IBM Security Identity Manager
バージョン6.0

製品概要

GA88-4857-00
(英文原典：GC14-7692-00)

IBM Security Identity Manager
バージョン6.0

製品概要

GA88-4857-00
(英文原典：GC14-7692-00)

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、 77 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 (製品番号 5724-C34) のバージョン 6.0、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： GC14-7692-00
IBM Security Identity Manager
Version 6.0
Product Overview 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

第1刷 2012.11

目次

表リスト

本書について

「*IBM Security Identity Manager 製品概要*」には、IBM Security Identity Manager に関する一般情報が記載されています。下記の情報を含んでいます。

- 新規または非推奨の製品機構および製品機能など、製品リリース
- 製品の基礎となるオープン・スタンダード、テクノロジー、およびアーキテクチャー
- 製品機能の基礎となるユーザー・モデルおよび役割
- 各種の user 役割をサポートするために提供されているグラフィカル・インターフェースおよびツール

資料および用語集へのアクセス

このセクションには、以下の内容が含まれています。

- IBM Security Identity Manager ライブラリー内の資料のリスト。
- 『オンライン資料』へのリンク。
- viii 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、以下の資料があります。

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

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htmサイトには、本製品に関するインフォメーション・センターのウェルカム・ページが掲載されています。

IBM Security インフォメーション・センター

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp サイトには、すべての IBM Security 製品資料のアルファベット順リストと一般情報が掲載されています。

IBM Publications Center

http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wssサイトには、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 リファレンス・ガイド*」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、以下の IBM Education Web サイトを参照してください。 http://www.ibm.com/software/tivoli/education

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 Troubleshooting Guide*」には、以下の事項に関する詳細が記載されています。

- IBM サポートに連絡を取る前に収集する必要のある情報。
- IBM サポートに連絡を取るためのさまざまな方法。

- IBM サポート・アシスタントの使用方法。
- 問題をユーザー自身で切り分けて修正するための手順および問題判別リソース。

注: 本製品のインフォメーション・センターにある「**コミュニティーとサポート**」タブに追加のサポート・リソースが提供されます。

第 1 章 ソフトウェア・イメージの入手方法

IBM® Security Identity Manager のインストール・ファイルとフィックスパックは、IBM Passport Advantage® Web サイトまたは DVD 配布で入手できます。

パスポート・アドバンテージ Web サイトには、IBM 製品用の eAssemblies と呼ばれるパッケージが用意されています。

IBM Security Identity Manager 向け eAssemblies を入手するには、IBM Security Identity Manager ダウンロード資料を参照してください。

「*IBM Security Identity Manager インストール・ガイド*」には、IBM Security Identity Manager および前提ミドルウェア製品をインストールするための詳しい手順が示されています。

以下の条件により、組織に適合する手順が決まります。

- IBM Security Identity Manager により使用されるオペレーティング・システム
- 製品を使用するための言語要件
- 実行する必要のあるインストールのタイプ:

製品およびすべての前提条件製品用の eAssembly

IBM Security Identity Manager のインストール・プログラムを使用し、「*IBM Security Identity Manager インストール・ガイド*」の説明に従うと、IBM Security Identity Manager、前提条件製品、および必要なフィックスパックをインストールできます。組織で IBM Security Identity Managerに必要な 1 つ以上の製品を現在使用していない場合、このタイプのインストールを使用してください。

手動インストール用の eAssembly

前提条件製品とは別に IBM Security Identity Managerをインストールすること、およびインストールされていない前提条件製品を個別にインストールすることができます。 各前提条件製品が、必要なフィックス・レベルまたはパッチ・レベルで作動するか検査する必要があります。

第 2 章 ハードウェア要件およびソフトウェア要件

IBM Security Identity Manager には、特定のハードウェア要件があり、特定バージョンのオペレーティング・システム、ミドルウェア、およびブラウザーをサポートします。

このセクション内のトピックでは、各ソフトウェア製品のハードウェア要件およびサポート対象バージョンをリストします。製品リリースのリリース時点でのサポート対象バージョンをリストします。

注: 前提ソフトウェアのサポートは、絶えず更新されます。この情報に関する最新情報については、https://www.ibm.com/support/docview.wss?uid=swg27020534を参照してください。

ハードウェア要件

IBM Security Identity Manager には、以下のハードウェア要件があります。

表 1. IBM Security Identity Manager のハードウェア要件

システム・コンポーネント	最小値 *	推奨値 **
システム・メモリー (RAM)	2 ギガバイト	4 ギガバイト
プロセッサー速度	シングル 2.0 ギガヘルツの Intel または pSeries® プロセッサー	デュアル 3.2 ギガヘルツの Intel または pSeries プロセッサー
製品および前提条件製品用のディスク・スペース	20 ギガバイト	25 ギガバイト
* 最小値: これらの値では、IBM Security Identity Manager の基本使用が可能になります。 ** 推奨値: 実稼働環境に適したさらに大きい値を使用する必要がある場合があります。		

オペレーティング・システムのサポート

IBM Security Identity Manager は複数のオペレーティング・システムをサポートします。

IBM Security Identity Manager のインストール・プログラムは、インストール・プロセスを開始する前に、特定のオペレーティング・システムおよびレベルが存在しているかどうかチェックします。

表 2. オペレーティング・システムのサポート

オペレーティング・システム	プラットフォーム	パッチまたは保守レベル
AIX® バージョン 6.1 および AIX バージョン 7.1	System p®	なし
Oracle Solaris 10	SPARC	なし

表 2. オペレーティング・システムのサポート (続き)

オペレーティング・システム	プラットフォーム	パッチまたは保守レベル
Windows Server 2008 Standard Edition および Enterprise Edition	x86-32、x86-64	なし
Windows Server 2008 Release 2 Standard Edition and Enterprise Edition	x86-64	なし
Red Hat Linux Enterprise 5.0、Red Hat Linux Enterprise 6.0	System z®、System p、x86-32、x86-64	• 5.0 については、更新 1 から更新 5 まで。 • 5.0 と 6.0 の両方については、Security Enhanced Linux を使用不可にする必要があります。「*IBM Security Identity Manager インストール・ガイド*」のトピック『Red Hat Linux サーバーの構成』を参照してください。
SUSE Linux Enterprise Server 10.0、SUSE Linux Enterprise Server 11.0	System z、System p、x86-32、x86-64	なし

仮想化のサポート

IBM Security Identity Manager では仮想化環境がサポートされています。

製品リリース時点で IBM Security Identity Manager でサポートされる仮想化製品のリストについては、表 3を参照してください。

表 3. 仮想化のサポート

製品	適用可能なオペレーティング・システム
IBM AIX Workload Partitioning (WPAR) および Logical Partitioning (LPAR) 6.1 および 7.1 と今後のフィックスパック	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用
IBM PowerVM® Hypervisor (LPAR、DPAR、Micro-Partition) のサポートされるすべてのバージョンおよび今後のフィックスパック	AIX
IBM PR/SM™ のすべてのバージョンおよび今後のフィックスパック	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用
IBM z/VM® Hypervisor 5.4 および今後のすべてのフィックスパック	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用
IBM z/VM Hypervisor 6.1 および今後のすべてのフィックスパック	Linux
SUSE Linux Enterprise Server (SLES) 11 内の KVM	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用

表 3. 仮想化のサポート (続き)

製品	適用可能なオペレーティング・システム
Red Hat Enterprise Linux (RHEL) 5.4 とともに配布される Red Hat KVM および今後のフィックスパック	Linux、Windows
Red Hat Enterprise Linux (RHEL) 6.0 とともに配布される Red Hat KVM および今後のフィックスパック	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用
Sun Solaris 10 Global/Local Zones (SPARC) 10 および今後のフィックスパック	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用
Sun/Oracle Logical Domains (LDoms) のすべてのバージョンおよび今後のフィックスパック	Solaris
VMware ESXi 4.0 および今後のフィックスパック	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用
VMware ESXi 5.0 および今後のフィックスパック	サポート対象のすべてのオペレーティング・システム・バージョンに自動的に適用

Java Runtime Environment のサポート

IBM Security Identity Manager には Java™ ランタイム環境 (JRE) バージョン 1.6 SR10 フィックスパック 1 が必要です。

WebSphere® Application Server バージョン 7.0 フィックスパック 23 がインストールされている場合、このバージョンは *WAS_HOME*/java ディレクトリーにインストールされます。

IBM または他のベンダーが提供している、個別にインストールされる Java 用開発キットの使用はサポートされていません。 ブラウザーを使用して IBM Security Identity Managerサーバーへのクライアント接続を作成するための Java ランタイム環境 の要件は、WebSphere Application Server を実行するための JRE の要件とは異なります。

WebSphere Application Server のサポート

IBM Security Identity Manager は、WebSphere Application Server 環境ではエンタープライズ・アプリケーションとして実行されます。

IBM Security Identity Manager では、以下が必要です。

- WebSphere Application Server バージョン 7.0
- WebSphere Application Server バージョン 7.0 および SDK 用の WebSphere フィックスパック 23
- WebSphere 暫定修正 PM64800
- WebSphere 暫定修正 PM66514
- WebSphere 暫定修正 7.0.0.23-WS-WAS-IFPM71296

注: 暫定修正を適用する前にフィックスパック 23 を適用する必要があります。

WebSphere は、IBM Security Identity Manager でサポートされる各オペレーティング・システム・バージョンをサポートします。各オペレーティング・システムの WebSphere 要件については、WebSphere Web サイト (http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg27012369) をお調べください。

データベース・サーバーのサポート

IBM Security Identity Manager は複数のデータベース・サーバー製品をサポートします。

表 4. データベース・サーバーのサポート

データベース・サーバー	フィックスパック	注釈
IBM DB2® Enterprise バージョン 9.5	フィックスパック 3b	IBM DB2 Enterprise 9.5 は、Linux 32 ビット・オペレーティング・システム、または pSeries ハードウェア上のすべての Linux オペレーティング・システムでサポートされません。 IBM DB2 9.5 WorkGroup Edition は、Linux 32 ビット・オペレーティング・システム用にバンドルされています。
IBM DB2 Enterprise バージョン 9.7	フィックスパック 4	• Linux では、DB2 9.7 Enterprise Server Edition は 64 ビット・アーキテクチャーでのみサポートされます。 http://www.ibm.com/support/docview.wss?uid=swg27020534を参照してください。 • IBM DB2 9.7 Workgroup Edition は Linux 32 ビット・オペレーティング・システムでは必須です。 • IBM Tivoli® Directory Server requires フィックスパック 2 • Red Hat Linux 6.0 では Fix Pack 4 が必要です
Microsoft SQL Server 2008、Enterprise Edition Microsoft SQL Server 2008 R2	なし	• WebSphere Application Server supports Microsoft SQL Server 2008、 Enterprise Edition • Microsoft SQL Server が IBM Security Identity Manager データベース用に使用されている場合、 IBM Security Identity Manager は、サポートされる Windows オペレーティング・システム上で稼働している必要があります。 Microsoft SQL Server 2008 での JDBC ドライバーのサポートについて詳しくは、http://www.ibm.com/support/docview.wss?uid=swg27020534 を参照してください。
Oracle 10g リリース 2 (バージョン 10.2.0.2) および Oracle 11g リリース 2	なし	• Oracle 10gR2 と Oracle 11g の両方のデータベースには、Oracle 11.1.0.7 データベース・ドライバーが必要です。 • Oracle 11g バージョン 11.1.0.7.0 は、Windows Server 2008 32 ビットおよび 64 ビット・オペレーティング・システムをサポートしています。 • Oracle11gR2 は、Oracle11gR1 ojdbc5 ドライバーを使用する場合にのみサポートされます。

ディレクトリー・サーバーのサポート

IBM Security Identity Manager は複数のディレクトリー・サーバーをサポートします。

表 5. ディレクトリー・サーバーのサポート

ディレクトリー・サーバー	フィックスパック	注釈
IBM Tivoli Directory Server バージョン 6.2	FP1	IBM Tivoli Directory Server は、IBM Security Identity Manager でサポートされるオペレーティング・システム・リリースをサポートします。
IBM Tivoli Directory Server バージョン 6.3	なし	
Sun Directory Server Enterprise Edition 6.3.1	なし	オペレーティング・システム・サポートを確認するには、Oracle の資料を参照してください。
Oracle Directory Server Enterprise Edition 11.1.1	なし	

Directory Integrator のサポート

IBM Security Identity Manager は、IBM Tivoli Directory Integrator をサポートします。

オプションで、IBM Security Identity Manager とともに使用する IBM Tivoli Directory Integrator をインストールすることができます。

IBM Tivoli Directory Integrator は、インストールしたエージェントレス・アダプターと IBM Security Identity Manager との間の通信を有効にするために使用されます。「*IBM Security Identity Manager インストール・ガイド*」を参照してください。

表 6. サポートされる IBM Tivoli Directory Integrator のバージョン

リリース	フィックスパック
IBM Tivoli Directory Integrator バージョン 7.1	フィックスパック 5
IBM Tivoli Directory Integrator バージョン 7.1.1	Fix Pack 1 および Limited Availability Fix 7.1.1-TIV-TDI-LA0001

IBM Tivoli Directory Integrator は、IBM Security Identity Manager でサポートされる各オペレーティング・システム・バージョンをサポートします。

レポート・サーバーのサポート

IBM Security Identity Manager は IBM Tivoli Common Reporting バージョン 2.1.1 をサポートします。

以下のフィックスパックおよび iFixes が必要です。フィックスは以下の順序でインストールしてください。

1. IBM Tivoli Common Reporting バージョン 2.1.1 暫定修正 2

2. IBM Tivoli Common Reporting バージョン 2.1.1 暫定修正 5
3. IBM Tivoli Integrated Portal フィックスパック 2.2.0.7
4. IBM Tivoli Common Reporting バージョン 2.1.1 暫定修正 6

フィックスを入手するには、以下のようにします。

- IBM Tivoli Common Reporting Server 用の最新フィックスは、Fix Central Web サイト (http://www.ibm.com/support/fixcentral/) からダウンロードします。
- IBM Tivoli Common Reporting バージョン 2.1.1 暫定修正 6 をインストールする前に、IBM Tivoli Integrated Portal フィックスパック 2.2.0.7 を入手してインストールしてください。IBM Tivoli Integrated Portal フィックスパック 2.2.0.7 の入手方法については、IBM developerWorks® のトピック『Tivoli Common Reporting 2.1.1 Interim Fix 6』を参照してください。

クライアント接続のためのブラウザー要件

IBM Security Identity Manager には、クライアント接続のためのブラウザー要件があります。

IBM Security Identity Manager では、以下のブラウザー・バージョンがサポートされています。

- Microsoft Internet Explorer 8.0
- Microsoft Internet Explorer 9.0
- Mozilla Firefox 3.6 (AIX のみでサポート)

  注: Firefox 3.6 は Next-Generation Java プラグインを必要とします。このプラグインは Java 6 更新 10 以降に含まれています。
- Mozilla Firefox 10 Extended Support Release (AIX ではサポートされません)
- IBM Security Identity Manager ソフトウェア配布には、サポート対象ブラウザーが含まれていません。
- IBM Security Identity Manager 管理ユーザー・インターフェースは、Sun Microsystems JRE バージョン 1.6 以降で提供される Java プラグインを必要とするアプレットを使用します。アプレットを含むページをブラウザーが要求すると、ブラウザーは Java プラグインを使用してアプレットの読み込みを試みます。必要な JRE がシステムにない場合、ブラウザーにより、正しい Java プラグインを要求するプロンプトがユーザーに出されるか、またはウィンドウ内への項目の表示が完了しません。 Java アプレットを含まないすべてのページで、JRE がインストールされているかどうかにかかわらず、IBM Security Identity Manager のユーザー・インターフェースは正常に表示されます。
- IBM Security Identity Manager とのセッションを確立するためには、ブラウザーの Cookie を有効にする必要があります。
- 同一のクライアント・コンピューターから、2 つ以上の別々のブラウザー・セッションを開始しないでください。 2 つのセッションは 1 つのセッション ID とみなされ、結果としてデータに関連する問題が発生します。

アダプター・レベルのサポート

IBM Security Identity Manager インストール・プログラムは、常にいくつかのアダプター・プロファイルをインストールします。

インストール・プログラムは以下のプロファイルをインストールします。

- AIX プロファイル (UNIX および Linux アダプター)
- Solaris プロファイル (UNIX および Linux アダプター)
- HP-UX プロファイル (UNIX および Linux アダプター)
- Linux プロファイル (UNIX および Linux アダプター)
- LDAP プロファイル (LDAP アダプター)

IBM Security Identity Manager インストール・プログラムは、オプションで、IBM Security Identity Manager LDAP アダプターと IBM Security Identity Manager UNIX および Linux アダプターをインストールします。これより新しいバージョンのアダプターを別個のダウンロードで入手できる場合があります。アダプターを使用する前に、最新バージョンをインストールしてください。

IBM Security Identity Manager のインストール時にアダプターをインストールしないように選択した場合には、アダプターをインストールするための追加ステップを実行する必要があります。

以下の表は、UNIX および Linux アダプターがサポートしている、UNIX および Linux システムのバージョンのリストです。

表 7. UNIX および Linux アダプターを実行するための前提条件

オペレーティング・システム	**バージョン**
AIX	AIX 6.1、 AIX 7.1
HP-UX	HP-UX 11iv1、HP-UX 11iv1 トラステッド、HP-UX 11iv2、HP-UX 11iv2 トラステッド、HP-UX 11iv3、HP-UX 11iv3 トラステッド
Red Hat Linux	Red Hat Enterprise Linux Enterprise Server 6.0、Red Hat Enterprise Linux Enterprise Server 6.1、Red Hat Enterprise Linux Enterprise Server 6.2
Oracle Solaris	Oracle Solaris 10
SUSE Linux	SLES 10.0, SLES 11.0

LDAP アダプターによってサポートされる、以下のディレクトリー・サーバー・バージョン

- IBM Tivoli Directory Server 6.1、IBM Tivoli Directory Server 6.2、IBM Tivoli Directory Server 6.3
- Sun Directory Server Enterprise Edition 6.3、Sun Directory Server Enterprise Edition 6.3.1

LDAP アダプターは、RFC 2798 スキームを使用する LDAP ディレクトリーをサポートします。このスキームは、IBM Security Identity Manager と IBM Tivoli Directory Server または Sun Directory Server Enterprise Edition を実行するシステム

との間の通信をサポートします。「*IBM Security Identity Manager LDAP アダプターインストールと構成のガイド*」に LDAP アダプターの構成方法が記載されています。

アダプターは、以下の IBM パスポート・アドバンテージ Web サイトで入手できます。

http://www.ibm.com/software/sw-lotus/services/cwepassport.nsf/wdocs/passporthome

アダプターのインストール・ガイドおよび構成ガイドは、IBM Security Identity Manager インフォメーション・センターの Web サイトで見つけることができます。

第 3 章 このリリースの新機能

IBM Security Identity Manager バージョン 6.0は、特権 ID 管理をサポートするための新しいインフラストラクチャー、プロセス、およびコントロールを備えています。また、運用上の役割管理、および他の識別管理およびアクセス管理ソリューションとの統合のための、拡張サポートも提供します。

新規機能の詳しい説明については、本章のトピックを参照してください。

アカウントの所有権タイプ

新しいアカウントの所有権タイプでは、個人アカウントと保護アカウントが分離されました。

個人使用のためのユーザー ID を表すアカウントは、個人アカウントです。それ以外のアカウントはすべてスポンサー付きアカウントです。スポンサー付きアカウントの例としては、UNIX システムにおける root アカウント、アプリケーション・アカウントおよびデバイス・アカウントがあります。スポンサー付きアカウントの所有者は、一般にそのアカウントを構成し、パスワードのリセットなどのメンテナンス・タスクを実行します。

