6W-3

簡易電子証明書発行システムの提案

岡田 大輔† 辻 秀一‡

東海大学大学院工学研究科† 東海大学電子情報学部‡

１．はじめに

インターネットが急速に普及する中、安全性を確保するのかが大きな課題になっている。ＰＫＩは「改ざん」「なりすまし」「盗聴」「否認」といったリスクを回避し、インターネット上で安全な商取引を行うためのインフラとして注目されている。

一方で導入していない企業・団体が多いのが現実である。導入しない理由として、手軽さがない、構造が複雑などいまいち使い勝手がよくないという理由が多い。そこで誰もが気軽に使えるようなプライベート向け簡易電子認証システム構築を目指す。

２．従来モデル

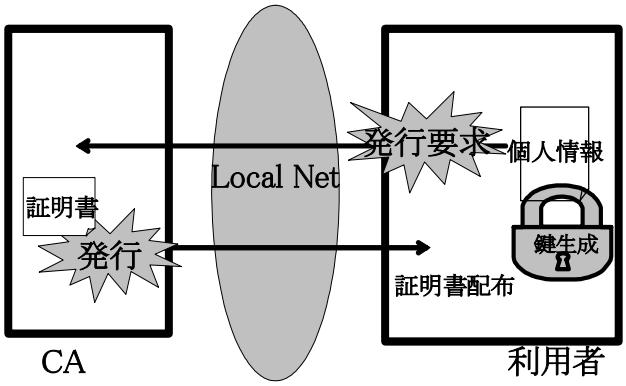

fig１．従来のＰＫＩモデル

ＣＡ構築ツールの 0penSSL では、証明書署名要求を受けた際、送られる個人情報（名前、国籍、所属など）と電子メールアドレスに対して本人確認はせず、送られた情報を元に証明書をその電子メールアドレスに発行する方法をとっている。これでは、登録した電子メールで受け取れる人物であるかを検証した事になり、身元の証明をしていな薄い事になる。ゆえに証明書としての信頼性は非常に薄くなる。

また、ベリサイン等にプライベート認証局構築を委託した場合、証明書要求要求を受けた際の本人確認手段は人手による確認となり、コストと時間がかかってしまう。

２．提案モデル

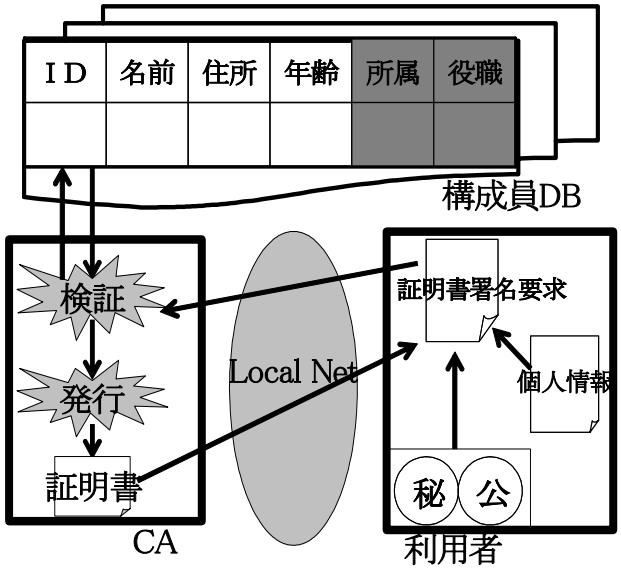

fig２．提案のＰＫＩモデル

fig２では小規模組織におけるプライベートＣＡを想定している。プライベートＣＡは誰でも比較的簡単に構築することができ、コストを抑えることができる。

提案システムを下に手順を示す。①利用者は公開鍵と秘密鍵を生成する。秘密鍵は外部記憶装置のほうに移動させ、ＰＣには残らないようにする②利用者は個人情報と公開鍵を含んだ証明書署名要求書を作成し、ＣＡに送る③ＣＡは送られた証明書署名要求書を解析し、個人情報と公開鍵に分ける④個人情報と構成員ＤＢとを検証し本人だと確認できれば構成員ＤＢに登録されている Email アドレス宛に証明書を発行できる。この際先ほど取り出した公開鍵によって暗号化メールを行う⑤利用者は暗号メールを秘密鍵によって解読し、証明書を受け取る。これによりＣＡ側に送った公開鍵と利用者が所持している秘密鍵とが対になっているかが確認できる。

