IC 旅券用プロテクションプロファイル

2009/04/28

バージョン 1.0

【目次】

1. PP 概説

PP概説を以下に記述する。

1.1. PP 参照

本PPを識別するための参照情報は以下の通りである。

タイトル	:	IC 旅券用プロテクションプロファイル
バージョン	:	バージョン 1.0
作成者	:	
公開日	:	

1.2. PP 概要

本PPはIC旅券に組み込まれるICチップのプロテクションプロファイルである。ICチップのセキュリティ機能として、ICAO（International Civil Aviation Organization　国際民間航空機関）国際標準で必須とされている受動認証（Passive Authentication　：PKIスキームによるデータの改竄防止機能）とオプションである基本アクセス制御(Basic Access Control：盗聴防止機能)ならびに能動認証(Active Authentication：クローン防止機能)を対象にしている。

1.3. TOE 概要

TOE概要を以下に記述する。

1.3.1. IC 旅券システム

IC旅券を使用したシステムの概要を以下に記述する。

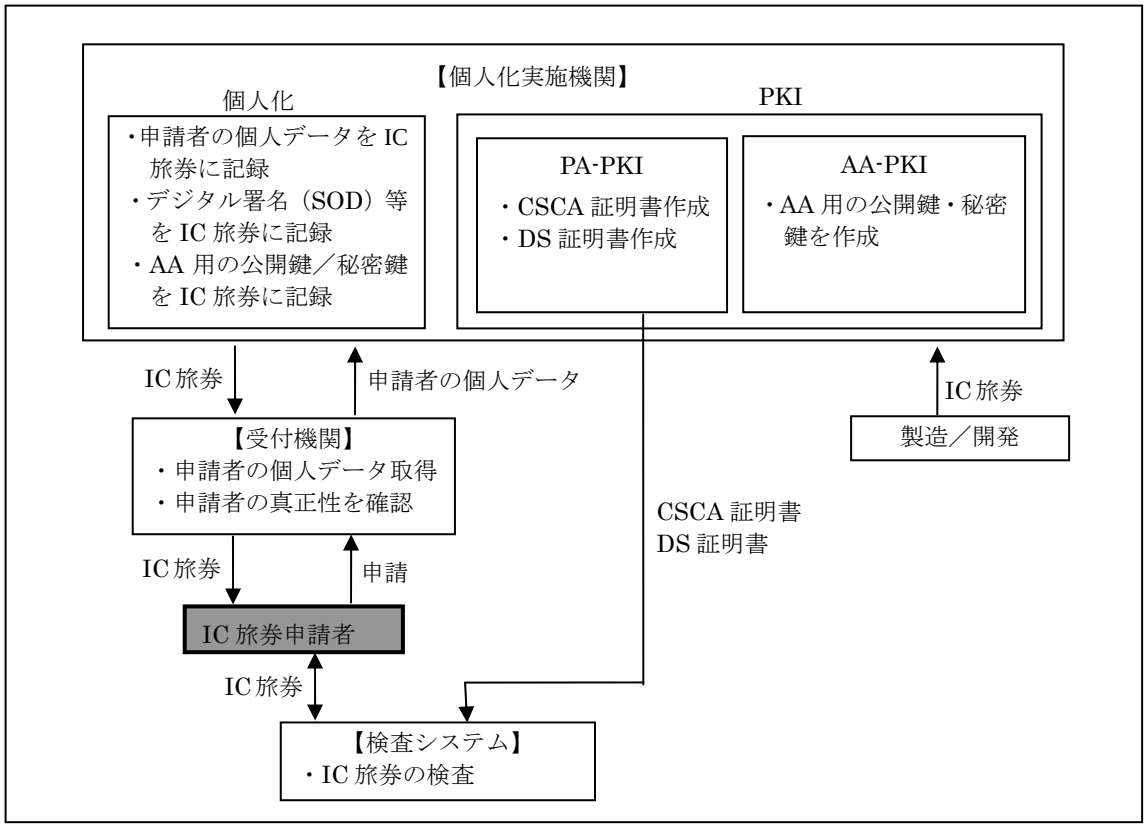

図 1 IC 旅券システムの概要

(1) IC旅券を保有しようとする者（以下、IC旅券申請者）は受付機関にIC旅券の申請を行い、IC旅券を入手する。

(2) 受付機関は申請者の個人データを収集するとともに関係機関に問い合わせるなどして当該データの真正性を確認する。

(3) 個人化実施機関はICチップに書き込むデータ（ドキュメントセキュリティオブジェクト（以下、SOD））に対する署名を作成し、当該署名とSODをチップに書き込む。
個人化実施機関は、さらに、TSFデータをセキュアメモリに書き込む。
IC旅券に記録されるデータについては「1.3.5.1**TOEの保護資産**」の「表 2　TOEの保護資産」に記述する。
IC旅券の開発／製造については「1.3.3.1　TOEのライフサイクル」に記述する。

(4) 次に、個人化実施機関が策定したIC旅券PKIシステムの認証局運用規定(CPS)にしたがって、CSCA証明書、DS証明書を発行し管理する。さらに能動認証のための公開鍵と秘密鍵を生成し、チップに書き込む。
IC旅券システムで使用する証明書を「表 1　IC旅券で使用する証明書」に示す。

表 1　IC 旅券で使用する証明書

目的	IC旅券PKIシステム	発行機関	証明書／鍵
個人データに対する	PA-PKI	CSCA	CSCA証明書

偽造・変造の検証	（受動認証）	（旅券発行国にあるルート認証局）	
		個人化実施機関	DS証明書

(5) 個人化実施機関はIC旅券を発行する。

アプリケーションノート：IC旅券システムは、TOEの運用環境によって異なる場合が考えられる。ここに示したIC旅券システムはその一例である。IC旅券システムについては、TOEの運用環境にあわせて記載されるべきである。「IC旅券用プロテクションプロファイル解説書」の「IC旅券システム」の項を参照

1.3.2. TOE 種別

TOEはIC旅券に組み込まれる非接触型ICチップである。IC旅券はICチップに情報を記録し情報の暗号化や盗聴対策などの安全対策を行うことにより旅券の偽変造を困難にしている。

TOEは、ICAO国際標準で必須とされている受動認証（Passive Authentication ：PKIスキームによるデータの改竄防止機能）、とオプションである基本アクセス制御(Basic Access Control：盗聴防止機能)に加え能動認証(Active Authentication：クローン防止機能)を搭載し、旅券の偽変造や、成りすましによる不正使用に対抗する。

1.3.3. TOE のライフサイクルと利用環境

TOEのライフサイクルと利用環境を以下に記述する。

1.3.3.1. TOE のライフサイクル

TOEのライフサイクルは、開発、製造、個人化、運用の4つのフェーズで構成される。

(1) フェーズ１：開発
- ICチップの開発者はICチップとICチップ専用のソフトウェアを開発する
- ソフトウェアの開発者はICチップのOSとIC旅券用のアプリケーションを開発する

(2) フェーズ２：製造
- ICチップの製造者はOSおよびアプリケーションをICチップのROMに書き込むとともに、ICチップの一意な識別を書き込んでICチップを製造する
- IC旅券製造者は個人データ等記録する領域をパスポートの標準規格であるICAOが規定するデータ構造 LDS（Logical Data Structure）でICチップのEEPROM上に作成する
- IC旅券製造者は個人化実施機関の識別／認証情報をEEPROMに書き込む
- IC旅券製造者はICチップをIC旅券（冊子）に組み込む

(3) フェーズ3：個人化

- 個人化実施機関はIC旅券に記録されている個人データに対して電子署名を行いSODを作成する
- 個人化実施機関は個人データ、認証データ（SODを含む）、TSFデータをICチップに書き込む

(4) フェーズ4：運用

- 検査システムはIC旅券とやり取りを行いIC旅券の検証と、IC旅券に格納された個人情報の検証を行う。

アプリケーションノート：TOEのライフサイクルはTOEの運用環境によって異なる場合が考えられる。ここに示したライフサイクルはその一例である。TOEのライフサイクルについては、TOEの運用環境にあわせて記載されるべきである。「IC旅券用プロテクションプロファイル解説書」の「TOEのライフサイクル」の項を参照

1.3.3.2. TOE の運用環境

TOEの個人化と運用のフェーズにおいてTOEとやり取りを行う外部エンティティならびに関係する主要なセキュリティ機能を以下に記述する。外部エンティティは個人化実施機関と検査システムである。

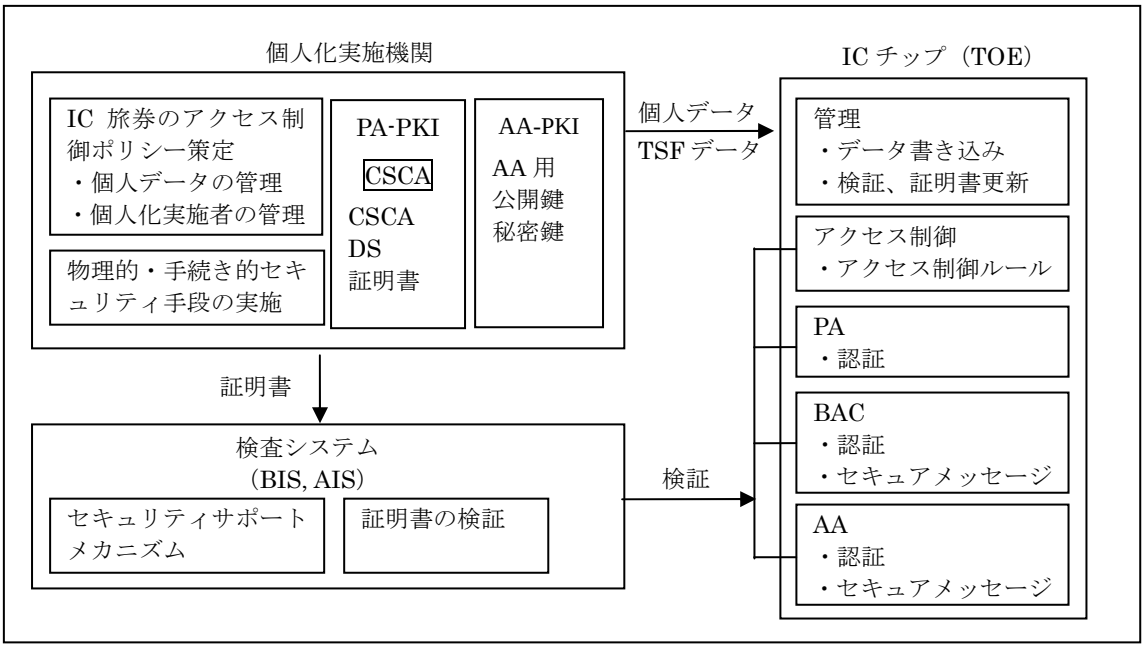

図 2 TOE の運用環境

アプリケーションノート：TOEの運用環境はその環境を構築する国等によって異なる場合

が考えられる。ここに示したその一例である。TOEの運用環境は、その実態あわせて記載されるべきである。「IC旅券用プロテクションプロファイル解説書」の「TOEの運用環境」の項を参照

