マルチメディア通信と分散処理 111－26
コンピュータセキュリティ 20－26
（２００３．２．２８）

“匿名認証方式”の運用に関する一検討

飯田 恭弘* 上野 正巳* 阿川 雄資*

著者らはこれまでに，利用者のプライバシ保護を考慮し，利用者の行動情報と利用者の身元に関する情報との関連付けを暗号学的に困難にした，証明書に基づく認証方式（匿名認証方式）について検討してきた．本稿では，匿名認証方式のフィジビリティスタディを行い，実用化に向けて必要となるいくつかの要件および技術的課題について述べる．匿名認証方式を運用するモデルでは，証明書の発行と使用の時系列関係によっては，実効的に匿名性を全く確保できなくなるユーザが存在し得る課題を明らかにする．この課題に対し，プロトコルを正しく実施する信頼できるカウンタを導入して課題を解決する方式を提案する．

A study of the anonymous authentication management

Yasuhiro IIDA* Masami Ueno* Yuji AGAWA*

The anonymous authentication system makes it difficult for a service provider to relate a user's profile and his or her for a service provider, which can protect the user's privacy. In this paper, we describe some requirements and a technical problem when we apply the anonymous authentication system to business situations. We also describe its operation models and clarify that there can be a user whose anonymity is no longer retained in a certain time sequence of issuing/using a certificate. To solve this problem, we propose a novel method that introduces a Trusted Counter (TC) which counts certificates.

１．はじめに

ISP（インターネットサービスプロバイダ）のようなサービス提供者の中には，ユーザの氏名，年齢，性別といった身元情報を取得するとともに，ユーザ毎に識別子（ID）を払出してユーザを一意に識別した認証を行うことが多い．このときサービス提供者は，ユーザの身元情報と行動情報とを結びつけることで，どのユーザが，いつ，どのようなサービスを利用したか，を容易に把握することができる．すなわち，ユーザの趣味・趣向といったユーザのプライバシにかかわる情報がサービス提供者へ簡単に把握され得ることなる．

このような課題に対し，著者らは，たとえユーザの身元情報があらかじめ知られていたとしても，このユーザの身元情報と行動情報の結びつきを秘匿できる認証方式（匿名認証方式と呼ぶ）を提案してきた[1,2,3]．この方式ではサービスを利用する際のユーザの匿名性を確保し，ユーザのプライバシを保護している．

我々は，今回，匿名認証方式の実用化に向けて，必要となる要件，運用形態，適用領域の観点からいくつかの考察を行った．また，従来の匿名認証方式では証明書の発行と使用の時系列関係によっては，実効的に匿名性を全く確保できなくなるユーザが存在し得るという課題を明らかにした．この課題は匿名認証方式を既存の ISP のようなサービス提供者の認証システムへ導入する際に大きな障壁となる．そこで，我々は処理を正しく実施する主体が証明書の発行や使用の時系列関係を把握し，ユーザの匿名性を確保する方式を提案する．

本稿の構成を以下に述べる．次章では匿名認証方式の概要を説明する．3 章では匿名認証方式の実用化のための検討について述べる．4 章では匿名認証方式の運用モデルとその課題について述べる．5 章では前章で述べた課題を解決する方式を提案する．６章では，前章で提案した方式を評価する．７章では著者らによる前章とは別の提案方式を補足として述べる．８章では全体をまとめる．

*NTT 情報流通プラットフォーム研究所
*NTT Information Sharing Platform Laboratories

２．匿名認証方式

2.1 概要

匿名認証方式[1,2,3]は，証明書を基盤とした権限の認証方式であり，リソースを利用するユーザ（User），証明書を発行する証明書発行局（CI），User にリソースを提供するリソース管理者（RM）の主体を定義している．証明書には User の権限が記され，ブラインド署名技術[4]および cut&choose 技術[5]によって作成されている．

ブラインド署名の流れは以下の通りである．まず，メッセージ m を保有する「依頼者」は，m に乱数要素を演算（ブラインド化処理）することで，「署名者」にメッセージ m の内容を知られることなく署名計算（デジタル署名）をさせる．「依頼者」は「署名者」によって署名計算されたものから乱数要素を排除（ブラインド解凍処理）するこ

とで, 最終的に m に対する署名 S(m)を取得する. ただし, ブラインド署名ではメッセージ m を秘匿したまま「署名者」に提出するため, 「依頼者」は「署名者」から任意のメッセージ m'に対する署名を取得することが可能である. cut&choose は, このような不正を防止する一方式であり, 「署名者」は「依頼者」から乱数要素が付加された元情報の候補を複数提出させ, その中からいくつかをランダムに開示させることで, 「依頼者」が処理を正しく実行していることを確認するものである.

