認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

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27年11月30日 (IT認証5575)
認証番号	C0500
認証申請者	外務省領事局旅券課
PPの名称	旅券冊子用ICのためのプロテクションプロファイル － SAC対応（BAC+PACE）及び能動認証対応 －
PPのバージョン	第1.00版
PP適合	なし
適合する保証パッケージ	EAL4 及び追加の保証コンポーネントALC_DVS.2
開発者	外務省領事局旅券課
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28年3月22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

「旅券冊子用ICのためのプロテクションプロファイル － SAC対応（BAC+PACE）及び能動認証対応 －」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、外務省領事局旅券課が開発した「旅券冊子用 IC のためのプロテクションプロファイル － SAC 対応(BAC+PACE)及び能動認証対応 －、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 28 年 3 月 9 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外務省領事局旅券課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[12]において詳述されている。

本認証報告書は、PP[12]に適合した旅券冊子用 IC を開発・納入する開発者及び旅券冊子用 IC を調達する旅券発行当局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 である。

また、PP[12]への適合を主張する PP、及び ST は正確適合を主張しなければならない。

1.1.2 PP概要

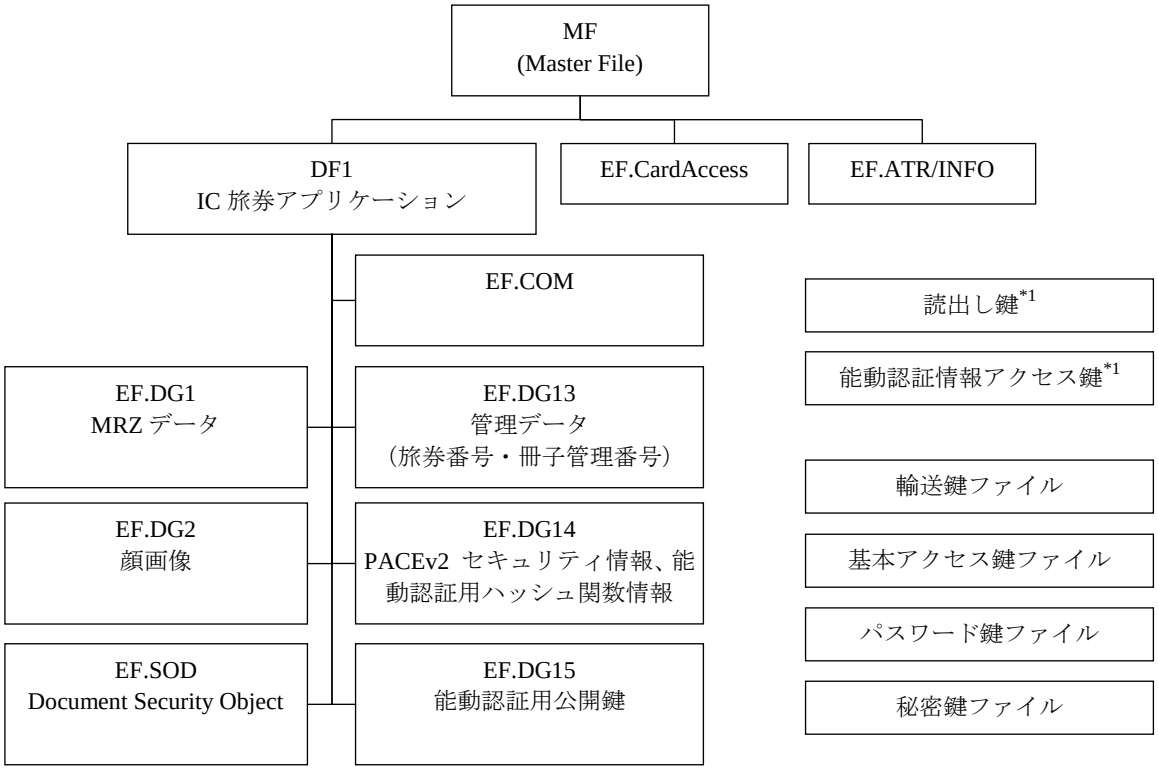
PP[12]は、国際民間航空機関(ICAO)による IC 旅券規格[15]に準拠する、旅券に綴じ込まれる旅券冊子用 IC に関わるセキュリティ要件を規定する。

PP[12]において、TOE は必要なソフトウェアを含む旅券冊子用 IC である。この旅券冊子用 IC は、非接触通信インタフェースを持つ IC チップハードウェア、それに搭載される基本ソフトウェア(OS)、及び IC 旅券用アプリケーションプログラム

からなる。その外部に非接触通信のためのアンテナが接続され、アンテナと共にプラスチックシートに埋め込まれて旅券冊子の一部を構成する。

旅券保持者の出入国において、出入国審査官は、旅券検査用端末装置（以下、端末装置と称する）を使用して旅券を検査する。通常の文字で旅券冊子に印刷された情報は、それと同じ内容が符号化されて旅券冊子の MRZ（機械読み取り領域）に印刷され、端末装置の光学文字読み取り装置で読み取られる。なお、これらの情報はデジタルデータ[1]化され、TOE である IC チップ内に格納されている。このデジタルデータは、TOE の非接触通信インタフェース経由で端末装置によって読み出される。このデジタルデータには、顔画像も含まれる。

図 1-1 は、IC 旅券規格[15] Part 10, Figure 2 を、PP 概要を説明する目的で再構成したものである。



*1 PP[12]上、ファイルであるとは明示されていない。

図 1-1 旅券冊子用ICのファイル構成

[1] デジタルデータの偽造を防ぐため、個々のデジタルデータに旅券発行者によるデジタル署名が付与される。デジタル署名の検証は、受動認証方式としてICAOによって標準化されている。受動認証に対応するため、デジタル署名付与から端末装置での検証に至るまで、すべての加盟国間で相互運用性を持つPKIが運用される。受動認証は、署名から検査に至るまで（バックグラウンドとなるPKIを含め、）TOEのセキュリティ機能が関与することなく実施されるので、TOEに対するセキュリティ要件には含まれない。

PP[12]では、IC 旅券アプリケーション配下のファイルの読出しに先立って、端末装置と TOE とが相互認証し、TOE と端末装置間の通信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る。IC 旅券規格[15]で規定された相互認証及びセキュアメッセージングの方式には、基本アクセス制御（BAC: Basic Access Control）と、鍵共有利用アクセス制御（PACE: Password Authenticated Connection Establishment v2）の 2 つがあり、後者は公開鍵暗号を取り入れ、セキュアメッセージングの中で使用されるセッション鍵の暗号強度を強化した方式である。

図 1-2 は、端末装置が旅券冊子用 IC にアクセスする手順の中で、基本アクセス制御、及び鍵共有利用アクセス制御がどのように関わってくるかを示したもので、基本アクセス制御又は鍵共有利用アクセス制御のどちらか一方が適用される。

