署名検証代行モデルを適用した匿名認証方式の検討

6H−04

飯田 恭弘† 上野 正巳† 阿川 雄資† 鬼頭 利之‡
†日本電信電話株式会社 NTT情報流通プラットフォーム研究所
‡東京理科大学 理工学部 情報科学科

1．はじめに

現在普及している認証方法は，主にユーザIDとパスワードによるもの，および公開鍵認証基盤（PKI）によるものが一般的である．これらの認証方法ではユーザの個人情報と利用情報の関連付けが容易であり，ユーザの利用履歴などプライバシに関わる情報が詳細に蓄積されることになる．すなわち，プライバシに関わるこれらの情報に対して，2次利用などの不当な扱いが極めて容易となる．

そこで我々はユーザのプライバシ保護を重視し，ユーザの個人情報と利用履歴情報の関連付けを暗号学的に困難にする認証方法（匿名認証方式）を提案してきた[1,2,3]．

本稿では匿名認証方式の概要を述べた後，他の認証方法との比較を通して匿名認証方式の位置づけを明らかにする．また，匿名認証方式の課題を述べ，これを解決するために，これまでの匿名認証方式を拡張した方式について述べる．

2．匿名認証方式の概要

本方式は公開鍵暗号系を基盤とした証明書（権利証明書）による認証方法であり，また，ユーザは匿名のまま権利の行使が可能である．ユーザの匿名性と権利の正当性の検証を同時に実現させるため，発行者による署名にはブラインド署名を，権利証明書の作成にはcut & chooseの手法を用いている[1]．

3．匿名認証方式の位置づけ

本節ではユーザの匿名性を実現する度合いの観点から（A）ユーザIDとパスワードによる認証方法，（B）PKIで規定する公開鍵証明書（および属性証明書）による認証方法，（C）SPKIを利用した認証方法，および（D）我々の提案する匿名認証方式の4つの認証方法を比較する（表1）．ここでユーザとは認証の対象となる主体を，発行者とはユーザの認証に必要な情報をユーザへ払出す主体を，検証者とはユーザの認証に必要な情報を検証する主体をそれぞれ指している．

	(A)	(B)	(C)	(D)
厳密なユーザ認証	×	○	○	○
検証者に対する匿名性	×	×	○	○
発行者に対する匿名性	×	×	×	○

表1：各認証方式が実現するユーザの匿名性

（A）は導入コストが低く現在最も普及している認証方法である．ところが，盗聴されたユーザID/パスワードに対しても正当な場合と同様にユーザ認証処理が可能なため，厳密なユーザ認証は困難である．

（B）はPKIで規定された公開鍵証明書による認証方法で，Subjectフィールドの DN（識別名）によってグローバルな空間でユーザを一意に識別できる．またユーザの認証はチャレンジ・レスポンスを用いて厳密に実施される．反面，誰もがユーザを一意に識別できるため，匿名性はどの主体に対しても確保されない．

（C）はSPKIで規定されている権限証明書[4]を用いた認証方法である．権限証明書では公開鍵と権限を関連付けるのみであるため，検証者に対してユーザの匿名性を確保することができる．しかし，この方法では検証者と発行者が同一の主体の場合にはユーザの匿名性が確保されない．

ところで，実際の認証サービスの形態を考えるとユーザID/パスワードを払出す主体（発行者）が同時にユーザID/パスワードの検証を行う主体（検証者）となることが多い．したがってユーザのプライバシを保護する認証サービスの運用を考えると，検証者に対してだけでなく発行者に対してもユーザの匿名性を確保することが重要となる．このような観点から，（D）の匿名認証方式はブラインド署名によって発行者に対しても匿名性を確保できるため，認証サービスの提供形態としてユーザのプライバシ保護上

"A Study of the anonymous authentication method with a signature-verifying authority"
Yasuhiro IIDA†, Masami UENO†, Yuji AGAWA†, Toshiaki KITOH‡
†NTT Information Sharing Platform Laboratories
‡Science University of Tokyo

最も望ましい形態であると考えられる．

4．匿名認証方式の課題

ところが，匿名認証方式では権利証明書の検証時に暗号文変換を複数回実施した後に署名検証を行うため，非常に負荷が高くなる．前節の（A）～（D）の認証方法において，ユーザの認証時の処理負荷を比較したものを表２に示す．

