27 PKIシステムの設計開発

-自治体システムへの適用-

辻孝裕*† 矢部圭市郎† 森賢一† 堤勝則‡ 後藤智路§ 畠山康博¶ 奥野拓¶ 大谷真¶
(北大工学) † (札幌市IT推進課) ‡ (札幌総合情報センター) § (北大情報科学)¶

1 はじめに

現在多くの自治体において，ITを効果的に使った行政改革が取り組まれている．独立して機能している従来の業務間をITを積極的に利用し連携を高め，統合された行政経営を実現させようという試みである．この統合による情報のネットワーク化の実現のためには，以下のネットワーク特有の脅威に対する，セキュリティ強化が必須である．

- 不正侵入
- コンピュータウィルス
- データの盗難
- 通信の盗聴
- データの改ざん
- なりすまし

通信の盗聴，データの改ざん，なりすましなどの脅威に対する取り組みは，不正侵入やコンピュータウィルス対策と同様十分意識され行われているが，技術の進歩とともに新たな脅威が生まれ，従来からの対策では不十分な可能性があるため，より根本的な解決を行う必要がある．

これらの対策として，近年PKI(Public Key Infrastructure)を導入する事例が増えている．その際の導入方法としては，これまではベンダーパッケージを購入しPKIを構築することが一般的であった．

一方で，昨今のOSS(Open Source Software)開発の広がりに伴って，PKIを実現するソフトウェアもいくつか現れてきている．代表的なものとしてOpenCA，IDX-PKI，newPKIがあり，これらを活用することでベンダーパッケージに比べ低コストでPKIを構築できる可能性がある．

本研究ではPKIシステムをOSSで構築することを前提に，PKIを実現するOSSの中で最も活発に開発が行われ，機能も充実しているOpenCAに注目し，自治体システムへの適用開発を行った．さらにPKIを導入する際の経済性，運用上の留意点といった点の調査も行った．

具体的なアプローチとしては，実際に自治体へPKIを導入するにあたっての共同研究を通し，機能要件・性能要件などを検討事項に取り入れ，OpenCAを現実に即したネットワーク環境下に構築し，実証検証を行った．

* t-tsuji@complex.eng.hokudai.ac.jp
† 札幌市北区北13条西8丁目北海道大学大学院工学研究科
‡ 札幌市中央区北2条西2丁目STV北2条ビル7階
§ 札幌市白石区菊水1条3丁目1-5 メディアミックス札幌
¶ 札幌市北区北14条西9丁目北海道大学大学院情報科学研究科

2 PKIシステム導入における検討事項

PKIシステムの導入には，利用目的を明確に定め，何をどのように実現するかを検討しなくてはならない．

今回，自治体への導入検討の打ち合わせから，クライアント-サーバ間の通信の保護や証明書ベースの職員認証が重要であることがわかった．その上で，利用者に負担がかからず，安全なPKIシステムの構築・運用を行わなくてはならない．

上記を実現するためには，PKIシステム導入における課題が幾つかあがり，技術的な課題としては，他システムと連携した認証基盤の実現，ICカードを用いた職員認証，情報に対するアクセスコントロールがあり，運用上の課題としては，PKIシステムの導入・運用コストの低減，認証局による個人証明書の大量発行，証明書の更新手続きの簡略化，署名したファイルに対する長期保存などがある．

3 経済性検討

今回調査に用いたOSSであるOpenCAは，ベンダーパッケージに比べて機能的に一部不足していることが事前の機能調査よりわかっている．その際は不足機能の開発を行わなければならないが，ベンダーパッケージの購入と比較して，追加開発し導入することが経済的に優れているかの判断は難しい．ここではOpenCAの導入を行うかの一つの指標として，A社より商品化されているPKI機能を持つソフトウェアパッケージのカタログ値との比較を行う．

3.1 コスト要素

PKIを導入する際に，導入コストとしては大きくは以下の項目がある．

- PKIシステム構築費用
- PKIシステムカスタマイズ費用
- 証明書ライセンス費用
- 環境構築費用
- 運用開発費用

これらのコストは，証明書の発行枚数，認証局の数といった，システムの規模や，証明書を一括で発行することやICカードとの連携機能の開発など，システムの目的によって変動する．

これらのコストについては，算出の軸として一般的な目的を抽出し，変数を定義することが困難であるため，ここでは議論の対象としない．結果としてシステムの規模によって変動する以下のコストについて比較を行う．

- PKI システム構築費用
- 証明書ライセンス費用

PKI のシステム規模に影響を与える変数としては以下の 3 つを対象とする.

