個人番号カード
プロテクションプロファイル

第1.00版

2014年4月24日

J-LIS 地方公共団体情報システム機構
Japan Agency for Local Authority Information Systems

JISEC C0431

(空白ページ)

このPPについて

PPの背景、及びPPを満たすカード製品開発について説明する。

個人番号カードのセキュリティ要件

本PPは、個人番号カードに対するセキュリティ要件を規定する。調達者に納入される個人番号カードは、セキュリティ評価の国際規格であるCCに基づく評価を受け、適切なセキュリティ対策が施されていることを実証しなければならない。CC評価を受ける個人番号カードは、本PPが提示する要件をすべて満たさねばならない。

セキュリティ評価の範囲

個人番号カードは、ICモジュール端子インタフェースと非接触インタフェースの両方を備えたICカードである。ICカードのハードウェア及び搭載されるソフトウェアを合わせた、製品全体がCC評価の対象となる。

評価において、コンポジット評価を適用してもよい。ICカードのハードウェア部分が既に評価済みの場合、コンポジット評価によって、既に評価済みのハードウェア部分の評価を省略できる。新たな評価が必要になるのは、ソフトウェアによるセキュリティ機能と、ソフトウェア・ハードウェアの協働によって実現されるセキュリティ機能である。

コンポジット評価を適用しない場合、ICカード製品全体に対して評価が実施されねばならない。

ST作成

開発者は、CC評価を受けるため、本PPに適合するSTを作成しなければならない。評価対象（TOE）は、コンポジット評価適用の有無に関わらず、ICカード全体である。

本PPは、適合を主張するSTに対し、論証適合を要求する。すなわち、PPへの適合を主張するSTは、PPに記述された一般的なセキュリティ課題に対する解を提供しなければならない。すなわち、ST作成者は、PPの記述に対し、同等か、あるいはより制限的な方法をとらねばならない。

ハードウェアのセキュリティ要件

本PPのTOE種別は、組み込みソフトウェアを含むICカード（スマートカード）である。ICカードというカテゴリに属するTOEでは、ハードウェアに関わるセキュリティ要件がほぼ一定の枠内に収まる。本PPは、特定のPPへの適合を主張しないが、ハードウェアに関わるセキュリティ要件を定めるにあ

たり、BSI-PP-0035として認証された “Security IC Platform Protection Profile, v1.0, 15.06.2007” を参考にした。BSI-PP-0035は、多くのスマートカード向けST/PPが適合を主張した実績を持っている。本PPのハードウェアに関わる要件は、BSI-PP-0035に規定された要件範囲を超えていないので、同PPに適合するTOEは、本PPのハードウェア部分の要件をすべて満たす。

ICカードのTOE評価では、JIWG supporting documentsが適用される。同文書は、物理的攻撃を主体とするICカード特有の攻撃を対象とし、CCとCEMを補足する。物理的攻撃は、ICカードのハードウェアに向けられる攻撃である。ハードウェアはTSFに相当するパーツであり、TSFに対する攻撃は、それがSTの脅威や組織のセキュリティ方針に明示されずとも、脆弱性分析の観点から評価の対象になる。同文書は、CC/CEMのバージョンと独立して随時改訂される。本PPに適合するTOE評価は、同文書の最新のバージョンを使用して実施される。

コンポジット評価

ソフトウェアとハードウェアを一体化した個人番号カードのセキュリティ評価を実施する際、ハードウェア部分が評価済みなら、コンポジット評価を適用して評価の重複を避けることができる。

コンポジット評価は、JIWG supporting documentsに規定される。その評価・認証結果は、CCRAに加盟するすべての制度下で有効である。コンポジット評価への対応を以下に説明する。

ICカードへのセキュリティ要件は、以下の方法で対応される。

(a) ハードウェアのセキュリティ機能で対応する。

(b) ソフトウェアのセキュリティ機能で対応する。

(c) ハードウェアとソフトウェアの組み合わせによるセキュリティ機能で対応する。

(a) に相当するセキュリティ機能は、ICチップをTOEとして既に評価済みである。従って、(b) と (c) に該当する部分を追加すれば、カード全体としてのセキュリティ機能を評価できる。すなわち、本PPのセキュリティ要件のうち、純粋にハードウェアだけで実現されるセキュリティ機能を除く部分がコンポジット評価の対象である。

(c) に該当するのは、ハードウェアのセキュリティ機能をソフトウェアで補完するようなケースである。例えば、DPA (差分電力分析) による暗号鍵暴露攻撃に対抗するため、暗号演算プログラムを工夫し、消費電力分析による暗号鍵の推定をし難くする。

コンポジット評価においては、ハードウェア評価とコンポジット評価のスキーム (各国のCC評価・認証制度) が異なるケースの場合、特に注意が必要である。ハードウェア評価の結果を滞りなくコンポジット評価のスキームで利用できることが必要である。すべての関係組織間で、事前調整を十分に行っておくことが求められる。

目次

1 PP概説

1.1 PP参照

タイトル: 個人番号カード プロテクションプロファイル
版数: 1.00
発行: 2014年4月24日
発行者: 地方公共団体情報システム機構
登録: C0431
キーワード: ICカード、スマートカード、住民基本台帳、住民基本台帳ネットワークシステム、個人番号カード、住基カード、公的個人認証、JPKI、券面事項入力補助、券面事項確認、条例利用AP

1.2 TOE概要

1.2.1 TOE種別

TOEは、ICカードである。日本の社会保障・税番号制度で使用される、特定用途向けの製品である。

1.2.2 TOEの用途

TOEは、日本の共通番号法に基づき、共通番号制度において“個人番号カード”として使用される。

(1) TOEの構造

TOEは、ハードウェアとソフトウェアから構成される。

TOEのハードウェアは、ICチップと物理的外部インタフェース部品が埋め込まれたプラスチックカードである。物理的外部インタフェースは、ICモジュール端子インタフェースと非接触インタフェースの両方を備える。カード券面には、カード保持者の氏名、顔写真などが印刷される。

TOEのソフトウェアは、個人番号カードのサービスを提供するプログラムとデータである。このソフトウェアは、プラットフォームとAP (Application program) から成る。プラットフォームは、APの動作環境を提供する。プラットフォーム上のAP動作環境は、セキュリティドメイン (SD) と呼ぶ論理的領域に区分され、管理される。プラットフォーム上に複数のSDを設定でき、APは、それが属するSD内で動作する。SDの中にさらにSDを置くこともできる。プラットフォーム全体をカバーする一つのSDがあり、それを発行者SD (ISD) と呼ぶ。ISDは、あらかじめ開発環境で設定される。ISD以外のSDはすべてサプリメンタリーSD (SSD) と呼ばれ、ISDの内部に設定される。SSDは、運用環境で設定・削除が可能である。

プラットフォーム上では、用途別に4種のAPが動作する。4種のAPとは、券面事項入力補助AP、住基AP、公的個人認証AP、券面事項確認APである。本PPでは、この4種のAPを「基本AP」と呼ぶ。基本APは、開発環境でISD上に直接設定され、SSDには属さない。

個人番号カードを交付する地方自治体（市町村）は、それぞれの条例に基づくAP (条例利用AP) を追加搭載できる。条例利用APはSSDに置かれ、基本APと区別される。

基本APの用途を以下に簡単に説明する。次節 (2) では、それぞれを詳しく説明する。

- 券面事項入力補助AP　カード保持者の個人番号と4情報（氏名・住所・生年月日・性別）をテキストデータで利用者に提供する。利用者とは、個人番号を取り扱う事業者、カード保持者の本人確認を必要とする事業者等である。
- 住基AP　住基ネットシステムにおける住民基本台帳カード（住基カード）と同一の機能を提供する。
- 公的個人認証AP　カード保持者の電子申請に使用する署名用証明書、カード保持者の電子認証に使用する電子証明書（利用者証明用証明書）を発行する。
- 券面事項確認AP　カード券面に印刷された4情報（氏名・住所・生年月日・性別）、個人番号、顔写真、有効期限を提供する。

次に、TOEの構成を説明する。TOEの内部構成例を図1-1に示す。図1-1は、TOEの動作を説明するためにTOEの主要構成要素を示したもので、TOEの実装方法を特定したり制限したりするものではない。

TOEのソフトウェアは、プラットフォームと4つの基本APである。これらは、それぞれのサービスを利用者に提供する。ここでいうサービスの提供とは、TOEの利用者がその権限に応じてTOEの機能を利用することを言う。サービスは、TOEに格納されたデータの読み出しだけに限定されない。TOEへのデータ格納・更新機能、TOEの演算機能など、利用者によるTOEとのインタラクション

は、すべてTOEが提供するサービスの利用に相当する。条例利用APは地方自治体ごとのオプションであり、TOEの構成要素には含まれない。

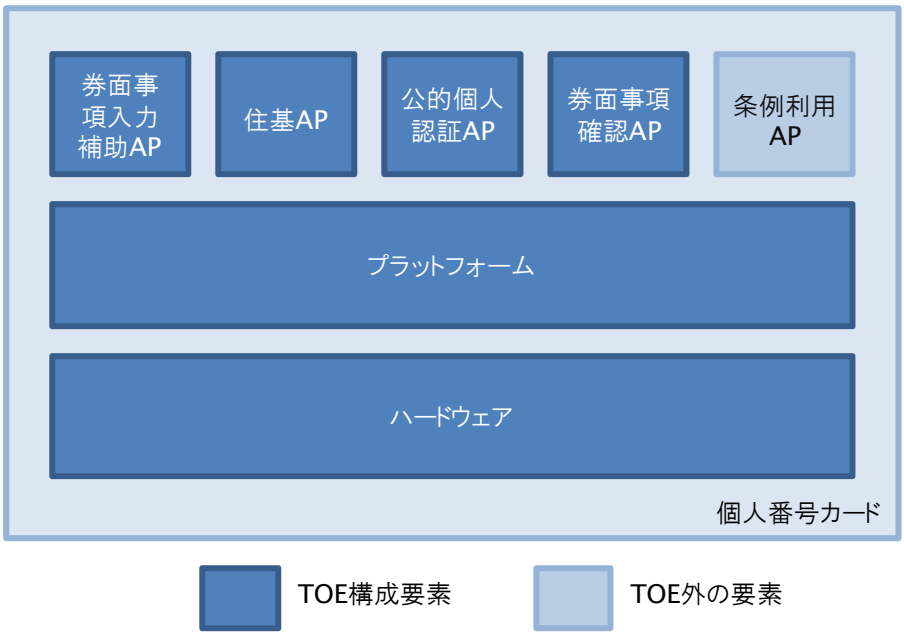

図1-1　TOEの構成

(2)　基本APが提供するサービス

個人番号カードは、市町村の地方自治体を介して住民に交付される。TOEが搭載する4つの基本APは、以下に示すサービスを提供する。サービスのいくつかは、地方自治体業務だけでなく、民間事業者の業務でも利用できる。サービスの利用には、原則として利用者認証が必要である。しかし、特定のいくつかのデータは、利用者認証なしで読み出せる。

[券面事項入力補助AP]

「社会保障・税番号制度」に基づき、カード保持者に付与された個人番号及び4情報を提供するアプリケーションである。4情報とは、カード保持者の氏名、住所、生年月日、性別を言う。これらのデータは、テキスト形式でTOEに格納され、認証された利用者によって読みだされる。

[住基AP]

