HP Select Identity

ソフトウェアバージョン： 4.21

コンセプトガイド

文書公開日 : 2008 年 1 月
ソフトウェアリリース日： 2008 年 1 月

ご注意

保証

HP の製品およびサービスの保証は、当該製品およびサービスに含まれる明示的保証書に明記されています。ここに記載されている内容は、その他の保証を付加するものではありません。HP は、本書の技術的または編集上の誤りに対して一切の責任を負わないものとします。

本書に記載されている内容は、予告なしに変更することがあります。

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Java™ は Sun Microsystems, Inc の米国商標です。

Microsoft および Windows® は Microsoft Corporation の米国登録商標です。

Oracle® は Oracle Corporation (Redwood City、California) の米国登録商標です。

UNIX® は The Open Group の登録商標です。

Select Identity 製品 CD の `license` ディレクトリには本製品で使用される各サードパーティ製品の使用許諾契約書が保存されています。

サポート

次の HP ソフトウェアサポート Web サイトをご利用いただけます。

http://h20230.www2.hp.com/selfsolve/manuals

HP ソフトウェアのオンラインサポートでは、対話形式による技術サポートツールを効率的にご利用いただけます。サポートサイトでは次のことが可能です。

- 関心のあるドキュメントを検索する
- サポートケースおよび機能拡張の要望を登録 / トラッキングする
- ソフトウェアパッチをダウンロードする
- サポート契約を管理する
- HP サポートの問合わせ先を調べる
- 利用可能なサービスに関する情報を確認する
- ソフトウェアを利用している他のユーザーとの情報交換
- ソフトウェアトレーニング情報の検索とお申し込み

大部分のサポートには、HP Passport へのユーザー登録とサインインが必要です。また、サポート契約が必要な場合もあります。

アクセスレベルと HP Passport に関する詳細は、次の URL で確認してください。

http://h20230.www2.hp.com/new_access_levels.jsp

目次

1 本書について

『HP Select Identity コンセプトガイド』へようこそ。

本書は、HP Select Identity (Select Identity) を理解し、実際に使用するために必要な情報を提供します。本書をお読みいただくと、Select Identity の基本概念を理解し、Select Identity の機能を最大限に活用する技術を習得することができます。

ただし、本書には Select Identity のグラフィカルユーザーインタフェースを含む詳細な手順は含まれていません。それらの情報は、以下の詳細なオンラインヘルプシステムで説明しています。

構成

『HP Select Identity コンセプトガイド』は、Select Identity の背景にある概念および原理をより詳細に説明しています。また、Select Identity が通常どのように配布されるかの概要と例も示されています。

この資料は、Select Identity を初めて使用する場合、配布プロセスの概要を知りたい場合、または Select Identity の機能とその目的を論理的に理解したい場合に特に役に立ちます。

対象読者

本書は対象者を限定しています。本書で想定している読者は以下のとおりです。

- Select Identity が業務に対して何をもたらすのか、配布には何が含まれるのかを深く理解する必要がある組織の意思決定者
- Select Identity の背景にある概念を完全に理解する必要があるアイデンティティ管理設計技術者
- 製品をよりよく理解したいシステム管理者および事業部管理者
- ユーザーの追加、変更、および削除を日常的に行っているユーザー管理者
- Select Identity についての最新情報を手に入れ、より大きな責任を遂行するための準備をしたいヘルプデスクユーザー

前提条件

この文書では、読者および読者の状況が以下の条件を満たしているものと想定していることにご注意ください。

- 読者は、アイデンティティ管理の分野全体について実用的な知識を持っている必要があります。

ヘルプの使用

Select Identity には、以下の主要なテーマ領域を含む詳細なヘルプシステムが付属しています。

- HP Select Identity 管理者向けオンラインヘルプ (管理者のみ)
- HP Select Identity My Identity オンラインヘルプ (全ユーザー)
- HP Select Identity Workflow Studio オンラインヘルプ (管理者のみ)

その他の Select Identity 文書

ほかにも、Select Identity についての情報を提供しているものがあります。以下の資料はすべて、Select Identity の製品 CD から参照することができます。

- 『HP Select Identity 管理者ガイド』- Select Identity を使用してアイデンティティ管理を設計、実装、および配布する方法について詳細な情報を提供します。
- 『HP Select Identity コネクタ開発者ガイド』- カスタムコネクタを作成するための技術リファレンスです。
- 『HP Select Identity 外部コール開発者ガイド』- 外部コールを作成、登録、使用する方法について説明しています。
- 『HP Select Identity インストールガイド』- 使用できるすべてのプラットフォームと移行に関する情報が含まれ、Web アプリケーションサーバーに Select Identity をインストールし、セットアップする方法について説明しています。
- 『HP Select Identity Web Services 開発者ガイド』- SPML を使用して Web サービスリクエストを開発するための技術リファレンスです。
- 『HP Select Identity 新情報 (提供されている場合)』およびソフトウェアに付属する『リリースノート』- Select Identity に関して後で追加された最新情報が記されています。

2 Select Identity へようこそ

はじめに

Select Identity は、アカウントや権限のプロビジョニング、承認ワークフロー、管理権限の委任、セキュリティポリシーの強制、およびレポート作成などの、アイデンティティ管理に関連したタスクの簡素化および自動化を目的としています。

Select Identity は、アイデンティティ管理の方法としてサービスベースのアプローチを提供し、アイデンティティ管理が組織内の現実のビジネスプロセスと一致するようにします。より高度に抽象化されたアプローチを採用し、従来のロールおよびルールベースのアイデンティティ管理の制限を緩和します。これにより、配布時間と管理コストの削減を実現し、スケーラビリティとセキュリティを向上させることができます。

Select Identity を業務に取り入れるということは、デジタルアイデンティティの作成、保守、および終了を、人、プロセス、テクノロジによってサポートし、サービス、システム、アプリケーションへのセキュアなアクセスをタイムリーに実現するということです。

Select Identity の機能

Select Identity は、プラットフォーム、アプリケーション、および企業間のユーザーアカウントおよび使用権のプロビジョニングと管理のプロセスを自動化します。Select Identity は組織内のビジネスプロセスを反映したアプローチを提供するので、アイデンティティ管理が簡素化されます。

Select Identity を配布することにより、ヘルプデスクの負荷と費用の軽減、迅速でエラーの少ないプロビジョニング、規制要件の確実な遵守、および重要な業務データのセキュリティの強化を期待できます。

Select Identity を使用する理由

産業から政府、教育から財務にいたるすべてのタイプの現代の組織は、ワークシェアリング、テレコミュニケーティング、地理的に分散したチーム、共同事業などの増大するニーズに直面しています。さらに、顧客、パートナー、納入業者、および従業員の間での相互のやりとりを効率的で生産的なものにするには、内部と外部の両方の情報にアクセスしなければならず、その中には機密情報に属するものも含まれます。特定の課題に取り組むチームやタスクフォースはすぐに形成されますが、任務を果たせばただちに解散するので、ニーズは個人の枠を超えたものになっています。

誰でも、またどの組織でも、企業または自分の属する環境の中で、新しいリソースを迅速に配布し、変更に対応する必要性を経験したことがあるはずです。

新しいビジネス環境のサポート、入れ替わるユーザーの管理、ビジネスプロセスの急激な発展への対応は、より困難さを増しています。同時に、さまざまな場所からデータやサービスに自由にアクセスできるようになったため、セキュリティに対する危険性も増大しています。

説明責任およびコーポレートガバナンスの透明性を求める関係者 (株主、議員、および業務監査委員) の声も大きくなっています。効果的なセキュリティとアクセス手段の実装は、もはや単に望ましいということでは済まなくなっているのです。これらは、企業の評判や財産をハッカーや詐欺師から守り、会計疑惑、訴訟、および懲罰的規制などの事態を防ぐために必須のものなのです。

大抵の場合、ネットワークを使った攻撃がネットワークの内側からも外側からも行われ、その巧妙さと、潜在的な被害について気が付く人はいません。特に、頻繁な社員の配置転換、人員整理、強制的配置転換、会社合併などがあるところではこの傾向が強くなります。

一方、重要なリソース (システム、アプリケーションおよび情報リポジトリ) へのアクセス管理の規模と複雑さを大きくすると、組織の効率と効果が妨げられます。当然、ユーザーにとって必要なリソースへのアクセスに遅延が生じることになります。持ち主のいないアカウントなどの問題が、知らない間に発生します。ユーザーは、パスワードを忘れたときに新しいパスワードを要求する面倒よりも、むしろパスワードをメモしておき、システムの使用を避けるようになります。

結局は、業務マネージャ、IT 業務、コールデスクのスタッフは、単純に受け入れることのできない結果に直面します。つまり、ヘルプデスクに殺到する問い合わせは、取るに足らない問題、最適とはいえないビジネスリソースの使用、潜在的なセキュリティ低下に関するものであふれてしまうのです。

問題への取り組み

課題に対処するため、組織は包括的なアイデンティティ管理戦略を開発する必要があります。

多くの場合、企業の発展に伴って、複数の異なるシステムおよびプロセスが有機的に成長します。その時点で適切でも、規模に応じて拡張することができず、セキュリティ手段は確実性に欠け、ユーザー、グループ、リソースの数が増えると複雑さが指数関数的に増大してしまいます。

アイデンティティ管理は、解決方法として重要になるとともに問題としても大きくなります。

問題の正しい答え、それは、真に効果的なアイデンティティ管理方法であり、それは次の 5 つの必須要件を備えていなければなりません。

- **識別 (または認証とも呼ぶ)**

  個人またはシステムのアイデンティティを明確にする機能。これによって電子資格証明が発行され、信頼されます。これは、「自分が自分自身であること」を証明することです。

- **承認**

  個人またはシステムを、特定のアプリケーション、システム、およびサービスの使用権に関連付ける機能。これは、ある何かへのアクセス権限を与えること、そしてそれ以外へのアクセス権限を自動的に拒否することです。

- **アクセス**

  承認済みの個人、アプリケーション、およびシステムに、システムおよびサービスへの管理されたアクセスを強制する機能。これは、ルータやファイアウォール上のアクセスコントロールリストなどの単純なものから、権限管理インフラストラクチャといった包括的なものにまで及びます。

- **説明責任**

  アイデンティティ管理システムへの変更をすべてドキュメント化し、すべての異常があれば検出して解決し、監査要件に準拠させること。

- **順応性**

  組織、組織のプロセス、提携先、人員の急速な変化を、包括的で費用効果に優れた方法で簡単にサポートする機能。

アイデンティティ管理へのアプローチ

すべてのアイデンティティ管理システムは、システムがアイデンティティ情報を編成して管理プロセスを実行するための枠組みを定義します。最も一般的なモデルは、ロールベースのアクセス制御 (RBAC) で、**ロール**という概念を使用してユーザーと使用権を編成します。Select Identity は、**サービス**と呼ばれるより高度な抽象概念および**コンテキスト**と呼ばれる補足的な概念を採用しています。

ロールベースのアクセス制御 (RBAC) について

ロールベースのアクセス制御 (RBAC) は、アイデンティティ管理システムとして従来から使用されているモデルです。これは、もともと個別アプリケーション内のアクセス管理の問題を扱うために考え出されました。その後、アイデンティティ管理の領域を扱うように拡張されて、複数のアプリケーション、組織、およびビジネスプロセスにわたる管理フレームワークを提供するようになりました。

高いレベルにおいて、RBAC は状況に応じた柔軟なモデルを提供しています。ロールは、広範囲の責任を扱うこともあれば、特定のタスクに焦点を置くこともあります。ロールは一般にロール管理者によって定義されるもので、業務、および業務が複数のリソースに対してどのように実行されるのかについての現実的な知識が要求されます。

ジョブの機能が相対的に適切に構成され、静的である場合は、RBAC は効果的なアイデンティティ管理を提供できます。しかし、大規模で非常に動的な組織では、管理可能で拡張可能な一連のロールを設計することは困難です。

現代の企業では、1 人のメンバーが単一のロールを持つことはまれです。品質保証マネージャがサポートエスカレーションチームの一員であると同時に、会社の慈善キャンペーンのコーディネータであることもあります。ジョブが変更された場合に、変更されるロールもあれば変更されないロールもあります。RBAC ソリューションでは、このような変更に簡単に対応できないことがあります。

さらに、テキサスの「マネージャ」ロールを持つ人が、カリフォルニアの「マネージャ」のアクセス権のほとんどを持っているが、一部は持っていないということがあります。通常、ルールは例外を処理して問題を緩和する目的で確立されます。しかしルールは、規定して維持するのが難しく、簡単にテストできるものではありません。

これらの理由で、純粋な RBAC ソリューションを企業の再編成または合併に適合させることは困難で費用もかかることになります。システムが成長し変化するにつれてロールも増殖するという性質があるため、ルールの変更や追加を行う際には、予測しない影響を避けることができません。

最後に、Sarbanes-Oxley 法などの現在のビジネス規制の遵守には、安全なインフラおよび強固な監査機能が必要となります。純粋な RBAC ソリューションでこれらの問題に対応できるものはほとんどありません。

Select Identity について

Select Identity は、サービス、そしてコンテキストという、アイデンティティ管理にとって中心となるシンプルな 2 つのアイデアを取り入れています。これらのアイデアは、アイデンティティ管理につての新しい考え方を提供し、ほかのソリューションの能力を飛躍的に発展させるものです。

サービスとコンテキストについて、ここではごく簡単に紹介します。詳細は本書の後半で説明します。

サービス

Select Identity では、サービスという概念を用いて、アイデンティティおよびアクセス管理をビジネスプロセスに対応させます。基本的に、サービスは従業員、顧客およびパートナーによって使用されるプロセスとリソース (システム、アプリケーションおよび情報) を表します。

Select Identity では、サービスという概念を通して、ビジネスの作業項目をアイデンティティ管理の組織的モデルに使用します。リソースは、サービス内に作成されます。電子メール、SAP、LDAP、データベースなどの数多くのリソースを単一のサービスに関連付けたり、複数の異なるサービスで同一のリソースを共有したりすることができます。

会社の組織構造ではなくビジネスプロセスに従ってアイデンティティ管理タスクが編成されます。その結果、ロールはサービスに従属したものになります。

このアプローチによって、企業のリソースおよびプロセスの動的な変化を、内部的にも外部的も、より簡単に管理できるようになります。これによって、効率と利益が大きく向上します。

Select Identity が提供するサービスの種類

- 業務サービス ― リソースと使用権へのアクセスを従業員、顧客、パートナーに提供するための標準サービス。
- 管理サービス ― 管理のためにユーザーに管理者ロールを割り当てるサービス。
- コンポジットサービス ― 2 つ以上の類似するサービスを 1 つのコンポジットユニットに組み合わせるサービス。

この 3 種類の中に、リソース、使用権、ワークフロー、ポリシー、その他のアイデンティティ管理要素を 1 つのエンティティにカプセル化する個々のサービスがあります。各ユーザーの異なるニーズやアクセス権に対応するため、サービスを追加したり、既存のサービスを変更したりして、これらの要素をさまざまにパーティション化またはグループ化することができます。

コンテキスト

コンテキストは、ユーザー ID プロファイル内の特定の属性値に基づいてユーザーをグループ化する動的な方法です。

たとえば、アイデンティティプロファイルに `Residency` という属性が含まれ、そこに従業員の居住国が含まれるとします。従業員は、`Italy`、`China`、`India`、あるいは `Canada` など、属性値に基づいたグループに分類されます。これらのグループのそれぞれがコンテキストです。

この属性値が変更されるとき (従業員が移動したときなど)、Select Identity はユーザーが現在属しているコンテキストはどれかを確認します。新しいコンテキストの下でなにが承認されているかに基づいて、ユーザーのリソースおよび使用権に適切な調整が加えられます。

RBAC モデルに関しては、コンテキストによってアイデンティティをロールに動的に割り当てることが可能です。これは、強力な拡張です。サービスと結びついたコンテキストは、アイデンティティ管理への強力で動的なアプローチとなります。

Select Identity の利点

Select Identity は、アイデンティティ管理ソリューションをあらゆる点で拡張するいくつかの重要な利点を提供します。

Select Identity によってセキュリティが向上し、規制への遵守が徹底されます。また、効率と生産性が向上し、複雑な、または拡大したエンタープライズの管理コストが大幅に削減されます。プロビジョニングに始まり、メンテナンスから終了までのアイデンティティのライフサイクル全体を、1 つの画面から簡単に管理できます。

Select Identity は、プラットフォーム、アプリケーション、さらに企業間での、ユーザーアカウントと使用権のプロビジョニングおよび管理のプロセスを自動化します。

アイデンティティ管理の中には時間の経過とともに現実に合わなくなるものがありますが、Select Identity は変化に簡単に適応します。ユーザーのアイデンティティを使用権から分離することによって、Select Identity は 2 つの独立した問題が絡み合うのを回避しています。

サービスの作成は 1 回限りの作業で、サービスは簡単に適切なユーザーに対して使用可能にすることが可能です。さらに、サービスは修正が可能で、時間の経過とともに変化する条件に適応させることができます。

Select Identity は、比類のないユーザビリティとスケーラビリティを提供します。堅牢なワークフロー管理、ユーザー自己サービス、監査機能、レポート作成、および委任管理機能とともに、Select Identity は包括的なアイデンティティ管理ソリューションを提供しています。

