情報システム 51－4
（1994．10．18）

証明書類の電子化とセキュリティ技術

榊原 裕之　田代 太一　安倍 紀之
岡田 謙一　松下 温

慶應義塾大学 理工学部 計測工学科

現在は光ファイバなどの高度通信網の整備が進んでいるが、これらの通信環境が整えば将来はテレショッピング、在宅勤務、（テレビ電話による）通信教育等が盛んになると期待されている。これらの通信網を利用したサービスにの一つとして、自治体の取り扱う証明書を電子化（デジタル化）することにより家庭の端末にて通信で証明書を申請・取得し、さらに他機関へ提出できるという便利なサービスが考えられる。

本稿では、自治体の発行する証明書類を電子化したものを電子証明書と定義し、これらを通信を用いて申請・発行・取得・提出する場合のプロトコルと必要となるセキュリティ技術について論ずる。

Electronic certificates and security

Hiroyuki Sakakibara　Tai-ichi Tashiro　Noriyuki Abe
Ken-ichi Okada　Yutaka Matsushita

Department of Instrumentation Engineering, Faculty of Science and Technology, Keio University

3-14-1 Hiyoshi Kohoku Yokohama 223, JAPAN

Currently, high performance network infrastructure such as optical fiber is developed, and in near future this infrastructure will supply new services to general users, for example, tele-shoping, telecommuting, and correspondence courses based on communication and so on . By means of dijitalizing certificates which local governments issue, namely “electronic certificates”, thus, a new convinient service where residents can get electronic certificates from local governments and submit them to others at home using their (personal) computer through tele-communication network will be realized.

This paper propose that protocols and security schemes for management(application, acquiring, issue, submission) of electronic certificates issued by local governments.

1 はじめに

マルチメディア時代の到来が期待される現在、ビデオオンデマンド、在宅勤務、テレショッピング、テレビ会議等、場所・時間という拘束から解放されるべくしたネットワークの利用方法が提案されている。将来的には、Fiber to The Home が実現されれば、これらの提案が実現され、我々の生活はより便利なものになるであろう。そこで、我々はこの将来的な展望の元に、地方自治体が管理、発行している証明書類（住民票、課税証明書等）をデジタル情報として扱い（以下、電子証明書）ネットワークを通して住民が家にいながらにして証明書を取得できるにはどのような方法があるかを検討してきた [1]。つまり、我々が目指すものは **"地域住民は、家庭にいて自宅端末よりネットワークを通して証明書取得の申請を行い、 地方自治体はこれを受信すると、電子証明書をネットワークを通して住民へ送る。住民は、送られてきた電子証明書を、自宅端末より、ネットワークを通して提出先（例えば、銀行など）へ送る。"** というものである（図 1）。通信を用いた電子証明書の 申請・発行・取得・提出 が実現されれば移動の手間や時間が省けるなどの利点が生じる。本提案では以上に述べた電子証明書の通信での取扱いに必要なプロトコルとセキュリティ技術について述べる。

提案の前提条件として各家庭にコンピューター端末が普及し、ネットワークと接続されている（Fiber to The Home 等）こと、各エンティティが RSA[2] 等の同種の公開鍵暗号の鍵（公開、秘密）を所持していること、電子証明書の使用が認められる法制度の整備がなされていることを仮定する。

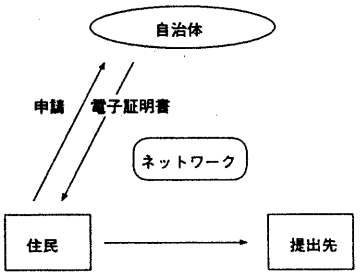


図 1: 提案の概念図

2 電子証明書のための情報と技術

2.1 電子証明書

本提案における電子証明書とは、現在紙媒体の証明書をデジタル情報として扱ったものである。

通常、証明書は複製不可能な特殊な用紙に

- 証明内容の表示
- 証明書発行者（自治体）とその印鑑の表示

の二点が記載されている。この特殊な用紙により、証明書の偽造と複製の防止がなされている。現存の証明書では、その安全性はこの紙にあるといえる。

一方、我々の定義する電子証明書では記載内容は現存の証明書のものと同じであるが、自治体が発行しているという証拠として公開鍵暗号系による（自治体の）デジタル署名を付加する（図 2）。公開鍵暗号 によるデジタル署名は、本人しか知らない秘密鍵によりデータに特殊な計算＝署名を行うために、**秘密鍵の値が他人に洩れない限りは、他人がなり済まして署名を行うことはできず，証明書の偽造が出来ない。**従ってこの性質を通常の印鑑として用いることが出来る。詳細は 3 章に述べる。

