社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－CSEC－21 (5)
2003／5／15

認証・認可情報流通基盤について

小林 信博　　中川路 哲男

概要： 今後のユビキタスコンピューティング環境においては、異なる情報システムが相互に連携協調動作を行うことで、より高度なサービスが提供されると期待される。一方、サービス提供者に蓄積された利用履歴などのプライバシー情報が、ユーザの予期せぬ用途に再利用されるリスクが発生する。そこで本論文では、サービス提供者が、PKI を応用した認可に必要な条件として証明経路の上位に位置するトラストポイントをユーザに提示し、ユーザが認可情報をブラインド署名により認証サーバとしてのCA から入手することで、プライバシー情報の安全を確保しつつ認証・認可情報をシステム間で流通させる手法を提案する。

Information exchange infrastructure about authentication and authorization

Nobuhiro Kobayashi　Tetuo Nakakawaji

Outline: In future ubiquitous computing environment, different information systems will collaborate ,and will achieve more advanced services. But, it may have the risk. Privacy information such as a use history accumulated in the server may be used for the use which a user does not expect. Then, we propose the following systems. The server shows the user the trust point of the certificate path as authorization conditions that is required in PKI.. The user receives digital signature from one higher-level CA by blind signature method. Without showing privacy information, the user can exchange the information about authentication and authorization between systems.

1. はじめに

今日の情報システムにおいては、PKI 等の暗号技術を応用した認証と、その結果に基づいた認可によって、資源の保護や操作の実行等におけるセキュリティ機能を実現しているケースが多く見られる。一方、今後のユビキタスコンピューティング環境においては、異なる情報システムが相互に連携協調動作を行うことで、より高度なサービスが提供されるものと期待されている。

例えば、従来の PKI 応用システムでは、サービス提供者が、直接ユーザに対して信頼の証としてID となる証明書を割り当てていたものが、今後は、他のサービス提供者がユーザに対して与えた証明書を、自分のサービスを提供する際の信頼の基として共有することが考えられる。このようなサービスは、我々の実際の生活においてごく普通に利用されている。一例として、ある学会の会員は、特典として列車の運賃や宿泊費が割引になるというサービスが挙げられ、これが情報システムにおいても広く普及することで、個人の資格や嗜好に応じたパーソナライゼーションによる、ユーザの利便性が一層向上すると期待できる。

しかしその一方では、各サービス提供者によりデータベースへ蓄積された利用履歴などのプライバシーに関するデータが、サービス提供者間で相互に交換されることにより、ユーザの予期せ

三菱電機株式会社　情報技術総合研究所
Mitsubishi Electric Corporation Information Technology R&D Center

ぬ用途に再利用されてしまうのではないかとの不安要因になっている。従って、ユーザをこのような不安感や危険から解放する為に、セキュリティ技術を活用し、各種のリスクから利用者を確実に守り、適切な認証のもとで誰もが安心して利用できる環境の構築が、今後のユビキタスコンピューティング環境を社会に広く普及させる上で重要であると考えられる。

2. 関連技術

異なる情報システムが相互に連携協調動作を行う際の、認証認可に利用可能な技術について以下に示す。

2.1. 属性証明書

ID とは対象者を識別（認証）するためのユニークな情報であり、属性とは対象者に与えられた資格や権限（認可）を表す情報である。しかし、ID と比較すると属性は短い周期で変更されることが予想される。これは、企業において証明書を発行する場合に、社員としてのアイデンティティは変わらず、所属する部署や役職が変化するという状況に相当する。従って、ID と属性を一つの証明書として取り扱うことは、属性の変更が証明書の失効を伴うこととなり、証明書の再発行などの運用コストが増すという問題を生じる。また、証明書の発行者と、属性の認可者は、異なることが考えらる。その場合、属性の変更が生じる度に両者の連携作業をとらねばならないという問題も発生する。そこで、これらの問題を解決する技術の一つとして、属性証明書が挙げられる。これを利用する場合、主に証明書所有者の認証目的に利用する公開鍵証明書と、証明書所有者の認可目的に利用する属性証明書とを併用する。属性証明書は公開鍵証明書に似た構造をしているが、サブジェクトの公開鍵の代わりにサブジェクトの公開鍵のへの関連付けが holder 情報として設定されている。また、属性証明書には、証明書所有者の資格や権限などの属性情報が含まれ、公開鍵証明書における証明書発行機関(CA:Certificate Authority)に相当する属性証明書発行機関(AA:Attribute Certificate Authority)からデジタル署名を付加して発行される。従って、属性証明書は証明書所有者の情報と容易に関連付けることが可能である。

