Sun Identity Manager 8.1 ビジネス管理者ガイド

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

Part No: 821–0064
2009 年 2 月

090729@22510

目次

はじめに 17

1 Identity Manager の概要 23
全体像 23
Identity Manager システムの目的 24
リソースへのユーザーアクセスの定義 25
ユーザータイプについて 26
管理の委任 26
Identity Manager オブジェクト 27
Identity Manager ユーザーアカウント 27
Identity Manager ロール 28
リソースとリソースグループ 29
組織と仮想組織 30
ディレクトリジャンクション 30
Identity Manager の機能 31
管理者ロール 31
Identity Manager のポリシー 31
監査ポリシー 32
オブジェクトの関係 32

2 Identity Manager ユーザーインタフェース入門 35
Identity Manager 管理者インタフェース 35
Identity Manager 管理者インタフェースへのログイン 37
▼管理者インタフェースを開く 37
セッション制限と Cookie 37
ユーザー ID を忘れた場合 37
Identity Manager エンドユーザーインタフェース 38

エンドユーザーインタフェースの 5 つのタブ 39
Identity Manager エンドユーザーインタフェースへのログイン 41
▼ エンドユーザーインタフェースを開く 41
ユーザー ID を忘れた場合 41
ヘルプとガイダンス 41
Identity Manager ヘルプ 41
Identity Manager ガイダンス 42
Identity Manager デバッグページ 43
Identity Manager IDE 45
以降の操作について 46

3 ユーザーとアカウントの管理 49
インタフェースの「アカウント」領域 49
「アカウント」領域のアクションリスト 50
「アカウントリスト」領域での検索 50
ユーザーアカウントの状態 50
ユーザーページ (作成/編集/表示) 52
ユーザーの作成およびユーザーアカウントの操作 56
プロセス図の有効化 56
▼ Identity Manager でユーザーを作成する 57
1 人のユーザーに対する複数のリソースアカウントの作成 59
ユーザーアカウントの検索と表示 60
ユーザーの編集 61
アカウントに関連付けられたリソースの更新 64
Identity Manager ユーザーアカウントの削除 66
ユーザーアカウントからのリソースの削除 67
ユーザーパスワードの変更 71
ユーザーパスワードのリセット 73
ユーザーアカウントの無効化、有効化、およびロック解除 74
一括アカウントアクション 78
一括アカウントアクションの起動 79
相関規則と確認規則 84
アカウントセキュリティーと特権の管理 86
パスワードポリシーの設定 86
ユーザー認証 90

管理特権の割り当て 94
ユーザーの自己検索 94
自己検索の有効化 94
匿名登録 95
匿名登録の有効化 95
匿名登録の設定 97
ユーザー登録プロセス 97

4 ビジネス管理オブジェクトの設定 99
Identity Manager ポリシーの設定 99
ポリシーとは 100
ポリシーでの使用禁止属性 102
辞書ポリシーとは 102
電子メールテンプレートのカスタマイズ 104
電子メールテンプレートの編集 106
電子メールテンプレートでの HTML 形式とリンクの使用 108
電子メール本文で使用できる変数 108
監査グループおよび監査イベントの設定 109
▼「監査設定」ページを開く 109
▼監査グループを設定する 109
▼監査設定グループにイベントを追加する 110
▼監査設定グループ内のイベントを編集する 110
Remedy との統合 110
エンドユーザーインタフェースの設定 111
▼エンドユーザーインタフェースに表示される情報を設定する 111
▼エンドユーザーインタフェースでプロセスダイアグラムを有効にする 111
Identity Manager の登録 112
コンソールからの Identity Manager の登録 113
▼Identity Manager を管理者インタフェースから登録する 115
Identity Manager 設定オブジェクトの編集 116

5 ロールとリソース 119
ロールとその管理について 119
ロールとは 119
ロールタイプの使用 121

ロールの作成 124
ロールの編集と管理 135
ユーザーロール割り当ての管理 144
ロールタイプの設定 154
Identity Manager ロールとリソースロールの同期 158
Identity Manager リソースとその管理について 158
リソースとは 158
インタフェースの「リソース」領域 159
リソースリストの管理 159
▼ リソースを作成する 161
リソースの管理 165
▼ リソースアカウント属性を表示または編集する 167
リソースグループ 168
グローバルリソースポリシー 169
一括リソースアクション 170
外部リソースとその管理について 172
外部リソースとは 172
外部リソースを使用する理由 172
外部リソースの設定 173
外部リソースの作成 190
外部リソースのプロビジョニング 193
外部リソースの割り当て解除とリンク解除 197
外部リソースのトラブルシューティング 198

6 管理 199
Identity Manager の管理について 199
委任された管理 200
管理者の作成と管理 201
▼ 管理者を作成する 201
管理者ビューのフィルタ 202
管理者パスワードの変更 203
管理者のアクションの認証 204
秘密の質問の回答の変更 206
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 206
Identity Manager の組織について 207

組織の作成 207
▼組織を作成する 207
組織へのユーザーの割り当て 208
管理する組織の割り当て 211
ディレクトリジャンクションおよび仮想組織について 211
ディレクトリジャンクションの設定 212
仮想組織の更新 213
仮想組織の削除 213
機能とその管理について 214
機能のカテゴリ 214
機能の操作 215
管理者ロールとその管理について 217
管理者ロールの規則 218
ユーザー管理者ロール 219
管理者ロールの作成および編集 220
「一般」タブ 221
制御の範囲 221
管理者ロールへの機能の割り当て 226
管理者ロールへのユーザーフォームの割り当て 227
エンドユーザー組織 228
「エンドユーザーが管理する組織」規則 229
作業項目の管理 229
作業項目のタイプ 229
作業項目リクエストの操作 230
作業項目履歴の表示 230
作業項目の委任 231
ユーザーアカウントの承認 234
アカウント承認者の設定 235
承認の署名 236
デジタル署名付き承認およびアクションの設定 237
トランザクション署名の表示 241
XMLDSIG 形式の署名付き承認の設定 242

7 データの読み込みと同期 245
データ同期ツール: 最適なツールの選択 245

アカウント検出機能 246
ファイルへ抽出 246
ファイルから読み込み 247
リソースから読み込み 250
アカウント調整 251
調整の概要 251
調整ポリシーについて 251
調整ポリシーの編集 252
調整の開始 256
調整ステータスの表示 257
アカウントインデックスの操作 258
アカウントインデックスの検査 259
タスクスケジュール繰り返し規則の使用 260
Active Sync アダプタ 262
同期の設定 262
Active Sync アダプタの編集 265
Active Sync アダプタのパフォーマンスのチューニング 266

8 レポート 269
レポートの操作 270
レポートのタイプ 270
レポートの実行 270
レポートの表示 272
レポートの作成 272
レポートの編集および複製 273
電子メールによるレポートの送信 273
レポートのスケジュール 274
レポートデータのダウンロード 274
レポート出力の設定 275
Identity Manager レポート 276
監査ログレポート 276
単一ユーザー用の監査ログレポート 277
リアルタイムレポート 278
概要レポート 278
システムログレポート 281

使用状況レポート 281
ワークフローレポート 283
監査レポート 285
グラフの操作 285
定義済みのグラフの表示 286
▼ダッシュボードグラフを作成する 287
▼ダッシュボードグラフを編集する 289
▼定義したグラフを削除する 290
ダッシュボードの操作 290
▼ダッシュボードを表示する 290
▼ダッシュボードを作成する 291
ダッシュボードの編集 292
ダッシュボードの削除 292
システムの監視 293
追跡イベント設定 293
リスク分析 294
▼リスク分析レポートを作成する 294
▼リスク分析レポートをスケジュールする 295

9 タスクテンプレート 297
タスクテンプレートの有効化 297
▼プロセスタイプをマップする 298
▼タスクテンプレートを設定する 300
タスクテンプレートの設定 302
「一般」タブの設定 302
「通知」タブの設定 305
「承認」タブの設定 311
「監査」タブの設定 326
「プロビジョニング」タブの設定 327
「サンライズとサンセット」タブの設定 328
「データ変換」タブの設定 334

10 監査ログ 337
監査ログの概要 337
Identity Manager 監査の機能 338

ワークフローからの監査イベントの作成 338
com.waveset.session.WorkflowServices アプリケーション 339
標準監査イベントをログするためのワークフローの変更 340
タイミング監査イベントをログするためのワークフローの変更 341
監査設定 344
filterConfiguration 属性 344
extendedTypes 属性 350
extendedActions 属性 351
extendedResults 属性 352
publishers 属性 352
データベーススキーマ 353
waveset.log テーブル 353
waveset.logattr テーブル 355
監査ログの切り捨て 356
監査ログ設定 356
列の長さ制限の変更 356
監査ログからのレコードの削除 357
カスタム監査パブリッシャーの使用 357
▼ カスタム監査パブリッシャーを有効にする 358
コンソール、ファイル、JDBC、およびスクリプトのパブリッシャータイプ 358
JMS パブリッシャータイプ 359
JMX パブリッシャータイプ 361
カスタム監査パブリッシャーの開発 366
パブリッシャーのライフサイクル 367
パブリッシャーの設定 367
フォーマッタの開発 368
パブリッシャー/フォーマッタの登録 368

11 PasswordSync 369
PasswordSync とは 369
インストールの前提条件 373
Microsoft .NET 1.1 のインストール 373
SSL に関する PasswordSync の設定 374
PasswordSync の以前のバージョンのアンインストール 374
Windows での PasswordSync のインストールと設定 375

▼ PasswordSync 設定アプリケーションをインストールする 375
▼ PasswordSync を設定する 376
PasswordSync のサイレントインストール 384
アプリケーションサーバーへの PasswordSync の配備 386
JMS リスナーアダプタの追加と設定 386
ユーザーパスワード同期ワークフローの実装 390
通知の設定 391
Sun JMS サーバーを使用する PasswordSync の設定 392
シナリオ例 392
管理オブジェクトの作成と格納 393
このシナリオに対する JMS リスナーアダプタの設定 398
Active Sync の設定 398
設定のテスト 400
Windows での PasswordSync のデバッグ 401
Windows での PasswordSync のアンインストール 401
PasswordSync についてのよくある質問 402

12 セキュリティー 405
セキュリティー機能 405
同時ログインセッションの制限 406
パスワードの管理 406
パススルー認証 407
ログインアプリケーションについて 407
ログインアプリケーションの編集 408
ログインモジュールグループの編集 410
ログインモジュールの編集 410
共通リソースの認証の設定 413
X509 証明書認証の設定 414
設定の必要条件 414
Identity Manager での X509 証明書認証の設定 414
ログイン相関規則の作成とインポート 416
SSL 接続のテスト 417
問題の診断 417
暗号化の使用と管理 418
暗号化によって保護されるデータ 418

サーバー暗号化キーについてのよくある質問 419
ゲートウェイキーについてのよくある質問 421
サーバー暗号化の管理 423
▼「サーバー暗号化の管理」ページにアクセスする 423
▼サーバー暗号化を設定する 424
認可タイプを使用したオブジェクトのセキュリティー保護 427
セキュリティーのベストプラクティス 429
設定時 429
実行時 430

13 アイデンティティー監査: 基本概念 431
アイデンティティー監査について 431
アイデンティティー監査の目的 432
アイデンティティー監査について 433
ポリシーベースのコンプライアンス 433
定期的アクセスレビュー 434
管理者インタフェースでのアイデンティティー監査の操作 435
インタフェースの「コンプライアンス」セクションの使用法 436
アイデンティティー監査タスクのインタフェースリファレンス 437
電子メールテンプレート 437
監査ログの有効化 438
監査ポリシーについて 438
監査ポリシー規則を使用したポリシーの作成 439
是正ワークフローによるポリシー違反への対応 439
是正者の指定 439
監査ポリシーのシナリオ例 439

14 監査: 監査ポリシー 441
監査ポリシーの操作 441
監査ポリシー規則 441
監査ポリシーの作成 442
▼監査ポリシーウィザードを開く 442
監査ポリシーの作成: 概要 442
開始する前に 443
監査ポリシーの名前と説明の指定 444

規則の追加 450
是正ワークフローの選択 451
是正者と是正タイムアウトの選択 452
このポリシーにアクセスできる組織の選択 453
監査ポリシーの編集 454
ポリシーの編集ページ 454
「是正者」領域 455
是正ワークフローと組織の領域 456
サンプルポリシー 458
監査ポリシーの削除 458
監査ポリシーのトラブルシューティング 459
監査ポリシーの割り当て 459
▼ユーザーレベルのポリシーを割り当てる 460
監査機能制限の解決 460

15 監査: コンプライアンスの監視 461
監査ポリシーのスキャンとレポート 461
ユーザーおよび組織のスキャン 461
監査レポートの操作 463
コンプライアンス違反の是正と受け入れ 468
是正について 468
是正電子メールテンプレート 471
「是正」ページでの操作 471
ポリシー違反の表示 471
ポリシー違反の優先度の設定 473
ポリシー違反の受け入れ 474
ポリシー違反の是正 475
是正リクエストの転送 476
是正作業項目のユーザーの編集 476
定期的アクセスレビューとアテステーション 477
定期的アクセスレビューについて 477
定期的アクセスレビューの計画 480
アクセススキャンの作成 482
アクセススキャンの削除 488
アクセスレビューの管理 488

アテステーション作業の管理 492
アクセスレビューレポート 496
アクセスレビュー是正 498
アクセスレビュー是正について 498
アクセスレビュー是正リクエストのエスカレーション 498
是正ワークフローのプロセス 498
アクセスレビュー是正応答 499
「是正」ページ 499
サポートされないアクセスレビュー是正アクション 499

16 データエクスポータ 501
データエクスポータの概要 501
データエクスポータの実装計画 502
▼データエクスポータを実装する 502
データエクスポータの設定 503
▼データエクスポータを設定する 503
読み取り接続と書き込み接続の定義 505
ウェアハウスの設定情報の定義 507
ウェアハウスモデルの設定 508
エクスポータの自動化の設定 510
ウェアハウスタスクの設定 511
設定オブジェクトの変更 513
データエクスポータのテスト 514
▼データウェアハウスエクスポータ起動ツールを開始する 514
フォレンジッククエリーの設定 515
クエリーの作成 515
フォレンジッククエリーの保存 518
クエリーの読み込み 519
データエクスポータの維持 519
データエクスポータの監視 519
監視ログ 520

17 サービスプロバイダの管理 523
サービスプロバイダ機能の概要 523
拡張エンドユーザーページ 524

初期設定 525
メイン設定の編集 525
ユーザー検索設定の編集 534
トランザクション管理 536
デフォルトのトランザクション実行オプションの設定 536
トランザクション持続ストアの設定 539
トランザクション処理の詳細設定 540
トランザクションの監視 542
サービスプロバイダユーザーの委任管理 545
組織認証による委任 545
管理者ロール割り当てによる委任 546
サービスプロバイダユーザー管理者ロールの委任 549
サービスプロバイダユーザーの管理 550
ユーザー組織 550
ユーザーとアカウントの作成 551
サービスプロバイダユーザーの検索 554
エンドユーザーインタフェース 559
サービスプロバイダのユーザー同期 562
同期の設定 562
同期の監視 563
同期の開始と停止 563
ユーザーの移行 564
サービスプロバイダ監査イベントの設定 565

A lh リファレンス 567
lh コマンドの構文 567
使用上の注意 569
lh コマンドの例 570
syslog コマンド 570
syslog コマンドの使用法 570
syslog コマンドのオプション 570

B 監査ログデータベーススキーマ 573
Oracle データベースタイプ 573
DB2 データベースタイプ 575

MySQL データベースタイプ 577
SQL Server データベースタイプ 578
監査ログデータベースマッピング 580

C ユーザーインタフェースクイックリファレンス 587
Identity Manager インタフェースのタスクリファレンス 587

D 機能の定義 595
タスクベースの機能の定義 595
実用上の機能の定義 619

用語集 627

索引 633

はじめに

このガイドでは、Sun™Identity Manager (Identity Manager) ソフトウェアを使用して、ユーザーが企業の情報システムやアプリケーションに安全にアクセスできるように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。

対象読者

この『Sun Identity Manager 8.1 ビジネス管理者ガイド』は、Identity Manager 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を対象としています。

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)

お読みになる前に

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となる、Sun Java Enterprise System のコンポーネントです。Sun Java Enterprise System で提供されているドキュメントをよく読んでください。ドキュメントは、`http://docs.sun.com/coll/entsys_04q4` からオンラインで入手できます。

Identity Manager の配備では、Identity Manager Directory Server がデータストアとして使用されるので、製品で提供されているドキュメントをよくお読みください。Directory Server のドキュメントは、`http://docs.sun.com/coll/DirectoryServer_04q2` からオンラインで入手できます。

内容の紹介

このガイドは次の章と付録で構成されています。

第 1 章「Identity Manager の概要」では、Identity Manager とさまざまな Identity Manager オブジェクトを、動的な作業環境の管理業務でいかに役立てられるかを説明します。

第 2 章「Identity Manager ユーザーインタフェース入門」では、Identity Manager のグラフィカルユーザーインタフェースの使用方法について説明します。

第 3 章「ユーザーとアカウントの管理」では、管理者インタフェースを使用してユーザーを作成および管理する方法について説明します。

第 5 章「ロールとリソース」では、Identity Manager のロールとリソースを理解する上で役立つ情報を説明します。

第 4 章「ビジネス管理オブジェクトの設定」では、ポリシー、電子メールテンプレート、監査グループ、監査イベントなどの Identity Manager のビジネス管理オブジェクトを設定および保守する際に役立つ情報と手順を説明します。

第 6 章「管理」では、管理者インタフェースを使用してさまざまな管理者レベルのタスクを実行する方法を説明します。また、この章では、ロール、管理ロール、および機能の使用法についても説明します。

第 7 章「データの読み込みと同期」では、Identity Manager のデータ読み込み機能と同期機能を使用して、データを最新の状態に維持する方法について説明します。

第 8 章「レポート」では、Identity Manager のレポートタイプについて紹介し、レポートを作成および管理する方法を説明します。

第 9 章「タスクテンプレート」では、Identity Manager のタスクテンプレートについて紹介し、これらを使用してワークフローの動作を設定する方法を説明します。

第 10 章「監査ログ」では、Identity Manager の監査システムについて説明します。

第 11 章「PasswordSync」では、パスワードの変更を検出して同期する PasswordSync 機能のインストール、設定、および使用方法について説明します。

第 12 章「セキュリティー」では、Identity Manager を使用してシステムのセキュリティーを管理する方法について説明します。

第 13 章「アイデンティティー監査: 基本概念」では、アイデンティティー監査の概念と監査の管理について説明します。

第 14 章「監査: 監査ポリシー」では、監査ポリシーウィザードを使用して、監査ポリシーを作成および管理する方法について説明します。

第 15 章「監査: コンプライアンスの監視」では、監査レビューの実行方法と、法規制へのコンプライアンスを管理する方法について説明します。

第 16 章「データエクスポータ」では、データエクスポータ機能について紹介し、この機能を使用してユーザー、ロール、およびその他のオブジェクトタイプに関する情報を外部のデータウェアハウスに書き込む方法を説明します。

第 17 章「サービスプロバイダの管理」では、サービスプロバイダ機能を設定および管理する方法について説明します。

付録 A「lh リファレンス」では、Identity Manager のコマンド行インタフェースの使用方法について説明します。

付録 B「監査ログデータベーススキーマ」では、サポートされるデータベースタイプと監査ログ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。

付録 C「ユーザーインタフェースクイックリファレンス」では、Identity Manager で一般的に行われるタスクの実行方法を説明したクイックリファレンスを示します。

付録 D「機能の定義」では、ユーザーに割り当て可能なタスクベースの機能と実用上の機能について説明したクイックリファレンスを示します。

関連ドキュメント

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ドキュメントと情報を提供しています。Sun Identity Manager 8.1 のライブラリには、次のドキュメントが含まれます。

主な対象読者	タイトル	説明
すべてのユーザー	『Sun Identity Manager の概要』	Identity Manager の機能の概要を説明しています。製品のアーキテクチャー情報を示し、Identity Manager を Sun のほかの製品 (Sun Open SSO Enterprise、Role Manager など) と統合する方法について説明します。
	『Sun Identity Manager 8.1 リリースノート』	既知の問題、修正された問題、および Identity Manager のドキュメントセットに記載されていない最新の情報を説明しています。

主な対象読者	タイトル	説明
システム管理者	『Sun Identity Manager 8.1 Installation』	Identity Manager と、Sun Identity Manager Gateway や PasswordSync などのオプションコンポーネントのインストール方法について説明しています。
	『Sun Identity Manager 8.1 Upgrade』	古いバージョンの Identity Manager を新しいバージョンにアップグレードする方法について説明しています。
	『Sun Identity Manager 8.1 System Administrator's Guide』	システム管理者がインストールした Identity Manager の管理、調整、およびトラブルシューティングを行う際に役立つ情報と手順を説明しています。
ビジネス管理者	『Sun Identity Manager 8.1 ビジネス管理者ガイド』	Identity Manager のプロビジョニング機能および監査機能を使用する方法について説明しています。ユーザーインタフェース、ユーザーとアカウントの管理、レポートなどの情報も説明しています。
システムインテグレータ	『Sun Identity Manager Deployment Guide』	Identity Manager を複雑な IT 環境に配備する方法について説明しています。 説明している内容は、アイデンティティー属性の操作、データの読み込みと同期、ユーザーのアクションの設定、カスタムブランディングの適用などです。
	『Sun Identity Manager Deployment Reference』	ワークフロー、フォーム、ビュー、規則、および XPRESS 言語について説明しています。
	『Sun Identity Manager 8.1 Resources Reference』	リソースアダプタのインストール、設定、および使用法について説明しています。
	『Sun Identity Manager Service Provider 8.1 Deployment』	Identity Manager Service Provider の配備方法と、標準の Identity Manager 製品とのビュー、フォーム、およびリソースの違いについて説明しています。
	『Sun Identity Manager 8.1 Web Services』	SPML サポートの設定方法、サポートされる SPML 機能とその理由、およびフィールドにサポートを拡張する方法について説明しています。

これらに加え、`http://docs.sun.com` の 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。

ドキュメントの更新

このドキュメントやほかの Identity Manager のドキュメントに関する訂正や更新は、Identity Manager Documentation Updates の Web サイトに掲載されます。

http://blogs.sun.com/idmdocupdates/

RSS フィードリーダーを使用して Web サイトを定期的に確認し、更新を利用できる場合に通知を受けることができます。サイトを購読するには、フィードリーダーをダウンロードして、ページの右側の「Feeds」の下にあるリンクをクリックします。バージョン 8.0 から、メジャーリリースごとのフィードを利用できます。

関連するサードパーティー Web サイト

このドキュメントでは、サードパーティー URL を参照して、追加の関連情報を提供します。

注 – このドキュメント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。Sun は、このようなサイトまたはリソースで得られるあらゆる内容、広告、製品、およびその他素材を保証するものではなく、責任または義務を負いません。Sun は、このようなサイトまたはリソースで得られるあらゆるコンテンツ、製品、またはサービスによって生じる、または生じたと主張される、または使用に関連して生じる、または信頼することによって生じる、いかなる損害または損失についても責任または義務を負いません。

ドキュメント、サポート、トレーニング

Sun の Web サイトでは、次の追加リソースに関する情報を入手できます。

- ドキュメント (http://www.sun.com/documentation/)
- サポート (http://www.sun.com/support/)
- トレーニング (http://www.sun.com/training/)

ご意見、ご要望の送付先

Sun ではドキュメントの品質向上のため、お客様のご意見、ご要望をお受けしております。ご意見をお寄せいただくには、http://docs.sun.com にアクセスして、「Feedback」をクリックしてください。

書体の表記規則

次の表は、本書で使用する表記上の規則について説明しています。

表 P–1 書体の表記規則

字体または記号	意味	例
`AaBbCc123`	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力を示します。	`.login` ファイルを編集します。 すべてのファイルを一覧表示するには、`ls -a` を使用します。 `machine_name% you have mail.`
`AaBbCc123`	ユーザーが入力する文字を、画面上のコンピュータ出力とは区別して示します。	`machine_name%` **`su`** `Password:`
aabbcc123	変数を示します。実際の名前または値で置き換えます。	ファイルを削除するコマンドは、`rm` *filename* です。
AaBbCc123	書名、新しい用語、強調する語句を示します。	『ユーザーズガイド』の第 6 章を参照してください。 キャッシュは、ローカルに保存されたコピーです。 ファイルを保存しないでください。 注意: 一部の強調語句は、オンラインでは太字で示されます。

コマンドのシェルプロンプトの例

次の表は、C シェル、Bourne シェル、および Korn シェルの、デフォルトの UNIX® システムプロンプトとスーパーユーザーのプロンプトを示しています。

表 P–2 シェルプロンプト

シェル	プロンプト
C シェル	`machine_name%`
C シェル (スーパーユーザーの場合)	`machine_name#`
Bourne シェルおよび Korn シェル	`$`
Bourne シェルおよび Korn シェル (スーパーユーザーの場合)	`#`

◆ ◆ ◆ 第 1 章

1 Identity Managerの概要

Sun 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管理および監査できます。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。

この章は次のトピックで構成されています。

- 23 ページの「全体像」
- 27 ページの「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必要とされます。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。現在では、アクセス管理は、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います。

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、企業内および企業外のユーザー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要求に直面しています。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し、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、という主要な課題を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設定できます。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 はこれらの機能を拡張して、エクストラネットユーザーも管理できるようにしました。

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。
- 各ユーザーの一連のアカウント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設定する。
- 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。

リソースへの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あり、従業員、顧客、パートナー、サプライヤ、買収した会社などが含まれます。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 つ以上のアイデンティティーを持つ場合が多いため、Identity Manager では単一の仮想 ID を作成して異種のリソースにマップします。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。

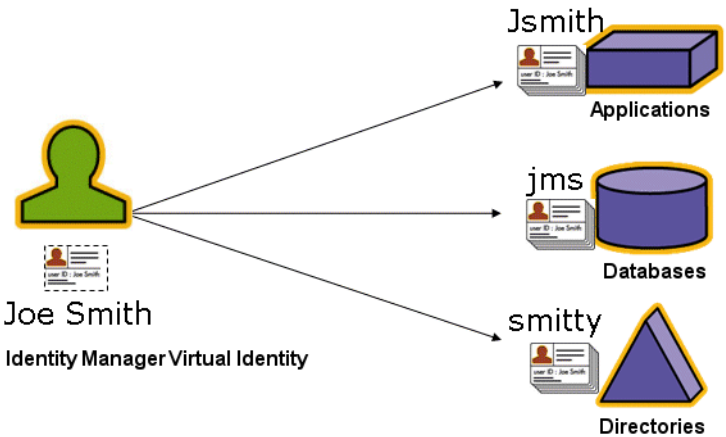


図 1–1　Identity Manager ユーザーアカウントとリソースの関係

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職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」と認識します。

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設定します。

ユーザータイプについて

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で設定する場合に使用する「サービスプロバイダユーザー」の 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 (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) を区別できます。

サービスプロバイダ実装で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実装の設定については、『Sun Identity Manager Service Provider 8.1 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 17 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

ユーザーのアイデンティティー管理の責任をうまく分散させるには、柔軟性と管理のバランスを適切にとる必要があります。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、『Sun Identity Manager Deployment Reference』の第 1 章「Workflow」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。

- 27 ページの「Identity Manager ユーザーアカウント」
- 28 ページの「Identity Manager ロール」
- 29 ページの「リソースとリソースグループ」
- 30 ページの「組織と仮想組織」
- 30 ページの「ディレクトリジャンクション」
- 31 ページの「Identity Manager の機能」
- 31 ページの「管理者ロール」
- 31 ページの「Identity Manager のポリシー」
- 32 ページの「監査ポリシー」
- 32 ページの「オブジェクトの関係」

注 – Identity Manager オブジェクトに名前を付けるときは、次の文字を使用しないでください。

' (アポストロフィー)、. (ピリオド)、| (パイプ)、[(左角括弧)、] (右角括弧)、, (コンマ)、: (コロン)、$ (ドル記号)、" (二重引用符)、\ (円記号)、= (等号)

また、_ (下線)、% (パーセント記号)、^ (キャレット)、および * (アスタリスク) の使用も避けてください。

Identity Manager ユーザーアカウント

ユーザーとは、Identity Manager システムアカウントを所有する個人です。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ます。これらの情報をまとめて、特定のユーザーの Identity Manager アイデンティティーを構成します。

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。
- ロールが割り当てられる。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。アカウントの設定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。

管理者とは、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する追加特権を持つユーザーです。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。

ユーザーアカウントの詳細については、第 3 章「ユーザーとアカウントの管理」を参照してください。管理者アカウントの詳細については、第 6 章「管理」を参照してください。

Identity Manager ロール

ロールは Identity Manager オブジェクトであり、リソースのアクセス権限をグループ分けし、ユーザーに効率的に割り当てることができるようにします。ロールは、次の 4 つのロールタイプに分けられます。

- ビジネスロール
- IT ロール
- Applications
- アセット

ビジネスロールは、組織内で類似のタスクを実行するユーザーがジョブの遂行に必要とするアクセス権をグループに編成します。通常、ビジネスロールはユーザーの職務機能を表します。

IT ロール、アプリケーション、およびアセットは、リソースの権利 (つまりアクセス権) をグループに編成します。ユーザーがリソースにアクセスできるようにするには、IT ロール、アプリケーション、およびアセットをビジネスロールに割り当てて、ジョブの実行に必要なリソースにユーザーがアクセスできるようにします。

IT ロール、アプリケーション、およびアセットは、必須、条件付き、オプションのいずれかにできます。

- 「必須ロール」は、常にユーザーに割り当てられます。
- 「条件付きロール」を割り当てるには、条件が true に評価される必要があります。
- 「オプションロール」は個別に要求することができ、承認されるとユーザーに割り当てられます。

ロールは条件付きまたはオプションにできるため、職務内容が同じユーザーに対して、同じビジネスロールを割り当てると同時に、異なるアクセス権を設定できます。この方法により、ビジネスロールの設計者はロールへのアクセスを大まかに定義して法規制の順守をはかり、ユーザーのマネージャーはユーザーのアクセス権を柔軟に調整できます。この方法では、企業内のアクセスニーズの順列ごとにビジネスロールを新たに定義する必要がないため、「ロールエクスプロージョン」と呼ばれる問題が発生しません。

ユーザーには 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可能です。

注 – ロールの詳細については、119 ページの「ロールとその管理について」を参照してください。

リソースとリソースグループ

Identity Manager は、リソースまたはシステムへの接続方法に関する情報を格納します。Identity Manager がアクセスを提供するリソースは次のとおりです。

- デジタルリソース。たとえば次のようなもの。
  - 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)
  - Applications
  - オペレーティングシステム
  - ERP システム (SAP™ など)
- Identity Manager 外部の非デジタルリソースまたは外部リソース
  - 携帯電話
  - デスクトップコンピュータ
  - ラップトップコンピュータ
  - セキュリティーバッジ

各 Identity Manager リソースは、次の種類の情報を格納します。

- リソースパラメータ
- Identity Manager 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)

リソースをユーザーに割り当てるには、2 つの方法があります。リソースをユーザーに直接割り当てる (個別または直接の割り当てと呼ばれる) ことも、リソースをロールに割り当て、そのロールをユーザーに割り当てる (ロールベースまたは間接の割り当てと呼ばれる) こともできます。

- 個別の割り当て。リソースを個別に直接ユーザーアカウントに割り当てます。
- ロールベースの割り当て。1 つ以上のリソースをロール (アプリケーション、アセット、または IT ロール) に割り当てます。続いて、アプリケーション、アセット、または IT ロールをビジネスロールに割り当てます。最後に、1 つ以上のビジネスロールをユーザーアカウントに割り当てます。

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、168 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、設定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。

組織の詳細については、207 ページの「Identity Manager の組織について」を参照してください。

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、階層的に関連付けられた組織のセットで、ディレクトリリソースの階層型コンテナの実際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、階層型コンテナを使用して、階層的な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。

ディレクトリジャンクションの詳細については、211 ページの「ディレクトリジャンクションおよび仮想組織について」を参照してください。

Identity Manager の機能

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一連のデフォルト機能を提供しています。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。

機能の詳細については、214 ページの「機能とその管理について」を参照してください。

管理者ロール

Identity Manager 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。

管理者ロールの詳細については、217 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。

Identity Manager のポリシー

「ポリシー」では、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。「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 でパスワードを単語データベースと照合して、単純な辞書攻撃から保護することができます。

ポリシーの詳細については、100 ページの「ポリシーとは」を参照してください。

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。

監査ポリシーの詳細については、438 ページの「監査ポリシーについて」を参照してください。

オブジェクトの関係

次の表は、Identity Manager オブジェクトと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で整理されます。組織は、Identity Manager 管理者によって管理されます。 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。

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
ロール	ビジネスロールは、組織内で類似のタスクを実行するユーザーがジョブの遂行に必要なアクセス権をグループに編成します。アプリケーションおよび IT ロールはリソースをグループに編成し、ビジネスロールを使ってリソースをユーザーに割り当てられるようにします。ロールベースのリソース割り当てにより、大規模な組織でのリソース管理が簡単になります。	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は、アセット、アプリケーション、および IT ロールに割り当てられます。 ユーザーアカウント。類似した特性を持つユーザーアカウントは、ビジネスロールに割り当てられます。 アセット、アプリケーション、および IT ロール。アセット、アプリケーション、および IT ロールは、ビジネスロールに割り当てられます。
Resource	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。リソースはアプリケーションおよび IT ロールに割り当てられ、これらのロールはビジネスロールに割り当てられます。ユーザーアカウントは、ビジネスロールの割り当てからリソースアカウントをゆるやかに「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。リソースグループはロールに割り当てられます。ユーザーアカウントは、ビジネスロールの割り当てから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。

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
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。組織内の管理者は、一部またはすべてのリソースにアクセスできます。 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	階層的に関連付けられた組織のセットで、ディレクトリリソースの階層型コンテナの実際のセットをミラー化したものです。	組織。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。
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 ユーザーインタフェース入門

この章では、Identity Manager のグラフィカルユーザーインタフェース (UI) と、Identity Manager をすぐに使用できるようにする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。

- 35 ページの「Identity Manager 管理者インタフェース」
- 37 ページの「Identity Manager 管理者インタフェースへのログイン」
- 38 ページの「Identity Manager エンドユーザーインタフェース」
- 41 ページの「Identity Manager エンドユーザーインタフェースへのログイン」
- 41 ページの「ヘルプとガイダンス」
- 43 ページの「Identity Manager デバッグページ」
- 45 ページの「Identity Manager IDE」
- 46 ページの「以降の操作について」

Identity Manager 管理者インタフェース

Identity Manager システムには、ユーザーがタスクを実行する際に使用できる、主要なグラフィカルインタフェースが 2 つ用意されています。それは、エンドユーザーインタフェースと管理者インタフェースです。エンドユーザーインタフェース (または「ユーザーインタフェース」) については、38 ページの「Identity Manager エンドユーザーインタフェース」で説明します。ここでは、管理者インタフェースについて説明します。

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使用して、Identity Manager システム内のユーザーの管理、リソースの設定と割り当て、権限とアクセスレベルの定義、およびコンプライアンスの監査を実行します。

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のタブ。各インタフェースページの上部に表示され、主な機能領域への移動に使用します。
- サブタブまたはメニュー。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、機能領域内のタスクにアクセスできます。

「アカウント」など、一部の領域では、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。

注 – UI を使用して管理タスクを実行する際のクイックリファレンスについては、付録 C「ユーザーインタフェースクイックリファレンス」を参照してください。

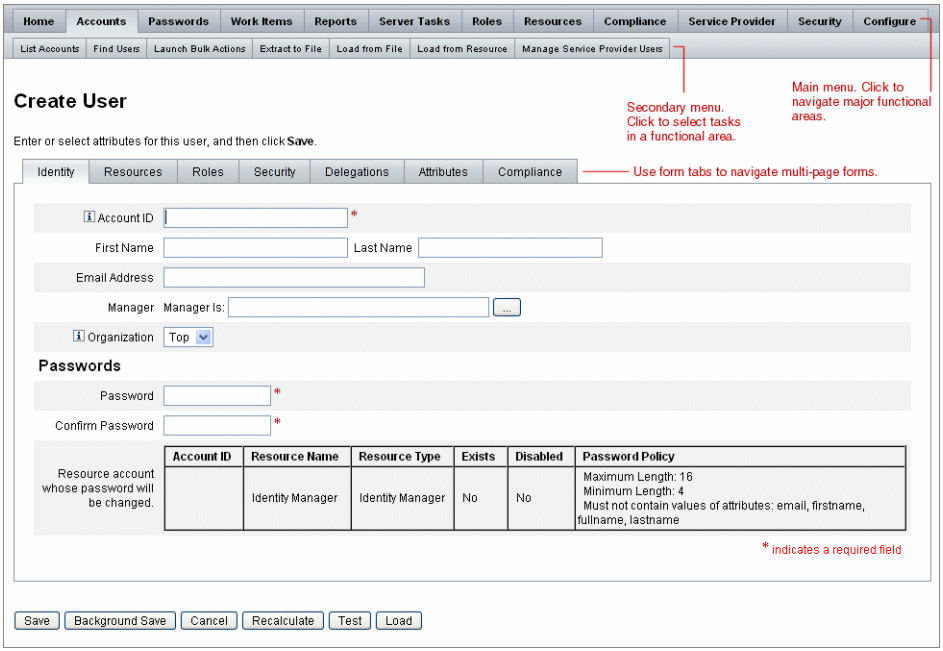


図 2–1　Identity Manager 管理者インタフェース

Identity Manager 管理者インタフェースへのログイン

▼ 管理者インタフェースを開く

1 **Web** ブラウザを開き、次の **URL** をアドレスバーに入力します。

`http://<AppServerHost>:<Port>/idm/login.jsp`

2 ユーザー **ID** とパスワードを入力して、「ログイン」をクリックします。

ユーザー ID に機能および管理する組織が割り当てられている場合、管理者インタフェースが開きます。

セッション制限と Cookie

管理者の Web ブラウザで Cookie が有効になっている場合、セッション制限で設定された時間まで、管理者インタフェースにログオンした状態が維持されます。ブラウザで Cookie が無効になっている場合、特定の操作を行うとセッション中に再ログインするよう求められます。

これらの操作には次のものがあります。

- 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。

ユーザー ID を忘れた場合

Identity Manager では、管理者は自分の忘れたユーザー ID を取得できます。管理者がログインページで「ユーザー ID をお忘れですか?」をクリックすると、問い合わせページが表示され、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 (姓名、電子メールアドレス、電話番号など) の入力を要求されます。

Identity Manager は、入力された値に一致する 1 人のユーザーを検索す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。

問い合わせ機能はデフォルトで有効になっていますが、次のいずれかの操作を実行し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。
- システム設定オブジェクトを編集し、`admin` 属性または `user` 属性、あるいはその両方で `disableForgotUserId` 属性の値を true に設定します。

  システム設定オブジェクトの編集方法については、116 ページの「Identity Manager 設定オブジェクトの編集」を参照してください。

注 – 古いバージョンの Identity Manager を 8.1 にアップグレードした場合、「ユーザー ID をお忘れですか?」機能はデフォルトで無効になります。

この機能を有効にするには、システム設定オブジェクトの次の属性を変更する必要があります (116 ページの「Identity Manager 設定オブジェクトの編集」)。

```
ui.web.user.disableForgotUserId = false
ui.web.admin.disableForgotUserId = false
```

表示されるユーザー属性名は、システム設定属性の `security.authn.lookupUserIdAttributes.<Administrator Interface | User Interface>` によって設定されます。指定できる属性は、`IDM Schema Configuration` 設定オブジェクトでクエリー可能な属性として定義されている属性です。

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 エンドユーザーインタフェース

Identity Manager エンドユーザーインタフェース (または、Identity Manager ユーザーインタフェース) は、Identity Manager システムの制限されたビューを提供します。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。

注 – エンドユーザーインタフェースにログオンする方法については、41 ページの「Identity Manager エンドユーザーインタフェースへのログイン」を参照してください。

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。

ユーザーがエンドユーザーインタフェースのログインページでリンクをクリックしてアカウントを要求できるように、Identity Manager を設定できます。詳細については、95 ページの「匿名登録」を参照してください。

エンドユーザーインタフェースの 5 つのタブ

エンドユーザーインタフェースは、5 つのセクションで構成されます。

「ホーム」タブ

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、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 (次の図を参照)。

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。ユーザーはリスト内の項目をクリックして、作業項目リクエストへの応答や、ほかの可能な操作を実行できます。

「作業項目」タブ

「作業項目」タブは、さらに「承認」、「アテステーション」、「是正」、および「その他」のタブに分かれています。このユーザーインタフェース領域では、ユーザーは所有している、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拒否できます。

「リクエスト」タブ

「リクエスト」タブには、「リクエストの起動」と「表示」の 2 つのサブタブが存在します。

「リクエストの起動」タブには、「自分のロールの更新」と「自分のリソースの更新」の 2 つの選択肢があります。

- 「自分のロールの更新」ページでは、ユーザーは自分に適した使用可能なロールのリストからリクエストを実行できます。エンドユーザーがロールリクエストを送信すると、作業項目が生成され、そのロールの指定された承認者に承認通知が送信されます。エンドユーザーは、1 つ以上のロールからの削除または割り当て解除もリクエストできます。

  エンドユーザーがアクセスをリクエストできるオプションロールの作成方法については、第 5 章「ロールとリソース」を参照してください。
- 「自分のリソースの更新」ページでは、ユーザーは自分に適した個別リソースのリストからリクエストを実行できます。ロールリクエストの場合と同様、リソースリクエストにより生成される作業項目を処理するには、事前に承認が必要となります。

「表示」サブタブには、ユーザーが送信した要求の状態に関する詳細情報が表示されます。この領域で、ユーザーは、自分の送信したリクエストのプロセスの状態およびタスク結果を表示できます。

「委任」タブ

「委任」タブを使用すると、ユーザーは作業項目をほかの Identity Manager ユーザーに委任できます。たとえば、1 つ以上のロールを割り当てられた承認者であるユーザーは、自分の休暇中、承認作業項目が一定の期間同僚に送信されるように指定できます。「委任」ページを使用すれば、ユーザーは、管理者の補助なしで委任を作成および管理できます。

「プロファイル」タブ

エンドユーザーは自身の Identity Manager パスワードとアカウント属性の設定を、「プロファイル」タブで管理できます。このタブは、次の 4 つのサブタブに分かれています。

- 「パスワードの変更」。エンドユーザーは選択したリソースまたはすべてのリソースのパスワードを変更できます。
- 「アカウント属性」。Identity Manager によってアカウント通知が送信されるアカウントの電子メールアドレスなど、エンドユーザーは特定の属性を変更できます。
- 「秘密の質問」。ユーザーアカウントの秘密の質問と回答を管理します。
- 「アクセス権限」。現在割り当てられているロールとリソースの割り当てを一覧表示します。

Identity Manager エンドユーザーインタフェースへのログイン

Identity Manager エンドユーザーインタフェースにログインするには、次の手順を使用します。

▼ エンドユーザーインタフェースを開く

1. **Web** ブラウザを開き、次の **URL** をアドレスバーに入力します。

   `http://<AppServerHost>:<Port>/idm/user/login.jsp`

2. ユーザー **ID** とパスワードを入力して、「ログイン」をクリックします。
   エンドユーザーインタフェースが表示されます。

ユーザー ID を忘れた場合

エンドユーザーは、Identity Manager を使用してユーザー ID を回復できます。詳細については、37 ページの「Identity Manager 管理者インタフェースへのログイン」節の 37 ページの「ユーザー ID を忘れた場合」を参照してください。

ヘルプとガイダンス

タスクを正常に実行するために、ヘルプや Identity Manager ガイダンス (フィールドレベルの情報と操作手順) の参照が必要となる場合があります。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で使用できます。

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、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 (次の図を参照)。

図 2–3　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」リンクが表示され、ほかのヘルプトピックや Identity Manager の用語集に移動できます。

Identity Manager ガイダンス

Identity Manager ガイダンスは、対象に関する簡潔なヘルプです。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、「i」の文字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。

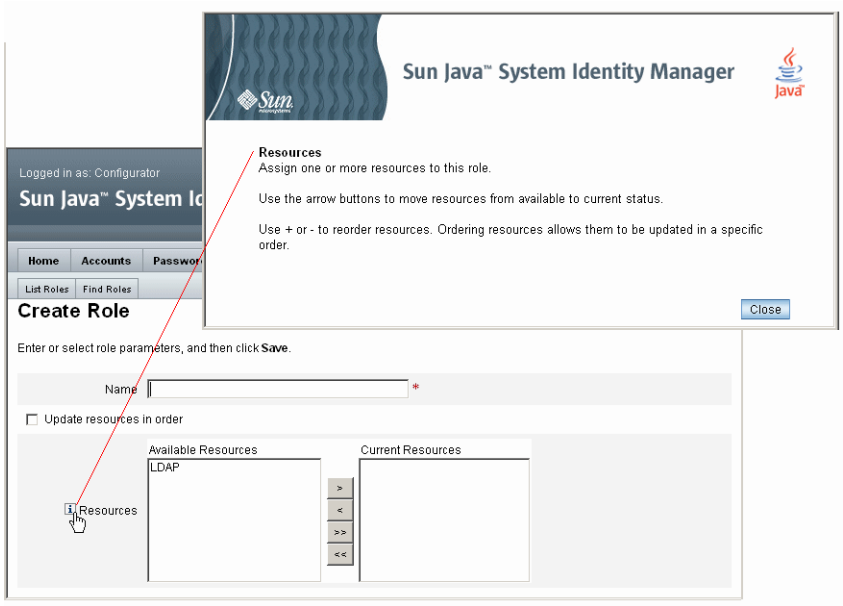


図 2–4　Identity Manager ガイダンス

Identity Manager デバッグページ

管理者インタフェースに含まれるページは、Identity Manager の最適化やトラブルシューティングが必要な場合に役立ちます。これらのページにアクセスするには、Identity Manager デバッグページを開きます。このページは、システム設定ページとも呼ばれます。

Identity Manager デバッグページを開くには、ブラウザに次の URL を入力します (プラットフォームおよび設定に応じて、URL の大文字と小文字が区別される場合があります)。

```
http://<AppServerHost>:<Port>/idm/debug/session.jsp
```

ユーザーが `/idm/debug/` ページを表示するには、デバッグ機能を使用できる必要があります。機能の詳細については、217 ページの「ユーザーへの機能の割り当て」を参照してください。

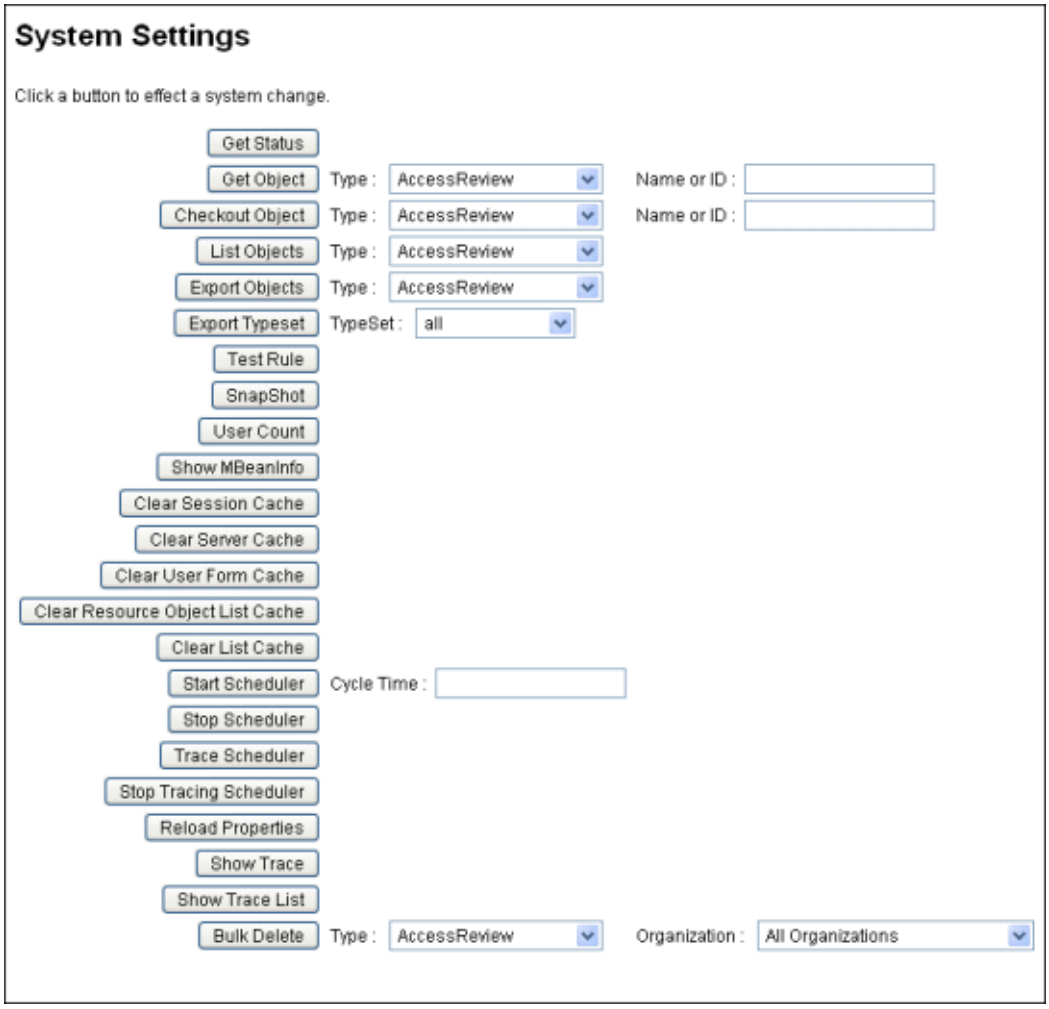


図 2–5　Identity Manager デバッグページ (システム設定)

Identity Manager のトラブルシューティングについては、『Sun Identity Manager 8.1 System Administrator's Guide』の第 5 章「Tracing and Troubleshooting」を参照してください。

Identity Manager IDE

Sun Identity Manager 統合開発環境 (Identity Manager 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。これは、Identity Manager とともに Identity Manager 配布パッケージで配布される、完全に統合された NetBeans プラグインです。

Identity Manager IDE を使用すると、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 の「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 で定義した規則も修正できます。

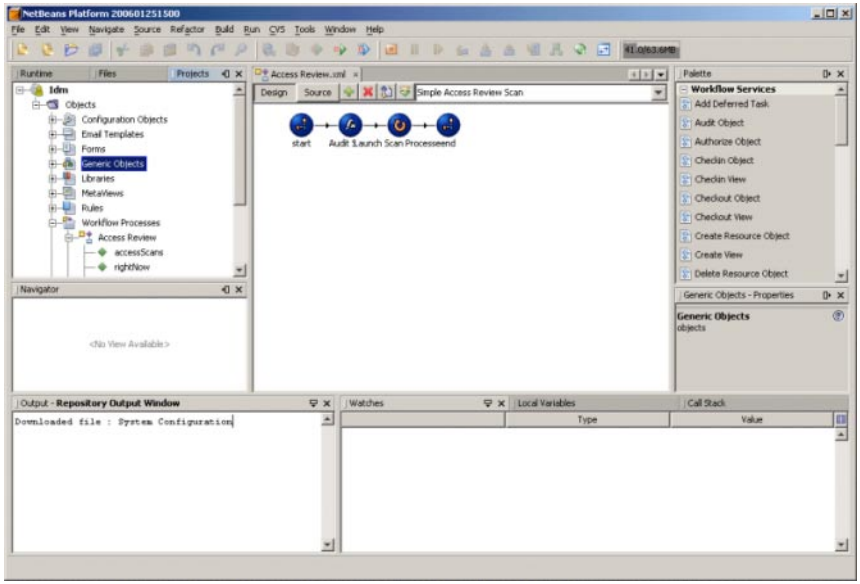


図 2–6　Identity Manager IDE インタフェース

Identity Manager IDE をダウンロードするには、次の Web サイトにアクセスしてください。

https://identitymanageride.dev.java.net/

Business Process Editor (BPE) が以前のバージョンの Identity Manager でインストールされている場合は、これを使用してカスタマイズを実行できます。

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できたら、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」領域と、ユーザーアカウントの管理手順について説明します。
第 5 章「ロールとリソース」	Identity Manager のロールとリソースの操作方法について説明します。
第 4 章「ビジネス管理オブジェクトの設定」	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 6 章「管理」	Identity Manager 管理者と組織の作成方法および管理方法について説明します。
第 7 章「データの読み込みと同期」	Identity Manager で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 8 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 9 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 10 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 11 章「PasswordSync」	Windows Active Directory ドメインでのパスワード変更と Identity Manager でのパスワード変更を同期させる、PasswordSync ユーティリティーの設定方法について説明します。
第 12 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 13 章「アイデンティティー監査: 基本概念」	監査の基本的な概念について説明します。
第 14 章「監査: 監査ポリシー」	監査ポリシーの作成方法について説明します。
第 15 章「監査: コンプライアンスの監視」	監査レビューの実施方法や、法規制へのコンプライアンス管理に役立つ手法の実装方法について説明します。
第 16 章「データエクスポータ」	データエクスポータ機能を使用すると、ユーザー、ロール、その他のオブジェクトタイプを外部のデータウェアハウスに書き込むことができます。

章のトピック	説明
第 17 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 の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「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 C「ユーザーインタフェースクイックリファレンス」	UI を使用して管理タスクを実行するのに役立つクイックリファレンス。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。
付録 D「機能の定義」	Identity Manager のデフォルトのタスクベースの機能と実用上の機能のリスト (定義を含む)。この付録では、タスクベースの各機能でアクセス可能なタブおよびサブタブも示します。

◆ ◆ ◆ 第 3 章

3 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の作成と管理の説明および手順を示します。

この情報は、次の節で構成されています。

- 49 ページの「インタフェースの「アカウント」領域」
- 56 ページの「ユーザーの作成およびユーザーアカウントの操作」
- 78 ページの「一括アカウントアクション」
- 86 ページの「アカウントセキュリティーと特権の管理」
- 94 ページの「ユーザーの自己検索」
- 95 ページの「匿名登録」

インタフェースの「アカウント」領域

Identity Manager システムアカウントを保持する者をユーザーといいます。Identity Manager は、ユーザーごとの各種データを格納します。この情報は、ひとまとめにされて、ユーザーの Identity Manager アイデンティティーを形成します。

Identity Manager の「アカウント」タブにある「ユーザーリスト」ページで、Identity Manager ユーザーを管理できます。この領域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の「アカウント」をクリックします。

アカウントリストにはすべての Identity Manager ユーザーアカウントが表示されます。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。特定の列順に並べ替えるには、その列のヘッダーをクリックします。同じヘッダーをクリックすることで、昇順と降順の並べ替えを切り替えることができます。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。

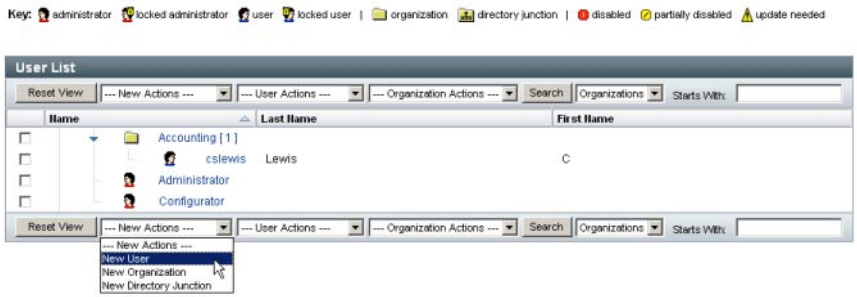
階層表示を展開して組織内のアカウントを表示するには、フォルダの隣にある三角形のマークをクリックします。表示を折りたたむには、インジケータをもう一度クリックします。

「アカウント」領域のアクションリスト

各種アクションを実行するときは、50 ページの「「アカウント」領域のアクションリスト」に示すように、「アカウント」領域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」。ユーザーの状態の編集、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」。組織とユーザーの各種アクションを実行します。



「アカウントリスト」領域での検索

ユーザーと組織を検索するときは、「アカウント」領域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 文字以上検索領域に入力して、「検索」をクリックします。「アカウント」領域での検索については、60 ページの「ユーザーアカウントの検索と表示」を参照してください。

ユーザーアカウントの状態

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の状態を表します。表 3–1 で、各アイコンが表す内容について説明します。

表 3–1 ユーザーアカウントの状態アイコンの説明

インジケータ	状態
	ユーザーの Identity Manager アカウントがロックされています。このアイコンは Identity Manager アカウントがロックされた状態にあることを表すだけで、ユーザーのリソースアカウントの状態を表すものではないことに留意してください。 Identity Manager アカウントのログイン試行の失敗回数が、Identity Manager アカウントポリシーで定義された最大数を超えると、ユーザーがロックされます。Identity Manager アカウントへのパスワードまたは質問によるログイン試行の失敗だけが、許容される最大失敗回数に数えられます。このため、Identity Manager ログインアプリケーション (管理者インタフェース、エンドユーザーインタフェースなど) のログインモジュールグループに Identity Manager ログインモジュールが含まれない場合は、Identity Manager の失敗パスワードポリシーは適用されません。ただし、特定の Identity Manager ログインアプリケーション用に設定されたログインモジュールのスタックに関係なく、質問によるログインの失敗が Identity Manager アカウントポリシーで設定された最大回数を超えると、ユーザーがロックされ、このアイコンが表示されることがあります。 アカウントのロック解除については、77 ページの「ユーザーアカウントのロック解除」を参照してください。
	管理者の Identity Manager アカウントがロックされています。このアイコンは Identity Manager アカウントがロックされた状態にあることを表すだけで、管理者のリソースアカウントの状態を表すものではないことに留意してください。詳細は、前述のユーザーロックアウトアイコンの説明を参照してください。
	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。 無効なアカウントを有効にする方法については、74 ページの「ユーザーアカウントの無効化、有効化、およびロック解除」を参照してください。
	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場合はアイコンは表示されません。

注 – Identity Manager がリストに表示された名前に一致する Identity Manager アカウントを見つけられなかった場合、「マネージャー」列にはマネージャーのユーザー名が括弧で囲んで表示されます。

ユーザーページ(作成/編集/表示)

この節では、管理者インタフェースで使用可能な「ユーザーの作成」、「ユーザーの編集」、および「ユーザーの表示」ページについて説明します。これらのページの使用方法については、この章のあとの部分で説明します。

注 – このマニュアルでは、Identity Manager の「ユーザーの作成」、「ユーザーの編集」、および「ユーザーの表示」ページの出荷時のデフォルトセットについて説明します。ただし、ビジネスプロセスや特定の管理者機能がより適切に反映されるよう、環境に合わせてカスタムのユーザーフォームを作成してください。ユーザーフォームのカスタマイズについては、『Sun Identity Manager Deployment Reference』の第 2 章「Identity Manager Forms」を参照してください。

- 52 ページの「「ID」タブ」
- 53 ページの「「リソース」タブ」
- 53 ページの「「ロール」タブ」
- 53 ページの「「セキュリティー」タブ」
- 54 ページの「「委任」タブ」
- 54 ページの「「属性」タブ」
- 55 ページの「「コンプライアンス」タブ」

Identity Manager のデフォルトユーザーページは、次のタブまたはセクションに分かれています。

- 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」タブ

「ID」領域では、ユーザーのアカウント ID、名前、連絡先情報、マネージャー、所属する組織、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 86 ページの「アカウントセキュリティーと特権の管理」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」領域を示します。

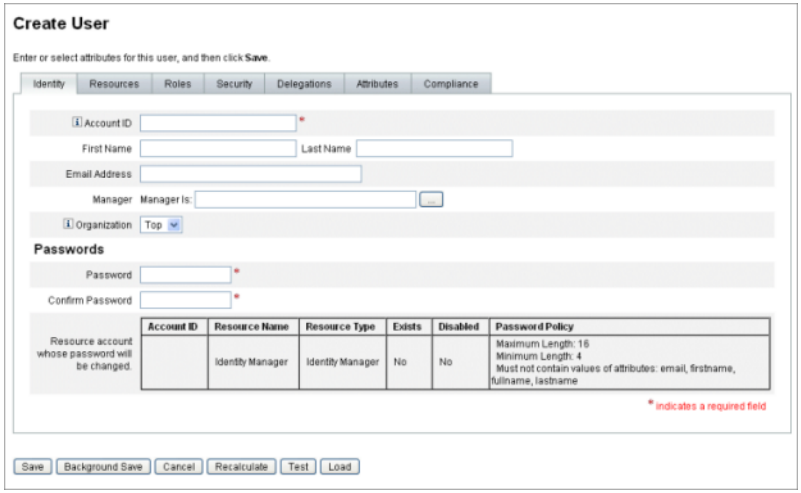


図 3–1 「ユーザーの作成」 - 「ID」

「リソース」タブ

「リソース」領域では、リソースおよびリソースグループをユーザーに直接割り当てることができます。除外するリソースを割り当てることもできます。

直接割り当てられるリソースは、「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。ロールの割り当ては、ユーザーのクラスをプロファイルします。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。

「ロール」タブ

「ロール」タブは、ユーザーに 1 つ以上のロールを割り当てたり、これらのロール割り当てを管理したりするのに使用します。

このタブについては、144 ページの「ロールをユーザーに割り当てる」を参照してください。

「セキュリティー」タブ

Identity Manager の用語では、拡張機能を割り当てられたユーザーが Identity Manager の「管理者」です。「セキュリティー」タブを使って、ユーザーに管理者特権を割り当てます。

「セキュリティー」タブを使用した管理者の作成については、201 ページの「管理者の作成と管理」を参照してください。

「セキュリティー」フォームは、次のセクションで構成されます。

- 「管理者ロール」。1 つ以上の管理者ロールをユーザーに割り当てます。ロールとは、機能および管理する組織の特定の組み合わせです。 このペアを使用することで、ユーザーに管理作業を組織的に割り当てることが容易になります。
- 「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。

  機能については、214 ページの「機能とその管理について」で説明します。タスクベースの機能と定義のリストは、付録 D「機能の定義」の付録 D「機能の定義」に示されています。この付録では、各機能でアクセス可能なタブおよびサブタブも示します。
- 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 管理者については、199 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表示フォームを継承します。
- 「アカウントポリシー」。パスワードおよび認証の制限を設定します。

「委任」タブ

「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。作業項目の委任については、231 ページの「作業項目の委任」を参照してください。

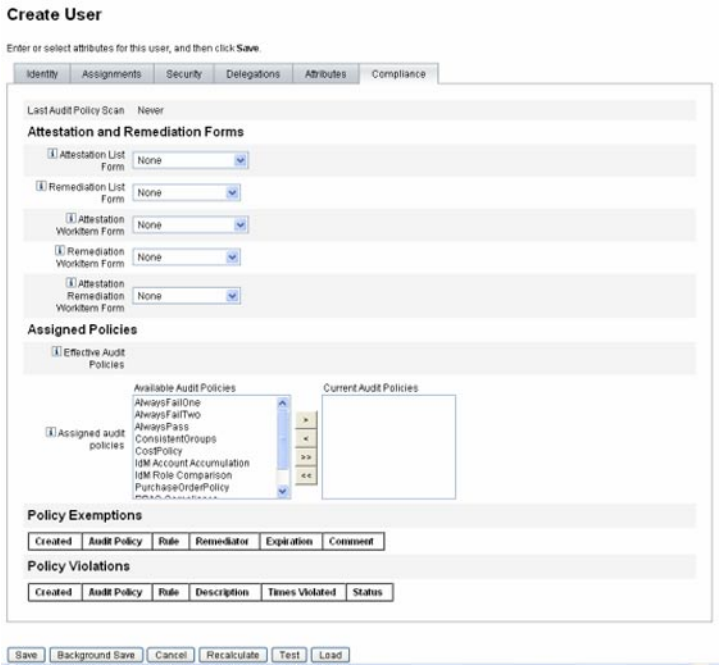
「属性」タブ

「ユーザーの作成」ページの「属性」領域では、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」タブ

「コンプライアンス」タブでは、次のことができます。

- 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。組織を介して割り当てられたポリシーについては、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状態も示されます。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。



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することによって、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できます。

ユーザーの作成および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」タブにある「ユーザーリスト」ページでは、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。

- 「管理者とユーザー」。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。

  管理者アカウントの作成と編集については、199 ページの「Identity Manager の管理について」を参照してください。
- 「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。

  組織については、207 ページの「Identity Manager の組織について」を参照してください。
- 「ディレクトリジャンクション」。階層的に関連する一連の組織を作成して、ディレクトリリソースの一連の実際の階層型コンテナをミラー化します。

  ディレクトリジャンクションについては、211 ページの「ディレクトリジャンクションおよび仮想組織について」を参照してください。

プロセス図の有効化

プロセス図には、ユーザーアカウントでの作成時やほかの操作時に Identity Manager が従うワークフローが示されます。有効にすると、Identity Manager のタスク完了時に作成される結果ページまたはタスクの概要ページにプロセス図が表示されます。

Identity Manager バージョン 8.0 では、新規インストールとアップグレードインストールの両方でプロセス図が無効に設定されていました。

▼ Identity Manager で使用するプロセス図を有効化する

1 116 ページの「Identity Manager 設定オブジェクトの編集」での手順に従って、編集するシステム設定オブジェクトを開きます。

2 次の XML 要素を見つけます。

```
<Attribute name='disableProcessDiagrams'>
  <Boolean>true</Boolean>
</Attribute>
```

3 値 true を false に変更します。

4 「保存」をクリックします。

5 変更を有効にするために、サーバーを再起動します。

プロセス図はエンドユーザーインタフェースでも有効にできますが、事前に上述の手順を実行して管理者インタフェースでプロセス図を有効にする必要があります。詳細は、111 ページの「エンドユーザーインタフェースでプロセスダイアグラムを有効にする」を参照してください。

▼ Identity Manager でユーザーを作成する

管理者インタフェースメニューバーの「アカウント」タブからユーザーを作成および管理できます。

1 管理者インタフェースで、「アカウント」をクリックします。

2 特定の組織内にユーザーを作成するには、組織を選択して、「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。

または、最上位の組織に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。

3 次のタブまたはセクションに情報を入力します。

- 「ID」。名前、組織、パスワード、およびその他の詳細。52 ページの「「ID」タブ」を参照してください。
- 「リソース」。個別のリソースおよびリソースグループの割り当て、および除外するリソース。53 ページの「「リソース」タブ」を参照してください。
- 「ロール」。ロール割り当て。ロールの詳細は、119 ページの「ロールとその管理について」を参照してください。「ロール」タブに情報を入力する手順については、144 ページの「ロールをユーザーに割り当てる」を参照してください。
- 「セキュリティー」。管理者ロール、管理する組織および機能。および、ユーザー書式設定とアカウントポリシー。53 ページの「「セキュリティー」タブ」を参照してください。
- 「委任」。作業項目の委任。54 ページの「「委任」タブ」を参照してください。
- 「属性」。割り当てられたリソースの特定の属性。54 ページの「「属性」タブ」を参照してください。

- 「コンプライアンス」。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します。コンプライアンスを使用すると、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することもできます。コンプライアンスは、ポリシーのスキャン、違反、および免除の現在の状態を示します。また、ユーザーの前回の監査ポリシースキャンの情報が含まれます。54 ページの「「属性」タブ」を参照してください。

  ある領域で利用可能な選択項目は、別の領域での選択内容により異なることに留意してください。

ビジネスプロセスや特定の管理者機能がより適切に反映されるよう、環境に合わせてユーザーフォームをカスタマイズしてください。ユーザーフォームのカスタマイズについては、『Sun Identity Manager Deployment Reference』の「Customizing Forms」を参照してください。

4 終了したら、アカウントを保存します。

ユーザーアカウントの保存には、次の 2 つのオプションがあります。

- 「Save」。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。

ステータスインジケータ	状態
	保存プロセスは進行中です。
	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、1 つ以上のエラーが発生して完了しました。

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。項目を拒否すると、アカウントの作成がキャンセルされます。サンライズの設定については、328 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。

1 人のユーザーに対する複数のリソースアカウントの作成

Identity Manager では、1 人のユーザーに複数のリソースアカウントを割り当てることができます。これには、各リソースに複数のリソースアカウントタイプまたはアカウントタイプを定義することを許可します。リソースアカウントタイプは、必要に応じ、リソースの実用上の各アカウントタイプに合わせて作成してください。たとえば、AIX SuperUser や AIX BusinessAdmin などです。

ユーザーに対してリソースごとに複数のアカウントを割り当てる理由

ある状況では、Identity Manager ユーザーはリソースに対して複数のアカウントを必要とすることがあります。ユーザーは、そのリソースに関連するいくつかの異なるジョブ機能を持つことができます。たとえば、ユーザーはそのリソースのユーザーと管理者の両方であることができます。機能ごとに別個のアカウントを使用することをお勧めします。これにより、あるアカウントが使用できなくなっても、ほかのアカウントで許可されているアクセスは引き続き保護されます。

アカウントタイプの設定

リソースで 1 人のユーザーに対する複数のアカウントをサポートするには、最初に Identity Manager でリソースのアカウントタイプを定義する必要があります。リソースに対してリソースアカウントタイプを定義するには、リソースウィザードを使用します。詳細は、159 ページの「リソースリストの管理」を参照してください。

リソースアカウントタイプは、ユーザーに割り当てる前に有効化および設定する必要があります。

アカウントタイプの割り当て

アカウントタイプを定義すると、それらをリソースに割り当てることができます。Identity Manager は、アカウントタイプの各割り当てを別個のアカウントとして扱います。そのため、ロール内の各割り当ては、それぞれ異なる属性セットを保持します。

リソースごとに 1 つのアカウントを指定する場合と同様に、特定タイプでの割り当てすべてで、割り当ての数に関係なく、アカウントが 1 つだけ作成されます。

ユーザーを割り当てることができるリソース上の異なるアカウントタイプの数は任意ですが、各ユーザーにはリソース上の指定したタイプのアカウントを 1 つ割り当てることができます。ただし、組み込み型の「デフォルト」タイプは例外です。ユーザーは、リソース上のデフォルトタイプのアカウントを任意の数だけ持つことができます。ただし、フォームやビューでアカウントを参照する際に多義的になるため、この方法は推奨されていません。

ユーザーアカウントの検索と表示

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、メニューバーから「アカウント」→「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を使用してアカウントを検索できます。

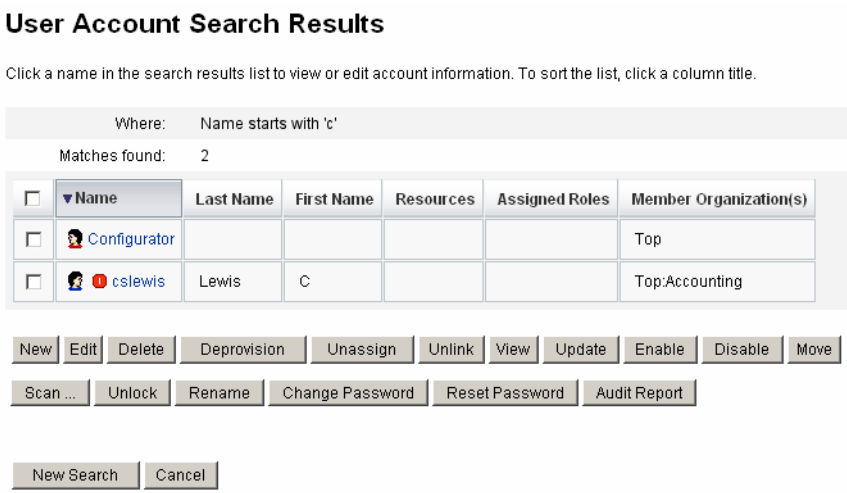
- アカウントの詳細 (ユーザー名、電子メールアドレス、姓、名など)。これらの選択肢は、機関固有の Identity Manager の実装によって異なります。
- ユーザーの管理者。ユーザー名が Identity Manager 内の既存のアカウントと一致しない場合、管理者のユーザー名が括弧内に表示されます。
- リソースアカウントの状態。次のオプションがあります。
  - 「無効」。ユーザーは、Identity Manager または割り当てられたリソースアカウントにアクセスできません。
  - 「一部無効」。ユーザーは、1 つ以上の割り当てられたリソースアカウントにアクセスできません。
  - 「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。
- 「割り当てられたリソース」。次のオプションがあります。
  - ロール (152 ページの「特定のロールに割り当てられたユーザーを検索する」を参照)
  - 所属している組織
  - 管理する組織
  - 機能
  - 管理者ロール
- 「ユーザーアカウントの状態」。次のオプションがあります。
  - 「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アクセスが制限されていません。

- 更新の状態。次のオプションがあります。
  - 「なし」。 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。

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。



ユーザーの編集

この節では、ユーザーアカウントの表示、編集、再割り当て、および名前の変更について説明します。

▼ ユーザーアカウントを表示する

「ユーザーの表示」ページを使用し、次の手順に従ってアカウント情報を表示します。

1 管理者インタフェースで、メニューの「アカウント」をクリックします。
「ユーザーリスト」ページが表示されます。

2 表示するアカウントを持つユーザーの横にあるボックスを選択します。

3 「ユーザーアクション」ドロップダウンメニューで、「表示」を選択します。
「ユーザーの表示」ページに、ユーザーの ID、割り当て、セキュリティー、委任、属性、およびコンプライアンス情報のサブセットが表示されます。「ユーザーの表示」ページの情報は表示専用であり、編集はできません。

4 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。

▼ ユーザーアカウントを編集する

「ユーザーの編集」ページを使用し、次の手順に従ってアカウント情報を編集します。

1 管理者インタフェースで、メニューの「アカウント」をクリックします。

2 編集対象のアカウントを持つユーザーの横にあるボックスを選択します。

3 「ユーザーアクション」ドロップダウンメニューで、「編集」を選択します。

4 変更を加え、それを保存します。
「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。

5 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。あるいは、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を個別に選択して更新するか、どのアカウントも選択しないこともできます。

6 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。

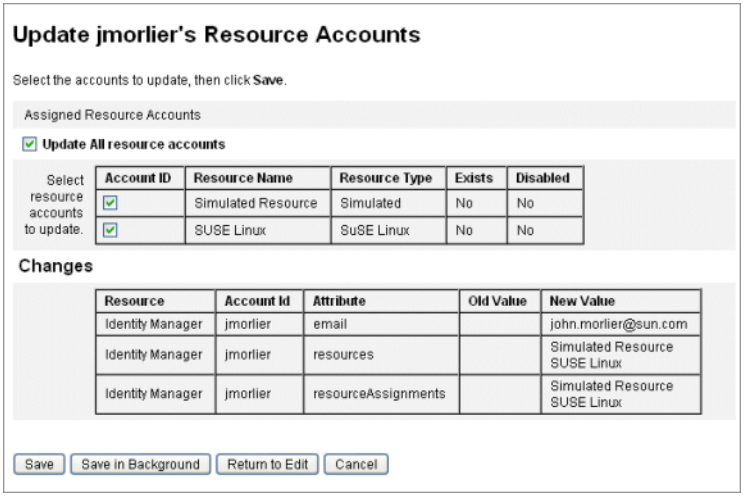


図 3–2 ユーザーの編集 (リソースアカウントの更新)

別の組織へのユーザーの再割り当て

移動操作を使用すると、1 人以上のユーザーをある組織から削除したり、ユーザーを新しい組織に再割り当て、または移動したりできます。

▼ ユーザーを移動する

1. 管理者インタフェースで、メニューの「アカウント」をクリックします。
   「ユーザーリスト」ページが表示されます。
2. 移動するユーザーの横にあるボックスを選択します。
3. 「ユーザーアクション」ドロップダウンメニューで、「移動」を選択します。
   「ユーザーの組織の変更」タスクページが開きます。
4. ユーザーを再割り当てする組織を選択して、「起動」をクリックします。

ユーザーの名前変更

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。

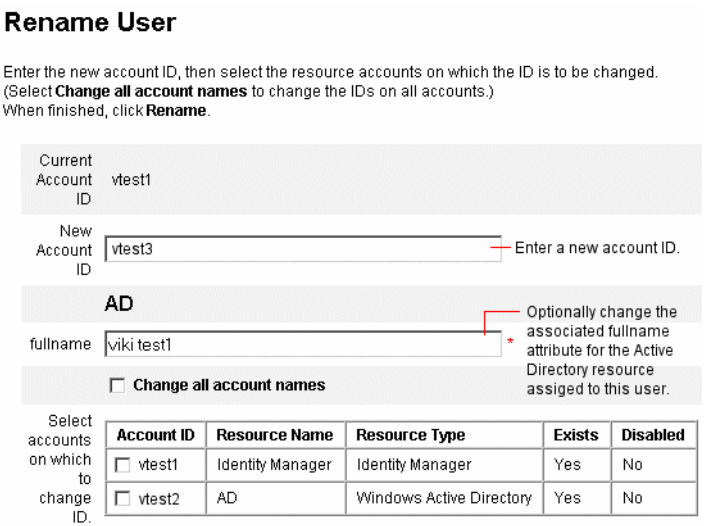
「ユーザーの名前変更」ページでは、ユーザーのアカウント名、関連付けられたリソースアカウント名、およびそのユーザーの Identity Manager アカウントに関連付けられたリソースアカウント属性を変更できます。

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)



アカウントに関連付けられたリソースの更新

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」領域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でのリソース更新

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 3–3 に「リソースアカウントの更新」ページを示します。

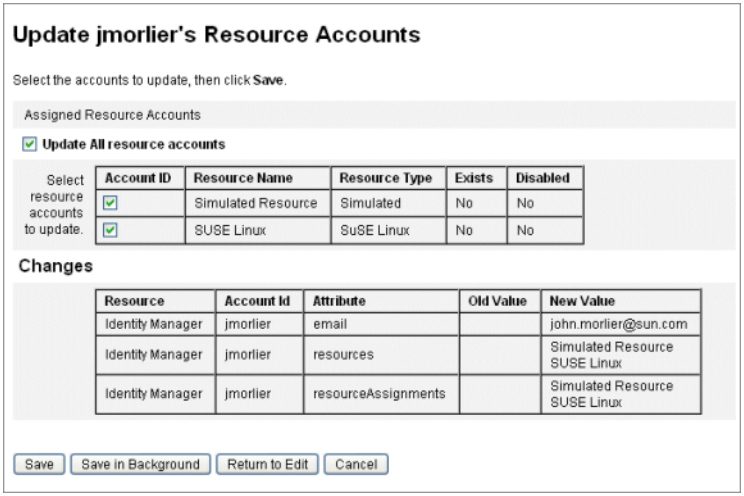


図 3–3　リソースアカウントの更新

複数のユーザーアカウントでのリソースの更新

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。

Identity Manager ユーザーアカウントの削除

Identity Manager では、Identity Manager ユーザーアカウントの削除方法は、リモートアカウントの削除方法と同じです。リソースアカウントを削除する際の手順に従いますが、削除するリモートリソースアカウントを選択する代わりに、Identity Manager アカウントを選択します。

注 – ユーザーが未処理の作業項目を保持しているか、別のユーザーに未処理の作業項目を委任している場合、そのユーザーの Identity Manager アカウントを削除することはできません。ユーザーの Identity Manager アカウントを削除する前に、委任された作業項目を解決するか、別のユーザーに転送する必要があります。

詳細は、68 ページの「1 つのユーザーアカウントからのリソース削除」および 69 ページの「複数のユーザーアカウントからのリソースの削除」を参照してください。

ユーザーアカウントからのリソースの削除

Identity Manager には、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複数の方法が用意されています。

- 「削除」。選択されたリソースごとに、Identity Manager はリモートリソースのユーザーアカウントを削除します。Identity Manager からユーザーを削除するには、Identity Manager をリソースとして選択してください。
  - 削除されたリソースアカウントは、Identity Manager ユーザーから自動的に「リンク解除」されます。
  - 削除されたリソースアカウントは、ユーザーから「割り当て解除」されません。また、「割り当て解除」操作を選択しない限り、リソースはユーザーに割り当てられたままになります。
- 「割り当て解除」。 選択されたリソースごとに、Identity Manager はユーザーの割り当てられたリソースリストからリソースを削除します。
  - 割り当てが解除されたリソースアカウントは、Identity Manager ユーザーから自動的に「リンク解除」されます。
  - リモートリソース上のユーザーアカウントは、削除されません。また、「削除」操作を選択しない限り、アカウントはそのままになります。
- 「リンク解除」。 選択されたリソースごとに、ユーザーのリソースアカウント情報は Identity Manager. から削除されます。
  - 「削除」操作を選択しない限り、リモートリソース上のユーザーのアカウントはそのままになります。
  - 「割り当て解除」操作を選択しない限り、リソースはユーザーの割り当て済みリソースのリストに残ります。
  - 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。

「プロビジョン解除」は、「ユーザーリスト」ページメニューにユーザーアクションとして表示されますが、Identity Manager に実際に存在する削除操作は、「削除」、「割り当て解除」、「リンク解除」の 3 つだけです。

リモートリソースのプロビジョンを解除するには、リソース上で「削除」および「割り当て解除」操作を実行します。

1つのユーザーアカウントからのリソース削除

1 人の Identity Manager ユーザーに対して削除操作を実行するには、次の手順に従います。一度に 1 つのユーザーアカウントを操作することで、個別のリソースアカウントに対して異なる削除、割り当て解除、またはリンク解除あるいはその組み合わせを指定できます。

▼ 1つのユーザーアカウントに対する削除、割り当て解除、またはリンク解除操作を開始する

1. 管理者インタフェースで、メインメニューの「アカウント」をクリックします。
   「アカウントのリスト」タブに「ユーザーリスト」ページが表示されます。

2. ユーザーを選択して、「ユーザーアクション」ドロップダウンメニューをクリックします。

3. リストからいずれかの「削除」操作 (「削除」、「プロビジョン解除」、「割り当て解除」、または「リンク解除」) を選択します。
   「リソースアカウントの削除」ページが表示されます (図 3–4)。

4. フォームに必要な情報を指定します。「削除」、「割り当て解除」、および「リンク解除」操作については、**67** ページの「ユーザーアカウントからのリソースの削除」を参照してください。

5. 「**OK**」をクリックします。
   図 3–4 に「リソースアカウントの削除」ページを示します。スクリーンショットでは、ユーザー jrenfro はリモートリソース (Simulated Resource) 上にアクティブなアカウントを 1 つ保持しています。「削除」操作を選択すると、フォームの送信時にリソース上の jrenfro のアカウントが削除されます。削除されたアカウントは自動的にリンク解除されるため、このリソースのアカウント情報は Identity Manager から削除されます。「割り当て解除」操作は選択されていないため、Simulated Resource は jrenfro に割り当てられたままです。

   jrenfro の Identity Manager アカウントを削除するには、Identity Manager に対して「削除」操作を選択してください。

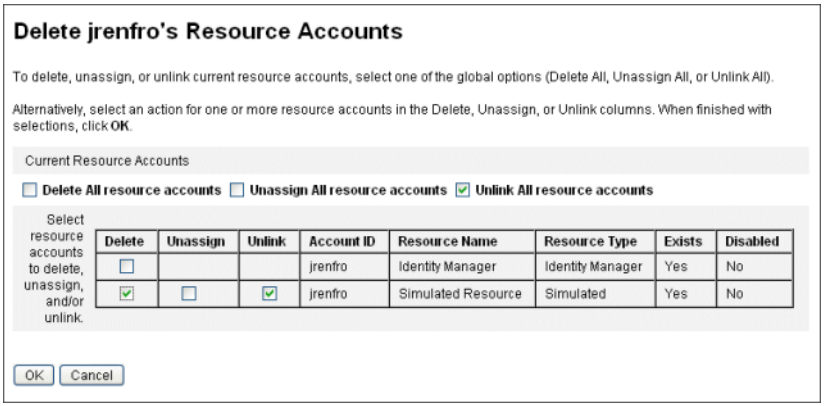


図 3–4 「リソースアカウントの削除」ページ

複数のユーザーアカウントからのリソースの削除

一度に複数の Identity Manager ユーザーアカウントに対して削除操作を実行できます。ただし、選択した削除操作を実行できるのは、ユーザーの「すべての」リソースアカウントに対してのみです。

削除操作は、Identity Manager の一括アカウントアクション機能を使って実行することもできます。80 ページの「Delete、DeleteAndUnlink、Disable、Enable、Unassign、および Unlink コマンド」を参照してください。

▼ 複数のユーザーに対して削除、割り当て解除、リンク解除操作を開始する

1. 管理者インタフェースで、メインメニューの「アカウント」をクリックします。
   「アカウントのリスト」タブに「ユーザーリスト」ページが表示されます。
2. 1 人以上のユーザーを選択して、「ユーザーアクション」ドロップダウンメニューをクリックします。
3. リストからいずれかの「削除」操作 (「削除」、「プロビジョン解除」、「割り当て解除」、または「リンク解除」) を選択します。
   Identity Manager に、「削除、割り当て解除、またはリンク解除の確認」ページが表示されます (図 3–5)。
4. 実行するアクションを指定します。

次のオプションがあります。

- 「ユーザーのみを削除」。ユーザーの Identity Manager アカウントを削除します。このオプションでは、ユーザーのリソースアカウントの削除や割り当て解除は実行されません。
- 「ユーザーとリソースアカウントを削除」。ユーザーの Identity Manager アカウントおよびユーザーのすべてのリソースアカウントを削除します。
- 「リソースアカウントのみ削除」。ユーザーのリソースアカウントをすべてを削除します。このオプションは、リソースアカウントの割り当て解除は行わず、ユーザーの Identity Manager アカウントの削除も行いません。
- 「リソースアカウントを削除し、ユーザーに直接割り当てたリソースの割り当てを解除」。ユーザーのリソースアカウントをすべて削除および割り当て解除しますが、ユーザーの Identity Manager アカウントは削除しません。
- 「ユーザーに直接割り当てたリソースアカウントの割り当てを解除」。直接割り当てられたリソースアカウントを割り当て解除します。このオプションは、リモートリソースのユーザーアカウントは削除しません。ロールまたはリソースグループによって割り当てられたリソースアカウントは、影響を受けません。
- 「ユーザーからリソースアカウントのリンクを解除」。ユーザーのリソースアカウント情報は Identity Manager. から削除されます。リモートリソースのユーザーのアカウントは削除されず、割り当て解除されません。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。

5 「**OK**」をクリックします。

図 3–5 に、「削除、割り当て解除、またはリンク解除の確認」ページを示します。ページの上部に、複数のユーザーに実行可能な 6 つの操作が表示されます。このページの下部には、選択されたアクションの影響を受けるユーザーが表示されます。

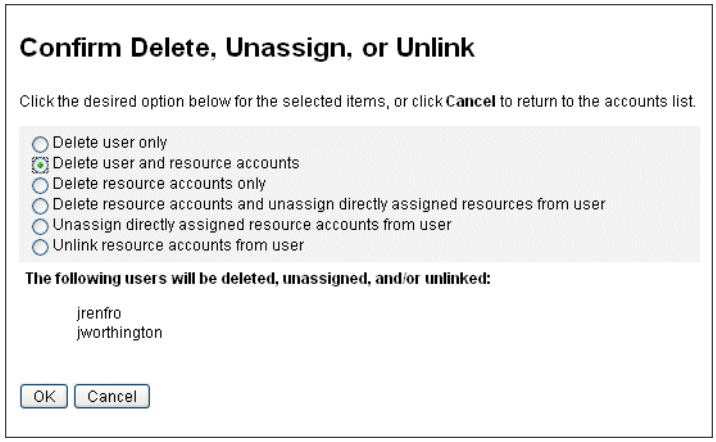


図 3–5 「削除、割り当て解除、またはリンク解除の確認」ページ

ユーザーパスワードの変更

すべての Identity Manager ユーザーにパスワードが割り当てられています。Identity Manager ユーザーパスワードが設定されると、そのパスワードを使用して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。

注 – アカウントパスワードポリシーおよびユーザー認証の一般情報については、86 ページの「アカウントセキュリティーと特権の管理」を参照してください。

▼ 「ユーザーリスト」ページからのパスワードの変更

「ユーザーリスト」ページ (「アカウント」→「アカウントのリスト」) から「パスワードの変更」ユーザーアクションを使用して、「ユーザーリスト」ページからユーザーアカウントパスワードを変更することができます。これには、次の手順を実行します。

1. 管理者インタフェースで、メインメニューの「アカウント」をクリックします。
   「アカウントのリスト」タブに「ユーザーリスト」ページが表示されます。
2. ユーザーを選択して、「ユーザーアクション」ドロップダウンメニューをクリックします。
3. パスワードを変更するには、「パスワードの変更」を選択します。
   「ユーザーパスワードの変更」ページが開きます。

4 新規パスワードを入力して、「パスワードの変更」ボタンをクリックします。

▼ メインメニューからパスワードを変更する

メインメニューからユーザーアカウントパスワードを変更するには、次の手順に従います。

1 管理者インタフェースで、メインメニューの「パスワード」をクリックします。
「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。

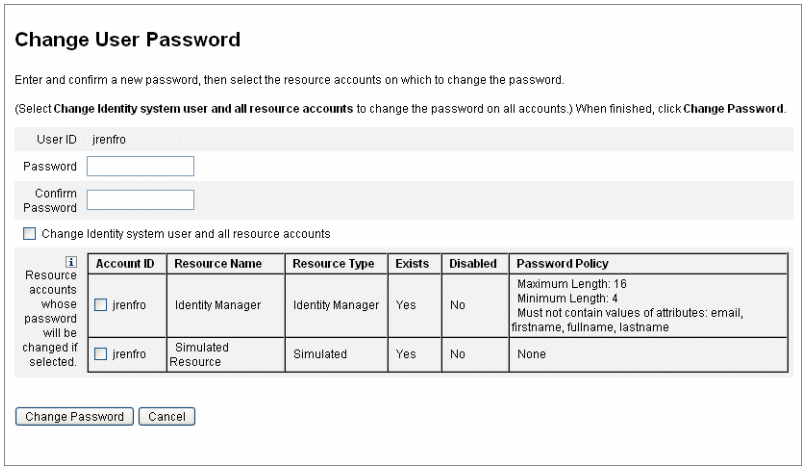


図 3–6 ユーザーパスワードの変更

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用語の 1 文字以上を入力し、「検索」をクリックします。**Identity Manager** は、入力された文字が **ID** に含まれるすべてのユーザーのリストを返します。クリックしてユーザーを選択し、「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たら、「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でユーザーパスワードを変更します。**Identity Manager** は、パスワードを変更するために実行する操作のシーケンスを示すワークフロー図を表示します。

ユーザー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。

▼ 「ユーザーリスト」ページからのパスワードのリセット

「パスワードのリセット」ユーザーアクションは、「ユーザーリスト」ページ (「アカウント」>「アカウントのリスト」) で実行できます。

「ユーザーリスト」ページからパスワードをリセットするには、次の手順に従います。

1. 管理者インタフェースで、メインメニューの「アカウント」をクリックします。「アカウントのリスト」タブに「ユーザーリスト」ページが表示されます。
2. ユーザーを選択して、「ユーザーアクション」ドロップダウンメニューをクリックします。
3. パスワードをリセットするには、「パスワードのリセット」を選択します。
   「ユーザーパスワードのリセット」ページが表示されます。
4. 「パスワードのリセット」ボタンをクリックします。

▼ Identity Manager アカウントポリシーを使用してパスワードを期限切れにする

ユーザーパスワードをリセットすると、そのパスワードはデフォルトでただちに期限切れになります。その結果、パスワードのリセット後に初めてログインするとき、ユーザーは新しいパスワードを選択してアクセスする必要があります。このデフォルトは「Edit the Reset User Password」フォームを使用して上書きできるた

め、ユーザーのパスワードは、そのユーザーに関連付けられた Identity Manager 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期限切れになります。

デフォルトのパスワード変更要件を上書きするには、次の手順に従います。

1 「**Reset User Password**」フォームを編集し、次の値を `false` に設定します。

```
resourceAccounts.currentResourceAccounts[Lighthouse].expirePassword
```

2 **Identity Manager** アカウントポリシーの「リセット」オプションを使用して、パスワードが期限切れになるときを指定します。

次の設定があります。

- 「半永久」。Identity Manager は、`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を計算し、その日付をユーザーに設定します。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」。Identity Manager は、`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を計算し、その日付をユーザーに設定します。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` 属性が適用されるのは、パスワードがリセットされる (ランダムに変更される) ときだけです。これは、パスワードの変更には適用されません。

ユーザーアカウントの無効化、有効化、およびロック解除

この節では、Identity Manager ユーザーアカウントを無効化および有効化する方法について説明します。また、Identity Manager アカウントがロックアウトされてしまったユーザーをサポートする方法についても説明します。

▼ ユーザーアカウントを無効化する

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。

管理者は管理者インタフェースからユーザーアカウントを無効化できますが、ユーザーアカウントをロックすることはできません。アカウントがロックされるのは、Identity Manager アカウントポリシーで定義されたログイン試行の失敗回数を超過した場合だけです。

注 – 割り当てられたリソースがアカウントの無効化をネイティブにサポートしてはいないが、パスワードの変更はサポートしている場合、ランダムに生成される新規パスワードを割り当てることにより、そのリソース上のユーザーアカウントを無効にするよう、Identity Manager を設定できます。

この機能が正しく動作することを確認するには、次の手順に従います。

1. リソースの編集ウィザードで、「アイデンティティーシステムのパラメータ」ページを開きます。このウィザードの表示方法については、165 ページの「リソースの管理」を参照してください。
2. 「アカウント機能の設定」テーブルで、「パスワード」機能と「無効化」機能の両方の「無効化」列にチェックマークが付いていないことを確認します。「無効化」機能を表示するには、「すべての機能を表示」を選択してください。

   「無効化」列にチェックマークが付いていない場合、リソースのアカウントを無効にすることはできません。

参考

1 つのユーザーアカウントの無効化

ユーザーアカウントを無効にするには、「ユーザーリスト」でユーザーアカウントを選択して、「ユーザーアクション」ドロップダウンメニューの「無効化」を選択します。

表示された「無効化」ページで、無効に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 は、Identity Manager ユーザーアカウントおよび関連付けられたすべてのリソースアカウントを無効にした結果を表示します。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。

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。

▼ パスワードをリセットすることによってリソース上のユーザーアカウントを有効化する

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。

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。

注 – 割り当てられたリソースがアカウントの有効化をネイティブにサポートしてはいないが、パスワードの変更はサポートしている場合、Identity Manager でパスワードをリセットすることにより、そのリソース上のユーザーアカウントを有効にできます。

この機能が正しく動作することを確認するには、次の手順に従います。

---

1. リソースの編集ウィザードで、「アイデンティティーシステムのパラメータ」ページを開きます。このウィザードの表示方法については、165 ページの「リソースの管理」を参照してください。

2. 「アカウント機能の設定」テーブルで、「パスワード」機能と「有効化」機能の両方の「無効化」列でリソースの選択を解除します。「有効化」機能を表示するには、「すべての機能を表示」を選択します。

   「有効化」列にチェックマークが付いていない場合、リソースのアカウントを有効にすることはできません。

参考 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、有効にするリソースを選択し、「OK」をクリックします。Identity Manager は、Identity Manager アカウントおよび関連付けられたすべてのリソースアカウントを有効にした結果を表示します。

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。

ユーザーアカウントのロック解除

ユーザーが Identity Manager へのログインに失敗した場合、そのユーザーはロックアウトされます。ロックアウトされるのは、Identity Manager アカウントポリシーで定義されたログイン試行の失敗回数を超過した場合です。

注 – Identity Manager のロックアウトに数えられるのは、Identity Manager ユーザーインタフェースに対するログイン試行だけです (つまり、管理者インタフェース、エンドユーザーインタフェース、コマンド行インタフェース、SPML API インタフェースのいずれか)。リソースアカウントへのログイン試行の失敗はカウントされず、Identity Manager アカウントのロックアウトの原因にはなりません。

パスワードまたは質問によるログイン試行の最大失敗回数は、Identity Manager アカウントポリシーにより設定されます。

- 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ユーザーは、秘密の質問によるログインインタフェースを含む Identity Manager アプリケーションインタフェースすべてでロックアウトされます。
- 質問によるログイン試行の最大失敗回数を超過したユーザーは、秘密の質問によるログインを除く任意の Identity Manager アプリケーションインタフェースへの認証を実行できます。

