4V-01

認証サーバからユーザが利用する Web サービスを秘匿する権限委譲方式の提案

角田 裕太† 渡邉 貴文‡ 西倉 裕太‡ 宮田 大地‡ 渡辺 亮平† 齋藤 孝道†
明治大学† 明治大学大学院‡

1. はじめに

Web の技術の進歩に伴い，ネットショッピングや SNS など様々な Web サービスが普及してきた．Web サービスでの会員登録やログインを簡潔に行える仕組みとして，ソーシャルログインがある．ソーシャルログインを利用することで，ユーザは自分が登録している SNS アカウントなどの ID を Web サービスで使用することができ，ID とパスワードを新たに設定する必要がなくなる．また，Web サービスは，ユーザの ID やパスワードを管理する必要がなくなる．現在，ソーシャルログインの多くは，OAuth 2.0[1]や OpenID Connect[2]で実装されている．しかし，OAuth 2.0 や OpenID Connect において，認証サーバはユーザが利用する Web サービスを知ることができる．このことがプライバシーの観点において問題と捉えられる場合があり，これを解決するための仕組みが提案されている[3][4]．本論文では，文献[3]の提案にユーザの属性情報を提供する機能を加えた権限委譲方式を提案する．

2. 提案方式

ここでは本論文での提案方式について説明する．

2.1 概要

エンドユーザがどの Web サービスを利用しているかを認証サーバに秘匿しつつ，認証情報及び認証サーバ上にあるエンドユーザの属性情報を，エンドユーザの利用する Web サービスに提供する方式を提案する．提案方式では，ブラウザの拡張機能を用いて実現した．

2.2 提案方式における構成要素

- Identity Provider (IdP)
  エンドユーザのアカウントを管理し，エンドユーザを認証する．
- Relying Party (RP)
  IdP に認証を委託し，エンドユーザにサービスを提供するアプリケーションである．

A Proposal of Authorization Scheme to Conceal a Web Service from an Authentication Server
†Yuta TSUNODA ‡Takafumi WATANABE
‡Yuta NISHIKURA ‡Daichi MIYATA
†Ryohei WATANABE †Takamichi SAITO
†Meiji University ‡Graduate School of Meiji University

RP は，IdP の公開鍵と IdP の URL を紐付けて登録する．

- エンドユーザ
  IdP に認証を受け，RP を利用する主体である．
- Endpoint
  IdP が発行する認証応答の送信先となる RP の URL である．
- Nonce
  ランダムな文字列である．
- Timestamp
  Token の発行日時を表す文字列である．
- Scope
  RP が要求するエンドユーザの属性情報の範囲を表す文字列である．
- KeyRP
  RP がサービス利用ごと(以降，セッションと呼ぶ)に生成する公開鍵である．
- Token
  Endpoint，Nonce，Timestamp，Scope 及び KeyRP を連結した文字列をハッシュ関数によってハッシュ化した文字列である．Token の値は，以下の式の通り定める．ただし，H はハッシュ関数，||は文字列の連結を表す．

  Token = H(Endpoint||Nonce||Timestamp||Scope||KeyRP)

2.3 提案方式の動作フロー

提案方式の動作フローについて説明する．ただし，IdP には，エンドユーザのアカウント情報が登録されているものとする．また，RP は，認証委託先とする IdP の公開鍵及び IdP の URL を保持しているものとする．また，IdP の公開鍵に対する秘密鍵は，漏えい・棄損していないことを想定する．

