平成１5年度経済産業省委託事業成果

基準認証研究開発事業
バイオメトリクス認証結果保証基盤の開発
平成１5年度成果報告書

平成１6年 3月

東芝ソリューション株式会社

目次

1. バイオメトリクス認証結果保証基盤の開発

１．１ 委託業務実施計画

１．１．１ 研究開発の目的

身体的特徴あるいは行動パターンなどを利用して本人の識別を行うバイオメトリクス要素技術の発展に伴い、これらの技術を応用したシステム構築の試みが活発化している。近い将来、実用展開が本格化するものと思われる。

こうした状況を踏まえ、バイオメトリクス技術に関するさまざまな標準化・規格化が ISO/IEC JTC1 SC37 を中心に進められている。しかし、これらの議論のほとんどは、バイオメトリクスデバイスの互換性や、バイオメトリクス関連データや情報の流通性の確保、客観的評価基準などについてのインタフェース、データ形式、プロトコル、評価方式の標準化が中心となっている。

しかし、バイオメトリクス技術をシステムレベルで、かつインターネットを利用したアプリケーションに活用していくためには、バイオメトリクスデバイス周辺の要素技術の標準化だけではなく、バイオメトリクスデバイスを利用した本人確認技術を適用するシステム側の視点からの標準化をも行うことが不可欠である。すなわち、この応用システム側の視点から見て、本人確認結果の信頼性を確認できるような、プロトコルや信頼性を裏付けるデータの形式、その検証方法などについて、何らかの標準的な仕組みが必要であると考える。

本調査研究では、現状のバイオメトリクスデバイス周りの技術の標準化に加え、応用システム側の視点からの標準化の必要性を世に問い、国際標準化の場での具体的な議論を喚起することが目的である。

応用システムの例としては、今後さらに大きく発展するであろう EC での利用を念頭に置いた、PKI をベースとした本人確認システムへバイオメトリクス技術を適用する利用モデルを対象とした。この応用システム側の視点からの見た様々な仕様や課題を抽出、検討し、標準化対象項目を洗い出し、適切かつ安全な仕様、対策案などを提案するのが狙いである。

１．１．２ 実施計画の細目

バイオメトリクスをインターネットなどのオープン環境に適用するためには、以下の 2点

- 認証が安全な環境（認証デバイス、環境）で行われていること
- 認証結果が改竄されていないこと

を認証者（認証する組織・人）に対して保証することが必要である。

本調査研究では、このような保証の仕組みを実現するために必要な、3つの国際標準

1. バイオメトリクス認証結果保証基盤に関する国際標準
2. バイオメトリクス認証プロトコルに関する国際標準
3. バイオメトリクス・デバイス証明書のプロファイルに関する国際標準

を提唱することを目標としている。

以下に3年間のスケジュールを示す。

研究項目	平成15年度	平成16年度	平成17年度
バイオメトリクス認証結果保証基	調査・課題抽出	仕様策	標準化活
バイオメトリクス認証プロトコル	調査・課題抽出	仕様策	標準化活
バイオメトリクスデバイス証明書のプロファイル	調査	各標準化団体への対	

1．1．3 実施場所

社団法人 日本自動認識システム協会 東芝ソリューション分室

住所 実施場所） 東京都府中市片町 3― 22

1．1．4 実施期間

平成 15 年 12 月 4 日 から 平成 16 年 3 月 25 日 まで

1．1．5 実施計画日程

研究項目	12月	1月	2月	3月
保証基盤の調査検討	問題点抽出・課題の明確化			
認証プロトコルの調査検討		調査・課題抽出		
デバイス証明書の調査検討		調査・検討		

１．２ 平成 15 年度活動報告

１．２．１ 活動項目

今年度の調査研究では、最終目標としている3つの国際標準の提唱に向けて、以下の 3つを行うことを目標としている。

1. バイオメトリクス認証結果保証基盤の調査検討
2. バイオメトリクス認証プロトコルの調査検討
3. デバイス証明書についての調査検討

バイオメトリクスをネットワークなどのオープン環境に適用するには、認証者（認証する組織・人）に対して安全な環境と認証結果が改竄されていない事を保証する必要がある。具体的には、以下の作業を実施する。

1. バイオメトリクス認証結果保証基盤の調査検討
   バイオメトリクスをオープン環境で利用する際の現状の問題点を整理し、今後の課題を明確にするとともに、本技術の仕様について纏める。
2. バイオメトリクス認証プロトコルの調査検討
   バイオメトリクス認証結果保証基盤を実現するために必要となる、公開鍵基盤（PKI）を用いたバイオメトリクス認証プロトコルに関する調査を行い、その有効性や付随する課題について纏める。
3. デバイス証明書についての調査検討
   ＳＣ37ＷＧ5、Biometrics WG（Biometrics Test Center（米国））、National Physical Laboratory（英国）、Communications Electoronics Security Group（英国）の共同ＷＧや、ＩＮＳＴＡＣ（国内）などで検討されているデバイスの精度評価基準との連携を取るための調査と、RFC3039 Qualified Certificate Profile、ANSＩX9．84などとの連携を取るための調査を行い、その結果を纏める。

１．２．２ 活動・成果の概要

バイオメトリクスを用いた認証には様々な応用方式が考えられる。本調査研究ではその中でもっとも発展性があると考えられるオープンネットワーク環境での Electronic Commerce(以降 EC)個人認証モデルを、バイオメトリクス認証技術を応用する対象個人認証システムとして想定した。まず、バイオメトリクスを用いたこのモデルの一般的な処理の流れについて整理し、データと処理フローの観点からその脅威分析を行い、セキュリティ面での課題を抽出した。

このモデルに存在するセキュリティ課題には、現時点での標準的な技術や仕様、あるいは標準化が進められている技術だけでは解決できないものが残っている。通常、システム処理上の重要なデータやアプリケーションに対する改竄やデータ盗難、処理結果のなりすましなどのセキュリティ課題を解決する手段がない場合、すなわち攻撃への防御や検知、対応が十分に行うことができる仕組みがなければ、そのシステムは当然信頼できないものと見なさざるを得ない。バイオメトリクス技

術による本人確認結果を用いた個人認証システムの場合も同様であり、その処理結果の有効性を保証するには、既存の技術や標準化に加えて、さらにこれら既存技術や標準仕様では解決できない課題に対応する仕組みが不可欠であると言える。

本調査研究ではその課題を解決するためのフレームワーク案を考案し、それらのリスクが克服できる見通しを得た。

本調査研究活動では、まず関連性の高い技術や標準化動向の調査を行い、その結果を踏まえた上で、以下ののように調査検討を実施した。

1. 対象モデルの定義
   概要：「1. 2. 2 (1) 1)対象モデルの定義」
   詳細：「1. 3. 1対象モデル」
2. 脅威分析
   概要：「1. 2. 2 (1) 2)脅威分析）
   詳細：「1. 3. 2脅威分析」
3. セキュリティ対策の検討
   概要：「1. 2. 2 (1) 3)セキュリティ対策の検討）
   詳細：「1. 3. 3セキュリティ対策の検討」
4. 解決方式案の提案
   概要：「1. 2. 2 (1) 4)解決方式の提案）、「1. 2. 2 (2)バイオメトリクス認証結果保証基盤」
   詳細：「1. 3. 4バイオメトリクス認証結果保証基盤」
5. 検討課題
   概要：「1. 2. 2 (1) 5)検討課題）
   詳細：「1. 3. 5検討課題」

本調査研究活動との関連のある技術についての調査結果は、特に関係の深いものを「1. 4関連する技術・標準化動向と検討課題」に抜粋し、他は付録として本報告書に含めている。ここで得られた調査結果は、次年度以降に実施する、システムモデルの明確な定義と、標準化すべき項目の確定、その仕様案の策定のベースとなる予定である。

また、本調査研究の今年度活動として、2004 年 2 月にシドニーで開催された ISO/IEC JTC 1/SC 37 WG4 Meeting にて、日本のアクティビティ紹介という形で発表を行った。（参照「1. 5国際標準化活動」）

(1) 活動概要

1) 対象モデルの定義

本調査研究では、バイオメトリクス技術応用モデルのうち、調査研究対象モデルを「図 2 - 1EC 個人認証モデル」に示すような EC 個人認証モデルとしている。このモデルを対象としたのは、PKI+バイオメトリクス技術のオープンなネットワーク環境での利用モデルとしてもっとも将来性の高い広

範なモデルであると考えられるためである。

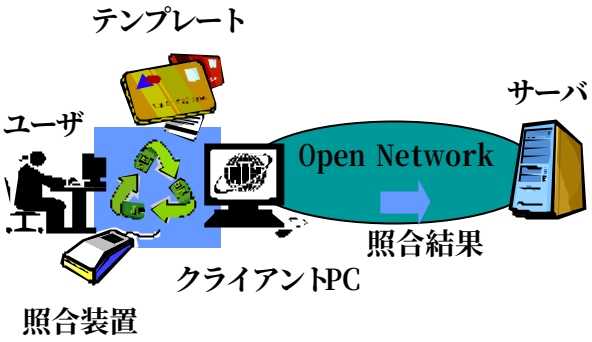


図 2 - 1 EC 個人認証モデル

このモデルの特徴は以下の通りである。

- サービスを提供するサーバと、サービスを受けるユーザが使用するクライアント端末はインターネットなどのオープンなネットワークで接続されている
- ユーザはバイオメトリクスを用いた認証を行いサーバからサービスを受ける
- クライアント端末は PCを想定する。PCのセキュリティ強度は利用形態や管理によって異なるため、ここではPCの信頼性や安全性は存在しないものとみなす。
- オープンネットワークはインターネットを想定する。
- テンプレートが入った個人情報管理用セキュアリポジトリは、ユーザ自身が管理する
- バイオメトリクス照合処理はクライアントPC に接続されたバイオメトリクスデバイス上で行う

このモデルには多様なシステム構成形態が存在するが、今回はそれぞれのモデルについて個別に検討する前に、共通する処理フローとデータを調査し、整理したものを検討対象モデルとしてまとめた。対象モデルの処理フローは検討のため、

- バイオメトリクス照合用テンプレートの登録と管理
- クライアント端末で実行されるユーザの本人確認処理
- サービス提供者へのサービス要求とサービス提供者側での個人認証処理

の 3つのフェーズに分割して、各フェーズ毎に一般的な処理について整理した。

本調査研究では、厳密には個人認証処理に直接関係する範囲のみを対象としているため、「バイオメトリクス照合用テンプレートの登録と管理」フェーズは主対象ではないが、他の 2つの処理の検討を行う上で、照合用テンプレートに関する処理の検討を全く行わずに実施するのは難しいため、一応の対象としてここで挙げている。

2) 脅威分析

対象モデルについて、取り扱うデータと処理フローの2つの観点からその脅威を分析し、セキュリティ課題を抽出した。この抽出されたセキュリティ課題の中で現時点での標準的な技術や仕様などで対応できない問題は、その解決のために何らかの新しい技術や仕様、フレームワークを必要とするものであると考えられる。本調査研究ではこれらを主対象課題とし、以降で検討および対策案の策定している。

分析は、対象モデルシステムの信頼性と可用性を守るためにセキュリティを保持しなければならないと考えられる資産を対象とし、まずこれらの資産毎の脅威分析を行った後、さらに対象モデルシステムの処理フロー上で脅威が発生する可能性について分析する、という方式をとった。また本調査研究では、

- 安全性が確保されなければ、システム全体の信頼性、すなわち個人認証結果の信頼性を失わせることになると思われるもの
- 攻撃によって何らかの損傷を被った場合、システム全体の可用性に影響を及ぼすと考えられるもの

のようなデータを資産と見なし、脅威を、「データ盗難」「データ改竄・破壊」「データすり替え」の3種類に限定している。

図 2 - 2 EC 個人認証モデルでの脅威」では、脅威分析結果の概略を示している。

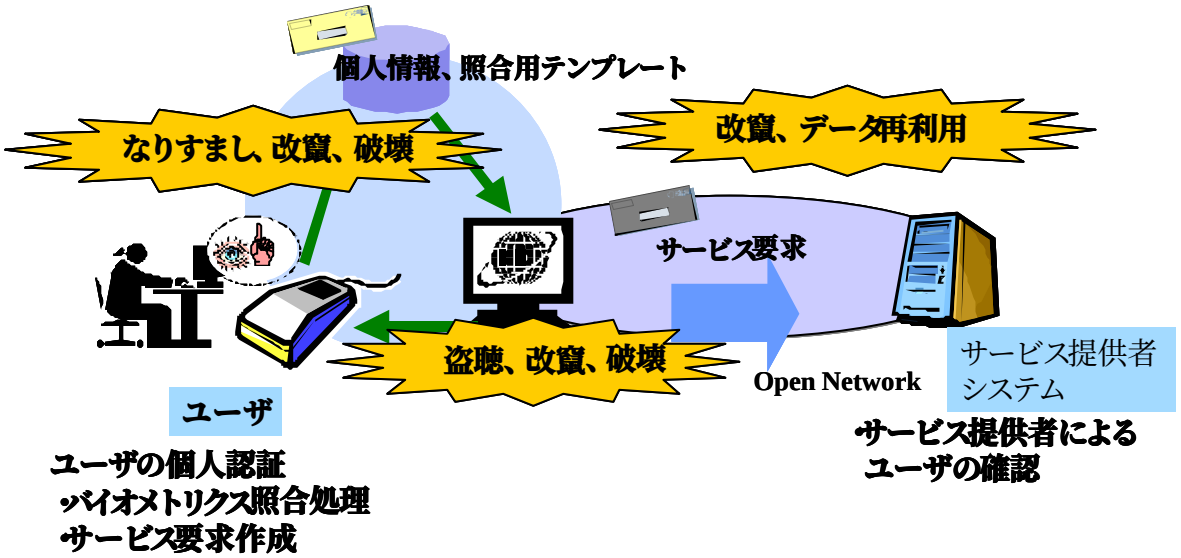


図 2 - 2 EC 個人認証モデルでの脅威

3) セキュリティ対策の検討

実装すべきセキュリティ機能を洗い出すため、脅威分析の実施結果から、それぞれの資産と脅威の組み合わせ毎に、個別にセキュリティ対策を検討した。これらの対策案を、本調査研究の目的である「ユーザの本人確認処理」から「サービス要求とサービス提供者側での個人認証処理」に至るまでの処理フローのセキュリティに関係する部分を抽出し、実装すべきセキュリティ対策を一覧にまとめた。

4) 解決方式の提案

検討したセキュリティ対策や機能を実装し、システム全体としてのセキュリティを実現するためのフレームワーク バイオメトリクス認証結果保証基盤を解決案として導いた。

- 主な構成

  本調査研究では、バイオメトリクス認証結果保証基盤フレームワークの構成を、以下の3つのパートに分けて機能実装することを提案している。

  - デバイス認証基盤

    バイオメトリクス本人確認処理を行うクライアント端末で使用するバイオメトリクスデバイスの情報を、デバイス証明書という形で保証することを主目的とする基盤。
  - デバイスと個人情報管理システム・リポジトリ間のセキュリティ強化プロトコル

    秘密鍵のような個人の機密情報を悪意のあるデバイスや攻撃から守るためのプロトコル。
  - 本人確認処理結果保証プロトコル

    サービス提供者側がオープンネットワークごしに、ユーザの本人確認処理の実行環境を確認し、そのデバイスの処理実行結果が改竄されていないかを検証するためのプロトコル。
  - その他

    実装形態がアプリケーション実行環境のハードウェア構成やソフトウェア構成に依存する部分が大きく、バイオメトリクス認証結果保証基盤フレームワーク内で基準となる案を限定しない方がよいと思われるものを、前提条件あるいは要求項目として挙げている。
- 構成要素

  また、バイオメトリクス認証結果保証基盤フレームワークを実現するために、必要な要素として、以下の項目を挙げている。

  - デバイス証明書

    バイオメトリクスデバイスに対してデバイス認証基盤により発行される証明書。バイオメトリクス照合処理結果などの改竄検知や、オープンネットワークごしでのデバイス情報の確認等に使用する。
  - テンプレート証明書

    ユーザの照合用テンプレートデータの証明書。
  - バイオメトリクスデバイスの機能拡張

バイオメトリクスデバイス自身も、個人の秘密情報の安全性を保障できるような実行環境を持つ必要がある。

- 個人情報管理用セキュアリポジトリ
  照合用テンプレートデータを管理する個人情報管理用セキュアリポジトリ側で、アクセス元のデバイス情報、正当性を確認するための情報、手段が必要である。

- 処理シーケンス例
  ここでは、フレームワーク案がどのように機能し、どのようなプロトコルを必要とするかについてシーケンスの具体例を挙げている。
  - ユーザの個人認証（ユーザの本人確認処理＋サービス要求とサービス提供者側での個人認証処理）
  - デバイス情報の登録～デバイス証明書の発行
  - バイオメトリクス照合用テンプレートの登録と管理

5) 検討課題

対象モデルのセキュリティ脅威への対策案として、必要だと考えられるセキュリティ機能やプロトコルを実装するようなフレームワーク案そのものについて、検討すべき課題について以下の項目毎にまとめた。

- デバイス認証基盤
- プロトコル
- デバイス証明書
- テンプレート証明書
- その他

これらの課題には、バイオメトリクス認証結果保証基盤の仕様詳細を検討する過程で何らかのセキュリティ仕様や対策によって解決しなければならないものと、このフレームワークを利用したシステムを構築する際に満たすべき要求項目として挙げるものの2種類が存在する。両者ともフレームワークの実現に密接に関連しているため、後者の要求事項を意識せずに調査研究を継続することは難しいが、来年度以降の調査研究では、本フレームワーク案に関係の深い、前者の課題の検討を重点的に実施する予定である。

⑵ バイオメトリクス認証結果保証基盤

本調査研究では、EC 個人認証モデルのセキュリティ課題の解決案として、バイオメトリクス認証結果保証基盤を導入した。「

図 2 - 3 バイオメトリクス認証結果保証基盤」は基盤の構成を簡単に示した図である。

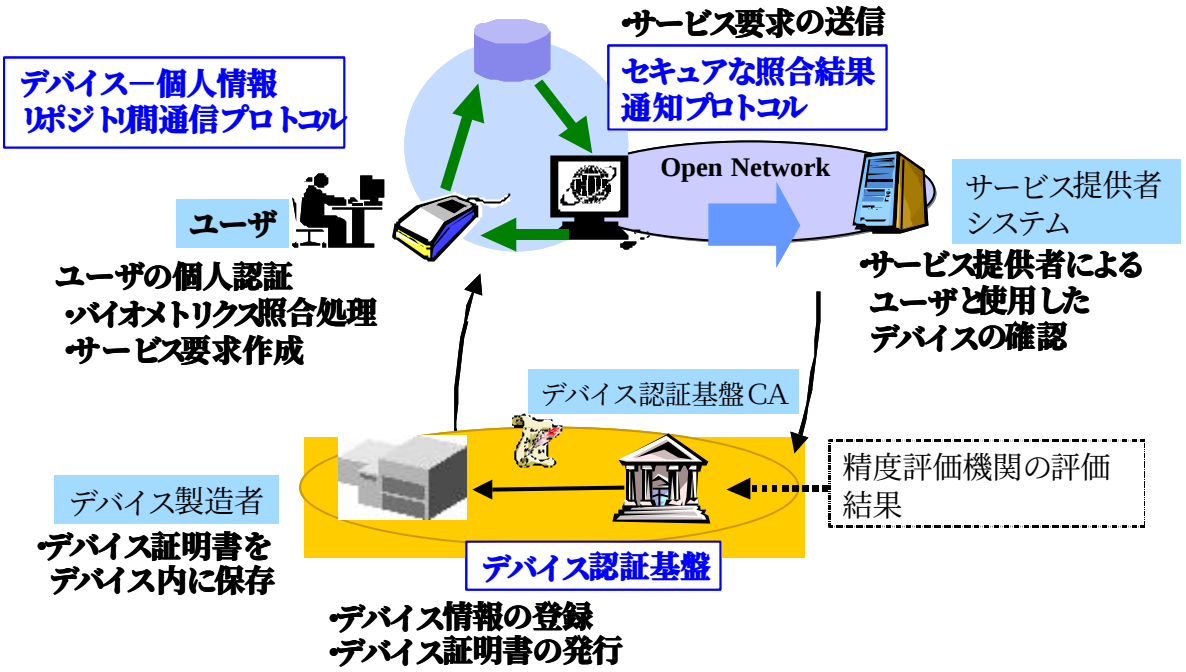


図 2 - 3 バイオメトリクス認証結果保証基盤

このバイオメトリクス認証結果保証基盤の構成する要素の1つであるデバイス証明書は、図の下部、デバイス認証基盤によって発行・管理が行われる。このデバイス証明書によって、以下の機能が実装可能になる。

- 照合用テンプレートデータや個人情報の保護
- ユーザが使用したバイオメトリクスデバイスをサービス提供者が知ることができる
- バイオメトリクスデバイスの認証
- 個人情報管理セキュアリポジトリの認証

なお、バイオメトリクス認証結果保証基盤のシーケンス例は「図 2 - 4 バイオメトリクス認証結果保証基盤のシーケンス例」のようなものが考えられる。詳細については、次年度以降、検討する。

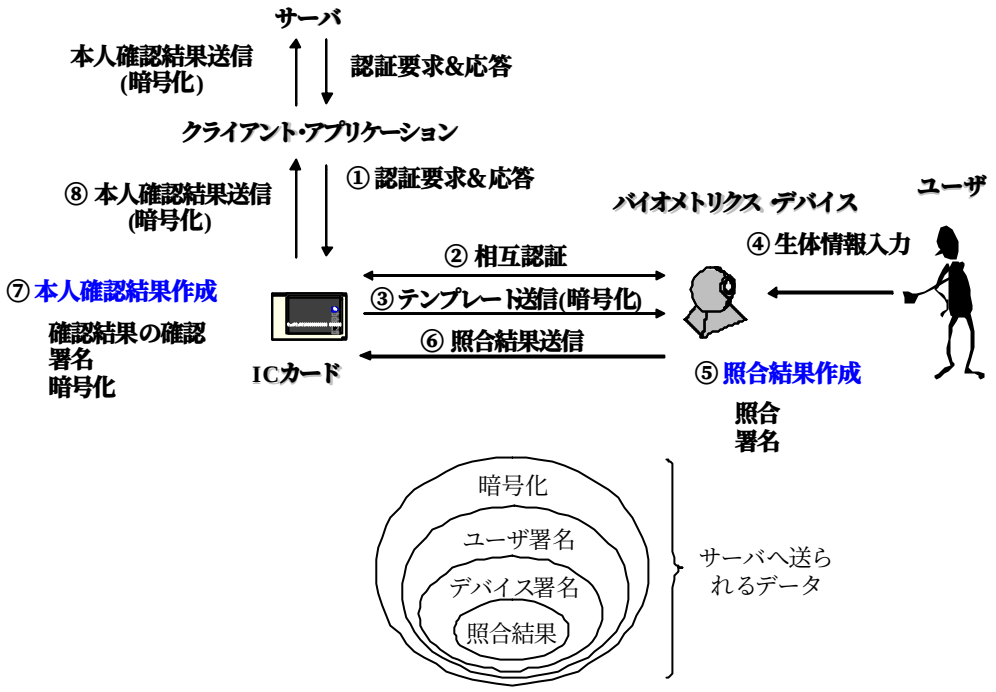


図 2 - 4 バイオメトリクス認証結果保証基盤のシーケンス例

1．2．3 活動項目ごとの検討結果(要約)

今年度は、目標として掲げた3つの項目について、以下のように調査研究を実施し、結果を得た。

- バイオメトリクス認証結果保証基盤の調査検討
  バイオメトリクス認証結果保証基盤に必要となるデバイス認証基盤の位置づけや、デバイスメーカーの役割などについて定義した。また、個人用証明書として公開鍵証明書を用いた場合、バイオメトリクスデバイスに耐タンパー性のようなセキュリティ強化機能が必要になることを明らかにした。
- バイオメトリクス認証プロトコルの調査検討
  バイオメトリクス認証結果保証基盤を実現する上で必要となる以下の2つのプロトコルについて、その主要部分についての検討を行った。
  - デバイスと個人情報管理用セキュアリポジトリ間のセキュリティ強化プロトコル
  - 本人確認処理結果保証プロトコル
- デバイス証明書についての調査検討
  フレームワーク案中でデバイス証明書によって実現されるセキュリティ機能の検討を行い、

フォーマットや実装のために解決すべき課題についてまとめた。ただし、デバイス証明書が使用する照合精度値やバイオメトリクスデバイスの評価手法の開発は、本調査研究では取り扱わず、SC37WG5 などで検討されている評価結果を利用するものとする。

１．３ Electronic Commerce 個人認証モデルにおける PKI+バイオメトリクス技術の適用検討

本章では、まず対象となるモデルについて整理し、次に、扱うデータと、処理フローの 2つの点からモデルの脅威分析を行いセキュリティ的な課題を抽出する。その後、抽出された課題について、現時点で一般に流通しているバイオメトリクスデバイスが実装しているセキュリティ技術や、標準的な技術によって対応できないまま残る問題点についての考察と対策の提案、さらに提案を実現するために検討すべき課題についてまとめる。

１．３．１ 対象モデルの定義

本調査研究では、バイオメトリクス技術応用モデルのうち調査研究対象モデルを、PKI+バイオメトリクス技術のオープンなネットワーク環境での利用モデルとしてもっとも将来性の高い EC 個人認証モデルとしている。このモデルの特徴は以下の通りである。

- サービスを提供するサーバと、サービスを受けるユーザが使用するクライアント端末はインターネットなどのオープンなネットワークで接続されている
- ユーザはバイオメトリクスを用いた認証を行いサーバからサービスを受ける
- クライアント端末は PCを想定する。PCのセキュリティ強度は利用形態や管理によって異なるため、ここではPCの信頼性や安全性は存在しないものとみなす。
- オープンネットワークはインターネットを想定する。
- テンプレートが入った個人情報管理用セキュアリポジトリは、ユーザ自身が管理する
- バイオメトリクス照合処理はクライアントPC に接続されたバイオメトリクスデバイス上で行う

まず初めに EC 個人認証モデルでの処理を、

- バイオメトリクス照合用テンプレートの登録と管理
- クライアント端末で実行されるユーザの本人確認処理
- サービス提供者へのサービス要求とサービス提供者側での個人認証処理

の 3つのフェーズに分割して検討する。

本調査研究では、厳密には個人認証処理に直接関係する範囲のみを対象としているため、「バイオメトリクス照合用テンプレートの登録と管理」フェーズは主対象ではないが、他の 2つの処理の検討を行う上で、照合用テンプレートに関する処理の検討を全く行わずに実施するのは難しいため、一応の対象としてここでは挙げている。

この章では、対象モデルの脅威分析を行う前に、この 3つのフェーズについて、それぞれ一般的な処理概要を記述している。

⑴ バイオメトリクス照合用テンプレートの登録と管理

バイオメトリクス照合用テンプレートの登録と管理モデルの処理フローと主な登録、管理先は以下のようなものが想定できる。

- 処理フロー
  1. ユーザのバイオメトリクスデータがデバイスを使って取得され、テンプレート生成アプリケーションに渡される。
  2. テンプレート生成アプリケーションは生成した照合用テンプレートを保管先に保存する。
  3. 保存されたテンプレートは、必要に応じて他の場所にコピーされる。
- バイオメトリクス照合用テンプレートの保存、管理先
  - バイオメトリクスデバイス内リポジトリ
    ユーザが使用するバイオメトリクスキャプチャ・照合用デバイス内の通常のデータ記憶用リポジトリに保持する方法。
  - PC内リポジトリ
    ユーザが使用する端末、PC、携帯電話、PDAなどに付属している通常のデータ記憶用リポジトリに保持する方法。セキュリティを強化はされていない。
  - セキュアリポジトリ
    Smart Cardなどセキュリティを強化したストレージ、リポジトリにテンプレートを保持する方式。
  - サービス提供者システム
    政府機関、サービスプロバイダなどクライアントの認証を行い、サービスを提供するサービス提供者側のサーバなどに保持する方式。
  - 第三者認証機関システム
    ユーザの認証のみを行う第三者機関のサーバなどに保持する方式。
- テンプレート生成アプリケーションの実行環境
  - バイオメトリクスデバイス内
    ユーザが使用するバイオメトリクスキャプチャ・照合用デバイス上でアプリケーションを実行する方法。
  - PC内リポジトリ
    ユーザが使用する端末、PC、携帯電話、PDA上でアプリケーションを実行する方法。セキュリティを強化はされていない。
  - セキュアリポジトリ
    Smart Cardのような、セキュリティを強化したリポジトリなどのシステムでアプリケーションを実行する方式。
  - サービス提供者システム
    政府機関、サービスプロバイダなどクライアントの認証を行い、サービスを提供するサ

ービス提供者側のサーバでアプリケーションを実行する方式。

■ 第三者認証機関システム

ユーザの認証のみを行う第三者機関のサーバなどでアプリケーションを実行する方式。

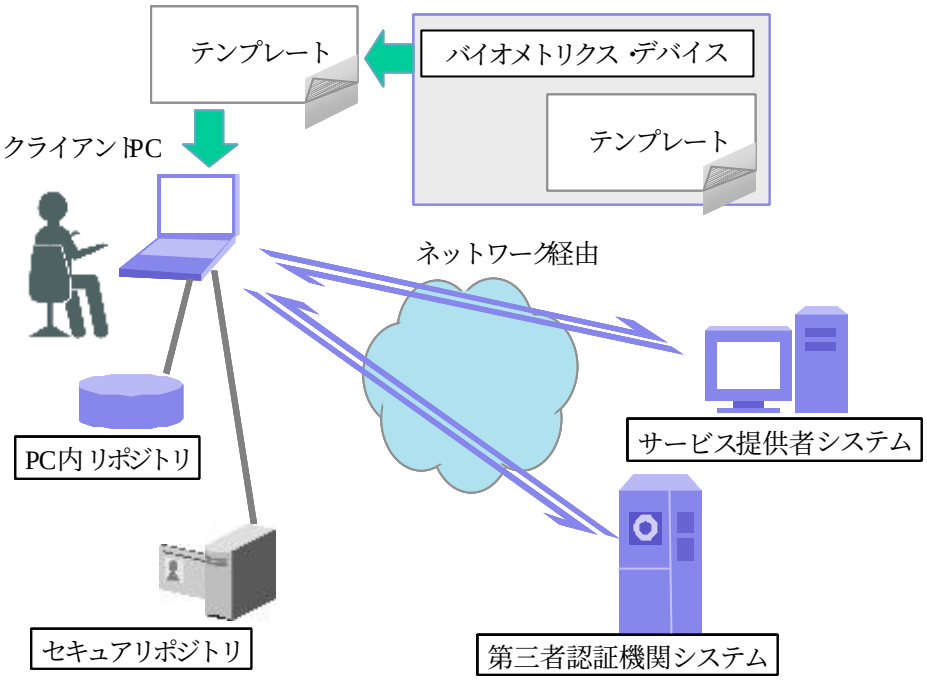


図 2 - 5 バイオメトリクス照合用テンプレートの管理

⑵ ユーザの本人確認処理

バイオメトリクス技術を使った本人確認処理モデルの処理フローは以下のものが想定できる。

➢ 処理フロー

1. サービス利用者からサービスを受けるための、ログインアプリケーションやサービス要求アプリケーションからの要求に応じて、クライアントPC上でバイオメトリクス技術を利用する本人確認アプリケーションが起動される。
2. ユーザのバイオメトリクスデータがデバイスを使って取得され、本人確認アプリケーションに渡される。
3. 本人確認アプリケーションが、照合用テンプレートをその保存先から得る。
4. 本人確認アプリケーションは、取得したバイオメトリクスデータとユーザの照合用テンプレートを元に、照合処理を実行する。
5. 本人確認アプリケーションは、本人であると判断可能かどうかの照合結果を出力する。

➢ バイオメトリクス照合・認証処理の実行環境

■ バイオメトリクスデバイス内でバイオメトリクスデータの照合、認証を行うモデル

■ クライアントPCでバイオメトリクスデータの照合、認証を行うモデル

■ ハードウェアセキュリティモジュール内でバイオメトリクスデータの照合、認証を行うモデル

■ サービス提供者システムで、バイオメトリクスデータの照合、認証を行うモデル

■ 第三者認証機関システムで、バイオメトリクスデータの照合、認証を行うモデル

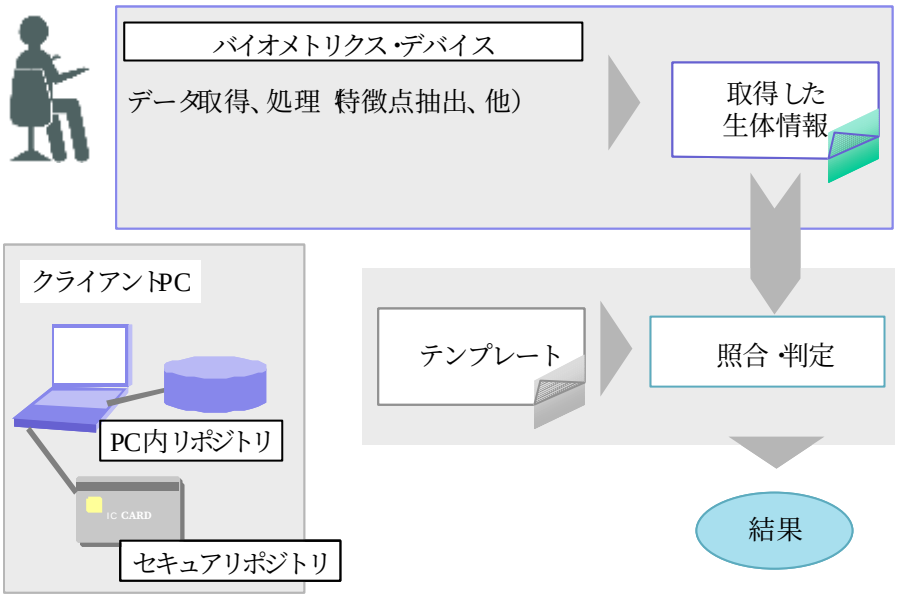


図 2 - 6 バイオメトリクス照合判定処理

1) 本人確認処理における検討対象モデル

テンプレートの管理とバイオメトリクスを使った本人確認処理の組み合わせには、上記の処理モデルの全ての組が考えられるが、ここでは、

- 本人確認処理の実行環境は、テンプレート保存先と同等か、それ以上のセキュリティ強度であること
- 本人確認処理の実行環境とテンプレート保存先との間で、オープンネットワークを経由しないこと。これは、ユーザのバイオメトリクス・ロウ・データと照合用テンプレートが、同じタイミングで、オープンネットワーク経由で送信されることを避けるためである。

の2つを条件とすると、次表のように示される。

		テンプレート保存先				
		デバイス	通常ストレージ	セキュアストレージ	サービス提供者システム	第三者認証機関システム
照合処理実行	デバイス	○	○	○		
	PC		○	○		
	セキュアストレージ			○		
	サービス提供者システム				○	
	第三者認証機関システム					○

図 2 - 7 本人確認処理における検討対象モデルの一覧

本調査研究では、「1. 3. 2脅威分析」の後に、さらにこの組み合わせから検討対象を絞り込む。

⑶ サービス要求とサービス提供者側での個人認証処理

ユーザの本人確認処理の実行結果を元に、サービス提供者にサービスを要求し、サービス提供者がその要求内容を認証するまでの処理について、処理フローと関連するデータを整理する。
本調査研究では、検討対象モデルを、PKI をベースとした個人認証システムへのバイオメトリクス技術を適用するモデルとしているため、ここでの処理内容は限定される。

- ユーザの個人情報の保存、管理先
  - 個人情報管理用セキュアリポジトリ
    Smart Cardのようなセキュリティを強化したストレージ、リポジトリにユーザの個人情報、公開鍵ペアなどの秘密情報を保持する。
- サービス利用要求の作成処理
  - セキュアリポジトリシステム上
    ユーザの個人情報を保存しているSmart Card、セキュアリポジトリ上で処理を実行する。
- 処理フロー

1. 「1. 3. 1 ⑵ ユーザの本人確認処理」に記述した処理が行われる。サービス要求アプリケーションからの要求に応じて、クライアントPC上でバイオメトリクス技術を利用する本人確認アプリケーションが起動され、照合結果が得られる。
2. 得られた照合結果は、クライアントPC 上で実行されているサービス要求実行アプリケーションに渡される。
3. 照合結果がOKの場合、サービス要求実行アプリケーションはユーザの秘密鍵を使用して、サービス利用要求データを作成する。
4. サービス利用要求データがサービス提供者システムに送信される。
5. サービス提供者システムは、受信した要求データの署名などを検証して、許可を求め

るユーザの個人認証を行う。認証結果がOKの場合、サービスの利用を許可する。

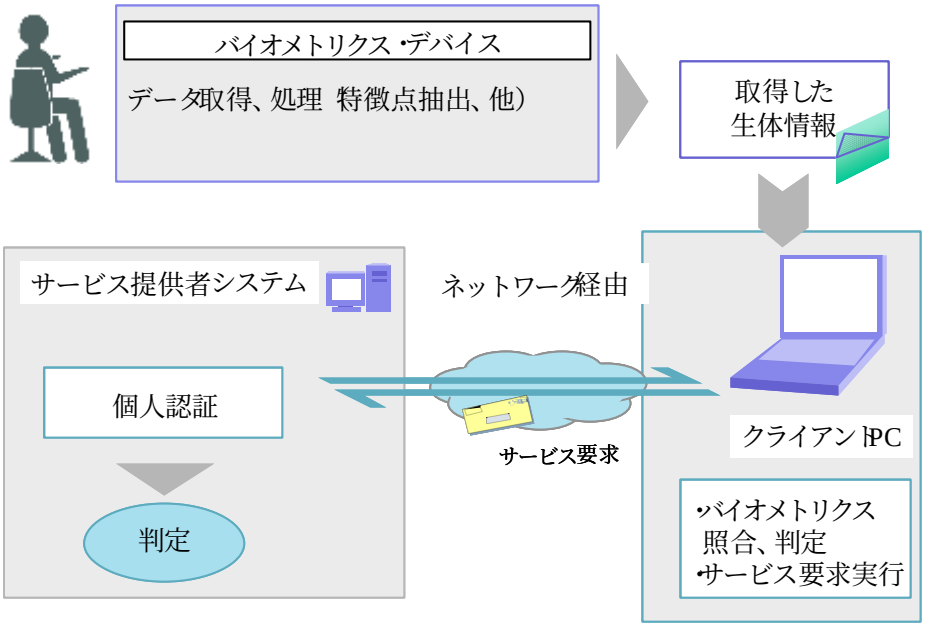


図 2 - 8 個人認証処理の流れ

1．3．2 脅威分析

この章では、前章で処理フローやデータ管理についてまとめたモデルについて、脅威分析を行っている。まず、データや秘密情報などの資産の安全性に問題がある場合に生じる損害についてまとめた後、それらの資産に対するセキュリティ侵害がどのような場合に起こりうるかを、前章同様に対象モデルを3つのフェーズに分けて行っている。

⑴ 資産

ここでは、バイオメトリクスを利用した個人認証処理上で、

- 安全性が確保されなければ、システム全体の信頼性、すなわち個人認証結果の信頼性を失わせることになると思われるもの
- 攻撃によって何らかの損傷を被った場合、システム全体の可用性に影響を及ぼすと考えられるもの

ようなデータを資産と見なした。具体的には、以下の4つのデータが資産として検討している。

- ユーザのバイオメトリクス照合用テンプレート
- ユーザのバイオメトリクス・ロウ・データ 認証のために都度採取するもの）
- バイオメトリクス照合処理結果

- 個人情報（個人認証用秘密鍵、個人識別可能な情報他）

それぞれの資産に対して、「データ盗難」「データ改竄・破壊」「データすり替え」の3種類の攻撃ごとに、攻撃が成功した場合にどのような問題が発生するか、その影響度について分析した。
攻撃自体がどの処理で起こりうるか、可能性などについては、この後の処理フローごとの脅威分析で検討している。

- ユーザのバイオメトリクス照合用テンプレート
  - データ盗難

    個人のバイオメトリクス情報から照合用テンプレートが生成されるが、逆に、照合用テンプレートから個人の情報を逆生成することは難しいため、テンプレートデータが盗まれても、即、なりすましなどの危険性が高まることは考えられにくい。
  - データ改竄・破壊

    テンプレートデータの改竄や破壊は、そのテンプレートの持ち主であるユーザの個人認証処理への妨害につながり、システム全体の利便性を損なうというセキュリティ脅威になる。
  - データすり替え

    管理者権限を持つユーザAのテンプレートの代わりに、権限を持たないユーザBのテンプレートをこっそり差し替えられれば、あたかも管理者AであるかのようにユーザBがなりすましできる可能性がある。
- ユーザのバイオメトリクス・ロウ・データ（認証のために都度採取するもの）
  - データ盗難

    盗んだデータのコピーの再利用が可能な場合、すなわち盗んだデータをあたかも今キャプチャしたかのようにバイオメトリクス照合用アプリケーションに渡すことができれば、本人へのなりすましが可能になる。
  - データ改竄・破壊

    データの改竄、破壊は、ユーザの個人認証処理への妨害につながり、システム全体の利便性を損なうというセキュリティ脅威になる。
  - データすり替え

    データのすり替えが可能な場合は、管理者権限を持つユーザAのデータにすり替えることで、あたかも管理者AであるかのようにユーザBがなりすましできる可能性がある。
- バイオメトリクス照合処理結果
  - データ盗難

    照合処理結果が盗み見られるだけでは、特にセキュリティ上の危険性が高まるとは考えられにくいが、データフォーマットが知られることは後述するような問題を引き起こす可能性がある。
  - データ改竄・破壊

    照合処理結果の改竄や破壊は、個人認証処理への妨害につながり、システム全体の

利便性を損なうため、有効なセキュリティ脅威になると見なせる。たとえば、OK であるという処理結果を他のシステムやアプリケーションに渡す場合、その間にデータの改竄が行われ、NGであるように書き換えられると当然受けることができるサービスが受けられないなどの被害をもたらす。

- データすり替え

  データすり替えによって実際にあたかも正当な照合処理を実行したかのように見せかけて、結果のみを再利用できれば、管理者権限を持つユーザAの照合結果を使って、権限を持たないユーザBがあたかも管理者Aであるかのようになりすましできる可能性がある。

- 個人情報（個人認証用秘密鍵、個人識別可能な情報他）
  - データ盗難

    個人情報の盗難は、詳細を記述するまでもなく、近年大きな問題となっている重要なセキュリティ懸念事項である。
  - データ改竄・破壊

    個人情報データを元に個人認証を行うため、このデータに対する改竄や破壊は、個人認証処理への妨害につながり、システム全体の利便性を損なうため、有効なセキュリティ脅威になると見なせる。
  - データすり替え

