コンピュータセキュリティ　5－6
（1999．5．21）

プライバシ保護に注目した証明書を基盤とした認証システムの一方式

佐藤 直之　　鈴木 英明
NTT 情報流通プラットフォーム研究所

本稿では、プライバシ保護を重視した、証明書を基盤とした新たな認証システムを提案する。本方式では、認証は、ユーザと個人識別子とを結び付けるのではなく、ユーザと権利とを直接結び付ける。認証によって確認されるのは、端末の前にいるユーザが、権利を持っているか否かという情報だけである。本方式では、個々の権利は、各々別々の証明書を用いて証明する。ユーザは、その目的に応じて複数の証明書を持ち、これらを適当に使い分ける。また、証明書は、その正規のユーザしか利用できない。

本方式では、ブラインド署名や意味的安全 (強秘匿) な暗号などの暗号技術と、秘密情報を格納し、計算能力を有するユーザ携帯端末を用いる。

A new authentication system based on certificate, concentrating on privacy protection

Naoyuki Sato　Hideaki Suzuki
NTT Information Sharing Platform Laboratories

In this report, we concentrate on privacy protection and suggest new authentication system which utilizes certificates. The system uses certificates for confirming user's rights. But, no one can use them for acquiring some user's personal information(name or etc.). We can't acquire any information by the authentication, except for the information that says the user, in front of his terminal, has the right or not. We use one certificate for proving one right. Users can have many certificates for their purposes. The certificate can be used by its owner, and can't be used by others.

We use some cryptographic techniques(blind signature, semantically secure cryptosystem) and wearable user terminal, which can conceal some secret information and has some computational power.

1　はじめに

近年、公共広域電子ネットワークであるインターネットが普及し、多くの人々が社会生活の活動の一つとしてこれを利用するようになってきた。これに伴い、電子ネットワークにおける個人情報の管理手法、匿名性についての研究が数多く行われている。

一般に、ネットワークの利用において完全な匿名性が保証されるとすると、匿名者の行った犯罪等違反行為に対する防衛が難しい。一方、多くのユーザは、匿名性が否定されないことを願う。電子ネットワークでは情報を簡単に配布及び収集できるので、個人情報が不必要に漏洩することは、個人の社会生活に重大な被害を与える可能性もある。このように、個人情報についての問題は非常に繊細な面を持つ。

このような背景の中、本稿では認証に注目し、個人情報の保護と不正者への対応法を備えた新しい認証方式を提案する。以下では、便宜上、『個人情報』を次の二つに明確に区別する。

特徴情報：名前、住所、身長、体重、容姿、収入などの社会的あるいは身体的特徴についての情報。

行動情報：行動についての情報。行動履歴。

認証と行動情報との間には密接な関係がある。通常認証は、ユーザにとって、資源を利用するための準備の一つである。このため、認証を行うこと自体が、行動情報の漏洩をもたらす原因になりやすい。

本稿では、ユーザが自分の名前や ID などを明かさずに、ある権利を持っていることのみを証明できる方式を提案する。認証時に検証者側が得られる情報は、端末の前にいるユーザが、ある権利を持っているという情報のみである。検証者側は、ユーザが『誰』であるかはもちろん、『誰』であるかに容易に結びつく情報を得ることもできない。ユーザの行動に結びつく全ての情報は、ユーザ自身の管理下にあり、例え名前がわからない匿名者としてでも、その行動を監視することはできない。本稿の方式では、これらの特徴によって行動情報を完全に保護する。また、行動情報と特徴情報が、ユーザの知らない間に収集及び結合できないことも保証する。

本稿ではこのような特徴を持った認証システムとして、証明書を基盤とした方式を提案する。個人の

個々の権利は、各々別々の証明書を用いて証明する。同一ユーザに対して発行された複数の証明書は、それぞれ完全に独立しているように見えるので、証明書を媒介として特徴情報や行動情報を収集することはできない。また、証明書の利用資格制限、無効化、ユーザ単位での無力化など不正行為に強い耐性を持つ。

次章では、本稿で取り扱う世界のモデルと、プロトコルの設計目標を述べる。第3章では利用する基盤的な技術を、第4章では提案するプロトコルを説明する。第5章で安全性などの特徴について検討し、第6章で関連研究を、第7章でまとめを行う。