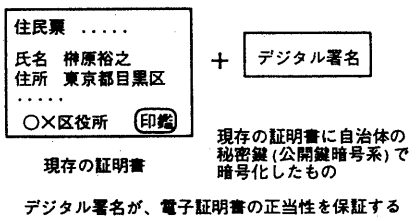


図 2: 電子証明書

2.2 現存の証明書の取得には何が必要か

証明書の取得のためにはどのような情報が必要かを、東京都目黒区役所をモデルにとり検討してみる。以下に記すのは、目黒区において取得できる証明書類の申請時に必要な情報である。すなわち、申請書に記入すべき必要事項とその他必要な提示物などである。必要事項が記入された申請書は区役所あるいはその出張所窓口へ提出される。

証明書の申請に必要な情報

1. 印鑑登録証明書以外の証明書（住民票、課税証明証等）の申請
   (a) 申請者の住所・電話番号等, (b) 被証明者の住所・電話番号等
   (c) 認め印, (d) 請求本数・種類等,
   (e) 使い道（目的・提出先）(f) その他（備考）

を申請書に記入し窓口に提出する（申請者と非証明者が異なる場合は委任状が必要な場合もある）。

2. 印鑑登録証明書の申請
(a) 印鑑登録番号、(b) 登録者の住所、氏名、生年月日、性別
(c) 申請者の住所、氏名、(d) 必要な本数
を記入した印鑑登録証明書交付申請書と (e) 印鑑登録証（カード）
を同時に窓口に提出する。

2.3 電子証明書の申込みに必要な情報

家庭の端末よりネットワークを通して電子証明書の取得の申請を行うための必要な情報を 2.2より検討する。

住民票など印鑑登録証明書以外の証明書の申請
2.2 に述べたものと同じ。ただし，認印は住民の公開鍵暗号系によるデジタル署名を用いて実現する。

印鑑登録証明書の申請 印鑑登録番号、登録者の住所、氏名、生年月日、性別、申請者の住所、氏名必要な本数。印鑑登録証（カード）についてはこのカードを所持している人が申請の資格を持っていることから、登録者がデジタル署名を付加することにより代替できる。

申し込みをネットワークを通じておこなう場合は、以上の情報を家庭の端末から入力し専用のフォーマットに従いパケット化して送信する。また，デジタル署名を印鑑（認め印）として用いることにより、現存の申請書の作成よりも確実に申請者の身元を証明できる。

※本提案では委任状に関する対応は考慮していない。現在の申請時に委任状が必要な場合は、(本人の) 証明書を取得したい本人が窓口に申請にこれずに、代理人に頼む場合である。本提案では、通信にて証明書を申請するので、そのような代理を頼む事態は考慮に入れていない。

3 電子証明書のプロトコル

図3 に、電子証明書の申請、発行、取得、提出のためのプロトコルを 示す。この図では、申請、発行、取得、提出までを示してある。以下に、プロトコルの表現に必要な表記を記す。

3.1 表記

記法	
KP_X	エンティティX の RSA の公開鍵
KS_X	エンティティX の RSA の秘密鍵
$E_k\{M\}$	M を鍵 k により暗号化する
$Sign_{U_i}\{M\}$	M をU_iがデジタル署名する
$h()$	一方向性ハッシュ関数（公開）
ID_X	エンティティ X の ID
SN	通し番号
Ts	タイムスタンプ
N	乱数