    データのすり替えは、個人認証処理への妨害、または管理者権限を持つユーザへのなりすましなどの問題を引き起こす。

(2) 処理フロー

1) バイオメトリクス照合用テンプレートの登録と管理

本章では、処理ごとに、これらのデータに対して考えられる脅威の可能性について記述している。

- 対象資産
  - ユーザのバイオメトリクス照合用テンプレート
  - ユーザのバイオメトリクス・ロウ・データ（認証のために都度採取するもの）
- 処理フロー上の脅威
  - バイオメトリクス照合用テンプレートの登録と管理
    - ① 照合用テンプレートへの攻撃
      - バイオメトリクス照合用テンプレート生成アプリケーション処理への妨害
      - テンプレート生成アプリケーション実行環境がウィルスに感染していたり、バックドアが存在する危険性
      - テンプレート保存先のセキュリティ脆弱性の存在や物理的破壊の可能性
      - テンプレートデータが保存先に送信される通信経路上での攻撃

② テンプレートを生成するために採取されるバイオメトリクス・ロウ・データへの攻撃

- バイオメトリクス照合用テンプレート生成アプリケーション処理への妨害
- バイオメトリクス・ロウ・データがデバイスからテンプレート生成アプリケーション実行環境まで送信される通信経路上での攻撃

2) ユーザの本人確認処理

クライアント端末上におけるユーザの本人確認処理で、アクセスすることになる資産は、以下のものになる。本章では、処理ごとに、これらのデータに対して考えられる脅威の可能性について記述している。

- 対象資産
  - ユーザのバイオメトリクス照合用テンプレート
  - ユーザのバイオメトリクス・ロウ・データ（認証のために都度採取するもの）
- 処理フロー上の脅威
  - バイオメトリクス技術を使った本人確認処理
    - ① 本人確認のために採取されるバイオメトリクス・ロウ・データへの攻撃
      - バイオメトリクスデバイス内での改竄、盗聴などの攻撃
      - バイオメトリクス・ロウ・データがデバイスから照合アプリケーション実行環境まで送信される通信経路上での攻撃
      - 照合アプリケーション実行環境がウィルスに感染していたり、バックドアが存在する危険性
    - ② 本人確認のために使用されるテンプレートデータへの攻撃
      - テンプレート保存先のセキュリティ脆弱性の存在や物理的破壊の可能性
      - テンプレートデータが保存先から照合アプリケーション実行環境に送信される通信経路上での攻撃
      - 照合アプリケーション実行環境がウィルスに感染していたり、バックドアが存在する危険性

3) サービス要求とサービス提供者側での個人認証処理

ユーザの本人確認処理の実行結果を元に、サービス提供者にサービスを要求し、サービス提供者がその要求内容を認証するまでの処理で、アクセスすることになる資産は、以下のものになる。本章では、処理ごとに、これらのデータに対して考えられる脅威について記述している。

- 対象資産
  - バイオメトリクス照合処理結果
  - 個人情報（個人認証用秘密鍵、個人識別可能な情報他）
- 処理フロー上の脅威
  - ① バイオメトリクス照合結果への攻撃

- 照合アプリケーション実行環境がウィルスに感染していたり、バックドアが存在する危険性
- バイオメトリクス照合結果が照合アプリケーション実行環境からサービス利用要求データ作成アプリケーション実行環境に送信される通信経路上での攻撃
- サービス利用要求データ作成アプリケーション実行環境がウィルスに感染していたり、バックドアが存在する危険性

② 個人情報への攻撃

- テンプレート保存先のセキュリティ脆弱性の存在や物理的破壊の可能性
- サービス利用要求データ作成アプリケーション実行環境がウィルスに感染していたり、バックドアが存在する危険性
- 個人情報を元に作成されたサービス利用要求データが作成アプリケーション実行環境からサービス提供者システムに送信される通信経路上での攻撃

１．３．３ セキュリティ対策の検討

この章では、前章での脅威分析の結果に対して、有効だと考えられる対策について検討している。まず、資産毎の脅威に対して個別に対策案を考え、その後でそれらを統合しシステム全体としてセキュリティを保つために必要な機能を洗い出す。

⑴ 資産－脅威別対策案

次表は、資産毎に発生する脅威と発生箇所、すなわちセキュリティ課題を表にし、課題に対する対策案をまとめたものである。

表 2 - 1 セキュリティ課題 :バイオメトリクス照合用テンプレート

保護資産	発生箇所	脅威内容		対策項目	
		種類	詳細	対策内容	案
ユーザのバイオメトリクス照合用テンプレート	テンプレート生成アプリケーション実行環	データ改竄・破壊	テンプレートデータの破壊 アプリケーションの処理妨害	アクセス制御	アクセス元、実行要求元の認証 物理的・光学的耐タンパー性
				実行アプリケーションの改竄防止	ソフトウェア耐タンパー性
	テンプレート生成アプリケーション実行環境－テンプレート保存先間ネットワーク	データ改竄・破壊 データすり替え	テンプレートデータの破壊 テンプレートデータのすり替 通信妨害 なりすましによる通信奪取	アクセス制御	相互認証 通信経路の物理的保護
				データ改竄検知	テンプレートへの署名付与 テンプレート証明書
	テンプレート保存先	データ改竄・破壊 データすり替え	テンプレートデータの破壊 テンプレートデータのすり替 不正アクセス 物理的不正アクセス	アクセス制御	アクセス元の認証 ハードウェア耐タンパー性
				データ改竄検知	テンプレートへの署名付与 テンプレート証明書
	テンプレート保存先－照合アプリケーション実行環境間	データ改竄・破壊 データすり替え	テンプレートデータの破壊 テンプレートデータのすり替 通信妨害 なりすましによる通信奪取	アクセス制御	相互認証 通信経路の物理的保護
				データ改竄検知	テンプレートへの署名付与 テンプレート証明書
	照合アプリケーション実行環境	データ改竄・破壊 データすり替え	テンプレートデータの破壊 テンプレートデータのすり替 不正アクセス アプリケーションの処理妨害	保存先のアクセス制御	アクセス元の認証 ハードウェア耐タンパー性
				データ改竄検知	テンプレートへの署名付与 テンプレート証明書
				実行アプリケーションの改竄防止	ソフトウェア耐タンパー性

表２－　２セキュリティ課題：バイオメトリクス・ロウ・データ

保護資産	発生箇所	脅威内容		対策項目	
		種類	詳細	対策内容	案
ユーザのバイオメトリクス・ロウ・データ	バイオメトリクスデバイス上	データ盗難 データ改竄・破壊 データすり替え	キャプチャデータの破壊 キャプチャデータのすり替え 不正アクセス アプリケーションの処理妨害 生体そのものの偽造	データ秘匿	暗号化
				キャプチャデータ再利用防御	時刻データなどの利用 フォーマット・プロトコルの秘匿
				アクセス制御	相互認証 ハードウェア耐タンパー性
				データ改竄検知	キャプチャデータへの署名付与
				実行アプリケーションの改竄防止	ソフトウェア耐タンパー性
				偽造生体の検知他	デバイス製造者の対策に依存
	デバイス－テンプレート生成アプリケーション実行環境間	データ盗難 データ改竄・破壊 データすり替え	キャプチャデータの破壊 キャプチャデータのすり替え 通信妨害 なりすましによる通信奪取	データ秘匿	暗号化
				アクセス制御	相互認証 通信経路の物理的保護
				データ改竄検知	キャプチャデータへの署名付与
	デバイス－照合アプリケーション実行環境間	データ盗難 データ改竄・破壊 データすり替え	キャプチャデータの破壊 キャプチャデータのすり替え 通信妨害 なりすましによる通信奪取	データ秘匿	暗号化
				アクセス制御	相互認証 通信経路の物理的保護
				データ改竄検知	キャプチャデータへの署名付与
	照合アプリケーション実行環境	データ盗難 データ改竄・破壊 データすり替え	キャプチャデータの破壊 キャプチャデータのすり替え 不正アクセス アプリケーションの処理妨害	データ秘匿	暗号化
				アクセス制御	相互認証 ハードウェア耐タンパー性
				データ改竄検知	キャプチャデータへの署名付与
				実行アプリケーションの改竄防止	ソフトウェア耐タンパー性

表 2 - 3 セキュリティ課題 :バイオメトリクス照合処理結果

保護資産	発生箇所	脅威内容		対策項目	
		種類	詳細	対策内容	案
バイオメトリクス照合処理結果	照合アプリケーション実行環境	データ盗難 データ改竄・破壊 データすり替え	処理結果の破壊 処理結果のすり替え 不正アクセス アプリケーションの処理妨害	処理結果データ再利用防御	時刻データなどの利用 フォーマット・プロトコルの秘匿
				アクセス制御	相互認証 ハードウェア耐タンパー性
				データ改竄検知	照合処理結果への署名付与
				実行アプリケーションの改竄防止	ソフトウェア耐タンパー性
	照合アプリケーション実行環境－サービス利用要求データ作成アプリケーション実行環境間	データ盗難 データ改竄・破壊 データすり替え	処理結果の破壊 処理結果のすり替え 通信妨害 なりすましによる通信奪取	アクセス制御	相互認証 通信経路の物理的保護
				データ改竄検知	照合処理結果への署名付与
	サービス利用要求データ作成アプリケーション実行環境	データ盗難 データ改竄・破壊 データすり替え	処理結果の破壊 処理結果のすり替え 不正アクセス アプリケーションの処理妨害	アクセス制御	相互認証 ハードウェア耐タンパー性
				データ改竄検知	照合処理結果への署名付与
				実行アプリケーションの改竄防止	ソフトウェア耐タンパー性

表 2 - 4 セキュリティ課題 :個人情報

保護資産	発生箇所	脅威内容		対策項目	
		種類	詳細	対策内容	案
個人情報	個人情報保存先	データ盗難 データ改竄・破壊 データすり替え	個人情報の破壊 個人情報のすり替え 不正アクセス 物理的不正アクセス	個人情報データ秘匿	暗号化
				アクセス制御	アクセス元の認証 ハードウェア耐タンパー性
				データ改竄検知	個人情報への署名付与 個人情報用証明書
	個人情報保存先ーサービス利用要求データ作成アプリケーション実行環境間	データ盗難 データ改竄・破壊 データすり替え	個人情報の破壊 個人情報のすり替え 通信妨害 なりすましによる通信奪取	アクセス制御	相互認証 通信経路の物理的保護
				データ改竄検知	個人情報への署名付与
	サービス利用要求データ作成アプリケーショ	データ盗難 データ改竄・破壊 データすり替え	処理結果の破壊 処理結果のすり替え 個人情報の破壊 個人情報のすり替え 不正アクセス アプリケーションの処理妨害	個人情報データ秘匿	暗号化
				サービス利用要求データ再利用防	時刻データなどの利用 フォーマット・プロトコルの秘匿
				アクセス制御	相互認証 ハードウェア耐タンパー性
				データ改竄検知	処理結果への署名付与
				実行アプリケーションの改竄防止	ソフトウェア耐タンパー性
	サービス利用要求データ作成アプリケーション実行環境ーサービス提供者システム間ネットワーク	データ盗難 データ改竄・破壊 データすり替え	処理結果の破壊 処理結果のすり替え 通信妨害 なりすましによる通信奪取	アクセス制御	相互認証 通信経路の物理的保護
				データ改竄検知	サービス利用要求データへの署

⑵ 実装する対策の検討

資産－脅威の組み合わせ毎に抽出したセキュリティ課題に対する対策案は、

- 現時点で完了しているあるいは進行中のセキュリティに関する標準仕様や技術の適用で対応可能なもの
- 既存技術では対応が難しいか何らかの拡張が必要なもの

の2種類に分けることができる。本調査研究の対象としているのは、「ユーザの本人確認処理」から「サービス要求とサービス提供者側での個人認証処理」に至るまでの処理フローに関係する部分である。したがって、ここではさらに、調査対象に該当するかどうかという条件を加え、対策案を

- 既存技術で対応可能なもの
- 既存技術で未対応あるいは何らかの既存技術の拡張が必要なもので、本調査研究の対象内
- 既存技術で未対応あるいは何らかの既存技術の拡張が必要なもので、本調査研究の対象外

の3つに分けてまとめた。その一覧を「表 2 - 5 セキュリティ課題に対する対策案一覧」に示している。表中、「対策－既存」欄で「○」で示しているものは、既存技術のみで対応可能だと思われるもの、「△」は既存技術をベースになんらかの拡張が必要だと考えられるものである。

表２－５セキュリティ課題に対する対策案一覧

保護資産	発生箇所	対策項目		対策			
		対策内容	案	番号	既存	対象内	対象外
	テンプレート生成アプリケーション実行環境	アクセス制御	アクセス元、実行要求元の認証				○
			物理的・光学的耐タンパー性				○
		実行アプリケーションの改竄防止	ソフトウェア耐タンパー性				○
	テンプレート生成アプリケーション実行環境－テンプレート保存先間ネットワーク	アクセス制御	相互認証		△		○
			通信経路の物理的保護				○
		データ改竄検知	テンプレートへの署名付与	1		○	
			テンプレート証明書				
	テンプレート保存先	アクセス制御	アクセス元の認証	2		○	
			ハードウェア耐タンパー性		△		○
		データ改竄検知	テンプレートへの署名付与	3		○	
			テンプレート証明書				
	テンプレート保存先－照合アプリケーション実行環境間	アクセス制御	相互認証	4	△	○	
			通信経路の物理的保護				○
		データ改竄検知	テンプレートへの署名付与	5		○	
			テンプレート証明書				
	照合アプリケーション実行環境	保存先のアクセス制御	アクセス元の認証	6		○	
			ハードウェア耐タンパー性		△		○
		データ改竄検知	テンプレートへの署名付与	7		○	
			テンプレート証明書				
		実行アプリケーションの改竄防止	ソフトウェア耐タンパー性				○
ユーザのバイオメトリクス・ログ・データ	バイオメトリクスデバイス上	データ秘匿	暗号化		△		○
		キャプチャデータ再利用防御	時刻データなどの利用				○
			フォーマット・プロトコルの秘匿				○
		アクセス制御	相互認証				○
			ハードウェア耐タンパー性		△		○
		データ改竄検知	キャプチャデータへの署名付与				○
		実行アプリケーションの改竄防止	ソフトウェア耐タンパー性				○
		偽造生体の検知他	デバイス製造者の対策に依存				○
	デバイス－テンプレート生成アプリケーション実行環境間	データ秘匿	暗号化		△		○
		アクセス制御	相互認証		△		○
			通信経路の物理的保護				○
		データ改竄検知	キャプチャデータへの署名付与				○
	デバイス－照合アプリケーション実行環境間	データ秘匿	暗号化		△		○
		アクセス制御	相互認証		△		○
			通信経路の物理的保護				○
		データ改竄検知	キャプチャデータへの署名付与				○
	照合アプリケーション実行環境	データ秘匿	暗号化				○
		アクセス制御	相互認証	8		○	
			ハードウェア耐タンパー性		△		○
		データ改竄検知	キャプチャデータへの署名付与				○
		実行アプリケーションの改竄防止	ソフトウェア耐タンパー性				○
バイオメトリクス照合処理結果	照合アプリケーション実行環境	処理結果データ再利用防御	時刻データなどの利用	9		○	
			フォーマット・プロトコルの秘匿				
		アクセス制御	相互認証	10		○	
			ハードウェア耐タンパー性		△		○
		データ改竄検知	照合処理結果への署名付与	11		○	
		実行アプリケーションの改竄防止	ソフトウェア耐タンパー性				○
	照合アプリケーション実行環境－サービス利用要求データ作成アプリケーション実行環境間	アクセス制御	相互認証	12		○	
			通信経路の物理的保護				○
		データ改竄検知	照合処理結果への署名付与	13		○	
	サービス利用要求データ作成アプリケーション実行環境	アクセス制御	相互認証	14		○	
			ハードウェア耐タンパー性		△		○
		データ改竄検知	照合処理結果への署名付与	15		○	
		実行アプリケーションの改竄防止	ソフトウェア耐タンパー性				○
個人情報	個人情報保存先	個人情報データ秘匿	暗号化		○		
		アクセス制御	アクセス元の認証		○		
			ハードウェア耐タンパー性		○		
		データ改竄検知	個人情報への署名付与		○		
			個人情報用証明書		○		
	個人情報保存先－サービス利用要求データ作成アプリケーション実行環境間	個人情報データ秘匿	暗号化		○		
		アクセス制御	相互認証	16		○	
			通信経路の物理的保護				○
		データ改竄検知	個人情報への署名付与		○		
	サービス利用要求データ作成アプリケーション実行環境	個人情報データ秘匿	暗号化		○		
		サービス利用要求データ再利用防	時刻データなどの利用	17		○	
			フォーマット・プロトコルの秘匿				

以上の検討結果を対策対象範囲に限ると、実装しなければならないセキュリティ機能は以下のようにまとめることができる。各末尾の番号は、「表 2 - 5 セキュリティ課題に対する対策案一覧」の対策番号と一致する。

① 照合用テンプレート生成アプリケーションによる、照合用テンプレートデータへの署名付加機能、あるいはテンプレート証明書かそれに類するものの利用 (1,3,5,7)
② 照合用テンプレート保存先のアクセス制御(2)
③ 照合用テンプレート保存先－照合アプリケーション実行環境間の相互認証(4)
④ 照合アプリケーション実行環境のアクセス制御(6,8,10)
⑤ 照合アプリケーション実行結果の再利用防止(9)
⑥ 照合アプリケーション実行結果の改竄検知(11,13,15)
⑦ 照合アプリケーション実行環境－サービス利用要求データ作成アプリケーション実行環境間の相互認証(12)
⑧ サービス利用要求データ作成アプリケーション実行環境のアクセス制御(14,18)
⑨ 個人情報保存先－サービス利用要求データ作成アプリケーション実行環境間の相互認証(16)
⑩ サービス利用要求データ作成アプリケーション実行結果の再利用防止(17)
⑪ サービス利用要求データ作成アプリケーション実行結果の改竄検知(19,21)
⑫ サービス利用要求データ作成アプリケーション実行環境－サービス提供者システム間の相互認証(20)

１．３．４ バイオメトリクス認証結果保証基盤

本章では、前章で検討したセキュリティ対策や機能を実装し、システム全体としてのセキュリティを実現するためのフレームワーク、バイオメトリクス認証結果保証基盤を解決案として導き、その構成、プロトコルの提案を記述している。

(1) 対象モデルとセキュリティ機能の整理

要求される機能から、以降では「1. 3. 1 (2)ユーザの本人確認処理」のテンプレートの保存・管理先と、バイオメトリクス照合処理実行環境の組み合わせ一覧「図 2 - 7 本人確認処理における検討対象モデルの一覧」のうち、検討対象をあらかじめ

- 照合用テンプレートは、個人情報管理用セキュアリポジトリに保存する
- バイオメトリクスデータ照合処理はバイオメトリクスデバイスで実行する

場合の組み合わせに絞ることとする。

対象を限定した理由は次の通りである。まず、実システム上、照合用テンプレートをデバイス上やサーバ上に持たせずに、Smart Card のようなセキュアリポジトリでユーザ毎に持たせる場合の利点には、ユーザが自分のプライバシーにかかわるデータを第三者へ提供せずに済むこと、照合テンプレートデータに対応しているバイオメトリクスデバイスならば、何でも使用できることなどが挙げられる。また、デバイスあるいはサーバ上に複数のユーザのテンプレートデータをまとめて管理する方法は外部あるいは内部犯による

情報流出などの脅威にさらされやすく、法制上こうしたデータの集中管理を禁じている国もある。

照合処理をバイオメトリクスデバイスで行うモデルを対象にした理由としては、一般に流通しているデバイスにこのタイプが多いことが挙げられる。また、最近、Smart Cardで使用しているような耐タンパーチップに従来のPKIベースの個人認証処理機能に加えて、バイオメトリクス情報のキャプチャや照合処理を行えるように拡張したチップの研究・開発が進んでいるが、第一段階としての処理シーケンスを検討しその問題点や課題を抽出する上では、バイオメトリクス情報のキャプチャや照合処理機能と、この個人認証処理機能を持つモジュールを分けて検討した方がよいと判断したためもある。

また、

- サービス利用要求データ作成は、個人情報管理用セキュアリポジトリ上で行う

ものとする。これはPKIをベースとした個人認証システムでは、個人の秘密鍵のような秘密情報を使用して行う処理は通常Smart Cardのようなセキュリティを強化したハードウェア上で行うのが一般的だからである。

以上のようにモデルを限定した結果、実装すべきセキュリティ機能は次のように整理できる。

① 個人情報管理用セキュアリポジトリ－バイオメトリクスデバイス間の相互認証(4,12)
② 個人情報管理用セキュアリポジトリ間－サービス提供者システム間の相互認証(20)
③ 照合用テンプレート生成アプリケーションによる、照合用テンプレートデータへの署名付加機能、あるいはテンプレート証明書かそれに類するものの利用 (1,3,5,7)
④ バイオメトリクスデバイスで実行される照合アプリケーション実行結果の改竄検知(11,13,15)
⑤ 個人情報管理用セキュアリポジトリで実行されるサービス利用要求データ作成アプリケーション実行結果の改竄検知(19,21)
⑥ バイオメトリクスデバイスで実行される照合アプリケーション実行結果の再利用防止(9)
⑦ 個人情報管理用セキュアリポジトリで実行されるサービス利用要求データ作成アプリケーション実行結果の再利用防止(17)
⑧ 個人情報管理用セキュアリポジトリのアクセス制御(2, 14,18)
⑨ バイオメトリクスデバイスのアクセス制御(6,8,10)

(2) 主な構成

バイオメトリクス認証結果保証基盤ではその機能を3つのパートに分けて、セキュリティ機能の実装方法を検討した。それぞれの機能概要は以下の通りである。

1) デバイス認証基盤

対応するセキュリティ機能：①(③)④

デバイス認証基盤は、デバイスに関する情報を保証された状態で提供する基盤である。デバイスの情報には名称や用途、製造者名、公称性能、仕様などの基本情報に加え、セキュリティ/精度評価基準に基づいた評価結果のような付加情報なども想定している。実装機能としては、デバイスに対するデバイス証明書の発行、証明書を発行したデバイスの情報のデータベース登録・管理、サービス提供者の問い合わせに応じた証明書の正当性確認などが考えられる。

デバイス認証基盤に基づいた個人認証処理の例では、まずデバイスが行った処理結果（バイオメトリクス照合結果）にはそのデバイス自身によるデジタル署名が付加される。サービス提供者はデバイス認証基盤が提供するデバイス証明書を用いて、受け取った処理結果のデジタル署名を確認し、デバイスの処理結果に対する改竄の有無を検証したり、どのデバイスを使用したのかを安全に知ることが可能になる。このようにサービス提供者は、ユーザが本人確認処理に利用されたクライアント端末環境をオープンネットワークごしに確認できるため、利用環境そのものの安全性や信頼性検証の一助にもなりうる。

2) デバイスと個人情報管理用セキュアリポジトリ間のセキュリティ強化プロトコル

対応するセキュリティ機能：①(③)④⑥

このプロトコルは、秘密鍵のような、個人を認証するのに必要な情報を悪意のあるデバイスや攻撃から守るためのプロトコルである。このプロトコルでは、デバイス認証基盤によって発行されたデバイス証明書を使って、どのデバイスを使用した結果を元に秘密情報にアクセスしようとしているかを、個人情報管理用セキュアリポジトリが確認できる。個人情報管理用セキュアリポジトリ側がそのデバイスによる処理結果を有効とし、個人情報へのアクセスを許可するかどうかは、さらにそのポリシーなどに依存する。

これまでに行った脅威分析結果から、バイオメトリクス照合用テンプレートは、Smart Cardのようなセキュリティが強化されているリポジトリで保持し、安全性を確保することが望ましい。今回の検討対象モデルでは、バイオメトリクス技術を使用して本人確認を行う際に、このようなセキュアなリポジトリから照合用テンプレートをいったんバイオメトリクスデバイスに送信するというような処理が発生する。また、照合した結果も個人情報管理用セキュアリポジトリに安全に送信される必要がある。これら照合テンプレートや本人確認結果の安全な送受信を実現するために、デバイスと個人情報管理システム・リポジトリ間でセキュリティを強化したプロトコルを策定する。

3) 本人確認処理結果保証プロトコル

対応するセキュリティ機能：②④⑤⑥⑦

このプロトコルは、サービス提供者に対して送信する個人認証・サービス提供要求に、クライアント端末でのデバイス処理実行結果を含めることで、サービス提供者側でそのデータがセキュリティ的に問題のない環境、およびプロセスによる実行結果かどうかを検証できるようにするためのプロトコルである。サービス提供者側にとって、クライアント側の本人確認環境の情報を、セキュリティが保証された状態で得た上で内容の正当性を確認できることは、特に、本調査研究での対象としているオープンネットワークなどを利用した環境での個人認証システムでは重要な要素といえる。

本調査研究での対象モデルでは、本人確認を行うのに使用したデバイスの処理結果にデバイス署名を付加したものを個人情報（個人の秘密鍵）を使ったサービス要求データ作成是非の判断の基とするが、サービス提供者間に、個人情報の開示を制限した上で、適切な範囲でこれらのクライアント環境の情報、処理内容を安全に通知するためのプロトコルが必要である。

4) その他

対応するセキュリティ機能：⑧⑨

これらのセキュリティ機能は、アプリケーションによる処理への割り込み防御や検知、アプリケーションそ

のものの改竄防止などによって対策することが考えられるが、実装形態がアプリケーション実行環境のハードウェア構成やソフトウェア構成に依存する部分が大きいため、本フレームワークでは基準となる案を策定せず、前提条件あるいは要求項目として挙げることとする。

⑶ 構成要素

本フレームワーク案がどのように機能し、どのようなプロトコルを必要とするかについて検討する上で、「1. 3. 4 ⑵主な構成」で記述した機能構成を元に、フレームワークの実現化において不可欠な構成要素や新たに必要だと思われる項目を抽出し、それらが満たすべき条件や実装内容について記述している。なお、今後さらに検討を要すると思われる内容については、「1. 3. 5検討課題」に記述している。

1) デバイス証明書

本調査研究では、バイオメトリクスデバイスに対して第三者機関であるデバイス認証基盤により発行される証明書として、デバイス証明書を想定している。そのデバイスを使って生成したユーザの照合用テンプレートや、採取したバイオメトリクス・ロウ・データ、照合処理結果などにはこの証明書とペアになるデバイス秘密鍵によって署名をつけることができる。

このデバイスを利用した本人確認プロセスは、このデバイス署名を確認することで、データの改竄検知や、ユーザの本人確認処理環境の確認を行うことができる。デバイス証明書に含まれる内容には、デバイスメーカー名や機種名、型番などの基本情報の他に、他の標準化機関や評価機関によるデバイスの評価データのような属性情報なども含むことが可能であると考えられる。

2) テンプレート証明書

バイオメトリクス認証プロトコルでは、バイオメトリクス照合用テンプレートに対して、テンプレート証明書かあるいはそれに類するものを持たせる必要がある。テンプレート証明書は、ユーザのバイオメトリクス本人確認が保証された照合用テンプレートとの照合処理結果によるものであること、言い換えればテンプレートもどきのようなものでなりすましやすり替えなどが行われていないことをサービス提供者が検証するのに最低限必要な情報である。

また、PKIに基づく個人認証へのバイオメトリクス技術の応用のためには、照合用テンプレートデータを個人情報の一部として個人用公開鍵証明書に何らかの手段で関連づけした状態で管理する必要がある。テンプレートデータと、個人用秘密鍵の間に関連づけがされていない場合、そのテンプレートを使ったバイオメトリクス照合結果と、個人用公開鍵証明書・秘密鍵ペアとの間にもなんの関係もないことになってしまい、持ち主の同一性を保証することができない。

ここまでの機能の実現に限れば、生成した照合用テンプレートのハッシュ値にデバイス署名を付加したもので対応することも可能である。

3) バイオメトリクスデバイスの機能拡張

デバイスと個人情報管理システム・リポジトリ間のセキュリティ強化プロトコルは、個人情報保護リポジトリ内の秘密情報を安全性を保つように設計されなければならない。そのためには、このリポジトリ内のデータ

を利用する必要のあるデバイスやサーバ等は以下のようなセキュリティ機能を実装することが不可欠である。

- 自分自身が何者であるかを示す第三者によって保障されたクレデンシャルを持っている
- リポジトリ内の秘密情報やそれに付随する処理結果などを安全にやりとりできるようなセキュア通信機能を実装している。具体的には、暗号化機能、ハッシュ関数、デジタル署名検証、乱数生成関数などである。
- 受信した秘密情報やそれに付随する処理結果、そのために必要な各種データなどを安全に扱える実行環境を持っている

バイオメトリクスデバイスの場合、はじめの1つは今回のフレームワークの機能の1つであるデバイス認証基盤によって実装可能であるが、後の2つについては、必要要件としてデバイス側で必ず実装しなければならない項目であると考えられる。

現在、実際に市場に流通し、個人認証用として使用されているバイオメトリクスデバイスについて、「1. 3. 2脅威分析　(1)資産」で対象とした資産に限定して検討すると、その機能やデータの保持方法、セキュリティの考え方には、以下のような問題点を持つものが多い。

- 照合用テンプレートの保護を行っていない
- 照合用アプリケーションの保護を行っていない
- 取得したユーザのバイオメトリクスデータのコピーや再利用などの防御を行っていない
- 照合用アプリケーションの中には、取得したユーザのバイオメトリクスデータが、再利用されているかどうかをチェックできていないものがある
- 照合結果に対して、照合用アプリケーションはセキュリティ対策を行っていないため、結果に対して改竄などの攻撃が行われた場合に検知できず、信頼性に欠ける

一部には、この問題点に対応する機能を持っているデバイスも存在しているが、それらのデバイスは独自の仕様を採用しており、相互接続性、移植性などは持たないと考えられる。

4) 個人情報管理用セキュアリポジトリ

個人情報管理用セキュアリポジトリは、ユーザの個人情報の他に、個人用公開鍵証明書にひも付けされた照合用テンプレートデータそのものを管理している。この照合用テンプレートデータのすり替えやなりすましを防ぐため、リポジトリ側もアクセス元のデバイス情報、正当性を確認しなければならない。また、リポジトリでは照合結果を元に個人の秘密鍵のような秘密情報へのアクセス可否を判断するが、この照合結果がどのようなデバイスを使用して得られたものかを確認できる手段も必要である。

このように、例えばデバイス証明書を発行しているデバイス認証基盤CAの公開鍵証明書かそれに類するものをリポジトリに持たせるなど、何らかの手段でデバイス証明書を検証できなければならない。

(4) 個人認証シーケンス案

以下では、このフレームワークを基にしてバイオメトリクスを使った個人認証を行う場合の処理シーケンスを記述している。これまで2つのパートに分けていた「ユーザの本人確認処理」と「サービス要求とサーバ側ユーザ認証処理」のフローを「ユーザの個人認証」として1つにまとめて記述した。このシーケンスは案

の1つであり、このフレームワークを実現するためにこれ以外の可能な処理シーケンス、インタフェース、プロトコルを含めたステップ毎の詳細や、順番、セキュリティ整合性の検討などを十分に行った上で、最適な案を採用する必要がある。

(1) 認証セッション確立プロセス

(1-1) ユーザは、クライアント端末上で、デバイス証明書を持つバイオメトリクスデバイスを用いる。まず、ユーザはサービス提供者システムに、サービス要求を行う。

(1-2) サービス提供者はユーザを認証するのに必要な情報を、ユーザに要求する。このときサービス提供者は認証セッションを一意に特定するための情報として、認証セッション情報 *SessionInfo* を送信する。またサービス提供者は自身を証明する情報としてサービス提供者の公開鍵証明書 $Cert_R$、および認証セッションで有効な認証方式のリスト *AuthList* を送信する。

(1-3) サービス提供者からの要求を受けたクライアント端末（個人情報リポジトリシステム）は所有する認証方式が有効であることを確認した後、本人確認プロセスを開始する。

(2) 本人確認プロセス

本人確認プロセスは、ユーザに対して本人確認処理を行い、サービス提供者に対する認証結果を生成するプロセスである。ここでは、公開鍵暗号方式を利用したチャレンジ＆レスポンスによるリポジトリーデバイス間相互認証と、暗号化用鍵交換、照合用テンプレートの提示、本人確認(バイオメトリクス照合処理)、認証結果情報の生成を行っている。

(2-1) 個人情報管理用セキュアリポジトリからバイオメトリクスデバイスに対して本人確認要求開始を通知する。このときチャレンジとして、個人情報管理用セキュアリポジトリが生成した乱数 $rand_U$ および *SessionInfo* を送信する。

(2-2) バイオメトリクスデバイスは個人情報管理用セキュアリポジトリに対して照合用テンプレートを要求する。このときチャレンジとしてバイオメトリクスデバイスが生成した乱数 $rand_D$ と、step2-1 のチャレンジに対するレスポンス $Response_{BD}$ を送信する。レスポンス $Response_{BD}$ にはセッション鍵情報 SK_{info} を含める。

(2-3) 個人情報管理用セキュアリポジトリは、$Response_{BD}$ を検証した後、step2-2 で共有したセッション鍵で暗号化した照合用テンプレート $Enc_{SK}(Sample)$ を送信する。このときともに、step2-2 のチャレンジに対するレスポンス $Response_U$ を送信する。

(2-4) バイオメトリクスデバイスは、ユーザの生体情報を取得する。

(2-5) バイオメトリクスデバイスは、$Response_U$ を検証した後、受け取ったテンプレートと読取った生体情報を照合し、照合結果情報 *VerfResultData* を生成する。

照合結果情報 *VerfResultData* はバイオメトリクスデバイスによる照合処理結果に対してデバイス秘密鍵によりデジタル署名を施したものである。このとき再利用等を防止するために、照合処理を一意に特定できるような情報を含めることが望ましい。たとえば、サービス提供者名や $Cert_R$ の署名値($Cert_R$ のフィールドより取得)、時刻データなどを組み合わせたものが考えられる。

(2-6) 照合結果情報 *VerfResultData* を個人情報管理用セキュアリポジトリに対して送信する。

(2-7) 個人情報管理用セキュアリポジトリは、照合結果情報 *VerfResultData* のデバイス署名を検証する。

(2-8)　個人情報管理用セキュアリポジトリは、認証結果情報 *AuthResultData* を生成する。認証結果情報を構成する要素は、照合結果情報 *VerfResultData* および、送信データに対して個人秘密鍵により施されたデジタル署名 Sig_U である。

(3) 認証応答プロセス

認証応答プロセスは、本人確認プロセスで生成した認証結果情報を、サービス提供者に対して送信するものである。サービス提供者は受け取った認証結果情報を検証することにより、クライアント端末で実行された本人確認処理がどのような環境下で行われたことを確認する。

(3-1)　個人情報管理用セキュアリポジトリは本人確認プロセスによって生成された認証結果情報 *AuthResultData* を、サービス提供者に送信する。このとき個人情報管理用セキュアリポジトリは step1-2 でサービス提供者から受け取った認証セッション情報 *SessionInfo* も送信する。これらの情報は、サービス提供者の公開鍵証明書 $Cert_R$、に含まれる公開鍵によって暗号化された状態で送信される。

(3-2)　サービス提供者は受信した認証結果情報を自身の秘密鍵を使って復号し、ユーザの *AuthResultData* を得る。サービス提供者はこの *AuthResultData* とこれに施されたユーザの署名を検証することで、サービスを要求しているユーザを認証する。

(3-3)　サービス提供者はさらに *AuthResultData* に含まれる照合結果情報 *VerfResultData* を確認し、これに施されたデバイス署名を検証することで、受信した認証結果情報がどのようなクライアント環境で得られたものなのか、またその結果に対して不正が行われていないかを確認した上で、ユーザに対するサービス提供の可否を決定する。

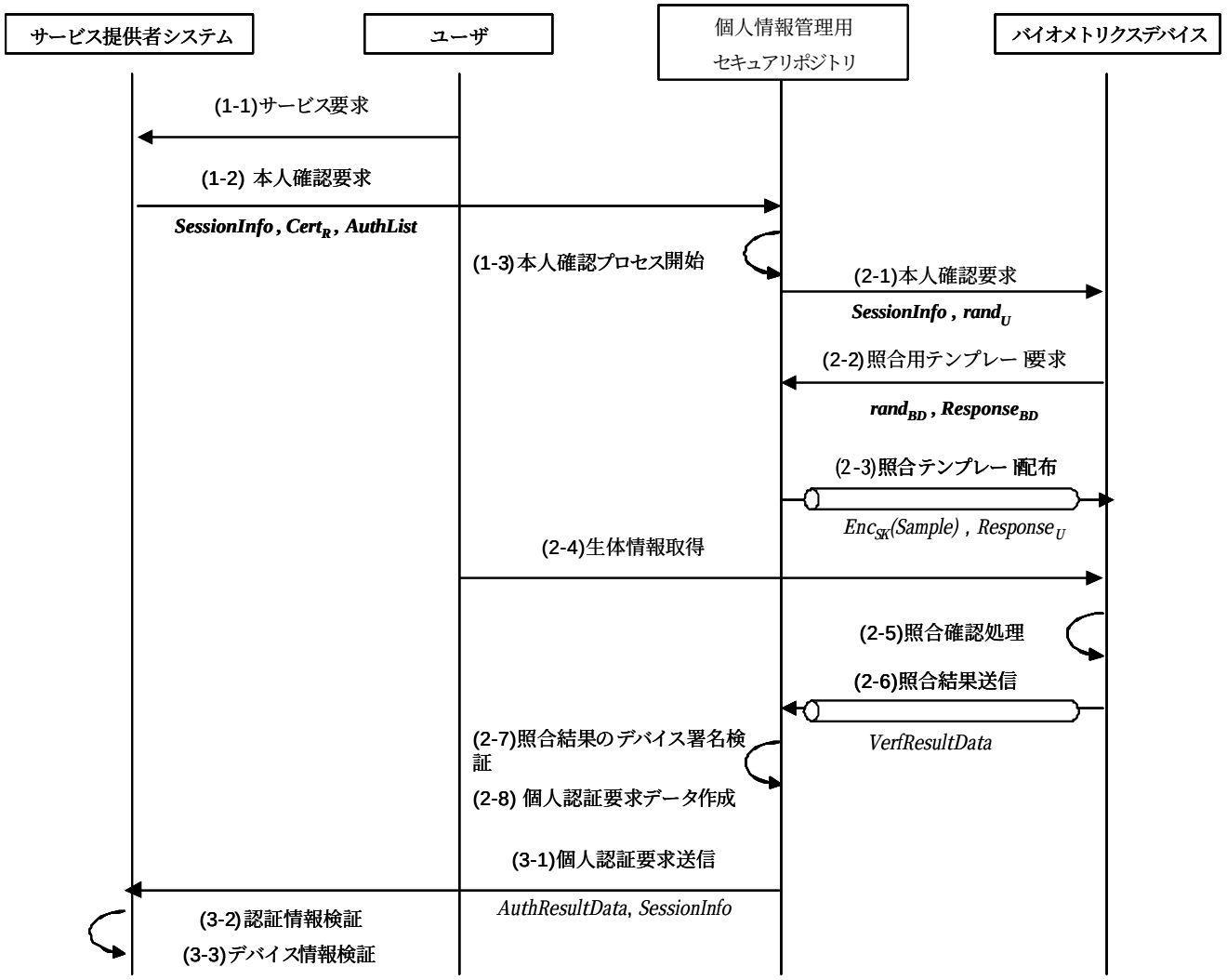


図 2 - 9 個人認証シーケンス

表 2 - 6 エンティティ一覧 :個人認証シーケンス

エンティティ	機能、所持データなど
ユーザ	【機能】 ・サービス提供者に対して、サービス利用要求を行う。 ・個人情報管理用リポジトリの管理や、クライアント端末の管理を実施する。
	【所持データなど】 ・個人情報管理用セキュアリポジトリシステム ・PCなどのサービス利用時に使用するクライアント端末
サービス提供者	【機能】 ・ユーザの要求に応じて、サービスを提供する。
	【所持データなど】 ・サービス提供者公開鍵ペア ・サービス提供者公開鍵証明書 ・ユーザの公開鍵証明書を発行したCAの公開鍵証明書 ・ユーザが使用するデバイスの証明書を発行したCAの公開鍵証明書
個人情報管理用セキュアリポジトリシステム	【機能】 ・ユーザの個人情報、照合用テンプレートなどを安全に保持するためのシステム ・ユーザの公開鍵ペアの生成機能、セキュア通信機能などを持つ。
	【所持データなど】 ・ユーザ公開鍵ペア ・ユーザ公開鍵証明書（照合余蘊テンプレートとひも付けされている） ・ユーザの照合用テンプレート ・使用するデバイスの証明書を発行したCAの公開鍵証明書
バイオメトリクスデバイス	【機能】 ・ユーザのバイオメトリクス情報を取得する。 ・照合用テンプレートを作成する。 ・取得したバイオメトリクス情報と、照合用テンプレートとの照合を行う。
	【所持データなど】 ・デバイス公開鍵ペア ・デバイス公開鍵証明書 ・ユーザの公開鍵証明書

⑸ 関連する処理シーケンス例

以下では、このフレームワークを実装した場合の関連する代表的な処理シーケンスを記述している。このシーケンスは案の1つであり、このフレームワークを実現するためにこれ以外の可能な処理シーケンス、インタフェース、プロトコルを含めたステップ毎の詳細や、順番、セキュリティ整合性の検討などを十分に行った上で、最適な案を採用する必要がある。

1) デバイス情報の登録～デバイス証明書の発行

以下のシーケンスでは、デバイス毎に公開鍵ペアを生成し、デバイスの情報を証明するものとして、その公開鍵に対する公開鍵証明書を用いるものとしている。

1. デバイスメーカーは、デバイス認証基盤にデバイス公開鍵証明書の発行依頼を行う。
2. デバイス認証基盤は、公開鍵証明書を発行するデバイスの情報をメーカーに対し要求する。
3. メーカーはデバイス認証基盤にデバイスの情報を送信する。
4. デバイス認証基盤は、デバイスの情報に第三者評価機関の評価結果などを含む場合は、その第三者評価機関に評価結果の正当性を確認する。
5. 第三者評価機関からの回答を得る。
6. デバイス認証基盤は、デバイスに対してデバイス公開鍵証明書を発行する。
7. 正当性が確認できた情報については、これを登録する。
8. デバイスメーカーにデバイス公開鍵証明書を送信する。
9. デバイスメーカーは、発行された公開鍵証明書とペアになる秘密情報（例：デバイス用秘密鍵）を、安全に保護された状態でデバイスに格納する。