- 証明書の発行枚数
- 認証局の数
- 登録局の数

3.2 コスト算出方法

コストを算出する際の変数として，以下のように定義する.

- ベンダーパッケージのコスト：F_v
- OpenCA の追加開発コスト：F_o
- 証明書の発行枚数：$Cert$
- 認証局の数：N_{ca}
- 登録局の数：N_{ra}

3.2.1 PKI システム構築費の算出

PKI システム構築費について以下のように定義する.

- PKI システム構築費：$f_a = f_{a1} + f_{a2}$
- 認証局構築費：f_{a1}
- 登録局構築費：f_{a2}

となる．ここでベンダーパッケージの場合

$$f_{a1} = \text{認証局ソフトウェア購入費用} \times N_{ca} \quad (1)$$

$$f_{a2} = \text{登録局ソフトウェア購入費用} \times N_{ra} \quad (2)$$

であり，OpenCA の場合

$$f_{a1} = Const_1(\text{認証局の追加開発費用}) \quad (3)$$

$$f_{a2} = Const_2(\text{登録局を追加開発費用}) \quad (4)$$

である．なお A 社におけるパッケージ費用は，OS によって変化はあるが，Windows サーバを用いるならば，

$$\text{認証局ソフトウェア購入費用} = ¥2,000,000$$

$$\text{登録局ソフトウェア購入費用} = ¥2,000,000$$

となっている.

3.2.2 証明書発行ライセンス費用

証明書発行ライセンス費用について以下のように定義する.

- 証明書ライセンス費用：f_b

ベンダーパッケージの場合

$$f_b = \text{一枚あたりの証明書ライセンス料} \times Cert \quad (5)$$

であり，OpenCA の場合は証明書を発行する際にライセンス料を必要としないため

$$f_b = 0 \quad (6)$$

となる．なお A 社における証明書ライセンス料は，総枚数が多くなれば，一枚あたりの証明書ライセンス料が下がり証明書ライセンス料と証明書発行枚数は以下の式を満たす.

$$\begin{aligned} f_b(X) &= 20000000x_1 + 10000000x_2 + 5000000x_3 \\ &\quad +3500000x_4 + 1000000x_5 + 750000x_6 \quad (7) \\ Cert &< 1000000x_1 + 100000x_2 + 10000x_3 \\ &\quad +5000x_4 + 1000x_5 + 500x_6 \quad (8) \end{aligned}$$

但し $X = (x_1, x_2, x_3, x_4, x_5, x_6)$ は $f_b(X)$ を最小とする組み合わせである.

3.2.3 コスト算出

前述した式より，システム規模によって決まるコストは以下のように算出できる.

$$\begin{aligned} F_v &= 2000000 \times N_{ca} + 2000000 \times N_{ra} \\ &\quad + f_b(X) \quad (9) \\ F_o &= Const_1 + Const_2 \quad (10) \end{aligned}$$

となり，F_v と F_o を比較することにより，OpenCA の追加開発実施の一つの基準を得ることができる.

一例として今回調査を行った自治体における導入規模を挙げると以下のとおりである。

- 証明書の発行枚数は 26,000 枚程度
- 認証局・登録局共に 2 つ

結果，$F_v = 18000000$ となり，OpenCA の導入検討はこのコストと比較することとなる.