1.3.4. TOE の物理的範囲

TOEの物理的範囲を「図 3　TOEの物理的範囲」に示す。

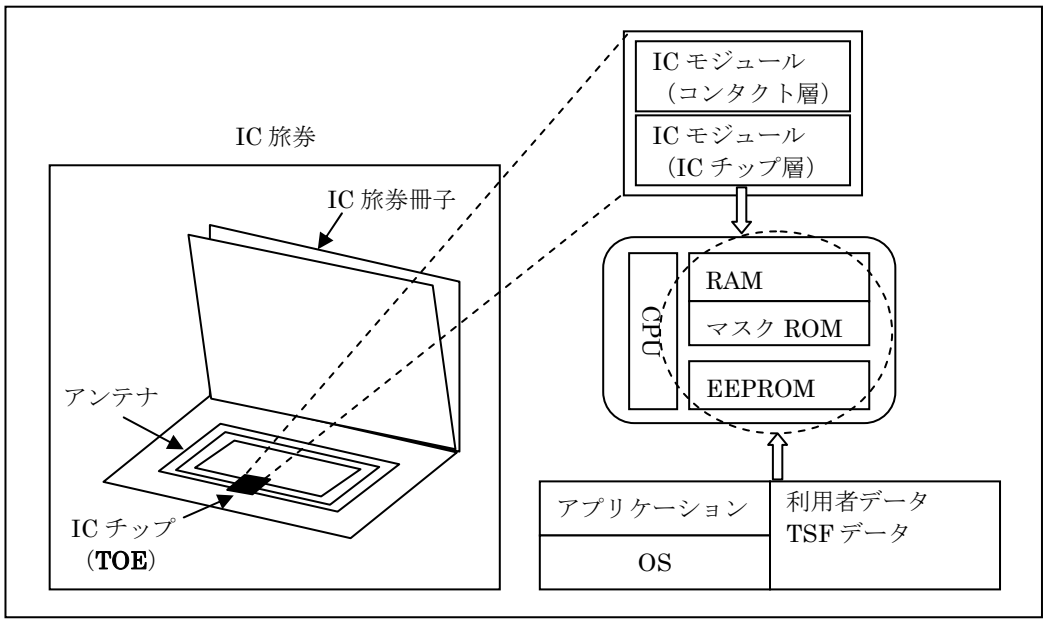

図 3　TOE の物理的範囲

TOEはIC旅券に組み込まれるICチップである。IC旅券はICチップならびにアンテナが埋め込まれた冊子であり、ICチップにはICモジュール、アプリケーション、OS、利用者データ、TSFデータが含まれている。ICモジュールは非接触のインタフェース、メモリ（RAM、ROM、EEPROM）、CPUなどから構成されている。

アプリケーションはICAOが規定するデータ構造 LDS（Logical Data Structure）で個人データを記録し処理するための機能を実装するものであり、合わせてセキュリティ機能も実装するものである。

アプリケーションノート：本PPはTOEの物理的範囲をICチップ全体としているが、本PPとは異なる範囲をTOEの物理的範囲としているPPも公開されている。「IC旅券用プロテクションプロファイル解説書」の「TOEの物理的範囲」の項を参照

1.3.5. TOE の論理的範囲

TOEはISO/IEC14443-4で定義されたトランスミッションプロトコルにしたがって、検査システムと通信する。TOEはICAOがドキュメントとAA(Active Authentication)仕様で規定しているセキュリティ機能を実装して、アクセス制御機能とセキュリティ管理機能を提供する。さらにTOEはTSFの自己保護機能を提供する。

アプリケーションノート：本PPは第1世代IC旅券PPで扱われている機能のうち、EACに代えてAA(Active Authentication)を実装する。第1世代IC旅券PPについては「IC旅券用プロテクションプロファイル解説書」の「PPの特徴」の項を参照

1.3.5.1. TOE の保護資産

TOEの保護資産を「表 2　TOEの保護資産」に示す。TOEはこの保護資産を保護するためのセキュリティ機能を提供する。

表 2　TOE の保護資産

カテゴリ			格納先
利用者データ	IC 旅券保有者の個人データ		EF.DG1、EF.DG2
	IC 旅券の検証用データ		EF.SOD
	LDS のバージョン情報、ファイルのインデックス情報など		EF.COM
TSF データ	旅券番号、冊子番号		EF.DG13
	AA 用公開鍵		EF.DG15
	BAC 認証鍵 （encryption key, MAC key）		セキュアメモリ (IEF:internal elementary file)
	AA 用秘密鍵		
	BAC セッション鍵	暗号化鍵 MAC 鍵	テンポラリメモリ

ICAOが規定するデータ構造 LDS（Logical Data Structure）とデータの関係を「表 3 LDSとデータ」に示す。

表 3　LDS とデータ

LDS	格納されるデータ
EF.COM	LDS のバージョン情報、ファイルのインデックス情報などの ICAO が規定するデータ

EF.DG1	氏名などの ICAO が規定するデータ
EF.DG2	デジタイズされた顔写真などの ICAO が規定するデータ
EF.DG15	AA 用公開鍵
EF.SOD	DS 署名、DS 証明書

1.3.5.2. TOE のセキュリティメカニズム

TOEはICAOが規定するBAC(Basic Access Control)とAA(Active Authentication)を提供する。さらに、BIS（BAC Inspection System）のためのSODも提供する。

(1) BAC

BACはIC旅券に記録されている個人データの通信時の機密性・完全性を保護するための機能である。この機能は認証機能（BAC manual authentication)、暗号通信に使用する鍵を配送する鍵配送機能（BAC key distribution)、暗号通信機能（BAC secure messaging）で構成されている。

BAC の概要を「図 4　BAC の仕組み」に示す。

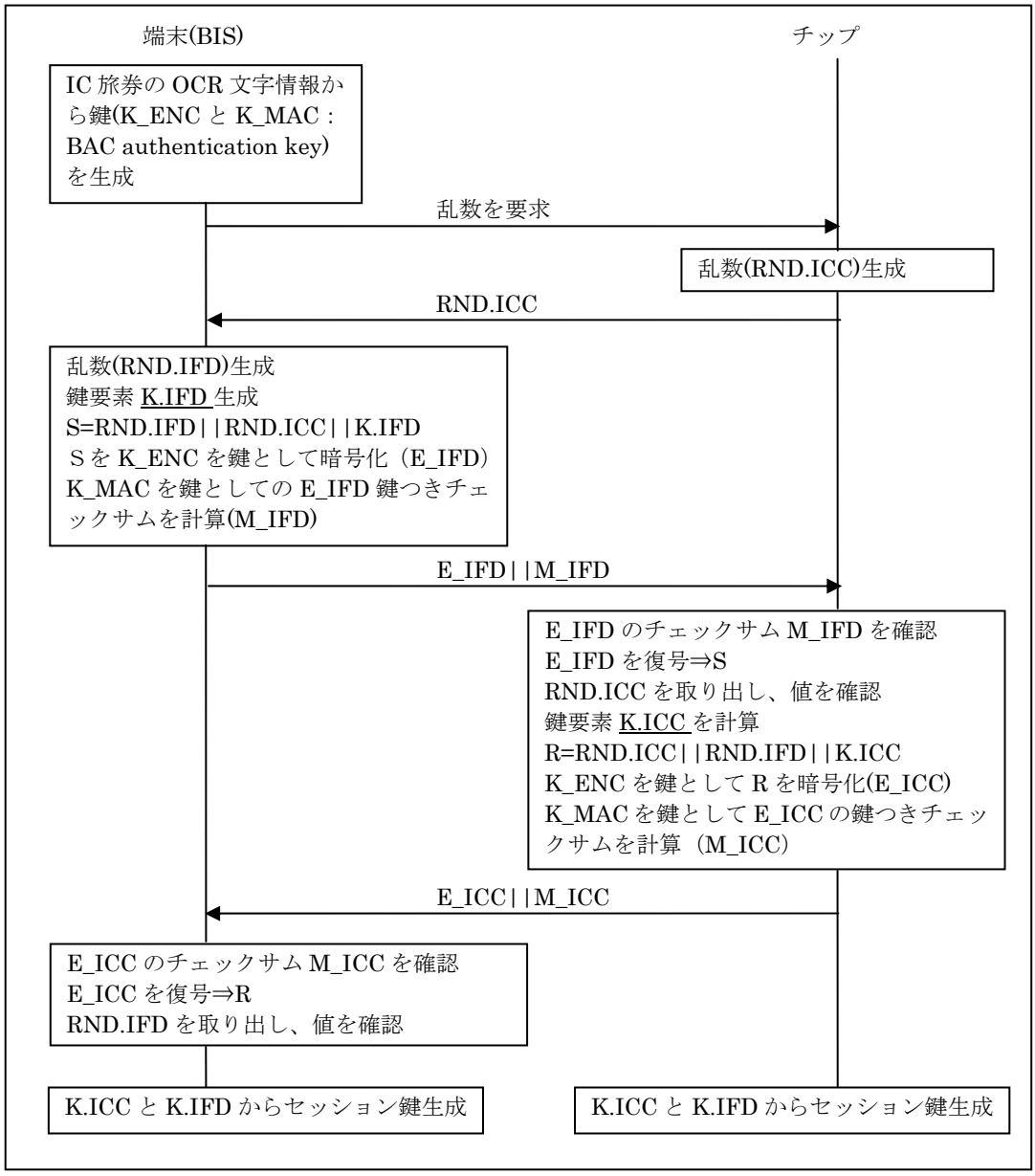

図 4　BAC の仕組み

アプリケーションノート：BACの詳細については「IC旅券用プロテクションプロファイル解説書」の「TOEのセキュリティメカニズム」の項を参照

(2) AA

AA(Active Authentication)は公開暗号方式に基づいたセキュリティ処理で、ICチップの読み出し可能領域に格納した公開鍵と、読出し不可領域に格納した秘密鍵の組み合わせによってICチップの正当性を検証する。

AAの概要を「図 5　AAの仕組み」に示す。

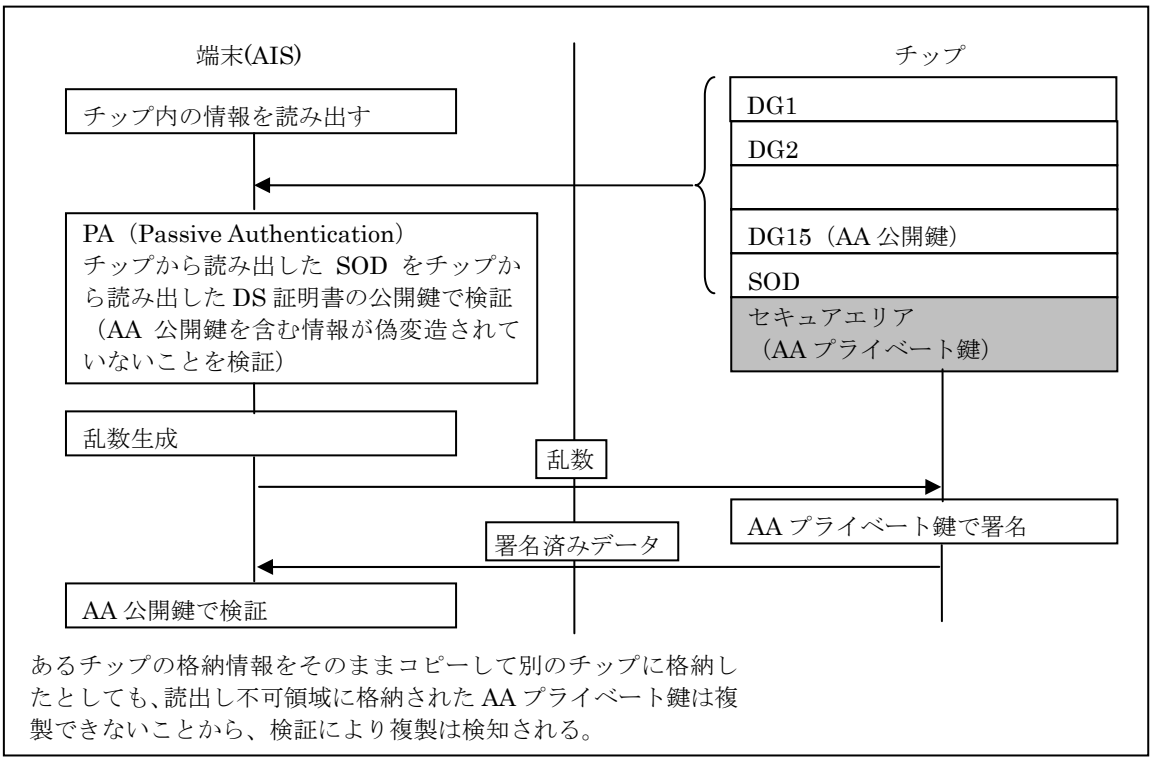

図 5　AA の仕組み

TOEのセキュリティメカニズムをまとめたものを「表 4　TOEのセキュリティメカニズム」に示す。

表 4　TOE のセキュリティメカニズム

メカニズム	内容	暗号	暗号鍵	TOE のセキュリティ機能
PA	データの検証	なし	なし	データが改竄されていないことを SOD を検証することによって確認する。
BAC	BAC Mutual authentication	TDES-CBC SHA MAC	BAC 認証鍵	検査システムがアクセス権限を持っているかどうかを復号や MAC(Massage Authentication Code)によって確認する。
	BAC 鍵配送	TDES-CBC SHA MAC	BAC セッション鍵	乱数を使用した TDES 用セッション鍵の生成と交換
	BAC 暗号通信	セキュアメッセージ	BAC セッション鍵	BAC セッション鍵による暗号化と MAC による検証
AA	署名	SHA RSA	AA 公開鍵 AA 秘密鍵	署名の検証による複製の検知

