4E-4

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

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，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．

一方，公衆無線LANサービスは，インターネットサービスを悪用する不正アクセス等，サービスプロバイダが望まないセキュリティリスクをはらんでいる．このようなセキュリティリスクは接続ユーザのトレーサビリティを高めることで抑止できるが，個別にアカウントを発行するとユーザ数に比例してアカウント管理コストが増加する．また，ユーザは登録手続き等を要求され，サービスの利便性が低下してしまう．

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した公衆無線LANサービスシステムを提案する．

2　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別アカウント管理方式が一般的である．両方式のユーザ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．

2.1　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．

2.2　ユーザ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を一意に特定可能である．ただし，ユーザ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．

3　OpenID属性認証

OpenID[1]は，ユーザが自由に選択した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とそのユーザが所有する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[2]は，ユーザ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，学生を対象にサービス利用を認可する場合，学生という属性情報をOpenID(例: http://example.ac.jp/students/)に紐付け，そのOpenIDで認証されたユーザは学生であることをサービスプロバイダに証明できる．

†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.

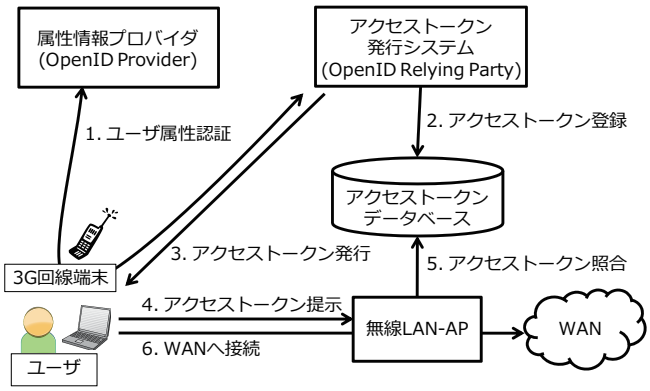

図 1: 提案する公衆無線 LAN サービスの概要図

4 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 1 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．

ユーザ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，OP，RP の三者間でユーザ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へ送信する．
4. ユーザは，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 を所有するユーザを OP に問い合わせることで，ユーザ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 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の既存アカウントを利用可能とし，ユーザ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．

参考文献

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

[2] 城間政司ほか. 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 DVD-ROM, 2010.

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