ネットワークを利用した電子化証明書発行システムのための安全なプロトコルに関する提案*

5N－7　田代 太一　安部 紀之　榊原 裕之　岡田 謙一　松下 温†

慶應義塾大学 理工学部‡

1　はじめに

我々はネットワークを利用したサービスの一つとして、自治体の発行する証明書を電子化し、住民が家庭に居ながらにしてこれを入手するシステムの提案を行なってきた [3]。本稿では公開鍵暗号系と秘密鍵暗号系を組み合わせることでこのサービスを利用するユーザの利便性と安全性を確立し、さらに自治体に電子証明書の正当性の問い合わせを行なうことで電子証明書の使い回しを可能にする方法について提案する。

2　セキュリティ技術と記法

証明書類の電子化において、その内容の正当性と安全な転送を実現するには、暗号技術が必要となる。暗号系として、ここではDESとRSAを利用する [1]。

表記はISO Directory, X.509 [2] で定義されている表記方法を用いる。ただし、DESの暗号化に関しては新しく追加してある。

記法

$X_P[M]$	X の公開鍵 X_p で M を暗号化する
$X_S[M]$	X の秘密鍵 X_s で M を暗号化する
$E_{DK}[M]$	DES の鍵 DK で M を暗号化する
$h()$	一方向性ハッシュ関数
M_1, M_2	メッセージ M_1 と M_1 を連結する
$X\{M\}$	Xのデジタル署名付データ

ここで、$X\{M\} = M, X_S[h(M)]$ である。

また、認証方式とDES鍵の配送については、ISO Directory, X.509 [2] で定義されている厳密認証方式を応用した。例えば A が Xの署名付きのデータ $X\{M\} = M, X_S[h(M)]$ を Bに送るときは以下のようにする (t=タイムスタンプ,r=乱数):

$A\{t, r, A, B, B_P[DK]\}$,
$E_{DK}[t, r, A, B, M], B_P[t, r, A, B, X_S[h(M)]]$

データを Mと $X_S[h(M)]$ に分割し、Mは DES で (最近はTriple DES が推奨されているがここでは、暗号化は一回とする)、$X_S[h(M)]$ は RSA で暗号化する。DESの鍵は送信先の公開鍵で暗号化して認証トークン中に入れる。Bは $A\{...\}$ を検証し、DKを得、後続の部分を復号する。そして得られた Mと $X_S[h(M)]$ を連結して $X\{M\}$ として、デジタル署名の検証を行う。

3　電子証明書の定義

電子証明書は以下のように定義される [3]。

- 電子証明書=画像化証明書+発行年月日 (TS)+通し番号 (SN)

また実際の有効な電子証明書は、自治体の印鑑に相当するデジタル署名部が付加されて、J｛電子証明書｝となる。

4　プロトコル

プロトコルを図1に示す。

J｛電子証明書｝の発行ステップ

1. 証明書の申請 ($U \rightarrow J$)
住民 Uは申請内容と提出先 “A” を “申請書” として、U｛申請書｝を自治体 Jに送る。

2. 電子証明書・提出先確認書の発行 ($J \rightarrow U$)
自治体 Jは申請書の内容と正当性を検証して、問題がなければ J｛電子証明書｝と、その提出先を保証した J｛提出先確認書$_1$｝を発行する。ただし、
提出先確認書$_1$ $= U, CertID, SN, TS, U \rightarrow A$
$CertID$ = 証明書識別番号 (住民票=1 等とする)
で、Uが取得する J｛電子証明書｝は U,CertID,SN,TS で一意に区別され、この J｛電子証明書｝は Uから Aに提出されることを示す。また、J｛受領書｝も同時に送信する。ただし、
受領書 = "Uは $U, CertID, SN, TS$で識別される証明書を受領しました"
となる。

3. J｛電子証明書｝の受領通知 ($U \rightarrow J$)
住民 Uは J｛電子証明書｝の内容と正当性を検証し、問題がなければ J｛受領書｝の内容を確認して、J｛受領書｝にデジタル署名を施して ($U\{J\{$受領書$\}\}$ となる)J に送り返す。

