L-032

ユーザが望むシングルサインオンを実現するための認可プロトコルに関する研究
Research on authorization protocol to achieve single sign-on for which user hopes

櫻木　陽介 †　　**今泉　貴史** ‡
Yosuke Sakuragi　　Takashi Imaizumi

1. はじめに

クラウドコンピューティングの発展と共に，シンクライアントシステムや SaaS といった，ネットワークを介してリソースやサービスを利用するシステムが増加している．これらのネットワークを介して利用するリソースやサービスは，ユーザにとっては自身の所有物であるが，サービス提供者にとっては自分が提供するサービスである．そのためサービス提供者は不正なアクセスを防ぐために，ユーザ認証により正当なユーザを識別し，適切なアクセス権限を与えることでアクセス制御を行っている．その結果ユーザには，自分のリソースではあるが自由に使えないという状況が生じている．例えば，シンクライアントシステム上のリソースを利用して SaaS からサービスを受ける場合を考えてみる．この場合，SaaS がユーザの ID やパスワードを知らないために，シンクライアントシステム上のリソースにアクセスできず，その結果ユーザがサービスを受けられないことがある．

このような状況に対処するために，アイデンティティ管理を複数のサービス提供者で連携するためのフレームワークの開発が進んでいる．例えば，シングルサインオンを実現する認証連携技術として，OpenID[1]・SAML[3]・Kerberos[4] などがある．特に Web のようなオープンな環境には，OpenID と認可プロトコルの OAuth[2] を組み合わせて，認証・認可のための連携を行うことが多い．OAuth はリソース所有者からアクセス許可の同意を得ることで，サービスが認可を行うことを可能とする．そのため，先ほど例で挙げた状況でも，リソース所有者から同意を得ることでシンクライアントシステムは認可を行うことができる．

しかし，OAuth はどんなサービスとでも連携できるわけではない．事前にサービス同士で信頼関係を構築していることを前提に動作しており，この関係構築はサービス同士の判断で行う．この関係を構築することは相手がリソースに対してアクセスしてくることを認めることを意味するので，サービスはリソースを守る立場として簡単に相手を信頼することができず，関係構築ができないことが多い．その結果，ユーザが連携して欲しい相手を実際にサービスが信頼するとは限らず，OAuth を利用すればユーザは所有するリソースを自由に利用できるという環境は実現していない．

2. 提案手法

本研究では，OAuth をユーザ主導で信頼関係構築を行えるように拡張することで，ユーザ主導のアクセス制御を行う認可プロトコルを提案する．ユーザがサービスの信頼性を保証し，サービスはユーザを信頼することで信頼関係を構築する．ただし利用するサービスが増えると，各サービスを 1 対 1 の信頼関係で管理することは困難になる．そのため，信頼の置ける第三者による間接的な信頼関係を構築する．OAuth はリソース所有者の同意に基づき認可を行うプロトコルであるので，リソース所有者が認可を一任する Authirization Manager（AM）を導入し，これを信頼の置ける第三者とする．各サービスはユーザが指定した AM と信頼関係を構築し，同じ AM を信頼するサービス同士が間接的に信頼できる仕組みを実現する．

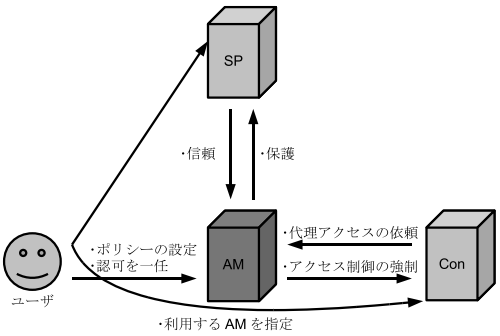

図 1: 提案手法の構成と 4 者の関係

提案するシステムはユーザ・Service Provider（SP）・Consumer（Con）・AM の 4 つのエンティティで構成される．図 1 に提案手法の構成と各エンティティの関係を示す．ユーザは Con のサービス利用者で，SP のリソース所有者である．SP はユーザのリソースを管理する Web サービスである．Con はユーザのリソースを利用しサービスを提供する Web サービスである．今回は SP が管理している認証によって保護されたリソースを利用して動作するサービスである．AM はリソース所有者に代わって認可を行うサーバである．役割は２つあり，ひとつは SP と Con の間接的な信頼関係を構築する仲介役をすること，もうひとつはリソース所有者の設定したルールを基にリソース所有者の代わりに認可の判断を行うことである．

2.1. 認可フロー

前提条件として，ユーザと AM，ユーザと SP，ユーザと Con は事前に信頼関係を構築しており，暗号化通信も可能であることを前提とする．この条件のもと，AM と SP，AM と Con の間で信頼関係を構築し，SP と Con の間接的な信頼関係を利用してリソースアクセスを可能とする．

