IBM Security Identity Manager
バージョン 6.0

構成ガイド

SA88-4862-00
(英文原典：SC14-7696-00)

IBM Security Identity Manager
バージョン 6.0

構成ガイド

SA88-4862-00
(英文原典：SC14-7696-00)

お願い

本書および本書で紹介する製品をご使用になる前に、 285 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM Security Identity Manager バージョン 6.0 (製品番号 5724-C34)、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： SC14-7696-00
IBM Security Identity Manager
Version 6.0
Configuration Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

テーブル・リスト

本書について

「*IBM Security Identity Manager 構成ガイド*」には、IBM Security Identity Manager の最初の構成とカスタマイズに関する情報が掲載されています。この製品は、必要なセットアップが最小限で済むように設計されており、必要なときにはいつでも、自分で決定してデフォルト設定を変更できます。

資料および用語集へのアクセス

このセクションでは、以下について述べます。

- IBM Security Identity Manager ライブラリーに含まれる資料のリスト。
- 『オンライン資料』へのリンク。
- x ページの『IBM Terminology Web サイト』へのリンク。

IBM Security Identity Manager ライブラリー

IBM Security Identity Manager ライブラリーには以下の文書があります。

- 「*IBM Security Identity Manager Quick Start Guide*」(CF3L2ML)
- *IBM Security Identity Manager 製品概要*、GA88-4857-00
- *IBM Security Identity Manager シナリオ*、SA88-4858-00
- *IBM Security Identity Manager 計画*、GA88-4859-00
- *IBM Security Identity Manager インストール・ガイド*、GA88-4860-00
- *IBM Security Identity Manager 構成ガイド*、SA88-4862-00
- 「*IBM Security Identity Manager Security Guide*」(SC14-7699)
- *IBM Security Identity Manager 管理ガイド*、SA88-4863-00
- *IBM Security Identity Manager トラブルシューティング・ガイド*、GA88-4864-00
- *IBM Security Identity Manager メッセージ・リファレンス*、GA88-4865-00
- *IBM Security Identity Manager リファレンス・ガイド*、SA88-4866-00
- *IBM Security Identity Manager Database and Directory Server Schema リファレンス・ガイド*、SA88-4867-00
- 「*IBM Security Identity Manager Glossary*」(SC14-7397)

オンライン資料

IBM では、製品のリリース時および資料の更新時に、以下の場所に製品資料を掲載しています。

IBM Security Identity Manager インフォメーション・センター

このサイト (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm)には、この製品の「インフォメーション・センターへようこそ」ページが表示されます。

IBM Security インフォメーション・センター

このサイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp) には、すべての IBM Security 製品資料のアルファベット順のリストと、一般情報が掲載されています。

IBM Publications Center

このサイト (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) には、必要なすべての IBM 資料を見つけるのに役立つカスタマイズ検索機能が用意されています。

IBM Terminology Web サイト

IBM Terminology Web サイトは、製品ライブラリーの用語を 1 つのロケーションに統合したものです。Terminology Web サイトには、http://www.ibm.com/software/globalization/terminology からアクセスできます。

アクセシビリティー

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。この製品では、インターフェースを音声出力してナビゲートする支援技術を利用できます。マウスの代わりにキーボードを使用して、グラフィカル・ユーザー・インターフェースのすべての機能を操作することもできます。

詳しくは、「*IBM Security Identity Manager Reference Guide*」のトピック『IBM Security Identity Manager のアクセシビリティー機能』を参照してください。

技術研修

以下は英語のみの対応となります。技術研修の情報については、IBM Education Web サイト (http://www.ibm.com/software/tivoli/education) を参照してください。

サポート情報

IBM サポートは、コード関連の問題、およびインストールまたは使用方法に関する短時間の定型質問に対する支援を提供します。IBM ソフトウェア・サポート・サイトには、http://www.ibm.com/software/support/probsub.html から直接アクセスできます。

「*IBM Security Identity Manager トラブルシューティング・ガイド*」には、以下について詳しく説明されています。

- IBM サポートに連絡する前に収集する情報。
- IBM サポートへのさまざまな連絡方法。
- IBM サポート・アシスタントの利用方法。
- 自分で問題を特定して修正するための指示および問題判別のリソース。

注: 製品のインフォメーション・センターの「**コミュニティーおよびサポート**」タブには、追加のサポート・リソースが掲載されています。

第 1 章 ユーザー・インターフェースのカスタマイズの概要

多くのお客様が要望するのは、従業員が IBM® Security Identity Managerと対話して基本的な管理機能やプロビジョニング機能を実行できるようにする、単純なユーザー・インターフェースです。IBM Security Identity Managerは、カスタマイズ可能で、ユーザーとアドミニストレーターの両方が必要とする基本的な IBM Security Identity Managerの機能を提供する、デュアル・ユーザー・インターフェースです。

IBM Security Identity Managerに用意されているインターフェースのカスタマイズ・オプションにより、お客様は、従業員に対する IBM Security Identity Managerの機能の提供方法を制御して柔軟に管理できます。これらのオプションを使用して、セルフ・サービス・ユーザー・インターフェースおよび管理コンソール・インターフェースを会社のイントラネット Web サイトに統合し、一貫した外観を維持することができます。

セルフサービス・ユーザー・インターフェースのカスタマイズ

このセクションでは、セルフサービス・ユーザー・インターフェースをカスタマイズする方法について説明します。

IBM Security Identity Managerセルフ・サービス・ユーザー・インターフェースはカスタマイズ性に優れています。お客様は、自分の役割と責任にとって不可欠なセルフケア識別管理タスクを行う柔軟性を保ちながら、会社のユーザー・インターフェースを共通の外観で統一できます。

セルフサービス・インターフェースは、組み込みコンソール・フレームワークを使用する方法と、IBM Security Identity Managerにインストールされているファイルを直接変更する方法の 2 とおりの方法で、定義およびカスタマイズすることができます。

- 組み込みコンソール機能は、以下の通りです。
  - アクセス・コントロール項目 (ACI)
  - ビュー
- 変更可能なファイルは、以下のとおりです。
  - プロパティー・ファイル
  - カスケーディング・スタイル・シート (CSS) ファイル
  - Java™Server Page (JSP) ファイルのサブセット
  - イメージ・ファイル

IBM Security Identity Managerに対してカスタマイズ変更を行う前に、リカバリー用に変更可能ファイルをバックアップします。

構成ファイルと説明

構成ファイルを使用して、IBM Security Identity Manager セルフ・サービス・ユーザー・インターフェースの外観を定義します。

以下のテーブルに、ファイル名および IBM Security Identity Manager のカスタマイズにおけるそれらの役割をリストします。

表 1. プロパティー構成ファイルと説明

ファイル名	ファイルの説明
SelfServiceUI.properties	• ユーザー・インターフェースのレイアウト (バナー、フッター、ナビゲーション・バー、ツールバー)、表示するページ数、および戻す検索結果数を制御します。 • セルフ・サービス・インターフェースでのユーザー検索のために、「検索基準」ボックスで選択可能な項目を構成できます。 • 「有効期限切れのパスワード」変更画面に直接アクセスできるようにし、一定の条件下でセルフ・サービス・ログイン・ページを迂回します。これらのアクションを可能にするプロパティー・キーは、ui.directExpiredChangePasswordEnabled です。
SelfServiceScreenText.properties	セルフ・サービス・ユーザー・インターフェースにテキストを提供します。
SelfServiceScreenText_*language*.properties	セルフ・サービス・ユーザー・インターフェースに言語固有のテキストを提供します。このファイルは、デフォルトでは、SelfServiceScreenText_en.properties であり、英語バンドルを含んでいます。
SelfServiceHomePage.properties	セルフ・サービス・ユーザー・インターフェースのホーム・ページのセクションとそれらの表示順序を定義します。
SelfServiceHelp.properties	セルフ・サービス・ユーザー・インターフェースに HTML ヘルプ・ページへのリンクを定義します。HTML ファイルは、*WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service_help.war ディレクトリーにあります。このファイル内の情報を変更することにより、ヘルプをリダイレクトできます。

表 1. プロパティー構成ファイルと説明 (続き)

ファイル名	ファイルの説明
SelfServiceScreenTextKeys .properties	セルフ・サービス・ユーザー・インターフェースにラベル・キーを提供します。このファイルは、ラベルおよび説明を作成するテンプレートを指定することによって、画面テキストをカスタマイズするときに補助的に利用できます。 このファイルは、キー名として設定されるラベルを格納します。例えば、password_title=password_title などです。このファイルをコピーして、SelfServiceScreenText_*language*.properties という名前を付け、カスタマイズおよび開発に使用できます。ここで *language* は、インストールしなかった言語サフィックスです。次に、ブラウザーのロケールを現行の言語からその未使用の言語に切り替えることができます。Web アプリケーションを再始動してページ間をナビゲートし、値テキストではなくラベル・キーを確認します。ブラウザーのロケールを切り替えることによって、キーと値を切り替えることができます。カスタマイズが完了した後で、ファイルをコピーし、使用したい言語サフィックス、例えば SelfServiceScreenText_en.properties に名前変更することによって、変更は完了です。

表 2. Java Server Pages (JSP) の構成ファイルと説明

ファイル名	ファイルの説明
loginBanner.jsp	セルフ・サービス・ログイン・ページのバナーのコンテンツを格納します。
loginFooter.jsp	セルフ・サービス・ログイン・ページのフッターのコンテンツを格納します。
loginToolbar.jsp	セルフ・サービス・ログイン・ページのツールバーのコンテンツを格納します。
Home.jsp	セルフ・サービス・ホーム・ページのコンテンツを格納します。
banner.jsp	セルフ・サービス・バナーのコンテンツを格納します。
footer.jsp	セルフ・サービス・フッターのコンテンツを格納します。
nav.jsp	セルフ・サービス・ナビゲーション・バーのコンテンツを格納します。
toolbar.jsp	セルフ・サービス・ツールバーのコンテンツを格納します。

表 3. カスケーディング・スタイル・シート (CSS) の構成ファイルと説明

ファイル名	ファイルの説明
calendar.css	カレンダー・ウィジェットに使用するスタイルを格納した CSS ファイルです。

表 3. カスケーディング・スタイル・シート (CSS) の構成ファイルと説明 (続き)

ファイル名	ファイルの説明
customForm.css	左から右方向の言語でのカスタム・フォームのレイアウトに使用するスタイルを格納した CSS ファイルです。
customForm_rtl.css	右から左方向の言語でのカスタム・フォームのレイアウトに使用するスタイルを格納した CSS ファイルです。
dateWidget_ltr.css	左から右方向の言語での日付ウィジェットに使用するスタイルを格納した CSS ファイルです。
dateWidget_rtl.css	右から左方向の言語での日付ウィジェットに使用するスタイルを格納した CSS ファイルです。
enduser.css	左から右方向の言語でのメイン CSS スタイルを格納した CSS ファイルです。
enduser_rtl.css	右から左方向の言語でのメイン CSS スタイルを格納した CSS ファイルです。
time.css	時刻ウィジェットに使用するスタイルを格納した CSS ファイルです。
widgets.css	左から右方向の言語で上記以外のウィジェットに使用するスタイルを格納した CSS ファイルです。
widgets_rtl.css	右から左方向の言語で上記以外のウィジェットに使用するスタイルを格納した CSS ファイルです。

セルフ・サービス・ユーザー・インターフェース構成ファイルのバックアップとリストア

セルフ・サービス・ユーザー・インターフェースのカスタマイズを開始する前に、後のリカバリー処理に備えて、IBM Security Identity Manager の構成ファイルをすべてバックアップします。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

IBM Security Identity Managerを実行している各コンピューターにログインします。以下のファイルをバックアップします。

- *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリー
  - banner.jsp
  - calendar.css
  - customForm.css
  - customForm_rtl.css
  - dateWidget_ltr.css
  - dateWidget_rtl.css
  - enduser.css

- enduser_rtl.css
- footer.jsp
- Home.jsp
- loginBanner.jsp
- loginFooter.jsp
- loginToolbar.jsp
- nav.jsp
- time.css
- toolbar.jsp
- widgets.css
- widgets_rtl.css

注: デフォルト・ファイルは、*ITIM_HOME*¥data¥defaults ディレクトリーにもあります。

- *ITIM_HOME*¥data ディレクトリー:
  - SelfServiceHelp.properties
  - SelfServiceHomePage.properties
  - SelfServiceScreenText.properties
  - SelfServiceUI.properties
  - SelfServiceScreenTextKeys.properties

このタスクについて

プロパティー・ファイルに変更を加えた場合は、IBM Security Identity Managerアプリケーションの再始動が必要です。例えば、いずれかのプロパティー・ファイルをリカバリーするには、以下の手順を実行します。

手順

1. WebSphere® 管理コンソールで、左方のフレームの「**アプリケーション**」グループをクリックしてから 「**エンタープライズ・アプリケーション**」リンクをクリックします。
2. IBM Security Identity Manager アプリケーションの横のチェック・ボックスを選択して、「**停止**」ボタンをクリックします。
3. アプリケーションが停止した後、IBM Security Identity Manager アプリケーションの横のチェック・ボックスを選択して「**開始**」ボタンをクリックします。
4. セルフ・サービス・ユーザー・インターフェースにログインして、リカバリーが完了したことを確認します。

ビュー定義の影響を受けるユーザー・インターフェース・エレメント

定義されたビューは、セルフ・サービス・インターフェースのタスク・パネルおよびその他のエレメントの表示に影響します。

ビュー定義エレメント

ビュー定義は、セルフ・サービス・ユーザー・インターフェースに対して以下の影響を与えることができます。

ホーム・ページ

ホーム・ページは、ユーザーが権限付与されているタスクおよびタスク・パネルのみをホーム・ページに表示することによってユーザーのビューに対応します。ユーザーがセクション内のどのタスクも表示することを許可されていない場合、ホーム・ページにはタスク・パネルも表示されません。

「アカウントの要求」タスクなど一部のタスク・ビューには、拡張ビューがあります。言い添えれば「アカウントの要求」タスクは単一タスクです。ユーザーに「アカウントの要求拡張 (Request Account Advanced)」ビューが権限付与されているか、「アカウントの要求」ビューと「アカウントの要求拡張 (Request Account Advanced)」ビューの両方が権限付与されている場合は、ホーム・ページに単一の「**アカウントの要求**」タスクが表示されます。「アカウントの要求」のメイン・ページには、ユーザーがアカウントを要求できるサービスを検索するための検索ページが表示されます。標準の「アカウントの要求」ビューの権限のみが付与されており、拡張ビューの権限は付与されていない場合、ホーム・ページには「**アカウントの要求**」タスクが表示されます。「アカウントの要求」のメイン・ページには、検索ページではなく、ユーザーがアカウントを要求できるサービスをリストしたテーブルが表示されます。

ユーザーが、アカウントまたはプロファイルの「変更」タスクと「表示」タスクの両方を実行できる場合、それらのタスクは単一のタスクとして結合されます。そのタスクは、例えば、「**アカウントの表示または変更**」と表示されます。

一部のタスクは、システム管理者によって使用可能にされていない場合には表示されません。例えば、「**パスワードを忘れた場合の情報の変更**」では、ユーザー確認の質問への応答が使用可能化されている必要があります。

「**必要なアクション**」タスクは、処理中の予定項目が存在しているか、ユーザー確認の質問への応答情報が構成されていない場合にのみ有効です。

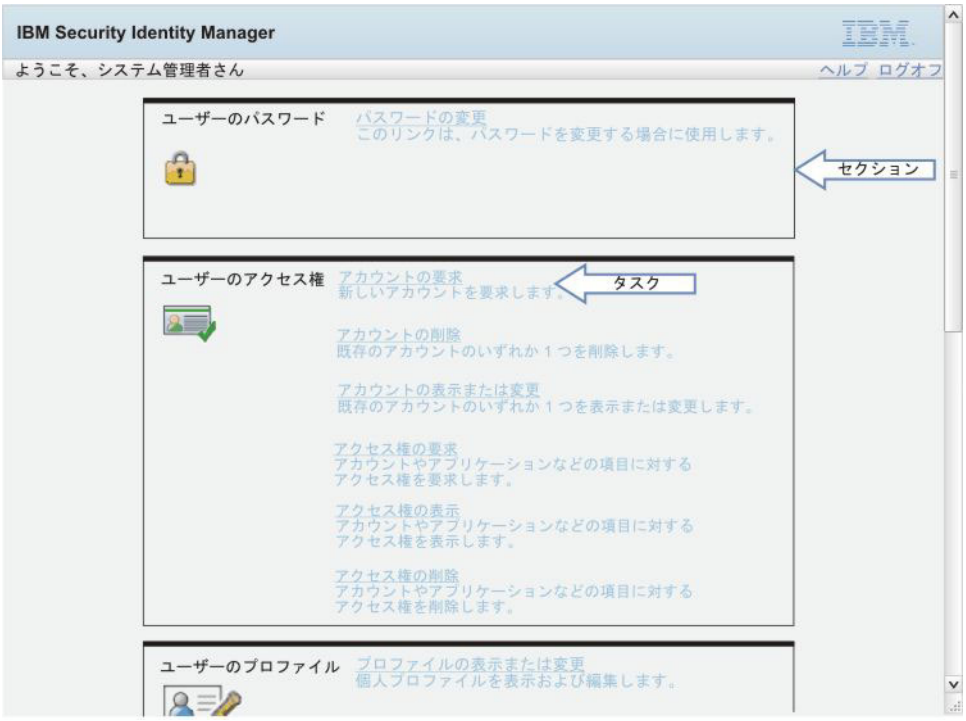


図 1. ホーム・ページ・エレメント

関連するタスク

関連するタスク・セクションは、セルフ・サービス・アプリケーションのいろいろな部分、例えば要求が実行されたときなどに表示されます。ビュー定義を使用すると、ビュー定義での許可に基づいて、これらのセクションの一部または全部の表示をフィルターできます。例えば、「**ユーザーの要求の表示**」に対する通常のアクセス権を持たないユーザーの場合は、このタスクが「**関連するタスク**」タスク・パネルから取り除かれます。

図 2. 関連するタスクのパネル・エレメント

パネル説明テキスト

一部の画面の説明テキストには、「**ユーザーの要求の表示**」タスクを含めることができます。ビュー定義でユーザーに「**ユーザーの要求の表示**」タスクが権限付与されていない場合は、このタスク・リンクを含まない異なる説明

メッセージが表示されます。

図 3. 説明テキストのパネル・エレメント

ラベル、説明、およびその他の画面テキストのカスタマイズ

カスタマイズを行って、セルフ・サービス・ユーザー・インターフェースに表示される大部分のテキストを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

ユーザーはすべてのラベルをカスタマイズできるわけではありません。SelfServiceScreenTextKeys.properties ファイルに項目が存在するラベルのみをカスタマイズできます。

以下の画面テキスト項目をカスタマイズできます。

- タイトル
- サブセクション・タイトル
- サブセクションの説明
- フィールド・ラベル
- テーブル列の見出しおよびフッター
- ボタン・テキスト

次の図に、これらの画面テキスト項目のビジュアル表示を示します。

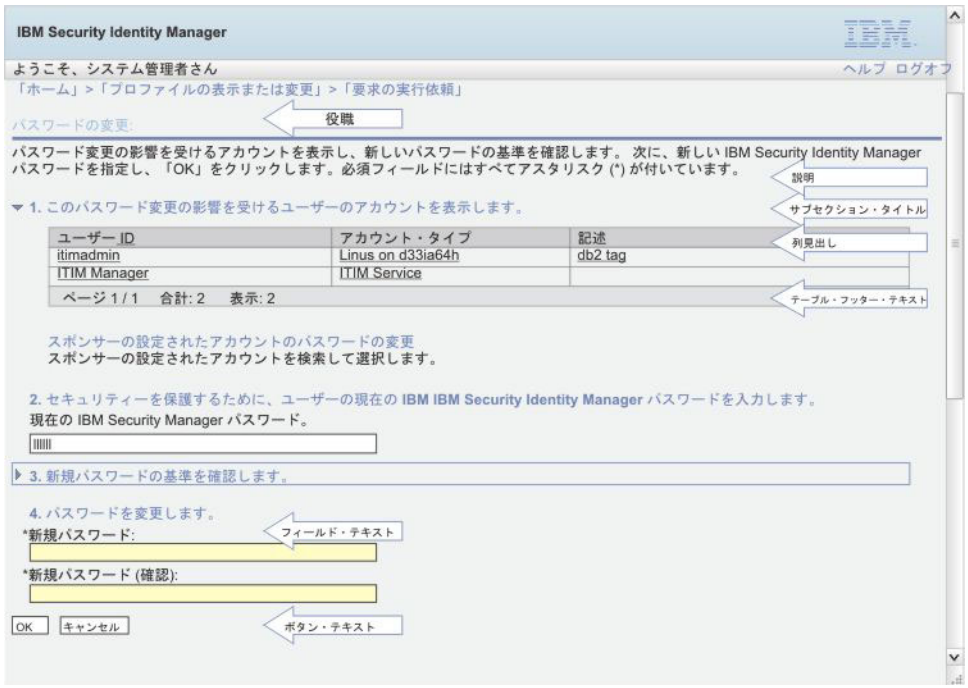


図 4. 画面テキスト

エラー・メッセージや、ヘルプ・リンクをクリックしてアクセスするヘルプ・コンテンツなどのテキストは置換できません。ただし、ヘルプ要求を別の URL サイトにリダイレクトすることはできます。

画面テキストをカスタマイズするには、以下の手順を完了します。

手順

1. `SelfServiceScreenText.properties` ファイルおよび `SelfServiceScreenTextKeys.properties` ファイルのバックアップ・コピーを作成します。言語パックをインストールしている場合は、`SelfServiceScreenText_en.properties` ファイルも含め、変更予定のその他の言語パック・ファイルをバックアップしてください。`SelfServiceScreenText.properties` は、他に一致する言語が検出されなかった場合に使用されるデフォルト・ファイルです。
2. プロパティー・ファイルを編集します。画面のテキスト・フィールドの値を変更し、ファイルを保存します。整合性を保つためには、`SelfServiceScreenText.properties` ファイルに対して加えたすべての変更を `SelfServiceScreenText_en.properties` ファイルにも加える必要があります。
3. IBM Security Identity Manager アプリケーションを再始動して、変更を有効にします。

Web サイト・レイアウトのカスタマイズ

カスタマイズを行って、セルフ・サービス・ユーザー・インターフェース内のレイアウトを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

SelfServiceUI.properties ファイル内の設定を使用して、セルフ・サービス・ユーザー・インターフェースでの上位レイアウト・エレメントの表示を有効または無効にできます。デフォルト・レイアウトには、バナー、ツールバー、およびフッターが含まれています。

ページ要素をオン/オフすることで、さまざまなレイアウトを実現できます。唯一の必須ページ要素は、コンテンツ要素です。コンテンツ要素は、タスクおよびタスク・ページを含んでいます。

ページ要素を表示または非表示にするには、SelfServiceUI.properties ファイル内の ui.layout.show*name* プロパティーを変更します。例えば、ui.layout.showBanner は、バナー・セクションの表示を制御します。要素をページに含めるときはプロパティーに true を設定します。要素をページに含めないときはプロパティーに false を設定します。

SelfServiceUI.properties に何らかの変更を加えた場合にその変更を有効にするには、WebSphere で IBM Security Identity Manager を再始動する必要があります。

以下の図に、さまざまなレイアウト・エレメントおよびオプションのビジュアル表示を示します。

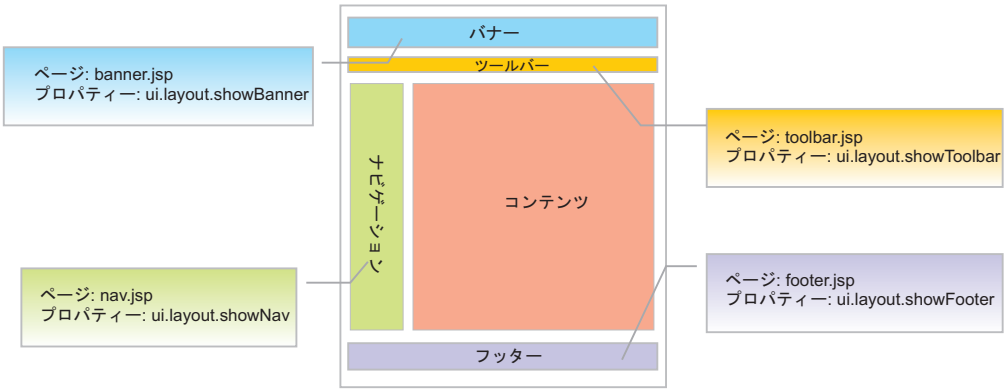


図 5. レイアウト・エレメント

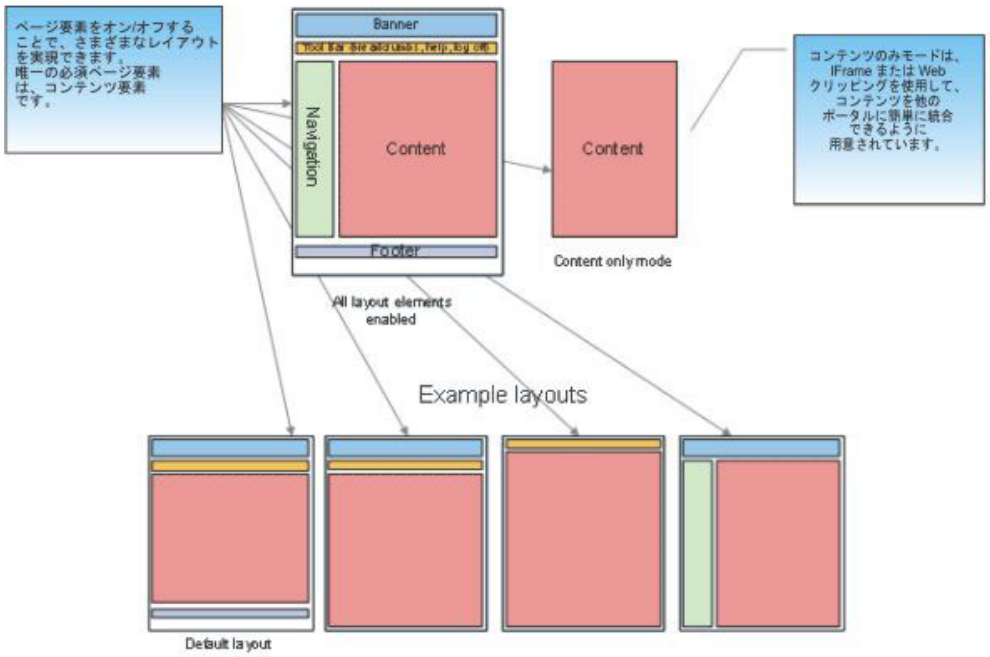


図 6. レイアウト・オプション

次の表に、プロパティーおよびそれらの詳細のリストを示します。

表 4. レイアウトのプロパティーと詳細

プロパティー	説明
ui.layout.showBanner	バナー・セクションを制御します。デフォルトのバナーは、IBM および製品のイメージを含んでいます。
ui.layout.showFooter	フッター・セクションを制御します。デフォルトのフッターは、製品の著作権表示を含んでいます。
ui.layout.showToolbar	ツールバー・セクションを制御します。デフォルトのツールバーは、ウェルカム・メッセージ、ヘルプ・リンク、ログオフ・リンク、およびパンくずを含んでいます。
ui.layout.showNav	ナビゲーション・バーを制御します。 **注:** ナビゲーション・バーは、デフォルトのコンテンツを含んでいません。

レイアウトをカスタマイズするには、以下の手順を実行します。

手順

1. *ITIM_HOME*¥data ディレクトリーにある SelfServiceUI.properties ファイルのバックアップ・コピーを作成します。
2. SelfServiceUI.properties ファイルを編集します。画面のテキスト・フィールドの値を変更し、ファイルを保存します。

3. IBM Security Identity Manager アプリケーションを再始動して、変更を有効にします。

バナー、フッター、ツールバー、およびナビゲーション・バーのコンテンツのカスタマイズ

バナー、フッター、ツールバー、およびナビゲーション・バーをカスタマイズして、セルフ・サービス・ユーザー・インターフェースの外観を変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

WAS_PROFILE_HOME¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーにあるコンテンツを置換または変更して、セルフ・サービス・ユーザー・インターフェースの外観を変更できます。 バナー、フッター、ツールバー、およびナビゲーション・バーを置換または変更できます。

レイアウト・エレメントは、JSP をレンダリングするときに Web ページのレイアウトに組み込まれる JSP フラグメントです。

次の表に、レイアウト・エレメントおよび対応するファイルをリストします。これらのファイルは、*WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーにあります。

表 5. レイアウト・エレメントおよびファイル名

レイアウト・エレメント	ファイル名
バナー	banner.jsp
フッター	footer.jsp
ツールバー	toolbar.jsp
ナビゲーション・バー	nav.jsp

これらのファイルを変更するには、以下の手順を実行します。

手順

1. ファイルのバックアップ・コピーを作成し、変更するファイルを一時ディレクトリーに保存します。
2. 一時ディレクトリーに保存したファイルを編集し、更新したファイルをコピーして、デプロイされた WebSphere ディレクトリーに戻します。これらの変更を有効にするために、IBM Security Identity Manager アプリケーションを再始動する必要はありません。

次のタスク

これらのファイルのデフォルト・バージョンは、製品アーカイブに付属しています。変更内容が失われないために、作成したカスタム・バージョンのファイルをバックアップするようにしてください。

ユーザー・インターフェース・コンテンツのカスタマイズで使用する要求パラメーターとコンテンツの例

このセクションでは、コンテンツをカスタマイズするために JSP ファイルで使用できる要求パラメーターについて説明します。

要求パラメーター値

パンくず、ヘルプ・リンク、ユーザー ID などの動的コンテンツをサポートするため、いくつかの要求パラメーターが使用可能になっています。次の表に、該当するプロパティー、それらに指定可能な値、および説明を示します。

表 6. 要求パラメーター、値、および説明

プロパティー名	値	説明
loggedIn	true または false	ユーザーが現在ログインしているかどうかを示すフラグです。
usercn	ログイン・アカウントの所有者の共通名	**注:** この値は、ユーザーがログインしている場合にのみ設定されます。
langOrientation	ltr または rtl	現行ロケールの言語の向き、左から右または右から左を示します。
helpUrl	/itim/self/Help.do?helpId=*example_url*	現行ページを *helpId* パラメーターに設定した、ヘルプ Web ページの URL です。
helpLink	例: home_help_url	現行ページの *helpId* です。値 *home_help_url* は、SelfServiceHelp.properties ファイル内の対応するキーにマップします。
breadcrumbs	*example_message_key1* *example_message_key2* *example_message_key3*	SelfServiceScreenText.properties ファイル内の項目に対応するメッセージ・キーのリストです。
breadcrumbLinks	*pathname1* *pathname2* *empty_string*	breadcrumbs リストと同じ長さの、リンクのリストです。

toolbar.jsp 内の要求パラメーターの例

デフォルトのファイル toolbar.jsp には、ウェルカム・メッセージとヘルプ・リンクを表示するロジックが含まれています。 このロジックを他のレイアウト・エレメントに移動することができ、例えば、ウェルカム・メッセージをバナーに表示することが可能です。

ウェルカム・メッセージの表示

以下のコードは、ユーザーの共通名が設定されているかどうかを検査します。設定されている場合は、ウェルカム・メッセージを変換し、名前を置換してメッセージ内に含めます。

注: セルフ・サービス・ユーザー・インターフェースのメッセージ・ラベルおよびキーは、SelfServiceScreenText.properties ファイルに定義されています。

```
<%-- ユーザーの共通名が空でない場合はそれを表示。この値は、
     ユーザーがログインしないうちは設定されません。 --%>

<c:if test="${!empty usercn and loggedIn == true}">
    <%-- 名前に引き渡すウェルカム、共通名メッセージの変換 --%>
    <fmt:message key="toolbar_username" >
        <fmt:param><c:out value="${usercn}"/></fmt:param>
    </fmt:message>
</c:if>
</div>
<%-- エンド・ユーザー情報 -- %>
```

ヘルプ・リンクの表示

次のコードでは、ページにヘルプ・リンクを追加します。helpUrl をヘルプ属性から検索し、ヘルプ・ラベルを表示用に変換します。

```
<%-- ページにヘルプ・リンクを追加 --%>

<a id="helpLink" href="javascript:launchHelp('<c:out value='${helpUrl}')">
      <fmt:message key="toolbar_help"/></a>
```

ログオフのサポート

ログオフ・リンクは、ユーザーがログインしているときにのみ表示する必要があります。次のコードは、loggedIn 要求パラメーターが true かどうかを検査します。true の場合、このコードはログオフ・リンクのラベルを変換し、そのリンクをページに組み込みます。

```
<%-- ユーザーがログインしている場合は、ログオフ・リンクを表示 --%>
<c:if test="${loggedIn == true}">
   <a id="logofflink" href="/itim/self/Login/Logoff.do">
       <fmt:message key="toolbar_logoff"/></a>
</c:if>
```

breadcrumbs の表示

次のコードでは、ページに breadcrumbs を追加します。breadcrumbs 属性は、その breadcrumbs 用のラベル・キーのリストを含んでいます。breadcrumbLinks は各 breadcrumb ラベルの URL 情報を含んでいます。breadcrumbLinks の値がヌルまたは空であれば、その breadcrumb にはリンクできません。

```
<%-- breadcrumbs ラベル・キーが空でない場合は、表示 --%>

<c:if test="${!empty breadcrumbs}">
    <c:forEach items="${breadcrumbs}" var="breadcrumb" varStatus="status">

        <c:if test="${status.index > 0}">
             &gt; 
        </c:if>

        <c:choose>
```

```
            <%-- 現行ラベルのアクション・リンクが空でない場合は、
                 breadcrumb のリンクを作成 --%>

            <c:when test="${!empty breadcrumbLinks{status.index}}">
                <html:link action="${breadcrumbLinks{status.index}}">
                <fmt:message key="${breadcrumb}"/></html:link>
            </c:when>
            <%-- アクション・リンクが空である場合は、
                 breadcrumb のラベルの変換のみを実行 --%>
            <c:otherwise>
                <fmt:message key="${breadcrumb}"/>
            </c:otherwise>
        <c:choose>

    </c:forEach>

</c:if>
```

セルフ・サービス・ホーム・ページのカスタマイズ

カスタマイズを行って、セルフ・サービス・ユーザー・インターフェース内のホーム・ページを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

ホーム・ページは、ユーザーがセルフ・サービス・ユーザー・インターフェースにログインしたときにコンテンツ・レイアウト・エレメントに読み込まれるメイン・ページです。

セクション定義とタスク定義を使用して、定義済みのビューとタスクを結び付け、タスクをセクション (タスク・ページとも呼ぶ) としてグループ化します。 これらのセクション定義およびタスク定義は、*ITIM_HOME*¥data ディレクトリー内の SelfServiceHomePage.properties に定義されています。

ホーム・ページ・レイアウト・エレメントは、Web ページのレイアウトに含まれている JSP フラグメントです。このレイアウト情報は、*WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーの Home.jsp ファイルに格納されます。

SelfServiceHomePage.properties ファイルを更新して、ホーム・ページにタスクおよびセクションを追加できます。ファイル内のコメントで、ファイル・フォーマットが説明されています。JSP ファイルを変更することなくコンテンツを変更できます。

ホーム・ページをカスタマイズするには、以下の手順を実行します。

手順

1. *ITIM_HOME*¥data ディレクトリーにある SelfServiceHomePage.properties ファイルのバックアップ・コピーを作成します。

2. *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーにある Home.jsp のバックアップ・コピーを作成します。
3. SelfServiceHomePage.properties ファイルを編集します。値を変更し、ファイルを保存します。
4. Home.jsp ファイルを別のディレクトリーにコピーし、その別のディレクトリーのファイルを変更してから、この更新したファイルをコピーして *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーに戻します。 これらのファイルのデフォルト・バージョンは、製品アーカイブに付属しています。実行済みのカスタマイズが失われないために、作成したカスタム・バージョンのファイルをバックアップするようにしてください。
5. WebSphere で IBM Security Identity Manager アプリケーションを再始動して、変更を有効にします。

ホーム・ページ・コンテンツのカスタマイズで使用する要求パラメーターとコンテンツの例

このセクションでは、ホーム・ページ・コンテンツをカスタマイズするために JSP ファイルで使用できる要求パラメーターについて説明します。

ホーム・ページ・フォームのパラメーター

セクション、アクションを要するセクション、タスクなど、動的なホーム・ページ・コンテンツをサポートするために、要求パラメーターとして **HomePageForm** という JavaBeanが使用可能になっています。このホーム・ページ Java Bean は、セクションやタスクに関する情報にアクセスするために使用できる多数のメソッドを含んでいます。

表 7. ホーム・ページ要求パラメーター、値、および説明

プロパティー名	値	説明
sections	セクション Java Bean のリスト	現在のユーザーが表示できるセクションのリストです。
sectionToTaskMap	セクションとそれに対応するタスクのマップ	指定されたセクション Java Bean をタスク Java Bean にリンクするマップです。
actionNeededSection	セクション Java Bean またはヌル	現行ユーザーの処理中アクションを含んでいるセクション Java Bean です。現行ユーザーの処理中アクションが存在しない場合は、ヌルが使用されます。

セクション Java Bean では、以下のプロパティーが使用可能です。

表 8. セクション Java Bean 要求パラメーター、値、および説明

プロパティー名	値	説明
titleKey	セクションのタイトル・メッセージ・キー	セクション・タイトルのメッセージ・キーです。

表 8. セクション Java Bean 要求パラメーター、値、および説明 (続き)

プロパティー名	値	説明
iconUrl	アイコンの URL またはヌル	このセクションに使用するアイコンの URL パスです。ヌルは、アイコンを使用しないことを示す場合に使用します。
iconAltTextKey	テキスト・キー	このセクションのアイコンの代替テキストとして使用するテキスト・キーです。
tasks	タスク JavaBean のリスト	このセクションに表示できるタスクのリストです。

タスク Java Bean では、以下のプロパティーが使用可能です。

表 9. タスク JavaBean 要求パラメーター、値、および説明

プロパティー名	値	説明
urlPath	URL	このタスクの URL パスです。
urlKey	テキスト・キー	このタスクへのリンクに使用するテキスト・キーです。
descriptionKey	テキスト・キー	このタスクの説明として使用するテキスト・キーです。

home.jsp 内の要求パラメーターの例

以下のコードでは、**HomePageForm** JavaBean を取得し、使用可能なセクションとタスクについて反復し、使用可能な各タスクのリンクを作成します。

```
<c:set var="pageConfig" value="${HomePageForm}" scope="page" />
<c:forEach items="${pageConfig.sections}" var="section">
      <%-- ここで各セクションを処理 --%>
      <c:forEach items="${pageConfig.sectionToTaskMap[section]}" var="task">
      <%-- ここで各セクションを処理 --%>
            <a href="/itim/self/<c:out value="${task.urlPath}"/>"
               title="<fmt:message key="${task.urlKey}" />">
               <fmt:message key="${task.urlKey}" />
            </a>
            <fmt:message key="${task.descriptionKey}" />
      </c:forEach>
</c:forEach>
```

スタイル・シートのカスタマイズ

カスケーディング・スタイル・シート (CSS) をカスタマイズして、セルフ・サービス・ユーザー・インターフェースの外観を変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

カスケーディング・スタイル・シート (CSS) は、セルフ・サービス・ユーザー・インターフェースの外観をスタイル設定するために使用します。スタイルシートを編集して、フォント、色、およびその他のセルフ・サービス・ユーザー・インターフェースに関連するスタイルを修正できます。このセクションでは、スタイル・シートのロケーションについて説明するとともに、Web サイトのルック・アンド・フィールに合わせてユーザー・インターフェースをカスタマイズ編集するときに重要なスタイルについて説明します。

デプロイされたデフォルトの CSS ファイルは、圧縮されており、スケーラビリティーよりも帯域幅を考慮して最適化されています。 (空白およびフォーマットが保たれた) 最適化されていないバージョンは、*ITIM_HOME*¥defaults¥custom ディレクトリーにあります。
WAS_PROFILE_HOME¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーにある CSS ファイルは編集に適していません。
ITIM_HOME¥defaults¥custom ディレクトリーに格納されているデフォルト・ファイルを別のディレクトリーにコピーします。スタイル・シートを編集し、変更したファイルを
WAS_PROFILE_HOME¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーにコピーします。

次の表に、セルフ・サービス・ユーザー・インターフェースを調整するために変更できる CSS ファイルを示します。

表 10. カスケーディング・スタイル・シート・ファイル名

CSS ファイル名	説明
end_user.css	左から右方向の言語でのメイン CSS スタイルを格納した CSS ファイルです。
end_user_rtl.css	右から左方向の言語でのメイン CSS スタイルを格納した CSS ファイルです。
widgets.css	左から右方向の言語での、プロファイル、アカウント、および RFI などのフォームに含まれているウィジェットに使用するスタイルを格納した CSS ファイルです。 **注:** このファイルを編集するには CSS の上級スキルが必要です。
widgets_rtl.css	右から左方向の言語での、プロファイル、アカウント、および RFI などのフォームに含まれているウィジェットに使用するスタイルを格納した CSS ファイルです。 **注:** このファイルを編集するには CSS の上級スキルが必要です。
dateWidget_ltr.css	左から右方向の言語での、プロファイル、アカウント、および RFI などのフォームに含まれている日付ウィジェットに使用するスタイルを格納した CSS ファイルです。 **注:** このファイルを編集するには CSS の上級スキルが必要です。

表 10. カスケーディング・スタイル・シート・ファイル名 (続き)

CSS ファイル名	説明
dateWidget_rtl.css	右から左方向の言語での、プロファイル、アカウント、および RFI などのフォームに含まれている日付ウィジェットに使用するスタイルを格納した CSS ファイルです。 **注:** このファイルを編集するには CSS の上級スキルが必要です。
time.css	プロファイル、アカウント、および RFI などのフォームに含まれている時刻ウィジェットに使用するスタイルを格納した CSS ファイルです。 **注:** このファイルを編集するには CSS の上級スキルが必要です。
customForm.css	左から右方向の言語での、プロファイル、アカウント、および RFI などのフォームに含まれている、フォームのレイアウトに使用するスタイルを格納した CSS ファイルです。 **注:** このファイルを編集するには CSS の上級スキルが必要です。
customForms_rtl.css	右から左方向の言語での、プロファイル、アカウント、および RFI などのフォームに含まれている、フォームのレイアウトに使用するスタイルを格納した CSS ファイルです。 **注:** このファイルを編集するには CSS の上級スキルが必要です。

以下の図は、スタイルの変更を適用できるページ要素のビジュアル表示を示します。

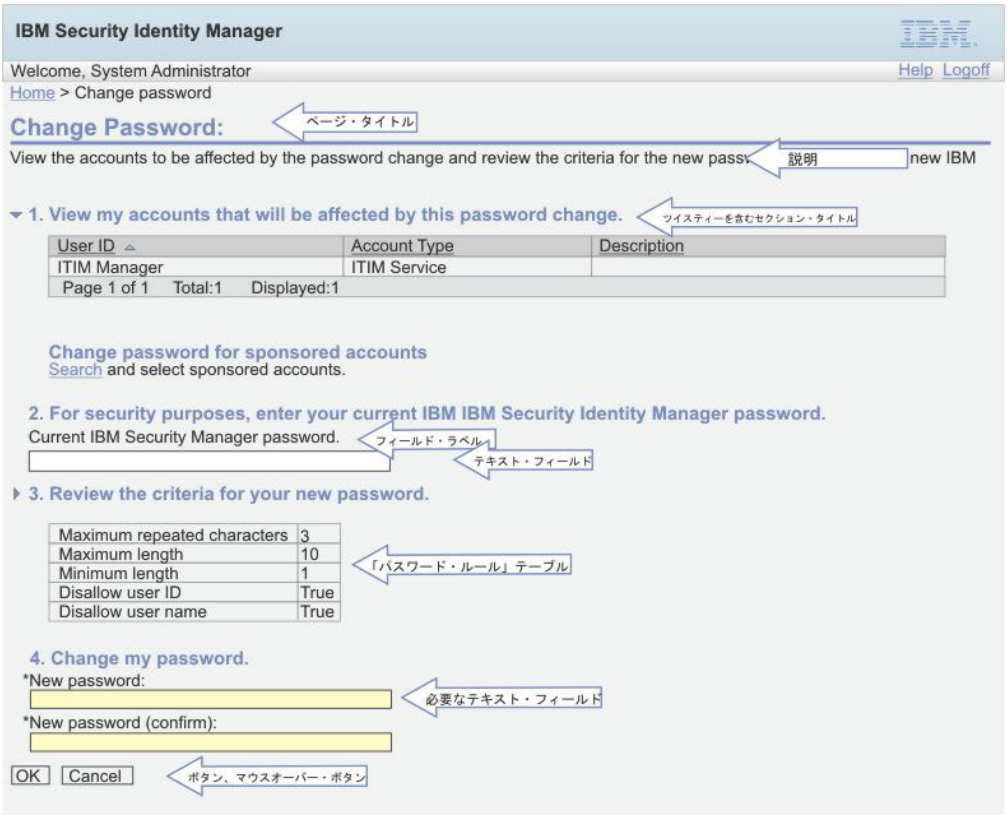


図 7. スタイル変更に対応するページ要素

図 8. スタイル変更に対応するページ要素 (続き)

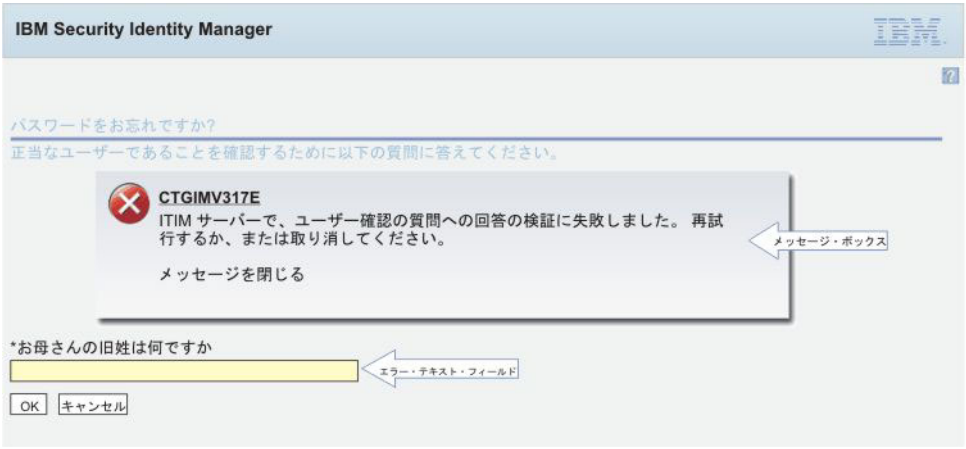


図 9. スタイル変更に対応するページ要素

次の表に、主な CSS スタイルのリファレンスを示します。

表 11. CSS スタイルのリファレンス

要素	例	主なスタイル・セレクター	説明
ページ・タイトル	**ページ・タイトル**	タイプ・セレクター: h1	すべてのページ・タイトルに使用される要素です。
セクション・タイトル	**サブセクション・タイトル**	タイプ・セレクター: h2	ツイスティーを含まないページのセクション・タイトルです。
セクション・タイトル (ツイスティー)	**ツイスティー・タイトル**	タイプ・セレクター: h3	ツイスティー・セクションを含むページのセクション・タイトルです。このタイトルはツイスティー・イメージを表示するスペースを空けるようになっています。
breadcrumbs	「ホーム」 >「プロファイルの表示または変更」	タイプ・セレクター: #breadcrumbs	ページ・タイトルの上、ページの左上に表示される breadcrumbs ナビゲーション・トレールです。

表 11. CSS スタイルのリファレンス (続き)

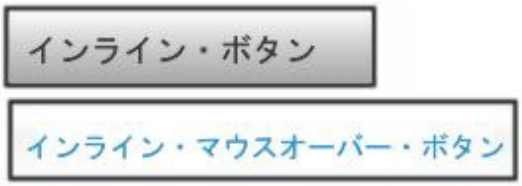
要素	例	主なスタイル・セレクター	説明
ボタン、マウスオーバー・ボタン、使用不可ボタン		クラス・セレクター: • .button • .button_hover • .button_disabled	これらのボタン・スタイルが、ユーザー・インターフェースのボタンの大部分をカバーします。hover スタイルは、マウスがボタン上に移動したときに使用されます。
インライン・ボタン、マウスオーバー・インライン・ボタン		クラス・セレクター: • .button_inline • .button_inline_hover	特別なレイアウト要件を持つボタンのサブセットに使用されます。
ページとセクションの説明	これは説明です。	クラス・セレクター: .description	ページとセクションの説明です。説明は ブロック内に含まれます。したがって、必要に応じて、ボーダー、色などを追加できます。
フィールド・ラベル	フィールド・ラベル	タイプ・セレクター: label	フォーム上のフィールド・ラベルです。
テキスト・フィールド	テキスト・フィールド (フィールド背景白がデフォルト)	クラス・セレクター: input.textField_std	標準テキスト・フィールドです。
必須テキスト・フィールド	必須テキスト・フィールド (フィールド背景黄がデフォルト)	クラス・セレクター: input.textField_required	必須テキスト・フィールドです。
エラー・テキスト・フィールド	エラー・テキスト・フィールド (フィールド枠赤がデフォルト)	クラス・セレクター: input.textField_error	テキスト・フィールドはエラー状態です。
警告テキスト・フィールド	警告テキスト・フィールド (フィールド枠黄がデフォルト)	クラス・セレクター: input.textField_warning	テキスト・フィールドは警告状態です。

表 11. CSS スタイルのリファレンス (続き)

要素	例	主なスタイル・セレクター	説明
フィールド/値テーブル	Field Name1 Field value1 Field Name2 Field value2 Multi-valued Field3 Item 1 Item 2 Item 3 Item 4 Multi-valued Field3 Item 1 Item 2	クラス・セレクター: table.nameValueTable	フィールド値テーブルは、フィールド名および 1 つ以上の対応する値を表示するためにユーザー・インターフェース全体で使用されています。例えば、要求実行後のページの「情報」セクションでは、名前値テーブルを使用しています。ここでは、テーブル用のセレクターを示してあります。他に、このテーブルの行、セル、複数値リスト、および名前列のスタイルを設定するセレクターがあります。

表 11. CSS スタイルのリファレンス (続き)

要素	例	主なスタイル・セレクター	説明
パスワード・ルール・テーブル	◆ Rule1 Value1 AccountInfo1 ◆ Rule2 Value2 AccountInfo2	クラス・セレクター: • .pwRulesTable • .pwRulesTable .ruleCol • .pwRulesTable .valueCol • .pwRulesTable .accountInfoCol • .button_inline_hover	パスワード・ルール・テーブルは、ユーザー・インターフェース全体で、パスワード・ルール・セクションのスタイルを設定するために使用されています。このテーブルは、ルール列、値列、およびアカウント情報列の 3 つの列で構成されています。
メッセージ・ボックス		div.messageBoxComposite	メッセージ・ボックス・コンポジットは、メッセージ・ボックスのメイン CSS セレクターです。他にそれぞれイメージ、リンク、およびメッセージ・レイアウトを指定するセレクターがあります。

スタイルシートをカスタマイズするには、以下の手順を実行します。

手順

1. *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥custom ディレクトリーにある CSS ファイルのバックアップ・コピーを作成します。
2. CSS ファイルを *ITIM_HOME*¥defaults¥custom ディレクトリーから別のディレクトリーにコピーし、その別のディレクトリーのファイルを変更してから、更新したファイルを *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_self_service.war¥

custom ディレクトリーにコピーします。実行済みのカスタマイズが失われないために、作成したカスタム・バージョンのファイルをバックアップするようにしてください。

前バージョンからのスタイル・シート・カスタマイズのマージ

前バージョンの IBM Tivoli® Identity Manager からアップグレードした後は、セルフ・サービス・ユーザー・インターフェースのカスケーディング・スタイル・シートに対して行ったすべてのカスタマイズを再適用する必要があります。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

IBM Tivoli Identity Manager がデプロイされているファイル・システムに対するアクセス権限が必要です。

IBM Security Identity Manager とカスケーディング・スタイル・シート (CSS) の実用的な知識が必要です。

このタスクについて

管理コンソールを使用して定義される、ビュー定義を含めたカスタマイズは、アップグレード時に保持されます。 SelfServiceScreenText.properties に対する更新も自動的にマージされます。

ただし、アップグレード・プログラムが完了した後、デプロイ済みのセルフ・サービス・カスケーディング・スタイル・シート (CSS) は出荷時のデフォルト値に復元されます。まず、更新済みの CSS 値を、前バージョンの製品用に作成されたカスタマイズ済みの CSS スキンにマージします。次に、カスタマイズしたファイルを、デプロイ済みのセルフ・サービス war ファイルにマージします。

注: アップグレードの実行中に、ITIM.ear ファイルが、WebSphere Application Server から *ISIM_HOME*/data/backup/ITIM.ear ディレクトリーにバックアップされます。アップグレード前にデプロイされていた CSS スキンのコピーについては、itim_self_service.war/custom ディレクトリーを調べることができます。

CSS のカスタマイズをマージするには、組織の元の IBM Tivoli Identity Manager CSS ファイルに対して以下の追加と変更を行ってください。

注: 右から左 (RTL) の CSS ファイル (例えば、enduser_rtl.css) に変更を加えた場合は、テキスト比較ツールを使用してその変更をマージします。enduser_rtl.css ファイルに対して、enduser.css ファイルに対するものと同等の変更を行います。ただし、右から左のレイアウトに合わせて調整します。

手順

1. 既存の CSS ファイルをエディターで開きます。

このファイルは、以下のディレクトリーにあります。ITIM_HOME/data/backup/ITIM.ear

注: 別のシステム・アップグレードの場合は、デプロイ済みの ITIM.ear ファイルからファイルをコピーしてください。

2. マイグレーション・パスに基づいて、適切な変更を追加します。 『CSS の更新』を参照してください。

   バージョン 5.0 からバージョン 6.0 にマイグレーションする場合は、バージョン 5.1 とバージョン 6.0 の両方で行われた CSS の変更を追加します。

   バージョン 5.1 からバージョン 6.0 にマイグレーションする場合は、バージョン 6.0 で行われた CSS の変更だけを追加します。

3. 更新済みの CSS ファイルを、セルフ・サービス・ユーザー・インターフェースのカスタム・ディレクトリー itim_self_service.war/custom にコピーします。

タスクの結果

変更は即座に有効になりますので、IBM Security Identity Manager アプリケーションの再始動は必要ありません。

CSS の更新

5.1 に追加された CSS の変更:

enduser.css

説明: h2 ヘッダーのツイスティーが追加されました。

次のテキストを追加します。

```
a.twistie_open h2{
 margin-left:0px;
 background-repeat: no-repeat;
 background-position: left;
 padding-left: 15px;
 background-image: url("/itim/self/images/twistie_open.gif");
}

a.twistie_closed h2{
 margin-left:0px;
 background-repeat: no-repeat;
 background-position: left;
 padding-left: 15px;
 background-image: url("/itim/self/images/twistie_closed.gif");
}
```

説明: アクティビティーの確認の説明がツイスティーに変更されました。

次のテキストを追加します。

```
/* Review Activity Styles */
#instructionDetailTwistieDiv {
 white-space: expression("pre"); /* IE */
 white-space: -moz-pre-wrap; /* Firefox */
 word-wrap: break-word;
}
/* End Review Activity Styles */
```

説明: ユーザー再認証用の CSS スタイルが追加されました。

次のテキストを追加します。

```
/* Recertification items table styles */
table.recertItemsTable {
 width: auto;
}

table.recertItemsTable th {
 padding: .2em 1em .2em 1em;
 background-color: #C0C0C0;
 white-space: nowrap;
 text-align: left;
}

table.recertItemsTable td {
 padding: .2em 1em .2em 1em;
 border: 1px solid #C0C0C0;
}

table.recertItemsTable tr.recertItemRow td {
 border-bottom-style: none;
}

table.recertItemsTable tr.recertSubItemRow td {
 border-top-style: none;
 border-bottom-style: none;
}

table.recertItemsTable tr.altRow {
 background-color: #F6F6F6;
}

table.recertItemsTable .selectAllOptions {
 display: inline;
 padding: 0 .5em 0 .5em;
 font-weight: normal;
}

table.recertItemsTable .selectAllOptions a {
 padding: 0 .3em 0 .3em;
 color:#1375D7;
 font-weight: normal;
}

table.recertItemsTable .recertItemSelectAllOptions {
 display: inline;
 padding: 0 .5em 0 .5em;
 font-weight: normal;
 font-size: .8em;
}

table.recertItemsTable .recertItemSelectAllOptions a {
 padding: 0 .3em 0 .3em;
}

table.recertItemsTable a.recertExpandCollapseLink {
 margin-right: .2em;
}

table.recertItemsTable a.recertExpandCollapseLink img {
 border: none;
 vertical-align: bottom;
}

table.recertItemsTable div.recertItem {
 display: inline;
 margin-bottom: 2px;
```

```
}

table.recertItemsTable td.recertItemImpact {
 text-align: center;
}

table.recertItemsTable div.recertItemDescription {
 max-width: 300px;
 font-size: .8em;
}

table.recertItemsTable div.recertItemImpactedBy {
 display: inline;
 margin-bottom: 2px;
}

table.recertItemsTable td.recertItemActionRecertify {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding-right: 0;
 border-right: none;
}

table.recertItemsTable td.recertItemActionRecertifyErrorNone {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding: .2em 0 .2em 13px;
 border-right: none;
}

table.recertItemsTable td.recertItemActionRecertifyErrorExists {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding: .2em 0 .2em 5px;
 border-right: none;
}

table.recertItemsTable td.recertItemActionReject {
 width: 0%;
 white-space: nowrap;
 padding-left: 0;
 border-left: none;
 border-right: none;
}

table.recertItemsTable td.recertItemActionBlank {
 height: 24px;
}

table.recertItemsTable label.recertItemAction {
 display: inline;
}

table.recertItemsTable td.recertItemSelectAll {
 width: 0%;
 white-space: nowrap;
 padding-left: 0;
 border-left: none;
}

table.recertItemsTable .recertSubItem {
    font-size: 1em;
    margin: 0 0 0 1em;
}
```

```
table.recertItemsTable div.recertItemDecision {
 display: block;
 margin-bottom: 2px;
 margin-top: 5px;
}
/* End recertification items table styles */

.simpleLink:link, .simpleLink:visited {
 font-weight: normal;
}


.requiredInstruction {
 font-size: .8em;
 margin: 1em 0 0 1em;
 background-image: url("/itim/self/images/required_field.gif");
 background-repeat: no-repeat;
 background-position: center left;
 padding-left: 12px;
}
```

6.0 に追加された CSS の変更:

enduser_extra.css

enduser_extra.css をインポートします。

次のテキストを追加します。

```
@import "enduser_extra.css";
```

説明: セルフ・コンソールの背景色がホワイト・スモーク色に変更されました。

本文タグ・セレクターに、以下のスタイルを追加します。

```
background-color: #F5F5F5;
```

説明: バナーの背景色が明るい青に変更されました。

バナー ID セレクターの以下のスタイルを更新します。

```
background-color: black;
```

これを以下のように変更します。

```
background-color: #c8e0f8;
```

説明: ログイン画面にさまざまな変更が加えられました。

loginContainer ID セレクターを、以下のスタイルで更新します。

```
#loginContainer{
  width:619px;
  margin:20px auto;
  margin-left: auto ;
  margin-right: auto ;
    background-position:left top;
   background-repeat:no-repeat;
  background-color:#FFF;
  padding:0;
  border: solid 1px #bbbbbb;
  font-family:Arial,Verdana,Helvetica,Tahoma,sans-serif;
  font-size:12px;
```

```
  color:#555555;
  overflow: hidden;
  text-align: left;
  }
```

説明: 製品ログイン・イメージのレイアウト変更。

loginImage ID セレクターに、以下のスタイルを追加します。

```
margin-left: 40px;
margin-top: -30px;
```

説明: 製品バージョンのレイアウト変更とフォント・サイズ変更。

loginVersion ID セレクターのコンテンツを、以下のように更新します。

```
margin-left: 110px;
font-size:10px;
```

説明: ログイン・コンテンツのレイアウト変更とフォント・サイズ変更。

loginContent ID セレクターのコンテンツを、以下のように更新します。

```
margin-left: 40px ;
margin-right: 20px ;
font-size:14px;
```

説明: ログイン画面の新しいヘルプ・リンクに対するスタイルの追加。

以下のスタイルを追加します。

```
#loginToolbar {
  margin-right: 20px ;
  }
```

説明: メッセージ・ボックスに対するスタイルの追加。

以下のスタイルを追加します。

```
#messageBox {
  margin-right:80px;
  font-size:14px;
  }
```

説明: h1、h2、h3 の既存のグループ・セレクター宣言ボックスに、追加のタグ・セレクター h2i を追加します。さらに、h2i タグ・セレクターに、対応するスタイルを追加します。

以下のスタイルを追加します。

```
h2i {
  font-size:120%;
  border-bottom-style: none;
  border-bottom-width: 2px;
  margin-bottom: 0px;
  margin-left: 15px;
  }
```

説明: アンカー用のハンド・カーソルが追加されました。

疑似クラス a:LINK, a:VISITED に以下のスタイルを追加します。

```
cursor: hand;
```

説明: 新規クラス **descriptioni** が追加されました。

以下のスタイルを追加します。

```
.descriptioni {
  display: block;
    margin-bottom: 20px;
  margin-left: 15px;
  }
```

説明: テーブルに新しいスタイルが追加されました。

以下のスタイルを追加します。

```
span.tableLayout {
  display:inline-block;
  min-width:80%;
  margin : 10px 10px 10px 0 ;
  }
```

説明: テーブルの列ヘッダーの幅が更新されました。

thead th セレクターに、以下のスタイルを追加します。

```
width: auto;
```

説明: 新規クラス dataTable が追加されました。

以下のスタイルを追加します。

```
.dataTable {
  width:100%;
  margin: 0px;
  }
```

説明: 新規クラス customHeader が追加されました。

以下のスタイルを追加します。

```
customHeader {
  text-align: left;
  border-style: solid;
  background-color: #E6E6E6;
   border-width:1px 1px 1px 1px;
  border-color:#C8C8C8 #C8C8C8 #737373 #C8C8C8;
  width: auto;
  }
```