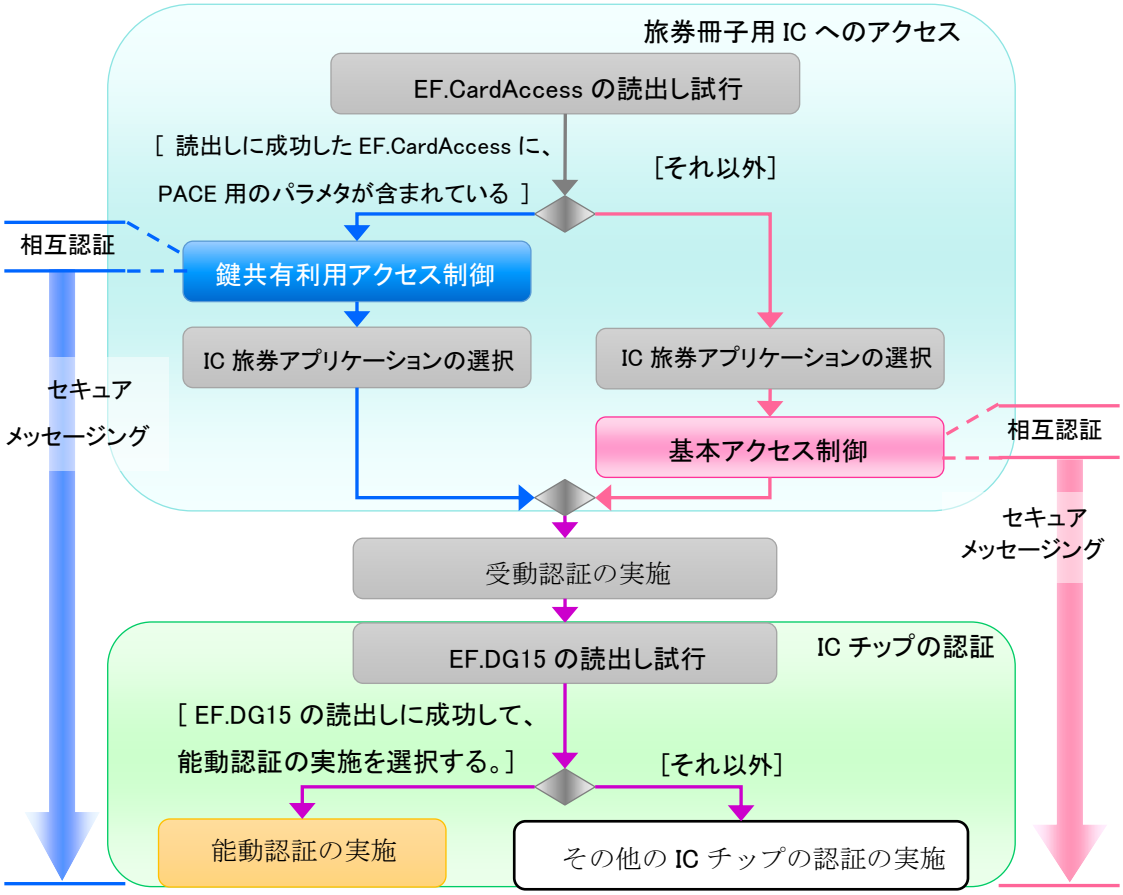


図 1-2　端末装置が旅券冊子用ICにアクセスする手順

将来は鍵共有利用アクセス制御が標準的な相互認証及びセキュアメッセージング方式となるが、互換性確保の観点から、2017 年末までは、基本アクセス制御機能を実装せずに鍵共有利用アクセス制御機能のみを IC チップに実装することは IC 旅券規格[15] Part 11 で禁止されている。

PP[12]では、基本アクセス制御機能及び基本アクセス制御機能の無効化機能を持つ IC チップを TOE と規定し、一方 PP[13]ではこの 2 つの機能が要求されない IC チップを TOE と規定している。

これらの 2 つの PP の使われ方としては、TOE を PP[12]に従って評価認証すると同時に、同じ TOE を PP[13]に従って別途評価認証することで、基本アクセス制御機能については AVA_VAN.3 で脆弱性評価が実施され、それ以外のセキュリティ機能については、AVA_VAN.5 で脆弱性評価が実施されることを意図している。このようなやり方で TOE が評価認証されることで、旅券発行当局に基本アクセス制御機能を実装した旅券冊子用 IC が納入されたとしても、旅券発行当局で基本アクセス制御機能の無効化機能を使用することによって、相互認証及びセキュアメッセージングに鍵共有利用アクセス制御のみを受け付ける TOE であって AVA_VAN.5 で実質的に評価されたものを、発行することが可能になる。

PP[12]では、旅券冊子用 IC の複製を防止するため、公開鍵暗号を利用したチャレンジレスポンスにより、IC チップの真正性を証明しようとする能動認証対応機能を要求している。能動認証対応機能は、過去に認証された PP[21]でも要求されていたが、能動認証に使用される暗号が RSA から ECDSA に変更されている。

