Tivoli software

IBM

SG88-4053-00
(英文原典 : REDP-3678-01)

Redpaper

Axel Buecker
Paul Ashley
Neil Readshaw

フェデレーテッド ID およびトラスト管理

概要

ユーザー ID のライフサイクルを管理するには、かなりのコストがかかります。大半の組織では、従業員 ID、ビジネス・パートナー ID、および顧客 ID の管理を行う必要があります。事業体とこれら個人の関係は頻繁に変わり、変更があるたびに管理アクションが必要になります。この状況は個人ユーザーにとっても不満を感じるものです。なぜなら、ユーザーがアクセスするすべての事業体で別個のアカウントを作成する必要があるためです。

*フェデレーション*とは、一緒に仕事をする 2 者以上のビジネス・パートナーからなるグループとして定義されます。このフェデレーションを形成すると、互いの顧客により良い対応をしたり、ID 管理コストを削減したりできるようになります。例えば、金融機関では、サード・パーティーのリサーチ会社が提供する金融マーケット情報に大口クライアントがシームレスにアクセスできるようにすることができます。行政機関の部門間で協力して、市民が 1 回のログインでさまざまな行政サービスを利用できるようにすることもできます。また、小規模なオンライン・ストアでは、自社で多数の顧客記録を管理するのではなく、そのようなサービスを提供する金融機関とパートナー関係を築くことができます。どのケースも、各事業体が共同で*ビジネス・フェデレーション*を作成する必要があります。

ビジネス・フェデレーションは、*トラスト関係*の上に成り立ちます。これらのトラスト関係は、フェデレーションの参加者間による通信外のビジネス契約と法的契約を使用して作成されます。これらの契約は、フェデレーションの運用を始める前に締結している必要があります。[1]

ビジネス契約と法的契約が締結されたら、これらのパートナー間でフェデレーション調整をサポートするテクノロジーを利用して、共同運営を開始することができます。つまりこのテクノロジーによって、フェデレーション機能とトラスト管理機能、暗号化サポート、およびプロトコル実装が実現され、インターネット環境でセキュアなパートナーシップを運用できるようになります。

フェデレーションを通して ID を管理するため、*フェデレーテッド ID 管理*は、企業の境界を越えた ID 管理を簡素化する標準システムを提供します。組織でこのシステムを利用すると、ID およびアクセス管理のコストをフェデレーション内のビジネス・パートナーに任

[1] この IBM® Redpaper で後述する新しいユーザー中心の ID プロトコルを使用すると、疎結合パートナーシップも可能になります。

せることができます。この機能により、事業体は顧客に関する信頼された情報を受け取ることができます。その事業体がその顧客を登録したり、顧客がログインして ID 情報の再入力を求められたりすることはありません。

もう 1 つの重要な考慮事項は、*Web サービス* の利用です。Web サービスが登場した目的は、企業間、プラットフォーム間、およびベンダー間のビジネス・インテグレーションの問題に対応するためです。Web サービスとは、情報技術 (IT) サービス間の相互運用を容易にし、企業の幅広いビジネス・プロセスにアプリケーションを組み込むことのできるテクノロジーを集結したものです。企業は Web サービス・テクノロジーを利用することで、使用可能なサービスについて可視化し、標準のインターネット・プロトコルでそれらのサービスへのアクセスを提供することができます。

この IBM Redpaper では、整合性と統一性のある先進的な方式で企業間の e- ビジネス環境を保護する IBM Tivoli® ソフトウェアについて説明します。オープンなセキュリティー標準の上に構築され、Web ミドルウェア (Java 2 Platform Enterprise Edition (J2EE) および Microsoft .NET) と緊密に統合された Tivoli セキュリティー・ソリューションを利用すると、ビジネスの範囲を広げることができます。これらは既存の Web セキュリティー投資環境の上に構築されるため、既存の環境を短期間で拡張して Web サービスとフェデレーション標準を利用することができます。

Tivoli ソフトウェアの技術戦略は多面的です。

- 企業間、プラットフォーム間、ベンダー間でのセキュアな統合を実現するために、オープン・スタンダードをサポートしています。
- Web サービスの ID サービス・メカニズムに対する拡張製品サポートを提供し、さまざまな Web サービス開発およびデプロイメント・プラットフォーム (IBM WebSphere®、Microsoft .NET など) とのシームレスな統合を実現します。
- 既存の ID 管理、エクストラネット・アクセス管理、およびトラスト管理の上に構築される先進の方式を使用します。
- 全く新しいクラスのセキュアな e- コマース・ビジネス・サービスをフェデレーテッド ID 管理上に構築できるようにします。

この Redpaper では、技術戦略をコンテキストに含めるために、フェデレーションに必要な機能およびフェデレーションのメリットと、適用されるセキュリティー標準を重点的に説明します。また、Web、Web サービス、およびサービス指向アーキテクチャー (SOA) 環境に対して標準ベースのセキュリティー方式を提供することで、IBM Tivoli Federated Identity Manager を使用してビジネス・フェデレーションを実現する方法についても重点的に説明します。

お客様のシナリオ

このセクションでは、フェデレーテッド ID およびトラスト管理によって新しいビジネス構想を実現できるお客様の事例について説明します。これらのシナリオに対応する技術ソリューションについては、本書で後述します。

公共部門 : 行政機関サービス向けのシングル・サインオン

このシナリオでは、ある行政機関が、市民がインターネット上のすべての行政サービスにシングル・ログインでき、さまざまな部門の行政サービスにシームレスにアクセスできるようにすることを希望していました。このシングル・ログインにより、ユーザーの利便性が向上し、ユーザーにオンライン・トランザクションを利用する動機付けを与え、部門内で処理する運用コストを削減することができます。また、この行政機関では、物理的な取引と比較し

てオンライン・トランザクションにかかるコストを削減するとともに、すべての部門で ID 管理プロセスが重複するために増大している ID 管理コストを削減したいと考えていました。

通信業 : 外部パートナーへのサービス提供

このシナリオでは、ある通信プロバイダーが、新しいサービスを外部のパートナーにセキュアな方法で提供することを希望していました。この通信プロバイダーは、外部パートナーからの付加価値サービスを提供することで、自社の事業を拡大しました。標準ベースの Web サービスを通じてアクセス可能なこれらの新しいサービスは、信頼されたパートナーのみ利用することができます。さらに、使用している IT 機能や標準設定の異なるパートナー各社から要求を受け入れるという要件もありました。また、社内アプリケーションで必要な変更を最小限にして、これらさまざまなパートナーに対応することも重要です。

金融業 : 既存の IT システムの再利用

このシナリオでは、金融サービス業のある組織が、ポータルから既存のメインフレーム CICS® アプリケーションのビジネス・ロジックを再利用することを希望していました。この再利用により、新しいビジネス・パートナーがアプリケーションにアクセスできるようになり、収益を増やし、新たな成長機会を得ることができます。この組織は、既存の IT リソースを柔軟に統合でき、サービスを再利用しやすいという理由から、SOA を選択しました。

フェデレーテッド ID 管理

ビジネス・フェデレーションを確立する際の主な要件の 1 つに、フェデレーション全体での ID 管理があります。このプロセスは一般に *フェデレーテッド ID 管理* と呼ばれます。ターゲット・アプリケーションやリソースに接続しているユーザーの監査証跡と共に、セキュアかつ高い費用効率でビジネス・コラボレーションを確立するには、このプロセスが必要です。組織でこのプロセスを利用すると、ID 管理のコストをフェデレーション内のビジネス・パートナーに任せることができます。

フェデレーテッド ID 管理には、ビジネス・フェデレーションのユーザーにとっても直接的なメリットがあります。ユーザーが自分の組織に対して自分の身元を証明し、認証を行うために必要なことは、自分の資格情報を覚えることのみです。フェデレーション内の他の組織に対する認証はシームレスに処理されるため、直接的なユーザー対話は不要です。この単純な認証により、ユーザーが覚える必要のある資格情報の数を減らすと共に、ユーザーがサービスにアクセスするために資格情報を提供しなければならない回数を減らせるため、より効率的なユーザー・エクスペリエンスが実現されます。

フェデレーションにおける役割

フェデレーションにおける重要な役割は、*アイデンティティー・プロバイダー* および *サービス・プロバイダー* です (4 ページの図 1 を参照)。

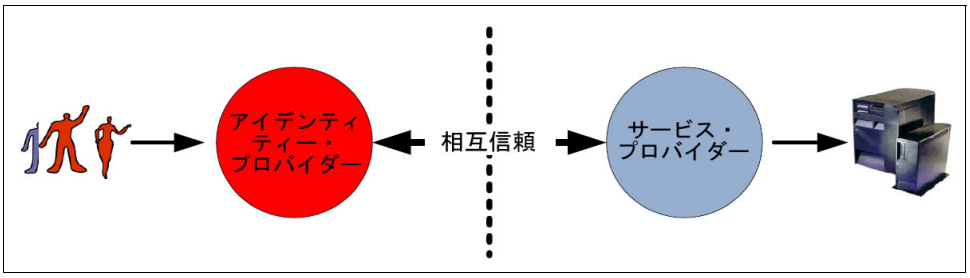

図 1　ビジネス・フェデレーションとアイデンティティー・プロバイダーおよびサービス・プロバイダー

次に、これらの役割について詳しく説明します。

アイデンティティー・プロバイダー

アイデンティティー・プロバイダー (*アカウント・プロバイダー*とも呼ばれる) は、ID フェデレーションの関係者の " 保証人 " となります。つまり、ユーザーの身元 (ID) を他の関係者に対して保証します。

アイデンティティー・プロバイダーは、以下の責任を持ちます。

- ユーザーとその ID を管理する
- 資格情報を発行する
- ユーザー管理を処理する
- ユーザーを認証する
- サービス・プロバイダーと共にユーザーの身元 (ID) を保証する

サービス・プロバイダー

サービス・プロバイダー (*Relying Party*、リソース・パートナー、またはコンシューマーとも呼ばれる) は、トランザクションにおける " 検証者 " です。