アプリケーションノート：BACの詳細については「IC旅券用プロテクションプロファイル解説書」の「TOEのセキュリティメカニズム」の項を参照

(3) アクセス制御

TOEはアクセス制御機能を提供する。この機能は、IC旅券の個人化および運用時に利用者のセキュリティ属性にしたがってアクセスを制御する機能である。

- TOEは認証された個人化担当者にのみデータの書き込み機能の使用を許可する。（個人化フェーズ）
- TOEは認証された個人化担当者のみに、利用者のセキュリティ属性の変更を許可する。（個人化フェーズ、運用フェーズ）

(4) その他

TOEは上記の機能のほか、以下の機能を有する。

- TSFを信頼できないサブジェクトによる物理的な攻撃から保護する機能
- バイパス防止
- ドメイン分離
- 自己テスト
- 障害発生時のセキュアな状態の維持
- TSFデータの完全性保護
- 観察不能性

2. 適合主張

適合主張を以下に記述する。

2.1. CC 適合主張

本PPおよびTOEのCC適合主張は、以下のとおりである。

STとTOEが適合を主張するCCのバージョン：

パート1： 概説と一般モデル 2007年3月 バージョン3.1 翻訳第1.2 版

パート2： セキュリティ機能コンポーネント 2008年3月 バージョン3.1 翻訳第2 .0 版

パート3： セキュリティ保証コンポーネント 2008年3月 バージョン3.1 翻訳第2 .0 版

CCパート2 に対するSTの適合： CCパート2 適合

CCパート3 に対するSTの適合： CCパート3 適合

2.2. PP 主張、パッケージ主張

PP主張およびパッケージ主張を以下に記述する。

2.2.1. PP 主張

本PPが適合しているPPはない。

本PPは、本PP を参照するST もしくはPP に対し、CCパート1の附属書D.3で定義される論証適合を要求する。

2.2.2. パッケージ主張

本PPはEAL4追加である。

追加保証コンポーネントは、ADV_IMP.2、ALC_CMC.5、ALC_DVS.2、AVA_VAN.5である。

3. セキュリティ課題定義

前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 前提条件

TOEの運用環境が満たすべき前提条件は以下のとおりである。

A. Personalization Agent

個人化担当者は以下のことを行う。

・IC 旅券申請者の正当性を確認する
・正しい BAC 認証鍵を記録する
・正しい DS 証明書を登録する
・正しい AA の公開鍵と秘密鍵を登録する
・TOE にプログラムを格納する場合は、TOE のセキュリティに影響を及ぼさないことを確認したうえでおこなう。

アプリケーションノート: 個人化担当者のおこなう作業はTOEの運用環境によって異なることが考えられる。また、プログラムの格納をおこなわないような運用環境も考えられる。この前提条件は運用環境の実態に合わせて記述されるべきである。「IC旅券用プロテクションプロファイル解説書」の「前提条件」の項を参照

A. Certificate Verification

BIS、AIS などの検査システムは TOE に記録されているデータの偽変造を検証するために PA の証明書の検証を行った後、SOD の検証を行う。

そのために DS 証明書と CRL を定期的に検査する。

アプリケーションノート：これは検査システムに求められる前提条件である。しかしながら検査システムの運用主体とTOEの運用主体は異なると考えられ、運用環境の実態に合わせて記述されるべきである。「IC旅券用プロテクションプロファイル解説書」の「前提条件」の項を参照

A. Inspection System

検査システムは ICAO が規定する以下のセキュリティメカニズムを実装する。
・PA
・BAC
・AA
検査システムはセッション終了時にBACセッション鍵などのセッション情報をセキュアに破棄する。
BAC と PA を実装している検査システム(BIS)においては、BAC 認証鍵を使用した BAC mutual authentication が成功した場合にのみ、データの読み込み権限が与えられる。
BAC セッション鍵を使用した暗号通信によって通信データの完全性と機密性が保護される。BIS は BAC の後に PA を実行し、SOD の検証を行う。これによりデータの偽変造を検知する。
AA 実装している検査システム(AIS)においては、BAC、PA を実行し、SOD の検証を行って AA の公開鍵が偽変造されていないことを確認したのちチャレンジレスポンスによって、チップのデータが複製でないことを確認する。

アプリケーションノート：これは検査システムに求められる前提条件である。しかしながら検査システムの運用主体とTOEの運用主体は異なると考えられ、この前提条件を設けないケースも考えられる。「IC旅券用プロテクションプロファイル解説書」の「前提条件」の項を参照

A. MRZ Entropy

BAC 認証鍵の種は十分なエントロピーを持つものとする。

アプリケーションノート：BAC認証鍵の種はパスポートに印刷されるOCR文字であるが、運用環境によっては、この前提条件を設けないケースも考えられる。「IC旅券用プロテクシ

ョンプロファイル解説書」の「前提条件」の項を参照

3.2. 脅威

前提条件で示されたTOEの意図する運用環境におけるTOEの保護資産に対する脅威を以下に示す。攻撃者は高い攻撃能力を有する。

3.2.1. 個人化フェーズにおける脅威

個人化フェーズにおいては、TOEにデータ等を格納するための管理用インタフェースが有効になっている。そのため、この管理用インタフェースを使用したデータの改竄や漏洩といった脅威が存在する。管理用インタフェースは、個人化が完了したのち、個人化担当者によって停止される。

T. Application Program Interference

攻撃者は管理用のインタフェースからチップに不正なプログラムをロードしてセキュリティ機能をバイパスしたり非活性化したりしてデータへのアクセスを試みるかもしれない。

T. TSF Data Modification

攻撃者は検査システムから、TOE の外部インタフェースにアクセスし、TOE に格納されている TSF データを改竄しようとするかも知れない。

3.2.2. 運用フェーズにおける BAC 関連の脅威

運用フェーズにおいて、BACに関係する脅威として以下のようなものが存在する。

T. BAC Authentication Key Disclose

攻撃者は TOE に格納されているデータを入手するために、BAC 認証鍵を取得しようとするかもしれない。

T. BAC Replay Attack

攻撃者は TOE と検査システムの間でやり取りされるデータを搾取し、リプレイ攻撃

を行うかも知れない。

T. Eavesdropping

攻撃者は TOE と検査システムの間でやり取りされるデータを盗聴し TOE に格納されているデータを入手しようとするかも知れない。

T. Forgery and Corruption of Personal Data

攻撃者は不正な検査システムを使用してTOEに格納されているデータを読み出そうとするかも知れない。

T. Skimming

攻撃者は不正な読み取り装置を使用してTOEに格納されているデータを読み出そうとするかも知れない。

3.2.3. 運用フェーズにおける IC チップへの脅威

運用フェーズにおいて、ICチップに直接関係する脅威として以下のようなものが存在する。

T. Malfunction

攻撃者は TOE にストレスを与えてセキュリティ機能をバイパスしたり、TOE に格納されている実行プログラムや TSF データを破壊するなどして、予期しない動作を引き起こそうとするかもしれない。

3.2.4. 運用フェーズにおけるその他の脅威

運用フェーズにおいて、その他の脅威として以下のようなものが存在する。

T. ePassport Reproduction

攻撃者は IC 旅券を偽造し、IC 旅券の保有者に成りすまそうとするかもしれない。

T. Leakage of Cryptographic Key Information

攻撃者は電力解析等により暗号鍵の解読を試みるかも知れない。

T. Residual Information

攻撃者は**一時的な記憶**に残る TSF データ（例えば BAC 認証鍵、BAC セッション鍵、AA 秘密鍵、その他）を悪用しようとするかも知れない。

T. Phys Tamper

IC チップに対するプローブ解析を試みるかもしれない。

3.3. 組織のセキュリティ方針

TOEを運用する組織において実現すべき組織のセキュリティ方針を以下に示す。

P. ePassport Access Control

個人化担当者と TOE は IC 旅券の利用者データ、TSF データを保護するため、「表 5 利用者データのアクセスポリシー」に示すアクセス制御ポリシーを構築しなければならない。

表 5 利用者データのアクセスポリシー

サブジェクト ＼ 利用者データ / 格納場所 / 属性		IC 旅券保有者の個人データ	IC 旅券の検証用データ	LDS の情報
		EF.DG1 EF.DG2	EF.SOD	EF.COM
BIS	BAC	Read	Read	Read
AIS	BAC	Read	Read	Read
	AA	Read	Read	Read
個人化担当	個人化担当	Read / Write	Read / Write	Read / Write

アプリケーションノート：アクセス制御ポリシーの設定についてはSTの開発者が決定すべきである。「IC旅券用プロテクションプロファイル解説書」の「組織のセキュリティ方針」の項を参照

P. International Compatibility

個人化担当者はIC旅券のセキュリティメカニズムと入国管理における検査システム

との整合性を保証しなければならない。

アプリケーションノート：個人化担当者が整合性を保証することが実態にそぐわない場合も考えられる。その場合は、この対策方針を定義しないことも考えられる。「IC旅券用プロテクションプロファイル解説書」の「組織のセキュリティ方針」の項を参照

P. PKI

IC 旅券の発行国は、PA-PKI の CPS に準拠した電子署名鍵、証明書の管理を行う。
また、IC 旅券の発行国は証明書の有効期限に関するポリシーに従い証明書を更新する。

アプリケーションノート：この対策方針を定義することが現実にそぐわない場合も考えられる。その場合は、この対策方針を定義しないことも考えられる。「IC旅券用プロテクションプロファイル解説書」の「組織のセキュリティ方針」の項を参照

P. Personalization Agent

個人化担当者は IC 旅券を安全に管理するとともに、IC 旅券が正常に動作することを確認した後に運用段階に移行させなければならない。
個人化担当者はIC旅券を運用段階に移行させる前に書込み機能を停止しなければならない。

P. Range of RF Communication

IC 旅券のチップと検査システムが通信できる距離は 5cm 未満でなければならない。
IC 旅券の身分事項のページが開かれなければ通信はできないようにしなければならない。

アプリケーションノート：この対策方針を定義することが現実にそぐわない場合も考えられる。その場合は、この対策方針を定義しないことも考えられる。「IC旅券用プロテクションプロファイル解説書」の「組織のセキュリティ方針」の項を参照

P. Security Mechanism Application Procedures

TOE は個人化担当者のアクセス制御ポリシーに反しないように、検査システムのタ

イプに応じたセキュリティメカニズムを提供しなければならない。

アプリケーションノート：この対策方針を定義することが現実にそぐわない場合も考えられる。その場合は、この対策方針を定義しないことも考えられる。「IC旅券用プロテクションプロファイル解説書」の「組織のセキュリティ方針」の項を参照

P. Manufact

IC 製造者ならびに旅券製造者は製造プロセスにおいて品質とセキュリティを保証する。
IC を一意に識別するデータを製造時に IC 製造者が書き込む。
旅券製造者は個人化担当者用の鍵を含む初期データを書き込む。

アプリケーションノート：この対策方針を定義することが現実にそぐわない場合も考えられる。その場合は、この対策方針を定義しないことも考えられる。「IC旅券用プロテクションプロファイル解説書」の「組織のセキュリティ方針」の項を参照

