個人番号カード Version 2

プロテクションプロファイル

第 1.00 版

2025 年 9 月 3 日

地方公共団体情報システム機構

Japan Agency for Local Authority Information Systems

株式会社 ECSEC Laboratory 技術センター

JISEC-C0858

略語・用語

CC 関連

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. 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。
CEM	Common Evaluation Methodology. 共通評価方法。評価機関が評価を行うための最低限のアクションを記述した文書。
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。
SFR	Security Functional Requirement. セキュリティ機能要件。TOE のセキュリティ対策方針を標準化された言語に書き換えたもの。
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。
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。

TOE 関連

AES	Advanced Encryption Standard. 共通鍵暗号アルゴリズムのひとつ。
AP	Application Program. ある特定の目的のために開発・使用されるソフトウェア。
APDU	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。
CBC	Cipher Block Chaining. 暗号利用モードのひとつ。
CMAC	Cipher-based MAC. ブロック暗号を使用したメッセージ認証符号アルゴリズム。
DRBG	Deterministic Random Bit Generator. 決定論的乱数生成器。
ECDSA	Elliptic Curve Digital Signature Algorithm. 楕円曲線を用いたデジタル署名アルゴリズム。
ECDH	Elliptic Curve Diffie-Hellman. 楕円曲線を用いた鍵合意アルゴリズム。
IC	Integrated Circuit. 集積回路。
ISD	Issuer Security Domain. 発行者のセキュリティドメイン。
MAC	Message Authentication Code. メッセージを認証するための短い情報。
NIST	National Institute of Standards and Technology. 米国国立標準技術研究所。
PIN	Personal Identification Number. 暗証番号。

PUK	PIN Unlock Key. 暗証番号を再設定するための情報。
receipt key	SCP11 において SD が生成するレシートを計算する鍵。
SCP11	Secure Channel Protocol 11. GlobalPlatform（IC カード管理システムの業界標準化組織）が定めたセキュア通信の仕様。TOE と外部端末との間に相互に認証を提供する SCP11a と外部端末が TOE を認証する SCP11b を使用する。詳しくは[GPC093] Section 4.1 を参照のこと。
SD	Security Domain. セキュリティドメイン。
SSD	Supplementary Security Domain. 許可されたエンティティが独自のライフサイクルに従って AP をインストールして管理できる領域。
SHA	Secure Hash Algorithm. 規格化された暗号学的ハッシュ関数。
S-DEK	Session Data Encryption Key. 機密データを暗号化する鍵。
S-ENC	Secure Channel Session Encryption Key. セキュアメッセージングのコマンド・レスポンスを暗号化／復号する鍵。
S-MAC	Secure Channel Session Message Authentication Code Key for Command. セキュアメッセージングのコマンドの MAC 鍵。
S-RMAC	Secure Channel Session Message Authentication Code Key for Response. セキュアメッセージングのレスポンスの MAC 鍵。
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、認証 AP、券面等 AP の 2 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区町村ごとに、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。
親展通信	公的機関からの通達物の保護、民間事業者からの圧着はがき等に代わる手段など、カードの保有者しか確認できない送信を可能にする機能。公的機関等や民間事業者は、送信情報を親展通信用の鍵で暗号化してカードの保有者に送信し、カードの保有者は、公的機関や民間事業者等から送付される一時公開鍵と個人番号カード内に保持される親展通信機能用

	秘密鍵をもとに、個人番号カード内で生成・出力される共有秘密から親展通信用の鍵を生成して送信情報を復号する。
共有秘密	親展通信の内容を暗号化・復号するために、カードの保有者と正規の親展通信相手の間で共有する秘密の情報。

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。

現行の個人番号カードは、平成 28 年（2016 年）1 月に発行が開始されて以来、一定の期間が経過した。デジタル社会の実現に向けた重点計画（2023 年 6 月閣議決定）に基づき、次期個人番号カードタスクフォースが、次期の個人番号カードについて、検討を行い、最終とりまとめを作成したことに対応して、個人番号カード Version 2 の PP を策定した。

個人番号カードは、対面でも非対面でも本人確認に用いることのできるデジタル社会のパスポートとして、官民のオンライン・デジタル化の基盤となるものであり、個人番号カードを基盤とした安全で便利なデジタル社会の実現が期待される。次期の個人番号カードでは、技術進展に対応して安全性を確保するために暗号アルゴリズムのセキュリティ強化、国民にとってより利便性が感じられるよう、２つの基本 AP となるよう構成変更等を行った。

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対象

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。

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、CC Part 1 に規定される。

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、消費電力解析による暗号鍵を暴露する攻撃に対抗するため、暗号演算プログラムを工夫し、消費電力解析による暗号鍵の推定を困難にする。

目次

1 PP 概説

1.1 PP 参照

タイトル：	個人番号カード Version 2 プロテクションプロファイル
版数：	1.00
発行：	2025 年 9 月 3 日
発行者：	地方公共団体情報システム機構
作成者：	株式会社 ECSEC Laboratory 技術センター
登録：	JISEC-C0858

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、行政手続等における特定の個人を識別するための番号の利用等に関する法律（個人番号（マイナンバー）制度）に基づき、“個人番号カード（マイナンバーカード）”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、ファームウェアを含む 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 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 2 種の AP が動作する。2 種の AP とは、認証カードアプリケーション（以下、認証 AP と表記）、券面等カードアプリケーション（以下、券面等 AP と表記）である。本 PP では、この 2 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市区町村は、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。次節（2）では、それぞれを詳しく説明する。

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。

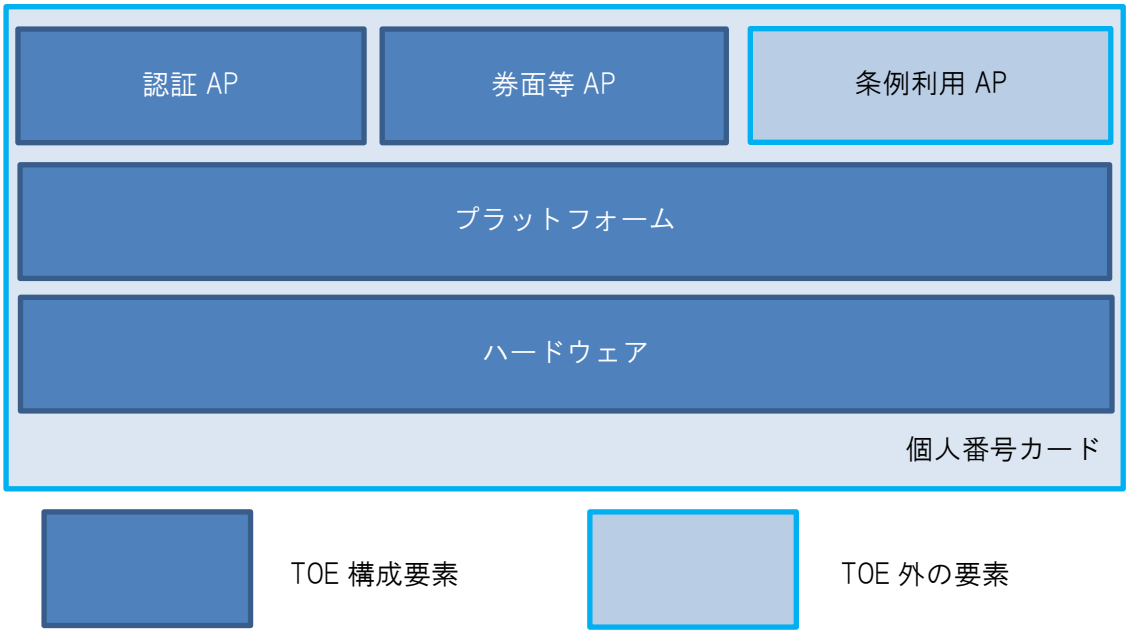

図 1-1 TOE の構成

TOE のソフトウェアは、プラットフォームと 2 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 は市区町村毎のオプションであり、TOE の構成要素に含まれない。

