認 証 報 告 書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　齊藤　裕

原紙押印済

プロテクションプロファイル（PP）

申請受付日（受付番号）	令和6年9月6日（IT認証4903）
認証識別	JISEC-C0858
認証申請者	地方公共団体情報システム機構
PPの名称	個人番号カード Version 2 プロテクションプロファイル
PPのバージョン	1.00
PP適合	なし
保証パッケージ	EAL4及び追加の保証コンポーネントALC_DVS.2、AVA_VAN.5
開発者	地方公共団体情報システム機構
ITセキュリティ評価機関の名称	株式会社ECSEC Laboratory 評価センター

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
令和7年12月1日

セキュリティセンター 技術評価部
技術管理者 橋本 徹

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 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 リリース1
② 情報技術セキュリティ評価のための共通方法 CEM:2022 リリース1
③ 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

評価結果：合格

「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」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、地方公共団体情報システム機構が開発した「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」（以下「PP[11]」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が令和 7 年 9 月 4 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である地方公共団体情報システム機構に報告するとともに、PP[11]に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応する PP[11]を併読されたい。特に PP[11]に適合する TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、PP[11]において詳述されている。

本認証報告書は、PP[11]に適合した製品開発を行う開発者及び製品調達者を読者と想定している。本認証報告書は、PP[11]に対する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価PP

PP[11]が要求するセキュリティ機能の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

PP[11]において要求される保証パッケージは、EAL4 追加である。追加の保証コンポーネントは、ALC_DVS.2、AVA_VAN.5 である。

また、PP[11]への適合を主張する PP、及び ST は論証適合を主張しなければならない。

1.1.2 PP概要

PP[11]は、社会保障・税番号制度において、「個人番号カード」として使用される IC カードに求められるセキュリティ要件を規定する。

PP[11]において、TOE は、IC チップと、TOE の外部インタフェースである接触・非接触インタフェースを含めた IC カードであって、その IC チップ上に、個人番号カードとしてのサービスを提供するアプリケーションプログラム（以下、「AP」という。）とデータを搭載するものである。

図 1-1 に TOE 構成を示す。

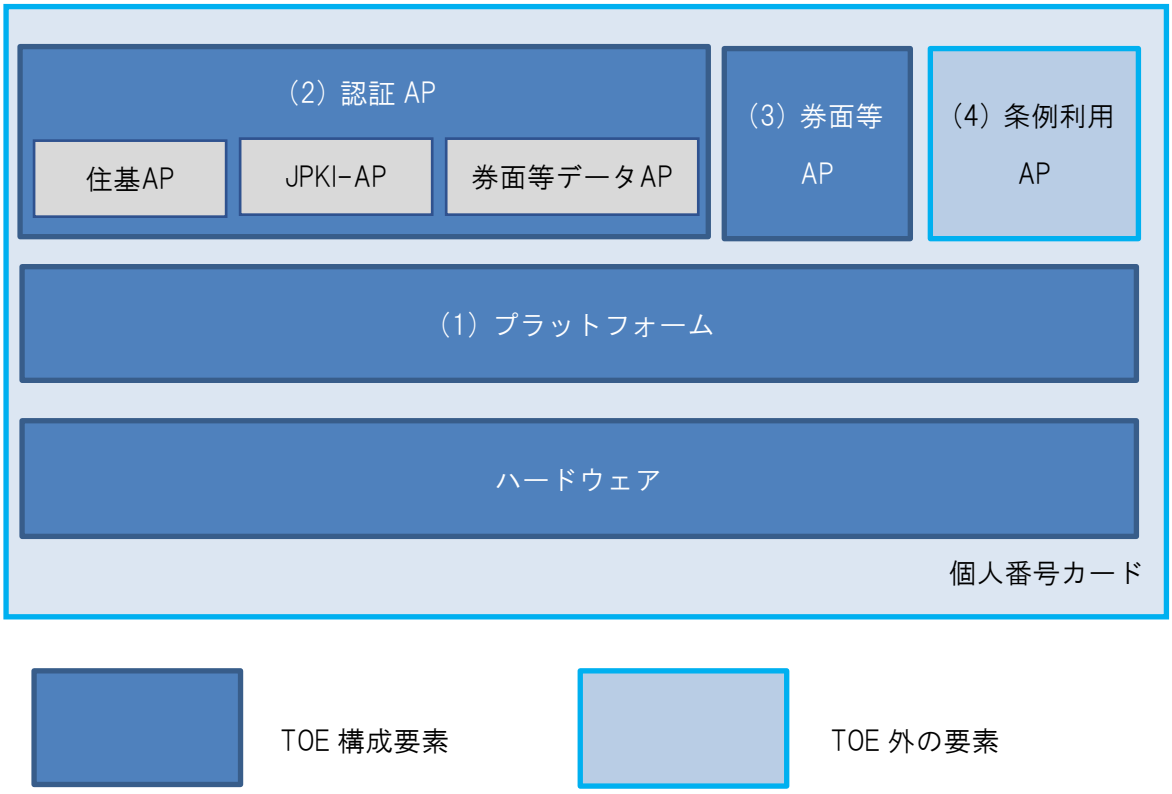

図 1-1 TOEの構成

図 1-1 において、TOE は、IC カードのハードウェア、及び、ソフトウェアである(1)プラットフォーム、(2)認証 AP、(3)券面等 AP で構成される。ソフトウェアである（4）条例利用 AP は TOE の範囲外である。