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の失敗回数の超過のために Identity Manager からロックアウトされたユーザーは、管理者がアカウントをロック解除するか、ロックが期限切れになるまでログインできません。

- 管理者は、ユーザーのメンバー組織、および `Unlock User` 機能を管理している場合にアカウントをロック解除できます。
- `Lock Timeout` が Identity Manager アカウントポリシーで設定されている場合、アカウントに設定されているロックは時間が経過すると期限切れになります。パスワードによるログイン試行失敗の `Lock Timeout` は、「パスワードログインに失敗したために発生したアカウントロックの有効期間」の値により設定されます。

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失敗回数を超過したために秘密の質問によるログインインタフェースでロックアウトされるユーザーは、管理者がアカウントのロックを解除するか、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か、ロックの期限が切れるまで、このインタフェースにログインできなくなります。

- 管理者は、ユーザーのメンバー組織、および `Lock Timeout` 機能を管理している場合にアカウントをロック解除できます。
- `Lock Timeout` が Identity Manager アカウントポリシーで設定されている場合、アカウントに設定されているロックは時間が経過すると期限切れになります。質問によるログイン試行の失敗の `Lock Timeout` は、「質問ログインに失敗したために発生したアカウントロックの有効期間」の値により設定されます。

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

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。

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」。選択したリソースアカウントを削除して、割り当てとリンクも解除します。「アイデンティティーシステムアカウントをターゲットにする」オプションを選択すると、ユーザーの各 Identity Manager アカウントを削除することもできます。
- 「Delete と Unlink」。選択したリソースアカウントをすべて削除して、そのアカウントとユーザーとのリンクを解除します。
- 「Disable」。 選択したリソースアカウントをすべて無効にします。「アイデンティティーシステムアカウントをターゲットにする」オプションを選択すると、ユーザーの各 Identity Manager アカウントを無効にすることもできます。

- 「Enable」。選択したリソースアカウントをすべて有効にします。「アイデンティティーシステムアカウントをターゲットにする」オプションを選択すると、ユーザーの各 Identity Manager アカウントを有効にすることもできます。
- 「Unassign、Unlink」。選択したリソースアカウントをすべてリンク解除し、Identity Manager ユーザーアカウントのそれらのリソースに対する割り当てを削除します。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わけではありません。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。
- 「Unlink」。リソースアカウントと 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わけではありません。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が回復されることがあります。

一括アクションは、ファイルまたは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。

これらのアクションの多くを、ユーザーの検索結果に対して実行できます。ユーザーの検索には、「ユーザーの検索」ページ (「アカウント」→「ユーザーの検索」) を使用します。

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

1. 管理者インタフェースで、メインメニューの「アカウント」をクリックします。
2. 二次的なメニューで、「一括アクションの起動」をクリックします。
3. フォームに必要な情報を指定して、「起動」をクリックします。
   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状態を監視するには、メインメニューの「サーバータスク」をクリックして、「すべてのタスク」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コンマ区切り値 (comma-separated value; CSV) 形式で指定できます。これにより、各種アクションを 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アクションも指定できます。

CSV 形式は、2 行以上の入力行で構成されます。各行は、コ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。残りの各行は、Identity Manager ユーザー、ユーザーのリソースアカウント、またはその両方に対して実行される処理に対応します。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。

- 「ユーザー」。Identity Manager ユーザーの名前が含まれます。
- 「コマンド」。Identity Manager ユーザーに対して実行する操作が含まれます。有効なコマンドは次のとおりです。
  - 「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して割り当てとリンクを解除します。
  - 「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にします。
  - 「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にします。
  - 「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。オプションで、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。オプションで、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アクションを実行します。存在する場合は更新アクションを実行します。

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。

resources フィールドには、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。Identity Manager アカウントを処理するように Identity Manager を指定します。

これらのアクションのいくつかを 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。使用されるフィールド名は、画面内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、『Sun Identity Manager Deployment Reference』の「User View Attributes」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 つ以上のロール名のリスト。
- 「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。

作成および更新アクションを、CSV 形式にした例を次に示します。

```
command,user,waveset.resources,password.password,
password.confirmPassword,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
```

CreateOrUpdate コマンドを使用すると、複数のアカウントタイプをサポートするリソースで特定のアカウントタイプを指定できます。したがって、ユーザーが特定のリソースに複数のアカウントを持ち、各アカウントのアカウントタイプが異なる場合は、次の例に示す方法で userAye ユーザーの admin アカウントタイプを更新します。

```
command,user,accounts[Sim1|admin].emailAddress
CreateOrUpdate,userAye,bbye8@example.com
```

注 –

CreateOrUpdate コマンドを使用すると、ユーザーのアカウントのアカウント固有の属性を設定できますが、ユーザー画面のグローバルセクションの次の値が指定した「すべての」アカウントに適用されることに注意してください。

- accountId
- email
- password
- disable
- すべての拡張属性

結果として、次の形式の BulkOps コマンドが期待したように動作しない場合があります。

```
command,user,accounts[Sim1].email
CreateOrUpdate,userAye,bbye8@example.com
```

userAye がすでに email の値を持つ場合、その値は Sim1 リソースの電子メール属性に適用されます。この動作を回避する方法はありません。

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、希望するとおりに指定できないことがあります。値を一部削除したり、現在の値に追加したい場合もあります。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。別の指示と共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、値が正確に一致する必要があります。

フィールド値の特殊文字

フィールド値にコンマ (,) 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 (|) またはバックスラッシュ (\) 文字をフィールド値に含める場合は、その前にバックスラッシュ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 アクションを実行する場合は、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* 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ています。*field_name* はフィールドの名前です。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` の属性の中にあります。
- `waveset.bulk.fieldDirectives.`*field_name* 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。
- 現在のアクションを中止するには、`waveset.bulk.abort` ブール型属性を true に設定します。
- `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に `waveset.bulk.abort` 属性を設定します。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。

相関規則と確認規則

使用するアクションの user フィールドに指定できる Identity Manager ユーザー名がない場合は、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。

相関規則は、アクションフィールドに一致する Identity Manager ユーザーを検索します。確認規則は、アクションフィールドに対して Identity Manager ユーザーを検査し、ユーザーが一致するかどうかを決定します。この 2 段階の方法によって、Identity Manager は、候補のユーザーを名前または属性に基づいて迅速に見つけ出しコストのかかる検査を可能性のあるユーザーに対してのみ行うことで、相関関係を最適化できます。

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については、『Sun Identity Manager Deployment Guide』の第 3 章「Data Loading and Synchronization」を参照してください。

相関規則

相関規則の入力は、アクションフィールドのマップです。出力は、次のいずれかでなければなりません。

- 文字列 (ユーザー名または ID を含む)
- 文字列要素のリスト (各要素にユーザー名または ID が含まれる)

- WSAttribute 要素のリスト
- AttributeCondition 要素のリスト

一般的な相関規則は、アクション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。

相関規則では、コストを抑えることを前提に、できるだけ選択肢を絞り込むようにします。可能であれば、コストのかかる処理は確認規則に回すことをお勧めします。

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、IDM Schema Configuration という名前の Identity Manager 設定オブジェクト内で設定されます。

拡張属性で相関関係を実現するには、特殊な設定が必要です。

拡張属性は、クエリー可能として指定する必要があります。

▼ 拡張属性をクエリー可能として設定する

1. IDM Schema Configuration を開きます。IDM Schema Configuration を表示または編集するには、**IDM Schema Configuration** 機能を保持している必要があります。
2. <IDMObjectClassConfiguration name='User'> 要素を見つけます。
3. <IDMObjectClassAttributeConfiguration name=' xyz '> 要素を見つけます。xyz はクエリー可能に設定する属性の名前です。
4. queryable='true' を設定します。

   84 ページの「相関規則」 では、email 拡張属性がクエリー可能として定義されています。

例 3–1 email 拡張属性をクエリー可能として定義する XML (抜粋)

```
<IDMSchemaConfiguration>
  <IDMAttributeConfigurations>
    <IDMAttributeConfiguration name='email' syntax='STRING'/>
    </IDMAttributeConfiguration>
  </IDMAttributeConfigurations>
  <IDMObjectClassConfigurations>
    <IDMObjectClassConfiguration name='User' extends='Principal' description='User description'>
      <IDMObjectClassAttributeConfiguration name='email' queryable='true'/>
    </IDMObjectClassConfiguration>
  </IDMObjectClassConfigurations>
 </IDMSchemaConfiguration>
```

IDM Schema Configuration の変更を有効にするには、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) を再起動する必要があります。

確認規則

確認規則の入力は次のとおりです。

- Identity Manager ユーザーの完全表示には、userview を使用します。
- アクションフィールドのマップには、account を使用します。

確認規則は、ユーザーがアクションフィールドに一致する場合、文字列形式のブール値で true を返します。 一致しない場合は false を返します。

一般的な確認規則は、ユーザー画面の内部値と、アクションフィールドの値とを比較します。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た一致ユーザー 1 人について 1 回実行されます。

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。

- 86 ページの「パスワードポリシーの設定」
- 90 ページの「ユーザー認証」
- 94 ページの「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、メインメニューの「セキュリティー」をクリックし、「ポリシー」をクリックします。

パスワードポリシーを編集するには、「ポリシー」リストで目的のポリシーをクリックします。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。

注 – ポリシーについては、99 ページの「Identity Manager ポリシーの設定」を参照してください。

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。

ポリシータイプ

いずれかのポリシータイプボタンを選択します。「その他」オプションを選択した場合は、所定のテキストフィールドにタイプを入力する必要があります。

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 3–7 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。

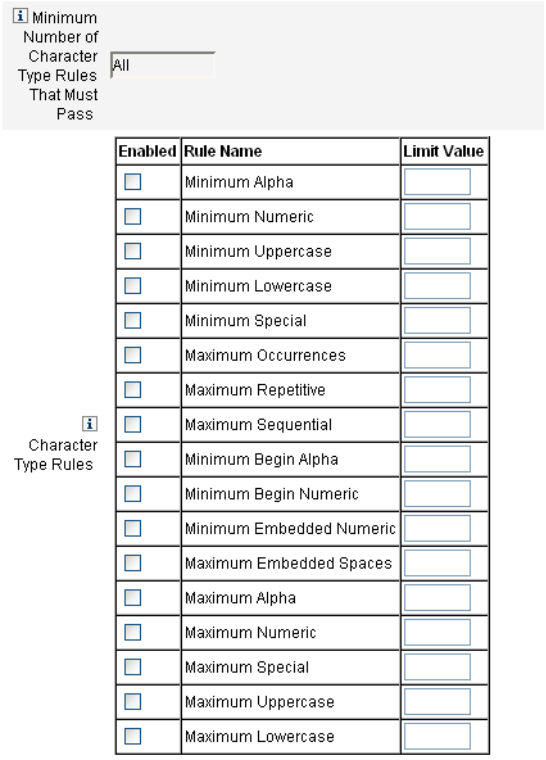


図 3–7　パスワードポリシー (文字タイプ) 規則

辞書ポリシーの選択

単純な辞書攻撃から保護するために、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

辞書の設定は、「ポリシー」ページで行います。辞書の設定方法については、102 ページの「辞書ポリシーとは」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 を指定した場合は、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。詳細は、102 ページの「辞書ポリシーとは」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 つ以上入力できます。

指定できる属性は次のとおりです。

- `accountID`
- `email`
- `firstname`
- `fullname`
- `lastname`

パスワードに含むことのできる一連の「使用禁止」属性を、`UserUIConfig` 設定オブジェクトで変更できます。詳細は、102 ページの「ポリシーでの使用禁止属性」を参照してください。

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」領域にあります。

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

1 メインメニューの「セキュリティー」をクリックしてから、「ポリシー」をクリックします。

2 「**Default Identity Manager Account Policy**」をポリシーのリストから選択します。

ページの「二次認証ポリシーオプション」領域で認証を選択できます。

重要: 最初の設定時に、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。

秘密の質問ポリシーは、ユーザーがログインページで「パスワードをお忘れですか?」ボタンをクリックしたときや、「自分の秘密の質問の回答の変更」ページにアクセスしたときにどうなるかが決まります。90 ページの「ユーザー認証」では、各オプションについて説明します。

オプション	説明
すべて	ユーザーは、ポリシーで定義された質問およびユーザー独自の質問のすべてに答える必要があります。
いずれか	Identity Manager は、ポリシーで定義された質問およびユーザー独自の質問をすべて表示します。ユーザーが回答する必要のある質問の数を指定する必要があります。

オプション	説明
次	ユーザーは、初回ログイン時に、ポリシーで定義されたすべての可能性のある質問に答える必要があります。 ユーザーがログイン時に「パスワードをお忘れですか?」ボタンをクリックした場合、Identity Manager は最初の質問を表示します。ユーザーの回答が正しくない場合、ユーザーが秘密の質問に正しく回答してログインするか、指定した試行回数の制限に基づいてロックアウトされるまで、Identity Manager は次の質問を表示します。ユーザー独自の質問は、このポリシーではサポートされません。
ランダム	管理者は、ユーザーが回答する必要のある質問の数を指定できます。Identity Manager は、ポリシーで定義された質問およびユーザー独自の質問のリストから、指定された数の質問をランダムに選択して表示します。ユーザーは、表示された質問のすべてに答える必要があります。
ラウンドロビン	Identity Manager は設定済みの質問リストから次の質問を選択して、ユーザーに割り当てます。最初のユーザーには秘密の質問のリストにある最初の質問が割り当てられ、2 番目のユーザーには 2 つ目の質問が割り当てられます。リスト上の質問数を超えるまで、このパターンが続きます。質問数を超えた時点で、また最初の質問から順番にユーザーに割り当てられます。たとえば 10 の質問がある場合、11 番目と 21 番目のユーザーには最初の質問が割り当てられます。 選択される質問は、表示される 1 つだけです。ユーザーに毎回異なる質問に答えてもらう場合には、「ランダム」ポリシーを使って質問の数を 1 に設定します。 ユーザーが秘密の質問を独自に定義することはできません。この機能については、91 ページの「ユーザー独自の秘密の質問」を参照してください。

Identity Manager ユーザーインタフェースにログインし、「パスワードをお忘れですか?」ボタンをクリックし、表示された質問に答えることによって、認証の選択肢を確認することができます。

図 3–8 に「ユーザーアカウント認証」画面の例を示します。

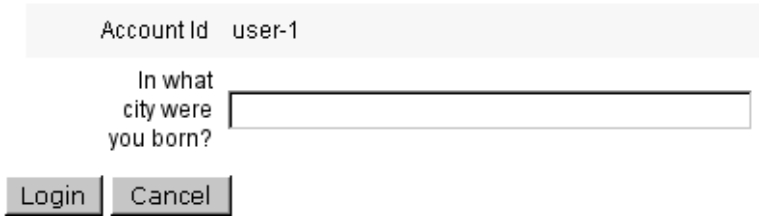


図 3–8 ユーザーアカウント認証

ユーザー独自の秘密の質問

Identity Manager 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 3–9 に示されています。

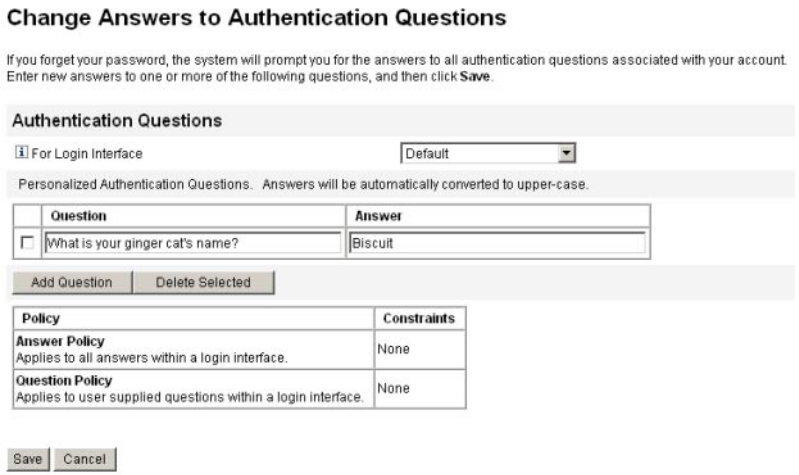


図 3–9　回答の変更: ユーザー独自の秘密の質問

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` System Configuration 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。

システム設定オブジェクトの編集については、116 ページの「Identity Manager 設定オブジェクトの編集」を参照してください。

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、システム設定オブジェクトで `bypassChangePassword` プロパティーを次のように設定します。

例 3–2　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">
```

例 3–2 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 (続き)

```
    <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。

例 3–3 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。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。管理者ロールの詳細な説明および作成手順については、第 5 章「ロールとリソース」の 158 ページの「Identity Manager リソースとその管理について」を参照してください。
- 機能。 機能は、規則によって定義されます。Identity Manager には、選択可能な実用上の機能にグループ化された機能のセットが用意されています。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。機能の説明および作成手順については、第 6 章「管理」の 214 ページの「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。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。詳細は、第 6 章「管理」の 207 ページの「Identity Manager の組織について」を参照してください。

Identity Manager 管理者および管理作業については、第 6 章「管理」を参照してください。

ユーザーの自己検索

Identity Manager エンドユーザーインタフェースによって、エンド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。

▼ 自己検索を有効化する

1 「エンドユーザーリソース」の設定オブジェクトを編集します。

Identity Manager 設定オブジェクトの編集手順については、116 ページの「Identity Manager 設定オブジェクトの編集」を参照してください。

2 <String>*Resource* </String> を追加します。図 3–10 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 3–10 エンドユーザーリソースの設定オブジェクト

3 「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」)。この領域により、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。

注 – Identity Manager 設定オブジェクトにエンドユーザーアクセスを提供するために、管理者は「エンドユーザー」組織も使用できます。詳細は、228 ページの「エンドユーザー組織」を参照してください。

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。

▼ 匿名登録機能を有効にする

1 管理者インタフェースで、「設定」をクリックしてから「ユーザーインタフェース」をクリックします。

2 「匿名登録」領域で「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、ログインページに「はじめてのユーザーですか?」というテキストに続いて「アカウントのリクエスト」リンクが表示されます。

注– 「はじめてのユーザーですか?アカウントのリクエスト」というテキストは、カスタマイズ可能です。詳細は、『Sun Identity Manager Deployment Guide』を参照してください。

図 3–11 「アカウントのリクエスト」リンクの有効な「ユーザーインタフェース」ページ

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」領域から、匿名登録プロセスの次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に通知を送信するため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」。選択すると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。デフォルトで有効になっています。
- 「検証の有効化」。選択すると、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。デフォルトで有効になっています。
- 「プロセス開始 URL」。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するために URL を入力します。
- 「通知の有効化」。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 ページにわたる登録ページの最初のページが表示され、名、姓、および従業員 ID が要求されます。「検証の有効化」属性が選択されている場合 (デフォルト) は、ユーザーが次のページに進む前にこの情報が検証される必要があります。

`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

ビジネス管理オブジェクトの設定

この章では、管理者インタフェースを使用した Identity Manager オブジェクトの設定および保守について説明するとともに、その実行手順を示します。Identity Manager オブジェクトの詳細については、概要の章の27 ページの「Identity Manager オブジェクト」を参照してください。

注 – サービスプロバイダ実装での Identity Manager の設定については、第 17 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。

- 99 ページの「Identity Manager ポリシーの設定」
- 104 ページの「電子メールテンプレートのカスタマイズ」
- 109 ページの「監査グループおよび監査イベントの設定」
- 110 ページの「Remedy との統合」
- 111 ページの「エンドユーザーインタフェースの設定」
- 112 ページの「Identity Manager の登録」
- 116 ページの「Identity Manager 設定オブジェクトの編集」

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について説明します。

この節は次のトピックで構成されています。

- 100 ページの「ポリシーとは」
- 102 ページの「ポリシーでの使用禁止属性」
- 102 ページの「辞書ポリシーとは」

ポリシーとは

Identity Manager ポリシーは、Identity Manager のアカウント 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で、Identity Manager ユーザーに制限を設定します。

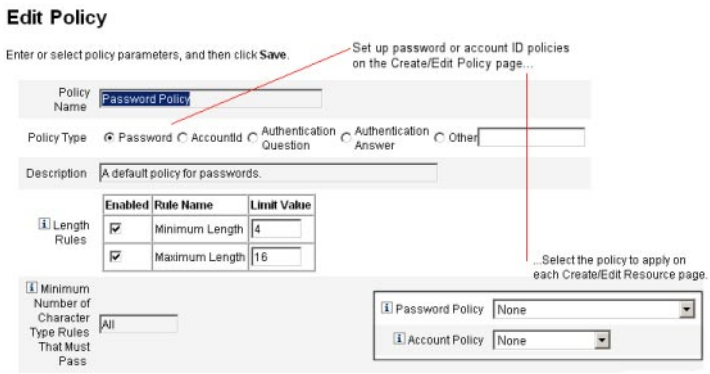
注 – Identity Manager には、特にユーザーのコンプライアンスを監査するように設計された監査ポリシーも用意されています。監査ポリシーについては、第 13 章「アイデンティティー監査: 基本概念」を参照してください。

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は、「組織の作成と編集」ページで組織に割り当てるか、「ユーザーの作成と編集」ページでユーザーに割り当てます。

  次のオプションを設定または選択できます。

  - ユーザーアカウント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かったときに、Identity Manager がユーザーアカウントを処理する方法を指定します。
  - パスワードポリシーオプション。パスワードの有効期限、期限切れ前の警告期間、およびリセットオプションを設定します。
  - 二次認証ポリシーのオプション。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、ユーザーに表示する一連の質問を設定します。
- サービスプロバイダシステムのアカウントポリシー。サービスプロバイダユーザーに対してユーザー、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する場合は、、サービスプロバイダ実装でこのポリシーを使用します。ポリシーは、「組織の作成と編集」ページで組織に割り当てるか、「ユーザーの作成と編集」ページでユーザーに割り当てます。
- 文字列の品質ポリシー。パスワード、アカウント ID、認証などのポリシータイプが含まれます。長さ規則、文字タイプ規則、使用できる語句、および属性値を設定します。このポリシータイプは、各 Identity Manager リソースに関連付けられ、各リソースのページで設定されます。次の図に例を示します。



パスワードとアカウント ID に対して、次のオプションと規則を設定できます。

- 長さ規則。使用できる文字列の最小または最大長さを決定します。
- 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。
- パスワード再利用の制限。パスワードの再利用を制限する、現在より前の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。
- 禁止語句および属性値。ID およびパスワードに使用できない語句と属性を指定します。

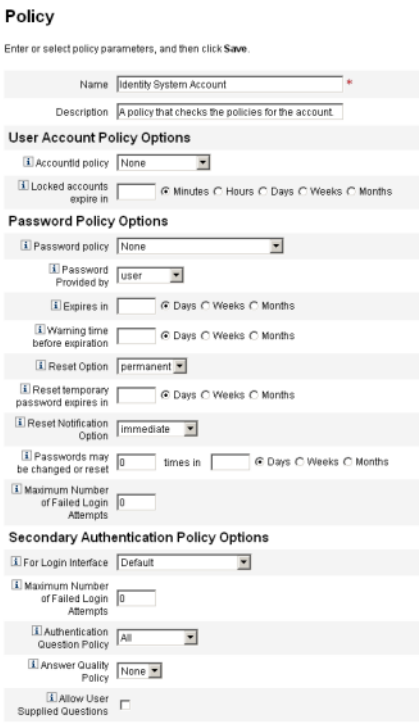
▼ 「ポリシー」ページを開く

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。このページを開くには、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 「セキュリティー」タブをクリックしてから、「ポリシー」サブタブをクリックします。

次の図のように、「ポリシー」ページが表示されます。



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>` 属性。ポリシータイプ「パスワード」
- `<PolicyAccountAttributeNames>` 属性。ポリシータイプ「アカウント ID」
- `<PolicyOtherAttributeNames>` 属性。ポリシータイプ「その他」

辞書ポリシーとは

辞書ポリシーを使用すると、Identity Manager はパスワードを単語データベースと照合してチェックし、単純な辞書攻撃から確実に保護します。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制限することにより、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。

▼ 辞書ポリシーを設定する

辞書ポリシーを設定するには、次の操作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

1. 101 ページの「「ポリシー」ページを開く」の説明に従って、「ポリシー」ページを開きます。
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。

   データベース情報には次のものがあります。

   - 「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」。データベースが待機中のポートを入力します。
   - 「接続 URL」。接続時に使用する 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」。データベースと対話するときに使用する 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。

▼ 辞書ポリシーを実装する

次の手順を使用して、辞書ポリシーを実装します。

1. 101 ページの「「ポリシー」ページを開く」の説明に従って、「ポリシー」ページを開きます。
2. 「パスワードポリシー」リンクをクリックして、パスワードポリシーを編集します。
3. 「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。
4. 変更を保存するには、「保存」をクリックします。

   いったん実装されると、変更および生成されたすべてのパスワードがその辞書と照合されます。

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。
- 外部リソース。プロビジョニングタスクの実行が必要なことを外部リソースのプロビジョニングツールに通知します。

- 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。すべてのリソース上でパスワードの変更が正常に行われ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のリストとパスワード変更リクエストの発信元が記載されます。
- パスワード同期エラー通知。すべてのリソース上でパスワードの変更が正常に行われなかったことをユーザーに通知します。通知には、エラーのリストとパスワード変更リクエストの発信元が記載されます。
- ポリシー違反情報。アカウントポリシー違反が発生したことを通知します。
- アカウントの調整イベント。リソースの調整イベント、調整の概要。それぞれ、Notify Reconcile Response、Notify Reconcile Start、および Notify Reconcile Finish のデフォルトワークフローから呼び出されます。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」タブ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。

注 – Identity Manager version 8.1 では、リクエストリソースは外部リソースに置き換えられます。リクエストアダプタを使用して新しい接続を作成できなくなりました。代わりに外部リソースアダプタを使用してください。詳細については、172 ページの「外部リソースとその管理について」を参照してください。

- 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。アカウントに一時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。復元したユーザー ID を指定した電子メールアドレスに送信します。

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。

アカウント作成承認テンプレートを例に使用して、次の手順で電子メールテンプレートをカスタマイズします。

▼ 電子メールテンプレートをカスタマイズする

1. 管理者インタフェースで、「設定」タブをクリックしてから「電子メールテンプレート」サブタブをクリックします。
   「電子メールテンプレート」ページが開きます。

2. 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。

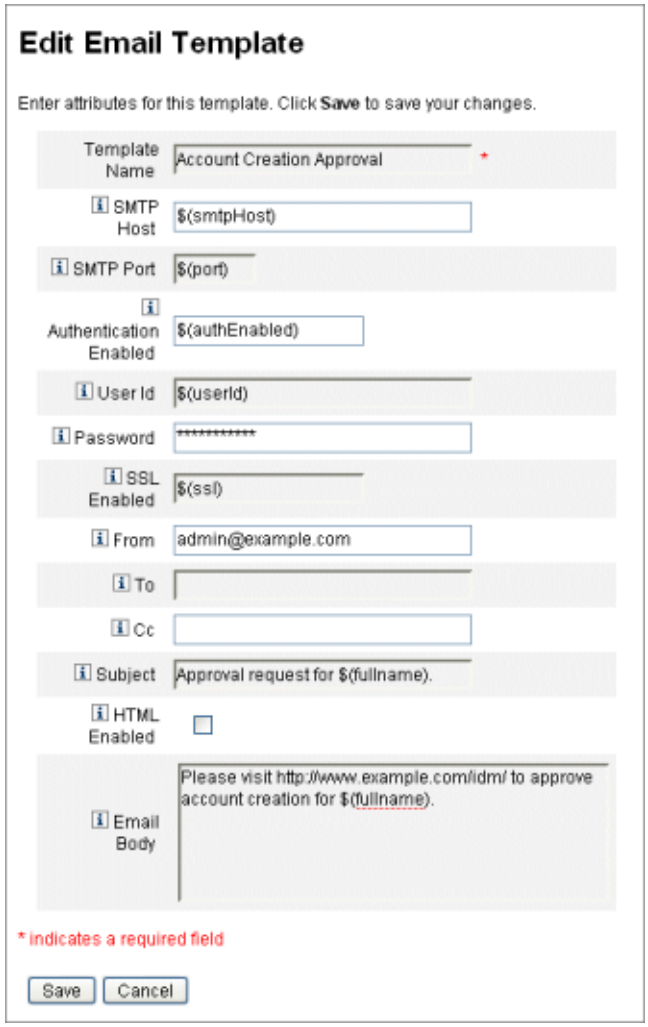


図 4–1　電子メールテンプレートの編集

3　テンプレートの詳細を入力します。

次の情報を入力できます。

- 「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。

4 「保存」をクリックします。

Sun Identity Manager 統合開発環境 (Identity Manager IDE) を使用して電子メールテンプレートを変更することもできます。Identity Manager IDE の詳細については、https://identitymanageride.dev.java.net/ の Web サイトを参照してください。

注 – このサイトにアクセスするには、登録とログインが必要です。

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 リンクを使用することができます。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 4–1 電子メールテンプレート変数

Template	許容変数
パスワードリセット	`$(password)` – 新規に生成されたパスワード
更新の承認	`$(fullname)` – ユーザーのフルネーム
	`$(role)` – ユーザーのロール
更新の通知	`$(fullname)` – ユーザーのフルネーム
	`$(role)` – ユーザーのロール

表 4–1 電子メールテンプレート変数 (続き)

Template	許容変数
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された ID
	$(timestamp)– 電子メールの送信時刻
リクエストリソース	$(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。監査グループを設定すると、あとで監査ログレポートも実行できるようになります。

▼ 「監査設定」ページを開く

監査グループを設定するには、「監査設定」ページを使用します。「監査設定」ページを開くには、次の手順に従います。

1 管理者インタフェースを開きます。

2 「設定」タブをクリックしてから、「監査」サブタブをクリックします。
「監査設定」ページが開きます。

▼ 監査グループを設定する

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。

1 前の節の手順に従って、「監査設定」ページを開きます。
「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。

2 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。

3 「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。

注 – 監査グループの詳細については、第 10 章「監査ログ」の344 ページの「監査設定」を参照してください。

▼ 監査設定グループにイベントを追加する

次の手順を使用して、グループにイベントを追加します。

1 「新規」をクリックします。
ページの下部にイベントが追加されます。

2 「オブジェクトタイプ」列のリストからオブジェクトタイプを選択して、「アクション」列の 1 つ以上の項目を、新しいオブジェクトタイプの「利用可能」領域から「選択」領域に移動します。

3 「**OK**」をクリックしてイベントをグループに追加します。

▼ 監査設定グループ内のイベントを編集する

オブジェクトタイプに対するアクションを追加または削除することで、グループ内のイベントを編集できます。

1 「アクション」列の項目を、オブジェクトタイプの「利用可能」領域から「選択」領域に移動します。

2 「**OK**」をクリックします。

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 つの領域で設定します。

- 「Remedy サーバーの設定」。「リソース」領域から Remedy リソースを作成することにより、Remedy を設定します (159 ページの「リソースリストの管理」 を参照)。リソースの設定後、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 リソースの設定後、Remedy テンプレートを定義します。管理者インタフェースを表示し、「設定」タブをクリックして、「Remedy との統合」をクリックします。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については、『Sun Identity Manager Deployment Reference』の第 1 章「Workflow」を参照してください。

エンドユーザーインタフェースの設定

管理者は、管理者インタフェースのフォームを変更することにより、エンドユーザーインタフェースの特定の側面を設定できます。

▼ エンドユーザーインタフェースに表示される情報を設定する

1. 管理者インタフェースで、メインメニューから「設定」をクリックします。
2. 二次的なメニューで「ユーザーインタフェース」をクリックします。
   「ユーザーインタフェース」ページが開きます。
3. フォームの「エンドユーザーダッシュボード」部分に必要な情報を指定して保存します。フォームのヘルプを参照するには、「ヘルプ」をクリックします。
   フォームの「匿名登録」部分への情報の指定については、95 ページの「匿名登録」を参照してください。

▼ エンドユーザーインタフェースでプロセスダイアグラムを有効にする

プロセスダイアグラムには、エンドユーザーによる要求の起動時またはプロファイルの更新時に Identity Manager が従うワークフローが示されます。有効にすると、エンドユーザーによるフォーム送信後の結果ページがプロセスダイアグラムに表示されます。

プロセスダイアグラムは、エンドユーザーインタフェースで有効にする前に、管理者インタフェース内で有効にする必要があります。詳細については、56 ページの「プロセス図の有効化」を参照してください。

1. 111 ページの「エンドユーザーインタフェースの設定」の手順に従って、ユーザーインタフェース設定ページを開きます。
2. フォームの「結果ページ」セクション内で「エンドユーザープロセスダイアグラムの有効化」オプションを選択します。

   「エンドユーザープロセスダイアグラムの有効化」オプションを選択できない場合は、最初に管理者インタフェースでプロセスダイアグラムを有効にする必要があります。56 ページの「プロセス図の有効化」を参照してください。
3. 「保存」をクリックします。

Identity Manager の登録

管理者には、Identity Manager のインストールを登録することをお勧めします。

登録には Sun Online アカウントとパスワードが必要です。Sun Online アカウントを持っていない場合は、次のアドレスでフォームに必要な情報を入力することで登録できます。

```
https://reg.sun.com/register
```

Identity Manager の登録はコンソールから、または管理者インタフェースを使用して行うことができます。

コンソールから登録する場合は、Sun Service Tag ソフトウェアで使用可能なローカルサービスタグを作成して、Sun システム、ソフトウェア、およびサービスのインベントリを追跡できます。サービスタグクライアントパッケージは、ローカルサービスタグを作成する前にインストールしてください。このパッケージは、次のアドレスにある「Download Service Tags」ボタンをクリックしてダウンロードできます。

```
http://inventory.sun.com/inventory
```

Identity Manager を登録するには、Identity Manager オブジェクトの設定が許可されている管理者アカウントでログオンする必要があります。このアカウントには製品登録の機能が必要です。機能の詳細については、217 ページの「ユーザーへの機能の割り当て」を参照してください。

注 – 製品登録機能を正しく動作させるには、Identity Managerアプリケーションサーバー上のJavaが、SSLに対して適切に設定されている必要があります。java.securityファイル(または同等のファイル)内で参照されるJARファイルがすべて存在する必要があります。

ここからは、Identity Managerの登録に関する情報と操作方法を説明します。この情報は、次のトピックで構成されています。

- 113ページの「コンソールからのIdentity Managerの登録」
- 115ページの「Identity Managerを管理者インタフェースから登録する」

コンソールからのIdentity Managerの登録

この節では、Identity Managerをコンソールから登録する場合に必要な情報について説明します。

registerコマンドの使用法

Identity Managerをコンソールから登録するには、registerコマンドを使用します。ここでは、このコマンドの使用方法について説明します。

registerコマンドの使用法

```
register -local
register -remote [-u <userid> [-p <password>]] [-prompt] -userSOA <userid>
-passSOA <password> [-proxy <proxyHost> [-port <proxyPortNumber>]]
register [-help | -?]
```

registerコマンドのオプション

次の表に、registerコマンドとともに指定できるオプションを示します。

表4–2 コマンドオプション

オプション	説明
-local	このホスト上にサービスタグを作成します。
-remote	このIdentity Managerインストールをネットワーク経由でSunに直接登録します。
-u <userid>	登録を実行する権限を与えられたIdentity Manager管理者のIdentity Managerユーザー ID。

表 4–2 コマンドオプション (続き)

オプション	説明
-p <password>	登録を実行する権限を与えられた Identity Manager 管理者の Identity Manager パスワード。
-prompt	パスワードが入力されていない場合に、対話的に入力を求めます。
-userSOA <userid>	登録に使用する Sun Online アカウントのユーザー ID。-remote オプションを使用して登録する場合に必要です。
-passSOA <password>	登録に使用する Sun Online アカウントのパスワード。-remote オプションを使用して登録する場合に必要です。
-proxy <proxyHost>	Sun オンライン登録サービスへのアクセスに使用するネットワークプロキシ。登録に -remote オプションを使用し、かつ外部インターネットアドレスへのアクセスにプロキシを使用するようにネットワークが設定されている場合に必要です。
-port <proxyPortNumber>	Sun オンライン登録サービスへのアクセスに使用するネットワークプロキシのポート。登録に -remote オプションを使用し、かつ外部インターネットアドレスへのアクセスにプロキシを使用するようにネットワークが設定されている場合に必要です。
-help | -?	このコマンドのヘルプをコンソールに出力します。

▼ Identity Manager をコンソールから登録する

Identity Manager をコンソールから登録するには、ローカルサービスタグを作成するか、インターネットを通じて Sun に登録する必要があります。次の手順を使用します。

1 **Identity Manager コンソール (コマンド行) インタフェースを起動します。**

- Windows のコマンド行で、次のコマンドを入力します。

  %WSHOME%\bin\lh

- UNIX のコマンド行で、次のコマンドを入力します。

  $WSHOME/bin/lh

2 register コマンドを次のように実行します。

- ローカルサービスタグを作成する場合は、次のように実行します。

  register -local

- インターネットを通じて Identity Manager を登録する場合は、次のコマンドを実行します。

  register -remote -u <*userid***> -p <***password***> -userSOA <***soaUserid***> -passSOA <***soaPassword* **> -proxy <***proxyHost***> -port <** *proxyPortNumber***>**

各表記の意味は次のとおりです。

- **userid** は、登録を実行する権限を与えられた Identity Manager 管理者の Identity Manager ユーザー ID です。
- **password** は、登録を実行する権限を与えられた Identity Manager 管理者の Identity Manager パスワードです。
- **soaUserid** は、登録に使用する Sun Online アカウントのユーザー ID です。
- **soaPassword** は、登録に使用する Sun Online アカウントのパスワードです。
- **proxyHost** は、Sun オンライン登録サービスへのアクセスに使用するネットワークプロキシです。これは、外部のインターネットアドレスへのアクセスにプロキシを使用するようにネットワークが設定されている場合にのみ必要です。
- **proxyPortNumber** は、Sun オンライン登録サービスへのアクセスに使用するネットワークプロキシのポートです。これは、外部のインターネットアドレスへのアクセスにプロキシを使用するようにネットワークが設定されている場合にのみ必要です。

▼ Identity Managerを管理者インタフェースから登録する

ローカルサービスタグを作成する必要がない場合は、管理者インタフェースから Identity Manager を登録します。

1. 管理者インタフェースで、「設定」をクリックします。
2. 二次的なメニューで「製品登録」をクリックします。
   「製品登録」ページが開きます。
3. フォームに値を入力し、「今すぐ登録」をクリックします。個別のフォームフィールドの情報を表示するには、**i-Help** をクリックします。

注 –

- アプリケーションサーバーで外部への SSL 接続が許可されていない場合は、次のエラーメッセージが表示されます。

  ```
  Failed to register on Sun Connection server
  due to invalid Sun Online Account user/password.
  ```

  この問題を解決するには、適切な信頼できるルート証明書をアプリケーションサーバーのキーストアに追加します。詳細については、使用しているアプリケーションサーバーのマニュアルを参照してください。
- 以前のバージョンの `xml-apis.jar` および `xercesImpl.jar` がアプリケーションサーバーのクラスパスに存在する場合は、次のエラーメッセージが表示されることがあります。

  ```
  java.lang.NoSuchMethodError:org.w3c.dom.Node.getTextContent()Ljava/lang/String;
  ```

  この問題を解決するには、クラスパスを修正して、最新バージョンの `xml-apis.jar` および `xercesImpl.jar` だけが存在するようにします。

Identity Manager 設定オブジェクトの編集

Identity Manager の管理中に、Identity Manager システム設定オブジェクト (「システム設定ファイル」とも呼ばれる) またはその他の類似オブジェクトを編集するように求められることがあります。

1. 次の URL をブラウザに入力して、Identity Manager デバッグページを開きます。

   `http://<` *AppServerHost*`>:<`*Port*`>/idm/debug/session.jsp`

   システム設定ページが開きます。

   注 – `/idm/debug/` ページを表示するには、デバッグ機能を使用できる必要があります。

2. 「List Objects」ボタンを見つけて、隣接する「Type」ドロップダウンリストから「Configuration」を選択します。
3. 「List Objects」ボタンをクリックします。

   「List Objects of type: Configuration」ページが表示されます。
4. オブジェクトのリストで、必要なオブジェクトを見つけて「編集」をクリックします。

   たとえば、システム設定オブジェクトを編集するには、「System Configuration」を検索して「編集」をクリックします。

5. オブジェクトを編集して、「保存」をクリックします。
6. サーバーを再起動するように指示された場合は、再起動します。

◆ ◆ ◆ 第 5 章

ロールとリソース

この章では、Identity Manager のロールとリソースについて説明します。

この章の情報は、次のトピックで構成されています。

- 119 ページの「ロールとその管理について」
- 158 ページの「Identity Manager リソースとその管理について」
- 172 ページの「外部リソースとその管理について」

ロールとその管理について

この節では、Identity Manager でのロールの設定について説明します。大規模な組織では、ロールベースのリソース割り当てにより、リソース管理が大幅に簡略化されます。

注 – ロールと管理者ロールを混同しないようにしてください。ロールは、外部リソースへのエンドユーザーアクセスの管理に使用されます。一方、管理者ロールの主な用途は、ユーザー、組織、機能など、内部の Identity Manager オブジェクトへの管理者アクセスの管理です。

この節では、ロールについて説明します。管理者ロールについては、217 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。

ロールとは

ロールとは、リソースのアクセス権限をグループ分けし、ユーザーに効率的に割り当てる Identity Manager オブジェクトです。

ロールは、次の 4 つのロールタイプに分けられます。

- ビジネスロール
- IT ロール
- アプリケーション
- アセット

「ビジネスロール」は、組織で類似したタスクを実行する人が職務を遂行するために必要とするアクセス権限をグループに編成します。通常、ビジネスロールはユーザーの職務機能を表します。たとえば金融機関では、ビジネスロールは出納係、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。

IT ロール、アプリケーション、およびアセットは、リソースエンタイトルメントをグループに編成します。エンドユーザーがリソースにアクセスできるようにするには、IT ロール、アプリケーション、およびアセットをビジネスロールに割り当てて、ジョブの実行に必要なリソースにユーザーがアクセスできるようにします。IT ロールには、アプリケーション、アセット、リソースの特定のセットが含まれます。 これには、割り当て済みリソースに対する特定のエンタイトルメントが含まれます。IT ロールには、ほかの IT ロールを含めることもできます。

注 – ロールタイプの概念は、Identity Manager Version 8.0 で新しくなりました。組織が以前のバージョンの Identity Manager からバージョン 8.0 にアップグレードした場合、従来のロールは IT ロールとしてインポートされています。詳細は、121 ページの「バージョン 8.0 より前のバージョンで作成されたロールの管理」を参照してください。

IT ロール、アプリケーション、およびアセットは、必須、条件付き、オプションのいずれかにできます。

- 必須ロールは、常にエンドユーザーに割り当てられます。
- 条件付きロールを割り当てるには、条件が true に評価される必要があります。
- オプションロールは個別にリクエストでき、承認されるとエンドユーザーに割り当てられます。

ビジネスロールデザイナは、必須、条件付き、およびオプションのロールを使用して、エンドユーザーの管理者がエンドユーザーのアクセス権をきめ細かく調整できるだけの柔軟性を確保しつつ、含まれるロールへの詳細なアクセスを定義して法規制へのコンプライアンスを達成できます。条件付きまたはオプションのロールを割り当てられたユーザーも、割り当てられた同じビジネスロールを共有できますが、割り当てられるアクセス権は異なります。この方法では、組織内のアクセス要件の順列ごとにビジネスロールを新たに定義する必要がないため、「ロールエクスプロージョン」と呼ばれる問題が発生しません。

ロールタイプの使用

ここでは、ロールタイプを効果的に使用する方法について説明します。ロールタイプの説明については、前の節を参照してください。

バージョン 8.0 より前のバージョンで作成されたロールの管理

以前のバージョンの Identity Manager からバージョン 8.0 にアップグレードした組織では、従来のロールが自動的に IT ロールに変換されています。これらの IT ロールは、ユーザーに直接割り当てられたままになります。アップグレード処理の過程で、従来のロールにロール所有者が割り当てられることはありません。ただし、あとでロール所有者を割り当てることは可能です。(ロール所有者については、132 ページの「ロール所有者とロール承認者の指定」」を参照)

デフォルトでは、バージョン 8.0 にアップグレードした組織は、IT ロールとビジネスロールの両方をユーザーに直接割り当てることができます (図 5–2を参照)。

従来のロールを持つ組織は、次の節に示すガイドラインに基づいて新しいロールを作成することを検討してください。

ロールタイプを使用した柔軟なロールの設計

IT ロール、アプリケーション、およびアセットは、ロールデザイナの構成単位です。これら 3 つのロールタイプを組み合わせて、ユーザーエンタイトルメント (アクセス権) が構築されます。IT ロール、アプリケーション、およびアセットは、その後、ビジネスロールに割り当てられます。

ビジネスロールの設計

Identity Manager では、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可能です。Identity Manager 8.0 でロールタイプが導入されたため、ビジネスロールをユーザーに直接割り当てることだけをお勧めします。実際には、組織が 8.0 より前のバージョンの Identity Manager をインストールし、バージョン 8.0 以上にアップグレードした場合を除き、デフォルトでは他のロールタイプのいずれもユーザーに直接割り当てることはできません。このデフォルトの制限は、ロール設定オブジェクトを変更することによって変更できます (154 ページの「ロールタイプの設定」)。

複雑さを軽減するため、ビジネスロールを入れ子にすることはできません。すなわち、1 つのビジネスロールに別のビジネスロールを含めることはできません。また、ビジネスロールにリソースおよびリソースグループを直接含めることもできません。その代わり、リソースおよびリソースグループを IT ロールまたはアプリケーションに割り当ててください。そうすると、IT ロールまたはアプリケーションを 1 つ以上のビジネスロールに割り当てることができます。

IT ロールの設計

IT ロールには、アプリケーション、アセット、およびほかの IT ロールを含めることができます。IT ロールに、リソースやリソースグループを含めることもできます。

IT ロールの作成および管理は、組織の IT スタッフ、またはリソース内の特定の特権の有効化に必要なエンタイトルメントを理解しているリソース所有者により行われることが想定されています。

アプリケーションとアセットの設計

アプリケーションおよびアセットとは、エンドユーザーがジョブの実行に必要なことを説明するための、よく使用されるビジネス用語を表すロールタイプです。たとえば、アプリケーションロールには、「Customer Support Tools」や「Intranet HR-Tool Admin」という名前が付けられる可能性があります。

- アプリケーションにロールを含めることはできませんが、リソースやリソースグループを含めることはできます。アプリケーションでは、含まれるリソース上の特定のアプリケーションへのアクセスを制限する特定のエンタイトルメントを定義することもできます。
- 通常、アセットは、手動のプロビジョニングを必要とする、携帯電話やポータブルコンピュータなどの非接続または非デジタルのリソースです。このため、アセットにロール、リソース、またはリソースグループを含めることはできません。

アプリケーションおよびアセットは、ビジネスロールおよび IT ロールに割り当てることが想定されています。

注 –

ロール管理者には、次の機能を 1 つ以上割り当ててください。

- Asset Administrator
- Application Administrator
- Business Role Administrator
- IT Role Administrator

詳細は、217 ページの「ユーザーへの機能の割り当て」を参照してください。

ロールタイプの概要

次の図に、4 つのロールタイプのそれぞれに割り当て可能なロールタイプ、リソース、およびリソースグループを示します。また、4 つのロールタイプすべてにロールタイプの除外を割り当て可能であることも示します。(ロールの除外については、127 ページの「リソースとリソースグループを割り当てる」を参照)

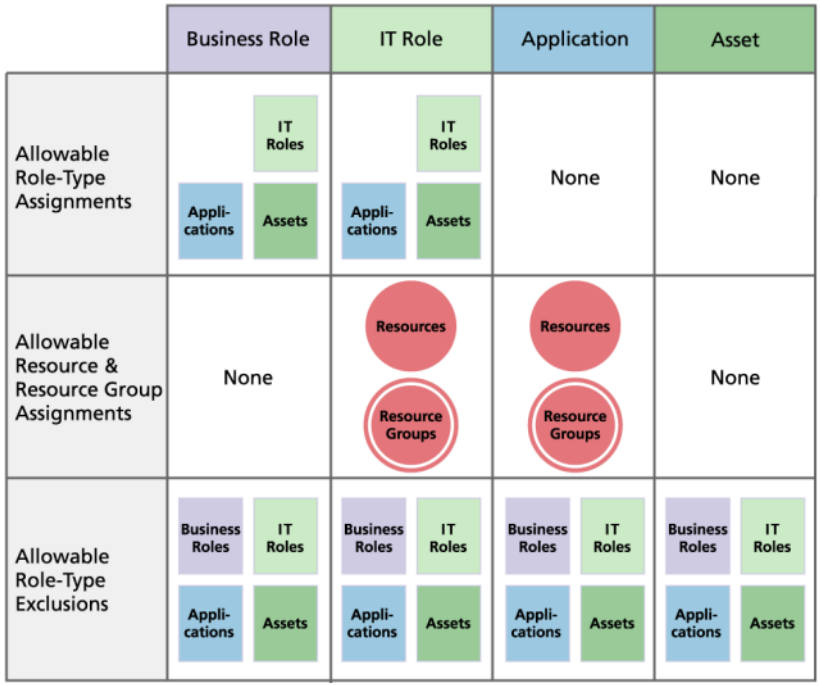


図 5–1 ビジネスロール、IT ロール、アプリケーション、およびアセットのロールタイプ

オプション、条件付き、および必須のロール (119 ページの「ロールとは」) により、柔軟性が増します。柔軟性の高いロール定義により、組織が管理する必要のあるロールの総数を減らすことができます。

図 5–2 は、8.0 より前のバージョンの Identity Manager がバージョン 8.0 以上にアップグレードされた場合に、ビジネスロールと IT ロールがユーザーに直接割り当てられることを示します。アップグレード時に、従来のロールは IT ロールに変換され、下位互換を保証するために、IT ロールはユーザーに直接割り当てられます。Identity Manager が 8.0 より前のバージョンからアップグレードされたものではない場合、ビジネスロールだけをユーザーに直接割り当てることができます。

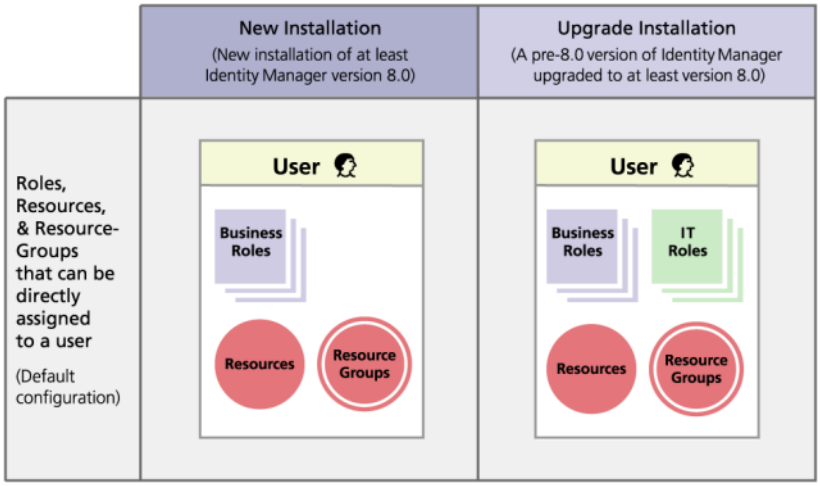


図5–2 ユーザーに直接割り当て可能なロールおよびリソース

ロールの作成

この節では、ロールを作成する方法を次のような構成で説明します。

- 124 ページの「「ロールの作成」フォームを使用してロールを作成する」
- 127 ページの「リソースとリソースグループを割り当てる」
- 128 ページの「割り当てられているリソース属性値を編集する」
- 130 ページの「ロールとロールの除外を割り当てる」
- 132 ページの「ロール所有者とロール承認者の指定」
- 134 ページの「通知の指定」
- 135 ページの「変更承認作業項目と承認作業項目の開始」

注 – ロールの指定のヒントについては、121 ページの「ロールタイプを使用した柔軟なロールの設計」を参照してください。

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。

▼ 「ロールの作成」フォームを使用してロールを作成する

1 管理者インタフェースで、メインメニューから「ロール」をクリックします。
「ロール」ページ(「ロールのリスト」タブ)が開きます。

2 ページ下部にある「新規」をクリックします。

「IT ロール の作成」ページが開きます。別のタイプのロールを作成するには、「タイプ」ドロップダウンメニューを使用します。

3 「ID」タブのフォームフィールドに必要な情報を指定します。

次の図は、「ID」タブを示したものです。

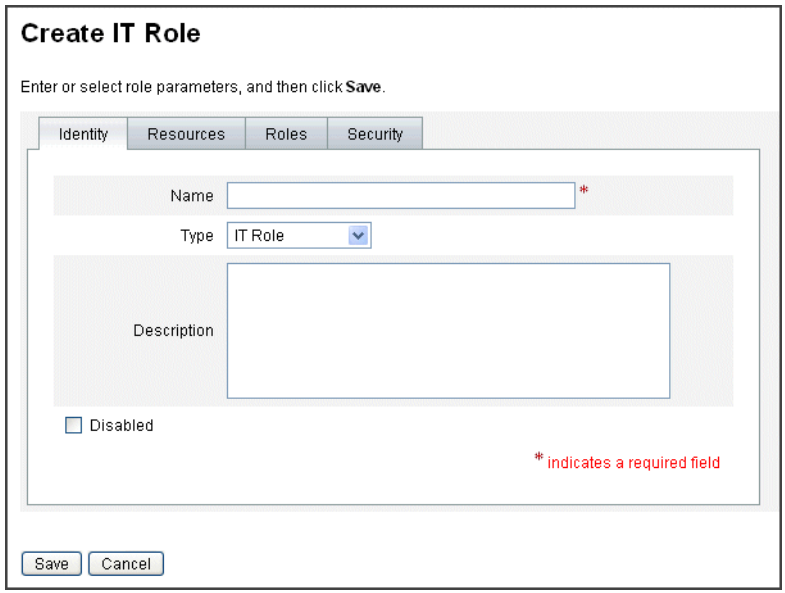


図 5–3 「IT ロール の作成」ページの「ID」タブ

4 「ID」タブのフォームフィールドに必要な情報を指定します (該当する場合)。このタブのフィールドに情報を指定するために役立つ情報については、オンラインヘルプ、および127 ページの「リソースとリソースグループを割り当てる」を参照してください。

ロールに拡張属性値を設定するために役立つ情報については、167 ページの「リソースアカウント属性を表示または編集する」を参照してください。

次の図は、「リソース」タブを示したものです。

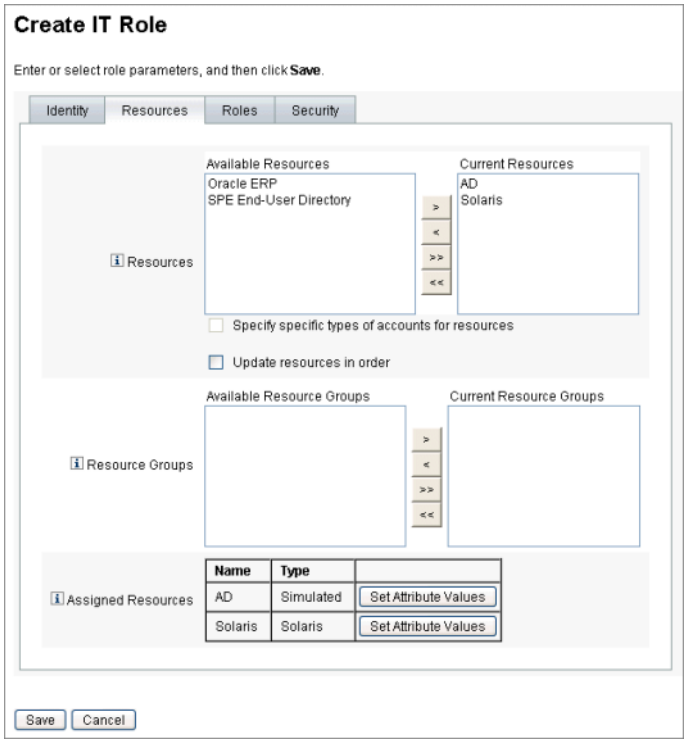


図 5–4 「IT ロールの作成」ページの「リソース」タブ

5 「ロール」タブのフォームフィールドに必要な情報を指定します (該当する場合)。このタブのフィールドに情報を指定するために役立つ情報については、オンラインヘルプ、および**130** ページの「ロールとロールの除外を割り当てる」を参照してください。

図 5–6 は、「ロール」タブを示したものです。

6 「セキュリティー」タブのフォームフィールドに必要な情報を指定します。このタブのフィールドに情報を指定するために役立つ情報については、オンラインヘルプ、および**132** ページの「ロール所有者とロール承認者の指定」と**134** ページの「通知の指定」を参照してください。

132 ページの「ロール所有者とロール承認者の指定」に、「セキュリティー」タブを示します。

7 ページの下部にある「保存」をクリックします。

8 ロール名と説明は、「ロールの作成」フォームの「**ID**」タブに入力します。新しいロールを作成する場合は、「タイプ」ドロップダウンメニューで作成するロールタイプを選択します。

図 5–4 は、「ロールの作成」フォームの「ID」タブの「ID」セクションを示したものです。このフォームの使用方法については、オンラインヘルプを参照してください。

▼ リソースとリソースグループを割り当てる

リソースとリソースグループは、「ロールの作成」フォームの「リソース」タブを使って、IT ロールおよびアプリケーションロールに直接割り当てることができます。リソースについては、158 ページの「Identity Manager リソースとその管理について」の節で後述します。リソースグループについては、168 ページの「リソースグループ」の節で説明します。

- 「ビジネスロール」に割り当てることができるのはロールのみのため、リソースとリソースグループを「ビジネスロール」に直接割り当てることはできません。
- リソースおよびリソースグループをアセットロールに割り当てることはできません。アセットロールは、手動プロビジョニングが必要な非接続または非デジタルのリソース用に予約されています。

ここでは、「ロールの作成」フォームに必要な情報を指定したあとで、リソースおよびリソースグループをロールに割り当てる方法について説明します。最初に、124 ページの「「ロールの作成」フォームを使用してロールを作成する」を参照してください。

1 「ロールの作成」ページの「リソース」タブをクリックします。

2 リソースを割り当てるには、「利用可能なリソース」列でリソースを選択し、矢印ボタンをクリックしてそのリソースを「現在のリソース」列に移します。

3 複数のリソースを割り当てる場合は、リソースを更新する順番を指定することができます。「順番にリソースを更新する」チェックボックスを選択し、「+」ボタンと「-」ボタンを使用して「現在のリソース」列のリソースの順番を変更します。

4 このロールにリソースグループを割り当てるには、「利用可能なリソースグループ」列でリソースグループを選択し、矢印ボタンをクリックしてそのリソースグループを「現在のリソースグループ」列に移動します。リソースグループはリソースの集まりであり、リソースアカウントを作成および更新する順番を指定するための別の方法を提供します。

5 このロールのアカウント属性をリソース単位で指定するには、「割り当てられたリソース」セクションの「属性値の設定」をクリックします。詳細は、**167** ページの「リソースアカウント属性を表示または編集する」を参照してください。

6 「保存」をクリックしてロールを保存するか、「**ID**」、「ロール」、または「セキュリティー」タブをクリックしてロールの作成処理を続行します。

次の図は、「ロールの作成」フォームの「リソース」タブを示したものです。

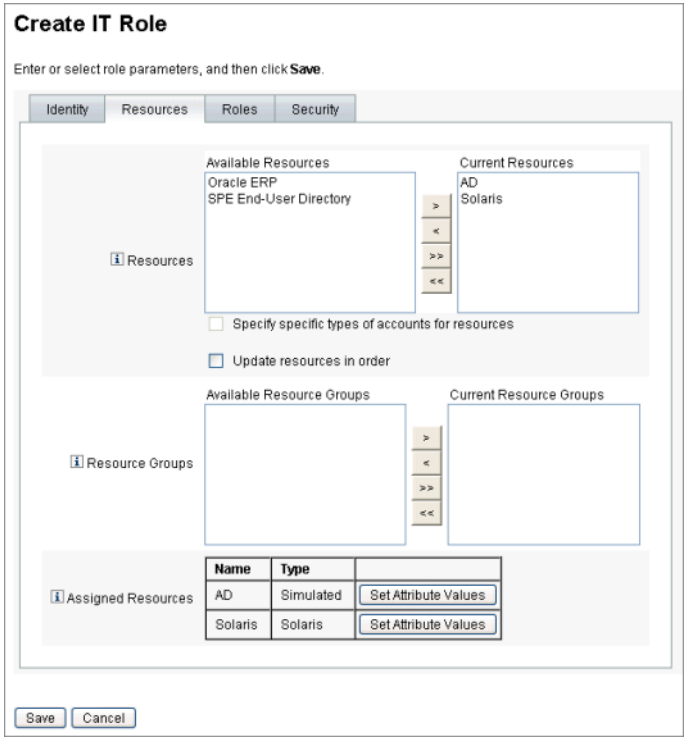
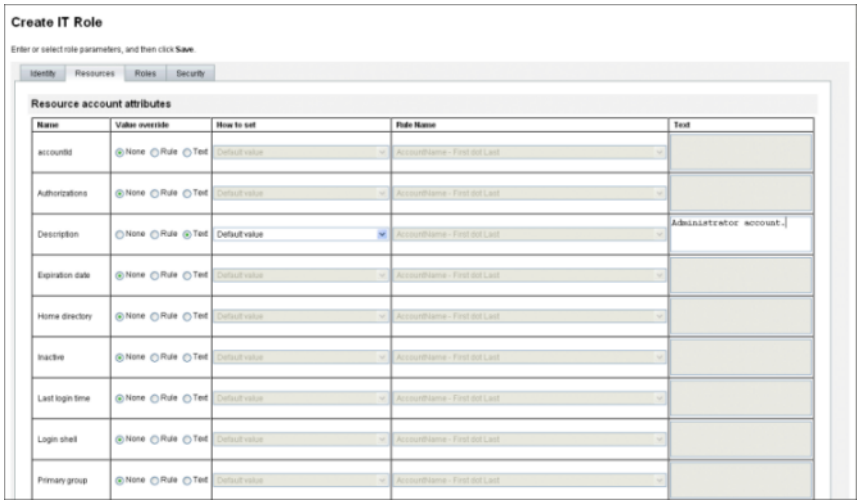


図 5–5 タブ付きの「ロールの作成」フォームの「リソース」セクション

▼ 割り当てられているリソース属性値を編集する

「割り当てられたリソース」テーブルを使用して、ロールに割り当てられたリソースのリソース属性値を設定または変更します。リソースには、ロールごとに定義された異なる複数の属性値を含めることができます。「属性値の設定」ボタンをクリックすると、「リソースアカウントの属性」ページが開きます。

次の図に「リソースアカウントの属性」ページを示します。このページを使って、ロールに割り当てられたリソースに拡張属性値を設定します。



1 「リソースアカウントの属性」ページから、属性ごとに新しい値を指定し、属性値の設定方法を決定します。

Identity Manager では、値を直接設定することや規則に従って設定することができ、既存の値を上書きしたり値を既存の値とマージしたりするためのさまざまなオプションが用意されています。リソース属性値についての一般的な情報は、167 ページの「リソースアカウント属性を表示または編集する」を参照してください。

次のオプションを使用して、リソースアカウント属性ごとに値を設定します。

- 「値の上書き」。次のオプションのいずれかを選択します。
  - 「なし」 (デフォルト)。値は何も設定されません。
  - 「規則」。規則に従って値を設定します。

    このオプションを選択した場合には、リストから規則名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、隣接する「テキスト」フィールドにテキストを入力する必要があります。
- 「設定方法」。次のオプションのいずれかを選択します。
  - 「デフォルト値」。規則またはテキストをデフォルトの属性値に設定します。

    ユーザーはこの値を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で指定された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で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で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で指定された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、過去に属性に値が指定されていた場合でも、新しい値は Null となります。
- 「 強制的に値とマージ」。規則またはテキストで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、ロールが割り当てられたときに割り当てられた値は削除されますが、元の属性値はそのままです。
- 「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」領域で「規則」を選択した場合には、このリストから規則を選択します。
- 「テキスト」。「値の上書き」領域で「テキスト」を選択した場合には、属性値に追加するテキスト、属性値から削除するテキスト、または属性値として使用するテキストを入力します。

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

▼ ロールとロールの除外を割り当てる

ロールは、「ロールの作成」フォームの「ロール」タブを使って、ビジネスロールと IT ロールに割り当てることができます。割り当てられたロールは、「含まれるロール」のテーブルに追加されます。

- ロールを「アプリケーション」ロールと「アセット」ロールに割り当てることはできません。
- 「ビジネスロール」をロールタイプに割り当てることはできません。

「ロールの作成」フォームの「ロール」タブを使って、ロールの除外を 4 つのロールタイプすべてに割り当てることができます。ロールの除外を含むロールをユーザーに割り当てた場合、除外されたロールをそのユーザーに割り当てることはできません。ロールの除外は、「ロールの除外」テーブルに追加されます。

ここでは、「ロールの作成」フォームに必要な情報を指定したあと、ロールに 1 つ以上のロールを割り当てる方法について説明します。最初に、124 ページの「「ロールの作成」フォームを使用してロールを作成する」を参照してください。

「ロール」タブに必要な情報を指定する

1. 「ロールの作成」ページの「ロール」タブをクリックします。
2. 「含まれるロール」セクションの「追加」をクリックします。
   タブが更新され、「含まれるロールの検索」フォームが表示されます。
3. このロールに割り当てるロールを検索します。最初に必須のロールを割り当てます。条件付きおよびオプションロールはあとで追加します。
   検索フォームの使用方法については、136 ページの「ロールを検索する」を参照してください。ビジネスロールを入れ子にしたり、ほかのロールタイプに割り当てたりすることはできません。
4. 割り当てる 1 つ以上のロールをチェックボックスで選択し、「追加」をクリックします。
   タブが更新され、「含まれるロールの追加」フォームが表示されます。
5. 「関連付けタイプ」ドロップダウンメニューから「必須」(あるいは必要に応じ「条件付き」または「オプション」)を選択します。
   「OK」をクリックします。
6. 前の 4 つの手順を繰り返して、条件付きロールを追加します (必要な場合)。前の 4 つの手順をもう一度繰り返して、オプションロールを追加します (必要な場合)。
7. 「保存」をクリックしてロールを保存するか、「ID」、「リソース」、または「セキュリティー」タブをクリックしてロールの作成処理を続行します。
   図 5–6 は、「ロールの作成」フォームの「ロール」タブを示したものです。このフォームの使用方法については、オンラインヘルプを参照してください。

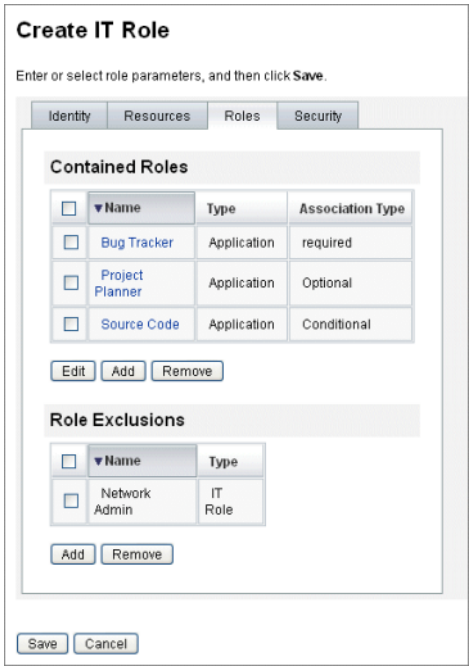


図 5–6 タブ付きの「ロールの作成」フォームの「ロール」セクション

ロール所有者とロール承認者の指定

ロールには、「所有者」と「承認者」が指定されています。ロール所有者だけが、ロールを定義するパラメータの変更を承認できます。また、ロール承認者だけがエンドユーザーへのロールの割り当てを承認できます。

注 – Identity Manager を Sun™ Role Manager に統合した場合は、Identity Manager の機能を手動で無効にしてすべてのロール変更承認および通知を実行することによって、Role Manager がこれらのアクションを処理できるようにしてください。

Identity Manager で、次のように、`RoleConfiguration` 設定オブジェクトを編集する必要があります。

- `changeApproval` のすべてのインスタンスを検索し、値を **`false`** に設定します。
- `changeNotificaiton` のすべてのインスタンスを検索し、値を **`false`** に設定します。

ロール所有者になるということは、ロールを介して割り当てられる、基盤となるリソースアカウント権限への責任があるビジネス所有者になることを意味します。管理者がロールに変更を加えた場合は、その変更を実行する前に、ロール所有者が変更を承認する必要があります。この機能によって、ビジネスの所有者の認識や承認

なしに、管理者が役割を変更することを防いでいます。ただし、変更承認がロール設定オブジェクトで無効化されている場合は、変更を実行するためにロール所有者の承認は必要ありません。

ロールの変更承認に加え、ロールの有効化、無効化、および削除もロール所有者の承認なしに行うことはできません。

所有者および承認者は、ロールに直接追加することも、ロール割り当て規則を使って動的に追加することもできます。Identity Manager では、所有者や承認者なしでロールを作成できます (ただし、この方法は推奨されていません)。

注 – ロール割り当て規則には、`RoleUserRule authType` があります。

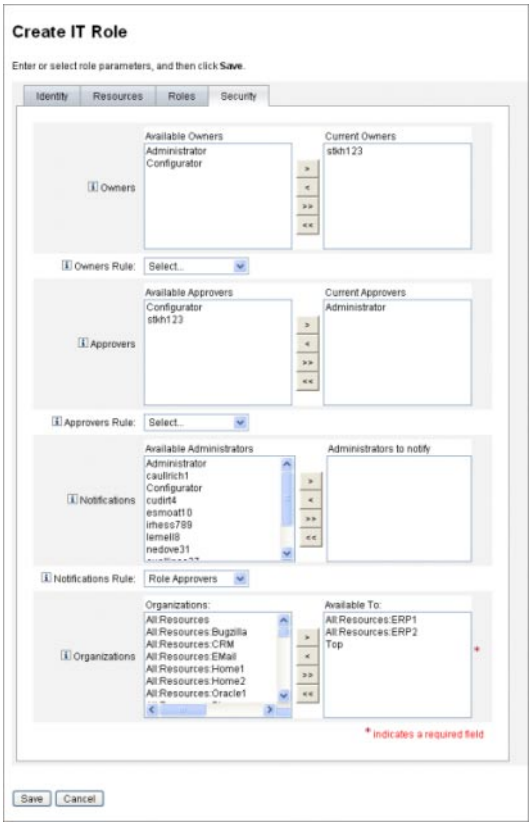
カスタムのロール割り当て規則を作成する必要がある場合は、デフォルトのロール割り当て規則オブジェクト 3 つを参照し、これらのオブジェクトをサンプルとして使用してください。

- Role Approvers
- Role Notifications
- Role Owners

作業項目に承認が必要な場合、所有者および承認者に電子メールで通知が送られます。変更承認作業項目および承認作業項目については、135 ページの「変更承認作業項目と承認作業項目の開始」の節で説明します。

所有者および承認者は、「ロールの作成」フォーム内の「セキュリティー」タブのロールに追加されます。

132 ページの「ロール所有者とロール承認者の指定」に、「ロールの作成」フォームの「セキュリティー」タブを示します。このフォームの使用方法については、オンラインヘルプを参照してください。



通知の指定

ロールがユーザーに割り当てられたときに、通知を 1 人以上の管理者に送信できます。

通知受信者の指定は、省略可能です。ロールがユーザーに割り当てられているときに、承認を不要に設定すると、管理者への通知を選択できます。また、承認を指定する際、ある管理者を承認者にして、別の管理者を通知の受信者にすることもできます。

所有者および承認者の場合と同様、通知をロールに直接追加することも、ロール割り当て規則を使って動的に追加することもできます。ロールがユーザーに割り当てられたときに、通知受信者は電子メールで通知されます。ただし、承認が不要なため、作業項目は作成されません。

通知は、「ロールの作成」フォームの「セキュリティー」タブでロールに割り当てます。132 ページの「ロール所有者とロール承認者の指定」に、「ロールの作成」フォームの「セキュリティー」タブを示します。

変更承認作業項目と承認作業項目の開始

ロールの変更時に、ロール所有者が「変更承認」の電子メール、または「変更通知」の電子メールを受信するようにできます。また、メールを受信しないようにすることもできます。ロールがユーザーに割り当てられると、ロール承認者はロール承認の電子メールを受信します。

デフォルトでは、ロール所有者は、所有しているロールが変更されたときは必ず、変更承認の電子メールを受信します。ただし、この動作はロールタイプごとに設定が可能です。たとえば、ビジネスロールとITロールで変更承認を有効にし、アプリケーションロールとアセットロールで変更通知を有効にできます。

変更承認および変更通知の電子メールを有効または無効にする手順については、154ページの「ロールタイプの設定」を参照してください。

次に、変更承認および変更通知がどのように機能するかを説明します。

- 「変更承認」が有効な場合、管理者がロールを変更すると、作業項目が生成され、承認の電子メールがロール所有者に送信されます。変更を実行するには、ロール所有者が作業項目を承認する必要があります。変更承認の作業項目は委任できます。詳細は、234ページの「ユーザーアカウントの承認」を参照してください。

  変更承認が無効な場合、作業項目は生成されず、変更承認の電子メールがロール所有者に送信されることもありません。
- 変更通知が有効な場合、管理者がロールを変更すると、変更はただちに実行され、通知の電子メールがロール所有者に送信されます。

  変更通知が無効な場合、通知はロール所有者に送信されません。

ロールがユーザーに割り当てられると、ロール承認者はロール承認の電子メールを受信します。Identity Managerでは、ロール承認の電子メールを無効にすることはできません。

ロール承認では、ユーザーにロールが割り当てられると、作業項目が生成され、承認の電子メールがロール承認者に送信されます。ロールをユーザーに割り当てるには、ロール承認者が作業項目を承認する必要があります。

変更承認作業項目と承認作業項目は委任できます。作業項目の委任については、231ページの「作業項目の委任」を参照してください。

ロールの編集と管理

大半のロール編集およびロール管理タスクは、「ロールの検索」および「ロールのリスト」タブで実行できます。これらのサブタブは、メインメニューの「ロール」タブ内にあります。

この節は次のトピックで構成されています。

- 136 ページの「ロールを検索する」
- 137 ページの「ロールを表示する」
- 138 ページの「ロールを編集する」
- 139 ページの「ロールを複製する」
- 139 ページの「ロールを別のロールに割り当てる」
- 140 ページの「別のロールに割り当てられたロールを削除する」
- 141 ページの「ロールを有効または無効にする」
- 142 ページの「ロールを削除する」
- 142 ページの「リソースまたはリソースグループをロールに割り当てる」
- 143 ページの「ロールに割り当てられているリソースまたはリソースグループを削除する」

▼ ロールを検索する

指定した検索条件を満たすロールを検索するには、「ロールの検索」タブを使用します。

「ロールの検索」タブを使用することで、ロール所有者と承認者、割り当てられたアカウントタイプ、含まれるロールなど、さまざまな条件に基づいてロールを検索できます。

ロールに割り当てられたユーザーの検索については、152 ページの「特定のロールに割り当てられたユーザーを検索する」を参照してください。

1. 管理者インタフェースで、「ロール」タブをクリックします。
   「ロールのリスト」タブが開きます。

2. 「ロールの検索」二次タブをクリックします。
   図 5–7 は、「ロールの検索」タブを示したものです。このフォームの使用方法については、オンラインヘルプを参照してください。

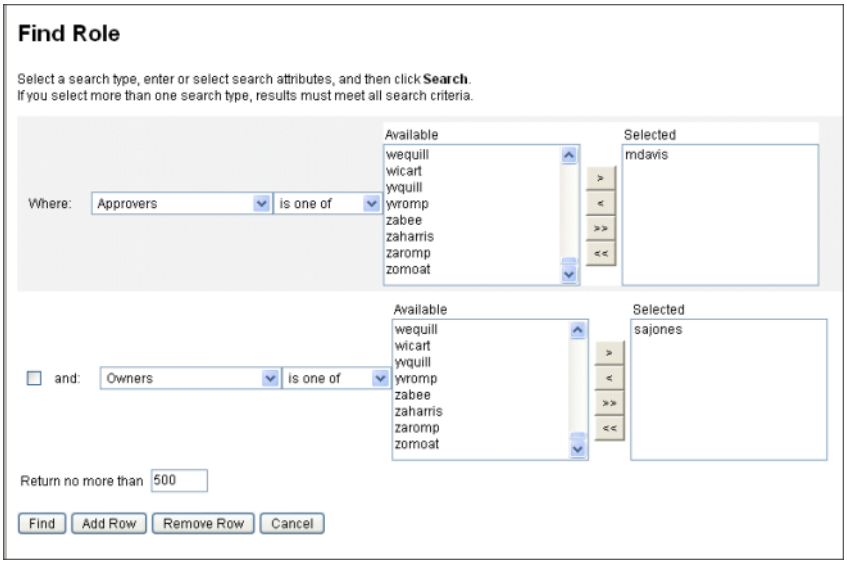


図 5–7 「ロールの検索」タブ

ドロップダウンメニューを使用して、検索用のパラメータを定義します。「行の追加」ボタンをクリックして、追加のパラメータを指定します。

▼ ロールを表示する

ロールを表示するには、「ロールのリスト」タブを使用します。「ロールのリスト」ページの上部にあるフィルタフィールドを使用して、名前またはロールタイプに基づいてロールを検索します。フィルタは、大文字と小文字を区別しません。

- 管理者インタフェースで、「ロール」タブをクリックします。

  「ロールのリスト」タブが開きます。

  図 5–8 は、「ロールのリスト」タブを示したものです。このフォームの使用方法については、オンラインヘルプを参照してください。

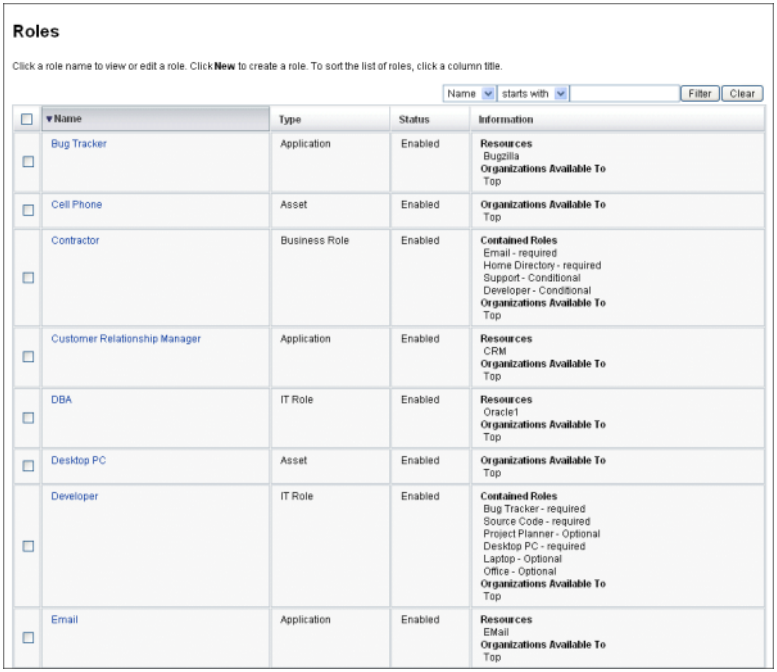


図 5–8 「ロールのリスト」タブ

▼ ロールを編集する

「ロールのリスト」または「ロールの検索」タブを使って、編集するロールを検索します。ロールの変更時に変更承認が true に設定されている場合は、変更を実行するために、ロール所有者が変更を承認する必要があります。

ロールが変更されたユーザーの更新については、147 ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

1. 136 ページの「ロールを検索する」または137 ページの「ロールを表示する」の手順に従って、編集するロールを検索します。

2. 編集するロールの名前をクリックします。
   「ロールの編集」ページが開きます。

3. 必要に応じてロールを編集します。「ID」、「リソース」、「ロール」、および「セキュリティー」タブに必要な情報を指定するために役立つ情報については、124 ページの「「ロールの作成」フォームを使用してロールを作成する」の手順を参照してください。
   「保存」をクリックします。「ロール変更の確認」ページが開きます。

4 このロールをユーザーに割り当てる場合は、ロールが変更されたユーザーをいつ更新するかを選択できます。詳細は、147 ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

5 変更を保存するには、「保存」をクリックします。

▼ ロールを複製する

1 136 ページの「ロールを検索する」または137 ページの「ロールを表示する」の手順に従って、編集するロールを検索します。

2 複製するロールの名前をクリックします。
「ロールの編集」ページが開きます。

3 「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。
「ロール: 作成または名前変更?」ページが開きます。

4 「作成」をクリックして、ロールのコピーを作成します。

▼ ロールを別のロールに割り当てる

ロールの割り当てに関する Identity Manager の要件については、119 ページの「ロールとは」および121 ページの「ロールタイプの使用」で説明します。ロールを割り当てる前にこの情報を理解しておいてください。

親ロールのロール所有者が承認すると、Identity Manager がロールのロール割り当てを変更します。

1 1 つ以上の「含まれるロール」の割り当て先となるビジネスロールまたは IT ロールを検索します。ロールの割り当て先にできるのはビジネスロールと IT ロールのみです。ロールを検索するには、136 ページの「ロールを検索する」または137 ページの「ロールを表示する」の手順を使用します。

2 ビジネスロールまたは IT ロールをクリックして開きます。
「ロールの編集」ページが開きます。

3 「ロールの編集」ページの「ロール」タブをクリックします。

4 「含まれるロール」セクションの「追加」をクリックします。
タブが更新され、「含まれるロールの検索」フォームが表示されます。

5 このロールに割り当てるロールを検索します。最初に必須のロールを割り当てます。条件付きおよびオプションロールはあとで追加します。

検索フォームの使用方法については、136 ページの「ロールを検索する」を参照してください。ビジネスロールを入れ子にしたり、ほかのロールタイプに割り当てたりすることはできません。

6 割り当てる 1 つ以上のロールをチェックボックスで選択し、「追加」をクリックします。

タブが更新され、「含まれるロールの追加」フォームが表示されます。

7 「関連付けタイプ」ドロップダウンメニューから「必須」(あるいは必要に応じ「条件付き」または「オプション」)を選択します。

「OK」をクリックします。

8 前の 4 つの手順を繰り返して、条件付きロールを追加します (必要な場合)。前の 4 つの手順をもう一度繰り返して、オプションロールを追加します (必要な場合)。

9 「保存」をクリックして、「ロール変更の確認」ページを開きます。

「ロール変更の確認」ページが開きます。

10 「割り当てられたユーザーの更新」セクションで、「割り当てられたユーザーの更新」メニューオプションを選択し、「保存」をクリックしてロールの割り当てを保存します。

詳細は、147 ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

▼ 別のロールに割り当てられたロールを削除する

Identity Manager は、親ロールのロール所有者が承認すれば、別のロールから含まれるロールを削除します。削除されたロールは、ユーザーがロールの更新を受け取ったときに、ユーザーから削除されます。(詳細は、147 ページの「ユーザーに割り当てられたロールを更新する」を参照)ロールを削除すると、ユーザーはロールによって与えられたエンタイトルメントを失います。

- 1 人以上のユーザーに割り当てられたロールの削除については、153 ページの「1 つ以上のロールをユーザーから削除する」を参照してください。
- ロールの無効化については、141 ページの「ロールを有効または無効にする」を参照してください。
- Identity Manager からのロールの削除については、142 ページの「ロールを削除する」を参照してください。

1 ロールを削除するビジネスロールまたは IT ロールを検索します。ロールを検索するには、**136 ページの「ロールを検索する」**または**137 ページの「ロールを表示する」**の手順を使用します。

2 ロールをクリックして開きます。
「ロールの編集」ページが開きます。

3 「ロールの編集」ページの「ロール」タブをクリックします。

4 「含まれるロール」セクションで、削除するロールの横のチェックボックスを選択して、「削除」をクリックします。複数のロールを削除する場合は、複数のチェックボックスを選択します。
テーブルが更新され、残りの「含まれるロール」が表示されます。

5 「保存」をクリックします。
「ロール変更の確認」ページが開きます。

6 「割り当てられたユーザーの更新」セクションで、「割り当てられたユーザーの更新」メニューオプションを選択します。詳細は、**147** ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

7 「保存」をクリックして、変更を確定します。

▼ ロールを有効または無効にする

「ロールのリスト」タブで、ロールを有効および無効にできます。ロールの状態が「状態」列に表示されます。「状態」列ヘッダーをクリックして、ロールの状態でテーブルを並べ替えます。

無効にされたロールは、「作成/編集」ユーザーフォームの「ロール」タブには表示されず、ユーザーに直接割り当てることはできません。無効化されたロールを含むロールをユーザーに割り当てることはできますが、無効化されたロールを割り当てることはできません。

あとで無効化されるロールが割り当てられているユーザーは、そのエンタイトルメントを失いません。ロールの無効化により妨げられるのは、将来のロール割り当てだけです。

ロールを無効にしてから再度有効にするには、ロール所有者の権限が必要です。

割り当てられたユーザーでロールを有効または無効にすると、Identity Manager によりこれらのユーザーを更新するように求められます。詳細は、147 ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

1 **136** ページの「ロールを検索する」または**137** ページの「ロールを表示する」の手順に従って、削除するロールを検索します。

2 有効または無効にするロールの横にあるチェックボックスをクリックします。

3 「ロール」テーブルの下部にある「有効化」または「無効化」をクリックします。
「ロールの有効化」または「ロールの無効化」確認ページが開きます。

4 「**OK**」をクリックして、ロールを有効化または無効化します。

▼ ロールを削除する

この節では、Identity Manager からロールを削除する手順について説明します。

- 別のロールに割り当てられたロールの削除については、140 ページの「別のロールに割り当てられたロールを削除する」を参照してください。
- 1 人以上のユーザーに割り当てられたロールの削除については、153 ページの「1 つ以上のロールをユーザーから削除する」を参照してください。

現在ユーザーに割り当てられているロールを削除する場合、ロールを保存しようとすると Identity Manager により削除が妨げられます。削除を完了するには、ロールに割り当てられているすべてのユーザーを事前に割り当て解除 (または再割り当て) しておく必要があります。また、ロールをほかのロールから削除する必要もあります。

Identity Manager で、ロールを削除する前に、ロール所有者の承認が必要です。

1 **136 ページの「ロールを検索する」**または**137 ページの「ロールを表示する」**の手順に従って、削除するロールを検索します。

2 削除する各ロールの横にあるチェックボックスを選択します。

3 「削除」をクリックします。
「ロールの削除」確認ページが表示されます。

4 「**OK**」をクリックして、**1** つ以上のロールを削除します。

▼ リソースまたはリソースグループをロールに割り当てる

リソースおよびリソースグループの割り当てに関する Identity Manager の要件については、119 ページの「ロールとは」および121 ページの「ロールタイプの使用」で説明します。リソースをロールに割り当てる前に、この情報を理解しておいてください。

Identity Manager は、ロール所有者が承認すれば、ロールのリソースおよびリソースグループの割り当てを変更します。

1 リソースまたはリソースグループを追加する **IT** ロールまたはアプリケーションを検索します。ロールの検索方法については、**136 ページの「ロールを検索する」**または**137 ページの「ロールを表示する」**を参照してください。

2 ロールをクリックして開きます。

3 「ロールの編集」ページの「リソース」タブをクリックします。

4 リソースを割り当てるには、「利用可能なリソース」列でリソースを選択し、矢印ボタンをクリックしてそのリソースを「現在のリソース」列に移します。

5 複数のリソースを割り当てる場合は、リソースを更新する順番を指定することができます。「順番にリソースを更新する」チェックボックスを選択し、「+」ボタンと「-」ボタンを使用して「現在のリソース」列のリソースの順番を変更します。

6 このロールにリソースグループを割り当てるには、「利用可能なリソースグループ」列でリソースグループを選択し、矢印ボタンをクリックしてそのリソースグループを「現在のリソースグループ」列に移動します。リソースグループはリソースの集まりであり、リソースアカウントを作成および更新する順番を指定するための別の方法を提供します。

7 このロールのアカウント属性をリソース単位で指定するには、「割り当てられたリソース」セクションの「属性値の設定」をクリックします。詳細は、**167** ページの「リソースアカウント属性を表示または編集する」を参照してください。

8 「保存」をクリックして、「ロール変更の確認」ページを開きます。
「ロール変更の確認」ページが開きます。

9 「割り当てられたユーザーの更新」セクションで、「割り当てられたユーザーの更新」メニューオプションを選択します。詳細は、**147** ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

10 「保存」をクリックして、リソースの割り当てを保存します。

▼ ロールに割り当てられているリソースまたはリソースグループを削除する

Identity Manager は、ロール所有者が承認すれば、リソースまたはリソースグループをロールから削除します。ユーザーがロールの更新を受信する際に、削除されたリソースがユーザーから削除されます。(詳細は、147 ページの「ユーザーに割り当てられたロールを更新する」を参照)リソースの削除時に、ユーザーにリソースが直接割り当てられているのでない限り、ユーザーはリソースに対するエンタイトルメントを失います。

1 リソースまたはリソースグループを削除する **IT** ロールまたはアプリケーションを検索します。ロールを検索するには、**136** ページの「ロールを検索する」または**137** ページの「ロールを表示する」の手順を使用します。

2 ロールをクリックして開きます。
「ロールの編集」ページが開きます。

3 「ロールの編集」ページの「リソース」タブをクリックします。

4 リソースを削除するには、「現在のリソース」列でリソースを選択し、矢印ボタンをクリックして「利用可能なリソース」列に移動します。
リソースグループを削除するには、「現在のリソースグループ」列でリソースを選択し、矢印ボタンをクリックして「利用可能なリソースグループ」列に移動します。

5 「保存」をクリックします。
「ロール変更の確認」ページが開きます。

6 「割り当てられたユーザーの更新」セクションで、「割り当てられたユーザーの更新」メニューオプションを選択します。詳細は、**147** ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

7 「保存」をクリックして、変更を確定します。

ユーザーロール割り当ての管理

ロールをユーザーに割り当てるには、Identity Manager の「アカウント」領域を使用します。

▼ ロールをユーザーに割り当てる

次の手順を実行して、1 つ以上のロールをユーザーに割り当てます。

エンドユーザーは、ロール割り当てリクエストを自分で作成することもできます。リクエストできるのは、親ロールがユーザーに割り当て済みのオプションロールのみです。エンドユーザーが利用可能なロールを要求できる方法については、39 ページの「「リクエスト」タブ」の節の38 ページの「Identity Manager エンドユーザーインタフェース」を参照してください。

1 管理者インタフェースで、「アカウント」タブをクリックします。
「アカウントのリスト」サブタブが開きます。

2 ロールを既存のユーザーに割り当てるには、次の手順に従います。

a. 「ユーザーリスト」でユーザーの名前をクリックします。

b. 「ロール」タブをクリックします。

c. 「追加」をクリックして、1 つ以上のロールをユーザーアカウントに追加します。

デフォルトでは、ユーザーに直接割り当てることができるのはビジネスロールだけです。(使用している Identity Manager が 8.0 より前のバージョンからアップグレードされたものである場合は、ビジネスロールと IT ロールをユーザーに直接割り当てることができます。)

d. ロールのテーブルで、ユーザーに割り当てるロールを選択して、「OK」をクリックします。

テーブルを、「名前」、「タイプ」、または「説明」でアルファベット順に並べ替えるには、列ヘッダーをクリックします。もう一度クリックすると、逆の順で並べ替えられます。リストをロールタイプでフィルタするには、「現在」ドロップダウンメニューから選択します。

テーブルが更新され、選択したロール割り当て、および親ロール割り当てに関連付けられたすべての必須ロール割り当てが表示されます。

e. 「追加」をクリックして、オプションロール割り当てを表示します。 これも、ユーザーに割り当てることができます。

ユーザーに割り当てるオプションロールを選択して、「OK」をクリックします。

f. (オプション)「アクティブになる日」列で、ロールをアクティブにする日付を選択します。日付を指定しない場合、指定したロール承認者がロール割り当てを承認するとすぐに、ロール割り当てがアクティブになります。

一時的にロールを割り当てる場合は、「非アクティブになる日」列でロールを非アクティブにする日付を選択します。選択した日付に変わると、ロールが非アクティブになります。

詳細は「145 ページの「特定の日付にロールをアクティブ化および非アクティブ化する」を参照してください。

g. 「保存」をクリックします。

特定の日付にロールをアクティブ化および非アクティブ化する

ロールをユーザーに割り当てる際に、「アクティブになる日」と「非アクティブになる日」を指定できます。ロール割り当て作業項目のリクエストは、割り当ての作成時に作成されます。ただし、設定されたアクティブ化の日付までにロール割り当てが承認されない場合、ロールは割り当てられません。ロールのアクティブ化および非アクティブ化は、指定された日付の午前零時を少し過ぎた時刻 (12:01 AM) に実行されます。

デフォルトでは、アクティブ化および非アクティブ化の日付を指定できるのはビジネスロールだけです。その他のロールタイプはすべて、ユーザーに直接割り当てら

れたビジネスロールのアクティブ化および非アクティブ化の日付を継承します。Identity Manager を設定することで、ほかのロールタイプに異なるアクティブ化および非アクティブ化の日付を直接割り当てることができます。手順については、「154 ページの「ロールタイプの設定」」を参照してください。

▼ 延期タスクスキャナのスケジュールを編集する

延期タスクスキャナは、ユーザーロール割り当てをスキャンし、必要に応じてロールをアクティブおよび非アクティブにします。デフォルトでは、延期タスクスキャナタスクは 1 時間ごとに実行されます。

1. 管理者インタフェースで、「サーバータスク」をクリックします。
2. 二次的なメニューの「スケジュールの管理」をクリックします。
3. 「スケジューリング可能なタスク」セクションで、「延期タスクスキャナ」タスク定義をクリックします。

   「Deferred Task Scanner タスクのスケジュールの新規作成」ページが開きます。
4. フォームに必要な情報を指定します。ヘルプについては、**i-Help** およびオンラインヘルプを参照してください。

   タスクが実行されるべき日時を指定するには、「開始日」で `mm/dd/yyyy hh:mm:ss` という形式を使用します。たとえば、2008 年 9 月 29 日の午後 7 時にタスクの実行が開始されるようにスケジュールするには、`09/29/2008 19:00:00` と入力します。

   「結果オプション」ドロップダウンメニューで、「名前の変更」を選択します。「待機」を選択した場合、このタスクの将来のインスタンスは、以前の結果を削除するまで実行されません。さまざまな「結果オプション」設定の詳細については、オンラインヘルプを参照してください。
5. 「保存」をクリックしてタスクを保存します。

