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 2.10 版

2022 年 1 月 24 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[Doc 9303]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 が対象とする旅券冊子用 IC は高度化基本アクセス制御（SAC： Supplemental Access Control）及び能動認証（AA： Active Authentication）に対応する IC 旅券に向けたものである。

高度化基本アクセス制御に対応した旅券冊子用 IC 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（PACEv2： Password Authenticated Connection Establishment v2）の両方をサポートすることが求められる。ただし、基本アクセス制御は本 PP の 1.2.3 で規定される TOE のライフサイクルのフェーズ 3 において基本アクセス制御の無効化機能を使って無効化される場合もある。

基本アクセス制御と鍵共有利用アクセス制御は、いずれも相互認証とセキュアメッセージングの方式で、後者はセッション鍵の暗号強度を強化した方式である。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。なお、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旅券冊子用 IC を TOE とする場合、本 PP 及び「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－」（以下、PACE PP）への適合が求められる。その際、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は本 PP に、それ以外のセキュリティ機能は PACE PP に適合した ST に基づく評価がなされる。一方、これらの機能を持たない旅券冊子用 IC を TOE とする場合は PACE PP への適合のみが求められる。

能動認証は、旅券冊子用 IC に格納された旅券冊子用 IC に固有の秘密鍵の真正性を検証することにより、不正な旅券冊子用 IC による旅券偽造を防止するものである。

本 PP は、CC バージョン 3.1 改訂第 5 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 及び BSI 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

1.1 PP 参照 1

1.2 TOE 概要 1

1.2.1 TOE 種別 1

1.2.2 TOE の用途と主要セキュリティ機能 1

1.2.3 TOE のライフサイクル 2

2. 適合主張 5

2.1 CC 適合主張 5

2.2 PP 主張 5

2.3 パッケージ主張 5

2.4 適合根拠 5

2.5 適合ステートメント 5

3. セキュリティ課題定義 6

3.1 脅威 6

3.2 組織のセキュリティ方針 7

3.3 前提条件 9

4. セキュリティ対策方針 11

4.1 TOE のセキュリティ対策方針 11

4.2 運用環境のセキュリティ対策方針 13

4.3 セキュリティ対策方針根拠 13

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 13

4.3.2 セキュリティ対策方針の根拠説明 14

5. 拡張コンポーネント定義 17

5.1 FCS_RND 乱数生成 17

6. セキュリティ要件 18

6.1 セキュリティ機能要件 18

6.1.1 FCS_CKM.1b 暗号鍵生成（基本アクセス制御） 19

6.1.2 FCS_CKM.1p 暗号鍵生成（鍵共有利用アクセス制御 セッション鍵）.....19
6.1.3 FCS_CKM.1e 暗号鍵生成（鍵共有利用アクセス制御 一時的鍵ペア）.....20
6.1.4 FCS_CKM.4 暗号鍵破棄.....20
6.1.5 FCS_.COP.1a 暗号操作（能動認証 署名生成）.....20
6.1.6 FCS_.COP.1h 暗号操作（能動認証 ハッシュ関数）.....21
6.1.7 FCS_.COP.1hb 暗号操作（基本アクセス制御 ハッシュ関数）.....21
6.1.8 FCS_.COP.1mb 暗号操作（基本アクセス制御 相互認証）.....21
6.1.9 FCS_COP.1sb 暗号操作（基本アクセス制御 セキュアメッセージング）.....22
6.1.10 FCS_.COP.1n 暗号操作（ナンス暗号化）.....22
6.1.11 FCS_COP.1e 暗号操作（鍵共有）.....23
6.1.12 FCS_.COP.1hp 暗号操作（鍵共有利用アクセス制御 ハッシュ関数）.....23
6.1.13 FCS_COP.1mp 暗号操作（鍵共有利用アクセス制御 相互認証）.....23
6.1.14 FCS_COP.1sp 暗号操作（鍵共有利用アクセス制御 セキュアメッセージング）.....24
6.1.15 FCS_RND.1 乱数に対する品質基準.....24
6.1.16 FDP_ACC.1a サブセットアクセス制御（発行処理）.....24
6.1.17 FDP_ACC.1b サブセットアクセス制御（基本アクセス制御）.....25
6.1.18 FDP_ACC.1p サブセットアクセス制御（鍵共有利用アクセス制御）.....25
6.1.19 FDP_ACF.1a セキュリティ属性によるアクセス制御（発行処理）.....26
6.1.20 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）.....26
6.1.21 FDP_ACF.1p セキュリティ属性によるアクセス制御（鍵共有利用アクセス制御）.....27
6.1.22 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.....27
6.1.23 FDP_UCT.1b 基本データ交換機密性（基本アクセス制御）.....28
6.1.24 FDP_UCT.1p 基本データ交換機密性（鍵共有利用アクセス制御）.....28
6.1.25 FDP_UIT.1b 基本データ交換完全性（基本アクセス制御）.....28
6.1.26 FDP_UIT.1p 基本データ交換完全性（鍵共有利用アクセス制御）.....29
6.1.27 FIA_AFL.1a 認証失敗時の取り扱い（能動認証情報アクセス鍵）.....29
6.1.28 FIA_AFL.1d 認証失敗時の取り扱い（輸送鍵）.....29
6.1.29 FIA_AFL.1r 認証失敗時の取り扱い（読出し鍵）.....30

