Sun Java™ System

Identity Manager 6.0 2005Q4M3
管理ガイド

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

Part No: 819-5518

目次

はじめに

Identity Manager の概要

全体像 1–1
- Identity Manager システムの目的 1–1
- ユーザーアクセスの定義 1–2
- 管理の委任 1–3

Identity Manager オブジェクト 1–4
- ユーザーアカウント 1–4
- ロール 1–4
- リソースとリソースグループ 1–5
- 組織 1–7
- 機能 1–7
- 管理者ロール 1–7
- オブジェクトの関係 1–8

Identity Manager の用語 1–10

Identity Manager 入門

Identity Manager インタフェース 2–1
- Identity Manager 管理者インタフェース 2–1
- Identity Manager ユーザーインタフェース 2–2
- Identity Manager Business Process Editor 2–3

ヘルプとガイダンス 2–4
- Identity Manager ヘルプ 2–4
  - 情報の検索 2–4
  - 検索の動作 2–5
  - 高度なクエリー構文 2–5
- Identity Manager ガイダンス 2–7
- Identity Manager タスク 2–8

以降の操作について 2–11

ユーザーとアカウントの管理

ユーザーアカウントデータについて 3–1
- ID 3–1
- 割り当て 3–2
- セキュリティー 3–2
- 属性 3–4

「アカウント」エリア 3–5
- 「アカウント」エリアの操作リスト 3–5
- 「アカウント」エリアでの検索 3–6

ユーザーアカウントステータス 3–6
ユーザーアカウントの操作 3–7
ユーザー 3–7
表示 3–7
作成 (「新規作成アクション」リスト、「新規ユーザー」選択) 3–7
複数のユーザーアカウント (アイデンティティー) の作成 3–8
編集 3–9
ユーザーの移動 (「ユーザーアクション」) 3–9
名前の変更 (「ユーザーアクション」) 3–10
ユーザーの無効化 (「ユーザーアクション」、「組織アクション」) 3–11
ユーザーの有効化 (「ユーザーアクション」、「組織アクション」) 3–12
ユーザーの更新 (「ユーザーアクション」、「組織アクション」) 3–12
ユーザーのロック解除 (「ユーザーアクション」、「組織アクション」) 3–14
削除 (「ユーザーアクション」、「組織アクション」) 3–15
アカウントの検索 3–17
パスワードポリシーの設定 3–18
ポリシーの作成 3–18
長さ規則 3–19
文字タイプ規則 3–19
文字タイプ規則の最小個数 3–19
辞書ポリシーの選択 3–20
パスワード履歴ポリシー 3–20
使用禁止単語 3–20
使用禁止属性 3–20
パスワードポリシーの実装 3–21
ユーザーアカウントパスワードの操作 3–22
ユーザーアカウントパスワードの変更 3–22
ユーザーアカウントパスワードのリセット 3–23
リセット時のパスワードの期限切れ 3–23
ユーザーの自己検索 3–24
自己検索の有効化 3–24
ユーザー認証 3–25
ユーザー独自の認証質問 3–26
認証後のパスワード変更要求のバイパス 3–26
一括アカウント操作 3–28
一括アカウント操作の起動 3–28
操作リストの使用 3–29
Delete、DeleteAndUnlink、Disable、Enable、Unassign、および Unlink コマンド 3–30
Create、Update、および CreateOrUpdate コマンド 3–30
複数の値を持つフィールド 3–31

フィールド値の特殊文字. 3–32
一括操作の表示属性 3–32
相関規則と確認規則. 3–32
相関規則 3–33
確認規則 3–33

管理

Identity Manager の管理について. 4–1
委任された管理 4–1
Identity Manager 組織について 4–2
組織の作成. 4–2
組織へのユーザーの割り当て 4–3
キーの定義と取り込み 4–4
ユーザーメンバー規則の例. 4–5
管理する組織の割り当て 4–6
ディレクトリジャンクションおよび仮想組織について 4–6
ディレクトリジャンクションのセットアップ. 4–7
仮想組織の更新 4–8
仮想組織の削除 4–8
管理者の作成 4–8
管理者ビューのフィルタ 4–10
管理者パスワードの変更 4–11
管理者のアクションの認証 4–12
認証質問の回答の変更. 4–13
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 . . .4–13
承認. 4–14
承認者のセットアップ. 4–14

設定

ロールについて. 5–1
ロールとは. 5–1
ロールの作成 5–2
割り当てられているリソース属性値の編集 5–2
ロールの編集 5–2
ロールの検索 5–2
ロールのクローン作成. 5–3
ロール名の変更 5–3
ロールとリソースロールの同期 Identity Manager. 5–4
リソースについて. 5–4
リソースとは 5–4
「リソース」エリア 5–4
リソースリストの管理. 5–5
リソースの作成 5–7
リソースの管理 5–12
アカウント属性の操作. 5–12
リソースグループ 5–13

ChangeLog について 5–14
ChangeLog とは 5–14
ChangeLog とセキュリティー 5–14
ChangeLog 機能の要件 5–15
ID 属性の設定 5–15
ID 属性の操作 5–15
アプリケーションの選択 5–15
ID 属性の追加と編集 5–15
ターゲットリソースの追加 5–16
ターゲットリソースの削除 5–17
ID 属性のインポート 5–17
ChangeLog の設定 5–18
ChangeLog ポリシーの概要 5–18
ChangeLog の概要 5–18
ChangeLog 設定変更の保存 5–19
ChangeLog ポリシーの作成と編集 5–19
ChangeLog の作成と編集 5–20
例 5–21
例 : ID 属性の定義 5–21
例 : ChangeLog の設定 5–22
CSV ファイル形式 5–23
列 5–23
行 5–24
テキスト値 5–24
バイナリ値 5–24
複数テキスト値 5–24
複数バイナリ値 5–25
出力形式の例 5–25
ローテーションとシーケンスの設定 5–25
ChangeLog スクリプトの作成 5–26
ポリシーについて 5–27
ポリシーとは 5–27
辞書ポリシー 5–30
辞書ポリシーの設定 5–30
辞書ポリシーの実装 5–31
機能について 5–31
機能のカテゴリ 5–32
機能の操作 5–32
機能の作成 5–32
機能の編集 5–32
機能の保存と名前の変更 5–32
機能の割り当て 5–33
機能の階層 5–33
機能の定義 5–36
管理者ロールについて 5–46
ユーザー管理者ロール 5–47

例. 5–47
管理者ロールの作成および編集. 5–48
管理する組織の範囲の設定 5–49
管理者ロールへのユーザーフォームの割り当て 5–50
機能規則と管理する組織規則 5–51
機能規則 : キーの定義と取り込み. 5–51
管理する組織規則 : キーの定義 5–53
管理する組織規則の例 5–53
電子メールテンプレートについて 5–55
電子メールテンプレートのカスタマイズ 5–56
電子メールテンプレートの HTML とリンク 5–57
電子メール本文の許容変数 5–57
監査グループの設定 5–58
監査設定グループ内のイベントの編集 5–58
監査設定グループへのイベントの追加 5–58
Remedy との統合 5–59
Identity Manager サーバーの設定. 5–59
調整サーバーの設定. 5–59
スケジューラの設定. 5–60
サーバーのデフォルト設定の編集. 5–60
署名付き承認 5–61
署名付き承認の設定. 5–61
サーバー側の設定 5–61
クライアント側の設定 5–63
承認の署名 5–64
その後の承認の署名 5–64
トランザクション署名の表示 5–65

データの同期と読み込み

この章のトピック 6–1
データ同期ツール : 最適なツールの選択 6–1
探索. 6–2
ファイルへ抽出 6–2
ファイルから読み込み. 6–3
CSV ファイル形式について 6–3
リソースから読み込み. 6–5
調整. 6–6
調整ポリシーについて. 6–6
調整ポリシーの編集. 6–7
調整の開始. 6–9
調整のキャンセル 6–9
調整ステータスの表示. 6–10
アカウントインデックスの操作. 6–10
アカウントインデックスの検索 6–10
アカウントインデックスの検査. 6–11
アカウントの操作 6–11

ユーザーの操作 6–11
ActiveSync アダプタ 6–12
アクティブな同期のセットアップ 6–12
同期モード. 6–12
動作設定 6–14
一般の Active Sync 設定 6–16
イベントタイプ 6–18
プロセスの選択 6–19
ターゲットリソース 6–20
ターゲット属性マッピング 6–21
ActiveSync アダプタの編集 6–21
クラスタ環境でのアクティブな同期 6–22
ActiveSync アダプタのパフォーマンスのチューニング 6–22
ポーリング間隔の変更. 6–22
アダプタを実行するホストの指定. 6–22
開始と停止. 6–23
アダプタログ 6–23
アダプタログの削除 6–23

セキュリティー

セキュリティー機能 7–1
パスワード管理. 7–1
パススルー認証 7–2
ログインアプリケーションについて 7–2
ログイン制約規則 7–3
ログインアプリケーションの編集 7–3
Identity Manager セッション制限の設定. 7–4
アプリケーションへのアクセスの無効化 7–4
ログインモジュールグループの編集 7–4
ログインモジュールの編集 7–4
共通リソースの認証の設定. 7–6
X509 証明書認証の設定 7–7
前提条件. 7–7
Identity Manager での X509 証明書認証の設定 7–7
ログイン設定規則の作成とインポート 7–9
SSL 接続のテスト 7–10
問題の診断 7–10
暗号化の使用と管理 7–11
暗号化によって保護されるデータ 7–11
サーバー暗号化キーに関する質問と答え. 7–12
サーバー暗号化キーとは何ですか？. 7–12
サーバー暗号化キーはどこで維持管理されますか？ 7–12
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？. 7–12
サーバー暗号化キーはどのようにして更新しますか？. . . 7–12

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？ 7–13
サーバーキーはどのように保護されますか？ 7–13
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？ 7–14
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？ 7–14
ゲートウェイキーに関する質問と答え 7–14
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？ 7–14
ゲートウェイキーはどのようにしてゲートウェイに配布されますか？ 7–14
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？ 7–15
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？ 7–16
ゲートウェイキーはどのように保護されますか？ 7–16
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？ 7–16
サーバーキーやゲートウェイキーはどのようにして破棄されますか？ 7–16
サーバー暗号化の管理 7–17
セキュリティーの実装 7–19
セットアップ時 7–19
実行時 7–19

レポート

レポートの操作 8–1
レポート 8–1
レポートの作成 8–2
レポートの複製 8–3
電子メールによるレポートの送信 8–3
レポートの実行 8–3
レポートのスケジュール 8–3
レポートデータのダウンロード 8–4
レポート出力のフォントの設定 8–4
レポートのタイプ 8–5
監査ログ 8–5
リアルタイム 8–5
概要レポート 8–6
システムログ 8–8
使用状況レポート 8–8
使用状況レポートのグラフ 8–8

リスク分析 8–9
タスクテンプレートの有効化 9–1

タスクテンプレート

タスクテンプレートの設定 9–4
「一般」タブの設定 9–5
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 9–5
ユーザー削除テンプレートの場合 9–6
「通知」タブの設定 9–8
管理者通知の設定 9–8
ユーザー通知の設定 9–11
「承認」タブの設定 9–12
承認の有効化 9–13
追加の承認者の指定 9–14
承認フォームの設定 9–22
「監査」タブの設定 9–25
「プロビジョニング」タブの設定 9–27
「サンライズとサンセット」タブの設定 9–28
サンライズの設定 9–28
サンセットの設定 9–31
「データ変換」タブの設定 9–32

PasswordSync

PasswordSync の概要 10–1
PasswordSync をインストールする前に 10–1
Microsoft .NET 1.1 のインストール 10–2
PasswordSync の以前のバージョンをアンインストールする . 10–2
PasswordSync のインストール 10–3
PasswordSync の設定 10–4
PasswordSync のデバッグ 10–9
エラーログ 10–9
トレースログ 10–9
レジストリキー 10–10
PasswordSync のアンインストール 10–11
PasswordSync の配備 10–11
JMS リスナーアダプタの設定 10–11
ユーザーパスワード同期ワークフローの実装 10–12
通知の設定 10–13
PasswordSync についてのよくある質問 10–13
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。 10–13

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。. 10–14
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。. 10–14
パスワード変更の結果、com.waveset.exception.ItemNotLocked が発生することがありますが、それはどうしてですか。. 10–14

lh リファレンス

使用法. A–1
クラス. A–1
コマンド A–1
例 A–2
license コマンド A–2
使用法 A–2
オプション A–2
例. A–2
syslog コマンド A–3
使用法 A–3
オプション A–3

オンラインマニュアルの高度な検索

ワイルドカード文字 B–1
クエリー演算子. B–2
優先度の規則 B–2
デフォルト演算子 B–2

索引

はじめに

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

このガイドの構成

このガイドは、次の章で構成されています。

- 第 1 章 : Identity Manager の概要 ー Identity Manager 製品とオブジェクトについての概要を示します。
- 第 2 章 : Identity Manager 入門 ー Identity Manager インターフェースを紹介し、Identity Manager の基本的なタスク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 ー ユーザー管理の概要およびタスクについて説明します。
- 第 4 章 : 管理 ー 委任された管理、および Identity Manager 管理者、組織、仮想組織の操作手順について説明します。
- 第 5 章 : 設定 ー ロール、リソース、ポリシー、機能、管理者ロールなどの Identity Manager オブジェクトの設定に関する追加情報および手順について説明します。
- 第 6 章 : データの同期と読み込み ー Identity Manager のデータの同期化およびユーザーグループの読み込み機能について説明します。
- 第 7 章 : セキュリティー ー Identity Manager のセキュリティー機能について説明し、Identity Manager 使用時の最良に実装するための推奨事項を示します。
- 第 8 章 : レポート ー Identity Manager システムのフルサービスレポートとリスク分析機能について詳細に説明します。
- 第 9 章 : タスクテンプレート ー 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動作を設定する方法について説明します。
- 第 10 章 : PasswordSync ー Windows システムでユーザーパスワードをセキュアに変更およびリセットし、Identity Manager を使用して同期するための、PasswordSync 機能について説明します。

関連ドキュメントとヘルプ

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

- 『Identity Manager Installation』

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

- 『Identity Manager Upgrade』

  Identity Manager とそれに関連するソフトウェアをアップグレードおよび設定する手順と参照情報が記載されています。

- 『Identity Manager Administration』

  ユーザーが企業情報システムにセキュアにアクセスできるようにするための Identity Manager の使用方法に関する手順、チュートリアル、および例が記載されています。

- 『Identity Manager Technical Deployment Overview』

  Identity Manager 製品の概念に関する概要 (オブジェクトアーキテクチャーを含む) および基本的な製品コンポーネントの紹介が記載されています。

- 『Identity Manager Workflows, Forms, and Views』

  Identity Manager のワークフロー、フォーム、およびビューの使用方法に関する参照と手順情報が記載されています。これらのオブジェクトをカスタマイズするために必要なツールに関する情報も含まれています。

- 『Identity Manager Deployment Tools』

  さまざまな Identity Manager 配備ツールの使用方法に関する参照と手順情報が記載されています。規則と規則ライブラリ、共通のタスクとプロセス、辞書サポート、Identity Manager サーバーによって提供される SOAP ベースの Web サービスインタフェースなどの情報が含まれます。

- 『Identity Manager Resources Reference』

  リソースから Identity Manager へのアカウント情報の読み込みおよび同期方法に関する参照と手順情報が記載されています。

- 『Identity Manager Audit Logging』

  リソースから Identity Manager へのアカウント情報の読み込みおよび同期方法に関する参照と手順情報が記載されています。

- 『Identity Manager Tuning, Troubleshooting and Error Messages』

  Identity Manager のエラーメッセージと例外に関する参照と手順情報、および作業中に発生する可能性のある問題の追跡とトラブルシューティングの手順が記載されています。

- Identity Manager ヘルプ

  Identity Manager に関する完全な手順、参照、用語情報が記載されたオンラインのガイダンスと情報です。ヘルプにアクセスするには、Identity Manager メニューバーの「ヘルプ」リンクをクリックします。重要なフィールドではガイダンス (フィールド固有の情報) が利用可能です。

製品サポート

Identity Manager の配備または使用に関する問題が発生した場合は、次のいずれかの方法でカスタマサポートにお問い合せください。

- オンラインサポートの Web サイト (http://www.sun.com/service/online/us)
- 保守契約に基づいて提供されるサポート電話番号

ご意見をお寄せください

このガイドおよび Identity Manager に同梱のほかのマニュアルについてのご意見をお待ちしております。どのようなことでも、この製品およびマニュアルをご使用になられた感想を、以下にお寄せください。

Sun Microsystems.
5300 Riata Park Court
Austin, TX 78727
宛先 : Identity Manager Information Development

電子メール : idm-idd@sun.com

1 Identity Manager の概要

Sun Java™ System Identity Manager システムを使用すると、アカウントおよびリソースへのアクセスをセキュアかつ効率的に管理することができます。Identity Manager は、定期的なタスクおよび日常の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する例外的なサービスを容易に実行できるようにします。

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要求されます。これまで、ビジネス情報およびシステムへのアクセス管理には、限られた数のアカウントとの直接的な対話しか必要ありませんでした。ところが、アクセス管理は次第に、増大する内部顧客の処理のみならず、企業外のパートナーや顧客の処理も意味するようになってきました。

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

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

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

Identity Manager システムの目的

Identity Manager ソリューションの機能を次に示します。

- 多種多様なシステムおよびリソースに対するアカウントアクセスを管理する。
- 各ユーザーのアカウント配列に対する動的なアカウント情報をセキュアに管理する。
- ユーザーアカウントデータの作成および管理に対する委任された権限をセットアップする。
- 多数の企業リソースと、ますます増大するエクストラネット顧客およびパートナーを処理する。

- 企業情報システムへのユーザーアクセスをセキュアに承認する。Identity Manager では、組織内外でのアクセス特権の許可、管理、および失効の機能が完全に統合される。
- データを保存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

ユーザーアクセスの定義

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

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

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

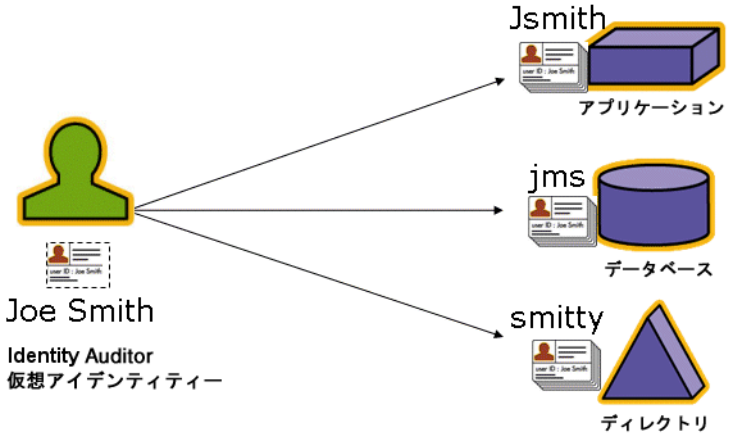


図 1 Identity Manager ユーザーアカウント | リソースの関係

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

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

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

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

管理の委任

ユーザーアイデンティティーマネージメントの役割の分散を成功させるには、柔軟性と管理の適切なバランスを取る必要があります。選択した Identity Manager ユーザーに管理者特権を与えて管理タスクを委任することにより、管理者のオーバーヘッドが軽減します。さらに、人事部長など、ユーザーニーズを熟知したユーザーに ID 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 管理者に異なるレベルの機能を割り当てることができます。機能は、システム内でのさまざまなレベルのアクセスおよび操作を承認します。

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

Identity Manager オブジェクト

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

- ユーザーアカウント
- ロール
- リソースとリソースグループ
- 組織と仮想組織
- 機能
- 管理者ロール

ユーザーアカウント

Identity Manager ユーザーアカウント

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

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

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

ロール

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

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

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

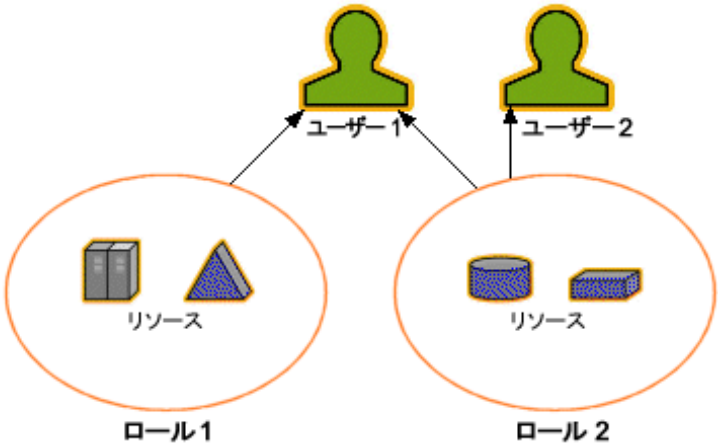


図 2 ユーザーアカウント、ロール、リソースの関係

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

リソースとリソースグループ

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

- メインフレームセキュリティーマネージャー
- データベース
- ディレクトリサービス (LDAP など)
- アプリケーション
- オペレーティングシステム
- ERP システム (SAPa など)
- メッセージプラットフォーム (Microsoft Exchange など)

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

- リソースパラメータ
- アカウント情報 (アカウント属性と ID テンプレートを含む)
- Identity Manager パラメータ

Identity Manager ユーザーアカウントは、次の方法によってリソースにアクセスできます。

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

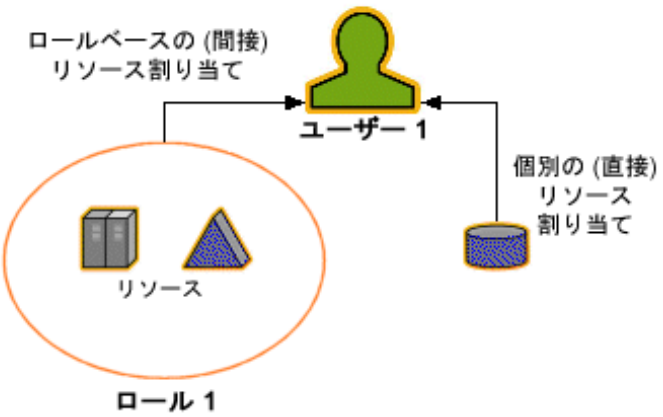


図 3 リソースの割り当て

関連する Identity Manager オブジェクトであるリソースグループを、リソースの割り当てと同じ方法でユーザーアカウントに割り当てることができます。リソースグループは、リソースを相互に関連付けて、アカウントを特定の順序でリソース上に作成できるようにします。

組織

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

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

ほかの組織を含む組織は、親組織です。組織はフラットな構造に作成することも、階層構造内に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。

機能

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

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

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

管理者ロール

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

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

オブジェクトの関係

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

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

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 ある組織内の管理者は、すべてまたは一部のリソースにアクセスできる可能性があります。 管理者 組織は、管理特権を持つユーザーによって管理 (制御) されます。管理者は 1 つ以上の組織を管理できます。ある組織内の管理特権は、子の組織にも継承されます。 ユーザーアカウント 各ユーザーアカウントは、Identity Manager 組織および 1 つ以上のディレクトリ組織に割り当てることができます。
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。

表 1 Identity Manager オブジェクトの関係

Identity Manager の用語

Identity Manager インタフェースおよびガイドでは、用語を次のように定義しています。

管理者ロール

一意の機能セット。管理ユーザーに割り当てられた組織の組み合わせごとに定義します。

管理者

Identity Manager をセットアップしたり、ユーザーの作成やリソースへのアクセスの管理などの操作タスクを実行する役割を持つ個人。

管理者インタフェース

Identity Manager の主要な管理ビュー。

承認者

アクセス要求を承認または却下する管理機能を持つユーザー。

Business Process Editor (BPE)

Identity Manager フォーム、規則、およびワークフローのグラフィカルな表示。

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。

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。

ID 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。

組織

管理の委任を可能にするために使用する Identity Manager コンテナ。組織は、管理者が制御または管理するエンティティー (ユーザーアカウント、リソース、管理者アカウントなど) の範囲を定義します。組織は、主として Identity Manager を管理する目的で「どこで」というコンテキストを提供します。

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。

リソース

Identity Manager では、アカウントが作成されたリソースやシステムへの接続方法についての情報が保存されます。Identity Manager がアクセスを提供するリソースには、メインフレームセキュリティーマネージャー、データベース、ディレクトリサービス、アプリケーション、オペレーティングシステム、ERP システム、およびメッセージプラットフォームがあります。

リソースアダプタ

Identity Manager エンジンとリソースの間のリンクを提供する Identity Manager コンポーネント。このコンポーネントにより、Identity Manager は所定のリソースのユーザーアカウントを管理 (作成、更新、削除、認証、およびスキャン機能を含む) するほか、そのリソースをパススルー認証に利用することができます。

リソースアダプタアカウント

管理するリソースにアクセスするために、Identity Manager リソースアダプタが使用するクレデンシャル。

リソースグループ

ユーザーリソースアカウントを作成、削除、および更新を順序付けするために使用するリソースの集まり。

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、ID テンプレート、および Identity Manager パラメータのセットアップと設定を含め、リソースの作成および修正プロセスの手順を案内する Identity Manager ツール。

ロール

Identity Manager におけるユーザーのクラス用のテンプレートまたはプロファイル。各ユーザーには、1 つ以上のロールを割り当てることができます。ロールはアカウントによるリソースのアクセスとデフォルトのリソース属性を定義します。

規則

XPRESS、XML オブジェクト、または JavaScript 言語で作成された関数を含む Identity Manager リポジトリ内のオブジェクト。規則は、頻繁に使用されるロジックや、フォーム、ワークフロー、およびロール内で再利用される静的な変数を格納するためのメカニズムを提供します。

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。

ユーザー

Identity Manager システムアカウントを所持する個人。Identity Manager では、ユーザーは特定の範囲の機能を持つことができます。拡張機能を持つユーザーは、Identity Manager 管理者です。

ユーザーアカウント

Identity Manager を使用して作成されたアカウント。Identity Manager アカウントと、Identity Manager リソース上のアカウントのいずれかを指します。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

Identity Manager システムの制限されたビュー。特に管理機能を持たないユーザー用に調整したものであり、パスワードの変更や認証質問への回答の設定など、一連の自己管理タスクを実行できます。

ワークフロー

論理的で反復可能なプロセスであり、ドキュメント、情報、またはタスクが、ある関与者から別の関与者に渡されます。Identity Manager ワークフローは、ユーザーアカウントの作成、更新、有効化、無効化、および削除を管理する複数のプロセスで構成されています。

2 Identity Manager 入門

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

- Identity Manager インタフェース
- ヘルプとガイダンス
- 実行可能なタスクとその開始場所

Identity Manager インタフェース

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

- 管理者インタフェース
- ユーザーインタフェース
- Business Process Editor (BPE)

Identity Manager 管理者インタフェース

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

インタフェースは、次のもので構成されます。

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

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

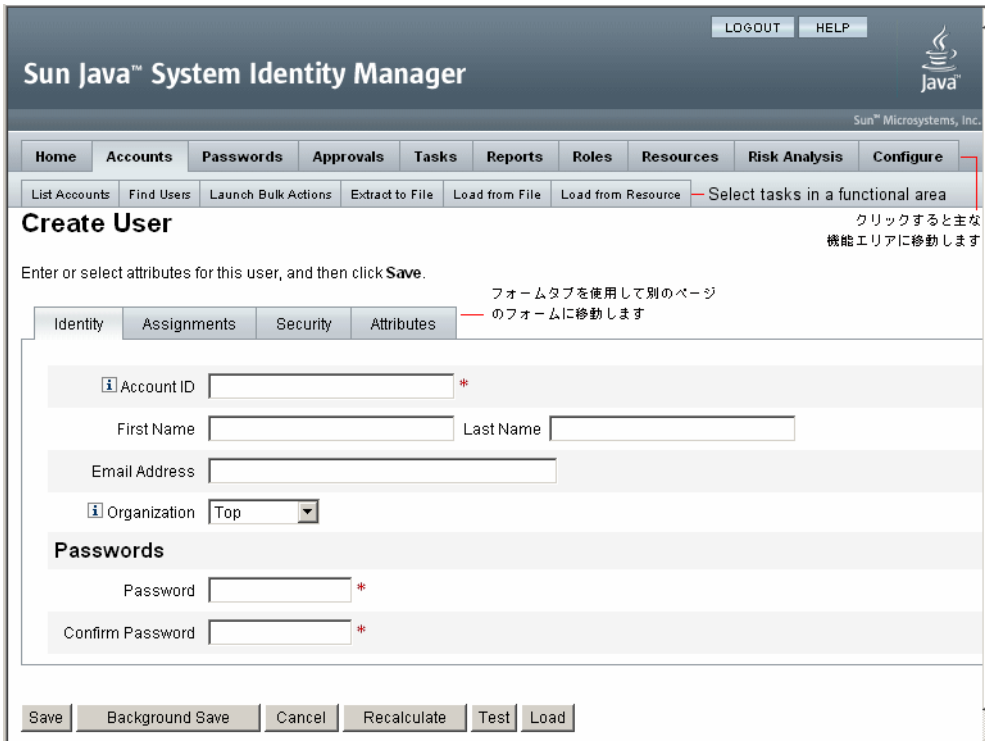


図 1 Identity Manager 管理者インタフェース

Identity Manager ユーザーインタフェース

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

ユーザーインタフェースでは、ユーザーが以下の操作を実行できます。

- 自分のパスワードの変更
- セルフプロビジョニングタスクの実行
- ユーザーアカウントに関連付けられたプロファイル情報の管理

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

ヒント ユーザーインタフェースのカスタマイズおよびブランド設定の詳細については、『Identity Manager Technical Deployment Overview』を参照してください。

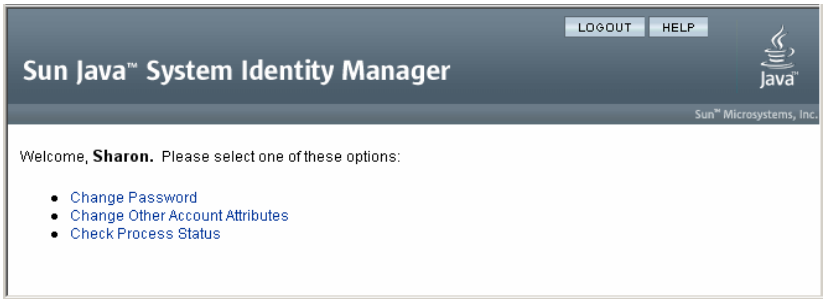


図 2 Identity Manager ユーザーインタフェース

Identity Manager Business Process Editor

Business Process Editor (BPE) は、Identity Manager フォーム、規則、およびワークフローをグラフィカルに表示する設定エディタとしても参照されます。BPE を使用して、Identity Manager の各ページで使用可能な機能を設定するフォームを作成および編集することができます。また、Identity Manager ワークフローを修正することもできます。ワークフローには、Identity Manager ユーザーアカウントを使用するときに適用する一連の処理手順や実行するタスクを定義します。

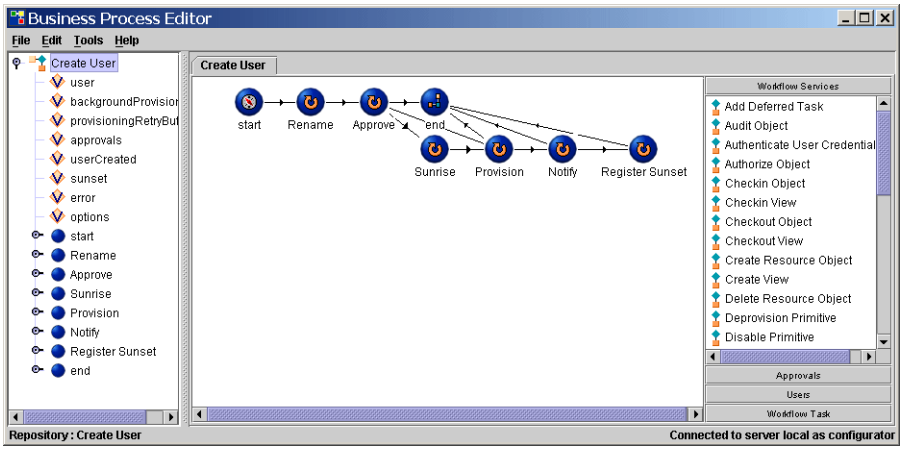


図 3 Business Process Editor (Configuration Editor)

BPE の詳細と、Identity Manager ワークフローでの BPE の使用方法については、『Identity Manager Workflows, Forms, and Views』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、ヘルプおよび Identity Manager ガイダンス (フィールドレベルの情報および指示) を参照しなければならないことがあります。ヘルプとガイダンスは、Identity Manager 管理者インタフェースとユーザーインタフェースから使用可能です。

Identity Manager ヘルプ

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

図 4 ヘルプ

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

情報の検索

ヘルプウィンドウで検索機能を使用して、Identity Manager のヘルプおよびマニュアルに含まれるトピックと情報を検索できます。検索を行うには、次を実行します。

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

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

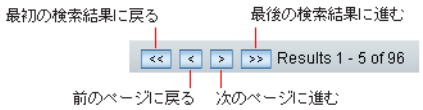


図 5 検索結果のナビゲーション

「リセット」をクリックすると、ヘルプウィンドウの内容がクリアされます。

検索の動作

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

たとえば、次の語句を入力したとします。

```
resource adapter
```

この場合、検索結果では、次の語に一致するものが返されます。

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

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

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

高度なクエリー構文

検索機能では、次を含む高度なクエリー構文がサポートされています。

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

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

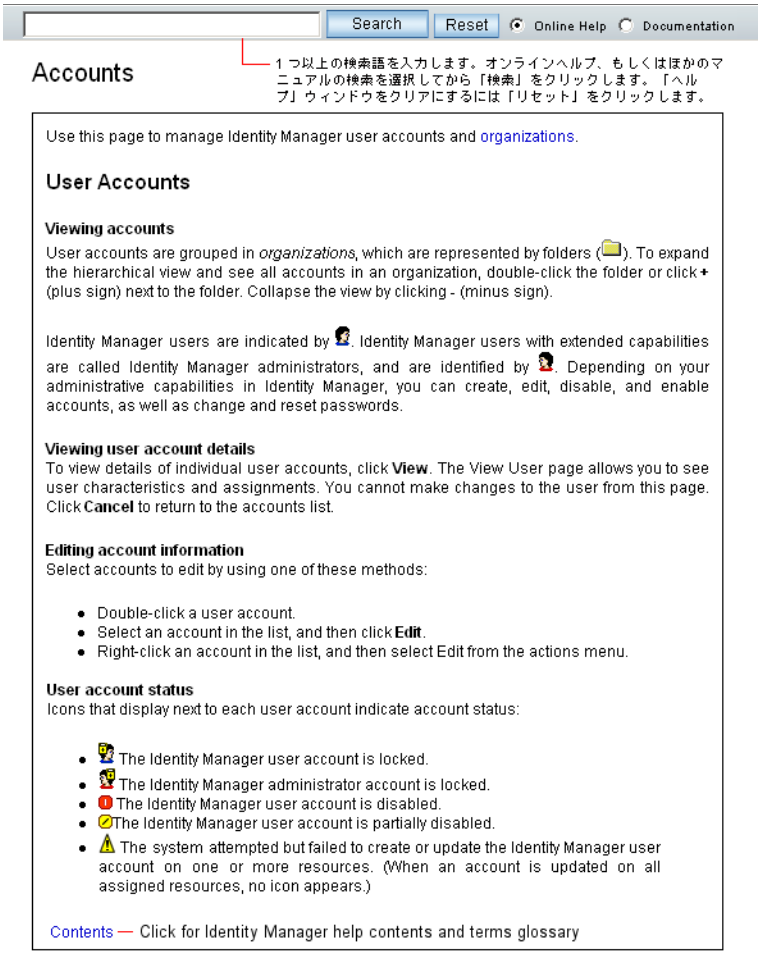


図 6 Identity Manager ヘルプ

Identity Manager ガイダンス

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

記号は、フィールドの横にガイダンスとともに表示されます。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。

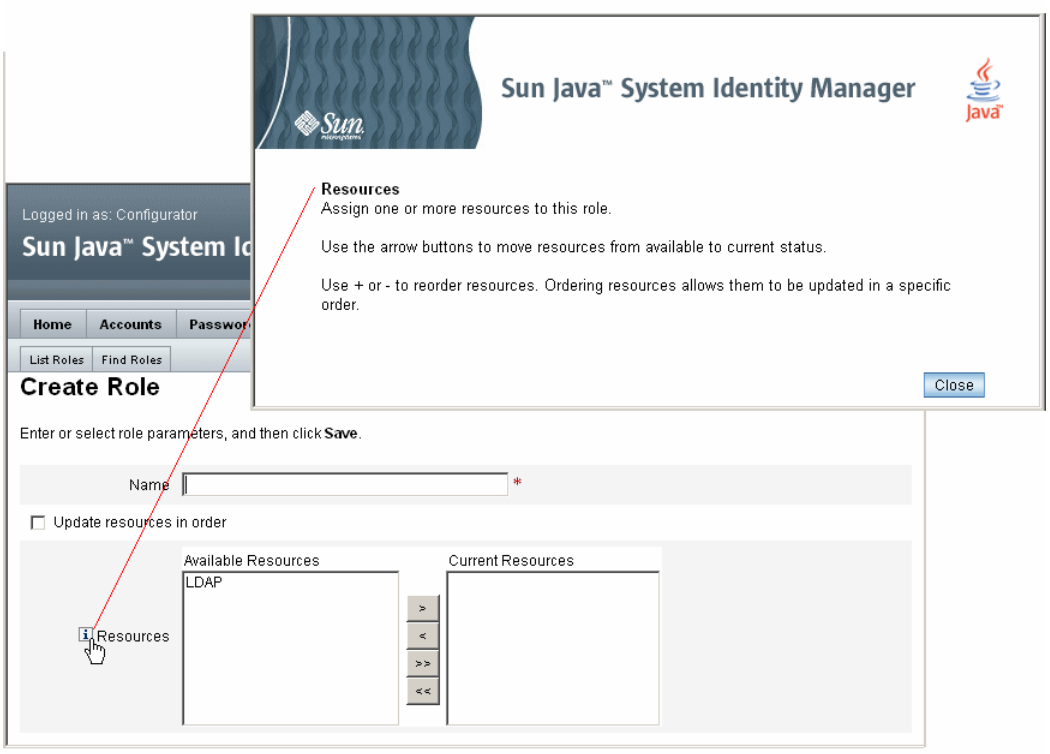


図 7 Identity Manager ガイダンス

Identity Manager タスク

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

Identity Manager ユーザーの管理		
操作	移動場所	代替方法
ユーザーの作成と編集	**「アカウント」**タブ、**「アカウントのリスト」**選択	**「アカウント」**タブ、**「ユーザーの検索」**選択 (「ユーザーアカウントの検索結果」ページ)
ユーザーアカウントの作成の承認	**「承認」**タブ	
ユーザー認証のセットアップ (ポリシー)	**「設定」**タブ、**「ポリシー」**選択	
ユーザーパスワードの変更	**「パスワード」**タブ、**「ユーザーパスワードの変更」**選択	• **「アカウント」**タブ、**「アカウントのリスト」**選択 • **「アカウント」**タブ、**「ユーザーの検索」**選択 (「ユーザーアカウントの検索結果」ページ) • Identity Manager ユーザーインタフェース
ユーザーパスワードのリセット	「パスワード」タブ、「ユーザーパスワードのリセット」選択	• **「アカウント」**タブ、**「アカウントのリスト」**選択 • **「アカウント」**タブ、**「ユーザーの検索」**選択 (「ユーザーアカウントの検索結果」ページ)
ユーザーの検索	**「アカウント」**タブ、**「ユーザーの検索」**選択	**「パスワード」**タブ、**「ユーザーパスワードの変更」**選択
ユーザーの有効化または無効化	**「アカウント」**タブ、**「アカウントのリスト」**選択	**「アカウント」**タブ、**「ユーザーの検索」**選択 (「ユーザーアカウントの検索結果」ページ)
ユーザーのロック解除	**「アカウント」**タブ、**「アカウントのリスト」**選択	**「アカウント」**タブ、**「ユーザーの検索」**選択 (「ユーザーアカウントの検索結果」ページ)

Identity Manager 管理者の管理	
操作	**移動場所**
組織を通じて委任された管理のセットアップ	**「アカウント」**タブ、**「アカウントのリスト」**選択、「ユーザーの作成」ページ
機能の割り当て	**「アカウント」**タブ、**「アカウントのリスト」**選択、「ユーザーの作成」ページ
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」ページ
承認者のセットアップ (アカウントの作成を検証するため)	• **「アカウント」**タブ、**「アカウントのリスト」**選択、「組織の作成」ページ • **「ロール」**タブ、「ロールの作成」ページ
Identity Manager の設定	
操作	**移動場所**
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	**「設定」**タブ、**「機能」**選択
管理者ロールの作成および編集	**「設定」**タブ、**「管理者ロール」**選択、「管理者ロールの作成 / 編集」ページ
電子メールテンプレートのセットアップ	**「設定」**タブ、**「電子メールテンプレート」**選択
パスワード、アカウント、および名前ポリシーのセットアップ。組織へのポリシーの割り当て	**「設定」**タブ、**「ポリシー」**選択
ID 属性の設定	**「設定」**タブ、**「ID 属性」**選択
ChangeLog の設定	**「設定」**タブ、**「ChangeLog」**選択

アカウントおよびデータの読み込みと同期		
操作	**移動場所**	
データファイルのインポート (XML 形式のフォームなど)	**「設定」**タブ、**「交換ファイルのインポート」**選択	
リソースアカウントの読み込み	**「アカウント」**タブ、**「リソースから読み込み」**選択	
アカウントのファイルからの読み込み	**「アカウント」**タブ、**「ファイルから読み込み」**選択	
Identity Manager ユーザーをリソースアカウントと比較	**「リソース」**タブ、**「リソースの調整」**選択	
監査、リスク分析、およびレポート		
操作	**移動場所**	**操作**
イベント監査取得のセットアップ	**「設定」**タブ、**「イベント監査」**選択	イベント監査取得のセットアップ
レポートの実行および管理	**「レポート」**タブ	レポートの実行および管理
リスク分析レポートの定義および実行	**「リスク分析」**タブ	リスク分析レポートの定義および実行

表 1 Identity Manager インタフェースタスクリファレンス

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学んだあとは、以下の任意のトピックに進むことができます。これらのトピックは、このガイドの章ごとに記載されています。

- 第 3 章 : ユーザーとアカウントの管理
- 第 4 章 : 管理
- 第 5 章 : 設定
- 第 6 章 : データの同期と読み込み
- 第 7 章 : セキュリティー
- 第 8 章 : レポート
- 第 9 章 : タスクテンプレート
- 第 10 章 : PasswordSync

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管理の説明および手順を示します。次に示す Identity Manager ユーザーおよびアカウントの管理タスクについて説明します。

- ユーザーアカウントデータとその格納方法
- Identity Manager 管理者インタフェースの「アカウント」エリア
- アカウントの作成と編集機能、およびその他のアカウント関連タスク
- ユーザーアカウントの検索機能
- パスワードポリシーとユーザーアカウントパスワード
- ユーザーの自己管理
- ユーザー認証
- 一括アカウント操作

ユーザーアカウントデータについて

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

Identity Manager の管理者インタフェースの**「アカウント」**タブにある「ユーザーの作成」ページでは、ユーザーデータが 4 つのエリアに分類されて表示されます。

- ID
- 割り当て
- セキュリティー
- 属性

ID

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

注　アカウントパスワードポリシーの設定の詳細については、この章の「パスワードポリシーの設定」セクションを参照してください。

次の図は、「ユーザーの作成」ページの「ID」エリアを示します。

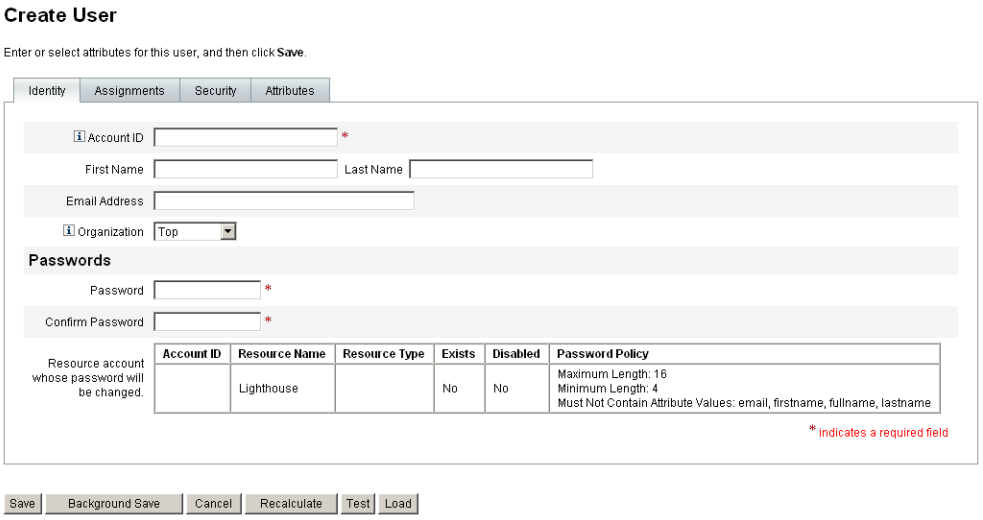


図 1 「ユーザーの作成」- 「ID」

割り当て

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

「割り当て」フォームのタブをクリックして、次を設定します。

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

セキュリティー

Identity Manager では、拡張機能が割り当てられたユーザーを Identity Manager 管理者と呼びます。「セキュリティー」エリアでは、次を割り当てることによって、これらの拡張管理機能をユーザーに設定します。

- **管理者ロール** ― 機能および管理する組織の一意のセットを組み合わせることによって、管理ユーザーに、調整済みの割り当てを簡単に設定できます。

- **機能** – Identity Manager システムでの権限を有効にします。各 Identity Manager 管理者には、多くの場合は職務に応じて、1 つ以上の機能が割り当てられます。
- **管理する組織** – ユーザーが管理者として管理する権限を持つ組織を割り当てます。管理者は、割り当てられた組織のオブジェクト、および階層内でその組織の下位にあるすべての組織のオブジェクトを管理できます。

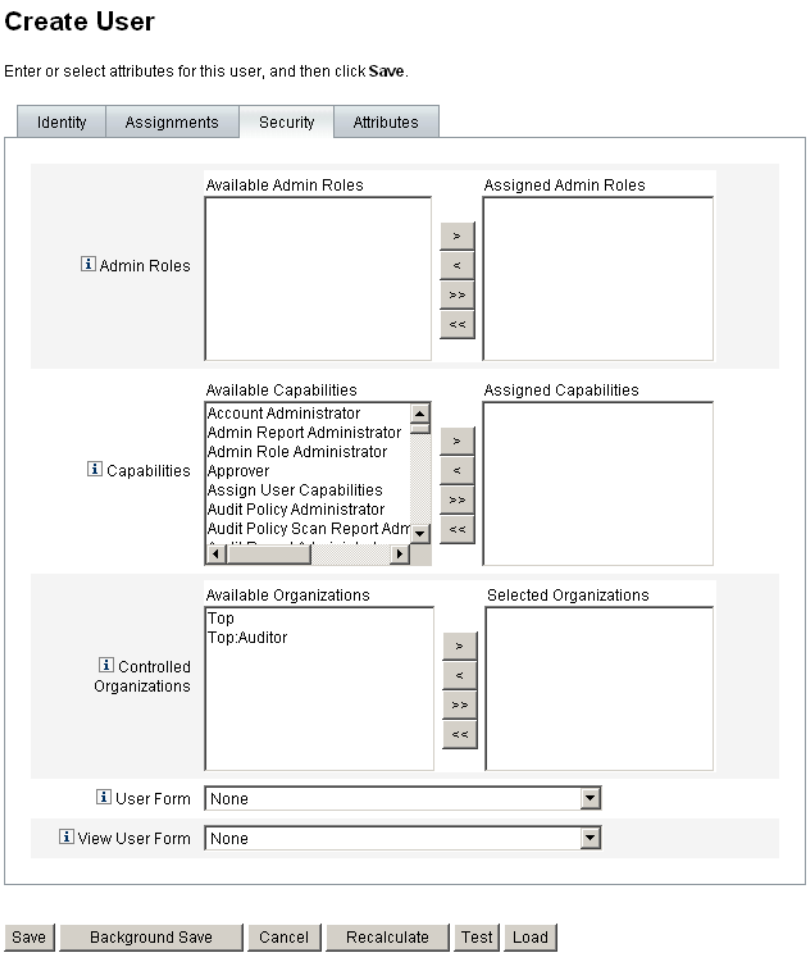


図 2 「ユーザーの作成」-「セキュリティー」

属性

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

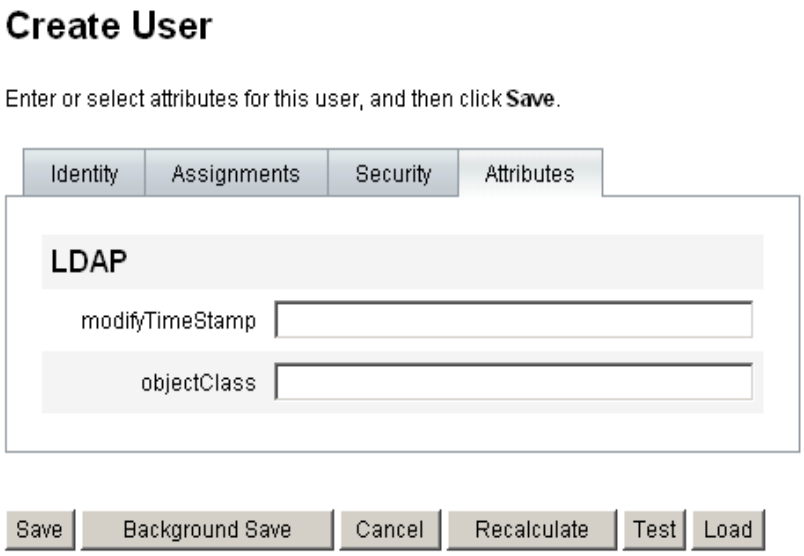


図 3 「ユーザーの作成」-「属性」

「アカウント」エリア

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

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

アカウントリストは、フルネーム (「名前」)、ユーザーの姓 (「姓」)、またはユーザーの名 (「名」) で並べ替えることができます。

列で並べ替えるには、ヘッダーバーをクリックします。同じヘッダーバーをクリックすると、昇順と降順が切り替わります。

注　フルネーム (「名前」列) で並べ替えると、階層内のすべてのレベルのすべての項目がアルファベット順に並べ替えられます。

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

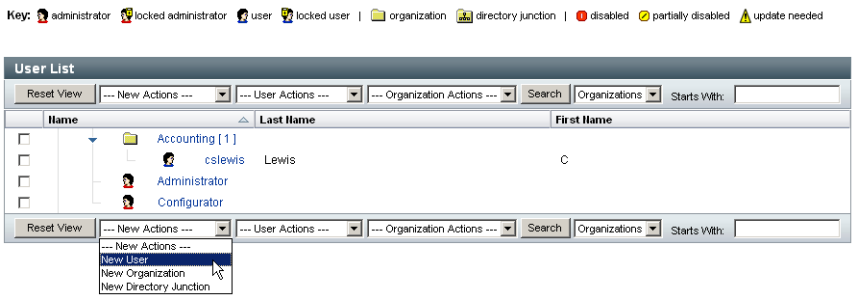


図 4　アカウントリスト

「アカウント」エリアの操作リスト

一連の操作を実行するときは、「アカウント」エリアの上部と下部にある操作リストを使用します。操作リストの選択項目は、次のように分類されています。

- **「新規作成アクション」**― ユーザー、組織、およびディレクトリジャンクションを作成します。
- **「ユーザーアクション」**― ユーザーのステータスの編集、表示、および変更、パスワードの変更およびリセット、ユーザーの削除、有効化、無効化、ロック解除、移動、更新、および名前変更、ユーザー監査レポートの実行を行います。
- **「組織アクション」**― 組織およびユーザーの一連の操作を実行します。