2.2 各主体と証明書

匿名認証方式で定義している主体および証明書の形式を以下に示す（ただし, 匿名認証方式の文献[1,2]では“裁判官”という特殊な存在を定義しているが, “裁判官”については本稿が扱う議論とは直接関係がないため, 説明を省略する）.

User：証明書を取得し, これを使用して RM のリソースを利用する主体. 証明書の正当な所有者であることをチャレンジ・レスポンスによって主張するための公開鍵, 秘密鍵のペア(P_U , S_U)を複数生成できる. 証明書の正当な所有者とは, P_U に対応した S_U を保持する User を意味する. なお, 証明書作成時には公開鍵 P_U は公開しない. また, User はブラインド署名の「依頼者」となる.

CI：User と協力して証明書を作成し, User へ証明書を発行する主体. 証明書を検証するための鍵（公開鍵）と, 証明書に署名するための鍵(秘密鍵)のペア(P_{CI} , S_{CI})を持つ. CI はブラインド署名の「署名者」となる.

RM：CI の公開鍵 P_{CI} によって証明書の署名を検証し, これに合格した User へリソースを提供する主体.

証明書：証明書を所有する User の公開鍵 P_U, User の権限 M, 証明書の検証に必要な付加情報{w_i}（詳細は発行プロトコルにて述べる）, およびこれらの組（P_U, M, {w_i}）に対する CI の署名 SIG_{CI} から成る.

$$\text{証明書} = (P_U,\ M,\ \{w_i\},\ SIG_{CI})$$

証明書の正当な所有者は, 何度でも証明書を利用できる. 各主体の役割を図１に表す.

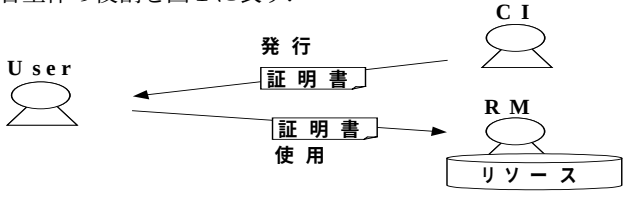

図１　匿名認証方式のモデル

2.3 発行・検証プロトコル

証明書の発行プロトコルおよび検証プロトコルについて, 処理手順を以下に示す.

発行プロトコル：

Step 1

User は公開鍵 P_U と秘密鍵 S_U のペアを生成し, 以下のように Z_j を計算（この計算はブラインド化処理を意味する）した後, 全ての{Z_j}を CI へ送信する.

$$Z_j = P_{CI}(r_j) \cdot g[g(P_U \| w_j) \| M] \quad (j = 1 \ldots N) \text{ for all } j$$

ここで, w_j, r_j は User の公開鍵 P_U を CI に秘匿するための乱数を, ‘・’は乗算を, ‘‖’はビット結合を, g( )は一方向性のハッシュ関数を, それぞれ表す. また, j, N は整数を表す.

Step 2

User は cut&choose の手順に従い, CI から開示要求のあった R 個の候補 Z_k（ここで k, R は整数を表す. $1 \leqq k \leqq R$, $R \leqq N$）について{r_k} および{$g(P_U \| w_k)$}を CI へ開示する. CI は開示された{r_k} および{$g(P_U \| w_k)$}から以下のように Z'_k を計算し, Z'_k と Z_k が一致することを確認する（これに失敗すると, User が不正に書き換えた M'に対する署名の取得を試みたとして本プロトコルを中止する）.

$$Z'_k = P_{CI}(r_k) \cdot g[g(P_U \| w_k) \| M]$$

Step 3

CI は開示されていない Z_i（ここで i は整数を表す. $1 \leqq i \leqq N\text{-}R$）に対して秘密鍵 S_{CI} を使用して S_{CI} $(\Pi_i Z_i)$を計算（この計算はデジタル署名を意味する）し, User へ送信する. ここで, ‘Π_i’は i について乗算することを表す.

