属性認証を利用したプライバシ保護方式

柿崎淑郎[†] 山本宙[††] 辻秀一[††]

Web サービス等のサービス利用時において，正規利用者であることを確認できれば，誰であるかを確認する必要がない場合が，しばしばある．近年の情報の爆発的な増加にともない，趣味趣向を活かしたリコメンデーションシステムが活躍する一方で，個人情報や利用情報等のプライバシ保護への対応の重要性が高まっている．本論文では属性認証を利用し，利用者が誰であるかをサービス提供者に特定されることなくサービスを利用することができる方式を提案する．これにより，どの利用者がどのようなサービスを利用したかを隠蔽し，利用者のプライバシ保護を実現する．

A Privacy Protection Method Using Attribute Authentication

Yoshio Kakizaki,[†] Hiroshi Yamamoto[††] and Hidekazu Tsuji[††]

When the Web services are used, there is a case that they need not identify who is the user if the user is the regular user. Information increases explosively in recent years, the recommendation system is used well in many services. On the other hand, the importance of the privacy protection has risen. In this paper, we propose the method that the service server can provide the services without identifying the user by using attribute authentication. Our method makes it possible to protect the user's usage information.

1. はじめに

ネットワークの急速な普及にともなって，様々な個人情報を含むデータが大量に流通し利用されている．日本では 2005 年 4 月からの個人情報保護法が施行され，プライバシ保護への対応の重要性が高まっている．また，個人情報の目的外利用や情報漏洩等への対策のために，不必要に個人情報を公開しないことが求められている．

ネットワーク上の盗聴，なりすまし，改ざん等の脅威を公開鍵暗号技術によって防ぐ基盤技術として，公開鍵基盤（Public-key Infrastructure: PKI）がある．PKI で使われる電子証明書として，本人性を証明する公開鍵証明書[4] や属性情報を証明する属性証明書[3] がある．PKI は暗号化とディジタル署名の機能を提供し，認証，機密性，完全性，否認防止を実現する．しかしながら，匿名化の機能はなくプライバシ保護の問題は解決されない．

† 東海大学連合大学院理工学研究科
Graduate School of Science and Technology, Tokai University Unified Graduate School
†† 東海大学情報理工学部
School of Information Science and Technology, Tokai University

Web サービス等のサービス利用時において，正規利用者であることを確認できれば，利用者が誰であるかを確認する必要がない場合はしばしばある．しかし，一般的に用いられている ID/パスワード方式の場合，本人認証と権限の適用が同時に行われるため，サービス提供者に誰がどのようなサービスを利用したかを知られる恐れがある．ユビキタス社会の急速な進展によって，こういった場面に適用できるプライバシ保護を可能とする認証方式の必要性が高まっている．

本論文では属性証明書を用いて，利用者が誰であるかを特定されることなく，利用者の権限に基づくサービスを利用することで，プライバシ保護を実現する認証方式を提案する．正規利用者であり，かつ正規権限を持つ利用者は，サービス利用時に誰であるかを特定されることなく，サービスを利用することが可能であり，サービス提供者は利用者が誰であるかを知ることはできない．これにより，Web サービス等のサービス利用時において，利用者のプライバシ情報を保護することが可能となる．

2. 関連研究

プライバシ保護を実現する方法は，様々なアプローチから研究が行われている．本人性を隠蔽する代表的な方法として，匿名方式と仮名方式がある．匿名方式

表 1 属性証明書のプロファイル
Table 1 Profile of Attribute Certificate standard fields.

フィールド名	説明
version	v2
holder	証明書所有者を識別するための情報
issuer	発行した認証局の名前
signature	発行者が証明書に署名したアルゴリズム
serialNumber	証明書を識別するための番号
attrCertValidityPeriod	有効期限
attributes	属性情報
issuerUniqueID	発行者を識別するための識別子
extensions	証明書の拡張領域

は本人性を隠蔽し，誰であるかを分からなくする方法であり，仮名方式は本人性を直接推測できない仮名を付与することにより，誰であるかを分からなくする方法である．匿名方式の場合は識別性がないが，仮名方式の場合には同一人物であることを識別することが可能である．