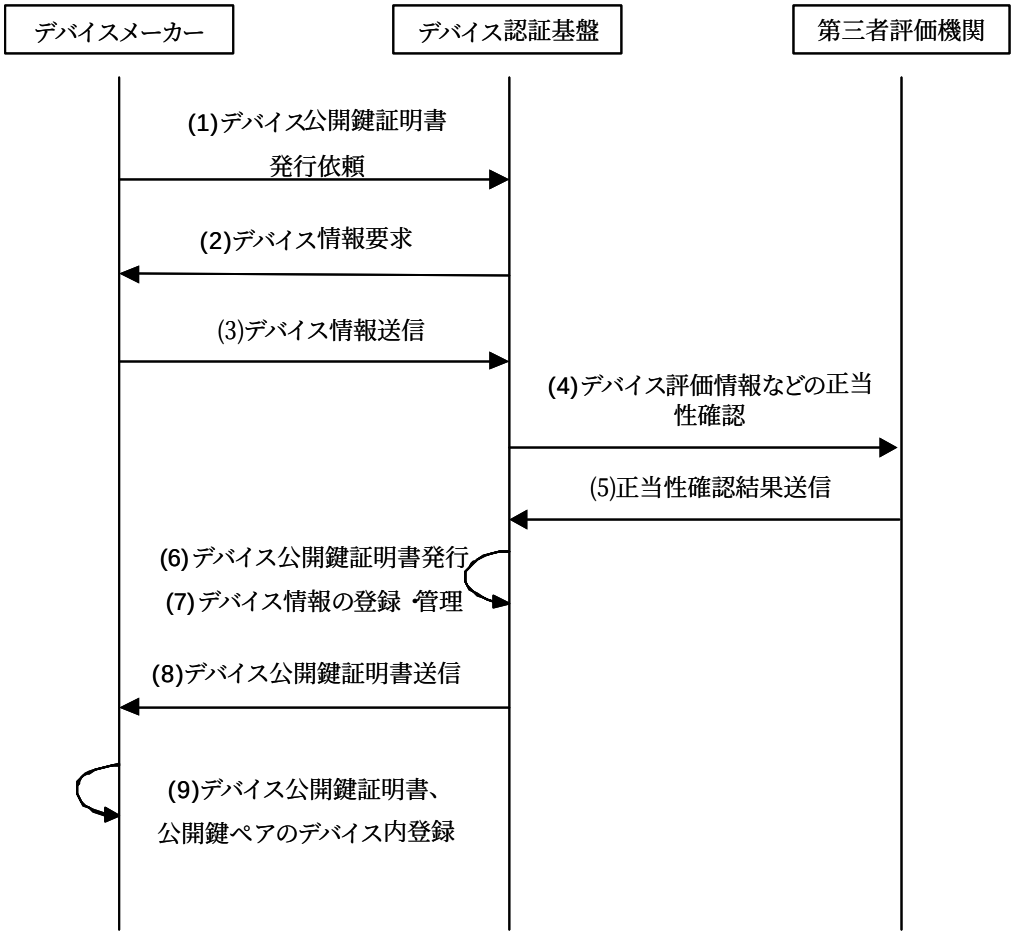


図 2 - 10 処理シーケンス例 :デバイス情報の登録～デバイス証明書の発行

表 2 - 7 エンティティ一覧 :デバイス情報の登録～デバイス証明書の発行シーケンス

エンティティ	機能、所持データなど
デバイスメーカー	【機能】 ・デバイスおよびそのデバイスを使用して行う処理用アプリケーションなどを製造する業者
	【所持データなど】 ・特になし
デバイス認証基盤	【機能】 ・デバイスに対して、公開鍵証明書を発行する
	【所持データなど】 ・デバイス認証基盤の公開鍵ペア ・デバイス認証基盤の公開鍵証明書
第三者評価機関	【機能】 ・固有の評価基準を持ち、それに従ってデバイスの評価を行う機関

2) バイオメトリクス照合用テンプレートの登録と管理

1. ユーザは、クライアントPC上で、デバイス証明書を持つバイオメトリクス照合用デバイスを用いる。まず、バイオメトリクス照合用テンプレート作成アプリケーションを起動する。
2. ユーザのバイオメトリクスデータがバイオメトリクスデバイスによって取得される。
3. バイオメトリクス照合用テンプレート作成アプリケーションによって、デバイス上で照合用テンプレートが作成される。
4. テンプレートデータ（のハッシュ値）に、デバイスによって署名が付加される。
5. デバイスからユーザに照合用テンプレートが出力され、そのデバイス署名ごと個人情報リポジトリに保存される。
6. ユーザは個人用公開鍵証明書の作成を開始する。
7. 個人情報リポジトリ内で、ユーザの公開鍵ペアが作成される。
8. 個人情報リポジトリから、個人用証明書発行 CA に対して、公開鍵データと照合用テンプレートのハッシュ値が送信される。
9. 個人用証明書発行CAは、受信した公開鍵と照合用テンプレートデータのハッシュ値に対してそれぞれ証明書を発行する。このとき最低どちらか1つの証明書には互いの証明書をひも付けするための情報を含む必要がある。それによって取得したテンプレートデータとユーザの秘密鍵とのひも付けが行われたことになる。
10. 発行された個人用公開鍵証明書とテンプレート証明書のペアが個人情報リポジトリに送信される。
11. 個人情報リポジトリ内に、受信した各証明書が保存される。

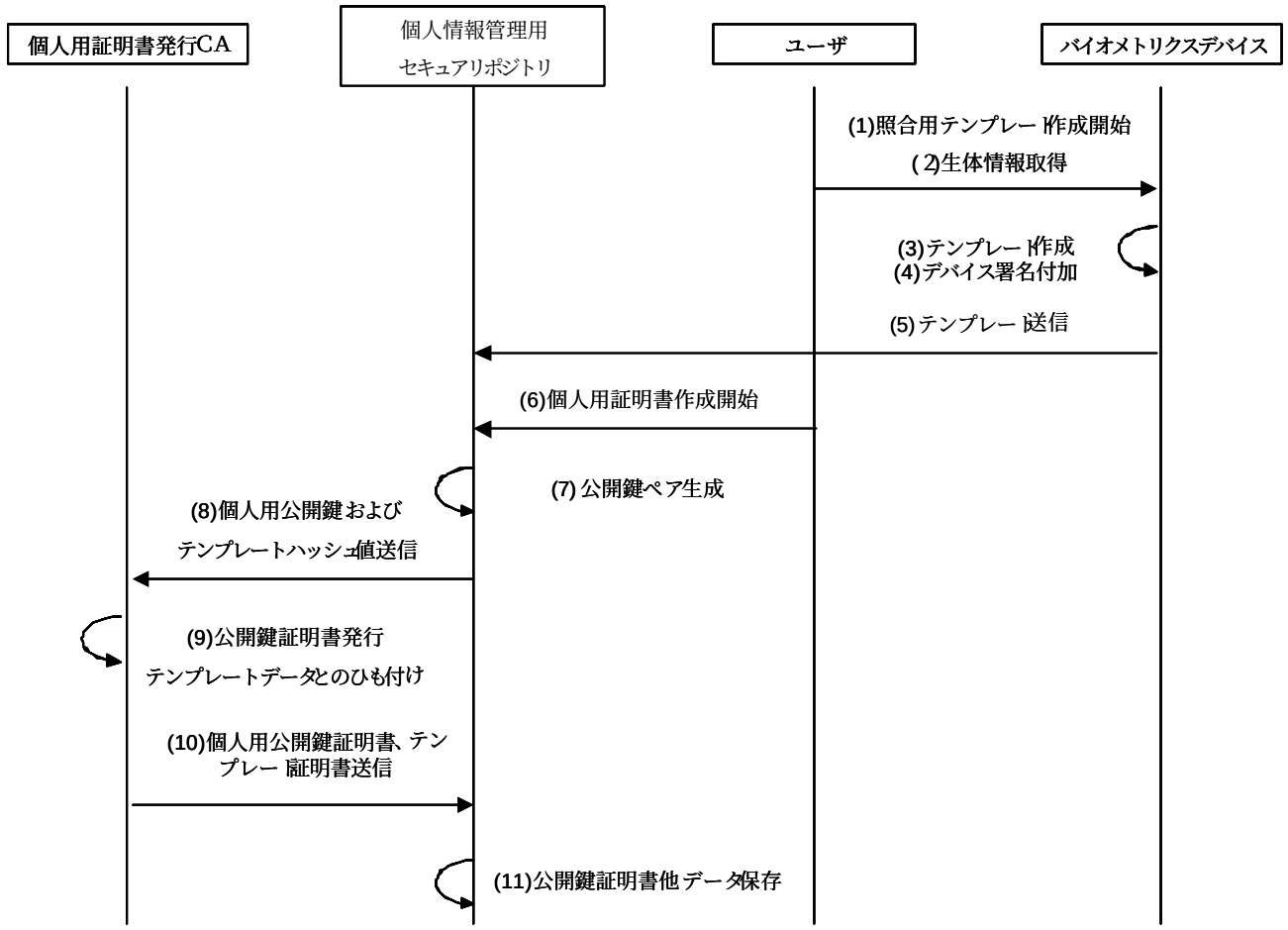


図 2 - 11 処理シーケンス例：バイオメトリクス照合用テンプレートの登録と管理

表 2 - 8 エンティティ一覧 :バイオメトリクス照合用テンプレートの登録と管理

構成要素	機能、所持データなど
ユーザ	【機能】 ・サービス提供者に対して、サービス利用要求を行う。 ・個人情報管理用リポジトリの管理や、クライアント端末の管理を実施する。
	【所持データなど】 ・個人情報管理用セキュアリポジトリシステム ・PCなどのサービス利用時に使用するクライアント端末
個人情報管理用セキュアリポジトリシステム	【機能】 ・ユーザの個人情報、照合用テンプレートなどを安全に保持するためのシステム ・ユーザの公開鍵ペアの生成機能、セキュア通信機能などを持つ。
	【所持データなど】 ・ユーザ公開鍵ペア ・ユーザ公開鍵証明書（照合余蘊テンプレートとひも付けされている） ・ユーザの照合用テンプレート ・使用するデバイスの証明書を発行したCAの公開鍵証明書
バイオメトリクスデバイス	【機能】 ・ユーザのバイオメトリクス情報を取得する。 ・照合用テンプレートを作成する。 ・取得したバイオメトリクス情報と、照合用テンプレートとの照合を行う。
	【所持データなど】 ・デバイス公開鍵ペア ・デバイス公開鍵証明書 ・ユーザの公開鍵証明書
個人用公開鍵証明書発行CA	【機能】 ・ユーザに対して、公開鍵証明書を発行する。
	【所持データなど】 ・CAの公開鍵ペア ・CAの公開鍵証明書

１．３．５ 検討課題

前章までにバイオメトリクスを利用した個人認証を行う際に、どのようなセキュリティ上の脅威が考えられるかを分析し、そしてその対策に必要だと考えられるセキュリティ機能やプロトコルを含むフレームワーク案、

バイオメトリクス認証結果保証基盤について検討した。しかしこの案の内容は荒削りであり、未検討の部分が多く、実現に向けて標準化案を策定する前に、検討すべき課題が多く残されている。本章ではその課題についてまとめている。

また、これらの課題には、フレームワークの詳細を検討する過程で仕様や対策を決定し解決すべきものと、このフレームワークを利用したシステムを構築する際に満たすべき要求項目との2種類が存在する。両者ともフレームワークの実現に密接に関連しているため、切り分けることが難しいが、来年度以降の調査研究では、本フレームワーク案に関係の深い課題の検討を重点的に実施する予定である。

⑴ デバイス認証基盤

- デバイス証明書の信頼性の確保

  デバイス証明書の信頼性、すなわち証明書発行機関の信頼性と権威をどう確保するかは、このフレームワークの実現において、もっとも重要な検討課題であると言える。

  デバイス証明書発行機能を持つデバイス認証基盤は、要求される性質上、公正中立な立場の機関であることが望ましいと考えられる。少なくとも政府機関によって設立され運営されることが望ましい。

- デバイス証明書の発行要求

  本フレームワークでは、デバイスメーカーはデバイス認証基盤に対して、デバイス証明書の発行要求を行う。デバイス認証基盤側ではこの発行依頼に対して、その正当性の確認をどのように行うか、何を以て発行依頼元が正しいメーカーであるとみなすか、などを判断する基準が必要である。

- デバイス証明書に含めるデバイス情報

  本フレームワークでは、デバイスメーカーはデバイス認証基盤に対して、デバイス証明書に含めたいデバイス情報を送信する。デバイス認証基盤側ではデバイス証明書の信頼性を損ねないためにも、受信したデバイス情報の正当性の確認を行う必要性がある。従って、フレームワーク実現のためにはこのようなメーカーの自己申告に依存する情報の正当性の確認手段や正当であると見なす条件、あるいは正当性を確認しなくてもよい条件などを明確にしたガイドラインが必要である。

- 第三者評価機関との連携、および、その評価結果データの取り扱い

  デバイスの属性情報の1つとして、既存の評価機関やテストセンターによるデバイスの評価データ、テストデータなどが考えられる。デバイス認証基盤が、発行するデバイス証明書にそれらのデータをデバイスの属性情報として含める場合、これらの第三者評価機関とどのように連携するのかを規定する必要がある。

  例えば、評価結果の正当性を確認する具体的な手段や情報の管理方法、どの評価機関のデータを保証対象として含めるのか、どの評価機関を信頼するのかというようなポリシーを持つのかなどが検討事項として考えられる。

- デバイス情報の登録・管理
  デバイス認証基盤では、その運用上、当然、どのデバイスに対して証明書を発行したかを管理する必要がある。それ以外の属性情報や評価情報などを含むすべてのデバイスに関する情報は、デバイス証明書の運用と連携して、登録や更新、削除などの処理方法を検討しなければならない。
  またデバイス証明書発行には必要だが一般には開示すべきではない情報を管理する可能性も考えられる。このような情報の管理については、十分なセキュリティの検討を行う必要がある。

- デバイス証明書とデバイス用秘密鍵の管理
  デバイス認証基盤が発行したデバイス証明書とペアになるデバイス用秘密鍵は、このフレームワークベースとした認証システム全体のセキュリティに大きく関わる重要な要素である。このデバイス秘密鍵データが不正アクセスによって漏洩したり、破壊された場合は、即、そのデバイスを使って行った個人認証の信頼性を失わせることにつながる。
  従って、このデータの管理は、個人用秘密鍵などの情報を管理するのと同様に、十分にセキュリティが守られた状態で行われる必要がある。また、デバイス認証基盤側でも、発行したデバイス証明書の信頼性喪失を避けるために、どのようにこの秘密情報が守られているのか、デバイス証明書の発行時までに、適当なガイドラインに従って監査する必要が考えられる。

- デバイス証明書の更新
  デバイス証明書、デバイス証明書発行機関の証明書など、これらの証明書の更新をどのように行うべきか。証明書の有効期限の設定を含めた議論が必要である。

- デバイス証明書の失効処理
  なんらかの問題によって有効期間中にデバイス証明書が失効した場合に、どこにどのように通知するのか、デバイス情報を管理しているデータベース更新を含め、適切な実施方法について検討する必要がある。

- デバイス証明書の無効化
  デバイス証明書の信頼性は、対になっているデバイス用秘密鍵のセキュリティ保持手段に依存しているため、場合によってはいったん発行したデバイス証明書を、デバイス認証基盤側から積極的に無効にしなければならない状況が考えられる。どのような場合に無効にするか、またその条件に抵触することをどのように監査するかなどのガイドラインが必要になる可能性が考えられる。

- 証明書の発行単位
  デバイス1台ごとに発行するか、デバイスメーカー単位で証明書を発行し、メーカー内ではその証明書をルートとして個々のデバイスに証明書を発行するか、それらを両立させるかなど、実運用を考慮した発行単位や証明書発行機関の権限の委譲条件などの策定が必要である。

- デバイス情報の問い合わせ

サービス提供者が受信した個人認証処理要求内のデバイス情報を確認するのに、何らかの問い合わせをデバイス認証基盤に対して行えるようにする必要がある。他にも開示する情報に制限を加える必要性や方法についても検討しなければならない。

⑵ プロトコル

- バイオメトリクスデバイスとアプリケーション間の通信インタフェース仕様
  現在、バイオメトリクスデバイスとアプリケーション間の通信インタフェース仕様としては、国際標準化が進められている BioAPI などが存在する。また現時点では、これらには本調査研究が対象としているようなデバイスの認証や鍵交換を組み込むような仕組みは考慮されていないと思われる。
  このフレームワークの仕様を策定する上で、これらの API はデバイスと個人情報管理システム・リポジトリ間のセキュリティ強化プロトコルにもっとも関係する。このプロトコルがこれらの API の拡張によって実現可能なものか、あるいは全く新しいインタフェースを実装することになるのか、国際標準化動向に留意しながらの十分な検討が必要である。

- デバイスと個人情報管理システム・リポジトリ間のセキュリティ強化プロトコル
  バイオメトリクスデバイスと、個人情報管理用セキュアリポジトリ間では相互認証および鍵交換を行ってセキュア通信を行うことを前提としているが、実際の運用を考えた場合にはあらかじめ検討すべき課題がいくつか存在する。
  例えば、両者間の通信セキュリティは使用する鍵生成アルゴリズムなどに依存しているが、どちらの実装している鍵アルゴリズムに問題が発見される危険性は常に存在している。このように鍵生成アルゴリズムのような基本的なセキュリティ技術の強度に問題が生じた場合、最初の相互認証の段階でこれらの弱いアルゴリズムを排除するような仕組みを持たせられるような プロトコルを、あらかじめ検討しておく必要性が考えられる。

- 本人確認処理結果保証プロトコル
  このプロトコルは、サービス提供者に対して、個人認証処理要求の中にクライアント端末で実施したバイオメトリクスによる本人確認結果を何らかの形で加えることで、サービス提供者側がデバイス情報の確認を含めた個人認証を実行可能にするのも目的の1つである。現在、一般に広く実装されているネットワーク経由での認証には SSL/TLS を利用したサーバ認証、あるいはクライアント認証があるが、本調査研究で提案しようとしている本人確認処理結果保証プロトコルを実装する上で、このプロトコルがこれらのセキュア通信標準化技術の単純な応用や仕様が持つ拡張性の利用だけで、これらの処理が実現可能なのか、他の既存セキュア通信標準化技術による実装の可能性を含め、十分に検討する必要がある。
  例えば、サービス提供者に対して、個人認証要求にバイオメトリクス照合結果を付加して送信する場合、SSL/TLS など既存の認証方法に適応させるためになんらかの対策・対応が必要ではないかと考えられる。

- 使用するバイオメトリクス技術の指定
  サービス提供者のシステム運用ポリシーでは、ユーザが本人確認に使用するバイオメトリクス技術の指定や制限が行われる可能性が高い。例えば、サービス提供者ごとに、指紋照合による本人確認のみを有効とするポリシーや、他の生体情報との組み合わせを指定するポリシーなど、異なるポリシーを持つことは十分予測可能である。このようなポリシーの元でのシステム運用形態に対応するためには、この本人確認手段の指定の実施タイミングやインタフェースなどのプロトコルを決定する必要がある。

⑶ デバイス証明書

- デバイス証明書のフォーマット
  本調査研究では、デバイス証明書には、デバイスメーカーから得られる情報と、第三者評価機関による評価結果など、最低二種類以上の異なる種類の情報が含まれることを想定している。これらの情報はその性質や重要性のレベル、利用形態が異なることが想像できる。従って情報の種類や信頼性レベルの違いを示すラベルのようなデータを実装することが考えられるが、その必要性を含めて検討しなければならない。

⑷ テンプレート証明書

- 照合用テンプレートデータと個人用公開鍵証明書の関連づけ
  本調査研究の対象モデルでは、バイオメトリクスによる本人照合結果によって個人用秘密鍵へのアクセスの可否を判断しているが、これを実現するためには、照合用テンプレートデータと個人用公開鍵証明書とのひもづけをセキュリティ的にも問題ない状態で行わなければならない。
  ここにはいくつかの課題が存在している。
  - 照合用テンプレート生成から公開鍵ペア作成、公開鍵と照合用テンプレートのひも付け、発行された証明書を安全に保存するまでの一連の処理を、途中にデータの再利用やなりすましなどの不正処理が割り込んでいないことを保証できるような手段で行う必要がある。
  - 2つ目の課題はこの2つの情報を関連づける方法である。案としては、
    - 公開鍵証明書を主とし、中に照合用テンプレートデータ(のハッシュ値など)を属性情報として追加することで、両者を関連づける方法
    - 照合用テンプレート証明書を主とし、中に公開鍵証明書のUIDなどの識別データを属性情報として追加することで、両者を関連づける方法

    などが考えられる。これらの証明書の運用や発行システム、利便性などを考慮して、実装案を検討する必要がある。
  - これらの証明書の発行を担うCAの条件や必要とされる機能、運用方法についての検討が必要である。

- テンプレート証明書のフォーマット
  テンプレート証明書は個人用公開鍵証明書との関連づけを行う必要があるため、それに合わせた

フォーマットを決定する必要がある。

- テンプレート証明書の有効期限
  テンプレート証明書は個人用公開鍵証明書との関連づけされるため、個人用公開鍵証明書の有効期限との兼ね合いを考慮してその期限を決定しなければならないことが考えられる。またテンプレートデータにはバイオメトリクスデバイスによる署名がつけれるため、さらに照合用テンプレートそのものを作成したデバイス証明書の有効期限も考慮に入れなければならない。

- テンプレート証明書の更新
  テンプレート証明書の更新は、証明書そのものの有効期限切れ以外に、関連づけされている個人用公開鍵証明書の失効、テンプレート証明書の発行機関や照合用テンプレートを作成したデバイスの証明書の失効など、他の証明書データの失効と密接な関係が存在している。これらの証明書の関係を考慮し、適切で素早い更新処理を策定する必要がある。

- テンプレート証明書の失効
  なんらかの問題によってテンプレート証明書が失効した場合に、その通知や更新をどこにどのように実施するのが適切か、他の証明書との関連性を考慮して、適切な処理や手段を検討する必要がある。

⑸ その他

- フレームワーク全体のセキュリティ評価
  この認証基盤フレームワークを全体として俯瞰したときに、セキュリティ上問題がないかどうかを、他システムとの連携や実運用を鑑みた上で検討し評価することが重要であると考えられる。また、問題があるとすれば、それを回避あるいは防御する手段を備えることが可能かどうかの検討が必要になる。

- 他処理シーケンス、インタフェース、プロトコル、機器類の検討
  本報告書では、検討対象を絞った上で、このフレームワークを適用した場合の処理シーケンス例を記述し、必要な機能や新規要求項目について検討している。が、現在一般に流通しているバイオメトリクスデバイスやその多様な機能、個人情報管理システムの実装方法等を考慮すると、この例だけでなく、他の場合についても十分な脅威分析や検討を行った上で標準化に最適な提案をまとめる必要がある。

- 様々な個人認証を利用したサービスモデルへの適用
  今回は一般的な代表例として、EC個人認証モデルをバイオメトリクス認証システムや他の認証手段のシステムに、このフレームワークを適用する場合、どのような仕様、プロトコルを決めるべきか。特に、システム全体のセキュリティ強度を低下させないに注意すべきであると考えられる。

- バイオメトリクスデバイス
  本書のフレームワークにおける構成要素の検討のため、実際に流通しているバイオメトリクスデバイスにどのような機能があり、どのようなシステムでの利用を目的としているなどかを机上で調査した。本書のフレームワークに適用させるために、これらのデバイスに対して機能追加や拡張が必要であることは当初より予想された結論である。しかし、実際にこうしたデバイスを使用し、運用しているシステムの構成や利用状況から得られるノウハウや利点、問題点を検討することは、このフレームワークの仕様の決定に有益であると考えられる。

1．4 関連する技術・標準化動向と検討課題

前章では、EC モデルへのバイオメトリクス技術の適用検討において、そのセキュリティ課題の解決案としてバイオメトリクス認証結果保証基盤を導入した。本章では、この基盤との関連が特に深いと考えられる技術について、以下の項目についてまとめた。

- 関連性
- 現状
- バイオメトリクス認証結果保証基盤の実現上での課題

1. 4. 1 BioAPI

【関連性】

BioAPI は、アプリケーションがバイオメトリクス装置にアクセスするための API である。バイオメトリクス認証結果保証基盤では、IC カードがバイオメトリクスデバイスにアクセスするためのインタフェースとして利用可能である。

【現状】

BioAPI は現在、ISO/IEC JTC1 の SC37 において、ISO/IEC 19784 として策定中である。

【課題】

BioAPI ではテンプレートの暗号化には対応しているが、データフォーマットに依存した暗号化となっており、柔軟な運用には対応することは難しい。さらに、バイオメトリクス認証結果保証基盤で利用する際には、バイオメトリクスデバイスが相互認証や暗号化通信を行なうので、PKI 操作に関する関数が必要となるが、そのための API が現状では提供されていない。様々な運用形態に対応したテンプレートの暗号化のための更なる議論が必要である。

1. 4. 2 データフォーマット（CBEFF、Biometric Data Interchange Format）

【関連性】

CBEFF とBiometric Data Interchange Format は、どちらも、バイオメトリクスデータを扱うための規格で

ある。

CBEFF は、バイオメトリクスデータを扱うためのフレームワークであり、バイオメトリクスに対する暗号化や署名、及び複数のバイオメトリクスデータを扱うためのフォーマットなどを規定している。基本的には、ヘッダブロック、バイオメトリクスデータブロック、署名ブロックから構成される。バイオメトリクスデータの暗号化にも対応している。

一方、Biometric Data Interchange Format は、バイオメトリクスデータを交換するためのフォーマットである。指紋や虹彩など、複数のフォーマットを規定している。CBEFF のバイオメトリクスデータブロックに、この Biometric Data Interchange Format 準拠のデータが格納される。この関係を下図に示す。

図 2 - 12 CBEFF とBiometric Data Interchange Format の関係図

バイオメトリクス認証結果保証基盤では様々なバイオメトリクスデータ（例：指紋、虹彩など）を扱うことを想定しているため、テンプレートのフォーマットや、IC カードとデバイス間の通信に利用することが可能であると考えられる。

【現状】

- CBEFF
  現在、ISO/IEC JTC1 の SC37 において、ISO/IEC 19785 として策定中である。
- Biometric Data Interchange Format
  現在、ISO/IEC JTC1 の SC37 において、ISO/IEC 19794 のマルチパートからなる規格として策定中である。

【課題】

今後、ネットワークを介した認証では、バイオメトリクス技術とPKI 技術を組み合わせる上で、テンプレートとクオリファイド証明書などのユーザに関する証明書を関連付けることが非常に重要になる。証明書に関連付けるテンプレートを、CBEFF に準拠したデータにするのか、或いは Biometric Data Interchange Format に準拠したデータにするのかなどについて、運用形態やセキュリティを考慮して議論する必要がある。

1. 4. 3 テンプレートプロテクション

【関連性】

現在、バイオメトリクステンプレートの保護についての議論もなされている。主な議題としては、既存のバ

イオメトリクス関連の標準（X9.84、BioAPI、CBEFF など）では考慮されていないテンプレートの利用方法などが挙げられる。バイオメトリクス認証結果保証基盤においてもテンプレートの保護は重要な課題の一つである。

【現状】

2002 年 11 月に米国からISO/IEC JTC1 SC37 に提案されたが、テンプレートデータのデジタル署名に関しSC 27 のスコープ範囲と認識された。

【課題】

テンプレートの暗号化は、運用形態によってはバイオメトリクスデータの相互運用性に大きく影響を及ぼす可能性があるので、今後の展開に注目する必要がある。

１．４．４ PKI 技術関連

【関連性】

バイオメトリクス認証結果保証基盤ではテンプレートとPKI ユーザ証明書が同一のユーザを示している必要がある。そのための仕組みとしては、クオリファイド証明書並びに(株)日立製作所(以下、日立)が提案するテンプレート証明書がある。

クオリファイド証明書では、公開鍵証明書を主として中に照合用のテンプレートデータ（のハッシュ値など）を属性情報として追加することにより、ユーザの証明書とテンプレートを関連づける。一方、日立のテンプレート証明書では、照合用テンプレート証明書を主として中に公開鍵証明書の UID などの識別データを属性情報として追加することで両者を関連付ける。

前章までに述べたように、バイオメトリクス認証結果保証基盤は、テンプレートと PKI ユーザ証明書の関連がとれていればよいので、どちらの方法でも問題はない。

ところで、テンプレート参照情報）自体をITU-T 及び ISO/IEC や IETF が公開している公開鍵証明書に格納するという方法もバイオメトリクス認証結果保証基盤のしくみとしては可能ではある。しかし、第三者に配布するための公開鍵証明書にテンプレートを格納するのは、個人の生体情報を保護する上では問題があると考えられるので、本報告書では議論しないものとする。

【現状】

1） クオリファイド証明書

まず、欧州電気通信標準化協会（ETSI：European Telecommunications Standards Institute）により標準化検討がなされ、IETF により2001年 1月に RFC3039（Internet X.509 Public Key Infrastructure Qualified Certificates Profile）が定められた。さらに、2004 年 3 月に RFC3739（Internet X.509 Public Key Infrastructure Qualified Certificates Profile）が公開された。

RFC3 739 クオリファイド証明書は物理的な自然人を特定できるな証明書である。そのために X.509 の公開鍵証明書拡張領域にで、対象者の属性と共に生体情報に関する項目を定義している。

証明書の内容としては、X.509 の基本情報に加えて、以下の拡張領域が設定されている。

- 対象者の属性情報
- この証明書の手続き及び運用ポリシー
- 公開鍵証明書の使用目的(Key Usage)
- バイオメトリクス情報
- クオリファイド証明書（QC）の独自宣言（QC に関する法的な説明文書）

RFC3039 から RFC3739 への相違点としては、以下の通りである。

- RFC3739 において RFC3280（公開鍵証明書）と連携するために、対象者フィールド(subject field)に domainComponent と title を追加して、postalAddress を削除した。
- RFC3039 では公開鍵証明書の使用目的が否認防止用途のためにその他の用途と組み合わせて使用できないような設定があったのに対して、RFC3739 では RFC3280 の使用目的設定に一致するものになった。
- 対象者の属性情報にある title 項目が非サポートになった。
- 生体情報を格納する場所である biometoricInfo EXTENSHION には変更はない。
- クオリファイド証明に関する法的な説明である qc-Statement の改変があった。

2) 日立製作所のテンプレート証明書フォーマット

日立が提案しているもので、最近では2004年 1 月の SCIS2004（The 2004 Symposium on Cryptography and information Security Sendai,Jan.27-30,2004 The Institute of Electronics,Information and Communication Engineers）等で発表されている。

このテンプレート証明書は PKI の X.509 公開鍵証明書と分離した書式になっており、テンプレートの証明書にユーザの識別情報を持つことにより PKI 証明書との関連付けを保持している。ユーザ識別情報には PKI の公開鍵証明書を一意に識別する識別情報のフィールドを用いる。テンプレートの発行者は、PKI の公開鍵証明書とは独立にテンプレート証明書に署名を添付することにより、テンプレート証明書の完全性を保持している。

テンプレートの発行者が独立に署名することで、PKI の公開鍵証明書とは独立にテンプレートを運用することが可能になっている。また、テンプレートの寿命が異なる問題に対しても、それぞれのバイオメトリクス技術ごとに個別に運用することができる。さらに必要な生体認証技術のテンプレートを後から、追加したり、複数所持したりすることが可能になっている。

日立製作所のテンプレート証明書のフォーマットは以下のようになっている。

1. テンプレートフォーマットを識別する情報
2. PKI の証明書を一意に指定する情報。例えば、発行者とそのシリアル番号
3. このテンプレートを発行した発行者の名前及び識別情報
4. テンプレート情報
5. このテンプレートの発行者によるデジタル署名

【課題】

バイオメトリクス認証結果保証基盤にクオリファイド証明書を適応する場合においては、以下のような課

題がある。

・テンプレートが変更・廃棄された場合のクオリファイド証明書の失効及び発行作業の簡素化

テンプレートの情報の更新がある度にクオリフィド証明書を再発行する必要があるわけであるが、その更新が頻繁にある場合の失効、発行処理のコスト増大の問題がある。

対応）失効に関しては OCSP への対応も必要に応じて考慮する必要がある。

日立のテンプレート証明書を適応させる場合においては、「1. 3. 5検討課題」で述べたように、以下のような課題がある。

・テンプレート証明書の更新

テンプレート証明書の更新は、証明書そのものの有効期限切れ以外に、関連づけされている個人用公開鍵証明書の失効、テンプレート証明書の発行機関や照合用テンプレートを作成したデバイスの証明書の失効など、他の証明書データの失効と密接な関係が存在している。これらの証明書の関係を考慮し、適切で素早い更新処理を策定する必要がある。

対応）公開鍵証明書及びテンプレート証明書の両者を扱う OCSP 的な枠組を検討する必要等がある。

・テンプレート証明書の失効

なんらかの問題によってテンプレート証明書が失効した場合に、その通知や更新をどこにどのように実施するのが適切か、他の証明書との関連性を考慮して、適切な処理や手段を検討する必要がある。

対応）公開鍵証明書及びテンプレート証明書の両者を扱う OCSP 的な枠組を検討する必要等がある。

１．４．５ カード内照合（MOC:Match on Card / On-Card Matching）に関連する標準・技術

【関連性】

生体情報を格納するセキュアデバイスの候補として IC カードが挙げられる。IC カードはテンプレートを格納するだけではなく、カードの内部でテンプレートの照合を行うことも考えられる。バイオメトリクス認証結果保証基盤においてもカード内で照合を行うことも想定される。

【現状】

現在、SC17 をはじめとするIC カード関連の標準・技術について議論している団体において、カード内照合が注目されている。これは、テンプレートをカードの外部に出すことなく認証を行うことができ、テンプレートの情報が外部に漏れる危険性が低いということが理由に挙げられる。ここでは MOC(Match on Card / On-Card Matching)に関連した主な技術・標準は団体を挙げ、それぞれの概要を示す。

- ISO/IEC 7816 -11
  - IC カードを利用したバイオメトリクス認証を行うために必要なセキュリティ関連コマンド、およびデータフォーマットを規定している。

- カード内照合、カード外照合の両方を想定して作成されている。
- 2004 年 3月 17 日に策定された。

- Java Card Biometric API
  - Java Card 内で照合を行うために必要な API を提供している。この API を利用することにより、カード外にテンプレートを出すことなく照合することが可能になる。
  - カードベンダ、バイオメトリクス技術に依存することなく、Java Card 上でバイオメトリクス照合を扱うことができるようにすることを目的としている。
- Government Smart Card Interoperability Specification (GSC-IS)
  - IC カードと IC カードを利用したアプリケーションの相互運用性を確保することを目的として策定された仕様。
  - GSC-IS はバイオメトリクスを意識した仕様になってはいないが、バイオメトリクスに連携することは可能である。AHGBISGF というアドホックグループにおいて BioAPI とGSC-IS とを連携させることでバイオメトリクスを用いた認証に GSC-IS を利用する際の考察が行われ、報告書が公開されている。報告書ではカード内で照合を行わない場合は GSC-IS に対して修正することなく利用できるが、MOC(Match on Card / On-Card Matching)の場合は GSC-IS に修正が必要であるという結論になっている。
- Smart Card Alliance
  - 「Smart Cards and Biometrics in Privacy-Sensitive Secure Personal ID Systems White Paper」にて IC カードとバイオメトリクスを利用したセキュリティシステムについて報告しており、MOC(Match on Card / On-Card Matching)に関する記述がなされている。

【課題】

バイオメトリクス認証結果保証基盤において MOC(Match on Card / On-Card Matching)を採用した場合、IC カードとデバイス間のプロトコルに関して影響を与える。バイオメトリクス認証結果保証基盤では IC カードからデバイスに対してテンプレートを配布しているが、MOC(Match on Card / On-Card Matching)を採用した場合は照合を行うための生体情報をデバイスから IC カードに対して配布しなくてはいけない。そうした場合に情報の送信元であるデバイスが送信先の IC カードを認証する必要があるかどうか検討する必要がある。そして、本報告書における個人認証シーケンス案ではデバイスの検証はサービス提供者システムで行っているが、MOC(Match on Card / On-Card Matching)を利用した場合ではデバイス情報の検証をサービス提供者システムで行うのか IC カードで行うのか再検討する必要があると考えられる。

また、デバイス内で照合を行わないために、デバイス証明書では照合結果について必ずしも保証できるわけではない。デバイスに格納されたデバイス証明書ではデバイス外の処理について保証ができるとは限らない。MOC(Match on Card / On-Card Matching)の照合結果について保証する方式として IC カード内に照合結果を証明するための証明書を付加することも考えられる。しかし、現在の MOC(Match on Card / On-Card Matching)の仕様では、カード内で照合を行うために必要なコマンド・データフォーマット・API を規定しており IC カード内の照合精度を保障することに関しては検討されていない。今後は、MOC(Match on Card / On-Card Matching)の照合結果を保証する方式について検討する必要もあると考えられる。

１．５ 国際標準化活動

１．５．１ ISO/IEC JTC 1/SC 37 WG4 Meeting 発表報告

⑴ 発表スケジュール

場所：オーストラリア シドニー（Australian Technology Park：http://www.atp.com.au/）
日時：2004年 2月 13日　9：30～
参加者：日本からの参加者を含め、約 25名。

⑵ 発表概要

タイトル：Development of Biometric Authentication via Open Networks - Device Identification Infrastructure –
内容の詳細は付録の発表資料を参照のこと。

まず、この発表が日本の国家プロジェクトのアクティビティの一つであるという背景を説明を行った。次に、オープンネットワーク経由での個人認証システムにおけるセキュリティ上の問題点を提示し、解決するために必要な機能を説明した。最後に、今回発表するデバイス認証基盤（Device Identification Infrastructure）によって、これらの問題点がどのように解決できるかを紹介し、さらにこの基盤が、バイオメトリクスを使った個人認証システムを実装する際にも重要であることを示して終了した。

⑶ 発表に対する反応

発表内容への関心を強く持ってもらえたらしく、後で、発表原稿のデータコピーを多数から求められた。また質問は予想以上に多かった。技術的な内容に関する質問よりも、ISO という団体らしく、標準化や今後のプロジェクトの進め方に対する質問がほとんどだった。

受けた質問には

- Q：このデバイス認証基盤の研究開発の主体は、どこにあるのか？国なのか、大学などの研究機関なのか？、
  A：日本のプロジェクトのひとつである
- Q：スケジュールはどうなっているのか？
  A：3年計画で、始まったのは去年の 12月ごろから
- Q：標準化の進め方の予定は？
  A：未定
- Q：政府と企業間のネットワークへの適用は考えているのか？
  A：未定、特に今の段階では限定していない
- Q：デバイス証明書のフォーマットはどのように考えているのか？
  A：現段階では、証明書の拡張領域にデータを乗せることを考慮している。（実際には未確定）

などがある。

⑷ 今後の課題

今回、発表したデバイス認証基盤は、バイオメトリクスを使った個人認証システム以外にも有効性があると思われるため、SC37 以外の委員会、SC27 などでも標準化活動を行うことが重要であると考えられる。

１．６ あとがき

本調査研究では、PKI+バイオメトリクス技術のオープンなネットワーク環境での利用モデルとしてもっとも将来性の高い EC 個人認証モデルを調査研究対象モデルとし、バイオメトリクス技術の応用について調査、検討を行い、セキュリティ課題と必要なセキュリティ要件を考察した。さらに解決案としてバイオメトリクス認証結果保証基盤を導入し、本人確認環境を確認する方式を提案した。これらの今年度の成果を目標として掲げた3つの項目についてのまとめは、「1. 2. 3活動項目ごとの検討結果(要約)」に記述しているので、ここでは割愛する。

今年度の活動を通じて、「1. 3. 5検討課題」で述べたような調査研究対象モデルやバイオメトリクス認証結果保証基盤に関係する技術的な課題を踏まえた上で、今後の活動の方針を以下に示す。

- 提案課題・モデルの詳細技術仕様の策定
  今年度の調査活動により、提案課題・モデルが国際的にもユニークであることがわかった。また、調査活動、モデル検討活動を通じ、次年度以降の検討課題、検討の視点を抽出できた。今後、本課題・モデルの更なる検討を行い、国際標準の可能性についての検討を進めていく。
- 提案課題・モデルの拡大の検討
  今年度の調査は、調査研究対象モデルに条件を課して実施したが、バイオメトリクス認証結果保証基盤の適用性について検討し、さらなる課題を抽出するために、特に次の二つの項目について、今後の調査研究対象範囲へ含めるかどうか、次年度以降検討する必要があると考えられる。
  - 個人情報格納デバイス内でバイオメトリクス照合を行うモデル
    現在は、バイオメトリクス照合はバイオメトリクスデバイスで行うモデルに限定
  - サーバ側等で照合するモデル
    現在は、照合はクライアント側で行うモデルに限定
- 国際的な関連活動との連携の検討
  欧州の第5期研究開発プログラム(FP5)における BANCA、BEE では、EC におけるバイオメトリクス技術の適用を検討中(詳細は不明)。今後詳細調査を進めると共に、可能であれば、これら関連団体との連携を検討していく。
- 国際標準への提案活動の場の再検討
  本活動の主成果は、セキュアな通信プロトコルとなることが、今年度の活動で明確になった。従って、今後、本調査研究における提案活動は、バイオメトリクスに関する標準化の場であるSC37よりも、情報セキュリティの標準化の場であるSC27を主な活動フィールドとする見込みが大きく、SC27での活動方針や関連コミュニティとの連携の検討が必要である。