Select Identity の機能

Select Identity は、その洗練されたアイデンティティ管理機能により、単純性、標準化、モジュール方式、および統合性を提供します。これらの機能によって、大規模な、あるいはグローバルな組織におけるアイデンティティ管理の複雑な問題を解決します。

- **プロビジョニング** ― 企業の情報システムに対するアカウントおよび使用権の作成、変更、削除を自動化します。
- **ワークフロー** ― 必要な承認など、ユーザーのプロビジョニングに必要なプロセスを自動化します。
- **ユーザー自己サービス** ― エンドユーザーは、単純な Web ブラウザインタフェースを介して、サービスへのアクセスの開始、変更、および終了、パスワードの変更、パスワードヒントの設定、アイデンティティに関する一般情報の更新を行うことができます。
- **管理の委任** ― 業務部門、顧客、およびパートナーの複数階層間で管理権限を委任することができます。
- **パスワードおよびプロファイルの管理** ― パスワードポリシーを定義して強制することができます。異種情報システム間で、パスワードおよびユーザープロファイル情報を管理、同期化および分配することができます。
- **監査およびレポート作成** ― Select Identity は、Sarbanes-Oxley 法およびその他の規制基準への準拠を達成するための基盤としてセキュアなインフラストラクチャを構築します。また、Select Identity はアクションおよびユーザーアカウントアクティビティに関する標準化されたレポート作成を提供します。HP Select Audit とともに使用することによって、文書への適合を迅速に達成することができます。
- **スケーラブルで柔軟** ― 大きなワークロードも正常のペースで処理します。

- **ユーザーのインポート** ― 既存のユーザー、プロファイル情報、および使用権をインポートします。
- **拡張性のあるコネクタアーキテクチャ** ― 現在および将来の IT 環境との接続性を保証します。
- **可変の使用権** ― ロールまたはルールを増やさずにロールベースの使用権割り当ての例外を処理します。
- **変更管理** ― ビジネスのスピード、および技術の変化に合わせてアイデンティティ管理の変更を実装します。
- **業界標準ベース** ― 企業内のシステムと技術との相互運用性を保証 ― Select Identity は、完全な J2EE アプリケーションであり、多くのディレクトリサーバー、主流となっているいくつかのオペレーティングシステム、一般的に使用されているデータベースサーバー、ビジネス統合ツール、および Microsoft Exchange Server とともに動作します。また、PeopleSoft、SAP、その他のエンタープライズアプリケーションとも連携します。サポートされているプラットフォームおよび統合アプリケーションの現在のリストについては、HP の担当者にご確認ください。
- **同期化** ― インフラストラクチャ全体でアイデンティティデータの同期を維持します。
- **Web ベースアクセス** ― 本書で説明している主要なユーザーインタフェースとともに、ユーザーは Web サービスの Web ベースインタフェースを使用できます。詳細については、『HP Select Identity Web サービス開発者ガイド』を参照してください。

使用シナリオ : 概要

最も基本的なレベルにおいて、Select Identity ではどのようなロールでもサービスモデルにマッピングできるので、一般の RBAC ソリューションの機能と同じように動作します。

ただし、Select Identity ではロールの変更に簡単に対応でき、それと同時にプロセスの変更とその変更の委任を行うことができます。これは、多くの比較的速度の遅いロールベースアクセスの問題を軽減します。

最初は、単純なロールベースモデルを配布するように決定します。時間の経過とともに、必要に応じてより最適なまたは複雑なモデルへ簡単に移行したり発展させたりすることができます。サービスモデルに動的でコンテキストベースのロール割り当てを組み合わせることで、驚異的な柔軟性が得られます。

さらに、Select Identity には、単にロールだけでなく、すべての機能にわたって広範な委任を実現する機能があり、ビジネスプロセスを動的にスケーリングすることができます。サービスは個別に管理でき、特に、サービスおよびロールの所有権を委任できます。これにより、ビジネスまたはビジネスプロセスの部分をより詳細に管理し、他の部分はより一般的なモデルに置いた状態から始めることができます。

このセクションの残りの部分では、いくつかの Select Identity の可能性を示すシナリオの概要を説明します。

新規ユーザー

組織に新しい従業員が加わるときには、必ず数多くのプロビジョニングアクションが発生します。たとえば、新しい従業員の電子メールアドレスと Windows アカウントを割り当て、賃金および福利厚生システム、従業員ポータルなどへのアクセス権を与える必要があります。リストは長くて複雑なものになります。

新規ユーザーを追加する場合は、できるだけ速く、かつ効率的に必要なプロビジョニングを終了し、ユーザーが生産的な活動を開始できるように、また IT に過剰な負荷を掛けないようにしなければなりません。しかし、多くの組織では、新規ユーザーを追加するときに、すべての詳細を説明することに労力を費やします。

Select Identity を用いると、プロセス全体を自動化することができます。ユーザーアカウントの作成、パスワードの生成、複数のリソースへのアクセスのプロビジョニングは自動的に処理され、すべての必要なアクションおよび承認は正しい順序で効率的に行われます。

ユーザーの移動

時間が経つと、ユーザーは別の組織、場所、またはジョブに移動します。このシナリオは、多くの組織で、個人ユーザーとグループの両方に適用します。

ユーザーが移動するときは、それまでのすべての使用権が移動先の組織でも有効かどうかを確認しなければなりません。不要になった使用権は、遵守の目的のために削除します。生産性を維持するには、新しい状況でできるだけ速くユーザーをプロビジョニングすることが必須となります。

ほとんどのアイデンティティ管理ソリューションでは、ユーザーまたはユーザーグループの移動に対応することは、すべての使用権を正しく更新するためのコーディングを必要とする複雑な業務になります。この状況は、たとえば単にユーザーの場所が変わるだけといった、組織上の構造とは関係がない変更の場合にはさらに複雑になります。

Select Identity のアプローチは組織の階層を必ずしも反映したものではないので、動的な実装を配布するのは比較的簡単です。ユーザーは、コンテキストを通じて自動的にロールに割り当てられます。たとえば、ユーザーが新しいロケールに移動すると、ユーザーの人事レコードの変更をもとにアクセス権限の変更が行われます。

アカウントの終了

さらに時間が経つと、組織内のメンバーは広範囲のリソースへのアクセスを獲得します。しばしば、これらのリソースは地理的に分散しており、会社内の複数サブユニットの管理下にあります。

ユーザーが組織を去るときに、そのユーザーに関連するアカウントと使用権をすべて識別して終了することは簡単ではありません。このような「持ち主のいないアカウント」の存在を発見して解決するのは難しく、重大な脆弱性へとつながります。

Select Identity を使用していれば、ユーザーを終了するときに、そのユーザーの使用権を自動的に破棄し、使用していたアカウントを任意に無効にしたり削除したりできます。

また、終了処理をスケジュールすることもできます。たとえば、契約社員をシステムに追加したときは、契約期間に対応した終了日をすぐに作成できます。これには、契約社員の電子メールアカウント、データベースアカウント、その他の許可されているすべてのアカウントの終了が含まれます。これは、持ち主のいないアカウントが原因で発生するセキュリティ上のリスクを未然に防ぎます。

合併および買収

企業には、独立したビジネス単位の統合や買収が必要な場合があります。

買収または合併される会社の従業員は、それまでのリソースの多くに引き続きアクセスしたり、ビジネスプロセスを継続して使用したりする必要があるかもしれません。

さらに、買収に適応するため、親会社のプロセスの変更も実装する必要があるかもしれません。

管理システムが初期の配置から会社内の新しいグループへと拡張される場合に、同じシナリオが適用されるので、既存のサービスとリソースにアクセスできます。

従来のアイデンティティ管理システムを使用する場合、既存の組織と一貫性のある方法で新しい組織を実装し、新しいグループのために必要なカスタマイズを行うのは非常に大掛かりな作業になります。新しいロール、ルール、ワークフロー全体を定義、実装、およびテストしなければなりません。

Select Identity では、これらの管理オブジェクトの定義をサービスという単一のエンティティにグループ化します。既存のサービスの複製を元に新しいサービスを作成し、特定の状況に従ってカスタマイズすることができます。その後、新しいユーザーの一括ロードを介して新しいサービスにデータが入ります。Select Identity は、各ユーザーに必要なすべてのプロビジョニングアクションを自動的に計算して適用します。

買収された会社またはビジネス単位は親会社に統合されているので、既存のプロセス、ワークフローなどは類似していることが予測できます。ワークフロー承認や使用権、または買収されたリソースの追加といったアイテムにわずかな変更を行うことによって、Select Identity は新しいグループをすぐに適応させます。

リソースの変更

リソースを追加、更新または使用停止にする場合、または 1 つまたは複数のビジネスプロセスによって使用または共有されている既存のリソースを変更する場合は、その変更の結果をすべて明らかにすることは困難です。その変更が既存のワークフロー、ロール、ルール、およびフォームにどのように影響するかを知る必要があります。これは、ロールおよびルールをリソースに関連付ける必要があるときに、特に言えることです。

これらすべてのアイデンティティ管理オブジェクトをリンクする方法、およびオブジェクトの関係を管理する方法が必要です。変更によるすべての影響を認識していないと、費用や時間のかかる問題に遭遇し、作業の進行が妨げられることがあります。

サービスには、サービスに関連するリソース、使用権、ワークフロー、ポリシー、およびその他のアイデンティティ管理要素のすべてがカプセル化されているので、計画されたリソース変更の影響をすぐに確認することができます。

新しいリソースに対し Select Identity でまだ定義されていない新しい属性が必要な場合

- 属性を追加します。
- リソース属性に属性をマッピングします。
- サービスへ属性を追加します。
- 新しい属性を含むように関連するフォームを変更します。

使用権の変更

通常、リソースを変更するには、任意または直接的にユーザーに割り当てられる使用権を変更する必要があります。これは多大な労力を必要とし、時間もかかり、エラーが発生しやすいプロセスです。

Select Identity では、コーディングの労力なしに即座に任意の使用権を追加することができます。Select Identity は、オプションおよび必須の属性に基づいて自動的にフォームを生成します。

リソース変更中の使用権の管理には、Select Identity の 2 つの基本ステップがあります。

1 リソースの定義内に新しい属性を追加する。

2 サービスのルートサービスロール内に固定および任意の使用権を指定する。(サービスロールの詳細については後述します。ここでは、サービスロールがサービスの一部または全部の使用権を持っていることを覚えておいてください。)

サービスの固定および任意の使用権は、サービス階層全体を通して継承されます。

必要に応じて従属するロールにさらにカスタマイズを加え、それらのロールに固有の要件を処理することができます。フォームは自動生成され、サービス固有のものになります。

複雑で動的な環境の管理

多くの場合、ユーザーの編成は、会社の組織図に描かれているものとは異なった階層に従います。

今日の市場に出ているほとんどのソリューションは、配布の開始時点で定義された 1 つの階層に RBAC を合わせます。これは、既存のディレクトリ配布または人事モデルにもとづく基本的な組織階層です。また、抽象的なロールまたはルールを介したカスタマイズにより例外を処理している可能性もあります。この場合、初期の段階で潜在的に迅速な配布を行うことができますが、組織が異なる階層を管理する必要があるときに、問題が顕在化します。

純粋な RABC ソリューションでは、ロール階層はしばしば単一モデル (通常は組織の階層) に密接に結合されています。このような密結合はロールの価値を制限することになります。それは、場所、役職、または部署といった他の属性に基づいてロール階層を定義することが難しいからです。

他の階層を多くのルールを使用して作成することは可能ですが、コストが高くなり、結果として複数の一貫性のない階層になってしまうことがあります。

Select Identity は、企業がユーザーの編成を行うのに採用する方法 (場所、職務、組織、またはその他の方法) に関わらず、1 つの一貫したサービス階層を使用します。

Select Identity では、特別なコーディングやプログラミングを使用せずに、複数の異なる階層を、場所、部門、職務などのコンテキスト属性に基づいて簡単に作成できます。また、異なる階層に基づく委任モデルを簡単に配布することもできます。

3 Select Identity のサービスベースモデル

この章は Select Identity の最も重要な概念である**サービス** に重点を置いて説明します。

この概念は Select Identity 以外のアイデンティティ管理ソ。リューションにはないもので、この概念を理解することが配布を成功に導く鍵となります。RBAC など、他のアイデンティティ管理モデルの概念および方法論を身に付けた方にとって、Select Identity について学習することは、価値のある挑戦といえます。

なぜサービスなのか

組織に属する人は、種類の違うさまざまなビジネスプロセスおよびサービスに従事しています。以下に例を示します。

- 従業員は、賃金および福利厚生サービスにアクセスする必要があります。
- 会社の会計係は、財務情報および関連するアプリケーションにアクセスする必要があります。
- マネージャは、従業員の実績レコードを更新できる必要があります。

各サービスまたはプロセスは、固有の使用権を必要とするアプリケーションまたは他のリソースを使用します。これらの使用権は、しばしばユーザーの特定のニーズに特有なものです。新しいユーザーのプロビジョニング、または新しいサービスの投入には、複数の新しい関係と、場合によっては新しい例外ルールセットの追加作業が含まれることがあります。これらのタスクは、エラーやセキュリティ上の過失を招く可能性が高く、通知メッセージの内容が疑わしいために混乱が発生する傾向があります。

Select Identity のサービスベースモデルでは、アイデンティティとアクセスの管理をビジネスプロセスに合わせます。そのため、組織の内部および外部のリソースにアクセスするすべてのユーザーおよびその使用権の管理が非常に簡単になります。

Select Identity で定義するサービスとは、1 つのエンティティに関連するリソース、使用権、ワークフロー、ポリシー、およびその他のアイデンティティ管理要素をすべてカプセル化したものです。この高度の抽象化によって、ドメインに固有の複雑な関係を管理するジョブが大幅に単純化されます。

サービスベースモデルでは、従業員の昇進など、ルーチン化された変更処理は簡単に行うことができます。さらに重要なのは、部署の立ち上げ、分割、または部署の統合など、より難しい問題への対応が簡単になるということです。最も注目すべきは、Select Identity のサービスベースモデルでは、会社の吸収合併のような非常に重要で大きなタスクにも、移行の促進と単純化を可能にするツールによって対応できるということです。

サービスの 3 つのポイント

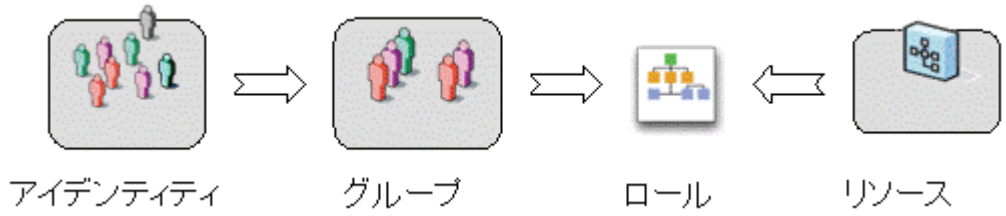
サービスについて理解するためには、以下の 3 つのポイントがあります。

- システム、プロセス、およびアプリケーションが**サービス**を構成します。
- ユーザーは、高度な論理**コンテキスト**を構成します。
- サービスへのアクセスは、**サービスロール**によって制御されます。

サービスについて

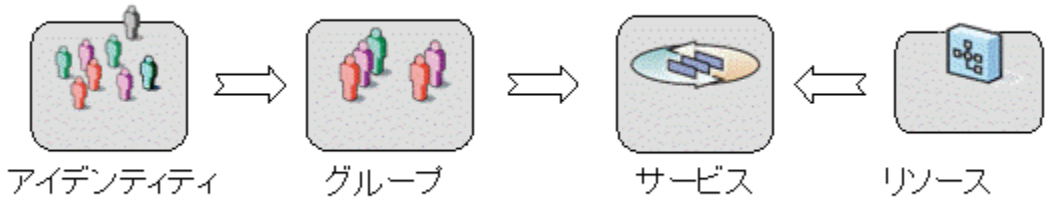
RBAC ソリューションでは、ロールが中心的な概念となります。ロールは、ユーザーのグループを、適切な**リソース**の使用権にリンクします。リソースは、それらの使用を制御するアイデンティティ情報を記録して使用するシステムやアプリケーションなどです。

