認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

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）	平成26年1月22日 (IT認証4485)
認証番号	C0431
認証申請者	地方公共団体情報システム機構[1]
PPの名称	個人番号カードプロテクションプロファイル
PPのバージョン	第1.00版
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
評価機関の名称	株式会社 ECSEC Laboratory 評価センター

上記のPP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。

平成26年5月15日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　近藤　潤一

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 バージョン3.1 リリース4
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「個人番号カードプロテクションプロファイル」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。

---

[1] 平成26年1月22日時点での認証申請者の名称は、財団法人地方自治情報センター（LASDEC）であったが、LASDECは、平成26年4月1日に設立された地方公共団体情報システム機構（J-LIS）に事業承継された。

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「個人番号カードプロテクションプロファイル、バージョン　第 1.00 版」（以下「PP[12]」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。）が平成 26 年 4 月 24 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[12]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[12]を併読されたい。特に PP[12]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 において詳述されている。

本認証報告書は、PP[12]に適合した個人番号カードを開発・納入する開発者を読者と想定している。本認証報告書は、PP[12]が適合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。

本認証報告書で使用する用語については、8 章を参照されたい。

1.1 評価PP

PP[12]が要求するセキュリティ機能性、運用条件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[12]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[12]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[12]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[12]において、TOE は、IC チップと接触・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プログラムとデータを搭載するものである。