今後はこれらの項目検討も含めた上で、個人情報の保護に配慮した、より厳密な個人認証技術・システムの可能性を追求したい。

１．７ 付録

１．７．１ バイオメトリクス国際標準化動向

⑴ 全体図

図 2 - 13 SC 37 を中心としたバイオメトリクス技術の関連」に、本章で説明するバイオメトリクス関連の標準同士の関係を示す。

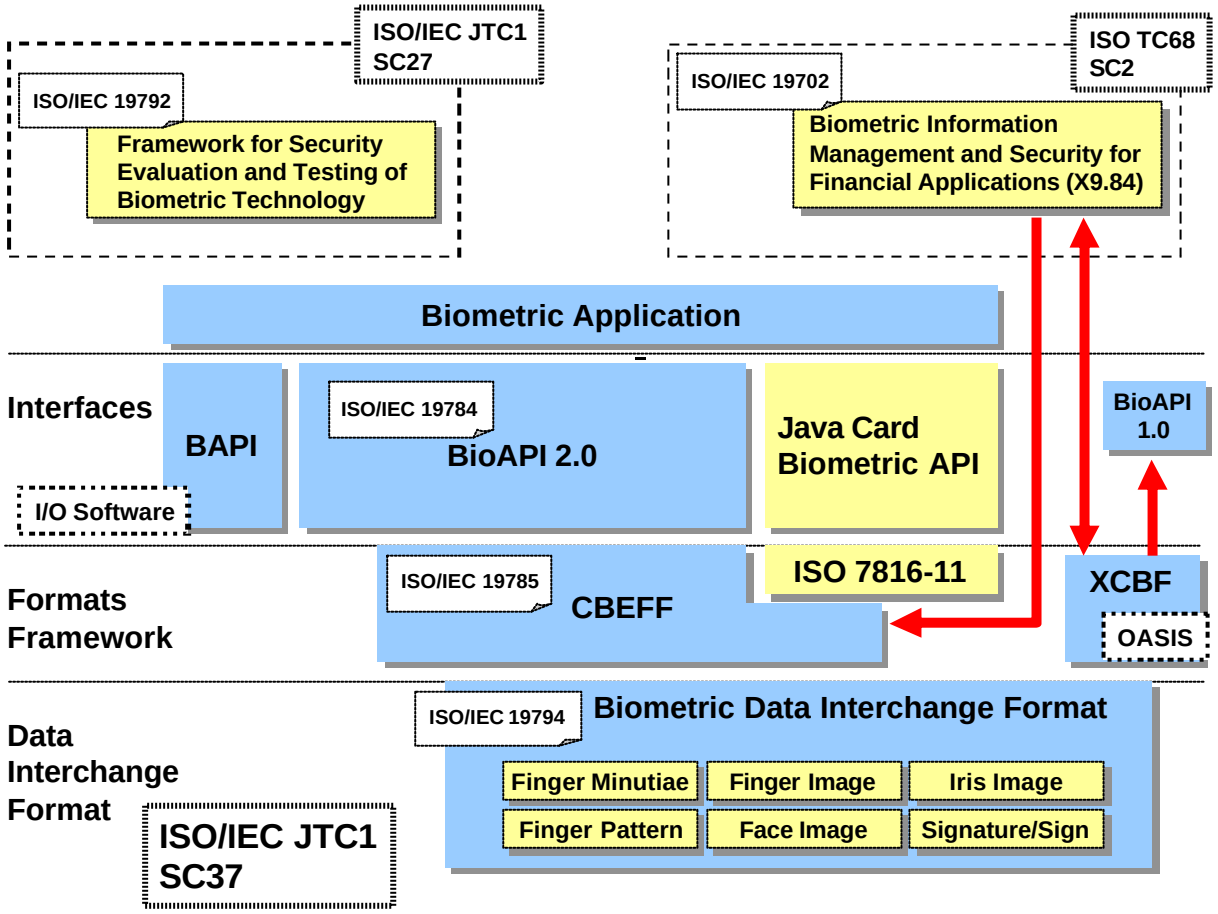


図 2 - 13 SC 37 を中心としたバイオメトリクス技術の関連

ISO/IEC 19794 では、バイオメトリクスデータを交換するためのフォーマットを規定している。ここでは、バイオメトリクスデータを運用するためのフレームワークや、指紋特徴点、指紋イメージ、虹彩イメージなど、複数のバイオメトリクスデータに関する標準化を行っている。

ISO/IEC 19785 では、バイオメトリクスデータを扱うためのフレームワークを規定している。この標準では、バイオメトリクスに対する暗号化や署名、及び複数のバイオメトリクスデータを扱うための、フォーマットなどを規定している。バイオメトリクスデータには、ISO/IEC 19794 の仕様に基づいたデータを扱うことができる。IC カードに格納するためのバイオメトリクスデータの仕様を規定している ISO/IEC 7816-11 では、CBEFF の仕様に準拠したフォーマットについても定義している。ISO/IEC 19784 や、ISO 19092 において CBEFF

に準拠したフォーマットを扱うことも可能である。OASIS によって策定された XCBF は、CBEFF (NISTIR 6529) に準拠したパトロンフォーマットに対して、セキュアな XML エンコーディングの共通セットを定義する。

アプリケーションに対する API には、BioAPI、BAPI、Java Card Biometric API 等がある。BioAPI は、バイオメトリクスアプリケーションのための API であり、ISO/IEC で標準化が進められている。BioAPI で使用するデータは、CBEFF に準拠したものである。また、I/O Software 社により開発されている BAPI もまたバイオメトリクスアプリケーション のための API を提供している。Java Card Biometric API は、Java カードに特化した API である。Java Card Biometric API で使用するバイオメトリクスデータは、ISO/IEC 7816-11 に準拠したものを用いる。また、Java Card Biometric API では、BioAPI の利用方法についても言及している。

その他、バイオメトリクス技術に関するセキュリティ評価及び試験の規定を目的とした ISO/IEC 19792 が策定中のほか、金融サービスのためのバイオメトリクス情報の管理及びセキュリティを規定した X9.84 は、ISO/IEC 19702 として策定中である。X9.84 で使用するバイオメトリクスデータは CBEFF に準拠しており、BioAPI 1.0 で扱われているバイオメトリクスデータとの互換性についても述べている。また、XML による符号化についても述べている。

本節では、バイオメトリクス技術に関する標準化を目的としている ISO/IEC JTC1 SC37 を中心に、現在のバイオメトリクス関連技術の国際標準化動向の説明を行う。 (2) では、ISO/IEC JTC1 SC37 の活動内容について述べる。また、 (4) では、バイオメトリクスのインタフェースに関する技術について述べ、 (5) では、バイオメトリクスのデータフォーマットに関する技術について述べる。 (6) では、バイオメトリクス技術の適用形態について述べる。

(2) ISO/IEC JTC 1 SC 37 (Biometric Technology)

【概要】

SC 37 は、アプリケーション及びシステム間における、相互運用性とデータ交換をサポートするための、一般的なバイオメトリクス技術の標準化を目的としている。以下の 6 つの WG (Working Group) により構成される。

WG 1 ：Harmonized Biometric Vocabulary
WG 2 ：Biometric Technical Interfaces
WG 3 ：Biometric Data Interchange Formats
WG 4 ：Biometric Functional Architecture and Related Profiles
WG 5 ：Biometric Testing and Reporting
WG 6 ：Cross-Jurisdictional and Societal Aspect

【動向】

2002 年 6 月に、ISO (International Organization for Standardization) と、IEC (International Electrotechnical Commission) の Joint Committee である JTC1 によって設立。

【詳細】

それぞれの WG について説明する。

- WG 1 (Harmonized Biometric Vocabulary)

WG 1 は、バイオメトリクス技術用語を標準化するグループである。他の ISO 標準に使用されている用語との調和を図ってバイオメトリクス技術用語の標準化を行うことを目的としている。

- WG 2 (Biometric Technical Interfaces)
  WG 2 は、バイオメトリクスの共通インタフェース仕様を策定するグループである。米国から提案された BioAPI（Biometrics Application Programming Interface）および CBEFF（Common Biometric Exchange File Format）が議論の中心となっている。尚、現在 BioAPI は ISO/IEC 19784 として、また CBEFF は ISO/IEC 19785 として策定中である。
- WG 3 (Biometric Data Interchange Formats)
  WG 3は、各技術間において共通に利用可能なバイオメトリクスデータの交換形式の標準化を行うことを目的としている。現在、このバイオメトリクスデータの交換形式を ISO/IEC 19794 として策定中である。
- WG 4 (Biometric Functional Architecture and Related Profiles)
  WG 4 は、バイオメトリクスの機能的なアーキテクチャ及び、バイオメトリクス関連標準を接続するプロファイルを開発することを目的としている。現在は、2 つのパートから成る「Biometric Profile - Interoperability and Data Interchange」が ISO/IEC 24713 として策定中であり、その 2 つ目のパートの WD が「Biometrics-Based Verification and Identification of Employees」というタイトルで発表された。
- WG 5 (Biometric Testing and Reporting)
  WG 5 は、認証に関連するバイオメトリクス技術、システム、コンポーネントの範囲における試験及び報告手法を作成することを目的としている。
- WG 6 (Cross-Jurisdictional and Societal Aspect)
  WG 6 は、アクセスのしやすさ、健康と安全、相互裁判権及び社会的事象と個人の情報に関連する社会的考慮の必要性と認識を尊重したバイオメトリクス技術の設計と実装を目的としている。

⑶ リエゾン関係

「図 2 - 14　SC 37 の主なリエゾン関係」に、SC 37 の主要なリエゾン関係を示す。

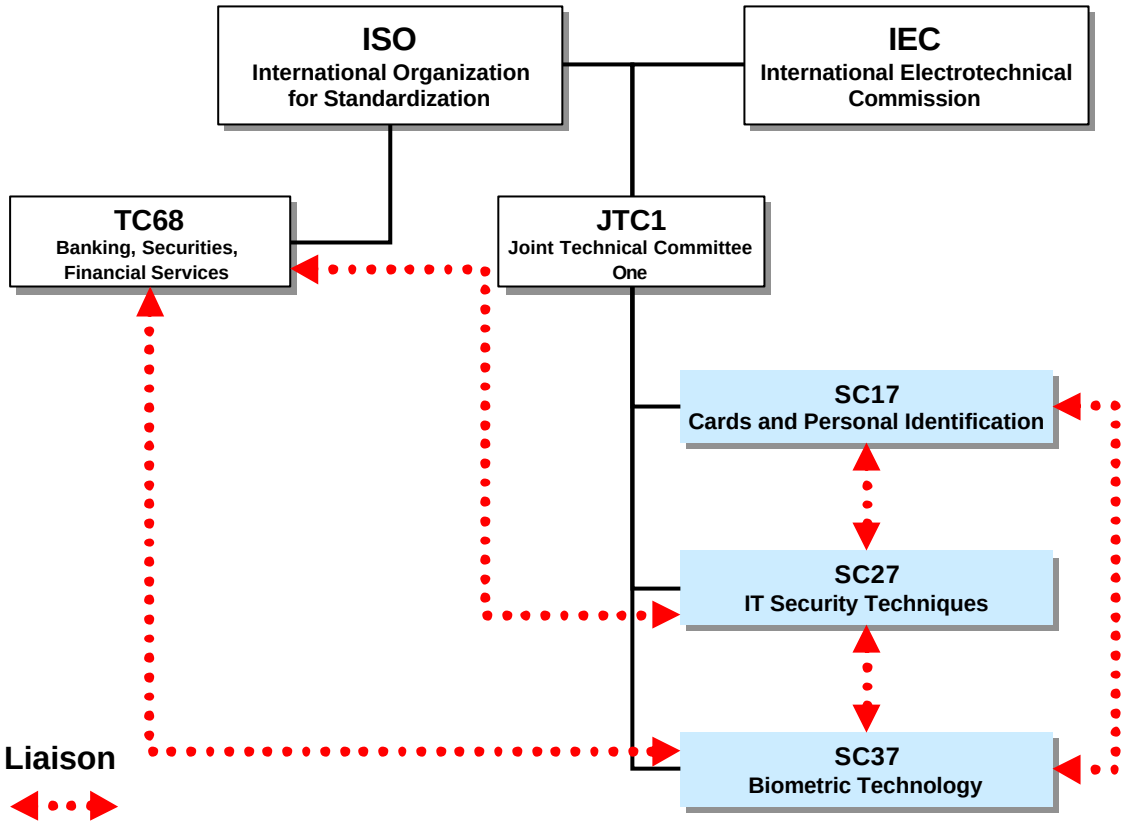


図 2 - 14 SC 37 の主なリエゾン関係

以下にそれぞれの委員会について紹介する。

1) ISO/IEC JTC1 SC17 (Cards and Personal Identification)

同じJTC1 のサブコミッティーである SC17 は、カード及び個人識別に関する技術の標準化を行っている。ここでは現在、カード内でバイオメトリクス認証を行うために必要なデータ要素などの規格を、ISO/IEC 7816-11 として標準化を行っている。

2) ISO/IEC JTC1 SC27 (IT Security Techniques)

SC 27 は、セキュリティ技術に関する技術の標準化を行っている。バイオメトリクス技術に関しては、プロトコルやアルゴリズムのセキュリティ評価試験のための枠組みを SC 27 で標準化する。SC 27 では現在、バイオメトリクスアルゴリズム、コンポーネント、システム、そしてバイオメトリック技術に関連する要素のセキュリティ評価及び試験のためのフレームワークを ISO/IEC 19792 として策定中である。

3) ISO TC68 (Financial Services)

ISO TC 68 は、銀行及び金融サービス業務に関する技術の標準化を行っている。現在、TC 68 において策定中の ISO/IEC 19702 は、金融サービスのためのバイオメトリクス情報の管理及びセキュリティを規定した X9.84 を基本として構成されている。

(4) API 関連技術

現在、バイオメトリクスの API の国際標準として BioAPI の標準化が、ISO において進められている。BioAPI は、BioAPI コンソーシアムにより標準化が進められてきた。BioAPI コンソーシアムは、1998 年 4 月、ベンダが独自に策定していた API の仕様を統一化することを目的として、Compaq Computer 社、IBM 社、Identicator Technology 社、Microsoft 社、Miros 社、Novell 社を主体として発足した。

当時、BioAPI 以外のバイオメトリクスの API として、米国防総省（DoD）の出資により開発された HA-API（Human Authentication API）、I/O Software 社が主体となり開発を進めていた BAPI（Biometric API）があった。

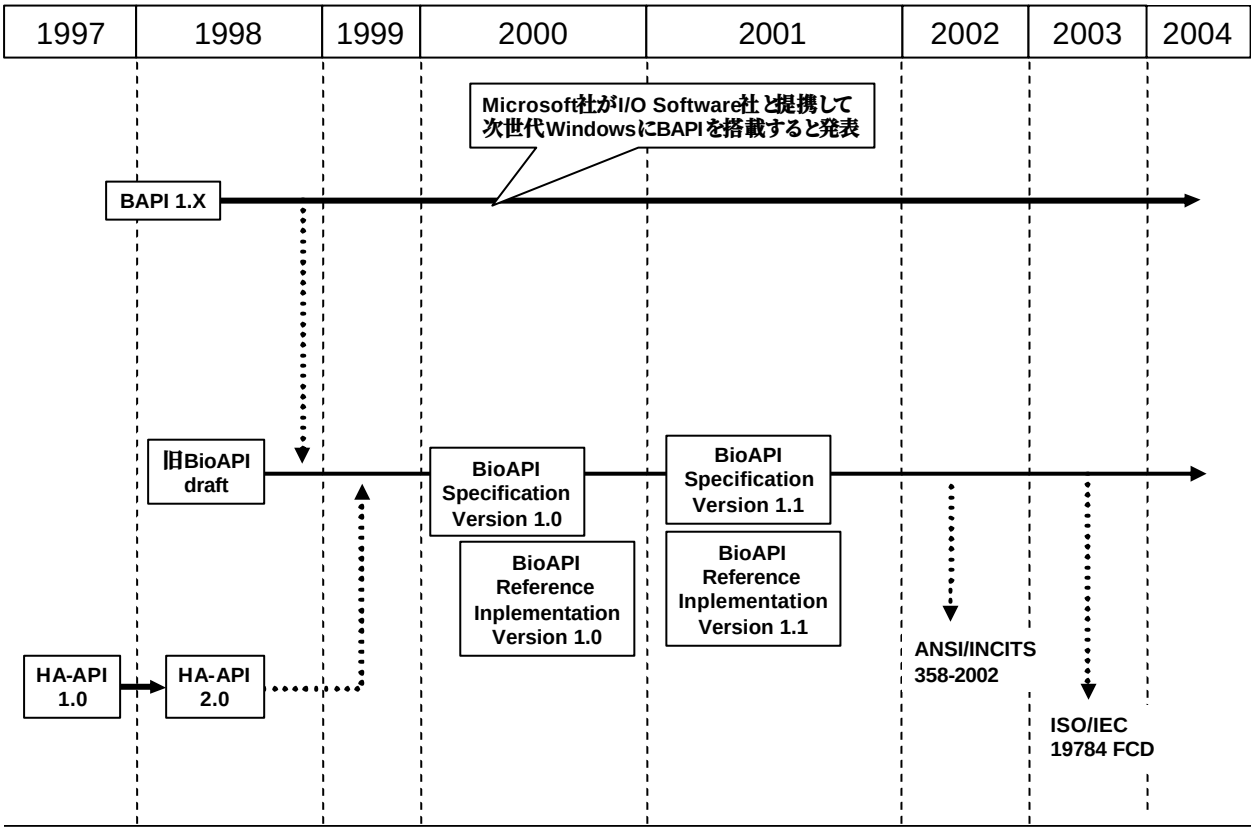


図 2 - 15 バイオメトリクス関連 API の動向

HA-API は、個人の認証や識別のためのバイオメトリクス技術を持つアプリケーションのインタフェースを定めたものである。米国防総省の出資によって National Registry 社が開発したものだが、バイオメトリクス技術の相互互換性を高めるため一般に公開された。1997 年 8 月 27 日に Rev. 1.0、1998 年 4 月 22 日に Rev. 2.0 が発表された。

BAPI は、アプリケーションとバイオメトリクスデバイスが通信する API を定義したものである。I/O Software

社が中心となって組織したワーキンググループにより提案された。

1998 年 12 月、BAPI の設立主体である I/O Software 社が BioAPI の推進主体の一員として加わることになり、その仕様は BioAPI に引き継がれる形で統合されることになった。1999 年 2 月には、NIST の仲立ちにより、BioAPI Consortium と、HA-API のワーキンググループとの間で仕様統一に向けた会合が持たれ、1999 年 3 月に両者の仕様を統合することが合意された。HA-API のその後の活動もまた BioAPI の策定に注がれることになった。

しかしながら、2000 年 5 月 2 日、当初の BioAPI コンソーシアムのメンバーであった Microsoft 社が、次世代 Windows には、BioAPI ではなく、I/O Software 社が開発を進めてきた BAPI（Biometric API）が搭載されると発表した[1]。その後は、Microsoft 社からの発表は無いが、I/O Software 社は BAPI の開発を進めており、BAPI の仕様に準拠した製品をリリースしている。

1) BioAPI (ISO/IEC FCD 19784)

【概要】

複数のベンダによるコンポーネントを使用することを目的とした高レベルなバイオメトリクス認証モデルにおける API (Application Programming Interface)と SPI (Service Provider Interface)を定義している。

【動向】

2001 年 3 月、BioAPI コンソーシアムより、BioAPI Version 1.1 がリリースされ、2002 年 8 月には ANSI/INCITS 358-2002 として承認される。ISO/IEC JTC1 SC37 WG2 において、ISO/IEC 19784 として標準化が進められており、現在 FCD。また、BioAPI の内部インタフェースを定義する BioAMI（Biometric Archive Module Interface）に関する NP、及び BioAPI 仕様要件へのバイオメトリクス製品の適合性のテストを定義する NP も承認された。

【詳細】

ここでは、ISO/IEC FCD 19784 の仕様に基づいて BioAPI の説明を行う。BioAPI のアーキテクチャを「図 2-16 BioAPI の構造」に示す。

[1] http://www.microsoft.com/presspass/press/2000/May00/BiometicsPR.asp

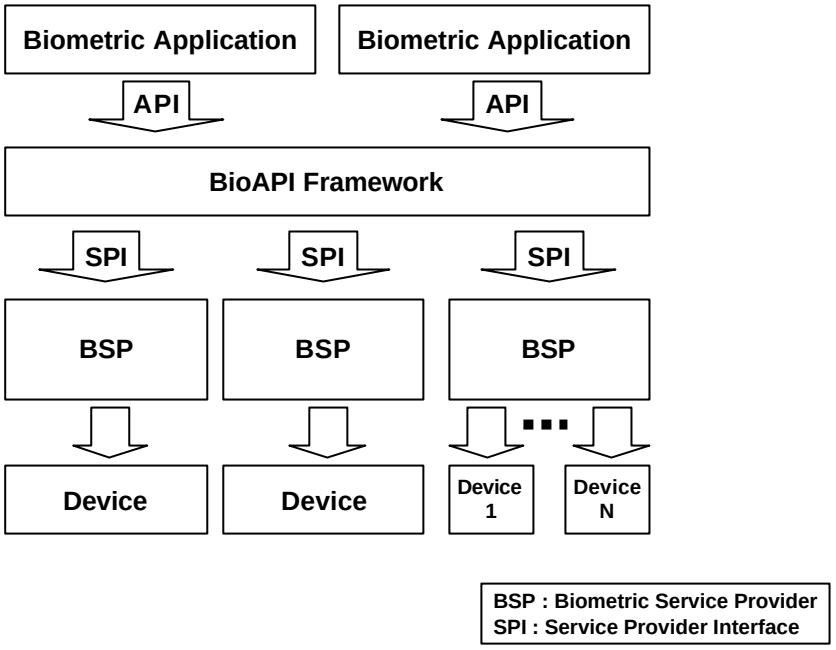


図 2 - 16 BioAPI の構造

この標準で定義されるAPI とは、BioAPI フレームワークとアプリケーションとの間のインタフェースとして、また、SPI は、BioAPI フレームワークとBSP との間のインタフェースとしてそれぞれ定義されている。 表 2 - 9「ISO/IEC FCD 19784 におけるバイオメトリクス関数」にISO/IEC FCD 19784 で定義している主なバイオメトリクス関数を示す。

表 2 - 9 ISO/IEC FCD 19784 におけるバイオメトリクス関数

BioAPI 関数	BioSPI 関数	コメント
BioAPI_Capture	BioSPI_Capture	用途に合ったサンプルをキャプチャする
BioAPI_CreateTemplate	BioSPI_CreateTemplate	登録用のテンプレートを作成する
BioAPI_Process	BioSPI_Process	キャプチャされた中間データを処理する
BioAPI_ProcessPrematchData	BioSPI_ProcessPrematchData	MOC(Match on Card / On-Card Matching 用のテンプレートを作成する
BioAPI_VerifyMatch	BioSPI_VerifyMatch	2 つの BIR の照合を行う
BioAPI_IdentifyMatch	BioSPI_IdentifyMatch	BIR の識別を行う
BioAPI_Enroll	BioSPI_Enroll	登録用の BIR を作成するためにデバイスからバイオメトリクスデータをキャプチャする
BioAPI_Verify	BioSPI_Verify	デバイスからバイオメトリクスデータをキャプチャし、テンプレートと照合する
BioAPI_Identify	BioSPI_Identify	デバイスからバイオメトリクスデータをキャプチャし、複数のテンプレートから識別する
BioAPI_Import	BioSPI_Import	BIR を作成するために、過去のバイオメトリクスデータをインポートする

アプリケーションは、BioAPI フレームワークに対して、API に準拠した関数を呼び出す。BioAPI フレームワークは、BSP (Biometric Service Provider)と呼ばれるコンポーネントと、バイオメトリクスデバイスの管理を行う。BSP とは、マッチング、プロセッシング、アーカイビング、バイオメトリクスデバイスの操作といったバイオメトリクスの機能を備えたコンポーネントである。BioAPI フレームワークは、複数の BSP を動的にロードしたり、呼出したりすることで、複数のアプリケーションが並行して動作することを可能にする。「表 2 - 10ISO/IEC FCD 19784 におけるコンポーネント管理関数」に、コンポーネントを管理する関数を示す。

表 2 - 10 ISO/IEC FCD 19784 におけるコンポーネント管理関数

BioAPI 関数	BioSPI 関数	コメント
BioAPI_EnumBSPs	—	インストールされた BSP を数える

BioAPI_BSPLoad	BioSPI_BSPLoad	BSP をロードする
BioAPI_BSPUnload	BioSPI_BSPUnload	BSP をアンロードする
BioAPI_BSPAttach	BioSPI_BSPAttach	BSP を接続する
BioAPI_BSPDetach	BioSPI_BSPDetach	BSP を切断する

BioAPI フレームワークは、アプリケーションが呼び出した関数を、適切な BSP に対応する SPI に準拠した関数へマッピングを行う。BSP が BioAPI フレームワークにロードされ接続されていれば、アプリケーションは BSP の関数に対してアクセスすることができる。また、アプリケーションが BSP を利用する必要がなくなったとき BSP は BioAPI フレームワークから切断されアンロードされる。

図 2 - 17「BioAPI の詳細な構造」に BSP の詳細なアーキテクチャの一例を示す。

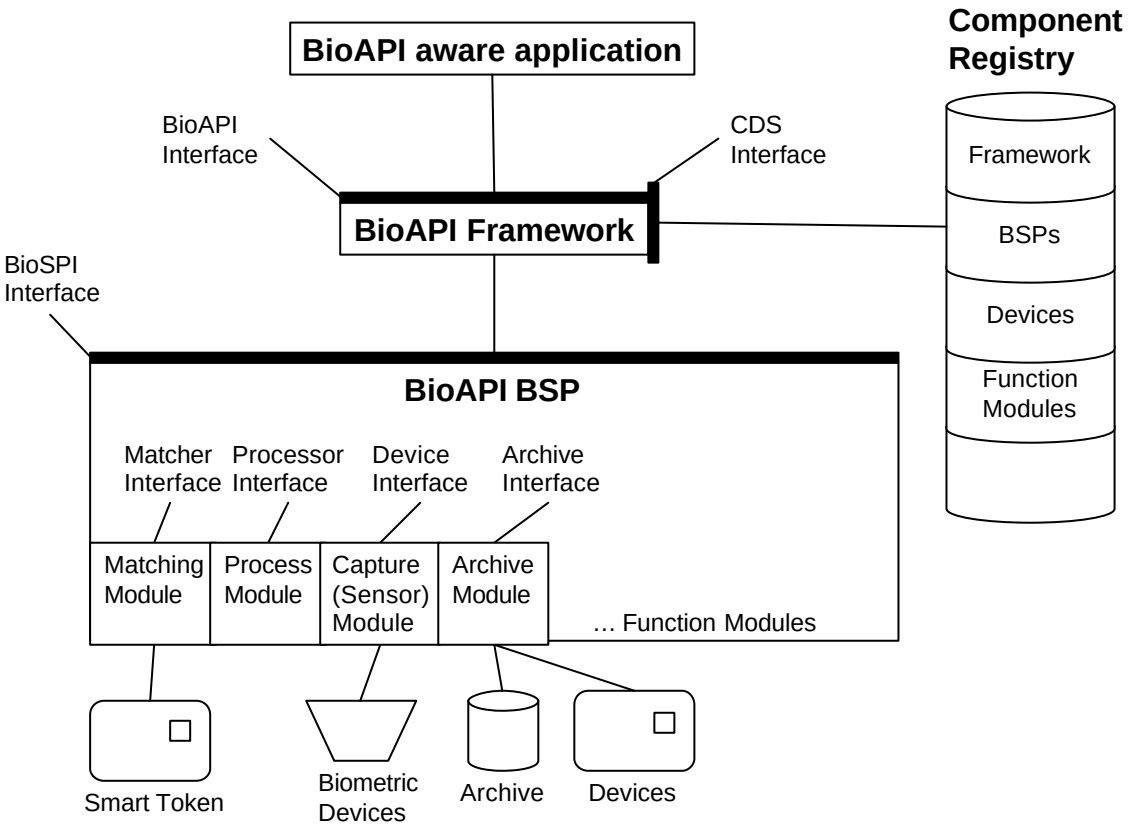


図 2 - 17 BioAPI の詳細な構造

BSP は、matching、processing、archiving、バイオメトリクス装置（装置の機能）の handling のバイオメトリクスの機能のうち、一つ以上の機能をサポートする。バイオメトリクスの機能は、BSP の本体で直接サポートしてもよいし、BSP に着脱可能なファンクションモジュールとしてサポートしてもよい。特定のバイオメトリクスの機能を BSP の本体で直接サポートしている場合、アプリケーションからはこの機能を操作することは不可能である。しかしながら、BSP ではなくファンクションモジュールがその機能をサポートしている場合、アプリケーションは、自由にファンクションモジュールを BSP にロードしたり接続したりすることができる。

ただし、第三者によるソフトウェアモジュールやハードウェアコンポーネントを操作するためには、BSP とデバイスとの間でインタフェースを持つ必要がある。ISO/IEC 19784 では BSP 内のインタフェースについては定めていないため、BSP 内部のインタフェースについては、別途標準化を行わなければならない。内部インタフェースが統一されていない場合には、BSP と BSP に接続されたデバイスが同一のベンダにより提供される必要がある。

BSP がロードされ接続されたとき、すべてのファンクションモジュールは自動的にロードされ、BSP がアンロードされたときにのみ、アンロードされる。

BSP は、同じ機能を持つファンクションモジュールを複数持つことができる。この場合、デフォルトのファンクションモジュールを指定する必要がある。BSP がロードされたときには、このデフォルトとなるファンクションモジュールが BSP の一部としてインストールされる。これらのファンクションモジュールは、同じバイオメトリクスの機能を持つファンクションモジュールと交換することも可能である。

これらのファンクションモジュールの BSP への着脱、インストールされたモジュールへの問合せ、そしてこれらのオペレーションのコントロールを行う関数を 表 2 - 11「ISO/IEC FCD 19784 におけるデバイス操作関数」に示す。ただし、標準化された内部インタフェースを持たない BSP は、これらの関数をサポートしない。

表 2 - 11 ISO/IEC FCD 19784 におけるデバイス操作関数

BioAPI 関数	**BioSPI 関数**	**コメント**
BioAPI_QueryDevices	BioSPI_QueryDevices	BSP の UUID とバージョン、BSP に接続されているデバイスのリストを返す
BioAPI_FunctionAttach	BioSPI_FunctionAttach	ファンクションモジュールを BSP に接続する
BioAPI_FunctionDetach	BioSPI_FunctionDetach	ファンクションモジュールを BSP から切断する
BioAPI_EnumFunctions	―	インストールされたファンクションモジュールのリストを計算する
BioAPI_QueryFunctionModules	BioSPI_QueryFunctionModules	BSP に接続されたファンクションモジュールのリストを計算する

また、この国際標準では、バイオメトリクスコンポーネントレジストリと呼ばれる、バイオメトリクスシステムにロードされているバイオメトリクスコンポーネントについての情報を格納するレジストリ、及びこのレジストリを操作するための CDS（Component Directory Service）インタフェースについての仕様も定めている。

CDS は、BioAPI コンポーネントの性能を記述した、静的な情報のためのレジストリを提供する。他のコンポーネントが CDS にこの情報を調達するために問い合わせてもよい。CDS は BioAPI フレームワークの一部である。インストールされた段階で、BioAPI コンポーネント（フレームワーク BSP、デバイス）は、BioAPI コンポーネントレジストリ内にある自身に関する情報を知らせる。この情報は、BioAPI フレームワークがイン

ストールされていれば、アプリケーションが決定するのに使用される。これもまた、アプリケーションとフレームワークが、どのBSPデバイスがインストールされているか、そしてこれらのコンポーネントの性能は、といった情報を得るために使用される。どのデバイスが接続されているかを識別するために利用することも可能である。 表 2 -　12ISO/IEC FCD 19784 におけるCDS 関数」に、CDSの関数を示す。

表 2 - 12 ISO/IEC FCD 19784 におけるCDS 関数

関数名	コメント
BioAPI_Util_InstallBsp	コンポーネントレジストリに BSP をインストール、アップデート削除する
BioAPI_Util_InstallDevice	コンポーネントレジストリにデバイスをインストール、アップデート削除する
BioAPI_CDSSetAttribute	コンポーネントレジストリの属性を設定する
BioAPI_CDSQueryAttribute	コンポーネントレジストリから値を返す
BioAPI_CDSQueryAttributeNames	コンポーネントレジストリから値の名前を返す
BioAPI_CDSQueryComponents	コンポーネントレジストリの一つのセクションから、すべてのUUID を返す
BioAPI_QuerySections	コンポーネントレジストリのすべてのセクション名を返す

2) BAPI (Biometric Application Program Interface)

【概要】

BAPI は、バイオメトリクスデバイスに対する共通インタフェースを提供することを目的としている。バイオメトリクスデータのフォーマットについては規定していない。

【動向】

1998 年 9 月に Biometric API (BAPI) Device Module Interface Specification (BDMI) Version 1.3、Biometric API (BAPI) Software Developer's Kit (SDK) Version 1.2 がリリースされている。

【詳細】

図 2 - 18「BAPI の構造」に BAPI の構造を示す。

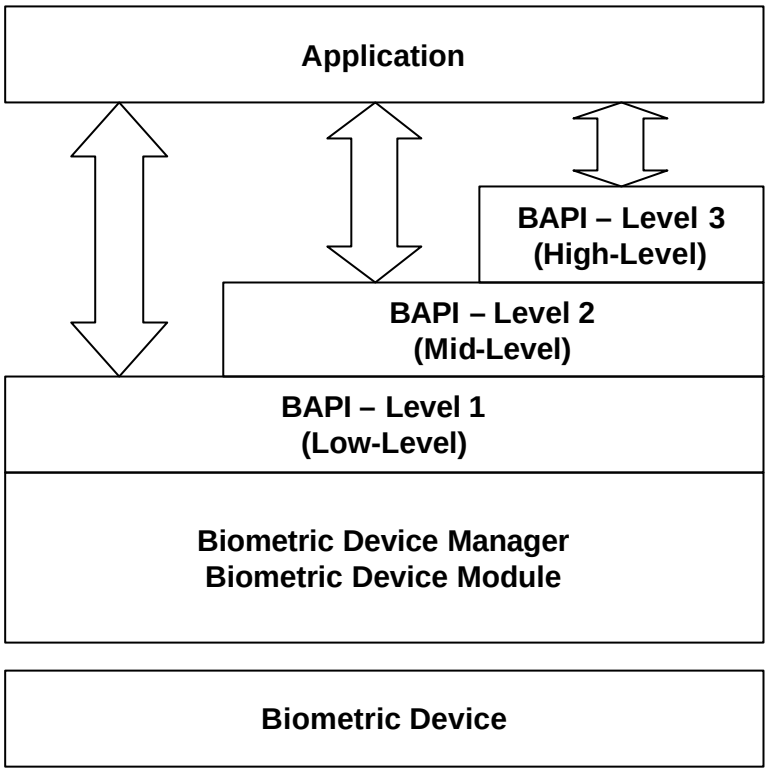


図 2 - 18 BAPI の構造

アプリケーション開発者に対して、BAPI は以下の 3 つのレベルのインタフェースを提供する。

Level 3

アプリケーション開発者に、短時間でアプリケーションのハイレベルなプロトタイプを作成するための非常に利用しやすい、シンプルなインタフェースを提供する。「登録（enrollment）」や「識別（identification）」や「照合（verification）」などの基本的なバイオメトリクス関数をサポートしている。

Level 2

開発者がバイオメトリクスデバイスにより特化した一般的に共通な関数を利用することを可能にする。ただし、特定のデバイスには依存しない。プログラミングは若干難しくなるが、デバイスに対してのアクセスが柔軟になる。

Level 1

特定のデバイスに特化した特性を利用するために、非常に特別で、ローレベルなデバイスプログラミングアクセスを提供する。利用し難いが、最も高い柔軟性と拡張性を提供する。特定のデバイスの機能を API に拡張する。

アプリケーションは BAPI のどのレベルも呼び出すことができるが、一般的には、Level 3 か、Level 2 のみが使用される。

また、BAPIでは、バイオメトリクスデバイス製品ごとに提供されるデバイスドライバに対して、I/O Software社が提供する共通のインタフェースを通じてアクセスするため、異なるベンダによって提供された複数のバイオメトリクスデバイスを同時に操作することが可能になる。

⑸ データフォーマット

1) CBEFF (ISO/IEC CD 19785)

【概要】

CBEFF は、バイオメトリクスを基盤としたアプリケーションとシステムの相互接続技術を、標準的なBiometric Information Record (BIR)の構造の仕様を定めることにより推進する。

【動向】

1999 年 2 月 21 日、NIST とBiometric Consortium は、共通の指紋テンプレートフォーマットにおいて、業界の一致した意見に達する可能性を議論するワークショップを発起した。その後、BioAPI Consortium、ANSI X9F4 金融サービスワーキンググループ、IBIA、TeleTrusT のインタフェースグループが協力し、CBEFF（Common Biometric Exchange Formats Framework）テクニカル開発チーム（NIST、NSA、SAFLINK社、Veridicom社、Biometrics Foundation、ANADAC（現Identix社）、Infineon社によって構成）がCBEFF を作成した。2001 年 1 月、NISTIR 6529 としてリリースされ、現在は、ISO/IEC JTC1 SC37 WG2によりISO/IEC 19785 として標準化が進められている。現在 CD。また、 CBEFF のフォーマット等に一意の識別子を割り当てるためのCBEFF 登録局の運用手続きを規定するための標準も提案されている。

【詳細】

CBEFF で定義しているBIR は、CBEFF パトロンフォーマットと呼ばれる、CBEFF に準拠したフォーマットに基づいたエンコーディングであり、データベースに格納したり、システム間で交換したりするための、バイオメトリクスデータの最も外郭となる構成単位である。基本的な BIR の構造を「図 2 - 19 基本的な BIR の構造」に示す。

SBH	BDB	SB

SBH : Standard Biometric Header　BDB : Biometric Data Block　SB : Signature Block

図 2 - 19 基本的な BIR の構造

基本的にBIR は、ヘッダ情報を格納するためのStandard Biometric Header (SBH)、バイオメトリクスデータを格納するための Biometric Data Block (BDB)、そして、BIR 全体の完全性を保証する署名や MAC を添付するための Signature Block (SB) により構成される。

このBIR は、その使用する目的により仕様を規定する必要がある。その使用目的に合ったBIR の仕様を規定する団体がCBEFF パトロンと呼ばれる団体である。CBEFF パトロンは、CBEFF 登録局と呼ばれる一意の識別子を割り当てる機関から、バイオメトリクス団体識別子を取得した公営もしくは民営の団体である。

CBEFF パトロンは、SBH とBIR の仕様を定義し発行する。この仕様は CBEFF パトロンフォーマットと呼ばれる。CBEFF パトロンフォーマットには、BioAPI の BIR(Biometric Information Record)、X9.84 の Biometric Object、ISO/IEC 7816-11 の BIT(Biometric Information Template)などがある。

この標準では、BIR の構造と、それぞれの BIR におけるヘッダである SBH が扱うデータ要素を規定している。ここでは、単一のバイオメトリクスデータを扱うことを目的とした BIR を simple BIR として、また、複数のバイオメトリクスデータを扱うことを目的とした BIR の構造を nested BIR として定義している。

CBEFFが扱うデータ要素には、BDB のデータフォーマット及び、暗号化や署名のアルゴリズムを記載するフィールドをサポートしているため、その BIR における BDB のフォーマットや暗号化アルゴリズムや署名アルゴリズムなどを識別することは可能である。しかしながら、この標準では、BDB とSB のフォーマットの標準化および、署名や暗号化のアルゴリズムの規定については扱っていない。

SBH の必須データ要素を、「表 2 - 13SBH の必須データ要素」に示す。

表 2 - 13 SBH の必須データ要素

要素名	説明
CBEFF_BDB_biometric_organization	CBEFF バイオメトリクス団体識別子
CBEFF_BDB_format_type	CBEFF バイオメトリクス団体により割り当てられた BDB フォーマット識別子
CBEFF_BDB_security_options	BDB の暗号化の有無 - NO-PRIVACY ・・・ 平文 - PRIVACY ・・・ 暗号化
CBEFF_BDB_integrity_options	署名・MAC の有無 - INTEGRITY - NO-INTEGRITY - MAC - SIGNATURE
CBEFF_subheader_count	（nested BIR のみ） 現在のヘッダに接続された次のレベルのサブヘッダブロックの数

simple BIR

一つの BDB を扱うことを目的とした、simple BIR の構造を「図 2 - 20simple BIR の構造」に示す。

SBH : Standard Biometric Header　BDB : Biometric Data Block　SB : Signature Block

図 2 - 20 simple BIR の構造

simple BIR は、それぞれ一つずつの SBH、BDB、SB により構成される。

nested BIR

nested BIR は、複数のバイオメトリクスデータを持つ BDB（例：指紋、顔、声、複数の指の指紋など）を扱うことを目的としている。

nested BIR は、

a) ルートヘッダ
b) 複数のサブヘッダブロック
c) 署名ブロック

により構成される。

nested BIR における SBH の必須要素である CBEFF_subheader_count フィールドの値は、そのヘッダが持つサブヘッダブロックの数である。そのため、ルートヘッダにおける CBEFF_subheader_count フィールドの値は正整数をとる。

b) のサブヘッダブロックは、

b-1) サブヘッダ
b-2) 以下のいずれか
　b-2-1) レベルゼロサブヘッダブロック
　b-2-2) サブヘッダブロック

により構成される。

SBH における CBEFF_subheader_count フィールドの値は、ルートヘッダと同様に正整数となる。これ以上のサブヘッダブロックを持たないサブヘッダブロックは、レベルゼロサブヘッダブロックと呼ばれる、BDB を格納するためのブロックを持つ。

b-2-1) のレベルゼロサブヘッダブロックは、

b-2-1-1) CBEFF_Subheader_count フィールドの属性が 0 であるサブヘッダ
b-2-1-2) 一つの BDB

により構成される。

尚、レベルゼロサブヘッダブロックの CBEFF_subheader_count フィールドの値が 0 となるのは、レベルゼロサブヘッダブロックはこれ以上の階層構造を持たないためである。

図 2 - 21 nested BIR の例」は、「指」と「声」データを含む nested BIR の構造の例である。ルートとなるヘッダの下に、「指」及び「声」のサブヘッダがあり、それぞれが別の標準に準拠した形式の BDB を持っている構造になっている。