4. セキュリティ対策方針

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、セキュリティ対策方針根拠を以下に記述する。

4.1. TOE のセキュリティ対策方針

TOEのセキュリティ対策方針は以下の通りである。

O. Access Control

TOE は個人化担当者のアクセス制御方針に従ってアクセス権が与えられた外部エンティティに対してのみ利用者データ、TSF データへのアクセスを許可する機能を提供しなければならない。

アプリケーションノート：P. ePassport Access Controlとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「TOEのセキュリティ対策方針」の項を参照

O. BAC

TOE は、認可された検査システムだけに IC 旅券所持者の個人データに対する読み込み権限をあたえるために、BAC 相互認証を実装しなければならない。また、TOE は安全なメッセージ発信のために使われる BAC セッションキーを生成しなければならない。

O. Certificate Verification

TOE は検査システムによって提供される関連証明書に基づいて証明書の有効期限をチェックし証明書を自動更新しなければならない。

アプリケーションノート：P. PKIとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「TOEのセキュリティ対策方針」の項を参照

O. Deleting Residual Information

TOE は資源の割り当てを行う際に以前に使用した BAC セッション鍵などのセキュリティに関係する情報を含まないようにすることを保証しなければならない。

O. Handling Information Leakage

TOE は暗号処理を実行中に漏出する情報が利用されることを防止する機能を提供しなければならない。

O. Management

TOE は、許可された個人化担当者に個人化段階で TOE の利用者データ、TSF データを管理する手段（書き込み用インタフェースを停止する機能を含む）を提供しなければならない。

アプリケーションノート：この対策方針が定義しているのは、TOEに対するデータの書き込みが禁止されるということである。データの書き込みを禁止する方法は複数存在することから、その詳細はSTの開発者が定義すべきである。「IC旅券用プロテクションプロファイル解説書」の「TOEのセキュリティ対策方針」の項を参照

O. Replay Prevention

TOE は、セキュアな暗号処理のため、セッションごとに暗号通信のために異なる乱数を生成しなければならない。

O. Secure Messaging

TOE は、送信データの完全性と機密性を保証しなければならない。

O. Security Mechanism Application Procedures

TOE は、PA、BAC、AA 仕様の IC 旅券検査手順を実施しなければならない。

アプリケーションノート：IC旅券検査手順は検査システムが該当する機能を実施しなければTOE単独で実施することはできない。したがって検査システムとの整合性に注意する必要がある。「IC旅券用プロテクションプロファイル解説書」の「TOEのセキュリティ対策方針」の項を参照

O. Self protection

TOE は、セキュリティ機能のバイパス、セキュリティ機能の実行コードの改竄、スタートアップのためのデータの改竄から自分自身を保護する機能を提供しなければならない。

O. Session Termination

TOE は、BAC 相互認証に失敗した場合およびデータの改竄を検知した場合（AA で偽変造が検知された場合を含む）は、セッションを終了しなければならない。

O. Prot Phys Tamper

TOE は、格納されている組み込みソフトウェアならびにデータを物理的な攻撃から保護する機能提供しなければならない。

O. Range of RF Communication

TOE と検査システムが通信できる距離を 5cm 未満にしなければならない。

TOE と検査システムは身分事項のページが開かれなければ通信はできないようにしなければならない。

アプリケーションノート：P. Range of RF Communicationとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「TOEのセキュリティ対策方針」の項を参照

4.2. 運用環境のセキュリティ対策方針

TOEの運用環境におけるセキュリティ対策方針は以下の通りである。

OD. Assurance

IC 製造者、旅券製造者は、攻撃者が TOE のセキュリティ機能を危殆化するために TOE を解析するためには、複雑な機械、高度な知識・技術、多大な時間が必要になるようにデザインしなければならない。
また、IC 製造者は製造時に IC を一意に識別するデータを書込み、旅券製造者は個人化担当者用の鍵を含む初期データを書き込まなければならない。

アプリケーションノート：本体策方針はTOEの製造過程に関する対策方針であり、STの開発者によって具体的に定義されるべきである。「IC旅券用プロテクションプロファイル解説書」の「運用環境のセキュリティ対策方針」の項を参照

OD. Material

TOE の製造者は、TOE の偽造を防止するため、作業環境・使用する材料・工程等を管理しなければならない。

OE. Personalization Agent

個人化担当者は以下のことを行わなければならない。
・IC 旅券申請者の正当性を確認する
・正しい BAC 認証鍵を記録する
・正しい DS 証明書を登録する
・正しい AA の公開鍵と秘密鍵を登録する
・TOE にプログラムを格納する場合は、TOE のセキュリティに影響を及ぼさないことを確認したうえでおこなう。

・「表 5　利用者データのアクセスポリシー」に示したアクセスポリシーを構築する
・IC 旅券を運用段階に移行させる前に書込み機能を停止する

アプリケーションノート：A. Personalization Agentとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「運用環境のセキュリティ対策方針」の項を参照

OE. Certificate Verification

BIS、AIS などの検査システムは TOE に記録されているデータの偽変造を検証するために PA の証明書の検証を行った後、SOD の検証を行わなければならない。
そして、そのために DS 証明書と CRL を定期的に検査しなければならない。

アプリケーションノート：A. Certificate Verificationとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「運用環境のセキュリティ対策方針」の項を参照

OE. Inspection System

検査システムは ICAO が規定する以下のセキュリティメカニズムを実装しなければならない。
・PA
・BAC
・AA
検査システムはセッション終了時にBACセッション鍵などのセッション情報をセキュアに破棄しなければならない。
BAC と PA を実装している検査システム(BIS)においては、BAC 認証鍵を使用した BAC mutual authentication が成功した場合にのみ、データの読み込み権限が与えられなければならない。
BAC セッション鍵を使用した暗号通信によって通信データの完全性と機密性が保護しなければならない。BIS は BAC の後に PA を実行し、SOD の検証をおこないデータの偽変造を検知しなければならない。
AA と PA を実装している検査システム(AIS)においては、PA を実行し、SOD の検証を行って AA の公開鍵が偽変造されていないことを確認したのちチャレンジレスポンスによって、チップのデータが複製でないことを確認しなければならない。

アプリケーションノート：P. Security Mechanism Application Proceduresとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「運用環境のセキュリティ対策方針」の項を参照

OE. MRZ Entropy

個人化担当者は BAC 認証鍵の種の十分なエントロピーを保証しなければならない。

アプリケーションノート：A. MRZ Entropyとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「運用環境のセキュリティ対策方針」の項を参照

OE. PKI

IC 旅券の発行国は、PA-PKI の CPS に準拠した電子署名鍵、証明書の管理を行わなければならない。
また、IC 旅券の発行国は証明書の有効期限に関するポリシーに従い証明書を更新しなければならない。

アプリケーションノート：A. Certificate Verificationとの整合性に注意して定義する必要がある。「IC旅券用プロテクションプロファイル解説書」の「運用環境のセキュリティ対策方針」の項を参照

OE. Procedures of ePassport holder Check

入国管理者は、IC 旅券の保持者を IC 旅券のページに記載されている識別情報と照合しなければならない。

アプリケーションノート：「IC旅券用プロテクションプロファイル解説書」の「運用環境のセキュリティ対策方針」の項を参照

4.3. セキュリティ対策方針根拠

セキュリティ対策方針と前提条件、脅威、組織のセキュリティ方針の対応を「表 6　セキュリティ方針と前提条件、脅威、組織のセキュリティ方針の対応」に示す。

表 6　セキュリティ方針と前提条件、脅威、組織のセキュリティ方針の対応

	A. Personalization Agent	A. Certificate Verification	A. Inspection System	A. MRZ Entropy	T. Application Program Interference	T. TSF Data Modification	T. BAC Authentication Key Disclose	T. BAC Replay Attack	T. Eavesdropping	T. Forgery and Corruption of Personal Data	T. Skimming	T. Malfunction	T. ePassport Reproduction	T. Leakage of Cryptographic Key Information	T. Residual Information	T. Phys Tamper	P. ePassport Access Control	P. International Compatibility	P. PKI	P. Personalization Agent	P. Range of RF Communication	P. Security Mechanism Application Procedures	P. Manufact
O. Access Control						●	●			●	●		●				●						
O. BAC										●	●		●				●						
O. Certificate Verification																			●				
O. Deleting Residual Information							●								●								
O. Handling Information Leakage														●									
O. Management						●	●										●			●			
O. Replay Prevention								●															
O. Secure Messaging						●			●														
O. Security Mechanism Application Procedures																						●	
O. Self protection												●											
O. Session Termination						●	●			●													
O. Prot Phys Tamper																●							
O. Range of RF Communication											●										●		
OD. Assurance																							●
OD. Material													●										●
OE. Personalization Agent	●				●												●	●		●			
OE. Certificate Verification		●																					
OE. Inspection System			●														●					●	
OE. MRZ Entropy				●																			
OE. PKI		●																	●				
OE. Procedures of ePassport holder													●										

Check																					

「表 6　セキュリティ方針と前提条件、脅威、組織のセキュリティ方針の対応」の通り、いずれのセキュリティ対策方針も少なくとも１つ以上のTOEセキュリティ環境にさかのぼることができる。

次に、セキュリティ対策方針が各セキュリティ環境を満たすこと、脅威に対抗すること、および組織のセキュリティ方針を満たすことの根拠を以下に示す。

A. Personalization Agent

OE. Personalization Agent により個人化担当者は A. Personalization Agent で要求されている作業を行う。
したがって、A. Personalization Agent を満たしている。

A. Certificate Verification

OE. Certificate Verification によって BIS､AIS などの検査システムは A. Certificate Verification が要求する処理を行うほか、OE. PKI によって、それらの処理に必要な電子署名鍵、証明書が管理される。したがって、A. Certificate Verification を満たしている。

A. Inspection System

OE. Inspection System によって A. Inspection System が要求するセキュリティメカニズムの実証、処理の実行が行われる。
したがって、A. Inspection System を満たしている。

A. MRZ Entropy

OE. MRZ Entropy によって個人化担当者は BAC 認証鍵の種の十分なエントロピーを保証することから、A. MRZ Entropy を満たしている。

T. Application Program Interference

OE. Personalization Agent は、個人化担当者により不正なプログラムがロードされることを防止している。したがって、この対策方針は、個人化、運用の各フェーズ

における攻撃に対抗している。

T. TSF Data Modification

・TOE に書き込まれているデータについて
外部エンティティからのアクセスは O. Access Control によって制限される。O. Access Control は個人化担当者のアクセス制御方針にしたがってアクセス制御を実施する。さらに O. Management により、個人化担当者は TOE へのデータの書き込みができなくなるようにすることができる。運用フェーズへの移行にあたり、個人化担当者が TOE へのデータの書き込みをできないようにすることで、運用フェーズにおけるデータの改竄を防止する。
・TOE に書き込まれるデータについて
O. Management により個人化フェーズにおいて個人化担当者がデータを管理するが、個人化担当者が TOE にデータを書き込む際、通信路上でデータが改竄されることを O.Secure Messaging および O.Session Termination により防止する。
以上のことから、これらの対策方針はこの脅威に対抗している。

T. BAC Authentication Key Disclose

O.Management は個人化担当者が TOE へデータを格納するための機能を提供することを求めている。これにより、個人化担当者は TOE にデータを格納し、必要な設定を行うが、この設定に従い、許可されたエンティティに対してのみアクセスを許可することを O.Access Control が求めている。
O.Deleting Residual Information はアクセス制限に関わる BAC 認証について、攻撃者が残存情報から BAC 認証鍵を入手することを防止することを求めている。さらに、O.Session Termination はセッションを終了することで連続的な攻撃を困難にすることを求めている。
以上のことから、これらの対策方針は、この脅威に対抗している。

T. BAC Replay Attack

O.Replay Prevention はセッションごとに異なる乱数を生成し、暗号通信に使用することで、搾取されたデータによる通信の確立を防止することを求めており、この脅威に対抗している。