A ‖ B は A と B を連結することを示し、暗号化においては以下の式が成り立つ。

$$E_{KP_X}\{E_{KS_X}\{M\}\} = E_{KS_X}\{E_{KP_X}\{M\}\}$$

$Sign_X\{M\}$ では、実際には、

$$Sign_X = E_{KS_X}\{h(M)\} \parallel M$$

となる。デジタル署名のチェック（検証）は、

$$E_{KP_X}\{E_{KS_X}\{h(M)\}\} = h(M)$$

として得られた、h(M) と、デジタル署名と連結されていた M をハッシュ関数にかけて得られた h(M) とを比較し、一致したならば検証は成功したとみなされる。

3.2 電子証明書の表記

電子証明書は以下のようにして表される。J を自治体とすると

$$Sign_J\{\text{証明書} \| Ts \| SN\}$$

記法中の “証明書” は、現存の証明書と同じ記載事項をもつものである。これに、タイムスタンプ Ts、通し番号 SN を付加し、前述の表記 $Sign\{\}$ の方法に従いデジタル署名を施したものである。

3.3 申請・発行・取得 ステップ

図 3にこのステップのプロトコルを示す。ここで、自治体を J、ユーザー（住民）を U_i、証明書の提出先を機関 U_kとする。

ユーザーは、申込書（自治体で決められたフォーマットでアプリケーションとして提供される）に 2.3 節で述べた必要事項を書き込む（入力）。現行で、認め印がいる申請の場合は $Sign$ が認め印のかわりをする。申込書の書き込みが終了したら、以下のフォーマットのデータを Req とする（図 3）。

1 ユーザー U_i は以下の Req を生成する。

$$Req = E_{KP_J}\{ID_J \| ID_{U_i} \| Sign_{U_i}\{\text{申込書}\} \| N_1\}$$

2 Req を自治体 J に送信する（申し込み）。

3 自治体は、U_i から、Req を受けとると、自治体の秘密鍵 KS_J により Req の復号を行う。このとき、
$ID_J \| ID_{U_i} \| Sign_{U_i}\{$ 申込書 $\} \| N_1$
が得られる。自治体は、一番目のパラメータ と二番目のパラメータから ID_{U_i} で示されるエンティティ U_i から、ID_J で示されるエンティティ J、即ち自分へのメッセージであることを確認する。従って依頼主が U_i であることを知る。次に U_iの公開鍵 KP_{U_i} により、$Sign_{U_i}\{$ 申込書 $\}$ を検証する。さらに申し込み内容を読み、U_i が正当に本人の証明書を請求していることが確認できたなら、自治体は必要な電子証明書を作成する。

4 自治体は
$Rep_1 = E_{KP_{U_i}}\{ID_{U_i} \| ID_J$
$\| Sign_J\{$ 証明書 $\| Ts \| SN\}$
$\| Sign_J\{$ 受領書 $\} \| N_1 \| N_2\}$
を作成する。受領書は **"U_i は、U_i に発行された SN=8970xx Ts=1994/6/15 の住民票 を受領しました"** という記述である。

5 自治体は Rep_1 を、U_i に送る。

6 U_i は Rep_1 を受信すると KS_{U_i} より復号を行う。
$ID_{U_i} \| ID_J \| Sign_J\{$ 証明書 $\| Ts \| SN\}$
$\| Sign_J\{$ 受領書 $\} \| N_1 \| N_2$
を得る。$ID_{U_i} \| ID_J$ より、自治体 J から U_i へのメッセージであることを知る。次に証明書と受領書のデジタル署名の検証を自治体の公開鍵 KP_J により行う。検証が成功したら

7 $Rep_2 = E_{KP_J}\{ID_J \| ID_{U_i} \|$
$Sign_{U_i}\{Sign_J\{$ 受領書 $\}\} \| N_2 \| N_3\}$
を作成して、

8 Rep_2 を自治体 J へ送る。これは、ユーザーが希望の証明書の受領通知となる。

9 J は Rep_2 を KS_J 復号化し、
$ID_J \| ID_{U_i} \| Sign_{U_i}\{Sign_J\{$ 受領書 $\}\} \| N_2 \| N_3$
を得る。$Sign_{U_i}\{Sign_J\{$ 受領書 $\}\}$ の署名の検証が成功したならば、自治体 J は、$Sign_{U_i}\{\}$ から、U_i が希望の証明書を受領したとみなす。
受領書_$U_i = Sign_{U_i}\{Sign_J\{$ 受領書 $\}\}$
とし、証明書管理用データーベースに
ID_{U_i} SN Ts 証明書内容 受領書_U_i
と記録する。以上の登録が完了すると、発行された証明書が効力をもつ。