パスワード同期は、個人アカウントのみに適用されます。プロビジョニング・ポリシーにおけるアカウント資格の指定は、アカウント・タイプによって異なります。

所有権のタイプは、パスワード管理プロセスとプロビジョニング・ポリシー評価に影響します。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のみが同期されます。プロビジョニング・ポリシーでは、特定のサービスの資格は、そのサービスの特定の所有権タイプに基づいています。

アカウント管理タスクの実行時に、アカウントを所有権タイプでフィルターに掛けることができます。所有権タイプは、アカウント要求タスクおよびアカウント採用タスクを完了させるときに指定できます。

「*IBM Security Identity Manager 構成ガイド*」の『所有権タイプ管理』

共有アクセス・モジュール

IBM Security Identity Manager の新しい共有アクセス・モジュールは、特権 ID 管理をサポートすることで ID およびアクセス管理ガバナンス機能を拡張します。

共有アクセス・モジュール は IBM の新製品 IBM Security Privileged Identity Manager で使用されます。IBM Security Privileged Identity Manager を購入すると、IBM Security Identity Manager 共有アクセス・モジュールを使用するためのライセンスを入手します。その後、IBM Security Identity Manager のインストール時にオプションの共有アクセス・モジュール・コンポーネントをインストールできます。

共有アクセス・モジュールの特権 ID 管理のサポートには以下のものがあります。

- 特権共有アカウント ID の管理、セキュア・アクセス、および保管の中央化。また、新規の管理機能により、共有アカウントの役割ベースでのアクセス・コントロールもサポートされます。
- アカウントの所有権タイプ。これにより、個々の所有アカウントと各種スポンサー付きアカウントが区別されます。所有権タイプに基づいてアカウント、パスワード、および資格を管理できます。
- 共有アカウントのライフサイクル管理。この管理には、役割ベースのアクセス要求、および共有 ID に関する特権アクセスの承認および確認が含まれます。
- アカウンタビリティーおよびコンプライアンスをモニターするための共有アカウント・アクティビティーの監査。
- 共有 ID および特権 ID の自動チェックインおよびチェックアウトを使用したシングル・サインオン。

  チェックアウトおよびチェックインの自動化は、IBM Security Identity Manager が IBM Security Privileged Identity Manager 製品ソリューションの一部としてデプロイされている場合に行われます。

詳しくは、以下を参照してください。

- 27 ページの『共有アクセス』
- IBM Security Privileged Identity Manager インフォメーション・センター。

役割管理

役割管理に、拡張された役割属性および役割の割り当て属性の管理が含まれるようになりました。

拡張役割属性

IBM Security Identity Manager 管理者は、役割の作成時または変更時に拡張役割属性を定義、設定、および変更することができます。これらのアクションは、役割カスタマイズのためにフォーム・デザイナーで導入された新規フォーム・テンプレートを使用して行うことができます。 拡張役割属性は、静的役割と動的役割の両方でサポートされます。

注: 拡張役割属性を使用するには、その前に、役割定義スキーマを拡張して LDAP で拡張役割属性を設定する必要があります。

LDAP で拡張役割属性を追加した後で、フォーム・デザイナーを使用して、IBM Security Identity Manager 管理コンソールでその役割のためのフォーム・テンプレートをカスタマイズし、保存してください。

拡張役割属性について詳しくは、IBM Security Identity Manager 技術情報を参照してください。

役割の割り当て属性

役割管理コンポーネントが拡張されて、役割の割り当て属性 (これらの属性は個人と役割の関係に関連付けられています) を定義する機能が含まれるようになりました。割り当て属性をサポートするのは、静的役割のみです。割り当て属性のストリング・タイプとテキスト・ウィジェットのみがサポートされています。

オプションの役割の割り当て属性タスクには以下のものがあります。

- 静的役割の作成または変更時における役割の割り当て属性の定義。
- カスタム・ラベルとそれぞれの割り当て属性との関連付け。
- ユーザー・メンバーを役割に追加する際の割り当て属性値の指定。
- その役割の既存のユーザー・メンバーへの割り当て属性値の指定。

役割の割り当て属性に関する ACI 機能

デフォルトおよび新規の ACI は、ともに、役割定義における他の属性と同様に、役割の割り当て属性に関する属性レベルの権限をサポートします。 ACI を変更または作成できるようになりました。役割定義におけるこれらの役割割り当て属性の使用を認可または拒否するための属性レベルの権限を設定できます。権限があるユーザーのみが、割り当て属性の読み取りまたは書き込みを行えます。さらに、以下のことができます。

- ユーザーをその役割に追加する際に割り当て属性値の読み取りまたは書き込みを行うように ACI を設定する。
- 割り当て属性値を既存のユーザー・メンバーに設定する。

ACI は、その他のエンティティーの場合と同様に機能します。特定の役割の割り当て属性には ACI がありません。次の属性が使用可能です。

- `erRoleAssignmentKey` は、役割を対象とし、役割の役割割り当て属性と 1 つの属性を定義する権限を指定します。
- `erRoleAssignments` は個人を対象とし、割り当て属性の値を割り当てる権限を指定します。

役割に対して定義した割り当て属性に ACI を定義することはできません。

役割の割り当て属性に関する JavaScript 機能

JavaScript インターフェースでは役割の割り当て属性に関する以下の機能にアクセスできます。

- 役割スキーマの役割の割り当て属性。
- 役割メンバーシップにおけるユーザーの役割割り当て属性およびその値。

新規 JavaScript API には以下のものがあります。

- 個人
- 役割
- RoleAssignmentAttribute
- RoleAssignmentObject

詳しくは、「*IBM Security Identity Manager リファレンス・ガイド*」の参照ページを参照してください。

役割の割り当て属性とセルフ・サービス・コンソール

セルフ・サービス・コンソールでのユーザー・プロファイルの役割割り当て属性の追加と変更についての詳細は、IBM Security Identity Manager 技術情報を参照してください。

追加情報

役割の割り当て属性の詳細については、以下のトピックを参照してください。

表 8. 役割の割り当て属性に関する詳細情報

トピックのタイトル	IBM Security Identity Manager 資料
『役割の割り当て属性』	*管理ガイド*
『役割の割り当て属性テーブル』	*Database と Directory Server スキーマ・リファレンス*
『個人』	*リファレンス・ガイド*
『役割』	
『RoleAssignmentAttribute』	
『RoleAssignmentObject』	

サービスの管理およびプロビジョニング

サービスの管理およびプロビジョニングが、新規のアカウント・フォーム、拡張接続モード、新規のサービス状況情報、およびサービス・タグ付けをサポートするようになりました。

以下を参照してください。

- 『サービス・レベル・フォーム』
- 15 ページの『サービス接続モード』
- 15 ページの『サービス状況と障害時再試行』
- 16 ページの『サービス・タグ付け』

サービス・レベル・フォーム

特定のサービス・タイプのサービス・インスタンスごとに異なるアカウント・フォームを指定できます。

サービスのアカウント・フォームはコンソールで定義することができます。例えば、Windows ローカル・アカウント・フォームなどのフォームを、アカウント・タイプ用にカスタマイズすることができます。この機能では、特定のサービス・タイプのサービス・インスタンスごとに異なるアカウント・フォームを指定できます。この機能により、特定タイプの各サービス・インスタンスに同じフォームを使用する必要があるという制約が削除されます。

新規フォームを使用して、新しいアカウントを要求したり、既存のアカウントを変更したりできます。プロビジョニング・ポリシー・パラメーター用の新規フォームも使用できます。サービス向けにカスタマイズされたアカウント・フォームがあり、プロビジョニング・ポリシーでそのサービスのサービス固有資格情報を選択すると、カスタマイズした属性に固有のウィジェットが表示されます。

また、この新規フォームを使用して、管理コンソールまたはセルフ・サービス・コンソールでアカウントの作成または変更を繰り返すこともできます。

「*IBM Security Identity Manager 構成ガイド*」の『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』を参照してください。

サービス接続モード

このリリースでは、接続モードのための新規サービス・フォーム属性が導入されました。自動化されたサービスまたは手動サービスのように機能することのできるサービスを作成するには、この属性を使用してください。

手動 または*自動* というサービス接続モードを指定できるようになりました。接続モードの設定により、アカウント管理に関する IBM Security Identity Manager の動作が規定され、さまざまな接続モードとエンドポイントの間の遷移に必要な構成が最小化されます。

接続モードの新規属性は erconnectionmode です。この属性を使用すると、管理対象リソース用のアダプターをインストールする前に、サービスを作成したり手動アカウント要求経路を指定したりすることができます。接続モードを使用すると、手動サービスを作成したり、後でそれを削除したりする必要がなくなります。アダプターをインストールした後でサービスを変更して、管理対象リソースがアカウント要求を処理するようにできます。このサービスの変更タスクを使用して接続モードを手動から自動に変更することができます。

サービス・タイプを自動に変更すると、そのサービス・タイプのすべてのサービスについて、それがデフォルト設定になります。

ITIM サービス上、または任意のタイプの ID フィード・サービス、ホスト・サービス、あるいは手動サービス・タイプでは、接続モードがサポートされていません。それらのサービス・タイプ用のフォームには erconnectionmode 属性を追加しないでください。

「*IBM Security Identity Manager 管理ガイド*」の『サービス管理』の章にある以下のトピックを参照してください。

- 『接続モードの使用可能化』
- 『手動接続モードを備えたサービスの作成』
- 『接続モードの手動から自動への変更』

サービス状況と障害時再試行

IBM Security Identity Manager 管理コンソールが拡張されて、各サービスの状況情報の表示、特定の状況になっているサービスの検索、およびブロックされた要求を再試行するオプションの提供が行われるようになりました。

サービス状況で示される値は、IBM Security Identity Manager サーバーの、アクションをプロビジョニングするサービスに関して管理対象リソースに問い合わせる能力を反映しています。ユーザー・インターフェースを使用して、特定の状況値になっているサービスを検索することもできます。この値を使用して、失敗したサービスまたは障害からの復旧が行われているサービスを見つけることができます。

このリリースでは、ブロックされた要求を「サービスの管理」パネルからただちに再試行するために使用できる、「**ブロックされた要求の再試行**」という新規アクションが提供されています。このアクションでは、問題が修正されたかどうかを調べ

るために、サービスがテストされます。テストに成功すると、失敗したサービスに関して、ブロックされた要求の再試行が行われます。

詳しくは、「*IBM Security Identity Manager 管理ガイド*」のトピック『サービス状況』を参照してください。

サービス・タグ付け

サービス・フォーム内で、サービスについて複数のタグを定義することができます。

サービス・タグを使用して、サービス・タイプに関するプロビジョニング・ポリシー資格を微調整できます。タグが一致するサービスについてのみその資格を適用できるように指定できます。

管理コンソールで、あるサービスのすべてのアカウントで新規アカウントおよびポリシー実行の自動プロビジョニングをトリガーすることができます。「サービスの管理」コンソールのエントリー・ポイントを使用し、「検索」を選択し、サービスのツイスティーを開いて、**「ポリシーの実行」**をクリックしてください。

「*IBM Security Identity Manager 管理ガイド*」の『サービス管理』の章にあるトピック『サービス・タグ付け』を参照してください。

アカウントおよびアクセスの管理

IBM Security Identity Manager では、複数のアクセス・レベルをサポートするため、およびセルフ・サービス・コンソールでのアカウント検索をサポートするために、アカウントおよびアクセスの管理が拡張されています。

以下を参照してください。

- 『複数レベルのアクセス・タイプ』
- 17 ページの『セルフ・サービス・コンソールでのアカウント検索』

複数レベルのアクセス・タイプ

IBM Security Identity Manager は、リンクされた一連のノードを使用して階層ツリー構造をシミュレートする、複数レベルのアクセス・タイプをサポートします。

階層によってアクセス・レベルが表されます。アクセス・タイプは、親子アクセス・タイプの形で分類されます。この構成は、大規模なデプロイメントの管理で役に立ちます。

管理者は以下のアクションを実行できます。

- 階層ツリー構造でアクセス・タイプを管理する。
- アクセス要求時に、ツリー構造を使用してカテゴリー別にアクセス・タイプを検索する。
- グループまたは役割と関連付けるために任意のレベルのアクセス・タイプを指定する。
- 組織のアクセス・タイプを、階層ツリー構造のシステム定義アクセス・タイプに変換する。

- 組織内の複数のアクセス・タイプを、特定のアクセス・カテゴリーに分類する。たとえば、すべての金融アプリケーションへのアクセスは「**アプリケーション**」 > 「**金融**」の下位に分類できます。

ユーザーは、アクセス・タイプに基づいてアクセスを探索、フィルター操作、または要求することができます。

「*IBM Security Identity Manager 構成ガイド*」のトピック『アクセス・タイプの管理』、および「*IBM Security Identity Manager 管理ガイド*」のトピック『役割に基づいたアクセス・タイプの作成』。

セルフ・サービス・コンソールでのアカウント検索

セルフ・サービス・コンソールでアカウント検索機能を使用できるようになりました。

セルフ・サービス・コンソールで以下の機能を使用しているときに、アカウントを検索できるようになりました。

- アカウントの表示または変更
- アカウントの削除
- パスワードの変更

アカウント検索は、所有権タイプ、アカウント ID、サービス・タイプ (アカウント・プロファイル)、サービス (アカウント・タイプ)、または組織のコンテナーに基づいて行うことができます。

WebSphere を使用して構成された外部ユーザー・レジストリーでの認証

IBM Security Identity Manager 認証メカニズムが、WebSphere Application Server のコンテナー・ベースのセキュリティー機能と統合されました。

IBM Security Identity Manager ユーザーは、WebSphere Application Server ユーザー・レジストリーに対して認証を行ってから、IBM Security Identity Manager ユーザーにマップされることが可能になります。

ログイン・サポートには以下のものが含まれます。

- パスワードを忘れた場合 (ユーザー確認の質問への回答)
- パスワード有効期限
- 最大ログオン試行回数によるアカウントのサスペンド

外部ユーザー・レジストリーは、IBM Security Identity Manager を最初にインストールするときに使用することができます。あるいは、カスタム・レジストリーを使用してIBM Security Identity Manager をインストールしてから、後で外部ユーザー・レジストリーを使用するように再構成することもできます。

外部ユーザー・レジストリーを使用するためには、WebSphere セキュリティー・ドメインを構成する必要があります。IBM Security Identity Manager には、外部ユーザー・レジストリーの構成方法を示すサンプル構成の資料があります。このサンプル資料は、製品配布の `extensions` ディレクトリーにあります。IBM Security Identity Manager を最初にインストールするときに外部ユーザー・レジストリーを使

用するには、インストールの前に構成手順を実行する必要があります。 IBM Security Identity Manager のインストール後に外部ユーザー・レジストリーを構成するためには、デフォルトのカスタム・ユーザー・レジストリーを使用してインストールを完了してから、外部ユーザー・レジストリーを手動で構成する必要があります。

詳しくは、「*IBM Security Identity Manager Security Guide*」のトピック『Using an external user registry for authentication』を参照してください。

垂直クラスター・サポート

垂直クラスターを使用する WebSphere デプロイメントに IBM Security Identity Manager をインストールできるようになりました。

垂直クラスターでは、同一ノード、または物理マシン上にクラスター・メンバーがあります。水平クラスターでは、セル内の多数のマシンにある複数のノードにクラスター・メンバーがあります。IBM Security Identity Manager を水平および垂直の両方のクラスター・トポロジーにインストールできるようになりました。

詳しくは、「*IBM Security Identity Manager インストール・ガイド*」の以下のトピックを参照してください。

- 『クラスター構成』
- 『IBM Security Identity Manager アプリケーション用の WebSphere クラスターの作成』

アプリケーション・プログラミング・インターフェース

IBM Security Identity Manager は、追加のアプリケーション・プログラミング・インターフェースをサポートします。

新規に追加された機能には、Web サービス API、再認証ポリシーを管理するための新規 API、および JavaScript で使用するための新規ロギング API などがあります。

以下を参照してください。

- 『Web サービス API』
- 19 ページの『再認証ポリシー API に対する拡張』
- 19 ページの『カスタム JavaScript で使用するための拡張ロギング API』

Web サービス API

IBM Security Identity Manager Web サービス・ラッパーは、IBM Security Identity Manager サーバーへの軽量の通信チャネルを提供します。

Web サービス API を使用して、ユーザー機能をご使用のカスタム・ビルド・アプリケーションに追加できます。

Web Services クライアントは、IBM Security Identity Manager または WebSphere Application Server がインストールされていなくても使用できます。

詳しくは、「*IBM Security Identity Manager リファレンス・ガイド*」のトピック『Web サービス API』を参照してください。

再認証ポリシー API に対する拡張

IBM Security Identity Manager は、ユーザーに付与された資格の再確認を自動化するために再認証ポリシーを使用します。

新規 API を導入することにより、リモート・アプリケーションから IBM Security Identity Manager の再認証ポリシーを検索、追加、変更、削除、および実行できるようになります。

再認証ポリシー API は一連の Java クラスからなります。これらのクラスは再認証ポリシー・ターゲット、参加者、再認証アクション、およびポリシー・スケジュールなどの、一般的に使用される再認証ポリシーの概念を要約したものです。

詳しくは、以下を参照してください。

- 「*IBM Security Identity Manager リファレンス・ガイド*」の『再認証ポリシー API』
- 「*IBM Security Identity Manager 管理ガイド*」の『再認証ポリシー』

カスタム JavaScript で使用するための拡張ロギング API

拡張ロギング API の導入によって、カスタム JavaScript 拡張機能で使用するための新規メソッドが提供されています。

新規メソッドにより、以下のように IBM Security Identity Manager の柔軟性が向上しました。

- メッセージを選択的に IBM Security Identity Manager のトレース・ログまたはメッセージ・ログに記録する機能。
- `msg.log` の場合の `ERROR`、`WARN`、または `INFO`、および `trace.log` の場合の `DEBUG_MIN`、`DEBUG_MID`、または `DEBUG_MAX` のような、指定された重大度のメッセージを記録する機能。
- `enRoleLogging.properties` ファイルでコンポーネント・ロギング・レベルを指定することにより、ログ・ファイルにどのようなメッセージが書き込まれるのかをランタイム構成する機能。

IBM Security Identity Manager バージョン 6.0 リリースより前には、JavaScript で提供されるロギング・オプションでは、`msg.log` に `ERROR` レベルでのみ書き込みを行うことができました。バージョン 6.0 の新規ロギング API を使用すると、さまざまなロギング・レベルでカスタム・ロギング・メッセージまたはカスタム・トレース・メッセージを定義できます。 また、記録されるステートメントをランタイム構成で制御することもできます。 ログ・ファイルまたはトレース・ファイルに書き込まれるログ・ステートメントは、`enRoleLogging.properties` ファイルでロギング・レベルを構成することによって制御されます。ロギング・レベル構成は、他のIBM Security Identity Manager コンポーネントと同じです。このファイル内のコンポーネントは、ユーザーによってログ・メソッドおよびトレース・メソッドで定義されます。この構成によって次の機能が提供されます。

- カスタム生成トレース・メッセージのきめ細かな制御。

- 生成されたログ・レコード内の *component* および *method* を調べることによって、どのカスタム JavaScript によってそのログ・メッセージまたはトレース・メッセージが生成されたのかがわかる柔軟性。

新規メソッドは、Enrole JavaScript 拡張機能に含まれます。

- msg.log に書き込む場合:
  - logInfo(String component, String method, String message)
  - logWarn(String component, String method, String message)
  - logError(String component, String method, String message)
- trace.log に書き込む場合:
  - traceMax(String component, String method, String message)
  - traceMid(String component, String method, String message)
  - traceMin(String component, String method, String message)