(2) 基本 AP が提供するサービス

個人番号カードは、市区町村その他法令により定められた機関を介して住民に交付される。TOE が搭載する 2 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、市区町村業務だけでなく、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。

［認証 AP］

認証 AP は、住民基本台帳ネットワークシステムカードアプリケーション（以下、住基 AP と表記）、公的個人認証サービスカードアプリケーション（以下、JPKI-AP と表記）、券面等データカードアプリケーション（以下、券面等データ AP と表記）の 3 つの AP を包含する。認証 AP は、セキュアメッセージングを実施して認証 AP と 3 つの AP の通信を保護し、また利用者の認証機能（外部認証を含む）と内部認証機能、親展通信機能を提供する。

［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、カード保持者の住民票コードが格納され、市区町村に設置された外部端末を用いて読み出す。

［JPKI-AP］

個人向けの公的認証サービスを提供する。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。

［券面等データ AP］

カード保持者に付与された個人番号及び 4 情報（氏名・住所・生年月日・性別）を提供する。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。

［券面等 AP］

券面の印刷情報を提供する。券面には、3情報（氏名・住所・生年月日）、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。また、個人番号及び 4 情報をテキストデータで利用者に提供する。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ないよう、読出し時に外部認証を要求する。券面等 AP はセキュアメッセージングを実施して通信を保護し、また内部認証機能、外部認証機能を提供する。

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 2 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（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。アクセス対象のセキュアメッセージング属性により、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 MAC 生成・検証を行い、機密性及び完全性を保護する。プラットフォームは SCP11a によるセキュアメッセージング、認証 AP・券面等 AP は SCP11b によるセキュアメッセージングを実施する。

（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。TOE 外の条例利用 AP 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。外部端末（外部装置ともいう）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[1]」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 カードが偽造品でないことを確認（真贋判定）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。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、認証 AP における署名・利用者証明などに使用される。楕円曲線を使用した署名生成、署名検証、鍵生成、共有秘密生成は鍵長 384 ビットである NIST P-384 を使用する。

（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。

[1] ”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。

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（2 種類）は、それぞれ利用方法が異なる。TOE を利用する者（市区町村、行政機関、民間事業者、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。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、地方公共団体情報システム機構の管理者によってプラットフォームと基本 2AP に必要なデータが書き込まれる。その後、市区町村その他法令により定められた機関を経て、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、あるいは市区町村その他法令により定められた機関の管理者によって、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） 市区町村による条例利用 AP の追加

個人番号カード交付窓口となる市区町村が独自の条例利用 AP を追加搭載することがある。この AP はオプションであり、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、市区町村、行政機関、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、CC:2022 リリース 1 日本語翻訳版 適合を主張する。また補足文書[ERT]を適用する。
本 PP は、[CC]パート 2 適合、[CC]パート 3 適合を主張する。

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 適合主張根拠

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	市区町村その他法令により定められた機関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、及びオプションであり TOE 外の AP のサービス機能を利用する。サービス内容に応じて、市区町村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、TOE 外の AP の生成・削除、プラットフォームや基本 AP のデータ設定・変更、あるいは、パスワードのロック解除など、TOE を適切に運用するための業務であり、プラットフォーム管理者、認証 AP 管理者、住基 AP 管理者、JPKI-AP 管理者、券面等データ AP 管理者、券面等 AP 管理者が存在する。空き領域管理者は、地方公共団体情報システム機構または当該機構から空き領域を管理する権限を付与された者であり、空き領域に条例利用 AP などを設定する。
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、市区町村、行政機関、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 の運用環境において、TOE とデータ授受を行う TOE の外部に位置する IT 装置。外部装置ともいう。

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。TSF による保護対象以外の利用者データは保護資産ではない。TOE は、TOE 外の空き領域に AP を追加搭載できる。これは、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。

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。物理的攻撃には、TOE 外の AP を悪用した攻撃も含まれる。

対抗すべき物理的攻撃の範囲は、[JILAP]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。

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.Phys_Attack

攻撃者は、TOE の構成要素（ハードウェア/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、及び市区町村その他法令により定められた機関を指す。

P.Secure_Messaging

TOE は、外部端末との通信において、アクセス対象にセキュアメッセージング属性が付与されている場合にセキュアメッセージングを適用する。

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 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、共有秘密の計算、あるいは認証にも使用される。表 4-1 に、TOE に要求される暗号アルゴリズム、暗号操作、暗号鍵長、及び暗号機能の用途を示す。使用する秘密鍵を TOE にインポートする場合、通信路を保護し、さらに TOE 内で秘密鍵を鍵暗号化鍵により復号する。使用する公開鍵を TOE インポートするとき TOE 内で署名を検証する。親展通信のために一時公開鍵をインポート[2]し、共有秘密の計算をしてエクスポートする。暗号鍵は使用後に消去する。

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。

[2] 親展通信用一時公開鍵はインポート時に署名検証を行わない。

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

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。

A.Terminal

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 内にデータまたは AP を設定する外部端末を、通信経路上での盗聴、改ざんを防止する安全な環境に設置する。

A.Card

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、有効期限切れなどの理由でカード保持者から返納された個人番号カードを、個人番号や暗号鍵を復元できないような方法で安全に廃棄する。

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

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。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。

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、TOE 外 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。

O.Secure_Messaging

TOE は、外部端末との通信において、アクセス対象にセキュアメッセージング属性が付与されている場合に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・改変を防ぐため共通鍵暗号アルゴリズムを適用し、暗号化・復号及び MAC 生成・検証による通信データの保護を行わねばならない。

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 2 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 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 AP に適用される暗号機能は、表 4-1 に示された方針に従わねばならない。使用する秘密鍵を TOE にインポートする場合、通信路を保護しなければならない。さらに TOE 内で秘密鍵を鍵暗号化鍵により復号しなければならない。外部認証に使用する公開鍵を TOE にインポートするとき TOE 内で署名を検証しなければならない。親展通信用に一時公開鍵をインポートし、共有秘密を計算し、エクスポートしなければならない。暗号鍵は使用後に消去しなければならない。

表 4-1 暗号機能方針

アルゴリズム	暗号操作	鍵長（ビット）	用途
AES CBC mode [FIPS197], [ISOIEC10116]	暗号化/復号	192	セキュアメッセージングの暗号化／復号
	復号		インポートする鍵の復号
CMAC with AES [ISOIEC9797_1], [FIPS197]	MAC 生成/検証		セキュアメッセージングの MAC 生成／検証 SCP11 のレシート生成
ECDSA [FIPS186_5]	公開鍵による署名検証	384 (NIST P-384)	外部認証
	秘密鍵による署名	384 (NIST P-384)	JPKI-AP による利用者証明 JPKI-AP による署名生成 認証 AP による内部認証
CTR_DRBG, Hash_DRBG, HMAC_DRBG [SP800_90A]	ノンスの生成	-	ECDSA の補助技術として使用
ECDH [TR03111]	一時鍵ペア生成	384 (NIST P-384)	セキュアメッセージングの鍵材料の共有
	共有秘密計算	384 (NIST P-384)	親展通信用の共有秘密の計算
KDF with SHA-384 [X9.63], [TR03111]	暗号鍵導出	192	セキュアメッセージングの鍵導出
SHA-384 [FIPS180_4]	ハッシュ演算	-	ECDSA の補助技術として使用
			セッション鍵導出

O.Phys_Attack

TSF は、TOE の構成要素（ハードウェア／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、[JILAP]に提示される。