2 世界モデルと目標機能

2.1 世界モデル

本稿の世界モデルは、四つの要素からなる (図1)。

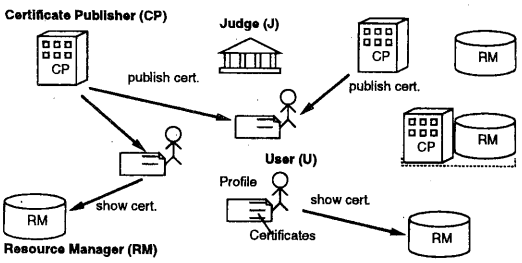

図 1: 世界モデル

証明書発行局 Certificate Publisher (CP)
ユーザの権利 (特徴) を保証する証明書を発行。

資源管理者 Resource Manager (RM)
資源を管理する。権利の検証を行う存在。

ユーザ User (U)
資源の利用者。証明書を管理し適当に利用する。

裁判官 Judge (J)
調停役。主に不正に対する防衛のため存在する。

上記のモデルでは、一つの証明書を複数の RM で共用することを許している。現在一般的な、資源ごとに個人パスワード等を設定する手法は、図中右側の CP と RM がペアになった場合に相当する。

2.2 目標機能

本稿では以下の機能を満たす認証方式を提案する。

(1) 認証時の特徴情報の漏洩防止とその制御可能性
認証実施時において、どの特徴情報が検証者側 (RM) に伝わるかを、ユーザ自身が制御できる。

(2) 行動の追跡不能性とその制御可能性
任意数の CP と RM が結託したとしても、行動が把握されうる範囲を、ユーザが制御できる。

(3) 証明書再利用性
証明書は何度でも使用できる。

(4) 証明書不正利用不可
証明書は正規のユーザ以外は利用できない。

(5) 任意の証明書の無効化
CP は、発行した任意の証明書を無効にできる。

(6) 任意のユーザの無力化
J は任意のユーザについて、このユーザに発行された全ての証明書を同時に無効にできる。

3 基盤となる各種技術

提案方式では4つの重要な基盤的技術を利用する。

3.1 ブラインド署名

CP が、発行した証明書を利用して情報収集するのを避けるため、ブラインド署名法を利用する [2]。

以下に、ブラインド署名に関係する四つの関数を定義する。上から二番目の関数は署名者が実行し、最後の関数は署名の検証者が実行する。残る二つは署名を要求するユーザが実行する。S は署名生成鍵 (署名者の秘密鍵)、P は署名検証鍵 (同公開鍵)、m は署名を行う文書、s は m の署名情報である。

- ブラインド関数 $Blind(P, m, r)$
  r は任意の乱数。$m' = Blind(P, m, r)$。r が未知なら、m'から m を導出できない。
- 署名関数 $Sign(S, m')$
  ユーザに示された情報 m'に対して署名を実行する関数。$s' = Sign(S, m')$。
- ブラインド削除関数 $Unblind(P, s', r)$
  署名 s を取り出す関数。r は関数 $Blind$ 実行時に選択した r である。$s = Unblind(P, s', r)$。
- 検証関数 $Verify(P, m, s)$
  公開鍵 P を用いて署名 s を検証する関数。

$$Verify(P, m, s) = \begin{cases} 1 & (s \text{ が } m \text{ の署名の場合}) \\ 0 & (\text{上記以外の場合}) \end{cases}$$

$Verify(P, m, Unblind(P, Sign(S, Blind(P, m, r)), r)) = 1$ である。ブラインド署名の実現法は幾つか提案されているが、RSA を利用した方法が有名である。

3.2 意味的安全な公開鍵暗号

本提案方式では、発行局を問わず、同一ユーザに対して発行する全ての証明書には、全て同じ識別情報を埋め込む。この情報は不正発覚時などに、ユーザを特定するために利用する。この目的で、次の条

件を満たす意味的安全(強秘匿)な公開鍵暗号系を利用する。また、この関数を以下のように記述する。

[条件] 暗号文と公開情報のみを用いて、同じ平文を持つ他の暗号文を容易に生成できること

- 暗号生成関数 $E_{crypt}(e,m,r)$
  公開鍵 e を用いて文書 m の暗号文を作成する関数。m の暗号文は多数存在するが、r によって一意に決定する。$c = E_{crypt}(e,m,r)$。
- 復号関数 $D_{crypt}(d,c)$
  暗号文 c を秘密鍵 d で復号し、文書 m を取り出す関数。$m = D_{crypt}(d,c)$。
- 暗号変換関数 $Conv_{crypt}(e,c,t)$
  公開鍵 e と暗号文 c より、同じ平文を持つ別の暗号文を生成する関数。$c' = Conv_{crypt}(e,c,t)$ で、t は c'を一意に決定する。