詳しくは、「*IBM Security Identity Manager* リファレンス・ガイド」の以下のトピックを参照してください。

- 『Enrole』
- 『enRoleLogging.properties』

レポート・データ同期化の機能強化

レポート・データ同期化が設計し直されて、パフォーマンスが向上し、新規ユーティリティーによってリモートデータ同期化機能が提供されるようになりました。

レポート・データ同期化では以下の機能が強化されています。

- 以下のエンティティー・タイプのデータ同期化のパフォーマンスを向上させるために再設計が行われました。
  - アカウント
  - 許可所有者
  - グループ
  - 組織のコンテナー
  - ユーザー
  - 役割
  - サービス

  以下のプロパティーについて詳しくは、*ISIM_HOME*/data/ReportDataSynchronization.properties ファイルを参照してください。
  - accountSynchronizationStrategy
  - authorizationOwnerSynchronizationStrategy
  - groupSynchronizationStrategy
  - organizationalContainerSynchronizationStrategy
  - personSynchronizationStrategy
  - roleSynchronizationStrategy
  - serviceSynchronizationStrategy

- IBM Security Identity Manager のレポート・データ同期化ユーティリティー。IBM Security Identity Manager 稼働環境外でレポート・データ同期化プロセスを実行するために使用できる、自己完結型ユーティリティー。

「*IBM Security Identity Manager 管理ガイド*」のトピック『データの同期化』を参照してください。

ヘルス・モニター

IBM Security Identity Manager サーバーが拡張されて、デプロイメント・ヘルス・モニター機能が備わるようになりました。これらの機能により、キー・コンポーネントにおけるパフォーマンスをモニターしたりさまざまな要求を使用したりできるようになりました。

プロビジョニング・コンポーネントとワークフロー・コンポーネントによりインスツルメンテーションが追加され、WebSphere Performance Monitoring Infrastructure (PMI) システム内のイベントが追跡されます。また、このサーバーには、IBM Tivoli Monitoring などのモニタリング製品との統合を行いやすくするための新規 API が含まれます。

詳しくは、「*IBM Security Identity Manager Performance Tuning Guide*」の『IBM Security Identity Manager deployment health monitoring』を参照してください。

第 4 章 既知の制限、問題、および回避策

ソフトウェアの既知の制限、問題、および回避策を IBM Security Identity Manager サポート・サイトで確認できます。

サポート・サイトでは、製品のリリース時点で存在した問題と制限、および製品リリース後に判明したすべての項目が説明されています。制限および問題が発見され解決されると、IBM ソフトウェア・サポート・チームがオンラインの知識ベースを更新します。知識ベースを検索することで、発生した問題の解決策または回避策を確認できます。

以下のリンクから、バージョン 6.0 固有の項目用の有効なライブ・ナレッジ・ベースのカスタマイズされたクエリーを起動できます。

IBM Security Identity Manager バージョン 6.0 技術情報

独自のクエリーを作成するには、IBM ソフトウェア・サポート Web サイトの拡張検索ページに移動します。

第 5 章 各機能の概要

IBM Security Identity Manager では、インストール、デプロイ、および管理の容易なソリューションで、簡易化された識別管理機能が提供されます。

IBM Security Identity Manager は、不可欠なパスワード管理、ユーザーのプロビジョニング、および監査の各機能を提供します。

アクセス管理

セキュリティー・ライフサイクルでは、IBM Security Identity Managerおよび他のいくつかの製品がアクセス管理を行います。保護されているご使用のシステムに誰が入れるのかを決めることができます。ユーザーが何にアクセスできるかを決定し、ユーザーのアクセスを、ビジネス・タスクで必要とするもののみに制限することもできます。

アクセス管理は、ビジネスの視点から見た次の 3 つの問題に対処します。

- どのユーザーがシステムに入ることができるようにするか。
- ユーザーが何を実行できるようにするか。
- ユーザーがそのアクセス権限で行ったことを簡単に確認できるか。

これらの製品は、リソースへアクセスするすべてのユーザーの信頼性を検証し、以下のように、アクセス・コントロールが適切に一貫して実行されるようにします。

- IBM Security Identity Manager

  安全で自動化されたポリシー・ベースのユーザー管理ソリューションを提供します。このユーザー管理ソリューションによって、ライフサイクル全体にわたり、レガシー環境および e-ビジネス環境の両方においてユーザー ID を効率的に管理できます。 IBM Security Identity Manager は、ユーザー・リソース・アクセスに関連する操作を簡素化するポリシーおよび機能を使用して、組織内のさまざまなリソースへのユーザー・アクセスを集中制御します。この結果、組織には以下を含む数多くの利益がもたらされます。

  – Web セルフ・サービス、およびパスワードのリセットと同期化。ユーザーは、複数のアプリケーションへのアクセスを管理するためのパスワード管理ポリシーのルールを使用して、自分のパスワードを自分で管理することができます。パスワード同期化により、ユーザーは IBM Security Identity Manager が管理するすべてのアカウントに単一のパスワードを使用できます。
  – 監査および規制委任に対する即時応答
  – ライフサイクル管理の提供による、ユーザー ID の変更に関連するビジネス・プロセスの自動化
  – 集中制御とローカル側の自律
  – 拡張 API の使用との統合強化
  – エージェントありのアプローチまたはエージェントなしのアプローチを選択してターゲット・システムを管理

- ヘルプ・デスクのコスト削減
- 孤立アカウントの削減による、アクセス・セキュリティーの向上
- ソフトウェアの自動化を使用したユーザーのプロビジョニングによる管理コストの削減
- 新規および変更済みのユーザーに対するリソース・アクセスの承認に関連したコストおよび遅延の削減

• IBM Security Access Manager

  組織が、指定されたユーザー・グループに対して集中型のセキュリティー・ポリシーを使用して、インターネットに直接さらされているぜい弱な Web サーバーを含むネットワーク全体にわたるアクセス許可を管理できるようにします。 IBM Security Access Manager は、IBM Security Identity Manager と密結合することにより、IBM Security Access Manager によって管理されるユーザー・グループおよびアカウントを IBM Security Identity Manager で管理される ID と調整することができます。これにより、リソース・アクセス・コントロールの統合化ソリューションを提供します。

  IBM Security Access Manager は以下を提供します。

  - 企業内の各所にあるさまざまな Web ベースのアプリケーションに対する、統合された承認および認証アクセス
  - Web 環境、Microsoft 環境、Telnet 環境、およびメインフレーム・アプリケーション環境への柔軟なシングル・サインオン (SSO)
  - Java 2 Enterprise Edition (J2EE) アプリケーションの標準ベースのサポートによる、迅速およびスケーラブルな Web アプリケーションのデプロイメント
  - 非常にスケーラブルなプロキシー・アーキテクチャー、簡単にインストールできる Web サーバー・プラグイン、ルール・ベースおよび役割ベースのアクセス・コントロール、主要なユーザー・レジストリーおよびプラットフォームのサポート、およびセキュリティーをカスタマイズするための拡張 API による設計の柔軟性

• IBM Security Federated Identity Manager

  パートナー・リレーションシップ、ID マッピング、ID トークン管理など、組織境界を越えてフェデレーションに関するすべての構成情報を処理します。

  IBM Security Federated Identity Manager は、組織がビジネス・パートナー組織とサービスを共有し、顧客、サプライヤー、および顧客の従業員などの第三者の ID に関する信頼できる情報を獲得できるようにします。組織が使用するサービスへのアクセス権を提供する他の組織側で ID アカウントの作成、登録、または管理を行わずに、ユーザー情報を取得できます。このため、ユーザーはパートナー・サイトで登録したり、追加のログインやパスワードを覚えておく必要性から解放されます。この結果、組織とそのサプライヤー、ビジネス・パートナー、および顧客との統合およびコミュニケーションが向上します。

セキュリティー・ライフサイクルのより大規模なソリューションにアクセス管理製品がどのように適応するかについて詳しくは、IBM Security Management の Web サイト (http://www.ibm.com/software/tivoli/solutions/security/) を参照してください。

IBM Redbooks® および Redpapers も、IBM セキュリティー製品のポートフォリオ内の IBM Security Identity Managerのインプリメントについて説明しています。

共有アクセス

IBM Security Identity Manager は共有アクセス・モジュールを提供し、共有アクセスをサポートします。

IBM 特権 ID 管理ソリューションを使用するには、共有アクセス・モジュールをインストールして使用する必要があります。共有アクセス・モジュールは IBM Security Privileged Identity Manager 製品の一部としてライセンスされています。IBM Security Privileged Identity Manager を購入すると、IBM Security Identity Manager 共有アクセス・モジュールを使用するためのライセンスを入手します。

共有アクセス・モジュールにより、IBM Security Identity Manager でのアカウント・プロビジョニングのサポートと、識別およびガバナンスのフレームワークが拡張されます。

ハイライト

- アカウント・プロビジョニング・フレームワークにより、特権ユーザーのアカウントとパスワードを中央で管理できます。
- 共有アクセスでは、クレデンシャル・ボールト・サーバーのアカウント資格情報が安全にチェックイン、チェックアウト、およびログ記録されます。
- 共有資格情報アクセスの管理コントロールにより、個別のアカウント指定が可能になりました。
- Java API および Web サービス API により、アプリケーション・クライアントが共有資格情報にプログラムでアクセスできます。
- 共有資格情報アクセスおよび共有アカウント所有権に関する役割ベースのアクセス・コントロールがあります。
- 特権 ID のライフサイクル管理があります。これらのタスクには、アカウント要求の管理と、アカウント所有権、役割ベースのアクセス要求、および共有資格情報アクセスの承認および再確認が含まれます。
- 管理アクティビティーおよび共有資格情報アクセス・アクティビティーのエンドツーエンドの監査があります。
- 共有資格情報管理および手動でのチェックアウトとチェックインのための Web アプリケーションがあります。

共有アクセスに関する資料

共有アクセスに関する資料は、共有アクセス・モジュールのインストール、構成、管理、およびトラブルシューティングについて説明するトピックで構成されています。また、この資料では共有プログラミング API、データベース・スキーマ、ディレクトリー・サーバー・スキーマ、およびユーザー・シナリオについても説明します。

機能

表 9. 共有アクセス機能

説明	資料へのリンク
共有アクセス・モジュールの機能	27 ページの『共有アクセス』
管理対象リソース用の共有アクセスをデプロイするためのロードマップ	30 ページの『管理対象リソース用の共有アクセスを構成するためのロードマップ』
特権管理者ビューとデフォルト・アクセス・コントロール項目	「*IBM Security Identity Manager 計画*」のトピック『特権管理者グループの有効範囲』を参照してください。
特権ユーザー・ビューとデフォルト・アクセス・コントロール項目	「*IBM Security Identity Manager 計画*」のトピック『特権ユーザー・グループの有効範囲』を参照してください。

インストールおよびアップグレード

表 10. インストールおよびアップグレード

説明	「*IBM Security Identity Manager インストール・ガイド*」の以下のトピックを参照してください。
共有アクセス・モジュールのインストール	『共有アクセス・モジュールの構成』
アップグレード時の WebSphere シングル・サーバーでの共有アクセス・モジュールの追加	『アップグレード時の WebSphere シングル・サーバーでの共有アクセス・モジュールの構成』
アップグレード時の WebSphere クラスター上での共有アクセス・モジュールの追加	『アップグレード時の WebSphere クラスター上での共有アクセス・モジュールの構成』
データベースまたはディレクトリー・サーバーの再構成後の共有アクセス・モジュールの更新	『共有アクセス・モジュールの再構成』

システム構成

表 11. システム構成

説明	「*IBM Security Identity Manager 構成ガイド*」の以下のトピックを参照してください。
共有アクセス構成 (外部クレデンシャル・ボールト・サーバーの構成を含む)	『共有アクセス構成』
共有アクセスの拡張構成 (操作のカスタマイズを含む)	『共有アクセスの拡張構成 』
Tivoli Common Reporting の共有アクセス・レポート	• 『共有アクセス監査履歴レポート』 • 『所有者に基づいた共有アクセス資格』 • 『役割に基づいた共有アクセス資格』

管理

表 12. 共有アクセス管理

説明	「*IBM Security Identity Manager 管理ガイド*」の**以下のトピックを参照してください。**
共有アクセス管理 • クレデンシャル・ボールトの管理。資格情報の追加、変更、除去、およびチェックインが含まれます。また、資格情報設定の変更、資格情報パスワードの登録、およびパスワード履歴の表示についても説明します。 • 資格情報プールの作成、変更、および削除 • 共有アクセス・ポリシーの作成、変更、および削除 • 共有アクセス・バルク・ロード	『共有アクセス管理』
共有アクセス・モジュールのデフォルト・アクセス・コントロール項目	『デフォルト・アクセス・コントロール項目』
レポート作成 • レポートのカスタマイズに使用できる共有アクセス・オブジェクト • 例: – チェックアウトされたすべての共有アクセス資格情報を表示するカスタム・レポートの作成 – チェックイン監査レポートの作成 – 役割および共有アクセス資格レポートの作成	『カスタム・レポートの共有アクセス・オブジェクト』

データ参照

表 13. データ参照

説明	「*IBM Security Identity Manager Database and Directory Server Schema リファレンス・ガイド*」**の以下のトピックを参照してください。**
共有アクセス・データベース・テーブルのリファレンス	『データベース・テーブルのリファレンス』セクションの『共有アクセス・テーブル』
IBM Tivoli Directory Server スキーマおよびクラスのリファレンスの共有アクセス・クラス	『IBM Tivoli Directory Server スキーマおよびクラスのリファレンス』セクションの『共有アクセス・クラス』
共有アクセス・ポリシー管理の監査スキーマ	『監査スキーマ・テーブル』セクションの以下の項目を参照してください。 • 『共有アクセス・ポリシー管理』 • 『資格情報のリース管理』 • 『資格情報のプール管理』 • 『資格情報の管理』

トラブルシューティング

表 14. 共有アクセスのトラブルシューティング

説明	以下のトピックを参照してください。
トラブルシューティング • LDAP スキーマまたはデータベース・テーブルの更新時には共有アクセス構成を更新する必要があります。 • プロパティー・ファイルの構成が誤っていることが原因で、クレデンシャル・ボールトへの資格情報の追加要求が失敗することがあります。 • 資格情報属性の構成が誤っていることが原因で、ユーザーが共有資格情報にアクセスできないことがあります。	「*IBM Security Identity Manager* トラブル・シューティング・ガイド」の『共有アクセス・モジュールの問題のトラブルシューティング』

アプリケーション・プログラミング・インターフェース

表 15. 共有アクセス・アプリケーション・プログラミング・インターフェース

説明	「*IBM Security Identity Manager* リファレンス・ガイド」の以下のトピックを参照してください。
共有アクセス・アプリケーション API	『共有アクセス・アプリケーション API』
共有アクセス Web サービス API	『共有アクセス Web サービス API』
共有アクセス許可拡張 API	『共有アクセス許可拡張 API』
共有アクセス JavaScript API	『CredentialModelExtension』

共有アクセスのユーザー・シナリオ

表 16. ユーザーの共有アクセス

説明	「*IBM Security Identity Manager* シナリオ」の以下のトピックを参照してください。
資格情報または資格情報プールのチェックアウトのユーザー・シナリオ	『資格情報または資格情報プールのチェックアウト』
共有の資格情報のパスワードの表示のユーザー・シナリオ	『共有の資格情報のパスワードの表示』
特権ユーザー・ビューとデフォルト・アクセス・コントロール項目	『特権ユーザー・グループの有効範囲』

管理対象リソース用の共有アクセスを構成するためのロードマップ

このロードマップは、IBM Security Privileged Identity Manager 内で新規の管理対象リソースの共有アクセスを構成するための高水準ステップを示しています。

IBM Security Privileged Identity Manager 製品ソリューションには、共有アクセス・モジュールにより実現する IBM Security Identity Manager 共有アクセス機能が組み

込まれています。IBM Security Privileged Identity Manager には、IBM Security Access Manager for Enterprise Single Sign-on での共有資格情報の自動チェックアウトおよびチェックインのサポートも含まれています。このロードマップでは、共有資格情報の自動チェックアウトおよびチェックインもサポートされているデプロイメントで共有アクセスを構成する方法を説明します。

前提条件

要件	インストール手順
共有アクセス・モジュール を IBM Security Identity Manager サーバーにインストールする。	「*IBM Security Identity Manager インストール・ガイド*」の『共有アクセス・モジュールの構成』を参照してください。
資格情報のチェックインとチェックアウトを自動化する必要があるクライアント・コンピューターに AccessAgent コンポーネントを、インストールする。	IBM Security Privileged Identity Manager Information Center Information の「*IBM Security Privileged Identity Manager Deployment Guide*」を参照してください。

管理対象リソース用の共有アクセスを構成するためのフローチャート

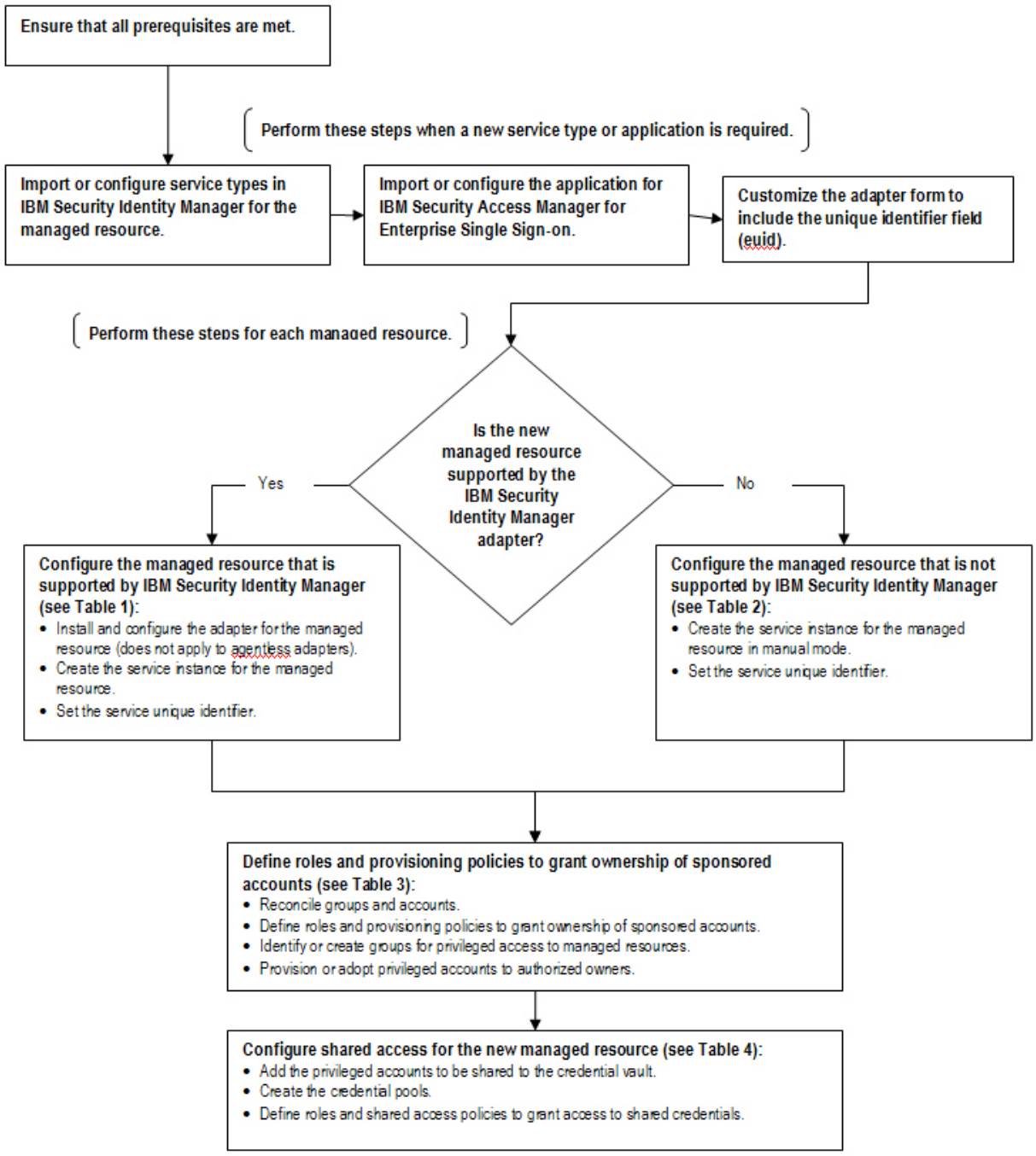

図 1. 管理対象リソース用の共有アクセスを構成するためのフローチャート

管理対象リソースのためのサービス・タイプを IBM Security Identity Manager 内にインポートまたは構成する

リソース・タイプごとに、サービス・タイプをインポートするか手動サービス用のサービス・タイプを作成するかして、IBM Security Identity Manager 内でプロファイル情報を構成する必要があります。