住民基本台帳ネットワークシステム用カードアプリケーションである。住基ネット（住民基本台帳ネットワークシステム）のサービスを利用するためのAPで、従来の「住基カード」と同一の機能を提供する。カード保持者の住民票コードが格納され、地方自治体に設置された専用装置を用いて読み出す。

[公的個人認証AP]

個人向けの公的認証サービスを提供するアプリケーションである。電子申請等に必要な「署名用証明書」、あるいはカード保持者の電子認証に使用する「利用者証明用証明書」の署名等に使用される。上記二つの用途ごとに、カード保持者の公開鍵・秘密鍵ペア及び証明書をTOEに格納する。カード内で、署名に関わる暗号演算を実行する。

[券面事項確認AP]

券面の印刷情報を提供するアプリケーション。券面には、4情報、個人番号、顔写真、有効期限が印刷されている。この印刷情報全体を券面事項情報と呼び、券面事項情報を一つの画像データとしてカードに格納する。さらに、個人番号だけを別の画像データとして格納する。券面の印刷改ざんが疑われる場合など、券面事項情報（または、個人番号）を外部端末画面に表示して比較検証する。さらに、生年月日のテキストデータを保管し、カード保持者の年齢確認が必要な場合などに使用する。これらの格納データは券面の印刷情報と同一なので、機密情報ではない。しかし、カード保持者に気付かれずにデータが読みだされたりしないよう、読出し時にパスワードを要求する。

1.2.3 主要セキュリティ機能

TOEは、その情報資産を保護するためのセキュリティ機能（security features）を備える。TOEのソフトウェア部分（プラットフォームと基本AP）は、外部インタフェースを介した論理的アクセスを管理する。すなわち、利用者を識別・認証し、利用者の権限に応じてTOEの情報・資源を利用させる。プラットフォームと4つの基本APは、すべて独立したソフトウェアであり、それぞれの利用者とサービス機能を別個に規定する。従って、TOEのセキュリティ機能要件（security functional requirements: SFR）は、それぞれのソフトウェア種別に応じて規定される。

本章では、TOE全体としてのセキュリティ機能（security features）を説明する。ソフトウェアごとに異なる部分は、3章以降で記述する。一方、TOEのハードウェアは、各ソフトウェアから共通資源として使用される。ハードウェアは、ソフトウェアの動作環境を提供するとともに、ハードウェア自身への攻撃にも対抗する。

以下、TOEの主要なセキュリティ機能（security features）を説明する。

[注釈_Security features] セキュリティ機能の後に“ (security features)”を付加した表記は、本節の記載が“security function”を対象にしたものでないことを明示するためのものである。どちらの英語表記も日本語では「セキュリティ機能」になるが、意味が異なる。“Security features”は、TOEセキュリティ機能の厳密な定義でなく、TOEの特徴的なセキュリティ特性を消費者に理解しやすい記述で説明したものである。

(1) 通信データ保護

TOEは、ICモジュール端子インタフェースと非接触インタフェースの二つの通信インタフェースを介して外部端末と通信する。盗聴・改変から保護が必要な通信は、“セキュアメッセージング”機能を適用して通信データ暗号化・復号及び/またはMAC (Message Authentication Code) 生成・検証を行い、機密性及び/または完全性を保護する。

(2) 利用者認証とアクセス制御

TOEは、利用者の権限に応じたサービスを提供するため、サービスごとに利用者認証を行い、アクセス制御を実施する。サービスとは、利用者にTOEの機能を利用させることを言う。例えば、TOEのファイルに格納されたデータ (ex. 個人番号) の読出し、署名機能の利用などである。条例利用AP (オプションであり、TOE外) を追加・削除する機能も、TOEのサービスに該当する。

典型的なICカードのセキュリティメカニズムでは、まず、利用者が処理対象 (ファイルや演算機能など) を選択する。TOEは、その処理対象のセキュリティ属性に基づき、利用者認証を行う。利用者認証に成功すると、TOEは、そのセキュリティ属性に基づいて処理対象へのアクセスを許可する。許可されるアクセスの内容も、セキュリティ属性の一つとして処理対象に設定される。

TOEの利用者には、人間利用者と外部端末の2種類がある。人間利用者とは、カード保持者、管理者[1]、カードのデータを利用する事業者などである。外部端末とは、TOEとデータを直接やり取りするIT装置である。TOEは、利用者認証に適用する認証メカニズムとして、パスワード方式と公開鍵暗号方式を備える。TOE (ICカード) が外部のIT装置 (外部端末) を認証することを、ICカード分野では、「外部認証[2]」と呼ぶ。外部認証と対の機能として、内部認証と呼ばれるものがある。ICカー

[1] 本PPにおいて、“管理者”とは、 ICカード交付者 (地方公共団体情報システム機構及び市町村の地方自治体) に属し、TOEのセキュリティ機能に関わる管理機能の運用権限を有する者を指す。管理者は、ICカード交付時のデータ設定、条例利用APの設定、カード交付後のデータ書き換えなどを行う。

[2] “外部認証”は、狭義の意味として、TOEであるICカードが特定の外部端末を暗号アルゴリズムに基づき認証することを指す。本PPでは、3章及び4章で具体的な認証メカニズムに言及する場面で、この狭義の意味を適用する。

ドが偽造品でないことを確認したい場合に、利用者である外部端末側がICカード（TOE）を認証する機能である。内部認証は、外部端末側のセキュリティのために必要なものである。TOEは、内部認証に対応するための暗号機能を備える。

(3) 暗号演算

TOEは、プラットフォームや各APのサービスに関わる暗号演算機能を提供する。暗号演算機能は、セキュアメッセージング、利用者認証、あるいは、公的個人認証APにおける署名・利用者証明などに使用される。

(4) 物理的攻撃への対抗

TOEのセキュリティ機能は、自身のハードウェア部分への物理的攻撃にも対抗する。想定される攻撃は、一般のICカードと同様である。例えば、ICチップ内部への物理的操作やプロービングによる情報の暴露・改変、あるいは、TOEの消費電力や電磁放射の観測・分析による暗号鍵暴露など、物理的手段を用いる多様な攻撃が存在する。TOEのハードウェア部分は、すべて、TSFの一部である。TSFに対する攻撃は、PPの脅威記述の有無に関わらず、脆弱性分析の評価対象になる。ICチップの脆弱性分析に関わる評価は、JIWG supporting documentsに示される評価方法に従って行われる。

1.2.4 TOEの動作に必要なIT環境

TOEは、個人番号カードに必要な組み込みソフトウェアと、そのソフトウェアが動作するハードウェアを一体化したICカードである。TOEは他のIT環境に依存せずに動作するが、動作に必要な電力は外部端末から供給される。

TOEの構成要素であるプラットフォームと基本AP（4種類）は、それぞれ利用方法が異なる。TOEを利用する者（地方自治体、国家機関、民間機関、個人など）は、利用目的に応じた端末装置等の準備が必要である。

1.2.5 TOEのライフサイクル

TOEのライフサイクルを説明する。ここに示すライフサイクルは、TOEを理解するための参考情報であり、開発方法や開発環境を特定するものではない。本PPに適合するPP/STの作成者は、本節の記述に関わらず、実際の環境に即したライフサイクル記述を行うことができる。

(1) ICチップ（ハードウェア）開発

ICチップ開発者によって、個人番号カードに埋め込まれるICチップが開発される。ICチップ製造に使用されるフォトマスク開発、ICチップ専用ソフトウェア/ファームウェア開発もこの工程に含まれる。

ICチップへのソフトウェア組込み（ソフトウェア開発は、(2) に示すフェーズで行われる）は、このフェーズか、あるいは (3) のフェーズで実施される。

ハードウェア開発に関わるこのフェーズでは、開発が複数サイトに分散することが多い。ハードウェア回路設計、ICチップ製造のためのマスク設計・製造、ICチップ製造など、多様な工程が異なる開発サイトで実施されるかもしれない。

(2) プラットフォーム及び基本AP開発

ソフトウェア（プラットフォーム及び基本AP) が開発される。これらソフトウェア開発は、(1) に示すハードウェア開発と独立して行うことができる。

(3) 個人番号カード製造

本PPのTOEに対応するソフトウェアがICチップに埋め込まれ（あるいは、ハードウェア製造の一環でソフトウェアが埋め込まれるかもしれない）、さらにICチップと非接触通信用アンテナがプラスチックカードに埋め込まれて個人番号カードが製造される。条例利用APがこの段階で搭載されることもある。この段階までがライフサイクル上の開発フェーズに相当する。製造された個人番号カードは、地方公共団体情報システム機構へ納付される。

(4) 個人番号カード交付

地方公共団体情報システム機構へ納付された個人番号カードは、市町村の地方自治体を経て、カード保持者となる住民に交付される。カード交付に際し、地方公共団体情報システム機構、あるいは地方自治体の管理者によって、カード保持者の固有情報を含む必要データが書き込まれる。この手続きは、カードのパーソナライゼーションと呼ばれる。本PPのTOEのライフサイクルにおいて、本項以降が運用フェーズに相当する。

(5) 地方自治体による条例利用APの追加

個人番号カード交付窓口となる市町村の地方自治体が独自の条例利用APを追加搭載することがある。条例利用APは、地方自治体によるオプションであり、必ず搭載されるものではない。

(6) 個人番号カード保持者による利用

個人番号カードを交付された住民はカード保持者と呼ばれ、個人番号カードのサービス機能を利用する。カード保持者のほか、個人番号カードのサービスに関わる各種組織が個人番号カードを利用する。サービスに関わる組織とは、地方自治体、国家機関、あるいは、法律等で個人番号カードのサービス利用を許可された民間事業者等である。

2 適合主張

2.1 CC適合主張

本PPは、以下のとおりCC適合を主張する。

- CC適合: CCバージョン3.1 改訂第4版適合 (日本語版: パート1、2、3のいずれもIPAによる「翻訳第1.0版」を使用)

  パート1: 概説と一般モデル 2012年9月 バージョン3.1 改訂第4版 CCMB-2012-09-001

  パート2: セキュリティ機能コンポーネント 2012年9月 バージョン3.1 改訂第4版 CCMB-2012-09-002

  パート 3: セキュリティ保証コンポーネント 2012年9月 バージョン3.1 改訂第4版 CCMB-2012-09-003

- パート2適合: CCパート2拡張

  定義した拡張セキュリティ機能コンポーネントは、FCS_RNG.1である。 (5章に定義を記述)

- パート3適合: CCパート3適合

2.2 PP主張

本PPは、他のPPへの適合を主張しない。

2.3 パッケージ主張

本PPは、EAL4追加を主張する。

追加する保証要件は、ALC_DVS.2及びAVA_VAN.5である。

2.4 適合根拠

本PPは、他のPPへの適合を主張しないので、適合根拠の記述を行わない。

2.5 適合ステートメント

本PPへの適合を主張するPP/STは、論証適合を主張しなくてはならない。

3 セキュリティ課題定義

本章では、TOEに関わるセキュリティ課題を定義する。セキュリティ課題は、脅威（TOE及び/または環境で対抗する）、組織のセキュリティ方針（TOE及び/または環境で対処する）、前提条件（環境で満たす）の三つの側面から定義される。これらのセキュリティ課題は、TOEのライフサイクルにおける運用フェーズに関わるものである（1.2.4参照）。TOE及び環境は、これらのセキュリティ課題に適切な形で対応しなければならない。

