Web サービスにおける共通認証技術の信頼性向上と運用手法に関する実証的研究開発

研究代表者	長　田　智　和	琉球大学工学部情報工学科　助教
共同研究者	谷　口　祐　治	琉球大学総合情報処理センター　准教授
共同研究者	城　間　政　司	琉球大学理工学研究科総合知能工学専攻　大学院生
共同研究者	玉　城　史　朗	琉球大学工学部情報工学科　教授
共同研究者	名嘉村　盛　和	琉球大学工学部情報工学科　教授

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．

一方，近年，ネットブックやスマートフォンの普及により，外出時のインターネット利用が一般的になっている．インターネットに接続するための通信回線は，携帯電話端末での利用を想定した 3G 回線が広く使われているが，通信帯域や通信データ容量が制限されていることが多い．そこで，飲食店や公共施設等では，3G 回線の通信制限や 3G 回線を利用できないユーザーを考慮し，公衆無線 LAN サービスを提供する事例が増えている．

我々は，上記のようなセキュリティリスクやサービスのアカウント管理コスト及び利便性の問題を改善するために，ID 連携が有効であると考えた．本稿では，ID 連携をアカウント管理方式に適用する手法について述べ，適用例として公衆無線 LAN サービスシステムを提案する．

2 OpenID について

2-1 OpenID の概要

OpenID は,ユーザーが自由に選択した ID(OpenID)をさまざまなウェブサービスで利用するための分散アイデンティティフレームワークである．OpenID を利用するとユーザーとそのユーザーが所有する OpenID との一意性を認証できるため，OpenID 対応サービスへサインインするための ID として利用されることが多い．

OpenID 属性認証は，ユーザーの属性情報を主体として認証し，属性情報を元にサービス利用の認可を判断するロールベースアクセス制御[3]を可能にする．ロールベースアクセス制御は，ユーザーではなく属性情報を制御の判断要素とするため，柔軟なアクセス制御が可能となる．また，ユーザーごとにアクセス制御する手法よりも制御の判断要素数が少ないため管理が容易である．

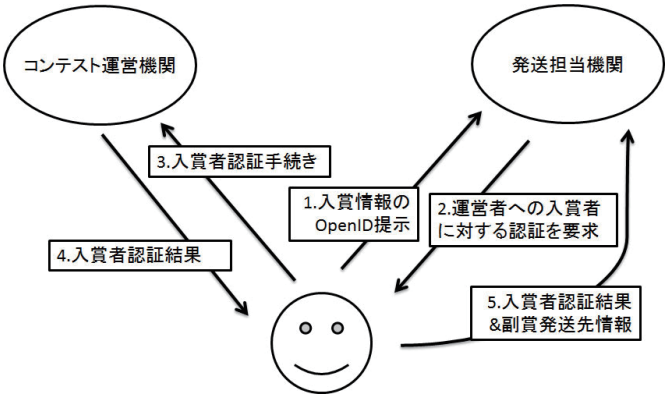
OpenID 属性認証の例として，コンテストの入賞者を対象にサービス利用を認可する場合，入賞者という属性情報を OpenID に紐付け，その OpenID で認証されたユーザーは学生であることをサービスプロバイダに証明できる．(図 1)

2-2 OpenID の関連研究

OpenID の関連研究として，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．我々の提案手法では，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．