秘密鍵を知らなければ、意味的安全性より (c,c') と $(c, E_{crypt}(e,m',r"))$ $(m \neq m')$ の区別は容易でない。

上記の条件を満たす暗号としては、ElGamal 暗号 [5, 12]、岡本龍明らの暗号 [10] などがある。

3.3 確率的符号判定手法

本提案方式では、あるユーザに対して発行された全ての証明書を同時に無効にできるようにするために、以下に示す特殊な符合化手法を利用する。

有限集合 ID、C、R、及び集合 $B = \{0,1\}$ において、$x, x' \in ID$、$c, c', c" \in C$、$r, r', r" \in R$ とする。

- 符号生成関数 $E_{code}(x,r) : ID, R \rightarrow C$
  x の符合 c を作成する。同一 x に対する符合の候補は複数あり、r を用いて一意に指定する。符号からは、その元 x の情報がほとんど得られない。特に、$c = E_{code}(x,r)$、$c' = E_{code}(x,r')$、$c" = E_{code}(x',r")(r \neq r', x \neq x')$ とすると、(c,c') と $(c,c")$ の違いを容易に判別できない。
- 判定関数 $D_{code}(x,c) : ID, C \rightarrow B$
  $c = E_{code}(x',r)$ の場合、以下の式が成り立つ。

$$D_{code}(x,c) = \begin{cases} 1 & (x = x' \text{の場合}) \\ 0 & (\text{上記以外の場合}) \end{cases}$$

また、前節の暗号に対する条件と同様に、ある符号 cに対して、これと同じ元 x を持つ別の符号 c'を容易に計算できることとする。この関数を $Conv_{code}(c,t)$ とおく。t は c'を一意に指定する。

$D_{code}(x, E_{code}(x,r)) = 1$ である。定義より、元 x を知らなければ、二つの符合 c と c'が同一の元を持つかどうかすらわからない。この関数の具体例としては、Diffie-Hellman 決定問題の困難性 [4] に根拠を置いた方法等がある[1] 。

[1] p を素数、$1 < x < p-1$、t を $p-1$ と素な乱数とする。

$E_{code}(x,r) = (a\ (mod\ p), a^x\ (mod\ p))(r$ より原始根 a 生成)
$D_{code}(x,(c_0,c_1)) = 1$ ($c_0^x = c_1 (mod\ p)$ の時) or 0(左記以外)
$Conv_{code}((c_0,c_1),t) = (c_0^t\ (mod\ p), c_1^t\ (mod\ p))$
注意: c_0^tは原始根となる。

3.4 秘密情報の格納媒体

本提案方式では、主としてユーザ自身による証明書の不正な利用を防止する目的で、ユーザごとに異なった秘密の情報を格納し、定義した計算の結果のみを出力する物理媒体 *B-box* を利用する。IC カードなどはこの条件を満たす媒体である。

B-box は関数として定義できるので、証明書発行時及び利用時の通信経路は、図 2 のようになる。

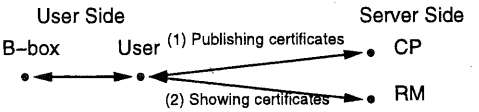

図 2: 通信のモデル

4 提案方式

4.1 各構成要素の役割と初期状態

証明書発行局 CP : 証明書に対して署名(ブラインド)を行う。CP は各々鍵ペア (P_{CP}, S_{CP}) を持ち、公開鍵 P_{CP}を公開している。

資源管理者 RM : RM は認証時の検証者となる。

ユーザ U : U は、各々自分の *B-box*(以後 B と表記) を持ち、自分の証明書を管理し利用する。

各 B には、あらかじめ個別の識別子 ID_B が割り当てられている。B は始めに、これが正しく動作することを保証する証明書(「B の正当性」の証明書) を添付して、U に渡される。ID_Bはこの証明書に埋め込まれているが、J の秘密鍵で暗号化されており、J 以外は読み取れない(後述)。