図 1　　ロールは、ユーザーのグループのリソースおよび使用権を定義します。



Select Identity では、サービスが中心的な概念となります。サービスは、ユーザーのグループを適切なリソースの使用権にリンクします。

図 2　　サービスは、ユーザーのグループのためのリソースおよび使用権を定義します。



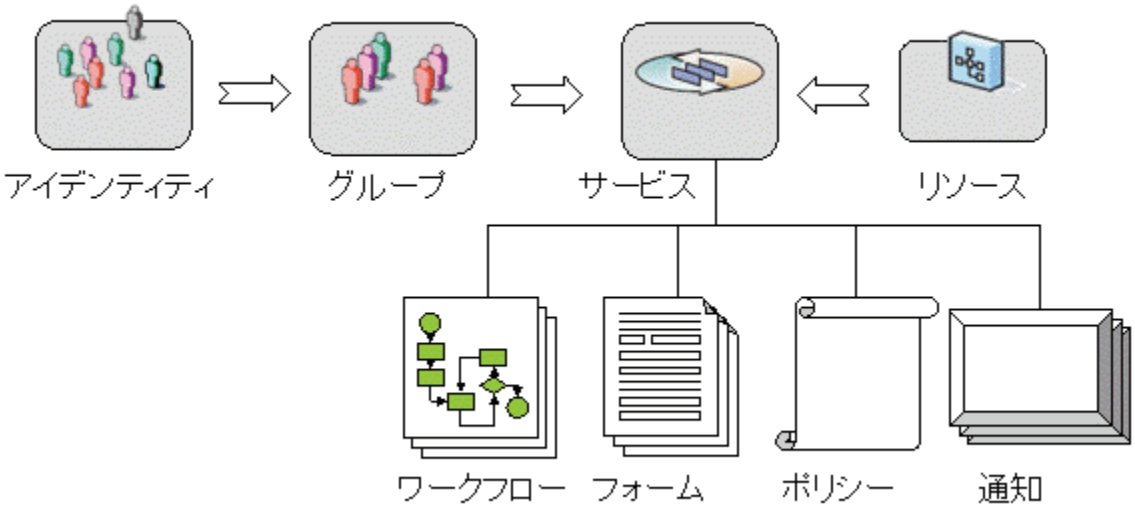
相違は、モデルの持つ強力さです。

サービスを RBAC スタイルのロールに直接マッピングすることは可能でも、それほど有用ではありません。そのようにしても、モデルに大きな違いは見られないでしょう。しかし、サービスの概念には、ロールでは利用できない多くの機能が含まれています。

サービスには、次のように多くの管理機能が組み込まれています。

- **ワークフロー**— 承認、プロビジョニング、およびユーザー登録
- **フォーム** —ユーザー属性の入力
- **ポリシー** —セキュリティ、除外、およびパスワード設定の定義
- **通知** — 警告、更新、および検証

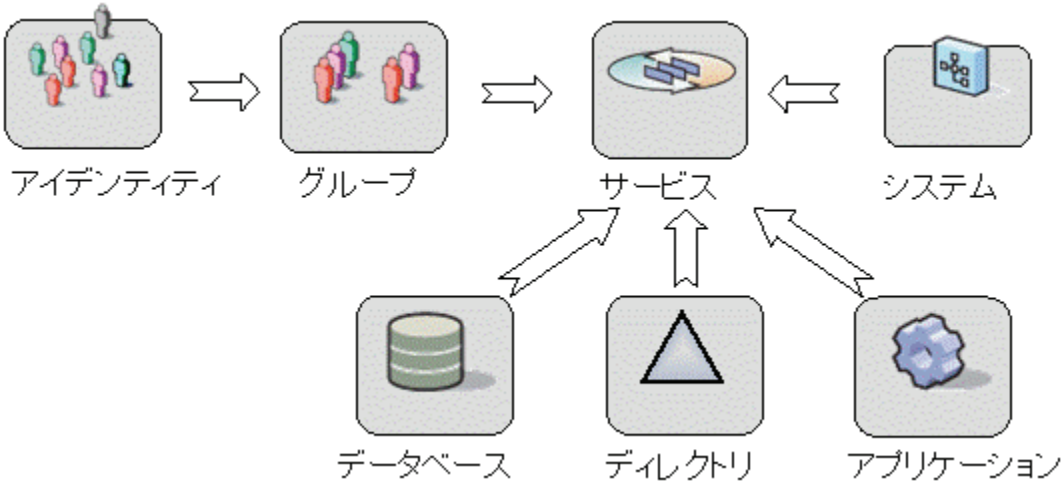
図 3　　サービスには、アイデンティティ管理の重要な考え方が取り入れられています。



サービスには、異なるリソースをいくつでも含めることができます。

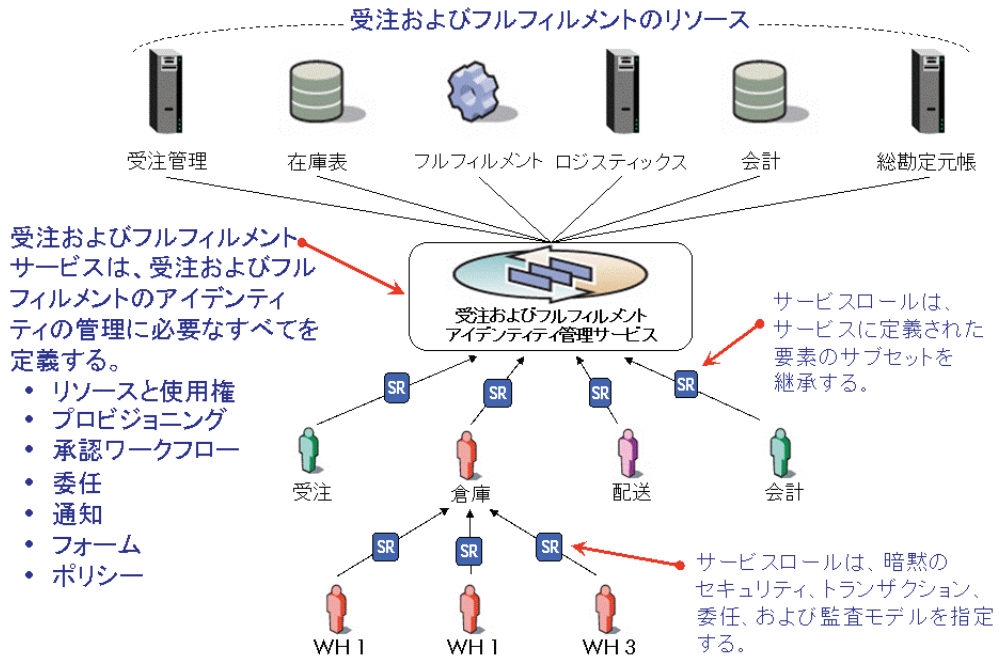
- データベース
- ディレクトリ
- アプリケーション
- Web サービス
- メッセージングシステム
- オペレーティングシステム
- ポータル
- ネットワークデバイス
- ロールベースのセキュリティシステム
- 非デジタルコンポーネントに対してもヘルプデスクのチケットが生成されるので、IT 部門のスタッフはプロビジョニングを手作業で行うように指示されます。

図 4　　単一のサービスに関連付けられた複数のリソース。複数のサービスでリソースを共有することができます。



次の図では、ある大規模な例を使ってこれらのポイントを説明します。これは、大規模な組織での典型的な受注およびフルフィルメントのプロセスを示しています。Select Identity では、サービスベースの管理内で、グループ、ロール、およびリソースを緩やか (密にではなく) に結合しています。緩やかな結合とは、さまざまなユーザーグループまたはロールが、高度の抽象化、すなわちアイデンティティプロビジョニングサービスで結合されていることを意味しています。この例では、サービスは「受注およびフルフィルメント」アイデンティティ管理サービスと呼ばれ、ビジネスプロセスを正確に反映しています。

図 5　　典型的な「受注およびフルフィルメント」アイデンティティ管理サービス



ユーザーグループは、「受注およびフルフィルメント」アイデンティティ管理サービスを通じて間接的にリソースへアクセスします。そのため、新しい倉庫作業者は、「受注およびフルフィルメント」アイデンティティ管理サービスへのアクセスに登録し、続いて倉庫での業務を実行するために必要なすべての使用権がプロビジョニングされます。また、出荷代理店もサービスへのアクセスに一度登録しますが、プロビジョニングと制御は別のサービスロールを使用して行われます (24 ページの「サービスロールについて」を参照してください)。

各サービスロールは、「受注およびフルフィルメント」サービスの機能のサブセットを使用し、それぞれが異なる使用権、ワークフロー、ポリシーなどを持っています。

このモデルの大きな利点は、「受注およびフルフィルメント」アイデンティティ管理サービスが、すべてのリソースと使用権、すべてのプロビジョニングと承認ワークフロー、委任オプション、通知、フォーム、およびポリシーの定義をそのサービス内にすでに持っていることです。

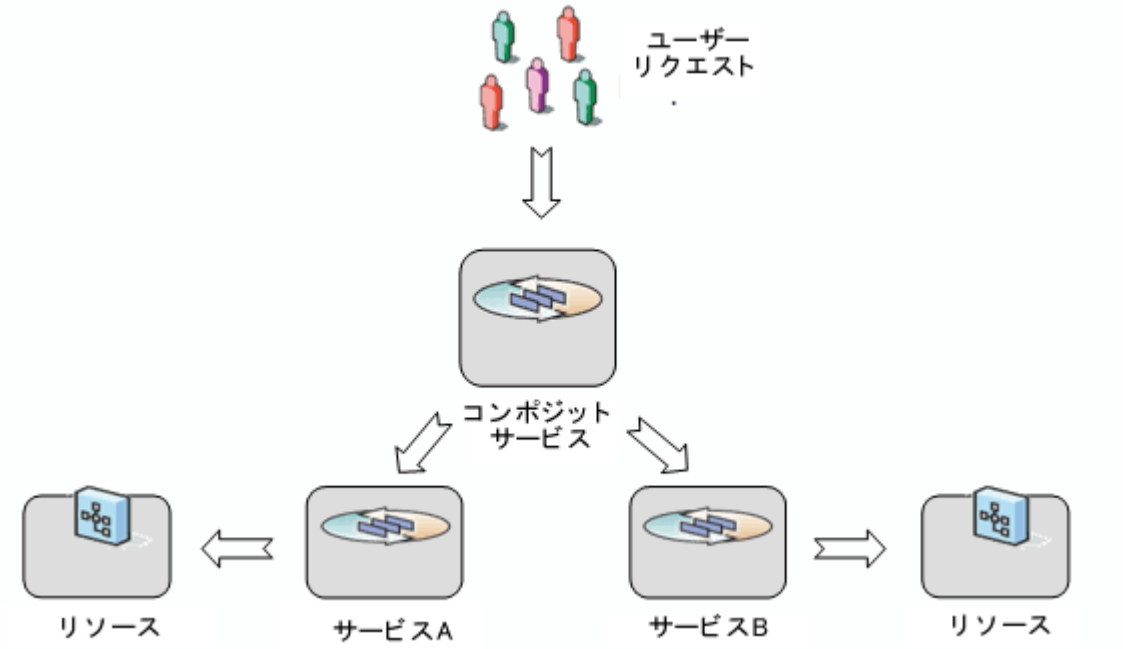
これにより、変更を簡素化するシステムが作成され、変更管理の一貫性が保証されます。

このアイデンティティ管理サービス内に新しいサービスロールを定義するのは簡単です。IT 部門のスタッフや専門のセキュリティ管理者を置く必要がなく、新しいロールまたはルールの定義を理解してテストするためのモデル作成ツールも必要ありません。

また 1 つのユニットに複数のサービスを組み合わせるために Select Identity のコンポジット サービス機能を使用できます。コンポジット サービスを作成し、複数の共通の属性を更新するために 1 つのワークフローで 1 つのリクエストを使用する機能を提供することにより、サービス登録のプロセスを簡素化できます。

たとえば新しい従業員が 5 つの異なるサービスで登録を必要としている場合、5 つのサービスを含むコンポジット サービスを作成できます。個別のサービスを登録するのではなく、従業員は 1 つのコンポジット サービス リクエストとワークフロー承認を通じて 5 つのサービスに登録できます。

図 6　　コンポジットサービス



コンテキストについて

コンテキストは、選択したアイデンティティプロファイルの属性値に基づいて、ユーザーの論理的なグループを定義します。ユーザーのコンテキストへのメンバーシップ (またはコンテキスからの除外) は、ユーザーのコンテキストアイデンティティプロファイルの属性値に依存します。

ある個人がコンテキストのメンバーかどうかを判断するため、Select Identity ではユーザーのアイデンティティプロファイル内のコンテキストの属性値を、そのコンテキストに定義されている値と比較します。一致すれば、そのユーザーは事実上そのコンテキストのメンバーです。

たとえば、サービスを利用するユーザーの国によって変化する給与計算サービスを考えてみます。従業員の Country 属性に依存する、イギリス、インド、および中国のコンテキストを作成します。この例では、従業員の Country 属性がコンテキストを決定します。最終的に、ユーザーがアクセスできるリソースおよび使用権が決定されます。

属性に基づいてコンテキストのメンバーシップを割り当てることによって、アイデンティティプロファイルへの変更を行うとサービス内のアイデンティティのコンテキストも変更されるようになります。つまり、新しいコンテキストに基づいて、ユーザーには異なるリソースのセットと使用権へのアクセスが許可されます。

コンテキストは階層的な構造にすることもできます。たとえば、運送業者のサービスでは、Driver という親コンテキストを定義し、その下に Long-Haul と Local ドライバのための異なる子のコンテキストを定義します。コンテキストのメンバーは、コンテキストに固有のワークフロー、通知、属性、およびリソースを共有します。

ユーザーのコンテキストは、最終的に、ユーザーのコンテキストに関連付けられている Long-Haul Driver などのサービスロールに基づいて、ユーザーが受け取る権限とアクセス権を決定します。

サービスロールについて

サービスは、そのリソースとして特定のシステムおよびアプリケーションを識別し、コンテキスト属性の値に基づいてコンテキストグループユーザを識別します。ここでコンテキストのメンバーは、特定の使用権を使ってそのサービス内のリソースにアクセスする必要があります。

コンテキストのメンバーをサービス内の特定の使用権にリンクするのが**サービスロール**です。つまり、サービスロールはさまざまな管理者およびユーザーのアクセス権を統制するための制御点となります。

コンテキストの概念をサービスロールと組み合わせることにより、Select Identity は、ビジネスプロセスの変更に適応する強力な機能を発揮します。

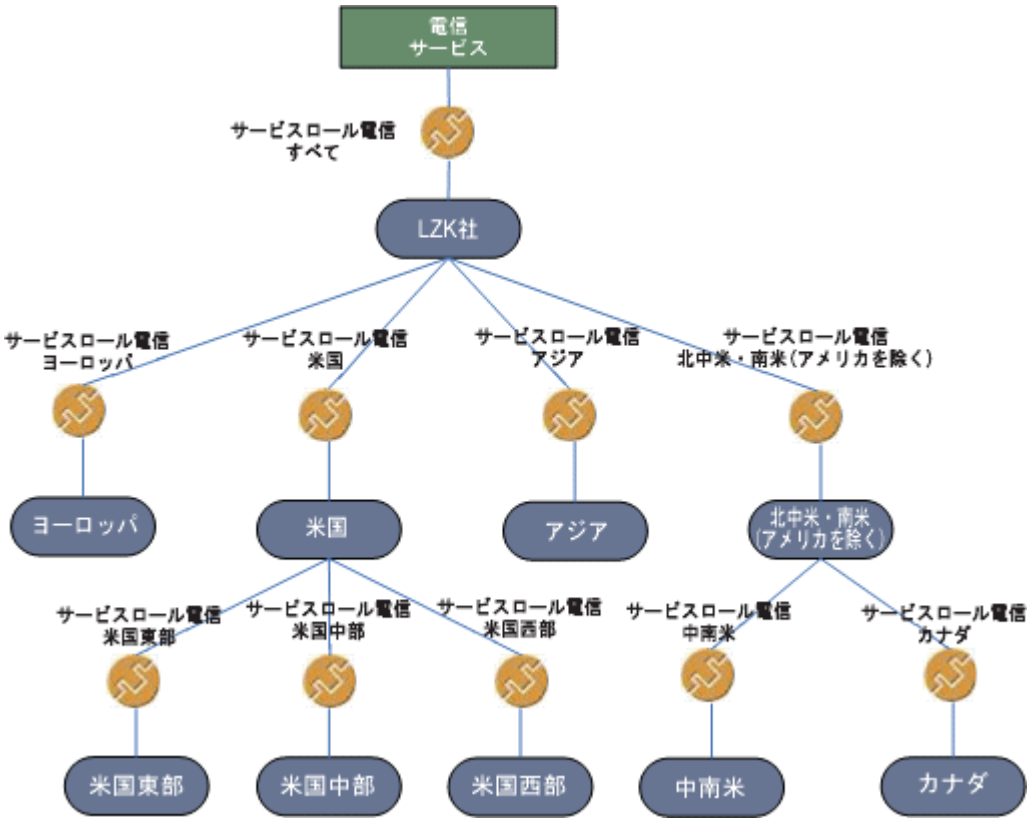
サービスを定義するとき、そのサービスのサービスロールの階層を定義することが重要な手順の 1 つになります。サービスロールには、それぞれ固有の目的があります。サービスロールは、そのメンバーに対してサービスのリソースへのアクセスを提供し、それらのリソースの特定の使用権を許可します。ルートの配下にあるサービスロールの各層は、ルートを継承します。

固定属性の継承は加法的であり、子は常に親の属性を継承し、さらに子レベルで定義される追加の固定属性を取得します。オプション属性の継承は、減法的です。すなわち、子レベルでオプションとなるものは、親レベルで指定されたオプション値のサブセットでなければなりません (潜在的にはまったく同じオプション値となることもあります)。

サービスロールの階層は、異なる企業や場所でサービスを共有するための安全な方法を作成します。コンテキストを使用して、さまざまな会社または場所にわたってだれがどのユーザーを管理できるのかを決定できます。

図 7 は、単純なサービスロール階層を示しています。

図 7　　サービスロールの階層



LZK Corporate でのルートサービスロールは、「電信送金」サービスの使用権をすべて定義しています。階層の下位レベルが親サービスロールから継承します。しかし、それぞれの子には、より制限されたオプションの使用権、親にはない使用権、および親と同一の固定の使用権があります (詳細については、29 ページの「固定の使用権とオプションの使用権」を参照してください)。