サービス・プロバイダーは、以下の責任を持ちます。

- サービスへのアクセスを制御する
- アイデンティティー・プロバイダーから表明された ID 情報を検証する (一般にはデジタル署名を検証する)
- 表明された ID に基づいてアクセス権を提供する
- ユーザー・プロファイル全体ではなく、関連するユーザー属性のみをローカルで管理する

特定のビジネス・シナリオでは、1 つの組織がアイデンティティー・プロバイダーにもサービス・プロバイダーにもなる場合があります。例えば、複数の行政機関が互いのアプリケーションにアクセスする場合、所定のケースでどちらの組織がサービスとアプリケーションを提供するかに応じて、各機関がアイデンティティー・プロバイダーの役割を担ったり、サービス・プロバイダーの役割を担ったりすることができます。

トラスト管理

*トラスト*は、関係の一方の関係者が、もう一方の関係者によって作成されたステートメント (*要求*とも呼ばれる) を信用することに同意したことを示す関係者間の表現です。トラストは、過去の履歴、経験、およびリスク許容度の組み合わせに基づくことができます。

トラスト管理 では、組織内、セキュリティー・ドメイン内、およびシステム内のエンティティー間の関係に対処します。これらの関係には、システム間や企業間などがあります。トラスト管理では、ビジネス面とテクノロジー面の 2 つを扱います。ビジネス面では、2 つのエンティティーによる一連のビジネス遂行ルールへの同意を扱います。これらのルールには、関係管理や責任管理などの法律面および契約面が含まれます。

信頼された関係を確立するには、ビジネス・プロセスとポリシーが必要です。これらのプロセスには、従うべき法的手順の選択や、責任を評価するためのプロセスなどが含まれる場合があります。また、リソース・アクセスに固有のポリシーが含まれる場合もあります。これらのポリシーは、企業とそのビジネス・パートナー間のビジネス調整の一部としてすでに存在することが多々あります。

トラスト管理のテクノロジー面では、暗号化方式によるトラスト確立機能をサポートするインフラストラクチャーの管理を扱います。これには、鍵管理 (強度、鍵の検証など) プロトコルや属性など、トラストを確立するための技術的な考慮事項が含まれます。

フェデレーテッド ID 管理のコンテキストにおいて、トラスト管理機能はアプリケーション・ビジネス・ロジックの一部ではなく、IT インフラストラクチャーの一部と見なす必要があります。トラスト・インフラストラクチャーには、ユーザーや Web サービスの ID を表すセキュリティー・トークンの検証、変換、発行を行う ID サービスなどのメカニズムがあります。環境内の各種システム、アプリケーション、プラットフォームと統合される共通のトラスト・インフラストラクチャーを使用することで、整合性および柔軟性の向上と TTM（商品化までの時間）の短縮を実現できます。本書では、IBM Tivoli Federated Identity Manager が提供するフェデレーションおよびトラスト・インフラストラクチャーにより、シームレスな B2B (Business to Business) および B2C (Business to Consumer) コラボレーションをどのように実現できるかを説明します。

フェデレーション・プロトコル

本書で扱う問題の 1 つは、ユーザーがアクセスする Web サイトごとに、異なる認証資格情報 (ユーザー名とパスワードなど) が必要であるという一般的なことです。ユーザーは、認証を必要とする Web サイトごとに登録と資格情報の作成を求められ、さらにこれらのユーザー名とパスワードをすべて覚える必要があります。また、各 Web サイトの要求に応じて、これらのパスワードやその他の ID データを更新する必要もあります。時間またはチャレンジ応答ベースのトークンを使用するなど、より強力な認証を必要とするサイトの場合、ユーザーは増え続ける物理トークン・セットと共に、新たに鍵チェーンの問題にも直面します。

しかも、これらのユーザー・アカウントの管理については、各企業にとって ID 管理コストの問題があります。このようなコストの問題は、たまに使用されるアカウントが数百万件もあるような、中小規模ビジネスには特に負担となります。例えば、パスワードの再設定に関連するコストが挙げられます。

これらの問題を解決するために、提携 Web サイトからなるフェデレーションにユーザーが一度サインオンするだけで良いフェデレーション・プロトコルが開発されました。このセクションでは、2 種類の Web シングル・サインオン・プロトコルについて説明します。最初のタイプは企業中心のモデルに重点を置いたもので、*Security Assertions Markup Language (SAML)*、*Liberty*、および *Web services (WS) Federation* の各仕様が含まれます。これらのフェデレーション・プロトコル仕様は数年前からあり、広く採用されています。2 番目のタイプはユーザー中心の ID スキーマです。これらは採用され始めたばかりの比較的新しい仕様で、ユーザーが自分のデジタル ID をより直接的に管理できるようにすることに重点を置いています。

トラスト関係は、これらの各種モデル・タイプによって異なります。企業中心のモデルの場合、トラスト関係は常に 2 社以上の企業間になります。これらの企業が、フェデレーション

に参加するビジネス・パートナーです。ユーザー中心のモデルでも、このような調整は可能です。ただし、ユーザー中心のモデルでは、自己発行の資格情報も可能です。自己発行の資格情報をパスワードの代わりとして使用すると、Web サイトのユーザー ID 管理に関する一部の問題を軽減できます。

フェデレーテッド・シングル・サインオン

*フェデレーテッド・シングル・サインオン*は、さまざまなブラウザー・ベースのシナリオに使用されます。ユーザー (コンシューマー) は、Web サイト (アイデンティティー・プロバイダー) に対して認証を行うことができ、その後は再度認証を行うことなく他の Web サイト (サービス・プロバイダー) にアクセスすることができます。サービス・プロバイダーは、ユーザーを認証するアイデンティティー・プロバイダーを信頼し、アイデンティティー・プロバイダーがユーザーに代わって発行するセキュリティー・トークンを受け入れます。図 2 に、このプロセスの一例を示します。このプロセスでは、SAML ブラウザー・アーティファクト・プロファイルを使用して、ユーザーが Web サイト A から Web サイト B にシングル・サインオンできるようにします。この図では、アイデンティティー・プロバイダーとサービス・プロバイダーの両方で IBM Tivoli Federated Identity Manager が使用されています。ただし、標準ベースの方式なので、他の製品やオープン・ソースの実装を使用することができます。

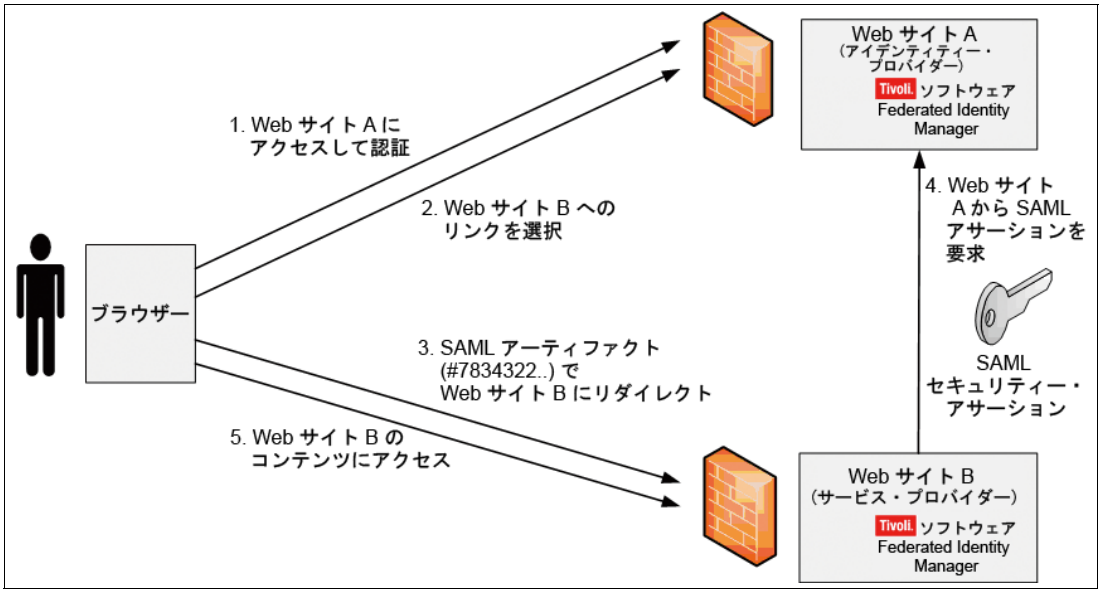

図 2　フェデレーテッド・シングル・サインオン用の SAML ブラウザー・アーティファクト・プロファイル

フェデレーテッド・シングル・サインオンは、以下のような多数の ID 機能を網羅しています。

シングル・サインオン　図 2 に示すように、ユーザーはアイデンティティー・プロバイダーに対して認証を行った後、再度認証を行うことなく他のサービス・プロバイダーにアクセスすることができます。

シングル・サインオフ　ユーザーがシングル・サインオフ・アクションを実行する場合、各ユーザーに対してアクティブなアイデンティティー・プロバイダー・セッションとサービス・プロバイダー・セッションがシステムによってすべて削除されます。

アカウント・リンク　シングル・サインオンの前提条件として、ユーザーのアイデンティティー・プロバイダー・アカウントとサービス・プロバイダー・アカウントをリンクします。

アカウントのリンク解除 ユーザーのアイデンティティー・プロバイダー・アカウントとサービス・プロバイダー・アカウントの結合を解除します。

別名管理 アイデンティティー・プロバイダーとサービス・プロバイダー間のユーザー・アクセスで、ユーザーの実際の ID ではなく別名を使用できるようにします。

属性要求 サービス・プロバイダーは、アイデンティティー・プロバイダーからユーザーに関する追加情報を要求できます。

したがって、フェデレーテッド・シングル・サインオンはフェデレーテッド ID 管理の特別なユース・ケースであり、Web を使用してアクセスする提携事業体間で ID を管理することに重点を置いています。