6.1.30 FIA_UAU.1 認証のタイミング 30
6.1.31 FIA_UAU.4 単一使用認証メカニズム 30
6.1.32 FIA_UAU.5 複数の認証メカニズム 30
6.1.33 FIA_UID.1 識別のタイミング 31
6.1.34 FMT_MOF.1 セキュリティ機能のふるまいの管理 31
6.1.35 FMT_MTD.1 TSF データの管理 31
6.1.36 FMT_SMF.1 管理機能の特定 32
6.1.37 FMT_SMR.1 セキュリティの役割 32
6.1.38 FPT_PHP.3 物理的攻撃への抵抗 32
6.1.39 FTP_ITC.1 TSF 間高信頼チャネル 32
6.2 セキュリティ保証要件 33
6.3 セキュリティ要件根拠 34
6.3.1 セキュリティ機能要件根拠 34
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 34
6.3.1.2 対応関係の根拠説明 35
6.3.1.3 セキュリティ機能要件の依存性 37
6.3.2 セキュリティ保証要件根拠 40
7. 用語 41
7.1 CC 関連 41
7.2 IC 旅券関連 41
8. 参照 43

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 －SAC 対応（BAC+PACE）及び能動認証対応 －

版数: 第 2.10 版

発行: 2022 年 1 月 24 日

作成者: JBMIA

発行者: 外務省領事局旅券課

登録: JISEC C0738

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交付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。国際連合の専門機関の一つである国際民間航空機関(ICAO)が旅券冊子に関わる仕様書を作成している。現在の旅券には、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込まれている。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 は旅券冊子に綴じ込まれる。旅券保持者の出入国において、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。旅券冊子の旅券ページ(身分事項ページ)に印刷された MRZ(機械可読領域)を除く情報の内、出入国審査に必要な情報が符号化されて光学

文字を使用して MRZ に印刷され、端末装置の光学文字読取り装置で読取られる。これらの情報はデジタル化される顔画像も含む他のデジタル化された情報と共に TOE である IC チップ内に格納される。このデジタルデータ[1]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出される。

TOE には端末装置と非接触通信を行うためのアンテナが接続される。TOE は、端末装置からの無線給電を利用して動作する。

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、[Doc 9303] Part11 が定める基本アクセス制御、鍵共有利用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。

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(旅券交付後の基本アクセス制御の動作禁止)
- 書込み禁止機能(旅券交付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。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)、アンテナとの接続
- フェーズ 3(個人情報設定): 旅券冊子作製、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

[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、ICAO 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。

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、TOE 製造者により 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。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 チップシリアル番号が書込まれる。IC チップ内部回路の機能テストは、IC チップ単体で実施される。その後は、アンテナと接続され、非接触通信インタフェースだけが利用可能となる。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。ここで対象となる TOE の処理とは、発行時の TOE 内ファイルの書込み、読出し、輸送鍵の更新、及び基本アクセス制御機能の無効化である。

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込まれる。この情報とは、旅券保持者の個人情報(氏名や生年月日など)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交付される。

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後のフェーズである。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、旅券保持者の身分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、正規の手続きを実施できる端末装置から読出される以外、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 外に読出されることはない。これらTOE 内の情報は、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。

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 バージョン 3.1(JISEC 公開の日本語版)に適合する。

- パート 1:
  概説と一般モデル 2017 年 4 月 バージョン 3.1 改訂第 5 版 [翻訳第 1.0 版]
  CCMB-2017-04-001
- パート 2:
  セキュリティ機能コンポーネント 2017 年 4 月 バージョン 3.1 改訂第 5 版 [翻訳第 1.0 版]
  CCMB-2017-04-002
- パート 3:
  セキュリティ保証コンポーネント 2017 年 4 月 バージョン 3.1 改訂第 5 版 [翻訳第 1.0 版]
  CCMB-2017-04-003
- CC パート 2 に対する適合: CCパート 2 拡張
- CCパート 3 に対する適合: CCパート 3 適合

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 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ため、適合根拠は記述しない。

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ければならない。

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

TOE を組込んだ旅券冊子交付後の運用環境において、旅券冊子の MRZ データを読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)を読出そうとするかもしれない。また、同インタフェース経由で、TOE 内ファイルへの書込みを試みるかもしれない。

［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取ったり、あるいは MRZ の印刷データを光学的に読取ることができる。これらの読取りを 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)の読出しや各ファイルへの書込みを試みる攻撃である。

T.Communication_Attack

TOEを組込んだ旅券冊子交付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 3-3]　攻撃者が旅券冊子に物理的にアクセスすることが可能な場合、MRZデータを知ることでICチップに格納されたデータを読出すことが可能となる。従って、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。

T.Physical_Attack

TOEを組込んだ旅券冊子交付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、無効化された基本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 3-4]　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)を読出したり、TOE内の情報を書換えたり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、内部回路をプロービングなどの方法で操作することにより情報を収集・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を組込んだ旅券冊子交付後の運用環境において、TOEは、[Doc 9303] 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、本PP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 を組込んだ旅券冊子交付後の運用環境において、TOE は、[Doc 9303] 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、本 PP に記載のないものは、その扱いを規定しない。

P.Authority

旅券発行当局の方針に従って、旅券発行当局の管理下にある TOE は、表 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認証に成功した者)だけに TOE 内部情報へのアクセスを許可する。

表 1 旅券発行当局による TOE 内部情報アクセス制御

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
読出し鍵による認証成功	EF.DG13*2	読出し	IC チップシリアル番号(TOE 製造者記入済み)
輸送鍵による認証成功	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	読出し及び書込み	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		共通情報
	EF.SOD		[Doc 9303] 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による認証成功	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、TOE 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