4. 使用許可証の発行 ($J \rightarrow U$)
Jは $U\{J\{$受領書$\}\}$ の Uのデジタル署名を確認して証明書管理用データベースにUに送った J｛電子証明書｝の詳細と $U\{J\{$受領書$\}\}$ を登録し、J｛使用許可書｝を送る。ただし、
使用許可書 = "$U, CertID, SN, TS$で示される証明書の使用を許可します"
となる。

J｛電子証明書｝の提出ステップ

5. 証明書の提出 ($U \rightarrow A$)
Uは J｛電子証明書｝を J｛提出先確認書$_1$｝とともに機関 Aに提出する。

6. 正当性の確認及び提出先の申請 ($A \rightarrow J$)
機関 Aは J｛電子証明書｝と J｛提出先確認書$_1$｝の内容を検証し、J｛電子証明書｝の正当性 (複製でないこと) を Jに問い合わせる。その際に次の提出先 “B” を申請するための A｛提出先申請書$_1$｝を提出する。ただし、
提出先申請書$_1$ $= U, CertID, SN, TS, A \rightarrow B$
である。

7. 検証結果の返答 ($J \rightarrow A$)
Jはデータベースを参照し、提出先 (この場合、A) と A｛提出先申請書$_1$｝の申請者 “A” との一致を調べる。一致していれば、$U \rightarrow A$ を $A \rightarrow B$に変更して、J｛提出先確認書$_2$｝を発行する。ただし、
提出先確認書$_2$ $= U, CertID, SN, TS, A \rightarrow B$
である。“一致していない、またはデータベースに登録がない場合” は該当する J｛電子証明書｝は無効であり、デジタル署名を施した無効通知を A に送る。

8. 受領結果の返答 ($A \rightarrow U$)
機関 A はJからの返答に基づき、Uに証明書の受領または受領拒否（デジタル署名付き）を通告する。

機関 A がさらに機関 Bに J｛電子証明書｝を提出する場合 (証明書の使い回し)、A は Uと同じように J｛電子証明書｝と J｛提出先確認書$_2$｝を Bに提出する。受け取った Bは Aと同様に Jに問い合わせる。提出先申請書の内容は、この先さらに別の機関 “C” に提出を行うなら “$U, CertID, SN, TS, B \rightarrow C$” とし、$J$はこれに従ってデータベースを更新して新しい提出先確認書を発行する。

---

*A proposal of secure protocol for electronic certificates system
†Taichi Tashiro, Noriyuki Abe, Hiroyuki Sakakibara, Kenichi Okada, Yutaka Matsushita
‡Faculty of Science and Technology, Keio University

