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

JBMIA

はじめに

本PPは、国際民間航空機関 (ICAO) によるIC旅券規格「ICAO Doc 9303-1 第6版」に準拠する旅券冊子用ICに関わるセキュリティ要件をとりまとめたものである。

本PPが対象とするICチップは、能動認証 (AA: Active Authentication) に対応するIC旅券に向けたものである。能動認証によってICチップ自体の真正性検証が可能になり、不正なICチップによる旅券偽造を防止できる。

能動認証は、ICチップごとに固有の公開鍵・秘密鍵ペアによって実施される。公開鍵と秘密鍵はICチップ内に格納される。公開鍵が外部から読み出せる一方、秘密鍵はICチップ内に秘匿され、内部処理にだけ使用される。万一秘密鍵が外部に読み出されてしまうと、IC旅券偽造に悪用される恐れが生じる。能動認証対応のICチップは、高度の攻撃力 (特殊な装置や解析技術) に対抗して秘密鍵を秘匿できねばならない。

本PPは、CC第3.1版に基づいて作成された。本PPに準拠する旅券冊子用IC開発者は、本PPの記載要件をすべて満たすSTを準備しなければならない。

旅券冊子用ICは、本PPの要件を満たすセキュリティ機能のほか、旅券冊子用ICに求められる技術仕様全般を満たす必要がある。セキュリティ機能に関わらない技術仕様は本PPの要件外であり、別途、調達者から提示される。

本PPの要件の一部に、ICAOが発行する規格・資料の参照が含まれる。これらの規格・資料は、暗号アルゴリズムや認証手順などに関わるもので、CC規格に含まれていない。本PPを満たすTOE開発においては、これらの規格・資料が必要である。

本PPは、日本国外務省領事局旅券課の委託によって、JBMIAが作成した。本PPの著作権は、外務省領事局旅券課に属する。

【本PPに含まれる注釈について】

本PPには、PP準拠のST作成に向けた [注釈] が各所に記載されている。[注釈] は、PPを正しく理解するための補足情報であり、規定や要件の一部ではない。しかし、いくつかの注釈はST読者にとっても有効な情報になるので、ST作成者の判断によってそれらの注釈を転載してもよい。その際、STの文脈に従って記述を修正してもよい。

目次

1 PP概説

1.1 PP参照

タイトル: 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 –
版数: 第1.00版
発行: 2010年2月15日
作成者: JBMIA
発行者: 外務省領事局旅券課
登録: JISEC C0247

1.2 TOE概要

1.2.1 TOE種別

TOEは、旅券冊子用IC (必要なソフトウェアを含む) 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 (以下、「ICチップ」とは「旅券冊子用IC」を示すものとする) 。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。

1.2.2 TOEの用途と主要セキュリティ機能

旅券とは、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であり、1冊の文書 (旅券冊子) 形式をとるのが一般的である。国際連合における国際民間航空機関 (ICAO) が旅券冊子に関わるガイドラインを作成している。旧来の旅券では、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。旅券は、不正な目的のために偽造されることがあり、その防止策として、デジタル署名付き個人情報を格納したICチップが旅券冊子に組み込まれるようになった。正規の旅券発行者だけが有効なデジタル署名を付与できるので、高い偽造防止効果が得られる。しかし、デジタル署名だけでは、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。このような偽造攻撃には、ICチップに能動認証機能を付加し、それによってICチップが正規のものであることを確認することで対抗が可能になる。

TOEは、プラスチックシートに埋め込まれ、旅券冊子に綴じ込まれる。旅券保持者の出入国において、出入国検査官は、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。さらに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から読み出される。このデジタルデータには、顔画像も含まれる。

TOEが端末装置と非接触通信を行うためのアンテナは、プラスチックシート内でTOEに接続される。TOEの動作電源は、端末装置から送られる無線信号電力を利用し、TOE内部で生成される。

TOEの主要なセキュリティ機能は、TOE内に格納されたデータを不正な読出しや書込みから保護するためのものである。端末装置との非接触通信に適用されるセキュリティ機能の動作は、ICAO Doc 9303 Part1[2]が定める基本アクセス制御、及び能動認証の規格に準拠する。

TOE内の保護情報に対する攻撃には、TOEの非接触通信インタフェースを経由するもののほか、TOEに物理的攻撃を加えて内部の機密情報 (能動認証用秘密鍵) を暴露しようとするものも含まれる。能動認証用秘密鍵に対する攻撃は、高度の攻撃力を持つ攻撃者によるものが想定される。

TOEが備える主要セキュリティ機能は、以下のようなものである。

- 基本アクセス制御 (相互認証とセキュアメッセージング)
- 能動認証対応機能 (端末装置にTOEを認証させる)
- 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)

1.2.3 TOEのライフサイクル

TOEへのセキュリティ要件を明確にするため、TOEのライフサイクルを説明する。一般的

---

[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。

[2] 本PPでは、以下の二つの文書を合わせて、ICAO Doc 9303 Part1と称する:

- ICAO Doc9303 Machine Readable Travel Documents Part1 Machine Readable Passports Sixth Edition Volume1,2
- SUPPLEMENT to Doc9303-Part1-Sixth Edition Release7

なICチップのライフサイクルは7つのフェーズで記述されることが多いが、ここでは、旅券用ICとして、以下に示す4つのフェーズでライフサイクルを記述する。

- フェーズ1 (開発): ICチップハードウェア、基本ソフトウェア (OS) 、及びアプリケーションソフトウェア開発
- フェーズ2 (製造): ICチップ製造 (ソフトウェアを搭載) 、アンテナと共にプラスチックシートへ埋め込み
- フェーズ3 (個人情報設定): 旅券冊子作成、個人情報書込み
- フェーズ4 (運用): 旅券保持者による運用環境での使用

フェーズ1

フェーズ1は、開発フェーズである。このフェーズでは、運用環境の脅威は考慮されないが、開発データの機密性・完全性を保護するため、適切な開発セキュリティが保たれねばならない。開発フェーズのTOEに関わるセキュリティは、保証要件における開発セキュリティとして評価される。TOEのセキュリティ機能は、開発フェーズではまだ有効に動作しない。

フェーズ1におけるICチップのハードウェア、OSあるいは旅券用アプリケーションソフトウェア開発は、それぞれが異なる開発者によってなされる場合がある。TOEのそれぞれの構成要素開発が複数のサイトにまたがる場合、すべての構成要素に対してセキュアな開発環境が求められる。