Step 4

User は以下のように割り算（ブラインド解凍処理）

$$SIG_{CI} = S_{CI}\ (\Pi_i Z_i)/\Pi_i r_i$$

によって署名 SIG_{CI} を得る. User は P_U, M, {w_i}, SIG_{CI} を証明書として一組で保存する.

$$\text{証明書} = (P_U,\ M,\ \{w_i\},\ SIG_{CI})$$

検証プロトコル：

Step 1

RM は証明書に含まれる SIG_{CI} に対し, CI の公開鍵 P_{CI} を用いて $P_{CI}(SIG_{CI})$を計算する. 一方で RM は証明書に含まれる P_U, M, {w_i}から$\Pi_i g[g(P_U \| w_i) \| M]$を計算する. このとき, 以下を検証する（署名 SIG_{CI} が正しいものであるかどうかの検証）.

$$P_{CI}(SIG_{CI}) \mathrel{?=} \Pi_i g[g(P_U \| w_i) \| M]$$

（ここで“?=”は両辺が一致するかどうかを確認するという意を表す）

Step 2

RM は証明書に含まれる P_U を用いてチャレンジ・レスポンスを実施し, User が証明書の正当な所有者であることを確認する.

2.4 特徴

User が証明書の取得時に生成した P_U は, 証明書を一意に識別するためのキーになりうるが, User は発行プロトコル Step 1 におけるブラインド処理によって P_U を CI

から隠蔽しておくため，CI は P_U からその証明書の所有者である User を特定できない．このようにして，User の匿名性は RM だけでなく CI に対しても確保することができる．したがって，証明書の発行（CI としての業務）と証明書の検証（RM としての業務）を 1 つの主体が同時に実施したとしても，ユーザの匿名性は損なわれない．

３．実用化のための検討

匿名認証方式を実用化するためには，現在広く普及している ID とパスワードによる認証方式が実現している利点を，匿名認証方式においても実現できることが望ましい．ID とパスワードによる認証方式が実現している次の４つの利点を匿名認証方式で実現できるかどうかを検討する．

1) 認証情報（ID とパスワード，または証明書）の発行と検証は同一の主体であるサービス提供者（Service Provider：SP）が実施できる
2) SP はユーザの趣味・趣向を統計的に把握できる
3) ユーザはトラブル時などに認証情報を利用して自身の本人性を一意に立証できる
4) 認証情報の発行と検証は任意の時系列で実施できる

なお，以下では認証情報を用いてサービスを利用するユーザを“ユーザ”と表記し，特に匿名認証方式において証明書を使用する主体を“User”と表記する．

1) ID とパスワードの発行と検証を同じ主体が実施することは自然であり，コスト面でも有利である．匿名認証方式では，2.4 で説明したように，証明書の発行と検証を同一の主体が実施してもユーザの匿名性は損なわれないという特徴があるため，1) を実現することができる．これは ID とパスワードによる認証方式以外の他の方式と比較しても明らかである．表１に（A）PKI で規定する公開鍵証明書（およびアクセスコントロールリスト（ACL）や属性証明書）による認証方式，（B）SPKI 証明書を利用した認証方式[6,7]，（C）匿名認証方式を，証明書の検証者，および発行者に対するユーザの匿名性の観点からの比較を示す．なお，表１において○は匿名性が確保できることを，×は匿名性が確保できないことをそれぞれ表す．

表１：各認証方式が実現するユーザの匿名性

	検証者に対する匿名性	発行者に対する匿名性
⒜ 公開鍵証明書を利用した認証方式	×	×
⒝ SPKI証明書を利用した認証方式	○	×
⒞ 匿名認証方式	○	○

2) どのような属性をもつユーザがどのようなリソースにアクセスするのか，といった情報は，サービス提供者にとって，効果的なプロモーション活動や，広告収入につながると考えられる．これを満たすためには，匿名認証方式の証明書において，権限を表す M に権限の他にユーザの属性に関する情報を含めればよい．属性とは，性別や年齢層など，その情報自体からはユーザを特定できない程度のものを想定している．このようにして，匿名認証方式においても 2) を実現することができる．なお，属性が真正なものであることの確認は本稿の範囲外であるが，属性が真正なものであることを確認するための枠組みは属性認証局や属性証明書の枠組み[8]と組み合せることによって実現できる．