図 1-1 に TOE 構成を示す。

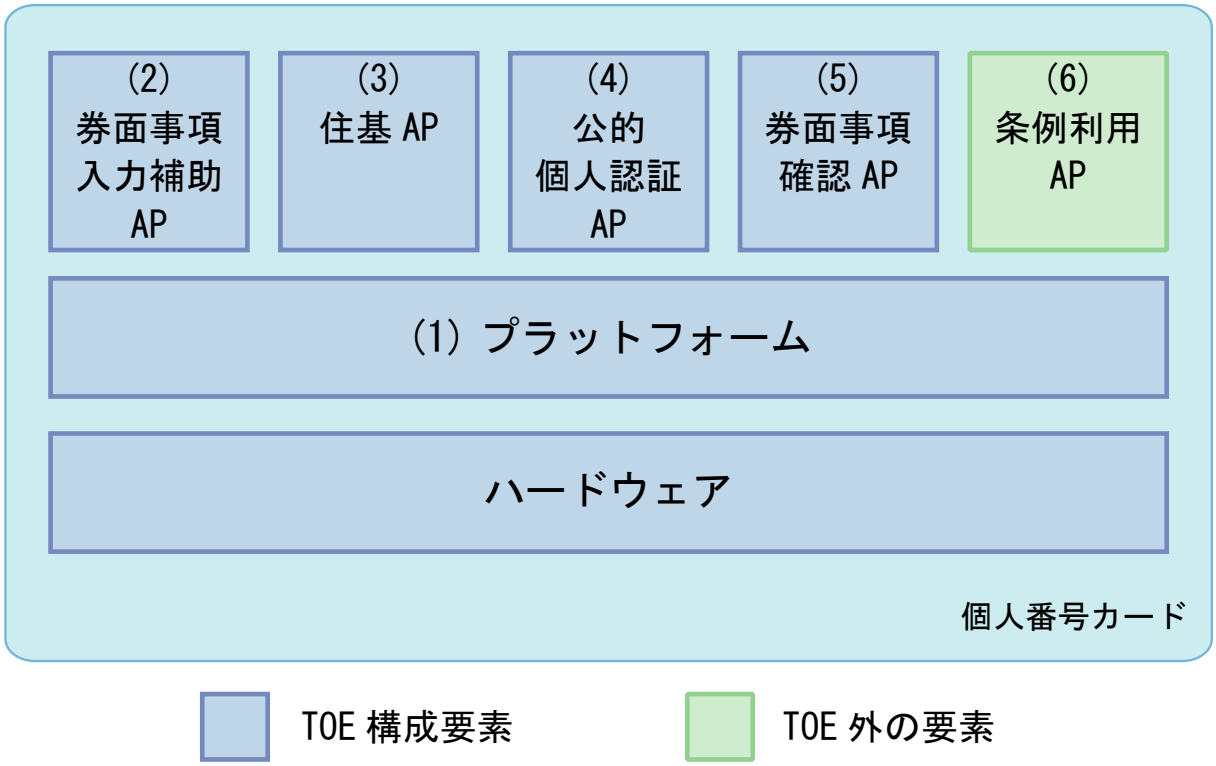

図 1-1 TOEの構成

図 1-1 の (1) プラットフォーム、(2) 券面事項入力補助 AP、(3) 住基 AP、(4) 公的個人認証 AP、(5) 券面事項確認 AP、(6) 条例利用 AP について、以下に説明する。

[プラットフォーム]

プラットフォームは、Application Program（以下「AP」という。）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。

[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出される。

[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。

[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。

(2) 券面事項入力補助 AP、(3) 住基 AP、(4) 公的個人認証 AP、(5) 券面事項確認 AP をまとめて、基本 AP と呼ぶ。

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、住民に交付される。個人番号カードの交付に際し、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、住民の固有情報が書き込まれる（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。

個人番号カードを交付された住民（カード保持者）は、個人番号カードに搭載された AP を用いて、サービスを利用する。

1.1.2.1 セキュリティ機能概要

PP[12]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、接触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。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のデータ暗号化・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(例えば個人番号) 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。

TOE を利用するシナリオとしては、カード保持者や地方自治体の管理者が TOE のサービスを利用しようとする場合、サービスの利用に先立って、外部端末が TOE にアクセスする。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。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したい場合に、外部端末側が IC カード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。

1.1.2.2 脅威とセキュリティ目標[2]

PP[12]に適合するTOEは、以下の通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

個人番号カードの券面の印刷改ざんが疑われる場合、券面事項確認APを使用して券面事項情報を外部端末に読み出し、外部端末側で比較検証する場合がある。PP[12]では、券面事項情報を読み出す際に、セキュアメッセージングを適用することを要求していない。したがって、個人番号カードから外部端末への券面事項情報の送信を改ざんすることによって、外部端末側が券面事項情報の改ざん検出することを結果として阻害する、という脅威には対抗していない。

また、券面事項入力補助AP、公的個人認証APと外部端末との通信において、セキュアメッセージングを適用するか否かは、外部端末がセキュアメッセージングを要求するかどうかに依存する。したがって、カード保持者が通信の機密性・完全

---

[2] CC Part 1 [4]で定義されている"security objective"の訳語として、日本語翻訳版[7]では「セキュリティ対策方針」を割り当てているが、本認証報告書の中では、"security objective"の訳語として、「セキュリティ目標」を用いることとする。

性を希望する場合でも、外部端末により、通信の機密性及び/または完全性が維持されないかもしれない。

個人番号カードの利用に関連する事項として、公的個人認証法の第十七条及び第三十六条に基づき、個人番号カードのサービスの利用を許可された民間事業者の存在がある。例えば、コンビニエンスストアで個人番号カードを使用して住民票の写しを請求するような使い方が想定されている。このような使い方に対応して、PP[12]では、公的個人認証 AP の利用者とその権限として、「証明書データを扱うシステム」が、利用者証明機能を利用することを規定している。これは、カード保持者の利用者証明に用いる電子署名を、カード保持者以外が生成可能であることを表している。個人番号カードを利用するシステムからは、生成された電子署名が、カード保持者本人による署名なのか、本人以外による署名なのかを判別できない可能性がある。しかしながら、生成された電子署名をどう取り扱うかは、個人番号カードを利用するシステム側の課題であり、PP[12]に適合する TOE の範囲外である。

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・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[12]に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 26 年 4 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[13]、所見報告書（[15][16][17][18][19]）、及び関連する評価証拠資料を検証し、PP[12]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、PP の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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[12]は、以下のとおり識別される。

PP名称：	個人番号カード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[12]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[12]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性は、大きく次の4つである。

- TOEと外部端末との間の通信データ保護、
- 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[12]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[12]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.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。