フェーズ2

フェーズ2は、製造フェーズである。このフェーズでは、ICチップのハードウェアが製造され、OS、旅券用アプリケーションソフトウェアが埋め込まれる。ソフトウェアはROM形式で実装されることが多いが、一部が不揮発性メモリ上のデータとして実現されることもある。TOE内部にIC旅券に必要なファイルオブジェクトが生成され、ICチップ識別用シリアル番号が書き込まれる。ICチップ内部回路の機能テストは、ICチップ封止前に実施される。その後は、外部インタフェースとして非接触通信インタフェースだけが利用可能となる。製造されたICチップは、非接触通信用アンテナと共にプラスチックシートに埋め込まれる。このフェーズでは、運用環境の脅威は考慮されないが、ICチップの構成要素の機密性・完全性を保護するため、適切な開発セキュリティが保たれねばならない。

フェーズ2のTOEは、輸送鍵、読出し鍵、能動認証情報アクセス鍵が設定され、旅券発行当局へ渡される。

フェーズ３

フェーズ3のTOEは、旅券発行当局[3]の管理下に置かれる。旅券発行当局管理下では、TOEへの明示的な攻撃は想定されないが、組織の方針として、権限を持つ者だけにTOEの処理を許可するようなセキュリティ機能性をTOEに要求する。

TOEはIC旅券冊子に綴じ込まれ、IC旅券として必要な情報が書き込まれる。この情報とは、旅券保持者の個人情報 (氏名や出生情報など) のほか、セキュリティ機能が使用する暗号鍵などがある。すべての情報が設定された後、IC旅券は旅券保持者に発行される。

フェーズ4

フェーズ4は、最終利用者である旅券保持者に旅券冊子が渡されたあとのフェーズである。旅券冊子は旅券保持者によって携行され、出入国手続きをはじめとする多様な局面で、旅券保持者の身元証明手段として使用される。

フェーズ4においては、TOEの内部情報が書き換えられたり削除されたりすることはない。出入国手続きに必要な情報は、正規の端末装置から読み出される以外、TOEのセキュリティ機能によって不正な読出しを防止する。能動認証に使用される秘密鍵は、TOEの内部処理だけに使用され、TOE外に読み出されることはない。これらTOE内の情報資産は、TOEのセキュリティ機能によって外部の不正アクセスから保護される。

[3] 日本国では、国立印刷局及び各地の旅券事務所が該当する。国立印刷局では、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。

2 適合主張

2.1 CC適合主張

本PPが適合するCCを特定する。本PPは、以下のCC V3.1 (JISEC公開の日本語版) に適合する。

- パート2: セキュリティ機能コンポーネント 改訂第3版 最終版 [翻訳第1.0版] 2009年7月 CCMB-2009-07-002
- パート3: セキュリティ保証コンポーネント 改訂第3版 最終版 [翻訳第1.0版] 2009年7月 CCMB-2009-07-003

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において、TOEに対して適用する保証要件パッケージは、EAL4追加である。
- 追加される保証コンポーネントは、ALC_DVS.2、AVA_VAN.5である。

2.4 適合根拠

本PPは、他のPPへの適合を主張しないので、適合根拠の記述を行わない。

2.5 適合ステートメント

本PPへの適合を主張するPP/STは、正確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。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。それぞれの内容記述において、必要に応じて [注釈] を付記する。[注釈] は、本PPを参照する際に誤解なく内容が理解されるために記載したもので、セキュリティ課題定義本文には含まれない。

3.1　脅威

本TOEに関して、対抗すべき脅威を示す。これらの脅威は、TOE、その運用環境、あるいは両者のコンビネーションによって対抗されねばならない。

T.Copy

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3-1]　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から、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

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3-2]　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.Physical_Attack

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3-3]　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) を読み出そうとする攻撃である。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。

3.2　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。本PPでは、ICAOが定める規格への適合、及び日本の旅券発行当局が求める条件を組織のセキュリティ方針に含める。

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、ICAO Doc9303 Part1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する。この基本アクセス制御手順は、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.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、本PPに記載のないものは、その扱いを規定しない。TOE内部データを格納する基本アクセス鍵ファイル、秘密鍵ファイルには、TOE外の利用者はアクセスできない。

[注釈3-4]　IC旅券に必要な国際レベルの相互運用性を満たすため、BAC手順への対応が必要である。この手順に含まれる相互認証機能、セキュアメッセージング機能は、高レベルの攻撃に対抗することを意図したものではないが、不正な装置によるTOE内部情報へのアクセスを防止する上で一定の効果がある。BAC手順を正確に実装することで、TOE

に対するスキミング攻撃 (IC旅券を開くことなく、旅券の固有情報の一部を取得する) や盗聴攻撃 (端末装置との通信データを盗聴し、データ中の情報を取得する) を防止できる。BAC手順は、強化基本の攻撃力に対抗できるとされている。本PPでは、能動認証用秘密鍵に対する高レベルの攻撃力を想定しているが、BAC手順が対抗するスキミング攻撃や盗聴攻撃は、そのような高レベルの攻撃力に該当しない。

P.Authority

旅券発行当局の管理下にあるTOEは、表3-1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。

表3-1　旅券発行当局によるTOE内部情報アクセス管理

認証状況[*1]	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)
	EF.DG15		能動認証用公開鍵
輸送鍵による照合成功	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		基本アクセス制御用暗号化鍵 認証子生成鍵
	EF.DG1[*3]		MRZデータ
	EF.DG2[*3]		顔画像
	EF.DG13[*2/*3]		管理データ (旅券番号・冊子管理番号)
	EF.COM[*3]		基本符号化規則の共通情報
	EF.SOD[*3]		ICAO Doc9303 Part1 Volume2 Section IV NORMATIVE APPENDIX 3に定められる受動認証関連セキュリティデータ
能動認証情報アクセス鍵による照合成功	EF.DG15[*3]	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及び読出し鍵、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用者アクセスは禁止される。(旅券保持者へ発行後の端末装置に対するアクセス制御 <基本アクセス制御> 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] 鍵照合成功時の読出し (許可/不許可) については規定しない。

[注釈3-5]　表に記載された各々のファイルは、利用者データあるいはTSFデータを格納する。TSFデータを格納するのは、輸送鍵ファイルである。それ以外のファイルは、利用者データ (暗号鍵管理は、利用者データとして扱う) を格納する。TSFデータファイルは、6章のセキュリティ機能要件におけるアクセス制御対象に含めず、FMT_MTD.1で扱う。