3) 本項目は，例えばサービスの利用中に何らかの事故等によって提供が中断された場合などのトラブル時に際し，ユーザが SP に対し本人性を一意に立証し，あらかじめ支払った料金のキャッシュバックを要求するなどの対処を可能にする．このためには，匿名認証方式において User が発行プロトコルの Step 1 で生成した r_j を全て保存しておき，トラブル時には r_j を用いて全ての Z_j を計算できることを CI および RM へ示せばよい．CI は発行プロトコルの Step 1 で保存していた Z_j と，User から提示された Z_j とを比較することで，この User の本人性を一意に確認することができる．したがって，匿名認証方式においても 3) を実現することができる．通常時には User はこの r_j を秘密に保存しておくため，本人性を一意に立証する際に，他の User がこの User になりすますことは困難である．

4) ID とパスワードの発行や検証は，通常，ユーザの要求に応じて任意のタイミングで実施される．匿名認証方式においても，User の要求に応じて任意のタイミングで証明書の発行と使用を認めることが望ましい．しかしこの場合，状況によっては User の匿名性が確保できなくなるという課題が発生する．したがって従来の匿名認証方式では 4) を実現することができない．この課題について次章で詳細を述べる．

４．運用モデルと課題

匿名認証方式では CI と RM の役割を同一のサービス提供者（SP）が担う場合，User と SP の証明書の発行，使用の時系列関係により２つの運用モデルが考えられる．

Model 1：証明書の発行期間と使用期間を明確に分離するモデル：

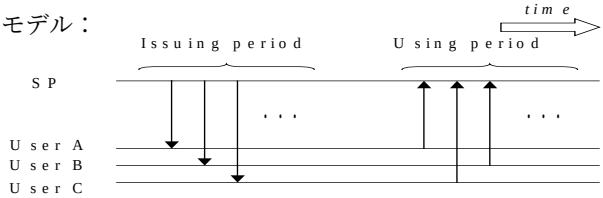

図２　Model 1

Model 2：任意のタイミングで証明書の新規発行と新規使用を認めるモデル：

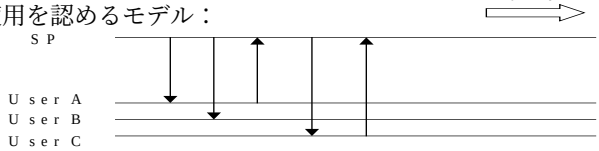

図３　Model 2

Model 1は証明書を電子的な投票に使用する投票券として使用する場合に適している．一方，Model 2 は証明書を電子的なチケットとして使用する場合に適している．

２つの運用モデルを「SP にとって User の識別がどれくらい困難であるか」の観点で評価する．Model 1 の場合，証明書を使用する User を X 人とすると，SP から見て，ある 1 枚の証明書が特定の User のものである確率は，全ての User に対して等しく 1/X となる．一方 Model 2 の場合，ある 1 枚の証明書が特定の User のものである確率は，その時点までに発行した証明書と，その時点までに使用された証明書の時系列関係に依存して変動する．例えば，図４のように２枚の証明書の発行(t1,t2)と使用(t3,t4)が発生した後，さらに 1 枚の発行(t5)と使用(t6)が連続して発生すると，t6 で使用された証明書が特定の User(User C)のものである確率は 1 となる．したがって Model 2 では User の匿名性が全く確保されなくなる場合があり得るといえる．すなわち，「発行された証明書が全て使用された後，新たに 1 枚だけ証明書が発行された状況」において，新たに発行された証明書は User の匿名性を確保できない．

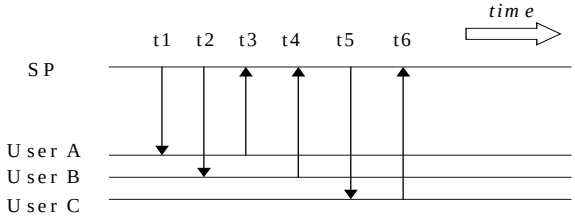

図４　User の匿名性が確保されなくなる場合

５．提案方式

本章では，前章での Model 2 における課題を解決する方式を述べる．課題を解決するため，既に使用された証明書の枚数(A1)を表す「使用済み証明書カウンタ」と，発行された枚数(A2)を表す「発行済み証明書カウンタ」を有し，この状況を User に通知する主体を設ける．この主体を「信頼できるカウンタ」（Trusted Counter：TC）と呼ぶ．TC は，User および SP の両方が信用する主体であって，A1 と A2 を正しくカウントするものとする．