このような階層によって、組織内の実際のサービスロールを表現することができます。また、親に許可されていない使用権は子にも許可されないので、このような階層はロールのプライバシーとセキュリティも保護します。

4 Select Identity の中心的な概念

前の章では、Select Identity の全体像と基本的な構造を理解するのに役立つ知識体系について説明しました。

この章では、これまで紹介してきた多くの概念についてさらに詳細に解説します。特に、この章では次の概念についてさらに深く掘り下げます。

- サービス、サービスロール、およびコンテキスト
- 30 ページの「管理ロール」
- 32 ページの「リソース管理」
- 33 ページの「ワークフロー管理」
- 34 ページの「設定の承認」
- 34 ページの「ユーザー管理」
- 38 ページの「リクエストステータス」
- 38 ページの「セキュリティ管理および監査レポート作成」
- 39 ページの「設定の複製」

サービス、サービスロール、およびコンテキスト

第 3 章「Select Identity のサービスベースモデル」では、Select Identity の**サービス**、**サービスロール**、および**コンテキスト**という用語およびその概念について紹介しました。これらは、Select Identity の中で最も基本的で重要な概念です。

サービス

Select Identity では、サービスは現実のビジネスプロセスまたはサービスに直接対応しています。単一のオブジェクトでは、サービスは実際のサービスに関係するすべてのアイデンティティ管理要素をカプセル化します。

- リソース
- 使用権
- ワークフロー
- ポリシー
- プロビジョニング
- 委任
- 通知
- フォーム

たとえば、カスタマサポートというサービスがあり、カスタマリレーションシップマネージメントや Internet のサポートポータルシステムなど、ヘルプデスクに関連するアイデンティティ管理コンポーネントがすべて含まれているとします。

サービスロール

サービスロールは、Select Identity の抽象概念で、ユーザーの論理グループが Select Identity サービスの使用権のサブセットにどのようにアクセスするのかを定義します。たとえば、Sales サービスは、East、Central、West の 3 つのサービスロールがあります。これらのサービスロールはさらに分割することもできます。たとえば、サービスロール West には、Northwest および Southwest という 2 つの下位サービスロールが含まれることがあります。サービスに含めることのできるサービスロールのレベル数に制限はありません。

サービスには、一般にさまざまなユーザーが、それぞれ異なる方法でアクセスします。たとえば、倉庫主任と会計係はまったく異なるニーズによって「受注処理およびフルフィルメント」サービスにアクセスします。これらの異なるニーズには別々のサービスロールが必要です。

サービスロールは、サービスのユーザーに対して、ユーザーのコンテキストに関係するすべてのものへのアクセスを与える安全なフレームワークを作成します。サービスのさまざまなユーザーの要件を満たすサービスロールを定義および作成する必要があります。

サービスロールを作成するときは、そのサービスロールに関係するワークフロープロセスおよび通知ポリシーを割り当てます。それぞれのサービスロールには、それ自身の使用権のセットを与えることができます。これはサービスに定義された使用権のサブセットです。また、サービスロールの下のサービスにアクセスするユーザーに対して固定された属性を定義できます。

サービスロールは階層構造になっています。最上位レベル、つまり「ルート」のサービスロールは使用権の全セットを定義します。階層の下位レベルは、ルートサービスロールを継承します。それぞれの子には、その親よりも制限されたオプションの使用権、および親と同一または親よりも多くの固定の使用権があります。これは、さまざまなユーザーや地理的に離れた場所、または異なる会社の間でサービスを共有するための安全な方法となります。

しかし、単にサービスロールを定義するだけでは十分ではありません。各サービスロールをその対象ユーザーに関連付けるしくみが必要です。

コンテキスト

Select Identity のコンテキストは、特定のサービスロールを使用して特定のサービスにアクセスできるユーザーの論理グループです。コンテキストは、2 つの重要な機能を提供します。

- まず、コンテキスト はプロファイル内の識別属性を共有するユーザーのグループを定義します。

  たとえば、「福利厚生」サービスに、「US Employees」、「Argentina Employees」、および「Japan Employees」というコンテキストがあるとします。それぞれのグループは、プロファイルの「CountryOfResidence」属性に対する特定の値を共有する従業員で構成されます。

  「受注処理およびフルフィルメント」サービスには、「Warehouse」および「Accounting」というコンテキストを定義します。コンテキストのメンバーはプロファイル内の「Job Title」属性の値に従って割り当てられます。

  Select Identity 管理者は、ユーザーのグループをコンテキスト属性値で管理します。

- 次に、コンテキストはそのメンバーを 1 つまたは複数のサービスロールにリンクします。

  それぞれのコンテキストには、サービスロールが 1 つ割り当てられています。これは、サービスのユーザーがあるコンテキストのメンバーとして識別されたとき、そのユーザーは、コンテキストに割り当てられたサービスロールに基づいてサービスにプロビジョニングされることを意味します。

要約すると、ユーザーがサービスに割り当てられるとき、ユーザーがどのコンテキストに属するかは、アイデンティティ属性によって判断されます。コンテキストは、どのサービスロールをそのメンバーに適用するかを決定します。

つまり、ユーザーがサービスに登録するとき、ユーザーは、そのコンテキスト属性に基づいてサービス内のリソースの適切な使用権を自動的に取得します。

後日、ユーザーの属性が変更される場合があります。たとえば、ユーザーが「CountryOfResidence」属性に基づいてコンテキストメンバーシップを決定するサービスのメンバーだとします。ユーザーが別の国に移住した場合、この属性の値は変更されます。Select Identity は、元のコンテキスト内のユーザーのメンバーシップを自動的に終了し、新しい「CountryOfResidence」に基づいてユーザーを別のコンテキストのメンバーにします。ユーザーは、そのコンテキストのサービスロールに適したアクセスを自動的に取得します。

コンテキスト変数の指定にワイルドカードを使用する方法については、『HP Select Identity 管理者ガイド』を参照してください。

固定の使用権とオプションの使用権

使用権は、ユーザーに許可されるリソース権限を抽象化したものです。使用権はリソースに固有で、アカウント ID、ロールメンバーシップ、グループメンバーシップ、アクセス権および特権などがあります。使用権はまた、特権、権限、またはアクセス権とも呼ばれます。

Select Identity では、サービスロールに基づいて使用権のセットを提供します。使用権には、固定のものとオプションのものがあります。

サービスロールは、サービスロールが作成されたサービスに属します。任意のサービスロールで使用できる使用権は、サービスレベルまたは属性レベルで定義されます。サービスロールは、サービスに属する 1 つまたは複数の使用権を割り当てることができますが、サービスに属さない使用権を割り当てることはできません。言い換えると、あるサービスロールのレベルで使用できる使用権は、親のサービスロールまたは属性で厳密に規定されます。

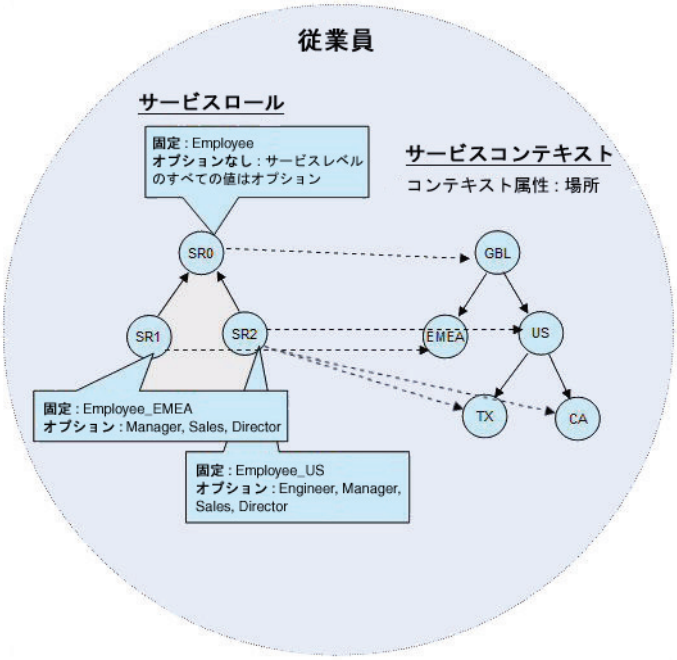
固定の使用権は、特定のユーザーに自動的に許可される使用権で、ユーザーのアイデンティティに関連付けられたコンテキスト (つまり、サービスロール) によって決定されるものです。固定使用権は、サービス内に作成された子サービスロールに自動的に継承されます。すべての子サービスロールはこの使用権を継承します。

オプションの使用権は、特定のユーザーが利用できる使用権で、ユーザーのアイデンティティに関連付けられたサービスロールおよびコンテキストによって決定されるものです。ユーザー自身が、この使用権を選択するかどうかを決めることができます。

オプションの使用権はサービスロールで定義できます。ルートサービスロールは、そのレベルに定義がない場合、サービスレベルで定義されたすべてのオプションの使用権を継承します。子サービスロールは、そのレベルに定義がない場合、親サービスロールからオプションの使用権を継承します。ただし、子が継承できるのは、親サービスロールレベルで定義されたオプションの使用権のサブセット (おそらくすべて) に限られます。

たとえば、業務に `Employee Service` が含まれていて、このサービス内の各ユーザーが特定のリソースに対する `Employee` 使用権を必要としているとします。アメリカ合衆国のユーザーは、`Employee US` 使用権を必要とし、同時に `Engineer`、`Manager`、`Sales` または `Director` の中の 1 つまたは複数の使用権も持つことができます。ヨーロッパ、中東、およびアフリカ (EMEA) 地域のユーザーは、`Employee EMEA` 使用権を必要とし、同時に `Sales`、`Manager`、または `Director` の中の 1 つまたは複数の使用権を持つこともできます。30 ページの図 8 は、この使用権の設定と、サービスロールがサービスコンテキストにどのようにアタッチされるかを示したものです。

図 8　　従業員サービスと使用権の例



ここでは、US コンテキストに属するユーザーには、Employee および Employee US 使用権が自動的に与えられます。管理者は、Engineer、Manager、Sales または Directror の各使用権から選択することができます。TX (Texas、US) または CA (California、US) に属するユーザーも同様です。

繰り返すと、すべての利用可能な使用権はすべて、サービスレベルで定義されます。その使用権のセットの中で、サービスロールはどれが固定でどれが任意かを決定します。

デフォルトでは、ルートサービスロールは、サービスに存在するオプションの使用権のすべてを持ちます。異なるサービスロール内の使用権は、ユーザーの異なるコンテキストグループに適するように制約できます。サービスロールは、親と子の階層で構成されます。子は親が使用できる、固定の使用権すべてとオプションの使用権のサブセットを受け取ります。子は、その親よりも多くのオプションの使用権を持つことはできません。

固定およびオプションの値の概念は、使用権以外の属性にも適用されます。値を固定することも、値のリストをすべての属性 (以下を除く) に対して制約することもできます。

- グローバル一意識別子 (GUID) および UserName 属性は固定にしたり制約したりすることはできません。
- 属性タイプが Password、またはプリミティブタイプが Date の場合は、この属性は固定にも任意にもなりません。

サービスレベル制約は、[**サービス属性値**] ページ上の各属性に対して設定されます。制約は、1 つのサービスロールだけではなく、サービス全体に適用されます。

管理ロール

管理ロールは、管理者が Select Identity 内で実行できる機能とアクションを決定します。

管理ロールは、管理サービスを通じて使用可能になります。つまり、ユーザーが管理サービスに割り当てられると、ユーザーは管理権限を持つことになります。

Select Identity 管理者の役割を果たすユーザーを管理サービスに追加できます。ユーザーを管理サービスに割り当てる際には、以下を選択します。

- 対象ユーザー
- 管理サービス
- 利用可能な機能とアクションのセットを指定する、1 つまたは複数の管理ロール
- 1 つ、数個、またはすべてのサービス
- 各サービスに対しては、コンテキスト値のサブセット、または `All Contexts`

Select Identity は、システム内で実行される機能やアクションを反映した 4 つの管理ロールを提供します。これらのロールはそのまま使用することもできますが、必要に応じて編集したり、各自のビジネスニーズを反映したより便利なロールを作成することもできます。4 つの基本ロールは、以下のとおりです。

- **End-User** − Select Identity で提供されるサービスのユーザーである人を示す。すべてのユーザーは、少なくともこのロールを持ちます。このロールは、権限のデフォルトセットを付与します。このロールを変更することで、デフォルトの権限を変更できます。End-User ロールは、技術的には管理ロールです。しかし、通常はそのユーザーのプロファイルの詳細を管理する以上の管理権限を持ちません。
- **Workflow Approver** − ユーザーアカウントへの変更を承認する権限を与えられたユーザーを示す。Select Identity では、このロールは承認タスクによって割り当てられたユーザーに自動的に付与されます。このロールが付与されたユーザーは、承認者のコンテキスト内のユーザーに対するユーザーアカウントの追加、変更、または削除を承認することができます。
- **Configuration Approver** − Select Identity への設定変更を承認する権限を与えられたユーザーを示す。詳細については、34 ページの「設定の承認」および『HP Select Identity 管理者ガイド』を参照してください。
- **Concero Sys Admin** − Select Identity のすべての設定および管理機能を持つユーザーを示す。このレベルのアクセスは、わずかに限られた人数に制限する必要があります。

追加可能なロールには、以下のような例が考えられます。

- Workflow Engineer − この特定のアイデンティティ管理タスクを実行する人を示す。
- User Administrator − ユーザーを管理することができる人を示す。
- Resource Administrator − リソースを管理することができる人を示す。
- Access Manager − サービスへのアクセスをユーザー (コンテキスト) のグループに許可する権限を与えられた人を示す。

管理ロールを持つ人は、その権限を別の管理者に委任することもできます。これは、一般に休暇や長期欠勤などの状況に対応するために行われます。

管理ロールは、特定のサービスを管理するために制限することはできません。

一方、管理サービスは、ロールを固定値に設定することによって、ユーザーに対する特定の管理ロールを定義できます。

管理サービス内のサービスロール

Select Identity では、管理サービス内のサービスロールを定義することによって、管理者の階層を作成することができます。サービスロール階層では、下位レベルほど多くの機能制限があります。これにより、管理責任および権限の一部を組織のより下層に移して、上位レベルの人員の負荷を軽減することができます。必要に応じて、管理権限の範囲を内部ユーザー、顧客、およびパートナーに割り当てることができます。

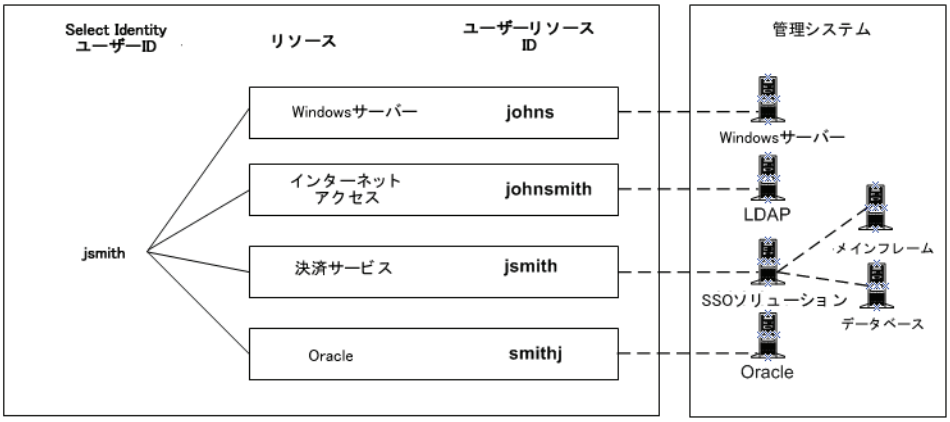
リソース管理

Select Identity では、すべてのリソース (システム、アプリケーション、ディレクトリ、データベースなど) はユーザーデータのリポジトリとして扱われ、このリポジトリに対してアカウントや使用権の追加、変更、削除が行われます。

Select Identity では論理 ID が作成され、ユーザーリポジトリに含まれるアイデンティティに対してリンクされます。リソースが環境内にいくつあるかに関係なく、Select Identity はユーザーのアイデンティティ情報を含むリソースすべてに渡り 1 つに統合されたユーザービューを作成します。ユーザーが退職したり、他部門へ異動、またはジョブを変更した場合には、Select Identity はそのユーザーがアカウントと使用権を持っていたリソースをすべて追跡し、適切な変更を加えます。

図 9 では、ユーザー (John Smith) に Select Identity ID (jsmith) が割り当てられ、その ID がすべてのユーザーリソース ID にリンクされています。これにより、管理システムにアクセスできます。

図 9　　Select Identity リンクの例



コネクタは、Select Identity とリソースの間の通信を確立するために使用されます。コネクタとは、リソース依存のプロトコルを使用してリソースにコマンドを送信するプログラムであり、Select Identity とリソースの間の通信チャネルとして機能します。

- 環境内のリソースの種類ごとにコネクタを配布します。

コネクタを配布しておくと、環境内のユーザーリポジトリの接続情報を指定するだけで、各リポジトリへのブリッジが作成されます。その後、Select Identity は管理権限を使用して、各リポジトリ内のユーザーデータを管理します。

リソース間でのアイデンティティデータの同期

たとえば、結婚によって名前が変わる場合を考えます。このようなイベントを管理するために、Select Identity では、変更を 1 回入力すれば情報がそのユーザーに関連するすべてのリソースに反映されるようになっています。