P.Data_Lock

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3-1に示される。

P.Prohibit

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。

3.3 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.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、旅券の発行国、受入国双方のPKI環境の相互運用性が保たれる。

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て、TOE及びその環境におけるセキュリティ対策方針を示す。セキュリティ対策方針は、TOEによって対処するものを4.1に、その環境によって対処するものを4.2に記載する。さらに、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なものであることの根拠を4.3に示す。

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

4.1 TOEのセキュリティ対策方針

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

O.AA

TOEは、デジタル署名を含む個人情報が不正なICチップ上に複製され旅券が偽造されるのを防ぐため、TOEを構成するICチップ自体の真正性を証明する手段を持たねばならない。この手段は、IC旅券の国際レベルでの相互運用性を保証できるよう、標準化されたものでなければならない。このため、ICAO Doc9303 Part1に定められた能動認証に対応できなければならない。

O.Logical_Attack

TOEは、いかなる場合においても、TOEの非接触通信インタフェースを介してTOE内の機密情報 (能動認証用秘密鍵) がTOE外へ読出されることを禁止しなくてはならない。

O.Pysical_Attack

TOEは、物理的手段によって、TOEの非接触通信インタフェースを経由せずにTOE内の機密情報 (能動認証用秘密鍵) を暴露しようとする攻撃を防止しなくてはならない。物理的手段には、非破壊攻撃、破壊攻撃の両方を考慮し、ICチップに対する既知の攻撃のうち、本TOEに適用し得る攻撃に対抗できなくてはならない。

O.BAC

本セキュリティ対策方針は、旅券冊子発行後の運用環境に適用される。IC旅券の国際レベルでの相互運用性を保証するため、ICAO Doc9303 Part1に規定される基本アクセス制御手順を使用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み、TOEと端末装置間の通信は、この手順を使用したものだけが許可されねばならない。端末装置が本TOEから読み出す情報は、同規定に含まれるファイルのうち、EF.DG1、EF.DG2、EF.DG13、EF.DG15、EF.COM、EF.SODに格納される。TOEは、相互認証に成功した端末装置だけに上記ファイルの読出しを許可しなければならない。同規定における上記以外のファイルについて、本PPに記載のないものは、その扱いを規定しない。TOE内部データを格納する基本アクセス鍵ファイル及び秘密鍵ファイルへは、TOE外の利用者がアクセスできてはならない。

ICAO Doc9303 Part1の規定によれば、基本アクセス制御手順が使用する共通暗号鍵は旅券冊子券面に印刷された情報から生成され、その情報の内容と記載様式も同規定に従う必要がある。そのため、この共通暗号鍵の持つエントロピーを旅券冊子券面の印刷情報固有のエントロピー以上に高めることは原理的にできない。この理由により、基本アクセス制御手順によって提供されるTOEのセキュリティ機能は、総当たり攻撃を想定した場合、旅券冊子券面の印刷情報固有のエントロピーが攻撃への抵抗力の上限となる。TOEは、基本アクセス制御手順を正確に実装することによってセキュリティ上の要件を満たさねばならない。

[注釈4-1] 基本アクセス制御手順では、IC旅券のMRZに印刷されたデータから生成する暗号鍵を使用して相互認証とセキュアメッセージングが行われる。この暗号鍵は、旅券券面を開けばその印刷データから生成可能であり、要求される機密性は高くない。生成される暗号鍵のエントロピーも高レベルの攻撃に対抗できるほど大きくない。しかし、基本アクセス制御手順のセキュリティ機能が能動認証用秘密鍵の保護に影響を与えることはない。本セキュリティ対策方針は、高レベルの攻撃への対抗を意図するものではなく、スキミングや盗聴など限定された攻撃からTOEを保護するため、基本アクセス制御手順を正確に実装することを意図したものである。

O.Authority

TOEは、旅券発行当局管理下の環境において、組織のセキュリティ方針P.Authorityに記載された表3-1に従い、TOE内部情報にアクセスできる利用者と操作方法を制限しなくてはならない。

O.Data_Lock

TOE内部情報の操作を正当な利用者 (発行当局管理下においては権限を持つ職員、旅券発行後は端末装置) だけに制限し、それ以外の利用者による不正な読出し・書込みを防がねばならない。そのための手段として、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、それぞれの鍵に関わる認証に基づいて許可されるTOE内部情報の読出し・書込みを恒久的に禁止しなければならない。このセキュリティ対策方針は、TOEが旅券保持者へ発行される前に、発行当局者が意図的に認証失敗を起こして読出し鍵・輸送鍵・能動認証情報アクセス鍵を無効化する際にも適用しなければならな

い。読出し鍵、輸送鍵及び能動認証情報アクセス鍵とそれに対応するTOE内部情報との関係は、組織のセキュリティ方針P.Authorityの表3-1に示される。O.Data_Lockが実施されたのちは、O.BACに記載されたTOEへのアクセスだけが許可される。

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、ここに記載されたセキュリティ対策方針は、すべて前提条件に由来するものである。

OE.Administrative_Env

旅券発行当局の管理下にあるTOEは、発行手続きを経て旅券所持者に渡されるまでの間、当局によってセキュアに管理され処理されねばならない。

OE.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 (旅券保持者に関わる情報及び能動認証用公開鍵) 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、旅券の発行国、受入国双方において、PKI環境の相互運用性が保たれた状況でTOEが使用されねばならない。

4.3 セキュリティ対策方針根拠

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

4.3.1 セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義とセキュリティ対策方針の対応を表4-1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 4-1 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 ＼ セキュリティ対策方針	O.AA	O.Physical_Attack	O.Logical_Attack	O.BAC	O.Authority	O.Data_Lock	OE.Administrative_Env	OE.PKI
T.Copy	x							
T.Physical_Attack		x						
T.Logical_Attack			x					
P.BAC				x				
P.Authority					x			
P.Data_Lock						x		
P.Prohibit						x		
A.Administrative_Env							x	
A.PKI								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、識別された脅威がすべて十分に対抗され、組織のセキュリティ方針が実施され、さらに、前提条件が適切に満たされることの根拠を示す。

T.Copy

攻撃者がTOEと同様の機能性を持つICチップにTOEから読み出した個人情報の複製 (デジタル署名付き) を使用すれば、デジタル署名による検証では偽造旅券を検出できない。この攻撃を防ぐため、TOEのセキュリティ対策方針O.AAによって、ICチップにチップ自身の真正性を検証できるデータをTOEに埋め込む。これによって不正なICチップを検出でき旅券の偽造を防げるので、T.Copyの脅威が除去される。