フェデレーテッド・シングル・サインオンでは、アイデンティティー・プロバイダーとなる企業とサービス・プロバイダーとなる企業が異なり、また各社の IT 環境も異なるのが一般的なので、業界標準が非常に重要です。このため、単一ベンダーのプロプラエタリー・ソリューションは適していません。

フェデレーテッド・シングル・サインオンをサポートしている一般的な業界標準は 3 つあります。それらは SAML、Liberty、WS-Federation です。IBM Tivoli Federated Identity Manager は、各種バージョンを含めてこれらの各仕様をサポートしています (表 1 を参照)。

表 1 IBM Tivoli Federated Identity Manager でサポートされるフェデレーテッド・シングル・サインオン標準

プロトコル	バージョン
SAML	1.0, 1.1, 2.0
Liberty	1.1, 1.2
WS_Federation	1.0

Security Assertions Markup Language

SAML は、ベンダー間シングル・サインオンの相互運用性を目的として設計された仕様です。SAML は、OASIS Security Services Technical Council (SSTC) を通じた OASIS の後援のもと、(IBM を含む) ベンダーのコンソーシアムによって開発されました。SAML には、以下の 2 つの主要コンポーネントがあります。

- ユーザーを表すセキュリティー・トークンを記述する *SAML アサーション* の定義
- シングル・サインオン・プロトコルの *SAML バインディングおよびプロファイル* の定義

SAML アサーションは XML 形式のトークンであり、ブラウザーのシングル・サインオン要求完了または Web サービス要求完了の一部として、ユーザー ID (および属性) 情報をユーザーのアイデンティティー・プロバイダーから信頼されたサービス・プロバイダーに転送する際に使用されます。このように SAML アサーションを使用すると、ベンダーを問わず、ビジネス・パートナーのフェデレーション内で情報を転送することができます。したがって、SAML アサーションは、フェデレーション・スペース全体において大きな牽引力を持ちます。

プロトコルとして、SAML には SAML 1.0、1.1、2.0 の 3 つのバージョンがあります。SAML 1.0 および SAML 1.1 (合わせて SAML 1.x) は、シングル・サインオン機能に重点を置いています。Liberty Identity Federation Framework (ID-FF) 1.2 を原型として SAML 2.0 は、SAML 1.x よりも機能性が大きく向上しています。SAML 2.0 では、ID のライフサイクル機能をより考慮して、フェデレーテッド環境に関連するいくつかのプライバシー問題に対処しています。

SAML の仕様について詳しくは、以下の URL を参照してください。

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Liberty

Liberty Alliance Project は、(IBM を含む) ベンダーとユーザー組織からなるグループであり、オープンなフェデレーテッド方式でコンシューマーおよびビジネス・ユーザー向けのサインオンを実現するフェデレーテッド・ネットワーク ID ソリューションの提供を目的としています。

フェデレーテッド・シングル・サインオン・プロトコルは、Liberty Identity Federation Framework (ID-FF) の一部として開発されました。Liberty ID-FF 1.1 リリースと 1.2 リリースがあり、1.2 リリースは SAML 2.0 原型として OASIS に提出されています (上記を参照)。Liberty 1.2 には、SAML 1.0 および 1.1 では元々考慮されていなかった ID ライフサイクル機能が多数あります。Liberty ID-FF も今までどおり使用可能ですが、OASIS に提出されたことにより、SAML 2.0 がそれを置き換える形になったと見ることができます。

Liberty Alliance Project について詳しくは、以下の URL を参照してください。

http://www.projectliberty.org

WS-Federation

WS-Federation は (IBM を含む) ベンダーのグループによって作成されたものであり、Web アプリケーションと Web サービスの両方の ID 要件に対応できるように、WS-Trust の使用に対する機能拡張を提供することを目的としています (次の段落および表 2 を参照)。この目的は、ブラウザー・ベースのアプリケーションと Web サービス・ベースのアプリケーションの両方をサポートする共通方式を提供することです。SAML と Liberty ID-FF シングル・サインオンのどちらの仕様でも、ブラウザーと Web サービス間の共通性は主要な考慮事項ではありません。さらに、WS-Federation は、WS-Security ファミリーのその他の標準と緊密に調整されています。

WS-Federation では、ID ブローカリング、属性の要求と取得、フェデレーション・パートナー間の認証要求と許可要求、およびこれらの要求のプライバシー保護を実現するために、WS-Trust Security Token Service に対する機能拡張が定義されています。

WS-Federation には 1.0 と 1.1 の 2 つのリリースがあります。

ユーザー中心の ID

フェデレーテッド・シングル・サインオン・システムに対する批判の 1 つとして、*ユーザー中心* ではなく *企業中心* だという点があります。つまりこれらのプロトコルは、アイデンティティー・プロバイダーとサービス・プロバイダーと共に情報制御のフェデレーションに加わる必要のある企業の要件を満たすために設計されています。ユーザーには、アイデンティティー・プロバイダーとサービス・プロバイダーによって要求される情報についての制御権がそれほどありません。また、関連するトランザクションのタイプに必要とされる以上の情報を渡していることもよくあります。

ユーザー中心の ID システム (*Identity 2.0* とも呼ばれる) は、この制御権をユーザーに返そうとするものです。この方法ならば、ユーザーはどのようなユーザー情報をどのサイトに何の目的で開示するかについて同意を得ることができます。他にも、ユーザー中心の ID システムには、疎結合関係を確立できるというメリットがあります。Relying Party は必ずしも、アイデンティティー・プロバイダー (管理対象アイデンティティー・プロバイダーであれ自己発行であれ) とのトラスト関係を事前に確立する必要はありません。この調整により、ユーザーと Relying Party の両者にとってパスワード入力などを伴わない簡潔な認証連携処理が行われます。

9 ページの図 3 に、ユーザー中心のシステムの典型的なフローを示します。この図では、アイデンティティー・プロバイダーと Relying Party で IBM Tivoli Federated Identity Manager が使用されています。ただし、標準ベースの方式なので、他の製品や標準ベースの実装を使用することができます。

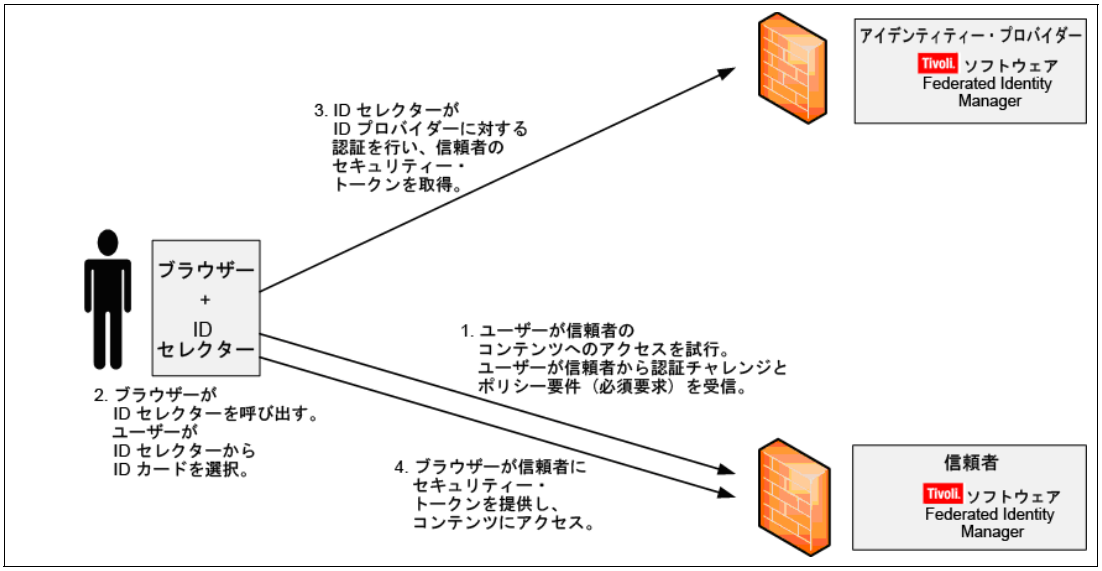

図 3　ユーザー中心のシングル・サインオン用の CardSpace

表 2 に示すように、IBM Tivoli Federated Identity Manager でサポートされるユーザー中心の ID プロトコルのファミリーは 2 つです。それは、OpenID[2] と、ID セレクターを使用する Information Card プロファイル (Microsoft Windows CardSpace[3]、Eclipse Higgins Project[4] など) です。

表 2　IBM Tivoli Federated Identity Manager でサポートされるユーザー中心のシングル・サインオン標準

プロトコル	バージョン
ID セレクター (Microsoft Windows CardSpace)	1.0 (WS-Trust 1.2 使用)
ID セレクター (Eclipse Higgins Project)	1.0
OpenID	認証プロトコル 1.1 Simple Registration Extension 1.0

Microsoft Windows CardSpace ID セレクター

Microsoft Windows CardSpace は、ユーザーのデジタル ID をユーザー自身が管理できるようにする ID メタシステムです。CardSpace によって導入された、ユーザーのデスクトップ上の新しいビジュアル・コンポーネントを *ID セレクター* と呼びます。ID セレクターは、ユーザーのブラウザーなどのクライアント側アプリケーションと連動して、認証要求をブローカー処理します。ID セレクターには、さまざまなユーザー ID のビジュアル表示である Information Card が含まれています。これらの ID は、個人 Information Card (外部検証なしでユーザーによって表明されたデータがカードに含まれる) または管理対象 Information Card (ユーザーがアイデンティティー・プロバイダーでのアカウントを持つ) にすることができます。

典型的な CardSpace のシナリオでは、ユーザーはブラウザーを使用してサービスを提供するサイト (*Relying Party* とも呼ばれる) にアクセスします。Relying Party の認証ページには、

[2] 詳しくは、http://openid.net/ を参照してください。
[3] 詳しくは、http://msdn2.microsoft.com/en-us/library/aa480189.aspx を参照してください。
[4] 詳しくは、http://www.eclipse.org/higgins/ を参照してください。

