社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30 (44)
2005／7／22

# 個人リポジトリの検証機構を備えたオンラインのバイオメトリック認証のフレームワーク

上繁 義史† 櫻井 幸一†‡

† (財) 九州システム情報技術研究所 〒814-0001 福岡市早良区百道浜 2-1-22 福岡 SRP センタービル 7 階
‡ 九州大学 大学院システム情報科学研究院 〒812-8581 福岡県福岡市東区箱崎 6-10-1
E-mail: † ueshige@isit.or.jp, ‡ sakurai@csce.kyushu-u.ac.jp

**あらまし** バイオメトリック認証は正当な利用者の識別において有望な技術として知られている．インターネットなどのオープンなネットワークにおける利用も期待されているが，その一方でバイオメトリックロウデータやテンプレートデータなどのバイオメトリック情報漏洩により個人情報の漏洩が懸念される．

そこで，本論文ではバイオメトリック認証の段階でバイオメトリック情報と氏名等の情報が同時に漏洩しないために，バイオメトリックテンプレート，公開鍵証明書などを格納した個人リポジトリを利用したバイオメトリック認証のフレームワークを提案する．このフレームワークでは個人リポジトリを検証する仕組みを設けることにより所有者の正当性が検証できる．

**キーワード** バイオメトリクス，個人リポジトリ，証明書，BioPKI，フレームワーク

# A Framework of Remote Biometric Authentication with Assuring Validity of Personal Repository

Yoshifumi UESHIGE† and Kouichi SAKURAI†‡

† Institute of Systems & Information Technology/KYUSHU Fukuoka SRP Center Building 7F, 2-1-22 Momochihama, Sawara-ku, Fukuoka, 814-0001, Japan
‡ Department of Computer Science and Communication Engineering, Kyushu University 6-10-1 Hakozaki, Fukuoka, 812-8581, Japan
E-mail: † ueshige@isit.or.jp, ‡ sakurai@csce.kyushu-u.ac.jp

**Abstract** Biometric authentication is remarkable with respect to identification of legitimate users. Biometric authentication is hopeful of services on the internet as reinforcement for conventional authentication such as ID and password, however, biometric information –acquisition raw data and template data– is unrenewable even though the data is compromised.

We propose a framework of online biometric authentication with verification of validity of user's personal repository based on PKI. In this framework, information of biometrics authentication (certificate of templates) is related to not information of ownership but personal repository. This framework achieves anonymity during biometric authentication process by verifying validity of the user's personal repository.

**Keyword** biometrics, personal repository, certificate, Bio-PKI, framework

## 1. はじめに

### 1.1. 背景

現在，様々な分野で個人認証技術が注目されている．これまで提案されてきた認証の考え方は主に 3 種類に分類される．すなわち，i) ID-パスワード，PIN のような利用者の記憶に基づいた認証方式，ii) カード（IC カードを含む）など所有物に基づいた認証方式，iii) バイオメトリクス[1]のような利用者の身体的行動的特徴による認証方式である．記憶による認証の場合，忘却，類推が容易なパスワード，メモによる漏洩が考えられる．また，所有物の場合では盗難，紛失の可能性がある．実際にスキミングやクローニングによるキャッシュカードの偽造という事件が発生している．バイオメトリクス認証は特別な認証装置を必要とすること

が課題とされる．しかしながら不正なパスポートでの入国，キャッシュカードの偽造などの社会問題に後押しされる形で，電子パスポート[2]やキャッシュカードの所有者の識別などに利用されている．

近年，E-commerce，インターネットバンキング,電子政府をはじめとするインターネット上で多くのサービスにて利用可能な個人認証技術が求められている．インターネットのようなオープンネットワーク環境における本人認証の基盤として公開鍵基盤（Public Key Infrastructure; 以下 PKI）[3]が知られている．PKI において，利用者はあらかじめ公開鍵と秘密鍵の対を生成する．公開鍵を認証局（Certificate Authority）に登録し，公開鍵証明書を発行してもらう．PKI では公開鍵証明書の検証により，秘密鍵の所持者からの送信であることを確認している．すなわち PKI における本人認証も所有物による方法に相当し，認証の問題は必ずしも解決されてはいないと思われる．