また、B は署名を行うための鍵ペア (P_B, S_B) を最低一つ持つ。鍵ペアの数は、所有者 U の意志で自由に増減できる。ただし、B 自身が鍵ペアを作成し、秘密鍵 S_B^iは誰にも教えない。

裁判官 J : J は 3.2 節の暗号系で使用する鍵ペア (e_J, d_J) を持ち、公開鍵 e_Jを公開している。また、「不正 B リスト」と「無効証明書リスト」(共に始めは空) を持ち、公開している。

4.2 証明書の構成

証明書 CS(Certificate Set) は以下の六つの要素から構成される。なお、ここではユーザの j 番目の証明書 CS^jに対する要素を示している。

i. 署名 s^j : CP の発行した署名情報
   s^jは紙の証明書における「印」に対応する。

ii. B の公開鍵 P_B^i : 証明書の利用条件となる鍵 P_B^iは、CS^jを利用できるユーザを一意に指定する。紙の証明書での「顔写真」などと対応する。鍵は各々複数の証明書の利用条件にできる。このために P_B^iのサフィックスは iで、jではない。

iii. 証明事項 M_{CP}^j : 証明書が保証する内容 紙の証明書での文書部分と同じ。

iv. ID_Bの暗号文 $E_{crypt}(e_J, ID_B, r^j)$:$B$ の情報識別子 ID_Bの、裁判官の鍵 e_Jによる暗号文。

v. ID_Bの符号 $E_{code}(ID_B, r'^j)$: B の情報識別子 ID_Bの符号。

vi. 指数 c^j: 詳細は下記プロトコルを参照のこと

上記の iv と v の情報は、匿名性を採り入れた本認証方式において、不正対策のために利用する。

証明書 CS^jを利用する際には、P_B^iに対応した秘密鍵 S_B^iも必要となる。S_B^iを知るのは一つの B だけで、この B を持つのは正規のユーザ U だけである。従って、正規のユーザしか証明書を利用できない。

4.3 証明書獲得プロトコル

以下に、U が j 番目の証明書 CS^jを 獲得するプロトコルを示す。プロトコル開始前に、U と CP の間で、証明事項 M_{CP}^jとパラメータ N_{CP}に合意しているとする。B 自身の正当性を証明するためのデータは、サフィックスを y(鍵番号は y') としている。

関数 g は適当な一方向性ハッシュ関数とする。

(1) U は「B の正当性」を保証する証明書から適当なもの CS^yを選ぶ。U は、M_{CP}^jと、新しい証明書 CS^jの利用条件としたい鍵の番号 i、CS^yの鍵の番号 y'、$E_{crypt}(e_J, ID_B, r^y)$、$E_{code}(ID_B, r'^y)$、$P_{CP}$、$e_J$、$N_{CP}$を B に送る。

(2) B は、以下の値 Z^k, W^kを N_{CP}個作成する。ここで u, v, w, c, x は任意の乱数、|| は結合を表す。

$$X^k = Conv_{crypt}(e_J, E_{crypt}(e_J, ID_B, r^y), u^k) \quad (1)$$

$$Y^k = Conv_{code}(E_{code}(ID_B, r'^y), v^k) \quad (2)$$

$$Z^k = Blind(P_{CP}, g(P_B^i||c^{j,k})||X^k||Y^k||M_{CP}^j, w^k) \quad (3)$$

$$W^k = E_{crypt}(e_J, w^k, x^k) \quad (4)$$

B は、秘密鍵 $S_B^{y'}$を用いて式 (5) の文の署名 s_Bを作成し、s_Bと $Z^k, W^k, u^k, v^k, w^k, c^{j,k}, x^k$を全て U に送る。

$$Z^1||Z^2||...||Z^{N_{CP}}||W^1||W^2||...||W^{N_{CP}}|| E_{crypt}(e_J, ID_B, r^y)||E_{code}(ID_B, r'^y)||M_{CP}^j \quad (5)$$

(3) U は全ての Z^k, W^kと s_B、CS^yを CP に送る。

(4) CP は、J の公開する二つのリストを用いて、CS^yの有効性を調べる (詳細は後述)。また、次式 (6) が成り立つかを調べる。ここで P_{CP}^yは CS^yを発行した証明書発行局の公開鍵である。

$$Verify(P_{CP}^y, m^y, s^y) = 1 \quad (6)$$

(但し、$m^y = g(P_B^{y'}||c^y)||E_{crypt}(e_J, ID_B, r^y)||E_{code}(ID_B, r'^y)||M_{CP}^y$)