説明: 新規クラス customHeaderTable が追加されました。

以下のスタイルを追加します。

```
.customHeaderTable {
  border-top-style:hidden;
  }
```

説明: 列ヘッダーのアンカーの幅が更新されました。

thead th a:LINK, thead th a:VISITED セレクターに、以下のスタイルを追加します。

```
width: auto;
```

説明: アカウント・テーブルにスタイルが追加されました。

以下のスタイルを追加します。

```
table #global_table_accounttype {
   width: 20%;
  }

  table #global_table_userid_10 {
    width: 10%;
    }

  table #global_table_description_30 {
  width: 30%;
  }
```

説明: 新規クラス viewRequestsCustomHeaderStyle が追加されました。

以下のスタイルを追加します。

```
.viewRequestsCustomHeaderStyle{
  text-align: left;
  padding: 5px;
  vertical-align: middle;
  }
```

説明: カスタム・ヘッダー・ラベルにスタイルが追加されました。

以下のスタイルを追加します。

```
div.viewRequestsCustomHeaderStyle label{
  display: inline;
  font-weight:bold;
  }
```

説明: recertItemOwnershipType に新規スタイルが追加されました。

以下のスタイルを追加します。

```
table.recertItemsTable div.recertItemOwnershipType {
   max-width: 300px;
  font-size: 1em;
  }
```

説明: テーブル・セルにスタイルが追加されました。

以下のスタイルを追加します。

```
div.tableCellContent {
  white-space:nowrap;
  overflow:hidden;
  width:25em;
  text-overflow:ellipsis;"
  }
```

tfoot th セレクターの既存のグループ・セレクター宣言ボックスに、追加のタグ・クラス tfootTd を追加します。さらに、ラベル・セレクターの既存のグループ・セレクター宣言ボックスに、追加のタグ・クラス・ラベルを追加します。

説明: 使用されなくなった以下のスタイルが除去されました。

以下のスタイルを除去します。

```
th.reviewActivitiesCustomHeader {
  text-align: left;
  border-style: solid;
  border-width:1px 1px 1px 1px;
  background-color: #E6E6E6;
  border-color:#FFFFFF #C8C8C8 #737373 #FFFFFF;
  }

.simpleLink:link, .simpleLink:visited {
  font-weight: normal;
  }

  .label_accessibility {
   display: none;
  }

.requiredInstruction {
   font-size: .8em;
   margin: 1em 0 0 1em;
   background-image: url("/itim/self/images/required_field.gif");
   background-repeat: no-repeat;
   background-position: center left;
   padding-left: 12px;
  }
```

次のタスク

これらの変更は即時に有効になります。IBM Security Identity Manager アプリケーションを再始動する必要はありません。

ヘルプ・コンテンツの宛先変更

ヘルプ要求を独自の Web サイトにリダイレクトして、カスタム・ヘルプ・コンテンツを提供できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

セルフ・サービス・ユーザー・インターフェースに付属の標準装備のヘルプ・コンテンツを編集することはできません。ただし、ヘルプ要求を独自の Web サイトにリダイレクトして、自社サイトと外観を合わせたカスタム・ヘルプ・コンテンツを提供することはできます。

SelfServiceHelp.properties ファイルは、ヘルプ要求の送信先のベース URL を指定します。これらのファイルは *ITIM_HOME*¥data ディレクトリーにあります。

次の表に、セルフ・サービス・ヘルプに関するプロパティーとそのプロパティー説明を示します。

表 12. セルフ・サービス・ヘルプのプロパティーと説明

プロパティー	説明
helpBaseUrl	ヘルプ要求の送信先ベース URL を指定します。ブランク値は、セルフ・サービス・ユーザー・インターフェースのデフォルト URL をヘルプで表示することを示します。
ヘルプ ID マッピング: helpId = 相対ページ URL	ヘルプ・マッピング・セクションは、個別ページからの ID をヘルプ・サーバーに送信する相対 URL にマップします。

ヘルプ URL は、helpBaseUrl とロケールと relativeHelppageURL を組み合わせたものです。

例えば、以下のとおりです。

```
helpBaseUrl=http://myserver:80
locale = en_US
```

ロケールは、現行ログイン・ユーザーの SelfServiceScreenText.properties リソース・バンドルを解決することおよび関連付けられたロケールを使用することによって決定されます。

```
loginId/relativeURL = login_help_url=ui/ui_eui_login.html
```

したがって、最終的な URL は http://myserver:80/en_US/ui/ui_eui_login.html になります。

ヘルプをリダイレクトするには、以下の手順を実行します。

手順

1. *ITIM_HOME*¥data ディレクトリーにある SelfServiceHelp.properties ファイルのバックアップ・コピーを作成します。
2. SelfServiceHelp.properties ファイルの helpBaseUrl プロパティーを変更します。
3. サーバーの相対 URL を使用するよう helpId のマッピングを更新します。
4. 適切なロケールのページをサーバーに追加します。
5. WebSphere で IBM Security Identity Manager アプリケーションを再始動して、変更を有効にします。

セルフ・サービス・タスクへの直接アクセスの構成

このセクションでは、セルフ・サービス・インターフェースのタスクに対する直接 URL アクセスを構成する方法を説明します。

インターフェースの多数のページは、他の HTML ページから直接アクセスできます。この結果、会社のイントラネット・ポータルとの統合が容易になっています。

ユーザーはまず、「ログイン」ページでログインするか、シングル・サインオンによって認証される必要があります。ユーザーが、直接アクセスに対応したページにアクセスしようとすると、以下の処理が実行されます。

- ユーザーがアクセスしようとしているページが、アドミニストレーターが構成したビューによって定義されている場合は、そのページが表示されます。
- 構成されたビューに、ユーザーがアクセスしようとしているページが含まれていない場合は、要求したページではなくエラー・ページが表示されます。

注: 「**要求の承認および確認**」タスクへの直接アクセスは、構成したビューでそのタスクが有効にされていない場合でもサポートされます。また、グループ・メンバーシップによっては、複数の構成が適用されることもあります。ユーザーに適用されるビュー構成の少なくとも 1 つに、そのユーザーがアクセスしようとしているタスクが含まれている場合は、目的のページが表示されます。

次のテーブルは、直接アクセスに対応しているタスクおよび URL を示します。会社のイントラネット・ポータルからこれらのタスクおよび URL にリンクできます。

表 13. 直接アクセスのタスクおよび URL

タスク	**URL**
ログオン・ページ	http://*server_name*/itim/self
パスワードの変更	http://*server_name*/itim/self/PasswordChange.do
パスワードを忘れた場合の情報の変更	http://*server_name*/itim/self/changeForgottenPasswordInformation.do
パスワードの有効期限切れ (「ログイン」ページを迂回)	http://*server_name*/itim/self/Login/DirectExpiredPasswordChange.do?expiredUserId=*userID* **注:** このソリューションは、シングル・サインオンが有効にされておらず SelfServiceUI.properties ファイルの ui.directExpiredChangePasswordEnabled プロパティーに true が設定されている場合にのみ有効です。
アクセス権の要求	http://*server_name*/itim/self/RequestAccess.do
(特定のアクセス権を要求する) アクセス権の要求	http://*server_name*/itim/self/RequestAccess.do?accessDN=*accessDN*
アクセス権の表示	http://*server_name*/itim/self/ViewAccess.do
アクセス権の削除	http://*server_name*/itim/self/DeleteAccess.do
(特定のアクセス権を削除する) アクセス権の削除の確認	http://*server_name*/itim/self/DeleteAccess.do?accessDN=*accessDN*
要求アカウント	http://*server_name*/itim/self/RequestAccounts.do
(特定のサービスからアクセス権の要求フォームに直接アクセスする) アカウントの要求	http://*server_name*/itim/self/RequestAccounts.do?serviceDN=*serviceDN*
アカウントの表示	• http://*server_name*/itim/self/ViewAccount.do (複数アカウントの表示) • http://*server_name*/itim/self/ViewAccount.do?userID=*userID*&serviceDN=*serviceDN* (特定のサービス・アカウント)
アカウントの表示または変更	http://*server_name*/itim/self/ViewChangeAccount.do

表 13. 直接アクセスのタスクおよび URL (続き)

タスク	URL
アカウントの変更	• http://*server_name*/itim/self/ChangeAccount.do (複数アカウントの表示) • http://*server_name*/itim/self/ChangeAccount.do?userID=*userID*&serviceDN=*serviceDN* (特定のサービス・アカウント)
アカウントの削除	http://*server_name*/itim/self/DeleteAccount.do
アカウントの削除の確認	http://*server_name*/itim/self/DeleteAccount.do?userID=*userID*&serviceDN=*serviceDN* (特定のサービス・アカウント)
プロファイルの表示	http://*server_name*/itim/self/ViewProfile.do
プロファイルの変更	http://*server_name*/itim/self/ChangeProfile.do
ユーザーの要求の表示	• http://*server_name*/itim/self/ViewRequests.do (複数要求の表示) • http://*server_name*/itim/self/ViewRequests.do?request=*requestID* (特定の要求の表示)
要求の承認および確認	• http://*server_name*/itim/self/ReviewActivities.do (複数アクティビティーの表示) • http://*server_name*/itim/self/ReviewActivities.do?activity=*activityID* (特定のアクティビティーの表示)
アクティビティーの代行	http://*server_name*/itim/self/delegateActivities.do

個人検索機能のカスタマイズ

セルフ・サービス・ユーザー・インターフェースの個人検索機能をカスタマイズできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

個人検索機能は、特定の検索基準に一致した個人のみを選択するために使用できる強力な機能です。個人検索は幅広い検索属性をフィルター処理します。

属性の名前は `ui.usersearch.attr.`*attribute_name*=*attribute_name* という形式をしています。ここで *attribute_name* は、すべての個人プロファイルおよびビジネス・パートナー個人プロファイルで共通です。*attribute_name* は、そのプロファイル属性にマップする値です。例えば、`ui.usersearch.attr.cn=cn` は共通名によって検索します。

一部の単一属性は、プロファイルが異なる場合は、複数の属性にマップできます。この場合、属性名は
ui.usersearch.attr.*attribute_name=profile1.attribute_name1*,*profile2.attribute_name1*
という形式になります。

例えば、ui.usersearch.attr.telephone=Person.mobile,BPPerson.telephonenumber は、個人プロファイルの携帯電話番号とビジネス・パートナー個人プロファイルの電話番号にマップします。

属性名を変換した値が、属性による検索のボックスに表示されます。

セルフ・サービス・ユーザー・インターフェースの個人検索機能を使用可能にするには、以下の手順を実行します。

手順

1. *ITIM_HOME*¥data ディレクトリーにある SelfServiceUI.properties ファイルのバックアップ・コピーを作成します。
2. SelfServiceUI.properties ファイルの「ユーザー検索 (User Search)」構成セクションで属性を追加または除去します。
3. WebSphere で IBM Security Identity Manager アプリケーションを再始動して、変更を有効にします。

管理コンソール・ユーザー・インターフェースのカスタマイズ

このセクションでは、管理コンソール・ユーザー・インターフェースをカスタマイズする方法を説明します。

IBM Security Identity Manager 管理コンソール・ユーザー・インターフェースはカスタマイズ可能です。お客様は、自分の役割と責任にとって不可欠な管理上の識別タスクを行う柔軟性を保ちながら、会社のユーザー・インターフェースを共通の外観で統一できます。

管理コンソールのインターフェースは、2 とおりの方法で定義およびカスタマイズできます。標準装備のコンソール・フレームワークを使用する方法と、IBM Security Identity Manager に付随してインストールされるファイルを直接変更する方法です。

- 組み込みコンソール機能は、以下の通りです。
  - アクセス・コントロール項目 (ACI)
  - ビュー
- 変更可能なファイルは、以下のとおりです。
  - プロパティー・ファイル
  - イメージ・ファイル

IBM Security Identity Managerに対してカスタマイズ変更を行う前に、リカバリー用に変更可能ファイルをバックアップします。

構成ファイルと説明

構成ファイルを使用して、IBM Security Identity Manager 管理コンソール・ユーザー・インターフェースの外観を定義します。

次のテーブルに、ファイル名および IBM Security Identity Manager のカスタマイズにおけるそれらの役割をリストします。

表 14. プロパティー構成ファイルと説明

ファイル名	ファイルの説明
ui.properties	ヘッダー、フッター、およびホーム・ページの外観を制御し、タイトル、表示するページ数、および戻す検索結果数を構成します。
helpmapping.properties	管理コンソール HTML ヘルプのリダイレクトとマッピングを制御します。

管理コンソール・ユーザー・インターフェース構成ファイルのバックアップとリストア

管理コンソール・ユーザー・インターフェースのカスタマイズを開始する前に、後のリカバリー処理に備えて、IBM Security Identity Manager の構成ファイルをすべてバックアップします。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

custom という名前のディレクトリーを *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_console.war ディレクトリー内に作成し、新しいカスタマイズ・ファイルをすべてこのカスタム・ディレクトリーに保存します。

IBM Security Identity Manager を実行している各コンピューターにログインし、以下のファイルをバックアップしてください。

- *ITIM_HOME*¥data ディレクトリー:
  - ui.properties
  - helpmappings.properties

このタスクについて

プロパティー・ファイルに変更を加えた場合は、IBM Security Identity Managerアプリケーションの再始動が必要です。例えば、いずれかのプロパティー・ファイルをリカバリーするには、以下の手順を実行します。

手順

1. WebSphere 管理コンソールで、左方のフレームの「**アプリケーション**」グループをクリックしてから 「**エンタープライズ・アプリケーション**」リンクをクリックします。
2. IBM Security Identity Manager アプリケーションの横のチェック・ボックスを選択して、「**停止**」ボタンをクリックします。

3. アプリケーションが停止した後、IBM Security Identity Manager アプリケーションの横のチェック・ボックスを選択して、「**開始**」ボタンをクリックします。
4. セルフ・サービス・ユーザー・インターフェースにログインして、リカバリーが完了したことを確認します。

バナー・コンテンツのカスタマイズ

バナーをカスタマイズして、管理コンソール・ユーザー・インターフェースの外観を変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

バナー・コンテンツを追加または変更して、管理コンソール・ユーザー・インターフェースの外観を変更できます。

デフォルトのバナー・エリアは、banner.jsp という名前の JSP ファイルと ui.properties という名前のプロパティー・ファイルの 2 つのファイルに定義されています。 バナー・エリアは 4 つの部分で構成されています。

- バナー起動リンク
- バナー起動ロゴ
- バナー・ロゴ
- バナー背景イメージ

バナーをカスタマイズする場合、banner.jsp 内のコンポーネントの大きさ (幅と高さ) を調整します。カスタム・ロゴ・イメージがゆがみなく適切なサイズになるように、これらの大きさを調節します。また、バナー・フレーム全体がゆがんでいないことを確認します。

バナー起動リンクとロゴは、ui.properties ファイルを変更して変更できます。 背景イメージとバナー・ロゴを変更する場合、独自のバナーを表示するためのファイルを作成する必要があります。このファイルは HTML または JSP バナー・ファイルのいずれかにすることができます。

ui.properties ファイル内の以下のプロパティー・キーは、バナー起動リンクとバナー起動ロゴを定義します。また、バナーの背景イメージとロゴの URL も定義します。

表 15. バナー・プロパティー・キー

プロパティー・キー	デフォルト値	説明
enrole.ui.customerLogo.image	ibm_banner.gif	起動リンク・ロゴ。*WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_console.war¥ html¥images ディレクトリーにあります。イメージ・ファイルを指す URL を指定するか、このファイルを *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_console.war¥custom ディレクトリーに配置することもできます。このディレクトリーが存在しない場合は作成する必要があります。ui.properties ファイル内でパス名に接頭部 /itim/console/custom を付けます。値を指定しなかった場合は、デフォルトの ibm_banner.gif ファイルが表示されます。
enrole.ui.customerLogo.url	www.ibm.com	起動リンク URL。この値は、HTTP 接頭部を使用して指定することも、使用しないで指定することもできます。例えば、www.ibm.com または http://www.ibm.com を使用して起動リンク URL を指定できます。
ui.banner.URL	この値は、デフォルトではブランクにされており、デフォルトのバナー・エリアが表示されます。	バナー・ロゴ、背景イメージ、および起動リンクとロゴを提供する HTML ファイルまたは JSP ファイル。URL を指定するか、このファイルを *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_console.war¥custom ディレクトリーに配置します。このディレクトリーが存在しない場合は作成する必要があります。ui.properties ファイル内でパス名に接頭部 /itim/console/custom を付けます。
ui.banner.height	48	バナーの高さ (ピクセル数) を入力します。

これらのファイルを変更するには、以下の手順を実行します。

手順

1. ファイルのバックアップ・コピーを作成し、変更するファイルを一時ディレクトリーに保存します。

2. 一時ディレクトリーに保存したファイルを編集し、更新したファイルをコピーして、デプロイされた WebSphere ディレクトリーに戻します。変更を有効にするには、IBM Security Identity Manager アプリケーションを再始動する必要があります。

次のタスク

実行済みのカスタマイズが失われないために、作成したカスタム・バージョンのファイルをバックアップするようにしてください。

フッター・コンテンツのカスタマイズ

フッターをカスタマイズして、管理コンソール・ユーザー・インターフェースの外観を変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

フッター・コンテンツを追加または変更して、管理コンソール・ユーザー・インターフェースの外観を変更できます。

デフォルトのフッター・エリアは、`ui.properties` ファイルに定義されています。

`ui.properties` ファイルにある以下のプロパティー・キーで、フッターを定義し、その可視性および高さを指定します。

表 16. フッター・プロパティー・キー

プロパティー・キー	デフォルト値	説明
ui.footer.isVisible	no	フッターを表示するかどうかを指定します。デフォルトでは、フッターは使用不可です。

表 16. フッター・プロパティー・キー (続き)

プロパティー・キー	デフォルト値	説明
ui.footer.URL	この値は、デフォルトでは、ブランクにされています。	フッターを記述する HTML ファイルまたは JSP ファイルのロケーションを指定します。URL を入力することもできます。あるいは、このファイルを *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_console.war¥custom ディレクトリー (存在しない場合は要作成) に配置し、ui.properties ファイル内のパス名に接頭部 /itim/console/custom を付けることができます。
ui.footer.height	50	フッターの高さ (ピクセル数) を入力します。

これらのファイルを変更するには、以下の手順を実行します。

手順

1. ui.properties ファイルのバックアップ・コピーを作成し、そのファイルを一時ディレクトリーに保存します。
2. 一時ディレクトリーに保存したファイルを編集し、更新したファイルをコピーして、デプロイされた WebSphere ディレクトリーに戻します。変更を有効にするには、IBM Security Identity Manager アプリケーションを再始動する必要があります。

次のタスク

実行済みのカスタマイズが失われないために、作成したカスタム・バージョンのファイルをバックアップするようにしてください。

管理コンソール・ホーム・ページのカスタマイズ

カスタマイズを行って、管理コンソール・ユーザー・インターフェース内のホーム・ページを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

ホーム・ページは、ユーザーが管理コンソール・ユーザー・インターフェースにログインしたときに読み込まれるメイン・ページです。

セクション定義とタスク定義を使用して、定義済みのビューとタスクを結び付け、タスクをセクション (タスク・ページとも呼ぶ) としてグループ化します。 これらのセクション定義およびタスク定義は、*ITIM_HOME*¥data ディレクトリー内のプロパティー・ファイルに定義されています。

ホーム・ページから管理機能へのタスクの直接リンクをコーディングできます。適切な権限を持つユーザーのみに管理機能を制限するように、JSP を使用して動的 HTML を生成してください。

ホーム・ページをカスタマイズするには、以下の手順を実行します。

手順

1. *ITIM_HOME*¥data ディレクトリーにある ui.properties ファイルのバックアップ・コピーを作成します。
2. ui.properties ファイルを編集します。 ui.homepage.path キーを変更し、ファイルを保存します。 ホーム・ページに使用する HTML または JSP ファイルの URL を入力します。あるいは、このファイルを *WAS_PROFILE_HOME*¥installedApps¥*node_name*¥ITIM.ear¥itim_console.war¥custom ディレクトリー (存在しない場合は要作成) に配置し、ファイル名に接頭部 /itim/console/custom を付けます。
3. WebSphere で IBM Security Identity Manager アプリケーションを再始動して、変更を有効にします。

管理コンソール・タスクへの直接アクセス URL リンク

このセクションでは、管理コンソール・ユーザー・インターフェースにあるタスクへの直接アクセス URL リンクを示します。

次のテーブルに、直接アクセスに対応しており、ホーム・ページからリンクできる、タスクのリンクを示します。

表 17. 直接アクセスのタスクおよびリンク

タスク	URL
パスワードの変更	パスワードの変更
役割の管理	役割の管理
組織構造の管理	組織構造の管理
ユーザーの管理	ユーザーの管理
サービスの管理	サービスの管理
識別ポリシーの管理	識別ポリシーの管理

表 17. 直接アクセスのタスクおよびリンク (続き)

タスク	URL
パスワード・ポリシーの管理	パスワード・ポリシーの管理
採用ルールの管理	採用ルールの管理
再認証ポリシーの管理	再認証ポリシーの管理
プロビジョニング・ポリシーの管理	プロビジョニング・ポリシーの管理
サービス選択ポリシーの管理	サービス選択ポリシーの管理
アカウント要求ワークフローの管理	アカウント要求ワークフローの管理
アクセス権要求ワークフローの管理	アクセス権要求ワークフローの管理
グループの管理	グループの管理
アクセス・コントロール項目の管理	アクセス・コントロール項目の管理
ビューの管理	ビューの管理
セキュリティー・プロパティーの設定	セキュリティー・プロパティーの設定
パスワードを忘れた場合の設定の構成	パスワードを忘れた場合の設定の構成
要求レポート	要求レポート
サービス・レポート	サービス・レポート
監査およびセキュリティー・レポート	監査およびセキュリティー・レポート
カスタム・レポート	カスタム・レポート
レポートのプロパティー	レポートのプロパティー
複製スキーマの構成	複製スキーマの構成
レポートの設計	レポートの設計
サービス・タイプの管理	サービス・タイプの管理

表 17. 直接アクセスのタスクおよびリンク (続き)

タスク	URL
フォームの設計	フォームの設計
ワークフロー通知プロパティーの設定	 ワークフロー通知プロパティーの設定
ポスト・オフィスの構成	ポスト・オフィスの構成
エンティティーの管理	エンティティーの管理
操作の管理	 操作の管理
ライフ・サイクル・ルールの管理	ライフ・サイクル・ルールの管理
アクセス・タイプの管理	アクセス・タイプの管理
ポリシー結合動作の構成	ポリシー結合動作の構成
グローバル・ポリシー実行の構成	グローバル・ポリシー実行の構成
データのインポート	データのインポート
データのエクスポート	データのエクスポート
ユーザー別の未処理要求の表示	 ユーザー別の未処理要求の表示
ユーザー別のすべての要求の表示	ユーザー別のすべての要求の表示
サービス別の未処理要求の表示	 サービス別の未処理要求の表示
サービス別のすべての要求の表示	サービス別のすべての要求の表示
すべての要求の表示	すべての要求の表示
アクティビティーの表示	アクティビティーの表示
ユーザー別のアクティビティーの表示	ユーザー別のアクティビティーの表示
代行スケジュールの管理	代行スケジュールの管理
製品情報	製品情報
パスワードを忘れた場合の質問の定義	パスワードを忘れた場合の質問の定義

タイトル・バーのカスタマイズ

IBM Security Identity Manager 管理コンソールにログインしたときに Web ブラウザーに表示されるタイトル・バーを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

タイトル・バーをカスタマイズするには、以下の手順を実行します。

手順

1. `ui.properties` ファイルのバックアップ・コピーを作成し、そのファイルを一時ディレクトリーに保存します。
2. ui.titlebar.text プロパティーを編集して使用するタイトルを設定し、ファイルを保存します。 デフォルト値はブランクであり、「IBM Security Identity Manager」というテキストが表示されます
3. 更新したファイルをコピーして、デプロイされた WebSphere ディレクトリーに戻します。変更を有効にするには、IBM Security Identity Manager アプリケーションを再始動する必要があります。

次のタスク

実行済みのカスタマイズが失われないために、作成したカスタム・バージョンのファイルをバックアップするようにしてください。

ヘルプ・コンテンツの宛先変更

ヘルプ要求を独自の Web サイトにリダイレクトして、管理コンソール・ユーザー・インターフェース用のカスタム・ヘルプ・コンテンツを提供できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

管理コンソール・ユーザー・インターフェースに付属の標準装備のヘルプ・コンテンツを編集することはできません。ただし、ヘルプ要求を独自の Web サイトにリダイレクトして、カスタム・ヘルプ・コンテンツを提供することはできます。

`helpmappings.properties` ファイルは、ヘルプ要求の送信先のベース URL を指定します。これらのファイルは *ITIM_HOME*¥data ディレクトリーにあります。

次の表に、ヘルプに関するプロパティーとそのプロパティー説明を示します。

表 18. セルフ・サービス・ヘルプのプロパティーと説明

プロパティー	説明
helpBaseUrl	ヘルプ要求の送信先ベース URL を指定します。ブランク値は、管理コンソール・ユーザー・インターフェースのデフォルト URL をヘルプで表示することを示します。
ヘルプ ID マッピング: helpID = 相対ページ URL	ヘルプ・マッピング・セクションは、個別ページからの ID をヘルプ・サーバーに送信する相対 URL にマップします。

ヘルプ URL は、helpBaseUrl とロケールと relativeHelppageURL を組み合わせたものです。

例えば、以下のとおりです。

```
helpBaseUrl=http://myserver:80
locale = en_US
```

注: ロケールは、現行ログイン・ユーザーのブラウザー設定と現在インストールされている IBM Security Identity Manager 言語パックを突き合わせて決定されます。

```
loginID/relativeURL = login_help_url=ui/ui_eui_login.html
```

したがって、最終的な URL は http://myserver:80/en_US/ui/ui_eui_login.html になります。

ヘルプをリダイレクトするには、以下の手順を実行します。

手順

1. *ITIM_HOME*¥data ディレクトリーにある helpmappings.properties ファイルのバックアップ・コピーを作成します。
2. helpmappings.properties ファイルの helpBaseUrl プロパティーを変更します。helpID は変更しないでください。 helpID は、IBM Security Identity Manager ユーザー・インターフェース・パネルが適切なヘルプを検索するために使用する ID です。
3. サーバーの相対 URL を使用するよう helpID のマッピングを更新します。
4. 適切なロケールのページをサーバーに追加します。
5. WebSphere で **ITIM** アプリケーションを再始動して、変更を有効にします。

ページに表示する項目の数のカスタマイズ

ページに表示する項目の数を変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

次の表に、これらのページ・パラメーターのプロパティー、デフォルト値、および説明を示します。

表 19. パネルのパラメーター、デフォルト値、および説明

プロパティー	デフォルト値	説明
enrole.ui.pageSize	50	ページに表示するリスト項目の数を指定します。
enrole.ui.maxSearchResults	1000	戻される検索項目の最大数を指定します。

注: 過大な値を設定した場合は、これらの変更が、メモリー使用量に影響する場合があります。

ページ・パラメーターを変更するには、以下の手順を実行します。

手順

1. *ITIM_HOME*¥data ディレクトリーにある ui.properties ファイルのバックアップ・コピーを作成します。
2. 一時ディレクトリーに保存したファイルを編集し、更新したファイルをコピーして、上記のディレクトリーに戻します。
3. WebSphere で IBM Security Identity Manager アプリケーションを再始動して、変更を有効にします。

次のタスク

実行済みのカスタマイズが失われないために、カスタム・バージョンのファイルをバックアップするようにしてください。

第 2 章 サービス・タイプの管理

サービス・タイプ とは、同一のスキーマを共用する関連するサービスのカテゴリーです。サービス・タイプは、類似した管理対象リソースのセット全体に共通するスキーマ属性を定義します。

概説

サービス・タイプは、管理対象リソースの特定のインスタンス用のサービスを作成するためのプロファイル、またはテンプレートです。例えば、ユーザーがアクセスする必要がある Lotus® Domino® サーバーが複数ある場合に、Lotus Domino サービス・タイプを使用して、Lotus Domino サーバーごとに 1 つのサービスを作成する場合があります。サービス・タイプは、前のバージョンの IBM Security Identity Manager では、*サービス・プロファイル*と呼ばれていました。

一部のサービス・タイプは、IBM Security Identity Manager のインストール時にデフォルトでインストールされます。その他のサービス・タイプは、管理対象リソースのアダプターのサービス定義ファイルをインポートするときにインストールできます。サービス・タイプ定義は、管理対象リソースの IBM Security Identity Manager アダプターによって提供されます。IBM Security Identity Manager がサポートする管理対象リソースのタイプ (UNIX、Linux、Windows、IBM Security Access Manager など) ごとにサービス・タイプがあります。

1 つのアダプターのサービス定義ファイルに 1 つのサービス・タイプが定義されます。このファイルは、プロファイルを含んでいる Java アーカイブ (JAR) ファイルです。アダプター・プロファイル (JAR ファイル) をインポートしたときに、そのアダプターのサービス・タイプが作成されます。例えば、1 つのサービス・タイプが `WinLocalProfileJAR` ファイルに定義されています。また、IBM Security Identity Manager のインターフェースを使用してサービス・タイプを定義することもできます。

IBM Security Identity Manager では、以下のタイプのサービス・プロバイダーがサポートされます。

- Windows ローカル・アダプター、Lotus Notes® アダプターなど用の DAML
- IDI (UNIX アダプターおよび Linux アダプター用 IBM Tivoli Directory Integrator)
- 独自実装のサービス・プロバイダーを定義するためのカスタム Java クラス
- ユーザー定義の「手」作業を管理するための手動サービス・プロバイダー

デフォルト・サービス・タイプ

以下のデフォルトのサービス・タイプが IBM Security Identity Manager に付属しています。

ID フィード・サービス・タイプ

DSML Directory Services Markup Language (DSML) ID フィード・サービスは、人的資源データベースまたはファイルからアカウント・デー

タなしのユーザー・データをインポートし、IBM Security Identity Manager ディレクトリーに情報をフィードします。サービスは、ユーザーが組織のどこに配置されるかを判断するために配置ルールを使用します。このサービスは、2 つの方法のいずれか (調整またはイベント通知) で情報を受け取ることができます。このサービスは、DSML ID フィード・サービス・プロファイルに基づいています。

注: DSMLv2 は、IBM Security Identity Manager バージョン 5.0 では推奨されません。リモート・メソッド呼び出し (RMI) ベースの IDI アダプター・フレームワークを採用してください。DSMLv2 の使用は、このリリースで引き続きサポートされます。

AD AD ID フィード・サービスは、Windows Active Directory からユーザー・データをインポートします。organizationalPerson オブジェクトが、IBM Security Identity Manager にフィードされ、IBM Security Identity Managerに対してユーザーを追加または更新します。このサービスから選択されるユーザー・プロファイルは、organizationalPerson クラスから派生されたオブジェクト・クラスを持つ必要があります。

CSV CSV ID フィード・サービスは、コンマ区切り値 (CSV) ファイルからユーザー・データをインポートし、ユーザーを IBM Security Identity Manager に追加または更新します。CSV ファイルには、復帰/改行 (CR/LF) のペア (¥r¥n) で区切られたレコードのセットが含まれています。 各レコードには、コンマで区切られたフィールドのセットが含まれています。フィールドにコンマまたは CR/LF が含まれている場合は、区切り文字として二重引用符を使用してコンマをエスケープする必要があります。CSV ソース・ファイルの最初のレコードでは、その後のそれぞれのレコードで提供される属性を定義します。属性は、このサービスに選択した個人プロファイルのクラス・スキーマに基づいて有効である必要があります。

IDI データ・フィード
IDI データ・フィード・サービス・タイプは、Tivoli Directory Integrator を使用して、アカウント・データなしのユーザー・データを IBM Security Identity Manager にインポートし、外部リソースの IBM Security Identity Manager データ・ストアでアカウントを管理します。このサービスは、IDI データ・フィード・サービス・プロファイルに基づいています。

INetOrgPerson
INetOrgPerson ID フィードは、ユーザー・データを LDAP ディレクトリーからインポートします。inetOrgPerson オブジェクトはロードされ、IBM Security Identity Manager でユーザーを追加または更新します。

アカウント・サービス・タイプ

Tivoli Directory Integrator ベース
このサービス・タイプは、IBM Security Identity Manager のインストール時にオプションでインストール可能です。これらはすべて

Tivoli Directory Integrator ベースのアダプターです。それぞれが固有のサービス・タイプです。Tivoli Directory Integrator は、サービス・プロバイダーの 1 タイプです。同じタイプのサービス・プロバイダーに、複数のサービス・タイプが定義されていることがあります。

ITIM サービス

ITIM サービス・タイプは、IBM Security Identity Manager システムでのアカウントの作成に使用され、IBM Security Identity Manager Server自体を表します。これは、構成パラメーターのない標準サービスです。IBM Security Identity Manager システムへのアクセス権が必要なすべてのユーザーに IBM Security Identity Manager アカウントをプロビジョンする必要があります。

ホスト・サービス

ホスト・サービス・タイプは、サービス・プロバイダーの組織にあるホスティング・サービスに対するプロキシーであるサービスを作成するために使用されます。

ホスト・サービスは、間接的にホスティング・サービスを介して管理対象リソースのターゲットに接続します。ホスティング・サービスの構成の詳細は非表示になっており、ホスト・サービスが定義されている 2 次組織の管理者から保護されています。管理者は、特にホスティング・サービスに影響を与えずに、ホスト・サービスのポリシーを定義できます。

ホスト・サービスの主な使用法は、ビジネス・パートナー組織のユーザーが組織の内部 IT リソースに対するアカウントとアクセス権を持つことができるようにすることと、2 次組織の管理者がユーザー・アカウントに固有のサービス・ポリシーを定義できるようにすることです。

カスタム Java クラス

カスタム Java クラス・サービス・タイプでは、Java クラスを定義および実装することによって、独自のプロファイルを定義できます。

手動サービスおよびサービス・タイプ

手動サービス・タイプでは、ターゲット・リソース上のユーザー・アカウントを手動で管理します。アカウント要求は、サービス・プロバイダーに経路指定される代わりに特定のユーザーに経路指定され、手動で処理したり、IBM Security Identity Manager Server 外部の他のツールで処理したりできます。

以下の記述の 1 つ以上に該当するリソースが、ここで扱うリソースです。

- プロビジョニングを実行するために使用可能なアダプターが現在存在せず、カスタム・アダプターを開発することが不可能であるか実際的でない。
- プロビジョニング・アクティビティーの一部または全部で、必須のセットアップ処理を実行する個人が必要である。
- タスクを手動で行うことを選択する。

手動サービス・タイプおよび手動サービスのリソースの例としては、以下のリソースがあります。

- ボイス・メールのセットアップ
- 電話のセットアップ
- パーソナル・コンピューターのセットアップ
- 物理メールのセットアップ
- 社員バッジの要求

手動サービス

接続モードの使用可能化

手動サービスの作成

IBM Security Identity Manager が管理対象リソース用のアダプターを提供しない場合は、手動サービス・インスタンスを作成します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

IBM Security Identity Manager で手動サービスを作成するには、まずサービス・タイプを作成するため、手動サービスの新規スキーマ・クラスと属性を LDAP ディレクトリーへ追加します。

このタスクについて

手動サービスとは、要求を完了するために手操作による介入を必要とするタイプのサービスのことです。例えば、手動サービスはユーザーのためにボイス・メールを設定するために定義される場合があります。手動サービスによって、必要な手操作による介入を定義する作業命令アクティビティーが生成されます。

このタスクの一部としてプロビジョニング・ポリシーを作成するように選択した場合は、サービスが自動的に資格としてプロビジョニング・ポリシーに追加されます。さらに、「すべて」のメンバーシップがプロビジョニング・ポリシーに定義されます。さらに、「個人」の所有権タイプがプロビジョニング・ポリシーに定義されます。その後、サービスを作成した後に、プロビジョニング・ポリシーを編集し、メンバーシップ・タイプと所有権タイプを変更することができます。

各サービスに指定したサービス名と説明がコンソールに表示されます。したがって、ユーザーおよびアドミニストレーターが理解できる値を指定することが重要です。

手動サービス・インスタンスを作成するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。

2. 「サービスの選択」ページで、「**作成**」をクリックします。 サービスの作成ウィザードが表示されます。
3. 「サービスのタイプの選択」ページで、「**検索**」をクリックして、ビジネス単位の場所を特定します。 「ビジネス単位」ページが表示されます。
4. 「ビジネス単位」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、ビジネス単位に関する情報を入力します。
   b. 「**検索基準**」リストからビジネス・タイプを選択した後、「**検索**」をクリックします。 検索基準に一致するビジネス単位のリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。

   c. 「**ビジネス単位**」テーブルで、サービスを作成するビジネス単位を選択してから、「**OK**」をクリックします。 「サービスのタイプの選択」ページが表示され、指定したビジネス単位が「**ビジネス単位**」フィールドに表示されます。
5. 「サービスのタイプの選択」ページで、手動サービス・タイプを選択してから、「**次へ**」をクリックします。

   テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
   - 矢印をクリックして次のページに進む。
   - 表示するページの番号を入力してから「**実行**」をクリックする。
6. 「一般情報」ページで、手動サービス・インスタンスの適切な値を指定してから、「**次へ**」をクリックします。 このページの内容は、作成しているサービスのタイプによって異なります。一部のサービスの作成では、追加ステップが必要になることがあります。
7. 「参加者」ページで、手動サービスのアクティビティーを完了することに関係するユーザーを指定します。サービスがエスカレートされるまでの時間を指定します。「**次へ**」をクリックします。
8. オプション: 「メッセージ」ページで、以下の手順を実行してから、「**調整**」をクリックします。
   a. 変更するデフォルトの電子メール・メッセージを選択してから、「**変更**」をクリックします。 「メッセージの変更」ページが表示されます。
   b. 「**件名**」フィールドと「**本文**」フィールドを変更してから、「**OK**」をクリックします。
9. 「ポリシーの構成」ページで、プロビジョニング・ポリシー・オプションを選択してから、「**次へ**」または「**完了**」をクリックします。 プロビジョニング・ポリシーにより、アカウントで使用可能な所有権タイプが決まります。デフォルトのプロビジョニング・ポリシーでは、個人の所有権タイプのアカウントのみを有効にします。その他の所有権タイプは、プロビジョニング・ポリシーで資格を作成することによって追加できます。

10. オプション: 「調整」ページで「**参照**」をクリックして、調整ファイルを見つけ出してから、「**ファイルのアップロード**」をクリックして、新規調整ファイルをロードします。 また、サポート・データのみを調整するかどうかを選択することもできます。

    注: 調整ファイルでサポートされるファイル・タイプは CSV です。詳しくは、「*IBM Security Identity Manager 管理ガイド*」のトピック『サンプルのコンマ区切り値 (CSV) ファイル』を参照してください。
11. 「**完了**」をクリックします。

タスクの結果

特定のサービス・タイプの新規サービス・インスタンスが正常に作成されたことを示すメッセージが表示されます。

次のタスク

別のサービス・タスクを選択するか、「**クローズ**」をクリックします。「サービスの選択」ページが表示されたら、「**リフレッシュ**」をクリックして、「**サービス**」テーブルをリフレッシュします。新規のサービス・インスタンスが表示されます。

手動サービスの変更

手動サービス・インスタンスの情報を変更します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

IBM Security Identity Manager でサービスを変更できるようにするには、サービス・インスタンスを作成する必要があります。

手順

手動サービス・インスタンスを変更するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドに、サービスに対する検索を実行するのか、ビジネス単位に対する検索を実行するのを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。

- 矢印をクリックして次のページに進む。
- 表示するページの番号を入力してから「**実行**」をクリックする。

3. 「**サービス**」テーブルで、変更する手動サービスの横にあるチェック・ボックスを選択してから、「**変更**」をクリックします。
4. 「一般情報」ページで、サービス・インスタンスの適切な値を変更してから、「**参加者**」をクリックします。
5. 「参加者」ページで、参加者タイプ、エスカレーション時間 (日数)、またはエスカレーション参加者タイプを変更します。
6. オプション: 「メッセージ」ページで、以下の手順を実行してから、「**調整**」をクリックします。
   a. 変更する電子メール・メッセージを選択してから、「**変更**」をクリックします。 「メッセージの変更」ページが表示されます。
   b. 必要に応じて「**件名**」フィールドと「**本文**」フィールドを変更してから、「**OK**」をクリックします。
7. オプション: 「調整」ページで「**参照**」をクリックして、調整ファイルを見つけ出してから、「**ファイルのアップロード**」をクリックして、新規調整ファイルをロードします。 また、サポート・データのみを調整するかどうかを選択することもできます。

   注: 調整ファイルでサポートされるファイル・タイプは CSV です。詳しくは、「*IBM Security Identity Manager 計画*」のトピック『コンマ区切り値 (CSV) ファイルの例 (Example comma-separated value (CSV) file)』を参照してください。
8. 「**OK**」をクリックして変更を保存し、ページをクローズします。

タスクの結果

メッセージが表示され、サービス・インスタンスが正常に変更されたことが示されます。

次のタスク

別のサービス・タスクを選択するか、「**クローズ**」をクリックします。「サービスの選択」ページが表示されたら、「**リフレッシュ**」をクリックして、「**サービス**」テーブルをリフレッシュします。

グループをサポートするように手動サービス・タイプを構成

グループの割り当てをサポートし、手動サービスのグループ管理をサポートしないようにするには、サービス・タイプの手動構成でグループ・プロファイルをセットアップする必要があります。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

手動サービスに対するグループ割り当てをサポートし、グループ管理 (これには、作成、読み取り、更新、削除が含まれます) をサポートしないように手動サービス・タイプをセットアップするには、以下の手順を実行します。

手順

1. IBM Security Identity Manager の LDAP サーバーで LDAP オブジェクト・クラスとしてグループ・スキーマを定義します。
2. 手動サービスを定義します (サービスとアカウントのオブジェクト・クラスを完成させます)。 アカウント・オブジェクト・クラスには、オプションの多値属性が含まれており、グループ・メンバーシップ情報を保存するために使用されます。このサービス・タイプは、前のステップで作成されたグループ・スキーマを参照します。

   「サービス・タイプの管理」ページでは、管理者が、グループ・スキーマ・クラスとして使用する既存の LDAP オブジェクト・クラスを選択できます。新規オブジェクト・クラスを作成する場合は、まずそれを手動で作成し、直接 LDAP サーバーへロードする必要があります。

   マップされた「**グループ ID**」、「**グループ名**」、および「**グループの説明**」属性はすべて、必要に応じて、同じグループ・スキーマ属性を参照できます。同じグループ ID を使用する複数のグループは定義できません。ID は、グループごとに固有である必要があります。

   特定のサービス・タイプについて複数のグループ・スキーマを定義できます。2 番目以降のスキーマの定義は、最初の定義と同じ方法で実行されます。
3. Form Designer を使用して、サービス・タイプのサービス・フォームおよびアカウント・フォームを変更します。 このステップでは、サービス・インスタンスの作成時およびアカウントの作成時に、必要な情報を適切に表示する必要があります。
4. このプロセスで以前に作成した手動サービス・タイプを使用して、手動サービス・インスタンスを作成します。

手動サービスの調整

手動サービスに関連する調整アクティビティーを開始します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

グループをサポートするように手動サービス・タイプを構成するための手順を実行しておく必要があります。このタスクを始める前に、手動サービス・インスタンスも作成しておく必要があります。

このタスクについて

サービス・インスタンスの作成手順では、ユーザーが提供するコンマ区切り値 (CSV) ファイルを使用して手動サービスの調整を実行できます。調整によって、手動サービスに存在するアカウントとグループが IBM Security Identity Manager に取り込まれます。CSV ファイルには、グループおよびアカウントの情報が格納されます。

サービス作成時またはサービス変更時に調整ファイルを提供できます。また、CSV ファイルからグループ情報をプルする必要があるが、IBM Security Identity Manager でアカウントにタッチしないようにするときには、調整に「サポート・データのみ」オプションを使用することもできます。

手動サービスで調整を実行するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドに、サービスに対する検索を実行するのか、ビジネス単位に対する検索を実行するのを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択してから「**検索**」をクリックします。 検索基準に一致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、サービスの隣のアイコン ( ) をクリックしてサービスに対して実行できるタスクを表示してから、「**変更**」をクリックします。 実行可能なタスクは、サービスのタイプによって異なります。 「照会の選択」ページが表示されます。
4. 「調整」ページで「**参照**」をクリックして、調整ファイルを見つけ出してから、「**ファイルのアップロード**」をクリックして、新規調整ファイルをロードします。 また、サポート・データのみを調整しないかどうかを選択することもできます。
5. 「**OK**」をクリックして変更を保存し、ページをクローズします。

タスクの結果

メッセージが表示され、調整要求が正常に実行されたことが示されます。

次のタスク

調整の結果を表示するには、「**調整要求の状況の表示**」をクリックします。また、別のサービス・タスクを選択することもでき、「**クローズ**」をクリックすることもできます。「サービスの選択」ページが表示されたら、「**リフレッシュ**」をクリッ

クして、「**サービス**」テーブルをリフレッシュします。

サービス定義ファイルまたはアダプター・プロファイル

サービス定義ファイル (*アダプター・プロファイル* ともいう) は、IBM Security Identity Manager が管理できる管理対象リソースのタイプを定義します。

サービス定義ファイルは、サービス・タイプを IBM Security Identity Manager Server上に作成します。

サービス定義ファイルは、以下の情報を含む Java アーカイブ (JAR) ファイルです。

- 追加、削除、サスペンド、または復元など、サービスに対して実行できるアカウント・プロビジョニング操作の定義を含むサービス情報。
- IBM Security Identity Manager Server による管理対象リソースとの通信方法の基本インプリメンテーションを定義するサービス・プロバイダー情報。
- LDAP クラスと属性を含むスキーマ情報。
- アカウント・フォームとサービス・フォーム、および属性のラベル。ラベルは、サービスを作成するときおよびこれらのサービスに対するアカウントを要求するときのユーザー・インターフェースに表示されます。

サービス・タイプの作成

アドミニストレーターは、サービス・タイプを作成できます。例えば、作成する手動サービスのサービス・タイプを作成できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

新規サービス・タイプを定義すると、新しい LDAP 属性およびオブジェクト・クラスを定義することができます。また、既存の LDAP 属性およびオブジェクト・クラスを変更することもできます。このタスクを通じて、LDAP スキーマを変更した場合の影響を理解してください。既存の属性およびオブジェクト・クラスの構文またはスキーマを変更しないでください。新規のサービス・タイプが必要な場合は定義します。スキーマの拡張に関する制限とベスト・プラクティスについては、ディレクトリーの資料を参照してください。IBM Tivoli Directory Server バージョン 6.1 の場合は、http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd13.htm#wq78 (英語) を参照してください。

このタスクについて

手動サービスのサービス・タイプやカスタム・サービスのサービス・タイプを作成できます。

サービス・タイプを作成するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**サービス・タイプの管理**」を選択します。 「サービス・タイプの管理」ページが表示されます。
2. 「サービス・タイプの管理」ページで、「**作成**」をクリックします。 「サービス・タイプの管理」ノートブックが表示されます。
3. 「サービス・タイプの管理」ノートブックの 「一般」ページで、以下の手順を実行します。
   a. 「**サービス・タイプ名**」フィールドに、サービス・タイプの固有の名前を入力します。
   b. 「**サービス・プロバイダー**」リストから、このサービス・タイプのアカウントをプロビジョンするために IBM Security Identity Manager が使用するプロトコルを選択します。
   c. 「**サービス**」タブをクリックします。
4. 「サービス」ページで、サービス・タイプに関連付ける LDAP クラスと属性を指定してから「**アカウント**」タブをクリックします。 LDAP クラスおよび属性は、管理対象リソースが提供するアカウントによって異なります。
5. 「アカウント」ページで、アカウント・スキーマに関連付ける LDAP クラスと属性を指定してから、「**グループ**」タブまたは「**OK**」をクリックします。
6. オプション: 「グループ」ページで、以下の手順を実行します。
   a. グループをサービス・タイプに追加するには、「**追加**」をクリックします。 「グループの追加」ページが表示されます。
   b. 「グループの追加」ページで、LDAP クラスおよびスキーマ情報を指定します。 このサービス・タイプのアダプターによって、1 つのグループ・スキーマがサポートされる必要があります。
   c. 「**各種**」タブまたは「**OK**」をクリックします。
7. オプション: 「各種」ページで、以下の手順を実行します。
   a. 休止アカウントに関するレポートに、このサービス・タイプを含める場合は、このチェック・ボックスを選択します。
   b. 「**最終アクセス日付**」リストから、サービス・タイプに関連付けられているアカウント・スキーマの属性を選択してから「**OK**」をクリックします。

タスクの結果

サービス・タイプが正常に作成されたことを示すメッセージが表示されます。

次のタスク

Form Designer を使用して、新規サービス・タイプについて生成されたサービス・フォームおよびアカウント・フォームを確認するか、サービス・タイプのアカウントのデフォルトをセットアップするか、**Close**をクリックします。

ヒント: `CustomLabels.properties` ファイルに、「**サービス・タイプ名**」フィールドおよび「**説明**」フィールドの値を指定することもできます。

サービス・タイプの変更

サービス・タイプを変更して別のサービス・プロバイダーを選択することができます。また、サービス・タイプを変更して、サービス・タイプまたはアカウントの LDAP クラスまたは属性を変更することもできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

サービス・タイプが存在している必要があります。ただし、このサービス・タイプのインスタンスは存在しない必要があります。

新規サービス・タイプを定義すると、新しい LDAP 属性およびオブジェクト・クラスを定義することができます。また、既存の LDAP 属性およびオブジェクト・クラスを変更することもできます。このタスクを通じて、LDAP スキーマを変更した場合の影響を理解してください。既存の属性およびオブジェクト・クラスの構文またはスキーマを変更しないでください。新規のサービス・タイプが必要な場合は定義します。スキーマの拡張に関する制限とベスト・プラクティスについては、ディレクトリーの資料を参照してください。IBM Tivoli Directory Server バージョン 6.1 の場合は、http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd13.htm#wq78 (英語) を参照してください。

このタスクについて

変更しようとしているサービス・タイプのサービス・インスタンスが存在する場合は、サービス・タイプを変更できません。ユーザーがこのサービス・インスタンス上のアカウントで作業中である可能性があります。

サービス・タイプを変更するには、以下のステップを行います。

手順

1. ナビゲーション・ツリーから**「システムの構成」** > **「サービス・タイプの管理」**を選択します。 「サービス・タイプの管理」ページが表示されます。
2. 「サービス・タイプの管理」ページで、変更するサービス・タイプの横のチェック・ボックスを選択して、**「変更」**をクリックします。 「サービス・タイプの管理」ノートブックが表示されます。
3. 「サービス・タイプの管理」ノートブックで、希望する変更を行ってから **「OK」** をクリックします。 サービス・タイプの名前を変更することはできません。

タスクの結果

サービス・タイプが正常に変更されたことを示すメッセージが表示されます。

次のタスク

Form Designer を使用し、サービス・タイプ属性の変更と一致するようサービス・フォームおよびアカウント・フォームを必要に応じて更新するか、「**クローズ**」をクリックします。

サービス・タイプのインポート

アドミニストレーターは、サービス・タイプを作成するサービス定義ファイルをインポートできます。サービス定義ファイルは、アダプター・プロファイル・ファイルとも呼ばれ、さまざまな IBM Security Identity Manager アダプターに付属しています。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

インポートするファイルは、Javaアーカイブ (JAR) ファイルである必要があります。

このタスクについて

JAR ファイルが提供されているアダプターのサービス・タイプを作成できます。

サービス・タイプをインポートするには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**サービス・タイプの管理**」を選択します。 「サービス・タイプの管理」ページが表示されます。
2. 「サービス・タイプの管理」ページで、「**インポート**」をクリックします。「サービス・タイプのインポート」ページが表示されます。
3. 「サービス・タイプのインポート」ページで、以下の手順を実行します。
   a. 「**サービス定義ファイル**」フィールドにファイルのディレクトリー・ロケーションを入力するか、「**参照**」をクリックしてファイルを見つけます。 例えば、Active Directory を実行している Windows サーバー用の IBM Security Identity Manager アダプターをインストールする場合は、`ADProfileJAR` ファイルを見つけてインポートします。
   b. 「**OK**」をクリックして、ファイルをインポートします。

タスクの結果

サービス・タイプが正常にインポートされたことを示すメッセージが表示されます。

次のタスク

インポートは、非同期で実行されます。つまり、しばらく時間がかかる場合があります。「サービス・タイプの管理」ページで、「**リフレッシュ**」をクリックすると新規サービス・タイプが表示されます。サービス・タイプが一定時間経過しても表示されない場合、ログ・ファイルを確認し、インポートが失敗した原因を判別してください。

サービス・タイプの削除

サービス・インスタンスを持たないサービス・タイプを削除できます。例えば、企業がアプリケーションを置き換える場合に、ユーザー・レコードを新規アプリケーションにマイグレーションすることができます。その次に、廃止するサービス・タイプを削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

サービス・タイプを削除する前に、そのサービス・タイプのサービス・インスタンスをすべて除去する必要があります。

このタスクについて

サービス・タイプの削除では、LDAP クラスに対して行った変更は、サービス・タイプの削除後であっても存続します。

サービス・タイプを削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**サービス・タイプの管理**」を選択します。 「サービス・タイプの管理」ページが表示されます。
2. 「サービス・タイプの管理」ページで、削除するサービス・タイプの横のチェック・ボックスを選択して、「**削除**」をクリックします。 この列の上部にあるチェック・ボックスを選択すると、すべてのサービス・タイプが選択されます。「サービス・タイプの管理」ノートブックが表示されます。
3. 「確認」ページで「**削除**」をクリックしてサービス・タイプを削除するか、「**キャンセル**」をクリックします。

タスクの結果

サービス・タイプが正常に削除されたことを示すメッセージが表示されます。

次のタスク

サービス・タイプの管理タスクをさらに実行するか、「**クローズ**」をクリックします。

サービス・タイプに対するアカウントのデフォルトの管理

サービスまたはサービス・タイプに対するアカウント属性のデフォルト値を定義できます。

アカウントのデフォルトのタイプ

サービス・タイプのアカウントのデフォルト

サービス・タイプ・レベルでアカウントのデフォルトを定義すると、そのタイプの全サービスに適用されます。ただし、サービス・タイプのデフォルトは、サービス・レベル でアカウントのデフォルトを定義して指定変更できます。

グローバルなアカウントのデフォルト値を 1 箇所、つまり 1 つのサービス・タイプで定義できます。1 つのサービスを対象とする同じアカウントのデフォルト値を複数の場所で定義する必要はありません。この 1 つの定義により、カスタマイズの量や、作業漏れまたはエラーの発生数が減少します。

サービスのアカウントのデフォルト

これらのデフォルトは、最初はサービス・タイプのアカウントのデフォルトから継承されますが、変更を加えた時点でそのサービスにローカルなデフォルトになります。それらは、ローカルなアカウントのデフォルトになり、変更または除去できるようになります。変更 (除去を含む) は、サービス・タイプのアカウントのデフォルトに影響しません。

アカウント属性のデフォルト値を定義するオプション

基本 デフォルト値をハードコーディングできます。任意の IBM Security Identity Manager 個人クラス・オブジェクトにある属性から情報を抽出するルールを作成することもできます。そのルールを使用して、アカウント属性の値を設定できます。

拡張 IBM Security Identity Manager オブジェクトから LDAP データを取得する JavaScript をコーディングし、アカウント属性の値を設定できます。開始点として基本のアカウントのデフォルトを作成してから、生成された JavaScript を、拡張オプションを使用して編集することができます。

サービス・タイプに対するアカウントのデフォルトの追加

アカウントのデフォルトをサービス・タイプに追加します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

目的のサービス・タイプが存在している必要があります。 存在しない場合は、そのサービス・タイプのプロファイルをインポートする必要があります。

このタスクについて

属性のデフォルト値を追加できます。このサービス・タイプからサービス・インスタンスを作成したときに、サービス・タイプのアカウントのデフォルトがサービスにコピーされます。

アカウントのデフォルトをサービス・タイプに追加するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから**「システムの構成」** > **「サービス・タイプの管理」**を選択します。 「サービス・タイプの管理」ページが表示されます。
2. **「サービス・タイプ」**テーブルで、サービス・タイプの横にあるアイコン ( ) をクリックしてから**「アカウントのデフォルト」**をクリックします。 「アカウント属性の選択」ページが表示されます。
3. 「アカウント属性の選択」ページで、**「追加」**をクリックして、属性を追加します。 「デフォルトの属性の選択」ページが表示されます。
4. 「デフォルトの属性の選択」ページで、アカウント属性を選択します。以下のいずれかの選択項目をクリックします。
   - **「追加」**。選択した属性にデフォルト値を追加します。適切なフィールド (サービスのタイプに応じて異なる) に入力してから、**「OK」**をクリックします。属性のデフォルトが「デフォルトの属性の選択」ページのリストに追加されます。
   - **「追加 (拡張)」**。選択した属性のデフォルト値を指定するスクリプトを追加します。希望する JavaScript コードを**「スクリプト」**フィールドに入力してから、**「OK」**をクリックしてください。属性のデフォルトが「デフォルトの属性の選択」ページのリストに追加されます。
5. 「アカウント属性の選択」ページで、サービス・タイプに対する属性のデフォルトの追加を終了します。次に、**「OK」**をクリックして変更を保存し、ページを閉じます。

タスクの結果

サービス・タイプにアカウントのデフォルトが正常に保存されたことを示すメッセージが表示されます。

サービス・タイプに対するアカウントのデフォルトの変更

サービス・タイプのアカウントのデフォルトを変更します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

サービス・タイプのアカウントのデフォルトを変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**サービス・タイプの管理**」を選択します。 「サービス・タイプの管理」ページが表示されます。
2. 「**サービス・タイプ**」テーブルで、サービス・タイプの横にあるアイコン ( ) をクリックしてから「**アカウントのデフォルト**」をクリックします。 「アカウント属性の選択」ページが表示されます。
3. 「アカウント属性の選択」ページで、変更する属性の横のチェック・ボックスを選択してから以下のいずれかの選択項目をクリックします。
   - 「**変更**」。選択した属性のデフォルト値を変更します。サービス・タイプによって異なる、適切なフィールドに入力してから、「**OK**」をクリックしてください。「デフォルトの属性の選択」ページのリストに表示されている、属性のテンプレート値が更新されます。

     注: 現行のデフォルト値がスクリプトによって設定される属性の場合にこのオプションを選択すると、指定したテンプレート値によって既存のスクリプトが上書きされます。
   - 「**変更 (拡張)**」。選択した属性のデフォルト値を指定するスクリプトを追加または変更します。希望する JavaScript コードを「**スクリプト**」フィールドに入力してから、「**OK**」をクリックしてください。「デフォルトの属性の選択」ページのリストに表示されている、属性のテンプレート値が更新されます。
4. 「アカウント属性の選択」ページで、サービス・タイプに対する属性のデフォルトの変更を終了します。次に、「**OK**」をクリックして変更を保存し、ページを閉じます。

タスクの結果

サービス・タイプにアカウントのデフォルトが正常に保存されたことを示すメッセージが表示されます。

サービス・タイプからのアカウントのデフォルトの除去

サービス・タイプからアカウントのデフォルトを除去します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

アカウントのデフォルトをサービス・タイプから除去するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**サービス・タイプの管理**」を選択します。 「サービス・タイプの管理」ページが表示されます。
2. 「**サービス・タイプ**」テーブルで、サービス・タイプの横にあるアイコン ( ) をクリックしてから「**アカウントのデフォルト**」をクリックします。 「アカウント属性の選択」ページが表示されます。
3. 「アカウント属性の選択」ページで、除去する属性の横のチェック・ボックスを選択してから「**除去**」をクリックします。この列の上部にあるチェック・ボックスを選択すると、すべての属性が選択されます。 属性のデフォルトが「デフォルトの属性の選択」ページにあるリストから除去されます。
4. 「アカウント属性の選択」ページで、サービス・タイプからの属性の除去を終了します。次に、「**OK**」をクリックして変更を保存し、ページを閉じます。

タスクの結果

サービス・タイプからアカウントのデフォルトが正常に除去されたことを示すメッセージが表示されます。

第 3 章 アクセス・タイプの管理

アクセス・タイプは、ユーザーに示されるアクセス権の種類を分類する 1 つの方法です。「**アクセス・タイプの管理**」タスクを使用して、組織におけるアクセス権のタイプを分類してください。

以下のアクセス・タイプが IBM Security Identity Manager に組み込まれています。

- AccessRole は、IT リソース・アクセス用の役割です。
- Application は、アプリケーションに対するアクセス権です。
- SharedFolder は、共用フォルダーに対するアクセス権です。
- MailGroup は、電子メール・グループ内のメンバーシップです。

アドミニストレーターは、イントラネット Web アプリケーションに対するアクセス・タイプや Active Directory (AD) アプリケーション共用フォルダーに対するアクセス・タイプなど、追加のアクセス・タイプを作成できます。

時間が経つうちに、いくつかのアクセス権が定義されることがあります。それらを、よく使用するアクセス権に分類するか、カテゴリーを使用して使用頻度の低いアクセス権の検索効率を高めてください。

アクセス・タイプの作成

アドミニストレーターは、イントラネット Web アプリケーションに対するアクセス・タイプや Active Directory (AD) アプリケーション共用フォルダーに対するアクセス・タイプなど、追加のアクセス・タイプを作成できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

時間が経つうちに、いくつかのアクセス権が定義されることがあります。それらをよく利用するアクセス権として分類したり、使用頻度の低いアクセス権の検索にカテゴリーを用いたりすることができます。

ツリー構造内にアクセス・タイプを作成するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**アクセス・タイプの管理**」をクリックして、「アクセス・タイプの管理」ページを開きます。 「アクセス・タイプの管理」ページにデフォルトのアクセス・タイプがリストされます。