【図１：OpenID による認証事例】

3 ロールベース OpenID

3-1 概要

ロールベース OpenID とは，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．

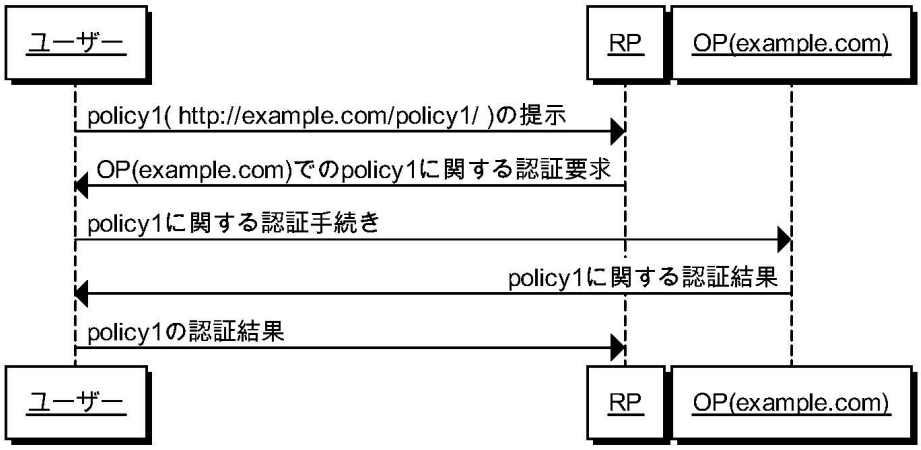
これら 2 種類の情報をユーザーに関する認証情報を判断要素とするアクセス制御ポリシーを設定する．

3-2 認証手順

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．

以上の認証手続き(図 2)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．



【図２：認証手続き】

4 公衆無線 LAN サービスシステム

4-1 従来のアカウント管理方式

公衆無線 LAN サービスにおけるアカウント管理方式は，WPA パーソナルモード等のパスワード共用方式，WPA エンタープライズ等のユーザー別アカウント管理方式が一般的である．両方式のユーザートレーサビリティとアカウント管理コスト及びサービスの利便性について考察する．

(1)パスワード共用方式

パスワード共用方式は，パスワードを共用するためユーザーによる登録手続きが必須ではなく，パスワードを通知する範囲を限定することで認可対象となるユーザーの範囲も制限できる．ただし，不正アクセスが起こった際にユーザーを一意に特定できず，また，セキュリティリスクを抑えるためにはパスワードの定期的な変更が必要となる．

(2)ユーザー別アカウント管理方式

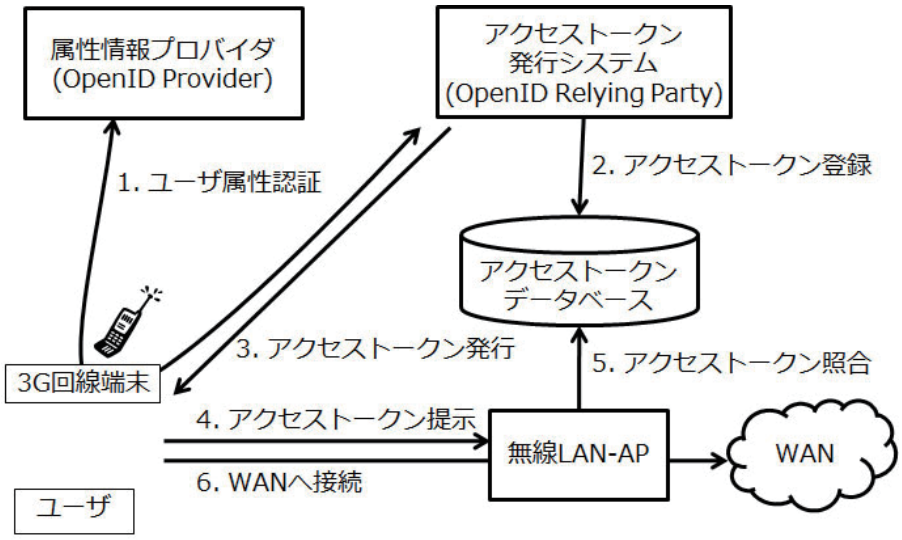
この方式は，アカウントを個別に発行することで，アカウントへのアクセスログ等からユーザーを一意に特定可能である．ただし，ユーザーの登録手続きやアカウントの管理が必要であるため，アカウント管理コストの増加やサービス利便性の低下につながる．