3.1.1.2 脅威に対するセキュリティ機能方針

PP[12]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」及び「T.Replay」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。また、「T.Replay」では個人番号カードと外部端末との通信における認証手順を再利用して、TOE に不正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、表 3-4 に示す暗号アルゴリズム（RSASSA-PKCS1-v1.5）を用いた、公開鍵暗号方式に基づく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。

⑵ 脅威「T.Phys_Attack」への対抗

PP[12]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[14]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

3.1.2.1 組織のセキュリティ方針

PP[12]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

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、表3-3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はない。
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3-4に要求される暗号アルゴリズム、暗号操作及び用途を、表3-5に暗号鍵長、暗号鍵管理方針を示す。
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。

表 3-3　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 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 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。

表 3-4 暗号機能方針

暗号アルゴリズム /標準	暗号操作	使用する暗号鍵 (表 3-5 の識別番号列を参照)	用途
AES-CBC mode /FIPS PUB 197・ NIST SP 800-38A	暗号化/復号	K1, K8	セキュアメッセージング、 秘密鍵復号(インポート時)
CMAC with AES /FIPS PUB 197・ NIST SP 800-38B	MAC 生成/検証	K2	セキュアメッセージング
RSASSA-PKCS1-V1.5 /PKCS#1 v2.2	公開鍵による署名検証	K3	外部認証
	秘密鍵による署名生成*1	K4, K5, K6	内部認証、 公的個人認証APにおける署名・利用者証明
RSA-OAEP /PKCS#1 v2.2	秘密鍵による復号	K7	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
SHA-256 /FIPS PUB 180-4	ハッシュ演算	-	RSA暗号演算の補助技術として使用

*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

（注）識別番号 K1～K8 は、PP[12]には記載されていないが、読者の理解を助ける目的で、整理・分類のために用いた。

表 3-5 暗号鍵長及び暗号鍵管理方法

識別番号	暗号鍵の名称	暗号鍵長 (ビット)	暗号鍵生成/インポート	暗号鍵破棄
K1	セッション鍵(暗号鍵)	128	インポート	PP[12]では特定しない
K2	セッション鍵(MAC鍵)	128		
K3	外部認証用公開鍵	2048		
K4	内部認証用鍵ペア	2048		
K5	署名用秘密鍵	2048		
K6	利用者証明用秘密鍵	2048		
K7	セッション鍵暗号化用鍵ペア	2048		
K8	秘密鍵復号用共通鍵	128		

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

PP[12]は、表 3-2 に示す組織のセキュリティ方針を満たす機能を TOE に要求する。

(1) 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/又は 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/又は完全性の意図した程度の保護を実現できる。

(2) 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 4 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。

(3) 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、及び鍵並びに鍵管理方針を規定している（表 3-4 及び 表 3-5）。

PP[12]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。

(4) 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[12]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、次のいずれかの乱数生成器を提供する。

- 物理乱数生成器、
- 物理乱数生成器と決定論的乱数生成器を組み合わせたハイブリッド乱数生成器

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[12]に適合する TOE の利用の判断に有用な情報として、PP[12]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[12]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[12]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	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を個人番号カードに搭載する。

5 評価機関による評価実施及び結果

5.1 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[12]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。

5.2 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、平成 26 年 1 月に始まり、平成 26 年 4 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。

各ワークユニットの評価作業中に発見された問題点は、すべて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。

5.3 評価結果

評価者は、PP[12]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

評価では以下について確認された。

評価結果概要
APE_INT.1　　PP 概説
PP[12]は、個人番号カードに求められる、次のセキュリティ機能を規定していることが、評価を通じて確認された。 ・通信データ保護、 ・利用者認証とアクセス制御、 ・暗号演算、 ・ハードウェア攻撃への対抗
APE_CCL.1　　適合主張
評価を通じて次の事実が確認された。 ・コモンクライテリア バージョン 3.1 リリース 4 への適合 ・セキュリティ機能要件：　コモンクライテリア　パート 2　拡張 ・セキュリティ保証要件：　コモンクライテリア　パート 3　適合 ・他の PP への適合主張をしないこと ・PP[12]への適合主張をする場合は、論証適合が求められていること
APE_SPD.1　　セキュリティ課題定義
評価を通じて次の事項が確認された。 ・脅威及び組織のセキュリティ方針が、CC/CEM に従った観点で記述されていること
APE_OBJ.2　　セキュリティ目標
評価を通じて次の事項が確認された。 ・セキュリティ課題定義で記述された脅威及び組織のセキュリティ方針を取り扱うセキュリティ目標が記述されていること、その根拠が適切であること
APE_ECD.1　　拡張コンポーネント定義
評価を通じて次の事項が確認された。 ・拡張コンポーネント定義の中で、CC Part 2 に記述されていない、用途を限定しない乱数生成に関するセキュリティ機能要件が規定されていること
APE_REQ.2　　セキュリティ要件