T.Logical_Attack

TOEのセキュリティ対策方針O.Logical_Attackによって、いかなる場合においても、TOEの非接触インタフェースからTOE内の機密情報 (能動認証用秘密鍵) 読出しが禁止される。このため、脅威T.Logical_Attackが除去される。

T.Physical_Attack

TOEのセキュリティ対策方針O.Physical_Attackによって、TOEの非接触通信インタフェース

を経由せず、物理的手段によってTOE内の機密情報 (能動認証用秘密鍵) を暴露しようとする攻撃に対抗する。物理的手段には非破壊攻撃、破壊攻撃の両方が考慮され、ICチップに対する既知の攻撃にTOEが対抗できるような対策を施す。これによって、実用上十分な程度に脅威を軽減できる。

P.BAC

TOEのセキュリティ対策方針O.BACは、ICAO Doc9303 Part1に規定される基本アクセス制御手順を適用することによって、許可された者 (端末装置) だけがセキュアな通信路を用いてTOEの内部情報を読み出せるようにする。O.BACは、P.BACの内容をすべてカバーしており、組織のセキュリティ方針P.BACが適切に実施される。

P.Authority

TOEのセキュリティ対策方針O.Authorityは、組織のセキュリティ方針P.Authorityを直接実施する内容である。

P.Data_Lock

TOEのセキュリティ対策方針O.Data_Lockは、組織のセキュリティ方針P.Data_Lockが求める内容をカバーしており、P.Data_Lockを適切に実施する。

P.Prohibit

組織のセキュリティ方針P.Prohibitは、その実施手段として、TOEの正当な利用者による意図的な認証失敗の実施を求めている。P.Prohibitに対応するためにTOEに求められるアクションは、TOEへの不正な攻撃を想定した組織のセキュリティ対策方針P.Data_Lockに対するものと重複する。従って、TOEのセキュリティ対策方針O.Data_Lockは、P.Prohibitの内容も同様に実施することとなる。

A.Administrative_Env

環境のセキュリティ対策方針OE.Administrative_Envは、前提条件A.Administrative_Envに直接対応しており、同前提条件が満たされる。

A.PKI

環境のセキュリティ対策方針OE.PKIは、前提条件A.PKIに直接対応しており、同前提条件が満たされる。

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を定義しない。

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。表6-1にSFRのリストを示す。

表6-1　SFRリスト

章番号	識別名	
6.1.1	FCS_CKM.1	暗号鍵生成
6.1.2	FCS_CKM.4	暗号鍵破棄
6.1.3	FCS_COP.1a	暗号操作 (能動認証)
6.1.4	FCS_COP.1m	暗号操作 (相互認証)
6.1.5	FCS_COP.1s	暗号操作 (セキュアメッセージング)
6.1.6	FDP_ACC.1a	サブセットアクセス制御 (発行処理)
6.1.7	FDP_ACC.1b	サブセットアクセス制御 (基本アクセス制御)
6.1.8	FDP_ACF.1a	セキュリティ属性によるアクセス制御 (発行処理)
6.1.9	FDP_ACF.1b	セキュリティ属性によるアクセス制御 (基本アクセス制御)
6.1.10	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
6.1.11	FDP_UCT.1	基本データ交換機密性
6.1.12	FDP_UIT.1	基本データ交換完全性
6.1.13	FIA_AFL.1a	認証失敗時の取り扱い (能動認証情報アクセス鍵)
6.1.14	FIA_AFL.1d	認証失敗時の取り扱い (輸送鍵)
6.1.15	FIA_AFL.1r	認証失敗時の取り扱い (読出し鍵)
6.1.16	FIA_UAU.2	アクション前の利用者認証
6.1.17	FIA_UAU.4	単一認証メカニズム
6.1.18	FIA_UAU.5	複数の認証メカニズム
6.1.19	FIA_UID.2	アクション前の利用者識別
6.1.20	FMT_MTD.1	TSFデータの管理
6.1.21	FMT_SMF.1	管理機能の特定
6.1.22	FMT_SMR.1	セキュリティの役割
6.1.23	FPT_PHP.3	物理的攻撃への抵抗
6.1.24	FTP_ITC.1	TSF間高信頼チャネル

CCパート2のセキュリティ機能コンポーネントに、必要に応じた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。

- 繰返し操作の対象となるSFRは、対応するコンポーネント識別の末尾に “a” などのアルファベット小文字及びSFRの目的を示すカッコ付けの短い説明「(能動認証)など」を付与することで識別する。
- 割付あるいは選択操作の箇所を[割付: ×××*(斜体)*]、[選択: ×××*(斜体)*]の形式で示す。詳細化部分も*斜体*で示すが、本PPでは詳細化を行っていない。

- 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。
- 本PPでは、一部の操作が未了であり、その個所を[割付: *ＸＸＸ(斜体・下線)*]のように下線で示す。ST作成者は、未了部分の操作を完了せねばならない。

以下、本PPで規定するSFRを示す。

6.1.1 FCS_CKM.1 暗号鍵生成

下位階層: なし

依存性: [FCS_CKM.2 暗号鍵配付、または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1 TSFは、以下の[割付: *ICAO Doc9303 Part1で特定される基本アクセス制御に含まれるセキュアメッセージング方式の規程*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *同規程において定められる暗号化用セッション鍵及び認証子生成用セッション鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *16バイト*]に従って、暗号鍵を生成しなければならない。

6.1.2 FCS_CKM.4 暗号鍵破棄

下位階層: なし

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

FCS_CKM.4.1 TSFは、以下の[割付: *なし*]に合致する、指定された暗号鍵破棄方法[割付: *[選択: 電源断による揮発性メモリ上の暗号鍵消去、新規暗号鍵データの上書き、[割付: その他の暗号鍵破棄方法]]*]に従って、暗号鍵を破棄しなければならない。

6.1.3 FCS_COP.1a 暗号操作 (能動認証)

下位階層: なし

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

FCS_COP.1.1a TSFは、[割付: *ICAO Doc9303 Part1で規定されるActive Authentication (能動認*

証）で使用するデジタル署名の標準（ISO/IEC 9796-2:2002 Digital signature scheme 1に準拠）]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *能動認証用データに対するデジタル署名*]を実行しなければならない。

