5Z-3

SAMLによる属性情報の選択的提示の可能なシングルサインオンシステムの提案と実装

磯 侑斗† 今野 真希‡ 武 佑香‡ 齋藤 孝道†
明治大学† 明治大学大学院‡

1. はじめに

企業内や大学内で利用されるシステムには認証が必要なものが多く，その増加に伴い，認証の手間や複数のアカウント管理といった問題が発生する．この問題を解決するために，一度の認証で複数のシステムの認証が完了する仕組みであるシングルサインオンが利用されている．加えて，近年では，クラウド上のWebアプリケーションなどといった外部のサービスを利用する企業や大学の増加に伴い，異なるドメイン間でのシングルサインオンも増えている．

このようなシングルサインオンを実現する方法の1つにSAML（Security Assertion Markup Language）[1]がある．SAMLでは，ユーザの属性情報（氏名，メールアドレス等，ユーザに関する情報）を予め登録しておき，認証時にWebアプリケーション等のシステムに送信することができる．

属性情報にはユーザの個人情報が含まれている場合があるが，一元的に送信されることが多い．その結果，ユーザには属性情報送信の可否を選択する機会が与えられず，送信したくない属性をも送信してしまうことが課題としてあげられる．

本論文では，認証時にユーザの属性情報をユーザが選択的に提示できる，SAMLを用いたシングルサインオンシステムを提案，実装し，この問題の解決を試みることとした．

2. SAML

2.1. 概要

SAMLはIdPとSP間で認証，認可，属性に関するデータ（アサーション）を交換するためのXMLベースのフレームワークである．SAMLではIdPとSP間でアサーションの交換することによりシングルサインオンを実現している．

A Proposal and Implementation of SSO with SAML That Provides User Attribute Selectively
†Yuto Iso
‡Maki Konno, Yuka Take
†Takamichi Saito
Meiji University (†), Graduate School of Meiji University (‡)

2.2. SAMLの構成主体

SAMLを構成する主体を説明する．

- Identity Provider（IdP）
  EndUserのアイデンティティ情報を生成，管理し，SPに対してEndUserの認証情報を提供する役割を持つエンティティ．
- Service Provider（SP）
  EndUserや他のエンティティにサービスや商品を提供するエンティティ．
- EndUser
  IdPによって認証を受け，SPを利用するユーザ．EndUserは，Webブラウザによって IdPやSPにアクセスする．

2.3. バインディング

SAMLではアサーションを交換する方法（バインディング）を複数規定しているが，ここでは，本論文で利用するHTTP Redirect/POSTバインディングについて説明する（図1）．

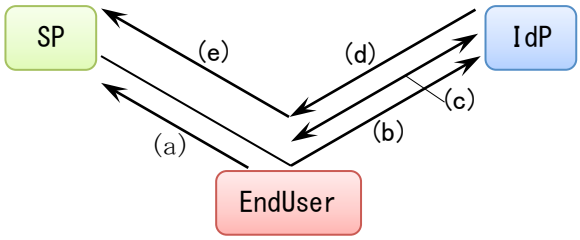

図1 HTTP Redirect/POSTバインディング

(a) EndUserがSPの提供するサービスをリクエストする．ただし，サービスを利用するためには認証が必要である．
(b) SPはEndUserをIdPへHTTPリダイレクトさせる．SPは，リダイレクト先URLのクエリ文字列に認証を要求するアサーションを含めることにより，IdPに認証要求を送信する．
(c) IdPはEndUserを認証する．ただし，SAMLではユーザ認証の方法を規定していない．別途パスワード認証などを実装する．
(d) IdPは，SPからの認証要求に対するアサーションをEndUserに送信する．
(e) EndUserはIdPから受け取ったアサーション

を HTTP POST メソッドを用いて SP に送信する.

3. 提案システム

3.1. 概要

本提案システムは, SAML によるシングルサインオン時に IdP に登録されている EndUser の属性情報のうち, EndUser が送信を許可した属性のみを SP に送信するシングルサインオンシステムである.

SP は IdP に, SP の動作に必須である属性(以降, 必須属性と呼ぶ) と必須ではない属性 (以降, 任意属性と呼ぶ) の区別をして IdP に要求する. 認証の際, IdP は SP が要求する属性を, それが必須属性であるか任意属性であるかを含め, EndUser に知らせ, SP に送信してよい属性を選択させる. IdP は EndUser の選択に基づき SP に EndUser の属性情報を送信する.

これにより, EndUser は任意属性の送信を許可または拒否することで, 属性情報の選択的提示が可能となる. また, 必須属性の送信を拒否することで, SP の提供するサービスの利用をやめることができる.

3.2. 構築環境

提案システムの IdP と SP は共に SimpleSAMLphp 1.10.0 [2]を利用した.

SimpleSAMLphp は PHP で記述されたオープンソースの認証フレームワークであり, SAML の IdP や SP として動作させることができる.

IdP での改修・追加事項は以下である.

- SP が要求する属性の一覧とそれぞれの属性が必須属性であるかを SP から受信する処理
- SP が要求する属性を認証画面に表示し, 送信を許可する属性を EndUser に選択させる処理
- 必須属性を EndUser が送信しないとした場合にエラー画面を表示する処理
- EndUser の選択に応じて属性情報を SP に送信する処理

SP での改修・追加事項は以下である.

- SP が要求する属性の一覧とそれぞれの属性が必須属性であるかを IdP に送信する処理

SP が要求する属性の一覧とその属性が必須属性であるかという情報の受け渡しは, 図 1 (b)でのアサーションの受け渡し時のクエリ文字列に追加する方法によって実現した. 例えば, SP の要求する属性が givenName, mail, uid であり, 必須とする属性が uid である場合, リダイレクト先 URL は図 2 となる (追加部分は波線部).

```
http://idp/?req=<アサーション>
&attr0=givenName&attr1=mail&attr2=uid&
reqAttr0=uid
```

図 2 リダイレクト先 URL

3.3. 利用シナリオ及び動作

本提案システムの利用シナリオおよび動作を HTTP Redirect/POST バインディングを利用した場合について, 図 1 を用いて説明する.

(a) EndUser が SP の提供するサービスをリクエストする. ただし, サービスを利用するためには認証が必要である.

(b) SP は EndUser を IdP へ HTTP リダイレクトさせる. リダイレクト先 URL のクエリ文字列にはアサーションに加え, 図 2 に示したような SP が要求する属性に関する情報も含まれる.

(c) IdP は EndUser を認証する. この際, EndUser は SP が要求する属性を SP に送信するかどうか, 図 3 に示すようなチェックボックスを用いて選択できる. ここで, EndUser が必須属性を送信しないとした場合, エラーとなる. すでに認証済みなどの理由で認証の必要がない場合でも, 属性送信の有無は SP 毎に確認される.

(d) IdP は, ユーザの選択に応じた属性情報を SP からの認証要求に応答するアサーションとして EndUser の Web ブラウザに送信する.

(e) EndUser は IdP から受け取ったアサーションを HTTP POST を用いて SP に送信する.

図 3 認証画面

4. まとめ

本論文は, 認証時に EndUser の属性情報を EndUser が選択的に提示できる SAML を用いたシングルサインオンシステムを提案し, その実装を示した.

5. 参考文献

[1] Standards | OASIS
https://www.oasis-open.org/standards#samlv2.0

[2] SimpleSAMLphp
http://simplesamlphp.org/