TOE のハードウェアは、ソフトウェアの動作環境を提供すると共に、ハードウェアへの攻撃に対抗する。以下、ソフトウェアである(1) プラットフォーム、(2) 認証 AP、(3) 券面等 AP、(4) 条例利用 AP について説明する。

(1) プラットフォーム

プラットフォームは、AP の動作環境を提供する。プラットフォームは、追加の機能として、地方自治体のそれぞれの条例に基づく AP（条例利用 AP）をカードに登録・削除する機能を有する。

(2) 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」という。）、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」という。）、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」という。）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。外部認証と内部認証の詳細は、後述の 1.1.2.1 (2)項を参照。

[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。

(3) 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。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。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。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、読出し時に利用者の認証機能（外部認証を含む）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、また利用者の認証機能（外部認証含む）、内部認証機能を提供する。

(4) 条例利用 AP

地方自治体の条例に基づき個人番号カードに搭載される AP。

以下、(2) 認証 AP、(3) 券面等 AP をまとめて、「基本 AP」という。

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 AP 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（カードのパーソナライゼーション）。また、必要に応じて個人番号カードに条例利用 AP が追加搭載される。

1.1.2.1 セキュリティ機能概要

PP[11]では、個人番号カードが提供するサービスに求められるセキュリティ機能と、IC カードとして標準的に求められるセキュリティ機能を TOE に要求する。その主要なものを以下に示す。

(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外部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。

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」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。

1.1.2.2 脅威とセキュリティ目標

PP[11]に適合する TOE は、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

個人番号カードは、地方自治体の管理者に許可されたサービスや、カード保持者に許可されたサービスなどを提供するため、必然的に複数の役割と複数のサービスをサポートする。その役割やサービスを利用する権限を持たない者が、接触インタフェース又は非接触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かもしれない。そこで、TOE は利用者を識別・認証した上で、その利用者の役割に対応した権限の範囲で TOE 内部への論理的アクセスを許可する。

また、TOE の接触インタフェース又は非接触インタフェースを用いた、外部端末との通信において、外部認証に対応した通信内容を傍受・記録し、その内容を再利用することで、正規の外部端末になりすます脅威が考えられる。そこで、この脅威に対抗するため、外部認証に使用する認証データ（この生成を TOE が担う）を再利用せず、毎回異なるデータを使用する外部認証機能を要求する。

IC カードに搭載される IC チップは、その物理形態の特性上、内部で処理している情報を、消費電力や放射電磁波を通じて漏えいする可能性がある。また、物理的

なプロービングによる IC チップ内部の情報の暴露、IC チップ上の回路の物理的な改ざん、環境ストレスの印加による誤動作を考慮する必要がある。そこで、こういった物理攻撃から TSF を保護する機能を要求する。

1.1.3 免責事項

なし。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって PP[11]に対する保証要件に基づいて IT セキュリティ評価が実施され、令和 7 年 9 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[12]、所見報告書([14][15])、及び関連する評価証拠資料を検証し、PP[11]の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6][7][8]）、CEM（[9]）、及び補助文書（[10]）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 PP識別

PP[11]は、以下のとおり識別される。

PP名称：	個人番号カード Version 2 プロテクションプロファイル
バージョン：	第1.00版
開発者：	地方公共団体情報システム機構

3 セキュリティ方針

本章では、PP に適合する TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

PP[11]では、個人番号カードが提供するサービスに求められるセキュリティ機能と、IC カードとして標準的に求められるセキュリティ機能を TOE に要求する。TOE に要求されるセキュリティ機能は、大きく次の 4 つである。

- 通信データ保護、
- 利用者認証とアクセス制御、
- 暗号演算、
- 物理的攻撃への対抗

3.1 セキュリティ機能方針

PP[11]では、3.1.1.1 に示す脅威に対抗し、3.1.2.1 に示す組織のセキュリティ方針を満たすセキュリティ機能を規定している。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

PP[11]は、表 3-1 に示す脅威を想定し、これに対抗する機能を TOE に要求する。

表 3-1 想定する脅威

識別子	脅威
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。

識別子	脅威
T.Phys_Attack	攻撃者は、TOEの構成要素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。