「アカウント」エリアでの検索

ユーザーと組織を検索するときは、「アカウント」エリアの検索機能を使用します。リストから「組織」または「ユーザー」を選択し、検索エリアに 1 文字以上を入力して、**「検索」**をクリックします。

ユーザーアカウントステータス

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

インディケータ	**ステータス**
	Identity Manager ユーザーアカウントはロックされています。これは、ログイン試行の失敗回数が、リソースに設定された制限を越えたために、ユーザーがリソースアカウントからロックアウトされていることを示します。
	Identity Manager 管理者アカウントはロックされています。
	アカウントは、割り当てられたすべてのリソースおよび Identity Manager で無効になっています。アカウントが有効なときは、アイコンは表示されません。
	アカウントは、一部無効になっています。これは、割り当てられた 1 つ以上のリソースで無効になっていることを示します。
	1 つ以上のリソースで Identity Manager ユーザーアカウントの作成または更新が試行されましたが、失敗しました。割り当てられたすべてのリソースでアカウントが更新されたときは、アイコンは表示されません。

ユーザーアカウントの操作

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

- **ユーザー** ― 表示、作成、編集、移動、名前変更、プロビジョン解除、有効化、無効化、更新、ロック解除、削除、割り当て解除、リンク解除、および監査
- **パスワード** ― 変更およびリセット
- **組織** ― 作成、編集、更新、および削除
- **ディレクトリジャンクション** ― 作成

ユーザー

表示

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

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

作成 (「新規作成アクション」リスト、「新規ユーザー」選択)

ユーザーアカウントを作成するには、「新規作成アクション」リストから「新規ユーザー」を選択します。

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

1 つのエリアで利用可能な選択項目は、別のエリアでの選択により異なります。

「ユーザーの作成」ページ (ユーザーフォームとも呼ばれる) は、複数ページのフォームであり、ユーザーに対して次のものをセットアップできます。

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

注 ビジネスプロセスや特定の管理者機能をより適切に反映するように、環境に合わせたユーザーフォームを設定できます。ユーザーフォームの詳細については、『Identity Manager Workflows, Forms, and Views』を参照してください。

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

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

ステータスインディケータ	ステータス
	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。
	プロセスは完了しましたが、1 つ以上のエラーが発生しました。

ヒント ステータスインディ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。

複数のユーザーアカウント (アイデンティティー) の作成

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

編集

アカウント情報を編集するには、次のいずれかの操作を選択します。

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

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

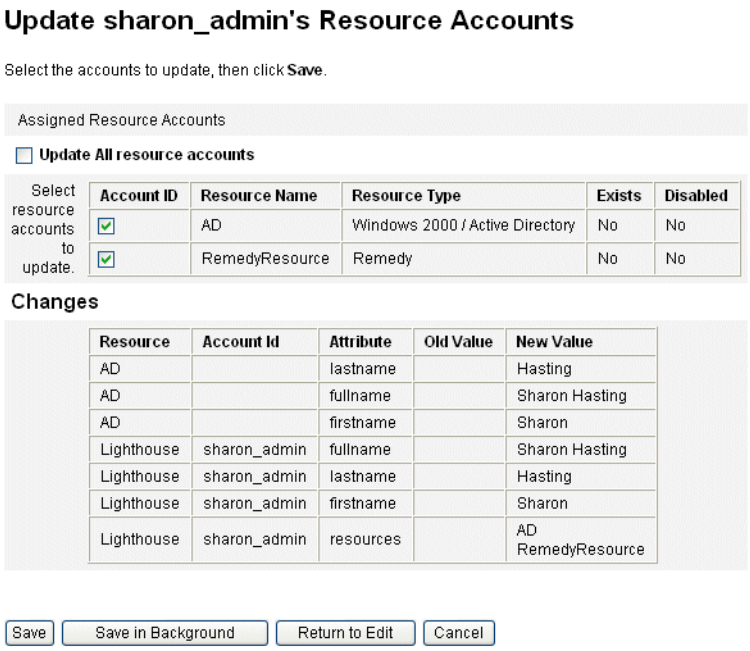


図 5 ユーザーの編集 (リソースアカウントの更新)

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

ユーザーの移動 (「ユーザーアクション」)

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

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

名前の変更 (「ユーザーアクション」)

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

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

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

注　　リソースタイプの一部では、アカウントの名前変更をサポートしません。

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

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

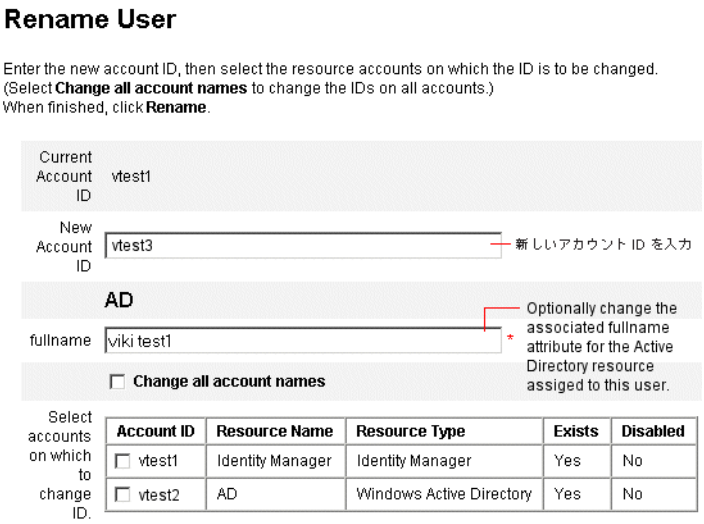


図 6 ユーザーの名前変更

ユーザーの無効化 (「ユーザーアクション」、「組織アクション」)

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

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

1 つのユーザーアカウントの無効化

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

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

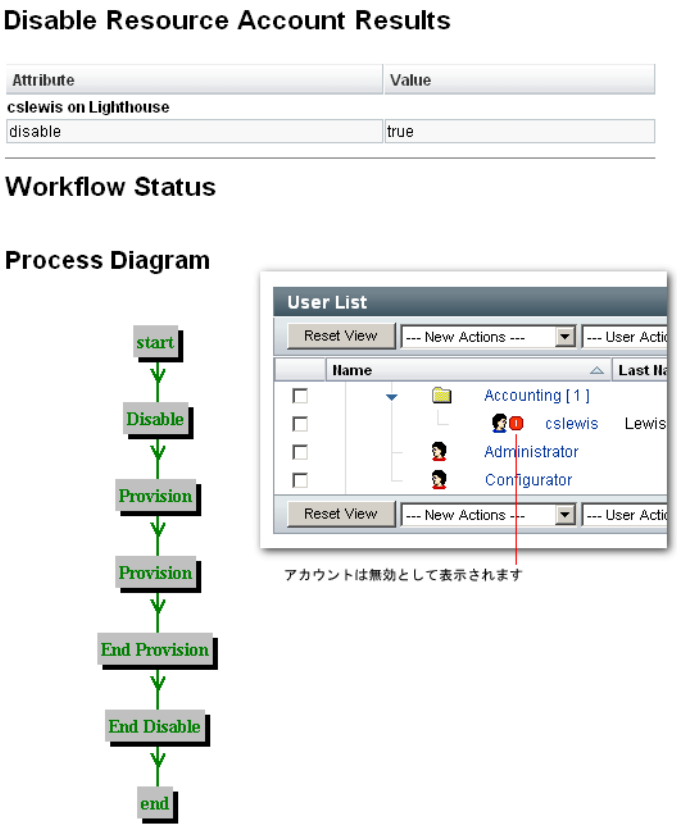


図 7 無効化されたアカウント

複数のユーザーアカウントの無効化

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

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

ユーザーの有効化 (「ユーザーアクション」、「組織アクション」)

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

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

1 つのユーザーアカウントの有効化

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

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

複数のユーザーアカウントの有効化

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

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

ユーザーの更新 (「ユーザーアクション」、「組織アクション」)

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

- 更新の実行時にリソースが利用不可能だった場合

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

ユーザーアカウントの更新時には、次を選択できます。

- 割り当てられたリソースアカウントが更新された情報を受け取るかどうか
- すべてのリソースアカウントを更新するか、リストから個別のアカウントを選択するか

1 つのユーザーアカウントの更新

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

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

確認ページで各リソースに送信されるデータを確認します。

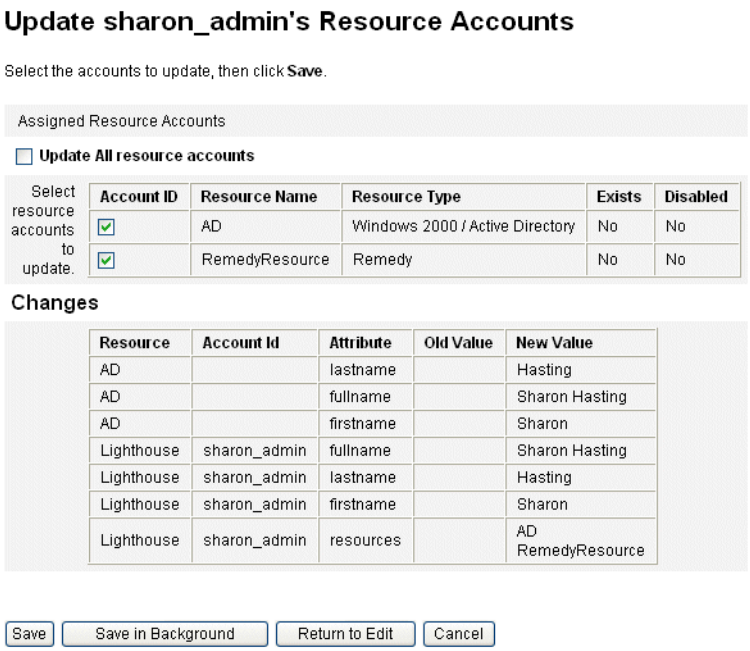


図 8 リソースアカウントの更新

複数のアカウントの更新

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

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

ユーザーのロック解除 (「ユーザーアクション」、「組織アクション」)

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

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

パスワードによるログイン試行の失敗

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

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

質問によるログイン試行の失敗

質問によるログイン試行の最大回数を超えたためにロックされた場合、ユーザーアカウントは、次の期間ロックされたままになります。

- 管理ユーザーがそのユーザーアカウントをロック解除するまで。アカウントを正常にロック解除するには、管理者に「Unlock User」機能が割り当てられていて、管理者がそのユーザーのメンバー組織の管理コントロールを持っている必要があります。

- ロックされたユーザー、または適切な機能を持つユーザーが、ユーザーのパスワードを変更またはリセットするまで。

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

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

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

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

削除 (「ユーザーアクション」、「組織アクション」)

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

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

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

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

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

ユーザーアカウントとリソースアカウントの削除

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

リソースアカウントの割り当て解除またはリンク解除

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

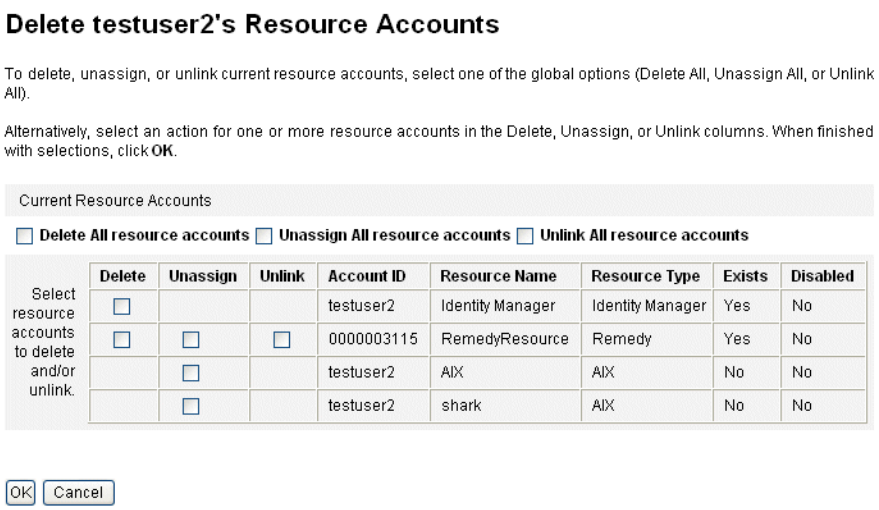


図 9 ユーザーアカウントとリソースアカウントの削除

アカウントの検索

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

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

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

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

- 編集するユーザーアカウントの選択。アカウントを編集するには、検索結果リストでそのアカウントをクリックするか、またはリストでそのアカウントを選択して**「編集」**をクリックします。

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

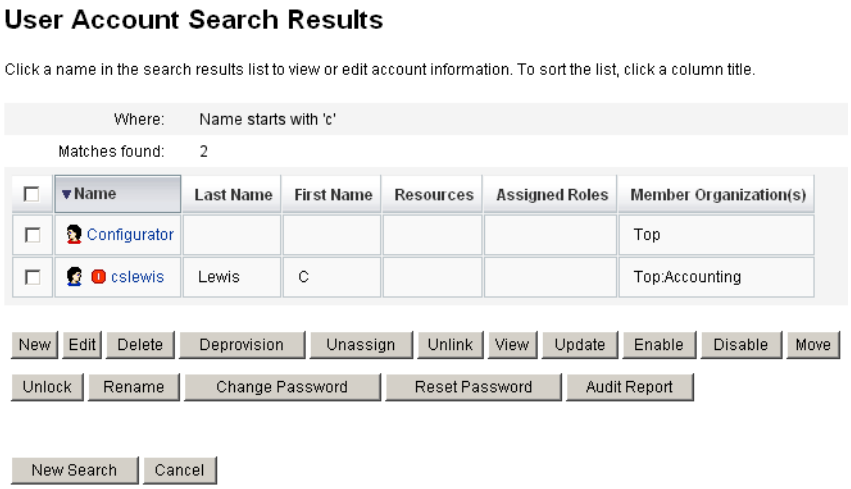


図 10 ユーザーアカウントの検索結果

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。パスワードポリシーを編集して、一連の特性に対する値を設定または選択することができます。

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

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

ポリシーの作成

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

長さ規則

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

文字タイプ規則

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

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

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

文字タイプ規則の最小個数

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。

ヒント　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。

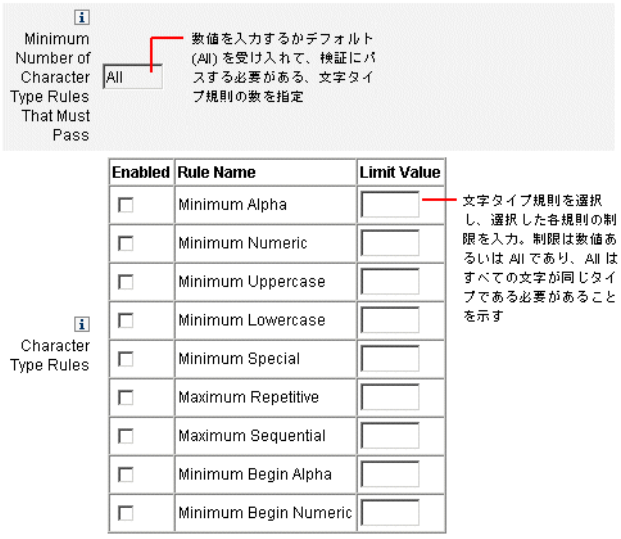


図 11　パスワードポリシー (文字タイプ) 規則

辞書ポリシーの選択

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

- 辞書の設定
- 辞書の単語の読み込み

辞書は「ポリシー」ページから設定します。辞書のセットアップの詳細については、『Identity Manager Deployment Tools』の「Configuring Dictionary Support」の章を参照してください。

パスワード履歴ポリシー

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

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

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

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

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

使用禁止単語

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

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

使用禁止属性

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

- accountID
- email
- firstname
- fullname
- lastname

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

パスワードポリシーの実装

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

ユーザーアカウントパスワードの操作

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

ユーザーアカウントパスワードの変更

ユーザーアカウントパスワードを変更するには、次を実行します。

1. メニューバーで、**「パスワード」**を選択します。
   「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。
2. パスワードを変更するユーザーを入力または検索します。次のいずれかのオプションを選択します。
   - ユーザー名を入力して、**「パスワードの変更」**をクリックします。
   - 「ユーザー ID」フィールドに、名前の文字を 1 つ以上入力して、**「検索」**をクリックします。Identity Manager により、入力した文字が ID に含まれているすべてのユーザーのリストが返されます。ユーザーをクリックして選択すると、「ユーザーパスワードの変更」ページに戻ります。

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

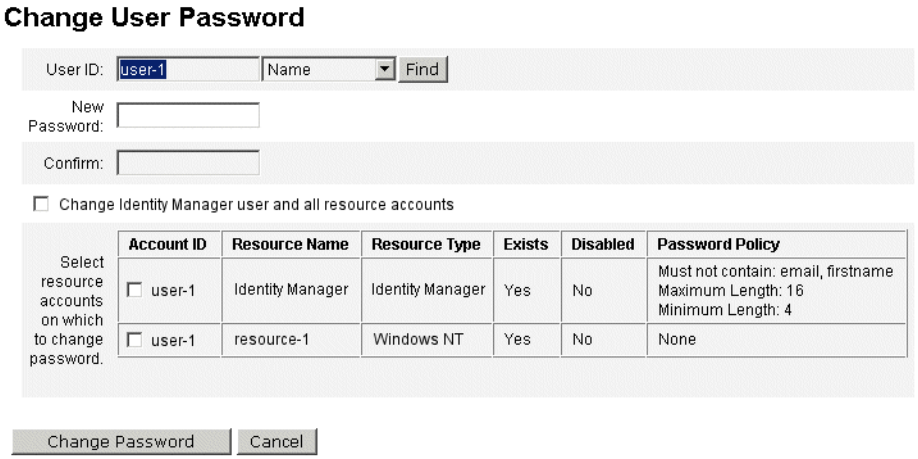


図 12 ユーザーパスワードの変更

ユーザーアカウントパスワードのリセット

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

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

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

リセット時のパスワードの期限切れ

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

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

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

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

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

ユーザーの自己検索

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

自己検索の有効化

自己検索を有効にするには、特別な設定オブジェクト (エンドユーザーリソース) を編集して、アカウントの検索を許可される各リソースの名前を追加する必要があります。その場合は、次を実行します。

1. Identity Manager システム設定ページを開きます (`idm/debug`)。
2. 「List Objects」ボタンの隣のリストから「Configuration」を選択し、**「List Objects」**ボタンをクリックします。
3. 「End User Resources」の隣の**「Edit」**をクリックすると、設定オブジェクトが表示されます。
4. `<String>`***Resource***`</String>` を追加します。ここで、***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。

Checkout Object: Configuration, #ID#Configuration:EndUserResources

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Configuration PUBLIC 'waveset.dtd' 'waveset.dtd'>
<!--  id="#ID#Configuration:EndUserResources" name="End User Resources"-->
 <Configuration id='#ID#Configuration:EndUserResources' name='End User Resources'
creator='Configurator' createDate='1026770940487' lastMod='7' counter='0'>
  <Extension>
    <List>
       <String>NT</String>  ← 自己検索に追加するリソースごとに１行を追加
    </List>
  </Extension>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' id='#ID#Top' name='Top'/>
  </MemberObjectGroups>
</Configuration>
```

Save Cancel

図 13 エンドユーザーリソースの設定オブジェクト

5. **「保存」**をクリックします。

自己検索が有効になっている場合は、Identity Manager ユーザーインタフェースに新しいメニュー項目 (**「ほかのアカウントについて Identity Manager に知らせる」**) が表示されます。このエリアにより、ユーザーは利用可能リストからリソースを選択し、リソースアカウント ID とパスワードを入力してアカウントを自分の Identity Manager ID にリンクすることができます。

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

アカウントポリシーで認証を設定するには、次を実行します。

1. メニューバーの**「設定」**を選択し、**「ポリシー」**を選択します。
2. ポリシーのリストから「Default Lighthouse Account Policy」を選択します。
   ページの「二次認証ポリシーオプション」エリアで認証を選択できます。

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

設定した認証規則に応じて、次に対して回答するようユーザーに要求することができます。

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

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

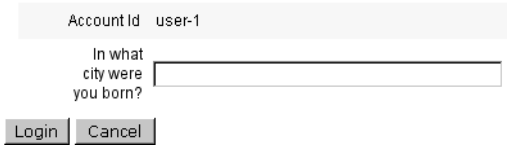


図 14 ユーザーアカウント認証

ユーザー独自の認証質問

Lighthouse アカウントポリシーでは、ユーザーがユーザーインタフェースおよび管理者インタフェースで独自の認証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、ユーザー独自の認証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、「認証質問の回答の変更」ページから質問を追加および変更できます。

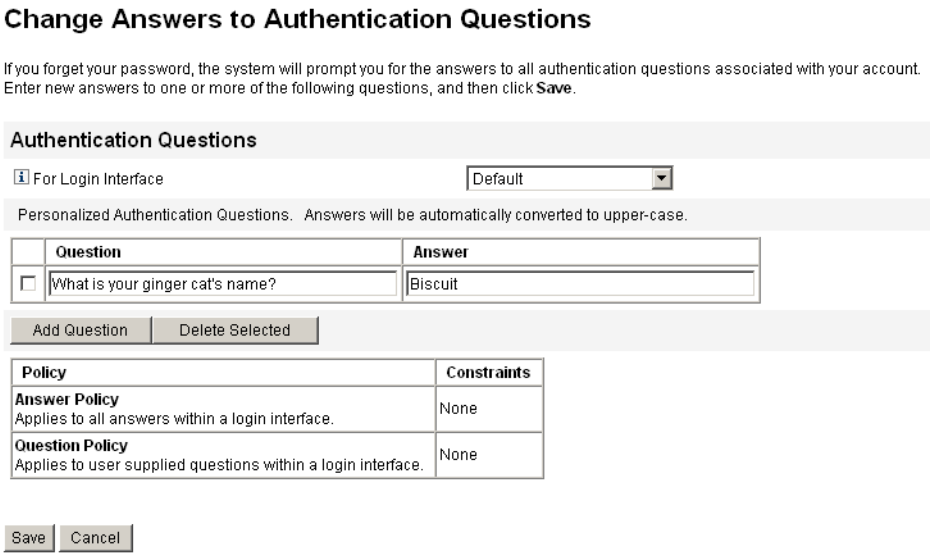


図 15 回答の変更 — ユーザー独自の認証質問

認証後のパスワード変更要求のバイパス

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要求されます。ただし、`bypassChangePassword` システム設定プロパティーを設定することによって、1 つ以上の Identity Manager アプリケーションでパスワードの変更要求をバイパスするように Identity Manager を設定できます。

認証に成功したあと、すべてのアプリケーションでパスワードの変更要求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。

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

特定のアプリケーションでバイパスを無効にするには、次のように設定します。

```
<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>
    ...
```

一括アカウント操作

Identity Manager アカウントに対していくつかの一括操作を実行できます。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。開始できる一括操作を、次に示します。

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

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

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

一括アカウント操作の起動

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

ヒント 一括操作タスクのステータスを監視するには、**「タスク」**タブに進んでタスクのリンクをクリックします。

操作リストの使用

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

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

どの一括操作 CSV にも必須のフィールドが 2 つあります。

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

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

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

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

これらの操作のいくつかを、CSV 形式にした例を次に示します。

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

Create、Update、および CreateOrUpdate コマンド

Create、Update、または CreateOrUpdate コマンドを実行する場合は、user フィールドと command フィールドのほかに、ユーザー画面のフィールドを指定できます。使用するフィールド名は、画面の属性のパス表現です。ユーザー画面で使用可能な属性については、『Identity Manager Workflows, Forms, and Views』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。

一括操作で使用する一般的なパス表現のいくつかを次に示します。

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

例

作成および更新操作を、CSV 形式にした例を次に示します。

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

複数の値を持つフィールド

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

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

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

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

選択できる指示は次のとおりです。

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

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

フィールド値の特殊文字

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

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

一括操作の表示属性

Create、Update、または CreateOrUpdate 操作を実行する場合は、ユーザー画面に、一括操作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、一括操作に固有の動作を可能にします。属性は次のとおりです。

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

相関規則と確認規則

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

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

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

相関規則

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

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

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

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

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

拡張属性の相関を行うには特別な設定が必要です。

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

確認規則

確認規則の入力は次のとおりです。

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

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

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

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

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

4 管理

この章では、Identity Manager システムで一連の管理レベルタスクを実行するための説明および手順を示します。次のタスクが含まれます。

- Identity Manager 管理者および委任された管理の作成
- 組織と仮想組織の定義
- 管理者の作成と管理

Identity Manager の管理について

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

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

Identity Manager 管理者は、次が割り当てられる点で、ユーザーと区別されます。

- **拡張機能**。管理者は、管理対象の各組織内のアカウント、ロール、およびリソースに対して拡張機能を利用します。
- **管理する組織**。組織の管理を割り当てられると、管理者は、その組織内と、階層内でその組織の下にあるすべての組織のオブジェクトを管理できます。

委任された管理

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

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

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

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

- 固有の組織およびその組織内のオブジェクトに対する管理を制限する

- Identity Manager ユーザーの作成および編集ページの管理者ビューをフィルタする
- 管理者に固有のジョブの任務を機能の形式で与える

Identity Manager 組織について

組織を使用して、次のことができます。

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

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

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

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

組織の作成

組織は、「Identity Manager アカウント」エリアで作成します。組織を作成するには、次を実行します。

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

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

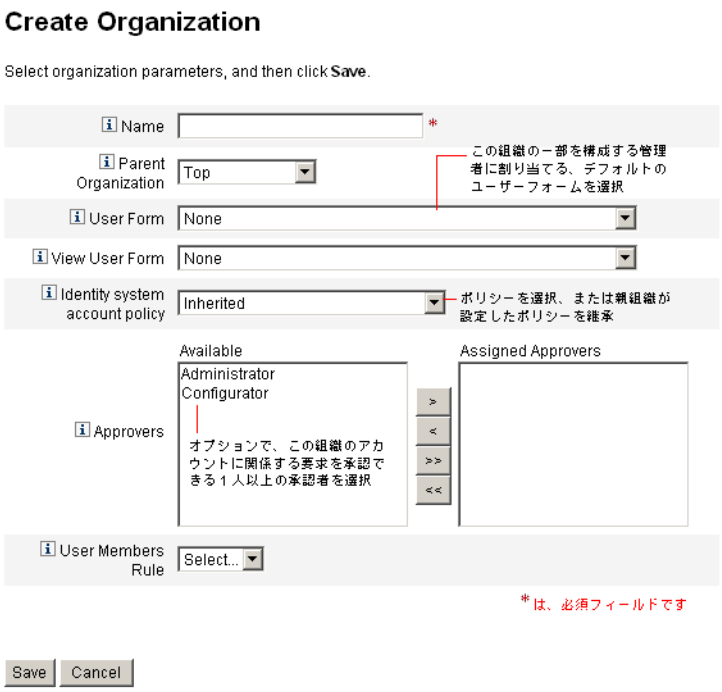


図 1 組織の作成

組織へのユーザーの割り当て

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

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

- ユーザーへのアクセスを要求する (現在の管理者がユーザーメンバー規則を持つ組織を管理している場合)

ユーザーメンバー規則は、「組織の作成」ページの「ユーザーメンバー規則」フィールドで選択します。

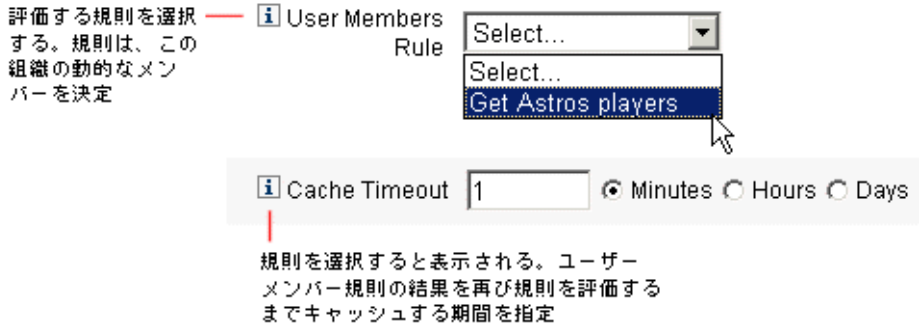


図 2 組織の作成 : ユーザーメンバー規則の選択

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

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

キーの定義と取り込み

- 「ユーザーメンバー規則」オプションボックスに規則を表示するには、authType を `authType='UserMembersRule'` と設定する必要があります。
  - コンテキストは、現在認証されている Identity Manager ユーザーのセッションです。
  - 定義された変数 (`defvar`) の「Astros players」は、Windows Active Directory の「Houston Astros」OU から、そのすべてのメンバーユーザーの 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、「Houston Astros」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 (「:dogbreath-AD」など)。
  - 結果は、Identity Manager リソース名が連結された DN (「<dn>:dogbreath-AD」など) のリストとして返されます。

ユーザーメンバー規則の例