このように，上記の両方式はそれぞれユーザートレーサビリティやアカウント管理コストの増加及び利便性の低下が欠点となっている．そこで，両方式の欠点を補う方式として，OpenID 属性認証による ID 連携手法をアカウント管理方式に適用する．

4-2 ID 連携を適用した公衆無線 LAN サービスシステム

OpenID 属性認証による ID 連携手法をアカウント管理方式に適用した公衆無線 LAN サービスシステムの構成を図 3 に示す．このシステムは，属性情報プロバイダ(OP, OpenID Provider)，サービス利用の認可を判断しアクセストークンを発行するシステム(RP, OpenID Relying Party)，アクセストークンデータベース(アクセストークン DB)，無線 LAN アクセスポイント(無線 LAN-AP)の 4 つで構成される．

アクセストークンは，無線 LAN を利用するときに必要なクレデンシャルであり，ワンタイムパスワードとなる暗証番号を含む．ワンタイムパスワードを用いることで，アクセストークンが盗まれた場合の安全性の確保やアクセストークンを取得した端末以外の端末を用いた公衆無線 LAN サービスの利用を可能にする．



【図３：公衆無線 LAN サービスシステムの構成図】

ユーザーは以下に示す手順で公衆無線 LAN サービスを利用する．

(1)アクセストークンを要求するユーザー，OP，RP の三者間でユーザーの属性情報を認証し，サービス利用の認可を判断する．

(2)サービス利用を認可した場合，RP はアクセストークンを発行し，アクセストークン DB に登録する．

(3)RP は，発行したアクセストークンをユーザーへ送信する．

(4)ユーザーは，アクセストークンを無線 LAN-AP に提示する．

(5)無線 LAN-AP は，アクセストークンが有効かどうかを確認する．

(6)アクセストークンが有効である場合，ユーザーは無線 LAN を利用できる．

このシステムは，公衆無線 LAN サービスのユーザートレーサビリティ，アカウント管理コスト及びサービス利便性について以下のような特徴がある．

・ユーザートレーサビリティ
発行したアクセストークン及び IP アドレスのアクセスログから OpenID を特定可能であり，この OpenID を所有するユーザーを OP に問い合わせることで，ユーザーを一意に特定できる．

・アカウント管理コスト
サービスプロバイダのアカウント管理において，ID 連携によりユーザー別のアカウント管理を OP に委譲でき，アクセストークンの制御はシステムで自動化できるため，サービス利用の認可対象となる属性を設定するだけでよい．

・サービス利便性
ユーザーは OP 上の既存アカウントを利用するため，アカウント登録の手続きを簡略化できる．ただし，OP 上で認証する際に WAN へ接続するため，携帯電話や 3G 回線対応端末が必要となる．

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．

さらに，本稿では，OpenID 属性認証による ID 連携をアカウント管理方式に適用した公衆無線 LAN サービスシステムを提案した．このシステムは，属性情報の ID プロバイダと ID 連携することでユーザーの既存アカウントを利用可能とし，ユーザー追跡可能性を保ったまま公衆無線 LAN サービスプロバイダのアカウント管理コストを軽減する．また，ユーザーは既存アカウントを使用することで，サービス利用までの手続きを簡略化できる．

公衆無線 LAN サービスシステムは、現時点では，実機(ノート PC 及びスマートフォン)によるプロトタイプシステムを実装中であり，間もなく完成する予定である．大学内での実証試験を経て，外部発表にて成果を公表する予定である。

【参考文献】

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

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

[3] Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.;Youman, C.E.;. Role-based access control mod-els. *Computer*, Vol. 29, No. 2, pp. 38-47, Aug 2002.

[4] mixi, Inc. OpenID Member-ship 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/.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
OpenID 属性認証にもとづく公衆無線 LAN サービスシステムの提案	情報処理学会第 73 回全国大会予稿集(DVD-ROM)	2011 年 3 月
OpenID を利用したアクセス制御手法の提案	情報処理学会創立 50 周年記念(第 72 回)全国大会予稿集(DVD-ROM)	2010 年 3 月(参考)