2004－CSEC－27　(2)
2004／12／20

属性証明書を用いた認証方式の提案

柿崎　淑郎 †　　辻　秀一 ‡

† 東海大学大学院　工学研究科
259-1292 平塚市北金目 1117 番地

‡ 東海大学　電子情報学部
259-1292 平塚市北金目 1117 番地
htsuji@keyaki.cc.u-tokai.ac.jp

あらまし 匿名性の高いネット社会において，認証は重要である．しかし，サービスによっては，利用者が正規利用者であるか，どのような権限を持っているかを確認できれば，厳密な本人認証を必要としないことが多い．本提案方式は，サービス利用時の権限証明手段として，属性証明書を用いることにより，サービスサーバに対するプライバシ保護された権限行使を PKI 上で実現する．

A Proposal of Authentication Method Using Attribute Certificate

Yoshio KAKIZAKI†　　Hidekazu TSUJI‡

†Graduate School of Engineering
Tokai University
1117 Kitakaname, Hiratsuka,
Kanagawa, 259-1292 Japan

‡School of Information Technology and Electronics
Tokai University
1117 Kitakaname, Hiratsuka,
Kanagawa, 259-1292 Japan
htsuji@keyaki.cc.u-tokai.ac.jp

Abstract In the net society, there is an anonymity by non-face-to-face. The authentication is important in the net society. However, in many service, if whether you are a regular user and what authority you have can be confirmed, a strict authentication is not necessary. Our proposal method achieves privacy protected authority exercise to the service server by using attribute certificate on PKI.

1　はじめに

情報化の普及に伴って，通信の安全性，認証，プライバシ，情報漏洩などが問題となっている．信頼される第三者と電子証明書で，電子署名や認証などを実現するためのインフラが PKI である．

公開鍵証明書は所有者の本人性を証明する証明書である．公開鍵証明書所有者の属性情報を証明する方法として，公開鍵証明書の拡張領域を用いる方法がある．しかし，属性情報は関連付けられる ID 情報と同じ寿命があるわけではないため，公開鍵証明書の拡張領域を利用するには問題がある．そのため，属性情報が変われば，公開鍵証明書の再発行が必要になる．属性証明書はこの問題を解決する．属性証明書は所有者の属性情報を証明する証明書である．たとえ属性の寿命が尽きたとしても，公開鍵証明書と属性証明書は異なる証明書であるために，公開鍵証明書の再発行は不必要である．

属性証明書は属性情報を証明するため，権限行使に用いることができる．本人性を公開鍵証明書で証明し，属性情報を属性証明書で証明する．RFC3281[1] は公開鍵証明書と属性証明書の関係を以下のように説明している．「公開鍵証明書はパスポートのようであり，属性証明書は入国ビザのようである」

本提案方式は，公開鍵証明書と属性証明書の

異なる二つの証明書を用いることで，新しいアクセス制御方式を提案する．これにより，公開鍵証明書によるセキュアな認証と属性証明書によるプライバシ保護された権限行使の両方を実現する．

2 関連研究

属性証明書は属性情報を証明する証明書である．属性証明書は，RFC3281[1] によって 2002 年４月に標準化提案された．ECOM は属性認証の適用ガイドラインとして，属性証明書を用いる技法，公開鍵証明書を用いる技法，属性認証サーバを用いる技法とを比較し，その結果として属性証明書を用いる技法を推奨している [2]. 今枝らは，属性証明書と公開鍵証明書とのリンクに関する課題とその対策案について述べている [3].

近年においては，証明書を用いた匿名性の研究が活発に行われている．斉藤らは，SPKI を用いたアクセス制御の提案 [4] を行っており，PKIX 上でその実装 [5] を行っている．斉藤らは，SPKI を利用して，認証と権限管理の分離という概念を導入して，プライバシを重視した安全なアクセス制御を実現している．佐藤らは，特殊な証明書を用いた匿名認証方式の提案を行っている [6].