2. 「アクセス・タイプの管理」ページで、「**アクセス・タイプ**」ノードの横のアイコンをクリックします。
3. 「**タイプの作成**」をクリックして、「アクセス・タイプの作成」ページを表示します。
4. 「アクセス・タイプの作成」ページで、以下の手順を実行します。
   a. 「**アクセス・タイプ・キー**」フィールドに、キー名を入力します。例えば、「Payroll」と入力します。
   b. 「**説明**」フィールドに、アクセス・タイプについての説明を入力します。
5. 「**OK**」をクリックして、アクセス・タイプを保存します。

タスクの結果

アクセス・タイプが正常に作成されたことを示すメッセージが表示されます。「アクセス・タイプの管理」ページで、ツリー構造内に新規のアクセス・タイプが表示されます。

次のタスク

このアクセス・タイプの表示ラベルを提供するために、CustomLabels.properties リソース・バンドルを更新する必要がある場合もあります。「*IBM Security Identity Manager リファレンス・ガイド*」の『CustomLabels.properties』トピックを参照してください。

ユーザーは、この新規アクセス・タイプに対するアクセスを要求できます。

アクセス・タイプをさらに作成するか、「**クローズ**」をクリックします。

アクセス・タイプの変更

アドミニストレーターは、イントラネット Web アプリケーションに対するアクセス・タイプや Active Directory (AD) アプリケーション共用フォルダーに対するアクセス・タイプなど、アクセス・タイプを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

ツリー構造に少なくとも 1 つのアクセス・タイプを必ず作成します。67 ページの『アクセス・タイプの作成』を参照してください。

このタスクについて

選択できるノードは、ツリー構造内で選択するノードの位置またはハイパーリンクによって異なります。

ツリー構造内のアクセス・タイプを変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**アクセス・タイプの管理**」をクリックして、「アクセス・タイプの管理」ページを開きます。 「アクセス・タイプの管理」ページにデフォルトのアクセス・タイプがリストされます。
2. 「アクセス・タイプの管理」ページで、「**アクセス・タイプ**」ノードの横のアイコンをクリックして、「**変更**」をクリックします。あるいは、アクセス・タイプをクリックします。 「アクセス・タイプの変更」ページが表示されます。
3. 「アクセス・タイプの変更」ページで、「**説明**」フィールドの記述を変更します。 そのアクセス・タイプ・キーに関連付ける説明を入力できます。

   注: 「**アクセス・タイプ・キー**」フィールド値は、読み取り専用です。
4. 「**OK**」をクリックして、アクセス・タイプを保存します。

タスクの結果

アクセス・タイプが正常に変更されたことを示すメッセージが表示されます。「アクセス・タイプの管理」ページで、ツリー構造内に変更されたアクセス・タイプが表示されます。

次のタスク

ユーザーは、この新規アクセス・タイプに対するアクセスを要求できます。

アクセス・タイプをさらに変更するか、「**クローズ**」をクリックします。

アクセス・タイプの削除

アドミニストレーターは、組織で不要になったアクセス・タイプを削除できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

アクセス・タイプを削除するには、その前に、そのアクセス・タイプのアクセス定義をすべて削除する必要があります。

このタスクについて

そのアクセス・タイプのアクセス定義が存在する場合は、アクセス・タイプを削除できません。

ツリー構造内のアクセス・タイプを削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**アクセス・タイプの管理**」をクリックして、「アクセス・タイプの管理」ページを開きます。 「アクセス・タイプの管理」ページにデフォルトのアクセス・タイプがリストされます。
2. 「アクセス・タイプの管理」ページで、削除する「**アクセス・タイプ**」ノードの横のアイコンをクリックします。次に、「**削除**」をクリックして、「確認」ページを表示します。 子項目、グループの関連付け、または役割の関連付けがあるアクセス・タイプ・ノードは削除できません。アクセス・タイプを削除する前に、まず子項目、グループの関連付け、または役割の関連付けを削除する必要があります。
3. 「確認」ページで「**削除**」をクリックしてアクセス・タイプを削除するか、「**キャンセル**」をクリックします。

タスクの結果

アクセス・タイプが正常に削除されたことを示すメッセージが表示されます。「アクセス・タイプの管理」ページで、削除されたアクセス・タイプはツリー構造内にもう表示されません。

次のタスク

アクセス・タイプを作成または変更するか、アクセス・タイプをさらに削除するか、「**閉じる**」をクリックします。

第 4 章 共有アクセスの構成

必要に応じ、デプロイメントに対して共有アクセスの構成設定を指定できます。資格情報のデフォルト設定の指定、外部クレデンシャル・ボールト・サーバーの構成、サービスの固有 ID の定義、および一部の各種操作のカスタマイズが可能です。

資格情報のデフォルト設定の構成

クレデンシャル・ボールトに追加される各資格情報に対して、デフォルト設定を指定します。

このタスクについて

管理コンソールでは、ユーザー資格情報のクレデンシャル・ボールトへの追加がサポートされています。資格情報をボールトに追加するときに、資格情報の各設定に対してデフォルト値を適用できます。このタスクは、各設定にデフォルト値を定義するときに使用します。

注: 一部のデフォルト設定は、個別の資格情報レベルで上書きできますが、グローバル・レベルでしか変更できないデフォルト設定もあります。

手順

資格情報のデフォルト設定を構成するには、以下のステップを実行します。

1. ナビゲーション・ツリーから、「**共有アクセスの管理**」 > 「**資格情報のデフォルト設定の構成**」を選択します。 「資格情報のデフォルト設定の構成」ページが表示されます。
2. 「**資格情報設定**」で、以下のいずれかのオプションを選択して、アカウントのチェックイン処理とチェックアウト処理を指定します。各設定について詳しくは、オンライン・ヘルプを参照してください。

   共有 ID のチェックインおよびチェックアウト処理を要求
   ユーザーが共有資格情報を使用する前に、デフォルトでその共有資格情報をチェックアウトする必要があることを指定する場合は、このオプションを選択します。このオプションを選択するときは、以下のオプションを指定します。

   チェックイン時にパスワードを変更
   パスワードを変更する場合は、このチェック・ボックスを選択します。

   最大チェックアウト期間
   資格情報をチェックアウトできる最大時間数、最大日数、または最大週数をスケジュールします。

   チェックアウト検索で資格情報を有効にするかどうかを指定します
   チェックアウト検索で資格情報を使用できるようにするには、「**チェックアウト検索の有効化**」チェック・ボックスを選択しま

す。これを選択すると、セルフ・サービス・ユーザー・インターフェースでのチェックアウト処理でアカウントが検索されます。

セルフ・サービスで資格情報のパスワードがユーザーに表示されるかどうかを指定します

セルフ・サービス・ユーザー・インターフェースでユーザーに資格情報パスワードを表示するには、「**ユーザーにパスワードを表示**」チェック・ボックスを選択します。

チェックアウト操作

グローバルなライフサイクル操作を定義し、チェックアウト・ワークフロー拡張機能を開始する場合は、「**操作名**」フィールドに操作名を入力します。

リースの有効期限の処理

違反を通知する

チェックアウトされた有効期限切れの資格情報がシステムによって検出されたときに通知を送信する場合は、このオプションを選択します。

違反を通知してチェックイン

有効期限切れの資格情報について受信者に通知し、それらの資格情報を自動的にチェックインする処理をシステムで実行する場合は、このオプションを選択します。

通知テンプレート

システムが有効期限切れ資格情報通知を作成するときに使用する電子メール・テンプレートを表示または変更する場合は、このリンクをクリックします。

通知の送信先

リストから受信者を選択します。

期限切れリースの検査間隔

有効期限切れの資格情報のリースをシステムが検査する時間頻度をスケジュールします。

注: 入力する時間は、有効期限切れリースの検査に指定された時間以上でなければなりません。例えば、有効期限切れリースの検査間隔を 1 時間に設定しているとします。この場合、有効期限切れのリースを担当する受信者への通知の送信には、1 時間以上の間隔を設定する必要があります。

通知の最大送信間隔

有効期限切れのリースを受信者に知らせるための通知を送信する時間頻度をスケジュールします。

共有 ID のチェックインおよびチェックアウト処理を要求しない

ユーザーが共有資格情報を使用する前に、デフォルトでその共有資格情報をチェックアウトする必要がないことを指定する場合は、このオプションを選択します。

セルフ・サービスで資格情報のパスワードがユーザーに表示されるかどうかを指定します

セルフ・サービス・ユーザー・インターフェースでユーザーに資格情報パスワードを表示する場合は、「**ユーザーにパスワードを表示**」チェック・ボックスを選択します。

資格情報を共有しない

クレデンシャル・ボールトに追加される資格情報に、共有アクセス・ポリシーを通じてデフォルトでアクセスできないように指定する場合は、このオプションを選択します。

3. 「**実行**」をクリックして構成設定を保存します。
4. 「成功」ページで「**クローズ**」をクリックします。

固有 ID (eruri) 属性を含めるサービス・フォーム・テンプレートのカスタマイズ

管理対象リソースのサービス・フォーム・テンプレートを更新して、管理対象リソースへの接続に使用する固有 ID 用のフィールドが含まれるようにします。

このタスクについて

共有アクセス用に構成するサービス・タイプごとに、以下のステップを実行する必要があります。サービス、グループ、およびアカウントのデフォルト・フォームは、アダプターに基づいています。

この作業を実行するには、システム管理者でなければなりません。

手順

eruri 属性をサービス・フォーム・テンプレートに追加するために、以下のステップを実行してください。

1. ナビゲーション・ツリーから、**システムの構成**」 > 「**フォームの設計**」を選択します。 **フォームの設計** という Java アプレットが表示されます。
2. オプション: このアプレットを別のブラウザー・ウィンドウで開くには、「**別のウィンドウで起動**」をクリックします。
3. 左のペインで「**サービス**」カテゴリー・フォルダーをダブルクリックしてオブジェクト・プロファイルを表示します。
4. 左のペインで「**POSIX Linux プロファイル**」などのプロファイルをダブルクリックして、そのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
5. 「**属性リスト**」ボックスで「**eruri**」属性を選択して、「**行の追加**」  アイコンをクリックします。 「$eruri」属性がフォーム・テンプレートに追加されます。
6. 「$eruri」属性を選択して、「**編集可能テキスト・リスト**」  アイコンをクリックします。 「$eruri」属性は複数値属性です。

7. 「**プロパティー**」ボックスで、「**ラベル**」フィールドに新規ラベル名を入力します。たとえば、「固有 ID」と入力します。 ここで入力したラベル名は、このプロファイルに基づくサービスを作成または変更するときに、サービス・フォームに表示されます。たとえば、作成または変更する POSIX Linux サービスでこのラベル名が表示されます。
8. 「**フォーム・テンプレートの保存**」  アイコンをクリックして変更内容を保存し、「**OK**」をクリックします。
9. オプション: 「**フォームの設計**」 Java アプレットを別のウィンドウで開いた場合には、そのウィンドウを閉じます。
10. 「**閉じる**」をクリックして「**フォームの設計**」アプレットを閉じます。

次のタスク

POSIX Linux などのプロファイルからサービス・インスタンスを作成し、新規の「**固有 ID**」フィールドへの記入を行います。

関連タスク:

サービス固有 ID の設定

サービスの作成

外部クレデンシャル・ボールト・サーバーの構成

外部クレデンシャル・ボールト・サーバーを構成するために必要なプロパティーを指定します。

このタスクについて

外部クレデンシャル・ボールト・サーバーにクレデンシャル・ボールト・クライアントとして接続するように、IBM Security Identity Manager を構成します。外部クレデンシャル・ボールト・サーバーは、Key Management Interoperability Protocol (KMIP) サービスを提供します。

いくつかの構成ファイルの設定に値を指定する必要があります。その後、クライアントとサーバーの間の SSL 通信を構成する必要があります。

手順

外部クレデンシャル・ボールト・サーバーを構成するには、以下のステップを実行します。

1. プロパティー・ファイル *ISIM_HOME*/data/pim.properties を編集して、秘密データ・プロバイダーを登録します。 SecretDataProvider インターフェースを実装するプロバイダーの名前を指定します。

   ```
   secret.data.provider=com.ibm.itim.pim.credstore.TKLMExternalCredProvider
   ```

2. IBM Security Identity Manager とクレデンシャル・ボールト・サーバーとの間で資格情報を同期化するハンドラーを登録します。 プロパティー・ファイル *ISIM_HOME*/data/dataSynchronization.properties を編集して、資格情報オブジェクト用に DirectoryObjectSynch インターフェースを実装するハンドラー・クラスの名前を指定または置換します。以下の項目を参照してください。

```
erCredential=com.ibm.itim.dataservices.synch.CredentialSynchHandler,
com.ibm.itim.pim.credstore.CVCredentialSynchHandler
```

注: この例は、読みやすくするために複数の行に分かれています。プロパティー・ファイルでは、コンマの後にスペースを入れずに、1 つの連続する行としてこれらの値を入力してください。

3. CVClient.properties ファイルを作成します。これを任意のディレクトリーに配置します。
   a. host パラメーターを、クレデンシャル・ボールト・サーバーを実行するコンピューターの名前に設定します。
   b. port パラメーターを、クレデンシャル・ボールト・サーバーを実行するポートの番号に設定します。

表 20. CVClient.properties ファイルの例

```
protocol=ssl
host=myCVserver.mySubnet.example.com
port=19696
path=/cvsvc/kmip.html
debug=all
debug.output.file=logs/kmip/tklm_debug.log
Audit.event.outcome=success,failure
Audit.eventQueue.max=0
Audit.handler.file.name=logs/kmip/audit/tklm_audit.log
Audit.handler.file.size=10000
Audit.event.types=runtime,authorization,authorization_terminate,
resource_management,key_management
```

4. ファイル *ISIM_HOME*/data/cvserver.properties を編集します。

   KMIPConfigProperties プロパティーを、CVClient.properties ファイルを配置した場所に設定します。例:

   ```
   KMIPConfigProperties=/opt/cvserver/CVClient.properties
   ```

   cvserver.properties の他のプロパティーに値を指定する必要はありません。オプションのプロパティーについては、表 21 を参照してください。

表 21. cvserver.properties のオプションのプロパティー

プロパティー	説明
javax.net.ssl.trustStore	Secure Sockets Layer (SSL) トランザクション用のトラストストア・ファイルの名前と場所を指定します。この値は、クレデンシャル・ボールト・サーバーの構成時に生成された clientTrust ファイルに対応しています。例: `javax.net.ssl.trustStore= /opt/cvserver/trustStore.jks`
javax.net.ssl.trustStorePassword	トラストストア・ファイルにアクセスするためのパスワードを指定します。例: `javax.net.ssl.trustStorePassword=password`

表 21. cvserver.properties のオプションのプロパティー (続き)

プロパティー	説明
javax.net.ssl.keyStore	Secure Sockets Layer (SSL) トランザクション用の鍵ストア・ファイルの名前と場所を指定します。この値は、クレデンシャル・ボールト・サーバーの構成時に生成された clientStore ファイルに対応しています。例: `javax.net.ssl.keyStore=/opt/cvserver/keyStore.jks`
javax.net.ssl.keyStorePassword	鍵ストア・ファイルのパスワードを指定します。例: `javax.net.ssl.keyStorePassword=password`
javax.net.ssl.keyStoreType	`javax.net.ssl.trustStore` に指定されているトラストストアのタイプを指定します。例: `javax.net.ssl.trustStoreType=jks`

オプションのプロパティーが指定された `cvserver.properties` ファイルの例については、表 22 を参照してください。

表 22. KMIP プロパティー・ファイルの例

```
KMIPConfigProperties=/opt/cvserver/CVClient.properties
javax.net.ssl.trustStore=/newcerts/clientTrust
javax.net.ssl.trustStorePassword=myPassw0rd
javax.net.ssl.keyStore=/newcerts/clientStore
javax.net.ssl.keyStorePassword=myPassw0rd
javax.net.ssl.keyStoreType=jks
javax.net.ssl.trustStoreType=jks
```

5. クレデンシャル・ボールト・クライアントをホストするコンピューター、およびクレデンシャル・ボールト・サーバーをホストするコンピューターで、SSL を構成します。

   各コンピューター上の WebSphere Application Server サーバーが、互いに信頼し合っている必要があります。

   クレデンシャル・ボールト・クライアントがデプロイされているコンピューターで SSL を構成します。例えば、あるコンピューターに IBM Security Identity Manager サーバーがクレデンシャル・ボールト・クライアントとしてデプロイされており、別のコンピューターにクレデンシャル・ボールト・サーバーがデプロイされているとします。この例では、IBM Security Identity Manager サーバーをホストするコンピューターで、以下のステップを実行します。

   a. WebSphere Application Server 管理コンソールにログインします。
   b. 「**セキュリティー**」 > 「**SSL 証明書と鍵の管理**」 > 「**鍵ストアおよび証明書**」 > 「**NodeDefaultTrustStore**」 > 「**署名者証明書**」を選択します。
   c. 「**ポートからの取得**」をクリックします。
   d. 「**ホスト**」フィールドと「**ポート**」フィールドに、外部資格情報サーバーの情報を入力します。
   e. 「**別名**」フィールドに、別名を入力します。
   f. 「**署名者情報の取得**」をクリックして、「**OK**」をクリックします。
   g. 構成変更を保存して、WebSphere Application Server を再始動します。

6. 外部クレデンシャル・ボールト・サーバーがデプロイされているコンピューターで SSL を構成します。

   WebSphere Application Server クラスター環境では、各ノードが別々の SSL 設定の範囲になっている場合があります。このため、各ノードのトラストストアを更新する必要があります。以下のステップを各ノードで繰り返します。

   a. WebSphere Application Server 管理コンソールにログインします。
   b. 「**セキュリティー**」 > 「**SSL 証明書と鍵の管理**」 > 「**鍵ストアおよび証明書**」 > 「**NodeDefaultTrustStore**」 > 「**署名者証明書**」を選択します。
   c. 「**ポートからの取得**」をクリックします。
   d. 「**ホスト**」フィールドと「**ポート**」フィールドに、クレデンシャル・ボールト・サーバーの値を入力します。
   e. 「**別名**」フィールドに、別名を入力します。
   f. 「**署名者情報の取得**」をクリックして、「**OK**」をクリックします。
   g. *ISIM_HOME*/data/KMIPServer.properties の trustStorePath を更新します。

      KMIPServer.properties を編集して、trustStorePath の値を **NodeDefaultTrustStore** のパスと一致するように設定します。

      trustStorePath の値は、クレデンシャル・ボールト・サーバーが実行されているノードのトラストストアの値と一致している必要があります。**NodeDefaultTrustStore** の値は、通常はデフォルトのトラストストア値ですが、管理者がこの値を変更している可能性があります。必ず正しいパスを指定してください。

      クラスター環境では、各ノードにクレデンシャル・ボールト・サーバーがインストールされています。しかし、クラスター外にある IBM Security Identity Manager サーバーがデプロイメントに含まれている場合は、クラスター内の 1 つだけのノードにあるクレデンシャル・ボールト・サーバーを使用するように、その IBM Security Identity Manager サーバーを構成します。特定のノード上にあるクレデンシャル・ボールト・サーバーを使用できるようにするには、trustStorePath を **NodeDefaultTrustStore** の値と一致するように指定する必要があります。
   h. *ISIM_HOME*/data/KMIPServer.properties を編集して、クレデンシャル・ボールト・サーバーが SSL を使用できるようにします。
      1) KMIPEnableSSL=true と設定します。

         デフォルト値は false です。
      2) SSL 通信に使用するポートを設定します。例: KMIPSSLServerPort=19696

      注: 外部クレデンシャル・ボールト・サーバーをホストするコンピューターでは、KMIP SSL サーバー・ポートの値が、クレデンシャル・ボールト・クライアントをホストするコンピューターで構成した値と一致している必要があります。

      一致している必要のある値は以下のとおりです。

表 23. SSL を有効にしてポートを指定するための構成設定

コンピューター	サーバー (例)	構成ファイル	設定
1	クレデンシャル・ボールト・クライアント。例えば、クレデンシャル・ボールト・サーバーに対するクライアントとして動作する IBM Security Identity Manager サーバー。	KMIP 構成プロパティー・ファイル。ファイル *ISIM_HOME*/data/cvserver.properties は、KMIPConfigProperties の場所を指定します。例えば、以下のとおりです。 `KMIPConfigProperties= /opt/cvserver/CVClient.properties`	この例では、ファイル `CVClient.properties` でポートが以下のように指定されています。 `port=19696`
2	外部クレデンシャル・ボールト・サーバー。例えば、外部クレデンシャル・ボールト・サーバーとしてのみ動作するようにデプロイされている IBM Security Identity Manager の個別のインストール済み環境。	*ISIM_HOME*/data/KMIPServer.properties	`KMIPEnableSSL=true` `KMIPSSLServerPort=19696`

i. 構成変更を保存して、WebSphere Application Server を再始動します。

共有アクセスの拡張構成

拡張構成タスクを使用して、必要に応じて共有アクセスをカスタマイズすることで、デプロイメントのユース・ケースをサポートすることができます。

以下のトピックを参照してください。

- 『チェックアウト操作のカスタマイズ』
- 79 ページの『共有アクセスの承認と再認証』
- 80 ページの『チェックアウト・フォームのカスタマイズ』

チェックアウト操作のカスタマイズ

共有アクセス・モジュールでは、共有アカウントの同期および非同期の両方のチェックアウトがサポートされています。同期チェックアウトは、デフォルトで有効になっています。非同期チェックアウトを使用する場合は、これを有効化して構成する必要があります。

非同期チェックアウトを有効にするには、チェックアウト・ワークフロー拡張機能を開始するためのグローバルなライフサイクル操作を定義する必要があります。また、共有アクセス・モジュールのグローバル設定で、操作名を構成する必要もあります。

IBM Security Identity Manager には、この構成を完了するための方法を示すコード例が用意されています。この例は、RFI ノードを対象とするチェックアウト拡張機能を持つチェックアウト操作と、この機能を持たないチェックアウト操作を定義する方法を示しています。

詳しくは、*ISIM_HOME*¥extensions¥6.0¥examples¥workflow¥sa_checkout にある『共有アクセス: 非同期チェックアウト (Shared Access Asynchronous Checkout)』の例を参照してください。

共有アクセスの承認と再認証

資格情報をボールトに追加するためのデフォルトの操作に、承認プロセスを追加できます。また、ボールト内の資格情報を再認証するためのカスタムのワークフローも定義できます。

資格情報のボールトへの追加に対する承認

共有アクセス・モジュールでは、ボールトに資格情報を追加するときに、既存のライフサイクル操作モジュールが使用されます。デフォルトの操作である addCredentialToVault には承認が含まれていませんが、この操作をカスタマイズして、承認アクティビティーを組み込むことができます。

IBM Security Identity Manager では、単一のグローバルな操作がサポートされています。サービス、サービス・タイプ、またはアカウントが属する組織単位に関係なく、すべての資格情報がこの操作を使用します。

IBM Security Identity Manager には、承認プロセスの追加方法を示す例が用意されています。詳しくは、*ISIM_HOME*¥extensions¥6.0¥examples¥workflow¥sa_addToVault にある『共有アクセス: ボールトへの資格情報の追加に対する承認 (Shared Access Add Credential to Vault Approval)』の例を参照してください。

共有資格情報の再認証

共有アクセス・モジュールを使用して、ボールト内の資格情報を管理できます。ボールト内の資格情報を、定期的に再検証できます。資格情報の再認証は、デフォルトでは構成されていません。再認証を構成するには、アカウント・エンティティー・タイプに対してライフサイクル・ルールを定義します。このルールによって、ボールト内のアカウントがフィルターに掛けられ、スケジュールに応じて起動されるカスタムのワークフロー操作が開始されます。

IBM Security Identity Manager には、再認証の追加方法を示す例が用意されています。この例では、以下の操作を行うための方法が示されています。

- ボールト内の資格情報を再認証するためのカスタム・ワークフローの定義
- ボールト内のアカウントをフィルターに掛けるためのライフサイクル・ルールの定義
- ルールとカスタム・ワークフローの関連付け

このカスタム・ワークフロー例では、再認証の承認アクティビティーが参加者によって拒否された場合に、資格情報がボールトから削除されます。

詳しくは、例 *ISIM_HOME*¥extensions¥6.0¥examples¥workflow¥sa_recertifyCerdential を参照してください。

チェックアウト・フォームのカスタマイズ

共有アカウントのチェックアウトに使用するフォームをカスタマイズできます。チェックアウト時に入力を求める属性をさらに追加できます。このカスタマイズにより、資格情報の共有時に個人に課せられる責任が増大します。

このタスクについて

この作業を行うには、システム管理者でなければなりません。チェックアウト・フォームは、すべての共有アクセスに対してグローバルに使用されます。チェックアウト・フォームをカスタマイズすると、その変更はすべての共有アクセスのチェックアウトに影響を及ぼします。この手順を使用すると、チェックアウト・フォーム・テンプレートに属性を追加したり、属性を除去したりできます。

手順

1. 管理コンソールにログインし、「**システムの構成**」>「**フォームの設計**」を選択します。

   「フォームの設計」Java アプレットが表示されます。
2. オプション: このアプレットを別のブラウザー・ウィンドウで開くには、「**別のウィンドウで起動**」をクリックします。
3. 左ペインで「資格情報のリース」カテゴリー・フォルダーをダブルクリックして、「資格情報のリース」フォームを選択します。フォームをダブルクリックして、Form Designer で開きます。
4. 「**カスタム属性**」を選択し、「**行の追加**」アイコンをクリックして、これをフォームに追加します。
5. 適切なアイコンをクリックしてウィジェットを選択します。各ウィジェットの必要な属性を指定します。また、各属性のフォーマットと制約も指定します。
6. 前の 2 つのステップを繰り返して、すべてのカスタム属性を追加します。
7. 「**フォーム・テンプレートの保存**」アイコンをクリックして変更を保存します。「**OK**」をクリックします。
8. オプション: 「フォームの設計」Java アプレットを別のウィンドウで開いた場合は、そのウィンドウを閉じます。
9. 「**閉じる**」をクリックして「フォームの設計」アプレットを閉じます。

第 5 章 グローバル採用ポリシー

採用ポリシー は、調整時にアカウント所有者の判別のために使用されます。*グローバル採用ポリシー* は、システム全体を対象に、1 つのサービス・タイプまたはすべてのサービス・タイプについて定義されます。特定のサービスに対して採用ポリシーが定義されていない場合は、グローバル採用ポリシーをすべてのサービス・インスタンスに適用することが可能です。

デフォルトのグローバル採用ポリシーは、アカウントの「ユーザー ID」属性が IBM Security Identity Manager ユーザーの UID 属性と一致している場合に、ユーザーにアカウントを割り当てます。サービス固有の採用ポリシーは、グローバル採用ポリシーよりも優先されます。

マイグレーションの考慮事項について詳しくは、『Tivoli Identity Manager バージョン 5.1 にマイグレーションした場合の既知の問題』を参照してください。

グローバル採用ポリシーの作成

IBM Security Identity Manager Server を使用すると、パスワードを生成するためのカスタマイズ・ルールを追加できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

グローバル採用ポリシーを作成するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから、**「システムの構成」** > **「グローバル採用ポリシー」**を選択します。
2. 「グローバル採用ポリシー」ページの**「採用ポリシー」**テーブルで、**「作成」**をクリックします。
3. 「グローバル採用ポリシー」ページの「一般」 ページで、採用ポリシーの名前を入力します。 説明を追加することもできます。
4. 「サービス・タイプ」タブをクリックし、ポリシーに関連付ける個別のサービス・タイプを選択します。グローバル採用ポリシーには少なくとも 1 つのサービス・タイプを指定する必要があります。1 つのサービス・タイプに複数のグローバル採用ポリシーを関連付けることはできません。
5. 「ルール」タブをクリックして、その採用ポリシーでアカウントとユーザーを突き合わせるために使用する属性を決定するカスタム・ルールを指定します。 突き合わせを定義する場合は、**「突き合わせフィールドの追加」**をクリックして、

調整の際に一致する必要のあるアカウントとユーザー属性を選択します。ユーザー属性ドロップダウン・リストには、突き合わせを定義するときに使用できる、属性の組み合わせの一般的なものがいくつか表示されます。例えば、「名の最初の文字 + 姓」または「名 + 姓の最初の文字」などです。もっと複雑な採用ルールの場合は、「**スクリプトの提供**」を選択して、より高度なパスを選択できます。突き合わせを定義したら、関連付けられたスクリプトがスクリプト定義フィールドに取り込まれます。

重要: スクリプトを提供することを選択した場合に、Security Identity Manager Server がその JavaScript が正しいことを検査することはありません。ポリシーの定義に使用する前に JavaScript を検証してください。

6. 「**OK**」をクリックして変更を保存します。
7. 「成功」ページで「**クローズ**」をクリックします。新規グローバル採用ポリシーが「グローバル採用ポリシー」ページに表示されます。 このグローバル採用ポリシーは変更したり削除したりできます。

グローバル採用ポリシーの変更

アドミニストレーターは、サービス・タイプに定義されているグローバル採用ポリシーを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

採用ポリシーを変更した場合の効果は、次に調整を実行するときに確認できます。既存の採用ポリシーを変更しても、特定のサービスまたはサービス・タイプの既存アカウントには影響しません。変更は、既に採用されているアカウントには影響しません。新規および既存の孤立アカウントのみが、新しいポリシーに基づいて採用されます。

グローバル採用ポリシーを変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**グローバル採用ポリシー**」を選択します。
2. 「**グローバル採用ポリシー**」テーブルで、変更する採用ポリシーを見つけて選択してから、「**変更**」をクリックします。
3. 「グローバル採用ポリシー」ページで、「一般」、「サービス」、または「ルール」ページの情報を変更します。
4. 「**OK**」をクリックして変更を保存します。
5. 「成功」ページで、「**クローズ**」をクリックします。

グローバル採用ポリシーの削除

アドミニストレーターは、サービス・タイプに定義されているグローバル採用ポリシーを削除できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

既存の採用ポリシーを削除しても、個別のサービス・タイプの既存アカウントには影響しません。

グローバル採用ポリシーを削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**グローバル採用ポリシー**」を選択します。
2. 「**グローバル採用ポリシー**」テーブルで、削除する採用ポリシーを見つけ出し、選択してから、「**削除**」 をクリックします。
3. 「確認」ページで削除する採用ポリシーを確認して、「**削除**」をクリックします。
4. 「成功」ページで、「**クローズ**」をクリックします。

第 6 章 ポスト・オフィスの構成

ポスト・オフィス機能を利用すると、ユーザーが受け取る、IBM Security Identity Manager の類似したタスクに関する電子メール通知の数を削減できます。

概説

ポスト・オフィスを構成して、一定期間内に類似の通知を収集することができます。この構成では、複数の電子メールを 1 つの通知に結合し、それからユーザーに送信します。ワークフロー設計機能で、各手作業の定義の **「グループ電子メール・トピック」**フィールドを使用して類似のタスクを判別し、電子メール通知をグループ化します。

例えば、ポスト・オフィスが有効になっているとします。通知を生成する手作業で**「グループ電子メール・トピックを使用」**オプションが使用可能になっている場合、ポスト・オフィスは、それらの手作業でシステムが生成する電子メール通知を代行受信します。ポスト・オフィスは、指定された期間、その通知を保存します。この保持期間が満了すると、ポスト・オフィスは、電子メール集約テンプレートを使用して、同じ **「グループ電子メール・トピック」**値を持つすべての通知を、電子メール受信者ごとに 1 通の電子メールにまとめます。「個人」オブジェクトで指定されている、受信者の優先ロケールが使用されます。この処理により、同じ**「グループ電子メール・トピック」**値の通知に関して、1 人のユーザーが受け取る個々の電子メール・メッセージのボリュームが削減されます。

ポスト・オフィスは、手作業構成ページの**「通知」**タブにある**「グループ電子メール・トピック」**の値を使用して、どのメッセージを集約するのかを決定します。 同じ**「グループ電子メール・トピック」**値を使用して生成されたすべての通知が、指定した収集間隔で集約されます。このフィールドには任意のストリングを入力できますが、デフォルトはアクティビティー ID です。またこのフィールドには、実行結果がストリングになる場合、JavaScript や動的コンテンツ・タグも入力できます。

収集間隔の有効期限が切れ、通知が集約されるとします。指定された**「グループ電子メール・トピック」**値と電子メール・アドレスについて通知が 1 通のみである場合、そのメッセージは元の形式のまま送信されます。ポスト・オフィスの電子メール・テンプレートは適用されません。通知は元の形式で送信されますが、送信は遅れて、ポスト・オフィスの収集間隔が終了してからになります。

個々の電子メールを集約しようとしている間に、エラーが発生することがあります。その場合は、メッセージは元の形式で送信され、エラー・メッセージがログに書き込まれます。つまりこのプロセスでは、通知の送信が遅れる場合はあっても、通知が欠落することはありません。「ポスト・オフィス」ページにある**「テスト」**ボタンは、テンプレートのエラーのトラブルシューティングに有用です。

電子メール通知の例

デフォルト・テンプレートでは、次のような電子メール通知が生成されます。

```
件名:  注意を要する作業項目が 3 件あります。

本文:
注意を要する作業項目が 3 件あります。

電子メールの件名:
これは件名 1 です
これは件名 2 です
これは件名 3 です

電子メールのメッセージ本文:
これはテキスト本文 1 です
これはテキスト本文 2 です
これはテキスト本文 3 です
```

テンプレートは、有効な動的コンテンツ・タグと JavaScript コードで構成できます。さらにポスト・オフィスには、一式のカスタム動的コンテンツ・タグと JavaScript 拡張機能があります。

ポスト・オフィス電子メール・テンプレートのカスタマイズ

ポスト・オフィスを使用可能にするか使用不可にしたり、ポスト・オフィスで集約するメッセージの収集に使用する時間間隔を設定したりできます。受信者に送信される集約メッセージを生成する際に使用する電子メール・テンプレートをカスタマイズすることもできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

ポスト・オフィスを使用可能にすると、指定した時間間隔まで、すべての電子メール通知が保存されます。指定した時点になると、通知は、受信者に送信する 1 通の電子メール・メッセージに集約されます。

ポスト・オフィス電子メール・テンプレートでは、動的コンテンツを使用できます。動的コンテンツには、動的コンテンツ・メッセージ・タグと JavaScript コードが含まれます。また、動的コンテンツには、変数を他の値に置換するタグや、`CustomLabels.properties` ファイルによって変換できるプロパティーを参照するタグも含まれます。

テンプレートは、特定の「**グループ電子メール・トピック**」値およびメッセージ受信者に対してシステムが保持する通知メッセージのコレクションに適用されます。このテンプレートは必要に応じて単純にすることも複雑にすることもできます。「**グループ電子メール・トピック**」値は、ワークフロー設計機能で設定します。

ポスト・オフィスを使用可能に設定し、ポスト・オフィス集約電子メール・テンプレートを構成するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**ポスト・オフィス**」をクリックします。 「ポスト・オフィス」ページが表示されます。
2. 「ポスト・オフィス」ページで、「**ストア転送を使用可能にする**」チェック・ボックスを選択します。
3. 「**収集間隔**」フィールドに、ポスト・オフィスが保存した電子メール・メッセージを集約し受信者に送信するまでの分単位の時間間隔を入力します。 収集間隔の値は、5 から 10080 の範囲の整数である必要があります。
4. 「**件名**」フィールドに、個別の電子メール・メッセージに代えて集約メッセージとして送信される電子メール通知の件名を指定します。 件名には、プレーン・テキストと動的コンテンツ・タグを組み込めます。
5. 「**プレーン・テキスト本文**」フィールドに、集約メッセージの本文に表示されるテキストを入力します。 内容としては、プレーン・テキスト、動的コンテンツ・タグ、JavaScript コードを組み込めます。これらのコンテンツは、HTML 電子メール通知を参照しない電子メール受信者に表示されます。
6. 「**XHTML 本文**」フィールドに、電子メール通知の本文に HTML として表示されるテキストを入力します。 内容としては、プレーン・テキスト、動的コンテンツ・タグ、JavaScript コードを組み込めます。これらのコンテンツは、HTML 電子メール通知を参照する電子メール受信者に表示されます。ポスト・オフィス電子メール集約テンプレートを使用して、個々の電子メール・テンプレートの XHTML 本文を正しく集約するには、オプションの属性「escapeentities」を使用します。この属性は、ポスト・オフィス XHTML 本文テンプレートの <JS> タグにあります。この値を `false` に設定してください。詳しくは、ポスト・オフィス電子メール集約テンプレートのサンプルを参照してください。
7. 「**OK**」をクリックして変更を保存してから、「**クローズ**」 をクリックします。

タスクの結果

次の間隔満了後に、組み合わされた通知が集約され、1 通の電子メール通知として送信されます。

次のタスク

作成したポスト・オフィス電子メール集約テンプレートを、アクティビティー参加者に送信される電子メール通知の集約に使用する前に、テストします。

ポスト・オフィスの動的コンテンツ・カスタム・タグ

ポスト・オフィスは、集約メッセージ・テンプレートの作成を簡単にするために、1 セットのカスタム・タグを定義しています。集約メッセージ・テンプレートは、1 人のユーザーの 1 つの電子メール通知に、複数の電子メール通知が表示される方法を定義するためのユーザー・インターフェース・テンプレートです。

データを入手するために、次のポスト・オフィス動的コンテンツ・カスタム・タグを使用できます。

<POGetAllBodies/>

改行で区切られた元のそれぞれの通知のテキスト本文を含むストリングを戻します。例えば、以下のとおりです。

```
Identity Manager には次の ToDo 項目があります。
ここには通知本文 <POGetAllBodies/> を示します。
```

<POGetAllSubjects/>

集約電子メール通知に関連した通知からすべての件名を、改行で区切られたストリングとして戻します。例えば、以下のとおりです。

```
Identity Manager には次の ToDo 項目があります。
通知の件名。<POGetAllSubjects/>
```

<POGetEmailAddress/>

集約電子メール通知の宛先である電子メール・アドレスを、改行なしのストリングとして戻します。例えば、以下のとおりです。

```
この通知のコレクションは、<POGetEmailAddress/> に送信されたものです。
```

<POGetNumOfEmails/>

集約電子メール通知に関連した電子メールの数を、改行なしのストリングとして戻します。例えば、以下のとおりです。

```
Identity Manager には <POGetNumOfEmails/> 件の ToDO 項目があります。
```

ポスト・オフィスのラベルとメッセージのプロパティー

インターフェース・エレメントのカスタム・ラベル

ポスト・オフィス構成 GUI エレメントのラベルは、Labels.properties ファイルに含まれる以下のプロパティーを編集してカスタマイズできます。

- POST_OFFICE_CONFIG=ポスト・オフィスの構成
- POST_OFFICE_PROPERTIES_CUE=ポスト・オフィスのプロパティーの変更
- POST_OFFICE_PATH=ポスト・オフィス
- GENERAL_TAB=一般
- AGGREGATE_MESSAGE_TAB=集約メッセージ
- ENABLE_STORE_FORWARDING_LABEL=ストア転送を使用可能にする
- COLLECTION_INTERVAL_LABEL=収集間隔
- SUBJECT=件名
- TEXT_BODY=テキスト本文
- HTML_BODY=XHTML 本文
- POST_OFFICE_DONE_ALT=ポスト・オフィスのプロパティーの保存
- POST_OFFICE_CANCEL_ALT=変更内容をキャンセル

通知メッセージのカスタム・プロパティー

ポスト・オフィス通知メッセージの場合、次のプロパティーをカスタマイズできます。これらのプロパティーは、デフォルトのポスト・オフィス・テンプレート構成に組み込まれる動的コンテンツ・タグ (<RE>) のメッセージ・キーです。

- postoffice_subject=注意を要する作業項目が {0} 件あります。
- postoffice_subject_list=E メールの件名:
- postoffice_body_list=E メールのメッセージ本文:

ポスト・オフィスのテンプレート拡張機能

「ポスト・オフィス」ページで入力できる動的コンテンツおよび JavaScript コードの使用例を検討します。

件名

```
Identity Manager: 注意を要する作業項目が <POGetNumOfEmails/> 件あります。
```

プレーン・テキスト本文

```
注意を要する作業項目が <POGetNumOfEmails/> 件あります。
すべての電子メールのアドレス先: <POGetEmailAddress/>
電子メールの件名:
<POGetAllSubjects/>
電子メールの本文:
<POGetAllBodies/>
JavaScript 拡張機能を使用してフェッチされたトピック:
<JS>
    return PostOffice.getTopic();
</JS>
JavaScript 拡張機能を使用してフェッチされた受信者の電子メール・アドレス:
<JS>
    return PostOffice.getEmailAddress();
</JS>
JavaScript 拡張機能を使用してフェッチされた電子メールのテキスト本文:
<JS>
       var msgListIterator = PostOffice.getAllEmailMessages().iterator();
       var returnString = "¥n";
       while (msgListIterator.hasNext()) {
                     returnString = returnString + msgListIterator.next().getMessage() + "¥n"; }
       return returnString;
</JS>
Here is the recipient's surname taken from the Person fetched using the JavaScript extension:
<JS>
        var person = PostOffice.getPersonByEmailAddress(PostOffice.getEmailAddress());
        return "Last: " + person.getProperty("sn")[0] + "¥n";
</JS>
```

XHTML 本文

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>注意を要する作業項目が <POGetNumOfEmails/> 件あります。</title>
</head>
<body>
Identity Manager ポスト・オフィスによって <POGetNumOfEmails/> 件の通知が収集され、以下に集約されました。
これらは、注意を要する作業項目が最大 <POGetNumOfEmails/> 件
存在することを示しています。<br />
すべての通知のアドレス先: <POGetEmailAddress/><br />
<hr />
通知の件名:<br />
<POGetAllSubjects/><br />
<hr />
通知の本文: <br />
<POGetAllBodies/><br />
<hr />
    JavaScript 拡張機能を使用してフェッチされたトピック:
    <JS>
return PostOffice.getTopic();
    </JS>
    <br />
    JavaScript 拡張機能を使用してフェッチされた電子メール・アドレス:
    <JS>
return PostOffice.getEmailAddress();
    </JS>
    <br />
    JavaScript 拡張機能を使用してフェッチされた電子メールのテキスト本文:
    <JS>
var msgListIterator = PostOffice.getAllEmailMessages().iterator();
var returnString = "<br />";
while (msgListIterator.hasNext()) {
```

```
     returnString = returnString + msgListIterator.next().getMessage() + "<br />"; }
return returnString;
    </JS>
    <br />
    Here is the recipient's surname taken from the Person fetched using the JavaScript extension:
    <JS>
var person = PostOffice.getPersonByEmailAddress(PostOffice.getEmailAddress());
return "<br />Last: " + person.getProperty("sn")[0] + "<br />";
    </JS>
<hr />
直ちに次のことに注意してください。良い一日を。<br />
     IT Dept
  </body>
</html>
```

ポスト・オフィスの JavaScript 拡張機能

メール・アプリケーション・プログラミング・インターフェース (API) を使用して、メール・コンテンツ、形式、および通知の受信者をカスタマイズします。

この API を使用すると、通知要求を作成したり、通知メッセージの作成を拡張したりできます。メール API には、通知要求を行うメール・クライアント API と、通知要求をインプリメントするメール・プロバイダー API が含まれています。

メール API には、ワークフローの参加者が類似した内容の電子メール通知を複数受信しないようにする、ポスト・オフィス機能も組み込まれています。類似した電子メール・メッセージは 1 つの電子メール通知に保存されて結合されてから、ユーザーに転送されます。

ポスト・オフィス電子メール・テンプレートのテストとトラブルシューティング

アクティビティー参加者に送信する前に、作成したポスト・オフィス電子メール集約テンプレートをテストおよび検証します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

ポスト・オフィス電子メール集約テンプレートが既に構成されている必要があります。

このタスクについて

電子メール集約テンプレートをテストするには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**ポスト・オフィス**」をクリックします。
2. 「**テスト**」をクリックします。 「電子メールのテスト」ページが表示されます。

3. 「電子メールのテスト」ページで、テスト・メッセージを受信する電子メール・アドレスを指定し、「**テスト**」をクリックします。 電子メール集約テンプレートが検証され、問題がなければサンプル電子メール通知が、指定した電子メール・アドレスに送信されます。この電子メール・メッセージには、シミュレートされたシステム情報が組み込まれ、デフォルトではプロパティー・ファイルで指定されます。メッセージは、作成したポスト・オフィス電子メール・テンプレートに表示されます。
4. 「**OK**」をクリックして変更を保存してから、「**クローズ**」 をクリックします。

次のタスク

エラー・メッセージが表示された場合は、エラーに示されたフィールドのコンテンツを訂正してから、「**テスト**」を再度クリックします。

エラー・メッセージには問題が記述されており、メッセージ内でエラーが発生した場所の大体の行番号と列番号も記載されています。戻される値は、問題が存在する大体の場所を示す汎用ポインターとして機能することが目的ですが、この場所は正確な位置ではありません。集約テンプレートの XHTML 本文に、元の通知の XHTML 本文のコンテンツを直接含めることはできません。デフォルトでは、ポスト・オフィスには XHTML 本文集約テンプレートがありません。

指定した電子メール・アドレスに送信されたサンプル電子メール通知を参照します。必要に応じて、テンプレートをさらに変更し、再度テストできます。

サンプル電子メール・コンテンツの変更

テストに使用するサンプル電子メール通知のコンテンツを変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

ポスト・オフィス電子メール集約テンプレートが既に構成されている必要があります。

このタスクについて

サンプル電子メール通知のコンテンツを変更するには、以下の手順を実行します。

手順

1. `enRole.properties` ファイルを編集します。
2. 新しい値を `enrole.postoffice` に指定してから、`enRole.properties` ファイルを保存します。 `enRole.properties` は、プロパティー・ファイルの名前です。`enrole.postoffice` は、値を指定するキーの名前です。キーと値のペアは、このプロパティー・ファイルにあります。
3. アプリケーション・サーバーを再始動すると新しい値が有効になります。

タスクの結果

このタスクの結果は、作成または変更した集約テンプレートをテストしたときのみにわかります。新しいサンプル電子メール通知が集約され、テスト電子メール・アドレスに送信されます。

例

enRole.properties ファイルは、以下のデフォルト値を含んでいます。

```
############################################################
## Post Office Template Test Configuration
############################################################
# これらは、「ポスト・オフィスの構成」ページで
# 「テスト」ボタンを使用したときに使用される電子メールの内容です。
# これら 3 つの電子メールは、テンプレートが適用される内容として
# 使用されます。
enrole.postoffice.test.subject1=これは件名 1 です
enrole.postoffice.test.textbody1=これはテキスト本文 1 です
enrole.postoffice.test.xhtmlbody1=これは xhtml 本文 1 です
enrole.postoffice.test.subject2=これは件名 2 です
enrole.postoffice.test.textbody2=これはテキスト本文 2 です
enrole.postoffice.test.xhtmlbody2=これは xhtml 本文 2 です

enrole.postoffice.test.subject3=これは件名 3 です
enrole.postoffice.test.textbody3=これはテキスト本文 3 です
enrole.postoffice.test.xhtmlbody3=これは xhtml 本文 3 です
# 上記のテスト電子メールに使用するトピックです
enrole.postoffice.test.topic=topic1