[注釈6-1]　本要件の割付操作を行う際、ST作成者は、旅券発行当局方針と整合をはからねばならない。

6.1.4　FCS_COP.1m　暗号操作 (相互認証)

下位階層: なし

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

FCS_COP.1.1m　TSFは、[割付: *ICAO Doc9303 Part1で規定される基本アクセス制御に含まれる相互認証方式の標準*]に合致する、特定された暗号アルゴリズム[割付: *CBCモード Triple DES*]と暗号鍵長[割付: *16バイト*]に従って、[割付: *相互認証における認証用データの暗号化あるいは復号、及び認証子生成・検証*]を実行しなければならない。

6.1.5　FCS_COP.1s　暗号操作 (セキュアメッセージング)

下位階層: なし

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

FCS_COP.1.1s　TSFは、[割付: *ICAO Doc9303 Part1で規定される基本アクセス制御に含まれるセキュアメッセージング方式の標準*]に合致する、特定された暗号アルゴリズム[割付: *表6-2に示す暗号アルゴリズム*]と暗号鍵長[割付: *表6-2に示す暗号鍵長*]に従って、[割付: *表6-2に示す暗号操作*]を実行しなければならない。

表6-2　セキュアメッセージングの暗号方式

暗号アルゴリズム	*暗号鍵長*	*暗号操作*
CBCモードSingle DES	*8バイト*	*認証子生成・検証(メッセージの最終ブロックを除く)*

CBCモードTriple DES	*16バイト*	*メッセージの暗号化・復号* *認証子生成・検証(メッセージの最終ブロック)*

6.1.6　FDP_ACC.1a　サブセットアクセス制御 (発行処理)

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.1.1a　TSFは、[割付: *サブジェクト<利用者プロセス>、オブジェクト<組織のセキュリティ方針P.Authorityの表3-1に示すファイル; ただし輸送鍵ファイルを除く>、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のリスト<オブジェクトへのデータ入出力操作>*]に対して[割付: *発行処理アクセス制御SFP*]を実施しなければならない。

[注釈6-2]　P.Authorityの表3-1に示すデータファイルのうち、「輸送鍵ファイル」に格納されるデータ「輸送鍵」は、利用者の認証データとして使われるTSFデータである。本PPでは、管理要件のFMT_MTD.1でこの輸送鍵の管理を規定するので、輸送鍵ファイルをアクセス制御対象に含めない。しかし、これはCCにおける利用者データとTSFデータを区別を反映したものであり、実装上のメカニズムの差異を意図するものではない。

6.1.7　FDP_ACC.1b　サブセットアクセス制御 (基本アクセス制御)

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

FDP_ACC.1.1b　TSFは、[割付: *サブジェクト[端末装置代行プロセス]、オブジェクト[ファイル EF.DG1、EF.DG2、EF.DG13、EF.DG15、EF.COM、EF.SOD、基本アクセス鍵ファイル、秘密鍵ファイル]、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のリスト[オブジェクトからのデータ読出し]*]に対して[割付: *基本アクセス制御SFP*]を実施しなければならない。

[注釈6-3]　ICAO Doc9303 Part1では、上記ファイル以外に、EF.DG3～12、EF.DG14、EF.DG16の各ファイルが規定される。これらファイルは本TOEで使用しないので、本PPではその扱いを規定しない。一方、日本国以外の調達者が本PPを利用する場合、これらファイルの追加が必要になることがある。PP/ST作成者がこれらファイルをオブジェクトに追加して本PPのSFRを変更する場合でも、

本PPのSFRが満たされていれば、本PPへの正確適合は維持される。しかしながら、ST作成においてオブジェクトとその操作が追加される場合、たとえ本PPへの正確適合が維持されるとしても、TOE調達者の合意の必要性を考慮すべきである。

6.1.8 FDP_ACF.1a セキュリティ属性によるアクセス制御 (発行処理)

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.1.1a TSFは、以下の[割付: *示されたSFP下において制御されるサブジェクト[利用者プロセス]、オブジェクト[組織のセキュリティ方針P.Authorityの表3-1に示すファイル; ただし輸送鍵ファイルを除く]、及び各々に対応する、SFP関連セキュリティ属性[組織のセキュリティ方針P.Authorityの表3-1に示す認証状況]*]に基づいて、オブジェクトに対して、[割付: *発行処理アクセス制御SFP*]を実施しなければならない。

FDP_ACF.1.2a 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: *組織のセキュリティ方針P.Authorityの表3-1に示された認証状況が満たされたとき、その認証状況に紐付けられたファイルへの操作が許可される*]。

FDP_ACF.1.3a 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.1.4a 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。

6.1.9 FDP_ACF.1b セキュリティ属性によるアクセス制御 (基本アクセス制御)

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

FDP_ACF.1.1b TSFは、以下の[割付: *示されたSFP下において制御されるサブジェクト[端末装置代行プロセス]とオブジェクト[ファイル EF.DG1、EF.DG2、EF.DG13、EF.DG15、EF.COM、EF.SOD]、及び、セキュリティ属性[相互認証に基づく端末装置の認証状態]*]に基づいて、オブジェクトに対して、[割付: *基本アクセス制*

御SFP]を実施しなければならない。

FDP_ACF.1.2b　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: *端末装置の認証状態が認証済みの場合に限り、サブジェクトは、オブジェクトからデータ読出しを許可される。*]。

FDP_ACF.1.3b　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.1.4b　TSFは、次の追加規則、[割付: *サブジェクトによる基本アクセス鍵ファイル及び秘密鍵ファイルへのアクセス禁止*]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。

6.1.10　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

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

FDP_ITC.1.1　TSFは、SFP制御下にある利用者データをTOEの外部からインポートするとき、[割付: *発行処理アクセス制御SFP*]を実施しなければならない。

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

FDP_ITC.1.3　TSFは、TOE外部からSFPの下で制御される利用者データをインポートするとき、[割付: *組織のセキュリティ方針P.Authorityの表3-1における「許可されるアクセス」に示されたとおりに書込み対象ファイルとデータを関連付け*]の規則を実施しなければならない。

6.1.11　FDP_UCT.1　　基本データ交換機密性

下位階層: なし
依存性:　[FTP_ITC.1 TSF間高信頼チャネル、または
FTP_TRP.1 高信頼パス]
[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]

FDP_UCT.1.1　TSFは、不当な暴露から保護した形で利用者データの[選択: *送信*、*受信*]を行うために、[割付: *基本アクセス制御SFP*]を実施しなければならない。

