IC 旅券用プロテクションプロファイル解説書

2009/04/28

バージョン 1.0

【目次】

1. はじめに 1

1.1. PP開発の背景 1
1.2. PP開発の目的 1

2. PPの特徴 2

3. PPの利用方法 3

4. EAL 4

5. PP主張 4

6. TOEについて 4

6.1. IC旅券システム 4
6.2. TOE種別 5
6.3. TOEのライフサイクル 5
6.4. TOEの運用環境 5
6.5. TOEの物理的範囲 6
6.6. TOEの論理的範囲 6
6.6.1. TOEの保護資産 6
6.6.2. TOEのセキュリティメカニズム 6

7. セキュリティ課題定義 8

7.1. 前提条件 8
7.2. 脅威 10
7.2.1. 個人化フェーズにおける脅威 10
7.2.2. 運用フェーズにおける脅威 11
7.3. 組織のセキュリティ方針 16
7.4. セキュリティ対策方針 18
7.4.1. TOEのセキュリティ対策方針 18
7.4.2. 運用環境のセキュリティ対策方針 21
7.4.3. セキュリティ対策方針と脅威、組織のセキュリティ方針の関係 23

8. セキュリティ機能要件 32

9. その他 35

9.1. 次期IC旅券システムの概要 35
9.2. 次期IC旅券の論理データ構造 36
9.3. 受動認証 (PASSIVE AUTHENTICATION) 37

9.3.1. CSCA証明書 37
9.3.2. DS証明書 38
9.3.3. 正当性検証の流れ 38
9.4. 基本アクセス制御(BASIC ACCESS CONTROL) 39
9.4.1. BAC認証鍵の生成 40
9.4.2. BACセッション鍵の確立 40
9.4.3. セキュアメッセージング 41
9.5. 能動認証(ACTIVE AUTHENTICATION) 42
9.5.1. 能動認証の手順 42
9.5.2. 複製防止の根拠 43
9.5.3. デジタル署名作成手順 43
10. 参考文書 45

1. はじめに

1.1. PP 開発の背景

近年、パスポートの偽変造や、成りすましによる不正使用が増加し、国際的な犯罪組織や不法な出入国に利用されている。特に 2001 年の米国同時多発テロ以降は、テロリストによるパスポートの不正使用を防止する観点から国際会議でも活発に議論され、また、米国がビザ免除継続の要件として各国にバイオメトリクスを採用したパスポートの導入を求めたことが、この議論に拍車をかけた。

パスポートは自国のみでなく世界中の国々で使用されることから国際的な相互運用性が重要とされ、ICAO（国際民間航空機関）において国際標準化作業が進められている。2003 年、ICAO は記録媒体として非接触型 IC チップを選択し、IC チップに記録する必須の生体情報として「顔画像」を採用した。

日本においても、2006 年から IC チップを内蔵したパスポート（IC 旅券）の申請受付が開始されており、IC チップに記録する必須の生体情報として「顔画像」を採用している。このことにより、顔写真を貼り替えたパスポートを使用しても、IC チップに記録されている情報と照合することにより、偽変造を見破ることが容易となる。また、IC チップに記録された情報が本人の気付かない間に読み取られることのないように､情報の暗号化や盗聴対策などの安全対策を施している。

現在採用されている第 1 世代の IC 旅券は、IC チップのセキュリティ機能として、ICAO 国際標準で必須とされている受動認証 PA（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 BAC(Basic Access Control：盗聴防止機能)を備えている。

日本の次期 IC 旅券では、IC チップのセキュリティ強化機能として、能動認証 AA(Active Authentication：クローン防止機能)の追加が検討されている。なお、次期 IC 旅券の仕様には、日本、オーストラリア、ニュージーランドが検討している能動認証の導入の他、EU 各国が追加を検討している生体情報としての指紋がある。

1.2. PP 開発の目的

今後日本での導入が予定されている、受動認証 PA 及び基本アクセス制御 BAC に加え、新たに能動認証 AA 機能を搭載した第 2 世代の IC 旅券の調達で使用できる、旅券冊子用 IC に対する IT セキュリティ要件を記述したプロテクションプロファイル*1（以下「PP」という）の作成を目的としている。