これに対してオープンネットワークでのバイオメトリック認証のフレームワークについて提案[5]～[11],[14],[15]がなされている．これらは BioPKI とも呼ばれ，秘密鍵の所持者とその正当な所有者の同一性をバイオメトリック認証を併用することにより証明するフレームワークである．認証局への登録情報としてバイオメトリクス情報を加えて，証明書とバイオメトリクス装置による認証から,本人性の確認を行うことが出来る．

[5],[6]は PKI に基づくフレームワークであり，公開鍵証明書と別にバイオメトリックテンプレートの証明書（テンプレートフォーマット）を定義している．テンプレートフォーマットは対応する公開鍵証明書の識別情報によって関連付けられている．このことから認証プロセス以外にも公開鍵証明書の登録者の名前とテンプレートを同時に入手される可能性があり，プライバシ保護の観点から対策が必要であると考えられる．

一方[7]はバイオメトリック認証の環境について機器の安全性，精度に関するデバイス証明書の検証を行うことにより認証結果の正当性が検証を行うフレームワークを提案している．[7]において，バイオメトリックテンプレートの証明にクォリファイド証明書[13]を用いているが，テンプレート情報は **http://**もしくは **https://**にて記述される URI にて入手することができるため，[5],[6]と同様の課題を持つと思われる．

### 1.2. 本研究のアプローチ

本論文では，テンプレート証明書と他の証明書の入手による個人情報流出とバイオメトリック認証以外のテンプレート情報へのアクセスを防止するための対策として,利用者の持つ個人リポジトリの所有者の検証をアプリケーションサーバに対して匿名のままで行うフレームワークを提案する．このフレームワークではバイオメトリック認証に関する情報（テンプレートの証明書など）を所有者ではなく個人リポジトリと関連付けを行う．個人リポジトリの所有者に関する証明書により所有者の検証を可能とする．ただし，この証明書へのアクセスは所有者本人と信頼できる検証機関のみに制限することにより所有者の個人情報としての証明書を保護する．この検証の後にバイオメトリック認証，公開鍵証明書の検証の順で認証プロセスを実行することにより，バイオメトリック認証が終わった段階ではアプリケーションサーバに対して匿名性を保持することを可能とする．

以下では 2 章で関連研究の概要を説明しその課題について述べる．3 章で我々の提案するフレームワークについて説明し，その安全性について議論を行い，4 章でまとめとする．

## 2. 関連研究

### 2.1. テンプレートフォーマットによるバイオメトリック認証を伴った PKI

磯部ら[5],[6]は，バイオメトリクス認証方式，精度などの差異を吸収し，ユーザのバイオメトリック情報の経年変化に対応するために，クォリファイド証明書を用いずに，テンプレートフォーマットを公開鍵証明書と独立に定義している．提案されたテンプレートフォーマットを表 1 に示す．表 1 において，**Certificate Identity Information** により対応する公開鍵証明書を特定することができるため，公開鍵暗号と併せて使用することができる．**Template Data** フィールドに

表 1　テンプレートフォーマットの内容

| # | Item | Contents |
|---|---|---|
| 1 | Format Identifier | テンプレートフォーマットを識別する情報 |
| 2 | Certificate Identity Information | PKI の証明書を一意に指定する情報．例えば，発行者名とそのシリアル番号 |
| 3 | Issuer Name & ID | このテンプレートを発行した発行者の名前および識別情報 |
| 4 | Template Data | テンプレートデータ（バイオメトリクスのタイプやアルゴリズム識別情報などを含む） |
| 5 | Issuer's Digital Signature | このテンプレートの発行者によるディジタル署名（署名アルゴリズム情報を含む） |

CBEFF[12]を利用してバイオメトリクスの種類，テンプレート情報などを格納する．

テンプレートフォーマットにより，テンプレート情報の可用性を高めることが可能であることを指摘し，それを利用した本人認証の方式を提案している．

本手法では，テンプレートフォーマットに公開鍵証明書の識別情報が含まれているため，リポジトリからテンプレートフォーマットが入手された場合，公開鍵証明書も容易に入手することができる．それゆえ，個人の氏名とテンプレート情報を同時に入手することが可能になると考えられる．

### 2.2. バイオメトリック認証環境検証方式

池田ら[7]は，図 1 に示すようにオープンネットワークを介した認証において，アプリケーションサーバがクライアントでのバイオメトリック認証結果の正当性を検証できるように，クライアントのバイオメトリック認証環境について認証を行うフレームワークを提案している．前提条件として，以下の 4 つが挙げられている．