T. Eavesdropping

O.Secure Messagingは送信データの完全性と機密性を保証することを求めており、この脅威に対抗している。

T. Forgery and Corruption of Personal Data

O.Access ControlはTOEに格納されているデータに対するアクセス権限の付与を個人化担当者のアクセス制御方針に従っておこなうことを求めており、不正な検査システムにアクセス権限が付与されないようにすることを求めている。O.BACは検査システムとの相互認証の実施を求めている。これによりアクセス権限を付与されていない不正な検査システムはTOEに格納されているデータにアクセスすることはできない。さらにO.Session Terminationはセッションを終了することで連続的な攻撃を困難にすることを求めている。
以上のことから、これらの対策方針はこの脅威に対抗している。

T. Skimming

O.Access ControlはTOEに格納されているデータに対するアクセス権限の付与を個人化担当者のアクセス制御方針に従っておこなうことを求めており、不正な装置にアクセス権限が付与されないようにすることを求めている。O.BACは検査システムとの相互認証の実施を求めている。これによりアクセス権限を付与されていない不正な装置はTOEに格納されているデータにアクセスすることはできない。また、O.Range of RF Communicationはページを開かない限り通信がおこなわれないこと、および、通信距離を5cm未満に制限することをもとめており、これにより離れた場所からデータが読み取られる危険を防止している。
以上のことから、これらの対策方針はこの脅威に対抗している。

T. Malfunction

O.Self-protectionはTOEに対し、自分自身を改竄から保護することを求めている。したがって、この対策方針はこの脅威に対抗する。

T. ePassport Reproduction

O.Access ControlはTOEに格納されているデータに対するアクセス権限の付与を個人化担当者のアクセス制御方針に従っておこなうことを求めており、不正な装置に

アクセス権限が付与されないようにすることを求めている。O.BACは検査システムとの相互認証の実施を求めている。これによりアクセス権限を付与されていない不正な装置はTOEに格納されているデータにアクセスすることはできず、偽造するためにデータを入手することはできない。
IC 旅券の偽造には冊子等の材料も必要となるが、OD.Material は IC 旅券の材料の管理を含む製造過程でのセキュリティを求めており、IC 旅券の偽造をより困難にする。また、OE. Procedures of ePassport holder Check は入国管理者による冊子の確認をもとめており、偽造旅券の検知に有効である。
以上のことから、これらの対策方針はこの脅威に対抗している。

T. Leakage of Cryptographic Key Information

O.Handling Information Leakage は暗号処理を実行中に漏出する情報が利用されることを防止する機能を提供することをもとめており、この脅威に対抗している。

T. Residual Information

O.Deleting Residual Information は資源の割り当てを行う際に以前に使用した BAC セッション鍵などのセキュリティに関係する情報を含まないようにすることを保証することをもとめており、この脅威に対抗している。

T.Phys Tamper

O.Prot_Phys-Tamper は、格納されている組み込みソフトウェアならびにデータを物理的な攻撃から保護する機能提供することを求めており、この脅威に対抗している。

P. ePassport Access Control

O.Management は個人化担当者にアクセス制御ポリシーを設定する機能を提供することを求めており、O.Access Control、O.BAC は設定を保護することを求めている。さらに、OE. Personalization Agent は個人化担当者がアクセスポリシーを設定することを求めている。また、OE. Inspection system は検査システムが TOE のセキュリティメカニズムに対応したメカニズムを実装することを求めており、これにより、TOE が実装するセキュリティメカニズムが実効性を伴ったものとなる。したがって、これらの対策方針によりこのセキュリティ方針は達成される。

P. International Compatibility

OE. Personalization Agentは個人化担当者に証明書の登録や鍵の登録など検査システムとの整合性を保証する上で必要な作業の実施を求めており、これによりこのセキュリティ方針は達成される。

P. PKI

OE. PKI はIC旅券の発行国が、PA-PKIのCPSに準拠した電子署名鍵、証明書の管理を行うこと、証明書の有効期限に関するポリシーに従い証明書を更新することをもとめており、また、O. Certificate Verificationは証明書の自動更新機能の実装を求めている。これによりこのセキュリティ方針は達成される。

P. Personalization Agent

O.Managementは利用者データ、TSFデータを管理する手段を個人化担当者に提供することで個人化担当者が書込み機能を停止できるようにしている。さらにOE. Personalization Agentは個人化担当者がIC旅券を安全に管理し、正常に動作することを確認した後に運用段階に移行すること、ならびに運用段階に移行させる前に書込み機能を停止することを求めている。したがって、これらにより、このセキュリティ方針は達成される。

P. Range of RF Communication

O.Range of RF Communicationはページを開かない限り通信がおこなわれないこと、および、通信距離を5cm未満に制限することをもとめており、これによりこのセキュリティ方針は達成される。

P. Security Mechanism Application Procedures

O.Security Mechanism Application Procedures は、AA仕様のIC旅券検査手順を実施することをもとめており、OE. Inspection Systemは検査システムにPA、BAC、AA仕様のIC旅券検査手順の実施を求めており、これによりこのセキュリティ方針は達成される。

P.Manufact

OD.Assurance は IC 製造者、旅券製造者に対して、セキュリティを満たすデザインを要求し、さらに、IC 製造者に対して製造時に IC を一意に識別するデータを書込むこと、旅券製造者に対して個人化担当者用の鍵を含む初期データを書き込むことを要求している。
また、OD.Material は製造者に作業環境・使用する材料・工程の管理を求めている。
以上のことから、これらにより、このセキュリティ方針は達成される。

5. 拡張コンポーネント定義

本PP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

TOEセキュリティ要件として、TOEセキュリティ機能要件およびTOEセキュリティ保証要件を記述する。

6.1. セキュリティ機能要件

TOEセキュリティ機能要件は以下の通りである。

6.1.1. 暗号サポート

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: 標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付: 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 暗号鍵長]に従って、暗号鍵（暗号鍵とMAC鍵）を生成しなければならない。

[割付: 標準のリスト] :
ICAOドキュメント
[割付: 暗号鍵生成アルゴリズム]
Appendix 5.1 Key Derivation Mechanism

[割付: 暗号鍵長]

112bit

アプリケーションノート：TOE は BAC authentication key, BAC session key を生成するが、個人化担当者あるいは旅券製造者等が BAC authentication key を生成し、TOE に書き込む場合は TOE は BAC authentication key の生成をおこなわない。

FCS_CKM.2 暗号鍵配付

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_CKM.2.1 TSFは、以下の[割付: 標準のリスト]に合致する、指定された暗号鍵配付方法[割付: 暗号鍵配付方法]に従って、暗号鍵（BACセッション鍵のKDF種）を配付しなければならない。

[割付: 標準のリスト] :

ISO/IEC 11770-2

[割付:その他の標準]

[割付: 暗号鍵配付方法] :

Establishment mechanism 6

[割付:その他の鍵配送アルゴリズム]

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: 標準のリスト]に合致する、指定された暗号鍵破棄方法[割付: 暗号鍵破棄方法]に従って、暗号鍵（暗号鍵とMAC鍵）を破棄しなければならない。

[割付: 標準のリスト] :
（標準のリスト）
[割付: 暗号鍵破棄方法] :
（暗号鍵の廃棄方法）

アプリケーションノート：ST 開発者は鍵配送メカニズムによって生成された鍵をセキュアに破棄する方法を割り付ける。参照する標準のリストがない場合は「なし」を割り付ける。

FCS_COP.1　暗号操作
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.1.1　TSFは、[割付: 標準のリスト]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: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト] :
ISO/IEC 18033-3
[割付:その他の標準]
[割付: 暗号アルゴリズム] :
TDES
[割付:その他の暗号アルゴリズム]
[割付: 暗号鍵長] :
112 bit,
[割付:その他の暗号鍵長]
[割付: 暗号操作のリスト] :
メッセージの暗号化
メッセージの復号

アプリケーションノート：TOE は BAC において TDES アルゴリズムを使用する。TDES では ISO/IEC10116 で定義されている IV=0 による CBC モードを使用する。

FCS_COP.1(2)　暗号操作

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.1.1(2)　TSFは、[割付: 標準のリスト]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: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト] :
ISO/IEC 9797-1
[割付:その他の標準]
[割付: 暗号アルゴリズム] :
Retail MAC
[割付:その他の暗号アルゴリズム]
[割付: 暗号鍵長] :
112 bit,
[割付:その他の暗号鍵長]
[割付: 暗号操作のリスト] :
MAC処理

アプリケーションノート：Retail MAC ではMAC algorithm 3, the block cipher DES, the sequence message counter and the padding mode 2を使用する。これらはISO/IEC 9797-1.で定義されている。

FCS_COP.1(3)　暗号操作

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.1.1(3) TSFは、[割付: 標準のリスト]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: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト] :
ISO/IEC 10118-3
[割付:その他の標準]
[割付: 暗号アルゴリズム] :
SHA1
[割付:その他の暗号アルゴリズム]
[割付: 暗号鍵長] :
なし
[割付: 暗号操作のリスト] :
ハッシュ値計算

FCS_COP.1(4) 暗号操作
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.1.1(4) TSFは、[割付: 標準のリスト]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: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト] :
ISO/IEC 9796-2
[割付: 暗号アルゴリズム] :
RSA
[割付: 暗号鍵長] :
2048 bit,
[割付: 暗号操作のリスト] :
電子署名

FDP_ACC.1　サブセットアクセス制御

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.1.1　TSFは、[割付: サブジェクト、オブジェクト、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]に対して[割付: アクセス制御SFP]を実施しなければならない。

[サブジェクト] :

(1)個人化担当者

(2) BIS

(3) AIS

(4) [割付 : その他のサブジェクトのリスト]

[オブジェクト] :

(1)パスポート保持者の個人情報

EF.DG1, EF.DG2, EF.DG5~EF.DG13, EF.DG16

(2) IC旅券の認証データ

EF.DG14,EF.DG15, EF.SOD

(3)EF.COM

(4)[割付 : その他のオブジェクト]

[サブジェクトとオブジェクト間の操作のリスト] :

(1) Read

(2) Write

(3)[割付 : その他の操作]

[割付: アクセス制御SFP] :

IC旅券アクセス制御ポリシー

FDP_ACF.1　セキュリティ属性によるアクセス制御

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.1.1　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とオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御SFP]を実施しなけ

ればならない。

[割付: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]:

表 7　サブジェクトとセキュリティ属性

表 8　オブジェクトとセキュリティ属性

[割付：その他のサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]

[割付: アクセス制御SFP]:

IC旅券アクセス制御ポリシー

アプリケーションノート：BAC mutual authenticationが成功した場合にFIA_UID.1で識別されたユーザにBAC authorizationの権限が与えられる。個人化担当者は個人化フェーズにおいて認証が成功することにより権限が与えられる。

FDP_ACF.1.2　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: 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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

サブジェクトのセキュリティ属性がオブジェクトへのアクセス権限属性の中にふくまれ、かつ、サブジェクトからの操作がオブジェクトの操作のセキュリティ属性に一致している場合にのみ実行が許可される。

[割付：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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

アプリケーションノート：STの開発者はアクセス制御の規則を割り付けるべきである。

FDP_ACF.1.3　TSFは、次の追加規則、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]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。

[割付: 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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

FDP_ACF.1.4　TSFは、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]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。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]

承認されていない検査システムからのオブジェクトに対するアクセスをすべて拒否する

[割付:その他のセキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]

表 7　サブジェクトとセキュリティ属性

サブジェクト	セキュリティ属性
BIS	BAC 認証、PA
AIS	BAC 認証、AA
個人化担当者	個人化担当者であることの認証

表 8　オブジェクトとセキュリティ属性

オブジェクト	セキュリティ属性	
	オブジェクトに対する操作の属性	オブジェクトへのアクセス権限の属性
IC 旅券保持者の個人データ	読み取り	BAC 認証
	書込み	個人化担当者であることの認証
IC 旅券の認証データ	読み取り	BAC 認証
	書込み	個人化担当者であることの認証
EF.COM	読み取り	BAC 認証
	書込み	個人化担当者であることの認証

FDP_RIP.1　サブセット情報保護

下位階層:　なし

依存性:　なし

FDP_RIP.1.1　TSFは、[割付: オブジェクトのリスト]のオブジェクト[選択: への資源の割当て、からの資源の割当て解除]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

