OpenIDとSAMLの相互運用の試み
—“Project Concordia”によるデモンストレーション—

2009年４月に米国サンフランシスコで開催された「RSAカンファレンス2009」で、認証プロトコルの相互運用を推進する“Project Concordia”の成果発表として、ID認証仕様であるOpenIDとSAMLの相互運用の実装例がデモンストレーションされた。今後、異なるID認証プロトコルを用いたフェデレーション（連携）認証の実現に向け弾みがつくことが期待される。

認証プロトコルの相互運用の取り組み

“Project Concordia”はID認証技術を開発するベンダーやユーザー企業から成るワーキンググループで、SAML（Security Assertion Markup Language）、WS-*（スター）、OpenIDといった異なる認証プロトコル間の相互運用を目指して活動している。

ID認証技術に携わる技術者が達成すべき目標は、フェデレーション認証を通じてインターネット全体に広く通用するIDを提供することにある。フェデレーション認証とは、異なる組織が１対１の直接契約は結んでいないが互いに信用しあえる環境で、IDとその属性情報を共有する仕組みである。

これが実現すれば、現在アプリケーションごとに管理されている認証用のIDを、信頼性と利便性を提供できる少数の認証サービス事業者のサービスに集約できるようになり、IDの新規作成や管理にかかる手間は大幅に削減される。

しかし、企業のイントラネットや特定企業間のエクストラネットを超えて、インターネット上で広くこの機能を提供する仕組みは、いまのところまだ実現していない。過去に認証プロトコルの主導権争いがベンダー間で長年行われ、複数のプロトコルが並立してきたからである。これらのプロトコルは互いに競争関係にあったため、ユーザー企業はいずれか１つのプロトコルを選択しなければならず、相互運用のための仕組みづくりは進まなかった。

Project Concordiaはこうした過去を教訓にして、SAML、WS-*、OpenIDの推進者が一堂に集うコミュニティを形成し、すべての認証プロトコルが互いに情報を交換できるフェデレーション認証の実現を目標として活動している。

OpenIDとSAML2.0の相互運用をデモ

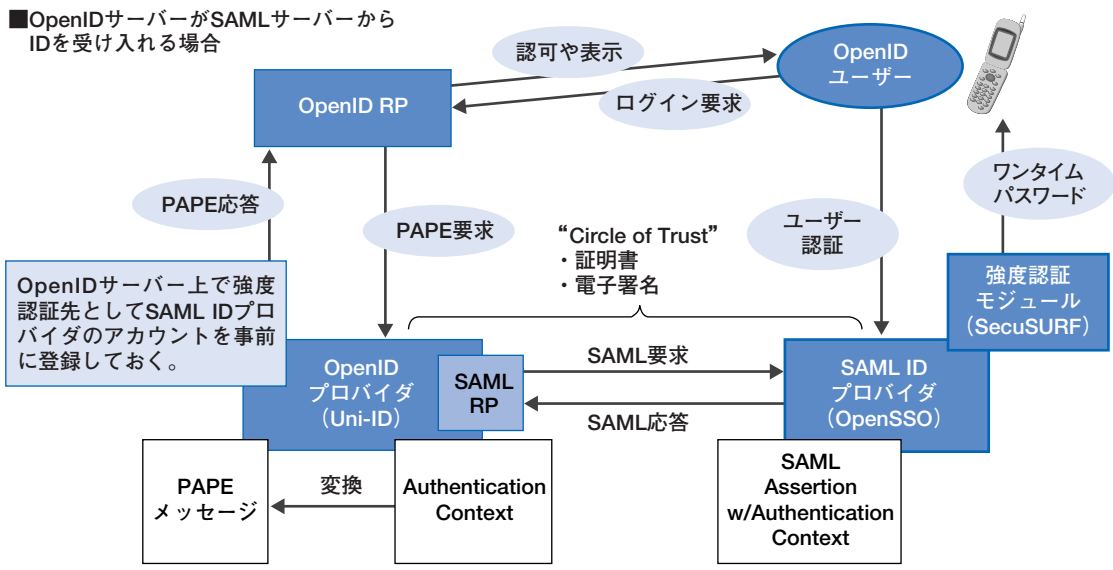
Project Concordiaは2008年３月にSAMLとWS-*間の相互認証の実装例のデモを行ったが、2009年４月にサンフランシスコで開催された「RSAカンファレンス2009」ではOpenID認証とSAML2.0認証を活用した利用シーンと相互運用のデモを行った。

具体的には、すでにSAMLにより社内向けにシングルサインオンやID管理を実施している企業が、そこで管理されるIDをOpenIDにしか対応していない外部のサービス（SNSや

NRIパシフィック
リサーチャー
作島立樹（さくしまたつき）

専門は米国の技術とサービスに関する調査・研究

図1　OpenIDとSAMLの相互運用



Eコマース）での認証に使うというケースである（http://projectconcordia.org/index.php/Planned_Scenarios_for_RSA_2009）。

デモのケースでは、OpenID対応サービスが認証を要求してくると、OpenIDサーバーがその要求の内容を判断し、ワンタイムパスワードのような強度認証が要求されていれば、その条件を満たすSAML認証サーバーへ要求を転送する（図1参照）。

認証プロトコルの発展の鍵は、もはや各プロトコルの優位性の競争にあるのではない。それぞれが適材適所で使われるべきであり、個々の特長を活かして実装されている既存の認証インフラを利用し、機能的に相互補完しあうことが必然となってくる。

技術や立場を超えた連携が重要

今回のデモで用いたシナリオは、野村総合研究所（NRI）とNTT情報流通プラットフォーム研究所が共同で提出したものである。推進する技術や業界での立場も異なる企業の技術者同士が、同じ目標に向けて協力できる環境を作っていくことは、認証技術の将来を展望する上で重要な意味を持つと考えている。

2009年4月には、ID認証技術の調和を目的に新組織「カンターラ・イニシアティブ」（理事はNRIの崎村夏彦）がスタートした。今後、Project Concordiaはカンターラ・イニシアティブのディスカッショングループの1つとして引き継がれる予定である。 ■