OpenIDを利用したアクセス制御手法の提案

城間　政司†　　長田　智和‡　　谷口　祐治††　　玉城　史朗‡　　名嘉村　盛和‡
†琉球大学理工学研究科総合知能工学専攻　　‡琉球大学工学部情報工学科
††琉球大学総合情報処理センター

1　はじめに

近年，ユーザーを識別することで，個人に合わせたサービスを提供するウェブサービスが一般的になっている．しかし，ユーザーはウェブサービスごとにIDとパスワードを覚える必要があるため，セキュリティの観点で問題視されている．この問題を解決する手段の1つとして，OpenIDが提案された[1].

OpenIDは，ユーザーが自由に選択したIDをさまざまなウェブサービスへのログインに利用できる，非集中型のアイデンティティフレームワークである．2010年現在，GoogleやYahoo!などがOP(OpenID Provider: OpenIDを発行するサイト)としてOpenIDを発行しており，RP(Relying Party: OpenIDに対応したサービスを提供するサイト)は約35,000サイトを超えている[2]．このようなOpenID対応サイトでは，ユーザーがシングルサインオンするための本人同一性を認証する手段として，OpenIDを利用するケースが多い．

ところで，我々の進めているプロジェクト[3]では，複数のウェブサイトにおける認証や課金方法を共通化する技術を開発している．この技術は，ユーザーの本人同一性だけではなく，認証や課金の状態をウェブ上の分散環境で共有するために，OpenIDを利用する．本稿では，ユーザーの持つ任意の情報をもとにした属性認証や資格認証をOpenIDの認証手段として拡張し，ウェブ上の分散環境におけるアクセス制御手法を提案する．

2　関連研究

本提案手法と同様の手法には，ミクシィ社のOpenIDメンバーシップ認証[4]がある．OpenIDメンバーシップ認証では，認証対象のユーザーがSNS内の任意のユーザーと交友関係にあることや，コミュニティグループに属していることを証明するためにOpenIDを利用している．また，米サン・マイクロシステムズ社では，自社の社員にのみOpenIDを発行し，このOpenIDの所持者が自社の社員であることを認証している[5]．RPはこれらのOpenIDを利用し，アクセス制御を行うことができる．

ところで，これらの手法は，ユーザーの交友関係や所属のみを判断要素としたアクセス制御手法であり，より汎用的なアクセス制御を行うことができない．本提案手法では，ユーザーの持つ任意の情報を判断要素としたアクセス制御を行う．

3　提案手法

本提案手法は，アクセス制御ポリシーにOpenIDを割り当てることで，ウェブ上の分散環境におけるアクセス制御を行う．

3.1　任意の判断要素を用いるアクセス制御ポリシー

本提案手法では，OpenIDのプロトコルに適したアクセス制御にするため，ユーザーに関する情報を，“認証時に確認できる情報”と“ユーザーによる入力が必要な情報”の2つに分類する．

認証時に確認できる情報とは，性別，居住地，IPアドレス，セッション情報，認証の有効期間など，ユーザーがOPに事前に入力した情報やユーザーの環境からOPが知り得る情報である．

また，ユーザーによる入力が必要な情報とは，パスフレーズの入力，別のOpenIDによる認証，アンケート回答行為，課金行為など，アクセス制御時にユーザーが直接入力する行為が必要な情報である．

これら2種類の情報をユーザーに関する認証情報を判断要素とするアクセス制御ポリシーを設定する．

3.2　アクセス制御ポリシーに対応するOpenID

OPは，前節で分類したユーザーの持つ任意の情報を判断要素としたアクセス制御ポリシーにOpenID(URI)を割り当てる．そして，ユーザーは，証明したい情報に対応するOpenIDをRPに提示し，このOpenIDに関する認証をOPに要求する．

次に，OPは与えられたOpenIDに対応するアクセス制御ポリシーに従ってユーザー認証を行い，認証結果をRPに受け渡す．最後に，RPは認証結果から得

†Tadashi SHIROMA　joma@ns.ie.u-ryukyu.ac.jp
‡Tomokazu NAGATA　nagayan@ie.u-ryukyu.ac.jp
†Graduate School of Science and Technology, University of the Ryukyus.
‡The Department of Information Engineering, University of the Ryukyus.