これを実現するために、Select Identity は 2 つのクラスのリソースを定義します。

- 信頼できるリソースは、重要なユーザーアイデンティティアカウントおよび属性値の「マスター」ソースと見なされます。信頼できるリソースの例は、従業員データを格納した人事サーバーです。この「マスター」ソースは、信頼できるリソースとして、他のリソースと主な従業員データを共有できます。
- 信頼できないリソースは、通常、信頼できるリソースにあるユーザーのアイデンティティの重要な側面と同期をとる必要があり、また、他のリソース固有のアイデンティティデータを含んでいます。信頼できないリソースの例は UNIX® のリソースまたはアカウントで、シェルやホームディレクトリとともに (信頼できるリソースから得た) 個人の姓と名を含んでいます。

Select Identity では、結婚によるユーザー名の変更など、重要なユーザー属性の変更に関して信頼できないリソースを更新する目的で信頼できるリソースを使用します。詳細については、『HP Select Identity 管理者ガイド』を参照してください。

また、属性の同期プロパティを正しく設定している場合、信頼できないリソース間でもほかのユーザー属性の同期をとることができます (詳細は『HP Select Identity 管理者ガイド』を参照してください)。たとえば、UNIX ユーザーがそのシェルを変更する場合、それに応じて Select Identity を更新できます。このプロセスはアカウント調整と呼ばれ、さまざまなリソース間でアカウントデータの同期を維持することができます。

アカウント調整では、外部的にアカウントに対して行った変更に合わせて Select Identity のアカウントを自動的に更新し同期を取ることができます。管理者は、リソースで行われた変更を調整するように Select Identity を設定することで、リソースのアカウントと Select Identity のアカウントの同期を取ることができます。Select Identity では、信頼できるリソースと信頼できないリソース両方について変更を調整できます。

たとえば、`LastName` などの属性を、人事アプリケーション (信頼できるリソース) 内で変更が発生した場合だけに Select Identity で変更されるようにすることができます。ただし、ユーザーの権限や使用権は、関連する属性の同期プロパティの設定によって、信頼できないリソースから更新することもできます。Select Identity では、どちらのタイプのリソースからの更新も可能です。Select Identity は、リソースに対するアカウントデータを定期的に自動調整できます。組織の状況に合わせて、自動調整の頻度は、月、週、日、時、分の単位で任意に設定できます。

調整については『HP Select Identity 管理者ガイド』を参照してください。

ワークフロー管理

ワークフローとは、ユーザーによるサービスアクセスリクエストが Select Identity によって承認およびプロビジョニングされるプロセスです。

たとえば、従業員がマネージャに昇進した場合、他の従業員を管理するために企業の HCM システムにアクセスする必要があります。新たな責任を果たせるよう、その従業員に対して新しい使用権を付与する必要があります。従業員がそれらのシステムにアクセスできるようにする前に、上級管理者がアクセスリクエストを承認し、関連システムで従業員が作成される必要があります。

このようなプロビジョニングイベントとしてはアカウントの追加や削除などが挙げられ、必要とする承認手順の数はいくつでも使用できます。各手順には、妥当性検査や承認のために、個人や外部システムの呼び出しを取り込むことができます。手順では、電子メール通知を 1 つまたは複数のアドレスに送信する必要があります。

Select Identity のワークフローには、以下の特徴および機能があります。

- 承認およびプロビジョニングプロセスを自動化します。
- Select Identity システムの外部にある情報の取得やアクションの開始のための外部システムへの同期コールおよび非同期コールをサポートします。

- コンテキストベースのワークフロー選択が可能です。これによって、異なるユーザーのグループに異なる承認プロセスを割り当てることができます。
- 直列および並列の処理手順が可能です。
- グループ承認処理をサポートします。
- 期限切れ承認のエスカレーションを提供します。
- リソースにプッシュされるユーザープロファイル属性の制御を提供します。
- 任意のロジック、分岐、およびカスタム関数をサポートします。

この種のワークフローは、Select Identity で **Workflow Studio** を使用して自動化できます。**Workflow Studio** では、異なる状況での承認およびプロビジョニングの特定のシーケンスをモデル化するワークフローテンプレートを作成できます。

さらに、ワークフローテンプレートを使用し、[リクエストステータス] ページからシステムイベントの進捗状況を追跡することもできます。

Workflow Studio は、グラフィカルインタフェースを使用してワークフローの作成を単純化する柔軟性のあるツールです。

Workflow Studio の使用方法に関する完全な情報は、HP Select Identity Workflow Studio オンラインヘルプで参照できます。

設定の承認

Select Identity 自身の設定に対する高リスクの変更を調整するには、設定の承認機能を使用します。設定の承認を使用して、Select Identity の設定変更用の承認ワークフローを確立できます。

設定承認の使用は必須ではありませんが、強くお勧めします。設定の承認を使用しない場合、管理者は属性、ルール、サービスなどの重要なシステム設定に対して、調整処理がされない大規模な変更を行うことができます。Select Identity の設定承認の設定は柔軟で、ユーザーの組織内に適切なレベルの制御を設定できます。

ユーザー管理

Select Identity のユーザー管理機能を使用すると、アカウント、使用権、およびプロファイル情報などのユーザーアイデンティティを集中管理することができます。作成から終了まで、アイデンティティの完全なライフサイクルを管理できます。

ユーザーは、サービスに定義されている登録プロセス (おそらく [自己登録] ページ) を介してシステムに追加されます。このプロセスがどのように行われるかは、各コンテキストに割り当てているワークフローおよびサービスロールによって決まります。

Select Identity の管理者は、[**ユーザー**] タブを介してユーザーアカウントを作成および管理できます。このタブでは、以下のアクションが承認されます。

- ユーザーアカウントの追加、変更、終了、およびアカウント属性の表示。
- サービス内のユーザーのメンバーシップの追加、表示、有効化、無効化、または削除。
- ユーザーのすべてのサービスの有効化および無効化。
- ユーザーのアカウントパスワードのリセット。

- ユーザーの有効期限の管理。

また、ユーザーアカウントが実際に削除される前に、バッファ期間を設定し、その間アカウントを無効にすることができます。さらに、アカウントが予定どおりに期限切れになる一時ユーザーを設定できます。パスワードの管理方法についての詳細は、36 ページの「パスワードおよび属性」を参照してください。

ユーザー自己管理

Select Identity は、ユーザーの自己サービスおよび自己管理を可能にする高度な機能を提供します。これは、ヘルプデスクの業務コストが増えるのを回避します。

ユーザーは、以下のようないくつかの重要なタスクを実行できます。

- ユーザーのアカウントプロファイルの表示と更新
- ユーザーのパスワードの変更または同期
- パスワードのヒントの変更
- 新規サービスへのアクセスの要求、またはサービスからの削除
- 必要に応じた管理ロールの委任

パスワード管理

Select Identity は、包括的なパスワード管理を用意しています。組織に適したパスワードポリシーを定義および強制します。これには、有効なパスワードの構成要素の定義、パスワードの期限、ロックアウトポリシー、質問 / 答えの質問などがあります。

プロビジョニング

ユーザー管理の一環として、アカウントおよび使用権の作成、メンテナンス、および失効の自動化が可能です。

管理を完全にするために、Select Identity で参照されるプロビジョニング依存関係を定義できます。プロビジョニングは、自動ロールバック機能を持つトランザクション処理です。ワークフローにはプロビジョニングリトライアクションを設定できます。

Select Identity は、リソースとの非同期通信を行い、企業リソースのプロビジョニングにはオープンスタンダードの J2EE コネクタアーキテクチャを使用します。

単一ユーザーの複数ユーザーアイデンティティ

個別のユーザーが、1 つのリソースに対して複数のアイデンティティアカウントを必要とする場合があります。ユーザーがロールに基づいて 1 つのリソースに複数のアカウントを持ち、アカウントを Select Identity の個人レベルで統合、管理したい場合があります。

Select Identity では、1 ユーザーの複数のユーザー ID を簡単に統合して管理することができます。

- 1 ユーザーの複数のリソースアカウントを、1 次アイデンティティと 2 次アイデンティティを含む複数ユーザー ID アカウントにグループ化できます。
- 1 人のユーザーの使用権をロールに基づいて管理 (追加、修正、または削除) できます。

- 別のユーザーへアカウントを移動したり、1 つのアカウントまたはユーザーのリソースアカウントのすべてを終了することができます。

さらに、複数ユーザー ID アカウントを使用すると、ユーザーのリソースに対する複数のアカウントをリソース上で互いに独立してメンテナンスしているが、Select Identity を使用して外部的にリンクしなければならない、といった状況に対応できます。

属性管理

Select Identity では、属性はアイデンティティプロファイルの定義に用いられるデータ項目、つまりフィールドです。各アイデンティティごとに、属性はそれぞれ対応する値を持っています。たとえば、EmployeeNumber と呼ばれる属性はユーザーの従業員番号を含みます。

Select Identity 実装内のすべてのアイデンティティは同じ属性を共有しますが、それぞれの特定のアイデンティティは属性値の独自の組み合せを持っています。要件を満たすユーザープロファイルを生成するために必要な属性をすべて定義できます。定義する属性は、実装で必要なすべてのアイデンティティを反映できます。

Select Identity では、属性を使用してアカウントおよびサービスを管理します。具体的には、Select Identity では各種のサービスでのユーザーのコンテキストを決定するために指定する属性の値を使用します。このコンテキストはユーザーをサービスロールにリンクします。このサービスロールは最終的に正しいリソースおよび使用権へのユーザーアクセスを提供します。

Select Identity 内の属性は、各種のリソース内の似ているが名前の異なるアイデンティティフィールドにマッピングすることができます。たとえば、EmployeeNumber と呼ばれる Select Identity 内の属性は、リソース上の empnum と呼ばれるアイデンティティフィールドにマッピングすることができます。

信頼できるリソースによってユーザーの EmployeeNumber が変更されたことが Select Identity に伝えられると、Select Identity はリソース属性のマッピングを使用して変更をリソースの empnum フィールドに反映します。

また、属性はプロビジョニング用、およびデータ妥当性検査用のフォームを自動的に生成するためにも使用されます。自動的に生成される属性値もあれば、あらかじめ決められた値に制約される属性値もあります。

パスワードおよび属性

Select Identity は、全社的に使用される複数のパスワードを管理し、その同期を取ります。複数のパスワードを管理する上で鍵となるのは、属性管理です。ユーザー関連のデータをリソースに正しくプロビジョニングするために必要な属性をいくつでも作成できます。リソースのパスワードは単に Select Identity のもう 1 つの属性であり、アカウントの作成およびリセット処理時にリソースにプッシュできます。

Select Identity には、Password というパスワード属性があります。この属性は Select Identity 自体へのアクセスの認証に使用されるため、削除することはできません。また、任意の数のリソースに同じパスワードをプッシュし、Select Identity とリソースの同期を取ることができます。

ただし、必要に応じてリソースごとに 1 つずつ、パスワードの属性を複数作成することも可能です。パスワードの属性にはそれぞれ一意のテキスト名が必要であり、許可される最小および最大文字数、または社内の規定に従いパスワードを自動生成するかどうかなど、それ自体のパスワードポリシーが含まれます。

一度パスワードの属性を使用してユーザーをプロビジョニングすると、Select Identity 内でユーザーのアイデンティティが存在する間は Select Identity によってこのパスワードがトラッキングされます。それ以降、パスワードのリセットリクエストがあると、このユーザーのパスワードの属性がすべて表示されるため、このパスワードの属性を使用するすべてのリソースの同期が取られます。パスワードの属性とリソースのこのマッピングは、1 対 1 でも 1 対多でも可能です。

外部コール

Select Identity のワークフロープロセスおよび属性は、外部プロセスまたはシステムと相互にやりとりするための機能をサポートしています。この機能は外部コールと呼ばれます。外部コールは、Select Identity の一部である Java API を使用して作成した関数を呼び出します。Select Identity の外部のプログラムまたはシステムと相互にやりとりする外部コールを書くことができます。

外部コールを使用すると、承認プロセスをほかのビジネスプロセスやシステムに統合することができます。外部コールを使用することで、以下のようなアクションを行うことができます。

- 承認者の選択 ― 外部プログラムを実行して、ワークフローの承認者のリストを取得します。
- 値の生成 ― 属性の値を生成します。
- 値の制約 ― 属性に使用可能な値のリストを提供します。
- 値の妥当性検査 ― 属性の値の妥当性を検査します。
- 値の検証 ― 値がすでに保存されているものであるかどうか検証します。これはパスワードの検証に使用されます。
- 証明書の管理 ― 外部システムから証明書を取得できます。
- SPML リクエストフィルタ ― 調整リクエストを処理する前に起動されます。
- ワークフローアクション ― ワークフローの一部としてタスクを実行し、承認プロセスを外部プロセスやシステムと統合できるようにします。
- リソースの直接操作の実行
- ワークフロー内の属性の更新

一度作成すると、外部コールは Select Identity インタフェースを通して管理されます。

外部コールの設計、開発、および使用方法についての完全な情報は、『HP Select Identity 外部コール開発者ガイド』を参照してください。

通知

Select Identity のユーザーインタフェースの [**通知**] セクションでは、システムイベントが発生したときにユーザーおよび管理者に送信する電子メール通知の内容を定義できます。

このようなメッセージは、ワークフロープロセスのさまざまな場面で効果的です。たとえば、アカウントの承認、拒否、または変更などのイベントのため、またはアカウントのパスワードまたはヒントへの変更の確認のためにユーザーに電子メールを送信したい場合があります。同様に、アカウントの承認が必要な場合、またはアカウントが指定の時間内に確認されなかった場合には、管理者に電子メールを送信したいと思うはずです。

ユーザーの大規模な追加

Select Identity では、大量のユーザーを一度に Select Identity に追加する方法が 2 つあります。

- 1 つは**ユーザーインポート**と呼ばれるもので、既存のリソースからユーザーデータを取り込むことでユーザーを迅速に Select Identity に設定し、属性および現在の使用権に基づいてサービスに割り当てることができます。

  ユーザーインポートは、主に新規の Select Identity インストールを設定するときに使用されます。

- もう 1 つの方法は**一括追加**または**一括移動**と呼ばれるもので、複数の新規ユーザーを迅速に Select Identity に追加し、属性に基づいてサービスに割り当て、適切なリソース上でプロビジョニングすることができます。

  一括追加は、主に新規ユーザーを既存の Select Identity インストレーションに追加するために使用します。

この 2 つの方法の主要な相違は、新規ユーザーをプロビジョニングする方法にあります。

- ユーザーインポートでは、新規ユーザーはジョブが開始する前にユーザーのリソースですでにプロビジョニング済みです。
- 一括追加では、Select Identity のジョブの一環として新規ユーザーをプロビジョニングします。

リクエストステータス

ユーザーアカウントがシステムに追加されていると、[**リクエストステータス**] 機能を使用して、ステータスや詳しい承認プロセスを表示することができます。

リクエストステータスでは、ワークフロー手順を実行済み、実行前、承認待ち別に色分けして表示できます。

Select Identity では、ワークフロー情報を表示するためにデフォルトのレポートテンプレートが用意されています。また、ユーザーは使用環境に固有の詳細情報を表示するために独自の XML テンプレートを作成できます。詳細については、Workflow Studio のオンラインヘルプを参照してください。

セキュリティ管理および監査レポート作成

アカウント管理プロセスはすべて、監査レポートおよび設定レポートを使用してチェックできます。監査レポートを使用して、アカウントの定期的なやりとりを監視できます。設定レポートには、Select Identity システムの設定に関連する最新情報が表示されます。

Select Identity は、データベースおよび監査ログのレポート機能が組み込まれており、すべてのシステムイベントの詳細な監査ログを提供します。Select Identity ではアイデンティティおよび監査データをキャッシュに保存するため、履歴レポートを生成できます。

スケジュールおよびデータ選択に関するレポートをカスタマイズできます。レポートはコンテキストによって自動的にフィルタされるので、管理者は管理対象ユーザーに関係するデータだけを参照できます。

設定の複製

Select Identity では、1 つの環境でシステムを設定し、その後で別の環境に設定を複製できます。

これを実施するには、サービス、属性、およびリソースなどの複製元のシステムの主要コンポーネントをエクスポートします。その後、複製先のシステムにそれらの要素をインポートします。

この手法により、テスト環境から実稼働環境へ簡単に移行できます。

詳細については、『HP Select Identity 管理者ガイド』を参照してください。

A Select Identity と他の HP Identity Center アプリケーションとの統合

この付録では、Select Identity と他の HP Identity Center アプリケーションを統合する際の組み合わせについて説明します。主に次の組み合わせがあります。

- Select Identity と Service Desk の統合
- Select Identity と Select Audit の統合
- Select Identity と ServiceCenter の統合

Select Identity は Service Desk、Select Audit、および ServiceCenter と一緒に構成することができ、相互にデータを交換し合うことでそれぞれの機能を高めることができます。Select Identity で統合を設定する方法については、『HP Select Identity インストールガイド』を参照してください。

Select Identity と Service Desk の統合

この項では Select Identity と Service Desk 4.5 (サービスパック 13) との統合に関する情報を記載します。

Select Identity のパスワード管理機能と Service Desk を統合すると、Service Desk のサービスコールチケットは Select Identity によって自動的に更新されます。これにより、Service Desk で問題点の追跡と SLA (Service Level Agreement) の実施が可能になります。