3 提案方式

証明書を用いた匿名性の研究として，SPKI を用いた認証と権限行使を分離する研究 [4] があり，本研究では，SPKI よりも一般的に普及している PKIX で同等の機能を提供するために，属性証明書を用いた認証方式を提案する．

本提案方式は，ID 情報と属性情報を分離することで，セキュアな認証とプライバシ保護された権限行使の両方を実現する．また，本人確認（認証）情報，サービス利用（権限行使）情報のそれぞれを分散させることが出来る．これにより，サービス利用時のプライバシ保護が実現できるだけでなく，サービスサーバからの情報漏洩による ID 情報の流出も防ぐことが出来る．また，ID 情報には公開鍵証明書を，属性情報には属性証明書を利用することで，PKIX のインフラを最大限に利用した運用が可能である．

属性証明書は PKC リンカによって，対応する公開鍵証明書に紐付けられた状態で利用するのが，通常の利用方法である．しかし，PKC リンカによって，公開鍵証明書が参照可能であり，権限行使時のプライバシに問題がある．そこで本提案方式では，PKC リンカを設定せず，それに変わる認証のための情報を拡張領域に記録する．

属性証明書は，その属性情報が変化しない限り再利用可能であるが，証明書再利用によるサービス履歴からの追跡が可能であるので，１サービス１証明書での利用を採用する．その際，属性証明書の有効期限を短命に設定することで，属性証明書の失効手続きを不要とすることが出来る．

本提案方式の要点は，ID 情報と属性情報の分離，および認証と権限行使の分離によるプライバシ保護である．

3.1 電子証明書

本提案方式では二つの証明書の特徴を利用し，公開鍵証明書による本人認証と属性証明書による属性適用を行う．また，公開鍵証明書に ID 情報，属性証明書に属性情報を分離させることで，それぞれの個人情報を独立させる．

ここでは二つの証明書について説明する．

公開鍵証明書　公開鍵証明書（PKC）は証明書利用者の本人性を証明する証明書である．公開鍵証明書は正当性を保証できる第三者（認証局）によって，デジタル署名された公開鍵であることを示す．

属性証明書　属性証明書（AC）は証明書利用者のアクセス権限を証明する証明書である．属性証明書も公開鍵証明書と同様に，X.509 証明書フォーマットであるが，権限行使に必要な属性情報（名前，所属，役職など）を含んでいる．また逆に，公開鍵ペアを含まない．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，これら双方の証明書を関連付ける必要がある場合，属性証明書で参照されている公開鍵証明書も保有しなければならない．

比較　このように，公開鍵証明書と属性証明書ではその目的や運用形態が異なるため，公開鍵証明書発行機関（CA : Certificate Authority）と同様に，属性証明書発行機関（AA : Attribute Authority）が必要となってくる．公開鍵証明書と属性証明書の特徴を表 1 で比較した．

3.2　構成

本提案方式の構成を図 1 に示す．図 1 の構成は学内や社内などの中小規模を想定し，構成要素が内部組織で完結するものとしている．

図 1 中の集中 DB には，管理するユーザの情報が保存されている．IDDB は ID 情報が保存された集中 DB のサブセットであり，属性 DB は属性情報が保存された集中 DB のサブセットである．属性認証局は属性証明書を発行する機関であり，サービスサーバはサービスを提供する．

以下に示す要素は，本提案方式の主体的な構成要素である．

認証局　認証局は公開鍵証明書の発行とその失効リストの公開を行う．認証局は IDDB の情報を基に，公開鍵証明書の発行と失効を行う．発行された公開鍵証明書はリポジトリに格納される．失効が行われた場合，失効した証明書は失効リストに記載される．

属性認証局　属性認証局は属性証明書の発行を行う．属性認証局は属性 DB の情報を基に，属性証明書の発行を行う．属性証明書の発行には，ユーザの公開鍵証明書が有効であることを認証局のリポジトリと失効リストで検証することと，ユーザが公開鍵証明書に対応する私有鍵を持っているかの検証が必要である．検証結果に問題がなければ，属性 DB に基づく属性情報で属性証明書を発行する．