評価を通じて次の事項が確認された。 ・セキュリティ目標を満たすセキュリティ機能要件が記述されていること ・EAL4+ALC_DVS.2+AVA_VAN.5 というセキュリティ保証要件についての選択理由が記述されていること

5.4 評価者コメント/勧告

評価者から指摘は、次の 3 点である。

TOE の利用方法や想定される運用環境（市町村に導入される端末などの仕様含む）に関する仕様や必要なガイダンスは地方公共団体情報システム機構から提供されなければならない。

PP[12]では信頼できる開発者により条例利用 AP が開発されることを要求しているが、その AP が他の AP 等を侵害しないことは要求していない。このため、TOE は必要に応じてアプリケーション分離機能を実装する必要がある。アプリケーション分離機能が実装された場合は評価対象に含める必要がある。

PP[12]では保護対象データが明記されていない。TOE 開発者は ST では保護対象データを特定する必要がある。

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、以下の項目について確認した。

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。

これらの確認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[12]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、本認証報告書を作成した。

6.1 認証結果

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[12]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

個人番号カードに条例利用 AP が搭載されるかどうかは、地方自治体に依存するが、個人番号カード自体は条例利用 AP を搭載可能であるということに変わりはない。条例利用 AP を搭載・使用・削除するといった操作によって、個人番号カードの保護資産を毀損しようとする攻撃への対抗については、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[14]に従い TOE の評価を通じて確認される必要がある。

PP[12]で規定する暗号アルゴリズムについては、PP[12]に適合する TOE の評価を行う時点での有効性を保証するものではない。したがって、PP[12]に適合する TOE の評価を行う際には、PP[12]が規定する暗号アルゴリズムの有効性の確認、及び危殆化についての評価が必要になる。

7　　附属書

特になし。

8 用語

8.1 CCに関する略語

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）

8.2 本認証報告書で使用された用語及び略語

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	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を総称して、基本APと呼ぶ。
4情報	氏名・住所・生年月日・性別を指す。
外部認証	ICカードが外部端末を認証することを指す。
内部認証	外部端末がICカードを認証することを指す。
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。
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。
カード保持者	個人番号カードを交付された住民を指す。
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。
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。
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。
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。
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。
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。
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。
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
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
RSA	Rivest - Shamir - Adleman algorithm
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, 平成24年3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, 平成25年4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, 平成25年4月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[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1: 概説と一般モデル, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11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2: セキュリティ機能コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002, (平成24年11月, 翻訳第1.0版)

[9] 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, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] 個人番号カードプロテクションプロファイル, バージョン 第1.00版, 2014年4月24日, 地方公共団体情報システム機構

[13] PP評価報告書 LYX-ETRPP-0002-00, 第2.0版, 2014年4月24日, 株式会社 ECSEC Laboratory 評価センター

[14] Joint Interpretation Library - Application of Attack Potential to Smartcards, Version 2.9, January 2013

[15] 所見報告書 LYX-EOR-7001-00, 2014年1月24日, 株式会社ECSEC Laboratory評価センター

[16] 所見報告書 LYX -EOR-7002-00, 2014年2月5日, 株式会社ECSEC Laboratory評価センター

[17] 所見報告書 LYX-EOR-7003-00, 2014年2月12日, 株式会社ECSEC Laboratory評価センター

[18] 所見報告書 LYX-EOR-7004-00, 2014年2月24日, 株式会社ECSEC Laboratory評価センター

[19] 所見報告書 LYX-EOR-7005-00, 2014年3月3日, 株式会社ECSEC Laboratory評価センター