2 つのアプリケーションを統合しない場合、Service Desk で開始したパスワードリセットのサービスコールは、Select Identity を使って `ResetPassword` プロセスを手動で有効にして処理する必要があります。SLA を実施するに当たり、Service Desk では Select Identity の ResetPassword プロセス管理が行われません。

機能シナリオ

ここでは Select Identity と Service Desk の統合について、用途に基づいたシナリオの例を示します。基本的に、パスワード管理リクエストを Select Identity または Service Desk のいずれからも開始できます。

パスワード管理機能については、以下の一覧を参照してください。

- **パスワードの変更** : ユーザーが自身のパスワードを変更します。
- **パスワードのリセット** : 管理者がユーザーの代わりにパスワードを変更します。
- **パスワードを忘れた場合** : 自動生成されるパスワードによりパスワードがリセットされるか、ユーザーが新しいパスワードを入力できます。これは、`com.hp.ovsi.forgetpassword.autogenerate` という `TruAccess.properties` 項目に割り当てた値によって決まります (「true」に設定されている場合、パスワードが自動生成されます)。

Select Identity からのパスワード管理リクエストにより、Service Desk で新しいサービスコールを開始

Select Identity のエンドユーザーまたはシステム管理者がパスワード管理リクエスト (パスワードのリセットまたは変更、忘れたパスワードの取得) を送信すると、新しい Service Desk でサービスコールが自動的に開始され、Select Identity で Service Desk ワークフローの各段階のステータスが更新されます。これは、リクエストを Select Identity の GUI 経由または Web サービス経由のいずれから送信しても実行されます。サービスコールはワークフローの終了時に**完了**ステータスに更新されます。

Service Desk からのリセットパスワードリクエストと対応する Select Identity ワークフローの各段階でのサービスコールステータスの更新

Service Desk 顧客サービス担当者 (CSR) はパスワード管理を行うために新しいサービスコールを開くか更新すると、Select Identity の [**パスワードのリセット**] ページが開き、Select Identity で直接リクエストを実行できます。サービスコールのステータスは、Select Identity で Service Desk ワークフローの各段階で更新されます。サービスコールはワークフローの終了時に**完了**ステータスに更新されます。

Service Desk の Select Identity リクエストステータスページにアクセス

Service Desk の CSR は Select Identity の [**リクエストステータス**] ページにアクセスし、パスワードリセットのサービスコールに関するリクエストのステータスを確認できます。

Select Identity と Select Audit の統合

Select Identity を Select Audit と一緒に構成することにより、2 つのアプリケーションで以下のような機能を実行できます。

- Select Identity のリクエスト、トランザクション、設定、およびメンテナンスのデータを Select Audit に送ると、Sarbanes-Oxley 法、HIPAA 法、その他の規制に関する設定の遵守を監査できます。
- Select Identity の XML 監査データストリームからのデータを各種のレポートに組み込めます。
- Select Identity 設定レポートへのアクセス権に基づき、Select Identity 管理者は Select Audit の監査レポートを表示できます。Select Audit では管理サービスおよび Select Identity 管理者の状況に応じて、レポートがフィルタされるため、管理者は管理しているユーザーやサービスに関するレポートのみを表示できます。

Select Audit の設定手順に関する詳細な説明は、Select Audit のドキュメントを参照してください。このドキュメントには、Select Audit 側からの統合設定方法の概要のみが記載されています。

Select Identity と ServiceCenter の統合

Select Identity と ServiceCenter を統合すると、ServiceCenter の管理者は、ユーザーの追加やパスワードのリセット、サービスへの登録などの Select Identity 操作を、ServiceCenter のインタフェースを通じて管理および監視できるようになります。ユーザー管理機能のリクエストワークフローでは、Select Identity はそのワークフローの操作に基づいて ServiceCenter チケットを更新します。

Select Identity と ServiceCenter の統合は、主に 4 つのアーキテクチャコンポーネントから構成されます。

- サービスカタログは、エンドユーザーが Select Identity サービスに登録するためのインタフェースを提供します。
- 変更管理カスタマイズは、ServiceCenter リクエストを処理し、Select Identity ワークフローとともに機能します。
- Web サービスは Select Identity と ServiceCenter の間の通信を処理します。
- Select Identity ワークフローは、ビジネスレイヤーで ServiceCenter と通信を行います。

この統合は双方向で機能します。つまり、Select Identity は ServiceCenter にリクエストを送信でき、ServiceCenter も Select Identity にリクエストを送信できます。

B Select Identity アーキテクチャの概要

はじめに

アイデンティティ管理システムは、すべてのソフトウェアソリューションに共通の厳しい要件をいくつも満たさなければなりません。

- 企業の全従業員ユーザーだけでなく、ビジネスパートナー、ベンダー、請負業者、および顧客といったユーザーも管理できるように拡張できる必要があります。
- これは単にパフォーマンスの拡張だけでなく、利用の規模や複雑さが増すのに応じて管理可能性も拡張されなければなりません。エンタープライズ情報システムは企業にとって活動の基盤をなすものであり、こうしたシステムへのアクセスを確保することはビジネスクリティカルな問題であるため、信頼できるアイデンティティ管理システムが求められます。
- また、システム、組織、およびビジネスプロセスが多種多様であれば、エンタープライズクラスのアイデンティティ管理システムには高い柔軟性が要求されます。

この付録では、特に企業にもたらす効果に注目しつつ、Select Identity の技術的なアーキテクチャについて説明します。この付録では Select Identity システムで使用しているテクノロジやアーキテクチャを詳しく解説しています。

Select Identity のアーキテクチャについて、以下の 3 つの側面から説明します。

- プラットフォームのアーキテクチャ
- 配布のアーキテクチャ
- システムのアーキテクチャ

プラットフォームのアーキテクチャ

Select Identity システムは、大規模かつ複雑で広範囲にわたるエンタープライズ環境でのアイデンティティ管理を想定して設計されています。こうした環境での要求に対応するために、Select Identity はいくつものテクノロジを活用してスケーラビリティ、信頼性、拡張性を高めています。

J2EE

Select Identity は J2EE (Java 2 Platform、Enterprise Edition) をプラットフォームとして利用しています。J2EE はオープンスタンダードに基づく移植性を備えているため、顧客にとってハードウェアとソフトウェアの選択肢が広がると同時に、エンタープライズクラスのスケーラビリティ、信頼性、および拡張性を提供します。また J2EE プラットフォームは、データベース (JDBC)、ディレクトリ (JNDI)、メッセージングサービス (JMS) など、他のエンタープライズシステムへの強力な API セットも備えています。Select Identity は BEA WebLogic、IBM WebSphere および JBoss など、主要な J2EE アプリケーションサーバー上で稼動します。

Select Identity は J2EE プラットフォームを活用し、大規模で広範囲に展開する企業向けにスケーラビリティを向上させる強力なオプションをいくつも備えています。Select Identity では、ロードバランシング、並行性、並列処理など標準的な Web アプリケーションのスケーラビリティテクノロジやテクニックを使用しているため、ユーザー、リソース、地理、企業の規模におけるビジネスニーズに応じて Select Identity のサイズを適合させることができます。

J2EE はイベント駆動型のトランザクション処理をサポートします。Select Identity は J2EE のトランザクションサポートを利用し、ロールバックやマルチフェーズのコミットなど高い信頼性をもたらす機能を提供します。

トランザクション処理により、アイデンティティ管理タスクが確実、正確、かつ完全に実行されます。

たとえば新しいユーザーをプロビジョニングする場合、Select Identity は複数のリソースにわたるユーザーのアカウント作成と使用権作成を単一のトランザクションとして処理し、何らかの理由でトランザクションが完了しなければロールバックできます。

これにより外部システムデータの整合性が保たれ、部分的にしかプロビジョニングされないユーザーの発生という不都合やコストを防止できます。失敗の原因が解決されると、Select Identity は再度処理を実行します。

J2EE の Web サービスアーキテクチャを使用しているため、Select Identity は柔軟に機能を拡張してビジネスニーズに対応します。たとえば、Web のシングルサインオン (SSO) アプリケーションを配布して共通認証機能を提供している環境では、Select Identity の内部認証サービス (ユーザーおよび管理者が Select Identity システムにログインする際に使用) を SSO 用にスワップアウトできます。

また重要な点を挙げると、Select Identity は J2EE の拡張 API セットを使って外部システムにアクセスするため、エンタープライズリソースへの接続が可能です。

リレーショナルデータベース

Select Identity はリレーショナルデータベースを利用してユーザー情報、内部システム情報、および監査ログを保存します。これは、ディレクトリ上に構築されたアイデンティティ管理システムのアーキテクチャで非常に有利に働きます。なぜならリレーショナルデータベースは、トランザクション、バックアップおよび復元、分散処理、データウェアハウジングをネイティブにサポートしているからです。

ディレクトリでは素早いレコード検索ができますが、大部分のリレーショナルデータベース製品で標準となっているデータ関係のマッピングと信頼性の機能はサポートしていません。しかし、Select Identity はディレクトリをプロビジョンする機能をサポートします。このため、ディレクトリは他のエンタープライズリソースと同様に扱われます。Select Identity は、Oracle、Microsoft SQL Server、IBM DB2 など、JDBC をアドレス指定可能なデータベースシステム上に導入できます。

ユーザーインタフェース

Select Identity はフル機能のグラフィカルユーザーインタフェース (GUI) の採用を方針としています。すべてのユーザーおよび管理者のアクションは GUI から実行できるため、設定ファイルのスクリプトやコードを手動で入力したり編集したりする必要はありません。この方針のおかげで利用が大幅に容易になり、導入時間も短縮できます。またユーザーのインポートなどバッチ方式の機能に対し、GUI に加えて API アクセスも備わっています。

Select Identity のインタフェースは各ユーザーに対して自動的にパーソナライズされるため、ユーザーが実行を許可された機能しか表示されません。

Select Identity のシンクライアントアプローチには、運用や管理をするクライアントソフトウェアが不要であるという大きな利点があります。これによってパッチや新バージョンのアップデートの導入が簡単になります。また Select Identity の Web ベースのクライアントがあれば、インターネットやダイアルアップ経由でどこからでもアクセスできます。これは緊急時対応計画で大きな効果を発揮します。セキュリティ確保のため、Select Identity は SSL を使って Web クライアントと Select Identity サーバーの通信を安全に行います。

また、Select Identity Web クライアントは標準のポートでサーバーにアクセスするため、ファイアウォールと競合しません。

Select Identity は幅広い企業向けに設計されているため、ユーザーインタフェースも規模に合わせてサイズ変更できます。たとえば、多数の項目を含むリストを表示する場合、Select Identity はそのリストをページに分割し処理しやすくすると共に、強力な検索機能を提供します。

セキュリティ

どのようなアイデンティティ管理製品でもそうですが、セキュリティは最も重要な事項です。Select Identity は、保存中でも通信中でもアプリケーションデータを暗号化します。保存時の暗号として、Select Identity は標準ハッシュアルゴリズムである SHA-256 を使用しています。データ通信中には SSL で情報の安全を確保します。

各企業のポリシーに応じて、サーバーとクライアントを手動で認証できます。保存中でも通信中でも、Select Identity は他の暗号化および認証のテクノロジをサポートできます。

配布のアーキテクチャ

他のエンタープライズソフトウェアと同様、配布が簡単であることはアイデンティティ管理システムを成功に導く重要な要素です。アイデンティティ管理システムは、企業内部に浸透するという役割上、配布が複雑になります。アイデンティティ管理システムは多種多様なアプリケーション、データベース、およびディレクトリと統合し、プロビジョニングとアイデンティティ関連の処理を行う必要があります。こうしたリソースは、複数の組織、地理的な場所、およびハードウェア / ソフトウェアのプラットフォームにまたがっている場合があります。

J2EE コネクタアーキテクチャ

Select Identity は J2EE コネクタアーキテクチャ (JCA) を使用し、オープンスタンダードに基づくアプローチを用いてエンタープライズリソースにアクセスします。JCA は、エンタープライズ情報システムへの接続の Java 標準です。他の J2EE コンポーネントと同様、企業規模と管理可能性に対応するように設計されています。JCA によりエンタープライズアプリケーションへのコネクタを Select Identity だけでなく複数の J2EE アプリケーションで作成し、使用できます。

Select Identity は強力なコネクタセットを備えているため、広範なエンタープライズリソースをカバーし、新しいコネクタも利用可能になると同時に提供できます。

Select Identity は JCA 内蔵のトランザクションプーリング機能を利用してトランザクションのスループットを最大化し、システムのパフォーマンスを向上します。トランザクションプーリングはリソースへの接続を管理しますが、リソースのアベイラビリティを確保するために可能な限り既存の接続を再利用して最適化します。この機能により、Select Identity コネクタのエンタープライズリソースに与えるパフォーマンス上の影響を最小化できます。

エージェントベースのコネクタ

アイデンティティ管理システムでのエージェントベースとエージェントレスのコネクタの利点に関しては、十分な議論が重ねられました。エージェントベースのコネクタは (通常同じホスト上の) リソースに常駐して、アイデンティティ管理システムからのリクエストを処理したり、他のリソースとの同期化アクションやプロビジョニングが必要となる変更がリソース内で発生した場合にアイデンティティ管理システムに通知したりします。

エージェントベースのコネクタはアイデンティティ管理システムとは独立して動作し、個別に管理する必要があるため、難点は日々の運用管理にあります。これは特に、アイデンティティ管理システムが管理するリソース数が増加した場合に負担となります。

エージェントベースのコネクタに代わるものが「エージェントレス」のコネクタですが、これはアイデンティティ管理システム内に常駐し、アイデンティティ関連の更新をリソースに送信します。エージェントレスのコネクタは、アイデンティティ管理システムと緊密に統合し、その内部で管理できるという利点を持っています。コネクタをアイデンティティ管理システム自体に統合することで、配布とメンテナンスが非常に容易になります。

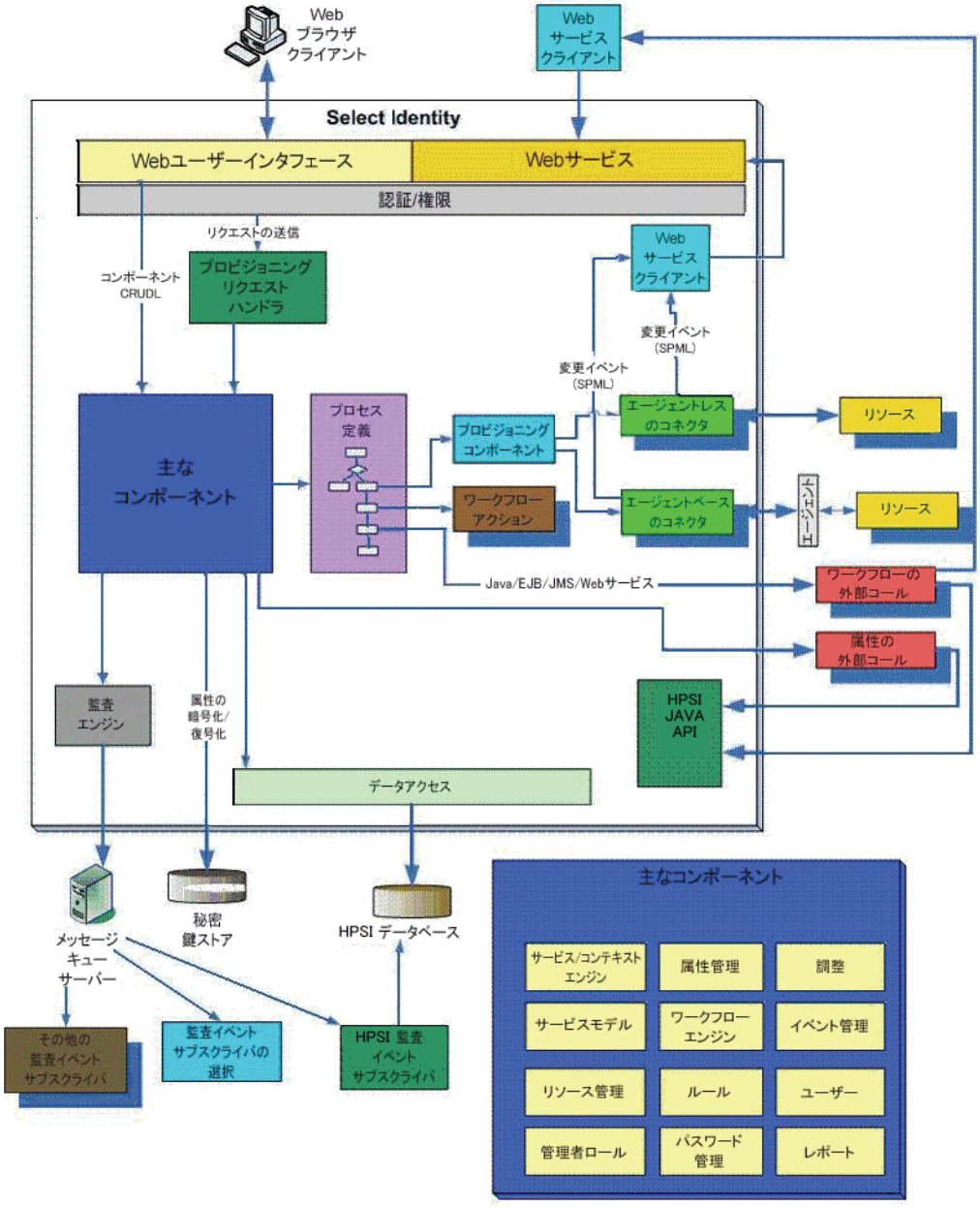
このアプローチで不利な点は、エージェントレスのコネクタがアイデンティティ管理システムからリソースへの一方向の通信に対して最適化されていることです。