のないファイルの読出しや書込みは禁止される。(TOE を組込んだ旅券冊子が旅券保持者へ交付された後の、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><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 TOE 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。

[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

旅券発行当局の方針に従って、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 1 に示される。

P.Disable_BAC

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 3-6] 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。

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、旅券保持者へ交付されるまでの間、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)の真正性は、受入国の旅券審査当局が検証できる。

A.BAC_Keys

基本アクセス制御に使用する基本アクセス鍵が十分な暗号強度を持つよう、その元になるMRZデータには強化基本の攻撃に耐えられるような十分なエントロピーが含まれているものとする。

4. セキュリティ対策方針

3 章に示したセキュリティ課題に対して、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、[Doc 9303] Part11 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)の TOE 外への読出しを禁止しなくてはならない。また、旅券冊子交付後の運用環境においては、同インタフェース経由での TOE 内ファイルへの書込みを禁止しなくてはならない。

O.Physical_Attack

TOE は、物理的手段による攻撃によって、TOE 内の機密情報(能動認証用秘密鍵)が暴露されたり、セキュリティに関わる情報が改ざんされたりすること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、旅券冊子交付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、端末からの要求に応じて[Doc 9303] Part11 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に使用されなければならない。端末装置が本 TOE から読出す情報は、同規定に含まれるファイルのうち、EF.DG1、EF.DG2、EF.DG13、EF.DG14、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が正規のセキュアメッセージングを適用した読出しを要求した場合にのみ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。

O.PACE

本セキュリティ対策方針は、旅券冊子交付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、端末からの要求に応じて[Doc 9303] Part11 に規定される鍵共有利用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に使用されなければならない。端末装置が本 TOE から読出す情報は、同規定に含まれるファイルのうち、EF.DG1、EF.DG2、EF.DG13、EF.DG14、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。

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 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(旅券発行当局管理下においては権限を持つ職員、旅券交付後は端末装置)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 が旅券保持者へ交付される前に、旅券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 1 に示される。O.Data_Lock が実施されたのちは、O.BAC または O.PACE に記載された TOE へのアクセスだけが許可される。

O.Disable_BAC

基本アクセス制御機能を有する TOE は、当該機能によるアクセス許諾を無効化するための手続きを提供しなければならない。このセキュリティ対策方針は、旅券発行当局の許可された利用者により当該手続きを実行する際に適用される。

[注釈 4-1]　　基本アクセス制御機能の無効化は、TOE が旅券保持者へ交付された後の運用環境では実行できないため注意が必要である。

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。

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保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、[Doc 9303] Part12 に準拠した PKI 環境を構築しなければならない。

OE.BAC_Keys

旅券発行当局は、基本アクセス鍵が十分な暗号強度を持つよう、その元になる MRZ データが強化基本の攻撃に耐えられるような十分なエントロピーを含むようにしなければならない。

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 2 に示す。ここに示すとおり、すべてのセキュリティ対策方針は、一つ(以上)のセキュリティ課題定義の項目にさかのぼることができる。

表 2 セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ対策	O.AA	O.Logical_Attack	O.Physical_Attack	O.BAC	O.PACE	O.Authority	O.Data_Lock	O.Disable_BAC	OE.Administrative_Env	OE.PKI	OE.BAC_Keys

セキュリティ課題定義											
T.Copy	x										
T.Logical _Attack		x									
T.Communication_Attack				x	x						
T.Physical _Attack			x								
P.BAC				x							
P.PACE					x						
P.Authority						x					
P.Data_Lock							x				
P.Disable_BAC								x			
A.Administrative_Env									x		
A.PKI										x	
A.BAC_Keys											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 チップ自身の真正性を証明できる能動認証を実現する。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。また、旅券冊子交付後の運用環境においては、同インタフェース経由での TOE 内ファイルへの書込みが禁止される。このため、脅威 T.Logical_Attack が除去される。

T.Communication_Attack

TOE のセキュリティ対策方針 O.BAC、O.PACE によって、端末装置との間の通信にはセキュアな通信路が用いられる。これによって、T.Communication_Attack の通信データ暴露及び改ざんに対する脅威は実用上十分な程度に軽減される。

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)を暴露したり、セキュリティに関わる情報を改ざん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、[Doc 9303] Part11 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.PACE

TOE のセキュリティ対策方針 O.PACE は、[Doc 9303] Part11 に規定される鍵共有利用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 の内部情報を読出せるようにする。O.PACE は、P.PACE 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.PACE 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.Disable_BAC

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

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。

A.BAC_Keys

環境のセキュリティ対策方針 OE.BAC_Keys は、前提条件 A.BAC_Keys 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