脅威、組織のセキュリティ方針、前提条件は、それぞれ、先頭が“T.”、“P.”、“A.”で始まる識別名が付与される。必要に応じて［注釈］を付記するが、［注釈］は、本PPの内容が誤解なく理解されることを目的とした参考情報である。セキュリティ課題定義の一部ではないので、PP/ST作成時に引用する必要はない。

3.1 利用者

本TOEに関わる利用者を説明する。TOE利用者は、以下に示す4つのカテゴリに分類できる。このカテゴリは、利用者の役割に応じた分類である。以下では、TOEを利用する観点から、各役割のTOE利用者を説明する。

- カード保持者　居住する市町村の地方自治体から個人番号カード（TOE）を交付された利用者。カード保持者は、TOEの基本AP、及び市町村の地方自治体が提供する条例利用AP（オプションであり、TOE外）のサービス機能を利用する。サービス内容に応じて、地方自治体窓口の外部端末やカード保持者所有のPC等が使用される。
- 管理者　運用環境でTOEの管理に関わる者。管理とは、TOEに対し、条例利用APの生成・削除、プラットフォームやAPのデータ設定・変更、あるいは、パスワードの閉塞解除など、TOEを適切に運用するための業務である。管理者は、地方公共団体情報システム機構、あるいは市町村の地方自治体に所属する。
- 機関・組織等　TOEのサービスに関わる各種機関・組織がTOEを利用する。サービスに関わる機関・組織とは、地方自治体、国家機関、あるいは、法律等で

TOEのサービス利用を許可された民間事業者等である。なお、本項の利用者は、PPにおいて、「××を扱うシステム」のように表記される。

- 外部端末　TOEの運用環境では、TOEと外部端末（TOEの外部に位置するIT装置）間でデータ授受が行われる。外部端末は、市町村の地方自治体窓口等に設置される。不正な外部端末が使用されるとTOEの保護資産が侵害されるので、外部端末は、TOE利用者として識別・認証の対象となる。なお、公的個人認証APでカード保持者が使用する自身のPC等、あるいは券面事項確認APで民間事業者が券面事項情報等を読み出すために使用する端末は、TOEから利用者として識別されず、本項の「外部端末」に相当しない。

3.2 保護資産

TOEのセキュリティ機能（TSF）が保護する情報資産は、TOEに格納される利用者データと、TOEが利用者に提供する演算機能である。利用者データは、カード保持者のために使用されるデータであり、カード保持者にとって価値がある情報である。利用者データの例は、「社会保障・税番号制度」に基づくカード保持者の個人番号である。利用者に提供する演算機能の例は、公的個人認証のため、公開鍵暗号を使用し、カード保持者の電子署名を実行する機能である。

TOEの利用者データ及び利用者に提供する演算機能は、TSFによる保護対象であり、一次資産と呼ばれる。一次資産は、PP/STの脅威記述における保護資産として明示される。

一次資産の保護のために必要なTOE資産を二次資産と呼ぶ。TOEのセキュリティ機能（TSF）と、TSFが使用するTSFデータが二次資産に相当する。TSF自身が改ざんされたり、TSFデータが暴露・改変されたりすると、TSFはセキュリティ機能を正しく実行できず、一次資産を保護できない。そのため、TSFとTSFデータも、TSF自身によって保護しなければならない。

二次資産として保護すべき対象は、一次資産の保護メカニズムに依存し、初めから特定する必要はない。PP/STの脅威や組織のセキュリティ方針では、一次資産だけを定義し、二次資産を含めないのが一般的である。しかしながら、本PPでは、ICカードに関わる物理的攻撃（TSFの一部であるハードウェアへの攻撃）を脅威記述に含めた。ハードウェアへの物理的攻撃には、一次資産に対する論理的攻撃と独立したものが含まれる。TOEは、それらの物理的攻撃にも対抗しなければならない。対抗すべき物理的攻撃の範囲は、JIWG supporting documentsで具体的に提示される。物理的攻撃に関わるTOE評価は、評価時点における最新の同文書に従って実施される。

TOEには、市町村の条例に基づく条例利用APを追加搭載できる。条例利用APは、市町村の地方自治体ごとに個別に実施されるサービスである。本PPの規定外であり、その利用者データは、本TOEの保護資産に含まれない。

3.3 脅威

本TOEが対抗すべき脅威を示す。これらの脅威は、TOE、その運用環境、あるいは両者の組み合わせによって対抗されねばならない。

T.Illegal_Attack

正当な利用権限を持たない者が外部インタフェースを使用してTOEにアクセスし、TOEの内部データを暴露・改変したり、TOEの演算機能を不正に利用したりする。正当な利用権限を持たない者とは、TOEの保護された資産へのアクセスに必要な認証データを持たない者をいう。

> [注釈_T.Illegal_Attack] この脅威は、個人番号カードが製造され出荷された後のすべての環境、つまり、カード輸送時、カード交付に関わる組織での保管下、パーソナライゼーションされてカード保持者へ交付された後など、いずれの運用環境でも生じる。

T.Replay

攻撃者は、TOEと外部端末間の通信における認証手順を傍受・記録し、記録した手順を再生してTOEから認証を受け、正規の外部端末になりすます。これによって、TOEの利用者データを暴露・改変したり、TOEの演算機能を不正に利用したりする。

> [注釈_T.Replay] この脅威は、T.Illegal_Attackの一つとも考えられるが、攻撃方法を特定しているので、独立した脅威として定義する。

T.Phys_Attack

攻撃者は、TOEの構成要素（ハードウェア/ファームウェア/ソフトウェア）を物理的手段で攻撃し、その結果として、TOEの利用者データを暴露・改変したり、TOEの演算機能を許可なく使用したりする。典型的な攻撃手法の例を以下に示す。

- 暗号演算中の消費電力変化を観測・分析し、使用された暗号鍵を割り出す。
- TOE内部のプロービングによってデータを暴露する。
- 動作中のTOEにグリッチや環境ストレスを加えてTSF動作の誤りや機能不全を生じさせ、データを暴露・改変したり、TOEの機能を不正に使用したりする。
- TOE内部の物理的操作によって、データを暴露・改変したり、TOEのふるまいを改ざんしたりする。

3.4 組織のセキュリティ方針

TOEあるいは運用環境に適用される組織のセキュリティ方針を示す。「組織」とは、個人番号カードの管理・運用主体である、地方公共団体情報システム機構、及び市町村の地方自治体を指す。

P.Secure_messaging

TOEは、外部端末との通信において、表3-1の「適用」と示された通信にセキュアメッセージングを適用する。「適用または非適用」及び「非適用」と示された通信は、表の注釈に示すとおり、セキュアメッセージング適用は必須でない。

表3-1 セキュアメッセージングの適用

適用箇所	暗号化/復号	MAC生成/検証
プラットフォーム	適用	適用
券面事項入力補助AP	適用または非適用[*1]	適用または非適用[*1]
住基AP	適用（住民票コード読出し）	非適用[*2]
公的個人認証AP	適用または非適用[*1]	適用または非適用[*1]
券面事項確認AP	非適用[*2]	非適用[*2]

[*1] [適用または非適用] TOEは、該当するセキュリティ機能を実装する。外部端末が要求した場合にその機能を使用する。

[*2] [非適用] TOEは、該当するセキュリティ機能を実装してもしなくてもよい。実装した場合、外部端末の要求があれば、その機能を使用してよい。

P.Delivery

開発者から出荷される個人番号カードは、TOEへの不正アクセス防止機能が活性化した状態でなければならない。不正アクセスとは、権限を持たない者によるTOE内部への論理的アクセスを言う。

[注釈_P.Delivery] TOEが開発者から出荷されるとき、TOEセキュリティ機能の一部が有効になっており、TOEへの不正アクセスを防止する。ICカードでは、一般的な名称として“輸送鍵”と呼ばれる認証データがTOEに格納され、輸送鍵を知る者だけがTOEにアクセスできる。攻撃者が輸送中のTOEを盗んでも、輸送鍵を知らなければTOEを初期化できず、使用開始できない。輸送鍵は、輸送時だけに限らず、交付前ICカード保管時の保護手段としても有効である。輸送鍵と同様のセキュリティ特性を持つ認証データとして、“initial key”、“発行者キー”などがある。本PPでは、これらをすべて輸送鍵と呼ぶ。

P.Cryptography

TOEは、プラットフォーム及び基本APが暗号機能を利用できるような環境を提供する。暗号機能は、データ保護のほか、署名、あるいは認証にも使用される。表3-2に、TOEに要求される暗号アルゴリズム、暗号操作、暗号鍵長、暗号鍵管理（鍵の生成/インポート、破棄）、及び暗号機能の用途を示す。

表3-2　暗号機能方針

<table>
<tr><th>暗号アルゴリズム
/標準</th><th>暗号操作</th><th>鍵長
(ビット)</th><th>暗号鍵生成
/インポート</th><th>暗号鍵破棄</th><th>用途</th></tr>
<tr><td>AES-CBC mode
/FIPS PUB 197・
NIST SP 800-38A</td><td>暗号化/復号</td><td rowspan="2">128</td><td rowspan="6">インポート</td><td rowspan="6">本PPでは破棄方法を特定しない</td><td>セキュアメッセージング、
秘密鍵復号(インポート時)</td></tr>
<tr><td>CMAC with AES
/FIPS PUB 197・
NIST SP 800-38B</td><td>MAC 生成/検証</td><td>セキュアメッセージング</td></tr>
<tr><td rowspan="3">RSASSA-PKCS1-
V1.5/PKCS#1
v2.2</td><td>公開鍵による署名検証</td><td rowspan="3">2048</td><td>外部認証</td></tr>
<tr><td>秘密鍵による署名[*1]</td><td>内部認証、
公的個人認証APにおける署名･利用者証明</td></tr>
<tr><td>RSA-
OAEP/PKCS#1
v2.2</td><td>秘密鍵による復号</td><td>セキュアメッセージング用セッション鍵共有、
秘密鍵復号用共通鍵共有[*2]</td></tr>
<tr><td>SHA-256/FIPS
PUB 180-4</td><td>ハッシュ演算</td><td>-</td><td>-</td><td>-</td><td>RSA暗号演算の補助技術として使用</td></tr>
</table>

[*1] 券面事項入力補助AP、公的個人認証AP、券面事項確認APでは、標準に沿った署名生成処理のうち、エンコード処理(ハッシュを含む)を外部端末等の外部装置が行い、TOEはPKCSパディング付与と秘密鍵による署名演算を実施する。なお、公的個人認証APでは、パディングに「機関コード」を追加する機能を併せ持ち、この機能を使用する場合、TOEのパディング付与は標準に準拠しない。

[*2] 公的個人認証APにおける共通鍵のオンライン更新時に適用

P.RND

TSFは、自らが使用する乱数を生成する。乱数は、攻撃者による予測を防止するのに必要な品質を持つ。

[注釈_P.RND]　乱数に求められる品質は、乱数の使用目的に依存する。乱数の品質は、客観的な品質尺度で表現することが望ましい。品質尺度の例は、エントロピーを単位とした数値である。

