5Z-4

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

大丸 雅人† 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

近年，インターネット上でサービスを提供する Web アケーションが普及している．その中でも，Web メールや SNS といった，利用者の権限毎に固有のサービスを提供する Web アプリケーションが広く利用されている．Web アプリケーションでは，エンドユーザの認証を行う．認証には ID とパスワードが用いられる場合が多い．そのため，エンドユーザが複数の Web アプリケーションを利用する場合，複数のアカウントを管理しなくてはならない．また，Web アプリケーションの管理者は認証システムの構築や，個人情報の管理にコストがかかる．この問題を解決するフレームワークの一つに OpenID[1]がある．

Web アプリケーションが OpenID を用いる場合，エンドユーザの認証情報だけでなく，属性情報も認証サーバから取得できる．しかし，認証サーバはエンドユーザの属性情報を一意に RP へ提供してしまう．

本論文では，エンドユーザが自身の属性情報を，選択的に提示することができ，認証サーバに，要求されている属性情報が登録されていない場合は入力できる OpenID システムの実装を示す．

２．OpenID

２．１．概要

OpenID は，エンドユーザが選択した一つの ID で複数の Web アプリケーションの認証を受けることを可能にするフレームワークである．各エンドユーザが持つ URI 形式の識別子を認証に利用する．OpenID を用いると，異なるドメイン間でシングルサインオン（SSO）を実現することができる．また，後述する拡張仕様を用いるとエンドユーザの属性情報のやり取りが可能になる．属性情報とはエンドユーザのデジタルアイデンティティであり，年齢，性別などである．

２．２．関連用語

ここでは，OpenID に関する用語を説明する．

OP（OpenID Provider）

OP はエンドユーザの認証を行う主体である．また，エンドユーザのアカウントの管理，及び主張識別子の発行を行う．RP(後述)から認証要求があると，RP へエンドユーザの認証情報を送信する．後述する拡張仕様を用いると属性情報の提供を行える．

RP（Relying Party）

OP にエンドユーザの認証を委託する Web アプリケーションである．OP へ認証要求を送信し，エンドユーザの認証情報を取得する．後述する拡張仕様を用いると，OP にエンドユーザの属性情報を要求し，取得することができる．

主張識別子

OP がエンドユーザに発行する URI 形式の識別子．主張識別子は，OP の URI と，OP がエンドユーザを一意に識別できる識別子から構成される．図１に主張識別子の例を示す．

```
https://example.jp/Cifq4SRHabyY3YAaFAg
OP の URI          エンドユーザの識別子
```

図１．主張識別子の例

エンドユーザ

RP を利用するために OpenID による認証を受ける主体．

２．３．拡張仕様

OpenID AX

OpenID AX（Attribute Exchange）[2]は OpenID の拡張仕様の一つである．OpenID AX を用いると，RP と OP の間でエンドユーザの属性情報のやり取りが可能になる．RP は属性情報を取得するために取得したい属性情報を認証要求に含める．その後，属性情報を含んだ認証応答を OP から取得する．また，属性情報を必須として要求することができる．

３．WordPress

WordPress は，オープンソースのブログソフトウェアである．PHP により動的なページを作成することが可能である．管理者，投稿者，購読者などの権限があり，権限により作業範囲が定め

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

られている．今回は WordPress において，RP を利用する．

４．提案システム

４．１．概要

エンドユーザが自身の属性情報を RP へ送信してよいかを，OP での認証時に選択することができる OpenID システムの実装を示す．また，RP が必須として要求する属性情報が OP に登録されていない場合に，OP でエンドユーザに認証応答を送信してよいかの承認を得る画面で属性情報を入力できる仕組みを実現した．

４．２．構築環境

提案システムを実現するにあたり，2 台のサーバ（CentOS6.2 kernel 2.6.32）及び 1 台のクライアントマシン（Windows 7）を用意した．

RP

- Apache Version 2.2.15
- PHP Version 5.3.3
- WordPress Version 3.4.1
- MySQL Version 5.1.61

wordpress.org において提供されている OpenID プラグインを WordPress に組み込んだ．また，このプラグインを OpenID AX による属性情報の要求を行うように変更した．

OP

- Apache Version 2.2.15
- PHP Version 5.3.3

janrain.com において提供されている PHP OpenID Library を使用して OP を構築した．また，以下の変更を加えた．

- OpenID AX による属性情報の要求があった場合，RP に属性情報を提供できるようにした．
- エンドユーザの認証後，要求された属性情報を提供してよいかどうかをエンドユーザが選択できるようにした．また，必須として要求された属性情報が OP に登録されていなかった場合は，エンドユーザに登録を要求し，その値を RP へ提供できるようにした．

４．３．利用シナリオ及び動作

提案システムの動作を図２に示す．

(a) エンドユーザはクライアントマシンのブラウザを用いて RP へリソースの要求を行う．その後，エンドユーザは主張識別子を入力する．RP は，エンドユーザが入力した主張識別子から OP の URI を得る．

(b) RP と OP の間でメッセージの完全性と真正性を検証するための共有秘密鍵を交換する．

(c) RP は OP へ提供する認証要求を作成する．認証要求は HTTP リダイレクトで送信する．認証要求にはエンドユーザの属性情報を要求するための，OpenID AX のパラメータを含む．

(d) OP は，エンドユーザが認証されてない場合はエンドユーザの認証を行い，認証応答を生成する．その後，OP は認証情報と属性情報を送信してよいかをエンドユーザに確認し，承認された場合，認証応答にエンドユーザの認証情報と属性情報を含める．また，必須として要求された属性情報が OP に登録されていない場合はエンドユーザに入力を促し，その値を認証応答に含める．

(e) OP は，作成された認証応答を HTTP リダイレクトで RP へ送信する．

(f) RP(WordPress)は，OP から取得した認証応答を検証し，エンドユーザの認証情報と属性情報を得る．認証情報からエンドユーザの真正性を確認し，また，属性情報を用いてエンドユーザ固有のコンテンツ管理画面を提供する．

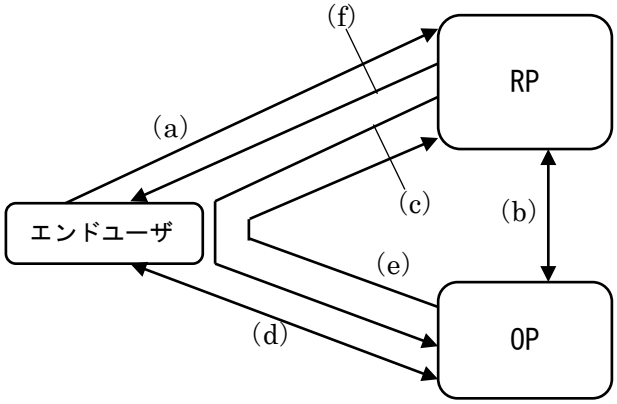

図２．提案システムの動作

５．まとめ

本論文では，エンドユーザが RP に対し選択的に属性情報を提供でき，また，RP が必須とする属性情報を OP が保持していない場合，ユーザに入力を促す OpenID システムを提案し，実装した．

６．参考文献

[1]OpenID Authentication 2.0
http://openid-foundation-japan.github.com/openid-authentication.html
[2]OpenID Attribute Exchange 1.0
http://openid-foundation-japan.github.com/openid-attribute-exchange.html
[3]PHP OpenID Library
http://janrain.com/openid-enabled/