電子証明書を用いた匿名性の研究として，SPKI（Simple PKI）[2] を用いた認証と権限行使を分離する研究[9),13)] がある．SPKI の証明書は ID 情報（本人情報）を含まない権限証明書の一種であり，この証明書を用いたアクセス制御により ID 情報の漏洩を防ぐことを可能としている．しかし，SSL や S/MIME 等の PKI アプリケーションの多くは，X.509 証明書を利用している．そのため，SPKI よりも普及度で勝る PKIX（PKI X.509）での実現は，既存インフラの再利用性および親和性，さらに導入の容易さを考えた場合に，大変有効である．

電子署名を用いた匿名認証の研究として，グループ署名を用いる研究が活発に行われている[14)]．たとえば，k-TAA（k-Times Anonymous Authentication）[7] は匿名性を保持したまま k 回のアクセスを実現している．しかしながら，グループ署名は通常のディジタル署名に比べ，計算量が 10 倍程度必要であるという問題がある．

属性証明書は証明書所有者の属性情報を証明する X.509 証明書であり，**表 1** に示す情報を含んでいる．属性情報を記載するための従来方式として，公開鍵証明書内の拡張領域に記載する方法があったが，一般に公開鍵の寿命よりも属性情報の寿命の方が短命であるため，属性情報の失効にともない，公開鍵証明書の再発行が必要となる問題があった．そこで属性情報を属性証明書に記載することで，属性情報の失効による公開鍵証明書の再発行が不要となり，鍵作成と管理のコストを抑制することができるようになった．

文献 3) は属性証明書を説明するにとどまり，実際の利用や運用に関する展開は行われていない．文献 16) は属性情報の登録・活用の制度面について展開している．また，文献 10) では，公開鍵のハッシュで公開鍵証明書と属性証明書をリンクさせる場合の問題点をあげ，その対策案について検討している．その中で，属性証明書が本人情報を含まないことによって，匿名性の性質があることに注目し，検討の必要性があることを指摘している．しかし，これらの文献における研究では，属性証明書に本人情報が含まれていない特徴や匿名性の性質については触れられているが，属性情報を有効活用した認証方式や具体的な技術展開は示されていない．そのため，属性情報を有効活用した認証方式や適用場面について検討する必要があった．

3. 提 案 方 式

3.1 アプローチ

属性証明書を用いた属性認証を行うことで，利用者の属性に基づくサービスの提供を行うことができる．属性証明書には本人情報が含まれていないが，公開鍵証明書に紐付けることで，公開鍵証明書による本人確認と属性証明書による権限の適用が可能となる．しかしながら，本人確認によって，個人が特定できるために，サービス利用時のプライバシを保護できないという問題があった．

個人情報は本人情報と属性情報の 2 つに大分することができる．本人情報は対象者を識別するための情報であり，属性情報は対象者に与えられる資格や権限を表す情報である．たとえば，「柿崎淑郎」は本人情報であり，「大学院生」は「柿崎淑郎」の属性情報である．属性情報は個人情報の 1 つであるが，本人情報と切り離すことで個人情報としての価値を失う．アンケート等で統計処理を行う場合，本人情報を切り捨て属性情報のみを集計することで，その匿名性を確保している．

本提案方式は個人情報である本人情報と属性情報を分離し，本人情報の証明に公開鍵証明書を用い，属性

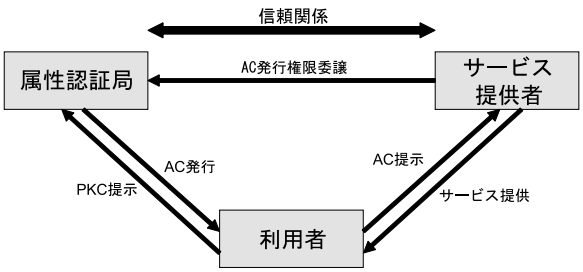

図 1 提案方式の構成図
Fig. 1 The structure of our method.

表 2 公開鍵証明書と属性証明書の比較
Table 2 A comparison of Public-key Certificate and Attribute Certificate.