- クライアント側に耐タンパ性をもつバイオメトリクスデバイスが接続されており，利用者の生体情報の採取と照合を行う．
- 利用者の個人情報格納デバイスはスマートカードのようなものを想定している．耐タンパ性をもち，公開鍵証明書，テンプレート情報に関する証明書，秘密鍵が格納されている．
- 公開鍵，テンプレート情報を認証する CA はこれらの情報に関する証明書（クオリファイド証明書）を発行する．
- バイオメトリクス認証に関する TTP は，バイオメトリクスデバイスの安全性，照合アルゴリズムの安全性や精度について証明書を発行する．

この手法は，認証環境と認証結果に関する情報をサーバに対して提示することにより，バイオメトリクス情報やテンプレート情報を提示せずに認証結果の正当性を検証することが可能である．

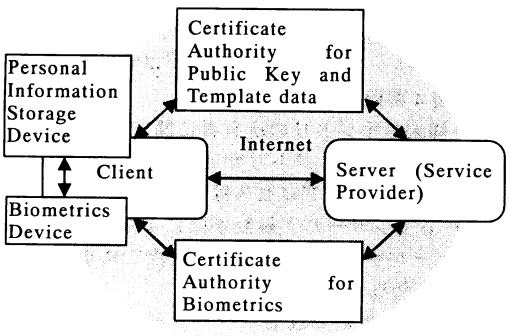


図 1　BioPKI の概要図

バイオメトリックテンプレートの証明にクォリファイド証明書を用いているが，テンプレート情報は **http:**//もしくは **https:**//にて記述される URI にて入手することができるため，[5],[6]と同様にそれゆえ，個人の氏名とテンプレート情報を同時に入手される可能性があると思われる．

## 3. 個人リポジトリ所有者検証フレームワーク

提案するフレームワークを図 3 に示す．このフレームワークは以下のエンティティから構成される．

- ユーザ：ユーザは秘密鍵，バイオメトリックテンプレート，テンプレート証明書（後述），公開鍵証明書を格納した個人リポジトリを持つ．
- アプリケーションサーバ：バイオメトリック認証による本人確認の後サービスを提供するサーバ
- ユーザの個人リポジトリの認証局：後述する個人リポジトリの所有者証明書を検証局に配布する TTP である．
- ユーザの個人リポジトリの検証局：アプリケーションサーバからの要求により個人リポジトリの所有者情報を検証し，個人リポジトリに格納されている証明書のリストからアプリケーションサーバが認証に必要な証明書が含まれているか検証を行う．この検証局は信頼できると仮定する．
- 公開鍵の認証局：利用者個人の公開鍵証明書を発行する認証局
- バイオメトリックテンプレートの認証局：テン

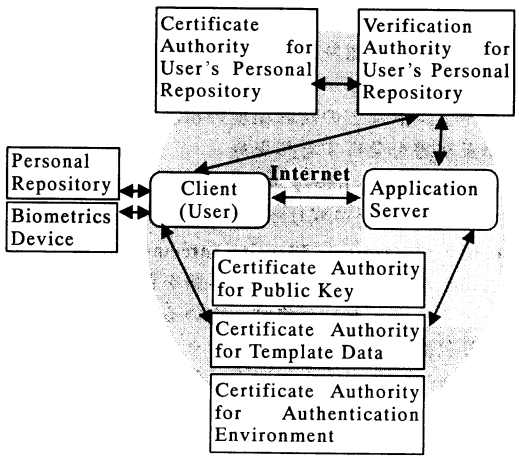


**図 3**　提案するオープンネットワーク上のバイオメトリック認証のフレームワーク

表 2 個人リポジトリ所有者証明書

| # | Item | Contents |
|---|---|---|
| 1 | Identify Information of personal repository. | 個人リポジトリの識別情報（例：ベンダ情報，製品のシリアル番号） |
| 2 | Owner's Identity Information | 個人リポジトリの所有者情報 |
| 3 | Issuer Name & ID | 証明書発行者の識別情報及び証明書の ID 番号 |
| 4 | Valid period of the certificate | 証明書の有効期間（X.509 の形式） |
| 5 | The number of stored certificates, ***n*** | 個人リポジトリに格納されている証明書の個数 |
| 6 | Information of stored certificate 1 | 個人リポジトリに格納されている証明書 1 の識別情報（例：証明書の種類，証明書を発行した CA の URI，証明書の ID) |
| | ... 以下証明書の個数分続く | |
| 5 + ***n*** | Information of stored certificate ***n*** | 個人リポジトリに格納されている証明書 ***n*** の識別情報 |
| 6 + ***n*** | Issuer's Digital Signature | #1～#6+***n*** のディジタル署名および署名アルゴリズム |