2.2. SAML

SAML(Secure Assertion Markup Language)は、WEB サービスで利用されるセキュリティ技術であり、OASIS(Organization for the Advancement of Structured Information Standars)により策定された。これは、セキュリティ情報を交換するための、XML ベースのフレームワークであり、認証情報を複数のサーバにて信頼するシングル・サイン・オンや、ユーザ情報を複数のサーバ間で交換する属性サービス(Attribute Service)等を実現する技術として利用可能であり、今後の WEB サービスにおけるセキュリティの中心的な役割を果たしていくと考えられる。この場合、ユーザの最初のログインにより認証情報を生成するサーバには、他のサーバからの信頼が集中することになる。従って、ユーザは TTP(Trusted Third Party)として認証情報を生成するサーバを利用することとなる。一方、このサーバの安全性が不正アクセス等により損なわれた場合や、サーバからの不正な情報持ち出しがなされた場合に、利用履歴ログなどのプライバシー情報流出の被害が広範囲に及ぶことが懸念される。また、WEB サービス自体が認証情報の再利用を前提とした

考え方であるため、各サーバの背信行為があった場合には、システム全体としての安全性が損なわれることになる。

3. 認証・認可情報流通基盤

3.1. 課題

認証・認可情報を複数の情報システム間で流通させる基盤に対する要求は、今後ますます高まることが予想される。これに対して、有益な機能やセキュリティ機能を備えた方式もしくはシステムが提案されているものの、ユーザのプライバシーについて考えた場合に、個人の行動を特定する情報の流出が懸念される。そこで、本論文では、個人の行動を特定する情報を示すことなく、システム間で認証認可情報をやりとりする手法について提案する。

3.2. 提案方式

ユーザのプライバシー保護を考えた場合、既に発信（流出）した情報に対する制御を行うことは難しいと考えられる。そこで、本提案では、ユーザを認証するサーバ（認証サーバ）及び、認可するサーバ（認可サーバ）に対して、個人の行動を特定するプライバシー情報の流出を制限する手法を考える。具体的には、認証サーバに対して、認可との関連性を排除し、認可サーバに対して、認証との関連性を排除する。図１に本提案の概略図を示す。また、以下に説明を述べる。