[割付: オブジェクトのリスト] :

BACセッション鍵

BAC認証鍵

[割付：その他のオブジェクトのリスト]

[選択: への資源の割当て、からの資源の割当て解除] :

アプリケーションノート：セッション終了後、TSFは、BACセッション鍵、BAC認証鍵、乱数などを一時記憶に残さない。これらは、FCS_CKM.4で定義された方法で破棄される。STの開発者は操作を完了しなければならない。

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]を行えるようにするために、[割付: アクセス制御SFP及び/または情報フロー制御SFP]を実施しなければならない。

[選択: 送信、受信] :

送信、受信

[割付: アクセス制御SFP及び/または情報フロー制御SFP] :

IC旅券アクセス制御ポリシー

アプリケーションノート：検査システムがBAC mutual authenticationに成功した場合、TSFはBAC session encryption keyでデータの機密性を保護する。

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]できるようにするために、[割付: アクセス制御SFP及び/または情報フロー制御SFP]を実施しなければならない。

[選択: 改変、消去、挿入、リプレイ] :

[選択: 送信、受信] :
送信、受信
[割付: アクセス制御SFP及び/または情報フロー制御SFP] :
IC旅券アクセス制御ポリシー

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。

[選択: 改変、消去、挿入、リプレイ] :

アプリケーションノート：TSFはBACセッションにおいてMAC鍵を使用することでデータの完全性を保護する。STの開発者は[選択]において「リプレイ」を選択する場合には、さらなるセキュリティ機能の実装が必要となる。

6.1.2. 識別と認証

FIA_AFL.1　　認証失敗時の取り扱い

下位階層:　なし

依存性:　FIA_UAU.1認証のタイミング

FIA_AFL.1.1　TSFは、[割付: 認証事象のリスト]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。

[割付: 認証事象のリスト] :
BAC相互認証
[割付：その他の認証事象]

[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] :

FIA_AFL.1.2 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: アクションのリスト]をしなければならない。

[選択：に達する、を上回った] :

[割付: アクションのリスト] :
セション終了

アプリケーションノート：BAC mutual authenticationが不成功の場合、BAC secure messagingは終了するのが望ましいが、STの開発者は終了を他の等価なメカニズムで置き換えることができる。STの開発者は、不成功の認証回数を割り付ける。

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: TSF仲介アクションのリスト]を許可しなければならない。

[割付: TSF仲介アクションのリスト] :
BACメカニズムのための前処理
[割付:その他のTSF仲介アクション]

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。

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: 識別された認証メカニズム]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。

[割付: 識別された認証メカニズム]
BAC相互認証
[割付：その他の認証メカニズム]

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実行される[割付: TSF仲介アクションのリスト]を許可しなければならない。

[割付: TSF仲介アクションのリスト]
ISO/IEC 14443-4に基づく通信路の確立

FIA_UID.1.2 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。

6.1.3. セキュリティ管理

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: 機能のリスト][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: 許可された識別された役割]に制限しなければならない。

[割付: 機能のリスト] :
書込み機能
[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] :
を停止する
[割付: 許可された識別された役割] :
個人化フェーズにおける個人化担当者

アプリケーションノート：個人化担当者は、個人化フェーズにおいてTOEにデータを書き込んだ後、TOEにデータを書き込めない状態にした上で、TOEを運用フェーズに移行する。

FMT_MSA.1　セキュリティ属性の管理

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_SMR.1セキュリティの役割
FMT_SMF.1管理機能の特定

FMT_MSA.1.1　TSFは、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を[割付: 許可された識別された役割]に制限する[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

[割付: セキュリティ属性のリスト]:
FDP_ACF.1で定義したサブジェクトのセキュリティ属性
[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]:
[割付: その他の操作]
初期化
[割付: 許可された識別された役割]:
TSF
[割付: アクセス制御SFP、情報フロー制御SFP]:
IC旅券アクセス制御ポリシー

アプリケーションノート：FPT_ITI.1で改ざんが検出された場合、TSFはFDP_ACF.1で定義されているサブジェクトのセキュリティ属性をリセットする。

FMT_MSA.3　静的属性初期化

下位階層:　なし

依存性:　FMT_MSA.1セキュリティ属性の管理
FMT_SMR.1セキュリティの役割

FMT_MSA.3.1　TSFは、そのSFPを実施するために使われるセキュリティ属性に対して[選択: 制限的、許可的、[割付: その他の特性]: から1つのみ選択]デフォルト値を与える[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

[選択: 制限的、許可的、[割付: その他の特性]: から1つのみ選択]:

制限的

[割付: アクセス制御SFP、情報フロー制御SFP]:

IC旅券アクセス制御ポリシー

FMT_MSA.3.2 TSFは、オブジェクトや情報が生成されるとき、[割付: 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[割付: 許可された識別された役割]:

個人化担当者

アプリケーションノート：個人化フェーズにおいて利用者データを生成する際、個人化担当者はFDP_ACF.1.1.の定義にしたがって、オブジェクトのセキュリティ属性ならびアクセス権限を定義する。

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: TSFデータのリスト]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: 許可された識別された役割]に制限しなければならない。

[割付: TSFデータのリスト]:

BAC認証鍵（秘密鍵）

AA用秘密鍵

[割付：その他のTSFデータ]

[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]]:

[割付: その他の操作]

セキュアメモリへの書込み

[割付: 許可された識別された役割]:

個人化フェーズにおける個人化担当者

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: TSFによって提供される管理機能のリスト]

[割付: TSFによって提供される管理機能のリスト] :
個人化フェーズにおける利用者データとTSFデータの書込み機能
[割付：その他の管理機能]

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: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割] :
個人化担当者
[割付：その他の役割]

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。

6.1.4. プライバシー

FPR_UNO.1　観察不能性
下位階層:　なし
依存性:　なし

FPR_UNO.1.1　TSFは、[割付: 利用者及び/またはサブジェクトのリスト]が[割付: 保護された利用者及び/またはサブジェクトのリスト]による[割付: オブジェクトのリスト]に対する操作[割付: 操作のリスト]を観察できないことを保証しなければならない。

[割付: 利用者及び/またはサブジェクトのリスト] :
外部エンティティ
[割付: 保護された利用者及び/またはサブジェクトのリスト] :
TSF
[割付: オブジェクトのリスト] :
BAC認証鍵
BACセッション鍵

AA秘密鍵
[割付：その他のオブジェクト]
[割付: 操作のリスト]:
FCS_COP.1(1)の暗号操作
FCS_COP.1(2) の暗号操作
FCS_COP.1(4) の暗号操作
[割付：その他の操作]

6.1.5. TSF の保護

FPT_FLS.1 セキュアな状態を保持する障害
下位階層: なし
依存性: なし

FPT_FLS.1.1 TSFは、以下の種別の障害が生じたときはセキュアな状態を保持しなくてはならない: [割付: TSFにおける障害の種別のリスト]。

[割付: TSFにおける障害の種別のリスト]:
FPT_TST.1における自己テストの失敗
ICチップにより感知される異常
[割付：その他のTSFにおける障害]

FPT_ITI.1 TSF間改変の検出
下位階層: なし
依存性: なし

FPT_ITI.1.1 TSFは、以下の尺度の範囲で、TSFと他の高信頼IT製品間で送出中のすべてのTSFデータの改変を検出する能力を提供しなければならない。:
[割付: 定義された改変尺度]

[割付: 定義された改変尺度]
Retail MACの強度

FPT_ITI.1.2 TSFは、TSFと他の高信頼IT製品間で送られるすべてのTSFデータの完全性を検証し、かつ改変が検出された場合には[割付: とられるアクション]を実行する能力を提供しなければならない。

[割付: とられるアクション]:
BAC暗号通信の停止

BACセッション鍵の消去
FMT_MSA.1で定義した操作
個人化担当者の通信チャネルの停止
[割付：その他のとられるアクション]

FPT_TST.1 TSFテスト
下位階層: なし
依存性: なし

FPT_TST.1.1 TSFは、[選択: TSF、[割付: TSFの一部]の正常動作を実証するために、[選択: 初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、条件[割付: 自己テストが作動すべき条件]下で]自己テストのスイートを実行しなければならない。

[選択: TSF、[割付: TSFの一部]の正常動作を実証するために、[選択: 初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、条件[割付: 自己テストが作動すべき条件]下で]：

FPT_TST.1.2 TSFは、許可利用者に、[選択: [割付: TSFデータの一部]、TSFデータ]の完全性を検証する能力を提供しなければならない。

[選択: [割付: TSFデータの一部]、TSFデータ]：

FPT_TST.1.3 TSFは、許可利用者に、格納されているTSF実行コードの完全性を検証する能力を提供しなければならない。

アプリケーションノート：STの開発者は操作を完了しなければならない。

FPT_PHP.3 物理的な攻撃への抵抗
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: TSF装置/エレメントのリスト]への[割付: 物理的な改ざんのシナリオ]に抵抗しなければならない。

[割付: TSF装置/エレメントのリスト]：
TSF

[割付: 物理的な改ざんのシナリオ]:
プロービングなどを含む物理的解析

6.2. セキュリティ保証要件

本TOEの評価保証レベルはEAL4追加（追加する保証コンポーネントはADV_IMP.2、ALC_DVS.2、AVA_VAN.5）であり、TOEセキュリティ保証要件は以下の通りである。

クラス	保証コンポーネント	
ADV:開発	ADV_ARC.1	セキュリティアーキテクチャ記述
	ADV_FSP.4	完全な機能仕様
	ADV_IMP.2	TSF の実装表現の完全なマッピング
	ADV_TDS.3	基本モジュール設計
AGD:ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ALC:ライフサイクルサポート	ALC_CMC.4	製造支援、受け入れ手続き、及び自動化
	ALC_CMS.4	課題追跡の CM 範囲
	ALC_DEL.1	配付手続き
	ALC_DVS.2	セキュリティ手段の十分性
	ALC_LCD.1	開発者によるライフサイクルモデルの定義
	ALC_TAT.1	明確に定義された開発ツール
ASE:セキュリティターゲット評価	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様
ATE:テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.2	テスト：セキュリティ実施モジュール
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テストーサンプル
AVA:脆弱性評定	AVA_VAN.5	高度な方法的脆弱性分析

6.3. セキュリティ要件根拠

TOEセキュリティ機能要件根拠、セキュリティ機能要件の依存性の妥当性、評価保証レベルの妥当性、およびセキュリティ保証要件の必要性について記述する。

6.3.1. セキュリティ機能要件根拠

TOEセキュリティ機能要件とTOEセキュリティ対策方針との対応を「表 9　TOEセキュリティ機能要件とTOEセキュリティ対策方針」に示す。

表 9　TOE セキュリティ機能要件と TOE セキュリティ対策方針

	O.Access Control	O.BAC	O.Deleting Residual Information	O.Handling Information Leakage	O.Management	O.Replay Prevention	O.Secure Messaging	O.Security Mechanism Application Procedures	O.Self protection	O.Session Termination	O.Prot Phys Tamper
FCS_CKM.1		●									
FCS_CKM.2		●				●					
FCS_CKM.4			●								
FCS_COP.1(1)		●					●				
FCS_COP.1(2)		●					●				
FCS_COP.1(3)								●			
FCS_COP.1(4)								●			
FDP_ACC.1	●										
FDP_ACF.1	●										
FDP_RIP.1			●								
FDP_UCT.1							●				
FDP_UIT.1							●				
FIA_AFL.1	●	●								●	
FIA_UAU.1	●	●								●	

FIA_UAU.4		●				●					
FIA_UID.1		●									
FMT_MOF.1	●				●						
FMT_MSA.1	●						●				
FMT_MSA.3	●										
FMT_MTD.1	●				●						
FMT_SMF.1					●						
FMT_SMR.1					●						
FPR_UNO.1				●							
FPT_FLS.1									●		
FPT_ITI.1							●				
FPT_PHP.3											●

「表 9　TOEセキュリティ機能要件とTOEセキュリティ対策方針」の通り、すべてのTOEセキュリティ機能要件は少なくともひとつのTOEセキュリティ対策方針にさかのぼることができる。