プレート証明書（後述）を発行する認証局．

- 認証環境の認証局：バイオメトリックデバイス，個人リポジトリデバイス，認証ソフトウェア，クライアントなどの認証環境の精度，安全性に関する証明書を発行する認証局

### 3.1. ユーザの個人リポジトリ所有者証明書

表 2 に個人リポジトリ所有者証明書の定義を示す．この証明書は"**Owner's Identity Information**"のフィールドにより所有者の氏名などの情報を格納している．また，個人リポジトリが格納している証明書の識別情報により公開鍵証明書とテンプレート証明書との関連付けを行っている．この証明書は個人リポジトリの所有者自身と所有者の検証局にのみ配布される．これにより公開鍵証明書とテンプレート証明書から個人の情報が漏洩する危険を減らすことが可能となると考えられる．

表 3 バイオメトリックテンプレート証明書

| # | Item | Contents |
|---|---|---|
| 1 | Certificate Identifier | テンプレート証明書の識別情報（シリアル番号） |
| 2 | Personal Repository Identity Information | 個人リポジトリの識別情報（個人情報リポジトリの URI，ベンダ情報，製品のシリアル番号） |
| 3 | Issuer Name & ID | 証明書発行者の識別情報及び証明書の ID 番号 |
| 4 | Valid period of the certificate | 証明書の有効期間（X.509 の形式） |
| 5 | Template Information | バイオメトリックテンプレートの種類，品質，ハッシュ値，バイオメトリック認証のアルゴリズム識別情報 |
| 6 | Issuer's Digital Signature | #1～#5 のディジタル署名，署名アルゴリズム識別情報 |

### 3.2. テンプレート証明書

表 1 において，テンプレートフォーマットは"**Certificate Identity Information**"フィールドと"**Template Data**"フィールドを含んでいる．この問題は上で述べた課題がある．そこで，テンプレート証明書と公開鍵証明書とを間接的に関連付けを行う目的で"**Personal Repository Identity Information**"フィールドを設ける．また，テンプレートデータの漏洩を防ぐためにテンプレートデータを証明書の内部に直接含むのではなく，ハッシュ値を含むことによりテンプレートデータの完全性を検証できるようにする必要があると考えられる[14],[15]．そこで，表 3 のテンプレート証明書を提案する．

### 3.3. 認証プロセス

この節では個人リポジトリ所有者証明書の検証とバイオメトリック認証による認証プロセスについて述べる．(図 4 参照)

1) 個人リポジトリの所有者に関する検証

ここでは個人リポジトリが正当な所有者について検証を行う．このプロセスは個人リポジトリ，アプリケーションサーバ，検証機関により行われる．アプリケーションサーバはこの段階ではまだ利用者は匿名となる．

i) 利用者は認証セッション開始のリクエスト ***RequestAuthSession*** をアプリケーションサーバ **AS** に送信する．

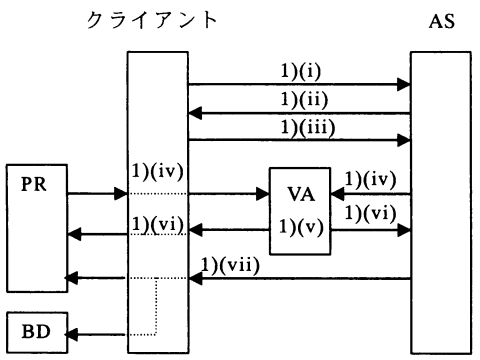


図 4　個人リポジトリの認証プロセス
（AS：アプリケーションサーバ，
PR：個人リポジトリ，BD：バイオメトリックデバイス，VA：個人リポジトリ所有者の検証機関）

