6W-06

SPKI 権限証明書を用いた Web における権限委譲の実現

宮田　大地†　　大丸　雅人‡　　渡邉　貴文‡　　西倉　裕太‡　　磯　侑斗‡　　齋藤　孝道†

明治大学†　　明治大学大学院‡

1　はじめに

Web2.0 技術登場以降，複数の Web サービスを組み合わせて，新しい Web サービスを開発するマッシュアップという設計手法が，Web サービス開発者の間で広く利用されるようになった．

マッシュアップサービスでは，Web サーバ上にあるエンドユーザのプロフィールや画像ファイルといったデータ（以降，保護されたリソースと呼ぶ）を取得する場合がある．この保護されたリソースへのアクセスには，アクセス権限が必要となる．エンドユーザがマッシュアップサービスにアクセス権限を委譲するために従来とっていた方法は，マッシュアップサービスにエンドユーザの ID とパスワードを預ける方法である．しかし，この方法ではエンドユーザの ID とパスワードを悪用することで，マッシュアップサービスがエンドユーザになりすますことが可能となるという問題がある．そこで，保護されたリソースにアクセスするマッシュアップサービスに ID とパスワードを渡さずに，アクセス権限を委譲する仕組みとして OAuth[1]が登場した．

OAuth は広く普及した一方，RFC6819[2]では OAuth における脅威モデルやその対策が多く挙げられている．すなわち，実装者は OAuth を実装する際，多くのセキュリティに関することを考慮しなければならず，OAuth をセキュアに実装することは容易ではない．

そこで，本論文では，仕様の設計段階で OAuth よりもセキュリティを確保することを目的としつつ，OAuth のような権限委譲を，別のアプローチで実現する方式の提案を行う．

2　SPKI 権限証明書

提案方式では，SPKI（Simple Public Key Infrastructure）[3][4]権限証明書を発行，送信することでアクセス権限の委譲を実現する．SPKI 権限証明書とは，公開鍵とアクセス権限の結びつきを SPKI 権限証明書の発行者がディジタル署名を付与することで保証したものである．

本論文で利用する SPKI 権限証明書の形式を以下に示す．[5]

$$<I,\ S,\ D,\ A,\ V>S(I)$$

I: *Issuer*　SPKI 権限証明書の発行者の公開鍵．

S: *Subject*　アクセス権限を行使する主体の公開鍵．

D: *Delegation*　S が更にアクセス権限を委譲することが可能かどうかを示すブール値．

A: *Authorization*　委譲するアクセス権限を示す値．

V: *Validity*　証明書の有効期限．

$S(I)$: SPKI 権限証明書の発行者 I の秘密鍵で，I, S, D, A, V に対してディジタル署名した値．

3　提案方式

3.1 概要

提案方式では，OAuth のような権限委譲を実現する．しかし，エンドユーザの保護されたリソースに対するアクセス権限の管理に，OAuth ではアクセストークンと呼ばれる（乱数などの）文字列を使用するが，提案方式では SPKI 権限証明書を用いる．

3.2 構成

・Server

エンドユーザの保護されたリソースを管理するサーバ．Client から受信した SPKI 権限証明書に応じて，エンドユーザの保護されたリソースを Client に送信する．

・Client

エンドユーザから委譲されたアクセス権限のもと，エンドユーザの代理として保護されたリソースにアクセスを行う Web サービス．

・エンドユーザ

Server 上にある保護されたリソースの持ち主．保護されたリソースに対してアクセス権限を持ち，Client にそのリソースに対するアクセス権限を委譲する．

・Cert1

Server からエンドユーザに発行される SPKI 権限証明書．エンドユーザが Server 上にある自身の保護されたリソースに対してアクセス権限を持つことを示す．

・Cert2

Implementation of SPKI Authorization over Web Application

†Daichi MIYATA
‡Masato OMARU, Takafumi WATANABE
‡Yuta NISHIKURA, Yuto ISO
†Takamichi SAITO
Meiji University(†), Graduate School of Meiji University(‡)

エンドユーザから Client に発行される SPKI 権限証明書．エンドユーザが Server 上にある自身の保護されたリソースに対するアクセス権限を Client に委譲することを示す．

3.3 動作フロー

提案方式の動作の説明を行う（図 1 参照）．動作フローとして，Client 上にあるエンドユーザの画像ファイルを Client が Server にアップロードし，その後に Server 上にある保護されたリソースをダウンロードすることを想定する．ただし，フローの開始前に，あらかじめエンドユーザと Client は自身の公開鍵証明書を Server に登録しておき，Client は Server の公開鍵を取得しておく．またエンドユーザは Server から Cert1 を取得しておく．