6.1.12　FDP_UIT.1 データ交換完全性

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]
[FTP_ITC.1 TSF間高信頼チャネル、または
FTP_TRP.1高信頼パス]

FDP_UIT.1.1　TSFは、利用者データを[選択: *改変*、*消去*、*挿入*、*リプレイ*]誤りから保護した形で[選択: *送信*、*受信*]を行うために、[割付: *基本アクセス制御SFP*]を実施しなければならない。

FDP_UIT.1.2　TSFは、利用者データ受信において、[選択: *改変*、*消去*、*挿入*、*リプレイ*]が生じたかどうかを判定できなければならない。

6.1.13　FIA_AFL.1a　認証失敗時の取り扱い (能動認証情報アクセス鍵)

下位階層: なし
依存性:　FIA_UAU.1 認証のタイミング

FIA_AFL.1.1a　TSFは、[割付: *能動認証情報アクセス鍵による認証*]に関して、[選択: *[割付: 正の整数値]、~~[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値~~*]回の不成功認証試行が生じたときを検出しなければならない。

[注釈6-4]　ST作成者は、1～15の範囲から正の整数値を指定する。

FIA_AFL.1.2a　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: *能動認証情報アクセス鍵による認証の恒久的停止（能動認証情報アクセス鍵による認証状態を「認証なし」に固定）*]をしなければならない。

6.1.14　FIA_AFL.1d　認証失敗時の取り扱い (輸送鍵)

下位階層: なし
依存性:　FIA_UAU.1 認証のタイミング

FIA_AFL.1.1d　TSFは、[割付: *輸送鍵による認証*]に関して、[選択: *[割付: 正の整数値]*、~~*[割付:*~~

~~*許容可能な値の範囲]内における管理者設定可能な正の整数値*~~]回の不成功認証試行が生じたときを検出しなければならない。

[注釈6-5] ST作成者は、1～15の範囲から正の整数値を指定する。

FIA_AFL.1.2d 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: *輸送鍵による認証の恒久的停止（輸送鍵による認証状態を「認証なし」に固定）*]をしなければならない。

6.1.15 FIA_AFL.1r 認証失敗時の取り扱い (読出し鍵)

下位階層: なし
依存性: FIA_UAU.1 認証のタイミング

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

[注釈6-6] ST作成者は、1～15の範囲から正の整数値を指定する。

FIA_AFL.1.2r 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: *読出し鍵による認証の恒久的停止（読出し鍵による認証状態を「認証なし」に固定）*]をしなければならない。

6.1.16 FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング
依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1 TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

6.1.17 FIA_UAU.4 単一使用認証メカニズム

下位階層: なし
依存性: なし

FIA_UAU.4.1 TSFは、[割付: *相互認証メカニズム*]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。

6.1.18　FIA_UAU.5　　複数の認証メカニズム

下位階層: なし
依存性:　なし

FIA_UAU.5.1　TSFは、利用者認証をサポートするため、[割付: *表6-3に示す複数の認証メカニズム*]を提供しなければならない。

FIA_UAU.5.2　TSFは、[割付: *表6-3に示す、複数の認証メカニズムがどのように認証を提供するかを記述する規則*]に従って、利用者が主張する識別情報を認証しなければならない。

表6-3　複数の認証メカニズム

認証メカニズムの名称	認証メカニズムに適用される規則
輸送鍵	TOEに格納済みの輸送鍵との照合
読出し鍵	TOEに格納済みの読出し鍵との照合
能動認証情報アクセス鍵	TOEに格納済みの能動認証情報アクセス鍵との照合
相互認証	ICAO Doc9303 Part1に定められた相互認証手順に基づく端末装置の認証規則

6.1.19　FIA_UID.2　　アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング
依存性:　なし

FIA_UID.2.1　TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.20　FMT_MTD.1　　TSFデータの管理

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

FMT_MTD.1.1　TSFは、[割付: *輸送鍵*]を[選択: ~~*デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]*~~]する能力を[割付: *旅券発行当局の権限者*]に制限しなければならない。

[注釈6-7]　本要件は、フェーズ3において、TOEが旅券冊子製造者から旅券

事務所へ輸送される際の輸送鍵設定に関わるものである。本要件においてTSFデータの管理を許可される旅券発行当局権限者は、国立印刷局の職員である。TOEが旅券事務所に輸送されたのちは、その職員が輸送鍵を書き換える機会はない。一方、TOEが国立印刷局、旅券事務所のどちらにあるときも、攻撃者が不正に輸送鍵を書き換えるという脅威が存在しないので、セキュリティ要件として国立印刷局職員と旅券事務所職員を区別する必然性がない。そのため、本要件では特に両者を区別せず、管理権限者を「旅券発行当局の権限者」と称している。

6.1.21　FMT_SMF.1　　管理機能の特定

下位階層: なし
依存性:　なし

FMT_SMF.1.1　TSFは、以下の管理機能を実行することができなければならない。: [割付: *輸送鍵の改変*]

6.1.22　FMT_SMR.1　　セキュリティの役割

下位階層: なし
依存性:　FIA_UID.1 識別のタイミング

FMT_SMR.1.1　TSFは、役割[割付: *旅券発行当局の権限者*]を維持しなければならない。

FMT_SMR.1.2　TSFは、利用者を役割に関連付けなければならない。

6.1.23　FPT_PHP.3　　物理的攻撃への抵抗

下位階層: なし
依存性:　なし

FPT_PHP.3.1　TSFは、SFRが常に実施されるよう自動的に対応することによって、[割付: *TOEのハードウェア及びTSFを構成するファームウェアとソフトウェア*]への[割付: *以下の物理的攻撃シナリオのリストに示した攻撃*]に抵抗しなければならない。

[物理的攻撃シナリオのリスト]

- *TOEの外殻を破壊し、内部回路への物理的プロービングや操作(manipulation)を通してTOEの動作を分析することによって機密情報（能動認証用秘密鍵）を暴露する。*
- *動作中のTOEに環境ストレス（正常動作範囲以外の温度・電源電圧・クロッ*

ク印加、あるいは、電磁パルス印加、光照射など）を加えることによってTOEの正常な動作を阻害し、そのときのTOEのふるまいを分析することによって機密情報（能動認証用秘密鍵）を暴露する。