Information Card をサポートしていることを示すアイコンが含まれています。このアイコンをクリックすると、Relying Party からユーザーのブラウザーに認証チャレンジが送信されます。このチャレンジには、要求されるユーザー ID の属性の判別が含まれます (これらの必須属性は*要求*と呼ばれることがあります)。ID セレクターはユーザーのデスクトップに表示され、Relying Party に対する認証時に使用する Information Card を選択するようユーザーに促します。ユーザーが要求されている情報を認識できるように、Relying Party から要求される必須要求とオプション要求のセットが表示されます。さらにユーザーは、どの Information Card を使用するかと、オプション属性が提供されるかどうかを制御できます。Information Card が選択されると (管理対象 Information Card の場合)、アイデンティティー・プロバイダーに対するユーザー認証が行われ、Relying Party に適したセキュリティー・トークンが生成され、ID セレクターに返されます。この後、ブラウザーから Relying Party にセキュリティー・トークンが送信され、Relying Party 側でこのトークンが検証されて、認証フローが完了します。

Higgins ID セレクター

Higgins は、Microsoft Windows CardSpace で提供されるユーザー中心の ID メタシステムと同様のものをオープン・ソースで実装したものです。Higgins には、ID セレクター (ブラウザーまたはスタンドアロン)、アイデンティティー・プロバイダー / コンシューマーの Web ベース・サービス、ID 属性サービスの 3 種類の ID 機能があります。

ID セレクターは、先進の*情報カード* (*i- カード*) ベースの認証方式と互換性があります。アイデンティティー・プロバイダー / コンシューマーの Web ベース・テクノロジーを使用すると、Web サイトとサーバーを i- カード互換および OpenID 互換にすることができます。ID 属性サービスでは、既存の ID データ上の相互運用性および移植性レイヤー用のフレームワーク、つまり現行システムおよびディレクトリーを活用できるようにするためのマッシュアップが提供されます。

Higgins 自体は、多数の Eclipse プラグイン (または OSGI バンドル) で構成されます。これにより、最小限の占有スペースと少ない依存関係でこれらのサービスの多くを構成することができます。以下のリンクには、Higgins コンポーネントを使用して作成できるソリューションのリストが記載されています。必要に応じてこのリンクを参照してください (http://wiki.eclipse.org/index.php/Solutions)。

OpenID

OpenID は、オープン・ソース・コミュニティーから提供されている、ユーザー中心の ID システム用の単純なフレームワークです。OpenID プロトコルを使用すると、ユーザー ID が以下のような見慣れた URL で表されます。

http://myid.myopenidprovider.com/

ここに記載される他のフェデレーション標準と同様に、OpenID にもアイデンティティー・プロバイダーと Relying Party の概念があります。OpenID は、将来的には認証以外の ID サービスも組み込まれることが予想されます。

OpenID は特に、サービス・プロバイダーがユーザーやアイデンティティー・プロバイダーとの密結合関係を必要としない場合に適しています。多数の非商業サイトで OpenID が採用され、America Online (AOL) などのインターネット・サービス・プロバイダーの関心と注目を得るようになったのはこのためです。

Web サービス ID

もう 1 つの一般的なフェデレーション・タイプは、Web サービスを使用して実装されます。これまでに説明したフェデレーテッド・シングル・サインオンのシナリオでは、Web ベース・アプリケーションにアクセスするためのブラウザー・ベースのユーザー対話を扱います

が、Web サービスのフェデレーションはアプリケーション間通信に基づきます。Web サービスにも ID があり、フェデレーテッド・シングル・サインオンの場合と同じ ID フェデレーションとトラストの問題があります。ただし、適用されるプロトコルとセキュリティー標準は異なり、多くの場合、直接的なユーザー対話では認証情報を提供できない可能性があります。

Web サービス

*Web サービス*は必要なものを完備したモジュラー・アプリケーションであり、ネットワーク上で記述、公開、検索、呼び出しを行うことができます。Web サービスは、単純な要求 / 応答から完全なビジネス・プロセス対話まで、カプセル化されたさまざまなビジネス機能を実行します。典型的な Web サービス・アプリケーションは、サービス・コンシューマー、サービス・プロバイダー、および Web サービス定義を格納するためのレジストリー (オプション) で構成されます。Web サービスには、プラットフォームやプログラミング言語に依存しない標準のインターネット・プロトコルを介してアクセスできます。

WSDL

Web サービスの疎結合は、Web サービス記述言語 (WSDL) を使用することで実現されます。WSDL はデータ・フォーマットの定義と、プラットフォームに依存しない Web サービス・メッセージのトランスポートを行います。WSDL には、メッセージを交換するエンドポイント・セットとしてサービスを記述するための文法があります。WSDL 文書は、各サービス、各サービスにアクセスする方法、および期待される応答のタイプ (存在する場合) を記述した XML 文書です。

SOAP

SOAP は、ネットワーク経由のトランスポート用のメッセージを記述するための業界公認の仕様です。SOAP は、伝送プロトコルや XML 文書の構造に関係なく、XML 文書を送受信できるようにするメカニズムです。SOAP XML プロトコルは、メッセージ・プロトコルの送信に使用するトランスポートの上で、なおかつプロトコル・スタック内のドメイン固有の XML 文書の下に位置付けられます。

SOAP 拡張メカニズムを使用すればセキュリティーを追加できることが仕様に示されていますが、SOAP 仕様自体はセキュリティーに対応していません。

WS-Policy

WS-Policy には、XML Web サービス・ベースのシステム内のエンティティーの機能、要件、および一般特性を表現するための、柔軟で拡張可能な文法があります。WS-Policy は、これらのプロパティーをポリシーとして表現するためのフレームワークとモデルを定義します。ポリシー表現では、単純な宣言アサーションと高度な条件付きアサーションの両方が可能です。

WS-Policy は、1 つ以上のポリシー・アサーションの集合となる 1 つのポリシーを定義します。最終的にネットワーク上で公開する従来の要件と機能 (認証スキームやトランスポート・プロトコルの選択など) を指定するアサーションもあれば、ネットワーク上で公開はしないが、適切なサービスの選択と使用に重要な要件と機能 (プライバシー・ポリシーや QoS 特性など) を指定するアサーションもあります。WS-Policy には、各種のアサーションを一貫した方法で表現するための単一ポリシー文法があります。WS-Security Policy（後述を参照）などの従属標準には、特定のポリシー・クラスでの相互運用性に関する、より具体的なプロファイルがあります。

WS-Policy を構成する仕様は、以下の URL からダウンロードできます。

http://www.w3.org/Submission/WS-Policy/

WS-Security の仕様

図 4 に示す WS-Security ファミリーの仕様は、Web サービスの識別と保護を行うためのレイヤー方式を形成する、相互に関係のある各標準をまとめたものです。

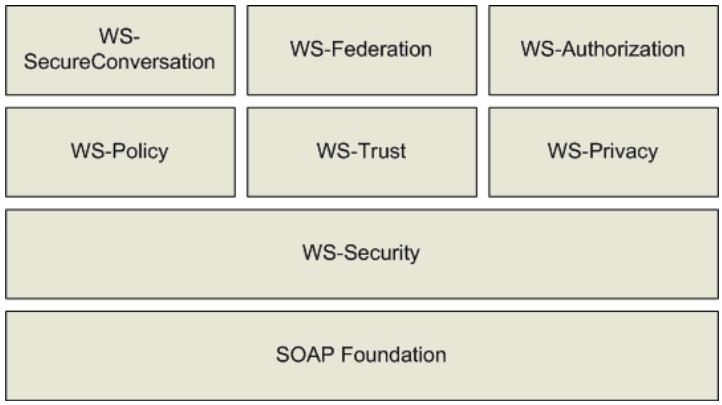

図 4 WS-Security ファミリーの仕様

13 ページの図 5 に、典型的な Web サービスの識別およびセキュリティー実装を示します。この図では、サービス・コンシューマーが Web サービス要求をサービス・プロバイダーに送信しようとしています。サービス・コンシューマーは、WS-Trust メッセージを使用して *セキュリティー・トークン・サービス* と通信し、セキュリティー・トークンを要求します。このトークンは、SOAP 要求を使用して送信されます。セキュリティー・トークンにはユーザーに関する ID 情報が含まれています。一般的な例は SAML アサーションです。

次に、この要求を暗号化して署名を付けるため、WS-Security 仕様に従って要求が保護されます。保護された要求とセキュリティー・トークンはサービス・プロバイダーに送信されます。サービス・プロバイダーでは、メッセージ上の署名がチェックされ、メッセージが復号化されます。さらに、要求が許可され、受信側のセキュリティー・トークン・サービスによってトークンが検証されます。

図 5 では、アイデンティティー・プロバイダーとサービス・プロバイダーの両方で IBM Tivoli Federated Identity Manager を使用して、セキュリティー・トークン・サービス (STS) が実装されています。ただし、この設計は Web サービスのセキュリティー標準に従っているため、代替製品やオープン・ソースの実装も使用可能です。