10 次に、証明書が効力を持ち、使用可能状態になったことを U_i に通知するために、$Validcert$ を生成する。
$Validcert = E_{KP_{U_i}}\{ID_J \| ID_{U_i}$
$\| Sign_J\{$ 使用許可書 $\}\}$

11 自治体 Jは Validcert を U_iに送る。

12 U_iは $Validcert$ を検証し成功すれば、始めて証明書を使用することができる。なお、使用許可書は **"U_i に発行された SN=8970xxx Ts=1994/6/15 住民票 は使用可能です"** という内容の記述とする。

3.4 提出ステップ

図 3 で U_i が取得した証明書をある機関 U_kに提出する場合の手続きを示す。

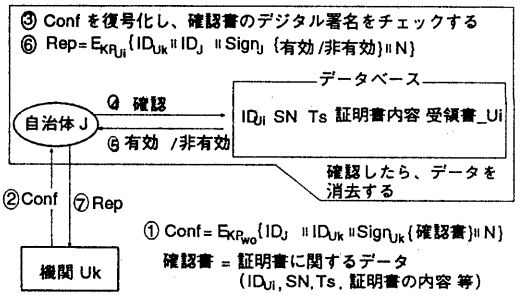


図 4: 電子証明書の有効性を確認するプロトコル

1. U_i は 以下の Sub を生成する
$Sub = E_{KP_{U_k}}\{ID_{U_k} \| ID_{U_i} \| Sign_{U_i}\{$ 提出届け $\}$
$\| Sign_J\{$ 証明書 $\| Ts \| SN\} \| N_4\}$
ここで、提出届とは **"U_iが SN=8970xxx Ts = 1994/6/15 住民票を U_kに提出します"** という内容の記述とする。
2. U_iは Sub を提出先の機関 U_k に送る。
3. U_k は Sub を KS_{U_k} で復号し、提出届の署名を KP_{U_i} で検証し、提出されてきた証明書に関する情報を確認する。
4. 次に、自治体から発行された自治体の署名つき証明書 $Sign_J\{$ 証明書 $\| Ts \| SN\}$ を有効かどうかを確認する。何故ならば、この証明書は、U_i が故意に複製して送りつけたものである可能性があるからである。証明書の有効性の確認については 3.5節で詳述する。
5. U_k は有効性の確認の結果により受領の場合は
$Rec_{ok} = E_{KP_{U_i}}\{ID_{U_i} \| ID_{U_k}$
$\| Sign_{U_k}\{$ 受領通知 $\} \| N_4\}$
を，受領拒否の場合は
$Rec_{no} = E_{KP_{U_i}}\{ID_{U_i} \| ID_{U_k}$

$\|Sign_{U_k}\{$ 受領拒否 $\}$
$\|Sign_J\{$ 証明書 $\|Ts\|SN\}\|N_4\}$
を U_iに送信する。

3.5 有効性確認ステップ

有効性の確認を行うために以下のプロトコルを示す(図 4)。

1 ユーザー U_i から証明書を受けとった 機関 U_k は、
$Conf = E_{KP_J}\{ID_J\|ID_{Uk}$
$\|Sign_{Uk}\{$ 確認書 $\}\|N\}$
を生成する。確認書の内容は、ユーザー U_i から送られてきた証明書が有効かどうかを依頼する内容の表記で、**"U_iに発行された SN=8970xxx、Ts=1994/6/15、住民票 の証明書は有効か ?"** という内容の記述である。これに、デジタル署名を施す。

2 $Conf$ を自治体 J にネットワークを通して送る。

3 J は U_k より $Conf$ を受けとると KS_J で復号化し、U_k の公開鍵 KP_{U_k} を用いて
$Sign_{Uk}\{$ 確認書 $\}$ を検証する。

4 検証に成功したならば、確認書の内容に従い、自治体内にある、証明書管理用のデータベースを検索し、該当するデータが存在したならば、その正当性をチエックする。もし、U_k が U_i から受信した電子証明書 $Sign_J\{$ 証明書 $\|Ts\|SN\}$ が正当に発行されたものであれば、このデータベースにはデータが存在する。次に、**"データが存在したのならば、内容が確認の依頼をされた 電子証明書の内容と一致するかを検証して、正当なものであると判断したのならば登録データを削除する"** という手続きをとる。

