2ZA-3

属性情報の選択的提示が可能なShibbolethシステムの試み

今野 真希† 武 佑香‡ 村上 智祐‡ 齋藤 孝道†
明治大学† 明治大学大学院‡

１．はじめに

インターネット上でサービスを提供するWebアプリケーションを利用する際，ユーザの真正性の確保，及び個人情報を含む機密情報や通信内容の保護といった目的で，ユーザ認証が行われる．ユーザ認証はシステムごとに行われているため，利用するWebアプリケーションが増えると，ユーザは複数のアカウントを管理することになる．また，システム管理者はシステムごとにアカウントを管理する仕組みを用意することとなる．これを解決する技術として，ID連携という概念が提案された．

ID連携を実現する手法の一つにShibboleth[1]がある．Shibbolethを導入することで，ドメインが異なる複数のWebアプリケーションの認証にシングルサインオンを導入することができる．

また，認証されたユーザの属性に基づきアクセス制御を行う技術（以下，ロールベースアクセス制御という）を導入しているWebアプリケーションが存在する．ShibbolethではLDAPと言ったアカウント管理ディレクトリに登録されたユーザの属性群を一意にWebアプリケーションに渡すため，ユーザに属性を渡すか否かの選択はできない．

本論文では，ユーザが自身の属性情報を，認証時に，選択することができるShibbolethシステムの提案を示した．

２． Shibboleth

２．１．概要

Shibbolethは，Internet2にて開発されるオープンソースミドルウェアで，SAML(Security Assertion Markup Language)［2］の実装の一つである．ドメインが異なるサイト間でフェデレーションを構築することで，シングルサインオンやアクセス制御を可能にする．ここで，SAMLとは，認証情報を安全にやり取りするためのXMLを用いた仕様である．認証情報はアサーションによって交換され，属性情報，認可情報も含まれる．

A Proposal of Shibboleth IdP system that gives only attributes to SP which User chooses
†Maki Konno, Takamichi Saito
‡Yuka Take, Tomosuke Murakami
Meiji University(†), Graduate School of Meiji University(‡)

２．２．構成

Shibbolethの構成を以下に示す．

・IdP(Identity Provider)
外部のディレクトリサーバ（本論文では，後述のLDAPを想定する）を参照し，ユーザ認証を行う．ユーザの認証情報をSPに提供する．この際，属性をSPに送信して良いかどうか，後述のMetadataと呼ばれるポリシーを確認し，各属性が送信可能である場合，SAML2.0に準拠して安全に属性情報を送信する．

・SP(Service Provider)
IdPに対して認証要求を行い，認証アサーションを受け取って認証がされているか否かの確認を行う．また，IdPに対して，属性の要求を行い，属性アサーションから属性情報を取得し，アプリケーションに提供する．ただし，既にShibboleth認証されているユーザからのアクセスの場合，ユーザ認証は行わずにSPに保持されているはずの認証情報を利用する．

・User
Webアプリケーションを利用しようとしているユーザ．ブラウザから，SPを機能として持つWebアプリケーションのURLへアクセスし，IdPにて，認証を行う．

・Metadata
IdPとSPは，異なる運営主体により運用されるケースがあるが，相互に保持するMetadataにより，信頼関係を定めることができる．このMetadataには，IdP，SP，それぞれの役割，提供する機能，それを利用するための通信方法及び公開鍵証明書等が含まれている．

３． LDAP

LDAP(Lightweight Directory Access Protocol)とは，ディレクトリサービスにアクセスするために使用するプロトコルの一つである．ネットワークを利用するユーザのメールアドレスや環境に関する情報を管理することができる．今回はActive DirectoryをLDAPサーバとして用いる[3]．

4. Moodle

Moodle [4]は，授業用の Web ページを作成し，教育管理を行う Web アプリケーションである．教師が学習用のページを作成し，生徒が利用する．管理者，教師，生徒等のロールがあり，ロールベースアクセス制御を行うことが可能である．今回は，これを Web アプリケーションとして用いる．

表 1 ロールとその権限の例

	管理者	教師	生徒
ユーザ作成	可能	不可能	不可能
コース作成		可能	不可能
コース履修			可能

5. 提案システム

5．1．概要

Shibboleth では，設定ファイルに基づいて，LDAP に登録されているユーザの属性情報を渡しており，ユーザはどの属性を渡すか否かの選択権はない．そこで，本論文では，ユーザが認証時に自身の属性情報を SP に対して送信するかどうか選択する仕組みを導入する．

5．2．構成

提案システムの構築環境は下表の通りである．

表 2 提案システム構築環境

IdP	Shibboleth IdP Version2.3.3
SP	Shibboleth SP Version2.3 Moodle Version1.9
LDAP	Active Directory (Windows Server2008 R2)

今回，改修する点は以下の 2 点である．

- 認証画面にチェックボックスを追加し，チェックをいれることによって，ユーザは属性を送信するかどうか選ぶ．
- Shibboleth の設定ファイルの一つである，attribute-filter.xml には，IdP から SP に対して送信する属性が記述されている．事前に，認証画面でのチェックに基づくファイルを複数用意し，このファイルを動的に切り替える．

以上より，ユーザが選択的に属性を SP へ送信することを可能とした．

5．3．利用シナリオ及び動作

ここでは，提案システムの動作例を示す．前提として，管理者，教師，生徒といった属性情報をもったアカウントが既に LDAP に登録されていることとする．

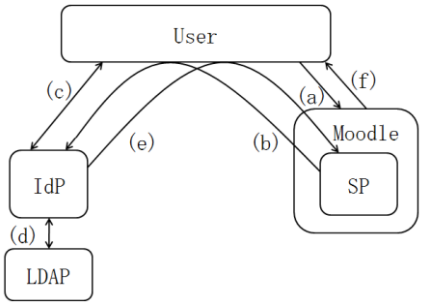

図 1 提案システム概念

(a) User は，SP を機能として持つ Web アプリケーションへアクセスする．この際，Cookie を確認し，すでに以前に Shibboleth 認証がなされ，シングルサインオンセッションが確立している場合，認証はされない．

(b) SP とシングルサインオンセッションが確立していない場合，SP から IdP へリダイレクトされる．SP は IdP に対し，認証要求(SAML リクエスト)を行う．リダイレクトメッセージには ID などの属性が含まれる．

(c) 認証を行う．User は ID，パスワードの入力に加え，SP に属性を送信するかどうかを選択し，チェックボックスにチェックを入れる．

(d) IdP は，LDAP へアカウント情報を参照する．認証が成功した場合，User の真正性を示す情報や属性情報を含むアサーションを発行する．

(e) 認証応答 (SAML レスポンス) を送信する．LDAP へ参照した結果，登録されたユーザなら，アサーションを送信し，属性を渡す．登録されていないユーザならその旨を SP に送信する．

(f) Web アプリケーション (Moodle) にて，ユーザに表 1 に基づき属性に対応するサービスを提供する．シングルサインオンセッションの維持は Cookie を用いて行われるため，Cookie が有効である間は，これにより，(b)～(e)を経ずに，Web サービスを受けることができる．

6. まとめ

本論文では，ユーザが Web アプリケーションに対し，選択的に属性情報を送信することのできる Shibboleth システムの実現方法を提案した．

7. 参考

[1] http://www.internet2.edu/
[2] http://www.oasis-open.org/
[3] 武佑香，後藤浩行，鳥居悟，齋藤孝道，2011，Shibboleth を用いた Web アプリケーションのアクセス制御の実現，情報処理学会 第 73 回全国大会
[4] http://moodle.org/