# 上記のテスト電子メールに使用するロケールです
enrole.postoffice.test.locale=en_US
```

次のタスク

新しい集約テンプレートを、テスト電子メール・アドレスに送信してテストします。

ポスト・オフィスをワークフロー・アクティビティーに使用可能にする

ワークフロー設計機能を使用して、ポスト・オフィス通知をワークフロー・アクティビティーに使用可能にします。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

ワークフロー・アクティビティーが存在する必要があります。

このタスクについて

グループ電子メール・トピックが同じであるすべての電子メール通知が、テンプレートを使用して集約され、各受信者に送信されます。

ポスト・オフィスをワークフロー・アクティビティーに使用可能にするには、以下の手順を実行します。

手順

1. ワークフロー設計機能で、既存のアクティビティーをダブルクリックして、その「プロパティー」ページにアクセスします。
2. 「プロパティー」ページで、「**通知**」タブをクリックします。
3. 「**グループ電子メール・トピックを使用**」チェック・ボックスを選択します。
4. 「**グループ電子メール・トピック**」フィールドで、同種のメッセージを集約するために使用する値を入力します。
5. 「**OK**」をクリックしてワークフロー・アクティビティーを保存してから、「**OK**」 をクリックして保存後にワークフロー設計機能を終了します。

タスクの結果

ワークフロー・アクティビティーが保存されます。このワークフローが次回起動されると、この変更が有効になります。

第 7 章 フォームのカスタマイズ

IBM Security Identity Manager インターフェースに属性のフォームを作成および変更できます。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

IBM Security Identity Manager には、システム・エンティティーの作成、表示、および変更のためのデフォルトのフォームが用意されています。Form Designer は、システム管理者が、一箇所からすべてのエンティティー・フォームを、管理できるようにします。

システム管理者は、Form Designer を使用して、以下のシステム・エンティティーのフォームを、カスタマイズできます。

- アカウント
- 管理ドメイン
- ビジネス・パートナー組織
- ビジネス・パートナー個人
- 資格情報のリース
- Identity Manager ユーザー
- ロケーション
- 組織
- 組織単位
- 個人
- 役割
- サービス

各フォーム・カテゴリー・フォルダーには、システム・エンティティーを表すオブジェクト・プロファイルがあります。各オブジェクト・プロファイルはフォーム・テンプレートに関連しています。

デフォルトのフォーム・テンプレートは、エンティティーの構成から生成されます。フォーム・テンプレートには少なくとも 1 つのタブと 1 つのフォーム・エレメントを持っています。タブは、フォーム・エレメントをグループ化するコンテナーです。フォーム・エレメントは、システム・エンティティーの属性です。各タブは、グループを示している 1 つのラベルと、1 つ以上のフォーム・エレメントで構成されています。各フォーム・エレメントは、そのデータとデータの入力形式を示している 1 つのラベルで構成されています。フォーム・エレメントは、エレメントがフォーム上に表されている順番にリストされています。

フォーム・テンプレートのカスタマイズ

Form Designer アプレットを使用して、フォーム・テンプレートをオープンできます。フォーム・テンプレートには、必須フォーム・エレメント、フォーム・エレメントの編成、およびフォーム・エレメントのコントロール・タイプが表示されます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレートをオープンするには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。

タスクの結果

中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。

次のタスク

フォーム・エレメントの 1 つを右クリックして、さまざまな操作を実行できます。フォームの上部にあるアイコンにマウスオーバーすると、そのアイコンの機能に関するヒントが表示されます。

フォーム・テンプレートへのタブの追加

この説明に従って、フォーム・テンプレートにタブを追加します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレートにタブを追加するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 「**タブ**」 > 「**タブの追加**」をクリックします。 フォーム・テンプレートに新規のタブが表示されます。
4. 新規のタブに名前を付けるには、「**タブ**」 > 「**タブの名前変更**」をクリックします。
5. 新規のタブの名前を入力フィールドに入力してから、「**OK**」をクリックします。 フォーム・テンプレートに新規のタブの名前が表示されます。
6. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

フォーム・テンプレート上のタブの名前変更

この説明に従って、フォーム・テンプレート上のタブを名前変更します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレート上のタブを名前変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 「**タブ**」 > 「**タブの名前変更**」をクリックします。
4. タブの新規名を入力フィールドに入力してから、「**OK**」をクリックします。 フォーム・テンプレートにタブの新規名が表示されます。
5. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

フォーム・テンプレート上のタブの整列

以下の説明に従って、フォーム・テンプレート上のタブを整列します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレート上でタブを別の位置に移動するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 中央ペインで、移動するタブを選択します。
4. 以下のいずれかのオプションを選択します。
   - 「**タブ**」 > 「**タブを左へシフト**」をクリックして、タブを 1 つ左へ移動します。
   - 「**タブ**」 > 「**タブを右へシフト**」をクリックして、タブを 1 つ左へ移動します。
5. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

フォーム・テンプレートからのタブの削除

以下の説明に従って、フォーム・テンプレートからタブを削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

必要な属性がタブに含まれている場合は、そのタブを削除できません。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレートからタブを削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 中央ペインで、削除するタブを選択します。

4. 「**タブ**」 > 「**タブの削除**」をクリックします。 そのタブがフォーム・テンプレートから削除されます。
5. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

フォーム・テンプレートへの属性の追加

この説明に従って、フォーム・テンプレートに属性を追加します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレートに属性を追加するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 属性を追加するタブを選択します。
4. 「属性リスト」ペインで、フォームに追加する属性名をダブルクリックします。フォームに属性が追加されます。
5. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、属性の追加を続行します。

属性のプロパティーの変更

フォーム・エレメント・プロパティー・セクションは、「**フォーマット**」と「**制約**」の 2 つのタブで構成されています。「**フォーマット**」タブには、エレメントに定義されている入力コントロール・タイプに応じて、適用可能または適用不能なすべてのフォーマット・プロパティーがリストされます。同様に、「**制約**」タブには、定義されている入力コントロール・タイプに適用可能または適用不能なすべての選択可能な制約がリストされます。適用可能でないプロパティーまたは制約については、値を選択したり設定したりできません。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

単一のフィールドに対する複数のカスタム制約を、そのフィールドに入力できなくなるように組み合わせることが可能です。 Form Designer アプレットは、単一のフィールドについて無効な組み合わせが起きないように制約の競合を検査します。

規則として、1 つのフィールドで 1 つの構文制約のみを使用するようにしてください。また、1 つのフィールドについて 1 つのデータ・タイプの制約のみを使用するようにしてください。

例えば、最小値が最大値を上回っているときに、両方の制約を同じフィールドに設定した場合は競合が存在します。競合が存在する場合は、値を変更するか、いずれかの制約を除去する必要があります。

属性のプロパティーを変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 中央ペインで、プロパティーを変更する属性を選択します。 属性のプロパティーは、「**プロパティー**」ペインに表示されます。

4. 「**フォーマット**」タブで、希望する値にプロパティーを変更します。 新規のプロパティー値が表示され、変更が属性に反映されます。
5. 「**制約**」タブで、変更する制約の横のチェック・ボックスを選択します。
6. 任意の値制約タイプのパラメーターを入力します。
7. 制約タイプのリストの下部にあるフィールドにサンプル値を入力します。
8. 「**制約の検証と更新**」ボタンをクリックします。

Form Designer アプレットは、制約間で競合が存在しているかどうかを通知します。あるいは、入力した値が使用した制約において有効であり、いずれの制約にも他の制約との競合が存在しない場合は、「**パス**」したことを示すメッセージが表示されます。

9. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

属性のコントロール・タイプの変更

コントロール・タイプは、フォーム・エレメントにユーザーがデータを入力するときのインターフェースを定義します。現在サポートされているコントロール・タイプは、チェック・ボックス、日付、ドロップダウン・ボックス、編集可能テキスト・リスト、リスト・ボックス、ログイン時間、パスワード、パスワード・ポップアップ、検索コントロール、検索の一致、サブフォーム、テキスト・フィールド、テキスト域、および UMask です。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

属性のコントロール・タイプを変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。

2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 中央ペインで、コントロール・タイプを変更する属性を選択します。
4. 「**属性**」 > 「**変更先**」をクリックします。 コントロール・タイプのリストが表示されます。
5. 望ましいコントロール・タイプを選択してください。 一部のコントロール・タイプでは、エディターが表示されます。
6. コントロール・タイプ・エディターが表示された場合は、必要なパラメーターを入力し、「**OK**」をクリックします。
7. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

フォーム・テンプレート上の属性の整列

以下の説明に従って、フォーム・テンプレート上の属性を整列します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存した後、ブラウザーを閉じます。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを再度開きます。

フォーム・テンプレート上で属性を別の位置に移動するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 中央ペインで、移動する属性を選択します。

4. 以下のいずれかのオプションを選択します。
   - 「**属性**」 > 「**属性を上に移動**」をクリックして、属性を 1 つ上に移動します。
   - 「**属性**」 > 「**属性を下に移動**」をクリックして、属性を 1 つ下に移動します。
5. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

フォーム・テンプレートからの属性の削除

この説明に従って、フォーム・テンプレートから属性を削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレートから属性を削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**フォームの設計**」をクリックします。 Form Designer アプレットが表示されます。
2. 左ペインで、希望するカテゴリー・フォルダーをダブルクリックしてエンティティー・タイプのオブジェクト・プロファイルを表示します。次に、希望のオブジェクト・プロファイルをダブルクリックしてそのプロファイルのテンプレートを開きます。 中央ペインに、そのオブジェクト・プロファイルに関連したフォーム・テンプレートが表示されます。
3. 中央ペインで、削除する属性を選択します。
4. 「**属性**」 > 「**属性の削除**」をクリックします。 その属性がフォーム・テンプレートから削除されます。
5. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

サービス・インスタンスのアカウント・フォーム・テンプレートのカスタマイズ

カスタマイズされたアカウント・フォームをサービス・インスタンスから直接開くことができます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

サービス・インスタンスごとにアカウント・フォームをカスタマイズできます。サービス・インスタンス・レベルでアカウント・フォームをカスタマイズするために Form Designer アプレットを起動すると、ナビゲーション・ツリー・パネルは表示されません。このセッションは、特定のサービス・インスタンスのアカウント・フォームのカスタマイズ専用です。フォームをカスタマイズする手順は、『フォーム・テンプレートのカスタマイズ』のセクションを参照してください。

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

注: ITIM サービス・インスタンスは 1 つしかないため、実際の ITIM サービスのカスタム・フォームはサポートされていません。このアカウント・フォームは、システム・レベルで構成されます。ただし、ホスティングされた ITIM サービス・インスタンスは 1 つ以上ある可能性があるため、ホスティングされた ITIM サービス・インスタンスではカスタム・アカウント・フォームがサポートされます。

手順

フォーム・テンプレートをオープンするには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

テーブルに複数のページが含まれている場合、以下の処理を行うことができます。

- 矢印をクリックして次のページに進む。
- 表示するページの番号を入力してから「**実行**」をクリックする。

3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックしてサービスに対して実行できるタスクを表示してから、「**アカウント・フォームのカスタマイズ**」を実行します。 Form Designer アプレットが開始されます。

タスクの結果

サービス・インスタンスに関連付けられているカスタマイズされたアカウント・フォームが表示されます。サービス・インスタンスにカスタマイズされたアカウント・フォームが存在しない場合、フォーム・テンプレートが表示されます。

次のタスク

フォーム・エレメントの 1 つを右クリックして、さまざまな操作を実行できます。フォームの上部にあるアイコンにマウスオーバーすると、その機能に関するヒントが表示されます。

サービス・インスタンスのフォーム・テンプレートへのタブの追加

この説明に従って、フォーム・テンプレートにタブを追加します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

フォーム・テンプレートにタブを追加するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。

c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

テーブルに複数のページが含まれている場合、以下の処理を行うことができます。

- 矢印をクリックして次のページに進む。
- 表示するページの番号を入力してから「**実行**」をクリックする。

3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタマイズ**」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。
4. 「**タブ**」 > 「**タブの追加**」をクリックします。 フォーム・テンプレートに新規のタブが表示されます。
5. 新規のタブに名前を付けるには、「**タブ**」 > 「**タブの名前変更**」をクリックします。
6. 新規のタブの名前を入力フィールドに入力してから、「**OK**」をクリックします。 フォーム・テンプレートに新規のタブの名前が表示されます。
7. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、タブの追加を続行します。

サービス・インスタンスのフォーム・テンプレート上のタブの名前変更

この説明に従って、フォーム・テンプレート上のタブを名前変更します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

フォーム・テンプレートに対してタブの名前変更を行うには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタマイズ**」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。
4. 「**タブ**」 > 「**タブの名前変更**」をクリックします。
5. タブの新規名を入力フィールドに入力してから、「**OK**」をクリックします。 フォーム・テンプレートにタブの新規名が表示されます。
6. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、タブの名前変更を続行します。

サービス・インスタンスのフォーム・テンプレート上のタブの整列

以下の説明に従って、サービス・インスタンスのフォーム・テンプレート上のタブを整列させます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

フォーム・テンプレートに対してタブを整列させるには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタマイズ**」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。
4. 移動するタブを選択します。
5. 以下のいずれかのオプションを選択します。
   - 「**タブ**」 > 「**タブを左へシフト**」をクリックして、タブを 1 つ左へ移動します。
   - 「**タブ**」 > 「**タブを右へシフト**」をクリックして、タブを 1 つ左へ移動します。
6. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、タブの整列を続行します。

サービス・インスタンスのフォーム・テンプレートからのタブの削除

以下の説明に従って、フォーム・テンプレートからタブを削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

フォーム・テンプレートからタブを削除するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタマイズ**」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。
4. 削除するタブを選択します。
5. 「**タブ**」 > 「**タブの削除**」をクリックします。 そのタブがフォーム・テンプレートから削除されます。

6. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、タブの削除を続行します。

サービス・インスタンスのフォーム・テンプレートへの属性の追加

この説明に従って、フォーム・テンプレートに属性を追加します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

フォーム・テンプレートに属性を追加するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、サービスの横のアイコン (▸) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタ**

マイズ」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。

4. 属性を追加するタブを選択します。
5. 「属性リスト」ペインで、フォームに追加する属性名をダブルクリックします。フォームに属性が追加されます。
6. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、属性の追加を続行します。

属性のプロパティーの変更

フォーム・エレメント・プロパティー・セクションは、「**フォーマット**」と「**制約**」の 2 つのタブで構成されています。「**フォーマット**」タブには、エレメントに定義されている入力コントロール・タイプに応じて、適用可能または適用不能なすべてのフォーマット・プロパティーがリストされます。同様に、「**制約**」タブには、定義されている入力コントロール・タイプに適用可能または適用不能なすべての選択可能な制約がリストされます。適用可能でないプロパティーまたは制約については、値を選択したり設定したりできません。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

属性のプロパティーを変更するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。

c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。

d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

テーブルに複数のページが含まれている場合、以下の処理を行うことができます。

- 矢印をクリックして次のページに進む。
- 表示するページの番号を入力してから「**実行**」をクリックする。

3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタマイズ**」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。
4. プロパティーを変更する属性を選択します。 属性のプロパティーは、「**プロパティー**」ペインに表示されます。
5. 「**フォーマット**」タブで、希望する値にプロパティーを変更します。 新規のプロパティー値が表示され、変更が属性に反映されます。
6. 「**制約**」タブで、変更する制約の横のチェック・ボックスを選択します。
7. 任意の値制約タイプのパラメーターを入力します。
8. 制約タイプのリストの下部にあるフィールドにサンプル値を入力します。
9. 「**制約の検証と更新**」ボタンをクリックします。

Form Designer アプレットは、制約間で競合が存在しているかどうかを通知します。あるいは、入力した値が使用した制約において有効であり、いずれの制約にも他の制約との競合が存在しない場合は、「**パス**」したことを示すメッセージが表示されます。

10. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、属性の変更を続行します。

属性のコントロール・タイプの変更

コントロール・タイプは、フォーム・エレメントにユーザーがデータを入力するときのインターフェースを定義します。現在サポートされているコントロール・タイプは、チェック・ボックス、日付、ドロップダウン・ボックス、編集可能テキスト・リスト、リスト・ボックス、ログイン時間、パスワード、パスワード・ポップアップ、検索コントロール、検索の一致、サブフォーム、テキスト域、テキスト・フィールド、および UMask です。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

属性のコントロール・タイプを変更するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタマイズ**」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。
4. コントロール・タイプを変更する属性を選択します。
5. 「**属性**」 > 「**変更先**」をクリックします。 コントロール・タイプのリストが表示されます。
6. コントロール・タイプを選択してください。 一部のコントロール・タイプでは、エディターが表示されます。
7. コントロール・タイプ・エディターが表示された場合は、パラメーターを入力し、「**OK**」をクリックします。

8. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、属性のコントロール・タイプの変更を続行します。

サービス・インスタンスのフォーム・テンプレート上の属性の整列

以下の説明に従って、フォーム・テンプレート上の属性を整列します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

フォーム・テンプレート上で属性を別の位置に移動するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、サービスの横のアイコン (▸) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタ**

マイズ」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。

4. 移動する属性を選択します。
5. 以下のいずれかのオプションを選択します。
   - 「**属性**」 > 「**属性を上に移動**」をクリックして、属性を 1 つ上に移動します。
   - 「**属性**」 > 「**属性を下に移動**」をクリックして、属性を 1 つ下に移動します。
6. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、属性の整列を続行します。

サービス・インスタンスのフォーム・テンプレートからの属性の削除

この説明に従って、フォーム・テンプレートから属性を削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

手順

フォーム・テンプレートから属性を削除するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。

d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

テーブルに複数のページが含まれている場合、以下の処理を行うことができます。

- 矢印をクリックして次のページに進む。
- 表示するページの番号を入力してから「**実行**」をクリックする。

3. 「**サービス**」テーブルで、サービスの横のアイコン (▸) をクリックして、サービスに対して実行できるタスクを表示します。「**アカウント・フォームのカスタマイズ**」をクリックします。 Form Designer アプレットが開始されます。サービス・インスタンスに関連付けられているフォーム・テンプレートが表示されます。
4. 中央ペインで、削除する属性を選択します。
5. 「**属性**」 > 「**属性の削除**」をクリックします。 その属性がフォーム・テンプレートから削除されます。
6. 「**フォーム**」 > 「**フォーム・テンプレートの保存**」をクリックし、フォーム・テンプレートが正常に保存されたことを示すメッセージが表示されたら「**OK**」をクリックします。

次のタスク

必要に応じて、属性の削除を続行します。

サービス・インスタンスからのカスタマイズされたフォーム・テンプレートの削除

カスタマイズされたアカウント・フォーム・テンプレートをサービス・インスタンスから削除して、システム・アカウント・フォームを復元することができます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

手順

カスタマイズされたアカウント・フォーム・テンプレートを削除するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。

c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。

d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

テーブルに複数のページが含まれている場合、以下の処理を行うことができます。

- 矢印をクリックして次のページに進む。
- 表示するページの番号を入力してから「**実行**」をクリックする。

3. 「**サービス**」テーブルで、サービスの横のアイコン ( ) をクリックして、サービスに対して実行できるタスクを表示します。「**カスタム・アカウント・フォームの削除 (Delete Custom Account Form)**」 をクリックします。 確認ページが表示されます。

4.

- 「**削除**」をクリックして、カスタマイズされたフォームをサービス・インスタンスから削除します。
- 「**キャンセル**」をクリックして、カスタマイズされたフォームを削除せずに、「サービスの選択」ページに戻ります。

アカウント・フォームが正常に削除されたかどうかを示すメッセージが表示されます。

5. 「**閉じる**」をクリックして、「サービスの選択」ページに戻ります。

次のタスク

追加のサービス・アクションを実行します。

フォーム・テンプレートのリセット

フォーム・テンプレートに変更を保存する前に、フォーム・テンプレートを元の構成にリセットできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

この機能にアクセスできるのは、アドミニストレーター・グループのメンバーである個人に限られます。

このタスクについて

Form Designer Java アプレットは、開始後に自動的にクローズされてメモリーから消去されるわけではありません。フォーム・テンプレートへの変更を完了して保存します。ブラウザーまたはシステム・パフォーマンスの問題が見つかった場合は、新規の手順を始める前に、ブラウザーを閉じて再度開きます。

フォーム・テンプレートを元の構成にリセットするには、以下の手順を実行します。

手順

1. Form Designer アプレットで、「**フォーム**」 > 「**フォーム・テンプレートのリセット**」をクリックします。
2. フォーム・テンプレートに対する変更が失われることを示すプロンプトが出されたら「**はい**」をクリックします。

Form Designer インターフェース

フォーム・テンプレート、タブ、および属性に対してアクションを実行することによってカスタム・フォームを設計するには、Form Designer アプレットの作業域を使用します。

Form Designer インターフェースには、以下に示す作業域があります。

メニューおよびツールバー・ボタン

フォーム・テンプレート、タブ、および属性に対してアクションを実行する場合は、メニュー・バーおよびツールバー・ボタンを使用します。ツールバー・ボタンの上にマウス・カーソルを置くと、ツールバー・ボタンの機能が表示されます。以下のメニュー項目およびツールバー・ボタンを使用できます。

表 24. Form Designer アプレットのメニューおよびツールバー・ボタン

メニュー・バー	メニュー項目	ツールバー・ボタン	アクション
フォーム・テンプレートを開く場合、保存する場合、またはフォーム・テンプレートを前回保存した設計に戻す場合は、「**フォーム**」をクリックします。	**フォーム・テンプレートのオープン**		フォーム・カテゴリー・フォルダーで選択したフォーム・テンプレートを開きます。
	フォーム・テンプレートの保存		現在開いているフォーム・テンプレートを保存します。
	フォーム・テンプレートのリセット	なし	フォーム・テンプレートを前回保存した設計に戻します。

表 24. *Form Designer* アプレットのメニューおよびツールバー・ボタン (続き)

メニュー・バー	メニュー項目	ツールバー・ボタン	アクション
タブの追加、名前変更、または削除を行うか、またはタブをインターフェース内で左から右へシフトするには、「**タブ**」をクリックします。 タブは、Form Designer アプレットの「テンプレートの属性」作業域に表示されます。 Form Designer のタブ名は、IBM Security Identity Manager インターフェースで作成されるノートブック・フォームのタブ名に対応します。	**タブの追加**		フォーム・エレメントをグループ化するためのコンテナーを追加します。
	タブの名前変更	なし	既存のタブ・コンテナーの名前を変更します。
	タブを左へシフト		既存のタブ・コンテナーを左へシフトします。
	タブを右へシフト		既存のタブ・コンテナーを右へシフトします。
	タブの削除		フォーム・テンプレートから既存のタブを削除します。
属性の編集または削除を行う場合、インターフェース内で属性を上下に移動する場合、または属性のコントロール・タイプを変更する場合は、「**属性**」をクリックします。 属性は、Form Designer アプレットの「テンプレートの属性」作業域に表示されます。	**属性の編集**	なし	属性を編集して構成します。
	属性の削除		フォーム・テンプレートから属性を削除します。
	属性を上に移動		フォーム・テンプレートの属性リスト内で属性の位置を 1 スペース分上に移動します。
	属性を下に移動		フォーム・テンプレートの属性リスト内で属性の位置を 1 スペース分下に移動します。
	変更先	なし	選択されている属性のコントロール・タイプを新規に選択したコントロール・タイプに変更します。

表 24. *Form Designer* アプレットのメニューおよびツールバー・ボタン (続き)

メニュー・バー	メニュー項目	ツールバー・ボタン	アクション
浮動作業域や、フォーム・テンプレートのソース表示など、さまざまなインターフェース表示オプションを選択するには、「**表示**」をクリックします。	**浮動属性リスト**		属性リストを Form Designer から浮動ポップアップ・ウィンドウに移動します。
	浮動プロパティー		プロパティー・リストを Form Designer から浮動ポップアップ・ウィンドウに移動します。
	ソースの表示		フォーム・テンプレートの XML ソースを表示しているポップアップ・ウィンドウを開きます。
Form Designer アプレットのインターフェース・テーマを選択するには、**Menu.theme** をクリックします。	**デフォルト・テーマ**	なし	デフォルトのメニュー・テーマを Form Designer インターフェースに適用。
	ハイ・コントラスト、大きなフォントのテーマ	なし	大きなフォントおよびハイ・コントラスト色を Form Designer インターフェースに適用。
	ハイ・コントラストのテーマ	なし	ハイ・コントラスト色を Form Designer インターフェースに適用。

カテゴリー

Form Designer の左側のペインを使用して、カテゴリー (「アカウント」、「組織」、「サービス」など) を選択します。各フォーム・カテゴリーは、システム・エンティティーを表すオブジェクト・プロファイルに関連付けられます。各オブジェクト・プロファイルはフォーム・テンプレートに関連しています。

カテゴリー・フォルダーをダブルクリックすると、そのカテゴリーで使用できるフォーム・テンプレートのリストを展開できます。フォーム・テンプレートのリストを読み込むには、ある程度の時間がかかる場合があります。一部のカテゴリーのフォーム・テンプレートのリストは、どのサービス・タイプが存在するかによって異なります。

フォーム・テンプレートを開くには、そのテンプレートをダブルクリックします。

テンプレートの属性

Form Designer の中央のペインは、選択したフォーム・テンプレートのアクティブな属性を表示および変更するために使用します。属性を右クリックしてその属性で使用可能なアクションを表示します。

例えば、「サービス」フォーム・テンプレートには、$servicename 属性があります。属性に関連したコントロール・タイプを変更するには、属性を右クリックし、リストで「**変更先**」をクリックします。

属性リスト

このリストは、選択したオブジェクトの属性のうち、現在フォームに含まれていない属性をすべて表示するために使用します。このリストは、昇順と降順のどちらでもソートできます。また、このリストからアクティブなテンプレート属性のリストへ属性を追加することもできます。例えば、「組織」オブジェクトには、アクティブなテンプレート属性のリストに追加できる追加の属性 ($postalcode など) があります。

プロパティー

「**フォーマット**」タブおよび「**制約**」タブがあります。これらのタブでは、特定の属性のデータ・タイプやその他のパラメーターを指定します。例えば、$servicename 属性のデータ・タイプはディレクトリー・ストリングであり、この属性は必須の属性です。

Form Designer で使用されるコントロール・タイプ

ユーザーが属性の値を入力する方法を指定するには、Form Designer アプレットでコントロール・タイプを使用します。

チェック・ボックス

単一のチェック・ボックスをデータ収集フィールドとして割り当てます。このコントロール・タイプは通常、その性質上ブール値になる属性に使用されます。

日付

ユーザーが希望の日付を選択できるカレンダー・ポップアップ・ウィンドウを表示します。このコントロール・タイプには、日付を構成する場合に使用できる追加の属性があります。

このコントロール・タイプを Form Designer アプレットで選択すると、「日付エディター」ページが表示されます。このエディターのフィールドを使用すると、コントロール・タイプを構成できます。「日付エディター」には次のフィールドが含まれています。

日付入力タイプ

カレンダー・ポップアップ・ウィンドウの日付入力のタイプを選択します。

デフォルト

カレンダー・ポップアップ・ウィンドウと「**なし**」チェック・ボックスを表示します。ユーザーがこのチェック・ボックスを選択すると、この属性値の有効期限が切れることはなくなります。

代替日付

「**なし**」チェック・ボックスのないカレンダー・ポップアップ・ウィンドウを表示します。ある時点で属性値の有効期限が切れるようにする必要がある場合は、このタイプを使用します。

時刻の表示

時刻の表示および指定に使用するポップアップ・ウィンドウを組み込む場合は、このチェック・ボックスを選択します。

ドロップダウン・ボックス

属性のリストを作成します。 以下のいずれかのオプションを使用して、リスト内に入れる属性を取り込む必要があります。

カスタム値

作成されるフォームのリストに表示される情報を制限します。 このオプションを選択すると、「エディターの選択」ページが表示されます。このエディターのフィールドを使用すると、コントロール・タイプを構成できます。「エディターの選択」には、以下のフィールドとツールバー・ボタンがあります。

行数 リストに組み込む行の数を入力して、「**実行**」を押します。このフィールドを使用して、リスト内の行の数を指定します。元のリストの行数が入力した数より多い場合、余分な行は削除されます。

データ値

データ値を入力します。

表示値 リストに表示する表示値を入力します。

ブランク行を使用

リストに空の項目を挿入するには、このチェック・ボックスを選択します。

行の追加

リストに表示する行を追加する場合にクリックします。

行の削除

リストから行を削除する場合にクリックします。

表示値をデータ値として使用

クリックして、「**表示値**」列に入力したのと同じ値を「**データ値**」列に使用します。

索引をデータ値として使用

クリックして、「**データ値**」列の索引と同じ値を使用します。

検索フィルター

ボックスにデータを取り込む場合の情報の収集元にする範囲を広げることができます。「LDAP 検索フィルター」を使用すると、検索コントロールを使用して属性に値が割り当てられます。このオプシ

ョンを選択すると、「検索フィルター・エディター」ページが表示されます。このエディターのフィールドを使用すると、コントロール・タイプを構成できます。「検索フィルター・エディター」には次のフィールドが含まれています。

検索ベース
検索の有効範囲を以下のオプションから選択します。

「**org**」を選択すると、組織ツリーの中の、選択したコンテナーの組織が検索されます。

「**コンテキスト**」を選択すると、組織ツリーの中の、選択した組織単位が検索されます。

オブジェクト・クラス
検索対象となる LDAP クラスの名前 (erNTGlobalGroup など) を入力します。作成されるフォームのグループ・フィールドの値は、erroles にする必要があります。

属性 検索対象となる属性 (erNTLocalName など) を入力します。

ソース属性
検索の完了後に返す属性値 (erNTGlobalGroupId など) を入力します。

フィルター
検索に適用する必要がある追加のフィルター (objectclass=erNTLocalGroup など) を入力します。 作成されるフォームのグループ・フィールドの値は、objectclass=erroles にする必要があります。

区切り文字
作成されるフォームで属性値を区切るときに使用する区切り文字を入力します。

複数値 このチェック・ボックスを選択すると、作成されるフォームのドロップダウン・ボックスをリスト・ボックスに変更できます。 リスト・ボックスを使用すると、ユーザーは複数の値を選択できます。

照会 UI の表示
このチェック・ボックスを選択すると、作成されるフォームに検索ページを表示できます。 このオプションを選択していない場合は、検索結果のみが別のページに表示されます。

結果のページ編集
このチェック・ボックスを選択すると、検索結果を複数のページにまたがって表示できます。

編集可能テキスト・リスト

複数の値を持つ属性をユーザー・インターフェースに表示できます。このコントロール・タイプは、ユーザーが入力した情報を表示するリスト・ボックスです。ユーザーは、テキスト・フィールドに情報を入力して「**追加**」をク

リックすると、その情報をリスト・ボックスに追加できます。また、項目を選択して「**削除**」をクリックすると、リスト・ボックスから該当項目の情報を削除できます。

リスト・ボックス

属性のリスト・ボックスを提供します。このリスト・ボックスには、ユーザーが選択したデータが入っています。ユーザーは 1 つ以上の項目をリスト・ボックスに追加できます。リスト・ボックスから 1 つ以上の項目を削除することもできます。

カスタム値

作成されるフォームのリストに表示される情報を制限します。 このオプションを選択すると、「エディターの選択」ページが表示されます。このエディターのフィールドを使用すると、コントロール・タイプを構成できます。「エディターの選択」には、以下のフィールドとツールバー・ボタンがあります。

行数 リストに組み込む行の数を入力して、「**実行**」を押します。このフィールドを使用して、リスト内の行の数を指定します。元のリストの行数が入力した数より多い場合、余分な行は削除されます。

データ値

データ値を入力します。

表示値 リストに表示する表示値を入力します。

ブランク行を使用

リストに空の項目を挿入するには、このチェック・ボックスを選択します。

行の追加

リストに表示する行を追加する場合にクリックします。

行の削除

リストから行を削除する場合にクリックします。

表示値をデータ値として使用

「**表示値**」列に入力したのと同じ値を「**データ値**」列に使用します。

索引をデータ値として使用

「**データ値**」列の索引と同じ値を使用します。

検索フィルター

ボックスにデータを取り込む場合の情報の収集元にする範囲を広げることができます。「LDAP 検索フィルター」を使用すると、検索コントロールを使用して属性に値が割り当てられます。このオプションを選択すると、「検索フィルター・エディター」ページが表示されます。このエディターのフィールドを使用すると、コントロール・タイプを構成できます。「検索フィルター・エディター」には次のフィールドが含まれています。

検索ベース
検索の有効範囲を以下のオプションから選択します。

「**org**」を選択すると、組織ツリーの中の、選択したコンテナーの組織が検索されます。

「**コンテキスト**」を選択すると、組織ツリーの中の、選択した組織単位が検索されます。

オブジェクト・クラス
検索対象となる LDAP クラスの名前 (erNTGlobalGroup など) を入力します。作成されるフォームのグループ・フィールドの値は、erroles にする必要があります。

属性 検索対象となる属性 (erNTLocalName など) を入力します。

ソース属性
検索の完了後に返す属性値 (erNTGlobalGroupId など) を入力します。

フィルター
検索に適用する必要がある追加のフィルター (objectclass=erNTLocalGroup など) を入力します。 作成されるフォームのグループ・フィールドの値は、objectclass=erroles にする必要があります。

区切り文字
作成されるフォームで属性値を区切るときに使用する区切り文字を入力します。

複数値 このチェック・ボックスを選択すると、作成されるフォームのドロップダウン・ボックスをリスト・ボックスに変更できます。 リスト・ボックスを使用すると、ユーザーは複数の値を選択できます。

照会 UI の表示
このチェック・ボックスを選択すると、作成されるフォームに検索ページを表示できます。 このオプションを選択していない場合は、検索結果のみが別のページに表示されます。

結果のページ編集
このチェック・ボックスを選択すると、検索結果を複数のページにまたがって表示できます。

ログイン時間

ユーザーがサービスにログインできる時間を定義します。このコントロール・タイプは、ログイン時間の制限をサポートするサービス (Windows 2000 サービスなど) のフォーム上でのみ使用してください。

このコントロール・タイプを Form Designer アプレットで選択すると、「ログイン時間エディター」ページが表示されます。このエディターのフィ

ールドを使用すると、特定の検索タイプがデフォルトになるようにコントロール・タイプを構成できます。「ログイン時間エディター」には次のフィールドが含まれています。

時間間隔

作成されるフォームに表示される時間間隔を以下から選択します。

「**1 時間**」を選択すると、時間間隔が 1 時間単位のブロックに設定されます。

「**30 分**」を選択すると、時間間隔が 30 分単位のブロックに設定されます。

方向 作成されるフォームでのログイン時間を定義するために使用するエディターの方向を選択します。

「**縦長**」を選択すると、X 軸に沿って 1 週間の日数が示され、Y 軸に沿って時間 (30 分単位または 1 時間単位) が示されます。

「**横長**」を選択すると、X 軸に沿って時間 (30 分単位または 1 時間単位) が示され、Y 軸に沿って 1 週間の日数が示されます。

パスワード

ユーザーが入力する情報を表示しない属性用のテキスト・ボックスを提供します。情報は、安全保護のために、スクリーン上ではマスクされています。

パスワード・ポップアップ

ユーザーが機密保護情報を入力するためのウィンドウを開きます。その情報は、スクリーン上ではマスクされ、情報を入力するための 2 つのテキスト・フィールドが提供されます。このコントロール・タイプは、通常、個人の共有秘密の場合に使用します。

検索コントロール

選択した属性のテキスト・フィールド検索ページを表示し、「**検索**」ボタンと「**消去**」ボタンを組み込みます。ユーザーは、希望する検索結果を選択することでテキスト・フィールドにデータを取り込みます。作成されるフォームのユーザー・インターフェースでは、「**検索**」ボタンを使用すると、検索タイプが既に選択されている状態で検索ページが開き、「**消去**」ボタンを使用すると、テキスト・フィールドの内容が消去されます。

このコントロール・タイプを Form Designer アプレットで選択すると、「検索コントロール・エディター」ページが表示されます。このエディター

のフィールドを使用すると、特定の検索タイプがデフォルトになるようにコントロール・タイプを構成できます。「検索コントロール・エディター」には次のフィールドが含まれています。

カテゴリー
検索のカテゴリーを選択します。

プロファイル
検索に使用するプロファイルを選択します。

属性 検索に使用する属性を選択します。

演算子 「**属性**」フィールドと「**値**」フィールドを結びつける演算子 (「**含む**」や「**同等**」 など) を選択します。

値 属性の値を入力します。

タイプ 返される属性のタイプを選択します。 単一値タイプを選択すると、ユーザーがデータを取り込むためのテキスト・フィールドが表示されます。複数値タイプを選択すると、属性のリスト・ボックスが表示されます。 このシナリオでは、ユーザーは検索の対象にしない属性を選択して「**削除**」ボタンをクリックすることにより、どの属性を検索するかを指定できます。 「削除」により、選択された属性は、検索可能な属性のリストから除去されます。

組織全体の検索 (チェックされない場合は現行コンテナーのみ)
このチェック・ボックスは、組織全体を検索の対象にする場合に選択します。

関連コントロール・タイプは、検索の一致コントロール・タイプです。このタイプは、追加機能を持った検索コントロール・コントロール・タイプで、属性のリスト・ボックスを自動検索して取り込むことができます。

検索の一致

検索コントロール・コントロール・タイプに似ており、属性のリスト・ボックスのデータを自動検索して取り込むことができる追加機能を備えています。ユーザーは、テキスト・フィールド内で希望する値の最初の数文字を入力し、「**追加**」をクリックすることによって、自動検索機能を使用することができます。1 つの結果が見つかれば、その結果は自動的にリスト・ボックスに追加されます。複数の結果が見つかった場合は、「検索結果」ページが表示されます。その後、ユーザーは、どの項目をリスト・ボックスに追加するかを選択できます。

選択した属性のテキスト・フィールド検索ページが表示されます。ユーザーは、希望する検索結果を選択することでテキスト・フィールドにデータを取り込みます。作成されるフォームで、「**検索**」ボタンをクリックすると、検索タイプが既に選択された状態で検索ページが開きます。「**消去**」ボタンをクリックすると、テキスト・フィールドの内容が消去されます。「**削除**」ボタンは、リスト・ボックスから選択した項目を除去するために使います。

このコントロール・タイプを Form Designer アプレットで選択すると、「検索コントロール・エディター」ページが表示されます。このエディター

のフィールドを使用すると、特定の検索タイプがデフォルトになるようにコントロール・タイプを構成できます。「検索コントロール・エディター」には次のフィールドが含まれています。

カテゴリー
検索のカテゴリーを選択します。

プロファイル
検索に使用するプロファイルを選択します。

属性 検索に使用する属性を選択します。

演算子 「**属性**」フィールドと「**値**」フィールドを結びつける演算子 (「**含む**」や「**同等**」 など) を選択します。

値 属性の値を入力します。

タイプ 返される属性のタイプを選択します。 単一値タイプを選択すると、ユーザーがデータを取り込むためのテキスト・フィールドが表示されます。複数値タイプを選択すると、属性のリスト・ボックスが表示されます。 このシナリオでは、ユーザーは検索の対象にしない属性を選択して「**削除**」ボタンをクリックすることにより、どの属性を検索するかを指定できます。 「削除」により、選択された属性が検索可能な属性のリストから除去されます。

組織全体の検索 (チェックされない場合は現行コンテナーのみ)
このチェック・ボックスは、組織全体を検索の対象にする場合に選択します。

関連したコントロール・タイプは、「検索コントロール」です。

サブフォーム

サブフォーム・コントロール・タイプは、複合多値属性の場合にカスタム・ユーザー・インターフェースを使用する方法を提供します。IBM Security Identity Manager アダプターの中には、このコントロール・タイプをあまり使用しないものもあります。

サブフォームは、カスタム IBM Security Identity Manager フォームから開くポップアップ・ウィンドウから、サーブレット、JSP、または静的 HTML ページを始動する場合に使用する特殊なコントロール・タイプです。サブフォームはカスタム Servlet または JSP に任意の数のパラメーター名と値を送信する手段を提供します。サブフォームを使用して、複合多値属性用にカスタム・ユーザー・インターフェースを作成します。

表 25. サブフォームのパラメーター

パラメーター	説明	値
customServletURI	メイン・フォームから開始される、Servlet、JSP、または静的 HTML ページへの URI。サーブレットが IBM Security Identity Manager のデフォルトの Web アプリケーションに実装およびデプロイされている場合は、このパラメーターの値は *servlet-mapping* タグ内の web.xml で定義されている *URL-pattern* 値からスラッシュ (*/*) を除いたものと同じです。 JSP が実装されている場合、このパラメーターの値は jsp ファイル拡張子を含めた JSP ファイル名です。このパラメーターはすべてのサブフォームで必要です。	サーブレット名または JSP ファイル名 (例: `sample.jsp`)
パラメーター名	customServletURI でリソースを開始する HTTP 要求に含まれている任意のパラメーター名および値。	*パラメーター値* 例: racfconnectgroup servlet

テキスト域

属性の隣にテキスト域を配置します。テキスト域とは、ユーザー入力を集めたり、以前に集められたデータを表示するために使用される、複数行のテキスト域のことです。

テキスト・フィールド

属性の隣にテキスト・フィールドを配置します。テキスト・フィールドは、ユーザーの入力を収集したり、以前に収集されたデータを表示するときに使用する 1 行の領域です。

UMask

ユーザーがファイルおよびディレクトリーに UNIX のアクセス権限を定義できます。

Form Designer で使用されるプロパティー

「プロパティー」ページを使用して、属性の形式と制約を構成します。

「プロパティー」ページには、以下のタブがあります。

フォーマット

このタブは、フォームのフォーマットを変更するために使用します。 このタブで使用可能なフィールドは、以下のとおりです。

名前 属性の名前を追加または変更するには、このフィールドを使用します。この値は、フォームが LDAP 属性の処理に使用する ID です。

データ・タイプ
ディレクトリー・ストリング、識別名、バイナリー・コードなどの属性のデータ・タイプを追加または変更するには、このフィールドを使用します。

ラベル ユーザー読取可能な属性のラベルを追加または変更するには、このフィールドを使用します。例えば、$homepostaladdress。この場合、$ (ドル) 記号はリソース・バンドルのストリングを検索するためのキーを示します。

サイズ 「テキスト・フィールド」、「パスワード」、「検索コントロール」、および「検索の一致」の 4 つのコントロール・タイプについて、ピクセル単位の表示幅を追加または変更する場合は、このフィールドを使用します。「サイズ」は、「リスト・ボックス」と「編集可能テキスト・リスト」の 2 つのコントロール・タイプの表示項目数を表します。

行 表示されるテキストの行数を表すためにテキスト域コントロール・タイプが使用する値を追加または変更するには、このフィールドを使用します。

列 表示幅を平均の文字幅で表すためにテキスト域コントロール・タイプが使用する値を追加または変更するには、このフィールドを使用します。

幅 ポップアップ・ウィンドウの幅をピクセル単位で表すためにサブフォーム・コントロール・タイプが使用する値を追加または変更するには、このフィールドを使用します。

このプロパティーは、
DropDownBox、EditableTextList、ListBox、SearchControl、および SearchMatch コントロールでも、関連付けられたコンボ・ボックス幅をピクセル単位で表すために使用します。EditableTextList および SearchMatch コントロールの場合は、関連付けられたテキスト・ボックスの幅もピクセル単位で決定します。

幅が指定されていない場合は、デフォルトの 300 ピクセルであると想定されます。これらのコントロールの幅を 0 に設定した場合は、関連付けられたコンボ・ボックスは固定サイズでなくなり、サイズが動的に変化するようになります。サイズは、追加されるオプションによって異なります。

高さ ポップアップ・ウィンドウの高さをピクセル単位で表すためにサブフォーム・コントロール・タイプが使用する値を追加または変更するには、このフィールドを使用します。

変更時に読み取り専用
属性を読み取り専用に設定するには、このチェック・ボックスを選択します。フォームにはラベルのみが表示され、ユーザーは属性値を変更できません。

向き　テキストの向きを以下から選択します。

「**継承**」を選択すると、テキストが表示される向きは、属性が属しているフォーム・カテゴリーと同じ向きになります。

「**ltr**」を選択すると、テキストは左から右に向かって表示されます。

「**rtl**」を選択すると、テキストは右から左に向かって表示されます。

変更時に非表示

フォームが「変更」状態の場合に属性フィールドを非表示にするには、このチェック・ボックスを選択します。例えば、サービス・フォーム内の「所有者」フィールドに対してこのチェック・ボックスを選択すると、ユーザーがサービスを作成した場合に「所有者」フィールドが表示されます。このフィールドは、ユーザーがサービスを変更すると表示されません。

制約　ユーザーがフォーム・フィールドに入力できるデータのタイプとデータの構文を保証するには、このタブを使用して「制約」フィールドに値を入力します。カスタム制約とは、さまざまなタイプのフィールド・レベル・データ制限のことです。「**SearchControl**」、「**SearchMatch**」、「**ListBox**」、または 「**DropDownBox**」のコントロール・タイプを選択した場合、すべての制約フィールドが使用不可になります。ただし、「**必須**」制約のみは使用可能です。

必須　この制約を適用するフィールドに値を入力しなければフォームを実行できないようにするには、このチェック・ボックスを選択します。

制約の検証と更新

制約タイプ・リストの下部にある「**制約の検証と更新**」ボタンの横のフィールドに、フォーム・テンプレート・レイアウト領域から選択した属性のサンプル値を入力し、「**制約の検証と更新**」ボタンをクリックします。これにより、属性に対してアクティブ化されている制約に基づいて入力した値がテストされます。入力したテスト値がすべての制約に適合している場合は、「**制約の検証と更新**」ボタンをクリックすると、成功したことを示すメッセージが表示されます。

制約は、以下の一般カテゴリーのいずれかに分類されます。

構文上の制約

文字や構造化された部分のシーケンスを定義するルールに適合する値のみを許可します。

電子メール・アドレス

この制約を適用するフィールドに指定できる値の構文に以下のルールを課すには、このチェック・ボックスを選択します。

- @ 記号が 1 つある

- < > ( ) . ; " ¥ [ ] などの無効文字が、@ 記号の前には存在しない
- @ 記号の後には、有効なドメイン名または IP アドレスが必要

IP アドレス (IPV4)
この制約が適用されるフィールドに入力した値が有効な IPv4 アドレス形式 (127.0.0.1) であることを保証するには、このチェック・ボックスを選択します。4 オクテットがドットで区切られ、どのオクテットも 255 を超えることはありません。

IP アドレス (IPV6)
フィールドに入力される値が、RFC 2373 で定義された IP アドレスのテキスト表記に準拠していることを保証するには、このチェック・ボックスを選択します。例えば: 0:0:0:0:0:0:0:1 は、ループバック IPV6 アドレスです。詳細については、RFC 2373 を参照してください。

ドメイン名
この制約を適用するフィールドに入力される値が、Windows NT のドメイン名構文に準拠するようにするには、このチェック・ボックスを選択します。名前は、先頭に 2 つの円記号 (¥¥) が必要であり、以降には " / ¥ [] : ; | = , + * ? < > の文字を使用せず、15 文字以内とします。

名前をピリオドやスペースのみで構成することはできません。

無効文字
このフィールドに入力するときに無効とする文字を定義するには、このフィールドにその無効文字を入力します。

DN フィールドに入力される値が、識別名構造に準拠していることを保証するには、このチェック・ボックスを選択します。例えば、cn=*共通*、*組織名*、o=*組織*です。

データ・タイプの制約
一定の範囲内の文字または数値が使用された値が許可されます。

ASCII-Only
フィールドに入力できる文字を ASCII に制限するには、このチェック・ボックスを選択します。

ASCII7
フィールドに入力できる文字を ASCII-7 に制限するには、このチェック・ボックスを選択します。

ASCII8
フィールドに入力できる文字を ASCII-8 に制限するには、このチェック・ボックスを選択します。

整数のみ
フィールドに整数のみを入力できるようにするには、このチェック・ボックスを選択します。

数値 フィールドに数値のみを入力できるようにするには、このチェック・ボックスを選択します。

日付範囲
終了日が開始日より後であるように強制するための日付範囲を入力します。

値の制約

`Max Length = 10` などのパラメーターが必要です。この場合、`10` とは、値の制約に使用するパラメーターです。

無効文字
却下する文字を入力します。

最大長 フィールドに入力される値の長さを所定の文字数に制限するための数値を入力します。

最小長 入力された値がこの制約を指定した文字数より短い場合にフォームが実行されないようにするための数値を入力します。

最大値 入力された値の最高点 (多くても *n*) を設定する数値を入力します。

最小値 入力された値の最低点 (少なくとも *n*) を設定する数値を入力します。

最大行 複数行フィールドにおいて、フォームに入力された値が所定の最大行数を超えないようにするための数値を入力します。

空白なし
フォームに空白文字を入力できないようにするには、このチェック・ボックスを選択します。

Form Designer のユーザー・インターフェースを変更するプロパティー

IBM Security Identity Manager には、Form Designer のインターフェースの外観を決定するプロパティーがあります。

`ui.properties` ファイルには、Form Designer のユーザー・インターフェースの外観を変更するための以下のようなプロパティーがあります。

express.java.formDesignHeightIE
Internet Explorer の場合の Form Designer アプレットの高さ (ピクセル)

express.java.formDesignWidthIE
Internet Explorer の場合の Form Designer アプレットの幅 (ピクセル)

express.java.formDesignHeightMZ
Mozilla の場合の Form Designer アプレットの高さ (ピクセル)

express.java.formDesignWidthMZ
Mozilla の場合の Form Designer アプレットの幅 (ピクセル)

第 8 章 手動通知テンプレートの管理

このタスクを使用して、手動サービスに表示されるデフォルトの電子メール・メッセージを変更します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

手動サービスに表示されるデフォルトのメッセージを変更できます。テンプレートを変更することによって、作成する任意の手動サービスに対する変更を適用できます。サービスに特定のメッセージ変更が必要な場合を除き、手動サービスを作成するたびにメッセージを変更する必要はありません。

注: 通知テンプレートに対する変更は、既存の手動サービスのメッセージに影響を与えません。

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**手動通知メッセージの構成 (Configure Manual Notification Templates)**」をクリックします。 「テンプレート」ページが表示されます。
2. 操作を選択して、「**変更**」をクリックします。 「テンプレートの変更 (Template Modify)」ページが表示されます。
3. 「**件名**」フィールドで、送信される電子メール通知の件名を指定するテキストを変更します。 件名には、プレーン・テキストと動的コンテンツ・タグを組み込めます。
4. **Plaintext body**フィールドで、メッセージの本文に表示されるテキストを変更します。 内容としては、プレーン・テキスト、動的コンテンツ・タグ、JavaScript コードを組み込めます。これらのコンテンツは、HTML 電子メール通知を参照しない電子メール受信者に表示されます。
5. 「**XHTML 本文**」フィールドに、電子メール通知の本文に HTML として表示されるテキストを入力します。 内容としては、プレーン・テキスト、動的コンテンツ・タグ、JavaScript コードを組み込めます。これらのコンテンツは、HTML 電子メール通知を参照する電子メール受信者に表示されます。
6. 「**OK**」をクリックして変更を保存します。 「テンプレート」ページに戻ります。

次のタスク

別の操作の通知テンプレートを変更するか、「**閉じる**」をクリックして終了します。

第 9 章 エンティティー管理

エンティティーは情報を保存する個人またはオブジェクトです。

システム・エンティティーには、ポリシーやワークフローなどの多くのタイプがありますが、カスタマイズに対応しているのは以下のエンティティー・タイプのみです。

- アカウント
- BP 個人 (ビジネス・パートナー個人)
- ビジネス・パートナー組織
- 組織
- 個人
- サービス

システム管理者は、エンティティー属性を選択的にカスタム LDAP クラス属性にマップして、既存のシステム・エンティティーをカスタマイズできます。システム管理者は、新しい個人および BP 個人 (ビジネス・パートナー個人) カスタム・エンティティーを作成することもできます。管理者は、固有のエンティティー名を標準の IBM Security Identity Managerエンティティー・タイプと関連付けます。

システム・エンティティーの追加

新規のカスタム LDAP クラスに関連付ける、新規の個人エンティティーおよび BP 個人エンティティーを作成します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

個人タイプまたは BP 個人タイプのエンティティーを追加するときは、このタスクを使用してエンティティーを追加する前に、そのエンティティーを格納する実際の LDAP クラスを作成する必要があります。

カスタム LDAP クラスおよびその属性は、LDAP データ・リポジトリー・ソフトウェアと互換性のあるツールを使用して、データ・ストア内に直接作成する必要があります。クラスは、カスタム IBM Security Identity Manager エンティティーと関連付ける前に作成します。クラスを作成後、カスタム IBM Security Identity Manager エンティティーと関連付けます。属性は、IBM Security Identity Manager 属性にマップします。

このタスクについて

「er」で始まる形式の補助および構造 LDAP クラスはすべて、IBM Security Identity Manager-managed クラスとみなされます。そのため、「エンティティーの管理」タスクで LDAP クラスのリストに表示されません。

カスタム・エンティティーの追加時には、各属性のデフォルトのコントロール・タイプを調べる必要があります。フォーム・カスタマイズ・ページにより、適切なコントロール・タイプに変更します。標準エンティティーの属性に割り当てられているコントロール・タイプを表示するには、カスタム・エンティティーと同じエンティティー・タイプの標準的な IBM Security Identity Manager エンティティーを参照してください。

カスタム・システム・エンティティーを追加するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから**「システムの構成」** > **「エンティティーの管理」**をクリックします。 「エンティティーの管理」ページが表示されます。
2. 「エンティティーの管理」ページで、**「追加」**をクリックします。 エンティティーの作成ウィザードが表示されます。
3. 「タイプを選択」ページで、作成するエンティティー・タイプを選択してから、**「次へ」**をクリックします。
4. 「エンティティーの詳細情報」ページで、以下の手順を実行します。
   a. **「エンティティー名」**フィールドに、エンティティーの固有の名前を入力します。
   b. **「検索」**をクリックして、エンティティーを保存する LDAP クラスを検索し、指定します。
   c. 「LDAP クラスの選択」ページで、**「検索」**をクリックします。LDAP クラスのリストが表示されます。
   d. オブジェクト・クラス名を選択してから**「OK」** をクリックします。 **「LDAP クラス」**フィールドに、指定したオブジェクト・クラス名が取り込まれます。
   e. **「名前属性の参照」**をクリックして検索および指定します。 **「名前属性 (Name attributes)」**フィールドの有効なエントリーは、選択した LDAP クラスによって異なります。 「属性の選択」ページが表示されます。選択した LDAP クラスの名前属性がリストされています。
   f. 「属性の選択」ページで、新しいエンティティーに関連付ける名前属性を選択してから**「OK」**をクリックします。 **「名前属性」**フィールドに、選択した名前属性が取り込まれます。
   g. **「デフォルト検索属性」**リストで、エンティティーに追加する検索属性を選択してから**「追加」**をクリックします。 ストリング・タイプまたは数値タイプなど、検索可能な属性を選択します。
   h. エンティティー情報の指定が完了したら、**「次へ」**をクリックします。
5. 「属性のマッピング」ページで、以下の手順を実行して属性をマップします。
   a. **「Identity Manager 属性」**リストから属性を 1 つ選択します。
   b. **「カスタム LDAP 属性」**リストから属性を 1 つ選択します。

c. 「**マップ**」をクリックします。
d. オプション: デフォルト・マッピングを取得するには、テーブルで属性のペアを選択して、「**リセット**」をクリックします。
e. マッピングが完了したら、「**終了**」をクリックします。

タスクの結果

エンティティーが正常に作成されたことを示すメッセージが表示されます。

次のタスク

エンティティー管理タスクをさらに実行するか、「**クローズ**」をクリックします。

システム・エンティティーの変更

IBM Security Identity Manager エンティティーをカスタム LDAP クラスにどのように関連付けるのかを指定するマッピングを表示および変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

エンティティー・タイプにはスキーマ定義が関連付けられているため、エンティティー・タイプを変更することはできません。代わりに、そのエンティティーを削除し、希望するタイプを使用して、エンティティーを作成する必要があります。

既存のエンティティーを変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**エンティティーの管理**」をクリックします。 「エンティティーの管理」ページが表示されます。
2. 「エンティティーの管理」ページで、変更するエンティティーの横のチェック・ボックスを選択してから「**変更**」をクリックします。 「エンティティーの変更」ノートブックが表示されます。
3. 「**エンティティーの詳細情報**」タブまたは「**属性のマッピング**」タブをクリックします。
4. エンティティーを変更し、「**OK**」をクリックします。

次のタスク

エンティティーが正常に更新されたことを示すメッセージが表示されます。

エンティティー管理タスクをさらに実行するか、「**クローズ**」をクリックします。

システム・エンティティーの削除

IBM Security Identity Manager システムからシステム・エンティティーを削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

エンティティーに従属単位が存在している場合は、そのシステム・エンティティーを削除できません。

システム・エンティティーを削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**エンティティーの管理**」をクリックします。 「エンティティーの管理」ページが表示されます。
2. 「エンティティーの管理」ページで、削除するエンティティーの横のチェック・ボックスを選択してから「**削除**」をクリックします。 この列の上部にあるチェック・ボックスを選択すると、すべてのシステム・エンティティーが選択されます。
3. 「確認」ページで、「**削除**」をクリックしてエンティティーを削除するか、「**キャンセル**」をクリックします。

タスクの結果

エンティティーが正常に削除されたことを示すメッセージが表示されます。

次のタスク

エンティティー管理タスクをさらに実行するか、「**クローズ**」をクリックします。

役割のスキーマのカスタマイズ

アドミニストレーターは、オプションの属性を IBM Security Identity Manager LDAP に追加し、次に役割の定義スキーマ (*erRole* objectclass) に追加することによって、役割のスキーマをカスタマイズします。

このタスクについて

手順

1. IBM Security Identity Manager LDAP にアクセスします。
2. 新しいオプションのタイプ属性を追加します。 例えば、属性 `designation` を追加します。 詳しくは、「*LDAP Installation and Configuration Guide* 」を参照してください。

3. IBM Security Identity Manager LDAP 内の *erRole* オブジェクト・クラスを更新して、新しい属性に関連付けます。 例えば、Tivoli Directory Server Web 管理コンソールを使用して、IBM Tivoli Directory Server の *erRole* オブジェクト・クラスを更新し、`designation` 属性を *erRole* オブジェクト・クラスと関連付けます。 Tivoli Directory Server について詳しくは、*IBM Security Identity Manager* インフォメーション・センター を参照してください。
4. 役割のスキーマが正しくカスタマイズされていることを確認してください。
5. IBM Security Identity Manager および IBM Security Identity Manager LDAP が稼働していることを確認します。
6. IBM Security Identity Manager 管理コンソールを起動します。
7. **「システムの構成」>「フォームの設計」**を選択します。
8. 役割フォーム・テンプレートを更新して、新しい属性を表示します。

タスクの結果

役割の定義を表示すると、IBM Security Identity Manager 管理コンソール上に新しい属性を表示できます。

次のタスク

役割を作成または変更すると、カスタム属性を定義、設定、変更、保存、および復元できます。

第 10 章 所有権タイプ管理

所有権タイプ によってアカウントを分類します。組織における所有権タイプを分類するには、「**所有権タイプの管理**」タスクを使用します。複数アカウントの所有権タイプを構成する場合、IBM Security Identity Manager は、新規アカウントを要求するとき、またはユーザーにアカウントを割り当てるときに、所有権タイプを選択するよう求めるプロンプトを出します。

IBM Security Identity Manager には、以下のものがあります。

- デバイス
- 個人
- システム
- ベンダー

管理者は、追加の所有権タイプを作成できます。

アカウントには、所有権のタイプを 1 つだけ持たせることができます。所有権タイプは、そのアカウントの使用目的に依存しています。所有権のタイプは、パスワード管理プロセスに影響します。例えば、パスワード同期では、所有権タイプが「個人」のアカウントのパスワードを変更できます。

所有権タイプの作成

管理者は、追加の所有権タイプを作成できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクにアクセスする方法または別のユーザーにこのタスクの完了を依頼する方法については、システム管理者に連絡してください。

このタスクについて

所有権タイプを作成するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**所有権タイプの管理**」をクリックします。「**所有権タイプの管理**」ページにデフォルトの所有権タイプがリストされます。

   デフォルトの所有権タイプは以下のとおりです。
   - デバイス
   - 個人
   - システム
   - ベンダー
2. 「**作成**」をクリックします。「**所有権タイプの作成**」ページが表示されます。

3. 以下の手順を実行します。
   a. 「**所有権タイプ・キー**」に、所有権タイプのカスタム名を入力します。
   b. (オプション) 「**説明**」に、所有権タイプの説明を入力します。
4. 「**OK**」をクリックして、新規所有権タイプを保存します。

タスクの結果

所有権タイプが正常に作成されたことを示すメッセージが表示されます。「**所有権タイプの管理**」ページに、その新規所有権タイプが表示されます。

次のタスク

所有権タイプをさらに作成または変更するか、「**閉じる**」をクリックします。

所有権タイプの削除

所有権タイプが有効でなくなった場合、管理者は「個人」を除くすべての所有権タイプを削除できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクにアクセスする方法または別のユーザーにこのタスクの完了を依頼する方法については、システム管理者に連絡してください。所有権タイプは、アカウントに関連付けられていない場合にのみ削除できます。

このタスクについて

所有権タイプは、アカウントに関連付けられている場合は削除できません。

手順

1. ナビゲーション・ツリーから「**所有権タイプの管理**」をクリックして、現在定義されている所有権タイプをリストするページを表示します。
2. 削除する所有権タイプを選択します。
   a. 特定の所有権タイプを選択するには、その横にあるチェック・ボックスを選択します。
   b. すべての所有権タイプを選択するには、列の最上部にあるチェック・ボックスをクリックします。
3. 「**削除**」をクリックします。確認ページが表示されます。
4. 確認ページで、以下のアクションのいずれかを実行します。
   a. 「**削除**」をクリックして、所有権タイプを削除します。
   b. 「**キャンセル**」をクリックして、削除プロセスを停止します。

タスクの結果

所有権タイプが正常に削除されたことを示すメッセージが表示されます。「**所有権タイプの管理**」ページで削除された所有権タイプはもう表示されません。

次のタスク

所有権タイプを作成または削除できます。

第 11 章 操作管理

IBM Security Identity Manager システム・エンティティーおよびエンティティー・タイプについての操作可能ワークフローを構成できます。標準装備のエンティティー・タイプ操作をカスタマイズして、組織のセキュリティー要件をインプリメントできます。

*操作*は、エンティティーに対して実行できるアクションを示します。特定のエンティティー・タイプに定義された操作は、その指定タイプのすべてのエンティティーで使用されます。ただし、特定のエンティティーに対して定義されている操作がある場合は、操作がエンティティー・タイプ操作より優先されます。

システム管理者は、エンティティーおよびエンティティー・タイプに対する新規操作を作成したり、既存の操作を変更したりできます。

以下のエンティティー・タイプに対する操作がカスタマイズ可能です。

- アカウント
- 個人
- ビジネス・パートナー個人

「個人」、「ビジネス・パートナー個人」、または「アカウント」の操作は、カスタマイズされた操作がエンティティー・レベルで定義されている場合を除いて、すべてのユーザー、ビジネス・パートナー・ユーザー、またはアカウント・エンティティーに適用されます。

追加操作

追加操作は、指定したエンティティー・タイプの追加要求が実行されるといつでも開始されます。例えば、新規ユーザーをシステムに追加すると、「個人」エンティティー・タイプに対する追加操作が開始されます。

追加操作のデフォルト・ワークフローは、追加されるエンティティーのタイプに依存します。

「個人」エンティティーおよび「ビジネス・パートナー個人」エンティティーの追加操作のデフォルト・ワークフローでは、`createPerson` および `enforcePolicyForPerson` というワークフロー拡張機能を使用します。

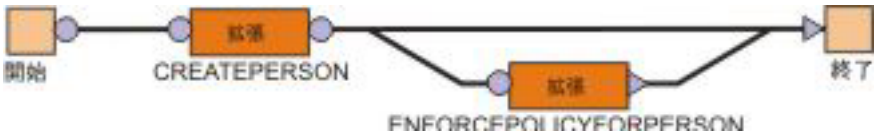


図 10. 「個人」および「ビジネス・パートナー個人」の追加操作ワークフロー

アカウント・エンティティー追加操作のデフォルト・ワークフローでは、createAccount ワークフロー拡張機能を使用します。

図 11. アカウント追加操作ワークフロー

図 12. Identity Manager ユーザー追加操作ワークフロー

パスワード変更操作

パスワード変更操作は、「アカウント」エンティティーのパスワード変更要求が実行されるといつでも開始されます。

changePassword 操作のデフォルト・ワークフローでは、changePassword ワークフロー拡張機能を使用します。

図 13. パスワード変更操作ワークフロー

削除操作

削除操作は、指定したエンティティー・タイプの削除要求が実行されるといつでも開始されます。

削除操作のデフォルト・ワークフローは deletePerson または deleteAccount ワークフロー拡張機能を使用します。

図 14. アカウント削除操作ワークフロー

図 15. 「個人」および「ビジネス・パートナー個人」の削除操作ワークフロー

変更操作

変更操作は、エンティティーを変更する要求が実行されるといつでも開始されます。

変更操作のデフォルト・ワークフローは、変更されるエンティティーのタイプに依存します。

アカウント・エンティティーのデフォルト・ワークフローでは、`modifyAccount` ワークフロー拡張機能を使用します。

図 16. アカウントの変更操作ワークフロー

「個人」および「ビジネス・パートナー個人」の追加操作のデフォルト・ワークフローでは、`modifyPerson` および `enforcePolicyForPerson` というワークフロー拡張機能を使用します。

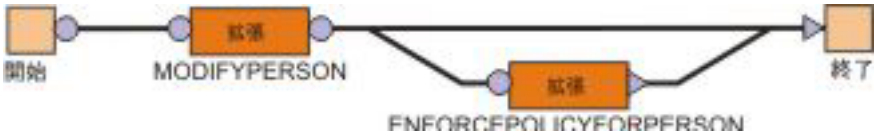


図 17. 「個人」および「ビジネス・パートナー個人」の変更操作ワークフロー

復元操作

復元操作は、指定したエンティティー・タイプの復元要求が実行されるといつでも開始されます。

復元操作のデフォルト・ワークフローは `restorePerson` または `restoreAccount` ワークフロー拡張機能を使用します。

図 18. アカウントの復元操作ワークフロー

図 19. 「個人」および「ビジネス・パートナー個人」の復元操作ワークフロー

自己登録操作

自己登録操作は、個人が自分自身を IBM Security Identity Manager で登録しようとするときに使用します。この操作は、「ユーザー」エンティティーまたは「ビジネス・パートナー個人」エンティティーでのみ使用できます。

デフォルトの自己登録操作には、以下のステップがあります。

1. 個人エンティティーの作成
2. 個人エンティティーが既存のポリシーに準拠することの確認

自己登録操作を使用する前に、開始エレメント、または開始エレメントと createPerson 拡張エレメントの間の遷移線に、個人エンティティーの追加先であるコンテナーを計算する JavaScript が記述されている必要があります。この JavaScript コードは、開始エレメント内では PostScript、遷移線の場合はカスタム定義とすることができます。

この図は、selfRegister のデフォルト・ワークフローを示しています。

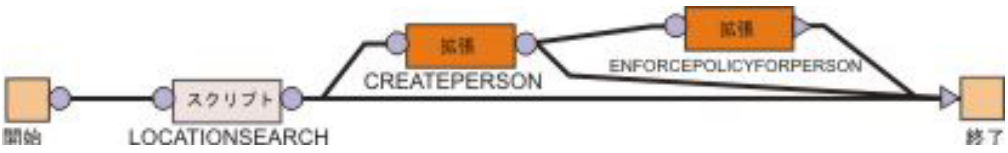


図 20. 自己登録操作ワークフロー

サスペンド操作

サスペンド操作は、指定したエンティティー・タイプのサスペンド要求が実行されるといつでも開始されます。

サスペンド操作のデフォルト・ワークフローは `suspendAccount` または `suspendPerson` ワークフロー拡張機能を使用します。この図は、基本サスペンド操作ワークフローを示しています。

図 21. アカウントのサスペンド操作ワークフロー

図 22. 「個人」および「ビジネス・パートナー個人」のサスペンド操作ワークフロー

転送操作

転送操作は、「個人」エンティティーまたは「ビジネス・パートナー個人」エンティティーの転送要求が実行されるたびに開始されます。

転送操作のデフォルト・ワークフローは、`transferPerson` および `enforcePolicyForPerson` ワークフロー拡張機能を使用します。

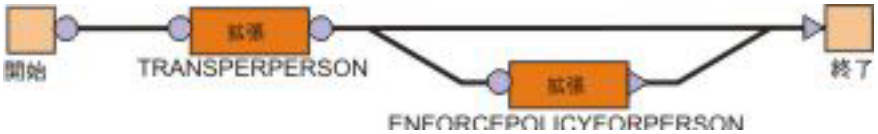


図 23. 「個人」および「ビジネス・パートナー個人」の転送操作ワークフロー

エンティティーの操作の追加

システム管理者がエンティティー操作を追加します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

例えば、新規操作を定義して、個人エンティティーまたはアカウント・エンティティーを再認証する操作を追加することができます。そのエンティティーを承認またはサスペンドする承認ワークフローを指定します。

エンティティーの操作を追加するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**操作の管理**」をクリックします。 「操作の管理」ページが表示されます。
2. 「操作の管理」ページで、以下のいずれかの操作レベルを選択します。
   - すべてのエンティティーおよびエンティティー・タイプに適用可能な操作を定義するには、「**グローバル・レベル**」を選択します。グローバル操作は、エンティティー・タイプまたはエンティティーのレベルの操作から明示的に開始し

ない限り、いずれかのエンティティーに暗黙的に影響することはありません。グローバル操作は、ライフ・サイクル・ルールから呼び出すこともできます。

- エンティティー・タイプ・レベルの操作を定義するには、「**エンティティー・タイプ・レベル**」を選択します。「**エンティティー・タイプ**」のリストからエンティティーのタイプを選択します。
- エンティティー・タイプ・レベルで定義された操作をオーバーライドするには、「**エンティティー・レベル**」を選択します。「**エンティティー・タイプ**」リストからエンティティー・タイプを選択してから、「**エンティティー**」リストからエンティティーを選択します。

3. 「**追加**」をクリックします。 「操作の追加」ページが表示されます。
4. 「**操作名**」フィールドに、対応するシステム・エンティティーに定義するワークフロー操作の名前を入力します。エンティティー・タイプ・レベルで定義されている操作をオーバーライドするには、オーバーライドする操作名を入力し、「**続行**」をクリックします。 「操作の定義」ページが表示され、ワークフロー設計機能 Java アプレットが開始されます。
5. ワークフロー設計機能でワークフロー・プロセスを定義してから、「**OK**」をクリックします。 操作ワークフロー・プロセスを定義するには、設計ノードをノード・パレットから操作設計スペースまでドラッグします。次に、設計ノード間を遷移線で接続します。設計ノードを操作設計スペースに配置したら、設計ノードをダブルクリックして、そのプロパティーを構成します。すべてのノードが接続されており、各ノードにすべての必須プロパティーが設定されていることを確認してください。各リンクの遷移条件が設定されていることを確認してください。

タスクの結果

指定したレベルの操作が正常に作成されたことを示すメッセージが表示されます。「**クローズ**」をクリックします。

次のタスク

「操作の管理」ページが表示されたら、「**リフレッシュ**」をクリックして、「**操作**」テーブルをリフレッシュします。新規の操作が表示されます。

エンティティーの操作の変更

システム管理者は既存のエンティティー操作を変更できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

エンティティーの操作を変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**操作の管理**」をクリックします。 「操作の管理」ページが表示されます。
2. 「操作の管理」ページで、「**グローバル・レベル**」、「**エンティティー・タイプ・レベル**」、または「**エンティティー・レベル**」を選択して、変更する操作をリストします。
3. 変更する操作の横のチェック・ボックスを選択してから「**変更**」をクリックします。 この列の上部にあるチェック・ボックスを選択すると、すべての操作が選択されます。 「操作の定義」ページが表示され、ワークフロー設計機能 Java アプレットが開始されます。
4. ワークフロー設計機能でシステム・エンティティーの操作を変更してから、「**OK**」をクリックします。 操作ワークフロー・プロセスを定義するには、設計ノードをノード・パレットから操作設計スペースまでドラッグします。次に、設計ノード間を遷移線で接続します。設計ノードを操作設計スペースに配置したら、設計ノードをダブルクリックして、そのプロパティーを構成します。すべてのノードが接続されており、各ノードにすべての必須プロパティーが設定されていることを確認してください。各リンクの遷移条件が設定されていることを確認してください。

タスクの結果

エンティティーの操作が正常に更新されたことを示すメッセージが表示されます。「**クローズ**」をクリックします。

次のタスク

「操作の管理」ページが表示されたら、「**リフレッシュ**」をクリックして、「**操作**」テーブルをリフレッシュします。

エンティティーの操作の削除

システム管理者は既存のエンティティー操作を削除できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

削除できるのはユーザー定義の操作のみです。

エンティティーの操作を削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**操作の管理**」をクリックします。 「操作の管理」ページが表示されます。

2. 「操作の管理」ページで、「**グローバル・レベル**」、「**エンティティー・タイプ・レベル**」、または「**エンティティー・レベル**」を選択して、削除する操作をリストします。
3. 削除する操作の横のチェック・ボックスを選択してから「**削除**」をクリックします。 この列の上部にあるチェック・ボックスを選択すると、すべての操作が選択されます。 確認ページが表示されます。
4. 「確認」ページで、「**削除**」をクリックして操作を削除するか、「**キャンセル**」をクリックします。

タスクの結果

エンティティーの操作が正常に削除されたことを示すメッセージが表示されます。「**クローズ**」をクリックします。

次のタスク

「操作の管理」ページが表示されたら、「**リフレッシュ**」をクリックして、「**操作**」テーブルをリフレッシュします。

第 12 章 ライフサイクル・ルールの管理

ライフサイクル・ルールを使用して、一般的な反復イベントの結果としてアドミニストレーターが実行する必要がある数多くの手動タスクを自動化できます。そのようなイベントには、ビジネス・ポリシーに従って実行される、アカウントの非活動化、パスワードの有効期限切れ、契約の有効期限切れなどがあります。またライフ・サイクル・ルールにより、ポリシーによる実行が漏れなく行われるようになります。

概説

ライフサイクル・ルールを作成することにより、アドミニストレーターは、時間間隔に基づいて、または時間とエンティティーに対して評価されるマッチング基準に基づいて、開始することができるイベントを定義できます。次に、アドミニストレーターは、そのイベントの結果として実行されるようライフ・サイクル操作を関連付けることができます。ライフ・サイクル・ルールは、2 つの部分で構成されます。

- ルールを起動するイベントの定義
- ルールに指定されているアクションを実行するライフ・サイクル操作の ID

各ルールは次のいずれかの方法で定義できます。

- グローバル
- エンティティー・タイプとの関連付け
- エンティティーとの関連付け

グローバル・ルールの場合、イベントは時間間隔で定義します。 例えば、月に一度、または毎週月曜の午前 8 時というように定義します。グローバル・ライフ・サイクル・ルールは、どの特定のシステム・エンティティーからも独立です。グローバル・ルールから呼び出せるライフ・サイクル操作も必然的にグローバル操作である必要があります。エンティティーまたはエンティティー・タイプをベースとして呼び出せるコンテキストは存在しないためです。

エンティティーおよびエンティティー・タイプのルールも、時間間隔を持つイベントを持ちます。ただし、これらのルールの目的は、一度に複数のエンティティーに影響することです。

イベントのマッチング基準

ライフ・サイクル・オブジェクトごとに別のイベントが起動されます。ルールに関連しない、数千に上る可能性のあるオブジェクトに対してイベントが発生しないようにするため、これらのイベントではマッチング基準を使用することができます。

マッチング基準なしの場合、特定のエンティティーまたはエンティティー・タイプのすべてのオブジェクトは、関連付けられているライフサイクル操作をそのオブジェクトで実行させます。

マッチング基準が存在する場合は、基準を満たすオブジェクトに対してのみ操作が実行されます。このマッチング基準は、LDAP のフィルター構文を使用して定義します。 フィルターは、基準を満たす各オブジェクトを識別し、それらのオブジェクトに対してのみイベントが起動されるようにします。フィルターに一致するオブジェクトが存在しない場合は、イベントは起動されません。例えば、すべてのアカウントを対象とする (erAccountStatus=1) という基準などを利用できます。この場合は、アカウントがサスペンドされていることを意味します。

ライフサイクル・ルールのフィルターとスケジュール

フィルターは属性に基づくため、エンティティーまたはエンティティー・タイプのスキーマに関連付けられた属性のみを受け入れます。

また、環境データや外部データをフィルターに組み込む必要もあります。例えば、現在時刻や、顧客データベースから取得した値を組み込むことが必要です。このデータを組み込むためには、フィルター内にマクロを組み込む必要があります。 例えば、最近 30 日以内にパスワードが変更されたかどうかを検証するフィルターは、(erPswdLastChanged>=${system.date - 30}) のようになります。

注: フィルターを空白のままにすると、すべてのエンティティーが戻されます。エンティティー・リレーションシップ・マクロをライフ・サイクル・ルール・フィルターで使用できます。

イベントの時間間隔の定義は、次のオプションから構成できます。

日次 ライフ・サイクル・イベントを毎日起動します。このオプションを選択した後で、クロック・アイコンをクリックして、「**現時点**」フィールド内に時刻を指定します。

週次 ライフ・サイクル・イベントを週に 1 回起動します。このオプションを選択した後で、「**曜日**」リストから曜日を選択し、クロック・アイコンをクリックして、「**次の時刻**」フィールド内に時刻を指定します。

月次 ライフ・サイクル・イベントを月に 1 回起動します。このオプションを選択した後で、「**日**」リストから日を選択し、クロック・アイコンをクリックして、「**次の時刻**」フィールド内に時刻を指定します。

毎時 ライフ・サイクル・イベントを 1 時間に 1 回起動します。このオプションを選択した後で、「**分**」リストから時刻を選択します。

年次 その年の特定の日時にライフ・サイクル・イベントを起動します。 このオプションを選択した後で、「**月**」リストから月を選択します。次に、「**日**」リストから日を選択し、クロック・アイコンをクリックして「**次の時刻**」フィールド内に時刻を指定します。

特定の月の間
特定の月、日、時刻にライフ・サイクル・イベントを起動します。このオプションを選択した後で、「**月**」リストから月を選択します。次に、「**曜日**」リストから曜日を選択し、クロック・アイコンをクリックして「**次の時刻**」フィールド内に時刻を指定します。

毎四半期
年に 4 回、四半期の特定の日時にライフ・サイクル・イベントを起動しま

す。調整は、1 月 1 日、4 月 1 日、7 月 1 日、および 10 月 1 日以降の指定日にそれぞれ実行されます。このオプションを選択したら、「**日**」リストから日を選択し、クロック・アイコンをクリックして、「**現時点**」フィールドに時刻を指定します。

毎半期 年に 2 回、半期の特定の日時にライフ・サイクル・イベントを起動します。調整は、1 月 1 日以降と 7 月 1 日以降の指定日に実行されます。このオプションを選択したら、「**日**」リストから日を選択し、クロック・アイコンをクリックして、「**現時点**」フィールドに時刻を指定します。

注: スケジュールは複数指定できます。

ライフ・サイクル・ルールの評価スケジュールには、対応するルール定義へのリファレンス 1 つのみが含まれます。スケジュールされた評価が開始される前にライフサイクル・ルールの定義を変更した場合、その評価では更新されたバージョンのルール定義が使用されます。最初にスケジュールされたルール定義は使用されません。

この例では、ライフサイクル・ルールが作成されます。このルールでは、90 日以内にパスワードが変更されたことがないアカウントがないかどうか、1 日に 1 度確認します。ライフサイクル・ルールの検索基準に合致するアカウントの所有者には電子メール通知が送信され、パスワードを変更する必要があることが知らされます。

最初に、`remindToChangePassword` という名前の、アカウント・エンティティー・タイプのライフ・サイクル操作を構成します。 この操作は、(static ではなく) インスタンス・ベースの操作として定義されるため、入力パラメーターとしてアカウント・オブジェクト自体を持ちます。この操作のビジネス・ロジックは、アカウントの所有者にリマインダー・メッセージを送信する 1 つの作業命令アクティビティーによって定義されています。メッセージには、アカウントのユーザー ID が含まれています。

次に、`remindToChangePassword` 操作を参照する `passwordExpiration` という名前のアカウント・エンティティー・タイプのライフサイクル・ルールが構成されます。このルールには、**毎日午前 12 時**という評価間隔のイベントが含まれます。さらに、`(&(erAccountStatus=0)(erPswdLastChanged<=${system.date - 90}))` というフィルターも定義されています。

ライフサイクル・ルールの処理

ライフサイクル・ルール操作では、ライフサイクル・ルール・フィルターの評価から結果セット全体が戻されるまでに要する時間が長くなる可能性があります。

完了は主に、操作に関連付けられた手動ワークフロー・アクティビティーを完了するための所要時間によります。ライフサイクル・ルールの評価は、最初のライフサイクル・ルールの評価の結果と発生する操作がすべてのターゲットで完了する前に再び実行されるように、スケジュールするか、または手動で開始することができます。ライフサイクル・ルール評価の 2 回目の反復実行では、最初の評価から処理状態のまま残っているターゲットを識別します。2 回目の反復実行では、それらのタ

ーゲットでライフサイクル操作を再び開始しません。ただし、2 回目のライフ・サイクル・ルールの評価で、処理状態ではないと識別した各ターゲットに対してはライフ・サイクル操作を開始します。

例えば、ライフサイクル・ルールで、その基準に一致するエンティティーが 100 個検出されたとします。そのルールは、それら 100 個のエンティティーに関連付けられている操作を開始します。10 個のエンティティーがシステムに追加されると仮定します。追加処理は、最初のライフサイクル評価の後と、ライフサイクル・ルール操作が元の 100 エンティティーに適用されている間に行われます。ライフサイクル・ルールの 2 回目の反復実行は、最初の反復実行が完了する前に開始されます。2 回目の反復実行では、最初の反復実行で開始されたライフサイクル・ルールの操作があるすべてのエンティティーをスキップします。2 回目の反復実行では、ライフサイクル・ルール・フィルター評価に一致しても、現時点ではこのライフサイクル・ルール (ルール名で一致する) が実行されていないエンティティーを発見するまで、エンティティーをスキップします。この例の場合、2 回目の反復実行では、追加された 10 個の新規エンティティーを発見し、それに対してライフ・サイクル・ルール操作を開始します。

この動作を理解することが重要です。最初のライフ・サイクル・ルールが完了する前に、2 回目のライフ・サイクル・ルールが完了する場合があるからです。理論上、午前 10 時にスケジュールしたライフ・サイクルルールの評価が、午前 9 時にスケジュールしたライフサイクル・ルールの評価より前に完了することがあります。同じライフサイクル・ルールの後続の反復実行が完了しても、それに基づいてすべての関連ターゲットでライフサイクル・ルールの操作が完了したとは考えないでください。完了した要求項目および無視された項目を確認するには、完了した要求の監査ログを確認します。

ライフサイクル・ルールの変更

ライフサイクル・ルールのフィルターまたは操作に対する変更は、ライフサイクル・ルールが次に評価されるまで有効になりません。

ライフサイクル・ルールは、変更が加えられるときに、システムによる評価の真っ最中である場合があります。その時実行中の評価では、処理が完了するまで、ライフサイクル・ルールの以前の定義を使用し続けます。ライフサイクル・ルールがシステムによって評価されている最中に、操作のワークフローが変更されることがあります。その変更は、変更が加えられたどの時点であっても、その時点で実行中の評価に反映されます。例えば、ライフサイクル・ルール・フィルターで 50 人の個人を識別し、そのライフサイクル・ルール操作に `Recertify` という名前が付いているとします。操作名を `CheckPassword` に変更しても、その時点で行われているルールの反復実行には影響しません。変更は、次にルールが開始されたときに反映されます。一方、`Recertify` 操作がアクティブの間にその操作のワークフローを変更すると、25 人は元のワークフローで処理されます。残りの 25 人は、新しいワークフローで処理されます。

ライフサイクル・ルールのインプリメンテーションは、データベースにスケジューリング情報を含めることに大きく依存しています。ライフ・サイクル・ルールのスケジューリング情報を含んでいるテーブルを削除、ダンプ、またはパージすると、

関連するライフ・サイクル・ルールが非活動化されます。これらの変更が発生した場合は、すべてのライフサイクル・ルールを再構成し、それらのスケジュールを再定義する必要があります。

ライフサイクル・ルールに関連付けられている操作を削除したり、名前を変更したりすると、ライフサイクル・ルールが再構成されるまではそのルール内で操作をインプリメントすることができません。

注: エンティティーのライフサイクル・ルールを追加または変更する場合、その更新内容はキャッシュのタイムアウト後 (デフォルトでは 10 分) に有効になります。

ライフ・サイクル・イベントのスキーマ情報

IBM Security Identity Manager では、ライフ・サイクル・イベントの作成を容易にする固有のスキーマ属性を提供しています。

これらの属性は、IBM Security Identity Manager Server により管理され、データ・サービスを介し利用したり、ライフ・サイクル・イベント・インターフェースから利用できます。以下は追加のリストです。

- erPersonItem
  - erCreateDate – 個人がシステムに追加された日付
  - erLastStatusChangeDate – 個人の状態が最後に変更された日付。個人が復元またはサスペンドされた際には、必ずタイム・スタンプが更新されます。
  - erlastoperation – カスタム使用の場合に使用可能
  - erpswdlastchanged – 個人の同期パスワードが最後に変更された日付
- erAccountItem
  - erCreateDate – システムにアカウントが追加された日付
  - erLastStatusChangeDate – アカウントの状態が最後に変更された日付。アカウントが復元またはサスペンドされた際には、必ずタイム・スタンプが更新されます。
  - erlastoperation – カスタム使用の場合に使用可能

カスタム使用アイテムを除いて、これらのスキーマ・アイテムはシステムが管理します。

エンティティーのライフ・サイクル・ルールの追加

以下の説明に従って、エンティティーのライフ・サイクル・ルールを定義します。

始める前に

このタスクを実行できるのは、システム管理者のみです。

このタスクについて

ライフ・サイクル・ルールは、「操作の管理」タスクで定義した操作を起動します。ライフ・サイクル・ルールのタイプに従って、該当のレベルに定義されている対応する操作が使用可能です。

ライフサイクル・ルールは操作とは異なります。エンティティー・タイプまたはエンティティーのレベルで定義されたライフ・サイクル・ルールは、より高いレベルで定義されたライフ・サイクル・ルールをオーバーライドしません。各レベルには、定義されたスケジュールに基づいて独立して実行できる有効なライフサイクル・イベントがあります。

エンティティー・タイプのライフ・サイクル・ルールを追加するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**ライフ・サイクル・ルールの管理**」をクリックします。 「ライフ・サイクル・ルールの管理」ページが表示されます。
2. 「ライフ・サイクル・ルールの管理」ページで、以下のいずれかのライフ・サイクル・ルール・レベルを選択します。
   - エンティティー・コンテキストを持たないライフ・サイクル・ルールを定義するには、「**グローバル・レベル**」を選択します。
   - エンティティー・タイプに適用可能なライフ・サイクル・ルールを定義するには、「**エンティティー・タイプ・レベル**」を選択します。「**エンティティー・タイプ**」のリストからエンティティーのタイプを選択します。
   - 特定のエンティティー・インスタンス・タイプに適用可能なライフ・サイクル・ルールを定義するには、「**エンティティー・レベル**」を選択します。「**エンティティー・タイプ**」リストからエンティティー・タイプを選択してから、「**エンティティー**」リストからエンティティーを選択します。
3. 「**追加**」をクリックします。 「ライフ・サイクル・ルールの管理」ノートブックが表示されます。
4. 「ライフ・サイクル・ルールの管理」ノートブックの「**一般**」ページで、以下の手順を実行します。
   a. 「**名前**」フィールドに、対応するシステム・エンティティーに定義するライフ・サイクル・ルールの固有の名前を入力します。
   b. オプション: 「**説明**」フィールドに、ライフ・サイクル・ルールの説明を入力します。
   c. 「**操作**」リストから、イベントが発生した際に呼び出される操作を選択します。 ライフ・サイクル・ルールで実行できるのは、入力パラメーターを使用しない操作のみです。
   d. 「**イベント**」タブをクリックします。
5. 「ライフ・サイクル・ルールの管理」ノートブックの「**イベント**」ページで、以下の手順を実行します。
   a. 「**検索フィルター**」フィールドに、イベントによって影響を受けるオブジェクトを識別する、LDAP フィルターを入力します。 例えば、以下のフィルターは、過去 90 日間にパスワードを変更していないアクティブな従業員をすべて収集します。収集は、ライフ・サイクル・イベント発生日から起算されます。`(&(employeeType=active)(erPswdLastChanged<=${system.date - 90}))`

注: グローバル・レベルのライフ・サイクル・ルールはエンティティー・コンテキストを持たないため、検索フィルターを適用することはできません。

b. 「**追加**」をクリックして、ライフ・サイクル・ルールのスケジュールを定義します。 「スケジュールの定義」ページが表示されます。

6. 「スケジュールの定義」ページで、ライフ・サイクル・ルールを実行するスケジュールを定義し、「**OK**」をクリックします。 表示されるフィールドは、選択したスケジューリング・オプションによって変わります。 「ライフ・サイクル・ルールの管理」ノートブックの「**イベント**」ページに、新規のスケジュールが表示されます。
7. 「**OK**」をクリックして、ライフ・サイクル・ルールを保存し、ノートブックを閉じます。

タスクの結果

エンティティーのライフ・サイクル・ルールが正常に作成されたことを示すメッセージが表示されます。「**クローズ**」をクリックします。

次のタスク

「ライフ・サイクル・ルールの管理」ページが表示されたら、「**リフレッシュ**」をクリックして、「**ライフ・サイクル・ルール**」テーブルをリフレッシュします。新規のライフ・サイクル・ルールが表示されます。

エンティティーのライフ・サイクル・ルールの変更

以下の説明に従って、ライフ・サイクル・ルールを変更します。

始める前に

このタスクを実行できるのは、システム管理者のみです。

このタスクについて

エンティティー・タイプのライフ・サイクル・ルールを変更するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**ライフ・サイクル・ルールの管理**」をクリックします。 「ライフ・サイクル・ルールの管理」ページが表示されます。
2. 「ライフサイクル・ルールの管理」ページで、変更するライフサイクル・ルールの横のチェック・ボックスを選択してから、「**変更**」をクリックします。 「ライフ・サイクル・ルールの管理」ノートブックが表示されます。
3. 「**一般**」タブまたは「**イベント**」タブをクリックします。
4. 必要な変更を行ってから「**OK**」 をクリックします。

タスクの結果

エンティティーの新規のライフ・サイクル・ルールが正常に更新されたことを示すメッセージが表示されます。「**クローズ**」をクリックします。

次のタスク

「ライフ・サイクル・ルールの管理」ページが表示されたら、「**リフレッシュ**」をクリックして、「**ライフ・サイクル・ルール**」テーブルをリフレッシュします。

エンティティーのライフ・サイクル・ルールの削除

この説明に従って、ライフ・サイクル・ルールを削除します。

始める前に

このタスクを実行できるのは、システム管理者のみです。

このタスクについて

エンティティー・タイプのライフ・サイクル・ルールを削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**ライフ・サイクル・ルールの管理**」をクリックします。 「ライフ・サイクル・ルールの管理」ページが表示されます。
2. 「ライフ・サイクル・ルールの管理」ページで、削除するライフ・サイクル・ルールの横のチェック・ボックスを選択してから「**削除**」をクリックします。 この列の上部にあるチェック・ボックスを選択すると、すべてのライフ・サイクル・ルールが選択されます。
3. 「確認」ページで「**削除**」をクリックしてライフ・サイクル・ルールを削除するか、「**キャンセル**」をクリックします。

タスクの結果

エンティティーのライフ・サイクル・ルールが正常に削除されたことを示すメッセージが表示されます。「**クローズ**」をクリックします。

次のタスク

「ライフ・サイクル・ルールの管理」ページが表示されたら、「**リフレッシュ**」をクリックして、「**ライフ・サイクル・ルール**」テーブルをリフレッシュします。

エンティティーのライフ・サイクル・ルールの実行

この説明に従って、ライフ・サイクル・ルールを実行します。

始める前に

このタスクを実行できるのは、システム管理者のみです。

このタスクについて

ライフ・サイクル・ルールを実行すると、定義したスケジュールに従ってではなく、即座にイベントが起動されます。

エンティティー・タイプのライフ・サイクル・ルールを実行するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**ライフ・サイクル・ルールの管理**」をクリックします。 「ライフ・サイクル・ルールの管理」ページが表示されます。
2. 「ライフサイクル・ルールの管理」ページで、実行するライフ・サイクル・ルールの横のチェック・ボックスを選択してから「**実行**」をクリックします。
3. 「確認」ページで「**実行**」をクリックしてライフ・サイクル・ルールを実行するか、「**キャンセル**」をクリックします。

タスクの結果

ライフ・サイクル・ルールの実行が正常に実行依頼されたことを示すメッセージが表示されます。「**クローズ**」をクリックします。

次のタスク

「ライフ・サイクル・ルールの管理」ページが表示されたら、「**リフレッシュ**」をクリックして、「**ライフ・サイクル・ルール**」テーブルをリフレッシュします。

LDAP フィルター式

IBM Security Identity Manager には、汎用 RFC 2254 LDAP フィルターおよび RFC により定義されたフィルター構文に対する 2 つのカスタム拡張に対する組み込みインタープリターが用意されています。

第 1 の拡張では、IBM Security Identity Manager関係を参照する LDAP フィルター内の変数の記法が規定されています。それらの変数は、関連オブジェクトまたは接続済みオブジェクトに解決されます。第 2 の拡張では、現在の日付と時刻に解決される日付キーワード、およびシステム・オブジェクトを参照する LDAP フィルター内の変数の記法が規定されています。LDAP フィルター構文に対するこの 2 つの拡張は、実行時に解釈、評価されるもので、*フィルター式*の形式をとります。このフィルター式を使用すると、アドミニストレーターは、IBM Security Identity Manager における有効な抽象を参照する動的なパーツでフィルターを定義することができます。サポートされている 2 つのタイプのフィルター式は、*関係式*とシステム式です。

関係式

IBM Security Identity Manager ドメイン・オブジェクト間の接続は、関係によって決まります。

例えば、アカウントの所有者は、所有者関係によって決まります。アカウントのホスト・サービスは、サービス関係によって決まります。個人の役割は、役割関係によって決まります。

一般的に、以下のとおりです。

ターゲット・オブジェクト	関係	関連オブジェクト

例えば、以下のとおりです。

個人	役割	役割

ここでは、個人は、役割関係によって役割に関連していることになっています。フィルター内の関係式は、他のドメイン・オブジェクトとの関係に基づいて、ドメイン・オブジェクトにマッチングする方法を提供します。

IBM Security Identity Manager ドメイン・オブジェクト間の接続は、関係によって決まります。

フィルター式の構文は、ドル記号 ($) が先頭に来て、左方の中括弧 ({) が続き、直後に関係名、ドット (.) 演算子、および属性名、そして式を終了する右方の中括弧 (}) で構成されます。例えば、以下のとおりです。