IC 旅券を開発する上で、必要十分なセキュリティ機能が備えられることを保証する最初のステップとして、PP が大変効果的な役割を持つ。適切な PP を使用することで、調達者はセキュリティの基本ニーズを正確に開発者に提示でき、開発者は、調達者の要求を満たすセ

キュリティターゲット*2（以下「ST」という）の作成が容易になる。

現在公開されている PP は、ドイツが開発した第 1 世代 IC 旅券用 PP と、EU 各国が導入する指紋入り旅券の２つであり、日本が導入しようとしている能動認証 AA を追加した PP は存在しない。日本が PP を作成し公開すると、指紋の導入は難しいが、IC チップのセキュリティ機能だけは強化しようとする国が、参照する可能性が考えられる。

*1

プロテクションプロファイル（PP ： Protection Profile)。IT 製品やシステムに関して、ある製品カテゴリを対象に必要なセキュリティ機能に関わる要件をまとめた文書。例えば、「OS」、「ファイアウォール」、あるいは「IC カード」などのカテゴリに対して PP が作成される。ある製品に関係した PP が既に公開済みである場合、その製品の ST 作成時に公開済みの PP を参照（引用）することができる。それにより、PP に含まれない、その製品固有の個所だけを ST として新たに書けばよいことになり、ST 作成が極めて容易になる。また、重要な脅威を見落としたりする恐れも減少する。PP の書き方は、IPA の Web サイトで公開されているセキュリティ評価基準「情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 改訂第 1 版 パート 1 附属書 B」で詳しく規定されている。

*2

セキュリティターゲット（ST ： Security Target)。IT 製品やシステムにおけるセキュリティ機能に関わる要件と仕様をまとめた文書。個々の IT 製品あるいはシステムごとに作成され、考慮すべき脅威や、脅威への対抗手段など、セキュリティ設計の基本方針がすべて明らかになる。ST の書き方は、IPA の Web サイトで公開されているセキュリティ評価基準「情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 改訂第 1 版 パート 1 附属書 A」で詳しく規定されている。

2. PP の特徴

本PPの特徴は以下の通りである。

(1) CC*3のバージョン

CCのバージョンは以下のバージョンを使用している。

- CC パート 1 は IPA が公開している「情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 パート 1: 概説と一般モデル 改訂第 1 版［翻訳第 1.2 版］(2007 年 4 月 18 日)」を使用する。
- CC パート 2 は IPA が公開している「情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 パート 2: セキュリティ機能コンポーネント 改訂第 2

版［翻訳第 2.0 版］(2008 年 3 月 19 日)」を使用する。

- CC パート 3 は IPA が公開している「情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 パート 3: セキュリティ保証コンポーネント 改訂第 2 版［翻訳第 2.0 版］(2008 年 3 月 19 日)」を使用する。

*3 コモンクライテリア(CC: Common Criteria)。情報技術セキュリティの観点から、IT 製品やシステムが適切に設計され、正しくその設計が実装されていることを評価するための国際標準規格である。この規格は IPA の Web サイトで「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」としてパート 1 からパート 3 までが公開されている。

(2) 第1世代IC旅券のPPとの関係

本PPの作成にあたっては第1世代IC旅券のPPの調査を行い、第1世代IC旅券のPPとの整合性に注意した。調査対象とした主なPPは以下の通りである。

- ePassport Protection Profile V1.0
  Developer: IT Security Evaluation Division, Evaluation Planning Team, KISA
  Certification Number : KECS-PP-0084-2008, Jan. 2008[5]
- Protection Profile — Machine Readable Travel Document with ICAO Application, Extended Access Control (PP-MRTD EAC)
  Registration: BSI-CC-PP-0026[8]