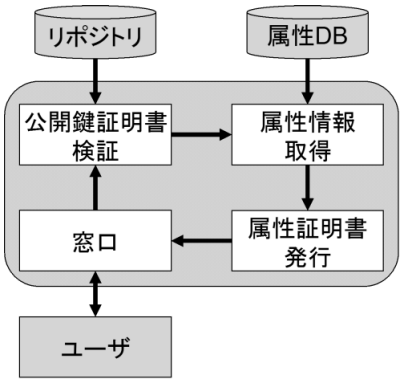

図 2: 属性認証局

登録局　登録局はユーザがサービスサーバを利用するための登録作業を行う．登録局はユーザからの利用申請を受けて，属性 DB に登録する．一度利用登録を行えば，公開鍵証明書の失効やユーザの失効などの理由で，サービスが利用できない状態にならない限り，再登録は不要である．また，サービスサーバの種類によって，集中 DB に登録されていない付加属性が必要であれば，審査を行い，属性 DB に付記する．

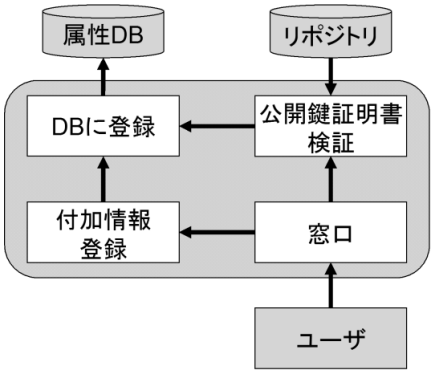

図 3: 登録局

サービスサーバ　サービスサーバはユーザに対するサービスの提供を行う．サービスサーバは属性証明書のディジタル署名を検証し，改ざんや捏造がないことを確認し，有効期限が切れていないことを確認する．また，属性証明書利用者が正規利用者かどうかを認証するために，属性証明書の拡張領域に記録されている認証値を用いて，ユーザ認証を行う．検証結果に問題がなければ，サービスの提供を行う．サービスにお

表 1: 公開鍵証明書と属性証明書の比較

	公開鍵証明書	属性証明書
目的	証明書利用者の本人性を証明	証明書利用者のアクセス権限を証明
証明書の拡張項目	利用者本人を特定できる情報	証明書利用者の属性情報
有効期間	長い	短い
証明書発行機関	認証局	属性認証局

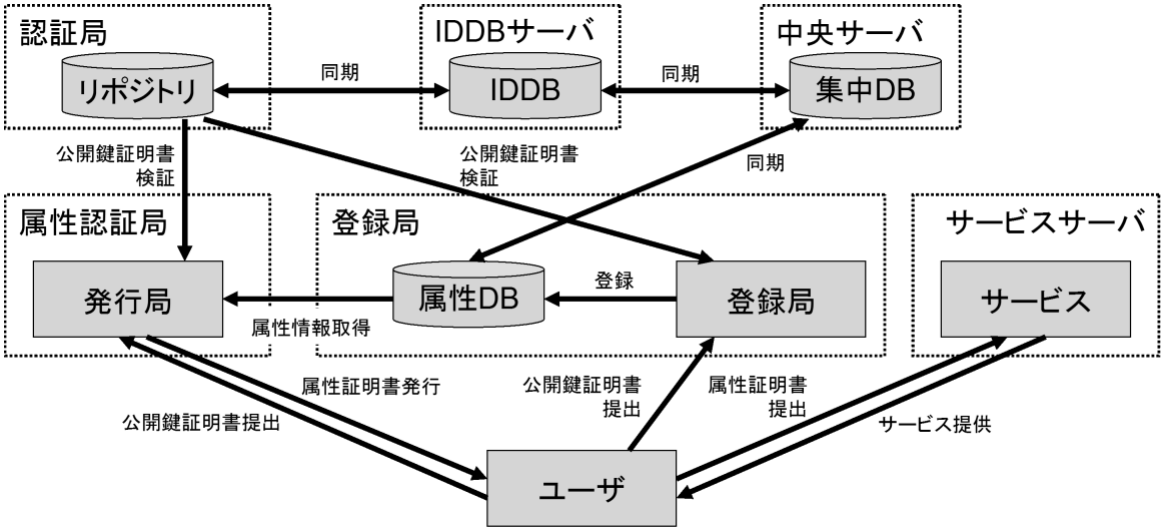

図 1: 提案方式の構成図

ける権限行使は属性証明書の属性情報に基づく．

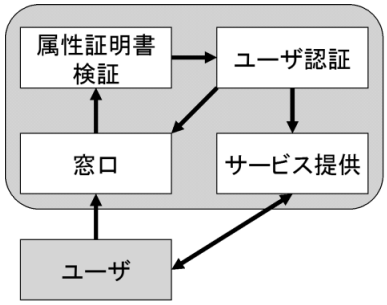

図 4: サービスサーバ

ユーザ　ユーザはサービスサーバからサービスを受けることができる組織の構成員として集中 DB に登録されている．集中 DB への登録時に，公開鍵証明書と対応する私有鍵の発行を受ける．