```
(${relationship.attribute}=value)
```

relationship は、IBM Security Identity Manager での関係の名前です。

- 親
- 所有者
- 組織
- スーパーバイザー
- スポンサー
- 管理者
- 役割
- アカウント
- サービス

attribute は、関連オブジェクトに有効な任意の属性名です。これらの接続への参照、またはドメイン・オブジェクト間のリンクは、検索で役立ちます。参照は、(ACI での) 許可処理中の突き合せや、操作実行中のライフサイクル管理 (ライフサイクル・ルール) でも役立ちます。

ACI では、関係式は、一部他のドメイン・オブジェクトとの関係に基づいて、ドメイン・オブジェクトに対するアクセスを認可するために使用されます。例えば、以下の関係式を ACI フィルターとして使用して変更を認可する個人の ACI により、Jen Jenkins という共通名のスーパーバイザーが存在する個人全員に許可が付与されます。

```
(${supervisor.cn}=Jen Jenkins)
```

同様に、以下の関係式を ACI フィルターとして使用して検索を認可する次のアカウント向け ACI では、サービス (ホスト) 名が SuSE Server であるすべてのアカウントに許可が与えられます。アクセス権は、オブジェクトと別のオブジェクトの関係に基づいて付与されます。

```
(${service.erservicename}=SuSE Server)
```

ライフサイクル管理では、管理式がライフサイクル・ルールでも使用され、他のドメイン・オブジェクトとの関係に基づいてドメイン・オブジェクトのマッチングが行われます。ルールにより、すべての一致で同じ操作を開始できます。例えば、ルールとして使用される関係式によって操作がサスペンドに設定される個人のライフ・サイクル・ルールでは、ライフ・サイクル・ルールが実行されるたびに、(動的または静的に) Brokers 役割に属するすべての個人が効率的にサスペンドされます。

```
(${role.errolename}=Brokers)
```

関係式の評価

関係式を評価するとは、「はい」または「いいえ」形式の質問に 4 ステップで回答することであると考えることができます。

4 つのステップは、以下のとおりです。

- 何が加わるのか (式自体)
- マッチング対象は何か (ターゲット・オブジェクト)
- 結果は何か (接続済みオブジェクトまたは関連オブジェクト)
- 関連オブジェクトは、等号の右辺の値と一致するか

一致する場合は、評価の回答は、「はい」であり、ターゲット・オブジェクトは、関係式に一致するといわれます。

次の表の 1 番目の列には、サンプル・フィルターで使用されている関係式がリストされています。 2 番目の列には、その式で有効なオブジェクトのタイプがリストされます。3 番目の列には、関係が指し示すオブジェクトのタイプが示されます。

表 26. サンプル・フィルターの関係式

関係式	ターゲット・オブジェクト	関連オブジェクト
(${parent.ou}=Sales)	任意 (アカウントを除く)	任意のコンテナー
(${owner.cn}=John Smith)	アカウント	個人
(${organization.o}=Marketing)	任意 (アカウントを除く)	組織
(${supervisor.cn}=Jen Jenkins)	任意 (アカウントを除く)	個人
(${sponsor.cn}=Pete West)	任意 (アカウントを除く)	個人
(${administrator.cn}=Joe Peterson)	任意 (アカウントを除く)	個人
(${role.errolename}=Brokers)	任意 (アカウントを除く)	役割
(${account.uid}=JUser)	任意 (アカウントを除く)	アカウント
(${service.erservicename}=SuSE Server)	アカウント	サービス

関係式の作成時には、評価ステップに留意することが重要です。中でも重要なのは、ドット (.) 演算子の後の有効な属性名を参照するために、関連オブジェクト・タイプを把握しておき、式を適格、有効に構成し、一致が必ず見つかるようにすることです。ここでの参照資料として LDAP スキーマに目を通しておくと役に立ちます。システムは、フィルター基準を満たす最初のエンティティーに関係式を解決します。その後、そのエンティティーのフィルターに指定されている関係を持つすべてのオブジェクトに対して照会を行います。対象のエンティティーが戻るよう、十分に具体的なフィルターを作成してください。

name キーワード

関係式の構文の変化形の一つとして、ドット (.) 演算子の後に特殊な name キーワードを組み込む構文があります。

ドット (.) 演算子の後に name キーワードを指定すると、プロファイル内の名前属性が参照されます。この構文は、明示的な属性名を使用するのではなく、名前によってオブジェクトを指し示す一般的な方法です。ただし、一般的に、評価時にプロファイルが既知であるコンテキストに限り有効であるという制限があります。

例えば、Lotus Notes アカウントに対する ACI が存在するとします。この ACI は、アカウントの変更権限を許可し、以下のフィルターを使用します。

```
(${service.name}=SuSE Server)
```

この name キーワードは、Lotus Notes サービスのプロファイル名前属性を参照します。このコンテキストでは、name の使用が有効です。権限許可時 (評価時) には、Lotus Notes サービス・プロファイルは常に既知であり、その name 属性が解決可能です。name キーワードは、特定のプロファイル内の名前属性に対する参照が、ライフ・サイクル・ルールの実行時に未確定であるため、ライフ・サイクル・ルールでは無効です。したがって、名前属性を解決できません。

システム式

システム式は、現在のシステム日付に相対する一般化時刻値に基づいて、ドメイン・オブジェクトを対象にするために使用されます。

システム式の構文では、比較的少数のエレメントを使用します。

システム式は次のエレメントで構成されています。

属性名

関係演算子 (<= or >=)

ドル記号 ($)、それに続く中括弧 ({)

その直後に system.date キーワード

正号または負号の算術演算子 (+/-)、それに続く日数

式を閉じる右中括弧 (})

例えば、以下のとおりです。

```
(gmtattributename[<=|>=]${system.date [ + | - ] days})
```

システム式は、具体的な LDAP フィルターに解決され、これは、LDAP ディレクトリー・サーバーまたは組み込み IBM Security Identity Manager フィルター・インタープリターによって認識されます。例えば、このフィルターの対象は、パスワードが 90 日以上経過したアカウントです。

```
(erpswdlastchanged<=${system.date - 90})
```

この例は、ユーザーがパスワードを更新することができるよう、パスワード属性に読み取り/書き込みアクセス権を付与するアカウントの ACI で使用できます。同じフィルターを、アカウントのパスワードが、最近 90 日間に変更されなかった場合

に、そのアカウントをサスペンドするライフ・サイクル・ルールで使用することもできます。このフィルター式自体は、以下の具体的な LDAP フィルターに解決されます。

```
(erpswdlastchanged<=200912311200Z)
```

また、ドメイン・オブジェクトとの突き合せのために、一定範囲の日付を基準として指定することが可能であり、構文的に有効です。次の例に示すように、複数のシステム式を複合フィルターに組み込みます。

```
(&(erpswdlastchanged>=${system.date - 90})(!(erpswdlastchanged>
=${system.date - 30})))
```

このフィルターは、30 日から 90 日までの日数が経過したパスワードを持つアカウントに一致します。その他の組み合わせや複合フィルターも、フィルターを複雑にする必要のある程度や、マッチングの対象にするオブジェクトの個数に応じて便利に使用できます。

第 13 章 ポリシー結合ディレクティブ構成

プロビジョニング・ポリシー結合ディレクティブ により、同じアカウントに複数のプロビジョニング・ポリシーが影響する場合に、支配するプロビジョニング・パラメーター値が決定されます。結合ディレクティブは、プロビジョニング・ポリシー間で競合が生じた場合の属性の処理方法を定義します。選択した属性にのみ適用できる結合ルールが表示されます。

資格ターゲット・タイプは、ポリシー間で矛盾が発生した場合に付与する資格をポリシー結合ディレクティブが決定する上でも、ある役割を果たします。複数のポリシーが同様な資格を付与する場合には、特定度の高い方の資格が優先されます。例えば、プロビジョニング・ポリシーに、任意のタイプのサービス (つまり、AIX105 という名前の AIX®) にアクセス権を付与するよう定義された資格が組み込まれているとします。2 番目のポリシーには、そのサービス (つまり、AIX) の特定のインスタンスへのアクセス権を付与するように定義された資格が組み込まれています。この場合、より具体的な資格が優先されます。

IBM Security Identity Manager には、複数のタイプの結合ディレクティブが用意されています。次の表は、各タイプとその説明のリストです。

注: Union タイプおよび Intersection タイプは、多値属性に対してのみ定義されます。

表 27. 結合ディレクティブ

結合ルール	説明
Union	属性値を結合して、冗長を除去します。 他の結合ディレクティブが指定されていない場合は、この結合ディレクティブが多値属性のデフォルト・パラメーターです。
Intersection	すべてのポリシーに共通のパラメーター値のみです。
Append	あるポリシーに定義されたテキスト属性値を、別のポリシーに定義された属性値に付加します。 APPEND 結合タイプは、winlocal サービスに対するコメントなどの一価テキスト属性で使用するように設計されました。 APPEND 結合タイプを使用してプロビジョニング・パラメーターを結合すると、個々の値すべてが 1 つのストリング値として連結されます。連結により、値間のユーザー定義区切り文字を提供します。区切り文字は、enrolepolicies.properties ファイルで定義 (変更) できます。現時点では次の行が記述されています。 provisioning.policy.join.Textual.AppendSeparator=<<<>>>
And	ブール値を表すブール・ストリングに使用される数学的な AND を指定します。TRUE & TRUE = TRUE TRUE & FALSE = FALSE FALSE & FALSE = FALSE
Or	ブール値を表すブール・ストリングに使用される数学的な OR を指定します。TRUE ‖ TRUE = TRUE TRUE ‖ FALSE = TRUE FALSE ‖ FALSE = FALSE

表 27. 結合ディレクティブ (続き)

結合ルール	説明
Highest	競合するポリシーの中から最大の数値属性値のみを使用します。
Lowest	競合するポリシーの中から最小の数値属性値のみを使用します。
Average	競合するポリシーから数値属性値を平均して、平均値を使用します。
Bitwise_Or	ビット・ストリングを表す属性値に使用される数学的なビット単位 OR を指定します。
Bitwise_And	ビット・ストリングを表す属性値に使用される数学的なビット単位 AND を指定します。
Precedence_Sequence	ユーザー定義順の優先順位を使用して、使用する属性値を決定します。
Priority	ポリシーの優先順位を使用して、使用する属性値を決定します。競合するポリシーの優先順位が同じ場合、それらの競合ポリシーが評価されるときの順序は無作為です。評価は、システムが最初に検索するポリシーに基づいて行われます。例えば、2 つのポリシーの優先順位が同じで、同じ属性を異なる値で定義しているとします。その属性で「優先順位」結合ルール・タイプを使用する場合、ポリシーによって戻される属性値は、システムの検索に基づいて異なります。

以下の表に、サービス属性の各タイプ、対応する結合ディレクティブ、およびデフォルトの結合ディレクティブを示します。

表 28. サービス属性

サービス属性タイプ	適用できる結合ディレクティブ	デフォルト結合ディレクティブ
多値のストリングまたは数値属性	UNION、 INTERSECTION、 PRIORITY、 CUSTOM	UNION
一価ストリング	PRECEDENCE_SEQUEN CE、 PRIORITY、 AND、OR、 APPEND、 BITWISE_AND、 BITWISE_OR、 HIGHEST、 LOWEST、 AVERAGE、 CUSTOM	PRIORITY
一価ブール・ストリング	AND、 OR、 PRIORITY、 CUSTOM	OR
一価整数	HIGHEST、 LOWEST、 AVERAGE、 PRIORITY、 PRECEDENCE_SEQUENCE、 CUSTOM	HIGHEST
一価ビット・ストリング	BITWISE_AND、BITWISE_OR、 PRIORITY、CUSTOM	BITWISE_OR

注: カスタム結合ディレクティブは Java を使用して定義できます。アドミニストレーターは、カスタム結合ディレクティブを使用して、標準装備の結合ロジックを完全に変更できます。

ポリシー結合動作のカスタマイズ

サービス・タイプに基づいて、各属性に対するプロビジョニング・ポリシーの結合ディレクティブの動作をカスタマイズできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

IBM Security Identity Manager には、複数のタイプの結合ディレクティブが用意されています。既存の結合ディレクティブ機能を拡張するか、独自の結合ディレクティブ機能を作成することができます。

カスタム結合ディレクティブを定義するには、カスタム Java クラスを記述して、アプリケーション・サーバーのクラスパスに追加します。属性の結合ディレクティブの設定時に、その完全修飾 Java クラス名をポリシー構成インターフェースで指定します。

既存の結合ディレクティブ・クラスの 1 つを拡張または置換する場合は、上記の作業に加えて、カスタム・プロパティー・キーおよび値を `enrolepolicies.properties` ファイルに追加する必要があります。例えば、新しいクラス (`com.abc.TextualEx`) を開発してテキスト結合用の既存のクラスを置換する場合は、以下の例のような登録行を使用します。

```
provisioning.policy.join.Textual= com.abc.TextualEx
```

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**ポリシー結合動作の構成**」を選択します。プロビジョニング・ポリシー結合ディレクティブを構成するためのポリシー結合動作テーブルは、ウィンドウに 2 つの画面区画として表示されます。
2. 「ポリシー結合動作」ウィンドウで、「**サービス・タイプ**」をクリックして、使用可能なサービス (`ITIMService` など) のリストから選択します。
3. タイプに対応するいずれかの属性を選択します。右画面区画には、選択した属性の名前、記述、および適用できる結合ディレクティブが表示されます。
4. 右画面区画の「**結合ルール**」をクリックし、リストされているいずれかの結合ディレクティブを選択することによって、プロビジョニング・ポリシーの優先順位を構成します。選択した属性に応じて、以下の値を適用できます。

   和集合 属性値を指定して、重複している値を除去します。この結合ディレクティブは、他の結合ディレクティブが指定されていない場合のデフォルトです。

   論理積 すべてのポリシーに共通するパラメーター値のみを指定します。

   優先順位
   ポリシーの優先順位を使用して、使用する属性値を決定します。矛盾するポリシーに同じ優先順位がある場合には、システムによって最初に検出されたポリシーが使用されます。

OR ブール値を表すブール・ストリングに使用される数学的な OR を指定します。TRUE || TRUE = TRUE TRUE || FALSE = TRUE FALSE || FALSE = FALSE

AND ブール値を表すブール・ストリングに使用される数学的な AND を指定します。TRUE & TRUE = TRUE TRUE & FALSE = FALSE FALSE & FALSE = FALSE

付加 あるポリシーに定義されたテキスト属性値を、別のポリシーに定義された属性値に付加します。

APPEND 結合タイプは、一価テキスト属性 (WinNT サービスに対する `comment` など) に使用されます。

APPEND 結合タイプを使用してプロビジョニング・パラメーターを結合した場合、個々の値がすべて連結され、ユーザー定義区切り文字が間に入れられて 1 つの文字列値になります。区切り文字は、enrolepolicies.properties ファイルで定義 (変更) できます。現時点では次の行が記述されています。

```
provisioning.policy.join.Textual.AppendSeparator=<<<>>>
```

ビット単位 OR
ビット・ストリングに使用される数学的なビット単位 OR を指定します。

ビット単位 AND
ビット・ストリングに使用される数学的なビット単位 AND を指定します。

最高 競合するポリシーの中から最大の数値属性値を使用します。

最低 競合するポリシーの中から最小の数値属性値を使用します。

平均 競合するポリシーから数値属性値を平均して、平均値を使用します。

優先順位シーケンス
ユーザー定義順の優先順位を使用して、使用する属性値を決定します。

カスタム
Java を使用してカスタム結合ディレクティブを定義します。カスタム結合ディレクティブにより、アドミニストレーターは、組み込み結合ロジックを完全に変更することができます。属性に対して作成したカスタム結合ディレクティブ・クラスの完全修飾 Java クラス名を入力します。

5. 「**準拠アラート・ルール**」をクリックして、いつ準拠アラートを送信するのかを指定する準拠アラート・ルールを構成します。準拠アラート・ルールを構成するには、以下のいずれかのオプションを選択します。

数値順 (より高い値の場合にアラートを生成)
このオプションは、より高い属性値を管理対象リソースに送信する前に準拠アラートを生成する場合に選択します。このオプションは、プロビジョニング・ポリシー評価の結果として属性値が増加した場合に使用します。評価の結果として属性値が減少すると、属性値が管理対象リソースに自動的に送信されます。アラートは生成されません。

数値順 (より低い値の場合にアラートを生成)
このオプションは、より低い属性値を管理対象ノードに送信する前に準

拠アラートを生成する場合に選択します。このオプションは、プロビジョニング・ポリシー評価の結果として属性値が減少した場合に使用します。評価の結果として属性値が増加すると、属性値は管理対象リソースに自動的に送信され、アラートは生成されません。

アラートを生成しない
このオプションは、プロビジョニング・ポリシー評価によって属性の値が新しい値になる可能性がある場合、準拠アラートを生成しない場合に選択します。準拠アラートが生成されないので、新しい属性値は管理対象リソースに自動的に送信されます。

常にアラートを生成する
このオプションは、プロビジョニング・ポリシー評価で属性の値が新しい値になる可能性がある場合、準拠アラートを生成する場合に選択します。参加者は新規属性値を管理対象リソースに送信する前に受信する必要があります。この値は、単一値を持つ属性のデフォルトです。

優先順位シーケンス
このオプションは、リスト中の高い方の値が低い値より多くの特権を持つとする場合に選択します。プロビジョニング・ポリシー評価でより高い値が割り当てられる可能性がある場合、属性値は管理対象リソースに送信されます。準拠アラートは生成されません。評価の結果として属性値が減少すると、準拠アラートが生成されます。次に、この属性値は、管理対象リソースに送信されます。

注: このオプションを選択した場合は、「**上に移動**」、「**下に移動**」、「**削除**」、または「**追加**」を選択して優先順位を編成できます。

6. 「**保存**」をクリックして変更を保存します。

アカウントの妥当性検査ロジック

アカウントの妥当性検査ロジックでは、ポリシー結合ルールの適用後に、パラメーター値の結合セットに作用する一群の妥当性検査ルールについて説明します。

許可パラメーターと否認パラメーターの和集合

許可 パラメーター値のセットは、以下の要素の和集合です。

- 必須定数パラメーター値 (ヌルを除く)
- オプション定数パラメーター値 (ヌルを除く)
- オプションの制約付き非否定正規表現
- 除外ヌル値

否認 パラメーター値のセットは、以下の要素の和集合です。

- 除外制約付き非否定正規表現
- 除外定数値 (ヌルを除く)
- オプション、必須、またはデフォルトの制約付きヌル値

注: 否定正規表現、例えば、「ある語を除いて、すべてに一致する」などは、手動で作成することが困難な場合があります。オプション・パラメーターおよび除外パラメーターはお互いに補完し合うため、可能な限り同時に使用してください。

ヌル・パラメーター値

ヌル必須パラメーター値は、新規または既存アカウントの対応する属性の値が、その他のいずれかの有効な値によって許可されているものを除き、すべて禁止されることを意味します。既存アカウントの属性値が、ヌル必須パラメーターによって否認された場合、否認された属性値は自動的に除去されます。

ヌル・デフォルト・パラメーター値またはヌル・オプション・パラメーター値は、新規または既存アカウントの対応する属性の値が、その他の許可値によって許可されているものを除いて、すべて禁止されることを意味します。現在設定されている値は除去されません。

ヌル除外パラメーターは、新規または既存アカウントの対応する属性の値が、その他の否認パラメーター値によって否認されているものを除いて、すべて許可されていることを意味します。

一価属性における統括パラメーター値の効果

一価属性のパラメーター値は、必須制約またはデフォルト制約によってのみ限定できます。

必須パラメーター値は、その属性が、その示された値のみを持つ必要があることを意味します。統括必須パラメーター値に対する変更は、影響を受けるアカウントの属性に自動的に反映されます。必須パラメーター値を支配資格から除去すると、対応する属性を支配する別の必須パラメーターが存在しない場合は、その属性の値が自動的に変更される可能性があります。

デフォルト・パラメーター値は、新規アカウントのプロビジョニングで使用されます。デフォルト・パラメーターに支配される属性値は、許可パラメーター・セットの任意の値に、いつでも変更できます。デフォルト・パラメーター値を、支配しているパラメーターから除去しても、パラメーター結合ルールが使用されていない限り、対応する属性から値が除去されることはありません。別の必須パラメーターを介して、同じ属性が支配されるようになります。

多値属性に対する支配パラメーター値の効果

多値属性のパラメーター値は、必須、デフォルト、オプション、および除外の各制約タイプによって修飾できます。

必須パラメーター値は、対応する属性が、その値を常時持つ必要のあることを意味します。新規の何らかの必須値 (ヌルを除く) を追加すると、この値が自動的に既存のすべてのアカウントに追加されます。既存の必須パラメーター値 (ヌルを除く) を除去すると、同じ値に対して別の許可パラメーターが存在する場合を除き、その値が属性から自動的に除去されます。必須パラメーター値に対する 1 回の変更は、1 回の除去・追加操作と同等になります。

非ヌル・デフォルト・パラメーター値は、実質的には新規アカウントのプロビジョニングに限り有効になります。対応する属性値は、許可セットの任意の値に後で変更できます。新規デフォルト・パラメーター値 (ヌルを除く) を追加しても、準拠性の異なる属性には何の影響もありません。デフォルト・パラメーター値 (ヌルを除く) を除去しても、同じ値に対して別の許可 (非デフォルト) パラメーターが存在する場合を除き、その値が対応する属性から除去されることはありません。

オプショナル・パラメーター値

オプショナル・パラメーター値は、定数または正規表現として定義することが可能です。

何らかの新規オプション定数パラメーター値 (ヌルを除く) を追加しても、準拠性の異なる属性には影響しません。オプション定数パラメーター値 (ヌルを除く) を除去すると、別の許可パラメーターによって同じ値が許可されている場合でなければ、その値が対応する属性から除去されます。オプション定数パラメーター値に対する 1 回の変更は、1 回の除去・追加操作と同等になります。

新規オプション正規表現を追加しても、準拠性の異なる属性には何の影響もありません。オプション正規表現を除去または変更すると、同じ値に対して別の許可パラメーターが存在する場合でなければ、準拠性の異なる属性の属性値が除去されます。

除外パラメーター値

除外パラメーター値は、定数または正規表現として定義することが可能です。除外制約のあるパラメーター値は、暗黙的ワイルドカード資格のコンテキスト内に限り実行されます。

何らかの新規の除外定数パラメーター値を追加すると、同じ値に対する別の許可パラメーターが存在する場合を除き、その値が対応する属性から除去されます。除外定数パラメーター値 (ヌルを除く) を除去しても、準拠性の異なる属性には何の影響もありません。除外定数パラメーター値に対する 1 回の変更は、1 回の除去・追加操作と同等になります。

何らかの新規の除外正規表現を追加すると、同じ値に対して別の許可パラメーターが存在する場合を除き、準拠性の異なる属性の属性値が除去されることがあります。除外正規表現を除去または変更しても、準拠性の異なる属性には何の影響もありません。

否認よりも許可の方が高い優先順位ルール

競合するパラメーター値の存在によって、属性値が同時に許可および否認される場合は、許可パラメーター値の方が、否認パラメーター値よりも優先されます。

暗黙的ワイルドカード属性資格

デフォルトのすべて認可ポリシーを簡単に作成するために、 *暗黙的ワイルドカード* 属性資格を使用します。属性の暗黙的ワイルドカードはその属性上に許可パラメーター値が 1 つも定義されていない場合に存在します。したがって、各除外 (否認) パラメーター値を除くすべての値が許可されます。ある属性に対して最後のパラメーターを除去すると、暗黙的ワイルドカードが復元されます。

結合ディレクティブの例

このトピックでは、プロビジョニング・ポリシー結合ディレクティブの使用方法の例を示します。

次の例では、一価属性のデフォルト結合ディレクティブであるポリシー優先度を使用した競合解決を調べます。 Windows サーバー上の erMaxStorage 属性を使用して、ユーザーにサーバー上の限定されたストレージ・スペースを容量を割り当てます。

ポリシー 1

メンバーシップ
管理職

優先順位
1

erMaxStorage
1000 (MB)、実行: 必須

ポリシー 2

メンバーシップ
従業員

優先順位
2

erMaxStorage
200 (MB)、実行: 必須

管理職と従業員の両方の役割に個人が属する場合は、優先順位を使用して 2 つの erMaxStorage パラメーター値間の矛盾が解決されます。両方のグループに属する個人は、erMaxStorage 値の 1000 (MB) を受けることになります。

次の例では、一価属性のデフォルトでない結合ディレクティブである、優先順位を使用する競合解決を調べます。

ポリシー 1

メンバーシップ
管理職

優先順位
2

eraddialincallback
4、実行: 必須

ポリシー 2

メンバーシップ
従業員

優先順位
1

eraddialincallback
2、実行: 必須

eraddialincallback 属性上のカスタム結合ディレクティブ
優先順位 (最重要が先頭)

- **4** ユーザー・コールバック
- **2** 固定コールバック
- **1** コールバックなし

個人は、管理職と従業員の両方の役割に属する場合があります。この場合は、従業員のポリシーの優先度が高いとしても、2 つのパラメーター値の矛盾を解決するために優先順位シーケンスが使用されます。この個人は、`eraddialincallback` 値 4 (ユーザー・コールバック) を受け取ります。

結合ロジックの例

このトピックでは、プロビジョニング・ポリシー結合ディレクティブの使用方法の例を示します。

このセクションでは、結合ロジックの例をさらに示します。

シナリオ 1

複数の該当する資格が結合される場合があります。あるポリシー内の属性に対してパラメーター値が選択されておらず (すべての値が許可される)、別のポリシー内の属性に対して 1 つの許可パラメーター値が入力される (指定された値のみが許可される) 場合、そのパラメーター値は、2 番目のポリシーで指定された値のみをとることが許可されます。

シナリオ 2

この例では、一価属性における優先順位ベースのプロビジョニング・ポリシー結合ディレクティブを示します。以下の表に、このシナリオで使用する 2 つのプロビジョニング・ポリシーを示します。

表 29. 2 つのプロビジョニング・ポリシー

ポリシー	説明
ポリシー 1	優先順位 = 1 属性: erdivision = divisionA, enforcement = DEFAULT
ポリシー 2	優先順位 = 2 属性: erdivision = divisionB, enforcement = MANDATORY

ポリシー 1 の優先度が高いため、erdivision 属性のポリシー 1 の定義のみが使用されます。erdivision 属性のポリシー 2 の定義は無視されます。 divisionA 以外の値は、すべて却下されます。

シナリオ 3

この例では、多値属性における和集合ベースのプロビジョニング・ポリシー結合ディレクティブを示します。以下の表に、このシナリオで使用する 2 つのプロビジョニング・ポリシーを示します。

表 30. プロビジョニング・ポリシーの例

ポリシー	説明
ポリシー 1	優先順位 = 1 属性: localgroup = groupA, enforcement = DEFAULT
ポリシー 2	優先順位 = 2 属性: localgroup = groupB, enforcement = MANDATORY

結合ディレクティブは UNION として定義されているので、結果のポリシーはそのポリシーの次の定義を使用します。

- アカウントの作成時に、localgroup 属性は、groupA と groupB の両方の値を設定して定義されます。

- 調整時に、属性が未定義であるか、属性の定義に誤りがあれば、localgroup は、groupB として定義されます。

第 14 章 グローバル・ポリシー実行

IBM Security Identity Manager システムは、*グローバル・ポリシー実行* によってプロビジョニング・ポリシーに違反するアカウントをグローバルに許可するか、却下します。

ポリシー実行アクションがグローバルである場合は、すべてのサービスのポリシー実行がデフォルト構成設定により定義されます。非準拠属性を持つアカウントの場合に実行されるポリシー実行アクションを、以下のうちから 1 つ指定できます。

マーク 非準拠属性を持つアカウントにマークを設定します。

サスペンド
非準拠属性を持つアカウントをサスペンドします。

修正 アカウントの非準拠属性を正しい属性に置き換えます。

アラート
非準拠属性を持つアカウントに対するアラートを発行します。

注: サービスが特定のポリシー実行設定を持つ場合は、この設定が非準拠アカウントに適用されます。グローバル実行設定は、適用されません。

グローバル実行ポリシーの構成

アドミニストレーターは、サービス上の不適合アカウントを解決するグローバル実行ポリシーを作成できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

グローバル実行ポリシーの構成では、以下のオプションを使用できます。

- **マーク**
- **サスペンド**
- **修正**
- **アラート**

アカウントへのマークの設定

アドミニストレーターは、グローバル実行ポリシーを作成して、非準拠属性を持つアカウントにマークを設定できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

非準拠属性を持つアカウントにマークを設定するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**グローバル・ポリシー実行の構成**」を選択します。
2. 「グローバル・ポリシー実行の構成」ページの「実行アクション」セクションで「**マーク**」を選択してから、「**実行**」を選択します。

   注: システムのグローバル・ポリシー実行アクションを変更すると、アカウント準拠の再評価とアカウント・データの変更が行われる場合があります。
3. 「確認」ページで、この操作をスケジュールする日時を選択します。

   注: このオプションを選択すると、カレンダー・アイコンおよびクロック・アイコンを選択して予定の日時をカスタマイズできます。
   - 要求を即時実行する場合は、「**即時**」を選択してから「**実行**」を選択します。

     注: 現在の日時が表示されます。
   - カスタマイズした日時に要求を実行する場合は、「**発効日**」を選択してから「**実行**」を選択します。
4. 「成功」ページで、「**クローズ**」をクリックします。

アカウントのサスペンド

アドミニストレーターは、グローバル実行ポリシーを作成して、非準拠属性を持つアカウントをサスペンドできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

非準拠属性を持つアカウントをサスペンドするには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**グローバル・ポリシー実行の構成**」を選択します。

2. 「グローバル・ポリシー実行の構成」ページの「実行アクション」セクションで「**サスペンド**」を選択してから、「**実行**」を選択します。

   注: システムのグローバル・ポリシー実行アクションを変更すると、アカウント準拠の再評価とアカウント・データの変更が行われる場合があります。
3. 「確認」ページで、この操作をスケジュールする日時を選択します。

   注: このオプションを選択すると、カレンダー・アイコンおよびクロック・アイコンを選択して予定の日時をカスタマイズできます。
   - 要求を即時実行する場合は、「**即時**」を選択してから「**実行**」を選択します。

     注: 現在の日時が表示されます。
   - カスタマイズした日時に要求を実行する場合は、「**発効日**」を選択してから「**実行**」を選択します。
4. 「成功」ページで、「**クローズ**」をクリックします。

準拠属性による非準拠属性の置換

アドミニストレーターは、サービス上の禁止された不適合アカウントを解決するグローバル実行ポリシーを作成できます。このグローバル実行ポリシーは、適用可能ないずれのプロビジョニング・ポリシー資格によっても認可されないアカウントをプロビジョン解除できます。禁止アカウントは、除外アカウントの基準に合致する場合、リモート・サービスでの除去を免除できます。基準は免除ハンドラーで定義されます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

免除ハンドラーでの免除アカウントの定義方法について詳しくは、「*IBM Security Identity Manager 管理ガイド*」の../admin/cpt/cpt_ic_services_policy.dita『ポリシー実行アクション』トピックの『*ポリシー実行アクション*』を参照してください。

注: アドミニストレーターは、ユーザーが定義または作成した免除ハンドラーをオーバーライドできます。

このタスクについて

アカウントの非準拠属性を準拠属性に置き換えるには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**グローバル・ポリシー実行の構成**」を選択します。
2. 「グローバル・ポリシー実行の構成」ページの「実行アクション」セクションで「**修正**」を選択してから、「**実行**」を選択します。

   注: システムのグローバル・ポリシー実行アクションを変更すると、アカウント準拠の再評価とアカウント・データの変更が行われる場合があります。さらに、

「**修正**」を選択すると、アカウントが免除されていない限り、アカウントの*プロビジョニング解除* 、つまりアカウントの削除が実行される場合もあります。これは、アカウントがいずれのプロビジョニング・ポリシー資格によっても認可されない場合です。

3. 「確認」ページで、この操作をスケジュールする日時を選択します。

   注: このオプションの選択後は、カレンダー・アイコンおよびクロック・アイコンを選択して予定の日時をカスタマイズできます。

   - 要求を即時実行する場合は、「**即時**」を選択してから「**実行**」を選択します。

     注: 現在の日時が表示されます。
   - カスタマイズした日時に要求を実行する場合は、「**発効日**」を選択してから「**実行**」を選択します。

4. 「成功」ページで、「**クローズ**」をクリックします。

アカウントへのアラートの作成

非準拠属性を持つアカウントについてアラームを発行する「**アラート**」を作成して、このアラートの電子メール通知をセットアップできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

ナビゲーション・ツリーの「**サービスの管理**」を使用して特定のサービスを処理する場合、そのサービスに関するグローバル・ポリシー実行アラートをセットアップできます。リストでそのサービスの横にあるアイコンをクリックします。「**ポリシー実行の構成**」を選択します。「**グローバル実行アクションの使用: アラート**」をクリックすると、そのサービスに対する、日時を指定したグローバル・ポリシー・アラートを設定できます。

非準拠属性を持つアカウントに対するアラートをセットアップするには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから、「**システムの構成**」 > 「**グローバル・ポリシー実行の構成**」を選択します。
2. 「グローバル・ポリシー実行の構成」ページの「実行アクション」セクションで「**アラート**」を選択します。
3. 「**続行**」をクリックします。
4. 「グローバル・ポリシー実行の構成」ページの「一般」ページを選択して、アラートの情報および設定を指定します。 参加者情報と時間間隔を指定します。アラートを生成するプロセス・タイプを指定し、「**実行**」をクリックします。

   以下の情報を指定してください。

アラート名
アラートを識別する名前を指定します。

準拠アラートの送信先
準拠アラートを受信する参加者を指定します。

準拠アラートをエスカレートするまでに待機する日数
アラートがエスカレートするまでの日数を指定します。

準拠アラートのエスカレート先
エスカレートされた準拠アラートを受信する参加者を指定します。

システムが修正アクションを実行するまでの日数
修正アクションを実行するまでの、システムの待機日数を指定します。

「プロセス・タイプ」テーブル
準拠アラートを生成するプロセスを指定します。

注: プロセス・タイプを選択しなかった場合は、システムが、該当するプロセス・タイプの非準拠アカウントを自動的に修正します。この修正により、アカウントは変更または削除されます。

アラートの生成
アラートを生成するプロセス・タイプを指定します。アラートを生成するプロセス・タイプのチェック・ボックスを選択します。

プロセス・タイプ
準拠アラートを生成するワークフロー・プロセスのタイプを指定します。

5. 「グローバル・ポリシー実行の構成」ページで、電子メール・ページを選択して、アラート通知電子メールのテキストを入力します。あるいは、デフォルト・テンプレートの使用を選択します。デフォルト・テンプレートを使用しない場合、電子メール通知の件名行を入力します。本文をプレーン・テキストで入力するか、XHTML 動的コンテキストを指定します。
6. 「**実行**」をクリックします。
7. 「確認」ページで、この操作をスケジュールする日時を選択します。

注: このオプションの選択後は、カレンダー・アイコンおよびクロック・アイコンを選択して予定の日時をカスタマイズできます。

- 要求を即時実行する場合は、「**即時**」を選択してから「**実行**」を選択します。

  注: 現在の日時が表示されます。
- カスタマイズした日時に要求を実行する場合は、「**発効日**」を選択してから「**実行**」を選択します。

8. 「成功」ページで、「**クローズ**」をクリックします。

第 15 章 データのインポートとエクスポート

IBM Security Identity Manager では、データ保全性を維持しながらデータをインポートおよびエクスポートします。

概説

IBM Security Identity Manager も含めて、エンタープライズ・アプリケーションの多くは、段階的にデプロイされます。新規のポリシー、ビジネス・ロジックはテスト環境で開発およびテストしてから、実稼働環境にマイグレーションできます。

インポート・タスクとエクスポート・タスクは、IBM Security Identity Manager のデータ項目と従属オブジェクトを、データ保全性を維持しながらテスト環境から実稼働環境にマイグレーションするときに役立ちます。

インポート・タスクおよびエクスポート・タスクを使用すると、前にエクスポートされたオブジェクトを Java アーカイブ (JAR) ファイルからインポートできます。サポートされているオブジェクト・タイプのインポートは、IBM Security Identity Managerによってエクスポートされたオブジェクトのみに制限されています。

ファイル・ダウンロード用の Java HTTPServletResponse には、2 バイト文字のファイル名の表示に制限があります。エクスポート JAR ファイルの名前を付けるときは、標準的な ASCII ファイル名を使用するようにしてください。

データ・マイグレーション

IBM Security Identity Manager サーバー間でのデータのマイグレーションは、ソース・サーバーでの構成済みオブジェクトの検索とそのオブジェクトのエクスポートで構成されます。マイグレーションでは、オブジェクトをターゲット・サーバーにインポートします。

データ・マイグレーションでは、一般的に構成されるオブジェクト・タイプとその依存関係の抽出を自動化しています。データ・マイグレーションとは、作動中またはステージング済みの構成をテスト環境から実稼働環境に移行するメカニズムのことです。このメカニズムにより、保全性を損なうことなくデータをインポートすることを保証します。この情報は、インポート・タスクおよびエクスポート・タスクを使用して、IBM Security Identity Manager のデータ・マイグレーション機能を活用するアドミニストレーターを対象にしています。

エクスポート

エクスポートには、部分的とフルの 2 つのタイプがあります。どちらのタイプのエクスポートでも、ダウンロード可能な JAR ファイルが 1 つ作成されます。そのファイルには、完了したエクスポートのリストに追加される直列化オブジェクトの XML ファイルが 1 つ含まれています。

インポート

インポートは、ソース・サーバーからのオブジェクト抽出終了後 (エクスポート JAR ファイル生成後)、ターゲット・サーバーのアドミニストレーターによって初期化されます。インポートは、以下のステージで構成されます。

- JAR ファイル・アップロード
- 差違評価
- 競合解決
- システムへのデータのコミット

ポリシー実行

プロビジョニング・ポリシーおよび動的な組織の役割をインポートすると、さまざまな個人が新しい役割に関連付けられる場合があります。インポートしたポリシーに、再評価を必要とする変更が存在する場合は、以下のポリシー実行タスクが実行される場合があります。

- 動的役割の変更の評価と役割メンバーシップの更新
- ホスト選択ポリシーに関連するプロビジョニング・ポリシーの検出
- 役割メンバーシップおよびプロビジョニング・ポリシーと、インポート中のポリシーの結合
- 新規ワークフロー・プロセスを通じた、影響のある全ユーザーへのポリシーの実行

組織図

組織図がテスト (ソース) システムとターゲット (実動) システムとの間で異なる場合、インポートされたオブジェクトは新規オブジェクトとして扱われます。

それらのオブジェクトが実動システムに存在する場合に重複オブジェクトが作成されるのを防止するには、各システムの組織図が一致するようにします。

データ・マイグレーションでのオブジェクトの依存関係

データをマイグレーションするには、マイグレーションされるオブジェクトのすべての依存関係を必ず含める必要があります。

一般的に、*依存関係*は親オブジェクトまたはルート・オブジェクトが参照する独立したオブジェクトで、親を正常にインポートするためにターゲット・システムで必要となるオブジェクトです。 マイグレーション・プロセス全体でデータ保全性を保証するため、インポート・タスクとエクスポート・タスクでは、エクスポートされるオブジェクトの依存関係を自動的に検出して組み込みます。

フル・エクスポートと部分的エクスポート

「**すべてエクスポート**」を使用してすべてをエクスポートすると、「**すべてエクスポート**」 によってサポートされるシステムのすべてのデータが保存されます。部分的エクスポートを使用して個々の項目をエクスポートすると、オブジェクトの動作に必要なすべての依存関係が、実際にはエクスポートされない場合があります。部分的エクスポートでは、保存するオブジェクトを作成するのに必要とされる依存関

係のみが保存されます。例えば、自動アカウント作成機能を含んだプロビジョニング・ポリシーをエクスポートできます。ユーザー ID の作成に必要な ID ポリシーは、プロビジョニング・ポリシーの依存関係としてエクスポートされません。ID ポリシーは、プロビジョニング・ポリシー・オブジェクトを作成するときには不要です。ただし、そのプロビジョニング・ポリシーについて意図した目的によっては、必要な場合があります。その場合は、依存関係を別個のオブジェクトとしてエクスポートおよびインポートしてください。

ポリシー

識別ポリシーおよびパスワード・ポリシーは、プロビジョニング・ポリシーがエクスポートされるときにはエクスポートされません。これらのポリシーは、エクスポート・プロセスの一部として明示的にエクスポートする必要があります。

識別、パスワード、またはプロビジョニング・ポリシーの役割、およびサービス・オブジェクトは、デフォルトではエクスポートされません。これらの項目をエクスポートするには、手動でエクスポート・リストに追加する必要があります。

サービス

サービスをエクスポートすると、そのサービスの所有者情報もエクスポートされます。dn は、ターゲット・システムに同じ名前の個人が存在する場合に、適切に設定されます。

役割関係

子役割関係または親役割関係を持つ役割がエクスポートされた場合は、その関係もエクスポートされます。関連する役割自体は、依存関係としてエクスポートされません。

従属役割がターゲット・システムに存在する場合は、その役割関係が作成されます。それ以外の場合、役割関係は作成されません。インポート中に役割関係が削除されることはありません。

複数オブジェクトのエクスポート

一定の期間にわたって複数のオブジェクトをエクスポートすると、システムの日々のアクティビティーの間に変更された差異を持つ相互共用の依存関係を保存することになる場合があります。エクスポート方針を計画する場合は、差異を持つ依存関係のことを念頭においてください。

依存関係および親オブジェクト

親オブジェクトは除去することができます。ただし、親オブジェクトを除去すると、インポート・タスクとエクスポート・タスクにより、エクスポート・リストの依存関係すべてが自動的に削除されます。

表 31. 依存関係および親オブジェクト

親オブジェクト	依存関係
ID ポリシー ライフサイクル・ルール ライフサイクル操作	オブジェクト・プロファイル
ID ポリシー ライフサイクル・ルール ライフサイクル操作 パスワード・ポリシー プロビジョニング・ポリシー サービス サービス選択ポリシー ワークフロー	サービス・プロファイル
プロビジョニング・ポリシー ワークフロー	組織の役割
採用ポリシー ID ポリシー パスワード・ポリシー プロビジョニング・ポリシー	サービス
ライフサイクル・ルール	ライフサイクル操作

フル・エクスポートの実行

この手順を使用して、すべてのエクスポート可能オブジェクト・タイプをエクスポートし、エクスポート・データを含んでいる 1 つの Java アーカイブ (JAR) ファイルを生成します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

このタスクによって生成される JAR ファイルは、依存関係およびコンテナー参照など、既存のすべてのエクスポート可能オブジェクトからの全抽出物を含んでいます。

フル・エクスポートを実行するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから**「システムの構成」** > **「データのエクスポート」**をクリックします。 「データのエクスポート」ページが表示されます。

2. 「データのエクスポート」ページで、**「すべてエクスポート」**をクリックします。 「すべてエクスポート」ページが表示されます。
3. オプション: **「エクスポート名」**フィールドに、エクスポートを識別する名前を入力します。
4. **「ファイルにエクスポート (.jar)」**フィールドに、エクスポートのファイル名を入力し、**「実行」**をクリックします。 「データのエクスポート」ページが表示されます。
5. 「データのエクスポート」ページで、**「リフレッシュ」**をクリックして、テーブルに表示されているエクスポート項目のリストを更新します。

タスクの結果

フル・エクスポート JAR ファイルが作成され、「データのエクスポート」ページに表示されます。

次のタスク

JAR ファイルのダウンロードなど、エクスポート管理タスクをさらに実行するか、**「クローズ」**をクリックします。

部分的エクスポートの実行

この手順を使用して、オブジェクト・タイプを選択してエクスポートし、エクスポート・データを含んでいる 1 つの Javaアーカイブ (JAR) ファイルを生成します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

エクスポートするオブジェクトに必要なすべての依存関係を識別しておいてください。

このタスクについて

このタスクによって生成される JAR ファイルは、指定したエクスポート可能オブジェクト・タイプからの全抽出物を含んでいます。全抽出物の内容は、依存関係およびコンテナー参照などです。

以下のオブジェクト・タイプを検索および選択して、部分的エクスポート JAR ファイルに含めることができます。

- 採用ポリシー
- グループ
- ID ポリシー
- ライフサイクル操作
- ライフサイクル・ルール
- 組織の役割

- パスワード・ポリシー
- プロビジョニング・ポリシー
- サービス
- サービス選択ポリシー
- ワークフロー

部分的エクスポートを実行するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**データのエクスポート**」をクリックします。 「データのエクスポート」ページが表示されます。
2. 「データのエクスポート」ページで、「**作成**」をクリックします。 「部分的エクスポートの作成」ページが表示されます。
3. エクスポートにオブジェクトを追加するには、「**追加**」をクリックします。 「オブジェクトの選択」ページが表示されます。
4. エクスポートするオブジェクトを見つけるには、以下の手順を実行します。
   a. 「**名前**」フィールドに、エクスポートするオブジェクトに関する情報を入力します。
   b. 検索するオブジェクト・タイプを「**オブジェクト・タイプ**」リストで選択してから、「**検索**」をクリックします。 検索基準に一致するオブジェクトがテーブルに表示されます。
5. エクスポートするオブジェクトの横のチェック・ボックスを選択してから「**OK**」をクリックします。 この列の上部にあるチェック・ボックスを選択すると、すべてのオブジェクトが選択されます。 追加したオブジェクトが、「部分的エクスポートの作成」ページに表示されます。
6. エクスポートする項目のリストを確認してから「**続行**」をクリックします。 「部分的エクスポート」ページが表示されます。
7. オプション: 「**エクスポート名**」フィールドに、エクスポートを識別する名前を入力します。
8. 「**ファイルにエクスポート (.jar)**」フィールドに、エクスポートのファイル名を入力し、「**実行**」をクリックします。 「データのエクスポート」ページが表示されます。
9. 「データのエクスポート」ページで、「**リフレッシュ**」をクリックして、テーブルに表示されているエクスポート項目のリストを更新します。

タスクの結果

部分的エクスポート JAR ファイルが作成され、「データのエクスポート」ページに表示されます。

次のタスク

JAR ファイルのダウンロードなど、エクスポート管理タスクをさらに実行するか、「**クローズ**」をクリックします。

JAR ファイルのダウンロード

この手順を使用して、部分的エクスポートまたはフル・エクスポートの Java アーカイブ (JAR) ファイルをローカル・システムにダウンロードします。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

すべての依存関係とコンテナーへの参照を含め、エクスポート・ファイルを作成済みであることを確認してください。

このタスクについて

エクスポート JAR ファイルは、エクスポートされたオブジェクトのタイプおよび数によってサイズが異なります。完了したエクスポートのリストの各行は、エクスポートのタイプ (部分的またはフル)、処理したオブジェクトの数を示します。各行は、エクスポートが開始および終了した時刻のタイム・スタンプ、エクスポートのステータス、および JAR ファイルそれ自体へのリンクを示します。この JAR ファイルへのリンクを使用して、ファイルをダウンロードし、ローカル・システム上の場所に保存できます。

JAR ファイルをローカル・システムにダウンロードするには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから**「システムの構成」** > **「データのエクスポート」**をクリックします。 「データのエクスポート」ページが表示されます。
2. 「データのエクスポート」ページで、ダウンロードする JAR ファイルの名前をクリックします。 「ファイルのダウンロード」ダイアログが表示されます。
3. 「ファイルのダウンロード」ダイアログで、**「保存」**をクリックします。 **「名前を付けて保存」**ダイアログが表示されます。
4. ファイルを保存する場所までナビゲートし、**「保存」**をクリックします。

タスクの結果

JAR ファイルがローカル・システムにダウンロードされます。

次のタスク

エクスポート管理タスクをさらに実行するか、**「クローズ」**をクリックします。

エクスポート・レコードの削除

この手順を使用して、エクスポート・レコードをテーブルから削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

エクスポート・レコードを削除すると、Java アーカイブ (JAR) ファイルなど、そのすべてのレコードがデータベースから削除されます。JAR ファイルを保持する場合は、エクスポート・レコードからローカル・システムに JAR ファイルをダウンロードしてから、エクスポート・レコードを削除するようにしてください。

エクスポートがまだ処理中の場合は、エクスポート・レコードを削除できません。

エクスポート・レコードをテーブルから削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから**「システムの構成」** > **「データのエクスポート」**をクリックします。 「データのエクスポート」ページが表示されます。
2. 「データのエクスポート」ページで、削除するエクスポートを選択して、**「削除」**をクリックします。

タスクの結果

エクスポート・レコードが、「データのエクスポート」ページのテーブルから除去されます。

次のタスク

エクスポート管理タスクをさらに実行するか、**「クローズ」**をクリックします。

JAR ファイルのアップロード

この手順を使用して、部分的エクスポートまたはフル・エクスポートの Javaアーカイブ (JAR) ファイルをローカル・システムからアップロードします。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

エクスポートされた JAR ファイルがローカル・システムに保存されていることを確認してください。

このタスクについて

コンテンツが BLOB としてバルク・データ・サービス・データベースに挿入されるため、このタスクでは、標準 Java ストリーム経由で JAR ファイルのインポートが初期化されます。

JAR ファイルをローカル・システムからアップロードするには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから**「システムの構成」** > **「データのインポート」**をクリックします。 「データのインポート」ページが表示されます。
2. 「データのインポート」ページで、**「ファイルのアップロード」**をクリックします。 「ファイルのアップロード」ページが表示されます。
3. オプション: **「インポート名」**フィールドに、インポートを識別する名前を入力してから、**「参照」**をクリックします。 「ファイルの選択」ダイアログが表示されます。
4. 「ファイルの選択」ダイアログで、ファイルの場所までナビゲートし、ファイルを選択してから**「開く」**をクリックします。 ファイル名が「データのインポート」ページに表示されます。
5. **「実行」**をクリックして、ファイルをアップロードします。 「データのインポート」ページが表示されます。
6. 「データのインポート」ページで、**「リフレッシュ」**をクリックして、テーブルに表示されているインポート項目のリストを更新します。

タスクの結果

JAR ファイルがローカル・システムからアップロードされ、「データのインポート」ページに表示されます。

次のタスク

インポート管理タスクをさらに実行するか、**「クローズ」**をクリックします。

競合の解決

インポート・プロセスは、インポート・データとターゲット・サーバーのデータの差違を評価し、この 2 つの間の競合を解決するために役立ちます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

ローカル・システムから Java アーカイブ (JAR) ファイルをインポート済みであることを確認してください。

このタスクについて

差違評価によって、インポート JAR ファイルおよびターゲット・システムに検出されたオブジェクトのリストが生成されます。アドミニストレーターは、このリストを使用してオブジェクト単位で競合を解決できます。アドミニストレーターは、既存データの優先順位を決定したり、インポートしたデータで既存データを上書きしたりします。差違評価と競合解決は、部分的エクスポートとフル・エクスポートの両方のタイプに対して実行されます。

競合の要約で上書きを選択したオブジェクトが、インポート時点で IBM Security Identity Manager に存在していた場合、このオブジェクトは更新されます。

アップロードした JAR ファイルに存在し、インポート時点で IBM Security Identity Manager に存在しないオブジェクトは、追加されます。

アップロードされた JAR ファイルのデータとサーバーに存在するデータの間の競合を解決するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**データのインポート**」をクリックします。 「データのインポート」ページが表示され、テーブルの「**状況**」列に、競合が検出されたかどうかが示されます。
2. テーブルの「**状況**」列にある「**競合が検出されました**」リンクをクリックします。 「インポート・ファイルの評価」ページが表示されます。
3. 「インポート・ファイルの評価」ページで、インポートするオブジェクトの横のチェック・ボックスを選択し、既存のオブジェクトをオーバーライドしてから「**インポート**」をクリックします。 この列の上部にあるチェック・ボックスを選択すると、すべてのオブジェクトが選択されます。 「データのインポート」ページが表示されます。
4. 「データのインポート」ページで、「**リフレッシュ**」をクリックして、テーブルに表示されているインポートの状況を更新します。 「**状況**」列に、インポートが成功したことが示されます。

タスクの結果

インポート・プロセスはデータをコミットし、親オブジェクトとその依存関係の関係を再確立します。このプロセスは、IBM Security Identity Manager 組織図の適切なコンテナーにオブジェクトを配置します。

競合の評価中に、IBM Security Identity Manager コンソールとのセッションがアイドルであり、タイムアウトになった場合や、明示的にログオフした場合は、インポート・プロセスの状況が「処理」から 「失敗 (競合が解決されていません)」に変わります。 この状況の変化が起こった場合は、手順を反復して、データがコミットされるようにしてください。ユーザー・セッションは、一般に、10 分間アイドルであった場合にタイムアウトするよう構成されています。

次のタスク

インポート管理タスクをさらに実行するか、「**クローズ**」をクリックします。

インポートの削除

この手順を使用して、インポート・レコードをテーブルから削除します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

このタスクについて

この手順では、インポート・レコードおよびアップロードされた Java アーカイブ (JAR) ファイルを削除します。

インポート・レコードをテーブルから削除するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**システムの構成**」 > 「**データのインポート**」をクリックします。 「データのインポート」ページが表示されます。
2. 「データのインポート」ページで、削除するインポートを選択して、「**削除**」をクリックします。

タスクの結果

インポート・レコードが、「データのインポート」ページのテーブルから除去されます。

次のタスク

インポート管理タスクをさらに実行するか、「**クローズ**」をクリックします。

インポートおよびエクスポート JAR ファイルを移植可能にする

インポートおよびエクスポート Java アーカイブ (JAR) ファイルを 2 つのマシン間で移植できるようにするには、特定の構成設定を両方のシステムで同じにする必要があります。

このタスクについて

インポートおよびエクスポート JAR ファイルを 2 つのシステム間で移植できるようにするには、以下の構成設定が両方のシステムで同じであることを確認してください。

- 鍵ストア・ファイル
- 鍵ストアのパスワード
- ハッシュ・アルゴリズム

第 16 章 IBM Tivoli Common Reporting の構成および管理

IBM Tivoli Common Reporting (レポート・パックとも呼ばれる) は、アカウント、サービス、および要求情報に焦点を合わせています。

IBM Tivoli Common Reporting には、IBM Security Identity Manager バージョン 6.0 ユーザー・インターフェースから使用できるデフォルト・レポートのサブセットが含まれています。これらのレポートでは、レポートの表示データに対して、IBM Security Identity Manager からのアクセス・コントロール情報 (ACI) は適用されません。

IBM Tivoli Common Reporting から実行されるすべてのレポートは、Tivoli Common Reporting コンソールからレポートのデータを表示するための全権限を持つ IBM Security Identity Manager 管理者が実行できます。これらのレポートでは、IBM Security Identity Manager で現在定義されている ACI を考慮しません。

これらのレポートは、IBM Security Identity Manager バージョン 6.0 がサポートする DB2®、Oracle、および Microsoft SQL Server のバージョンでもサポートされます。

IBM Security Identity Manager 6.0 に付属する Tivoli Common Reporting ソフトウェアを使用して、レポートを管理および実行できます。Tivoli Common Reporting について詳しくは、次の Web サイトを参照してください。

http://www.ibm.com/developerworks/spaces/tcr

レポートを編集するには、次の Web サイトにある Eclipse Business Intelligence Reporting Tool バージョン 2.2.1 を使用します。

http://catalog.lotus.com/wps/portal/topal/details?catalog.label=1TW10OT02

Tivoli Common Reporting バージョン 2.1.1 のインストールまたはバージョン 7.1.5 へのアップグレード

Tivoli Common Reporting バージョン 2.1.1 をインストールするか、バージョン 2.1.1 にアップグレードすることができます。

注:

- ご使用のコンピューターに、IBM Security Role and Policy Modeler を介して Tivoli Common Reporting バージョン 2.1.1 のインスタンスがすでにインストールされている場合は、再インストールせずにそのバージョンを使用できます。
- Tivoli Common Reporting サーバーの要件を満たしていることを確認します。「*IBM Security Identity Manager 製品概要*」のレポート・サーバーの要件を参照してください。
- IBM Security Identity Manager バージョン 6.0 の前提条件を満たしている同じシステムにインストールする場合は、デフォルト以外のポートで実行されるように IBM Tivoli Common Reporting を構成します。Tivoli Common Reporting のデフ

ォルト・ポートは、インストール済み製品のポートと競合する可能性が高く、そのため、Tivoli Common Reporting のインストールに失敗しやすくなります。

- Tivoli Common Reporting バージョン 2.1.1 をインストールするには、Web サイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ttcr_install.html) を参照してください。
- Tivoli Common Reporting バージョン 2.1.1 にアップグレードするには、Web サイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ctcr_upgrade.html) を参照してください。

レポート・パッケージを Tivoli Common Reporting にインポートする

レポート・パッケージを Tivoli Common Reportingにインポートして、IBM Security Identity Manager Server バージョン 6.0 レポートを Tivoli Common Reporting 内から実行します。レポート・パッケージは IBM Security Identity Manager のバージョン 6.0 レポートを Tivoli Common Reporting にインストールします。

始める前に

- IBM Security Identity Manager バージョン 6.0 をインストールします。詳しくは、「*IBM Security Identity Manager インストール・ガイド*」を参照してください。
- Tivoli Common Reporting バージョン 2.1.1 をインストールします。http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.htmlを参照してください。

手順

1. `tcr_tim6.0_reporting_pack.zip` ファイルを *ISIM_HOME*`/extensions/tcr/tcrpack` ディレクトリーから取得します。*ISIM_HOME* は IBM Security Identity Manager インストール・ディレクトリーです。
2. **`trcmd -import`** コマンドでレポート・パッケージをインポートします。http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ctcr_birt_reps_in_cog_importing.htmlを参照してください。

タスクの結果

レポートをインポートして、「**Common Reporting**」 > 「**パブリック・フォルダー**」 > 「**Tivoli 製品**」に配置します。「**IBM Security Identity Manager 6.0**」を選択して、有効なレポートを参照します。

次のタスク

レポートを生成します。

「*IBM Security Identity Manager 管理ガイド*」のトピック『Tivoli Common Reporting でのレポートの生成』を参照してください。

組み込み WebSphere Application Server の構成

IBM Security Identity Manager レポートを実行するには、IBM Tivoli Common Reporting 組み込み WebSphere Application Server 上に JDBC データ・ソースを構成する必要があります。

このタスクについて

IBM Security Identity Manager データベースに接続するように Tivoli Common Reporting を構成する必要があります。以下の手順を実行します。

- 201 ページの『Java 認証・承認サービス (JAAS) 別名の作成』
- 203 ページの『Java Database Connectivity (JDBC) プロバイダーの作成』
- 206 ページの『データ・ソースの作成』
- 210 ページの『構成の保存』

この手順は、以下のように、手動または自動で実行できます。

- 手動構成については、200 ページの『**wsadmin** コマンドを使用した 組み込み WebSphere Application Server の構成』で説明します。
- 自動構成については、『Jython スクリプトを使用した 組み込み WebSphere Application Server の構成』で説明します。

どちらの方法でも、得られる結果は同じです。

次のタスク

wsadmin コマンドまたは Jython スクリプトを使用して、組み込み WebSphere Application Server を構成します。

Jython スクリプトを使用した 組み込み WebSphere Application Server の構成

IBM Security Identity Manager には、パッケージされたレポートの必須データ・ソースの構成を容易にするスクリプトが含まれています。

このタスクについて

ITIM_HOME/extensions/tcr/scripts/TIMsetupDatasource.py ファイルは、ご使用の IBM Security Identity Manager 環境の Tivoli Common Reporting 構成を自動化するために使用される Jython スクリプトです。このスクリプトを使用するには、以下の手順を実行します。

1. TIMsetupDatasource.py ファイルを *ITIM_HOME*/extensions/tcr/scripts/TIMsetupDatasource.py から Tivoli Common Reporting がインストールされているコンピューターにコピーします。
2. TIMsetupDatasource.py ファイルを編集して、以下のパラメーターを、ご使用の環境の値と一致するように更新します。

   ```
   aliasUser
   aliasPW
   dsDBVendor
   ```

   DB2 または MS SQL データベース・サーバー用:

```
dsDBName
dsDBServer
dsDBPort
dsDBType
```

Oracle データベース・サーバー用:

```
dsDBURL
```

すべてのデータベース・サーバー用:

```
providerCP
providerImplClass
dsDBHelper
```

スクリプトには、上記の各パラメーターの値が記録されます。

3. Tivoli Common Reporting 組み込み WebSphere Application Server で、以下のように **wsadmin** コマンドを実行します。
   - Windows の場合は、コマンド・プロンプトを開いて、次の例のようにコマンドを入力します。

     ```
     TCR_HOME¥profiles¥TIPProfile¥bin¥wsadmin.bat –f TIMsetupDatasource.py
     ```
   - UNIX の場合は、シェルを開いて、次の例のようにコマンドを入力します。

     ```
     TCR_HOME/profiles/TIPProfile/bin/wsadmin.sh –f TIMsetupDatasource.py
     ```

次のタスク

Tivoli Common Reporting のデータ・ソースを構成します。詳しくは、211 ページの『Tivoli Common Reporting のデータ・ソースの構成』を参照してください。

wsadmin コマンドを使用した 組み込み WebSphere Application Server の構成

手動で IBM Tivoli Common Reporting を IBM Security Identity Manager 用に構成するには、一連の **wsadmin** コマンドを実行する必要があります。

このタスクについて

以下の手順を実行します。

- 201 ページの『Java 認証・承認サービス (JAAS) 別名の作成』
- 203 ページの『Java Database Connectivity (JDBC) プロバイダーの作成』
- 206 ページの『データ・ソースの作成』
- 210 ページの『構成の保存』

wsadmin コマンドは **wsadmin** プロンプトから実行する必要があります。 **wsadmin** コマンドを実行する準備として **wsadmin** を開始するには、Tivoli Common Reporting 組み込み WebSphere Application Server プロファイルの `bin` ディレクトリーにナビゲートして、**wsadmin** Jython インタープリターを開始します。

手順

1. 次のいずれかを実行して、Tivoli Common Reporting 組み込み WebSphere Application Server プロファイルの `bin` ディレクトリーにナビゲートします。

- Windows の場合は、コマンド・プロンプトを開いて、次の例のようにコマンドを入力します。

  ```
  cd "C:¥Program Files¥IBM¥tcr¥eWas61¥profiles¥tcrProfile¥bin"
  ```

- UNIX の場合は、シェルを開いて、次の例のようにコマンドを入力します。

  ```
  cd /opt/IBM/tcr/eWas61/profiles/tcrProfile/bin
  ```

2. 以下のいずれかのコマンドを入力します。
   - Windows の場合は、`wsadmin.bat -lang jython` と入力します。
   - UNIX の場合は、`./wsadmin.sh -lang jython` と入力します。
3. ログインのプロンプトが出されたら、Tivoli Common Reporting アドミニストレーターの資格情報を入力します。 これらのエントリーは、Tivoli Common Reporting 管理コンソールにアクセスする際に使用する資格情報と同じです (例: `tcrAdmin`)。

次のタスク

JAAS 認証別名を作成します。詳しくは、『Java 認証・承認サービス (JAAS) 別名の作成』を参照してください。

Java 認証・承認サービス (JAAS) 別名の作成

IBM Tivoli Common Reporting サーバーから IBM Security Identity Manager データベース・サーバーへのデータベース接続を認証できるように JAAS 認証別名を作成します。

このタスクについて

JAAS 認証別名は、データベース・ベンダーに依存しません。

別名を作成する前に、別名によって識別されるユーザーに関する以下の情報を検討してください。

- ユーザーは、定義されたレポートのデータを保持するテーブルにアクセスできなければなりません。
- 通常、ユーザーは、IBM Security Identity Manager データベース・サーバーへのデータベース接続用に構成された個人です。
- IBM Security Identity Manager バージョン 5.0 およびバージョン 5.1 のデフォルト・ユーザー ID は `itimuser` です。
- 旧リリースのデフォルト・ユーザー ID は `enrole` でした。

表 32 に、**wsadmin** コンソールを使用して JAAS 認証別名を作成する際の必須パラメーターを示します。

表 32. JAAS 認証別名の必須データ

パラメーター	説明	値の例
別名	ユーザー定義による、このデータ・コレクションを識別する名前。	IBM Security Identity Manager データベース別名

表 32. JAAS 認証別名の必須データ (続き)

パラメーター	説明	値の例
説明	ユーザー定義による、このデータ・コレクションの説明。	IBM Security Identity Manager データベースの JAAS 認証別名
userId	データベース接続時に使用するユーザー ID。	itimuser
パスワード	ユーザー ID に関連付けられているパスワード。 ユーザー ID は、IBM Security Identity Manager サーバーの以下の場所で確認できます。 *ITIM_HOME*/data/enRoleDatabase.properties # IBM Tivoli Identity Manager データベース・ユーザー database.db.user=itimuser ここで、*ITIM_HOME* は IBM Security Identity Manager のインストール・ディレクトリーです。	mypassword

1. 201 ページの表 32 の説明に従って、必要なデータを収集します。
2. Tivoli Common Reporting サーバーの WAS_HOME/bin/ ディレクトリーにある **wsadmin** コマンドを実行します。
3. 収集したデータを使用して、以下の **wsadmin** 形式で JAAS 認証別名構成を作成します。

```
wsadmin> AdminConfig.create(
'JAASAuthData',
AdminConfig.getid("/Security:/"),
[["alias", "alias"],
["description", "description"],
["userId", "userId"],
["password", "password"]])
```

各部の意味は、次のとおりです。

- *alias* および *description* は、ユーザーが選択する任意の値です。これらの値は後のステップで使用するので、覚えておく必要があります。
- *userId* は、IBM Security Identity Manager データベースに接続してデータを読み取るのに必要な権限を持つ、IBM Security Identity Manager データベース・サーバー上の有効なユーザーに相当します。
- *password* は、*userId* に関連付けられたパスワードです。

wsadmin コマンドの例を以下に示します。

```
wsadmin> AdminConfig.create(
'JAASAuthData',
AdminConfig.getid("/Security:/"),
[["alias", "IBM Tivoli Identity Manager DB Alias"],
["description", "JAAS alias for the IBM Tivoli Identity Manager DB"],
["userId", "itimuser"],
["password", "mypassword"]])
```

次のタスク

JDBC プロバイダーを作成します。詳しくは、203 ページの『Java Database Connectivity (JDBC) プロバイダーの作成』を参照してください。

Java Database Connectivity (JDBC) プロバイダーの作成

データ・ソースの作成では、ご使用の環境に対する JDBC プロバイダー値の識別と、単一の **wsadmin** コマンドの実行の両方が必要です。

このタスクについて

JDBC プロバイダー情報は、データベース・ベンダーに依存します。

表 33 に、**wsadmin** コンソールで JDBC プロバイダーを作成する際に必要なパラメーターを示します。

表 33. JDBC プロバイダーの必須データ

パラメーター	説明	値の例
classpath	JDBC プロバイダー・クラスに必要なクラスパス	表 34 を参照してください。
implementationClassName	JDBC プロバイダー実装クラス	表 35 を参照してください。
name	ユーザー定義による、この JDBC プロバイダーの名前	IBM Security Identity Manager データベースの JDBC プロバイダー
説明	ユーザー定義による、この JDBC プロバイダーの説明	IBM Security Identity Manager データベースをデータ・ソースとして追加するときに使用される JDBC プロバイダー。

表 34. IBM Security Identity Manager でサポートされる JDBC プロバイダーのサンプル・クラスパス値

データベース・タイプ	クラスパス
DB2	`/opt/IBM/db2/V9.1/java/db2jcc.jar;/opt/IBM/db2/V9.1/java/db2jcc_license_cu.jar`
Microsoft SQL Server	`C:/Program Files/Microsoft SQL Server 2005 JDBC Driver/sqljdbc_1.1/enu/sqljdbc.jar`
Oracle	`/u01/app/oracle/product/10.2.0/Db_1/jdbc/lib/ojdbc14.jar`

表 35. IBM Security Identity Manager でサポートされる JDBC プロバイダーの実装クラス名

データベース・タイプ	実装クラス名
DB2	`com.ibm.db2.jcc.DB2ConnectionPoolDataSource`
Microsoft SQL Server	`com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource`
Oracle	`oracle.jdbc.pool.OracleConnectionPoolDataSource`

1. 以下の表の説明に従って、必要なデータを収集します。
   - 表 33
   - 表 34

- 203 ページの表 35

このデータの収集については、『IBM Security Identity Manager からの JDBC プロバイダー情報の識別』を参照してください。

2. 200 ページの『**wsadmin** コマンドを使用した 組み込み WebSphere Application Server の構成』の説明に従って、**wsadmin** コマンドを開始します。
3. 収集したデータを使用して、以下の形式で JDBC プロバイダーを作成します。

```
wsadmin> AdminConfig.create(
'JDBCProvider',
AdminConfig.getid("/Cell:/"),
[["classpath", "classpath"],
["implementationClassName", "implementationClassName"],
["name", "name"],
["description", "description"]])
```

例で、'JDBCProvider' および "/Cell:/" は、この構成オブジェクトのタイプと場所を識別します。

ペアになっている各属性リストの最初の要素、つまり "classpath"、"implementation"、"name"、および "description" は、この構成要素の作成時に使用される特定の属性の名前を識別します。

ペアになっている各属性リストの 2 番目の要素は値であり、この値はインストールによって異なる可能性があります。

"name" および "description" の値は、ユーザーが選択する値です。"name" の値は後のステップで使用するので、覚えておく必要があります。

"classpath" および "implementationClassName" の値は、使用するデータベースの実際の実装クラス名および必須クラスパスに対応していなければなりません。

wsadmin コマンドの例を以下に示します。

```
wsadmin> AdminConfig.create(
'JDBCProvider',  AdminConfig.getid("/Cell:/"),
[["classpath",
"C:/Program Files/Microsoft SQL Server 2005 JDBC Driver/
sqljdbc_1.1/enu/sqljdbc.jar"],
["implementationClassName",
"com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource"],
["name", "JDBC provider for the ITIM DB"],
["description", "JDBC provider for the ITIM DB
under which to add the ITIM DB as a data source"]])
```

次のタスク

データ・ソースを作成します。 詳しくは、 206 ページの『データ・ソースの作成』を参照してください。

IBM Security Identity Manager からの JDBC プロバイダー情報の識別

JDBC プロバイダーを作成するには、正しいパラメーターを識別する必要があります。このセクションでは、IBM Security Identity Manager で既に使用されている値を特定する方法を示します。

このタスクについて

実装クラス名およびサンプルのクラスパス情報は、IBM Security Identity Manager WebSphere Application Server から入手することもできます。

IBM Security Identity Manager WebSphere Application Server サーバーに定義されたクラスパス値が依存するサーバー変数は、Tivoli Common Reporting 組み込み WebSphere Application Server サーバーには存在しません。したがって、クラスパス値は、特定の場所を指すのではなく、一般的にどのファイルが必要かをユーザーに示すことが可能です。

手順

1. IBM Security Identity ManagerWebSphere Application Server サーバーの WebSphere Application Server 管理コンソールで、ログインし、「**リソース**」 > 「**JDBC**」 > 「**JDBC プロバイダー**」にナビゲートします。
2. JDBC プロバイダーのリストを表示します。 IBM Security Identity Manager に関連する JDBC プロバイダーが複数表示される場合は、non-XA として識別されるプロバイダーを選択します。 例えば、IBM Security Identity Manager non-XA DB2 JDBC プロバイダーを選択すると、実装クラス名とクラスパスが表示されます。

例

もう一つの方法として、IBM Security Identity Manager WebSphere Application Server サーバー上で **wsadmin** セッションを使用して JDBC プロバイダー識別子 (ID) をリストすることにより、そのサーバーに関するこの情報を取得できます。

以下に示すのは、この **wsadmin** コマンド行の出力例であり、この中の引用符付きの各ストリングが JDBC プロバイダー ID です。

```
wsadmin> print AdminConfig.list("JDBCProvider")
"Derby JDBC Provider (XA)(cells/fooNode01Cell/nodes/fooNode01/servers/server1|
resources.xml#builtin_jdbcprovider)"
"Derby JDBC Provider (XA)(cells/fooNode01Cell|resources.xml#builtin_jdbcprovider)"
"Derby JDBC Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201014593661)"
"ITIM XA DB2 JDBC Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201032904744)"
"ITIM non-XA DB2 JDBC Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201032906859)"
```

JDBC プロバイダーのリストがあれば、以下の **wsadmin** コマンドを使用して、特定の JDBC プロバイダー ID のパラメーター属性を取得できます。以下で使用されている JDBC プロバイダー ID は、例で指定された JDBC プロバイダー ID リストのものです。

```
wsadmin> print AdminConfig.show("ITIM non-XA DB2 JDBC
Provider(cells/fooNode01Cell/nodes/fooNode01/servers/server1|resources.xml
#JDBCProvider_1201032906859)")

[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc.jar;$
{ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar;$
{ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (DB2)"]
[implementationClassName com.ibm.db2.jcc.DB2ConnectionPoolDataSource]
[name "ITIM non-XA DB2 JDBC Provider"]
[nativepath []]
[xa false]
```

Microsoft SQL Server データベースを使用するように構成された Windows ベースの IBM Security Identity Manager WebSphere Application Server 上でこの **wsadmin** セッションを実行した場合の出力例を以下に示します。

```
wsadmin> print AdminConfig.show(AdminConfig.getid("/
JDBCProvider:ITIM non-XA MSSQL JDBCProvider"))
[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/sqljdbc.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (MSSQL)"]
[implementationClassName com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource]
[name "ITIM non-XA MSSQL JDBC Provider"]
[nativepath []]
[xa false]
```

あるいは、包含ストリング "/JDBCProvider:Provider Name" を使用すると、以下のようになります。

```
wsadmin> print AdminConfig.show(AdminConfig.getid("/
JDBCProvider:ITIM non-XA DB2 JDBC Provider"))

[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc.jar;
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar;
${ITIM_DB_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (DB2)"]
[implementationClassName com.ibm.db2.jcc.DB2ConnectionPoolDataSource]
[name "ITIM non-XA DB2 JDBC Provider"]
[nativepath []]
[xa false]
```

Oracle データベースを使用するように構成された Solaris ベースの IBM Security Identity Manager WebSphere Application Server 上でこの **wsadmin** セッションを実行した場合の出力例を以下に示します。

```
wsadmin> print AdminConfig.show(AdminConfig.getid("/
JDBCProvider:ITIM non-XA ORACLE JDBC Provider"))
[classpath
${ITIM_DB_JDBC_DRIVER_PATH}/ojdbc14.jar]
[description "ITIM JDBC2 non-XA Compliant Driver (ORACLE)"]
[implementationClassName oracle.jdbc.pool.OracleConnectionPoolDataSource]
[name "ITIM non-XA ORACLE JDBC Provider"]
[nativepath []]
[providerType "Oracle JDBC Driver"]
[xa false]
```

注: IBM Security Identity Manager サーバー構成から取得されたクラスパス値には、変数 *${ITIM_DB_JDBC_DRIVER_PATH}* が使用されていますが、Tivoli Common Reporting サーバーでは、JDBC プロバイダーを定義するときにこの変数を使用できません。JDBC プロバイダーのクラスパスを指定するときは、絶対パスを使用する必要があります。

次のタスク

JDBC プロバイダーを作成します。詳しくは、203 ページの『Java Database Connectivity (JDBC) プロバイダーの作成』を参照してください。

データ・ソースの作成

データ・ソースの作成は、ベンダーに依存する、最も複雑なステップです。

このタスクについて

この作業では、ご使用のデータベースに関する詳細な接続およびサーバーの情報 (例えば、ホスト名、ポート、データベース名、その他のベンダー依存の設定値) が必要になります。詳しくは、表 36 を参照してください。

表 36. DB2 および Microsoft SQL Server データベースのプロパティー

パラメーター	説明	値の例
databaseName	ターゲット・サーバー上のデータベースの名前。	`itimdb`
serverName	データベース・サーバーのホスト名または IP アドレス。	`myserver.my.com`
portNumber	データベース・サーバー接続用のポート番号。	`1433`

DB2 および Microsoft SQL Server データベースの場合は、*databaseName*、*serverName*、および *portNumber* パラメーターを使用して JDBC データ・ソースが定義されます。Oracle データベースの場合は、URL プロパティーだけが使用されます。

表 37. データ・ソース・ヘルパー・クラス名

データベース・ベンダー	データ・ソース・ヘルパー・クラス名
DB2	com.ibm.websphere.rsadapter.DB2UniversalDataStoreHelper
Microsoft SQL Server	com.ibm.websphere.rsadapter.ConnectJDBCDataStoreHelper
Oracle	com.ibm.websphere.rsadapter.Oracle10gDataStoreHelper

手順

1. 表 36 の説明に従って、必要なデータを収集します。このデータの収集については、209 ページの『IBM Security Identity Manager からのデータ・ソース情報の識別』を参照してください。
2. 200 ページの『**wsadmin** コマンドを使用した 組み込み WebSphere Application Server の構成』の説明に従って、**wsadmin** コマンドを開始します。
3. データ・ソースを作成します。 このコマンドの結果をローカル変数 *ds* に保存すると、残りのコマンドを実行する際に役立ちます。

```
wsadmin> ds = AdminConfig.create(
 'DataSource',
 AdminConfig.getid("/JDBCProvider:JDBC provider for the ITIM DB"),
 [["name", "ITIM DB Data Source"],
  ["description", "ITIM DB Data Source"]])
```

4. 追加のプロパティーを保持するリソース・プロパティー・セットを作成します。このコマンドの結果をローカル変数 *ds_props* に保存すると、残りのコマンドを実行する際に役立ちます。

```
wsadmin> ds_props = AdminConfig.create('J2EEResourcePropertySet', ds, [])
```

5. J2EE プロパティーを作成します。 DB2 および Microsoft SQL Server データ・ソースの場合、設定するプロパティーは 4 つあります。これらのプロパティーは、データベース名、データベース・サーバー、サーバー・ポート、およびドラ

イバー・タイプを識別します。Oracle データ・ソースの場合、これらは完全な JDBC 接続 URL を識別する単一プロパティーで設定されます。

DB2 および Microsoft SQL Server のデータベース名
必要な場合は、以下の呼び出し内の値 itimdb を実際のデータベース名に置き換えます。

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "databaseName"],
  ["type", "java.lang.String"],
  ["value", "itimdb"]])
```

DB2 および Microsoft SQL Server 名
必要な場合は、以下の呼び出し内の値 localhost を実際のデータベース・サーバー名または IP アドレスに置き換えます。

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "serverName"],
  ["type", "java.lang.String"],
  ["value", "localhost"]])
```

DB2 および Microsoft SQL Server ポート番号
必要な場合は、以下の呼び出し内の値 1433 を実際のデータベース・サーバーのポート番号に置き換えます。

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "portNumber"],
  ["type", "java.lang.Integer"],
  ["value", "1433"]])
```

DB2 および Microsoft SQL Server ドライバー・タイプ
IBM Security Identity Manager データ・ソースに使用されるすべてのドライバーは、DB2 および Microsoft SQL Server データベースの場合はタイプ 4 で、Oracle データベースの場合は thin です。

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "driverType"],
  ["type", "java.lang.String"],
  ["value", "4"]])
```

Oracle URL
このプロパティーは、Oracle データベース用の唯一の必須プロパティーであり、DB2 または Microsoft SQL Server データベース用のプロパティーではありません。必要な場合は、以下の呼び出し内の値 jdbc:oracle:thin:@myserver.mydomain.com:Port_Number:itimdb を実際のデータベース URL に置き換えます。

```
wsadmin> AdminConfig.create(
 'J2EEResourceProperty',
 ds_props,
 [["name", "URL"],
  ["type", "java.lang.String"],
  ["value", "jdbc:oracle:thin:@myserver.mydomain.com:Port_Number:itimdb"]])
```

6. データ・ソースを変更します。
   a. 以下で予期される Java Naming and Directory Interface (JNDI) 名を使用してデータ・ソース構成を更新します。
      - IBM Security Identity Manager
      - Tivoli Common Reporting レポート・パック (jdbc/ibm/tivoli/tim)

- この構成プロセスの前の方で定義した JAAS 認証別名
- ベンダー依存のデータ・ソース・ヘルパー・クラス名 (207 ページの表 37 を参照)

b. 必要な場合は、以下のコード内で ITIM DB Alias をこの構成プロセスの前の方で作成した JAAS 認証別名に置き換えます。

c. 以下のように、com.ibm.websphere.rsadapter.ConnectJDBCDataStoreHelper を、ご使用のデータベースに応じた適切なデータ・ソース・ヘルパー・クラス名に置き換えます。

```
wsadmin> AdminConfig.modify(
  ds,
  [["jndiName", "jdbc/ibm/tivoli/tim"],
   ["authDataAlias", "ITIM DB Alias"],
   ["datasourceHelperClassname",
"com.ibm.websphere.rsadapter.ConnectJDBCDataStoreHelper"]])
```

次のタスク

構成を保存します。 詳しくは、 210 ページの『構成の保存』を参照してください。

IBM Security Identity Manager からのデータ・ソース情報の識別

データ・ソースを作成するには、IBM Security Identity Manager が使用する正しい構成パラメーターを識別する必要があります。

このタスクについて

必要なデータベース構成情報は、ご使用の IBM Security Identity Manager WebSphere Application Server から入手できます。

手順

1. IBM Security Identity Manager WebSphere Application Server 上の WebSphere Application Server ISC 管理コンソールを使用して、ログインし、「**リソース**」 > 「**JDBC**」 > 「**データ・ソース**」にナビゲートします。
2. データ・ソースのリストを表示して、「**ITIM データ・ソース (ITIM Data Source)**」を選択します。

例

もう一つの方法として、この情報は、IBM Security Identity Manager WebSphere Application Server 上で簡単に取得することができます。そのためには、以下のように、そのサーバー上で **wsadmin** セッションを使用します。

```
wsadmin> print AdminConfig.showall
(AdminConfig.showAttribute(AdminConfig.getid("/
DataSource:ITIM Data Source"), "propertySet"))
[resourceProperties "[[[name databaseName]
[required false]
[type java.lang.String]
[value itimdb]] [[name driverType]
[required false]
[type java.lang.Integer]
[value 4]] [[name serverName]
[required false]
[type java.lang.String]
```

```
[value localhost]] [[name portNumber]
[required false]
[type java.lang.Integer]
[value 50000]]]"]
```

この情報の一部は、IBM Security Identity Manager サーバー上のファイル *ITIM_HOME*/data/enRoleDatabase.properties でも使用できます。*ITIM_HOME* ディレクトリーは、IBM Security Identity Manager がインストールされている場所です。

Microsoft SQL Server の例を以下に示します。

```
# JDBC ドライバー URL
database.jdbc.driverUrl=jdbc:sqlserver://;
server=myserver.mydomain.com;port=1433;database=itimdb
```

各部の意味は、次のとおりです。

- *myserver.mydomain.com* は、IBM Security Identity Manager データベース・サーバーのホスト名です。
- *1433* は、データベース・サーバーが listen するポートです。
- *itimdb* は、IBM Security Identity Manager データベース名です。

Oracle の例を以下に示します。

```
# JDBC ドライバー URL
database.jdbc.driverUrl=jdbc:oracle:thin:@myserver.mydomain.com:1521:itimdb
```

各部の意味は、次のとおりです。

- *myserver.mydomain.com* は、IBM Security Identity Manager データベース・サーバーのホスト名です。
- *1521* は、データベース・サーバーが listen するポートです。
- *itimdb* は、IBM Security Identity Manager データベース名です。

次のタスク

データ・ソースを作成します。 詳しくは、 206 ページの『データ・ソースの作成』を参照してください。

構成の保存

wsadmin セッション内では、すべての変更は構成ワークスペースのコピーに対して行われます。変更をコミットするには、変更を明示的に保存する必要があります。

始める前に

次のコマンドを入力して、構成を保存します。

```
wsadmin> AdminConfig.save()
```

IBM Tivoli Common Reporting サーバーは、ご使用の IBM Security Identity Manager データベースに接続するように構成されています。

このタスクについて

手順

1. Tivoli Common Reporting サーバーを停止し、再始動して、新しい構成設定が有効になるようにします。
2. quit と入力して、**wsadmin** を終了します。 保存せずに終了する場合は、もう一度 quit と入力して変更を破棄します。
3. **wsadmin** を使用して、接続をテストします。
4. 以下のコマンドを入力し、この構成プロセスの前の方で作成したデータ・ソースの名前の代わりに *ITIM DB Data Source* を使用します。

```
wsadmin> AdminControl.testConnection (AdminConfig.getid(
"/DataSource:ITIM DB Data Source"))
```

タスクの結果

コマンドを正常に実行すると、以下のメッセージが表示されます。

```
WASX7217I: 指定されたデータ・ソースへの接続は成功しました。(Connection to
provided datasource was successful.)
```

次のタスク

Tivoli Common Reporting のデータ・ソースを構成します。詳しくは、『Tivoli Common Reporting のデータ・ソースの構成』を参照してください。

Tivoli Common Reporting のデータ・ソースの構成

IBM Security Identity Manager Server バージョン 6.0 レポートで動作する Tivoli Common Reporting のデータ・ソースを構成します。

始める前に

- IBM Security Identity Manager バージョン 6.0 をインストールします。詳しくは、「*IBM Security Identity Manager インストール・ガイド*」を参照してください。
- Tivoli Common Reporting バージョン 2.1.1 をインストールします。 http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.htmlを参照してください。

手順

1. Tivoli Common Reporting にログオンします。 http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ttcr_login.htmlを参照してください。
2. **trcmd -modify** コマンドでデータ・ソースを構成します。 http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/rtcr_cli_modify.htmlを参照してください。

   注:

   - MS SQL データベース・パスワードには特殊文字を含めることはできません。

- Classpath に SQL サーバーの JDBC ドライバーを含めるように設定する必要があります。

タスクの結果

新しいデータ・ソースが Tivoli Common Reporting に作成されます。

レポートの実行

レポートをオンデマンドで実行したり、そのレポートを後で表示できるようにスナップショットを作成したりできます。

手順

1. レポートをオンデマンドで実行するには、以下の手順を実行します。
   a. レポートの「**フォーマット**」列で、「**HTML**」または「**PDF**」をクリックします。 「オンデマンド・レポート・パラメーター (On-Demand Report Parameters)」ウィンドウが表示されます。
   b. 「オンデマンド・レポート・パラメーター (On-Demand Report Parameters)」ウィンドウで、必要なパラメーターを入力して、「**実行**」をクリックします。
2. レポートのスナップショットを作成するには、以下の手順を実行します。
   a. レポートを右クリックして、「**パラメーター**」をクリックします。 「レポート・パラメーター (Report Parameters)」ウィンドウが表示されます。
   b. 「レポート・パラメーター (Report Parameters)」ウィンドウで、必要なパラメーターを入力して、「**保管**」をクリックします。
   c. レポートを右クリックして、「**スナップショットの作成 (Create Snapshot)**」を選択します。
   d. 「レポート・パラメーター (Report Parameters)」ウィンドウで、必要なパラメーターを入力して、「**作成**」をクリックします。 「レポートのスナップショット (Report Snapshots)」ウィンドウが表示されます。ウィンドウにスナップショットの状況が示されます。
   e. 「レポートのスナップショット (Report Snapshots)」ウィンドウで、完成したスナップショットを右クリックし、「**表示フォーマット (View as)**」を選択して、スナップショットのフォーマットを HTML、PDF、Excel、PostScript のいずれにするかを指定します。

次のタスク

Business Intelligence Reporting Tool デザイナーを使用して、新規レポートを作成します。詳しくは、『Eclipse Business Intelligence Reporting Tool デザイナーを使用した新規レポートの作成』を参照してください。

Eclipse Business Intelligence Reporting Tool デザイナーを使用した新規レポートの作成

Eclipse Business Intelligence Reporting Tool デザイナーを使用して、レポートを作成して編集することができます。

このタスクについて

レポート設計をカスタマイズする方法のヒントについては、DeveloperWorks の「*Customizing Tivoli Common Reporting Report Designs*」(http://www.ibm.com/developerworks/tivoli/library/t-tcr/ibm_tiv_tcr_customizing_report_designs.pdf) を参照してください。

IBM Security Identity Manager データベースとスキーマについて詳しくは、「*Database and Schema リファレンス・ガイド*」を参照してください。このマニュアルは、http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/im51_dbschema.htmにあります。

手順

1. Eclipse Business Intelligence Reporting Tool デザイナーを、この Web サイト http://catalog.lotus.com/wps/portal/topal/details?catalog.label=1TW10OT02 からダウンロードします。
2. DVD メディア、またはPassport Advantage®からの ZIP ダウンロード・パッケージを開きます。 ファイルのリストを確認します。
3. ファイルを選択した順に Eclipse レポート・プロジェクトに配置します。

次のタスク

レポートの説明、およびレポートの出力例を表示します。詳しくは、『レポートの説明およびパラメーター』を参照してください。

レポートの説明およびパラメーター

このセクションでは、レポートおよびレポート・パラメーターについて説明します。

監査およびセキュリティー: アクセス

このセクションでは、システムのすべてのアクセス定義をリストする「監査およびセキュリティー」レポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 38. アクセス・レポートのフィルター

パラメーター	説明
アクセス・タイプ	共用フォルダーやアプリケーションなどのアクセスのタイプを表示します。このパラメーターのデフォルト値は、パーセント記号 (%) です。パーセント記号 (%) をワイルドカードとして使用できます。例えば、`%abc1%` とできます。アクセス階層を入力する場合は、`Parent Access:Child Access:Child's Child Access` などのフォーマットを使用します。
アクセス	レポートを生成するアクセスを表示します。「**任意**」は、選択したアクセス・タイプに基づいてすべてのアクセス権を含めることができることを示します。

表 38. アクセス・レポートのフィルター (続き)

パラメーター	説明
サービス	アクセスが関連付けられているサービス情報を表示します。
アクセス権の所有者 (個人)	アクセス管理所有者の名前を表示します。

休止アカウント

このセクションでは、最近使用されていないアカウントをリストする休止アカウント・レポートについて説明します。

最終アクセス情報を持たないアカウントは休止とは見なされません。休止ではないアカウントには、「**最終アクセス日付**」フィールドが空白になっている新規アカウントおよび未使用の既存のアカウントの両方が含まれます。これらのタイプのアカウントは、休止アカウント・レポートには表示されません。 サービスに対して調整を実行する必要があります。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 39. 休止アカウント・レポートのフィルター

パラメーター	説明
サービス	休止アカウントのサービス情報を表示します。
休止期間	休止日数を表示します。休止期間は、有効な正の整数でなければなりません。
アカウントが休止としてリストされた日	この日付において休止しているアカウントのリストを表示します。

個人に許可された資格

このセクションでは、資格が与えられたプロビジョニング・ポリシーを持つすべてのユーザーをリストする、個人に許可された資格レポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 40. 個人に許可された資格レポートのフィルター

パラメーター	説明
所有者 (個人)	資格が与えられた所有者を表示します。

注: このレポートには、直接資格が表示され、継承した資格は表示されません。

不適合アカウント

このセクションでは、すべての不適合アカウントをリストするレポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 41. 不適合アカウントのフィルター

パラメーター	説明
サービス	不適合アカウントのサービス情報を表示します。
アカウント準拠	アカウントの準拠理由を表示します。例: 「却下」または「非準拠」

孤立アカウント

このセクションでは、所有者を持たないすべてのアカウントをリストするレポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 42. 孤立アカウント・レポートのフィルター

パラメーター	説明
サービス	孤立アカウントのサービス情報を表示します。
アカウント状況	孤立アカウントの状況を表示します。例: 「アクティブ」または「非アクティブ」

要求: 承認および否認

このレポートは、承認または否認された要求アクティビティーを示します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 43. 承認および否認レポートのフィルター

パラメーター	説明
承認者	特定の承認者によって行われた要求に関する情報を表示します。
ユーザー ID	ユーザーの ID 情報を表示します。パーセント記号 (%) をワイルドカードとして使用できます。例: `%joe01%`
サービス	承認および否認のサービス情報を表示します。
承認要求状況	承認要求の状況を表示します。
承認アクティビティー名	承認アクティビティーの名前を表示します。パーセント記号 (%) をワイルドカードとして使用できます。例: `%Approval for joe01%`
日付範囲	承認の日付範囲を日数で表示します。
開始日	承認および否認の開始日を表示します。
終了日	承認および否認の終了日を表示します。

職務分離ポリシー・レポート

このセクションでは、さまざまな職務分離ポリシー・レポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 44. 職務分離ポリシー定義レポートのフィルター

パラメーター	説明
職務分離ポリシー	職務分離ポリシーの名前を表示します。
ビジネス単位	ビジネス単位の名前を表示します。
注: ポリシー名およびビジネス単位パラメーターは、それぞれに対応するメニューから選択する必要があります。	

職務分離違反レポート

このセクションでは、職務分離違反レポートについて説明します。このレポートには、個人、ポリシー、違反したルール、承認および理由 (ある場合)、違反となる変更を要求したユーザーが表示されます。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 45. 職務分離違反レポート

パラメーター	説明
ポリシー	職務分離ポリシーの名前を表示します。
ビジネス単位	ビジネス単位の名前を表示します。
ルール名	職務分離ポリシーに関連付けられたルール名を表示します。

サービス

このセクションでは、システムに現在定義されているサービスをリストするレポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 46. サービス・レポートのフィルター

パラメーター	説明
サービス	サービス情報を表示します。
所有者 (個人)	サービス所有者情報を表示します。
ビジネス単位	ビジネス単位の名前を表示します。

サービスに関連するアカウントの要約

このセクションでは、システムに定義された特定サービスに関連するアカウントの要約をリストするレポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 47. サービスに関連するアカウントの要約レポートのフィルター

パラメーター	説明
サービス	アカウントのサービス情報を表示します。

表 47. サービスに関連するアカウントの要約レポートのフィルター (続き)

パラメーター	説明
アカウント状況	サービス・アカウントの状況を表示します。例: 「アクティブ」または「非アクティブ」

サスペンドされたアカウント

このセクションでは、サスペンドされたアカウントをリストするレポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 48. サスペンドされたアカウント・レポートのフィルター

パラメーター	説明
ユーザー ID	ユーザーの ID 情報を表示します。パーセント記号 (%) をワイルドカードとして使用できます。
アカウント所有者 (個人)	サスペンドされたアカウントの所有者情報を表示します。
サービス	サスペンドされたアカウントのサービス情報を表示します。
日付範囲	サスペンドされたアカウントでの日付範囲の日数を表示します。
開始日	サスペンドされたアカウントの開始日を表示します。
終了日	サスペンドされたアカウントの終了日を表示します。

ユーザー再認証ヒストリー・レポート

このセクションでは、(特定の再認証プログラムにより) 手動で、または (タイムアウト・アクションのため) 自動で実行されたユーザー再認証のヒストリーをリストするレポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 49. ユーザー再認証ヒストリー・レポートのフィルター

パラメーター	説明
日付範囲	ユーザー再認証ヒストリーの日付範囲を日数で表示します。 **注:** 標準レポート期間 (例えば、過去 30 日) を選択するか、レポートの特定の開始日と終了日を入力することができます。
開始日	ユーザー再認証ヒストリーの開始日を表示します。
終了日	ユーザー再認証ヒストリーの終了日を表示します。
ビジネス単位	ビジネス単位の名前を表示します。
ユーザー再認証ポリシー	ユーザー再認証ポリシーに関する情報を表示します。
ユーザー	ビジネス単位からのユーザーを表示します。パーセント記号 (%) をワイルドカードとして使用できます。例: `%joe%`
ユーザー状況	選択されるユーザーの状況を表示します。
再認証プログラム	再認証プログラムとして選択されるユーザーを表示します。

表 49. ユーザー再認証ヒストリー・レポートのフィルター (続き)

パラメーター	説明
再認証の決定	選択される再認証の決定を表示します。

ユーザー再認証ポリシー定義レポート

このセクションでは、システムに定義されたユーザー再認証ポリシーに関する情報をリストするレポートについて説明します。

次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 50. ユーザー再認証ポリシー定義レポートのフィルター

パラメーター	説明
ユーザー再認証ポリシー	ユーザー再認証ポリシーの名前を表示します。
ビジネス単位	ビジネス単位の名前を表示します。

ユーザー再認証ポリシー詳細定義レポート

詳細定義レポートには、この情報が表示されます。

- ユーザー再認証ポリシー情報
- 再認証プログラム情報
- 役割ターゲット
- アカウント・ターゲット
- グループ・ターゲット

共有アクセス監査履歴レポート

このレポートには、共有アクセス監査履歴が示されます。次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 51. 共有アクセス監査履歴レポートのフィルター

パラメーター	説明
日付範囲	共有アクセスの日付範囲を日数で表示します。 **注:** リモート・マシンにインストールされている Tivoli Common Reporting を使用できます。まれですが、レポートにデータがまったく、または一部しか表示されないことがあります。この省略を防止するには、Security Identity Manager サーバーでの日時を入力してください。
開始日	共有アクセス履歴の開始日を表示します。
終了日	共有アクセス履歴の終了日を表示します。
サービス・ビジネス単位	サービスに関連付けられたビジネス単位を表示します。
サービス	共有アクセスが関連付けられているサービス情報を表示します。
共有アクセス所有者のビジネス単位	共有アクセス所有者に関連付けられているビジネス単位を表示します。
共有アクセス所有者	共有アクセス所有者の名前を表示します。

表 51. 共有アクセス監査履歴レポートのフィルター (続き)

パラメーター	説明
共有アクセス	資格情報名や資格情報プール名などの、共有アクセス資格の名前を表示します。

所有者に基づいた共有アクセス資格

このレポートには、選択した所有者の共有アクセス資格が示されます。次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

表 52. ユーザーに基づいた共有アクセス資格レポートのフィルター

パラメーター	説明
サービス・ビジネス単位	サービスに関連付けられたビジネス単位を表示します。
サービス	共有アクセス資格が関連付けられているサービス情報を表示します。
共有アクセス所有者のビジネス単位	共有アクセス所有者のビジネス単位名を表示します。
共有アクセス所有者	共有アクセス所有者 (個人または役割) 名を表示します。

役割に基づいた共有アクセス資格

このレポートには、選択した役割の共有アクセス資格が示されます。次の表では、レポートを仕様に合うようにフィルタリングする際に使用できるパラメーターについて説明します。

所有者属性はデフォルトで表示されません。「組織の役割」の「所有者」属性は、スキーマ・マッピングと関連付ける必要があります。

「*IBM Security Identity Manager 管理ガイド*」のトピック『レポート・スキーマ・マッピング』を参照してください。

表 53. 役割に基づいた共有アクセス資格レポートのフィルター

パラメーター	説明
ビジネス単位	ビジネス単位の名前を表示します。
役割	役割のリストを表示します。
資格タイプ	資格情報や資格情報プールなどの資格のタイプを表示します。

レポートの保守

保守期間の一例としては、通常のダウン時間がビジネス要件に影響しない期間が考えられます。保守作業の一例として、データベース資格情報のパスワードが失効するか、変更される場合が挙げられます。

JAAS 認証別名の変更

データベースのユーザー名またはパスワードが変更された場合は、Java 認証・承認サービス (JAAS) の認証別名を更新する必要があります。

手順

1. コマンド・シェルを開きます。
2. 次のようにして、modify コマンドで参照できるように構成オブジェクトを識別します。

   ```
   wsadmin>print AdminConfig.list("JAASAuthData")
   ```

   表示する構成オブジェクトは以下のような値です。

   ```
   (cells/tcrCell|security.xml#JAASAuthData_1202487694421)
   ```

3. 以下のコマンドを実行して、パスワードとユーザー ID を変更します。

   ```
   wsadmin>AdminConfig.modifyconfiguration_object
        [["userid", "newid"]])
       [["password", "newpassword"]])
   ```

   各部の意味は、次のとおりです。

   - *configuration_object* は、事前に識別したオブジェクトです。
   - *newid* は、データベースの新規ユーザー ID です。
   - *newpassword* は、このユーザー ID に関連付けられている新規パスワードです。

例

次の例では、構成オブジェクト (cells/tcrCell|security.xml#JAASAuthData_12024876944 21) のパスワードを mynewpassword に変更します。

```
wsadmin>AdminConfig.modify("(cells/tcrCell|
security.xml#JAASAuthData_12024876944 21)",
[["password", "mynewpassword"]])
```

同様の呼び出しを使用して、userId 属性を更新することができます。

次のタスク

JDBC プロバイダーを変更します。詳しくは、『JDBC プロバイダーの変更』を参照してください。

JDBC プロバイダーの変更

あるデータベース・ベンダー (Oracle、Microsoft SQL など) から別のデータベース・ベンダー (DB2 など) にマイグレーションすると、JDBC ドライバーが変更されます。データベース・ベンダーのプラットフォームをまたがって (Oracle から DB2 など) データベースをマイグレーションすることができます。既存の JDBC 構成を削除して、JDBC プロバイダーとデータ・ソース構成を作成します。

このタスクについて

構成セクションでデータ・ソース構成を作成するには、以下の手順を実行します。

手順

1. 以下のようにしてデータ・ソースを除去します。

```
wsadmin> AdminConfig.remove(
 AdminConfig.getid("/DataSource:ITIM DB Data Source"))
```

2. データ・ソースを除去した後、以下のようにして JDBC プロバイダーを除去します。

```
wsadmin> AdminConfig.remove(
 AdminConfig.getid("/JDBCProvider:JDBC provider for the ITIM DB"))
```

3. 新しいベンダーおよびデータベースの JDBC プロバイダーとデータ・ソースを作成します。詳しくは、203 ページの『Java Database Connectivity (JDBC) プロバイダーの作成』を参照してください。

次のタスク

データ・ソースを変更します。詳しくは、『データ・ソースの変更』を参照してください。

データ・ソースの変更

データベース・サーバーのホストまたはポート、またはデータベース名が変わる場合は、データ・ソース構成を更新する必要があります。

このタスクについて

Oracle データベースの場合、この構成では、新しい JDBC URL を反映するように URL プロパティーを変更する必要があります。DB2 および Microsoft SQL Server データベースの場合、この構成では、変更された特定のプロパティーに対して変更を加える必要があります。次の例では、`portNumber` プロパティーが `1435` に更新されます。

例

```
AdminConfig.modify(AdminConfig.getid("/DataSource/
ITIM DB Data Source/J2EEResourcePropertySet:/
J2EEResourceProperty/portNumber/"),
[["value", "1435"]])
```

同様のコマンドを使用して、以下に示すその他のデータ・ソース J2EE リソース・プロパティーを更新できます。

`URL` (Oracle データベースの場合)

`serverName` および `databaseName` (DB2 および Microsoft SQL Server データベースの場合)

次のタスク

構成変更を保存します。詳しくは、『構成変更の保存』を参照してください。

構成変更の保存

データ・ソースの変更を更新するには、構成を保存する必要があります。

このタスクについて

データ・ソース構成を保存するには、以下の手順を実行します。

手順

1. **wsadmin** コマンドを使用して、構成を保存します。
2. WebSphere Application Server を再始動します。

タスクの結果

構成変更が WebSphere Application Server に保存されます。

デバッグ

このトピックでは、デバッグの手順を示します。

レポート生成およびフォーマット設定のエラー

このトピックでは、レポート生成およびフォーマット設定のエラーについて説明します。

このタスクについて

レポートのフォーマット設定が失敗すると、次のようなエラー・メッセージが表示されます。