以下では，TC が A1，A2 をカウントするために，証明書の発行時におけるブラインド署名の実施，および証明書の検証時におけるブラインド署名の検証を TC が代行するものとする．TC はブラインド署名の実施，検証のための公開鍵と秘密鍵（P_{TC} ，S_{TC}）のペアをあらかじめ生成し，P_{TC} を公開しておく．

提案方式では User, SP, TC の３つの主体を定義する．User は 2 章で述べた User と同じ主体である．SP は 2 章における CI と RM の役割を同時に持った主体である．TC は A1，A2 をカウントする主体である．SP と TC はそれぞれ SSL のサーバ証明書などの，認証局(CA)によって保証された既存の公開鍵証明書（以降サーバ証明書と呼ぶ）を保持するものとする．User は SP，TC 両方の会員となり，SP からパスワード $Passwd_{SP}$ を，TC からパスワード $Passwd_{TC}$ をあらかじめ受け取っておく．M は User が SP のサービスを利用する権限を表す．

以下に，証明書の発行プロトコルおよび検証プロトコルを述べる．

発行プロトコル（図 5）

Step I-1

TC と SP はあらかじめ共有鍵暗号系の共有鍵 key を共有しておく．

Step I-2

User と SP は M に合意し，User は SP へ身元情報とともに Z_j を送信する．なお，User は SP をサーバ証明書で認証し，SP は User を $Passwd_{SP}$ で一意に認証する．

$$Z_j = P_{TC}(r_j) \cdot g[g(P_U \| w_j) \| M] \quad (j = 1 \ldots N) \text{ for all } j$$

SP と User は 2 章の発行プロトコル Step 2 で実施したように cut&choose を行う．次に SP は$\{Z_i\}$を鍵付ハッシュ関数で以下のようにメッセージ認証子(MAC)を生成し，User へ送信する．

$$MAC = g(Z_1 \| Z_2 \| \cdots \| Z_i \| key)$$

Step I-3

User は MAC を受け取ると，TC へ MAC と，自身が保持している$\{Z_i\}$を送信する．このとき，User は TC をサーバ証明書で認証し，TC は User を $Passwd_{TC}$ で一意に認証する．

Step I-4

TC は key と User から受け取った$\{Z_i\}$によって MAC を検証する．

$$MAC \stackrel{?}{=} g(Z_1 \| Z_2 \| \cdots \| Z_i \| key)$$

これに成功すると，$S_{TC}(\Pi_i Z_i)$を計算し User へ送信する．また，TC は「発行済み証明書カウンタ」の値 A2 を１つカウントアップする．一方，検証に失敗したときは，User か SP のどちらかが不正をしているとしてプロトコルを中止する．

Step I-5

User は以下のようにして SIG_{TC} を獲得する

$$SIG_{TC} = S_{TC}(\Pi_i Z_i)/\Pi_i r_i$$

User は以下を一組として証明書を保存する．この形式は従来の匿名認証方式の証明書の形式と同じである．

$$\text{証明書} = (P_U,\ M,\ \{w_i\},\ SIG_{TC})$$

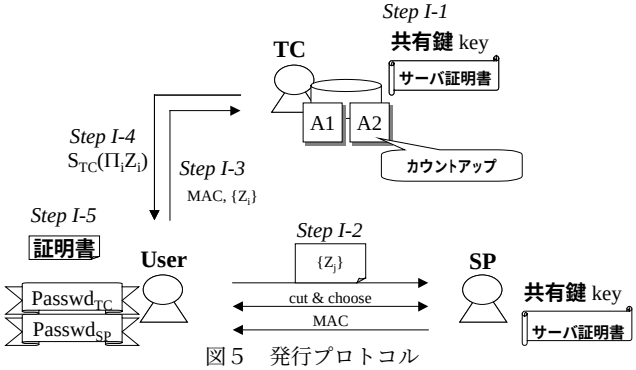

図５　発行プロトコル

検証プロトコル（図 6）

Step V-1

User は使用したい証明書の M のみを TC へ提示する．TC は A1 と A2 のカウントアップ状況を記憶しておき，「発行された証明書が全て使用された後，新たに 1 枚だけ証明書が発行された状況」となっていないことを User へ通知する．また，このとき TC は User へ証明書を要求する．なお，User は TC をサーバ証明書で認証する．一方，TC は User を一意に認証しない．