3.5 前提条件

TOEの運用環境で対処されるべき前提条件を示す。これらの前提条件は、TOEのセキュリティ機能性が効果を発揮するために必要である。

A.PKI

TSFが有効に動作するため、TOEの公開鍵暗号システム用鍵（公開鍵・秘密鍵のペア）の有効性を証明するPKI環境が提供される。

A.Administrator

TOEのデータあるいはAPの新規設定、変更もしくは削除を行う管理者は信頼できる利用者であり、許可された権限の範囲において、TOEを適切に操作する。

A.AP

条例利用APの搭載に責任を持つ者は、信頼できる開発者によって適切な開発手法に基づいて開発されたAPをTOEに搭載する。

4 セキュリティ対策方針

3章に示したセキュリティ課題に対し、TOE及びその運用環境に対するセキュリティ対策方針を示す。TOEによって対処するセキュリティ対策方針を4.1に、TOEの運用環境によって対処するセキュリティ対策方針を4.2に記載する。これらのセキュリティ対策方針がセキュリティ課題に対して適切であることの根拠は、4.3に示される。

TOEのセキュリティ対策方針、運用環境のセキュリティ対策方針は、それぞれ、先頭に “O.”、“OE.” を付与した識別名で表す。

4.1 TOEのセキュリティ対策方針

セキュリティ課題として定義された脅威と組織のセキュリティ方針に関して、課題解決のためにTOEが対処すべきセキュリティ対策方針を示す。

O.I&A

TOEは、TOE利用者を識別・認証し、認証に成功した利用者に利用者役割に応じた権限を付与しなければならない。識別・認証の対象となる利用者、利用者の権限は、表4-1に示すとおりである。利用者認証には、パスワード（PW）や輸送鍵などの秘密情報照合、あるいは、公開鍵暗号方式による認証メカニズムを使用する。

[注釈_O.I&A] 認証メカニズムと利用者権限の詳細は、調達者から別途仕様が提示される。

表4-1 利用者と権限

適用箇所	利用者	権限
プラットフォーム	プラットフォーム管理者	データ設定･変更、SSD生成･削除
	条例利用AP管理者	条例利用AP生成･削除
券面事項入力補助AP	券面事項入力補助AP管理者	データ設定･変更
	カード保持者	個人番号･4情報の読出、自身のPW変更
	個人番号･4情報を扱うシステム	個人番号･4情報の読出
住基AP	住基AP管理者	データ設定･変更
	カード保持者	住民票コード読出、自身のPW変更
	住基データを扱うシステム	住民票コード読出
公的個人認証AP	公的個人認証AP管理者	データ設定･変更
	カード保持者	署名機能/利用者証明機能の利用、自身のPW変更

	証明書データを扱うシステム	利用者証明機能の利用
券面事項確認AP	券面事項確認AP管理者	データ設定･変更
	カード保持者	券面事項情報読出し
	券面事項情報を扱うシステム	券面事項情報の読出し、カード保持者PWの変更
	個人番号を扱うシステム	個人番号の読出し
	生年月日を扱うシステム	生年月日の読出し
プラットフォームと基本APに共通	外部端末	セッションキー暗号化用公開鍵読出し(券面事項確認APを除く) 内部認証用公開鍵読出し

O.Access_Control

TOEは、管理下のTOE内オブジェクトに対し、TOE内サブジェクトによる権限範囲内のアクセスを許可し、それ以外のアクセスを禁止しなければならない。サブジェクトとは、TOE内の能動的プロセスであり、オブジェクトに対する操作を実行する。サブジェクトは、TOE利用者に関連付けられ、認証された利用者を代行してオブジェクトを操作する。オブジェクトは、サブジェクトに操作される、TOE内の受動的エンティティである。オブジェクトの例は、TOE内の利用者データファイル、条例利用AP、SSD、あるいは演算機能である。操作とは、利用者データ入出力、演算機能の実行、オブジェクトの生成・削除などである。

サブジェクト、オブジェクト、及びサブジェクトによるオブジェクトの操作は、TOEのアクセス制御規則に従う。アクセス制御規則は、表4-2に示される。TOE利用者が認証に成功したとき、その利用者を代行するサブジェクトは、表4-2に示すとおり、オブジェクトに対する操作が許可される。

表4-2　TOEのアクセス制御

適用箇所	サブジェクト(対応する利用者)	オブジェクト	操作
プラットフォーム	プラットフォーム管理者	利用者データを格納するファイル*	書込み及び/または読出し*
		SSD	生成･削除
	条例利用AP管理者	条例利用AP	生成･削除
券面事項入力補助AP	券面事項入力補助AP管理者	利用者データを格納するファイル*	書込み及び/または読出し*
	カード保持者	個人番号ファイル 4情報ファイル	読出し
	個人番号･4情報を扱うシステム		
住基AP	住基AP管理者	利用者データを格納するファイル*	書込み及び/または読出し*
	カード保持者	住民票コードファイル	読出し
	住基データを扱うシステム		

公的個人認証AP	公的個人認証AP管理者	利用者データを格納するファイル*	書込み及び/または読出し*
	カード保持者	署名用秘密鍵による署名機能 利用者証明用秘密鍵による署名機能	署名
	証明書データを扱うシステム	利用者証明用秘密鍵による署名機能	
券面事項確認AP	券面事項確認AP管理者	利用者データを格納するファイル*	書込み及び/または読出し*
	カード保持者	券面事項情報を格納するファイル	読出し
	券面事項情報を扱うシステム		
	個人番号を扱うシステム	個人番号を格納するファイル	
	生年月日を扱うシステム	生年月日を格納するファイル	
プラットフォームと基本APに共通	外部端末	セッション鍵暗号化用公開鍵ファイル(券面事項確認APを除く) 内部認証用公開鍵ファイル	読出し

* オブジェクト「利用者データを格納するファイル」とその操作は、本PPでは特定されない。詳細仕様は、調達者から別途提示される。

O.Replay

TOEの外部認証において、攻撃者による認証データの複製・再使用を防ぐため、同一認証データを再使用してはならない。

O.Secure_messaging

TOEは、外部端末との通信において、表3-1に示すとおりセキュアメッセージングを適用しなければならない。セキュアメッセージングでは、通信データの暴露・改変を防ぐため、表3-2に示す共通鍵暗号アルゴリズムを適用し、暗号化・復号及び/またはMAC (Message Authentication Code) 生成・検証による通信データの保護を行わねばならない。

TOEと外部端末の通信は、コマンド（入力）とレスポンス（出力）の二つからなる。この両方に同一のセキュアメッセージングを適用する。セキュアメッセージングのセッション確立手順において、外部端末との相互認証には、P.Cryptographyの表3-2のRSA暗号アルゴリズムとSHA関数を使用する。セッション鍵(暗号鍵、MAC鍵) の交換には、 表3-2の「セキュアメッセージング用セッション鍵共有」に示すRSA暗号アルゴリズムを使用する。

O.Delivery

開発者が出荷する個人番号カードは、カード内部に秘密の認証データを格納し、その認証データを知らない者がカード内部にアクセスするのを禁止しなければならない。この対策手段は、プラットフォームと4つの基本APそれぞれが個別に実施する。

O.Cryptography

TOEは、プラットフォーム及び基本APが使用する暗号演算機能及び暗号鍵管理機能を提供しなければならない。

プラットフォーム及び基本APに適用される暗号機能は、P.Cryptographyの表3-2に示された方針に従わねばならない。表3-2では、TOEに要求される暗号アルゴリズム・暗号操作・暗号鍵長・暗号鍵管理（生成/インポート、破棄）、及び用途が定義される。

O.Phys_Attack

TSFは、TOEの構成要素（ハードウェア/ファームウェア/ソフトウェア）に対する物理的攻撃によって、TOE内のデータが暴露・改変されたり、TOEの機能が許可なく使用されたりすることを防止しなければならない。

TSFが対抗すべき物理的攻撃は、JIWG supporting documentsに提示される。

> [注釈_O.Phys_Attack]　上記文書が扱う攻撃は、スマートカードに対する攻撃全般であり、物理的攻撃だけに限定されない。一方、O.Phys_Attackは、TOEのソフトウェアだけでは対応できない、物理的手段による攻撃を対象にしたものである。対象範囲が同文書と同じでないことに注意すること。

O.RND

TSFは、TSFが使用する乱数の用途に応じ、必要な品質尺度を満たす乱数を生成しなければならない。さらに、TSFは、生成される乱数を攻撃者が予測するのに利用できる情報の提供を防がねばならない。

4.2 運用環境のセキュリティ対策方針

セキュリティ課題として定義された脅威、組織のセキュリティ方針及び前提条件に関して、課題解決のためにTOEの運用環境において対処すべきセキュリティ対策方針を示す。なお、ここに記載するセキュリティ対策方針は、すべて前提条件に由来する。

OE.PKI

カード交付に関わる組織において個人番号カードの管理・運用に責任を持つ者は、TOEの運用環境において、TOEの公開鍵暗号システム用鍵（公開鍵・秘密鍵のペア）の有効性を証明できるPKIシステムを準備する。

OE.Administrator

カード交付に関わる組織における個人番号カードの管理・運用に責任を持つ者は、TOE内のデータまたはAPの新規設定、変更あるいは削除を担当する管理者の選定において、該当するIT装置を正しく操作でき、かつTOEの保護資産に対して悪意ある行為をしない者を管理者として選定し、それらの行為を行う権限を付与する。さらに、該当するIT装置として、信頼できる装置を選定・導入する。

OE.AP

市町村の地方自治体において個人番号カードの管理・運用に責任を持つ者、あるいはTOEの管理者は、TOEに条例利用APを搭載する際、そのAPが信頼できる開発者によって適切な開発手法に基づいて開発されたものであることを確認し、信頼できない条例利用APを搭載しない。

4.3 セキュリティ対策方針根拠

本章では、上述のセキュリティ対策方針がセキュリティ課題定義の各項目に対して有効であることの根拠を示す。4.3.1では、各々のセキュリティ対策方針がいずれかのセキュリティ課題にさかのぼれること、4.3.2では、各々のセキュリティ課題が対応するセキュリティ対策方針によって有効に対処されることを説明する。

4.3.1 セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義とセキュリティ対策方針の対応を表4-3に示す。ここに示すとおり、すべてのセキュリティ対策方針は、一つ（以上）のセキュリティ課題定義の項目にさかのぼることができる。

表4-3 セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ対策方針 / セキュリティ課題定義	O.I&A	O.Access_Control	O.Replay	O.Phys_Attack	O.Secure_messaging	O.Delivery	O.Cryptography	O.RND	OE.PKI	OE.Administrator	OE.AP
T.Illegal_Attack	x	x									
T.Replay			x								
T.Phys_Attack				x							
P.Secure_messaging					x		x				
P.Delivery	x					x					
P.Cryptography							x				
P.RND								x			
A.PKI									x		
A.Administrator										x	
A.AP											x

4.3.2 セキュリティ対策方針の根拠説明

TOE及び環境に対するセキュリティ対策方針によって、脅威がすべて対抗され、組織のセキュリティ方針が実施され、さらに、前提条件が満たされることの根拠を示す。

T.Illegal_Attack

TOEは、O.I&AによってTOE利用者を識別・認証し、認証に成功した利用者だけに、利用者役割に応じた権限を付与する。さらに、O.Access_Controlによって、利用者の識別情報に基づき、オブジェクトへのアクセスを権限範囲内に制限する。これらのセキュリティ対策方針によって、利用者は、アクセス権限外のデータを暴露・改変したり、サービス機能を不正に利用したりできず、T.Illegal_Attackの脅威を十分に軽減できる。