```
<Rule name='Get Astros players'
         authType='UserMembersRule'>
   <defvar name='Astros 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>dogfish-AD</s>
      <map>
         <s>searchContext</s>
         <s>OU=Houston Astros,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>:dogbreath-AD</s>
      </concat>
      </append>
   </dolist>
      <ref>player names</ref>
   </block>
   </defvar>
      <ref>Astros players</ref>
</Rule>
```

管理する組織の割り当て

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

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

ディレクトリジャンクションおよび仮想組織について

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

ディレクトリジャンクション内の各組織が、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。

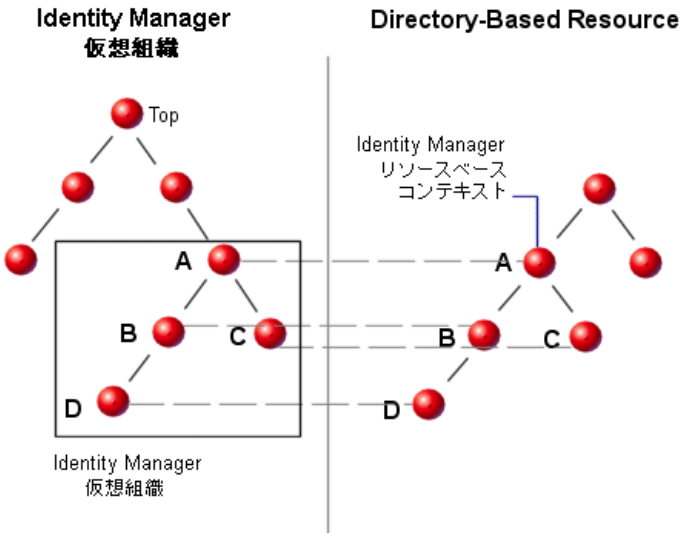


図 3 Identity Manager 仮想組織

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

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

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

ディレクトリジャンクションのセットアップ

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

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

   選択した組織は、セットアップする仮想組織の親組織になります。

   Identity Manager に「ディレクトリジャンクションの作成」ページが表示されます。
3. 項目を選択して、仮想組織をセットアップします。

- **「親組織」** ― このフィールドには「アカウント」リストから選択した組織が含まれています。ただし、リストから異なる親組織を選択することもできます。
- **「ディレクトリリソース」** ― 構造を仮想組織にミラー化する既存のディレクトリを管理するディレクトリリソースを選択します。
- **「ユーザーフォーム」** ― この組織の管理者に適用するユーザーフォームを選択します。
- **「Identity Manager アカウントポリシー」** ― ポリシーを選択します。または、デフォルトのオプション (継承) を選択すると親組織からポリシーが継承されます。
- **「承認者」** ― この組織に関係する要求を承認できる管理者を選択します。

仮想組織の更新

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

仮想組織の削除

仮想組織を削除する場合は、次の 2 つの削除オプションから選択できます。

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

いずれかのオプションを選択して、**「削除」** をクリックします。

管理者の作成

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

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

ユーザーに管理特権を与えるには、**「アカウント」** を選択して「Identity Manager アカウント」エリアに移動し、**「セキュリティー」** フォームタブを選択します。

1 つ以上の項目を選択して、管理コントロールを設定します。

- **「管理する組織」** − 組織を 1 つ以上選択します。管理者は、選択した組織内と、階層内でその組織の下にある任意の組織内のオブジェクトを管理できます。管理の範囲は、割り当てられた機能によってさらに定義されます。このエリアで項目を 1 つ選択する必要があります。
- **「機能」** − この管理者が管理する組織内でこの管理者が持つ機能を 1 つ以上選択します。Identity Manager 機能の詳細については、第 5 章「設定」を参照してください。
- **「ユーザーフォーム」** − Identity Manager ユーザーの作成および編集時にこの管理者が使用するユーザーフォームを選択します (その機能が割り当てられている場合)。ユーザーフォームを直接割り当てない場合、管理者は自分の所属する組織に割り当てられたユーザーフォームを継承します。ここで選択されたフォームは、この管理者の組織で選択されたどのフォームよりも優先されます。
- **「承認要求転送先」** − すべての保留中承認要求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。

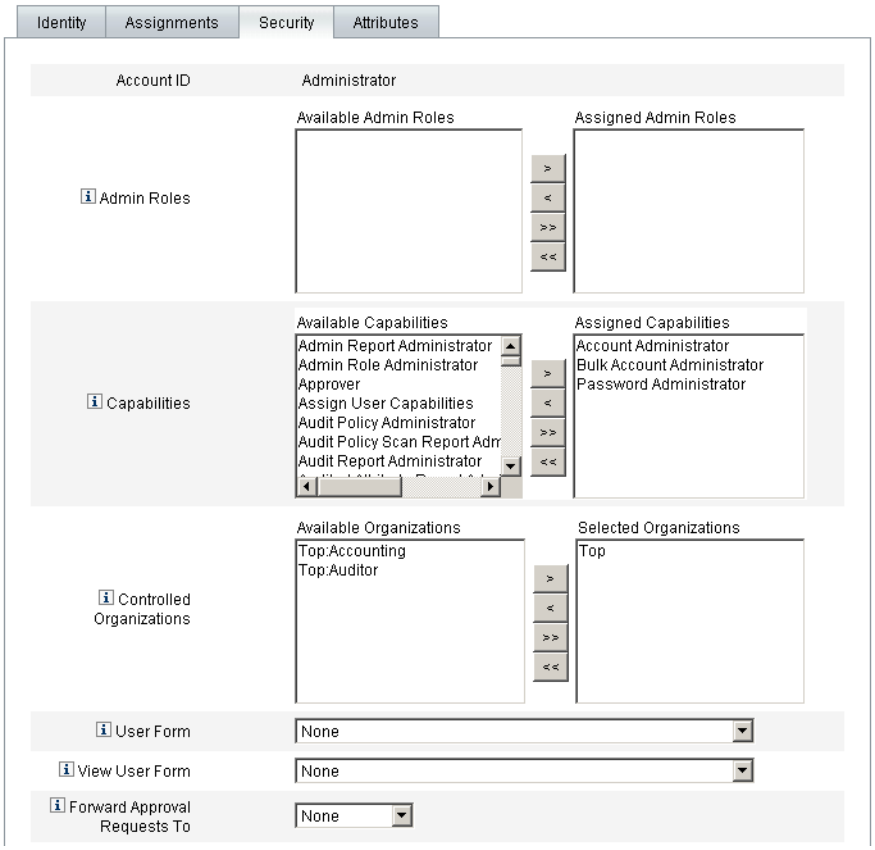


図 4 管理者の作成

管理者ビューのフィルタ

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

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

- **管理者** ー 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。

注 第 5 章「設定」で、割り当て可能な Identity Manager 組み込み機能について説明します。

管理者パスワードの変更

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

管理者は、次の場所から別の管理者のパスワードを変更できます。

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

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

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

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

管理者のアクションの認証

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

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

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

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

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

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

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

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

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

オプションの値として `true` または `false` を指定できます。

認証質問の回答の変更

「パスワード」エリアを使用して、アカウント認証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、**「自分の認証質問の回答の変更」**を選択します。

認証の詳細については、「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いくつかのページおよびエリアでは、accountId ではなく属性 (email や fullname など) に基づいて Identity Manager 管理者を表示することができます。次のものがあります。

- 「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、次のように UserUIconfig に追加します。

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

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して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、Identity Manager オブジェクトに適用される次の 3 つの承認カテゴリをサポートします。

- **組織** — 組織に追加されるユーザーアカウントに承認が必要です。
- **ロール** — ロールに割り当てられるユーザーアカウントに承認が必要です。
- **リソース** — リソースに対するアクセス権を与えられるユーザーアカウントに承認が必要です。

注 Identity Manager では、デジタル署名された承認を設定できます。この機能の詳細については、「設定」の章の「署名付き承認」を参照してください。

承認者のセットアップ

これらの各カテゴリに対する承認者のセットアップはオプションですが、セットアップすることを推奨します。アカウントの作成では、承認者をセットアップするカテゴリごとに、少なくとも 1 つの承認が必要です。1 人の承認者が要求の承認を却下した場合、アカウントは作成されません。

各カテゴリに複数の承認者を割り当てることができます。1 つのカテゴリ内で必要な承認は 1 つのみであるため、複数の承認者をセットアップして、ワークフローが遅延または停止していないかどうかを確認できます。1 人の承認者が利用不可能な場合は、ほかの承認者を利用して要求を処理できます。承認は、アカウント作成にのみ適用されます。デフォルトでは、アカウントの更新と削除に承認は必要ありません。ただし、承認を必要とするように、このプロセスをカスタマイズできます。

Identity Manager は、承認プロセスとアカウント作成要求のステータスをワークフロー図として図示します。Business Process Editor (BPE) を使用すると、承認の流れを変更したり、アカウントの削除を取得したり、更新を取得したりして、ワークフローをカスタマイズすることができます。

BPE、ワークフローの詳細、承認ワークフローの変更を図示した例については、『Identity Manager Workflows, Forms, and Views』を参照してください。

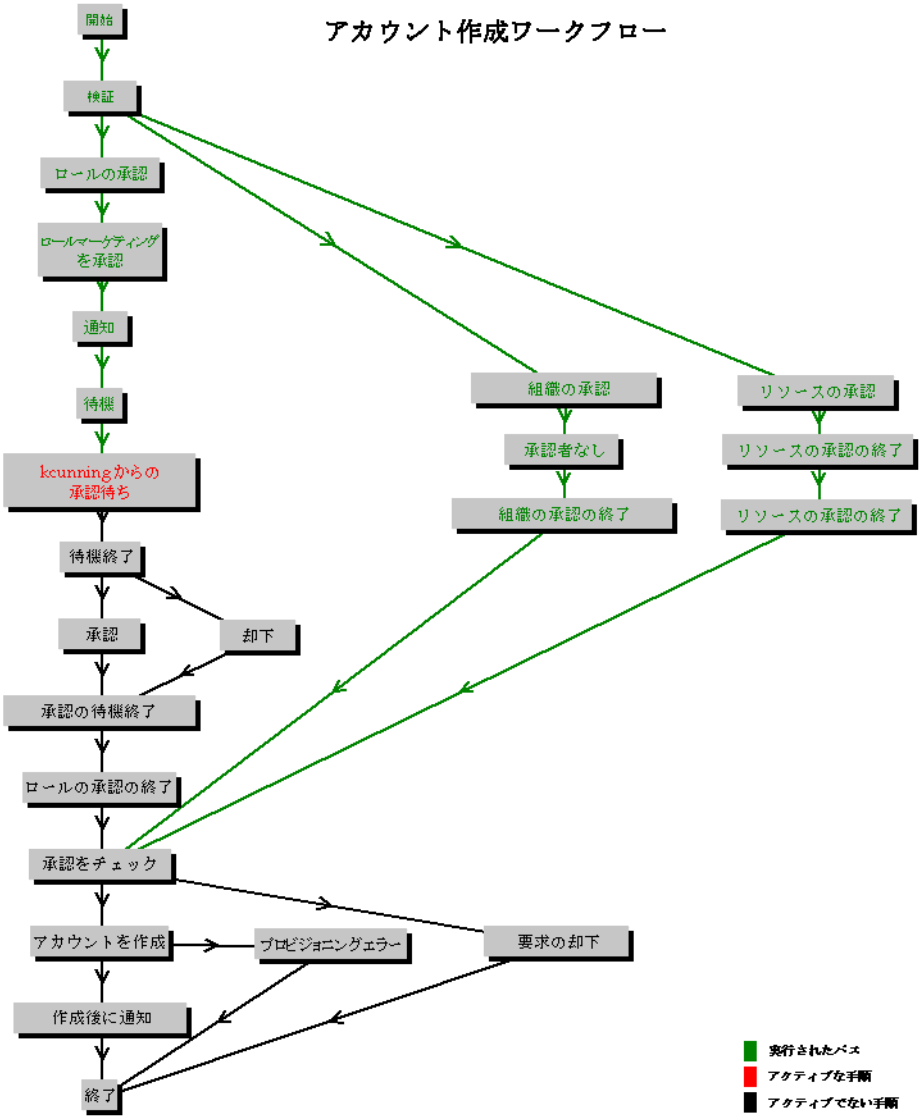


図 5 アカウント作成ワークフロー

承認

5 設定

この章では、管理者インタフェースを使用した Identity Manager オブジェクトのセットアップの説明および手順を示します。

この章では、次について詳細に説明します。

- 次のような Identity Manager オブジェクトを作成および編集する。
  - ロール
  - リソース
  - ChangeLogs
  - ポリシー
  - 機能
  - 管理者ロール
  - 電子メールテンプレート
  - サーバー
- 監査設定グループ (監査イベント) の設定
- Identity Manager と Remedy サーバーを統合する
- デジタル署名付き承認を設定する

ロールについて

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

ロールとは

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

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

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

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

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

ロールの作成

ロールを作成するには、次を実行します。

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

「ロールの作成」ページでは、次のことができます。

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

ヒント 承認プロセスの詳細については、「管理」の章の「承認」を参照してください。

- ロールを除外する。つまり、このロールがユーザーに割り当てられているときに、除外されたロールを割り当てることはできません。
- このロールを割り当て可能にする組織を選択する。
- ロールに割り当てられているリソースの属性値を編集する。

割り当てられているリソース属性値の編集

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

ロールの編集

ロールを変更するには、次を実行します。

1. メニューバーで、**「ロール」**を選択します。
2. 「ロール」リストページで、リスト内のロールをクリックします。

ロールの検索

「ロールの検索」エリアを使用して、ロールを検索します。検索機能により、検索条件に一致したロールのリストが戻されます。

ロールは、以下の 1 つ以上の検索の種類によって検索できます。

- 名前

- 可用性
- 承認者
- リソース
- リソースグループ

注意：

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

ロールを検索するには、**「ロール」**を選択し、**「ロールの検索」**を選択します。

ロールのクローン作成

既存のロールの選択項目を使用して、新しいロールを作成することができます。その場合は、次を実行します。

1. 編集するロールを選択します。
2. 「名前」フィールドに新しい名前を入力して、**「保存」**をクリックします。
   Identity Manager に「作成または名前変更」ページが表示されます。
3. 新しいロールを作成するには、**「作成」**をクリックします。

ロール名の変更

ロール名を変更するには、次を実行します。

1. 編集するロールを選択します。
2. 「名前」フィールドに新しい名前を入力して、**「保存」**をクリックします。
   Identity Manager に「作成または名前変更」ページが表示されます。
3. ロール名を変更するには、**「名前の変更」**をクリックします。

ロールとリソースロールの同期 Identity Manager

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

メニューバーで、**「タスク」**を選択してから**「タスクの実行」**を選択して、「Identity Manager ロールをリソースロールと同期する」タスクページを表示します。

リソースについて

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

リソースとは

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

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

- メインフレームセキュリティーマネージャー
- データベース
- ディレクトリサービス
- オペレーティングシステム
- Enterprise Resource Planning (ERP) システム
- メッセージプラットフォーム

「リソース」エリア

既存のリソースに関する情報は、「リソース」ページに表示されます。Identity Manager

リソースにアクセスするには、メニューバーの**「リソース」**をクリックします。

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

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

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

-  組織
-  組織単位
-  グループ
-  ロール

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

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

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

リソースリストの管理

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

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

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

カスタムリソースを追加するには、次の手順を実行します。

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

次の表は、カスタムリソースのクラスの一覧です。

カスタムリソース	リソースクラス
Access Manager	com.waveset.adapter.AccessManagerResourceAdapter
ACF2	com.waveset.adapter.ACF2ResourceAdapter
ActivCard	com.waveset.adapter.ActivCardResourceAdapter
Active Directory	com.waveset.adapter.ADSIResourceAdapter
Active Directory ActiveSync	com.waveset.adapter.ActiveDirectoryActiveSyncAdapter
ClearTrust	com.waveset.adapter.ClearTrustManagerResourceAdapter
DB2	com.waveset.adapter.DB2ResourceAdapter
INISafe Nexess	com.waveset.adapter.INISafeNexessResourceAdapter
Microsoft SQL Server	com.waveset.adapter.MSSQLServerResourceAdapter
MySQL	com.waveset.adapter.MySQLResourceAdapter
Natural	com.waveset.adapter.NaturalResourceAdapter
NDS SecretStore	com.waveset.adapter.NDSSecretStoreResourceAdapter
Oracle	com.waveset.adapter.OracleResourceAdapter
Oracle Financials	com.waveset.adapter.OracleERPResourceAdapter
OS400	com.waveset.adapter.OS400ResourceAdapter

PeopleSoft	com.waveset.adapter.PeopleSoftCompIntfcAdapter com.waveset.adapter.PeopleSoftComponentActiveSyncAdapter
RACF	com.waveset.adapter.RACFResourceAdapter
SAP	com.waveset.adapter.SAPResourceAdapter
SAP HR	com.waveset.adapter.SAPHRResourceAdapter
SAP Portal	com.waveset.adapter.SAPPortalResourceAdapter
Scripted Host	com.waveset.adapter.ScriptedHostResourceAdapter
SecurID	com.waveset.adapter.SecurIdResourceAdapter com.waveset.adapter.SecurIdUnixResourceAdapter
Siebel	com.waveset.adapter.SiebelResourceAdapter
SiteMinder	com.waveset.adapter.SiteminderAdminResourceAdapter com.waveset.adapter.SiteminderLDAPResourceAdapter com.waveset.adapter.SiteminderExampleTableResourceAdapter
Sun ONE Identity Server	com.waveset.adapter.SunISResourceAdapter
Sybase	com.waveset.adapter.SybaseResourceAdapter
Top Secret	com.waveset.adapter.TopSecretResourceAdapter

リソースの作成

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

リソースウィザードを使用して、次の項目を設定します。

- **「リソース固有のパラメータ」** – これらの値は、このリソースタイプの特定のインスタンスを作成するときに Identity Manager インタフェースから修正できます。
- **「アカウント属性」** – リソースのスキーママップに定義されます。これらによって、Identity Manager ユーザー属性がリソースの属性にどのようにマップされるかが決まります。
- **「アカウントの DN または ID テンプレート」** – ユーザーに対するアカウント名の構文が含まれています。アカウント名の構文は、階層構造の名前空間で特に重要です。
- **「リソースの Identity Manager パラメータ」** – ポリシーをセットアップし、リソースの承認者を設定し、リソースに対する組織のアクセス権をセットアップします。

リソースを作成するには、次を実行します。

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

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

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

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

3. **「次へ」**をクリックして、リソースの定義を開始します。リソースウィザードの手順とページは、次の順序で表示されます。
   - **「リソースパラメータ」** ― 認証とリソースアダプタの動作を管理するためのリソース固有のパラメータをセットアップします。パラメータを入力して**「テスト接続」**をクリックし、接続が有効であることを確認します。確認できたら、**「次へ」**をクリックして、アカウント属性をセットアップします。

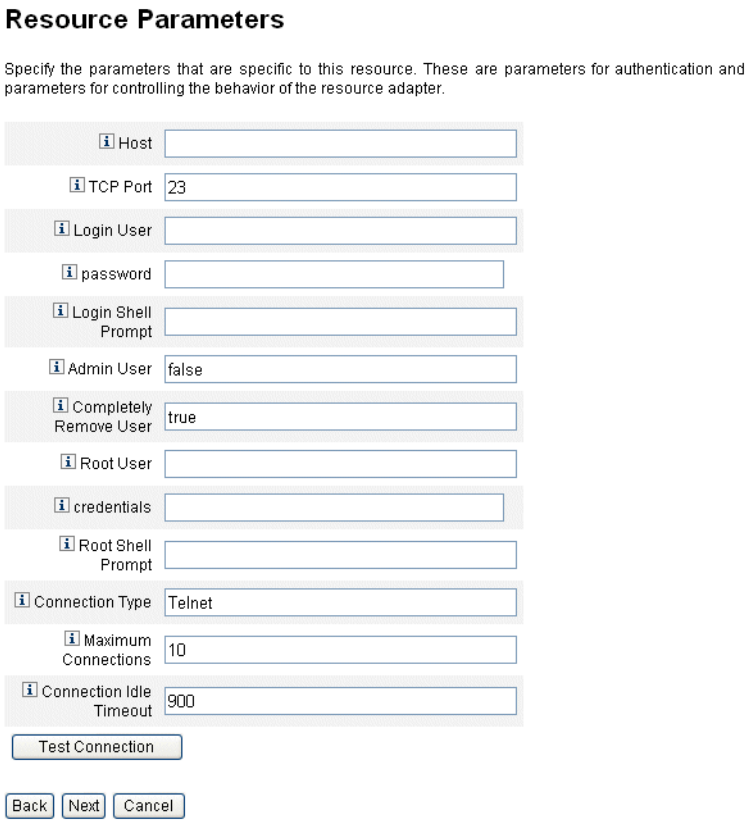


図 1 リソースウィザード : リソースパラメータ

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

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

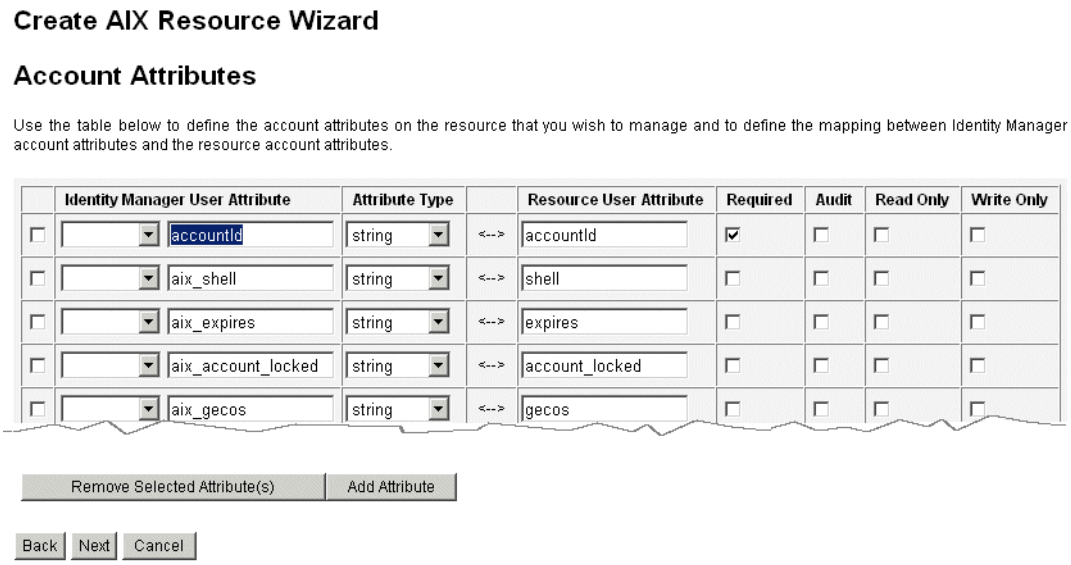


図 2 リソースウィザード : アカウント属性 (スキーママップ)

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

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

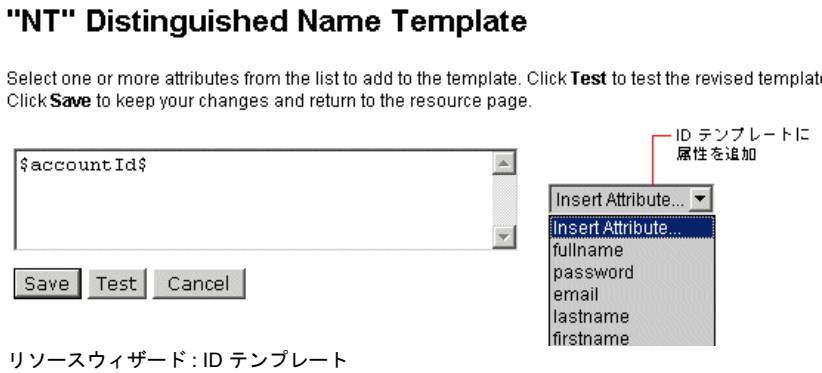


図 3 リソースウィザード : ID テンプレート

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

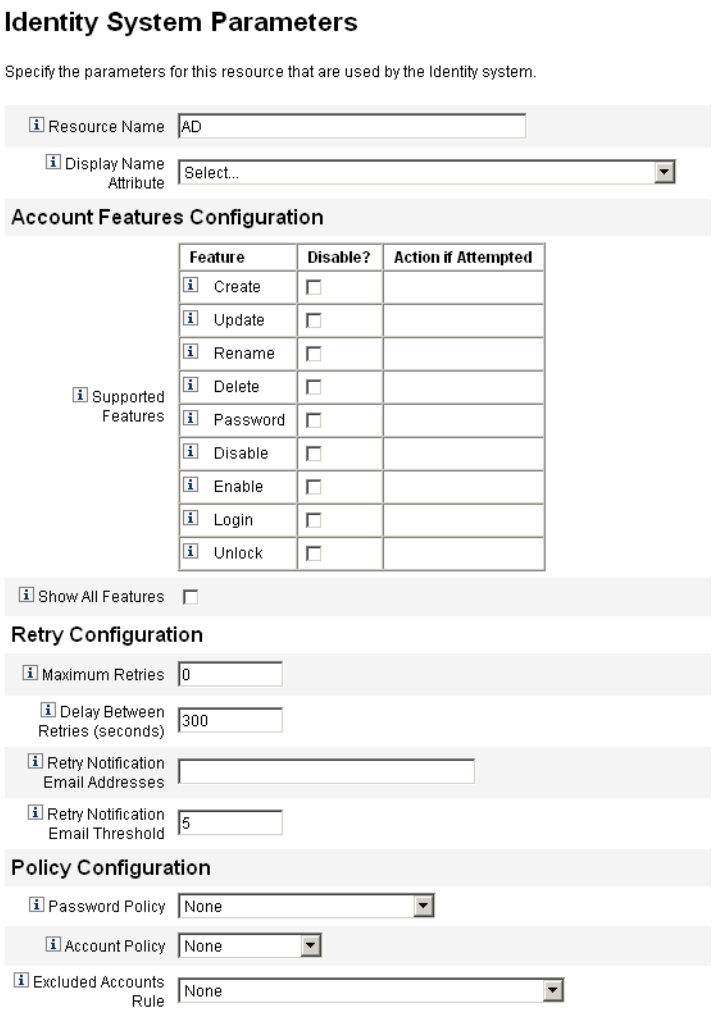


図 4 リソースウィザード : アイデンティティーシステムのパラメータ

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

リソースの管理

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

- **リソースの削除**－ 1 つ以上のリソースを選択して、「リソースアクション」リストから「削除」を選択します。複数のリソースタイプを同時に選択することができます。ロールまたはリソースグループが関連付けられているリソースは削除できません。
- **リソースオブジェクトの検索** － リソースを選択して「リソースオブジェクトアクション」リストから「検索」を選択すると、オブジェクト特性によってリソースオブジェクト (組織、組織単位、グループ、または個人など) を検索できます。
- **リソースオブジェクトの管理** － リソースタイプによっては、新しいオブジェクトを作成できるものがあります。リソースを選択して、「リソースオブジェクトアクション」リストから「リソースオブジェクトの作成」を選択します。
- **リソース名の変更** －リソースを選択して、「リソースアクション」リストから「名前の変更」を選択します。表示される入力ボックスに新しい名前を入力して、**「名前の変更」**をクリックします。
- **リソースのクローン作成**－ リソースを選択して、「リソースアクション」リストから「名前を付けて保存」を選択します。表示される入力ボックスに新しい名前を入力します。クローンとして作成されたリソースが、選択した名前でリソースリストに表示されます。

アカウント属性の操作

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

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

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

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

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

リソースグループ

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

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

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

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

ChangeLog について

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

ChangeLog とは

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

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

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

ChangeLog とセキュリティー

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

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

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

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

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

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

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

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

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

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

ChangeLog 機能の要件

ChangeLog 機能の要件として、ChangeLog を設定する前に ID 属性を設定する必要があります。

ID 属性の設定

次の情報と手順を使用して、ID 属性を設定し、ID 属性が適用されるアイデンティティーシステムアプリケーションを選択してください。

ID 属性の操作

ID 属性を設定するには、**「設定」**を選択して、Identity Manager 管理者インタフェースから**「ID 属性」**を選択します。「ID 属性」ページが表示されます。

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

注　アクションを実行する前に、必ず**「保存」**をクリックしてください。

アプリケーションの選択

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

注　ChangeLog 機能を使用するには、ActiveSync アプリケーションを使用可能にする必要があります。

ID 属性の追加と編集

「ID 属性の追加」または「ID 属性の編集」ページから、次の項目に関して選択して、ID 属性を追加または編集します。

- **「属性名」** – 属性名を選択または入力します。与えられているデフォルト値から (リーススキーママップエントリ、オペレーショナル ID 属性、およびユーザー拡張属性から) 選択するか、またはテキストボックスに値を入力します。

- **「ソース」** ― この ID 属性の値に利用する 1 つ以上のソースを選択します。ソースは順番に評価され、ID 属性は最初の null 以外の値に設定されます。
  - **「リソース」** ― 値は、選択したリソース上の選択済み属性に由来します。
  - **「規則」** ― 値は選択した規則の評価に由来します。
  - **「定数」** ― 値は提供された定数値に設定されます。

  + (プラス記号) をクリックすると、新規行が追加され、別のソースを選択できます。ソースの横にある **-** (マイナス記号) をクリックすると、新規行は削除されます。
- **「属性のプロパティー」** ― このエリアを使用して、ID 属性のプロパティーを設定します。
  - **「ID 属性を優先する」** ― ID 属性の値がすべてのターゲットに対して優先的に設定されます。このオプションを選択すると、ソースによって決められた値はユーザーがフォームに入力したすべての値に優先して適用されます。通常はこのオプションを選択します。
  - **「IDM リポジトリに属性を保存」** ― ID 属性をアイデンティティーシステムリポジトリにローカルに格納することを選択します。このオプションは、アイデンティティーシステムユーザーに ID 属性を保存する権限があるか、または ID 属性がクエリーを処理できるようにする必要がある場合に選択します。
  - **「割り当てられたすべてのリソースに値を設定」** ― ID 属性をサポートするすべての割り当て済みリソースに対して ID 属性をグローバルに設定する場合に、このオプションを選択します。
- **「ターゲット」** ― この ID 属性を設定するターゲットリソースを選択します。ターゲットが何も定義されていない場合は、**「ターゲットの追加」** をクリックします。リストからターゲットを削除するには、ターゲットを選択して、**「選択したターゲットを削除」** をクリックします。

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

ターゲットリソースの追加

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

次の項目の選択を行って、ID 属性を設定するターゲットリソースを追加します。

- **「ターゲットリソース」**－ 選択した ID 属性を設定するターゲットリソースを選択します。
- **「ターゲット属性」**－値を受け取るターゲットリソースの属性の名前を選択します。
- **「条件」**－選択した ID 属性の設定をこのターゲットリソースで行うかどうかを決めるときに実行する規則を選択します。この規則からは true または false の値が戻されるようにします。条件が設定されていない場合、ターゲット属性は常に選択されたイベントタイプに対して設定されます。
- **「適用イベント :」**－ このターゲットリソースで、選択した ID 属性を設定するイベントのタイプを選択します。この選択内容が「条件」と組み合わされて、ターゲット属性を設定するかどうかが判別されます。

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

ターゲットリソースの削除

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

ID 属性のインポート

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

次のインポート項目について選択を行います。

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

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

  「保存」をクリックして、ID 属性の変更を保存します。

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

ChangeLog の設定

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

ChangeLog と ChangeLog ポリシーを設定するには、**「設定」**を選択してから、管理者インタフェースのメニューバーで**「ChangeLog」**を選択します。

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

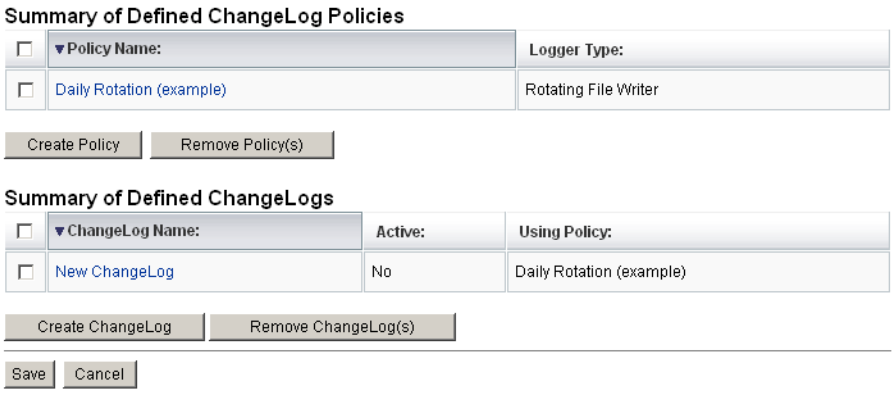


図 5 「ChangeLog 設定」

ChangeLog ポリシーの概要

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

1 つ以上の ChangeLog ポリシーを削除するには、リスト内のポリシーを選択して、「ポリシーの削除」をクリックします (このアクションに確認は不要)。

ChangeLog の概要

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

1 つ以上の ChangeLog を削除するには、リスト内の ChangeLog を選択して、「ChangeLog の削除」をクリックします (このアクションに確認は不要)。

ChangeLog 設定変更の保存

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

ChangeLog ポリシーの作成と編集

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

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

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

  開始時刻を '00:00'、ローテーション回数を 3 にし、ChangeLog を午前 9:24 に起動することにした場合、朝の順番のローテーション名には最近のローテーション開始時刻 (08:00 など) が組み込まれます。この例の場合は、ファイル名が cl_User_yyyyMMdd080000 で始まります。そして、新しいローテーション (ファイル名の新しいプレフィックス) が 16:00 に開始します。
- **「1 日のローテーション数」** – 1 日にログを切り替える回数を指定します。たとえば、4 時間ごとにローテーションを切り替える場合は、6 の値を入力します。

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

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

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

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

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

ChangeLog の作成と編集

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

- **「ChangeLog 名」** ― 一意な ChangeLog の名前を入力します。
- **「アクティブ」** ― このオプションを選択した場合、ChangeLog は監視を行い、ActiveSync リソースを通して ID 属性に変更が伝達されたときに、その変更を記録します (この処理が行われるためには、ActiveSync が ID 属性アプリケーションであることが必要)。
- **「フィルタ」** ― 使用する ChangeLog フィルタの名前を入力します。「Noop」はデフォルトフィルタを使用し、すべての変更を受け入れることを意味します。ほとんどの場合、この設定で十分です。この設定を使用しない場合は、com.sun.idm.changelog.ChangeLogFilter を実装する Java クラスを指定することになります。このクラスはサーバーのクラスパスに配置され、またパブリックなデフォルトコンストラクタが含まれている必要があります。
- **「次の操作をログに記録」** ―作成、更新、および削除など、選択したタイプのイベントのログを記録します。選択されていないイベントは無視されます。

- **「ChangeLog ビュー」** ― このテーブルを使用して、ChangeLog の内容 (列) を定義します。テーブルの各行は ChangeLog の列を指定します。ChangeLog 列を追加するには「列の追加」をクリックします。それぞれの列には、名前、タイプ、ID 属性名があります。行の順序は列の順序を示します。列を定義したあとで列の順序を並び替えるには、「上へ」と「下へ」のボタンを使用します。

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

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

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

例

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

例 : ID 属性の定義

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

Resource 1: EmployeeInfo
employeeNumber*
givenname
mi
surname
phone

Resource2 : OrgInfo
employeeNum*
managerEmpNum
departmentNumber

Resource 3 : PhoneList
empId*
fullname
phone
department

注　　* はレコードを相互に関連付けるキーを表します。

ID 属性は次のようにして定義されます。

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

例 : ChangeLog の設定

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

PhoneList ChangeLog の ChangeLogView

列名	タイプ	ID 属性
empId	テキスト	employee
fullname	テキスト	fullname
phone	テキスト	phoneNumber

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

CSV ファイル形式

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

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

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

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

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

列

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

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

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

行

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

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

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

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

テキスト値

テキスト値は文字列として書き込まれますが、次の 2 つの例外があります。

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

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

バイナリ値

バイナリ値は Base64 でエンコードされます。

複数テキスト値

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

複数バイナリ値

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

出力形式の例

次に例を挙げて、さまざまな出力形式を示します。例の書式は次のとおりです。

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

各例の Column 3 にサンプルテキストが示されます。

- テキスト (T) データは、ファイル内で次のように文字列として表示されます。
  ```
  ADD,account0,some text data,column4
  ```
- バイナリ (B) データは Base64 でエンコードされて表示されます。
  ```
  ADD,account0,FGResWE23WDE==,column4
  ```
- 複数テキスト (MT) は次のように表示されます。
  ```
  ADD,account0,[one,two,three],column4
  ```
- 複数バイナリ (MB) は次のように表示されます。
  ```
  ADD,account0,[FGResWE23WDE==,FGRCAFEBADE3sseGHSD],column4
  ```

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

ChangeLog のファイル名

ファイル名の形式は次のとおりです。

*servername*_User_*timestamp.sequenceNumber.suffix*

各表記の意味は次のとおりです。

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

ローテーションとシーケンスの設定

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

例

あるポリシーが次の条件でローテーションを定義するとします。

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

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

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

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

1 月 1 日は 07:00:00 から始まって 8 時間ごとに 3 回ローテーションされており、1 月 2 日も同様であることが示されています。名前の中で 20060102 という日付に対応する部分だけが異なっています。

ChangeLog スクリプトの作成

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

- スクリプトは、新しいデータや新しいファイルを待ったり、あるいはアクティビティーの合間に休眠しながら、取得したファイルを読み取っては各行の変更内容をバックエンドリソースに適用するというように、継続的に実行されるものです。
- ChangeLog は削除操作をサポートしますが、その場合 accountId 値が DEL 行に書き込まれるだけです。
- ローテーションとシーケンスを使用することにより、スクリプトを実行する頻度を決めることができます。たとえば、次のように指定できます。
  - 午前零時にローテーションし、毎晩前回のローテーションに対してスクリプトを実行する。
  - 午前 8:00 から始めて 4 時間ごとにローテーションし、スクリプトを 4 時間ごとに (8 時、12 時、16 時、20 時、24 時、4 時、...) 実行する。
  - ローテーションはなしにして、シーケンス番号が増えるときにシーケンスファイルを読み取るかたちでスクリプトを実行する。シーケンス番号を増やす基準は、サイズベース、数値演算ベース、時間ベースで制御できます。

- 各 ChangeLog をバックエンドシステム内のレコードの表現と見ることができます。ログを読み取るスクリプトにとって処理しやすくするために、Identity Manager は特定のレコードに関しては、それが変更されているかどうかに関わりなく必ずそのすべてのデータを書き込みます。スクリプトはそのレコードのすべてのデータをそのまま適用します。

  ただし、スクリプトはバックエンドリソース (またはスクリプト) が、特に ADD と DEL に関して、次のいずれかの方法を取れるようにしておく必要があります。

  - べき等な操作を行える。べき等とは、データを複数回適用しても 1 回適用したときと変わらないこと意味します。スクリプトが ChangeLog を最初から最後まで 2 回受け取って読み取る場合、受け取った後のリソース内のデータレコードの状態は 2 回とも厳密に一致しているべきです。
  - 操作を 1 回しか行えない。たとえば、追加および削除アクションに関してリソースをべき等にできない場合、ログエントリを一回だけ読み取るか、そうでなければ進捗を追跡するかして、スクリプトによる変更の適用が必ず一回だけになるようにする必要があります。
- 1 つのシーケンスファイルが作成されたことを確認してから、その前のシーケンスファイルを適用する方法がよいこともあります。.2 ファイルが作成されるまでは .1 ファイルを適用しないようにし、.3 ファイルが表示されたら .2 ファイルを適用するという要領で行います。ファイルを適用したあとは、ディスク上で適用を行なったことを確認します。この方法により、`fstat` や `tail -f` などの呼び出しを使用しないで済みます。

ポリシーについて

この節では、ポリシーの設定の説明および手順を示します。

ポリシーとは

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

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

ポリシーは、以下のよう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」および「ユーザーの作成と編集」ページを使用して組織またはユーザーに割り当てます。

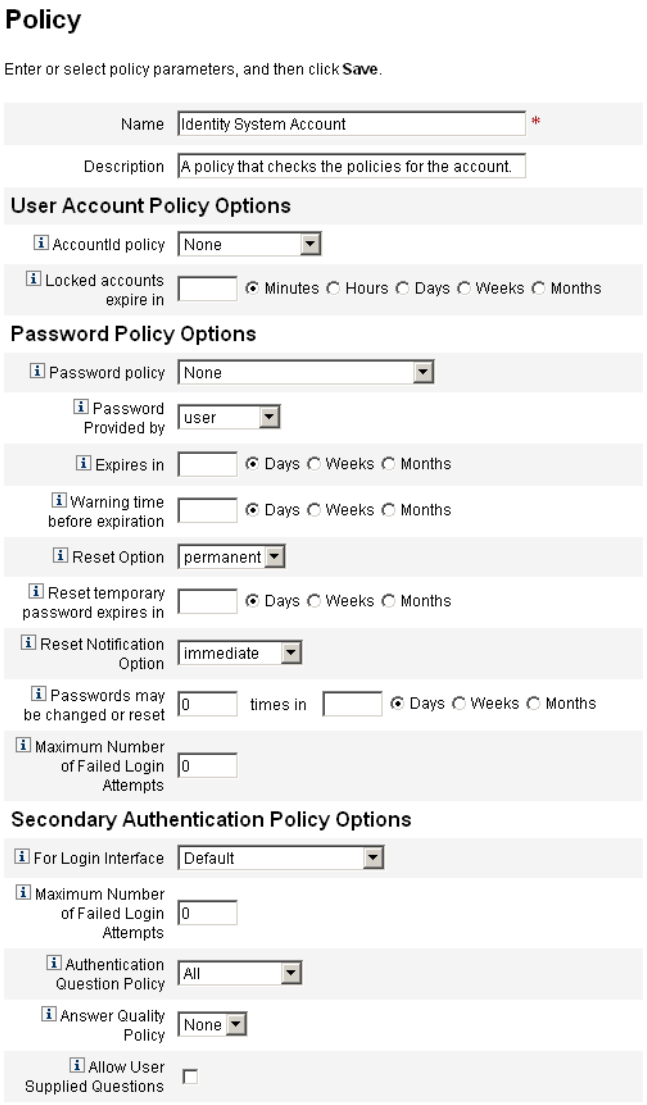


図 6 Identity Manager ポリシー

設定または選択できるオプションは、次のとおりです。

- **ユーザーポリシーオプション** – ユーザーが認証質問に正しく回答できない場合に、Identity Manager がユーザーアカウントをどのように処理するかを指定します。
- **パスワードポリシーオプション** – パスワードの有効期限、期限切れ前の警告時間、およびリセットオプションを設定します。
- **認証ポリシーオプション** – 認証質問をユーザーにどのように表示するか、またユーザーが独自の認証質問を設定できるかを決定し、ユーザーに表示できる質問 (最大 10 個) の貯蔵場所を設定します。

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

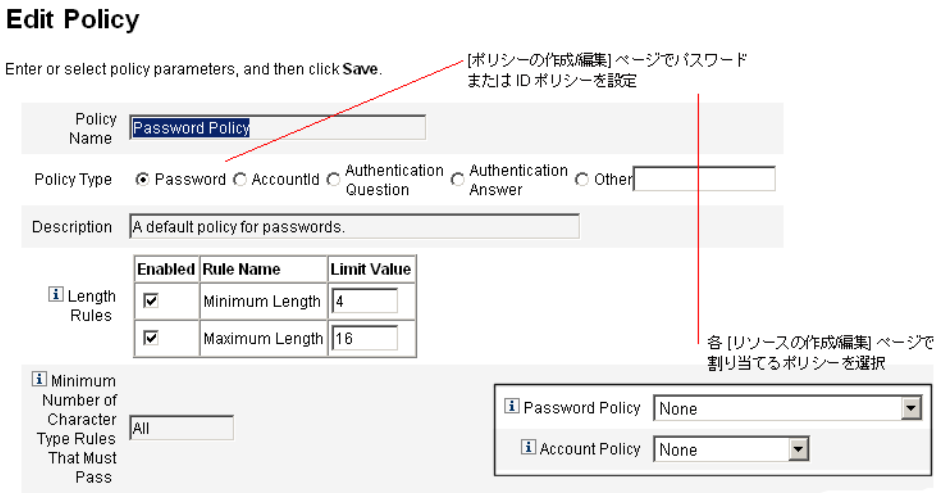


図 7 パスワードポリシーの作成 / 編集

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

- **長さ規則** – 最大長および最小長を決定します。
- **文字タイプ規則** – 英字、数字、大文字、小文字、繰り返し、および連続文字に使用可能な最小値と最大値を設定します。
- **パスワードの再利用の制限** – 現在のパスワードより前に使用されていたパスワードのうち、再利用できないようにするパスワードの数を指定します。ユーザーがパスワードを変更しようとすると、新規パスワードがパスワードの履歴と比較され、一意のパスワードであることが確認されます。セキュリティーを確保する目的で以前のパスワードのデジタル署名が保存され、新規パスワードと比較されます。

- **禁止される単語および属性値** – ID またはパスワードとして使用できない単語および属性を指定します。

辞書ポリシー

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

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

辞書ポリシーの設定

辞書ポリシーを設定するには、次を実行する必要があります。

- 辞書サーバーサポートの設定
- 辞書の読み込み

次の手順を実行します。

1. メニューバーの**「設定」**を選択してから、**「ポリシー」**を選択します。
2. **「辞書の設定」**をクリックすると、「辞書の設定」ページが表示されます。
3. データベース情報を選択および入力します。
   - **「データベースタイプ」** – 辞書の保存に使用するデータベースタイプ (Oracle、DB2、SQLServer、または MySQL) を選択します。
   - **「ホスト」** – データベースが実行されているホストの名前を入力します。
   - **「ユーザー」** – データベースに接続するときに使用するユーザー名を入力します。
   - **「パスワード」** – データベースに接続するときに使用するパスワードを入力します。
   - **「ポート」** – データベースがリスニング中のポートを入力します。
   - **「接続 URL」** – 接続のときに使用する URL を入力します。次のテンプレート変数を使用することができます。
     - %h - ホスト
     - %p - ポート
     - %d - データベース名
   - **「ドライバクラス」** – データベースを操作する際に使用する JDBC ドライバクラスを入力します。
   - **「データベース名」** – 辞書の読み込み先のデータベースの名前を入力します。

- **「辞書ファイル名」** ― 辞書を読み込むときに使用するファイルの名前を入力します。

4. データベース接続をテストするには、**「テスト」**をクリックします。
5. 接続テストが成功したら、**「単語の読み込み」**をクリックして、辞書を読み込みます。

注　読み込み作業が完了するまでに、数分かかる場合があります。

6. その辞書が正しく読み込まれたかどうかを確認するには、**「テスト」**をクリックします。

辞書ポリシーの実装

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

機能について

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

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

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

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

機能のカテゴリ

Identity Manager の機能は、次のように分類されています。

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

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

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

機能の操作

1. メニューバーで、**「設定」**を選択します。
2. **「機能」**を選択すると、Identity Manager 機能のリストが表示されます。

機能の作成

機能を作成するには、**「新規」**をクリックします。

機能の編集

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

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

機能の保存と名前の変更

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

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

コピー元の機能は保護されていますが、新しい機能は編集できます。

機能の割り当て

「ユーザーの作成」および「ユーザーの編集」ページから、ユーザーに機能を割り当てます。

注　「セキュリティー」エリアでセットアップした管理者ロールを割り当てる方法で、ユーザーに機能を割り当てることもできます。詳細は、「管理者ロールについて」を参照してください。

機能の階層

タスクベースの機能は、次のような実用上の機能階層に分類されます。

Account Administrator

- 承認者
- ユーザーへの機能の割り当て
- ユーザーアカウント管理者
  - ユーザーの作成
  - ユーザーの削除
    - › IDM ユーザーの削除
    - › ユーザーのプロビジョン解除
    - › ユーザーの割り当て解除
    - › ユーザーのリンク解除
  - ユーザーの無効化
  - ユーザーの有効化
  - パスワード管理者
    - › パスワード変更管理者
    - › パスワードリセット管理者
  - ユーザーの名前変更
  - ユーザーのロック解除
  - ユーザーの更新
  - ユーザーの表示
  - ユーザーのインポート

Admin Role Administrator

- 機能の接続
- 機能規則の接続
- 管理する組織規則の接続
- 組織の接続

Bulk Account Administrator

- 承認者
- ユーザーへの機能の割り当て
- ユーザーアカウントの一括管理者
  - ユーザーの一括作成
  - ユーザーの一括削除
    - IDM ユーザーの一括削除
    - ユーザーの一括プロビジョン解除
    - ユーザーの一括割り当て解除
    - ユーザーの一括リンク解除
  - ユーザーの一括無効化
  - ユーザーの一括有効化
  - パスワード管理者
  - ユーザーの名前変更
  - ユーザーのロック解除
  - ユーザーの表示
  - ユーザーのインポート

Bulk Change Account Administrator

- 承認者
- ユーザーへの機能の割り当て
- ユーザーアカウントの一括変更を行う管理者
  - ユーザーの一括無効化
  - ユーザーの一括有効化
  - ユーザーの一括更新
  - パスワード管理者
  - ユーザーの名前変更
  - ユーザーのロック解除
  - ユーザーの表示

Capability Administrator

Change Account Administrator

- 承認者
- ユーザーへの機能の割り当て
- ユーザーアカウント変更管理者
  - ユーザーの無効化
  - ユーザーの有効化
  - パスワード管理者

    - パスワード変更管理者
    - パスワードリセット管理者
  - ユーザーの名前変更
  - ユーザーのロック解除
  - ユーザーの更新
  - ユーザーの表示

Import/Export Administrator

Login Administrator

Organization Administrator

Password Administrator (Verification Required)

- パスワード変更管理者 (検証が必要)
- パスワードリセット管理者 (検証が必要)

Policy Administrator

Reconcile Administrator

- 調整要求管理者

Remedy Integration Administrator

Report Administrator

- 管理者レポート管理者
  - 管理者レポートの実行
- 監査レポート管理者
  - 監査レポートの実行
- 監査の設定
- 調整レポート管理者
  - 調整レポートの実行
- リソースレポート管理者
  - リソースレポートの実行
- リスク分析管理者
  - リスク分析の実行
- ロールレポート管理者
  - ロールレポートの実行
- タスクレポート管理者
  - タスクレポートの実行
- ユーザーレポート管理者

- ユーザーレポートの実行

Resource Administrator

- リソースグループ管理者
- リソース Active Sync 管理者の変更
- リソース Active Sync 管理者の管理

Resource Object Administrator

Resource Password Administrator

- リソースパスワード変更管理者
- リソースパスワードリセット管理者

Role Administrator

Security Administrator

View Organizations

- 組織のリスト

View Resources

- リソースのリスト

Waveset Administrator

機能の定義

次の表で、各タスクベースの機能と、各機能でアクセスできるタブおよびサブタブについて説明します。

すべての機能で、ユーザーまたは管理者は、**「自分のパスワードの変更」**および**「自分の認証質問の回答の変更」**サブタブ (**「パスワード」**タブ) にアクセスすることができます。

機能	**管理者 / ユーザーに許可する操作**	アクセス可能なタブとサブタブ
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 (一括操作を除く)。	**「アカウント」**- **「アカウントのリスト」**、**「ユーザーの検索」**、**「ファイルへ抽出」**、**「ファイルから読み込み」**、**「リソースから読み込み」**サブタブ **「パスワード」**- すべてのサブタブ **「承認」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Admin Report Administrator	管理者レポートの作成、編集、削除、および実行	**「レポート」**- **「レポートの管理」**、**「レポートの実行」**サブタブ (管理者レポートのみ)
Admin Role Administrator	管理者ロールの作成、編集、および削除	**「設定」**- **「管理者ロール」**サブタブ
Approver	ほかのユーザーにより発行された要求の承認または却下	**「承認」**- すべてのサブタブ
Assign User Capabilities	ユーザー機能の割り当ての変更 (割り当て、割り当て解除)	**「アカウント」**- **「アカウントのリスト」**(編集のみ)、**「ユーザーの検索」**サブタブ。 別のユーザー管理者機能 (「ユーザーの作成」、「ユーザーの有効化」など) に割り当てる必要があります。
Audit Report Administrator	監査レポートの作成、編集、削除、および実行	**「レポート」**- 監査レポートのみ
Bulk Account Administrator	機能の割り当てなど、ユーザーに対する通常操作および一括操作の実行	**「アカウント」**- すべてのサブタブ **「パスワード」**- すべてのサブタブ **「承認」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Bulk Change Account Administrator	機能の割り当てなど、既存のユーザーに対する、既存のユーザーの削除以外の通常操作および一括操作の実行	**「アカウント」**- **「アカウントのリスト」**、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ。ユーザーを作成または削除することはできません。 **「パスワード」**- すべてのサブタブ **「承認」**- すべてのサブタブ **「タスク」**- すべてのサブタブ

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	**「アカウント」**- **「アカウントのリスト」**、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ。機能の作成と削除、およびユーザーへの機能の割り当てを行うことはできません。 **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Bulk Create User	リソースの割り当てとユーザー作成要求の発行 (個別のユーザーに対する操作または一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(作成のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk Delete User	Identity Manager ユーザーアカウントの削除、リソースアカウントのプロビジョン解除、割り当て解除、およびリンク解除 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(作成のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk Delete IDM User	既存の Identity Manager ユーザーアカウントの削除 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(削除のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk Deprovision User	既存のリソースアカウントの削除およびリンク解除 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(プロビジョン解除のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk Disable User	既存のユーザーとリソースアカウントの無効化 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(無効化のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk Enable User	既存のユーザーとリソースアカウントの有効化 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(有効化のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk Unassign User	既存のリソースアカウントの割り当て解除およびリンク解除 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(割り当て解除のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ

Bulk Unlink User	既存のリソースアカウントのリンク解除 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(リンク解除のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk Update User	既存のユーザーとリソースアカウントの更新 (個別のユーザーに対する操作および一括操作を使用した操作)	**「アカウント」**- **「アカウントのリスト」**(更新のみ)、**「ユーザーの検索」**、**「一括操作の起動」**サブタブ **「タスク」**- すべてのサブタブ
Bulk User Account Administrator	ユーザーに対するすべての通常操作および一括操作の実行	**「アカウント」**- すべてのサブタブ **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Capability Administrator	機能の作成、修正、および削除	**「設定」**- **「機能」**サブタブ
Change Account Administrator	機能の割り当てなど、既存のユーザーに対する、削除以外のすべての操作の実行 (一括操作を除く)。	**「アカウント」**- すべてのサブタブ。ユーザーを削除することはできません。 **「パスワード」**- すべてのサブタブ **「承認」**- すべてのサブタブ **「タスク」**- すべてのサブタブ **「レポート」**- 管理レポートおよびユーザーレポートの作成、管理レポートの実行と編集、および範囲内の監査ログレポートを実行します。範囲外の組織の管理レポートおよびユーザーレポートを実行することはできません。
Change Active Sync Resource Administrator	Active Sync リソースパラメータの変更	**「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ **「リソース」**- Active Sync リソース : 「編集」操作メニュー、「Active Sync パラメータの編集」
Change Password Administrator	ユーザーおよびリソースアカウントパスワードの変更	**「アカウント」- 「アカウントのリスト」**、**「ユーザーの検索」**サブタブ (パスワードの変更のみ) **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (**「タスクの実行」**サブタブから)

Change Password Administrator (Verification Required)	ユーザーの認証質問の回答が正しく検証されたあとの、ユーザーおよびリソースアカウントパスワードの変更	**「アカウント」- 「アカウントのリスト」、「ユーザーの検索」**サブタブ (パスワードの変更のみ、操作の前に検証が必要) **「パスワード」** - すべてのサブタブ **「タスク」** - すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (**「タスクの実行」**サブタブから)
Change Resource Password Administrator	リソース管理者のアカウントパスワードの変更	**「タスク」** - すべてのサブタブ **「リソース」- 「リソースのリスト」**サブタブ リソースパスワードの変更のみ (操作メニューの**「接続の管理」-->「パスワードの変更」**から)
Change User Account Administrator	既存のユーザーに対する、削除以外のすべての操作の実行 (一括操作を除く)。	**「アカウント」** - **「アカウントのリスト」、「ユーザーの検索」**サブタブ。機能の作成と削除、およびユーザーへの機能の割り当てを行うことはできません。 **「パスワード」** - すべてのサブタブ **「タスク」** - すべてのサブタブ
Configure Audit	システム内で監査されるアクティビティーの設定	**「設定」** - **「イベント監査」**サブタブ
Control Active Sync Resource Administrator	Active Sync リソースの状態 (開始、停止、更新など) の管理	**「タスク」** - **「タスクの検索」、「すべてのタスク」、「タスクの実行」**サブタブ **「リソース」** - Active Sync リソース : 「Active Sync」操作メニュー (すべての選択肢)
Create User	リソースの割り当てとユーザー作成要求の発行 (一括操作を除く)。	**「アカウント」** - **「アカウントのリスト」**(作成のみ)、**「ユーザーの検索」**サブタブ **「タスク」** - すべてのサブタブ
Delete User	Identity Manager ユーザーアカウントの削除、リソースアカウントのプロビジョン解除、割り当て解除、およびリンク解除 (一括操作を除く)。	**「アカウント」** - **「アカウントのリスト」**(削除のみ)、**「ユーザーの検索」**サブタブ **「タスク」** - すべてのサブタブ
Delete IDM User	Identity Manager ユーザーアカウントの削除 (一括操作を除く)。	**「アカウント」** - **「アカウントのリスト」**(削除のみ)、**「ユーザーの検索」**サブタブ **「タスク」** - すべてのサブタブ

Deprovision User	既存のリソースアカウントの削除およびリンク解除 (一括操作を除く)。	**「アカウント」**- **「アカウントのリスト」**(プロビジョン解除のみ)、**「ユーザーの検索」**サブタブ **「タスク」**- すべてのサブタブ
Disable User	既存のユーザーとリソースアカウントの無効化 (一括操作を除く)。	**「アカウント」**- **「アカウントのリスト」**(無効化のみ)、**「ユーザーの検索」**サブタブ **「タスク」**- すべてのサブタブ
Enable User	既存のユーザーとリソースアカウントの有効化 (一括操作を除く)。	**「アカウント」**- **「アカウントのリスト」**(有効化のみ)、**「ユーザーの検索」**サブタブ **「タスク」**- すべてのサブタブ
Import User	定義済みリソースからのユーザーのインポート	**「アカウント」**- **「ファイルへ抽出」**、**「ファイルから読み込み」**、**「リソースから読み込み」**サブタブ
Import/Export Administrator	全タイプのオブジェクトのインポートとエクスポート	**「設定」**- **「交換ファイルのインポート」**サブタブ
License Administrator	アイデンティティーシステム製品ライセンスの設定	`lh license` コマンドアクセスを提供します (この機能には「管理者インタフェース」タブはない)。
Login Administrator	所定のログインインタフェースに対するログインモジュールセットの編集	**「設定」**- **「ログイン」**サブタブ
Organization Administrator	組織の作成、編集、および削除	**「アカウント」**- **「アカウントのリスト」**サブタブ (組織およびディレクトリジャンクションの編集と作成、組織の削除のみ)
Password Administrator	ユーザーおよびリソースアカウントパスワードの変更とリセット	**「アカウント」**- **「アカウントのリスト」**(パスワードのリスト、変更、およびリセットのみ)、**「ユーザーの検索」**サブタブ **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ
Password Administrator (Verification Required)	ユーザーの認証質問の回答が正しく検証されたあとの、ユーザーおよびリソースアカウントパスワードの変更とリセット	**「アカウント」**- **「アカウントのリスト」**(パスワードのリスト、変更、およびリセットのみ、操作が成功するためには検証が必要)、**「ユーザーの検索」**サブタブ **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ

Policy Administrator	ポリシーの作成、編集、および削除	**「設定」**- **「ポリシー」**サブタブ
Reconcile Administrator	調整ポリシーの編集と調整タスクの管理	**「タスク」**- すべてのサブタブ (調整タスクの表示) **「リソース」**- **「リソースのリスト」**サブタブ
Reconcile Report Administrator	調整レポートの作成、編集、削除、および実行	**「レポート」**- **「レポートの実行」**(アカウントインデックスレポートのみ)、**「レポートの管理」**サブタブ
Reconcile Request Administrator	調整要求の管理	**「タスク」**- すべてのサブタブ **「リソース」**- **「リソースのリスト」**サブタブ (リストおよび調整機能のみ)
Remedy Integration Administrator	Remedy との統合の設定の修正	**「タスク」**- すべてのサブタブ (タスクの表示、ロールの同期の実行) **「設定」**- **「Remedy との統合」**サブタブ
Rename User	既存のユーザーアカウントとリソースアカウントの名前の変更	**「アカウント」**-「アカウントのリスト」サブタブ (範囲内のすべてのアカウントのリスト、ユーザーの名前変更)
Report Administrator	監査の設定と全タイプのレポートの実行	**「タスク」**- すべてのサブタブ (タスクの表示、ロールの同期の実行) **「レポート」**- すべてのサブタブ
Reset Password Administrator	ユーザーおよびリソースアカウントパスワードのリセット	**「アカウント」- 「アカウントのリスト」**、**「ユーザーの検索」**サブタブ (パスワードのリセットのみ) **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (**「タスクの実行」**サブタブから)

Reset Password Administrator (Verification Required)	ユーザーの認証質問の回答が正しく検証されたあとの、ユーザーおよびリソースアカウントパスワードのリセット	**「アカウント」**- **「アカウントのリスト」**、**「ユーザーの検索」**サブタブ (パスワードのリセットのみ、操作が成功するためには検証が必要) **「パスワード」**- すべてのサブタブ **「タスク」**- すべてのサブタブ。「期限切れパスワードのスキャン」タスクのみ (**「タスクの実行」**サブタブから)
Reset Resource Password Administrator	リソース管理者のアカウントパスワードのリセット	**「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ **「リソース」**- **「リソースのリスト」**サブタブ リソースパスワードのリセットのみ (アクションメニューの **「接続の管理」** **--> 「パスワードのリセット」**から)
Resource Administrator	リソースの作成、修正、および削除	**「レポート」**- リソースユーザーレポート、リソースグループレポートは範囲外のリソースに関するエラーを返します。 **「リソース」**- **「リソースのリスト」**サブタブ (グローバルポリシーの編集、パラメータの編集、リソースグループ。接続またはリソースオブジェクトを管理することはできない)。
Resource Group Administrator	リソースグループの作成、編集、および削除	**「リソース」**- **「リソースグループのリスト」**サブタブ
Resource Object Administrator	リソースオブジェクトの作成、修正、および削除	**「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ (リソースオブジェクトを含むタスクの表示)。 **「リソース」**- **「リソースのリスト」**サブタブ (リソースオブジェクトのリストおよび管理のみ)
Resource Password Administrator	リソースプロキシアカウントパスワードの変更とリセット	**「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ **「リソース」**- **「リソースのリスト」**サブタブ リソースパスワードの変更のみ (操作メニューの **「接続の管理」--> 「パスワードの変更」**から)

Resource Report Administrator	リソースレポートの作成、編集、削除、および実行	**「レポート」**- すべてのサブタブ (リソースレポートのみ)
Risk Analysis Administrator	リスク分析の作成、編集、削除、および実行	**「リスク分析」**- すべてのサブタブ
Role Administrator	ロールの作成、修正、および削除	**「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ (ロールの同期) **「ロール」**- すべてのサブタブ
Role Report Administrator	リソースレポートの作成、編集、削除、および実行	**「レポート」**- ロールレポートのみ
Run Admin Report	管理者レポートの実行	**「レポート」**- 管理レポートのみ
Run Audit Report	監査レポートの実行	**「レポート」**- 監査ログレポートおよび使用状況レポートのみ
Run Reconcile Report	調整レポートの実行	**「レポート」**- 監査ログレポートおよび使用状況レポートのみ
Run Resource Report	リソースレポートの実行	**「レポート」**- 監査ログレポートおよび使用状況レポートのみ
Run Risk Analysis	リスク分析の実行	
Run Role Report	ロールレポートの実行	**「レポート」**- ロールレポートのみ
Run Task Report	タスクレポートの実行	**「レポート」**- タスクレポートのみ
Run User Report	ユーザーレポートの実行	**「レポート」**- ユーザーレポートのみ
Security Administrator	暗号化鍵、ログイン設定、およびポリシーの管理などの機能を持つユーザーの作成	**「アカウント」**- **「アカウントのリスト」**(パスワードの削除、作成、更新、編集、および変更)、**「ユーザーの検索」**サブタブ (監査レポート) **「パスワード」**- すべてのサブタブ **「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ **「レポート」**- すべてのサブタブ **「リソース」**- **「リソースのリスト」**サブタブ (リソースオブジェクトのリストおよび管理) **「設定」**- **「ポリシー」**、**「ログイン」**サブタブ
Task Report Administrator	タスクレポートの作成、編集、削除、および実行	**「レポート」**- タスクレポートの作成および管理

Unassign User	既存のリソースアカウントの割り当て解除およびリンク解除 (一括操作を除く)。	**「アカウント」**- **「アカウントのリスト」**(割り当て解除のみ)、**「ユーザーの検索」**サブタブ **「タスク」**- すべてのサブタブ
Unlink User	既存のリソースアカウントのリンク解除 (一括操作を除く)。	**「アカウント」**- **「アカウントのリスト」**(リンク解除のみ)、**「ユーザーの検索」**サブタブ **「タスク」**- すべてのサブタブ
Unlock User	ロック解除をサポートする既存のユーザーリソースアカウントのロック解除 (一括操作を除く)。	**「アカウント」**- **「アカウントのリスト」**(ロック解除のみ)、**「ユーザーの検索」**サブタブ **「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ
Update User	既存のユーザーの編集と、ユーザー更新要求の発行	**「アカウント」**- ユーザーの編集および更新 **「タスク」**- 既存のタスクの管理 (**「すべてのタスク」**サブタブから)
User Account Administrator	ユーザーに対するすべての操作	**「アカウント」**- **「アカウントのリスト」**、**「ユーザーの検索」**、**「ファイルへ抽出」**、**「ファイルから読み込み」**、**「リソースから読み込み」**サブタブ ユーザー機能を割り当てることはできません (**「アカウントのリスト」**サブタブの**「セキュリティー」**フォームタブから)。 **「タスク」**- **「タスクの検索」**、**「すべてのタスク」**、**「タスクの実行」**サブタブ

User Report Administrator	ユーザーレポートの作成、編集、削除、および実行	**「レポート」** - ユーザーレポートの実行
View User	個別のユーザーの詳細の表示	**「アカウント」** - リストからユーザーを選択して、個別のユーザーアカウント情報を表示します。変更操作は許可されません。
Waveset Administrator	システム設定オブジェクトの修正など、システム全体にわたるタスクの実行	**「タスク」** - すべてのサブタブ。ロールの同期、ソースアダプタテンプレートの編集、およびレポートのスケジュール **「レポート」** - すべてのサブタブ **「リソース」** - 「リソースのリスト」(リストのみ、変更操作は許可されない) **「設定」** - **「イベント監査」**、**「電子メールテンプレート」**、**「フォームおよびプロセスマッピング」** サブタブ

表 1 Identity Manager 機能の説明

管理者ロールについて

管理者ロールを使用すると、管理者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の組み合わせを割り当てることができます。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。

機能および組織を管理者ロールに割り当てるときには、次の方法を利用できます。

- **直接** ー 特定の機能または管理する組織、あるいはその両方を管理者ロールに割り当てることができます。
- **動的** (間接) ー 機能および管理する組織の規則を使用して、機能および管理する組織が動的に決定されます。管理者ロールが割り当てられているユーザーが Identity Manager にログインすると、その管理者ロールに基づいて機能および管理する組織が割り当てられます。

注 これらの規則の設定方法については、「機能規則と管理する組織規則」を参照してください。

1 つ以上の管理者ロールを各ユーザーに割り当てることができます。管理者ロールは、1 人以上のユーザーに割り当てることができます。

ユーザー管理者ロール

Identity Manager には「User」という組み込み管理者ロールがあります。このロールにはデフォルトでは機能や管理する組織の割り当ては含まれておらず、このロールを削除することもできません。この管理者ロールは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。

「User」管理者ロールは、管理者インタフェースで**「設定」**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。

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

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

例

次の例の手順は、「User」管理者ロールを動的な環境で使用する方法を示しています。

1. 次の 2 つの Active Directory の ou を作成します。
   - "Chicago Cubs" && "New York Yankees"
2. それぞれの ou に 3 つの Active Directory ユーザーを、次の属性セットを指定して作成します。
   - Chicago Cubs:
     - Dusty Baker (title = 'manager', manager = '')
     - Kerry Woods (title = 'pitcher', manager = 'Dusty Baker')
     - Mark Prior (title = 'pitcher', manager = 'Dusty Baker')
   - New York Yankees
     - Joe Torre (title = 'manager', manager = '')
     - Alex Rodriguiz (title = '3rd', manager = 'Joe Torre')
     - Derek Jeter (title = 'shortstop', manager = 'Joe Torre')

3. 「User」管理者ロールに次の規則を割り当てます。
   - capabilitesRule ==> If Team Manager Assign Account Admin Capability
   - controlledOrganizationsRule ==> If Team Manager Assign Control of My Team
4. "My Team" という名前の Identity Manager 組織を作成して、次の規則を割り当てます。
   - userMembersRule ==> Get My Team

ユーザーがログインすると、次のような処理が行われます。

- ユーザーの Active Directory ユーザータイトルが 'manager' (監督) である場合には、「Account Administrator」機能が割り当てられて、"My Team" 組織の管理を担当することになります。
- ユーザーの Active Directory ユーザータイトルが 'manager' でない場合には、機能も管理する組織も割り当てられません。
- ログインユーザーのタイトルが 'manager' である場合、"My Team" 組織をオープンすると、"Get My Team" 規則が Active Directory リソースに対して getResourceObjects を呼び出して、manager が現在ログインしているユーザーの accountInfo.accounts[AD].accountId になっているすべてのユーザーが要求されます。

このようにセットアップすることで、ユーザーインタフェースにログインする監督が人材 (選手) を管理できるようになり、選手はユーザーインタフェースにログインするときに管理者機能を実行する必要がありません。

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、管理者ロールの管理者機能が必要です。管理者ロールエリアにアクセスするには、**「設定」**をクリックしてから**「管理者ロール」**をクリックします。「管理者ロール」リストページでは、Identity Manager の管理者ロールを作成、編集、および削除できます。

既存の管理者ロールを編集するには、リスト内の名前をクリックします。管理者ロールを作成するには、**「新規」**をクリックします。Identity Manager の「管理者ロールの作成」ページが表示され、新しい管理者ロールの機能および範囲を指定します。

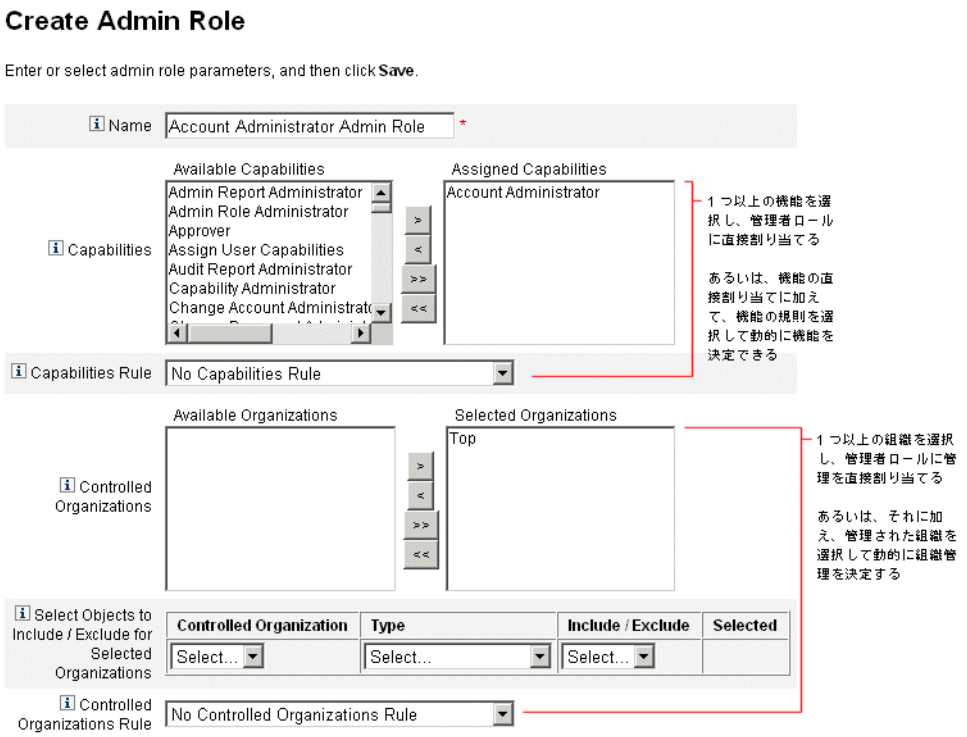


図 8 管理者ロール : ページの作成

管理する組織の範囲の設定

管理する組織を管理者ロールに直接割り当てられるときに、管理者ロールごとにユーザーが操作できるオブジェクトの範囲を定義することができます。そのユーザーが管理している各組織で利用できるオブジェクトのうち、1 つ以上のオブジェクトを範囲に含めたり除外したりすることができます。

たとえば、組織に多数のリソースが含まれる場合に、組織内のユーザーを作成、更新、および削除する機能を持つユーザーについて、指定した一部のリソースにしかアクセスできないようにすることができます。この設定を適用するには、次の特性を持つ管理者ロールを作成します。

- 名前 ― NT ユーザーの管理者
- 機能 ― ユーザーの作成、ユーザーの更新、ユーザーの削除
- 管理する組織 ― *OrganizationName*
- 範囲に含めるリソース ― NT

範囲を設定するために、「管理者ロールの作成」ページの「選択された組織に含めるまたは除外する」エリアで以下の選択を行います。

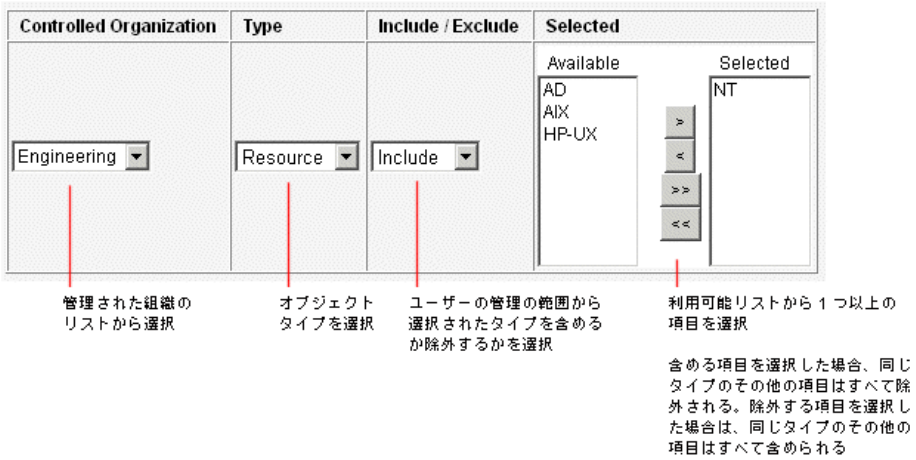


図 9 管理者ロール : 管理する組織に含める / 除外するオブジェクトの選択

「含める」リストと「除外する」リストの両方に選択した項目は、管理者ロールから除外されます。

管理者ロールへのユーザーフォームの割り当て

管理者ロールの属性としてユーザーフォームを指定することができます。管理者ロールを割り当てられた管理者は、その管理者ロールによって管理されている組織内のユーザーを作成または編集するときにこのユーザーフォームを使用します。管理者ロールを介して割り当てられたユーザーフォームは、管理者がメンバーになっている組織から継承したすべてのユーザーフォームよりも優先されます。ただし、管理者に直接割り当てられたユーザーフォームよりも優先されることはありません。

ユーザーを編集するときに使用されるユーザーフォームは、次の優先順位で決定されます。

- ユーザーフォームが管理者に直接割り当てられている場合は、そのユーザーフォームが使用されます。
- 管理者に直接割り当てられているユーザーフォームがなくても、次のような管理者ロールが管理者に割り当てられる場合があります。
  - 作成または編集するユーザーがメンバーになっている組織を管理する
  - その組織に対して、ユーザーフォームが指定されている

  この場合は、そのユーザーフォームが使用されます。
- 管理者に直接割り当てられているかまたは管理者ロールを介して間接的に割り当てられているユーザーフォームがない場合は、管理者のメンバー組織 (管理者のメンバー組織から最上位組織のすぐ下の組織まで) に割り当てられているユーザーフォームが使用されます。

- 管理者のメンバー組織に割り当てられているユーザーフォームがない場合は、デフォルトのユーザーフォームが使用されます。

管理者に、同じ組織を管理しながら異なるユーザーフォームを指定している複数の管理者ロールが割り当てられている場合、その組織内のユーザーを作成または編集しようとするとエラーが表示されます。管理者が、同じ組織を管理しながら異なるユーザーフォームを指定している複数の管理者ロールを割り当てようとすると、エラーが表示されます。この競合を解決するまで変更は保存できません。

機能規則と管理する組織規則

次の例は、機能規則または管理する組織規則の設定方法を示しています。管理者ロールが適用されたユーザーに割り当てる機能または管理する組織を動的に制御することができます。

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

機能規則：キーの定義と取り込み

- 機能規則には、`authType='CapabilitiesRule'` エントリを含める必要があります。管理者ロールページで機能規則を選択するには、このエントリが必要です。
- コンテキストは、現在認証されている Identity Manager ユーザーのユーザービューです。
- 次のサンプル規則では、定義された変数 (`defvar`) `'user groups'` が、Windows Active Directory サーバー上で現在認証されている `'ranger-AD'` という名前の Identity Manager ユーザーアカウントを取得し、このユーザーが現在登録されているグループのリストを返します。
- 条件ロジック (`cond`) は、現在認証されている Identity Manager ユーザーが `'manager'` グループのメンバーであるかどうかを確認します。真の場合、このユーザーに Identity Manager 機能のログイン管理者およびリソース管理者が割り当てられます。偽の場合、Identity Manager 機能は割り当てられません。

機能規則の例