	公開鍵証明書	属性証明書
目的	証明書所有者の本人性を証明	証明書所有者の属性を証明
証明書の項目	利用者を特定できる情報と公開鍵	証明書所有者の属性情報
有効期間	長い	短い
証明書発行機関	認証局	属性認証局

情報の証明に属性証明書を用いる．属性証明書発行時の本人確認は公開鍵証明書で行い，属性証明書利用時には本人情報を含まない情報で利用者確認を行う．この本人情報を含まない属性証明書を利用することで，サービス利用時に利用者が誰であるかを特定されることなく，サービスを利用することができる．

本提案方式は誰がどのようなサービスを利用したかという情報を隠蔽し，利用者のプライバシ保護を実現する．また，本人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を可能とする．

3.2 構　　成

本提案方式の構成を**図 1** に示す．本提案方式は一般的な三者モデルであり，属性認証局，サービス提供者，利用者により構成される．

3.2.1 構 成 要 素

属性認証局

属性認証局は属性証明書の発行を行う．属性認証局はサービス提供者と信頼関係にあり，サービス提供者から属性証明書の発行権限を委譲されている．

属性認証局は利用者がサービスを利用するための認証情報と属性証明書を作成する．認証情報は属性証明書所有者が正規利用者であることをサービス提供者が確認することができる情報である．属性証明書には認証情報のハッシュと利用者の権限である属性情報が記載されている．

サービス提供者

サービス提供者は利用者に対して，Web サービス等のサービスを提供する．サービス提供者は属性認証局と信頼関係にあり，属性証明書の発行権限を属性認証局に委譲している．

サービス提供者は提示された属性証明書の holder フィールドから対応する認証情報を探し出す．認証情報を用いて，利用者が属性証明書正規所有者であることを検証し，正規利用者であることを確認したうえで，属性証明書に記載された属性に基づいて，利用者にサービスを開始する．

利　用　者

利用者はサービス提供者から Web サービス等のサービスを利用する．

サービス利用に必要な属性証明書を発行されるために，公開鍵証明書を属性認証局に提示して，認証される．属性証明書が発行されたら，サービス提供者に属性証明書を提示して，属性証明書に記載された権限のサービスを利用する．

3.2.2 電子証明書

本提案方式では公開鍵証明書と属性証明書を利用する．ここでは 2 つの証明書について説明する．また，公開鍵証明書と属性証明書の比較を**表 2** に示す．

公開鍵証明書

公開鍵証明書（Public-key Certificate: PKC）は証明書所有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，ディジタル署名された公開鍵であることを証明する．

属性証明書

属性証明書（Attribute Certificate: AC）は証明書所有者の属性を証明する証明書である．属性証明書も

表 3 holder フィールドのプロファイル
Table 3 Profile of holder field options.

フィールド名	説明
baseCertificateID	公開鍵証明書の serialNubmer と issuer
entityName	公開鍵証明書の subject または subjectAltName
objectDigestInfo	対象のハッシュ

公開鍵証明書と同様に，X.509 証明書フォーマットであり，権限行使に必要な属性情報（名前，所属，役職等）を含んでいるが，公開鍵は含んでいない．属性証明書には証明書所有者の本人性を証明する情報が含まれていないため，属性証明書所有者の公開鍵証明書等に紐付ける必要がある．この紐付けには属性証明書の holder フィールドを用いる．

holder フィールドには**表 3** に示すように，baseCertificateID，entityName，objectDigestInfo の異なる 3 つのオプションがある．baseCertificateID と entityName は直接的に公開鍵証明書を検証することができ，本人情報を確認することができる．objectDigestInfo は対象のハッシュであり，対象を検証することができる．

本提案方式では本人情報を含む公開鍵証明書へのリンクを行わないため，属性証明書の holder フィールドには，baseCertificateID や entityName を用いずに，objectDigestInfo を用いる．objectDigestInfo の対象を属性認証局が作成した認証情報とすることで，属性証明書検証者は属性証明書所有者が正規所有者であることを検証できるが，属性証明書検証者は属性証明書所有者が誰であるかを特定することはできない．