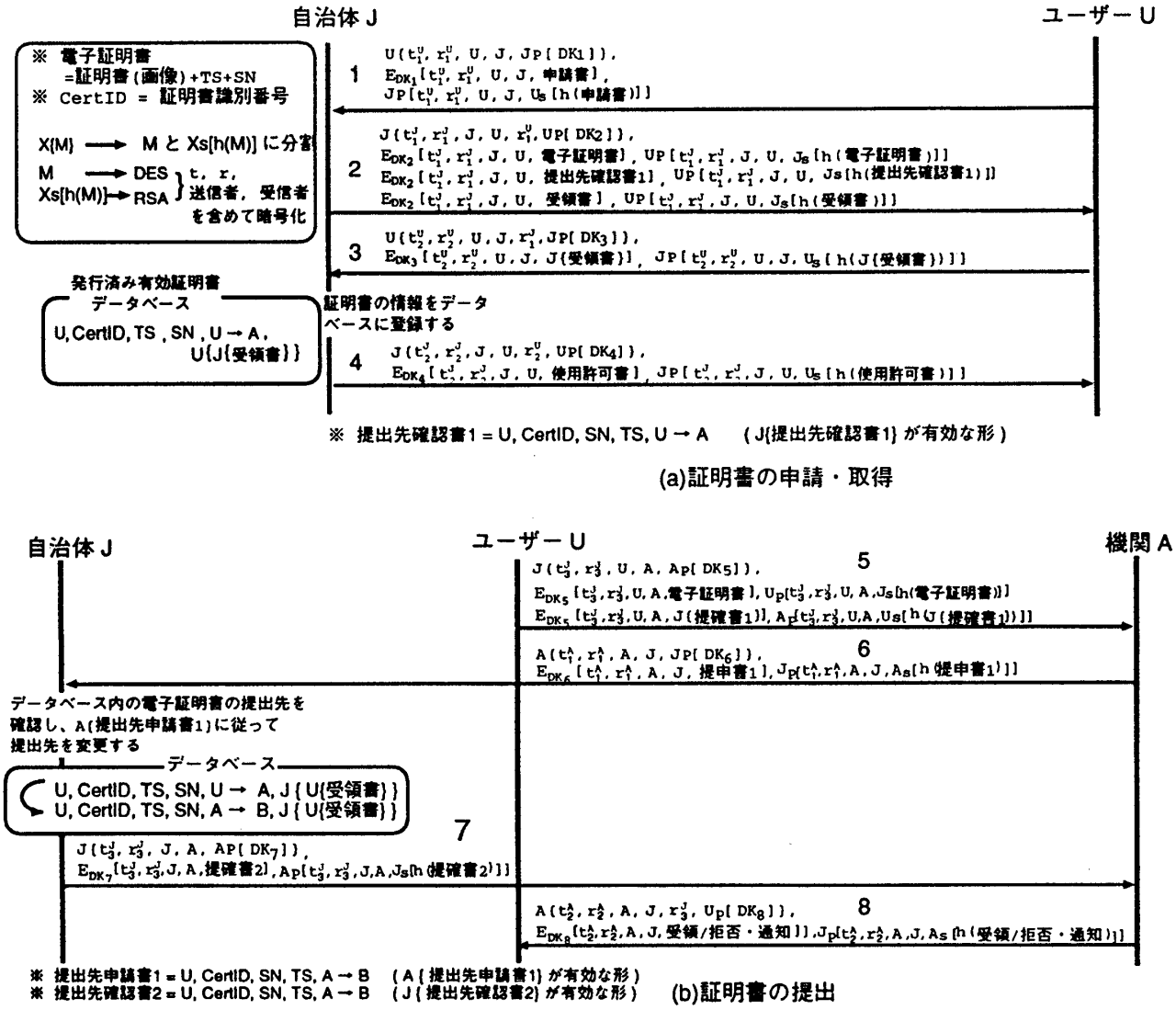

図 1: 提案プロトコル

Bがこれ以上提出を行わない場合、提出先申請書の内容を"$U, CertID, SN, TS, B \rightarrow B$" とし、$J$はデータベースの該当する $J\{$ 電子証明書 $\}$ の登録に "確認済みのマーク" を付加し、{ 電子証明書 } の検証結果（正当である）にデジタル署名を施して返す。従って、$J\{$ 電子証明書 $\}$ の複製が機関 X に提出された場合は、X がその正当性の確認を（提出先申請書で）J に以来した時には該当する登録は変更或は "確認済みのマーク" が付加されており、X には複製であると通知される。

5 検討

本稿で提案されるプロトコルでは自治体にデータベースを設け、ここに発行された電子証明書の詳細を登録しておく。機関が証明書の有効性を問い合わせてきたら、このデータベースを調べる。機関が証明書を他に提出するなら申請先確認書に従ってデータベースを書き換え、他に提出しないなら該当データに "確認済みのマーク" を付加して、"確認結果にデジタル署名を施して返す" ことにより複製の利用を防止する。

また、署名付きデータのデータ本体の暗号化に DES を用いることで暗号／復号にかかる時間は短縮されており、署名部分を別に RSA で暗号化しているので安全性は損なわれない。さらに、DES では毎回異なる鍵を用いることでより安全にしている。

課題点としては、自治体のデータベースに提出元と提出先が常に記録されるため、証明書の流れを自治体に把握されることでプライバシーの保護が守られないことが挙げられる。これに関しては匿名通信 [4] を利用する方法などが考えられる。

6 おわりに

本提案では証明書の検証をオンラインで行っているが、今後はこれをオフラインで行えるような方式を提案したい。

参考文献

[1] 辻井重男・笠原正雄 編著, "暗号と情報セキュリティ", 昭光堂, 1990.

[2] ISO IEC 9594-8:1990 "The Directory-Part8: Authentication framework"

[3] 榊原, 田代, 安倍, 岡田, 松下, " 証明書類の電子化とセキュリティ技術 ", 情報処理学会第 51 回情報システム研究会研究報告, pp19-26, 1994

[4] D.Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 1981, Vol24, No2