```
<?xml version='1.0' encoding='UTF-8'?>

<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>

<Rule authType='CapabilitiesRule' name='If Manager'>

   <block>

      <defvar name='user groups'>

         <get>
```

```
            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>
          <ref>context</ref>
            <s>ranger-AD</s>
            <s>User</s>
          <ref>accountInfo.accounts[ranger-AD].accountId</ref>
          <map>
            <s>searchAttrsToGet</s>
               <list>
            <s>memberOf</s>
               </list>
          </map>
          </invoke>
            <s>user.attributes.memberOf</s>
          </get>
       </defvar>
    <cond>
       <contains>
          <ref>user groups</ref>
             <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
       </contains>
       <list>
          <s>Login Administrator</s>
          <s>Resource Administrator</s>
       </list>
    </cond>
    </block>
    <MemberObjectGroups>
       <ObjectRef type='ObjectGroup'
id='#ID#ObjectGroup:Waveset'        name='Waveset'/>
```

```
   </MemberObjectGroups>
</Rule>
```

管理する組織規則：キーの定義

- 管理する組織規則には、`authType='ControlledOrganizationsRule'` エントリを含める必要があります。このエントリによって、管理者ロールページで管理する組織規則を選択できるようになります。
- コンテキストは、現在認証されている Identity Manager ユーザーのユーザービューです。
- 次のサンプル規則では、定義された変数 (`defvar`) `'user groups'` が、Windows Active Directory サーバー上で現在認証されている `'ranger-AD'` という名前の Identity Manager ユーザーアカウントを取得し、このユーザーが現在登録されているグループのリストを返します。
- 条件ロジック (`cond`) は、現在認証されている Identity Manager ユーザーが `'manager'` グループのメンバーであるかどうかを確認します。真の場合、Identity Manager `'Waveset'` 組織管理がユーザーに割り当てられます。偽の場合、組織管理は割り当てられません。

管理する組織規則の例

```
<?xml version='1.0' encoding='UTF-8'?>

<!DOCTYPE Rule PUBLIC 'waveset.dtd' 'waveset.dtd'>

<Rule authType='ControlledOrganizationsRule' name='Get managed
departments'>

   <block>

      <defvar name='user groups'>

         <get>

            <invoke name='getResourceObject'
              class='com.waveset.ui.FormUtil'>

            <ref>context</ref>

               <s>ranger-AD</s>

               <s>User</s>

            <ref>accountInfo.accounts[ranger-
AD].accountId</ref>

            <map>
```

```
                <s>searchAttrsToGet</s>
              <list>
                <s>memberOf</s>
              </list>
              </map>
            </invoke>
              <s>user.attributes.memberOf</s>
            </get>
          </defvar>
        <cond>
          <contains>
          <ref>user groups</ref>
            <s>CN=manager,DC=dev-ad,DC=waveset,DC=com</s>
        </contains>
          <list>
            <s>Waveset</s>
          </list>
         </cond>
        </block>
        <MemberObjectGroups>
        <ObjectRef type='ObjectGroup' id='#ID#ObjectGroup:Waveset'
            name='Waveset'/>
        </MemberObjectGroups>
    </Rule>
```

電子メールテンプレートについて

Identity Manager では、電子メールテンプレートを使用して、情報および操作の要求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。

- **アカウントの作成の承認** – 新しいアカウントが承認待ちであるという通知を承認者に送信します。関連付けられているロールの「プロビジョン通知」オプションが「承認」に設定されている場合に、この通知が送信されます。
- **アカウントの作成の通知** – アカウントが作成され、特定のロールが割り当てられたという通知を送信します。「ロールの作成」または「ロールの編集」ページの「通知受信者」フィールドで、1 人以上の管理者が選択されている場合に、この通知が送信されます。
- **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。
- **パスワード同期情報** – パスワードの変更がすべてのリソースで正常に完了したことをユーザーに通知します。通知には、正常に更新されたリソースが一覧表示され、パスワード変更の要求元が示されます。
- **パスワード同期エラー情報** – パスワードの変更がすべてのリソースでは成功しなかったことをユーザーに通知します。通知には、エラーが一覧表示され、パスワード変更の要求元が示されます。
- **アカウントイベントの調整、リソースイベントの調整、調整の概要** – Notify Reconcile Response、Notify Reconcile Start、および Notify Reconcile Finish デフォルトワークフローからそれぞれ呼び出されます。通知は、各ワークフローの設定に基づいて送信されます。
- **レポート** – 生成されたレポートを指定されたリストの受信者に送信します。
- **リソースの要求** – リソースが要求されたという通知をリソース管理者に送信します。管理者が「リソース」エリアからリソースを要求したときに、この通知が送信されます。
- **再試行通知** – あるリソースに関する特定の操作の試行が指定回数失敗したという通知を管理者に送信します。
- **リスク分析** – リスク分析レポートを送信します。リソーススキャンの一部として、1 人以上の電子メール受信者が指定されている場合に、このレポートが送信されます。
- **一時パスワードリセット** – アカウントに暫定パスワードが提供されたという通知をユーザーまたはロール承認者に送信します。関連付けられた Identity Manager ポリシーに対して選択したパスワードリセット通知オプションの値に応じて、ユーザーの Web ブラウザにただちに通知が表示されるか、ユーザーまたはロール承認者に電子メールが送信されます。

電子メールテンプレートのカスタマイズ

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、承認者に次のような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カスタマイズするには、次を実行します。

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

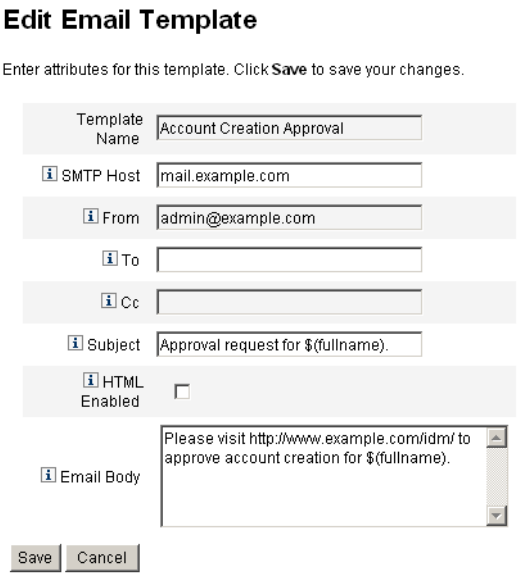


図 10 電子メールテンプレートのカスタマイズ

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

5. **「保存」**をクリックします。

注 Business Process Editor (BPE) を使用して電子メールテンプレートを修正することもできます。BPE の詳細については、『Identity Manager Deployment Tools』を参照してください。

電子メールテンプレートの HTML とリンク

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

電子メール本文の許容変数

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。

各テンプレートの許容変数を、次の表に定義します。

テンプレート	許容変数
パスワードリセット	`$(password)` **— 新規に生成されたパスワード**
承認の更新	`$(fullname)` **— ユーザーのフルネーム** `$(role)` **— ユーザーのロール**
通知の更新	`$(fullname)` **— ユーザーのフルネーム** `$(role)` **— ユーザーのロール**
レポート	`$(report)` **— 生成されたレポート** `$(id)` **— タスクインスタンスのエンコード ID** `$(timestamp)` **— 電子メールの送信時刻**
リソースの要求	`$(fullname)` **— ユーザーのフルネーム** `$(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**

表 2 電子メールテンプレート変数

監査グループの設定

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。

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

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

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

監査設定グループ内のイベントの編集

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

監査設定グループへのイベントの追加

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

Remedy との統合

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

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

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

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

Identity Manager サーバーの設定

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

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

調整サーバーの設定

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

- **「並列リソースの制限」**－ 調整サーバーが同時に処理できるリソースの最大数を指定します。
- **「最小ワークスレッド」**－ 調整サーバーが常にライブ状態で維持する処理スレッドの最小数を指定します。
- **「最大ワークスレッド」**－ 調整サーバーが使用できる処理スレッドの最大数を指定します。調整サーバーは、作業の負荷に応じて、スレッドを必要な数だけ開始します。ここで指定する最大数でその数が制限されます。

スケジューラの設定

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

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

「保存」をクリックして、サーバー設定の変更を保存します。

サーバーのデフォルト設定の編集

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

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

「保存」をクリックして、サーバー設定の変更を保存します。

署名付き承認

次の情報と手順を使用して、デジタル署名付きの承認を設定します。次の作業を行う手順と例を示します。

- 署名付き承認の設定 (サーバー側およびクライアント側)
- Identity Manager への証明書と CRL の追加
- 承認の署名

署名付き承認の設定

次の手順を実行して、署名付き承認を設定します。

サーバー側の設定

サーバー側の設定を有効にするには、次のようにします。

1. システム設定に `security.nonrepudiation.signedApprovals=true` を設定します。
2. 自分の認証局 (CA) の証明書を信頼できる証明書として追加します。そのためには、まず証明書のコピーを取得する必要があります。

   たとえば、Microsoft CA を使用している場合には、行う手順は次のようになります。

   a. http://***IPAddress***/certsrv にアクセスして、管理特権でログインします。

   b. 「CA 証明書または証明書失効リストの取得」を選択して、**「次へ」**をクリックします。

   c. CA 証明書をダウンロードして保存します。
3. この証明書を Identity Manager に信頼できる証明書として追加します。

   a. 管理者インタフェースから、**「設定」**を選択し、**「証明書」**を選択すると、Identity Manager は「証明書」ページを表示します。

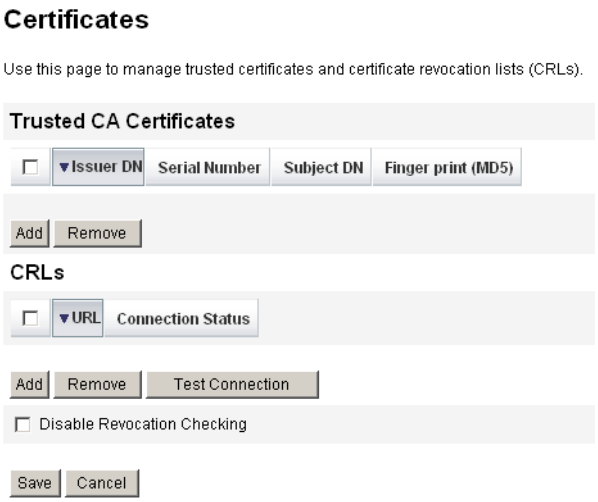


図 11 証明書

b. 「信頼できる認証局証明書」エリアで、**「追加」**をクリックします。Identity Manager は「証明書のインポート」ページを表示します。

c. 信頼できる証明書を参照および選択して、**「インポート」**をクリックします。

これで、証明書が信頼できる証明書のリストに表示されます。

4. 次のようにして、CA の証明書失効リスト (CRL) を追加します。
   a. 「証明書」ページの「CRL」エリアで、**「追加」**をクリックします。
   b. CA の CRL の URL を入力します。

注意 :

- 証明書失効リスト (CRL) は、失効したか有効ではない証明書シリアル番号のリストです。
- CA の CRL の URL は http または LDAP にすることができます。
- CRL 配布先の URL は CA ごとに異なりますが、CA 証明書の「CRL 配布点」拡張を参照して決めることができます。

5. **「テスト接続」**をクリックして、URL を確認します。
6. **「保存」**をクリックします。
7. jarsigner を使用して applets/ts1.jar に署名します。

注 詳細については、http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/jarsigner.html を参照してください。Identity Manager とともに提供されている `ts1.jar` ファイルは、自己署名付き証明書を使用して署名されているため、本稼働システムには使用しないでください。本稼働では、信頼できる CA によって発行されたコード署名証明書を使用して、このファイルを署名し直すことをお勧めします。

クライアント側の設定

次の手順を実行して、クライアント側の設定を有効にします。

前提条件

クライアントシステムで、JRE 1.4 以上が動作する Web ブラウザが実行されている必要があります。

手順

証明書と非公開鍵を取得して、PKCS#12 キーストアにエクスポートします。

たとえば、Microsoft CA を使用している場合には、行う手順は次のようになります。

1. Internet Explorer を使用して、http://***IPAddress***/certsrv を参照し、管理特権でログインします。
2. 「証明書の要求」を選択して、**「次へ」**をクリックします。
3. 「要求の詳細設定」を選択して、**「次へ」**をクリックします。
4. **「次へ」**をクリックします。
5. 「証明書テンプレート」で「ユーザー」を選択します。
6. 次のオプションを選択します。
   a. エクスポート可能なキーとして指定する
   b. 秘密キーの強力な保護を有効にする
   c. ローカルコンピュータストアを使用する
7. **「送信」**をクリックして、**「OK」**をクリックします。
8. **「この証明書のインストール」**をクリックします。
9. 「ファイル名を指定して実行」—> mmc を実行して、mmc を起動します。

10. 証明書スナップインを追加します。
    a. 「コンソール」—>「スナップインの追加と削除」を選択します。
    b. **「追加 ...」**をクリックします。
    c. 「コンピュータアカウント」を選択します。
    d. **「次へ」**をクリックして、**「完了」**をクリックします。
    e. **「閉じる」**をクリックします。
    f. **「OK」**をクリックします。
    g. 「証明書」—>「個人」—>「証明書」の順に進みます。
    h. 「管理者」を右クリックして、「すべてのタスク」—>「エクスポート」を選択します。
    i. **「次へ」**をクリックします。
    j. **「次へ」**をクリックして、非公開鍵がエクスポートされていることを確認します。
    k. **「次へ」**をクリックします。
    l. パスワードを設定して、**「次へ」**をクリックします。
    m. ファイル ***CertificateLocation***。
    n. **「次へ」**をクリックして、**「完了」**をクリックします。**「OK」**をクリックして確認します。

承認の署名

次の手順を実行して、承認に署名します。

1. Identity Manager 管理者インタフェースから、**「承認」**を選択します。
2. リストから承認を選択します。
3. 承認のコメントを入力して、**「承認」**をクリックします。
   Identity Manager はアプレットを信頼するかどうかを確認するように要求します。
4. **「常時」**をクリックします。
   Identity Manager は承認の日付入りの概要を表示します。
5. キーストアの場所 (サーバー側の設定手順 10m で指定した場所) を、入力するかまたは「参照」をクリックして特定します。
6. キーストアパスワード (サーバー側の設定手順 10l で設定したパスワード) を入力します。
7. **「署名」**をクリックして、要求を承認します。

その後の承認の署名

一度承認に署名すると、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よくなります (Identity Manager は、前回の承認で使用したキーストアの場所を記憶しているはず)。

トランザクション署名の表示

次の手順を実行して、Identity Manager の監査ログレポートにトランザクション署名を表示します。

1. Identity Manager の管理インタフェースから、**「レポート」**を選択します。
2. 「レポートの実行」ページで、オプションの「新規 ... リストから「監査ログレポート」を選択します。
3. 「レポートタイトル」フィールドに、「承認」などのタイトルを入力します。
4. 「組織」選択エリアで、すべての組織を選択します。
5. 「アクション」オプションを選択して、「承認」を選択します。
6. **「保存」**をクリックしてレポートを保存し、「レポートの実行」ページに戻ります。
7. **「実行」**をクリックして、「承認」レポートを実行します。
8. 詳細リンクをクリックして、次に示すトランザクション署名情報を表示します。
   - 発行者
   - 対象者
   - 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

署名付き承認

6 データの同期と読み込み

この章では、Identity Manager でのデータの同期と読み込み機能の説明および手順を示します。

この章のトピック

この章では、次について詳細に説明します。

- Identity Manager データ同期ツール (検索、調整、および ActiveSync)
- 検索、調整、および ActiveSync 機能を使用してデータを最新に保つ方法

データ同期ツール：最適なツールの選択

Identity Manager データ同期ツールを選択してタスクを実行する場合は、次のガイドラインに従います。

実行するタスク	使用する機能
最初からリソースアカウントを Identity Manager に取得する。読み込みの前に表示はしない	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 に取得する。オプションで、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 に取得する。設定されたポリシーに従って各アカウントを操作する	リソースの調整
リソースアカウントの変更を Identity Manager に適用する、または取得する	ActiveSync (複数リソースの実装)

探索

Identity Manager アカウント検索機能を使用すると、導入とアカウント作成タスクの速度が向上します。検索機能には次のものがあります。

- **ファイルへ抽出** ― リソースアダプタによって返されたリソースアカウントをファイル (CSV または XML 形式) に抽出します。データを Identity Manager にインポートする前に、このファイルを処理することができます。
- **ファイルから読み込み** ― ファイル (CSV または XML 形式) のアカウントを読み取り、Identity Manager に読み込みます。
- **リソースから読み込み** ― ほかの 2 つの検索機能を組み合わせたもので、リソースからアカウントを抽出し、それを Identity Manager に直接読み込みます。

これらのツールを使用して、新しい Identity Manager ユーザーを作成したり、リソースのアカウントを既存の Identity Manager ユーザーアカウントに相互に関連付けたりすることができます。

ファイルへ抽出

この機能は、リソースアカウントをリソースから XML または CSV テキストファイルに抽出するために使用します。これにより、抽出したデータを表示して変更したあとに、Identity Manager にインポートすることができます。

リソースアカウントを抽出するには、次を実行します。

1. メニューバーで**「アカウント」**を選択し、**「ファイルへ抽出」**を選択します。
2. アカウントの抽出元となるリソースを選択します。
3. 出力のアカウント情報のファイル形式を選択します。データを XML ファイルまたはテキストファイルに抽出することができます。アカウント属性はカンマ区切り値 (CSV) 形式で表示されます。
4. **「ダウンロード」**をクリックします。Identity Manager は「ファイルのダウンロード」ダイアログを表示し、そこで、抽出したファイルを保存するか表示するかを選択できます。

ヒント ファイルを開く場合は、そのファイルを表示するプログラムを選択しなければならない場合があります。

ファイルから読み込み

この機能は、リソースアカウント、つまり Identity Manager を通じてリソースから抽出されたリソースアカウントか、別のファイルソースから抽出されたリソースアカウントを Identity Manager に読み込むために使用します。Identity Manager のファイルへ抽出機能で作成されたファイルは XML 形式です。新しいユーザーのリストを読み込んだ場合、通常、データファイルは CSV 形式です。

CSV ファイル形式について

ほとんどの場合、読み込まれるアカウントはスプレッドシート (Excel など) にリストされ、値をカンマで区切った CSV 形式で保存されて、Identity Manager に読み込まれます。CSV ファイルの内容は、次のフォーマットガイドラインに従っている必要があります。

1 行目 ― 各フィールドの列見出しまたはスキーマ属性を、カンマで区切ってリストします。

2 行目から最後まで ― 1 行目で定義した各属性の値を、カンマで区切ってリストします。フィールド値のデータが存在しない場合は、連続するカンマでそのフィールドを表します。

たとえば、ファイルの最初の 3 行が次のようになることがあります。

