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。

ＰＫＩのディジタル証明書を発行する場合の本人認証要素は電子メールアドレスだけの低保証のディジタル証明と、証明の写真と申請者とを照合できるよう、ＣＡは申請者に対して、本人が来社し、本人を確認するためのもの（免許証やパスポート）を２種類以上提示するような高保証のディジタル証明と大きく分ける。低保証のディジタル証明の場合、申請者の電子メールアドレスさえわかっていれば第三者によるディジタル証明を取得してしまう。また、高保証のディジタル証明は時間もかかりコストも莫大である。そこで、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発行するＣＡシステムを提案する。

２．従来モデル

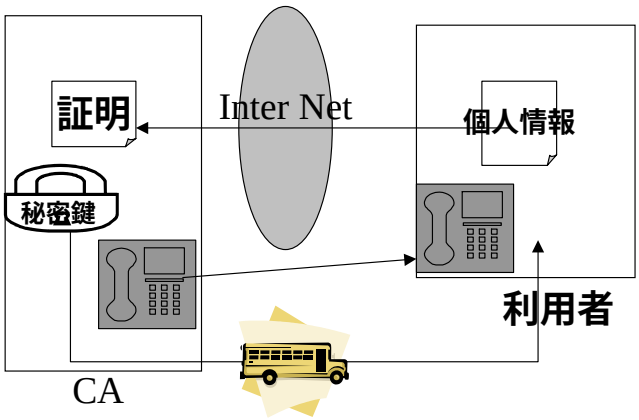

図１．従来のＰＫＩモデル

従来のＰＫＩは証明書を作成する上での本人確認は、電話による確認や免許証、パスポートでの確認が一般的である。これはインターネットを介さず、実世界で本人認証をする事で非常にセキュリティの高い本人認証となる。しかし、コストや時間がかかってしまう。また、個人情報（名前、住所、所属など）と電子メールアドレスのみで証明書を発行する場合もある。これ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い事になる。ゆえに証明書としての信頼性は薄くなる。

２．提案モデル

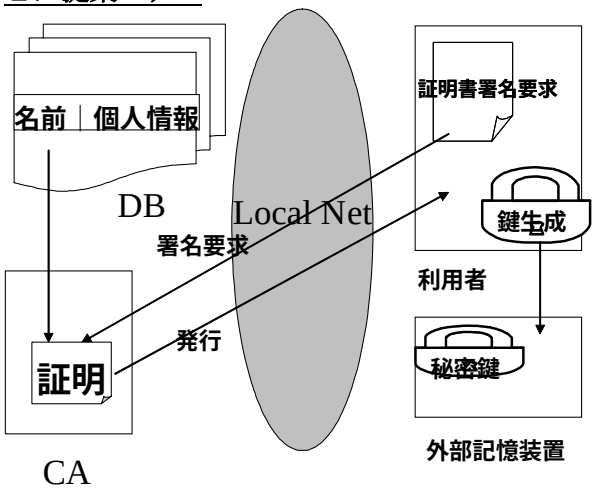

図２．提案のＰＫＩモデル

図２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。プライベートＣＡは公的なＣＡからの署名をもらえば、外部からの信頼も受けた証明書の発行ができる。

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は社員ＤＢと証明書署名要求書を検証し本人だと確認できれば利用者に対して証明書を発行できる。

３．安全面

（１）鍵の生成はＣＡ側で行うのが圧倒的であ

A Proposal Method of Low-Cost / High-Reliability for Certificates Issue
†Daisuke Okada　‡Hidekazu Tsuji
†Graduate School of Engineering, Tokai University
‡School of Information Technology and Electronics,University

る。この場合、ＣＡ側で生成した秘密鍵は利用者側に渡さなければならない。しかし安易に秘密鍵をインターネットに流すわけにはいかない。提案システムでは鍵の生成は利用者自身が行っている。利用者側で鍵を生成する事によってインターネット上での秘密鍵の盗聴を防止する。また秘密鍵は外部記憶装置のみに記憶させておく。

（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。

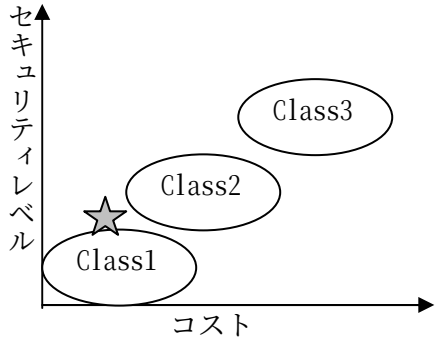

図３．セキュリティレベルとコスト
（verisign より）

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．システムの問題点と改善策

（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）証明書の再設定などの際、鍵生成を利用者側で行うので、本当にその人が正しい鍵を持っているかを示すものをＣＡに送らなければならない。

（３）鍵リカバリしようとした場合、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。

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。

６．今後の展望

今後の課題として、以下の点が挙げられる。

・鍵生成・証明書管理などの機能を持った利用者側ツールの開発
・属性認証局を含めたシステムの提案

参考文献

[1] verisign:　http://www.verisign.co.jp/
[2]H.X.メル+ドリス・ベイカー： 暗号技術のはなし pp.179-181
[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