認証情報は以下のように決定される．まず，十分に大きくランダムな整数を 2 つ生成する．1 つは利用者とサービス提供者間の認証用の鍵であり，もう 1 つは利用者のセッション鍵である．認証用の鍵とセッション鍵の排他的論理和を利用者鍵とする．認証情報は

(1) 認証用の鍵

(2) 利用者鍵を利用者の公開鍵で暗号化したものの 2 つをサービス提供者の公開鍵で暗号化したものとする．属性証明書の holder フィールドの objectDigestInfo には，この認証情報のハッシュが記載される．

また，同じ属性証明書を利用することによって，サービス利用履歴からの追跡をされる可能性があるため，その可能性を排除するために，属性証明書を使い捨てとする．つまり，属性証明書は 1 セッション 1 枚とする．そのため，属性証明書の有効期限を非常に短く設定することができる．これにより，属性証明書の失効手続が不要となり，CRL（Certificate Revocation List）や OCSP（Online Certificate Status Protocol）を準備する必要がなくなる．

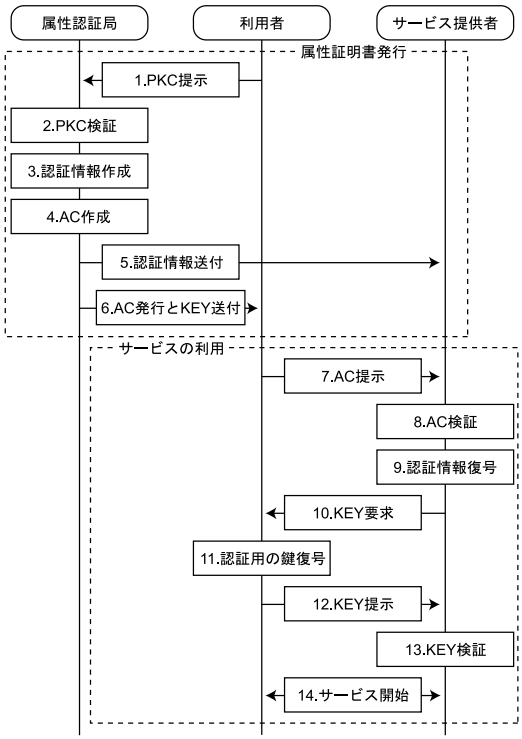

図 2 提案方式の処理フロー図
Fig. 2 The flow of our method.

3.3 処 理 手 順

利用者はサービス提供者のサービスを利用するために，以下の手順を行う．属性証明書発行からサービス提供者利用までの処理フロー図を**図 2** に示す．また，手順の説明に**表 4** の記号を用いて説明する．

属性証明書発行

(1) 利用者は属性認証局に対し，公開鍵証明書を提示する．

(2) 属性認証局は公開鍵証明書の有効性を検証する．また，利用者が公開鍵証明書に対応する私有鍵を持っていることを確認する．

(3) 属性認証局は認証情報を以下のように作成する．まず，十分に大きくランダムな整数を 2 つ生成する．1 つは利用者とサービス提供者間の認証

表 4 表記
Table 4 Notation.

記号	意味
$E(M, A)$	M を A の公開鍵で暗号化
$D(M, A)$	M を A の私有鍵で復号
$H(M)$	M のハッシュ
$AC.holder$	属性証明書の holder フィールド
KEY	十分に大きくランダムな整数
$AuthInfo$	認証情報
SP	サービス提供者
U	利用者
$A \overset{sendto}{\longrightarrow} B$	A を B に送る
$A \overset{?}{=} B$	A と B が等しいかの比較