TOE のライフサイクルは 4 つのフェーズに分けられ、それらを図示したものが図 1-3 である。

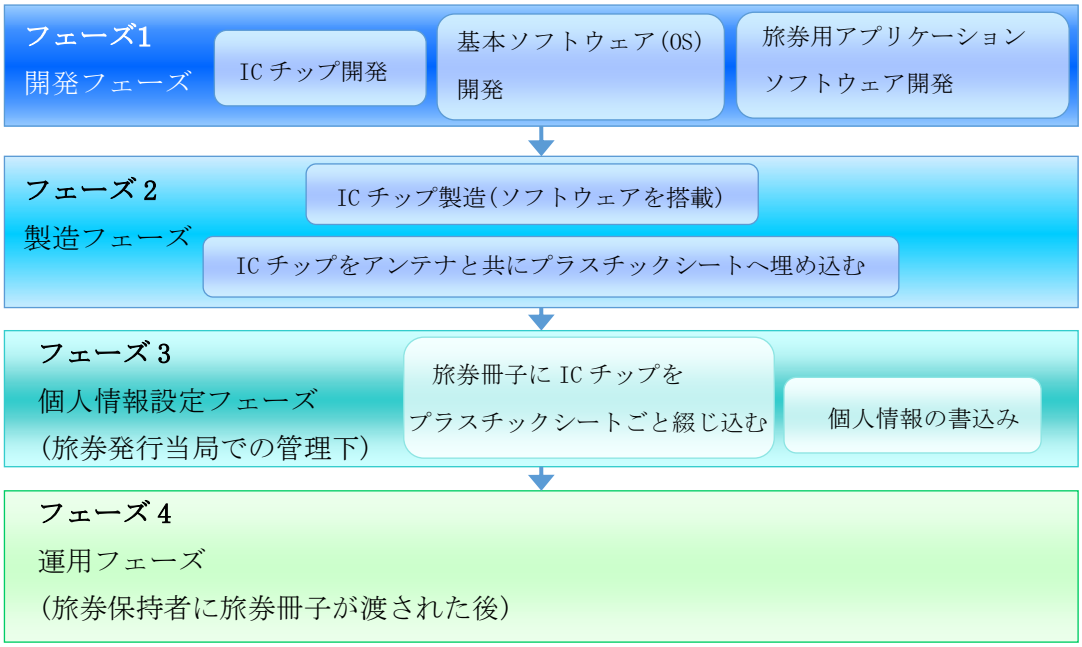


図 1-3　PP[12]に適合するTOEのライフサイクル

フェーズ 1、及びフェーズ 2 では運用環境の脅威は想定されていないが、開発データや IC チップの構成要素の機密性・完全性を保護するために適切な開発セキュリティが保たれていなければならない。フェーズ 3 では、権限を持つものだけに TOE

の処理を許可するようなセキュリティ機能性が要求される。フェーズ 4 では強化基本的な攻撃能力を持つ攻撃者からの攻撃に対抗できるセキュリティ機能性が要求される。

1.1.3 セキュリティ機能概要

PP[12]では、TOE 内に格納されたデータの不正な読出しや書込みから保護する機能、IC 旅券規格[15] Part 11 が規定する基本アクセス制御機能及び鍵共有利用アクセス制御機能、能動認証対応機能、基本アクセス制御機能の無効化機能、輸送時の保護機能、並びに物理的攻撃に備える耐タンパー機能を TOE に要求する。その概要を以下に示す。

(1) 基本アクセス制御機能

TOE は、端末装置との間で相互認証を行い、相互認証に成功した端末装置との間にセキュアメッセージングを適用して、TOE 内のアクセス制御対象のファイルの読出しを許可する。

基本アクセス制御の相互認証及びセキュアメッセージングに使用される暗号は、共通鍵暗号（2-key Triple DES、Single DES）及びハッシュ関数（SHA-1）である。

(2) 鍵共有利用アクセス制御機能

TOE は、端末装置との間で相互認証を行い、相互認証に成功した端末装置との間にセキュアメッセージングを適用して、TOE 内のアクセス制御対象のファイルの読出しを許可する。

鍵共有利用アクセス制御の相互認証及びセキュアメッセージングに使用される暗号は、公開鍵確立手法（ECDH[2]）、共通鍵暗号（AES[3]）及びハッシュ関数（SHA-1[4]、SHA-256[5]）である。

(3) 能動認証対応機能

TOE は、旅券冊子用 IC の複製を防止するため、公開鍵暗号を利用したチャレンジレスポンスにより、IC チップの真正性を証明しようとする能動認証対応機能を提供する。

---

[2] IC旅券規格[15]ではDHを使う選択肢も記載されているが、PP[12]ではECDHを選択している。
[3] IC旅券規格[15]ではTriple DESを使う選択肢も記載されているが、PP[12]ではAESを選択している。PP[12]では128ビットのAES鍵を使う場合と256ビットのAES鍵を使う場合の両方に対応できることを要求している。
[4] SHA-1は、128ビットのAES鍵を使う場合に使用される。
[5] SHA-256は、256ビットのAES鍵を使う場合に使用される。

能動認証に使用される暗号は、デジタル署名（ECDSA[6]）及びその中で使用されるハッシュ関数（SHA-256、SHA-384）である。

(4) 基本アクセス制御機能の無効化機能

ある時期以降に発行される旅券冊子用 IC は基本アクセス制御手順を受け付けないものとする旅券発行当局の方針に対応して、TOE は、基本アクセス制御機能を無効化する機能を提供する。

(5) 書込み禁止機能

旅券保持者への発行後、TOE 内のファイルに対する一切の書込みを禁止する機能である。

(6) 輸送時の保護機能

TOE は、輸送途中の不正利用から IC カードを保護する目的で、輸送鍵を用いた認証に成功して初めて TOE 内の所定のファイルにアクセスできる機能を提供する。

(7) 物理攻撃に備える耐タンパー機能

TOE のセキュリティ機能は、自身のハードウェア部分及び TSF を構成するソフト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。

1.1.3.1 脅威とセキュリティ目標[7]

PP[12]に適合する TOE は、以下のとおり、セキュリティ機能によりそれぞれの脅威に対抗する。

身分証明書として必要な情報がすべて紙の冊子に印刷されていた旧来の旅券については、偽造等による不正使用が懸念されていた。この課題を解決すべく旅券冊子用 IC では、IC チップ内に格納されるデジタルデータに、正規の旅券発行者によるデジタル署名を施し、旅券発行側と受け入れ側の双方が相互運用性の保証された

---

6 IC旅券規格[15]ではRSAを使う選択肢も記載されているが、PP[12]ではECDSAを選択している。その上で、256ビット又は384ビットの秘密鍵を用いて署名生成を行う。256ビットの秘密鍵の場合には、SHA-256が、384ビットの場合にはSHA-384が使用される。

7 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。

PKI システムを用いることによって、IC チップから読み出されたデータの真正性を確認できるようにする受動認証が採用されている。

しかし、受動認証だけでは、正規の署名付き個人情報を複製して別の IC チップに格納する偽造に対抗できない。そこで PP[12]では、IC 旅券規格[15]で規定された、能動認証（Active Authentication）と呼ばれる公開鍵暗号を利用したチャレンジレスポンス方式を採用し、その能動認証に使う秘密鍵（以下「能動認証用秘密鍵」という。）の IC チップからの読出しを制限することによって、偽造に対抗しようとしている。

IC 旅券規格[15]では、ISO/IEC 7816-4 で規定されたファイルシステムを採用している。能動認証用秘密鍵もこのファイルシステムの中に格納されていることを想定すると、ISO/IEC 7816-4 で規定されたコマンドを用いて能動認証用秘密鍵が読み出せる可能性がある。PP[12]では、そのような脅威に対して読出しアクセスを拒否することを TOE に要求する。

旅券冊子用 IC から読み出し可能なデータには顔画像や受動認証のための情報が含まれている。出入国審査の窓口の端末装置と旅券冊子用 IC との間で通信されるこのようなデータを暴露・改ざんしようとする試みが想定される。この脅威に、TOE と端末装置間の相互認証及び TOE と端末装置間のセキュアメッセージングを適用することで対抗する。

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 TOE に要求する。

1.1.4 認証に際しての免責事項

PP[12]では、基本アクセス制御及び鍵共有利用アクセス制御を、相互認証及びセキュアメッセージング機能であると謳っている。IC 旅券規格[15]で規定された基本アクセス制御及び鍵共有利用アクセス制御は、MRZ データを知らない攻撃者が、無線通信に割り込み、旅券冊子用 IC から端末装置に読み出される情報を盗聴・改ざんしようとする攻撃にのみ対抗しようとする機能である。