Step V-2

User は証明書を TC へ送信する．

Step V-3

TC は 2 章で述べた検証プロトコルに基づき証明書を検証する，これに成功すると，「使用済み証明書カウンタ」の値 A1 を 1 つカウントアップするとともに，SP へ「証明書の検証に成功した」ことを証明書とともに通知する．なお，一度証明書が使用されれば，以降はこの証明書の使用状況を TC が把握する必要はない．

Step V-4

SP は User へサービスを提供する．

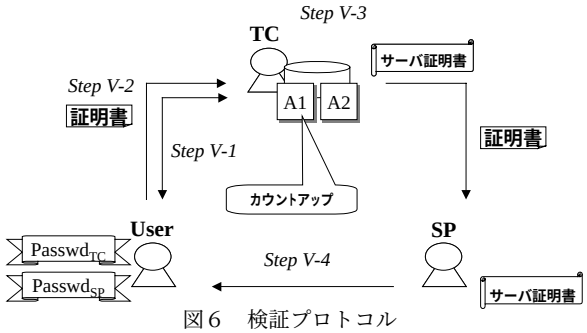

図６　検証プロトコル

6. 評価

本章では，提案方式について，実効的な匿名性に関する評価，TC の役割，SP の不正に対する考察について述べる．また，提案方式の有効な適用分野について考察する．

6.1 実効的な匿名性に関する評価

新規に SP から証明書を取得する User にとっては，SP に対し自分自身と識別不能な User がいるかどうかを Step V-1 において TC から知ることができる．したがって User は証明書から自分自身を一意に特定されることはない．なお自分自身と識別不能な User の数は(A2)-(A1)-1 に相当する．

6.2　TC の役割

匿名認証方式では CI がブラインド署名をするが，提案方式では TC が証明書の発行状況を正しく把握するため，TC がブラインド署名を実施するようにした．このため，ブラインド署名の元情報{Z_i}は SP から TC へ渡される必要がある．本稿では，SP が cut&choose によって確認済みの{Z_i}を，Step I-3 において一旦 User を介して TC へ渡している．Step I-2 における鍵付ハッシュ関数は，User が Z_i を TC へ送信する際，自分の都合のいいように{Z_i}を作り変えないようにするためにある．また，SP がでたらめな情報を TC に渡し，無効な証明書を作成させることを防ぐため，Step I-3 において User からも{Z_i}を TC へ提出させている．

TC は証明書の発行状況だけでなく，使用状況も把握する必要がある．このため，本方式では TC がブラインド署名の実施だけでなく，検証も実施するようにした．

TC を導入し，発行，使用状況をカウントすることで，User が証明書を取得し，これを使用する際，匿名性を確保できるタイミングを知ることができる．このタイミングは TC が能動的に全ての User へ状況を通知してもよい．

なお，TC は純粋に証明書の発行と使用状況を正しくカウントするための主体である．したがって，TC ですら一旦発行された証明書から，User を特定することはできない．

6.3　SP の不正に対する考察

本章では提案方式において SP が実施しうる不正に関して考察する．なお，User が実施しうる不正に関しては匿名認証方式[1,2]で述べられている以上のものはないため，考察の対象としない．

SP は TC を騙して A1 と A2 の数を不正に操作し，することで，User の匿名性を剥奪しようと試みる可能性がある．この不正な操作には 2 種類ある．1 つは (A2)-(A1)-1=0 の際，故意に「使用済み証明書カウンタ」の値 A1 を実際より少なくみせることである．これによって，新たに証明書を取得した User に証明書を使用させ，この User の匿名性を剥奪するというものである．しかし，User は TC へ証明書を送信し，TC から SP へ証明書の検証結果を通知するので，SP はこの操作を実施できない．

もう 1 つの不正な操作は，(A2)-(A1)-1=0 の際，故意に「発行済み証明書カウンタ」の値 A2 を実際より多くみせることである．このためには SP は一部の User と結託する必要がある．しかし，本稿では User と SP は利害関係上相異なる主体と考えるため，この場合はもともと本稿の対象外である．