4 PKI システムの運用

4.1 CP・CPS

PKI システムの運用にとって最も重要なことは，信頼の起点となるトラストアンカー[1] を設置する機関（認証局）の安全性を確保し，それを利用者に広告することである．なぜなら PKI システムは，認証局（第三者）を信頼する（信頼を預ける）ことを起点として全体が成立するシステムであるからである．この目的のため記述された文書として証明書ポリシー（CP）及び認証局運用規定（CPS）がある．CP・CPS の策定方法については，ECOM の報告書 [1] や RFC でフレームワーク [2] が提供されており，通常これらの手順に沿って行われる.

CP・CPS は互いに相補的に存在し，主に以下の点について定めたものである.

- サービスモデル：発行する証明書の種類
- サービスレベル：発行する証明書の信頼性の確保
- 運営体制と業務手順：信頼性を確保するための体制やルールの策定

[1] トラストアンカーは通常，認証局に対して設置される．具体的には，認証局（CA）に対して発行された CA 証明書を利用者のコンピュータの信頼リストに加えることと等価である.

ここでは，主にサービスレベルに関わる証明書のライフサイクルの定義に関する考察を行い，その定め方に関する提案を行う．

4.2 証明書のライフサイクル

証明書のライフサイクルは，一般に Fig.1 に示されるものである．

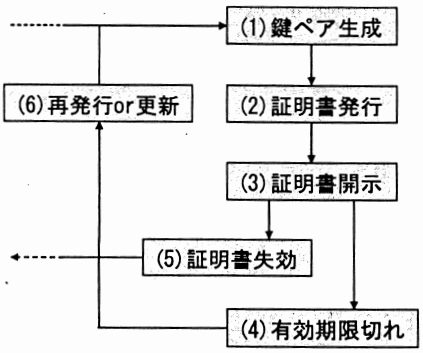

Fig. 1 証明書ライフサイクル

本節で対象とするのは，この中でも中心的な箇所である証明書の更新部分，つまり「公開鍵の有効期限と対応する私有鍵の有効期限」についてである．これらの有効期限を定めるためには，次の点に考慮が必要である．

- 証明書の更新においては，更新間隔 (運用負荷) と安全性はトレードオフの関係にある
- 私有鍵の有効期限は，信頼パスにおける下位の証明書の有効期限に影響を与える

運用負荷と安全性の問題については，情報資産の見積もりやリスク評価を適切に行うことで最適な均衡点を設定することが望ましい．

ここでは主に 2 点目について注目する．例えば CA 証明書の有効期限が切れれば，その CA が発行した証明書に含まれる署名を検証することが不可能となり，証明書は失効扱いとなる．また，失効した証明書に対応する私有鍵でなされた電子署名の検証も不可能となる．これらの問題を解決するため，更新の際に新旧の証明書の重複期間を設定する[2]．特に，公開鍵の有効期限と私有鍵の有効期限を分けて設定すれば，証明書の更新に関する運用を固定化でき，証明書利用者は特別な配慮なしに証明書の更新とその利用が可能となる．

これらの観点から，本節では Fig.3 で示す証明書パスに対して次のようなライフサイクルを提案する．

$$p_n < P_n \leq 2p_n \tag{11}$$

$$p_{n-1} = N_n p_n (N_n \in \boldsymbol{N}) \tag{12}$$

ただし P, p はそれぞれ，公開鍵，私有鍵の有効期限を表し N は任意の自然数を表す．また，添え字 n は証明書

[2] ただし，電子署名文書の長期保存に関してはここでの範囲を超えるため扱わないが [3] に詳しい．

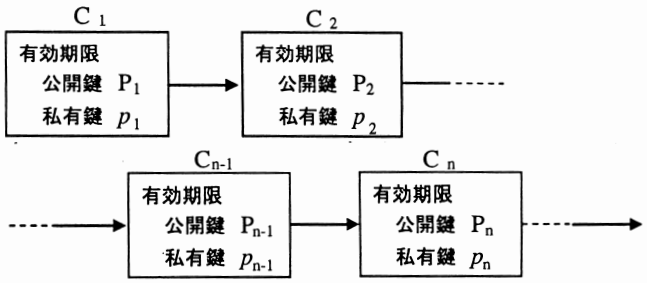

Fig. 2 証明書パス

パス中の位置を表し C は，パス n の公開鍵と私有鍵を合わせたものとする．

式 (11) は，証明書が重複して存在する期間においても，有効な私有鍵を重複して持つことが無いことを意味している．また，式 (12) は，証明書の更新サイクルが常に同じ時期に行われることを表している (Fig.3)．

