを選択した後、「条件の編集」をクリックして「条件パネル」を使用し、条件を定義します。

イベントタイプを決定するためのオプションは次のとおりです。

- **「なし」**― イベントタイプを決定する方法はありません。
- **「規則」**― 規則を使用してイベントタイプを決定します。このオプションを選択した場合、オプションリストからさらに規則を選択する必要があります。
- **「条件」**―条件を使用してイベントタイプを決定します。このオプションを選択した後、「条件の編集」をクリックして「条件パネル」を使用し、条件を定義します。

「次へ」をクリックしてウィザードを続行します。「プロセスの選択」ページが表示されます。

プロセスの選択

このページを使用して、ユーザー画面がチェックされているときに特定の Active Sync イベントインスタンスまたは Active Sync イベントのタイプに対して実行するワークフローまたはプロセスを選択します。

プロセスモード

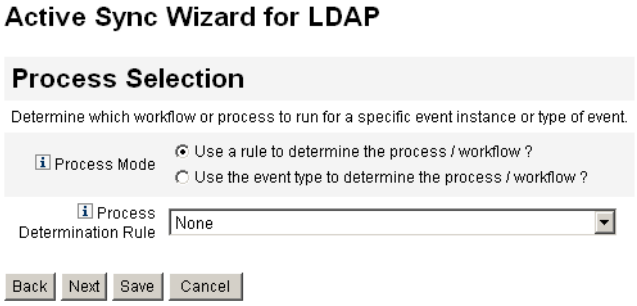
Active Sync イベントが発生したときに実行するワークフローまたはプロセスを決定する方法を次の 2 つのモードから選択します。

- **「規則」** – 特定の規則を使用して、それぞれの Active Sync イベントインスタンスに対してどのワークフローまたはプロセスを実行するかを決定します。これは、イベントが発生するたびに規則が実行されることを意味します。

  このオプションを選択した後、規則 (プロセス決定規則) をリストから選択します。

  図 D-4 に、規則の選択を指定する「プロセスの選択」ページを示します。

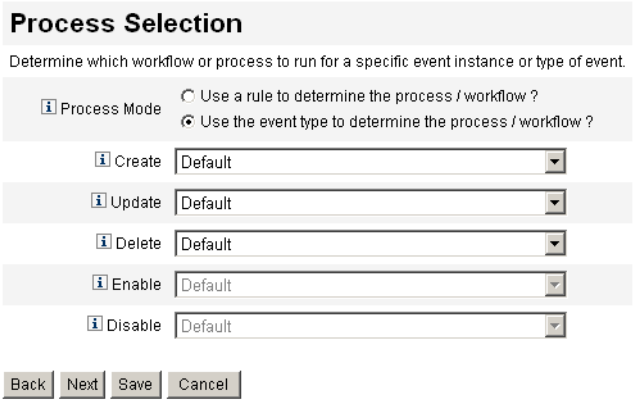
図 D-4　　Active Sync ウィザード : プロセスの選択 (規則)



- **「イベントタイプ」** – それぞれのイベントインスタンスのイベントタイプに基づいて、ワークフローまたはプロセスを実行できます。これは、デフォルトの選択です。

  このオプションを選択した後、図 D-5 に示すように、リストされているそれぞれのイベントタイプに対して実行するワークフローまたはプロセスを選択します。

図 D-5　　Active Sync ウィザード : プロセスの選択 (イベントタイプ)

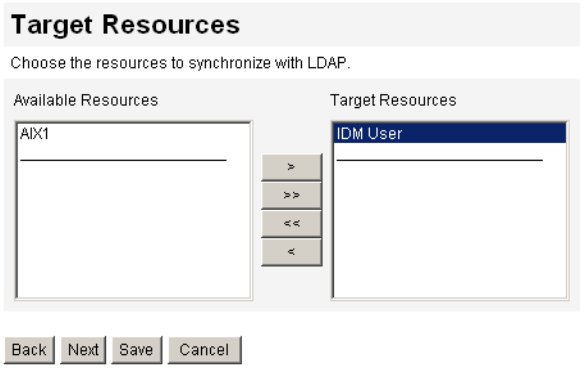


「次へ」をクリックしてウィザードを続行します。「ターゲットリソース」ページが表示されます。

ターゲットリソース

このページを使用して、このリソースと同期させるターゲットリソースを指定します。

図 D-6　　Active Sync ウィザード : ターゲットリソース

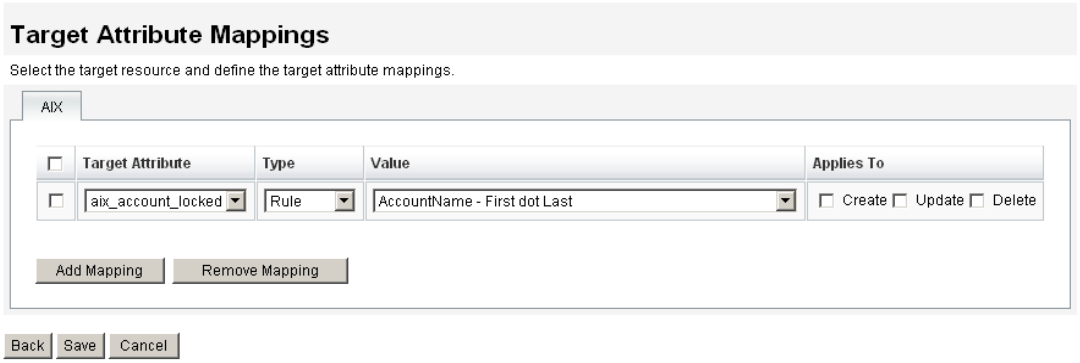


1. 1 つ以上のリソースを利用可能なリソースエリアから選択し、ターゲットリソースエリアへ移動します。
2. 「次へ」をクリックして続行します。「ターゲット属性マッピング」ページが表示されます。