- *動作中のTOEから漏洩する電磁波をモニタすることによってTOE動作を解析し、機密情報（能動認証用秘密鍵）を暴露する。*

[注釈6-8]　物理的攻撃に対抗するためのセキュリティ機能要件は、すべてこの要件に集約している。TOEの動作に伴う電磁波漏えいをモニタするような攻撃は、TSFへの干渉や損壊を伴わないかもしれない。そのような攻撃への対抗手段として、物理的手段（電磁波シールドなど）が使われるかもしれず、あるいは論理的手段（消費電力のランダム化など）が併用されるかもしれない。しかし、攻撃手段にTOEの論理的インタフェースを経由しない物理的手段が使われるという点で、他の物理的攻撃と同じカテゴリに含めることが合理的である。そのため、本要件中の物理的攻撃シナリオにモニタ攻撃を加え、そのような攻撃への対抗要件を定義した。

6.1.24　FTP_ITC.1　　TSF間高信頼チャネル

下位階層: なし
依存性:　なし

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

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

FTP_ITC.1.3　TSFは、[割付: *TOEからのデータ読み出し*]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。

[注釈6-9]　端末装置とTSF間の通信は、ICAO Doc9303 Part1に規定されるセキュアメッセージングチャネル経由で行わねばならない。セキュアメッセージングチャネルの確立後、端末装置とTOE間の通信路は、セキュアメッセージングチャネルだけとなる。

6.2　セキュリティ保証要件

本TOEに適用するセキュリティ保証要件は、表6-4に示す保証コンポーネントで定義される。これらは、すべて、CC パート3に含まれる。ALC_DVS.2とAVA_VAN.5を除くコンポーネ

ントは、保証パッケージEAL4に含まれる。ALC_DVS.2はALC_DVS.1の、AVA_VAN.5はAVA_VAN.3の上位コンポーネントである。

表6-4に示すすべてのコンポーネントにおいて、本PPでは、操作を適用していない。

表6-4　保証コンポーネント

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

6.3　セキュリティ要件根拠

6.3.1　セキュリティ機能要件根拠

本章では、定義されたSFRがTOEのセキュリティ対策方針を適切に達成することの根拠を示す。6.3.1.1では、各々のSFRがいずれかのTOEのセキュリティ対策方針にさかのぼれること、6.3.2.2では、各々のTOEのセキュリティ対策方針が対応する有効なSFRによって適切に満たされることを説明する。

6.3.1.1 セキュリティ対策方針とセキュリティ機能要件の対応

TOEのセキュリティ対策方針に対応するSFRを表6-5に示す。この表は、すべてのSFRが少なくとも一つのTOEのセキュリティ対策方針にさかのぼれることの根拠となる。

表6-5 TOEセキュリティ対策方針とSFRの対応

TOEセキュリティ対策方針 / SFR	FCS_CKM.1	FCS_CKM.4	FCS_COP.1a	FCS_COP.1m	FCS_COP.1s	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FDP_UCT.1	FDP_UIT.1	FDP_ITC.1	FIA_AFL.1a	FIA_AFL.1d	FIA_AFL.1r	FIA_UAU.2	FIA_UAU.4	FIA_UAU.5	FIA_UID.2	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_PHP.3	FTP_ITC.1
O.Logical_Attack							x		x															
O.Physical_Attack																							x	
O.AA			x			x		x				x												
O.BAC	x	x		x	x		x		x	x	x	x				x	x	x	x					x
O.Authority						x		x				x				x		x	x	x	x	x		
O.Data_Lock													x	x	x									

6.3.1.2 対応関係の根拠説明

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

O.AA

セキュリティ対策方針O.AAを達成するため、ICAO Doc9303 Part1に定められた能動認証手順に対応しなければならない。この能動認証は、端末装置がTOEのICチップを認証する行為であり、TOE自体に認証メカニズムは要求されない。TOEは、端末装置が要求する認証手順に正しく応答することで認証を受ける。端末装置からの認証手順要求に対応するため、TOEは、公開鍵暗号方式の公開鍵・秘密鍵ペアを内部に持ち、FCS_COP.1aで規定される秘密鍵を用いた暗号操作を行う。公開鍵・秘密鍵ペアは、FDP_ITC.1によってTOEへインポートされる。FDP_ITC.1に伴うアクセス制御は、FDP_ACC.1a及びFDP_ACF.1aで規定される。これらのSFRによって、O.AAが十分に達成される。

O.Logical_Attack

保護の対象となる機密情報 (能動認証用秘密鍵) は、TOEの秘密鍵ファイルに格納される。旅券発行後のTOEに適用されるFDP_ACC.1b及びFDP_ACF.1bによって、端末装置を代行する利用者プロセスによる秘密鍵ファイルからのデータ読出しが拒否される。これらSFRによって、O.Logical_Attackが十分に達成される。

O.Physical_Attack

物理的手段によって機密情報である能動認証用秘密鍵を暴露しようとする攻撃シナリオは、FPT_PHP.3に示された攻撃リストに示される。これらの攻撃に対し、FPT_PHP.3に従ってTSFが自動的に対抗し、機密情報の暴露を防ぐ。これによって、O.Physical_Attackが十分に達成される。

O.BAC

FIA_UID.2、FIA_UAU.2によって、識別・認証に成功した利用者 (端末装置が相当する) にTOEのサービスが提供される。利用者認証にはICAOが定める基本アクセス制御方式の相互認証手順が要求され、これは、FIA_UAU.5によって規定される。この相互認証手順では、1回の認証ごとに乱数に基づく新たな認証データが必要となり、FIA_UAU.4で規定される。同じく、基本アクセス制御方式が要求するセキュアメッセージングは、FDP_UCT.1、FDP_UIT.1による送受信データ保護、FTP_ITC.1による暗号通信チャネルの要件で規定される。さらに、基本アクセス制御手順で必要な暗号処理に関して、FCS_COP.1mで相互認証手順に必要な暗号操作、FCS_COP.1sでセキュアメッセージング用の暗号操作が規定される。セキュアメッセージングに使用される暗号鍵に関しては、FDP_ITC.1で基本アクセス鍵のインポート、FCS_CKM.1でセッション鍵の生成、FCS_CKM.4で鍵の破棄が規定される。許可された者だけがTOEから所定の情報を読み出せるようにするため、FDP_ACC.1b、FDP_ACF.1bによるアクセス制御規則が定められる。これらのSFRによって、O.BACが十分に達成される。