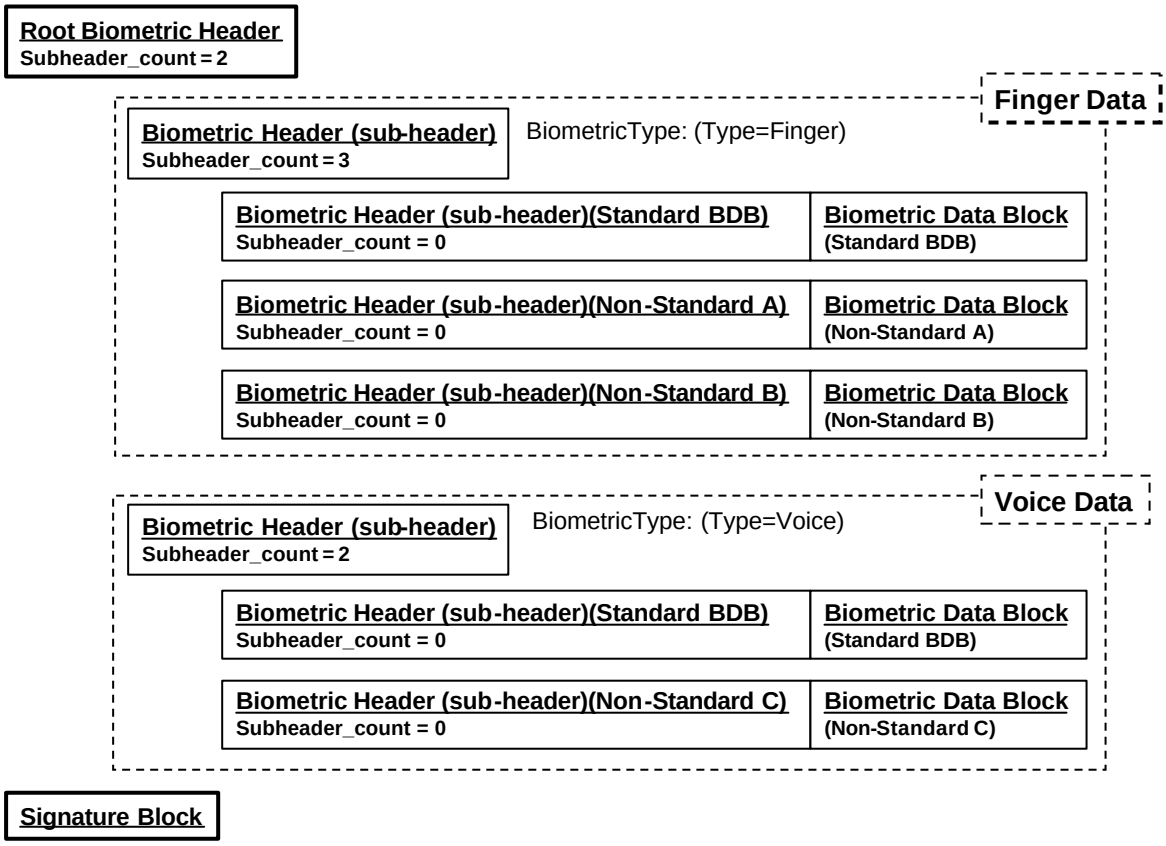
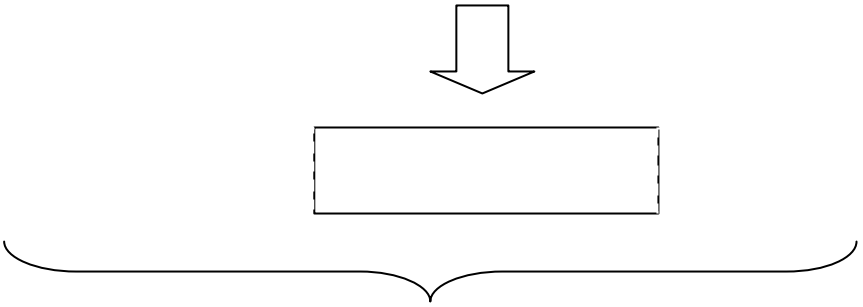


図 2 - 21 nested BIR の例

2) Biometric Data Interchange Format (ISO/IEC 19794)

【概要】

この標準では、バイオメトリクスデータ交換フォーマットを定義している。この標準で仕様を規定しているバイオメトリクスデータ交換フォーマットは、CBEFF の BDB に組み込まれる。すなわち、ISO/IEC 19785（CBEFF）のようなバイオメトリクスフォーマットのフレームワークは、この標準において規定するバイオメトリクスデータのラッパー（wrapper）としての役割を持つ。図 2 - 22Biometric Data Interchange Format と CBEFF の関係」に、Biometric Data Interchange Format とCBEFF の関係を示す。



Part 6: Iris Image Data

Part 7: Signature/Sign Data

以下に, それぞれのパートについて述べる。

Part 1: Framework

このパートでは、この標準におけるフレームワークを規定することを目的としている。

Part 2: Finger Minutiae Data

このパートでは、特徴点の基本的な概念を使用した指紋の表現の概念とデータフォーマットの仕様を定めている。この標準は、関連項目の定義、特徴点が配置される位置の記述、一般的な利用とカードを用いた利用のためのデータを含むデータフォーマット、そして、一致情報を含んでいる。

Part 3: Finger Pattern Data

このパートでは、パターンによる指紋認識データの交換フォーマットを規定する。

Part 4: Finger Image Data

このパートでは、イメージによる指紋認識データの交換フォーマットを規定する。

Part 5: Face Image Data

このパートでは、イメージによる顔面認証データの交換フォーマットを規定する。

Part 6: Iris Image Data

このパートでは、イメージによる虹彩認証データの交換フォーマットを規定している。

Part 7: Signature/Sign Data

このパートでは、バイオメトリクス識別や照合を目的として、ベクトル化されたイメージとして読取られたデジタル化されたサインや署名データの表現に対するコンセプト及びデータフォーマットを規定する。

3) XCBF (XML Common Biometric Format)

【概要】

この仕様は、CBEFF (NISTIR 6529) パトロンフォーマットのためのセキュアな XML エンコーディングの共通セットを定義する。

【動向】

2003 年 8 月、OASIS からVersion 1.1.がリリースされた。

【詳細】

この仕様は、CBEFF (NISTIR 6529) に準拠したパトロンフォーマットに対して、セキュアなXMLエンコーディングの共通セットを定義する。これらの XML エンコーディングは、ANSI X9.84 において定義された ASN.1 スキーマに基づいている。これらのエンコーディングは、セキュリティを目的として、ITU-T Rec. X.693 において定義された ASN.1 に対する Canonical XML Encoding Rule (CXER) を利用し、X9.96 XML Cryptographic Message Syntax (XCMS) 及び X9.73 Cryptographic Message Syntax (CMS) において規定されたセキュリティと処理の要件に依存している。

⑹ 適用形態

1) X9.84

【概要】

金融サービスのためのバイオメトリクス情報の管理及びセキュリティについて規定している。

【動向】

2003 年 7 月に、ANSI から X9.84-2003 が発行された。現在は、TC 68 において ISO/IEC 19702 として標準化が進められている。

【詳細】

この標準では、バイオメトリクスデータの効果的な管理のための最小のセキュリティ要件の仕様を規定している。この標準の範囲には以下のトピックを含む：

- バイオメトリクスデータの抽出、配布、処理、網羅的なデータの完全性、信頼性、否認防止のためのセキュリティ
- 登録、交換と格納、照合、識別、抹消処理により構成されるライフサイクルを通したバイオメトリクスデータの管理
- 銀行顧客及び従業員の識別及び認証を目的とした、1 対 1 認証、1 対 N 認証を含むバイオメトリクス技術の使用方法
- 論理的かつ物理的なアクセス制御および、内部的及び外部的なバイオメトリクス技術のアプリケーション
- バイオメトリクスデータのカプセル化
- バイオメトリクスデータのセキュアな交換及び格納のための技術
- バイオメトリクスデータのライフサイクルにおいて使用される物理的ハードウェアのセキュリティ
- バイオメトリクスデータの完全性とプライバシー保護のための技術

以下のトピックについてはこの標準では対象外としている：

- 個人のプライバシーとバイオメトリクスデータの所有者
- アプリケーションの仕様要件と、バイオメトリクス技術の採用のための制限

また、X9.84-2003 では、この標準で扱うバイオメトリクスデータ（Biometric Object）と、XCBF 及び BioAPI 1.0 で扱うバイオメトリクスデータ（BIR：Biometric Identification Record）の交換形式についても言及している。

１．７．２ PKI

⑴ PKI とは

PKI とは「Public Key Infrastructure」の略で、公開鍵暗号技術と電子署名を使って、安全な通信ができるようにするための環境のことをいう。

⑵ PKI の仕様をとりまく代表的な団体

PKI の仕様をとりまく代表的な団体をまずは示しておく。なお、それぞれの詳細及びその他は次章以降

で示していく。

[標準化団体]

- ITU-T（International Telecommunication Union - Telecommunication sector）
  PKI の証明書フォーマットである X.509 を ISO/IEC と協調してを規定している。

- ISO/IEC （ International Organization for Standardization / International Electro-technicalCommission）
  JTC1(Joint Technical Committee1) SC6 において PKI の証明書フォーマットである 9594-8 を ITU-T と協調して規定している。

- IETF (Internet Engineering Task Force)
  ワーキンググループ Security Area 分野の
  - PKIX(Public-Key Infrastructure)
  - SPKI(Simple Public Key Infrastructure)
  - TLS(Transport Layer Security)
  - SMIME(S/MIME Mail Security)
  - Ipsec(IP Security Protocol)

  のワーキンググループにおいて PKI に関する標準化を行っている。特に PKIX が主体で進められている。IETF の成果は RFC (Request for Comments)の規格を公開している。

[企業]

- RSA Security
  公開鍵暗号方式を用いた関連技術である Public Key Cryptography Standards(PKCS)を定めている。一部は IETF に採用されている。PKCS の詳細に関しては 1. 7. 2 (12)PKCS（Public-Key Cryptography Standard）を参照のこと。

(3) 関連表

以下に PKI に関する標準化団体とその技術関連表を示す。なお、詳細は次節以降に示す。

表 2 - 15 PKI 技術関連表

		標準化団体			
		ITU-T	ISO/IEC	IETF	RSA Security
機能	暗号処理			RFC2437、RFC2898	PKCS #1、PKCS #5、PKCS#13
	鍵処理				PKCS #3、PKCS #8
	署名処理			RFC2315	PKCS #7
	証明書及び鍵の交換形式				PKCS #12
	証明書の申請に使用する形式			RFC2986	PKCS #10
	公開鍵証明書形式	X.509	9594-8	RFC3280	
	CRL形式	X.509	9594-8	RFC3280	
	クオリファイド証明書形式			RFC3039	
	属性証明書形式	X.509	9594-8	RFC3281	
	認証局運用			RFC3647	

⑷ 電子証明書及び認証局

1) 証明書の概要

PKI 基盤で使われる証明書の標準として ITU-T が策定した X.509 がある。X.509 で規定されている電子証明書には、公開鍵証明書(Public Key Certificate)、証明書失効リスト(CRL :Certificate Revocation List)、属性証明書(Attribute Certificate)がある。公開鍵証明書には通常のものに加えて、拡張領域が発展したクオリファイド証明書（特定証明書）も規定されている。

⑸ 動向

1) X.509 の版について

X.509 の最初の版は 1988 年に発行された。その後、1994 年に公開鍵証明書のフォーマットを Version 2 にした 2nd Edition が発行されたが、これは現在ではほとんど使用されていない。さらに 1997 年に発行された 3rd Edition においては、公開鍵証明書に拡張領域が設けられて任意の拡張が可能になった。その後、2000 年に属性証明書の定義が明確化された属性証明書のフォーマット Verision 2 が盛り込まれた 4th Editon が発行された。以下に対応一覧を示す。

表 2 - 16 X.509 証明書変遷

YEAR	X.509 Edition	公開鍵証明書	CRL	属性証明書
1988	1st Edition	v1	v1	
1994	2nd Edition	v2	v1	
1997	3rd Edition	v3	v2	v1
2000	4th Edition	v3	v2	v2

2) IETF との関連

X.509v3 をインターネットで利用することを目的として、IETF の PKIX 作業部会によって証明書プロファイル RFC2459（現時点では廃止）が 1999 年に公開された。RFC2459 では、1997 年版の X.509v3 証明書

とCRLv2 に関するプロファイルを規定している。さらにX.509 4th Edition が反映されたRFC 3280 が2002年に公開された。

IETFで策定されたこのプロファイルは、X.509 使用方法をアプリケーションの実装を容易にするために証明書拡張の存在が必須なのか、任意なのか等を規定して使用方法を限定することによって、例えばGPKIのプロファイルのような相互運用が必要な比較的汎用的なサービスや製品に対応されたものが範疇に考慮されている。

⑹ 公開鍵証明書

【概要】

1. 7. 2 ⑷ 1)証明書の概要を参照のこと。

【動向】

1. 7. 2 ⑸動向を参照のこと。

【詳細】

1) 公開鍵証明書 プロファイル

公開鍵証明書 v3 のプロファイルについて示す。

表 2 - 17 公開鍵証明書プロファイル

領域名			説明	型	本人確認機器証明書に用いる場合
tbsCertificate(署名前証明書)	version		X.509証明書のバージョン	INTEGER	TRUE
	serialNumber(シリアル番号)		証明書を一意に識別するための番号。発行者(CA)が割り当てる。	INTEGER	TRUE
	signature(アルゴリズム識別子)		発行者が証明書に署名する際に用いるアルゴリズムである。OIDで指定する。	AlgorithmIdentifier	TRUE
	issuer(発行者)		証明書を発行した機関(CA) の名前。X.500 識別名 (DN) において記述される。CA の証明書に含まれる subject と同じDNが記述される。	Name	TRUE
	validity(証明書の有効期間)	notBefore(開始時刻)	証明書が有効になる時刻。2049 年までは UTCTime としてエンコードしなければならない。2050 年以降の証明書の有効期限の日付は GeneralizedTime としてエンコードされなければならない。	Time	TRUE
		notAfter(終了時刻)	証明書が無効になる時刻。2049 年までは UTCTime としてエンコードしなければならない。2050 年以降の証明書の有効期限の日付は GeneralizedTime としてエンコードされなければならない。	Time	TRUE
	subject(主体者)		証明書の所有者の名前です。発行者と同じくDNで記述される。ユーザの名前やサーバー名などが記述される。	Name	必須
	subjectPublicKeyInfo(証明書所有者(主体者)の公開鍵に関する情報)	algorithm	公開鍵のアルゴリズム名	AlgorithmIdentifier	TRUE
		subjectPublicKey	主体者が所有している公開鍵	BIT STRING	TRUE
	issuerUniqueID(主体者ユニーク識別子)		主体者名を再利用した際に、主体者を識別するために使用される。バージョン2 で追加された。発行者ユニーク識別子と同様に、主体者ユニーク識別子は使用しないことが推奨される。この項目は省略可能。	UniqueIdentifier	不必要
	extensions		証明書の拡張領域。バージョン 3で追加された。	Extensionのシーケンス	不必要
signatureAlgorithm(署名アルゴリズム)			発行者が証明書に署名する際のアルゴリズム。OID で指定する。tbsCertificate の signature(アルゴリズム識別子)と同じ値を指定する。	AlgorithmIdentifier	TRUE
signatureValue(署名値)			発行者のデジタル署名が入る	BIT STRING	TRUE

TRUE :確認必須
FALSE :確認不必須

2) 公開鍵証明書の拡張領域

X.509 公開鍵証明書 v3 フォーマットより、証明書に拡張領域 (extensions) を追加できるようになった。拡張領域を用いることにより、目的に応じた証明書の拡張が可能となる。

拡張領域は、以下の 3 つのフィールドの並び (シーケンス)で構成される。

- 識別子(extnID):拡張子の種別を表す。OID で指定する。
- 重要度 (critical) :拡張子の重要度(critical)を示す。重要度は BOOLEAN 型であり、真(True) か偽(False) にて指定する。拡張子が重要と指定されている場合は、公開鍵証明書を利用する PKI アプリケーションはその拡張子を認識できなければならない。PKI アプリケーションがその拡張子を認識できない場合は、該当する証明書を拒絶しなければならない。
- 拡張値 (extnValue):拡張子のデータが入る。データの型は識別子の OID にて決まる。

以下に、RFC2459 による公開鍵証明書の拡張プロファイルを示す。

表 2 - 18 公開鍵証明書拡張領域プロファイル

領域名	重要度	説明	本人確認機器証明書に用いる場合の確認
Subject Type Extensions (主体タイプ拡張)			
basicConstraints(基本制約)	TRUE	CAの証明書であるか否かを示す。EE (エンドエンティティ)に発行した証明書が、不正にCAの証明書として使われることを防ぐために使用する。CAの証明書である場合は、そのCAの下位CAとなることができる階層数を指定できる。	TRUE
Name Extensions (名前拡張)			
issuerAltName(発行者別名)	FALSE	発行者(issuer)の別名を指定	不必要
subjectAltName(主体者別名)	TRUE	基本領域の主体者(subject)の別名 (メールアドレス等)を指定。主体者(subject)領域が空の場合、このフィールドは重要フラグとともに必須となる。	TRUE
nameConstraints(名前制約)	TRUE	下位CAの証明書に使用される。下位 CA が発行できる証明書の範囲を限定する。	TRUE
Key Attributes (**鍵属性**)			
keyUsage(鍵使用目的)	TRUE	**証明書に含まれる公開鍵の使用目的を示す。暗号用の鍵と署名検証用の鍵を区別するために使用する。使用目的はビット列で指定する**	TRUE
extendedKeyUsage(拡張鍵使用目的)	どちらでもよい	keyUsage フィールドよりも詳細に、証明書に含まれる公開鍵の使用目的を示す。使用目的は、OID で指定され、Webや電子メールの保護などがある。	不必要
privateKeyUsagePeriod(秘密鍵有効期間)	FALSE	デジタル署名に使用する秘密鍵の有効期間を指定する。RFC2459では、このフィールドは使用しないことが推奨される	不必要
subjectKeyIdentifier(主体者鍵識別子)	FALSE	主体者が複数の鍵ペアと証明書を持つ場合に、特定の公開鍵を特定するために用いる。公開鍵の特定には、公開鍵のハッシュ値などを用いる。	不必要
authorityKeyIdentifier(機関鍵識別子)	FALSE	subjectKeyIdentifier と同様、CA が複数の鍵ペアと証明書を持つ場合に、特定の公開鍵を特定するために用いる。	不必要
Policy Information (ポリシー情報)			
certificatePolicies(証明書ポリシー)	どちらでもよい	証明書ポリシー (CP：Certificate Policy)を OID で指定しする。また、認証局運用規定(CPS) への URL を指定する。CP を規定しない場合は AnyPolicy という OID を指定する。	不必要
policyMappings(ポリシーマッピング)	FALSE	複数の CA が相互認証を行う場合に、それぞれの CP を対応付けるために使用する。	不必要
policyConstraints(ポリシー制約)	どちらでもよい	下位 CA に対して、ポリシーマッピングの制限と CP の義務付けを行う。	不必要
inhibitAnyPolicy(AnyPolicyの禁止)	TRUE	下位CAに対して、CP に AnyPolicy を記載した証明書を発行することを禁止する。X.509v3 の 2000年版において追加された	TRUE
Additional Information (追加情報)			
cRLDistributionPoints(CRL配布点)	FALSE	デルタ CRL を入手するための情報を記載する。記述方法は、cRLDistributionPoints と同様です。X.509v3 の 2000年版において追加された。	FALSE
subjectDirectoryAttributes(主体者ディレクトリ属性)	FALSE	主体者の属性を指定する。このフィールドは使用しないことが推奨される。	不必要

(7) クオリファイド証明書（特定証明書）

【概要】

公開鍵証明書の拡張領域を利用して、発展したものである。以下のような特徴を持つ。

- 基本領域、拡張領域への記載内容にルールを設けている。
- 特定証明書に特化した「生体情報」と「QC 宣言」などが拡張領域で持たれる。

【動向】

まず記載内容に関するルールとして欧州電子署名指令案（EU-directive）の指示のもと、欧州電気通信標準化協会（ETSI：European Telecommunications Standards Institute）によりまず標準化見当がなされた。

そして、IETF により 2001 年 1 月に RFC3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile（インターネット X.509 公開鍵インフラストラクチャ QC プロファイル）が定められている。さらに、2004 年 3 月に RFC3739 Internet X.509 Public Key Infrastructure Qualified Certificates Profile が公開された。

【詳細】

1) 証明書プロファイル

以下にクオリファイド証明書プロファイルを示す。

表 2 - 19 クオリファイド証明書プロファイル

領域名		説明
基本領域	発行者名（Issuer）	発行者組織・名称は公的に登録された名称を用いることになっている。
	主体者名（Subject）	証明書の発行を受ける本名ないしは通称を用いることになっている。
拡張領域	主体者ディレクトリ属性（Subject Directory）	主体者の役職、生年月日、出生地、性別、国籍、居住地が記載できる。この項目は必須ではない。
	証明書ポリシー（Certificate Policies）	証明書ポリシー（OID）を最低一つは記載することになっている。この項目は必須にすることもできる。
	鍵使用目的（Key Usage）	この項目は必ず設定することになっており、必須にすることもできる。否認防止（NonRepudiation）に指定した場合は他の使用目的の指定はできないことになっている。
	生体情報（BiometricInfo）	この項目はオプション的に、写真、署名筆跡、指紋などの生体情報のハッシュ値などを記載できる。値の実態を格納したアドレス（URLなど）も記載できる。必須は不可。
	QC宣言（QcStatements）	法的な説明文（QC 宣言）を登録した OID を記載します。この項目は必須にすることができる。

2) 生体情報

RFC3039 によると、バイオメトリクスの情報は、バイオメトリクスのハッシュ値の形で格納される。格納されたハッシュ値に対応する生体情報そのものは拡張に格納されないが、拡張にその情報が取得可能な場

所を指し示す URI を含めることができる。URI が含まれていても、該当の情報にアクセスする唯一の方法を意味するものではない。この拡張にある生体情報は、人間による検証に適した情報形式に限定することが推奨される。すなわち、当該情報が主体者を正確に代表しているかどうか、人間が自然に判断できることである。例えば、証明書所有者（relying party）に画像イメージを表示し、主体者を識別する手段を強化するために利用することができる。

⑧ 属性証明書

【概要】

公開鍵証明書によって、システムに対する本人認証（Authentication）を行った後は、そのユーザに割り当てられた「権限」によるアクセス制御（アクセスコントロール）が必要となる。公開鍵証明書のみを用いたアクセスコントロールには 2 通りの方法があるが、以下のような問題がある。

1. （方法）権限情報はシステム内部で保持し、本人認証と結果を結び付ける方法→（問題点）システムの作りにより権限情報の安全管理レベルがまちまちになる。権限管理機能の開発維持にコストがかかる。
2. （方法）公開鍵証明書に権限を記載する→（問題点）権限の変更に伴い、公開鍵証明書の再発行が必要となる。複雑な権限情報を記載できる適当な領域（プロファイル）が無い。

そこで、ユーザの権限に関する「属性」のみを記載した証明書、「属性証明書（Attribute Certificate）」が考案された。

【動向】

ISO/IEC が1997年にX.509 3rd Editionの属性証明書v1を発行し、続いて2000年にX.509 4th Editionの属性証明書 v2 が公開された。

それを受けて、IETF も 2002 年 4 月に RFC3281[分類：スタンダードトラック]（An Internet Attribute Certificate Profile for Authorization）公開している。

【詳細】

属性証明書には公開鍵証明書の発行者とシリアル番号が保持されており、それにより公開鍵証明書に紐付けられている。本人認証を公開鍵証明書で行い、その後のアクセスコントロールに属性証明書を利用することになる。属性証明書は、前述の問題をクリアするため、公開鍵証明書を発行する CA とは別の組織（人）により運営される属性認証機関（AA: Attribute Authority）により発行されることが想定されている。また、属性証明書には公開鍵が含まれないため、属性証明書の発行に関する運用形態はシンプルなものになる。

1） 属性証明書を利用したモデル

以下に属性証明を利用したモデルを示す。

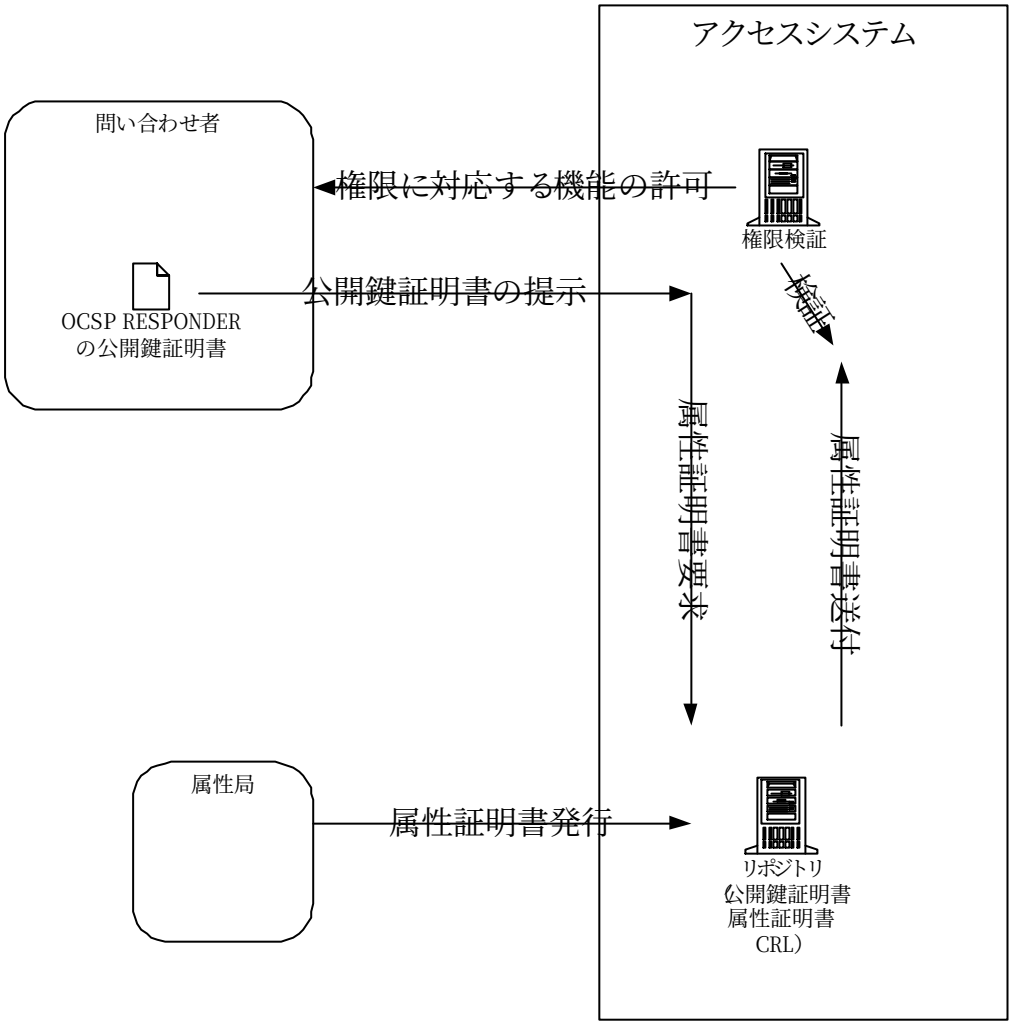


図 2 - 23 属性証明書を利用したモデル

2) 利点と欠点

利点）

- 属性が変更され場合に公開鍵証明書を破棄せずに済む。
- 認証局と権限付与者を分離することが可能である。
- 権限委譲の仕組みが実現できる。

欠点）

- 公開鍵証明書のみの場合に比べて、管理が複雑になる。

3) バイオメトリクス関連適応の検討

本人確認機器認証システムにおいて、個々の確認機器において権限等を持たせて制御する場合は有効であると思われる。

(9) PKI の運用について

認証局運用規定(Certificate practice statement : CMP)

【概要】

証明書の利用用途（Certificate Policy :CP）をどのように実施するかというCA の運用規定を定めたもの。CA のシステムや運用手順を明示的な文書にして、証明書に記載された URI などで利用者に公開される。

【動向】

IETF から 1999 年に RFC2527 [現在は廃止されている] (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)が公開された。

その後、2003 年 11 月に RFC3647 [分類 :Informational]が後継として公開されて、今に至る。

【詳細】

RFC3647 において一般規定、本人確認と認証、運用要件、物理面・手続面及び人事面のセキュリティ管理、技術的管理、証明書とCRL プロファイル、仕様の管理、法規について規定されている。

(10) 証明書の失効処理

1) CRL

【概要】

失効された証明書の一覧を「**CRL**（証明書失効リスト）」という。CRL は、証明書を発行した CA が運用ポリシーに則り、即時的に、また定期的な周期で発行する。CRL には更新日時の領域があり、ある時点での証明書の有効性を確認できるようになっている。期間内に新たに失効された証明書が無くても CRL は発行される。

CRL には失効された証明書のシリアル番号、CRL の発行者名(通常は CA の名前と同じ)、更新日、次回更新日などが記載されている。有効期限切れとなった証明書は CRL には記載されない。

【動向】

まず、ISO/IEC から1988 年に X.509 CRL v1 が公開された。その後、1997 年に CRL 拡張とCRL エントリ拡張が設けられたX.509 CRL v2 が公開された。

IETF は X.509 を受けて、1991 年 1 月に RFC2459(現在は廃止)[分類 :スタンダードトラック](インターネットX.509 PKI - 証明書と CRL のプロファイル(Internet X.509 Public Key Infrastructure Certificate and CRL Profile))を公開した。さらにその後継として、2002 年 4 月に RFC3280 [分類 :スタンダードトラック](Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile が公開されて今に至っている。

【詳細】

一般的なデータフォーマットはX.509 CRL v2 フォーマットで規定されている。CAは失効した証明書のリストを一定期間で CA の署名をつけて公開される。この CRL の入手元と入手のための通信プロトコルは、X.509 証明書拡張領域のCRL 配布項目にあるCRL Distribution Points で記述される。CRL Distribution

Points エクステンションには配布点（DistributionPoint）を複数記述することができる。

また、CRL には発行者の電子署名が付与されているため、第三者による改ざんを防ぐことができる。また、CA 以外が CRL を発行する間接 CRL (Indirect CRL)のしくみを用いる場合もある。

2) CRL プロファイル

基本フォーマットは以下のようになる。

表 2 - 20 CRL プロファイル

領域名			説明	本人確認機器証明書に用いる場合
tbsCertList(署名前証明書リスト)	version		CRLのバージョン	TRUE
	signature(アルゴリズム識別子)		発行者が証明書に署名する際に用いるアルゴリズムである。OIDで指定する。	TRUE
	issuer(発行者)		このCRLの発行者名	TRUE
	thisUpdate(今回更新日時)		CRLの更新日時	TRUE
	nextUpdate(次回更新日時)		次回のCRLの更新日時	TRUE
	revokedCertificates（失効証明書のリスト）	userCertficate（ユーザ証明書）	失効された証明書のシリアル番号	TRUE
		revocation（失効日時）	証明書が失効された日時	TRUE
		crlEntryExtensions（CRLエントリ拡張）	個々の証明書の拡張領域	任意
signatureAlgorithm(署名アルゴリズム)			CRL発行者が証明書に署名する際のアルゴリズム。OID で指定する。	TRUE
signature(署名)			CRL発行者のデジタル署名が入る。	TRUE

TRUE :確認必須
FALSE :確認不必須

3) CRL の ASN.1 モジュールの一部例

CRL の ASN.1 モジュールの一部の例を以下に示す。

```
CertificateList  ::=  SEQUENCE  {
        tbsCertList                 TBSCertList,
        signatureAlgorithm          AlgorithmIdentifier,
        signature           BIT STRING }
TBSCertList  ::= SEQUENCE  {
        version                             Version OPTIONAL,
                                                -- if present, shall be v2
        signature                   AlgorithmIdentifier,
        issure                              Name,
```

```
        thisUpdate                      Time,
        nextUpdate                      Time OPTIONAL,
        revokedCertificates             SEQUENCE OF SEQUENCE {
                userCertificate                 CertficateSerialNumber,
                revocationDate                  Time,
                crlEntryExtensions              Extensions OPTIONAL
                                                  --if present, shall be v2
                                        } OPTIONAL,
        crlExtensions                   [0] Extensions OPTIONAL
                                                --if present, shall be v2
    -- }
```

4) CRL の利点・欠点

利点）

- ネットワークにつながっていなくても、CRL ファイルがあれば失効の確認ができる。

欠点）

- CRL は、決められた周期で発行されるため、証明書が失効された場合でも、次回の CRL が発行されるまでは失効情報が利用者に伝わらない。CRL の発行周期を長くすると、失効情報が利用者に通知されるまでの時間が長くなってしまう。逆に、発行周期を短くすると、利用者が CRL を取得するための負荷が増大してしまう。

(11) Online Certificate Status Protocol（OCSP）

【概要】

オンラインで証明書の失効情報を確認するためのプロトコルである。証明書利用者（OCSP リクエスタ）は、OCSP レスポンダ（OCSP サーバとも呼ばれる）に失効情報を問い合わる。OCSP レスポンダは、問い合わせに対して証明書の状態について、有効(good)、失効(revoked)、不明(unknown) のいずれかとして返す。

【動向】

IETF が 1999 年 6 月に RFC2560[分類：スタンダードトラック](X.509 インターネット PKI オンライン証明書状態プロトコル（OCSP）(X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP))を公開している。

【詳細】

1) モデル図

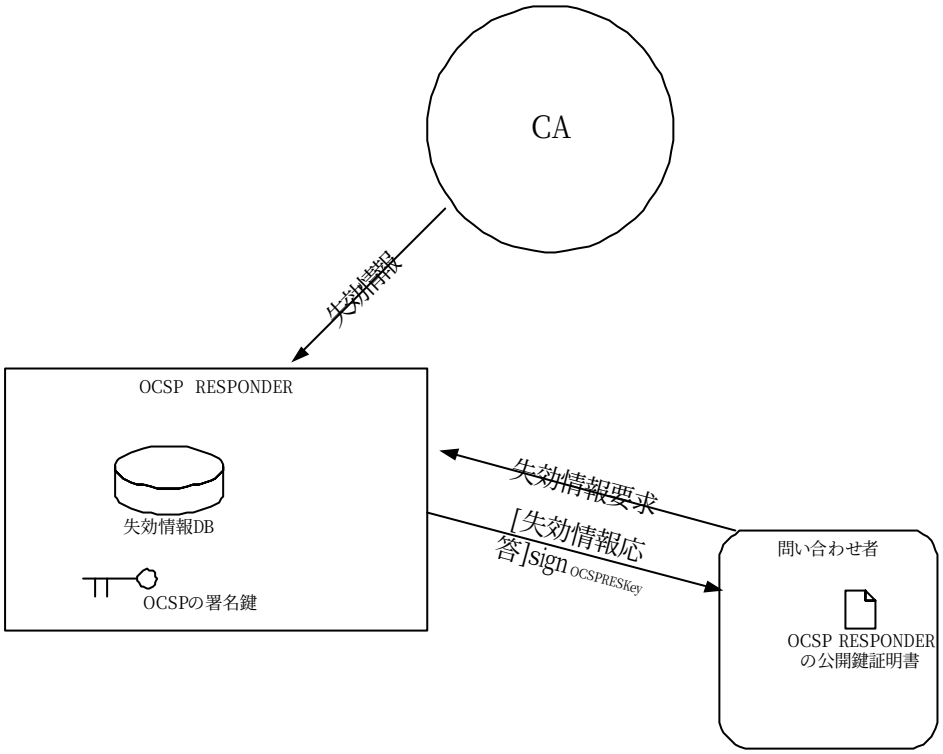


図 2 - 24 OCSP モデル

2) 利点と欠点

利点）

- CRL による有効性検証の処理を証明書利用者が行わずに、常に最新の情報を得ておくことが可能である。
- 自分のリストに関係ない情報を所持しておく必要がない。

欠点）

- ネットワークにつながっていることが必須となる。
- 証明書が失効されているかどうかを確認するだけであり、証明書の有効性を検証するための証明書のパス構築と検証は、証明書利用者が実施しなければならない。これらの処理は証明書利用者にとって、負荷のかかるものとなる。

  なお、サーバ側で失効状態の確認だけでなく、証明書のパス構築と検証までを行う方式が検討されている。次章で述べる。）
- OCSP レスポンダの証明書の失効の場合に通常処理できない。

3) OCSP の問題点対応

サーバ側で失効状態の確認だけでなく、証明書のパス構築と検証までを行う以下の証明書パス構築＋証明書パス検証方式とOCSP の単純化の2つの方式が IETF に おいて検討されている。

(a) Delegated Path Discovery(DPD)+ Delegated Path Validation(DPV)

【概要】

OCSP を拡張し、証明書パス構築 (DPD : Delegated Path Discovery)と証明書パス検証 (DPV : Delegated Path Validation) を連携させる。

【動向】

DPD に関しては IETF が 2000 年 9 月に Internet Draft draft-ietf-pkix-scvp-03.txt :September, 2000 “Delegated Path Discovery with OCSP”を公開している。

また、DPV に関しては 2000 年 8 月に
Internet Draft draft-ietf-pkix-ocsp-valid-00.txt :August, 2000
“Delegated Path Validation”を公開している。

(b) Smple Certificate Validation Protpcol (SCVP)

【概要】

証明書利用者側アプリケーションでの証明書に関する処理を OCSP より単純化したものである。

【動向】

IETF が 2000 年 6 月に Internet Draft draft-ietf-pkix-scvp-03.txt :June 12, 2000 「Simple Certificate Validation Protocol」を公開している。

(12) PKCS (Public-Key Cryptography Standard)

PKCS とは PKI で利用する証明書や秘密鍵などのフォーマットを定めた標準である。RSA Security 社によって策定されている。データフォーマットは ASN.1をベースにしている。

表 2 - 21 PKCS の種別

種別	名称	説明
PKCS #1	RSA Encryption Standard	RSA 暗号方式のアルゴリズムとデータフォーマット。RFC2437 にて公開。
PKCS #3	Diffie-Hellman Key-Agreement Standard	DH を用いた鍵交換方式の実装方法。
PKCS #5	Password-Based Cryptography Standard	パスワードをベースとした用いた暗号方式。RFC2898 にて公開。
PKCS #6	Extended-Certificate Syntax Standard	証明書の形式を規定したもの。
PKCS #7	Cryptographic Message Syntax Standard	暗号データやデジタル署名のフォーマット。証明書や CRL の配布、S/MIME にも利用。RFC2315 にて公開。
PKCS #8	Private-Key Information Syntax Standard	秘密鍵のデータフォーマットを定めたもの。

種別	名称	説明
PKCS #9	Selected Object Classes and Attribute Types	PKCS #7, PKCS #10, PKCS #12 等の属性型を定めたもの。RFC2985 にて公開。
PKCS #10	Certification Request Syntax Standard	証明書の申請に使用するフォーマット。RFC2986 にて公開。
PKCS #11	Cryptographic Token Interface Standard	暗号トークン（スマートカード）とのインターフェースを定義。
PKCS #12	Personal Information Exchange Syntax Standard	秘密鍵と証明書を交換するためのフォーマット。秘密鍵はパスワードで保護。
PKCS #13	Elliptic Curve Cryptography Standard	楕円鍵暗号に関するアルゴリズム
PKCS #15	Cryptographic Token Information Format Standard	暗号トークンのデータフォーマットを定めたもの

PKCS #2, PKCS #4 は、PKCS #1 に吸収されたため廃止。また、PKCS#14 は未定義。
（http://www.ipa.go.jp/security/pki/033.html より抜粋）

1) PKCS#1

【概要】

RSA による暗号化方式のアルゴリズム、公開鍵ペアのフォーマットなどを規定。PKCS#1 では以下の 4 つの項目について記載している。

- 暗号化の基本要素
- 暗号化のスキーム
- 署名のスキーム
- ASN.1 データフォーマット

例) RSAEP((n,e),m)
入力：(n,e) RSA 公開鍵
m 平文データ（0<m<n-1 を満たす整数）
出力：暗号化データ（0<m<n-1 を満たす整数）

【動向】

2002 年 6 月 14 日にリリースされた Version 2.1 が最新。

2) PKCS#3

【概要】

Diffie-Hellman 方式による鍵交換の方法を規定している。

【動向】

1993 年 11 月 1 日にリリースされた Version 1.4 が現行バージョン。

3) PKCS#5

【概要】

パスワードをベースにして秘密鍵を暗号化する方式を定めている。暗号化方法は"MD2 with DES-CBC"と" MD5 with DES-CBC"を定義している。

【動向】

1993 年 11 月 1 日にリリースされた Version 1.5 が現行バージョン。

4) PKCS#6

【概要】

拡張証明書のフォーマットを定義している。拡張証明書は 3つのパートからなっていて、(1) 拡張証明書の情報、(2) 署名アルゴリズムを特定する情報、(3)デジタル署名で構成されている。拡張証明書の情報には X.509 証明書と X.509 証明書で保証される公開鍵を持ったエンティティの情報で構成される。X.509 証明書の署名をした issuer と拡張証明書の署名をした issuer とは同一になる。

【動向】

1993 年 11 月 1 日にリリースされた Version 1.5 が現行バージョン。

【詳細】

例)拡張証明書のフォーマット

```
ExtendedCertificate ::= SEQUENCE {
   extendedCertificateInfo  ExtendedCertificateInfo,
   signatureAlgorithm  SignatureAlgorithmIdentifier,
   signature Signature }

SignatureAlgorithmIdentifier ::= AlgorithmIdentifier

Signature ::= BIT STRING

ExtendedCertificateInfo ::= SEQUENCE {
   version  Version,
   certificate  Certificate,
   attributes Attributes }

Version ::= INTEGER

Attributes ::= SET OF Attribute
```

5) PKCS#7

【概要】

S/MIME 用に鍵や証明書を扱えるようにした規格。デジタル署名やデジタル封書（暗号化）に利用される暗号データを定義している。再帰的な処理を可能にしているので、封書の中に封書を入れることや封書したデータに署名をつけることができる。また、署名した時刻など任意のデータを認証することも可能。証明書および CRL の配布方法も提供している。

【動向】

1993 年 11 月 1 日にリリースされた Version 1.5 が現行バージョン。Version 1.6 が「Bulletin」となっている。（1997 年 5 月 13 日）

【詳細】

例）署名データ

```
SignedData ::= SEQUENCE {
  version Version,
  digestAlgorithms DigestAlgorithmIdentifiers,
  contentInfo ContentInfo,
  certificates
    [0] IMPLICIT ExtendedCertificatesAndCertificates OPTIONAL,
  crls
    [1] IMPLICIT CertificateRevocationLists OPTIONAL,
  signerInfos SignerInfos }

DigestAlgorithmIdentifiers ::=
  SET OF DigestAlgorithmIdentifier

SignerInfos ::= SET OF SignerInfo
```

6) PKCS#8

【概要】

秘密鍵の情報のデータフォーマット、および秘密鍵の情報を暗号化した場合のデータフォーマットを定めている。秘密鍵の情報の暗号化にはパスワードベースの暗号化（PKCS#5 など）を用いる。

【動向】

現行は 1993 年 11 月 1 日にリリース（revised）された Version 1.2。

【詳細】

例 1）秘密鍵の情報

```
PrivateKeyInfo ::= SEQUENCE {
  version Version,
  privateKeyAlgorithm PrivateKeyAlgorithmIdentifier,
```

privateKey PrivateKey,
attributes [0] IMPLICIT Attributes OPTIONAL }

Version ::= INTEGER

PrivateKeyAlgorithmIdentifier ::= AlgorithmIdentifier

PrivateKey ::= OCTET STRING

Attributes ::= SET OF Attribute

例 2)暗号化された秘密鍵の情報

EncryptedPrivateKeyInfo ::= SEQUENCE {
encryptionAlgorithm EncryptionAlgorithmIdentifier,
encryptedData EncryptedData }

EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

EncryptedData ::= OCTET STRING

7) PKCS#9

【概要】

2つの追加 Object Class とPKCS#7, #8, #12, #15 で利用される属性型、マッチングルールを定義している。

【動向】

2000 年 2 月 25 日に公開されたV2.0 が現行のバージョン。その後、2003 年 1 月 31 日に修正がなされた。(1993 年にリリースされたV1.1 では PKCS #6, PKCS #7, PKCS #8, PKCS #10 で利用される属性型を定めたものであった)