リソース内でのアイデンティティの変更を他のリソースに通知する必要がある場合、エージェントベースのコネクタの方が適しています。この理由から Select Identity は「エージェントベース」のコネクタモデルを採用していますが、リソースおよびビジネスの処理要件に応じてエージェントベースまたはエージェントレスの両方のコネクタに対応できます。

システムアーキテクチャ

Select Identity はイベント駆動型の J2EE アプリケーションであり、クラスタ化、フェイルオーバー、マルチフェーズのコミット、非同期操作が可能です。以下の図は、Select Identity システムとシステムコンポーネントの構成の概略図です。

図 10　　Select Identity アーキテクチャ



システムとの間で送受信するすべてのリクエストでは、HTTP プロトコルを使用します。ユーザーアカウントは 1 つの仮想 ID を使ってバックエンドシステムおよびサービスにアクセスし、Select Identity システムの機能とアクションによって管理されます。また、アカウントは、企業の製品およびサービスのアクセス要件に基づく属性と使用権によっても管理されます。

Select Identity アーキテクチャのコンテキストエンジンコンポーネントとアイデンティティビジネスプロセスサービのスコンポーネントは、Select Identity システムの配布とメンテナンスを実行する管理者や担当者にとって特に有用です。これらのコンポーネントには、管理者が最もよく使用する機能が含まれています。

Select Identity の主なコンポーネントは以下のとおりです。

- **サービス / コンテキストエンジン** - サービスおよびサービスロールの階層を構築します。コンテキストユーザーグループに基づき、グループに対するフィルタ処理を行います。
- **属性管理** - サービス属性の構成および設定を支援します。たとえば、定義、属性に使用する文字、適用する制約などです。
- **調整** - 複数のリソースにおけるユーザーのアイデンティティデータの整合性についてレポートを作成します。同期入出力が指定されているフィールドで発生した電話番号の変更などの変更を、該当するすべてのリソースと Select Identity データベースの両方または一方に複製することにより同期します。
- **サービスモデル** - サービスに所属しているユーザーの変更管理を可能にする抽象化レイヤーを提供し、より動的で柔軟な処理を可能にします。Select Identity のサービスモデルでは、市場に存在する他のアイデンティティ管理製品とは異なり、ユーザーやグループはリソースやシステムに緊密に関係付けられているわけではありません。
- **ワークフローエンジン** - 1 人または複数のユーザーのプロビジョニングに使用するプロセスのステップを容易に作成、変更、削除できるようにします。
- **イベント管理** - ユーザーの追加などのイベントに適用するワークフロープロセスまたはビューを決定します。
- **リソース管理** - 信頼できるかどうかにかかわらず、リソースに関する定義と詳細を取得し、管理者がリソースへの接続を検証できるようにします。
- **ルール** - 調整プロセスを通じて情報をどのようにインポートおよびエクスポートするかを決定するルールの作成、変更、表示、削除を可能にします。
- **ユーザー** - サービスのユーザー管理を可能にします。これには、ユーザーアカウントの作成、変更、削除が含まれます。ユーザーは登録したサービスに割り当てられ、それらのサービスに適用される属性もユーザーアカウントに適用されます。
- **管理者ロール** - 1 つまたは複数のサービスアカウントを管理する 1 人または複数のユーザーのロールを定義します。社内の多様な管理ニーズに対応するため、複数の管理者ロールを作成することもできます。

用語集

AD

Active Directory

Concero sys admin

最高レベルの使用権とアクセス権が与えられる、特殊な用途の管理者ロール。

EAR ファイル

エンタープライズアーカイブ。Select Identity などのアプリケーションパッケージを格納するための圧縮ファイル形式。

HSM

ハードウェアセキュリティモジュール。

JCA

Java Connection Architecture (Java 接続アーキテクチャ)

JDBC

Java Database Connectivity (Java データベースコネクティビティ)

JDK

Java 開発キット (JDK)

JMS

Java Messaging Services (Java メッセージングサービス)

JNDI

Java Naming Directory Interface (Java ネーミングディレクトリインタフェース)

LDAP

Lightweight Directory Access Protocol (軽量ディレクトリアクセスプロトコル)

LDIF

Lightweight Directory Interchange Format (軽量ディレクトリ交換形式)

Liberty Identity Federation Framework (ID-FF)

一般的なオープンスタンダード連携プロトコルで、世界中の 150 を超える企業、NPO、政府組織により結成された Liberty Alliance Project により開発されました。この組織は、連携ネットワークアイデンティティのオープンスタンダード開発に取り組んでいます。

Lightweight Directory Access Protocol (LDAP、軽量ディレクトリアクセスプロトコル)

任意の者がネットワーク内の組織、個人、およびその他のリソース (ファイルやデバイスなど) を特定することを可能にするソフトウェアプロトコル。LDAP ディレクトリは複数のサーバーに分散することが可能です。LDIF は各 LDAP ディレクトリの同期化に利用されます。

Lightweight Directory Interchange Format (LDIF、軽量ディレクトリ 交換フォーマット)

ASCII ファイル形式です。DSA (ディレクトリ システムエージェント) と呼ばれる LDAP (軽量ディレクトリ アクセスプロトコル) サーバー間でのデータ交換とそのデータの同期に利用します。

logging.properties ファイル

Select Identity がメッセージおよび例外をログする方法を定義するテキストファイル。

OASIS

Organization for the Advancement of Structured Information Standards (構造化情報標準を促進する組織)。非営利の国際コンソーシアムで、E ビジネス標準の開発、統合、および採用を推進しています。コンソーシアムでは、公的部門および特定の市場向けに、セキュリティ、E ビジネス、および標準化作業用の Web サービス標準を作成しています。

properties

名前 - 値ペア (値は文字列)。プロパティは、テンプレートが作成される際の定数データを定義します。実行中はプロパティ値は変更されません。グローバルプロパティは、ワークフローインスタンス内の全アクティビティで共有されます。初めてプロパティを設定する場合、そのタイプを初期化します。指定されたプロパティは、Select Identity のワークフロー API を使用して、外部アプリケーションから読み取ることができます。このプロパティはレポートテンプレートから参照し、ステータスレポートに関連情報を表示することも可能です。一部のプロパティ名はワークフローエンジンによって定義されます。アクティビティやブロックを定義する際に、これらのプロパティを使用します。ワークフローテンプレートを作成する場合、プロパティに値を割り当てる必要があります。これらのプロパティ値でワークフローの動作を指定します。たとえば 3 という値を joinCount プロパティに割り当てた場合、3 人の承認者がワークフローに加わるとワークフローは承認ブロックを終了します。

SHA

Secure Hash Algorithm (セキュアハッシュアルゴリズム)

SOAP

Simple Object Access Protocol (簡易オブジェクトアクセスプロトコル)

SPML

Service Provisioning Markup Language (サービスプロビジョニングマークアップ言語)

SPML データファイル

Select Identity におけるアカウントの追加とプロビジョニングに使用されるサーバー解析の XML ファイル。調整する場合、SPML データファイルは信頼できるリソースとそれ以外のリソースの両方から生成できます。通常、各リソースにつき 1 つの SPML ファイルが生成されます。SPML ファイルには、一定期間内の追加、削除、変更といったユーザーアカウント情報への変更が格納されます。ファイルは Select Identity にアップロードされ、Select Identity 内のユーザーアカウント情報は調整時に更新されます。

SSO

シングルサインオン

TruAccess.properties ファイル

カスタマイズ可能な多数の Select Identity 設定を含むテキストファイル。

URI

Uniform Resource Identifier (統一資源識別子)

WAR ファイル

Web Archive ファイル。複数のファイルをまとめて圧縮するフォーマットです。拡張子は .war で、サーブレットで使用します。

Web Application Server (Web アプリケーションサーバー)

インターネットベースのデータと通信トランザクションのためのインフラストラクチャを提供するように設定されたコンピュータまたはコンピュータのグループ。

Web サービス

Service Provisioning Markup Language (SPML) を使用して、Select Identity 内のカスタマイズ可能なユーザー管理機能を提供する、XML ベースのリクエストフレームワーク。

Web サービス定義言語 (WSDL)

ドキュメント指向またはプロシージャ指向の情報を含むメッセージ上で動作するエンドポイントの集まりとしてネットワークサービスを記述する XML フォーマット。動作とメッセージは抽象的に記述され、その後具体的なネットワークプロトコルやメッセージフォーマットにバインドされ、エンドポイントを定義します。関連する具体的なエンドポイントが組み合わされ、抽象的なエンドポイント (サービス) を形成します。通信に使用するメッセージフォーマットやネットワークプロトコルに関係なく、WSDL を拡張してエンドポイントとメッセージを記述できます。

WfMC

Workflow Management Commission

Workflow Studio

ワークフローテンプレートを作成および管理するための機能。

Workflow Studio Editor

ワークフローテンプレートを作成および管理できる特別なユーザーインタフェースを備えた Select Identity の機能。

WSDL

Web サービス定義言語 (WSDL)

XML プロセス定義言語 (XPDL)

ワークフローテンプレートを保存すると、Select Identity リポジトリに XML (Extensible Markup Language) ファイルとして保存されます。フォーマットは、Workflow Management Coalition (WfMC) が規定する XML プロセス定義言語 (XPDL) です。

XPDL

XML プロセス定義言語 (XML Processing Description Language)

1 次ユーザー

Select Identity ログイン名として機能する、ユーザークラスタ内のユーザー ID。クラスタ内の他のすべてのユーザーアカウントは、2 次アカウントとしてこれに関連付けられます。

2 次ユーザー

ユーザークラスタ内の 1 次ユーザー以外のアカウント。

アイデンティティ

個人の詳細情報、連絡先情報、各種リソースやサービスへのアクセス権など、システム内の特定個人に関連しているデータのセット。たとえばシステム管理者など、一部のアイデンティティには特殊な用途があります。

アイデンティティ管理 (IdM)

アイデンティティ管理とは、組織と個人間での合意、プロセス、およびツールのセットを指します。これにより、人、システム、およびサービスがリソースにアクセスし、ビジネス目標を達成できます。

アイデンティティプロバイダ (IdP)

アイデンティティプロバイダ (つまり IDP) とは、ユーザーを関連 Web サイトに転送する前にユーザーを認証する Web サイトのことです。Web サイトで IDP と SP を同時に機能させることができます。

アクション

アクションはワークフローのアクティビティに関連しています。アクションは、Select Identity のワークフローエンジンまたは外部アプリケーションにより提供される機能を呼び出します。アクションにより、たとえば、ログファイルへの情報の記録、ワークフローで後で使用する変数の設定、Select Identity にユーザーをプロビジョニングするための外部プロセスの呼び出し、およびデータベースへのデータの格納が可能です。

アクティビティ

アクティビティは、ワークフローテンプレートによって表わされるプロセス中の 1 つのステップです。アクティビティはワークフローテンプレートの主なコンポーネントです。アクティビティで定義するアクションは、ユーザーをプロビジョニングするのに必要な作業を実行します。アクティビティには、ワークフロー変数の設定、承認のトラッキング、サブワークフローの開始、電子メールの送信、外部アプリケーションの呼び出しなどのアクションを含めることができます。

アプリケーション呼び出し

アプリケーションの呼び出しワークフローアクションを使用して Select Identity アプリケーションを呼び出すことができます。Select Identity は使用可能な多数のアプリケーションを用意しています。Select Identity 内で独自にカスタマイズしたアプリケーションを開発することもできます。

あらかじめ定義された変数

管理者名、ユーザー名、および電子メールアドレスの変数。これらの変数により、アクションおよびアクションを実行するユーザーに基づいた適切な情報がシステムにより提供可能になります。

暗号化

送信者と意図した受信者によってのみ読み取ることが可能になるようにメッセージをエンコードするプロセス。

移動ポリシーを適用オプション

ユーザーのコンテキストを変更する場合、調整時に使用可能な Select Identity 機能。移動ポリシーを適用の有効化により、Select Identity は、調整時に影響を受ける各サービスのサービスロールとサービスレベル属性移動ポリシーに従って、ユーザーの属性を変更できます。

委任管理

エンドユーザーに代わって管理者が実行するユーザーアイデンティティ管理機能。自己サービスも参照してください。

委任登録

他者に代わって管理者が実行するアカウント登録。

イベントハンドラ

特定のシステムイベントに関連付けられた通知テンプレートやワークフローテンプレート。通知テンプレートは通知イベントハンドラで、ワークフローテンプレートはリクエストイベントハンドラです。

イベントマネージャ

イベントハンドラのインターフェイスとなるシステムで、電子メール通知の送信や特定システムイベントに関連したワークフロー実行など、システムの全イベントを処理します。通知テンプレートは通知イベントハンドラです。ワークフローテンプレートはリクエストイベントハンドラです。

インポート

別のアプリケーションやシステムからのデータを読み込み、フォーマットし直し、保存すること。

エージェント

SI データストアからエンタープライズリソースへの逆データフローを可能にするコネクタ。これにより、双方向の複製が可能になります。

エージェントベースのコネクタ

双方向のコネクタインタフェース。Select Identity と同じシステム上にあるコネクタと、リソースと同じシステム上にあるエージェントという 2 つのコンポーネントがあります。エージェントは、リソースに生じる変更のリッスン、および Select Identity に加えられる変更に関してリソースとの交信を行います。

エージェントレスのコネクタ

一方向のコネクタ。コネクタは Select Identity サーバー上に存在し、リソースとの通信を仲介します。

エクスポート

他のアプリケーションやシステムで利用する目的でデータをフォーマットまたは保存すること。

エンドユーザー

Select Identity 内のすべてのユーザーにデフォルトで割り当てられるロール。エンドユーザーのロールでは、自己サービスのページにアクセスできますが、管理者権限はありません。

オプションの使用権

各ユーザーのアイデンティティに関連するサービスロールとコンテキストに基づき、ユーザーが利用できる使用権。ユーザーは使用権選択のオプションを保有しています。

外部コール

アカウントの検証または属性値の制限を目的とした、サードパーティのアプリケーションまたはシステムに対するプログラムによる呼び出し。

監査

システムの利用、操作、メンテナンスに関するデータ、イベント、トランザクション、設定変更その他のデータの記録。

監査レポート

整理された読みやすい監査データのレポート。

管理サービス

承認者を追加するために Select Identity システム管理者により使用されるサービス。担当するサービスごとに毎回管理者を追加しなくて済むようにする、管理者向けの個別サービスです。これにより、管理者は複数のサービスからのユーザー承認要請を管理できます。

キー

プレーンテキストが暗号テキストに変換される方法、または復号化時に逆の処理が行われる方法を定める情報。

キーストア

キーおよび証明書のデータベース。秘密キーは証明書チェーンと関連付けられています。証明書チェーンは対応する公開キーを認証します。証明書は信頼できるエンティティから受け取ります。

キーストアエイリアス

キーストアエントリに割り当てられる、大文字と小文字を区別する名前。すべてのキーストアエントリ (キーおよび信頼できる証明書エントリ) は一意のエイリアスによりアクセスされます。

キーローテーション

Select Identity セキュリティキーを変更し、オプションとして新しいキーによりデータを再暗号化する、スケジュールされたプロセス。

機能

Select Identity の権限のグループ化。

業務サービス

組織が提供したり利用したりする製品、設備、または不可欠なビジネスプロセスで、日々の業務の基礎となります。たとえば、オンラインバンキングサービス、顧客サポートプロセスのほか、電子メール、カレンダ機能、ネットワークアクセスなどの IT インフラストラクチャサービスがあります。「サービス」も参照。

業務サービスアイデンティティ管理 (BSIM)

企業内および企業間でのアイデンティティ管理に対する新たな動的かつスケーラブルなアプローチ。BSIM を使用すると、複数のプラットフォーム間、アプリケーション間、および企業間の、ユーザーアカウントとアクセス権限のプロビジョニングや管理のプロセスを自動化できます。

許可

アイデンティティの使用権をリアルタイムに強制すること。認証は許可を得るための前提条件です。

クラスパス

重要なシステムファイルのディレクトリの位置を指定する設定。

クラスタ

単一のエンティティとして機能するサーバーのグループ。たとえば jBoss AS、BEA WebLogic、または IBM WebSphere などの Web アプリケーションサーバーです。この用語はユーザーアカウントのグループを指す場合にも使われ、その場合はユーザークラスタと言います。

権限

ユーザーが Select Identity 内で管理タスクを実行することを可能にする権限。

固定使用権

各ユーザーのアイデンティティに関連するサービスロールとコンテキストに基づき、そのユーザーに自動的に付与される使用権。

固定属性

サービスロールとアイデンティティに関連付けられたコンテキストによって判別され、特定のユーザーに自動的に付与される属性。

コネクタ

コネクタとは、Sun Microsystems 社の J2EE プラットフォーム上で稼動している Java アプリケーションサーバーに各種のデータベースとアプリケーションがアクセスできるようにするプログラムです。コネクタにより、Select Identity はエンタープライズアプリケーションにアクセスし、アイデンティティプロファイル情報を含むシステムリソースと通信することができます。SI には事前定義された複数のコネクタが付属しており、バックエンドのデータストアとのデータアクセスをサポートします。たとえば、アイデンティティプロファイル情報を保有する Select Identity システムリソースと通信する J2EE コネクタが含まれています。