［注釈：O.Phys_Attack］上記文書が扱う攻撃は、IC 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。

OE.AP

市区町村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 TOE 外の 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 AP を搭載しない。

OE.Terminal

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 内にデータまたは AP を設定する外部端末を、物理的に保護された安全な環境に設置されていることを確認し、通信経路上での盗難、改ざんを防止する。

OE.Card

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、有効期限切れなどの理由でカード保持者から返納された個人番号カードを安全に廃棄し、個人番号や暗号鍵の復元を防止する。

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 4-2 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 4-2 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 ＼ セキュリティ対策方針	O.I&A	O.Access_Control	O.Phys_Attack	O.Secure_Messaging	O.Delivery	O.Cryptography	O.RND	OE.PKI	OE.Administrator	OE.AP	OE.Terminal	OE.Card
T.Illegal_Attack	X	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		
A.Terminal											X	
A.Card												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.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、CC サポート文書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 2 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、アクセス対象にセキュアメッセージング属性が付与されている場合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 4-1 を参照し、それに対応することを述べている。また鍵のインポート、親展通信と鍵の消去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。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、TOE 外の 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。

A.Terminal

OE.Terminal は、TOE 内にデータまたは AP の設定を実施する外部端末が、物理的に保護された安全な環境に設置されていることの確認を求める。このセキュリティ対策方針は A.Terminal を直接満たす。

A.Card

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

5 拡張コンポーネント定義

本 PP では拡張コンポーネント定義を行わない。

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。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：ｘｘｘ］、［選択：ｘｘｘ］*斜体*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***明朝体の斜体***で示す。詳細化で置き換えられる SFR の記述を抹消線（~~抹消線~~）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、さらに短縮名に識別子を付けて示す。

本PPでは、一部の操作が未了であり、その個所を［割付：ｘｘｘ］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 クラス:暗号サポート

6.1.1.1 FCS_CKM.1 暗号鍵生成(鍵共有一時鍵ペア)

コンポーネント間の関係

下位階層： なし

依存性： ［FCS_CKM.2 暗号鍵配付、又は
FCS_CKM.5 暗号鍵導出、又は
FCS_COP.1 暗号操作］
［FCS_RBG.1 ランダムビット生成（RBG）、又は
FCS_RNG.1 乱数生成］
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_CKM.1.1

TSF は、次の［割付：*[FIPS186_5] A.2*］に合致する、指定された暗号鍵生成アルゴリズム［割付：*楕円曲線鍵ペア生成*］と指定された暗号鍵長［割付：*384 ビット（P-384）*］に従って、***鍵共有のための一時鍵ペア***~~暗号鍵~~を生成しなければならない。

6.1.1.2 FCS_CKM.2 暗号鍵配付(楕円曲線ディフィーヘルマン鍵共有)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出］

FCS_CKM.2.1

TSF は、次の[割付: *[GPC093] Section 4.1*]に合致する、指定された暗号鍵配付方法[割付: *SCP11a と SCP11b に準拠する鍵配付方法*]に従って、暗号鍵を配付しなければならない。

6.1.1.3 FCS_CKM.5 暗号鍵導出(楕円曲線ディフィーヘルマン鍵共有)

コンポーネント間の関係

下位階層： なし

依存性： [FCS_CKM.2 暗号鍵配付、又は
FCS_COP.1 暗号操作]
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_CKM.5.1

TSF は、次の［割付：*[TR03111] Section 4.3.3, [X9.63] Section 5.6.3*］に合致する、指定された暗号鍵導出アルゴリズム［割付：*KDF with SHA-384*］と指定された暗号鍵長［割付：*192 ビット*］に従って、［割付：*下記に示す秘密*］から暗号鍵［割付：*セッション鍵（Receipt key, S-DEK, S-ENC, S-MAC, S-RMAC）*］を導出しなければならない。

SCP11a の場合：外部端末から受信した一時公開鍵と TOE が生成した一時秘密鍵から生成した秘密と、外部端末から受信した証明書から抽出した公開鍵と外部端末へ送信する鍵合意用公開鍵証明書に対応する鍵合意用秘密鍵から生成する秘密

SCP11b の場合（認証 AP・券面等 AP の内部認証）：外部端末から受信した一時公開鍵と TOE が生成した一時秘密鍵から生成した秘密と、外部端末から受信した一時公開鍵と外部端末へ送信する鍵合意用公開鍵証明書に対応する鍵合意用秘密鍵から生成する秘密

6.1.1.4 FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出]

FCS_CKM.6.1

TSF は、［選択：*不要、［割付: 鍵又は鍵材料の破棄に関するその他の状況］*］になった場合、［割付：*下記に示す鍵または鍵材料*］を破棄しなければならない。

SCP11a：外部端末から受信した証明書から抽出した公開鍵と外部端末へ送信する鍵合意用公開鍵証明書に対応する鍵合意用秘密鍵から生成する秘密

SCP11b：外部端末から受信した一時公開鍵と外部端末へ送信する鍵合意用公開鍵証明書に対応する鍵合意用秘密鍵から生成する秘密

SCP11 共通：鍵共有のための一時秘密鍵、外部端末から受信した一時公開鍵と TOE が生成した一時秘密鍵から生成した秘密、Receipt key、S-DEK、S-ENC、S-MAC、S-RMAC

FCS_CKM.6.2

TSF は、次の［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、FCS_CKM.6.1 で指定した暗号鍵及び鍵材料を破棄しなければならない。

［注釈：FCS_CKM.6］揮発メモリのために、暗号破棄方法へ揮発メモリへの電源供給断を含めてもよい。

6.1.1.5 FCS_COP.1/ED 暗号操作(AES 暗号復号)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出］
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/ED

TSF は、［割付：*[FIPS197] (AES), [ISOIEC10116] (CBC)*］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：*192 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、S-DEK による機密データの復号*］を実行しなければならない。

6.1.1.6 FCS_COP.1/MAC 暗号操作(MAC)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出］
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/MAC

TSF は、［割付：*[ISOIEC9797_1] Section 7.6*］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：*192 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。

6.1.1.7 FCS_COP.1/KeyDec 暗号操作(鍵復号)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出］

FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/KeyDec

TSF は、[割付：*[FIPS197] (AES), [ISOIEC10116] (CBC)*]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：*192 ビット*］に従って、［割付：*インポートする鍵合意用秘密鍵、署名用秘密鍵、利用者証明用秘密鍵、内部認証用秘密鍵の復号*］を実行しなければならない。

6.1.1.8 FCS_COP.1/Receipt 暗号操作(レシート生成)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出］
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/Receipt

TSF は、[割付：*[ISOIEC9797_1] Section 7.6*]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：*192 ビット*］に従って、［割付：*SCP11 におけるレシート生成*］を実行しなければならない。

6.1.1.9 FCS_COP.1/SigGen 暗号操作(署名生成)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出］
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/SigGen

TSF は、[割付：*[FIPS186_5] Section 6*]に合致する、特定された暗号アルゴリズム［割付：*SHA-384 を使用した ECDSA*］と暗号鍵長［割付：*384 ビット（P-384）*］に従って、［割付：*署名生成*］を実行しなければならない。

6.1.1.10 FCS_COP.1/PersoAuth 暗号操作(利用者証明用署名生成)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は

FCS_CKM.5 暗号鍵導出]
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/PersoAuth

TSF は、[割付：*[FIPS186_5] Section 6*]に合致する、特定された暗号アルゴリズム［割付：*SHA-384 を使用した ECDSA*］と暗号鍵長［割付：*384 ビット（P-384）*］に従って、［割付：*利用者証明用署名生成*］を実行しなければならない。