サービス・タイプのインポートについては、IBM Security Identity Manager インフォメーション・センターにある「*構成*」の『サービス・タイプのインポート』を参照してください。

手動サービス・タイプの作成については、IBM Security Identity Managerインフォメーション・センターにある「*構成*」の『サービス・タイプの作成』を参照してください。

固有 ID (eruri) フィールドを含めるためのサービス・フォーム・テンプレートのカスタマイズ

サービス・フォーム・テンプレートに固有 ID (eruri) フィールドを追加してください。

詳しくは、「*IBM Security Identity Manager 管理ガイド*」の『固有 ID (eruri) フィールドを含めるためのサービス・フォーム・テンプレートのカスタマイズ』を参照してください。

IBM Security Access Manager for Enterprise Single Sign-on用のアプリケーションのインポートまたは構成

IBM Security Access Manager for Enterprise Single Sign-on でサポートされる各アプリケーションについて、以下の手順を実行してください。

ステップ	参照情報
IMS™ Server で特権 ID ポリシーおよび AccessProfiles を準備します。	IBM Security Privileged Identity Manager インフォメーション・センターにある「*IBM Security Privileged Identity Manager Deployment Guide*」の『IMS サーバーでの特権 IP ポリシーと AccessProfiles の準備』

IBM Security Identity Manager での新規管理対象リソースの構成

注: システムに新規の管理対象リソースが含まれるたびに、以下の手順を実行する必要があります。

新規管理対象リソースは IBM Security Identity Manager アダプターによってサポートされますか?	参照情報
はい	表 17
いいえ	34 ページの表 18

表 17. IBM Security Identity Manager アダプターによってサポートされる管理対象リソースの構成

手順	参照情報
管理対象リソース用の IBM Security Identity Manager アダプターをインストールして構成する。 **注:** この手順はエージェントレス・アダプターには適用されません。	IBM Security Identity Manager インフォメーション・センターにあるアダプターの資料

表 17. IBM Security Identity Manager アダプターによってサポートされる管理対象リソースの構成 (続き)

手順	参照情報
管理対象リソース用の IBM Security Identity Manager サービス・インスタンスを作成する。	「*管理ガイド*」の『サービスの作成』
IBM Security Identity Manager の管理対象リソースサービス定義のサービス固有 ID を (管理コンソールを使用して) AccessAgent にある管理対象リソースへの接続に使用する固有 ID に設定する。例えば、この固有 ID は IP アドレス、またはサーバーのホスト名にすることができます。	「*管理ガイド*」の『サービス固有 ID の設定』

表 18. IBM Security Identity Manager アダプターによってサポートされない管理対象リソースの構成

手順	参照情報
手動サービス・タイプを使用して IBM Security Identity Manager サービス・インスタンスを作成する。	「*構成ガイド*」の『手動サービスおよびサービス・タイプ』 「*管理ガイド*」の『手動サービスの作成』
IBM Security Identity Manager の管理対象リソースサービス定義のサービス固有 ID を (管理コンソールを使用して) AccessAgent にある管理対象リソースへの接続に使用する固有 ID に設定する。例えば、この固有 ID は IP アドレス、またはサーバーのホスト名にすることができます。	「*管理ガイド*」の『サービス固有 ID の設定』

スポンサーの設定されたアカウントの所有権を付与するための役割およびプロビジョニング・ポリシーの定義

IBM Security Identity Manager で以下の作業を行ってください。

表 19. スポンサーの設定されたアカウントの所有権を付与するための役割およびプロビジョニング・ポリシーの定義

手順	「*管理ガイド*」**の以下のトピックを参照してください。**
グループおよびアカウントを調整する。	『調整スケジュールの管理』
スポンサーの設定されたアカウントの所有権を付与するために役割およびプロビジョニング・ポリシーを定義する。	『プロビジョニング・ポリシーの作成』 『役割の作成』 『役割の所有者の指定』
管理対象リソースに特権アクセスするためのグループを識別または作成する。	『グループの作成』 『グループに関連するアクセス権の定義』

表 19. スポンサーの設定されたアカウントの所有権を付与するための役割およびプロビジョニング・ポリシーの定義 (続き)

手順	**「*管理ガイド*」の以下のトピックを参照してください。**
権限がある所有者に特権アカウントをプロビジョンまたは採用する。共有アクセスに使用されるアカウントは、スポンサーの設定されたアカウントでなければなりません。アカウントの所有権タイプは、「個人」以外の任意のタイプにすることができます。	このサービスにアカウントが存在していない場合は、『サービスに関連するアカウントの要求』を参照してください。 このサービスにアカウントが存在している場合は、『ユーザーへのアカウントの割り当て』を参照してください。 スポンサーの設定されたアカウントに関する一般情報については、『アカウントの管理』を参照してください。

新規の管理対象リソース用の共有アクセスの構成

表 20. 新規の管理対象リソース用の共有アクセスの構成

手順	**「*管理ガイド*」の以下のトピックを参照してください。**
共有対象の特権アカウントをクレデンシャル・ボールトに追加する。資格情報 (ユーザー ID およびパスワード) をクレデンシャル・ボールトに保管することによって、スポンサーの設定された共有対象アカウントを指定します。これらの資格情報へのアクセスは、役割ベースの共有アクセス・ポリシーによって管理されます。	『ボールトへの資格情報の追加』
資格情報プールを (一般には、サービスのグループに基づいて) 作成する。この資格情報プールは、同じ特権アクセス権限が指定された共有資格情報を編成するために使用します。	『資格情報プールの作成』
共有資格情報へのアクセス権限を付与するために役割および共有アクセス・ポリシーを定義する。共有アクセス・ポリシーは、役割メンバーが資格情報または資格情報プールを共有することを許可します。	『共有アクセス・ポリシーの作成』

企業の規制準拠のサポート

IBM Security Identity Manager は企業の規制準拠のサポートを提供しています。

準拠領域

IBM Security Identity Manager は、以下の主要な領域で企業の規制準拠に対処します。

- プロビジョニングと承認ワークフロー・プロセス

- 監査証跡追跡
- *拡張* 準拠状況
- パスワード・ポリシーとパスワードの準拠
- アカウントおよびアクセス権限のプロビジョニング許可と実行
- 再認証ポリシーとプロセス
- レポート

プロビジョニングと承認ワークフロー・プロセス

IBM Security Identity Manager は、プロビジョニングおよびユーザー・アカウントのサポート、および各種リソースへのアクセスのサポートを提供します。IBM Security Identity Manager は、セキュリティー製品スイート内にインプリメントされ、リソースを権限のある個人のみに確実にプロビジョンするための主要な役割を担います。IBM Security Identity Manager は、情報処理方法の正確性および完全性を保護し、権限のあるユーザーに、情報および関連する資産へのアクセス権限を付与します。IBM Security Identity Manager は、従業員、ビジネス・パートナー、サプライヤーに対し、およびプラットフォーム、組織、および地理を越えて組織に関連するその他の対象に対し、サービス、アプリケーション、およびコントロールのプロビジョンを管理する統合ソフトウェア・ソリューションを提供します。 このプロビジョニング機能を使用して、システムへのユーザー・アクセス権限のセットアップおよび保守を制御すること、および管理対象リソースのアカウントの作成を制御することができます。

大まかに述べると、ID 管理ソリューションは、リソースをプロビジョンするプロセスを自動化および集中化します。このソリューションには、オペレーティング・システムやアプリケーション、組織内のユーザーまたは組織と提携しているユーザーなどが含まれます。組織の構造を変更することで、プロビジョニング・ポリシーおよび手順に対応できます。ただし、リソースのプロビジョニングのために使用される組織ツリーは、組織の管理上の構造を必ずしも反映しません。 すべてのレベルのアドミニストレーターは、標準化された手順を使用して、ユーザーの資格情報を管理できます。 一部のレベルの管理は、プロビジョニング管理ソリューションの幅に基づいて、削減または省略できます。 さらに、管理機能を各種の組織間で手動または自動で安全に分配できます。

承認プロセスは、アカウントおよびアクセス権限のプロビジョニング要求など、さまざまなタイプのプロビジョニング要求に関連付けることができます。 ライフサイクル操作もカスタマイズして承認プロセスに取り込むことができます。

プロビジョニングのモデル

IBM Security Identity Manager では、ビジネス・ニーズに基づき、*要求*ベース・モデル、*役割*ベース・モデル、またはハイブリッド・モデルのいずれかで、権限のあるユーザーに対しリソースをプロビジョンできます。

承認ワークフロー

アカウントおよびアクセス権の要求ワークフローは、アカウントおよびアクセス権のプロビジョニング中に開始されます。通常、アカウントおよびアクセス要求のワークフローを使用して、アカウントおよびアクセスのプロビジョニングの承認ワークフローを定義します。

アカウント要求ワークフローは、プロビジョニング・ポリシーが提供する資格を認可するかどうかを決定するために必要な判断ベースのプロセスを提供します。プロビジョニング・ポリシーにより提供される資格により、プロビジョニング・ポリシー・メンバーシップの一連のユーザーに適用するアカウント要求ワークフローが指定されます。 複数のプロビジョニング・ポリシーを、同じサービス・ターゲットの同じユーザーに対して適用することができます。また、プロビジョニング・ポリシーごとに異なるアカウント要求ワークフローが存在することもあります。そのユーザーに関するアカウント要求ワークフローは、プロビジョニング・ポリシーの優先順位に基づいて決定されます。プロビジョニング・ポリシーに関連するワークフローがなく、そのポリシーがアカウント資格を付与する場合、要求に関連するこの操作がただちに実行されます。 例えば、操作によりアカウントが追加される場合があります。

ただし、プロビジョニング・ポリシーに関連するワークフローがある場合、ポリシーにより資格が付与される前に、そのワークフローが実行されます。ワークフローが**承認済み**の結果を返すと、ポリシーにより資格が付与されます。 ワークフローが**否認済み**の結果を返すと、資格は付与されません。 例えば、ワークフローでマネージャーの承認が必要な場合があります。 その承認がサブミットされ、ワークフローが完了するまで、アカウントはプロビジョンされません。 ワークフローを設計する場合、プロビジョニング・ポリシーの意図と資格自体の目的を考慮する必要があります。

トラッキング

IBM Security Identity Manager は、ユーザーがアクセス権限を所有する方法および理由についての監査証跡情報を提供します。 要求に基づいて、IBM Security Identity Manager によって、企業全体にわたるリソースへのアクセス権限の付与、変更、および削除を実行するための処理が提供されます。この処理では、自動化されたレポートを使用した有効な監査証跡が提供されます。

アカウントの承認およびプロビジョニングなど、このプロセスに関連する手順は、要求の監査証跡に記録されます。対応する監査イベントが監査レポート用のデータベースに生成されます。アカウントとアクセス権限の変更、再認証、準拠違反の警告など、ユーザーとアカウントのライフサイクル管理イベントも監査証跡に記録されます。

拡張準拠状況

IBM Security Identity Manager は、休止アカウントおよび孤立アカウントなどの項目 の拡張準拠状況、プロビジョニング・ポリシーの準拠状況、再認証状況、および各種のレポートを提供します。

- **休止アカウント**。 レポート機能を使用して、休止アカウントのリストを表示できます。IBM Security Identity Manager では、サービスの未使用アカウントを検出および管理するために使用できる休止アカウント属性がサービス・タイプに組み込まれています。

- **孤立アカウント**。 Security Identity Manager サーバー で、管理対象リソースのアカウントの所有者を特定できない場合、そのアカウントは*孤立アカウント* です。これらのアカウントは、調整時に、適用可能な採用ルールではアカウントの所有者を正常に判別できない場合に識別されます。
- **プロビジョニング・ポリシー準拠状況**。 アカウントおよびアクセス権限の、プロビジョニング・ポリシーの仕様に基づく準拠状況を確認できます。 アカウントの準拠状況は、準拠、属性値の違反による非準拠、または却下のいずれかです。アクセス権限は、準拠または却下です。
- **再認証状況**。 ユーザー、アカウント、およびアクセス権限というターゲット・タイプの再認証状況を確認できます。これは、ターゲット・タイプが認証されたか、否認されたか、または認証されなかったかを示します。 再認証のタイム・スタンプも確認できます。

パスワード・ポリシーとパスワードの準拠

パスワード・ポリシーを作成および管理するには、IBM Security Identity Manager を使用します。*パスワード・ポリシー* は、新規パスワードが許容できるかどうか判定するのに使用されるパスワード・ストレングス規則を定義します。 *パスワード・ストレングス規則* とは、パスワードを準拠させる必要がある規則のことです。例えば、パスワード・ストレングス規則で、パスワードの最小文字数を 5 文字と指定することができます。パスワード・ストレングス規則で、パスワードの最大文字数を例えば 10 文字と指定することもできます。

IBM Security Identity Manager 管理者は、パスワード・ポリシーで使用する新しいルールも作成できます。

パスワード同期化が有効になっている場合、管理者は、パスワード・ポリシーに競合するパスワード・ストレングス規則が含まれないように注意する必要があります。 パスワード同期化を有効にすると、使用されるパスワードを判断するために、ユーザーが所有しているすべてのアカウント用のポリシーが IBM Security Identity Manager によって結合されます。 パスワード・ポリシー間に矛盾がある場合は、パスワードが設定されないことがあります。

プロビジョニング・ポリシーとポリシー実行

プロビジョニング・ポリシー は、IBM Security Identity Manager サーバー、Windows NT サーバー、Solaris サーバーなど、各種の管理対象リソースへのアクセス権を認可します。

システム・アドミニストレーターは、プロビジョニング・ポリシーのパラメーターを使用して、必須の属性値および許可される属性値を定義できます。

ポリシー実行 は、プロビジョニング・ポリシーに違反したアカウントを IBM Security Identity Manager が許可または却下する方法です。

非準拠の属性を持つアカウントに対し、以下のいずれかのポリシー実行アクションが実行されるように指定できます。

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。

再認証ポリシーとプロセス

再認証ポリシー には、指定されたターゲット・タイプ (ユーザー、アカウント、およびアクセス権限) に対する有効で継続的な必要性をユーザーが持っていることをユーザー自身が確認できるようにするアクティビティーが含まれます。 このポリシーでは、継続的な必要性をどのくらいの頻度でユーザーが検証する必要があるのかが定義されます。 また、受信者が再認証要求を拒否した場合やこれに応答しなかった場合に実行する操作もポリシーにより定義されます。 IBM Security Identity Manager は、一連の通知を使用して、再認証プロセスに関連するワークフロー・アクティビティーを開始する再認証ポリシーをサポートしています。 再認証ポリシーでは、ユーザーの応答に基づいて、ユーザーの役割、アカウント、グループ、またはアクセス権限を再認証済みとマークすることができます。このポリシーは、アカウントをサスペンドまたは削除すること、もしくは役割、グループ、またはアクセス権限を削除することができます。

再認証に関連する複数のレポートで使用するために、以下の再認証に固有の監査が作成されます。

アカウント、アクセス権限、またはユーザーの保留中の再認証
完了していない再認証のリストを提供します。

再認証ヒストリー
指定されたターゲット・タイプの再認証の履歴リストを提供します。

再認証ポリシー
すべての再認証ポリシーのリストを提供します。

ユーザー再認証ヒストリー
ユーザー再認証のヒストリーを提供します。

ユーザー再認証ポリシー
すべてのユーザー再認証ポリシーのリストを提供します。

レポート

組織内のセキュリティー・アドミニストレーター、監査員、マネージャー、およびサービス所有者は、以下の 1 つ以上のレポートを使用して、企業の規制準拠を管理およびサポートできます。

- アクセス・レポート。システムのアクセス権定義をすべてリストします。
- 承認および否認レポート。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。
- 休止アカウント・レポート。最近使用されていないアカウントをリストします。
- 個人に許可された資格レポート。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します。
- 非準拠アカウント・レポート。すべての非準拠アカウントをリストします。

- 孤立アカウント・レポート。所有者を持たないすべてのアカウントをリストします。
- 保留再認証レポート。再認証対象の個人がアカウントまたはアクセス許可に関するアクションを行わない場合に実行できる再認証イベントを強調表示します。このレポートは、特定のサービス・タイプまたは特定のサービス・インスタンスによるデータのフィルタリングをサポートしています。
- 再認証変更ヒストリー・レポート。アクセス権限 (アカウントを含む) のヒストリーと、それらが最後に再認証された日時を示します。このレポートは、過去の再認証の証拠として役立ちます。
- 再認証ポリシー・レポート。所定のアクセス権限またはサービスに対する現在の再認証の構成を示します。
- 職務分離ポリシー定義レポート。職務分離ポリシー定義をリストします。
- 職務分離ポリシー違反レポート。違反した個人、ポリシー、ルールを示します。また、承認、理由 (ある場合)、および違反する変更を要求したユーザーも示します。
- サービス・レポート。 システムに現在定義されているサービスをリストします。
- サービスに関連するアカウントの要約レポート。システムで定義されている指定のサービスに関連するアカウントの要約をリストします。
- サスペンドされたアカウント・レポート。サスペンドされたアカウントをリストします。
- ユーザー再認証ヒストリー・レポート。(特定の再認証プログラムによって) 手動で実行されたユーザー再認証のヒストリー、または (タイムアウト・アクションによって) 自動的に実行されたユーザー再認証のヒストリーをリストします。
- ユーザー再認証ポリシー定義レポート。ユーザー再認証ポリシー定義をリストします。

適切なアクセス・コントロールが構成されている場合、すべてのレポートをすべてのユーザーが利用できます。 ただし、一部のレポートは、特定タイプのユーザー専用に設計されています。

表 21. レポートの概要

使用対象者	**使用可能なレポート**
セキュリティー・アドミニストレーター	• 休止アカウント • 孤立アカウント • 保留再認証 • 再認証ヒストリー • 再認証ポリシー • ユーザー再認証ヒストリー • ユーザー再認証ポリシー
マネージャー	• 保留再認証 • 再認証ヒストリー • 再認証ポリシー • ユーザー再認証ヒストリー • ユーザー再認証ポリシー

表 21. レポートの概要 (続き)

使用対象者	使用可能なレポート
サービス所有者	• 休止アカウント • 孤立アカウント • 保留再認証 • 再認証ヒストリー • 再認証ポリシー • ユーザー再認証ヒストリー • ユーザー再認証ポリシー
監査員	• 休止アカウント • 孤立アカウント • 保留再認証 • 再認証ヒストリー • 再認証ポリシー • ユーザー再認証ヒストリー • ユーザー再認証ポリシー
エンド・ユーザー、ヘルプ・デスク、および開発者	なし