ターゲット属性マッピング

このページを使用して、それぞれのターゲットリソースに対するターゲット属性マッピングを定義します。

図 D-7　　Active Sync ウィザード : ターゲット属性マッピング



1. オプションリストからターゲットリソースを選択します。ターゲット属性を追加する場合は、**「マッピングの追加」**をクリックします。
2. それぞれのターゲット属性に対して、属性、タイプ、および属性値を選択します。
3. 「適用先」の列では、マッピングを適用する 1 つ以上の操作 (作成、更新、または削除) を選択します。
4. 各ターゲットリソースに対して選択を続けます。

リストから属性行を削除するには、行を選択して**「マッピングの削除」**をクリックします。

「保存」をクリックして、属性マッピングを保存し、リソースリストに戻ります。

用語集

Business Process Editor (BPE)　Identity Manager 7.0 より前のバージョンで提供されていた Identity Manager フォーム、規則、およびワークフローをグラフィカルに表示するツールです。BPE は現在のバージョンの Identity Manager では Identity Manager IDE に置き換わっています。「Identity Manager IDE」を参照してください。

ide　Identity Manager IDE を参照。

Identity Manager IDE　Identity Manager Integrated Development Environment (IDE) は、配備で Identity Manager オブジェクトを表示、カスタマイズ、デバッグできるようにする Java アプリケーションです。

アイデンティティーテンプレート　ユーザーのリソースアカウント名を定義します。

アクセスレビュー　特定の日に従業員セットが適切なユーザーエンタイトルメントを持っているとアテストする管理および監査プロセス。

アテスター　ユーザーエンタイトルメントが適切であることを保証 (アテステーション) する責任を持つユーザー。アテスターは、アテステーションを必要とするユーザーエンタイトルメントを管理するために必要な Identity Manager の拡張特権を持ちます。

アテステーション　ユーザーエンタイトルメントが適切であることを確認するために、アクセスレビュー中にアテスターが行う操作。

アテステーションタスク　アテステーションを必要とするユーザーエンタイトルメントレビューの論理的集まり。ユーザーエンタイトルメントは、同じアテスターに割り当てられ、同じアクセスレビューインスタンスから作成されると、1 つのアテステーションタスクにグループ化されます。

エスカレーションタイムアウト　作業項目を割り当てられた所有者が作業項目リクエストで指定された時間内に応答しなかった場合、タイムアウトとなり Identity Manager プロセスは次に割り当てられている応答者にリクエストを送信します。

仮想組織　ディレクトリジャンクション内で定義された組織。ディレクトリジャンクションを参照。

管理者　Identity Manager をセットアップしたり、ユーザーの作成やリソースへのアクセスの管理などの操作タスクを実行したりする役割を持つ個人。

管理者インタフェース　Identity Manager の主要な管理ビュー。

管理者ロール　管理ユーザーに割り当てられた組織の組み合わせごとに定義します。

規則　XPRESS、XML オブジェクト、または JavaScript 言語で作成された関数を含む Identity Manager リポジトリ内のオブジェクト。規則は、頻繁に使用されるロジックや、フォーム、ワークフロー、およびロール内で再利用される静的な変数を格納するためのメカニズムを提供します。

機能　ユーザーアカウントに割り当てるアクセス権限のグループ。Identity Manager で実行される操作を制御する、Identity Manager での最小レベルのアクセス管理です。

サービスプロバイダユーザー　サービスプロバイダ企業の従業員やイントラネットユーザーとは区別される、エクストラネットユーザーまたはサービスプロバイダの顧客。

作業項目　承認者、アテスター、是正者に指定されたユーザーに割り当てられた、Identity Manager 内のワークフロー、フォーム、手順によって生成された操作リクエスト。

承認者　アクセスリクエストを承認または却下する管理機能を持つユーザー。

スキーマ　あるリソースに対するユーザーアカウント属性のリスト。

スキーママップ　あるリソースについての、リソースアカウント属性を Identity Manager アカウント属性にマップしたもの。
Identity Manager アカウント属性は、複数のリソースへの共通リンクを作成し、フォームによって参照されます。

是正者　監査ポリシーの割り当てられた是正者に指定された Identity Manager ユーザー。Identity Manager が是正の必要なコンプライアンス違反を検出すると、是正作業項目を作成し、その作業項目を是正者の作業項目リストに送信します。