【詳細】

例)オブジェクトクラス

pkcsEntity OBJECT-CLASS ::= {
SUBCLASS OF { top }
KIND auxiliary
MAY CONTAIN { PKCSEntityAttributeSet }
ID pkcs-9-oc-pkcsEntity
}

naturalPerson OBJECT-CLASS ::= {

```
        SUBCLASS OF     { top }
        KIND            auxiliary
        MAY CONTAIN     { NaturalPersonAttributeSet }
        ID              pkcs-9-oc-naturalPerson
    }
```

8) PKCS#10

【概要】

証明書を要求するときのフォーマットを定義している。要求は (1)証明書要求情報、 (2)署名アルゴリズム、 (3)証明書を要求するエンティティの署名で構成されており、証明書要求情報は名前、公開鍵、そのほかの情報で構成されている。

【動向】

現行は 2000 年 5 月 26 日にリリースされた Version 1.7。

【詳細】

例)証明書要求

```
CertificationRequest ::= SEQUENCE {
    certificationRequestInfo  CertificationRequestInfo,
    signatureAlgorithm  AlgorithmIdentifier{{ SignatureAlgorithms }},
    signature           BIT STRING
    }

CertificationRequestInfo ::= SEQUENCE {
    version INTEGER { v1(0) } (v1,...),
    subject Name,
    subjectPKInfo SubjectPublicKeyInfo{{ PKInfoAlgorithms }},
    attributes [0] Attributes{{ CRIAttributes }}
    }
```

9) PKCS#11

別章「PC 上で利用する標準」(小阪殿担当分)を参照のこと。

10) PKCS#12

【概要】

PKCS#7 証明書とPKCS#8 秘密鍵のファイル化を行ったものであり、ファイルへの Import/Export 時にファイルの暗号化を行える。 複数の証明書を格納する事ができ、自分の証明書の他、CA の証明書等を格納する。

【詳細】

例）

```
PKCS12BagSet BAG-TYPE ::= {
        keyBag |
        pkcs8ShroudedKeyBag |
        certBag |
        crlBag |
        secretBag |
        safeContentsBag,
        ... -- For future extensions
    }
```

11）PKCS#15

別章「IC カード内で利用する標準」（小阪殿担当分）を参照のこと。

12）PKCS の利用イメージ

PKI における本人確認において、PKCS の各パートが規定している部分を示す。ただし、秘密鍵を格納するときなどで IC カードを利用する場合は PKCS#11,PKCS#15 を利用する場合もある。

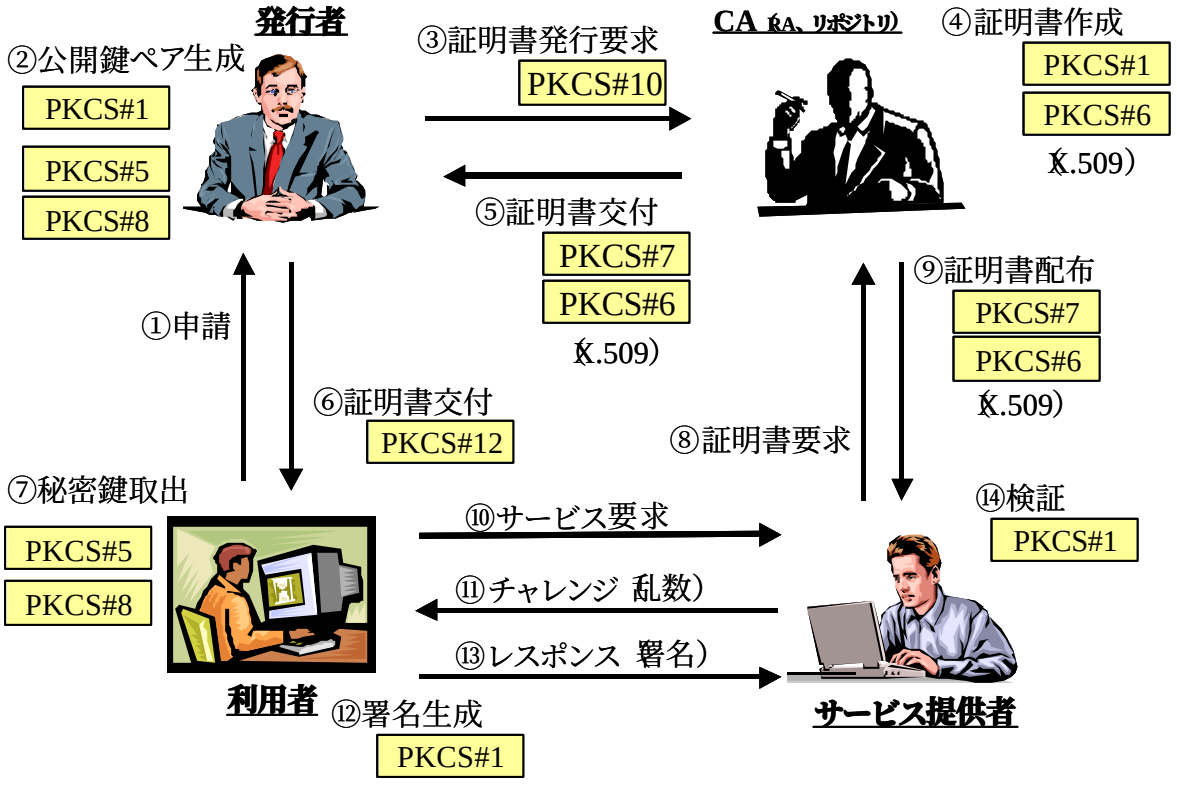


図 2 - 25 本人確認における PKCS の利用イメージ（発行者が公開鍵ペアを生成する場合）

①．申請

利用者が発行者に対して秘密鍵と公開鍵証明書の発行を申請する。

②. 公開鍵ペア生成

PKCS# 1をつかい、利用者の公開鍵ペアを生成する。秘密鍵のフォーマットは PKCS#8 を利用する。秘密鍵を暗号化する場合は PKCS#5 を利用する方法もある。

③. 証明書発行要求

PKCS#10 のフォーマットに従い、公開鍵証明書の交付を要求する。

④. 証明書生成

X.509 形式または PKCS#6 形式の公開鍵証明書を生成する。

⑤. 証明書交付

CA から利用者の証明書が交付される。この際、証明書の形式は X.509、PKCS#7、PKCS#6 が考えられる。

⑥. 証明書交付

発行者から利用者の証明書が交付される。ここでは公開鍵証明書に加えて秘密鍵も一緒に送信する必要があるため、PKCS#12 を利用する。ただし、証明書を IC カードに格納して証明書を交付する場合もある。

⑦. 秘密鍵取出

PKCS#12 形式で配布された証明書から秘密鍵を取得する。

⑧. 証明書要求

利用者の公開鍵証明書を取得する。（署名検証を行うより以前に行う必要がある）

⑨. 証明書配布

利用者の証明書が配布される。この際、証明書の形式は X.509、PKCS#7、PKCS#6 が考えられる。

⑩. サービス要求

サービス提供者にサービスを要求する。

⑪. チャレンジ

本人確認のため、利用者に対してチャレンジ（乱数）を送信する。

⑫. 署名生成

サービス提供者から送信された乱数に対して署名を生成する。

⑬. レスポンス

利用者が生成した署名をサービス提供者に送信する。

⑭. 検証

利用者の署名の検証、利用者の公開鍵証明書の検証を行う。

(13) PKI の派生モデル

1) Government PKI (GPKI)

【概要】

従来、国民等から行政機関に対する申請・届出等や行政機関から国民等への結果の通知等は、署名

又は記名押印した書面に行われるのが通常であった。しかし、インターネットを利用してこのやり取りを行う場合には、申請・届出等や結果の通知等が本当にその名義人(申請者や行政機関の処分権者)によって作成されたものか、申請書や通知文書の内容が改ざんされていないかを確認できなければならず、これを確認できるようにするための行政機関側の仕組みが政府認証基盤(GPKI：Government Public Key Infrastructure)である。

【動向】

日本国政府は、申請・届出等手続のオンライン化を推進するため、「行政情報化推進基本計画の改定について」(平成9年12月20日閣議決定)をはじめとして、累次の決定を行ってきた。「ミレニアム・プロジェクト(新しい千年紀プロジェクト)について」(平成11年12月19日内閣総理大臣決定)では、民間から政府、政府から民間への行政手続をインターネットを利用しペーパーレスで行える電子政府の基盤を構築することとし、また、「申請・届出等手続の電子化推進のための基本的枠組み」(平成12年3月31日行政情報システム各省庁連絡会議了承)においては、総務省、経済産業省及び国土交通省は先導的に府省認証局を、また総務省においてはこれらを相互に接続するブリッジ認証局を平成12年度(2000年度)中に整備することとした。さらに、高度情報通信ネットワーク社会推進戦略本部(IT戦略本部)において、高度情報通信ネットワーク社会形成基本法(IT基本法)に基づく「e-Japan重点計画」(平成13年3月29日IT戦略本部)や「e-Japan重点計画-2002」(平成14年6月18日IT戦略本部)が策定され、平成14年度(2002年度)までに全府省において府省認証局を整備するこが決定された。

一方、民間側の認証基盤については、総務省、法務省及び経済産業省において電子署名・認証に関する法制度の整備を図り、「電子署名及び認証業務に関する法律」(平成12年法律第102号)が成立した。これにより電子署名が手書きの署名や押印と同等に通用する法的基盤が整備された。また、この法律で、認証業務のうち一定の水準を充たすものは、国の認定を受けることができる制度が導入された。また、法務省においては、商業登記法その他の関係法令等に基づき、平成12年10月から、法人代表者に電子証明書を発行する商業登記制度に基礎を置く電子認証システムの運用を行っている。

(14) 今後のPKIの動向

1) PKI関連のその他の動向

(a) 日本ネットワークセキュリティ協会のChallenge PKI 2002

Challenge PKI 2002は、GPKI/LGPKI/公的個人認証基盤などのPKIアプリケーションの相互運用性の確保を支援するためのフレームワークの確立を目指したプロジェクトである。プロジェクトの成果は55th-IETF等で発表されており、今後は成果を活かしたRFC作成も検討しているとのこと。

(b) OASIS PKI Technical Committeeによる"PKI Action Plan prepared and published by OASIS PKI Technical Committee"

【概要】

ビジネスにおける情報交換用技術標準を作成する国際的な団体であるOASIS (Organization for the Advancement of Structured Information Standards)のPKI技術委員会がPKI対応のアプリケーション不足や相互運用可能性の問題等を克服するためにPKIアクションプラン構築した。

【動向】
2003 年 11 月に Ver0.4 ドラフトが公開されて今に至る。
【詳細】
調査を通して

- ソフトウェアアプリケーションが PKI をサポートしていない
- コストが高すぎる
- PKI の理解不足
- 技術に注目しすぎて、ニーズに応えていない
- 相互運用可能性が貧弱である

という5つの問題点を明確化して、その各問題点に対するアクションプランを立てて実行していく。

- UTCTIME :日時を表す。西暦を下 2 桁で表現する。
- Generalized Time :日時を表す。西暦を 4 桁で表現する

(15) ANS.1

1) 概要

ASN.1 とは Abstract Syntax Notation One の略であり、情報構造の記述規則である。この記法を用いることにより、X.509 公開鍵証明書、CRL、PKCS#7、#10、#12、OCSP 等のデータ形式に用いられている。

2) 動向

1998 年に国際電信電話諮問委員会（CCITT ;現在の ITU-T）から"CCITT Recommendation X.208：Specification of Abstract Syntax Notation One,1988"
が勧告された。その後に記述方法が拡張されて、1997 年に ITU-T から"ITU-T Recommendation X.680 (1997)"が勧告され、1998 年に ISO/IEC から"8824-1:1998,Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation "が公開された。

現在は、1998 年版に対して最近の動向に合わせた新しい符号化規則，すなわち符号化制御記法（Encoding Control Notation，ECN）及び XML を使った符号化規則（XML Encoding Rule (XER)），の追加などを取り込んだ新たな ASN.1 の版を IS 化する作業が進んでおり IS 化が承認された段階である。JIS 化も検討されている。

また、通信データ記述への XML 利用の拡大に対応するために XML スキーマとの関係を 1998 年版に対して整理することも行われており、上述の IS に対するアメンドメントという形式で作業が進められている. 具体的には，XML スキーマと等価な記述ができること（これを ASN.1 スキーマと呼ぶこともある）及びそれに合わせた XER の細かい指定方法が検討されている. 現時点では WD だが，ITU-T を中心に精力的な作業が行われている。

3) 詳細

ASN.1 のデータは、「識別子」「データ長」「値」の順で並べられる。データ構造はネストすることも可能であり、ネストする場合、値にはさらに「識別子」「データ長」「値」のフィールドが入る。

- 識別子 :値に含まれるデータの種別を指定する。これは規定される範囲を示すクラス部と、データ型を示すタグ部に細分化される。
- データ長 :値に含まれるデータの長さを指定する
- 値 :データの内容が記述される

4) ASN.1 の基本的なデータ型

以下に ASN.1 の基本的なデータ型を示す。

- BOOLEAN :真(True)と偽(False)の値を表現する。
- INTEGER :任意の長さの整数を表す。
- BITSTRING :任意の長さのバイト列を表す。
- OBJECT IDENTIFIER (OID) :基本データ型以外のいろいろなもの (データの名称、アルゴリズム ID、X.509 証明書エクステンション名、X.509 証明書 policyQualifierlds、プロトコル名、証明書ポリシー名など)を、階層化された番号の並びで表現する。

例) X.509 エクステンション名である subjectAltName は以下のように表現される。

{ 2 5 29 7}

アルゴリズム ID 名 sha1withRSAEncryption は以下のように表現される。

{ 1 2 840 113549 1 1 5 }

- SEQUNCE :いくつかのデータの並び (シーケンス)を表す。
- SET :いくつかのデータの集合 (セット)を表す。
- PrintableString :印字可能な文字列を表す。
- T61String :ASCII を 8 ビットに拡張した、T.61 文字列を表す。
- IA5String :ASCII 文字列を表す。

１．７．３ IC カード

バイオメトリクス認証において IC カードは生体情報のテンプレートを格納する場所などの利用方法がある。バイオメトリクス認証で利用される IC カードには以下の 3 種類がある。

- テンプレートの格納のみ行う IC カード（STOC:Store on Card / Off-Card Matching 等）
- テンプレートの照合を内部で行う IC カード（MOC:Match on Card / On-Card Matching）
- 生体情報の取得、テンプレートの格納、照合まですべてを行う IC カード（All on Card）

生体情報の取得からデータ照合までのバイオメトリクス認証を行う場合の処理のうち、それぞれの IC カードが担当する処理の範囲を「図 2 - 26 バイオメトリクス認証で利用される IC カードが行う処理内容」に示す。

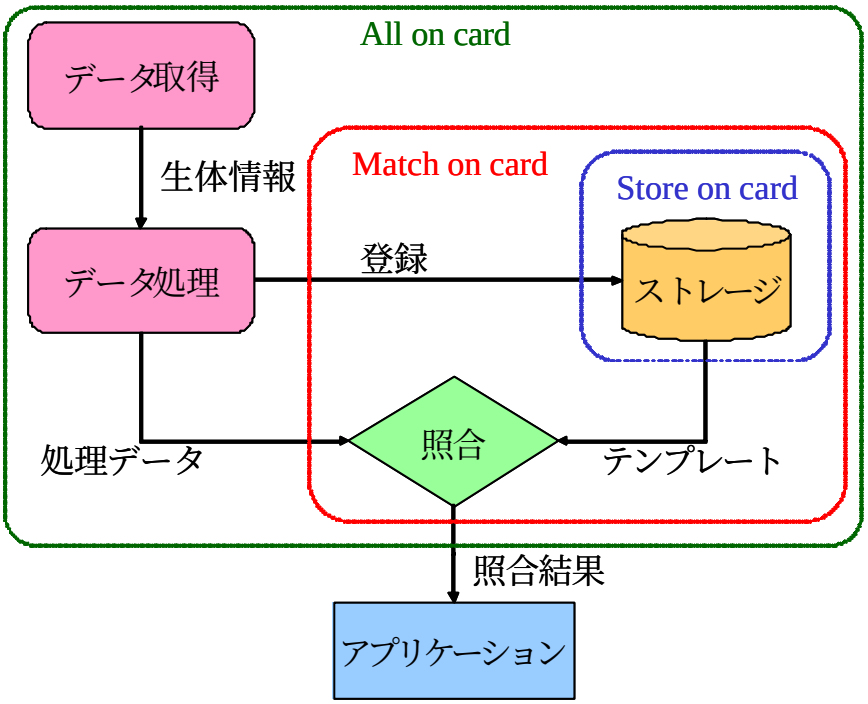


図 2 - 26 バイオメトリクス認証で利用される IC カードが行う処理内容

IC カード関連の標準・技術には、カードの内部にテンプレートを格納する際のフォーマットを定義しているもの（ISO/IEC 7816-15・PKCS #15）、カードに対してテンプレートを送信する際のフォーマットを定義したもの（ISO/IEC 7816-11）、カード内照合に関連したもの（ISO/IEC 7816-11、Java Card Biometirc API）と、バイオメトリクス認証と関連のある標準も存在する。本節では、バイオメトリクス認証とかかわりのあるものに限定することなく、IC カード関連の ISO を審議している委員会、IC カードに関連する標準および技術について記述する。

(1) ISO/IEC JTC1/ SC17

【概要】

カードおよび個人識別（Cards and Personal identification）に関する検討を行っているSub Committee。磁気カード、外部端子付きIC カード、非接触IC カード、光カードの技術標準とパスポート アプリケーションの登録、金融取引カード、運転免許証のアプリケーション関連の標準化が行われている。

【詳細】

2004 年 2 月現在、SC17 には 9 つの WG があり、それぞれ以下の内容を審議している。

表 2 - 22 WG 一覧

WG 名称	タイトル名	概要
WG1	PHYSICAL CHARACTERISTICS AND TEST METHODS FOR IDENTIFICATION CARDS	IDカードの物理特性と試験方法
WG3	MACHINE READABLE TRAVEL DOCUMENTS	機械可読旅行文書
WG4	INTEGRATED CIRCUIT CARDS WITH CONTACTS	接触型 IC カード
WG5	REGISTRATION MANAGEMENT GROUP	カード発行者付番体系と様式
WG7	FINANCIAL TRANSACTION CARDS THIS WORKING GROUP HAS BEEN STOOD DOWN	金融取引カード
WG8	CONTACTLESS INTEGRATED CIRCUIT(S) CARDS, RELATED DEVICES AND INTERFACES	非接触型 IC カード
WG9	OPTICAL MEMORY CARDS AND DEVICES	光メモリカードとデバイス
WG10	MOTOR VEHICLE DRIVER LICENCE AND RELATED DOCUMENTS	運転免許証と関連文書
WG11	BIOMETRICS	バイオメトリクス

（http://www.sc17.com/ による）

以下、各 WG で審議している内容について解説を行う。

1) SC17/WG1

【概要】

ID カードの物理特性、試験方法等に関する案件を審議している。対象は ISO/IEC 10373 Part 1 （テスト方法の全体仕様）, Part 2 （磁気ストライプカードのテスト方法）、ISO/IEC 7810 （識別カード―物理特性）、ISO/IEC 7811 Part 1, 2, 6, 7 （識別カード―記録技術）、ISO/IEC 15457 Part 1, 2, 3 （搭乗券・定期券用の薄型カード）。

2) SC17/WG3

【概要】

機械可読旅行文書（Machine Readable Travel Document)およびカードについて審議している。パスポート

は機械可読旅行文書の一部。対象は ISO/IEC 7501（機械可読旅行文書）。

3) SC17/WG4

【概要】

接触型 IC カードに関する標準化活動を行っている。2004 年 2 月現在、GSC-IS（詳細は「(10) Government Smart Card - Interoperability Specification (GSC-IS)」を参照）の ISO 化に関しても審議が進められている。対象となるISO は ISO/IEC 7816 part 1 - 12、ISO/IEC 7816 part 15、ISO/IEC 10373 part 3（外部端子付きIC カードのテスト方法）、ISO/IEC 20060（カード端末等に関する技術標準）。

4) SC17/WG5

【概要】

カード発行者番号システム(Registration Management Group) について審議している。対象は ISO/IEC 7812（カード発行者付番体系および登録管理様式）とISO/IEC 7816-5。

表 2 - 23 ISO 7812 の一覧

パート	タイトル	タイトル訳	公開日 (Stage date)
Part 1	Identification cards -- Identification of issuers -- Part 1: Numbering system	カード発行者付番体系	2003-10-14
Part 2	Identification cards -- Identification of issuers -- Part 2: Application and registration procedures	カード発行者のアプリケーションと申請登録手続き	2003-10-14

5) SC17/WG７

【概要】

ISO/IEC 7813（金融取引カード）の修正を行っている。対象とするISO は ISO/IEC 7813。

6) SC17/WG8

【概要】

非接触 IC カードに関して審議を行っている。通信距離に応じてタスクフォースが分かれており、ISO も異なっている。審議対象としている非接触型 IC カードの種類および、対象となる ISO は以下のとおりである。

表 2 - 24 WG8 で審議している非接触型 IC カードの種類

英語表記	略語	日本語	ISO/IEC	審議組織	参考通信距離

Proximity	PICC	近接型	14443	WG8/TF2	10 cm
Vicinity	VICC	近傍型	15693	WG8/TF3	70 cm

密接型の非接触IC カード（英語表記：Close-coupled、通信距離：2mm）について審議をしていたTF1は、1995 年に ISO/IEC 10536-4 の CD が設立の後に解散している。

7） SC17/WG9

【概要】

大容量、高速アクセス、高信頼性を可能にした光メモリーカード（OMC）に関する審議を行っている。OMC に格納されているデータにアクセスするためのインターフェース、OMC の物理的、論理的メモリ割り当て、メモリ内のデータ構造を審議している。対象は ISO/IEC 11693（光カードのサイズや対環境特性）、ISO/IEC 11694（記録方式など）。

8） SC17/WG10

【概要】

運転免許証及び関連する資料に関する国際標準化活動を行っている。運転免許証製作上の技術的項目に関して国際標準化を行い、関連官庁へ提示することを目的としている。対象は ISO/IEC 18013-1（カードの国際互換データセット）, ISO/IEC 18013-2（データ要素の技術相関性）, ISO/IEC 18013-3（バイオメトリクスと暗号化）。

表 2 - 25 ISO18013（運転免許および関連する書類）の現状

パート	タイトル	タイトル訳	状態	日付
Part 1	Model Data Element Set	カードの国際互換データセット	CD	2002-10-18
Part 2	Data Element Mapping of Technologies	データ要素の技術相関性	AWI	2003-03-01
Part 3	Biometrics and Encryption	バイオメトリクスと暗号化	AWI	2003-03-01

9） SC17/WG11

【概要】

バイオメトリクスについて審議を行っている。標準化の対象範囲は「個人識別技術（例えば生体識別）を使用する産業間及び政府利用業務への相互運用性」であり、SC 37 で審議されている総括的な生体識別については対象外である。ISO/IEC 19771 の担当が WG11 から WG3 に移行された。2004 年 4 月 1 日まで

に新たな提案がない場合、WG11 は閉鎖される。

⑵ ISO/IEC 7816

【概要】

接触型 IC カードの国際標準規格。物理的特性、端子の寸法および位置、電気特性及び伝送プロトコル、共通コマンドなどが定義されている。1から15 までのパートに分かれており、策定中のものもある。以下、タイトルの一覧を示す。

表 2 - 26 ISO/IEC 7816 タイトル一覧

パート	英文タイトル	日本語タイトル
Part 1	Physical characteristics	物理特性
Part 2	Dimensions and location of the contacts	外部端子の寸法及び位置
Part 3	Electronic signals and transmission protocols	電子信号と転送プロトコル
Part 4	Interindustry commands for interchange	共通コマンド
Part 5	Numbering system and registration procedure for application identifiers.	アプリケーション識別子のナンバリングシステム及び登録
Part 6	Interindustry data elements	共通データ要素
Part 7	Interindustry commands for Structured Card Query Language (SCQL)	構造化カード照会言語(SCQL)用共通コマンド
Part 8	Security related interindustry commands	セキュリティ関連共通コマンド
Part 9	Additional interindustry commands and security attributes	追加共通コマンド及びセキュリティ属性
Part 10	Electronic signals and answer to reset for synchronous cards	同期カード用電子信号及び初期応答（正誤票を含む）
*Part 11	Personal verification through biometric methods	バイオメトリクスによる個人認証
*Part 12	USB electrical interface and operating procedures	USB インターフェースとオペレーション処理
*Part 13	Registration of integrated circuit manufacturers	IC 製造者の登録
Part 15	Cryptographic information application	暗号情報アプリケーション

（part 14 は利用されていない。*印は策定中であることを示す。）

ISO 7816 は接触型特有のものと物理特性に依存しないものの大きく2 つに分類できる。それぞれのパートを分類すると以下のようになる。

表 2 - 27 ISO7816 の分類

分類	パート

接触型特有のパート	ISO7816-1, ISO7816-2, ISO7816-3, ISO7816-10, ISO7816-12
物理特性に依存しないパート	ISO7816-4, ISO7816-5, ISO7816-6, ISO7816-7, ISO7816-8, ISO7816-9, ISO7816-11, ISO7816-13, ISO7816-15

物理特性に依存しないパートについては接触型 IC カード以外にも非接触型 IC カードが準拠する場合もある。以下、パートごとに解説をする。

1) ISO/IEC 7816-1

【概要】

カード面に IC の外部端子をもつ IC カードの物理的特性について規定する。

【動向】

2004 年 2 月現在、1998 年リリースが最新版。2003 年に補足が発表されている。

2) ISO/IEC 7816-2

【概要】

カード面に IC の外部端子をもつ IC カードの外部端子の寸法及び位置について規定する。

【動向】

2004 年 2 月現在、1999 年リリースが最新版。

3) ISO/IEC 7816-3

【概要】

電力, 信号構成及び IC カードと端末機などの接続装置との間の情報交換について規定。信号の速度, 電圧値, 電流値, パリティ規約, 動作手順, 伝送機構及び IC カードによる通信も含まれる。

【動向】

2004 年 2 月現在、1997 年にリリースが最新版。2002 年に補足が発表されている。2003 年 4 月 1 日に出された CD の投票結果が 2003 年 8 月 5 日に出ている。

【詳細】

(伝送プロトコル)

ISO/IEC 7816-3 では IC カードと通信を行う際のプロトコルが記載されている。本節では IC カードの伝送プロトコルの中で代表的な T=0 と T=1 のプロトコルについて解説**をする**。

1. T=0 プロトコル (Half-duplex transmission of asynchronous characters)

バイト単位で構成されていて、最小プロトコルが1バイト。伝送データにはヘッダーがついており、命令バイトと3つのパラメータバイトから成り立つ。そのあとにデータバイトが続く。

2. T=1 プロトコル (Half-duplex transmission of blocks)

ブロック単位のプロトコル。ブロック構成を以下に示す。

表 2 - 28 T=1 プロトコルにおけるデータのブロック構成

フィールド	種類	データ長
先頭フィールド	ノードアドレス	1byte
	プロトコル制御	1byte
	データ長	1byte
情報フィールド	APDU	0～254 byte
最終フィールド	EDC	1～2 byte

4) ISO/IEC 7816-4

【概要】

物理特性に依存しない形式で、IC カード内のアプリケーションの基本的な仕様を規定している。ISO/IEC 7816-4 で記述されている項目は以下のとおりである。

- 接続装置とICカードとの間で伝送されるメッセージ, コマンド及びレスポンスの内容
- 初期応答の際にICカードから送信される管理情報バイトの構造及び内容
- 共通コマンドを実行する際に, インターフェースに表現されるファイル及びデータの構成
- ICカード内のファイル及びデータへのアクセス方法
- ICカード内のファイル及びデータへのアクセス権を規定するセキュリティアーキテクチャ
- セキュアメッセージの方法
- カードによって処理されるアルゴリズムのアクセス方法

【動向】

2004 年 2 月現在、1995 年リリースされたものが現行のバージョン。1997 年に補足が発表されている。2003 年 9 月 30 日に FCD が SC17/WG 4で作成され、2004 年 1 月 30 日で投票が締め切られている。なお、審議中の FCD では現行の ISO/IEC 7816-4 で規定されているコマンドに加え、現行の ISO/IEC 7816-8 で規定されているコマンドの一部が追加されている。

【詳細】

本報告書では 1995 年にリリースされたものに基づき、ファイル構成、コマンドおよびレスポンスの内容、規定コマンドについて解説をする。

（ファイル構成）

IC カード内部の階層的なファイル構成の例を「図 2 - 27 IC カード内部のファイル構成」に示す。「図 2 - 27 IC カード内部のファイル構成」では最上位に MF があり、以下 DF が階層的にある。EF はそれぞれのディレクトリ（MF または DF）の下に配置される。

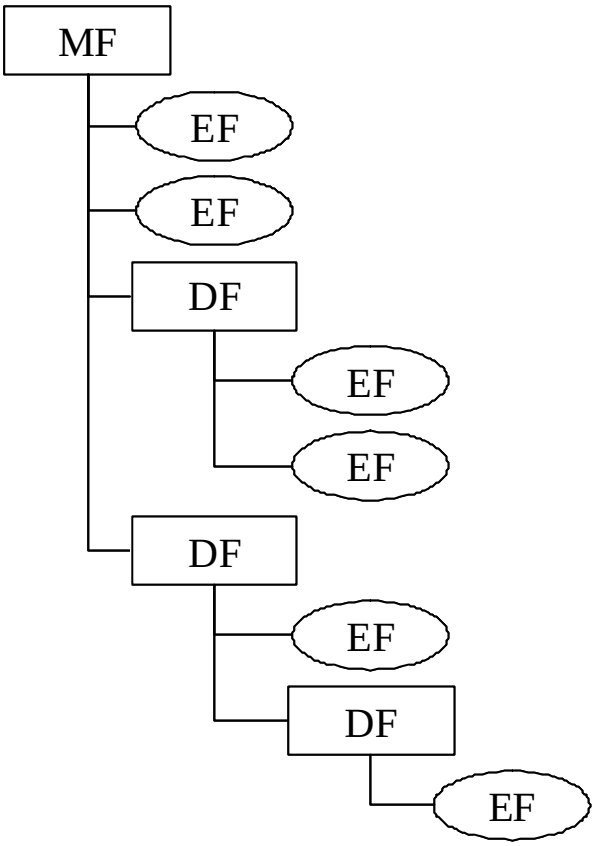


図 2 - 27 IC カード内部のファイル構成例

表 2 - 29 「図 2 - 27 IC カード内部のファイル構成」内の用語

用語	説明
MF	Master File。ルートディレクトリに相当する。
DF	Dedicate File。MF に従属し、ディレクトリに相当する。
EF	Elementary File。データを格納する領域。ファイルに相当する。

（コマンドおよびレスポンスの内容）

PC に搭載されているアプリケーションと IC カード内のアプリケーションとの間では APDU（application protocol data unit）を使って通信を行う。アプリケーションから送信されるAPDU をコマンドAPDU、IC カードから返されるAPDU をレスポンスAPDU と呼ぶ。コマンドAPDU およびレスポンスAPDU の仕様をそれぞれ「表 2 - 30 コマンドAPDU の構造」、「表 2 - 31 レスポンスAPDU の構造」に示す。コマンドAPDU は大きくコマンドヘッダフィールド、Lc フィールド、データフィールド、Le フィールドの 4つに別れており、コマンドヘッダフィールドは必須である。レスポンス APDU はデータフィールドとステータスフィールドがあり、ステータスフィールドは必須である。ステータスフィールドにはコマンドAPDU の実行結果が格納される。

表 2 - 30 コマンドAPDU の構造

フィールド	説明	長さ	備考
コマンドヘッダ	CLA :クラスバイト	1 byte	必須
	INS :命令バイト	1 byte	必須
	P1、P2 :パラメータ	1 byte	必須
Lc	Lc :コマンドデータ長	0, 1, 3byte	コマンドデータのバイト数
データ	Data :コマンドデータ	可変	コマンドデータがあるときのみ
Le	Le :レスポンスデータ長	3byte 以下	予想されるレスポンスデータの最大の長さ

表 2 - 31 レスポンス APDU の構造

フィールド	説明	長さ	備考
データ	Data :レスポンスデータ	可変 (最大 Le)	レスポンスデータがあるときのみ
ステータス	SW1、SW2 :ステータスコード	2 byte	APDU の実行結果を格納。必須。

（コマンド一覧）

ISO 7816-4 では IC カードを利用する際の基本的なコマンドを規定している。ISO/IEC 7816-4 で規定されているコマンドの一覧を 表 2 - 32 ISO/IEC 7816-4 で規定されているコマンド一覧」に示す。

表 2 - 32 ISO/IEC 7816-4 で規定されているコマンド一覧

コマンド名称	処理概要
READ BINARY	EF のデータを読み取る。
WRITE BINARY	EF のデータを書き換える。送信データに書き換える場合、送信データと論理和をとる場合、論理積をとる場合の 3 種類ある。
UPDATE BINARY	EF 内のデータを更新する。
ERASE BINARY	EF 内のデータを消去された状態にする。
READ RECODE	レコードを読み取る。

WRITE RECODE	レコードを書き換える。送信データに書き換える場合、送信データと論理和をとる場合、論理積をとる場合の 3 種類ある。
UPDATE RECODE	レコードを更新する。
APPLEND RECODE	レコードに新しいレコードを追記する。
ERASE RECODE	レコードのデータを消去された状態にする。
GET DATA	データオブジェクトを読み取る。セキュリティ条件が満たされている場合のみ、利用可能。
PUT DATA	データオブジェクトを書き換える。セキュリティ条件が満たされている場合のみ、利用可能。
SELECT FILE	論理チャンネルを開く。
VERIFY	(パスワードなどの)認証データをカードに送信し、カード内で照合する。このコマンドが成功した後、カード内の機能が利用可能になる。
INTERNAL AUTHENTICATE	外部 Entity がカードを認証する。
EXTERNAL AUTHENTICATE	GET CHALLENGE で取得した情報を基にして、カードが外部 Entity を認証する。GET CHALLENGE の後に実行される。
GET CHALLENGE	カードが外部 Entity を認証するために必要な情報（例．乱数）をカードから取得する。
MANAGE CHANNEL	論理チャンネルの管理（Open または Close）を行う。
GET RESPONSE	利用可能な送信プロトコルによってレスポンス APDU を送信する。
ENVELOPE	利用可能な送信プロトコルによって、コマンドAPDU または BER-TLV 形式のデータを送信する。

5) ISO/IEC 7816-5

【概要】

外部端子付きICカードのアプリケーション識別子の付番システム及びアプリケーション提供者識別子の登録手続について規定。付番システムは，与えられたカードがアプリケーション，又はそれに関連したサービスが必要とする要素を含む場合，カード提供者によって行われたそれらの識別のための手段を提供している。

【動向】

2004 年 2 月現在、1994 年リースが最新版。1995 年に補足が発表されている。2003 年 1 月 17 日に出された FCD の投票結果が 2003 年 5 月 22 日に出されている。

6) ISO/IEC 7816-6

【概要】

ICカードを基盤として共通に交換される合成データ要素を含む各種データ要素を規定。データ要素には識別子、名称、説明または参照、フォーマットが含まれる。Biometric information template、biometric data template などのデータ要素も定義されている。これらのデータの詳細は ISO 7816-11 を参照。

【動向】

2004 年 2 月現在、1996 年にリリースされたものが現行のバージョン。1998、2000 年に補足が発表されている。2003 年 1 月 17 日に出された FCD の投票結果が 2003 年 5 月 22 日に出されている。

7) ISO/IEC 7816-7

【概要】

IC カードをデータベースとして見立てた際に IC カードに対して発行する命令、Structured Card Query Language (SCQL) について規定している。

【動向】

2004 年 2 月現在、1999 年 3 月 11 日に公開されたものが現行バージョン。現在、SCQL を拡張した ESCQL について策定が進められている。

8) ISO/IEC 7816-8

【概要】

IC カードのセキュリティに関する事項について、以下の内容を規定している。

- カード用セキュリティプロトコル
- セキュアメッセージング拡張機能
- カードのセキュリティ機能/サービスに対するカードのセキュリティ機構のマッピング (カード内のセキュリティ機能の記述も含む)
- セキュリティ支援のためのデータ要素
- カードに実装されたアルゴリズムの使用方法 (アルゴリズム自身の詳細の規定はしない)
- 認証書の使用方法
- セキュリティに関連するコマンド

【動向】

2004 年 2 月現在、1999 年にリリースされたものが最新バージョン。2003 年 01 月 17 日に FCD が出され、その投票結果が 2003 年 5 月 22 日に出されている。

【詳細】

規定コマンド)

ISO/IEC 7816-8 では ISO/IEC 7816-4 で規定されているコマンド以外にセキュリティに関連したコマンドが幾つか規定されている。ISO/IEC 7816-8 で規定しているコマンドの一覧を以下に示す。

表 2 - 33 ISO/IEC 7816 -8 で規定されているコマンド一覧

コマンド名称	概要
MANAGE SECURITY ENVIRONMENT	セキュリティ環境の管理（設定、置き換え、保存、消去）および、暗号コマンドの初期化を行う。
PREFORM SECURITY OPERATION	暗号 CHECKSUM の計算、デジタル署名の計算、Hash コードの計算、暗号 CHECKSUM の検証、デジタル署名の検証、証明書の検証、暗号化、復号といったセキュリティ処理を行う。
CHANGE REFERENCE DATA	（PIN などの）カード内の参照データを変更する。
ENABLE VERIFICATION REQUIREMENT	照合データと参照データの比較を可能にする。セキュリティ状態が満たされている場合にのみ実行可能である。
DISABLE VERIFICATION REQUIREMENT	照合データと参照データの比較を不可能にする。セキュリティ状態が満たされている場合にのみ実行可能である。
RESET RETRY COUNTER	照合の失敗回数をリセットする。セキュリティ状態が満たされている場合にのみ実行可能である。
GENERATE PUBLIC KEY PAIR	公開鍵を生成し、IC カード内に保存する。ただし、このコマンドの実行前に、鍵のパラメータの設定のために、MANAGE SECURITY ENVIRONMENT コマンドが実行される。セキュリティ状態が満たされている場合にのみ実行可能である。
MUTUAL AUTHENTICATE	INTERNAL AUTHENTICATE コマンドおよび EXTERNAL AUTHENTICATE コマンドの両方の機能をもつ（ISO/IEC 9798 -2, 3 で記述されている認証を行う場合に利用する）。セキュリティ状態が満たされている場合にのみ実行可能である。

9) ISO/IEC 7816-9

【概要】

カード関連オブジェクトのライフサイクルの記述及び符号化，カード関連オブジェクトのセキュリティ属性の記述及び符号化，追加共通コマンドの機能及び形式，これらのコマンドに関連付けられたデータ要素，並びにカード発信メッセージ初期化機構を規定。

【動向】

2004 年 2 月現在、2000 年にリリースされたものが現行のバージョン。2003 年 01 月 17 日に FCD が出され、その投票結果が 2003 年 05 月 22 日に出されている。

10) ISO/IEC 7816-10

【概要】

IC カードと端末間の電子信号と初期応答（ATR）の構造について規定。また、信号レート・IC カードと端末の通信についても記述。ISO 7816 -3 を一部参照している。

【動向】
2004 年 2 月現在、1999 年 11 月 4 日リリースが最新。その後、特に動きはない。

11）ISO/IEC 7816-11

【概要】
カード内でバイオメトリクス認証を行うために必要なコマンド、格納するバイオメトリクスデータ要素など，カード内照合（Match on Card）に関する規格。バイオメトリクス認証自体は対象としない。

【動向】
2003 年 9 年 3 日 に FDIS が出され、現在投票中。2004 年 2 月 18 日が期限である。

【詳細】
本節では ISO7816-11 で規定されている認証コマンドおよびデータ要素について解説をする。

（認証コマンド）
バイオメトリクスによる認証には ISO/IEC 7816-4 で定義されている VERFIY コマンドを利用する。また、ダイナミックな認証（キーストロークによる認証など）を行う場合は、GET CHALLENGE コマンドを使いチャレンジデータを取得した後、VERFIY コマンドによって認証する。

（データ要素）
ISO7816-11 で規定しているデータは 2 種類 Biometric Infomation と Biometric data の 2 種類ある。それぞれの内容は以下のとおりである。

1. Biometric Information

Biometric Information は Biometric data に関連する情報を記述したものである。Biometric Information の中には ISO7816-11 で規定されたデータオブジェクトを利用してもよいし、CBEFF などのほかの標準で規定したデータオブジェクトも利用できるようになっている。Biometric Information のテンプレートを以下に示す。

表 2 - 34 Biometric Information

タグ	長さ	値			備考
7F60	可変	バイオメトリクス情報テンプレート（BIT）			
		タグ	長さ	値	
		80	1	コマンドで利用するアルゴリズム	オプション
		83	1	コマンドで利用するリファレンスデータ	オプション
		A0	可変	ISO7816-11 で定義している Biometric Information データオブジェクト	オプション
		06	可変	オブジェクト識別子（ISO 7816-4 参照）	A1 がない場合、少なくとも1つが必要
		41	可変	国コード、および国情報（ISO 7816-4 参照）	
		42	可変	カード製造者（ISO 7816-4 参照）	

		4F	可変	アプリケーション識別子(ISO7816-5 参照)			
		A1	可変	Biometric Information データオブジェクト			A0がない場合、必須
				タグ	**長さ**	**値**	
				―	―	データオブジェクト（CBEFF などで定義されているものなど）	DO に依存

表 2 - 34 Biometric Information」内の' A1'に 7816-11 で規定してないデータオブジェクト（例えば CBEFF で規定されたデータオブジェクト）を格納することが可能である。また、複数の Biometric Information を扱う場合は Biometric Information Group を利用し、以下のような要素で構成される。

表 2 - 35 Biometric Information Group

タグ	**長さ**	**値**			**備考**
7F61	可変	BIT グループテンプレート			
		タグ	**長さ**	**値**	
		B1	可変	バイオメトリクス情報テンプレート1（BIT1）	必須
				・・・	
		B2	可変	バイオメトリクス情報テンプレート2（BIT2）	オプション
				・・・	
		B3	可変	バイオメトリクス情報テンプレート3（BIT3）	オプション
				・・・	
		・・・	・・・	・・・	

2. Biometric Data

Biometric data はバイオメトリクス認証を行うために必要な特徴などを抽出したデータであり、以下の要素が含まれる。

表 2 - 36 Biometric data

タグ	長さ	値			備考
5F2E	可変	Biometric data			
7F2E	可変	Biometric data template			
		タグ	長さ	値	
		5F2E	可変	Biometric data	少なくとも 1 つは必要
		81 / A1	可変	標準的なデータ	
		82 / A2	可変	照合アルゴリズム固有のデータ	