```
firstname,middleinitial,lastname,accountId,asciipassword,EmployeeID,Department,Ph
John,Q,Example,E1234,E1234,1234,Operations,555-222-1111
Jane,B,Doe,E1111,E1111,1111,,555-222-4444
```

この例では、2 番目のユーザーである Jane Doe には部署がありません。値がない場合は、連続するカンマ (,,) で表します。

アカウントをロードするには、次を実行します。

1. メニューバーで**「アカウント」**を選択し、**「ファイルから読み込み」**を選択します。
   Identity Manager は「ファイルから読み込み」ページを表示します。ここで次の読み込みオプションを指定してから処理を続行します。
   - **「ユーザーフォーム」**― 読み込み結果により Identity Manager ユーザーが作成される場合、ユーザーフォームは、ロール、リソース、およびその他の属性と同様に組織を割り当てます。各リソースアカウントに割り当てるユーザーフォームを選択してください。
   - **「アカウント相関規則」**― アカウント相関規則は、所有者のいない各リソースアカウントの所有者候補の Identity Manager ユーザーを選択します。所有者のいないリソースアカウントの属性が与えられると、相関規則は、所有者候補のユーザーを選択するために使用される名前のリストまたは属性条件のリストを返します。所有者のいない各アカウントを所有している可能性のある Identity Manager ユーザーを検索するための規則を選択してください。

- **「アカウント確認規則」**― アカウント確認規則は、相関規則が選択した所有者の候補から非所有者を除外します。Identity Manager ユーザーの完全なビューと所有されていないリソースアカウントの属性が与えられた場合、確認規則はユーザーがアカウントを所有していれば true を、そうでない場合は false を返します。リソースアカウントの各所有者候補をテストするための規則を選択します。「確認規則なし」を選択した場合、Identity Manager はすべての所有者候補を確認なしで受け入れます。

注　お使いの環境で、相関規則が各アカウントに対して多くとも 1 つの所有者しか選択しない場合、確認規則は必要ありません。

- **「一致のみ読み込み」**― 既存の Identity Manager ユーザーと一致するアカウントのみを読み込むことを選択します。このオプションが選択されている場合、不一致のリソースアカウントはすべて読み込みから破棄されます。
- **「属性の更新」**― 現在の Identity Manager ユーザー属性値を、読み込まれたアカウントの属性値で置き換えることを選択します。
- **「属性値のマージ」**― その属性値が上書きではなく (重複を除いて) 結合されるような、1 つ以上の属性名をカンマで区切って入力します。このオプションは、グループやメーリングリストなどの、リストタイプの属性にのみ使用できます。また、「属性値の更新」オプションも選択する必要があります。
- **「結果レベル」**― 読み込みプロセスがアカウントの個々の結果を記録するしきい値を選択します。
  - **「エラーのみ」**― アカウントの読み込みでエラーメッセージが生成されたときにのみ個々の結果を記録します。
  - **「警告およびエラー」**― アカウントの読み込みで警告またはエラーメッセージが生成されたときに個々の結果を記録します。
  - **「情報以上」**― すべてのアカウントの個々の結果を記録します。これを選択すると、読み込みの速度が低下します。

2. 「アップロードするファイル」フィールドで、読み込むファイルを指定して**「アカウントの読み込み」**をクリックします。

注意 :

- 入力ファイルにユーザー列が含まれていない場合は、読み込みを正常に続行するために確認規則を選択する必要があります。
- 読み込みプロセスに関連付けられているタスクインスタンス名は、入力ファイル名に基づいています。そのため、ファイル名を再利用すると、最後の読み込みプロセスに関連付けられているタスクインスタンスによって以前のすべてのタスクインスタンスが上書きされます。

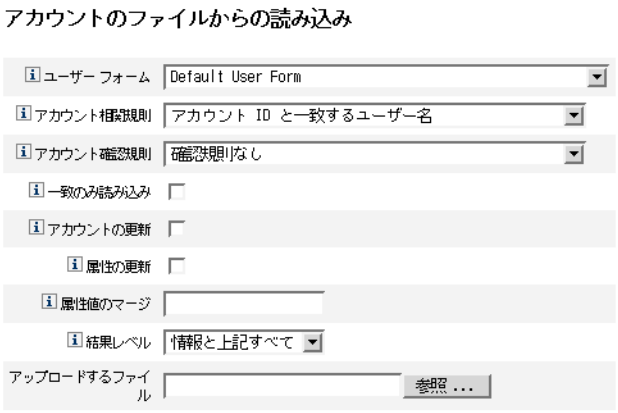


図 1 ファイルから読み込み

アカウントが既存のユーザーと一致する (または相互に関連する) 場合、読み込みプロセスではアカウントがユーザーにマージされます。また、相互に関連しない入力アカウントから新しい Identity Manager ユーザーも作成されます (「相関は必須」が指定されていない場合)。

`bulkAction.maxParseErrors` 設定変数は、ファイルの読み込み時に発生するエラーの数の制限を設定します。デフォルトでは、エラー数の制限は 10 です。`maxParseErrors` の数のエラーが発生した場合、解析が停止します。

リソースから読み込み

この機能は、指定した読み込みオプションに従ってアカウントを Identity Manager に直接抽出してインポートするために使用します。

アカウントをインポートするには、メニューバーで**「アカウント」**を選択し、**「リソースから読み込み」**を選択します。

注 Identity Manager では、処理を続行する前に、読み込みオプションを指定できます。「リソースから読み込み」ページで利用可能な読み込みオプションと、その結果の操作は、「ファイルから読み込み」ページと同じです。

調整

調整機能は、Identity Manager のリソースアカウントと実際にリソースに存在するアカウントの不整合をハイライト表示し、アカウントデータを定期的に相互に関連付けるために使用します。

調整は処理の進行中に比較するために設計されており、次の特徴があります。

- 検索プロセスよりも具体的なアカウント状況の診断と、より広範囲な応答のサポート
- スケジュール可能 (検索では不可能)
- 差分モードの提供 (検索では常に完全モード)
- ネイティブ変更の検出 (検索では不可能)

また、リソース処理の次の各時点で任意のワークフローを起動するように調整を設定できます。

- アカウントの調整前
- アカウントごと
- すべてのアカウントの調整後

Identity Manager 調整機能には、「リソース」エリアからアクセスします。リソースリストには、各リソースが最後に調整された日時および現在の調整ステータスが表示されます。

調整ポリシーについて

調整ポリシーを使用して、調整タスクごとに各リソースに対して一連の応答を設定できます。ポリシーでは、調整を実行するサーバーを選択し、どのような場合にどのような頻度で調整を実行するかを指定して、調整中に発生した各状況に対する応答を設定します。また、アカウント属性に対して (Identity Manager を経由せずに) ネイティブに行われた変更を検出するように調整を設定することもできます。

調整ポリシーの編集

調整ポリシーを編集するには、次の手順を実行します。

1. メニューバーで**「リソース」**を選択します。
2. 「リソース」リスト階層内のリソースを選択します。
3. 「リソースアクション」オプションリストから「調整ポリシーの編集」を選択します。

   Identity Manager は「調整ポリシーの編集」ページを表示し、ここで、次のようなポリシーの項目を選択できます。

   - **「調整サーバー」**― クラスタ環境では、各サーバーが調整を実行できます。ポリシーで、どの Identity Manager サーバーがリソースに対して調整を実行するのかを指定します。
   - **「調整モード」**― 調整は、いくつかの異なるモードで実行でき、これにより品質を最適化できます。
     - **「完全調整」**― スピードを犠牲にして徹底的に最適化します。
     - **「差分調整」**― ある程度の妥協により速度を最適化します。

     ポリシー内で、Identity Manager がリソースに対して調整を実行するモードを選択します。目的のリソースの調整を無効化する場合は、「調整しない」を選択します。
   - **「完全調整スケジュール」**― 完全調整モードが有効になっている場合、調整は固定されたスケジュールで自動的に実行されます。ポリシー中で、完全調整がリソースに対してどのような頻度で実行されるかを指定します。より高いレベルのポリシーから指示されたスケジュールを継承する場合は、「継承」オプションを選択します。
   - **「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。ポリシー中で、差分調整がリソースに対してどのような頻度で実行されるかを指定します。より高いレベルのポリシーから指示されたスケジュールを継承する場合は、「継承」オプションを選択します。

注　差分調整をサポートしないリソースもあります。

   - **「属性レベル調整」**― 調整は、アカウント属性に対してネイティブな (つまり、Identity Manager を介さない) 変更が加えられたことを検出するように設定できます。**「調整アカウント属性」**で、指定された属性へのネイティブな変更を検出するかどうかを指定します。
   - **「アカウント相関規則」**― アカウント相関規則は、所有者のいない各リソースアカウントの所有者候補の Identity Manager ユーザーを選択します。所有者のいないリソースアカウントの属性が与えられると、相関規則は、所有者候補のユーザーを選択するために使用される名前のリストまたは属性条件のリストを返します。所有者のいない各アカウントを所有している可能性のある Identity Manager ユーザーを検索するための規則を選択してください。

- **「アカウント確認規則」** ― アカウント確認規則は、相関規則が選択した所有者の候補から非所有者を除外します。Identity Manager ユーザーの完全なビューと所有されていないリソースアカウントの属性が与えられた場合、確認規則はユーザーがアカウントを所有していれば true を、そうでない場合は false を返します。リソースアカウントの各所有者候補をテストするための規則を選択します。「確認規則なし」を選択した場合、Identity Manager はすべての所有者候補を確認なしで受け入れます。

注 お使いの環境で、相関規則が各アカウントに対して多くとも 1 つの所有者しか選択しない場合、確認規則は必要ありません。

- **「プロキシ管理者」** ― 調整応答の実行時に使用される管理者を指定します。調整では、指定されたプロキシ管理者が実行を許可されている操作のみを実行できます。応答は、(必要な場合) この管理者と関連付けられたユーザーフォームを使用します。

  「プロキシ管理者なし」オプションを選択することもできます。このオプションを選択した場合、調整の結果を表示できますが、応答の操作またはワークフローは実行されません。

- **「状況オプション」**(および「応答」) ― 調整では、数種類の状況が認識されます。「応答」列で、調整が実行する操作を指定します。
  - **「確認」** ― 予想されるアカウントは存在します。
  - **「削除済み」** ― 予想されるアカウントは存在しません。
  - **「存在」** ― 調整プロセスは、割り当てられたリソースに対して、一致するアカウントを発見しました。
  - **「存在しない」** ― 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。
  - **「衝突」** ― 2 人以上の Identity Manager ユーザーが、単一のリソースに対して同じアカウントを割り当てられています。
  - **「未割り当て」** ― 調整プロセスは、このユーザーに割り当てられていないリソースに対して、一致するアカウントを発見しました。
  - **「不一致」** ― アカウントはどのユーザーとも一致しません。
  - **「複数ユーザー」** ― アカウントは 1 人以上のユーザーと一致します。

  次のいずれかの応答オプションを選択します (状況により、選択できるオプションは異なる)。
  - **「リソースアカウントに基づく新規 Identity Manager ユーザーの作成」** ― リソースアカウント属性に基づいてユーザーフォームが実行され、新規ユーザーが作成されます。リソースアカウントは、どのような変更が行われても更新されません。
  - **「Identity Manager ユーザーのリソースアカウントの作成」** ― ユーザーフォームを使用してリソースアカウント属性を再生成し、存在しないリソースアカウントを再作成します。
  - **「リソースアカウントの削除」**および**「リソースアカウントの無効化」** ― リソースのアカウントを削除 / 無効化します。

- **「Identity Manager ユーザーへリソースアカウントをリンク」**および**「Identity Manager ユーザーからリソースアカウントへのリンク解除」**― リソースアカウント割り当てをユーザーに追加するか、ユーザーから削除します。フォーム処理は実行されません。

- **「調整前ワークフロー」**― 調整は、リソースを調整する前にユーザー指定のワークフローを実行するように設定できます。調整が実行するワークフローを選択してください。どのワークフローも実行しない場合は、「ワークフローを実行しない」を選択してください。
- **「アカウント単位ワークフロー」**― 調整がリソースアカウントの状況に応答したあと、ユーザー指定のワークフローを実行するように設定できます。調整が実行するワークフローを選択してください。どのワークフローも実行しない場合は、「ワークフローを実行しない」を選択してください。
- **「調整後ワークフロー」**― リソースの調整が完了したあとに、ユーザー指定のワークフローを実行するように設定できます。調整が実行するワークフローを選択してください。どのワークフローも実行しない場合は、「ワークフローを実行しない」を選択してください。

ポリシーの変更を保存するには、**「保存」**をクリックしてください。

調整の開始

調整タスクを開始する場合は、次の 2 つのオプションが利用可能です。

- 調整のスケジュール ― 「調整ポリシーの編集」ページで、調整スケジュールを設定できます。これにより、調整が定期的に実行されます。
- 即座に調整 ― 調整をただちに実行します。このためには、リソースリスト内のリソースを選択し、「リソースアクション」リストから次のオプションのどちらかを選択します。
  - ただちに完全調整
  - ただちに差分調整

  調整は、ポリシーに設定されたパラメータに従って実行されます。定期的に調整を実行するようにポリシーを設定すると、指定どおりに調整が実行されます。

調整のキャンセル

調整をキャンセルするには、リソースを選択し、「リソースアクション」リストから「調整のキャンセル」を選択します。

調整ステータスの表示

リソースリストの「ステータス」列には、次のような調整ステータスの状態が表示されます。

- **「不明」** ― ステータスは不明です。最後に実行された調整の結果はわかりません。
- **「無効」** ― 調整は無効化されています。
- **「失敗」** ― 直前の調整は正常に完了していません。
- **「成功」** ― 直前の調整は正常に完了しています。
- **「エラーありで完了」** ― 直前の調整は完了しましたが、エラーがありました。

注　ステータスの変更を確認するには、このページを更新する必要があります (情報は自動更新されない)。

リソースの各アカウントの詳細なステータス情報を表示できます。リスト内のリソースを選択し、「リソースアクション」リストから「調整ステータスの表示」を選択してください。

アカウントインデックスの操作

アカウントインデックスは、Identity Manager に認識される各リソースアカウントの最後の既知の状態を記録します。アカウントインデックスは主に調整によって保守されますが、ほかの Identity Manager 機能も、必要に応じてアカウントインデックスを更新します。

注　検索ツールはアカウントインデックスを更新しません。

アカウントインデックスの検索

アカウントインデックスを検索するには、「リソースアクション」リストから「アカウントインデックスの検索」を選択します。

検索タイプを選択してから、検索属性を入力または選択します。**「検索」**をクリックすると、検索条件と一致するアカウントを検索します。

- **リソースアカウント名** ― このオプションを選択した場合は、「が次の文字列で始まる」、「が次の文字列を含む」、「が次の文字列と等しい」のいずれかの修飾子を選択してから、アカウント名の一部または全部を入力します。
- **検索対象リソース** ― このオプションを選択した場合は、リストから 1 つ以上のリソースを選択して、指定したリソース上にある調整済みアカウントを検索します。
- **所有者** ― このオプションを選択した場合は、「が次の文字列で始まる」、「が次の文字列を含む」、「が次の文字列と等しい」のいずれかの修飾子を選択してから、所有者名の一部または全部を入力します。所有者のいないアカウントを検索するには、UNMATCHED または DISPUTED 状況のアカウントを検索します。

- **調整状況** – このオプションを選択した場合、リストから 1 つ以上の状況を選択して、指定した状況と一致する調整済みアカウントを検索します。

「検索」をクリックすると、検索パラメータに従ってアカウントを検索します。検索結果の数を制限するために、「結果表示を次の件数に限定」フィールドに数を指定することもできます。デフォルトの制限数は、検出されたアカウントの最初から 1000 件目までです。

「クエリーのリセット」をクリックすると、ページがクリアされ、新たに選択を行えます。

アカウントインデックスの検査

すべての Identity Manager ユーザーアカウントを表示することができます。また、オプションとして、それらをユーザーベースで調整することができます。このためには、**「リソース」**を選択してから、**「アカウントインデックスの検査」**を選択します。

Identity Manager が認識するすべてのリソースアカウントが表形式で表示されます (Identity Manager ユーザーに所有されるアカウントかどうかに関係なく)。この情報は、リソース別、または Identity Manager の組織別にまとめられます。この表示を変更するには、「インデックス表示の変更」リストから選択を行います。

アカウントの操作

リソースのアカウントを操作するには、「リソースごとのグループ」インデックス表示を選択します。リソースタイプごとにフォルダが表示されます。フォルダを展開して特定のリソースに移動します。リソースの隣の + または - をクリックすると、Identity Manager が認識するリソースアカウントがすべて表示されます。

注　リソースに対する最後の調整後に、そのリソースに直接追加されたアカウントは、表示されません。

アカウントの現在の状況に応じて、いくつかの操作を実行できます。また、アカウントの詳細を表示したり、その 1 つのアカウントを調整したりすることを選択できます。

ユーザーの操作

Identity Manager ユーザーを操作するには、「ユーザーごとのグループ」インデックス表示を選択します。この表示では、「アカウントのリスト」ページのように、Identity Manager ユーザーおよび組織が階層構造で表示されます。Identity Manager で現在ユーザーに割り当てられているアカウントを表示するには、ユーザーに移動してユーザー名の隣のインジケータをクリックします。ユーザーのアカウントと、Identity Manager が認識するそのアカウントの現在のステータスがユーザー名の下に表示されます。

アカウントの現在の状況に応じて、いくつかの操作を実行できます。また、アカウントの詳細を表示したり、その 1 つのアカウントを調整したりすることを選択できます。

ActiveSync アダプタ

Identity Manager ActiveSync 機能を使用すると、権限外部リソース (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 ユーザーデータと同期させることができます。Identity Manager リソースにアクティブな同期をセットアップすると、権限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。

アクティブな同期のセットアップ

Identity Manager リソースエリアにある「ActiveSync ウィザード」を使用して、アクティブな同期をセットアップします。このウィザードは手順のさまざまなセットを示し、このセットによりリソース用のアクティブな同期が設定されます (手順は選択によって異なる)。

「Active Sync ウィザード」を起動するには、リソースリスト内のリソースを選択し、「リソースアクション」オプションリストから「Active Sync ウィザード」を選択します。

「Active Sync ウィザード」の「同期モード」ページが表示されます。

同期モード

「同期モード」ページでは、アクティブな同期の設定中に選択可能な設定オプションの範囲を指定できます。

次のいずれかのオプションを選択します。

「入力フォームの使用」 ― アクティブな同期のセットアップ時に使用するモードを選択します。既存のフォームを使用するよう選択できますが、その場合このリソースの設定の選択が制限されます。代わりに、Active Sync ウィザードで生成したフォームを使用すると、設定の選択の完全なセットが提供されます。

- 「既存の入力フォーム」(デフォルト) を選択した場合、次のオプションの選択を行います。
  - **「入力フォーム」** ― データ更新を処理する入力フォームを選択します。このオプション設定項目を使用すると、属性を変換してからアカウントに保存することができます。
  - **「処理規則」** ― 各受信アカウントに対して実行する処理規則をオプションで選択します。この選択は、ほかのすべての選択よりも優先されます。処理規則を指定した場合、このリソースに関するほかの設定に関係なく、すべての行に対して処理が実行されます。これは、プロセス名か、またはプロセス名として評価される規則です。

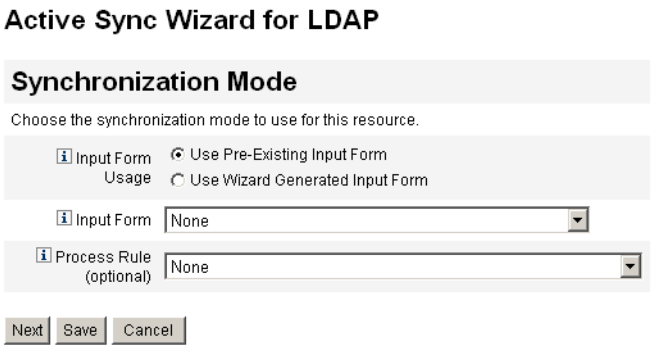


図 2 Active Sync ウィザード：「同期モード」、「既存のフォーム」の選択

- 「ウィザードで生成した入力フォームを使用」を選択した場合、次のオプションの選択を行います。
  - **「設定モード」** – Active Sync ウィザードに基本モードを使用するか詳細モードを使用するかを選択します。基本モードがデフォルトのオプションです。詳細モードを選択した場合、イベントタイプを定義し処理規則を設定できます。
  - **「処理規則」** – (詳細設定モードでのみ表示) 各受信アカウントに対して実行する処理規則をオプションで選択します。この選択は、ほかのすべての選択よりも優先されます。処理規則を指定した場合、このリソースに関するほかの設定に関係なく、すべての行に対して処理が実行されます。これは、プロセス名か、またはプロセス名として評価される規則です。
  - **「処理後のフォーム」** – (詳細設定モードでのみ表示) Active Sync ウィザードで生成されるフォームに追加して実行するフォームをオプションで選択します。このフォームは、Active Sync ウィザードによる設定に優先して適用されます。

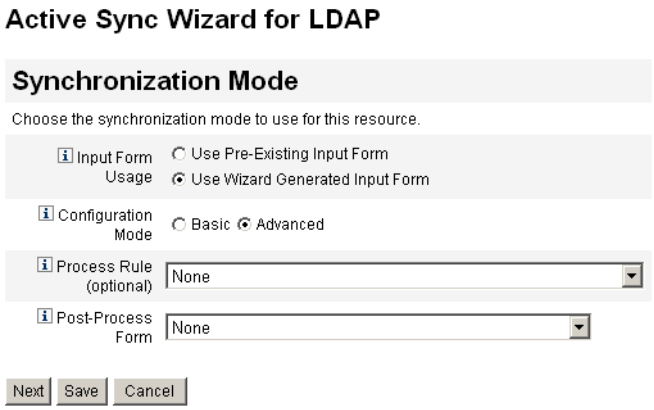


図 3 Active Sync ウィザード：「同期モード」、「ウィザード生成のフォーム」の選択

「次へ」をクリックしてウィザードを続行します。「Active Sync の動作設定」ページが表示されます。

動作設定

このページでは、Active Sync の以下の項目を設定します。

- スタートアップ
- ポーリング
- ログ

スタートアップ設定

Active Sync スタートアップの選択を行います。

- **「スタートアップタイプ」** ― 次のいずれかを選択します。
  - **「自動」**または**「フェイルオーバー付自動」** ― アイデンティティーシステムの開始時にこの権限ソースを開始します。
  - **「手動」** ― 管理者が権限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。
- **「プロキシ管理者」** ― 更新を処理する管理者を選択します。すべての操作は、この管理者に割り当てられた機能を通して承認されます。ユーザーフォームが空のプロキシ管理者を選択する必要があります。

ポーリング設定

ポーリング開始日と時刻を将来の日時に設定すると、指定した日時にポーリングが開始します。ポーリング開始日と時刻を過去の日時に設定すると、Identity Manager はこの情報とポーリング間隔に基づいて、いつポーリングを開始するかを決定します。次に例を示します。

- リソースのアクティブな同期を 2005 年 7 月 18 日 (火曜) に設定
- リソースのポールを週単位で、開始日を 2005 年 7 月 4 日 (月曜)、時刻を午前 9 時に設定

この場合、リソースのポーリングは 2005 年 7 月 25 日 (次の月曜) に開始されます。

開始日または開始時刻を指定しない場合、ただちにリソースのポーリングが開始されます。ただし、開始日と開始時刻を設定するようお勧めします。設定しない場合、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。

ポーリングの設定の選択を行います。

- **「ポール間隔」** ― ポールを行う頻度を指定します。数値を入力し、次に時間の単位 (日、時間、分、月、秒、または週) を選択します。デフォルトの単位は分です。

- **「ポーリング開始日」** ― 最初にスケジューリング間隔を開始する日付を yyyyMMdd 形式で入力します。
- **「ポーリング開始時刻」** ― 最初にスケジューリング間隔を開始する時刻を HH:mm:ss 形式で入力します。

ログ設定

ログ情報およびログレベルの設定の選択を行います。

- **「ログアーカイブの最大数」** ― 値が 0 (ゼロ) より大きい場合、最新の N 個のログファイルが保持されます。0 (ゼロ) の場合は 1 つのログファイルが繰り返し利用されます。-1 の場合、ログファイルは破棄されません。
- **「アクティブログの最大有効期間」** ― この期間を経過すると、アクティブログはアーカイブされます。期間が 0 (ゼロ) の場合、期間ベースのアーカイブは行われません。ログアーカイブの最大数が 0 (ゼロ) に設定されている場合、この期間が経過してもアーカイブは行われず、アクティブログは切り捨てられ、再使用されます。この有効期間条件は、「ログファイルの最大サイズ」に指定される条件とは別に評価されます。

  数値を入力し、次に時間の単位 (日、時間、分、月、秒、または週) を選択します。デフォルトの単位は日です。
- **「ログファイルパス」** ― アクティブログとアーカイブされたログのファイルが作成されるディレクトリへのパスを入力します。ログファイル名はリソース名から開始します。
- **「ログファイルの最大サイズ」** ― アクティブログファイルの最大サイズをバイト数で入力します。指定した最大サイズに達すると、アクティブログファイルはアーカイブされます。ログアーカイブの最大数が 0 (ゼロ) に設定されている場合、この期間が経過してもアーカイブは行われず、アクティブログは切り捨てられ、再使用されます。このサイズ条件は、「アクティブログの最大有効期間」に指定される条件とは別に評価されます。
- **「ログレベル」** ― ログのレベルを入力します。
  - 0 ― ログなし
  - 1 ― エラー
  - 2 ― 情報
  - 3 ― 詳細
  - 4 ― デバッグ

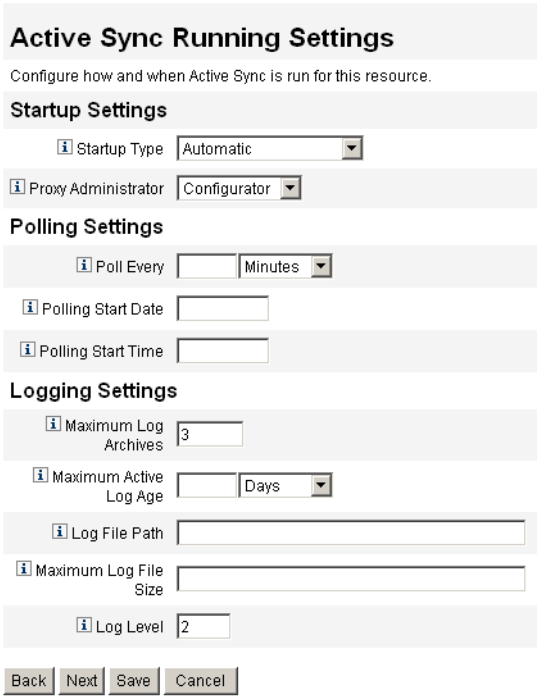


図 4 Active Sync ウィザード : 動作設定

「次へ」をクリックしてウィザードを続行します。「Active Sync の一般設定」ページが表示されます。

一般の Active Sync 設定

このページを使用して、一般的な Active Sync の設定パラメータを指定します。

リソース固有の設定

注 利用可能なリソース固有の設定は、リソースタイプによって異なります。次の 1 つまたは複数の選択は、表示されない場合があります。次の設定は、LDAP リソースに適用されます。

- **「同期するオブジェクトクラス」** – 同期させるオブジェクトクラスを入力します。変更ログはすべてのオブジェクトに対してですが、このフィルタは、ここでリストされたオブジェクトクラスのみを更新します。

- **「同期させるアカウントの LDAP フィルタ」**－同期させるオブジェクトの LDAP フィルタをオプションとして指定します。変更ログはすべてのオブジェクトに対してですが、このフィルタは、指定されたフィルタと一致するオブジェクトのみを更新します。フィルタを指定した場合、フィルタと一致し、同期されるオブジェクトクラスを含むオブジェクトだけが同期されます。
- **「同期する属性」**－ 同期する属性名を指定します。変更ログファイルからの更新のうち、指定属性以外の更新は無視されます。たとえば、部署属性のみを指定した場合、部署属性に影響する変更のみが処理されます。それ以外の更新は無視されます。空欄 (デフォルト) の場合、すべての変更が処理されます。
- **「変更ログブロックサイズ」**－クエリーをフェッチする変更ログエントリ数を入力します。デフォルトの数は 100 です。
- **「変更番号属性名」**－変更ログエントリ中の変更番号属性の名前を入力します。
- **「変更者フィルタ」**－変更からフィルタするディレクトリ管理者の名前 (RDN) を入力します。このリストのエントリに属性修正者名が一致する変更がフィルタされます。

標準値は、ループを防ぐため、このアダプタにより使用される管理者名です。エントリは、cn= ディレクトリマネージャの形式です。

共通の設定

- **「相関規則」**－ リソースの調整ポリシーに指定されている相関規則に優先して適用される相関規則をオプションで指定します。相関規則は、リソースアカウントをアイデンティティーシステムアカウントに相互に関連付けます。
- **「確認規則」**－ リソースの調整ポリシーに指定されている確認規則に優先して適用される確認規則をオプションで指定します。
- **「プロセス解決規則」**－ フィード内の複数のレコードと一致した場合に実行する TaskDefinition の名前をオプションで指定します。これは、管理者に手動アクションを求めるプロセスである必要があります。これは、プロセス名か、またはプロセス名として評価される規則です。
- **「削除規則」**－ 削除操作を行うかどうかを決定するために、受信するユーザー更新ごとに評価される、true または false を返す規則をオプションで指定します。
- **「一致しないアカウントの作成」**－ true に設定すると、アダプタはアイデンティティーシステム上に存在しないアカウントの作成を試みます。false に設定した場合、アダプタはプロセス解決規則が返すプロセスを使用してアカウントを実行します。
- **「作成イベントで Active Sync リソースを割り当てる」**－ このオプションを選択した場合、Active Sync ソースリソースは作成イベントが検出されたときに作成されるユーザーに割り当てられます。
- **「グローバルで利用」**－ ActiveSync ネームスペースの下のフォームは、受信するアカウント内のすべての属性を常に利用できます。このオプションを選択した場合、グローバルネームスペースでもすべての属性 (accountId を除く) を利用できます。

- **「リセット時に過去の変更を無視する」** ― アダプタの最初の開始時またはリセット時に、過去の変更を無視するよう選択します。アダプタをリセットするには、設定オブジェクトの `IAPI_resourceName` を削除します。このオプションは、すべてのアダプタで利用可能ではありません。
- **「ポール前のワークフロー」** ― 各ポールの直前にオプションとして実行するワークフローを選択します。
- **「ポール後のワークフロー」** ― 各ポールの直後にオプションとして実行するワークフローを選択します。

「保存」または**「次へ」**をクリックして、リソースの一般設定の変更を保存します。

- 既存の入力フォームを使用している場合、**「保存」**をクリックしてウィザードの選択を終了し、リソースリストに戻ります。
- ウィザードで生成した入力フォームを使用している場合、**「次へ」**をクリックして続行します。
  - 「基本」設定モードを使用している場合、「ターゲットリソース」ページが表示されます (この章の「ターゲットリソース」に進む)。
  - 「詳細」設定モードを使用している場合、「イベントタイプ」ページが表示されます。

イベントタイプ

このページを使用して、Active Sync リソースに特定のタイプのイベントの変更が発生したかどうかを確認するメカニズムを設定します。

イベントについて

アクティブな同期イベントは、Active Sync リソースで発生した変更として定義されます。リソースごとにリストされたイベントタイプは、リソースのタイプおよび変更イベントに影響を受けるオブジェクトに応じて異なります。イベントタイプには、作成、削除、更新、無効化、有効化、および名前の変更があります。

イベントの無視

Active Sync イベントを無視するかどうかを決定するメカニズムを選択できます。次のオプションがあります。

- **「なし」** ― どの Active Sync イベントも無視されません。
- **「規則」** ― 規則を使用して Active Sync イベントを無視するかどうかを決定します。このオプションを選択した場合、オプションリストからさらに規則を選択する必要があります。
- **「条件」** ― 条件を使用して Active Sync イベントを無視するかどうかを決定します。このオプションを選択した後、「条件の編集」をクリックして「条件パネル」を使用し、条件を定義します。

イベントタイプを決定するためのオプションは次のとおりです。

- **「なし」**― イベントタイプを決定する方法はありません。
- **「規則」**― 規則を使用してイベントタイプを決定します。このオプションを選択した場合、オプションリストからさらに規則を選択する必要があります。
- **「条件」**―条件を使用してイベントタイプを決定します。このオプションを選択した後、「条件の編集」をクリックして「条件パネル」を使用し、条件を定義します。

「次へ」をクリックしてウィザードを続行します。「プロセスの選択」ページが表示されます。

プロセスの選択

このページを使用して、ユーザー画面がチェックされているときに特定の Active Sync イベントインスタンスまたは Active Sync イベントのタイプに対して実行するワークフローまたはプロセスを選択します。

プロセスモード

Active Sync イベントが発生したときに実行するワークフローまたはプロセスを決定する方法を次の 2 つのモードから選択します。

- **「規則」**― 特定の規則を使用して、それぞれの Active Sync イベントインスタンスに対してどのワークフローまたはプロセスを実行するかを決定します。これは、イベントが発生するたびに規則が実行されることを意味します。

  このオプションを選択した後、規則 (プロセス決定規則) をリストから選択します。

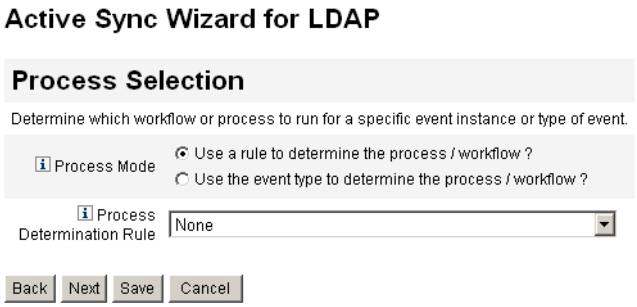


図 5 Active Sync ウィザード : プロセスの選択 (規則)

- **「イベントタイプ」**― それぞれのイベントインスタンスのイベントタイプに基づいて、ワークフローまたはプロセスを実行できます。これは、デフォルトの選択です。

  このオプションを選択した後、リストされているそれぞれのイベントタイプに対して実行するワークフローまたはプロセスを選択します。

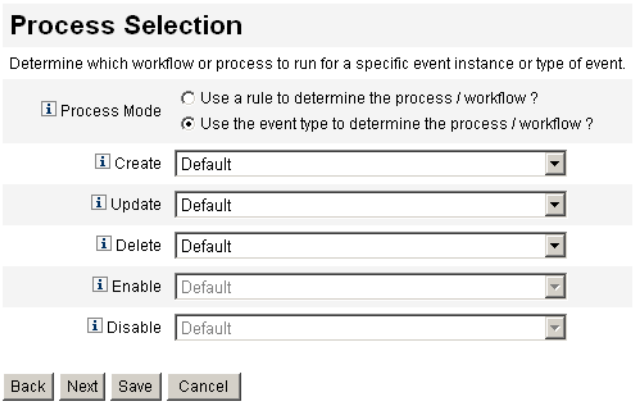


図 6 Active Sync ウィザード : プロセスの選択 (イベントタイプ)

「次へ」をクリックしてウィザードを続行します。「ターゲットリソース」ページが表示されます。

ターゲットリソース

このページを使用して、このリソースと同期させるターゲットリソースを指定します。

1 つ以上のリソースを利用可能なリソースエリアから選択し、ターゲットリソースエリアへ移動します。

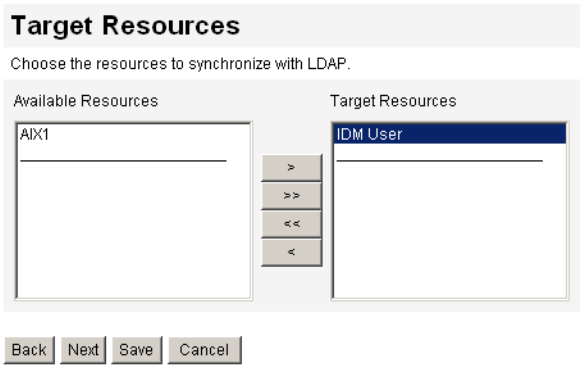


図 7 Active Sync ウィザード : ターゲットリソース

「次へ」をクリックして続行します。「ターゲット属性マッピング」ページが表示されます。

ターゲット属性マッピング

このページを使用して、それぞれのターゲットリソースに対するターゲット属性マッピングを定義します。

オプションリストからターゲットリソースを選択します。ターゲット属性を追加する場合は、**「マッピングの追加」**をクリックします。

それぞれのターゲット属性に対して、属性、タイプ、および属性値を選択します。「適用先」の列では、マッピングを適用する 1 つ以上の操作 (作成、更新、または削除) を選択します。

それぞれのターゲットリソースごとに、手順 1 から 3 を繰り返します。リストから属性行を削除するには、行を選択して**「マッピングの削除」**をクリックします。

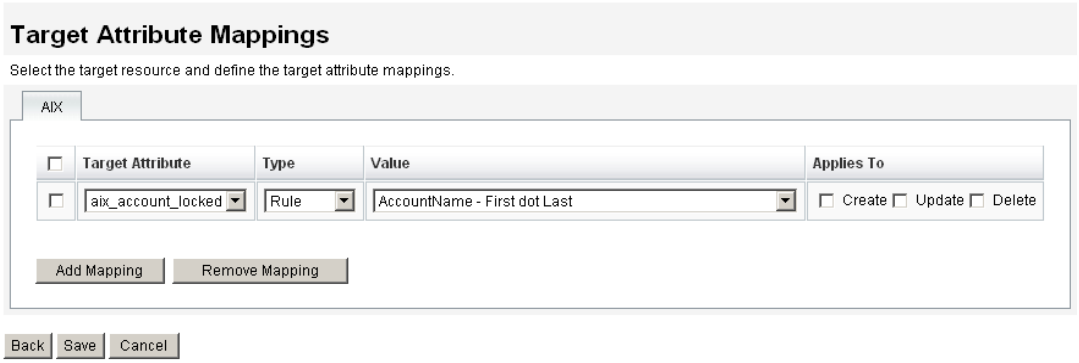


図 8 Active Sync ウィザード : ターゲット属性マッピング

「保存」をクリックして、属性マッピングを保存し、リソースリストに戻ります。

ActiveSync アダプタの編集

ActiveSync アダプタを編集する前に、アクティブな同期を停止する必要があります。「動作設定」ページで、スタートアップタイプを「無効」と選択します。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。

注 リソースに対してアクティブな同期を無効にすると、リソースの保存時に Active Sync タスクが停止されます。

クラスタ環境でのアクティブな同期

エラーステータスインジケータは、リソースに対してアクティブな同期を実行する Identity Manager サーバー上にのみ存在します。

ActiveSync アダプタのパフォーマンスのチューニング

アクティブな同期はバックグラウンドタスクであるため、ActiveSync アダプタ設定によってはサーバーのパフォーマンスが影響を受ける可能性があります。次のタスクを実行して、ActiveSync アダプタのパフォーマンスをチューニングします。

- ポーリング間隔の変更
- アダプタを実行するホストの指定
- 開始と停止
- アダプタログの管理

ActiveSync アダプタは、リソースリストを通じて管理します。ActiveSync アダプタを選択し、「リソースアクション」リストから処理を制御する実行、停止、ステータス更新を利用してください。

ポーリング間隔の変更

- ポーリング間隔は、ActiveSync アダプタが新しい情報の処理を開始する時期を決定します。ポーリング間隔は、実行するアクティビティーのタイプに基づいて決定する必要があります。たとえば、アダプタがデータベースから多数のユーザーのリストを読み込むたびに、Identity Manager の全ユーザーを更新する場合、この処理を毎日早朝に実行するとします。アダプタによっては処理する新しい項目を即座に検索するため、10 秒ごとに実行するよう設定できるかもしれません。

アダプタを実行するホストの指定

アダプタを実行するホストを指定するには、`waveset.properties` ファイルを編集します。このファイルで、次のいずれかを編集できます。

- `sources.hosts=hostname1,hostname2,hostname3` と設定します。これにより、ActiveSync アダプタを実行するマシンのホスト名がリストされます。アダプタは、このフィールドで最初に利用可能なホスト上で実行されます。

  または

- `sources.hosts=localhost` と設定します。

後者に設定すると、アダプタは、アダプタが設定された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。

メモリと CPU サイクルを多く必要とする ActiveSync アダプタは、専用のサーバー上で実行するように設定して、システムの負荷を分散することができます。

開始と停止

ActiveSync アダプタは、NT でのサービスと同様に、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。また、Identity Manager 管理者として実行するよう割り当てる必要もあります。この管理者は、ActiveSync アダプタが実行可能な操作のアクセス権を調査し、変更を行った管理者として監査ログにリストされます。オプションの属性には、ログファイルサイズとパス、ログレベルがあります。

自動に設定すると、アプリケーションサーバーが再起動したときにアダプタが再起動されます。Åú アダプタを開始すると、アダプタは指定したポーリング間隔で即座に実行します。アダプタを停止すると、アダプタは次回に停止フラグを検出したときに停止します。

アダプタログ

アダプタログは、現在処理中のアダプタの情報を取得します。ログが取得する詳細の量は、設定したログレベルに応じて異なります。アダプタログは、問題のデバッグとアダプタプロセスの進行状況の監視に役立ちます。

各アダプタには独自のログファイル、パス、およびログレベルがあります。これらの値は「動作設定」ページで指定します。

アダプタログの削除

アダプタログは、アダプタが停止されたときにのみ削除しなければなりません。ほとんどの場合は、ログを削除する前に、ログをコピーしてアーカイブしておきます。

7 セキュリティー

この章では、Identity Manager セキュリティー機能と、セキュリティー上のリスクを軽減するための手順について詳しく説明します。

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。

- アカウントへのアクセスの即時無効化 ー Identity Manager では、1 回の操作で組織または個々のアクセス権限を無効にすることができます。
- アクティブリスク分析 ー Identity Manager では、非アクティブなアカウントや疑わしいパスワードのアクティビティーなどのセキュリティー上のリスクを絶えずスキャンします。
- 包括的なパスワード管理 ー 完全で柔軟性に富んだパスワード管理機能によって、完全なアクセス管理が保証されます。
- 監査およびレポートによるアクセスのアクティビティーの監視 ー 一連のレポートを実行して、アクセスのアクティビティーについての対象を絞った情報を提供します (レポート機能の詳細については、レポートを参照)。
- サーバーキーの暗号化 ー Identity Manager では、「タスク」エリアでサーバー暗号化キーを作成および管理できます。

また、システムアーキテクチャによってセキュリティー上のリスクを可能な限り軽減するようにしています。たとえば、一度ログアウトすると、ブラウザの「戻る」機能を使用しても、以前にアクセスしたページにアクセスすることはできません。

パスワード管理

Identity Manager は、複数のレベルでパスワード管理を実行します。

- **変更の管理**
  - ユーザーのパスワードを複数の場所から変更する (**「ユーザーの編集」**、**「ユーザーの検索」**、または **「パスワードの変更」** ページ)
  - リソースを細分化して選択することにより、ユーザーの任意のリソースでパスワードを変更する
- **パスワードリセットの管理**
  - ランダムなパスワードを生成する
  - パスワードをエンドユーザーまたは管理者に表示する

- **ユーザーによるパスワードの変更**
  - http://*localhost*:8080/idm/user 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
  - オプションとして、エンドユーザーの環境に適するように自己管理ページをカスタマイズする
- **ユーザーによるデータの更新**
  - エンドユーザーが管理するユーザーのスキーマ属性をセットアップする
- **ユーザーによるアクセスの復旧**
  - 認証質問を使用して、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

パススルー認証

パススルー認証を使用して、1 つ以上の異なるパスワードによるアクセス権をユーザーと管理者に与えます。Identity Manager は、次のものを実装することによって認証を管理します。

- ログインアプリケーション (ログインモジュールグループの集まり)
- ログインモジュールグループ (順序づけされたログインモジュールのセット)
- ログインモジュール (割り当てられたリソースごとに認証を設定し、認証の成功条件を複数ある中から 1 つ指定する)

ログインアプリケーションについて

ログインアプリケーションはログインモジュールグループの集まりを定義し、さらにログインモジュールグループはユーザーが Identity Manager にログインするときに使用するログインモジュールのセットと順序を定義します。各ログインアプリケーションは 1 つ以上のログインモジュールグループで構成されます。

ログインアプリケーションは、ログイン時にログインモジュールグループのセットをチェックします。設定されているログインモジュールグループが 1 つだけの場合は、そのログインモジュールグループが使用され、それに含まれるログインモジュールがグループ内で定義された順序で処理されます。ログインアプリケーションに複数のログインモジュールグループが定義されている場合には、Identity Manager が各ログインモジュールに適用されるログイン制約規則をチェックして、処理するグループを決定します。

ログイン制約規則

ログイン制約規則は、ログインアプリケーションに定義されているログインモジュールグループに対して適用されます。ログインアプリケーションのログインモジュールグループの各セットの中で、1 つのログインモジュールグループだけは適用されるログイン制約を持つことができません。

セットの中のどのログインモジュールグループを処理するかを決めるにあたって、Identity Manager は最初のログインモジュールグループの制約規則を評価します。評価が成功した場合は、そのログインモジュールグループが処理されます。評価に失敗すると、制約規則が成功するかまたは制約規則を持たないログインモジュールグループが評価された後に使用されるまで、各ログインモジュールグループが次々に評価されます。

注　ログインアプリケーションに複数のログインモジュールグループが含まれる場合には、ログイン制約規則を持たないログインモジュールグループをセットの最後の位置に置くようにしてください。

ログイン制約規則の例

次に示す場所に基づいたログイン制約規則の例では、規則がヘッダーから要求側の 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。

```
<Rule authType='LoginConstraintRule' name='Sample On Local Network'>
  <match>
    <ref>remoteAddr</ref>
    <s>192.168.</s>
  </match>
  <MemberObjectGroups>
    <ObjectRef type='ObjectGroup' name='All'/>
  </MemberObjectGroups>
</Rule>
```

ログインアプリケーションの編集

メニューバーで、**「設定」**を選択してから**「ログイン」**を選択して、「ログイン」ページにアクセスします。

ログインアプリケーションリストには次の内容が表示されます。

- 定義済みの各 Identity Manager ログインアプリケーション (インタフェース)
- ログインアプリケーションを構成するログインモジュールグループ
- 各ログインアプリケーションに設定された Identity Manager セッションのタイムアウト制限

「ログイン」ページから次の操作を行えます。

- カスタムログインアプリケーションの作成

- カスタムログインアプリケーションの削除
- ログインモジュールグループの管理

ログインアプリケーションを編集するには、リストからログインアプリケーションを選択します。

Identity Manager セッション制限の設定

「ログイン設定の修正」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。

アプリケーションへのアクセスの無効化

「ログインアプリケーションの作成」ページと「ログインアプリケーションの修正」ページで、「無効化」オプションを選択してログインアプリケーションを無効化し、ユーザーがログインできないようにすることができます。ユーザーが無効化されたアプリケーションにログインしようとすると、インタフェースによって、アプリケーションが現在無効にされていることを示す代替ページにリダイレクトされます。カスタムカタログを編集することで、このページに表示されるメッセージを編集することができます。

このオプションの選択を解除するまで、ログインアプリケーションは無効にされたままになります。安全措置として、管理者ログインは無効化できません。

ログインモジュールグループの編集

ログインモジュールグループリストには次の内容が表示されます。

- 定義済みの各 Identity Manager ログインモジュールグループ
- 各ログインモジュールグループに含まれるログインモジュール
- ログインモジュールグループに制約規則が含まれるかどうか

「ログインモジュールグループ」ページから、ログインモジュールグループを作成、編集、削除できます。リストからログインモジュールグループを 1 つ選択して、それを編集します。

ログインモジュールの編集

詳細を入力するか、ログインモジュールに関して次のように選択します (すべてのオプションがどのログインモジュールでも選択できるとは限らない)。

- **「ログイン成功条件」** ― このモジュールに適用する条件を選択します。次の中から選択できます。

- **「必須」** – 成功するにはそのログインモジュールが必要です。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。ログインモジュールが 1 つしかない場合、管理者は正常にログインします。
- **「必要条件」** – 成功するにはそのログインモジュールが必要です。成功すると、認証はリスト内の次のログインモジュールに進みます。失敗した場合、認証は続行しません。
- **「十分条件」** – 成功するためにそのログインモジュールが必要ではありません。成功すると、認証は次のログインモジュールに進まず、管理者は正常にログインします。失敗した場合、認証はリスト内の次のログインモジュールに進みます。
- **「オプション」** – 成功するためにそのログインモジュールが必要ではありません。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。

- **「ログイン検索属性」** – (LDAP のみ) 関連する LDAP サーバーへのバインド (ログイン) 試行時に使用する、LDAP ユーザー属性名の順序付けられたリストを指定します。指定したユーザーのログイン名とともに、指定された LDAP ユーザー属性を使用して、一致する LDAP ユーザーを順番に検索します。これにより、LDAP へのパススルーが設定されている場合、LDAP の cn 属性または電子メールアドレス属性により、ユーザーは Identity Manager にログインできます。

  たとえば、次のように指定するとします。

  ```
  cn
  mail
  ```

  そして、ユーザーは gwilson としてログインしようとするとします。このとき LDAP リソースはまず `cn=gwilson` という条件で LDAP ユーザーの検索を試行します。これに成功すると、そのユーザーによって指定されたパスワードでバインドを試みます。成功しない場合、LDAP リソースは `mail=gwilson` という条件で LDAP ユーザーを検索します。これにも失敗すると、ログインが失敗します。

  値を指定しない場合のデフォルト LDAP 検索属性は次のとおりです。

  ```
  uid
  cn
  ```

- **「ログイン相関規則」** – ログイン情報と Identity Manager ユーザーのマッピングに使用されるログイン相関規則を選択します。選択する規則は、LoginCorrelationRule authType を持つ必要があります。
- **「新規ユーザー命名規則」** – ログインの一環として新規 Identity Manager ユーザーを自動的に作成する場合に使用される、新規ユーザー命名規則を選択します。

「保存」 をクリックして、ログインモジュールを保存します。一度保存すると、このモジュールをログインモジュールグループ内のほかのすべてのモジュールと関連づけて配置できます。

警告 Identity Manager ログインが複数のシステムから認証を受けるよう設定する場合は、Identity Manager の認証のターゲットとなるすべてのシステムで、アカウントのユーザー ID とパスワードを同じにすることを推奨します。

ユーザー ID とパスワードの組み合わせが異なる場合、ユーザー ID およびパスワードが「Identity Manager ユーザーログイン」フォームに入力されたユーザー ID およびパスワードと一致しないシステムで、ログインが失敗します。これらのシステムの中には、ログイン試行回数が一定数を超えるとアカウントを強制的にロックするロックアウトポリシーを持つものもあります。このようなシステムでは、Identity Manager によるユーザーのログインが成功し続けた場合でも、ユーザーアカウントは最終的にロックされます。

共通リソースの認証の設定

物理的または論理的に同一の複数のリソースがある場合 (たとえば、同一の物理ホストに対して定義された 2 つのリソース、NT または AD ドメイン環境内の信頼できるドメインを表す複数のリソース)、システム設定オブジェクト内でそれらのリソースのセットを「共通リソース」として指定することができます。

リソースを共通リソースとして設定することで、あるユーザーを共通リソースの 1 つのリソースに対して認証しながら、共通リソースの別のリソースを使用してそのユーザーの関連付けられた Identity Manager ユーザーにマップすることができます。たとえば、あるユーザーのリソース AD-1 に対するリソースアカウントが、自分の Identity Manager ユーザーにリンクされているとします。ログインモジュールグループでは、ユーザーがリソース AD-2 を認証する必要があることが定義されているとします。AD-1 と AD-2 が、共通リソースとして定義されている場合 (この場合、同じ信頼できるドメイン内にある)、ユーザーが AD-2 に対して正常に認証されると、Identity Manager はリソース AD-1 で同じ accountId を持つユーザーを見つけることによって、関連付けられた Identity Manager ユーザーにマップすることができます。

このシステム設定オブジェクトの属性は次の形式で指定します。

```
<Attribute name='common resources'>
    <Attribute name='Common Resource Group Name'>
        <List>
            <String>Common Resource Name</String>
            <String>Common Resource Name</String>
        </List
    </Attribute>
</Attribute>
```

X509 証明書認証の設定

次の情報と手順を使用して、Identity Manager の X509 証明書認証を設定します。

前提条件

Identity Manager で X509 証明書ベースの認証をサポートするには、クライアントとサーバーの 2 方向の SSL 認証が正しく設定されているかを確認します。クライアントの観点では、これは、X509 準拠のユーザー証明書がブラウザにインポートされ (またはスマートカードリーダーで利用可能で)、ユーザー証明書に署名するために使用された信頼できる証明書が、Web アプリケーションサーバーの信頼できる証明書のキーストアにインポートされている必要があることを意味します。

さらに、使用したクライアント証明書がクライアント認証のために選択されている必要があります。これを確認するには、次を実行します。

1. Internet Explorer を使用して、**「ツール」**を選択し、**「インターネットオプション」**を選択します。
2. **「コンテンツ」**タブを選択します。
3. 「証明書」エリアで、**「証明書」**をクリックします。
4. クライアント証明書を選択し、**「詳細」**をクリックします。
5. 「証明書の目的」エリアで、「クライアント認証」オプションが選択されていることを確認します。

Identity Manager での X509 証明書認証の設定

Identity Manager で X509 証明書認証を設定するには、次を実行します。

1. 管理者インタフェースに設定者 (または同等の権限を持つユーザー) としてログインします。
2. **「設定」**を選択し、**「ログイン」**を選択して、「ログイン」ページを表示します。
3. **「ログインモジュールグループの管理」**をクリックし、「ログインモジュールグループ」ページを表示します。
4. リストからログインモジュールグループを選択します。
5. 「ログインモジュールの割り当て」リストから「Identity Manager X509 証明書ログインモジュール」を選択します。「ログインモジュールグループの修正」ページが表示されます。
6. ログインの成功条件を設定します。使用可能な値は次のとおりです。
   - **「必須」**― 成功するにはそのログインモジュールが必要です。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。ログインモジュールが 1 つしかない場合、管理者は正常にログインします。

- **「必要条件」** ― 成功するにはそのログインモジュールが必要です。成功すると、認証はリスト内の次のログインモジュールに進みます。失敗した場合、認証は続行しません。
- **「十分条件」** ― 成功するためにそのログインモジュールが必要ではありません。成功すると、認証は次のログインモジュールに進まず、管理者は正常にログインします。失敗した場合、認証はリスト内の次のログインモジュールに進みます。
- **「オプション」** ― 成功するためにそのログインモジュールが必要ではありません。成功か失敗かに関係なく、認証はリスト内の次のログインモジュールに進みます。

7. ログイン相関規則を選択します。組み込み規則またはカスタム相関規則を選択できます (カスタム相関規則の作成については、次の節を参照)。
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. オプションで、ログインモジュールの順序を変更し (複数のログインモジュールがログインモジュールグループに割り当てられている場合)、**「保存」** をクリックします。
10. ログインモジュールグループがログインアプリケーションに割り当てられていない場合はここで割り当てます。「ログインモジュールグループ」ページで、「ログインアプリケーションに戻る」をクリックし、ログインアプリケーションを選択します。ログインモジュールグループをログインアプリケーションに割り当てたら、**「保存」** をクリックします。

注 `waveset.properties` ファイルで `allowLoginWithNoPreexistingUser` オプションの値が true に設定されている場合、「Identity Manager X509 証明書ログインモジュール」を設定するときに、新規ユーザー命名規則を選択するように要求されます。この規則は、関連付けられたログイン相関規則によってユーザーが検出されないときに作成される新しいユーザーの命名方法を決定するために使用されます。

新規ユーザー命名規則では、ログイン相関規則と同じ入力引数を使用できます。この規則は、1 つの文字列を返し、これが、新しい Identity Manager ユーザーアカウントを作成するためのユーザー名として使用されます。

サンプルの新規ユーザー命名規則が、`NewUserNameRules.xml` という名前で `idm/sample/rules` にあります。

ログイン設定規則の作成とインポート

ログイン相関規則は、Identity Manager X509 証明書ログインモジュールによって、証明書データを適切な Identity Manager ユーザーにマップする方法を決定するために使用されます。Identity Manager には、「X509 証明書 subjectDN を使用した相関」という名前の組み込み相関規則が 1 つ用意されています。

独自の相関規則を追加することもできます。各相関規則は、次のガイドラインに従っている必要があります。

- `authType` 属性は `LoginCorrelationRule` に設定する必要があります (`<LoginCorrelationRule>` 要素で authType='LoginCorrelationRule' に設定する)。
- 相関規則は、関連付けられた Identity Manager ユーザーを検出するためにログインモジュールが使用する `AttributeConditions` のリストのインスタンスを返す必要があります。たとえば、ログイン相関規則は、関連付けられた Identity Manager ユーザーを電子メールアドレスによって検索する `AttributeCondition` を返す場合があります。

次の引数がログイン設定規則に渡されます。

- 標準の X509 証明書フィールド (`subjectDN`、`issuerDN`、有効な日付など)
- 重要な拡張プロパティーと重要ではない拡張プロパティー

次の証明書引数の命名規則がログイン相関規則に渡されます。