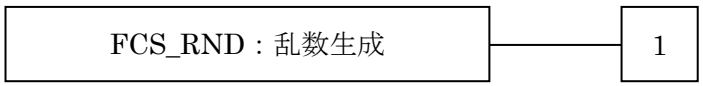
本 PP では、以下の拡張コンポーネントを定義する。

5.1 FCS_RND 乱数生成

ファミリのふるまい

このファミリは、暗号目的での使用が意図された乱数生成に対する品質の要件を定義する。

コンポーネントのレベル付け



FCS_RND.1 乱数生成は、その乱数が定義された品質基準に合致することを要求する。

管理: FCS_RND.1

予見される管理アクティビティはない。

監査: FCS_RND.1

予見される監査対象事象はない。

FCS_RND.1 乱数に対する品質基準

下位階層: なし

依存性: なし

FCS_RND.1.1 TSF は、[割付：定義された品質基準]に合致した乱数生成メカニズムを提供しなければならない。

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 のリストを表 3 に示す。

表 3 SFR リスト

章番号	識別名	
6.1.1	FCS_CKM.1b	暗号鍵生成(基本アクセス制御)
6.1.2	FCS_CKM.1p	暗号鍵生成(鍵共有利用アクセス制御 セッション鍵)
6.1.3	FCS_CKM.1e	暗号鍵生成(鍵共有利用アクセス制御 一時的鍵ペア)
6.1.4	FCS_CKM.4	暗号鍵破棄
6.1.5	FCS_COP.1a	暗号操作(能動認証 署名生成)
6.1.6	FCS_COP.1h	暗号操作(能動認証 ハッシュ関数)
6.1.7	FCS_COP.1hb	暗号操作(基本アクセス制御 ハッシュ関数)
6.1.8	FCS_COP.1mb	暗号操作(基本アクセス制御 相互認証)
6.1.9	FCS_COP.1sb	暗号操作(基本アクセス制御 セキュアメッセージング)
6.1.10	FCS_COP.1n	暗号操作(ナンス暗号化)
6.1.11	FCS_COP.1e	暗号操作(鍵共有)
6.1.12	FCS_COP.1hp	暗号操作(鍵共有利用アクセス制御 ハッシュ関数)
6.1.13	FCS_COP.1mp	暗号操作(鍵共有利用アクセス制御 相互認証)
6.1.14	FCS_COP.1sp	暗号操作(鍵共有利用アクセス制御 セキュアメッセージング)
6.1.15	FCS_RND.1	乱数に対する品質基準
6.1.16	FDP_ACC.1a	サブセットアクセス制御(発行処理)
6.1.17	FDP_ACC.1b	サブセットアクセス制御(基本アクセス制御)
6.1.18	FDP_ACC.1p	サブセットアクセス制御(鍵共有利用アクセス制御)
6.1.19	FDP_ACF.1a	セキュリティ属性によるアクセス制御(発行処理)
6.1.20	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)
6.1.21	FDP_ACF.1p	セキュリティ属性によるアクセス制御(鍵共有利用アクセス制御)
6.1.22	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
6.1.23	FDP_UCT.1b	基本データ交換機密性(基本アクセス制御)
6.1.24	FDP_UCT.1p	基本データ交換機密性(鍵共有利用アクセス制御)
6.1.25	FDP_UIT.1b	基本データ交換完全性(基本アクセス制御)
6.1.26	FDP_UIT.1p	基本データ交換完全性(鍵共有利用アクセス制御)
6.1.27	FIA_AFL.1a	認証失敗時の取り扱い(能動認証情報アクセス鍵)
6.1.28	FIA_AFL.1d	認証失敗時の取り扱い(輸送鍵)
6.1.29	FIA_AFL.1r	認証失敗時の取り扱い(読出し鍵)

6.1.30	FIA_UAU.1	認証のタイミング
6.1.31	FIA_UAU.4	単一認証メカニズム
6.1.32	FIA_UAU.5	複数の認証メカニズム
6.1.33	FIA_UID.1	識別のタイミング
6.1.34	FMT_MOF.1	セキュリティ機能のふるまいの管理
6.1.35	FMT_MTD.1	TSF データの管理
6.1.36	FMT_SMF.1	管理機能の特定
6.1.37	FMT_SMR.1	セキュリティの役割
6.1.38	FPT_PHP.3	物理的攻撃への抵抗
6.1.39	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 の目的を示す括弧付けの短い説明「例:(能動認証)」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。
- 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、一部の操作が未了の場合、その箇所を[割付: ×××(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.1b 暗号鍵生成(基本アクセス制御)

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.1.1b TSF は、以下の[割付:*[Doc 9303] Part11 で特定される基本アクセス制御におけるセッション鍵生成方式の標準*]に合致する、指定された暗号鍵生成アルゴリズム[割付:*[Doc 9303] Part11 で定められる基本アクセス制御における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:*112 ビット*]に従って、暗号鍵を生成しなければならない。

6.1.2 FCS_CKM.1p 暗号鍵生成(鍵共有利用アクセス制御 セッション鍵)

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.1.1p TSF は、以下の[割付:*[Doc 9303] Part11 及び[TR-03111]で特定される鍵共有利用アクセス制御におけるセッション鍵生成方式の標準*]に合致する、指定された暗号鍵生成アルゴリズム[割付:*[Doc 9303] Part11 及び[TR-03111]で定められる鍵共有利用アクセス制御における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: *256 ビット*]に従って、暗号鍵を生成しなければならない。

6.1.3 FCS_CKM.1e 暗号鍵生成(鍵共有利用アクセス制御 一時的鍵ペア)

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.1.1e TSF は、以下の[割付:*[TR-03111]で特定される鍵ペア生成方式の標準*]に合致する、指定された暗号鍵生成アルゴリズム[割付:*Elliptic Curve Key Pair Generation*]と指定された暗号鍵長[割付: *384 ビット*]に従って、暗号鍵を生成しなければならない。

6.1.4 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、新規暗号鍵データによる廃棄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。

[注釈 6-1] [Doc 9303] Part11 9.8.3 Session Termination の要求事項を満たすため、ST 作者は必要に応じて本要件を繰り返し定義しなければならない。

6.1.5 FCS_.COP.1a 暗号操作(能動認証 署名生成)

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: *[TR-03111]で特定されるデジタル署名方式の標準*]に合致する、特定された暗号アルゴリズム[割付: *ECDSA*]と暗号鍵長[割付:*384 ビット、512 ビット及び 521 ビット*]に従って、[割付: *能動認証用データに対するデジタル署名生成*]を実行しなければならない。