T.Replay

外部端末における認証手順を攻撃者が傍受・記録し、外部端末になりすましてTOEに認証を試みた場合、O.Replayによって、傍受した認証データは次回の認証では無効であり、認証を拒否される。これによって、T.Replayに示された、同一認証手順の再使用によるなりすましの脅威が除去される。

T.Phys_Attack

O.Phys_Attackが実施されれば、TOEへの物理的攻撃による保護資産のセキュリティ侵害を防止できる。O.Phys_Attackは、JIWG supporting documentsへの対応を示すことで、T.Phys_Attackの脅威をすべてカバーするものとなり、T.Phys_Attackの脅威が十分に軽減される。

P.Secure_messaging

O.Secure_messagingによって、TOEと外部端末間の通信データを暴露・改変から保護する。プラットフォーム及び4つの基本APでは、それぞれのデータに要求される機密性・完全性のレベル、あるいは運用環境が異なる。そのため、P.Secure_messagingの表3-1を参照し、必要な箇所にセキュアメッセージングを適用する。セキュアメッセージングの暗号アルゴリズムは、O.Cryptographyの規定に従って提供される。これらのセキュリティ対策方針によって、P.Secure_messagingが実施される。

P.Delivery

P.Deliveryは、運用環境だけでなく、TOE輸送時のTOE保護要件を含む。このため、運用環境でのTOEに適用するセキュリティ対策方針O.I&Aだけでは不十分で、O.Deliveryによってセキュリティ対策を補完する。

O.Deliveryは、P.Deliveryに対応し、TOEの輸送や保管時の攻撃からTOEを保護する対策方針を規定する。この段階のTOEは、セキュリティ設定が不完全で、十分なセキュリティ特性を発揮できない。しかし、TOE内部へのアクセスに関わる認証機能を有効にすることは可能で、それによってP.Deliveryに対応できる。この認証機能が使用する認証データは、ICカードにおいて、“輸送鍵”と呼ばれる秘密情報である。O.Deliveryは、輸送鍵による認証メカニズムを要求することでP.Deliveryに対応する。O.Deliveryの認証メカニズムはTOEセキュリティ機能の一部であり、O.I&Aに対応するセキュリティメカニズムの一部と重複する。これらセキュリティ対策方針によって、輸送中及びカード交付組織での管理下のTOEに対する不正アクセスが防止され、P.Deliveryが実施される。

P.Cryptography

O.Cryptographyは、P.Cryptographyが規定する暗号機能方針（暗号演算と暗号鍵管理の方針）を示す表3-2を参照し、それに対応することを述べている。O.Cryptographyは、P.Cryptographyを直接実施しており、P.Cryptographyが適切に実施される。

P.RND

O.RNDが実施されれば、TSFの用途に必要とされる品質尺度を満たす乱数が生成され、かつ生成される乱数の予測に利用できる情報が攻撃者に提供されるのを防ぐことができる。O.RNDによって、生成される乱数を攻撃者が予測することが困難になり、P.RNDが適切に実施される。

A.PKI

OE.PKIは、A.PKIの内容に直接対応しており、A.PKIを適切に満たす。

A.Administrator

OE.Administratorは、TOE内のデータまたはAPの新規設定、変更あるいは削除を担当する管理者について、該当するIT装置を正しく操作でき、かつTOEの保護資産に対して悪意ある行為をしない者を選定すること、その管理者に、管理行為に伴う権限を付与することを示している。さらに、管理者が使用するIT装置には、信頼できるものを準備することが示されている。これらの内容は、A.Administratorに記述された内容を適切に満たす。

A.AP

OE.APは、条例利用APが信頼できる開発者によって適切な開発手法に基づいて開発されたものであることの確認を求める。このセキュリティ対策方針は、A.APを直接満たす。

5 拡張コンポーネント定義

本PPでは、拡張セキュリティ機能要件を記述するため、CCパート2に含まれない拡張コンポーネントを定義する。

5.1 拡張セキュリティ機能コンポーネント

本PPで定義する拡張コンポーネントとそれを含むファミリを5.1.1に示す。この拡張ファミリ、拡張コンポーネントは、CCパート2（セキュリティ機能コンポーネント）の既存クラスであるFCSクラスに属する。これらは、CCパート2のファミリ及びコンポーネントをモデルとして構成された。

5.1.1 FCS_RNGファミリの定義

TOEの一部である暗号機能が実施する暗号演算の一つに、乱数生成がある。乱数は、共通鍵暗号の鍵生成、セキュアな鍵交換、相互認証などに使用される。攻撃者から予想されにくい、十分なエントロピーを持つ乱数生成が必要である。CCパート2には乱数生成要件を規定するコンポーネントがないので、乱数生成に関わる拡張コンポーネントを定義する。本項では、まず“FCS_RNG”ファミリを定義し、そのファミリに属する拡張コンポーネントを定義する。これら拡張ファミリと拡張コンポーネントは、以下のPPから引用したものである。

“Security IC Platform Protection Profile” Version 1.0, 15.06.2007; BSI-PP-0035

以下は、同PPのコンポーネント定義を日本語化したものである。

TOEのセキュリティ機能要件を定義するため、FCSクラス（暗号サポート）の追加ファミリ(FCS_RNG)を以下に定義する。このファミリは、暗号に関わる目的で使用される乱数生成への機能要件を記述する。

FCS_RNG 乱数の生成

ファミリのふるまい

このファミリは、暗号に関わる目的で使用することを意図した乱数生成への品質要件を定義する。

コンポーネントのレベル付け

FCS_RNG: 乱数の生成	1

FCS_RNG.1　乱数の生成は、乱数が定義された品質尺度を満たすことを要求する。

管理:　FCS_RNG.1

予見される管理アクティビティはない。

監査:　FCS_RNG.1

予見される監査事象はない。

FCS_RNG.1　乱数生成

下位階層:　なし
依存性:　なし

FCS_RNG.1.1　**TSFは、[割付: *セキュリティ能力のリスト*] を実現する [選択: *物理的*、*非物理的真*、*決定論的*、*ハイブリッド*] 乱数生成器を提供しなければならない。**

FCS_RNG.1.2　**TSFは、[割付: *定義された品質尺度*] を満たす乱数を提供しなければならない。**

[注釈_EXT_FCS_RNG.1] 物理的乱数生成器（乱数生成器: RNG）は、物理的にランダムな処理に基づく雑音源によって乱数を生成する。非物理的真RNGは、人間が関わる操作などの非物理的でランダムな処理（キーボード入力やマウスの動き）を使用する。決定論的RNGは、疑似乱数出力を作り出すランダムなシード（種）を使用する。ハイブリッドRNGは、物理的及び決定論的RNGの原理を組み合わせる。

6 セキュリティ要件

6.1 セキュリティ機能要件

本PPで規定するSFRは、すべてCCパート2に含まれるコンポーネントを使用する。表6-1にSFRのリストを示す。

表6-1 SFRリスト

章番号	識別名	
6.1.1	FCS_CKM.4	暗号鍵破棄
6.1.2	FCS_COP.1(1)	暗号操作 (AES)
6.1.3	FCS_COP.1(2)	暗号操作 (MAC)
6.1.4	FCS_COP.1(3)	暗号操作 (RSA_crpt)
6.1.5	FCS_COP.1(4)	暗号操作 (RSA_sign)
6.1.6	FCS_COP.1(5)	暗号操作 (SHA256)
6.1.7	FCS_RNG.1	乱数生成
6.1.8	FDP_ACC.1	サブセットアクセス制御
6.1.9	FDP_ACF.1	セキュリティ属性によるアクセス制御
6.1.10	FDP_IFC.1	サブセット情報フロー
6.1.11	FDP_IFF.1	単純セキュリティ属性
6.1.12	FDP_ITC.1(1)	セキュリティ属性なし利用者データのインポート(セッション鍵・外部認証用公開鍵)
6.1.13	FDP_ITC.1(2)	セキュリティ属性なし利用者データのインポート(セッション鍵・外部認証用公開鍵以外)
6.1.14	FIA_AFL.1	認証失敗時の取り扱い
6.1.15	FIA_UAU.1	認証のタイミング
6.1.16	FIA_UAU.4	単一使用認証メカニズム
6.1.17	FIA_UAU.5	複数の認証メカニズム
6.1.18	FIA_UID.1	識別のタイミング
6.1.19	FMT_MSA.3	静的属性初期化
6.1.20	FMT_MTD.1	TSFデータの管理
6.1.21	FMT_SMF.1	管理機能の特定
6.1.22	FMT_SMR.1	セキュリティの役割
6.1.23	FPT_PHP.3	物理的攻撃への抵抗
6.1.24	FTP_ITC.1	TSF間高信頼チャネル

それぞれのセキュリティ機能コンポーネントに必要な操作を施すことによってSFRを規定する。操作内容は、各SFRにおいて、以下の表記方法で示される。

- 割付あるいは選択操作の箇所を[割付: ×××*(斜体)*]、[選択: ×××*(斜体)*]の形式で示す。
- 選択操作において、選択対象外の項目を抹消線 *(~~抹消線~~)* で示す。
- 詳細化部分をSFR中に***斜体・ゴシック体***で示す。
- 繰返し操作は、SFR名称の後ろにカッコ付きで区別のための情報を示し、さらに短縮名に（1）、(2) のように番号を付けて示す。
- 本PPでは、一部の操作が未了であり、その個所を[割付: *×××(斜体・下線)*]のように下線で示す。ST作成者は、未了部分の操作を完了せねばならない。

以下、本PPで規定するSFRを示す。

6.1.1 FCS_CKM.4 暗号鍵破棄

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]

FCS_CKM.4.1 **TSFは、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵破棄方法[割付: *暗号鍵破棄方法*]に従って、暗号鍵を破棄しなければならない。**

6.1.2 FCS_COP.1(1) 暗号操作 (AES)

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 **TSFは、[割付: *FIPS PUB 197/NIST SP800-38A*] に合致する、特定された暗号アルゴリズム [割付: *AES-CBC mode*] と暗号鍵長 [割付: *128ビット*] に従って、[割付: *セキュアメッセージングにおけるAPDU*暗号化/復号、インポートする秘密鍵の復号*] を実行しなければならない。**

* *Application Protocol Data Unit: ICカードに対するコマンド・レスポンスとして送受信されるデータブロック*

6.1.3 FCS_COP.1(2) 暗号操作 (MAC)

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 **TSFは、[割付: *FIPS PUB 197/NIST SP 800-38B*] に合致する、特定された暗号アルゴリズム [割付: *CMAC with AES*] と暗号鍵長 [割付: *128ビット*] に従って、[割付: *セキュアメッセージングにおけるAPDUへのMAC生成/検証*] を実行しなければならない。**

6.1.4 FCS_COP.1(3) 暗号操作 (RSA_crpt)

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 **TSFは、[割付: *PKCS#1 v2.2*] に合致する、特定された暗号アルゴリズム [割付: *RSA-OAEP*] と暗号鍵長 [割付: *2048ビット*] に従って、[割付: *セキュアメッセージング用セッション鍵の復号、秘密鍵復号用共通鍵の復号**] を実行しなければならない。**

* *公的個人認証APにおける共通鍵オンライン更新時に適用*

6.1.5 FCS_COP.1(4) 暗号操作 (RSA_sign)

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 **TSFは、[割付: *表6-2に示す標準*] に合致する、特定された暗号アルゴリズム [割付: *表6-2に示す暗号アルゴリズム*] と暗号鍵長 [割付: *2048ビット*] に従って、[割付: *表6-2に示す操作*] を実行しなければならない。**