ii)　アプリケーションサーバはレスポンスとしてセッション開始情報 ***SessionInfo*** を利用者（個人リポジトリ）に送信する．

iii)　利用者は個人リポジトリのデバイス証明書 $Cert_{PRdevice}$ をアプリケーションサーバ AS に対して送信する．

iv)　アプリケーションサーバ **AS** は検証機関 **VA** に対して個人リポジトリ **PR** についての正当な所有者の存在について検証のリクエスト $RequestVerf_{Prowner}$，利用者の個人リポジトリのデバイス証明書，認証に必要な証明書のリストを送信する．同時に利用者は VA に対して個人リポジトリの所有者検証のリクエスト $RequestVerf_{Prowner}$，利用者が認証を求めているアプリケーションサーバの URI，個人リポジトリのデバイス証明書 $Cert_{PRdevice}$，個人リポジトリの所有者証明書 $Cert_{Prowner}$ を送付する．

v)　**VA** は利用者とアプリケーションサーバ **AS** からのリクエストが同一の認証セッションであることを検証する．**VA** は個人リポジトリのデバイス証明書 $Cert_{PRdevice}$，所有者証明書の $Cert_{Prowner}$ のディジタル署名の検証，失効の検証を行う．検証結果として，個人リポジトリに正当な所有者の有無の確認結果を示す ***PrownerExist***，アプリケーションサーバが認証に必要な証明書の有無の確認結果 ***CertExist*** と **VA** によるディジタル署名 $h(k_{VA}, PrownerExist \mid CertExist)$ により

$$VerfResult = PrownerExist \mid CertExist \mid h(k_{VA}, PrownerExist \mid CertExist)$$

を生成する．ただし式中の $k_{VA}$ は **VA** の秘密鍵を表す．

vi)　**VA** は利用者とアプリケーションサーバに対して検証結果 ***VerfResult*** を送信する．

vii)　アプリケーションサーバは ***VerfResult*** の検証を行い，**VA** の検証結果から個人リポジトリの所有者の存在が確認され，認証に必要な証明書を格納していることが分かった場合，アプリケーションサーバにて利用可能なバイオメトリック認証方式のリスト ***BioAuthList*** を利用者（個人リポジトリ）に送信する．個人リポジトリの所有者の検証に失敗した，もしくはアプリケーションサーバが要求する証明書を個人リポジトリが保持していない場合には，セッション終了コード ***ExitSession*** を送信する．

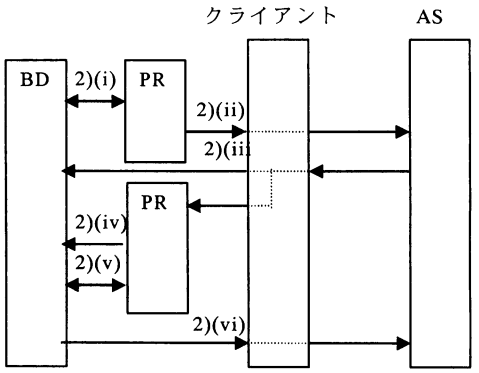


図 5　バイオメトリック認証プロセス

2)　バイオメトリック認証プロセス

バイオメトリック認証は図 5 のフローに従って実行される．ここでは ***BioAuthList*** によるバイオメトリックデバイス **BD** の選択，テンプレート証明書の検証，バイオメトリック認証の照合が行われる．

i)　利用者はクライアントに接続されているバイオメトリックデバイス **BD** のうち，***BioAuthList*** に挙がっているデバイス証明書 $Cert_{BD}$ を収集する．

ii)　収集した $Cert_{BD}$ に個人リポジトリが署名しアプリケーションサーバに送信する．ただし ***BioAuthList*** にクライアントで利用可能なバイオメトリック認証方式が無かった場合には，***NoBioAuthSys*** をアプリケーションサーバに送信する．

iii)　アプリケーションサーバはバイオメトリックデバイス **BD** のデバイス証明書を検証してセキュリティポリシを満たした場合には

バイオメトリック認証開始コード ***StartBioAuth*** を送る．そうでない場合にはセッション終了コード ***ExitSession*** を送信する．

iv) 利用者はバイオメトリックデバイス **BD** に表3のテンプレート証明書を送信する．

v) バイオメトリックデバイス **BD** はテンプレート証明書を検証し，テンプレートが認証に必要な品質を持っていた場合，利用者の個人リポジトリにテンプレート送信のリクエストを行い，照合を行う．

vi) 照合結果，スコア情報をアプリケーションサーバに送信する．

### 3.4. 安全性に関する考察

上で提案したフレームワークは個人リポジトリを正当な所有者が利用していることをバイオメトリック認証により認証を行っており，この段階まではアプリケーションサーバでは利用者は匿名となっている．利用者と所有者の同一性は検証機関 **VA** において検証され，アプリケーションサーバは検証結果として同一性の情報しか受け取ることが出来ない．したがってこのモデルにおいて検証機関 **VA** が利用者と結託した場合に安全なシステムと言えなくなる．