O.Authority

旅券発行当局のTOE処理において、正当な権限を持つ利用者だけに処理権限を付与するため、識別・認証の要件FIA_UID.2、FIA_UAU.2が適用される。利用者認証のメカニズムには、FIA_UAU.5によって、輸送鍵、読出し鍵、あるいは能動認証情報アクセス鍵の使用が規定される。これらの鍵の照合によって認証に成功した利用者には、FDP_ACC.1a、FDP_ACF.1aのアクセス制御規則が適用され、O.Authorityに規定されたTOEの内部情報アクセスが許可される。利用者の操作には、認証鍵 (輸送鍵) 、暗号鍵 (能動認証用公開鍵・秘密鍵ペア、セキュアメッセージング用基本アクセス鍵) 、その他の利用者データのTOEへの書込みが含まれ、書込み時のオブジェクトとセキュリティ属性の対応付けは、FDP_ITC.1で規定される。O.Authorityには、旅券発行当局の権限者による輸送鍵の更新 (書換え) が含まれ、これは、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1で規定される。これらのSFRによって、O.Authorityが十分に達成される。

O.Data_Lock

FIA_AFL.1a、FIA_AFL.1d及びFIA_AFL.1rの3つのSFRによって、能動認証情報アクセス鍵、輸送鍵あるいは読出し鍵による認証失敗が生じたとき、それぞれの鍵に対応する認証を恒

久的に禁止するというセキュリティ対策方針が十分に達成される。

6.3.1.3　セキュリティ機能要件の依存性

各SFRに規定された依存性とその対応状況を表6-6に示す。

表において、「依存性の要求」欄にはSFRに規定された依存性を示す。「依存性の対応」欄には、規定された依存性がPP中のどのSFRによって満たされるか、あるいは満たされない場合の正当性を示す根拠が記述される。

表6-6　SFRの依存性

SFR	依存性の要求	依存性への対応
FCS_CKM.1	[FCS_CKM.2または FCS_COP.1] FCS_CKM.4	FCS_COP.1s及び FCS_CKM.4が対応し、依存性が満たされる。
FCS_CKM.4	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1]	FCS_CKM.1が対応し、依存性が満たされる。
FCS_COP.1a	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1] FCS_CKM.4	FDP_ITC.1が対応する。暗号鍵の改変・破棄は禁止なので、破棄の要件FCS_CKM.4は適用されない。
FCS_COP.1m	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1] FCS_CKM.4	FDP_ITC.1が対応する。暗号鍵の改変・破棄は禁止なので、破棄の要件FCS_CKM.4は適用されない。
FCS_COP.1s	[FDP_ITC.1または FDP_ITC.2または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1及びFCS_CKM.4が対応し、依存性が満たされる。
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1aが対応し、依存性が満たされる。
FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1bが対応し、依存性が満たされる。
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1aが対応する。オブジェクトは、初期設定で生成され、TOE運用環境では生成されない。このため、ファイル生成に関わるFMT_MSA.3は適用されない。
FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1bが対応する。オブジェクトは、初期設定で生成され、TOE運用環境では生成されない。このため、ファイル生成に関わるFMT_MSA.3は適用されない。
FDP_ITC.1	[FDP_ACC.1 または FDP_IFC.1]	FDP_ACC.1aが対応する。オブジェクトは、初期設定で生成され、TOE運用環境では生成

	FMT_MSA.3	されない。このため、ファイル生成に関わるFMT_MSA.3は適用されない。
FDP_UCT.1	[FTP_ITC.1またはFTP_TRP.1] [FDP_ACC.1またはFDP_IFC.1]	FTP_ITC.1及びFDP_ACC.1bが対応し、依存性が満たされる。
FDP_UIT.1	FDP_ACC.1またはFDP_IFC.1] [FTP_ITC.1またはFTP_TRP.1]	FTP_ITC.1及びFDP_ACC.1bが対応し、依存性が満たされる。
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.2が対応し、依存性が満たされる。
FIA_AFL.1d	FIA_UAU.1	FIA_UAU.2が対応し、依存性が満たされる。
FIA_AFL.1r	FIA_UAU.1	FIA_UAU.2が対応し、依存性が満たされる。
FIA_UAU.2	FIA_UID.1	FIA_UID.2が対応し、依存性が満たされる。
FIA_UAU.4	なし	不要
FIA_UAU.5	なし	不要
FIA_UID.2	なし	不要
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1及びFMT_SMF.1が対応し、依存性が満たされる。
FMT_SMF.1	なし	不要
FMT_SMR.1	FIA_UID.1	FIA_UID.2が対応し、依存性が満たされる。
FPT_PHP.3	なし	不要
FTP_ITC.1	なし	不要

6.3.2 セキュリティ保証要件根拠

本TOEのセキュリティ機能性の特徴は、能動認証機能を採用してTOE (ICチップ) の偽造を困難にした点にある。このセキュリティ特性は、TOE内の機密情報 (秘密鍵) 保護によって達成される。ICチップ内に秘匿された情報を読み出すには、高度な物理的攻撃手段が必要で、このような攻撃を行い得る高レベルの攻撃者を想定し、脆弱性評定の保証要件としてAVA_VAN.5を要求する。関連して、攻撃手段に利用される開発情報の保護を厳密にするため、開発セキュリティ保証要件をALC_DVS.2とする。

一方、ICチップをTOEとする場合、要求されるSFRやそれを実現する設計手法に最新の技術が要求されるが、製品のセキュリティ機能性に大きなバリエーションがある訳ではなく、評価上の確認ポイントも明確である。このため、開発セキュリティと脆弱性評定を除いた開発・製造の保証要件として、商用製品として最高レベルではあるがEAL5ほどの厳密性を必要としない、EAL4を設定する。

なお、ALC_DVS.2には他のコンポーネントへの依存性がなく、AVA_VAN.5に規定される依存性はAVA_VAN.3 (EAL4) と同一である。従って、依存性に関してEAL4保証パッケージと変わる部分がないため、表6-4に示す各保証コンポーネント間の依存性はすべて満たされ

る。

7　用語

7.1　CC関連

PP	Protection Profile
CC	Common Criteria; CCと同一の内容がISO/IEC 15408規格としても制定される。
ST	Security Target
TOE	Target of Evaluation; 評価対象

7.2　IC旅券関連

ICAO	International Civil Aviation Organization; 国際民間航空機関
国立印刷局	旅券冊子を作成し、TOEに基本的データ (旅券番号などの管理データ、能動認証用公開鍵・秘密鍵ペアなど) を設定する。
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。
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。
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。