表6-2 RSA署名・検証の暗号操作

標準	*暗号アルゴリズム*	*操作*
PKCS#1v2.2	*RSASSA-PKCS1-V1.5*	*プラットフォーム、住基APの内部認証における対象メッセージへの署名生成*
		プラットフォーム、各基本APの外部認証

		における署名検証
PKCS#1v2.2における RSASSA-PKCS1-V1.5パディング	*RSA*	*券面事項入力補助AP・公的個人認証AP・券面事項確認APの内部認証、及び公的個人認証APの署名における、対象メッセージへのPKCSパディング付与と秘密鍵による署名演算*
なし (PKCS#1v2.2における RSASSA-PKCS1-V1.5パディングに独自コードを追加)		*公的個人認証APの署名において、PKCSパディングに標準外のコードを追加し、対象メッセージへのパディング付与と秘密鍵による署名演算*

6.1.6 FCS_COP.1(5) 暗号操作 (SHA256)

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 **TSFは、[割付: *FIPS PUB 180-4*]に合致する、特定された暗号アルゴリズム[割付: *SHA-256*]と暗号鍵長[割付: *なし*]に従って、[割付: *RSA暗号演算 (復号、署名生成、署名検証) に関連して要求されるメッセージダイジェスト計算*]を実行しなければならない。**

6.1.7 FCS_RNG.1 乱数生成

下位階層: なし
依存性: なし

FCS_RNG.1.1 **TSFは、[割付: *なし*] を実現する [選択: *物理的、~~非物理的真、決定論的、~~ハイブリッド*] 乱数生成器を提供しなければならない。**

FCS_RNG.1.2 **TSFは、[割付: *定義された品質尺度*] を満たす乱数を提供しなければならない。**

6.1.8 FDP_ACC.1 サブセットアクセス制御

下位階層: なし
依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1 **TSFは、[割付:**

サブジェクト: <表6-3のサブジェクト欄に示すプロセス> 、

オブジェクト: <表6-3のオブジェクト欄に示すエンティティ> 、

及びSFPで扱われるサブジェクトとオブジェクト間の操作: <表6-3の操作欄に示す操作> **]**

に対して **[割付:** *個人番号カードアクセス制御SFP***]** を実施しなければならない。

表6-3 サブジェクト・オブジェクト・操作

適用箇所	*サブジェクト*	*オブジェクト*	*操作*
プラットフォーム	*プラットフォーム管理者を代行するプロセス*	*[割付: 利用者データを格納するファイルのリスト]**	*[選択: 書込み、読出し]**
		SSD	*生成・削除*
	条例利用AP管理者を代行するプロセス	*条例利用AP*	*生成・削除*
券面事項入力補助AP	*券面事項入力補助AP管理者を代行するプロセス*	*[割付: 利用者データを格納するファイルのリスト]**	*[選択: 書込み、読出し]**
	カード保持者を代行するプロセス	*個人番号ファイル* *4情報ファイル*	*読出し*
	個人番号・4情報を扱うシステムを代行するプロセス		
住基AP	*住基AP管理者を代行するプロセス*	*[割付: 利用者データを格納するファイルのリスト]**	*[選択: 書込み、読出し]**
	カード保持者を代行するプロセス	*住民票コードファイル*	*読出し*
	住基データを扱うシステムを代行するプロセス		
公的個人認証AP	*公的個人認証AP管理者を代行するプロセス*	*[割付: 利用者データを格納するファイルのリスト]**	*[選択: 書込み、読出し]**
	カード保持者を代行するプロセス	*署名用秘密鍵による署名機能* *利用者証明用秘密鍵による署名機能*	*署名*
	証明書データを扱うシステムを代行するプロセス	*利用者証明用秘密鍵による署名機能*	
券面事項確認AP	*券面事項確認AP管理者を代行するプロセス*	*[割付: 利用者データを格納するファイルのリスト]**	*[選択: 書込み、読出し]**
	カード保持者を代行するプロセス	*券面事項情報を格納するファイル*	*読出し*
	券面事項情報を扱うシステムを代行するプロセス		
	個人番号を扱うシステムを代行	*個人番号を格納するファイル*	

	するプロセス		
	生年月日を扱うシステムを代行するプロセス	*生年月日を格納するファイル*	
プラットフォーム、基本AP	*外部端末を代行するプロセス*	*セッション鍵暗号化用公開鍵ファイル(券面事項確認APを除く)* *内部認証用公開鍵ファイル*	*読出し*

* *オブジェクト「利用者データを格納するファイル」とその操作は、本PPでは特定されない。ST作成者は、調達者が提示する仕様を満たすように操作を完了すること。なお、操作は、オブジェクト（利用者データを格納するファイル）ごとに選択を繰り返す。*

6.1.9 FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし
依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1 **TSF**は、以下の**[**割付**:** *示された**SFP** 下において制御される*

*サブジェクト**:** <表**6-3**のサブジェクト欄に記載されたプロセス>* と

*オブジェクト**:** <表**6-3**のオブジェクト欄に記載されたエンティティ>* 、及び

*サブジェクトに対応するセキュリティ属性**:** <サブジェクトに関連付けられる利用者の認証結果* >、

オブジェクトに対応するセキュリティ属性:* <サブジェクトごとに許可する操作の内容> **]**

に基づいて、オブジェクトに対して、**[**割付**:** *個人番号カードアクセス制御**SFP***] を実施しなければならない。

FDP_ACF.1.2 **TSF**は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない**: [**割付**:**

*サブジェクトに関連付けられた利用者の認証結果が認証成功であるとき、該サブジェクトは、該オブジェクトに対し、許可された操作を実行できる***]** 。

FDP_ACF.1.3 **TSF**は、次の追加規則、**[**割付**:** *なし***]** に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

FDP_ACF.1.4 **TSF**は、次の追加規則、**[**割付**:** *なし***]** に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

- オブジェクトのセキュリティ属性は、認証済みサブジェクトに許可する操作種別情報を含む。実際のオブジェクトごとの詳細情報は、別途調達者から提示される（FDP_ACC.1 表6-3注釈参照）。

6.1.10 FDP_IFC.1 サブセット情報フロー制御

下位階層: なし
依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFC.1.1 **TSFは、[割付:**

サブジェクト: <外部端末から暗号鍵 (セッション鍵または外部認証用公開鍵) をインポートするTOEのプロセス>、

情報: <暗号鍵(セッション鍵または外部認証用公開鍵)>

操作: <インポート>]

に対して**[割付:** *暗号鍵インポート情報フロー制御SFP***]**を実施しなければならない。

6.1.11 FDP_IFF.1 単純セキュリティ属性

下位階層: なし
依存性: FDP_IFC.1 サブセット情報フロー制御
FMT_MSA.3 静的属性初期化

FDP_IFF.1.1 **TSFは、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[割付:** *暗号鍵インポート情報フロー制御SFP***]**を実施しなければならない。**: [割付:**

サブジェクト: <外部端末からセッション鍵をインポートするTOEのプロセス、外部認証用公開鍵をインポートするTOEのプロセス>、

情報: <セッション鍵、外部認証用公開鍵 >

サブジェクトのセキュリティ属性: <情報検証用の参照データ>

情報のセキュリティ属性: <情報に付随する検証用データ>]

FDP_IFF.1.2 **TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付:**

TSFは、情報検証用の参照データと情報に付加された検証用データを使用して情報の検証に成功したとき、その情報のサブジェクトへの流入を許可する。検証成功の判定方法は、以下のとおり:

セッション鍵: 外部端末がTOEの公開鍵を使用して暗号化したデータをTOEが自身の秘密鍵で復号したとき、復号データに所定の文字列が含まれることを確認 (秘密鍵と所定の文字列が情報検証用の参照データ)、

外部認証用公開鍵: 外部端末から送られた証明書 (公開鍵を含む)の署名をTOEに格納済みの署名者の公開鍵で検証 (署名者の公開鍵が情報検証用の参照データ)

]。

FDP_IFF.1.3 TSFは、[割付: *なし*]を実施しなければならない。

FDP_IFF.1.4 TSFは、以下の規則、[割付: *なし*]に基づいて、情報フローを明示的に許可しなければならない。

FDP_IFF.1.5 TSFは、以下の規則、[割付: *なし*]に基づいて、情報フローを明示的に拒否しなければならない。

6.1.12 FDP_ITC.1(1) セキュリティ属性なし利用者データのインポート (セッション鍵・外部認証用公開鍵)

下位階層: なし
依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.3 静的属性初期化

FDP_ITC.1.1 TSFは、SFP制御下にある利用者データ *(セキュアメッセージング用セッション鍵、外部認証用公開鍵)* をTOEの外部からインポートするとき、[割付:*暗号鍵インポート情報フロー制御SFP*]を実施しなければならない。

FDP_ITC.1.2 TSFは、TOE外からインポートされるとき、利用者データに関連付けられたいかなるセキュリティ属性も無視しなければならない。

FDP_ITC.1.3 TSFは、TOE外部からSFPの下で制御される利用者データをインポートするとき、[割付: *なし*]の規則を実施しなければならない。

6.1.13 FDP_ITC.1(2) セキュリティ属性なし利用者データのインポート (セッション鍵・外部認証用公開鍵以外)

下位階層: なし
依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.3 静的属性初期化

FDP_ITC.1.1 **TSFは、SFP制御下にある利用者データ *(セキュアメッセージング用セッション鍵、外部認証用公開鍵を除く)* をTOEの外部からインポートするとき、[割付:*個人番号カードアクセス制御SFP*]を実施しなければならない。**

FDP_ITC.1.2 **TSFは、TOE外からインポートされるとき、利用者データに関連付けられたいかなるセキュリティ属性も無視しなければならない。**

FDP_ITC.1.3 **TSFは、TOE外部からSFPの下で制御される利用者データをインポートするとき、[割付: *なし*]の規則を実施しなければならない。**

6.1.14 FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし
依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 **TSFは、[割付: *認証事象のリスト*] に関して、[選択: *[割付: 正の整数値]、[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*] 回の不成功認証試行が生じたときを検出しなければならない。**

FIA_AFL.1.2 **不成功の認証試行が定義した回数[選択：*に達する、を上回った*] とき、TSFは、[割付: *アクションのリスト*] をしなければならない。**

[注釈_FIA_AFL.1] FIA_AFL.1.2の割付例は、認証機能の閉塞である。もし、閉塞した認証機能の解除が管理機能として必要な場合、ST作成者は、それを管理要件に追加すべきである。

6.1.15 FIA_UAU.1 認証のタイミング

下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 **TSFは、利用者が認証される前に利用者を代行して行われる [割付: *TSF仲介アクションのリスト*] を許可しなければならない。**

FIA_UAU.1.2 **TSFは、その利用者を代行する他のすべてのTSF仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。**

6.1.16 FIA_UAU.4 単一使用認証メカニズム

下位階層: なし
依存性: なし

FIA_UAU.4.1 **TSFは、[割付: *表6-4に示す利用者認証に適用する認証メカニズム*] に関係する認証データの再使用を防止しなければならない。**