用の鍵であり，もう 1 つは利用者のセッション鍵である．

$$\text{Generate } KEY_A, KEY_S$$

認証用の鍵とセッション鍵を排他的論理和したものを利用者鍵とする．

$$KEY_U = KEY_A \oplus KEY_S$$

認証用の鍵，利用者鍵を利用者の公開鍵で暗号化したもの，以上 2 つをサービス提供者の公開鍵で暗号化したものを認証情報とする．

$$AuthInfo = E((KEY_A, E(KEY_U, U)), SP)$$

(4) 属性認証局は認証情報のハッシュを計算し，属性証明書の holder フィールドの objectDigestInfo に記載する．

$$AC.holder = H(AuthInfo)$$

また，利用者の属性を attributes フィールドに記載し，属性証明書を作成する．

(5) 属性認証局は認証情報をサービス提供者に送る．

$$AuthInfo \overset{sendto}{\longrightarrow} SP$$

(6) 属性認証局は属性証明書とセッション鍵を利用者の公開鍵で暗号化し，利用者に発行する．

$$(AC, E(KEY_S, U)) \overset{sendto}{\longrightarrow} U$$

サービスの利用

(7) 利用者は属性証明書をサービス提供者に提示する．

(8) サービス提供者は属性証明書のディジタル署名を検証し，発行権限を委譲した属性認証局が発行した属性証明書であることを確認すると同時に，改ざんや捏造がないことを確認する．また，有効期限が切れていないことを確認する．

(9) サービス提供者は属性認証局から送られてきた認証情報のハッシュを計算し，提示された属性証明書の holder フィールドに対応する認証情報を探し出す．

$$H(AuthInfo) \overset{?}{=} AC.holder$$

もし，複数の認証情報のハッシュが一致する場合，それらの認証情報を破棄する．また，それらの認証情報に対応する属性証明書を利用しようとする利用者に，属性証明書を再取得するように知らせる．認証情報を私有鍵で復号し，認証用の鍵を取り出す．

$$(KEY_A, E(KEY_U, U)) = D(AuthInfo, SP)$$

(10) サービス提供者は利用者が正規利用者であることを確認するため，利用者の公開鍵で暗号化した利用者鍵を利用者に送る．

$$E(KEY_U, U) \overset{sendto}{\longrightarrow} U$$

(11) 利用者はサービス提供者から送られてくる暗号化された利用者鍵を私有鍵で復号し，利用者鍵を取り出す．

$$KEY_U = D(E(KEY_U, U), U)$$

また，属性認証局から送られてくる暗号化されたセッション鍵を私有鍵で復号し，セッション鍵を取り出す．

$$KEY_S = D(E(KEY_S, U), U)$$

利用者鍵とセッション鍵の排他的論理和から，認証用の鍵を計算する．

$$KEY_{A'} = KEY_U \oplus KEY_S$$

(12) 利用者は認証用の鍵をサービス提供者に送る．

$$KEY_{A'} \overset{sendto}{\longrightarrow} SP$$

(13) サービス提供者は利用者から送り返された認証用の鍵が，認証情報から取り出した認証用の鍵と同じならば，利用者が属性証明書の正規所有者であると判断する．

$$KEY_A \overset{?}{=} KEY_{A'}$$

(14) サービス提供者は属性証明書に記載された属性に基づくサービスを開始する．

属性認証局は利用者の本人情報とその権限の情報を持ち，サービスを利用するための属性証明書を発行するが，利用者がどのようなサービスを利用したかは知りえない．属性認証局は，利用者の権限を記載した属性証明書と認証情報を発行する．属性認証局は認証情報のために，KEY_A と KEY_S と KEY_U を作成する．$KEY_A = KEY_U \oplus KEY_S$ であり，$KEY_S = KEY_U \oplus KEY_A$ だが，KEY_S は利用者が持ち，KEY_U は利用者の公開鍵で暗号化されている．利用者は KEY_S と復号した KEY_U から，KEY_A を得ることができる．そのため，属性証明書所有者の公開鍵に対応する私有鍵と属性認証局から発行される KEY_S の両方がないと属性証明書を利用することはできない．

また，認証情報には属性証明書利用者が正規利用者

であることを確認するための情報が含まれているが，利用者が正規利用者の誰であるかを特定することはできない．そのため，属性証明書検証者は属性証明書利用者が誰であるかを特定することはできない．

サービス提供者は利用者がどのようなサービスを利用したかを知りうるが，利用者が正規利用者の誰であるかは知りえない．認証情報には利用者を特定する情報が含まれているが，利用者が誰であるかを特定する情報は含まれていない．