組織　管理の委任を可能にするために使用する Identity Manager コンテナ。

組織は、管理者が制御または管理するエンティティー (ユーザーアカウント、リソース、管理者アカウントなど) の範囲を定義します。組織は、主として Identity Manager を管理する目的で「どこで」というコンテキストを提供します。

定期的アクセスレビュー　暦四半期など定期的な間隔で実行されるアクセスレビュー。

ディレクトリジャンクション　階層的に関係する組織のセットであり、ディレクトリリソースの実際の階層構造コンテナのセットをミラー化したものです。ディレクトリジャンクション内の各組織は、仮想組織です。

フォーム　Web ページに関連付けられたオブジェクトであり、ブラウザでユーザー表示属性をそのページにどのように表示するかについての規則が含まれています。フォームにはビジネスロジックを組み込むことができ、通常は、ユーザーに表示する前に、表示データを処理するために使用します。

ポリシー　Identity Manager アカウントの制限を設定します。
Identity Manager ポリシーは、ユーザー、パスワード、および認証オプションを設定し、組織またはユーザーに関連付けられます。リソースパスワードポリシーとアカウント ID ポリシーは、規則、許可される単語、および属性値を設定し、個々のリソースに関連付けられます。

ユーザー　Identity Manager システムアカウントを所持する個人。Identity Manager では、ユーザーは特定の範囲の機能を持つことができます。拡張機能を持つユーザーは Identity Manager 管理者です。

ユーザーアカウント　Identity Manager を使用して作成されたアカウント。
Identity Manager アカウントと、Identity Manager リソース上のアカウントのいずれかを指します。つまり、入力する情報またはフィールドは、ロールの割り当てによって直接または間接的にユーザーに提供されたリソースに応じて異なります。

ユーザーインタフェース　Identity Manager システムの制限されたビュー。
特に管理機能を持たないユーザー用に調整したものであり、パスワードの変更、秘密の質問への回答の設定、委任割り当ての管理など、一連の自己管理タスクを実行できます。

ユーザーエンタイトルメント　特定の日の 1 人のユーザーに割り当てられたリソースとこれらのリソース上の重要な属性を示すユーザービュー。

リソース　アカウントが作成されたリソースやシステムへの接続方法についての情報が保存される Identity Manager オブジェクト。
Identity Manager がアクセスを提供するリソースには、メインフレームセキュリティーマネージャー、データベース、ディレクトリサービス、アプリケーション、オペレーティングシステム、ERP システム、およびメッセージプラットフォームがあります。

リソースアダプタ　Identity Manager エンジンとリソースの間のリンクを提供する Identity Manager コンポーネント。
このコンポーネントにより、Identity Manager は所定のリソースのユーザーアカウントを管理 (作成、更新、削除、認証、およびスキャン機能を含む) するほか、そのリソースをパススルー認証に利用することができます。

リソースアダプタアカウント　管理するリソースにアクセスするために、Identity Manager リソースアダプタが使用するクレデンシャル。

リソースウィザード　リソースパラメータ、アカウント属性、アイデンティティーテンプレート、および Identity Manager パラメータのセットアップと設定を含め、リソースの作成および修正プロセスの手順を案内する Identity Manager ツール。

リソースグループ　ユーザーリソースアカウントを作成、削除、および更新を順序付けするために使用するリソースの集まり。

ロール　Identity Manager におけるユーザーのクラス用のテンプレートまたはプロファイル。各ユーザーには、1 つ以上のロールを割り当てることができます。ロールはアカウントによるリソースのアクセスとデフォルトのリソース属性を定義します。

ワークフロー　論理的で反復可能なプロセスであり、ドキュメント、情報、またはタスクが、ある関与者から別の関与者に渡されます。Identity Manager ワークフローは、ユーザーアカウントの作成、更新、有効化、無効化、および削除を管理する複数のプロセスで構成されています。

索引

A

Access Review Detail Report Administrator の機能 174
Account Administrator の機能 174
Active Sync アダプタ
  LDAP 設定 506
  一般設定 506
  イベントタイプ 508
  共通の設定 506
  スタートアップ設定 503
  セットアップ 501
  ターゲット属性マッピング 510
  ターゲットリソース 510
  同期モード 501
  プロセスの選択 508
  ポーリング設定 504
  ログ設定 504
ActiveSync アダプタ
  開始 227
  概要 222
  セットアップ 222
  停止 227
  パフォーマンスのチューニング 225
  編集 225
  ポーリング間隔の変更 226
  ホストの指定 226
  ログ 227
  ログ設定 224
Active Sync ウィザード、起動 501
Active Sync のターゲット属性マッピング 510
Active Sync のターゲットリソース 510
Active Sync のプロセスの選択 508
Admin Report Administrator の機能 175
Admin Role Administrator の機能 175
allowInvalidCerts 301
Assign User Capabilities の機能 175
auditconfig.xml ファイル 422
Auditor 是正者の機能 176
Audit Policy Administrator の機能 175
Audit Report Administrator の機能 175

B

BPE、「Identity Manager IDE」を参照
Business Process Editor (BPE) 52, 484

C

Capability Administrator の機能 178
ChangeLog
  CSV ファイル形式 126
  作成と編集 124
  スクリプトの作成 130
  セキュリティー 120
  設定 121