次に、TOEセキュリティ機能要件が各TOEセキュリティ対策方針を満たすことの根拠を以下に示す。

O.Access Control

この対策方針は、個人化担当者のアクセス制御方針に従ってアクセス権が与えられた外部エンティティに対してのみアプリケーションデータへのアクセスを許可する機能を提供することを求めている。

FMT_MSA.3により個人化担当者がセキュリティ属性の初期値を特定する（デフォルト値は制限的である）。

FMT_MSA.1によりセキュリティ属性は、初期値で初期化される。

FDP_ACC.1、FDP_ACF.1はセキュリティ属性を参照し、アクセス制御を行う。

個人化担当者はFIA_UAU.1によって認証され、認証失敗時の扱いはFIA_AFL.1で定義されている。

セキュリティ属性を特定するためには書込み機能を使用する必要があるが、書込み機能を使用した書込みならびに停止はFMT_MOF.1、FMT_MTD.1により個人化担当者に制限される。

以上のことから、これらの機能要件はこの対策方針を満たし、また、この対策方針を満たす上で不要な要件は含まれていない。

O.BAC
この対策方針は、BAC相互認証により不正な検査システムからのアクセスを防止するとともに安全なメッセージ発信のためのセッションキーの生成を求めている。
FCS_CKM.1はセッション鍵の生成を行ううえで必要な暗号鍵とMAC鍵の生成を求めている。
FCS_CKM.2はセッション鍵の種の配付を求めている。
FCS_COP.1(1)、FCS_COP.1(2)は安全なメッセージ発信のための暗号操作を定義している。
FIA_UID.1、FIA_UAU.1は相互認証に先だつ前処理ならびに認証処理を定義しており、FIA_AFL.1は認証失敗時の処理を定義している。さらにFIA_UAU.4は認証機能が危殆化されることを防止するための機能を定義している。
以上のことから、これらの機能要件はこの対策方針を満たし、また、この対策方針を満たす上で不要な要件は含まれていない。

O.Deleting Residual Information
この対策方針は、以前に使用したBACセッション鍵などのセキュリティに関係する情報が残存し、悪用されることを防止することを求めている。
FCS_CKM.4は暗号鍵をセキュアに破棄することを求めている。さらにFDP_RIP.1は残存情報からの暗号鍵の漏洩を防止することを求めている。
以上のことから、これらの機能要件はこの対策方針を満たし、また、この対策方針を満たす上で不要な要件は含まれていない。

O.Handling Information Leakage
この対策方針は、暗号処理を実行中に漏出する情報が利用されることを防止することを求めている。
FPR_UNO.1は暗号処理中の観察を防止することを求めている。したがって、この機能要件はこの対策方針を満たすのに十分であり、また、この機能要件はこの対策方針を満たす上で余分な機能を定義していない。

O.Management
この対策方針は、許可された個人化担当者に個人化段階でTOEのアプリケーションデータを管理する手段を提供することを求めている。
FMT_SMF.1はデータの書込み機能の実装をもとめており、FMT_MOF.1は当該機能の停止を個人化フェーズにおける個人化担当者に制限することを求めている。これは、必要な機能の提供を求めるとともにその機能が悪用されることを防止するためのものであり、この対策方針の実現に貢献する。
FMT_MTD.1は書込み機能を利用したデータの書込みを個人化フェーズにおける個人化担

当者に制限することを求めており、FMT_SMR.1は個人化担当者という役割の維持を求めている。これにより、書込み機能が提供され、かつ、その利用は許可された個人化担当者に制限されるとともに、悪用を防止するため、許可された個人化担当者は書込み機能を停止することができる。
以上のことから、これらの機能要件はこの対策方針を満たし、また、この対策方針を満たす上で不要な要件は含まれていない。

O.Replay Prevention
この対策方針は、セッションごとに暗号通信のために異なる乱数を生成することを求めている。
FCS_CKM.2は、セッション鍵の種（乱数）の生成を求めている。さらに、FIA_UAU.4は認証データの再使用を防止することを求めている。これにより、セッション鍵の種（乱数）は再使用されることなく、毎回異なる値が生成される。
以上のことから、これらの機能要件はこの対策方針を満たし、また、この対策方針を満たす上で不要な要件は含まれていない。

O.Secure Messaging
この対策方針は、送信データの完全性と機密性を保証することを求めている。
FCS_COP.1(1)、 FCS_COP.1(2)は送信データの暗号化を求めている。この暗号化により送信データは暗号化により完全性、機密性が保証される。
FDP_UCT.1はデータの送受信にあたりアクセス制御を行うことを求めている。これにより不正な相手に対してデータが送信されることを防止する。FDP_UIT.1は不正な通信が行われることを防止するためのアクセス制御を求めており、FDP_UCT.1と同様、不正な相手に対してデータが送信されることを防止する。また、FMT_MSA.1はアクセス制御のもとになるセキュリティ属性の管理を定義している。さらに、FPT_ITI.1は送信されるTSFデータの改変検出を求めている。
送信データにはTOEと検査システムの間でやり取りされるデータのほか、個人化担当者がTOEに格納するデータが存在し、これらの機能要件により、それらの送信データが保護される。
以上のことから、これらの機能要件はこの対策方針を満たし、また、この対策方針を満たす上で不要な要件は含まれていない。

O.Security Mechanism Application Procedures
この対策方針は、PA、BAC、AA仕様のIC旅券検査手順を実施することを求めている。
FCS_COP.1(3)、FCS_COP.1(4)はPA、BAC、AA仕様のIC旅券検査を行ううえで必要となる暗号操作を定義しており、この対策方針の実現に貢献する。また、余分な機能を定義し

ていない。

O.Self-protection
この対策方針は、セキュリティ機能のバイパス、セキュリティ機能の実行コードの改竄、スタートアップのためのデータの改竄から自分自身を保護することを求めている。
FPT_FLS.1は自己テストの失敗、ならびにICチップにより感知される異常を検出しセキュアな状態を保持することを求めており、この対策方針の実現に貢献する。また、余分な機能を定義していない。

O.Session Termination
この対策方針は、BAC相互認証に失敗した場合およびデータの改竄を検知した場合（AAで偽変造が検知された場合を含む）は、セッションを終了することを求めている。
FIA_UAU.1はBAC相互認証の実施を定義しており、FIA_AFL.1は認証に失敗した場合、セッションを終了することを求めている。したがって、これらの機能要件はこの対策方針を満たし、また、この対策方針を満たす上で不要な要件は含まれていない

O.Prot_Phys-Tamper
この対策方針は、格納されている組み込みソフトウェアならびにデータを物理的な攻撃から保護することを求めている。
FPT_PHP.3はプロービングなどを含む物理的解析に対抗することを求めており、この対策方針の実現に貢献する。また、余分な機能を定義していない。

6.3.2. セキュリティ機能要件の依存性の妥当性

セキュリティ機能要件とその依存先の対応を「表 10　セキュリティ機能要件と依存先」に示す。

表には、セキュリティ機能要件で要求された依存先（依存性欄）と実際に選択した依存先を示している。

表 10　セキュリティ機能要件と依存先

セキュリティ機能要件	Part2 の依存性	本 TOE が満たすべき依存性
FCS_CKM.1	[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.2 FCS_CKM.4
FCS_CKM.2	[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_CKM.1 FCS_CKM.4
FCS_CKM.4	[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.1
FCS_COP.1(1)	[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_CKM.1 FCS_CKM.4
FCS_COP.1(2)	[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_CKM.1 FCS_CKM.4
FCS_COP.1(3)	[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_CKM.1 FCS_CKM.4
FCS_COP.1(4)	[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_CKM.1 FCS_CKM.4
FDP_ACC.1	FDP_ACF.1セキュリティ属性によるアクセス制御	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1サブセットアクセス制御	FDP_ACC.1

	FMT_MSA.3静的属性初期化	FMT_MSA.3
FDP_RIP.1	なし	なし
FDP_UCT.1	[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]	なし FDP_ACC.1
FDP_UIT.1	[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_ACC.1 なし
FIA_AFL.1	FIA_UAU.1認証のタイミング	FIA_UAU.1
FIA_UAU.1	FIA_UID.1識別のタイミング	FIA_UID.1
FIA_UAU.4	なし	なし
FIA_UID.1	なし	なし
FMT_MOF.1	FMT_SMR.1セキュリティの役割 FMT_SMF.1 管理機能の特定	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[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_SMR.1セキュリティの役割 FMT_SMF.1 管理機能の特定	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1セキュリティ属性の管理 FMT_SMR.1 セキュリティの役割	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1セキュリティの役割 FMT_SMF.1 管理機能の特定	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	なし	なし
FMT_SMR.1	FIA_UID.1識別のタイミング	FIA_UID.1
FPR_UNO.1	なし	なし
FPT_FLS.1	なし	なし
FPT_ITI.1	なし	なし
FPT_PHP.3	なし	なし

FDP_UCT.1とFDP_UIT.1はFTP_ITC.1またはFTP_TRP.1に依存性を持っているが、FDP_UCT.1とFDP_UIT.1は検査システムとTOEの間のセキュアな通信のための要件である。検査システムとTOEの間の通信チャネルは１つだけであることから、他のチャネルからの分離を考慮する必要がない。

6.3.3. セキュリティ保証要件の依存性

EAL4は商用のIT製品やシステムに求められる最高水準の保証である。しかしながら、TOEは高い攻撃能力を有する攻撃者を想定していることから、開発・ライフサイクル・脆弱性評定の各クラスにおいて、以下の保証ファミリを追加で選択している。

ADV_IMP.2：

これにより、故意でない機能の欠如に対するより高い保証を提供する。

ALC_DVS.2、ALC_CMC.5：

これにより、特に MRTD の材料の安全な取り扱いのための MRTD の開発と製造のセキュリティの、より高い保証を提供する。

AVA_VAN.5：

これにより、評価者が高い攻撃能力を想定した侵入テストを実施することを要求し、攻撃者が TOE の運用環境で潜在的脆弱性を悪用できないことを保証する。

これらの追加されたファミリはいずれも高い攻撃能力を有する攻撃者を想定した保証を与える上で適切であり、本 PP で選択した保証要件は適切である。

6.3.4. セキュリティ保証要件根拠

セキュリティ保証要件とその依存先の対応を「表 11　セキュリティ保証要件と依存先」に示す。

表には、セキュリティ保証要件で要求された依存先（依存性欄）と実際に選択した依存先を示している。この表に示したとおり、すべての依存性は満たされている。

表 11　セキュリティ保証要件と依存先

セキュリティ機能要件	Part3 の依存性	本 TOE が満たすべき依存性
ADV_IMP.2	ADV_TDS.3 基本モジュール設計	EAL4
	ALC_TAT.1　明確に定義された開発ツール	EAL4
	ALC_CMC.5 高度なサポート	ALC_CMC.5
ALC_CMC.5	ALC_CMS.1 TOEのCM範囲	EAL4
	ALC_DVS.2 セキュリティ手段の十分性	ALC_DVS.2
	ALC_LCD.1 開発者によるライフサイクルモデルの定義	EAL4
ALC_DVS.2	なし	なし
AVA_VAN.5	ADV_ARC.1 セキュリティアーキテクチャ記述	EAL4
	ADV_FSP.2 セキュリティ実施機能仕様	EAL4
	ADV_TDS.3 基本モジュール設計	EAL4