6.1.1.11 FCS_COP.1/TOEAuth 暗号操作(TOE 内部認証用署名生成)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出]
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/TOEAuth

TSF は、[割付：*[FIPS186_5] Section 6*]に合致する、特定された暗号アルゴリズム［割付：*SHA-384 を使用した ECDSA*］と暗号鍵長［割付：*384 ビット（P-384）*］に従って、［割付：*TOE 内部認証用署名生成*］を実行しなければならない。

6.1.1.12 FCS_COP.1/ExtAuth 暗号操作(外部認証用署名検証)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出]
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/ExtAuth

TSF は、[割付：*[FIPS186_5] Section 6*]に合致する、特定された暗号アルゴリズム［割付：*SHA-384 を使用した ECDSA*］と暗号鍵長［割付：*384 ビット（P-384）*］に従って、［割付：*署名検証*］を実行しなければならない。

6.1.1.13 FCS_COP.1/Hash 暗号操作(ハッシュ演算)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は

FCS_CKM.5 暗号鍵導出]
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/Hash

TSF は、[割付：*[FIPS180_4]*に合致する、特定された暗号アルゴリズム［割付：*SHA-384*］と暗号鍵長［割付：*なし*］に従って、［割付：*ECDSA 署名生成、ECDSA 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、ECDH に関連する鍵導出、［割付：ハッシュ計算対象のリスト］*］を実行しなければならない。

6.1.1.14 FCS_COP.1/ShSes 暗号操作(親展通信用共有秘密計算)

コンポーネント間の関係

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のインポート、又は
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、又は
FCS_CKM.1 暗号鍵生成、又は
FCS_CKM.5 暗号鍵導出]
FCS_CKM.6 暗号鍵破棄のタイミング及びイベント

FCS_COP.1.1/ShSes

TSF は、[割付：*[TR03111] Section 4.3.2.2*]に合致する、特定された暗号アルゴリズム［割付：*エルガマル鍵合意*］と暗号鍵長［割付：*384 ビット（P-384）*］に従って、［割付：*親展通信用共有秘密計算*］を実行しなければならない。

6.1.1.15 FCS_RNG.1/ES 乱数生成(エントロピー源)

コンポーネント間の関係

下位階層： なし

依存性： なし

FCS_RNG.1.1/ES

TSF は、［割付：*セキュリティ能力のリスト*］を実装する［選択：*物理的、~~非物理的な真性、決定論的、ハイブリッド物理的、ハイブリッド決定論的~~*］乱数生成器を提供しなければならない。

FCS_RNG.1.2/ES

TSF は、［割付：*定義された品質尺度*］を満たす［選択：*ビット、ビットのオクテット、数値［割付：数値の形式］*］を提供しなければならない。

［注釈：FCS_RNG.1/ES］想定される乱数生成器は[KS2011]における PTG.2 クラスである。このセキュリティ機能要件は[FIPS186_5]で要求されている DRBG のエントロピー源[3]である。

6.1.1.16 FCS_RNG.1/DRBG 乱数生成(DRBG)

コンポーネント間の関係

[3] [FIPS186_5] A.3.3 の deterministic ECDSA に使用される HMAC_DRBG を除く。

下位階層： なし

依存性： なし

FCS_RNG.1.1/DRBG

TSF は、［割付：*表 6-1 の適用する DRBG*］を実装する［選択：*~~物理的、非物理的な真性、決定論的、ハイブリッド物理的、ハイブリッド決定論的~~*］乱数生成器を提供しなければならない。

FCS_RNG.1.2/DRBG

TSF は、［割付：*表 6-1 の生成長*］を満たす［選択：*ビット~~、ビットのオクテット、数値 ［割付：数値の形式］~~*］を提供しなければならない。

表 6-1 使用する DRBG

生成物	*[FIPS186_5]における生成法*	*適用する DRBG*	*標準*	*生成長*
一時鍵	*［選択：A.2.1、A.2.2］*	*［選択：CTR_DRBG、Hash DRBG、HMAC_DRBG］*	*[SP800_90A]*	*［割付：生成長］*
［選択：ノンス、なし］	*［選択：A.3.1、A.3.2、A.3.3、なし］*	*［選択：CTR_DRBG、Hash DRBG、HMAC_DRBG、なし］*	*［選択：[SP800_90A]、なし］*	*［選択：［割付：生成長］、なし］*

［注釈：FCS_RNG.1/DRBG］ このセキュリティ機能要件は[FIPS186_5] A.2 の一時鍵生成、A.3 の Per-massage secret（ノンス）に使用される DRBG である。ST 作者は一時鍵生成について[FIPS186_5] A.2.1 または A.2.2 を選択し、使用している DRBG を割付ける。また、ノンスの生成について[FIPS186_5] A.3.1、A.3.2、A.3.3 のいずれかを選択し、使用している DRBG を選択する。生成長は 384～511 である。A3.3 を使用し、HMAC_DRBG を使用しない場合、すべて「なし」を選択すること。

6.1.2 FDP クラス：利用者データ保護

6.1.2.1 FDP_ACC.1 サブセットアクセス制御

コンポーネント間の関係

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 6-2 のサブジェクト欄に示すプロセス、オブジェクト：表 6-2 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 6-2 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 6-2 サブジェクト、オブジェクト、操作

サブジェクト（対応する利用者）	*オブジェクト*	*成功が必要な認証*	*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：外部認証、輸送鍵照合、［割付：認証のリスト］］*	*［選択：書換え、読出し］＊*
	SSD	*外部認証*	*生成・削除*
空き領域管理者を代行するプロセス	*TOE 外 AP*	*外部認証*	*生成・削除*
外部端末を代行するプロセス	*SCP11a 用の鍵合意用公開鍵証明書ファイル*	*なし*	*読出し*
認証 AP			
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：外部認証、輸送鍵照合、［割付：認証のリスト］］*	*［選択：書換え、読出し］＊*
外部端末を代行するプロセス	*SCP11b の鍵合意用公開鍵証明書ファイル*	*なし*	*読出し*
外部端末を代行するプロセス	*内部認証用公開鍵証明書ファイル*	*なし*	*読出し*
カード保持者を代行するプロセス	*親展通信用公開鍵証明書ファイル*	*暗証番号照合*	*読出し*
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：外部認証、輸送鍵照合、［割付：認証のリスト］］*	*［選択：書込み、書換え、読出し］＊*
住基 AP 管理者を代行するプロセス	*住民票コードファイル*	*輸送鍵照合*	*書込み*
		外部認証	*書換え*
		外部認証	*読出し*
カード保持者かつ住基データを扱うシステムを代行するプロセス[4]	*住民票コードファイル*	*外部認証かつ暗証番号照合*	*読出し*
JPKI-AP			
JPKI-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：外部認証、輸送鍵照合、［割付：認証のリスト］］*	*［選択：書換え、読出し］＊*