```
cert.field name.subfield name
```

次の例のような引数名を規則で使用できます。

- `cert.subjectDN`
- `cert.issuerDN`
- `cert.notValidAfter`
- `cert.notValidBefore`
- `cert.serialNumber`

ログイン設定規則は、渡された引数を使用して、1 つ以上の `AttributeConditions` のリストを返します。Identity Manager X509 証明書ログインモジュールは、これらを使用して関連付けられた Identity Manager ユーザーを検出します。

サンプルのログイン相関規則が、`LoginCorrelationRules.xml` という名前で、`idm/sample/rules` にあります。

カスタム相関規則を作成したら、その規則を Identity Manager にインポートする必要があります。管理者インタフェースで、**「設定」**を選択し、**「交換ファイルのインポート」**を選択して、ファイルインポート機能を使用します。

SSL 接続のテスト

SSL 接続をテストするには、SSL を介して、設定済みのアプリケーションインタフェースの URL (例 : https//idm007:7002/idm/user/login.jsp) にアクセスします。セキュアなサイトに入ったことを知らせるメッセージが表示され、Web サーバーに送信する個人用証明書を指定するように要求されます。

問題の診断

X509 証明書を使用した認証に関する問題は、ログインフォーム上でエラーメッセージとして報告されます。詳しい診断情報を得るには、Identity Manager サーバーで次のクラスとレベルのトレースを有効にします。

- `com.waveset.session.SessionFactory 1`
- `com.waveset.security.authn.WSX509CertLoginModule 1`
- `com.waveset.security.authn.LoginModule 1`

http 要求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 要求内に見つからないことを知らせるメッセージが表示されます。これを解決するには、次を実行します。

1. `SessionFactory` のトレースを有効にして、http 属性の完全なリストを表示し、X509Certificate の名前を特定します。
2. Identity Manager デバッグ機能を使用して、`LoginConfig` オブジェクトを編集します。
3. Identity Manager X509 証明書ログインモジュールの `<LoginConfigEntry>` 内の `<AuthnProperty>` の名前を正しい名前に変更します。
4. 保存して、もう一度試します。

さらに、Identity Manager X509 証明書ログインモジュールをログインアプリケーションから削除して、もう一度追加することが必要な場合があります。

暗号化の使用と管理

暗号化は、メモリーおよびリポジトリ内のサーバーデータだけでなく、サーバーとゲートウェイの間で送信されるすべてのデータの機密性と完全性を保証するために使用されます。

続く節では、Identity Manager サーバーとゲートウェイで暗号化が使用および管理される方法を詳しく説明し、サーバーとゲートウェイの暗号化キーに関する質問を検討します。

暗号化によって保護されるデータ

次の表は、Identity Manager 製品で暗号化によって保護されるデータの種類と、各データの種類を保護するために使用される暗号を示したものです。

データの種類	**RSA MD5**	**NIST トリプル DES 168 ビットキー (DESede/ECB/NoPadding)**	**PKCS#5 パスワードベースの暗号化 56 ビットキー (PBEwithMD5andDES)**
サーバー暗号化キー		デフォルト	設定オプション[1]
ゲートウェイ暗号化キー		デフォルト	設定オプション [1]
ポリシー辞書単語			
ユーザーパスワード			
ユーザーパスワード履歴			
ユーザーの回答			
リソースパスワード			
リソースパスワード履歴			
サーバーゲートウェイ間のすべてのペイロード			

1. pbeEncrypt 属性または「サーバー暗号化の管理」タスクによりシステム設定オブジェクト経由で設定します。

サーバー暗号化キーに関する質問と答え

続く節では、サーバー暗号化キーのソース、場所、保守、使用についてよく尋ねられる質問に答えていますのでご覧ください。

サーバー暗号化キーとは何ですか？

サーバー暗号化キーはトリプル DES 168 ビットの対称キーです。サーバーでサポートされるキーには 2 つのタイプがあります。

- **デフォルトキー** ― このキーはコンパイル時にサーバーコードに組み込まれます。
- **ランダムに生成されるキー** ― このキーは、サーバーの最初の起動時、または現在のキーのセキュリティーに不安がある場合にいつでも生成することができます。

サーバー暗号化キーはどこで維持管理されますか？

サーバー暗号化キーはリポジトリで維持管理されるオブジェクトです。どのリポジトリにも多数のデータ暗号化キーがある可能性があります。

暗号化されたデータの復号化や再暗号化にどのキーを使用するかを、サーバーはどのようにして認識するのですか？

リポジトリに格納された各暗号化データの先頭には、そのデータを暗号化する際に使用したサーバー暗号化キーの ID が付加されます。暗号化データを含むオブジェクトがメモリーに読み込まれると、Identity Manager はその暗号化データ の ID プレフィックスに関連づけられたサーバー暗号化キーを使用して復号化し、データが変更されている場合には同じキーで再暗号化します。

サーバー暗号化キーはどのようにして更新しますか？

Identity Manager には「サーバー暗号化の管理」というタスクが用意されています。このタスクを使用することにより、承認されたセキュリティー管理者は次のようなキー管理タスクを実行することができます。

- 新しい現在のサーバーキーの生成
- 現在のサーバーキーを使用して暗号化したデータを含む既存オブジェクトに対する、タイプ別の再暗号化

このタスクの使用法の詳細については、この章の「サーバー暗号化の管理」を参照してください。

現在のサーバーキーが変更された場合、既存の暗号化データはどうなりますか？

何も問題はありません。既存の暗号化データは、引き続き、暗号化データの ID プレフィックスで参照されているキーを使用して復号化や再暗号化されます。新しいサーバー暗号化キーが生成され、そのキーが現在のキーに設定された場合、新たに暗号化されるデータには新しいサーバーキーが使用されます。

注　サーバー暗号化キーがいずれかのオブジェクトの暗号化データによって参照されている場合、そのサーバー暗号化キーをリポジトリから削除しないでおくことはとても重要です。削除すると、サーバーはその暗号化データを復号化できなくなります。暗号化データを含むオブジェクトを別のリポジトリからインポートする場合、そのオブジェクトを正常にインポートするために、関連づけられているサーバー暗号化キーを先にインポートする必要があります。

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。

サーバーキーはどのように保護されますか？

サーバーがパスワードベースの暗号化 (PBE) - PKCS#5 暗号化を使用するよう `pbeEncrypt` 属性または「サーバー暗号化の管理」タスクによって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 暗号化を有効化するには、暗号 PBEwithMD5andDES が使用できなければなりません。この暗号は Identity Manager にはデフォルトでパッケージされていませんが、Sun や IBM が提供する実装をはじめ、多くの JCE プロバイダ実装で使用可能な PKCS#5 標準です。

サーバーキーを安全な外部記憶装置にエクスポートしてもよいですか？

はい。サーバーキーが PBE 暗号化されている場合、エクスポートの前に、サーバーキーは復号化されてデフォルトキーで再暗号化されます。これにより、それ以後ローカルサーバー PBE キーに依存することなく、同じサーバーまたは別のサーバーにサーバーキーをインポートできるようになります。サーバーキーがデフォルトキーで暗号化されている場合は、エクスポート前の事前処理は行われません。

サーバーキーをサーバーにインポートするときには、サーバーが PBE キー用に設定されていればキーが復号化され、次いで、そのサーバーが PBE キー暗号化用に設定されていればローカルサーバーの PBE キーで再暗号化されます。

どのデータがサーバーとゲートウェイの間で暗号化されますか？

サーバーとゲートウェイの間で送信されるすべてのデータ (ペイロード) が、ランダムに生成されたサーバーゲートウェイセッション対称 168 ビットキーを使用してトリプル DES で暗号化されます。

ゲートウェイキーに関する質問と答え

続く節では、ゲートウェイのソース、記憶装置、配布、保護についてよく尋ねられる質問に答えていますのでご覧ください。

データの暗号化または復号化に使用するゲートウェイキーとは何ですか？

Identity Manager サーバーがゲートウェイに接続するたびに、初期ハンドシェークによって新規のランダム 168 ビットのトリプル DES セッションキーが生成されます。それ以降サーバーとゲートウェイの間で送信されるすべてのデータは、このキーを使用して暗号化または復号化されます。サーバー / ゲートウェイのペアごとに一意のセッションキーが生成されます。

ゲートウェイキーはどのようにしてゲートウェイに配布されますか？

セッションキーはサーバーによってランダムに生成された後、初期サーバーゲートウェイ間ハンドシェークの一環として共有秘密マスターキーによって暗号化されることにより、サーバーとゲートウェイの間でセキュアに交換されます。

初期ハンドシェーク時に、サーバーはゲートウェイに問い合わせて、ゲートウェイがサポートするモードを判別します。ゲートウェイは次の 2 つのモードで作動します。

- **「デフォルト」モード** – サーバーゲートウェイ間の初期プロトコルハンドシェークは、コンパイル時にサーバーコードに組み込まれている、デフォルトの 168 ビットトリプル DES キーで暗号化されます。
- **「セキュア」モード** – 共有リポジトリを使用する、ランダムな 168 ビットキーであるトリプル DES ゲートウェイキーが生成され、初期ハンドシェークプロトコルの一環としてサーバーからゲートウェイに送信されます。このゲートウェイキーは他の暗号化キーと同様にサーバーリポジトリに格納され、ゲートウェイによりゲートウェイ自身のローカルレジストリにも格納されます。

  セキュアモードでかつサーバーがゲートウェイに接続している場合、サーバーはテストデータをゲートウェイキーで暗号化してゲートウェイに送信します。ゲートウェイはテストデータの復号化を試み、テストデータにゲートウェイ固有のデータを追加してから、元のデータと追加したデータの両方を再暗号化してサーバーに送り返します。サーバーがテストデータとゲートウェイ固有のデータを正常に復号化できた場合、サーバーはサーバーゲートウェイ間用に一意のセッションキーを生成し、それをゲートウェイキーで暗号化してゲ—トウェイに送信します。ゲートウェイはセッションキーを受け取ると、すぐに復号化し、サーバーゲートウェイ間のセッションが持続する間そのキーを保持して使用します。サーバーがテストデータとゲートウェイ固有のデータを正常に復号化できない場合、サーバーはデフォルトキーを使用してゲートウェイキーを暗号化し、ゲートウェイに送信します。ゲートウェイはコンパイル時に組み込まれたデフォルトキーを使用してゲートウェイキーを復号化し、そのゲートウェイキーをレジストリに格納します。その後、サーバーはそのゲートウェイキーを使ってサーバーゲートウェイ間で一意のセッションキーを暗号化し、セッションキーをゲートウェイに送信して、サーバーゲートウェイ間のセッションが持続する間そのセッションキーを使用します。

  それ以後、ゲートウェイは自身のゲートウェイキーでセッションキーを暗号化したサーバーからの要求のみを受け入れます。ゲートウェイは、起動時にキーのレジストリをチェックします。キーのレジストリがあれば、そのキーを使用します。ない場合は、デフォルトキーを使用します。いったんゲートウェイがレジストリにキーを設定してしまうと、デフォルトキーを使用してセッションを確立することはできなくなります。それにより、だれかが不正なサーバーをセットアップしてゲートウェイに接続することを防げます。

サーバーゲートウェイ間ペイロードの暗号化や復号化に使用するゲートウェイキーを更新できますか？

Identity Manager には「サーバー暗号化の管理」というタスクが用意されており、承認されたセキュリティー管理者はいろいろなキー管理タスクを実行することができます。そのタスクには、新しい現在のゲートウェイキーの生成や生成された現在のゲートウェイキーによるすべてのゲートウェイの更新などが含まれます。このキーはサーバーゲートウェイ間で送信されるすべてのペイロードを保護する、セッション単位のキーを暗号化するために使用されます。新たに生成されるゲートウェイキーは、システム設定の `pbeEncrypt` 属性の値に基づいて、デフォルトキーまたは PBE キーで暗号化されます。

ゲートウェイキーはサーバー上とゲートウェイ上のどこに格納されますか？

サーバー上では、ゲートウェイキーはサーバーキーとまったく同じようにリポジトリに格納されます。ゲートウェイ上では、ローカルレジストリキー内に格納されます。

ゲートウェイキーはどのように保護されますか？

ゲートウェイキーはサーバーキーの場合と同じように保護されます。サーバーが PBE 暗号化を使用するように設定されている場合、ゲートウェイキーは PBE が生成するキーで暗号化されます。このオプションが false に設定されている場合には、ゲートウェイキーはデフォルトキーで暗号化されます。詳細については、前述の「サーバーキーはどのように保護されますか ?」の節を参照してください。

ゲートウェイキーを安全な外部記憶装置にエクスポートしてもよいですか？

ゲートウェイキーは、サーバーキーの場合と同じく、「サーバー暗号化の管理」タスクを使用してエクスポートできます。詳細については、前述の「サーバーキーを安全な外部記憶装置にエクスポートしてもよいですか ?」の節を参照してください。

サーバーキーやゲートウェイキーはどのようにして破棄されますか？

サーバーキーとゲートウェイキーは、サーバーリポジトリからそれらを削除することによって破棄されます。あるキーを使用して暗号化されたサーバーデータがある間や、そのキーに依存するゲートウェイがある間は、そのキーを削除しないように注意してください。「サーバー暗号化の管理」タスクを使用して、現在のサーバーキーですべてのサーバーデータを再暗号化し、現在のゲートウェイキーをすべてのゲートウェイで同期することによって、古いキーを削除する前に、確実にどの古いキーも使用されていない状態になるようにしてください。

サーバー暗号化の管理

Identity Manager のサーバー暗号化機能を使用して、新しい 3DES サーバー暗号化キーを作成してから、3DES または PKCS#5 暗号化を使ってこれらのキーを暗号化できます。サーバー暗号化の管理タスクは、セキュリティー管理者機能を持つユーザーだけが実行でき、**「タスク」**タブからアクセスします。

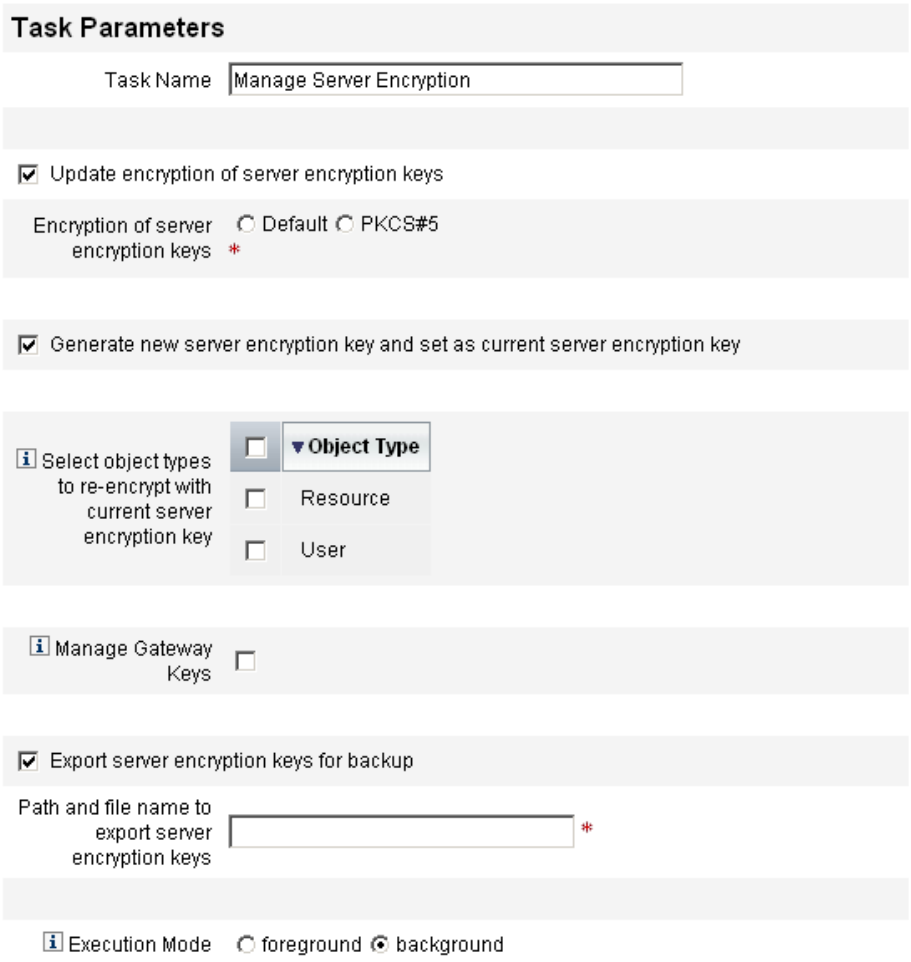


図 1 「サーバー暗号化の管理」タスク

「タスクの実行」を選択し、リストから「サーバー暗号化の管理」を選択して、タスクに関する次の情報を設定します。

- **「サーバー暗号化キーの暗号化の更新」**－サーバー暗号化キーの暗号化を、デフォルトの 3DES 方式または PKCS#5 方式のどちらを使用して行うかを選択します。このオプションを選択すると、2 つの暗号化方式 (「デフォルト」と「PKCS#5」) が表示されるので、どちらかを選択します。
- **「新しいサーバー暗号化キーを生成し、現在のサーバー暗号化キーとして設定する」** － 新しいサーバー暗号化キーを生成する場合に選択します。このオプションを選択した場合は、それ以降に生成される暗号化データでは、このキーが使用されます。新しいサーバー暗号化キーを生成しても、既存の暗号化データに適用されているキーはそのまま使用できます。
- **「現在のサーバー暗号化キーを使用して再暗号化するオブジェクトタイプを選択」** － 1 つ以上の Identity Manager オブジェクトタイプ (リソースやユーザーなど) を選択し、現在の暗号化キーを使用して再度暗号化します。
- **「ゲートウェイ鍵の管理」** － 選択すると、ページに次のゲートウェイキーオプションが表示されます。
  - **「新しい鍵を生成し、すべてのゲートウェイを同期させる」**
    最初からセキュリティー保護されたゲートウェイ環境を有効にする場合は、このオプションを選択します。このオプションは、新しいゲートウェイキーを生成し、それをすべてのゲートウェイに送信します。
  - **「現在のゲートウェイ鍵を使用して、すべてのゲートウェイを同期させる」**
    新しいゲートウェイ、または新しいゲートウェイキーが送信されていないゲートウェイを同期させる場合に選択します。すべてのゲートウェイが現在のゲートウェイキーを使用して同期されている状況で 1 つのゲートウェイが停止した場合、または新規ゲートウェイにキーを更新させる場合は、このオプションを選択します。
- **「バックアップ用にサーバー暗号化キーをエクスポート」** － 既存のサーバー暗号化キーを XML 形式のファイルにエクスポートする場合に選択します。このオプションを選択すると、追加フィールドが表示され、キーをエクスポートするためのパスおよびファイル名を指定できます。Identity Manager

注 PKCS#5 暗号化を使用しているときに、新しいサーバー暗号化キーを生成および設定することを選択した場合には、このオプションも選択する必要があります。さらに、エクスポートしたキーは、リムーバブルメディアに保存した上で、ネットワークに接続されていない安全な場所に保管する必要があります。

- **「実行モード」** － このタスクをバックグラウンド (デフォルトオプション) またはフォアグラウンドのどちらで実行するかを選択します。新しく生成したキーを使用して 1 つ以上のオブジェクトタイプを再暗号化する場合には、時間がかかることがあるため、バックグラウンドで実行することをお勧めします。

セキュリティーの実装

Identity Manager 管理者は、セットアップ時とそれ以降に以下の推奨事項に従うことで、保護されたアカウントおよびデータに対するセキュリティー上のリスクをさらに軽減できます。

セットアップ時

以下の操作を実行する必要があります。

- https を使用するセキュアな Web サーバーを通じて Identity Manager にアクセスする。
- デフォルトの Identity Manager 管理者アカウント (Administrator と Configurator) 用のパスワードをリセットする。これらのアカウントのセキュリティーをさらに向上させるには、アカウント名を変更します。
- 設定者のアカウントへのアクセス権を制限する。
- 管理者の機能セットをその職務権限に必要な操作のみに制限し、組織階層をセットアップして管理者の機能を制限する。
- Identity Manager インデックスリポジトリのデフォルトパスワードを変更する。
- Identity Manager アプリケーションでのアクティビティーの追跡の監査をオンにする。
- Identity Manager ディレクトリのファイルに対する権限を編集する。
- 承認またはほかのチェックポイントを挿入してワークフローをカスタマイズする。
- 復旧手順を作成して、緊急の際に Identity Manager 環境を復旧する方法を記述しておく。

実行時

以下の操作を実行する必要があります。

- デフォルトの Identity Manager 管理者アカウント (Administrator と Configurator) に対する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または認識する。

  アプリケーションサーバーが Servlet 2.2 準拠の場合、Identity Manager のインストールプロセスでは、http セッションのタイムアウトをデフォルトの 30 分に設定します。この値はプロパティーを編集して変更できますが、セキュリティーを向上させるため、この値を低く設定する必要があります。30 分を超える値を設定しないでください。

  セッションのタイムアウト値を変更するには、次を実行します。

1. web.xml ファイルを変更します。
   このファイルは、アプリケーションサーバーのディレクトリツリーの idm/WEB-INF ディレクトリにあります。
2. 次の行の数値を変更します。

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

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。

Identity Manager のレポート機能の使用方法を示す情報および手順については、この章をお読みください。この章で説明する内容は次のとおりです。

- Identity Manager のレポートタイプ。監査ログ、リアルタイム、概要、システムログ、および使用状況の各レポートを含む
- レポートを作成、編集、実行、および電子メールで送信する方法
- レポート情報のダウンロード方法

レポートの操作

Identity Manager では、レポートは特別なタスクカテゴリとみなされます。そのため、Identity Manager 管理者インタフェースの次の 2 つのエリアでレポートを操作します。

- **「レポート」** – レポートを定義、実行、削除、およびダウンロードできます。また、スケジュールされたレポートの管理もできます。
- **「タスク」** – レポートを定義したあとに、「タスク」エリアに移動して、レポートタスクをスケジュールおよび処理します。

レポート

レポート関連のアクティビティーのほとんどは、「レポートの実行」ページから実行できます。このページでは、次のことを実行できます。

- レポートの作成、修正、および削除
- レポートの実行
- Microsoft Excel などの別のアプリケーションで使用するためのレポート情報のダウンロード

このページを表示するには、メニューバーから **「レポート」** を選択します。**「レポートの実行」** サブタブページが表示されます。

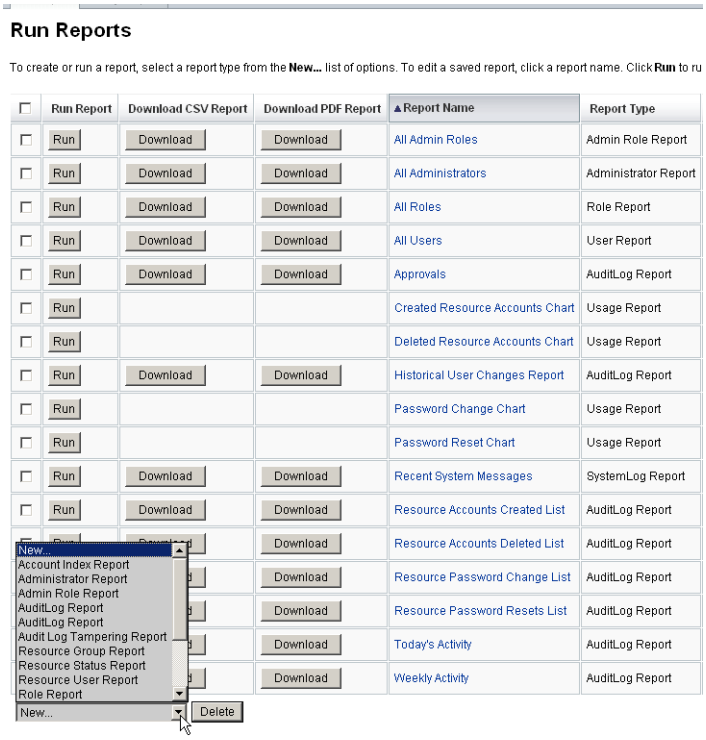


図 1 「レポートの実行」ページの選択項目

レポートの定義を開始するには、次のいずれかの方法を使用します。

- レポートを作成する
- レポートを選択して修正し、新しい名前で保存する (レポートのクローン作成とも呼ばれる)

レポートの作成

レポートを作成するには、次を実行します。

1. メニューバーで**「レポート」**を選択します。
2. オプションの**「新規」**リストからレポートの種類を選択します。

Identity Manager の「レポートの定義」ページが表示されます。ここでオプションを選択して保存すると、レポートが作成されます。

レポートの複製

レポートを複製するには、リストからレポートを選択します。新しいレポート名を入力し、オプションでレポートパラメータを調整して**「保存」**をクリックします。レポートは新しい名前で保存されます。

電子メールによるレポートの送信

レポートを作成または編集するときには、レポートの結果を 1 人または複数の電子メール受信者に送信するオプションを選択できます。このオプションを選択すると、ページが更新され、電子メール受信者を指定するように要求されます。アドレスをカンマで区切り、1 人以上の受信者を入力します。

電子メールに添付するレポートの形式を選択することもできます。

- **「CSV 形式のレポートの添付」**― カンマ区切り値 (CSV) 形式でレポートの結果を添付します。
- **「PDF 形式のレポートの添付」**― PDF (Portable Document Format) 形式でレポートの結果を添付します。

レポートの実行

レポートの条件を入力および選択したら、次を実行できます。

- 保存せずにレポートを実行する ― **「実行」**をクリックしてレポートを実行します。レポート (新しいレポートを定義した場合) または変更したレポートの条件 (既存のレポートを編集した場合) は保存されません。
- レポートを保存する ― **「保存」**をクリックしてレポートを保存します。保存後は、「レポートの実行」ページ (レポートのリスト) からこのレポートを実行できます。

レポートのスケジュール

レポートをただちに実行するのか、定期的に実行するようスケジュールするのかによって、選択は異なります。

- **「レポート」→「レポートの実行」**― 保存されたレコードをただちに実行できます。レポートのリストから**「実行」**をクリックします。Identity Manager によりレポートが実行され、結果が要約および詳細形式で表示されます。
- **「タスク」→「タスクのスケジュール」**― 実行するレポートタスクをスケジュールします。レポートタスクの選択後、レポートの頻度とオプションを設定できます。また、レポートの特定の詳細を調整することもできます (「レポートの定義」ページの「レポート」エリアで)。

レポートデータのダウンロード

「レポートの実行」ページで、次のいずれかの行の**「ダウンロード」**をクリックします。

- **「CSV レポートのダウンロード」** ― 監査レポートの出力を CSV 形式でダウンロードします。保存したあとは、Microsoft Excel などの別のアプリケーションでレポートを開いて操作することができます。
- **「PDF レポートのダウンロード」** ― 監査レポートの出力を Portable Document Format 形式でダウンロードします。

図 2 レポートのダウンロード

レポート出力のフォントの設定

PDF (Portable Document Format) で生成されるレポートについて、レポートで使用するフォントを決定するための選択を行うことができます。

レポートのフォント選択を設定するには、**「設定」**をクリックして**「レポート」**を選択します。次のオプションを選択できます。

- **「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だけが示されます。ただし、フォント定義ファイルを製品の fonts/ ディレクトリにコピーしてサーバーを再起動することにより、アジア言語をサポートするために必要なフォントなどの追加フォントをシステムに追加できます。

  追加できるフォント定義形式には .ttf、.ttc、.otf、および .afm があります。これらのフォントのいずれかを選択する場合、レポートが表示されるマシンでそのフォントが使用可能である必要があります。フォントが使用できない場合、代わりに「PDF ドキュメントにフォントを埋め込む」オプションを選択してください。
- **「PDF ドキュメントにフォントを埋め込む」** ― 生成される PDF レポートにフォント定義を埋め込むには、このオプションを選択します。これにより、レポートがどの PDF ビューアでも表示できることが保証されます。

注　フォントを埋め込むと、ドキュメントのサイズが非常に大きくなる可能性があります。

「保存」をクリックしてレポート設定オプションを保存します。

レポートのタイプ

Identity Manager のレポートのタイプには、次のものがあります。

- 監査ログ
- リアルタイム
- 概要
- システムログ
- 使用状況

監査ログ

監査レポートは、システム監査ログに取得されたイベントに基づいています。このレポートには、生成されたアカウント、承認された要求、失敗したアクセス試行、パスワードの変更とリセット、およびセルフプロビジョニングアクティビティ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、**「監査イベント」**を選択します。グループごとに成功したイベントと失敗したイベントを記録するために、監査グループ名を 1 つ以上選択します。監査設定グループの設定の詳細については、第 5 章の「監査グループの設定」を参照してください。

監査ログレポートを定義するには、「レポートの実行」ページのレポートオプションのリストから「監査ログレポート」を選択します。

レポートパラメータを設定して保存したら、「レポートの実行」リストページからレポートを実行します。**「実行」**をクリックすると、保存した条件を満たすすべての結果を含んだレポートが作成されます。レポートには、イベントの発生日、実行された操作、および操作の結果が表示されます。

リアルタイム

リアルタイムレポートは、リソースを直接ポーリングしてリアルタイム情報をレポートします。リアルタイムレポートには次の情報が含まれます。

- **リソースグループ** – ユーザーメンバーシップを含むグループ属性の概要を表示します。
- **リソースステータス** – 各リソースに対して testConnection メソッドを実行することにより、1 つ以上の指定されたリソースの接続ステータスをテストします。
- **リソースユーザー** – ユーザーリソースアカウントとアカウント属性を一覧表示します。

リアルタイムレポートを定義するには、「レポートの実行」ページのレポートオプションのリストからこのレポートタイプを選択します。

レポートパラメータを設定して保存したら、「レポートの実行」リストページからレポートを実行します。**「実行」**をクリックすると、保存した条件を満たすすべての結果を含んだレポートが作成されます。

概要レポート

概要レポートのタイプには、次のものが含まれます。

- アカウントインデックス ― 調整状況に従って選択したリソースアカウントについてレポートします。
- **管理者** ― Identity Manager 管理者、管理者が管理する組織、および管理者に割り当てられている機能が表示されます。管理者レポートを定義するときには、レポートに含める管理者を組織によって選択できます。
- **管理者ロール** ― 管理者ロールに割り当てられているユーザーを一覧表示します。
- **ロール** ― Identity Manager ロールとそれに関連付けられたリソースが要約されます。ロールレポートを定義するときには、レポートに含めるロールを、関連付けられた組織によって選択できます。
- タスク ― 保留中または終了済みのタスクをレポートします。含める情報の詳細さは、承認者、説明、有効期限、所有者、開始日、状態などの属性のリストから選択することによって決まります。
- **ユーザー** ― ユーザー、ユーザーに割り当てられたロール、およびユーザーがアクセスできるリソースが表示されます。ユーザーレポートを定義するときには、レポートに含めるユーザーを名前、ロール、組織、またはリソース割り当てによって選択できます。
- **ユーザー質問** ― アカウントポリシー要件で指定した認証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。

「レポートの実行」リストページから概要レポートを実行します。

次の図に示すように、管理者レポートには、Identity Manager 管理者、管理者が管理する組織、および管理者に割り当てられている機能と管理者ロールが一覧表示されます。

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

図 3 管理者概要レポート

システムログ

システムログレポートは、リポジトリに記録されるシステムメッセージおよびエラーを示します。このレポートを設定するとき、次の情報を含めるか除外するかを指定できます。

- システムコンポーネント (プロビジョニングツール、スケジューラ、サーバーなど)
- エラーコード
- 重要度レベル (エラー、致命的、または警告)

表示するレコードの最大数 (デフォルトは 3000) や、表示可能なレコード数が指定された最大値を超えた場合に古いレコードと新しいレコードのどちらを優先して表示するかも設定できます。

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、「lh リファレンス」の「syslog コマンド」を参照してください。

システムログレポートを定義するには、「レポートの実行」ページのレポートオプションのリストから「システムログレポート」を選択します。

使用状況レポート

使用状況レポートを作成して実行すると、管理者、ユーザー、ロール、またはリソースなどの Identity Manager オブジェクトに関連するシステムイベントの要約をグラフ形式または表形式で表示できます。出力を円グラフ、棒グラフ、または表形式で表示することができます。

使用状況レポートを定義するには、「レポートの実行」リストページのレポートオプションのリストから「使用状況レポート」を選択します。

レポートパラメータを設定して保存したら、「レポートの実行」リストページからレポートを実行します。

使用状況レポートのグラフ

次の図では、最上部の表にレポートを構成するイベントが表示されます。その下にあるグラフは、この表の情報をグラフ化したものです。マウスポインタをグラフの各部に移動すると、その部分の値が表示されます。

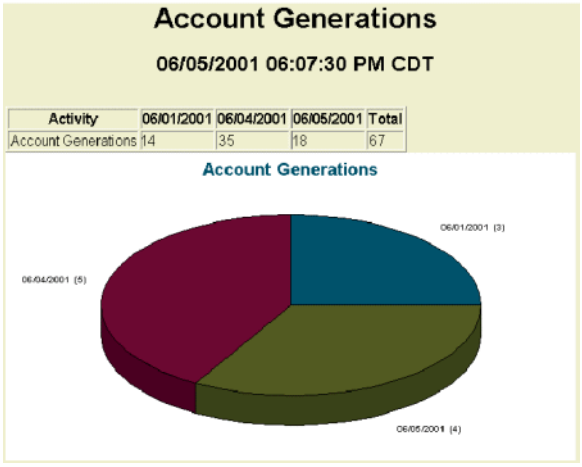


図 4 使用状況レポート (生成されたユーザーアカウント)

円グラフの一部をハイライト表示処理することができます。データスライスの一部を右クリックしたまま、ほかのデータスライスから離れて見えるように中央からドラッグします。この処理は、グラフ内の複数の部分で実行できます。ほとんどの管理の場合、スライスの中央に近い部分をクリックすると、ほかのスライスとの間隔がさらに広くなるようドラッグすることができます。

表示したい方向に円グラフを回転させることもできます。グラフの端の部分をクリックしたまま、表示したい方向へマウスを右または左に移動して回転します。

リスク分析

Identity Manager リスク分析機能を使用すると、プロファイルが特定のセキュリティー制限の外部にあるユーザーアカウントについてレポートを作成できます。リスク分析レポートは、物理的なリソースをスキャンしてデータを収集し、無効化されたアカウント、ロックされたアカウント、および所有者のいないアカウントについての詳細をリソースごとに表示します。また、リスク分析では期限切れパスワードについての詳細も表示されます。レポートの詳細は、リソースタイプによって異なります。

注　標準のレポートは、AIX、HP、Solaris、NetWare NDS、Windows NT、および Windows Active Directory リソースに対して実行可能です。

リスク分析ページは、フォームによって制御され、環境に合わせて設定できます。フォームのリストは、`idm¥debug` ページの RiskReportTask オブジェクトの下に表示され、Business Process Editor を使って修正できます。Identity Manager フォームの設定方法の詳細は、『Identity Manager Technical Reference』を参照してください。

リスク分析レポートを作成するには、メニューバーの**「リスク分析」**をクリックして、オプションの「新規」リストからレポートを選択します。

選択したリソースをスキャンするようにレポートを制限できます。また、リソースタイプによっては、次のアカウントをスキャンすることができます。

- 無効化されているか、期限が切れているか、非アクティブか、ロックされている
- まったく使用されたことがない
- フルネームまたはパスワードがない
- パスワードを必要としない
- パスワードの期限が切れているか、指定された日数の間変更されていない

定義したあとは、リスク分析レポートを指定した間隔で実行するようにスケジュールすることができます。

1. **「タスクのスケジュール」**をクリックして、実行するレポートを選択します。
2. 「タスクスケジュールの作成」ページで、名前とスケジュール情報を入力し、オプションでその他のリスク分析の選択を調整します。
3. **「保存」**をクリックして、スケジュールを保存します。

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、カスタマイズされ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。

Identity Manager には、ユーザーによる設定が可能な次のタスクテンプレートが用意されています。

- **ユーザー作成テンプレート** – ユーザー作成タスクのプロパティーを設定します。
- **ユーザー削除テンプレート** – ユーザー削除タスクのプロパティーを設定します。
- **ユーザー更新テンプレート** – ユーザー更新タスクのプロパティーを設定します。

タスクテンプレートの操作に関する情報は、次の各節をお読みください。

- タスクテンプレートの有効化 – タスクテンプレートをシステムで利用できるようにする方法について説明します。
- 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について説明します。

タスクテンプレートの有効化

タスクテンプレートを使用する前に、タスクテンプレートのプロセスをマップする必要があります。プロセスタイプをマップするには、次の手順に従います。

1. Identity Manager 管理者インタフェースから**「タスク」**を選択し、**「タスクの設定」**を選択します。

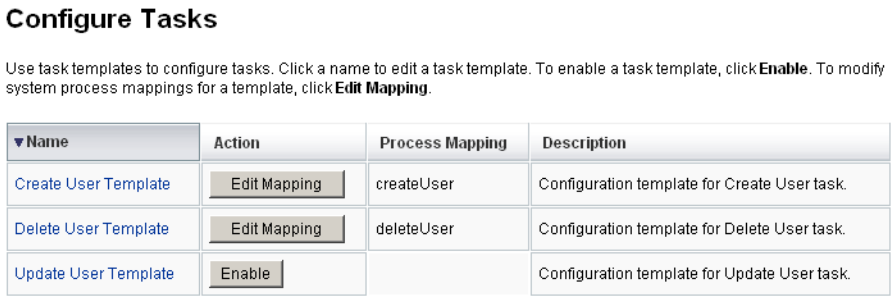


図 1 タスクの設定

「タスクの設定」ページには、次の列を持つテーブルがあります。

- **「名前」** – ユーザー作成、ユーザー削除、およびユーザー更新の各テンプレートへのリンクがあります。

- **「アクション」**― 次のいずれかのボタンがあります。
  - **「有効化」**― テンプレートをまだ有効にしていない場合に表示されます。
  - **「マッピングの編集」**― テンプレートを有効にしたあとで表示されます。

  プロセスマッピングを有効化する手順と編集する手順は同じです。
- **「プロセスマッピング」**― 各テンプレートにマップされたプロセスタイプが一覧表示されます。
- **「説明」**― 各テンプレートの簡単な説明です。

2. **「有効化」**をクリックして、テンプレートのプロセスマッピングの編集ページを開きます。

   たとえば、ユーザー作成テンプレートに対して次のページが表示されます。

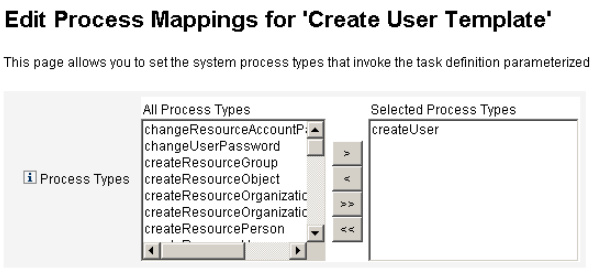


図 2 プロセスマッピングの編集ページ

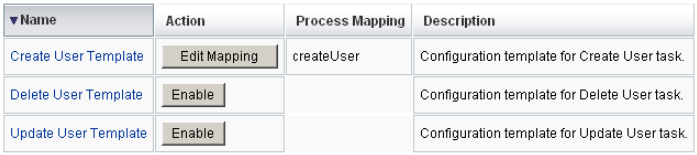
注 「選択したプロセスタイプ」リストには、デフォルトのプロセスタイプ (この場合 `createUser`) が自動的に表示されます。必要に応じて、メニューから別のプロセスタイプを選択できます。

- 一般に、各テンプレートに複数のプロセスタイプをマップすることはありません。
- 「選択したプロセスタイプ」リストからプロセスタイプを削除し、代わりのプロセスタイプを選択しない場合、「必須のプロセスマッピング」セクションに、新しいタスクマッピングを選択するように指示が表示されます。

図 3 「必須のプロセスマッピング」セクション

3. **「保存」**をクリックして、選択したプロセスタイプをマップし、「タスクの設定」ページに戻ります。

注 「タスクの設定」ページが再表示されると、**「有効化」**ボタンが**「マッピングの編集」**ボタンに変化し、「プロセスマッピング」列にプロセス名が表示されます。



▼Name	Action	Process Mapping	Description
Create User Template	Edit Mapping	createUser	Configuration template for Create User task.
Delete User Template	Enable		Configuration template for Delete User task.
Update User Template	Enable		Configuration template for Update User task.

図 4 更新された「タスクの編集」テーブル

4. 残りの各テンプレートに対して、マッピングプロセスを繰り返します。

注意：

- **「設定」-->「フォームおよびマッピングプロセス」**を選択することにより、マッピングを検証することができます。「フォームおよびプロセスマッピングの設定」ページが表示されたら、下にスクロールして「プロセスマッピング」テーブルを表示し、テーブル内に示される「マップされるプロセス名」エントリに次のプロセスタイプがマップされていることを確認します。

プロセスタイプ	マップされるプロセス名
createUser	Create User Template
deleteUser	Delete User Template
updateUser	Update User Template

  テンプレートが正しく有効化されていれば、すべての「マップされるプロセス名」エントリに「Template」という文字列が含まれています。
- テーブルに示されるとおりに「マップされるプロセス名」列に「Template」と入力することで、このページから直接、これらのプロセスタイプをマップすることもできます。

テンプレートのプロセスタイプを正しくマップしたら、タスクテンプレートの設定に進むことができます。

タスクテンプレートの設定

各種のタスクテンプレートを設定するには、次の手順に従います。

1. タスクテンプレートテーブル内の「名前」リンクを選択します。次のいずれかのページが表示されます。
   - **「タスクテンプレート「Create User Template」の編集 :」** ― 新しいユーザーアカウントの作成に使用するテンプレートを編集するには、このページを開きます。
   - **「タスクテンプレート「Delete User Template」の編集 :」** ― ユーザーアカウントの削除またはプロビジョニング解除に使用するテンプレートを編集するには、このページを開きます。
   - **「タスクテンプレート「Update User Template」の編集 :」** ― 既存ユーザーの情報の更新に使用するテンプレートを編集するには、このページを開きます。

   それぞれのタスクテンプレートの編集ページには、ユーザーワークフローの主な設定領域に対応する一連のタブがあります。

   次の表は、それぞれのタブの名前、目的、そのタブを使用するテンプレートについて説明したものです。

タブ名	目的	テンプレート
一般 (デフォルトタブ)	「ホーム」および「アカウント」の各ページのタスクバー内と、「タスク」ページ上のタスクインスタンステーブル内でのタスク名の表示形式を定義します。	ユーザー作成タスクテンプレートとユーザー更新タスクテンプレートのみ
	ユーザーアカウントの削除 / プロビジョニング解除形式を指定できます。	ユーザー削除テンプレートのみ
通知	Identity Manager がプロセスを起動したときに管理者およびユーザーに送信される電子メール通知を設定できます。	すべてのテンプレート
承認	タイプ別に承認を有効または無効にする、追加の承認者を指定する、Identity Manager が特定のタスクを実行する前にアカウントデータの属性を指定するなどの作業を行うことができます。	すべてのテンプレート
監査	ワークフローの監査を有効化および設定できます。	すべてのテンプレート

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のみ
データ変換	プロビジョニング中にユーザーデータがどのように変換されるかを設定することができます。	ユーザー作成タスクテンプレートとユーザー更新タスクテンプレートのみ

2. いずれかのタブを選択して、テンプレートのワークフロー機能を設定します。
   これらのタブでの設定方法については、次の各節を参照してください。
   - 9-5 ページの「「一般」タブの設定」
   - 9-8 ページの「「通知」タブの設定」
   - 9-12 ページの「「承認」タブの設定」
   - 9-27 ページの「「プロビジョニング」タブの設定」
   - 9-28 ページの「「サンライズとサンセット」タブの設定」
   - 9-32 ページの「「データ変換」タブの設定」
3. テンプレートの設定を完了したら、**「保存」**ボタンをクリックして変更を保存します。

「一般」タブの設定

この節では、「一般」タブでの設定手順を説明します。

注　ユーザー作成テンプレートとユーザー更新テンプレートのタスクテンプレートの編集ページは共通なため、タブの設定手順は 1 つの節にまとめられています。

ユーザー作成テンプレートまたはユーザー更新テンプレートの場合

「タスクテンプレート「Create User Template」の編集 :」または「タスクテンプレート「Update User Template」の編集 :」ページを開くと、「一般」タブページがデフォルトで表示されます。次の図に示すように、このページは「タスク名」テキストフィールドおよびメニューで構成されます。

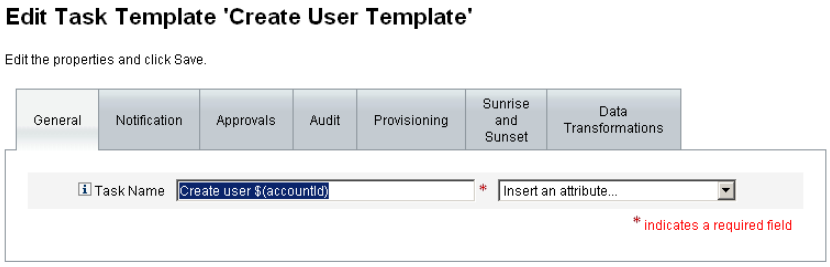


図 5 「一般」タブ : ユーザー作成テンプレート

タスク名はリテラルテキストまたはタスク実行時に解決される属性参照、あるいはその両方で指定できます。

デフォルトのタスク名を変更するには、次の手順に従います。

1. **「タスク名」**フィールドに名前を入力します。

   デフォルトのタスク名を編集することも、完全に別の名前にすることもできます。
2. **「タスク名」**メニューには、このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されている属性のリストが表示されます。メニューから属性を選択します (省略可能)。

   Identity Manager によって、「タスク名」フィールド内のエントリに属性名が追加されます。次に例を示します。

   ```
   Create user $(accountId) $(user.global.email)
   ```
3. 終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - **「保存」**をクリックして変更を保存し、「タスクの設定」ページに戻ります。

     新しいタスク名が Identity Manager のタスクバーに表示されます。タスクバーは「ホーム」タブおよび「アカウント」タブの最下部にあります。
   - **「キャンセル」**をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

ユーザー削除テンプレートの場合

「タスクテンプレート「Delete User Template」の編集 :」ページを開くと、「一般」タブページがデフォルトで表示されます。

ユーザーアカウントの削除 / プロビジョニング解除形式を指定するには、次の手順に従います。

1. **「Identity Manager アカウントの削除」**ボタンを使用して、削除操作の間に Identity Manager アカウントを削除できるかどうかを指定します。
   - **「なし」**— アカウントが削除されるのを防ぐには、このボタンを有効にします。

- **「プロビジョニング解除後にユーザーがリンクされたアカウントを持っていない場合のみ」**― プロビジョニング解除後にリンクされたリソースアカウントがない場合にのみユーザーアカウントの削除を許可するには、このボタンを有効にします。
- **「常時」**― 割り当てられたリソースアカウントがまだ存在する場合も含めてユーザーアカウントの削除を常に許可するには、このボタンを有効にします。

2. **「リソースアカウントのプロビジョニング解除」**ボックスを使用して、すべてのリソースアカウントを対象にリソースアカウントのプロビジョニング解除を制御します。
   - **「すべて削除」**― すべての割り当て済みリソース上の、ユーザーを表すすべてのアカウントを削除するには、このボックスを有効にします。
   - **「すべて割り当て解除」**― すべてのリソースアカウントをユーザーから割り当て解除するには、このボックスを有効にします。リソースアカウントは削除されません。
   - **「すべてをリンク解除」**― Identity Manager システムからリソースアカウントへのすべてのリンクを解除するには、このボックスを有効にします。割り当てられているがリンクされていないアカウントを持つユーザーは、更新が必要なことを示すバッジのマークとともに表示されます。

注 これらの制御設定は、「個々のリソースアカウントのプロビジョニング解除」テーブルでの動作よりも優先されます。

3. (「リソースアカウントのプロビジョニング解除」と比較して) ユーザーのプロビジョニング解除についてより詳細な設定を行うには、次に示すように**「個々のリソースアカウントのプロビジョニング解除」**ボックスを使用します。
   - **「削除」**― リソース上のユーザーを表すアカウントを削除するには、このボックスを有効にします。
   - **「割り当て解除」**―このボックスを有効にすると、ユーザーはリソースに直接割り当てられなくなります。リソースアカウントは削除されません。
   - **「リンク解除」**― Identity Manager システムからリソースアカウントへのリンクを解除するには、このボックスを有効にします。割り当てられているがリンクされていないアカウントを持つユーザーは、更新が必要なことを示すバッジのマークとともに表示されます。

注 **「個々のリソースアカウントのプロビジョニング解除」**オプションは、複数の異なるリソースに対してプロビジョニング解除ポリシーを個別に指定したい場合に便利です。たとえば、個々の Active Directory ユーザーは削除後に再生成できないグローバル ID を持つため、ほとんどの顧客は Active Directory ユーザーを削除したくないと考えます。

一方、プロビジョニング解除設定は新しいリソースを追加するたびに更新しなければならないため、新しいリソースが追加される環境ではこのオプションを使用しないほうが適している場合もあります。

4. 終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。

- **「保存」**をクリックして変更を保存し、「タスクの設定」ページに戻ります。
- **「キャンセル」**をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

「通知」タブの設定

すべてのタスクテンプレートは、Identity Manager がプロセスを起動したとき (通常はプロセスの完了後) に、管理者およびユーザーに電子メールで通知を送信する動作をサポートします。「通知」タブを使用してこれらの通知を設定できます。

注　Identity Manager では、電子メールテンプレートを使用して、情報および操作の要求を管理者、承認者、およびユーザーに配信します。Identity Manager の電子メールテンプレートの詳細については、このガイドの「電子メールテンプレートの理解」の節を参照してください。

次の図は、ユーザー作成テンプレートの「通知」ページを示したものです。

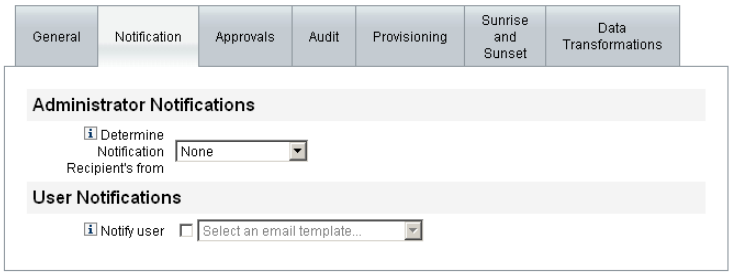


図 6 「通知」タブ : ユーザー作成テンプレート

Identity Manager が通知の受信者を決定する方法を指定するには、次の手順に従います。

1. 「管理者通知」セクションの設定を完了します。
2. 「ユーザー通知」セクションの設定を完了します。
3. 終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - **「保存」**をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - **「キャンセル」**をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

管理者通知の設定

管理者である受信者に通知するための方法を決定するには、**「通知の受信者を決定する方法」**メニューからオプションを選択します。

- **「なし」**(デフォルト) ― 管理者への通知を行いません。

- **「属性」**― 通知の受信者のアカウント ID を、ユーザービューで指定された属性から取得する場合に選択します。9-9 ページの「属性による受信者の指定」に進みます。
- **「規則」**― 指定された規則を評価することによって通知の受信者のアカウント ID を取得する場合に選択します。9-10 ページの「規則による受信者の指定」に進みます。
- **「クエリー」**― 特定のリソースへのクエリーを作成することによって通知の受信者のアカウント ID を取得する場合に選択します。9-10 ページの「クエリーによる受信者の指定」に進みます。
- **「管理者リスト」**― 通知の受信者をリストから直接選ぶ場合に選択します。9-11 ページの「管理者リストからの受信者の指定」に進みます。

属性による受信者の指定

指定された属性から通知の受信者のアカウント ID を取得するには、次の手順に従います。

注　属性は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストに解決する必要があります。

1. **「通知の受信者を決定する方法」**メニューから**「属性」**を選択します。次の新しいオプションが表示されます。

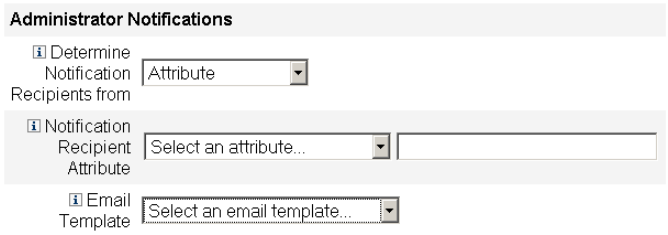


図 7　管理者通知 : 属性

- **「通知の受信者の属性」**― 受信者のアカウント ID を決定するために使われる属性 (このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されている) のリストが提示されます。
- **「電子メールテンプレート」**― 電子メールテンプレートのリストが提示されます。

2. **「通知の受信者の属性」**メニューから属性を選択します。
   メニューの隣にあるテキストフィールドに属性名が表示されます。
3. **「電子メールテンプレート」**メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

規則による受信者の指定

指定された規則から通知の受信者のアカウント ID を取得するには、次の手順に従います。

注　評価されたとき、規則は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストを返す必要があります。

1. **「通知の受信者を決定する方法」**メニューから**「規則」**を選択します。「通知」フォームに次の新しいオプションが表示されます。

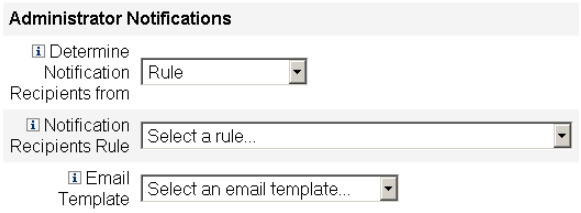


図 8 管理者通知 : 規則

- **「通知の受信者の規則」**― 評価されたときに受信者のアカウント ID を返す規則 (システムに対して現在定義されているもの) のリストが提示されます。
- **「電子メールテンプレート」**― 電子メールテンプレートのリストが提示されます。

2. **「通知の受信者の規則」**メニューから規則を選択します。
3. **「電子メールテンプレート」**メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

クエリーによる受信者の指定

注　現時点では、LDAP および Active Directory リソースのクエリーのみがサポートされています。

指定されたリソースを問い合わせることで通知の受信者のアカウント ID を取得するには、次の手順に従います。

1. **「通知の受信者を決定する方法」**メニューから**「クエリー」**を選択します。「通知」フォームに次の新しいオプションが表示されます。

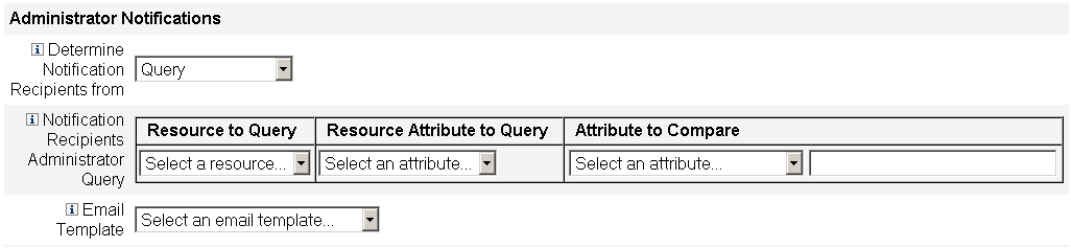


図 9 管理者通知 : クエリー

- **「通知受信者の管理者クエリー」**— 次のメニューで構成されるテーブルが提示されます。このテーブルを使用してクエリーを作成できます。
  - **「問い合わせ先のリソース」**— システムに対して現在定義されているリソースのリストが提示されます。
  - **「問い合わせ先のリソース属性」**— システムに対して現在定義されているリソース属性のリストが提示されます。
  - **「比較対象の属性」**— システムに対して現在定義されている属性のリストが提示されます。
- **「電子メールテンプレート」**— 電子メールテンプレートのリストが提示されます。

2. これらのメニューからリソース、リソース属性、および比較対象の属性を選択し、クエリーを作成します。
3. **「電子メールテンプレート」**メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

管理者リストからの受信者の指定

「通知の受信者を決定する方法」メニューから**「管理者リスト」**を選択します。「通知」フォームに次の新しいオプションが表示されます。

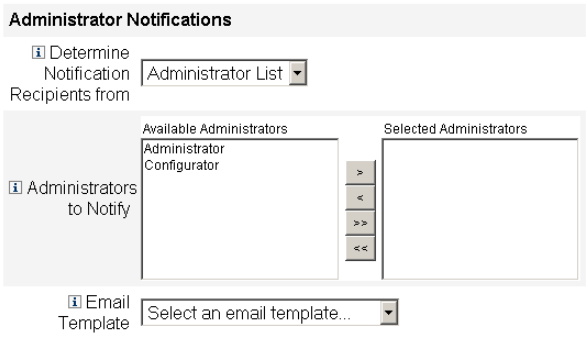


図 10 管理者通知 : 管理者リスト

- **「通知する管理者」**— 通知可能な管理者のリストと選択ツールが提示されます。
- **「電子メールテンプレート」**— 電子メールテンプレートのリストが提示されます。

4. 「利用可能な管理者」リストから 1 人以上の管理者を選択し、 > ボタンまたは >> ボタンを使用して、選択された名前を「選択された管理者」リストに移動します。
5. **「電子メールテンプレート」**メニューからテンプレートを選択して、管理者の通知電子メールの形式を指定します。

ユーザー通知の設定

通知を受けるユーザーを指定するとき、通知のための電子メールを生成するために使われる電子メールテンプレートの名前も指定する必要があります。

作成、更新、または削除中のユーザーに通知するには、**「ユーザーへの通知」**チェックボックスをオンにし、メニューから電子メールテンプレートを選択します。

図 11 電子メールテンプレートの指定

「承認」タブの設定

Identity Manager がユーザーの作成、削除、または更新の各タスクを実行する前に、「承認」タブを使用して、追加の承認者やタスク承認フォームの属性を指定することができます。

従来の方式では、特定の組織、リソース、またはロールと関連付けられた管理者は、実行前に特定のタスクを承認する必要があります。Identity Manager では、追加の承認者 (タスクを承認する必要がある追加の管理者) を指定することもできます。

注 ワークフローに対して追加の承認者を設定する場合、従来からの承認者による承認に加えて、テンプレートで指定された追加の承認者による承認も要求することになります。

次の図は、初期状態の「承認」ページの管理ユーザーインタフェースの例です。

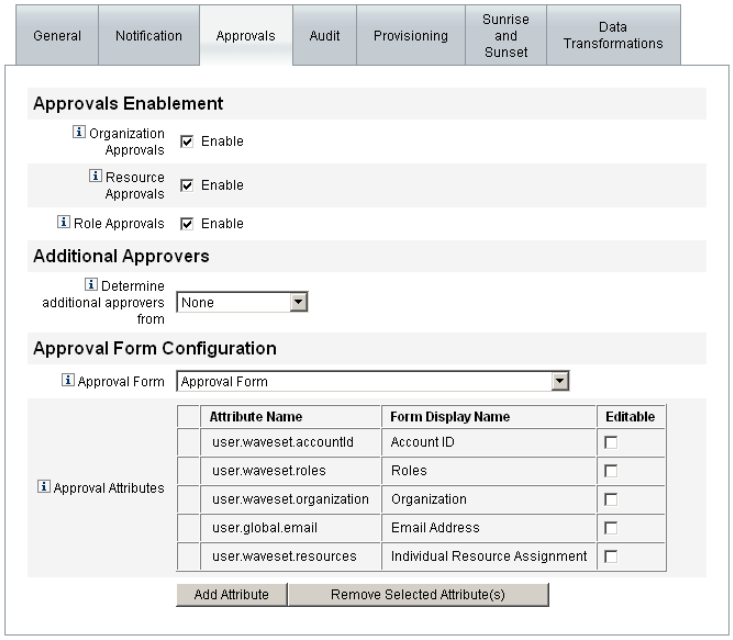


図 12 「承認」タブ : ユーザー作成テンプレート

承認を設定するには、次の手順に従います。

1. 「承認の有効化」の節の手順を完了します (9-13 ページの「承認の有効化」を参照)。
2. 「追加の承認者」の節の手順を完了します (9-14 ページの「追加の承認者の指定」を参照)。
3. ユーザー作成テンプレートおよびユーザー更新テンプレートのみを対象に、「承認フォームの設定」の節の手順を完了します (9-22 ページの「承認フォームの設定」を参照)。
4. 「承認」タブの設定を完了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - **「保存」**をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - **「キャンセル」**をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

承認の有効化

次のそれぞれの**「承認の有効化」**チェックボックスを使用して、ユーザー作成、ユーザー削除、またはユーザー更新の各タスクの実行前に承認を要求するように設定します。

注　デフォルトでは、これらのチェックボックスはユーザー作成テンプレートおよびユーザー更新テンプレートに対しては有効になっていますが、ユーザー削除テンプレートに対しては無効になっています。

- **「組織の承認」**― 設定済みの任意の組織承認者による承認を必須とするには、このチェックボックスをオンにします。
- **「リソースの承認」**― 設定済みの任意のリソース承認者による承認を必須とするには、このチェックボックスをオンにします。
- **「ロールの承認」**― 設定済みの任意のロール承認者による承認を必須とするには、このチェックボックスをオンにします。

追加の承認者の指定

「追加の承認者を決定する方法」メニューを使用して、Identity Manager がユーザー作成、ユーザー削除、またはユーザー更新の各タスクに対して追加の承認者を決定する方法を指定します。このメニューのオプションには、次のものがあります。

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、管理ユーザーインタフェースに追加のオプションが表示されます。これらのオプションを設定するための手順は、9-14 ページ 以降で説明します。

以下の各節の指示に従って、追加の承認者を決定する方法を指定します。

- 属性から (9-15 ページ)
- 規則から (9-16 ページ)
- クエリーから (9-17 ページ)
- 管理者リストから (9-18 ページ)

属性から

属性から追加の承認者を決定するには、次の手順に従います。

1. **「追加の承認者を決定する方法」**メニューから**「属性」**を選択します。

注　属性は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストに解決する必要があります。

次の新しいオプションが表示されます。

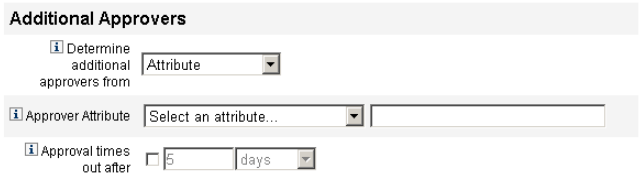


図 13 追加の承認者 : 属性

- **「承認者の属性」**― 承認者のアカウント ID を決定するために使われる属性 (このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されているもの) のリストが提示されます。
- **「承認がタイムアウトになるまでの時間」**― 承認がいつタイムアウトするかを指定できます。

注　**「承認がタイムアウトになるまでの時間」**の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

2. **「承認者の属性」**メニューを使用して属性を選択します。
   選択した属性が隣のテキストフィールドに表示されます。
3. 指定された時間が経過したら承認要求をタイムアウトさせるかどうかを決定します。
   - タイムアウト時間を指定する場合は、9-19 ページの「承認のタイムアウトの設定」の手順に進みます。
   - タイムアウト時間を指定しない場合、9-22 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

規則から

承認者のアカウント ID を指定された規則から取得するには、次の手順に従います。

1. **「追加の承認者を決定する方法」**メニューから**「規則」**を選択します。

注 評価されたとき、規則は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストを返す必要があります。

次の新しいオプションが表示されます。

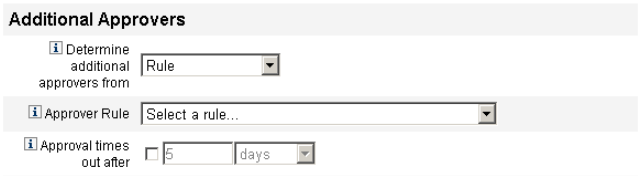


図 14 追加の承認者 : 規則

- **「承認者の規則」**— 評価されたときに受信者のアカウント ID を返す規則 (システムに対して現在定義されているもの) のリストが提示されます。
- **「承認がタイムアウトになるまでの時間」**— 承認がいつタイムアウトするかを指定できます。

注 **「承認がタイムアウトになるまでの時間」**の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

2. **「承認者の規則」**メニューから規則を選択します。
3. 指定された時間が経過したら承認要求をタイムアウトさせるかどうかを決定します。
   - タイムアウト時間を指定する場合は、9-19 ページの「承認のタイムアウトの設定」の手順に進みます。
   - タイムアウト時間を指定しない場合、9-22 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

クエリーから

注　現時点では、LDAP および Active Directory リソースのクエリーのみがサポートされています。

指定されたリソースを問い合わせることで承認者のアカウント ID を取得するには、次の手順に従います。

1. **「追加の承認者を決定する方法」**メニューから**「クエリー」**を選択します。次の新しいオプションが表示されます。

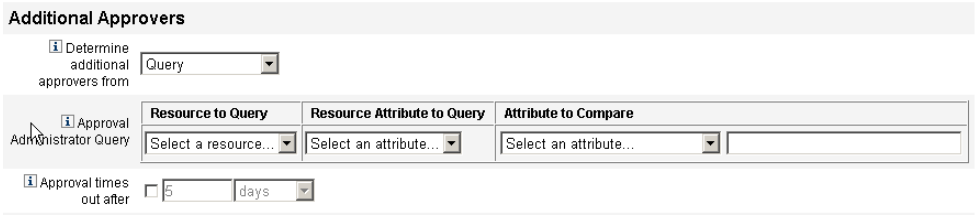


図 15　追加の承認者 : クエリー

- **「承認の管理者のクエリー」**― 次のメニューで構成されるテーブルが提示されます。このテーブルを使用してクエリーを作成できます。
  - **「問い合わせ先のリソース」**― システムに対して現在定義されているリソースのリストが提示されます。
  - **「問い合わせ先のリソース属性」**― システムに対して現在定義されているリソース属性のリストが提示されます。
  - **「比較対象の属性」**― システムに対して現在定義されている属性のリストが提示されます。
- **「承認がタイムアウトになるまでの時間」**― 承認がいつタイムアウトするかを指定できます。

注　**「承認がタイムアウトになるまでの時間」**の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

2. 次のようにしてクエリーを作成します。
   a. **「問い合わせ先のリソース」**メニューからリソースを選択します。
   b. **「問い合わせ先のリソース属性」**メニューおよび**「比較対象の属性」**メニューから属性を選択します。
3. 指定された時間が経過したら承認要求をタイムアウトさせるかどうかを決定します。
   - タイムアウト時間を指定する場合は、9-19 ページの「承認のタイムアウトの設定」の手順に進みます。
   - タイムアウト時間を指定しない場合、9-22 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

管理者リストから

追加の承認者を管理者リストから明示的に選択するには、次の手順に従います。

1. **「追加の承認者を決定する方法」**メニューから**「管理者リスト」**を選択します。次の新しいオプションが表示されます。

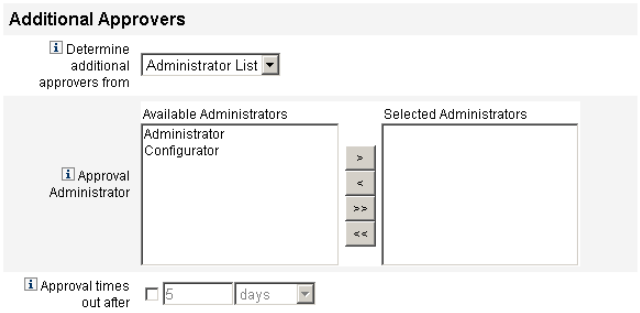


図 16 追加の承認者 : 管理者リスト

- **「通知する管理者」**― 通知可能な管理者のリストと選択ツールが提示されます。
- **「承認フォーム」**― 追加の承認者が承認要求を承認または却下するために使用できるユーザーフォームのリストが提示されます。
- **「承認がタイムアウトになるまでの時間」**― 承認がいつタイムアウトするかを指定できます。

注 **「承認がタイムアウトになるまでの時間」**の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

2. 「利用可能な管理者」リストから 1 人以上の管理者を選択し、> ボタンまたは >> ボタンを使用して、選択された名前を「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要求をタイムアウトさせるかどうかを決定します。
   - タイムアウト時間を指定する場合は、9-19 ページの「承認のタイムアウトの設定」の手順に進みます。
   - タイムアウト時間を指定しない場合、9-22 ページの「承認フォームの設定」に進むか、または変更を保存して別のタブの設定に移ることができます。

承認のタイムアウトの設定

承認のタイムアウトを設定するには、次の手順に従います。

1. チェックボックスをオンにします。

   次の図に示すように、隣接するテキストフィールドとメニューがアクティブになり、**「タイムアウトのアクション」**ボタンが表示されます。

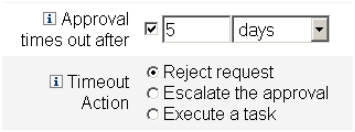


図 17 承認のタイムアウトのオプション

2. 次のように、**「承認がタイムアウトになるまでの時間」**のテキストフィールドとメニューを使用してタイムアウト時間を指定します。
   a. メニューから秒、分、時間、または日を選択します。
   b. テキストフィールドに数値を入力して、タイムアウトの秒数、分数、時間数、または日数を指定します。

注 **「承認がタイムアウトになるまでの時間」**の設定は、最初の承認とエスカレーションされた承認の両方に影響します。

3. **「タイムアウトのアクション」**のいずれかのラジオボタンを選択して、承認要求がタイムアウトしたときの動作を指定します。
   - **「要求の却下」**― 指定されたタイムアウト時間までに要求が承認されない場合、Identity Manager は自動的にその要求を却下します。
   - **「承認のエスカレーション」**― 指定されたタイムアウト時間までに要求が承認されない場合、Identity Manager はその要求を別の承認者に自動的にエスカレーションします。

     このラジオボタンを選択すると、エスカレーションされた承認の承認者を Identity Manager が決定する方法を指定する必要があるため、新しいオプションが表示されます。続きの手順については、9-20 ページの「承認のエスカレーション」を参照してください。
   - **「タスクの実行」**― 指定されたタイムアウト時間までに承認要求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、承認要求がタイムアウトした場合に実行するタスクを指定するための**「承認のタイムアウト時のタスク」**メニューが表示されます。続きの手順については、9-22 ページの「タスクの実行」を参照してください。

承認のエスカレーション

「タイムアウトアクション」で**「承認のエスカレーション」**ラジオボタンを選択すると、次のような**「エスカレーション承認者を決定する方法」**メニューが表示されます。

図 18 「エスカレーション承認者を決定する方法」メニュー

このメニューから次のいずれかのオプションを選択して、エスカレーションされた承認の承認者を決定する方法を指定します。

- **「属性」**― 新しいユーザーのビューで指定された属性の内部から承認者のアカウント ID を決定します。

注　属性は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストに解決する必要があります。

「エスカレーション管理者属性」メニューが表示されたら、リストから属性を選択します。選択した属性が隣のテキストフィールドに表示されます。

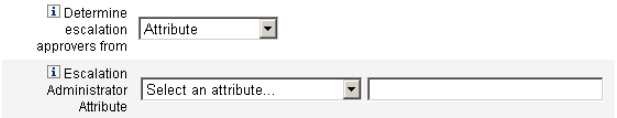


図 19 「エスカレーション管理者属性」メニュー

- **「規則」**― 指定された規則を評価することによって承認者のアカウント ID を決定します。

注　評価されたとき、規則は単一のアカウント ID を表す文字列、またはアカウント ID を要素とするリストを返す必要があります。

「エスカレーション管理者規則」メニューが表示されたら、リストから規則を選択します。

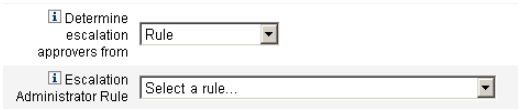


図 20 「エスカレーション管理者規則」メニュー

- **「クエリー」**— 特定のリソースを問い合わせることで承認者のアカウント ID を決定します。

  「エスカレーション管理者クエリー」メニューが表示されたら、次のようにしてクエリーを作成します。

  a. **「問い合わせ先のリソース」**メニューからリソースを選択します。
  b. **「問い合わせ先のリソース属性」**メニューから属性を選択します。
  c. **「比較対象の属性」**メニューから属性を選択します。

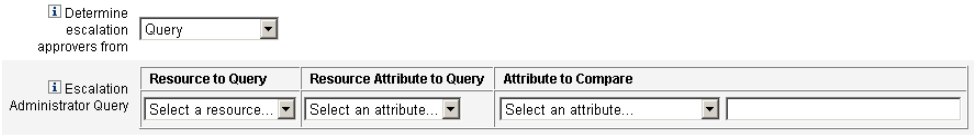


図 21 「エスカレーション管理者クエリー」メニュー

- **「管理者リスト」**(デフォルト) — リストから承認者を明示的に選択します。

  「エスカレーション管理者」選択ツールが表示されたら、次のようにして承認者を選択します。

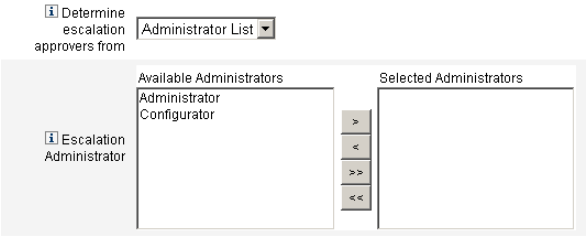


図 22 「エスカレーション管理者」選択ツール

  a. **「利用可能な管理者」**リストから、1 人または複数の管理者の名前を選択します。
  b. > ボタンまたは >> ボタンを使用して、選択した名前を**「選択された管理者」**リストに移動します。

タスクの実行

「タイムアウトアクション」で**「タスクの実行」**ラジオボタンを選択すると、次のような**「承認のタイムアウト時のタスク」**メニューが表示されます。

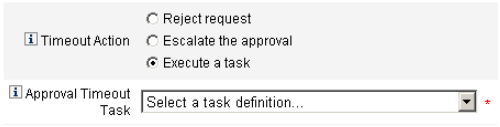


図 23 「承認のタイムアウト時のタスク」メニュー

承認要求がタイムアウトした場合に実行するタスクを指定します。たとえば、要求者がヘルプデスク要求を送信したり、レポートを管理者に送信したりすることを許可できます。

承認フォームの設定

注 ユーザー削除テンプレートには「承認フォーム設定」セクションは含まれません。このセクションはユーザー作成テンプレートおよびユーザー更新テンプレートに対してのみ設定できます。

「承認フォーム設定」セクションの機能を使用して、承認フォームの選択や、属性の承認フォームへの追加 (または承認フォームからの削除) を行うことができます。

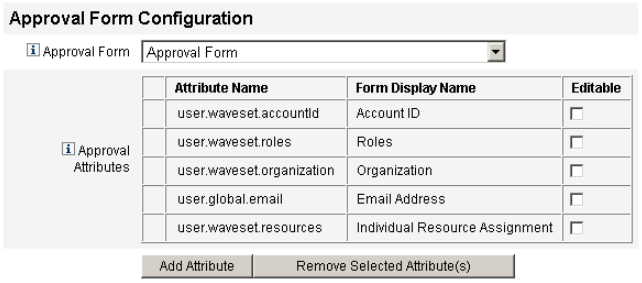


図 24 承認フォームの設定

デフォルトでは、「承認の属性」テーブルには次の標準属性が含まれます。

- `user.waveset.accountId`
- `user.waveset.roles`
- `user.waveset.organization`
- `user.global.email`

- user.waveset.resources

注 デフォルトの承認フォームは、承認属性の表示を許可するように設定されています。デフォルトフォーム以外の承認フォームを使用する場合、「承認の属性」テーブルで指定された承認属性を表示するようにフォームを設定する必要があります。

追加の承認者のための承認フォームを設定するには、次の手順に従います。

1. **「承認フォーム」**メニューからフォームを選択します。
   承認者はこのフォームを使用して承認要求を承認または却下します。
2. 承認者による属性値の編集を許可する場合、**「承認の属性」**テーブルで、各属性の**「編集可能」**列のチェックボックスをオンにします。
   たとえば、user.waveset.accountId 属性のチェックボックスをオンにすると、承認者はユーザーのアカウント ID を変更できます。

注 承認フォーム内でアカウント固有の属性値を変更すると、ユーザーが実際にプロビジョニングされるときに、同じ名前のグローバル属性値もすべてオーバーライドされます。

たとえば、スキーマ属性 description を持つリソース R1 がシステムに存在し、user.accounts[R1].description 属性を編集可能な属性として承認フォームに追加する場合、承認フォーム内で description 属性の値を変更すると、リソース R1 のみを対象に、global.description から伝播された値がオーバーライドされます。

3. **「属性の追加」**または**「選択している属性の削除」**ボタンをクリックして、新しいユーザーのアカウントデータ内の属性のうち承認フォームに表示するものを指定します。
   - 属性をフォームに追加する方法については、9-24 ページの「属性の追加」を参照してください。
   - 属性をフォームから削除する方法については、9-24 ページの「属性の削除」を参照してください。

注 XML ファイルを変更しない限り、デフォルトの属性を承認フォームから削除することはできません。

属性の追加

属性を承認フォームに追加するには、次の手順に従います。

1. 「承認の属性」テーブルの下にある**「属性の追加」**ボタンをクリックします。
   次の図に示すように、「承認の属性」テーブルの**「属性名」**列内で選択メニューがアクティブになります。

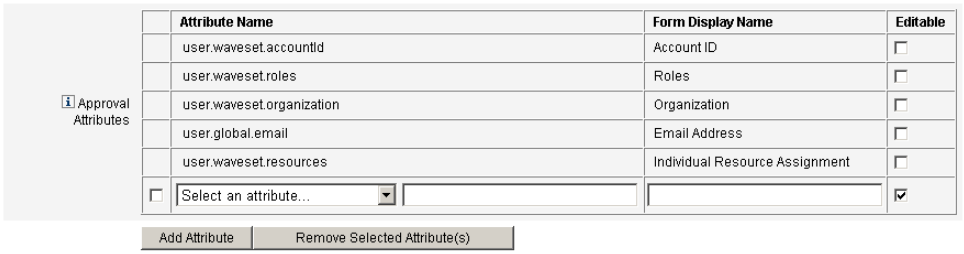


図 25 承認属性の追加

2. メニューから属性を選択します。
   選択された属性名が隣のテキストフィールドに表示され、属性のデフォルトの表示名が「フォーム表示名」列に表示されます。
   たとえば、`user.waveset.organization` 属性を選択した場合、表には次の情報が含まれます。
   - 必要に応じて、それぞれのテキストフィールドに新しい名前を入力することによって、デフォルトの属性名またはデフォルトのフォーム表示名を変更できます。
   - 承認者による属性値の変更を許可する場合、**「編集可能」**チェックボックスをオンにします。
     たとえば、あらかじめ定義されているユーザーの電子メールアドレスなどの情報を承認者が変更したい場合があります。
3. これらの手順を繰り返して、必要な属性を指定します。

属性の削除

注 XML ファイルを変更しない限り、デフォルトの属性を承認フォームから削除することはできません。

承認フォームから属性を削除するには、次の手順に従います。

1. 「承認の属性」テーブルの左端の列で、1 つ以上のチェックボックスをオンにします。
2. **「選択している属性の削除」**ボタンをクリックすると、選択した属性が「承認の属性」テーブルからただちに削除されます。
   たとえば、次の状態のテーブルで**「選択している属性の削除」**ボタンをクリックすると、`user.global.firstname` および `user.waveset.organization` がテーブルから削除されます。

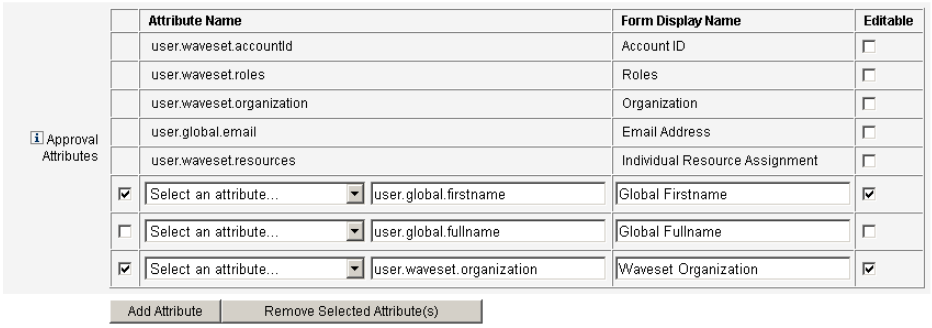


図 26 承認属性の削除

「監査」タブの設定

設定可能なすべてのタスクテンプレートで、特定のタスクを監査するためのワークフローを設定することができます。特に、「監査」タブを設定することにより、ワークフローイベントの監査の有無や、レポート対象として記録する属性を指定することができます。

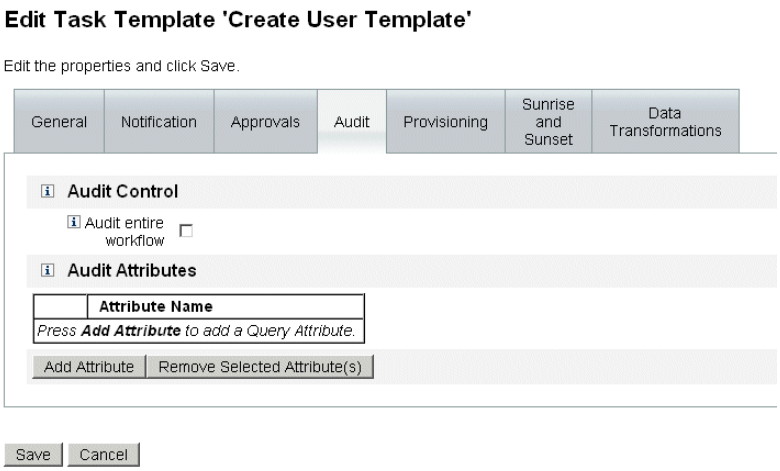


図 27 ユーザー作成テンプレートの監査設定

ユーザーテンプレートの「監査」タブから監査を設定するには、次の手順に従います。

1. **「ワークフロー全体の監査」**チェックボックスをオンにして、ワークフローの監査機能を有効にします。
2. 「属性の監査」セクションの**「属性の追加」**ボタンをクリックして、レポート対象として記録する属性を選択します。

3. 「属性の監査」テーブルに**「属性の選択」**メニューが表示されたら、リストから属性を選択します。
   属性名が隣のテキストフィールドに表示されます。

図 28 属性の追加

「属性の監査」テーブルから属性を削除するには、次の手順に従います。

1. 削除する属性の隣にあるチェックボックスを有効にします。

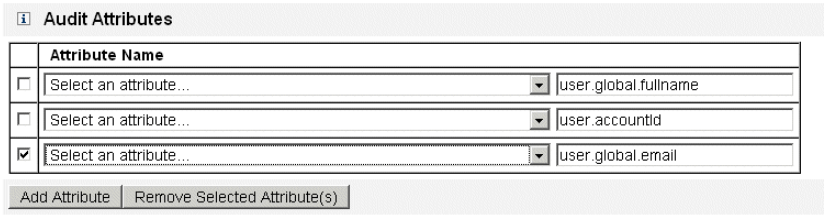


図 29 user.global.email 属性の削除

2. **「選択している属性の削除」**ボタンをクリックします。

このタブの設定を終了したら、次の処理を実行できます。

- 別のタブを選択して、テンプレートの編集を続けます。
- **「保存」**をクリックして変更を保存し、「タスクの設定」ページに戻ります。
- **「キャンセル」**をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

「プロビジョニング」タブの設定

注　このタブはユーザー作成テンプレートおよびユーザー更新テンプレートに対してのみ使用できます。

「プロビジョニング」タブでは、プロビジョニングに関連する次のオプションを設定できます。

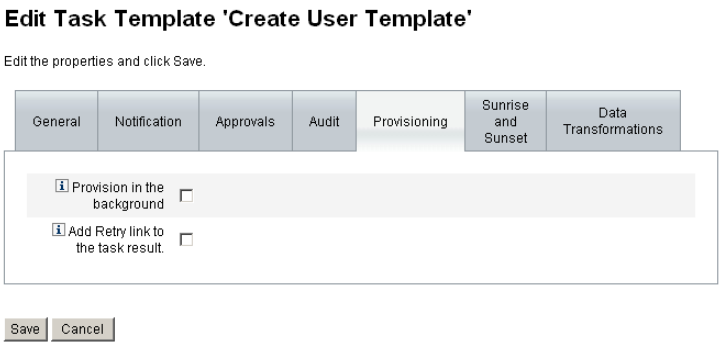


図 30 「プロビジョニング」タブ : ユーザー作成テンプレート

- **「バックグラウンドでプロビジョニング」** ― 作成、削除、または更新タスクを同期的に実行するのではなくバックグラウンドで実行するには、このチェックボックスをオンにします。

  バックグラウンドでプロビジョニングを行うことにより、タスクの実行中も Identity Manager での作業を継続できます。
- **「再試行リンクをタスク結果に追加します」** ― タスク実行の結果としてプロビジョニングエラーが発生したときに**再試行**リンクをユーザーインタフェースに追加する場合は、このチェックボックスをオンにします。**再試行**リンクにより、ユーザーは最初の試行でタスクが失敗した場合にタスクを再試行できます。

「プロビジョニング」タブの設定を終了したら、次の処理を実行できます。

- 別のタブを選択して、テンプレートの編集を続けます。
- **「保存」**をクリックして変更を保存し、「タスクの設定」ページに戻ります。
- **「キャンセル」**をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

「サンライズとサンセット」タブの設定

注　　このタブはユーザー作成テンプレートのみに対して使用できます。

「サンライズとサンセット」タブでは、次の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。

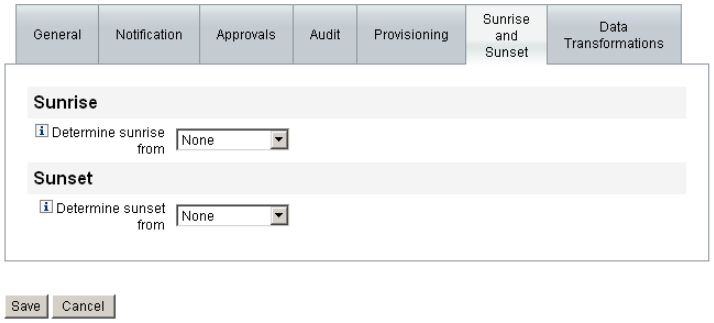


図 31　「サンライズとサンセット」タブ : ユーザー作成テンプレート

この節の残りでは、「サンライズとサンセット」タブの設定手順を説明します。説明する内容は次のとおりです。

- 9-28 ページの「サンライズの設定」
- 9-31 ページの「サンセットの設定」

サンライズの設定

ここでは、新しいユーザーのプロビジョニングが行われる日時を決定する手順と、サンライズの作業項目を所有するユーザーを指定する手順について説明します。

サンライズを設定するには、次の手順に従います。

1. **「サンライズを決定する方法」**メニューから次のいずれかのオプションを選択して、Identity Manager がプロビジョニングの日時を決定する方法を指定します。
   - **経過時間の指定** ― 指定された時間が経過するまでプロビジョニングを保留します。続きの手順については、9-29 ページを参照してください。
   - **日付の指定** ― 将来の指定された日付までプロビジョニングを保留します。続きの手順については、9-29 ページを参照してください。

- **属性の指定** — ユーザーのビューでの属性値に基づいて、指定された日時までプロビジョニングを保留します。属性には日付 / 時刻文字列が含まれている必要があります。日付 / 時刻文字列を含むように属性を指定するとき、データが従うべきデータ形式を指定できます。

  続きの手順については、9-30 ページを参照してください。
- **規則の指定** — 評価されたときに日付 / 時刻文字列を生成する規則に基づいてプロビジョニングを保留します。属性を指定するとき、データが従うべきデータ形式を指定できます。

  続きの手順については、9-31 ページを参照してください。

注　**「サンライズを決定する方法」**メニューのデフォルトでは、プロビジョニングをただちに行うようにする**「なし」**が選択されています。

2. **「作業項目の所有者」**メニューからユーザーを選択して、サンライズの作業項目を所有する人物を指定します。

注　サンライズ作業項目は「承認」タブから利用可能です。

3. サンライズの設定が終了したら、次の処理を実行できます。
   - 別のタブを選択して、ユーザー作成テンプレートの編集を続けます。
   - **「保存」**をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - **「キャンセル」**をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

経過時間の指定

指定された時間が経過するまでプロビジョニングを保留するには、次の手順に従います。

1. **「サンライズを決定する方法」**メニューから**「指定された経過時間」**を選択します。
2. **「サンライズを決定する方法」**メニューの右側に新しいテキストフィールドとメニューが表示されたら、空のテキストフィールドに数値を入力し、メニューから時間の単位を選択します。

   たとえば、新しいユーザーを 2 時間後にプロビジョニングしたい場合、次のように指定します。

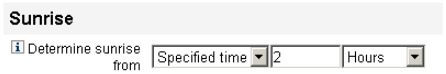


図 32　新しいユーザーを 2 時間後にプロビジョニングする設定

日付の指定

指定された日付までプロビジョニングを保留するには、次の手順に従います。

1. **「サンライズを決定する方法」**メニューから**「日付の指定」**を選択します。

   「サンライズを決定する方法」メニューの右側に、次の新しいメニューが表示されます。

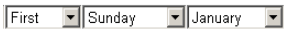


図 33 新しいメニュー

2. これらの新しいメニューを使用して、プロビジョニングを実行する週、曜日、および月を指定します。

   たとえば、新しいユーザーを 9 月の第 2 月曜日にプロビジョニングしたい場合、次のように指定します。

図 34 日付による新しいユーザーのプロビジョニング

属性の指定

ユーザーアカウントデータ内の属性値に基づいてプロビジョニング日時を決定するには、次の手順に従います。

1. **「サンライズを決定する方法」**メニューから**「属性」**を選択します。次のオプションがアクティブになります。
   - **「サンライズの属性」**メニュー ― このテンプレートで設定するタスクと関連付けられたビューに対して現在定義されている属性のリストが提示されます。
   - **「特定の日付形式」**チェックボックスおよびメニュー ― 必要に応じて、属性値の日付形式文字列を指定できます。

注 **「特定の日付形式」**チェックボックスをオンにしない場合、日付文字列は `FormUtil` メソッドの `convertDateToString` に対して使用できる形式に従う必要があります。サポートされている日付形式の完全な一覧については、製品ドキュメントを参照してください。

2. **「サンライズの属性」**メニューから属性を選択します。
3. 必要な場合、**「特定の日付形式」**チェックボックスをオンにし、アクティブになった**「特定の日付形式」**フィールドに日付形式文字列を入力します。

   たとえば、ユーザーの `waveset.accountId` 属性値に基づき、日、月、および年の形式を使用して新しいユーザーをプロビジョニングするには、次のように指定します。

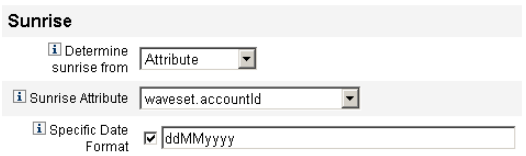


図 35 属性による新しいユーザーのプロビジョニング

規則の指定

指定された規則を評価することでプロビジョニング日時を決定するには、次の手順に従います。

1. **「サンライズを決定する方法」**メニューから**「規則」**を選択します。次のオプションがアクティブになります。
   - **「サンライズの規則」**メニュー ― システムに対して現在定義されている規則の一覧が提示されます。
   - **「特定の日付形式」**チェックボックスおよびメニュー ― 必要に応じて、規則の戻り値の日付形式文字列を指定できます。

注 **「特定の日付形式」**チェックボックスをオンにしない場合、日付文字列は `FormUtil` メソッドの `convertDateToString` に対して使用できる形式に従う必要があります。サポートされている日付形式の完全な一覧については、製品ドキュメントを参照してください。

2. **「サンライズの規則」**メニューから規則を選択します。
3. 必要な場合、**「特定の日付形式」**チェックボックスをオンにし、アクティブになった**「特定の日付形式」**フィールドに日付形式文字列を入力します。

   たとえば、「電子メール」規則に基づき、年、月、日、時、分、および秒の形式を使用して新しいユーザーをプロビジョニングするには、次の手順に従います。

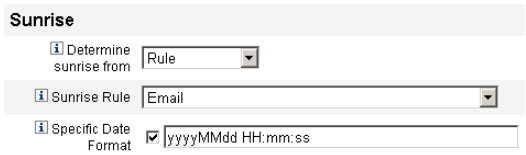


図 36 規則による新しいユーザーのプロビジョニング

サンセットの設定

サンセット (プロビジョニング解除) を設定するためのオプションおよび手順は基本的に、「サンライズの設定」で説明した、サンライズ (プロビジョニング) の設定に使用するものと同じです。

唯一の違いは、「サンセット」セクションには**「サンセットタスク」**メニューがある点です。このメニューを使用して、指定された日時にユーザーをプロビジョニング解除するためのタスクを指定する必要があります。

サンセットを設定するには、次の手順に従います。

1. **「サンセットを決定する方法」**メニューを使用して、プロビジョニング解除がいつ行われるかを決定するための方法を指定します。

注 **「サンセットを決定する方法」**メニューでは、プロビジョニング解除をただちに行える**「なし」**オプションがデフォルトによって選択されます。

- **「指定された経過時間」** ― 指定された時間が経過するまでプロビジョニング解除を保留します。手順については、9-29 ページの「経過時間の指定」を参照してください。
- **「日付の指定」** ― 将来の指定された日付までプロビジョニング解除を遅らせます。手順については、9-29 ページの「日付の指定」を参照してください。
- **「属性」** ― ユーザーのアカウントデータ内の属性の値に基づいて、指定された日時までプロビジョニング解除を保留します。属性には日付 / 時刻文字列が含まれている必要があります。日付 / 時刻文字列を含むように属性を指定するとき、データが従うべき日付形式を指定できます。

  手順については、9-30 ページの「属性の指定」を参照してください。
- **「規則」** ― 評価されたときに日付 / 時刻文字列を生成する規則に基づいてプロビジョニング解除を保留します。属性を指定するとき、データが従うべき日付形式を指定できます。

  手順については、9-31 ページの「規則の指定」を参照してください。

2. **「サンセットタスク」** メニューを使用して、指定された日時にユーザーをプロビジョニング解除するためのタスクを指定します。
3. このタブの設定を終了したら、次の処理を実行できます。
   - 別のタブを選択して、テンプレートの編集を続けます。
   - **「保存」** をクリックして変更を保存し、「タスクの設定」ページに戻ります。
   - **「キャンセル」** をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

「データ変換」タブの設定

注 このタブはユーザー作成テンプレートおよびユーザー更新テンプレートに対してのみ使用できます。

ワークフローの実行時にユーザーアカウントデータを変更したい場合、「データ変換」タブを使用して、Identity Manager がプロビジョニング中にデータを変換する方法を指定できます。

例としては、企業のポリシーに準拠した電子メールアドレスをフォームまたは規則に生成させたい場合や、サンライズまたはサンセット日付を生成したい場合があります。

「データ変換」タブを選択すると、次のページが表示されます。

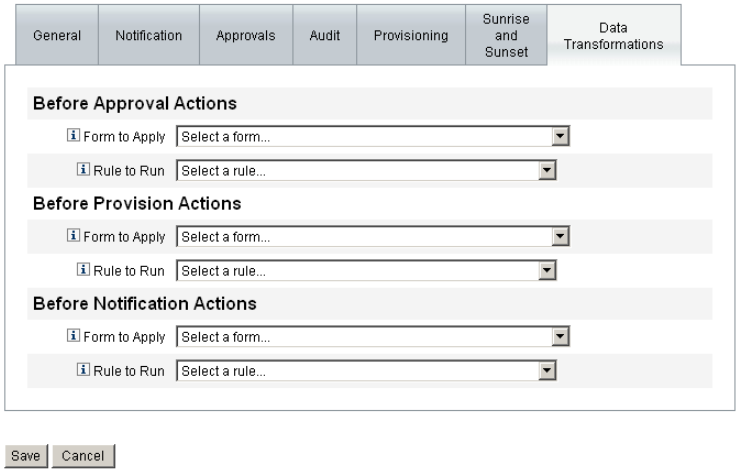


図 37 「データ変換」タブ : ユーザー作成テンプレート

このページは次のセクションで構成されます。

- **「承認アクション前」** ― 指定された承認者に承認要求を送信する前にユーザーアカウントデータを変換したい場合、このセクションのオプションを設定します。
- **「プロビジョニングアクション前」** ― プロビジョニングアクションの前にユーザーアカウントデータを変換したい場合、このセクションのオプションを設定します。
- **「通知アクション前」** ― 指定された受信者に通知が送信される前にユーザーアカウントデータを変換したい場合、このセクションのオプションを設定します。

各セクションで、次のオプションを設定できます。

- **「適用するフォーム」** メニュー ― システムに対して現在設定されているフォームのリストが提示されます。これらのメニューを使用して、ユーザーアカウントからのデータを変換するために使われるフォームを指定します。
- **「実行する規則」** メニュー ― システムに対して現在設定されている規則のリストが提示されます。これらのメニューを使用して、ユーザーアカウントからのデータを変換するために使われる規則を指定します。

このタブの設定を終了したら、次の処理を実行できます。

- 別のタブを選択して、テンプレートの編集を続けます。
- **「保存」** をクリックして変更を保存し、「タスクの設定」ページに戻ります。
- **「キャンセル」** をクリックして変更を破棄し、「タスクの設定」ページに戻ります。

10 PasswordSync

この章では、Sun Java™ System Identity Manager の PasswordSync 機能について説明します。この機能を使用すると、Windows クライアントが Windows Active Directory または Windows NT ドメイン内でパスワードを変更し、Identity Manager と変更を同期できるようになります。

PasswordSync の概要

PasswordSync 機能は、Windows Active Directory および Windows NT ドメイン上で行われたユーザーパスワードの変更を、Identity Manager で定義されているほかのリソースと同期された状態に保ちます。PasswordSync は、Identity Manager と同期されるドメイン内の各ドメインコントローラにインストールする必要があります。PasswordSync は Identity Manager とは別にインストールする必要があります。

PasswordSync をドメインコントローラにインストールすると、コントローラは、Java Messaging Service (JMS) クライアントのプロキシとして機能するサーブレットと通信します。その後、サーブレットが JMS 対応のメッセージキューと通信します。JMS Listener リソースアダプタはキューからメッセージを削除し、ワークフロータスクを使用してパスワード変更を処理します。ユーザーに割り当てられたすべてのリソース上でパスワードが更新され、SMTP サーバーがユーザーに電子メールを送信し、パスワード変更の状態をユーザーに通知します。

注 パスワード変更は、同期のために Identity Manager サーバーに転送される変更要求に対するネイティブのパスワードポリシーと符合する必要があります。提案されたパスワード変更がネイティブのパスワードポリシーと符合しない場合、ADSI はエラーダイアログを表示し、同期データは Identity Manager に送信されません。

PasswordSync をインストールする前に

PasswordSync 機能は、Windows 2000、Windows 2003、および Windows NT のドメインコントローラ上でのみセットアップできます。Identity Manager と同期されるドメイン内の各ドメインコントローラに PasswordSync をインストールする必要があります。

PasswordSync は JMS サーバーと接続できる必要があります。JMS システムの要件の詳細については、『Identity Manager Resources Reference』の JMS Listener リソースアダプタに関するマニュアルを参照してください。

加えて、PasswordSync には次の要件があります。

- 各ドメインコントローラに Microsoft .NET 1.1 以降がインストールされている必要があります。
- PasswordSync の以前のバージョンをすべて削除する必要があります。

これらの要件については、以降の各節で詳しく説明します。

Microsoft .NET 1.1 のインストール

PasswordSync を使用するには、Microsoft .NET Framework 1.1 以降をインストールする必要があります。
このフレームワークは、Windows 2003 ドメインコントローラを使用している場合にはデフォルトでインストールされています。Windows 2000 または Windows NT ドメインコントローラを使用している場合、次の場所の Microsoft Download Center からツールキットをダウンロードできます。

http://www.microsoft.com/downloads

注意

- Microsoft .NET Framework 1.1 の動作には Internet Explorer 5.01 以降を必要とします。
  (Windows 2000 SP4 に付属の) Internet Explorer 5.0 は使用できません。
- フレームワークツールキットをすばやく見つけるには、**「Keywords」**検索フィールドに「**`NET Framework 1.1 Redistributable`**」と入力してください。
- ツールキットにより . NET Framework 1.1 がインストールされます。

PasswordSync の以前のバージョンをアンインストールする

新しいバージョンをインストールする前に、以前にインストールした PasswordSync のインスタンスをすべて削除する必要があります。

- 以前にインストールしたバージョンの PasswordSync が `IdmPwSync.msi` インストーラをサポートする場合、Windows の「プログラムの追加と削除」標準ユーティリティーを使用してプログラムを削除できます。
- 以前にインストールしたバージョンの PasswordSync が `IdmPwSync.msi` インストーラをサポートしない場合、InstallAnywhere アンインストーラを使用してプログラムを削除します。

PasswordSync のインストール

ここでは、PasswordSync 設定アプリケーションをインストール、設定、およびアンインストールするための手順について説明します。

注　Identity Manager と同期されるドメイン内の各ドメインコントローラに PasswordSync をインストールする必要があります。

1. Identity Manager のインストールメディアから、`pwsync¥IdmPwSync.msi` アイコンをクリックします。「Welcome」ウィンドウが表示されます。

   インストールウィザードには、次のナビゲーションボタンがあります。
   - **「Cancel」**：このボタンをクリックすると、変更を保存せずにいつでもウィザードを終了できます。
   - **「Back」**：1 つ前のダイアログボックスに戻る場合にクリックします。
   - **「Next」**：次のダイアログボックスに進む場合にクリックします。
2. 「Welcome」画面の情報を読み、「Next」をクリックして「Choose Setup Type PasswordSync Configuration」ウィンドウを表示します。
   PasswordSync のセットアップ
3. PasswordSync のフルパッケージをインストールする場合は**「Typical」**または**「Complete」**をクリックします。インストールするパッケージ内容を変更する場合は**「Custom」**をクリックします。
4. **「Install」**をクリックして製品をインストールします。PasswordSync が正常にインストールされると、次のウィンドウが表示されます。
5. **「Finish」**をクリックしてインストールプロセスを終了します。PasswordSync の設定を開始できるように、**「Launch Configuration Application」**が選択されていることを確認してください。このプロセスの詳細については、「PasswordSync の設定」を参照してください。

注　変更を有効にするにはシステムを再起動する必要がある、というメッセージがダイアログボックスに表示されます。PasswordSync の設定を完了するまでは再起動の必要はありませんが、PasswordSync を実装する前にドメインコントローラを再起動する必要があります。

次の表は、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の一覧です。

インストールされるコンポーネント	説明
`%$INSTALL_DIR$%¥configure.exe`	PasswordSync 設定プログラム
`%$INSTALL_DIR$%¥configure.exe.manifest`	設定プログラムのデータファイル
`%$INSTALL_DIR$%¥DotNetWrapper.dll`	.NET SOAP 通信を処理する DLL

インストールされるコンポーネント	説明
%$INSTALL_DIR$%¥passwordsyncmsgs.dll	PasswordSync メッセージを処理する DLL
%SYSTEMROOT%¥SYSTEM32¥lhpwic.dll	パスワード通知 DLL。この DLL は Windows の PasswordChangeNotify() 関数を実装する

PasswordSync の設定

インストーラから設定アプリケーションを実行する場合、ウィザード形式の設定画面が表示されます。ウィザードを終了し、以後 PasswordSync 設定アプリケーションを実行するときは、タブの選択によって設定画面を切り替えることができます。

PasswordSync を設定するには、次の手順に従います。

1. まだ実行されていない場合、PasswordSync 設定アプリケーションを開始します。デフォルトでは、設定アプリケーションはプログラム > Sun Java System Identity Manager PasswordSync>Configuration ディレクトリにインストールされています。

   次のダイアログが表示されます。

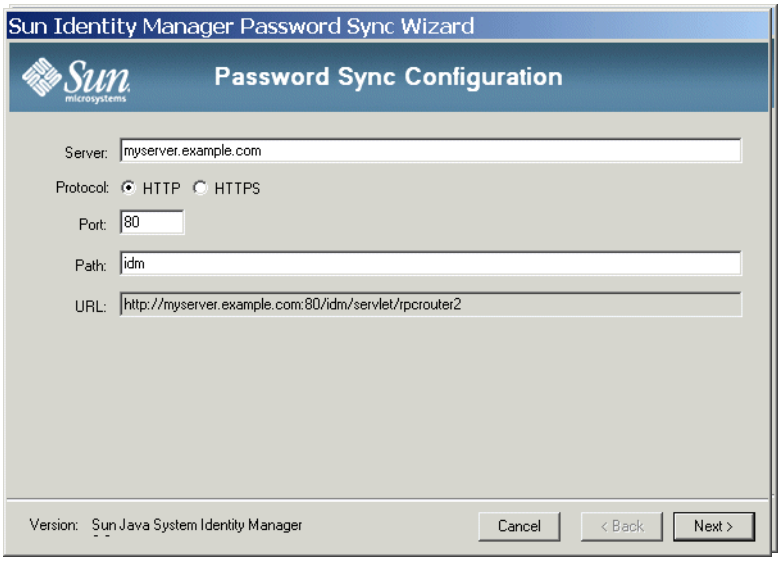


図 1 サーバー設定ダイアログ

   必要に応じてフィールドを編集します。

- 「**Server**」は、Identity Manager がインストールされたアプリケーションサーバーの完全修飾ホスト名または IP アドレスと置き換える必要があります。
- 「**Protocol**」では、Identity Manager へのセキュア接続を行うかどうかを指定します。「HTTP」を選択した場合、デフォルトのポートは 80 です。「HTTPS」を選択した場合、デフォルトのポートは 443 です。
- 「**Path**」には、アプリケーションサーバー上の Identity Manager へのパスを指定します。
- 「**URL**」の値はほかのフィールドの値を基に生成されます。「URL」フィールドの値は編集できません。

2. 「**Next**」をクリックして、プロキシサーバーの設定ページを表示します。

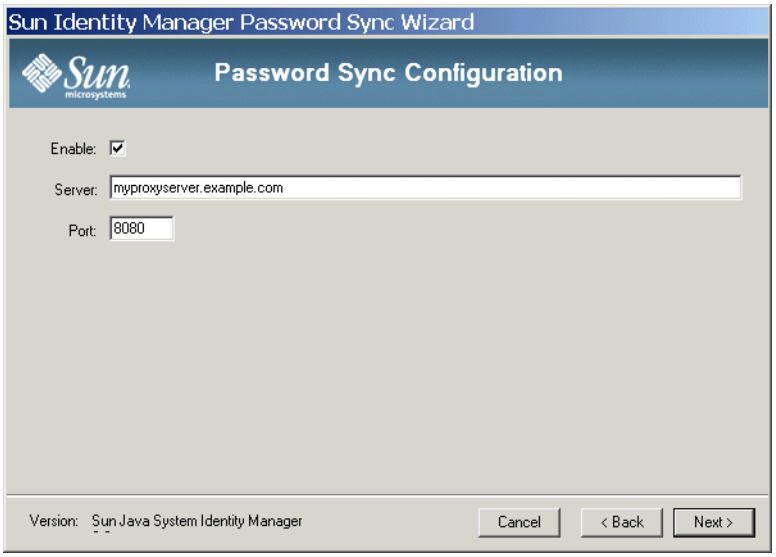


図 2 プロキシサーバーダイアログ

必要に応じてフィールドを編集します。

- プロキシサーバーが必要な場合は「**Enable**」をクリックします。
- 「**Server**」は、プロキシサーバーの完全修飾ホスト名または IP アドレスと置き換える必要があります。
- 「**Port**」: サーバーに対して使用可能なポート番号を指定します
  (デフォルトのプロキシポートは 8080、デフォルトの HTTPS ポートは 443)。

3. 「**Next**」をクリックして、JMS 設定ダイアログを表示します。

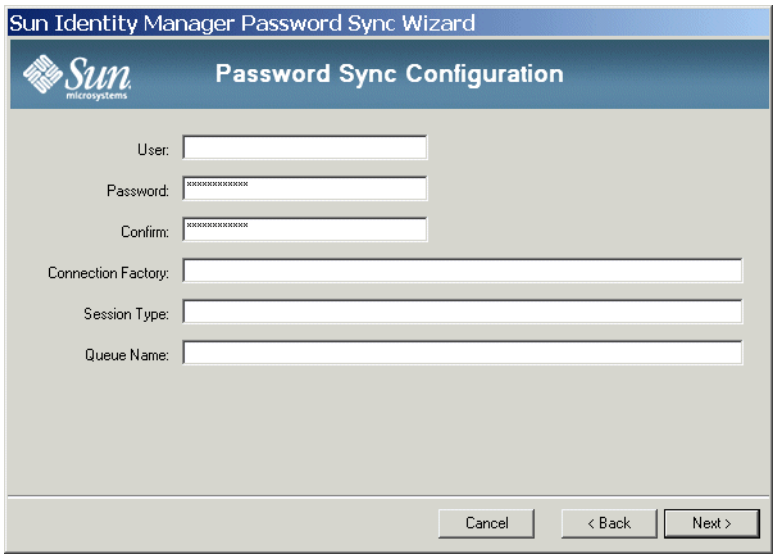


図 3 JMS 設定ダイアログ

必要に応じてフィールドを編集します。

- 「**User**」には、新しいメッセージをキューに送る JMS ユーザー名を指定します。
- 「**Password**」と「**Confirm**」では、JMS ユーザーのパスワードを指定します。
- 「**Connection Factory**」には、使用する JMS 接続ファクトリの名前を指定します。JMS システム上にすでに存在しているファクトリを指定する必要があります。
- 「**Session Type**」はほとんどの場合、ローカルセッショントランザクションが使われることを表す LOCAL に設定することが推奨されます。セッションは各メッセージの受信後にコミットされます。指定できるその他の値は AUTO、CLIENT、および DUPS_OK です。
- 「**Queue Name**」には、パスワード同期イベントの送信先を指定します。

4. 「**Next**」をクリックして、JMS プロパティーダイアログを表示します。

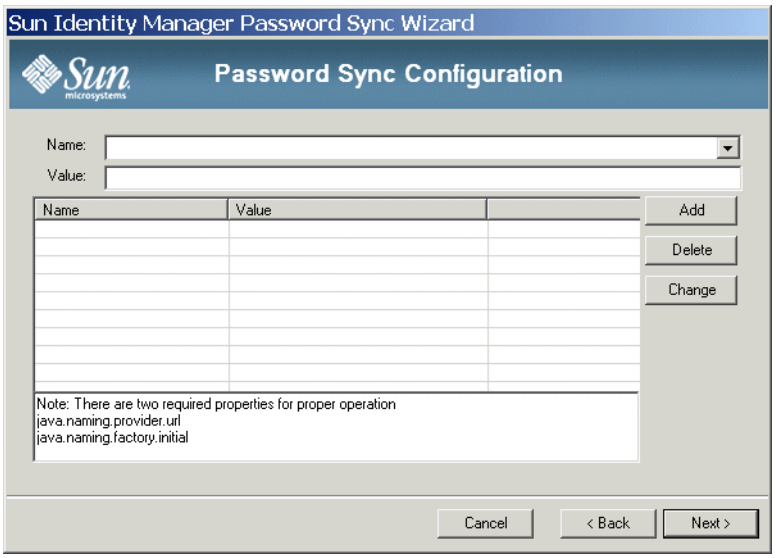


図 4 JMS プロパティーダイアログ

JMS プロパティーダイアログでは、初期 JNDI コンテキストの構築に使われる一連のプロパティーを定義します。次の名前と値のペアを定義する必要があります。

- `java.naming.provider.url` ー 値は JNDI サービスを実行しているマシンの URI に設定する必要があります。
- `java.naming.factory.initial` ー 値は JNDI サービスプロバイダの初期コンテキストファクトリのクラス名 (パッケージを含む) に設定する必要があります。

「Name」プルダウンメニューの内容は、`java.naming` パッケージのクラスの一覧です。クラス名としてクラスまたは型を選択し、「Value」フィールドにその対応する値を入力します。

5. **「Next」**をクリックして電子メールダイアログを表示します。

   電子メールダイアログでは、通信エラーや Identity Manager の外部で発生したその他のエラーが原因でユーザーのパスワード変更が正しく同期されない場合に、電子メール通知を送信するかどうかを設定できます。

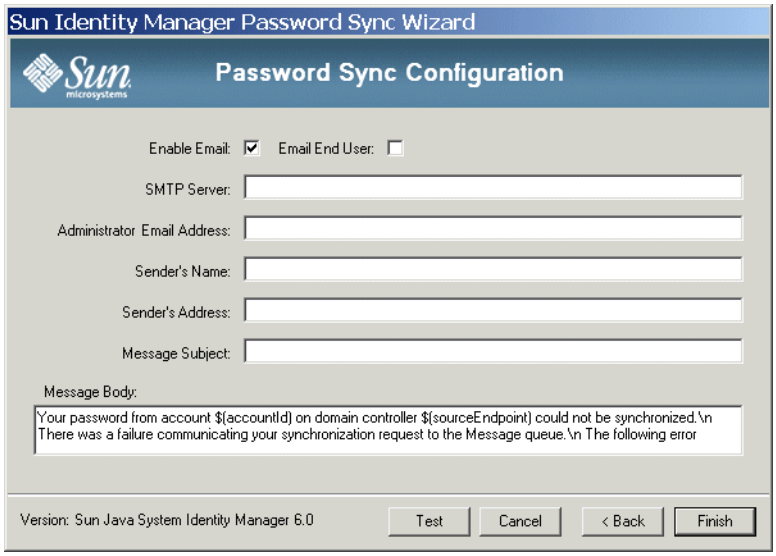


図 5 電子メールダイアログ

必要に応じてフィールドを編集します。

- この機能を有効にするには「**Enable Email**」を選択します。ユーザーが通知を受け取る場合は「**Email End User**」を選択します。このオプションを選択しない場合、管理者だけが通知を受け取ります。
- 「**SMTP Server**」は、障害通知の送信時に使われる SMTP サーバーの完全修飾名または IP アドレスです。
- 「**Administrator Email Address**」は、通知の送信に使われる電子メールアドレスです。
- 「**Sender's Name**」は送信者の「friendly name」です。
- 「**Sender's Address**」は送信者の電子メールアドレスです。
- 「**Message Subject**」には、すべての通知に共通する件名行を指定します。
- 「**Message Body**」には通知のテキストを指定します。

  メッセージの本文には次の変数を含めることができます。

  - `$(accountId)` — パスワードを変更しようとしているユーザーのアカウント ID。
  - `$(sourceEndpoint)` — パスワード通知ツールがインストールされたドメインコントローラのホスト名。この情報は、トラブルが発生したマシンの特定に役立ちます。
  - `$(errorMessage)` — エラーが発生したことを説明するエラーメッセージ。

6. 「**Finish**」をクリックして変更を保存します。

設定アプリケーションの 2 回目以降の実行時には、ウィザードではなく一連のタブで構成される画面が表示されます。設定アプリケーションをウィザード形式で表示したい場合、コマンド行から次のコマンドを入力します。