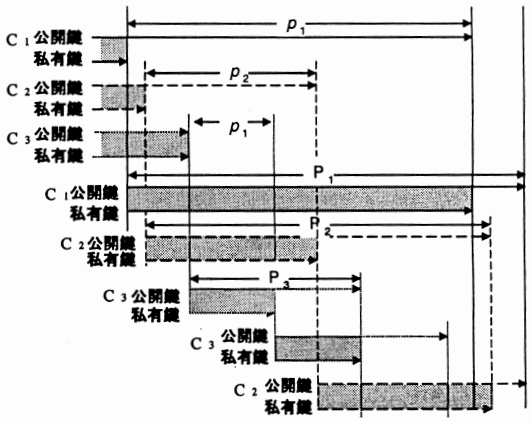

Fig. 3 提案するライフサイクルの例

以上より，これらの式で表される関係は次のような特徴を持つ．

- 私有鍵を重複して持つことがないため運用負荷が低い
- 誤って古い私有鍵で署名した署名が検証できない，という人為的ミスを防ぐことができる．
- 新旧の証明書の有効期限が重なる期間において，高々 2 枚の証明書しか重ならない．
- 私有鍵の有効期限（更新サイクル）が下位の更新サイクルの倍数になっているため，通常の更新であれば，常に同じ時期に証明書の更新が行われる．

これらの特徴は PKI システムの運用という観点からはどれも価値の高いものであると考えられる．なお，証明書パスが分岐する場合 (上位の証明書が下位の証明書を複数発行する場合）についても式 (11)，(12) を拡張し対応することが可能である．

5 OSS による PKI システムの構築

PKI システムを OSS を用いて構築することで高い安全性・低コスト化が期待できる．だが，そのためには適

切な OSS の選択を行い，業務適応性の検討を行わなくてはならない．そのため，PKI システム導入に際し事前に必要な機能の検討やシステム間連携の実現，インターフェイスの日本語化は必須である．以下では OSS による PKI システム構築の検討・作業内容を述べる．

5.1 OSS の選択

PKI を実現する OSS は多く存在しているが，そのどれもがすぐに業務へ適用できるとは限らない．しかし OSS はソースコードが公開されているため，ライセンスを遵守する中でカスタマイズでき，目的にかなう PKI システムの構築が可能である．

土台となる OSS は機能，ソフトウェア品質，サポート (コミュニティの活発さ)，ライセンス，標準準拠性，普及率の点を考慮することで，構築・運用コストは低減できる．一般に OSS の使用実績が多い場合には，多数の人が監視する状態になり，機能の拡充や不具合の改善が十分に行われ，セキュリティに対して高い効果があると言われている．

以上のことを考慮し，現時点で代表的な PKI の OSS である OpenCA，IDX-PKI，newPKI を比較検討した結果，OpenCA が最も適した PKI ソフトウェアであると結論付けられた．具体的には，証明書のデータベースによる管理機能，国際化対応，コミュニティの活発さ，数万件のダウンロード実績などの点で特に優れていることがわかった．日本ではまだ認知度が低く，日本語化のドキュメントも無いが，最近の国内における PKI システムの関心の高さから，今後日本でも OpenCA を用いた PKI システム構築事例が増えると推測される．

5.2 証明書の相互運用性

異なるシステム間で証明書を扱うためには互いのシステムが仕様どおりの実装がなされてなくてはならない．証明書は認証に使われることが多く，自治体内の種々の環境で正しく扱うことができなければ PKI システムの導入により実際の業務に支障をきたす．この相互運用性を確認するために OpenCA で発行した証明書を用いてクライアント-サーバ間で HTTPS 通信で検証を行った．検証環境・検証手順は以下のとおりである．