   図 5–9に、「延期タスクスキャナ」タスクのスケジュールタスクフォームを示します。

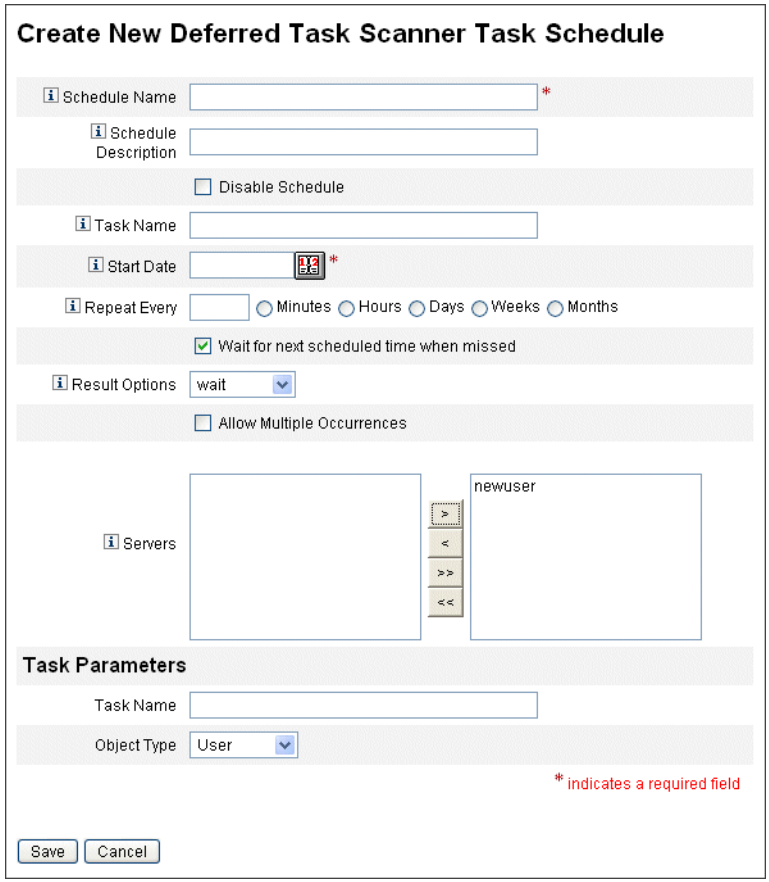


図 5–9 「延期タスクスキャナ」スケジュールタスクフォーム

ユーザーに割り当てられたロールを更新する

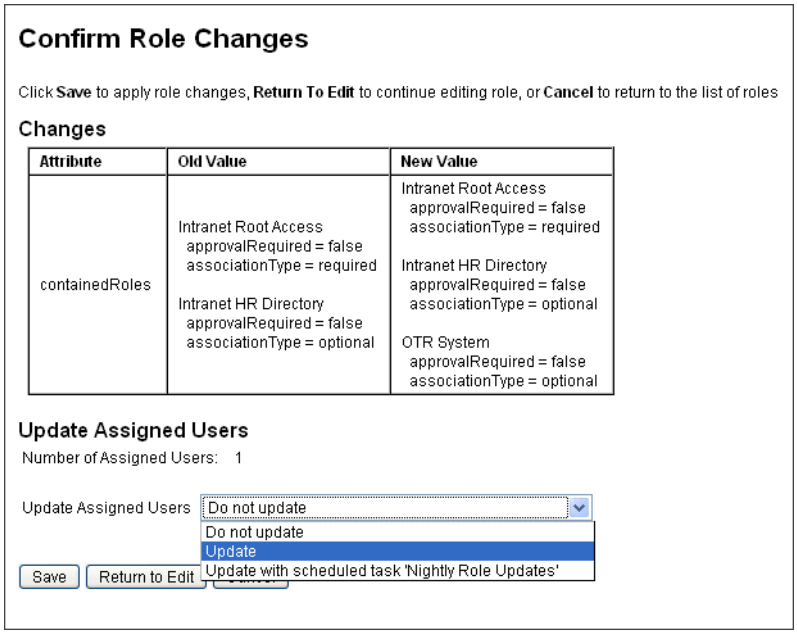
ユーザーに割り当てられたロールの編集時に、新しいロール変更に従ってユーザーをただちに更新することも、スケジュールした保守時間を使ってあとで更新することもできます。

ロールを変更すると、「ロール変更の確認」ページが開きます。「ロール変更の確認」ページは、147 ページの「ユーザーに割り当てられたロールを更新する」に示されています。

- このページの「割り当てられたユーザーの更新」セクションには、ロールが現在割り当てられているユーザーの数が示されます。
- 「割り当てられたユーザーの更新」メニューを使用して、ユーザーを新しいロール変更でただちに更新するか (「更新」)、ユーザーの更新を延期するか (「更新しない」)、スケジュールしたカスタム更新タスクを選択します。

- 「更新」はユーザーを即座に更新するため、多数のユーザーが影響を受ける場合は、このオプションを選択しないようにしてください。ユーザーの更新は、多くの時間とリソースを必要とする可能性があります。多数のユーザーを更新する必要がある場合は、オフピークの時間帯の更新をスケジュールすることをお勧めします。
- ロールに「更新しない」を選択すると、管理者がユーザーのユーザープロファイルを表示するまで、またはユーザーが「ロールのユーザーの更新」タスクによって更新されるまで、ロールに割り当てられたユーザーはロールの更新を受け取りません。「ロールユーザーの更新」タスクのスケジュールについては、次の節を参照してください。
- 「ロールユーザーの更新」タスクスケジュールが作成されている場合は、メニューから選択することができます。選択した「ロールのユーザーの更新」タスクは、タスクに定義されたスケジュールに従って、ロールに割り当てられたユーザーを更新します。詳細は、次の節を参照してください。

  147 ページの「ユーザーに割り当てられたロールを更新する」に、「ロール変更の確認」ページを示します。「割り当てられたユーザーの更新」セクションには、このロールが現在割り当てられているユーザーの数が示されます。「割り当てられたユーザーの更新」ドロップダウンメニューには、「更新しない」と「更新」の 2 つのデフォルトオプションがあります。スケジュールした「ロールユーザーの更新」タスクのリストから選択することもできます。スケジュールした「ロールユーザーの更新」タスクの作成手順については、150 ページの「ロールユーザーの更新タスクをスケジュールする」を参照してください。



▼ 割り当てられたユーザーを手動で更新する

1 つ以上のロールを選択して「割り当てられたユーザーの更新」ボタンをクリックすることで、ロールが割り当てられているユーザーを更新できます。この手順により、指定したロールの「ロールユーザーの更新」タスクのインスタンスが実行されます。

1 136 ページの「ロールを検索する」または137 ページの「ロールを表示する」の手順に従って、割り当てられたユーザーを更新するロールを検索します。

2 チェックボックスを使ってロールを選択します。

3 「割り当てられたユーザーの更新」をクリックします。
「ロールが割り当てられているユーザーの更新」ページ (図 5–10) が表示されます。

4 「起動」をクリックして更新を開始します。

5 メインメニューの「サーバータスク」をクリックしてから、二次的なメニューの「すべてのタスク」をクリックして、「ロールユーザーの更新」タスクの状態を確認します。

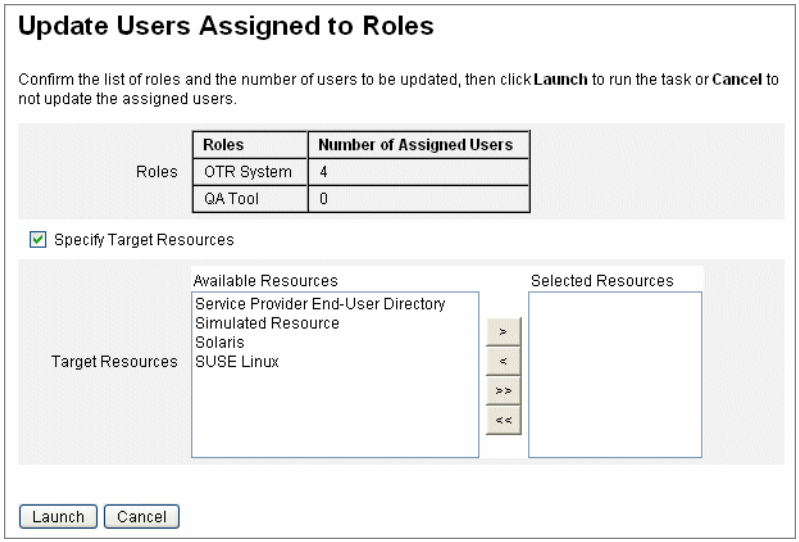


図 5–10 「ロールが割り当てられているユーザーの更新」ページ

▼ ロールユーザーの更新タスクをスケジュールする

注 – ロールユーザーの更新タスクが定期的に実行されるようにスケジュールしてください。

次のようにロールユーザーの更新タスクをスケジュールして、未処理のロール変更があるユーザーを更新します。

1 管理者インタフェースで、「サーバータスク」をクリックします。

2 二次的なメニューの「スケジュールの管理」をクリックします。

3 「スケジューリング可能なタスク」セクションで、「ロールユーザーの更新」タスク定義をクリックします。

「Update Role Users タスクのスケジュールの新規作成」ページが開きます。既存のタスクを編集している場合は、「タスクスケジュールの編集」ページが開きます (図 5–11)。

4 フォームに必要な情報を指定します。ヘルプについては、**i-Help** およびオンラインヘルプを参照してください。

タスクが実行されるべき日時を指定するには、「開始日」で `mm/dd/yyyy hh:mm:ss` という形式を使用します。たとえば、2008 年 9 月 29 日の午後 7 時にタスクの実行が開始されるようにスケジュールするには、`09/29/2008 19:00:00` と入力します。

「結果オプション」ドロップダウンメニューで、「名前の変更」を選択します。「待機」を選択した場合、このタスクの将来のインスタンスは、以前の結果を削除するまで実行されません。さまざまな「結果オプション」設定の詳細については、オンラインヘルプを参照してください。

5 「保存」をクリックしてタスクを保存します。

図 5–11に、「ロールユーザーの更新」タスクのスケジュールタスクフォームを示します。特定の「ロールユーザーの更新」タスクに特定のロールを割り当てることができます(「タスクパラメータ」セクションを参照。詳細は、147 ページの「ユーザーに割り当てられたロールを更新する」を参照してください。

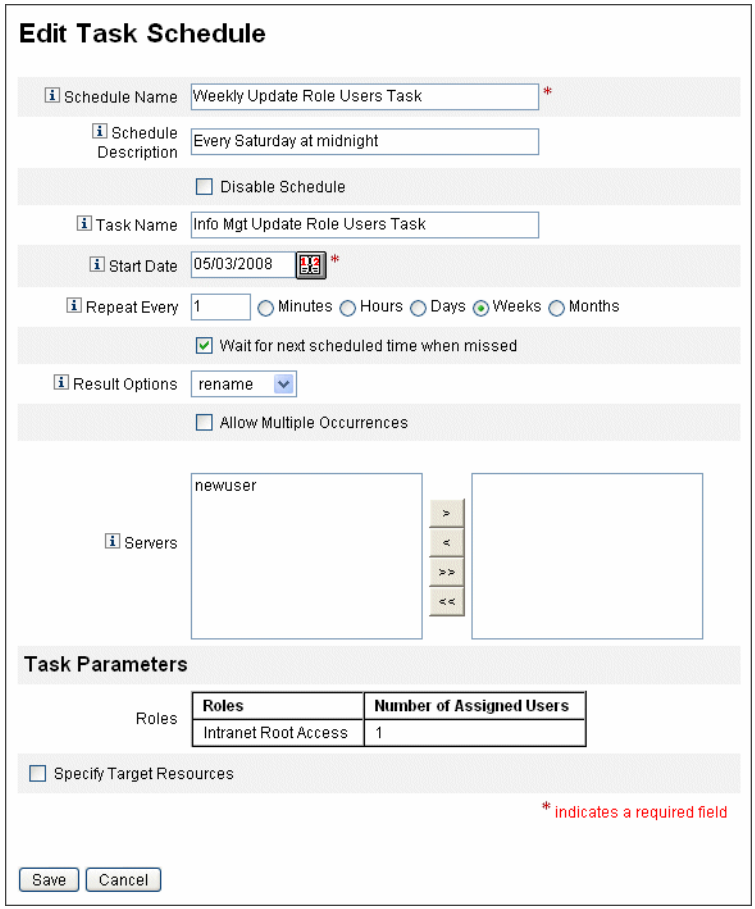


図 5–11 「ロールユーザーの更新」スケジュールタスクフォーム

▼ 特定のロールに割り当てられたユーザーを検索する

特定のロールが割り当てられたユーザーを検索できます。

1 管理者インタフェースで、「アカウント」をクリックします。

2 二次的なメニューの「ユーザーの検索」をクリックします。「ユーザーの検索」ページが開きます。

3 検索タイプ「[ロールタイプを選択]ロールが割り当てられているユーザー」を見つけます。

4 オプションボックスを選択し、「ロールタイプの選択」ドロップダウンメニューを使用して利用可能なロールのリストをフィルタします。

二次的なロールメニューが開きます。

5 ロールを選択します。

6 検索をさらに絞り込む必要がなければ、その他の検索タイプチェックボックスを選択解除します。

7 「検索」をクリックします。

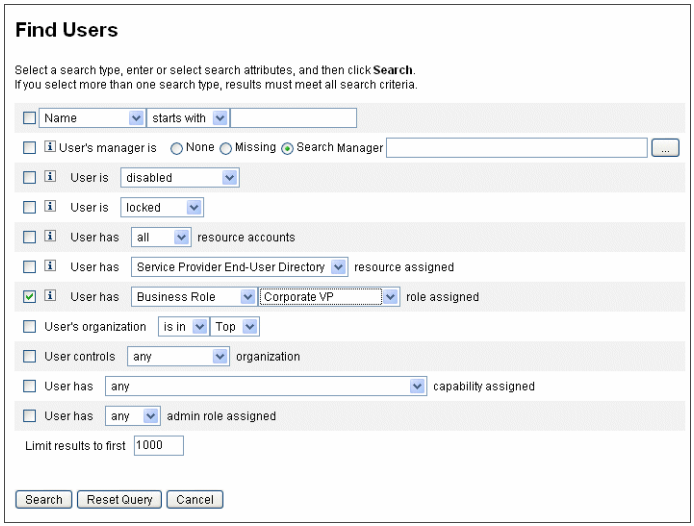


図 5–12 「ユーザーの検索」ページを使用した、ロールに割り当てられたユーザーの検索

▼ 1つ以上のロールをユーザーから削除する

「ユーザーの編集」ページを使って、1つ以上のロールをユーザーアカウントから削除できます。削除できるのは、直接割り当てられたロールだけです。間接的に割り当てられたロール(つまり、条件付きまたは必須、あるいはその両方の含まれるロール)は、親ロールの削除時に削除されます。間接的に割り当てられたロールをユーザーから削除する別の方法は、ロールを親ロールから削除することです(140ページの「別のロールに割り当てられたロールを削除する」を参照)。

エンドユーザーは、割り当てられたロールのユーザーアカウントからの削除もリクエストできます。39ページの「「リクエスト」タブ」の節の38ページの「Identity Managerエンドユーザーインタフェース」を参照してください。

スケジュールされた非アクティブ化の日付を使用したロールの削除については、145ページの「特定の日付にロールをアクティブ化および非アクティブ化する」を参照してください。

1. 管理者インタフェースで、「アカウント」タブをクリックします。
   「アカウントのリスト」サブタブが開きます。
2. 規則を削除するユーザーをクリックします。
   「ユーザーの編集」ページが開きます。
3. 「ロール」タブをクリックします。
4. ロールのテーブルで、ユーザーから削除するロールを選択して、「**OK**」をクリックします。
   テーブルを「名前」、「タイプ」、「アクティブになる日」、「非アクティブになる日」、「親ロール」、または「状態」でアルファベット順に並べ替えるには、列ヘッダーをクリックします。もう一度クリックすると、逆の順で並べ替えられます。リストをロールタイプでフィルタするには、「現在」ドロップダウンメニューから選択します。

   テーブルに、親ロールの割り当て(選択可能なロール)、および親ロールの割り当てに関連付けられたすべてのロール割り当て(選択不可のロール)が表示されます。
5. 「削除」をクリックします。
   割り当てられたロールのテーブルが更新され、割り当てられた残りのロールが表示されます。
6. 「保存」をクリックします。
   「リソースアカウントの更新」ページが開きます。削除しないリソースアカウントをすべて選択解除します。
7. 変更を保存するには、「保存」をクリックします。

ロールタイプの設定

ロールタイプ機能は、Role 設定オブジェクトを編集することで変更できます。

▼ ロールタイプを設定してユーザーに直接割り当て可能にする

デフォルトでは、ユーザーに直接割り当てることができるのは特定のロールタイプだけです。これらの設定を変更するには、次の手順に従います。

注 – もっとも推奨されるのは、ビジネスロールだけをユーザーに直接割り当てることです。詳細は、121 ページの「ロールタイプを使用した柔軟なロールの設計」を参照してください。

ユーザーに直接割り当て可能なロールタイプを変更するには、次の手順に従います。

1. 116 ページの「Identity Manager 設定オブジェクトの編集」の手順に従って、編集するロール設定オブジェクトを開きます。
2. 編集するロールタイプに対応するロールオブジェクトを探します。
   - IT ロールを編集する場合は、`Object name='ITRole'` を見つけます。
   - アプリケーションロールを編集する場合は、`Object name='ApplicationRole'` を見つけます。
   - アセットロールを編集する場合は、`Object name='AssetRole'` を見つけます。
3. 一連の手順を指定して、設定を更新します。

   設定を更新する方法に応じて、次のいずれかを選択します。
   - ロールタイプを変更してユーザーに直接割り当て可能にするには、ロールオブジェクト内で次の `userAssignment` 属性を見つけます。

```
<Attribute name='userAssignment'>
        <Object/>
    </Attribute>
```

これを次の属性で置き換えます。

```
<Attribute name='userAssignment'>
        <Object>
            <Attribute name='manual' value='true'/>
         </Object>
    </Attribute>
```

- ロールタイプを変更してユーザーへの直接割り当てを不可にするには、ロールオブジェクト内で userAssignment 属性を見つけて、次に示すように manual 属性を削除します。

```
<Attribute name='userAssignment'>
        <Object>
        </Object>
    </Attribute>
```

4 Role 設定オブジェクトを保存します。変更を有効にするために、アプリケーションサーバーを再起動する必要はありません。

▼ 割り当て可能なアクティブ化の日付および非アクティブ化の日付のロールタイプを有効にする

デフォルトでは、アクティブ化の日付および非アクティブ化の日付を設定できるのはビジネスロールだけです。これらの日付は、ロールの割り当て時に指定できます。その他のロールはすべて、ユーザーに直接割り当てられたビジネスロールのアクティブ化または非アクティブ化の日付を継承します。

注– もっとも推奨されるのは、ビジネスロールだけをユーザーに直接割り当てることです。詳細は、121 ページの「ロールタイプを使用した柔軟なロールの設計」を参照してください。

別のロールタイプ (IT ロールタイプなど) をユーザーに直接割り当て可能にする場合は、そのロールタイプをアクティブにする日付や非アクティブにする日付も割り当て可能にできます。

どのロールタイプでアクティブ化および非アクティブ化の日付を割り当て可能にできるかを変更するには、次の手順に従います。

1 116 ページの「Identity Manager 設定オブジェクトの編集」の手順に従って、編集するロール設定オブジェクトを開きます。

2 編集するロールタイプに対応するロールオブジェクトを探します。

- ビジネスロールを編集する場合は、Object name='BusinessRole' を見つけます。
- IT ロールを編集する場合は、Object name='ITRole' を見つけます。
- アプリケーションロールを編集する場合は、Object name='ApplicationRole' を見つけます。
- アセットロールを編集する場合は、Object name='AssetRole' を見つけます。

3 一連の手順を指定して、設定を更新します。

設定を更新する方法に応じて、次のいずれかを選択します。

- ロールタイプを変更して、直接割り当て可能なアクティブ化および非アクティブ化の日付を設定可能にするには、ロールオブジェクト内で次の userAssignment 属性を見つけます。

```
<Attribute name='userAssignment'>
        <Attribute name='manual' value='true'/>
     </Attribute>
```

これを次の属性で置き換えます。

```
<Attribute name='userAssignment'>
        <Object>
            <Attribute name='activateDate' value='true'/>
             <Attribute name='deactivateDate' value='true'/>
             <Attribute name='manual' value='true'/>
        </Object>
    </Attribute>
```

- ロールタイプを変更して、直接割り当て可能なアクティブ化および非アクティブ化の日付を設定できなくするには、ロールオブジェクト内で userAssignment 属性を見つけて、次に示すように activateDate および deactivateDate 属性を削除します。

```
<Attribute name='userAssignment'>
        <Object>
        </Object>
    </Attribute>
```

4 **Role** 設定オブジェクトを保存します。変更を有効にするために、アプリケーションサーバーを再起動する必要はありません。

▼ 変更承認作業項目および変更通知作業項目を有効または無効にする

デフォルトでは、変更承認作業項目はすべてのロールタイプで有効です。このため、ロールに所有者がいる場合、ロールが変更されるたびに (ビジネスロール、IT ロール、アプリケーション、またはアセットのいずれであっても)、変更を実行するために所有者が変更を承認する必要があります。

変更承認作業項目および変更通知作業項目については、135 ページの「変更承認作業項目と承認作業項目の開始」を参照してください。

ロールタイプの変更承認作業項目および変更通知作業項目を有効または無効にするには、次の手順に従います。

1. 116 ページの「Identity Manager 設定オブジェクトの編集」の手順に従って、編集するロール設定オブジェクトを開きます。
2. 編集するロールタイプに対応するロールオブジェクトを探します。
   - ビジネスロールを編集する場合は、Object name='BusinessRole' を見つけます。
   - IT ロールを編集する場合は、Object name='ITRole' を見つけます。
   - アプリケーションロールを編集する場合は、Object name='ApplicationRole' を見つけます。
   - アセットロールを編集する場合は、Object name='AssetRole' を見つけます。
3. <Attribute name='features'> 要素内の <Object> 要素で、次の属性を検索します。

   ```
   <Attribute name='changeApproval' value='true'/>
    <Attribute name='changeNotification' value='true'/>
   ```
4. 必要に応じて、属性値を **true** または **false** に設定します。
5. 必要に応じ、手順 **2** ～ **4** を繰り返して別のロールタイプを設定します。
6. **Role** 設定オブジェクトを保存します。変更を有効にするために、アプリケーションサーバーを再起動する必要はありません。

▼ ロールリストページで読み込み可能な最大行数を設定する

管理者インタフェースの「ロールのリスト」ページには、設定可能な最大行数を表示できます。デフォルト値は 500 です。この節の手順に従って、この数を変更します。

次の手順に従って、「ロールのリスト」ページで表示可能な最大行数を変更します。

1. 116 ページの「Identity Manager 設定オブジェクトの編集」の手順に従って、編集するロール設定オブジェクトを開きます。
2. 次の属性を検索して、値を変更します。

   ```
   <Attribute name='roleListMaxRows' value='500'/>
   ```
3. **Role** 設定オブジェクトを保存します。変更を有効にするために、アプリケーションサーバーを再起動する必要はありません。

Identity Manager 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。同期させると、リソースはデフォルトでロールに割り当てられます。これには、同期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。

▼ Identity Manager ロールをリソースロールと同期する

1. 管理者インタフェースで、メインメニューから「サーバータスク」をクリックします。
2. 「タスクの実行」をクリックします。「利用可能なタスク」ページが開きます。
3. 「アイデンティティーシステムのロールとリソースのロールの同期」タスクをクリックします。
4. フォームに必要な情報を指定します。詳細については、「ヘルプ」をクリックしてください。
5. 「起動」をクリックします。

Identity Manager リソースとその管理について

この節では、Identity Manager リソースの設定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関する情報を格納します。Identity Manager リソースは、リソースについての関連属性を定義し、Identity Manager でのリソース情報の表示方法を指定するために役立ちます。

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」領域

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。

リソースリスト内のリソースは、タイプごとにグループ化されています。各リソースタイプは、フォルダアイコンで表されます。現在定義されているリソースを表示するには、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、インジケータ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を編集、作成、削除、名前変更、別名保存、および検索します。
- 「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

新しいリソースを作成する前に、管理可能にするリソースタイプを Identity Manager に指定する必要があります。リソースを有効にして、カスタムリソースを作成する場合は、「管理するリソースの設定」ページを使用します。

▼ 「管理するリソースの設定」ページを開く

「管理するリソースの設定」ページを開くには、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 「リソース」タブをクリックします。

「管理するリソースの設定」ページを開くには、次のいずれかの方法を使用します。

- 「リソースタイプアクション」ドロップダウンリストを見つけて、「管理するリソースの設定」を選択します。
- 「タイプの設定」タブをクリックします。

「管理するリソースの設定」ページが開きます。

このページには、次の 3 つのセクションがあります。

- 「リソースコネクタ」。このセクションには、リソースコネクタのタイプ、コネクタのバージョン、およびコネクタサーバーが一覧表示されます。
- 「リソースアダプタ」。このセクションには、大企業の環境によく見られるリソースタイプが一覧表示されます。リソースに接続する Identity Manager アダプタのバージョンが、「バージョン」列に示されます。
- 「カスタムリソースアダプタ」。このセクションを使用して、カスタムリソースを「リソース」リストに追加します。

▼ リソースタイプを有効にする

以下の手順に従って、「管理するリソースの設定」ページからリソースタイプを有効にすることができます。

1 「管理するリソースの設定」ページがまだ開いていない場合は、開きます (159 ページの「リソースリストの管理」)。

2 「リソース」セクションで、有効にするリソースタイプの「管理しますか?」列のボックスを選択します。

リスト表示されているすべてのリソースタイプを有効にするには、「すべてのリソースを管理しますか?」を選択します。

3 ページの下部にある「保存」をクリックします。

リソースが「リソース」リストに追加されます。

▼ カスタムリソースを追加する

以下の手順に従って、「管理するリソースの設定」ページからカスタムリソースを追加できます。

1. 「管理するリソースの設定」ページがまだ開いていない場合は、開きます(159 ページの「リソースリストの管理」)。
2. 「カスタムリソース」セクションの「カスタムリソースの追加」をクリックして、テーブルに行を追加します。
3. リソースのリソースクラスパスを入力するか、カスタマイズしたリソースを入力します。**Identity Manager** で提供されるアダプタでの完全なクラスパスについては、『**Sun Identity Manager 8.1 Resources Reference**』を参照してください。
4. 「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。

▼ リソースを作成する

リソースタイプが有効になると、そのリソースのインスタンスを Identity Manager 内で作成できるようになります。リソースを作成するには、「リソースウィザード」を使用します。

リソースウィザードを使用すると、次の項目を手順に従って設定できます。

- 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で定義します。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 DN またはアイデンティティーテンプレート。階層的な名前空間で特に重要な、ユーザーに対するアカウント名の構文が含まれます。
- リソースの Identity Manager パラメータ。ポリシーの設定、リソース承認者の設定、およびリソースへの組織アクセスの設定を行います。

1. 管理者インタフェースにログインします。
2. 「リソース」タブをクリックします。「リソースのリスト」サブタブが選択されていることを確認します。
3. 「リソースタイプアクション」ドロップダウンリストを見つけて、「新規リソース」を選択します。
   「新規リソース」ページが開きます。
4. ドロップダウンリストからリソースの種類を選択します。(該当するリソースタイプがリストに表示されない場合は、それを有効にする必要があります。159 ページの「リソースリストの管理」を参照してください)

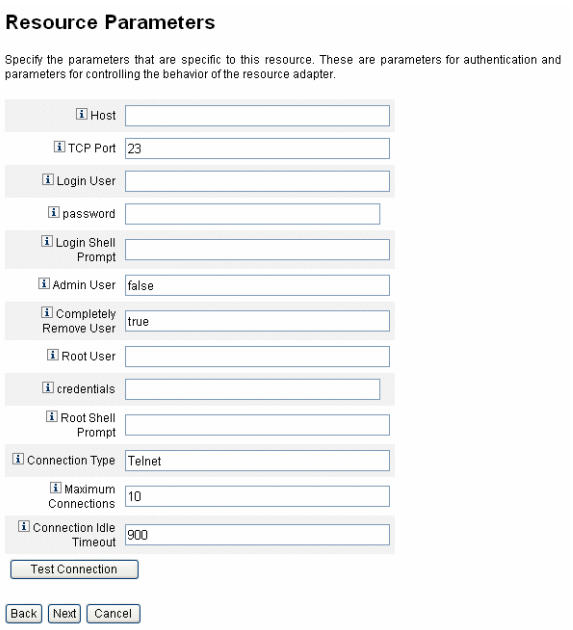
5 「新規」をクリックして、リソースウィザードの「ようこそ」ページを表示します。

6 「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。

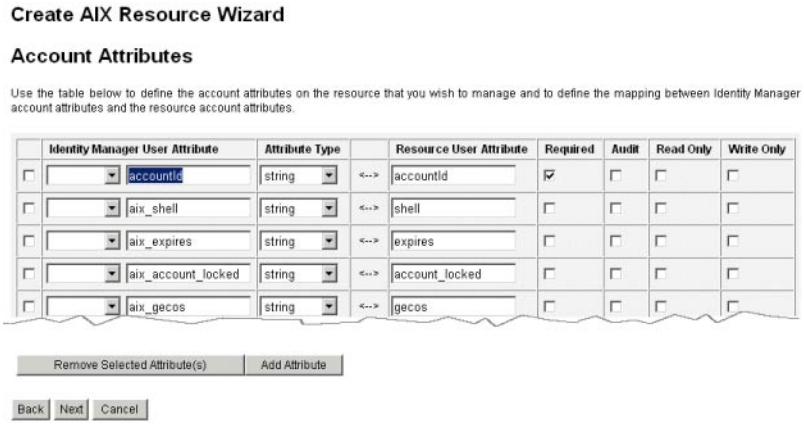
- リソースパラメータ。認証とリソースアダプタの動作を管理するためのリソース固有のパラメータを設定します。パラメータを入力して「テスト接続」をクリックし、接続が有効であることを確認します。確認できたら、「次へ」をクリックして、アカウント属性を設定します。

  次の図に、Solaris リソースの「リソースパラメータ」ページを示します。このページのフォームフィールドは、リソースにより異なります。



- 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。リソースアカウント属性については、167 ページの「リソースアカウント属性を表示または編集する」を参照してください。
  - 属性を追加する場合は、「属性の追加」をクリックします。
  - 1 つ以上の属性を削除するには、属性の横のボックスを選択して「選択している属性の削除」をクリックします。

    次の図に、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。



注 – EXT_RESOURCEACCOUNT_ACCTATTR テーブルに属性をエクスポートする場合は、エクスポートする属性ごとに「監査」ボックスをチェックする必要があります。

操作が終了したら、「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設定します。

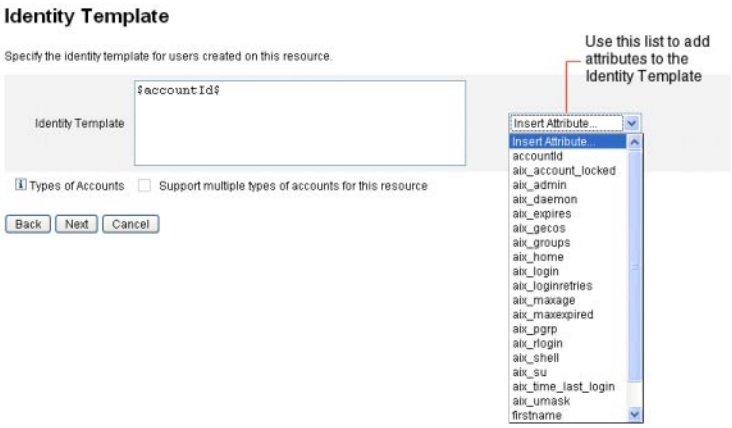
- アイデンティティーテンプレート。ユーザーに対するアカウント名の構文を定義します。この機能は、階層的な名前空間で特に重要です。
  - 属性をテンプレートに追加するには、「属性の挿入」リストから属性を選択します。
  - 属性を削除するには、文字列内でその属性を強調表示して、キーボードの Del キーを押します。属性名と前後の $ (ドル記号) の両方を削除してください。
  - アカウントタイプ。Identity Manager では、1 人のユーザーに複数のリソースアカウントを割り当てることができます。たとえば、ユーザーは、特定のリソースの通常のユーザーアカウントのほか、管理者レベルのアカウントが必要になる場合があります。このリソースで複数のアカウントタイプをサポートするには、「アカウントタイプ」チェックボックスを選択します。

注 – サブタイプ IdentityRule で識別されるアイデンティティー生成規則を 1 つ以上作成していない場合、「アカウントタイプ」チェックボックスは選択できません。accountIds は区別できるものである必要があるため、さまざまなタイプのアカウントが特定のユーザーのさまざまな accountIds を生成する必要があります。アイデンティティー生成規則は、これら一意の accountIds の作成方法を指定します。

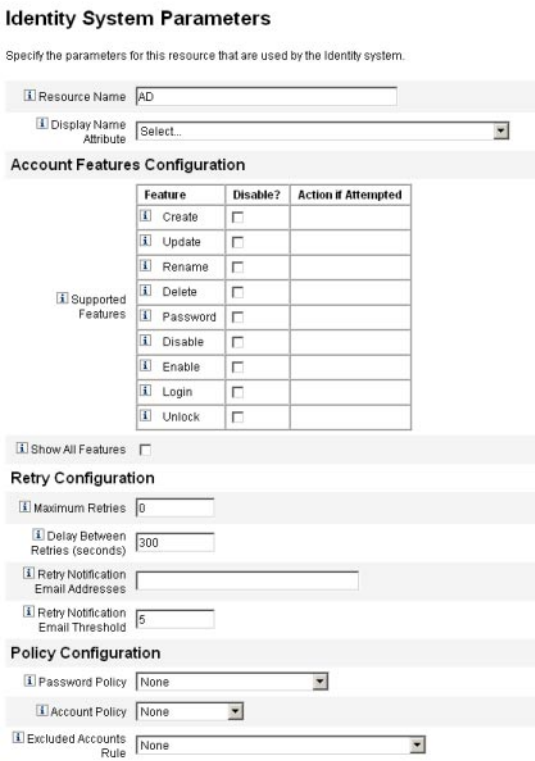
サンプルのアイデンティティー規則は、`sample/identityRules.xml` にあります。

アカウントタイプは、Identity Manager 内のほかのオブジェクトから参照されなくなるまで削除できません。また、アカウントタイプの名前を変更することはできません。

「アカウントタイプ」フォームへの必要な情報の指定については、Identity Manager のオンラインヘルプを参照してください。ユーザーに対する複数のリソースアカウントの作成については、59 ページの「1 人のユーザーに対する複数のリソースアカウントの作成」を参照してください。



- アイデンティティーシステムのパラメータ。161 ページの「リソースを作成する」に示したとおり、再試行やポリシーの設定などの、リソースの Identity Manager パラメータを設定します。



7 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

この節では、既存のリソースの管理方法について説明します。

トピックは次のように構成されます。

- 165 ページの「リソースリストを表示する」
- 166 ページの「リソースウィザードを使用してリソースを編集する」
- 166 ページの「「リソースリスト」コマンドを使用してリソースを編集する」

▼ リソースリストを表示する

リソースリストの既存のリソースを表示できます。

1 管理者インタフェースにログインします。

2 メインメニューの「リソース」をクリックします。
「リソースのリスト」サブタブにリソースリストが表示されます。

▼ リソースウィザードを使用してリソースを編集する

リソースウィザードを使用して、リソースパラメータ、アカウント属性、およびアイデンティティーシステムパラメータを編集します。リソース上で作成されたユーザーに使用するアイデンティティーテンプレートを指定することもできます。

1 **Identity Manager** の管理者インタフェースで、メインメニューの「リソース」をクリックします。
「リソースのリスト」サブタブにリソースリストが表示されます。

2 編集するリソースを選択します。

3 「リソースアクション」ドロップダウンメニューで、「リソースウィザード」(「編集」の下) を選択します。
リソースウィザードが起動し、選択したリソースを編集モードで開きます。

▼ 「リソースリスト」コマンドを使用してリソースを編集する

リソースの編集ウィザードのほかに、「リソースリスト」コマンドを使用して、リソースに対する一連の編集アクションを実行できます。

1 リソースリストから **1** つ以上のオプションを選択します。
次のオプションがあります。

- 「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。複数のタイプのリソースを同時に選択できます。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」。一部のリソースタイプでは、新しいオブジェクトを作成できます。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。

- 「リソースの複製」。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。
- 「リソースについて一括操作を実行」。リソースとアクションのリストを指定して、(CSV 形式の入力から) リスト内のすべてのリソースに適用します。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。

2 変更を保存します。

▼ リソースアカウント属性を表示または編集する

リソースアカウント属性 (またはスキーママップ) は、管理するリソースの属性を参照する abstract メソッドを提供します。スキーママップを使用すると、Identity Manager 内で属性を参照する方法 (スキーママップの左側) およびその名前を実際のリソース上の属性名にマッピングする方法 (スキーママップの右側) を指定できます。次に、フォームまたはワークフロー定義内で Identity Manager 属性名を参照したり、リソース自体の属性を効果的に参照したりできます。

Identity Manager の属性と LDAP リソースの属性間のマッピング例を、次に示します。

Identity Manager の属性		**LDAP** リソースの属性
`firstname`	`<-->`	`givenName`
`lastname`	`<-->`	`sn`

リソースに対してアクションを実行する際、Identity Manager 属性 `firstname` への参照はすべて、実際には LDAP 属性 `givenName` への参照です。

Identity Manager から複数のリソースを管理する際、共通の Identity Manager アカウント属性を多数のリソース属性にマッピングすると、リソースの管理が大幅に簡略化されます。たとえば、Identity Manager `fullname` 属性を Active Directory リソース属性 `displayName` にマッピングできます。一方、LDAP リソース上で、同じ Identity Manager `fullname` 属性を LDAP 属性 `cn` にマッピングできます。結果として、管理者は `fullname` 値を一度指定するだけで済みます。ユーザーを保存する際、さまざまな属性値を持つリソースに `fullname` 値が渡されます。

リソースウィザードの「アカウント属性」ページでスキーママップを設定することにより、次を実行できます。

- 管理するリソースから取得される属性の属性名およびデータ型を定義する
- リソース属性を、企業または組織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

リソースアカウント属性を表示または編集するには、次の手順に従います。

1 管理者インタフェースで、「リソース」をクリックします。

2 アカウント属性を表示または編集するリソースを選択します。

3 「リソースアクション」リストで、「リソーススキーマの編集」をクリックします。

リソースアカウント属性の編集ページが開きます。

スキーママップの左の列 (タイトルは「アイデンティティーシステムのユーザー属性」) には、Identity Manager の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。

リソースグループ

「リソース」領域は、リソースグループを管理するために使用します。 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 Server 2007 のリソースは、既存の 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、その前にこのアカウントが存在している必要があります。Windows Active Directory のリソースと Exchange Server 2007 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、選択領域で選択を行い、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

このセクションでは、グローバルリソースポリシーの編集方法と、リソースのタイムアウト値の設定方法について説明します。

▼ ポリシー属性を編集する

「グローバルリソースポリシー属性の編集」ページから、リソースポリシー属性を編集できます。

1 「グローバルリソースポリシー属性の編集」ページを開き、必要に応じて属性を編集します。

次の属性があります。

- 「デフォルトの収集タイムアウト」。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、ミリ秒単位で指定します。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。
- 「デフォルトの待機タイムアウト」。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、ミリ秒単位で指定します。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。
- 「大文字と小文字を区別しない場合のデフォルトの待機タイムアウト」。アダプタが、タイムアウトするまでに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、ミリ秒単位で指定します。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。
- 「リソースアカウントパスワードポリシー」。該当する場合は、選択されたリソースに適用され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。
- 「リソースアカウント除外規則」。該当する場合は、除外されたリソースアカウントを管理する規則を選択します。「なし」がデフォルトの選択です。

2 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。

▼ 追加のタイムアウト値を設定する

Waveset.properties 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。この値を指定しない場合は、デフォルト値の 50 が使用されます。

1 次の行を Waveset.properties ファイルに追加します。

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

2 ファイルを保存します。

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 5–13 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。

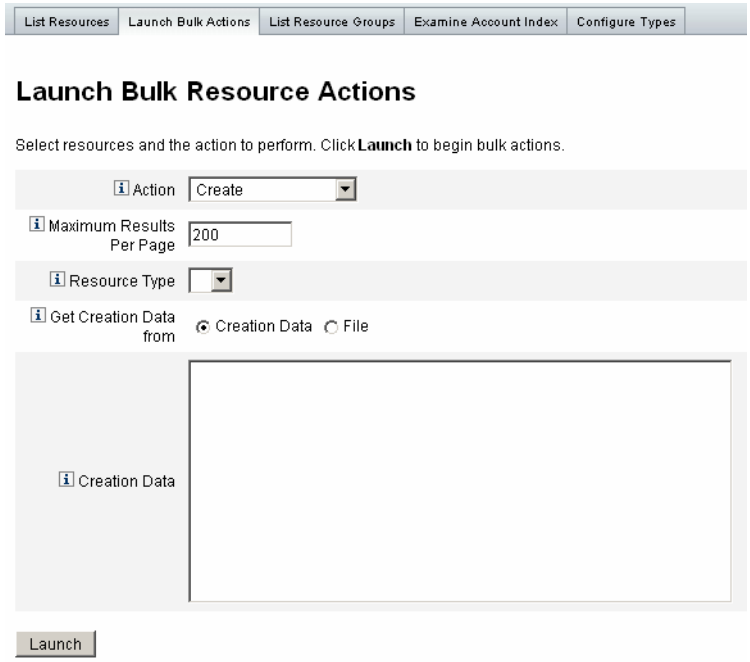


図 5–13 「一括リソースアクションの起動」ページ

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、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のいずれかのオプションを 1 つ選択します。

  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」領域を使用して、アクションを含んだ使用するファイル、または「入力」領域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領域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。

外部リソースとその管理について

Identity Manager を使用すると、自社の外部リソースを作成、プロビジョニング、および集中管理することもできます。

この節では、外部リソースを操作する方法を説明します。トピックは次のように構成されています。

- 172 ページの「外部リソースとは」
- 172 ページの「外部リソースを使用する理由」
- 173 ページの「外部リソースの設定」
- 190 ページの「外部リソースの作成」
- 193 ページの「外部リソースのプロビジョニング」
- 197 ページの「外部リソースの割り当て解除とリンク解除」
- 198 ページの「外部リソースのトラブルシューティング」

外部リソースとは

「外部リソース」とは、ユーザーアカウント情報を直接格納しない一意のリソースタイプです。Identity Manager の動作の外部にあるリソースであるといえます。こうしたリソースには、デスクトップコンピュータ、ノートパソコン、携帯電話、セキュリティーバッジなどがあります。

外部リソースのプロビジョニングでは、ほとんどの場合、1 つ以上の手動プロセスが必要です。たとえば、新入社員のノートパソコンをプロビジョニングするために初期要求を行なって必要な承認を得たあと、会社の注文要求システムに購買請求要求を送信する必要が生じることがあります。注文情報を指定したあと、ノートパソコンを新入社員個人に配布してプロビジョニング要求を完了する前に、そのノートパソコンに業務アプリケーションをインストールして事前設定する必要が生じることがあります。

外部リソースを使用する理由

Identity Manager を使用して外部リソースをプロビジョニングすると、申請中の要求について、プロビジョニングしている対象の詳細も含めて、1 人または複数のプロビジョニングツールに通知できます。

たとえば、ユーザーのためにノートパソコンを手動で注文し、事前設定する必要がある IT マネージャーが、外部リソースのプロビジョニングツールである場合があります。

また、Identity Manager は、特定のユーザーに対してプロビジョニングされた外部リソースについての情報を維持し、プロビジョニング要求の完了時にその情報を更新します。さらに、この情報は Identity Manager によって表示、レポート、コンプライアンス監査の検証、およびエクスポートに使用できるようになります。

注 – 外部リソースを設定するには、「External Resource Administrator」機能が必要です。新しい外部リソースを作成するには、「Resource Administrator」機能が必要です。

外部リソースの設定

この節では、外部リソースデータストアと外部リソースのプロビジョニングツール通知設定プロセスについて説明します。

外部リソースデータストアの設定

Identity Manager の外部リソースデータストアは、外部リソースと外部リソースの割り当てに関する情報を保持する単一のデータストアです。このデータストアは、データベースである場合とディレクトリである場合があります。

- 外部リソースデータストアが「データベース」である場合、そのデータストアは ScriptedJdbcResourceAdapter によって管理されます。
- 外部リソースデータストアが「ディレクトリ」である場合、そのデータストアは LDAPResourceAdapter によって管理されます。

注 – 外部リソースデータストアを設定するには、「External Resource Administrator」機能が必要です。

外部リソースデータストアには、データを必要に応じた属性値で格納でき、それらの値を 1 つまたは複数のテーブルに格納できます。

たとえば、MySQL データベースを使用している場合、外部リソース情報は次のテーブルに格納されます。

- `extres.accounts` テーブルには accountID と resourceID が含まれます。外部リソースデータストアは単一のデータストアであるため、Identity Manager は一意の ID キー、`<accountId>@<resourceId>` を指定し、その resourceID によってアカウントを一意に識別します。
- `extres.attributes` テーブルには、名前と値のペアの属性の集合が含まれます。外部リソースの作成時にスキーママッピングでこれらの属性を定義します。

データベーステーブルの作成に使用するサンプルスクリプトは、Identity Manager のパッケージの次の場所に同梱されています。

wshome`/sample/ScriptedJdbc/External`

Identity Manager では複数のデータベースタイプがサポートされ、タイプごとにサンプルスクリプトが用意されています。これらのスクリプトは、特定の環境に対して必要に応じて変更できます。

外部リソースデータストアでは、LDAPResourceAdapter を使用して LDAP もサポートされます。これにより、データを既存のクラスまたはカスタムクラスで格納できます。LDIF のサンプルスクリプトも、Identity Manager のパッケージの次の場所に同梱されています。

wshome`/sample/other/externalResourcePerson.ldif`

このスクリプトは、外部リソースディレクトリデータストアの設定の一環として変更できます。

▼ データベースタイプのデータストアを設定する

変更は簡単に行うことができますが、外部リソースデータストアは、通常、一度だけ設定します。設定を変更すると、Identity Manager によって既存の外部リソースが自動的に更新されて、新たに設定したデータストアが使用されます。

データベースタイプのデータストアを設定するには、次の手順に従います。

1. **Identity Manager** 管理者インタフェースのメニューバーから、「設定」→「外部リソース」の順に選択します。
2. 「データストアの設定」ページが表示されたら、「データストアのタイプ」メニューから「**Database**」を選択します。さらにオプションが表示されます。

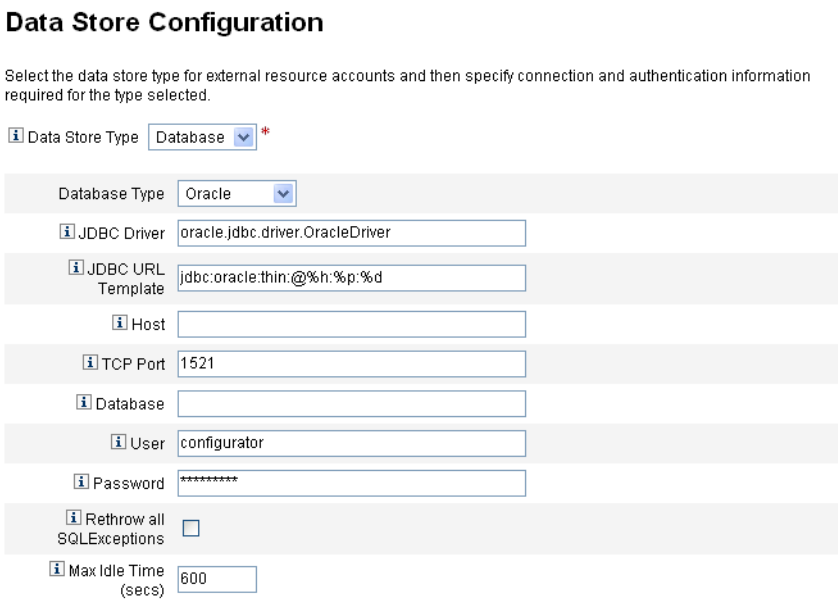


図 5–14 「データストアの設定」ページ:「Database」

3 次の接続および認証情報を指定します。

注 – Identity Manager は、自動的に、「JDBC ドライバ」、「JDBC URL テンプレート」、ポート、および「最大アイドル時間（秒）」フィールドにデフォルト値を取り込みます。これらのデフォルト値は、必要に応じて変更できます。

- 「JDBC ドライバ」。JDBC ドライバのクラス名を指定します。
- 「JDBC URL Template」。JDBC ドライバの URL テンプレートを指定します。
- 「ホスト」。データベースを実行しているホストの名前を入力します。
- 「TCP ポート」。データベースが待機中のポート番号を入力します。
- 「データベース」。データストアテーブルが含まれるデータベースサーバーのデータベース名を入力します。
- 「ユーザー」。データストアテーブルから行を読み込み、更新、および削除するために十分な権限を持つデータベースユーザーの ID を入力します。たとえば、root などです。
- 「パスワード」。データベースユーザーのパスワードを入力します。
- 「すべての SQLException を再スローする」。例外エラーコードが 0 の場合に SQL 例外を SQL 文に再スローするには、このボックスをチェックします。

  このオプションを有効にしなかった場合、Identity Manager はこれらの例外を取り込み、抑制します。

- 「Max Idle Time」。プール内で JDBC 接続を未使用のままにしておく最大時間を秒単位で指定します。

  指定した時間が経過する前に接続が使用されていない場合、Identity Manager は接続を閉じ、プールから削除します。

  - デフォルト値は 600 秒です。
  - 値を -1 にすると、接続は期限切れになりません。

4 データストアへの接続に成功したら、サポートされるリソースアクションごとに、実行するスクリプトを 1 つ以上指定する必要があります。手順については、176 ページの「アクションスクリプトを設定する」を参照してください。

▼ アクションスクリプトを設定する

Identity Manager で特定の要求の状態の取得、作成、更新、削除、有効化、無効化、テストを追跡および実行するために使用する、一連の BeanShell (`bsh`) スクリプトを指定する必要があります。

次の場所に、サンプルのアクションスクリプトがあります。

wshome`/sample/ScriptedJdbc/External/beanshell`

注 – これらのサンプルを変更して、独自のカスタムアクションスクリプトを作成できます。カスタムスクリプトはアクションスクリプト選択ツールに追加され、「利用可能」リストと「選択されたカスタム列」リストの行の下に表示されます。

Identity Manager には、外部リソースに対してサポートされるデータベースタイプのリソースアクションのサンプルスクリプトが用意されています。これらのスクリプトにアクセスするには、次の場所にある ResourceAction スクリプトを使用します。

wshome`/sample/ScriptedJdbc/External/beanshell`

デフォルトのデータベース名、ユーザー名、およびパスワードは、すべて `extres` です。

- 他のデータベースオプションのいずれかを選択する場合や、別のユーザー名やデータベース名を使用したい場合は、サンプルのデータベース作成スクリプトや ResourceAction スクリプトを別の値に変更する必要があります。

  たとえば、MySQL データベースを選択して、既存のデータベース名、ユーザー名、およびパスワードを変更する場合は、デフォルトのデータベース名、ユーザー名、およびパスワードを `extres` から `externalresources`、`externaladmin`、および `externalpassword` にそれぞれ変更することによって、`create_external_tables.mysql` スクリプトを更新する必要があります。

- 次に、ResourceAction スクリプトを、デフォルトの `extres.accounts` および `extres.attributes` の値から `externalresources.accounts` および `externalresources.attributes` にそれぞれ変更する必要があります。

アクションスクリプトを設定するには、次の手順に従います。

1 「**Data Store Configuration**」ページのアクションスクリプト選択ツールを使用して、リソースアクションごとに **1** つ以上のアクションスクリプトを指定します。リソースアクションごとに少なくとも **1** つのスクリプトを選択する必要があります。

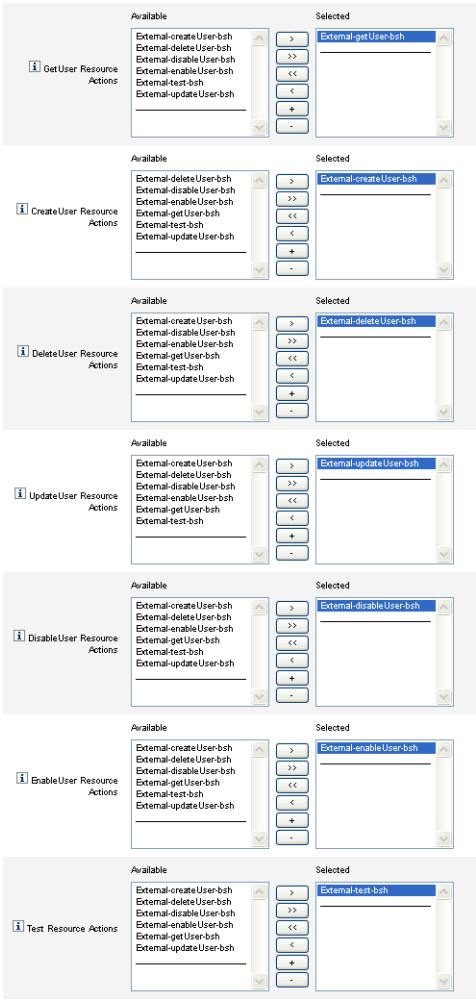


図 **5–15** アクションスクリプト領域

リソースアクションに一致するデフォルトのアクションスクリプトを選択する必要があります。たとえば、次を使用します。

- GetUser リソースアクションには `External-getUser-bsh`

注 – GetUser リソースアクションは、検索操作に使用されます。

- CreateUser リソースアクションには `External-createUser-bsh`
- DeleteUser リソースアクションには `External-deleteUser-bsh`
- UpdateUser リソースアクションには `External-updateUser-bsh`
- DisableUser リソースアクションには `External-disableUser-bsh`
- EnableUser リソースアクションには `External-enableUser-bsh`
- Test リソースアクションには `External-test-bsh`

注 – Test リソースアクションは、「テスト接続」ボタンのすべての機能を有効にするために使用されます。

リスト内のサンプルスクリプトから他の `bsh` スクリプトのいずれかを使用すると、うまくいきません。

2 メニューから「アクションコンテキストモード」を選択して、属性値をアクションスクリプトに渡す方法を指定します。

- 「Strings」。属性値を文字列値として渡します。
- 「Direct」。属性値を `com.waveset.object.AttributeValues` オブジェクトとして渡します。

3 ここで、データストア接続設定をテストします。ページの下にある「テスト接続」ボタンをクリックします。

接続が成功したことを確認するメッセージ、またはその設定でのエラーを報告するメッセージが表示されます。

4 終了したら、「次へ」をクリックして「プロビジョニング担当者への通知設定」ページに進みます。

▼ ディレクトリタイプのデータストアを設定する

ディレクトリタイプのデータストアを設定するには、次の手順に従います。

1 「データストアのタイプ」メニューから「**Directory**」を選択します。さらにオプションが表示されます。

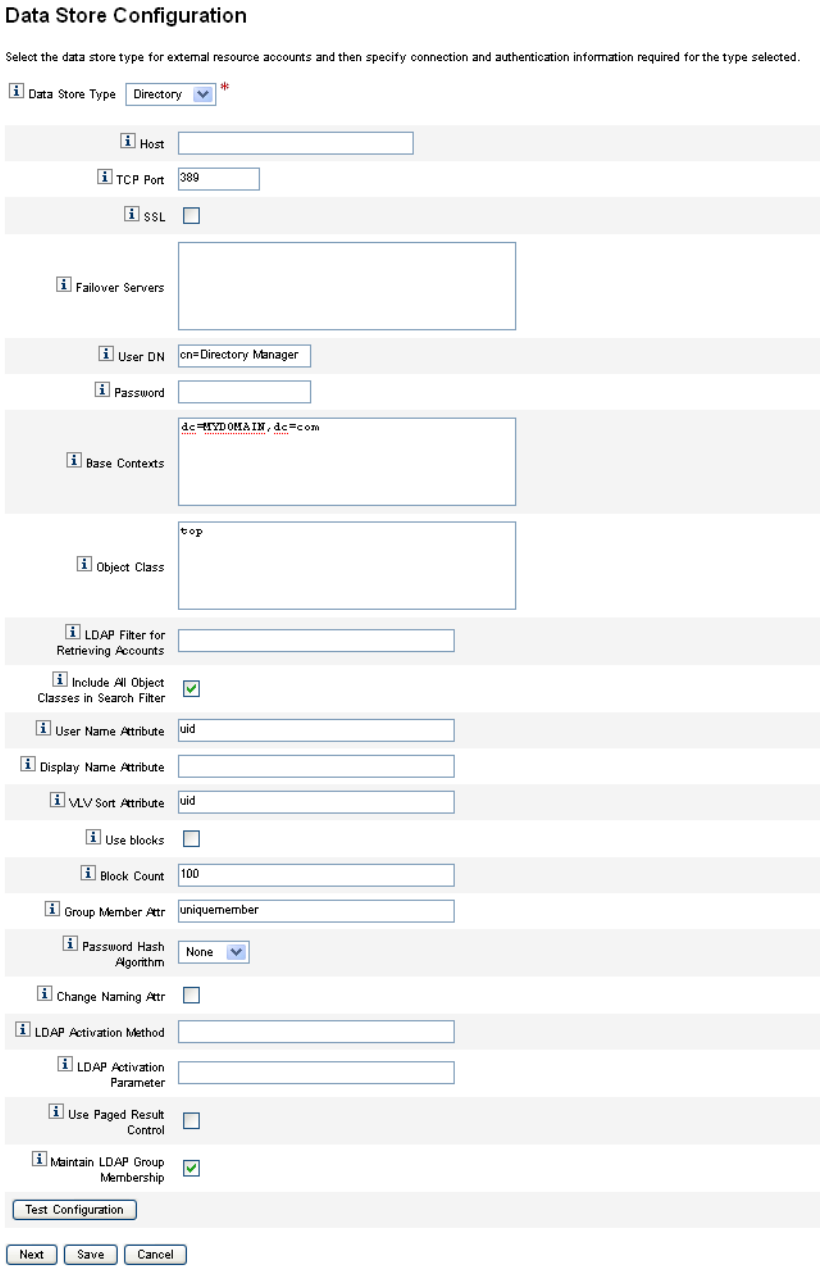


図 5–16 「Data Store Configuration」 ページ: 「Directory」

2 ディレクトリタイプのデータストアの接続および認証情報を指定する必要があります。

次のオプションを設定します。

- 「ホスト」。LDAP サーバーが実行されているホストの IP アドレスまたは名前を入力します。
- 「TCP ポート」。LDAP サーバーとの通信に使用されている TCP/IP ポートを入力します。
  - SSL を使用している場合、このポートは通常、636 です。
  - SSL 以外を使用している場合、このポートは通常、389 です。
- 「SSL」。SSL を使用する LDAP サーバーに接続するには、このオプションをチェックします。
- 「フェイルオーバーサーバー」。選択されたサーバーに障害が発生した場合にフェイルオーバーに使用されるサーバーをすべて一覧表示します。この情報を次の形式で入力します。これは、RFC 2255 に記載されている LDAP Version 3 の URL に従っています。

  ```
  ldap://ldap.example.com:389/o=LdapFailover
  ```

  URL のホスト、ポート、および識別名 (distinguished name、dn) の部分のみがこの設定に関係します。

  選択されたサーバーに障害が発生した場合、JNDI はリスト内の次のサーバーに自動的に接続します。
- 「ユーザー DN」。更新時に LDAP サーバーに対する認証に使用する dn を入力します。(デフォルトは `cn=Directory Manager`)
- 「パスワード」。プリンシパルのパスワードを入力します。
- 「ベースコンテキスト」。Identity Manager がユーザーの LDAP ツリーを検索するときに使用できる 1 つ以上の開始位置を指定します。(デフォルトは `dc=MYDOMAIN,dc=com`)

  Identity Manager は、LDAP サーバーからユーザーを検出しようとするとき、またはユーザーがメンバーであるグループを探すときに、検索を実行します。
- 「オブジェクトクラス」。LDAP ツリーで新しいユーザーオブジェクトを作成するときに使用する、1 つ以上のオブジェクトクラスを入力します。(デフォルトは top)

  エントリごとに個別の行に入力する必要があります。エントリを区切るのにコンマやスペースは使用しません。

  一部の LDAP サーバーでは、クラス階層のオブジェクトクラスをすべて指定する必要があります。たとえば、`inetorgperson` だけではなく、`top`、`person`、`organizationalperson`、および `inetorgperson` とすべてを指定する必要がある場合があります。

- 「アカウント検索用の LDAP フィルタ」。LDAP リソースから返すアカウントを制御する LDAP フィルタを入力します。フィルタを指定しなかった場合、Identity Manager は、指定されたオブジェクトクラスのすべてを含むアカウントをすべて返します。
- 「検索フィルタ内のすべてのオブジェクトクラスを含む」。すべてのアカウントが指定したすべてのオブジェクトクラスを含み、さらに「アカウント検索用の LDAP フィルタ」フィールドの LDAP フィルタで指定したフィルタに一致するようにするには、このボックスをチェックします。

注 – 検索フィルタが指定されていないときは、このオプションを有効にする必要があります。このオプションを無効にした場合は、調整やリソースからの読み込み機能を使用することによって、指定したオブジェクトクラスの一部が含まれないアカウントを Identity Manager に読み込むことができます。

読み込み後にアカウントの `objectclass` 属性が自動的に更新されることはありません。存在しないオブジェクトクラスの属性が管理者インタフェースを介して公開された場合に、`objectclass` 属性を修正せずにこの属性の値を指定すると失敗します。この問題を回避するには、「調整」や「リソースから読み込み」フォームの `objectclass` の値を上書きします。

- 「ユーザー名属性」。ディレクトリからユーザーを検索する場合に、Identity Manager ユーザー名にマップする LDAP 属性名を入力します。この名前は、多くの場合、`uid` または `cn` です。
- 「表示名属性」。このアカウント名を表示するときに使用されるリソースアカウント属性名を入力します。
- 「VLV 並べ替え属性」。リソース上の VLV インデックスに使用するソート属性の名前を入力します。
- 「ブロックを使用」。ブロック内のユーザーを検出したり処理したりするには、このボックスをチェックします。

  多数のユーザーに対して操作を実行するときにブロックでユーザーを処理すると、操作で使用されるメモリー容量が減ります。
- 「ブロック数」。処理のためにブロックにグループ化されるユーザーの最大数を入力します。
- 「グループメンバー属性」。ユーザーがグループに追加されるときにそのユーザーの識別名 (DN) で更新されるグループメンバー属性の名前を入力します。

  属性名は、グループのオブジェクトクラスに依存します。たとえば、Sun Java™ System Enterprise Edition Directory Server および他の LDAP サーバーでは、`groupOfUniqueNames` オブジェクトクラス、および `uniqueMember` 属性を持つグループが使用されます。他の LDAP サーバーでは、`groupOfUniqueNames` オブジェクトクラスおよびメンバー属性を持つグループが使用されます。

- 「パスワードハッシュアルゴリズム」。Identity Manager がパスワードのハッシュに使用できるアルゴリズムを入力します。サポートされる値は、次のとおりです。
  - SSHA
  - SHA
  - SMD5
  - MD5

  0 を指定したか、このフィールドを空白のままにした場合、Identity Manager は、パスワードをハッシュせず、LDAP サーバーがハッシュを実行しない限り、LDAP に平文パスワードを格納します。たとえば、Sun Java System Enterprise Edition Directory Server はパスワードをハッシュします。
- 「名前属性の変更」。一番左側にある相対識別名 (DN) を表すユーザー属性の変更を許可するには、このボックスをチェックします。多くの場合、ネーミング属性は uid または cn に変更されます。
- 「LDAP アクティブ化メソッド」。
  - リソースで有効化または無効化アクションへのパスワードの割り当てが使用されるようにする場合は、このフィールドを空白にします。
  - nsmanageddisabledrole キーワード、nsaccountlock キーワード、またはこのリソースのユーザーに対してアクティブ化アクションを実行するときに使用するクラス名を入力します。
- 「LDAP アクティブ化パラメータ」。「LDAP アクティブ化メソッド」フィールドで指定した内容に基づいて、値を入力します。
  - nsmanageddisabledrole キーワードを指定した場合は、次の形式で値を入力する必要があります。

    IDMAttribute=CN=nsmanageddisabledrole,*baseContext*
  - nsaccountlock キーワードを指定した場合は、次の形式で値を入力する必要があります。

    IDMAttribute=true
  - クラス名を指定した場合は、次の形式で値を入力する必要があります。

    IDMAttribute

注 – 「LDAP アクティブ化メソッド」および「LDAP アクティブ化パラメータ」については、『Sun Identity Manager 8.1 Resources Reference 』を参照してください。

- 「Paged Results Control の使用」。調整中にアカウントを繰り返し使用するために、VLV Control の代わりに LDAP Paged Results Control を使用するには、このチェックボックスをチェックします。

注 – リソースが単純なページング制御をサポートしている必要があります。

- 「LDAP グループメンバーシップの維持」。ユーザーの名前を変更したり、ユーザーを削除したりするときに、アダプタで LDAP グループのメンバーシップを維持するには、このボックスをチェックします。

  このオプションを有効にしなかった場合は、LDAP リソースでグループのメンバーシップが維持されます。

3 「テスト接続」ボタンをクリックして、データストアの接続設定をテストします。

接続が成功したことを確認するメッセージ、またはその設定でのエラーを報告するメッセージが表示されます。

4 終了したら、「保存」をクリックしてから「次へ」をクリックして「プロビジョニング担当者への通知設定」ページに進みます。

注 – LDAP リソースにユーザーを作成する前に、有効なアカウント属性とアイデンティティーテンプレートを設定する必要があります。

プロビジョニングツール通知を設定する

外部リソースのデータストアを設定したあと、プロビジョニングツール通知を設定する必要があります。要求元通知を設定することもできます。この節では、電子メールまたは Remedy を使用して通知を設定するプロセスについて説明します。

▼ 電子メール通知を設定する

注 – 電子メールテンプレートについては、「タスクテンプレートの設定」を参照してください。

1 人以上のプロビジョニングツールへの電子メール通知を設定および送信するには、次の手順に従います。

1 「プロビジョニング担当者への通知設定」ページで、「プロビジョニング担当者への通知のタイプ」メニューから「**Email**」を選択します。次の図に示すように、さらにオプションが表示されます。

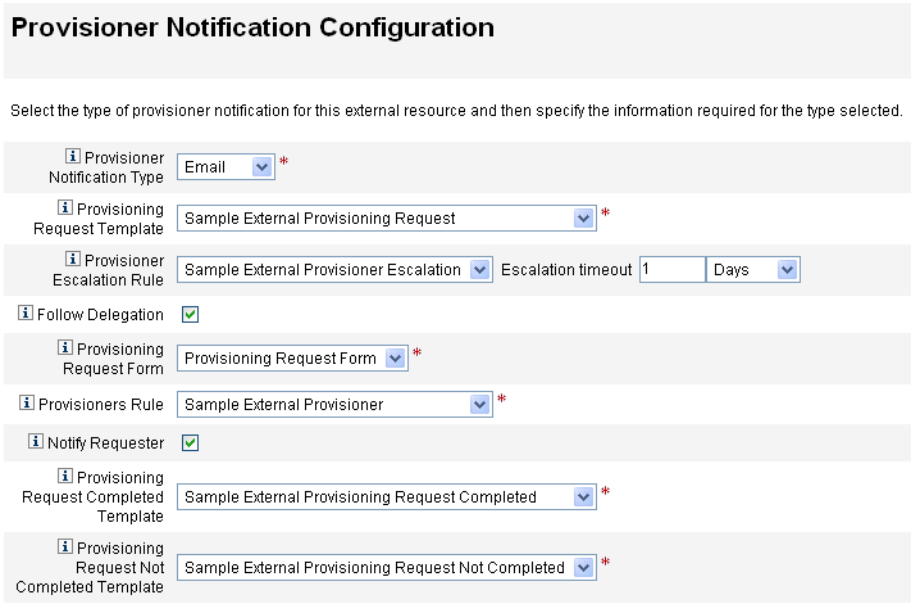


図 5–17 「プロビジョニング担当者への通知設定」ページ:「Email」通知タイプ

2 次のオプションを設定します。

- 「プロビジョニングリクエストテンプレート」。メニューから「Sample External Provisioning Request」を選択します。電子メールテンプレートを使用して、プロビジョニングツールに外部リソース要求を通知するために使用する電子メールを設定します。
- 「委任に従う」。Identity Manager でプロビジョニングツールに対して定義された委任に従う場合は、このボックスをチェックします。
- 「プロビジョニング担当者のエスカレーション規則」(省略可能)。指定されたタイムアウト期間の前に現在のプロビジョニングツールが要求に応答しなかった場合に、その要求のエスカレーション先となるプロビジョニングツールの決定規則を選択します。

注 – このメニューで使用可能なサンプル規則がいくつかありますが、「Sample External Provisioner Escalation」規則を選択するか、独自の規則を使用する必要があります。「Sample External Provisioner Escalation」規則では、外部プロビジョニングツールのエスカレーション規則を使用して、エスカレーション先のプロビジョニングツールを決定します。

- 「エスカレーションタイムアウト」。プロビジョニング要求を次のプロビジョニングツールにエスカレーションするまで待機する最大時間を指定します。

注 –

- このフィールドを空白のままにした場合や 0 を入力した場合、要求はエスカレーションされません。
- タイムアウトを指定したが、「プロビジョニング担当者のエスカレーション規則」を選択していない場合、要求が指定されたタイムアウトを過ぎると、Identity Manager は要求を設定者にエスカレーションします。設定者が存在しない場合、タイムアウトの期限が切れると、要求は「未完了」として分類されます。

- 「プロビジョニングリクエストフォーム」。外部リソースのプロビジョニングツールがプロビジョニング要求を完了または未完了としてマークするために使用できるフォームを選択します。
- 「プロビジョニング担当者の規則」。外部リソースがユーザーに割り当てられる場合にプロビジョニング要求の送信先となるプロビジョニングツールを定義する規則を選択する必要があります。

注 –

- このために、独自のルールを記述することができます。複数のプロビジョニングツールを定義することもできます。いずれかのプロビジョニングツールがタスクを完了すると、そのタスクはすべてのプロビジョニングツールのキューから削除されます。カスタム規則の記述については、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。
- このメニューで使用可能なサンプルルールがいくつかありますが、「Sample External Provisioner」ルールを選択するか、独自の規則を使用する必要があります。「Sample External Provisioner」ルールでは、設定者がプロビジョニングツールになります。

- 「リクエストした人への通知」。要求によって発生した事象についての情報が書かれた電子メールを元の要求元に返信するには、このボックスをチェックします。たとえば、プロビジョニング要求が完了であるか、未完了であるか、といった情報が追加情報として必要です。

  このオプションを有効にすると、次の追加フィールドが表示されます。

注 –

- 「プロビジョニングリクエストの完了テンプレート」。要求が完了したときに要求元に通知するための「Sample External Provisioning Request Completed」テンプレートを選択します。
- 「プロビジョニングリクエストの未完了テンプレート」。要求が完了していないときに要求元に通知するための「Sample External Provisioning Request Not Completed」テンプレートを選択します。

3 「保存」をクリックします。

「設定」ページに、引き続き別の設定タスクを実行できることが示されます。

4 「リソース」→「リソースのリスト」タブに移動します。これで、この設定に基づいて個々の外部リソースを作成する準備ができました。手順については、161 ページの「リソースを作成する」を参照してください。

▼ Remedy 通知を設定する

プロビジョニングツールへの Remedy チケットを作成および送信するには、次の手順に従います。

1 「プロビジョニング担当者への通知のタイプ」メニューから「**Remedy**」を選択します。次の図に示すように、さらにオプションが表示されます。

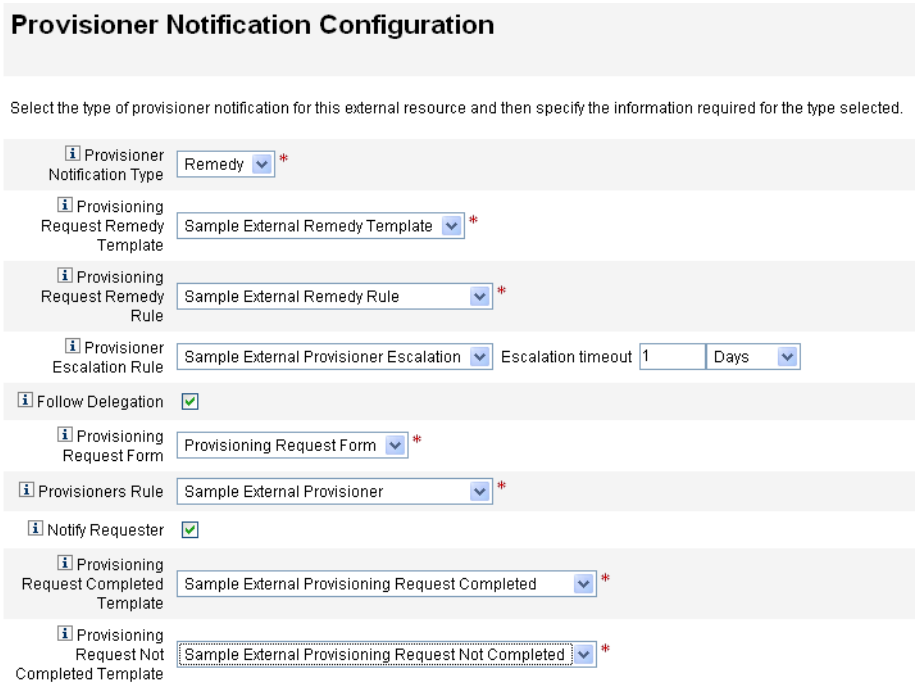


図 5–18 「プロビジョニング担当者への通知設定」ページ:「Remedy」通知タイプ

2 次のオプションを設定します。

- 「プロビジョニングリクエストの Remedy テンプレート」。メニューから「Sample External Remedy Template」を選択します。

注 – Identity Manager には、サンプルの Remedy テンプレートが用意されており、それを使用することも、必要に応じて変更することもできます。

Remedy テンプレートには、Remedy チケットの作成に使用される一連のフィールドが含まれています。Identity Manager では、Remedy のチケット状態に関するクエリーを実行し、タスクが完了したか完了していないかを確認するためにも、このテンプレートが使用されます。

- 「プロビジョニングリクエストの Remedy 規則」。Remedy の設定を定義するには、このメニューからルールを選択する必要があります。

注 – このメニューで使用可能なサンプルルールがいくつかありますが、「Sample External Remedy Rule」ルールを選択するか、独自のカスタムルールを使用する必要があります。「Sample External Remedy Rule」では、Remedy ルールを使用して、Remedy チケットの現在の状態が完了しているか完了していないかを判断します。

Remedy テンプレートには、Remedy チケットの作成に使用される一連のフィールドが含まれています。Identity Manager では、Remedy のチケット状態に関するクエリーを実行し、タスクが完了したか完了していないかを確認するためにも、このテンプレートが使用されます。

Identity Manager は、このルールを使用して、Remedy チケットの現在の情報に対してクエリーを実行します。チケット状態が完了または未完了の場合、Identity Manager は作業項目をそれぞれ完了または未完了としてマークします。

注 – このために、独自のルールを記述することができます。「Sample External Remedy Rule」というサンプルルールを使用するか、必要に応じて変更することができます。カスタム規則の記述については、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。

- 「委任に従う」。Identity Manager でプロビジョニングツールに対して定義された委任に従う場合は、このボックスをチェックします。
- 「プロビジョニング担当者のエスカレーション規則」(省略可能)。指定されたタイムアウト期間の前に現在のプロビジョニングツールが要求に応答しなかった場合に、その要求のエスカレーション先となるプロビジョニングツールの決定規則を選択します。

注 – このメニューで使用可能なサンプル規則がいくつかありますが、「Sample External Provisioner Escalation」規則を選択するか、独自の規則を使用する必要があります。「Sample External Provisioner Escalation」規則では、外部プロビジョニングツールのエスカレーション規則を使用して、エスカレーション先のプロビジョニングツールを決定します。

- 「エスカレーションタイムアウト」。プロビジョニング要求を次のプロビジョニングツールにエスカレーションするまで待機する最大時間を指定します。

注 –

- このフィールドを空白のままにした場合や 0 を入力した場合、要求はエスカレーションされません。
- タイムアウトを指定したが、「プロビジョニング担当者のエスカレーション規則」を選択していない場合、要求が指定されたタイムアウトを過ぎると、Identity Manager は要求を設定者にエスカレーションします。設定者が存在しない場合、タイムアウトの期限が切れると、要求は「未完了」として分類されます。

- 「プロビジョニングリクエストフォーム」。外部リソースのプロビジョニングツールがプロビジョニング要求を完了または未完了としてマークするために使用できるフォームを選択します。
- 「プロビジョニング担当者の規則」。この外部リソース要求に対して 1 人以上のプロビジョニングツールを決定するルールを選択します。

注 – このために、独自のルールを記述することができます。複数のプロビジョニングツールを定義することもできます。いずれかのプロビジョニングツールがタスクを完了すると、そのタスクはすべてのプロビジョニングツールのキューから削除されます。カスタム規則の記述については、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。

  - 「Sample External Provisioner」。設定者がプロビジョニングツールになります。
  - 「Sample External Provisioner Escalation」。外部プロビジョニングツールのエスカレーションルールを使用して、エスカレーション先のプロビジョニングツールを決定します。
  - 「Sample External Remedy Rule」。Remedy の設定者の設定を定義します。
- 「リクエストした人への通知」。要求が完了したとき、または完了しないときに、要求元に電子メールを送信する場合は、このボックスをチェックします。このオプションを有効にすると、次の追加フィールドが表示されます。
  - 「プロビジョニングリクエストの完了テンプレート」。要求が完了したときに使用する電子メールテンプレートを選択します。
  - 「プロビジョニングリクエストの未完了テンプレート」。要求が完了しないときに使用する電子メールテンプレートを選択します。

注 – 電子メールテンプレートについては、302 ページの「タスクテンプレートの設定」を参照してください。

3 「保存」をクリックします。

「設定」ページに、引き続き別の設定タスクを実行できることが示されます。

4 「リソース」→「リソースのリスト」タブに移動します。これで、この設定に基づいて個々の外部リソースを作成する準備ができました。手順については、190 ページの「外部リソースの作成」を参照してください。

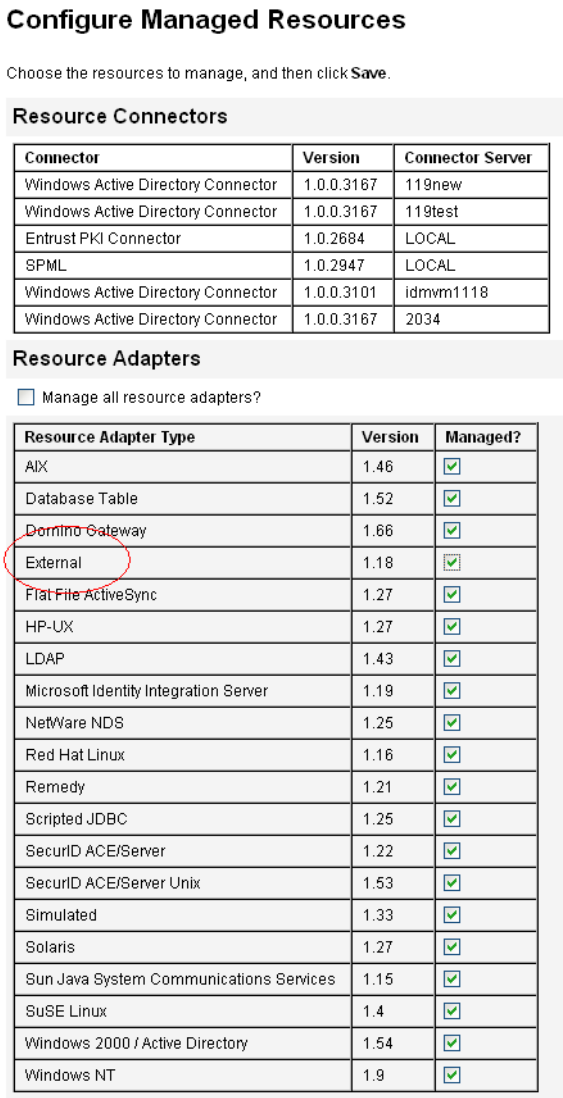
外部リソースの作成

外部リソースデータストアとプロビジョニングツール通知の設定後、新しい外部リソースを作成できます。

注 – 新しい外部リソースを作成するには、リソース管理者機能が必要です。

新しい外部リソースを作成するには、次の手順に従います。

1. メインメニューバーから、「リソース」タブを選択します。デフォルトでは「リソースのリスト」タブが表示されます。
2. 「タイプの設定」タブをクリックすると、「管理するリソースの設定」ページが表示されます。



Configure Managed Resources

Choose the resources to manage, and then click **Save**.

Resource Connectors

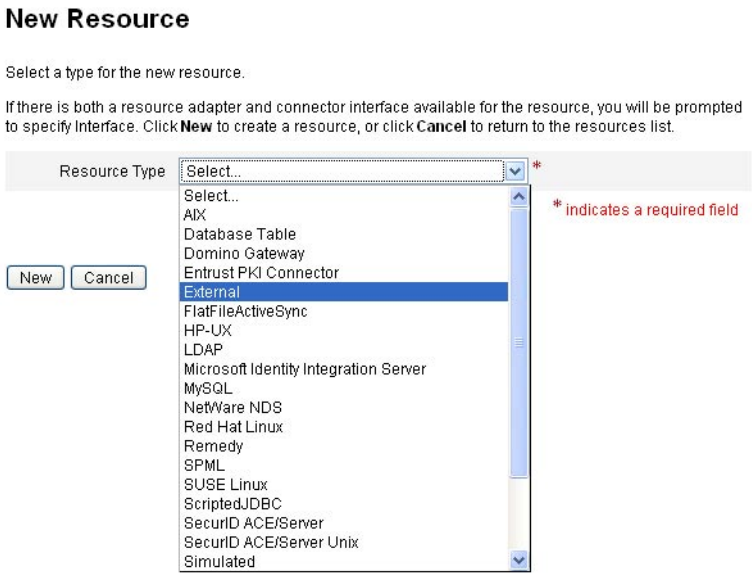
Connector	Version	Connector Server
Windows Active Directory Connector	1.0.0.3167	119new
Windows Active Directory Connector	1.0.0.3167	119test
Entrust PKI Connector	1.0.2684	LOCAL
SPML	1.0.2947	LOCAL
Windows Active Directory Connector	1.0.0.3101	idmvm1118
Windows Active Directory Connector	1.0.0.3167	2034

Resource Adapters

☐ Manage all resource adapters?

Resource Adapter Type	Version	Managed?
AIX	1.46	☑
Database Table	1.52	☑
Domino Gateway	1.66	☑
External	1.18	☑
Flat File ActiveSync	1.27	☑
HP-UX	1.27	☑
LDAP	1.43	☑
Microsoft Identity Integration Server	1.19	☑
NetWare NDS	1.25	☑
Red Hat Linux	1.16	☑
Remedy	1.21	☑
Scripted JDBC	1.25	☑
SecurID ACE/Server	1.22	☑
SecurID ACE/Server Unix	1.53	☑
Simulated	1.33	☑
Solaris	1.27	☑
Sun Java System Communications Services	1.15	☑
SuSE Linux	1.4	☑
Windows 2000 / Active Directory	1.54	☑
Windows NT	1.9	☑

3. 「リソースアダプタ」テーブルで、「外部」リソースタイプが使用可能であることを確認します。
4. 「リソースのリスト」タブに戻り、「リソースタイプアクション」メニューから「新規リソース」を選択します。
5. 「新規リソース」ページが表示されたら、「リソースタイプ」メニューから「External」を選択し、「新規」をクリックします。



6. 外部リソース作成ウィザードの開始画面が表示されます。「次へ」をクリックします。

   「Data Store Configuration」ページの読み取り専用ビューが表示され、先ほど定義した接続および認証情報が示されます。

   前述のとおり、設定はすべての外部リソースに適用されるため、通常、このデータストアは一度だけ設定します。この情報のいずれかを変更する場合は、「設定」→「External Resources」タブに戻る必要があります。

注 – 先に進む前に現在のデータストアの構成を再テストする場合は、ページの下部にある「設定のテスト」をクリックします。

---

7. 「次へ」をクリックすると、「プロビジョニング担当者への通知設定」ページが開きます。このページは、「設定」→「External Resources」タブで設定したページと同じです。
8. 現在の「Provisioner Notification」設定を確認し、新しいリソースに対して必要な変更を行います。

注 – 必要に応じて、「183 ページの「プロビジョニングツール通知を設定する」」の設定手順をもう一度参照してください。このページに対して行なった変更はいずれも、このリソースにのみ影響します。

---

9. 「次へ」をクリックします。

   ここからの外部リソースの作成プロセスは、他のリソースの作成プロセスと同じです。ウィザードには、さらにいくつかのページが表示されます。

   - 「アカウント属性」ページ。このページを使用して、リソースのオプションのアカウント属性を定義し、アイデンティティーシステム属性を新しいリソースアカウント属性にマップします。たとえば、「ノートパソコン」という外部リソースを作成する場合は、モデルやサイズの属性を追加するといいでしょう。

     注 – このページにはデフォルトは指定されません。

   - 「アイデンティティーテンプレート」ページ。このページを使用して、この外部リソースで作成されたユーザーのアカウント名の構文を定義します。デフォルトのアイデンティティーテンプレート、`$accountId$` を使用することも、別のテンプレートを指定することもできます。
   - 「アイデンティティーシステムのパラメータ」ページ。このページを使用して、外部リソースのアイデンィティーシステムパラメータを設定します。たとえば、ポリシーを無効にしたり、再試行を設定したり、承認者を指定したりすることができます。

   これらのページの詳細や、このリソースの設定を終了するために必要な手順については、161 ページの「リソースを作成する」を参照してください。

10. 「アイデンティティーシステムのパラメータ」ページの設定が終了したら、「保存」をクリックします。これで、他のリソースと同様に、このリソースをユーザーに割り当てることができます。

外部リソースのプロビジョニング

この節では、次の実際のプロビジョニングプロセスについて説明します。

- 193 ページの「外部リソースをユーザーに割り当てる」
- 194 ページの「外部リソースのプロビジョニング要求に応答する」

▼ 外部リソースをユーザーに割り当てる

外部リソースをユーザーに割り当てるには、次の手順に従います。

注 – 外部リソースを割り当てるには、リソース管理者機能が必要です。

1 「アカウント」→「アカウントのリスト」をクリックし、そのページのユーザー名をクリックします。

2 「ユーザーの編集」ページが表示されたら、「リソース」タブをクリックします。

3 「個別リソース割り当て」の「利用可能なリソース」リストで外部リソースを見つけ、「現在のリソース」リストに移動して、「保存」をクリックします。

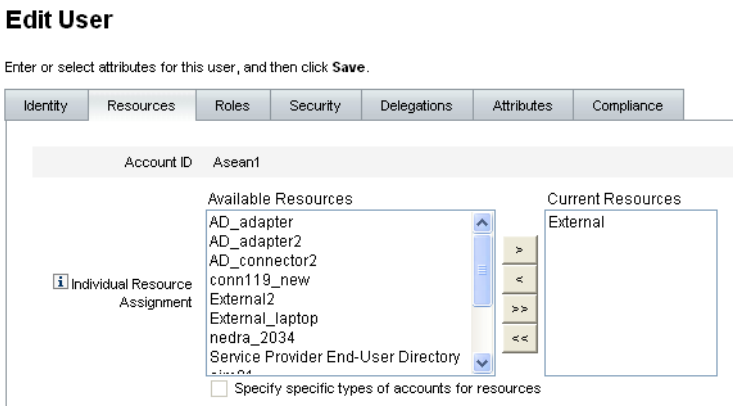


図 5–19 「ユーザーの編集」ページ

Identity Manager は、プロビジョニングタスクを作成し、そのプロビジョニングタスクの所有者を示すメッセージを送信します。このリソースに「プロビジョニング担当者への通知」ページが設定されているときは、「プロビジョニング担当者の規則」を使用して、1 人以上のプロビジョニングツールが定義されています。

Identity Manager は、電子メールまたは Remedy チケットを使用して、要求が申請中であることをプロビジョニングツールに通知することもできます。

注 – 他のリソースと同様に、ユーザーは承認者を定義することができ、承認者が要求を承認したり拒否したりすることができます。また、ユーザーはプロビジョニングツールを定義する必要がありますが、プロビジョニングツールは要求を承認したり拒否したりすることはできません。その代わりに、プロビジョニングツールはタスクを完了する場合も、完了しない場合もあります。

---

4 「アカウント」→「アカウントのリスト」ページに戻るには、「**OK**」をクリックします。ユーザー名の横の作業項目アイコン内に砂時計が表示され、要求が申請中であることを示します。

▼ 外部リソースのプロビジョニング要求に応答する

プロビジョニング要求が生成されると、その要求は、定義されたプロビジョニングツールが手動プロビジョニングを完了するか、要求を未完了としてマークするま

で、または要求がタイムアウトするまで、プロビジョニングプロセスを中断します。Identity Manager は、これらのプロビジョニング応答を監査します。

他の作業項目と同様に、「作業項目」→「プロビジョニングリクエスト」タブから申請中の外部リソースのプロビジョニング要求をすべて確認できます。

プロビジョニング要求には次のように応答します。

1 「作業項目」>「プロビジョニングリクエスト」タブをクリックして、「プロビジョニング待ち」ページを開きます。

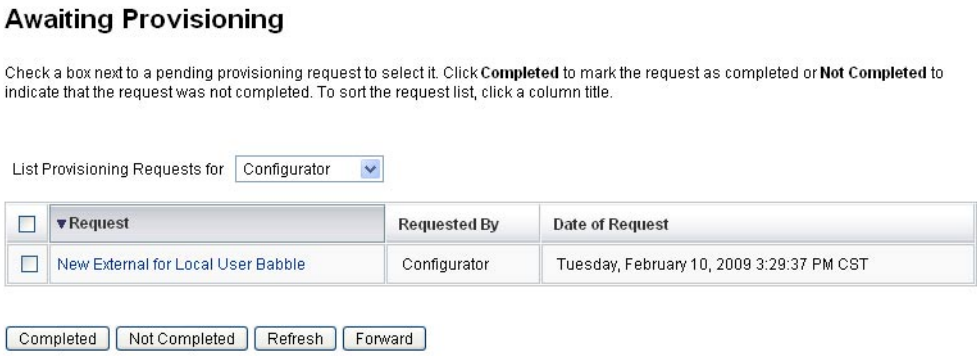


図 5–20 「プロビジョニング待ち」ページ

2 申請中のプロビジョニング要求を見つけ、選択します。

3 オプションで、プロビジョニング要求の電子メールを開き、「プロビジョニングリクエストテンプレート」で定義されたリンクをクリックし、ログインしてプロビジョニング要求についての詳細を含むページを表示します。

このページから、要求された属性を更新し、ユーザーに対してプロビジョニングされた内容を正確に反映することができます。たとえば、ユーザーがソニーのノートパソコンを要求したが、そのモデルを用意できなかった場合、実際にプロビジョニングしたモデルでこのページを更新します。

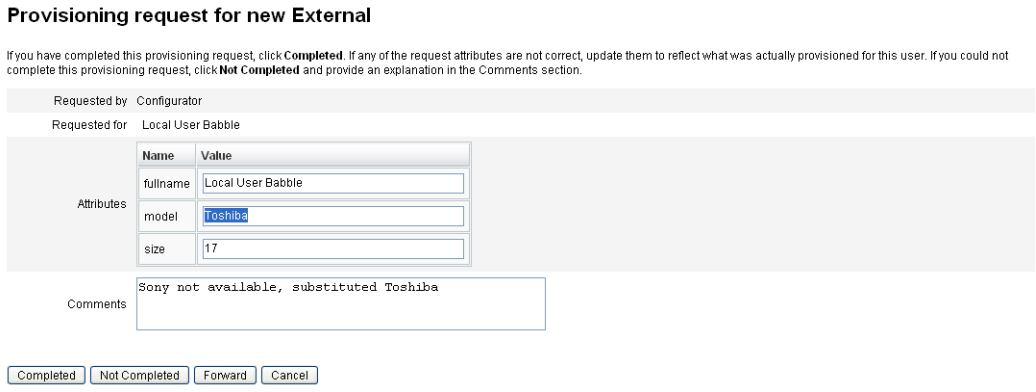


図 5–21 新しいノートパソコンに対するプロビジョニング要求

4 次のボタンのいずれかをクリックして、要求を処理します。

- リソースをプロビジョニングできる場合は、「完了しました」をクリックします。

  Identity Manager は、ユーザーの外部リソースアカウント属性を更新して、実際にプロビジョニングされた内容を示し、申請中のプロビジョニング状態フラグを削除して、プロビジョニング要求の作業項目の更新を完了します。

  設定されると、Identity Manager は、そのために設定された電子メールテンプレートを使用して、要求元にプロビジョニング要求が完了したことを通知します。
- リソースをプロビジョニングできない場合は、理由を明らかにし、「未完了」をクリックします。

  要求を「未完了」としてマークすると、
  - ユーザーは外部リソースに対してプロビジョニングされません。
  - 外部リソースはユーザーに割り当てられたままになります。
  - 黄色のアイコンは、ユーザーに更新が必要であることを示し、ユーザー名の横に表示されます。

    このユーザーを編集すると、エラーメッセージが表示され、ユーザーが外部リソースに見つからないことが示されます。
  - 設定されると、Identity Manager は、そのために設定された電子メールテンプレートを使用して、要求元に通知します。
- リソースをプロビジョニングできない場合は、「転送」をクリックして、要求をほかの第三者に転送することもできます。

プロビジョニング要求の作業項目が完了したとき、または完了していないとき、Identity Manager はユーザーに割り当てられた外部リソースの申請中状態を消去し、外部リソースデータストアに対して更新は発生しません。

リソースは、そのリソースに関するユーザーの accountId も含めて、そのユーザーの割り当てられたリソースのリストと、現在のリソースアカウントのリストに表示されます。

注 – 割り当てられたプロビジョニングツールが指定されたタイムアウトの前にプロビジョニング要求に応答しない場合、Identity Manager は関連付けられたプロビジョニング要求の作業項目を取り消します。

参考 プロビジョニング要求のエスカレーション

- 「Provisioner Notification」ページを設定するときにタイムアウト期間を指定し、プロビジョニング要求がタイムアウト期間を過ぎた場合、Identity Manager は次のアクションのいずれかを実行します。
  - 「プロビジョニング担当者のエスカレーション規則」を指定した場合、Identity Manager はそのルールを使用して次のプロビジョニングツールを決定し、要求をそのプロビジョニングツールにエスカレーションします。
  - 「プロビジョニング担当者のエスカレーション規則」を選択しなかった場合、Identity Manager は要求を設定者にエスカレーションします。設定者が存在しない場合、タイムアウトの期限が切れると、要求は「未完了」として分類されます。
- 「エスカレーションタイムアウト」フィールドを空白のままにした場合や 0 を入力した場合、Identity Manager は要求をエスカレーションしません。

プロビジョニング要求の委譲

外部リソースのプロビジョニング作業項目は、他のプロビジョニング要求と同様に委任できます。詳細と手順については、231 ページの「作業項目の委任」を参照してください。

外部リソースの割り当て解除とリンク解除

外部リソースは、他のリソースと同様に、「一般」タブでユーザーから割り当て解除またはリンク解除できます。手順については、56 ページの「ユーザーの作成およびユーザーアカウントの操作」を参照してください。

注 – ユーザーから外部リソースを割り当て解除またはリンク解除しても、プロビジョニング要求や作業項目は作成されません。外部リソースを割り当て解除またはリンク解除しても、Identity Manager がリソースアカウントのプロビジョニングを解除したりリソースアカウントを削除したりすることはないため、作業は発生しません。

外部リソースのトラブルシューティング

外部リソースにまだ割り当てられているユーザーを削除することはできません。ユーザーを削除する前に、まず、それらの外部リソースのプロビジョニングを解除するか、外部リソースを削除する必要があります。

Identity Manager では、次の方法を使用して外部リソースをデバッグしたり監視したりすることができます。

- 外部リソースアダプタを監視できます。
  - データベースのデータストアを使用している場合は、`com.waveset.adapter.ScriptedJdbcResourceAdapter` および `com.waveset.adapter.JdbcResourceAdapter` 監視クラス名を監視します。
  - ディレクトリのデータストアを使用している場合は、`com.waveset.adapter.LDAPResourceAdapter` 監視クラス名を監視します。
- ワークフロー監視を使用した追加データフローおよびワークフロー監視や、NetBeans または Eclipse Identity Manager IDE プラグインを使用したデバックが可能です。
- ユーザーはデータストアを設定および制御するので、データストアの検査を使用して、そのデータストアの情報が正しいことを確認することができます。
- Identity Manager は、発生するすべてのアクティビティーに対して監査記録を作成します。

監視とトラブルシューティングについては、『Sun Identity Manager 8.1 System Administrator's Guide』を参照してください。

◆ ◆ ◆ 第 6 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情報と手順を説明します。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。