[注釈 6-2] 本要件の鍵長と FCS_COP.1h のハッシュアルゴリズムは、384 ビットと SHA-384、あるいは 512 ビット又は 521 ビットと SHA-512 の組合わせのみが許容される。

[注釈 6-3] 本要件の鍵長 384 ビット及び 521 ビットは NIST 曲線を、512 ビットは Brainpool 曲線の使用を想定している。

6.1.6 FCS_.COP.1h 暗号操作（能動認証 ハッシュ関数）

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.1.1h TSF は、[割付: *[TR-03111]で特定されるデジタル署名方式の標準*]に合致する、特定された暗号アルゴリズム[割付: *SHA-384 及び SHA-512*]と暗号鍵長[割付:*なし*]に従って、[割付: *能動認証用データの生成*]を実行しなければならない。

6.1.7 FCS_.COP.1hb 暗号操作（基本アクセス制御 ハッシュ関数）

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.1.1hbTSF は、[割付: *[Doc 9303] Part11 で特定される基本アクセス制御におけるセッション鍵生成方式の標準*]に合致する、特定された暗号アルゴリズム[割付: *SHA-1*]と暗号鍵長[割付:*なし*]に従って、[割付:*基本アクセス制御用セッション鍵の生成*]を実行しなければならない。

6.1.8 FCS_.COP.1mb 暗号操作（基本アクセス制御 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.1.1mb　TSF は、[割付:*[Doc 9303] Part11 で特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:*表 4 に示す暗号アルゴリズム*]と暗号鍵長[割付:*表 4 に示す暗号鍵長*]に従って、[割付:*表 4 に示す暗号操作*]を実行しなければならない。

表 4 相互認証とセキュアメッセージングの暗号方式（基本アクセス制御）

暗号アルゴリズム	*暗号鍵長*	*暗号操作*
CBC モード Single DES	*56 ビット*	*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	*112 ビット*	*認証用データの暗号化・復号*
		認証子生成・検証（メッセージの最終ブロック）

[注釈 6-4]　表 4 に記載の認証子の生成方法は ISO/IEC 9797-1 MAC Algorithm3 に規定された方式と等価である。

6.1.9　FCS_COP.1sb　暗号操作（基本アクセス制御 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.1.1sb　TSF は、[割付：*[Doc 9303] Part11 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標準*]に合致する、特定された暗号アルゴリズム[割付：*表 4 に示す暗号アルゴリズム*]と暗号鍵長[割付：*表 4 に示す暗号鍵長*]に従って、[割付：*表 4 に示す暗号操作*]を実行しなければならない。

[注釈 6-5]　セキュアメッセージングの適用可否はコマンドの種類により異なるため、すべてのコマンド・レスポンスに対してデータの暗号化と認証子の付与がなされるわけではない。

6.1.10　FCS_.COP.1n　暗号操作（ナンス暗号化）

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.1.1n TSF は、[割付：*[Doc 9303] Part11 で特定される鍵共有利用アクセス制御手順の標準*]に合致する、特定された暗号アルゴリズム[割付：*AES-CBC*]と暗号鍵長[割付： *256 ビット*]に従って、[割付：*ナンスの暗号化*]を実行しなければならない。

6.1.11 FCS_COP.1e 暗号操作（鍵共有）

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.1.1e TSF は、[割付：*[Doc 9303] Part11 で特定される鍵共有利用アクセス制御手順の標準*]に合致する、特定された暗号アルゴリズム[割付：*ECDH*]と暗号鍵長[割付： *384 ビット*]に従って、[割付：*鍵共有*]を実行しなければならない。

6.1.12 FCS_.COP.1hp 暗号操作（鍵共有利用アクセス制御 ハッシュ関数）

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.1.1hpTSF は、[割付: *[Doc 9303] Part11 で特定される鍵共有利用アクセス制御におけるセッション鍵生成方式の標準*]に合致する、特定された暗号アルゴリズム[割付: *SHA-256*]と暗号鍵長[割付:*なし*]に従って、[割付:*鍵共有利用アクセス制御用セッション鍵の生成*]を実行しなければならない。

6.1.13 FCS_COP.1mp 暗号操作（鍵共有利用アクセス制御 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.1.1mp TSF は、[割付：*[Doc 9303] Part11 で特定される鍵共有利用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：*AES-CMAC*]と暗号鍵長[割付： *256 ビット*]に従って、[割付：*認証トークンの生成及び検証*]を実行しなければならない。

6.1.14 FCS_COP.1sp　　暗号操作（鍵共有利用アクセス制御 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.1.1sp　TSF は、[割付: *[Doc 9303]で特定される鍵共有利用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 5 に示す暗号アルゴリズム*]と暗号鍵長[割付: *表 5 に示す暗号鍵長*]に従って、[割付: *表 5 に示す暗号操作*]を実行しなければならない。

表 5 セキュアメッセージングの暗号方式（鍵共有利用アクセス制御）

暗号アルゴリズム	*暗号鍵長*	*暗号操作*
CBC モード AES	*256 ビット*	*メッセージの暗号化・復号*
AES-CMAC	*256 ビット*	*認証子の生成・検証*

[注釈 6-6]　セキュアメッセージングの適用可否はコマンドの種類により異なるため、すべてのコマンド・レスポンスに対してデータの暗号化と認証子の付与がなされるわけではない。