Table 1 検証環境

用途	ソフトウェア
クライアント	Windows 98SE/2000/XP
	Internet Explorer(IE) 5.0/6.0
Web サーバ	IIS(Internet Information Services) 5.0/6.0
	Apache2.0.4+mod_ssl2.0.40-21
CA 環境	OpenCA 0.9.1.7
	OpenSSL 0.9.7a

検証手順

1. サーバで証明書署名要求（CSR）を作成する
2. OpenCA で CSR を処理し，証明書を発行する
3. 発行された証明書をサーバに格納し，HTTPS の設定を行う
4. クライアント環境からサーバに HTTPS でアクセスを行う

結果，1 つの例を除き全ての組み合わせにおいて証明書の相互運用性が確認された．1 つの例とは，Windows 98SE で IE5.0 を使用する場合で，サーバで 128 ビットの強度の暗号化通信を強制する設定で，アクセスすることができないという問題があった．

これは高度暗号化技術が輸出規制の対象だったため 40 ビットに制限されたソフトウェアとなっていたからである．しかし、現在は暗号の輸出規制は緩和されており，高度暗号化パックを適用することで 128 ビットの暗号化通信が可能となる．

6 おわりに

本論文では，PKI システムを自治体に適用するために行われた共同研究の成果を基に報告を行った．経済的側面からは PKI システムのコストについて定量化して考察を述べ，運用面ではシステムの安全性の確保，具体的にはサービスレベルの定義における証明書ライフサイクルの定め方の提案を行った．更に OSS を用いて PKI システムを構築する際の OSS の選択方法や，OSS を用いた場合の証明書の相互運用性の検証結果報告を示した．この結果は，OSS が自治体の業務に適用可能であることを強く示唆するものであった．

ただし，今回の共同研究が範囲とする領域は導入調査全体の一部であるため，今後は今回明らかになった問題点の整理・解決策の検討，プロトタイプ作成による更なる問題抽出など，自治体への PKI システムの本格導入へ向けては継続的な調査研究を行うこと必要である．

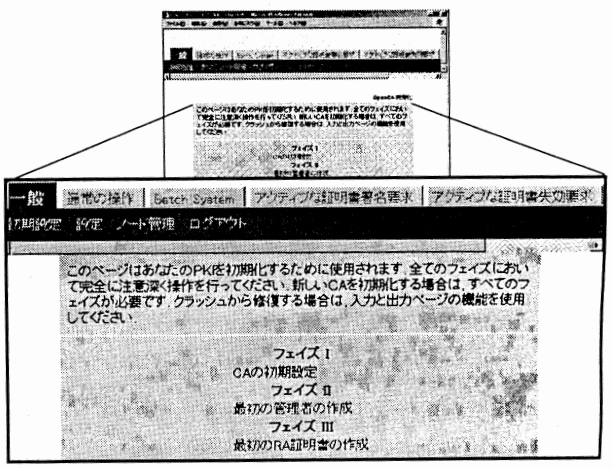

Fig. 4 日本語 OpenCA

なお，今回の設計開発を通して OpenCA0.9.2-RC3 の gettext による翻訳対象，約 1700 箇所全てを翻訳した．この翻訳の成果物は，OpenCA のコミュニティである OpenCA Lab(http://www.openca.org/) にコミットをし，新たに日本語ロケールが追加された．これは日本で初めてのことであり，OpenCA の日本語翻訳文に対しリポジトリに対する権限を獲得し，サポートの窓口として公表されている．Fig.4 に日本語化した画面イメージを示す．

A 付録

A.1 OpenCA の機能

PKI システムの構築調査を行うにあたり，OpenCA の機能の調査を行った．OpenCA はドキュメントが完備されていないため実装機能を把握しにくい．また，日々改良されているが安定して機能を使うことができず，実装が不完全なものもある．

そのため実際に OpenCA を用いて PKI システムを運用することで機能を検証した．その結果として有効な機能の一覧を得た．その中で PKI システムを自治体へ適用するために必要な機能のうち主要なものを以下に挙げる．