サービスサーバを利用するときは，まず登録局で利用登録を行う．一度利用登録を行えば，公開鍵証明書の失効やユーザの失効などの理由で，サービスが利用できない状態にならない限り，再登録は不要である．

サービスサーバを利用する場合，ユーザは属性認証局に属性証明書の発行を要求し，その属性証明書を用いて，サービスサーバのサービスを受ける．

3.3　サービス利用モデル

ユーザはサービスサーバのサービスを受けるために，以下の手順を行う．

3.3.1　サービスサーバの利用登録

実際にサービスを利用するためには，サービスサーバの利用登録が必要である．サービスサーバの利用登録は登録局が行う．ユーザは登録局へ公開鍵証明書を提出する．登録局はユーザの公開鍵証明書が有効であることを認証局のリポジトリと失効リストで検証する．また，ユー

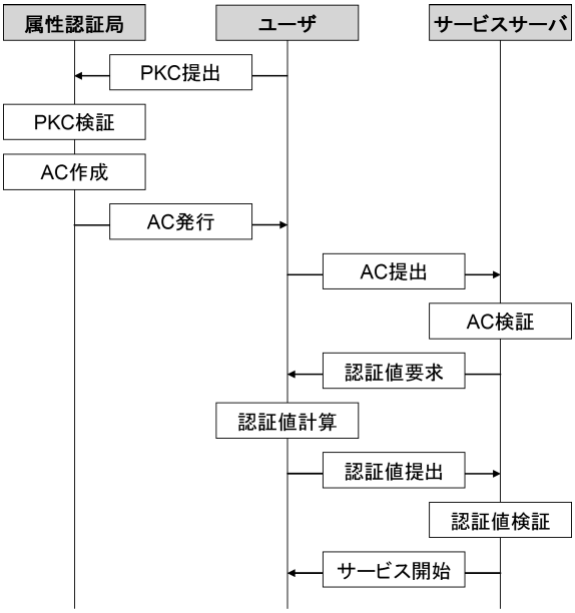

図 5: 提案方式のフロー図

ザが公開鍵証明書に対応する私有鍵を持っているかも検証する．もし，サービスサーバの種類によって，集中 DB に登録されていない付加属性が必要であれば，審査を行い，属性 DB に追加する．問題がなければ，サービスサーバの利用登録を完了する．

サービスサーバの利用登録が完了すれば，公開鍵証明書の失効やユーザの失効などの理由で，サービスが利用できない状態にならない限り，再登録は不要である．

3.3.2 属性証明書発行要求

ユーザはサービスサーバからサービスを受けるために，属性認証局から属性証明書の発行を受ける必要がある．

ユーザは属性認証局へ公開鍵証明書を提示し，属性証明書の発行を要求する．属性認証局はユーザの公開鍵証明書が有効であることを認証局のリポジトリと失効リストで検証する．また，ユーザが公開鍵証明書に対応する私有鍵を持っているかを検証する．問題がなければ，属性認証局は属性証明書の発行を行う．発行される属性証明書には，属性 DB の情報に基づく属性値（権限）が記載されている．また，サービスサーバが属性証明書の正規利用者かどうかを認証できるように，認証値を作成して，サービスサーバの公開鍵で暗号化したものと，ユーザの公開鍵で暗号化したものを，拡張領域に記録する．