```
CTGTRV014E: エラーで終了したため、レポートは正常にフォーマット設定できません。
参照 ID (The report cannot be successfully formatted because it completed with errors,
reference ID) [REPORTIT_33_OBJECTID_7fe67fe6]
エラーのあったレポートを表示するには、次のリンクをクリックしてください。
(Click on the following link to view the report with the errors.)
CTGTRV011E: 詳しくは Tivoli Common Reporting ログ・ファイルを参照してください。
(See the Tivoli Common Reporting log files for more information.)
https://localhost:30343/TCR/Reports/view
```

フォーマット設定のエラーのあったレポートとその詳細をレポートで表示するには、以下の手順を実行します。

手順

1. エラー・メッセージ内のリンクをクリックします。 生成されたレポートのエラーを確認してください。
2. スクロールダウンして、レポートの下部にある赤いテキストのエラーを表示します。
3. エラー・メッセージの表題の横にある正符号 (+) をクリックします。 リストを展開すると、スタック・トレース全体を表示できます。このスタック・トレースは、問題を識別したり、エラーの種類を見分けるのに役立ちます。例えば、データ・ソースのパスワードの期限が切れている場合は、**wsadmin** コンソールでデータベース資格情報に対して特定の更新を行う必要があります。Tivoli Common Reporting では、データベースまたは JDBC の資格情報を更新するための保守が必要です。
4. Eclipse Business Intelligence Reporting Tool デザイナーでレポートを変更して、問題を修正します。

次のタスク

ログを確認します。詳しくは、『ログ』を参照してください。

ログ

このセクションでは、Tivoli Common Reporting に関連付けられたログについて説明します。

このタスクについて

Tivoli Common Reporting には、次の 2 つのログ・ファイルがあります。

SystemErr.log
システム・エラー・ログを示します。

SystemOut.log
システム出力ログを示します。

これらのログ・ファイルは、次のいずれかのディレクトリーにあります。

- `TCR_HOME¥eWas61¥profiles¥tcrProfile¥logs¥tcrServer`
- Tivoli Common Reporting がインストールされている一時ディレクトリー。例えば、Windows では `C:¥temp`、UNIX では `/temp` です。

ログの情報の解釈方法については、Tivoli Common Reporting インフォメーション・センター http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.tivoli.tcr.doc/tcr_welcome.html を参照してください。

新しい Tivoli Common Reporting レポートのロギングおよび作成について詳しくは、「*Report Logging for JavaScript Routines*」を参照してください。

http://www.ibm.com/developerworks/tivoli/library/t-tcr/ibm_tiv_tcr_report_logging.pdf

Tivoli Common Reporting は、ロガー・スクリプトを使用してレポート生成時のログを記録します。

既知の問題および解決策

このセクションでは、Tivoli Common Reporting に関連する既知の問題および解決策について説明します。

棒グラフの小さい方の値が表示されない

問題

棒グラフで、2 つの合計値が一定の距離を置いて表示される場合、小さい方の値が表示されないことがあります。例えば、孤立アカウント・レポートを実行するときに、あるサービスには休止アカウントが 10,000 個あるとします。もう一方のサービスには、休止アカウントが 3 つしかありません。この場合ソフトウェアには、休止アカウントが 3 つだけのサービスを表示しません。

解決策

この省略は既知の問題です。

Eclipse Business Intelligence Reporting Tool 図表エンジンが一部の X 軸カテゴリーを表示しない

問題

図表付きのレポートを実行すると、X 軸カテゴリーの一部の有効な項目が表示されないことがあります。

解決策

このすべての使用可能な項目が欠落することは、既知の問題です。

図表の凡例に却下シリーズが表示されたままになる

問題

アカウント準拠パラメーターを「却下」に設定して不適合アカウント・レポートを実行すると、そのパラメーターによって不適合アカウントは除外されますが、図表には依然として「非準拠」が表示されます。

解決策

以下の手順を実行します。

1. 図表を非準拠シリーズなしで複写しますが、却下シリーズは保持します。
2. この図表を却下シリーズなしでもう一度複写し、非準拠シリーズは保持します。これで非準拠レポートの図表は 3 つになります。
3. アカウント準拠パラメーターの値に基づいて、各図表の可視性を条件付きで設定します。

PDF レポートを実行すると Firefox バージョン 1.5 に前のレポート生成が表示される

問題

レポートを実行し、PDF 出力を指定できます。次に、同じレポートを異なるパラメーターで 2 回目に実行する間、レポート・ウィンドウを開いたままにします。Firefox バージョン 1.5 に、2 番目のレポートを表示する代わりに、最初の PDF レポートが再表示されます。Tivoli Common Reporting では 2 回目のレポートが実行され、Firefox に送信されていることが確認されますが、Firefox バージョン 1.5 には最初の PDF レポートが再表示されます。

解決策

ウィンドウを開いたままレポートを実行しないでください。

グラフ図表の凡例に、定義されたすべてのシリーズが表示される

問題

レポート・パラメーターが指定されたシリーズ値を除外する可能性がある場合でも、図表にはすべてのシリーズが表示されます。

解決策

この表示でのフィルター処理の欠落は、既知の問題です。

レポート内のハイパーリンクが常に表示される

問題

個人に許可された資格レポート上のドリルダウン・ハイパーリンクでは、パラメーターに対して所有者が指定されている場合でも、常にハイパーリンクが表示されます。

解決策

Eclipse Business Intelligence Reporting Tool では、JavaScript を使用してハイパーリンクを条件付きで使用不可にすることができません。

テーブル行の最終レコードが 2 ページに分割される

問題

Eclipse Business Intelligence Reporting Tool では、テーブル行が 2 ページに分割されることがあります。

解決策

この行の分割は既知の問題です。

大量の結果セットに対して OutOfMemoryException エラーが発生する

問題

デフォルトの組み込み 組み込み WebSphere Application Server Java Virtual Machine (JVM) 構成が原因で、メモリーが不足する可能性があります。この問題は、結果セットを大量に含む (数万単位) レポートを処理するときに発生します。

解決策

以下のように、Tivoli Common Reporting 組み込み WebSphere Application Server サーバー上で **wsadmin** コマンドを使用して、JVM 最大ヒープ・サイズを変更します。

1. 以下のコマンドを入力します。

```
AdminConfig.modify(
 AdminConfig.getid("/JavaVirtualMachine:/"),
  [["maximumHeapSize", "1024"]])
```

これにより、最大ヒープ・サイズが 1024 MB に設定されます。

2. AdminConfig.save() を使用して、変更を保存します。
3. Tivoli Common Reporting サーバーを再始動して、構成変更が有効になるようにします。

JVM プロセスの現在の構成を取得するには、以下の **wsadmin** コマンドを入力します。

```
print AdminConfig.show(
 AdminConfig.getid("/JavaVirtualMachine:/"))
```

OutOfMemoryException ログは Tivoli Common Reporting WebSphere トレース・ログ内にあります。

パラメーター・リストに重複する名前が表示される

問題

動的リスト・ボックス・パラメーターで重複する値を使用する場合、適切な項目を選択できないことがあります。例えば、異なる 2 人のユーザーの名前がどちらも Bob Smith であり、それらの基盤となる値が固有の ID であるとします。この場合、レポートを実行すると、IBM Security Identity Manager は Bob Smith を 2 回表示しますが、これは基盤となる値が固有であるためです。しかし、ユーザーがドロップダウン・リストから 2 番目の Bob Smith 項目を選択すると、リストでは常に最初の Bob Smith が選択されます。

解決策

Eclipse Business Intelligence Reporting Tool デザイナーでレポートを実行して、プレビューを選択し、「**ファイル**」->「**レポートの表示**」を選択すると、2 つのパラメーターが正しく選択されます。

大規模レポートの PDF がロードされない

問題

大規模なレポートを実行するときに、データをフィルタリングするためのレポート・パラメーターを何も指定しないと、PDF 出力がロードされません。

解決策

多くの結果を伴う可能性のあるレポートを実行する場合は、できるだけ多くのレポート・パラメーターを指定します。また、大規模なレポートを実行する場合は、HTML 出力オプションを指定してください。

円グラフの値が重なり合う

問題

「サスペンドされたアカウント」レポート図表などの円グラフで、小さなシリーズ区分の数値が重なり合い、読めなくなることがあります。

解決策

この値の重なり合いは既知の問題です。

レポート・パラメーター・リストに一部の値が表示されない

問題

Tivoli Common Reporting ユーザー・インターフェースでは、リストでのレポート・パラメーターの表示が限定されます。

解決策

必要な値がリストに表示されない場合は、その値の先頭から文字をいくつか入力します。文字は、リストに値が表示されて選択できるようになるまで入力してください。例えば、IBM Security Identity Manager デプロイメントで、**ホスト・サービス** *N* サービス定義が 1000 個セットアップされているとします。変数 *N* は、ホスト・サービスの名前です。「**Hosted service 810**」を選択するには、`Hosted service 81` と入力します。

レポートにビジネス・パートナー個人を含めることができない

問題

Eclipse Business Intelligence Reporting Tool レポート・デザイナーを介してレポートをカスタマイズしないと、IBM Security Identity Manager レポートでビジネス・パートナー個人についてのレポートを作成することができません。

解決策

レポートのカスタマイズについては、DeveloperWorks の「*Customizing Tivoli Common Reporting Report Designs*」 (http://www.ibm.com/developerworks/tivoli/library/t-tcr/ibm_tiv_tcr_customizing_report_designs.pdf) を参照してください。

大規模なレポートを実行するとメモリーがフラグメント化される

問題

Tivoli Common Reporting トレース・ファイルによると、大規模なレポート (例えば 400,000 行あるレポートなど) の生成は、正常に実行できます。大規模なレポート・データ・セットのトレース・メッセージの例を以下に示します。

```
[3/21/08 1:13:55:593 IST] 00000026 DiskCache     I
プロセス終了。データ数は 418128 です。
(End of process, and the count of data is 418128)
```

レポートされるデータ量が原因で、多くのレポートで Java Virtual Machine (JVM) メモリー割り振りに関連した問題が発生する可能性があります。ボリュームにより、JVM でメモリーのフラグメント化が引き起こされる可能性があります。メモリー不足例外のため、後続のレポートの実行が失敗する可能性があります。

解決策

Tivoli Common Reporting サーバーを再始動します。

サービス・パラメーターが無効値を表示する

問題

レポートで使用されたサービス・パラメーターは、すべてのサービス名をリストに表示します。しかし、IBM Security Identity Manager コンソールには、特定のサービス・パラメーター値が表示されません。

解決策

このレポートとコンソールのリストにおける差異は、既知の問題です。

スナップショット・パラメーターが通常のテキストを表示しない

問題

スナップショット・パラメーターが、動的リスト・ボックス・パラメーターの通常の表示テキストではなく、固有値を表示します。

解決策

この固有値の表示は既知の問題です。

スナップショット・レポートが Excel フォーマットでは空である

問題

レポートのスナップショットを作成し、そのスナップショットを実行したときに返された結果がゼロ個の場合、Microsoft Excel フォーマットのスナップショットをダウンロードすると、Excel エラーが発生します。例えば、以下のとおりです。

```
'スタイルの XML エラー (XML ERROR in Style)'
```

PDF フォーマットおよび HTML フォーマットは正しくダウンロードされます。

解決策

この省略は既知の問題です。

アジア言語を使用すると、レポートのテキストが正しく表示されない

問題

レポートを実行して、その結果を PDF または HTML フォーマットで表示しようとすると、テキストが壊れているように表示されます。この問題は、中国語、韓国語、および日本語を使用する場合に発生します。

解決策

Tivoli Common Reporting は、サーバー上で図表をイメージにレンダリングします。サーバーに使用言語のフォント・サポートが存在しない場合、図表のテキストは文字化けして表示されます。

適切なアジア言語のフォントをオペレーティング・システムにインストールし、有効にします。例えば、Windows の場合は以下の手順を実行します。

1. 「**スタート**」->「**コントロール パネル**」->「**地域と言語のオプション**」をクリックします。
2. 「**言語**」タブを選択します。
3. 「**東アジア言語のファイルをインストールする**」チェック・ボックスを選択して、「**OK**」を 2 回クリックします。

ユーザー DN レポート・パラメーターのスケールの問題

IBM Tivoli Common Reporting ベースの IBM Security Identity Manager レポートの「**ユーザー**」ドロップダウン・リストで**「ユーザー DN」**パラメーターが完全なスケールでは表示されません。

問題

User Dn パラメーターは、ユーザー・エントリー数が多い場合、「**ユーザー**」ドロップダウン・リストで完全なスケールで表示されません。ユーザー・エントリーが多くなる例の 1 つは、「個人に許可された資格」レポートです。

解決策

以下の手順を実行します。

1. Eclipse Business Intelligence Reporting Tool デザイナーを使用して、**User Dn** 動的ドロップダウン・リストのレポート・パラメーターを持つ Tivoli Common Reporting レポートを変更します。**User DN** レポート・パラメーターを、静的テキスト・ボックスのレポート・パラメーターに変更します。
2. `Entitlements Granted to an Individual Table` という名前のデータ・セットで、パラメーターを「`AND NAPerson.DN like ?`」 から「`AND NAPerson.GIVENNAME like ?`」に置き換えます。
3. Eclipse Business Intelligence Reporting Tool デザイナーで、変更処理を正常に実行します。次に、レポート・パッケージのエクスポートされた ZIP アーカイブ・ファイルを Tivoli Common Reporting にインポートします。そこでは、この変更されたレポートを **User Dn** パラメーターなしで実行することができます。

第 17 章 ID フィードの管理

アドミニストレーターは、1 つ以上の人材管理リソース・リポジトリーから従業員のデータを取り込むため、いくつかの初期ステップを実行する必要があります。そのデータを使用して、IBM Security Identity Managerレジストリーに同等のユーザー・セットを取り込みます。

概説

ID とは、1 つ以上のリポジトリーで個人を一意的に表すプロファイル・データと、その個人に関連する追加情報のサブセットです。例えば、個人の名前、姓、氏名、および従業員番号の固有の組み合わせによって ID が表現されることがあります。データには、電話番号、担当マネージャー、および電子メール・アドレスなどの追加情報が含まれていることもあります。データ・ソースは、顧客のユーザー・リポジトリーまたはファイル、ディレクトリー、カスタム・ソースなどです。

IBM Security Identity Managerを使用し、ユーザー・リポジトリー、ディレクトリー、ファイル、またはカスタム・ソースなどのデータ・ソースを読み取ることにより、多数のユーザーをシステムに追加します。ユーザー・データ・リポジトリーを基にユーザーを追加する処理を *ID* フィードまたは *HR* フィードと呼びます。

ID フィードにおける*調整*とは、データ・ソースと IBM Security Identity Manager 間のデータ同期処理を指します。初回調整では IBM Security Identity Manager に新規ユーザー (プロファイル・データを含む) が取り込まれます。後続の調整では、新規ユーザーの作成と、検出された各既存ユーザーのユーザー・プロファイルの更新の両方が実行されます。

ID レコードを IBM Security Identity Manager のユーザー・レジストリーに読み込むために、複数のソース・フォーマットを使用できます。

ユーザー・レコードで情報が欠落している場合の影響を予想しておく必要があります。例えば、IBM Security Identity Managerに送るレコードにユーザーの電子メール・アドレスが含まれていない可能性があります。その場合、そのユーザーは新規アカウントのパスワードを電子メールで受信できないため、ヘルプ・デスクに問い合わせるか、マネージャーに連絡する必要があります。

ID フィードの一般的ソース

IBM Security Identity Manager では、ID フィードに使用する一般的なソースの大部分を扱うために以下のサービス・タイプを提供しています。

- コンマ区切り値 (CSV) ID フィード
- DSML ID フィード
- AD OrganizationalPerson ID フィード (Microsoft Windows Active Directory)
- INetOrgPerson (LDAP) ID フィード
- IDI データ・フィード

以下のソースから初期内容と以降の変更内容をユーザー・レジストリーに取り込むことができます。

コンマ区切り値 (CSV) ファイル
コンマ区切り値 (CSV) ファイルを使用します。CSV ファイルでは、一連のレコードが復帰改行 (CR/LF) フィード・ペアで区切られています。各レコードには、コンマで区切られたフィールドのセットが含まれています。グローバル識別ポリシーを使用して、ユーザー ID を作成するスキーマ属性を選択できます。

Directory Services Markup Language (DSML) v1 ファイル
DSML v1 ファイルを使用してユーザー・レジストリーにデータを取り込みます。DSML ファイルは、XML ファイル・フォーマットのディレクトリー構造情報を表します。ID フィードを複数回実行する場合、重複ユーザーは最新のファイルに基づいて更新されます。グローバル識別ポリシーは DSML ファイルには適用されません。

Windows Server Active Directory
Windows Server Active Directory から、Windows Server Active Directory ユーザーの `inetOrgPerson` スキーマ部分で検出された情報のみをインポートします。グローバル識別ポリシーを使用して、ユーザー ID を作成するスキーマ属性を選択できます。ID フィード・プロセスでは、指定されたベースのすべてのユーザー・オブジェクトが使用されます。

INetOrgPerson ID フィード
LDAP ディレクトリー・サーバーを使用します。このデータでは、サービス定義に指定された個人のプロファイル名が暗示するオブジェクト・クラスを使用しています。グローバル識別ポリシーを使用して、ユーザー ID を作成するスキーマ属性を選択できます。ID フィード・プロセスは、指定されたオブジェクト・クラスを持たないレコードを無視します。

カスタム ID ソース
カスタム ID ソースを使用して、初回の内容と以降の変更内容をユーザー・レジストリーに取り込みます。ID ソースによっては、グローバル識別ポリシーを使用して、ユーザー ID を作成するスキーマ属性を選択できます。

例えば IBM Tivoli Directory Integrator ID フィードを使用すると、標準データ・フィードよりも柔軟性が向上します。追加される機能には以下のものがあります。

- データ・サブセットの処理 (指定部門のユーザーの選別など)。
- 標準マッピング以外の追加属性マッピングを使用可能にする。
- 他のデータ・ソースから取得したデータ (従業員の担当マネージャーなど) のデータ検索を使用可能にする。
- データ・ソースの変更検出。
- データベースおよび人材管理システム (DB2 Universal Database™ および SAP など) の使用。
- 属性の制御、例えば、個人のサスペンドなどの状況更新。
- ID レコードの削除。
- IBM Security Identity Manager 調整ではなく IBM Tivoli Directory Integrator を使用した変更の実行。

カスタマイズ ID フィードの提供方法についての詳細は、IBM Security Identity Manager extensions ディレクトリーでの IBM Tivoli Directory Integrator 統合の情報を参照してください。

ID フィードのワークフローの使用可能化

使用するメソッドに関わらず、IBM Security Identity Manager Server を構成して、ID フィード・レコード用のワークフロー・エンジンを呼び出すことができます。ワークフロー・エンジンを使用可能にすると、着信する ID の該当するプロビジョニング・ポリシーすべてが強制的に適用されます。構成の結果、フィードの実行速度が遅くなります。ワークフロー・エンジンで ID フィードが使用可能にされていない場合であっても、個人は、すべての適用可能な動的役割に自動的に登録されます。初期読み込みの場合は、システムに ID をインポートした後で、適用可能なプロビジョニング・ポリシーを使用可能化して、ID フィードのパフォーマンスを向上することを検討してください。

コンマ区切り値 (CSV) ID フィード

コンマ区切り値 (CSV) ID フィードは、コンマ区切り値 (CSV) ファイルを読み取って IBM Security Identity Manager にユーザーを追加する機能を提供します。

CSV サービス・タイプ

この ID フィード・サービス・タイプは、RFC 4180 文法に準拠した CSV ファイル形式を使用して ID フィードを解析します。IBM Security Identity Manager パーサーには、以下の RFC 拡張機能が用意されています。

- フィールド内の引用符のないテキストから先頭と末尾の空白文字を切り取ります。それとは異なり、RFC 4180 では、すべてのスペース文字を (引用符区切り文字の内側や外側に関係なく) 有効と見なします。
- 引用符で囲んだテキストと囲んでいないテキストを同じフィールドに表示できます。それとは異なり、RFC 4180 では、両方のテキスト・タイプを同じフィールドに表示することはできません。
- すべてのレコードのフィールド数を同一にするという RFC 4180 の制限を適用しません。ただし、CSV ヘッダーのフィールド数を超えている数のフィールドを持つレコードがあれば、CSV パーサーを呼び出すコードはエラーを報告します。
- レコードの終了位置では、復帰 (CR) を使用するか、または復帰/改行 (CR/LF) を使用して UNIX と DOS の両方の基本ファイルとの互換性を持たせることができます。それとは異なり、RFC 4180 はすべてのレコードを復帰/改行 (CR/LF) で終了します。

CSV ファイルを使用するサービス

IBM Security Identity Manager では、以下のサービス・タイプで、CSV ファイルを入力として使用します。

- CSV ID フィード
- 手動サービス・プロバイダー・タイプを使用するカスタム・サービス。この種のカスタム・サービスでは、調整アップロード・ファイルに CSV ファイル形式を使用します。このサービス・タイプは、ID フィードにもアカウント・フィードにも使用できます。

デフォルトでは、手動サービス調整用に CSV ファイルで定義されたすべてのアカウントは、IBM Security Identity Manager でアクティブとしてマークされます。手動サービス調整を使用して、個人またはアカウントをサスペンドするには、ID またはアカウントのどちらのフィードであるかに基づいて、erpersonstatus 属性または eraccountstatus 属性を CSV ファイルに追加します。値 0 (ゼロ) は、アクティブであることを示します。値 1 は、非アクティブであることを示します。

- IBM Tivoli Directory Integrator CSV コネクターを使用する Directory Integrator アダプター・プロバイダー・タイプを使用するカスタム・サービス。このサービス・タイプは、ID フィードにもアカウント・フィードにも使用できます。

CSV ファイル形式

CSV ファイルには、復帰/改行 (CR/LF) のペア (¥r¥n) または改行 (LF) 文字で区切られたレコードのセットが含まれています。各レコードには、コンマで区切られたフィールドのセットが含まれています。フィールドにコンマまたは CR/LF が含まれている場合は、区切り文字として二重引用符を使用してコンマをエスケープする必要があります。CSV ソース・ファイルの最初のレコードでは、その後のそれぞれのレコードで提供される属性を定義します。例えば、以下のとおりです。

```
uid,sn,cn,givenname,mail,initials,employeenumber,erroles
```

sn 属性と cn 属性は、IBM Security Identity Manager で使用するオブジェクト・クラスで個人を表すために必要な属性です。ID フィード・プロセスは、そのファイルに記述されているすべてのオブジェクトを使用します。CSV ファイルにバイナリー属性を組み込むことはできません。

多値属性を使用して、複数のグループでメンバーシップを持つユーザーを指定することができます。グループには、サービス所有者、Windowsローカル管理 (自己定義グループ)、およびマネージャーなどがあります。複数の値を持った属性を含める場合は、同じ属性名を持つ複数の列を使用して表す必要があります。

多値属性を指定するには、必要な回数だけ列を繰り返します。例えば、以下のとおりです。

```
cn, erroles, erroles, erroles, sn
cn1,role1, role2, role3, sn1
cn2,rolea,,,sn2
```

IBM Security Identity Managerに送るレコードには、ユーザーの電子メール・アドレスが含まれていないことがあります。その場合、そのユーザーは新規アカウントのパスワードが記載された通知電子メールを受信することができず、ヘルプ・デスクに問い合わせるか、マネージャーに連絡する必要があります。

IBM Tivoli Directory Integrator の CSV コネクター

IBM Tivoli Directory Integrator の CSV コネクターについての情報は、以下の製品ディレクトリーにあります。

ITIM_HOME/extensions/examples/idi_integration/HRFeedCSV/ITDIFeedExpress

ID フィード・ファイルの UTF-8 エンコード

ID フィード・ファイルは、UTF-8 形式でなければなりません。そのため、UTF-8 エンコードをサポートするエディターを使用する必要があります。

- Windows

  Microsoft Word 97 かそれ以降、または Windows 2003 Server または Windows XP オペレーティング・システムに含まれているメモ帳エディターは、UTF-8 に対応しています。

  メモ帳を使用してファイルを UTF-8 形式で保存するには、「**ファイル**」 > 「**名前を付けて保存**」をクリックします。「**文字コード**」フィールドの選択項目のリストを展開し、「UTF-8」を選択します。

- Linux

  Vim テキスト・エディター (標準的な vi エディターのバージョンの一つ) は、UTF-8 に対応しています。vim テキスト・エディターを使用して UTF-8 形式のファイルを扱うには、以下の指定を行います。

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  ご使用になっている UNIX のバージョンにこのテキスト・エディターがない場合、次の Web サイト (英語) にアクセスしてみてください。

  http://www.vim.org

注: 7 ビット ASCII コード・サブセットについては、UTF-8 エンコードの Unicode 形式は、7 ビット ASCII 形式と同一です。したがって、7 ビット ASCII を含む入力ファイル (16 進 20 から 16 進 7e の間の ASCII 文字値) に関しては、ファイル作成に通常のテキスト・エディターを使用することができます。他の文字値を含むファイル (ヨーロッパの拡張文字を含む) については、UTF-8 形式でファイルを保存する必要があります。

UTF-8 がサポートする 7 ビット ASCII 文字の正確なリストを得るには、次の Web サイト (英語) にアクセスして、最初の欄にある「**Basic Latin**」というリンクをクリックします。

http://www.unicode.org/charts

Directory Services Markup Language (DSML) ID フィード

Directory Services Markup Language (DSML) ID フィードは、DSML ファイルを読み取って IBM Security Identity Manager にユーザーを追加する機能を提供します。

DSML サービス・タイプ

IBM Security Identity Manager Server では、さまざまな人的資源 (HR) タイプのデータ・フィードを統合できます。手動で各個人を追加しなくても、多数の個人を IBM Security Identity Manager Server に追加することができます。HR データの ID レコードは、IBM Security Identity Manager の個人オブジェクトのインスタンスになります。HR タイプ・データ・フィードのタイプの 1 つは、DSML ID フィー

ド・サービスです。このサービスは、2 つの方法のいずれか (調整またはイベント通知プログラムを介した非送信請求イベント通知) で情報を受け取ることができます。

IBM Security Identity Manager で HR データを処理する機構では、HR データを XML フォーマットにする必要があります。このフォーマットでは、Directory Services Markup Language (DSML バージョン 1) によって定義された標準スキーマを使用します。DSMLv1 については、DSML の Web サイト (http://www.oasis-open.org) を参照してください。非同期通知の送信時には、Directory Access Markup Language (DAML バージョン 1) によって定義される XML メッセージ・フォーマットが使用されます。DAML は、IBM によって定義された XML 仕様であり、追加、変更、および削除の操作仕様を可能にします。

DSML ファイル形式

DSML は、ディレクトリー情報を記述する XML フォーマットです。*DSML* ファイルでは、ディレクトリー構造の情報を XML ファイル・フォーマットで表します。DSML ファイルは、IBM Security Identity Manager プロファイルの有効な属性のみを含む必要があります。 ID フィード・プロセスは、そのファイルに記述されているすべてのオブジェクトを使用します。

erPersonPassword 属性は、ID フィードの個人の変更プロセスでは使用されず、個人の作成プロセスでのみ使用されます。erPersonPassword 属性の値が設定されている場合は、個人とアカウントの作成時に、IBM Security Identity Manager アカウントのパスワードがその値に設定されます。 erPersonPassword 属性の値を設定するステートメントを以下に示します。

```
<attr name="erpersonpassword"><value>panther2</value></attr>
```

ID フィードで DSML ファイル・フォーマットを使用する場合は、以下のような DSML ファイルを指定してください。

```
<entry dn="uid=sparker">
<objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
<attr name="givenname"><value>Scott</value></attr>
<attr name="initials"><value>SVP</value></attr>
<attr name="sn"><value>Parker</value></attr>
<attr name="cn"><value>Scott Parker</value></attr>
<attr name="telephonenumber"><value>(919) 321-4666</value></attr>
<attr name="postaladdress"><value>222 E. First Street Durham, NC  27788</value></attr>
</entry>
```

ID フィード・ファイルの UTF-8 エンコード

ID フィード・ファイルは、UTF-8 形式でなければなりません。そのため、UTF-8 エンコードをサポートするエディターを使用する必要があります。

- Windows

  Microsoft Word 97 かそれ以降、または Windows 2003 Server または Windows XP オペレーティング・システムに含まれているメモ帳エディターは、UTF-8 に対応しています。

  メモ帳を使用してファイルを UTF-8 形式で保存するには、「**ファイル**」 > 「**名前を付けて保存**」をクリックします。「**文字コード**」フィールドの選択項目のリストを展開し、「UTF-8」を選択します。

- Linux

  Vim テキスト・エディター (標準的な vi エディターのバージョンの一つ) は、UTF-8 に対応しています。vim テキスト・エディターを使用して UTF-8 形式のファイルを扱うには、以下の指定を行います。

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  ご使用になっている UNIX のバージョンにこのテキスト・エディターがない場合、次の Web サイト (英語) にアクセスしてみてください。

  http://www.vim.org

注: 7 ビット ASCII コード・サブセットについては、UTF-8 エンコードの Unicode 形式は、7 ビット ASCII 形式と同一です。したがって、7 ビット ASCII を含む入力ファイル (16 進 20 から 16 進 7e の間の ASCII 文字値) に関しては、ファイル作成に通常のテキスト・エディターを使用することができます。他の文字値を含むファイル (ヨーロッパの拡張文字を含む) については、UTF-8 形式でファイルを保存する必要があります。

UTF-8 がサポートする 7 ビット ASCII 文字の正確なリストを得るには、次の Web サイト (英語) にアクセスして、最初の欄にある「**Basic Latin**」というリンクをクリックします。

http://www.unicode.org/charts

DSML ID フィード内の JavaScript コード

人的資源データベースは、変更内容の検出時に、先行して IBM Security Identity Manager サーバーに変更を提供することも可能です。

IBM Security Identity Managerサーバーは、Java Naming and Directory Interface (JNDI) サービス・プロバイダーに付属しています。このプロバイダーは、サーバーに変更内容を送信するためのプログラミング・インターフェースとして使用できます。これらの変更内容は、変更内容のイベント通知としてサーバーに受信されます。このフィーチャーは、イベント通知と呼ばれます。 HR データをインポートするためにイベント通知プログラムを使用するときには、追加、変更、および削除操作を使用できます。

DAML の JNDI サービス・プロバイダーの使用

DAML 用 JNDI サービス・プロバイダーを使用する前に、JNDI インターフェース仕様と LDAP の両方を理解する必要があります。 JNDI サービス・プロバイダーは両方の概念を使用します。このセクションでは、JNDI インターフェースと LDAP の理解に必要な情報へのリンクを示します。

JNDI Java プログラムからディレクトリー・タイプの情報にアクセスするための Java Naming and Directory Interface です。 JNDI のチュートリアルについては、Sun Microsystem の Web サイト (http://java.sun.com/products/jndi/tutorial/)を参照してください。

LDAP Lightweight Directory Access Protocol です。このプロトコルについての情報は、例えば http://www.openldap.org の OpenLDAP Foundation など、多くのソースから入手できます。

JNDI および DAML/DSML を使用するために必要な Java ライブラリーは、IBM Security Identity Manager サーバー・ディレクトリーの `lib` ディレクトリー内に入っています。

HR データのイベント通知

HR データは別のプログラムから IBM Security Identity Manager サーバーに DAML/HTTPS メッセージとして送信できます。

DAML/HTTPS メッセージは、IBM Security Identity Manager サーバーに HTTPS Post 要求として送信されます。DAML/HTTPS の Java Naming and Directory Interface JNDI サービス・プロバイダーは、この目的のために提供されています。

コンテキストの初期化

DAML 用 JNDI SP を使用する操作では、必ず、最初のステップとしてコンテキストを初期化します。コンテキストは、IBM Security Identity Manager Server と通信するために必要なすべてのプロトコル・プロパティーを使用して初期化する必要があります。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

以下のパッケージをインポート済みであることを確認してください。

- `import javax.naming.*;`
- `import javax.naming.directory.*;`
- `import java.util.*;`

このタスクについて

コンテキストを初期化するには、次の環境変数を変更してください:

```
Hashtable env = new Hashtable();
env.put (Context.INITIAL_CONTEXT_FACTORY,
"com.ibm.daml.jndi.DAMLContextFactory");
env.put(Context.SECURITY_PRINCIPAL,serviceUserName);
env.put(Context.SECURITY_CREDENTIALS, servicePassword);
env.put("com.ibm.daml.jndi.DAMLContext.CA_CERT_DIR", certDirLocation);
env.put(Context.PROVIDER_URL,providerURL);
env.put("com.ibm.daml.jndi.DAMLContext.URL_TARGET_DN", serviceDN);

DirContext damlContext = new InitialDirContext (env);
```

タスクの結果

コンテキストを初期化するときに、バインド要求が Security Identity Manager Server に送信されます。 環境変数が正しくない場合は、NamingException がスローされます。

次のタスク

初期化後は、以下のタスクを実行できます。

- 個人項目の追加
- 個人項目の変更
- 個人項目の除去

個人項目の追加

個人の追加のための属性は、ファイル調整メソッドに使用される属性と同じです。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

コンテキストを初期化済みであることを確認してください。

このタスクについて

個人の追加のための属性は、ファイル調整メソッドに使用される属性と同じです。新規の個人項目の DN は、少なくとも、個人を識別するために使用される固有属性 (UID など) を 1 つ含む必要があります。DSML ID フィード・サービスに定義された JavaScript 配置ルールは、その個人項目の追加先である組織単位を判別するために使用されます。組織情報が提供されないと、個人は組織のルートに追加されます。(DN は、以下の例にある createSubcontext / destroySubcontext / modifyAttributes メソッドを使用して指定されます。)

objectclass 属性を定義する必要があり、この属性は、追加する個人タイプにマップされた LDAP オブジェクト・クラスと一致する必要があります。このクラスは通常は inetOrgPerson です。その他のオブジェクト・クラスは IBM Security Identity Manager Server のエンティティー構成フィーチャーを使用して定義することにより使用できます。必要なオブジェクト・クラスを新規エンティティーとして、"Entity Type" = "Person" を使用して追加します。

個人を追加するには、以下の手順を実行します。

手順

1. 追加する個人の DN を定義します。
2. 新規ユーザーの属性オブジェクトのリストを格納する属性オブジェクトを作成します。
3. コンテキストの createSubContext を呼び出します。

タスクの結果

個人の DN および属性を作成した後で、createSubcontext に対する呼び出しが JNDI コンテキストを使用して行われます。

例

```
BasicAttributes ba = new BasicAttributes(true);
ba.put(new BasicAttribute("objectclass","inetorgperson"));
ba.put(new BasicAttribute("uid", uid));
ba.put(new BasicAttribute("cn", "JoeSmith"));
ba.put(new BasicAttribute("mail", uid + "@acme.com"));

damlContext.createSubcontext("uid="+ uid, ba);
```

次のタスク

以下のタスクを実行できます。

- 別の個人項目の追加
- 個人項目の情報の変更
- 個人項目の除去

個人項目の変更

個人エンティティーを変更するには、変更項目のリストを作成してから、コンテキストの modifyAttributes を呼び出す必要があります。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

コンテキストを初期化済みであることを確認してください。

このタスクについて

個人の属性値を変更する (新規属性の追加や既存属性の削除を含む) には、以下の手順を実行します。

手順

1. 変更する個人の DN を定義します。
2. 必要な変更内容を含んでいる ModificationItems のリストを作成します。
3. コンテキストの modifyAttributes を呼び出します。

タスクの結果

個人の DN を定義した後で、modifyAttributes に対する呼び出しが JNDI コンテキストを使用して行われます。

例

```
Vector mods = new Vector();
// 新規属性の追加 (属性が既に存在する場合は値の追加)
mods.add(new ModificationItem(DirContext.ADD_ATTRIBUTE, new BasicAttribute("roomnumber", "102")));
```

```
// 既存の属性の変更
mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, new BasicAttribute("title","Consultant")));
// 既存の属性を多値の値属性へ変更
newOuAt = new BasicAttribute("ou");
newOuAt.add("Research Department");
newOuAt.add("DevelopmentDivision");
mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, newOuAt));
// 既存の属性を 1 つ削除
mods.add(new ModificationItem(DirContext.REMOVE_ATTRIBUTE,new BasicAttribute("initials", null)));
String dn = "uid=" + uid;
damlContext.modifyAttributes(dn,(ModificationItem[])mods.toArray(new ModificationItem[mods.size()]));
```

次のタスク

以下のタスクを実行できます。

- 個人項目の追加
- 個人項目の除去

個人項目の除去

個人を除去するには、個人の DN を定義してから、コンテキストの destroySubContext を呼び出します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

コンテキストを初期化済みであることを確認してください。

このタスクについて

個人項目を除去するには、以下の手順を実行します。

手順

1. 除去する個人の DN を定義します。
2. コンテキストの destroySubContext を呼び出します。

タスクの結果

個人の DN を定義した後で、destroySubContext に対する呼び出しが JNDI コンテキストを使用して行われます。

例

```
damlContext.destroySubcontext("uid=" + uid);
```

次のタスク

以下のタスクを実行できます。

- 個人項目の追加
- 個人項目の情報の変更

HR データのイベント通知のサンプル・ドライバー

この Java テスト・プログラムおよびサンプル・コンパイラーは、100 人の個人を IBM 組織に追加します。

目的

このプログラムでは、短縮名が ibm であるテナントが存在しており、このテナントが IBM Security Identity Manager という名前の組織を含んでいると仮定しています。 この組織には、以下の属性をもつ DSML ID フィード・サービスがあります。

- サービス名 - dsmltest
- UID - dsml
- パスワード - dsml

このすべての情報が、以下のサンプル・プログラムの serviceDN 行、 serviceUID 行、および servicePassword 行で指定されています。

IBM Security Identity Manager Server のロケーションは、providerURL 行で指定されています。

サンプル・プログラム

このサンプル・プログラムは、クライアント証明書を使用しません (これは 2 方向 SSL 認証を使用していません)。IBM Security Identity Manager Server にインストールされたサーバー証明書の CA 証明書のコピーが、ディレクトリー ¥certificates (cerDirLocation 行) に存在する必要があります。

```
// TestDSML.java
import java.io.*;
import java.util.*;
import javax.naming.*;
import javax.naming.directory.*;

public class TestDSML {
  // Service DN は 4 つの部分で構成されています。
  // "erservicename=dsmltest" は、サービスの名前を指定します。
  // "ou=itim" は組織です。
  // "ou=ibm" はテナントです。
  // "dc=com" は、IBM Security Identity Manager の LDAP ツリーのベースです。
 static final String DEFAULT_SERVICEDN  =
     "erservicename=dsmltest, ou=itim, ou=ibm, dc=com";
 static final String DEFAULT_HOST  =
     "localhost:4443";

public static void main(String arg[]) {
  // 処理する個人の数
  int noOfPeople = Integer.getInteger("count", 100).intValue();
  // 必要な操作 ("add", "del", "mod")
  String op = System.getProperty("op", "add").toLowerCase();

  String certDirLocation = "¥¥certificates";    // CA 証明書を受領する場所
  // 使用する URL。
  // "/enrole/unsolicited_notification" を使用して非送信請求通知サーブレットを指定します。
  // これは、DSML 要求に使用されるサーブレットです。
  String host = System.getProperty("host", DEFAULT_HOST);
  String providerURL = "https:// " + host + "/enrole/unsolicited_notification";
  // ターゲット DN
  String serviceDN = System.getProperty("servicedn", DEFAULT_SERVICEDN);

  String serviceUID = "dsml";      // サービスに対して定義したユーザー ID
  String servicePassword = "dsml";   // サービスに対して定義したパスワード

  // 環境テーブルの生成および書き込み
  Hashtable env = new Hashtable();
  env.put (Context.INITIAL_CONTEXT_FACTORY,
    "com.ibm.daml.jndi.DAMLContextFactory");
  env.put(Context.SECURITY_PRINCIPAL, serviceUID);
  env.put(Context.SECURITY_CREDENTIALS, servicePassword);
  env.put("com.ibm.daml.jndi.DAMLContext.CA_CERT_DIR", certDirLocation);
  env.put(Context.PROVIDER_URL, providerURL);
```

```
  env.put("com.ibm.daml.jndi.DAMLContext.URL_TARGET_DN", serviceDN);

  DirContext damlContext = null;
  try {
    // 接続要求の生成
    damlContext = new InitialDirContext (env);
  }
  catch (NamingException e) {
    System.out.println("Error connecting to server at ¥"" + providerURL + "¥": " + e.getMessage());
    return;
  }
  for (int i = 1; i&lt;=noOfPeople; i++) {
    String sn = "smith" + i;
    String uid = "jsmith" + i;
    String dn = "uid=" + uid;

    try {
     if (op.startsWith("add")) {
      BasicAttributes ba = new BasicAttributes(true);
      ba.put(new BasicAttribute("objectclass","inetorgperson"));
      ba.put(new BasicAttribute("uid", uid));
      ba.put(new BasicAttribute("cn", "Joe Smith"));
      ba.put(new BasicAttribute("mail", uid + "@acme.com"));
      ba.put(new BasicAttribute("sn"));


     damlContext.createSubcontext(dn, ba);
    }
    else if (op.startsWith("del")) {
     damlContext.destroySubcontext(dn);
    }
    else if (op.startsWith("mod")) {
     Vector mods = new Vector();
     // 新規属性の追加 (属性が既に存在する場合は値の追加)
     mods.add(new ModificationItem(DirContext.ADD_ATTRIBUTE, new BasicAttribute("roomnumber", "102")));
     // 既存の属性の変更
     mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, new BasicAttribute("title", "Consultant")));
     // 既存の属性を多値の値に変更
    Attribute newOuAt = new BasicAttribute("ou");
    newOuAt.add("Research Department");
    newOuAt.add("Development Division");
    mods.add(new ModificationItem(DirContext.REPLACE_ATTRIBUTE, newOuAt));
    // 既存の属性を 1 つ削除
    mods.add(new ModificationItem(DirContext.REMOVE_ATTRIBUTE, new BasicAttribute("initials", null)));

    damlContext.modifyAttributes(dn, (ModificationItem[])mods.toArray(new ModificationItem[mods.size()]));
    }
   }
   catch (Exception e)  {
     System.out.println("Error, DN ¥"" + dn + "¥": " + e.getMessage());
     e.printStackTrace();
     }
   }
 }
}
```

サンプル・コンパイラー

先のテスト・プログラムをコンパイルするためのサンプルの Windows XP スクリプトは、以下のとおりです。

```
@rem compileDsmlTest.cmd - DSML テスト・プログラムのコンパイル
setlocal
rem 次のソースからの JAR ファイルを含んでいる lib ディレクトリーのロケーション
rem IBM Security Identity Manager installation lib directory, as listed below
set LIB=C:¥ITIM¥lib
set APP=TestDSML

rem Library files from IBM Security Identity Manager lib directory -
set AGENTLIB=%LIB%¥enroleagent.jar
set CLASSPATH=.;%AGENTLIB%;%LIB%¥jlog.jar

javac -classpath %CLASSPATH% -d . %APP%.java
endlocal
```

調整を使用した HR データのインポート

DSML ID フィード・サービス・プロバイダーを使用して、DSML で記述されたファイルから IBM Security Identity Manager Server に HR データをインポートできます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

クラスター環境では、すべてのクラスター・メンバー・マシンで同じ場所に DSML ファイルが存在します。調整の実行時に、どのクラスター・メンバーが調整を開始したかにかかわらずDSML ファイルを検出できます。

単一サーバー・セットアップでは、Security Identity Manager Server・マシンに DSML ファイルが存在する必要があります。

このタスクについて

DSML ID フィード・サービスを使用して DSML ファイルから HR データをインポートするときは、個人の追加と変更の操作のみが実行されます。個人の削除の操作は、DSML ファイルから識別レコード情報をインポートしているときにはできません。

注: DSML ファイルから識別レコード情報を処理するときは、調整されたデータ・セットが Security Identity Manager Server の個人集団全体を示さないことを前提とします。この前提事項により、ポーリング・メソッドは個人の追加または変更に使用できますが、削除には使用できません。個人を削除するには、イベント通知インターフェースを使用する必要があります。

DSML ID フィード・サービス・タイプを使用して HR データをインポートするには、以下の手順を実行します。

手順

1. DSML ID フィード・サービスのインスタンスを作成します。
2. 識別レコード・データが入っている DSML ファイルを参照するために、サービスを構成します。 DSML ファイルの絶対パス名を指定します。サービス・テスト・フィーチャーを使用して、ファイル名が正しいかどうかを調べます。
3. サービスを調整します。

タスクの結果

DSML ID フィード・サービスの調整時には、識別レコード項目は DSML ファイルから読み取られます。識別レコード項目ごとに、オブジェクト・クラスが IBM Security Identity Manager 内の適切な個人プロファイルが見つかるまでマッチングされます。一致が見つかると、識別名 (DN) が検索フィルターに変換されます。検索フィルターは、サービスが入っている組織に存在している個人の項目に対して既存する一致を探します。単一の一致が見つかると、個人の項目は既存の項目に対する

更新として使用されます。一致が見つからないと、個人は新規の個人項目として追加されます。重複する一致はエラーを戻し、項目は追加されません。

例

以下のステートメントは、個人の DSML エントリーのサンプルです。

```
<entry dn="uid=jsmith">
   <objectclass>
          <oc-value>inetOrgPerson</oc-value>
   </objectclass>
   <attr name="sn"><value>smith</value></attr>
   <attr name="uid"><value>jsmith</value></attr>
   <attr name="mail"><value>jsmith@IBM.com</value></attr>
   <attr name="givenname"><value>John</value></attr>
   <attr name="cn"><value>John Smith</value></attr>
</entry>
```

次のタスク

IBM Security Identity Manager インターフェースを使用して識別情報を追加、変更、および削除できるようになりました。

さらなるユーザーの追加、DSML ファイルを使用した既存ユーザーの変更、およびユーザーの削除を実行できます。

DSML ID フィード・サービス・フォーム

DSML ID フィード・サービス・フォームのフィールドを使用して、Directory Services Markup Language (DSML) の ID フィードに関する情報を指定します。 例えば、サービス・プロファイルを選択して、DSML で識別データをインポートできます。フォームのフィールドに必要な値を入力して、そのサービスが常駐するサーバーに接続します。

以下のフィールドが、DSML ID フィード・サービス・フォームで使用できます。

サービス名
サービス・インスタンスの識別に使用する名前を指定します。

説明 サービス・インスタンスに関する追加情報を指定します。

ユーザー ID
サービス・インスタンスの管理ユーザー ID を指定します。

パスワード
サービス・インスタンスの管理パスワードを指定します。パスワード認証が使用されている場合は、値を入力してください。使用されていない場合は、後で調整が失敗します。

ファイル名
ユーザー情報を格納するファイルのパス名を含むファイル名を指定します。

注: クラスター環境では、ファイルをすべてのクラスター・メンバー上の同じロケーションに格納する必要があります。

ワークフローを使用
このサービス・インスタンスでワークフローを使用し、項目のアカウントを自動的に作成するかどうかを決定する場合は、このチェック・ボックスを選

択します。この機能は、小規模な増分フィードの場合に使用できます。大量のデータをインポートするためには、使用できません。

配置ルール

ユーザー (個人) を組織ツリーに配置する場合に使用するルールを指定します。このルールはスクリプトで定義されます。スクリプトのコンテキストは、フィード内の現行ユーザーと、フィード自体を定義するサービスの識別情報です。

調整用 DSML ファイルのサンプル

この例をモデルとして使用して、調整を使用した HR データのインポートに使用する DSML ファイルを作成します。

サンプル

以下の DSML ファイルは、調整に使用する XML の完全なサンプルです。

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

   <directory-entries>

   <entry dn="uid=janesmith">
      <objectclass>
         <oc-value>inetOrgPerson</oc-value>
      </objectclass>
      <attr name="ou"><value>Engineering</value></attr>
      <attr name="sn"><value>Smith </value></attr>
      <attr name="uid"><value>janesmith</value></attr>
      <attr name="mail"><value>j.smith@ibm.com</value></attr>
      <attr name="givenname"><value>Jane</value></attr>
      <attr name="cn"><value>Jane Smith</value></attr>
      <attr name="initials"><value>JS</value></attr>
      <attr name="employeenumber"><value>E_1974</value></attr>
      <attr name="title"><value>Research and Development</value></attr>
      <attr name="telephonenumber"><value>(888) 555-1614</value></attr>
      <attr name="mobile"><value>(888) 555-8216</value></attr>
      <attr name="homepostaladdress"><value>15440 Laguna Canyon Rd, Irvine, CA 92614</value></attr>
      <attr name="roomnumber"><value>G-114</value></attr>
      <attr name="homephone"><value>(888) 555-3222</value></attr>
      <attr name="pager"><value>(888) 555-7756</value></attr>
      <attr name="erAliases">
         <value>j.smith</value>
         <value>jane_smith</value>
         <value>JaneSmith</value>
      </attr>
      <attr name="erRoles">
         <value>Engineering</value>
         <value>Development</value>
      </attr>
   </entry>
   <entry dn="uid=johndoe">
      <objectclass>
         <oc-value>inetOrgPerson</oc-value>
      </objectclass>
      <attr name="ou"><value>Sales-West</value></attr>
      <attr name="sn"><value>Doe</value></attr>
      <attr name="uid"><value>johndoe</value></attr>
      <attr name="mail"><value>j.doe@ibm.com</value></attr>
      <attr name="givenname"><value>John</value></attr>
      <attr name="cn"><value>JohnDoe</value></attr>
      <attr name="initials"><value>JD</value></attr>
      <attr name="employeenumber"><value>S_1308</value></attr>
      <attr name="title"><value>Sales Engineer</value></attr>
      <attr name="telephonenumber"><value>(888) 555-1620</value></attr>
      <attr name="mobile"><value>(888) 555-8210</value></attr>
      <attr name="homepostaladdress"><value>15440 Laguna Canyon Rd, Irvine, CA 92614</value></attr>
      <attr name="roomnumber"><value>G-120</value></attr>
      <attr name="homephone"><value>(888) 555-3228</value></attr>
      <attr name="pager"><value>(888) 555-7750</value></attr>
      <attr name="erAliases">
         <value>j.doe</value>
```

```
         <value>john_doe</value>
         <value>JohnDoe</value>
      </attr>
      <attr name="erRoles">
         <value>Sales</value>
      </attr>
   </entry>

</directory-entries>

</dsml>copy from here to there
```

AD Organizational ID フィード

AD Organizational ID フィードは、Windows Server Active Directory (AD) からのユーザー・レコードを基にユーザーを作成する機能を提供します。

このフィードでは、フィードのソースとしてディレクトリー・リソースを使用します。 AD `organizationalPerson` オブジェクト・クラスからの情報は、`inetOrgPerson` スキーマにマップされます。この ID フィードでは、指定されたベースの下にあるすべてのユーザー・オブジェクトを読み込みます。

AD Organizational サービス・タイプ

この ID フィード用のサービス・インスタンスを作成するときは、以下の情報が必要です。

- ディレクトリー・リソースへの接続に使用する URL
- リソースにアクセスするためのユーザー ID およびパスワード
- LDAP 用語の検索ベースであり、ディレクトリー・ツリー内での検索開始場所を定義する命名コンテキスト
- 名前属性 (提供された値から選択する必要があります)

このサービスは、作成後に、ディレクトリーの特定のブランチを調整するために設定されます。

属性マッピングのカスタマイズ

「**属性マッピング・ファイル名**」オプションを使用すると、LDAP 属性の IBM Security Identity Manager 属性へのマッピングをカスタマイズできます。

属性マッピング・ファイルのフォーマットは `feedAttrName=itimAttrName` です。番号記号 (`#`) またはセミコロン (`;`) で始まる行は、コメント行と解釈されます。

属性マッピング・ファイルによって、デフォルトのマッピングが完全にオーバーライドされます。フィード・ソースで必要なすべての属性をマッピング・ファイルに含める必要があります。

以下の属性がマッピング・ファイルに含まれていなければなりません。

- 個人のプロファイル・フォームにおいて必須であると指定されている属性
- ターゲットの個人のプロファイルに対する LDAP スキーマにおいて必須であると指定されている属性

フィード・ソースからの属性が属性マッピング・ファイルに含まれていない場合は、値が IBM Security Identity Manager 属性に設定されません。

次の例は、6 個の属性のマップを示しています。他の LDAP 属性はすべて無視されます。

```
#feedAttrName=itimAttrName
cn=cn
sn=sn
title=title
telephonenumber=mobile
mail=mail
description=description
```

ID フィード・ファイルの UTF-8 エンコード

ID フィード・ファイルは、UTF-8 形式でなければなりません。そのため、UTF-8 エンコードをサポートするエディターを使用する必要があります。

- Windows

  Microsoft Word 97 かそれ以降、または Windows 2003 Server または Windows XP オペレーティング・システムに含まれているメモ帳エディターは、UTF-8 に対応しています。

  メモ帳を使用してファイルを UTF-8 形式で保存するには、「**ファイル**」 > 「**名前を付けて保存**」をクリックします。「**文字コード**」フィールドの選択項目のリストを展開し、「UTF-8」を選択します。

- Linux

  Vim テキスト・エディター (標準的な vi エディターのバージョンの一つ) は、UTF-8 に対応しています。vim テキスト・エディターを使用して UTF-8 形式のファイルを扱うには、以下の指定を行います。

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  ご使用になっている UNIX のバージョンにこのテキスト・エディターがない場合、次の Web サイト (英語) にアクセスしてみてください。

  http://www.vim.org

注: 7 ビット ASCII コード・サブセットについては、UTF-8 エンコードの Unicode 形式は、7 ビット ASCII 形式と同一です。したがって、7 ビット ASCII を含む入力ファイル (16 進 20 から 16 進 7e の間の ASCII 文字値) に関しては、ファイル作成に通常のテキスト・エディターを使用することができます。他の文字値を含むファイル (ヨーロッパの拡張文字を含む) については、UTF-8 形式でファイルを保存する必要があります。

UTF-8 がサポートする 7 ビット ASCII 文字の正確なリストを得るには、次の Web サイト (英語) にアクセスして、最初の欄にある「**Basic Latin**」というリンクをクリックします。

http://www.unicode.org/charts

inetOrgPerson ID フィード

inetOrgPerson ID フィードは、RFC2798 を使用して LDAP ディレクトリー・サーバーをサポートします (inetOrgPerson LDAP オブジェクト・クラス)。

このフィードでは、フィードのソースとしてディレクトリー・リソースを使用します。この ID フィードでは、指定されたベースの下にあるすべての inetOrgPerson オブジェクトを読み込みます。objectclass=inetOrgPerson が指定されていないレコードは無視されます。

inetOrgPerson サービス・タイプ

この ID フィード用のサービス・インスタンスを作成するときは、以下の情報が必要です。

- ディレクトリー・リソースへの接続に使用する URL
- リソースにアクセスするためのユーザー ID およびパスワード
- LDAP 用語の検索ベースであり、ディレクトリー・ツリー内での検索開始場所を定義する命名コンテキスト
- 名前属性 (提供された値から選択する必要があります)

このサービスは、作成後に、ディレクトリーの特定のブランチを調整するために設定されます。

属性マッピングのカスタマイズ

「**属性マッピング・ファイル名**」オプションを使用すると、LDAP 属性の IBM Security Identity Manager 属性へのマッピングをカスタマイズできます。

属性マッピング・ファイルのフォーマットは feedAttrName=itimAttrName です。番号記号 (#) またはセミコロン (;) で始まる行は、コメント行と解釈されます。

属性マッピング・ファイルによって、デフォルトのマッピングが完全にオーバーライドされます。フィード・ソースで必要なすべての属性をマッピング・ファイルに含める必要があります。個人のプロファイル・フォーム、またはターゲットの個人プロファイルの LDAP スキーマで必須として指定された属性は、マッピング・ファイルに含める必要があります。フィード・ソースからの属性が属性マッピング・ファイルに含まれていない場合は、値が IBM Security Identity Manager 属性に設定されません。

次の例は、6 個の属性のマップを示しています。他の LDAP 属性はすべて無視されます。

```
#feedAttrName=itimAttrName
cn=cn
sn=sn
title=title
telephonenumber=mobile
mail=mail
description=description
```

ID フィード・ファイルの UTF-8 エンコード

ID フィード・ファイルは、UTF-8 形式でなければなりません。そのため、UTF-8 エンコードをサポートするエディターを使用する必要があります。

- Windows

  Microsoft Word 97 かそれ以降、または Windows 2003 Server または Windows XP オペレーティング・システムに含まれているメモ帳エディターは、UTF-8 に対応しています。

  メモ帳を使用してファイルを UTF-8 形式で保存するには、「**ファイル**」 > 「**名前を付けて保存**」をクリックします。「**文字コード**」フィールドの選択項目のリストを展開し、「UTF-8」を選択します。

- Linux

  Vim テキスト・エディター (標準的な vi エディターのバージョンの一つ) は、UTF-8 に対応しています。vim テキスト・エディターを使用して UTF-8 形式のファイルを扱うには、以下の指定を行います。

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  ご使用になっている UNIX のバージョンにこのテキスト・エディターがない場合、次の Web サイト (英語) にアクセスしてみてください。

  http://www.vim.org

注: 7 ビット ASCII コード・サブセットについては、UTF-8 エンコードの Unicode 形式は、7 ビット ASCII 形式と同一です。したがって、7 ビット ASCII を含む入力ファイル (16 進 20 から 16 進 7e の間の ASCII 文字値) に関しては、ファイル作成に通常のテキスト・エディターを使用することができます。他の文字値を含むファイル (ヨーロッパの拡張文字を含む) については、UTF-8 形式でファイルを保存する必要があります。

UTF-8 がサポートする 7 ビット ASCII 文字の正確なリストを得るには、次の Web サイト (英語) にアクセスして、最初の欄にある「**Basic Latin**」というリンクをクリックします。

http://www.unicode.org/charts

IBM Tivoli Directory Integrator (IDI) データ・フィード

IBM Tivoli Directory Integrator (IDI) ID フィードは、カスタム ID ソースからのデータ・フィードをサポートするために使用します。標準のデータ・フィードよりも柔軟性に優れています。

IDI データ・フィードは、例えば、他の HR フィードでは不十分である場合のために用意されています。IDI データ・フィールドを使用して、カスタム ID フィードを定義することができます。

このデータ・フィードを使用するには、IBM Tivoli Directory Integrator (IDI) の知識が必要です。

このデータ・フィードは、標準のデータ・フィードを超える柔軟性を提供するために使用されます。例えば、次のような柔軟性を持ちます。

- 指定された部門のユーザーの選別など、データのサブセットを処理する能力
- 標準フィードに備わっている 1 対 1 マッピングを超える追加の属性マッピング
- 他のデータ・ソースからスーパーバイザーまたはマネージャーを派生させるためなどのデータ検索
- データ・ソースの変更検出
- DB2、Oracle、PeopleSoft、および SAP などのデータベースおよび HR システム
- 状況の更新、個人のサスペンドなど、属性の制御
- 個人の削除
- IBM Security Identity Manager 調整によってではなく、IBM Tivoli Directory Integrator によって起動される変更 (削除、更新、および変更検出に使用)

ID フィード・ファイルの UTF-8 エンコード

ID フィード・ファイルは、UTF-8 形式でなければなりません。そのため、UTF-8 エンコードをサポートするエディターを使用する必要があります。

- Windows

  Microsoft Word 97 かそれ以降、または Windows 2003 Server または Windows XP オペレーティング・システムに含まれているメモ帳エディターは、UTF-8 に対応しています。

  メモ帳を使用してファイルを UTF-8 形式で保存するには、「**ファイル**」 > 「**名前を付けて保存**」をクリックします。「**文字コード**」フィールドの選択項目のリストを展開し、「UTF-8」を選択します。

- Linux

  Vim テキスト・エディター (標準的な vi エディターのバージョンの一つ) は、UTF-8 に対応しています。vim テキスト・エディターを使用して UTF-8 形式のファイルを扱うには、以下の指定を行います。

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  ご使用になっている UNIX のバージョンにこのテキスト・エディターがない場合、次の Web サイト (英語) にアクセスしてみてください。

  http://www.vim.org

注: 7 ビット ASCII コード・サブセットについては、UTF-8 エンコードの Unicode 形式は、7 ビット ASCII 形式と同一です。したがって、7 ビット ASCII を含む入力ファイル (16 進 20 から 16 進 7e の間の ASCII 文字値) に関しては、ファイル作成に通常のテキスト・エディターを使用することができます。他の文字値を含むファイル (ヨーロッパの拡張文字を含む) については、UTF-8 形式でファイルを保存する必要があります。

UTF-8 がサポートする 7 ビット ASCII 文字の正確なリストを得るには、次の Web サイト (英語) にアクセスして、最初の欄にある「**Basic Latin**」というリンクをクリックします。

http://www.unicode.org/charts

IBM Tivoli Directory Integrator による識別情報の管理

IBM Tivoli Directory Integrator を使用して、識別情報を IBM Security Identity Manager にインポートし、IBM Security Identity Manager データ・ストアにある外部リソース上のアカウントを管理できます。識別データのソースは、人的資源リポジトリーや、全社規模のディレクトリーなどの別の場所です。 HR データの ID レコードは、IBM Security Identity Manager の個人オブジェクトのインスタンスになります。IBM Tivoli Directory Integrator との統合には、IBM Security Identity Manager システムへのネットワーク接続とデータ・フィードを管理する新規サービス・タイプが必要です。

IBM Tivoli Directory Integrator を使用する利点が含まれます。

- カスタム・プログラミングで未加工の個人情報データを扱い、IBM Security Identity Manager にインポートできる形式に加工する必要がなくなります。IBM Tivoli Directory Integrator を使用することにより、コンマ区切りファイルやデータベースからのデータを構文解析し、その結果を、個人情報データとして、またはそのデータに対する変更として IBM Security Identity Managerに送ることができます。以前は、Directory Services Markup Language (DSML) ファイルまたはカスタム Java Naming and Directory Interface (JNDI) クライアントが必要でした。
- DSMLv2 サーバーとして動作する IBM Tivoli Directory Integrator に対して検索を実行することにより、IBM Security Identity Manager が DSMLv2 クライアントとして動作して、調整時に IBM Tivoli Directory Integrator から個人データを検索できる識別データを管理します。また、IBM Security Identity Manager も DSMLv2 サーバーとして動作し、DSMLv2 クライアント (例えば IBM Tivoli Directory Integrator など) からの要求を受け入れ、JNDI サービス・プロバイダーを使用できます。

  注: DSMLv2 は、IBM Security Identity Manager バージョン 5.0 では推奨されません。リモート・メソッド呼び出し (RMI) ベースの IDI アダプター・フレームワークを採用してください。DSMLv2 は、このリリースでも引き続きサポートされています。
- アカウント管理に利点があります。詳しくは、`extensions` ディレクトリーにある追加文書を参照してください。

また、IBM Tivoli Directory Integrator 製品に付属の追加文書も参照してください。スキーマのカスタマイズと ID データ・フィードでのデータのインポートの例については、*ITIM_HOME*`/extensions/examples` ディレクトリーにナビゲートしてください。

シナリオ: バルク・ロード識別データ

IBM Tivoli Directory Integrator を使用する代表的なシナリオとしては、識別データを IBM Security Identity Managerにバルク・ロードすることを検討しているアドミニストレーターが考えられます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

Tivoli Directory Integrator のインスタンスが実行されている必要があります。

このタスクについて

このシナリオは、以下のハイレベル・タスクを含みます。

手順

1. Tivoli Directory Integrator 構成をセットアップします。これには、DSMLv2 イベント・ハンドラーの構成および目的のデータ・ソースへのコネクターを使用するアセンブリー行の構成を含みます。
2. Tivoli Directory Integrator イベント・ハンドラーを開始します。
3. Tivoli Directory Integrator 構成と通信するよう IBM Security Identity Manager サービスをセットアップします。
4. 調整を実行して、通信を開始します。

タスクの結果

調整後に以下のイベントが生起します。

1. IBM Security Identity Manager は検索要求メッセージを Tivoli Directory Integrator に送信し、これがエンタープライズ・データ・ストアから識別データを検索します。
2. Tivoli Directory Integrator は、データを処理する IBM Security Identity Manager にデータを戻します。この処理には、個人を配置する組織ツリーでの位置の評価と役割メンバーシップの評価が含まれます。また、スーパーバイザー関連の評価、(場合によっては) プロビジョニング・ポリシーの評価、IBM Security Identity Manager データ・ストアへのデータの挿入が含まれます。プロビジョニング・ポリシーの評価は、アカウント管理アクションでの結果の場合があります。
3. 識別情報が、エンタープライズ・データ・ストアから IBM Security Identity Manager に読み込まれます。

