2Z-6

OAuth2.0 に SPKI を適用したアクセス権限委譲方法の提案

西倉　裕太†　　大丸　雅人‡　　今野　真希‡　　磯　侑斗‡　　齋藤　孝道†

明治大学†　　明治大学大学院‡

1　はじめに

インターネットの普及とともに，Web を用いてサービスを提供する Web アプリケーションが広く普及している．さらに，Web API によるサービスの提供や Ajax といった技術が登場し，複数の Web サービスを組み合わせることで，新たなサービスを構築するマッシュアップが利用されている．

マッシュアップサービスにおいては，Web アプリケーションを提供するサーバ上の保護されたエンドユーザのリソースに対し，アクセス権限を必要とする場合がある．マッシュアップサービスがエンドユーザに代わってアクセス権限を利用する場合，従来ではマッシュアップサービス側で，ID・パスワードを保持する運用形態が多かった．それに対し，エンドユーザが ID・パスワードを渡さずに，保護されたリソースにアクセスする権限を委譲する仕組みとして OAuth [1]が提案された．しかし，RFC6819 [2]では，OAuth における脅威モデルやセキュリティ上の検討項目が多く挙げられている，という現状がある．

そこで本論文では，RFC6819 の 4 節において脅威の指摘されている認可コード（後述）及びアクセストークン（後述）への対策の一つとして，権限と公開鍵の結び付けを行う SPKI（Simple Public Key Infrastructure）[3] [4]の権限証明書を OAuth2.0 に適用したアクセス権限委譲方式の提案を行う．

2　OAuth

2.1　概要

OAuth はエンドユーザのリソースに対するアクセス権限の委譲を実現する．OAuth1.0 はディジタル署名を利用し，OAuth2.0 は HTTPS を利用する．OAuth1.0/2.0 では，エンドユーザのリソースを保持する Server（後述）が，エンドユーザの同意のもと Client（後述）に権限を委譲することが可能である．

2.2　構成

●認可コード

エンドユーザがアクセス権限の委譲をする際，Server（後述）から Client（後述）へ発行される．アクセストークン（後述）の取得の際に利用する．

●アクセストークン

認可コードを提示した際に発行される文字列．権限の範囲を示す Scope，有効期限を示す Expires_in 等と合わせて Server（後述）に保存され，リソースへのアクセスの際に利用される．

●Server

AuthorizationServer 及び ResourceServer から成る．エンドユーザの認証，認可コード及びアクセストークンの発行を行う．また，保護されたエンドユーザのリソースを管理し，アクセストークンが提示された際にこれを提供する．

●Client

エンドユーザから権限の委譲を受けるために，Server にアクセストークンの要求をする．また，取得したアクセストークンを利用してリソースにアクセスし，自らの Web サービスに利用する．

●エンドユーザ（ResourceOwner）

Server に保護されたリソースの利用権限を持ち，Client にそのリソースへのアクセスを許可する．

2.3　動作フロー

OAuth2.0 でフローが複数定義されているが，ここでは本論文で利用する Authorization Code Grant について説明する（図 1）．ただし Client はフローを開始する前に，予め自らのアプリケーション情報（リダイレクト先 URI 等）を Server に登録しておく．

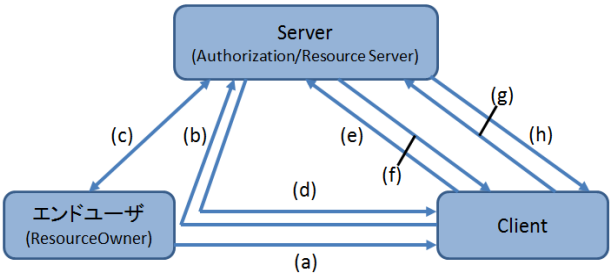

図 1.　Authorization Code Grant

(a)　エンドユーザが Client にアクセスする．

(b)　エンドユーザは Client により，Server へリダイレクトされる．

(c)　Server はエンドユーザを認証し，エンドユーザは権限の委譲の許可／拒否を伝える．

(d)　許可した場合，エンドユーザは Server によ

Delegation of access authority that applies the SPKI to OAuth2.0
†Yuta NISHIKURA
‡Masato OMARU, Maki KONNO, Yuto ISO
†Takamichi SAITO
Meiji University(†), Meiji University Graduate School.(‡)