表6-4　認証データ再使用を防止する認証メカニズム

利用者認証箇所	*認証の対象･目的*	*認証メカニズム*
プラットフォーム	*外部認証*	*公開鍵暗号方式に基づくチャレンジレスポンス方式*
券面事項入力補助AP		
住基AP		
公的個人認証AP		
券面事項確認AP		

6.1.17　FIA_UAU.5 複数の認証メカニズム

下位階層:　なし
依存性:　なし

FIA_UAU.5.1　**TSFは、利用者認証をサポートするため、[割付: *複数の認証メカニズムのリスト*] を提供しなければならない。**

FIA_UAU.5.2　**TSFは、[割付: *複数の認証メカニズムがどのように認証を提供するかを記述する規則*] に従って、利用者が主張する識別情報を認証しなければならない。**

6.1.18　FIA_UID.1 識別のタイミング

下位階層:　なし
依存性:　なし

FIA_UID.1.1　**TSFは、利用者が識別される前に利用者を代行して実行される [割付: *TSF仲介アクションのリスト*] を許可しなければならない。**

FIA_UID.1.2　**TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。**

6.1.19　FMT_MSA.3 静的属性初期化

下位階層:　なし
依存性:　FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1　**TSFは、そのSFPを実施するために使われるセキュリティ属性に対して[選択: *制限的、許可的、[割付: その他の特性]: から一つのみ選択*]デフォルト値を与える [割付: *個人番号カードアクセス制御SFP*] を実施しなければならない。**

FMT_MSA.3.2 **TSFは、*オブジェクト (条例利用AP、SSD) ~~オブジェクトや~~情報*が生成されるとき、[割付: *オブジェクトの管理者*] が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。**

[注釈_FMT_MSA.3] FMT_MSA.3.1では、オブジェクト（条例利用AP、SSD）設定時のセキュリティ属性デフォルト値の特性を規定する。プラットフォーム及び基本APは、開発環境において設定済みであり、本SFRの対象ではない。

オブジェクトのセキュリティ属性は、設定後に変更されない（オブジェクト自体の削除、再設定は可能な場合がある）。そのため、運用環境でのセキュリティ属性の管理要件FMT_MSA.1は適用されない。

オブジェクトの管理者はセキュリティ属性の初期値設定権限を有するが、これを実現するメカニズム（FMT_MSA.3.2のエレメントに対応）は実装に依存する。例えば、対象APを削除・再インストールし、それによってセキュリティ属性を一括して変更する方法は、本要件を満たす。

6.1.20 FMT_MTD.1 TSFデータの管理

下位階層: なし
依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 **TSFは、[割付: *表6-5に示すTSFデータ*]を [選択: *~~デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]~~*] する能力を [割付: *表6-5に示す管理者*] に制限しなければならない。**

表6-5 管理対象のTSFデータ

適用箇所	*TSFデータ*	*TSFデータの管理者に相当する者*
プラットフォーム	*該当なし*	*–*
券面事項入力補助AP	*カード保持者PW*	*カード保持者及び券面事項入力補助AP管理者*
	個人番号読出しPW *4情報読出しPW*	*券面事項入力補助AP管理者*
住基AP	*カード保持者PW*	*カード保持者及び住基AP管理者*
公的個人認証AP	*署名用PW* *利用者証明用PW*	*カード保持者及び公的個人認証AP管理者*
券面事項確認AP	*生年月日用PW* *券面事項情報用PW* *個人番号用PW*	*券面事項確認AP管理者*
	カード保持者PW	*券面事項確認AP管理者及び*

		券面事項情報を扱うシステム[*]

[*] *券面事項情報を扱うシステムは、カード保持者PW変更権限を持つ。変更されたカード保持者PWは、カード保持者へ通知される。*

6.1.21 FMT_SMF.1 管理機能の特定

下位階層: なし
依存性: なし

FMT_SMF.1.1 **TSFは、以下の管理機能を実行することができなければならない。: [割付: *表6-6に示す管理機能*]**

表6-6 管理機能

適用箇所	*管理機能*
プラットフォーム	*該当なし*
券面事項入力補助AP	*各PWの改変*
住基AP	*カード保持者PWの改変*
公的個人認証AP	*各PWの改変*
券面事項確認AP	*各PWの改変*

6.1.22 FMT_SMR.1 セキュリティの役割

下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 **TSFは、役割[割付: *プラットフォームと各基本APにおいて、表6-7に示す役割*]を維持しなければならない。**

表6-7 セキュリティの役割

適用箇所	*役割*
プラットフォーム	*管理者* *条例利用AP管理者*
券面事項入力補助AP	*カード保持者* *券面事項入力補助AP管理者*
住基AP	*カード保持者* *住基AP管理者*
公的個人認証AP	*カード保持者* *公的個人認証AP管理者*
券面事項確認AP	*券面事項確認AP管理者* *券面事項情報を扱うシステム(表6-5参照)*

FMT_SMR.1.2 **TSFは、利用者を役割に関連付けなければならない。**

6.1.23 FPT_PHP.3 物理的攻撃への抵抗

下位階層: なし

依存性: なし

FPT_PHP.3.1 **TSFは、SFRが常に実施されるよう自動的に対応することによって、[割付: *TSF*]への[割付: *物理的手段を使用した攻撃であって、JIWG supporting documentsが定めるIC評価方法に含まれる攻撃*]に抵抗しなければならない。**

[注釈_FPT_PHP.3] JIWG supporting documentsは、TOE評価時の最新のものが適用される。PP発行時点の同文書は、“Joint Interpretaion Library – Application of Attack Potential to Smartcards, Version 2.9, January 2013”である。

6.1.24 FTP_ITC.1 TSF間高信頼チャネル

下位階層: なし
依存性: なし

FTP_ITC.1.1 **TSFは、それ自身と他の高信頼IT製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。**

FTP_ITC.1.2 **TSFは、[選択: ~~*TSF*~~、*他の高信頼IT製品*] が、高信頼チャネルを介して通信を開始するのを許可しなければならない。**

FTP_ITC.1.3 **TSFは、[割付: *表6-8に示す適用箇所ごとの暗号化/復号、MAC生成/検証に対応するデータ転送*] のために、高信頼チャネルを介して通信を開始しなければならない。**

表6-8 高信頼チャネルの適用形態

適用箇所	*暗号化/復号*	*MAC生成/検証*
プラットフォーム	*適用*	*適用*
券面事項入力補助AP	*適用または非適用*[1]	*適用または非適用*[1]
住基AP	*適用（住民票コード読出し）*	*非適用*[2]
公的個人認証AP	*適用または非適用*[1]	*適用または非適用*[1]
券面事項確認AP	*非適用*[2]	*非適用*[2]

[1] *[適用または非適用] TOEは、該当するセキュリティ機能を実装する。外部端末が要求した場合にその機能を使用する。*

*2 *[非適用] TOEは、該当するセキュリティ機能を実装してもしなくてもよい。実装した場合、外部端末の要求があれば、その機能を使用してよい。*

6.2 セキュリティ保証要件

本TOEに適用するセキュリティ保証要件は、表6-9に示す保証コンポーネントで定義される。これらは、すべて、CC パート3に含まれる。

表6-9に示すすべてのコンポーネントにおいて、本PPでは、操作を適用しない。

表6-9 保証コンポーネント

保証クラス	保証コンポーネント
セキュリティターゲット評価	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
開発	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
ガイダンス文書	AGD_OPE.1
	AGD_PRE.1
ライフサイクルサポート	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.1
テスト	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
脆弱性評定	AVA_VAN.5

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

本章では、定義されたSFRがTOEのセキュリティ対策方針を適切に達成することの根拠を示す。6.3.1.1では、各々のSFRがいずれかのTOEのセキュリティ対策方針にさかのぼれること、6.3.1.2では、各々のTOEのセキュリティ対策方針が対応する有効なSFRによって適切に満たされることを説明する。

6.3.1.1 セキュリティ対策方針とセキュリティ機能要件の対応

TOEのセキュリティ対策方針に対応するSFRを表6-10に示す。この表は、すべてのSFRが少なくとも一つのTOEのセキュリティ対策方針にさかのぼれることの根拠となる。

表6-10 TOEセキュリティ対策方針とSFRの対応

TOEセキュリティ対策方針 / SFR	FCS_CKM.4	FCS_COP.1(1)	FCS_COP.1(2)	FCS_COP.1(3)	FCS_COP.1(4)	FCS_COP.1(5)	FCS_RNG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1(1)	FDP_ITC.1(2)	FIA_AFL.1	FIA_UAU.1	FIA_UAU.4	FIA_UAU.5	FIA_UID.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_PHP.3	FTP_ITC.1
O.I&A	x				x	x		x	x	x	x	x	x	x	x	x	x	x		x	x	x		
O.Access_Control								x	x				x						x			x		
O.Replay																x								
O.Secure_messaging	x	x	x	x				x	x	x	x	x	x											x
O.Delivery															x		x	x						
O.Cryptography	x	x	x	x	x	x		x	x	x	x	x	x											x
O.Phys_Attack																							x	
O.RND							x																x	

6.3.1.2 対応関係の根拠説明

TOEのセキュリティ対策方針がそれに対応づけられるSFRによって満たされることの根拠を示す。個々のSFRがTOEのセキュリティ対策方針を満たす上での有効性を持つことも同時に示される。

O.I&A

認証された利用者へのサービス提供を、FIA_UAU.1、FIA_UID.1で規定する。適用される複数の認証メカニズムは、FIA_UAU.5で規定される。公開鍵暗号方式に基づく外部認証では、FCS_COP.1(4) によるRSA署名・検証操作、FCS_COP.1(5) によるメッセージダイジェスト計算が適用される。公開鍵暗号演算に使用する暗号鍵のインポートは、外部認証用公開鍵についてはFDP_ITC.1(1)、FDP_IFC.1、FDP_IFF.1で、それ以外については、FDP_ITC.1(2)、FDP_ACC.1、FDP_ACF.1で規定する。暗号鍵破棄は、FCS_CKM.4で規定される。さらに、不正手段による認証を防止するため、同一認証データの再使用防止を規定するFIA_UAU.4を適用する。各認証メカニズムにおける認証失敗時のTSFアクションをFIA_AFL.1で規定する。TOEの利用者認証に使用する認証データの管理要件として、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1を用いる。これらSFRによって、O.I&Aが十分に達成される。

O.Access_Control

セキュリティ対策方針O.Access_Controlは、利用者データに対し、正当な権限を持つものだけが許可されたアクセスを実行できることを求める。この要件は、FDP_ACC.1/FDP_ACF.1で規定される。FDP_ACF.1で使用されるセキュリティ属性の管理には、FMT_MSA.3が適用される。FMT_MSA.3は、条例利用APとSSDの生成だけに関わる。それ以外のオブジェクトはすべて開発環境で生成されるため、FMT_MSA.3の適用外である。FMT_MSA.3に関わる管理者役割を規定するため、FMT_SMR.1が用いられる。本TOEは、外部から暗号鍵をインポートする。インポートされる暗号鍵は、利用者データとしてアクセス制御対象となる。この要件は、FDP_ITC.1(2)で対応される。これらのSFRによって、O.Access_Controlが十分に達成される。