6.4 適用分野に対する考察

ID とパスワードによる認証は最も普及している形態である．しかし，これは各ユーザへ一意の識別子を付与することになり，匿名性の確保は難しい．また，たとえ権限毎にユーザをグループ化し，グループ単位に作成した識別子でユーザを認証することで，ユーザを特定しないようにしたとしても，逆に，トラブル時などにユーザが自身の身元を主張することが困難になる．匿名認証方式または 5 章の提案方式は，ユーザの匿名性の確保とトラブル時のユーザの身元の主張を同時に実施できる点で優れている．

5 章の提案方式を有効に適用できる分野としては以下が考えられる.

P１. ユーザの権限に応じてアクセス制限をしたデジタルコンテンツを提供する分野

P２. プライバシが重要視されるサービスを提供する分野

P３. 証明書の発行者と検証者が同一の主体となる分野

逆に, 以下のような分野には適用が困難, あるいは適用の効果が低いと考えられる.

N１. 非常時などにおいて, ユーザの意思に無関係にユーザの匿名性を剥奪する必要がある分野

N２. 電子投票のように, 証明書の内容（投票内容）自体を秘匿する分野

N３. 電子現金のように, 証明書の内容（金額）に再利用性を認めない分野

P1, P3 の分野においては, 決済状況や特定の組織への帰属状況を認証することが考えられる. P2 の分野には, 映像コンテンツ配信産業, 医療・カウンセリング産業が考えられる. しかし, N1 を考慮すると, 結局, 医療・カウンセリング産業への適用は難しい. したがって, N2, N3 も考慮し, 総合的に考察すると, 証明書を実社会での映画の鑑賞用チケットに対応する, 電子チケットのようなものとして利用することが効果的であると考えられる.

7. 補足

著者らは[9]において, ユーザの IC カードにあらかじめ複数の証明書を格納しておき, そのうち実際に使用する証明書の枚数を SP に秘匿することで, 4 章で述べた課題を解決する方式を提案している. [9]の方式では, SP が「どのユーザが何枚の証明書を使用しうるか」を知らないため, 例え発行した証明書の総数と SP へ戻ってきた証明書の総数を SP に記憶させたとしても, 図 4 のような状況であるかどうかを把握させないようにしている. 5 章の提案方式と[9]の方式の比較・検討は今後実施する予定である.

8. むすび

本稿ではユーザの匿名性を認めたままその権利を認証する「匿名認証方式」のフィジビリティスタディを行い, 実用化に向けた検討を行った. また, 証明書を発行する主体と検証する主体が同一のサービス提供者であるとき, サービス提供者によるユーザの識別の困難性は運用モデルに依存し, 運用モデルによっては匿名性が全く確保されないユーザが存在しうるという課題を指摘した. さらに, 信頼できるカウンタを用いてこの課題を解決する方式を提案した. 今後は本方式についてさらに検討を進めるとともに, 他の基盤技術を適用した方式についても検討する予定である.

文献

[1] 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,p2138-2147 (2000)

[2] 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,p2138-2147 (2000)

[3] 飯田恭弘, 佐藤直之, 鈴木英明, ユーザを識別しない認証方式の実装, 情報処理学会第 61 回全国大会, 平成 12 年後期

[4] Chaum, D, Security without identification: transaction systems to make big brother obsolete, Communication of the ACM,Vol.28, No.10, pp.1030-1044 (1986)

[5] Chaum, D, Fiat, Naor, Untraceable Electronic Cash LNCS 403, pp.319-327 (1988)

[6] 斎藤孝道, 梅澤健太郎, 奥野博, プライバシを重視するアクセス制御システムの一方式, 電子情報通信学会誌 D-Ⅰ Vol.J84-D-1, No.11 pp.1553-1562 (2001)

[7] 梅澤健太郎, 斎藤孝道, 奥野博, プライバシを重視したアクセス制御機構の提案, 情報処理学会論文誌, Vol.42, No.8, pp.2067-pp.2076 (2001)

[8] Farrell, Housley, An Internet Attribute Certificate Profile for Authorization, RFC3281 (2002)

[9] 飯田恭弘, 上野正巳, 阿川雄資, “匿名認証方式”の運用における事実上の匿名性についての考察, 信学会全国大会, 平成 15 年前期, to be appeared