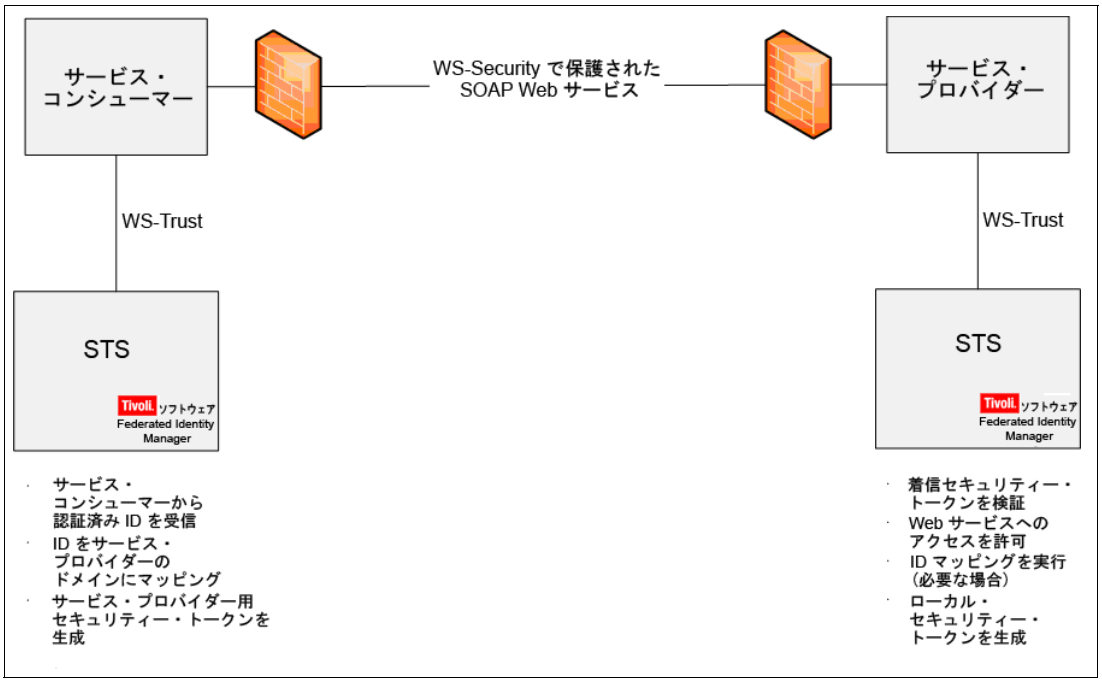

図 5　Web サービスの保護

WS-Security

WS-Security 仕様には、メッセージ・レベルのセキュリティーを得るための標準方式があります。SSL ではなく WS-Security を使用することの利点は、エンドツーエンドでメッセージ・レベルのセキュリティーを提供できることです。これはつまり、メッセージが複数のノード (つまり中継) を通る場合でも、メッセージが保護されることを意味します。また、WS-Security はトランスポート層のプロトコルに依存しません。SOAP over HTTP だけでなく、任意の SOAP バインディングに使用できます。

概要として、13 ページの図 6 に SOAP ヘッダーに追加できる Web サービスのメッセージ・セキュリティー・エレメントを示します。

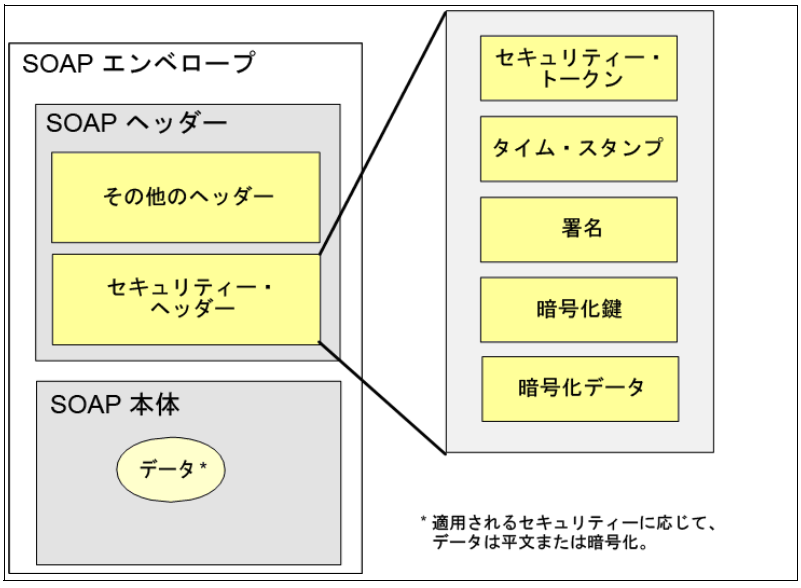

図 6　WS-Security

WS-Security 仕様のバージョン 1.1 は、2006 年 2 月に OASIS WSS Technical Committee によって承認されました。この仕様では、標準セットの SOAP 拡張機能を提案しています。この仕様は柔軟性があり、幅広いセキュリティー・モデル (PKI、Kerberos、SSL など) で Web サービスを保護するための基礎として使用することを目的に設計されています。この仕様では、整合性や機密性を実現するために、複数のセキュリティー・トークン形式、複数のトラスト・ドメイン、複数の署名形式、および複数の暗号化テクノロジーをサポートしています。

WS-Security 仕様では、*XML 署名* および *XML 暗号化* の使用法が定義されています。この仕様には、セキュリティー・トークンの伝搬、メッセージの整合性、およびメッセージの機密性が含まれています。ただし、これらのメカニズムだけで、完全なセキュリティー・ソリューションのあらゆる面に対処できるわけではありません。したがって、WS-Security は、セキュアな Web サービス・ソリューション設計におけるレイヤーの 1 つのみを表します。

OASIS Web サービスのセキュリティー仕様について詳しくは、以下の URL を参照してください。

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

WS-Trust

Web サービス・トラスト言語 (WS-Trust) は、WS-Security のセキュア・メッセージング・メカニズムを使用して、セキュリティー・トークンの発行、交換、検証を行うための追加プリミティブと拡張機能を定義します。WS-Trust を使用すると、さまざまなトラスト・ドメイン内で資格情報を発行および配布することもできます。

2 者間の通信を保護するには、2 者間でセキュリティー資格情報を (直接的または間接的に) 交換する必要があります。ただし、両者とも、互いの表明済み資格情報を信頼できるかどうかを判断する必要があります。この仕様では、セキュリティー・トークンを発行および交換するための WS-Security への機能拡張と、トラスト関係の存在を確立し、この関係にアクセスする方法が定義されています。

IBM Tivoli Federated Identity Manager は、WS-Trust で定義された *セキュリティー・トークン・サービス* を実装しています。このサービスは、WS-Security および WS-Federation 対応のセキュリティー・トークンの作成、検証、交換に使用できます。また、STS は Web サービス要求の許可にも対応しています。

WS-Trust を構成する仕様は、以下の OASIS Web サイトからダウンロードできます。

http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf

WS-SecureConversation

Web サービス・セキュア会話言語 (WS-SecureConversation) は、サービス間のセキュア通信を実現する目的で WS-Security の上に構築されています。WS-Security は、セキュリティー・コンテキストの確立ではなく、個々のメッセージ保護に重点を置いています。この仕様では、セキュリティー・コンテキストを確立および共有し、セキュリティー・コンテキストから鍵を導出して、セキュアな会話を実現するメカニズムが定義されています。セキュリティー・コンテキストが重要な理由は、両者間で対称的なセッション鍵を確立し、メッセージごとに効率的な暗号処理が可能になるからです。これは SSL で使用される方式と同じです。

WS-SecureConversation 仕様は、以下の URL からダウンロードできます。

http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.pdf

WS-SecurityPolicy

Web サービス・ポリシー言語 (WS-Policy) 仕様では、Web サービスに適用される一連のポリシー・アサーションが定義されています。WS-SecurityPolicy は、セキュリティーに関する

WS-Policy のプロファイルを 1 つ定義して、WS-Security、WS-Trust、および WS-SecureConversation 用のポリシー・アサーションを提供します。WS-SecurityPolicy では、メッセージの保護方法を記述したアサーションの基本セットを定義するという方式をとります。設計には、使用するトークン・タイプ、暗号アルゴリズム、メカニズム (トランスポート・レベルのセキュリティーの使用を含む) に関する柔軟性が組み込まれているため、時間の経過と共に拡張していくことができます。この目的は、参加者が実際にセキュアなメッセージ交換を行えるようにするために必要な全情報と共に、Web サービスの参加者が互換性と相互運用性を判断できるだけの十分な情報を提供することです。

WS-SecurityPolicy 仕様は、以下の URL からダウンロードできます。

http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.2/ws-securitypolicy.pdf

サービス指向アーキテクチャー対応の ID サービス

SOA は、疎結合サービスに接続して新しいアプリケーションを構成します。このサービスの実装には、専用のユーザー・レジストリーを使用することがよくあります。これらのレジストリーは、他のサービス実装のレジストリーとは分離して管理されます。この環境内のユーザーとサービス・エンティティーは、コンポジット・アプリケーションを構成する各種サービスの点で異なる場合があります。サービス要求ごとにサービス要求者の ID を設定することは、許可、監査、準拠などのビジネス要件を確実に実装するための基本ステップとなります。

したがって、SOA インフラストラクチャーでは、正しい ID を伝搬する一方で、サービスどうしが容易に相互接続できるように、ID サービスが必要となります。IBM Tivoli Federated Identity Manager のセキュリティー・トークン・サービス (STS) には、SOA ID メディエーションの課題に対応するプラグ可能 ID サービス・ソリューションがあります。このソリューションには、以下のような特長があります。

- さまざまな ID 表現形式を認識して処理できる
- さまざまな ID 間の変換 (マッピング) ができる
- SOA プリンシパルに基づいて、アプリケーションのビジネス・ロジックから切り離された、柔軟性の高いインフラストラクチャー・ベースのソリューションを提供する
- SOA ソリューションの構成対象となるプラットフォームやシステムとの相互運用性が最大限に高まるように、オープン・スタンダードを使用して構成されている

図 7 は、SOA コンポーネント (XML ファイアウォール、エンタープライズ・サービス・バス、バックエンド・メインフレーム・リソース・ベースのサービスなど) と、WS-Trust 標準を使用する IBM Tivoli Federated Identity Manager STS の間の対話を示しています。SOA コンポーネントは、セキュリティー・トークンの生成、検証、または交換のためにセキュリティー・トークン・サービスを呼び出します。これにより、現行環境での Web サービスを識別しやすくなります。