6.1.15 FCS_RND.1　　乱数に対する品質基準

下位階層: なし

依存性: なし

FCS_RND.1.1　TSF は、[割付: *定義された品質基準*]に合致した乱数生成メカニズムを提供しなければならない。

[注釈 6-7]　乱数に対する品質基準としては、BSI AIS20、BSI AIS31、NIST SP800-90、ISO/IEC 18031 等の文書が参考となる。

[注釈 6-8]　FCS_COP.1a で規定される ECDSA 演算を上位ソフトウェアで実装する場合、演算過程で生成される乱数の品質に対して ST 作者は本要件を繰り返し定義しなければならない。

6.1.16 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 1 に示すファイル〉、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。

6.1.17 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.1.1bTSF 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.DG14、EF.DG15、EF.COM、EF.SOD、基本アクセス鍵ファイル、パスワード鍵ファイル、輸送鍵ファイル、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 6-9] 日本国以外の調達者が本 PP を利用する場合、[Doc 9303]に規定された上記以外のファイルの追加が必要になることがある。PP/ST 作成者がこれらのファイルをオブジェクトに追加しても、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。ただし、オブジェクトとその操作を PP/ST に追加する場合は、TOE 調達者との合意が必要であろう。

[注釈 6-10] 基本アクセス制御 SFP は基本アクセス制御に基づく相互認証に成功した後に適用されるアクセス制御ポリシである。

6.1.18 FDP_ACC.1p サブセットアクセス制御（鍵共有利用アクセス制御）

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.1.1p 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.DG.2、EF.DG13、EF.DG14、EF.DG15、EF.COM、EF.SOD、基本アクセス鍵ファイル、パスワード鍵ファイル、輸送鍵ファイル、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: *鍵共有利用アクセス制御 SFP*]を実施しなければならない。

[注釈 6-11] [Doc 9303]には、上記以外のファイルも規定される。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。

[注釈 6-12]　鍵共有利用アクセス制御 SFP は鍵共有利用アクセス制御に基づく相互認証に成功した後に適用されるアクセス制御ポリシである。

6.1.19 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 1 に示すファイル〉、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 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 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: *組織のセキュリティ方針 P.Authority の表 1 に記載のないファイルアクセスは禁止される*]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。

6.1.20 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.DG14、EF.DG15、EF.COM、EF.SOD、基本アクセス鍵ファイル、パスワード鍵ファイル、輸送鍵ファイル、秘密鍵ファイル〉、及び、SFP 関連セキュリティ属性〈相互認証に基づく端末装置の認証状況〉*]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: *端末装置の認証状況*

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輸送鍵ファイル、基本アクセス鍵ファイル、パスワード鍵ファイル、及び秘密鍵ファイルへのデータ書込みまたはデータ読出しは禁止される*]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。

6.1.21 FDP_ACF.1p セキュリティ属性によるアクセス制御(鍵共有利用アクセス制御)

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.1.1p 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.DG14、EF.DG15、EF.COM、EF.SOD、基本アクセス鍵ファイル、パスワード鍵ファイル、輸送鍵ファイル、秘密鍵ファイル>、及び、SFP 関連セキュリティ属性<相互認証に基づく端末装置の認証状況>*]に基づいて、オブジェクトに対して、[割付: *鍵共有利用アクセス制御 SFP*]を実施しなければならない。

FDP_ACF.1.2p 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: *端末装置の認証状況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.1.3p 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.1.4p TSF は、次の追加規則、[割付:*サブジェクトによる輸送鍵ファイル、基本アクセス鍵ファイル、パスワード鍵ファイル及び秘密鍵ファイルへのデータ書込みまたはデータ読出しは禁止される*]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。

6.1.22 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: *なし*]の規則を実施しなければならない。

6.1.23　FDP_UCT.1b　　基本データ交換機密性（基本アクセス制御）

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.1.1bTSF 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。

6.1.24　FDP_UCT.1p　　基本データ交換機密性（鍵共有利用アクセス制御）

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.1.1pTSF 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: *鍵共有利用アクセス制御 SFP*]を実施しなければならない。

6.1.25　FDP_UIT.1b　　基本データ交換完全性（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、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.1.1b　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.1.2b　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。

6.1.26　FDP_UIT.1p　　基本データ交換完全性（鍵共有利用アクセス制御）

下位階層:　なし
依存性:　[FDP_ACC.1 サブセットアクセス制御、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.1.1p　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:*鍵共有利用アクセス制御 SFP*]を実施しなければならない。

FDP_UIT.1.2p　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。

6.1.27　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:1～15]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 6-13]　　管理者は、能動認証情報アクセス鍵の認証試行回数を設定する TOE 製造者における権限者を意味しており、旅券発行当局における権限者ではないことに注意が必要である。FIA_AFL.1.1d 及び FIA_AFL.1.1r に記載の管理者も同様である。

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況を「未認証」に固定*]をしなければならない。

6.1.28　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:1～15]内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2d　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況を「未認証」に固定)*]をしなければならない。

6.1.29　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:1～15]内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2r　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況を「未認証」に固定)*]をしなければならない。

6.1.30　FIA_UAU.1　　認証のタイミング

下位階層：　なし
依存性：　　FIA_UID.1　識別のタイミング

FIA_UAU.1.1　TSF　は、利用者が認証される前に利用者を代行して行われる[割付: *EF.CardAccess 及び EF.ATR/INFO の読出し*]を許可しなければならない。

FIA_UAU.1.2　TSF　は、その利用者を代行する他のすべての TSF　仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

6.1.31　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: *基本アクセス制御手順及び鍵共有利用アクセス制御手順による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。