(3) 運用者に対するヒアリング

IC旅券の運用の知識を保有する部門(外務省の当該部門等)にヒアリングをおこない、実際の運用と不整合等が生じないように注意した。

3. PP の利用方法

PPの想定される利用方法は以下の通りである。

(1) 本PPを正式に評価・認証し、PP登録後の活用を図る。

ア) MRTDのICチップを開発する者が本PPを参照したSTを作成し、セキュリティ保証に関するISO/IEC15408の評価認証取得を図る。

(2) 参考文書としての活用を図る

ア) 指紋の導入は難しいがICチップのセキュリティは強化したいというような場合において参考とする。

イ) 他の製品分野におけるPP作成を検討する際の参考とする。

4. EAL

TOEはIC旅券に組み込まれるICチップであり、不正な入出国等を防止する目的を有していることから、高い攻撃力を持った攻撃者を想定しており、保証レベルとしてEAL4追加（追加保証コンポーネントは、ADV_IMP.2、ALC_CMC.5、ALC_DVS.2、AVA_VAN.5）とした。

5. PP 主張

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。

6. TOE について

TOEの概要は以下の通りである。

6.1. IC 旅券システム

IC旅券を使用したシステムの概要はPPに記述されている通りである。PPではIC旅券を使用したシステムを構成する要素として以下のものを識別している。

表 1 IC 旅券を使用したシステムの構成要素

構成要素	内容
IC旅券申請者	IC旅券を申請する者。 IC旅券は申請によって発行され、申請者は以後、当該IC旅券の保有者となる。
受付機関	IC旅券の申請を受け付ける機関。 受付機関は申請者に関する調査を実施し、申請受付の可否を決定する。調査には、申請者の本人確認等も含まれ、関係機関への問い合わせ等も行われる。
個人化実施機関	IC旅券発行の中心となる機関。 ICチップにデータを書込み個人化を行うほか、PKIの構築等も行う。
IC旅券の製造／開発者	IC旅券（ICチップを含む）の製造開発を行う。 ICチップに初期データ（ICチップの識別等）および認証データの書込みを行う。 認証データはICチップにデータを書き込む際に、書き込みを行う者を認証するためのデータであり、認証されたものだけがICチップにデータを書き込むことができる。 また、ICチップはデータを書き込むためのインタフェースを停止する機能を持ち、個人化機関はICチップにデータを書き込んで個人化を行った後、データを書き込むためのインタフェースを停止する。
検査システム	IC旅券に組み込まれているICチップと通信を行い、検査を行うシステム。

受付機関、個人化実施機関、IC旅券の製造／開発者は、IC旅券の運用を行う国等において異なると考えられる。これらは例であって、受付機関と個人化実施機関が同一の機関であるケースや、個人化実施機関が行うと想定している作業をIC旅券の製造／開発者がおこなうといったケースも考えられる。受付機関、個人化実施機関、IC旅券の製造／開発者は信頼できる機関であり、それぞれの国等の実態にあわせて記述されるべきである。

6.2. 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。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。

6.3. TOE のライフサイクル

PPではTOEのライフサイクルを以下の4つのフェーズでとらえている。

(1) フェーズ１：開発
(2) フェーズ２：製造
(3) フェーズ３：個人化
(4) フェーズ４：運用

しかしながら、TOEのライフサイクルをどのようなフェーズで捕らえるかは、TOEの運用環境によって異なると考えられる。TOEの運用環境によっては、開発と製造が１つのフェーズになっていたり、製造と個人化が１つのフェーズになっていたりするケースも考えられる。TOEのライフサイクルは、「6.1IC旅券システム」と同様に、それぞれの運用環境（国等）の実態に合わせて記載されるべきである。

6.4. TOE の運用環境

PPでは個人化機関がTOEにデータを書き込むことを想定している。しかしながら、「6.1IC旅券システム」で示したとおり、IC旅券システムを構成する構成要素は、国等によって異なると考えられ、TOEにデータを書き込む機関も、PPにおける想定と異なることが考えられる。データの書き込みに関する要求事項は、

- 信頼できるサブジェクトが、TOEのライフサイクルの特定のフェーズにおいてのみ書き込みができる（それ以外のサブジェクト、それ以外のフェーズにおいては書き込みできない）こと

