2S-04 X.509証明書とSSLを用いた簡潔な匿名アクセス制御方式

梅澤 健太郎　齋藤 孝道　奥乃 博
東京理科大学 理工学部 情報科学科

現在, EC市場やオンライン株取引等においてSSL (Secure Sockets Layer) とX.509証明書を組み合わせてセキュアチャネルの確立及びクライアント認証によるアクセス制御を行う方式が一般に利用されている. 本論文では, SSL及びX.509証明書を利用して現行方式よりも簡潔な匿名アクセス制御を行う方法を提案し, 匿名性に関する議論及び他方式との比較を行う.

1. はじめに

これまで我々は権限証明書☆を用いた簡潔な匿名アクセス制御に関して研究を行ってきた[1)2)3)]. そのアイデアは, 「証明書の発行主体」と「権限の行使先 (サーバ)」を分離することで, 権限証明書の利点である簡潔なアクセス制御に, 匿名性を付加することにある. 実装では, 権限証明書による簡潔なアクセス制御を目的とするPKI (公開鍵基盤) の一つであるSPKI[4)]を利用してきた. しかしSPKIは, 普及度においてPKIX (PKI with X.509) に劣る. 本論文では, 既存のPKIX上で権限証明書によるアクセス制御を実現することを目的として, X.509証明書を権限証明書として利用するWebでのアクセス制御を検討する. この際, セキュアチャネル☆☆の確保にはSSL相互認証モードを利用した. 本論文では, 権限証明書の匿名性に関する議論及びその他のアクセス制御方式との比較など設計段階の考察を記述し, PKIX上で権限証明書を利用する匿名アクセス制御方式の実装について述べる.

2. 設　計

以下の図中の記号は, 図1と対応する.

2.1 権限証明書におけるIDと匿名性

本稿におけるサーバSに対するクライアントの匿名性は, 認証局CAとSを分離した状況において, Sが「公開鍵」と「実世界での本人」の対応を知りえないことから保証される. 我々は「ID」を識別子となり得る全ての情報を指すとの立場を取るので, X.500名前, SDSI名前, 公開鍵などはIDとなる. 本論文で規定する匿名性は, **IDと実世界での本人の対応を秘匿した状況**を指し, **IDを秘匿した状況**を指すものではない. その為, 複数の証明書に含まれる同一のIDをキーとした情報の統合を防ぐ[5)]ためには, **権限毎に異なった公開鍵を使う**, 崔らの方式[6)]のように**グループ署名を取り入れる (グループのIDは特定出来るが, 個人のIDは秘匿される)** などの対策を取る必要がある.

2.2 権限証明書によるアクセス制御の設計

証明書を用いたオフラインのアクセス制御は, 名前証明書☆☆☆を利用する**名前証明書+属性情報方式**と, 権限証明書を利用する**権限証明書方式**に大別される.

(1) **名前証明書+属性情報方式：** **(公開鍵⇒名前⇒権限)** という対応関係を利用してアクセス制御を行う. **X.509属性証明書**[7)]**とX.509名前証明書**の組を利用する方式や, RSA社の提唱するPKCS#6[8)]等がある. これらの方式は, 公開鍵と名前の対応と, 名前と権限の対応によりアクセス制御を行う.

(2) **権限証明書方式：** **(公開鍵⇒権限)** という対応関係を利用してアクセス制御を行う. 権限と公開鍵の対応を権限証明書という形でクライアントが保持する. SPKI権限証明書, 今回利用したX.509V3証明書の形態がある. 公開鍵と権限の対応によりアクセス制御を行う.

2.3 両方式のトレードオフ

権限証明書方式 (以下 (2) 方式) と「名前証明書+属性情報」方式 (以下 (1) 方式) の比較を表1にしめす.

表1 アクセス制御方式の比較

	(1) 方式	(2) 方式
公開鍵失効によるアクセス制御への影響	少	多
権限決定に要する処理量 (比較)	多	少

- 複数の権限に関連付けられた公開鍵が失効した場合, (1) 方式は名前証明書の再発行のみでよいのに対して, (2) 方式は全ての証明書の再発行が必要である
- 権限決定において, (1) 方式は公開鍵と名前, 名前と権限の対応を検証することが必要なのに対して, (2) 方式は公開鍵と権限の対応のみを検証すればよい

ことを判断基準とする. 表1から分かるように, どちらの方式を選ぶかは状況に大きく依存する.

IDをキーとした多様な情報の統合を防ぎ、匿名性を確保するためには, (2) 方式の適用が望ましい. というのは, 公開

Simple Access Control with X.509 and SSL
by Kentaro Umesawa, Takamichi Saito, Hiroshi G. Okuno
Dept. of Information Sciences, Science University of Tokyo
2461 Yamazaki, Noda, Chiba 274-8510

☆ 本稿では権限と公開鍵の対応を保証する証明書を指す
☆☆ 本稿では機密性・完全性の確保された通信路を指す
☆☆☆ 本稿では識別名と公開鍵の対応を保証する証明書を指す.

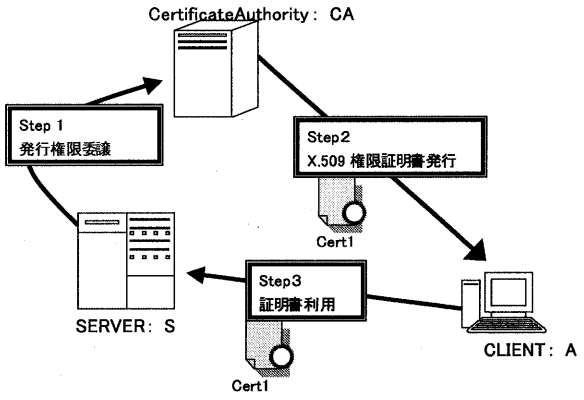

図 1　処理における相関関係

鍵失効によるアクセス制御への影響が少ないという (1) 方式の利点が活用できないからである.