6.1.32　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 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 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 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の認証により、旅券発行当局の権限者を認証する規則*
読出し鍵	*TOE に格納済みの読出し鍵の認証により、旅券発行当局の権限者を認証する規則*
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の認証により、旅券発行当局の権限者を認証する規則*
相互認証	*[Doc 9303]に定められた基本アクセス制御及び鍵共有利用アクセス制御における相互認証手順に基づいて端末装置を認証する規則*

6.1.33　FIA_UID.1　　識別のタイミング

下位階層:　なし
依存性:　なし

FIA_UID.1.1　TSF は、利用者が識別される前に利用者を代行して行われる[割付: *EF.CardAccess 及び EF.ATR/INFO の読出し*]を許可しなければならない。

FIA_UID.1.2　TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.34　FMT_MOF.1　　セキュリティ機能のふるまいの管理

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_MOF.1.1 TSF は、機能[割付: *基本アクセス制御*][選択: ~~*のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*~~]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。

6.1.35　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 6-14] 本要件は、フェーズ 3 において、TOE が旅券発行当局の拠点間で輸送される際の輸送鍵設定に関わるものである。

6.1.36 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: *輸送鍵の改変及び基本アクセス制御機能の停止*]

6.1.37 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。

6.1.38 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 を構成するソフトウェア*]への[割付: *スマートカードに関する CC サポート文書に規定される攻撃*]に抵抗しなければならない。

[注釈 6-15] サポート文書は TOE 評価時点で最新のものが適用される。PP 発行時点の同文書は”Application of Attack Potential to Smartcards and Similar Devices, Version 3.1, June 2020”である。

6.1.39 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 6-16]　[Doc 9303]に規定されるセキュアチャネルが確立された後は、端末装置と TOE 間の通信はセキュアチャネルのみで行わなければならない。

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 7 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 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 の上位コンポーネントである。

表 7 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 7 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_DEL.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.3

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 8 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 8 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	O.Logical_Attack	O.Physical_Attack	O.AA	O.BAC	O.PACE	O.Authority	O.Data_Lock	O.Disable_BAC
FCS_CKM.1b				x				
FCS_CKM.1p					x			
FCS_CKM.1e					x			
FCS_CKM.4			x	x	x			
FCS_COP.1a			x					
FCS_COP.1h			x					
FCS_COP.1hb				x				
FCS_COP.1mb				x				
FCS_COP.1sb				x				
FCS_COP.1n					x			
FCS_COP.1e					x			
FCS_COP.1hp					x			
FCS_COP.1mp					x			
FCS_COP.1sp					x			
FCS_RND.1					x			
FDP_ACC.1a			x			x		
FDP_ACC.1b	x			x				

FDP_ACC.1p	x				x			
FDP_ACF.1a			x			x		
FDP_ACF.1b	x			x				
FDP_ACF.1p	x				x			
FDP_ITC.1			x	x	x	x		
FDP_UCT.1b				x				
FDP_UCT.1p					x			
FDP_UIT.1b				x				
FDP_UIT.1p					x			
FIA_AFL.1a							x	
FIA_AFL.1d							x	
FIA_AFL.1r							x	
FIA_UAU.1				x	x	x		x
FIA_UAU.4				x	x			
FIA_UAU.5				x	x	x		x
FIA_UID.1				x	x	x		x
FMT_MOF.1								x
FMT_MTD.1						x		
FMT_SMF.1						x		x
FMT_SMR.1						x		x
FPT_PHP.3		x						
FTP_ITC.1				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、[Doc 9303] Part11 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及び FCS_COP.1h で規定されるハッシュ操作を行う。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。揮発性メモリ上の秘密鍵が破棄されることは FCS_CKM.4 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。旅券交付後の TOE に適用される FDP_ACC.1b、FDP_ACC.1p、FDP_ACF.1b 及び FDP_ACF.1p 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及び TOE 内ファイルへの書込みが拒否される。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たり、TOE 内のセキュリティに関わる情報を改ざん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.1、FIA_UAU.1 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[Doc 9303] Part11 に規定され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.1b、FDP_UIT.1b 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.1mb で相互認証手順に必要な暗号操作、FCS_COP.1sb 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.1b 及び FCS_COP.1hb 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出せるようにするため、FDP_ACC.1b、FDP_ACF.1b 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.PACE

FIA_UID.1、FIA_UAU.1 によって、識別・認証に成功した利用者に TOE のサービスが提供される。利用者認証には[Doc 9303] Part11 に規定される鍵共有利用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、鍵共有利用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.1p、FDP_UIT.1p 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、鍵共有利用アクセス制御手順で必要な暗号処理に関して、FCS_COP.1mp で相互認証手順に必要な暗号操作、FCS_COP.1sp 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 でパスワード鍵のインポート、FCS_CKM.1e で一時的鍵ペア生成、FCS_COP.1e で鍵共有、FCS_CKM.1p 及び FCS_COP.1hp でセッション鍵の生成、FCS_RND.1 でナンス等の乱数生成、FCS_COP.1n でナンスの暗号化、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出せるようにするため、FDP_ACC.1p、FDP_ACF.1p 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.PACE が十分に達成される。

O.Authority

旅券発行当局による発行時の TOE 内ファイルの書込み、読出し及び輸送鍵の更新において、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.1、FIA_UAU.1 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。これらの鍵の認証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及びパスワード鍵)、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が恒久的に禁止され、その結果これらの鍵による認証成功で得られる TOE 内部情報の読出し許諾と書込み許諾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。

