4E-3

ワンストップ認証のためのプロトコルに関する考察[1]

阿部　玲子　　竹田　義聡　　北山　泰英
三菱電機株式会社　情報技術総合研究所

1　はじめに

1つの Web サイトでユーザを認証した結果を他の Web サイトでも利用する「ワンストップ認証」に対するニーズが高まっている。本研究では、既存の認証情報伝達プロトコルである OASIS Security Assertion Markup Language[1](SAML)をワンストップ認証に適用する場合の問題点について考察し、認証性能を向上させる手法を提案する。

2　ワンストップ認証とは

ワンストップ認証とは、ユーザが ID・パスワードなどの個人認証用のユーザ情報を登録していないサービスを利用する場合、当該サービスが信頼する他のサービスによる認証結果に基づきユーザを認証する方法、と本稿では規定する。これは、SAML や Liberty Alliance Project[2]のような既存のシングルサインオンを発展させ、1箇所にあるユーザ情報を用いて複数のサービスを受けることができるようにし、ユーザの利便性向上とユーザ情報分散防止を実現するものである。図 1に、ワンストップ認証を実現するシステム例を示す。

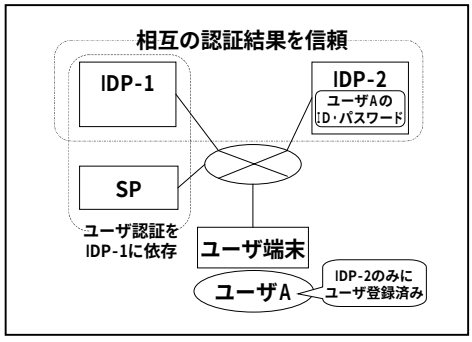

図 1　ワンストップ認証システムの例

図 1中、SP（Service Provider）はオンラインショッピングなどのサービス提供者、IDP（Identity Provider）は、ユーザのアイデンティティ情報の真正性を担保しうる組織・機関のサイトを示す。IDP-1 と IDP-2 は相互に認証結果を信頼し合う関係にあるものとする。また、SP と IDP-1 の関係は、オンラインショッピングモールビジネスにおけるショッピングモールサイトと参加のショッピングサイトのように、SP がユーザ管理を IDP-1 に依存するケースを想定する。図 1においては、ワンストップ認証は、SP へのアクセスを要求するユーザ A が IDP-1 にユーザ情報を登録していない場合にも、IDP-2 に登録情報があればこれを用いてユーザ認証を行う事を可能にするものである。

3　SAML によるワンストップ認証の課題

ワンストップ認証は、SAML をはじめとするシングルサインオンのための認証情報伝達プロトコルを用いて実現できる。本節では、SAML を図 1のワンストップ認証に適用した場合の課題を示す。IDP-2 から IDP-1、および IDP-1 から SP に対しては、SAML で規定された認証アサーションを送信し、これをもとに SP がユーザに対する利用許可を行う。ここで、SAML では認証アサーションを送信する際にユーザ端末を経由する HTTP リダイレクト処理を用いる。図 2にこの様子を示す。

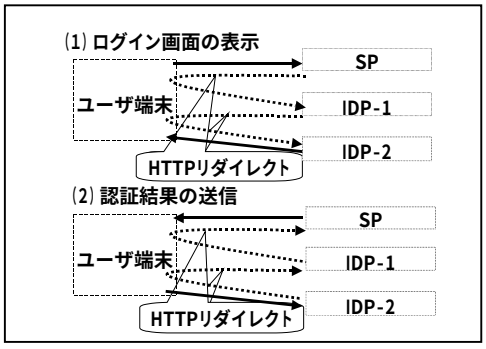

図 2　SAML による ワンストップ認証の課題

SAML がユーザ端末を経由した HTTP リダイレクト処理を用いるのは、SAML がオープンな規格でありユーザ端末上の機能に依存しない柔軟性が求められるためである。しかし、ユーザ端末は SP や IDP で用いているサーバよりも処理速度や接続先通信回線速度が低速である場合が多く、この処理を多用すると処理効率が低下する。図 2

[1] A study about one-stop authentication protocol.
Reiko ABE, Yoshisato TAKEDA, and Yasuhide KITAYAMA,
Information Technology R&D Center, Mitsubishi Electric Corporation