12) ISO/IEC 7816-12

【概要】

IC チップの USB インターフェースとオペレーション処理を規定している。

【動向】

2003 年 12 月 16 日に ISO/IEC CD 7816-12 が公開され、2004 年 2 月現在、投票中。期限は 2004 年 3 月 16 日となっている。

13) ISO/IEC 7816-13

【概要】

IC 製造者の登録について規定している。もとは ISO/IEC 7816-6/AMD1 のチップ製造者登録であったが、移行されて策定が開始された。参考までに、東芝は'0C'である。

【動向】

2002 年 1 月 21 日に ISO/IEC CD 7816-13 が公開されている。2004 年 2 月現在、この CD が最新。

14) ISO/IEC 7816-15

【概要】

プラットフォームに依存せず、また、既存の標準と矛盾しない形でカードに搭載する暗号機能をもったアプリケーションの仕様について規定している。ISO 7816 -15 は PKCS#15 v1.1 がベースになって策定され、PKCS #15 との関係は以下のとおりである。

- コアな部分では共通である。
- PKCS #15 において、IC カードに関係しない部分は削除している。
- IC カードの要求仕様を含めた仕様を追加している。

【動向】

2004 年 1 月 6 日に策定。JIS 化もされている。

【詳細】

PKCS#15 がベースになって策定され、カードに搭載する暗号機能をもったアプリケーションの仕様および cryptographic information のデータフォーマット、メカニズムを規定している。ISO/IEC 7816-15 では以下の項目をサポートしている。

- カード内に暗号情報のインスタンスを複数もつ
- 暗号情報の利用
- 暗号情報の訂正
- ISO7816 で定義されているデータオブジェクトと暗号情報の関連
- 異なる認証方式
- 複数の暗号アルゴリズム

⑶ ISO/IEC 14443

【概要】

近接型非接触 IC カードの国際標準規格。周波数が 13.56MHz、通信距離が 10cm 程度の非接触 IC カードを対象にしており SC17/WG8 にて標準化が進められている。タイプ A・B の 2 種類があり、日本ではタイプ A が IC テレホンカードに、タイプ B が住民基本台帳カードに利用されている。ISO/IEC 14443 のタイトル一覧を 表 2 - 37 ISO/IEC 14443 タイトル一覧」に示す。

表 2 - 37 ISO/IEC 14443 タイトル一覧

パート	英文タイトル	日本語タイトル
Part 1	Physical characteristics	物理特性
Part 2	Radio frequency power and signal interface	高周波出力及び信号インターフェース
Part 3	Initialization and anticollision	初期設定及び衝突防止
Part 4	Transmission protocol	伝送プロトコル

1) ISO/IEC 14443-1

【概要】

近接型非接触 IC カードの物理特性を規定している。ISO/IEC 7810 の ID-1 タイプのカードの物理特性を持つことおよび、紫外線・X 線を照射しても動作を保障するなどの追加物理特性が規定されている。

【動向】

2004 年 2 月現在、2003 年 10 月 13 日に公開されたバージョンが最新。

2) ISO/IEC 14443-2

【概要】

デバイスとカード間で通信を行うためのフィールドの特性を規定。周波数、電力、タイプ A・B それぞれの信号インターフェースなどが定められている。

【動向】

2004 年 2 月現在、2001 年 6 月 28 日に公開されたバージョンが最新。その後、ISO/IEC 14443-2:2001/AWI Amd 1 が 2002 年 10 月 4 日に、ISO/IEC 14443-2:2001/CD Amd 2 が 2003 年 7 月 28 日に公開されている。

3) ISO/IEC 14443-3

【概要】

IC カードとデバイス間で通信を行う際の初期化および衝突防止（アンチコリジョン）について規定している。規定項目は以下のとおり。

- IC カードの特定（polling）
- 初期通信におけるバイトフォーマット・フレーム・タイミング
- 初期要求および ATR
- アンチコリジョン
- 初期通信時のパラメータ
- IC カードを特定する簡単でかつ迅速な方法

【動向】

2004 年 4 月現在、2001 年 2 月 1 日にリリースされたものが最新。その後、ISO/IEC 14443-3:2001/CD Amd 1 が 2003 年 7 月 29 日に公開されている。

4) ISO/IEC 14443-4

【概要】

非接触通信における半二重ブロック伝送プロトコルとプロトコルシーケンスを定義している。

【動向】

2004 年 4 月現在、2001 年 01 月 18 日にリリースされたものが最新。その後、ISO/IEC 14443-4:2001/AWI Amd 1 が 2002 年 10 月 4 日に公開されている。

(4) JIS

【概要】

JIS とは Japanense Industrial Standards（日本工業規格）の略で、工業標準化の促進を目的とする工業標準化法に基づき制定される国家規格。この中にも IC カードに関連する規格があり、その一覧を「表 2-38 IC カードに関連する JIS 規格」に示す。一覧の中の規格は ISO 規格を基にして作られているものが多い。

表 2 - 38 IC カードに関連するJIS 規格

JIS 番号	タイトル	対応 ISO/IEC
JISX6300-8	外部端子付きIC カード－セキュリティ関連共通コマンド	ISO/IEC 7816-8:1999
JISX6300-9	外部端子付きIC カード－追加共通コマンド及びセキュリティ属性	ISO/IEC 7816-9:2000
JISX6303	外部端子付きIC カード－物理的特性及び端子位置	ISO/IEC 7816-1:1998 ISO/IEC 7816-2:1999
JISX6304	外部端子付きIC カード－電気信号及び伝送プロトコル	ISO/IEC 7816-3:1997
JISX6305-3	識別カードの試験方法－外部端子付き IC カード及び接続装置	ISO/IEC 10373-3:2001
JISX6305-6	識別カードの試験方法－第 6 部 :外部端子なしIC カード－近接型	ISO/IEC 10373-6:2001
JISX6305-7	識別カードの試験方法－第 7 部 :外部端子なしIC カード－近傍型	ISO/IEC 10373-7:2001
JISX6306	外部端子付きIC カード－共通コマンド	ISO/IEC 7816-4:1994
JISX6307	外部端子付きIC カード－共通データ要素	ISO/IEC 7816-6:1996
JISX6308	外部端子付きIC カード－第 5 部 :アプリケーション識別子のための付番システム及び登録手続	ISO/IEC 7816-5:1994
JISX6321-1	外部端子なしICカード－密着型－第 1部 :物理的特性	ISO/IEC 10536-1:2000
JISX6321-2	外部端子なし IC カード－密着型－第 2 部 :結合領域の寸法及び位置	ISO/IEC 10536-2:1995
JISX6321-3	外部端子なしIC カード密着型－第 3 部 :電気信号及びリセット手順	ISO/IEC 10536-3:1996
JISX6322-1	外部端子なしIC カード－近接型－第 1 部 :物理的特性	ISO/IEC 14443-1:2000
JISX6322-2	外部端子なしIC カード－近接型－第 2 部 :電力伝送及び信号インタフェース	ISO/IEC 14443-2:2001
JISX6322-3	外部端子なしIC カード－近接型－第 3 部 :初期化及び衝突防止	ISO/IEC 14443-3:2001
JISX6322-4	外部端子なしIC カード－近接型－第 4部 :伝送プロトコル	ISO/IEC 14443-1:2001
JISX6323-1	外部端子なしIC カード－近傍型－第 1 部 :物理的特性	ISO/IEC 15693-1:2000
JISX6323-2	外部端子なしIC カード－近傍型－第 2 部 :電波インタフェース及び初期化	ISO/IEC 15693-1:2000
JISX6323-3	外部端子なしIC カード－近傍型－第 3 部 :衝突防止及び伝送プロトコル	ISO/IEC 15693-1:2001

⑤ JICSAP 仕様

【概要】

IC カードシステム利用促進協議会（JICSAP : Japan Ic Card System APplication council）が制定した IC カード仕様。ISO 7816 および ISO 14443 をベースにして作られており、いくつかのコマンドが追加されている。

【動向】

1997 年 9 月に第 1.0 版、1998 年 7 月には第 1.1 版が開示され、平成 13 年 7 月 31 日に JICSAP 仕様 V2.0 が公開された。2004 年 2 月現在、V2.0 が最新バージョンである。V2.0 仕様書が近く JIS 化される。

【詳細】

JICSAP 仕様 V1.1 では、接触型 IC カードにおけるハードウェア概要、伝送プロトコル、ファイル構造、セキュリティ構造、共通コマンドなど、接触型 IC カードのすべての機能を 1 本化した仕様書としていた。V1.1 を改定した JICSAP 仕様 V2.0 では接触型 IC カードに依存する仕様と、接触型 IC カード及び近接型 IC カードに共通する仕様を分離されている。V2.0 の構成および引用する主な ISO を「表 2 - 39JICSAP のタイトル一覧」に示す。

表 2 - 39 JICSAP のタイトル一覧

パート	タイトル	概要	主な参照（引用）ISO規格
第 1 部	接触型ICカード	接触型IC カードの物理的特性、電気的特性、伝送制御手順について規定	ISO/IEC 7816-1,2,3,4
第 2 部	近接型 IC カード	近接型 IC カードの物理特性、カードとリーダライタ間の非接触通信に係る機能、および試験法について規定	ISO/IEC 14443 ISO/IEC 10373-6
第 3 部	共通コマンド	接触型、近接型の両方のIC カードに共通に利用可能な、ファイル構造、セキュリティ構造、共通コマンドについて規定	ISO/IEC 7816-4,8,9 ISO/IEC 9796-2 ISO/IEC 9798-2,3 ISO 9992-2 ISO/IEC 9979
第 4 部	高速処理用ICカード	高速化機能を有するカードの物理特性，電波インターフェース，伝送プロトコル，ファイル構造及びコマンドについて規定	IEC 61000-4-2 ISO/IEC 7810 ISO/IEC 7816-2 ISO/IEC 10373 ISO/IEC 10373-6 ISO/IEC 14443-1,2

⑹ PKCS #11

【概要】

RSA Security 社が策定した仕様。暗号情報を保持し、暗号機能を実行するデバイスに対する「Cryptoki」と呼ばれるAPI を規定している。

【動向】

1995 年 4 月 28 日に V1.0 が公開されて、2001 年 11 月に公開されたV2.11 が 2004 年 2 月現在の最新バージョン。V2.11 ではC 言語で実装するにあたり必要なデータ構造や関数を定義している。以降のバージョン（ドキュメント）で実装言語に対して依存しない API を提供するかもしれない（may）。V2.20 のドラフトが公開されている。

【詳細】

暗号情報を保持し、暗号機能を実行するデバイスに対する「Cryptoki」と呼ばれる API を規定。PKCS#11 はデバイスに依存せず（any kind of device）、複数のデバイスに対して複数のアプリケーションがアクセスする（multi applications accessing multi devices）ことを目標としている。

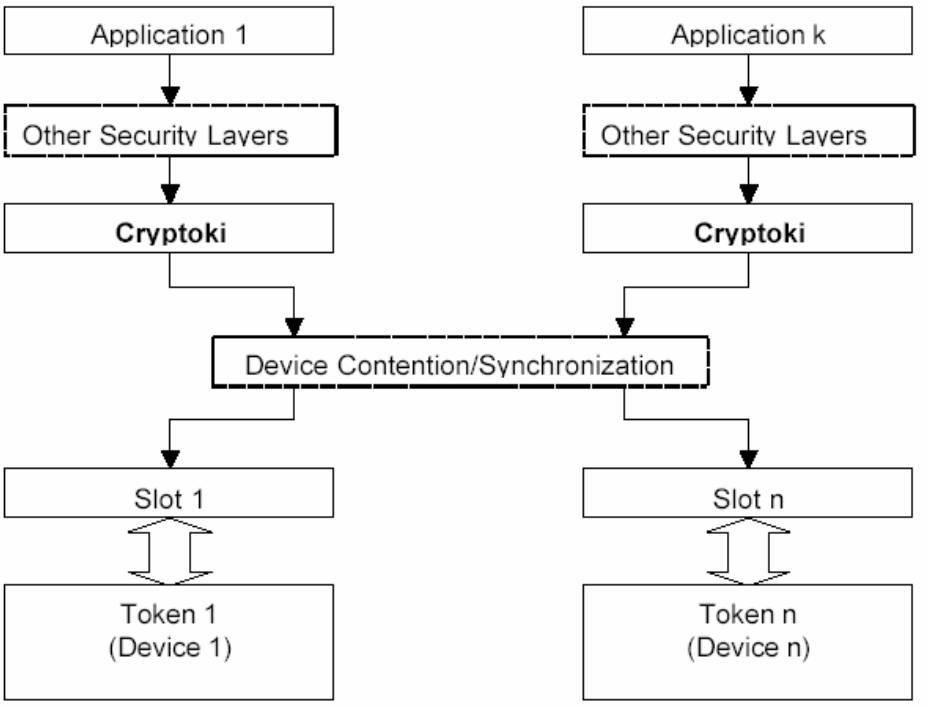


図 2 - 28 PKCS#11 の構成

（「PKCS #11 v2.11: Cryptographic Token Interface Standard」より抜粋）

Cryptoki で定義されている関数は大きく 13 種類に分類され、暗号サービスに必要な関数をそろっている。関数の分類一覧を「表 2 - 40 Cryptoki で定義されている関数」に示す。

表 2 - 40 Cryptoki で定義されている関数

分類	説明	関数の数
general-purpose functions	Cryptoki の初期化、リソースの開放などを行う関数。	4 関数
slot and token management functions	スロットおよびトークンの情報取得など、暗号デバイスに対する操作を行う関数。	9 関数
session management functions	セッションの確立・終了などセッションの管理を行う関数。	8 関数
object management functions	データ、鍵、証明書などのオブジェクトの生成・削除・検索などを扱う関数。	9 関数
encryption functions	暗号化を行う関数。	4 関数
decryption functions	復号を行う関数。	4 関数
message digesting functions	メッセージダイジェストを行う関数。	5 関数
signing and MACing functions	署名・MAC を生成する関数。	6 関数
functions for verifying signatures and MACs	署名・MAC の検証を行う関数。	6 関数
dual-purpose cryptographic functions	暗号化と署名など複数の暗号機能を利用する関数。	4 関数
key management functions	鍵の生成、暗号化、配信など鍵の管理を行う関数。	5 関数
random number generation functions	乱数を生成する際に使用する関数。	2 関数
parallel function management functions	実行中の関数に対して行う関数。しかし、V2.11 では利用しない。	2 関数

上記 68 の関数以外に、callback 関数が定義されている。

⑺ CryptoAPI

【概要】

Microsoft 社が開発した暗号化と署名の機能を提供する API。アプリケーションに対してサービスプロバイダに依存しない形式で、暗号機能の API を提供する。

【動向】

2004 年 2 月現在のバージョンは 2.0。CryptoAPI 1.0 では基本的な暗号機能しか提供されていなかったが、CryptoAPI 2.0 でメッセージを扱うための機能および証明書を扱うための機能が追加された。

【詳細】

暗号鍵の生成・交換・保管、暗号化や復号、デジタル署名の生成と検証などの機能をアプリケーションに提供する。

構成図）

CryptoAPI 2.0 のアーキテクチャを 図 2 - 29 CryptoAPI 2.0 の」に、CryptoAPI 2.0 が提供する機能を 表 2 - 41 CryptoAPI 2.0 が提供する機能」に示す。

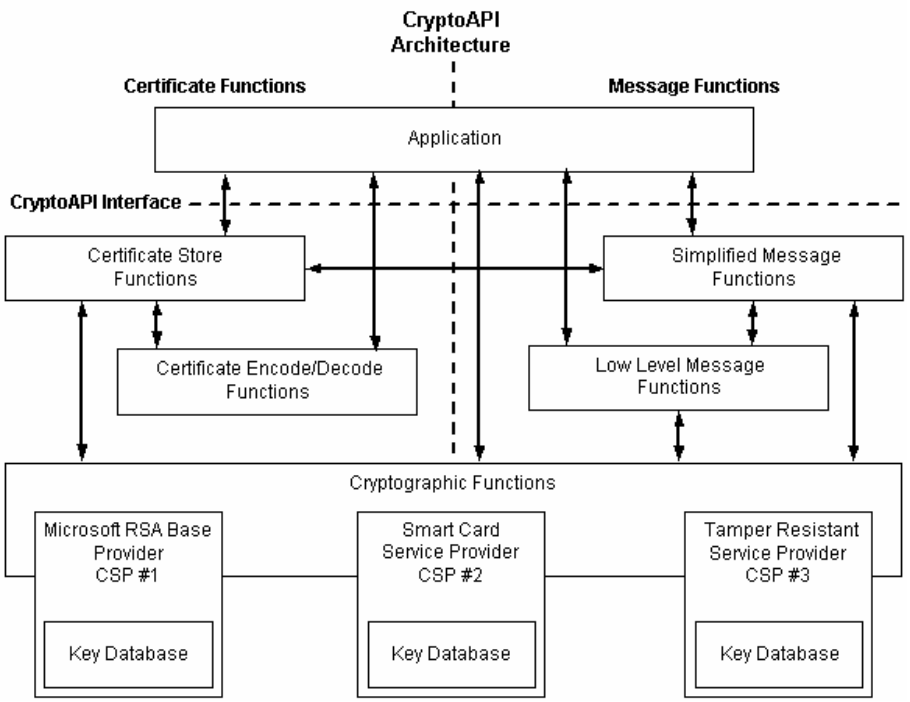


図 2 - 29 CryptoAPI 2.0 のアーキテクチャ

（MSDN ライブラリ Microsoft Visual Studio 6.0」より抜粋）

表 2 - 41 CryptoAPI 2.0 が提供する機能

機能	概要
Certificate Store Functions	証明書の格納・検索・検証などを行う関数。
Simplified Message Functions	メッセージの暗号化・復号、署名の生成・検証を行うために必要な処理をまとめた関数。
Certificate Encode/Decode Functions	デジタル証明書（X.509）の ASN.1 エンコード、デコードを行う関数。
Low-Level Message Functions	PKCS#7 のエンコード、デコードを行う関数。
Cryptographic Functions	暗号化・復号などの基本的な暗号機能を行う関数。

表 2 - 41 CryptoAPI 2.0 が提供する機能」にあるように CryptoAPI 2.0 では 5 つの機能が提供されており、機能は階層的な構造になっている。図 2 - 29 CryptoAPI 2.0 のアーキテクチャ」では、下部に位

置している「Cryptographic Functions」は基本的な暗号機能であり、「Certificate Store Functions」や「Simplified Message Functions」といった上部にある機能はサービスよりであり、下部に記されている基本的な機能を利用していることを示している。

⑧ PC/SC

【概要】

PC/SC とは Personal Computer Smart Card の略であり、異なるメーカの IC カードや IC カードリーダ･ライタを相互運用を可能にし、PC や他のプラットフォーム上で動作するアプリケーションの開発を容易にすることを目的とする仕様である。1996 年 5 月に Bull CP8･Gemplus･Hewlett-Packard･Microsoft･Schlumberger･Siemens Nixdorf によって設立された PC/SC ワークグループによって作成されている。

【動向】

2004 年 2 月現在、1997 年 12 月に公開された V1.0。V2.0 が現在作成中。

【詳細】

異なるメーカの IC カードや IC カードリーダ･ライタを Windows 上で、相互運用できるように決めた仕様。PC/SC ワークグループでは以下のことを行っている。

- 標準仕様を広めること
- カードリーダーのインターフェースを標準化すること
- PC からアクセスする共通のインターフェースと操作の仕様を策定すること

参加メンバ）

PC/SC ワークグループに参加している企業は以下のとおりである。

表 2 - 42 PC/SC ワークグループ参加メンバ一覧

クラス	企業名			
コア	Apple	Gemplus	Infineon	Ingenico
メンバ	Microsoft	Philips Semiconductors	Schlumberger	東芝
参加	ActivCard	Alcor Micro	Cherry GmbH	大日本印刷
メンバ	Kobil Systems GmbH	LOGICO Smartcard Solutions	O2Micro, Inc.	Omnikey AG
	Orga Kartensysteme	SCM Microsystems	Securealink	Sesam-Vitale
	Siemens	Lite-On Peripherals/Silitek	Soliton Systems	Standard Microsystems Corp.

構成図）

PC/SC のアーキテクチャを「図 2 - 30 PC/SC のアーキテクチャおよび各パートの定義領域」に示す。

PC/SC を利用してアプリケーションからIC カードにアクセスする場合、Resource Manager を経由してアクセスする。Service Provider、Crypto Service Provider からIC カードを利用する場合においても、同様にResource Manager を経由してIC カードにアクセスする。Resource Manager がカードリーダーの検索、IC カードの検索、IC カードへの接続、APDU の送受信、IC カードからの切断などの機能を提供する。
また、PC/SC の仕様の一覧を「表 2 - 43 PC/SC のタイトル一覧」に示す。PC/SC ではIC カードを利用したアプリケーションからIC カードに至るまで、広範囲の仕様を定めている。それぞれのパートが定めている対象については「図 2 - 30 PC/SC のアーキテクチャおよび各パートの定義領域」を参照のこと。

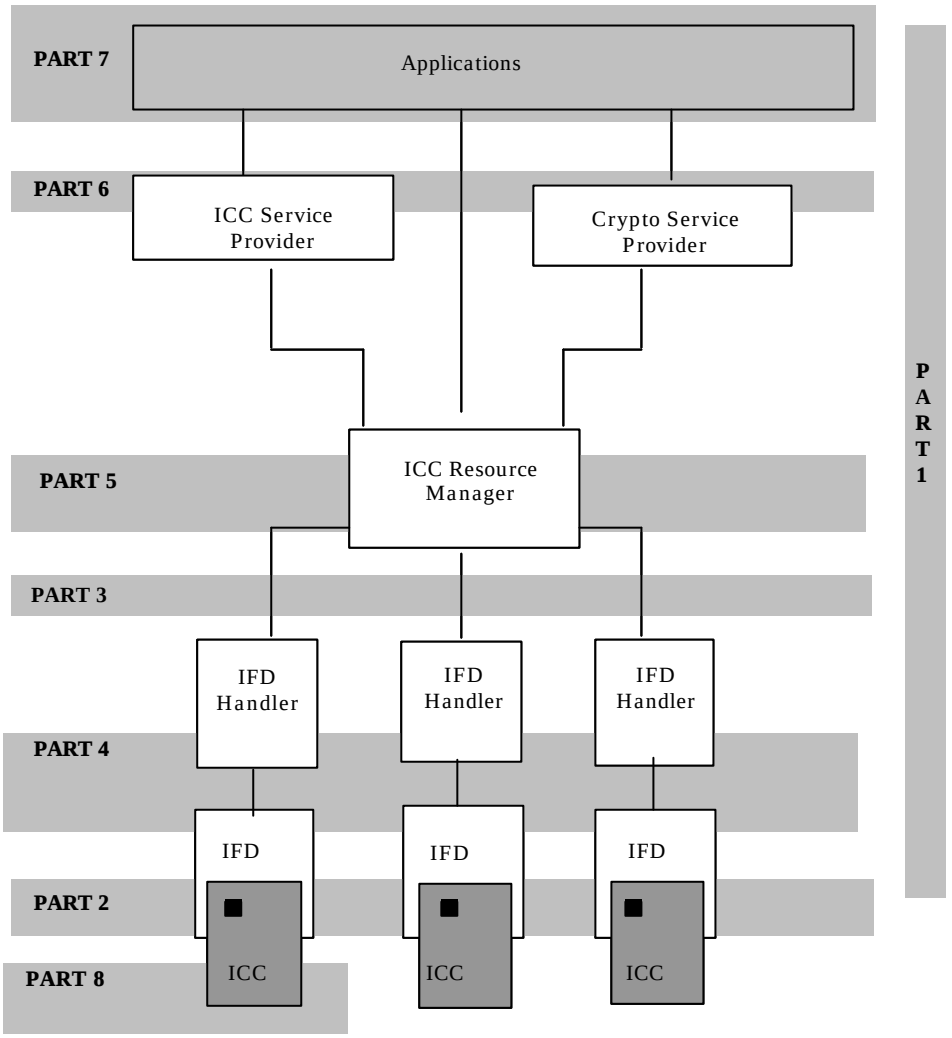


図 2 - 30 PC/SC のアーキテクチャおよび各パートの定義領域

（「PC/SC Part1 "Introduction and Architecture Overview"」より抜粋）

用語	説明
ICC	IC カード（IC Card）。
IFD	カードリーダー（Interface Device）。
IFD Handler	リーダードライバ。
ICC Resource Manager	リソースマネージャ。カードリーダーの検索、IC カードの検索、IC カードへの接続、APDU の送受信、IC カードからの切断などの機能を提供する。
ICC Service Provider	IC カードにアクセスするサービスプロバイダ。
Crypto Service Provider	暗号機能を提供するサービスプロバイダ。ここでは特に、IC カードを利用した暗号機能を提供するサービスプロバイダ。
Applications	IC カードを利用するアプリケーション。

表 2 - 43 PC/SC のタイトル一覧

part	タイトル	概要
Part 1	Introduction and Architecture Overview	システムの構成, コンポーネントについての概要について記述。
Part 2	Interface Requirements for Compatible IC Cards and Readers	IC カードと接続される機器の物理特性、電気特性について規定している。ISO/IEC 7816 -1, 2, 3 に相当。
Part 3	Requirements for PC-Connected Interface Devices	PC と接続される機器とのインターフェースについて規定している。
Part 4	IFD Design Considerations and Reference Design Information	接続される機器の設計情報について規定。
Part 5	ICC Resource Manager Definition	リソースマネージャの I/F と機能について規定している。
Part 6	ICC Service Provider Interface Definition	IC カードサービスプロバイダのモデルについて規定している。
Part 7	Application Domain/Developer Design Considerations	IC カードを利用するアプリケーションの開発について規定している。
Part 8	Recommendations for ICC Security and Privacy Devices	暗号および ストレージ機能をもつ IC カードの要求機能について規定している。

⑼ Open Card Framework

【概要】

カードリーダー、IC カードの種類、カードベンダ、プラットフォームに依存せずに、アプリケーションを作成できるようにすることを目的としてできた仕様。

【動向】

2004 年 2 月現在の Version は 1.2。

【詳細】

異なるプラットフォーム上で動作する Java ベースの IC カード・アプリケーションを開発するための仕様。Java で開発できるため、IC カード・アプリケーションは異なるプラットフォーム間であっても同一のソースコードが利用できる。また、Open Card Framework から PC/SC を利用することも可能である。

参加メンバ）

OCF に参加しているメンバを 表 2 - 44 Open Card Framework 参加メンバ」に示す。

表 2 - 44 Open Card Framework 参加メンバ一覧

3-G International	American Express Travel Related Services	Bull
First Access	Gemplus	Giesecke & Devrient
IBM	東芝	TOWITOKO
Schlumberger	Siemens	Sun Microsystems
UbiQ Inc.	Visa International	XAC Automation

PC/SC との比較）

Open Card Framework と PC/SC とは「アプリケーションが IC カードにアクセスするための仕様」という点では同一であるが、両者にはいくつか異なる点がある。その中でもっとも大きな相違点は対象としているプラットフォームである。

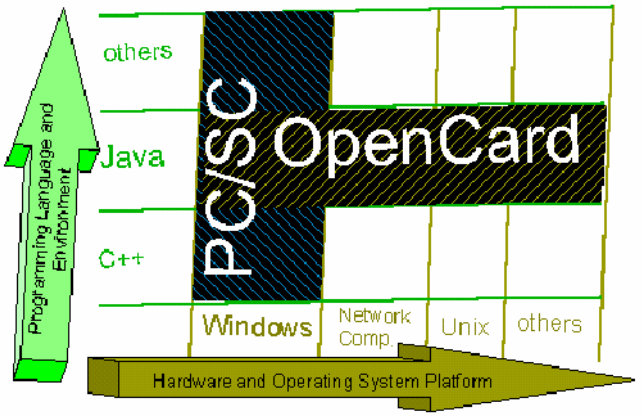


Figure 6: PC/SC and OpenCard have a different scope and overlap only where Java is used on Windows

図 2 - 31 PC/SC とOpen Card Framework との違い

（OpenCard and PC/SC - Two New Industry Initiatives for Smart Cards」より抜粋）

図 2 - 31 PC/SC とOpen Card Framework との違い」にあるように、Open Card Framework は Java をベースにしているために、プラットフォームに依存しない。一方、PC/SC は実装言語には依存しないが、現時点では Windows 上でしか実装されていない。

(10) Government Smart Card - Interoperability Specification (GSC-IS)

【概要】

NIST によって策定され、米国政府の発行する IC カードと IC カードを利用したアプリケーションの相互運用性を確保することを目的として策定された仕様書。

【動向】

2000 年 8 月に Version 1.0 がリリースされ、Version 2.1 が 2003 年 7 月 16 日にリリースされた。2004 年 2 月現在、Version 2.1 について SC17 の WG 4にて ISO 化が進められている。

【詳細】

GSC-IS はICカードとICカードを利用したアプリケーションの相互運用性を確保することを目的として策定された仕様であり、以下の項目を目標に掲げている。

- ISO/IEC 7816 などの既存の標準上で構築する
- 標準化された高水準の IC カード･サービス API を提供する
- IC カードベンダから中立である
- 色々なカードリーダーでも動作する
- 拡張性がある

ただし、以下の内容にいては GSC-IS では対象としない。

- IC カードの初期化
- 暗号鍵の管理
- IC カードとカードリーダーとの間の通信
- カードリーダーとPC との通信

構成図）

GSC-IS のアーキテクチャを「図 2 - 32 GSC-IS のアーキテクチャ」に示す。GSC-IS はアプリケーションに対して暗号化・復号、署名生成などのサービスを提供する層とAPDU を構築し、カードに送信する層と、2 つの層に分かれている。「図 2 - 32 GSC-IS のアーキテクチャ」において、BSI・XSI がサービスを提供する層に、VCEI が APDU を構築する層にあたる。アプリケーションから GSC-IS を利用する際には BSI または XSI を利用して IC カードにアクセスする。

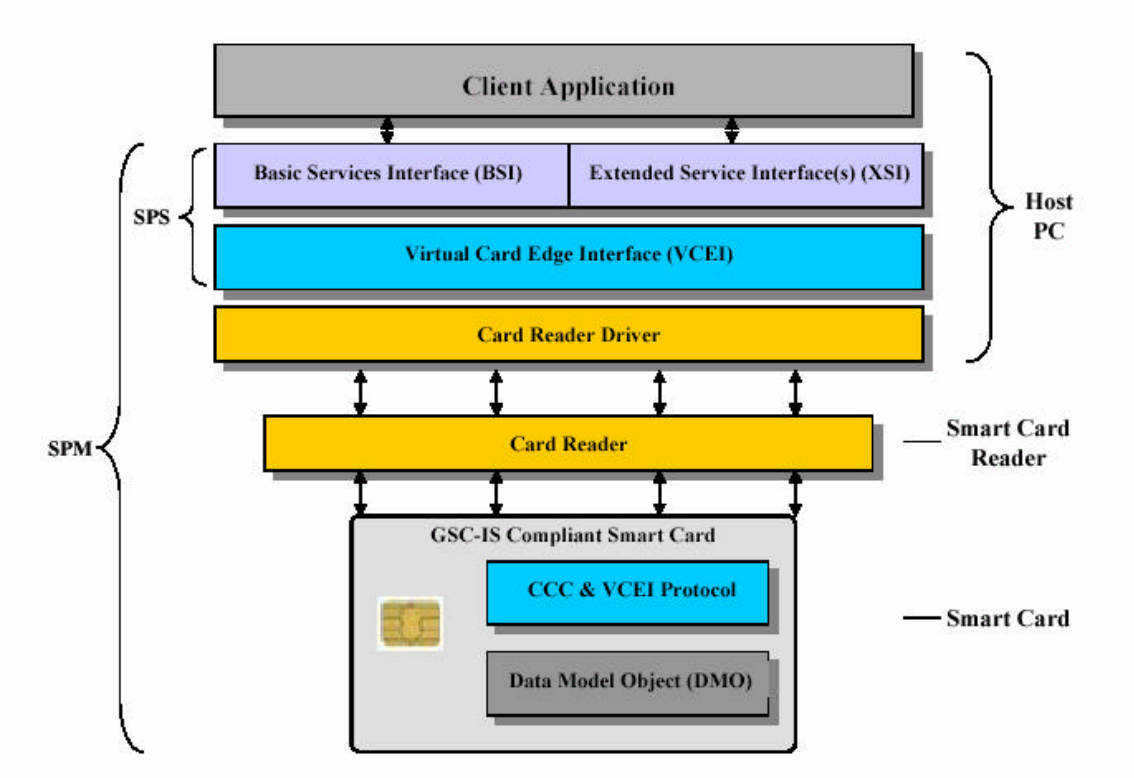


図 2 - 32 GSC-IS のアーキテクチャ

（「Government Smart Card Interoperability Specification Version 2.1」より抜粋）

表 2 - 45 アーキテクチャ図内の用語

名称	説明
BSI	IC カードを利用したサービスのうち基本的なサービスのインターフェース。

	IC カードとの接続（Utility Provider Module）、データの格納（Generic Container Provider Module）、暗号機能（Cryptographic Provider Module）などのサービスを提供。
XSI	BSI の拡張インターフェース。BSI とXSI をあわせて、SPM の API にあたる。
VCEI	バーチャルカードエッジインターフェース。IC カードに送信するAPDU を定義している。
SPS	サービスプロバイダソフトウェア。SPM のソフトウエア部分。
SPM	サービスプロバイダモジュール。クライアントアプリケーションにサービスを提供するモジュール。
CCC	Card Capabilities Container。カード内で VCEI から送信された APDU を Smart Card native APDU に変換する。GSC-IS に対応したカードは CCC 持っている必要がある（shall）。

（バイオメトリクスとの関連）

GSC-IS においてデータバイオメトリクス関連のデータを扱う際には以下のようなフォーマットを用いる。

Biometrics – X.509 Certificate File / Buffer		EF6000	Always Read
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
Template	60	Variable	512
Certificate	61	Variable	1500
Error Detection Code	FE	LRC	1

図 2 - 33 GSC-IS で利用されるバイオメトリクス関連のデータ

（「Government Smart Card Interoperability Specification Version 2.1」より抜粋）

また、GSC-IS V2.1 はバイオメトリクスを利用した認証に関して具体的な記述はされていないが、バイオメトリクス認証にも拡張可能な仕様になっている。GSC-IS のバイオメトリクス認証への対応に関して Ad Hoc Group on Biometric Interoperability in Support of the Government Smartcard Framework (AHGBISGF) というアドホックグループが検討結果を報告している。報告書では BioAPI、Java Card Biometric API（詳細は「(15) JavaCard Biometric API」を参照）などのバイオメトリクスに関連する標準と組み合わせてバイオメトリクス認証に対応する場合を想定し、生体情報を格納するためのストレージとして IC カードを利用する場合には GSC-IS の仕様を修正するがないが、IC カード内で照合を行う場合にはいくつか修正が必要であると記載されている。GSC-IS、BioAPI、Java Card Biometric API を利用し、IC カード内でバイオメトリクス認証を行う場合のアーキテクチャの例を「図 2 - 34 GSC-IS を利用してカード内照合を行う場合のアーキテクチャ」に示す。図中では、アプリケーションが利用するインターフェースとして、登録（enrollment）を行う場合は XSI Bio を利用し、照合（verification）を行う場合には BSI を利用する構成になっている。BioAPI

はGSC-IS のインターフェース BSIおよび XSI Bio）から呼び出され、Vender B SP for MOC(Match on Card / On-Card Matching)および Smart Card BrovideBSP に接続する。Vender BSP for MOC(Match on Card / On-Card Matching)はバイオメトリクスデバイスから生態情報を取得し、Smart Card Brovider BSP は IC カードへのデータの格納・照合データの送信を行う。

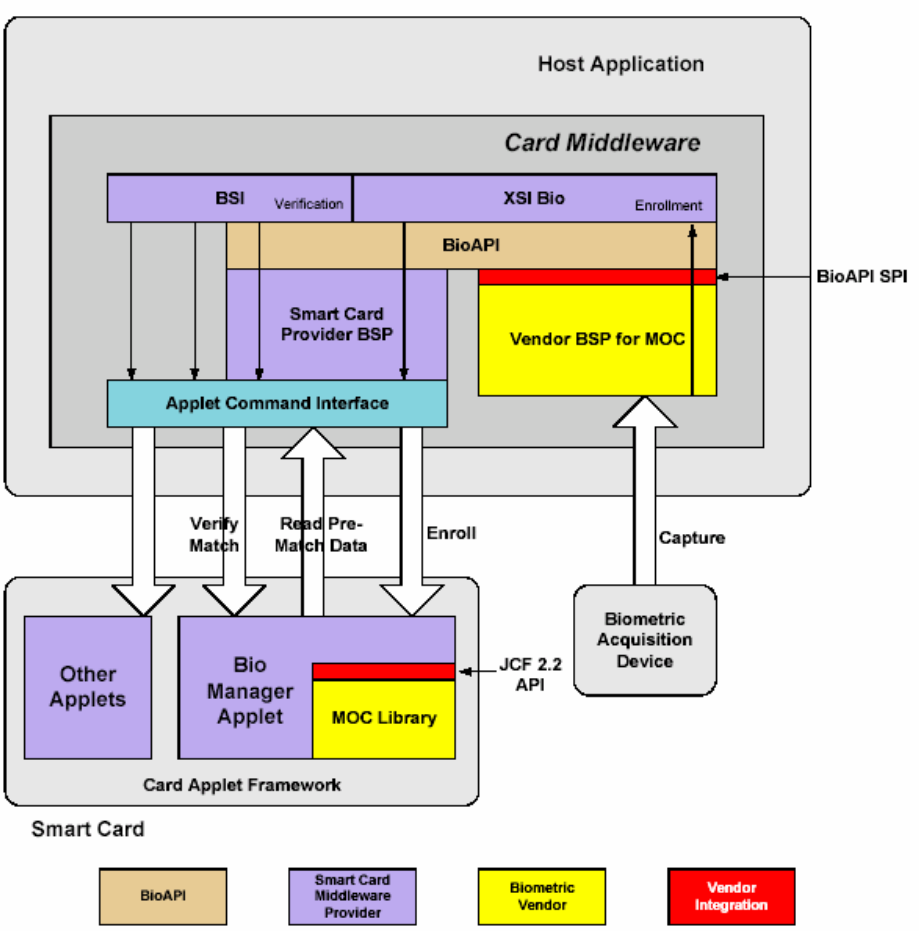


図 2 - 34 GSC-IS を利用してカード内照合を行う場合のアーキテクチャの例

（「Smart Card Biometric Interoperability Study Report」より抜粋）

用語	解説
XSI Bio	GSC-IS の XSI をバイオメトリクス用に拡張したもの。
MOC(Match on Card / On-Card Matching) Library	カード内照合を行うために必要な Java Card のライブラリ。
Smart Card Brovider BSP	IC カードへのアクセスが可能な BSP。登録テンプレート、照合データなどを IC カードに送信し、照合結果を受け取る。

Bio Manager Applet	Java Card 内でバイオメトリクス情報（テンプレート）を管理するアプレット。
Vender BSP for MOC(Match on Card / On-Card Matching)	BioAPI Framwork からロードされるBSP。バイオメトリクスセンサーとのインターフェースの提供、MOC(Match on Card / On-Card Matching)に必要な生体情報の作成を行う。

(11) Java Card

【概要】

IC カード上で Java プログラムが動作可能なカードであり、SUN によって提供されている。Java Card は以下のような特徴をもつ。

- カード発行後でもアプリケーションの追加、削除、変更が可能
- Java 言語によるアプリケーションの開発が可能
- マルチアプリケーション環境を実現

【動向】

1996 年 10 月 26 日に初めて Java Card API が公開された。2004 年 2 月現在、2003 年 11 月に公開された Version 2.2.1 が最新版。

【詳細】

構成図)

Java Card の構成図を「図 2 - 35 Java Card のアーキテクチャ」に示す。

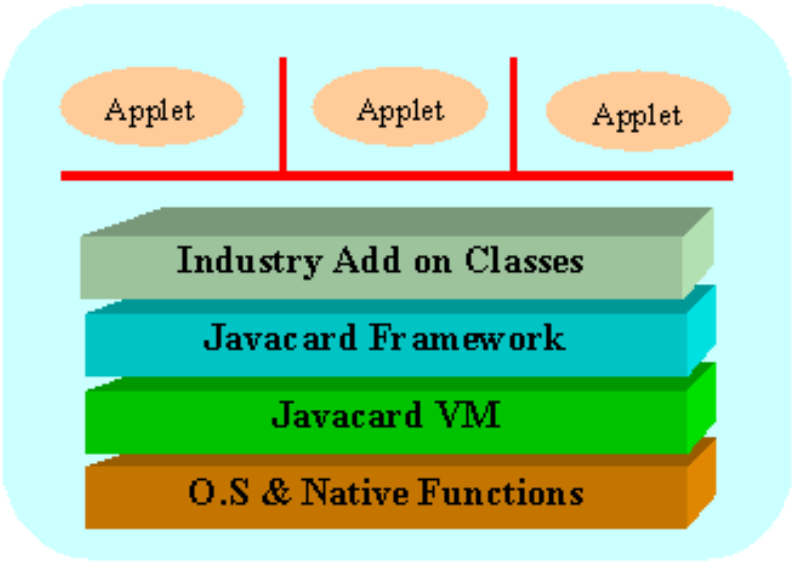


図 2 - 35 Java Card のアーキテクチャ

(http://www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev-p2.html より抜粋)

用語	説明
Applet	Java Card 上で動作するアプリケーション。
Javacard Framework	Java Card API を定義し、Applet に対してサービスを提供する。

Javacard VM	Java Card バーチャルマシン。アプレットのバイトコードを解釈する。

Java Card はアプリケーション（Java Card Applet）を Javacard VM 上で動作させることで、異なるベンダーで製造された IC カード間であっても、同一のアプリケーションを動作させることが可能になる。また、Java Card 上では複数のアプリケーションが動作することが可能である。

(12) MULTOS

【概要】

MULTOS とは、複数のアプリケーションを搭載可能である IC カードの OS。発行後であっても、安全にアプリケーションの追加、搭載済みのアプリケーションの削除が可能である。MULTOS の技術仕様は MAOSCO コンソーシアムで管理・運営されている。

【動向】

1997 年 5 月に MAOSCO コンソーシアムが設立されて以来、MULTOS の推進が進められている。

【詳細】

MULTOS は複数のアプリケーションを搭載可能な IC カード用 OS である。MULTOS の技術的な特徴をまとめると以下のようになる。

- 共通プラットフォーム
  CPU の違う半導体チッププラットフォームであっても、OS 側に共通のバーチャルマシンと API を持つことによって、搭載するアプリケーションを再開発することなしに共有することが可能
- アプリケーションのロード、削除
  アプリケーションは通常 IC カードの不揮発性メモリ上に搭載されるため、搭載アプリケーションをパーソナライズ時や発行後に追加、または削除が可能
- 高セキュリティを実現（ITSEC L6 を取得）
  アプリケーション間はファイアーウォールで分離され、アプリケーションの追加・削除を行う際には MULTOS CA が発行する証明書を利用するため、高いセキュリティが実現可能