IC 旅券規格[15]によれば、基本アクセス制御及び鍵共有利用アクセス制御を突破するために必要な情報が MRZ データである[8]ため、MRZ データを知ることができ

---

[8] 国立研究開発法人 情報通信研究機構(NICT)が運営しているCPVPが実施した、基本アクセス制御の暗号プロトコル評価(http://crypto-protocol.nict.go.jp/AKE_zoo/11770-2-6-epass/11770-2-6-epass_Main.html)からも同様の記述が読み取れる。

れば、正規の端末装置になりすまして、最終的に受動認証のための情報を読み出すことが可能である。したがって、MRZ データを知っている攻撃者が、基本アクセス制御及び/又は鍵共有利用アクセス制御を突破して、旅券冊子用 IC のデータを読み出す、という脅威には対抗できない。しかしながら、攻撃者が MRZ データを知ることができても、PP[12]に適合する TOE であれば能動認証用秘密鍵を論理的に読み出すことはできない。

また、PP[12]では旅券冊子用 IC の複製防止のための能動認証対応機能を TOE に要求しているが、TOE の機能だけで、旅券の偽造による悪用を防止できるわけではない。能動認証の仕組みがシステムとして適切に機能するためには、能動認証用秘密鍵の機密性及び能動認証用公開鍵の完全性・真正性が重要である。旅券発行当局の許可された利用者は、後述する前提条件 A.Administrative_Env に対応して、次の事項をセキュアに行う必要がある。

— 能動認証用鍵ペアを生成する

— 能動認証用公開鍵にデジタル署名を付ける

— 能動認証用鍵ペアを旅券冊子用 IC に格納する

加えて、旅券発行当局の許可された利用者は、後述する前提条件 A.PKI に対応して、旅券冊子用 IC に格納するデータのデジタル署名生成に使う鍵ペアをセキュアに管理すると共に、PKI 環境を適切に維持する必要がある。

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 28 年 3 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（[18][19][20]）、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： 旅券冊子用ICのためのプロテクションプロファイル
－ SAC対応（BAC+PACE）及び能動認証対応 －
バージョン： 第1.00版
開発者： 外務省領事局旅券課

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、次の 7 つの機能を TOE に要求する。

― 基本アクセス制御機能（相互認証とセキュアメッセージング）

― 鍵共有利用アクセス制御機能（相互認証とセキュアメッセージング）

― 能動認証対応機能（旅券 IC チップの複製防止）

― 基本アクセス制御機能の無効化機能（旅券発行後の基本アクセス制御機能の動作禁止）

― 書き込み禁止機能（旅券発行後のデータ書込み禁止）

― 輸送時の保護機能（発行前 TOE を輸送時の攻撃から保護）

― 耐タンパー性（物理的攻撃による機密情報漏えい防止）

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

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

識別子	脅威
T.Copy[9]	IC 旅券の偽造を意図する攻撃者がTOE からデジタル署名付きの個人情報を読み出し、その複製データをTOE と同様の機能性を持つIC チップに書き込んでIC 旅券を偽造しようとするかもしれない。この攻撃によって、TOE を含む旅券冊子全体に対する信用が毀損される。 [注釈] 不正なICチップに正規のTOEから取り出された情報が複製されると、デジタル署名ごとTOE内情報が複製されるので、デジタル署名の検証による偽造防止が無効になる。デジタル署名によって元情報の改ざんは防止できるため、顔画像の比較検証で旅券偽造を検出できるかもしれない。しかし、顔だちの判別だけでは、確実に旅券偽造を検出することは困難である。
T.Logical_Attack[10]	TOE を組み込んだ旅券冊子発行後の運用環境において、旅券冊子のMRZデータを読み取れる状態にある攻撃者が、TOE の非接触通信インタフェース経由でTOE 内に格納された機密情報（能動認証用秘密鍵）を読み出そうとするかもしれない。 [注釈] 攻撃者が旅券冊子に物理的にアクセスできれば、攻撃者は、目視で旅券冊子に印刷された個人情報を読み取ったり、あるいはMRZの印刷データを光学的に読み取ることができる。これらの読み取りをTOEのセキュリティ機能で防止することはできないので、これらの情報は、この脅威に関わる保護資産に含まれない。つまり本脅威の趣旨は、攻撃者がMRZから読み取ったデータを利用してTOEの非接触インタフェース経由でTOEにアクセスし、内部の機密情報（能動認証用秘密鍵）を読み出そうとする攻撃である。
T.Communication_Attack[11]	TOEを組み込んだ旅券冊子発行後の運用環境において、MRZデータを知らない攻撃者が端末装置とTOE間の通信に割込み、秘匿が必要な通信データを暴露・改ざんするかもしれない。 [注釈] 端末装置と旅券冊子間の通信に割り込むような攻撃においては、攻撃者が旅券保持者や出入国審査官に気づかれずに攻撃対象の旅券冊子へ物理的にアクセスすることは不可能と考えられる。攻撃者は旅券冊子に物理的にアクセスできる場合のみ、MRZデータを知ることができるため、本脅威の想定する攻撃者はMRZデータを知らないものと考えられる。

9 脅威「T.Copy」は、受動認証のみをサポートする旅券冊子用ICの限界を指摘するものである。

10 脅威「T.Logical_Attack」は、TOEがISO/IEC 7816-4で規定されたファイルシステムを採用していることに対応して、ISO/IEC 7816-4で規定されたコマンドを用いて能動認証用秘密鍵の出力が可能かもしれないという可能性を表したものである。

11 脅威「T.Communication_Attack」は、顔画像などの読出し可能なデータの、攻撃者による暴露・改ざんの懸念を表したものである。対象となるデータが異なるという点で、脅威「T.Logical_Attack」とは独立である。

識別子	脅威
T.Physical_Attack[12]	TOEを組み込んだ旅券冊子発行後の運用環境において、攻撃者が物理的手段を用いてTOE内部の機密情報（能動認証用秘密鍵）を暴露しようとしたり、閉塞された鍵の閉塞状態を解除したり、無効化されたアクセス制御機能を再活性化したりするかもしれない。この物理的手段には、TOEの機能を損なわずに攻撃する非破壊攻撃と、TOEの一部を破壊して内部に機械的にアクセスする破壊攻撃の両方が含まれる。 [注釈] 攻撃者がTOEに物理的にアクセスし、内部の機密情報（能動認証用秘密鍵）を読み出したり、TOE内の情報を書き換えたりそうとする攻撃が考えられる。このような物理的攻撃が行われると、TOEのプログラムによって動作するセキュリティ機能は本来の機能を発揮できず、SFR侵害の恐れが生じる。非破壊攻撃の例は、TOEの動作に伴う漏えい電磁波観測、動作中のTOEに環境ストレス（温度やクロックの変化、高エネルギーの電界・磁界印加など）を与えてセキュリティ機能の誤動作を誘起するものである。破壊攻撃の例は、内部回路のプロービングや操作(manipulation）によって情報を収集・分析し、機密情報を暴露するものである。内部に残されたテスト用端子や電源端子も攻撃に利用され得る。破壊攻撃を受けたTOEは、旅券用ICとして再使用できないかもしれない。しかしその場合でも、読み出された秘密鍵がTOEの偽造に悪用される恐れがある。

