3Y-7

Shibboleth を用いた Web アプリケーションのアクセス制御の実現

武　佑香†　　後藤　浩行†　　鳥居　悟‡　　齋藤　孝道†

明治大学†　　株式会社富士通研究所‡

1. はじめに

インターネットにおける Web サービスを利用する際，パスワードによるユーザ認証を行うことが多い．しかしながら，利用する Web サービス数が増加すると，ユーザはその Web サービス毎にアカウントを管理することとなる．この解決策として，Cookie を用いたシングルサインオン技術が広く知られている．しかし，従来の Cookie を用いた方式では，ドメインが違う複数の Web サービスの認証にシングルサインオンを実現することができない．それを可能とする技術として ID 連携がある．ここで，ID 連携とは，組織毎に管理されているアカウントを，信頼関係を築いている組織間で相互に利用できるようにする仕組みのことである．

本論文では，一般にユーザのアカウント管理において Active Directory(以下，AD という)[1]が広く利用されていることを鑑み，AD 上で定義されているアカウント情報に基づき，ID 連携技術の一つである Shibboleth [2]を用いた認証方式を実現した．

2. Shibboleth

2.1. 概要

Shibboleth は，SAML（Security Assertion Markup Language）[3]の実装であり，ID 連携によるシングルサインオンを実現する Web アプリケーションソフトウェアである．また，ユーザの属性情報に基づいたアクセス制御をすることも可能である．ここで，SAML とは，標準化団体 OASIS（Organization for the Advancement of Structured Information Standards）によって策定された，ID やパスワードなどの認証情報を安全に交換するための XML（eXtensible Markup Language）仕様である．認証情報の交換方法は SAML プロトコルとしてまとめられており，メッセージの送受信には HTTP もしくは SOAP が用いられる．

Access Control of Web Application in Shibboleth
† Yuka Take, Hiroyuki Goto, Takamichi Saito
‡ Satoru Torii
Meiji University(†)
Fujitsu Laboratories LTD.(†)

特に，従来の Cookie のみを用いた Web の認証方式では実現できない，ドメイン間でのシングルサインオンを実現できることが特徴である．

2.2. Shibboleth の構成主体

Shibboleth の構成を以下に示す．

IdP(IdentityProvider)

IdP とは，ディレクトリサービスやデータベース経由でユーザの属性情報を取得し，それを用いたユーザ認証，及びユーザの属性情報の提供を実現する．本論文では，LDAP [4]として動作している AD を参照することで，ユーザ認証と属性情報の提供を行う．

SP(Service Provider)

ユーザ認証を IdP に要求し，IdP からの認証情報を受け取り，それをアプリケーションに提供することを実現する．ただし，既に，ユーザ認証がされていた場合，保持する認証情報をアプリケーションに提供する．SP 内でモジュールとして動作している shibd により，IdP へのメッセージの生成と，Web アプリケーションへの認証情報の提供が行われる．また，IdP と SP は，異なる運営主体により運用されるが，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．

user

Web アプリケーションを利用しようとするユーザもしくは Web ブラウザである．Internet Explorer や Firefox といった一般的な Web ブラウザを想定する．

3. 関連技術

AD について

前述の通り，本論文では，AD を LDAP サーバとして利用する．AD には，ユーザのアカウント（ID 及びパスワード）が登録されており，そのアカウントで Shibboleth による認証を受ける．

Moodle について

Moodle [5]は，授業用の Web ページを作成し，資料等を提供するための 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（表１）．

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

また，Moodle は，LDAP，RADIUS，Shibboleth といった外部の認証サーバの利用に対応している．

4. 提案システム

4.1. 概要

提案システムは，AD と連携した Shibboleth を用いて，Web アプリケーションである Moodle におけるユーザのアクセス制御を行うものである．特に，本論文では，Moodle におけるユーザへのロール付与を AD 上で定義されたユーザの属性を基に行い，ロールへの権限割り当ては Moodle 側で行うことを実現した．

4.2. 構築環境

提案システムを動作させるにあたり，下記のように 4 台のサーバを用意し構築環境とした．

- IdP ：CentOS5.4 kernel 2.6.18
- SP ：CentOS5.4 kernel 2.6.18
- AD ：Windows Server 2008 R2
- Moodle：CentOS5.4 kernel 2.6.18

また，Shibboleth の IdP のバージョンは 2.2.0 とし，SP はバージョン 2.0 とした．

4.3. 利用シナリオ及び動作

ここで，提案システム及びその利用シナリオに基づき，その動作を示す．番号に a が付加されているものを利用シナリオ，b が付加されているものを提案システムの動作を以下に説明し，図１と併せて示す．

(1a) user は，SP が保護している Web アプリケーションへアクセスする．この際，Cookie を確認し認証されていない場合，SP によって IdP へリダイレクトされる．リダイレクトメッセージには ID や属性等が含まれる．これにより，リクエストとレスポンスを対応付ける．

(1b) SP から IdP へのリダイレクトの際，IdP に認証要求（SAML リクエスト）を行う．送信方法は，SAML の規定により，SOAP と HTTP を用いる事ができるが，本論文では HTTP を用いた．

(2a) ログイン状態に関連付けられた Cookie を確認する．当該 Cookie がログイン状態を保持するとき，4b へ．

(2b) user は，ID とパスワードの入力する．IdP によるユーザ認証方式は任意だが，本論文ではパスワード認証を採用した．

(3b) IdP は，AD へユーザアカウント及び属性情報等を参照する．ユーザ認証が成功した場合，その情報に関連付けられた Cookie を発行する．

(4b) 認証応答（SAML レスポンス）を送信する．AD へ参照した結果，登録されたユーザなら，認証情報等を，登録されていないユーザならその旨を SP に送信する．

(5b) Web アプリケーションにて，当該ユーザに当該ユーザに対応するサービスを提供する．ユーザが Shibboleth を利用している間，当該セッションの維持は Cookie を用いて行われるため，当該 Cookie が有効である間は，これにより Web サービスを受けることができる．

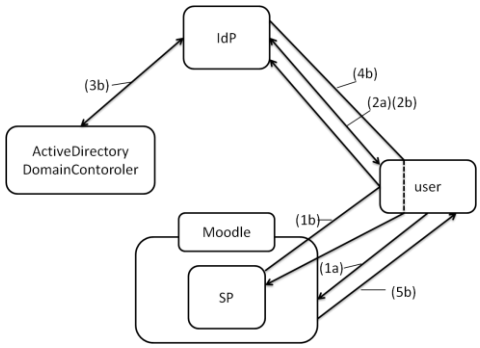

図１ 提案システム概念図

5. まとめ

本論文では，AD と連携した Shibboleth を用いて，Moodle におけるアクセス制御を提案した．特に，AD へ参照する際，AD 上の属性情報を SAML R レスポンスに埋め込むことで Moodle 上のロールに基づくアクセス制御を可能とした．

謝辞

本研究を実施するに当たり，多大な貢献を頂いた笠原卓也氏に，記して感謝する．

参考文献

[1]http://www.microsoft.com/japan/windowsserver2008/r2/technologies/ad-main.mspx
[2]http://www.internet2.edu/
[3]http://www.oasisopen.org/home/index.php
[4]http://www.ietf.org/rfc/rfc4511.txt
[5]http://moodle.org/