[4] 住民票コードファイルの読出しはカード保持者の認証成功と住基データを扱うシステムの認証成功の両方を必要とする。

サブジェクト（対応する利用者）	*オブジェクト*	*成功が必要な認証*	*操作*
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*	*署名用パスワード照合*	*署名*
	利用者証明用秘密鍵による署名機能	*暗証番号照合*	*署名*
	利用者証明用証明書ファイル	*なし*	*読出し*
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*	*［割付：認証のリスト］*	*署名*
	利用者証明用証明書ファイル	*なし*	*読出し*
券面等データ AP			
券面等データ 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：外部認証、輸送鍵照合、認証のリスト］*	*［選択：書換え、読出し］＊*
券面等データ AP 管理者を代行するプロセス	*個人番号（テキスト）ファイル* *4 情報（テキスト）ファイル* *個人番号・4 情報署名ファイル*	*輸送鍵照合または外部認証*	*書換え*
カード保持者を代行するプロセス		*暗証番号照合または署名用パスワード照合*	*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		*外部認証*	*読出し*
券面等 AP			
券面等 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：外部認証、輸送鍵照合、認証のリスト］*	*［選択：書換え、読出し］＊*
券面等 AP 管理者を代行するプロセス	*券面事項情報ファイル* *生年月日情報（画像）ファイル* *個人番号（画像）ファイル* *個人番号（テキスト）ファイル* *4 情報（テキスト）ファイル* *個人番号・4 情報署名ファイル*	*輸送鍵照合または外部認証*	*書換え*
外部端末を代行するプロセス	*SCP11b 用の鍵合意用公開鍵証明書ファイル*	*なし*	*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	*券面事項情報ファイル*	*外部認証*	*読出し*
生年月日を扱うシステムを代行するプロセス	*生年月日情報（画像）ファイル*	*外部認証*	
個人番号を扱うシステムを代行するプロセス	*個人番号（画像）ファイル*	*外部認証*	
個人番号・4 情報を扱うシステムを代行するプロセス	*個人番号（テキスト）ファイル* *4 情報（テキスト）ファイル* *個人番号・4 情報署名ファイル*	*外部認証*	

*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。

6.1.2.2 FDP_ACF.1 セキュリティ属性によるアクセス制御

コンポーネント間の関係

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、次の［割付：*サブジェクト：表 6-2 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 6-2 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：表 6-2 の成功が必要な認証欄に記載されたサブジェクトに関連付けられる利用者の認証結果*］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、当該サブジェクトは、当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。

6.1.2.3 FDP_ETC.1 セキュリティ属性なし利用者データのエクスポート

コンポーネント間の関係

下位階層： なし

依存性： ［FDP_ACC.1 サブセットアクセス制御、又は
FDP_IFC.1 サブセット情報フロー制御］

FDP_ETC.1.1

TSF は、SFP 制御下にある利用者データ ***(親展通信用共有秘密)***を TOE の外部にエクスポートするとき、［割付: *親展通信情報フロー制御 SFP*］を実施しなければならない。

FDP_ETC.1.2

TSF は、利用者データに関係したセキュリティ属性なしで利用者データをエクスポートしなければならない。

6.1.2.4 FDP_IFC.1/PubKey サブセット情報フロー制御

コンポーネント間の関係

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/PubKey

TSF は、［割付：*サブジェクト：外部端末から外部認証用公開鍵・鍵合意用公開鍵をインポートする TOE のプロセス、情報：外部認証用公開鍵・鍵合意用公開鍵、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。

6.1.2.5 FDP_IFC.1/Pri サブセット情報フロー制御

コンポーネント間の関係

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/Pri

TSF は、［割付：*サブジェクト：外部端末から親展通信用一時公開鍵をインポートして親展通信用共有秘密をエクスポートする TOE のプロセス、情報：親展通信用一時公開鍵、親展通信用共有秘密、操作：親展通信用一時公開鍵のインポート、親展通信用共有秘密のエクスポート*］に対して「割付：*親展通信情報フロー制御 SFP*」を実施しなければならない。

6.1.2.6 FDP_IFF.1/PubKey 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/PubKey

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：外部認証用公開鍵・鍵合意用公開鍵をインポートする TOE のプロセス、情報：外部認証用公開鍵・鍵合意用公開鍵、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/PubKey

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：*

外部認証用公開鍵・鍵合意用公開鍵：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/PubKey

TSF は、［割付：*なし*］を実施しなければならない。

FDP_IFF.1.4/PubKey

TSF は、次の規則、［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/PubKey

TSF は、次の規則、［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。

6.1.2.7 FDP_IFF.1/Pri 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/Pri

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：*親展通信情報フロー制御 SFP*］を実施しなければならない。：［割付：*サブジェクト：外部端末から親展通信用一時公開鍵をインポートして親展通信用共有秘密をエクスポートする TOE のプロセス、情報：親展通信用一時公開鍵・親展通信用共有秘密、サブジェクトのセキュリティ属性：セキュアメッセージング実施かつ暗証番号照合の成功*］

FDP_IFF.1.2/Pri

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、セキュアメッセージングが実行され、外部端末から親展通信用一時公開鍵をインポートして親展通信用共有秘密をエクスポートする TOE のプロセスが暗証番号の照合に成功したとき、親展通信用一時公開鍵のサブジェクトへのインポートを許可し、親展通信用共有秘密のエクスポートを許可する*］。

FDP_IFF.1.3/Pri

TSF は、［割付：*なし*］を実施しなければならない。

FDP_IFF.1.4/Pri

TSF は、次の規則、［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/Pri

TSF は、次の規則、［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。

6.1.2.8 FDP_ITC.1/PubKey セキュリティ属性なし利用者データのインポート(外部認証用公開鍵・鍵合意用公開鍵)

コンポーネント間の関係

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/PubKey

TSF は、SFP 制御下の利用者データ ***(外部認証用公開鍵・鍵合意用公開鍵)***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/PubKey

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/PubKey

TSF は、SFP 制御下の利用者データを TOE 外部から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。

6.1.2.9 FDP_ITC.1/Pri セキュリティ属性なし利用者データのインポート(親展通信用一時公開鍵)

コンポーネント間の関係

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/Pri

TSF は、SFP 制御下の利用者データ ***(親展通信用一時公開鍵)***を TOE の外部からインポートするとき、［割付：*親展通信情報フロー制御 SFP*］を実施しなければならない。

FDP_ITC.1.2/Pri

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/Pri

TSF は、SFP 制御下の利用者データを TOE 外部から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。

6.1.2.10 FDP_ITC.1/UData セキュリティ属性なし利用者データのインポート(外部認証用公開鍵・鍵合意用公開鍵・親展通信用一時公開鍵以外のデータ)

コンポーネント間の関係

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/UData

TSF は、SFP 制御下の利用者データ ***(外部認証用公開鍵・鍵合意用公開鍵・親展通信用一時公開鍵を除くデータ)***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/UData

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/UData

TSF は、SFP 制御下の利用者データを TOE 外部から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。

6.1.3 FIA クラス：識別と認証

6.1.3.1 FIA_AFL.1 認証失敗時の取り扱い

コンポーネント間の関係

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：*表 6-3 の認証事象のリスト*］に関して、［選択：*［割付：表 6-3 の回数］*、~~［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：*表 6-3 のアクションのリスト*］をしなければならない。

表 6-3 認証失敗時の取り扱い

認証事象のリスト	*回数*	*アクションのリスト*
署名用パスワード[5]認証	*5*	*署名用パスワードのロック* *認証 AP の外部認証成功によりロック解除*
暗証番号認証	*3*	*暗証番号のロック* *PUK の照合成功、あるいは認証 AP の外部認証成功によりロック解除*
PUK 認証	*10*	*PUK のロック* *署名用パスワードの照合成功、あるいは認証 AP の外部認証成功によりロック解除*
輸送鍵認証	*3*	*輸送鍵のロック*
［割付：認証事象のリスト］	*［割付：回数］*	*［割付：アクションのリスト］*

6.1.3.2 FIA_API.1 識別情報の認証証明

コンポーネント間の関係

下位階層： なし

依存性： なし

[5] 署名用パスワードはアルファベットと数字、暗証番号・PUK は数字のみで構成される。

FIA_API.1.1

TSF は、外部エンティティに次の特性［*割付：プラットフォームの SCP11a 鍵合意用公開鍵証明書、認証 AP の SCP11b 鍵合意用公開鍵証明書、券面等 AP の SCP11b 鍵合意用公開鍵証明書*］を含めることにより、［*割付：プラットフォーム、認証 AP、券面等 AP*］の識別情報を証明する［*割付：プラットフォームは SCP11a に基づく内部認証プロトコル、認証 AP と券面等 AP は SCP11b による内部認証プロトコル*］を提供しなければならない。