説明 119
ポリシーの作成 122
要件 120
clientConnectionFlags 301
clientSecurityFlags 301
com.waveset.object.Type クラス 428
com.waveset.security.Right オブジェクト 430
com.waveset.session.WorkflowServices アプリケーション 419
Configure Audit 機能 179
Control Active Sync Resource Administrator 機能 180
convertDateToString 284, 285
CreateOrUpdate コマンド 86
createUser 255, 256
Create User 機能 180
Create コマンド 86
CSV 形式 85, 211
抽出 210

D

DB2 監査スキーマ 495
DeleteAndUnlink コマンド 86
deleteUser 256
Delete コマンド 86
Deprovision User 機能 180
Disable User 機能 180
Disable コマンド 86

E

enabledEvents 属性 428
Enable User 機能 180
Enable コマンド 86
extendedActions 422, 430
extendedObjects 属性 429
extendedResults 422, 431
extendedTypes 422, 428

F

filterConfiguration 422, 423
FormUtil メソッド 284, 285

I

IDE、「Identity Manager インタフェース」を参照
Identity Manager
アカウントインデックス 220
インタフェース
Identity Manager IDE 51
管理者 47
ユーザー 49
オブジェクト 37, 42
概要 33
管理者ロール 41
管理について 152
機能 41, 166
サーバーの設定 148
組織 40, 159
タスク 58
データベース 432
ヘルプとガイダンス 53
ポリシー 138
目的 34
ユーザーアカウント 38
削除 259
リソース 39, 107, 109
リソースグループ 39, 116
ロール 38, 104
「Identity Manager アカウントの削除」ボタン 259
Identity Manager イベントグループ外部での変更 428
Identity Manager 作業項目 196
Identity Manager 用語 513
Identity System 属性名 116

IDMXUser 458
ID、ユーザーアカウント 64
Import/Export Administrator 機能 180
Import User 機能 180
installdir 301

J

JMS 設定、PasswordSync 295
JMS リスナーアダプタ、PasswordSync 用に設定 302

L

LDAP
  Active Sync 設定 506
  サーバー 164
  リソースクエリー 263, 270
lh コマンド
  license 486
  syslog 487
  クラス 484
  コマンド引数 484
  使用法 483
License Administrator 機能 181
license コマンド 486
Lighthouse
  タスクマトリックス 414
Login Administrator 機能 181

M

ManageResource ワークフロー 108
Microsoft .NET 1.1 291
Microsoft .NET 1.1 のインストール 291
MySQL 監査スキーマ 496

O

objectType 435
Oracle 監査スキーマ 493
Organization Administrator 機能 181

P

Password Administrator 機能 181
PasswordSync
  JMS 設定 295
  JMS リスナーアダプタ、設定 302
  アンインストール 302
  以前のバージョンのアンインストール 291
  インストール 292
  インストールの前提条件 290
  概要 290
  サーバー設定 294
  設定 292, 293
  通知の設定 304
  デバッグ 299
  電子メール設定 297
  トレースログ 299
  配備 302
  プロキシサーバー設定 294
  ユーザーパスワード同期ワークフロー 303
  よくある質問 328
  レジストリキー 300
PasswordSync のアンインストール 302
PasswordSync の以前のバージョンのアンインストール 291
PasswordSync のインストール
  前提条件 290
  手順 292
PasswordSync のデバッグ 299
PasswordSync の配備 302
Policy Administrator 機能 181

R

Reconcile Administrator 機能 182
Reconcile Report Administrator 機能 182
Reconcile Request Administrator 機能 182
Remedy Integration Administrator 機能 182
Remedy との統合 148
Rename User 機能 182
Report Administrator 機能 182
Reset Password Administrator 機能 182
Reset Resource Password Administrator 機能 183
Resource Administrator 機能 183
Resource Group Administrator 機能 183
Resource Object Administrator 機能 183
Resource Password Administrator 機能 183
Resource Report Administrator 機能 183
Risk Analysis Administrator 機能 183
Role Administrator 機能 184
Role Report Administrator 機能 184

S

Security Administrator 機能 186
Service Provider Edition
  委任された管理 463
  監査グループの設定 482
  管理者ロール委任の有効化 464
  管理者ロールの作成 465
  検索のデフォルト設定 453
  コールアウト設定 452
  初期設定 445
  追跡イベント設定 450
  同期の設定 480
  トランザクション持続ストア 457
  トランザクション処理の詳細設定 458
  トランザクションデータベースの設定 448
  トランザクションの監視 460
  トランザクションのデフォルト設定 454
  ユーザーアカウントの検索 471
  ユーザーアカウントの削除 474
  ユーザーアカウントの作成 469
Service Provider Edition ユーザーの管理 468
soapClientTimeout 301
Solaris
  サポート 31
  パッチ 31
SSL 接続、テスト 342
Sybase 監査スキーマ 498
syslog コマンド 487

T

Task Report Administrator 機能 187

U

Unassign User 機能 187
Unassign コマンド 86
Unlink User 機能 187
Unlink コマンド 86
Unlock User 機能 187
updateUser 256
Update User 機能 187
Update コマンド 86
User Account Administrator 機能 188
user.global.email 属性 276
User Report Administrator 機能 188
user.waveset.accountId 属性 276
user.waveset.organization 属性 276
user.waveset.resources 属性 276
user.waveset.roles 属性 276