CP は署名 s_Bも確認する。全てに合格した場合、CP は $k'(0 < k' \leq N_{CP})$ を選び U に送る。

(5) U は、$k \neq k'$となる全ての k について、u^k, v^k, w^k, x^kと $g(P_B^i||c^{j,k})$ を CP に送る。

(6) CP は、(5) で受け取った情報を用いて、(3) での情報 $(Z^k, W^k(k = k'$は除く)) が正当な手順で作成されていたかを検証する。

CP は以下の値 s'を計算し U に送る。CP は s'と $W^{k'}$を保存する。

$$s' = Sign(S_{CP}, Z^{k'}) \quad (7)$$

(7) U は以下の値 s^jを計算し、証明書 CS^j として六つ組 $(s^j, P_B^i, M_{CP}^j, X^{k'}, Y^{k'}, c^{j,k'})$ を得る。

$$s^j = Unblind(P_{CP}, s', w^{k'}) \quad (8)$$

4.4 証明書提示プロトコル

証明書を提示し利用する手順は以下の通りである。

(1) U は証明書 CS^jを RM に送る。

(2) RM は CS^jについて三つの検証を行う。

- 以下の式が成り立つことを確認する。

$$Verify(P_{CP},\ g(P_B^i||c^j)||E_{crypt}(e_J, ID_B, r^j)|| E_{code}(ID_B, r'^j)||M_{CP}^j,\ s^j) = 1 \quad (9)$$

この検証の合格は、「公開鍵 P_B^iと対応した秘密鍵を持った存在について、CP が事項 M_{CP}^jを保証している」ことを意味する。

- 既存の公開鍵署名を利用した認証手順を用いて、ユーザ側 (即ち B) が公開鍵 P_B^iに対応した秘密鍵 S_B^iを保持していることを確認する。
- J の公開する二つのリストを用いて、CS^jの有効性を調べる。この詳細は次節で説明する。

4.5 証明書無効化手法

4.5.1 証明書の無効化

CP は、無効とする証明書に対応した s'と $W^{k'}$を J に送る。J は、秘密鍵 d_Jを用いて、$W^{k'}(= E_{crypt}(e_J, w^{k'}, x^{k'}))$ から $w^{k'}$を取り出す。証明書発行時に U が受け取った署名 s^jは、$s^j = Unblind(P_{CP}, s', w^{k'})$ となるので、J はこの s^jを計算し、「無効証明書リスト」に登録する。このリストに登録された s^jが含まれる証明書は、無効である。

4.5.2 ユーザの無力化

Jは、特定Uに対して発行された全ての証明書を同時に無効にできる。Jは、このために、目的のUに対して発行された証明書を一枚入手する。Jは、この証明書に含まれる情報$E_{crypt}(e_J, ID_B, r^j)$より、秘密鍵$d_J$を用いて、$U$の持つ$B$の識別子$ID_B$を導出する。$J$は$ID_B$を「無効$B$リスト」に登録する。

ある証明書において、証明書に含まれる$E_{code}(ID_B, r'^j)$が、無効Bリストに登録されたID_Bの一つと対応している場合、即ち以下の式が成り立つ時この証明書は無効である。

$$\exists k : D_{code}(ID_B^k, E_{code}(ID_B, r'^j)) = 1 \qquad (10)$$

5 安全性及び機能についての検討

本提案方式の特徴を (1) 証明書の偽造、(2) 証明書の不正利用、(3) 証明書の運ぶ情報、の三つの点から検討する。

5.1 証明書の偽造

証明書はそれぞれ六つの要素より構成されているが、署名s^jを除く各要素は、公開情報のみを用いて、誰でも自由に作成できる。従って、証明書の偽造は、署名s^jの偽造とほぼ等価である。

署名の偽造の可能性は、下位で使われる具体的な署名方法に大きく依存する。このため、プロトコルで利用する署名方法を決定する場合には、署名方法自体のもつ本質的な欠点を考慮し、必要なら欠点を補うようにプロトコルを修正しなければならない。

Bの行う署名s_BとB自身の正当性を保証する証明書CS^yは、ブラインド署名を行うCPが、自分が署名する文書の中身 (の一部) を確認するためにある。「Bの正当性」を保証する証明書は、正しい動作のみを行うBに対して発行しなければならない。