5 4 の正当性の確認の結果で、有効か非有効をデータベース内の情報より判断し、

6 $Rep = E_{KP_{Ui}}\{ID_{Uk}\|ID_J$
$\|Sign_J\{$ 有効/非有効 $\}\|N\}$
を生成する。$Sign_J\{$ 有効/非有効 $\}$ の部分では、有効/非有効の表現は、例えば **" Ui に対して発行された、 SN=8970xxx、Ts=1994/6/15 の住民票 は 有効（非有効）である。"** という表現である。

7 自治体は Rep を Uk へ送る。

4 安全性の検討

4.1 通信途中での盗聴について

通信の途中で盗聴された場合は、データはすべて公開鍵暗号系を使用し、送信先の公開鍵で暗号化しているので、安全である。

4.2 証明書の偽造について

証明書は必ず、自治体の秘密鍵によるデジタル署名がなされ、自治体の公開鍵により検証されるので、偽造は不可能である。一般に自治体の秘密鍵が漏洩しない限りは偽造できない。

4.3 証明書の申請時のなりすましについて

例えば、A さんが B さんの印鑑証明書を得たいとする。電子証明書の場合は、申込時に必ず、申請者のデジタル署名が施されるようになっているので、A が B の秘密鍵を知らない限りはなり済ましはできない。どの証明書にも限らずこのことはいえるので、デジタル署名を用いた認証を行えば、なりすましは防げる。

4.4 複製した電子証明書の利用について

電子証明書の場合は、前述のように、公開鍵暗号系を利用して通信中のデータを保護するので、盗聴されても安全である。従って、提案したプロトコルが正常に機能すれば、他人に自分の電子証明書類が渡ることはない。ところが、電子証明書はその名の通りにデジタル情報なので複製が可能である。ここで問題となるのは、ユーザーが自分のために発行された 1 枚の電子証明書を複製して、1 枚分の料金で、何枚分も利用してしまうことである。

この問題を解決するために、提案プロトコルでは、証明書管理用データベースを設け、発行時に証明書に関するデータを登録し、あるユーザーの提出先の機関はユーザーから証明書を提出されたら必ず自治体へ電子証明書が有効かどうかを確かめてもらう方法を取っている。

図 5に、複製を利用した場合にどのようになるかを表してある。

ユーザー U が機関 A に正当な 証明書 1 を、機関 B に 証明書 1 のコピーである証明書 2 を提出したとする。機関 A の証明書の有効性の確認の問合せが、B より早いとする。

1. 機関 A は受信した証明書の有効性を確認するために自治体に問い合わせると、自治体はその証明書が発行済みとしてデータベースに登録されていることで、証明書が有効であることを知る。なぜなら、正当に発行された証明書は発行時に発行済みとしてデータベースに登録されるからである。機関などから確認の問い合わせがない限り、あるいは有効期限が切れない限りは登録は削除されない。確認が済んだら、データベースより 証明書 1 の登録を削除し、Uに "（証明書が）有効" の通知を送る。

2. 機関 B は A と同様に、自治体に証明書の有効性を確認する。しかし、1 で A が先に確認を行っているので自治体は有効な証明書として登録されていた 証明書 1 のデータをすでに削除している。従ってその複製である 証明書 2 のデータは、データベースには存在しないので、自治体は非有効な証明書と判断をする。この結果が機関 B に返され、U が複製を利用したことが判明する。

各証明書はタイムスタンプ Ts（発行日時）と、通し番号 SN を持つので自治体のデータベースには同じ住民（ユーザー）に対して同種の証明書を複数発行していてもそれぞれ区別されて登録される。