V

View User 機能 188

W

waveset.accountId 属性 284
Waveset Administrator 機能 188
waveset.logattr テーブル 434
waveset.log テーブル 432
Windows Active Directory リソース 164
WSUser オブジェクト 429

X

X509 証明書 subjectDN を使用した相関 341
X509 証明書ベースの認証 339
XML ファイル
  承認フォーム 277, 278
  抽出 210
  読み込み 211

あ

アイデンティティーイベント 137
アイデンティティー監査
  説明 355
  タスク 414
アイデンティティーシステムのパラメータ、リソース 113
アイデンティティー属性
  設定 131
アイデンティティーテンプレート 113
アカウント ID
  承認のエスカレーション用 273
  承認用 267
  追加の承認者 268
  通知の受信者 262
アカウントインデックス
  検査 221
  検索 220
  操作 220
  レポート 236
アカウントインデックスレポート
  必須機能 182
「アカウント」エリア、管理者インタフェース 68
アカウント管理イベントグループ 425
アカウント属性 112, 115
アクション 435
  拡張 430
アクションキーテーブル 499
アクションステータスキーテーブル 499
アクセススキャン
  作成 397
  変更 405
アクセスレビュー 392
アクセスレビューの管理 402
アテステーション
  エンタイトルメントの承認 407
  管理 406
アプリケーション、アクセスの無効化 336
暗号化
  暗号化キー 344
  概要 343
  保護されるデータ 343
暗号化キー、サーバー 344

い

一括アクション
  アクションリスト 85
  確認規則 98, 99
  相関規則 98, 99
  タイプ 84
  表示属性 88
  ユーザーアカウント 84
一括機能
  Bulk Account Administrator 176
  Bulk Change Account Administrator 176
  Bulk Change User Account Administrator 177
  Bulk Create User 177
  Bulk Delete IDM User 177
  Bulk Deprovision User 177
  Bulk Disable User 177

Bulk Enable User 177
Bulk Unassign User 178
Bulk Unlink User 178
Bulk Update User 178
Bulk User Account Administrator 178
一括リソースアクション 118
「一般」タブ
設定 258 ～ 260
説明 257
委任された管理 152
イベント、監査の作成 419
イベントグループ
Identity Manager 外部での変更 428
アカウント管理 425
コンプライアンス管理 425
セキュリティー管理 427
属性 423
タスク管理 427
リソース管理 426
ロール管理 427
ログイン / ログオフ 426
イベントタイプ 508

え

エスカレーションされた承認
承認者 273
タイムアウト 269, 270, 271, 272, 273

お

オブジェクト、Identity Manager 37, 42
オブジェクトキータイプテーブル 499
オンラインヘルプ 53
オンラインマニュアル検索のワイルドカード 489

か

改ざん、防止 437
ガイダンス、Identity Manager 53, 56
確認規則 98, 99
カスタムリソース 109
仮想組織
概要 164
更新 166
削除 166
監査
extendedActions 430
extendedResults 431
extendedTypes 428
filterConfiguration 423
概要 418
セッション 418
設定 279 ～ 280, 422
データ記憶領域
waveset.log 432
waveset.logattr 434
ビューハンドラ 418
プロビジョニングツール 418
ログデータベースキー 435
ワークフロー 418, 419
監査イベント、作成 419
監査スキャン 377
監査設定 422
監査設定グループ 147
監査、タスクテンプレートの設定 257
「監査」タブ
設定 279 ～ 280
説明 279
監査ポリシー
概要 360
規則の作成 368
規則のデバッグ 376
作成 362
是正者の割り当て 373
是正ワークフローのインポート 363
必須機能 175
編集 372
ワークフローの割り当て 374

監査ポリシー規則ウィザード 368
監査ポリシー規則のデバッグ 376
監査レポート 380
  Auditor Report Administrator の機能 176
  作成 381
監査ログ
  改ざんの検出 437
  改ざん防止 437
  データベースマッピング 499
監査ログのマッピング 499
監査ログレポート機能の実行 184
カンマ区切り値 (CSV) 形式、「CSV 形式」を参照
管理、Identity Manager について 152
管理、委任 152
管理者
  作成 153
  名前の表示のカスタマイズ 158
  パスワード 156
  秘密の質問 158
  ビューのフィルタ 155
管理者インタフェース 48
  「アカウント」エリア 68
管理者リスト
  承認者の選択 268, 271, 274
  通知の受信者の選択 262, 264
管理者ロール
  概要 41, 189
  作成と編集 191
  ユーザーフォームの割り当て 195
  ユーザーロール 190
管理する組織
  範囲 193
  ユーザーの割り当て 154
管理する組織の範囲の設定 193
「管理するリソース」ページ 109

き

キー
  ゲートウェイ 347
  サーバー暗号化 344
規則
  アクセスレビュー 396
  現在の設定 287
  修正 51
  職務分掌 363
  データ変換用 287
  評価によりアカウント ID を取得 262, 263, 268, 269, 274
  プロビジョニング解除用 286
  プロビジョニング用 282, 284, 285
  ユーザーメンバーの例 163
規則に基づく割り当て 161
機能
  概要 166
  カテゴリ 167
  作成 167
  実用上の階層 168
  定義の表 174
  名前の変更 167
  編集 167
  ユーザーの割り当て 154
  割り当て 168
共通リソース、認証の設定 338