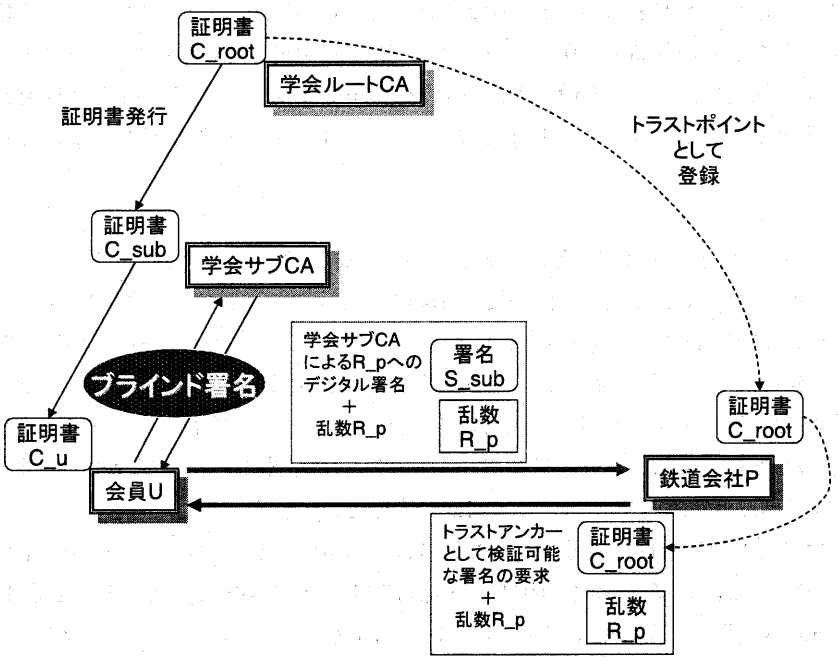

図 1　認証認可情報流通基盤概略

まず、ユーザUをある学会の会員とし、ある鉄道会社Pが、この学会の会員Uに対して運賃の割引サービスを行っている認可サーバであることを想定する。ここで会員Uは、学会の発行した会員証を持つものとする。この場合の信頼モデルは、学会ルート CA:CA_root→学会サブCA:CA_sub→会員:Uとなる。なお、ここでは説明の便宜上、サブCAは1つとしてあり、このサブCAを認証サーバとする。

次に、本提案における処理手順について述べる。

(1) まず、事前準備として、学会サブCA:CA_subはユーザUの会員証としての公開鍵証明書C_uを発行し、これを配布しておく。また学会は、学会ルートCAの証明書C_rootを、運賃の割引サービスを行っている認可サーバとしての鉄道会社Pへ渡しておく。

(2) 次に、運用段階として会員Uが鉄道会社Pからチケットを購入する。
会員Uが鉄道会社Pに対して、割引サービスでのチケット購入を要求する。この際、鉄道会社Pがチケットの割引を判断する為に必要な情報は、会員Uのプライバシー情報を含む学会の会員証すなわち公開鍵証明書 C_u ではなく、学会の会員証をもっているという”申告(Claim)”の”表明(Assertion)”である。そこで、鉄道会社Pは会員Uに対して、学会の会員証を持っているという申告の表明を要求する。この要求には、学会の会員証をもっているという申告が保障される条件として、鉄道会社 P が信頼の基点（トラストアンカー）として利用する学会のルートCA : CA_rootの公開鍵証明書C_rootを含める。即ち、会員Uが鉄道会社Pの示した学会の公開鍵証明書C_rootにて有効性の検証可能なデジタル署名S_xを表明することで、鉄道会社に対する所有の証明(proof-of-possession)とする。また、鉄道会社Pはリプレイアタック防止の為に乱数R_pを生成し、これを保障される条件と共に会員Uに対して送る。

(3) 次に会員Uは、自分の保有する公開鍵証明書の内、認可サーバである鉄道会社Pから示されたトラストアンカーである公開鍵証明書C_rootにて証明書経路検証の可能な、学会の会員証に相当する公開鍵証明書 C_user を検索する。そして、認証サーバである学会のサブCA:CA_subに対して、鉄道会社Pから受け取った乱数R_pに対するブラインド署名の要求に、自分自身のデジタル署名S_uを付加して送る。ブラインド署名とは、署名者に署名対象となる情報を開示することなく、署名を付加してもらう技術である。ブラインド署名の具体的な方法として、今回はChaumによるRSA暗号を利用する。
ここで、サブCAの公開鍵証明書CA_subに含まれるRSA暗号の公開鍵を(e,n)、秘密鍵を(d)とする。また、会員Uの公開鍵証明書C_uに対応する秘密鍵をK_uとする。会員Uがサブ CA:CA_subへ送信するデータは以下のように算出する。
まず、秘密の乱数R_uを生成する。ブラインド署名の入力となるXは、以下の式で表される。