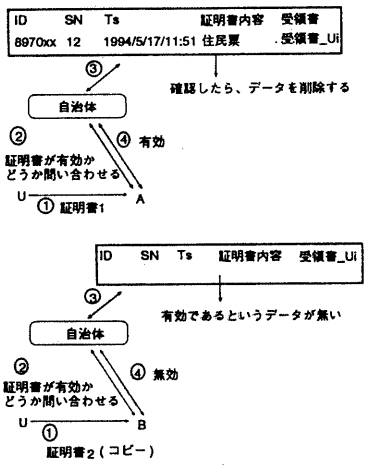


図 5: 複製の使用防止

問題点

ここで、問題となるのは、自治体が問い合わせを受けたら、有効であるというデータを削除してしまうので証明書を提出先でタライ回しできないということである。なぜなら、図 5で、A がさらに他の機関 C に証明書を回した場合、C は受けとった時点で、そのA から回ってきた証明書が、コピーかどうか調べなくてはならない。ここで、自治体に問い合わせても自治体のデータベースにはデータが残っていないので（A が前に問い合わせたから）有効な（コピーでない）証明書を受けとっても、無効であると返答されてしまうのである。

5 証明書のたらい回しについて

以上説明したプロトコルは、一つの証明書が一つの機関のみに提出されるという前提が必要である。そこで、ユーザーが証明書を提出した機関が更に他の機関にその証明書を提出した場合、つまり “証明書のたらい回し” が発生した場合について適用できるプロトコルを構築する。

5.1 多重署名によるたらい回し

多重署名を利用した文書の閲覧等が提案されている [3]。同様の考え方で、証明書のたらい回しをデジタル署名を多重に用いて実現する方法を示す。今、ユーザー U_iが 3.3に従って電子証明書を取得し、3.4に従い機関 A に提出したとする。

1. 機関 A が地方自治体に証明書の正当性の確認を 3.5 に従い行う。
2. 次に、A が B へ証明書を提出する場合には、メッセージ M_A= “提出者 U_i、受取者 A、A が正当性を確認した” を電子証明書に連結しデジタル署名を施す。
   $KP_B\{ID_B \| ID_A \| Sign_A\{$ 提出届 $\}$
   $\| Sign_A\{Sign_J\{$ 証明書 $\| Ts \| SN\} \| M_A\}\}$
   これを、B に送る。
3. B は A から送られてきたデータの A のデジタル署名を検証し、更に証明書の自治体のデジタル署名を検証する。以上の検証に成功したらメッセージ M_B= “提出者 A、受取者 B、証明書を確認した” を付加し B のデジタル署名を施して
   $KP_C\{ID_C \| ID_B \| Sign_B\{$ 提出届 $\}$
   $\| Sign_B\{Sign_A\{Sign_J\{$ 証明書 $\| Ts \| SN\} \| M_A\}$
   $\| M_B\}\}$
   を C に送る。
4. これを繰り返す。

この場合、タライ回しの途中で証明書に問題が生じた場合に一番最初に証明書の正当性を確認する A に責任が集中する可能性がある。また、タライ回しの回数が増えると送るデータ量が徐々に増す。

5.2 “提出先確認書” と “提出先申請書” による電子証明書のタライ回しの実現

これを解決するために、“提出先確認書” と “提出先申請書” を、用いる方法を提案した。以下に解説する。

申請・発行・取得 ステップ

まず、3.3 **申請・発行・取得 ステップ** における 4 の Rep_1 を

$Rep_1 = E_{KP_{U_i}}\{ID_{U_i} \| ID_J \|$ 証明書$_{U_i}$
$\| Sign_J\{$ 受領書 $\} \|$ 提出先確認書 $1 \| N_1 \| N_2\}$

と置き換える。ここで，U_i に発行された証明書は表記の簡潔化のために

証明書$_{U_i}$ = $Sign_J\{$ 証明書 $\| Ts \| SN\}$

とする。また，提出先確認書1は，その証明書が何処へ向けて提出されるべきであるかを示したものであり，自治体のデジタル署名が必ずつく。自治体Jは提出先がどこであるかをU_iがJに送信した申込書の記入から知ることができる。この場合，

提出先確認書1 $= Sign_J\{ID_{U_i}\|Ts\|SN$
$\|U_i \rightarrow A\|$ 証明書内容 $\}$

となっており，対になっている証明書がどこへ提出されるべきかを示すつまり，この 証明書$_{U_i}$ は U_i からAへ提出されることを示す。また、同ステップの9において証明書管理用データベースの登録情報を