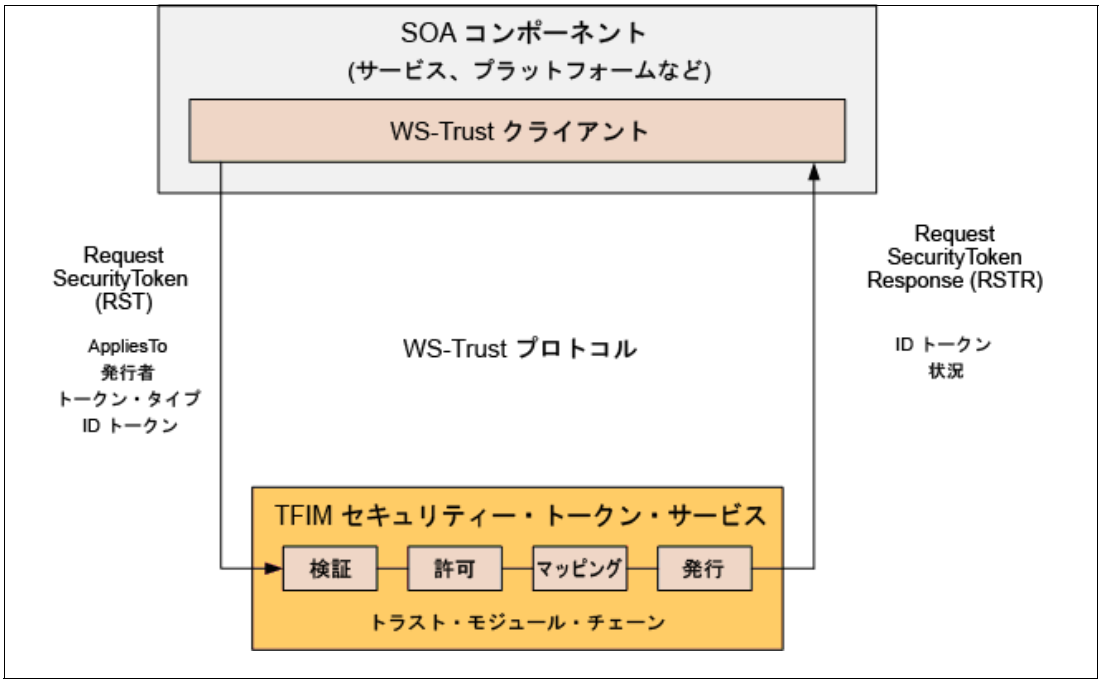

図 7　Tivoli Federated Identity Manager での WS-Trust の実装

SOA ID メディエーションのシナリオで IBM Tivoli Federated Identity Manager の ID サービスを利用するメリットは、既に使用可能になっている Tivoli Federated Identity Manager STS を使用する統合ソリューションの数によってもたらされます。ここで説明するソリューションでは、WS-Trust クライアントが組み込まれた、IBM Tivoli Federated Identity Manager STS を使用して ID メディエーションを使用可能にするソフトウェア・コンポーネントの例をいくつか示します。これらの例については、IBM SOA Foundation のシナリオのコンテキストで説明します。SOA 環境の保護について詳しくは、IBM Redbooks 資料の『*SOA セキュリティー設計および実装について (Understanding SOA Security Design and Implementation)*』(SG24-7310) を参照してください。

シナリオ 1: サービスの作成

サービスの作成のシナリオ (サービス・プロバイダーおよびサービス・コンシューマー) では、既存のアプリケーションまたは新しいビジネス・ロジックのアプリケーション機能をサービスとして公開する方法をデモンストレーションします。これらのサービスを、企業内および企業間で他のサービスやクライアント・アプリケーションが利用できます。このシナリオの主な推進要因は、既存または新規のアプリケーション機能をサービスとして再利用する点です。

Tivoli Federated Identity Manager の Web サービス・セキュリティー管理 (WSSM) コンポーネントは、WebSphere Application Server の Web サービス・セキュリティー機能と統合されます。このコンポーネントには、以下の機能があります。

- WSSM トークン・コンシューマー

  トークン・コンシューマーは、Tivoli Federated Identity Manager STS を使用して、着信 Web サービス要求で受信した ID トークンを検証した後、WebSphere Application Server に対してサービス要求元を認証します。この機能を使用すると、WebSphere Application Server で稼働しているアプリケーションが、アプリケーション・サーバーではネイティブ・サポートされない幅広い ID トークン・タイプをサポートできるようになります。

- WSSM トークン・ジェネレーター

トークン・ジェネレーターは Tivoli Federated Identity Manager STS を使用して、WebSphere Application Server にある現在の ID を、発信 Web サービス要求で送信するための別の ID トークン・タイプに変換します。この機能を使用すると、サービス内でカスタマイズを行う必要がなく、サービス要求に含まれる ID をサービスが容易に利用できるようになります。

IBM Tivoli Federated Identity Manager 用の CICS 統合パックには、JAAS ログイン・モジュールが用意されています。このモジュールは、WebSphere Application Server サブジェクトからの ID を UsernameToken で Tivoli Federated Identity Manager STS に送信し、モジュールの呼び出し側に返される ID を表す別の UsernameToken を受信します。このモジュールには、以下のような用途があります。

- WebSphere Application Server 内の CICS JCA モジュールから呼び出して、CICS Transaction Gateway に送信するユーザー名とパスワードまたは RACF® パスチケットを取得する
- WebSphere Application Server 内の JDBC™ ドライバーから呼び出して、IBM DB2® などのリレーショナル・データベースに接続するための資格情報を取得する
- Java アプリケーションからプログラムによって呼び出す

シナリオ 2: サービス接続

サービス接続のシナリオでは、サービス・プロバイダーとコンシューマーを統合して、複数のチャネル間で既存および新規のサービスを再利用できるようにする方法をデモンストレーションします。このシナリオは、企業が所有している一連のコア・サービスやシステムを、内部クライアントと外部クライアントがサービスとして使用できるようにする必要がある場合に適しています。互いに独立したサービス・プロバイダーとサービス・クライアントに変更を加える際の柔軟性が要件となります。

このシナリオの重点は、ビジネス中心の SOA をサポートするために使用する基本的な接続にあります。エンタープライズ・サービス・バス (ESB) には、クライアントとプロバイダー間の分離機能があります。これにより柔軟性が実現され、アプリケーションをより短期間で実装できるようになります。サービスがサード・パーティーに提供される、あるいはサービスがサード・パーティーから利用されるような環境では、ESB ゲートウェイと ESB を併用して、セキュリティー手段を追加することができます。すべてのサービス対話をサード・パーティーと行う場合や、サービス・コンシューマーとプロバイダー間でメディエーションを行う基本要件がある場合は、ESB ゲートウェイのみで十分である可能性があります。

IBM Tivoli Federated Identity Manager の ID サービスは、3 つの IBM ESB ソリューションに対して ID 処理機能を提供します。

- WebSphere ESB

  このソリューションを使用すると、ツールの観点から WebSphere Integration Developer と統合して、ID メディエーション・プリミティブをメディエーション・モジュールにグラフィック形式で追加することができます。WebSphere ESB および WebSphere Process Server でのランタイムでは、ID メディエーション・プリミティブが着信要求から ID トークンを抽出し、Tivoli Federated Identity Manager STS を使用してそれを検証し、別の ID トークンとマッピングします。この ID トークンは、ESB からのサービス要求に組み込まれます。

- WebSphere Message Broker

  この統合では、ID サービスのユーザー定義ノードが提供されます。このノードは、着信 SOAP メッセージから ID トークンを抽出した後、検証および代替 ID とのマッピングを行うために、これらを Tivoli Federated Identity Manager STS に送信します。STS から受け取った ID は、WebSphere Message Broker からの発信要求に組み込まれます。

- WebSphere DataPower® SOA アプライアンス

DataPower SOA アプライアンスはネットワーク・エッジで使用されることが多く、XML ファイアウォールの役割を果たします。DataPower SOA アプリケーションは、信頼されていないネットワークから要求を受信した後、XML 検証と WS-Security 処理 (署名のチェック、メッセージの復号化など) を実行します。

IBM Tivoli Federated Identity Manager は、認証、許可、監査 (AAA) ポリシー定義に外部インターフェイスを提供することで DataPower と統合され、トークンの検証と交換、および要求の認証と許可を実現します。DataPower と IBM Tivoli Federated Identity Manager 間の通信は WS-Trust によって行われ、IBM Tivoli Federated Identity Manager によってトークンを検証および交換するための STS 機能が提供されます。

シナリオ 3: 対話およびコラボレーション・サービス

対話およびコラボレーション・サービスのシナリオは、シングル・サインオンと役割ベースのポータルを特長とします。このポータルは、企業内および企業間で情報とアプリケーションへのアクセスを統合する目的で使用されます。このシナリオの主な推進要因は、アプリケーションおよびコンテンツに対するユーザーの生産性と使用量が向上する点です。コンテンツは、ユーザーの役割に基づいて、集約ポータル・ページでパーソナライズすることができます。

前述した IBM Tivoli Federated Identity Manager のシングル・サインオン機能を使用すると、ポータルと他の Web アプリケーション間でシングル・サインオンを実現できます。この機能には、さまざまな管理ドメイン内の Web アプリケーションに対するフェデレーテッド・シングル・サインオンが含まれます。

ポータルから、Web Services for Remote Portlets (WSRP) などの標準を使用している他のポータルによって提供されるコンテンツへ、Web サービス・ベースで統合する場合、シナリオ 1 および 2 で説明した統合機能がこのシナリオにも適用されます。

お客様のシナリオに対するソリューション

本書の冒頭で、お客様のシナリオに関するいくつかの問題を紹介しました。ここで、考えられるソリューションを見てみましょう。

公共部門 : 行政機関サービス向けのシングル・ログイン

行政機関サービスへのシングル・ログインを解決するために、この機関では SAML 2.0 と IBM Tivoli Federated Identity Manager を使用して、フェデレーテッド・シングル・サインオンを実装することを選択しました。19 ページの図 8 に示すように、この行政機関では、ユーザーのログイン資格情報を管理するアイデンティティー・プロバイダーを実装しました。この中央管理方式により、各部門で異なる資格情報を管理する必要が減りました。アイデンティティー・プロバイダーはユーザーを認証し、ユーザーに対して SAML 2.0 セキュリティー・アサーションを生成します。これにより、ユーザーは参加部門にアクセスできるようになります。

