M_021

認証プロキシーによる統合認証基盤の実現

Integrated authentication system by an authentication proxy

鈴木 美幸†、岡本 康介†
Yoshiyuki Suzuki、Kohsuke Okamoto

1．まえがき

セキュリティ対策において認証は対策の基本的な部分である。認証とは本人の正当性を検証する作業であり、ユーザーID/パスワードによる認証を始め、認証バイオメトリックス認証など様々な認証する手段が最近実用化されてきている。また、Web サービスの WS-Federation や Liberty Alliance[1]においては企業間（ID Provider と Service Provider 間）の認証結果とユーザー属性の交換方法について検討/標準化がなされている。一方、企業内においては、サービスを組み合わせて企業内のシステムを構築する SOA(サービス指向アーキテクチャー)が提唱されてきている。

本稿では、サービスを構成する様々な製品やパッケージの統合認証基盤の実現方法のひとつとして認証プロキシーを紹介する。

2．企業内の統合認証基盤とは

2.1 認証・認可ポイントの統一の必要性

企業は、企業活動を行うために社員に業務アプリケーション（以下、サービスと呼ぶ）を使わせている。その際、サービスは社員の本人性を社員情報データーベースに問い合わせて確認する。いろいろなサービスがあるとそれぞれに認証方式が異なり、社員にとっては、それぞれごとにユーザーID/パスワード等の ID の入力が必要となる。サービス開発者にとってはそれぞれごとに認証の開発が必要である。さらに企業の管理者にとっては社員情報データーベース内に Identity を複数のサービス間で矛盾なく、かつ人事異動に合わせてタイムリーに反映することが求められる。

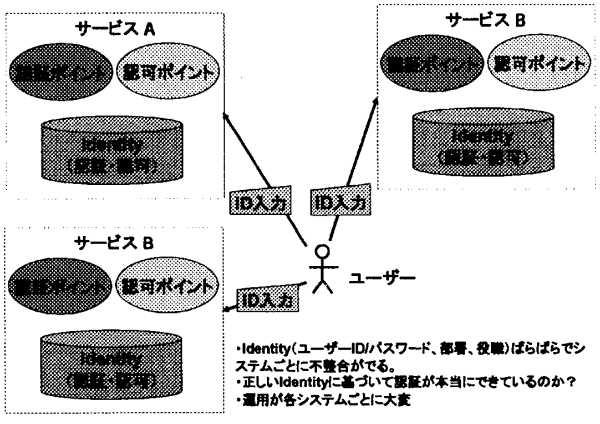

図1. Identity/認証ポイントがばらばらな状況

この際、認証に必要な情報（Identity）と認証するポイント、認証をもとに認可（認証された後に、ユーザー属性に基づいて情報へのアクセス権限を付与する事）を行うポイントおよび ユーザーの入力がばらばらな状況を示したのが図1である。

†日本アイ・ビー・エム（株）大和研究所、インテグレーション・サービス

このような状況の場合、下記のような問題点が発生する。

1．Identity がそれぞれのサービスごとに分かれており、整合性を保証するのが難しい。また、ユーザー情報の管理が難しい。
2．サービスごとに認証の仕組みを作成する必要がある。
3．サービスにログインするたびに、違うユーザーID/パスワード等の認証に必要な情報を入力する必要がある。

2.2 既存の認証製品

現在、認証製品として出荷されている製品は、下記の３種類に分けられる。

1．リバースプロキシー型
2．認証代行型
3．プラグイン型

この中でネットワークのゾーンニングによりセキュリティを保ちやすいリバースプロキシー型が主流になってきている。（図２）これらの認証製品はユーザー端末として Web Browser の使用を前提に作られており、すべての業務アプリが一回のログインで使えるというシングルサインオンの操作性の簡便化を実現している。

しかしながら、HTTP プロトコルでユーザーと認証サーバーおよび認証サーバーと各サービスが通信することを前提にしている。および、認証後のサービスが認可を行うためには認可用の Identity を各サービス内に分散して持つ必要がある。このため、Identity が格納されているディレクトリ間の同期が必要となり、各ディレクトリ間のプロトコル、データ構造の相違の吸収、データの整合性の維持、障害時の回復の難しさが発生する。

そこで統合した Identity を基に認証する統合認証基盤が望まれる。

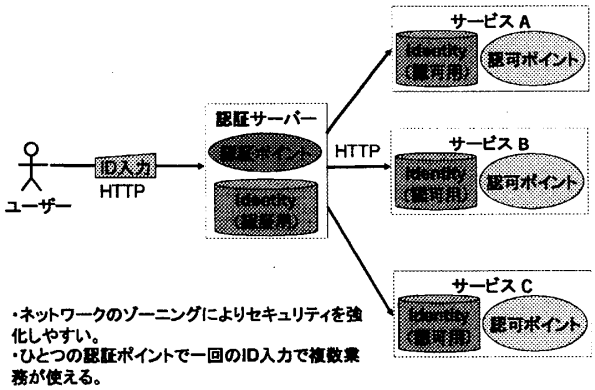

図2. HTTPプロトコルにおけるリバースプロキシー型認証製品

2.3 統合認証基盤

Identity をまとめて統合ディレクトリに保管し、統合的にユーザー管理を行い、保管された情報をもとに統合され

た認証ポイントで認証を行う統合認証基盤である。このような統合認証基盤により Identity が統一保管されれば、管理もしやすくなる。一箇所で管理することにより、データの整合性の問題はなくなり、人事異動等の結果が即座にすべての認証のサービスに反映され、セキュリティも向上する。