3.1.1.2 脅威に対するセキュリティ機能方針

PP[11]に適合する TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能で対抗する。

(1) 脅威「T.Illegal_Attack」への対抗

脅威「T.Illegal_Attack」は、個人番号カードの接触インタフェース、あるいは非接触インタフェース経由で TOE 内部のプログラム、及びデータに不正にアクセスすることを想定している。

これらの脅威に対して、TOE では個人番号カードと通信を行う外部端末の認証を行うことで正当性を確認し、正当な権限を持つことが確認された場合のみ、その権限の範囲でデータ及び暗号演算機能へのアクセスを許可する。外部端末の認証を行う際は、チャレンジレスポンス方式を使用する。また、その際の認証データは再利用せず、毎回異なるデータが使用される。これにより正当な外部端末のみが TOE の内部プログラム、及びデータにアクセスすることができる。

(2) 脅威「T.Phys_Attack」への対抗

PP[11]に適合する TOE は、IC という物理形態という特性上、物理的な改ざん（観察、分析、あるいは改変）にさらされる。また、TOE の振る舞いは、電圧、周波数、温度といった動作条件からの影響を受ける。

これらの脅威に対して、TOE は、SOG-IS の IC カード及び類似デバイスに関する必須技術文書[13]に記載された攻撃に耐えるべく、TSF に対する保護機能を提供する。

例えば、この攻撃は次を含む。

- TOE 内部を流れる信号を読み取ろうとする攻撃、
- TOE 内部を流れる信号を改変しようとする攻撃、
- TOE の自己保護機能を非活性化又はバイパスすべくセンサー類を無効化する攻撃、
- 故障注入攻撃(DFA を含む)、
- サイドチャネル攻撃(DPA、DEMA を含む)、
- IC チップのテスト機能の悪用、
- 乱数生成器の出力乱数を予測したり、出力乱数のエントロピーを減らしたりする攻撃。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

PP[11]に適合する TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

表 3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
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。

識別子	組織のセキュリティ方針
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3-3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。

表 3-3 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 (FIPS PUB 197, ISO/IEC 10116)	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 (ISO/IEC 9797-1, FIPS PUB 197)	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 (FIPS PUB 186-5)	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 (BSI-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 (ANSI X9.63, BSI-TR03111)	暗号鍵導出	192	セキュアメッセージングの鍵導出
SHA-384 (FIPS 180-4)	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

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、3.1.2.1 に示す組織のセキュリティ方針を満たす機能を具備する。

⑴ 組織のセキュリティ方針「P.Secure_messaging」への対応

本組織のセキュリティ方針は、TOE 内部のソフトウェアと外部端末との通信において、通信データに求められる機密性及び完全性の程度と外部端末の要求に応じて、通信データの暗号化・復号する機能、又は通信データに対応した MAC を生成・検証する機能を規定している。

TOE が、TOE 内部の個別のソフトウェアと外部端末との間の通信について、表 3-3 に従って暗号化・復号を行う機能、及び MAC 生成・検証を行う機能を提供することにより、通信データの機密性及び完全性の意図した程度の保護を実現できる。

⑵ 組織のセキュリティ方針「P.Delivery」への対応

本組織のセキュリティ方針は、個人番号カードの交付者である市区町村の管理下にある TOE に対して、正当な利用者のみが TOE 内部へ論理的にアクセスできることを規定している。

プラットフォームと 2 つの基本 AP のそれぞれにアクセスするために、TOE はそれぞれ独立した認証を要求し、輸送鍵を用いて認証が成功した場合のみ、認証に成功した TOE 内部の個別のソフトウェア（プラットフォーム、又は基本 AP の内の１つ）へアクセスできる。

⑶ 組織のセキュリティ方針「P.Cryptography」への対応

本組織のセキュリティ方針は、TOE が使用する暗号アルゴリズム及び鍵を規定している（表 3-3）。

PP[11]に適合する TOE は、本組織のセキュリティ方針の中で指定された暗号機能及び暗号鍵管理機能を提供する。

⑷ 組織のセキュリティ方針「P.RND」への対応

本組織のセキュリティ方針は、攻撃者による予測に耐える乱数を生成することを規定している。

PP[11]に適合する TOE は、乱数の用途に応じ必要な品質尺度を満たす、次の乱数生成器を提供する。

- 物理乱数生成器

- 決定論的乱数生成器

4 前提条件と評価範囲の明確化

本章では、想定する読者が PP[11]に適合する TOE の利用の判断に有用な情報として、PP[11]に適合する TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

PP[11]に適合する TOE を運用する際の前提条件を**表 4-1** に示す。これらの前提条件が満たされない場合、PP[11]に適合する TOE のセキュリティ機能が有効に動作することは保証されない。