このように，属性認証局とサービス提供者で知りうる情報が分散されるため，どの利用者がどのようなサービスを利用したかというプライバシ情報を保護することが可能である．

4. 本方式の展開

4.1 適用範囲

本提案方式は個人情報である本人情報と属性情報を分離することで，本人認証と属性認証を分離させ，サービス提供者に誰であるかを特定されることなく，サービスを利用することを可能とし，サービス利用履歴を秘匿することで，プライバシ情報を保護する方式である．本提案方式を適用できる条件は，以下である．

- サービス自体に本人情報が含まれていないこと
- 複数のサービスが存在すること
- 従量制サービスではないこと

利用しようとするサービス自体に個人情報が含まれている場合，利用したサービスから個人情報が特定される可能性がある．この問題に該当する例として，医療情報サービスがある．医療情報はきわめて重要な属性情報であり，そのプライバシを保護したいという要望は強い．しかし，医療情報は本人情報と属性情報に分離してしまうと，情報自体に価値がなくなってしまう．それゆえに，こういった場面においては，我々の提案方式を適用することはできない．

単一のサービスの場合，その唯一のサービスを利用することが目的であることは明らかであり，利用履歴を隠すことに意味を見出すことができない．

従量制サービスの場合，利用するサービスごとまたは利用量によって利用料金が異なるため，利用料金から利用したサービスを推測することが可能である．そのため，サービス利用履歴を秘匿するだけでは，プライバシ情報を保護することが難しい．

4.2 具体例

本提案方式を適用できる例として，e-learning や図書閲覧サービス，ビデオ配信サービス等が考えられる．

e-learning では，授業料を支払うことで，提供される授業を自由に受講ができるとする．利用者はどの授業を受講しているかという傾向を知られたくなく，サービス提供者は正規権限での利用であれば，どの利用者がどの授業を受講していてもかまわない．また，サービス提供者はどの授業がどれだけ受講されているかを知ることはできる．

利用者は e-learning を提供するサービス提供者に会員登録をする．サービス提供者はサービス利用に必要な属性証明書の発行権限を属性認証局に委譲する．利用者は e-learning を利用するために，属性証明書と認証用の鍵を属性認証局によって発行される．利用者はサービス提供者に属性証明書を提示し，認証用の鍵で正規利用者であることを証明し，e-learning を利用する．

属性認証局は利用者が誰であり，どの授業を受講できるかを知っているが，利用者がどの授業を受講したかを知ることはできない．サービス提供者は利用者がどの授業を受講できるかを確認でき，どの授業を受講したかを知ることができるが，利用者が誰であるかを知ることはできない．このように，どの利用者がどの授業を受講したかという情報は，属性認証局もサービス提供者も知りえない．

同様にして，図書閲覧サービスでは，有料会員はすべての図書を閲覧することができるが，無料会員は有料会員用の図書を閲覧することができないとする．利用者はどのような図書を閲覧しているかを知られたくなく，サービス提供者は正規権限での利用であれば，どの利用者がどの図書を閲覧していてもかまわない．

ビデオ配信サービスでは，映画，スポーツ，ドラマ等の複数のジャンルがあり，そのジャンルを契約している利用者は，そのジャンル内にあるコンテンツを自由に試聴することができるとする．利用者はどのようなコンテンツを試聴しているかを知られたくなく，サービス提供者は正規権限での利用であれば，どの利用者がどのコンテンツを試聴していてもかまわない．また，サービス提供者はどのコンテンツがどれだけ利用したかを知ることはできる．

このように，利用者は利用できるサービスを自由に利用でき，サービス提供者に受講履歴を記録されないため，サービス利用履歴のプライバシ保護が可能となる．

5. 議論

5.1 利点

本提案方式は本人情報と属性情報を分離し，属性証明書に正規利用者であることを示す認証情報を記載す

ることで，サービス利用時に誰であるかを特定されることなく権限行使を可能とし，利用者のプライバシ保護を実現した．属性認証局は誰がサービスを利用しようとしたかは分かるが，どのようなサービスを利用したかは分からない．サービス提供者は正規利用者の誰かがサービスを利用したことは分かるが，その正規利用者が誰であるかは分からない．これにより，正規利用者のみにサービスを提供したいが，正規利用者であることを確認できれば，誰であるかを確認する必要がないサービスに対して，利用者のプライバシ保護を可能とする方式である．