†千葉大学融合科学研究科
‡千葉大学総合メディア基盤センター

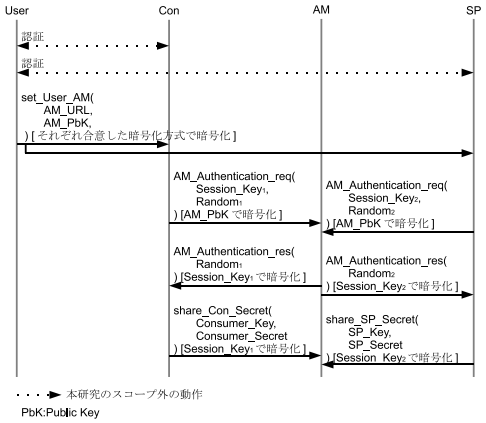

図 2: 事前準備フロー

まず認可フローの事前準備として，AM と SP，AM と Con の信頼関係を構築する．そのフローは図 2 のようになる．これによって，AM と Con は Consumer Key と Consumer Secret，AM と SP は SP Key と SP Secret を共有する．この Key と Secert は AM と Con，AM と SP の間で真正性§を確認するために使うので，共有する 2 者以外には知られないよう管理する．また，この事前準備により，認可フローでは共通鍵に Consumer Key，SP Key を利用した暗号化通信が可能となる．

認可フローは図 3 のようになる．まず，事前準備で築いた間接的な信頼関係を確認し，リクエストトークン (RT) を発行する．そして AM が RT の要求するアクセスを許可するかどうかを，ユーザの決めたルールに従って判断する．そうして許可された RT は SP によってリソースのアクセスを可能とするアクセストークン (AT) と交換され，アクセスが可能となる．

2.2.SP と Con の信頼関係構築の仲介機能

AM は，SP と Con の信頼関係構築の仲介役として機能する．本手法では，SP が AM を信頼し，AM が SP に対して Con の真正性を保障する．

AM が SP に対して Con の真正性を保障する前に，AM は Con の真正性を確認する必要がある．それは事前準備で Consumer Key と Counsumer Secret を共有することで可能となる．この 2 つの情報は，Con の ID とそのクレデンシャルにあたる．そのため Con がアクセスを依頼するときにこの 2 つの情報を提示することで，AM が Con の真正性を確認することができる．

AM が SP に対して Con の真正性を保障するための手続きは，AM と Con が Consumer Secret と乱数を用いて署名を生成し，それを SP に提示することで確認する．SP は AM と Con から送られてきた署名をが同一であれば，AM が保障する Con であることを確認することができる．

SP と AM の信頼関係構築は事前準備で行っており，SP はこのときユーザが指定した AM を信用する．ただしユーザが指定した AM からの要求であっても，自身が払いだした RT かどうかを確認を行い，不正な RT を許可することを防ぐ．

§本人であること．

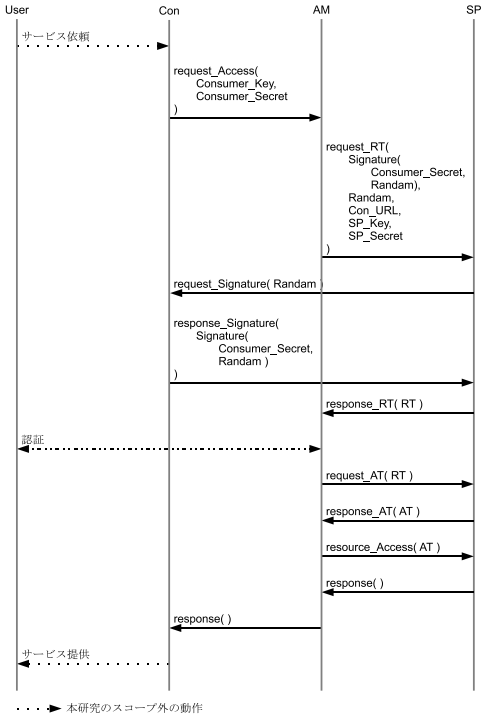

図 3: 認可フロー

2.3. ユーザのポリシー代弁機能

AM はユーザのポリシーを反映したルールに基づき認可の判断をおこなう．AM はユーザのログイン状態と RT の内容を確認し，許可を出す．そのため，ユーザにはどの RT を許可するかを，AM に事前に設定してもらう．このとき，必要であれば AM はユーザのログイン状態を確認するために認証を行う．

3. おわりに

本研究では，ユーザ主導のアクセス制御を行う認可プロトコルを提案した．OAuth をユーザ主導で信頼関係構築を行えるように拡張することで，ユーザが望むサービスの間でリソースのアクセス権限を融通することが可能となった．また，認可の判断をユーザの代わりに行う AM を導入し，これを信頼の置ける第三者として信頼関係構築の仲介役とした．こうしてユーザのポリシーと，SP と Con の信頼関係を AM で集中管理し，アクセス制御を管理しやすい構造をとった．

参考文献

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

[2] The OAuth 2.0 Protocol
http://tools.ietf.org/html/draft-ietf-oauth-v2

[3] Security Assertion Markup Langage SAML
OASIS Security Services (SAML) TC
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[4] Kerberos The Network Authentication Protocol
http://web.mit.edu/Kerberos/