く

クエリー
  LDAP リソース 263, 270
  承認者のアカウント ID の取得 268, 270, 274
  属性の比較 264, 270
  通知の受信者のアカウント ID の取得 262, 263
  ヘルプとマニュアル 54
  リソース属性 264, 270
グラフ形式のレポート 242
グローバルリソースポリシー 117

け

ゲートウェイキー 347
結果 435
　拡張 431
検索
　サービスプロバイダトランザクション 460
　ヘルプとマニュアル 53
　ユーザーアカウント 69
検出、ログの改ざん 437

こ

コンプライアンス管理イベントグループ 425

さ

サーバー暗号化
　管理 343, 349
　キー 344
サーバー暗号化の管理 349
サーバーのデフォルト設定 150
サービスプロバイダエンドユーザーインタフェース 476
サービスプロバイダユーザータイプ 36
サービスプロバイダユーザーの検索 471
再試行リンク、設定 280
作業項目
　委任 198
　管理 196
　タイプ 196
　保留中 49
　履歴の表示 197
作業項目の委任 198
削除
　削除タスクの保留 257
　ユーザーアカウント 80, 257, 259
作成
　アクセススキャン 397
　監査ポリシー 362
　監査ポリシー規則 368
作成タスク、保留 257
サポート
　Solaris 31
サンセット
　設定 281
　プロビジョニング解除 285
サンライズ
　新しいユーザーのプロビジョニング 281
　設定 281
「サンライズとサンセット」タブ
　設定 281 ～ 286
　説明 257

し

自己検索 97
辞書ポリシー
　概要 141
　実装 142
　設定 141
　選択 92
実行機能
　Run Admin Report 184
　Run Audit Report 184
　Run Reconcile Report 185
　Run Resource Report 185
　Run Risk Analysis 185
　Run Role Report 185
　Run Task Report 185
　Run User Report 185
実用上の機能 167
指定
　アカウントデータの属性 257
　通知の受信者 262, 263, 264
　ユーザー通知 265
承認
　エスカレーション 269, 270, 271, 272, 273
　カテゴリ 200
　設定 266 ～ 278

フォーム 275
無効化 257
有効化 257, 267
承認者
設定 266
セットアップ 201
組織 267
追加 257, 266, 267 ～ 275
通知の設定 261
リソース 267
ロール 267
「承認」タブ
概要 257
設定 266 ～ 278
説明 257, 266
「承認のエスカレーション」ボタン 273
承認の無効化 257, 267
証明書ベースの認証 339
署名付き承認、設定 204

す

スキーママップ 116
スケジューラの設定 149
ステータスインジケータ、ユーザーアカウント 69

せ

制約規則、ログイン 334
セキュリティー
機能 332
パススルー認証 334
パスワード管理 333
ベストプラクティス 351
ユーザーアカウント 65
セキュリティー管理イベントグループ 427
是正
違反の受け入れ 389
違反の是正 390
概要 383
必須機能 176
標準是正ワークフロー 384
リクエストの転送 391
リクエストの表示 386
ワークフローの割り当て 374
セッション監査 418
セッション制限、設定 336
設定 137
Identity Manager サーバーの設定 148
PasswordSync 292, 293
Service Provider Edition 445
アイデンティティーイベント 137
アイデンティティー属性 132
「一般」タブ 258, 260
監査 279, 280
監査グループ 147
「監査」タブ 279, 280
「サンライズとサンセット」タブ 281, 286
承認 266, 278
承認フォーム 275
署名付き承認 204
タイムアウト 272, 273, 275
タスクテンプレート 256
タスクテンプレートの監査 257
追加の承認者 257
通知 261, 265
電子メール通知 257
同期 222
「プロビジョニング」タブ 280
ユーザー更新テンプレート 258
ユーザー作成テンプレート 258
設定、監査 422
「選択している属性の削除」ボタン 277, 278, 280

そ

相関規則 98, 99
属性
user.global.email 276
user.waveset.accountId 276

user.waveset.organization 276
user.waveset.resources 276
user.waveset.roles 276
waveset.accountId 284
アカウント ID の取得 262, 267, 268, 273
アカウントデータから指定 257
値の編集 276, 278
クエリーの作成 264
承認フォームからの削除 277
承認フォームへの追加 277
タスク承認のための指定 266
タスク名での指定 258
デフォルト 276, 277
デフォルトの表示名 278
ユーザーアカウント 66
「属性の追加」ボタン 277, 279
組織
概要 40, 159
仮想 164
管理割り当て 163
作成 159
ユーザーの割り当て 161
組織の承認 267