しかしながら、さまざまなサービスから同じ統合ディレクトリにある Identity をアクセスするのは実装面から制約が多い。可能な限りサポートできるサービスを増加させるために認証プロキシーを開発した。（図３に示す）

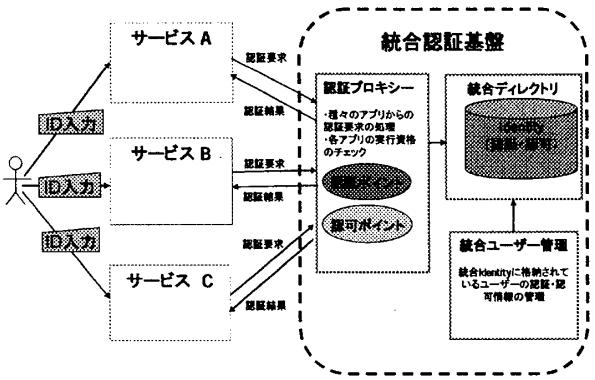

図3. 認証プロキシーによる統合認証基盤

3. 認証プロキシーの実装

3.1 認証プロキシーに必要な機能

現在、ほとんどの製品（サービス）において認証・認可に使う Identity の格納場所としてディレクトリの標準である LDAP V3 をサポートしているので LDAP を前提に下記の認証プロキシーに必要な機能を実装した。

（１）スキーマ変換機能

LDAP サーバーに格納された属性を各種サービスに対して異なる属性に対応付ける機能である。対応づけは変換ルールとして定義する。LDAP サーバーのスキーマを変更しなくても、サービスが必要とするスキーマに適合させることが可能となる。サービスを追加する際に既存サービスへ与える影響を最小限にできる

（２）認可判定つき認証機能

認可判定とは、ユーザーごとのサービス利用可否の判定である。サービスからユーザー認証要求が行われたとき、ユーザー情報、サービス情報、および認可条件に基づいて利用可否を判定し、その利用可否結果に応じて認証応答をサービスへ返す機能である。認可機能を備えないサービスでも、サービスの改修なしに認可判定機能を実現することが可能となる。認可条件は認可情報としてサービスごとに定義可能とする。

（３）サービス識別機能

スキーマ変換機能、認可判定つき認証機能は、サービスごとに振る舞いを変える必要がある。LDAP 通信の通信情報（要求元 IP アドレス、TCP ポート番号）に基づいてサービスの識別を行う。

3.2 認証プロキシーの処理概要

下記のような流れで認証プロキシー認証処理を行う。（図４の①－⑦も参照）

①サービスは認証プロキシーへ LDAP プロトコルを用いて認証要求を行う。

②認証プロキシーは、LDAP メッセージの種別により付加処理を行うかどうか判断する。

付加処理を行わない場合はそのままバックエンド LDAP サーバーへメッセージを中継する。

③認証プロキシーは、要求元との IP アドレスなど通信情報、およびサービス識別情報に基づいてサービスを識別し、各種サービスごとに設定された認可プラグインを呼び出す。

④許可プラグインは、LDAP メッセージを処理して、認証要求に含まれる利用者を識別する。

⑤,⑥許可プラグインは、サービスごとに設定された認可情報と利用者情報に基づいて認可判定を行いサービスの利用可否を判定する。利用不許可の場合は直ちに認証失敗をサービスへ通知する。

⑦利用可の場合は、認証要求を処理して処理結果をサービスへ通知する。

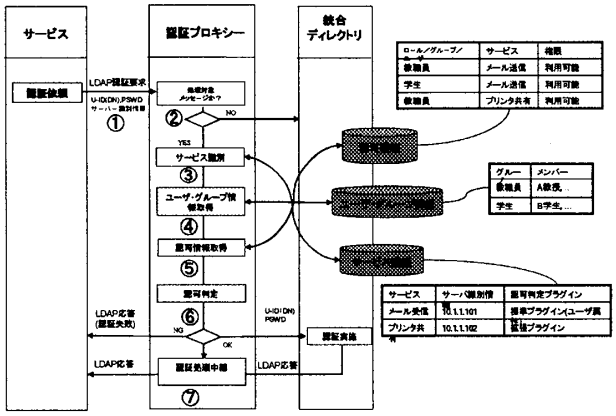

図4. LDAPベースの認証プロキシーの処理概要

4. まとめ

今回は認証プロキシーを介して認証を行うことにより複数サービス間で統合された認証基盤を使える方法を示した。一方、SOA は「サービス」の組み合わせによってアプリケーションを構成するシステム構築の考え方であり、業務処理などの単位でサービス化し、オープンな標準的なインタフェースでサービスを定義し、呼び出すサービスを組み合わせてアプリケーションを構築することである。本稿の方法は今後 SOA の認証基盤のひとつとして考えられる。

最後に日本アイ・ビー・エム株式会社 大和研究所の開発を支援していただいた方々に心より感謝します。

参考文献

[1] Liberty Alliance (http://www.projectliberty.org
[2] SOA（サービス指向アーキテクチャー）(http://www-06.ibm.com/jp/solutions/soa/)