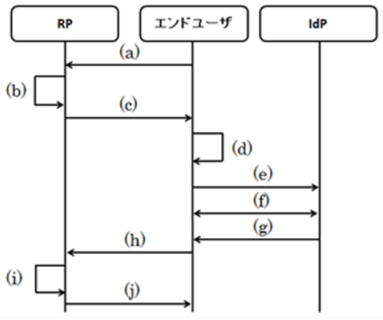

図 1 提案方式の動作フロー

(a) エンドユーザは，サービスを利用するためにRPにアクセスする．
(b) RPは，Endpoint，Nonce，Timestamp，Scope及びKeyRPを生成し，Tokenを計算する．
(c) RPは，(b)で生成したEndpoint，Nonce，Timestamp，Scope，KeyRP及びTokenをエンドユーザに送信する．
(d) エンドユーザは(c)で受け取ったEndpoint，Nonce，Timestamp，Scope及びKeyRPを連結した文字列をハッシュ化し，そのハッシュ値がTokenと一致するかを検証する．また，RPのドメインとEndpointのドメインが一致するかを確認する．これらが一致しない場合は，エラーとする．
(e) エンドユーザは，認証要求として，Token，Timestamp，Scope及びKeyRPをIdPに送信する．
(f) IdPは，IDとパスワード等を用いてエンドユーザを認証する．
(g) IdPは，(e)で受け取ったScopeに対応するエンドユーザの属性情報をKeyRPで暗号化する(以降，暗号化した属性情報と呼ぶ)．そして，認証応答として，Token，Timestamp，IdPのURL及び暗号化した属性情報を連結した文字列にIdPの秘密鍵でディジタル署名した値をエンドユーザに送信する．
(h) エンドユーザは，(g)で受け取った認証応答を(c)で受け取ったEndpointの示すURLへ送信する．
(i) RPは，エンドユーザから受け取った認証応答に関して，Tokenが自身で生成したものであるか，有効期限内であるか，その上でTokenがすでに使用されたものでないか，ディジタル署名が正しいものかを検証する．検証が正しければ，KeyRPに対応する秘密鍵でエンドユーザの属性情報を復号する．
(j) RPは，(i)の検証でエンドユーザがIdPによって認証されたと確認できるため，サービスを提供する．

3. 評価

ここでは提案方式に対して評価を行う．

3.1 提案方式の秘匿性の検証

ここではIdPに対してRPが秘匿できていることを確認する．提案方式では，ブラウザの拡張機能を用いることにより，リファラ情報が認証サーバへ伝わることを防止する．またIdPに対して，エンドユーザが渡す情報は図1の(e)の通り，Token，Timestamp，KeyRP及びScopeである．これらのパラメータからRPが推測できないことを示す．

- Token
  Tokenはハッシュ化されているので，TokenからRPを推測することはできない．
- KeyRP
  KeyRPは，提案方式においてセッションごとに生成されるので，IdPはKeyRPからRPを推測することはできない．
- Timestamp
  Timestampは Tokenの発行日時であり，RPを推測できる情報は含んでいない．
- Scope
  ScopeはRPが取得したいエンドユーザの属性情報の範囲を表す文字列であり，RPを推測できる情報は含んでいない．

3.2 RPのパラメータ生成時間の測定

提案方式ではセッションごとに公開鍵ペアの生成を行う．今回，公開鍵ペアの生成及びTokenの生成を1,000回行うphpプログラムを実行した時の処理時間を計測した．計測はIntel CPUの2種で行った．実行環境のOSはCentOS 7.2.1511，phpのバージョンは5.4.6である．なお，公開鍵暗号アルゴリズムはRSA，鍵長は2048bitである．

表1 RPのパラメータ生成時間

	生成時間（1000回）	生成時間（1回）
i5-3317U	2m32.452s	152.452ms
Celeron N2830	5m43.5625s	343.5625ms

測定結果からRPのパラメータ生成はCPUの性能に依存するが，RPのパラメータ生成において，大きな遅延は発生しないと考えられる．

4. まとめ

本論文では，認証サーバからユーザが利用するWebサービスを秘匿する権限委譲方式の提案をした．また，提案方式の評価を行い，IdPに対して，RPが秘匿できていることを示し，また，処理速度も問題ないことを確認した．

5. 参考文献

[1] “The OAuth 2.0 Authorization Framework” https://tools.ietf.org/html/rfc6749
[2] "The OpenID Foundation Launches the OpenID Connect Standard” http://openid.net/2014/02/26/the-openid-foundation-launches-the-openid-connect-standard/
[3] Yuto Iso, Takamichi Saito “A Proposal and Implementation of an ID Federation that Conceals a Web Service from Authentication Server” The 29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015)
[4] Daniel Fett, Ralf Küsters, Guido Schmitz “SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web” Computer and Communications Security 2015