$$X = R\_p * R\_u \hat{} e \ mod \ n$$

また、デジタル署名 S_u は、以下の式で表される。

$$S\_u = Sign(X, K\_u)$$

次に、ブラインド署名のリクエストに X と S_u を含めてサブ CA:CA_sub へ送信する。

(4) 学会のサブ CA:CA_sub は、会員 U のデジタル署名 S_u を会員 U の公開鍵証明書 C_u にて以下の等式により確認する。

$$Verify(S\_u, C\_u) = X$$

次に、秘密鍵 K_sub とし、ブラインド署名 Y は、以下の式で表される。

$$Y = X^{K\_sub} \bmod n = R\_p \wedge K\_sub * R\_u \bmod N$$

ここで求められたブラインド署名 Y を、会員 U へ送りかえす。

(5) 会員 U は、ブラインド署名 Y を受け取り、ブラインド署名 Y と、乱数 R_u の逆数 R_u^-1 から、ブラインド署名を取り除いたサブ CA:CA_sub のデジタル署名 S_sub を以下の式にて求める。

$$S\_sub = Y * R\_u^{(-1)} = R\_p \wedge K\_sub \bmod N$$

そして、会員 U は、学会のサブ CA のデジタル署名 S_sub と、鉄道会社 P から受け取った乱数 R_p を鉄道会社 P に申告の表明の証明として送り返す。

(6) 鉄道会社 P は、受け取った乱数 R_p が会員 U に送ったものと等しいことを確認し、デジタル署名 S_sub を以下の等式により確認する。

$$Verity(S\_sub, C\_sub) = R\_p$$

更に、C_root をトラストアンカーとして C_sub の証明経路検証を行う。
全ての検証が成功した場合、会員 U が学会の会員証をもっているという申告は認可サーバである鉄道会社 P に受理され、割引サービスでのチケット販売が行われる。なお、チケット販売の代金に関しては、匿名性の確保された電子マネー等の方式により実現されるものとする。

4. おわりに

本稿における提案手法によれば、ユーザに対して認可サーバが、申告の表明の受理される条件として、信頼の基点（トラストアンカー）となる公開鍵証明書を示し、ユーザがこの公開鍵証明書にて証明経路検証の可能な認証サーバのデジタル署名を送り返す。これにより、ユーザは個人情報を示すことなく申告の表明の証明が可能である。また、認証サーバに対してブラインド署名を要求することで、認可サーバに関する情報を隠蔽することも可能である。

以上により、個人の行動を特定する情報を示すことなく、システム間で認証認可情報をやりとりすることが可能となった。

今後は、属性証明書を利用する場合や、その他のサービス形態への応用について更に検討を進める予定である。また、WEB サービスへの導入に関しても考えていきたい。

参考文献

[1] ユビキタス ネットワーキング フォーラム編, “ユビキタスネットワーク戦略　ユビキタスNW 技術の将来展望”, 株式会社クリエイト・クルーズ, 平成 14 年 12 月 20 日

[2]小松 文子, “PKI ハンドブック”, 株式会社ソフト・リサーチ・センター, 2000 年 11 月 25 日

[3] C.Adams, S.Lloyd, “PKI 公開鍵インフラストラクチャーの概念、標準、展開”, ピアソン・エデュケーション, 2000

[4]IETF, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC3280, 2002.4

[5]IETF, “An internet Attribute Certificate Profile for Authorization”, RFC3281, 2002.4

[6]OASIS, “Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) “, http://www.oasis-open.org/committees/security/docs/oasis-sstc-saml-sec-consider-1.0.pdf, OASIS Standard, 2002.11.5

[7] D. Chaum, "Blind Signatures for Untraceable Payments", Proceedings of Advances in Cryptology - CRYPTO '82, 1983

[8]Peter Wayner, 川副 博(監訳), “デジタルキャッシュ テクノロジー”, ソフトバンク株式会社, 1997 年 9 月 20 日