識別ガバナンス

IBM Security Identity Manager は、運用上の役割管理に焦点を当てることにより、識別管理ガバナンス機能を拡張します。 役割を使用すると、IT リソースへのアクセスを容易に管理できるようになります。

識別ガバナンスには、以下の IBM Security Identity Manager 機能が含まれます。

役割管理

リソースへのユーザー・アクセスを管理します。ただし、ユーザー・プロビジョニングとは異なり、役割管理では、ユーザー・アクセス権の付与または除去は行われません。 その代わり役割管理では、役割構造を設定してより効率的に管理を行います。

資格管理

権限をきめ細かく管理および強制することにより、アクセス・コントロールを簡素化します。

アクセス認証

リソースへのアクセスを役割レベルまたは資格レベルで継続的に検討および検証できます。

特権ユーザー管理

高度なユーザー管理を行い、高い特権を持つシステムまたは管理者のアカウントをモニターすることができます。

職務分離

ビジネス特有の矛盾を役割レベルまたは資格レベルで防止および検出します。

デュアル・ユーザー・インターフェース

IBM Security Identity Manager には、ジョブを実行するためにユーザーが必要とするもののみをユーザーに対して表示する、デュアル・ユーザー・インターフェースが備わっています。

インターフェースは分離しており、ユーザーは別々の Web アドレスを使用してそれらにアクセスします。 IBM Security Identity Manager には、管理コンソール・インターフェースとセルフケア・インターフェースという、2 つのタイプのユーザー・インターフェースが用意されています。

管理コンソール・ユーザー・インターフェース

管理コンソール・ユーザー・インターフェースは、管理用タスクの拡張セットを提供し、新しいマルチタスク機能を備えています。

個人ベースのコンソールのカスタマイズ

管理コンソール・ユーザー・インターフェースには、役割、ポリシー、およびレポートの管理など、管理用タスクの全セットが含まれます。 この個人ベースのコンソールは、以下のデフォルトの管理ユーザー・タイプのニーズに合わせたタスク・セットを提供します。

- システム管理者
- サービス所有者
- ヘルプ・デスク・アシスタント
- 監査員
- マネージャー

システム・アドミニストレーターは、ユーザーが実行できるタスクを、ユーザーのタイプごとに簡単にカスタマイズできます。 例えば、アカウントとタスクへのユーザーのアクセス権限をコントロールするには、ユーザー・グループ、アクセス・コントロール項目、およびビューのデフォルトのセットを使用します。 追加のユーザー・グループ、ビュー、およびアクセス・コントロール項目を定義して、ユーザーのアクセス権限をカスタマイズすることもできます。

マルチタスク管理

管理コンソール・ユーザー・インターフェース内のウィザードにより、ユーザーの追加、アカウントの要求、および新規サービスの作成などの管理用タスクが迅速化されます。 管理者は、複数のタスクを並行して管理できます。

拡張検索機能

管理コンソール・ユーザー・インターフェースは、強力な拡張検索機能も提供しています。

セルフケア・ユーザー・インターフェース

セルフケア・ユーザー・インターフェースは、ユーザーのみに適用される個人タスクのよりシンプルなサブセットを提供します。 ユーザーは、IBM Security Identity Manager のセルフケア・インターフェースを使用して、個人情報とパスワードを更新することができます。ユーザーは、要求の表示、アクティビティーの完了および委任、および自分のアカウントとアクセス権限の要求および管理を行えます。

セルフケア・ユーザー・インターフェースは、ユーザーがシンプルで直観的な各種のタスクを実行するためのセントラル・ロケーションを提供します。

システム・アドミニストレーターが付与した権限に基づき、セルフケア・ホーム・ページから以下のタスク・パネルを利用できます。

必要なアクション
完了する必要があるタスクのリスト。

ユーザーのパスワード
パスワードを変更するためのタスクのリスト。 パスワード同期化が有効になっている場合は、ユーザーは自分のすべてのアカウントに対して同期化される単一のパスワードを入力できます。 パスワードを忘れた場合の質問がシステムで構成されている場合、ユーザーは、その質問に正しく回答することによって、忘れたパスワードを再設定できます。

ユーザーのアクセス権
フォルダー、アプリケーション、役割、およびその他のリソースへのアクセス権限を要求および管理するためのタスクのリスト。

ユーザーのプロファイル
個人情報を表示および更新するためのタスクのリスト。

ユーザーの要求
ユーザーが送信した要求を表示するためのタスクのリスト。

ユーザーのアクティビティー
ユーザーのアクションを必要とするアクティビティーのリスト。 ユーザーはアクティビティーを委任することもできます。

再認証

IBM Security Identity Manager サーバー の再認証により、ユーザー、アカウントおよびアクセス権の定期的な再検査の処理が簡素化および自動化されます。

この再認証プロセスにより、有効なビジネス上の目的においてユーザー、アカウント、およびアクセス権が現在も必要かどうかを検査する処理が自動化されます。この処理では、指定した参加者に再認証通知と承認イベントが送信されます。

レポート作成

IBM Security Identity Manager の各レポートにより、監査を準備するための時間が削減され、すべての管理対象ユーザーとシステムに対するアクセス権限およびアカウント・プロビジョニング・アクティビティーの統合表示が提供されます。

レポート とは、IBM Security Identity Manager アクティビティーとリソースの要約のことです。要求、ユーザーおよびアカウント、サービス、または監査およびセキュリティーに基づいてレポートを生成できます。

レポート・データは、データ同期化プロセスによって段階的に処理されます。このプロセスは、IBM Security Identity Manager ディレクトリー情報ストアからデータを収集し、レポート・エンジン向けにこのデータを準備します。データの同期化は必要に応じて実行するか、または定期的に実行するようスケジュールすることができます。

レポートのアクセス可能性
IBM Security Identity Manager レポートは PDF フォーマットで使用できます。

以下のカテゴリーのレポートを利用できます。

要求 アカウント操作、承認、否認など、ワークフロー・プロセスのデータを提供するレポート。

ユーザーおよびアカウント
ユーザーおよびアカウントに関するデータを提供するレポート。例えば、個人のアクセス権限、アカウントのアクティビティー、処理中の再認証、およびサスペンドされた個人に関するデータが示されます。

サービス
調整統計、サービスのリスト、サービスのアカウントの要約など、サービスのデータを提供するレポート。

監査およびセキュリティー
アクセス・コントロール情報、監査イベント、不適合アカウントなど、監査およびセキュリティーのデータを提供するレポート。

共有アクセス
共有アクセスの履歴、役割別共有資格のリスト、および所有者別共有アクセス資格のリストを示すレポートです。

静的役割と動的役割

IBM Security Identity Manager は、静的役割と動的役割を提供しています。

静的な組織の役割では、静的役割への個人の割り当ては手動のプロセスです。

動的役割の場合、アクセス権限の有効範囲は、組織単位のみにすること、または組織単位とそのサブ単位にすることができます。動的な組織の役割は、有効な LDAP フィルターを使用して、特定の役割にユーザーのメンバーシップを設定します。 例えば、動的役割は、LDAP フィルターを使用して、audit123 という名前の監査部門のメンバーであるユーザーに対し、特定のリソースへのアクセス権限を提供します。 例えば、以下のように入力します。

```
(departmentnumber=audit123)
```

動的な組織の役割は、以下の各時点で評価されます。

- IBM Security Identity Manager システムで新規ユーザーが作成された時点
- タイトル、部門のメンバーシップなど、ユーザーの情報が変更された時点

- 新規の動的な組織の役割が作成された時点

セルフアクセス管理

IBM Security Identity Manager により、ユーザーおよびアドミニストレーターは、共有フォルダー、電子メール・グループ、アプリケーションなどのリソースへのアクセス権限を要求および管理できます。

アクセスはアカウントとは異なります。 アカウントは、管理対象サービスのオブジェクトとして存在します。アクセス権限は、管理対象サービス上のリソース (共有フォルダーなど) を使用する資格です。リソースにアクセスできるかどうかは、ユーザー・アカウントが属するグループの属性に基づきます。 したがって、リソースへのユーザーのアクセス権限は、アカウントとそのグループのマッピングに基づきます。 アカウントがサスペンドされると、それらのアクセス権限は非アクティブになり、それと同様に、アカウントが復元されると、それらのアクセス権限は再びアクティブになります。 アカウントが削除されると、そのユーザーのリソースへのアクセス権限も削除されます。 グループがサービスから除去されると、そのグループにマップしているユーザーのアクセス権限も除去されます。

アドミニストレーターは、通常、特定のユーザー・グループのニーズに基づいてサービス上のリソースへのアクセス権限を構成します。ユーザーは、アクセス権限を要求または削除できます。ユーザーはアカウント属性など、根底にあるテクノロジーを理解していなくても、使用するリソースへのアクセス権限を管理できます。

プロビジョニング機能

IBM Security Identity Manager は、企業においてサービスまたはコンポーネントを提供、デプロイ、および追跡するプロセスである*プロビジョニング* をサポートしています。 IBM Security Identity Manager は、セキュリティー製品スイートの 1 つとしてインプリメントされ、権限のある個人のみがリソースに確実にアクセスできるようにするための重要な役割を担います。IBM Security Identity Manager は、情報処理方法の正確性および完全性を保護し、権限のあるユーザーに、情報および関連する資産へのアクセス権限を付与します。

概説

IBM Security Identity Manager は、従業員、ビジネス・パートナー、サプライヤーに対し、およびプラットフォーム、組織、および地理を越えて組織に関連するその他の対象に対し、サービス、アプリケーション、およびコントロールのプロビジョンを管理する統合ソフトウェア・ソリューションを提供します。 このプロビジョニング機能を使用して、システムへのユーザー・アクセス権限のセットアップおよび保守を制御すること、および管理対象リソースのアカウントの作成を制御することができます。 情報の主なタイプは、個人データとアカウント・データの 2 つです。 *個人データ* は、管理対象のアカウントを所有するユーザーを表します。 *アカウント・データ* は、個人の資格情報、およびその個人にアクセス権限が付与されている管理対象リソースを表します。

大まかに述べると、ID 管理ソリューションは、リソースをプロビジョンするプロセスを自動化および集中化します。リソースには、オペレーティング・システムやアプリケーション、組織内のユーザーまたは組織と提携しているユーザーなどが含ま

れます。組織の構造を変更することで、プロビジョニング・ポリシーおよび手順に対応できます。 ただし、リソースのプロビジョニングのために使用される組織ツリーは、組織の管理上の構造を必ずしも反映しません。

すべてのレベルのアドミニストレーターは、標準化された手順を使用して、ユーザーの資格情報を管理できます。 一部のレベルの管理は、プロビジョニング管理ソリューションの幅に基づいて、削減または省略できます。 さらに、管理機能を各種の組織間で手動または自動で安全に分配できます。例えば、ドメイン・アドミニストレーターは、そのドメイン内のユーザーおよびリソースのみ処理することができます。 このユーザーは、管理タスクおよびプロビジョニング・タスクは実行できますが、ワークフローの作成など、構成タスクを実行する権限は付与されていません。

IBM Security Identity Manager は、プロビジョニング・タスクなどを各種の組織間で手動または自動で安全に分配する、*分配* 管理機能をサポートしています。 組織内で管理タスクを分配すると、管理の正確性および効率性が改善され、組織の作業負荷のバランスが改善されます。

IBM Security Identity Manager は、以下の領域で、企業のサービスとコンポーネントのプロビジョニングに対処します。

- アカウント・アクセス管理
- ワークフローおよびライフサイクルの自動化
- プロビジョニング・ポリシー
- 役割ベースのアクセス・コントロール
- 職務分離機能
- 自己調整型ユーザー管理
- カスタマイズ

アカウント・アクセス管理とプロビジョニング・システム

有効なアカウント・アクセス管理ソリューションにより、組織はどのユーザーがどの情報へのアクセス権限を持っているかを組織全体にわたって正確に追跡することが可能になります。 アクセス・コントロールは、集中化した、単一ポイントのプロビジョニング・システムの重要な機能です。 アクセス・コントロールにより、機密情報が保護され、さらに未承認の権限を所有する既存のアカウント、または必要なくなった既存のアカウントが判明します。 *孤立アカウント* は、正当なユーザーに関連付けることのできないアクティブなアカウントです。 管理対象リソースの孤立アカウントのアカウント所有者を、プロビジョニング・システムは自動的に判別できません。 プロビジョニング・システムは、孤立アカウントを制御するために、アカウント情報を、そのアカウントを所有するユーザーの権限情報に関連付けます。正式なユーザー ID 情報が、データベースおよび人的リソースのディレクトリー内に通常は保持されます。

不適切に構成されたアカウント は、正当なユーザーに関連付けられているにもかかわらず、不適切な権限が付与されたアクティブ・アカウントです。これは、組織がローカル管理者に IBM Security Identity Manager の外部のユーザーを追加または変更することを許可しているために発生します。不適切なアカウントの制御はさらに困難で、アカウント権限レベルで「どうする必要があるか」と「どうなっているか」を比較する必要があります。 アカウントが存在しても、その機能が必ずしも判

明するわけではありません。 洗練された IT システムのアカウントには、権限を定義する数百のパラメーターが含まれており、これらの詳細はプロビジョニング・システムで制御できます。

新規ユーザー は、人的リソース・ディレクトリーから確立したデータ・フィードを使用して簡単に識別できます。アクセス要求承認機能により、新規ユーザーのリソース・プロビジョニングを承認 (または拒否) するプロセスが開始されます。

ワークフローおよびライフサイクルの自動化

ユーザーが組織と提携するか、または組織に雇用されると、ユーザーのライフサイクルが開始します。 ビジネス・ポリシーおよびプロセスは、手動の場合も半自動の場合も、役割および責務に基づき、特定のリソースへのアクセス権限をユーザーにプロビジョンします。 時間が経過し、ユーザーの役割および機能が変更された場合も、ビジネス・ポリシーおよびプロセスは、そのユーザーが使用できるリソースをプロビジョンできます。最終的に、ユーザーと組織間の提携が解除されると、関連するアカウントはサスペンドされ、その後削除されます。これにより、組織でのユーザーのライフサイクルは終了となります。 *ワークフロー* を使用して、アカウントがプロビジョンされる方法をカスタマイズできます。ユーザーとアカウントの追加、除去、変更などの、ユーザーとアカウントのライフサイクルの管理をカスタマイズすることができます。完全なプロビジョニング・ワークフロー・システムでは、要求は適切な承認者に自動的にルーティングされ、その要求に対してアクションが実行されない場合は、別の承認者にルーティングされます。

IBM Security Identity Manager では、2 つのタイプのワークフローを定義できます。プロビジョニング・アクティビティーに適用される資格付与ワークフローと、エンティティー・タイプに適用される操作ワークフローの 2 つです。 *資格付与ワークフロー* は、プロビジョニング・ポリシーのプロビジョニング・アクションに特異的に結合されるビジネス・ロジックを定義します。 プロビジョニング・ポリシーの資格付与では、プロビジョニング・アクションは資格付与ワークフローに結合されます。 例えば、資格付与ワークフローは、アカウントを管理するための承認を定義するために使用されます。 *操作ワークフロー* は、エンティティー・タイプおよびエンティティーのライフサイクル・プロセスのビジネス・ロジックを定義します。 ワークフロー・プログラミング・ツールを使用して、プロビジョニング・ライフサイクルの主要な局面 (特に組織が使用する承認プロセス) を自動化できます。組織ツリー内のワークフロー・オブジェクトには、1 人以上の承認者またはエスカレーション承認者を含めることができます。 *承認者* は、プロビジョニング要求を承認または否認する権限を持つユーザーです。

プロビジョニング・ポリシーと監査

IBM Security Identity Manager が管理するリソースに対し、役割ベースのアクセス・コントロールをインプリメントすると、組織の役割エンティティーが 1 つ以上の ID に割り当てられます。 組織の役割は、*プロビジョニング・ポリシー* によって制御されます。このポリシーは、アプリケーションやオペレーティング・システムなどのリソースを管理するために Security Identity Manager サーバー が使用する、一連の組織ルールとロジックを表します。

役割がプロビジョニング・ポリシーの別の組織の役割のメンバーである場合は、役割メンバーはプロビジョニング・ポリシーの権限も継承します。

プロビジョニング・ポリシーにより、組織の役割のユーザーが、IBM Security Identity Manager 内の対応するリソースを表すサービスにマップされます。このポリシーにより、サービスにアクセスするときにユーザーが備えている必要のある資格が設定されます。インプリメントするプロビジョニング・ポリシーは、セキュリティー・プランの、組織の識別管理ポリシーを反映している必要があります。 有効なプロビジョニング・ポリシーをインプリメントするには、組織内の既存のビジネス承認プロセスを分析および文書化する必要があります。自動化した識別管理ソリューションをインプリメントするために、どのような調整をそれらのプロセスに行う必要があるか判断する必要があります。プロビジョニング・ポリシーは、ID ライフサイクル管理を自動化するためのフレームワークの中で、鍵となる部分を占めています。

IBM Security Identity Manager は、IBM Security Identity Manager で定義されるプロビジョニング・ポリシーに関する情報へのインターフェースとなる API、および個々のタスクに付与されるアクセス権限へのインターフェースとなる API を提供しています。 これらの API を効果的に使用して監査データを生成できます。 プロビジョニング・ポリシーが定義されると、調整機能により、ポリシー・ルールの実行が有効になります。調整機能により、参加システム (Security Identity Manager サーバー と管理対象リソースのリポジトリーの両方) が Single Point of Failure となる可能性が回避されます。

2 つ以上のプロビジョニング・ポリシーが適用される場合、*結合ルール* により、属性の処理方法が定義されます。 複数のポリシーの有効範囲がオーバーラップする場合があるため、その場合は、結合ルールにより、実行するアクションが指定されます。

プロビジョニング・ポリシーは、組織階層の特定の部分または特定のレベルにマップできます。 例えば、その単位の組織の役割にのみ影響を与える特定の組織単位で、ポリシーを定義することができます。サービス選択ポリシーは、個人属性に基づいてアカウントのプロビジョニングを有効にすることで、プロビジョニング・ポリシーの機能を拡張します。 サービス選択ポリシーは、プロビジョニング・ポリシーのターゲットとして定義された場合に実行されます。 JavaScript スクリプトを使用してどのサービスを使用するか指定すると、サービス選択ポリシーは、スクリプトの指示に基づきプロビジョニングを定義します。 JavaScript のロジックでは、通常、個人オブジェクトの属性を使用して、どのサービスを使用するのかを判別します。これらの属性は、通常、組織ツリー内の個人のロケーションです。

役割ベースのアクセス・コントロール

*役割*ベースのアクセス・コントロール (RBAC) では、役割とプロビジョニング・ポリシーを使用して、アクセス権限をユーザーに付与するビジネス・プロセスおよびルールが評価、テスト、および実行されます。 主要なアドミニストレーターは、プロビジョニング・ポリシーを作成し、ユーザーを役割に割り当て、それらの役割に対しリソースの資格セットを定義します。 RBAC タスクは、リソースに対する役割ベースのアクセス・コントロールを設定します。RBAC により識別管理ソリューションが拡張され、ソフトウェア・ベースのプロセスを使用できるようになり、プロビジョニング・プロセスにおけるユーザーの手動での対話が削減されます。

役割ベースのアクセス・コントロールは、ユーザー情報の変更を評価して、この変更によりユーザーの役割メンバーシップが変更されるかどうかを判定します。 変更

が必要な場合は、ポリシーが検討され、資格の変更がただちに実行されます。同様に、ポリシーのリソース・セットの定義が変更された場合、関連する資格に変更が生じる可能性があります。 役割ベースのアクセス・コントロールには、以下の機能があります。