り作成された認可コードを URI に付加して，クライアントへリダイレクトされる．

(e) Client は取得した認可コードを，Server に対して送信する．

(f) Server は認可コードを検証し，アクセストークンを発行する．

(g) Client は受け取ったアクセストークンを Server に対して提示する．

(h) Server はアクセストークンの正当性を確認し，それに基づいたリソースを提供する．

3 SPKI 権限証明書

本論文では SPKI において用いられている権限証明書を利用する．これは，公開鍵と権限の対応に，権限証明書の発行者がディジタル署名を付加したものである．具体的な SPKI 権限証明書（以降，権限証明書という）の様式は次のようになっている：<I, S, D, A, V>S(I) [5]

I：Issuer．権限証明書の発行者の公開鍵．
S：Subject．権限を行使する主体の公開鍵．
D：Delegation．ブール値．S が更に権限を委譲することが可能かどうかを示している．
A：Authorization．権限を表現している．
V：Validity．証明書の有効期限．
S(I)：権限証明書の発行者 I の秘密鍵．

4 提案システム

4.1 概要

本論文では，認可コード及びアクセストークンを利用せず，代わりにエンドユーザのリソースに対するアクセス権限を権限証明書によって管理する．また，証明書の所有者が，権限証明書を Server に対して提示することで，自らの公開鍵で暗号化されたリソースを Server から取得可能なアクセス権限委譲方式を提案，実装した．

4.2 構成

●Server
・Apache Version 2.2.15
・PHP Version 5.3.3
・OpenSSL 1.0.1e
●Client
・Apache Version 2.2.15
・PHP Version 5.3.3
・OpenSSL 1.0.1e
●権限証明書

“3 SPKI 権限証明書”で示した権限証明書を OAuth2.0 に以下のように適用する．

D：エンドユーザによる委譲は可，Client は不可．
A：権限の範囲を表す scope と対応させる．
V：有効期限を表す Expires_in と対応させる．

4.3 動作フロー

提案システムの動作の説明を行う（図 2）．ただしフローを開始する前に，予め Client 及びエンドユーザは自身の公開鍵証明書を Server にそれぞれ登録しておく．また，エンドユーザは Server から権限証明書 Cert1（エンドユーザがアクセス権限及びその権限を委譲する権限を有することを示す．I=*Server*，S=*エンドユーザ*，D=**可**，A=*全てのリソース*）を取得しておく．

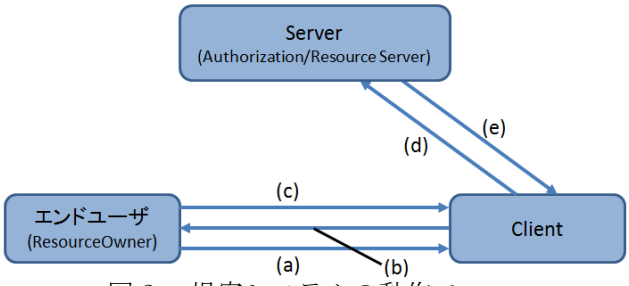

図 2. 提案システムの動作フロー

(a) エンドユーザが Client にアクセスする．

(b) Client は自らの公開鍵証明書及び Web サービスを提供するために必要な scope と Expires_in の値をエンドユーザに提示する．

(c) エンドユーザは Client の提示した公開鍵証明書及び 2 つの値を検証する．権限の委譲を許可する場合，検証した証明書及び値を基に，Client に対する権限証明書 Cert2（Client がアクセス権限を有することを示す．I=*エンドユーザ*，S=*Client*，D=**不可**，A=*エンドユーザが委譲するリソース*）を発行し，Cert1 とともに Client へ送信する．

(d) Client はエンドユーザから受け取った Cert1 及び Cert2 を Server に送信する．

(e) Server は Cert1 及び Cert2 の正当性を確認し，Cert2 に基づいたリソースを Cert2 に含まれる Client の公開鍵で暗号化し，Client に提供する．

5 まとめ

本論文では，権限証明書を利用したアクセス権限委譲方式を提案，実装した．これにより，RFC6819 の 4 章で脅威の指摘されている認可コード及びアクセストークンへの対策を行った．

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