各行政部門は SAML 2.0 準拠のサービス・プロバイダーであり、受信したアサーションに基づいてユーザーの ID を検証することができます。初期実装では、参加部門も Tivoli Federated Identity Manager を使用しました。ただし、SAML 2.0 標準が実装されているため、各部門で別の製品やオープン・ソースの実装環境を選択できることに注意してください。

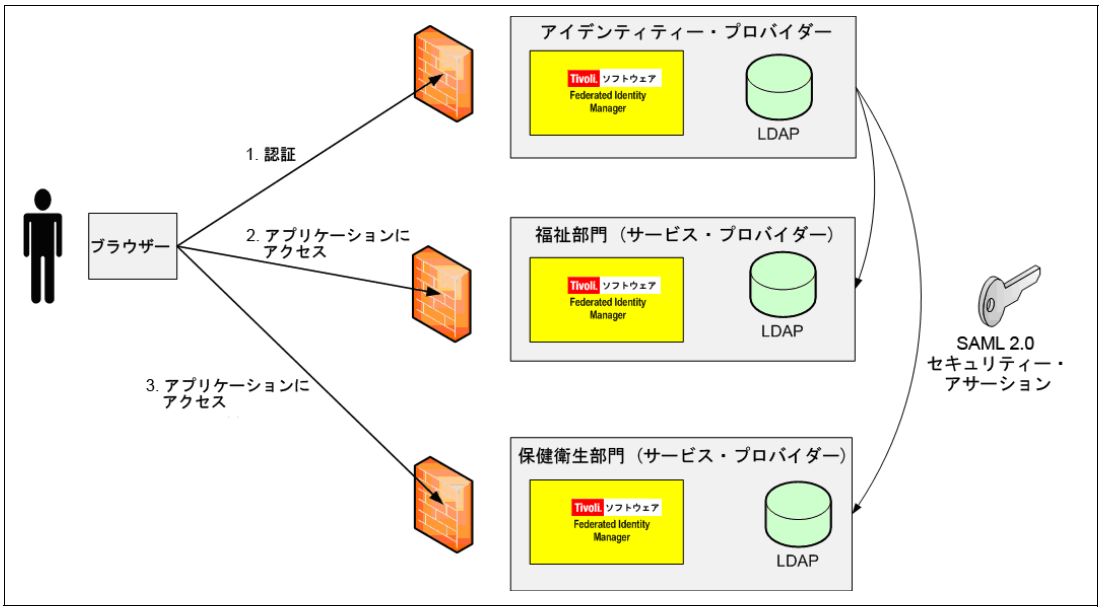

図 8　SAML 2.0 を使用した行政機関サービス向けのシングル・ログイン

ジャストインタイムのプロビジョニング・モデルを使用して、サービス・プロバイダーでアカウントを作成できる場合もあります。サービス・プロバイダーで事前にアカウントを作成しておく必要はなく、サービス・プロバイダー側でのフェデレーテッド・シングル・サインオン処理の一部として、サービス・プロバイダーでユーザー・アカウントのプロビジョニングを行うことができます。この機能は、SAML 2.0 アサーションの拡張可能な特性によって実現されます。このアサーションでは、任意の拡張属性が含まれている可能性があります。IBM Tivoli Federated Identity Manager には、SAML 2.0 アサーションを構成する前に、アイデンティティー・プロバイダー側でこれらの属性を取得するための柔軟なメカニズムがあります。また、アサーションからこれらの属性を抽出して、サービス・プロバイダーで他のシステムと統合する方法もあります。

通信業：外部パートナーへのサービス提供

通信会社が外部パートナーにサービスを公開できるようにするため、社内 DMZ で着信サービス要求を処理するためのエッジ・ゲートウェイをセットアップしました。20 ページの図 9 に示すように、WebSphere DataPower XS40 は着信要求用の Web サービス・プロキシー機能を提供します。着信メッセージは Web サービス要求であり、WS-Security を使用して保護され、SAML セキュリティー・アサーション (またはビジネス・パートナーから要求されるその他のトークン) が含まれています。

XS40 は IBM Tivoli Federated Identity Manager と通信して、着信セキュリティー・トークンを検証し、要求を許可し、(追加属性を付加して) ID をマッピングして、組織の内部に適した新しいトークンを生成します。この図では、SAML 1.0 の新しい未署名トークンが生成されています。

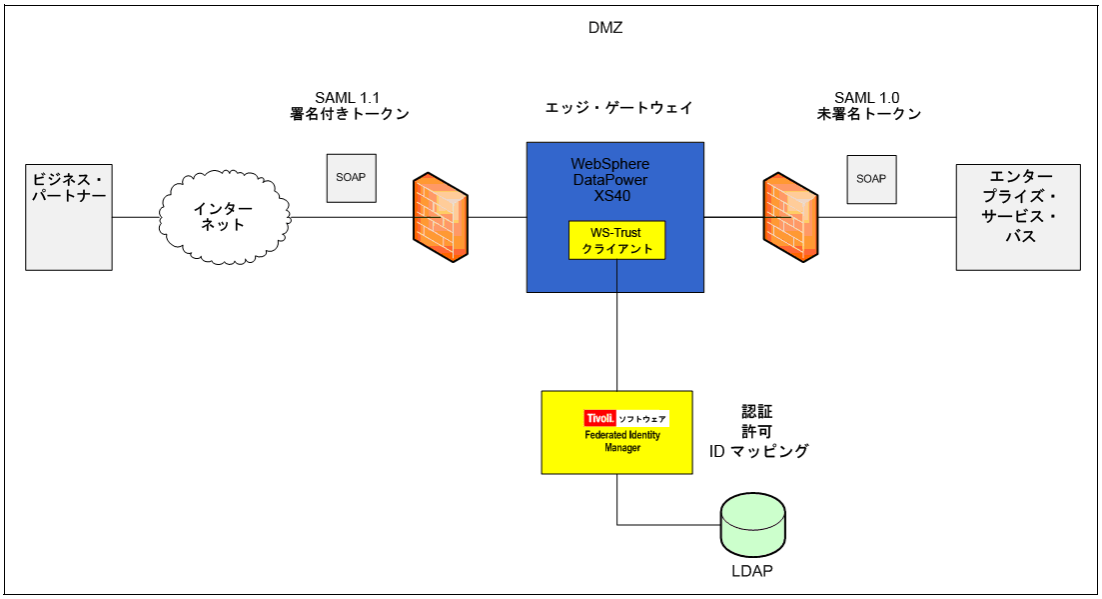

図 9　外部パートナーからのサービス要求を処理する通信業

金融業：既存の IT システムの再利用

金融サービス業のある組織が、ポータルから既存のメインフレーム CICS アプリケーションのビジネス・ロジックを再利用することを希望していました。WebSphere Message Broker はエンタープライズ・サービス・バスとして使用されていました。ポータルは IBM Tivoli Access Manager および IBM Tivoli Directory Server を使用して保護されていました。RACF セキュリティー・サーバーによって保護される環境では、CICS 環境が稼働していました。

ID 伝搬ソリューションでは、IBM Tivoli Federated Identity Manager と統合される WebSphere Message Broker でカスタム・ノードを使用して、ID の検証と変換を行うようにしました (図 10 を参照)。

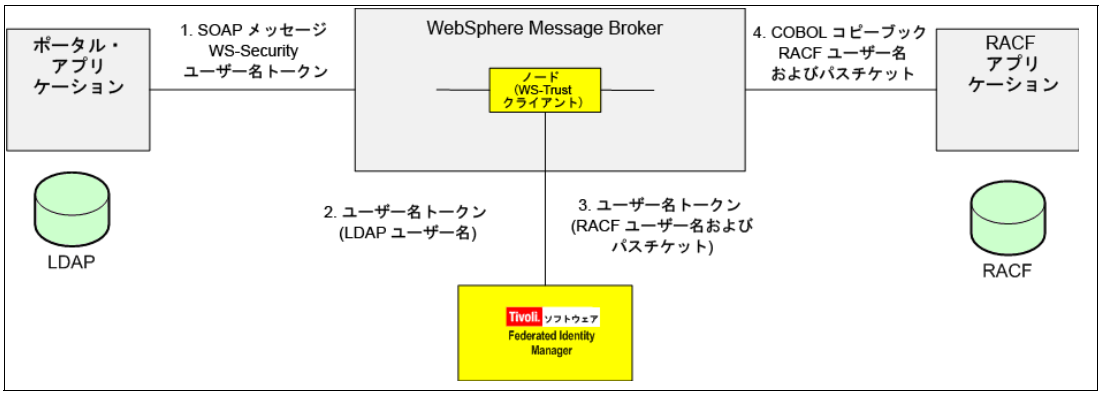

図 10　バックエンド CICS 統合への IBM Tivoli Federated Identity Manager の使用

IBM Tivoli Access Manager for e-business はユーザーを認証した後、自動的にユーザーをポータルにサインオンします。CICS コンテンツにアクセスするポートレットが呼び出されると、認証済みのユーザー ID が WS-Security UsernameToken で WebSphere Message Broker に送信されます。WebSphere Message Broker 内のノードは WS-Trust 要求を構成し、IBM Tivoli Federated Identity Manager にアクセスし、IBM Tivoli Directory Server でユーザーを見つけて、その RACF ユーザー名を調べます。ユーザー名は、ユーザーの LDAP エントリー内の属性に格納されています。

次に、以下のものに基づいて、CICS アプリケーション用の RACF パスチケットが IBM Tivoli Federated Identity Manager で生成されます。

- IBM Tivoli Federated Identity Manager 内の処理コンテキストから取得した RACF ユーザー名
- RACF 内の値とマッチングするための、IBM Tivoli Federated Identity Manager で構成された共有秘密鍵
- RACF 内の値とマッチングするための、IBM Tivoli Federated Identity Manager で構成されたアプリケーション ID
- 現在時刻

RACF ユーザー名とパスチケットが、再び WS-Security のユーザー名トークンで、WebSphere Message Broker 内のノードに返されます。この時点で、WebSphere Message Broker から CICS または CICS Transaction Gateway への Web サービス要求には、RACF ユーザー名とパスチケットが含まれています。これらは、サービス要求の認証に使用されます。