- 必須資格とオプション資格。オプション資格は、自動的にプロビジョンされませんが、グループのユーザーはこれを要求できます。
- 前提条件サービス。特定のアクセス権限を設定する前に、特定のサービスの権限を付与する必要があります。
- 資格のデフォルト値と制約。資格の各特性をデフォルト値に設定することができます。付与する資格の特性に基づき、資格の範囲を制約することができます。
- 異なるポリシーが支配する複数の権限を持つ単一のアカウント。
- ユーザーおよび使用可能リソースに関する情報の、専用のフィルター・ビュー。
- 内部セキュリティー・ポリシーと整合するユーザー認証方式。
- 確実に WAN 環境およびインターネット環境にある、プロビジョニング・システム・コンポーネントの分配 (ファイアウォールの交差を含む)。
- 一貫性のあるユーザー定義のアルゴリズムを使用するユーザー ID。

自己調整型ユーザー管理

組織で、すべての内部組織に対するリソースのプロビジョンを開始する場合は、自己調整ユーザー管理機能をインプリメントしてください。組織の境界を越えてユーザーをプロビジョンすることの利点を実感できます。この環境では、ユーザーの状況の変更が、組織の境界および地理的位置を越えて自動的にアクセス権限に反映されます。 プロビジョニング・コストを削減し、またアクセスおよび承認プロセスを簡素化することができます。実装環境では、組織内のエンドツーエンドのアクセス管理のための役割ベースのアクセス・コントロールをインプリメントする効果を実感できるようになります。ユーザー・プロビジョニングを管理する手順の自動化により、管理コストを削減できます。セキュリティー・ポリシーの適用の自動化によりセキュリティーを改善でき、さらに多数のユーザーがいる場合のユーザー・ライフサイクル管理とリソース・プロビジョニングを合理化および集中化できます。

増分プロビジョニングとその他のカスタマイズ・オプション

チームは、ビジネスの計画および要件を使用して、IBM Security Identity Manager をどの程度カスタマイズするか決定できます。 例えば、大規模な企業では、地理的位置を越えて幅広く使用されるアプリケーションを増分的にプロビジョンするタイム・ラインに基づいた、ワークフローおよびカスタム・アダプターの段階的なロールアウト計画が必要となる場合があります。別のカスタマイズ計画では、テストが成功した後、組織全体に複数のアプリケーションをプロビジョンする場合があります。 ユーザーとアプリケーションとの相互作用はカスタマイズできます。また、自動化プロビジョニングに対応させるために、リソースをプロビジョンする手順を変更する場合があります。

サービスまたはコンポーネントを除去するには、*プロビジョン解除* します。 例えば、アカウントをプロビジョニング解除すると、そのアカウントがリソースから削除されます。

リソース・プロビジョニング

IBM Security Identity Manager では、ビジネス・ニーズに基づき、権限のあるユーザーにリソースをプロビジョンするために使用できる、いくつかの代替方法が用意されています。これらの代替方法は、要求、役割、または要求と役割の組み合わせをベースにしています。

リソースへの要求ベースのアクセス

IBM Security Identity Manager は、要求に基づいて、企業全体にわたるリソースへのアクセス権限の付与、変更、および削除を実行するための処理を提供します。この処理では、自動化されたレポートを使用した有効な監査証跡が設定されます。

要求ベースのプロビジョニングでは、ユーザーとそのマネージャーは、特定のアプリケーション、特権レベル、またはシステムのリソースへのアクセス権限を検索し要求します。 要求は、ワークフローで実行される承認により許可され、レポートまたは準拠の目的で監査されます。

例えば、ユーザーまたはそのマネージャーが新規アカウントへのアクセス権限を要求できます。 また、マネージャーまたは他のアドミニストレーターには、未使用のアカウントについてのアラートが送信され、再認証プロセスによってアカウントを削除するオプションが与えられます。 このようなユーザーのアクセス権限の定期的な確認により、以前の承認に基づくアクセス権限は、必要なくなった場合に確実に除去できます。

役割とアクセス・コントロール

組織の役割は、顧客のデプロイメントにおいて各種のアクセス・コントロール・モデルとアクセス・プロビジョニング・モデルをサポートします。

組織の役割を、プロビジョニング・ポリシーの IBM Security Identity Manager アクセス資格にマップできます。 この役割のメンバーであるユーザーのために、特定の IBM Security Identity Manager グループに権限を付与したり、グループを自動的にプロビジョンしたりできます。

役割がプロビジョニング・ポリシーの別の組織の役割のメンバーである場合は、役割メンバーはプロビジョニング・ポリシーの権限も継承します。

IBM Security Identity Manager のグループを使用して、IBM Security Identity Manager で管理される各タイプのエンティティーのビューおよびアクセス・コントロールを定義できます。

ハイブリッド・プロビジョニング・モデル

リソースのプロビジョニングのハイブリッド・モデルは、IBM Security Identity Manager がサポートしている要求ベースのアプローチと役割ベースのアプローチを結合したものです。

企業では、従業員または管理対象システムのサブセットに対し、役割ベースの割り当てを使用して、アクセス権限を自動化することができます。また、要求ベースのモデルを使用して、その他のすべてのアクセス権限要求または例外を処理すること

もできます。一部の企業では、最初は手動の割り当てを採用し、将来は完全に役割ベースのデプロイメントに移行するために、その手動割り当てをハイブリッド・モデルに発展させる場合があります。

これとは別に、完全に役割ベースのプロビジョニングを実現するのはビジネス上の理由から実際的ではないと判断し、必要な目標としてハイブリッド・アプローチをターゲットにする企業もあります。また別の企業では、要求ベースのプロビジョニングのみで十分であると判断し、役割ベースの自動化プロビジョニング・ポリシーを定義および管理するための余分な労力は必要ないと判断する場合があります。

第 6 章 技術概要

IBM Security Identity Manager を使用して、企業の組織内の従業員を表す識別レコードを管理できます。このセクションでは、製品体系および主要なコンポーネントについて説明します。

IBM Security Identity Manager は、オペレーティング・システムとアプリケーションのアカウントのユーザーへのプロビジョニングなど、リソースのプロビジョニング処理を集中管理する識別管理ソリューションです。

IBM Security Identity Manager を使用すると、ビジネス・プロセスおよびセキュリティー・ポリシーを基本的なユーザー管理に追加できます。これには、リソースにアクセスするためのユーザー要求の承認の追加が含まれます。また、IBM Security Identity Manager では、統一された方法でユーザー・アカウントの管理や管理の委任を行うことができ、セルフ・サービスやヘルプ・デスク・ユーザー・インターフェースなども提供しています。

ユーザー、許可、およびリソース

管理者は、IBM Security Identity Manager がユーザー、許可、およびリソースに提供するエンティティーを使用して、変化し続ける組織内で、初期アクセスおよび継続的なアクセスの両方を提供します。

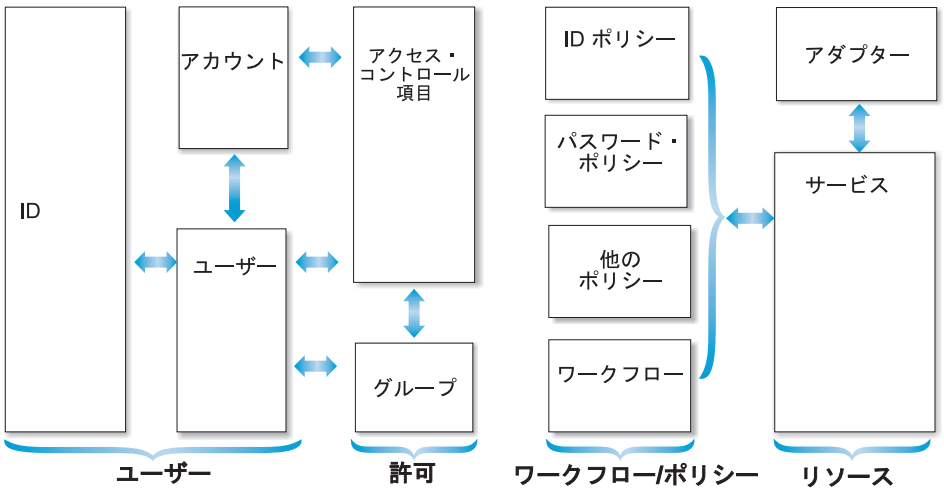

図 2. ユーザー、許可、およびリソース

ID 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・データのサブセットで、その個人に関連する追加情報を含んでいます。

アカウント
アカウントは、ユーザーの ID、ユーザー・プロファイル、および資格情報を定義する、管理対象リソースのパラメーターのセットです。

ユーザー

ユーザーは、IBM Security Identity Manager を利用してアカウントを管理する個人です。

アクセス・コントロール項目

アクセス・コントロール項目とは、指定されたタイプのリソースに対してユーザーが持っている許可を識別するデータのことです。 一連の操作および許可を指定するためのアクセス・コントロール項目を作成してください。その後で、どのグループがそのアクセス・コントロール項目を使用するのかを指示します。

グループ

グループは、IBM Security Identity Manager の機能とデータへのユーザーのアクセスを制御するために使用されます。 IBM Security Identity Manager グループでは、グループのメンバーシップにより、グループ・メンバーが必要とするデフォルトのアクセス許可および操作が、ビューとともに提供されます。

ポリシー

ポリシーとは、管理対象リソース (IBM Security Identity Manager ではサービスと呼ばれる) またはユーザーの動作に影響を与える考慮事項のセットのことです。 ポリシーは、IBM Security Identity Manager がユーザー ID などの他のエンティティーを管理するために使用する組織的なルールとロジックのセットを表し、サービス固有のポリシーなど、特定の管理対象リソースに適用されます。

アダプター

アダプターは、管理対象リソースと IBM Security Identity Manager サーバー の間のインターフェースを提供するソフトウェア・コンポーネントです。

サービス

サービスは、IBM Security Identity Manager が管理するオペレーティング・システム、データベース・アプリケーション、他のアプリケーションなどの管理対象リソースを表します。例えば、Lotus Notes® アプリケーションが管理対象リソースに相当する場合があります。 ユーザーは、サービスのアカウントを使用することで、これらのサービスにアクセスします。

メイン・コンポーネント

IBM Security Identity Manager ソリューションのメイン・コンポーネントには、IBM Security Identity Manager サーバー と、管理対象リソースへのインターフェースを提供するアダプターなど、必須およびオプションのミドルウェア・コンポーネントが含まれます。

クラスター構成では、メイン・コンポーネントには以下が含まれます。

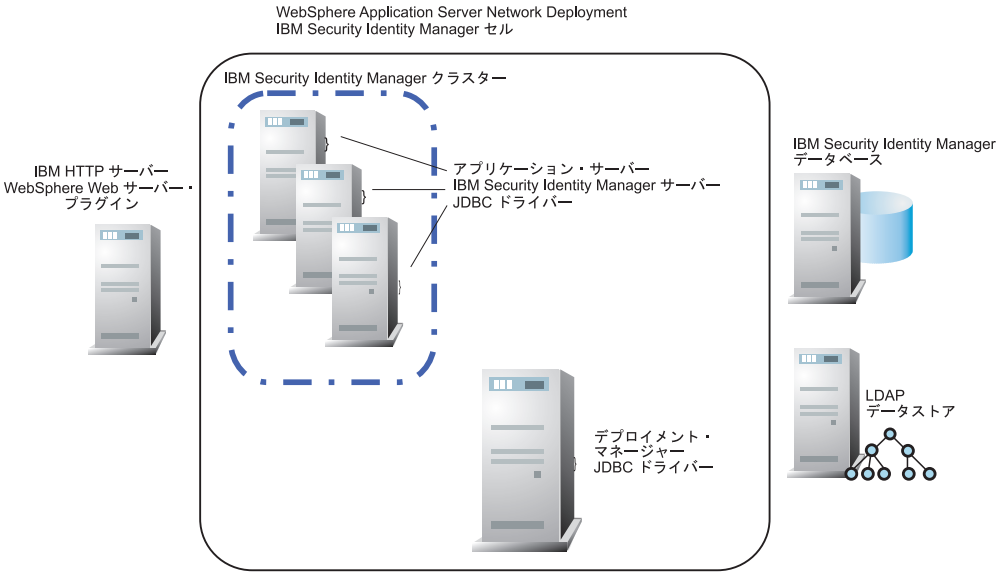

図 3. メイン・コンポーネント

代替構成についての詳細は、「*IBM Security Identity Manager インストール・ガイド*」を参照してください。

コンポーネントには以下が含まれます。

データベース・サーバー製品

IBM Security Identity Manager は、トランザクション・データおよびヒストリカル・データを、データの現在の状態およびヒストリカルな状態を管理するリレーショナル・データベースであるデータベース・サーバーに保管します。

データベースと通信するコンピューターは、Java Database Connectivity ドライバー (JDBC ドライバー) を必要とします。例えば、JDBC ドライバーは、IBM Security Identity Manager Server がデータ・ソースと通信することを可能にします。IBM Security Identity Manager は、Java ベースのアプリケーションをデータベースに接続するために JDBC タイプ 4 ドライバーをサポートします。

サポートされるデータベース製品は、IBM DB2 Database、Oracle DB、および MS SQL Server データベースです。各データベース製品用のタイプ 4 JDBC ドライバーに関する情報を以下に示します。

IBM DB2 Database

DB2 は、タイプ 4 JDBC ドライバーをサポートします。DB2 タイプ 4 JDBC ドライバーは、IBM Security Identity Manager インストール・プログラムにバンドルされています。

Oracle データベース

Oracle データベースは、タイプ 4 JDBC ドライバーをサポートします。IBM Security Identity Manager インストール・プログラムが、JDBC ドライバーの場所と名前の入力を要求するプロンプトを出します。

IBM Security Identity Manager Server をインストールする前に、*ORACLE_HOME*¥jdbc¥lib¥ ディレクトリー内の Oracle Database Server インストール済み環境からこの JDBC ドライバーを取得してください。あるいは、Web サイト http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.htmlからドライバーをダウンロードすることもできます。

WebSphere Application Server バージョン 7.0 用の JDBC ドライバーは ojdbc6.jar です。

Microsoft SQL Server データベース

SQL Server データベースは、タイプ 4 JDBC ドライバーをサポートします。IBM Security Identity Manager インストール・プログラムが、JDBC ドライバーの場所と名前の入力を要求するプロンプトを出します。

このドライバーは Web サイト http://msdn.microsoft.com/en-us/data/aa937724.aspxからダウンロードすることができます。

サポートされるデータベース・サーバー製品について詳しくは、IBM Security Identity Manager インフォメーション・センターの「*データベース・サーバーの要件*」を参照してください。

ディレクトリー・サーバー製品

IBM Security Identity Manager は、ユーザー・アカウントおよび組織のデータを含む、管理対象 ID の現在の状態を LDAP ディレクトリーに保管します。

IBM Security Identity Manager は、以下の製品をサポートします。

- IBM Tivoli Directory Server
- Sun Enterprise Directory Server

IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator は、異なるディレクトリー、データベース、およびアプリケーション内の ID データを同期化します。IBM Tivoli Directory Integrator は、アプリケーションまたはディレクトリー・ソース間の情報交換を同期化および管理します。

WebSphere Application Server

WebSphere Application Server は、WebSphere 環境の基本コンポーネントです。 WebSphere Application Server は、Java 仮想マシンを実行して、アプリケーション・コード用のランタイム環境を提供します。 アプリケーション・サーバーは、通信セキュリティー、ロギング、メッセージング、および Web サービスを提供します。

IBM Security Identity Manager アプリケーションは、WebSphere Application Server ベース・サーバーを使用したシングル・サーバー構成で実行することができます。IBM Security Identity Manager は、より大きなクラスター構成でも実行できます。この構成には 1 つ以上の WebSphere Application Server と、クラスターを管理するデプロイメント・マネージャーを含めることができます。

HTTP サーバーおよび WebSphere Web サーバー・プラグイン

HTTP サーバーは、Web ブラウザーのクライアント・インターフェースを

介して IBM Security Identity Manager を管理できるようにします。 IBM Security Identity Manager では、HTTP サーバーとともに WebSphere Web サーバー・プラグインをインストールする必要があります。 WebSphere Application Server のインストール・プログラムは、IBM HTTP Server と WebSphere Web サーバー・プラグインを別々にインストールできます。

IBM Security Identity Manager アダプター
アダプターは、管理対象リソースと IBM Security Identity Manager Server の間のインターフェースを提供するプログラムです。アダプターは、ターゲット・プラットフォーム上の信頼された仮想管理者として機能し、アカウントの管理を行います。アダプターは、例えば、アカウントの作成、アカウントのサスペンド、アカウント属性の変更などのタスクを実行します。

IBM Security Identity Manager アダプターは、エージェント・ベースにすることも、エージェントレスにすることもできます。

エージェント・ベースのアダプター
アダプター・コードの設計時に通信相手として指定された管理対象リソースに、アダプター・コードを直接インストールします。

エージェントレス・アダプター
IBM Security Identity Manager Server、および IBM Tivoli Directory Integrator をホストするシステムに、アダプター・コードをデプロイします。アダプター・コードは、その設計時に通信先として指定された管理対象リソースから独立しています。

注: エージェントレス・アダプターの場合は、SSH プロセスまたはデーモンが管理対象リソース上でアクティブになっている必要があります。

ユーザーの概要

従業員や請負業者などのユーザーは、組織が提供するリソースを使用する必要があります。 IBM Security Identity Manager アカウントを持つユーザーは IBM Security Identity Manager ユーザーです。

ユーザーは作業の際、リソースに対するさまざまなレベルのアクセス権を必要とします。 一部のユーザーは、特定のアプリケーションを使用する必要があります。別のユーザーは、他のユーザーをそのユーザーの作業に必要なリソースにリンクするシステムを管理する必要があります。

IBM Security Identity Manager は、ユーザーの ID、アカウント、それらのアカウントに基づくアクセス資格、およびパスワードなどのユーザー資格情報を管理します。

ユーザー

ユーザーは、IBM Security Identity Managerによって管理される個人です。 IBM Security Identity Manager アカウントを持つユーザーは、IBM Security Identity Manager ユーザーと呼ばれます。このユーザーは、アカウントを管理するため、またはその他の管理用タスクを実行するために、 IBM Security Identity Manager を使用することができます。

ユーザーは作業の際、リソースに対するさまざまなレベルのアクセス権を必要とします。 一部のユーザーは、特定のアプリケーションを使用する必要があります。別のユーザーは、他のユーザーをそのユーザーの作業に必要なリソースにリンクするシステムを管理する必要があります。 IBM Security Identity Manager ユーザーは、特定ビューへのアクセス権限を提供し、IBM Security Identity Manager で特定タスクを実行することをユーザーに許可する特定グループに割り当てられます。

管理者は、ID レコードをインポートすることで、または IBM Security Identity Manager を使用することで、ユーザーを作成します。

ID

ID とは、個人またはエンティティーを一意的に表すプロファイル・データのサブセットです。データは、1 つ以上のリポジトリーに保管されます。

例えば、ID は個人の名、姓、氏名、および従業員番号の固有な組み合わせによって表される場合があります。 ID プロファイルには、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る場合もあります。

アカウント

アカウントは、ID、ユーザー・プロファイル、および資格情報を定義する、管理対象リソースのパラメーターのセットです。

アカウントは、ログイン情報 (例えば、ユーザー ID およびパスワードなど) と、アカウントに関連付けられた特定のリソースへのアクセス権を定義します。

IBM Security Identity Manager ではアカウントは、管理対象リソースを表すサービス上に作成されます。このようなリソースとして、オペレーティング・システム (UNIX)、アプリケーション (Lotus Notes)、またはその他のリソースがあります。