ID_{U_i} SN Ts $U_i \rightarrow A$ 証明書内容　受領書$_U_i$

と変更する。以上の変更を行って、**3.3の申請・発行・取得ステップ 1-12** と同じ通信を行う（図6の1-5)。

提出ステップ

U_i は

$KP_A\{ID_A\|ID_{U_i}\|Sign_{U_i}\{$ 提出届 $\}$
$\|$ 証明書$_{U_i}\|$ 提出先確認書1$\}$

をAに送る（図6の6)。

Aが他の機関に証明書を回す場合のプロトコルを次に解説する。

タライ回しステップ

図6の7-11

7 Aは提出届のU_iの署名より送り元をU_iを認証する。次に，自治体に問い合わせて証明書が有効かどうかを調べてもらい、有効であれば回す先を指定するために“提出先申請書”を生成する。Bに回す場合，

提出先申請書1 $= Sign_A\{ID_{U_i}\|Ts\|SN$
$\|U_i \rightarrow A\|A \rightarrow B\|$ 証明書内容 $\}$

提出先申請書1は以上の表記になる。$U_i \rightarrow A$ は提出先確認書1より，自治体がU_iからAに対する証明書として発行したものであることを示す。A→Bは，AからBに回すことを示す。Aは提出先申請書1を以下のフォーマットで自治体Jへ送る。

$KP_J\{ID_J\|ID_A\|$ 提出先申請書1$\}$

8 自治体は送り主がAであることを認証し，データベースを検索する。データベースの登録情報の，$U_i \rightarrow A$ からこの証明書がA宛てであることを確認する。ここでは，正当な提出先であるAが，さらに他へ回そうとしていることを確認する。従ってこの時点では，自治体は証明書の有効性を確認することになる。提出先申請書1に基づき，データベースを以下のように更新する

ID_{U_i}，SN，Ts，A → B 証明書内容

9 次に，自治体は新しい提出先確認書2を以下のフォーマットでAに送る。

$KP_A\{ID_A\|ID_J\|$ 提出先確認書2$\}$
提出先確認書2 $= Sign_J\{ID_{U_i}\|Ts\|SN$
$\|A \rightarrow B\|$ 証明書内容 $\}$

この確認書が送られてくることで，証明書が有効であることと，Bに回す正当性を得たことになる。

10 Aは提出先確認書2を受け取ると，以下のフォーマットでBに送る。

$KP_B\{ID_B\|ID_A\|Sign_A\{$ 提出届 $\}$
$\|$ 証明書$_{U_i}\|$ 提出先確認書2$\}$

11 Bが他機関Cに回す場合は，Aと同様の作業をすればよい。以降これを繰り返す。

仮に、Aがこれ以上回さない場合は上記ステップの2において、提出先申請書1の5番目の要素 $A \rightarrow B$ を $A \rightarrow A$ と変更すれば良い。つまり，証明書を受け取った機関がその証明書を他機関へ回さない場合は、証明書の宛先を自分にした提出先申請書を 上記ステップの2、3の様に作成して自治体へ送る。自治体はこの様な提出先申請書を受け取った場合にはその証明書に関するデータを削除すればよい。

6 おわりに

本稿では、自治体の発行する証明書をデジタル化した電子証明書を定義しこれを 申請・発行・取得・提出する場合に必要なセキュリティを考慮したプロトコルを提案した。プロトコルの構築はなるべく現存の証明書の流れにそったものにしたが、証明書を受けとった機関が自治体にその正当性を確認するという部分は現存の証明書の取扱には見られない。また、タライ回し用のプロトコルにおいては自治体が証明書の流れを把握できるという点でプライバシーの問題が生じる可能性がある。

謝辞

本研究に関して貴重な御意見を頂きました、三菱電機株式会社、三菱電機東部コンピュータシステム株式会社の皆様に心より御礼申し上げます。

参考文献

[1] 榊原, 江田, 関, 岡田, 松下, “電子化された証明書類の取得と提出に関する提案”, 情報処理学会第48回（平成4年前期）全国大会予稿集, 4-293, 4-294

[2] 辻井・笠原 編著, “暗号と情報セキュリティ”, 昭光堂, 1990.

