5W-1

属性証明書を用いた認可サービスシステムの構築

今川　俊明†　　柿崎　淑郎‡　　辻　秀一††

†東海大学大学院工学研究科　‡東海大学連合大学院理工学研究科　††東海大学情報理工学部

1　はじめに

インターネットが急速に普及したことにより，インターネットショッピングの利用や，企業間の取引などに活用されている．しかし，インターネットでは安全性や信頼性に対する不安が払拭されていない．さらに，電子商取引では個人を特定しなければならず，インターネットの特性である匿名性とは正反対の性質を持たなければならない．公開鍵基盤（PKI）は公開鍵暗号技術と電子署名を使って，本人性の証明を可能とする技術である．

しかし，実際の社会的・経済的活動，Web サービスなどにおいては，資格のような属性で認証や認可を行う事が多い．そこで，本人の属性を証明する属性証明書がある [1]．属性証明書については今まで提案はされているものの，実際に実装・利用・運用されているものはまだ少なく，有効性についての検討も十分に行なわれていない．そこで，本論文では，属性証明書を用いた認可サービスシステムを実装し，その有効性を検証する．

2　従来の方式

2.1　電子証明書

公開鍵証明書（PKC）は本人性を証明する証明書である．属性証明書（AC）は本人の属性を証明する証明書であり，証明書利用者のアクセス権限を証明する．属性証明書も公開鍵証明書と同様に，X.509 規定に準拠しており，アクセス制限を行うために必要な個人の属性情報（所属，部署，役職など）を含んでいる．属性証明書には証明書利用者の本人性を証明する情報が明示されていないため，公開鍵証明書に関連付ける形で用いられる．

2.2　属性認証方式

属性情報を使った認証方式は，公開鍵証明書に属性情報を書いて権限を証明する方式や，属性情報はシステム内部のデータベースで保持し，本人認証の結果と結びつける方式，属性情報を管理するのは信頼ある機関で行い，そこに属性情報を問い合わせる方式などがある．しかし，属性情報を記載する適当なスペースがないことや，情報漏洩などの問題点があった．そこで，属性証明書を使った認証方式が提案されている [2,3].

3　実装方式

RFC3281 の基本的な push 型モデルに基づき，その実現可能性と有効性を示すために実装する．

3.1　基本方式

属性情報を用いてのアクセスコントロールを，属性証明書を使用して行なう．以下に属性認証局 (AA)，登録局 (RA)，サービスを行なうサービスサーバ，属性証明書発行モデルとしての認証局 (CA) の基本となる方式の構成と機能を示す．

3.2　構成と機能

基本方式の構成を図 1 に示す．属性証明書には証明書利用者の本人性を証明する情報が明示されていないため，公開鍵証明書のを利用する．

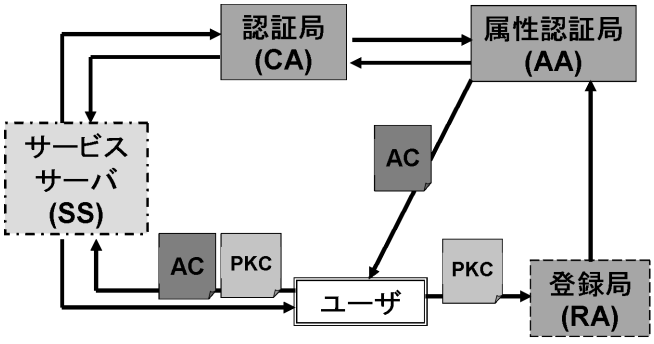

図 1: 基本方式の構成図

登録局 (RA)

登録局では，まずユーザが属性情報を登録する．その時に，ユーザの公開鍵証明書を受け取り，認証局が発行している失効リストで，提示された公開鍵証明書が，失効していないことを確認する．また，ユーザが公開鍵証明書に対応する私有鍵を保持しているかチェックする．登録された属性情報を属性情報データベースに格納する．次に，属性認証局へ属性証明書の発行を要求する．

属性認証局 (AA)

属性認証局は，まず登録局から属性証明書の発行要求を受ける．登録局から受け取った属性情報に基づき属

A Construction of Authorization Service System that Uses Attribute Certificate

†Toshiaki IMAGAWA　‡Yoshio KAKIZAKI　††Hidekazu TSUJI

†Graduate School of Engineering, Tokai University

‡Graduate School of Science and Technology, Tokai University Unified Graduate School