属性認証局はユーザに属性証明書を安全に送付し，発行作業を完了する．

3.3.3 サービスサーバの利用

ユーザはサービスサーバからサービスを受けるために，属性証明書をサービスサーバに安全に提出する．

サービスサーバは属性証明書の有効期限を確認し，ディジタル署名を検証する．属性証明書利用者が正規利用者かどうかを認証するために，属性証明書の拡張領域に記録されている認証値を，サービスサーバの私有鍵で復号化して，Challenge & Response 方式等で認証を行う．この際，ユーザは属性証明書の拡張領域に記録されている認証値を，ユーザ（自分）の私有鍵で復号化して，サービスサーバからの認証に応じる．問題がなければ，属性証明書に記載された属性値に基づくサービスを提供する．

4 議論

4.1 利点

本提案方式は，ID 情報と属性情報を分離することで，サービスサーバに対するプライバシ保護された権限行使を実現した．これにより，正規利用者のみにサービスを提供したいが，プライバシに配慮して，サービス利用者個々の識別を必要としないサービスに対して有効である．

また，情報がネットワーク上で通信される場合，ID 情報と属性情報は同時に通信されない．ID 情報は個人を示すコア情報であり，属性情報は権限を示す情報だが，それぞれは個々別々では価値が無く，それぞれが組み合わさることにより，プライバシ情報となる．よって，本提案方式は通信路での盗聴やサーバからの情報漏洩によって，価値あるプライバシ情報の流失を防ぐことが可能である．

4.2 安全性

改ざんと捏造 属性証明書は X.509 証明書フォーマットであり，発行者の署名が行われている．署名の検証を行うことによって，改ざんと捏造の検出が可能である．この安全性は PKI の他の証明書と同等である．

再利用 属性証明書は一セッション一枚を前提に，証明書の寿命を非常に短く設定している．そのため，再利用の可能性は低く抑えられている．しかしながら，技術的に再利用は不可能ではない．そこで，サービスサーバが利用された属性証明書のシリアル番号を記録することによって，再利用防止を実現する．

不正入手となりすまし もし，第三者が属性証明書を不正に入手したとしても，なりすましを行うためには，属性証明書を発行されたユーザの私有鍵が必要である．属性証明書には，属性証明書使用者が属性証明書を発行されたユーザかどうかを確認するための認証値が含まれている．認証値の一つは属性証明書を発行されたユーザの公開鍵で暗号化されている．そのため，属性証明書を不正に利用するためには，属性証明書を発行されたユーザの私有鍵を使って，認証値を取り出す必要がある．よって，なりすましには属性証明書を発行されたユーザの私有鍵が必要であるが，PKI において，私有鍵の管理を厳重に行うのは当然であり，この問題は本提案方式に限ったことではない．

5 まとめ

我々は，サービス利用時の権限証明手段として，属性証明書を用いることにより，サービスサーバに対するプライバシ保護された権限行使を PKI 上で実現する方法を提案した．属性証明書には個人を示す ID 情報は含まれず，権限行使のための属性情報が含まれている．また，属性証明書には個人を示す情報が含まれていないため，第三者による不正利用を防止する手段が必要であり，属性証明書を発行されたユーザを確認するための認証値を用いることで，この問題を解決した．これにより，正規利用者がプライバシを保護された状態での権限行使を実現した．

参考文献

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

[2] ECOM and JIPDEC. *ECOM and JIPDEC Joint Forum 2003*, 2003.

[3] 今枝直彦, 小田原秀幸, 政本廣志. 属性証明書利用における属性証明書と公開鍵証明書のリンクに関する一考察. 信学技報, IEICE, 2003. ISEC2002-106.

[4] 齋藤孝道, 梅澤健太郎, 奥乃博. プライバシーを重視するアクセス制御システムの一方式. 電子情報通信学会論文誌, Vol. J84-D1, No. 11, pp. 1553–1562, 2001.

[5] T. Saito, K. Umesawa, T. Kito, and H.G. Okuno. Privacy-Enhanced SPKI Access Control on PKIX and Its Application to Web Server. In *AINA2003*, pp. 696–703, 2003.

[6] 佐藤直之, 鈴木英明. 匿名のままの権利行使を可能とした認証方式. 情報処理学会論文誌, Vol. 41, No. 8, pp. 2138–2147, 2000.

[7] 柿崎淑郎, 辻秀一. 属性証明書を用いた匿名アクセス制御の提案. 第 66 回情報処理学会全国大会, 2004. 6V-3.