- 199 ページの「Identity Manager の管理について」
- 200 ページの「委任された管理」
- 201 ページの「管理者の作成と管理」
- 207 ページの「Identity Manager の組織について」
- 207 ページの「組織の作成」
- 211 ページの「ディレクトリジャンクションおよび仮想組織について」
- 214 ページの「機能とその管理について」
- 217 ページの「管理者ロールとその管理について」
- 228 ページの「エンドユーザー組織」
- 229 ページの「作業項目の管理」
- 234 ページの「ユーザーアカウントの承認」

Identity Manager の管理について

Identity Manager 管理者は、Identity Manager の拡張特権を持つユーザーです。

Identity Manager 管理者は、次のものを管理します。

- 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

ユーザーとは異なり、Identity Manager の管理者には機能と管理する組織が割り当てられます。これらは次のように定義されます。

- 「機能」。Identity Manager のユーザー、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子孫で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、管理タスクを実行する従業員は、それぞれ固有の役割を持っています。その結果、これらの管理者が実行可能なアカウント管理タスクの範囲が制限されます。

たとえば、管理者は Identity Manager ユーザーアカウントを作成する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、管理者の役割を定義した範囲内の特定のタスクに限定することもできます。

Identity Manager は、役割の分離および委任された管理モデルを次のようにサポートします。

- 機能の割り当て。 管理者を特定の職務に限定します
- 管理する組織の割り当て。 特定の組織とその組織内のオブジェクトの管理のみに管理者を限定します
- 「ユーザーの作成」および「ユーザーの編集」ページのフィルタ付きビューにより、職務に関係のない情報が管理者に表示されないようにします

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。委任の詳細については、231 ページの「作業項目の委任」を参照してください。

管理者の作成と管理

この節は、次のトピックで構成されています。

- 201 ページの「管理者を作成する」
- 202 ページの「管理者ビューのフィルタ」
- 203 ページの「管理者パスワードの変更」
- 204 ページの「管理者のアクションの認証」
- 206 ページの「秘密の質問の回答の変更」
- 206 ページの「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」

▼ 管理者を作成する

管理者を作成するには、ユーザーに 1 つ以上の機能を割り当て、それらの機能を適用する組織を指定します。

1 管理者インタフェースで、メニューバーの「アカウント」をクリックします。

「ユーザーリスト」ページが開きます。

2 既存のユーザーに管理特権を与えるには、ユーザー名をクリックして(「ユーザーの編集」ページが開きます)、「セキュリティー」タブをクリックします。

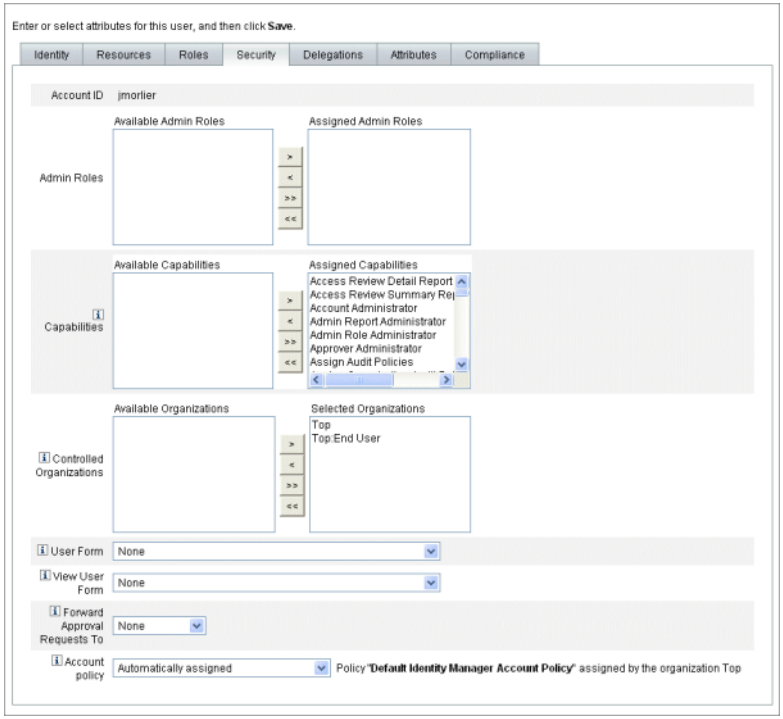
新しいユーザーアカウントを作成する必要がある場合は、56 ページの「ユーザーの作成およびユーザーアカウントの操作」を参照してください。

3 管理する属性を指定します。

設定できる属性は次のとおりです。

- 「機能」。この管理者に割り当てる 1 つ以上の機能を選択します。この情報は必須です。詳細については、214 ページの「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」。管理者に割り当てる 1 つ以上の組織を選択します。管理者は、割り当てた組織内と、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します。この情報は必須です。詳細については、207 ページの「Identity Manager の組織について」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」。現在保留中のすべての承認リクエストを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」。使用可能な場合は、このオプションを使用して、このユーザーアカウント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管理者の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、親組織に対して選択したフォームが継承されます。親組織に対してフォームが設定されていない場合は、システム設定のデフォルトのフォームが使用されます。
- 「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。

割り当て可能な Identity Manager の組み込み機能については、214 ページの「機能とその管理について」を参照してください。

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、次のフォームを使用して別の管理者のパスワードを変更できます。

- 「Change User Password」フォーム。このフォームを開くには 2 つの方法があります。
  - メニューの「アカウント」をクリックします。「ユーザーリスト」が開きます。管理者を選択し、「ユーザーアクション」リストの「パスワードの変更」を選択します。「ユーザーパスワードの変更」ページが開きます。
  - メニューの「パスワード」をクリックします。「ユーザーパスワードの変更」ページが開きます。
- タブ付きユーザーフォーム。メニューの「アカウント」をクリックします。「ユーザーリスト」が開きます。管理者を選択し、「ユーザーアクション」メニューの「編集」を選択します。「ユーザーの編集」ページ (タブ付きユーザーフォーム) が開きます。「ID」フォームタブの「パスワード」と「パスワードの確認」フィールドに新しいパスワードを入力します。

管理者は、「パスワード」領域から自分自身のパスワードを変更できます。メニューの「パスワード」をクリックし、「自分のパスワードの変更」をクリックします。

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、通知選択など、パスワードに関する制限を決定します。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

Identity Manager では、管理者がアカウントの変更処理を行う前に、パスワードの入力を求めるように設定できます。認証に失敗すると、アカウントの変更は取り消されます。

管理者がユーザーパスワードの変更に使用できるフォームは 3 つあります。タブ付きユーザーフォーム、「Change User Password」フォーム、および「Reset User Password」フォームです。Identity Manager でユーザーアカウントの変更が処理される前に、管理者にパスワードの入力を確実に要求するために、3 つのフォームすべてを必ず更新してください。

▼ タブ付きユーザーフォームでパスワード認証の要求を有効にする

タブ付きユーザーフォームでパスワード認証を要求するには、次の手順に従います。

1. 管理者インタフェースで、ブラウザに次の **URL** を入力して **Identity Manager** デバッグページ (**43** ページの「**Identity Manager** デバッグページ」) を開きます (このページを開くにはデバッグ機能が有効である必要があります)。

   `http://<AppServerHost>:<Port>/idm/debug/session.jsp`

   システム設定ページ (Identity Manager デバッグページ) が表示されます。

2. 「**List Objects**」ボタンにあるドロップダウンメニューから「**UserForm**」を選択して、「**List Objects**」ボタンをクリックします。

   「List Objects of type: UserForm」 ページが開きます。

3. 本稼働しているタブ付きユーザーフォームのコピーを検索して、「**Edit**」をクリックします (**Identity Manager** で配布されているタブ付きユーザーフォームはテンプレートなので、変更しないでください)。

4. `<Form>` 要素内に次のコードを追加します。

```
<Properties>
  <Property name='RequiresChallenge'>
    <List>
      <String>password</String>
```

```
      <String>email</String>
      <String>fullname</String>
    </List>
  </Property>
</Properties>
```

プロパティーの値は、次のユーザー表示属性名を 1 つ以上格納できるリストです。

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

5 変更を保存します。

▼ 「Change User Password」および「Reset User Password」フォームでパスワード認証を有効にする

「Change User Password」および「Reset User Password」フォームでパスワード認証を要求するには、次の手順に従います。

1 管理者インタフェースで、ブラウザに次の **URL** を入力して **Identity Manager** デバッグページ (**43** ページの「**Identity Manager** デバッグページ」) を開きます (このページを開くにはデバッグ機能が有効である必要があります)。

`http://<AppServerHost>:<Port>/idm/debug/session.jsp`

システム設定ページ (Identity Manager デバッグページ) が表示されます。

2 「**List Objects**」ボタンにあるドロップダウンメニューから「**UserForm**」を選択して、「**List Objects**」ボタンをクリックします。

「List Objects of type: UserForm」 ページが開きます。

3 本稼働している「**Change User Password**」フォームのコピーを検索して、「**Edit**」をクリックします (**Identity Manager** で配布されている「**Change User Password**」フォームはテンプレートなので、変更しないでください)。

4 `<Form>` 要素を見つけ、`<Properties>` 要素に移動します。

5 <Properties> 要素内に次の行を追加し、変更を保存します。

```
<Property name='RequiresChallenge' value='true'/>
```

6 本稼働の「**Reset User Password** フォーム」のコピーの編集を除いて、手順 **3** から **5** を繰り返します。

秘密の質問の回答の変更

「パスワード」領域を使用して、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、第 3 章「ユーザーとアカウントの管理」の 90 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

Identity Manager 管理者インタフェースの一部のページおよび領域では、Identity Manager 管理者をアカウント ID ではなく属性 (`email` や `fullname` など) に基づいて表示できます。

たとえば、次の領域では Identity Manager 管理者を属性で表示できます。

- 「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の組織について

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。ユーザーを別の組織に動的に割り当てることもできます。

Identity Manager 管理者はさらに、管理する組織にも割り当てられます。

組織の作成

▼ 組織を作成する

Identity Manager の「アカウント」領域で組織を作成します。

1 管理者インタフェースで、メニューバーの「アカウント」をクリックします。
「ユーザーリスト」ページが開きます。

2 「新規作成アクション」メニューの「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」メニューの「新規組織」を選択します。

図 6–1 に、「組織の作成」ページを示します。

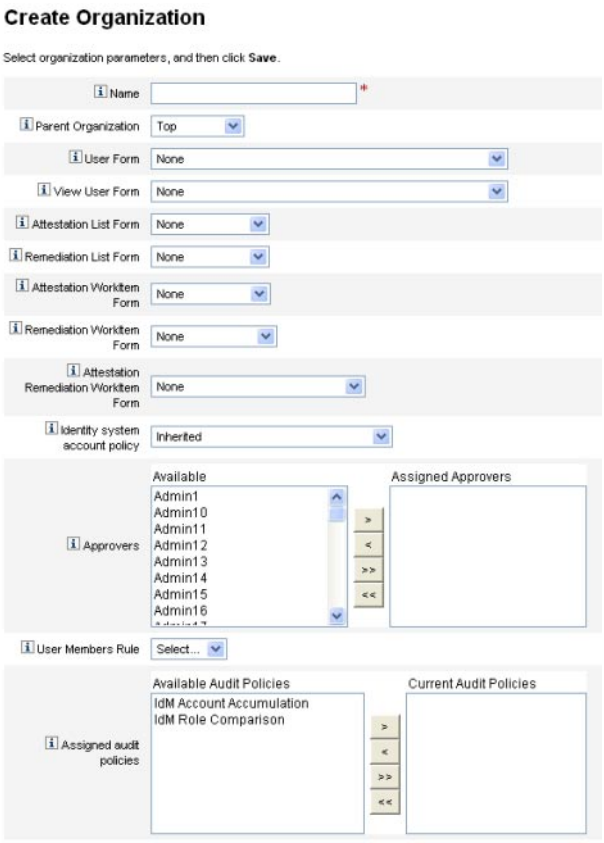


図 6–1 「組織の作成」ページ

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。

次のいずれかの方法を使用して、組織のメンバーシップを定義します。

- 「直接 (静的) 割り当て」。「ユーザーの作成」ページまたは「ユーザーの編集」ページで「ID」フォームタブを選択して、ユーザーを組織に直接割り当てます。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」。組織に割り当てられているユーザーメンバー規則を使用して、ユーザーを組織に割り当てます。規則が評価されると、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)

注 – Identity Manager で規則を作成および操作する方法については、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。

「組織の作成」ページの「ユーザーメンバー規則」メニューでユーザーメンバー規則を選択します。次の図に、ユーザーメンバー規則の例を示します。

次の例は、組織のユーザーメンバーシップを動的に管理するための、サンプルのユーザーメンバー規則の構文を示しています。

注 –

ユーザーメンバー規則を作成する前に、次の点に注意してください。

- 規則を「ユーザーメンバー規則」オプションボックスに表示する場合は、`authType` を `authType='UserMembersRule'` に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) 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。

例 6–1 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>
```

注 –Waveset.properties の一部のプロパティーを設定して、規則に基づくユーザーメンバーリストのキャッシュを制御できます。これは、メモリーとパフォーマンスに影響します。詳細については、『Sun Identity Manager 8.1 System Administrator's Guide』の「Tracing Rule-Driven Members Caches」を参照してください。

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、階層的に関連する一連の組織で、ディレクトリリソースの実際の階層型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、階層型コンテナを使用して、階層的な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 6–2 に示します。

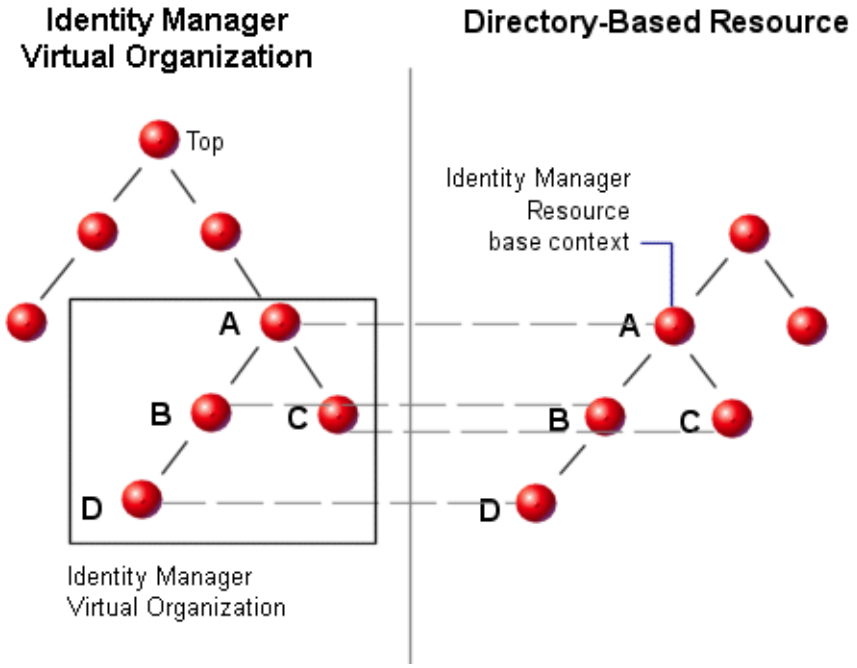


図 6–2　Identity Manager 仮想組織

ディレクトリジャンクションは、既存の Identity Manager 組織構造の任意の場所に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一連の仮想組織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、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設定

この節では、ディレクトリジャンクションの設定方法について説明します。

▼ ディレクトリジャンクションを設定する

1. 管理者インタフェースでメニューバーの「アカウント」を選択します。
   「ユーザーリスト」ページが開きます。

2. 「アカウント」リストで **Identity Manager** 組織を選択します。
   選択した組織は、設定する仮想組織の親組織になります。

3. 「新規作成アクション」メニューの「新規ディレクトリジャンクション」を選択します。
   「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。

4. 「ディレクトリ ジャンクションの作成」ページのオプションを使用して、仮想組織を設定します。
   次のオプションがあります。

   - 「親組織」。このフィールドには、「アカウント」リストで選択した組織が表示されます。リストから別の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。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 組織のみを削除する。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する。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の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、データ保護を危険にさらすことなく、一連の特権を提供します。

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 で 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領域にアクセスできるかが決まります。

Identity Manager 管理ユーザーはすべて、Identity Manager の次の領域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)

注 – Identity Manager のデフォルトのタスクベース機能と実用上の機能 (定義を含む) のリストについては、付録 D 「機能の定義」を参照してください。この付録では、タスクベースの各機能でアクセス可能なタブおよびサブタブも示します。

機能のカテゴリ

Identity Manager では、機能を次のように定義しています。

- 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。
- 実用上。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 (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

この節では、機能の作成、編集、割り当て、および名前の変更を行う方法について説明します。これらのタスクは「機能」ページから実行します。

「機能」ページの表示

「機能」ページは「セキュリティー」タブにあります。

▼ 「機能」ページを開く

1. 管理者インタフェースでトップメニューの「セキュリティー」をクリックします。
2. 二次的なメニューで「機能」をクリックします。
   「機能」ページが開き、Identity Manager の機能一覧が表示されます。

機能の作成

機能を作成するには、次の手順に従います。機能の「複製」については、216 ページの「機能の保存と名前の変更」を参照してください。

▼ 機能を作成する

1. 管理者インタフェースでトップメニューの「セキュリティー」をクリックします。
2. 二次的なメニューで「機能」をクリックします。
   「機能」ページが開き、Identity Manager の機能一覧が表示されます。
3. 「新規」をクリックします。
   「機能の作成」ページが開きます。
4. 次のようにフォームを設定します。
   a. 新しい機能に名前を付けます。
   b. 「機能」セクションの矢印ボタンを使って、ユーザーに割り当てる機能を「割り当てられた機能」ボックスに移動します。
   c. 「譲渡者」ボックスで、この機能のほかのユーザーへの割り当てを許可する 1 人以上のユーザーを選択します。
      - ユーザーを選択しない場合、この機能を割り当てることのできるユーザーは、機能を作成したユーザーのみになります。

- 機能の作成者に「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は、少なくとも 1 人のユーザーが別のユーザーに機能を割り当てられるように、1 人または複数のユーザーを選択する必要があります。

d. 「組織」ボックスで、この機能を使用できるようにする 1 つ以上の組織を選択します。

e. 「保存」をクリックします。

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は編集できます。

▼ 保護されていない機能を編集する

1. 管理者インタフェースでトップメニューの「セキュリティー」をクリックします。
2. 二次的なメニューで「機能」をクリックします。
   「機能」ページが開き、Identity Manager の機能一覧が表示されます。
3. リスト内の機能を右クリックし、「編集」を選択します。「機能の編集」ページが開きます。
4. 変更を行い、「保存」をクリックします。
   組み込み機能は編集できません。ただし、それらを別の名前で保存して、独自の機能を作成することはできます。作成する機能の中で組み込み機能を使用することもできます。

機能の保存と名前の変更

既存の機能に新しい名前を付けて保存することにより、新しい機能を作成できます。この操作は機能の「複製」とも呼ばれます。

▼ 機能を複製する

1. 管理者インタフェースでトップメニューの「セキュリティー」をクリックします。
2. 二次的なメニューで「機能」をクリックします。
   「機能」ページが開き、Identity Manager の機能一覧が表示されます。

3 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。
新しい機能の名前を入力するダイアログボックスが開きます。

4 名前を入力して「**OK**」をクリックします。
これで新しい機能を編集できるようになります。

ユーザーへの機能の割り当て

「ユーザーの作成」ページ (56 ページの「ユーザーの作成およびユーザーアカウントの操作」) または「ユーザーの編集」ページ (61 ページの「ユーザーの編集」) を使用して、機能をユーザーに割り当てます。インタフェースの「セキュリティー」領域で設定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、217 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。

注 – Identity Manager のデフォルトのタスクベース機能と実用上の機能 (定義を含む) のリストについては、付録 D 「機能の定義」を参照してください。この付録では、タスクベースの各機能でアクセス可能なタブおよびサブタブも示します。

管理者ロールとその管理について

「管理者ロール」では 2 つのもの、つまり一連の機能と制御の範囲を定義します。「制御の範囲」という語は、管理対象の 1 つ以上の組織を指します。管理者ロールを定義してから、それを 1 人以上の管理者に割り当てることができます。

注 – ロールと管理者ロールを混同しないようにしてください。ロールは、エンドユーザーの外部リソースへのアクセスを管理するために使用するのに対し、管理者ロールは主に、Identity Manager 管理者の Identity Manager オブジェクトへのアクセスを管理するために使用します。

この節の情報は、管理者ロールのみに限定されています。ロールの詳細については、119 ページの「ロールとその管理について」を参照してください。

---

1 人の管理者に複数の管理者ロールを割り当て可能です。これによって、管理者は 1 つの制御の範囲内ではある一連の機能を持ち、別の制御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する組織のユーザーの作成および編集の権限を与えます。次に 2 つ目の管理者ロールを同じ管理者に割り当てますが、今度はその管理者ロールで定義した管理する組織の別個のセット内に「ユーザーのパスワードの変更」権限のみを与えます。

管理者ロールによって、機能と管理範囲の組み合わせの再利用が可能になります。管理者ロールで、多数のユーザーに対する管理者特権の管理を簡素化することもできます。個々のユーザーに機能と管理する組織を直接割り当てるのではなく、管理者ロールを使用して管理者特権を付与するようにしてください。

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、直接または動的 (間接的) に行うことができます。

- 直接。機能や管理する組織を、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 User Report Administrator 機能と管理する組織「Top」を割り当てることが考えられます。
- 動的 (間接)。この方法では、機能および管理する組織を割り当てる規則を使用します。管理者ロールが割り当てられた管理者がログインするごとに、規則が評価されます。管理者が認証されると、割り当てられる機能や管理する組織のセットが、規則に基づいて動的に決定されます。

  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、機能規則は割り当てる機能として「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、管理する組織の規則は割り当てる管理組織として「マーケティング」を返します。

管理者ロールのユーザーへの動的割り当ては、ユーザーインタフェース、管理者インタフェースなどログインインタフェースごとに有効または無効にできます。この場合は、次のシステム設定属性を `true` または `false` 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。

システム設定オブジェクトを編集する方法については、116 ページの「Identity Manager 設定オブジェクトの編集」を参照してください。

管理者ロールの規則

Identity Manager には、管理者ロールの規則を作成するためのサンプル規則が用意されています。これらの規則は、Identity Manager インストールディレクトリの `sample/adminRoleRules.xml` にあります。

表 6–1 に、規則の名前と各規則に指定する `authType` を示します。

表 6–1 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、第 17 章「サービスプロバイダの管理」の 545 ページの「サービスプロバイダユーザーの委任管理」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」という組み込みの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 (ユーザー、管理者、コンソール、Identity Manager IDE など) にかかわらず、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ロールの作成については、第 17 章「サービスプロバイダの管理」の 545 ページの「サービスプロバイダユーザーの委任管理」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。

ただし、ユーザーに、ワークフローの外部 (および状況によっては内部) にある 1 つ以上のオブジェクトへの特定のアクセス権があるとよい場合も考えられます。そのような場合には、機能および管理する組織を動的に割り当てる規則を使用して、それらのオブジェクトに対するきめ細かい承認を行うことができます。

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。「管理者ロールの作成」のオプションが表示されます (図 6–3)。「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。

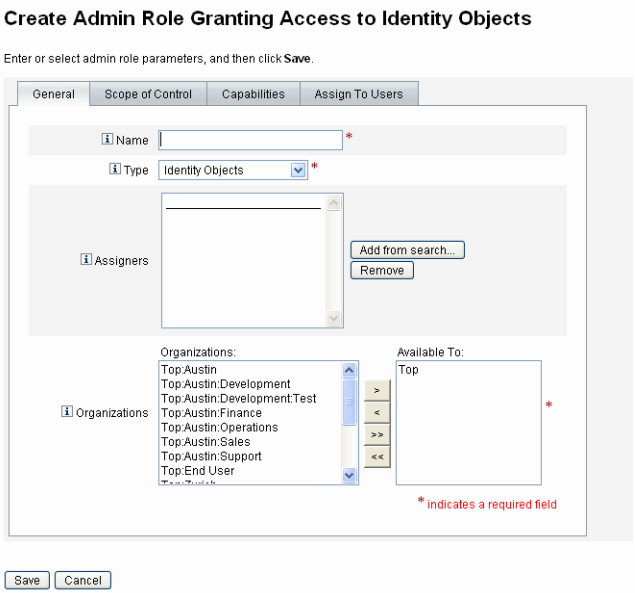


図 6–3　「管理者ロールの作成」ページ:「一般」タブ

「一般」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「一般」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 – 管理者ロールを作成してサービスプロバイダユーザーにアクセス権限を与える方法については、第 17 章「サービスプロバイダの管理」の 545 ページの「サービスプロバイダユーザーの委任管理」を参照してください。

- 「譲渡者」。この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するユーザーを、選択または検索します。選択の対象となるユーザーセットには、「割り当て機能」権を割り当てられた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」。この管理者ロールを使用できる組織を 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。

制御の範囲

Identity Manager では、どのユーザーをエンドユーザーの制御範囲に置くかを管理できます。

「制御の範囲」タブ (図 6–4) を使用して、この組織のメンバーで管理可能な組織を指定するか、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。

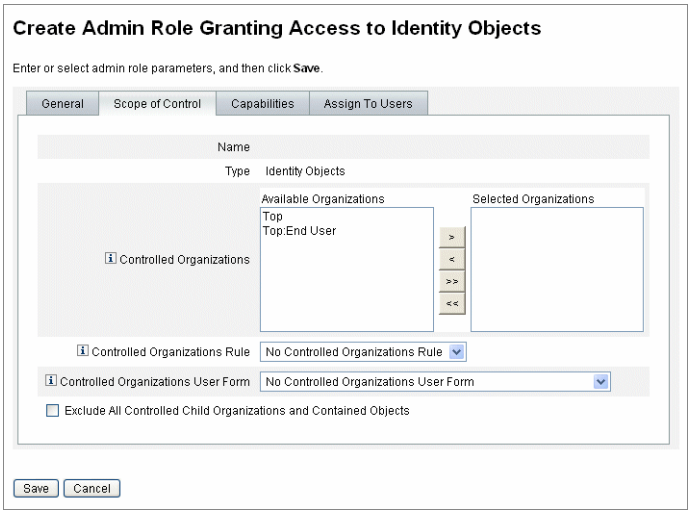


図 6–4 「管理者ロールの作成」:「制御の範囲」

- 「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持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。

  `EndUserControlledOrganizations` 規則を使用して必要なロジックを定義し、組織のニーズに応じて委任に適した一連のユーザーを選択可能にすることができます。

  ユーザーが管理者インタフェースとエンドユーザーインタフェースのどちらにログインしていても、管理者に表示されるユーザーリストの範囲が同じになるようにするには、`EndUserControlledOrganizations` 規則を変更します。

  認証中のユーザーが管理者かどうかを最初にチェックするように規則を変更し、それから次のように設定します。

  - ユーザーが管理者でない場合は、そのユーザー自身の組織など、エンドユーザーによって管理される一連の組織を返します (例: `waveset.organization`)。
  - ユーザーが管理者である場合はどの組織も返さず、管理者であるために割り当てられた組織のみをそのユーザーが管理するようにします。

    たとえば、次のようにします。

```
<Rule protectedFromDelete='true'
      authType='EndUserControlledOrganizationsRule'
```

```
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'>
  <Comments>
    If the user logging in is not an Idm administrator,
    then return the organization that they are a member of.
    Otherwise, return null.
  </Comments>
  <cond>
    <and>
      <isnull><ref>waveset.adminRoles</ref></isnull>
      <isnull><ref>waveset.capabilities</ref></isnull>
      <isnull><ref>waveset.controlledOrganizations</ref></isnull>
    </and>
    <ref>waveset.organization</ref>
  </cond>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>
```

- 動的な組織に所属しているユーザーまたは管理者は、検索結果に返されません。

  ただし、動的な組織のユーザーを返すように規則を作成することもできます。次のサンプル規則で、`Idm Schema Configuration` オブジェクトで定義されている Identity Manager ユーザースキーマ定義に新しい属性を追加し、このオブジェクトをインポートして、Identity Manager サーバーを再起動します。

```
        <IDMAttributeConfigurations>
            ...
            <IDMAttributeConfiguration name='region'
                                       syntax='STRING'
                                       description='region of the country'/>
        </IDMAttributeConfigurations>

        <IDMObjectClassConfigurations>
            ...
            <IDMObjectClassConfiguration name='User'
                                         extends='Principal'
                                           description='User description'>
                ...
                <IDMObjectClassAttributeConfiguration name='region'
                                                      queryable='true'/>
            </IDMObjectClassConfiguration>
        </IDMObjectClassConfigurations>

Next, import the following Identity Manager objects:

<!-- User member rule that will include all users whose region attribute
```

```
matches the region organization display name -->

<Rule name="Region User Member Rule" authType="UserMembersRule">
  <Description>User Member Rule</Description>
  <list>
    <new class='com.waveset.object.AttributeCondition'>
      <s>region</s>
      <s>equals</s>
      <ref>userMemberRuleOrganizationDisplayName</ref>
    </new>
  </list>
  <MemberObjectGroups>
    <ObjectRef type="ObjectGroup" id="#ID#All" name="All"/>
  </MemberObjectGroups>
</Rule>

<!-- North & South Region organizations with user member rule assigned -->

<ObjectGroup id='#ID#North Region' name='North Region'
displayName='North Region'> <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<ObjectGroup id='#ID#South Region' name='South Region'
displayName='South Region'>  <UserMembersRule cacheTimeout='3600000'>
    <ObjectRef type='Rule' name='Region User Member Rule'/>
  </UserMembersRule>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- Organization containing all employees -->

<ObjectGroup id='#ID#Employees' name='Employees' displayName='Employees'>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='Top' id='#ID#Top'/>
  </MemberObjectGroups>
</ObjectGroup>

<!-- End user controlled organization rule that give each user control
of the regional organization they are a member of -->

<Rule protectedFromDelete='true'
```

```
      authType='EndUserControlledOrganizationsRule'
      id='#ID#End User Controlled Organizations'
      name='End User Controlled Organizations'
      primaryObjectClass='Rule'>
  <switch>
    <ref>waveset.attributes.region</ref>
    <case>
      <s>North Region</s>
      <s>North Region</s>
    </case>
    <case>
      <s>South Region</s>
      <s>South Region</s>
    </case>
    <case>
      <s>East Region</s>
      <s>East Region</s>
    </case>
    <case>
      <s>West Region</s>
      <s>West Region</s>
    </case>
  </switch>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Rule>

<!-- 4 employees (2 in North and 2 in South region) -->

<User name='emp1' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee One'/>
  <Attribute name='lastname' type='string' value='One'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp2' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Two'/>
  <Attribute name='lastname' type='string' value='Two'/>
  <Attribute name='region' type='string' value='North Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
```

```
      displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp4' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Four'/>
  <Attribute name='lastname' type='string' value='Four'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>

<User name='emp5' primaryObjectClass='User' asciipassword='1111'>
  <Attribute name='firstname' type='string' value='Employee'/>
  <Attribute name='fullname' type='string' value='Employee Five'/>
  <Attribute name='lastname' type='string' value='Five'/>
  <Attribute name='region' type='string' value='South Region'/>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Employees' name='Employees'
     displayName='Employees'/>
  </MemberObjectGroups>
</User>
```

続いて、Identity Manager エンドユーザーインタフェースを使用して、North 地域のユーザー emp1 としてログインします。「委任」、「新規」の順に選択します。検索を変更します。条件として「が次の文字で始まる」を選択し、値を **emp** に変更して「検索」を選択します。これにより、利用可能なユーザーのリストに emp2 が返されます。

- 「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。

管理者ロールへの機能の割り当て

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。

「機能」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「ユーザーに割り当てる」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。このユーザーフォームが、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。
- 管理者にはユーザーフォームが直接割り当てられていないが、作成または編集しているユーザーがメンバーとなる組織を制御してユーザーフォームを指定する管理者ロールが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い、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 `Top` 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。
- ユーザーフォームが管理者のメンバー組織に割り当てられていない場合は、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。

エンドユーザー組織

エンドユーザー組織は、管理者が、リソースやロールなど特定のオブジェクトをエンドユーザーが使用できるようにする場合に便利です。エンドユーザーはユーザーインタフェースを使用して、指定したオブジェクトを表示したり、状況によっては自分自身に割り当てる (承認プロセスを保留する) ことができます (41 ページの「Identity Manager エンドユーザーインタフェースへのログイン」を参照)。

注 – エンドユーザー組織は、Identity Manager Version 7.1.1 で導入されました。

以前は、ロール、リソース、タスク、その他の Identity Manager 設定オブジェクトへのアクセス権をエンドユーザーに付与するために、管理者は設定オブジェクトを編集して、エンドユーザータスク、エンドユーザーリソース、およびエンドユーザー authType を使用する必要がありました。

今後は、「エンドユーザー」組織を使用して、エンドユーザーに Identity Manager 設定オブジェクトへのアクセス権を付与することをお勧めします。

エンドユーザー組織はすべてのユーザーによって暗黙的に管理され、すべてのユーザーが、タスク、規則、ロール、リソースなどいくつかのオブジェクトのタイプを表示できます。ただし、最初は、この組織にメンバーオブジェクトはありません。

エンドユーザー組織は `Top` 組織のメンバーであり、子組織を持つことはできません。また、エンドユーザー組織は「アカウント」ページの一覧に表示されません。ただし、ロール、管理者ロール、リソース、ポリシー、タスク、その他のオブジェクトを編集する場合は、管理者ユーザーインタフェースを使用して任意のオブジェクトをエンドユーザー組織で使用できるようにすることができます。

エンドユーザーがエンドユーザーインタフェースにログインすると、次の処理が発生します。

- エンドユーザーに `EndUser` 組織 (`ObjectGroup`) の管理権限が付与されます。
- Identity Manager が、組み込みの「エンドユーザーが管理する組織」規則を評価します。これにより、規則によって返される組織名の管理権限が自動的にユーザーに与えられます。この規則は、Identity Manager Version 7.1.1 で追加されました。詳細については、229 ページの「「エンドユーザーが管理する組織」規則」を参照してください。
- エンドユーザーに、`EndUser` 機能で指定されたオブジェクトタイプに対する権限が付与されます。

「エンドユーザーが管理する組織」規則

「エンドユーザーが管理する組織」規則には、入力引数として認証中のユーザーのビューを指定します。Identity Manager では、この規則から、エンドユーザーインタフェースにログイン中のユーザーが管理する 1 つ以上の組織が返されることを想定しています。返される組織が 1 つの場合は文字列、複数の場合はリストになります。

これらのオブジェクトを管理するには、ユーザーに End User Administrator 機能が必要です。End User Administrator 機能が割り当てられたユーザーは、「エンドユーザーが管理する組織」規則の内容を表示および変更できます。これらのユーザーは、EndUser 機能で指定されたオブジェクトタイプの表示と変更も行えます。

End User Administrator 機能は、デフォルトでは Configurator ユーザーに割り当てられます。リストの変更や「エンドユーザーが管理する組織」規則の評価によって返される組織の変更が、ログイン済みのユーザーに動的に反映されることはありません。変更を確認するには、ログアウトしてもう一度ログインしてください。

「エンドユーザーが管理する組織」規則から、無効な組織 (Identity Manager に存在しない組織など) が返された場合、その問題がシステムログに記録されます。問題に対処するには、管理者ユーザーインタフェースにログインして、規則を修正します。

作業項目の管理

Identity Manager のタスクによって発生する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す。

Identity Manager では、保留中のリクエストを集中的に表示して対応できるように、すべての作業項目をインタフェースの「作業項目」領域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、メニューの「作業項目」をクリックします。

注 – 作業項目の所有者が Identity Manager ユーザーインタフェースにログインしたときに、保留中の作業項目 (または委任された作業項目) がある場合は、そのユーザーの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。

- 234 ページの「ユーザーアカウントの承認」
- 492 ページの「アテステーション作業の管理」
- 468 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」領域の「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 6–5 に、作業項目履歴の表示例を示します。

図 6–5　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。メインメニューから「作業項目」を選択し、「自分の作業項目の委任」ページを使用すると、承認リクエストなどの今後発生する作業項目を 1 人以上のユーザー (被委任者) に委任できます。ユーザーを委任先にするために、承認者としての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。

作業項目は、次のようにほかのページからも委任できます。

- 管理者インタフェースでは、「ユーザーの作成」および「ユーザーの編集」ページから作業項目を委任できます (52 ページの「ユーザーページ (作成/編集/表示)」)。「委任」フォームタブをクリックしてください。
- エンドユーザーインタフェースで (38 ページの「Identity Manager エンドユーザーインタフェース」)、「委任」メニュー項目をクリックします。

被委任者は有効な委任期間中、作業項目の所有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、委任先の名前が含まれます。

どのユーザーも、自分の将来の作業項目に対する 1 つ以上の委任を作成できます。ユーザーを編集できる管理者も、そのユーザーに代わって委任を作成できます。ただし、ユーザーが委任できない人に、管理者が委任することはできません。委任に関しては、管理者の管理範囲は、委任を代わってもらうユーザーの管理範囲と同じです。

監査ログエントリ

委任された作業項目が承認または拒否されると、監査ログエントリに委任者の名前が記録されます。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記録されます。

現在の委任の表示

「現在の委任」ページに委任を表示します。

▼ 現在の委任を表示する

1. 管理者インタフェースでメインメニューの「作業項目」をクリックします。
2. 二次的なメニューで「自分の作業項目の委任」をクリックします。
   Identity Manager の「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

「以前の委任」ページに以前の委任を表示します。

▼ 以前の委任を表示する

1. 管理者インタフェースでメインメニューの「作業項目」をクリックします。
2. 二次的なメニューで「自分の作業項目の委任」をクリックします。
   「現在の委任」ページが開きます。
3. 「委任履歴 **(Previous)**」をクリックします。
   「以前の委任」ページが開きます。以前に委任された作業項目を利用して、新しい委任を設定できます。

委任の作成

「新しい委任」ページを使用して委任を作成します。

▼ 委任を作成する

1. 管理者インタフェースでメインメニューの「作業項目」をクリックします。
2. 「自分の作業項目の委任」をクリックします。
   「現在の委任」ページが開きます。

3 「新規」をクリックします。
「新しい委任」ページが開きます。

4 次のようにフォームを設定します。

a. 「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。すべての作業項目を委任するには、「すべての作業項目タイプ」を選択します。

ロールタイプ、組織、またはリソースの作業項目を委任する場合は、矢印を使って「利用可能」列から「選択」列に項目を移動すると、指定した特定のロール、組織、またはリソースによってこの委任が定義されます。

b. 「作業項目の委任先」。

次のオプションのいずれかを選択します。

- 「選択されたユーザー」。自分の制御の範囲内で、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いずれかが、この作業項目をさらに別のユーザーに委任した場合、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」領域で 1 人以上のユーザーを選択。もう 1 つの方法として、「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。リストから委任先を削除するには、その委任先を選択し、「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)。
  - 「作業項目委任規則」。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。

c. 「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、選択した日付の午前 **12** 時 **1** 分に開始します。

d. 「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** 時 **59** 分に終了します。

注 – 開始日と終了日を同じにして、作業項目を 1 日だけ委任することもできます。

---

e. 「**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。

注 – 委任を設定したあと、有効な委任期間中に作成されたすべての作業項目は、委任先のリストに追加されます。委任を終了するか委任期間が満了すると、委任された作業項目は委任者のリストに戻ります。そのため、委任者のリストで作業項目が重複する可能性があります。ただし、一方の作業項目を承認または却下すると、重複していた作業項目はリストから自動的に削除されます。

削除されたユーザーへの委任

保留中の作業項目を所有しているユーザーを削除すると、Identity Manager は次の処理を行います。

- 保留中の作業項目が委任されていて、委任者がまだ削除されていない場合、保留中の作業項目は委任者に返されます。
- 保留中の作業項目が委任されていない場合、または保留中の作業項目が委任済みであるが、委任者が削除されている場合は、ユーザーの保留中の作業項目が解決されるか別のユーザーに転送されるまで、削除は失敗します。

委任の終了

「現在の委任」ページで 1 つ以上の委任を終了します。

▼ 1 つ以上の委任を終了する

1. 管理者インタフェースでメインメニューの「作業項目」をクリックします。
2. 二次的なメニューで「自分の作業項目の委任」をクリックします。
   「現在の委任」ページが開きます。
3. 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。
   Identity Manager は選択した委任設定を削除し、選択されているタイプのすべての委任済み作業項目を保留中の作業項目のリストに戻します。

ユーザーアカウントの承認

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、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。

加えて、変更承認が有効にされている状態でロールが変更された場合、変更承認作業項目が、指定されたロール所有者に送信されます。

Identity Managerは、「ロール定義」による変更承認をサポートします。管理者がロール定義を変更すると、指定されたロール所有者からの変更承認が必要になります。変更を実行するには、ロール所有者が作業項目を承認する必要があります。

注 –

- Identity Managerでは、デジタル署名された承認を設定できます。手順については、237 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。
- Identity Managerに慣れていない管理者は、「承認」の概念と「アテステーション」の概念を混同しないように注意してください。意味は同じように思えますが、承認とアテステーションでは発生するコンテキストが異なります。

  承認は、新しいユーザーアカウントの検証に関連があります。ユーザーがIdentity Managerに追加されると、その新しいアカウントの認可を検証するために、1つ以上の承認が必要になります。

  アテステーションは、既存のユーザーが適切なリソースに対する適切な特権のみを持っていることの検証に関連があります。定期的アクセスレビュープロセスの一環として、Identity Managerユーザー (アテスター) が、別のユーザーのアカウントの詳細 (つまり、そのユーザーの割り当て済みリソース) が有効かつ適切であることを保証するように求められる場合があります。このプロセスをアテステーションといいます。

アカウント承認者の設定

組織、ロール、およびリソースを承認するアカウント承認者の設定は省略可能ですが、推奨されています。アカウントの作成では、承認者を設定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拒否した場合、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、複数の承認者を設定して、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。承認を必要とするように、このプロセスをカスタマイズすることもできます。

Identity Manager IDEを使用すると、承認の流れを変更したり、アカウントの削除や更新を取得して、ワークフローをカスタマイズすることができます。

Identity Manager IDE の詳細については、https://identitymanager.dev.java.net を参照してください。作業項目の詳細と、承認ワークフローの変更例については、『Sun Identity Manager Deployment Reference』の第 1 章「Workflow」を参照してください。

Identity Manager 承認者は、承認リクエストを承認または拒否できます。

管理者は、Identity Manager インタフェースの「作業項目」領域で、保留中の承認を表示および管理することができます。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」タブをクリックします。

承認の署名

デジタル署名を使用して作業項目を承認する場合は、237 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。

▼ 承認を署名する

1 **Identity Manager** 管理者インタフェースで、「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 からアプレットを信頼するかどうか尋ねられます。

5 「常時」をクリックします。
承認の概要が日付付きで表示されます。

6 キーストアの場所を入力するか、「参照」をクリックして指定します。この場所は、署名付き承認の設定 **(****239** ページの「**PKCS12** を使用した署名付き承認のサーバー側設定を有効にする」の手順 **10m)** で設定します。

7 キーストアのパスワードを入力します。このパスワードは、署名付き承認の設定 **(****239** ページの「**PKCS12** を使用した署名付き承認のサーバー側設定を有効にする」の手順 **10l)** で設定します。

8 「署名」をクリックしてリクエストを承認します。

参考 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。

- 承認 (変更承認を含む)
- 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、& Product_IDMgr; に署名付き承認の証明書と CRL を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。

▼ 署名付き承認に関するサーバー側の設定を有効にする

1 システム設定オブジェクトを開いて、`security.nonrepudiation.signedApprovals=true` と設定します。

システム設定オブジェクトを編集する方法については、116 ページの「Identity Manager 設定オブジェクトの編集」を参照してください。

PKCS11 を使用している場合は、`security.nonrepudiation.defaultKeystoreType=PKCS11` も設定する必要があります。

カスタム PKCS11 キープロバイダを使用している場合は、さらに `security.nonrepudiation.defaultPKCS11KeyProvider=<プロバイダ名>` も設定する必要があります。

注 – カスタムプロバイダを記述する必要がある状況の詳細については、REF キットの次の項目を参照してください。

```
com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)
REF/transactionsigner/SamplePKCS11KeyProvider
```

REF (Resource Extension Facility) キットは、製品の CD の `/REF` ディレクトリまたはインストールイメージにあります。

---

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で、「セキュリティー」を選択し、「証明書」を選択します。「証明書」ページが表示されます。

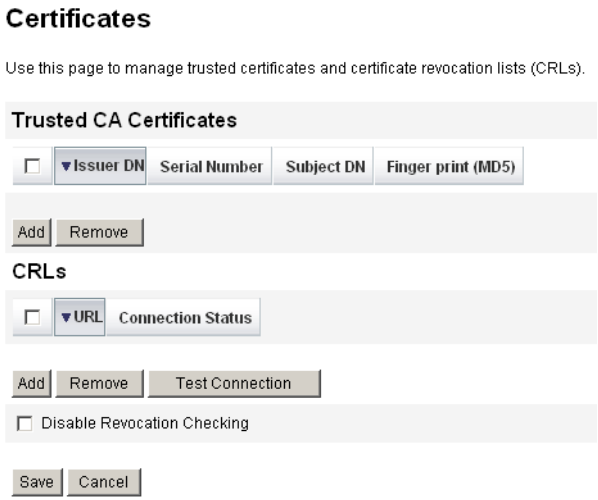


図 6–6 「証明書」ページ

b. 「信頼できる認証局証明書」領域で、「追加」をクリックします。「証明書のインポート」ページが表示されます。

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。

選択した証明書が、信頼できる証明書のリストに表示されます。

4 次の手順で、**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**」領域で、「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**/`ts2.jar` に署名します。

注 – 詳細については、`http://java.sun.com/j2se/1.5.0/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 `ts2.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。

▼ PKCS12 を使用した署名付き承認のサーバー側設定を有効にする

PKCS12 を使用した署名付き承認のための設定情報は、次のとおりです。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。

始める前に Identity Manager では、JRE 1.5 以上が必要になりました。

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」を選択し、**mmc** と入力して **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」の順に選択します。

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」の順に選択します。

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」の順に選択します。

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. 証明書の場所を指定します。

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。

▼ PKCS11 を使用した署名付き承認のクライアント側設定を有効にする

署名付き承認に PCCS11 を使用している場合は、次の操作を行います。

- **REF** キットにある次のリソースを参照して、設定情報を確認します。

  `com.sun.idm.ui.web.applet.transactionsigner.DefaultPKCS11KeyProvider (Javadoc)`
  `REF/transactionsigner/SamplePKCS11KeyProvider`

  REF (Resource Extension Facility) キットは、製品の CD の `/REF` ディレクトリまたはインストールイメージにあります。

トランザクション署名の表示

この節では、Identity Manager 監査ログレポートで、トランザクション署名を表示する方法について説明します。

▼ トランザクション署名を表示する

1. **Identity Manager** 管理者インタフェースで、「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、タイトルを入力します (「承認」など)。
4. 「組織」選択領域で、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、トランザクション署名情報を表示します。
表示されるトランザクション署名情報は、次のとおりです。

- 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

XMLDSIG 形式の署名付き承認の設定

Identity Manager では、RFC 3161 準拠のデジタルタイムスタンプを含む XMLDSIG 形式の署名付き承認を、Identity Manager 承認プロセスに追加できます。XMLDSIG 署名付き承認を使用するように Identity Manager を設定する場合、監査ログで承認を確認しないかぎり、承認者が認識できる変更はありません。監査ログレコードに格納される署名付き承認の形式だけが変更されます。

これまでの Identity Manager の署名付き承認と同様、クライアントマシンでアプレットが起動され、承認者に対して署名のための承認情報が表示されます。承認者は承認の署名に使用するキーストアとキーを選択します。

承認者が承認に署名すると、承認データを含む XMLDSIG ドキュメントが作成されます。このドキュメントは、XMLDSIG 署名付きドキュメントを検証するサーバーに返されます。処理が成功し、RFC 3161 デジタルタイムスタンプが設定されている場合は、このドキュメントに対してデジタルタイムスタンプも生成されます。タイムスタンプ証明局 (TSA) から取得したタイムスタンプのエラーがチェックされ、証明書の有効性が確認されます。問題がなければ、最後に Identity Manager は監査ログレコードを生成し、XMLDSIG 形式の署名付き証明書オブジェクトを XML のブロブ列に格納します。

承認データの形式

XMLDSIG 形式の証明書オブジェクトは、次のような形式になります。

```
<XMLSignedData signedContent="...base64 transaction text ...">
   <XMLSignature>
      <TSATimestamp>
         ...The base64 encoded PKCS7 timestamp token returned by the TSA...
      </TSATimestamp
      <Signature>
        <SignedInfo>...XMLDSIG stuff...</SignedInfo>
        <SignatureValue>...base64 signature value</SignatureValue>
        <KeyInfo>...cert info for signer</KeyInfo>
      </Signature>
```

```
   </XMLSignature>
</XMLSignedData>
```

次の点に注意してください。

- base64 承認データは、アプレットで承認者に表示される実際の承認データテキストで構成され、base64 形式でエンコードされます。
- <TSATimestamp> 要素には、base64 でエンコードされた、タイムスタンプ証明局 (TSA) からの PKCS7 タイムスタンプ応答が含まれます。
- <Signature> 全体で、XMLDSIG 署名データを構成します。

この XMLDSIG ドキュメントは、監査ログ承認レコードの XML 列に格納されます。

インストールと設定

XMLDSIG 署名付き承認を使用するためのインストールと設定の要件は、237 ページの「署名付き承認に関するサーバー側の設定を有効にする」 で説明した要件と同じです。ただし、追加の手順が 1 つだけあります。ts2.jar ファイルへの署名に加えて、xmlsec-1.4.2.jar ファイルにも署名が必要です。

承認の設定

システム設定属性を使用して、次の操作を実行できます。

- SignedData 形式または XMLSignedData 形式を選択できます。一度に設定できるのはどちらか一方の形式だけです。管理者は必要に応じて、この設定を変更できます。
- 設定された RFC 3161 タイムスタンプ証明局 (TSA) から取得した、デジタルタイムスタンプを含めることができます。
- このタイムスタンプを取得する URL を、HTTP のみで指定できます。

これらの属性を編集するには、Identity Manager デバッグページを使用して、システム設定オブジェクトを編集します。これらの設定はすべて、ほかの署名付き承認属性と一緒に security.nonrepudiation 以下で指定します。

XMLDSIG 属性には次のものがあります。

- security.nonrepudiation.useXmlDigitalSignatures は、XMLDSIG 署名を有効にするブール型の値です。
- security.nonrepudiation.timestampXmlDigitalSignatures は、XMLDSIG 署名に RFC 3161 デジタルタイムスタンプを含めるブール型の値です。
- security.nonrepudiation.timestampServerURL は、タイムスタンプを取得する HTTP ベースの TSA の URL を指定する文字列値です。

注 –

- これらの属性を有効にするには、既存の `useSignedApprovals` 属性を **`true`** に設定する必要があります。
- Identity Manager は、一般的なプロビジョニングリクエストで、1 つの承認または複数の署名付き承認に対して複数の署名をサポートしません。

◆ ◆ ◆ 第 7 章

7 データの読み込みと同期

この章では、Identity Manager でのデータの読み込みと同期機能の説明および手順を示します。また、Identity Manager のデータ同期ツール (検出、調整、および同期) を使用して、データを最新の状態に維持する方法も説明します。

この章の情報は、次のように構成されています。

- 245 ページの「データ同期ツール: 最適なツールの選択」
- 246 ページの「アカウント検出機能」
- 251 ページの「アカウント調整」
- 262 ページの「Active Sync アダプタ」

Identity Manager でのデータの読み込みと同期の動作については、『Sun Identity Manager Deployment Guide』の第 3 章「Data Loading and Synchronization」を参照してください。

データ同期ツール: 最適なツールの選択

Identity Manager には、アカウントデータのインポートと同期に使用できるいくつかのツールがあります。表 7–1 を参考にして、タスクごとに正しいツールを選択してください。

注 – Identity Manager でのデータの読み込みと同期の動作については、『Sun Identity Manager Deployment Guide』の第 3 章「Data Loading and Synchronization」を参照してください。

表 7–1 各タスクで使用するデータ同期ツール

実行するタスク	使用する機能
読み込みの前に表示確認を行わずに、最初からリソースアカウントを Identity Manager に読み込む	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 に読み込む。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 に読み込む。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、または読み込む	Active Sync アダプタを使用した同期 (複数リソースの実装)

アカウント検出機能

Identity Manager のアカウント検出機能を使用すると、配備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、CSV 形式または XML 形式でファイルに抽出します。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。CSV 形式または XML 形式のファイルから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。先に述べた 2 つの検出機能を組み合わせて、リソースからアカウントを抽出し、直接 Identity Manager に読み込みます。

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。

注 – この節では、Identity Manager の検出機能を使用する方法について説明します。データの読み込みと同期の詳細については、『Sun Identity Manager Deployment Guide』の第 3 章「Data Loading and Synchronization」を参照してください。

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。抽出したデータを確認して変更したあと、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

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** ファイルに抽出できます。また、コンマ区切り値 **(CSV)** 形式になったアカウント属性を使用してテキストファイルに抽出することもできます。

4 「ダウンロード」をクリックします。「ファイルのダウンロード」ダイアログが表示され、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

この機能を使用すると、Identity Manager を通してリソースから抽出されたリソースアカウント、または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 に読み込むことができます。Identity Manager の「ファイルへ抽出」機能で作成されるファイルは 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、コンマ区切り (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、コンマで区切ってリストします。
- 2 行目以降。1 行目で定義した各属性の値を、コ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、隣接するコンマでそのフィールドを表します。

  たとえば、CSV ファイルの最初の 3 行は次のようになります。

```
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
```

  この例では、Jane Doe (2 番目のユーザー) には部署 (Department) の値がありません。値がない場合は、隣接するコンマ (,,) で表します。

▼ アカウントを読み込む

1 管理者インタフェースで、メニューから「アカウント」をクリックし、「ファイルから読み込み」をクリックします。
「アカウントのファイルからの読み込み」ページが表示されます。

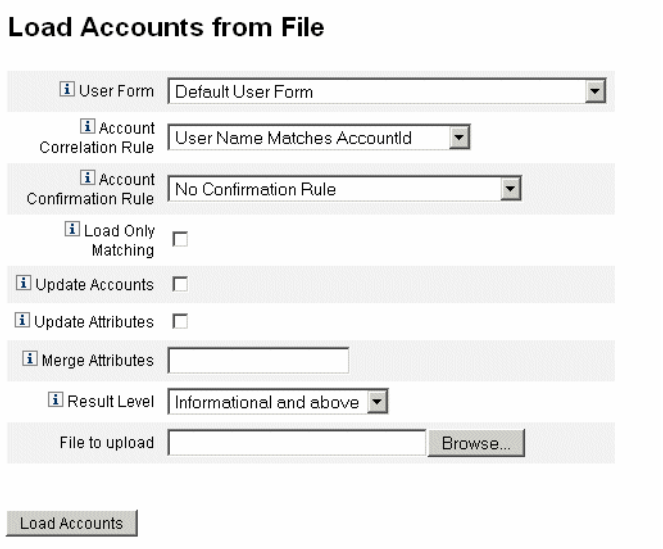


図 7–1 ファイルから読み込み

2 このページを使用して、必要なアカウントの読み込みオプションを指定します。
このページには次のオプションがあります。

- 「ユーザーフォーム」。読み込み結果によって Identity Manager ユーザーが作成される場合に、ユーザーフォームは組織、ロール、リソース、およびその他の属性を割り当てます。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できる Identity Manager ユーザーを検索する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、相関規則で選択され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に対して、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 ユーザーに一致するアカウントだけを Identity Manager に読み込みます。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ます。
- 「属性値のマージ」。1 つ以上の属性名をコンマで区切って入力し、その値を上書きせずに (重複を除いて) 結合します。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。
  - 「すべて」。すべてのアカウントで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。

3 「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ない場合、読み込みを正しく実行するには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。

  「ファイルから読み込み」画面で利用可能なフィールドとオプションについては、247 ページの「CSV ファイル形式について」を参照してください。

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検出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。発生したエラーの数が `maxParseErrors` に達すると、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、アカウントを直接抽出して Identity Manager にインポートします。

▼ アカウントをインポートする

1 管理者インタフェースで、メニューから「アカウント」をクリックし、「リソースから読み込み」をクリックします。

「リソースからのアカウントの読み込み」ページが表示されます。

2 「リソースからのアカウントの読み込み」ページで、読み込みオプションを指定します。

このページの読み込みオプションは、「ファイルから読み込み」ページ (247 ページの「ファイルから読み込み」) のオプションと同じです。

アカウント調整

調整機能を使用すると、Identity Manager 内のリソースアカウントとリソース上に実際に存在するアカウントを定期的に比較できます。調整により、アカウントデータが関連付けられ、違いが強調表示されます。

注 – この節では、管理者インタフェースを使用して調整タスクを実行する方法について説明します。調整の詳細については、『Sun Identity Manager Deployment Guide』の第 3 章「Data Loading and Synchronization」を参照してください。

調整の概要

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 の調整機能には、「リソース」領域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。

注 – 調整は、Identity Manager の調停コンポーネントによって実行されます。調停サーバーの設定については、マニュアルを参照してください。

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

1. 管理者インタフェースで、メニューから「リソース」をクリックします。
2. 「リソースリスト」からリソースを選択します。
3. 「リソースアクション」リストから「調整ポリシーの編集」を選択します。

   「調整ポリシーの編集」ページが表示されます。このページでは、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。速度が低下しますが、完全性を最適化します。
     - 差分調整。完全性がいくらか低下しますが、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。
     - 指示されたスケジュールを上位レベルのポリシーから継承する場合は、「デフォルトポリシーを継承」オプションを選択します。
     - スケジュールを指定する場合は、「デフォルトポリシーを継承」オプションの選択を解除します。繰り返しのスケジュールを確立するために提供されたフィールドを使用するか、調整スケジュールに対するカスタム調整を作成する場合は、タスクスケジュールの繰り返し規則を使用します。タスクスケジュール繰り返し規則の作成については、260 ページの「タスクスケジュール繰り返し規則の使用」を参照してください。
   - 「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。
     - 上位レベルのポリシーからスケジュールを継承する場合は、「デフォルトポリシーを継承」オプションを選択します。
     - スケジュールを指定する場合は、「デフォルトポリシーを継承」オプションの選択を解除します。繰り返しのスケジュールを確立するために提供されたフィールドを使用するか、調整スケジュールに対するカスタム調整を作成する

場合は、タスクスケジュールの繰り返し規則を使用します。タスクスケジュール繰り返し規則の作成については、260 ページの「タスクスケジュール繰り返し規則の使用」を参照してください。

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 を通さずに) 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」で指定した属性に対する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できる Identity Manager ユーザーを検索する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、相関規則で選択され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に対して、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す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許可されているアクションのみを実行できます。応答は管理者に関連付けられたユーザーフォームを必要に応じて使用します。

  「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、調整結果は参照できますが、応答アクションや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、いくつかの状況が認識されます。状況は次のとおりです。「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。

    「CONFIRMED」と認識される場合、次の条件が true となっています。
    - Identity Manager で、当該アカウントの存在が予想される。

- 当該アカウントがリソースに存在する。

- COLLISION。2 人以上の Identity Manager ユーザーが、1 つのリソースで同じアカウントを割り当てられています。
- DELETED。予想されるアカウントは存在しません。

  「DELETED」と認識される場合、次の条件が true となっています。

  - Identity Manager で、当該アカウントの存在が予想される。
  - 当該アカウントがリソースに存在しない。
- FOUND。調整プロセスは、割り当てられたリソースで一致するアカウントを発見しました。

  「FOUND」と認識される場合、次の条件が true となっています。

  - Identity Manager で当該アカウントは存在するとも存在しないとも予想される。(リソースがユーザーに割り当て済みだがまだプロビジョニングされていない場合は、アカウントはリソースに存在することもしないこともある。
  - 当該アカウントがリソースに存在する。
- 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。

  「MISSING」と認識される場合、次の条件が true となっています。

  - Identity Manager で当該アカウントは存在するとも存在しないとも予想される。(リソースがユーザーに割り当て済みだがまだプロビジョニングされていない場合は、アカウントはリソースに存在することもしないこともある。
  - 当該アカウントがリソースに存在しない。
- 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で、一致するアカウントを発見しました。

  「UNASSIGNED」と認識される場合、次の条件が true となっています。

  - Identity Manager で当該アカウントの存在が予想されない。(リソースがユーザーに割り当てられていない場合、Identity Manager ではアカウントが存在しないと予想される)
  - 当該アカウントがリソースに存在する。
- UNMATCHED。リソースアカウントはどのユーザーとも一致しません。
- DISPUTED。リソースアカウントは複数のユーザーと一致しています。

  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ユーザーの作成」。リソースアカウント属性に対してユーザーフォームを実行し、新しいユーザーを作成します。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。

- 「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、存在しないユーザーアカウントを作成し直します。
- 「リソースアカウントの削除」または「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または無効にします。
- 「リソースアカウントをユーザーにリンク」および「「ユーザーからリソースアカウントへのリンクの解除」。ユーザーに対するリソースアカウントの割り当てを追加または削除します。フォーム処理は実行されません。
- 「何もしない」。このオプションは、調整で修復を実行しない場合に選択します。

  調整で見つかったどのアカウント状況も手動で修正できます。メニューで、「リソース」、「アカウントインデックスの検査」の順にクリックします。そこから、調整済みのすべてのアカウントに対して記録された状況を閲覧できます。アカウントを右クリックすると、有効な修復オプションの一覧が表示されます。詳細については、259 ページの「アカウントインデックスの検査」を参照してください。

- 「調整前ワークフロー」。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、調整を設定できます。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」。リソースアカウントの状況に応答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、調整を設定できます。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、調整を設定できます。調整が実行するワークフローを選択してください。ワークフローを実行しない場合は、「ワークフローを実行しない」を選択します。
- 「状況を説明する」。このオプションを有効にすると、アカウントの状況がどのように分類されたかを説明する追加情報が記録されます。デフォルトでは、このオプションは無効になっています。説明を記録することで、調整プロセスの実行時間が長くなります。
- 「エラー制限」。このオプションを有効にすると、処理中に指定数のエラーが発生した場合に調整が自動的に終了します。0 を設定すると、エラー数の制限がなくなります。「デフォルトポリシーを継承」オプションの選択を解除すると、「許容最大エラー数」フィールドが表示され、値を入力できます。
- 「ネイティブに削除されたアカウントの最大数」。このオプションは、リソース上の見つからないアカウントの数を評価し、しきい値を超過した場合に調停サーバーがそれらをリンク解除するのを防ぐための安全措置です。

この機能を有効にするには、「デフォルトポリシーを継承」チェックボックスをオフにし、「ネイティブに削除されたアカウントの最大許容数」フィールドにパーセンテージを指定します。しきい値は 0 ～ 100 の全パーセンテージに設定する必要があります。(0 に設定すると、この機能はオフになります。)

削除されたアカウントのパーセンテージがしきい値を超えると、調整は存在しないアカウントに関係しないすべての処理を続行し、エラーありで終了します。

「保存」をクリックして、ポリシーの変更を保存します。

調整の開始

この節では、調整タスクを開始する次の 2 つの方法を説明します。

- スケジュールした間隔で調整を実行する
- ただちに調整を実行する

▼ 調整を定期的に実行する

1. 252 ページの「調整ポリシーの編集」の手順に従って、「調整ポリシーの編集」ページを開きます。
2. 調整のスケジュールパラメータを指定します。
   ポリシーに設定されたパラメータに従って調整が実行されます。

▼ ただちに調整を実行する

1. 管理者インタフェースで、メニューから「リソース」をクリックします。
2. 「リソースリスト」からリソースを選択します。
3. 「リソースアクション」リストからオプションを選択します。
   このページには次のオプションがあります。
   - ただちに完全調整
   - ただちに差分調整

     ポリシーに設定されたパラメータに従って調整が実行されます。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。

▼ 調整をキャンセルする

1 管理者インタフェースで、メニューから「リソース」をクリックします。

2 「リソースリスト」から、調整をキャンセルするリソースを選択します。

3 「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

調整ステータスを表示する主な方法は2つあります。詳細な調整ステータスを表示する場合は、特定のリソースの調整結果の概要ページを開きます。調整ステータスの一部を「リソースリスト」から直接確認することもできます。

▼ 詳細な調整ステータスを表示する

調整結果の概要ページを使用して、詳細な調整ステータスを表示します。

1 管理者インタフェースで、メニューから「リソース」をクリックします。

2 「リソースリスト」で、調整ステータスを表示するリソースを選択します。

3 「リソースアクション」リストから「調整ステータスの表示」を選択します。
そのリソースの調整結果の概要ページが開きます。

▼ 「リソースリスト」に調整ステータスを表示する

調整スタータスは、「リソースリスト」から確認することもできます。

1 管理者インタフェースを開きます。

2 メインメニューの「リソース」をクリックします。
「ステータス」列に、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」。調整は無効です。
- 「失敗」。最後に実行された調整は正常に完了していません。
- 「成功」。最後に実行された調整は正常に完了しました。
- 「エラーありで完了」。最後に実行された調整は完了しましたが、エラーが発生しました。

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ません。

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には、Identity Manager が認識している各リソースアカウントの最新の状態が記録されています。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を検索する

アカウントインデックスを検索して、リソースアカウントの最後の既知の状態を表示します。

1. 管理者インタフェースで、メニューから「リソース」をクリックします。
2. 「リソースリスト」から、アカウントインデックスを検索するリソースを選択します。
3. 「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。
   「アカウントインデックスの検索」ページが開きます。
4. 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。
   - 「リソースアカウント名」。このオプションを選択する場合は、「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する場合は、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する場合は、「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する場合は、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。

5 「検索」をクリックし、検索パラメータに従ってアカウントを検索します。検索結果を制限するには、オプションで、「結果表示を次の件数に限定」フィールドに数を指定します。デフォルトでは、最初に見つかった**1000**個のアカウントに制限されます。

「クエリーのリセット」をクリックしてページをクリアし、新しい項目を選択します。

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したり、ユーザーアカウントをユーザーごとに調整することもできます。

▼ アカウントインデックスを検査する

1 管理者インタフェースで、メニューから「リソース」をクリックします。

2 二次的なメニューで「アカウントインデックスの検査」をクリックします。

「アカウントインデックスの検査」ページが開きます。

Identity Managerが認識するすべてのリソースアカウントが、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表形式で表示されます。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。リソースの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が認識してい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。アカウントを右クリックすると、有効な修復オプションの一覧が表示されます。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ユーザーと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 が認識している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。

タスクスケジュール繰り返し規則の使用

タスクスケジュール繰り返し規則を使用して、調整スケジュールを設定できます。たとえば、土曜日にスケジュールされている調整を次の月曜日に適用するには、タスクスケジュール繰り返し規則を使用します。

タスクスケジュール繰り返し規則は、完全調整と差分調整の両方のスケジュール設定に使用できます。

タスクスケジュール繰り返し規則を選択する方法については、252 ページの「調整ポリシーの編集」を参照してください。

調整実行時間のスケジュール方法

調停サーバーコンポーネントは、調整ジョブが完了すると、次の実行スケジュールをチェックします。

調停サーバーは、最初にデフォルトスケジュールをチェックして次の実行時間を取得します。次に調停サーバーは、適用可能なすべてのタスクスケジュール繰り返し規則を実行し、スケジュールの調整が必要かどうか確認します。調整が必要な場合、その調整のデフォルトスケジュールより規則のスケジュールが優先されます。

注 – タスクスケジュール繰り返し規則でデフォルトスケジュールを上書きすることはできません。ジョブごとの開始時間をスケジュールする際に「優先される」だけです。

▼ サンプルの「**Accept All Dates**」規則を表示する

この節では、組み込みの「Accept All Dates」サンプル規則について説明します。

1 テキストエディタで、**Identity Manager** の `sample` ディレクトリにある `ReconRules.xml` を開きます。

2 SCHEDULING_RULE_ACCEPT_ALL_DATES という名前の規則を検索します。

規則を「調整ポリシーの編集」ページの「タスクスケジュール繰り返し規則」ドロップダウンメニューに表示するには、subtype 属性を SUBTYPE_TASKSCHEDULE_REPETITION_RULE: に設定する必要があります。

```
<Rule subtype='SUBTYPE_TASKSCHEDULE_REPETITION_RULE'
name='SCHEDULING_RULE_ACCEPT_ALL_DATES'>
```

前の説明にもあるとおり、タスクスケジュール繰り返し規則でデフォルトの調整スケジュールを変更できます。

変数 calculatedNextDate には、デフォルトの方法で計算された次の日付を設定することも、別の日付を返すこともできます。サンプル規則に記述されているように、calculatedNextDate は無条件にデフォルトの日付を受け付けます。次の箇所を参照してください。

```
<RuleArgument name='calculatedNextDate'/>
<block>
  <ref>calculatedNextDate</ref>
</block>
```

カスタムスケジュールを作成するには、<block> 要素の間にある規則のロジックを書き換えます。たとえば、調整開始時間を土曜日の午前 10:00 に変更するには、次のような JavaScript を <block> 要素の間に記述します。

```
<block>
  <script>
     var calculatedNextDate = env.get('calculatedNextDate');

    // Test to see if this task is scheduled for a Saturday
    // (Note that 6 is used to denote Saturday in JavaScript)
    if(calculatedNextDate.getDay() == 6) {
      // If so, set the time to 10:00:00
      calculatedNextDate.setHours(10);
      calculatedNextDate.setMinutes(0);
      calculatedNextDate.setSeconds(0);
    }
    // Return the modified date
    calculatedNextDate;
  </script>
</block>
```

260 ページの「サンプルの「Accept All Dates」規則を表示する」 では、calculatedNextDate は最初にデフォルトのスケジュール時刻に設定されています。次回のスケジュールされた実行日が土曜の場合、規則は調整を 10:00 に開始するようにスケジュールします。次回のスケジュールされた実行日が土曜以外の場合、260 ページの「サンプルの「Accept All Dates」規則を表示する」は時間の調整を行わずに calculatedNextDate を返し、デフォルトのスケジュールが使用されます。

Identity Manager で使用するカスタム規則の作成については、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。

Active Sync アダプタ

Identity Manager の Active Sync 機能を使用すると、「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、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。

リソースの同期ポリシーの入力フォームを適切なターゲットオブジェクトタイプに対して指定することにより、リソース属性変更を Identity Manager に伝達する方法を設定できます。

注 – この章では、管理者インタフェースを使用して Active Sync タスクを実行する方法について説明します。Active Sync の詳細については、『Sun Identity Manager Deployment Guide』の第 3 章「Data Loading and Synchronization」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。

▼ 同期を編集または設定する

各リソースには固有の同期ポリシーがあります。次の手順を使用して、同期ポリシーを設定または編集します。

1. 管理者インタフェースで、メニューから「リソース」をクリックします。
2. 「リソースリスト」から、同期を設定するリソースを選択します。
3. 「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。

   そのリソースの「同期ポリシーの編集」ページが開きます。

   「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 ユーザーまたはサービスプロバイダ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 の実装で同期ポリシー (オブジェクトタイプとしてサービスプロバイダ 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 17 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」。このセクションを使用して、起動方法とポーリングスケジュールを指定します。

  次の起動タイプを指定できます。

  - 「自動」または「フェイルオーバー付き自動」。アイデンティティーシステムの起動時にこのソースを開始します。
  - 「手動」。管理者がこのソースを開始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)。

    注 – 起動方法またはポーリングスケジュールを変更した場合は、サーバーを再起動して、変更を有効にする必要があります。

    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。

    たとえば、次のようにします。

    - 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。(この機能は非推奨です。
- 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。
- 「一般的な設定」。データ同期アクティビティーの一般的な設定を指定します。

  次の設定があります。

  - 「プロキシ管理者」。更新を処理する管理者を選択します。すべてのアクションは、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」 (省略可能)。データの同期処理中に使用する規則を選択します。

    次の設定を指定できます。

    - 「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。
    - 「プロセス解決規則」。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。
- 「ログの設定」。ログオプションの値を指定します。

  ログオプションは次の設定で構成されます。

  - 「ログアーカイブの最大数」。0 より大きい値を指定すると、最新の N 個のログファイルを保持します。0 を指定した場合は、1 つのログファイルが繰り返し利用されます。-1 を指定すると、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」。この期間が経過すると、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は、この期間が経過してもアーカイブは行われず、アクティブログが切り捨てられて再使用されます。この期間条件は、「ログファイルの最大サイズ」に指定した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単位で入力します。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は、この期間が経過してもアーカイブは行われず、アクティブログが切り捨てられて再使用されます。このサイズ条件は、「アクティブログの最大有効期間」に指定した期間条件とは別に評価されます。
  - 「ログレベル」。ログのレベルを指定します。

    次のログレベルを指定できます。

    - 0。ログを記録しない
    - 1。エラー
    - 2。情報
    - 3。詳細
    - 4。デバッグ

4 「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。

Active Sync 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。

▼ 同期を停止する

1 「同期ポリシーの編集」ページを開きます。手順については、262 ページの「同期を編集または設定する」を参照してください。

2 「スケジューリングの設定」で「起動タイプ」から「無効」を選択します。
サービスプロバイダユーザーでは、「同期の有効化」オプションを選択解除します。

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。

3 「保存」をクリックします。
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。

Active Sync 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、Active Sync 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、Active Sync アダプタのパフォーマンスをチューニングします。

- 266 ページの「ポーリング間隔の変更」
- 267 ページの「アダプタを実行するホストの指定」
- 267 ページの「開始と停止」
- 268 ページの「アダプタログ」

Active Sync アダプタは、リソースリストを通じて管理します。Active Sync 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、Active Sync 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み、毎回 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ことを検討してください。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` ファイルの `sources.hosts` プロパティーを編集する必要があります。

次のいずれかの設定を指定します。

- `sources.hosts=`*hostname1,hostname2,hostname3* を設定します。この設定により、Active Sync 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、Identity Manager のサーバーのリスト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。

- `sources.hosts=localhost` を設定します。この設定では、アダプタは、そのリソースに対して Active Sync 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。

メモリーと CPU サイクルを多く必要とする Active Sync 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

Active Sync 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。Active Sync アダプタを起動または停止するには、Active Sync 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、214 ページの「機能のカテゴリ」を参照してください。

アダプタを自動に設定すると、アプリケーションサーバーを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されます。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。各ユーザータイプ (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は、アダプタが停止しているときにのみ実行してください。通常は、アダプタログを削除する前にログファイルをコピーしてアーカイブしてください。

◆ ◆ ◆ 第 8 章

8 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 のレポートタイプ、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、次のトピックで構成されています。

- 270 ページの「レポートの操作」
- 276 ページの「Identity Manager レポート」
- 285 ページの「監査レポート」
- 285 ページの「グラフの操作」
- 290 ページの「ダッシュボードの操作」
- 293 ページの「システムの監視」
- 294 ページの「リスク分析」

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見なされます。このため、レポートの操作は Identity Manager 管理者インタフェースの次の 2 つの領域で行います。

- 「レポート」(レポートの実行)。「レポートの実行」領域では、レポートの定義、実行、削除、およびダウンロードを行います。レポートを定義、実行、削除、およびダウンロードできるのは、十分な機能を持つ管理者のみです。詳細については、付録 D 「機能の定義」を参照してください。
- 「サーバータスク」。レポートを定義したあとに、「スケジュールされたタスク」領域に移動して(「サーバータスク」、「スケジュールの管理」の順に選択)、レポートタスクをスケジュールおよび変更します。TaskDefinition オブジェクトをスケジュールするには、その中に `visibility=schedule` を含めます。この変更を行うには、デバッグページを使用します。詳細については、116 ページの「Identity Manager 設定オブジェクトの編集」を参照してください。

レポートのタイプ

レポートは次の 2 つのカテゴリに分類されます。

- Identity Manager レポート。リアルタイム、概要、監査ログ、システムログ、使用状況レポートなど、さまざまなレポートのタイプが含まれます。
- 監査レポート。監査ポリシーで定義された条件に基づいて、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。

レポートはこれら 2 つのカテゴリからさらに多様なレポートタイプに分類されます。レポートのタイプについては、この章の後のほうで詳しく説明します。Identity Manager レポートについては、276 ページの「Identity Manager レポート」を参照してください。監査レポートについては、285 ページの「監査レポート」を参照してください。

Identity Manager レポートおよび監査レポートを表示する方法については、272 ページの「レポートの表示」を参照してください。

レポートの実行

▼ レポートを実行する

1 管理者インタフェースで、メインメニューから「レポート」をクリックします。「レポートの実行」ページが開きます。

2 利用可能な Identity Manager レポートのリストを表示するには、「レポートタイプ」ドロップダウンメニューから「Identity Manager レポート」を選択します。(このオプションはデフォルトで選択されています。

利用できる監査レポートの一覧を表示するには、「レポートタイプ」ドロップダウンメニューから「監査レポート」を選択します。詳細については、第 15 章「監査: コンプライアンスの監視」の463 ページの「監査レポートの操作」を参照してください。

図 8–1 に、「レポートの実行」ページの例を示します。「レポートタイプ」ドロップダウンメニューで「監査レポート」が選択されています。

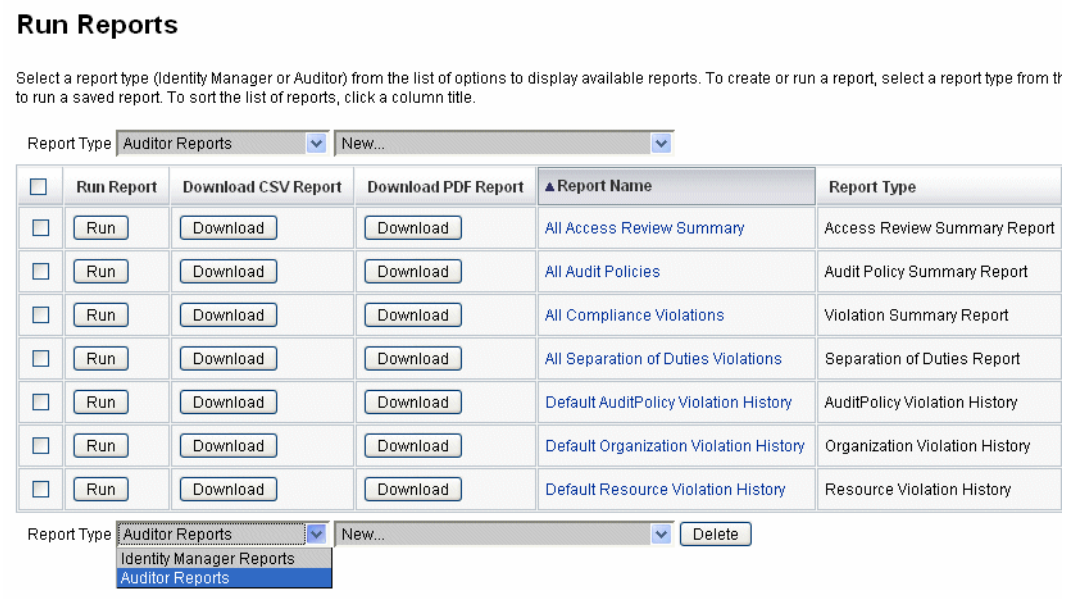


図 8–1 「レポートの実行」の選択項目

3 「実行」をクリックして、レポートを実行します。

注 – 同じレポートの複数のインスタンスを同時に実行できるようにするには、レポートを編集して、「レポートの同時実行を許可」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、複数の管理者が同じレポートを同時に実行できるようになります。

同じレポートの 2 つ以上のインスタンスを同時に実行すると、レポート名に管理者の ID とタイムスタンプが付加されます。

レポートの表示

「レポートの実行」ページからレポートを実行したあと、ただちにまたはあとで出力を表示することができます。

▼ レポートを表示する

1 管理者インタフェースで、メインメニューから「レポート」をクリックします。
「レポートの実行」ページが開きます。

2 「レポートの表示」タブをクリックします。
「レポートの表示」ページが開きます。

3 レポートをクリックして表示します。

レポートの作成

この節では、既存のレポートを使用しないで、新しい Identity Manager レポートまたは Identity Auditor レポートを作成する方法を説明します。

注 – 既存のレポートを修正して新しい名前で保存する場合は、次の節の 273 ページの「レポートの編集および複製」を参照してください。

▼ 新しいレポートを作成する

1 管理者インタフェースで、メインメニューから「レポート」をクリックします。
「レポートの実行」ページが開きます。

2 「レポートタイプ」ドロップダウンメニューからレポートのカテゴリを選択します。
次の 2 つのレポートカテゴリがあります。

- Identity Manager レポート
- Identity Auditor レポート

3 次のドロップダウンメニューで、作成するレポートタイプを選択します (このメニューでは、一番上が「新規」)。
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、レポートの作成、実行、または保存を行います。

レポート基準を入力または選択すると、次の手順を実行できます。

- レポートを保存せずに実行します。「実行」をクリックして、レポートを実行します。新しいレポートを定義した場合、レポートは保存されません。また、既存のレポートを編集した場合、変更されたレポート基準は保存されません。
- レポートを保存します。「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。

レポートの実行については、270 ページの「レポートの実行」を参照してください。

レポートの編集および複製

この節では、既存のレポートを修正または複製して、新しい名前で保存する方法を説明します。

▼ レポートを編集または複製する

1. 管理者インタフェースで、メインメニューから「レポート」をクリックします。
   「レポートの実行」ページが開きます。
2. 「レポートタイプ」ドロップダウンメニューからレポートのカテゴリを選択します。
   次の 2 つのレポートカテゴリがあります。
   - Identity Manager レポート
   - 監査レポート

     レポートの表に、選択したカテゴリ内の既存のレポートが表示されます。
3. レポート名をクリックして編集します。
4. レポートを編集するには、必要に応じてレポートパラメータを調整し、「保存」をクリックします。
   レポートを複製するには、新しいレポート名を入力します。必要に応じてレポートのパラメータを調整し、「保存」をクリックして新しい名前でレポートを保存します。

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。1 人以上の受信者を入力します。 複数の受信者を入力する場合は、コンマで区切ります。

また、電子メールに添付するレポートの形式として、次のいずれかを選択できます。

- 「CSV 形式のレポートの添付」。レポート結果をコンマ区切り (CSV) 形式で添付します。
- 「PDF 形式のレポートの添付」。レポート結果を PDF (Portable Document Format) 形式で添付します。

レポートのスケジュール

次のいずれかを選択して、レポートをただちに実行するか、定期的に実行するようにスケジュールすることができます。

- 保存したレポートをただちに実行する場合は、「レポート」、「レポートの実行」の順に選択します。レポートのリストで、「実行」をクリックします。Identity Manager によりレポートが実行され、結果が要約と詳細の形式で表示されます。
- レポートタスクの実行をスケジュールする場合は、「サーバータスク」、「スケジュールの管理」の順に選択します。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」領域で)。

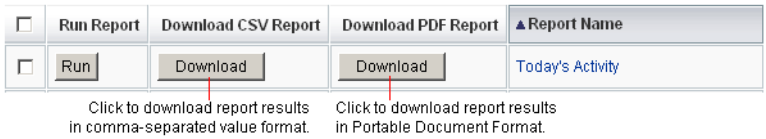
  このリストにレポートのタスク定義を表示するには、タスク定義オブジェクトの `visibility` 属性を `schedule` に設定する必要があります。

レポートデータのダウンロード

「レポートの実行」ページからレポート情報をダウンロードして、Acrobat Reader、StarOffice などのほかのアプリケーションで使用することができます。

「レポートの実行」ページを開き、次のいずれかの列の「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。



レポート出力の設定

レポートの出力を設定するには、「レポート」をクリックして「レポートの設定」を選択します。

「レポートの設定」ページで、次のように設定できます。

- **PDF** レポートオプション

  PDF (Portable Document Format) 形式で生成されるレポートについて、使用するフォント、ページサイズ、およびページの向きを選択できます。

  - 「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のみが表示されます。ただし、フォントの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、その他のフォント (アジア言語のサポートに必要なフォントなど) をシステムに追加できます。

    使用可能なフォント定義の形式は、`.ttf`、`.ttc`、`.otf`、および `.afm` です。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」。生成した PDF レポートにフォント定義を埋め込む場合は、このオプションを選択します。これによりすべての PDF ビューアでレポートが表示できるようになります。

    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。

  - 「Page Size」。メニューから「レター」 (8 ½ x 11 インチ) または「リーガル」1 (8 ½ x 14 インチ) を選択して、PDF のページサイズを指定します。デフォルト値は「レター」です。

    注 – 「Reports Config Libarary」フォームの「pdfPageSize」フィールドを使用して、このメニューにほかのサイズを追加することもできます。pdfPageSize の値は、`itext` パッケージの `com.lowagie.text.Rectangle` クラスで認識できる値である必要があります。

- 「向き」。メニューから「縦向き」または「横向き」を選択して、PDF ページの向きを指定します。デフォルト値は「縦向き」です。

- 「CSV レポートオプション」。「文字セット名」オプションを選択して、CSV レポートを生成するときに使用する文字セットを指定します。CSV ファイルをインポートするすべてのアプリケーションがデフォルトの UTF-8 エンコーディングをサポートするとはかぎりません。必要に応じてほかの文字セットを選択します。
- 「追跡イベント設定」。「イベント収集の有効化」オプションを選択して、システム監視用のレポートを設定します。このオプションは、レポートの出力形式のカスタマイズには適用されません。詳細については、293 ページの「追跡イベント設定」を参照してください。

「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。

Identity Manager レポート

Identity Manager レポートタイプは、次のカテゴリに分類できます。

- 276 ページの「監査ログレポート」
- 277 ページの「単一ユーザー用の監査ログレポート」
- 278 ページの「リアルタイムレポート」
- 278 ページの「概要レポート」
- 281 ページの「システムログレポート」
- 281 ページの「使用状況レポート」
- 283 ページの「ワークフローレポート」

監査ログレポート

監査ログレポートは、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については、109 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。

▼ 監査ログレポートを定義する

1 272 ページの「レポートの作成」のレポートの作成手順に従います。

最初の「レポートタイプ」メニューから「Identity Manager レポート」を選択し、二次的なメニューから「監査ログレポート」を選択します。

「レポートの定義」ページが開きます。

2 フォームに値を入力し、「保存」をクリックします。

フォームの操作がわからないときは、「ヘルプ」をクリックします。

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」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。

単一ユーザー用の監査ログレポート

監査ログレポートと同様に、単一ユーザー用の監査ログレポートは、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。ただし、このレポートではレポート対象のユーザーの指定が要求され、そのユーザーが実行したアクティビティーのリストが返されます。最大の結果を得るため、このレポートでは監査ログの `AccountId` フィールドと `ObjectDesc` フィールドの両方で、一致するユーザー名を検索します。

返される列のセットを固定することも、列のカスタムセットを選択することもできます。列は、`reporttasks.xml` と `defaultreports.xml` で定義します。どちらのファイルも、Identity Manager インストールディレクトリ内の `sample` ディレクトリにあります。

▼ 単一ユーザー用の監査ログレポートを定義する

1 272 ページの「レポートの作成」のレポートの作成手順に従います。

最初の「レポートタイプ」メニューから「Identity Manager レポート」を選択し、二次的なメニューから「単一ユーザー用の監査ログレポート」を選択します。

「レポートの定義」ページが開きます。

2 フォームに値を入力し、「保存」をクリックします。

フォームの操作がわからないときは、「ヘルプ」をクリックします。

リアルタイムレポート

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ような種類があります。

- リソースグループレポート。ユーザーメンバーシップなどのグループ属性の要約を示します。
- リソースステータスレポート。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。
- リソースユーザーレポート。ユーザーリソースアカウントとアカウント属性の一覧を示します。

▼ リアルタイムレポートを定義する

1 272 ページの「レポートの作成」のレポートの作成手順に従います。

最初の「レポートタイプ」メニューから「Identity Manager レポート」を選択し、二次的なメニューから「リソースグループレポート」、「リソースステータスレポート」、または「リソースユーザーレポート」を選択します。

「レポートの定義」ページが開きます。

2 フォームに値を入力し、「保存」をクリックします。

フォームの操作がわからないときは、「ヘルプ」をクリックします。

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。

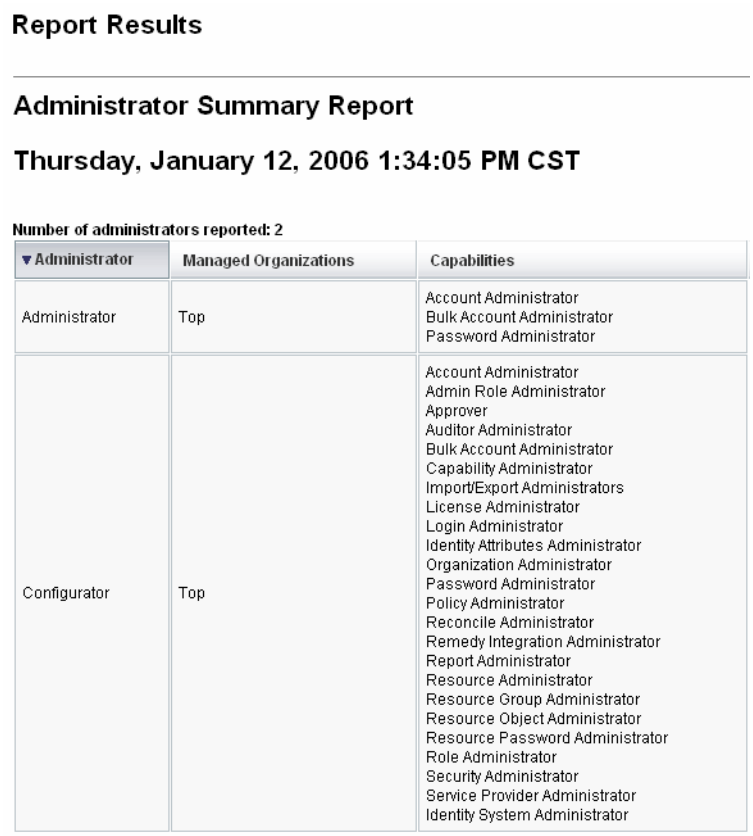
- アカウントインデックスレポート。調整の状況に従って、選択したリソースアカウントについてレポートします。
- 管理者レポート。Identity Manager 管理者、管理者が管理する組織、および割り当てられた機能を示します。管理者レポートを定義するときには、レポートに含める管理者を組織によって選択できます。
- 管理者ロールレポート。管理者ロールに割り当てられたユーザーのリストを示します。

- ロールレポート。ロールと関連リソースの詳細な情報をレポートします。
- タスクレポート。開いているタスクおよび完了した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。
- ユーザーレポート。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。
- ユーザー質問レポート。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。

注 – 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

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。



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

▼ 概要レポートを定義する

1 272 ページの「レポートの作成」のレポートの作成手順に従います。

二次的なメニューから、前の一覧にあるいずれかの概要レポートタイプを選択します。

「レポートの定義」ページが開きます。

2 フォームに値を入力し、「保存」をクリックします。

フォームの操作がわからないときは、「ヘルプ」をクリックします。

システムログレポート

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、次の項目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ます。次に、要求された 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570 ページの「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

1 272 ページの「レポートの作成」のレポートの作成手順に従います。

最初の「レポートタイプ」メニューから「Identity Manager レポート」を選択し、二次的なメニューから「システムログレポート」を選択します。

「レポートの定義」ページが開きます。

2 フォームに値を入力し、「保存」をクリックします。

フォームの操作がわからないときは、「ヘルプ」をクリックします。

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

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、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

式や表形式で表示できます。使用状況レポートの表示データは、表、棒グラフ、円グラフ、または線グラフの形式で表示できます。

▼ 使用状況レポートを定義する

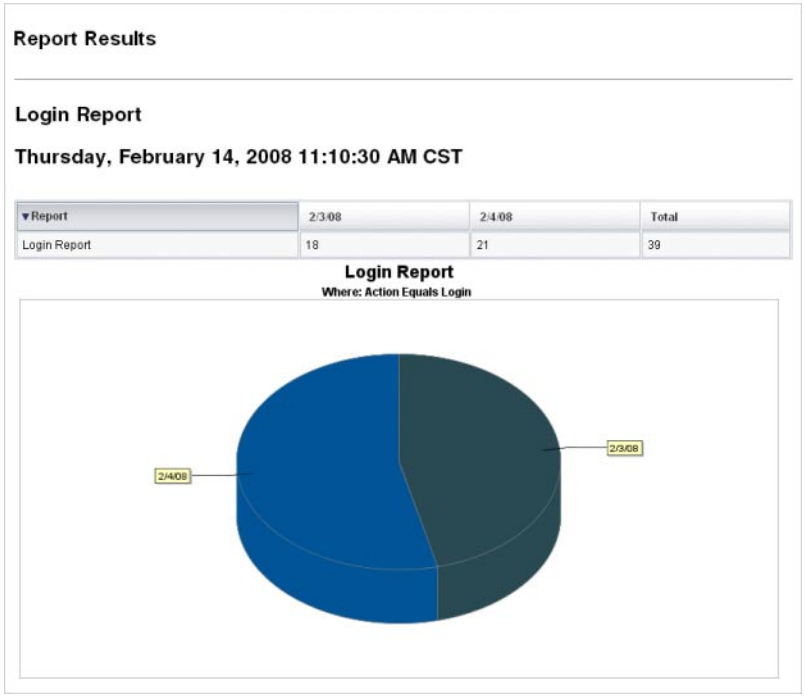
1 272 ページの「レポートの作成」のレポートの作成手順に従います。

2 最初の「レポートタイプ」メニューから「**Identity Manager** レポート」を選択し、二次的なメニューから「使用状況レポート」を選択します。
「レポートの定義」ページが開きます。

3 フォームに値を入力し、「保存」をクリックします。
フォームの操作がわからないときは、「ヘルプ」をクリックします。
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。

例 8–1 使用状況レポートのグラフ (生成されたユーザーアカウント)

次の図に、使用状況レポートの例を示します。上部の表にレポートを構成するイベントが示され、下のグラフに同じ情報がグラフ形式で示されています。



ワークフローレポート

このレポートはワークフロー名の一覧とともに、次の情報を提供します。

- ワークフローが完了するまでの平均時間
- ワークフローがリクエストされた回数
- 完了したワークフローリクエストの数

さらに、ワークフロー名をクリックするとそのワークフローの詳細表示が開き、ワークフロー内部に設定された各アクティビティーとそれらが完了するまでの平均時間がわかります。

ワークフローレポートは、サービスレベル契約 (SLA) の目標が達成されているかどうかを確定する助けとなる、パフォーマンス測定基準を得るのに特に役立ちます。

ワークフローレポートを実行する前提条件として、ワークフローの計時測定基準を取得するように Identity Manager を設定します。詳細については、次の節を参照してください。

監査計時イベントを取得するワークフローの設定

ワークフローレポートを実行する前に、まず、レポートの対象となるワークフロータイプごとにワークフロー監査を有効にします。

注 – ワークフローの監査を行うと、パフォーマンスが低下します。ワークフローレポートを使用する予定のワークフローでのみ、ワークフロー監査を有効にすることをお勧めします。

ワークフロー監査を有効にする方法は次のとおりです。

- タスクテンプレートを使用して管理者インタフェースで設定できるワークフローの場合は、タスクテンプレート設定フォームの「監査」タブの「ワークフロー全体の監査」チェックボックスを選択します。手順については、326 ページの「「監査」タブの設定」を参照してください。
- タスクテンプレートのないワークフローについては、341 ページの「タイミング監査イベントをログするためのワークフローの変更」を参照してください。

ワークフローレポート用に保存する属性の指定

属性の定義は必須ではありませんが、ワークフローレポートを最大限に活用するため、あとでレポートのフィルタに使用する予定の属性を保存することは重要です。

ワークフローのタイプごとに保存する一連の属性を定義するには、管理者インタフェースのタブ付きタスクテンプレート設定フォームを使用します。「監査」タブの「ワークフロー全体の監査」チェックボックスの下に「属性の監査」セクションがあります。手順については、326 ページの「「監査」タブの設定」を参照してください。

▼ ワークフローレポートを定義する

1 **272 ページの「レポートの作成」**のレポートの作成手順に従います。

最初の「レポートタイプ」メニューから「Identity Manager レポート」を選択し、二次的なメニューから「ワークフローレポート」を選択します。

「レポートの定義」ページが開きます。

2 フォームに値を入力し、「保存」をクリックします。監査対象に選んだ任意の属性を追加することに加え、時間のパラメータを定義できます。前の節の**284 ページの「ワークフローレポート用に保存する属性の指定」**を参照してください。

結果を絞り込むには、`user.global.state` のように属性名を指定し、条件を選択して、属性値を入力します。属性は必要に応じていくつでも入力できます。

フォームの操作がわからないときは、「ヘルプ」をクリックします。

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」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。

このレポートではワークフローの名前ごとに、ワークフローが完了するまでの平均時間、ワークフローがリクエストされた回数、およびそれらのリクエストのうち完了したものの数がわかります。

ワークフロー名をクリックするとそのワークフローの詳細表示が開き、ワークフローに設定された各アクティビティーが表示されます。同名のアクティビティーが複数のプロセスに存在する可能性があるため、アクティビティーの範囲はプロセス単位になります。

監査レポート

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。

Identity Manager には、次の監査レポートが用意されています。

- アクセスレビュー範囲レポート
- アクセスレビュー詳細レポート
- アクセスレビュー概要レポート
- アクセススキャンユーザー範囲レポート
- 監査ポリシーの概要レポート
- 監査属性レポート
- 違反履歴 (監査ポリシー別)
- 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
- 職務分掌レポート
- 違反の概要レポート

監査レポートを定義するには、272 ページの「レポートの作成」の手順に従います。

監査レポートの詳細については、第 15 章「監査: コンプライアンスの監視」の463 ページの「監査レポートの操作」を参照してください。

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。

- 286 ページの「定義済みのグラフの表示」
- 287 ページの「ダッシュボードグラフを作成する」
- 289 ページの「ダッシュボードグラフを編集する」
- 290 ページの「定義したグラフを削除する」

定義済みのグラフの表示

Identity Manager には、サンプルのグラフが用意されています。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。

▼ 定義済みのグラフを表示する

1. 管理者インタフェースで、メインメニューから「レポート」をクリックします。
2. 二次的なメニューで「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 – グラフのいずれかでエラーメッセージが表示される場合は、システム設定オブジェクトを開いて (116 ページの「Identity Manager 設定オブジェクトの編集」)、`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。

▼ ダッシュボードグラフを作成する

1 管理者インタフェースで、「レポート」、「ダッシュボードグラフ」の順に選択します。

2 「ダッシュボードグラフの種類の選択」オプションで、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。

3 「新規」をクリックして「ダッシュボードグラフの作成」ページを開き、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。

4 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。

---

5 リストから追跡イベントの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。

- 「プロビジョニング担当者の実行回数」。操作タイプごとのプロビジョニングツール操作の回数を追跡します。
- 「プロビジョニング担当者の実行時間」。操作タイプごとのプロビジョニングツール操作の時間を追跡します。
- 「リソース操作の回数」。リソース操作の回数を追跡します。
- 「リソース操作の期間」。リソース操作の時間を追跡します。
- 「ワークフロー時間」。ワークフローの実行にかかった時間を追跡します。
- 「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。

6 リストからタイムスケールを選択します。

このオプションは、データ収集の間隔 (1 時間など) と、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。

7 リストから測定基準を選択します。

選択した追跡イベントに応じて、測定基準 (カウントまたは平均) がデフォルトで選択されます。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。

使用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

8 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。

9 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。

10 「ベース次元」を指定します (省略可能)。

次のリストから選択します。

- 「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。

11 「グラフオプション」フィールドにテキストを入力し、グラフのメインタイトルの下に表示されるサブタイトルを指定します (省略可能)。

12 「グラフの詳細オプション」を選択します (省略可能)。
次の設定を指定する場合は、このオプションを使用します。

- グリッドライン
- フォント
- カラーパレット

13 グラフを作成するには、「保存」をクリックします。

▼ ダッシュボードグラフを編集する

1 管理者インタフェースで、メインメニューから「レポート」をクリックします。

2 二次的なメニューで「ダッシュボードグラフ」をクリックします。
「ダッシュボードグラフ」ページが開きます。

3 「ダッシュボードグラフの種類の選択」ドロップダウンメニューからカテゴリを選択します。
ダッシュボードグラフの一覧表が開きます。

4 グラフ名をクリックして編集します。
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するイベントの説明を指定します。現在は SAMPLE、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」。追跡する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。

- 「グラフの詳細オプション」。次の設定を行う場合に選択します。
  - グリッドライン
  - フォント
  - カラーパレット

5 「保存」をクリックします。

▼ 定義したグラフを削除する

1 管理者インタフェースで、メインメニューから「レポート」をクリックします。

2 二次的なメニューで「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 削除するグラフをチェックボックスで選択し、「削除」をクリックします。

注 – グラフは、そのグラフの含まれているすべてのダッシュボードから警告なしで削除されます。

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 にはサンプルのダッシュボードセットが用意されており、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、291 ページの「ダッシュボードを作成する」を参照してください。

▼ ダッシュボードを表示する

1 管理者インタフェースで、メインメニューから「レポート」をクリックします。

2 二次的なメニューで「ダッシュボードの表示」をクリックすると、現在定義されているダッシュボードが表示されます。
「ダッシュボード」ページが開きます。

3 表示する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。

- 291 ページの「ダッシュボードを作成する」
- 292 ページの「ダッシュボードの編集」
- 292 ページの「ダッシュボードの削除」

▼ ダッシュボードを作成する

1. 管理者インタフェースで、メインメニューから「レポート」をクリックします。
2. 二次的なメニューで「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、291 ページの「ダッシュボードを作成する」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て、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。そのグラフをほかのダッシュボードで使用することができます。

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 8–2 に、ダッシュボードの編集ページの例を示します。

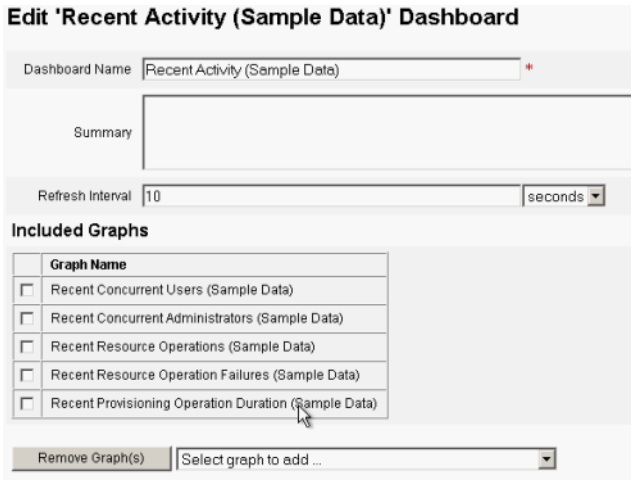


図 8–2　ダッシュボードの編集

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」領域から「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。グラフの削除には、「ダッシュボードグラフの管理」ページを使用します (290 ページの「定義したグラフを削除する」を参照)。

システムの監視

イベントをダッシュボードグラフに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 を設定できます。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、時刻や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。

グラフィカルなダッシュボードの表示を作成して、自動化されたアクティビティーや手動のアクティビティーを詳細に追跡することができます。Identity Manager には、サンプルの「リソース操作」ダッシュボードグラフが用意されています。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法については、290 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」領域から、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、日付の変わるタイミングを決定します。

  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。
- 「データ収集を行うタイムスケール」。データ収集の時間間隔 (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利用可能です。デフォルトでは、これらの間隔がすべて選択されています。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。スライダが表示されている場合は、それを使用してグラフの断片をズームインできます。

リスク分析

Identity Manager の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から外れてい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、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 (43 ページの「Identity Manager デバッグページ」) の RiskReportTask オブジェクトの下に表示され、Identity Manager IDE を使用して修正できます。設定フォームの詳細については、『Sun Identity Manager Deployment Reference』の第 2 章「Identity Manager Forms」を参照してください。

▼ リスク分析レポートを作成する

1. 管理者インタフェースで、メインメニューから「レポート」をクリックします。
2. 二次的なメニューで「リスク分析の実行」をクリックします。

3 「新規」ドロップダウンメニューで、作成するレポートを選択します。
「リスク分析レポート設定」ページが開きます。

4 フォームに必要な情報を指定します。
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、次の条件に適合するアカウントをスキャンできます。

- 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

5 「保存」をクリックします。

▼ リスク分析レポートをスケジュールする

定義したリスク分析レポートは、次の手順を使用して、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 管理者インタフェースで、メインメニューから「サーバータスク」をクリックします。

2 二次的なメニューから「スケジュールの管理」をクリックします。
「スケジュールされたタスク」ページが開きます。

3 スケジュールするリスク分析レポートを選択します。
リスク分析タスクスケジュールの新規作成ページが開きます。

4 名前とスケジュール情報を入力し、必要に応じてほかのリスク分析の選択を調整します。

5 「保存」をクリックして、スケジュールを保存します。

◆ ◆ ◆ 第 9 章

9 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。

この章は、次の節で構成されています。

- 297 ページの「タスクテンプレートの有効化」。システムでタスクテンプレートを使用可能にする方法を説明します。
- 302 ページの「タスクテンプレートの設定」。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を説明しています。

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。
- 「ユーザーテンプレートの更新」。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

1 管理者インタフェースのメニューから「サーバータスク」を選択し、「タスクの設定」を選択します。

図 9–1 に「タスクの設定」ページを示します。

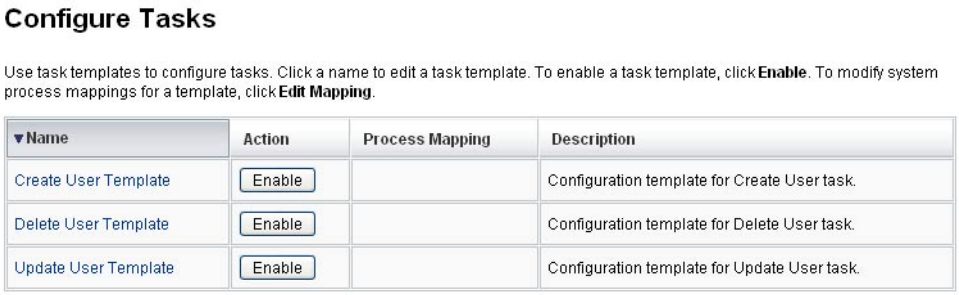


図 9–1 最初の「タスクの設定」ページ

「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」。次のボタンのいずれかが含まれます。
  - 「有効」。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に表示されます。

    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るプロセスタイプを一覧表示します。
- 「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 9–2) が表示されます。

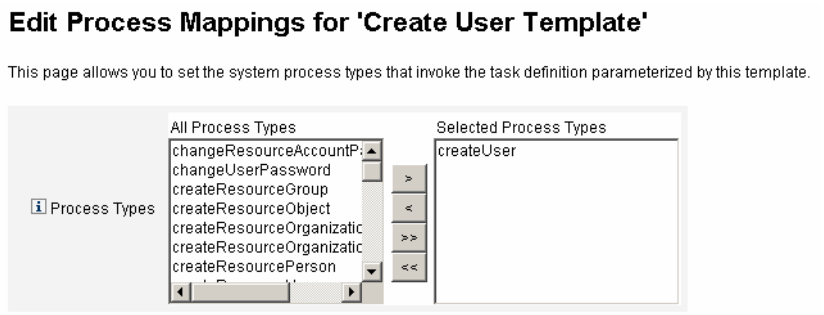
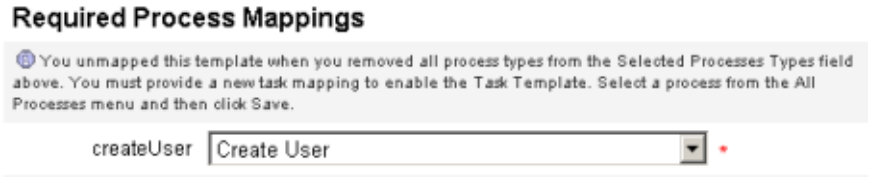


図 9–2 プロセスマッピングの編集ページ

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。



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。

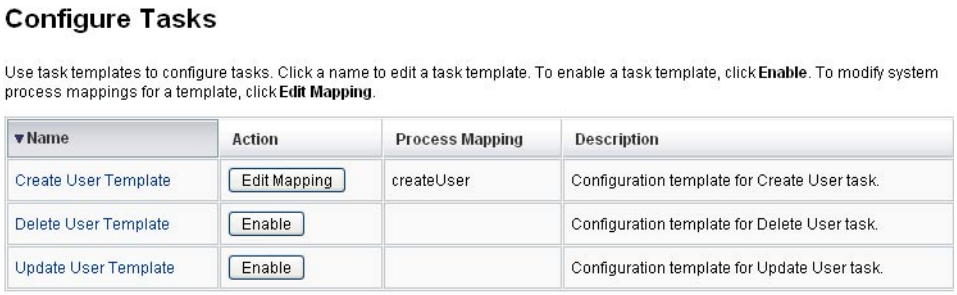


図 9–3 更新された「タスクの設定」テーブル

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。

参考 マッピングの検証

- 「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`	ユーザー作成テンプレート
`deleteUser`	ユーザー削除テンプレート
`updateUser`	ユーザー更新テンプレート

  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。

▼ タスクテンプレートを設定する

テンプレートプロセスタイプのマッピング (297 ページの「タスクテンプレートの有効化」) 後、タスクテンプレートを設定できます。

1 管理者インタフェースのメインメニューで「サーバータスク」をクリックし、「タスクの設定」をクリックします。

「タスクの設定」ページが開きます。

2 「名前」列のリンクを選択します。

次のページのいずれかが表示されます。

- 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されるテンプレートを編集するために開きます。
- タスクテンプレート「Delete User Template」の編集。ユーザーのアカウントの削除またはプロビジョニング解除に使用されるテンプレートを編集するために開きます。
- タスクテンプレート「Update User Template」の編集。既存のユーザー情報の更新に使用されるテンプレートを編集するために開きます。

  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。

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または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。このタブでワークフローを設定し、ワークフローレポート用の情報を取得します。	すべてのテンプレート

タブ名	目的	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
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

3 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。

- 298 ページの「プロセスタイプをマップする」
- 300 ページの「タスクテンプレートを設定する」

4 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。

タスクテンプレートの設定

この節では、タスクテンプレートの設定の説明および手順を示します。次のトピックを扱います。

- 302 ページの「「一般」タブの設定」
- 305 ページの「「通知」タブの設定」
- 311 ページの「「承認」タブの設定」
- 326 ページの「「監査」タブの設定」
- 327 ページの「「プロビジョニング」タブの設定」
- 328 ページの「「サンライズとサンセット」タブの設定」
- 334 ページの「「データ変換」タブの設定」

「一般」タブの設定

この節では、タスクテンプレート設定プロセスの一部として利用できる、「一般」タブの設定手順を説明します。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」を参照してください。

注 – 管理者インタフェースの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ページは同一なので、設定手順を 1 つの節で説明します。

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」フォーム、「タスクテンプレート「Update User Template」の編集」フォームのいずれかを開くと、デフォルトで「一般」タブページが表示されます。図 9–4 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と「属性の挿入」メニューから成ります。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」の節を参照してください。

図 9–4 「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

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。たとえば、次のようにします。