3.1.1.2 脅威に対するセキュリティ機能

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.Copy」への対抗

受動認証は、デジタル署名が付与された個人情報を旅券冊子用 IC に格納し、その個人情報を端末装置が読み出して、PKI システムを用いて検証する方式である。脅威「T.Copy」は、デジタル署名を含めて個人情報を複製し、別の IC チップに書き込んで偽造した IC 旅券を用いて、受動認証による検査を突破することを想定している。

この脅威に対して、IC 旅券規格[15]は、次の手順による能動認証を規定している。

a). 端末装置は、ナンス(8 バイト)を旅券冊子用 IC に送信する。

---

[12] 脅威「T.Physical_Attack」は、TOEに物理的手段を用いるという点で、利用可能な手段が論理的な手段に限定されている脅威「T.Logical_Attack」と対比される。しかしながら、脅威「T.Physical_Attack」には、攻撃者が、差分故障利用攻撃(Differential Fault Analysis：DFA)のような、論理的な手段(非接触通信インタフェースを介したデータ出力)と物理的な手段とを組み合わせて攻撃することも含まれる。

b). 旅券冊子用 IC は、受信したナンスに旅券冊子用 IC 内で格納している能動認証用秘密鍵を用いて署名生成し、その署名文を端末装置に送信する。

c). 端末装置は、旅券冊子用 IC から別途読み取った能動認証用公開鍵を用いて、署名文を検証し、検証に成功すれば正規の旅券冊子用 IC であると判断する。なお、能動認証用公開鍵にはデジタル署名が付けられており、端末装置は PKI システムを用いることによって、能動認証用公開鍵の完全性・真正性を検証することができる。

能動認証用のデジタル署名アルゴリズムとして、PP[12]では、IC 旅券規格[15]から参照される[16]で規定された ECDSA(但し、256 ビット又は 384 ビットの秘密鍵を用いる)を規定している。

関連する能動認証用秘密鍵の機密性、及び能動認証用公開鍵・能動認証用秘密鍵の完全性の観点について、PP[12]では、3.1.2.1 に示す組織のセキュリティ方針 P.Data_Lock を通じて、次の 2 つが禁止された状態で旅券保持者に発行される仕組みを要求している。

— 能動認証用秘密鍵の読出し及び書込み

— 能動認証用公開鍵の書込み

(2) 脅威「T.Logical_Attack」への対抗

脅威「T.Logical_Attack」は、TOE を組み込んだ旅券冊子が旅券保持者に発行された運用環境において、非接触通信インタフェースを経由して能動認証用秘密鍵が論理的に読み出される可能性を想定している。

この脅威に対して、TOE は、旅券冊子発行後の運用環境において、能動認証用秘密鍵の論理的な読出しを禁止することで対抗する。

(3) 脅威「T.Communication_Attack」への対抗

脅威「T. Communication_Attack」は、顔画像などの読出し可能なデータの、攻撃者による暴露・改ざんを想定している。

この脅威に対して、TOE と端末装置間の相互認証及び TOE と端末装置間のセキュアメッセージングを適用することで対抗する。

適用される相互認証及びセキュアメッセージングの方式については、IC 旅券規格[15]で規定された次の 2 つがある。

a). 基本アクセス制御

b). 鍵共有利用アクセス制御

PP[12]は、TOEに基本アクセス制御及び鍵共有利用アクセス制御の両方をサポートすることを要求している。端末装置と TOE との間の相互認証及びセキュアメッセージングに、実際にどちらが使用されるかは、図 1-2 に示すように TOE がサポートする鍵共有利用アクセス制御に端末装置側が対応しているかどうかに依存する。

a). IC 旅券規格[15]で規定された基本アクセス制御については、表 3-2 に示す暗号アルゴリズムを ISO/IEC 11770-2 Key Establishment Mechanism 6 に組み合わせている。

表 3-2　基本アクセス制御に用いられる暗号アルゴリズム

暗号アルゴリズム	暗号操作	暗号鍵長 (ビット)	用途
SHA-1	基本アクセス制御用セッション鍵の導出	—*1	セキュア メッセージング
CBC モード Triple DES	認証用データの暗号化・復号	112	相互認証
	認証子生成・検証 （メッセージの最終ブロック）*2	112	
	メッセージの暗号化・復号	112	セキュア メッセージング
	認証子生成・検証 （メッセージの最終ブロック）*2	112	
CBC モード Single DES	認証子生成・検証 （メッセージの最終ブロックを除く）*2	56	相互認証
	認証子生成・検証 （メッセージの最終ブロックを除く）*2	56	セキュア メッセージング

*1　鍵導出関数の入力は、相互認証で確立した128ビットにカウンタ32ビットを連結した160ビットである。

*2　ISO/IEC 9797-1 MAC Algorithm 3を説明した内容である。

b). 鍵共有利用アクセス制御に用いられる暗号アルゴリズムを表 3-3 に示す。

表 3-3　鍵共有利用アクセス制御に用いられる暗号アルゴリズム

暗号アルゴリズム	暗号操作	暗号鍵長 (ビット)	用途
SHA-1*1	鍵共有利用アクセス制御用セッション鍵の導出	—*3	相互認証及び セキュアメッセージング
SHA-256*2	鍵共有利用アクセス制御用セッション鍵の導出	—*3	相互認証及び セキュアメッセージング
ECDH	鍵共有	256又は384	相互認証及び セキュアメッセージング

暗号アルゴリズム	暗号操作	暗号鍵長 (ビット)	用途
CMAC モード AES	認証トークンの生成および検証	128又は256	相互認証
	認証子の生成・検証	128又は256	セキュアメッセージング
CBC モード AES	ナンス*4 の暗号化	128又は256	相互認証
	メッセージの暗号化・復号	128又は256	セキュアメッセージング

*1 128ビットのAESのセッション鍵を導出するために使用される。

*2 256ビットのAESのセッション鍵を導出するために使用される。

*3 ハッシュ関数とみると暗号鍵は存在しないが、鍵導出関数と見た場合の入力は、ECDHで確立したShared Secretにカウンタ32ビットを連結したものである。