```
C:¥InstallDir¥Configure.exe -wizard
```

PasswordSync のデバッグ

この節では、PasswordSync で発生する問題の診断に必要な情報の見つけ方と、設定ツールを使用してトレースを有効にする方法について説明します。また、PasswordSync をデバッグしたり、設定ツールからは実装できない機能を有効にしたりするために必要なレジストリキーの一覧を示します。

エラーログ

PasswordSync はすべての障害情報を Windows イベントビューアに書き込みます。エラーログエントリのソース名は PasswordSync です。

トレースログ

設定ツールを最初に実行するとき、ウィザードにはトレースを設定するためのパネルがありません。ただし、設定ツールの 2 回目以降の実行では、**「Trace」**タブが常に表示されます。

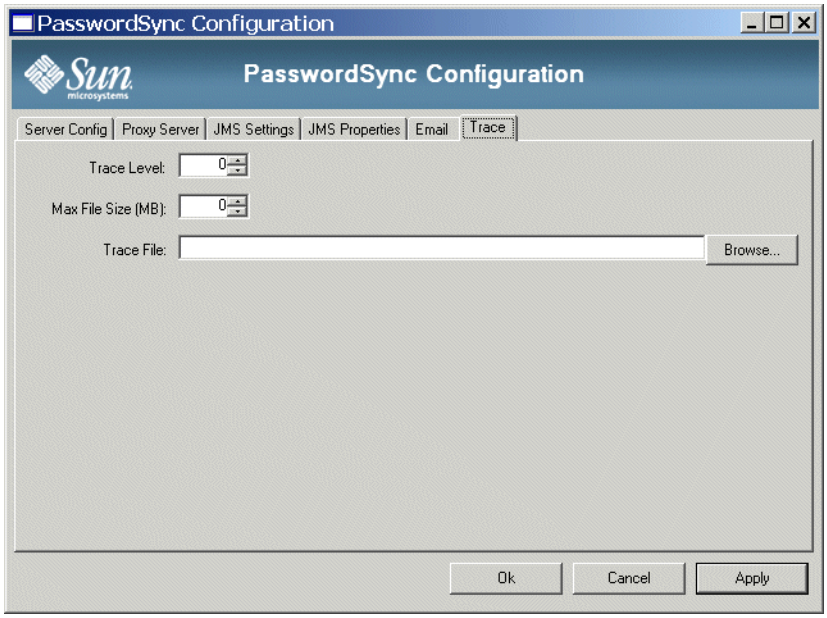


図 6 トレースダイアログ

「Trace Level」フィールドでは、PasswordSync がトレースログに書き込む情報の詳細度を指定します。値 0 はトレースが無効であることを表し、値 4 は最も詳細な情報を出力することを表します。

トレースファイルが**「Max File Size (MB)」**フィールドで指定されたサイズを超えると、PasswordSync はベース名に .bk を追加したファイルにそれまでのログを移動します。たとえば、トレースファイルを C:¥logs¥pwicsvc.log に、トレースファイルの最大サイズを 100M バイトに設定した場合、トレースファイルが 100M バイトを超えると、PasswordSync はそれまでのファイルの名前を C:¥logs¥pwicsvc.log.bk に変更し、以降のデータを新しい C:¥logs¥pwicsvc.log ファイルに書き込みます。

レジストリキー

次の表に示すレジストリキーは、Windows レジストリエディタを使用して編集できます。キーの位置は HKEY_LOCAL_MACHINE¥SOFTWARE¥Waveset¥Lighthouse¥PasswordSync キーです。この場所にはその他のキーもありますが、それらのキーは設定ツールを使用して編集できます。

キー名	種類	説明
allowInvalidCerts	REG_DWORD	1 に設定すると、.NET クライアント上で次のフラグが設定されます。 • SECURITY_FLAG_IGNORE_UNKNOWN_CA • INTERNET_FLAG_IGNORE_CERT_CN_INVALID • INTERNET_FLAG_IGNORE_CERT_DATE_INVALID その結果、期限が切れた証明書や CN またはホスト名が無効な証明書をクライアントが受け入れるようになります。この設定は SSL 使用時にのみ適用されます。 この設定は、ほとんどの証明書が無効な認証局 (CA) から発行されるテスト環境でデバッグを行っているときに役立ちます。 デフォルトは 0 です。
clientConnectionFlags	REG_DWORD	.NET SOAP クライアントに渡されるオプションの接続フラグ。 デフォルトは 0 です。
clientSecurityFlags	REG_DWORD	.NET SOAP クライアントに渡すことができるオプションのセキュリティーフラグ。 デフォルトは 0 です。

キー名	種類	説明
installdir	REG_SZ	PasswordSync アプリケーションがインストールされたディレクトリ。
soapClientTimeout	REG_DWORD	SOAP クライアントが Identity Manager サーバーと通信してエラーが発生するまでのタイムアウト時間 (ミリ秒)。

PasswordSync のアンインストール

PasswordSync アプリケーションをアンインストールするには、Windows のコントロールパネルから**「アプリケーションの追加と削除」**を選択します。次に、「Sun Java System Identity Manager PasswordSync」を選択して**「削除」**をクリックします。

注　PasswordSync は、Identity Manager のインストールメディアをロードし、`pwsync¥IdmPwSync.msi` アイコンをクリックしてアンインストール (または再インストール) することもできます。

アンインストールを完了するにはシステムを再起動する必要があります。

PasswordSync の配備

PasswordSync を配備するには、Identity Manager で次の作業を行う必要があります。

- JMS リスナーアダプタを設定する
- ユーザーパスワード同期ワークフローを実装する
- 通知を設定する

JMS リスナーアダプタの設定

メッセージがドメインコントローラによって間接的にキューに配置されたら、それらのメッセージを受け入れるためにリソースアダプタを設定する必要があります。JMS リスナーリソースアダプタを作成し、キューと通信するようにそのアダプタを設定する必要があります。このアダプタの設定の詳細については、『Identity Manager Resources Reference』を参照してください。

次のリソースパラメータを設定する必要があります。

「宛先タイプ」 – 通常、この値はキューに設定されます。1 人の加入者が存在し、また複数の発行者が存在する可能性があるため、トピックは通常は関係しません。

「初期コンテキスト JNDI プロパティー」 – このテキストボックスでは、初期 JNDI コンテキストの構築に使われる一連のプロパティーを定義します。次の名前と値のペアを定義する必要があります。

- java.naming.provider.url — 値は JNDI サービスを実行しているマシンの URI に設定する必要があります。
- java.naming.factory.initial — 値は JNDI サービスプロバイダの初期コンテキストファクトリのクラス名 (パッケージを含む) に設定する必要があります。

追加のプロパティーの定義が必要な場合があります。プロパティーと値のリストは、設定アプリケーションの JMS 設定ページで指定するものと一致することが推奨されます。

「接続ファクトリの JNDI 名」 — 接続ファクトリの名前 (JMS サーバー上で定義されたもの)。

「ユーザー」および**「パスワード」** — キューから新しいイベントを要求する管理者のアカウント名とパスワード。

「Reliable Messaging サポート」 — LOCAL (ローカルトランザクション) を選択します。それ以外のオプションはパスワード同期には使用しません。

「メッセージマッピング」 — 「java:com.waveset.adapter.jms.PasswordSyncMessageMapper」を入力します。このクラスは、JMS サーバーからのメッセージを、ユーザーパスワード同期ワークフローで使用できる形式に変換します。

ユーザーパスワード同期ワークフローの実装

デフォルトのユーザーパスワード同期ワークフローは、JMS リスナーアダプタから送られてくる個々の要求を受け取ってチェックアウトし、ChangeUserPassword ビューアに戻します。チェックインが完了したあと、ワークフローはすべてのリソースアカウントに対して処理を繰り返し、ソースリソースを除くすべてのリソースを選択します。Identity Manager は、すべてのリソースに対してパスワード変更が成功したかどうかを電子メールでユーザーに通知します。

ユーザーパスワード同期ワークフローのデフォルト実装を使用する場合、JMS リスナーアダプタインスタンスの処理規則にその実装を割り当てます。処理規則はアダプタの Active Sync ウィザードで割り当てることができます。

デフォルトのユーザー同期パスワードワークフローを変更したい場合、$WSHOME/sample/wfpwsync.xml ファイルをコピーして変更を行います。その後、変更したワークフローを Identity Manager にインポートします。

デフォルトのワークフローに対して行うことが考えられる変更には、次のようなものがあります。

- パスワードが変更されたときに通知を受けるエントリ
- Identity Manager アカウントが見つからない場合に行う処理
- ワークフロー内でリソースを選択する方法
- Identity Manager からのパスワード変更を許可するかどうか

ワークフローの使用方法の詳細については、『Identity Manager Workflows, Forms, and Views』を参照してください。

通知の設定

Identity Manager には、パスワード同期情報およびパスワード同期失敗通知の電子メールテンプレートが用意されています。これらのテンプレートは、複数のリソースに対するパスワード変更の試みが成功したかどうかをユーザーに知らせます。

さらに補助が必要な場合にユーザーが従うべき手順について、企業ごとに異なる情報を提供するために、どちらのテンプレートも更新することが推奨されます。詳細については、「設定」の章の「電子メールテンプレートについて」を参照してください。

PasswordSync についてのよくある質問

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。

はい、PasswordSync はほかの _WINDOWS_ パスワードフィルタと組み合わせて使用できます。ただし PasswordSync は、レジストリの「Notification Package」エントリの値で列挙されるパスワードフィルタのうち最後のフィルタである必要があります。

次のレジストリパスを使用する必要があります。

`HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Lsa¥Notification Packages`（種類 `REG_MULTI_SZ` の値）

デフォルトでは、インストーラは Identity Manager のパスワードインターセプトをリストの最後に置きますが、インストール後にカスタムのパスワードフィルタをインストールした場合、`lhpwic` を「Notification Packages」リストの最後に移動する必要があります。

PasswordSync はほかの Identity Manager パスワードポリシーと組み合わせて使用できます。Identity Manager サーバーの側でポリシーがチェックされるとき、パスワード同期をほかのリソースにプッシュするために、すべてのリソースのパスワードポリシーが基準を満たす必要があります。結果として、Windows のネイティブパスワードポリシーの制約度を、Identity Manager で定義される最も制約的なパスワードポリシーと同じくらいにすることが推奨されます。

注　パスワードインターセプト DLL はパスワードポリシーを一切施行しません。

PasswordSync サーブレットを、Identity Manager と異なるアプリケーションサーバー上にインストールできますか。

はい。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` の各 JAR ファイルを必要とします。

PasswordSync サービスは lh サーバーにクリアテキストでパスワードを送信しますか。

Sun では PasswordSync を SSL 上で実行することを推奨しますが、すべての重要なデータは Identity Manager サーバーに送信される前に暗号化されます。

パスワード変更の結果、com.waveset.exception.ItemNotLocked が発生することがありますが、それはどうしてですか。

PasswordSync を有効にすると、(ユーザーインタフェースから開始されたものも含めた) パスワード変更の結果としてリソース上でパスワード変更が発生し、それによってリソースが Identity Manager と通信するからです。

thepasswordSyncThreshold 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。

A lh リファレンス

使用法