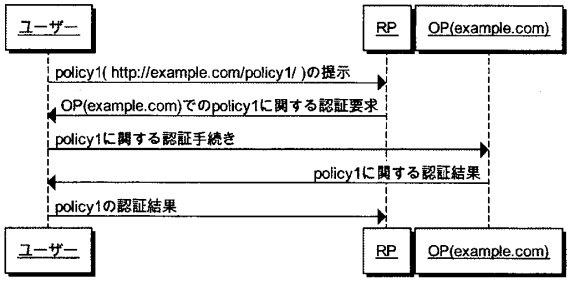

図 1: ユーザー情報の認証手順

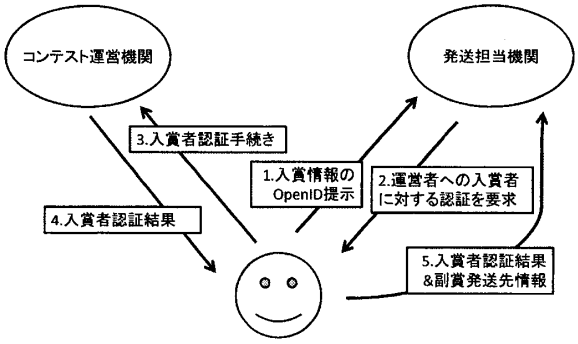

図 2: 入賞情報の認証手順

られるユーザー情報を判断要素としてアクセス制御を行う.

上記の認証手続き (図 1) を行うことで，RP は OP 上のアクセス制御ポリシーに適合したユーザーであることを識別することができ，ユーザー情報の認証結果を判断要素とするアクセス制御を行うことができる.

4 応用事例

我々の進めているプロジェクトでは，2010 年 1 月 15 日現在，オンラインフォトコンテストを実施している. 当コンテストでは，応募者が写真をコンテストウェブサイト上にアップロードし，投票・審査を経て入賞者を決定する. 入賞者には副賞が用意されており，入賞者は副賞発送前に本名や住所等の個人情報を，コンテスト運営機関とは別の担当機関 (以降，発送担当機関) に通知する必要がある.

コンテスト運営機関が入賞者に関する個人情報を保持しないようにするために，本提案手法を用いて入賞情報を発送担当機関と共有する. 入賞者は，コンテスト運営機関の発行した入賞情報に対応する OpenID を発送担当機関に提示し，副賞の受け取りに必要な個人情報 (名前や住所等) を発送担当機関のウェブサイト上で入力する (図 2).

一般的な方法では，入賞者はコンテスト運営機関のウェブサイト上で個人情報を入力し，コンテスト運営機関が入力された個人情報を発送担当機関に受け渡すため，個人情報を管理するリスクがコンテスト運営機関に生じる. 一方，本提案手法を用いると，コンテスト運営機関は入賞者に関する個人情報を保持する必要がないので，個人情報管理に対するリスクを軽減できる.

また，発送担当機関は，入賞情報の認証結果であるポインター (OpenID) を保持するだけでよいので，仮に入賞情報が重要な情報であっても，それを保持するリスクは高くならない.

5 まとめ

本稿では，OpenID を利用するアクセス制御手法を提案した. この手法は，アクセス制御ポリシーに OpenID を割り当てることで，ウェブ上の分散環境でのアクセス制御を可能にする. この手法では，ウェブ上のさまざまな要素を認証処理に利用することで，ウェブサービスにおける汎用的なアクセス制御ができる. また，重要な認証要素は必要な機関のみ保持するため，各機関における個人情報管理等に対するリスクを軽減することができる.

謝辞

本研究開発およびコンテンツチャンプルプロジェクトは，総務省の戦略的情報通信研究開発推進制度 (SCOPE) の支援を受けて行っております. ここに深く感謝の意を表します.

参考文献

[1] OpenID. http://openid.net/.

[2] JanRain, Inc. Relying Party Stats as of Mar. 1, 2009, 2009. http://blog.janrain.com/2009/03/relying-party-stats-as-of-mar-1-2009.html.

[3] コンテンツチャンプルプロジェクト. http://www.contents-chample.net/project/.

[4] mixi, Inc. OpenID Membership Authentication Method Draft-1. http://developer.mixi.co.jp/draft/openid-membership-authentication-method-draft-1.

[5] Sun Microsystems, Inc. Sun Identity Provider for OpenID. https://openid.sun.com/.