6.1.3.3 FIA_SOS.2 TSF 秘密生成

コンポーネント間の関係

下位階層： なし

依存性： なし

FIA_SOS.2.1

TSF は、［*割付：[FIPS186_5] [選択： A.3.1、A.3.2、A.3.3]* ］に合致する*ノンス*秘密を生成するメカニズムを提供しなければならない。

FIA_SOS.2.2

TSF は、［*割付：署名生成*］に対し、TSF 生成の*ノンス*秘密の使用を実施できなければならない。

［注釈：FIA_SOS.2］[FIPS186_5] A.3 に記載されている Per-massage secret に従いノンスを生成する。ST 作者は、使用している生成法を FCS_RNG.1/DRBG に記述すること。ただし、[FIPS186_5] A.3.3 を選択し、HMAC_DRBG を使用せず、A.3.3 に記述されている生成アルゴリズムを使用する場合、FCS_COP.1/Hash の割付に「ECDSA 署名生成に関連して要求されるノンス」を記入すること。

6.1.3.4 FIA_UAU.1 認証のタイミング

コンポーネント間の関係

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：*表 6-4 の TSF 仲介アクションのリスト*］を許可しなければならない。

表 6-4 TSF 仲介アクションのリスト

AP	*TSF 仲介アクション*
すべての AP	*ISD、SSD、AP の選択*
プラットフォーム	*SCP11a 用の鍵合意用公開鍵証明書ファイルの読出し*
	TOE に格納済みの署名者の公開鍵による、外部装置が入力する公開鍵証明書の検証
	［割付：個人番号カードアクセス制御 SFP、暗号鍵インポート情報フロー制御 SFP に競合せず、TSF データにアクセスしない TSF 仲介アクションのリスト］
認証 AP	*SCP11b の鍵合意用公開鍵証明書ファイルの読出し*

AP	*TSF 仲介アクション*
	内部認証用公開鍵証明書ファイルの読出し
	SCP11b の開始
	チャレンジの送信
	［割付：個人番号カードアクセス制御 SFP、親展通信情報フロー制御 SFP、暗号鍵インポート情報フロー制御 SFP に競合せず、TSF データにアクセスしない TSF 仲介アクションのリスト］
JPKI-AP	*利用者証明用証明書ファイルの読出し*
	［割付：個人番号カードアクセス制御 SFP に競合せず、TSF データにアクセスしない TSF 仲介アクションのリスト］
券面等 AP	*SCP11b の鍵合意用公開鍵証明書ファイルの読出し*
	SCP11b の開始
	チャレンジの送信
	［割付：個人番号カードアクセス制御 SFP、暗号鍵インポート情報フロー制御 SFP に競合せず、TSF データにアクセスしない TSF 仲介アクションのリスト］
［割付：AP のリスト］	*［割付：個人番号カードアクセス制御 SFP、暗号鍵インポート情報フロー制御 SFP に競合せず、TSF データにアクセスしない TSF 仲介アクションのリスト］*

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。

6.1.3.5 FIA_UAU.4 単一使用認証メカニズム

コンポーネント間の関係

下位階層： なし

依存性： なし

FIA_UAU.4.1

TSF は、［割付：*表 6-5 に示す認証メカニズム*］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 6-5 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	*認証メカニズム*	*対象*
認証 AP、住基 AP、JPKI-AP、券面等データ AP、券面等 AP	*外部認証*	*外部認証におけるチャレンジ*

6.1.3.6 FIA_UAU.5 複数の認証メカニズム

コンポーネント間の関係

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：*表 6-6 に示す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：*表 6-6 に示す認証の提供方法*］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。

表 6-6 複数の認証メカニズム

認証メカニズム	***認証を必要とする AP***	***認証の提供方法***
署名用パスワード照合	*認証 AP* *JPKI-AP* *券面等データ AP*	*カード保持者が入力した値と認証 AP が格納している署名用パスワードが一致したときに認証を提供する。*
暗証番号照合	*認証 AP* *住基 AP* *JPKI-AP* *券面等データ AP*	*カード保持者が入力した値と認証 AP が格納している暗証番号が一致したときに認証を提供する。*
PUK 照合	*認証 AP*	*カード保持者が入力した値と認証 AP が格納している PUK が一致したときに認証を提供する。*
輸送鍵照合	*プラットフォーム*	*プラットフォーム管理者が入力した値とプラットフォームが格納している輸送鍵が一致したときに認証を提供する。*
	認証 AP *住基 AP* *JPKI-AP* *券面等データ AP*	*左記の AP 管理者が入力した値と認証 AP が格納している輸送鍵が一致したときに認証を提供する。*
	券面等 AP	*券面等 AP 管理者が入力した値と券面等 AP が格納している輸送鍵が一致したときに認証を提供する。*
外部認証	*プラットフォーム*	*外部装置* が入力する公開鍵証明書をプラットフォームが格納している公開鍵で検証して成功したとき認証を提供する。*
	認証 AP *住基 AP* *JPKI-AP* *券面等データ AP* *券面等 AP*	*外部装置が入力する公開鍵証明書を左記の各 AP が格納している公開鍵で検証して成功したとき、その証明書に含まれている公開鍵を一時的に保存する。* *外部装置のチャレンジ要求に従い、TOE がチャレンジを外部装置に送信する。外部装置がチャレンジに一時的な公開鍵に対応する秘密鍵で署名を付与する。* *外部装置が署名を TOE に送信し、TOE が一時的な公開鍵で署名を検証して、成功したとき認証を提供する。*
［割付：認証メカニズムのリスト］	*［割付：認証する AP のリスト］*	*［割付：認証の提供方法のリスト］*

*外部装置は、表 6-2 のサブジェクトを代行するプロセスに相当する。

6.1.3.7 FIA_UID.1 識別のタイミング

コンポーネント間の関係

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：*表 6-4 の 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すべての 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。

6.1.4 FMT クラス：セキュリティ管理

6.1.4.1 FMT_LIM.1 制限された能力

コンポーネント間の関係

下位階層： なし

依存性： FMT_LIM.2 制限された可用性

FMT_LIM.1.1

TSF は、「制限された可用性(FMT_LIM.2)」と合わせて、以下の方針が実施されるように、その能力を制限しなければならない。

［割付：*パーソナライゼーション時の輸送鍵の閉塞[6]後、輸送鍵の閉塞解除、輸送鍵認証の成功を禁止する。*］

［注釈：FMT_LIM.1］FMT_LIM.2 と合せて、輸送鍵認証の成功を禁ずることにより、TSF データの暴露、改変を防止する。

6.1.4.2 FMT_LIM.2 制限された可用性

コンポーネント間の関係

下位階層： なし

依存性： FMT_LIM.1 制限された能力

FMT_LIM.2.1

TSF は、「制限された能力(FMT_LIM.1)」と合わせて、以下の方針が実施されるように、その可用性を制限するように設計されなければならない。

［割付：*パーソナライゼーション時の輸送鍵の閉塞後、輸送鍵の閉塞解除、輸送鍵認証の成功を禁止する。*］

6.1.4.3 FMT_MSA.3 静的属性初期化

コンポーネント間の関係

下位階層： なし

[6] 閉塞には、輸送鍵のロックと輸送鍵認証コマンド APDU の停止の二つの方法がある。

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(TOE 外 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（プラットフォーム管理者、空き領域管理者）*］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（TOE 外 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。

6.1.4.4 FMT_MTD.1 TSF データの管理

コンポーネント間の関係

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 6-7 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：閉塞解除、その他の操作］*］する能力を［割付：*表 6-7 に示す管理者*］に制限しなければならない。