（参加メンバ）

MAOSCO のメンバは以下のとおりである。

表 2 - 46 MAOSCO 参加メンバ一覧

Axalto	大日本印刷	Discover Financial Services
Giesecke & Devrient	日立製作所	Infineon Technologies
SyntiQ International	Keycorp	MasterCard International
Oberthur Card Systems		

(13) Windows for Smart Cards

【概要】

Microsoft が提供している多機能型スマートカード用のオペレーティングシステム。FAT ファイルシステムを採用しており、GUI のない Windows のような存在。開発言語は Visual Basic や Visual C++である。Windows for Smart Cards は以下の機能をもつ。

- カード内に複数のアプリケーションを搭載することが可能。
- カード外のファイルと同様のアクセスコントロールが可能。
- 暗号機能を搭載。
- ISO 7816-4 で定義されているコマンドのサポート。

【動向】

1998 年 10 月にプレスリリースが公開された。

(14) Global Platform

【概要】

Global Platform は多目的スマートカード用の標準化体制の確立や管理，普及促進を行うことを目的として、1999 年 10 月に Visa International を中心に多くの企業、団体によって設立され、Visa International がそれまで開発していた多機能 IC カード・端末のプラットフォームの仕様書である VISA Open Platform の権利を譲り受けた。Global Platform はカード OS・カードベンダに依存することなく、複数のアプリケーションを展開・管理することができる標準の策定を行っている。Global Platform は、カード仕様・システム仕様・デバイス仕様の 3 つの仕様書から成り立っている。

【動向】

（カード仕様）

2004 年 2 月現在、「GlobalPlatform Card Specification v2.1.1」が 2003 年 3 月に、「GlobalPlatform Card Security Requirements Specification v1.0」が 2003 年 5 月に公開されているものが最新の仕様である。

（デバイス仕様）

2004 年 2 月現在、「GlobalPlatform Device API v2.0」2002 年 10 月に公開されているものが最新の仕様である。

（システム仕様）

2004 年 2 月現在、「GlobalPlatform Systems Card Customization Guide v1.0」が 2002 年 8 月、「GlobalPlatform Systems Profile Specification v1.0」および「GlobalPlatform Systems Scripting Language Specification v1.0」が 2002 年 11 月に公開されているものが最新の仕様である。

【詳細】

Global Platform は様々な業種のイシュアが様々なデバイスを通じて顧客向けに複数のアプリケーションを展開・管理できることを可能とするオープンな標準と IC カードインフラを整備し普及させることを目的としている。Global Platform の特徴をまとめると以下のようになる。

- 複数のアプリケーションが安全かつ管理された形で共存できる。

- カードのライフサイクル上どの時点でもカードを再発行することなくロード、再設定、削除などのカスタム化が可能。
- アプリケーションのロード、再設定、削除はカード発行者が決定できる。

参加メンバ）

2004年2月現在、Global Platformには52の企業が参加しており、参加企業の一覧を「表2 - 47 Global Platform参加メンバ一覧」に示す。

表2 - 47 Global Platform参加メンバ一覧

Full Members（19社）			
ActivCard	Datacard	Gemplus	Giesecke & Devrient
日立製作所	IBM	Infineon Technologies	Ingenico S.A.
JCB	MasterCard International	NTT	Oberthur Card Systems
Renesas	SERMEPA	STMicroelectronics	Sun Microsystems, Inc.
Thales	Total System Services, Inc.	Visa International	

Participating Members（8社）			
ACI Worldwide Inc.	Aspects Software Ltd.	CardBASE Technologies, Inc	CRYPTOMATHIC
大日本印刷	Orga	SyntiQ International B.V.	UbiQ Incorporated

Observer/Public Entity Members（14社）			
Bell ID	Cards Etc	GoldKey Technology Corporation	ICC Solutions Limited
INCARD S.p.A	KEB Technology	NMDA	オムロン
Sagem	Setec Oy	SSP Solutions Inc.	凸版印刷
東芝	Trusted Logic		

Others（11社）			
American Express	Axalto	Cartes Bancaires	Department of Defense
富士通	Industrial Technology Research Institute	Interpay	松下電器産業
NBS Technologies	Philips Semiconductors	Smart Card Laboratory, Inc	

(15) JavaCard Biometric API

【概要】

JavaCard Biometric API は Java Card Forum の Biometrics Task Force とNIST の Biometric Consortium ワーキンググループによって制定された仕様。バイオメトリクス照合に共通するインターフェースを提供することで、カードベンダ、バイオメトリクス技術に依存することなく、Java Card 上でバイオメトリクス照合を扱うことができるようにすることを目的としている。

【動向】

2002 年 7 月にバージョン 1.0 が公開され、同年 8 月にバージョン 1.1 が公開された。

【詳細】

Java Card の内部で生態情報を扱う際のクラス、インターフェースを定義している。これにより、安全にバイオメトリクスデータをカードに格納し、カード外に参照データを出すことなく照合が可能となる。JavaCard Biometric API の要件は以下のとおりである。

- カード内照合 (MOC: Match on Card / On-Card Matching)が可能
- シンプルかつコンパクト (インターフェース3 種、クラス2 種)
- 複数バイオメトリクス技術のサポート
- Global Platform の尊重
- 既存のインターフェース (たとえば PIN 検証など) の利用
- BioAPI や CBEFF と同調する

構成図)

Java Card Biometric API を利用したシステムのアーキテクチャを 図 2 - 36 JavaCard を利用した生態認証のアーキテクチャ」に示す。この図では Java Card 内部には生体情報を登録するアプレット (Bio Manager Applets)と照合を行うアプレット (Bio Client Applets)が格納されており、生体情報の保管と照合を別々のアプレットで行う。照合を行うためのアルゴリズムは Java Card Biometric API を介してアクセスするようになっていて、Applet 間で共有できるようになっている。つまり、アプレットは異なったアルゴリズムに対しても共通の API でアクセスすることが可能である。また、デバイスから取得した生体情報は CBEFF などで定義しているデータフォーマットに変換されて Java Card 内に送られる。

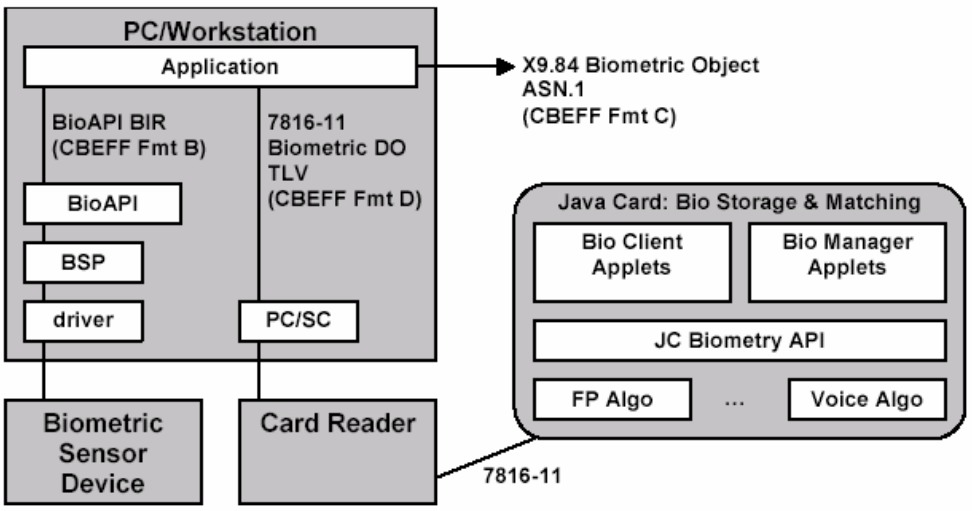


Figure 3. Interactions between various existing biometric standards.

図 2 - 36 JavaCard を利用した生態認証のアーキテクチャ

（「Java Card Biometric API White Paper」より抜粋）

表 2 - 48 「図 2 - 36 JavaCard を利用した生態認証のアーキテクチャ」内の用語

用語	説明
Bio Client Applets	テンプレートと照合を行うアプレット
Bio Manager Applets	テンプレートを管理するアプレット
JC Biometry API	本 API
FP Algo	指紋照合のアルゴリズム
Voice Algo	声帯照合のアルゴリズム
Biometric Sensor Device	生体情報を取得するデバイス

（クラスおよび メソッド）

Java Card Biometrics API が提供するクラスおよびインターフェースを 「表 2 - 49 クラスおよび」に、各クラスが提供する主なメソッドとその機能を 「表 2 - 50 メソッド」に示す。バイオメトリクスによる認証の基本的な操作である登録（enroll）と照合（match）において、登録に必要な基本的な API は *OwnerBioTemplate* に規定されており、照合に必要な基本的な API は *BioTemplate* に規定されている。なお、基本的な登録および照合のフローチャートを 「図 2 - 37 Java Card Biometric API を用いた場合のフローチャート」に示す。登録では *OwnerBioTemplate* の init メソッドによって登録の初期化を行い、カードに送信できなかったデータを update メソッドで追加して、最後に doFinal メソッドを呼び出してテンプレートの登録を行う。また、照合の場合は initMatch メソッドによって照合の初期化を行ったのち、match メソッドに照合を行う。

表 2 - 49 クラスおよびインターフェース

分類	名称	概要
クラス	**BioBuilder**	空のテンプレートを作成するクラス。
	BioException	本パッケージで発生する例外クラス。
インターフェース	***BioTemplate***	テンプレート照合（Matching）を行うためのインターフェースである。
	OwnerBioTemplate	***BioTemplate*** を継承し、テンプレートを登録する関数を提供する。
	SharedBioTemplate	***BioTemplate*** を継承し、テンプレートを管理するアプレットと照合を行うアプレット間でテンプレートを共有する場合に利用する。

表 2 - 50 メソッド一覧

クラス	メソッド名	概要
BioBuilder	buildBioTemplate	空のテンプレートを作成する。
BioException	throwIt	Exception を発生させる。
BioTemplate	getBioType	バイオメトリクスのタイプを取得する。
	getPublicTemplateData	テープレートに関するデータ（バージョン，フォーマットなど）を取得する。
	getTriesRemaining	照合のチャレンジできる残り回数を取得する。
	getVersion	照合アルゴリズムのバージョンとID を取得する。
	initMatch	照合の初期化を行う。
	isInitialized	照合が開始できる状態かどうか判定する。
	isValidated	照合が完了しているかどうか判定する。
	match	照合を行う。
	reset	照合の残りチャレンジ回数をリセットする
OwnerBioTemplate	init	登録初期化を行う。
	update	不足データを追加する。
	doFinal	照合用のテンプレートを作成する。

	resetUnblockAndSetTryLimit	照合の確認フラグのリセット、チャレンジの最大回数の変更、その最大回数に残りチャレンジ回数をセットすることを行う。
SharedBioTemplate	—	***SharedBioTemplate*** で定義しているメソッドはない）

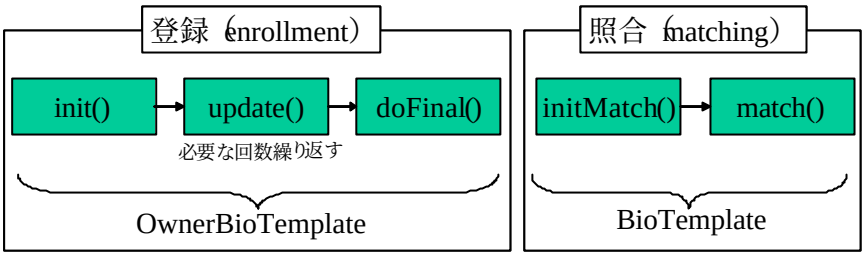


図 2 - 37 Java Card Biometric API を用いた場合のフローチャート

(16) PKCS #15

【概要】

RSA Security 社が策定した仕様で、ユーザーが暗号トークン（IC カードなど）を共通的に利用できるようにすることを目的として、暗号トークンに記録される暗号オブジェクトの共通フォーマット、IC カード内のファイル構造、ASN.1 で記載する際の構造（syntax）を規定している。

【動向】

1999 年 4 月 23 日に Version 1.0 が公開され、現行は 2000 年 6 月 6 日にリリースされた Version 1.1。

【詳細】

デバイスに記録される暗号オブジェクトの共通フォーマット、IC カード内のファイル構造、ASN.1 で記載する際の構造（syntax）を規定している。これらはプラットフォーム、ベンダー、アプリケーションなどに依存されない形式になっている。PKCS#15 では鍵データを格納する"Key Object"，証明書のデータを格納する"Certificate Object",認証用のデータを格納する"Authentication Object"，その他のデータを格納する"Data Object"の 4 種類のオブジェクトを規定しており、Authentication Object に Biometric Template を格納することが可能である。

構成図）

PKCS #15 に準拠したとしても、IC カード内のファイル構造が一意に決まるわけではないが、本報告書では 1 つの例を示す。PKCS #15 を利用した IC カード内のファイル構造の例を「図 2 - 38 PKCS #15 を利用した IC カード内のファイル構造」に示す。ここでは、秘密鍵と公開鍵のペア、およびその証明書、ならびに秘密鍵の所有者を認証するためのデータを PKCS #15 形式で IC カード内に格納する場合を想定している。図中では MF の下に PKCS#15 の DF があり、この DF の内部にいくつかの EF が格納される。EF

（ODF）は EF（PriKey）・EF（PubKey）・EF（Certificate）・EF（Authenticate）へのポインタになっており、それぞれの EF はデータ本体へのポインタになっている。PKCS#15 では、データの本体の保管場所までは規定しいない。各データは ASN.1 で記述される。他のファイル構造の例は「PKCS #15 v1.1: Cryptographic Token Information Syntax Standard」を参照のこと。

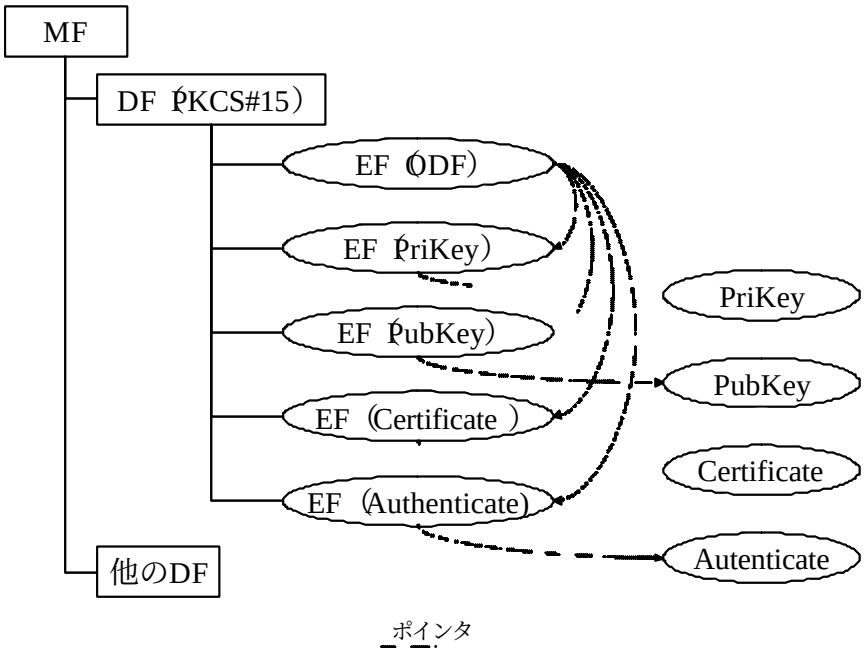


図 2 - 38 PKCS #15 を利用した IC カード内のファイル構造

用語	説明
DF(PKCS#15)	PKCS#15 の DF。
EF(ODF)	PKCS#15 で規定されている他の EF へのポインタを格納した EF。必須のファイル。
EF(PriKey)	秘密鍵のデータへのポインタを格納した EF。
EF(PubKey)	公開鍵のデータへのポインタを格納した EF。
EF(Certificate)	証明書のデータへのポインタを格納した EF。
EF(Authenticate)	認証用のデータへのポインタを格納した EF。
PriKey	秘密鍵のデータ。ASN.1 で記述。
PubKey	公開鍵のデータ。ASN.1 で記述。
Certificate	証明書のデータ。ASN.1 で記述。
Authenticate	認証用のデータ。ASN.1 で記述。

（17）EMV

【概要】

ユーロペイ（Europay）、マスターカード（MasterCard）、ビザ（Visa）が策定したクレジットカード用の IC カードの標準仕様。IC カードを使用したクレジット取引において、カードと端末との間の相互運用性を確保しつつ、カードの不正利用に対するセキュリティを向上させることを目的としている。

【動向】

1998 年に EMV Version 3.1.1 が公開され、1999 年 2 月に EMVCo が設立された。2004 年 2 月現在では、2000 年 12 月に出版された EMV 2000 version 4.0 が最新。

【詳細】

EMV とは、クレジットカード用 IC カードの標準仕様であり、ISO7816 をベースにして拡張を行っている。IC カードを使用したクレジット取引において、カードと端末との間の相互運用性を確保しつつ、暗号鍵を使い本物のカードであるか確認を行うこと、またはカードと端末の間で相互認証を行うことで増加するカードの不正利用に対するセキュリティを向上させることを主な目的としている。IC カードや端末、アプリケーション等の仕様を規定している。現行の EMV 2000 におけるタイトル一覧、および概要を「表 2 - 51 EMV タイトル一覧」に記載する。

表 2 - 51 EMV タイトル一覧

章	タイトル	概要
Book 1	Application independent ICC to Terminal Interface requirements	アプリケーションに依存せず、正しく動作して相互運用が可能になるために必要な、ICカードと端末が持つべき最小限の機能。
Book 2	Security and Key Management	ICカードと端末が持つべき最小限のセキュリティ機能。
Book 3	Application Specification	決済処理を行うために必要な、端末とICカードに必要な手順。
Book 4	Cardholder, Attendant, and Acquirer Interface Requirements	ICカードを受け取るための必要、推奨、オプションの条件を定義する。

(18) 全銀協 ICキャッシュカード標準仕様

【概要】

全国銀行協会連合会（全銀協）によって制定された仕様。EMV仕様に準拠し、国内キャッシュカード、国内デビットカード仕様などが規定されている。各銀行より発行される IC カード仕様を標準化する事で、各銀行顧客であるカード利用者の利便性の向上、セキュリティの確保などを目的としている。

【動向】

『全銀協 IC カード標準仕様』（昭和 63 年 2 月制定、平成 9 年 4 月改訂）を改定して作成され、平成 13 年 3 月 21 日に発表された。なお、標準仕様は 5 年ごとに見直しの計画である。

(19) PC 上で利用する標準同士の関係

PC 上で利用する技術、標準の対象を「図 2 - 39PC 上で利用するIC カードに関連する技術、標準」に示す。

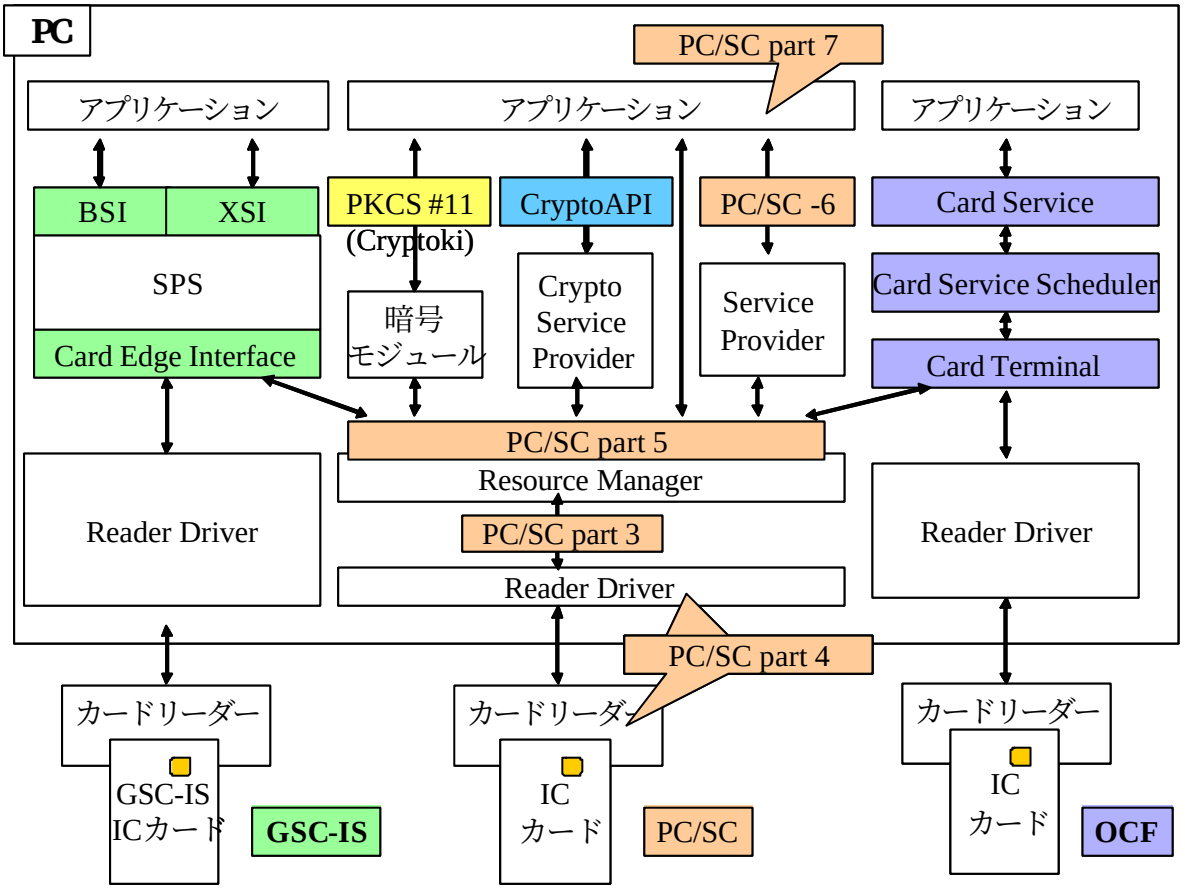


図 2 - 39PC 上で利用するIC カードに関連する技術、標準

「図 2 - 39PC 上で利用するIC カードに関連する技術、標準」では左から順に GSC-IS、PC/SC、Open Card Framework (OCF)のアーキテクチャを掲示し、それぞれの標準が規定している部分を示している。さらに、PKCS #11、CryptoAPI が規定している箇所も合わせて示している。ただし、PKCS #11 は API のみ規定しており、IC カードにアクセスするまでの仕様に関しては規定していないが、図では PC/SC を利用して IC カードにアクセスする場合の構成を記載している。図より、GSC-IS の BSI および XSI、PKCS #11、CryptoAPI、PC/SC の Part 6、OCF における Card Service がアプリケーションに対してサービスレベルのインターフェースを規定している。また、GSC-IS とOCF は Reader Driver を介して IC カードにアクセスすることも可能であるが、PC/SC を介して IC カードにアクセスすることも可能である。

(20) Smart Card Alliance

【概要】

Smart Card Alliance はマルチアプリケーション対応 IC カードの技術のために活動している非営利団体。Smart Card Alliance のミッションは以下のとおりである。

- IC カードの相互運用のビジョンを確立することにより、産業の発展を進めること
- マーケットトライアルを促進する環境を確立すること
- メンバおよび興味を持っている関係者に対して情報をタイムリーに提供すること
- 技術、ビジネス、法制、公共政策に関する問題に対して、業際的な立場を築くこと
- 産業の発展に重大な問題について議論すること

【動向】

2001 年に Smart Card Industry Association と Smart Card Forum が合併し、発足。

【詳細】

Smart Card Alliance には 100 以上の企業・団体が参加している。2004 年 2 月現在の参加メンバは以下のとおり。

Leadership Council

Assa Abloy, ITG	Atmel Corporation	Axalto
Bank of America	Datacard Group	First Data Resources
Gemplus	Hitachi America Ltd	IBM
Identix Incorporated	Infineon Technologies	JCB International Credit Card Co., Ltd
MasterCard International	Northrop Grumman Information Technology	Oberthur Card Systems
Philips Semiconductors	Samsung Electronics Co., Ltd.	SCM Microsystems, Inc
Smart Card Alliance	Unisys Corporation	VeriSign, Inc.
Visa USA	XTec, Incorporated	

General

Accelitec, Inc	ACI Worldwide	ACT Canada
ActivCard	Alegra Technologies, Inc.	Alliance Data Systems
AMAG Technology, Inc.	American Bankers Association	Anteon Corporation
AOS-Hagenuk B.V.	Arthur Blank & Company, Inc.	BearingPoint
Booz Allen Hamilton	Citicorp Electronics Financial Services, Inc.	Concord EFS, Inc./Star Systems Inc.
CU Cooperative Systems	Cubic Transportation Systems, Inc.	Datakey, Inc.

Datatrac Information Services, Inc.	Dawar Technologies	ERG Transit Systems
Exponent, Inc.	Fargo Electronics, Inc.	First National Bank of Omaha
Giesecke & Devrient	Hypercom Corporation	ICMA
ID TECH	ImageWare Systems, Inc.	Integrated Engineering
LaserCard Systems Corp	Lockheed Martin	Martsoft
Maximus	NBS Card Technology Corp.	NDS Technologies
OmniTek	ORGA Card Systems, Inc.	OTI America
Pace Integration	Precise Biometrics, AB	RSA Security, Inc.
Smart Card Solutions	Smart Systems Co., LLC	STMicroelectronics
SuperCom, Inc.	Tata Consultancy Services	TDK Electronics Corp.
Thales e-Security	Thomson Media	Uniliance Health
Vivotech, Inc.	Wisconsin Physicians Service Insurance Corporation	X-Ident USA LLC
Zebra Tech Corp		

Government

Bermuda Government	Bureau of Public Debt	Defense Manpower Data Center
DISA	Disbursing & Cash Management Activity	General Services Administration
MTA Bridges and Tunnels	NASA	Navy e-Business Operations Office
New Jersey Transit	Port Authority of NY/NJ	Transportation Security Admininstration
U.S. Customs	U.S. Department of State	U.S. Dept. of Transportation Volpe Center
U.S. Treasury FMS	US Department of Defense	Washington (MATA)

University

Cornell University	

Associate

CNB-E-Lysium Systems, Inc.	EPI, Inc.	Intersecting Technologies, LLC
SC Solutions, Inc.		

Smart Card Alliance には以下の8つの Work Group がある。

- Terminal and eTransaction Infrastructure Task Force
- Secure Personal ID Task Force
- Digital Security Initiative
- Stable Points Work Group
- Educational Institute Work Group
- Telecommunications Advocacy Work Group
- Transportation Work Group
- Market Research Work Group

この中の「Secure Personal ID Task Force」において「Smart Cards and Biometrics in Privacy-Sensitive Secure Personal ID Systems White Paper」が出されており、IC カードとバイオメトリクスとを組み合わせたセキュリティID システムについて White Paper を出している。この White Paper においても、MOC(Match on Card / On- Card Matching)に関して記述がある。

１．７．４ バイオメトリクスデバイス製品調査

表 2 - 52 照合機能付きデバイス【PC 接続用】

	企業名	製品名	目的	備考	
指紋	NEC	指紋認証ユニット（USB） PU800-20	PC	OSログイン、スクリーンセーバロック解除、アプリケーションパスワード代替、等の機能が必要な場合、別途、 指紋認証基本ユーティリティ」が必要	**指紋認証ユーティリティ（サーバ版）**：指紋認証ユニット（PC カード：PK-FP001/M/シリアル:PK-FP002/M/VersaPro内蔵）添付ソフトウェア、および、指紋認証基本ユーティリティを利用し、ドメインサーバ上で指紋データを管理するためのユーティリティ。ただし、ワークグループ環境、分散サーバや複数ドメインサーバ、ActiveDirectoryネイティブモード環境には対応していない。セットアップ時に指紋認証ユニットが必須です（FI300PU-01は利用不可）。また、本ソフトウェアを搭載したマシンに、指紋認証ユニット（PC カード：PK-FP001/M/シリアル:PK-FP002/M/VersaPro内蔵）添付ソフトウェア、および、指紋認証基本ユーティリティを同時インストールできません。サーバ上で、指紋認証基本ユーティリティと同じ機能を利用したい場合は、指紋認証基本ユーティリティ(DC)をご利用ください。さらに、Windows2000 Server/Professionalの新機能は一部未対応となります
		指紋認証ユニット（PC カード） PK-FP001M		OSログイン機能、スクリーンセーバのロック解除機能、主要アプリケーションのパスワード代替機能	
		指紋認証ユニット（シリアル） PK-FP002M			
	NECフロンティア	指紋認証付きICカードリーダライタ ユビキタッチ（エムコマース社製？）	PC	非接触ICカードリーダライタと指紋認証装置を一体化。ICカードと指紋の二重認証により、高度なセキュリティを実現します。上位サーバに指紋データを保管する従来の指紋認証装置異なり、ユビキタッチは読み込んだ指紋データとカードデータを装置内で照合するので、データ流出の不安がありません。住民基本台帳カードでも利用される、ISO/IEC14443タイプBに対応しています。	
	ソニー	FIU-900-N04 FIU-810-N03 FIU-600-N03	PC	1.ログインパスワードを指紋でロック 2.大切なデータ（ファイル）を暗号化して指紋でロック 3.指紋を使っていろいろなパスワードを記録 4. 「公開カギ」を使って安全なファイルのやりとり 5.指先だけでお気に入りにウェブサーフィン 6.席から離れるときでもPCを簡単ガード 7.メールソフトと組み合わせて「暗号メール」8.「デジタル証明書」も使えます	
	大日本印刷株式会社	DNP Standard-9 ADVANCE-FP	PC	JICSAP11コマンドや各種PKIコマンドを実装しているため、電子商取引やネットワークセキュリティなど幅広い用途に利用可能です。今回開発したシステムはWindowsR2000用CSPドライバへの組み込みが完了しており、1. WindowsR2000へのログオン，2. メールの暗号化／復号 などを、ICカードと指紋認証によりセキュアに行うことが可能です。	今後、当社が開発・販売しているネットワークセキュリティ「ICカードシステム『TranC'ert（トランザート）』」にも組み込む予定。**TranC'ert：**電子証明書をベースとした社員証システム．PKCS#11、CSPドライバを同梱しており、VPN、相互認証SSL、暗号メールも利用可能。ISMS（情報セキュリティマネジメントシステム）を強化するシステムとして利用でき、WindowsR起動制御、WindowsRログオン、スクリーンロック、自動ファイル暗号化、プログラム起動制御、サイニングインターフェース、簡易シングルサインオン、自動PIN入力、PIN閉塞解除、仮カード発行、仮カード再利用などの機能がある。
	大日本印刷株式会社 サイレックス・テクノロジー株式会社	ユビネットパスFP / COMBO-Mini	PC	DNPが2003年8月より販売開始している指紋認証機能付ICカード「DNP StandardR-9 ADVANCE-FP」をUIM形状に加工したものを、当リーダライタに装着することで、日本初のPKIとバイオメトリクスを組み合わせた携帯型認証ツールとなります。	1.所有者以外による電子証明書等の利用を完全に防止 2.秘密鍵や指紋特徴点データなどの流出の可能性がない 3.携帯が容易 4.メールの暗号化，電子署名添付，サーバ認証，パソコン起動制御などを手軽に利用 5.既存システムと混在した運用が可能
	富士通株式会社	バイオ認証装置 FMSE-C1010	PC	Secure Login Boxは、より大規模なシステムでの利用、外出先からのアクセス、多様なログイン、ユーザービリティの向上など、企業ユースにおけるさまざまなニーズに応えるため、装置間連携をはじめとする新機能を追加。低コスト、短期間で、ID／パスワードに代わる高度なログインシステムが構築できます。	**装置間連携**：Secure Login Boxを最大20台まで連携し、10,000ユーザーまで対応。トラフィックの軽減、バックアップによる信頼性も向上しています。**ファイアウォール対応：**ファイアウォールを通過して、インターネット環境から指紋認証ログインが実現できます。**スマートカード対応：**スマートカードの利用時に必要なPINコードの入力を指紋で代行。カードと指紋でセキュリティー性を大幅に向上できます。**シングルサインオン：**最初に指紋でログインすると、以降のさまざまなアプリケーションやWebへのログインが自動に行えます。**信頼性：**1.ネットワークを流れるデータを暗号化 2.ハードディスク内のデータの暗号化 3.RAID1によるハードディスクの二重化 4.ホットスワップの採用 5.ハードディスク電源自動停止 6.システムスケジュール機能 7.最新の指紋認証技術を内蔵
	三菱電機株式会社	三菱小型指紋照合装置 FPR-DTU 三菱小型指紋照合装置 FPR-ICRU／FPR-ICRS	PC	1. ローコストでハイセキュリティを実現 2. 照合装置内にて、照合処理を完結する事が可能です。3. SDKにより、指紋認証システムを容易に構築できます。	
	テクノイマジア株式会社	FP-PLUS	PC	1.ICカード内に所有者の指紋情報を記録し，カード使用時に「本人の指紋認証」を実施． 2.所有者の指紋情報をカードの外に出さずに，指紋照合を耐タンパ性の高いICカード内で完結させることが可能． 3.PC上での照合も可能． 4.指紋読取りユニットには，ユニークな機器IDを暗号化して保有． 5.機器IDを指紋データと組合わせて秘密鍵として使うことも可能（PKI対応アプリケーションが必要）	

表 2 - 53 照合機能なしデバイス

	企業名	製品名	目的	テンプレート保管
指紋	日本セキュアジェネレーション株式会社	EyeD ハムスターIII	PC	外部
		EyeD オプティマウス III		外部
		EyeD マウス		外部
		EyeD キーボード		外部
		EyeD スマートカードキーボード		外部
	日立エンジニアリング株式会社	HFP-PA0102 (Finger Attestor) パラレル	PC	外部
		HFP-US0102 USB		外部
		HFP-XJ0101 PCカード		外部
		HFP-CMB0101 ICカード一体		外部
	富士通株式会社	指紋認識装置 FS-210U/210P	PC	外部
		指紋認証付OADGキーボード FMV-KB331F		外部
	株式会社ディー・ディー・エス	指紋認証ユニット UB-USB-COB	PC	外部
	サイレックス・テクノロジー株式会社	FIC-200	PC	デバイス
		FUS-200		外部
		MUSB200-COMBO		ICカード
	株式会社スターテック・テクノロジー・ジャパン	パソコン用指紋認証システム FM200 / MKC200	PC	外部
	テクノイマジア株式会社	FP-STICK	PC	デバイス
	シーメンス	IDマウス C98451	PC	?
虹彩	沖電気工業株式会社	アイリスパスーｈ 情報セキュリティシステム	PC	外部?
署名	日本システム開発株式会社	個人認証ペン「DP―1000」	PC	外部?
血流	日立ソフトウェアエンジニアリング㈱	指静脈認証システム 静紋（じょうもん）	PC	外部

表 2 - 54 ソフトウェアシステム

	企業名	製品名	目的
指紋	NTTデータ	SmartBIO	PC
	日立エンジニアリング株式会社	指紋認証システム Finger Attestor	PC
		ICカード内指紋認証システム セキュアバイオロック	PC
	NECソフト	指紋認証システム iSecAssist	PC
	テクノイマジア株式会社	FP-AUTH	PC
		FP-figuard	PC
	日本セキュアジェネレーション株式会社	SecuDesktop2000	PC
		SeculBAS	PC
		SecuVLAN	PC
		Qvoice Wholslt?	PC
	サイレックス・テクノロジー株式会社	DIGITUS-Logon	PC
	株式会社スターテック・テクノロジー・ジャパン	パソコン用指紋認証システム BioSecret	PC
	SONY	標準指紋認証統合ソフト PUPPY Suite	PC
		インターネットセキュリティソフト Puppy Internet Token	PC
		Entrust、PKIソリューション対応ソフト Puppy Suite for Entrust	PC
顔	NEC	顔検出/照合エンジン NeoFace	PC
	東芝情報機器株式会社	顔de ろぐおん	PC

表 2 - 55 入退室 ･出退勤管理用

	企業名	製品名
指紋	NEC	ドアコントロールパネル FingerThroughⅡ
	株式会社アート	F-7130
		F-7140
	株式会社スターテック ･テクノロジー ･ジャパン	指紋認証入退室管理システム FINGER GUARD
	テクノイマジア株式会社	FP-KEY
	セコム	SESAMO-IDs
	三菱電機株式会社	三菱小型指紋照合装置 FPR-200AC1／FPR-1000AC1
		三菱小型指紋照合装置 FPR-1000AC2／FPR-1000AC4
		三菱小型指紋照合装置 FPR-200TR／FPR-1000TR
	株式会社デナロ	指紋照合式タイムレコーダー dft-100
	スガツネ工業株式会社	フィンガーチェック FP-320
	NTT-AT	指紋入退室 ･出退勤ターミナル＆システム AT-500FP
顔	オムロン	Face Key
	東芝	顔照合セキュリティシステム FacePassR
	株式会社アート	AF-2000
虹彩	沖電気工業株式会社	アイリスパスーWG ゲート管理システム
	松下電器産業 (株) パナソニックシステムソリューションズ社	入退室用虹彩認証カメラBM-ET300
		入退室用虹彩認証カメラBM-ET500
	株式会社ロックシステム	IrisAccess3000
掌形	エム ･エー ･ジェー株式会社	HK-2 (米 Recognition Systems Inc.製)
		ID3D-R (米 Recognition Systems Inc.製)
血流	バイオニクス	血流認証装置 VA－100
	デジコム株式会社	静脈パターン認証技術システム BK300s
	株式会社ロックシステム	VP-ⅡM
	株式会社アイ ･ディ ･テクニカ	VP-ⅡM
	東西電気産業株式会社	VP-ⅡM
複合	株式会社ジクシス	IDコントローラ

表 2 - 56 その他

	企業名	製品名	目的
証明書	RSAセキュリティ	RSA Keon Certificate Authority 6.5	ディジタル 証明書
DNA	株式会社アイ ･ディ ･テクニカ	DNA認証システム	偽造防止

1．8 参考文献および WWW サイト

- 「本人確認環境認証方式の提案」池田、森尻、才所、
- IPA セキュリティ関連 http://www.ipa.go.jp/security/
- ITU-T http://www.itu.int/ITU-T/
- ISO/IEC http://www.iso.org/
- IETF http://www.ietf.org/
- (財) 日本ネットワークインフォメーションセンター (JPNIC) http://www.nic.ad.jp
- OASIS PKI Technical Committee http://www.oasis-open.org/committees/

- 総務省行政管理局 政府認証基盤(GPKI) http://www.gpki.go.jp/
- 「ユビキタス時代のバイオメトリクスセキュリティ」瀬戸洋一著
- 「企業システムのための PKI」塚田孝則著
- 「PKI ハンドブック」小松文子著
- "ISO/IEC 7816-1:1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics"
- "ISO/IEC 7816-1:1998/Amd 1:2003 Maximum height of the IC contact surface"
- "ISO/IEC 7816-2:1999 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 2: Dimensions and location of the contacts"
- "ISO/IEC 7816-3:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols"
- "ISO/IEC 7816-3:1997/Amd 1:2002 Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V"
- "ISO/IEC 7816-4:1995 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange"
- "ISO/IEC 7816-4:1995/Amd 1:1997 secure messaging on the structures of APDU messages"
- "ISO/IEC 7816-5:1994 Identification cards -- Integrated circuit(s) cards with contacts -- Part 5: Numbering system and registration procedure for application identifiers"
- "ISO/IEC 7816-5:1994/Amd 1:1996"
- "ISO/IEC 7816-6:1996 Identification cards -- Integrated circuit(s) cards with contacts -- Part 6: Interindustry data elements"
- "ISO/IEC 7816-6:1996/Amd 1:2000 IC manufacturer registration"
- "ISO/IEC 7816-7:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)"
- "ISO/IEC 7816-8:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 8: Security related interindustry commands"
- "ISO/IEC 7816-9:2000 Identification cards -- Integrated circuit(s) cards with contacts -- Part 9: Additional interindustry commands and security attributes"
- "ISO/IEC 7816-10:1999 Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards"
- "ISO/IEC FDIS 7816-11 Identification cards -- Integrated circuit cards with contacts -- Part 11: Personal verfication through biometric methods"
- "ISO/IEC 7816-15 Identification cards -- Integrated circuit cards with contacts -- Part 15: Cryptographic information application"
- "ISO/IEC 14443-1:2000 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 1: Physical characteristics"
- "ISO/IEC 14443-2:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity

cards -- Part 2: Radio frequency power and signal interface"
- "ISO/IEC 14443-3:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision"
- "ISO/IEC 14443-4:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 4: Transmission protocol"
- IC カードシステム利用促進協議会, "JICSAP IC カード仕様 V2.0 第 1 部 接触型 IC カード"
- IC カードシステム利用促進協議会, "JICSAP IC カード仕様 V2.0 第 2 部 近接型 IC カード"
- IC カードシステム利用促進協議会, "JICSAP IC カード仕様 V2.0 第 3 部 共通コマンド"
- IC カードシステム利用促進協議会, "JICSAP IC カード仕様 V2.0 第 4 部 高速処理用 IC カード"
- PC/SC Workgroup, "Interoperability Standards for ICCs and Personal Computer Systems: Part 1. Introduction and Architecture Overview"
- NIST, "Government Smart Card Interoperability Specification Version 2.1"
- Ad Hoc Group on Biometric Interoperability in Support of the Government Smart Card Framework, "Smart Card Biometric Interoperability Study Report"
- RSA Laboratories, "PKCS #11 v2.11: Cryptographic Token Interface Standard"
- RSA Laboratories, "PKCS #15 v1.1: Cryptographic Token Information Syntax Standard"
- Microsoft, "MSDN ライブラリ Microsoft Visual Studio 6.0"
- Global Platform, "GlobalPlatform Card Specification v2.1.1"
- NIST/Biometric Consortium Interoperability, Assurance, and Performance Working Group, "Java Card Biometric API White Paper"
- Smart Card Alliance, "Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems"
- SC17, http://www.sc17.com/
- ISO, http://www.iso.ch/
- 情報規格調査会, http://www.itscj.ipsj.or.jp/
- 日本規格協会, http://www.jsa.or.jp/
- 日本工業標準調査会, http://www.jisc.go.jp/
- IC カードシステム利用促進協議会, http://www.jicsap.com/
- PC/SC Workgroup, http://www.pcscworkgroup.com/
- OpenCard, http://www.opencard.org/
- NIST, http://smartcard.nist.gov/