```
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。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」を参照してください。

▼ 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

1 **「Identity Manager アカウントの削除」ボタンを使用して、削除処理中に Identity Manager アカウントを削除するかどうかを指定します。**

次のボタンがあります。

- 「なし」。アカウントが削除されるのを防ぐ場合に選択します。
- 「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存在しないときにのみユーザーアカウントの削除を許可する場合に選択します。
- 「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場合に選択します。

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。**

注 – ユーザーから「外部」リソースを割り当て解除またはリンク解除しても、プロビジョニング要求や作業項目は生成されません。外部リソースを割り当て解除またはリンク解除しても、Identity Manager がリソースアカウントのプロビジョニングを解除したりリソースアカウントを削除したりすることはないため、作業は発生しません。

次のボックスがあります。

- 「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。

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をさらにきめ細かく行えます。

次のボックスがあります。

- 「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、ユーザーを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。

「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する場合に便利です。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。

「通知」タブの設定

この節では、タスクテンプレート設定プロセスの一部として利用できる、「通知」タブの設定手順を説明します。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」を参照してください。

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については、このガイドの 104 ページの「電子メールテンプレートのカスタマイズ」の節を参照してください。

図 9–5 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。

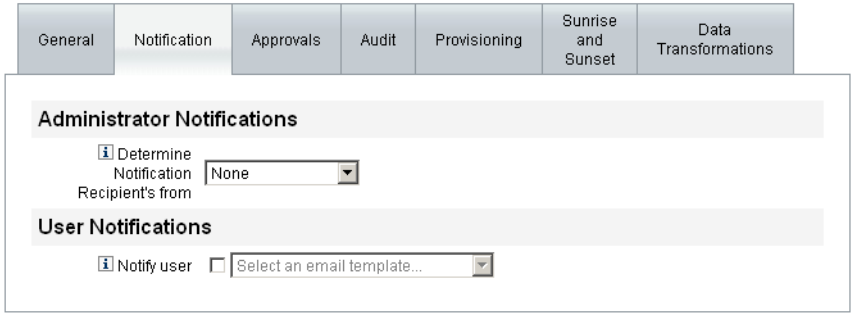


図 9–5 「通知」タブ: ユーザー作成テンプレート

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 9–6 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 9–6 電子メールテンプレートの指定

管理者通知の設定

管理者通知の受信者を Identity Manager で決定する方法を指定するには、「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。

使用できるオプションは次のとおりです。

- 「なし」(デフォルト)。通知される管理者はいません。
- 「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。詳細は、307 ページの「属性による管理者通知の受信者の指定」を参照してください。
- 「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。詳細は、308 ページの「規則による管理者通知の受信者の指定」を参照してください。
- 「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。詳細は、309 ページの「クエリーによる管理者通知の受信者の指定」を参照してください。
- 「管理者リスト」。リストから通知受信者を明示的に選択する場合に選択します。詳細は、307 ページの「属性による管理者通知の受信者の指定」を参照してください。

属性による管理者通知の受信者の指定

注 – この属性により、1 つのアカウント ID を表す文字列、またはアカウント ID のリストが決まります。

▼ 指定された属性から通知受信者のアカウント ID を取得する

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。次の図に示すように、新しいオプションが表示されます。

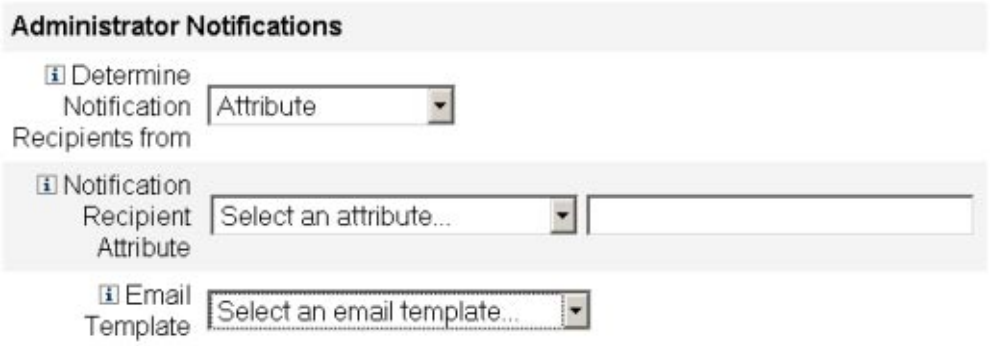


図 9–7 管理者通知: 属性

次のオプションがあります。

- 「通知の受信者の属性」。受信者のアカウント ID の決定に使用される属性のリスト (このテンプレートに設定されているタスクに関連付けられたビューに、現在定義されている属性) が返されます。
- 「電子メールテンプレート」。電子メールテンプレートリストが返されます。

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。

規則による管理者通知の受信者の指定

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。

▼ 指定された規則から通知受信者のアカウント ID を取得する

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 9–8 管理者通知: 規則

- 「通知の受信者の規則」。規則が評価されると、受信者のアカウント ID を返すための規則のリスト (システムに現在定義されているもの) が返されます。
- 「電子メールテンプレート」。電子メールテンプレートリストが返されます。

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。

クエリーによる管理者通知の受信者の指定

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へのクエリーを作成することによって通知受信者のアカウント ID を取得する

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 9–9 に示すように、「通知」フォームに新しいオプションが表示されます。

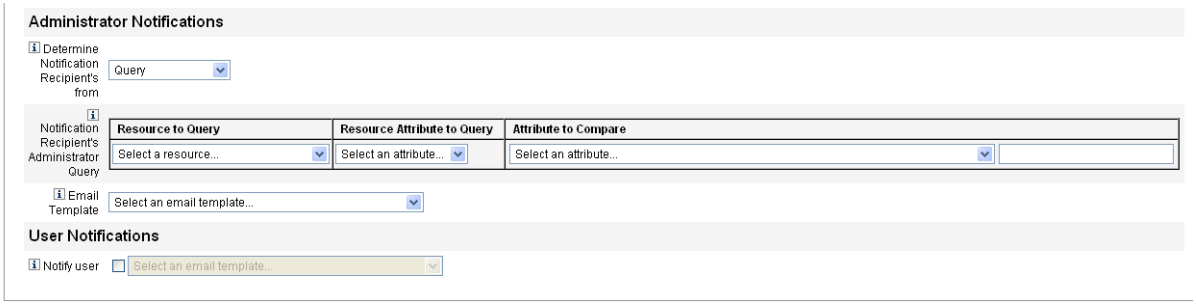


図 9–9 管理者通知: クエリー

「通知の受信者の管理者のクエリー」テーブルは、クエリーを作成するための次のメニューで構成されます。

- 「問い合わせ先のリソース」。システムに現在定義されているリソースのリストが返されます。
- 「問い合わせ先のリソース属性」。システムに現在定義されているリソース属性のリストが返されます。
- 「比較対象の属性」。システムに現在定義されている属性のリストが返されます。
- 「電子メールテンプレート」。電子メールテンプレートリストが返されます。

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。

▼ 管理者リストから管理者通知の受信者を指定する

1 「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。次の図に示すように、「通知」フォームに新しいオプションが表示されます。

図 9–10 管理者通知: 管理者リスト

次のオプションがあります。

- 「通知する管理者」。選択ツールおよび通知できる管理者のリストが返されます。
- 「電子メールテンプレート」。電子メールテンプレートリストが返されます。

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、「選択された管理者」リストに移動します。

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。

「承認」タブの設定

この節では、タスクテンプレート設定プロセスの一部として利用できる、「承認」タブの設定手順を説明します。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」の節を参照してください。

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、特定の組織、リソース、またはロールに関連付けられた管理者は、実行前に所定のタスクを承認する必要がありました。Identity Manager では、「追加の承認者」を指定することもできます。タスクを承認する必要のある追加の管理者です。

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。

図 9–11 は、初期状態の「承認」ページの管理者ユーザーインタフェースの例です。

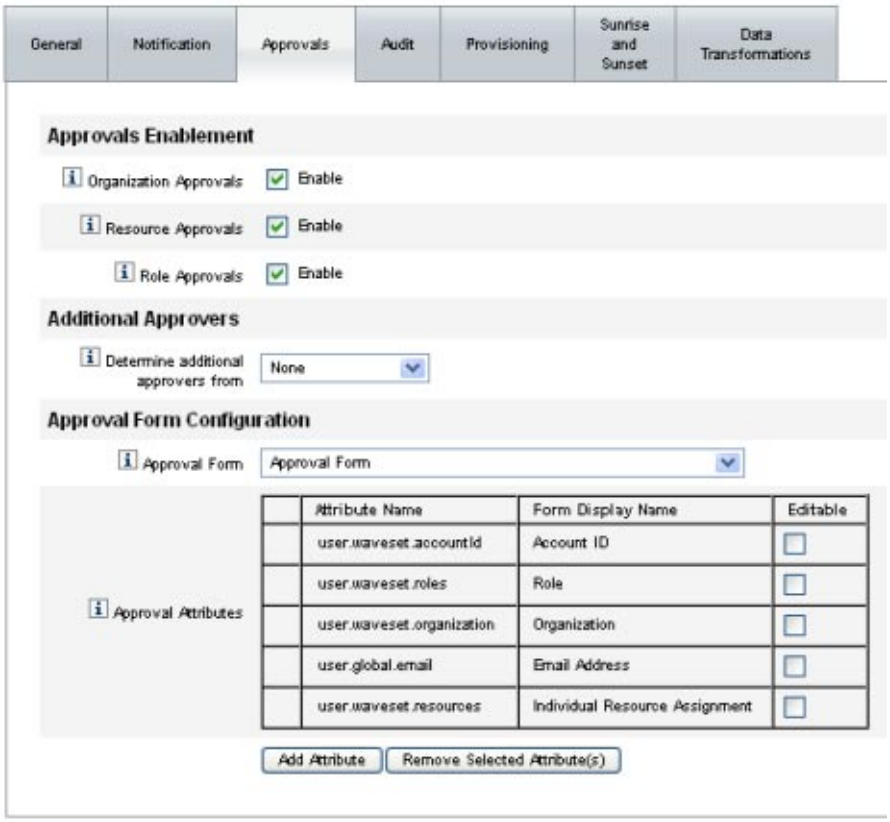


図 9–11 「承認」タブ: ユーザー作成テンプレート

▼ 承認を設定する

1 「承認の有効化」セクションに必要な情報を指定します (313 ページの「承認の有効化 (「承認」タブ、「承認の有効化」セクション)」を参照)。

2 「追加の承認者」セクションに必要な情報を指定します (313 ページの「追加の承認者の指定 (「承認」タブ、「追加の承認者」セクション)。」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に対してのみ、「承認フォーム設定」セクションに必要な情報を指定します (322 ページの「承認フォームの設定 (「承認」タブ、「承認フォーム設定」セクション)」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 (「承認」タブ、「承認の有効化」セクション)

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 (「承認」タブ、「追加の承認者」セクション)。

「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を表 9–1 に示します。

表 9–1 メニューオプションからの追加の承認者の決定

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。
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、管理者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。

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。

▼ 属性から追加の承認者を決定する

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 – この属性により、1 つのアカウント ID を表す文字列、またはアカウント ID のリストが決まります。

次の図に示すように、新しいオプションが表示されます。

図 9–12 追加の承認者: 属性

- 「承認者の属性」。承認者のアカウント ID の決定に使用される属性のリスト (このテンプレートに設定されているタスクに関連付けられたビューに、現在定義されている属性) が返されます。
- 「承認がタイムアウトになるまでの時間」。承認がタイムアウトするまでの時間を指定する方法が返されます。

  「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。

- タイムアウト期間を指定する場合の手順は、318 ページの「承認タイムアウトを設定する」を参照してください。
- タイムアウト期間を指定しない場合は、322 ページの「承認フォームの設定 (「承認」タブ、「承認フォーム設定」セクション)」に進むか、変更を保存して別のタブの設定を続けます。

▼ 規則から追加の承認者を決定する

指定された規則から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「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。

次の図に示すように、新しいオプションが表示されます。

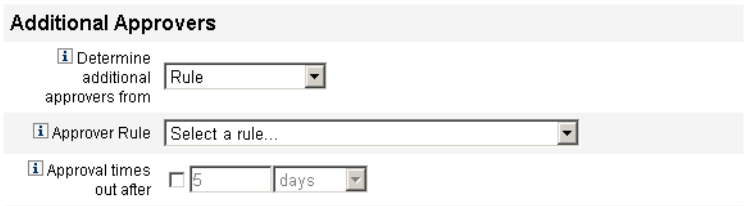


図 9–13 追加の承認者: 規則

- 「承認者の規則」。規則が評価されると、受信者のアカウント ID を返すための規則のリスト (システムに現在定義されているもの) が返されます。

- 「承認がタイムアウトになるまでの時間」。承認がタイムアウトするまでの時間を指定する方法が返されます。

  「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。

- タイムアウト期間を指定する場合の手順は、318 ページの「承認タイムアウトを設定する」を参照してください。
- タイムアウト期間を指定しない場合は、322 ページの「承認フォームの設定 (「承認」タブ、「承認フォーム設定」セクション)」に進むか、変更を保存して別のタブの設定を続けます。

▼ クエリーから追加の承認者を決定する

指定されたリソースへのクエリーを作成することによって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。

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。

---

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。次の図に示すように、新しいオプションが表示されます。

図 9–14 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」。システムに現在定義されているリソースのリストが返されます。

- 「問い合わせ先のリソース属性」。システムに現在定義されているリソース属性のリストが返されます。
- 「比較対象の属性」。システムに現在定義されている属性のリストが返されます。

- 「承認がタイムアウトになるまでの時間」。承認がタイムアウトするまでの時間を指定する方法が返されます。

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。

- タイムアウト期間を指定する場合の手順は、318 ページの「承認タイムアウトを設定する」を参照してください。
- タイムアウト期間を指定しない場合は、322 ページの「承認フォームの設定 (「承認」タブ、「承認フォーム設定」セクション)」に進むか、変更を保存して別のタブの設定を続けます。

▼ 管理者リストから追加の承認者を決定する

管理者リストから追加の承認者を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。次の図に示すように、新しいオプションが表示されます。

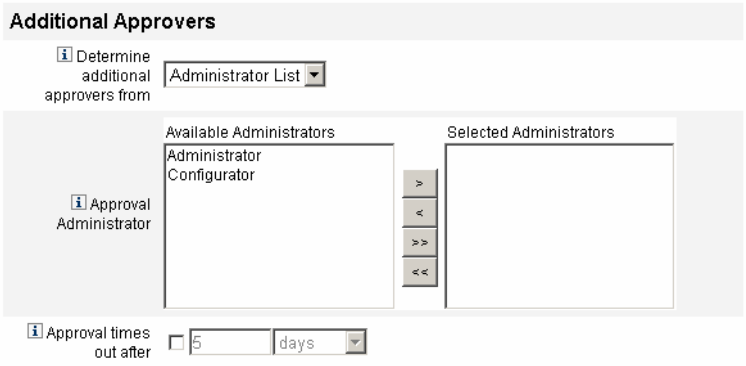


図 9–15　追加の承認者: 管理者リスト

- 「通知する管理者」。選択ツールおよび通知できる管理者のリストが返されます。
- 「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拒否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」。承認がタイムアウトするまでの時間を指定する方法が返されます。

「承認がタイムアウトになるまでの時間」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。

- タイムアウト期間を指定する場合の手順は、318 ページの「承認タイムアウトを設定する」を参照してください。
- タイムアウト期間を指定しない場合は、322 ページの「承認フォームの設定 (「承認」タブ、「承認フォーム設定」セクション)」に進みます。

▼ 承認タイムアウトを設定する

「承認がタイムアウトになるまえでの時間」セクションで承認タイムアウトを設定するには、次の手順に従います。

1　「承認がタイムアウトになるまでの時間」チェックボックスを選択します。

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」オプションが表示されます。

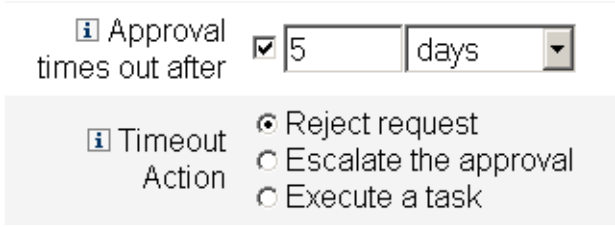


図 9–16 承認のタイムアウトのオプション

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」ボタンを使用して、承認リクエストがタイムアウトしたときの動作を選択します。

次のいずれかをクリックします。

- 「リクエストの拒否」。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拒否します。
- 「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。手順については、320 ページの「「エスカレーション承認者を決定する方法」セクションを設定する方法」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。手順については、322 ページの「「承認のタイムアウト時のタスク」セクションを設定する」を参照してください。

▼ 「エスカレーション承認者を決定する方法」セクションを設定する方法

「タイムアウトのアクション」セクションの「承認のエスカレーション」を選択すると (318 ページの「承認タイムアウトを設定する」)、次の図に示すように、「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。

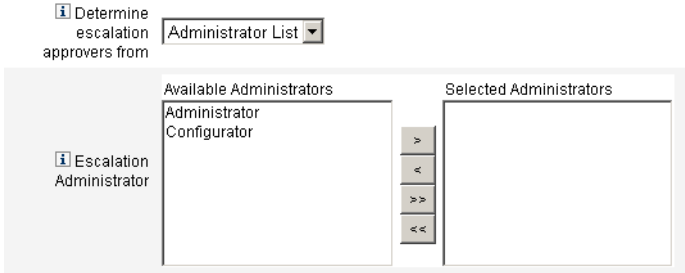
- このメニューからオプションを選択して、エスカレーションされた承認の承認者を決定する方法を指定します。

  次のオプションがあります。

  - 「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 – この属性により、1 つのアカウント ID を表す文字列、またはアカウント ID のリストが決まります。

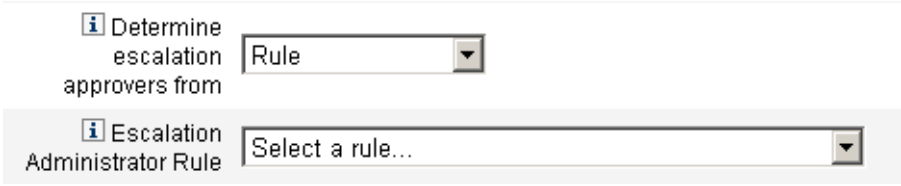
    このオプションを選択すると、「エスカレーション管理者属性」メニューが表示されます。リストから属性を選択すると、次の図に示すように、選択した属性が隣のテキストフィールドに表示されます。



  - 「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。

このオプションを選択すると、次の図に示すように、「エスカレーション管理者規則」メニューが表示されます。リストから規則を選択します。

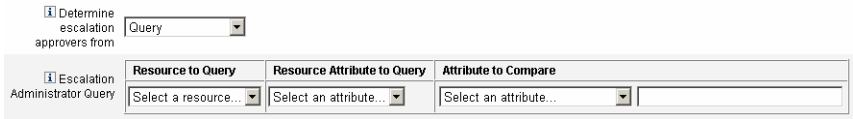


- 「クエリー」。特定のリソースを問い合わせることで承認者のアカウント ID を決定します。

  次の図に示すように「エスカレーション管理者クエリー」メニューが表示されます。

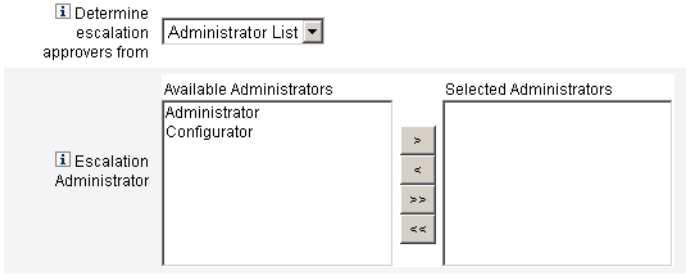
  次のようにクエリーを作成します。

  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。



- 「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。

  次の図に示すように「エスカレーション管理者」選択ツールが表示されます。

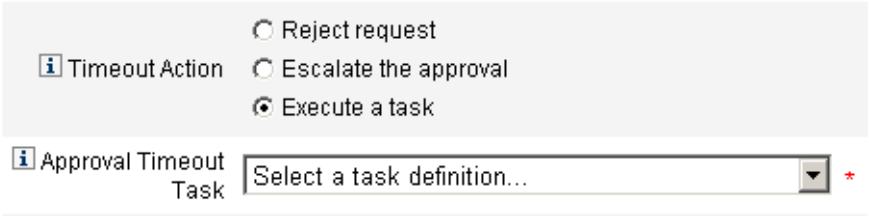


次のように承認者を選択します。

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。

▼ 「承認のタイムアウト時のタスク」セクションを設定する

「タイムアウトのアクション」セクションの「タスクの実行」オプションを選択すると (318 ページの「承認タイムアウトを設定する」)、次の図に示すように「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。



- 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選択します。
  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 (「承認」タブ、「承認フォーム設定」セクション)

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。

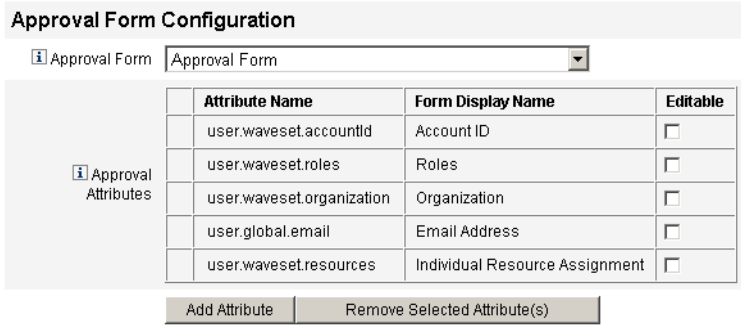


図 9–17 承認フォーム設定

デフォルトでは、「承認時に表示する属性」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、「承認時に表示する属性」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。

▼ 追加の承認者の承認フォームを設定する

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拒否します。

2 承認者による属性値の編集を許可する場合、「承認時に表示する属性」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、324 ページの「属性を承認フォームに追加する」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、325 ページの「属性の削除」を参照してください。

デフォルトの属性を承認フォームから削除するには、XML ファイルを修正する必要があります。

▼ 属性を承認フォームに追加する

1 「承認時に表示する属性」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、「承認時に表示する属性」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。

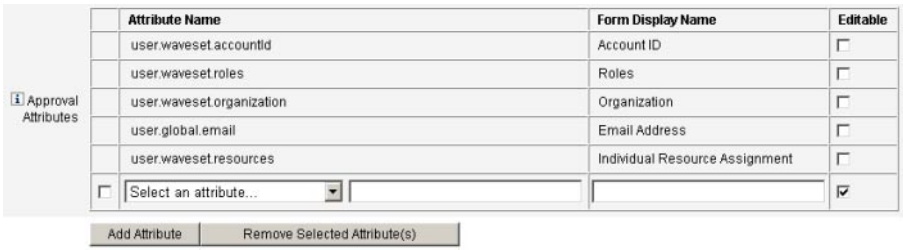


図 9–18 承認属性の追加

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は、次のことができます。

- 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します。
- 「編集可能」チェックボックスを有効にして、承認者による属性値の変更を許可します。

  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する場合があります。

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 – デフォルトの属性を承認フォームから削除するには、XML ファイルを修正する必要があります。

▼ 属性を承認フォームから削除する

1 「承認時に表示する属性」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「承認時に表示する属性」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 9–19 承認属性の削除

「監査」タブの設定

この節では、タスクテンプレート設定プロセスの一部として利用できる、「監査」タブの設定手順を説明します。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」を参照してください。

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。

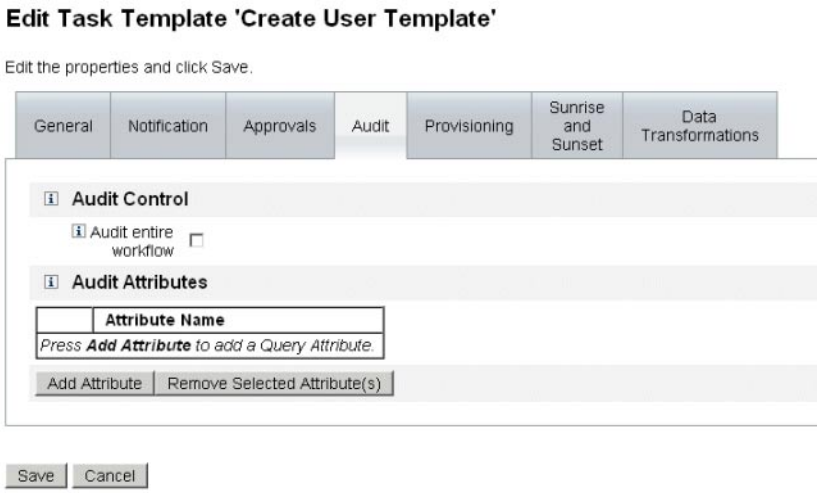


図 9–20 ユーザー作成テンプレートの監査

▼ 監査を設定する

1 「ワークフロー全体の監査」チェックボックスを選択して、ワークフローの監査機能を有効にします。

ワークフローの監査については、338 ページの「ワークフローからの監査イベントの作成」を参照してください。ワークフローの監査を行うとパフォーマンスは低下します。

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監査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。
選択した属性名が隣のテキストフィールドに表示されます。

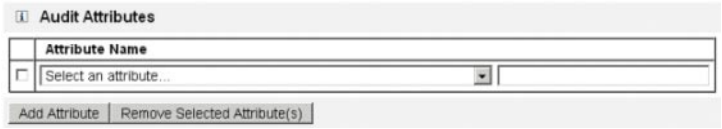


図 9–21 属性の追加

▼ 属性を削除する

1 削除する属性に隣接するチェックボックスを有効にします。

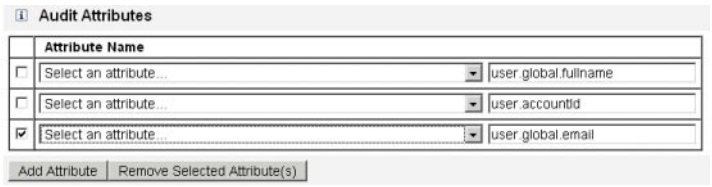


図 9–22 user.global.email 属性の削除

2 「選択している属性の削除」ボタンをクリックします。

「プロビジョニング」タブの設定

この節では、タスクテンプレート設定プロセスの一部として利用できる、「プロビジョニング」タブの設定手順を説明します。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」を参照してください。

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。

図 9–23 「プロビジョニング」タブ:ユーザー作成テンプレート

「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。

- 「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。」。タスクの実行からのエラー結果をプロビジョニングするときにユーザーインタフェースに再試行リンクを追加するには、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。

「サンライズとサンセット」タブの設定

この節では、タスクテンプレート設定プロセスの一部として利用できる、「サンライズとサンセット」タブの設定手順を説明します。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」を参照してください。

注 – このタブはユーザー作成タスク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 9–24 に「サンライズとサンセット」タブでの設定を示します。

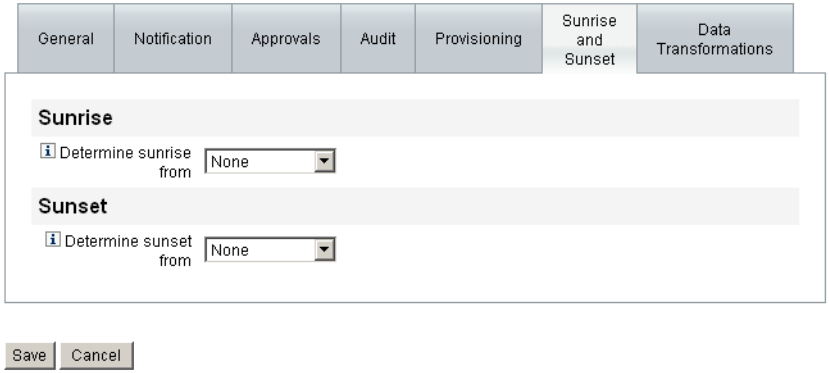


図 9–24 「サンライズとサンセット」タブ:ユーザー作成テンプレート

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

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」。指定した時間後にプロビジョニングを実行します。手順については、330 ページの「指定した時間後にプロビジョニングを実行する」を参照してください。
- 「日付の指定」。指定したカレンダー日付にプロビジョニングを実行します。手順については、330 ページの「指定したカレンダー日付にプロビジョニングを実行する」を参照してください。
- 「属性の指定」。ユーザービューの属性値に基づいて指定した日時にプロビジョニングを実行します。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。

  手順については、331 ページの「属性の指定によってプロビジョニング日時を決定する」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、プロビジョニングの実行を遅延します。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。

  手順については、332 ページの「規則の評価によってプロビジョニング日時を決定する」を参照してください。

「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。

指定された経過時間

この節では、特定の時間後にプロビジョニングを実行する手順について説明します。

▼ 指定した時間後にプロビジョニングを実行する

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、2 時間後に新しいユーザーをプロビジョニングするには、次の図に示す情報を指定します。

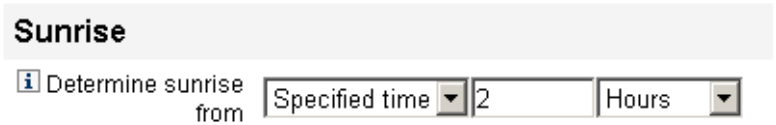


図 9–25　2 時間後の新しいユーザーのプロビジョニング

▼ 指定したカレンダー日付にプロビジョニングを実行する

この節では、特定の日付にプロビジョニングを実行する手順について説明します。

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するには、次の情報を指定します。

図 9–26 日付による新しいユーザーのプロビジョニング

▼ 属性の指定によってプロビジョニング日時を決定する

この節では、ユーザーアカウントデータの属性値に基づいてプロビジョニング日時を決定する手順について説明します。

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。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」チェックボックスとメニュー。属性値の日付形式文字列を指定できます (必要に応じて)。

「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リストについては、製品の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、次の図に示す情報を指定します。

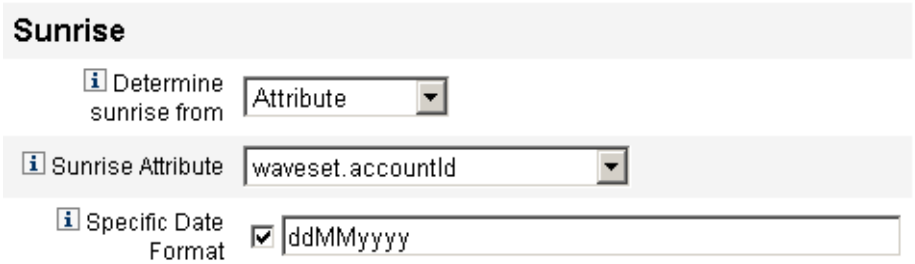


図 9–27 属性による新しいユーザーのプロビジョニング

▼ 規則の評価によってプロビジョニング日時を決定する

この節では、特定の規則を評価することによってプロビジョニング日時を決定する手順について説明します。

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。システムに現在定義されている規則のリストが返されます。
- 「特定の日付形式」チェックボックスとメニュー。規則が返す値の日付形式文字列を指定できます (必要に応じて)。

「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リストについては、製品の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、次の図に示す情報を指定します。

図 9–28 規則の使用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

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」。指定した時間後にプロビジョニングを解除します。手順については、330 ページの「指定した時間後にプロビジョニングを実行する」を参照してください。
- 「指定された日」。指定したカレンダー日付にプロビジョニングを解除します。手順については、330 ページの「指定したカレンダー日付にプロビジョニングを実行する」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値に基づいて、指定した日時にプロビジョニングを解除します。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、331 ページの「属性の指定によってプロビジョニング日時を決定する」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遅延します。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、332 ページの「規則の評価によってプロビジョニング日時を決定する」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。

「データ変換」タブの設定

この節では、タスクテンプレート設定プロセスの一部として利用できる、「データ変換」タブの設定手順を説明します。設定プロセスの開始手順については、302 ページの「タスクテンプレートの設定」を参照してください。

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する場合、「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。

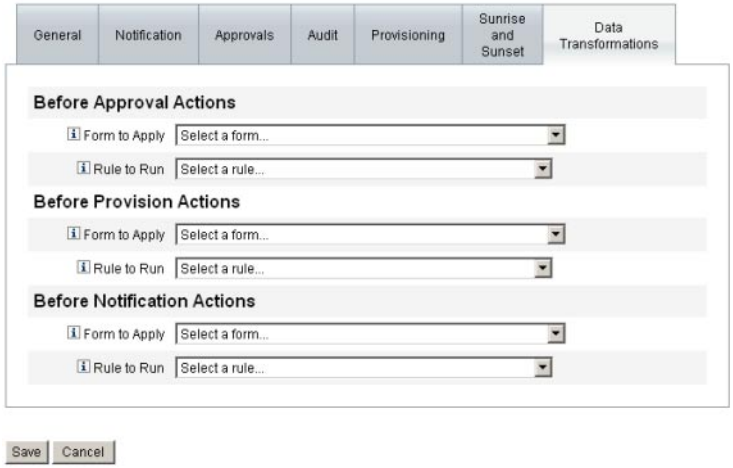


図 9–29 「データ変換」タブ:ユーザー作成テンプレート

このページは、次のセクションで構成されています。

- 「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する場合、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する場合、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する場合、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。システムに現在設定されているフォームのリストが返されます。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。システムに現在設定されている規則のリストが返されます。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。

◆ ◆ ◆ 第 10 章

10 監査ログ

この章では、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。

これらの情報は、次のトピックで構成されています。

- 337 ページの「監査ログの概要」
- 338 ページの「Identity Manager 監査の機能」
- 338 ページの「ワークフローからの監査イベントの作成」
- 344 ページの「監査設定」
- 353 ページの「データベーススキーマ」
- 356 ページの「監査ログ設定」
- 357 ページの「監査ログからのレコードの削除」
- 357 ページの「カスタム監査パブリッシャーの使用」
- 366 ページの「カスタム監査パブリッシャーの開発」

監査ログの概要

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と管理については、第 13 章「アイデンティティー監査: 基本概念」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、Identity Manager の内部コンポーネントによって実行されます。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します。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。詳細については、次の節を参照してください。

ワークフローからの監査イベントの作成

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。この節では、`com.waveset.session.WorkflowServices` アプリケーションを使用して、任意のワークフロープロセスから追加の監査イベントを生成する方法について説明します。

追加の監査イベントは、カスタムワークフローのレポートで必要になる場合があります。ワークフローに監査イベントを追加する方法については、340 ページの「標準監査イベントをログするためのワークフローの変更」を参照してください。

ワークフローレポートのサポートとして、ワークフローに特別な監査イベントを追加することもできます (283 ページの「ワークフローレポート」)。ワークフローレポートでは、ワークフローが完了するまでの時間をレポートします。特別監査イベントは、時間計算で使用するデータの格納に必要です。タイミング監査イベントをワークフローに追加する方法については、341 ページの「タイミング監査イベントをログするためのワークフローの変更」を参照してください。

com.waveset.session.WorkflowServices アプリケーション

com.waveset.session.WorkflowServices アプリケーションは、任意の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 10–1 に、このアプリケーションに指定できる引数を示します。

表 10–1　com.waveset.session.WorkflowServices の引数

引数	種類	説明
op	String	WorkflowServices の操作。audit または auditWorkflow に設定する必要があります。標準ワークフロー監査では audit を使用します。時間計算に必要なタイミング監査イベントの格納には auditWorkflow を使用します。必須。
type	String	監査対象のオブジェクトタイプの名前。監査可能なオブジェクトタイプの一覧については、表 B–5 を参照してください。標準監査イベントのログに必須。
action	String	実行されるアクションの名前。監査可能なアクションの一覧については、表 B–6 を参照してください。必須。
status	String	指定されたアクションの状態名。状態の一覧については、表 B–7 の「結果」列を参照してください。標準監査イベントのログに必須。
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。標準監査イベントのログに必須。
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。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大 5 つまでマップします。

表 10–1 com.waveset.session.WorkflowServices の引数 (続き)

引数	種類	説明
organizations	List	(オプション) 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。
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、監査ログに保存しておく必要がある任意の以前の値になります。

標準監査イベントをログするためのワークフローの変更

ワークフロー内に標準監査イベントを作成するには、ワークフローに次の <Activity> 要素を追加します。

```
<Activity name='createEvent'>
```

次に、<Activity> 要素の入れ子として、com.waveset.session.WorkflowServices アプリケーションを参照する <Action> 要素を記述します。

```
<Action class='com.waveset.session.WorkflowServices'>
```

<Action> 要素の入れ子として、必須およびオプションの <Argument> 要素を記述します。引数の一覧については、表 10–1 を参照してください。

標準監査イベントをログするには、op 引数を audit に設定します。

340 ページの「ワークフローの例」では、標準監査イベントの作成に必要な最小限のコードを示しています。

ワークフローの例

次の例は、簡単なワークフローアクティビティーを示しています。この例では、ResourceAdministrator によって実行される、ADSIResource1 という名前のリソース削除アクティビティーをログに記録するイベントを生成しています。

例 10–1 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'/>
```

例 10–1 単純なワークフローアクティビティー (続き)

```
<Argument name='name' value='ADSIResource1'/> </Action> <Transition to='end'/> </Activity>
```

次の例では、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。

例 10–2 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> </map> </Argument> <Argument name='subject'> <or> <ref>ACTUAL_APPROVER</ref>
<ref>APPROVER</ref> </or>
</Argument> <Argument name='approver' value='$(APPROVER)'/> </Action>
```

タイミング監査イベントをログするためのワークフローの変更

ワークフローレポートのサポートとして、計時イベントをログに記録するようにワークフローを変更できます (283 ページの「ワークフローレポート」)。標準監査イベントではイベントが発生したことのみをログしますが、タイミング監査イベントではイベントの開始時刻と停止時刻を記録して、時間計算の実行を可能にします。計時イベントデータに加えて、標準監査イベントでログに記録される情報の大部分が格納されます。詳細については、343 ページの「タイミング監査イベントで格納される情報」を参照してください。

注 – タイミング監査イベントをログに記録するには、監査を行うワークフロータイプごとに、ワークフローの監査を有効にする必要があります。

- タスクテンプレートを使用して管理者インタフェースで設定できるワークフローの場合は、最初に、監査するワークフローに対応するタスクテンプレートを有効にします。手順については、297 ページの「タスクテンプレートの有効化」を参照してください。

  次に、「ワークフロー全体の監査」チェックボックスを選択して、ワークフローの監査を有効にします。手順については、326 ページの「「監査」タブの設定」を参照してください。
- タスクテンプレートのないワークフローの場合は、そうする代わりに、`auditWorkflow` という名前の変数を定義してその値を `true` に設定します。

ワークフローの監査を行うとパフォーマンスは低下します。

例 10–3 に、タイミング監査イベントの作成に必要なコードを示します。タイミング監査イベントをログするには、`op` 引数を `auditWorkflow` に設定します。

`action` 引数も必須で、次のいずれかの値に設定します。

- `StartWorkflow`
- `EndWorkflow`
- `StartProcess`
- `EndProcess`
- `StartActivity`
- `EndActivity`

`auditconfig.xml` にそのほかの action 引数も定義できます。

例: ワークフローでの監査イベントの開始と停止

例 10–3 は、ワークフローでタイミング監査イベントを有効にする場合を示しています。ワークフローを設定するには、ワークフロー、プロセス、アクティビティーの最初と最後に `auditWorkflow` イベントを追加してください。

`auditWorkflow` の処理は `com.waveset.session.WorkflowServices` で定義されています。詳細については、339 ページの「`com.waveset.session.WorkflowServices` アプリケーション」を参照してください。

例 10–3　ワークフローでのタイミング監査イベントの開始

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/>
<Argument name='action' value='StartWorkflow'/>
```

例 10–3 ワークフローでのタイミング監査イベントの開始 (続き)

```
</Action>
```

ワークフローでタイミング監査イベントのログを停止するには、ワークフローの終わりにある pre-end アクティビティーに例 10–4 のコードを追加します。ワークフローまたはプロセスの設定時には、end アクティビティーには何も追加できません。最後の auditWorkflow イベントの実行後、無条件に end イベントに移行する pre-end アクティビティーを作成してください。

例 10–4 ワークフローでのタイミング監査イベントの停止

```
<Action application='com.waveset.session.WorkflowServices'>
<Argument name='op' value='auditWorkflow'/> <Argument name='action' value='EndWorkflow'/>
</Action>
```

タイミング監査イベントで格納される情報

デフォルトでは、タイミング監査イベントは、次に示す属性など通常の監査イベントで保存されるほとんどの情報をログに記録します。

属性	説明
WORKFLOW	実行中のワークフローの名前
PROCESS	実行中の現在のプロセスの名前
INSTANCEID	実行中のワークフローの一意のインスタンス ID
ACTIVITY	イベントがログされているアクティビティー
MATCH	ワークフローインスタンス内での一意の識別子

これらの属性は auditableAttributesList にあり、logattr テーブルに格納されます。Identity Manager は、workflowAuditAttrConds 属性が定義されているかどうかもチェックします。

プロセスまたはワークフローの 1 つのインスタンス内でアクティビティーを複数回呼び出すことができます。監査イベントを特定のアクティビティーインスタンスと対応させるために、ワークフローインスタンス内で一意の識別子が logattr テーブルに格納されます。

ワークフローの logattr テーブルに追加の属性を格納するには、workflowAuditAttrConds リストを定義します。 これは GenericObjects のリストと見なされます。workflowAuditAttrConds リストに attrName 属性を定義する

と、Identity Manager はコード内のオブジェクトから attrName を取得します。最初に attrName をキーとして使用し、続いて attrName 値を保存します。すべてのキーと値は、大文字の値として記録されます。

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で構成されます。

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。

最上位には次の属性があります。

- 344 ページの「filterConfiguration 属性」
- 350 ページの「extendedTypes 属性」
- 351 ページの「extendedActions 属性」
- 352 ページの「extendedResults 属性」
- 352 ページの「publishers 属性」

filterConfiguration 属性

filterConfiguration 属性には、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の、イベントグループのリストを指定します。filterConfiguration 属性に指定した各グループには、表 10–2 に示す属性が含まれます。

表 10–2 filterConfiguration 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 (String)– objectType の名前。 ■ actions (List)– 1 つ以上のアクションのリスト。 ■ results (List)– 1 つ以上の結果のリスト。

例 10–5 に、デフォルトのリソース管理グループを示します。

例 10–5 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、デフォルトの監査イベントグループが用意されています。これらのイベントグループと、イベントグループ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。

- 346 ページの「アカウント管理グループ」
- 346 ページの「アイデンティティーシステム外部での変更グループ」
- 346 ページの「コンプライアンス管理グループ」
- 347 ページの「設定管理グループ」
- 347 ページの「イベント管理グループ」
- 348 ページの「ログイン/ログオフグループ」
- 348 ページの「パスワード管理グループ」
- 348 ページの「リソース管理グループ」
- 348 ページの「ロール管理グループ」
- 349 ページの「セキュリティー管理グループ」
- 349 ページの「サービスプロバイダ グループ」
- 349 ページの「タスク管理グループ」

監査イベントグループは、Identity Manager 管理者インタフェースの「監査設定」ページ (「設定」 > 「監査」) で設定できます。手順については、109 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。

また、「監査設定」ページでは、成功したイベントと失敗したイベントをグループごとに設定できます。このインタフェースでは、グループで有効にしたイベントの追加や変更はサポートされていません。これらの操作は、Identity Manager デバッグページ (43 ページの「Identity Manager デバッグページ」) を使用して実行できます。

注 – 監査イベントグループに選択できるアクションのすべてが、ログレコードに記録されるとは限りません。また、「すべてのアクション」オプションを選択しても、一覧に表示されたすべてのアクションが、すべての監査イベントグループで利用可能になるわけではありません。

アカウント管理グループ

このグループはデフォルトで有効になっています。

表 10–3 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
Encryption Key	すべてのアクション
Identity System Account	すべてのアクション
Resource Account	承認、作成、削除、無効化、有効化、変更、拒否、名前の変更、ロック解除
Workflow Case	アクティビティーの終了、プロセスの終了、ワークフローの終了、アクティビティーの開始、プロセスの開始、ワークフローの開始
User	承認、作成、削除、無効化、有効化、変更、拒否、名前の変更

アイデンティティーシステム外部での変更グループ

このグループはデフォルトで無効になっています。

表 10–4 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

コンプライアンス管理グループ

このグループはデフォルトで有効になっています。

表 10–5 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
Audit Policy	すべてのアクション
AccessScan	すべてのアクション
ComplianceViolation	すべてのアクション
Data Exporter	すべてのアクション
UserEntitlement	アテスターによる承認、アテスターによる拒否、リクエストされた是正、リクエストされた再スキャン、終了
Access Review Workflow	すべてのアクション
Remediation Workflow	すべてのアクション

設定管理グループ

このグループはデフォルトで有効になっています。

表 10–6 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
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	インポート
Log	すべてのアクション

イベント管理グループ

このグループはデフォルトで有効になっています。

表 10–7 デフォルトのイベント管理イベントグループ

種類	アクション
Email	通知

表 10–7 デフォルトのイベント管理イベントグループ (続き)

種類	アクション
TestNotification	通知

ログイン/ログオフグループ

このグループはデフォルトで有効になっています。

表 10–8 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	資格失効、ロック、ログイン、ログアウト、ロック解除、ユーザー名の復元

パスワード管理グループ

このグループはデフォルトで有効になっています。

表 10–9 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、パスワードのリセット

リソース管理グループ

このグループはデフォルトで有効になっています。

表 10–10 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
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
Workflow Case	アクティビティーの終了、プロセスの終了、ワークフローの終了、アクティビティーの開始、プロセスの開始、ワークフローの開始

ロール管理グループ

このグループはデフォルトで無効になっています。

表 10–11 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グループ

このグループはデフォルトで有効になっています。

表 10–12 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
Capability	すべてのアクション
EncryptionKey	すべてのアクション
Organization	すべてのアクション
Admin Role	すべてのアクション

サービスプロバイダ グループ

このグループはデフォルトで有効になっています。

表 10–13 サービスプロバイダ イベントグループとイベント

種類	アクション
Directory User	チャレンジ応答、作成、削除、変更、操作後コールアウト、操作前コールアウト、秘密の質問の回答の更新、ユーザー名の復元

タスク管理グループ

このグループはデフォルトで無効になっています。

表 10–14 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
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

extendedTypes 属性

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.object.Type 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、各イベントに 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 と 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。拡張された各オブジェクトには、次の表に示す属性が必要になります。

表 10–15 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。予約済みの値については、580 ページの「監査ログデータベースマッピング」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。

例 10–6 に、拡張タイプの Identity Manager アカウントを示します。

例 10–6 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 属性

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 10–16 に示す属性を含んでいる必要があります。

表 10–16 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。
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。 予約済みの値については、580 ページの「監査ログデータベースマッピング」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。

表 10–16 に、ログアウトのアクションを追加する例を示します。

例 10–7　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 属性

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 10–17 に示す属性を含んでいる必要があります。

表 10–17　extendedResults の属性

属性	種類	説明
name	String	結果の名前。 これは AuditEvents での状態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 属性

publishers リスト中の各項目は汎用オブジェクトです。各 publishers オブジェクトには次の属性があります。

表 10–18　publishers の属性

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。

表 10–18 publishers の属性 (続き)

属性	種類	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

監査データを格納する Identity Manager リポジトリには、次の 2 つのテーブルがあります。

- waveset.log– イベントの詳細のほとんどを格納します。
- waveset.logattr– 各イベントが属する組織の ID を格納します。

これらのテーブルについてはこの節で説明します。

監査ログデータがこれらのテーブルに指定された列の長さ制限を超えると、Identity Manager は 制限に合わせてデータを切り捨てます。監査ログの切り捨てについては、356 ページの「監査ログの切り捨て」を参照してください。

監査ログには、列の長さ制限を変更できる列がいくつかあります。これらの列の詳細と、長さ制限を変更する方法については、356 ページの「監査ログ設定」を参照してください。

waveset.log テーブル

この節では、waveset.log テーブルで使用される列名とデータ型を説明します。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一覧については、付録 B 「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。キーの定義については、580 ページの「監査ログデータベースマッピング」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。
- actionDateTimeVARCHAR(21) – 上記のアクションが実行された日時。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) – 操作中に使用されたリソース名 (該当する場合)。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) – 影響を受けているアカウント ID (該当する場合)。
- server VARCHAR(128) – アクションが実行される (イベントロガーによって自動的に割り当てられた) サーバー。
- message VARCHAR(255*) または CLOB – 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。この列の長さ制限は設定可能です。デフォルトのデータ型は VARCHAR で、デフォルトのサイズ制限は 255 文字です。サイズ制限を調整する方法については、356 ページの「監査ログ設定」を参照してください。
- 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 などのインタフェース)。
- acctAttrChanges VARCHAR(4000) または CLOB – 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。

  次のコード例は、acctAttrChanges 列の値を示しています。

```
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"
```

注 – Identity Manager のインストールで Oracle リポジトリを使用しているときに、監査ログに切り捨てエラーが見つかった場合は、監査ログテーブルの accountAttrChanges フィールドを VARCHAR(4000) から CLOB に変換できます。Identity Manager には、/web/sample ディレクトリにサンプルの DDL スクリプトが用意されています。このスクリプトは、log.acctAttrChanges を VARCHAR(4000) から CLOB に変換します。convert_log_acctAttrChangesCHAR2CLOB.oracle.sql スクリプトは、既存のデータを保存し、4000 文字を超える accountAttrChanges フィールドを読み取ることができます。

この変換はオプションです。切り捨てエラーに気付いたときにだけ実行してください。また、変換スクリプトを実行する前に、影響を受けるテーブルを必ずバックアップしてください。

変換スクリプトを実行したあとに、Web アプリケーションサーバーを停止し、再起動してください。新しいレポートを実行したときに、正しく表示されます。

- acctAttr01label-acctAttr05label VARCHAR(50) – これらの 5 つの追加 NAME スロットは、最大 5 つの属性名を、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。「リソーススキーマの設定」ページで "audit?" 設定を使用して、属性を格上げできます。これにより、属性をデータマイニングに利用できます。
- acctAttr01value-acctAttr05value VARCHAR(128) – ブロブではなく、個別の列に格納されるように最大 5 つの属性値を格上げできる 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。例として、Client IP 名と Session ID 名があります。
- parm01value-parm05value VARCHAR(128*) または CLOB – 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。例として、Client IP 値と Session ID 値があります。これらの列の長さ制限は設定可能です。デフォルトのデータ型は VARCHAR で、デフォルトのサイズ制限は 128 文字です。サイズ制限を調整する方法については、356 ページの「監査ログ設定」を参照してください。
- 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。
- xml BLOB – Identity Manager で内部的に使用されます。

waveset.logattr テーブル

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) – イベントが属する MemberObject グループの ID。

監査ログの切り捨て

監査ログデータの 1 つ以上の列が、指定した列の長さ制限を超えると、その列のデータは制限内になるように切り捨てられます。具体的には、切り捨て後のデータは指定された制限値より 3 文字短くなります。次に列データに省略記号 (...) が付加され、データが切り捨てられたことを示します。

さらに、切り捨てられたレコードを見つけやすいように、その監査レコードの NAME 列の先頭に #TRUNCATED# という文字列が付加されます。

注 – Identity Manager では、UTF–8 エンコーディングを想定して、メッセージを切り捨てる位置を計算します。UTF–8 以外のエンコーディングを使用する設定では、切り捨て後のデータがデータベース内の実際の列サイズをまだ超過する可能性があります。こうした状態が発生すると、切り捨て後のメッセージは監査ログに表示されず、エラーがシステムログに出力されます。

監査ログ設定

監査ログには、リポジトリに大容量のデータを格納するように設定できる列があります。

列の長さ制限の変更

監査ログのいくつかの列では、列の長さの制限を変更できます。長さの制限を変更できる列は次のとおりです。

- message 列
- parmNNvalue 列 (NN = 01、 02、 03、 04、 または 05)
- xml 列

注 – 監査ログ列の詳細については、353 ページの「データベーススキーマ」を参照してください。

列の長さ制限は、RepositoryConfiguration オブジェクトを編集することで変更できます。RepositoryConfiguration オブジェクトの編集方法については、116 ページの「Identity Manager 設定オブジェクトの編集」を参照してください。

- message 列の長さ制限を変更するには、maxLogMessageLength 値を変更します。
- parmNNvalue 列の長さ制限を変更するには、maxLogParmValueLength 値を変更します。5 つの列すべてに同じ制限値が適用されます。(列ごとに長さの値を定義することはできません。
- xml 列の長さ制限を変更するには、maxLogXmlLength 値を変更します。

新しい値を有効にするには、サーバーの再起動が必要です。

RepositoryConfiguration オブジェクト内の列の長さ制限の設定値によって、列に格納できるデータの最大量が決まります。格納されるデータがこれらの設定値を超える場合は、Identity Manager によりデータが切り捨てられます。詳細については、356 ページの「監査ログの切り捨て」を参照してください。

RepositoryConfiguration オブジェクト内の列の長さの設定値を大きくする場合は、データベースの列サイズの設定値が RepositoryConfiguration オブジェクトで設定されるサイズ以上であることも確認してください。

監査ログからのレコードの削除

監査ログは、サイズが大きくなりすぎないよう定期的に切り捨てるようにしてください。監査ログメンテナンスタスクを使用して、監査ログから古いレコードを削除するタスクをスケジュールできます。

1. 管理者インタフェースで、「サーバータスク」、「スケジュールの管理」の順にクリックします。
2. 「スケジューリング可能なタスク」セクションで「監査ログメンテナンスタスク」をクリックします。

   「AuditLog Maintenance Task タスクのスケジュールの新規作成」ページが開きます。
3. フォームに値を入力し、「保存」をクリックします。

カスタム監査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が提供されています。

- 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出力します。
- 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。
- JMX。JMX (Java Management Extensions) クライアントで Identity Manager の監査ログアクティビティーを監視できるように、監査イベントをパブリッシュします。
- 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。

独自のパブリッシャーを作成する場合は、366 ページの「カスタム監査パブリッシャーの開発」を参照してください。

この節では、次のトピックについて説明します。

- 358 ページの「カスタム監査パブリッシャーを有効にする」
- 358 ページの「コンソール、ファイル、JDBC、およびスクリプトのパブリッシャータイプ」
- 359 ページの「JMS パブリッシャータイプ」
- 361 ページの「JMX パブリッシャータイプ」

▼ カスタム監査パブリッシャーを有効にする

カスタム監査パブリッシャーは「監査設定」ページから有効にします。

1. 管理者インタフェースのメインメニューで「設定」をクリックし、二次的なメニューで「監査」をクリックします。
   「監査設定」ページが開きます。

2. ページの下にある「カスタムパブリッシャーの使用」オプションを選択します。
   現在設定されている監査パブリッシャーの一覧表が表示されます。

3. 新しい監査パブリッシャーを設定するには、「新規パブリッシャー」ドロップダウンメニューからカスタムパブリッシャータイプを選択します。
   「新規監査パブリッシャーの設定」フォームに入力します。「OK」をクリックします。

4. 重要:「保存」をクリックして、新しい監査パブリッシャーを保存してください。

コンソール、ファイル、JDBC、およびスクリプトのパブリッシャータイプ

コンソール、ファイル、JDBC、またはスクリプトの監査パブリッシャーを有効にする場合は、358 ページの「カスタム監査パブリッシャーを有効にする」の手順に従ってください。「新規パブリッシャー」ドロップダウンメニューから適切なパブリッシャータイプを選択します。

「新規監査パブリッシャーの設定」フォームに入力します。このフォームの詳細については、i-Helps およびオンラインヘルプを参照してください。

- コンソール監査パブリッシャーは、監査イベントを標準出力または標準エラーに出力します。
- ファイル監査パブリッシャーは、監査イベントをフラットファイルに書き込みます。
- JDBC 監査パブリッシャーは、監査イベントを JDBC データストアに記録します。
- スクリプト監査パブリッシャーでは、JavaScript または BeanShell で記述したカスタムスクリプトで監査イベントを格納できます。

JMS パブリッシャータイプ

JMS 監査ログカスタムパブリッシャーでは、JMS (Java Message Service) キューまたはトピックに監査イベントレコードをパブリッシュできます。

JMS の利点

JMS にパブリッシュすると、Identity Manager サーバーが複数ある環境でより柔軟な相関を実現できます。加えて、JMS はファイル監査ログパブリッシャーの使用が制限される状況でも使用できます。 たとえば、Windows 環境では、サーバーの稼動中にクライアントのレポートツールからログにアクセスできない場合があります。

複数サーバー環境での JMS の利点は次のとおりです。

- JMS のメッセージストアにより、メッセージ記憶領域と検索が一元化および単純化される。
- JMS アーキテクチャーは、サービスにアクセス可能なクライアント数に制限がない。
- JMS プロトコルはファイアウォールその他のネットワークインフラストラクチャーを通過しやすい。

ポイントツーポイントとパブリッシュ/サブスクライブ

Java Message System は 2 つのメッセージングモデルを提供します。ポイントツーポイントのキューイングモデルと、パブリッシュ/サブスクライブのトピックモデルです。Identity Manager は両方のモデルをサポートします。

ポイントツーポイントモデルでは、「プロデューサ」が特定のキューにメッセージを送信し、「コンシューマ」がキューからメッセージを読み取ります。この場合、プロデューサはメッセージの宛先を知っており、メッセージをコンシューマのキューに直接送信します。

ポイントツーポイントモデルの特性は次のとおりです。

- 1 つのコンシューマのみがメッセージを取得する。
- プロデューサは受信側がメッセージを読み取るときに稼動している必要はなく、受信側もメッセージの送信時に稼動している必要はない。
- 正常に処理されたすべてのメッセージの確認応答が受信側で行われる。

これに対し、パブリッシュ/サブスクライブモデルでは、特定のメッセージ「トピック」へのメッセージのパブリッシュをサポートします。0 個以上のサブスクライバが、特定のメッセージトピックのメッセージを受信対象とするための登録を行えます。このモデルでは、パブリッシャーもサブスクライバも互いを認識しません。このモデルの例として、匿名の掲示板があります。

パブリッシュ/サブスクライブモデルの特性は次のとおりです。

- 複数のコンシューマがメッセージを受信できる。
- パブリッシャーとサブスクライバの間に時間的な依存関係が存在する。クライアントがサブスクライブする前に、パブリッシャーでサブスクリプションを作成する必要があります。一度サブスクライブすると、永続サブスクリプションが確立されないかぎり、サブスクライバはメッセージを受信するためにアクティブであり続けます。永続サブスクリプションの場合は、サブスクライバが未接続の間にパブリッシュされたメッセージが、サブスクライバの再接続時に再配信されます。

注 – JMS の詳細については、`http://www.sun.com/software/products/message_queue/index.xml` を参照してください。

JMS パブリッシャータイプの設定

JMS パブリッシャーでは、監査イベントが JMS テキストメッセージにフォーマットされます。次にこれらのテキストメッセージが、設定に応じてキューまたはトピックに送信されます。テキストメッセージは、設定に応じて XML または Universal Logging Format (ULF) としてフォーマットできます。

JMS パブリッシャータイプを有効にするには、358 ページの「カスタム監査パブリッシャーを有効にする」の手順に従って、「新規パブリッシャー」ドロップダウンメニューから「JMS」を選択します。

JMS パブリッシャータイプを設定するには、「新規監査パブリッシャーの設定」フォームに入力します。このフォームの詳細については、i-Helps およびオンラインヘルプを参照してください。

JMX パブリッシャータイプ

JMX 監査ログパブリッシャーは、JMX (Java Management Extensions) クライアントで Identity Manager の監査ログアクティビティーを監視できるように、監査イベントをパブリッシュします。

JMX の説明

JMX (Java Management Extensions) は、アプリケーション、システムオブジェクト、デバイス、およびサービス指向ネットワークの管理や監視を可能にする Java テクノロジです。管理/監視対象のエンティティーは、MBean (Managed Bean) と呼ばれるオブジェクトによって表されます。

Identity Manager の JMX パブリッシャー実装

Identity Manager の JMX 監査ログパブリッシャーでは、イベントの監査ログを監視します。イベントが検出されると、監査イベントレコードが JMX パブリッシャーによって MBean でラップされ、メモリーに保持されている一時履歴も更新されます。JMX クライアントには、イベントごとに個別の短い通知が送信されます。そのイベントが処理対象の場合、JMX クライアントから監査イベントをラップしている MBean に問い合わせを行なって詳細な情報を取得できます。

注 – 監査イベントレコードの詳細については、`com.waveset.object.AuditEvent` Javadoc を参照してください。Javadoc は REF キットから入手できます。REF キットについては、366 ページの「カスタム監査パブリッシャーの開発」を参照してください。

適切な MBean から情報を取得するには、履歴シーケンス番号が必要です。この番号はイベント通知に含まれています。

各イベント通知に含まれる情報は次のとおりです。

- 種類。イベントの種類を示す文字列。文字列は、`AuditEvent.<ObjectType>.<Action>` の形式に従います。`ObjectType` および `Action` は、`com.waveset.AuditEvent` から返されます。たとえば、ロック解除イベントが送信されると、種類は `AuditEvent.LighthouseAccount.Unlock` となります。
- シーケンス番号。MBean への情報の問い合わせに使用する履歴バッファーキー。

▼ JMX パブリッシャータイプを設定する

1 **JMX** パブリッシャータイプを有効にするには、**358** ページの「カスタム監査パブリッシャーを有効にする」の手順に従って、「新規パブリッシャー」ドロップダウンメニューから「**JMX**」を選択します。

2 **JMX** パブリッシャータイプを設定するには、「新規監査パブリッシャーの設定」フォームに入力します。このフォームの詳細については、**i-Helps** およびオンラインヘルプを参照してください。

- 「パブリッシャー名」。JMX 監査イベントパブリッシャーの一意の名前を入力します。
- 「履歴制限」。必要に応じてデフォルト値を変更し、パブリッシャーがメモリーに保持するイベント項目の数を指定します (デフォルトは 100)。

3 「テスト」をクリックして、「パブリッシャー名」が使用可能であることを確認します。

4 「**OK**」をクリックします。「新規監査パブリッシャーの設定」フォームが閉じます。

5 重要:「保存」をクリックします。

JMX クライアントを使用した監査イベントの表示

JMX パブリッシャーの表示には JMX クライアントを使用します。次のスクリーンショットの作成では、JDK 1.5 に含まれている JConsole を使用しました。

JConsole を使用する場合は、`IDM:type=AuditLog` MBean を表示するプロセスへの接続を指定します。JConsole を JMX クライアントとして使用する場合の設定方法については、『Sun Identity Manager 8.1 System Administrator's Guide』の「Viewing JMX Data」を参照してください。

JConsole の「通知」タブをクリックして監査イベントを表示します。通知のシーケンス番号に注意してください。シーケンス番号は、MBean に詳細な情報を問い合わせる際に必要です。

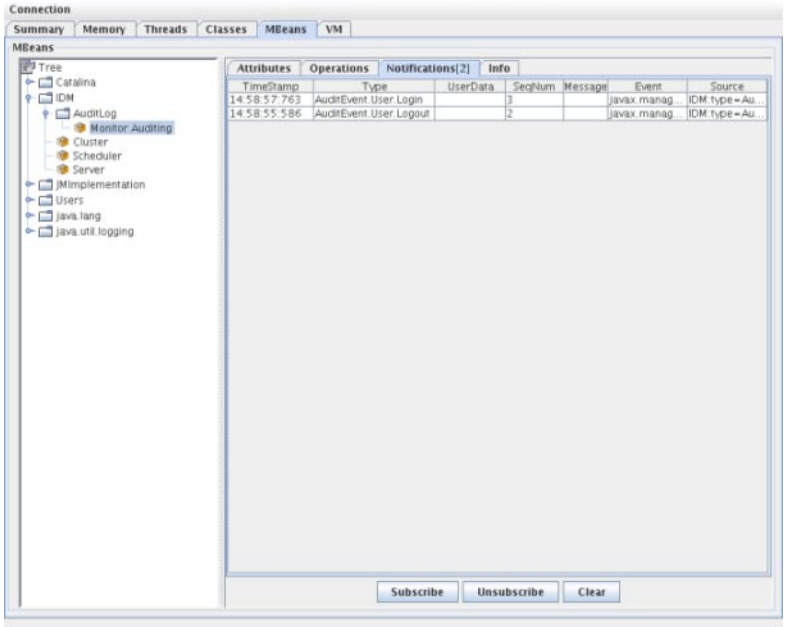


図 **10–1** JConsole による JMX 監査イベント通知の表示

MBean への詳細情報の問い合わせ

JConsole の「Operations」タブをクリックします。通知のシーケンス番号を使用して、イベントの詳細を MBean に照会します。各操作の先頭に「get」が付加され、「シーケンス」番号が唯一のパラメータになります。

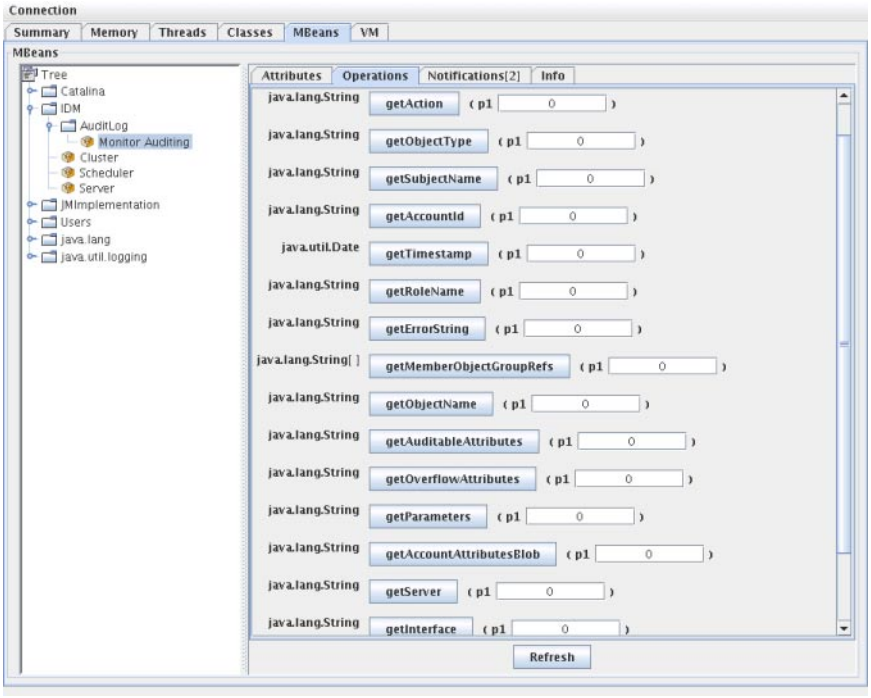


図 **10–2** JConsole による MBean への詳細情報の問い合わせ

MBean は、`com.waveset.object.AuditEvent` クラスに 1 対 1 でマッピングされます。表 10–19 に、MBean が提供する各属性と操作の説明を示します。

表 **10–19** MBeanInfo 属性/操作の説明

属性/操作	説明
`AccountAttributesBlob`	変更された属性のリスト
`AccountId`	イベントと関連する AccountId
`Action`	イベント中に実行されたアクション
`AuditableAttributes`	監査可能な属性
`ErrorString`	エラー文字列
`Interface`	監査インタフェース
`MemberObjectGroupRefs`	メンバーオブジェクトグループ参照
`ObjectName`	オブジェクト名
`ObjectType`	オブジェクトタイプ

表 10–19 MBeanInfo 属性/操作の説明 (続き)

属性/操作	説明
OverflowAttributes	すべてのオーバーフロー属性
Parameters	すべてのパラメータ
Reason	イベントの理由
ResourceName	イベントと関連するリソース
RoleName	イベントと関連するロール
SubjectName	イベントと関連するユーザーまたはサービス
Server	イベントの発生元サーバーの名前
Status	監査イベントのステータス
Timestamp	監査イベントの日付と時刻

Jconsole で、「属性」タブをクリックします。属性の先頭に Current が付加され、システムに送信された最新の監査イベントがその属性に含まれていることを示します。

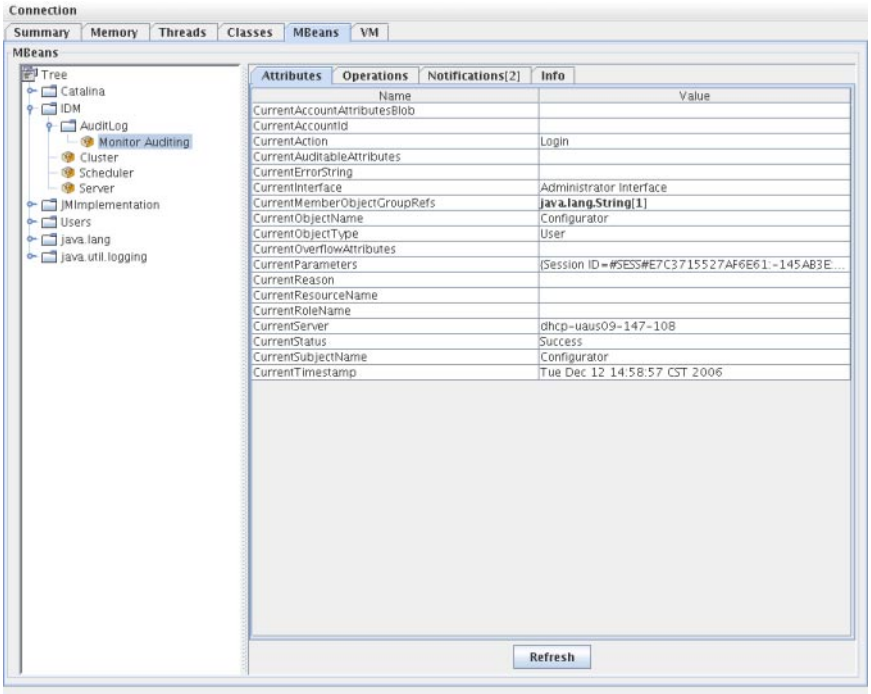


図 10–3　JConsole による MBean 属性の表示

カスタム監査パブリッシャーの開発

この節では、新しいカスタム監査パブリッシャーを Java で作成する方法を説明します。

Identity Manager が提供するコンソール、ファイル、および JDBC のカスタムパブリッシャーは、`AuditLogPublisher` インタフェースを実装します。これらのパブリッシャーのソースコードは REF キットにあります。REF 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。(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。

注 – REF (Resource Extension Facility) キットは、製品 CD の `/REF` ディレクトリまたはインストールイメージにあります。

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。(REF 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 `no-arg` コンストラクタが必要になります。

パブリッシャーのライフサイクル

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. オプションは、`configure(` *Map*`)` メソッドを使用して指定します。
4. イベントは、`publish(` *Map, LoggingErrorHandler*`)` メソッドを使用してパブリッシュされます。
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、同じパブリッシャーオブジェクトに対して一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。

パブリッシャーの設定

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 (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、サーバーの起動時と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

REF 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 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 `no-arg` コンストラクタが必要になります。詳細については、REF 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 11 章

11 PasswordSync

PasswordSync は Windows ドメインで開始されたユーザーパスワードの変更を検出し、それらの変更を Identity Manager に転送します。続いて Identity Manager は、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します。

この章で説明する内容は次のとおりです。

- 369 ページの「PasswordSync とは」
- 373 ページの「インストールの前提条件」
- 375 ページの「Windows での PasswordSync のインストールと設定」
- 386 ページの「アプリケーションサーバーへの PasswordSync の配備」
- 392 ページの「Sun JMS サーバーを使用する PasswordSync の設定」
- 400 ページの「設定のテスト」
- 401 ページの「Windows での PasswordSync のデバッグ」
- 401 ページの「Windows での PasswordSync のアンインストール」
- 402 ページの「PasswordSync についてのよくある質問」

PasswordSync とは

PasswordSync は、Windows Active Directory 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 で定義されたほかのリソースと継続的に同期します。PasswordSync は、Identity Manager と同期されるドメイン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。また PasswordSync は、Identity Manager とは別にインストールする必要があります。

PasswordSync は、各ドメインコントローラに配置される DLL (`lhpwic.dll`) で構成されます。この DLL が Windows からパスワードの更新の通知を受け取り、それを暗号化して、HTTPS 経由で PasswordSync サーブレットに送信します。PasswordSync サーブレットは、Identity Manager を実行しているアプリケーションサーバーに配置されます。

注 – HTTPS の使用が優先されますが、HTTP もサポートされています。

PasswordSync サーブレットは、Identity Manager が認識できる形式に通知を変換します。続いて、サーブレットは次のいずれかの方法を使用して、まだ暗号化されているパスワードの変更を Identity Manager に送信します。

- 直接の方法。サーブレットはネイティブの Identity Manager クラスを使用して、パスワードの変更を直接 Identity Manager に送信します (369 ページの「PasswordSync とは」を参照)。

  直接接続する方法は、メッセージを配信する必要があるシステムが 1 つだけで、メッセージ配信を保証する必要がない、小規模で複雑でない環境にのみ使用することをお勧めします。何らかの理由で直接のメッセージ配信が失敗した場合、メッセージは失われます。バックアップの配信はできません。

- JMS による方法。サーブレットは、JMS (Java Message Service) を使用してパスワード情報を Identity Manager に送信します。JMS を使用して、サーブレットはパスワードの変更を JMS Message Queue に送信します。それとは別に、Identity Manager の JMS リスナーリソースアダプタが、新しいメッセージがないかキューをチェックします。キューで待機しているパスワード変更のメッセージが見つかると、JMS リスナーアダプタはメッセージをキューから取り出し、Identity Manager にインポートします (図 11–2 を参照)。

  大量の要求が発生して、複数のシステムへのメッセージ配信とメッセージ配信の保証が必要となるような複雑な環境では、JMS による方法をお勧めします。JMS Message Queue の可用性を向上できます。メッセージがキューに入っているかぎり、Identity Manager へのメッセージ配信が失敗しても、メッセージを Identity Manager に配信できるまで変更はキューに保持されます。

  JMS は、別個にインストールおよび設定する必要があります。

図 11–1 に、直接接続を示します。この設定では、PasswordSync サーブレットは更新メッセージを直接 Identity Manager に送信します。

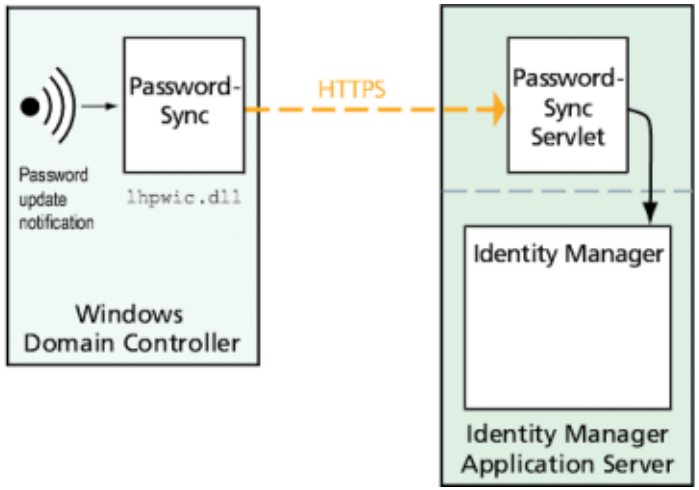


図 11–1　PasswordSync の論理図 (直接接続)

図 11–2 に、JMS 接続を示します。この設定では、PasswordSync サーブレットは更新メッセージを JMS Message Queue に送信します。Identity Manager の JMS リスナーリソースアダプタは、新しいメッセージがないかキューを定期的にチェックします (明るい青色の矢印)。キューはメッセージを Identity Manager に送信して応答します (濃い青色の矢印)。

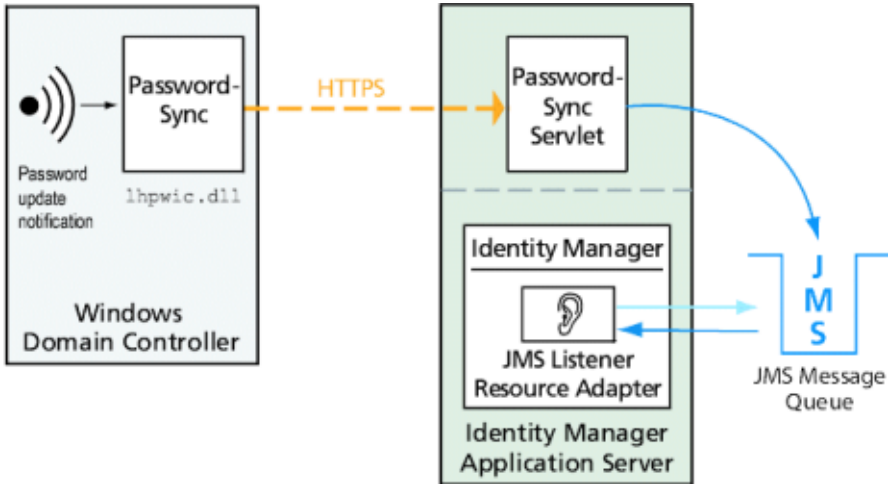


図 11–2　PasswordSync の論理図 (JMS 接続)

Identity Manager はパスワードの変更の通知を受信すると、通知を復号化し、ワークフロータスクを使用して変更を処理します。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 – Windows が更新の通知を送信するのは、パスワードの変更が成功した場合のみです。パスワード変更リクエストがドメインのパスワードポリシーを満たさない場合、Windows はリクエストを拒否し、同期データは Identity Manager に送信されません。

図 11–3 は、パスワード更新の通知を受信したあとに、Identity Manager がワークフローを開始して、ユーザーに電子メールを送信するようすを示しています。

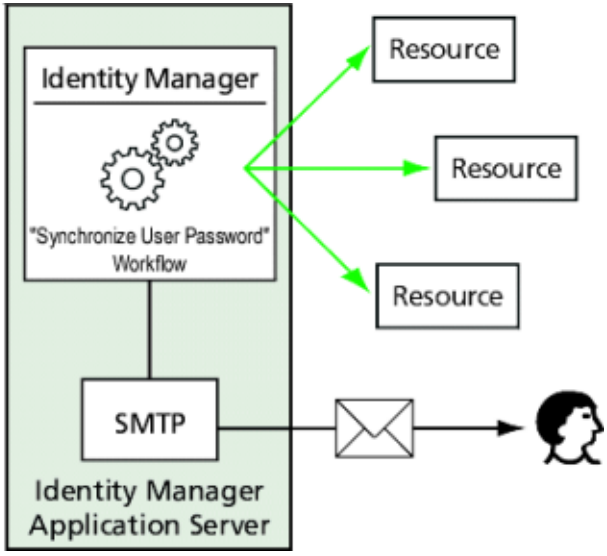


図 11–3　PasswordSync によるワークフローのトリガー

注 – PasswordSync は、名前の末尾が $ (ドル記号) のアカウントについては、アカウントの変更通知をすべて破棄します。$ で終わるアカウント名は、Windows コンピュータアカウントとみなされます。$ で終わるユーザーアカウント名はいずれも Identity Manager に転送されません。

インストールの前提条件

PasswordSync 機能は、Windows 2008、Windows 2003、および Windows 2000 のドメインコントローラ上でのみ設定できます。Windows NT ドメインコントローラのサポートは、Identity Manager の Version 8.0 で終了しました。Identity Manager と同期するドメイン内のプライマリおよびバックアップのドメインコントローラそれぞれに、PasswordSync をインストールする必要があります。HTTPS を使用するよう PasswordSync を設定することを強くお勧めします。

注 – すべてのドメインコントローラで、バージョン 7.1.1 より古いバージョンの PasswordSync をバージョン 7.1.1 以上に更新する必要があります。

rpcrouter2 サーブレットのサポートはバージョン 8.0 で打ち切られました。将来のリリースでは削除されます。PasswordSync の 7.1.1 以降のバージョンは新しいプロトコルをサポートしています。

JMS を使用する場合、PasswordSync は JMS サーバーと接続できる必要があります。JMS システムの要件については、『Sun Identity Manager 8.1 Resources Reference』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。

また、PasswordSync では、次の操作も必要です。

- 各ドメインコントローラへの Microsoft .NET 1.1 以降のインストール
- 以前のバージョンの PasswordSync の削除

これらの要件については、次の節で詳細に説明します。

Microsoft .NET 1.1 のインストール

PasswordSync を使用するには、Microsoft .NET 1.1 Framework 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。Microsoft .NET 2.0 Framework は、Windows 2008 ドメインコントローラにデフォルトでインストールされます。Windows 2000 ドメインコントローラを使用している場合、Framework はデフォルトではインストールされていません。Microsoft Download Center で、ツールキットをダウンロードできます。

`http://www.microsoft.com/downloads`

注 –

- Framework ツールキットを簡単に見つけるには、検索フィールドに **`.NET Framework Redistributable`** と入力します。
- ツールキットにより .NET Framework がインストールされます。

SSL に関する PasswordSync の設定

機密データは Identity Manager サーバーに送信される前に暗号化されますが、セキュリティー保護された SSL 接続 (HTTPS 接続) を使用するように PasswordSync を設定することをお勧めします。

インポートした SSL 証明書をインストールする方法については、マイクロソフトサポート技術情報の次の [HOWTO] 記事を参照してください。

`http://support.microsoft.com/kb/816794`

PasswordSync をインストールしたら、「PasswordSync Configuration」ダイアログに HTTPS の URL を指定して、SSL 接続が正しく設定されているかをテストできます。手順については、400 ページの「設定のテスト」を参照してください。

PasswordSync の以前のバージョンのアンインストール

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。

- 以前インストールした PasswordSync のバージョンが `IdmPwSync.msi` インストーラをサポートしている場合は、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。
- 以前インストールした PasswordSync のバージョンが `IdmPwSync.msi` インストーラをサポートしていない場合は、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。

Windows での PasswordSync のインストールと設定

この節では、PasswordSync のインストールおよび設定についての情報と手順を説明します。

この情報は、次のように構成されています。

- 375 ページの「PasswordSync 設定アプリケーションをインストールする」
- 376 ページの「PasswordSync を設定する」

▼ PasswordSync 設定アプリケーションをインストールする

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 と同期す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。

以前にインストールしたバージョンの PasswordSync があれば、必ずアンインストールしてから続行してください。

---

1 **Identity Manager** インストールメディアから、次の操作を実行します。

- 32 ビット版の Windows にインストールする場合は、`pwsync\IdmPwSync_x86.msi` をダブルクリックします。
- 64 ビット版の Windows にインストールする場合は、`pwsync\IdmPwSync_x64.msi` をダブルクリックします。

インストールウィザードが起動し、開始ウィンドウに次のナビゲーションボタンが表示されます。

- 「取消し」。いつでも変更を保存せずにウィザードを終了します。
- 「戻る」。1 つ前のダイアログボックスに戻ります。
- 「次へ」。次のダイアログボックスに進みます。

2 開始画面の情報を読み、「次へ」をクリックして「セットアップの種類」ウィンドウを表示します。

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「カスタム」をクリックします。「次へ」をクリックして続行します。

4 「インストール可能」ウィンドウが表示されたら、「インストール」をクリックして製品をインストールします。

5 最後のウィンドウが表示されます。**PasswordSync** の設定を開始できるように「**Launch Configuration Application**」ボックスを選択し、「完了」をクリックしてインストール処理を終了します。

PasswordSync を設定する手順については、第 11 章「PasswordSync」を参照してください。

注 – ダイアログに、変更を有効にするにはシステムの再起動が必要であることを示すメッセージが表示されます。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。

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については、375 ページの「Windows での PasswordSync のインストールと設定」を参照してください。

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
`%$INSTALL_DIR$%\passwordsyncmsgs.dll`	PasswordSync の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()` 関数を実装します

▼ PasswordSync を設定する

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。

1 **PasswordSync** 設定アプリケーションを起動します **(**まだ実行していない場合**)**。

デフォルトでは、設定アプリケーションは「Program Files」、「Sun Identity Manager」、「PasswordSync」、「Configuration」にインストールされています。

注 – JMS を使用しない場合は、設定アプリケーションをコマンド行から起動します。次のように、`-direct` フラグを指定してください。