ここで、「Bの正当性」を保証する証明書の条件である公開鍵$P_B^{y'}$に対する秘密鍵$S_B^{y'}$を入手した者は、Bの動作を真似て不正を行える可能性があることに注意を要する。通常、公開鍵署名法では、公開鍵から秘密鍵を導出することは計算量的に難しい。だが、物理的にBを分解するなどの別の手法を用いて秘密鍵を入手することは可能かも知れない。

このような事態が発生した場合、秘密鍵を入手した者は、次の証明書獲得時において、以下の五種類の情報の偽造が可能である。

- M_{CP}^j：任意の内容を保証する証明書
- P_B^i：任意の鍵を条件とした証明書
- $E_{crypt}(e_J, ID_B, r^j)$： 不正$B$摘発を妨害
- $E_{code}(ID_B, r'^j)$： Bの無力化を妨害
- CPの保存する$W^{k'}$： 証明書の無効化を妨害

このうち、P_B^i以外の偽造については、証明書発行時にN_{CP}を母数とした"Cut & Choose"の手法を用いることで防止している。P_B^i以外の偽造が成功する確率は$1/N_{CP}$である。逆に、この偽造行為が発覚する確率は$(N_{CP}-1)/N_{CP}$である。N_{CP}の値は、CPが保証する内容に応じて適切に定めなければならない。S_B^iが物理的に簡単には導出できないことを仮定すれば、多くの場合、$N_{CP}=1$で十分だと予想する。この場合、証明書獲得プロトコルの"Cut & Choose"の部分は全て省略できる。また、指数c^j及び関数gの一方向性も必要なくなる (後述)。

P_B^iの偽造については、プロトコル中では対応していない。しかし、P_B^iが偽造された証明書が発見された後には、その証明書に含まれる情報から、当該ユーザ及び証明書の無効化を行うことができる。

5.2 証明書の不正利用

証明書CS^jを利用する時には、CS^jに含まれる公開鍵P_B^iに対応する秘密鍵S_B^iが必要である。従って、S_B^iをB以外が知らないとすれば、証明書を利用するためには、B自身が必要となる。また、Bを持つのは、証明書の正規のユーザUのみである。

盗難対策としては、B自身がUに対する認証手段を備えていることが好ましい。だが、いずれにせよ、証明書が不正に利用されたことが分かった後には、無効化の手段を採ることができる。

5.3 証明書の運ぶ情報

証明書CS^jの持つ情報について考える。まず、署名s^j以外の全ての要素は、誰でも自由に作成できるので、正しい署名s^jが含まれない証明書は全く情報がない。正しい署名s^jを含む証明書は、各要素の結び付きを、署名者CPが保証することを示す。

ところで、CPは、ユーザについての多くの特徴情報をあらかじめ知っているかもしれない。名前や電話番号、支払い能力などの情報は、証明書を発行するためにCPが要求する情報であることが予想できる。だがCPは、これらの特徴情報を、証明書CS^jと結び付けて不当に利用することができない。CPは証明書発行時に目隠しをしたまま (ブラインドで) 署名を行うので、同じ内容M_{CP}^jを保証する証明書を複数のユーザに発行した場合、その各々の所有者が誰なのかわからない。関数gの一方向性と乱数c^jは、"Cut & Choose"によってP_B^iがCPに知れないためにある。P_B^i以外の三つの要素$(X^k, Y^k, c^{j,k})$は、N_{CP}個の署名候補で各々異なり、またこれらは

秘密鍵 d_J を知らない限り、乱数と区別がつかない。CP は s' と $W^{k'}$ も知っているが、d_J を知らないのでこれらを直接には利用できない。

以上の考察より、J を除いた全ての存在に対して、証明書がもたらす情報は、『CP が公開鍵 P_B^i に対応した秘密鍵 S_B^i を持った存在について、事項 M_{CP}^j を保証している』という内容だけであることがわかる。これは、証明書に署名を行った CP 自身に対しても成り立つことが重要である。この性質より、任意の数の CP と RM が結託しても、ユーザの特徴情報と行動情報とを結び付けることは困難となる。