所有されている場合、アカウントは個人アカウントまたはスポンサーの設定されたアカウントのいずれかです。 個人アカウントは、単一の所有者により使用されることを目的としており、個人の所有権タイプを持ちます。 スポンサーの設定されたアカウントは、当該アカウントの責任がある所有者に割り当てられますが、リソースへのアクセスにそれらを実際には使用しない場合があります。スポンサーの設定されたアカウントでは、個人以外のさまざまな所有権タイプを使用できます。 IBM Security Identity Manager では、スポンサーの設定されたアカウントの所有権タイプとして、「デバイス」、「システム」、および「ベンダー」の 3 種類が用意されています。 システムの構成ユーティリティーを使用して、スポンサーの設定されたアカウントについて追加の所有権タイプを作成できます。

アカウントはアクティブまたは非アクティブの状態にあります。 システムにログインするには、アカウントがアクティブである必要があります。 アカウントがサスペンドされている場合、そのアカウントは非アクティブになります。アカウント使用の再認証要求が拒否され、再認証アクションがサスペンド になっている場合、サスペンドが発生する可能性があります。サスペンドされたアカウントは、存在はしていますが、システムのアクセスに使用することはできません。システム・アドミニストレーターは、アカウントが削除されていない場合には、サスペンドされたアカウントを復元して再びアクティブにすることができます。

アクセス

アクセスは、共有フォルダーやアプリケーションなどの特定のリソースを使用するための機能です。

IBM Security Identity Manager では、アクセス権限を作成してアクセス・タイプへのアクセスを表すことができます。これらのアクセス・タイプとしては、共有フォルダー、アプリケーション (Lotus Notes など)、電子メール・グループ、その他の管理対象リソースなどがあります。

アカウントはアクセス権限の 1 つの形式であり、その点においてアクセス権限はアカウントとは異なります。アカウントはリソース自体へのアクセス権限です。

*アクセス権限*はリソースを使用するための許可です。*アクセス資格*は、管理対象リソースでユーザー・アカウントの一連の属性値を使用して、ユーザーに対してアクセス権限を与える条件を定義します。IBM Security Identity Manager では、アクセス権は、管理対象サービスの既存のグループで定義されます。この場合は、サービスでアカウントを作成してユーザーをグループに割り当てることによって、ユーザーにアクセス権が付与されます。また、アクセス資格は、プロビジョニング・ポリシーを使用するサービスのアカウントでパラメーター・セットとして定義することもできます。

ユーザーが新規アクセス権限を要求すると、デフォルトで、そのサービスにアカウントが作成されます。アカウントが既に存在している場合、アクセス資格を満たすようにそのアカウントが変更されます。例えば、アクセス・タイプに対するアクセス権限を付与するグループに、そのアカウントが割り当てられます。アカウントが 1 つ存在する場合、そのアカウントがアクセス権に関連付けられます。 複数のアカウントが存在する場合は、アクセスを関連付けるアカウントのユーザー ID を選択する必要があります。

多くの場合、アクセス権は、ビジネス・ユーザーにとって理解しやすい用語で説明されます。

パスワード

*パスワード*は、システムにアクセスするユーザーを認証するのに使用される文字ストリングです。 ユーザー ID とパスワードは、システムへのアクセスを認可する 2 つのエレメントです。

アドミニストレーターは、自分のユーザー・パスワード、およびユーザーに対し設定され IBM Security Identity Manager により使用されるユーザー・パスワードを管理できます。

パスワードを忘れた場合の管理

パスワードを忘れた場合の情報を管理および定義して、忘れた IBM Security Identity Manager パスワードをユーザーが再設定できるようにすることができます。この情報は、質問と回答の形式で指定します。

パスワード同期

パスワード同期は、ユーザーが所有するすべての個人アカウントに対して 1 つのパスワードを割り当てて保守する処理です。パスワード同期により、ユーザーが記憶していなければならないパスワードの数を減らすことができます。

あるユーザーが所有するすべての個人アカウントのパスワードが自動的に同期するようにシステムを構成できます。これによりユーザーは、1 つのパスワードを覚えるだけで済むようになります。例えば、ユーザーが IBM Security Identity Manager アカウントと Lotus Notes アカウントの 2 つの個人アカウントを所有しているとします。このユーザーが IBM Security Identity Manager のアカウントのパスワードを変更または再設定した場合、Lotus Notes のパスワードは IBM Security Identity Manager と同じパスワードに自動的に変更されます。アカウントをプロビジョンした場合、またはサスペンド状態のアカウントを復元した場合も、パスワードが同期します。

パスワードの同期が有効になっている場合、ユーザーは自分が所有する他の個人アカウントに別のパスワードを指定できません。

注: アカウントをプロビジョンする場合、またはサスペンド状態のアカウントを復元する場合、アカウントのパスワードを指定する必要があります。 パスワードの同期が有効な場合、パスワードを要求するプロンプトは出されません。 代わりに、そのユーザーの既存の個人アカウントのパスワードと同じパスワードがその個人アカウントに自動的に与えられます。

パスワード・ストレングス規則

パスワード・ストレングス規則は、パスワードを準拠させる必要がある規則または要件です。 例えば、パスワード・ストレングス規則で、パスワードの最小文字数を 5 文字と指定することができます。パスワード・ストレングス規則で、パスワードの最大文字数を例えば 10 文字と指定することもできます。

パスワード・ストレングス規則をパスワード・ポリシーに定義できます。

リソースの概要

リソースとは、ユーザーが自分の作業割り当てを完了するために必要とするアプリケーション、コンポーネント、処理、およびその他の機能のことです。

IBM Security Identity Manager は、サービスを使用してユーザー・アカウントとリソースへのアクセスを管理し、またアダプターを使用してリソースと IBM Security Identity Manager 間の信頼できるデータ通信を提供します。

サービス

サービス とは、オペレーティング・システム、データベース・アプリケーション、または IBM Security Identity Manager が管理する別のアプリケーションなどの管理対象リソースのことです。例えば、管理対象リソースが、Lotus Notes アプリケーションである場合もあります。

ユーザーは、サービスのアカウントを使用することで、これらのサービスにアクセスします。

サービスはサービス・タイプから作成されます。サービス・タイプは、類似属性を共有する管理対象リソースのセットを表します。 例えば、Linux マシンを表すデフォルトのサービス・タイプがあります。 これらのサービス・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。あるいは、それらの管理対象リソースのアダプター用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されます。

サービスのアカウントは、サービスのユーザーを識別します。 アカウントにはユーザーのログイン情報およびアクセス情報が含まれ、アカウントにより特定リソースの使用が許可されます。

大部分のサービスが IBM Security Identity Manager を使用してアカウントをプロビジョンします。これには、通常、正しく完了する必要のあるワークフロー・プロセスが含まれます。 ただし手動サービスは、要求の完了、またはユーザーへのアカウントのプロビジョンに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を生成します。

サービス所有者 は、IBM Security Identity Manager の特定のサービスを所有し、保守します。サービス所有者は、個人または静的な組織の役割のいずれかです。静的な組織の役割の場合、この組織の役割のメンバーはすべて、サービス所有者と見なされます。この静的な組織の役割にその他の役割が含まれる場合は、これらの役割のすべてのメンバーもサービス所有者と見なされます。

サービス・タイプ

サービス・タイプ とは、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。

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に使用されます。 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があります。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ことができます。

サービス前提条件

サービスには、サービスの前提条件として別のサービスが定義されている場合があります。ユーザーは、前提条件となるサービスで既存のアカウントを所持する場合にのみ、新規アカウントを受け取ることができます。

例えば、サービス B にサービス前提条件サービス A があるとします。ユーザーがアカウントを受け取るためにサービス B でアカウントを要求する場合は、ユーザーはまずサービス A のアカウントを取得する必要があります。

サービス定義ファイル

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 サーバー 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 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ユーザー・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 サーバー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。 有効なサービス・プロバイダーは、Tivoli Directory Integrator および DSMLv2 です。
- 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。アカウントのプロパティー・ファイルと、サービス・グループなどのサポート・データは、これらのフォームの属性のラベルを定義します。ラベルは、サービスを作成するため、およびそれらのサービスのアカウントを要求するために、ユーザー・インターフェースに表示されます。

手動サービス

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・メールをセットアップするために定義される場合があります。

手動サービスは、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を生成します。

IBM Security Identity Manager がアカウントをプロビジョンする管理対象リソース用のアダプターを提供しない場合は、手動サービスを作成する場合があります。

手動サービスを作成する場合は、手動サービス用の新規スキーマ・クラスと属性をご使用の LDAP ディレクトリーへ追加します。

以下のトピックを参照してください。

- 「*IBM Security Identity Manager 構成ガイド*」の『手動サービスおよびサービス・タイプ』
- 「*IBM Security Identity Manager 管理ガイド*」の『接続モードの使用可能化』

アダプター

アダプターは、管理対象リソースと IBM Security Identity Manager の間のインターフェースを提供するソフトウェア・コンポーネントです。

アダプターは、管理対象リソース用の信頼された仮想アドミニストレーターとして機能します。アダプターは、アカウントの作成やサスペンドなどのタスク、およびその他の通常はアドミニストレーターが行う機能を実行します。

アダプターは、サービス定義ファイルとアカウントの管理用の実行可能コードから構成されます。

アダプターは、次の 2 つの方法のいずれかでデプロイされます。

エージェント・ベースのアダプター

エージェント・ベースのアダプターは、アカウントを管理するために管理対象リソース上に存在する必要があります。例えば、AIX® 用の Lotus Notes アダプターは、エージェント・ベースのアダプターです。

エージェントレス・アダプター
エージェントレス・アダプターは、リモート・サーバー上に配置して、アカウント管理に使用することができます。例えば、UNIX/Linux アダプターは、エージェントレス・アダプターです。

アダプターは、次の 2 つのテクノロジーのいずれかで作成されます。

Adapter Development Kit (ADK)
ADK を使用して作成されるアダプターは、エージェント・ベースのアダプターまたはエージェントレス・アダプターのいずれかです。 ADK はアダプターの基本コンポーネントであり、ランタイム・ライブラリー、フィルター処理とイベント通知の機能、プロトコル設定、およびロギング情報を含んでいます。 ADK はすべてのアダプターで同じです。

IBM Tivoli Directory Integrator
IBM Tivoli Directory Integrator を使用して作成されるアダプターは、エージェント・ベースのアダプターまたはエージェントレス・アダプターのいずれかです。これらのアダプターは組み立てラインとしてインプリメントされ、各組み立てラインはデータ転送と変換のための単一パスです。 IBM Tivoli Directory Integrator は、ある組み立てラインからのデータを次の組み立てラインに渡すことができます。

IBM Security Identity Manager をインストールする際に、数個のエージェントレス・アダプターが自動的にインストールされます。追加のエージェントレスまたはエージェント・ベースのアダプターをインストールできます。

管理対象リソースとのアダプター通信

IBM Security Identity Manager と管理対象リソース間の通信には、いくつかのソリューションがあります。

Linux および UNIX の管理対象リソースは、IBM Tivoli Directory Integrator を使用して作成されるエージェントレス・アダプターを使用します。その他の管理対象リソースは、ADK アダプターを使用します。

64 ページの図 4 では、ソフトウェア製品とコンポーネント間の通信リンクをどのように構成できるかを示しています。

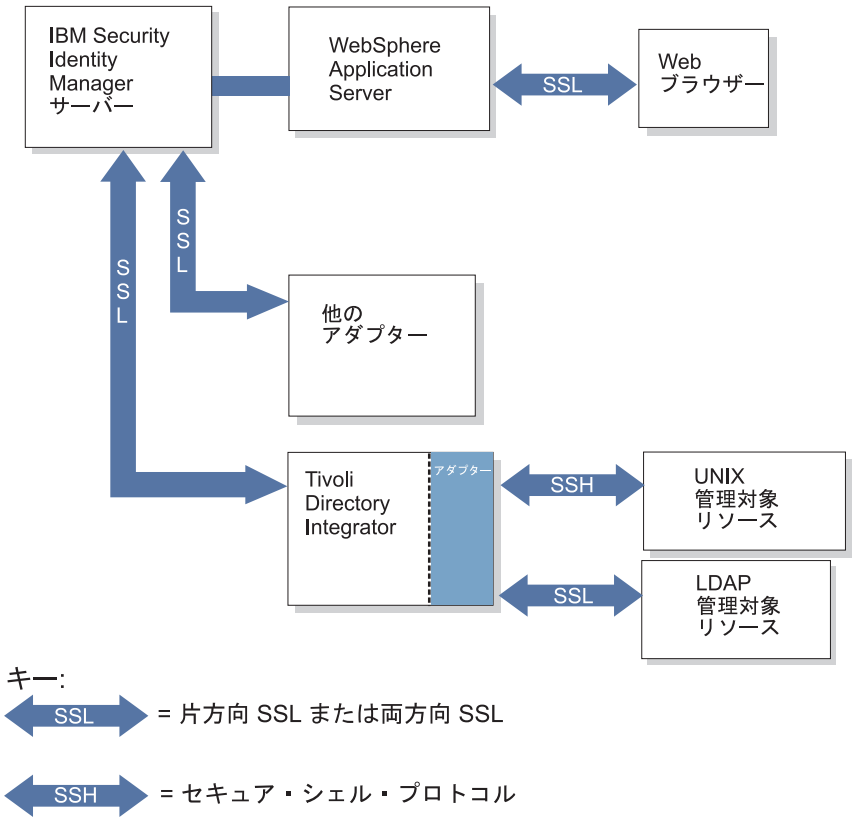

図 4. IBM Security Identity Manager 環境におけるセキュア通信

システム・セキュリティーの概要

組織では、ユーザーのアクセスを制御し、機密情報を保護することが特に必要です。

最初に、組織がビジネスで必要なセキュリティー要件について合意します。次に、システム・アドミニストレーターが、IBM Security Identity Manager によってデータのセキュリティーのために提供されているグループ、ビュー、アクセス・コントロール項目、およびフォームを構成します。

セキュリティー・モデルの特性

組織は、そのビジネス・ニーズを満たすためにセキュリティー・モデルを定義します。 モデルは、セキュリティー・システムの要件および実際のインプリメンテーションを定義するための基礎として役立ちます。

セキュリティー・モデルの主な目的を以下に示します。

- ユーザーの ID を検査する (パスワード・ストレングスおよびその他の要因を組み込んでいる認証システムにより実現)。
- 権限があるユーザーがリソースにアクセスできるようにする (要求または役割ベースのプロセス、および関連するプロビジョニングを定義する許可システムによ

り実現)。リソースとは、例えば、アカウント、サービス、ユーザー情報、IBM Security Identity Manager の機能などです。

セキュリティー・モデルには、ユーザーのアクセスを許可するリソースを選択する、追加のプロビジョニング・プロセスも必要です。

- どの操作および権限がアカウントおよびユーザーに許可されているか管理する。
- 要求または割り当てに基づき、ユーザーのアクティビティー・リストを他のユーザーに委任する。
- ユーザー・リスト、アカウント属性などの機密情報を保護する。
- 通信およびデータの整合性を保証する。

業務要件

IBM Security Identity Manager が提供するプロセスをインプリメントする前に、業務のセキュリティー要件を取り決める必要があります。

例えば、要件の定義で以下の問題に対処する場合があります。

- IBM Security Identity Manager ユーザーのどのようなグループが存在しているか。
- 各ユーザー・グループがどの情報を参照する必要があるか。
- 各グループのユーザーがどのタスクを実行する必要があるか。
- ユーザーが組織内でどの役割を実行するか。
- どのようなアクセス権限を定義する必要があるか。
- 一部のユーザーが異なる権限レベルを所有することを要求する作業関係には、どのようなものがあるか。
- 確立されたポリシーに違反するアクティビティーの修正を、防止および監査でどのように実現できるか。

一般的な業務ニーズを満たすには、マネージャー、ヘルプ・デスク・アシスタント、監査員グループなど、複数のグループが必要になる場合が頻繁にあります。また、タスクの拡張セットまたは制限セットを実行するカスタマイズ・グループを用意することもできます。

ユーザーのパースペクティブからのリソース・アクセス

特定の業務リソースにおけるタスクの範囲内で作業するユーザーに対しデータのセキュリティーを提供するために、IBM Security Identity Manager により、1 つ以上の役割、および 1 つ以上のグループのメンバーシップを提供する場合があります。

例えば、ビジネス単位のユーザーは、購買担当者など、責任のある肩書きまたは役割を通常は持ちます。 ユーザーは、地域購買担当など、ユーザーが実行できるタスクのビューを提供するグループのメンバーである場合もあります。これらの関係は、 66 ページの図 5で示されています。

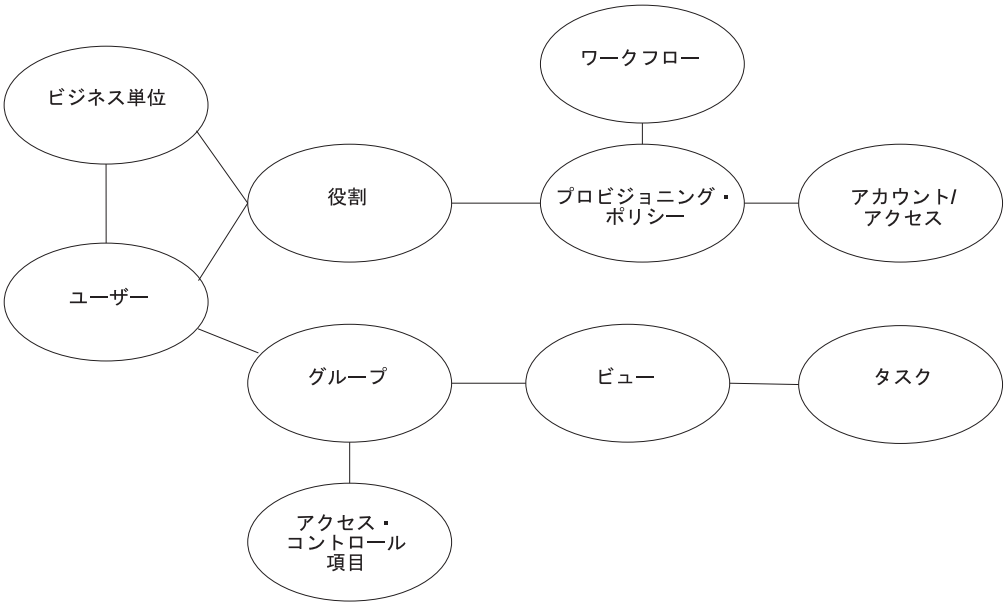

図 5. ユーザーがリソースにアクセスするためのデータの保護

各役割には、アカウントなど、1 つ以上のリソースにユーザーがアクセスできるようにするための、関連するプロビジョニング・ポリシーおよびワークフローがあります。

各グループには、特定のタスクのビュー、およびタスクを実行するための特定の操作および権限を付与する 1 つ以上のアクセス・コントロール項目があります。 Form Designer アプレットを使用することで、ユーザーに表示するユーザー・インターフェースを変更することもできます。アカウント、サービス、またはユーザー属性に関する不要なフィールドを削除することもできます。

グループ

グループ は、IBM Security Identity Manager の機能とデータへのユーザーのアクセスを制御するために使用されます。

グループ・メンバーは、IBM Security Identity Manager サービスのアカウントを所持します。 IBM Security Identity Manager グループでは、グループのメンバーシップにより、グループ・メンバーが必要とするデフォルトのアクセス許可および操作が、ビューとともに提供されます。 また、お客様のサイトで、カスタマイズしたグループを作成することもできます。