すなわち, (1) 方式は名前証明書をキーとした情報の統合を防ぐために, 名前証明書を権限毎に異なったものにする必要が生じ, その結果, 一つの公開鍵に複数の権限が関連付けられることがないからである.

3. SSL と X.509 証明書によるアクセス制御

この章では, 提案方式の理論的背景・処理概要を実装したシステムを例に説明する.

3.1 X.509 証明書と SSL[9)]

本稿では, X.509 証明書を権限証明書として利用する. X.509v3 拡張フィールドに権限情報を入れ, Subject フィールド (主体の名前) に発行主体にとってのみ意味を持つ識別子を入れる. これで, 発行主体以外に対する匿名性を備える権限証明書として利用することが出来る.

提案方式では SSL 相互認証モードを利用する. その際, クライアントは, 上記の権限情報を含む X.509 証明書をサーバに提出する.

3.2 処 理 概 要

提案方式の概要を図 1 に示す. 以下で用いる記号は, 図 1 と対応する. CA と S の結託がない状況では $CLIENT$ は S に対して匿名での権限行使が可能である. CA と S が同一主体の場合, このモデルは匿名性をもたない権限証明書によるアクセス制御を表す. この場合, **Step1** は不要となる.

3.2.1 処理の流れ

[Step1] : 発行権限の委譲

S は CA に対して, 権限の記述様式及びポリシーを与える. 本稿では例として, 「同一研究室の大学院生は情報を完全に閲覧する権利を持ち, 同一研究室の学部生は情報の一部を閲覧する権利を持つ. その他の主体は情報が閲覧できない」という単純なポリシーを定めた.

[Step2] : X.509 権限証明書発行

CA は $CLIENT$ に対して認証を行った後, X.509 証明書の発行を行う. その際, X.509 証明書拡張フィールドに入れる権限を確定する. 発行形態はオフラインとし, PKCS#12 形式の証明書 $Cert_1$ を FD に入れ, それを $CLIENT$ に渡す.

[Step3] : 証明書利用

$CLIENT$ は, $Cert_1$ を Web ブラウザにインポートし, S にアクセスする. SSL セッション確立時に S は, $CLIENT$ が提出した証明書の署名検証, 拡張フィールドの権限情報の解釈を行い, $CLIENT$ のアクセス制御を行う.

3.3 実　　装

実装は, **JDK1.2, IAIK2.51[10)], iSaSiLk3.01[10)]** を用いており, その詳細は, http://csai03.is.noda.sut.ac.jp/SACS/ にあるので参照していただきたい.

3.4 権限の記述様式

今回の実装では権限をポリシー (3.2.1 の Step1 で示したもの) に対応する 3 つのタイプ (大学院生, 学生, その他) に分け, それぞれのタイプに応じて閲覧できる URL のリストを作成した. サーバは起動時にその URL リストを読み込む. そしてクライアントの要求した URL が, クライアントの権限タイプで閲覧可能かどうかの判定を行う. この方法では, 従来のように各 URL 毎にパスワードなどでアクセス制御を行う必要はない. さらに, 権限 (閲覧できる URL) 変更は, URL リストを変更すればよく証明書破棄は必要ない.

また今回, 権限証明書に閲覧できる URL を直接記述する実装も行ったが, 実装のテスト運用において破棄される証明書が急増した. その理由は, 権限 (URL) 変更が証明書破棄と対応するためであった.

4. ま と め

本稿では, X.509V3 証明書を権限証明書として利用する匿名アクセス制御を提案した. さらに, ID による情報の統合を防いで匿名性の保証するためには, 権限証明書を利用したアクセス制御が望ましいことを述べた. 今後の課題は, 実際の大規模な運営での定量的な評価, 実装システムの公開にむけたプログラムの洗練化である.

参 考 文 献

1) 梅澤, 齋藤, 奥乃: SPKI (Simple Public Key Infrastructure) によるプライバシー重視の権限管理の提案と Java を用いた実装, 情処全大 60 回, 3Q-03, 2000.
2) 梅澤, 齋藤, 奥乃: SPKI によるプライバシー重視機能の提案とその株主優待券の電子的発行への応用, 情報処理学会セキュリティ研究会, Jul. 2000.
3) Saito, Umesawa, Okuno: Privacy Enhanced Access Control by SPKI, Proc. of NGITA00, 301–306, 2000.
4) C. Ellison, *et al.*: SPKI Certificate Theory, RFC2693, Sep 1999.
5) Stefan A. Brands: Rethinking Public Key Infrastructures and Digital Certificates, The MIT Press, 2000.
6) 崔, 菊地, 中西: 効率的な匿名権限委託, CSS2000, 61–66, Oct. 2000.
7) S. Farrell, *et al.*: An Internet Attribute Certificate Profile for Authorization, RFC2026, July 2000.
8) RSA Laboratories. PKCS #6 : Extended-certificate syntax standard. Version 1.5, November 1993.
9) Alan O.Freier, *et al.*: The SSL Protocol Version 3.0, Nov 1996.
10) http://jcewww.iaik.tu-graz.ac.at