た

タイプ、拡張 428
タイムアウト
エスカレーションされた承認 269, 270, 271, 272, 273
設定 272, 273, 275
タイムアウト値、設定 336
「タイムアウトのアクション」ボタン 272
タスク
アイデンティティー監査 414
クイックリファレンス 58
再試行 257
サンライズ / サンセット 257
バックグラウンドでの実行 257
保留 257
タスク管理イベントグループ 427
タスクテンプレート
設定 256
プロセスタイプのマッピング 253
編集 256
有効化 253, 256
ユーザー更新テンプレート 253
ユーザー削除テンプレート 253
ユーザー作成テンプレート 253
タスクテンプレートの編集ページ
ユーザー更新テンプレート 256, 258
ユーザー削除テンプレート 256, 259
ユーザー作成テンプレート 256, 258
タスクの再試行 257
「タスクの実行」ボタン 275
「タスクの設定」タブ 257
タスクの保留 257
タスクベースの機能 167
タスク名
属性参照 258
定義 257, 258
ダッシュボード、レポートのグループ化 246
タブ
一般 257
サンライズとサンセット 257
承認 257
タスクの設定 257
通知 257
データ変換 257
プロビジョニング 257
探索
概要 210
ファイルから読み込み 211
ファイルへ抽出 210
リソースから読み込み 214

ち

調整
開始 219
概要 215

ステータスの表示 219
ポリシー 216
ポリシー、編集 216
調整サーバーの設定 148
調整レポート 182

つ

通知
PasswordSync での設定 304
設定 261 ～ 265
ユーザーアカウントデータの変換 287
「通知」タブ
設定 261 ～ 265
説明 257
通知の受信者
アカウント ID の取得 262
管理者リストからの指定 264
規則による指定 263
クエリーによる指定 263
属性による指定 262
ユーザーの指定 265

て

定期的アクセスレビュー
アクセススキャン 397
エンタイトルメント 407
概要 392
起動 403
計画 395
終了中 405
進行状況の管理 404
スケジュール 403
認証 393
レポート 410
ワークフロープロセス 393
ディレクトリジャンクション
概要 164
セットアップ 165
ディレクトリリソース 164
データの同期
ActiveSync アダプタ 222
探索 210
調整 215
ツール 209
データベース
DB2 495
MySQL 496
Oracle 493
Sybase 498
キー 435
理由 436
キーマッピング 499
スキーマ 432
データ変換
プロビジョニング中 286
プロビジョニング前 257
「データ変換」タブ
設定 286
説明 257
デフォルト
承認の有効化 267
承認フォームの属性 276, 277
属性の表示名 278
タスク名 258
プロセスタイプ 255
電子メール設定、PasswordSync 297
電子メール通知、設定 257, 261
電子メールテンプレート 263, 265
HTML とリンク 146
概要 143, 261
カスタマイズ 144
変数 146
テンプレート、電子メール 261, 263, 265

と

同期
Service Provider Edition 479

設定 222
無効化 225
同期ポリシー 222
同期モード 501
ドキュメント
Identity Manager の検索 53
概要 29
高度なクエリーを使用した検索 489
トラブルシューティング
監査ポリシー 376
トリプル DES 暗号化 344, 347
トレースログ、PasswordSync 299

に

認証 393
X509 証明書ベース 339
委任 395
共通リソースの設定 338
質問 158
ユーザー 94

は

パススルー認証 334
パスワード
管理者の認証 156
管理者の変更 156
ユーザーアカウント、「ユーザーアカウントパスワード」を参照
ログインアプリケーション 334
パスワード管理 333
パスワードポリシー
辞書ポリシー 92
実装 94
使用禁止属性 93
使用禁止単語 93
設定 91
長さ規則 91
文字タイプ規則 92
履歴 92
パスワード文字列の品質ポリシー 140
バックグラウンド、タスクの実行 257
バックグラウンドでのタスク実行 257
パブリッシャー 432

ひ

日付形式文字列 284, 285, 286
「必須のプロセスマッピング」セクション 255
ビューハンドラ監査 418
表示
作業項目履歴 197
保留中のアテステーション 407
保留中の作業項目 196
ユーザーアカウント 70
レポートのタイプ 234

ふ

ファイルへ抽出 209, 210
フィールドレベルのヘルプ 56
フォーム
現在の設定 272, 287
承認の設定 275
属性の追加 277
タスクの承認 266
通知 263
編集 51
「フォームおよびプロセスマッピングの設定」ページ 256
プロキシサーバー設定、PasswordSync 294
プロセスタイプ
createUser 255
updateUser 256
削除 255
選択 255
デフォルト 255

マッピング 253, 255, 256
プロセスマッピング
一覧表示 254
検証 256
必須 255
編集 254
有効化 254
プロセスマッピングの一覧表示 254
プロセスマッピングの検証 256
プロセスマッピングの編集ページ 254
プロビジョニング
再試行リンク 280
サンライズ 281
時刻 283
事前のデータ変換 257
データ変換 286
バックグラウンド 280
日付 283
プロビジョニング解除
サンセットの設定 285
ユーザーアカウント 80, 257, 259, 260
「プロビジョニング」タブ
設定 280
説明 257
プロビジョニングツール監査 418