本提案方式は公開鍵証明書と属性証明書を用いているため，PKIX との親和性が高い．SSL や S/MIME 等の PKI アプリケーションの多くは，X.509 証明書を利用している．そのため，SPKI を用いた方式[9),13)]に比べ，PKI での普及度で勝る PKIX での実現は，既存設備との親和性が高い．

サービス利用履歴からの追跡を防ぐために，属性証明書を使い捨てにしている．しかし，属性が変化しない限り，属性証明書を再利用できることが，望ましい．特に，頻繁に利用されるサービスの場合，属性証明書の発行コストがネックになる可能性が高い．サービスの利用頻度が高い場合，属性証明書を数回再利用しても，十分に安全な場合もある．この場合，プライバシ保護のレベルと属性証明書発行コストは，トレードオフの関係になる．

5.2 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，発行者である属性認証局によって，ディジタル署名が行われている．ディジタル署名を検証することで，属性証明書の改ざんと捏造の検出が可能である．この安全性は PKI の他の電子証明書と同等である．

悪意ある利用者が属性認証局になりすまして属性証明書を発行する場合，サービス提供者はその属性証明書のディジタル署名を検証することで，捏造された属性証明書であることを検出することができる．

再 利 用

属性証明書は 1 セッション 1 枚を前提に，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．厳密に再利用を防ぐためには，利用された属性証明書のシリアル番号をサービス提供者が記録することによって，再利用を防止することが可能である．

不正入手となりすまし

悪意ある利用者が何らかの方法で属性証明書を不正入手した場合を評価する．悪意ある利用者は属性証明書をサービス提供者に提示する．サービス提供者は属性証明書利用者を確認するために，属性証明書所有者の公開鍵で暗号化された鍵を属性証明書利用者に送る．しかし，悪意ある利用者は属性証明書の正規所有者ではないので，属性証明書正規所有者の私有鍵を持っていないため，暗号化された鍵を復号することができない．よって，悪意ある利用者が属性証明書を不正に入手しても，利用することができない．これは正規利用者が他の正規利用者の属性証明書を利用する場合も同様である．

5.3 追跡不能性

サービスを利用するために必要な属性証明書には本人情報が含まれず，属性証明書から直接的に利用者を特定することはできない．しかし，利用者が誰であるかを特定できない状況下においても，サービス利用履歴からの追跡が可能である．たとえば，同じ属性証明書を利用する利用者は同一利用者であることが特定でき，状況によっては個人を特定することができる可能性がある．我々はサービス利用履歴からの追跡もプライバシ保護の側面から問題があると認識しており，これを防止するために，属性証明書を再利用できないようにした．

5.4 認証情報のハッシュ

3.3 節の手順 (9) において，サービス提供者は複数の認証情報から，提示された属性証明書の holder フィールドに対応する認証情報を探し出している．属性証明書の holder フィールドには認証情報のハッシュが記載されている．ハッシュには衝突困難性があるが，ハッシュどうしの衝突は皆無ではない．そのため，複数の認証情報のハッシュが一致する場合が考えられる．

もし複数の認証情報のハッシュが一致する場合，それらの認証情報をすべて破棄する．また，それらの認証情報に対応する属性証明書を利用しようとする利用者に，属性証明書を再取得するように知らせる．

このようなハッシュの衝突が発生する確率は，利用するハッシュアルゴリズムの衝突困難性に依存している．

6. ま と め

本論文では属性証明書に公開鍵が含まれていない点と属性情報のみが記載されている点に着目し，個人情報である本人情報と属性情報を分離し，属性情報だけでサービスを利用することにより，サービス利用者のプライバシ情報を保護することができる方式を提案