ただし、ユーザが同一証明書を複数回利用した場合は、証明書をインデックスとして、RM や CP がユーザの行動の一部を監視できる。この問題は、ユーザが、同一内容を保証する証明書を複数枚保持し、適宜に使い分けることによって容易に解決できる。また、同一鍵ペア (P_B^i, S_B^i) を複数の証明書に対する条件として利用した場合、P_B^i をインデックスとして行動を監視できる。このため、ユーザは鍵の利用範囲を適宜に調節しなければならない。このように、行動情報の公開度合をユーザ自身が決定し操作することは、自然かつ必要なことと考えている。

以上の全ての検討より、本提案方式は、第2章の機能を満たしている。本方式では、裁判官という特権階級が存在することも大きな特徴の一つである。

6 関連研究

電子ネットワーク上での認証処理における匿名性の実現法は、1986年に D. Chaum によって初めて原始的な手法が紹介された [2]。この論文で、Chaum はブラインド署名を提案し、電子現金の方向性を示した。その後、匿名性は、電子現金の分野で活発に議論され、採り入れられている ([3, 1, 13] 等)。これらの分野では、電子現金 (証明書に相当) が重複して利用されると、その利用者の名前が判別可能となる手法を用いて、匿名性と不正対策を両立しているものが多い。この手法はとても有効だが、本方式のように証明書に再利用性が必要な場合には利用できない。プロトコルの一部として、*B-box* のような要素を用いる方法は、[1] などでも提案されている。

意味的安全な暗号の定義と実現方法は、S. Goldwasser らによってに示された [9]。これらについても積極的に研究されている。本研究では特に [8, 12, 10] などを参考とした。確率的符合の定義は本稿独特のものであるが、暗号における意味的安全性と対応する形で決定している。

ユーザの公開鍵を認証時に識別子として利用する手法については、SDSI[11] や SPKI[6, 7] などでも検討されている。ただし、これらは個人情報の保護をその対象とはしていない。

7 まとめ

本稿では、プライバシ保護を重視し、証明書を基盤とした新たな認証システムを提案した。本方式では、個々の権利を各々別々の証明書で証明する。証明書は、権利と個人とを直接結び付ける。証明書はそれぞれ完全に独立しているように見えるので、これを媒介として個人の特徴情報を収集できない。また、ユーザ自身が適当に制御を行うことによって、他人がユーザの行動情報を調べることは難しい。さらに証明書はその正規のユーザしか利用できない。

今後は、特に証明書の無効化部分について検討を加え、より効率的で安全な方法を模索していく。

参考文献

[1] Stefan Brands. Untraceable Off-line Cash in Wallet with Observers. *CRYPTO'93*, 1993. LNCS 773, pp.302-318.

[2] D. Chaum. Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Commun. of ACM*, Vol. 28, No. 10, 1986. pp.1030-1044.

[3] David Chaum, Amos Fiat, and Moni Naor. Untraceable Electronic Cash. *CRYPTO'88*, 1988. LNCS 403, pp.319-327.

[4] W. Diffie and M. Hellman. New direction in cryptography. *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, Nov. 1976. pp.644-654.

[5] T. Elgamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, July 1985. pp.469-472.

[6] Carl M. Ellison. Establishing Identity Without Certification Autorities. In *6th USENIX Security Symposium*, July 1996.

[7] Carl M. Ellison, Bill Frantz, and et al. *SPKI Certificate Theory*, Nov. 1998. Internet-Draft, draft-ietf-spki-cert-theory-04, work in progress.

[8] Shafi Goldwasser and Mihir Bellare. Lecture Notes on Cryptography, 1997. http://www-cse.ucsd.edu/users/mihir/.

[9] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *journal of computer and system sciences*, Vol. 28, 1984. pp.270-299.

[10] Tatuaki Okamoto and Shigenori Uchiyama. A New Public-Key Cryptosystem as Secure as Factoring. *Eurocrypt'98*, 1998. LNCS 1403, pp.308-318.

[11] Ronald L. Rivest and Butler Lampson. SDSI - A Simple Distributed Security Infrastructure, Apr. 1996. http://theory.lcs.mit.edu/~cis/sdsi.html.

[12] Yiannis Tsiounis and Moti Yung. On the Security of ElGamal Based Encrypsion. *PKC'98*, 1998. LNCS 1431, pp.117-134.

[13] 岡本龍明, 太田和夫. 理想的電子現金方式の一方法. 電子通信学会論文誌 (D-I), Vol. J76-D-I, No. 6, June 1993. pp.315-323.