また、役職が変わるなどの属性が変更になる

A Proposal of the Simple Electronic Certificates Issue System
†Daisuke Okada ‡Hidekazu Tsuji
†Graduate School of Engineering, Tokai University
‡School of InformationTechnology and Electronics,University

場合証明書の再発行の必要が出てくる。以下に手順を示す。①ＣＡは構成員ＤＢの項目変更に伴い、証明書の再発行の必要性があるか調べる。②照合し再発行の必要がある場合は、証明書の破棄を利用者側に報告をする。またディレクトリの証明書も破棄する。③利用者側は証明書署名要求書をＣＡ側送り証明書を得ることができる。

３．安全面

（１）個人に対する証明でなく属性に対する証明もしているので、属性によるアクセス許可や属性毎にカスタマイズされたコンテンツ表示などの多彩なアクセスコントロールが可能になる。

（２）証明書署名要求書を使用することにより秘密鍵を丸ごと送ったり、扱いの難しい情報を危険にさらしたりすることなく、証明書を作成するに足る情報を証明書発行機関に送る事ができる。

（３）セキュリティレベルは本人認証をどうのように行うかに依存する。システムではプライベートＣＡを想定しているので、小規模組織の構成員ＤＢを利用することによって本人認証を行っている。まず証明書署名要求書から個人情報と電子メールアドレスを取り出し、構成員ＤＢの構成員名、住所、所属、メールアドレスを照合する。一致していればそのメールアドレスに証明書を送り返す。構成員ＤＢは信頼性の面で高いと言え、これを利用して、本人認証を行うことで比較的高い証明書を発行する事を可能にする。

（４）以上の点から提案システムのセキュリティレベルの位置づけとして Class1 の低コスト、Class2 のセキュリティレベルの高さから、図 3 の☆の位置と考察する。

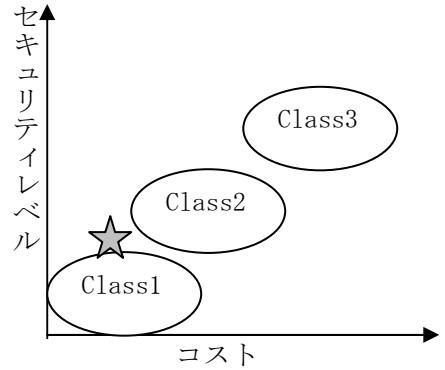

fig３．セキュリティレベルとコスト
(verisign より)

Class1　一義的な名称と電子メールアドレスの自動検索。

Class2　クラス 1 に加え、クレジット会社等の第三者が保持する記憶と比較することにより検証する。同一性について絶対確実なものではない。

Class3　クラス 1 に加え、出頭と身分証明書類によって同一性を検証。同一性に対して確実性の高い保証。

４．問題点と改善策

（１）鍵ペアの生成を利用者側で行う点、証明書署名要求書も作成する点で利用者側の負担が増えてしまうことになる。これでは実現的ではない。これをおぎなうためにＣＡと直結したツールの作成が必要である。利用者は個人情報を入れるだけで、鍵や証明書署名要求書の生成・送信、秘密鍵の保存と削除などはツールが行う。

（２）鍵リカバリをしようとした場合、ＣＡ側は利用者側の秘密鍵に関与していないために鍵リカバリができない。暗号化した文書を永久に復元できなくなる可能性が出てしまう。

（３）本システムはしっかりと管理されセキュリティの強固な構成員ＤＢでなければ機能しない。

５．まとめ

小規模組織内の重要書類のやりとりにおいてディジタル署名や暗号化メールを使用する場合、Class1 の証明書ではディジタル署名としての効果は薄く、また Class2、3 の証明書ではコストがかかりすぎてしまうため、結局直接渡しにいくというのが現状でありＰＫＩを導入しない組織が多い原因でもある。またセキュリティレベルの高い証明書では実世界の認証も必要としていた。

本システムでは、時間やコストを抑えた比較的高い保証のディジタル証明をインターネットのみの手続きで発行できるというシステムを提案した。

参考文献

[1] verisign:　http://www.verisign.co.jp/
[2] OpenSSL :　http://www.openssl.org/
[3] 若山公威他 ,”暗号ライブラリと認証局パッケージの開発”第５９回情報処理学会全国大会,Oct,1999