Webアプリケーションにおける ユーザ間でのアクセス権限委譲に関する考察

関口 聖美† 笠原 卓也†† 黒羽 秀一† 齋藤 孝道††
†明治大学大学院 ††明治大学

1 はじめに

従来のアクセス制御方式として，管理者による強制アクセス制御方式では，権限のユーザへの割り当てを変更する際には，管理者の権限を必要とする．しかし，管理者の仲介なしで，ユーザ間で権限の割り当ての変更や委譲を行いたいケースもある．

そこで本論文では，Webアプリケーションにおけるアクセス制御の課題について検討し，この課題を解決することが可能なアクセス制御方式の提案を行う．提案方式を用いることにより，権限の委譲や割り当ての度に管理者の手続きを介さなくても，ユーザは他者に権限を委譲することが可能となる．

2 Webアプリケーションにおけるアクセス制御の問題点と必要な要件

Webアプリケーションのアクセス制御を行う場合，権限管理者が所有している権限は，自らがリソースにアクセスするための権限の他に，他者 (一般ユーザ) にアクセス権限を委譲するための権限 (以降，権限委譲のための権限と呼ぶ) がある．しかし，この権限を所有しているのは，強制アクセス制御方式の場合は，管理者のみであり，任意アクセス制御方式では，そのリソースの所有者のみである．Webアプリケーションのアクセス制御を実現するためには，権限委譲のための権限を，許可されたユーザが所有する必要がある．

3 提案方式

3.1 概要

ユーザ間でのアクセス権限の委譲を可能にするため，提案方式は「Ticket (チケット)」を利用する．サービスの提供を受けるユーザは，Ticketを持っており，ユーザは，Ticketをサーバに提出することでサービスを提供される．Ticketは，ユーザ，つまり，Ticketの所有者に割り当てられるべきアクセス権限やTicketの発行者・所有者を特定する情報，有効期限などが記載されているデータである．Ticket発行者 (ユーザ) がTicketを生成し，これを他者に委譲することで，ユーザ間でのアクセス権限の分割・委譲を実現する．Ticketの詳細については，3.3副節で述べる．

アクセス権限を分割し，委譲を行う際，Ticket発行者 (ユーザ) は自身に割り当てられている権限の範囲内で，権限の委譲を行う．例えば，Ticket発行者 (ユーザ) が権限AとBを所持している．権限AとBが，それ以上分割することができない最小権限だった場合，他者に委譲できる権限は，権限AまたはBのどちらかになる．また，権限を委譲すると，Ticket発行者 (ユーザ) の権限は，発行前に割り当てられていた権限より縮小される．例えば，権限AとBを割り当てられているTicket発行者 (ユーザ) が，権限Aを他者に委譲すると，Ticket発行者 (ユーザ) が持つ権限は，権限Bのみということになる．このようにして，ユーザ間でのアクセス権限の分割や委譲を行う．

3.2 提案方式の構成と前提

提案方式は，Server (サーバ)，Issuing Agent (Ticket発行者)，Client (クライアント)，Repository (リポジトリ) の4つの主体から構成される．ServerとIA，Clientは，各々公開鍵と秘密鍵を保持しており，各々の秘密鍵は各主体のみが保持しており，保持する公開鍵と秘密鍵は真正であると仮定する．以下に各主体の役割について説明し，図1に主体構成を示す：

Server：Clientから Ticketの提出を受け，サービスを提供する主体である．本論文では，サービスの種類として，Apache [1] やIIS [2] のようなWebサーバを用いて，ファイル共有等を提供するサービスを想定する．また，サーバリソースのアクセス権限をClientに委譲できる権限を，Issuing Agentに委任する機能も持つ (図1中の (1))．

Issuing Agent：Clientにアクセス権限の割り当てをする主体，つまりClientにTicketを発行する (図1中の (2)) 主体である．以降，IAと表記する．

Client：サービスの提供を受ける主体である．IAからTicketを受け取り，そのTicketをServerに提出することでサービスを利用する (図1中の (3)(5))．また，他のClientにアクセス権限の委譲を行う (図1中の (4)) 主体でもある．本論文では，他のClientに権限の委譲を行うClientを「C1 (Client1)」と表記し，Client1から権限を委譲されるClientを「C2 (Client2)」と表記する．

Repository：C1からC2にTicketが委譲されたときに，権限の委譲情報 (誰がどの権限を委譲したか) が登録される (図1中の (6)) 主体である．

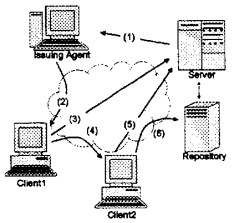

図1: 提案方式における主体構成

各主体は悪意あるものに侵入されたりせず，常に正しく機能するものと仮定する．主体間の信頼関係として，ServerとIA，IAとC1，C1とC2，ServerとRepository間は，お互い信頼する関係にある．つま

† Kiyomi SEKIGUCHI, Shuichi KUROBA
†† Takuya KASAHARA, Takamichi SAITO
Graduate School of Meiji University (†)
Meiji University (††)