表 4-1 前提条件

識別子	前提条件
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。

5 評価機関による評価実施及び結果

5.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

5.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、PP[11]の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

5.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、令和 6 年 9 月に始まり、令和 7 年 9 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

評価作業中に発見された問題点は、所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

5.4 評価結果

評価者は、評価報告書をもって PP[11]が CEM のワークユニットすべてを満たしていると判断した。

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

・APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、APE_REQ.2

5.5 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

6 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の観点で認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、PP[11]及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

6.1 認証結果

評価機関より提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、PP[11]の評価が CC パート 3 の APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、及び APE_REQ.2 に対する保証要件を満たすものと判断する。

6.2 注意事項

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。

外部端末との通信では、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が適用される。セキュアメッセージング属性を付与するかどうかは別途示される調達仕様に依存する。

7 附属書

特になし。

8 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された用語の定義及び略語を以下に示す。

基本AP	認証AP、券面等APを総称して、基本APと呼ぶ。
カード保持者	個人番号カードを交付された住民を指す。
外部認証	ICカード(TOE)が外部端末を認証することを指す。
管理者	地方公共団体情報システム機構又は地方自治体に属し、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。
共通鍵	対称鍵暗号アルゴリズムの中で使用される暗号鍵を指す。
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。
公開鍵	非対称暗号アルゴリズムの中で使用されるpublic keyを指す。
住民基本台帳ネットワーク	住民の方々の利便性の向上と国及び地方公共団体の行政の合理化に資するため、居住関係を公証する住民基本台帳をネットワーク化し、全国共通の本人確認ができるシステムを指す。
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。
セキュアメッセージング	暗号アルゴリズムを用いて通信データの機密性及び/または完全性を保護するための方法を指す。

地方公共団体情報システム機構	地方公共団体情報システム機構法に基づき平成26年4月1日に設立され、財団法人地方情報センター(LASDEC)の権利義務の一切を承継した組織である。地方公共団体情報システム機構の略称は、J-LISである。 「行政手続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」等の関係法令に基づいて、国から委託された個人番号付番システムなどの個人番号関連システムの構築・整備等を行うとともに、個人番号の生成や市区町村からの委託を受けて個人番号カードの発行の業務を行う。
内部データ	TOE内に格納されているデータを指す。利用者データ及びTSFのふるまいに影響を与えるデータ(TSFデータ)を含む。
内部認証	外部端末がICカード(TOE)を認証することを指す。
秘密鍵	非対称暗号アルゴリズムの中で使用されるprivate keyを指す。
利用者データ	利用者に関するデータで、TSFのふるまいに影響を与えないものを指す。
4情報	氏名・住所・生年月日・性別を指す。
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CBC	Cipher Block Chaining
CMAC	Cipher-based MAC
DEMA	Differential Electro-Magnetic Analysis
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
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。ICカードと外部端末が相互に認証するSCP11a、外部端末がICカードを認証するSCP11bの規格の定義が含まれている。
SHA	Secure Hash Algorithm
SOG-IS	Senior Officials Group Information Systems Security

SP 800	Special Publication 800 series

9 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 令和7年8月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 令和5年12月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 令和3年10月, 独立行政法人情報処理推進機構, CCM-03

[4] 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 パート1: 概説と一般モデル CC:2022 改訂第1版, 2022年11月, CCMB-2022-11-001 (令和5年9月翻訳第1.0版)

[5] 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 パート2: セキュリティ機能コンポーネント CC:2022 改訂第1版, 2022年11月, CCMB-2022-11-002 (令和5年9月翻訳第1.0版)

[6] 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 パート3: セキュリティ保証コンポーネント CC:2022 改訂第1版, 2022年11月, CCMB-2022-11-003 (令和5年9月翻訳第1.0版)

[7] 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 パート4: 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 CC:2022 改訂第1版, 2022年11月, CCMB-2022-11-004 (令和5年9月翻訳第1.0版)

[8] 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 パート5: 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 CC:2022 改訂第1版, 2022年11月, CCMB-2022-11-005 (令和5年9月翻訳第1.0版)

[9] 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, 2022年11月, CCMB-2022-11-006 (令和5年9月翻訳第1.0版)

[10] 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, 2024年7月22日, CCMB 2024-07-22 (令和6年12月翻訳第1.0版)

[11] 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

[12] PP評価報告書 LYX23-ETRPP-0001-05B, 第1.5版, 2025年9月4日, 株式会社ECSEC Laboratory 評価センター

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

[14] 所見報告書 LYX23-EOR-0001-00, 2025年6月10日, 株式会社ECSEC Laboratory 評価センター

[15] 所見報告書 LYX23-EOR-0001-01, 2025年7月4日, 株式会社ECSEC Laboratory 評価センター