*4 能動認証に登場するナンスとは異なるもので、TOE自身が乱数生成器を使って生成する。

(4) **脅威「T.Physical_Attack」への対抗**

PP[12]に適合する TOE は、IC という物理形態の特性上、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、PP[12]に適合する TOE は、IC カード及び類似デバイスに関する必須技術文書[17]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、

— 故障注入攻撃(DFA を含む）、

— サイドチャネル攻撃(DEMA を含む)、

— IC チップのテスト機能の悪用、

— 無効化されたアクセス制御機能の再活性化、

— 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 3-4 に示す。

表 3-4　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.BAC	TOE を組み込んだ旅券冊子発行後の運用環境において、TOE は、IC旅券規格[15] Part11 で規定される基本アクセス制御手順に従って端末装置がTOE から所定の情報を読み出すことを許可しなければならない。この手順は、TOE と端末装置の相互認証及びTOE と端末装置間のセキュアメッセージングを含む。読出し対象となるTOE のファイルは、同規定におけるEF.DG1、EF.DG2、EF.DG13、EF.DG14、EF.DG15、EF.COM、EF.SOD である。同規定における上記以外のファイルについて、PP[12] に記載のないものは、その扱いを規定しない。 なお、本組織のセキュリティ方針は、P.Disable_BAC による基本アクセス制御機能の無効化後は適用されない。
P.PACE	TOE を組み込んだ旅券冊子発行後の運用環境において、TOE は、IC旅券規格[15] Part11 で規定される鍵共有利用アクセス制御手順に従って端末装置がTOE から所定の情報を読み出すことを許可しなければならない。この手順は、TOE と端末装置の相互認証及びTOE と端末装置間のセキュアメッセージングを含む。読出し対象となるTOE のファイルは、同規定におけるEF.DG1、EF.DG2、EF.DG13、EF.DG14、EF.DG15、EF.COM、EF.SOD である。同規定における上記以外のファイルについて、PP[12] に記載のないものは、その扱いを規定しない。
P.Authority[13]	旅券発行当局の管理下にあるTOE は、表 3-5　に示すとおり、許可された利用者（読出し鍵、輸送鍵、あるいは能動認証情報アクセス鍵の照合に成功した者）だけにTOE 内部情報へのアクセスを許可する。
P.Data_Lock[14]	TOE が輸送鍵、読出し鍵あるいは能動認証情報アクセス鍵による認証失敗を検出したとき、それぞれの鍵に関わる認証を恒久的に無効とし、それによって、その認証成功に基づくファイル読出し・書込みを禁止する。認証に用いる鍵とそれに対応するTOE 内ファイルとの関係は、表 3-5 に示される。
P.Prohibit[15]	旅券保持者への発行後、TOE 内ファイルに対する一切の書込み、及び読出し鍵による認証成功に基づく読出しを禁止する。その手段として、輸送鍵、読出し鍵及び能動認証情報アクセス鍵の認証失敗による認証無効化（P.Data_Lock に示す）を利用する。

[13] 輸送時の保護機能に対応する。
[14] 書き込み禁止機能に対応する。
[15] 書き込み禁止機能に対応する。

識別子	組織のセキュリティ方針
P.Disable_BAC[16]	基本アクセス制御の危殆化に対する旅券発行当局の方針に従って、ある時期以降に発行されるTOE は基本アクセス制御手順を受け付けないものとする。その手段として、TOE は基本アクセス制御機能を無効化するための手続きを提供し、旅券発行当局の許可された利用者は当該手続きを実行することによって基本アクセス制御機能を無効化する。 [注釈] 本組織のセキュリティ方針は、旅券発行当局が基本アクセス制御機能を有するICチップの発行停止を要求する場合にのみ適用される。

表 3-5　旅券発行当局におけるTOE内部情報アクセス制御

認証状況	アクセス制御対象となるファイル	許可される操作	参考：操作対象データ
読出し鍵*1による照合成功	EF.DG13*2	読出し	IC チップシリアル番号(製造者記入済み)
輸送鍵*1による照合成功	輸送鍵ファイル	書込み	輸送鍵データ（旧データの更新）
	基本アクセス鍵ファイル		基本アクセス鍵（暗号化鍵） 基本アクセス鍵（認証子生成鍵）
	パスワード鍵ファイル		パスワード鍵
	EF.DG1	読出し又は書込み	MRZ データ
	EF.DG2		顔画像
	EF.DG13*2		管理データ（旅券番号・冊子管理番号）
	EF.DG14		PACEv2 セキュリティ情報 能動認証用ハッシュ関数情報
	EF.COM*3		共通情報
	EF.SOD		IC 旅券規格[15] Part10 に定められる受動認証関連セキュリティデータ
	EF.CardAccess	書込み	PACEv2 セキュリティ情報
	EF.DG15	読出し	能動認証用公開鍵
能動認証情報アクセス鍵*1による照合成功	EF.DG15	書込み	能動認証用公開鍵
	秘密鍵ファイル		能動認証用秘密鍵

*1　読出し鍵、輸送鍵、能動認証情報アクセス鍵は、製造者によって設定される。輸送鍵は、利用者が変更（更新）できる。本表に含まれるアクセス制御対象ファイルや認証状況を変化させる読出し鍵、能動認証情報アクセス鍵を格納したファイルについては、本表及び注に記載のない利

16 基本アクセス制御無効化機能に対応する。

用者アクセスは禁止される。(TOEを組み込んだ旅券冊子が旅券保持者へ発行された後の、端末装置からのTOE内部の情報へのアクセス制御<基本アクセス制御>と<鍵共有利用アクセス制御>は別途規定する)

*2 EF.DG13 にはIC チップシリアル番号が製造者によって記入済みであり、旅券発行当局によって管理データが追記される。

*3 EF.COM ファイルは、旅券発行当局の指示により生成されない場合がある。

表 3-4 に示す組織のセキュリティ方針とそれが適用されるフェーズの関係を表 3-6 に示す。

表 3-6 組織のセキュリティ方針と適用されるフェーズ

組織のセキュリティ方針	フェーズ			
	フェーズ 1	フェーズ 2	フェーズ 3	フェーズ 4
P.BAC				X*1
P.PACE				X
P.Authority			X	
P.Data_Lock			X	
P.Prohibit			X	X
P.Disable_BAC			X	

*1 フェーズ3で基本アクセス制御機能が無効化された場合には、フェーズ4でP.BACは適用されない。

注 'X' は、組織のセキュリティ方針が適用されることを表す。

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 3-4 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.BAC」への対応（基本アクセス制御機能）

本組織のセキュリティ方針は、TOE を組み込んだ旅券冊子発行後の運用環境において、IC 旅券規格[15]で規定される基本アクセス制御手順に従って端末装置が TOE から所定の情報を読み出すことを規定している。