- 単独・階層型認証局
  一つの OpenCA で単独認証局を構築することができ，複数の OpenCA を用いることで階層型認証局の構築が可能である．
- OpenSSL や OpenLDAP との連携機能
  証明書発行 (署名) を行うための核となるソフトウェアである OpenSSL やリポジトリ機能を持つ OpenLDAP と連携し，Web 上で操作が可能である．
- データバックアップ&リカバリ
  発行や失効した証明書の情報や認証局がもつ PKI 利用者の情報などをバックアップ&リカバリする機能である．
- 証明書ベースの管理者認証機能
  認証局や登録局は Web ブラウザから操作を行うため管理者を認証する必要がある．その認証を行うために証明書を用いた認証をし，利用できる機能を制限（権限の設定）する機能である．
- 証明書発行者へメールで通知
  証明書発行申請を行った PKI 利用者に認証局より証明書発行完了の通知をメールで行う機能である．
- 役割に応じた証明書プロファイルの切り替え
  PKI 利用組織に複数の部門があり，それぞれで証明書の利用用途が異なる場合に各部門に対応する証明書プロファイルを用意する必要がある．この機能は用意した証明書プロファイルをそれぞれに対し容易に切り替えを行うものである．
- 国際化対応
  現在の OpenCA の最新版である OpenCA0.9.2-RC4 では英語，ドイツ語，スペイン語，フランス語，イタリア語，ポーランド語に対応している．時期バージョンより日本語が追加される．
- 要求・証明書状態管理機能
  証明書署名要求や失効要求，発行した証明書の状態を認証局ごとに一元管理する機能である．この機能は認証局の規模が大きいほど重要で，PKI システムを効果的に運用するためには欠かせないものである．OpenCA では内部にデータベースを保持していて，要求や証明書の状態を細かく管理できる．各要求や証明書がどのような状態で管理されるかを Table.2, Table.3 で示す．

Table 2 要求状態一覧

証明書署名要求	証明書失効要求
未処理	未処理
承認済	承認済
アーカイブ済	アーカイブ済
削除済	削除済

Table 3 証明書状態一覧

CA 証明書	エンドエンティティ証明書	CRL
正当	正当	最新
期限切れ	期限切れ	履歴
	一時停止	
	失効済	

A.2 自治体への報告内容

OpenCA を用いた PKI システムのデモンストレーションを行った．この内容は自治体において PKI システムを導入した時に，PKI 利用者が行わなくてはならない初期設定や暗号化通信，認証機能についてが主なものである．これは，PKI システムを利用するために運用上必ず必要な事柄に加え，OpenCA を用いた場合に特有の運用も含まれる．

以下にその一部であるクライアントと Web サーバの PKI 利用時の初期設定と Web サーバに対する HTTP や HTTPS のアクセスに関する内容を示す．システム環境は Table.4 に示し，次に PKI システム利用の手順を示す．

Table 4 システム環境

対象	ソフトウェア
クライアント	Windows 2000 (IE 6.0)
Web サーバ	Windows 2000 Server(IIS 5.0)
CA 環境	OpenCA 0.9.1.7
	OpenSSL 0.9.7a

手順

1. クライアントの初期設定
   (a) ルート証明書の取得
   (b) クライアント証明書の取得
2. Web サーバの初期設定
   (a) ルート証明書の取得
   (b) サーバ証明書の取得
   (c) サーバの SSL 等アクセス設定
3. クライアント-サーバ通信
   (a) HTTPS 通信の確認 (証明書完備)
   (b) HTTPS 通信の確認 (証明書完備 & SSL 強制)
   (c) HTTPS 通信の確認 (証明書不備)
   (d) HTTP 通信の確認 (証明書完備)
   (e) HTTP 通信の確認 (証明書不備)