O.Replay

FIA_UAU.4は、認証データの単一使用を規定するSFRで、セキュリティ対策方針O.Replayに合致する。

O.Secure_messaging

セキュアメッセージングでは、AESによる暗号化/MACによってセッションデータの機密性・完全性を保護する。セッション鍵 (AES) は、外部端末で生成され、RSA鍵で暗号化されてTOEにインポートされ復号される。AESの暗号操作はFCS_COP.1(1)、FCS_COP.1(2)で、RSAの暗号操作(復号)はFCS_COP.1(3)でそれぞれ規定される。セキュアメッセージング用セッション鍵のインポートは、FDP_ITC.1(1)、FDP_IFC.1、FDP_IFF.1で規定される。セキュアメッセージングに使用したセッション鍵の破棄は、FCS_CKM.4で規定される。RSA公開鍵方式で使用する鍵のインポートはFDP_ITC.1(2)、FDP_ACC.1、FDP_ACF.1で規定される。インポートされた鍵の破棄は、FCS_CKM.4で規定される。セキュアメッセージング自体の要件 (通信チャネルデータの保護) は、FTP_ITC.1で規定される。これらのSFRによって、O.Secure_messagingが十分に達成される。

O.Delivery

セキュリティ対策方針O.Deliveryが要求する「秘密情報によるカード内部データ保護」は、秘密情報（一般的に、輸送鍵と呼ばれる）をパスワードとする認証機能をTOEに要求するSFRで達成できる。認証のために、識別が必要である。識別・認証の要求はFIA_UAU.1、FIA_UID.1で規定し、それぞれの認証メカニズムをFIA_UAU.5で規定する。これらのSFRによって、O.Deliveryが十分に達成される。

O.Cryptography

セキュリティ対策方針O.Cryptographyが要求する暗号アルゴリズム、暗号操作、暗号鍵管理(鍵長、暗号鍵インポート、暗号鍵破棄)は、O.Cryptographyが参照するP.Cryptographyの表3-2で詳細に規定される。暗号アルゴリズムと暗号操作は、FCS_COP.1(1)～(5)で規定される。使用される暗号鍵は、すべてTOE外部で生成されてTOEにインポートされる。暗号鍵のインポート要件はFDP_ITC.1(1)、(2)で規定され、セキュアなインポートのためにFDP_ACC.1、FDP_ACF.1、FDP_IFC.1、FDP_IFF.1が規定される。暗号鍵インポート時に要求される通信路保護は、FTP_ITC.1で規定される。不要になった暗号鍵の破棄要件はFCS_CKM.4で規定される。これらのSFRによって、O.Cryptographyが十分に達成される。

O.Phys_Attack

O.Phys_Attackは、物理的攻撃によるTOEのデータや機能へのセキュリティ侵害への対抗を要求する。FPT_PHP.3は、TSFに対する物理的攻撃への抵抗を要求する。TSFが物理的攻撃で侵害されなければ、TSFは、その論理的セキュリティ機能でデータや機能へのセキュリティ侵害を阻止する。従って、このSFRを満たすことで、O.Phys_Attackを十分に達成できる。

O.RND

セキュリティ対策方針O.RNDは、生成される乱数が十分な品質を持ち、攻撃者による予測を困難にする対策を求める。FCS_RNG.1は、必要な品質尺度を満たす乱数生成を要求する。さらに、FPT_PHP.3によって、RNGへの物理的攻撃でRNG出力が予測される攻撃に対抗する。これらSFRによって、O.RNDが十分に達成される。

6.3.1.3 セキュリティ機能要件の依存性

各SFRに規定された依存性とその対応を表6-11に示す。

表6-11において、「依存性の要求」欄にはCCパート2のコンポーネントに規定された依存性を示す。「依存性の対応」欄には、規定された依存性がPP中のどのSFRによって満たされるか、あるいは満たされない場合の正当性を示す根拠が記述される。

表6-11 SFRの依存性

SFR	依存性の要求	依存性の対応
FCS_CKM.4	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1]	破棄対象となる暗号鍵は、外部端末からインポートされる。鍵のインポートにはFDP_ITC.1(1)/FDP_ITC.1(2)が対応し、依存性が満たされる。
FCS_COP.1(1)	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1] FCS_CKM.4	使用する暗号鍵(セッション鍵、秘密鍵復号用共通鍵)は、外部端末からインポートされる。セッション鍵、秘密鍵復号用共通鍵のインポートには、それぞれFDP_ITC.1(1)、FDP_ITC.1(2)が対応し、依存性が満たされる。 鍵の破棄はFCS_CKM.4で規定され、依存性が満たされる。
FCS_COP.1(2)		使用する暗号鍵(セッション鍵)は、外部端末からインポートされる。セッション鍵のインポートにはFDP_ITC.1(1)が対応し、依存性が満たされる。 鍵の破棄はFCS_CKM.4で規定され、依存性が満たされる。
FCS_COP.1(3)		使用する暗号鍵は、外部端末からインポートされる。外部認証用公開鍵のインポートにはFDP_ITC.1(1)、それ以外にはFDP_ITC.1(2)が対応し、依存性が満たされる。 鍵の破棄はFCS_CKM.4で規定され、依存性が満たされる。
FCS_COP.1(4)		
FCS_COP.1(5)		本SFRはハッシュ演算だけを規定するもので、暗号鍵を使用しない。そのため、鍵のインポート、生成、破棄の規定は不要であり、依存性を満たす必要はない。
FCS_RNG.1	なし	不要
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1が対応し、依存性が満たされる。
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1が対応し、依存性が満たされる。 本SFRの対象となるオブジェクトは、条例利用APとSSDを除き、すべて開発環境でファイル設定済みになるので、FMT_MSA.3が適用されず、依存性を満たす必要がない。条例利用APとSSDについては、FMT_MSA.3が対応し、依存性が満たされる。
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1が対応し、依存性が満たされる。
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1が対応し、依存性が満たされる。 本SFRの対象となる情報(セッション鍵)は外部端末で生成されるので、FMT_MSA.3は適用されず、依存性を満たす必要がない。
FDP_ITC.1(1)	[FDP_ACC.1 または FDP_IFC.1] FMT_MSA.3	
FDP_ITC.1(2)		FDP_ACC.1が対応し、依存性が満たされる。 本SFRに関わる利用者データを格納するオブジェクトは、すべて開発環境でファイル設定される。そのため、FMT_MSA.3は適用されず、依存性を満たす必要がない。
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1が対応し、依存性が満たされる。
FIA_UAU.1	FIA_UID.1	FIA_UID.1が対応し、依存性が満たされる。
FIA_UAU.4	なし	不要
FIA_UAU.5	なし	不要

FIA_UID.1	なし	不要
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.3の対象となるオブジェクトは条例利用APとSSDである。これらの属性は、設定後に変更されない。そのため、FMT_MSA.1は適用されず、依存性を満たす必要がない。 オブジェクト生成に関わる役割はFMT_SMR.1が対応し、依存性が満たされる。
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1、FMT_SMF.1が対応し、依存性が満たされる。
FMT_SMF.1	なし	不要
FMT_SMR.1	FIA_UID.1	FIA_UID.1が対応し、依存性が満たされる。
FPT_PHP.3	なし	不要
FTP_ITC.1	なし	不要

6.3.2 セキュリティ保証要件根拠

本TOEのセキュリティ機能は、ソフトウェアによるセキュリティ機能、ハードウェア（ICチップ）によるセキュリティ機能、及びソフトウェアとハードウェアの協働によるセキュリティ機能と、3通りの方法で実現される。

TOEに要求されるセキュリティ機能の多くは、ソフトウェアによるセキュリティメカニズムで実現される。このセキュリティメカニズムは、一次資産である個人情報（個人番号など）と個人認証サービスの保護が主たる目的である。これらの資産は、社会情報基盤としての信用性が重要であり、十分なセキュリティ評価を実施する。そのため、評価保証レベルを、商用レベルとして最高レベルのEAL4とする。

一方、本TOEは、ICカードのハードウェアによるセキュリティ機能を含む。ICカードの脆弱性を悪用する攻撃手法は高度に発達しており、高レベルの攻撃を想定しないと、十分な安全性を保証できない。すなわち、ICカードの脆弱性に関しては、物理的攻撃を含む高レベルの攻撃に対抗しなくてはならない。このため、TOEの脆弱性を適切に評価できるよう、AVA_VAN.5を保証要件に追加する。すなわち、TOEのソフトウェア、ハードウェア共に、脆弱性に関し、高レベルの攻撃に対抗することを保証要件とする。

本TOEは、その開発環境（製造環境）で、条例利用APを除くすべてのファイルを設定する。暗号鍵と認証データの一部も開発環境で設定される。これら設定情報には高い機密性・完全性が要求され、ハードウェアの開発環境と合わせ、十分な開発セキュリティを保証しなくてはならない。そのため、開発環境に対し、ALC_DVS.2を追加する。

追加保証要件のAVA_VAN.5に規定される依存性はAVA_VAN.3（EAL4）と同一である。ALC_DVS.2は他の保証要件に依存しない。従って、保証要件の依存性はEAL4保証パッケージと変わる部分がなく、表6-9に示す各保証コンポーネント間の依存性はすべて満たされる。

7 用語

7.1 CC関連

PP	Protection Profile: TOEの種別に対するセキュリティニーズについての実装に依存しないステートメント。
CC	Common Criteria; IT装置のセキュリティ評価基準。CCと同一の内容がISO/IEC 15408規格としても制定される。
CCRA	The Common Criteria Recognition Arrangementの; CC承認アレンジメント。CCRAに加盟する各国のCC評価・認証制度において、他国の制度下での評価・認証結果を相互に承認し受け入れることの協定。
ST	Security Target: 識別された特定のTOEに対するセキュリティニーズについての実装に依存するステートメント。
TOE	Target of Evaluation; 評価対象。ソフトウェア、ファームウェア、及び/またはハードウェアのセットであり、ガイダンスを伴うこともある。
TSF	TOE security functionality; TOEのすべてのハードウェア、ソフトウェア、及びファームウェアが結合した機能性であり、SFRの正確な実施のために信頼されねばならないもの。

7.2 TOE関連

個人番号カード	住民基本台帳ネットワークシステムで使用されていた住基カードの機能とサービスを含み、搭載APを拡張した多目的の公的ICカード。利用対象者を希望者だけでなく、全国民とした。1枚のICカードに、券面事項入力補助AP、住基AP、公的個人認証AP、券面事項確認APの4つのAPを基本機能として搭載する。さらに、カードを交付する市町村地方自治体ごとに、条例に基づくAPを追加搭載できる。
コンポジット評価	ICカードは、ハードウェア（ICチップや非接触通信用アンテナなどから構成される）とソフトウェアが一体化されたIT製品である。同一のハードウェアにさまざまなソフトウェアを組み合わせてICカード製品とする場合、まずハードウェア部分を評価し、その後にソフトウェアを搭載したICカードとして追加部分を評価すれば、時間のかかるハードウェア評価を共通化でき、トータルの評価コストを減らせる。このように、初めに基本部分を

評価し、その後、追加部分を含めたIT製品全体の評価を行う方式をコンポジット評価と言う。上記ICカードの例では、後から搭載されるソフトウェア部分及びソフトウェアとハードウェアの協働部分がコンポジット評価の対象となる。既に評価が実施されたハードウェア部分については、評価済みのSTと評価報告書を再利用できる。しかしながら、評価報告書は公開資料ではなく、再利用には評価報告書を作成した評価機関、評価を監督した認証機関の了承が必要になる。特に、基本部分の評価とコンポジット評価とを各々異なる認証機関のもとで行う場合、了承を得るための関係者が多くなり、十分な事前調整が必要である。