表 6-7 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*
認証 AP	*暗証番号*	*カード保持者* *認証 AP 管理者* *認証 AP の情報を扱うシステム*[7]
	署名用パスワード	
	PUK	
券面等 AP	*［割付: TSF データのリスト］*	*券面等 AP 管理者*

[7] 認証情報を扱うシステムは、暗証番号を変更する権限を持つ。変更された暗証番号はカード保持者へ通知される。

適用箇所	*TSF データ*	*TSF データの管理者に相当する者*
		券面事項情報を扱うシステム

6.1.4.5 FMT_SMF.1 管理機能の特定

コンポーネント間の関係

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 6-8 に示す管理機能*］

表 6-8 管理機能

適用箇所	*管理機能*
認証 AP	*署名用パスワードの閉塞解除・変更、暗証番号の閉塞解除・変更、PUK の閉塞解除・変更*
券面等 AP	*［割付：管理機能のリスト］*

6.1.4.6 FMT_SMR.1 セキュリティの役割

コンポーネント間の関係

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 AP において、表 6-9 に示す役割*］を維持しなければならない。

表 6-9 セキュリティの役割

適用箇所	*役割*
プラットフォーム	*プラットフォーム管理者、空き領域管理者*
認証 AP	*カード保持者、認証 AP 管理者、認証 AP の情報を扱うシステム*
券面等 AP	*券面等 AP 管理者、券面事項情報を扱うシステム*

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。

6.1.5 FPT クラス：TSF の保護

6.1.5.1 FPT_PHP.3 物理的攻撃への抵抗

コンポーネント間の関係

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 を実装する全てのハードウェアコンポーネント*］への［割付：*物理的手段を使用した攻撃であって、[JILAP]最新版が定める 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］[JILAP]は、TOE 評価時の最新のものが適用される。

6.1.6 FTP クラス:高信頼パス／チャネル

6.1.6.1 FTP_ITC.1 TSF 間高信頼チャネル

コンポーネント間の関係

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 6-10 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 6-10 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*
認証 AP	*アクセス対象にセキュアメッセージング属性が付与されている場合に適用*	*アクセス対象にセキュアメッセージング属性が付与されている場合に適用*
住基 AP		
JPKI-AP		
券面等データ AP		
券面等 AP		

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、ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1,

ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_VAN.5 である。

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

TOE のセキュリティ対策方針に対応する SFR を表 6-11 に示す。

表 6-11　TOE セキュリティ対策方針と SFR の対応

セキュリティ対策方針 / SFR	O.I&A	O.Access_Control	O.Phys_Attack	O.Secure_Messaging	O.Delivery	O.Cryptography	O.RND
FCS_CKM.1				X		X	
FCS_CKM.2				X		X	
FCS_CKM.5				X		X	
FCS_CKM.6				X		X	
FCS_COP.1/ED				X		X	
FCS_COP.1/MAC				X		X	
FCS_COP.1/KeyDec						X	
FCS_COP.1/Receipt						X	
FCS_COP.1/SigGen						X	
FCS_COP.1/PersoAuth						X	
FCS_COP.1/TOEAuth						X	
FCS_COP.1/ExtAuth	X					X	
FCS_COP.1/Hash	X					X	
FCS_COP.1/ShSes						X	
FCS_RNG.1/ES				X			X
FCS_RNG.1/DRBG				X		X	
FDP_ACC.1		X		X		X	
FDP_ACF.1		X		X		X	
FDP_ETC.1						X	
FDP_IFC.1/PubKey	X			X		X	
FDP_IFC.1/Pri						X	
FDP_IFF.1/PubKey	X			X		X	
FDP_IFF.1/Pri						X	

セキュリティ対策方針 / SFR	O.I&A	O.Access_Control	O.Phys_Attack	O.Secure_Messaging	O.Delivery	O.Cryptography	O.RND
FDP_ITC.1/PubKey	X			X		X	
FDP_ITC.1/Pri						X	
FDP_ITC.1/UData		X		X		X	
FIA_AFL.1	X						
FIA_API.1				X			
FIA_SOS.2						X	
FIA_UAU.1	X				X		
FIA_UAU.4	X						
FIA_UAU.5	X				X		
FIA_UID.1	X				X		
FMT_LIM.1					X		
FMT_LIM.2					X		
FMT_MSA.3		X					
FMT_MTD.1	X						
FMT_SMF.1	X						
FMT_SMR.1	X	X					
FPT_PHP.3			X				X
FTP_ITC.1				X		X	

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認証では、FCS_COP.1/ExtAuth による ECDSA 検証操作、FCS_COP.1/Hash 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外部認証用公開鍵・鍵合意用公開鍵のインポートは、FDP_ITC.1/PubKey、FDP_IFC.1/PubKey、FDP_IFF.1/PubKey で規定し、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。これらの 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、TOE 外の 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、外部から暗号鍵と利用者データをインポートする。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/UData 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.Secure_Messaging

セキュアメッセージングは、FTP_ITC.1 によってアクセス対象にセキュアメッセージング属性が付与されている場合、適用される。SCP11a では、FCS_CKM.1、FCS_RNG.1/ES・FCS_RNG.1/DRBG によって一時鍵を生成し、FCS_CKM.2 によって外部端末へ一時公開鍵を送信する。生成した一時秘密鍵と、外部端末から受信した一時公開鍵、外部端末から受信した証明書から抽出する公開鍵、ならびに外部端末へ送信する鍵合意用公開鍵証明書に対応する鍵合意用秘密鍵から、FCS_CKM.5 によってセッション鍵を導出する。SCP11b では、FCS_CKM.1、FCS_RNG.1/ES・FCS_RNG.1/DRBG によって一時鍵を生成し、FCS_CKM.2 によって外部端末へ一時公開鍵を送信する。生成した一時秘密鍵と外部端末から受信した一時公開鍵、外部端末へ送信する鍵合意用公開鍵証明書に対応する鍵合意用秘密鍵から FCS_CKM.5 によってセッション鍵を導出する。

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、外部端末と交換した一時鍵、外部端末から送付された証明書から得られる公開鍵、カードに保持されている鍵合意用秘密鍵から導出される。鍵導出に使用する外部認証用公開鍵・鍵合意用公開鍵のインポートは、FDP_ITC.1/PubKey、FDP_IFC.1/PubKey、FDP_IFF.1/PubKey で規定し、鍵合意用公開鍵証明書または内部認証用公開鍵証明書の外部端末への送信は FDP_ACC.1、FDP_ACF.1、FIA_API.1 で規定する。生成した一時秘密鍵の破棄は FCS_CKM.6 で規定される。AES の暗号操作は FCS_COP.1/ED、FCS_COP.1/MAC でそれぞれ規定される。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.6 で規定される。公開鍵方式で使用する鍵合意用公開鍵証明書・鍵合意用秘密鍵のインポートは FDP_ITC.1/UData、FDP_ACC.1、FDP_ACF.1 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、輸送鍵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。輸送鍵による認証成功後のアクセス機能を無効化するために、FMT_LIM.1 と FMT_LIM.2 が規定される。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（暗号鍵生成、暗号鍵導出）は、表 4-1 で規定される。暗号アルゴリズムと暗号操作は、FCS_CKM.1、FCS_CKM.2、FCS_CKM.5、FCS_COP.1/ED、FCS_COP.1/MAC、FCS_COP.1/Receipt、FCS_COP.1/SigGen 、 FCS_COP.1/PersoAuth 、 FCS_COP.1/TOEAuth, FCS_COP.1/ExtAuth 、FCS_COP.1/Hash で規定される。署名生成におけるノンスの生成は FIA_SOS.2・FCS_RNG.1/DRBG で規定される。暗号鍵のインポート要件は FDP_ITC.1/PubKey、FDP_ITC.1/UData で規定され、セキュアなインポートのために FCS_COP.1/KeyDec、FDP_ACC.1、FDP_ACF.1、FDP_IFC.1/PubKey、FDP_IFF.1/PubKey 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.6 で規定される。親展通信においては、共有秘密の生成は FCS_COP.1/ShSes で規定され、親展通信用公開鍵証明書の読出しは FDP_ACC.1. FDP_ACF.1 で、親展通信用一時公開鍵のインポートは FDP_IFC.1/Pri、FDP_IFF.1/Pri、FDP_ITC.1/Pri で、親展通信用共有秘密のエクスポートは FDP_ETC.1 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。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/ES 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、乱数生成器への物理的攻撃で出力乱数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。