である。

したがって、この要求事項が満たされる限り、IC旅券システムを構成する構成要素が異なってもよく、その国等の実態に従って記述されるべきである。

6.5. TOE の物理的範囲

PPではTOEの物理的範囲を、IC旅券に組み込まれるICチップ全体としている。TOEの物理的範囲としては、IC旅券全体（例：Protection Profile — Machine Readable Travel Document with ICAO Application, Extended Access Control (PP-MRTD EAC)）、ICチップ上のソフトウェア（例：ePassport Protection Profile V1.0）が存在するが、本PPにおけるTOEの物理的範囲は、ICチップである。

6.6. TOE の論理的範囲

TOE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。TOEの論理的範囲はPPに記載されている通りである。

6.6.1. TOE の保護資産

TOEの保護資産はPPに記載されている通りである。

TOEはICチップに記録されている利用者データならびに利用者データを保護するためのセキュリティ機能が参照するTSFデータを保護資産としている。さらにセキュリティ機能に影響を与えるおそれのあるテンポラリデータもあわせて保護資産としている。

6.6.2. TOE のセキュリティメカニズム

TOEはBAC、AA等のセキュリティメカニズムを実装する。これらのセキュリティメカニズムはPPに記述されている通りであるが、それぞれのメカニズムの概要は以下の通りである。

(1) PA(Passive Authentication)

ICAO（International Civil Aviation Organization）で規定されている。

これは、データの改竄を検出するための機能である。ICチップに記録されているデータのハッシュ値（秘密鍵で署名）を同チップに記録しておき、ICチップから読み出したデータのハッシュ値を計算し、同チップから読み出したハッシュ値と比較することで、データが改竄されているかどうかを検査する。

(2) BAC(Basic Access Control)

ICAO（International Civil Aviation Organization）で規定されている。

これは、セキュアな通信（暗号通信）を実現するための機能である。セキュアな通信のために暗号鍵の交換を行うが、この鍵交換にあたっては、TOEの通信相手である検査システムが、IC旅券に記載されているOCR文字から鍵を生成する必要があり、この鍵生成ができない場合、鍵交換は成立せず、通信はおこなわれない。

(3) AA(Active Authentication)

ICAO（International Civil Aviation Organization）で規定されている。

これは、TOE(ICチップ)のクローンが作成されることを防止するための機能である。TOE(ICチップ)のデータ領域はセキュアメモリと呼ばれる読出し不能な領域とそうでない領域で構成されており、TOE(ICチップ)がセキュアメモリに書き込まれている秘密鍵で暗号化した値を、検査システムがTOE(ICチップ)から読み出した公開鍵で復号し、その結果を確認することでTOE(ICチップ)の真正性を確認する。TOE(ICチップ)のクローンを作成するためにTOE(ICチップ)のコピーを作成したとしても、セキュアメモリに書き込まれているデータはコピーされないため、上記の検証を行うことにより、コピーにより作成されたTOE(ICチップ)は認証されない。

(4) アクセス制御機能

これは認証された個人化担当者のみがTOEにデータを書き込めるようにするための機能である。データの書込みは

- TOEのデータ書込みインタフェースを有効化する（この方法ならびに有効化に必要なパラメタ等は個人化担当者だけが知っている）
- 個人化担当者はTOEに対して認証操作を行う。
- 認証が成功した場合、データの書込みが可能となる。

といった手順でおこなわれる。

個人化の完了時に個人化担当者はTOEのデータ書込みインタフェースを停止することから、個人化の完了後、個人化担当者以外のものは、TOEのデータ書込みインタフェースを呼び出すことはできない。

(5) 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

これはTOEのセキュリティ機能を物理的な改竄や干渉から保護する機能である。

(6) バイパス防止

これはTOEのセキュリティ機能がバイパスされないことを保証する機能である。セキュリティ機能のバイパスは、セキュリティ機能による保護がバイパス（迂回）されることを意味する。TOEはこのバイパスを防止する。

(7) ドメイン分離

これはセキュリティドメインを分離する機能である。これにより信頼できないプロセスがセキュリティ機能にアクセスして変更を行うことを回避する。

(8) 自己テスト

これはTOEのセキュリティ機能を自己テストし異常を検出する機能である。これにより、TOEのセキュリティ機能に障害が生じている状態で運用がおこなわれることを防止する。自己テストは通常TOEの起動時等に行われる。