O.Disable_BAC

旅券発行当局による発行時の基本アクセス制御機能の無効化において、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.1、FIA_UAU.1 が適用される。FIA_UAU.5 の輸送鍵の認証によって認証に成功した利用者には、基本アクセス制御機能の無効化が許可され、これらは FMT_MOF.1、FMT_SMF.1、FMT_SMR.1 で規定される。これらの SFR によって、O.Disable_BAC 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 9 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 9 SFR の依存性

SFR	依存性の要求	依存性への対応
FCS_CKM.1b	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4	FCS_COP.1sb 及び FCS_CKM.4 が対応し、依存性が満たされる。
FCS_CKM.1p	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4	FCS_COP.1sp、FCS_COP.1mp 及び FCS_CKM.4 が対応し、依存性が満たされる。
FCS_CKM.1e	[FCS_CKM.2 または FCS_COP.1]	FCS_COP.1e 及び FCS_CKM.4 が対応し、依存性が満たされる。

	FCS_CKM.4	
FCS_CKM.4	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]	FDP_ITC.1、FCS_CKM.1b、FCS_CKM.1e 及び FCS_CKM.1p が対応し、依存性が満たされる。ただし、FDP_ITC.1 は揮発性メモリ上の鍵のみが対応する。
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。揮発性メモリ上の鍵については FCS_CKM.4 が対応する。ただし、不揮発性メモリ上の鍵については改変・破棄が禁止されるため、FCS_CKM.4 は適用されない。
FCS_COP.1h	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	鍵が存在しないため、いずれの要件も適用されない。
FCS_COP.1hb	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	鍵が存在しないため、いずれの要件も適用されない。
FCS_COP.1mb	[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。揮発性メモリ上の鍵については FCS_CKM.4 が対応する。ただし、不揮発性メモリ上の鍵については改変・破棄が禁止されるため、FCS_CKM.4 は適用されない。
FCS_COP.1sb	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1b 及び FCS_CKM.4 が対応し、依存性が満たされる。
FCS_COP.1n	[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。揮発性メモリ上の鍵については FCS_CKM.4 が対応する。ただし、不揮発性メモリ上の鍵については改変・破棄が禁止されるため、FCS_CKM.4 は適用されない。
FCS_COP.1e	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1e 及び FCS_CKM.4 が対応し、依存性が満たされる。
FCS_COP.1hp	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1]	鍵が存在しないため、いずれの要件も適用されない。

	FCS_CKM.4	
FCS_COP.1mp	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p 及び FCS_CKM.4 が対応し、依存性が満たされる。
FCS_COP.1sp	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1p 及び FCS_CKM.4 が対応し、依存性が満たされる。
FCS_RND.1	なし	不要
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_ACC.1p	FDP_ACF.1	FDP_ACF.1p 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_ACF.1p	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1p 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] 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_UCT.1b	[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_UCT.1p	[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.1p が対応し、依存性が満たされる。
FDP_UIT.1b	[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。

	[FTP_ITC.1 または FTP_TRP.1]	
FDP_UIT.1p	[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.1p が対応し、依存性が満たされる。
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.1 が対応し、依存性が満たされる。
FIA_AFL.1d	FIA_UAU.1	FIA_UAU.1 が対応し、依存性が満たされる。
FIA_AFL.1r	FIA_UAU.1	FIA_UAU.1 が対応し、依存性が満たされる。
FIA_UAU.1	FIA_UID.1	FIA_UID.1 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.1	なし	不要
FMT_MOF.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_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.1 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 が使用される運用環境では、基本アクセス制御手順を使用する検査端末との通信が想定される。基本アクセス制御手順は、強化基本レベルの攻撃に対抗することを想定しており、そのレベルの攻撃に対抗できることを保証するため、TOE に対する脆弱性評定の保証要件は AVA_VAN.3 とする。

さらに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あり、軍事用途向けを想定した 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いため、表 7 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
SAC	Supplemental Access Control：相互認証とセキュアメッセージングによる IC 旅券アクセス制御で鍵共有利用アクセス制御と基本アクセス制御の二つの方式を装備し、いずれか一方の実行でアクセスが可能となる構成の名称。
TOE 製造者	IC 旅券冊子に埋め込むソフトウェアを搭載したハードウェアを開発・製造するチップベンダ。
旅券発行当局	旅券冊子を作製し、IC チップへ基本的データ（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）及び個人情報データを設定する。日本国においては国立印刷局が該当する。
能動認証	TOE に公開鍵暗号方式に基づく公開鍵・秘密鍵ペアを格納し、秘密鍵は秘匿する。TOE を認証しようとする外部装置に公開鍵を渡し、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。[Doc 9303]にて規定されている。
受動認証	TOE に格納する個人情報データに旅券発行者がデジタル署名を施し、受け入れ側は旅券発行側が用意した PKI システムを用いることによって、TOE から読出されたデータの真正性を確認できるようにする方式。[Doc 9303]にて規定されている。
読出し鍵	発行時に使用する鍵であり、製造フェーズで TOE に埋め込まれる。認証成功により許可される操作は表 1 を参照のこと。
輸送鍵	同上。
能動認証情報アクセス鍵	同上。

MRZ データ	IC 旅券の旅券ページ(身分事項ページ)の光学読取り文字が記載される特定領域で示される情報。
基本アクセス鍵ファイル	MRZ データから派生され、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。
パスワード鍵ファイル	MRZ データから派生され、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。
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。

8. 参照

[Doc 9303] ICAO Doc9303 Machine Readable Travel Documents Eighth Edition, 2021

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