はワンストップ認証を SP と IDP-1、IDP-1 と IDP-2 のシングルサインオンの組み合わせとして実現しているが、一般にワンストップ認証は、このように単純なシングルサインオンよりも多数のサービスにより構成され、HTTP リダイレクト処理の発生頻度がより高くなり、認証性能低下がより深刻となる。この性能低下を回避することが課題である。

4　課題を解決するプロトコルの例

3章で述べた課題は、SAML をそのままワンストップ認証に流用したことに起因する。本研究では課題を解決したプロトコル設計を行った。このプロトコルの例を図 3に示す。

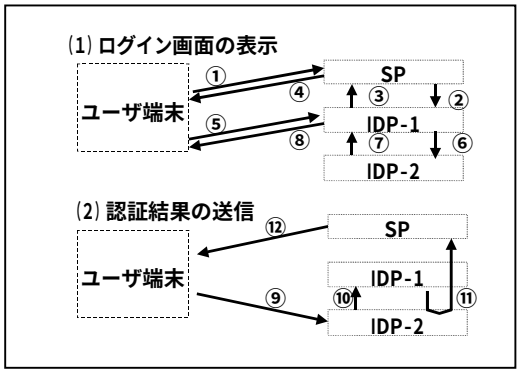

図 3 ワンストップ認証処理改善例

図 3に示した処理の流れについて概要を示す。

図 3の（１）では以下の処理を行う。

① ユーザはユーザ端末から SP のサービスを要求

② SP はユーザ認証を依存している IDP-1 にユーザが認証済であるかを問い合わせる

③ IDP-1 は、当該ユーザが認証済みでなく IDP-1 に登録されていない場合、ワンストップ認証を許可する信頼関係のある IDP のリストを SP に返す。

④ SP は、返された IDP のリストをユーザ端末に返し、認証を受ける IDP を指定するための画面を IDP-1 の URL を埋め込んでユーザに提供する（※１）

⑤ ユーザが IDP リストから IDP-2 を指定すると、※１で提供された IDP-1 の URL に IDP-2 によるユーザ認証要求が送付される。

⑥ IDP-1 ではこれを受け、IDP-2 にユーザ認証を要求すると共に IDP-2 に対して IDP-1 の URL を登録する（※２）。

⑦ 要求を受けた IDP-2 は、IDP-1 に対し ID・パスワード入力画面の送付を要求し、情報の入力を待つ。

⑧ IDP-1 では、IDP-2 の要求に従ってユーザ端末へ当該画面を送付する。その際、画面には IDP-2 の URL を付加する（※３）。

（２）では以下の処理を行う。

⑨ ユーザが ID・パスワードを入力すると、※３にて画面に埋め込まれた URL により情報が IDP-2 に送付される（※４）。

⑩ IDP-2 では送付された ID・パスワードを検証し、成功した場合 IDP-1 に当該ユーザの認証に成功したことを証明する情報を送る（※５）。

⑪ 情報を受け取った IDP-1 は、その情報が確かに IDP-2 により認証成功した結果であるという事が確認できたら、当該ユーザに対して SP のサービス利用を許可するという情報を SP に送る。

⑫ SP では受け取った情報が IDP-1 により発行されたことを確認し、ユーザに SP のサービス利用を許可する。

以上が本プロトコルの概要であり、以下の点により HTTP リダイレクト処理を回避している。

・IDP-1 から SP 経由でユーザに IDP リスト画面を※１で送付するよう構成し、当該画面に URL を埋め込む。

・※２で登録した情報を用い、※５で HTTP リダイレクト処理なしに IDP-2 から IDP-1 に情報を送る。

・※３で付加した URL により、※４でユーザが ID・パスワードを IDP-2 に直接送付する。

5　まとめ

個人情報保護に対する意識の高まりや情報漏洩事件の続発を受けて、個人情報の分散を抑止する技術であるワンストップ認証に対する潜在的ニーズが高まっている。本稿では、代表的な既存の認証情報伝達プロトコルであるSAMLをワンストップ認証に適用する場合の課題について考察し、プロトコルレベルから見直すことで課題を解決する具体的な手法の例を提案した。

※本研究は（独）情報通信研究機構の平成17年度委託研究「異なるCA間の認証ローミング技術に関する研究開発」の一環として行った。

＜参考文献＞

[1] OASIS Security Services (SAML) TC.
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[2] Liberty Alliance Project.
http://www.projectliberty.org/