へ

ページ
タスクテンプレート「Create User Template」の編集 : 256, 258
タスクテンプレート「Delete User Template」の編集 : 256, 259
タスクテンプレート「Update User Template」の編集 : 256, 258
フォームおよびプロセスマッピングの設定 256
プロセスマッピングの編集 254
ヘルプ、オンライン 53
変更機能
Change Account Administrator 178
Change Active Sync Resource Administrator 179
Change Password Administrator 179
Change Resource Password Administrator 179
Change User Account Administrator 179
編集
属性値 276, 278
タスクテンプレート 256
タスク名 258
プロセスマッピング 254

ほ

防止、改ざん 437
方法
FormUtil 284, 285
管理者への通知 261
サンライズ / サンセットの決定 281
承認者の決定 268
承認のタイムアウトの決定 269
プロビジョニング解除の決定 285
ボタン
Identity Manager アカウントの削除 259
承認のエスカレーション 273
選択している属性の削除 277, 278, 280
属性の追加 277, 279
タイムアウトのアクション 272
タスクの実行 275
マッピングの編集 254, 255
有効化 254
ポリシー
Identity Manager アカウント 138
アカウント ID 140
概要 138
監査 360
グローバルリソースポリシー 117
辞書 141
調整 216
リソースパスワード 91, 140
ポリシー違反
アクセススキャン時 398
受け入れ 389
是正 390

是正リクエストの転送 391
ポリシーの編集ページ 372

ま

マッピング
検証 256
プロセス 256
プロセスタイプ 253, 256
「マッピングの編集」ボタン 254, 255

め

メタビュー 132, 137

ゆ

有効化
承認 257, 267
承認のタイムアウト 272
タスクテンプレート 256
プロセスマッピング 254
「有効化」ボタン 254
ユーザーアカウント
ID 64
一括アクション 84
移動 73
概要 38
検索 69, 82
更新 77
削除 80, 257, 259
作成 71
自己検索 97
ステータスインジケータ 69
セキュリティー 65
属性 66
データ 63
データ変換 286
名前の変更 74
認証 94
パスワード
操作 89
変更 89
リセット 90
表示 70
プロビジョニング解除 80, 257, 259
編集 72
無効化 75
有効化 77
ロック解除 79
割り当て 65
割り当てられた監査ポリシー 66
ユーザーアカウントの移動 73
ユーザーアカウントの検索 82
ユーザーアカウントの更新 77
ユーザーアカウントの名前の変更 74
ユーザーアカウントの無効化 75
ユーザーアカウントの有効化 77
ユーザーアカウントのロック解除 79
ユーザーアカウントパスワードのリセット 90
ユーザーアクセス、定義 35
ユーザーインタフェース、Identity Manager 49
ユーザーエンタイトルメントレコード 410
ユーザー管理者ロール 190
ユーザー更新テンプレート
設定 258
説明 253
マッピングプロセス 256
ユーザー削除テンプレート
説明 253
マッピングプロセス 256
ユーザー作成テンプレート
設定 258
説明 253
マッピングプロセス 256
ユーザータイプ 36
ユーザーテンプレート
選択 256
編集 258, 259

ユーザーの削除機能 180
「ユーザーの作成」ページ 71
ユーザーパスワード同期ワークフロー 303
ユーザーフォーム 71, 155
　管理者ロールへの割り当て 195
「ユーザーメンバー規則」オプションボックス 162
ユーザーメンバー規則の例 163

よ

用語集 513
読み込み
　ファイル 209, 211
　リソース 209, 214

り

リスク分析 240
リソース 39
　Identity Manager 109
　アイデンティティーシステムのパラメータ 113
　アイデンティティーテンプレート 113
　アカウント属性 112, 115, 264
　アダプタ 110
　一括アクション 118
　概要 107
　カスタム 109
　管理 115
　グローバルリソースポリシー 117
　作成 110
　タイムアウト値の設定 117
　問い合わせ 268, 270, 274
　パラメータ 111
　リスト 109
リソースアカウント
　Identity Manager アカウントの削除 259
　プロビジョニング解除 259, 260
　リンク解除 260
　割り当て解除 81, 259, 260
リソースアカウントのリンク解除 81, 260
リソースアカウントの割り当て解除 81, 259, 260
リソースウィザード 110
「リソース」エリア 108
リソース管理イベントグループ 426
リソースグループ 39, 116
リソース属性 270
リソースの承認 267
リソースの調整 209

れ

レジストリキー、PasswordSync 300
レポート
　概要 236
　監査タイプ 380
　監査ログ 235
　グラフの定義 242
　システムログ 238
　実行 232
　使用状況 238
　スケジュール 232
　操作 229, 242
　ダッシュボードの操作 246
　定義 231
　データのダウンロード 233
　名前の変更 232
　リアルタイム 236
　リスク分析 240

ろ

ロール
　Identity Manager ロールとリソースロールの同期 107
　概要 38
　管理者 41
　作成 104
　承認 267

割り当てられているリソース属性値の編集 105
ロール管理イベントグループ 427
ログイン
アプリケーション 334
編集 335
制約規則 334
相関規則 341
モジュール
編集 337
モジュールグループ 334
編集 336
ログインアプリケーション、アクセスの無効化 336
ログイン / ログオフ監査イベントグループ 426
ログデータベースキー 435

わ

ワークフロー監査 418, 419
ワークフロー、修正 51
割り当て、ユーザーアカウント 65