6.3.1.1 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 6-12 に示す。

表 6-12 SFR の依存性

SFR	依存性の要求	依存性の対応
FCS_CKM.1	［FCS_CKM.2 又は FCS_CKM.5 又は FCS_COP.1］、［FCS_RBG.1 又は FCS_RNG.1］、FCS_CKM.6	FCS_CKM.5、FCS_CKM.2、FCS_RNG.1/ES、FCS_RNG.1/DRBG、FCS_CKM.6
FCS_CKM.2	［FDP_ITC.1 又は FDP_ITC.2 又は FCS_CKM.1 又は FCS_CKM.5］	FCS_CKM.1
FCS_CKM.5	［FCS_CKM.2 又は FCS_COP.1］、FCS_CKM.6	FCS_COP.1/ED、FCS_COP.1/MAC、FCS_COP.1/Receipt、FCS_CKM.6、注 1
FCS_CKM.6	［FDP_ITC.1 又は FDP_ITC.2 又は FCS_CKM.1 又は FCS_CKM.5］	FCS_CKM.1、FCS_CKM.5
FCS_COP.1/ED		FCS_CKM.5、FCS_CKM.6
FCS_COP.1/MAC		

SFR	依存性の要求	依存性の対応
FCS_COP.1/Receipt	［FDP_ITC.1 又は FDP_ITC.2 又は FCS_CKM.1 又は FCS_CKM.5］、FCS_CKM.6	
FCS_COP.1/KeyDec		FDP_ITC.1/UData、注２
FCS_COP.1/SigGen		
FCS_COP.1/PersoAuth		
FCS_COP.1/TOEAuth		
FCS_COP.1/ExtAuth		FDP_ITC.1/PubKey、注３
FCS_COP.1/Hash		注４
FCS_COP.1/ShSes		FDP_ITC.1/Pri、FDP_ITC.1/UData、注２、注３
FCS_RNG.1/ES	なし	NA
FCS_RNG.1/DRBG		
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1、FMT_MSA.3	FDP_ACC.1、注５
FDP_ETC.1	［FDP_ACC.1 又は FDP_IFC.1］	FDP_IFC.1/Pri
FDP_IFC.1/PubKey	FDP_IFF.1	FDP_IFF.1/PubKey
FDP_IFC.1/Pri		FDP_IFF.1/Pri
FDP_IFF.1/PubKey	FDP_IFC.1、FMT_MSA.3	FDP_IFC.1/PubKey、注６
FDP_IFF.1/Pri		FDP_IFC.1/Pri、注６
FDP_ITC.1/PubKey	［FDP_ACC.1 又は FDP_IFC.1］、FMT_MSA.3	FDP_IFC.1/PubKey、注６
FDP_ITC.1/Pri		FDP_IFC.1/Pri、注６
FDP_ITC.1/UData		FDP_ACC.1、注７
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_API.1	なし	NA
FIA_SOS.2	なし	NA
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4	なし	NA
FIA_UAU.5	なし	NA
FIA_UID.1	なし	NA
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FMT_MSA.3	FMT_MSA.1、FMT_SMR.1	FMT_SMR.1、注８
FMT_MTD.1	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_SMF.1	なし	NA
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_PHP.3	なし	NA
FTP_ITC.1	なし	NA

注１：FCS_COP.1/KeyDec、FCS_COP.1/SigGen、FCS_COP.1/PersoAuth、FCS_COP.1/TOEAuth, FCS_COP.1/ExtAuth は、これらのセキュリティ機能要件の暗号操作を行う暗号鍵がカードの交付前に書込まれているため FCS_CKM.5 からの依存性は必要ない。FCS_COP./1/Hash は鍵がないため依存性は必要ない。

注２：FDP_ITC.1/UData によってカードに書き込まれる鍵は、OE.Card により、個人番号カードの有効期限切れや、カード保持者の要望により返納された後、適切に廃棄される。

注３：FDP_ITC.1/PubKey、FDP_ITC.1/Pri にてインポートする暗号鍵は公開鍵のため破棄をしない。

注４：暗号鍵を使用しないため要求する依存性は必要ない。

注５：TOE 外 AP と SSD については、FMT_MSA.3 が対応、その他は開発環境でファイル設定済みであり、依存性を満たす必要がない。

注６：外部認証用公開鍵、親展通信用一時公開鍵は一時的に使われるため依存 SFR は必要ない。

注７：開発環境でファイル設定済みであり、依存性を満たす必要がない。

注８：FMT_MSA.3 の対象となるオブジェクトは条例利用 AP と SSD であり、これらの属性は設定後に変更されない。そのため依存性を満たす必要がない。

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、TOE 外の 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、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 参考文書

[CC] 情報技術セキュリティ評価のためのコモンクライテリア CC:2022 改訂第 1 版 翻訳第 1.0 版
パート 1: 概説と一般モデル CCMB-2022-11-001
パート 2: セキュリティ機能コンポーネント CCMB-2022-11-002
パート 3: セキュリティ保証コンポーネント CCMB-2022-11-003
パート 4: 評価方法及び評価アクティビティの仕様のための枠組み CCMB-2022-11-004
パート 5: セキュリティ要件の定義済みパッケージ CCMB-2022-11-004

[CEM] 情報技術セキュリティ評価のための共通方法 評価方法 CEM:2022 改訂第 1 版 翻訳第 1.0 版 CCMB-2022-11-006

[ERT] CC:2022(リリース 1)及び CEM:2022(リリース 1)の正誤表と解釈, バージョン: 1.1, 発行日:2024 年 7 月 22 日 令和 6 年 12 月 翻訳第 1.0 版

[FIPS180_4] FIPS PUB 180-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), August 2015

[FIPS186_5] FIPS PUB 186-5, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Digital Signature Standard (DSS), Published: February 3, 2023

[FIPS197] FIPS PUB 197 Federal Information Processing Standards Publication Advanced Encryption Standard (AES), Published November 26, 2001; Updated May 9, 2023

[GPC093] GlobalPlatform Technology Secure Channel Protocol '11' Card Specification v2.3 - Amendment F, Version 1.2, Public Release July 2018

[ISOIEC9797_1] ISO/IEC 9797-1:2011, Information technology - Security techniques - Message Authentication Codes (MACs), Part 1: Mechanisms using a block cipher, Edition 2, 2011

[ISOIEC10116] ISO/IEC 10116:2017, Information technology - Security techniques - Modes of operation for an n-bit block cipher, Edition 4, 2017

[JILAP] Joint Interpretation Library Application of Attack Potential to Smartcards and Similar Devices, Version 3.2.1, February 2024

[KS2011] A proposal for: Functionality classes for random number generators Version 2.0 18 September 2011

[SP800_90A] NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

[TR03111] Technical Guideline BSI TR-03111, Elliptic Curve Cryptography, Version 2.10, Date: 2018-06-01

[X9.63] ANSI X9.63. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011

以上