手順 1 のクライアント証明書の取得は Web ブラウザを用いてキーペアを作成し，証明書署名要求を提出する．この証明書署名要求にはメールアドレスを記入でき，認証局側からメールで発行の通知を受けることができる．受け取った証明書が本当に正しい証明書であることを検証するために，クライアントで保持している秘密鍵を用いて検証を行う．OpenCA では受け取った証明書の自動インストールや検証結果を Web 上で確認できる．詳細な流れは Fig.5 に示す．

手順 2 のサーバ証明書の取得は証明書署名要求を IIS 自身が作成することになるため，認証局側はファイルを受け取る機能が必要になる．OpenCA にはこの機能が実装されている．しかし，IIS では証明書署名要求にメールアドレスを含むことができないため，OpenCA は証明書の発行や認証局側からメールで発行通知を受け取ることができない．そのため証明書の発行に関しては，証明書署名要求からメールアドレスの取得を強制している部分を修正し，メールアドレスは取得しないよう変更した．また，サーバ証明書の発行通知については，システムが通知するのではなく，運用上，人が直接行うことを想定する．詳細な流れは Fig.6 に示す．

手順 3 のクライアント-サーバ通信では PKI 利用環境が整った状態で IIS に対し HTTPS を行うことで暗号化通信&サーバ認証を確認することができる．また，IIS で SSL 通信を強制した場合に，HTTP ではアクセスできなくなる．これにより，暗号化した通信のみを許可するので，第 3 者からのデータの盗聴が行えなくなる．さらに，クライアントがルート証明書を保持していない場合，通信を行うサーバを自動的に信頼することはできない．その場合注意を促すダイアログが表示され，安易に不正なサーバへアクセスすることが防止できることを確認できる．

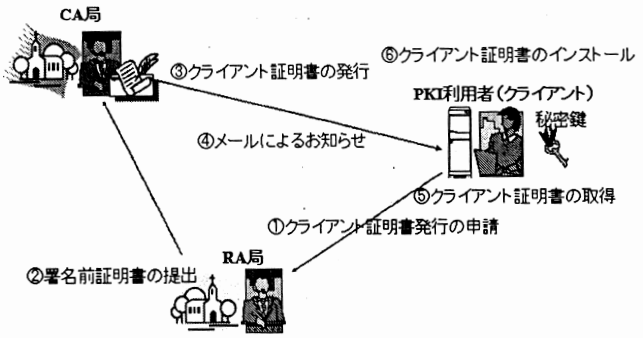

Fig. 5 クライアント証明書取得の流れ 1-b

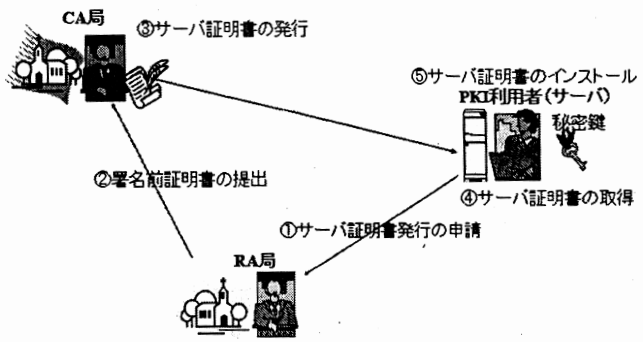

Fig. 6 サーバ証明書取得の流れ 2-b

参考文献

[1] 電子商取引実証推進協議会, "企業間電子商取引における認証・公証適用の考え方", 認証・公証 WG, 1999

[2] S. Chokhani and W. Ford, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework(インターネット X.509 PKI 証明書ポリシーと認証実施フレームワーク)", RFC 2527, March 1999

[3] 電子商取引実証推進協議会, "電子署名文書長期保存に関するガイドライン", 認証・公証 WG, 2001

[4] STEIN, L., "Web Security, A Step-by-Step Reference Guide. Readin, MA", Addison-Wesley, 1998

[5] Andrew Nash 他, 株式会社スリー・エー・システムズ訳, "PKI e セキュリティの実装と管理 PKI", RSA PRESS, 翔泳社, 2002

[6] 塚田孝則, "企業システムのための PKI ハンドブック", 日経 BP, 2001