次のタスク

IBM Security Identity Manager インターフェースを使用して識別情報を追加、変更、および削除できるようになりました。

Tivoli Directory Integrator を使用する追加のシナリオは、`extensions` ディレクトリーでこれらの説明を参照してください。

- JNDI を使用する識別フィード
- エンド・ユーザー・アカウント管理
- アカウント・イベント通知

グループ・メンバーシップを保持する ID フィード

ID フィードでカスタマイズ・グループとデフォルト・グループの両方のユーザー・メンバーシップが保持されていることを確認する必要があります。

初期状態では、IBM Security Identity Manager のすべてのデフォルト・グループにメンバーが含まれていません。ただし、アドミニストレーター・グループだけは例外で、このグループには `itim manager` というアカウント名のユーザーが 1 人含まれています。最初の ID レコードを IBM Security Identity Manager にロードすると、一部の個人がマネージャー・グループのメンバーになることがあります。

表 54. 初期 ID フィード実行後のグループ・メンバーシップ

グループ名	メンバーシップ
管理者	アカウント (名前 `itim manager`) の 1 メンバー。
マネージャー	0 以上のメンバー。メンバーの数は、ユーザーに管理対象関係があることを示す ID レコードが初期 ID フィードにあるかどうかに基づきます。
サービス所有者	ゼロ
ヘルプ・デスク・アシスタント	ゼロ

最初のヘルプ・デスク・アシスタントと最初のサービス所有者は、アドミニストレーターが明示的にグループに追加するユーザーです。あるいは、ユーザーをサービス所有者として指定すると、そのユーザーに対しサービス所有者グループのメンバーシップが自動的に設定されます。ユーザーを別のユーザーのマネージャーとして指定すると、そのユーザーに対しマネージャー・グループのメンバーシップが自動的に設定されます。

カスタマイズ・グループのメンバーになっているユーザーは、同じカテゴリーのデフォルト・グループのメンバーでもある必要があります。そうでない場合、処理の結果は予測できません。

受信するユーザーの ID レコードで最初にカスタマイズ・グループのメンバーであることが示されている場合、IBM Security Identity Manager はこのユーザーを、カスタマイズ・グループと、同じカテゴリーのデフォルト・グループの両方のメンバーとして組み込みます。IBM Security Identity Manager は、同一ユーザーが含まれている後続の ID フィードを、既存の IBM Security Identity Manager ユーザーの変更として解釈します。後続の ID フィードで、ユーザーがカスタマイズ・グループのみのメンバーであり、同一カテゴリーのデフォルト・グループのメンバーではないと指定されている場合は、このユーザーはデフォルト・グループのメンバーシップから除去されます。この問題を防止するため、初回 ID フィードと後続の ID フィードの両方で、ユーザーがカスタマイズ・グループと、同一カテゴリーのデフォルト・グループの両方のメンバーであることが指定されるようにしてください。

inetOrgPerson 属性の Windows Server Active Directory 属性へのマップ

IBM Security Identity Manager の inetOrgPerson 属性は、Windows Server Active Directory 属性にマップします。相違点は**太字**で示します。

表 55. inetOrgPerson 属性と Windows Server Active Directory の organizationalPerson 属性のマップ

IBM Security Identity Manager の inetOrgPerson 属性	Windows Server Active Directory の organizationalPerson 属性
cn	cn
departmentNumber	**department**
description	**comment**
employeeNumber	**employeeID**
givenName	givenName
homePhone	homePhone
homePostalAddress	homePostalAddress
initials	initials
internationaliSDNNumber	internationallSDNNumber
jpegPhoto	**thumbnailPhoto**
l	l
mail	mail
manager	manager
mobile	mobile
o	o
ou	ou
pager	pager
physicalDeliveryOfficeName	physicalDeliveryOfficeName
postalAddress	postalAddress
postalCode	postalCode
postOfficeBox	postOfficeBox
preferredDeliveryMethod	preferredDeliveryMethod
registeredAddress	registeredAddress
secretary	**assistant**
seeAlso	seeAlso
sn	sn
st	st
street	**streetaddress**
telephoneNumber	telephoneNumber
teletexTerminalIdentifier	teletexTerminalIdentifier
telexNumber	telexNumber
title	title
uid	**< - ブランク - >**

表 55. inetOrgPerson 属性と Windows Server Active Directory の organizationalPerson 属性のマップ (続き)

IBM Security Identity Manager の inetOrgPerson 属性	Windows Server Active Directory の organizationalPerson 属性
userPassword	userPassword **注:** ディレクトリー・サーバーによる暗号化のため、IBM Security Identity Manager はこの属性の値を使用できません。
x121Address	x121Address

ID フィードで提供されるユーザー・パスワード

inetOrgPerson スキーマの userPassword 属性はディレクトリー・サーバーによって暗号化されていて、IBM Security Identity Manager から使用できないため、LDAP からの inetOrgPerson ID フィードまたは Windows Server Active Directory ID フィードではユーザー・パスワード・データは提供されません。

CSV、DSML または IBM Tivoli Directory Integrator ベースの形式を使用するその他の ID フィードは、新規ユーザー用のパスワードを提供できます。ID フィード値が与えられると、IBM Security Identity Manager は、erPersonPassword 属性を使用して、新規ユーザーの IBM Security Identity Manager アカウント用にパスワードを作成します。erPersonPassword 属性は、IBM Security Identity Manager の新規ユーザー用にパスワードを作成する目的にのみ使用されます。ユーザーが存在している場合は、erPersonPassword 属性の値を使用して IBM Security Identity Manager ユーザーのログイン・パスワードを変更することはできません。

erPersonPassword が指定されていない ID フィードでは、IBM Security Identity Managerが新規ユーザー用の新規パスワードを生成します。アプリケーションは、生成されたパスワードを電子メールで新規ユーザーに送信します。ユーザーの電子メール・アドレスに記載されていない場合、そのユーザーはヘルプ・デスクに連絡してパスワードを入手する必要があります。ご使用のサイトの要件によっては、新規ユーザーのパスワードがユーザーの上司にも送信される場合があります。

IBM Tivoli Directory Integrator が提供するパスワード値は、Base 64 形式でエンコードされる必要があります。

以下の ID フィード属性は、新規ユーザー用のパスワード値を平文で提供します。

- CSV カラム名: erPersonPassword
- DSML タグ: erPersonPassword

スキーマに存在しない ID フィードの属性

ID フィードのオブジェクト・クラス (Windows Server Active Directory の場合は organizationalPerson、IBM Security Identity Managerの場合は inetOrgPerson) に含まれていない一部の属性を ID フィードに組み込むことができます。

例えば、erRoles 属性によって、IBM Security Identity Manager グループでのユーザーのメンバーシップが決定されます。この erRoles 属性は、

organizationalPerson スキーマにも inetOrgPerson スキーマにも含まれていません。初期 ID フィードの erRoles 属性の値に基づいて、ユーザーはカスタマイズ・グループのメンバーになることがあります。ユーザーはまた、デフォルトのヘルプ・デスク・アシスタント・グループのメンバーになることもあります。

反復 ID フィードには、organizationalPerson および inetOrgPerson の両スキーマの場合に、以前にそのユーザーについて指定した属性の値が含まれていないことがあります。 ID フィード・プロセスでは、IBM Security Identity Managerユーザーのためにその属性を削除します。

受信するユーザーの ID レコードで最初にカスタマイズ・グループのメンバーであることが示されている場合、IBM Security Identity Manager はこのユーザーを、カスタマイズ・グループと、同じカテゴリーのデフォルト・グループの両方のメンバーとして組み込みます。IBM Security Identity Manager は、同一ユーザーが含まれている後続の ID フィードを、既存の IBM Security Identity Manager ユーザーの変更として解釈します。後続の ID フィードで、ユーザーがカスタマイズ・グループのみのメンバーであり、同一カテゴリーのデフォルト・グループのメンバーではないと指定されている場合は、このユーザーはデフォルト・グループのメンバーシップから除去されます。この問題を防止するため、初回 ID フィードと後続の ID フィードの両方で、ユーザーがカスタマイズ・グループと、同一カテゴリーのデフォルト・グループの両方のメンバーであることが指定されるようにしてください。

Windows Server Active Directory フィードの場合は、organizationalPerson スキーマに含まれていない各 inetOrgPerson 属性についてもこの問題が発生します。inetOrgPerson の ID フィードの場合は、ID フィードでサポートされていないすべての inetOrgPerson 属性についてこの問題が発生します。

属性のサポート形式と特殊処理

IBM Security Identity Manager では、manager 属性、secretary 属性、erRoles 属性の特殊処理を実行できます。

manager 属性と secretary 属性のサポート形式と特殊処理

manager 属性と secretary 属性は、IBM Security Identity Manager 内の他の個人項目を参照します。

注: Windows Server Active Directory の ID フィードは、Windows Server Active Directory の assistant 属性を secretary 属性に対応付けます。

IBM Security Identity Managerの内部では、個人ディレクトリー項目の識別名 (DN) として特殊なフォーマットを使用します。このフォーマットは使いにくく、ID フィード・データで指定するのが困難です。そのため、ID フィード・コードでは、それらの属性をもっと使いやすいフォーマットで指定できるようにしています。IBM Security Identity Manager では、値を指定するために以下の 3 つの形式をサポートしています。

- 検索フィルター (等号 (= 演算子を含んでいますが、erglobalid は含んでいません)。attribute=value ペアのコンマ区切りリストです。
- 単純名 (等号 (=) 演算子は含んでいません)。個人オブジェクト・クラスの名前属性 (つまり、cn) の値になります。

- 完全 IBM Security Identity ManagerDN (等号 (=) 演算子と erglobalid を含んでいます)。式は、現在定義されているいずれかの個人オブジェクトの IBM Security Identity ManagerLDAP DN と完全に一致する必要があります。

最初の 2 つの場合、IBM Security Identity Managerは値を LDAP 検索フィルターに変換します。このプロセスでは、組織のサブツリー検索を実行して一致する固有の個人を検出します。この検索で一致する項目がゼロまたは複数の場合、その値は無効と見なされ、リストから除去されます。適切な警告メッセージが IBM Security Identity Manager ログに書き込まれます。

manager 属性の場合も secretary 属性の場合も、参照先の個人が同じフィードで定義されている場合は、問題が発生する可能性があります。その場合は、属性の値が上記の方法で処理される時点で、参照先の個人がまだ作成されていない、という状況が起こり得ます。この問題は、manager または secretary の個人が ID フィード・ファイルで先に定義されている場合でも発生することがあります。原因は、ID フィードの実行時に IBM Security Identity Managerによって実行されるマルチスレッドの非同期処理です。この状況では、属性が無効な個人を参照することになるため、その個人から属性が削除されます。ログには警告が書き込まれます。

参照の依存関係に由来するこの問題には、2 つの解決方法があります。1 つは、最初の実行によるすべての処理が完了した後に、2 回目の ID フィードを実行するという方法です。フィード中の主な処理は、変更のあった項目についてのみ実行されることになるため、この 2 回目のフィードの処理は大幅に速くなります。あるいは、manager と secretary の個人を別の ID フィード・ファイルに定義する、という方法もあります。その ID フィードを最初に実行して、そのフィードが完了してから、メインのフィードを実行します。この別に定義した最初のフィードには、同じフィードで定義されている manager を参照する項目が含まれている場合もあります。別に定義した最初のフィードを 2 回実行するか、フィードをもう一度分割することが必要になることもあります。

ID フィードの状況が完了になっているように見えても、個人を作成または変更する非同期ワークフロー・アクティビティーがまだ実行されている場合があります。その場合は、最初のフィードが完了したように見えてからさらに余分の時間が経過するのを待ち、それから 2 回目のフィードを実行する必要があります。

erRoles 属性値のサポート形式と特殊処理

erRoles 属性は、個人が属する役割リストを指定するために使用します。IBM Security Identity Manager のグループは、エンタープライズ製品である IBM Security Identity Manager に用意されている役割に相当します。IBM Security Identity Manager では、erRoles 属性を使用して、ユーザーの所属グループを指定します。例えば、値を Help Desk Assistant にして ID フィード属性 erRoles を指定すると、ユーザーはヘルプ・デスク・アシスタント・グループに所属することになります。erRoles 属性は複数の値を指定することができます。

サポートされている形式は以下のとおりです。

- 単純名 (等号 (=) 演算子は含んでいません)。erRoleName 属性の値になります。IBM Security Identity Manager は、サブツリー検索を実行して、一致する固有の静的役割を検出します。一致する役割がゼロまたは複数の場合は、名前が無効になります。

- 完全 IBM Security Identity Manager DN。現在定義されているいずれかの静的役割の IBM Security Identity Manager LDAP DN と完全に一致する必要があります。

無効な値は値リストから除去されます。その結果、残っている値の数がゼロになれば、その属性が属性リストから除去されます。適切な警告メッセージがログに書き込まれます。

変更可能なスキーマのクラスと属性

IBM Security Identity Manager スキーマの一部のクラスと属性は、変更が可能です。

以前は、IBM Security Identity Manager スキーマのクラスと属性用に予約されていた接頭部 `er` で始まる名前を使って新規クラスを作成できます。

変更可能な IBM Security Identity Manager スキーマのクラスと属性には、固有のオブジェクト ID (OID) 接頭部が付いています。OID は、LDAP スキーマで固有のクラスを識別する数値ストリングです。読み取り専用のままの IBM Security Identity Manager スキーマのクラスと属性には、以下の OID 接頭部が付いています。

`1.3.6.1.4.1.6054.1.1`

個人の命名および組織配置

IBM Security Identity Manager Serverサーバーは、HR データをインポートすると、ID レコードごとに識別名 (DN) を作成します。また、提供された情報に基づいて、特定の組織単位に個人を配置します。

各個人を一意的に識別して配置するには、IBM Security Identity Manager Serverが個別の部分 (属性) として 認識できる方法で、各項目 (または個人) がそれぞれのデータを編成する必要があります。渡された属性を認識するよう、IBM Security Identity Manager Server を構成する必要もあります。認識は、定義済みの個人プロファイルに対してオブジェクト・クラス属性を突き合わせることにより実行されます。デフォルトでは、LDAP 標準の `inetOrgPerson` オブジェクト・クラスが予期されます。

個人の配置の決定

IBM Security Identity Manager Serverは、組織図の中での位置を決定します。このサーバーは、DSML ID フィード・サービスで定義されている配置ルールを使用します。

個人は、識別ソースのマーケティング部門のメンバーとして定義されることがあります。サーバーは、配置ルールに従って、IBM Security Identity Manager組織図のマーケティング部門にその個人を配置します。このルールは、追加操作時に個人を初期配置する場合と、変更操作時に個人を別の場所に移動する場合に使用します。

注: 組織コンテナーの指定に組織パスを使用しない限り、配置ルールによって戻される組織名は、サービスのコンテキスト内で固有のものでなければなりません。組織パスが配置ルールによって提供される場合、組織名は組織コンテナー内で固有のものでなければなりません。

配置ルールは、JavaScript で作成され、識別名 (DN) フォーマットで組織パスを戻します。この情報を使用して、個人の配置先となる組織単位を検索します。この DN は、組織の基本に相対する必須組織パスを示します。このパスの構文は、以下の疑似 BNF 表記を使用して表示できます。

```
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= prefix '=' name
prefix ::= 'l' | 'o' | 'ou'
name ::= string
```

ここで、string は組織構造上の値です。l はロケーションです。o は組織です。ou は組織単位、ビジネス・パートナー組織、または管理ドメインです。

注: ここに記載された接頭部はデフォルト値です。カスタマーが異なるスキーマを使用している場合は、これらの接頭部はエンティティー構成にマップされた値です。

例

図示するには、以下の組織表を調べてください。

```
IBM (組織)
   Marketing (組織単位)
   Facilities (組織単位)
      Irvine (部署)
```

Marketing 部門のパスは、ou=Marketing, o=IBM です。Irvine Facilities 部門のパスは、l=Irvine, ou=Facilities, o=IBM です。

JavaScript 機能はこのフォーマットでストリングを戻しますが、組織は省略します。識別ソースからの識別レコードの属性は、パスを構成する JavaScript コードから検索できます。JavaScript コードにより提供されるプログラミングの柔軟性のために、識別ソースから使用される情報をいくつかの方法で操作できます。プログラミング構成 (例えば切り替えステートメントなど) を使用して、特定の組織名をサーバー中の別のパスにマップできます。ストリング処理は、名前をトークン化または連結してパスを派生させるために使用できます。例えば、IBM/Facilities/Irvine ストリングを DN フォーマットでトークン化して再構成し、l=Irvine, ou=Facilities, o=IBM とすることができます。

次の例は、このスクリプト能力の使用のデモンストレーションです。Acme 組織の識別ソースでは、課に div、ビジネス単位に bu、部門に dept という属性を使用します。組織の論理レイアウトは以下のとおりです。

```
組織
   部門
      ビジネス単位
         部
```

IBM Security Identity Manager Serverシステムでは、この構造は組織および組織単位にマップされ、次の例のようになります。

```
組織
   組織単位 (部門)
      組織単位 (ビジネス単位)
         組織単位 (部)
```

次の JavaScript コードは、この変換を実行する配置ルールに使用できます。

```
return "ou=" + entry.dept[o] + ",ou=" + entry.bu[o]  + ",ou=" + entry.dw[o];
```

注: このフィードのすべての識別は、Acme 組織内部にあると想定されています。

多値 ou 属性を使用する組織の場合は、配置ルールは次のようになります:

```
var ou =entry.ou;
var filt = '';
for (i = 0, i < ou.length, ++i)
{
  if (i==0)
      filt = ''ou='' + ou[i];
  }
else
     {
filt = filt + '',ou='' + ou[i];
     }
}
return filt;
```

IBM Security Identity Manager Serverは、個人を追加するときにこのスクリプトを評価して、その個人を組織内に配置します。変更要求中、このスクリプトが評価されます。個人の現在の配置と値が異なる場合、その個人は、戻されたパスに基づいて新しいロケーションに移動されます。

ID フィード・サービスの作成

CSV や DSML など、1 つの ID タイプのサービス・インスタンスを作成します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

IBM Security Identity Manager でサービスを作成するには、まずサービス・タイプを作成しておく必要があります。あるいは、IBM Security Identity Manager Server のインストール時に自動的に作成されたいずれかのサービス・タイプを使用することもできます。サービス・タイプは、アダプター・プロファイルをインストールすることによって作成できます。サービス用の新規スキーマ・クラスおよび属性を LDAP ディレクトリーに追加することもできます。アダプターのサービスを作成するには、その前に、アダプターがインストールされている必要があり、アダプター・プロファイルが作成されている必要があります。

このタスクについて

各サービスに指定したサービス名と説明がコンソールに表示されます。したがって、ユーザーおよびアドミニストレーターが理解できる値を指定することが重要です。

ID フィード・サービス・インスタンスを作成するには、以下の手順を実行します。

手順

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、「**作成**」をクリックします。 サービスの作成ウィザードが表示されます。
3. 「サービスのタイプの選択」ページで、ID フィード・サービス・タイプを 1 つ選択してから「**次へ**」をクリックします。

   テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
   - 矢印をクリックして次のページに進む。
   - 表示するページの番号を入力してから「**実行**」をクリックする。
4. 「サービス情報」ページで、サービス・インスタンスの適切な値を指定します。
5. 「**接続のテスト**」をクリックして、フィールド内のデータが正しいことを検証してから、「**終了**」をクリックします。

タスクの結果

inetOrgPerson ID フィードの場合に、テスト接続の成功メッセージが表示された場合は、すべての必須フィールドが入力されており、指定したターゲットに到達できることを示します。これは、LDAP リソースの調整が正常に行われることや、期待通りの結果が得られることを保証するものではありません。

特定の ID フィード・サービス・タイプに対するサービス・インスタンスが正常に作成されたことを示すメッセージが表示されます。

次のタスク

調整をスケジュールするか、サービスに関連付けられたタスク・リストを使用して調整を即座に実行します。

「サービスの選択」ページが表示されたら、「**リフレッシュ**」をクリックして、「**サービス**」テーブルをリフレッシュします。新規のサービス・インスタンスが表示されます。

ID フィード・サービスに対する即時調整の実行

ID フィード・サービスに対する調整アクティビティーを直ちに開始します。IBM Security Identity Manager Serverでは、調整の実行中に、指定されたファイルからの識別レコード情報を必要とします。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

適切な ID フィード・サービスをセットアップします。

手順

調整を即座に実行するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、ID フィード・サービスの横にあるアイコン（ ） をクリックしてから「**今すぐ調整**」をクリックします。

タスクの結果

即座に実行する調整要求が正常に実行依頼されたことを示すメッセージが表示されます。

次のタスク

「**ユーザーの要求の表示**」をクリックして調整の結果を表示するか、「**クローズ**」をクリックします。

ID フィード・サービスの調整スケジュールの作成

特定の間隔で実行されるよう調整をスケジュールします。IBM Security Identity Manager Serverでは、調整の実行中に、指定されたファイルからの識別レコード情報を必要とします。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権を得る方法、または別のユーザーにこのタスクの完了を依頼する方法については、システム・アドミニストレーターにお問い合わせください。

適切な ID フィード・サービスをセットアップします。

手順

ID フィード・サービスの調整スケジュールを作成するには、以下の手順を実行します。

1. ナビゲーション・ツリーから「**サービスの管理**」をクリックします。 「サービスの選択」ページが表示されます。
2. 「サービスの選択」ページで、以下の手順を実行します。
   a. 「**検索情報**」フィールドに、サービスについての情報を入力します。
   b. 「**検索基準**」フィールドで、サービスまたはビジネス単位に対して検索するかどうかを指定します。
   c. 「**サービス・タイプ**」リストからサービス・タイプを選択します。
   d. 「**状況**」リストから状況を選択し、「**検索**」をクリックします。 検索基準に合致するサービスのリストが表示されます。

      テーブルに複数のページが含まれている場合、以下の処理を行うことができます。
      - 矢印をクリックして次のページに進む。
      - 表示するページの番号を入力してから「**実行**」をクリックする。
3. 「**サービス**」テーブルで、ID フィード・サービスの横にあるアイコン (▸) をクリックしてから「**調整のセットアップ**」をクリックします。 「スケジュールの管理」ページが表示されます。
4. 「スケジュールの管理」 ページで、以下の手順を実行します。
   a. 調整が戻すアカウントをポリシーで評価するかどうかを指定します。
   b. 「**作成**」をクリックします。 「アカウント調整のセットアップ」ノートブックが表示されます。
5. 「一般」ページで、調整スケジュールについての情報を入力します。
6. 「スケジュール」ページで、調整のスケジュール間隔を選択します。 表示されるフィールドは、選択したスケジューリング・オプションによって変わります。
7. オプション: 「照会」ページで、照会に含めるアカウント属性の LDAP 検索フィルターを指定します。 このオプションは、「サポート・データのみ」を調整する場合に選択します。
8. 「**OK**」をクリックして、新規のスケジュールを保存し、ページを閉じます。

タスクの結果

調整スケジュールが正常に作成されたことを示すメッセージが表示されます。

次のタスク

別のサービス・タスクを選択するか、「**クローズ**」をクリックします。「サービスの選択」ページが表示されたら、「**リフレッシュ**」をクリックして、「**サービス**」テーブルをリフレッシュします。

第 18 章 IBM Security Identity Manager ユーティリティー

IBM Security Identity Manager には、データベース・スキーマ、LDAP、およびよく使用されるシステム・プロパティーを構成するユーティリティーが用意されています。

システム構成ツール (runConfig)

共通に使用されるシステム・プロパティーを構成するには、システム構成ツール (runConfig) を使用して、IBM Security Identity Managerシステムの設定を含んでいるプロパティー・ファイルを変更することができます。また、IBM Security Identity Manager用の WebSphere Application Server 設定も変更する必要があります。

例えば、サイトのメール・サーバーとして使用するコンピューターを変更すると、メール・サーバーの IP アドレスが変わることがあります。システム構成ツールを使用して、メール・サーバーの新しいアドレスを指定できます。

このユーティリティーの詳細については、「*IBM Security Identity Manager インストールと構成のガイド*」を参照してください。

runConfig コマンド

runConfig コマンドは、IBM Security Identity Manager に用意されているシステム構成ツール を開始します。

コマンドの説明

システム構成ツールを手動で開始するには、以下のコマンドを実行します。

ITIM_HOME/bin/**runConfig**

EJB ユーザーまたはシステム・ユーザーのユーザー ID またはパスワードがオペレーティング・システムで変更された場合は、追加の `install` 引数を使用して、WebSphere Application Server での更新を強制指定できます。これらのユーザー ID またはパスワードが変更された場合は、以下のコマンドを実行します。

ITIM_HOME/bin/**runConfig install**

システム構成ツールに問題がある場合は、*ITIM_HOME*/install_logs/runConfig.stdout ログ・ファイルを調べて詳細を確認してください。システムの構成が完了するまでには、数分の時間がかかります。`install` 引数を使用した場合は、さらに時間がかかります。

データベース構成ツール (DBConfig)

IBM Security Identity Manager データベースを構成するために、データベース構成ツール (DBConfig) を使用できます。

データベース構成ツールは、IBM Security Identity Manager が必要とするデータベース・スキーマおよびデフォルト・データを作成します。このツールは、インストール時にこのコマンドによってデータベースを構成できなかった場合にのみ 実行してください。IBM Security Identity Managerデータベース表が以前に構成されている場合は、DBConfig コマンドを実行するとユーザーにプロンプトが出されます。その場合ユーザーは、IBM Security Identity Managerのすべての既存の表をドロップするのか、またはデータベースを構成せずに終了するのかを選択できます。

「*IBM Security Identity Manager インストールと構成のガイド*」を参照してください。

DBConfig コマンド

DBConfig コマンドは、IBM Security Identity Manager に用意されているデータベース構成ツールを開始します。

コマンドの説明

データベース構成ツールを手動で開始するには、以下のコマンドを実行します。

ITIM_HOME/bin/**DBConfig**

フィールド値を変更してから、「**テスト**」をクリックして、データベース接続がアクティブになっていることを確認します。データベースのテストが成功したら、「**テスト**」ボタンが「**続行**」に変わります。「**続行**」をクリックしてからデータベース構成が完了するまでには、数分の時間がかかります。

データベース構成ツールに問題がある場合は、*ITIM_HOME*/install_logs/dbConfig.stdout ログ・ファイルを調べて詳細を確認してください。

ディレクトリー・サーバー構成ツール (ldapConfig)

ディレクトリー・サーバー構成ツール (ldapConfig) を使用して、IBM Security Identity Manager のディレクトリー・サーバーを構成できます。

ldapConfig のインストール・プロセスで LDAP の構成が失敗したとき以外は、ディレクトリー・サーバー構成ツールを使用しないでください。ディレクトリー・サーバー構成ツールは、IBM Security Identity Manager 用の LDAP スキーマおよびデフォルト・データを作成します。ディレクトリー・サーバーの構成後にディレクトリー・サーバー構成ツールを実行すると、IBM Security Identity Manager が使用するデフォルト値が復元されます。 IBM Security Identity Manager のいずれかの属性の値を変更してあった場合は、その値がデフォルト値で上書きされます。ldapConfig は、例えば、itim manager というユーザー ID のパスワードをデフォルトのパスワードである「secret」にリセットします。

「*IBM Security Identity Manager インストールと構成のガイド*」を参照してください。

ldapConfig コマンド

ldapConfig コマンドは、IBM Security Identity Manager に用意されているディレクトリー・サーバー構成ツールを開始します。

コマンドの説明

ディレクトリー・サーバー構成ツールを手動で開始するには、以下のコマンドを実行します。

ITIM_HOME/bin/**ldapConfig**

「**テスト**」をクリックして、ディレクトリー・サーバー接続を確立できることを確認します。ディレクトリー・サーバー接続のテストが成功したら、「Identity Manager ディレクトリー情報」セクションの各フィールドがアクティブになります。

ディレクトリー・サーバー構成ツールに問題がある場合は、*ITIM_HOME*/install_logs/ldapConfig.stdout ログ・ファイルを調べて詳細を確認してください。ディレクトリー・サーバーの構成が完了するまでには、数分の時間がかかります。

SAConfig: 共有アクセス・モジュール・ユーティリティー

SAConfig は、共有アクセス・モジュールを手動で構成するときに使用します。

このユーティリティーは、IBM Security Identity Manager のインストール・ロケーションの bin ディレクトリーから実行します。

表 56. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、SAConfig をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

第 19 章 IBM Security Identity Manager integration for IBM SmartCloud Control Desk

このセクションでは、IBM Security Identity Manager integration for IBM SmartCloud Control Desk パッケージについて概要を述べ、このパッケージのインストールと構成方法を説明します。

IBM Security Identity Manager integration for IBM SmartCloud Control Desk の概要

IBM Security Identity Manager integration for IBM SmartCloud Control Desk により、IBM Security Identity Manager と IBM SmartCloud Control Desk の間で通信することができます。

以下のセクションでは、IBM SmartCloud Control Desk と、その IBM Security Identity Manager との統合について概要を説明します。

IBM SmartCloud Control Desk

IBM SmartCloud Control Desk はコンピューター処理の資産管理システムで、これにより企業は、エンタープライズ・アセット管理と情報技術 (IT) 資産管理の両方の観点から、収益生成資産の運用を保持、修正、およびサポートすることができます。IBM SmartCloud Control Desk は、資産、設備、およびインベントリーに関するデータを格納および保守します。IBM SmartCloud Control Desk を使用して、保守作業のスケジュール、資産状況の追跡、インベントリーとリソースの管理、サポート要求への応答、購入管理、およびコスト分析を行うことができます。

IBM SmartCloud Control Desk ソフトウェアはモジュールに分割されており、各モジュールは、特定のビジネス機能の管理に役立つ関連アプリケーションのグループで構成されています。例えば、購入モジュールには以下のアプリケーションが含まれています。

- *送り状* アプリケーションは、送り状を記録し、それらの送り状を注文書および領収書と照合するために使用します。
- *注文書* アプリケーションは、資材またはサービスの購入で使用します。
- *受領* アプリケーションは、資材を受け取ってインベントリー内に格納するか、サービスの受領を記録するために使用します。
- 購入に関連した他のいくつかのアプリケーション。

サービス・デスク・モジュールには、お客様からの支援、情報、およびサービス要求を管理するためのアプリケーションが組み込まれています。サービス・デスク・モジュールのプリンシパル・ユーザーは、ソフトウェアを使用して内外のお客様からの要求を記録し、その問題を解決する手順を実行するサービス・デスク・エージェント です。問題の解決では、多くの場合、数人のユーザーが関係するアクティビティーのワークフローが必要とされます。だれでも知識ベースに解決策を記録することができ、解決策はそこで検索され、同様の性質の問題に適用されます。

IBM Security Identity Manager 統合と最も直接的に関連があるサービス・デスク・アプリケーションは、以下のチケット アプリケーションです。

- *サービス要求* アプリケーションは、サービスを要求する利用者からの電話または電子メール・メッセージのレコードを作成するために使用されます。
- *インシデント・アプリケーション*は、サービスの中断またはサービス品質の縮小をもたらすインシデントのレコードを作成するために使用されます。
- *問題* アプリケーションは、インシデントおよびサービス要求の原因となる、背後にある問題のレコードを作成するために使用されます。

サービス要求、インシデント、および問題のレコードは、*チケット・レコード* または*チケット・タイプ* と呼ばれます。チケット・レコードは、サービス・デスク・エージェントによって作成されるか、電子メール・メッセージ、システム・モニター・ツール、または IBM Security Identity Manager などの外部ソフトウェア・アプリケーションからのデータを使用して自動的に作成されます。チケット・レコードが作成されると、担当者またはグループがチケットの所有権を獲得し、解決に至るまで問題に対処します。IBM Security Identity Manager integration for IBM SmartCloud Control Desk では、発生するすべての changePassword 操作で、サービス要求タイプのチケットを作成できます。作成されるサービス要求には、IBM Security Identity Manager で changePassword 操作が成功したかどうかに応じ、状況として「**クローズ済み**」または「**新規**」のいずれかが指定されます。

IBM Security Identity Manager と IBM SmartCloud Control Desk の統合

この統合により、IBM Security Identity Manager から IBM SmartCloud Control Desk ユーザーを管理することができます。

IBM SmartCloud Control Desk ユーザーの管理は、IBM SmartCloud Control Desk 固有レジストリーが 1 次ユーザー・リポジトリーとして使用されている場合にサポートされます。アプリケーション・サーバーのセキュリティーが有効な場合には LDAP によって IBM SmartCloud Control Desk ユーザーが管理されており、サービス・プロバイダーを使用してユーザーを管理することはできません。この統合では、IBM Security Identity Manager によっていずれのパスワードも変更されていない場合、IBM SmartCloud Control Desk サービス要求を作成することができます。この機能により、パスワードの変更要求を自動化できるようにするという必要を満たすことができます。IBM SmartCloud Control Desk のほとんどのサービス要求には、パスワードの変更が関係しています。ユーザーがリアルタイムでパスワードを変更できるようにしてパスワードの変更タスクを自動化することにより、プロセスのボトルネックを緩和させることができます。サービスの要求の作成は、アプリケーション・サーバーのセキュリティーが使用されているかどうかに関係なく実行されます。アプリケーション・サーバーのセキュリティーが使用されている場合は、サービス要求チケットを作成するために認証が必要になります。IBM Security Identity Manager と IBM SmartCloud Control Desk の間の統合により、2 つの製品間の柔軟性を高め、IBM SmartCloud Control Desk でのユーザー管理の処理速度を速めることができます。

前提ソフトウェア

このセクションでは、IBM Security Identity Manager integration for IBM SmartCloud Control Desk の前提ソフトウェア製品について説明します。

IBM Security Identity Manager integration for IBM SmartCloud Control Desk をインストールする前に、指定オペレーティング・システムのいずれかに以下の製品をインストールし、実行されている状態にしておく必要があります。

- IBM Security Identity Manager バージョン 6.0 (Windows、AIX、HP-UX、または Solaris)
- IBM SmartCloud Control Desk バージョン 7.5 (Windows、AIX、Linux)
- Base Services がインストールされている IBM Maximo® 管理マシン (Windows)

IBM SmartCloud Control Desk 製品は、Web アプリケーション・サーバーとデータベース・サーバーでサポートされている必要があります。サポートされるソフトウェアのリストについては、IBM SmartCloud™ Control Desk Wiki を参照してください。

IBM Security Identity Manager integration for IBM SmartCloud Control Desk のコンポーネント

このセクションでは、IBM Security Identity Manager と IBM SmartCloud Control Desk を統合するために必要なコンポーネントと、それらの間の通信パスについて説明します。

IBM Security Identity Manager integration for IBM SmartCloud Control Desk ソリューションのコンポーネントは、Maximo Enterprise Adapter (MEA)、Maximo Application Server、および IBM Security Identity Manager サーバーです。 IBM Security Identity Manager サーバーは、Maximo Application Server に要求を送信します。Maximo Application Server は、IBM Security Identity Manager に応答を送信します。

インストール・ロードマップ

このセクションでは、IBM Security Identity Manager と IBM SmartCloud Control Desk の間の通信のセットアップで必要なタスクの概要を説明します。

前提ソフトウェアをインストールしたら、 272 ページの表 57 のリストにあるタスクを実行して、IBM Security Identity Manager と IBM SmartCloud Control Desk の統合をセットアップします。 272 ページの表 57 に、インストールにおける各コンポーネントの役割を示します。

表 57. インストールおよび構成タスク

ステップ	タスク	説明
1	インストール・パッケージを入手します。詳しくは、『インストール・パッケージの入手』を参照してください	IBM Security Identity Manager と IBM SmartCloud Control Deskの統合のインストール・パッケージには、統合において必要な主要なコンポーネントのインストールまたは構成で必要なファイルが含まれています。
2	IBM SmartCloud Control Desk アプリケーション・サーバーを構成します。詳しくは、273 ページの『IBM SmartCloud Control Desk の構成』 を参照してください	IBM SmartCloud Control Desk と IBM Security Identity Manager の間の通信を許可する IBM SmartCloud Control Desk アプリケーション・サーバー・インターフェースをインストールしてアクティブ化します。 このステップでは、新規の maximo.ear ファイルを IBM SmartCloud Control Desk アプリケーション・サーバーにデプロイして、IBM Security Identity Manager と IBM SmartCloud Control Desk の間の統合をサポートします。
3	IBM Security Identity Manager を構成します。詳しくは、278 ページの『IBM Security Identity Manager の構成』 を参照してください	IBM Security Identity Manager を構成して、新規 changePassword ワークフロー拡張を使用するとともに、新規 IBM SmartCloud Control Desk サービス・プロバイダーを使用可能にします。

インストール・パッケージの入手

このセクションでは、IBM Security Identity Manager integration for IBM SmartCloud Control Desk インストール・パッケージの内容について説明します。

1. IBM Security Identity Manager integration for IBM SmartCloud Control Desk インストール・パッケージを入手します。
2. tim_sd_integration.zip ファイルを、Base Services がインストールされている Maximo Administration Machine にダウンロードします。このファイルは以下のディレクトリーにあります。
   - UNIX および Linux オペレーティング・システム

     ITIM_HOME/extensions/6.0/maximo
   - Windows オペレーティング・システム

     C:¥Program Files¥IBM¥itim60¥extensions¥6.0¥maximo
3. そのファイルを Maximo Base Services のインストール・ディレクトリーに解凍します。

   例: C:¥IBM¥Maximo; C:¥IBM¥SMP¥Maximo

273 ページの表 58 に、インストール・パッケージを解凍した後に Maximo Base Services インストール・ディレクトリーに存在するサブディレクトリーとファイルのリストを示します。Maximo_Install は、Maximo Base Services のインストール・ディレクトリーを意味します。

表 58. IBM Security Identity Manager integration for IBM SmartCloud Control Desk インストール・パッケージ

最上位ディレクトリー	ファイル	説明
Maximo_Install¥tim_51	maximo.jar maximoserviceprofile.jar	tim_51 サブディレクトリー内のファイルは、IBM SmartCloud Control Desk との統合をサポートする IBM Security Identity Manager バージョンを構成するために使用します。

IBM SmartCloud Control Desk の構成

以下のセクションにおいて、Maximo_Install は、Maximo Base Services のインストール・ディレクトリーを意味します。

表 59. IBM SmartCloud Control Desk の構成ステップ

ステップ	タスク	説明
1	272 ページの『インストール・パッケージの入手』の説明に従って、IBM Security Identity Manager 統合をダウンロードして展開します。	パッケージを展開すると、Maximo_Install¥tim_51 サブディレクトリーに、IBM Security Identity Manager 統合のコンポーネントである maximo.jar ファイルと maximoserviceprofile.jar ファイルが格納されます。
2	maximo.properties ファイルが正しく構成されており、正しいデータベース・サーバーを指していることを確認してください。	maximo.properties ファイルは次のフォルダーにあります。 Maximo_Install¥applications¥maximo¥properties. JDBC 接続ストリングで、IBM SmartCloud Control Desk のインストールをサポートするデータベース・サーバーの正しい場所が指定されていることを確認します。
3	Maximo Enterprise Adapter を構成します。 274 ページの『Maximo Enterprise Adapter の構成』 で説明されている指示に従います。	Maximo Enterprise Adapter は、外部アプリケーションと Maximo を統合するためのフレームワークです。Maximo Enterprise Adapter を構成するときには、IBM SmartCloud Control Deskと IBM Security Identity Manager の間の通信を確立するために必要な Maximo インターフェースをインストールしてアクティブ化します。

表 59. IBM SmartCloud Control Desk の構成ステップ (続き)

ステップ	タスク	説明
4	maximo.ear ファイルを再作成して WebSphere にデプロイします。 275 ページの『WebSphere の構成』で説明されている指示に従います。	IBM SmartCloud Control Desk をインストールすると、maximo.ear ファイルが作成されて IBM SmartCloud Control Desk サーバーにインストールされ、続いて IBM SmartCloud Control Desk のインストール済み環境をサポートする WebSphere にデプロイされます (Web アプリケーション・サーバーは、Maximo Base Services と同じホスト・コンピューターか別のホスト・コンピューターに存在します)。IBM Security Identity Manager と IBM SmartCloud Control Desk の統合が正常に機能するには、maximo.ear ファイルを Maximo サーバーで再作成する必要があります。再作成後は、その maximo.ear を WebSphere に再デプロイする必要があります。

Maximo Enterprise Adapter の構成

このセクションでは、IBM Security Identity Manager をサポートするように Maximo Enterprise Adapter を構成する方法について説明します。

Maximo Enterprise Adapter の構成手順は、以下の 2 つの部分で構成されます。

1. Maximo Base Services に添付されている updatedb.bat スクリプトを実行します。このスクリプトは、IBM SmartCloud Control Desk アプリケーション・サーバーと IBM Tivoli Directory Integrator サーバー の間の通信で必要とされる Maximo 統合インターフェースを自動的にインストールします。
2. IBM SmartCloud Control Desk の統合モジュール内から統合インターフェースをアクティブ化することにより、Maximo Enterprise Adapter の構成を完了します。

updatedb.bat の実行

以下の手順を実行して、updatedb.bat スクリプトを入手および実行します。

始める前に

以下の指示において、Maximo_Install は、Maximo Base Services のインストール・ディレクトリーを意味します。

このタスクについて

updatedb.bat スクリプトを入手して実行するには、以下の手順を実行します。

手順

1. WebSphere Application Server 管理コンソールにログオンします。
2. 「**サーバー**」>「**サーバー・タイプ**」>「**WebSphere Application Server**」をクリックします。
3. 「**MXServer**」」を選択し、「**停止**」」をクリックします。

4. サーバーが停止したら、コマンド・プロンプトを開きます。
5. ディレクトリーを Maximo_Install¥tools¥maximo に変更します。
6. updatedb.bat スクリプトを実行します。
7. 管理コンソールに戻ります。
8. 「**MXServer**」」を選択し、「**開始**」をクリックします。

タスクの結果

updatedb.bat スクリプトが IBM SmartCloud Control Desk の場合の IBM Security Identity Manager 更新スクリプトを呼び出し、これにより、統合で必要とされるオブジェクト構造が作成されます。

WebSphere の構成

このセクションでは、WebSphere の構成方法について説明します。以下の指示において、Maximo_Install は、Maximo Base Services のインストール・ディレクトリーを意味します。

IBM Security Identity Manager の統合が正常に機能するためには、IBM Security Identity Manager 統合によって提供されるクラスを maximo.ear ファイル内に作成する必要があります。

IBM SmartCloud Control Desk のインストールが WebSphere Application Server によってサポートされる場合は、以下の手順を実行して IBM SmartCloud Control Desk 管理マシンの maximo.ear ファイル内に MaxUserProcess.class を作成し、それからご使用の WebSphere Application Server に maximo.ear ファイルをデプロイします。

注: tim_sd_integration.zip ファイルを Maximo_Install ディレクトリー内に解凍すると、自動的に MaxUserProcess.class が正しいディレクトリーに追加されます。このクラスのためにさらに構成操作を行う必要はありません。

IBM SmartCloud Control Desk ユーザーの削除の使用可能化 (オプション)

IBM SmartCloud Control Desk では、*LOGINTRACKING* 変数が有効な場合、ユーザーを削除することができません。

IBM SmartCloud Control Desk ユーザーを削除する場合は、*LOGINTRACKING* 変数を無効にしてください。このセクションでは、次の手順を使用することによって、操作を実行します。

1. 管理権限で IBM SmartCloud Control Desk サーバーにログオンします。
2. 「**移動**」 → 「**セキュリティー**」 → 「**ユーザー**」をクリックします。
3. 「**アクション**」メニューで、「**セキュリティー・コントロール**」を選択します。
4. 「**ログイン・トラッキングを有効にする**」チェック・ボックスにチェック・マークが付いている場合は、それをクリアします。

注: *LOGINTRACKING* にチェック・マークが付いていない場合は、IBM SmartCloud Control Deskサービス・フォームで「**Maximo ユーザーの削除を有効に**

しますか? (Maximo User Deletion Enabled?)」 チェック・ボックスを選択します。IBM Security Identity Manager でのこのチェック・ボックスは、IBM SmartCloud Control Desk ユーザーを削除するために必要です。IBM SmartCloud Control Desk サービスの構成に関して詳しくは、 278 ページの『IBM Security Identity Manager の構成』を参照してください。

IBM SmartCloud Control Deskへのパスワード・リンクの追加 (オプション)

IBM Security Identity Manager は、固有レジストリーが使用されているか、LDAP を使用してユーザー情報を保管しているときに、IBM SmartCloud Control Desk ユーザーを管理します。LDAP は、J2EE アプリケーション・サーバーのセキュリティーが有効な場合に、ユーザー情報を保管するために使用します。IBM SmartCloud Control Desk 固有レジストリーを使用する場合は、IBM SmartCloud Control Desk サービス・プロバイダーを使用してユーザーを管理します。ただし、LDAP を使用する場合は、IBM Security Identity Manager による IBM SmartCloud Control Desk ユーザーの管理で LDAP アダプターのみを使用します。

J2EE アプリケーション・サーバーのセキュリティーが有効な場合、「**パスワードを忘れましたか?**」リンクは使用可能になりません。ただし、固有レジストリーの使用中は使用可能になります。オプションで、このリンク先を IBM Security Identity Manager セルフ・サービス・ユーザー・インターフェースにすることにより、IBM SmartCloud Control Desk ユーザーを保管するために LDAP または固有レジストリーを使用中の場合にはパスワードをリセットすることができ、これにより、IBM SmartCloud Control Desk サーバーを管理するようにサービスを構成できます。

IBM SmartCloud Control Desk インターフェースは、オプションで、「**パスワードを忘れましたか?**」のリンク先が IBM Security Identity Manager セルフ・サービス・インターフェースとなるように変更することができます。このアクションにより IBM SmartCloud Control Desk ユーザーは、IBM Security Identity Manager を介して自分のパスワードを管理できます。さらに、パスワードを忘れてログインできない場合には、IBM SmartCloud Control Desk のパスワードをリセットすることもできます。

IBM SmartCloud Control Desk ログイン・ページにリンクを追加するには、以下の手順を実行します。

1. `Maximo_Install¥applications¥maximo¥maximouiweb¥webmodule¥webclient¥login` ディレクトリーを選択します。
2. `login.jsp` ファイルに変更を加えます。
   a. `login.jsp` ファイルで次の行を検索します。`<button id="forgotpwdlink" class="link" type="submit"><span><%=labels.forgotPassword%></span></button>`
   b. 次のようにして、その行をコメント化します。`<!--button id="forgotpwdlink" class="link" type="submit"><span><%=labels.forgotPassword%></span></button -->`
   c. コメント化した行の下に次の行を追加します。`<a href="http://hostname:port/itim/self"><%=labels.forgotPassword%></a>`

d. ホスト名とポートを、特定の IBM Security Identity Manager 展開に適切な値で置換します。

e. 手順 a. に進み、すべての「パスワードを忘れましたか?」リンクを検索して変更します。

IBM SmartCloud Control Deskの作成

このセクションでは、IBM SmartCloud Control Desk の作成について説明します。

以下の手順を実行します。

1. Maximo Base Services 管理マシンでコマンド・プロンプトを開きます。

   注: Maximo Base Services ソフトウェアは、IBM SmartCloud Control Desk をサポートする WebSphere Application Server と同じまたは別のコンピューターにインストールできます。

2. ディレクトリーを `Maximo_Install¥deployment` に変更します。

3. 次のコマンド入力して `maximo.ear` ファイルを再作成します。

   ```
   buildmaximoear.cmd
   ```

   `buildmaximoear.cmd` ファイルは `maximo.ear` ファイルを再作成し、変更されたクラス・ファイルを自動的に引き込み、`maximo.ear` ファイルに元々存在していたファイルを置き換えます。このプロセスが完了するまで待ちます。

4. 新しい `maximo.ear` ファイルを、Maximo Base Services サーバーから WebSphere Application Server 上の任意の場所にコピーします。新しい `maximo.ear` ファイルは、Maximo Base Services 管理マシン上の次のディレクトリーに格納されます。

   ```
   Maximo_Install¥deployment¥default
   ```

WebSphere Application Server での IBM SmartCloud Control Desk のデプロイ

このセクションでは、WebSphere Application Server での IBM SmartCloud Control Desk のデプロイについて説明します。

WebSphere Application Server で IBM SmartCloud Control Desk をデプロイするには、以下の手順を実行します。

1. WebSphere Application Server 管理コンソールにログオンします。
2. ナビゲーション・ペインで「**アプリケーション**」ノードを展開し、「**エンタープライズ・アプリケーション**」を選択します。「エンタープライズ・アプリケーション」ウィンドウが表示されます。
3. 「**MAXIMO**」の横のチェック・ボックスを選択し、「**更新**」をクリックします。
4. 「**アプリケーション全体を置換する**」をクリックします。
5. 「**リモート・ファイル・システム**」をクリックして、「**参照**」をクリックします。
6. WebSphere Application Server のノードを選択します。

7. コピーした maximo.ear ファイルの場所を参照します。ファイルを選択し、「**OK**」をクリックします。
8. 「**次へ**」をクリックします。
9. 「**インストールのオプションを選択 (Select Installation options)**」で、「**次へ**」をクリックします。
10. 「**サーバーにモジュールをマップ**」で「**次へ**」をクリックします。
11. 「要約」ページで「**終了**」をクリックします。maximo.ear ファイルが再デプロイされます。このプロセスには数分かかる場合があります。
12. 「**マスター構成に保存**」をクリックします。
13. ナビゲーション・ペインで「**アプリケーション**」ノードを展開し、「**エンタープライズ・アプリケーション**」を選択します。
14. 「**MAXIMO**」の横のチェック・ボックスを選択し、「**開始**」をクリックします。このプロセスが完了するまで待ちます。
15. WebSphere Application Server 管理コンソールからログアウトします。

IBM Security Identity Manager の構成

このセクションでは、IBM Security Identity Manager を構成する手順について説明します。

注: 以下のセクションにおいて、ISIM_HOME は IBM Security Identity Manager がインストールされているディレクトリーを意味します。

表 60. IBM Security Identity Manager の構成ステップ

ステップ	タスク	説明
1	maximo.jar を共有ライブラリー・ディレクトリーに追加します。	maximo.jar アーカイブには、IBM Security Identity Manager と IBM SmartCloud Control Desk の間の統合処理を行うコードが含まれています。
2	maximo.jar を共有ライブラリー・エントリーに追加します。	IBM Security Identity Manager は、maximo.jar ファイルを使用するために、そのファイルについての情報が必要です。
3	enRole.properties の変更	パスワード拡張のための IBM SmartCloud Control Desk 接続情報は、プロパティー・ファイルで設定する必要があります。
4	scriptframework.properties の変更	changePassword 拡張はスクリプト拡張で、プロパティー・ファイルを変更してこの変更を反映させる必要があります。
5	WebSphere Application Server の再始動	変更を有効にするには、WebSphere Application Server を再始動する必要があります。
6	ワークフロー拡張の構成	changePassword 拡張は、IBM Security Identity Manager 構成でセットアップする必要があります。
7	IBM SmartCloud Control Desk サービス・プロファイルの構成	IBM SmartCloud Control Desk ユーザーを管理するには、サービス・プロファイルを構成する必要があります。

WebSphere の構成

IBM Security Identity Manager と IBM SmartCloud Control Desk の間の統合が正常に機能するには、以下の手順を実行する必要があります。

1. maximo.jar ファイルを、Maximo Base Services 管理マシンの Maximo_Install¥tim_51 ディレクトリーから IBM Security Identity Manager Server の ISIM_HOME¥lib ディレクトリーにコピーします。クラスター環境の場合は、各クラスター・メンバーの ISIM_HOME/lib ディレクトリーにこのファイルをコピーします。
2. IBM Security Identity Manager をインストールするため、WebSphere Application Server 管理コンソールにログオンします。installation.
3. 「**環境**」 → 「**共有ライブラリー**」 → 「**ITIM_LIB**」をクリックします。
4. 次の行を追加してクラスパスを変更します。

   ```
   ${ISIM_HOME}/lib/maximo.jar
   ```
5. 「**OK**」をクリックします。

IBM Security Identity Manager 6.0 の構成

IBM Security Identity Manager と IBM SmartCloud Control Desk の間の統合が正常に機能するには、以下の手順を実行する必要があります。

enRole.properties の変更

1. ISIM_HOME¥data ディレクトリーにナビゲートします。
2. 次のテキストを追加することにより、enRole.properties ファイルを編集します。

   ```
   ###################################
   ## Maximo Workflow Extension Properties
   ###################################
   maximo.url=http://hostname:port
   maximo.security=true
   maximo.user=maxadmin
   maximo.password=maxadmin
   ```
3. *hostname* と *port* を、IBM SmartCloud Control Desk 環境に対応する値で置換します。
4. maximo.security 値を、アプリケーション・サーバーのセキュリティーが有効かどうかに応じて、true または false に設定します。値を true に設定する場合は、アプリケーション・サーバーのセキュリティーが有効になっているときの IBM SmartCloud Control Desk でのサービス要求作成を使用可能にするため、maximo.user フィールドと maximo.password フィールドが必要になります。クラスター環境では、このファイルを各クラスター・メンバーで変更する必要があります。
5. enRole.properties ファイルを保存して閉じます。

scriptframework.properties の変更

1. ISIM_HOME¥data ディレクトリーにナビゲートします。
2. ワークフロー拡張セクションの下に次の行を追加することにより、scriptframework.properties ファイルを編集します。

   ```
   ITIM.extension.Workflow.Maximo=com.ibm.itim.maximo.MaximoExtension
   ```
3. scriptframework.properties ファイルを保存して閉じます。

WebSphere Application Server の再始動

WebSphere Application Server を停止して始動することで再始動します。クラスター環境では、すべてのアプリケーション・クラスター・メンバーを再始動します。

changePasssword ワークフロー拡張の構成

changePassword 拡張が正常に機能するようにするには、以下の手順を実行します。

1. アドミニストレーターとして IBM Security Identity Manager にログインします。
2. 「**システムの構成**」 → 「**操作の管理**」をクリックします。
3. 「**エンティティー・タイプ・レベル**」ラジオ・ボタンを選択します。
4. 「**changePassword**」リンクをクリックします。
5. **CHANGEPASSWORD** 拡張ボックスをダブルクリックします。
6. 「**ポストスクリプト**」タブをクリックし、次のテキストを追加します。

   ```
   Maximo.addTicket(Entity.get(), activity);
   ```

7. 「**OK**」をクリックします。
8. 「**適用**」をクリックし、次に「**OK**」をクリックして変更を検証します。

IBM SmartCloud Control Desk サービス・プロバイダーの構成

IBM SmartCloud Control Desk ユーザー管理のサポートを有効にするには、以下の手順を実行します。

1. maximoserviceprofile.jar ファイルを、Maximo_Install¥tim_51 ディレクトリーから、IBM Security Identity Manager にログイン可能な Web ブラウザーを備えたマシンにコピーします。そのマシンから残りの手順を実行します。
2. 管理コンソールを使用して、IBM Security Identity Manager にログインします。
3. 「**サービス・タイプの管理**」をクリックします。
4. 「**インポート**」をクリックします。
5. 「**参照**」をクリックし、maximoserviceprofile.jar ファイルがあるディレクトリーにナビゲートします。
6. maximoserviceprofile.jar を選択します。
7. 「**OK**」をクリックし、操作が完了するまで数分待ちます。
8. 「**サービスの管理**」をクリックします。
9. 「**作成**」をクリックし、メニューから「**Maximo サービス**」を選択して、「**次へ**」をクリックします。
10. 固有のサービス名を入力し、IBM SmartCloud Control Desk サーバーで SSL が使用されているかどうかに応じて、IBM SmartCloud Control Desk の URL を http://*hostname:port* または https://*hostname:port* のどちらかの形式で入力します。
11. デフォルト・ユーザー MXINTADM ではなく、特定のユーザーとして操作を実行する場合は、ユーザー ID とパスワードを入力します。これらのフィールドを空白のままにすると、操作は MXINTADM として実行されます。

12. *LOGINTRACKING* が false で、IBM SmartCloud Control Desk ユーザーを削除する場合は、「**Maximo ユーザーの削除を有効にしますか? (User Deletion Enabled?)**」チェック・ボックスを選択します。
13. 「**接続のテスト**」をクリックしてテストが成功したことを確認し、次に「**終了**」をクリックします。

注: 特定のユーザーとして操作を実行することを選択する場合は、そのユーザーに必要な特権を忘れずに付与してください。例えば、ユーザーをグループに追加する場合、グループ割り当てを実行するように構成されているアカウントには、ユーザーをそれらのグループに割り当てる権限が必要です。グループの再割り当て権限について詳しくは、IBM SmartCloud Control Desk の資料を参照してください。また、新規サービスの作成時に作成されるデフォルトのプロビジョニング・ポリシーを変更して、すべての必要な属性が設定されていることを確認する必要もあります。IBM Security Identity Manager API を使用して Maximo サービスを作成する場合のサービス・プロファイル名は *maximoserviceprofile* です。アカウントを作成する場合、アカウント・プロファイル名は *MaximoAccount* です。SSL を使用している場合の証明書の追加方法については、ご使用のバージョンの WebSphere の適切な資料を参照してください。

アダプター属性

このセクションでは、アダプター属性について説明します。

属性の説明

IBM Security Identity Manager Server は、ネットワーク経由で送信される伝送パケット内に含まれる属性を使用して、IBM SmartCloud Control Desk サービス・プロバイダーと通信します。パケット内に含まれる属性の組み合わせは、Security Identity Manager Serverが IBM SmartCloud Control Desk サービス・プロバイダーに要求するアクションのタイプによって異なります。

表 61 に、IBM SmartCloud Control Desk サービス・プロバイダーが使用する属性のリストと、それらの属性の概要とデータ・タイプを示します。

表 61. 属性、説明、および対応するデータ・タイプ

属性	ディレクトリー・サーバー属性	説明	データ・フォーマット
Userid	eruid	アカウントのユーザー ID を指定します。	ストリング
パスワード	erpassword	アカウント・パスワードを指定します。	ストリング
状況	eraccountstatus	アカウントの状況を指定します (ACTIVE、INACTIVE)。	ストリング
タイプ	ermaximousertype	Maximo ユーザーのタイプを指定します。	ストリング
Defsite	ermaximodefsite	アカウントのデフォルト・サイトを指定します。	ストリング
Storeroomsite	ermaximostoresite	アカウントのストアルーム・サイトを指定します。	ストリング

表 61. 属性、説明、および対応するデータ・タイプ (続き)

属性	ディレクトリー・サーバー属性	説明	データ・フォーマット
Querywithsite	ermaximoquerysite	挿入サイトを表示フィルターとして使用するかどうかを指定します。	ブール
Emailpswd	ermaximoemailpswd	アカウント作成時にユーザーにパスワードを電子メールで送信するかどうかを指定します。	ブール
Sysuser	ermaximosysuser	アカウントがシステム・アカウントかどうかを指定します。	ブール
Screenreader	ermaximoscreen	アカウントでスクリーン・リーダーを必要とするかどうかを指定します。	ブール
Firstname	ermaximofirstname	ユーザー・アカウントをサポートするユーザーの名を指定します。	ストリング
Lastname	ermaximolastname	ユーザー・アカウントをサポートするユーザーの姓を指定します。	ストリング
Phonenum	ermaximophone	ユーザーの 1 次電話番号を指定します。	ストリング
PhoneType	ermaixmophonetype	ユーザーの 1 次電話番号のタイプを指定します。	ストリング
電子メール	ermaximoemail	ユーザーの 1 次電子メール・アドレスを指定します。	ストリング
Memo	ermaximomemo	ユーザーのメモを指定します。	ストリング
Addressline1	ermaximoaddress	ユーザーの住所を指定します。	ストリング
市区町村	ermaximocity	ユーザーの市区町村を指定します。	ストリング
Stateprovince	ermaximostate	ユーザーの都道府県を指定します。	ストリング
Postalcode	ermaximozip	ユーザーの郵便番号を指定します。	ストリング
国	ermaximocountry	ユーザーの国を指定します。	ストリング
Groupname	ermaximogroupname	グループ名を指定します。	ストリング
GroupDescription	ermaximogroupdescription	グループの説明を指定します。	ストリング

アクション別の IBM SmartCloud Control Desk サービス・プロバイダー属性

以下のリストに、機能的なトランザクション・グループによって編成される一般的な IBM SmartCloud Control Desk サービス・プロバイダーのアクションを示します。これらのリストには、そのアクションを完了するために IBM SmartCloud Control Desk サービス・プロバイダーに送信される必須属性とオプション属性に関する追加情報が含まれています。

System Login Add

System Login Add は、指定された属性を持つユーザー・アカウントをドメイン内で作成するための要求です。

表 62. 追加要求属性

必要な属性	オプション属性
eruid ermaximoemailpswd	サポートされる他のすべての属性

System Login Change

System Login Change は、指定されたユーザーの 1 つ以上の属性を変更するための要求です。

表 63. 変更要求属性

必要な属性	オプション属性
eruid	サポートされる他のすべての属性

System Login Delete

System Login Delete は、指定したユーザーを IBM SmartCloud Control Desk レジストリーから除去するための要求です。

表 64. 削除要求属性

必要な属性	オプション属性
eruid	なし

System Login Suspend

System Login Suspend は、ユーザー・アカウントを使用不可にするための要求です。ユーザーは除去されず、属性は変更されません。

表 65. サスペンド要求属性

必要な属性	オプション属性
eruid eraccountstatus	なし

System Login Restore

System Login Restore は、以前にサスペンドされたユーザー・アカウントをアクティブ化するための要求です。 アカウントが復元された後、ユーザーは、Suspend 機能が呼び出される前と同じ属性を使用してシステムにアクセスできます。

表 66. 復元要求属性

必要な属性	オプション属性
eruid eraccountstatus	なし

Reconciliation

Reconciliation 要求は、IBM Security Identity Manager とサービス・プロバイダー間のユーザー・アカウント情報を同期します。

表 67. 復元要求属性

必要な属性	オプション属性
なし	なし

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として『現存するままの状態で』提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向性および指針に関するすべての記述は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。 従って IBM は、これらのサンプル・プログラムについて信頼性、

利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生した創作物にも、次のように、著作権表示を入れていただく必要があります。「© (お客様の会社名) (西暦年)」このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. 2004, 2012. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

ここに含まれる Oracle Outside In Technology は、制限付きご使用条件の適用を受け、このアプリケーションとともに使用する場合のみ使用できます。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

C

D

E

F

H

I

J

K

L

M

S

T

U

W

Printed in Japan

SA88-4862-00

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21