さらに、一部のユーザーを、特定のアプリケーションまたは他の機能への特定のアクセス権のあるサービス・グループのメンバーにすることもできます。例えば、会計アプリケーションでデータを直接操作するメンバーをサービス・グループに含める場合があります。

事前定義のグループ、ビュー、およびアクセス・コントロール項目

IBM Security Identity Manager には、事前定義のグループが用意されています。 これらのグループは、ビューおよびアクセス・コントロール項目に関連付けられています。

以下の 2 つのユーザー・インターフェースまたはコンソールを使用できます。

- 個人プロファイル情報 (電話番号など) の変更などのセルフケア・アクティビティーでの、すべてのユーザー向けのセルフ・サービス・コンソール。
- 特定範囲の管理タスクを実行できる 1 つ以上のグループに所属する、選択されたユーザー向けの管理コンソール。

他のグループ・メンバーシップを所有しない IBM Security Identity Manager ユーザーは、IBM Security Identity Manager を使用する基本特権を所有します。

この一連のユーザーは、セルフケア機能用のセルフ・サービス・コンソールのみ必要とします。 これらのユーザーは、ヘルプ・デスク・アシスタント・グループなどの、ラベルのある「グループ」には所属しません。

図 6 に示されているように、事前定義グループは、事前定義のビューおよびアクセス・コントロール項目に関連付けられており、メンバーが表示できるもの、および実行できることを制御しています。

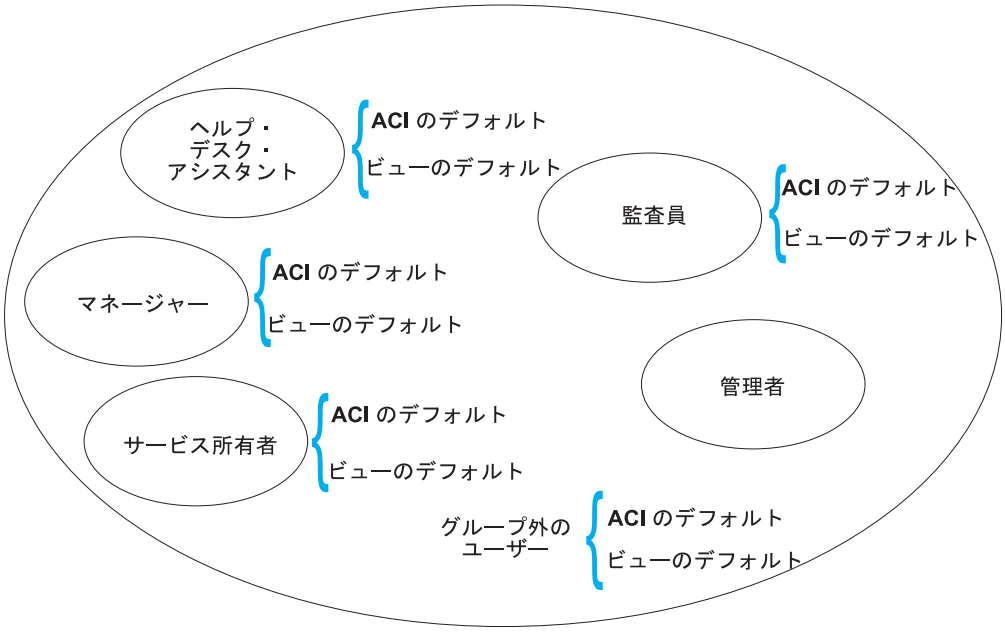

図 6. 事前定義のグループ、ビュー、およびアクセス・コントロール項目

事前定義のグループを以下に示します。

管理者 管理者グループは、デフォルトのビューまたはアクセス・コントロール項目によって制限は設定されておらず、IBM Security Identity Manager のすべてのビューにアクセスでき、すべての操作を実行できます。最初のシステム管理者ユーザーは、「itim manager」という名前になります。

監査員 監査員グループのメンバーは、監査目的のレポートを要求できます。

ヘルプ・デスク・アシスタント
ヘルプ・デスク・アシスタント・グループのメンバーは、アカウントを要求、変更、サスペンド、復元、および削除することができます。 また、メンバーは、アクセス権限を要求、変更、および削除すること、および他のユ

ーザーのパスワード、プロファイル、およびアカウントをリセットすることもできます。 さらに、メンバーは、ユーザーのアクティビティーを委任することもできます。

マネージャー
マネージャー・グループのメンバーは、直接従属ユーザーのアカウント、プロファイル、およびパスワードを管理するユーザーです。

サービス所有者
サービス所有者グループのメンバーは、サービスを管理します。これには、そのサービスのユーザー・アカウントと要求の管理も含まれます。

ビュー

ビュー は、グラフィカル・ユーザー・インターフェースで、特定タイプのユーザーが表示できるが、実行はできない場合があるタスクのセットです。例えば、IBM Security Identity Manager を使用するためにユーザーが必要とする、毎日のアクティビティーのタスク・ポートフォリオなどです。

セルフ・サービス・コンソールと管理コンソールの両方で、ユーザーが表示できるビューを指定できます。

アクセス・コントロール項目

アクセス・コントロール項目 (ACI) とは、ユーザーが指定されたタイプのリソースに対して持っている許可を識別するデータのことです。 一連の操作および許可を指定するためのアクセス・コントロール項目を作成してください。また、どのグループがそのアクセス・コントロール項目を使用するのかも指示します。

アクセス・コントロール項目では、以下の項目を定義します。

- アクセス・コントロール項目が適用されるエンティティー・タイプ
- ユーザーがエンティティー・タイプに対して実行できる操作
- ユーザーが読み取りまたは書き込みできるエンティティー・タイプの属性
- アクセス・コントロール項目によって管理されるユーザーのセット

IBM Security Identity Manager では、デフォルトのアクセス・コントロール項目が提供されます。

カスタマイズされたアクセス・コントロール項目を作成することもできます。例えば、カスタマイズしたアクセス・コントロール項目で、特定のヘルプ・デスク・アシスタント・グループが他のユーザー用の情報を変更する能力を制限する場合が考えられます。 また、アクセス・コントロール項目では、マネージャー、サービス所有者などのリレーションシップも指定できます。

カスタマイズ・レポートを作成する場合、その新しいレポート用のレポート・アクセス・コントロール項目およびエンティティー・アクセス・コントロール項目も手動で作成する必要があります。これらの ACI を使用すると、監査員などの管理者でないユーザーが、カスタム・レポートを実行したり、カスタム・レポート内のデータを表示したりできるようになります。

アクセス・コントロール項目を作成した後、または既存のアクセス・コントロール項目を変更した後、データの同期化を実行して、レポート・エンジンなどの他の

IBM Security Identity Manager プロセスが、新しいアクセス・コントロール項目または変更されたアクセス・コントロール項目を使用するようにします。

フォーム

フォーム とは、アカウント、サービス、またはユーザー属性の値の収集と表示に使用されるユーザー・インターフェースのウィンドウのことです。

IBM Security Identity Manager には、既存のユーザー、サービス、およびアカウントの各フォームの変更に使用する、Java アプレットとして実行される Form Designer が含まれています。 例えば、FAX 番号属性および関連する入力フィールドを追加して、特定のアカウントの FAX 番号を収集することができます。組織がユーザーに表示したくないアカウント属性を削除することもできます。フォームから属性を除去すると、属性は完全に除去されます。つまり、システム・アドミニストレーターでさえ属性を見ることはできません。

見ることができるのは、フォーム上にあり、(アクセス・コントロール項目によって付与された) 読み取りアクセス権限または書き込みアクセス権限を持つ属性のみです。また、Form Designer を使用すると、部署単位、組織単位など、組織ツリー内の他のエレメントのフォームをカスタマイズすることもできます。

組織ツリーの概要

ビジネス組織には、サービスや従業員など、従属単位を含むさまざまな構成があります。

一連の特定ビジネス・ニーズに応じて、サービス階層を示すように IBM Security Identity Manager を構成できます。組織、ユーザー、および他の要素を、ユーザー数のニーズに対応したツリー形式で構成できます。

注: このリリースは、特定のユーザーを検索するための拡張メニューを提供していますが、同じ目的のためのグラフィック組織ツリーは提供していません。

このリリースでは、組織ツリーを移動してエンティティーを参照および作成することはできません。 組織ツリー内のビジネス単位への関連は、エンティティーの作成時に指定されます。

組織ツリー内のノード

組織ツリーは、組織、従属ビジネス単位、その他の要素などのノードを所有します。

組織ツリーは、以下のノードを所有できます。

組織 組織階層の最上部を示します。これは、組織単位、ビジネス・パートナー組織単位、およびロケーションなどの従属エンティティーを含む場合があります。 組織は、ノード・ツリーの最上部にある親ノードです。

組織単位
事業部や部門など、組織の従属的な部分を示します。 組織単位は、他の任意のコンテナー (組織、組織単位、ロケーション、ビジネス・パートナー組織など) に従属させることができます。

ビジネス・パートナー組織単位
ビジネス・パートナー組織を示します。通常は、サプライヤー、顧客、および請負業者など、ユーザー組織の提携先の会社が相当します。

ロケーション
地理的に異なるものの、組織エンティティーの中に含まれるコンテナーを示します。

管理ドメイン
組織の従属的な部分を、独自のポリシー、サービス、およびアクセス・コントロール項目を持つ、独立したエンティティー (アクションとビューがそのドメインに制限されている管理者を含む) として示します。

ビジネス単位に関連するエンティティー・タイプ

各種のエンティティーを、組織ツリー内のビジネス単位に関連付けることができます。

ビジネス単位への関連は、エンティティーが作成されるときに指定されます。 通常、エンティティーは、作成された後、ビジネス単位の関連を変更できません。 唯一の例外は、ユーザー・エンティティーです。 IBM Security Identity Manager は、異なるビジネス単位間でのユーザーの転送をサポートしています。

以下のエンティティー・タイプを、組織ツリー内のビジネス単位に関連付けることができます。

- ユーザー
- ITIM グループ
- サービス
- 役割
- 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
- サービス選択ポリシー
- 再認証ポリシー
- アカウントおよびアクセス要求ワークフロー
- アクセス・コントロール項目

組織ツリーのエンティティー検索

このリリースは、特定のユーザーを検索するためのメニューは提供していますが、特定のユーザーを見つけるためのグラフィック組織ツリーは提供していません。

検索メニューを使用して特定のユーザーを見つけるには、個人やビジネス・パートナー個人など、ユーザー・タイプごとに検索する拡張検索フィルターを使用します。検索では、ビジネス単位とそのサブ単位、およびアクティブなどのユーザー状況も選択できます。 さらに、LDAP フィルター・ステートメントなど、検索を限定するその他のフィールドを追加することもできます。

ポリシーの概要

ポリシー とは、管理対象リソース (IBM Security Identity Manager ではサービス と呼ばれる) またはユーザーの動作に影響を与える考慮事項のセットのことです。

ポリシーは、IBM Security Identity Manager がユーザー ID などの他のエンティティーを管理するために使用する組織的なルールとロジックのセットを表し、サービス固有のポリシーなど、特定の管理対象リソースに適用されます。

IBM Security Identity Manager により、組織は、指定したユーザー・グループに対して集中型のセキュリティー・ポリシーを使用できます。 IBM Security Identity Manager ポリシーを使用すると、組織内のさまざまなリソースへのユーザー・アクセスを集中管理することができます。リソースへのユーザー・アクセスに関連する操作を簡素化する追加ポリシーおよび機能をインプリメントすることができます。

IBM Security Identity Manager では、以下のタイプのポリシーがサポートされます。

- 採用ポリシー
- 識別ポリシー
- パスワード・ポリシー
- プロビジョニング・ポリシー
- 再認証ポリシー
- 職務分離ポリシー
- サービス選択ポリシー

ポリシーは、サービス・タイプにより識別できる、またはサービスを明示的にリストすることにより識別できる、1 つ以上の対象サービスに適用できます。 これらのポリシーは、ID フィードを示すサービスには適用されません。

- 採用ポリシーは、サービスに適用されます。 グローバル採用ポリシーは、特定のサービス・タイプのすべてのサービスに適用されます。
- 識別ポリシー、パスワード・ポリシー、およびプロビジョニング・ポリシーは、すべてのサービス・タイプ、特定のサービス・タイプのすべてのサービス、または特定のサービスに適用できます。
- 再認証ポリシーは、すべてのサービス・タイプに作用できませんが、特定の再認証ポリシーに対し異なるすべてのサービスを追加できます。
- 職務分離ポリシーは、サービス・タイプに直接適用されず、ユーザーの役割メンバーシップにのみ適用されます。
- サービス選択ポリシーは、1 つのサービス・タイプのみに適用されます。

ポリシーのタイプおよびナビゲーション

表 22. ポリシーのタイプおよびナビゲーション

ポリシーのタイプ	ナビゲーション
採用	**「ポリシーの管理」>「採用ポリシーの管理」**
ID	**「ポリシーの管理」>「識別ポリシーの管理」**

表 22. ポリシーのタイプおよびナビゲーション (続き)

ポリシーのタイプ	ナビゲーション
パスワード	**「ポリシーの管理」>「パスワード・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」**
再認証	**「ポリシーの管理」>「再認証ポリシーの管理」**
職務分離	**「ポリシーの管理」>「職務分離ポリシーの管理」**
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」**

アカウントのデフォルト

アカウントのデフォルトは、新規アカウントの作成時のアカウントのデフォルト値を定義します。 デフォルトは、そのタイプのすべてのサービスに適用されるサービス・タイプ・レベルで定義できます。あるいは、サービスのみに適用されるサービス・レベルで定義することもできます。

ポリシー実行

グローバル・ポリシー実行 は、プロビジョニング・ポリシーに違反したアカウントを、IBM Security Identity Manager がグローバルに許可または却下する方法です。

ポリシー実行アクションがグローバルの場合、サービスに対するポリシー実行は、デフォルトの構成設定により定義されます。 非準拠の属性を持つアカウントに対し、以下のいずれかのポリシー実行アクションが実行されるように指定できます。

注: サービスに特定のポリシー実行設定がある場合、その設定が非準拠の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。 ポリシー実行は、特定のサービスに対しても設定できます。

マーク 古いサービスの既存のユーザー・アカウントが却下とマークされ、新規アカウントが新規サービスに作成されます。

サスペンド
古いサービス・インスタンスの既存のユーザー・アカウントがサスペンドされ、新規アカウントは新規サービスに作成されません。

アラート
古いサービスでの古いアカウントの削除を確認するよう要求するアラートが受信側管理者に送信されます。ユーザーが新規サービスにアカウントを所有しておらず、資格付与が自動の場合は、新規サービスで新規アカウントが作成されます。

修正 古いサービスで既存のアカウントが除去されます。ユーザーが新規サービスでアカウントを所有しておらず、資格付与が自動の場合は、新規サービスで新規アカウントが作成されます。

グローバル・ポリシー実行に関する操作を行うには、ナビゲーション・ツリーに移動し、「**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。

注: サービス・ポリシー実行を設定するには、ナビゲーション・ツリーに移動し、「**サービスの管理**」を選択します。

ワークフローの概要

ワークフロー は、ビジネス・プロセスを表すアクティビティーの順序を定義します。 ワークフローを使用して、アカウント・プロビジョニング、アクセス権限プロビジョニング、およびライフサイクル管理をカスタマイズできます。

ワークフローは、ビジネス・プロセスを定義する一連のステップまたはアクティビティーです。 IBM Security Identity Manager ワークフローを使用して、アカウント・プロビジョニングおよびライフサイクル管理をカスタマイズできます。 例えば、アカウント・プロビジョニング・プロセスまたはアクセス権限プロビジョニング・プロセスに承認要求および情報要求を追加できます。ライフサイクル管理プロセス (IBM Security Identity Manager でのユーザーおよびアカウントの追加、削除、変更など) を外部システムに統合することができます。

IBM Security Identity Manager が提供しているワークフローの主なタイプを以下に示します。

操作ワークフロー

アカウント、ユーザー、または特定のサービス・タイプ (すべての Linux システムなど) のライフサイクルの管理をカスタマイズするには、操作ワークフローを使用します。

操作ワークフローでは、アカウント、ユーザーなどのシステム・エンティティーが追加、削除、変更、復元、およびサスペンドされます。 また、新規アカウントの承認など、ビジネス・プロセスで必要な操作を新規追加することもできます。例えば、通知とマネージャーの承認など、アカウントを承認するアクティビティーを定義する操作ワークフローを指定する場合があります。

アカウント要求ワークフローとアクセス権要求ワークフロー

組織のビジネス・ポリシーに従い、アカウントまたはサービスなどのリソースがユーザーにプロビジョンされるようにするには、アカウント要求ワークフローおよびアクセス権要求ワークフローを使用します。

注: IBM Security Identity Manager バージョン 4.6 では、*資格付与ワークフロー* という用語がこのタイプのワークフローを表すのに使用されていました。

- *アカウント要求ワークフロー* は、アクセス権限またはアカウントの資格付与にバインドできます。

  プロビジョニング・ポリシーでは、アカウントの資格付与ワークフローにより、アカウントの追加、変更などのアカウント要求にデシジョン・ポイントが追加されます。 要求が承認されると、プロセスが続行されます。要求が否認されると、要求はキャンセルされます。

アカウント要求ワークフローは、IBM Security Identity Manager ユーザーにより実行される、またはアカウント自動プロビジョニング中に実行される、アカウント・プロビジョニング要求 (アカウントの追加、変更など) 時に開始されます。また、アカウント要求ワークフローは、アクセス権要求ワークフローが定義されていない場合には、アクセス権要求時に開始することもできます。

- *アクセス権要求ワークフロー* は、プロビジョニング・ポリシーではなく、アクセス権限定義によってアクセス権限にバインドされます。 このワークフローでは、要求されたリソースへのアクセス権限を付与する手順および承認を指定できます。

  アクセス権要求ワークフローは、IBM Security Identity Manager ユーザーによって行われたアクセス権要求についてのみ開始されます。このワークフローは、外部または内部アカウント要求の結果としてユーザーにアクセス権限がプロビジョンされる場合には開始されません。外部アカウント要求は、IBM Security Identity Manager ユーザーが実行するアカウント要求です。 内部アカウント要求は、IBM Security Identity Manager システムが実行するアカウント要求です。例えば、自動アカウント・プロビジョニングは、アクセス権限にマップされるデフォルト・グループまたは必須グループをユーザーに付与します。

第 7 章 初回ログインおよびパスワードに関する情報

IBM Security Identity Manager をインストールした後、始動するには、ログイン URL と初回用ユーザー ID およびパスワードを知っている必要があります。

ログイン URL

ログイン URL を使用すると、IBM Security Identity Managerの Web インターフェースにアクセスできます。

IBM Security Identity Manager 管理コンソールのログイン URL を以下に示します。

`http://`*`ip-address:port`*`/itim/console/main/`

ip-address は IBM Security Identity Manager サーバーの IP アドレスまたは DNS アドレスで、*port* はポート番号です。 IBM Security Identity Manager の新しいインストールのデフォルト・ポートは 9080 です。

IBM Security Identity Manager セルフ・サービス・コンソールのログイン URL を以下に示します。

`http://`*`ip-address:port`*`/itim/self`

ip-address は IBM Security Identity Manager サーバーの IP アドレスまたは DNS アドレスで、*port* はポート番号です。 IBM Security Identity Manager の新しいインストールのデフォルト・ポートは 9080 です。

初回用ユーザー ID およびパスワード

IBM Security Identity Manager で認証される初回用ユーザー ID およびパスワードを以下に示します。

表 23. IBM Security Identity Manager の初回用ユーザー ID およびパスワード

ユーザー ID	パスワード
itim manager	*secret*

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。

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］

［ワ行］

A

I

T

Printed in Japan

GA88-4857-00

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