```
C:\InstallDir\Configure.exe -direct
```

PasswordSync Configuration ウィザードのダイアログが表示されます (図 11–4)。

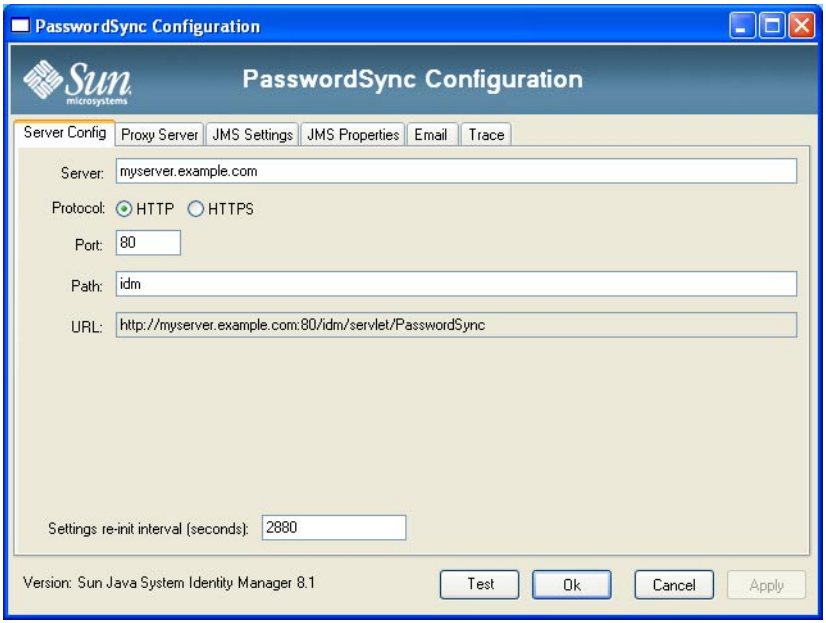


図 11–4　PasswordSync Configuration ウィザード

2　このダイアログのフィールドを、必要に応じて編集します。

次のフィールドがあります。

- 「サーバー」は、Identity Manager がインストールされている完全修飾ホスト名または IP アドレスで置き換える必要があります。
- 「プロトコル」は、Identity Manager とセキュリティー保護された通信を行うかどうかを指定します。

PasswordSync は、HTTP 通信の証明書確認動作の設定をサポートします。HTTPS を有効にすると、次のオプションが表示されます。

- 「Allow revoked certificates」。この設定は、接続の `securityIgnoreCertRevoke` レジストリ値に対応します。デフォルトでは、PasswordSync は失効の問題を無視せず、`securityIgnoreCertRevoke` レジストリ値は 0 に設定されます。

  失効した証明書のメッセージを PasswordSync で無視する場合は、このチェックボックスを選択 (`SECURITY_FLAG_IGNORE_REVOCATION` レジストリ値を 1 に設定) します。

- 「Allow invalid certificates」。この設定は、接続の `SECURITY_FLAG_IGNORE_CERT_CN_INVALID`、`SECURITY_FLAG_IGNORE_CERT_DATE_INVALID`、および `SECURITY_FLAG_IGNORE_UNKNOWN_CA` オプションに影響します。デフォルトでは、PasswordSync は無効な証明書を許可せず、レジストリ値は 0 に設定されます。

  このボックスを選択すると、`securityAllowInvalidCert` レジストリ値が 1 に設定され、多数の安全性確認をパスしていない証明書を PasswordSync で使用できます。本稼働環境では、このオプションを有効にすることは推奨しません。

注 – HTTP プロトコルタイプではこれらの設定は表示されません。また、これらの設定は HTTP 設定に影響しません。

- 「ポート」は、サーバーで使用可能なポート番号を指定します。HTTP では、デフォルトのポートは 80 です。HTTPS では、デフォルトのポートは 443 です。
- 「パス」は、アプリケーションサーバー上の Identity Manager 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。
- 「Settings re-init interval (seconds)」は、PasswordSync の `dll` がレジストリから設定を読み直す頻度を指定します。デフォルト値は 2880 秒 (8 時間) です。

注 – この PasswordSync Configuration ウィザードでは値が秒単位で表示されますが、実際のレジストリの値はミリ秒単位で格納されます。

PasswordSync の `dll` は、`dll` が動作している間、レジストリから設定情報を読み取ります。この間隔の値は、`reinitIntervalMilli` レジストリ値に格納されます。

設定が更新されている間はパスワードを同期できません。このため、パスワード変更の処理にわずかな遅延が生じる場合があります。通常、この遅延は 1 秒未満です。PasswordSync は、更新中に受信したパスワード変更をすべて、更新の完了後すぐに処理します。また、パスワード同期の実行中には、PasswordSync は設定の更新を処理しません。更新は延期され、あとで実行されます。

3 「次へ」をクリックして、プロキシサーバーの設定ページ (図 11–5) を表示し、必要に応じてフィールドを編集します。

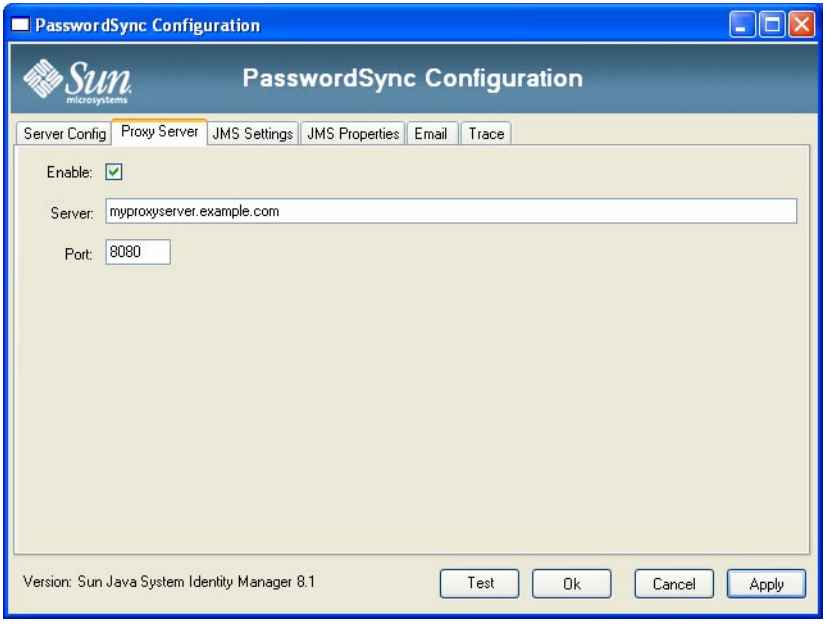


図 11–5 PasswordSync ウィザードの「プロキシサーバー」ダイアログ

次のフィールドがあります。

- 「有効化」。プロキシサーバーが必要な場合は選択します。
- 「サーバー」。プロキシサーバーの完全修飾ホスト名または IP アドレスを入力する必要があります。
- 「ポート」。サーバーで利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 です。

4 「次へ」をクリックします。

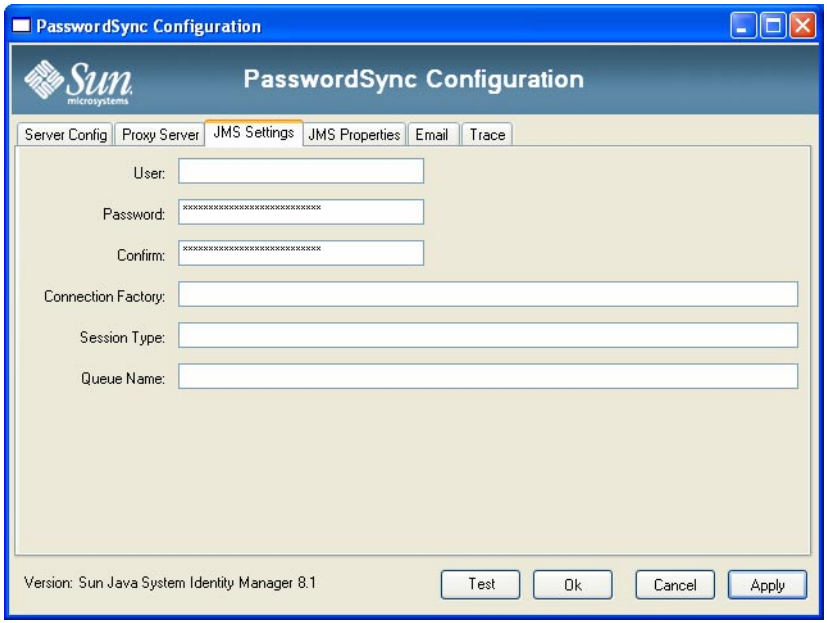


図 11–6　PasswordSync ウィザードの「JMS 設定」ダイアログ

「JMS 設定」ダイアログ (図 11–6) が表示されたら、次のいずれかの操作を実行します。

- 次のフィールドを、必要に応じて編集します。
  - 「**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。
- JMS を使用する予定がなく、`-direct` フラグを指定して設定ウィザードを起動した場合は、「次へ」をクリックして「ユーザー」ダイアログを表示します。図 11–7 の手順に進みます。

5　「次へ」をクリックして、「**JMS プロパティー**」ダイアログを表示します (**図 11–7**)。

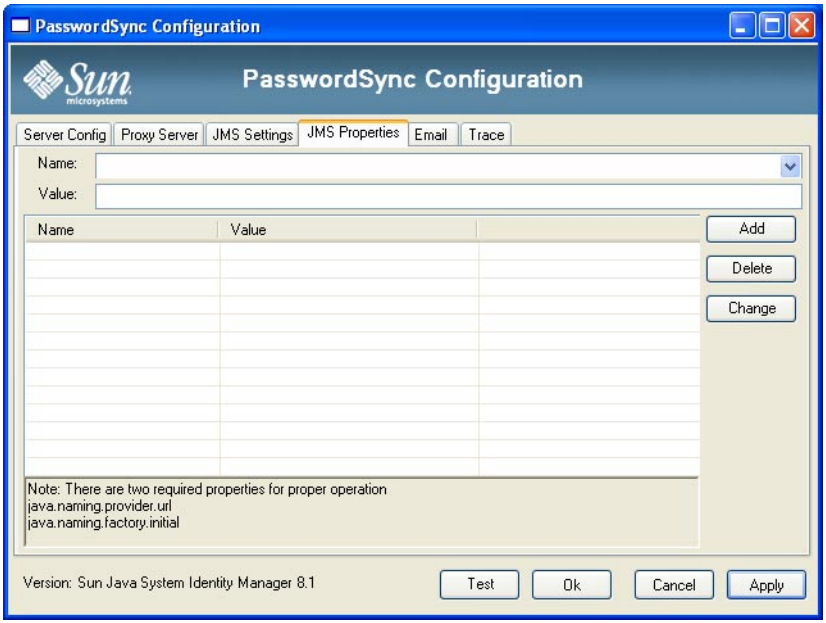


図 11–7　PasswordSync ウィザードの「JMS プロパティー」ダイアログ

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` — JNDI サービスを実行するマシンの URL を指定します。
- `java.naming.factory.initial` — 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) を指定します。

  「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。

6 **JMS を使用する予定がなく、`-direct` フラグを指定して設定ウィザードを起動した場合は、「ユーザー」タブを設定します。その他の場合は、この手順をスキップして次の手順に進みます。**

「User」タブを設定するには、必要に応じてフィールドを編集します。

- 「アカウント ID」。Identity Manager との接続に使用するユーザー名を指定します。
- 「パスワード」。Identity Manager との接続に使用するパスワードを指定します。

7 「次へ」をクリックして、「電子メール」ダイアログ (図 11–8) を表示し、必要に応じてフィールドを編集します。

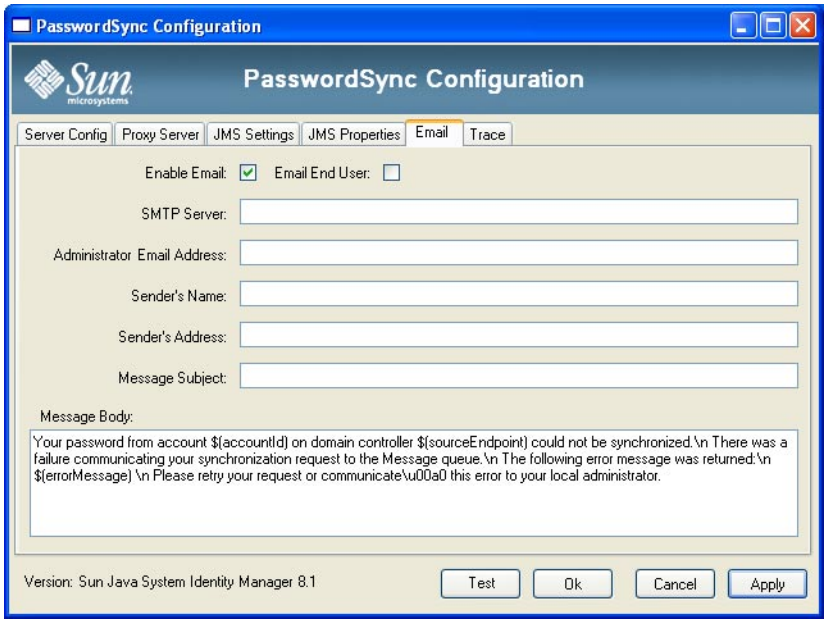


図 11–8 PasswordSync ウィザードの「電子メール」ダイアログ

通信エラーや Identity Manager 外部のその他のエラーにより、ユーザーのパスワード変更が正しく同期されなかったときに電子メール通知を送信するには、次に示す「電子メール」ダイアログのオプションを使用して、通知と電子メールを設定します。

- 「Enable Email」。選択すると、この機能が有効になります。
- 「Email End User」。ユーザーが通知を受け取る場合に選択します。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 サーバー」。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 アドレスを入力します。
- 「Administrator Email Address」。通知の送信先とする電子メールアドレスを入力します。
- 「Sender's Name」。差出人の名前を入力します。
- 「Sender's Address」。差出人の電子メールアドレスを入力します。
- 「Message Subject」。すべての通知に使用する件名を入力します。
- 「Message Body」。通知するテキストを入力します。

メッセージの本文では次の変数を使用できます。

- `$(accountId)` — パスワードを変更しようとしているユーザーのアカウント ID。
- `$(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。トラブルが発生したマシンの特定に役立ちます。
- `$(errorMessage)` — 発生したエラーを説明するエラーメッセージ。

8 「**Trace**」タブをクリックします (図 11–9)。

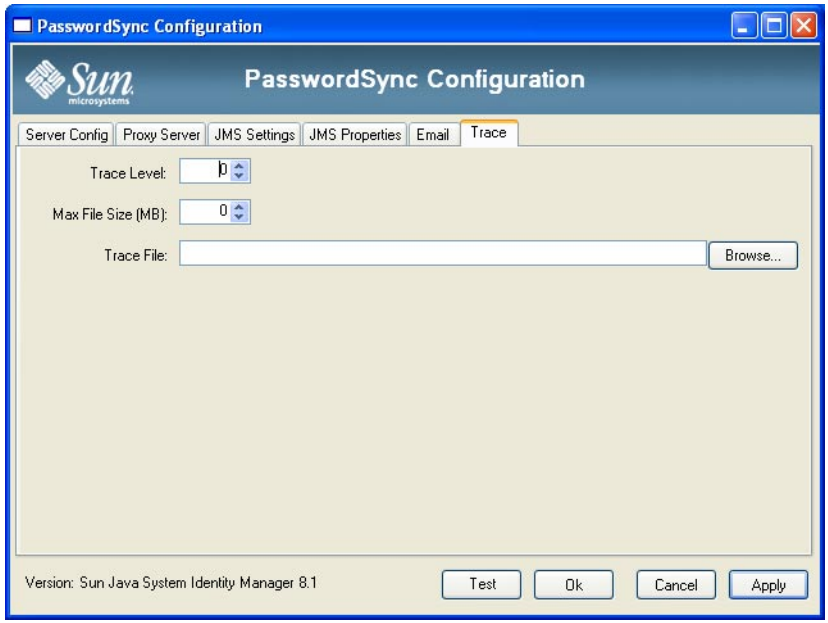


図 11–9 「Trace」タブ

次のフィールドを設定します。

- 「Trace Level」。
- 「Max File Size (MB)」。
- 「Trace File」。

9 「完了」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する場合は、コマンド行に次のコマンドを入力します。

```
C:\InstallDir\Configure.exe -wizard
```

PasswordSync の設定をテストする場合は、400 ページの「設定のテスト」を参照してください。

PasswordSync のサイレントインストール

サイレントインストールを実行するように、PasswordSync インストーラを設定することができます。この機能を使用するには、まず PasswordSync のインストール中に設定パラメータをファイルに記録する必要があります。以降のインストールでは、このファイルを参照して同じ設定を再現します。

注 – サイレントインストールの手順を使用する場合は、サイレントインストールを使用するサーバーごとに完全な製品をインストールする必要があります。設定の記録と再現は、システムにインストールする設定アプリケーションに依存します。

サイレントインストール処理では、Windows の `msiexec` ユーティリティーを使用します。このユーティリティーは、`.msi` ファイルをコマンド行からインストールします。

このユーティリティーの使用方法を表示するには、コマンドプロンプトで `msiexec /?` と入力します。

Microsoft の Web サイトでもドキュメントを入手できます。たとえば、Windows Server 2003 で `msiexec` を使用する場合は、`http://technet.microsoft.com/en-us/library/cc759262.aspx` を参照してください。

▼ インストールパラメータを設定ファイルに記録する

次の手順に従い、インストールウィザードを使用して PasswordSync をインストールします。設定ユーティリティーが設定パラメータを取得して、XML ファイルに書き込みます。

始める前に　インストールする前に、古いバージョンの PasswordSync を削除してください。

1. **PasswordSync のインストールファイル (`.msi` ファイル) があるディレクトリに移動します。**
   詳細については、375 ページの「PasswordSync 設定アプリケーションをインストールする」を参照してください。

2. コマンドプロンプトに次のコマンドを入力します。引数と値は、大文字と小文字を区別します。

   ```
   msiexec /i pwSyncInstallFile CONFIGARGS="-writexml fullPathToFile"
   ```

   各表記の意味は次のとおりです。

- **pwSyncInstallFile** は、PasswordSync のインストールファイルです。(`IdmPwSync_86.msi` または `IdmPwSync_x64.msi`)
- **fullPathToFile** は、XML ファイルを書き込む場所を指定します。

たとえば、次のようにします。

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-writexml c:\tmp\myconfig.xml"
```

3 製品をインストールします。

▼ PasswordSync をサイレントインストールする

始める前に
- インストール設定 XML ファイルを作成している必要があります。手順については、384 ページの「インストールパラメータを設定ファイルに記録する」を参照してください。
- インストールする前に、古いバージョンの PasswordSync を削除してください。

1 作成したインストール設定 **XML** ファイルを、インストーラが読み取ることができる場所にコピーします。

2 コマンドプロンプトに次のコマンドを入力します。引数と値は、大文字と小文字を区別します。

```
msiexec /i pwSyncInstallFile ADDLOCAL="installFeature" CONFIGARGS="-readxml fullPathToFile"
 INSTALLDIR="installDir" /q
```

各表記の意味は次のとおりです。

- **pwSyncInstallFile** は、PasswordSync のインストールファイルです。(`IdmPwSync_86.msi` または `IdmPwSync_x64.msi`)
- **installFeature** は、インストールする PasswordSync の機能を指定します。次のいずれかを選択します。
  - `MainProgram` — インターセプタ `.dll` ファイルのみをインストールします。
  - `Configuration` — 設定アプリケーションのみをインストールします。
  - `ALL` — 完全な製品をインストールします。

  `/q` オプションが指定されている場合は、何も指定しないと、デフォルトで `MainProgram` が使用されます。
- **fullPathToFile** は、設定 XML ファイルのパスを指定します。
- **installDir** は、カスタムインストールディレクトリのフルパスを指定します。省略可能です。
- **/q** は、処理が完了したときにサーバーを自動的に再起動する非 GUI インストールを指定します。このオプションを指定しないとインストールウィザードが表示されますが、設定は定義済みの内容で実行されます。省略可能です。

次に例を示します。

```
msiexec /i IdmPwSync_x86.msi CONFIGARGS="-readxml c:\tmp\myconfig.xml"

msiexec /i IdmPwSync_x86.msi ADDLOCAL="MainProgram"
CONFIGARGS="-readxml c:\tmp\myconfig.xml" /q

msiexec /i IdmPwSync_x64.msi ADDLOCAL="Complete"
CONFIGARGS="-readxml c:\tmp\myconfig.xml"
INSTALLDIR="C:\Program Files\Sun Microsystems\MyCustomInstallDirectory" /q
```

アプリケーションサーバーへの PasswordSync の配備

PasswordSync を Windows ドメインコントローラにインストールしたら、Identity Manager を実行しているアプリケーションサーバーで追加の手順を実行する必要があります。

アプリケーションサーバーに PasswordSync サーブレットをインストールする必要はありません。Identity Manager をインストールしたときに自動的にインストールされています。

ただし、PasswordSync の配備を完了するために、Identity Manager で次の操作を実行する必要があります。

- JMS リスナーアダプタを追加して設定します (JMS 使用時)。
- 「ユーザーパスワード同期」ワークフローを実装します。
- 通知を設定します。

JMS リスナーアダプタの追加と設定

PasswordSync サーブレットが JMS を使用して Identity Manager にメッセージを送信している場合は、Identity Manager の JMS リスナーリソースアダプタを追加する必要があります。JMS リスナーリソースアダプタは、PasswordSync サーブレットによって置かれたメッセージがないか、定期的に JMS Message Queue をチェックします。キューに新しいメッセージがある場合、メッセージは Identity Manager に送信されて処理されます。

▼ JMS リスナーリソースアダプタを追加する

1. **Identity Manager** 管理者インタフェースにログオンします (35 ページの「Identity Manager 管理者インタフェース」)。

2. メインメニューで、「リソース」、「タイプの設定」の順に選択します。
   図 11–10 に示すように、「管理するリソースの設定」ページが表示されます。

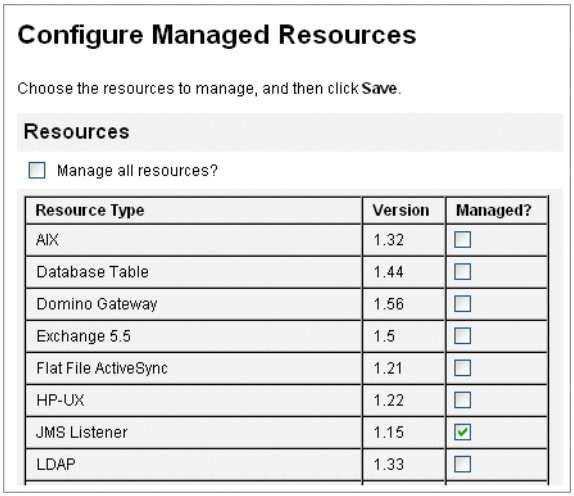


図 11–10 「管理するリソースの設定」ページ

3 「管理しますか?」列で「JMS リスナー」チェックボックスが選択されていることを確認します (図 11–10)。

チェックボックスが選択されていない場合は、チェックボックスを選択して「保存」をクリックします。

4 二次的なメニューから「リソースのリスト」をクリックします。

5 「リソースタイプアクション」ドロップダウンメニューを見つけて、「新規リソース」を選択します。

「新規リソース」ページが表示されます。

6 JMS リスナーアダプタを追加するには、ドロップダウンメニューから「JMS リスナー」を選択し (図 11–11)、「新規」をクリックします。

図 11–11 新規リソースウィザード

7 「リソースパラメータ」ページで次の項目を設定し、「次へ」をクリックします。

- 「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」。初期 JNDI コンテキストを構築するためのプロパティーのセットを定義します。

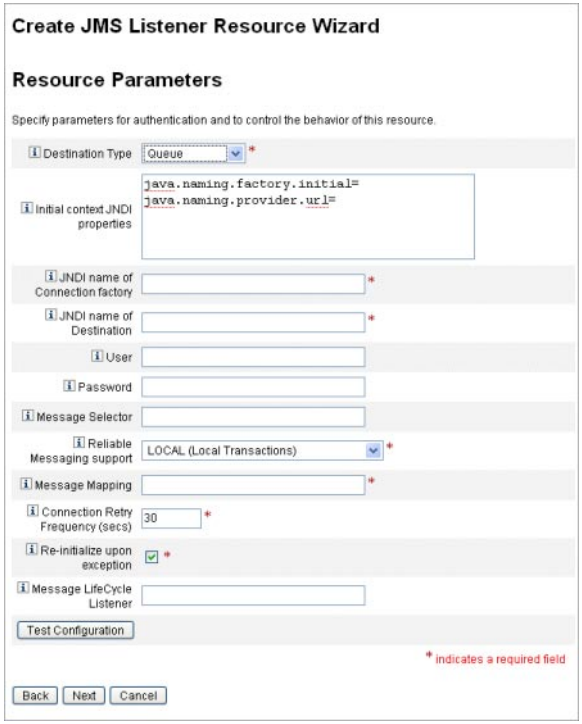
  次の名前と値のペアを定義する必要があります。

  - `java.naming.factory.initial`。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) を指定します。
  - `java.naming.provider.url`。JNDI サービスを実行するマシンの URL を指定します。

    追加プロパティーの定義が必要となる場合があります。プロパティーと値のリストは、JMS サーバーの 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。たとえば、資格およびバインドメソッドを提供するため、次のサンプルプロパティーを指定することが必要な場合があります。

    - `java.naming.security.principal` — バインド DN (例: cn=Directory manager)
    - `java.naming.security.authentication` — バインドメソッド (例: simple)
    - `java.naming.security.credentials` — パスワード
- 「接続ファクトリの JNDI 名」。JMS サーバーで定義されている、接続ファクトリの名前を入力します。
- 「宛先の JNDI 名」。JMS サーバーで定義されている、送信先の名前を入力します。
- 「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 (Local Transactions)」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。



8 ウィザードの「アカウント属性」ページ (図 11–12) で、「属性の追加」をクリックし、次の属性をマップします。これらは、PasswordSyncMessageMapper により **JMS** リスナーアダプタで利用できるようになります。

- IDMAccountId — この属性は、JMS メッセージで渡される resourceAccountId と resourceAccountGUID 属性に基づいて、PasswordSyncMessageMapper によって解釈処理されます。
- password — JMS メッセージで転送される暗号化されたパスワード。

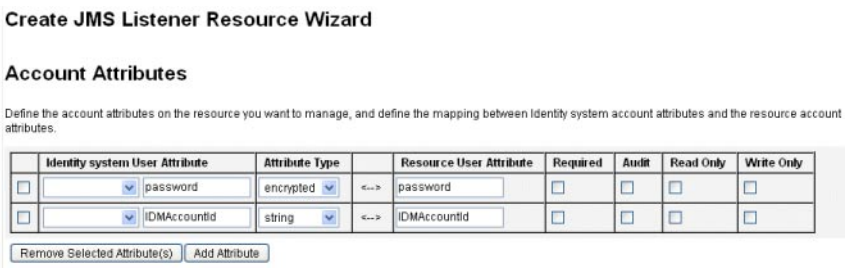


図 11–12 「JMS リスナーリソースの作成」ウィザードの「アカウント属性」ページ

9 「次へ」をクリックします。

ウィザードの「アイデンティーテンプレート」ページが表示されます (図 11–13)。前の手順で追加した属性は、リソースウィザードの「属性マッピング」セクションで使用できます (図 11–13)。

図 11–13 JMS リスナーリソースウィザードの「属性マッピング」

10 「次へ」をクリックして、「アイデンティティーシステムのパラメータ」ページのオプションを必要に応じて設定します。

JMS リスナーリソースアダプタの設定については、『Sun Identity Manager 8.1 Resources Reference』を参照してください。

ユーザーパスワード同期ワークフローの実装

Identity Manager はパスワード変更の通知を受信すると、ユーザーパスワード同期ワークフローを開始します。デフォルトのユーザーパスワード同期ワークフローは、ChangeUserPassword ビューアをチェックアウトしてから、ChangeUserPassword ビューアを再度チェックインします。次に、ワークフ

ローは (最初にパスワードの変更の通知を送信した Windows リソースを除く) すべてのリソースアカウントを処理します。最後に、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示す電子メールをユーザーに送信します。

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、JMS で同期を設定するときに割り当てることができます (398 ページの「Active Sync の設定」を参照)。

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。続いて、修正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については、『Sun Identity Manager Deployment Reference』の第 1 章「Workflow」を参照してください。

通知の設定

Identity Manager には、すべてのリソースでパスワードの変更が成功したかどうかをユーザーに知らせる電子メールテンプレートが 2 種類用意されています。

次のテンプレートです。

- パスワード同期通知
- パスワード同期エラー通知

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。詳細については、第 4 章「ビジネス管理オブジェクトの設定」の 104 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 サーバーを使用する PasswordSync の設定

Identity Manager は Java Message Service (JMS) を使用して、PasswordSync サーブレットからパスワードの変更の通知を受信できます。配信の保証に加えて、JMS はメッセージを複数のシステムに配信できます。

注 – このアダプタの詳細については、『Sun Identity Manager 8.1 Resources Reference』を参照してください。

この節ではサンプルのシナリオを使用して、Sun JMS サーバーを使用する 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。

- 392 ページの「シナリオ例」
- 393 ページの「管理オブジェクトの作成と格納」
- 398 ページの「このシナリオに対する JMS リスナーアダプタの設定」
- 398 ページの「Active Sync の設定」

シナリオ例

JMS サーバーを使用する PasswordSync の設定で一般的な (単純な) 例は、ユーザーが Windows 上で自身のパスワードを変更できるようにして、Identity Manager で新しいパスワードを取得し、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
- 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 1.5 (Java 5.0)

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ています。

- `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)

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

LDAP 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。ファイルを使用している場合、ファイルのすべてのインスタンスが同じである必要があります。

手順については、次を参照してください。

- 393 ページの「LDAP ディレクトリへの管理オブジェクトの格納」
- 395 ページの「ファイルへの管理オブジェクトの格納」

注 –

- この節の手順では、Sun Message Queue がインストール済みであると想定しています。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`) またはコマンド行ツール (`imqobjmgr`) 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 ディレクトリへの管理オブジェクトの格納

PasswordSync と JMS リスナーは、LDAP ディレクトリに格納されている管理オブジェクトを使用するように設定できます。図 11–14 は、この処理を示しています。PasswordSync サーブレットと JMS リスナーアダプタはどちらも、メッセージを送受信するために、LDAP ディレクトリから接続ファクトリとデスティネーション設定を取得する必要があります。

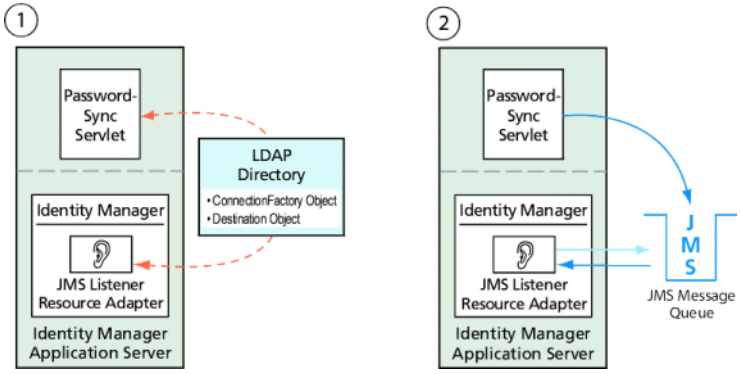


図 11–14　LDAP ディレクトリからの接続ファクトリおよびデスティネーションオブジェクトの取得

Message Queue コマンド行ツールの使用法

この節では、Message Queue コマンド行ツール (imqobjmgr) を使用して、LDAP ディレクトリに管理オブジェクトを格納する方法を説明します。

接続ファクトリオブジェクトの格納

Message Queue コマンド行ツール (imqobjmgr) を開き、394 ページの「接続ファクトリオブジェクトの格納」のコマンドを入力して、接続ファクトリオブジェクトを格納します。

例 11–1　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.
```

394 ページの「接続ファクトリオブジェクトの格納」では、imqAddressList によって JMS サーバー/ブローカのホスト名 (gwenig.coopsrc.com)、ポート (7676)、およびアクセス方法 (jms) を定義しています。

デスティネーションオブジェクトの格納

Message Queue コマンド行ツール (imqobjmgr) で、395 ページの「デスティネーションオブジェクトの格納」のコマンドを入力して、デスティネーションオブジェクトを格納します。

例 11–2 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"
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.
```

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。

LDAP サーバーに管理オブジェクトを格納することについての節はこれで終了です。次の節 (管理オブジェクトをファイルに格納する方法) を省略して、398 ページの「このシナリオに対する JMS リスナーアダプタの設定」の節に進みます。

ファイルへの管理オブジェクトの格納

PasswordSync と JMS リスナーは、ファイルに格納されている管理オブジェクトを使用するように設定できます。管理オブジェクトを LDAP サーバーに格納 (393 ページの「LDAP ディレクトリへの管理オブジェクトの格納」) していない場合は、この節の手順に従います。

接続ファクトリオブジェクトの格納

Message Queue コマンド行ツール (imqobjmgr) を開き、396 ページの「接続ファクトリオブジェクトの格納」のコマンドを入力して、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します。

例 11–3　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
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 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は、396 ページの「ブローカでのデスティネーションの作成」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。このとき、*myTestQueue* がデスティネーションを表します。

例 11–4　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: ディレクトリを使用すると、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 PasswordSync サーブレットと 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それぞれのマシンでもう一度繰り返しても、`.bindings` ファイルを各マシンの適切な場所にコピーしてもかまいません。

- ファイルの場合: Identity Manager PasswordSync サーブレットと Identity Manager サーバーの両方が、同一のサーバー上で実行されている (つまり、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`) 以下に、単一のファイル (Windows と UNIX のどちらでも `.bindings` ファイル) 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

アプリケーションサーバーで JMS リスナーアダプタを設定します。386 ページの「JMS リスナーアダプタの追加と設定」の手順に従います。

Active Sync の設定

次に、同期のために JMS リスナーを設定します。Active Sync は、JMS を使用する場合は必要ですが、直接接続の場合は使用されません。

▼ JMS リスナーで同期を設定する

1. 管理者インタフェースで、メニューから「リソース」をクリックします。
2. 「リソースリスト」で、「**JMS** リスナー」チェックボックスを選択します。
3. 「リソースアクション」リストで、「同期ポリシーの編集」を選択します。
   JMS リスナーリソースの「同期ポリシーの編集」ページが表示されます (図 11–15)。

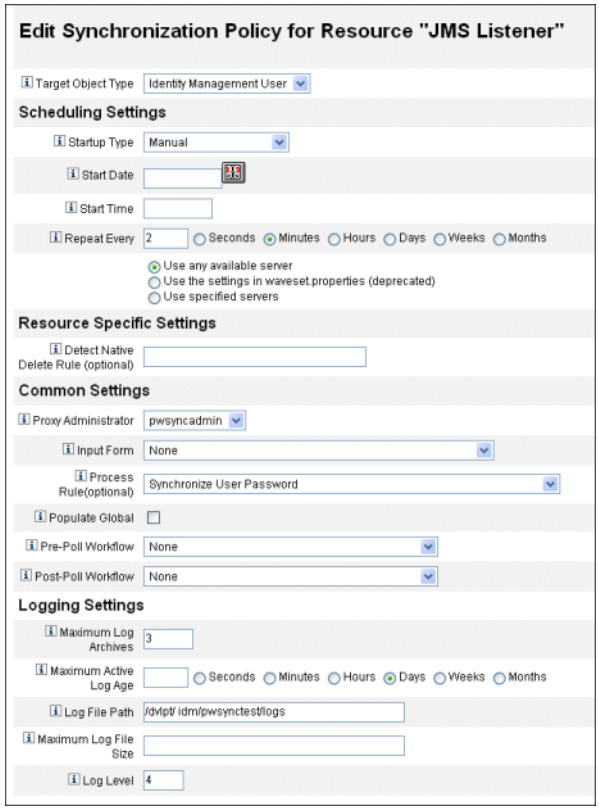


図 11–15　JMS リスナーの Active Sync の設定

4 「共通設定」の「プロキシ管理者」で、pwsyncadmin を選択します。(この管理者は、空のフォームと関連付けられています。

5 「共通設定」の「処理規則」で、リストから「**Synchronize User Password**」を選択します。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。

6 「ログファイルパス」ボックスで、アクティブログとアーカイブされるログのファイルを作成するディレクトリへのパスを指定します。

7 デバッグ目的であれば、「ログレベル」を **4** に設定し、詳細なログを生成します。

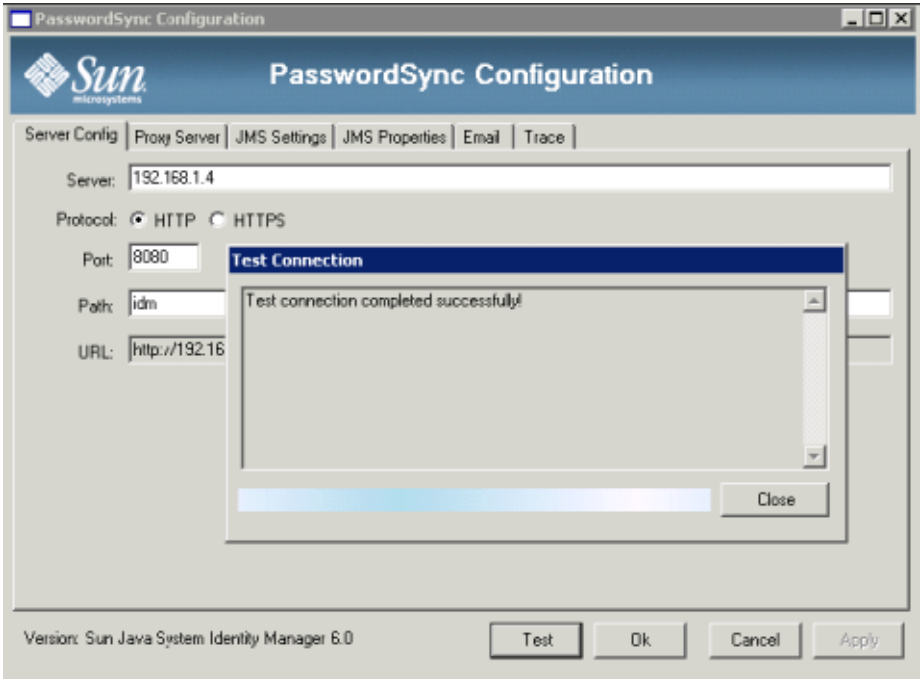
8 「保存」をクリックします。

設定のテスト

Windows の PasswordSync 設定アプリケーションを使用して、Windows 側の設定をデバッグできます。

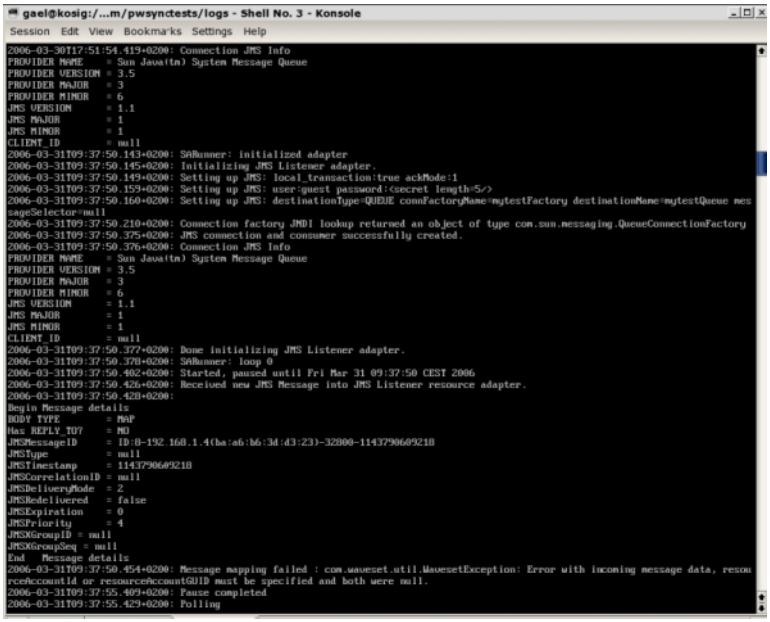
1. PasswordSync 設定アプリケーションを起動します (実行していない場合)。

   デフォルトでは設定アプリケーションは、「Program Files」、「Sun Identity Manager PasswordSync」、「Configuration」にインストールされています。
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. JMS を使用している場合は、「テスト接続」ダイアログが表示され、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。



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され、次のようなデバッグ情報をファイルに生成します。



Windows での PasswordSync のデバッグ

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。イベントビューアの使用法のヘルプについては、Windows ヘルプを参照してください。エラーログエントリのソース名は「PasswordSync」です。

Windows での PasswordSync のトラブルシューティングについては、『Sun Identity Manager 8.1 System Administrator's Guide』を参照してください。

Windows での 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。続いて、「Sun Identity Manager PasswordSync」を選択し、「削除」をクリックします。

注 – また、Identity Manager のインストールメディアを読み込み、`pwsync\IdmPwSync.msi` アイコンをクリックしても、PasswordSync をアンインストール (または再インストール) 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 についてのよくある質問

この節では、PasswordSync についてのよくある質問に対する回答を示します。

質問: Java Messaging Service なしで PasswordSync を実装することはできますか。

回答: 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。

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、386 ページの「アプリケーションサーバーへの PasswordSync の配備」に示した手順は省略してください。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 – これ以降、`-direct` フラグを指定せずに設定アプリケーションを実行する場合は、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、再度 JMS を使わずに PasswordSync を使用できます。

質問: 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。

回答: 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 (value of type REG_MULTI_SZ)
```

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 で定義されるもっとも制約的なパスワードポリシーと同等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。

質問: 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。

回答: はい。PasswordSync 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 `jar` ファイルを必要とします。

質問: 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。

回答: ベストプラクティスは PasswordSync を SSL 上で実行することですが、機密データはすべて、Identity Manager サーバーに送信する前に暗号化されます。

詳細については、374 ページの「SSL に関する PasswordSync の設定」を参照してください。

質問: パスワード変更によって、`com.waveset.exception.ItemNotLocked` が発生する場合があるのはなぜですか。

回答: 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 と通信するためです。

`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 12 章

12 セキュリティー

この章では、Identity Manager の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。

次のトピックで、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。

- 405 ページの「セキュリティー機能」
- 406 ページの「同時ログインセッションの制限」
- 406 ページの「パスワードの管理」
- 407 ページの「パススルー認証」
- 413 ページの「共通リソースの認証の設定」
- 414 ページの「X509 証明書認証の設定」
- 418 ページの「暗号化の使用と管理」
- 423 ページの「サーバー暗号化の管理」
- 427 ページの「認可タイプを使用したオブジェクトのセキュリティー保護」
- 429 ページの「セキュリティーのベストプラクティス」

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。Identity Manager では、1 回の操作で組織または個人のアクセス権限を無効にできます。
- ログインセッションの制限。現在のログインセッションに制限を設定できます。
- アクティブリスク分析。Identity Manager では、活動していないアカウントや疑念のあるパスワード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。
- 総合的なパスワード管理。完全で柔軟なパスワード管理機能により、完全なアクセス制御が実現します。

- アクセス行為を監視するための監査とレポート。アクセス行為についての対象情報を提供するあらゆる種類のレポートを実行できます。(レポート機能の詳細については、第 8 章「レポート」を参照)
- 管理特権の詳細な制御。Identity Manager では、ユーザー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対して単一の機能を割り当てることにより、管理者としての制御能力を付与し管理できます。
- サーバーキーの暗号化。Identity Manager では、「タスク」領域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ー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、以前にアクセスしたページにブラウザの「戻る」機能を使用して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 ユーザーは複数の同時ログインセッションを持つことができます。ただし、システム設定オブジェクトを開き (116 ページの「Identity Manager 設定オブジェクトの編集」)、`security.authn.singleLoginSessionPerApp` 設定属性の値を編集して変更すれば、同時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、ログインアプリケーション名ごとに 1 つの属性を含むオブジェクトです (管理者インタフェース、ユーザーインタフェース、Identity Manager IDE など)。この属性の値を `true` に変更すると、ユーザーごとに 1 つのログインセッションに制限されます。

制限された場合でも、ユーザーは 2 つ以上のセッションにログインできます。 ただし、アクティブで有効な状態なのは最後にログインしたセッションのみです。ユーザーが無効なセッションでアクションを実行すると、そのユーザーは自動的にセッションからログオフされ、セッションが終了します。

パスワードの管理

Identity Manager では、複数のレベルでのパスワード管理が可能です。

- 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 (「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
- 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
  - 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 (任意)
- 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設定する
- 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、ユーザーと管理者に 1 つまたは複数の異なるパスワードによるアクセス権を付与します。

Identity Manager は、次の実装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 (順序づけされた一連のログインモジュール)
- 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の中から 1 つ指定)

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、ユーザーが Identity Manager にログインするときに使用する一連の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から構成されます。

ログイン時に、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セットを確認します。ログインモジュールグループが 1 つだけ設定されている場合は、そのグループが使用され、そこに含まれるログインモジュールはグループに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、ログインモジュールグループに適用されます。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について、ログイン制約規則を適用できないログインモジュールグループが 1 つだけ存在します。

セットのどのログインモジュールグループを処理するかを決定する際、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、Identity Manager はそのログインモジュールグループを処理します。評価が失敗した場合、Identity Manager は各ログインモジュールグループを順番に評価していき、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る (そして続いて使用される) まで評価を続けます。

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 HTTP 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。

例 12–1　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、「セキュリティー」→「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。

- 定義された各 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 セッションの制限の設定

「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使用されていないとき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」および「ログインアプリケーションの修正」ページから、「無効」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にし、それによって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。無効化されたアプリケーションにユーザーがログインしようとすると、そのユーザーはアプリケーションが現在無効になっ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。安全確保のため、管理者ログインは無効にすることができません。

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。

- 各ログインモジュールグループ
- ログインモジュールグループを構成する個々の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選択して編集します。

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。ただし、各ログインモジュールですべてのオプションが使用可能なわけではありません。

- 「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。次の項目があります。
  - 「必須」。成功するにはこのログインモジュールが必須です。成功したか失敗したかにかかわらず、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」。成功するにはこのログインモジュールが必須です。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」。このログインモジュールは成功するために必須ではありません。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。
  - 「オプション」。このログインモジュールは成功するために必須ではありません。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 ユーザーを検索します。これによりユーザーは、LDAP の cn 属性または電子メールアドレス属性を使用して Identity Manager にログインできます (Identity Manager で LDAP へのパススルーが設定されている場合)。

  たとえば、次のように指定するとします。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。

```
cn

mail
```

検索が成功した場合、ユーザーが指定したパスワードを使用してバインドが試行されます。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。この検索も失敗した場合、ログインは失敗します。

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。ユーザーから提供されたログイン情報を、Identity Manager ユーザーにマッピングするためのログイン相関規則を選択します。この規則は、指定されているロジックを使用し Identity Manager ユーザーを検索するために使用されます。この規則は、一致する Identity Manager ユーザーを検索するために使用される、1 つ以上の `AttributeConditions` のリストを返す必要があります。選択する規則は、`LoginCorrelationRule` authType を持つ必要があります。認証されたユーザー ID を Identity Manager ユーザーにマッピングするために Identity Manager が実行する手順の説明については、例 12–2 を参照してください。
- 新規ユーザー命名規則。ログインの一環として新しい Identity Manager ユーザーを自動的に作成するとき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。

注意 – Identity Manager ログインが複数のシステムで認証されるように設定する場合は、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 とパスワードが「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。これらのシステムでは、ユーザーアカウントが最終的にロックされ、ユーザーが Identity Manager を通してログインした場合でも、引き続き成功します。

例 12–2 には、認証されたユーザー ID を Identity Manager ユーザーにマップするために Identity Manager が従う手順について説明する擬似コードが含まれています。

例 12–2 ログインモジュールの処理ロジック

```
if an existing IDM user's ID is the same as the specified user ID

   if that IDM user has a linked resource whose resource name matches the
   resource that was authenticated and whose accountId matches the resource
   accountId returned by successful authentication (e.g. dn), then we have
   found the right IDM user

   otherwise if there is a LoginCorrelationRule associated with the
   configured login module

      evaluate it to see if it maps the login credentials to a single IDM
      user

      otherwise login fails

   otherwise login fails

if the specified userID does not match an existing IDM user's ID

   try to find an IDM user that has a linked resource whose resource
   name matches the resource accountID returned by successful authentication

     if found, then we have found the right IDM user

     otherwise if there is a LoginCorrelationRule associated with the
     configured login module

         evaluate it to see if it maps the login credentials to a single
         IDM user

         otherwise login fails

     otherwise login fails
```

例 12–2 では、システムはユーザーのリンクされたリソース (リソース情報) を使用して、一致する Identity Manager ユーザーを見つけようとします。ただし、リソース情報による方法が失敗し、loginCorrelationRule が設定されている場合、システムは loginCorrelationRule を使用して、一致するユーザーを見つけようとします。

共通リソースの認証の設定

論理的に同一のリソースが複数ある (たとえば、信頼関係を共有する Active Directory ドメインサーバーが複数ある) 場合や、複数のリソースがすべて同一物理ホスト上に置かれている場合、これらのリソースは「共通リソース」であることを指定できます。

リソースのグループを一度だけ試行して認証すればよいことが Identity Manager に認識されるように、共通リソースを宣言してください。そのようにしないと、ユーザーが誤ったパスワードを入力した場合、Identity Manager は同じパスワードを各リソースに対して試行します。これにより、ユーザーが誤ったパスワードを 1 回入力しただけでも、ログインが複数回失敗するためにユーザーのアカウントがロックされることになる場合があります。

共通リソースを使用すると、ユーザーは 1 つの共通リソースに対して認証を行うことができ、Identity Manager は自動的に、共通リソースグループ内の残りのリソースに対して、ユーザーの試行とマッピングを行います。たとえば、Identity Manager ユーザーアカウントが、リソース AD-1 のリソースアカウントにリンクされており、ログインモジュールグループで、ユーザーがリソース AD-2 に対して認証される必要があることが定義されている場合があります。

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 で同じユーザーの accountId を見つけることによって、そのユーザーを AD-1 にもマップすることができます。

注意 – 共通リソースグループ内にリストされるすべてのリソースは、ログインモジュールの定義にも含まれている必要があります。共通リソースの完全なリストがログインモジュールの定義にも記載されていない場合、共通リソース機能は正しく動作しません。

共通リソースは、システム設定オブジェクト (116 ページの「Identity Manager 設定オブジェクトの編集」) で以下の形式で定義できます。

例 12–3　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。

設定の必要条件

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。

▼ クライアント証明書の「クライアント証明書」オプションが選択されていることを確認する

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」領域で、「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」領域で、「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

▼ X509 証明書認証を設定する

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** の **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。

次の値が有効です。

- 「必須」。成功するにはこのログインモジュールが必須です。成功したか失敗したかにかかわらず、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」。成功するにはこのログインモジュールが必須です。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」。このログインモジュールは成功するために必須ではありません。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。
- 「オプション」。このログインモジュールは成功するために必須ではありません。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プロンプトが表示されます。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。user name used to create the new Identity Manager user account という 1 つの文字列が返されます。サンプルの新規ユーザー命名規則は、idm/sample/rules に NewUserNameRules.xml という名前で含まれます。

ログイン相関規則の作成とインポート

Identity Manager の X509 証明書ログインモジュールは、ログイン相関規則を使用して証明書データを該当する Identity Manager ユーザーにマップする方法を決定します。Identity Manager には、Correlate via X509 Certificate subjectDN という名前の組み込み型の相関規則が含まれます。

独自の相関規則を追加することもできます。例として、idm/sample/rules ディレクトリにある LoginCorrelationRules.xml を参照してください。

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。
- 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相関規則に渡されます。

- 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

ログイン相関規則は、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 を使用して、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の問題は、ログインフォーム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。

▼ HTTP リクエスト内のクライアント証明書の属性名を修正する

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** のデバッグ機能 (**43** ページの「**Identity Manager** デバッグページ」) を使用して、LoginConfig オブジェクトを編集します。
3. **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、Identity Manager 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 サーバーおよびゲートウェイでの暗号化の使用および管理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疑問を解決します。

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 12–1 暗号化によって保護されるデータの種類

データ型	RSAMD5	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 Crypto56 ビットキー (PBEwithMD5andDES)
サーバー暗号化キー		Default	設定オプション
ゲートウェイ暗号化キー		Default	設定オプション1
ポリシー辞書単語	はい		
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	

サーバー暗号化キーについてのよくある質問

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。

質問: サーバー暗号化キーとは何ですか？

回答: 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。

質問: サーバー暗号化キーはどこで維持管理されますか？

回答: 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。

質問: 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？

回答: 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。

質問: サーバー暗号化キーはどのようにして更新しますか？

回答: 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423 ページの「サーバー暗号化の管理」を参照してください。

質問: 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？

回答: 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。

質問: 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？

回答: 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。

質問: サーバーキーはどのように保護されますか？

回答: 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」タスクを使用してシステム設定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 暗号化を有効にするには、暗号 PBEwithMD5andDES が使用可能である必要があります。Identity Manager はデフォルトではこの暗号をパッケージ化しませんが、この暗号は、Sun や IBM によって提供される実装など、多くの JCE プロバイダの実装で使用可能な PKCS#5 標準です。

質問: 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？

回答: 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。

質問: 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？

回答: 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ついてのよくある質問

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。

質問: 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?

回答: 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、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。

質問: ゲートウェイキーはどのようにゲートウェイに配布されますか?

回答: 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、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?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、サーバーと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。キーが存在する場合、ゲートウェイはそのキーを使用します。キーが存在しない場合、ゲートウェイはデフォルトキーを使用します。ゲートウェイがレジストリにキーセットを持つと、ゲートウェイはデフォルトキーを使用したセッションの確立を許可しなくなり、第三者が不正なサーバーを設定したりゲートウェイへの接続を確立したりするのを防ぎます。

質問: 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？

回答: 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 (116 ページの「Identity Manager 設定オブジェクトの編集」) 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。

質問: 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？

回答: 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。

質問: ゲートウェイキーはどのように保護されますか？

回答: 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。詳細は、419 ページの「サーバー暗号化キーについてのよくある質問」を参照してください。

質問: 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？

回答: 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。詳細は、419 ページの「サーバー暗号化キーについてのよくある質問」を参照してください。

質問: サーバーキーとゲートウェイキーはどのように破棄されますか？

回答: 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

Identity Manager のサーバー暗号化機能を使用すると、新しい 3DES サーバー暗号化キーを作成し、これらのキーを 3DES、PKCS#5、または AES (Advanced Encryption Standard) 暗号化を使用して暗号化できます。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、「サーバー暗号化の管理」ページから設定します。

▼ 「サーバー暗号化の管理」ページにアクセスする

「サーバー暗号化の管理」ページを開くには、次の手順に従います。

1. メニューバーから「サーバータスク」>「タスクの実行」を選択します。
2. 「利用可能なタスク」ページが表示されたら、「サーバー暗号化の管理」をクリックして「サーバー暗号化の管理」ページを開きます。

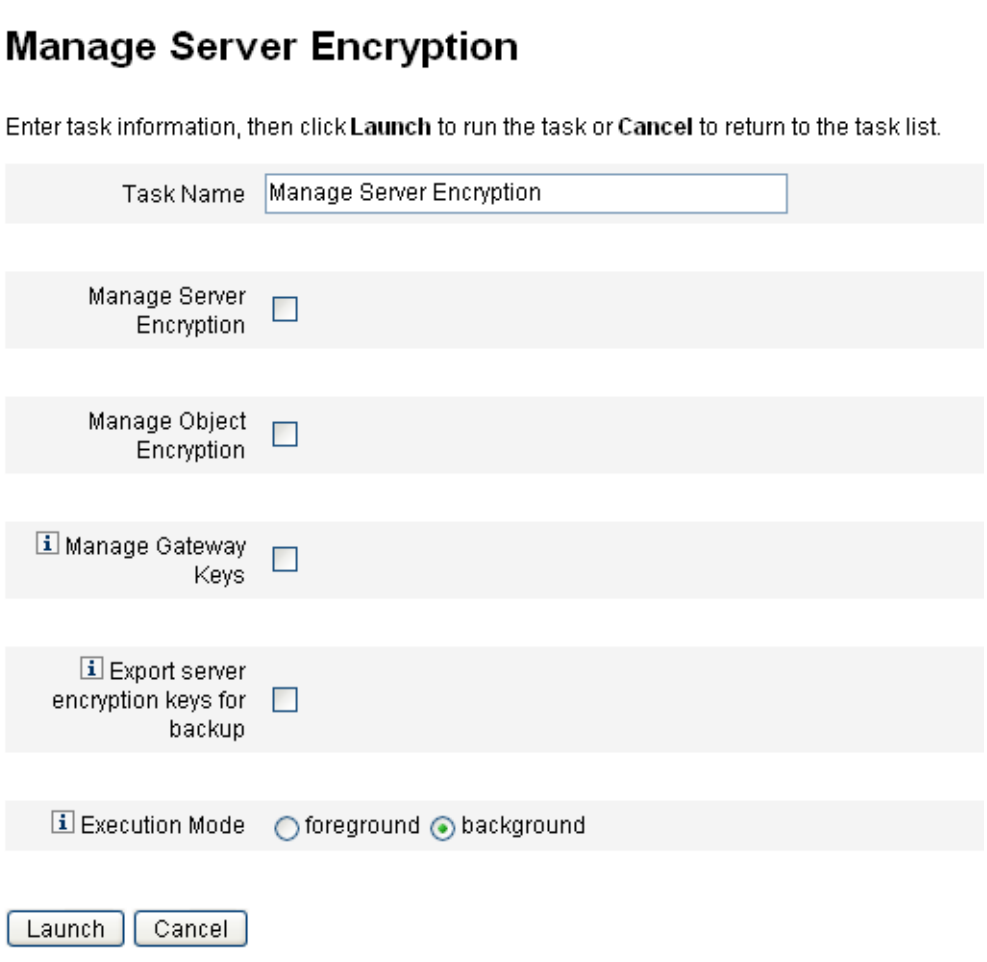


図 12–1 「サーバー暗号化の管理」ページ

▼ サーバー暗号化を設定する

このページを使用してサーバーとオブジェクトの暗号化、ゲートウェイキー、バックアップオプション、および実行モードを設定します。

1 「タスク名」を入力します。

このフィールドのデフォルトは、「サーバー暗号化の管理」です。デフォルト設定を使用しない場合は、別のタスク名を入力できます。

2 次のオプションの 1 つ以上を選択します。

選択に応じて、以下の処理を行うことができます。

- サーバー暗号化の管理. サーバー暗号化を設定するには、このオプションを選択します。

  さらに次のオプションが表示されます。

  - 「サーバー暗号化キーの暗号化」。サーバー暗号化キーの暗号化方法を指定する必要があります。暗号化タイプには、トリプル DES、PKCS#5 (DES)、PKCS#5 (AES) が含まれます。

    注 –

    - このページには、システム上でインスタンス化が可能な暗号化タイプのみが表示されます。たとえば、PKCS#5 (AES) がサポートされない場合は、トリプル DES と PKCS#5 (DES) のみが表示されます。
    - PKCS#5 (AES) では、Identity Manager を実行する JVM の「Unlimited Strength Jurisdiction Policy Files」をダウンロードして設定する必要があります。詳細は、Java ベンダーのマニュアルを参照してください。

      また、PKCS#5 (AES) では、Identity Manager を実行する JVM の JCE プロバイダとして、`Bouncy Castle JCE provider jar` ファイルをインストールして設定する必要があります。この `jar` ファイルは、Identity Manager のインストールイメージにパッケージ化され、*wshome*`/WEB-INF/lib` ディレクトリに配置されます。対応する Java のバージョンで使用するために、2 つの `jar` ファイル、`bcprov-jdk15-137.jar` と `bcprov-jdk16-137.jar` が提供されます。詳細は、Java ベンダーのマニュアルや Bouncy Castle のマニュアルを参照してください。

  - 「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の生成を選択します。このオプションを選択した後に暗号化されるデータは、この鍵を使用して暗号化されます。新しいサーバー暗号化鍵を生成しても、すでに暗号化されているデータに適用された鍵には影響しません。
  - 「セキュリティー保護された新規ランダム PBE パスワードの生成」。サーバーが起動するたびにサーバー固有の秘密キーに基づいて新しいパスワードを生成するには、このオプションを選択します。このオプションを選択しなかった場合や、サーバーがパスワードベースの暗号化を使用するように設定されていない場合、Identity Manager はデフォルトキーを使用してサーバーキーを暗号化します。
- 「オブジェクト暗号化の管理」。再暗号化すべきオブジェクトタイプや使用する暗号化方法を指定するには、このオプションを選択します。
  - 「オブジェクトタイプの暗号化」。表示されている暗号化タイプのいずれかを選択します。暗号化タイプには、トリプル DES (デフォルト)、AES 256 ビットキー、AES、192 ビットキー、AES 128 ビットキーが含まれます。

注 – 192 ビットキーまたは 256 ビットキーを使用する AES では、Identity Manager を実行する JVM の「Unlimited Strength Jurisdiction Policy Files」をダウンロードして設定する必要があります。詳細は、Java ベンダーのマニュアルを参照してください。

このページには、システム上でインスタンス化が可能な暗号化タイプのみが表示されます。たとえば、「Unlimited Strength Jurisdiction Policy Files」を使用する AES 192 ビットキーまたは 256 ビットキーがサポートされない場合は、トリプル DES および AES 128 ビットキーオプションのみが表示されます。

- 「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」。表に一覧表示される 1 つ以上の Identity Manager オブジェクトタイプを選択します。

- 「ゲートウェイ鍵の管理」。ゲートウェイ暗号化を指定するには、このオプションを選択します。

  次のオプションが表示されます。

  - 「ゲートウェイ鍵オプションの選択」。次のオプションのいずれかを選択します。
    - 「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鍵を生成し、その鍵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鍵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鍵の更新を強制する場合は、このオプションを選択します。
  - 「ゲートウェイ鍵のタイプ」。表示されているキータイプのいずれかを選択します。キータイプには、トリプル DES、AES 256 ビットキー、AES、192 ビットキー、AES 128 ビットキーが含まれます。

注 – 192 ビットキーまたは 256 ビットキーを使用する AES では、Identity Manager を実行する JVM の「Unlimited Strength Jurisdiction Policy Files」をダウンロードして設定する必要があります。詳細は、Java ベンダーのマニュアルを参照してください。

このページには、システム上でインスタンス化が可能な暗号化タイプのみが表示されます。たとえば、「Unlimited Strength Jurisdiction Policy Files」を使用する AES 192 ビットキーまたは 256 ビットキーがサポートされない場合は、トリプル DES および AES 128 ビットキーオプションのみが表示されます。

- 「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には、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、鍵のエクスポート先となるパスとファイル名を指定するための追加フィールドが表示されます。

注 – PKCS#5 暗号化を使用していて、新しいサーバー暗号化キーを生成および設定するように選択した場合は、このオプションを選択します。さらに、エクスポートした鍵を取り外し可能な媒体に保存し、ネットワーク上ではない安全な場所に保管してください。

3 「実行モード」を選択します。

このタスクは、フォアグラウンドまたはバックグラウンド (デフォルト設定) で実行できます。

注 – 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。

4 このページでオプションの設定が終了したら、「起動」をクリックします。

認可タイプを使用したオブジェクトのセキュリティー保護

通常は `AdminGroup` 機能で指定した権限を使用して、設定、規則、`TaskDefinition` などの Identity Manager の `objectType` に対するアクセス権を付与します。ただし、1 つ以上の管理する組織内にある Identity Manager `objectType` のすべてのオブジェクトに対してアクセス権を付与するのは範囲が広すぎます。

認可タイプ (`AuthType`) を使用すると、特定の Identity Manager `objectType` に関して、オブジェクトのサブセットに対するアクセスの範囲を指定したり、制限したり

することができます。たとえば、ユーザーフォームでの選択元になる規則を作成している場合、ユーザーの管理範囲内にあるすべての規則に対しては、ユーザーにアクセスを付与したくない場合があります。

新しい認可タイプを定義するには、Identity Manager リポジトリで AuthorizationTypes 設定オブジェクトを編集し、新しい <AuthType> 要素を追加します。

この要素には次の 2 つのプロパティーが必要です。

- 新しい認可タイプの名前
- 新しい要素で拡張または範囲の指定を行う、既存の認可タイプまたは objectType

たとえば、Rule を拡張する Marketing Rule という名前の新しい Rule 認可タイプを追加する場合は、次のように定義します。

```
<AuthType name='Marketing Rule' extends='Rule'/>
```

次に、使用するために認可タイプを有効にするには、その認可タイプを 2 つの場所で参照する必要があります。

- 新しい認可タイプに対する権限を 1 つ以上与えるカスタム AdminGroup 機能の内部
- このタイプであるべきオブジェクトの内部

以下に、両方の参照の例を示します。最初の例は、Marketing Rule に対するアクセス権を与える AdminGroup 機能の定義を示しています。

例 12–4 AdminGroup 機能の定義

```
<AdminGroup name='Marketing Admin'>
  <Permissions>
    <Permission type='Marketing Rule' rights='View,List,Connect,Disconnect/>
  </Permissions>
  <AdminGroups>
    <ObjectRef type='AdminGroup' id='#ID#Account Administrator'/>
  </AdminGroups>
</AdminGroup>
```

次の例は、Rule または Marketing Rule に対するアクセス権を付与されているため、ユーザーがオブジェクトにアクセスできるようになる Rule 定義を示しています。

例 12–5 Rule 定義

```
<Rule name='Competitive Analysis Info' authType='Marketing Rule'>
 ...
</Rule>
```

注 – 親の認可タイプに対して、または認可タイプによって拡張された静的タイプに対してアクセス権を付与されたすべてのユーザーは、子であるすべての認可タイプに対して同じ権限を持つことになります。このため、前の例を使用すると、`Rule` に対する権限を付与されたユーザーはすべて、`Marketing Rule` に対しても同じ権限を持つことになります。ただしその逆は成り立ちません。

セキュリティーのベストプラクティス

Identity Manager 管理者は、設定時とそれ以降に次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。

設定時

設定時のセキュリティーリスクを軽減するには、次の推奨事項に従います。

- 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、組織階層を設定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

実行時のセキュリティーリスクを軽減するには、次の推奨事項に従います。

- 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。

▼ セッションタイムアウト値を変更する

1. `web.xml file` を編集します。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 13 章

13 アイデンティティー監査: 基本概念

この章では、アイデンティティー監査と監査の管理の背景にある概念について紹介します。監査の管理を使用すると、企業情報システムおよびアプリケーション全体にわたり、監査とコンプライアンスを監視および管理できます。

この章では、次の概念およびタスクについて説明します。

- 431 ページの「アイデンティティー監査について」
- 432 ページの「アイデンティティー監査の目的」
- 433 ページの「アイデンティティー監査について」
- 435 ページの「管理者インタフェースでのアイデンティティー監査の操作」
- 438 ページの「監査ログの有効化」
- 438 ページの「監査ポリシーについて」

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 の監査機能では、各企業に有効なコンプライアンスソリューションを柔軟な方法で実装できます。

大半の環境で、内部および外部の監査チーム (監査がもっとも重要と考える) 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ための支援を行います。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。

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より、監査のパフォーマンスは以下のように向上します。

- アイデンティティー監査により、コンプライアンス違反が自動的に検出され、すぐに通知が行われることで迅速な是正が促進される

  Identity Manager の監査ポリシー機能で、違反の「規則」 (つまり条件) 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がオンデマンドで提供される

  監査レポートに、違反や例外に関する状態情報の概要が表示され、危険な状態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の自動化によって操作上のリスクが減少する

  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できる

  「レポート」領域で、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が簡素化される

  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できる

  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は、ユーザーアカウントの特権とアクセス権を監査するための機能と、コンプライアンスを維持および保証するための別個の機能を備えています。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。たとえば、次のようにします。

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

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
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、第 6 章「管理」の 214 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す。これらのスキャンでは監査ポリシーが実行され、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 に用意された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

図 13–1 に、ポリシーベースの監査を設定するための論理タスクフローを示します。

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、477 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。

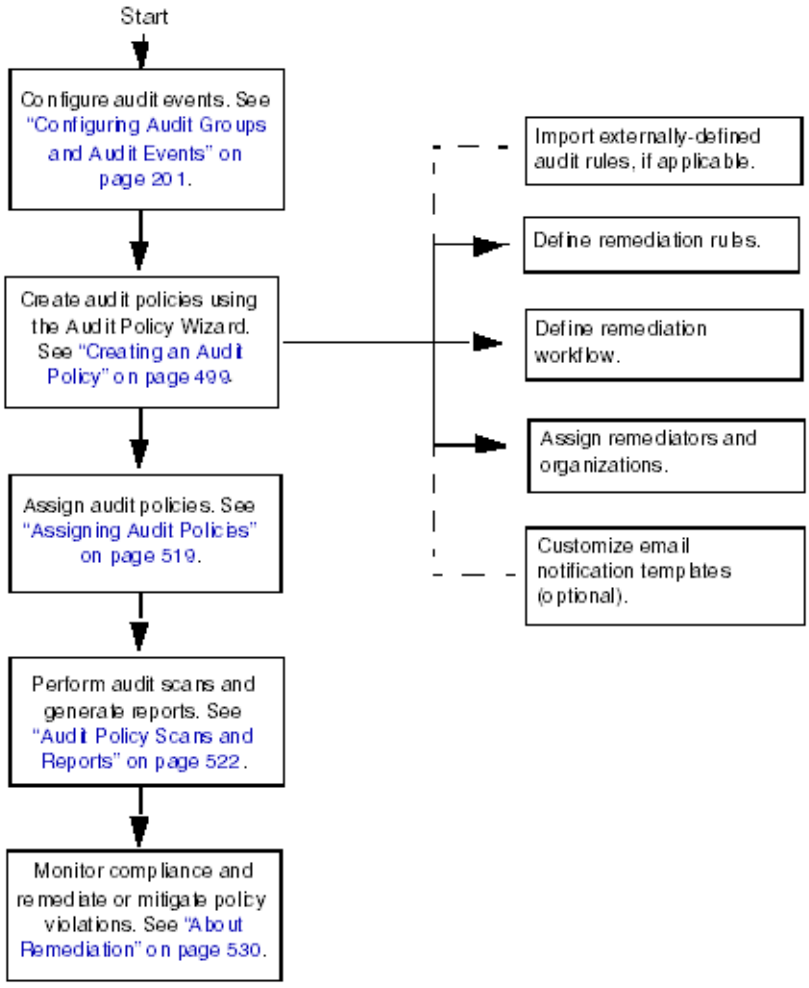


図 13–1　ポリシーベースのコンプライアンスを設定するための論理タスクフロー

管理者インタフェースでのアイデンティティー監査の操作

この節では、管理者インタフェースでアイデンティティー監査機能にアクセスする方法について説明します。アイデンティティー監査で使用される電子メール通知テンプレートについても説明します。

インタフェースの「コンプライアンス」セクションの使用法

監査ポリシーの作成と管理を行うには、Identity Manager 管理者インタフェースの「コンプライアンス」セクションを使用します。

▼ 「コンプライアンス」セクションを使用して監査ポリシーを作成および管理する

1 管理者インタフェースにログインします (41 ページの「Identity Manager エンドユーザーインタフェースへのログイン」)。

2 メニューバーの「コンプライアンス」をクリックします。

「コンプライアンス」セクションでは、次のサブタブ (またはメニュー項目) を使用できます。

- ポリシーの管理
- アクセススキャンの管理
- アクセスレビュー

ポリシーの管理

「ポリシーの管理」ページには、表示と編集の権限を持っているポリシーのリストが表示されます。また、アクセススキャンもこの領域で管理できます。

「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、439 ページの「監査ポリシーのシナリオ例」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、「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、477 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

「アクセスレビュー」タブでは、アクセスレビューの起動、終了、削除、および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、488 ページの「アクセスレビューの管理」を参照してください。

アイデンティティー監査タスクのインタフェースリファレンス

管理者インタフェースでその他のアイデンティティー監査タスクを実行する方法については、表 B–8 を参照してください。このクイックリファレンスを参照すると、さまざまな監査タスクを開始するためにはどこに移動すればよいかがわかります。

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 13–1 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。
ポリシー違反情報	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。
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。

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。監査を設定できるのは、Configure Audit 機能を持つ Identity Manager 管理者です。

Identity Manager には、コンプライアンス管理監査設定グループが用意されています。

コンプライアンス管理グループによって保存されたイベントを表示または修正するには、次の手順を使用します。

1. 管理者インタフェースにログインします (41 ページの「Identity Manager エンドユーザーインタフェースへのログイン」)。
2. メニューバーの「設定」を選択し、「監査」をクリックします。
3. 「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。

注 –

- 監査設定グループの設定については、109 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。
- 監査システムによるイベントの記録方法については、第 10 章「監査ログ」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。監査スキャンは監査ポリシーで定義された条件を使用して、組織内で違反が起きた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。

- ポリシー規則は特定の違反を定義します。ポリシー規則には、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」は、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」は、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です。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。

監査ポリシー規則を使用したポリシーの作成

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。

是正ワークフローによるポリシー違反への対応

ポリシー違反を定義する規則を作成したら、監査スキャン中に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、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。このワークフローは、監査ポリシースキャンに対してデフォルトの是正処理を行います。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、443ページの「Identity Managerへの職務分掌規則のインポート(省略可能)」を参照してください。

是正者の指定

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。是正の詳細については、468ページの「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であり、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ると仮定します。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。

- 一連の規則。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、この領域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。

次の節の「監査ポリシーの操作」では、監査ポリシーウィザードを使用して監査ポリシーを作成する方法について説明します。

◆ ◆ ◆ 第 14 章

14 監査:監査ポリシー

この章では、監査ポリシーウィザードを使用して監査ポリシーの作成、編集、削除、および割り当てを行う方法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。

- 441 ページの「監査ポリシーの操作」
- 442 ページの「監査ポリシーの作成」
- 454 ページの「監査ポリシーの編集」
- 458 ページの「監査ポリシーの削除」
- 459 ページの「監査ポリシーのトラブルシューティング」
- 459 ページの「監査ポリシーの割り当て」

監査ポリシーの操作

監査ポリシーを作成するには、Identity Manager の監査ポリシーウィザードを使用します。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。

監査ポリシー規則

監査ポリシー規則は特定の違反を定義します。ポリシー規則には、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。

監査ポリシーウィザードを使用して簡単な規則を作成したり、Identity Manager IDE や XML エディタを使用してより高度な規則を作成することが可能です。

- 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。

- 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。

監査ポリシーウィザードを使用して作成された規則は、true または false の値を返します。true の値を返すポリシー規則がポリシー違反となります。ただし、Identity Manager IDE を使用すると、監査スキャンやアクセスレビューの間にユーザーをスキップする規則を作成できます。ignore の値を返す監査ポリシー規則は、そのユーザーに対する規則の処理を停止し、次の対象ユーザーに進みます。

監査ポリシー規則の作成については、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。

監査ポリシーの作成

監査ポリシーを作成するには、監査ポリシーウィザードを使用します。

▼ 監査ポリシーウィザードを開く

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。ウィザードにアクセスするには、次の手順を使用します。

1. 管理者インタフェースにログインします (41 ページの「Identity Manager エンドユーザーインタフェースへのログイン」)。
2. 「コンプライアンス」タブをクリックします。
   「ポリシーの管理」サブタブまたはメニューが開きます。
3. 新しい監査ポリシーを作成するには、「新規」をクリックします。

監査ポリシーの作成: 概要

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

十分に計画してから監査ポリシーを作成してください。開始する前に、以下のタスクを完了したことを確認します。

- 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。詳細については、443 ページの「必要な規則を確認する」を参照してください。
- 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。詳細については、443 ページの「Identity Manager への職務分掌規則のインポート (省略可能)」を参照してください。
- 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。第 6 章「管理」の 214 ページの「機能とその管理について」で、必要な機能を確認してください。

▼ 必要な規則を確認する

ポリシーで指定する制限は、作成またはインポートする一連の規則に実装されます。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は、次の手順を実行します。

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。

   監査ポリシーウィザードの外部で監査ポリシー規則を作成する場合は、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。

Identity Manager への職務分掌規則のインポート (省略可能)

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。これらの規則は、Identity Manager の外部で作成し、「設定」タブの「交換ファイルのインポート」オプションを使用してインポートする必要があります。

Identity Manager へのワークフローのインポート (省略可能)

▼ 外部ワークフローをインポートする

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、外部ワークフローをインポートします。XML エディタまたは Identity Manager IDE を使用して、カスタムワークフローを作成できます。

1. `authType='AuditorAdminTask' and add subtype='SUBTYPE_REMEDIATION_WORKFLOW'` を設定します。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。

   a. 管理者インタフェースにログインします (**41** ページの「**Identity Manager** エンドユーザーインタフェースへのログイン」)。

   b. 「設定」タブをクリックし、次に「交換ファイルのインポート」サブタブまたはメニューをクリックします。
   「交換ファイルのインポート」ページが表示されます。

   c. アップロードするワークフローファイルを参照し、「インポート」をクリックします。
   正常にインポートされたワークフローは、監査ポリシーウィザード (442 ページの「監査ポリシーの作成」) の「是正ワークフロー」のオプションリストに表示されます。

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に、新しいポリシーの名前と簡単な説明を入力します (図 14–1)。

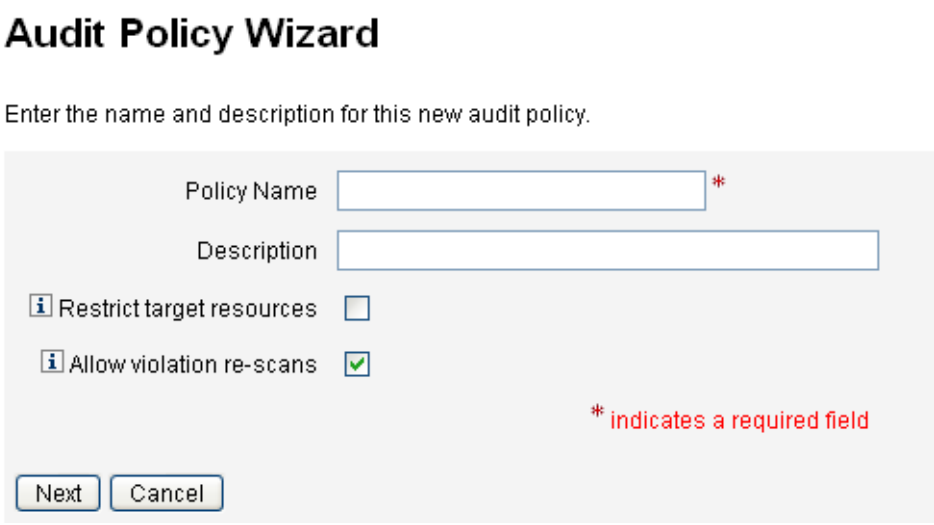


図 14–1　監査ポリシーウィザード: 名前と説明の入力画面

注 – 監査ポリシー名には、次の文字を使用できません。'(アポストロフィー)、.(ピリオド)、|(パイプ)、[(左角括弧)、](右角括弧)、,(コンマ)、:(コロン)、$(ドル記号)、“(二重引用符)、\(バックスラッシュ)、=(等号)。

また、_(下線)、%(パーセント記号)、^(キャレット)、および*(アスタリスク)の使用も避けてください。

スキャン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」オプションを選択します。

違反の是正として、ただちにユーザーを再スキャンする場合は、「違反の再スキャンを許可」オプションを選択します。

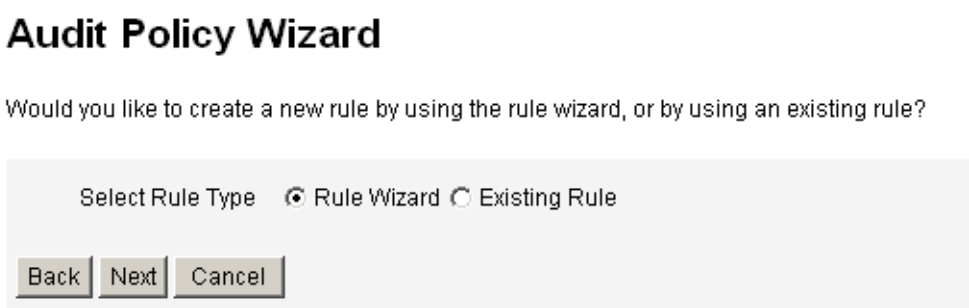
注 – 監査ポリシーでリソースを制限しない場合、スキャンでは、ユーザーがアカウントを持つすべてのリソースがアクセスされます。規則で使用するリソースが少ない場合は、ポリシーの適用をそれらのリソースに限定するほうが効率的です。

「次へ」をクリックして次のページに進みます。

▼ 規則のタイプを選択する

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。

次の図に示すように、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。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。



1 新しい規則を作成するか、既存の規則を使用するかを決定します。

次のオプションのいずれかを選択します。

- 新しい規則を作成する場合は、「規則ウィザード」オプションを選択します (デフォルト)。
- Identity Manager IDE を使用して作成した既存の規則を組み込む場合は、「既存の規則」オプションを選択します。

2 「次へ」をクリックします。

3 手順 1 の選択に基づいて、次のいずれかの操作を行います。

- 「規則ウィザード」を選択した場合は、447 ページの「規則ウィザードを使用した新しい規則を作成する」に進み、説明されている手順に従ってください。
- 「既存の規則」を選択した場合は、446 ページの「既存の規則を選択する」に進み、説明されている手順に従ってください。

既存の規則を選択する

新しいポリシーに既存の規則を含めるには、「規則の種類の選択」画面で「既存の規則」を選択し、「次へ」をクリックします。次に、「既存の規則の選択」ドロップダウンメニューから既存の監査ポリシー規則を選択します。

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、439 ページの「監査ポリシー規則を使用したポリシーの作成」で説明した追加属性を規則に追加していることを確認してください。

「次へ」をクリックします。

450 ページの「規則の追加」に進みます。

規則ウィザードを使用した新しい規則を作成する

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。

新しい規則に名前を付けて説明する

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。

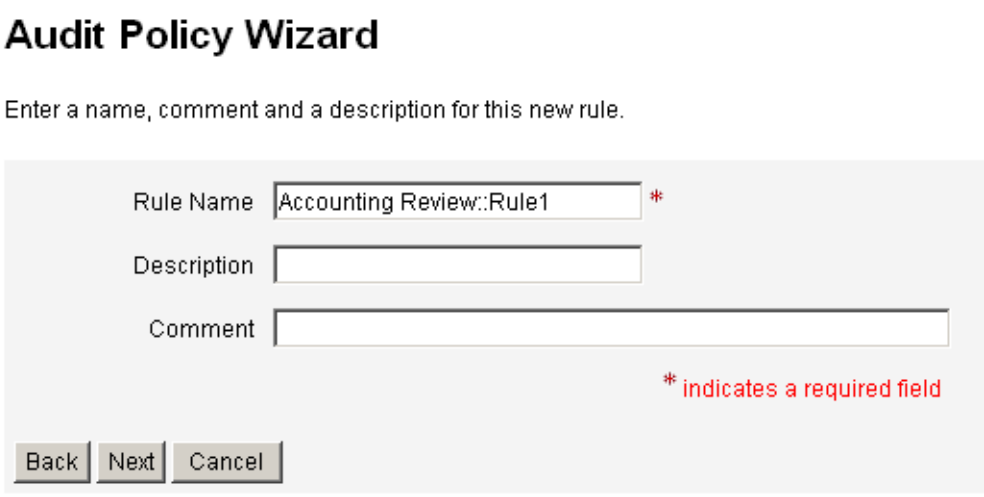


図 14–2　監査ポリシーウィザード: 規則の説明の入力画面

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は、「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**」などの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。

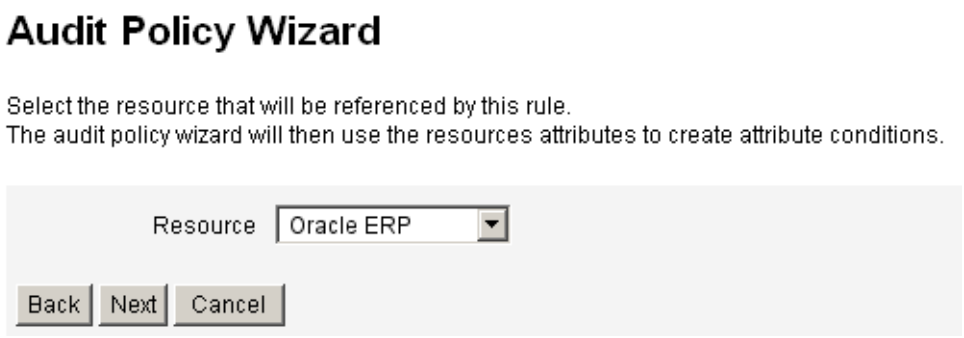


図 14–3　監査ポリシーウィザード: リソースの選択画面

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。利用可能な特定の属性の詳細については、『Sun Identity Manager 8.1 Resources Reference』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。

▼ 規則式を作成する

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 属性の Payable user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」の演算子をクリックし、行を追加して、別の式を作成します。

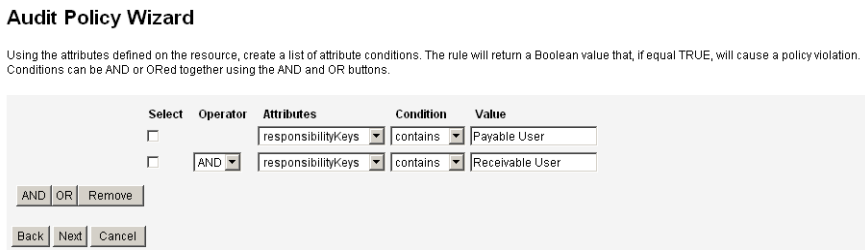


図 14–4 監査ポリシーウィザード:規則式の選択画面

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。また、監査ポリシーウィザードを使用して、規則間で異なるブール演算子を使用したポリシーを作成すると、評価の順序が指定されていないため、予期しない結果となる可能性があります。

複雑な規則式の場合は、監査ポリシーウィザードを使用するのではなく、XML エディタを使用して規則を作成してください。XML エディタを使用すると、必要な場所で否定を指定し、ルール間で 1 つのブール演算子のみを使用するようにできます。

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。

```
<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。既存の規則を追加するか、もう一度ウィザードを使用して、より多くの規則を追加することができます。

規則の追加

既存の規則をインポートするか、ウィザードを使用して、追加規則を作成することができます。詳細については、445 ページの「規則のタイプを選択する」を参照してください。

必要な場合は、「AND」または「OR」の演算子をクリックして、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。規則を AND または OR の演算子でグループ化すると、すべての規則が true でなくても、ポリシーが true に評価される場合があります。Identity Manager は、true に評価された規則に対してのみ、およびポリシー式が true に評価された場合のみ、違反を作成します。

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。また、監査ポリシーウィザードを使用して、規則間で異なるブール演算子を使用したポリシーを作成すると、評価の順序が指定されていないため、予期しない結果となる可能性があります。

複雑な規則式の場合は、監査ポリシーウィザードを使用するのではなく、XML エディタを使用して規則を作成してください。XML エディタを使用すると、必要な場所で否定を指定し、ルール間で 1 つのブール演算子のみを使用するようにできます。

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。

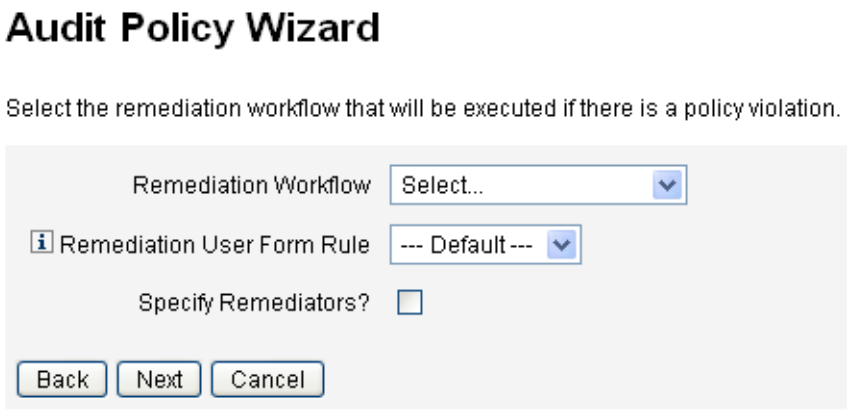


図 14–5　監査ポリシーウィザード: 是正ワークフローの選択画面

注 – XML エディタまたは Identity Manager IDE で作成したワークフローのインポートについては、443 ページの「Identity Manager への職務分掌規則のインポート (省略可能)」を参照してください。

「是正ユーザーフォーム規則」ドロップダウンメニューを使用して、是正を通してユーザーを編集するときに適用するユーザーフォームを判定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」チェックボックスを選択します。このオプションを選択して「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。このオプションを選択しなかった場合は、監査ポリシーウィザードの組織の割り当て画面が表示されます。

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。Identity Manager ユーザーはだれでも、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。レベル 1 是正者が応答する前に、指定したエスカレーションタイムアウト期間が経過すると、Identity Manager は続いて、ここで指定したレベル 2 是正者に連絡します。エスカレーションタイムアウト期間が経過するまでに、レベル 1 是正者とレベル 2 是正者のどちらも応答しなかった場合のみ、Identity Manager はレベル 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 に設定されます。この場合、作業項目は期限切れにならず、是正者のリストに残ります。

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、ユーザー名を検索します。「が次の文字列で始まる」フィールドに文字を入力し、「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、検索領域を閉じます。

是正者のリストからユーザー ID を削除するには、リストでユーザー ID を選択して、「削除」をクリックします。

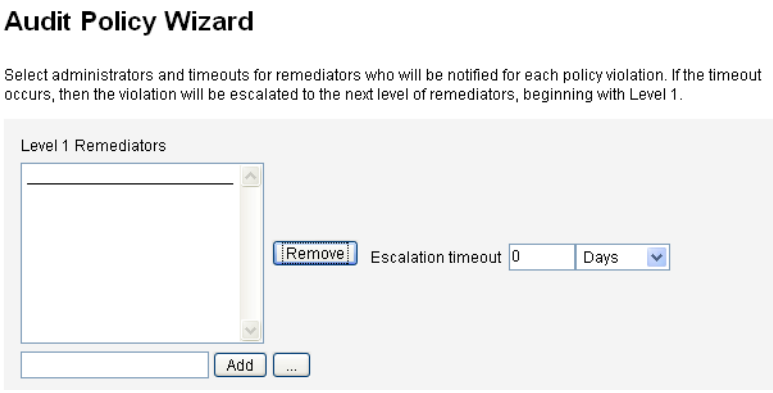


図 14–6　監査ポリシーウィザード: レベル 1 是正者の選択領域

このポリシーにアクセスできる組織の選択

この画面を使用して、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 14–7)。

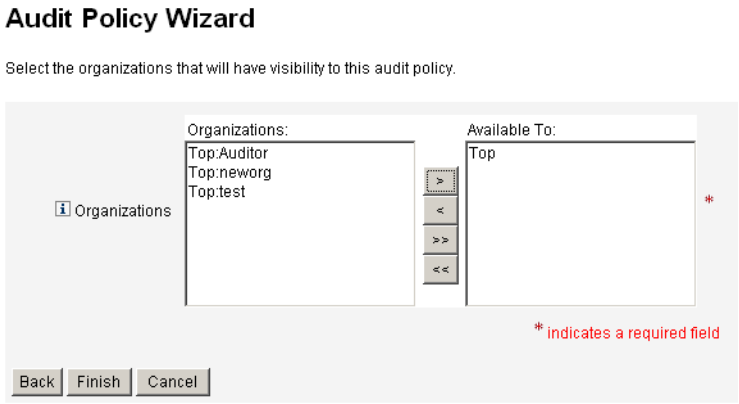


図 14–7　監査ポリシーウィザード: 閲覧を許可された組織の割り当て画面

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。

監査ポリシーの編集

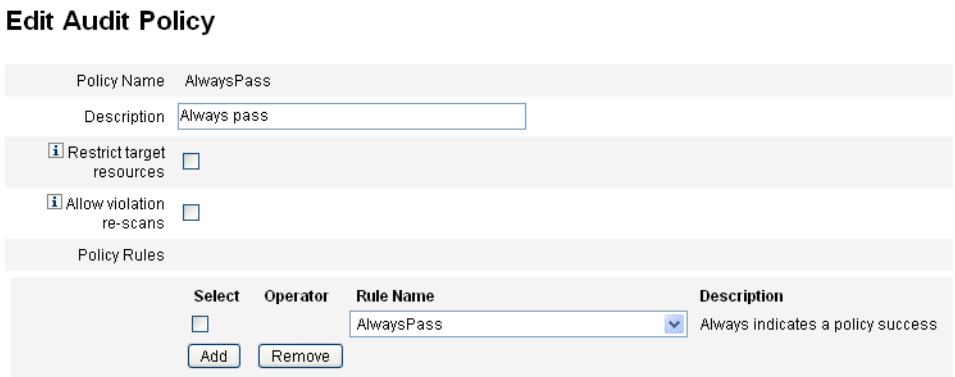
監査ポリシーに関する一般的な編集タスクは次のとおりです。

- 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領域に分類されています。

- 識別と規則の領域
- 是正者とエスカレーションタイムアウトの領域
- ワークフローと組織の領域



ページのこの領域では、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、これを 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」領域