	ADV_IMP.1 TSFの実装表現	EAL4
	AGD_OPE.1 利用者操作ガイダンス	EAL4
	AGD_PRE.1 準備手続き	EAL4

7. 用語

用語	定義
Active Authentication （AA：能動認証）	公開鍵暗号方式を利用したデジタル署名により、MRTD チップの複製を検出するセキュリティメカニズムのこと。デジタル署名検証用の鍵情報は、AA 公開鍵（KPu_AA）と、その対になる AA 秘密鍵（KPr_AA）である。
Basic Access Control （BAC：基本アクセス制御）	MRTD チップと検査システム端末間でセッション鍵（KS_ENC, KS_MAC）を確立することにより、通信データに対する盗聴を防止するセキュリティメカニズムのこと。端末から MRTD チップに送信されるコマンド1及び MRTD チップによるレスポンス2に対して、暗号鍵（KS_ENC）による暗号化、並びに認証鍵（KS_MAC）による認証子付与を行なう。
BAC Authentication Key3 （BAC 認証鍵）	IC 旅券券面に記載される MRZ（Machine Readable Zone）データの一部を鍵のシード（K_seed）として、ICAO で規定される鍵生成メカニズム（KDM：Key Derivation System）により作成される暗号化鍵（K_ENC）及び認証子生成鍵（K_MAC）のこと。
BAC mutual authentication （BAC 相互認証）	MRTD チップと検査システム端末間でセッション鍵を確立するための認証プロトコルのこと。セッション鍵の種データに対して、暗号化及び認証子付与を行なう。
Clone (クローン)	本 PP では、MRTD チップの格納データに対する複製を意味する。
Country Signing Certification Authority （CSCA）	CSCA 証明書（C_CSCA）を作成、発行、及び/又は管理する主体。旅券発行国に唯一つ存在するルート認証局。公開鍵暗号方式により、公開鍵と秘密鍵のペア（KPu_CSCA）,

[1] C-APDU: Command Application Protocol Data

[2] R-APDU: Response APDU

[3] この表記法は韓国の PP[5]に準拠したものであり、ICAO の「Document Basic Access Key」 に対応する（文献[2]の Annex E を参照）。

	（KPr_CSCA）を生成、及び/又は管理する。また、CSCA 秘密鍵（KPr_CSCA）を使用して、自国の DS 証明書(C_DS)にデジタル署名を施す。
CPS	Certification Practice Statement 認証局（CA）を運用する際に証明書の利用目的を定める証明書ポリシー（CP：Certificate Policy）と、CA の運用方法を定める認証実施規定。
CRL	Certificate Revocation List 証明書失効リスト 有効期間内に無効（取消された）となった公開鍵証明書のシリアル番号の一覧。証明書を発行した認証機関である認証局（CA）や検証局（VA）が管理を行い、失効した証明書シリアル番号、失効理由、CRL の発行者、発行日時 などを付加し、電子署名を付与する。
CSCA Certificate （CSCA 証明書）	CSCA が生成、発行、及び/又は管理する公開鍵証明書のこと。（C_CSCA）で表記する。格納された CSCA 公開鍵（KPu_CSCA）により、DS 証明書（C_DS）にデジタル署名を施す。
Document Security Object （SOD）	RFC3369 及び/又は“Cryptographic Message Syntax, August 2002”に明記された Signed Data Type のこと。（（SO_D））で表記する。 全てのセキュリティオブジェクトは、それらのデジタル署名の完全性保のため、Distinguished Encoding Rule(DER)フォーマットにより生成される。 セキュリティオブジェクトには、Personalization Agent によって記録された IC 旅券の識別データ、並びに認証データ等が含まれる。
Document Signer （DS）	DS 証明書（C_DS）を生成、発行、及び/又は管理する主体。公開鍵暗号方式により、公開鍵と秘密鍵のペア（KPu_DS, KPr_DS）を生成し、これらを管理する。また、DS 秘密鍵（KPr_DS）を使用して、MRTD チップの Document Security Object にデジタル署名を施す。
DS Certificate （DS 証明書）	DS が作成、発行、及び/又は管理する公開鍵証明書のこと。（C_DS）で表記する。格納された DS 公開鍵（KPu_DS）により、MRTD チップの SOD（SO_D）に施されたデジタル署名を検証する。

EAC	Extended Access Control 拡張アクセス制御 IC 旅券の非接触チップに格納された生体認証データ（虹彩や指紋のスキャン）に、承認された団体のみがアクセスできるように定義されたプロセス
IC module (IC モジュール)	非接触のインタフェース、メモリ（RAM、ROM、EEPROM）、CPU などから構成されるハードウェア構成要素のこと。
International Civil Aviation Organization （ICAO： 国際民間航空機構）	国際民間航空が安全かつ整然と発達し、また国際航空運送業務が機会均等主義に基づいて健全かつ経済的に運営されるように各国の協力を図ることを目的として、国連に発足した専門機関のこと。
Inspection System （IS： 検査システム）	光学的 MRZ 読み取り機能、IC 旅券の照合をサポートするためのセキュリティメカニズムを実装した情報システムのこと。MRTD チップと無線通信を行うための端末、及びこの端末を通じて MRTD チップにコマンドを伝送し、さらにその伝送したコマンドに対する MRTD チップからのレスポンスを処理するためのシステムから構成される。本 PP では、BAC 処理を行なう BIS と、AA 処理を行なう AIS に分類される。
Internal Elementary File （IEF： 内部基礎ファイル）	JIS X 6306 で規定された、外部からの格納情報の読み出し、及び書き込みが不可能なセキュアエリアのこと。
Logical Data Structure （LDS： 論理データ構造）	MRTD チップの利用者データを格納するために、ICAO document で規定された論理データ構造のこと。
Machine Readable Travel Document （MRTD）	旅券、ビザ、又は旅行者の識別に係る公式文書のこと。
MRTD Application (MRTD アプリケーション)	MRTD チップにロードされたプログラムのこと。ICAO document で規定された LDS に準拠して設計され、BAC、PA 並びに AA のセキュリティメカニズムを提供する。
MRTD chip (MRTD チップ)	MRTD アプリケーション及び専用 OS が実装された非接触 IC チップのこと。ISO/IEC 14443 に準拠した通信プロトコルをサポートする。
MRZ （Machine Readable Zone）	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 文字の機械読取領域のこと。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 Entropy	MRZ 情報の情報量とその拡散程度のこと。

(MRZ エントロピー)	
Passive Authentication （PA）	受入国側の検査システムが、公開鍵基盤（PKI: Public Key Infrastructure）による証明書チェーンを利用して旅券発行国及び MRTD チップを照合するセキュリティメカニズムのこと。検査システムは、CSCA 証明書（C_CSCA）を使って旅券発行国の DS 証明書（C_DS）に施されたデジタル署名を照合することにより、旅券発行国の正当性を保証する。さらに、DS 証明書を使って MRTD チップの Document Security Object （SO_D）に施されたデジタル署名を照合することにより、MRTD チップの格納データが改ざんされていないことを保証する。
PA-PKI	CSCA 証明書（C_CSCA）と DS 証明書（C_DS）による証明書チェーンを利用した公開鍵基盤のこと。PA-PKI にはルート認証局が存在しないため、旅券発行国と受入国間で自国の CSCA 証明書を交換する。
Personalization agent （個人化機関）	受入れ機関（Reception organization）から IC 旅券の識別データを受領し、そのデータに対してデジタル署名を施すことにより Document Security Object （SO_D）を生成する。Document Security Object （SO_D）を MRTD チップに格納した後、TSF データの生成、及び MRTD チップの内部基礎ファイル（IEF） への格納を行なう。
Power Analysis (電力解析)	ハードウェア等の消費電力より暗号鍵を推定する暗号解析方法。単純電力解析（SPA）や差分電力解析（DPA）などがある。
Probing (プロービング)	IC の内部バスに直接探針を当ててレジスタのビット値を観測することにより、暗号鍵等の秘密情報を得る破壊型解析方法のこと。
Secure Messaging （セキュアメッセージング）	セッション鍵（KS_ENC, KS_MAC）を使い、端末から MRTD チップに送信されるコマンド4及び MRTD チップによるレスポンス5に対する暗号化、及び認証子付与を行なう機能のこと。セキュアメッセージングが開始される直前に、MRTD チップと検査システム端末間でセッション鍵の種データの交換が行なわれる。
TSF Data （TSF データ）	IC 旅券のセキュリティメカニズムをサポートするために、

[4] C-APDU: Command Application Protocol Data

[5] R-APDU: Response APDU

	MRTD チップの内部基礎ファイル（IEF）に格納されるデータのこと。
User Data （利用者データ）	IC 旅券の識別データ、認証データ等のこと。
Working Elementary File （WEF： 作業用基礎ファイル）	JIS X 6306 で規定された、外部から読出し可能な情報を格納する領域のこと。

8. 参考文書

[1] Doc 9303 “Machine Readable Travel Documents” Part 1 “Machine Readable Passports” Volume 2 “Specification for Electronically Enabled Passports with Biometric Identification Capability" Sixth Edition, International Civil Aviation Organization(ICAO), 2006. 8

[2] Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version - 1.1, Date - October 01, 2004, published by authority of the secretary general, International Civil Aviation Organization

[3] Common Criteria Security Target - SHRP Passport Booklet module Version 1.1, 2006, SHARP

[4] Common Criteria Security Target - E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller, 2007, NTTDATA

[5] Common Criteria Protection Profile - ePassport Protection Profile Version 1.0 (KECS-PP-0084-2008), 2008, KECS

[6] Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-PP-0017, 18 August 2005

[7] Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0026, BSI-PP-0026, 7 September 2006

[8] Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-CC-PP-0026, 19 November 2007

[9] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001

[10] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements September 2007 Version 3.1 Revision 2 CCMB-2007-09-002

[11] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements September 2007 Version 3.1 Revision 2 CCMB-2007-09-003

[12] 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 2006 年 9 月 バージョン 3.1 改訂第 1 版 CCMB-2006-09-001（平成 19 年 3 月翻訳代 1.2 版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）

[13] 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 2007 年 9 月 バージョン 3.1 改訂第 2 版 CCMB-2007-09-002（平成 20 年 3 月翻訳代 2.0 版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）

[14] 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 2007 年 9 月 バージョン 3.1 改訂第 2 版 CCMB-2007-09-003（平成 20 年 3 月翻訳代 2.0 版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）

[15] ISO/IEC 7810: 2003, Identification cards - Physical characteristics

[16] ISO/IEC 7816-4:2005, Identification cards - Integrated circuit cards -- Part 4: Organization, security and commands for interchange

[17] ISO/IEC 7816-5:2004, Identification cards - Integrated circuit cards -- Part 5: Registration of application providers

[18] ISO/IEC 7816-6:2004, Identification cards - Integrated circuit cards -- Part 6: Interindustry data elements for interchange

[19] ISO/IEC 9796-2:2002, Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

[20] ISO/IEC 10118-3:2004, Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

[21] ISO/IEC 10373-6:2001, Identification cards - Test methods -- Part 6: Proximity cards
[22] ISO/IEC 14443-2:2001, Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards - Part 2: Radio frequency power and signal interface
[23] ISO/IEC 14443-3:2001, Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision
[24] ISO/IEC 14443-4:2008, Identification cards - Contactless integrated circuit cards -- Proximity cards - Part 4: Transmission protocol
[25] JIS X 0201:1997, 7 ビット及び 8 ビットの２バイト情報交換用符号化漢字集合
[26] JIS X 0208:1997, 7 ビット及び 8 ビットの２バイト情報交換用符号化漢字集合
[27] JIS X 6301:2005, 識別カードー物理特性
[28] JIS X 6305-6:2001, 識別カードの試験方法ー第 6 部：外部端子なし IC カードー近接型
[29] JIS X 6306:1995, 外部端子付き IC カードー共通コマンド
[30] JIS X 6308:1999, 外部端子付き IC カードー第 5 部：アプリケーション識別子のための付番システム及び登録手続
[31] JIS X 6332-2: 2001, 外部端子なし IC カードー近接型ー第２部電力伝送及び信号インタフェース
[32] JIS X 6322-3: 2001, 外部端子なし IC カードー近接型ー第 3 部初期化及び衝突防止
[33] JIS X 6322-4: 2002, 外部端子なし IC カードー近接型ー第 4 部伝送プロトコル
[34] 外務省調査報告書「平成 18 年度　IC 旅券の高度化に係る調査」、平成 19 年 3 月、社団法人　ビジネス機械・情報システム産業協会
[35] 「IC 旅券用 IC 機能仕様（案）ー実証実験向け能動認証機能（Active Authentication）追記」、第 3.2c 版、2009 年 2 月 7 日、外務省領事局旅券課