り，お互いの正しい公開鍵を所持，もしくは，取得することができる関係にあると仮定する．また，Client は Server を信頼するが，逆はないと仮定する．

3.3 Ticket の様式

提案方式の Ticket は，SPKI (Simple Public Key Infrastructure) における権限証明書 [3] (以降，SPKI 権限証明書と呼ぶ) として，作成される．SPKI 権限証明書の定義を簡潔に述べる．

Ticket は，以下の 5 つの項目により構成され，それを発行者 I の秘密鍵 $S(I)$* によって電子署名したものである．

$\langle I, S, D, A, V \rangle_{S(I)}$

ここで，各シンボルは以下の通り表される：

Issuer I：Ticket を発行した主体の公開鍵，もしくは，その主体自体を示すシンボル．本論文では，発行者の公開鍵とする．

Subject S：Ticket が委譲される主体の公開鍵，もしくは，その主体自体を示すシンボル．本論文では，権限を委譲された主体の公開鍵とする．

Delegation D：Ticket で指定される権限が他者に委譲可能であるかどうかを指定する．その真偽はブール値，すなわち 1 または 0 によって表される．

Authorization A：Ticket によって行使できる権限を記述する．権限の記述方法は，サービスの種類により変化するので，本論文では明記しない．

Validity V：Ticket の使用期限を記述する．提案方式では，Ticket の使用開始日と終了日の日付を与える．Ticket の利用日がこの項目に記されている日付の期間内であれば，その証明書は有効であると解釈する．

権限を委譲するときは，Ticket を所有しているユーザが，新たな Ticket を生成する．そして，自らが所有している Ticket と共に，新たな Ticket を渡す．

3.4 提案方式の処理の流れ

図 2 を用いて，具体的な処理の流れを説明する．以下に示す Step が，図中のそれと対応している:

Step0 : Server から IA への発行権限の委任

Server は IA に，「Client に権限委譲のための権限 *Auth0*」を Ticket0 (以降，T0 と表記する) を用いて委譲する．

Step1 : IA から C1 への権限委譲

C1 は，Server において権限を行使するために，IA からアクセス権限の委譲を以下の通りに受ける：

(1) C1 はアクセス権限の委譲を受けるため，IA にアクセスし，認証を行う．
(2) 認証が成功した場合，C1 は安全な通信路を用いて，C1 の公開鍵 *P(C1)* を IA に送信する．
(3) IA は，C1 に割り当てるべき権限 *Auth1* と C1 が更なる委譲可能かを表すブール値 D_1 を決定し，Ticket1 (以降，T1 と表記する) を作成する．
(4) IA は，T0 と T1 を C1 に送信する．

Step2 : Client 間の権限委譲

C2 は Server において権限を行使するために，C1 からアクセス権限の委譲を以下の通りに受ける：

(1) C2 はアクセス権限の委譲を受けるため，C1 にアクセスし，認証を行う．
(2) 認証が成功した場合，C2 は安全な通信路を用いて，C2 の公開鍵 *P(C2)* を C1 に送信する．
(3) C1 は，C2 に割り当てる権限 *Auth2* を決定し，Ticket2 (以降，T2 と表記する) を作成する．
(4) C1 は，T0，T1，T2 を C2 に送信する．
(5) C2 は，Repository に委譲情報を登録するため，受信した Ticket 全てを Repository に送信する．
(6) C2 から，Ticket を受信した Repository は，T1 と権限 *Auth2* を取り出し，保存する．C2 に登録完了の ACK (ACKnowledgement) を返す．
(7) ACK を受け取った C2 は，権限委譲が完了した旨を報告するため，C1 に ACK を返す．

Step3 : 権限行使

Client による権限の行使について説明する．ここでは，C2 が Server に権限を行使する場合を取り上げる：

(1) C2 は権限 *Auth2* を行使するために，安全な通信路を用いて，T0，T1，T2 を Server に送信する．
(2) Server は，提出された Ticket が正当なものかを検証する．具体的には，電子署名，Delegation 項目，Authorization 項目，Validity 項目の検証がある．
(3) その Ticket を用いて行使しようとしている権限が，既に他者に委譲されていないか確認するため，Server は Repository に問い合わせる．
(4) Repository は検索結果を Server に返す．この時送信されるものは，Ticket とその Ticket に記されている権限から委譲された権限のセットである．
(5) Server は，Repository からの Ticket と権限のセットを受け取り，これと，C2 から送信された Ticket を元にして，サービスを提供する．ただし，Server から C2 に渡されるデータは，C2 の公開鍵で暗号化されているので，安全な通信が可能である．

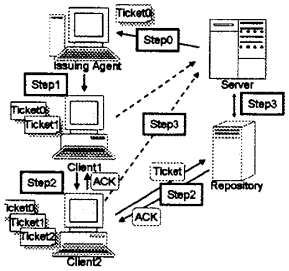

図 2: 提案方式の概要図

4 まとめ

本論文では，管理者の仲介なしで，ユーザ同士でアクセス権限を分割・委譲が可能なアクセス制御方式を示した．

参考文献

[1] The Apache Software Fundation, http://www.apache.org/
[2] Internet Information Service, Microsoft http://www.microsoft.com/
[3] C.Ellison, SPKI Requirements, RFC2692, 1999.

* 主体 I の秘密鍵を $S(I)$，公開鍵を $P(I)$ と表記する