図 14–8 に、ポリシーにレベル 1、レベル 2、およびレベル 3 の是正者を割り当てる、「是正者」領域の一部を示します。

図 14–8 「監査ポリシーの編集」ページ: 是正者の割り当て

ページのこの領域では、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

ユーザー ID を入力して 1 つ以上の是正レベルに対して是正者を選択し、「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、リストでユーザー ID を選択し、「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領域

図 14–9 に、監査ポリシーの是正ワークフローと組織を指定する領域を示します。

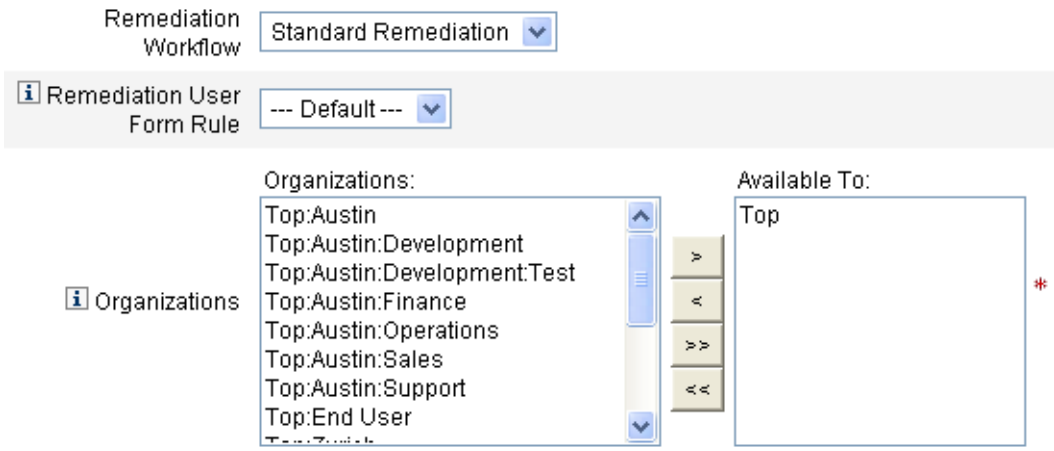


図 14–9 「監査ポリシーの編集」ページ: 是正ワークフローと組織

ページのこの領域では、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すると、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」領域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>
```

- Identity Manager インタフェースにワークフローが表示されない場合は、次の点を確認してください。
  - ワークフローに `subtype='SUBTYPE_REMEDIATION_WORKFLOW'` 属性を追加している。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。
  - ワークフローを含む組織を管理している。
- インポートした規則が監査ポリシーウィザードに表示されない場合は、次の点を確認してください。
  - 各規則に `subtype="SUBTYPE_AUDIT_POLICY_RULE'` または `subtype="SUBTYPE_AUDIT_POLICY_SOD_RULE'` が指定されている。
  - authType `AuditPolicyRule` に対する権限が設定されている機能を持っている。
  - ワークフローを含む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

1 「アカウント」領域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が是正されるときに常に再評価されます。

監査機能制限の解決

デフォルトでは、監査タスクを実行するために必要な機能は最上位 (Top) 組織 (オブジェクトグループ) に含まれています。このため、最上位 (Top) を管理する管理者のみが、これらの機能をほかの管理者に割り当てることができます。

別の組織に機能を追加することで、この制限を解決できます。Identity Manager には、このタスクに使用できる 2 つのユーティリティーが用意されています。これらのユーティリティーは、`sample/scripts` ディレクトリに格納されています。

▼ 機能を追加する

監査タスクを実行するために必要な機能を、最上位 (Top) 以外の組織に追加するには、次の手順に従います。

1 次のコマンドを実行し、すべての機能 **(AdminGroups)** およびそれらに関連する組織 **(**オブジェクトグループ**)** をリスト表示します。

```
beanshell objectGroupUpdate.bsh -type AdminGroup -action list -csv
```

このコマンドは、カンマ区切り値 (CSV) ファイルへの出力を取得します。

2 **CSV** ファイルを編集し、組織上の機能の場所を必要に応じて調整します。

3 このコマンドを実行して、**Identity Manager** を更新します。

```
beanshell objectGroupUpdate.bsh -data CSVFileName -action add -groups NewObjectGroup
```

◆ ◆ ◆ 第 15 章

15 監査: コンプライアンスの監視

この章では、監査レビューの実施方法と、法規制へ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。

- 461 ページの「監査ポリシーのスキャンとレポート」
- 468 ページの「コンプライアンス違反の是正と受け入れ」
- 477 ページの「定期的アクセスレビューとアテステーション」
- 498 ページの「アクセスレビュー是正」

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」領域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。

▼ ユーザーアカウントまたは組織をスキャンする

1 管理者インタフェースで、メインメニューから「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。図 15–1 に、監査ポリシーユーザースキャンの「タスクの起動」ページの例を示します。

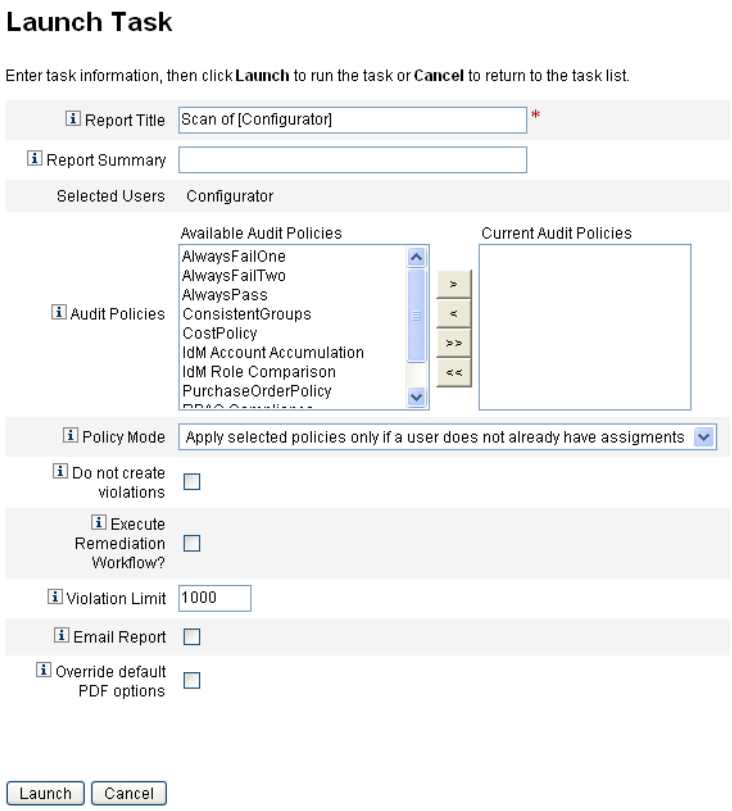


図 15–1 タスクの起動ダイアログ

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入力します。(必須)

4 その他のオプションを指定します。

次のオプションがあります。

- 「レポートの概要」: レポートの説明を入力します。
- 「ポリシーの追加」: 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。
- 「ポリシーモード」: ポリシーモードを選択します。ポリシーがすでに割り当てられているユーザーに、選択したポリシーを適用する方法を決定します。ユーザーから直接、またはユーザーが割り当てられている組織から割り当てることができます。
- 「違反を作成しない」: 監査ポリシーを評価して違反の報告は行うが、コンプライアンス違反を作成および更新せず、是正ワークフローを実行しない場合は、このボックスを有効にします。スキャンによるタスク結果にどの違反が発生したかが示されるため、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。
- 「是正ワークフローを実行しますか?」: 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、このボックスを有効にしします。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。
- 「違反数の最大値」: このボックスを編集して、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。
- 「レポート結果を送信」: レポートの受信者を指定するには、このボックスを有効にします。また、CSV (コンマ区切り) 形式のレポートを含むファイルを添付するように設定することもできます。
- 「デフォルトの PDF オプションを上書き」: デフォルトの PDF オプションを上書きする場合は、このボックスを有効にします。

5 「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、多数の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 15–1 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。
アクセスレビューの概要	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。このレポートによって、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は含まれないが、1 つ以上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、スキャンの用途に応じて、同一のユーザーセットを、あるいは異なるユーザーセットを網羅するように複数のアクセススキャンを編成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。このレポートの設定については、467 ページの「監査された属性のレポートの設定」を参照してください。

表 15–1 監査レポートの説明 (続き)

監査レポートのタイプ	説明
違反履歴 (監査ポリシー別)	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のフィルタを適用でき、日、週、月、四半期でグループ化することができます。
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。組織のフィルタを適用できき、日、週、月、四半期でグループ化することができます。
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。

注 – RULE_EVAL_COUNT 値は、ポリシースキャンの間に評価された規則の数と同じです。この値はレポートに含まれることがあります。

Identity Manager は、RULE_EVAL_COUNT 値を次のように計算します。

スキャンしたユーザーの数 x (ポリシー内の規則の数 + 1)

「+1」が計算に含まれているのは、ポリシー違反であるかどうかを実際に決定する規則であるポリシー規則も数えられているからです。ポリシー規則は監査の規則の結果を調べ、ブール式のロジックを実行してポリシーの結果を見つけ出します。

たとえば、3 つの規則があるポリシー A と 2 つの規則があるポリシー B が存在し、10 人のユーザーをスキャンした場合、RULE_EVAL_COUNT 値は、次の計算によって 70 になります。

10 ユーザー x (3 + 1 + 2 + 1 規則)

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。

次の図に、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。

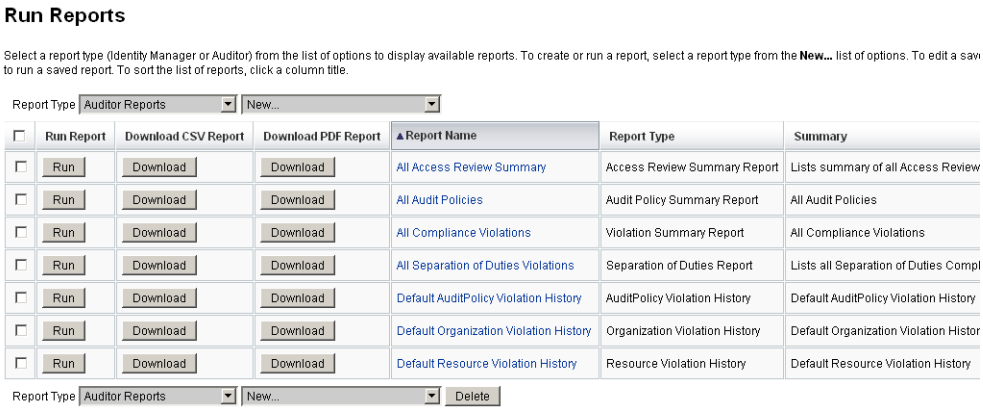


図 15–2　「レポートの実行」ページの選択項目

▼ 監査レポートを作成する

1. 管理者インタフェースで、メインメニューから「レポート」をクリックします。
   「レポートの実行」ページが開きます。

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 のヘルプを参照してください。

レポート基準を入力または選択すると、次の手順を実行できます。

- レポートを保存せずに実行できます。

  「実行」をクリックして、レポートの実行を開始します。新しいレポートを定義した場合、レポートは保存されません。また、既存のレポートを編集した場合、変更されたレポート基準は保存されません。

- レポートを保存できます。

  「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、274 ページの「レポートのスケジュール」を参照してください。

監査された属性のレポートの設定

監査された属性のレポート (表 15–1) は、Identity Manager のユーザーおよびアカウントに対する属性レベルの変更を報告できます。しかし標準の監査ログでは、完全なクエリー式をサポートするのに十分な監査ログデータが生成されません。

標準の監査ログでも、変更された属性が監査ログの `acctAttrChanges` フィールドに書き込まれます。ただし、書き込まれた属性に対して、レポートクエリーでは変更された属性の名前に基づいてしかレコードを照合できません。レポートクエリーでは、属性の値を正確に照合することができません。

次のパラメータを指定することで、`lastname` 属性に対する変更を含むレコードを照合するように、このレポートを設定できます。

```
Attribute Name = 'acctAttrChanges'
Condition = 'contains'
Value = 'lastname'
```

注 – データは `acctAttrChanges` フィールドに保存されるため、`Condition='contains'` の使用が必要です。これは複数値のフィールドではありません。基本的に、変更されたすべての属性の `before/after` 値を、`attrname=value` の形式で格納するデータ構造です。結果として、前の設定では、`lastname=`*xxx* であるすべてのインスタンスを照合するレポートクエリーが可能です。

特定の属性に特定の値を持つ監査レコードのみを収集することもできます。この場合は、326 ページの「「監査」タブの設定」の手順に従ってください。「ワークフロー全体の監査」チェックボックスを選択し、「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、「保存」をクリックします。

次に、まだ有効になっていない場合は、タスクテンプレートの設定を有効にします。この場合は、297 ページの「タスクテンプレートの有効化」の手順に従ってください。「選択したプロセスタイプ」リストのデフォルト値は変更せずに、「保存」をクリックするだけにしてください。

これでワークフローでは、属性の名前と値の両方の照合に適した監査レコードを提供できるようになりました。このレベルの監査を有効にするとより多くの情報を得られますが、パフォーマンスの負荷も非常に大きく、ワークフローの実行速度が低下することに注意してください。

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。

- 468 ページの「是正について」
- 471 ページの「是正電子メールテンプレート」
- 471 ページの「「是正」ページでの操作」
- 471 ページの「ポリシー違反の表示」
- 473 ページの「ポリシー違反の優先度の設定」
- 474 ページの「ポリシー違反の受け入れ」
- 475 ページの「ポリシー違反の是正」
- 476 ページの「是正リクエストの転送」
- 476 ページの「是正作業項目のユーザーの編集」

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、権限付与チェックの動作は次のいずれかです。

- 所有者が、アクションを実行しようとしているユーザー自身である
- 所有者が、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所属している
- 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 です。
- 「subordinate」。有効な値は true または false です。
- 「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します。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 には、監査ポリシースキャンの是正プロセスを行う標準是正ワークフローが用意されています。

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、438 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。

- 是正する。是正者は、何らかの処理を実行し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、是正者の名前と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。

- 転送する。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、第 4 章「ビジネス管理オブジェクトの設定」の 104 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」ページでの操作

「是正」ページにアクセスするには、「作業項目」、「是正」タブの順に選択します。

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応じて、ほかの是正者の違反を表示してアクションを実行することもできます。

以下のトピックは、違反の表示に関するものです。

- 472 ページの「保留中のリクエストの表示」
- 472 ページの「完了したリクエストの表示」
- 473 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。

- 直接報告される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」領域を閉じます。

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」。是正者のリクエストされたアクション。
- 「監査ポリシー/説明」。リクエストに関する是正のコメント。
- 「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。

`AuditLog` レポートで生成される結果テーブルには、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か、是正したか
- 「タイプ」。`ComplianceViolation` または `User Entitlement`
- 「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 (または「なし」)
- 「ID」。ポリシー違反に関連するアカウント ID
- 「結果」。常に `Success`

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。

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

1. リスト内の **1** つ以上の違反を選択します。
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。是正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

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。

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 15–3 「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。(必須)

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、日付の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

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。

▼ 是正リクエストを転送する

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 15–4 「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入して、「**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、「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、検索領域を閉じます。

「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」領域から使用できる「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、必要なときに実行したり、定期的に実行するようにスケジュールすることができます。四半期ごとなど、アクセスレビューを定期的に実行することで、ユーザーの特権を正しいレベルに維持することができます。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、一連の従業員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。このスキャンでは、「ユーザーエンタイトルメント」について規則ベースの評価を実行し、アテステーションが必要かどうかを判定します。
- 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拒否することによって、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なレコードです。

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

一般的に、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拒否を待つ
- 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

是正機能の詳細については、498 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については、第 6 章「管理」の 214 ページの「機能とその管理について」を参照してください。

アテステーションプロセス

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拒否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、権限付与チェックの動作は次のいずれかです。

- 所有者が、アクションを実行しようとしているユーザー自身である
- 所有者が、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所属している
- 所有者が、アクションを実行しようとしているユーザーの部下である

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します。

`lastLevel` の整数値は、デフォルトでは `-1` に設定されます。これは、直属の部下と直属以外の部下を含むことを意味します。

これらのオプションは、次のように追加または変更できます。

```
UserForm: AccessApprovalList
```

注 – 組織管理にアテステーションのセキュリティーを設定する場合 (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 の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高速化できます。

  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と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向上させることができます。

  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)。ユーザーをロックする際の待ち時間 (ミリ秒単位)。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にスリープする時間 (ミリ秒単位)。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。詳細については、『Sun Identity Manager Deployment Reference』の第 2 章「Identity Manager Forms」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

1. 「コンプライアンス」、「アクセススキャンの管理」の順に選択します。
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 – アクセススキャンの名前には、次の文字を使用できません。

'(アポストロフィ)、.(ピリオド)、|(パイプ)、[(左角括弧)、](右角括弧)、,(コンマ)、:(コロン)、$(ドル記号)、"(二重引用符)、\(バックスラッシュ)、=(等号)

また、_(下線)、%(パーセント記号)、^(キャレット)、および*(アスタリスク)の使用も避けてください。

4 スキャンを識別する説明を追加します(省略可能)。

5 「動的エンタイトルメント」オプションを有効にして、アテスターに追加のオプションを与えます。

次のオプションがあります。

- 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転送して是正を依頼できます。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決定されます。

6 「ユーザー範囲タイプ」を指定します(必須)。

次のオプションから選択します。

- 「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します。

  Identity Manager では、次のデフォルトの規則を使用できます。

  - 「All Administrators」

    注 – ユーザーの範囲を指定する規則を追加するには、Identity Manager IDE を使用します。Identity Manager IDE の詳細については、https://identitymanageride.dev.java.net/ を参照してください。

  - All My Reports
  - 「All Non-Administrators」
  - My Direct Reports
  - 「Users without a Manager」
- 「リソースに割り当て」。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。

- 「特定のロールに従う」。指定したロールを、少なくとも 1 つ持つメンバー、またはすべて持つメンバーをスキャンします。
- 「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」。選択したマネージャーに報告しているすべてのユーザーをスキャンします。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拒否が容易になります。

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」。スキャンをターゲットのリソースだけに制限する場合は、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」。違反が検出されたとき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。

.

注 – この手順と次の手順で説明している Identity Auditor 規則の詳細については、『Sun Identity Manager Deployment Reference』の第 4 章「Working with Rules」を参照してください。

---

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。

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。

マニュアルには、アテスターエスカレーション規則に関する追加の情報が含まれています。

16 「レビュー決定規則」(必須)。

次のいずれかの規則を選択して、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します。

- 「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拒否します。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。

「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。

この規則は次の値を返します。

- **-1**。アテステーションの必要なし
- **0**。アテステーションを自動的に却下
- **1**。手動アテステーションが必要
- **2**。アテステーションを自動的に承認
- **3**。アテステーションを自動的に是正する (自動是正)

  マニュアルには、レビュー決定規則に関する追加の情報が含まれています。

17 「是正者規則」。自動是正の場合に、特定のユーザーのエンタイトルメントを誰が是正すべきかを決定するため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」。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」。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。482 ページの「アクセススキャンの作成」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。フィールドを空にした場合は、制限なしを表します。

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 潤オ 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。

- 489 ページの「アクセスレビューの起動」
- 489 ページの「アクセスレビュータスクのスケジュール」
- 490 ページの「アクセスレビューの進行状況の管理」
- 491 ページの「スキャン属性の変更」
- 491 ページの「アクセスレビューのキャンセル」
- 492 ページの「アクセスレビューの削除」

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」の順に選択し、「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」の順に選択し、「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」領域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 週間保存されます。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。

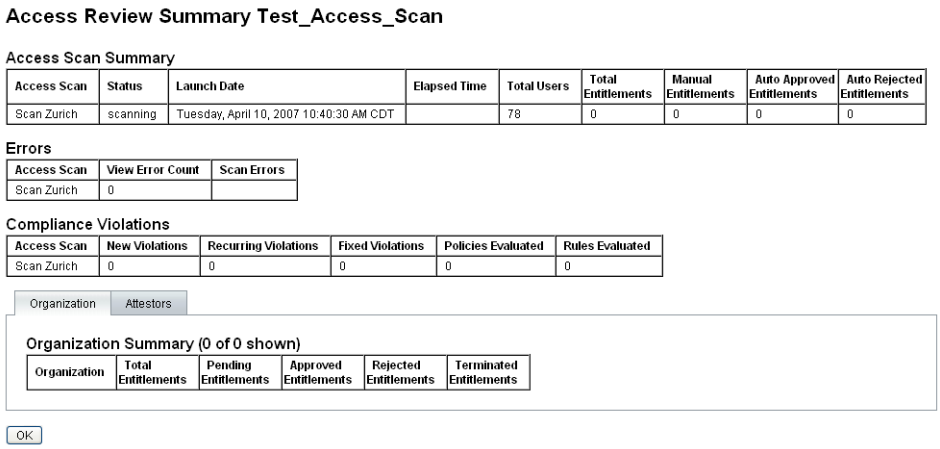
「アクセスレビュー」タブから、すべてのアクティブなアクセスレビューおよび以前に処理されたアクセスレビューの概要をレビューできます。一覧表示されるアクセスレビューごとに、次の情報が表示されます。

- 「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を開始する日付 (タイムスタンプ)。
- 「全ユーザー数」。スキャンされるユーザーの総数。
- 「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、拒否済み、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 15–5 に、アクセスレビュー概要レポートの例を示します。



Access Review Summary Test_Access_Scan

Access Scan Summary

Access Scan	Status	Launch Date	Elapsed Time	Total Users	Total Entitlements	Manual Entitlements	Auto Approved Entitlements	Auto Rejected Entitlements
Scan Zurich	scanning	Tuesday, April 10, 2007 10:40:30 AM CDT		78	0	0	0	0

Errors

Access Scan	View Error Count	Scan Errors
Scan Zurich	0	

Compliance Violations

Access Scan	New Violations	Recurring Violations	Fixed Violations	Policies Evaluated	Rules Evaluated
Scan Zurich	0	0	0	0	0

Organization | Attestors

Organization Summary (0 of 0 shown)

Organization	Total Entitlements	Pending Entitlements	Approved Entitlements	Rejected Entitlements	Terminated Entitlements

OK

図 15–5 「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、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」の順に選択し、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

スキャン中に、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。

保留中のアテステーションリクエストの表示

インタフェースの「作業項目」領域からアテステーション作業項目を表示します。「作業項目」領域の「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。
- 「拒否」。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」。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」タブの順に選択し、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拒否する前に、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、評価し直されます。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。

▼ 別のユーザーからの是正をリクエストする

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、検索領域を閉じます。

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。

   自動的にアテステーションのリストに戻ります。

注 – 各ユーザーエンタイトルメントの「履歴」領域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

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」領域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

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 ユーザー名を「転送先」フィールドに入力します。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 転送アクションに関するコメントを「コメント」フィールドに入力します。

4 「続行」をクリックします。
自動的にアテステーションのリストに戻ります。

注 – 各ユーザーエンタイトルメントの「履歴」領域に転送アクションの詳細が表示されます。

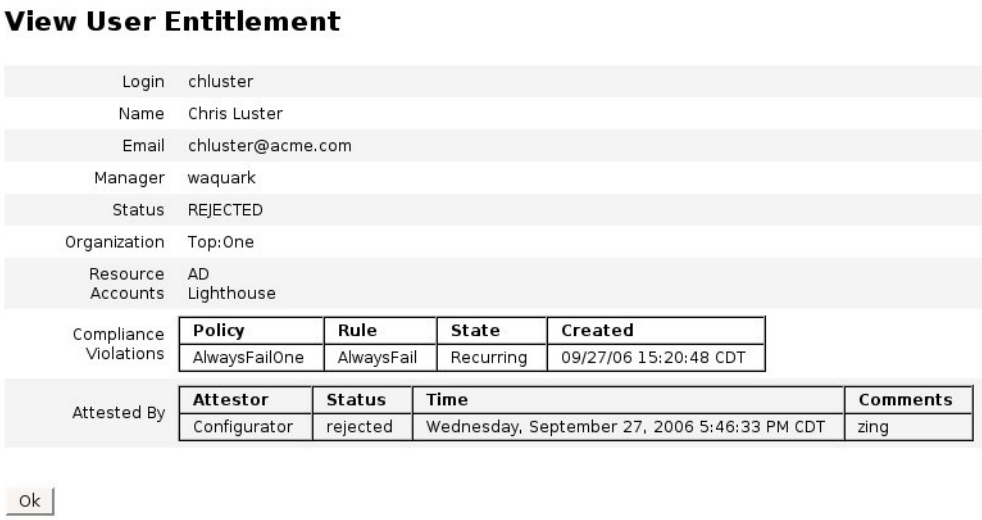
アクセスレビューアクションのデジタル署名

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、236 ページの「承認の署名」を参照してください。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 には、アクセスレビューの結果を評価するために使用できる、次のレポートが用意されています。

- アクセスレビュー範囲レポート。ユーザーエンタイトルメントのオーバーラップまたは相違、あるいはその両方を含むユーザーのリストが、レポートの定義に応じて、表形式で表示されます。このレポートには、どのアクセスレビューにオーバーラップや相違が含まれているかを示す追加の列が含まれる場合もあります。
- アクセスレビュー詳細レポート。このレポートには、次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」。スキャンの実行が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、レポートで名前をクリックします。496 ページの「アクセスレビューレポート」に、ユーザーエンタイトルメントレコードビューに表示される情報の例を示します。



View User Entitlement

Login	chluster
Name	Chris Luster
Email	chluster@acme.com
Manager	waquark
Status	REJECTED
Organization	Top:One
Resource Accounts	AD Lighthouse

Compliance Violations

Policy	Rule	State	Created
AlwaysFailOne	AlwaysFail	Recurring	09/27/06 15:20:48 CDT

Attested By

Attestor	Status	Time	Comments
Configurator	rejected	Wednesday, September 27, 2006 5:46:33 PM CDT	zing

Ok

- アクセスレビュー概要レポート。

  このレポートは、490 ページの「アクセスレビューの進行状況の管理」でも説明されています。また、図 15–5 に、このレポートを示しています。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次の概要情報が表示されます。

  - 「レビュー名」。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
  - 「User Count」。レビューでスキャンされたユーザー数
  - 「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」。拒否されたエンタイトルメントレコードの数
  - 「保留中」。保留中のエンタイトルメントレコードの数
  - 「却下済み」。取り消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」領域から管理します。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に固有の動作について説明し、468 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示します。

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。

アクセスレビュー是正リクエスト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 (`accessReviewRemediation` タイプ) 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。

アクセスレビュー是正応答

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」領域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」領域に転送アクションの詳細が表示されます。
- 「ユーザー編集」。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」領域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

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。

◆ ◆ ◆ 第 16 章

16 データエクスポータ

データエクスポータ機能を使用すると、ユーザー、ロール、その他のオブジェクトタイプを外部のデータウェアハウスに書き込むことができます。

この章では、データエクスポータの設定と維持に役立つ説明および手順を示します。データエクスポータの計画と実装については、『Sun Identity Manager Deployment Guide』の第 5 章「Data Exporter」を参照してください。

この章で説明する内容は次のとおりです。

- 501 ページの「データエクスポータの概要」
- 502 ページの「データエクスポータの実装計画」
- 503 ページの「データエクスポータの設定」
- 514 ページの「データエクスポータのテスト」
- 515 ページの「フォレンジッククエリーの設定」
- 519 ページの「データエクスポータの維持」

データエクスポータの概要

Identity Manager は、分散システムおよびアプリケーション全体にわたってアイデンティティー管理関連データを格納し、処理します。全体のパフォーマンスを向上させるため、Identity Manager は通常のプロビジョニングやその他の日常的なアクティビティーで生成されるデータの一部を保持しません。たとえば、中間ステータスのワークフローアクティビティーとタスクインスタンスは、デフォルトで保持されません。Identity Manager が通常は破棄するデータのすべてまたは一部を収集する必要がある場合は、データエクスポータ機能を有効にすることができます。

データエクスポータを有効にすると、Identity Manager は指定したオブジェクト (データタイプ) に対する変更を検出するごとに、変更をリポジトリ内のテーブルにレコードとして格納します。これらのイベントはキューに入れられ、その後、タスクがそれらを外部のデータウェアハウスに書き込みます。(各タイプのデータをエク

スポートする頻度を設定することができます。)エクスポートされたデータは、市販の変換、レポート、分析ツールを使ったクエリーおよび変換のベースとして、さらに処理または使用することができます。

データウェアハウスにデータをエクスポートすると、Identity Manager サーバーのパフォーマンスが低下するため、エクスポートするデータに対してビジネスニーズがある場合以外、この機能は有効にしないでください。

Identity Manager では、フォレンジッククエリーの作成と実行も可能です。フォレンジッククエリーは、データウェアハウスを検索して、指定された条件を満たすユーザーオブジェクトやロールオブジェクトを特定します。詳細については、515 ページの「フォレンジッククエリーの設定」を参照してください。

データエクスポータの実装計画

データエクスポータはデフォルトでは無効にされるため、操作可能になるよう設定する必要があります。データエクスポータの設定では、設定を開始する前にいくつかの決定を行う必要があります。

- エクスポートするデータタイプ
- 各データタイプのデータを収集するために使用する方法
- 各タイプのデータをエクスポートする頻度
- 各タイプのエクスポートされるスキーマに何を含めるか
- カスタムのウェアハウスインタフェースコード (WIC) ファクトリクラスが必要か

データエクスポータが有効にされると、デフォルトの設定では、すべてのデータタイプのすべての属性がエクスポートされます。これにより、使用されないはずのウェアハウスの記憶領域が消費されて、Identity Manager とウェアハウスで不必要な処理負荷が発生する可能性があります。データウェアハウスは保存力が高く、あとでデータが使用される可能性がある場合にはデータを収集する傾向があります。エクスポートできるデータをすべてエクスポートする必要はありません。エクスポートするデータタイプを設定し、一部のイベントがエクスポートされないように制限することができます。

上記の点について決定したら、以下の手順に従ってデータエクスポータを実装します。

▼ データエクスポータを実装する

1 (省略可能) 選択したタイプのエクスポートスキーマをカスタマイズし、ウェアハウス **DLL** を再作成します。詳細については、**『Sun Identity Manager Deployment Guide』の「Customizing Data Exporter」**を参照してください。

2 ウェアハウスの RDBMS にユーザーアカウントを作成し、そのシステムでウェアハウス DDL を読み込みます。詳細については、『Sun Identity Manager Deployment Guide』の「Customizing Data Exporter」を参照してください。

3 503 ページの「データエクスポータの設定」の説明に従って、データエクスポータを設定します。

4 データエクスポータをテストして正しく設定されたことを確認します。詳細については、514 ページの「データエクスポータのテスト」を参照してください。

5 (省略可能) データウェアハウスに書き込まれるデータを検索できるフォレンジッククエリーを作成します。詳細については、515 ページの「フォレンジッククエリーの設定」を参照してください。

6 JMX を使用し、ログファイルを監視して、データエクスポータを維持します。詳細については、519 ページの「データエクスポータの維持」を参照してください。

データエクスポータの設定

データエクスポータの設定ページでは、保持するデータのタイプを定義し、エクスポートする属性を指定して、データをいつエクスポートするかをスケジュールできます。各データタイプは別個に設定できます。

▼ データエクスポータを設定する

1 管理者インタフェースで、メインメニューから「設定」をクリックします。「ウェアハウス」二次タブをクリックします。「データエクスポータの設定」ページが開きます。

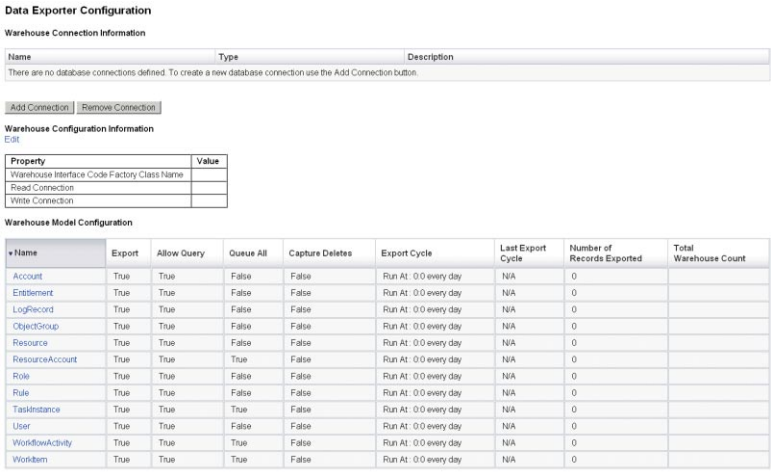


図 16–1 「データエクスポータウェアハウスの設定」ページ

2 読み取り接続と書き込み接続を定義するには、「接続の追加」ボタンをクリックします。「データベース接続の編集」ページが開きます。

このページにあるフィールドの設定を完了し、「保存」をクリックして「データエクスポータの設定」ページに戻ります。詳細については、505 ページの「読み取り接続と書き込み接続の定義」を参照してください。

3 **WIC** クラスとデータベース接続を割り当てるには、「ウェアハウスの設定情報」セクションにある「編集」リンクをクリックします。「データエクスポータウェアハウスの設定」ページが開きます。

このページにあるフィールドの設定を完了し、「保存」をクリックして「データエクスポータの設定」ページに戻ります。詳細については、507 ページの「ウェアハウスの設定情報の定義」を参照してください。

4 「ウェアハウスのモデル設定」テーブルで、データタイプのリンクをクリックします。「データエクスポータタイプの設定」ページが開きます。

このページにある「エクスポート」タブ、「属性」タブ、および「スケジュール」タブの設定を完了し、「保存」をクリックして「データエクスポータの設定」ページに戻ります。詳細については、508 ページの「ウェアハウスモデルの設定」を参照してください。

すべてのデータタイプについてこの手順を繰り返します。

5 各データタイプのエクスポートの前後にどのワークフローを実行するかを設定するには、「エクスポータ自動化」セクションの「編集」リンクをクリックします。「データエクスポータ自動化の設定」ページが表示されます。

このページにあるフィールドの設定を完了し、「保存」をクリックして「データエクスポータの設定」ページに戻ります。詳細については、マニュアルを参照してください。

6 エクスポートタスクデーモンを設定するには、「ウェアハウスのタスク設定」セクションにある「編集」リンクをクリックします。「データエクスポータウェアハウスの設定」ページが開きます。

このページにあるフィールドの設定を完了し、「保存」をクリックして「データエクスポータの設定」ページに戻ります。詳細については、511 ページの「ウェアハウスタスクの設定」を参照してください。

注 – これらの手順が完了すると、エクスポートの操作がすべて可能になります。エクスポートが有効にされると、エクスポートのためにデータレコードのキューイングが開始されます。エクスポートタスクを有効にしないと、キューテーブルがいっぱいになり、キューイングが中断されます。一般に、大きなバッチよりも小さなバッチを (より頻繁に) エクスポートする方が効率的ですが、エクスポートはウェアハウス自体での書き込みが可能かどうかに左右されるため、別の理由による制約を受けることがあります。

---

7 オプションの作業として、最大キューサイズを設定します。詳細については、**513 ページの「設定オブジェクトの変更」**を参照してください。

読み取り接続と書き込み接続の定義

Identity Manager は、エクスポートサイクル中に書き込み接続を使用します。読み取り接続は、ウェアハウス内に現在いくつのレコードがあるかを (ウェアハウスの設定中に) 示し、フォレンジッククエリーインタフェースにサービスを提供するために使用されます。

ウェアハウスの接続は、アプリケーションサーバーのデータソース、JDBC 接続、またはデータベースリソースへの参照として定義できます。JDBC 接続またはデータベースリソースが定義された場合、データのエクスポートでは、書き込み操作中に少数の接続が集中的に使用され、その後、すべての接続が閉じられます。データエクスポータが読み取り接続を使用するのは、ウェアハウスの設定中、およびフォレンジッククエリーの実行中のみで、それらの接続は操作が完了するとすぐに閉じられます。

エクスポータは、書き込み接続と読み取り接続に同じスキーマを使用するので、同じ接続情報を両方のために使用できます。ただし、別個の接続がある場合、配備時にはウェアハウスのステージングテーブルのセットに対して書き込みを行い、それ

らのテーブルを実際のウェアハウスに変換し、ウェアハウステーブルを Identity Manager の読み込み元になるデータマートに変換することができます。

Identity Manager がウェアハウスから読み取りを行えないように、「データエクスポータの設定」フォームを編集できます。このフォームには、`includeWarehouseCount` プロパティーが含まれています。これは、Identity Manager でウェアハウスに問い合わせを行い、各データタイプのレコード数を表示するためのプロパティーです。この機能を無効にするには、「データエクスポータの設定」フォームをコピーし、`includeWarehouseCount` プロパティーの値を `true` に変更して、カスタマイズしたフォームをインポートします。

▼ 読み取り接続と書き込み接続を定義する

1 「データエクスポータの設定」ページから、「接続の追加」ボタンをクリックします。

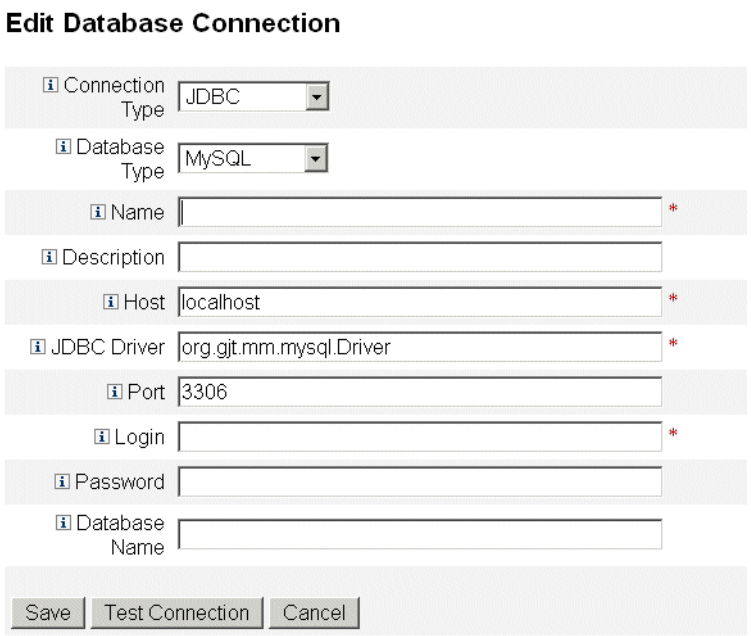


図 16–2 「データエクスポータウェアハウスの設定」ページ

2 「接続タイプ」ドロップダウンメニューからオプションを選択し、**Identity Manager** でデータウェアハウスに対する読み取り接続または書き込み接続を作成する方法を指定します。

- 「JDBC」。Java Database Connectivity (JDBC) アプリケーションプログラミングインタフェースを使用してデータベースに接続します。ウェアハウスインタフェースコードによって接続プールが提供されます。
- 「リソース」。リソースで定義されている接続情報を使用します。ウェアハウスインタフェースコードによって接続プールが提供されます。
- 「データソース」。接続の管理とプールのため、基盤となるアプリケーションサーバーを使用します。このタイプの接続では、アプリケーションサーバーからの接続が必要とされます。

  ページに表示されるフィールドは、「接続タイプ」ドロップダウンメニューで選択したオプションに応じて変化します。データベース接続の設定の詳細については、オンラインヘルプを参照してください。

3 「保存」をクリックして設定の変更を保存し、「データエクスポータの設定」ページに戻ります。

別個の読み取り接続と書き込み接続を使用する場合は、この手順を繰り返します。

ウェアハウスの設定情報の定義

ウェアハウスを設定するには、読み取り接続と書き込み接続を選択し、ウェアハウスインタフェースコードのファクトリクラスを指定する必要があります。WIC ファクトリクラスは、Identity Manager とウェアハウスの間のインタフェースを提供します。Identity Manager にはデフォルトのコード実装が用意されていますが、独自に作成することもできます。カスタムファクトリクラスの作成については、『Sun Identity Manager Deployment Guide』の第 5 章「Data Exporter」を参照してください。

ファクトリクラスを含む `jar` ファイルとサポート用の `jar` ファイルは、エクスポートタスクを実行する Identity Manager サーバーと、データエクスポータを設定するすべてのサーバーの `$WSHOME/exporter` ディレクトリに配置する必要があります。データをエクスポートできるのは常に 1 つの Identity Manager サーバーのみです。

▼ ウェアハウスの設定情報を定義する

1 「データエクスポータの設定」ページで、「ウェアハウスの設定情報」セクションにある「編集」リンクをクリックします。

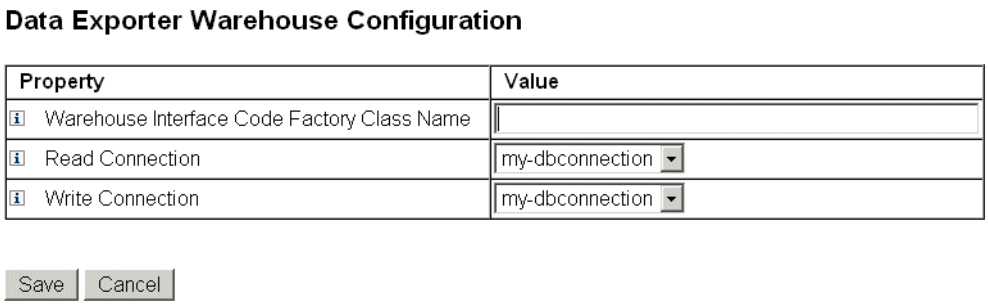


図 16–3 「データエクスポータウェアハウスの設定」ページ

2 「ウェアハウスインタフェースのコードファクトリクラス名」フィールドに値を指定します。インテグレータがカスタムクラスを作成していない場合は、`com.sun.idm.warehouse.base.Factory` の値を入力します。

3 「接続の読み取り」および「接続の書き込み」ドロップダウンメニューの両方からオプションを選択し、接続を指定します。

4 「保存」をクリックして設定の変更を保存し、「データエクスポータの設定」ページに戻ります。

ウェアハウスモデルの設定

エクスポート可能な各データタイプには、そのタイプが、エクスポートされるかどうか、どのようにエクスポートされるか、およびいつエクスポートされるかの制御に使用される一連のオプションがあります。データのエクスポートによって Identity Manager サーバーの負荷が増加するため、ビジネス上の利点があるデータタイプについてのみ、エクスポートを有効にしてください。

次の表に、エクスポート可能な各データタイプの説明を示します。

表 16–1 サポートされるデータタイプ

データ型	説明
`Account`	User と ResourceAccount の間のリンクを含むレコード
`AdminGroup`	すべての ObjectGroups で利用可能な Identity Manager 権限のグループ
`AdminRole`	1 つまたは複数の ObjectGroups に割り当てられた権限
AuditPolicy	Identity Manager オブジェクトに対して評価され、ビジネスポリシーへのコンプライアンスを判定する規則の集合

表 16–1 サポートされるデータタイプ (続き)

データ型	説明
ComplianceViolation	AuditPolicy に対するユーザーのコンプライアンス違反を含むレコード
Entitlement	特定の User のアテステーションのリストを含むレコード
LogRecord	1 つの監査レコードを含むレコード
ObjectGroup	組織としてモデルになっているセキュリティーコンテナ
Resource	アカウントがプロビジョニングされる場所としてのシステムまたはアプリケーション
ResourceAccount	特定の Resource でアカウントを構成している一連の属性
Role	アクセス用の論理コンテナ
Rule	Identity Manager で実行できるロジックのブロック
TaskInstance	実行中のプロセスまたは完了したプロセスを示すレコード
User	0 個以上のアカウントを含む論理ユーザー
WorkflowActivity	Identity Manager ワークフローの 1 つのアクティビティー
WorkItem	Identity Manager ワークフローで実行する手動のアクション

▼ ウェアハウスモデルを設定する

1 「データエクスポータの設定」ページから、データタイプのリンクをクリックします。

2 「エクスポート」タブで、このデータタイプをエクスポートするかどうかを指定します。このデータタイプをエクスポートしない場合は、「エクスポート」チェックボックスを選択解除して「保存」をクリックします。エクスポートする場合はこの「エクスポート」タブで、必要に応じて残りのオプションを選択します。

- 「クエリーを許可」。モデルを照合できるかどうかを決定します。
- 「すべてをキューに入れる」。このタイプのオブジェクトに対するすべての変更を収集します。このオプションを選択すると、エクスポータに大きな処理負荷がかかる可能性があります。このオプションは慎重に使用してください。
- 「削除結果を収集」。このタイプの削除されたオブジェクトをすべて記録します。このオプションを選択すると、エクスポータに大きな処理負荷がかかる可能性があります。このオプションは慎重に使用してください。

3 「属性」タブでは、フォレンジッククエリーの一部として指定することができる属性と、クエリー結果に表示することができる属性を選択できます。管理者インタ

フェースからデフォルトの属性を削除することはできません。デフォルト属性の変更については、『Sun Identity Manager Deployment Guide』の第 1 章「Working with Attributes」を参照してください。

新しい属性名には次の特性があります。

- `attrName` — この属性は最上位で、スカラーです。
- `attrName[]` — この属性はリスト値がある最上位属性で、リスト内の要素はスカラーです。
- `attrName['key']` — この属性にはマップ値が格納され、指定されたキーを持つマップの値が必要です。
- `attrName[].name2` — この属性はリスト値がある最上位属性で、リスト内の要素は構造体です。*name2* はアクセスする構造体の属性です。

注 – 属性を `EXT_RESOURCEACCOUNT_ACCTATTR` テーブルにエクスポートする場合は、エクスポートする各属性の「監査」ボックスを選択する必要があります。

---

4 「スケジュール」タブで、このデータタイプと関連付けられている情報をエクスポートする頻度を指定します。サイクルの基準は、サーバーでの午前零時です。**20** 分ごとのサイクルであれば、指定の時間と、その時間の **20** 分後および **40** 分後にエクスポートが行われます。エクスポートがスケジュールされたサイクルより長くかかった場合は、次のサイクルがスキップされます。たとえば、**20** 分で定義されたサイクルが午前 **0** 時に開始される場合、エクスポートの完了までに **25** 分かかると、次のエクスポートは午前 **0** 時 **40** 分に開始されます。午前 **0** 時 **20** 分にスケジュールされていたエクスポートは実行されません。

エクスポータの自動化の設定

Identity Manager では、データのエクスポートの前後に実行するワークフローを指定できます。

Cycle Start ワークフローを使用すると、エクスポートの取り消しを保証するイベントが発生したときに、エクスポートの実行を禁止できます。たとえば、エクスポートの実行がスケジュールされている時刻に、ステージングテーブルに対して読み取りまたは書き込みを行うアプリケーションで排他的アクセスが必要となった場合は、このエクスポートを取り消す必要があります。ワークフローは 1 の値を返して、エクスポートを取り消します。Identity Manager は、エクスポートがスキップされたことを示す監査レコードを作成し、エラーの結果を示します。ワークフローが 0 を返して、エラーが発生していない場合は、データタイプがエクスポートされます。

Cycle Complete ワークフローは、すべてのレコードがエクスポートされたあとに実行されます。通常、このワークフローはエクスポートしたデータを処理するため

に、ほかのアプリケーションをトリガーします。このワークフローが完了したあと、エクスポータはほかのデータタイプのエクスポートを確認します。

サンプルワークフローは、`$WSHOME/sample/web/exporter.xml` ファイルにあります。エクスポータワークフローの `subtype` は `DATA_EXPORT_AUTOMATION` で、`authType` は `WarehouseConfig` です。

▼ エクスポータの自動化を設定する

1. 「データエクスポータの設定」ページで、「エクスポータ自動化」セクションにある「編集」リンクをクリックします。
2. 必要に応じて、「サイクルの開始ワークフロー」ドロップダウンメニューから、エクスポートの前に実行するワークフローを選択します。
3. 必要に応じて、「サイクルの開始ワークフロー」ドロップダウンメニューから、エクスポートのあとに実行するワークフローを選択します。

ウェアハウスタスクの設定

専用サーバーでエクスポートタスクを実行することは必須ではありませんが、大量のデータをエクスポートする予定であれば、専用サーバーの利用を検討してください。エクスポートタスクでは、データが効率的に Identity Manager からウェアハウスに転送されますが、エクスポート操作中には CPU が最大限に使用されます。専用サーバーを利用しない場合は、サーバーでの対話型のトラフィックの処理を制限する必要があります。 これは、大量のデータのエクスポート中には応答時間が大幅に増加するためです。

▼ ウェアハウス設定情報を設定する

1. 「データエクスポータの設定」ページで、「ウェアハウスのタスク設定」セクションにある「編集」リンクをクリックします。

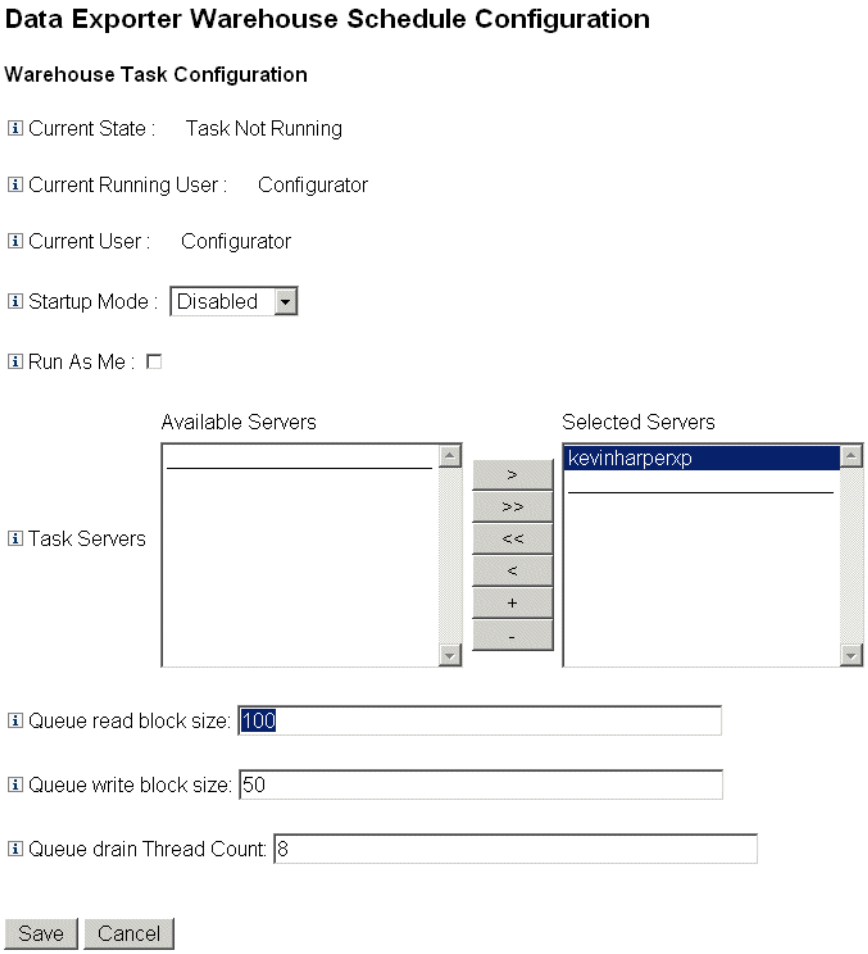


図 16–4 データエクスポータウェアハウスのスケジュールのページ

2 「起動モード」ドロップダウンメニューからオプションを選択し、**Identity Manager** の起動時にウェアハウスタスクを自動的に開始するかどうかを指定します。「無効」を選択すると、タスクを手動で開始する必要があることになります。

3 自分の管理アカウントでエクスポータタスクが実行されるようにする場合は、「自分でタスクを実行」チェックボックスをオンにします。

4 タスクを実行できるサーバーを選択します。複数のサーバーを指定できますが、任意の時点で実行できるウェアハウスタスクは **1** つだけです。タスクを実行するサーバーが停止している場合、スケジューラは自動的に、リストに含まれる別のサーバーでタスクを再開します **(**リストがある場合**)**。

5 「キュー読み取りブロックのサイズ」フィールドでは、書き込みの前にキューからメモリーバッファーに読み取るレコードの数を指定します。このフィールドのデフォルト値は、ほとんどのエクスポートで適切です。**Identity Manager** リポジトリサーバーがウェアハウスサーバーに比べて低速である場合は、この値を大きくします。

6 「キュー書き込みブロックのサイズ」フィールドでは、**1** つのトランザクションでウェアハウスに書き込むレコードの数を指定します。

7 「キュードレインスレッドの数」フィールドでは、キューにあるレコードの読み取りに使用する **Identity Manager** スレッドの数を指定します。キューテーブルに異なるタイプのレコードが多数ある場合には、この数を増やします。キューテーブルのデータタイプの数が少ない場合はこの値を減らします。

8 「保存」をクリックして設定の変更を保存し、「データエクスポータの設定」ページに戻ります。

設定オブジェクトの変更

データエクスポータが設定されて動作可能になると、キューに入れるよう設定されたすべてのデータタイプが、内部キューテーブルに収集されます。デフォルトではこのテーブルに上限はありませんが、`Data Warehouse Configuration` 設定オブジェクトを編集することで設定が可能です。このオブジェクトには、`warehouseConfig` という名前の入れ子になったオブジェクトがあります。次の行を `warehouseConfig` オブジェクトに追加します。

```
<Attribute name='maxQueueSize' value='YourValue'/>
```

`maxQueueSize` の値は、2^{31} より小さい任意の正の整数です。データエクスポータは、制限に達するとキューを無効にします。生成されたデータは、キューが空にされるまでエクスポートできません。

通常の Identity Manager の動作では、変更されたレコードが 1 時間に数千生成されることもあるため、キューテーブルが急速に拡大する場合があります。キューテーブルは Identity Manager リポジトリ内にあるため、このテーブルの拡大によって RDBMS 内の表スペースが使われ、表スペースが使い尽くされる可能性があります。表スペースの容量に限度がある場合は、キューに上限を設定することが必要になる場合があります。

キューテーブルのサイズを監視するには、データキュー JMX Mbean を使用します。詳細については、519 ページの「データエクスポータの監視」を参照してください。

データエクスポータのテスト

データエクスポータは、正しく設定された後、バックグラウンドプロセスとして動作し、設定された間隔でウェアハウスにデータを送信します。エクスポータをオンデマンドで実行するには、「データウェアハウスエクスポータ起動ツール」のタスクを使用します。

▼ データウェアハウスエクスポータ起動ツールを開始する

1. ウェアハウスタスクを無効にします。詳細については、**511** ページの「ウェアハウスタスクの設定」を参照してください。
2. メインメニューの「サーバータスク」をクリックします。次に、「タスクの実行」二次タブをクリックします。「利用可能なタスク」ページが開きます。
3. 「データウェアハウスエクスポータ起動ツール」リンクをクリックします。「タスクの起動」ページが開きます。
4. 「デバッグオプション」チェックボックスを選択して追加のオプションを表示します。
5. 「初期 **LastMods** を無視」チェックボックスを選択します。これによりエクスポータは、**Identity Manager** リポジトリ内のエクスポート済みレコードを判別するために使用する「最後にポーリングされた」タイムスタンプを無視します。このオプションを選択すると、**Identity Manager** リポジトリ内にある、選択したタイプのレコードがすべてエクスポートされます。
6. 「一度エクスポートする」リストから、どのタイプのデータをエクスポートするかを選択します。「一度エクスポートする」リストでどのタイプも選択しないと、エクスポートタスクはデーモンとして実行され、前に定義されたスケジュールに基づいてエクスポートを行います。**1** つ以上のデータタイプを選択すると、**Identity Manager** はそれらのタイプをただちにエクスポートし、エクスポートタスクが終了します。
7. ページのほかのフィールドの値を必要に応じて設定します。
8. 「起動」をクリックしてタスクを開始します。

フォレンジッククエリーの設定

フォレンジッククエリーを使用すると、データウェアハウスに格納されているデータを Identity Manager で読み取ることができます。このクエリーは、ユーザー、ロール、または関連するデータタイプの現在値または履歴値に基づいて、ユーザーやロールを特定できます。フォレンジッククエリーは「ユーザーの検索」や「ロールの検索」のレポートと似ていますが、履歴値に対して一致条件を評価できる点が異なります。また、照会しようとしているユーザーやロールとはデータタイプが異なる属性を検索できる点が異なります。

フォレンジッククエリーの目的は、Identity Manager を使用して結果に対するアクションを実行することです。フォレンジッククエリーは汎用のレポートツールではありません。

フォレンジッククエリーでは次のような質問をすることができます。

- 時間 A と時間 B の間にシステム X にアクセスしたのはどのユーザーか。そのアクセスを承認したのはだれか。
- 過去 48 時間でいくつのプロビジョニングリクエストが処理されたか。各リクエストの所要時間はどれだけだったか。

フォレンジッククエリーの結果は、保存することができません。ウェアハウスデータに関する一般的なレポートは、市販のレポートツールで作成するようにしてください。

クエリーの作成

フォレンジッククエリーでは、ユーザーオブジェクトやロールオブジェクトを検索できます。クエリーは非常に複雑にすることができ、作成者は関連するデータタイプについて 1 つ以上の属性の条件を選択できます。ユーザーのフォレンジッククエリーでは、データタイプが User、Account、ResourceAccount、Role、Entitlement、および WorkItem である属性を検索できます。ロールのフォレンジッククエリーでは、データタイプが Role、User、および WorkItem である属性を検索できます。

1 つのデータタイプ内で、すべての属性条件の論理積が求められるため、一致と判定されるにはすべての条件が満たされる必要があります。デフォルトでは、データタイプ全体にわたる一致の論理積が求められますが、「OR の使用」チェックボックスを選択すると、データタイプ全体にわたる一致の論理和が求められます。

ウェアハウスでは、1 つのユーザーオブジェクトまたはロールオブジェクトについて複数のレコードが含まれていることがあり、1 つのクエリーで、同一のユーザーまたはロールについて複数の一致が返される可能性があります。これらの一致を区別する助けになるように、日付の範囲によって各データタイプに制約を設定できます。そのようにすると、指定した日付の範囲にあるレコードのみが一致だと見なされます。関連するデータタイプはそれぞれ日付の範囲で制約を設定できるため、次の形式のクエリーを発行することができます。

```
find all Users with Resource Account on ERP1 between May and July 2005
who were attested by Fred Jones between June and August 2005
```

日付の範囲は午前零時から午前零時です。たとえば、範囲が 2007 年 5 月 3 日から 2007 年 5 月 5 日であれば 48 時間です。2007 年 5 月 5 日からのレコードは含まれません。

各属性条件のオペランド (比較対象の値) は、クエリー定義の一部として指定する必要があります。スキーマでは、一部の属性で可能な値のセットが限定されるよう制限が設定されており、その他の属性には制限がありません。たとえば、ほとんどのデータフィールドは、YYYY-MM-DD HH:mm:ss の形式で入力する必要があります。

注– ウェアハウス内のデータ量が多い可能性があり、クエリーが複雑であるため、クエリーの結果が生成されるまで長い時間がかかることがあります。フォレンジッククエリーの実行中にクエリーページから移動すると、クエリーの結果を確認できなくなります。

▼ フォレンジッククエリーを作成する

1. 管理者インタフェースで、メインメニューの「コンプライアンス」をクリックします。
   「監査ポリシー」ページ (「ポリシーの管理」タブ) が開きます。
2. 「フォレンジッククエリー」二次タブをクリックします。
   「データウェアハウスの検索」ページが開きます。

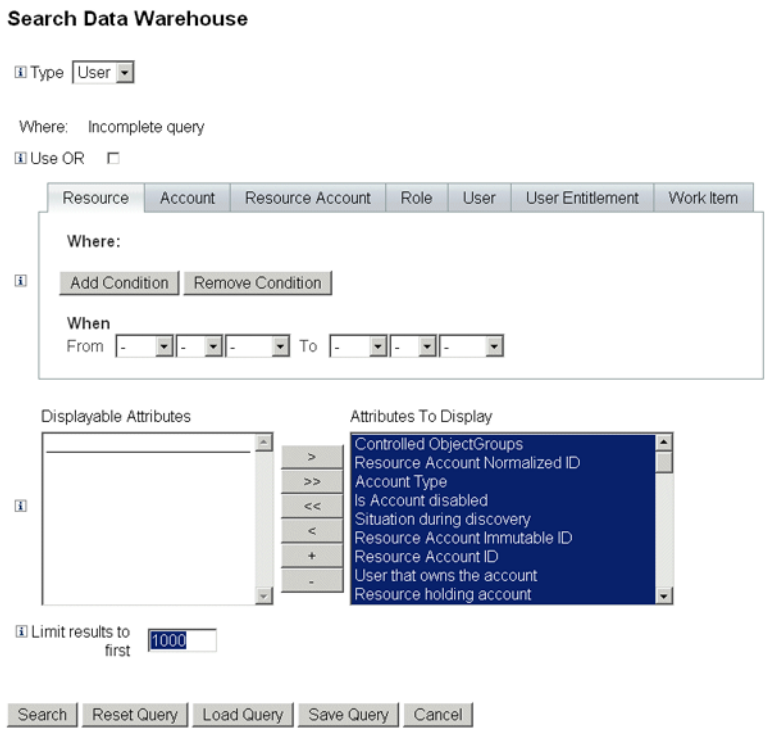


図 16–5 「データウェアハウスの検索」ページ(フォレンジッククエリー)

3 「タイプ」ドロップダウンメニューから、ユーザーレコードとロールレコードのどちらを検索するかを選択します。

4 照会した各データタイプの結果について **Identity Manager** で論理和を求める場合は、「**OR** の使用」チェックボックスを選択します。デフォルトでは、結果の論理積を求める処理が実行されます。

5 フォレンジッククエリーに含める予定のデータタイプが示されているタブを選択します。

   a. 「条件の追加」をクリックします。一連のドロップダウンメニューが表示されます。

   b. 左側のドロップダウンメニューからオペランド(チェックする条件)を選択し、右側のドロップダウンメニューから実行する比較のタイプを選択します。次に、検索する文字列または整数を入力します。使用できるオペランドのリストは外部のスキーマで定義されています。各オペランドの説明については、オンラインヘルプを参照してください。

c. オプションの作業として、日付の範囲を選択してクエリーの範囲を絞り込みます。

必要に応じて、現在選択されているデータタイプにさらに条件を追加します。フォレンジッククエリーの定義の一部になるすべてのデータタイプについて、この手順を繰り返します。

6 選択可能な属性から、フォレンジッククエリーの結果に表示する属性を選択します。

7 「結果表示を次の件数に限定」フィールドに値を指定します。複数のデータタイプからの条件を使用する場合、各タイプのサブクエリーに制限が適用され、最終結果はすべてのサブクエリーの共通部分になります。そのため、サブクエリーの制限が原因で、最終結果から一部のレコードが除外される場合があります。

8 「検索」をクリックしてフォレンジッククエリーをただちに実行するか、クエリーを再利用できるように「クエリーの保存」をクリックします。フォレンジッククエリーの再使用については、**518** ページの「フォレンジッククエリーの保存」を参照してください。

フォレンジッククエリーの保存

クエリーを設定 (オプションの作業として、クエリーを実行して必要な結果が生成されることを確認) したら、あとで実行するためにクエリーを保存できます。

▼ フォレンジッククエリーを保存する

1 「データウェアハウスの検索」ページから、「クエリーの保存」をクリックします。「フォレンジッククエリーの保存」ページが開きます。

2 クエリーの名前を説明を指定します。

3 「条件値の保存」チェックボックスを選択し、「データウェアハウスの検索」ページで入力した条件の値 (文字列と整数) を保存します。このチェックボックスを選択しない場合、保存したフォレンジッククエリーはテンプレートとして機能し、クエリーを実行するたびに値を入力する必要があります。

4 保存されたクエリーはどのユーザーでも実行できますが、デフォルトでは、クエリーを修正できるのはクエリーの作成者だけです。ほかのユーザーがクエリーを変更できるようにするには、「ほかのユーザーがこのクエリーを変更することを許可」チェックボックスを選択します。

5 クエリーではユーザーオブジェクトまたはロールオブジェクトが返されるため、結果にオブジェクトのどちらのオブジェクトの属性を表示するかを選択できます。「表示する属性」リストに含まれない属性を表示する場合は、「データエクスポータの設定」ページに移動し、表示可能な新しい属性をユーザーまたはロールのタイプに追加します。

クエリーの読み込み

任意のユーザーが保存した任意のクエリーを読み込むことができますが、変更できるのは自分が作成したクエリーか、ほかのユーザーが作成したもののうち、だれでも修正可能とマークされたクエリーのみです。

▼ フォレンジッククエリーを読み込む

1 「データウェアハウスの検索」ページから、「クエリーの読み込み」をクリックします。「フォレンジッククエリーの読み込み」ページが開きます。クエリーがテンプレートとして保存されている場合は、「クエリーの概要」列に「未完了のクエリー」と表示されます。

2 クエリーの左側にあるチェックボックスを選択し、「クエリーの読み込み」をクリックします。

データエクスポータの維持

この節では、データエクスポータの状態を追跡する方法を説明します。この情報は、次のトピックで構成されています。

- 519 ページの「データエクスポータの監視」
- 520 ページの「監視ログ」

データエクスポータの監視

エクスポータが設定されて動作可能になったら、継続的な動作の確認のためにエクスポータの監視を行うことを選択できます。エクスポータには、エクスポータがどのように動作しているかを判断する場合に役立つ JMX Beans がいくつか用意されています。これらの JMX Beans には、エクスポータの平均読み取り/書き込みレート、内部メモリーキューの現在/最大のサイズ、および持続的なキューのサイズについての統計情報が含まれます。エクスポータでは、エクスポート中に監査レコードも作成されます。 各データタイプの 1 サイクルごとに 1 つのレコードが作成されます。監査レコードには、そのタイプのレコードがエクスポートされた数や、エクスポートの所要時間が含まれます。

データエクスポータには、エクスポータの監視を行う次の JMX 管理 Beans が用意されています。

表 16–2　JMX 管理 Beans

Beans の名前	説明
DataExporter	現在キューにあるエクスポートの数と、キューの上限についての情報を格納しています。
DataQueue	現在キューにありキャッシュされているエクスポートの数と、キャッシュへの到着レートについての情報を格納しています。
ExporterTask	Identity Manager からのエクスポートの読み取り数、ウェアハウスに対する書き込み数、読み取りと書き込みのレート (レコード数/秒)、およびエラーの数についての情報を格納しています。

通常の Identity Manager の操作中にエクスポートレコードをキューテーブルに入れるように、データエクスポータを設定できます。キューは、場合によっては多数のレコードに応じて拡張し、サーバーの再起動後も保持する必要があるため、Identity Manager リポジトリ内のテーブルによって保持されます。一般的にリポジトリへの書き込みは、通常の Identity Manager 操作の速度を低下させるため、レコードがリポジトリ内で持続可能になるまで、キューは少量のメモリーキャッシュを使用してメモリー内にレコードをバッファーします。

DataQueue MBean 属性は、1 台の Identity Manager サーバー上でメモリーのキューに入れられたレコードの最大数を表示するように計画できます。バランスのとれたシステムでは、メモリーキャッシュ内のレコード数が少なく、数がすばやくゼロに向かうはずです。この数が大きくなったり (数千単位)、数秒以内にゼロに戻らなかったりすることが観察される場合、リポジトリの書き込みパフォーマンスを調査する必要があります。

ExportTask MBeans には、2 種類のエラー数の情報が含まれています。 1 つが読み取り、もう 1 つが書き込みのエラーです。これらの数はゼロであるべきですが、特に書き込み中には、エラーが発生することがある理由がいくつか存在します。もっともよくある書き込みエラーは、エクスポートされたデータがウェアハウスのテーブル列内に入らないことから発生します。 これは一般的に、文字列のオーバーフローです。エクスポートされる文字列データにはサイズの限度がないものがあります。 この場合、エクスポートテーブル列に上限が設定されている必要があります。

監視ログ

Identity Manager には、「監査ログ」および「システムログ」というサイズ制限のない 2 セットのオブジェクトがあります。データエクスポータは、ログテーブルに関連するメンテナンスの問題のいくつかに対処しています。

監査ログ

Identity Manager は不変の監査レコードを監査ログに書き込み、実行する操作の監査証跡の履歴として提供します。Identity Manager はこれらのレコードを特定のレポートで使用します。また、レコードのデータは管理者インタフェースに表示できます。しかし、監査ログは限度なく拡大しますが、あまり速くない速度で拡大するため、配備担当者はいつ監査ログの切り捨てを行うかを判断する必要があります。データエクスポータの前に、切り捨てに先立ってレコードを保持したい場合は、リポジトリからテーブルをダンプする必要があります。データエクスポータが有効にされていて、ログレコードをエクスポートするよう設定されている場合、古いレコードはウェアハウスに保持され、Identity Manager が必要に応じて監査テーブルを切り捨てることがあります。

システムログ

システムログは、監査ログと同じ不変のプロパティーを持っていますが、通常、監査ログと同じ頻度では生成されません。データエクスポータはシステムログをエクスポートしません。システムログを切り捨てて古いレコードを保持するには、リポジトリ内のテーブルをダンプする必要があります。

◆ ◆ ◆ 第 17 章

17 サービスプロバイダの管理

この章では、Sun Identity Manager のサービスプロバイダ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。Identity Manager Service Provider (サービスプロバイダ) 実装については、『Sun Identity Manager Service Provider 8.1 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。

- 523 ページの「サービスプロバイダ機能の概要」
- 525 ページの「初期設定」
- 536 ページの「トランザクション管理」
- 545 ページの「サービスプロバイダユーザーの委任管理」
- 550 ページの「サービスプロバイダユーザーの管理」
- 562 ページの「サービスプロバイダのユーザー同期」
- 565 ページの「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。サービスプロバイダ機能により、企業の管理者はアンデンティティーアカウントを Identity Manager ユーザーと サービスプロバイダユーザーの 2 つの異なるタイプに分類できます。Identity Manager のサービスプロバイダユーザーは、サービスプロバイダユーザータイプとして設定された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。

メインのポリシーテーブルに追加されている「サービスプロバイダシステムの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 とサービスプロバイダの同期

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、どの Identity Manager サーバーでも実行されるように設定することも、選択したサーバーに制限されるように設定することもできます。

サービスプロバイダ同期は、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。563 ページの「同期の開始と停止」を参照してください。

Identity Manager ユーザー同期の入力フォームとサービスプロバイダユーザー同期の入力フォームは異なります。559 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

サービスプロバイダのエンドユーザーページでの認証に Sun 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。

サービスプロバイダでは、認証にユーザー名が必要です。`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

サービスプロバイダ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、Service Provider 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。

  必要に応じて、サービスプロバイダのアカウントポリシーを設定します。
- 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。

メイン設定の編集

▼ サービスプロバイダ実装の設定オブジェクトを編集する

1. 管理者インタフェースで、メニューの「サービスプロバイダ」をクリックします。
2. 「メイン設定の編集」をクリックします。

   「サービスプロバイダ設定」ページが開きます。
3. 「サービスプロバイダ設定」フォームに必要な情報を指定します。

   次の節で説明されている手順に従います。

   - 526 ページの「ディレクトリの設定」
   - 529 ページの「ユーザーフォームとポリシー」
   - 530 ページの「トランザクションデータベース」
   - 531 ページの「追跡イベント設定」
   - 532 ページの「同期アカウントインデックス」
   - 534 ページの「コールアウト設定」

ディレクトリの設定

「ディレクトリ設定」領域では、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 17–1 に、「サービスプロバイダ設定」ページのこの領域と、次の節で説明する「ユーザーフォームとポリシー」領域を示します。

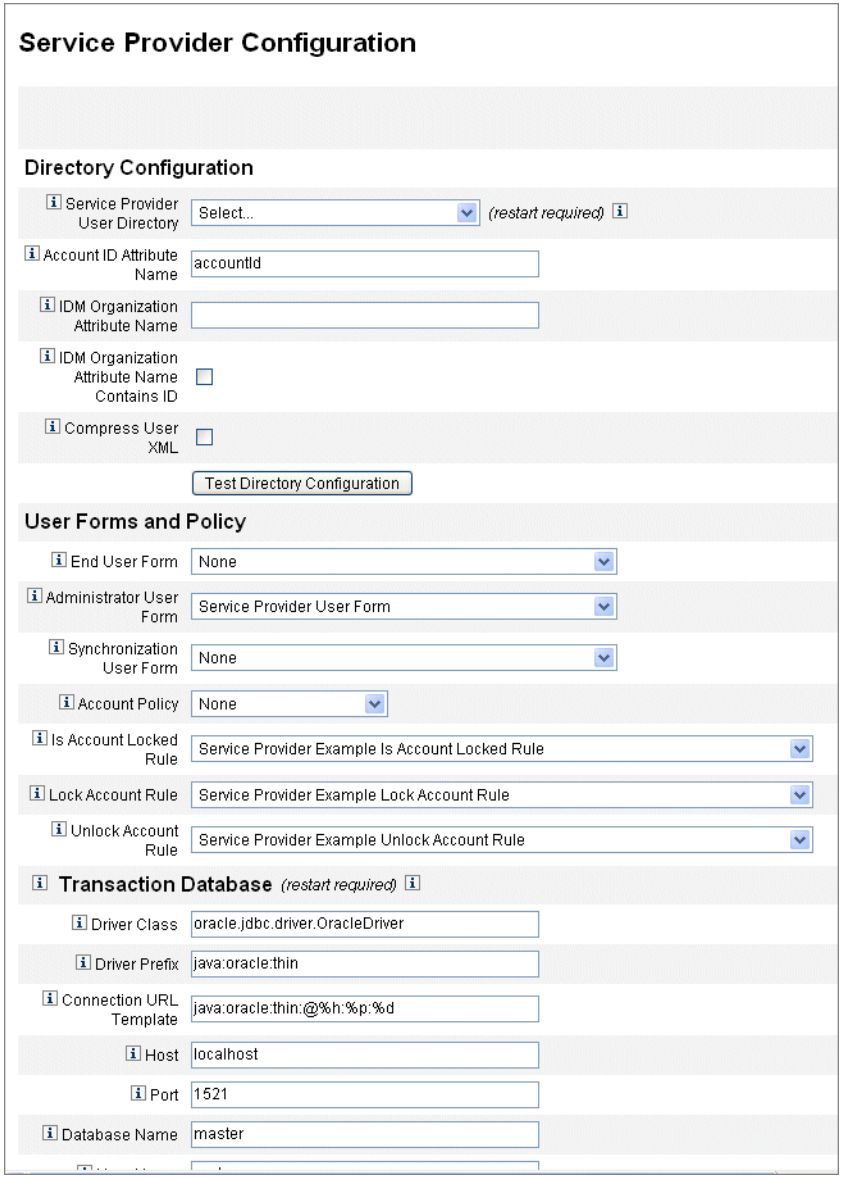


図 17–1　サービスプロバイダ設定 (ディレクトリ、ユーザーフォーム、およびポリシー)

▼ 「ディレクトリ設定」フォームに必要な情報を指定する

1 「**Service Provider End-User Directory**」をリストから選択します。

すべての サービスプロバイダ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 **ID** 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。これは、LDAP アカウントの管理を委任する場合に使用されます。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」を指定します。

---

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」領域では、前の図 17–1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。

▼ サービスプロバイダユーザー管理のフォームとポリシーを指定する

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」を選択すると、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、サービスプロバイダアカウントの編集ページが含まれます。「なし」を選択すると、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 でサービスプロバイダ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。

サービスプロバイダ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対して入力フォームが指定されている場合は、代わりにそのフォームが使用されます。リソースは通常、それぞれに異なる同期入力フォームを使用します。この場合は、リストからフォームを選択せずに、各リソースに対して同期ユーザーフォームを設定してください。

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、サービスプロバイダ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。

属性を設定するサービスプロバイダ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。

属性を設定するサービスプロバイダ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

「サービスプロバイダ設定」ページのこの領域では、図 17–2 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。

トランザクションのデータベーステーブルは、`create_spe_tables` DDL スクリプト (使用している Identity Manager インストールの `sample` ディレクトリにある) に示されているスキーマに従って設定する必要があります。ターゲットの環境に合うように、適切なスクリプトのカスタマイズが必要な場合があります。

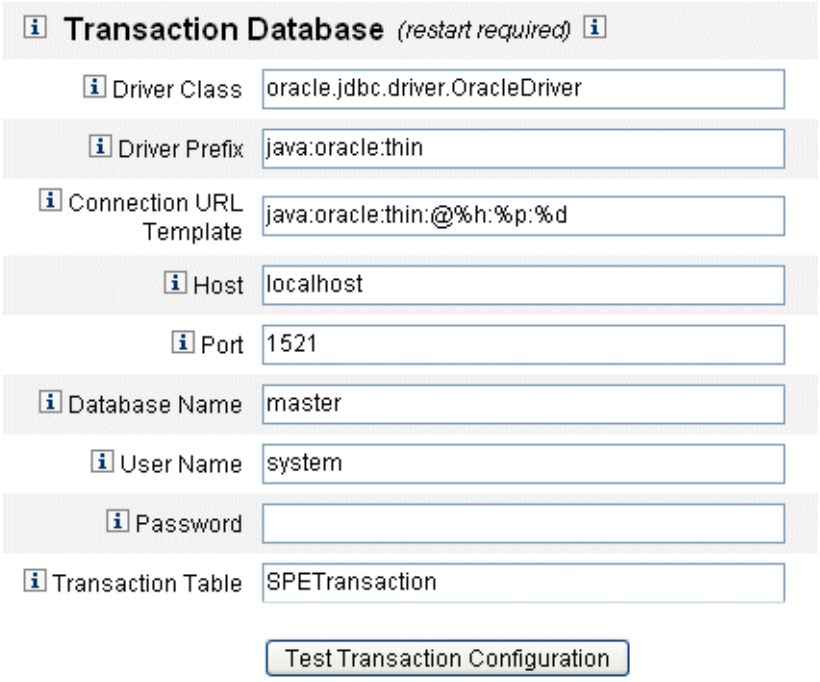


図 17–2 サービスプロバイダ設定 (トランザクションデータベース)

▼ トランザクションデータベースを設定する

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。
- 「ドライバプリフィックス」。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のパスワードを入力します。
- 「トランザクションテーブル」。保留中のトランザションを格納するために使用する、選択したデータベース内のテーブルの名前を入力します。

2 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設定」ページの次の領域に進み、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 17–3 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。

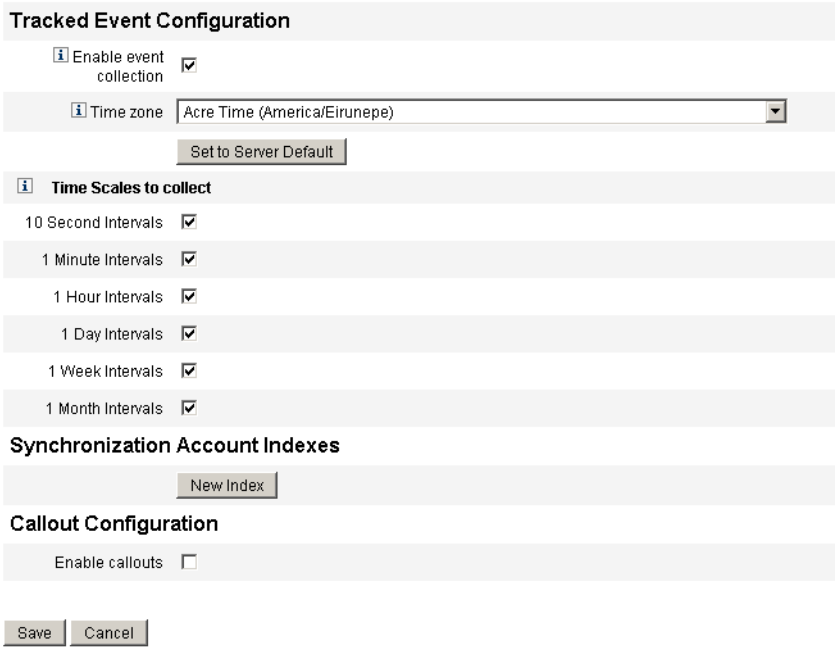


図 17–3　サービスプロバイダ設定 (追跡イベント、アカウントインデックス、およびコールアウトの設定)

▼ サービスプロバイダの追跡イベントのタイムゾーンと収集間隔を設定する

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

サービスプロバイダ実装でリソースの同期を行う場合、リソースが送信するイベントがサービスプロバイダ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、サービスプロバイダディレクトリのリソース定義を編集し、各 Active Sync 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。

▼ リソースのインデックス属性を定義する

サービスプロバイダリソースのインデックス属性のすべてを定義したら、次の手順を実行します。

1 設定ページの「同期アカウントインデックス」領域で、「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であり、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であり、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」領域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。これにより、すべての依存トランザクションは、操作後のコールアウトが正常に完了したあとにのみ実行されます。

注–「サービスプロバイダ設定」ページですべての領域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 17–4 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。

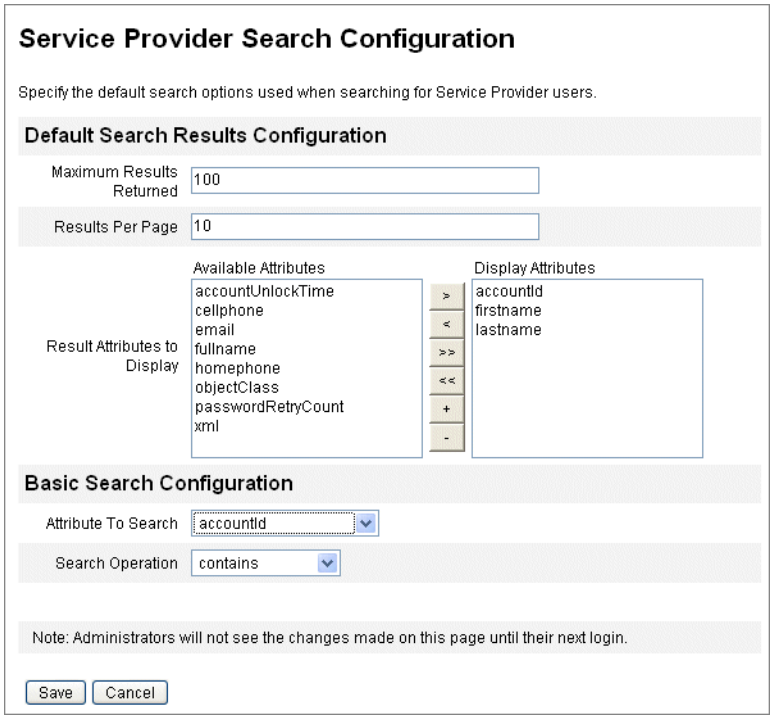


図 17–4　検索設定

▼ サービスプロバイダユーザーを検索するデフォルトの検索設定を行う

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. 「返される最大結果数」に数値を入力します (デフォルト値は 100)。
4. 「ページあたりの結果数」に数値を入力します (デフォルト値は 10)。
5. 「表示する結果属性」の横にある「利用可能な属性」を矢印キーで選択します。
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。

サービスプロバイダ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。

- 536 ページの「デフォルトのトランザクション実行オプションの設定」
- 539 ページの「トランザクション持続ストアの設定」
- 540 ページの「トランザクション処理の詳細設定」
- 542 ページの「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、トランザクションの実行方法を制御します。 これには、同期/非同期の処理、トランザクション持続ストアに書き込むタイミングなどが含まれます。これらのオプションは、IDMXUser ビューまたはその処理に使用されるフォームを使用して、上書きできます。詳細は、『Sun Identity Manager Service Provider 8.1 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

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。
「サービスプロバイダのトランザクション設定」ページが開きます。

図 17–5 に、「デフォルトのトランザクション実行オプション」領域を示します。

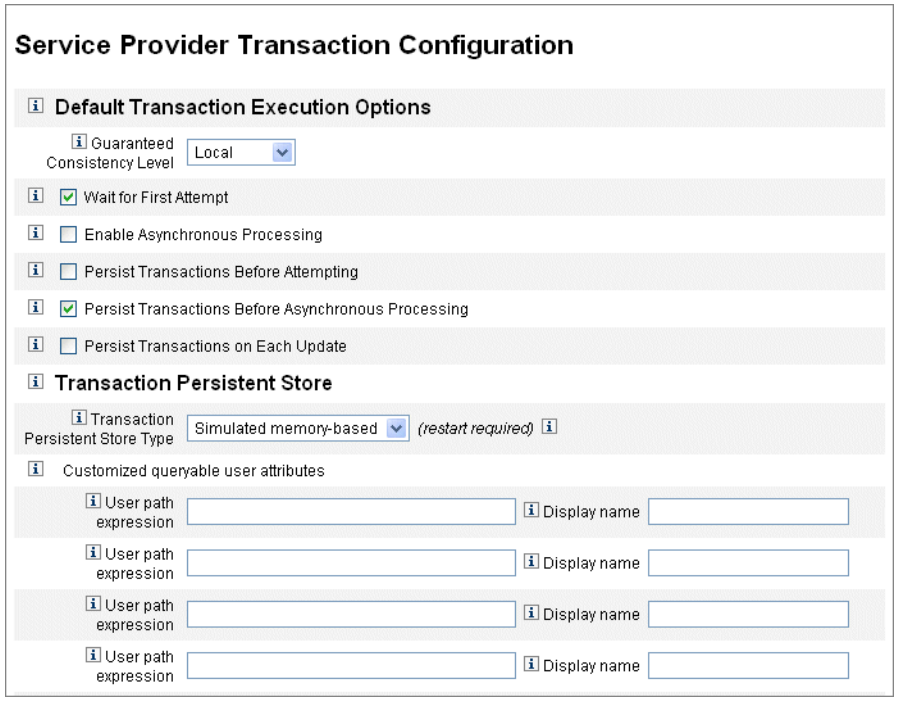


図 17–5 トランザクションの設定

2 「保証される整合性レベル」で適切なオプションを選択して、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。

次のオプションがあります。

- 「なし」。ユーザーのリソース更新の順序付けは保証されません。
- 「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」。ユーザーのすべてのリソース更新の順番付けがサーバー全体で保証されます。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 必要に応じて「デフォルトのトランザクション実行オプション」領域を有効にします。

次のオプションがあります。

- 「最初の試行を待機」。IDMXUser ビューオブジェクトがチェックインされるときにどのように呼び出し元に制御が戻されるかを指定します。このオプションを有効にすると、プロビジョニングトランザクションが試行を 1 回完了するまで、チェックイン操作が遮断されます。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。非同期処理が有効になっている場合、トランザクションは引き続きバックグラウンドで再試行されます。このオプションを無効にすると、プロビジョニングトランザクションの試行の前に、チェックイン操作から呼び出し元に制御が戻ります。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が戻ったあとでプロビジョニングトランザクションの処理を継続するかどうかを制御します。

  非同期処理を有効にすると、トランザクションの再試行が可能になります。540 ページの「トランザクション処理の詳細設定」で設定されているワークスレッドを非同期で実行させることで、スループットも向上します。このオプションを選択した場合は、同期入力フォームを使用してリソースをプロビジョニングまたは更新する再試行間隔および試行回数を設定します。

  「非同期処理の有効化」を選択したときは、「再試行タイムアウト」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」。 このオプションを有効にすると、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」(デフォルトの選択)。 このオプションを有効にすると、プロビジョニングトランザクションは非同期で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」オプションが有効になっている場合、再試行が必要なトランザクションは、制御がコールアウト元に戻る前に持続ストアに書き込まれます。「最初の試行を待機」オプションが無効になっている場合、トランザクションは試行される前に常に持続ストアに書き込まれます。このオプションは有効にすることをお勧めします。「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」。このオプションを有効にすると、プロビジョニングトランザクションは再試行後に持続ストアに書き込まれます。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

「サービスプロバイダのトランザクション設定」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。

図 17–6 サービスプロバイダのトランザクション持続ストアの設定

▼ 「サービスプロバイダのトランザクション設定」ページのオプションを設定する

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、サービスプロバイダ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。これにより、サーバーが再起動された場合でも、再試行する必要のあるトランザクションが失われることはなくなります。このオプションを選択する場合は、メインのサービスプロバイダ設定ページで 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、「クエリー可能なユーザー属性のカスタマイズ」を選択します。

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。

次の属性があります。

- 「ユーザーパス表現」。IDMXUser オブジェクトに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。すべてのエントリが必須です。

図 17–5 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」領域を示します。

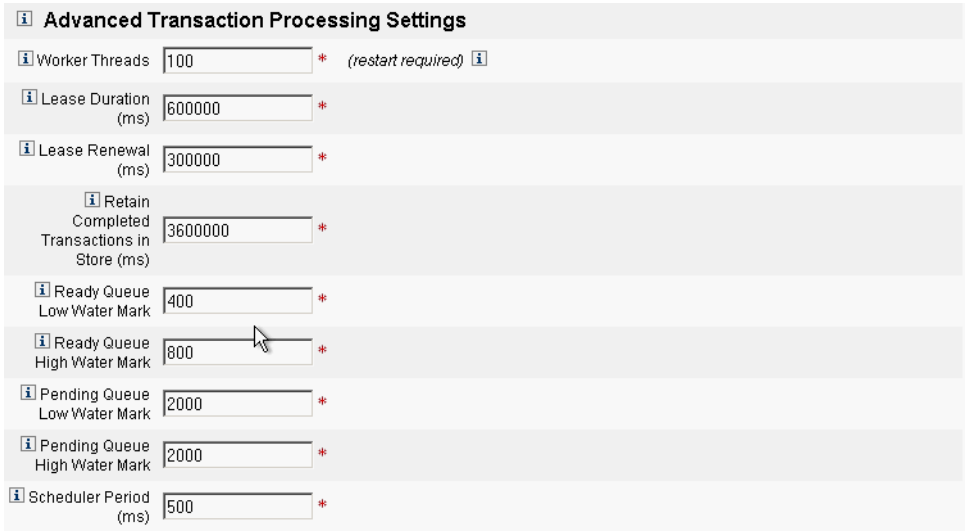


図 17–7　トランザクション処理の詳細設定

▼ 「トランザクション処理の詳細設定」を指定する

1 「ワークスレッド」に数値を入力します (デフォルト値は 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)」に数値を入力します (デフォルト値は 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。それより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可能性があります。

3 「リース更新 (ms)」に数値を入力します (デフォルト値は 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。リースの残り時間がこの値になったときにリースが更新されます。 この値の単位はミリ秒です。

4 「終了トランザクションのストア内での保持時間 (ms)」に数値を入力します (デフォルト値は 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。トランザクションがただちに持続ストアに書き込まれるように設定されている場合を除き、完了したすべてのトランザクションがトランザクション持続ストアに格納されているとはかぎりません。

5 「実行可能キュー最低水準点」に数値を入力します (デフォルト値は 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」に数値を入力します (デフォルト値は 2000)。

トランザクションスケジューラの保留中キューには、再試行のために保留されている、失敗したトランザクションが保持されます。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」に数値を入力します (デフォルト値は 2000)。

トランザクションスケジューラの保留中キューには、再試行のために保留されている、失敗したトランザクションが保持されます。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

1 管理者インタフェースで、「サーバータスク」→「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。

「サービスプロバイダの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。

2 検索を設定します。

次のオプションのいずれかを選択します。

- 「ユーザー名」。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 – サービスプロバイダトランザクション設定ページで「クエリー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、クエリー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。

- 「タイプ」。選択したタイプのトランザクションを検索できます。
- 「状態」。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。

- 「試行回数」。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。
- 「送信時間」。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。
- 「終了時間」。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。
- 「キャンセルステータス」。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。
- 「トランザクションID」。一意の ID に基づいてトランザクションを検索できます。すべての監査ログレコードに表示される、ユーザーが入力する ID に基づいてトランザクションを検索するには、このオプションを使用します。
- 「SPE サーバー名」。実行中の サービスプロバイダ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。
- 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。ほかの結果がある場合でも通知は表示されません。

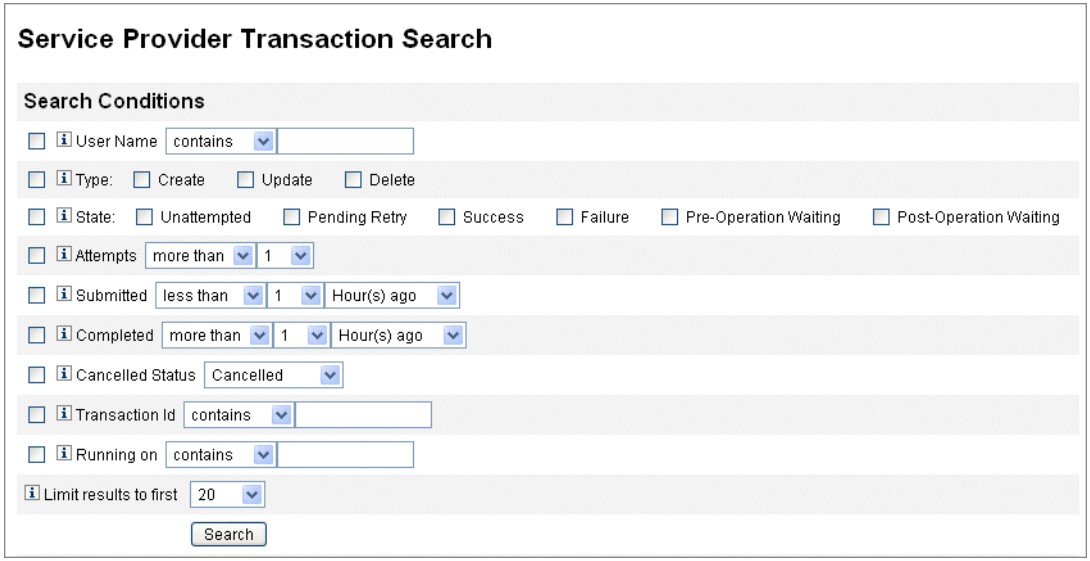


図 17–8　トランザクションの検索

3 「検索」をクリックします。
検索結果が表示されます。

4 結果ページの一番下にある「一致したすべてのトランザクションをダウンロード」をクリックして、結果を XML 形式のファイルに保存します。

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には、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。

サービスプロバイダユーザーの委任管理

サービスプロバイダユーザーの委任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、特定の機能と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 組織の名前またはオブジェクト ID のいずれかです。これは、「Identity Manager メイン設定」画面の「Identity Manager 組織の属性名が ID を含む」フィールドの設定によって異なります。
- 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` はサービスプロバイダ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、そのサービスプロバイダユーザーは最上位 (Top) 組織のメンバーとみなされます。このため、サービスプロバイダ管理者は、それらのユーザーを管理するために、Top 内でサービスプロバイダユーザー機能を持っていることが必要です。

属性設定により、サービスプロバイダ管理者による検索範囲が決まります。

- 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 サービスプロバイダ管理者機能を追加します。ユーザーに割り当てることができる Service Provider 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サービスプロバイダユーザーを指定します。サービスプロバイダユーザーが利用可能なリソースはいずれも、すべての Identity Manager 管理者が利用可能です。

注 – Identity Manager の委任管理については、第 6 章「管理」の200 ページの「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制御の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に対して管理者ロールの委任を使用するには、Identity Manager システム設定オブジェクト (116 ページの「Identity Manager 設定オブジェクトの編集」) で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、「サービスプロバイダ設定」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 (サービスプロバイダ委任管理) を有効にするには、変更のために システム設定オブジェクトを開き (116 ページの「Identity Manager 設定オブジェクトの編集」)、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 管理者のサービスプロバイダ委任管理を有効にするには、System Configuration 設定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サービスプロバイダ委任管理を無効に (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。

サービスプロバイダ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、管理者ロールを作成し、制御の範囲、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。

次の規則を使用するには、規則の `authType` を指定する必要があります。

- SPEUsersSearchContextRule
- SPEUsersSearchFilterRule
- SPEUsersAfterSearchFilterRule
- CapabilitiesOnSPEUserRule
- UserIsAssignedAdminRoleRule
- SPEUserIsAssignedAdminRoleRule

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。

実際の環境でのサンプル規則の作成については、『Sun Identity Manager Service Provider 8.1 Deployment』を参照してください。

▼ サービスプロバイダユーザー管理者ロールを設定する

1 管理者インタフェースで、メニューから「セキュリティー」をクリックし、「管理者ロール」をクリックします。

「管理者ロール」ページが開きます。

2 「新規」をクリックします。

「管理者ロールの作成」ページが開きます。

3 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。

4 次の節の説明に従って、「制御の範囲」、「機能」、および「ユーザーに割り当てる」のオプションを指定します。

制御の範囲の指定

サービスプロバイダユーザー管理者ロールの制御の範囲は、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制御の範囲では、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され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制御の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。

「機能」タブで、この管理者ロールに適用する「機能規則」を選択します。

ユーザーへの管理ロールの割り当て

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。

「ユーザーに割り当てる」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、次のシステム設定オブジェクト (116 ページの「Identity Manager 設定オブジェクトの編集」) 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

サービスプロバイダユーザーは、デフォルトで、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、自分の制御の範囲内のサービスプロバイダユーザーに割り当てる (または「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、自分の制御の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、制御の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.による サービスプロバイダユーザーの管理とその手順について説明します。

この節は次のトピックで構成されています。

- 550 ページの「ユーザー組織」
- 551 ページの「ユーザーとアカウントの作成」
- 554 ページの「サービスプロバイダユーザーの検索」
- 559 ページの「エンドユーザーインタフェース」

ユーザー組織

サービスプロバイダでは、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、Identity Manager のメイン設定の「Identity Manager 組織の属性名」フィールドによって指定されます (525 ページの「初期設定」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サービスプロバイダ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サービスプロバイダユーザー管理ページで使用されます。

注 – 現在、サービスプロバイダ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。

「サービスプロバイダシステムの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、サービスプロバイダ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 サービスプロバイダ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。詳細は、『Sun Identity Manager Deployment Reference』の第 2 章「Identity Manager Forms」を参照してください。

▼ サービスプロバイダアカウントを作成する

1. 管理者インタフェースで、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. 「ユーザーの作成」をクリックします。

注 – デフォルトの サービスプロバイダ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、サービスプロバイダ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領域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. 必要に応じてこれらのリソースの属性値を指定します。

   次の属性値があります。

   - **accountid** (必須)
   - **password**
   - **confirmation** (パスワードの確認)

- **firstname** (必須)
- **lastname** (必須)
- **fullname**
- **email**
- 「**home phone**」
- 「**cell phone**」
- 「**password retry count**」
- 「**account unlock time**」

5 矢印キーを使用して、目的の「リソース」を「利用可能」リストから選択します。

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。

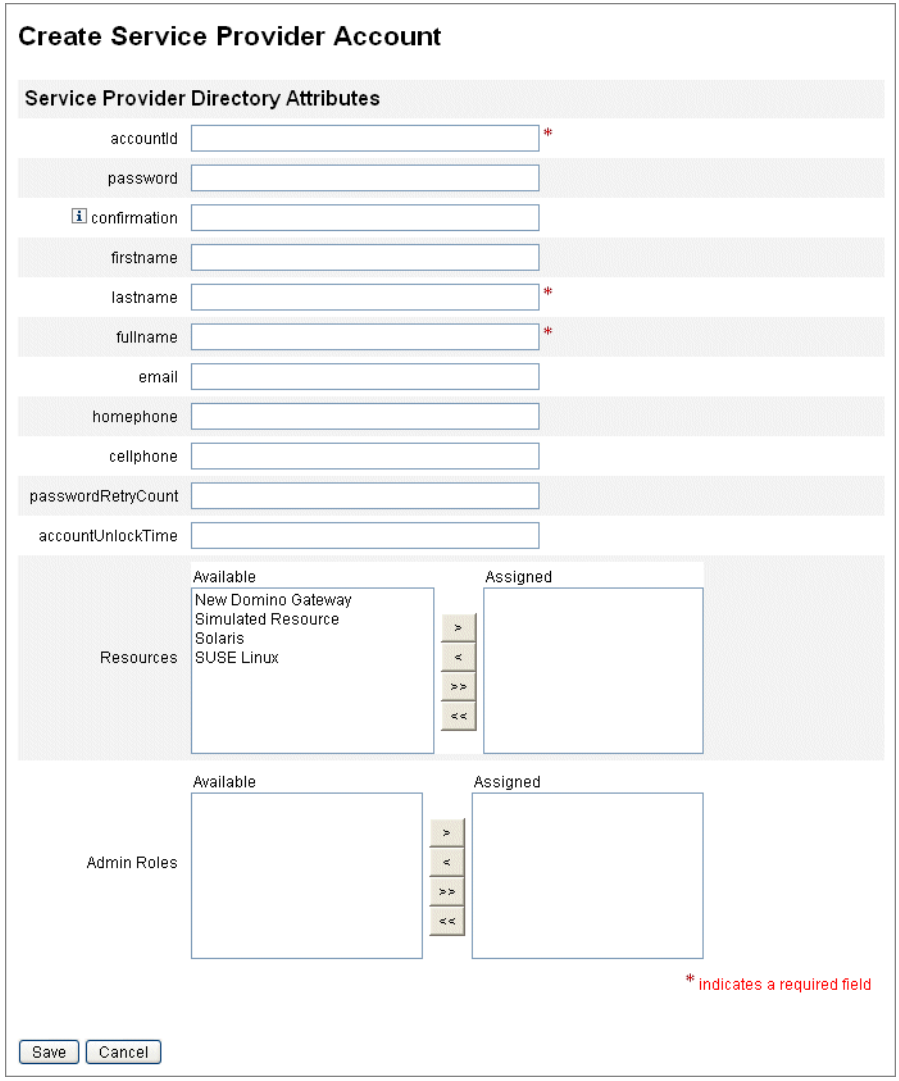


図 17–9　サービスプロバイダのユーザーとアカウントの作成

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、提供されているサンプルの サービスプロバイダ ユーザーフォームをカスタマイズします。

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

サービスプロバイダには、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」領域で、「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。

次のトピックでは、サービスプロバイダの検索機能について説明します。

- 554 ページの「詳細検索」
- 555 ページの「検索結果」
- 556 ページの「アカウントのリンク」
- 557 ページの「アカウントの削除、割り当て解除、またはリンク解除」
- 558 ページの「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、次の手順に従います。

▼ サービスプロバイダユーザーの詳細検索を実行する

1 サービスプロバイダユーザーの検索ページから・・・「詳細」をクリックします。

2 目的の「属性」をリストから選択します。

3 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。

4 目的の検索値を入力し、「検索」をクリックします。

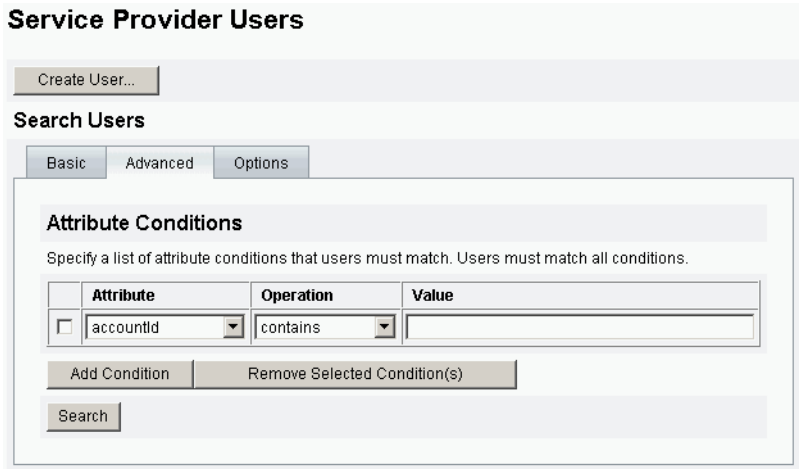


図 17–10　ユーザーの検索

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

サービスプロバイダの検索結果は、図 17–11 に示すようなテーブルに表示されます。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。

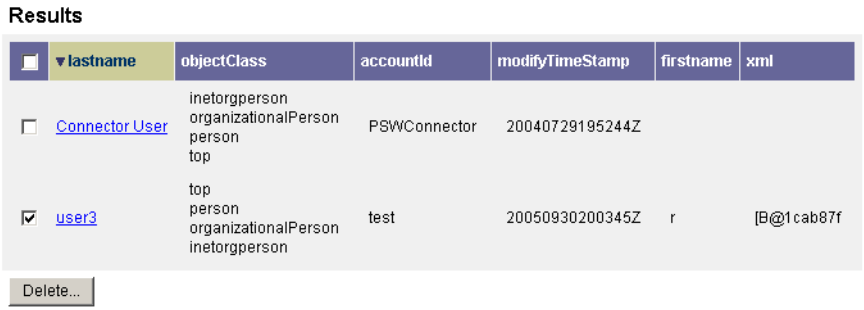


図 17–11 検索結果の例

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。この操作により、ユーザーの削除ページが表示され、さらにオプションが表示されます (557 ページの「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

サービスプロバイダは、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。サービスプロバイダのアカウントリンク機能により、既存のリソースアカウントを サービスプロバイダユーザーにインクリメント方式で割り当てることができます。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 サービスプロバイダ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

1. 管理者インタフェースで、メニューバーの「リソース」をクリックします。
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. リンク確認規則を選択します。この規則は、リンク相関規則が選択したアカウントの候補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 サービスプロバイダ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を削除、割り当て解除、またはリンク解除する

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 省略可能なグローバルオプションのいずれかを選択します。

次のオプションがあります。

- すべてのリソースアカウントの削除

  注 – リソースを削除すると、アカウントが削除されますが、リソース割り当ては残ります。そのあとでユーザーを更新すると、アカウントが再作成されます。削除すると必ずリソースアカウントがリンク解除されます。

- 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、そのリソースの割り当てが削除されます。割り当て解除するとリソースアカウントがリンク解除されます。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 – リンク解除すると、ユーザーとリソースアカウントの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。どちらの場合もリソース割り当ては削除されないので、そのあとでユーザーを更新すると、アカウントに再リンクされるか新しいアカウントがリソースに作成されます。

7 または、「削除」、「割り当て解除」、または「リンク解除」列で 1 つ以上のリソースアカウントの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、「**OK**」をクリックします。

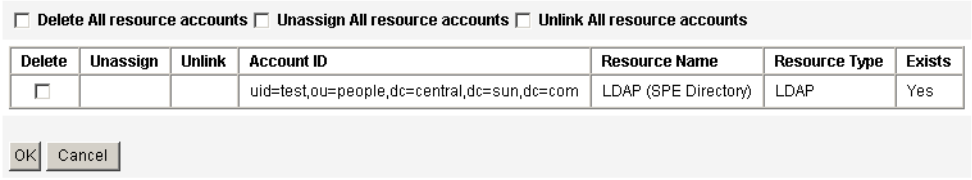


図 17–12 アカウントの削除、割り当て解除、またはリンク解除

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

1 管理者インタフェースで、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。

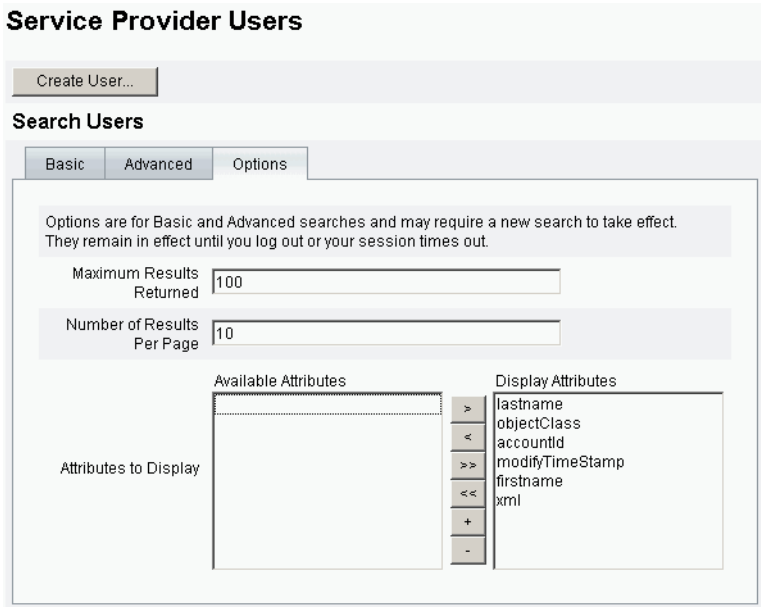


図 17–13　サービスプロバイダユーザーの検索オプションの設定

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方法は、『Sun Identity Manager Service Provider 8.1 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も Identity Manager フォームを利用できます。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 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。

サンプルエンドユーザーページ

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では、登録に検証テーブルが使用されます。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。

サンプルページは、配備に合わせて簡単にカスタマイズできます。

配備に合わせて次のように簡単にカスタマイズできます。

- ブランドの変更
- 設定オプション (たとえば、ログイン試行エラー回数など) の変更
- ページの追加または削除

ページのカスタマイズ方法は、『Sun Identity Manager Service Provider 8.1 Deployment』を参照してください。

新しいユーザーの登録

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。

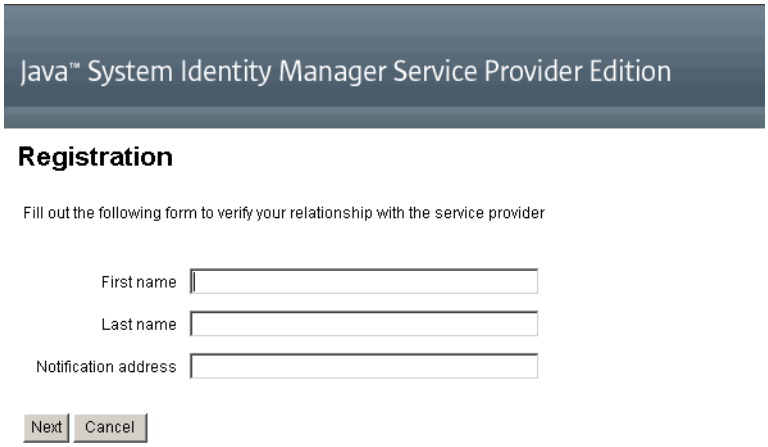


図 17–14 「登録」ページ

ホーム画面とプロファイル画面

図 17–15 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。

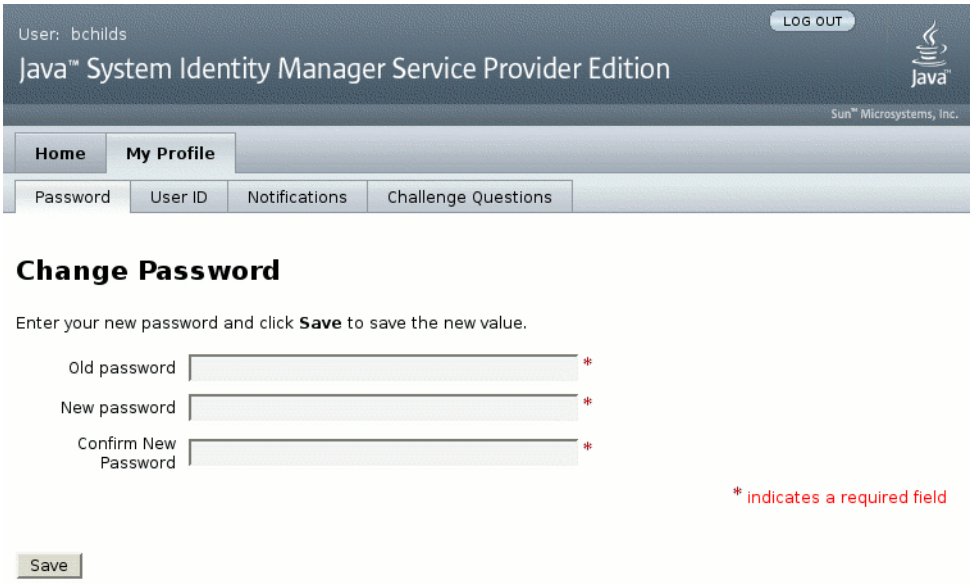


図 17–15 「自分のプロフィール」ページ

サービスプロバイダのユーザー同期

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なります。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。

- 562 ページの「同期の設定」
- 563 ページの「同期の監視」
- 563 ページの「同期の開始と停止」
- 564 ページの「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」領域のリソースリストから設定します。

同期の設定

サービスプロバイダ同期を設定するには、262 ページの「同期を編集または設定する」の説明に従って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「サービスプロバイダユーザー」を選択します。
- 「スケジューリングの設定」領域で、「同期の有効化」を選択します。

262 ページの「同期を編集または設定する」の説明に従って、実際の環境に合わせて他のオプションを指定します。サービスプロバイダ同期タスクのデフォルトの同期間隔は 1 分です。

注 – 確認規則とフォームでは、Identity Manager 入力ユーザービューではなく、IDMXUser ビューを使用する必要があります (詳細は『Sun Identity Manager Service Provider 8.1 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 には、サービスプロバイダ同期を監視するために次の方法が用意されています。

- 「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。

▼ サービスプロバイダの **Active Sync** を無効にする

1 管理者インタフェースで、メニューから「リソース」をクリックします。
「リソースのリスト」ページが開きます。

2 「サービスプロバイダ」領域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。

3 「同期の有効化」チェックボックスを選択解除します。

4 「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

サービスプロバイダ機能には、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。このタスクにより、既存の Identity Manager ユーザーが サービスプロバイダユーザーディレクトリに移行されます。この節では、サンプル移行タスクの使用方法について説明します。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

1 管理者インタフェースで、メニューから「サーバータスク」をクリックします。
「タスクの検索」ページが開きます。

2 二次的なメニューから「タスクの実行」をクリックします。

3 「**SPE** の移行」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、サービスプロバイダディレクトリサーバーを表す Identity Manager 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の実装では、Identity Manager の監査ログシステムがエクストラネットのユーザーアクティビティーに関連するイベントを監視します。Identity Manager には、サービスプロバイダの監査設定グループ (デフォルトで有効) が用意されており、サービスプロバイダユーザーのログが記録される監査イベントを指定します。図 17–16 を参照してください。

監査ログ、およびサービスプロバイダの監査設定グループのイベントの変更については、第 10 章「監査ログ」を参照してください。

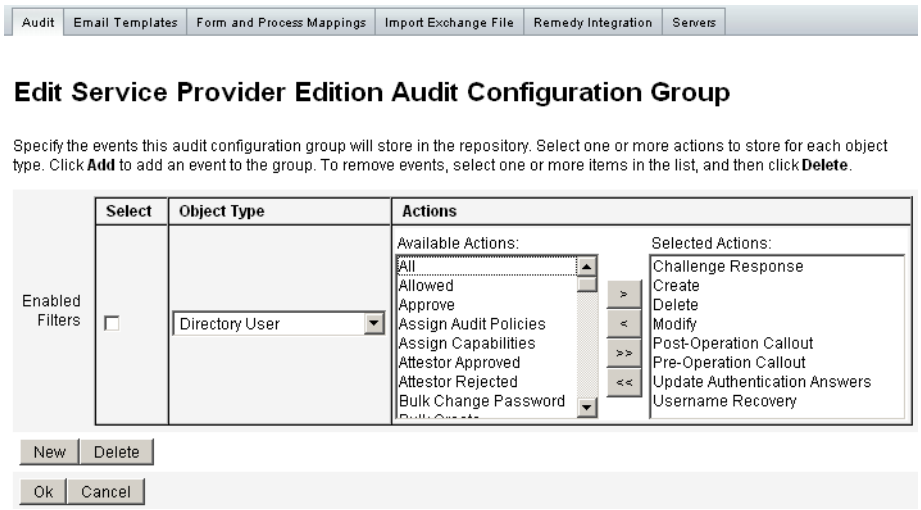


図 17–16 「サービスプロバイダ監査設定グループの編集」ページ

◆ ◆ ◆ 付 録 A

lh リファレンス

この付録では、Identity Manager コマンド行インタフェースを使用して、Identity Manager のコマンドを実行する際に役立つ情報を説明します。

この付録は、次のトピックで構成されています。

- 567 ページの「lh コマンドの構文」
- 570 ページの「lh コマンドの例」
- 570 ページの「syslog コマンド」

lh コマンドの構文

Identity Manager コマンド行インタフェースを呼び出して、Identity Manager コマンドを実行するには、次の構文を使用します。