```
lh { $class | $command } [ $arg [$arg… ] ]
```

注意

- コマンドの使用法についてのヘルプを表示するには、`lh` と入力します (引数は指定しない)。
- `lh` コマンドの使用時には、`JAVA_HOME` を、Java 実行可能ファイルを保存した `bin` ディレクトリが含まれている JRE ディレクトリに設定する必要があります。この場所は、インストールごとに異なります。

  Sun から標準的な (JDK なしの) JRE を取得している場合、通常のディレクトリの場所は `C:¥Program Files¥Java¥j2re1.4.1_01` です。このディレクトリには、Java 実行可能ファイルを保存した `bin` ディレクトリが含まれています。この場合は、`JAVA_HOME` を `C:¥Program Files¥Java¥j2re1.4.1_01` に設定します。

  JDK のフルインストールには複数の Java 実行可能ファイルがあります。この場合は、`JAVA_HOME` を、内蔵の `jre` ディレクトリに設定します。このディレクトリには、正しい `bin/java.exe` ファイルが含まれています。通常のインストールでは、`JAVA_HOME` を `D:¥java¥jdk1.3.1_02.jre` に設定します。

クラス

`com.waveset.session.WavesetConsole` などの完全修飾クラス名でなければなりません。

コマンド

次のコマンドのいずれかでなければなりません。

- `config` ー Business Process Editor を起動します。
- `console` ー Identity Manager コンソールを起動します。
- `js` ー JavaScript プログラムを起動します。
- `license [options] {status | set {parameters }}` ー Identity Manager ライセンスキーを設定します。
- `setRepo` ー Identity Manager インデックスリポジトリを設定します。

- setup ー Identity Manager セットアッププロセスを開始します。これにより、ライセンスキーの設定、Identity Manager インデックスリポジトリの定義、および設定ファイルのインポートができるようになります。
- syslog [options] ー システムログからレコードを抽出します。
- xpress [options] ファイル名 ー 式を評価します。有効なオプションは次のとおりです。
  -trace (トレース出力を有効にする)

例

- lh com.waveset.session.WavesetConsole
- lh console
- lh console -u$user -p$password
- lh setup -U 管理者 -P パスワード
- lh setRepo -c -A 管理者 -C パスワード
- lh setRepo -t ローカルファイル -f$WSHOME

license コマンド

使用法

license [options] { status | set {parameters} }

オプション

-U ユーザー名 (設定者のアカウント名が変更されている場合)

-P パスワード (設定者のパスワードが変更されている場合)

set オプションのパラメータは、「-f ファイル」の形式でなければなりません。

例

- lh license status
- lh license set -f ファイル

syslog コマンド

使用法

```
syslog [options]
```

オプション

-d 日数 ー 指定された直近の日数分のレコードを表示します (デフォルト =1)

-F ー 重要度レベルが「fatal」のレコードのみを表示します

-E ー 重要度レベルが「error」以上のレコードのみを表示します

-W ー 重要度レベルが「warning」以上のレコードのみを表示します (デフォルト)

-X ー エラーの原因がレポートされている場合、出力に含めます

B オンラインマニュアルの高度な検索

Identity Manager のオンラインマニュアルを検索するとき、複雑なクエリーを作成するための高度な構文を使用できます。使用できる構文には次のものがあります。

- ワイルドカード文字 ― 完全な語句の代わりにスペルのパターンを指定できます。
- クエリー演算子 ― クエリー要素がどのように結合または変更されるかを指定します。

注　同じ検索の中でワイルドカード文字とクエリー演算子を併用できます。

ワイルドカード文字

ワイルドカードは、検索においてほかの文字または文字のグループを表す特殊文字です。

Identity Manager のオンラインマニュアルの検索では、次のワイルドカード文字を使用できます。

ワイルドカード文字	説明
疑問符 (?)	任意の 1 文字と一致します。 たとえば、「t?p」を検索すると tap、tip、top などの語と一致します。「ball????」を検索すると ballpark、ballroom、ballyhoo などの語と一致しますが、「ball」に続く文字数が 4 文字ではない ballet や balloon などの語は検索されません。
アスタリスク (*)	任意の文字のグループと一致します。 たとえば、「comp*」を検索すると、computer、company、comptroller など、「comp」で始まるすべての語が検索されます。

クエリー演算子

クエリー演算子を使用して、検索の要素を結合、変更、または除外することができます。クエリー演算子は大文字、小文字、または両者の混合で入力できます。通常、クエリー演算子は <CONTAINS> のように山括弧で囲みます。

注　基本的なブール演算子 (AND、OR、および NOT) と特殊文字演算子 (<、=、!= など) には山括弧は必要ありません。

優先度の規則

1 つのクエリーの中で複数のタイプの演算子を使用するとき、優先度の規則と括弧の使い方によって演算子の有効範囲が決まります。AND 演算子は OR 演算子より優先されます。たとえば、次のようなクエリーがあるとします。

```
resource AND adapter OR attribute
```

これは次のクエリーと同じ働きです。

```
(resource AND adapter) OR attribute
```

「adapter」と「attribute」が、「resource」とともに検索される二者択一の用語として解釈されるようにするには、次のように括弧を使う必要があります。

```
resource AND (adapter OR attribute)
```

デフォルト演算子

演算子を指定せずにクエリー用語またはクエリー要素を連続して入力すると、標準のデフォルト演算子 <AND> を使ってクエリー要素が結合されます。

<EXACT>、<MORPH>、<EXPAND> などの明示的な単項用語演算子が付かない 1 つの単語でクエリーが構成される場合、その単語にはデフォルトの用語演算子 <MORPH> が適用されるとみなされます。

次の表は、オンラインマニュアル検索で最もよく使われるクエリー演算子の一覧です。

演算子	説明	例
<AND> または AND	必須の基準を検索に追加します。	「apples AND oranges」を検索すると、順序を問わず「apples」および「oranges」の両方を含む一致結果が返されます。どちらか 1 つの単語しか含まれないドキュメントは無視されます。
<CASE>	後続の 1 つ以上の用語の一致を、大文字と小文字を区別して検索します。 注意 : Identity Manager では、大文字を含むクエリー用語は自動的に大文字と小文字を区別する検索とみなされるため、<CASE> を付ける必要は必要ありません。すべて小文字の用語は大文字と小文字を区別しない検索として扱われるため、すべて小文字の一致結果だけを得るには <CASE> を使う必要があります。	「<CASE> bill」を検索すると「bill」に一致しますが「Bill」には一致しません。
<EXACT>	指定された単語と完全に一致する単語を含むドキュメントを検索します。	「<EXACT> soft」を検索すると、単語「soft」を含むドキュメントが検索されますが、「softest」や「softer」を含むドキュメントは検索されません。
<MORPH>	指定された単語に加えて、その単語が形態変化した単語を含むドキュメントも検索します。これには複数形や過去形に加えて、接頭辞、接尾辞、複合語を含む複合形が含まれます。不規則な形式を正しく扱うために、語彙データベースの情報も利用します。	「<MORPH> surf」を検索すると、「surfs」、「surfed」、「surfing」のような単語「surf」の単純な変化形に加えて、接頭辞付き (「resurf」) や複合語 (「surfboard」) などの変化形も対象としてドキュメントを検索します。

演算子	説明	例
<NEAR>	指定された単語どうしが 1000 語以内の近さにあるドキュメントを検索します。単語どうしが近いドキュメントほど検索結果の上位に表示されます。	「resource <NEAR> configuration」を検索すると、両方の単語を含み、単語間の距離が 1000 語以内であるドキュメントが検索されます。
<NEAR/n>	指定された単語間の距離が n 語以下であるドキュメントを検索します。 注意 : ***n*** の値は 1 〜 1024 の範囲で指定する必要があります。	「buy <NEAR/3> sell」を検索すると、「buy」と「sell」の間が 3 語以下である「buy low and sell high」のような表現を含むドキュメントが検索されます。
<NOT> または NOT	特定の単語または語句を含まないドキュメントを検索します。	「surf <AND> <NOT> channel」を検索すると、「surf」を含み「channel」を含まないドキュメントが検索されます。

索引

A

Account Administrator の機能 5-37
Active Sync ウィザード、起動 6-12
ActiveSync アダプタ
  LDAP 設定 6-16
  一般設定 6-16
  イベントタイプ 6-18
  開始 6-23
  概要 6-12
  共通の設定 6-17
  クラスタ環境 6-22
  スタートアップ設定 6-14
  セットアップ 6-12
  ターゲット属性マッピング 6-21
  ターゲットリソース 6-20
  停止 6-23
  同期モード 6-12
  パフォーマンスのチューニング 6-22
  プロセスの選択 6-19
  編集 6-21
  ポーリング間隔の変更 6-22
  ポーリング設定 6-14
  ホストの指定 6-22
  ログ 6-23
  ログ設定 6-15
ActiveSync のターゲット属性マッピング 6-21
ActiveSync のターゲットリソース 6-20
ActiveSync のプロセスの選択 6-19
Admin Report Administrator の機能 5-37
Admin Role Administrator の機能 5-37
allowInvalidCerts 10-10
Approver の機能 5-37
Assign User Capabilities の機能 5-37
Audit Report Administrator の機能 5-37

B

BPE、「Business Process Editor (BPE)」を参照
Business Process Editor (BPE) 1-10, 2-3, A-1

C

Capability Administrator の機能 5-39
ChangeLog
  CSV ファイル形式 5-23
  作成と編集 5-20
  スクリプトの作成 5-26
  セキュリティー 5-14
  設定 5-18
  説明 5-14
  ポリシーの作成 5-19
  要件 5-15
clientConnectionFlags 10-10
clientSecurityFlags 10-10
Configure Audit 機能 5-40
Control Active Sync Resource Administrator 機能 5-40
convertDateToString 9-30, 9-31
Create User 機能 5-40
CreateOrUpdate コマンド 3-30
createUser 9-2, 9-3
Create コマンド 3-30
CSV 形式 3-29, 6-3
  抽出 6-2

D

DeleteAndUnlink コマンド 3-30
deleteUser 9-3
Delete コマンド 3-30
Deprovision User 機能 5-41
Disable User 機能 5-41
Disable コマンド 3-30

E

Enable User 機能 5-41
Enable コマンド 3-30

F

FormUtil メソッド 9-30, 9-31

I

Identity Manager
  アカウントインデックス 6-10
  インタフェース
    Business Process Editor (BPE) 2-3
    管理者 2-1
    ユーザー 2-2
  オブジェクト 1-4, 1-8
  概要 1-1
  管理 4-1
  管理者ロール 1-7
  機能 1-7, 5-31
  サーバーの設定 5-59
  セキュリティー 7-1
  設定 5-1

組織 1-7, 4-2
タスク 2-8
データの同期 6-1
ヘルプとガイダンス 2-4
ポリシー 5-27
目的 1-1
ユーザーアカウント 1-4
削除 9-6
用語 1-10
リソース 1-5, 5-4, 5-6
リソースグループ 1-5, 5-13
レポート 8-1
ロール 1-4, 5-1
「Identity Manager アカウントの削除」ボタン 9-6
Identity System 属性名 5-13
ID 属性
設定 5-15
ID テンプレート 1-10, 5-10
ID、ユーザーアカウント 3-1
Import User 機能 5-41
Import/Export Administrator 機能 5-41
installdir 10-11

J

JMS 設定、PasswordSync 10-5
JMS リスナーアダプタ、PasswordSync 用に設定 10-11

L

LDAP
Active Sync 設定 6-16
サーバー 4-6
リソースクエリー 9-10, 9-17
lh コマンド
license A-2
syslog A-3
クラス A-1
コマンド引数 A-1
使用法 A-1
リファレンス A-1
License Administrator 機能 5-41
license コマンド A-2
Login Administrator 機能 5-41

M

ManageResource ワークフロー 5-5
Microsoft .NET 1.1 10-2
Microsoft .NET 1.1 のインストール 10-2

O

Organization Administrator 機能 5-41

P

Password Administrator 機能 5-41
PasswordSync
JMS 設定 10-5
JMS リスナーアダプタ、設定 10-11
アンインストール 10-11
以前のバージョンのアンインストール 10-2
インストール 10-3
インストールの前提条件 10-1
概要 10-1
サーバー設定 10-4
設定 10-3, 10-4
通知の設定 10-13
デバッグ 10-9
電子メール設定 10-7
トレースログ 10-9
プロキシサーバー設定 10-5
ユーザーパスワード同期ワークフロー 10-12
よくある質問 10-13
レジストリキー 10-10
配備 10-11
PasswordSync のアンインストール 10-11
PasswordSync の以前のバージョンのアンインストール 10-2
PasswordSync のインストール
前提条件 10-1
手順 10-3
PasswordSync のデバッグ 10-9
PasswordSync の配備 10-11
Policy Administrator 機能 5-42

R

Reconcile Administrator 機能 5-42
Reconcile Report Administrator 機能 5-42
Reconcile Request Administrator 機能 5-42
Remedy Integration Administrator 機能 5-42
Remedy との統合 5-59
Rename User 機能 5-42
Report Administrator 機能 5-42
Reset Password Administrator 機能 5-42
Reset Resource Password Administrator 機能 5-43
Resource Administrator 機能 5-43
Resource Group Administrator 機能 5-43
Resource Object Administrator 機能 5-43
Resource Password Administrator 機能 5-43
Resource Report Administrator 機能 5-44
Risk Analysis Administrator 機能 5-44

Role Administrator 機能 5-44
Role Report Administrator 機能 5-44

S

Security Administrator 機能 5-44
soapClientTimeout 10-11
SSL 接続、テスト 7-10
syslog コマンド A-3

T

Task Report Administrator 機能 5-44

U

Unassign User 機能 5-45
Unassign コマンド 3-30
Unlink User 機能 5-45
Unlink コマンド 3-30
Unlock User 機能 5-45
Update User 機能 5-45
updateUser 9-3
Update コマンド 3-30
User Account Administrator 機能 5-45
User Report Administrator 機能 5-46
user.global.email 属性 9-22
user.waveset.accountId 属性 9-22
user.waveset.organization 属性 9-22
user.waveset.resources 属性 9-23
user.waveset.roles 属性 9-22

V

View User 機能 5-46

W

Waveset Administrator 機能 5-46
waveset.accountId 属性 9-30
Windows Active Directory リソース 4-6

X

X509 証明書 subjectDN を使用した相関 7-9
X509 証明書ベースの認証 7-7
XML ファイル
  承認フォーム 9-23, 9-24
  抽出 6-2
  読み込み 6-3

あ

アイデンティティーシステムのパラメータ、リソース 5-10
アカウント ID
  承認のエスカレーション用 9-20
  承認用 9-14
  追加の承認者 9-15
  通知の受信者 9-9
アカウントインデックス
  検査 6-11
  検索 6-10
  操作 6-10
「アカウント」エリア、管理者インタフェース 3-5
アカウント属性 5-9, 5-12
アプリケーション、アクセスの無効化 7-4
暗号化
  暗号化キー 7-12
  概要
  保護されるデータ 7-11
暗号化キー、サーバー 7-12

い

一括機能
  Bulk Account Administrator 5-37
  Bulk Change Account Administrator 5-37
  Bulk Change User Account Administrator 5-38
  Bulk Create User 5-38
  Bulk Delete IDM User 5-38
  Bulk Deprovision User 5-38
  Bulk Disable User 5-38
  Bulk Enable User 5-38
  Bulk Unassign User 5-38
  Bulk Unlink User 5-39
  Bulk Update User 5-39
  Bulk User Account Administrator 5-39
一括操作
  確認規則 3-32, 3-33
  相関規則 3-32, 3-33
  操作リスト 3-29
  タイプ 3-28
  表示属性 3-32
  ユーザーアカウント 3-28
「一般」タブ
  設定 9-5–9-8
  説明 9-4
委任された管理 4-1
イベントタイプ 6-18

え

エスカレーションされた承認
  承認者 9-20
  タイムアウト 9-15, 9-16, 9-17, 9-19

お

オブジェクト、Identity Manager 1-4, 1-8
親組織 1-7
オンラインヘルプ 2-4
　高度な検索 B-1
オンラインマニュアル検索のワイルドカード B-1

か

ガイダンス、Identity Manager 2-4, 2-7
確認規則 3-32, 3-33
カスタムリソース 5-6
仮想組織
　概要 1-7, 4-6
　更新 4-8
　削除 4-8
監査
　設定 9-25–9-26
監査、設定 9-4
監査設定グループ 5-58
「監査」タブ
　設定 9-25–9-26
　説明 9-25
カンマ区切り値 (CSV) 形式、「CSV 形式」を参照
管理、Identity Manager 4-1
管理、委任 4-1
管理者
　作成 4-8
　定義 1-10
　名前の表示のカスタマイズ 4-13
　認証質問 4-13
　パスワード 4-11
　ビューのフィルタ 4-10
管理者インタフェース 1-10, 2-1
　「アカウント」エリア 3-5
管理者リスト
　承認者の選択 9-14, 9-18, 9-21
　通知の受信者の選択 9-9, 9-11
管理者ロール
　概要 1-7, 5-46
　作成と編集 5-48
　定義 1-10
　ユーザーの割り当て 3-2
　ユーザーフォームの割り当て 5-50
管理する組織
　規則 5-51, 5-53
　範囲の設定 5-49
　ユーザーの割り当て 3-3, 4-9
管理する組織の範囲の設定 5-49
「管理するリソース」ページ 5-6

き

キー
　ゲートウェイ 7-14
　サーバー暗号化 7-12
規則
　現在設定されている 9-33
　定義 1-11
　データ変換用 9-33
　評価によりアカウント ID を取得 9-9, 9-10, 9-14, 9-16, 9-20
　プロビジョニング解除用 9-32
　プロビジョニング用 9-29, 9-31
　ユーザーメンバーの例 4-5
規則に基づく割り当て 4-3
機能
　階層 5-33
　概要 1-7, 5-31
　カテゴリ 5-32
　規則 5-51
　作成 5-32
　定義 1-10
　定義の表 5-36
　名前の変更 5-32
　編集 5-32
　ユーザーの割り当て 3-3, 4-9
　割り当て 5-33
共通リソース、認証の設定 7-6

く

クエリー
　LDAP リソース 9-10, 9-17
　承認者のアカウント ID の取得 9-14, 9-17, 9-21
　属性の比較 9-11, 9-17
　通知の受信者のアカウント ID の取得 9-9, 9-10
　ヘルプとマニュアル 2-5, B-1
　リソース属性 9-11, 9-17
クラスタ環境での ActiveSync 6-22

け

ゲートウェイキー 7-14
検索
　ヘルプとマニュアル 2-4, B-1
　ユーザーアカウント 3-6

こ

コマンドリファレンス、lh コマンド A-1

さ

サーバー暗号化

管理 7-11, 7-17
キー 7-12
サーバー暗号化の管理 7-17
サーバーのデフォルト設定 5-60
再試行リンク、設定 9-27
削除
削除タスクの保留 9-5
ユーザーアカウント 3-15, 9-4, 9-6
作成タスク、保留 9-5
サンセット
設定 9-28
プロビジョニング解除 9-31
サンライズ
新しいユーザーのプロビジョニング 9-28
設定 9-28
「サンライズとサンセット」タブ
設定 9-28–9-32
説明 9-5

し

自己検索 3-24
辞書ポリシー
概要 5-30
実装 5-31
設定 5-30
選択 3-20
実行機能
Run Admin Report 5-44
Run Audit Report 5-44
Run Reconcile Report 5-44
Run Resource Report 5-44
Run Risk Analysis 5-44
Run Role Report 5-44
Run Task Report 5-44
Run User Report 5-44
実用上の機能 5-32
指定
アカウントデータの属性 9-4
通知の受信者 9-9, 9-10, 9-11
ユーザー通知 9-11
承認
エスカレーションされた 9-15, 9-16, 9-17, 9-19, 9-20
カテゴリ 4-14
設定 9-12–9-25
フォーム 9-22
無効化 9-4
有効化 9-4, 9-13
承認者
設定 9-12
セットアップ 4-14
組織 9-13
追加 9-4, 9-12, 9-14–9-22
通知の設定 9-8
定義 1-10
リソース 9-13
ロール 9-13
「承認」タブ
概要 9-4
設定 9-12–9-24
説明 9-4, 9-12
「承認のエスカレーション」ボタン 9-20
承認の無効化 9-4, 9-13
証明書ベースの認証 7-7
署名付き承認、設定 5-61

す

スキーマ 1-12
スキーママップ 1-12, 5-12
スケジューラの設定 5-60
ステータスインディケータ、ユーザーアカウント 3-6

せ

制約規則、ログイン 7-3
セキュリティー
概要 7-1
機能 7-1
パススルー認証 7-2
パスワード管理 7-1
ベストプラクティス 7-19
ユーザーアカウント 3-2
セッション制限、設定 7-4
設定
Identity Manager サーバーの設定 5-59
PasswordSync 10-3, 10-4
「一般」タブ 9-5, 9-8
監査 9-4, 9-25, 9-26
「監査」タブ 9-25, 9-26
「サンライズとサンセット」タブ 9-28, 9-32
承認 9-12, 9-25
承認フォーム 9-22
署名付き承認 5-61
タイムアウト 9-19, 9-20, 9-22
タスクテンプレート 9-4
追加の承認者 9-4
通知 9-8, 9-12
電子メール通知 9-4
「プロビジョニング」タブ 9-27
ユーザー更新テンプレート 9-5
ユーザー作成テンプレート 9-5

設定エディタ、「Business Process Editor (BPE)」を参照
「選択している属性の削除」ボタン 9-23, 9-24, 9-26

そ

相関規則 3-32, 3-33
属性
  user.global.email 9-22
  user.waveset.accountId 9-22
  user.waveset.organization 9-22
  user.waveset.resources 9-23
  user.waveset.roles 9-22
  waveset.accountId 9-30
  アカウント ID の取得 9-9, 9-14, 9-15, 9-20
  アカウントデータから指定 9-4
  値の編集 9-23, 9-24
  クエリーの作成 9-11
  承認フォームからの削除 9-23
  承認フォームへの追加 9-23, 9-24
  タスク承認のための指定 9-12
  タスク名での指定 9-6
  デフォルト 9-22, 9-23
  デフォルトの表示名 9-24
  ユーザーアカウント 3-4
「属性の追加」ボタン 9-23, 9-24, 9-25
組織
  概要 1-7, 4-2
  仮想 1-7, 4-6
  管理割り当て 4-6
  作成 4-2
  定義 1-10
  ユーザーの割り当て 4-3
組織の承認 9-13

た

タイムアウト
  エスカレーションされた承認 9-15, 9-16, 9-17, 9-19
  設定 9-19, 9-20, 9-22
タイムアウト値、設定 7-4
「タイムアウトのアクション」ボタン 9-19
タスク
  クイックリファレンス 2-8
  再試行 9-5
  サンライズ / サンセット 9-5
  バックグラウンドでの実行 9-5
  保留 9-5
タスクテンプレート
  概要 9-1
  設定 9-4
  プロセスタイプのマッピング 9-1
  編集 9-4
  有効化 9-1, 9-3
  ユーザー更新テンプレート 9-1
  ユーザー削除テンプレート 9-1
  ユーザー作成テンプレート 9-1
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 9-4, 9-5
  ユーザー削除テンプレート 9-4, 9-6
  ユーザー作成テンプレート 9-4, 9-5
タスクの再試行 9-5
「タスクの実行」ボタン 9-22
「タスクの設定」タブ 9-4
タスクの保留 9-5
タスクベースの機能 5-32
タスク名
  属性参照 9-6
  定義 9-4, 9-6
タブ
  一般 9-4
  サンライズとサンセット 9-5
  承認 9-4
  タスクの設定 9-4
  通知 9-4
  データ変換 9-5
  プロビジョニング 9-5
探索
  概要 6-2
  ファイルから読み込み 6-3
  ファイルへ抽出 6-2
  リソースから読み込み 6-5

ち

調整
  開始 6-9
  概要 6-6
  ステータスの表示 6-10
  ポリシー 6-6
    編集 6-7
調整サーバーの設定 5-59

つ

通知
  PasswordSync での設定 10-13
  設定 9-8–9-12
  ユーザーアカウントデータの変換 9-33
「通知」タブ
  設定 9-8–9-12
  説明 9-4
通知の受信者

アカウント ID の取得 9-9
管理者リストからの指定 9-11
規則による指定 9-10
クエリーによる指定 9-10
属性による指定 9-9
ユーザーの指定 9-11

て

ディレクトリジャンクション
概要 4-6
セットアップ 4-7
ディレクトリリソース 4-6
データの同期
ActiveSync アダプタ 6-12
概要 6-1
探索 6-2
調整 6-6
ツール 6-1
データの読み込み 6-1
データ変換
プロビジョニング中 9-32
プロビジョニング前 9-5
「データ変換」タブ
設定 9-32
説明 9-5
デフォルト
承認の有効化 9-13
承認フォームの属性 9-22, 9-23
属性の表示名 9-24
タスク名 9-6
プロセスタイプ 9-2
電子メール設定、PasswordSync 10-7
電子メール通知、設定 9-4, 9-8
電子メールテンプレート 9-9, 9-11
HTML とリンク 5-57
概要 5-55, 9-8
カスタマイズ 5-56
変数 5-57
テンプレート、タスク、「タスクテンプレート」を参照
テンプレート、電子メール 9-8, 9-9, 9-11

と

同期、データの「データの同期」を参照
同期モード 6-12
トリプル DES 暗号化 7-12, 7-14
トレースログ、PasswordSync 10-9

に

認証
X509 証明書ベース 7-7
共通リソースの設定 7-6
質問 4-13
ユーザー 3-25

は

パススルー認証 7-2
パスワード
管理者の認証 4-12
管理者の変更 4-11
ユーザーアカウント、「ユーザーアカウントパスワード」を参照
ログインアプリケーション 7-2
パスワード管理 7-1
パスワードポリシー
辞書ポリシー 3-20
実装 3-21
使用禁止属性 3-20
使用禁止単語 3-20
設定 3-18
長さ規則 3-19
文字タイプ規則 3-19
履歴 3-20
バックグラウンド、タスクの実行 9-5
バックグラウンドでのタスク実行 9-5

ひ

日付形式文字列 9-30, 9-31, 9-32
「必須のプロセスマッピング」セクション 9-2

ふ

ファイルから読み込み 6-1, 6-3
ファイルへ抽出 6-1, 6-2
フィールドレベルのヘルプ 2-7
フォーム
現在設定されている 9-18, 9-33
承認の設定 9-22
属性の追加 9-24
タスクの承認 9-12
通知 9-10
定義 1-10
編集 2-3
「フォームおよびプロセスマッピングの設定」ページ 9-3
プロキシサーバー設定、PasswordSync 10-5
プロセスタイプ
createUser 9-2
updateUser 9-3
削除 9-2
選択 9-2

デフォルト 9-2
マッピング 9-1, 9-2, 9-3
プロセスマッピング
一覧表示 9-2
検証 9-3
必須 9-2
編集 9-2
有効化 9-2
プロセスマッピングの一覧表示 9-2
プロセスマッピングの検証 9-3
プロセスマッピングの編集ページ 9-2
プロビジョニング
再試行リンク 9-27
サンライズ 9-28
サンライズの設定 9-28
時刻 9-29
事前のデータ変換 9-5
データ変換 9-32
バックグラウンドで 9-27
日付 9-29
プロビジョニング解除
サンセットの設定 9-31
ユーザーアカウント 3-15, 9-4, 9-6, 9-7
「プロビジョニング」タブ
設定 9-27
説明 9-5

へ

ページ
タスクテンプレート「Create User Template」の編集 : 9-4, 9-5
タスクテンプレート「Delete User Template」の編集 : 9-4, 9-6
タスクテンプレート「Update User Template」の編集 : 9-4, 9-5
フォームおよびプロセスマッピングの設定 9-3
プロセスマッピングの編集 9-2
ヘルプ、オンライン 2-4
検索 B-1
変更機能
Change Account Administrator 5-39
Change Active Sync Resource Administrator 5-39
Change Password Administrator 5-39
Change Resource Password Administrator 5-40
Change User Account Administrator 5-40
編集
属性値 9-23, 9-24
タスクテンプレート 9-4
タスク名 9-6
プロセスマッピング 9-2

ほ

方法
管理者への通知 9-8
サンライズ / サンセットの決定 9-28
承認者の決定 9-14
承認のタイムアウトの決定 9-15
プロビジョニング解除の決定 9-31
ボタン
Identity Manager アカウントの削除 9-6
承認のエスカレーション 9-20
選択している属性の削除 9-23, 9-24, 9-26
属性の追加 9-23, 9-24, 9-25
タイムアウトのアクション 9-19
タスクの実行 9-22
マッピングの編集 9-2
有効化 9-2
ポリシー
Identity Manager アカウント 5-27
アカウント ID 5-29
概要 5-27
辞書 5-30
調整 6-6
定義 1-11
リソースパスワード 3-18, 5-29

ま

マッピング
検証 9-3
プロセス 9-3
プロセスタイプ 9-1, 9-3
「マッピングの編集」ボタン 9-2
マニュアル、Identity Manager 2-4
検索 B-1

め

メソッド
FormUtil 9-30, 9-31

ゆ

有効化
承認 9-4, 9-13
承認のタイムアウト 9-19
タスクテンプレート 9-3
プロセスマッピング 9-2
「有効化」ボタン 9-2
ユーザー 1-12
ユーザーアカウント
ID 3-1
一括操作 3-28
移動 3-9

概要 1-4
管理 3-1
検索 3-6, 3-17
更新 3-12
削除 3-15, 9-4, 9-6
作成 3-7
自己検索 3-24
ステータスインディケータ 3-6
セキュリティー 3-2
属性 3-4
定義 1-12
データ 3-1
データ変換 9-32
名前の変更 3-10
認証 3-25
パスワード
操作 3-22
変更 3-22
リセット 3-23
表示 3-7
プロビジョニング解除 3-15, 9-4, 9-6
編集 3-9
無効化 3-11
有効化 3-12
ロック解除 3-14
割り当て 3-2
ユーザーアカウントの移動 3-9
ユーザーアカウントの検索 3-17
ユーザーアカウントの更新 3-12
ユーザーアカウントの名前の変更 3-10
ユーザーアカウントの無効化 3-11
ユーザーアカウントの有効化 3-12
ユーザーアカウントのロック解除 3-14
ユーザーアカウントパスワードのリセット 3-23
ユーザーアクセス、定義 1-2
ユーザーインタフェース、Identity Manager 1-12, 2-2
ユーザー更新テンプレート
設定 9-5
説明 9-1
マッピングプロセス 9-3
ユーザー削除テンプレート
説明 9-1
マッピングプロセス 9-3
ユーザー作成テンプレート
設定 9-5
説明 9-1
マッピングプロセス 9-3
ユーザーテンプレート
選択 9-4
編集 9-5, 9-6
ユーザーの削除機能 5-40
「ユーザーの作成」ページ 3-7
ユーザーパスワード同期ワークフロー 10-12
ユーザーフォーム 3-7, 4-9
管理者ロールへの割り当て 5-50
「ユーザーメンバー規則」オプションボックス 4-4
ユーザーメンバー規則の例 4-5

よ

用語、Identity Manager 1-10
用語集 1-10

り

リスク分析 8-9
リソース 1-5
Identity Manager 5-6
ID テンプレート 5-10
アイデンティティーシステムのパラメータ 5-10
アカウント属性 5-9, 5-12, 9-11
アダプタ 5-7
概要 5-4
カスタム 5-6
管理 5-12
作成 5-7
定義 1-11
問い合わせ 9-14, 9-17, 9-21
パラメータ 5-8
リスト 5-5
リソースアカウント
Identity Manager アカウントの削除 9-7
プロビジョニング解除 9-7
リンク解除 9-7
割り当て解除 3-16, 9-7
リソースアカウントのリンク解除 3-16, 9-7
リソースアカウントの割り当て解除 3-16, 9-7
リソースアダプタ 1-11
リソースアダプタアカウント 1-11
リソースウィザード 1-11, 5-7
「リソース」エリア 5-4
リソースから読み込み 6-1, 6-5
リソースグループ 1-5, 5-13
定義 1-11
リソース属性 9-17
リソースの承認 9-13
リソースの調整 6-1

れ

レジストリキー、PasswordSync 10-10
レポート 8-1
概要 8-6

監査ログ 8-5
システムログ 8-8
実行 8-3
使用状況 8-8
スケジュール 8-3
操作 8-1
定義 8-2
データのダウンロード 8-4
名前の変更 8-3
リアルタイム 8-5
リスク分析 8-9

ろ

ロール
Identity Manager ロールとリソースロールの同期 5-4
概要 1-4, 5-1
管理者 1-7
クローン作成 5-3
検索 5-2
作成 5-2
承認 9-13
定義 1-11
名前の変更 5-3
編集 5-2
割り当てられているリソース属性値を編集する 5-2
ログイン
アプリケーション 7-2
編集 7-3
制約規則 7-3
相関規則 7-9
モジュール
編集 7-4
モジュールグループ 7-2
編集 7-4
ログインアプリケーション、アクセスの無効化 7-4

わ

ワークフロー 1-12, 2-3
割り当て、ユーザーアカウント 3-2