[3] 小林, 岡本, 桜井, 富樫, 佐伯, 伊串、“検印付き電子メールによる回覧システム”, 情報処理学会第45回（平成4年後期）全国大会予稿集, 4-269, 4-279

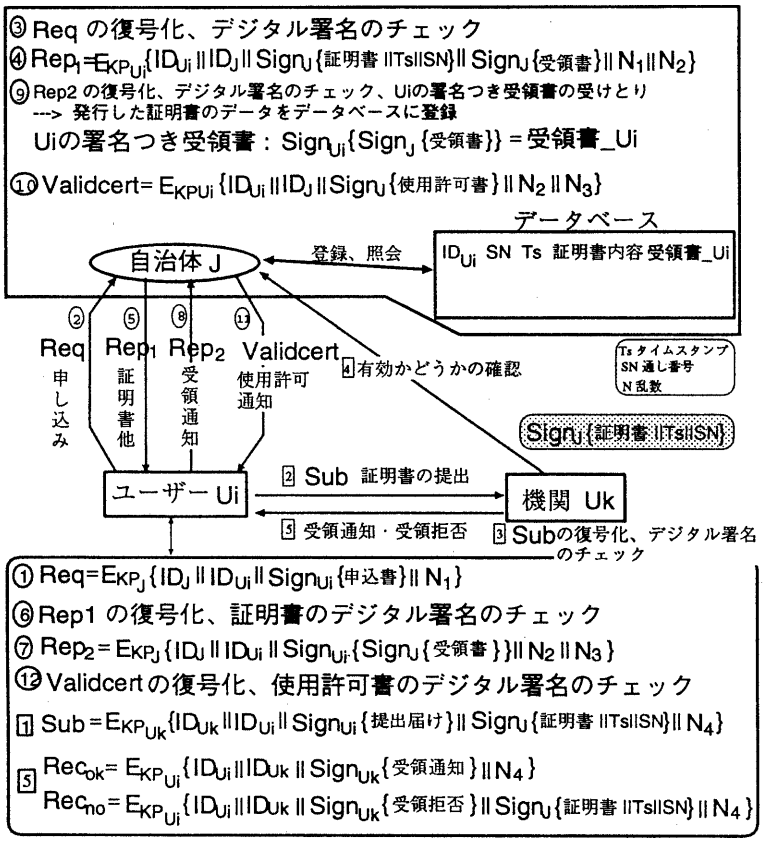
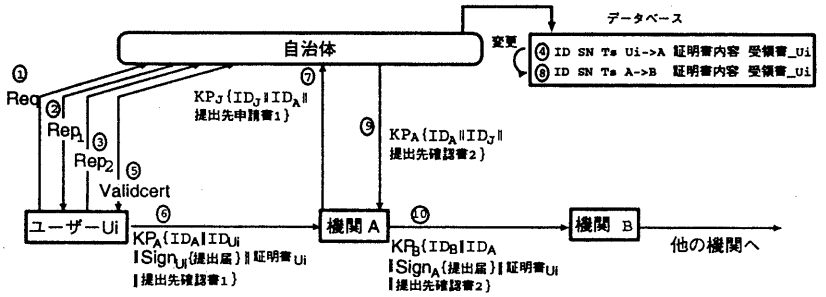


図 3: 電子証明書 申請・発行・取得 プロトコル



証明書Ui=SignJ{証明書‖Ts‖SN} : Uiのために自治体Jが発行した証明書

* Req, Rep2, Validcert 図3に同じ

* Rep1= KPUi{IDUi‖IDJ‖証明書Ui‖SignJ{受領書}‖提出先確認書1‖N1‖N2}

* 提出先確認書1= SignJ{IDUi‖Ts‖SN‖Ui->A‖証明書内容}
提出先確認書2= SignJ{IDUi‖Ts‖SN‖A->B‖証明書内容}
提出先申請書1= SignA{IDUi‖Ts‖SN‖Ui->A, A->A‖証明書内容}

* SN, Ts は 証明書Ui に記載されているものと同一とする

図 6: タライ回しを考慮したプロトコル