Tivoli ソリューションのデプロイメントおよびランタイム

次に、ソリューションのデプロイメントおよびランタイム・モデルを見てみましょう。

フェデレーテッド・シングル・サインオン

図 11 は、フェデレーテッド・シングル・サインオン (SAML、Liberty、WS-Federation) や、OpenID または ID セレクター (Microsoft Windows Cardspace™、Eclipse Higgins Project など) を実装する際に使用される IBM Tivoli Federated Identity Manager コンポーネントを示しています。この構成は、フェデレーション内のアイデンティティー・プロバイダーまたはサービス・プロバイダーとして機能する Web サイトでは標準的です。

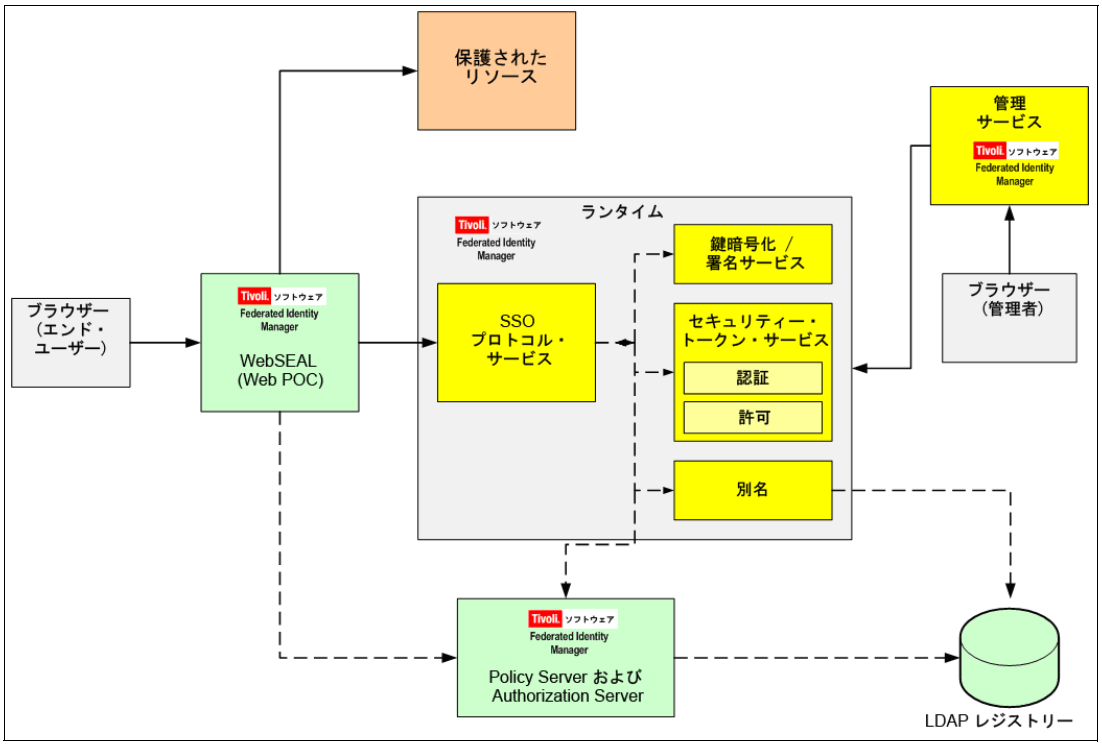

図 11　フェデレーテッド・シングル・サインオン用の IBM Tivoli Federated Identity Manager デプロイメント

図 11 で重要なコンポーネントは以下のとおりです。

- IBM Tivoli Access Manager for e-business WebSEAL: Web POC サーバーに使用します。ユーザーからのブラウザー要求はすべて POC を通過します。
- SSO プロトコル・サービス : SAML、Liberty、および WS-Federation のプロトコルを実装します。
- セキュリティー・トークン・サービス : WS-Trust STS を実装します。さまざまなフェデレーション (作成、検証、交換) 用のトークンを管理します。
- IBM Tivoli Federated Identity Manager 管理サービス: フェデレーション特性を構成するための Web ベース・アプリケーションです。
- IBM Tivoli Access Manager for e-business Policy Server: 認証/許可ポリシーの管理および配布に使用されます。
- IBM Tivoli Access Manager for e-business Authorization Server: STS 認証/許可コンポーネントからの LDAP ディレクトリーとの対話を提供します。
- LDAP レジストリー : ユーザー ID と別名の格納に使用します。

柔軟なフェデレーテッド SSO デプロイメント・モデル

IBM Tivoli Federated Identity Manager では、IBM Tivoli Access Manager for e-business を必要とせずに、SSO サービスを Microsoft .NET および WebSphere アプリケーションと直接統合できるデプロイメント・モデルもサポートしています。この方式は特に、企業が既にサード・パーティーのアクセス管理ソリューションを所有している環境や、単に Web アプリケーション・サーバーを POC として使用してフェデレーションに参加するためにデプロイメント・モデルを必要とするビジネス・パートナーの環境に適しています。

まとめ

トラスト管理およびフェデレーテッド ID 管理は、企業の境界を越えて ID 管理を簡素化するための標準化されたメカニズムを提供します。ビジネスでこのメカニズムを利用すると、ID およびアクセス管理のコストをフェデレーション内で信頼されたビジネス・パートナーに任せることができます。ビジネスでフェデレーテッド ID を使用すると、企業間で信頼された方式で、ID 情報と資格を共有できるようになります。

Web サービス・モデルの柔軟性と魅力は、このモデルの根本的な要素です。企業は新しいサービスを容易に構築して、革新的なビジネス・モデルを提供したり、パートナー、サプライヤー、顧客、従業員と緊密な関係を築いてバリュー・チェーン・ネットワークをより効率的につなげたりすることができます。このようなモデルが成功するのは、顧客、パートナー、およびユーザーが、これらのサービスをサポートする Web サイト間を容易にナビゲートできる場合のみです。

この使いやすさを実現するには、ユーザーがビジネス・フェデレーション内のさまざまなサイトに対して、自分自身の認証と識別を何度も行わずに済むようにする必要があります。Web サービスを実装してフェデレーテッド ID 管理を利用できるようにすると、企業の実際の ROI が向上します。この方法により、サプライヤー、ビジネス・パートナー、顧客の間での統合、通信、および情報交換を改善することができます。この方法では IT を生産的に活用することで、企業のコストを削減し、生産性を向上させ、事業運営の効率性を最大限に高めます。

本書では、企業が IBM Tivoli Federated Identity Manager と共に今すぐ生産的に活用することのできる、具体的なフェデレーション・シナリオについて説明しています。これらのシナリオは、企業のバリュー・ネットを確実につなぎ、使いやすさの向上、(ユーザーおよびインフラストラクチャーの) 管理コストの削減、および開発コストの削減によって ROI を実現する、一般的なお客様のユース・ケースを表しています。

本書の執筆チーム

本書は、オースティン・センターの International Technical Support Organization で働く、世界中から集まったスペシャリストのチームによって制作されました。

Axel Buecker は、オースティン・センターの International Technical Support Organization で認定コンサルティング・ソフトウェア IT スペシャリストをしています。彼は幅広い執筆活動を行うと共に、ソフトウェア・セキュリティー・アーキテクチャーとネットワーク・コンピューティング・テクノロジーの分野に関する IBM クラスを世界各地で教えています。彼はドイツのブレーメン大学でコンピューター・サイエンスの学位を取得しました。また、ワークステーションおよびシステム管理、ネットワーク・コンピューティング、e- ビジネス・ソリューションに関する各種分野で 21 年の経験があります。Axel は 2000 年 3 月に ITSO に参加する前は、ドイツの IBM でソフトウェア・セキュリティー・アーキテクチャーのシニア IT スペシャリストとして働いていました。

Paul Ashley は IBM Software Group の一部である SOA Advanced Technologies Asia Pacific チームでシニア認定 IT スペシャリストとリード・アーキテクトをしています。このチームは、新しい SOA エンゲージメントとテクノロジーを専門としています。Paul は IT 業界で 18 年働いており、電子工学およびコンピューター・サイエンスの学位と、情報セキュリティーの博士号を保有しています。SOA Advanced Technologies チームに参加する前、Paul は米国とオーストラリアの両方で Tivoli Security のセキュリティー・スペシャリストとして働いていました。彼は現在、ゴールド・コーストの Australian Development Labs に所属しています。

Neil Readshaw は、Tivoli's Worldwide Customer Solutions (SWAT) チームでシニア認定 IT スペシャリストをしています。彼は現在、オーストラリアのゴールド・コーストに配属されてい

ます。彼は、ソフトウェア開発、ネットワーク管理、情報セキュリティー、システム統合の各分野で 15 年の経験があります。彼は、クイーンズランド大学でコンピューター・システム・エンジニアリングとコンピューター・サイエンスの学位を取得したほか、認定情報システム・セキュリティー・プロフェッショナル (CISSP) および IT Infrastructure Library (ITIL) の認定も保有しています。また、IBM developerWorks サイトの Tivoli Developer Domain で幅広い執筆活動も行っています。

このプロジェクトに貢献してくださった以下の方々に感謝の意を表します。

Anne Johnson (編集者)
International Technical Support Organization、Research Triangle Park (ノースカロライナ州)

Bruce Rich、Shane Weeden、Davin Holmes、Patrick Wardrop、Ravi Srinivasan、Sridhar Muppidi
IBM

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。本書の提供により、お客様にこれらの特許権の実施権を許諾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。

〒 242-8502
神奈川県大和市下鶴間 1623 番 14 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。

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。

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。

本書の原典 (REDP-3678-01) の作成日または更新日は 2008 年 5 月 15 日です。

以下のいずれかの方法でコメントをお寄せください。

- オンラインで以下のサイトにある「**Contact us**」から Redbook のレビュー・フォームを使用する。
  `ibm.com/redbooks`
- 下記のアドレスに E メールでコメントを送信する。
  `redbooks@us.ibm.com`
- 下記の宛先に郵送する。
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

商標