††School of Information Science and Technology, Tokai University

性証明書を作成する．その属性証明書をユーザに送る．

サービスサーバ

サービスサーバは，ユーザからサービスの要求を受ける．そのときに，公開鍵証明書と属性証明書を受け取る．認証局が発行している失効リストで，提示された公開鍵証明書が，失効していないことを確認する．また，ユーザが公開鍵証明書に対応する私有鍵を保持しているかチェックする．確認することができたら，その属性情報に応じたサービスをて提供する．

3.3 ソフトウェア構成

実装環境として OS は WindowsXP を用いた．開発言語は Java を，HTTP サーバは Apache を用いた．

属性認証局 (AA)

属性認証局の機能を実装するためのクラスは，TS_AA クラス・time クラス・DigestImpl クラス・KeyPairGene クラス・rsaEn クラスの 5 つである．

TS_AA クラスでは，まず属性証明書を出力するときに保存するディレクトリを作成する．次に，属性証明書のフォーマットを読み込み，属性情報を追加して属性証明書を作成する．最後に属性証明書を出力する．作成した属性証明書をリポジトリに保存する．

time クラスでは，TS_AA クラスで属性証明書を作成するにあたって，属性証明書の発行日と有効期限の記述のために，現在の時間を取得する．そして，戻り値として現在の時間を TS_AA クラスに返す．

DigestImpl クラスでは，TS_AA クラスで属性情報を追加していった属性証明書の acinfo フィールドのハッシュ値を計算し，メッセージダイジェストを作成する．ハッシュ値を TS_AA クラスに返す．

KeyPairGene クラスでは，rsaEn クラスで使用する秘密鍵と検証者に公開する公開鍵を作成し，ファイルに書き出す．

rsaEn クラスでは，DigestImpl クラスによって計算されたハッシュ値を RSA 方式により KeyPairGene クラスによって作成された秘密鍵で暗号化し，その値を TS_AA クラスに返す．

認証局 (CA)

OpenSSL を用い，公開鍵証明書と失効リストを発行する．

4 適用例

一例として，観光地のホームページを属性情報によってアクセスコントロールするサービスを提案する．

ホームページにアクセスする時に，住所属性と年齢属性でアクセスコントロールする．住所属性によって市民なのか，観光客なのかを判断し，市民であれば，観光情報・選挙情報・市民が利用できる施設の情報や申請書類についてなどくらしに関する情報の表示の優先度が同じである．観光客であれば，観光情報の表示の優先度は高く，観光客に関係が浅い選挙情報や，くらしに関する情報は表示の優先度を低くする．年齢属性によって成年か未成年か 60 歳以上かを判断し，成年であれば，居酒屋の情報・選挙情報にアクセスできるが，未成年であれば，居酒屋の情報にはアクセスすることが出来ず，選挙情報の表示の優先度を低くする．さらに，65 歳以上であれば，ユーザインターフェースが高齢者に適した形で表示される．属性証明書を持っていない人のアクセスは，一般的な観光案内や店舗情報のみ許可される．

表 1: 属性によるアクセスコントロール

住所属性

	観光情報	選挙情報	くらしの情報
市民	○	○	○
観光客	○	×	×

年齢属性

	居酒屋情報	選挙情報
成年	○	○
未成年	×	×

5 おわりに

属性証明書は RFC3281 によって策定され，その後も属性証明書を利用した認証方式の提案がされている．しかし，実際に実装・利用・運用されているものはまだ少なく，有効性についての検討も十分に行なわれていない．属性証明書を発行し，適用例に当てはめて運用できるように実装を行うことで属性証明書を利用した認証方式の有効性を示した．

参考文献

[1] S. Farrell and R. Housley. *An Internet Attribute Certificate Profile for Authorization*, 2002. RFC3281.

[2] 前田陽二, 川松和成. 属性認証ハンドブック, 2005.

[3] 柿崎淑郎, 辻秀一. 属性証明書を用いた認証方式の提案. 情報処理学会コンピュータセキュリティ研究会報告, 2004. 2004-CSEC-27(2).

[4] 鈴木優一. 属性証明書（Attribute Certificate）. エントラストジャパン, 2002.

[5] 独立行政法人 情報処理推進機構 セキュリティセンター. PKI 関連技術解説, 2004. http://www.ipa.go.jp/security/pki/.