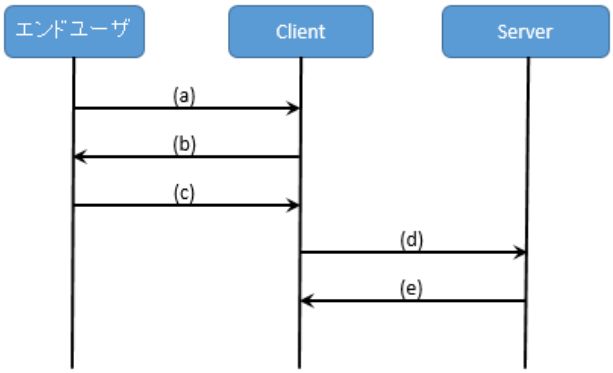

図 1　提案方式の動作フロー

(a) エンドユーザは，Client にアクセスする．

(b) Client は自身の公開鍵証明書，要求するアクセス権限及び証明書の有効期限をエンドユーザに送信する．

(c) エンドユーザは Client から受信した公開鍵証明書，要求するアクセス権限及び証明書の有効期限を検証する．エンドユーザが Client にアクセス権限の委譲を許可する場合，Cert2 を発行し，Cert1 及び Cert2 を Client に送信する．

(d) Client はエンドユーザから受信した Cert1，Cert2，画像ファイルを Server の公開鍵で暗号化したもの及びディジタル署名を Server に送信する．

(e) Server は Cert1 及び Cert2 に含まれている有効期限，公開鍵，アクセス権限及びディジタル署名を検証する．検証の結果，Cert1 及び Cert2 が正当であった場合，受信した画像ファイルを自身の秘密鍵を用いて復号する．また，Client の公開鍵を用いて，ディジタル署名を検証する．その後，Cert2 に含まれているアクセス権限に基づいたエンドユーザの保護されたリソースを Client の公開鍵で暗号化し，Client に送信する．

Client の公開鍵で暗号化する目的は，対応する秘密鍵を所持する Client 以外に秘匿性を保つためである．Client は自身の秘密鍵を用いて暗号化されたリソースを復号することで，エンドユーザの保護されたリソースを取得できる．

4　考察

提案方式が，基本仕様の段階で確保しているセキュリティについて，考察を行う．

権限委譲の際のセキュリティに Proof of Possession[6]（以降，PoP と呼ぶ）という考え方がある．PoP とは，提案方式における Cert1 及び Cert2 といった，セキュリティトークンの送信者の真正性を確認できるようにする考え方である．

OAuth 2.0 において，PoP は拡張仕様として考えられている．そのため，提案方式と同様に，PoP を実現するためには，基本仕様とは別に，処理を追加で実装する必要がある．

一方，提案方式は基本仕様の段階で，PoP を実現している．つまり，Server に Cert1 及び Cert2 を送信した Client が，Cert1 及び Cert2 の正当な持ち主であることを確認することが可能である．具体的には，Client から Cert1 及び Cert2 と同時に受信したディジタル署名を，Server が Cert2 に含まれている公開鍵を用いて検証することで実現できる．また，検証された証明書の公開鍵によりセッションを確立すれば，真正な主体へサービスを提供できる．

よって，提案方式は OAuth とは違い，基本仕様の段階で，PoP を実現しているといえる．これにより，セキュリティトークンの窃取等の脅威への耐性が高まると期待できる．

5　まとめ

本論文では，OAuth と異なるアプローチとして，SPKI 権限証明書を用いた権限委譲方式を提案し，実装した．また，提案方式が，仕様の設計段階で確保しているセキュリティについて，考察をした．

6　参考文献

[1] http://tools.ietf.org/html/rfc6749
[2] http://tools.ietf.org/html/rfc6819
[3] http://tools.ietf.org/html/rfc2962
[4] http://tools.ietf.org/html/rfc2963
[5] 齋藤孝道，梅澤健太郎，奥乃博，2000 個人情報の扱いを考慮したアクセス制御の一方法，インターネットコンファレンス 2000
[6] “OAuth 2.0 Proof-of-Possession （ PoP ） Security Architecture” https://tools.ietf.org/html/draft-bradley-oauth-pop-key-distribution-00