また，本提案では個人リポジトリにおいてデバイスとしての耐タンパ性を仮定する必要がある．また，通信内容の検証を必要とするため，チャレンジレスポンスの検証，ディジタル署名の生成，検証の演算能力を仮定する必要がある．

## 4. まとめ

本論文でオープンネットワークでのバイオメトリック認証のフレームワークについて提案した．本提案ではテンプレート証明書と公開鍵証明書が同時に送信されることによる個人情報漏洩の可能性を提言するために，個人リポジトリの所有者に関する検証機関を設置し，アプリケーションサーバに対して利用者の匿名性を保持した．これによりバイオメトリック認証時の匿名性を保証することが可能となった．また，提案したフレームワークの安全性について議論を行った．

今後の課題として本モデルをより一般的な認証モデルに拡張し，バイオメトリックデータ(ロウデータ，テンプレートデータなど)の保護技術について検討を行う必要がある．

**謝辞**

本研究は（財）電気通信普及財団研究助成を受けて行われた．

## 文　献

[1] Paul Reid, “Biometrics for Network Security”, PRENTICE HALL Professional Technical Reference, 2004.

[2] 榊純一，“IC 旅券の標準化動向と日本の取り組み”，信学会，ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会第3回研究発表会，pp. 69-82, Sep. 2004

[3] Russell Housley, Warwick Ford, Tim Polk, David Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC3280, Network Working Group Standard Track, 2002

[4] Antonio Lioy, Marius Marian, Natalia Moltchanova, *et al.* ,” The EuroPKI Experience”, Public Key Infrastructure: First European PKI Workshop: Research and Applications, EuroPKI 2004 (LNCS3093), pp. 14- 27, 2004

[5] Yoshiaki Isobe, Youich Seto, Masanori Kataoka, “Development of Personal Authentication System Using Fingerprint with Digital Signature”, Proceedings of the 34th Hawaii International Conference on System Sciences 2001, 2001

[6] 磯部義明，瀬戸洋一，“PKI とバイオメトリクスを連携した本人認証の課題と要件”，2004 年暗号と情報セキュリティシンポジウム，pp. 561-566, Jan. 2004

[7] 池田竜朗，森尻智昭，才所敏明，“本人確認環境認証方式の提案”，コンピュータセキュリティシンポジウム 2002，pp. 337-342, Oct. 2002.

[8] Yasushi Yamazaki, Naohisa Komatsu, “A Secure Communication System Using Biometric Identity Verification”, IEICE Transaction of Information & Systems, Vol. E84-D, No. 7, pp. 879-884, 2001

[9] Kaoru Uchida, “Fingerprint Identification for Enhanced User Interface and for Secure Internet Services”, IEICE Transaction of Information & Systems, Vol. E84-D, No. 7, pp. 806-811, 2001

[10] Hao Feng, Chan Choong Wah, “Private key generateon from on-line handwritten signatures”, Information Management & Computer Security, 10/4, pp.159-164, 2002

[11] Yukio Itakura, Shigeo Tsujii, “Proposal on Bio-PKI in which DNA Personal Identifier is embedded in Public Key”, The Third International Workshop for Applied Public Key Infrastructure, pp. 108-113, Oct. 2004.

[12] Fernaldo L. Podio, Jeffrey S. Dunn, Lawrence Reinert, Catherine Tilton, Lawrence O’ Gorman, M. Paul Collier, Mark Jerde, Brigitte Wirtz, “Common Biometric Exchange File Format (CBEFF)”, National Institute of Standards and Technology (NIST), (2001)

[13] Stefan Santesson, Tim Polk, Magnus Nystrom, “Internet X. 509 Public Key Infrastructure: Qualified Certificate Profile”, RFC3739, Network Working Group Standard Track, 2001.

[14] 上繁義史，櫻井幸一，“BioPKI の生体認証過程における生体情報の機密性に関する研究”，コンピュータセキュリティシンポジウム 2004(CSS2004)，pp. 517-522, Oct. 2004

[15] 上繁義史，櫻井幸一，“生体認証を伴う PKI の認証過程における生体情報の機密性確保に関する考察”．学際的情報セキュリティ総合科学シンポジウム，Nov. 2004