した．

属性証明書には個人を特定する本人情報は含まれず，権限行使のための属性情報だけが含まれており，その属性証明書所有者を holder フィールドで紐付ける．属性証明書の holder フィールドに objectDigestInfo を用い，その対象を属性認証局が作成した認証情報とすることで，属性証明書検証者は直接的に属性証明書所有者を特定することはできないが，属性証明書所有者が正規利用者であることを確認できる．これにより，利用者はサービスを利用する場合に，誰であるかを特定されずにサービスを利用でき，かつサービス提供者は正規利用者のみにサービスを提供することができる．その結果，利用者が誰であるかを特定できないため，誰がどのようなサービスを利用したかを隠蔽することができ，利用者のプライバシ情報の保護が可能となった．

参 考 文 献

1) Benjumea, V., Lopez, J., Montenegro, J.A. and Troya, J.M.: A First Approach to Provide Anonymity in Attribute Certificates, *PKC 2004*, Vol.2947 of LNCS, pp.402–415 (2004).
2) Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B. and Ylonen, T.: SPKI Certificate Theory, RFC2693 (1999).
3) Farrell, S. and Housley, R.: An Internet Attribute Certificate Profile for Authorization, RFC3281 (2002).
4) Housley, R., Polk, W., Ford, W. and Solo, D.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC3280 (2002).
5) Kakizaki, Y., Yamamoto, H. and Tsuji, H.: A Proposal of An Anonymous Authentication Method For Flat-rate Service, *ARES 2006*, pp.551–557 (2006).
6) Nakanishi, T. and Sugiyama, Y.: Anonymous Statistical Survey of Attributes, *ACISP2001*, Vol.2119 of LNCS, pp.460–473 (2001).
7) Nguyen, L. and Safavi-Naini, R.: Dynamic k-Times Anonymous Authentication, *ACNS 2005*, Vol.3531 of LNCS, pp.318–333 (2005).
8) Park, J.S. and Sandhu, R.: Binding Identities and Attributes using Digitally Signed Certificates, *16th ACSAC*, pp.120–127 (2000).
9) Saito, T., Umesawa, K., Kito, T. and Okuno, H.: Privacy-Enhanced SPKI Access Control on PKIX and Its Application to Web Server, *AINA2003*, pp.696–703 (2003).
10) 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，ISEC2002-106 (2003).
11) 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，6V-3 (2004).
12) 柿崎淑郎，辻 秀一：属性証明書を用いた認証方式の提案，情報処理学会研究報告，2004-CSEC-27(2) (2004).
13) 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).
14) 佐古和恵，米沢祥子，古川 潤：セキュリティとプライバシを両立させる匿名認証技術について，情報処理，Vol.47, No.4, pp.410–416 (2006).
15) 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).
16) 千葉昌幸，漆嶌賢二，前田陽二：属性情報プロバイダ：安全な個人属性の活用基盤の提言，情報処理学会論文誌，Vol.47, No.3, pp.676–685 (2006).

(平成 18 年 5 月 16 日受付)
(平成 18 年 12 月 7 日採録)

柿崎 淑郎（学生会員）

1980 年生．2003 年東海大学工学部電子工学科卒業．2005 年東海大学大学院工学研究科電子工学専攻博士課程前期修了．同年東海大学連合大学院理工学研究科総合理工学専攻博士課程進学．現在に至る．情報セキュリティ，属性情報の研究に従事．

山本 宙

1991 年大阪大学基礎工学部情報工学科卒業．1996 年大阪大学大学院基礎工学研究科博士課程修了，博士（工学）．同年大阪大学基礎工学部助手，以来，符号理論，情報・セキュリティとその応用に関する研究に従事．2000 年 4 月より東海大学に勤務，2004 年 4 月より情報理工学部情報メディア学科助教授．2006 年ハワイ大客員研究員．電子情報通信学会会員．

辻　　秀一（正会員）

1969年大阪大学基礎工学部電気工学科卒業．1974年大阪大学大学院基礎工学研究科博士課程修了，工学博士．1974〜2000年三菱電機（株）に勤務．この間ヒューマンインタフェースや人工知能システム等の研究開発に従事．1997〜2000年電子商取引実証推進協議会へ出向．2000年4月より東海大学に勤務．現在，情報理工学部情報メディア学科教授．電子情報通信学会，人工知能学会，電気学会，IEEE各会員．