TOE が、IC 旅券規格[15] Part 11 で規定された基本アクセス制御手順に従った機能を提供することにより、TOE からの所定の情報の読出しを基本アクセス制御手順で意図した程度でセキュアにすることができる。

(2) 組織のセキュリティ方針「P.PACE」への対応（鍵共有利用アクセス制御機能）

本組織のセキュリティ方針は、TOE を組み込んだ旅券冊子発行後の運用環境において、IC 旅券規格[15]で規定される鍵共有利用アクセス制御手順に従って端末装置が TOE から所定の情報を読み出すことを規定している。

TOE が、IC 旅券規格[15] Part 11 で規定された鍵共有利用アクセス制御手順に従った機能を提供することにより、TOE からの所定の情報の読出しを鍵共有利用アクセス制御手順で意図した程度でセキュアにすることができる。

(3) 組織のセキュリティ方針「P.Authority」への対応（輸送時の保護機能）

本組織のセキュリティ方針は、旅券発行当局の管理下にある TOE に対して、TOE 内のファイルを、表 3-5 に従ってアクセス制御することを規定している。

TOE 内のファイルにアクセスするために、輸送鍵、読出し鍵、又は能動認証情報アクセス鍵を用いて利用者を認証することを TOE が要求し、認証が成功した場合のみ、それぞれの鍵の認証に基づく TOE 内のファイルへのアクセスを許可する。

(4) 組織のセキュリティ方針「P.Data_Lock」への対応（書き込み禁止機能）

本組織のセキュリティ方針は、TOE が輸送鍵、読出し鍵あるいは能動認証情報アクセス鍵による認証失敗を検出したとき、それぞれの鍵に関わる認証を恒久的に無効とし、それによって、表 3-5 に示される認証成功を必要とするファイルの読出し・書込みが禁止されることを規定している。

読出し鍵、輸送鍵あるいは能動認証情報アクセス鍵による認証失敗を TOE が検出したとき、TOE はそれぞれの鍵を用いる認証メカニズムを無効化する機能を提供する。これによって、読出し鍵、輸送鍵又は能動認証情報アクセス鍵を用いてファイルにアクセスすることが禁止される。

(5) 組織のセキュリティ方針「P.Prohibit」への対応（書き込み禁止機能）

本組織のセキュリティ方針は、旅券保持者への発行後、TOE 内ファイルに対する一切の書込み、及び読出し鍵の認証成功に基づく読出しを禁止することを規定している。

旅券保持者への発行前に、読出し鍵、輸送鍵、能動認証情報アクセス鍵による認証失敗を起こし、TOE が提供する前述(4)に示す機能を利用して、TOE 内のファイルに対する書込み、及び読出し鍵の認証に基づいた読出しを禁止する。

(6) 組織のセキュリティ方針「P.Disable_BAC」への対応（基本アクセス制御機能の無効化機能）

本組織のセキュリティ方針は、ある時期以降に発行される TOE は基本アクセス制御手順を受け付けないものとする旅券発行当局の方針を実現するため、次の 2 つによって TOE の基本アクセス制御機能を無効化することを規定している。

a). TOE が基本アクセス制御機能を無効化するための手続きを提供すること

b). 旅券発行当局の許可された利用者が、基本アクセス制御機能を無効化するための手続きを実行すること

a)については、TOE が、基本アクセス制御機能を無効化するための機能を提供することにより対応する。

b)については、旅券発行当局の許可された利用者が、旅券発行当局の指示に従って、TOE の基本アクセス制御機能を無効化する手続きを実行することにより対応する。

4 前提条件と評価範囲の明確化

本章では、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.Administrative_Env	TOE 製造者から旅券発行当局へ納入され当局の管理下にあるTOE は、旅券保持者へ発行されるまでの間、セキュアに管理され発行処理を受ける。
A.PKI	旅券発行者によってデジタル署名されTOE に格納された情報（能動認証用公開鍵を含む)について、その真正性を受入国の旅券審査当局が検証できるようにするため、旅券発行当局により旅券の発行国、受入国双方のPKI 環境の相互運用性が保たれる。

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）と相互承認している認定機関（独立行政法人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[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。

5.3 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、平成 27 年 11 月に始まり、平成 28 年 3 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。

5.4 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。

表 5-1 評価結果概要

評価結果概要
APE_INT.1　　PP 概説
PP[12]は、旅券冊子用 IC 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。 ・基本アクセス制御機能 ・鍵共有利用アクセス制御機能 ・能動認証対応機能 ・基本アクセス制御機能の無効化機能 ・書き込み禁止機能 ・輸送時の保護機能 ・耐タンパー性
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、正確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 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

5.5　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[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、本認証報告書を発行した。

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

PP[12]では、乱数生成に関する規格及び乱数の品質が規定されていない。乱数生成に関する規格及び乱数の品質の規定にあたっては、乱数の用途、乱数生成器に求められるセキュリティ特性などを考慮すべきである。TOE 開発者は ST を通じて、これらを規定しなければならない。

申請者の意図としては、PP[12]に適合しようとする TOE について、別途 PP[13]に従って評価認証を TOE 開発者が取得することを想定している。このようなやり方によって、基本アクセス制御以外のセキュリティ機能について、AVA_VAN.5 で脆弱性評価が実施される。無効化された基本アクセス制御機能を再活性化させるような攻撃への対処は、PP[13]に適合する評価を通じて、AVA_VAN.5 で脆弱性評価が実施される。

基本アクセス制御機能の無効化機能は、旅券発行当局で使用することを目的とした機能であり、TOE を組み込んだ旅券冊子が旅券保持者に発行された後の運用環境では、実行することができない。したがって、基本アクセス制御機能が利用可能な状態で旅券保持者に発行された TOE については、旅券保持者が希望しても TOE の基本アクセス制御機能を無効化できないことに留意されたい。

PP[12]は、IC 旅券の国際レベルでの相互運用性に配慮して作成されているが、IC 旅券規格[15]で規定された全てのファイル及び機能を網羅するものではない。日本国以外の調達に PP[12]を利用しようとする場合、ファイルや機能の追加が必要になることがある。

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）
SFR	Security Functional Requirement（セキュリティ機能要件）
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及び略語を以下に示す。