コンテキスト

サービスにアクセスできるユーザーの論理的なグループ化。

コンテキストエンジン

サービスとユーザーのコンテキスト定義に基づいてデータを取得するシステムコンポーネント。

コンテキスト属性

ユーザーをグループ化する共通の属性で、特定のサービスロールを通じてサービスにアクセスできるようにします。たとえば、「East」コンテキストは「East」属性を持つユーザーをグループ化し、ユーザーは「XYZ サービス」内で「East」サービスロールを担えるようになります。

コンポジットサービス

1 つのユニットとしてアクセスできるようにサービスをグループ化する仕組み。たとえば、ユーザーがコンポジットサービスに登録した場合、結果として実際には複数のサービスへのアクセス権を所有します。

サービス属性

サービスが利用できる、またはサービスが必要とする属性と値のセット。属性は、[属性] ページを通じて作成および管理されます。

サービス属性値

ユーザーや承認者がフォームから選択できる値を限定します。

サービス属性のプロパティ

フォームのフィールドの表示方法を定義する設定。

サービスフォーム

ユーザーグループにとって有効なサービスの制限付きフォーム。フォームを使用すると、サービス登録フィールドのサブセットの定義、フィールド名の変更、フィールドの並べ替え、および特定のユーザーに対するフィールド値のマスクが可能です。

サービスロール

ユーザーの論理的なグループが Select Identity のサービスの使用権のサブセットにアクセスする方法を定義した、Select Identity の抽象概念。たとえば、XYZ サービスは「東部」、「中部」、および「西部」という 3 つのビジネス関係を持つことが考えられます。これらのビジネス関係をさらに分割することができます。たとえば、ビジネス関係「西部」は「北西部」および「南西部」という 2 つの詳細なビジネス関係を持つことが考えられます。サービスに含められるビジネス関係のレベル数に制限はありません。

サブジェクト証明書

クライアントまたはサーバーを識別し、認証を必要として、クライアントとサーバーの両方のキーストアに格納される証明書。

資格証明

セキュリティとアクセスコントロールの目的で、ユーザーのアイデンティティ確認に使用される情報です。たとえば、ユーザー名、パスワード、質問 / 答え、デジタル証明書、バイオメトリクスなどです。

自己サービス

エンド ユーザーが自分自身で安全にアイデンティティの管理やサービスへのアクセスができる機能。

自己署名証明書

作成者により署名され、作成者により正当であることを承認されるアイデンティティ証明書。

質問

システムへのアクセスを要求している個人から特定の応答を聞き出すために使用される質問。たとえば、「母親の名は何ですか」や「出生地はどこですか」といったものです。Select Identity には標準と個人という 2 種類の質問があります。標準の質問は管理者により作成されます。一般に、個人は初期ログオン時にこれらの質問に対して特定の答えを返し、答えはユーザープロファイルに格納されます。個人の質問はエンドユーザーにより作成されます。個人は独自の質問を作成し、特定の答えを返します。質問と答えは両方ともユーザープロファイル内に格納されます。

質問と答え

パスワードを忘れてしまった場合など、代わりとなる別の認証を行う方法。Select Identity はユーザーに質問を出し、答えが正しかった場合、パスワードをランダム値にリセットし、電子メールでユーザーに送信します。

自動検出

データファイルからインポートすることにより、指定したサービスに対して Select Identity にユーザーアカウントを追加するプロセス。

終了

存在しないユーザーのアカウントを Select Identity から削除すること。

使用権

使用権とは、アイデンティティに付与されたリソース別の特権。アカウント ID、ロールメンバーシップ、グループメンバーシップ、アクセス権、特権などです。使用権は、許可、つまりアクセス権ともみなされます。

除外ルール

例外を処理するルール。除外ルールは、共通の属性または使用権の値を持つ一連のユーザーを、特定サービスへの登録、特定使用権の割り当て、特定属性値の使用の対象から除外します。外部コールを使用することで、除外ルールはどのワークフローからでも呼び出すことができます。

承認者

ユーザー管理リクエストを承認する Select Identity 管理者。承認者は、承認者レベル権限を持つ管理者ロールを保有していなければなりません。

承認プロセス

あるアイデンティティに関する使用権の関連付け、変更、または失効を承認するプロセス。このプロセスは、これらのワークフローテンプレート経由で自動化されます。

証明書

エンティティ (発行者) からのデジタル署名された記述で、別のエンティティ (サブジェクト) の公開キーと情報が特定の値を持つことを示します。

証明書失効リスト (CRL)

無効化または取り消された証明書のリスト。

シングルサインオン (SSO)

ユーザーが資格証明 (名前とパスワード) のセットを 1 回入力して、複数のアプリケーションにアクセスすることのできる、セッション / 認証プロセス。Web SSO は、Web アプリケーション用の特殊な SSO システムです。

信頼ストア

サブジェクト 証明書の検証に使用される、対応する 自己署名または署名証明書を保存するファイル。

信頼できるリソース

アイデンティティ情報の「機関」として指定されているリソース。Select Identity のアカウントは、信頼できるソースのアカウントに対して調整されます。

セキュリティリポジトリ

物理キーをクライアントに透明化する論理キーを格納するファイル。

設定

設定機能により、ワークフロー、リソース、サービス、および属性など、Select Identity の設定と構成をインポートおよびエクスポートできます。これはテスト環境から実稼動環境へ移行する際に便利です。

設定管理

設定管理機能により、Select Identity の設定変更のための承認ワークフローが設けられます。

設定承認者

この機能が有効になっているシステムで設定管理変更を承認する権限が与えられる、特殊な用途の管理者ロール。このロールを所有するユーザーだけがシステム設定への変更を承認できます。

設定レポート

設定レポートは、ユーザー、管理者、サービス管理アクティビティに関する現在のシステム情報を提供します。

遷移

遷移とは、あるアクティビティから別のアクティビティへのリンクです。遷移には、条件付きと無条件の 2 種類があります。条件なしの遷移を使用して 2 つのアクティビティをリンクさせると、2 つ目のアクティビティは常に 1 つ目の後に実行されます。条件付き遷移の場合、ある条件に合致しなければ次のアクティビティが実行されません。たとえば、少なくとも 2 人の管理者がリクエストを承認した場合にのみワークフローが先に進むように遷移を定義できます。

相互認証

X.509 PKI (公開キーインフラストラクチャ) に定義された標準に準拠したデジタル証明書を使用して、クライアントとサーバーの間に双方向のセキュリティ保護された通信を確立する方法。各クライアントとサーバー (通信エンドポイント) は、クライアントまたはサーバーをそれぞれ認証する目的で発行された、有効な証明書を提示する必要があります。この証明書は他方のエンドポイントにより信頼され、無効になっていません。

属性

サービスまたはアイデンティティプロファイルなど、Select Identity 内のオブジェクトを定義する際に役立つ、値を含むデータフィールド。たとえば、有効値として“IT”、“sales”、または“support”を持つ“department”という属性が考えられます。単一値属性により、ユーザーは属性の有効値を 1 つ入力または選択できます。複数値属性により、複数の有効値を選択できます。

属性マッピング

リソース属性の名前を対応する Select Identity 属性の名前に関連付けるプロセス。これにより、両者間でのデータ交換が簡単になると共に整合性が維持されます。

待機アクティビティ

次のアクティビティに移動する前に現在作成中のアクティビティでアクションを発生させる必要がある場合、待機アクティビティのチェックボックスを選択します (たとえば、承認者がアカウントリクエストを承認または拒否する場合)。

待機インスタンス

実行中のワークフローインスタンスで待機アクティビティが発生すると、ワークフローインスタンスは外部リソースによって再開されるまで一時停止します。一時停止したワークフローインスタンスは待機インスタンスと呼ばれます。

対称キー

対称キーは秘密キーとも呼ばれます。暗号化と復号化の両方に使用されます。メッセージの送信者と受信者は、メッセージの暗号化と復号化に使用される、単一の共通キーを共有します。

調整

Select Identity アカウントとシステムリソースとの同期をとるためのプロセス。アカウントデータは SPML データファイルから Select Identity システムに追加されます。

調整の停止

Select Identity のユーザーインタフェースを使用し、調整タスクの処理を手動で停止するプロセス。完了しているタスクには影響しません。処理されていないタスクは停止されます。

調整の復旧

Select Identity のユーザーインタフェースを使用し、調整タスクを手動で再試行または再送信するプロセス。タスクの再試行は最後の障害ポイントまたはスタックポイントからタスクを回復し、レコードを再試行します。元のタスクまたは回復されたタスクのステータスは、最新の実行結果で書き換えられます。タスクの再送信は古いタスクからのデータをそのままコピーして、新しいタスクを最初から実行します。新しいタスクは専用のレコードとレポートを持ちます。前のジョブの実行で処理中の状態で残されたレコードは停止されます。

調整ルール

ユーザーアカウントで実行される操作を定義するルール。調整ルールは、資格条件に基づいてこれらの処理を実行します。ルールに指定されたアクションは、ユーザーが資格条件を満たす場合にのみ適用されます。調整ルールは、リソースの調整ポリシーに基づいて調整の実行中に、またはワークフローの外部コールによって呼び出すことができます。

通信エンドポイント

通信リンクが終了するポイント。

通知

システムイベントが発生した場合、通常電子メール経由で送信されるメッセージ。Select Identity における通知は、通知メッセージ内に送信された情報を制御するテンプレートを使用して構成および設定します。

通知テンプレート

通知テンプレートは、ユーザーのアカウントリクエストの承認、アカウントの削除、パスワードのリセットといった特定のタイプのシステムイベントが発生した際、Select Identity により自動送信される標準的な電子メールメッセージの形式および内容を定義します。

データサービステンプレート

プリンシパルに関連するデータ属性のクエリと修正のプロトコルを定義する仕様書で、データサービスによって公開されます。プロトコルは、これらの属性に関する通知の登録と、その通知の送受信に対しても定義されています。また、データサービスに関するガイドライン、共通 XML 属性、およびデータ型も定義されています。

データファイル

「自動検出」または「調整」を通じて Select Identity に追加されるユーザーアカウントを定義することのできる SPML ファイル。

デフォルトのワークフローテンプレート

Select Identity では、デフォルトのワークフローテンプレートを提供しています。これらのテンプレートは、それぞれ一般的なワークフロープロセスのサンプルになっています。毎回新しいワークフローテンプレートを作成する手間を省くために、デフォルトのテンプレートをサービスロールに割り当てられます。テンプレートはそのまま使うことも、コピーして名前を変更し、自由に修正することもできます。ワークフローテンプレートも参照してください。

登録

1 つまたは複数のリソースへのアクセスをリクエストするプロセス。登録は、通常、リソースアクセスを求めるエンドユーザー、またはユーザーに代わってユーザーを登録する管理者によって実行されます。

名 - 値ペア

名前 - 値ペアは、属性識別子 (フィールド名) と、あるオブジェクトに対するその属性値との組み合わせです。たとえば、「名前 : ジョンスミス」は人物に対する属性名 - 値ペアとなります。

認証

パスワードとユーザー ID の組み合わせなどアイデンティティに関する証明書の確認。不正なアクセスを防止します。

認証機関 (CA)

他者が使用できるデジタル証明書を発行し、証明書に含まれるキーが証明書に記載されている人、サーバー、組織、またはその他のエンティティに属することを保証する組織またはエンティティ。

配布

ビジネス環境で意図したとおりに機能するようにソフトウェア、ハードウェア、機能、またはサービスをインストールして起動すること。

パスワード検証機能

パスワードを認可パスワードのリストに対比させて検証する機能。

パスワード妥当性検査機能

パスワードの値を事前定義されたパラメータと対比して妥当かどうか確認する機能。定義はたとえば、少なくとも数字を 2 つ含む英数字 6 ～ 12 文字などです。

パスワードのリセット

システムが生成した値にパスワードを設定すること。

ビジネス関係

サービスロールの定義を参照してください。

ビジネスプロセスエンジン

すべてのワークフロー、調整、ポリシー、フォーム、階層式アクセス、監査、およびレポートの機能のサービスを提供するシステムコンポーネント。

非対称キー

公開キーと秘密キーを含むキーまたはキーペア。公開キーは暗号化に使用され、秘密キーは復号化に使用されます。秘密キーは署名にも使用できますが、公開キーは署名の検証にのみ使用できます。秘密キーは秘密が維持されますが、公開キーは広く配布できます。

非同期呼び出し

ワークフローがリクエストの処理を継続できるようにした上で、呼び出したアプリケーションの動作を完了させるようにする、アクティビティやアクションのプロパティ。このプロパティにより、リクエスト処理のボトルネックを低減できます。

フォーム

エンドユーザーからの情報を収集するために使用される電子的な文書。フォームは、多くの業務プロセスにおいて、情報の捕捉とシステム操作のために Select Identity により使用されます。ほとんどの Select Identity フォームは、特定の論理グループユーザーが値を入力可能なプレゼンテーションビューにおいて、サービス属性フィールドのサブセットで構成されます。たとえば、管理者用のユーザー追加フォーム、管理者用のユーザー使用権付与フォーム、ユーザー用のプロファイル修正フォームなどを定義できます。

不変変数

インスタンスを非活性化 (Passivate) して不変になった変数。インスタンス全体に変数のライフサイクルを拡張するには、変数を不変にしなければなりません。これにより、待機アクティビティより先に変数が作成でき、ワークフローインスタンスが再開された後にアクセスが可能となります。変数を不変にするには、名前の頭に「$」を付けます。たとえば、$retryCount は不変変数ですが retryCount は不変ではありません。

ブロック

ワークフロー内の関連アクティビティのセット。ブロックには、アクティビティのサブセット (ブロックレベルのプロパティ) で共有する情報を定義すること、およびブロックレベルのレポート作成を行うことの 2 つの目的があります。たとえば、承認リクエストを送信し、応答を待ち、リクエストのステータスをワークフローに戻すようなブロックを作成することができます。ブロックはワークフロー内のサブプロセスと考えることができます。

ブロックビュー

ワークフロー内の特定ブロックに関連付けられたビュー。たとえば、ワークフローは各承認ブロックに対して複数のビューを保有でき、それぞれ異なるユーザー属性のセットを表示できます。

ブロックフォーム

ワークフロー内のブロックに明確に関連付けられたフォーム。たとえば、ワークフローは各承認ブロックに対して異なるフォームを保有でき、そのフォームは異なるユーザー属性のセットを表示できます。

プロファイル

名前、住所、肩書き、会社名、コストセンターなど、アイデンティティに関連付けられている記述的な属性のグループ。

プロファイルの属性

名前、住所、肩書き、会社名、コストセンターなど、アイデンティティに関連付けられている記述的な属性。

ポリシー

組織の業務管理を支援するために、組織で設定された規則の集合。たとえば、従業員がアクセスできる内部情報リソースおよび外部情報リソースの種類をポリシーで規定できます。

無効化

削除することなく使用を停止することで、通常は一時的に行います。たとえば、Select Identity でユーザーアカウントとサービスを無効化できます。

ユーザークラスタ

ユーザー ID のグループで、1 次ユーザーアカウント 1 つと、関連する複数の 2 次アカウントで構成されます。これは、複数のリソース上で複数のユーザーアカウントを持つように 1 名のユーザーのアイデンティティを Select Identity で管理できる機構です。

ユーザーのインポート

データファイルからデータベースにコピーすることにより、指定した Select Identity のサービスに対してユーザーアカウントを追加するプロセス。

リクエスト

ユーザーアカウントの追加、変更、または削除を開始する、Select Identity 内のイベント。

リクエストイベント

ユーザーアカウントが追加、変更、または削除されるたびに、Select Identity 内にリクエストイベントとして登録されます。

リソース

Select Identity BSIM ソリューションの一部である、任意の単一アプリケーションまたは情報リポジトリ。リソースには、一般的に、アプリケーション、ディレクトリ、アイデンティティ情報を保存するデータベースがあります。

ロール

使用権をアイデンティティに関連付けるシンプルな抽象概念。ロールは使用権の集合体で、一般的にジョブ機能別に編成されます。

ルール

システムの動作を制御するために Select Identity で使用される XML ファイル。Select Identity で使用されるルールのタイプに関する詳細については、調整ルールおよび除外ルールを参照してください。

有効化

ユーザーアカウントなど無効になっているものを復元したり、機能や設定を稼動状態にしたりすること。

ワークフロー

Select Identity でリクエストを完了させるプロセス。多様なリクエストに必要なさまざまなレベルの承認を含みます。ワークフローはプロセスフローの形で記述され、Workflow Studio で作成するワークフローテンプレートで定義されます。リクエストはワークフローを使って追跡することにより、現在の進捗状態を詳細に把握できます。

ワークフロー外部コール

ワークフロープロセスの途中で呼び出される「サブルーチン」。これは、通常のワークフロープロセス以外の外部プロセスを呼び出す小規模なカスタムアプリケーションのような外部アプリケーション呼び出しとなります。

ワークフロー承認者ロール

ユーザープロビジョニングワークフロー操作の承認権限を付与するデフォルトの管理者ロール。

索引

か行

さ行

た行

は行

や行

ら行

わ行