	(A)	(B)	(C)	(D)
認証時の処理負荷	○	△	△	×

表２：各認証方式の処理負荷

発行者の署名の検証をユーザの認証時に行うと，高い処理負荷によって長い待ち時間やマシン資源占有などのサービス品質低下につながるという課題がある．これに対し文献２では第３者（Third Party：TP）が権利証明書の署名の検証をあらかじめ行っておく（本稿ではこれを署名検証代行モデルと呼ぶ）ことで課題を解決できることを示唆している[2]．本稿では署名の発行者を信頼できる第３者（Trusted Third Party：TTP）とし，ユーザの匿名性を保ったまま処理負荷を低減する具体的な権利証明書の発行手順を示す．

5．課題を解決するための匿名認証方式の拡張

以下では権利証明書の発行手順を Step.1 から Step.3 に分けて述べる（図１）．

Step.1：ユーザは新たな権利証明書の発行要求と共に，以前に取得した権利証明書（既得の権利証明書）を発行者へ提示する．発行者はこの既得証明書を，TTP の署名の検証，無効リスト検索，チャレンジ・レスポンスによって検証する．これらの処理は公開鍵証明書の検証と同様である．

Step.2：ユーザは証明内容 M，公開鍵 P，暗号文 E，およびその他の情報 A の組（証明書元情報：Pre-Cert）に乱数等でブラインド化演算を行った Bld-Pre-Cert を N 組発行者へ送信する．発行者はこのうち，任意の R 個の Bld-Pre-Cert を選び，ブラインドの解凍をユーザへ要求する（cut & choose）．ユーザは指定された R 個の Bld-Pre-Cert について，それぞれブラインド解凍処理を行い，R 個の Pre-Cert を発行者へ送信する．発行者はこの検証に成功すると，ブラインド化されている N－R 組の Bld-Pre-Cert に対し，署名 Bld-S_{CI} を生成し，ユーザへ送信する．ユーザは Bld-S_{CI} からブラインド解凍処理を行い，結局，署名 S_{CI} および権利証明書 Cert を取得する．ここまではこれまでの匿名認証方式における証明書発行処理と同じである．本提案では，Step.2 の直後に以下の Step.3 の手順を追加する．

Step.3：ユーザは取得した権利証明書 Cert および発行者の署名 S_{CI} を TTP へ送信する．TTP は S_{CI} を検証した後，検証合格の証として署名 S_{TTP} を生成し，ユーザへ送信する．結局，ユーザは Cert，S_{CI}，S_{TTP} の１組を有効な権利証明書として管理する．

以上の Step.1 から Step.3 までの手順によって，ユーザの匿名性を少しも損なうことなく権利証明書の検証時（ユーザのサービス利用時）の処理負荷を低減することができる．

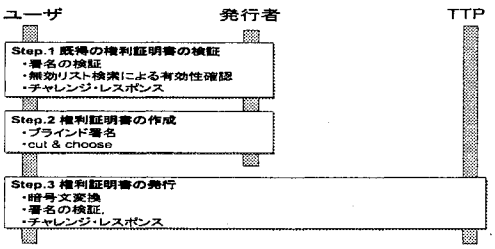

図１：権利証明書の発行手順

6．まとめ

本稿では他の認証方式との比較を通して，匿名認証の位置づけを明らかにした．また，匿名認証方式の処理のボトルネックとなる署名検証処理を，信頼できる第３者が代行する際の権利証明書の発行手順を具体的に規定した．

今後は　匿名認証サービスを運用する観点から必要な機能について検討を進める予定である．

参考文献

[1] 佐藤直之，鈴木英明，“耐タンパ個人端末を利用し個人情報の保護を可能とした認証方式”，情報処理学会論文誌，Vol.41，No.8，2000，pp2129-2137

[2] 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.8,2000，pp2138-2147

[3] 飯田恭弘，佐藤直之，花木三良，“ユーザを識別しない認証方式の実装と評価” 第 62 回情報処理学会全国大会講演論文集，2S-3，2001

[4] C. Ellison，”SPKI Requirements”，RFC2692，1999