鍵共有利用アクセス制御	IC旅券規格[15]で規定された相互認証及びセキュアメッセージングの方式の一つで、PACEv2を指す。
基本アクセス制御	IC旅券規格[15]で規定された相互認証及びセキュアメッセージングの方式の一つで、BACを指す。
基本アクセス鍵ファイル	MRZデータから導出され、基本アクセス制御の相互認証手続きにおいて暗号化及び認証子生成に使われる鍵が格納されるファイル。TOEでは、鍵をMRZデータから都度計算せず、予め導出された鍵をフェーズ3でTOEに格納する。
受動認証	TOE に格納する個人情報データに旅券発行者のデジタル署名を施し、旅券発行側と受け入れ側の双方が相互運用性の保証されたPKI システムを用いることによって、TOE から読み出されたデータの真正性を確認できるようにする方式。 ICAOにおいて、手順が標準化されている。
セキュアメッセージング	コマンド及びその応答に対してその一部又は全体を暗号によって保護するための方法 ([JIS X 6320-8:2006, 定義3.5]を参照)
能動認証	TOE のパーツである IC チップ内に公開鍵暗号方式に基づく公開鍵・秘密鍵ペアを格納し、秘密鍵を秘匿する。TOE を認証しようとする外部装置に公開鍵を渡し、TOE 内に秘匿された秘密鍵を用いたチャレンジレスポンス方式による暗号演算によって

	TOE 認証を実施する。 ICAOにおいて、手順が標準化されている。
能動認証情報アクセス鍵	能動認証用鍵ペアを書き込むための認証データ。
パスワード鍵ファイル	MRZ データから導出され、鍵共有利用アクセス制御手続きにおいてナンスの暗号化に使われる鍵が格納されるファイル。
発行	法的にその効力を有する状態におくこと。旅券そのものを作成，旅券として使用できる状態にすること。
輸送鍵	輸送途中の不正利用からICカードを保護するための認証データ。
読出し鍵	ICチップシリアル番号を読み出すための認証データ。
旅券	各国の政府あるいはそれに相当する公的機関が発行する国外渡航者のための身分証明書のこと。旅券は1冊の文書(旅券冊子)形式をとるのが一般的である。
旅券事務所	TOEを含む旅券冊子に旅券保持者の個人情報を設定し、旅券発行を行う。各地に設置され、旅券保持者に旅券冊子を交付する窓口となる。
旅券製造業者	旅券冊子を作成し、TOEに基本的データ(旅券番号等の管理データ、能動認証用公開鍵・秘密鍵ペア等)を設定する。
旅券発行当局	外務省とその指示下にある旅券製造業者及び各地の旅券事務所が該当する。旅券製造業者は、TOEを埋め込んだプラスチックシートを旅券冊子に綴じ込み、個人情報（生年月日や顔画像データ、それらのデータに関わるセキュリティ上のデータなど）以外の必要データを設定する。旅券事務所では、個人情報に関わる旅券データを設定する。
AES	Advanced Encryption Standard
ATR	Answer To Reset。リセット応答
BAC	Basic Access Control
CBC	Cipher Block Chaining
CMAC	Cipher-based MAC
DEMA	Differential Electro-Magnetic Analysis
DES	Data Encryption Standard
DF	専用ファイル。ファイル制御情報と任意選択として割付け利用可能なメモリとを含んでいる構造。 ([JIS X 6320-4:2009, 定義3.15]を参照)
DFA	Differential Fault Analysis
DG	Data Group
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm

EF	基礎ファイル。同一ファイル識別子と同一セキュリティ属性とを共有するデータオブジェクト、レコード、又はデータ単位の集合 ([JIS X 6320-4:2009, 定義3.19]を参照)
EF.ATR/INFO	Answer-to-Reset file, or Information file ([ISO/IEC 7816-4:2013, 4]を参照)
EF.CardAccess	MF直下に配置されるEFで、PACEv2セキュリティ情報を格納する。
EF.COM	旅券冊子用ICにどのようなフォーマットでデータを格納するかを規定する論理データ構造(Logical Data Structure：LDS)のバージョン情報、及び旅券用アプリケーションプログラムが格納されるDF配下に格納されるData Groupの一覧を提供する。
EF.DG1	MRZデータを格納するEF
EF.DG2	顔画像を格納するEF
EF.DG13	管理データ（旅券番号・冊子管理番号）を格納するEF
EF.DG14	PACEv2 セキュリティ情報、能動認証用ハッシュ関数情報を格納するEF
EF.DG15	能動認証用公開鍵を格納するEF
EF.SOD	他のData Groupのハッシュ値と受動認証用のデジタル署名を格納している。
ICAO	International Civil Aviation Organization (国際民間航空機関)
MAC	Message Authentication Code
MF	主ファイル。DFの階層構造を用いているカードでファイル構成の根幹となる唯一のDF。 ([JIS X 6320-4:2009, 定義3.26]を参照)
MRZ	Machine Readable Zone (機械読み取り領域) IC旅券の身分事項ページに印刷されたデジタル顔画像、身分事項ページ下部の88文字の機械読み取り領域のこと。姓名、国籍、性別、生年月日、旅券番号、有効期間満了日等が記載される。
MRZデータ	IC旅券券面に印字され、端末装置によって読み取られる情報。
PACE	Password Authenticated Connection Establishment
PACEv2	Password Authenticated Connection Establishment v2
PACEv2セキュリティ情報	PACEv2で使用する暗号アルゴリズムやドメインパラメタ等の情報。
PKI	Public Key Infrastructure
SAC	Supplemental Access Control [22] 1.1.3 Supplemental Access Controlでは次のように説明されている。 “This Technical Report specifies PACE v2 as an access control mechanism that is supplemental to Basic Access Control. PACE MAY be implemented in addition to Basic

	Access Control, i.e. ・States MUST NOT implement PACE without implementing Basic Access Control if global interoperability is required. ・Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip.”
SHA	Secure Hash Algorithm
SOD	Document Security Object

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27年6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27年10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27年10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] 旅券冊子用ICのためのプロテクションプロファイル － SAC対応（BAC+PACE）及び能動認証対応 －, 第 1.00 版, 2016年3月8日, 外務省領事局旅券課

[13] 旅券冊子用ICのためのプロテクションプロファイル － SAC対応（PACE）及び能動認証対応 －, 第 1.00 版, 2016年3月8日, 外務省領事局旅券課

[14] PP評価報告書 QXE-ETRPP-0002-00, 第2.0版, 2016年3月9日, 株式会社 ECSEC Laboratory 評価センター

[15] ICAO Doc9303 Machine Readable Travel Documents Seventh Edition, 2015

[16] Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012,

Bundesamt für Sicherheit in der Informationstechnik

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

[18] 所見報告書 QXE-EOR-7001-00, 2015年12月7日, 株式会社ECSEC Laboratory評価センター

[19] 所見報告書 QXE-EOR-7002-00, 2015年12月21日, 株式会社ECSEC Laboratory評価センター

[20] 所見報告書 QXE-EOR-7003-00, 2015年12月25日, 株式会社ECSEC Laboratory評価センター

[21] 旅券冊子用ICのためのプロテクションプロファイル －能動認証対応－ 第1.00版 2010年2月15日 外務省領事局旅券課

[22] International Civil Aviation Organization, ICAO MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control for Machine Readable Travel Documents, Version 1.1, 15 April 2014