```
lh { $class | $command } [ $arg [$arg... ] ]
```

各表記の意味は次のとおりです。

- class には、完全修飾クラス名を指定する必要があります (com.waveset.session.WavesetConsole など)。
- command には、次のコマンドのいずれかを指定する必要があります。
  - assessment は、アップグレード中に使用できます。変更されたすべてのオブジェクトと、インストールされている Identity Manager のすべてのバージョンについてレポートするサブコマンドをサポートしています。詳細については、『Sun Identity Manager 8.1 Upgrade』を参照してください。
  - config は、Business Process Editor を起動します。
  - console は、Identity Manager コンソールを起動します。
  - genReports は、Identity Manager レポート機能のサンプルとして使用できるランダムなデータのセットを生成します。

- `import` は、Identity Manager オブジェクトをインポートします。厳密モードの場合は `-s` オプションを指定します。厳密モードを有効にすると、インポート中の参照チェックがより厳しく行われます。
- `js` は、JavaScript プログラムを起動します。
- `javascript` も、JavaScript プログラムを起動します。
- `msgtool` は、`WPMessages.properties` からカスタムメッセージカタログを生成します。このカタログを操作して、テキストや言語に独自の変更を加えることができます。
- `script` は、JavaScript または BeanShell を実行します。
- `setRepo` は、Identity Manager インデックスリポジトリを設定します。
- `setup` は、Identity Manager 設定プロセスを開始します。ライセンスキーの設定、Identity Manager インデックスリポジトリの設定、および設定ファイルのインポートを実行できます。
- `spml` は、SPML ブラウザを起動します。
- `syslog [options]` は、システムログからレコードを抽出します。詳細については、570 ページの「`syslog` コマンド」を参照してください。
- `waveset` は、`console` コマンドの別名です。上の「`console`」を参照してください。
- `xmlparse` は、Identity Manager オブジェクトの XML を検証します。
- `xpress [options]` *Filename* は、式を評価します。有効なオプションは、`-trace` (トレース出力の有効化) です。

使用上の注意

lh コマンドを使用する場合は、次の点に注意する必要があります。

- コマンドの使用方法についてヘルプを表示するには、引数を指定せずに lh を入力します。
- lh コマンドのパス環境変数を設定する場合は、次のように設定します。
  - JAVA_HOME の場所を、Java の実行可能ファイルが格納されている bin ディレクトリを含む JRE ディレクトリに設定します。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\jre1.5.0_14 (または同様の場所) 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\jre1.5.0_14 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、組み込み型の 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 C:\java\jdk1.5.0_14\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、次のように入力します。

    ```
    set WSHOME=C:\Program Files\tomcat\webapps\idm
    ```

    注 – WSHOME 変数の値に、次の文字を使用することはできません。

    - 引用符 (“ “)

      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。
    - パスの末尾にバックスラッシュ (\)

    また、UNIX システム上では次のように入力してパス変数をエクスポートする必要があります。

    ```
    export WSHOME
    export JAVA_HOME
    ```

- コマンドを 64 ビットモードで実行するには、lh スクリプトの FLAGS="$FLAGS -d64" 行のコメントを解除します。
- Identity Manager コマンド行インタフェースを起動するには、次のように入力します。
  - Windows では、コマンド行に次のように入力します。

    ```
    %WSHOME%\bin\lh
    ```
  - UNIX では、コマンド行に次のように入力します。

    ```
    $WSHOME/bin/lh
    ```

lh コマンドの例

- lh com.waveset.session.WavesetConsole
- lh console
- lh console– u $user– p *PathtoPassword*.txt
- lh setup -U *Administrator* -P *PathtoPassword*.txt
- lh setRepo– c -A *Administrator* -C *PathtoPassword* .txt
- lh setRepo– t *LocalFiles* – f $WSHOME

syslog コマンド

この節では、syslog コマンドについて、次の内容を説明します。

- 570 ページの「syslog コマンドの使用法」
- 570 ページの「syslog コマンドのオプション」

syslog コマンドの使用法

syslog コマンドを呼び出すには、次の構文を使用します。

```
syslog [options]
```

syslog コマンドのオプション

次のオプションを使用して、表示する情報の範囲を決定します。

表 A–1 syslog コマンドのオプション

オプション	説明
-d *Number*	直近の *Number* 日分のレコードを表示します (デフォルト =1)。
-E	重要度レベルが「error」以上のレコードのみを表示します。
-F	重要度レベルが「fatal」のレコードのみを表示します。
-i *LogID*	指定した syslog ID を持つレコードのみを表示します。 syslog ID は一部のエラーメッセージに表示され、特定のシステムログエントリを参照するものです。
-W	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	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。

◆ ◆ ◆ 付 録 B

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。

- 573 ページの「Oracle データベースタイプ」
- 575 ページの「DB2 データベースタイプ」
- 577 ページの「MySQL データベースタイプ」
- 578 ページの「SQL Server データベースタイプ」
- 580 ページの「監査ログデータベースマッピング」

Oracle データベースタイプ

表 B–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 B–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
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)

表 B–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
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) または CLOB (表の最後の注 [1] を参照)
acctAttrChanges	VARCHAR(4000) または CLOB
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) または CLOB (表の最後の注 [1] を参照)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
sequence	CHAR(19)

表 B–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
xmlSize	NUMBER(19,0)
xml	BLOB

注 – これらの列の長さ制限は設定可能です。デフォルトのデータ型は VARCHAR で、デフォルトのサイズ制限を括弧内に示しています。サイズ制限を調整する方法については、356 ページの「監査ログ設定」を参照してください。

DB2 データベースタイプ

表 B–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 B–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
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(50)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) または CLOB (表の最後の注 [1] を参照)
acctAttrChanges	CLOB(16M)

表 B–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
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) または CLOB (表の最後の注 [1] を参照)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
sequence	CHAR(19)
xmlSize	DECIMAL(19,0)
xml	CLOB(16M)

注 – これらの列の長さ制限は設定可能です。デフォルトのデータ型は VARCHAR で、デフォルトのサイズ制限を括弧内に示しています。サイズ制限を調整する方法については、356 ページの「監査ログ設定」を参照してください。

MySQL データベースタイプ

表 B–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 B–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
repomod	TIMESTAMP
resourceName	VARCHAR(128)
accountName	VARCHAR(255)
objectType	CHAR(2)
objectName	VARCHAR(128)
action	CHAR(2)
actionDateTime	CHAR(21)
actionStatus	CHAR(1)
interface	VARCHAR(50)
server	VARCHAR(128)
subject	VARCHAR(128)
reason	CHAR(2)
message	VARCHAR(255) または CLOB (表の最後の注 [1] を参照)
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)

表 B–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
acctAttr05label	VARCHAR(50)
acctAttr05value	VARCHAR(128)
parm01label	VARCHAR(50)
parm01value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm02label	VARCHAR(50)
parm02value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm03label	VARCHAR(50)
parm03value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm04label	VARCHAR(50)
parm04value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm05label	VARCHAR(50)
parm05value	VARCHAR(128) または CLOB (表の最後の注 [1] を参照)
sequence	CHAR(19)
xmlSize	BIGINT
xml	MEDIUMTEXT

注 – これらの列の長さ制限は設定可能です。デフォルトのデータ型は VARCHAR で、デフォルトのサイズ制限を括弧内に示しています。サイズ制限を調整する方法については、356 ページの「監査ログ設定」を参照してください。

SQL Server データベースタイプ

表 B–4 に SQL Server データベースタイプのデータスキーマ値を示します。

表 B–4 SQL Server 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	NVARCHAR(50) NOT NULL
name	NVARCHAR(128) NOT NULL
repomod	DATETIME NOT NULL CURRENT_TIMESTAMP

表 B–4 SQL Server 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
resourceName	NVARCHAR(128)
accountName	NVARCHAR(255)
objectType	NCHAR(2)
objectName	NVARCHAR(128)
action	NCHAR(2)
actionDateTime	NCHAR(21)
actionStatus	NCHAR(1)
interface	NVARCHAR(50)
server	NVARCHAR(128)
subject	NVARCHAR(128)
reason	NCHAR(2)
message	NVARCHAR(255) または CLOB (表の最後の注 [1] を参照)
acctAttrChanges	NTEXT
acctAttr01label	NVARCHAR(50)
acctAttr01value	NVARCHAR(128)
acctAttr02label	NVARCHAR(50)
acctAttr02value	NVARCHAR(128)
acctAttr03label	NVARCHAR(50)
acctAttr03value	NVARCHAR(128)
acctAttr04label	NVARCHAR(50)
acctAttr04value	NVARCHAR(128)
acctAttr05label	NVARCHAR(50)
acctAttr05value	NVARCHAR(128)
parm01label	NVARCHAR(50)
parm01value	NVARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm02label	NVARCHAR(50)
parm02value	NVARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm03label	NVARCHAR(50)

表 B–4 SQL Server 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
parm03value	NVARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm04label	NVARCHAR(50)
parm04value	NVARCHAR(128) または CLOB (表の最後の注 [1] を参照)
parm05label	NVARCHAR(50)
parm05value	NVARCHAR(128) または CLOB (表の最後の注 [1] を参照)
sequence	NTEXT
xmlSize	NUMERIC(19,0)
xml	NTEXT

注 – これらの列の長さ制限は設定可能です。デフォルトのデータ型は VARCHAR で、デフォルトのサイズ制限を括弧内に示しています。サイズ制限を調整する方法については、356 ページの「監査ログ設定」を参照してください。

監査ログデータベースマッピング

表 B–5 に、格納される監査ログデータベースキーと、監査レポート出力でこれらのキーに対応する表示文字列のマッピングを示します。Identity Manager 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項目を短いデータベースキーとして保存します。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 B–6 には監査可能なアクションのデータベースキー、表 B–7 にはアクション状態キー、および表 B–8 にはデータベース内にキーとして格納されている理由コードを示します。

表 B–5 オブジェクトキータイプのデータベースキー

タイプ名	説明	DbKey
AccessReview	AccessReview	AV
AccessReviewWorkflow*	Access Review Workflow	AW
AccessScan	AccessScan	AS
Account	Account	AN

表 B–5 オブジェクトキータイプのデータベースキー (続き)

タイプ名	説明	DbKey
AdminGroup	Capability	AG
Administrator	Administrator	AD
AdminRole	Admin Role	AR
Application	Resource Group	AP
AttributeDefinition	AttributeDefinition	AF
AttrParse	AttrParse	AT
AuditConfig	AuditConfig	AC
AuditPolicy	AuditPolicy	CP
BeanPod	Bean Pod	BP
ComplianceViolation	ComplianceViolation	CV
Configuration	Configuration	CN
DataExporter	Data Exporter	DE
Discovery	Discovery	DS
Email*	Email	EM
EmailTemplate	EmailTemplate	ET
EncryptionKey	EncryptionKey	KY
Event	Event	EV
Extract	Extract	ER
ExtractTask	ExtractTask	EX
IDMXUser*	Directory User	UX
LighthouseAccount*	Identity System Account	LA
LoadConfig	LoadConfig	LD
LoadTask	LoadTask	LT
Log	Log	LG
LoginApp	LoginApp	LP
LoginConfig	LoginConfig	LC
LoginModGroup	LoginModGroup	LF
MetaView	Meta View	MV

表 B–5 オブジェクトキータイプのデータベースキー (続き)

タイプ名	説明	DbKey
ObjectGroup	Organization	OG
Policy	Policy	PO
ProvisioningTask	ProvisioningTask	PT
RemediationWorkflow*	Remediation Workflow	RW
RemedyConfig	RemedyConfig	RC
Resource	Resource	RS
ResourceAccount*	Resource Account	RA
ResourceAction	ResourceAction	RN
ResourceForm	ResourceForm	RF
ResourceObject	ResourceObject	RE
RiskReportTask	RiskReportTask	RR
Role	Role	RL
Rule	Rule	RU
SnapShot	SnapShot	SS
ServerObject	ServerObject	SV
SysLog	SysLog	SL
System	System	SY
TaskDefinition	TaskDefinition	TD
TaskInstance	TaskInstance	TI
TaskResult	TaskResult	TR
TaskResultPage	ResultPage	TP
TaskSchedule	TaskSchedule	TS
TaskTemplate	TaskTemplate	TT
TestNotification*	Test Notification	TN
User	User	US
UserEntitlement	UserEntitlement	UE
UserForm	UserForm	UF
WorkflowCase*	Workflow Case	WC

表 B–5 オブジェクトキータイプのデータベースキー (続き)

タイプ名	説明	DbKey
WorkItem	WorkItem	WI
XmlData	XmlData	XD

1

表 B–6 アクションのデータベースキー

アクション名	説明	DbKey
Allowed*	Allowed	AL
Approve	Approve	AP
Assign Audit Policies	Assign Audit Policies	AA
Assign Capabilities	Assign Capabilities	AC
AttestorApproved*	Attestor Approved	TA
AttestorRejected*	Attestor Rejected	AR
AttestorRemediate*	Remediation Requested	AF
AttestorRescan*	Rescan Requested	AN
Bulk Change Password	Bulk Change Password	BW
Bulk Create	Bulk Create	BC
Bulk Delete	Bulk Delete	BD
Bulk Deprovision	Bulk Deprovision	BP
Bulk Disable	Bulk Disable	BF
Bulk Enable	Bulk Enable	BE
Bulk Modify	Bulk Modify	BM
Bulk Reset Password	Bulk Reset Password	BR
Bulk Unassign	Bulk Unassign	BU
Bulk Unlink	Bulk Unlink	BL
Bypass Verify	Bypass Verify	BV
CancelReconcile*	Cancel Reconcile	CR

[1] * 拡張タイプ

表 B–6 アクションのデータベースキー (続き)

アクション名	説明	DbKey
challengeResponse*	Challenge Response	CD
Change Password	Change Password	CP
Connect	Connect	CN
Control Active Sync	Control Active Sync	CA
Create	Create	CT
CredentialsExpired*	Credentials Expired	CE
Debug	Debug	DB
Delegate	Delegate	DG
Delete	Delete	DL
Deprovision	Deprovision	DP
Disable	Disable	DS
Disconnect	Disconnect	DC
Enable	Enable	EN
End Activity	End Activity	EA
End Process	End Process	PE
End Workflow	End Workflow	EW
Execute	Execute	LN
Expired*	Expired	EX
Export	Export	EP
Fixed*	Fixed	FX
Import	Import	IM
List	List	LI
Lock	Lock	LK
Login	Login	LG
Logout*	Logout	LO
Mitigated*	Mitigated	VM
Modify	Modify	MO
Modify Active Sync	Modify Active Sync	MA

表 B–6 アクションのデータベースキー (続き)

アクション名	説明	DbKey
NativeChange*	Native Change	NC
Notify*	Notify	NO
PostOperation*	Post-Operation Callout	PT
PreOperation*	Pre-Operation Callout	PP
Prioritize*	Prioritize	PR
Provision	Provision	PV
Recurring*	Recurring	RC
Reject	Reject	RJ
Remediated*	Remediated	VR
Rename	Rename	RE
RequestReconcile*	Request Reconcile	RR
ResetPassword	ResetPassword	RP
Run Debugger	Run Debugger	RD
ScanBegin*	Scan Begin	SB
ScanEnd*	Scan End	SE
StartActivity*	Start Activity	SA
StartProcess*	Start Process	SP
StartWorkflow*	Start Workflow	SW
Terminate*	Terminate	TR
Unassign	Unassign	UA
Unlink	Unlink	UN
Unlock	Unlock	UL
updateAuthenticationAnswers*	Update Authentication Answers	AQ
usernameRecovery*	Username Recovery	UR
View	View	VW
View Only	View Only	VO

2

表 B–7 アクション状態のデータベースキー

結果	DbKey
Success	S
Failure	F

表 B–8 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	不正なクレデンシャル	CR
InsufficientPrivileges	不十分な特権	IP
DatabaseAccessFailed	データベースアクセス失敗	DA
AccountDisabled	アカウント無効	DI

[2] * 拡張アクション

◆ ◆ ◆ 付録 C

ユーザーインタフェースクイックリファレンス

表 C–1 に、一般的に使用される Identity Manager タスクのクイックリファレンスを示します。この表では、各タスクを開始する主要な 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は、それらも示します。

Identity Manager インタフェースのタスクリファレンス

表 C–1 タスクリファレンス

実行するタスク	使用するインタフェース	その他のインタフェース
Identity Manager ユーザーの管理:		
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」タブ	
ユーザー認証の設定 (ポリシー)	「セキュリティー」タブ、「ポリシー」選択	

表 C–1 タスクリファレンス (続き)

実行するタスク	使用するインタフェース	その他のインタフェース
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)
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:		
組織を通じて委任された管理の設定	「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」タブ	

表C–1 タスクリファレンス (続き)

実行するタスク	使用するインタフェース	その他のインタフェース
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」タブ	
承認者の設定(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:		
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設定	「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設定。 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	
アカウントとデータの読み込みと同期:		

表 C–1 タスクリファレンス (続き)

実行するタスク	使用するインタフェース	その他のインタフェース
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 ユーザーとリソースアカウントの比較	「リソース」タブ、「リソースの調整」選択	
コンプライアンスの監査と管理:		
監査の無効化または有効化	「設定」タブ、「監査」選択	
イベント監査取得の設定	「設定」タブ、「監査」選択	
監査ポリシーの定義 (作成、編集、削除)	「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	
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」タブ	
ポリシー違反是正リクエストに対する応答	「自分の作業項目」タブ、「是正」選択	
ポリシー違反の受け入れ	「作業項目」タブ、「是正」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」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」タブ	

表C–1 タスクリファレンス (続き)

実行するタスク	使用するインタフェース	その他のインタフェース
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	
定期的アクセスレビューの設定	「コンプライアンス」タブ、「アクセススキャンの管理」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	
管理者監査機能の編集	「セキュリティー」タブ、「機能」タブ	
監査通知用の電子メールテンプレートの設定	「設定」タブ、「電子メールテンプレート」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」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、「アクセススキャンの管理」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」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」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」タブ	
定期的アクセスレビューの設定	「コンプライアンス」タブ、「アクセススキャンの管理」タブ	

表 C–1 タスクリファレンス (続き)

実行するタスク	使用するインタフェース	その他のインタフェース
アクセスレビュー状態の監視	「コンプライアンス」タブ、「アクセスレビュー」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」タブ	
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」タブ	
リスク分析とレポート:		
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では「レポート」タブ、「レポートの実行」選択、レポート結果の表示では「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	
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」タブ	
Identity Manager タスクの管理:		
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	

表C–1 タスクリファレンス (続き)

実行するタスク	使用するインタフェース	その他のインタフェース
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:		
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	

◆ ◆ ◆ 付 録 D

機能の定義

この付録では、Identity Manager で使用する各種機能の定義について説明します。

これらの情報は、次のように構成されています。

- 595 ページの「タスクベースの機能の定義」
- 619 ページの「実用上の機能の定義」

機能の一般的な情報については、214 ページの「機能とその管理について」を参照してください。

注 – すべての機能で、ユーザーと管理者は、「パスワード」から「自分のパスワードの変更」タブおよび「自分の秘密の質問の回答の変更」タブにアクセスできます。

タスクベースの機能の定義

この節では、ユーザーに割り当てることができるタスクベースの各機能について説明します。各機能でアクセスできるタブとサブタブも示します。機能は、名前のアルファベット順に並べられています。

注 – この表には、「自分のパスワードの変更」タブなどの、すべてのユーザーが利用できるデフォルトのタブおよびサブタブについての情報は含まれていません。

表 D–1 Identity Manager タスクベースの機能の定義

機能	管理者とユーザーが実行できる操作	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、アクセスレビュー範囲レポート、およびアクセススキャンユーザー範囲レポートの作成、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
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」→「レポートの実行」タブ、「レポートの表示」タブ
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。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ、「ファイルへ抽出」タブ、「ファイルから読み込み」タブ、「リソースから読み込み」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Admin Report Administrator	管理者レポートおよび管理者ロールレポートの作成、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 (管理者レポートおよび管理者ロールレポートのみ)
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」タブ
Application Administrator	アプリケーションロールの作成、編集、および削除	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ (ロールの同期) 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Asset Administrator	アセットロールの作成、編集、および削除	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ (ロールの同期) 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Assign Audit Policies Administrator	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 「ユーザーアクション」リストのユーザー監査ポリシーの編集、および「組織アクション」リストの組織監査ポリシーの編集。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ
Assign Organization Audit Policies Administrator	組織のみへの監査ポリシーの割り当て。 「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」→「アカウントのリスト」タブ
Assign User Audit Policies Administrator	ユーザーのみへの監査ポリシーの割り当て。 「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」→「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) 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。	「アカウント」→「アカウントのリスト」タブ (編集のみ)、「ユーザーの検索」タブ
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」タブ
Audit Policy Scan Report Administrator	監査ポリシースキャンタスクの実行またはスケジュール。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ、「スケジュールの管理」タブ
Audit Report Administrator	監査レポートの作成、修正、削除、および実行 監査ログレポート、ユーザーの変更履歴レポート、単一ユーザー用の監査ログレポート、および使用状況レポートのみへのアクセス。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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」→「レポートの実行」タブ
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」→「レポートの実行」タブ、「レポートの表示」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」タブ
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。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ、「スケジュールの管理」タブ 「レポート」→「レポートの実行」タブ、「レポートの表示」タブ 「コンプライアンス」→「ポリシーの管理」タブ、「アクセススキャンの管理」タブ、「アクセスレビュー」タブ
Auditor Attestor	組織のセキュリティーを有効にしているとき、ほかのユーザーのアテステーションのアテストに必要。	デフォルトの「パスワード」タブおよび「作業項目」タブのみ
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	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「コンプライアンス」→「アクセススキャンの管理」タブ、「アクセスレビュー」タブ
Auditor Remediator	監査ポリシー違反の是正、受け入れ、および転送。	デフォルトの「パスワード」タブおよび「作業項目」タブのみ
Auditor Report Administrator	任意の監査レポートの作成、修正、削除、および実行	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ、「スケジュールの管理」タブ 「レポート」→監査レポートのすべての操作

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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」タブ、「ユーザーの検索」タブ
Audit Policy Violation History Administrator	違反履歴 (監査ポリシー別) レポートの作成、修正、削除、および実行。	「レポート」→「レポートの実行」タブ
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」→「アカウントのリスト」タブ、「ユーザーの検索」タブ、「一括アクションの起動」タブ、「ファイルへ抽出」タブ、「ファイルから読み込み」タブ、「リソースから読み込み」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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、削除以外の通常操作および一括操作の実行。 ユーザーを作成または削除することはできません。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Bulk Change Resource Password Administrator	指定されたリソースでの、指定されたリソース接続アカウントのパスワードの変更	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ、「一括アクションの起動」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操作の実行。 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。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Bulk Create Users	リソースの割り当てと、ユーザー作成リクエストの発行 (ユーザーごとに一括操作によって作)。	「アカウント」→「アカウントのリスト」タブ (作成のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Bulk Delete Users	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ニング解除、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」タブ、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 *(続き)*

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Bulk Delete IDM Users	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」タブ (削除のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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 (ユーザーごとに一括操作によって)。	「アカウント」→「アカウントのリスト」タブ (プロビジョニング解除のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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」タブ (無効化のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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」タブ (有効化のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Bulk Reset Resource Password Administrator	指定されたリソースでの、指定されたリソース接続アカウントのパスワードのリセット	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ、「一括アクションの起動」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 (ユーザーごとに一括操作によって)。	「アカウント」→「アカウントのリスト」タブ (割り当て解除のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Bulk Unlink User	既存のリソースアカウントのリンク解除 (ユーザーごとに一括操作によって)。	「アカウント」「アカウントのリスト」タブ (リンク解除のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Bulk Update Users	既存のユーザーとリソースアカウントの編集、移動、および更新 (ユーザーごとに一括操作によって)	「アカウント」→「アカウントのリスト」タブ (アクションの編集、移動、更新のみ)、「ユーザーの検索」タブ、「一括アクションの起動」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 *(続き)*

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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操作の実行。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ、「一括アクションの起動」タブ、「ファイルへ抽出」タブ、「ファイルから読み込み」タブ、「リソースから読み込み」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Business Role Administrator	ビジネスロールの作成、編集、および削除	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ (ロールの同期) 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Capability Administrator	機能の作成、修正、および削除。	「セキュリティー」→「機能」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。一括操作は含まれません。 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の実行。 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。ユーザーを削除することはできません。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Change Resource Active Sync Administrator	Active Sync リソースパラメータの変更。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ
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。 Export Password Scan タスクへのアクセスのみ (「タスクの実行」タブから)。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「パスワード」→「ユーザーパスワードの変更」 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
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。 「期限切れパスワードのスキャン」 タスクへのアクセスのみ (「タスクの実行」タブから)。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「パスワード」→「ユーザーパスワードの変更」タブ (アクションの前に検証が必要) 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Change Resource Password Administrator	リソース管理者アカウントパスワードの変更。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)。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Change User Account Administrator	削除と一括操作を除く、既存のユーザーに対するすべての操作の実行。機能の作成と削除、およびユーザーへの機能の割り当ても実行できません。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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」→「監査」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」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	「リソース」→「リソースのリスト」タブ Active Sync リソース: Active Sync アクションのメニュー
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。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (作成のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Data Warehouse Administrator	データエクスポータの設定と「データウェアハウスエクスポータ起動ツール」タスクの実行	「レポート」→「ダッシュボードグラフ」タブ、「ダッシュボードの表示」タブ 「リソース」→「リソースのリスト」タブ 「設定」→「ウェアハウス」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Data Warehouse Query	フォレンジッククエリーの設定と実行	「レポート」→「ダッシュボードグラフ」タブ、「ダッシュボードの表示」タブ 「リソース」→「リソースのリスト」タブ 「コンプライアンス」→「フォレンジッククエリー」
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ニング解除、割り当て解除、リンク解除。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (削除のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Delete IDM User	Identity Manager ユーザーアカウントの削除。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (削除のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (プロビジョニング解除のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 *(続き)*

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (無効化のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (有効化のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
End User Administrator	End User 機能および End User が管理する組織の規則で指定されているオブジェクトタイプに対する権限の表示と変更	すべてのデフォルトのタブ
External Resource Administrator	外部リソースの表示と設定のみ。新しいリソースは作成できません。	「設定」→「External Resources」タブ
Configure Identity Manager Schema	ユーザーまたはロールに対して有効なスキーマの、Identity Manager 設定オブジェクトの `IDM Schema Configuration` を使用した表示と設定。	すべてのデフォルトのタブ
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」→「アカウントのリスト」タブ、「ユーザーの検索」タブ、「ファイルへ抽出」タブ、「ファイルから読み込み」タブ、「リソースから読み込み」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
IT Role Administrator	IT ロールの作成、編集、および削除	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ (ロールの同期)
		「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
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。	「セキュリティー」→「ログイン」タブ
Organization Administrator	組織とディレクトリジャンクションの作成および編集。組織の削除のみ。	「アカウント」→「アカウントのリスト」タブ
Organization Approver	新しい組織に対するリクエストの承認	デフォルトの「パスワード」タブおよび「作業項目」タブのみ
Organization Violation History Administrator	組織別違反履歴表示レポートの作成、編集、削除、実行のみ。	「レポート」→「レポートの実行」タブ
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スト、変更、およびリセット。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ
		「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ
		「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ
		「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Password Administrator (Verification Required)	ユーザーおよびリソースアカウントパスワードのリスト、変更、およびリセット。操作が成功するには、ユーザーの秘密の質問の回答が正しく検証される必要があります。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Perform Debug	Identity Manager のデバッグページからの操作の実行。 注 – メニューからは Identity Manager デバッグページにアクセスできません。デバッグページにアクセスするには、ブラウザに次の URL を入力します。 `http://<AppServerHost>:<Port>/idm/debug`	すべてのデフォルトのタブ
Policy Administrator	ポリシーの作成、編集、および削除。	「セキュリティー」→「ポリシー」タブ
Policy Summary Report Administrator	ポリシーの概要レポートの作成、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
Register Identity Manager Product Component	Identity Manager のインストールの Sun Microsystems への登録、またはローカルサービスタグの作成。	「設定」→「製品登録」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」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ (調整タスクの表示) 「リソース」→「リソースのリスト」タブ、「アカウントインデックスの検査」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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」タブ (アカウントインデックスレポートのみ)、「レポートの表示」タブ
Reconcile Request Administrator	調整リクエストの管理	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ (リストおよび調整機能のみ)、「レポートの表示」タブ
Remedy Integration Administrator	Remedy との統合設定の編集 (タスクの表示、ロール同期の実行)。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「設定」→「Remedy との統合」タブ
Rename User	既存のユーザーおよびリソースアカウントの名前変更 (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)。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Report Administrator	監査設定の設定、すべてのレポートタイプの実行 (タスクの表示、ロール同期の実行)。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「レポート」→「レポートの実行」タブ、「レポートの表示」タブ、「リスク分析の実行」タブ、「リスク分析の表示」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ 「設定」→「監査」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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」タブ、「ユーザーの検索」タブ (パスワードのリセットのみ) 「パスワード」→「ユーザーパスワードのリセット」 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ (この機能を持つユーザーが利用できるタスクはありません) 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Reset Password Administrator (Verification Required)	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。操作が成功するには、ユーザーの秘密の質問の回答が正しく検証される必要があります。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「パスワード」→「ユーザーパスワードのリセット」 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ (この機能を持つユーザーが利用できるタスクはありません) 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Reset Resource Password Administrator	リソース管理者アカウントパスワードのリセット (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」)。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ
Resource Administrator	リソースの作成、編集、および削除。リソースユーザーレポートおよびリソースグループレポートは、範囲外のリソースではエラーを返します。グローバルポリシー、パラメータ、およびリソースグループの編集。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ません。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ、「リソースグループのリスト」タブ、「アカウントインデックスの検査」タブ 「設定」→「コネクタサーバー」

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Resource Approver	リソースの割り当ての承認	すべてのデフォルトの「パスワード」タブおよび「作業項目」タブ
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」タブ
Resource Object Administrator	リソースオブジェクトの表示、作成、修正、および削除。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ
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。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「リソース」→「リソースのリスト」タブ (アクションメニューの「接続の管理」→「パスワードの変更」で、リソースパスワードの変更のみ)
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」→「レポートの実行」タブ、「レポートの表示」タブ
Resource Violation History Administrator	違反履歴 (リソース別) 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」
Risk Analysis Administrator	リスク分析の作成、編集、削除、および実行。	「レポート」→「リスク分析」タブ、「リスク分析の表示」タブ
Role Administrator	ロールの作成、編集、同期、および削除。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Role Approver	ロールの割り当ての承認	すべてのデフォルトの「パスワード」タブおよび「作業項目」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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」→「レポートの実行」タブ、「レポートの表示」タブ 「ロール」→「ロールのリスト」タブ
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」→「レポートの実行」タブ、「レポートの表示」タブ
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」→「レポートの実行」タブ、「レポートの表示」タブ
Run Admin Report	管理者レポートの実行。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run Audit Policy Scan Report	監査ポリシースキャンレポートの実行	「サーバータスク」→「すべてのタスク」、「タスクの検索」、「タスクの実行」のみ
Run Audit Report	監査レポート、監査ログレポート、Historical User Change レポート、単一ユーザー用の監査ログレポート、および使用状況レポートの実行のみ。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run Audited Attribute Report	監査された属性のレポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run Auditor Report	監査ログレポートタイプのすべてのレポートの実行。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run AuditLog Report	監査ログレポート、Today's Activity レポート、Weekly Activity レポートの実行および表示。	「レポート」→「レポートの実行」
Run Audit Policy Violation History	組織別違反履歴表示レポート、Today's Activity レポート、Weekly Activity レポートの実行および表示。	「レポート」→「レポートの実行」

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Run Policy Summary Report	ポリシーの概要レポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」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」→「レポートの実行」タブ
Run Reconcile Report	アカウントインデックスレポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run Resource Report	リソースユーザーレポートとリソースグループレポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run Resource Violation History	リソース別違反履歴レポートの実行。	「レポート」→「レポートの実行」タブ
Run Risk Analysis	リスク分析の実行および表示。	「レポート」→「リスク分析の実行」タブ、「リスク分析の表示」タブ
Run Role Report	ロールレポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ 「ロール」→「ロールのリスト」タブ
Run Separation of Duties Report	職務分掌レポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run Task Report	タスクレポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run User Access Report	「ユーザーの詳細」 レポートと「ユーザーアクセス」 レポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run User Report	ユーザーレポートの実行および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Run Violation Summary Report	違反の概要レポートの実行	「レポート」→「レポートの実行」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Security Administrator	機能を持つユーザーの作成、ユーザーの有効化と無効化、リソースオブジェクトのリスト表示と制御、暗号化キーの管理、ログインと監査設定の管理、およびポリシーの管理。	「アカウント」→「アカウントのリスト」タブ (一部のアクション)、「ユーザーの検索」タブ (監査レポート) 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ、「タスクの設定」タブ 「レポート」→「レポートの実行」タブ、「レポートの表示」タブ、「ダッシュボードグラフ」タブ、「ダッシュボードの表示」タブ、「レポートの設定」タブ 「リソース」→「リソースのリスト」 「設定」→「監査」タブ、「ウェアハウス」タブ 「セキュリティー」→「証明書」タブ、「ログイン」タブ、「ポリシー」タブ 「サービスプロバイダ」→「ユーザー検索設定の編集」
Separation of Duties Report Administrator	職務分掌レポートの作成、編集、実行、表示、および削除。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Service Provider Admin Role Administrator	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

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
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」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」→「ダッシュボードグラフ」タブ 「レポート」→「ダッシュボードの表示」タブ 「サービスプロバイダ」→「メイン設定の編集」タブ、「トランザクション設定の編集」タブ、「ユーザー検索設定の編集」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」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」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」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」
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」タブ
Task Report Administrator	タスクレポートの作成、編集、削除、実行、および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
Unassign User	既存のリソースアカウントの割り当て解除とリンク解除。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (割り当て解除のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Unlink User	既存のリソースアカウントのリンク解除。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (リンク解除のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
Unlock User	ロック解除をサポートしている既存のユーザーのリソースアカウントのロック解除。一括操作は含まれません。	「アカウント」→「アカウントのリスト」タブ (ロック解除のみ)、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」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。既存のサーバータスクの管理。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
User Access Report Administrator	ユーザーアクセスレポートの作成、編集、削除、実行、および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	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 (ユーザーへの機能の割り当てを除く)。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ、「ファイルへ抽出」タブ、「ファイルから読み込み」タブ、「リソースから読み込み」タブ 「パスワード」→「ユーザーパスワードの変更」タブ、「ユーザーパスワードのリセット」タブ 「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ 「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
User Report Administrator	ユーザーレポートの作成、編集、削除、実行、および表示。	「レポート」→「レポートの実行」タブ、「レポートの表示」タブ
View Application	アプリケーションタイプロールのリスト、およびアプリケーションタイプロール情報の表示。変更操作は許可されません。	「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
View Asset	アセットタイプロールのリスト、およびアセットタイプロール情報の表示。変更操作は許可されません。	「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
View Business Role	ビジネスロールのリスト、およびビジネスロール情報の表示。変更操作は許可されません。	「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
View IT Role	IT ロールのリスト、および IT ロール情報の表示。変更操作は許可されません。	「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
View Role	すべてのロールタイプのリスト、およびすべてのロール情報の表示。変更操作は許可されません。	「ロール」→「ロールのリスト」タブ、「ロールの検索」タブ
View User	個々のユーザーの詳細の表示。変更操作は許可されません。	「アカウント」→「アカウントのリスト」タブ、「ユーザーの検索」タブ

表 D–1 Identity Manager タスクベースの機能の定義 (続き)

機能	管理者とユーザーが実行できる操作	アクセス可能なタブとサブタブ
Violation Summary Report Administrator	違反の概要レポートの作成、編集、削除、および実行。	「レポート」→「レポートの実行」タブ
Identity System Administrator	システム設定オブジェクトの編集、ロールの同期、ソースアダプタテンプレートの編集、レポートの実行など、システム全体に関するタスクの実行。	「サーバータスク」→「タスクの検索」タブ、「すべてのタスク」タブ、「タスクの実行」タブ、「スケジュールの管理」タブ、「タスクの設定」タブ 「レポート」→「レポートの実行」タブ、「レポートの表示」タブ、「ダッシュボードグラフ」タブ、「ダッシュボードの表示」タブ、「レポートの設定」タブ 「リソース」→「リソースのリスト」 「設定」→「監査」タブ、「ウェアハウス」タブ、「電子メールテンプレート」タブ、「フォームおよびプロセスマッピング」タブ、「サーバー」タブ、「ユーザーインタフェース」タブ、「製品登録」タブ 「コンプライアンス」→「アクセスレビュー」 「セキュリティー」→「証明書」

実用上の機能の定義

実用上の機能は、タスクベースの機能のほか、それ以外の実用上の機能から構成されます。

- **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**
- **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

- Audit Policy 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

- **Auditor View User**

  View User

- **Bulk Account Administrator**
  - Approver Administrator
  - Assign User Capabilities
  - Bulk User Account Administrator
    - Bulk Create User
    - Bulk Delete 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 Administrator**
        - Change Active Sync Resource Administrator
        - Control Active Sync Resource Administrator
        - Resource Group Administrator
    - **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**
    - **Data Warehouse Administrator**
    - **Data Warehouse Query**

- **Debug**
- **End User Administrator**
- **IDM Schema Configuration**
- **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**
- **Product 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
    - 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
    - AuditLog Report Administrator

      Run AuditLog Report
    - Audit Policy Violation History Administrator

      Run Audit Policy Violation History

- Organization Violation History Administrator

  Run Organization Violation History
- Policy Summary Report Administrator

  Run Policy Summary Report
- Reconcile Report Administrator

  Run Reconcile Report
- Resource Violation History Administrator

  Run Resource Violation History
- Run Auditor Report
  - Run Access Review Detail Report
  - Run Access Review Summary Report
  - Run Audit Policy Scan Report
  - Run Audited Attribute Report
  - Run AuditLog Report
  - Run Audit Policy Violation History
  - Run Organization Violation History
  - Run Policy Summary Report
  - Run Resource Violation History
  - Run Separation of Duties Report
  - Run User Access Report
  - Run Violation Summary Report
- Separation of Duties Report Administrator

  Run Separation of Duties Report
- User Access Report Administrator

  Run User Access Report
- Violation Summary Report Administrator

  Run Violation Summary Report

- 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**
  - Application Administrator
  - Asset Administrator
  - Business Role Administrator
  - IT 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**
- **Waveset Administrator**

用語集

Business Process Editor (BPE)
バージョン 7.0 より前の Identity Manager に用意されていた、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するツール。現在のバージョンの Identity Manager では、Identity Manager IDE に置き換えられています。用語集を参照してください。

Identity Manager IDE
Identity Manager Integrated Development Environment (Identity Manager IDE) は、配備された Identity Manager オブジェクトを表示、カスタマイズ、およびデバッグするアプリケーションです。Identity Manager IDE は、NetBeans プラグインとして提供されています。

IT ロール
「IT ロール」ロールタイプは、Identity Manager に備わる 4 つのロールタイプのうちの 1 つで、ロール (アセット、アプリケーション、その他の入れ子になった IT ロール)、リソース、およびリソースグループの集まりです。設定によっては、IT ロールを直接ユーザーに割り当てることも可能ですが、通常、IT ロールはビジネスロールに割り当てられ、それらのビジネスロールがユーザーに割り当てられます。

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。

アカウント属性
アカウント属性は、Identity Manager 管理者に、管理対象リソースの属性にマップする標準的な名前のセットを作成する手段を提供します。たとえば、*fullname* という名前の Identity Manager 属性を、Active Directory リソースの *displayName* 属性と LDAP リソースの *cn* 属性にマップするとします。Identity Manager でユーザーの *fullname* 属性に対して行なった変更は、ユーザーのリモートリソースアカウントにある、そのユーザーの *displayName* 属性と *cn* 属性に渡されます。

アクセスレビュー
マネージャーなどの責任のある関係者が、ユーザーのアクセス特権をレビューおよび確認できるようにする、監査されたプロセス。ユーザーエンタイトルメントレコードは、自動的に承認または却下できます。 または、手動でアテストできます。「アテステーション」も参照してください。

アセット (ロール)
Identity Manager の 4 つのロールタイプのうちの 1 つ。「アセット」ロールタイプは通常、手動のプロビジョニングを必要とする、携帯電話やポータブルコンピュータなどの接続されていないリソースやデジタルでないリソース用に予約されています。アセットロールは、ユーザーに直接割り当てることはできませんが、IT ロールとビジネスロールに割り当てることができます。

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	特定のユーザーが特定の時点で、適切なリソースに対する適切な権限を持つことを確認するプロセス。アテステーション作業項目を参照して応答する権限を持つ Identity Manager ユーザーは、「アテスター」と呼ばれます。Identity Manager の規則により、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拒否できるかが決まります。
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合。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。
アテスト	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。
アプリケーション (ロール)	Identity Manager の 4 つのロールタイプのうちの 1 つ。「アプリケーション」ロールタイプは、リソース、リソースグループ、リソースの特定のアプリケーションの集まりで、ユーザーが自分のジョブを実行するために必要なものです。アプリケーションロールは、ユーザーに直接割り当てることはできませんが、IT ロールとビジネスロールに割り当てることができます。
エスカレーションタイムアウト	作業項目リクエストに対して指定される期間。割り当てられた作業項目の所有者はこの期間内に応答する必要があります。応答しない場合、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。
エンタイトルメント	「ユーザーエンタイトルメント」を参照してください。
サービスプロバイダユーザー	エクストラネットユーザー、または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サービスプロバイダの顧客。
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。
ディレクトリジャンクション	階層的に関連付けられた組織のセットで、ディレクトリリソースの階層型コンテナの実際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。
ビジネスロール	Identity Manager の 4 つのロールタイプのうちの 1 つ。「ビジネスロール」は、組織で類似したタスクを実行するユーザーに必要なアクセス権限を、グループに編成するために使用されます。「ビジネスロール」ロールタイプは、アセットロール、アプリケーションロール、および IT ロールを 1 つ以上組み合わせて構成されます。「ビジネスロール」は、ユーザーに直接割り当てることが意図されています。

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。 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	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、または Identity Manager によって管理されるリモートリソースのアカウントの、いずれかを指すことができます。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。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	管理機能を持たないユーザーは、Identity Manager のユーザーインタフェースを使用して、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。「エンドユーザーインタフェース」とも呼ばれます。
ユーザーエンタイトルメント	Identity Manager で、アクセスを制限するリソースまたはシステムのユーザーに許可された監査可能なアクセス特権。
リソース	Identity Manager では、リソースはアカウントが作成されたリモートのリソースやシステムへの接続方法に関する情報を格納しています。Identity Manager がアクセスを提供するリモートリソースには、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などがあります。
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	管理された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示す 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の作成、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	ロールは Identity Manager オブジェクトであり、リソースのアクセス権限をグループ分けし、ユーザーに効率的に割り当てることができるようにします。ロールは、ビジネスロール、IT ロール、アプリケーションロール、およびアセットロールの 4 つのロールタイプにまとめられています。「IT ロール」、「アプリケーション」、「アセット」は、リソースエンタイトルメントをグループに編成します。これら 3 つのグループは、その後、ユーザーがジョブを実行するために必要なリソースにアクセスできるように、「ビジネスロール」に割り当てられます。
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参加者から別の参加者に渡されます。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。
委任	指定した期間に今後の作業項目を 1 人以上のほかのユーザーに一時的に割り当てるプロセス。
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」を参照してください。
管理者	Identity Manager を設定したり、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する役割を持つユーザー。
管理者インタフェース	管理者が Identity Manager の設定と管理に使用するユーザーインタフェース。
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それぞれ対応する、一意の機能セット。
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。
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機構を提供します。
作業項目	Identity Manager のワークフロー、フォーム、または手順によって生成された操作リクエスト。承認、変更の承認、アテステーション、および是正という 4 種類の作業項目があります。
承認	ロール、リソース、または組織に対するユーザーのアクセスリクエストを許可または拒否するプロセス。承認作業項目を参照して応答する権限を持つ Identity Manager 管理者は、「承認者」と呼ばれます。
承認者	アクセスリクエストを承認または拒否する管理機能を持つユーザー。

是正	Identity Manager の監機能によって検出されたコンプライアンス違反を修正するプロセス。Identity Manager は、企業の内部と外部のポリシーと規制のコンプライアンスを確保するため、企業全体のデータを監査します。ポリシー違反を表示して対応する権限を持つ管理者は、「是正者」と呼ばれます。
是正者	監査ポリシーの是正者として指定された Identity Manager ユーザー。 Identity Manager は是正が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、主に 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。
調整	Identity Manager のリソースアカウントを、リソース自体に置かれているアカウントと定期的に比較する Identity Manager の機能。調整により、アカウントデータが関連付けられ、違いが強調表示されます。
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。

索引

A

Access Review Detail Report Administrator 機能，595-619
Account Administrator 機能，595-619
Active Sync アダプタ
　パフォーマンスのチューニング，266-268
　ホストの指定，267
　ポーリング間隔の変更，266
　ログ，268
　ログの設定，262-265
　開始，267
　概要，262-268
　設定，262-265
　停止，267
　編集，265-266
Admin Report Administrator 機能，595-619
Admin Role Administrator 機能，595-619
Assign User Capabilities 機能，595-619
Audit Policy Administrator 機能，595-619
Audit Report Administrator 機能，595-619
auditconfig.xml ファイル，344-353
Auditor Remediator 機能，595-619

B

BPE.，「Identity Manager IDE」を参照
Bulk 機能
　Bulk Account Administrator，595-619
　Bulk Change Account Administrator，595-619
　Bulk Change User Account Administrator，595-619
　Bulk Create User，595-619
Bulk 機能 (続き)
　Bulk Delete User，595-619
　Bulk Deprovision User，595-619
　Bulk Disable User，595-619
　Bulk Enable User，595-619
　Bulk Unassign User，595-619
　Bulk Unlink User，595-619
　Bulk Update User，595-619
　Bulk User Account Administrator，595-619
Business Process Editor (BPE)，45

C

Capability Administrator 機能，595-619
Change 機能
　Change Account Administrator，595-619
　Change Active Sync Resource Administrator，595-619
　Change Password Administrator，595-619
　Change Resource Password Administrator，595-619
　Change User Account Administrator，595-619
`com.waveset.object.Type` クラス，350-351
`com.waveset.security.Right` オブジェクト，351-352
`com.waveset.session.WorkflowServices` アプリケーション，338-344
com.waveset.session.WorkflowServices アプリケーション，339
Configure Audit 機能，595-619
Control Active Sync Resource Administrator 機能，595-619

convertDateToString，331, 332
Correlate via X509 Certificate subjectDN，416-417
Create User 機能，595-619
Create コマンド，81-82
CreateOrUpdate コマンド，81-82
createUser，298-300
CSV 形式，80-83, 247-250
　抽出，246-247

D

DB2 監査スキーマ，575-577
Delete User 機能，595-619
Delete コマンド，80-81
DeleteAndUnlink コマンド，80-81
deleteUser，298-300
Deprovision User 機能，595-619
Disable User 機能，595-619
Disable コマンド，80-81

E

Enable User 機能，595-619
Enable コマンド，80-81
enabledEvents 属性，350-351
extendedActions，351-352
extendedActions，344-353
extendedObjects 属性，350-351
extendedResults，352
extendedResults，344-353
extendedTypes，350-351
extendedTypes，344-353

F

filterConfiguration，344-350
filterConfiguration，344-353
FormUtil メソッド，331, 332

I

Identity Manager IDE.，「Identity Manager インタフェース」を参照
Identity Manager の登録，112-116
Identity Manager の用語，627-631
Identity Manager アカウントの削除ボタン，304-305
Identity Manager ユーザータイプ，26
Identity Manager 外部での変更イベントグループ，346
Identity Manager 作業項目，229-234
Identity Manager
　アカウントインデックス，258-259
　インタフェース
　　Identity Manager IDE，45
　　ユーザー，38-40
　オブジェクト，27-34, 427-429
　データエクスポータ，501-521
　データベース，353-356
　ヘルプとガイダンス，41-42
　ポリシー，99-104
　ユーザーアカウント，27-28
　　削除，304-305
　リソース，29-30, 158-172
　リソースグループ，29-30, 168-169
　ロール，28-29, 119-158
　概要，23-26
　管理について，199-200
　管理者ロール，31
　機能，31, 214-217
　製品登録，112-116
　組織，30, 207
　目的，24
IDM Schema Configuration
　機能，595-619
　設定オブジェクト，84-86
IDMXUser，539-540
ID、ユーザーアカウント，52
Import/Export Administrator 機能，595-619
Import User 機能，595-619

J

JConsole, JMX クライアントとして監査イベントの表示に使用，362

JMS の設定、PasswordSync，376-384
JMS リスナーアダプタ、PasswordSync での設定，386-390
JMX 管理 Beans，519-520
JMX，361-362
　監査ログ，357-365

L

LDAP
　サーバー，211-214
　リソースのクエリー，309
　リソースへのクエリー，316-317
lh コマンド
　syslog，570-571
　クラス，567-570
　コマンドの引数，567-570
　使用法，567-570
Login Administrator 機能，595-619

M

ManageResource ワークフロー，159
MBeans，519-520
Microsoft .NET 1.1 のインストール，373-374
Microsoft .NET 1.1，373-374
MySQL 監査スキーマ，577-578

O

Oracle 監査スキーマ，573-575
Organization Administrator 機能，595-619

P

Password Administrator 機能，595-619
PasswordSync のアンインストール，401
PasswordSync のインストール
　手順，375-386
　前提条件，373-374
PasswordSync のデバッグ，401
PasswordSync の配備，386-391
PasswordSync
　JMS の設定，376-384
　JMS リスナーアダプタ、設定，386-390
　よくある質問，402-403
　アンインストール，401
　インストール，375-386
　インストールの前提条件，373-374
　サーバー設定，376-384
　デバッグ，401
　プロキシサーバーの設定，376-384
　ユーザーパスワード同期ワークフロー，390-391
　以前のバージョンのアンインストール，374
　概要，369-373
　設定，375-376, 376-384
　通知の設定，391
　電子メールの設定，376-384
　配備，386-391
Policy Administrator 機能，595-619
publishers 属性，352-353

R

Reconcile Administrator 機能，595-619
Reconcile Report Administrator 機能，595-619
Reconcile Request Administrator 機能，595-619
Remedy Integration Administrator 機能，595-619
Remedy との統合，110-111
Rename User 機能，595-619
Report Administrator 機能，595-619
Reset Password Administrator 機能，595-619
Reset Resource Password Administrator 機能，595-619
Resource Administrator 機能，595-619
Resource Group Administrator 機能，595-619
Resource Object Administrator 機能，595-619
Resource Password Administrator 機能，595-619
Resource Report Administrator 機能，595-619
Risk Analysis Administrator 機能，595-619
Role Administrator 機能，595-619
Role Report Administrator 機能，595-619
Run AuditLog Report 機能，595-619
Run 機能
　Run Admin Report，595-619

Run 機能 *(続き)*
Run Audit Report，595-619
Run Reconcile Report，595-619
Run Resource Report，595-619
Run Risk Analysis，595-619
Run Role Report，595-619
Run Task Report，595-619
Run User Report，595-619

S

Security Administrator 機能，595-619
SSL 接続、テスト，417
SSL, PasswordSync の設定，374
Sybase 監査スキーマ，578-580
`syslog` コマンド，570-571

T

Task Report Administrator 機能，595-619

U

Unassign User 機能，595-619
Unassign コマンド，80-81
Unlink User 機能，595-619
Unlink コマンド，80-81
Unlock User 機能，595-619
Update User 機能，595-619
Update コマンド，81-82
updateUser，298-300
User Account Administrator 機能，595-619
`user.global.email` 属性，322-325
User Report Administrator 機能，595-619
`user.waveset.accountId` 属性，322-325
`user.waveset.organization` 属性，322-325
`user.waveset.resources` 属性，322-325
`user.waveset.roles` 属性，322-325

V

View User 機能，595-619

W

`waveset.accountId` 属性，331
Waveset Administrator 機能，595-619
`waveset.log` テーブル，353-355
`waveset.logattr` テーブル，355-356
Windows Active Directory リソース，211-214
`WSUser` オブジェクト，350-351

X

X509 証明書ベースの認証，414-418
XML ファイル
承認フォーム，323-324, 325
抽出，246-247
読み込み，247-250

「

「アカウント」領域、管理者インタフェース，49-56
「サンライズとサンセット」タブ, 設定，328-334
「タイムアウトのアクション」ボタン，318-319
「タスクの実行」ボタン，322
「データ変換」タブ, 設定，334-335
「プロビジョニング」タブ, 設定，327
「ユーザーメンバー規則」オプションボックス，208-211
「リソース」領域，159
「監査」タブ
設定，326-327
説明，326-327
「管理するリソース」ページ，160
「承認」タブ
設定，311-325
説明，311-325
「承認のエスカレーション」ボタン，320-322
「選択している属性の削除」ボタン，322-325, 325, 326-327

「属性の追加」ボタン，322-325, 326-327

ア
アイデンティティーシステムパラメータ、リソース，161-165
アイデンティティーシステム属性名，167-168
アイデンティティーテンプレート，161-165
アイデンティティー監査
　タスク，437
　説明，433-434
アカウント ID の取得，307-311
アカウント ID
　承認，314
　承認のエスカレーション，320-322
　追加の承認，314-315
　通知受信者，307-311
アカウントインデックス
　レポート，278-280
　検査，259
　検索，258-259
　操作，258-259
アカウントインデックスレポート, 必須機能，595-619
アカウント管理イベントグループ，346
アカウント属性，161-165, 167-168
アクション, 拡張，351-352
アクションスクリプト、設定，176-178
アクセススキャン
　作成，482-488
　変更，491
アクセスレビュー，477-497
アクセスレビューの管理，488-492
アテステーション，479-480
　エンタイトルメントの承認，493
　委任，480
　管理，492-496
アプリケーション、アクセスの無効化，409

イ
イベント、監査の作成，338-344
イベントグループ
　Identity Manager 外部での変更，346
　アカウント管理，346
　コンプライアンス管理，346-347
　セキュリティー管理，349
　タスク管理，349-350
　リソース管理，348
　ロール管理，348-349
　ログイン/ログオフ，347-348
　属性，344-350

ウ
ウェアハウスの設定，507-508

エ
エスカレーションされた承認
　タイムアウト，314-315, 315-316, 316, 317-318
　タイムアウトの設定，318-319

オ
オブジェクト、Identity Manager，27-34
　セキュリティー保護，427-429
オンラインヘルプ，41-42

カ
カスタムリソース，160

ガ
ガイダンス、Identity Manager，41-42, 42

キ
キー
　ゲートウェイ，421-423

キー (続き)
サーバー暗号化，419-420

ク
クエリー
LDAP リソース，309, 316-317
リソース属性，309, 316
承認者のアカウント ID の取得，314, 316-317, 320-322
属性の比較，309, 316
通知受信者アカウント ID の取得，307-311

グ
グラフ形式のレポート，285-290
グローバルリソースポリシー，169-170

ゲ
ゲートウェイキー，421-423

コ
コンプライアンス管理イベントグループ，346-347
コンマ区切り (CSV) 形式，「CSV 形式」を参照

サ
サーバープロバイダ, トランザクション持続ストア，539-540
サーバー暗号化
キー，419-420
管理，418-423, 423-427
サーバー暗号化の管理，423-427
サービスプロバイダ
コールアウト設定，534
デフォルトの検索設定，534-536
トランザクションのデフォルトの設定，536-539
サービスプロバイダ (続き)
トランザクションの監視，542-545
トランザクションデータベースの設定，530-531
トランザクション処理の詳細設定，540-542
ユーザーアカウントの検索，554-558
ユーザーアカウントの作成，551-554
ユーザーアカウントの削除，557-558
委任管理，545-550
監査グループの設定，565
管理者ロールの作成，547-549
管理者ロール委任の有効化，546-547
初期設定，525-534
追跡イベント設定，531-532
同期の設定，562-563
サービスプロバイダエンドユーザーインタフェース，559-561
サービスプロバイダユーザーの管理，550-561
サービスプロバイダユーザーの検索，554-558
サービスプロバイダユーザータイプ，26
サンセット
プロビジョニング解除，333-334
設定，328-334
サンプルユーザーメンバー規則，208-211
サンライズ
新しいユーザーのプロビジョニング，328-334
設定，328-334
サンライズとサンセットタブ, 説明，300-302

シ
システムログ
syslog lh コマンド，570-571
コマンド行でのレコードの表示，570-571
データエクスポータ，521
レポートの定義，281
システム設定オブジェクト, 編集，116-117
システム設定ページ，43-44

ス
スキーママップ，167-168

セ
セキュリティ, パススルー認証，407-412
セキュリティー
　パスワード管理，406-407
　ベストプラクティス，429-430
　ユーザーアカウント，53-54
　機能，405-406
セキュリティー管理イベントグループ，349
セッションの制限、設定，409

タ
タイプ、拡張，350-351
タイムアウト
　エスカレーションされた承認，314-315, 315-316, 316, 317-318
　設定，318-319, 320-322, 322
タイムアウト値、設定，409
タスク
　アイデンティティー監査，437
　サンライズ/サンセット，300-302
　データエクスポータ，511-513
　バックグラウンドでの実行，300-302
　再試行，300-302
　保留，300-302
タスクの再試行，300-302
タスクの作成、保留，300-302
タスクの設定タブ，300-302
タスクの保留，300-302
タスクテンプレート
　プロセスタイプのマップ，297-302
　ユーザー更新テンプレート，297-302
　ユーザー作成テンプレート，297-302
　ユーザー削除テンプレート，297-302
　設定，300-302
　編集，300-302
　有効化，297-302
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，300-302, 303-304
　ユーザー作成テンプレート，300-302, 303-304
　ユーザー削除テンプレート，300-302, 304-305
タスクベースの機能，214
タスク管理イベントグループ，349-350
タスク名
　属性参照，303-304
　定義，300-302, 303-304
タブ
　サンライズとサンセット，300-302
　タスクの設定，300-302
　データ変換，300-302
　プロビジョニング，300-302
　一般，300-302
　承認，300-302
　通知，300-302

ダ
ダッシュボード、レポートのグループ化，290-293

テ
テンプレート、電子メール，305-311, 307-308

デ
データの同期, 検出，246-250
データエクスポータ，521
　ウェアハウスの設定，507-508
　ウェアハウスタスク，511-513
　システムログ，521
　スケジュール，508-510
　テスト，514
　データタイプ，508-510
　モデル，508-510
　概要，501-502
　監査ログ，521
　監視，519-520
　計画，502-503
　設定，503-513
　設定オブジェクト，513
　読み取り接続と書き込み接続，505-507
データストア，173-174
データタイプ，508-510
データベース
　DB2，575-577

データベース (続き)
MySQL，577-578
Oracle，573-575
Sybase，578-580
キーマッピング，580-586
スキーマ，353-356
データエクスポータの接続，505-507
データ同期
Active Sync アダプタ，262-268
ツール，245-246
調整，251-262
データ変換
プロビジョニング前，300-302
プロビジョニング中，334-335
データ変換タブ, 説明，300-302
ディレクトリジャンクション
概要，211-214
設定，212-213
ディレクトリリソース，211-214
デフォルト
タスク名，303-304
プロセスタイプ，298-300
承認の有効化，313
承認フォームの属性，322-325
属性表示名，324-325

ト
トラブルシューティング
外部リソース，198
監査ポリシー，459
トラブルシューティングページ，43-44
トリプル DES 暗号化，419-420, 421-423

ド
ドキュメント, 概要，19-20

バ
バックグラウンド、タスクの実行，300-302
バックグラウンドでのタスクの実行，300-302

パ
パススルー認証，407-412
パスワード
ログインアプリケーション，407-408
管理者の認証，204-206
管理者の変更，203-204
パスワードポリシー
禁止属性，89
禁止単語，89
辞書ポリシー，88
実装，90
設定，86-90
長さ規則，87
文字タイプ規則，87-88
履歴，89
パスワード管理，406-407
パスワード文字列の品質ポリシー，100-101

ビ
ビューハンドラの監査，338

フ
ファイルへ抽出，245-246, 246-247
フィールドレベルヘルプ，42
フォーム
タスク承認，311-325
現在設定されている，317-318, 334-335
承認の設定，322-325
属性の追加，324-325
通知，308-309
編集，45
フォームおよびプロセスマッピングの設定
ページ，298-300
フォレンジッククエリー
概要，515-519
作成，515-518
読み込み，519
保存，518-519

プ

プロキシサーバーの設定、PasswordSync，376-384
プロセスタイプ
  createUser，298-300
  updateUser，298-300
  デフォルト，298-300
  マッピング，297-302
  削除，298-300
  選択，298-300
プロセスダイアグラム, エンドユーザーインタフェースでの有効化，111-112
プロセスマッピング
  一覧表示，298-300
  検証，298-300
  必須，298-300
  編集，298-300
  有効化，298-300
プロセスマッピングの一覧表示，298-300
プロセスマッピングの検証，298-300
プロセスマッピングの編集ページ，298-300
プロセス図, 管理者インタフェースでの有効化，56
プロビジョニング
  サンライズ，328-334
  データの変換，300-302
  データ変換，334-335
  バックグラウンド，327
  外部リソース，193-197
  再試行リンク，327
  時間，330
  日付，330
プロビジョニングタブ, 説明，300-302
プロビジョニングツールの監査，338
プロビジョニングツール通知
  Remedy，186-190
  電子メール，183-186
プロビジョニング解除
  サンセットの設定，333-334
  ユーザーアカウント，300-302, 304-305
  ユーザーアカウントからのリソースの削除，67-70

ヘ

ヘルプ、オンライン，41-42

ペ

ページ
  タスクテンプレート「Create User Template」の編集，300-302, 303-304
  タスクテンプレート「Delete User Template」の編集，300-302, 304-305
  タスクテンプレート「Update User Template」の編集，300-302, 303-304
  フォームおよびプロセスマッピングの設定，298-300
  プロセスマッピングの編集，298-300

ボ

ボタン
  Identity Managerアカウントの削除，304-305
  タイムアウトのアクション，318-319
  タスクの実行，322
  マッピングの編集，298-300
  承認のエスカレーション，320-322
  選択している属性の削除，322-325, 325, 326-327
  属性の追加，322-325, 326-327
  有効化，298-300

ポ

ポリシー
  Identity Managerアカウント，100-101
  アカウントID，100-101
  グローバルリソースポリシー，169-170
  リソースパスワード，86-90, 100-101
  概要，99-104
  監査，438-440
  辞書，102-104
  調整，251
ポリシーの編集ページ，454-455
ポリシー違反
  アクセススキャン中，482-488
  受け入れ，474-475
  是正，475-476
  是正リクエストの転送，476

マ

マッピング
- プロセス，298-300
- プロセスタイプ，297-302
- 検証，298-300

マッピングの編集ボタン，298-300

メ

メソッド
- `FormUtil`，331, 332

ユ

ユーザーアカウント
- ID，52
- セキュリティー，53-54
- データ，52-56
- データ変換，334-335
- パスワード
  - リセット，73-74
- プロビジョニング解除，67-70, 300-302, 304-305
- ロック解除，77-78
- 移動，63
- 一括アクション，78-86
- 概要，27-28
- 割り当てられた監査ポリシー，55-56
- 検索，50, 60-61
- 更新，64-66
- 削除，300-302, 304-305
- 自己検索，94-95
- 状態インジケータ，50-52
- 属性，54
- 認証，90-93
- 表示，61-64
- 名前変更，63-64
- 有効化，76-77

ユーザーアカウントのロック解除，77-78
ユーザーアカウントの移動，63
ユーザーアカウントの検索，60-61
ユーザーアカウントの更新，64-66
ユーザーアカウントの名前変更，63-64
ユーザーアカウントの有効化，76-77
ユーザーアカウントパスワードのリセット，73-74
ユーザーアクセス、定義，25-26
ユーザーインタフェース、Identity Manager，38-40
ユーザーエンタイトルメントレコード，496-497
ユーザータイプ，26
ユーザーテンプレート
- 選択，300-302
- 編集，303-304, 304-305

ユーザーパスワード同期ワークフロー，390-391
ユーザーフォーム，201-202
- 管理者ロールへの割り当て，227

ユーザー管理者ロール，219-220
ユーザー更新テンプレート
- プロセスのマッピング，298-300
- 設定，302-305
- 説明，297-302

ユーザー作成テンプレート
- プロセスのマッピング，298-300
- 設定，302-305
- 説明，297-302

ユーザー削除テンプレート
- プロセスのマッピング，298-300
- 説明，297-302

リ

リスク分析，294-295
リソース
- Identity Manager，160
- アイデンティティーシステムパラメータ，161-165
- アイデンティティーテンプレート，161-165
- アカウント属性，161-165, 167-168, 309
- アダプタ，161-165
- カスタム，160
- グローバルリソースポリシー，169-170
- タイムアウト値の設定，170
- トラブルシューティング，198
- バルク操作，170-172
- パラメータ，161-165
- プロビジョニング，193-197
- 外部，172-198
- 概要，158-172
- 管理，165-167

リソース *(続き)*
作成，161-165, 190-193
問い合わせる，314, 316-317, 320-322
リソースの承認，313
リソースの調整，245-246
リソースアカウント
Identity Manager アカウントの削除，304-305
プロビジョニング解除，304-305
リンク解除，304-305
割り当て解除，304-305
リソースアカウントのリンク解除，304-305
リソースアカウントの割り当て解除，304-305
リソースウィザード，161-165
リソースグループ，29-30, 168-169
リソース管理イベントグループ，348
リソース属性，316
リンク解除, 外部リソース，197-198

レ

レポート
グラフの定義，286-287
サービスレベル契約，283-285
システムログ，281
スケジュール，274
ダッシュボードの操作，290-293
データのダウンロード，274
リアルタイム，277, 278
リスク分析，294-295
ワークフローレポート，283-285, 338, 341-344
概要，278-280
監査のタイプ，463-468
監査ログ，276-277
使用状況，281-282, 283-285
実行，274
操作，270-276, 285-290
単一ユーザー用の監査ログレポート，277
定義，272-273
名前の変更，273

ロ

ロール
Identity Manager ロールとリソースロールの同期，158
およびリソース，127-128, 142-143, 143-144
アクティブ化および非アクティブ化の日付，145-146
ユーザーに割り当てられたロールの削除，153
ユーザーの更新，146
ユーザーへの割り当て，144-145
ロールからのリソースの削除，143-144
ロールからのロールの削除，140-141
ロールに割り当てられたユーザーの検索，150-151, 152
ロールの割り当て規則，132-133
ロールの除外，130-131
ロールへのリソースの割り当て，142-143
ロールへのロールの割り当て，139-140
ロールタイプ，121
ロールユーザーの更新タスク，150-151
ロール割り当てのスキャン，146
ロール所有者，132-133
延期タスクスキャナ，146
概要，28-29, 119-158
割り当て，130-131
割り当てられているリソース属性値の編集，128-130
管理者，31
検索，136-137
更新，147-152
作成，124-135
削除，142
承認，132-133, 313
設定，154-157
通知，132-133, 134
表示，137
編集，138-139
有効化および無効化，141-142
ロール管理イベントグループ，348-349
ログイン/ログオフ監査イベントグループ，347-348, 348
ログイン
アプリケーション，407-408
編集，408-409

ログイン (続き)
モジュール
編集，410-412
モジュールグループ，407-408
編集，410
制約規則，408
相関規則，416-417
ログインアプリケーション、アクセスの無効化，409

ワ

ワークフロー、修正，45
ワークフローの監査，338
ワークフロー監査，338-344

暗

暗号化
暗号化キー，419-420
概要，418-423
保護されるデータ，418-419
暗号化キー、サーバー，419-420

以

以前のバージョンの PasswordSync のアンインストール，374

委

委任された管理，200

一

一括アクション
アクションリスト，80-83
タイプ，78-86
ユーザーアカウント，78-86
確認規則，84-86, 86
一括アクション (続き)
相関規則，84-86
表示属性，83-84
一括リソースアクション，170-172
一般タブ, 説明，300-302

仮

仮想組織
概要，211-214
更新，213
削除，213-214

外

外部リソース，172-198
アクションスクリプト，176-178
データストア，173-174
トラブルシューティング，198
プロビジョニング，193-197
プロビジョニングツール通知，183-190
プロビジョニング要求への応答，194-197
割り当て，193-194
割り当て解除またはリンク解除，197-198
作成，190-193
設定，173-190
定義，172

確

確認規則，84-86, 86

割

割り当て解除, 外部リソース，197-198

監

監査
extendedActions，351-352

監査 (続き)
extendedResults，352
extendedTypes，350-351
filterConfiguration，344-350
データストレージ
waveset.logattr，355-356
waveset.log，353-355
ビューハンドラ，338
プロビジョニングツール，338
ワークフロー，338
概要，337-338
設定，326-327, 344-353
監査、タスクテンプレートの設定，300-302
監査イベント、作成，339
監査スキャン，461-468
監査ポリシー
ワークフローの割り当て，456-457
規則のデバッグ，459
規則の作成，447
作成，442-453
是正ワークフローのインポート，444
是正者の割り当て，455-456
説明，438-440
必須機能，595-619
編集，454-458
監査ポリシー規則のデバッグ，459
監査ポリシー規則ウィザード，447
監査レポート
Auditor Report Administrator 機能，595-619
作成，466-467
監査ログ，521
データの切り捨て，356
データベースマッピング，580-586
列の長さ制限の設定，353-356, 356-357
監査ログのマッピング，580-586
監査設定，344-353
監査設定グループ，109-110

管

管理、Identity Manager について，199-200
管理、委任，200
管理する組織
ユーザーの割り当て，201-202
管理する組織 (続き)
範囲，221-226
管理する組織の範囲，221-226
管理者
パスワード，203-204
ビューのフィルタリング，202-203
作成，201-202
秘密の質問，206
名前の表示のカスタマイズ，206
管理者インタフェース，35-36
「アカウント」領域，49-56
管理者リスト
承認者の選択，314, 317-318, 320-322
通知受信者の選択，307-311
管理者ロール
ユーザーフォームの割り当て，227
ユーザーロール，219-220
概要，31, 217-227
作成と編集，220

機

機能
カテゴリ，214
ユーザーの割り当て，201-202
概要，214-217
割り当て，217
作成，215-216
実用上の機能の階層，619-625
編集，216
名前の変更，216-217

規

規則
アクセスレビュー，481
エスカレーション承認者のアカウント ID を取得するための評価，320-322
サンプルユーザーメンバー，208-211
データ変換，334-335
プロビジョニング，329-330, 332
プロビジョニング解除，333-334

規則 (続き)
管理者アカウント ID を取得するための評価，307-311
現在設定されている，334-335
修正，45
職務分掌，443
追加の承認者のアカウント ID を取得するための評価，314, 315-316
規則に基づく割り当て，208-211

共
共通リソース、認証の設定，413

結
結果, 拡張，352

検
検索
サービスプロバイダトランザクション，542-545
ユーザーアカウント，50
検出
ファイルから読み込み，247-250
ファイルへ抽出，246-247
リソースから読み込み，250
概要，246-250

再
再試行リンク、設定，327

作
作業項目
タイプ，229-230
委任，231-234
管理，229-234
作業項目 (続き)
保留中，39-40
履歴の表示，230
作業項目の委任，231-234
作成
アクセススキャン，482-488
フォレンジッククエリー，515-518
外部リソース，190-193
監査ポリシー，442-453
監査ポリシー規則，447

削
削除
ユーザーアカウント，300-302, 304-305
ユーザーアカウントのリソース，67-70
削除タスクの保留，300-302

指
指定
アカウントデータの属性，300-302
ユーザー通知，306
通知受信者，307, 308, 309, 310-311

自
自己検索，94-95

辞
辞書ポリシー
概要，102-104
実装，104
設定，103
選択，88

実
実用上の機能，214

署
署名付き承認、設定，237-241

承
承認
　「承認がタイムアウトになるまでの時間」設定，314-315
　エスカレーションされた，318-319
　タイムアウト，315-316, 316, 317-318
　タイムアウトの設定，318-319
　フォーム，322-325
　署名付きの設定，237-241
　設定，311-325
　無効化，300-302, 313
　有効化，300-302, 313
承認の無効化，300-302, 313
承認カテゴリ，234-244
承認タブ
　概要，300-302
　説明，300-302
承認者
　リソース，313
　ロール，313
　設定，235-236, 311-325
　組織，313
　追加，300-302, 311-325
　通知の設定，305-311

証
証明書ベースの認証，414-418

状
状態インジケータ、ユーザーアカウント，50-52

是
是正
　リクエストの転送，476
是正 (続き)
　リクエストの表示，472
　ワークフローの割り当て，456-457
　違反の受け入れ，474-475
　違反の是正，475-476
　説明，468-471
　必須機能，595-619
　標準是正ワークフロー，469

制
制約規則、ログイン，408

製
製品登録，112-116

設
設定
　PasswordSync，375-376, 376-384
　「サンライズとサンセット」タブ，328-334
　「プロビジョニング」タブ，327
　「監査」タブ，326-327
　ウェアハウス，507-508
　ウェアハウスタスク，511-513
　サービスプロバイダ機能，525-534
　タイムアウト，318-319, 320-322, 322
　タスクテンプレート，300-302
　タスクテンプレートの監査，300-302
　データエクスポータ，503-513
　フォレンジッククエリー，515-519
　ユーザー更新テンプレート，302-305
　ユーザー作成テンプレート，302-305
　監査，326-327
　監査グループ，109-110
　署名付き承認，237-241
　承認，311-325
　承認フォーム，322-325
　追加の承認者，300-302
　通知，305-311
　電子メール通知，300-302

設定 (続き)
同期，262-265
設定、監査，344-353

組

組織
ユーザー割り当て，208-211
仮想，211-214
概要，30, 207
割り当ての管理，211
作成，207
組織の承認，313

相

相関規則，84-86

属

属性
user.global.email，322-325
user.waveset.accountId，322-325
user.waveset.organization，322-325
user.waveset.resources，322-325
user.waveset.roles，322-325
waveset.accountId，331
アカウントデータからの指定，300-302
エスカレーション承認者のアカウント ID の取得，320-322
クエリーの作成，309
タスク承認に対する指定，311-325
タスク名での指定，303-304
デフォルト，322-325
デフォルトの表示名，324-325
ユーザーアカウント，54
管理者アカウント ID の取得，307-311
承認フォームからの削除，322-325
承認フォームへの追加，322-325
値の編集，322-325
追加の承認者のアカウント ID の取得，314

調

調整
ステータスの表示，257-258
ポリシー，251
ポリシー、編集，252-256
開始，256-257
概要，251-262
調整レポート，595-619

通

通知
PasswordSync での設定，391
ユーザーアカウントデータの変換，334-335
設定，305-311
通知タブ
設定，305-311
説明，300-302
通知受信者
アカウント ID の取得，307-311
クエリーによる指定，309
ユーザーの指定，306
管理者リストからの指定，310-311
規則による指定，308
属性による指定，307

定

定期的アクセスレビュー
アクセススキャン，482-488
アテステーション，479-480
エンタイトルメント，493
スケジュール，489-490
レポート，496-497
ワークフロープロセス，478
起動，489
計画，480-482
終了，491-492
進行状況の管理，490-491
説明，477-497

電
電子メールの設定、PasswordSync，376-384
電子メールテンプレート
　HTML とリンク，108
　カスタマイズ，106-108
　概要，104-109, 305-311
　変数，108-109
電子メール通知、設定，300-302, 305-311

同
同期
　サービスプロバイダ機能，562-565
　設定，262-265
　無効化，265-266
同期ポリシー，262-265

読
読み込み
　ファイルから，245-246, 247-250
　リソースから，245-246, 250

日
日付形式文字列，331, 332, 333-334

認
認可タイプ，427-429
認証
　X509 証明書ベース，414-418
　ユーザー，90-93
　共通リソースの設定，413
　質問，206

必
必須プロセスマッピングセクション，298-300

表
表示
　ユーザーアカウント，61-64
　レポートのタイプ，276-285
　作業項目履歴，230
　保留中のアテステーション，493
　保留中の作業項目，229-230

編
編集
　タスクテンプレート，300-302
　タスク名，303-304
　プロセスマッピング，298-300
　属性値，322-325

方
方法
　サンライズ/サンセットの決定，328-334
　プロビジョニング解除の決定，333-334
　承認タイムアウトの決定，314-315
　承認者の決定，314

有
有効化
　タスクテンプレート，298-300
　プロセスマッピング，298-300
　承認，300-302, 313
　承認のタイムアウト，318-319
有効化ボタン，298-300

用
用語集，627-631