(9) 障害発生時のセキュアな状態の維持

これは障害が発生した場合においても、TOEが正しい運用を維持することを保証する機能である。TOEは識別された障害が発生した場合に、識別した能力の正しい運用を続けることを保証する。

(10) TSFデータの完全性保護

これは送信中（TOEと検査システムの間など）のTSFデータの完全性を保護する機能である。

(11) 観察不能性

これは他者が資源あるいはサービスが使用されていることを観察できない状態で利用者がその資源あるいはサービスを使用できることを保証する機能である。

7. セキュリティ課題定義

7.1. 前提条件

本PPにおける前提条件は4つである。

表 2 前提条件

前提条件	解説
A. Personalization Agent	個人化担当者に関する前提条件である。 個人化担当者はTOEに対してデータの書込みを行うことができるが、TOE は書き込まれるデータに対するチェックを行わない。 そのため、個人化担当者はTOEにデータを書き込むにあたり、正しいデータを書き込む必要がある。また、プログラムを格納する場合は、格納するプログラムがTOEのセキュリティに影響を及ぼさないことを個人化担当者の責任で保証しなければならない。 注意）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。たとえばAAの鍵の登録を個人化担当者がおこなうのではなく旅券製造者がおこなうといったことも考えられる。これらの行為を個人化担当者、旅券製造者のいずれがおこなうのかといった点については、運用環境にあわせて決定されるべきである。また、プログラムの格納については、プログラムの格納をおこなわないような運用環境においてはこの前提は不要である。
A. Certificate Verification	PA を利用するための前提条件である。 TOE にはデータの改竄を検出するためのハッシュ値（秘密鍵で署名）が書き込まれているが、検証す

	るためには、公開鍵を使用した復号処理が必要となる。検証は検査システムが行うが、公開鍵の有効性を確認するためには証明書と CRL を定期的に確認する必要がある。 注意）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。
A. Inspection System	検査システムに関する前提条件である。 TOE が実装するセキュリティ機能が有効に動作するためには、TOE の通信相手となる検査システムが TOE のセキュリティ機能に対応していなければならない。 注意）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。
A. MRZ Entropy	BAC 認証鍵の種のエントロピーに関する前提条件である。BAC 認証鍵の種とは IC 旅券に記載される OCR 文字のことであり、この種のエントロピーが BAC 認証鍵の強度を決定する。 注意）OCR 文字については別途規定が存在するなどにより、この前提条件を設けることが適切出ないケースも考えられる。そのような場合、この前提条件は定義されない。

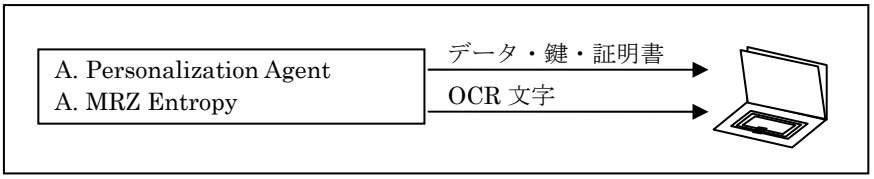

図 1 TOE のデータ等に関する前提条件

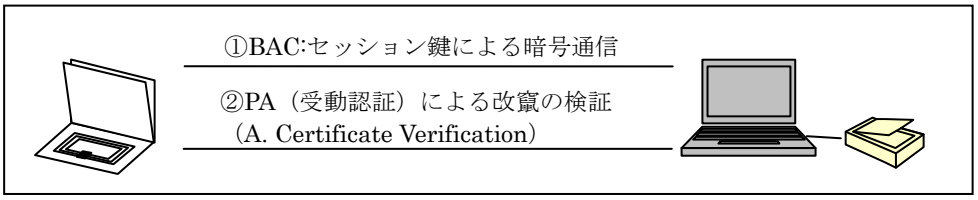

図 2 BIS（BAC に対応した検査システム）

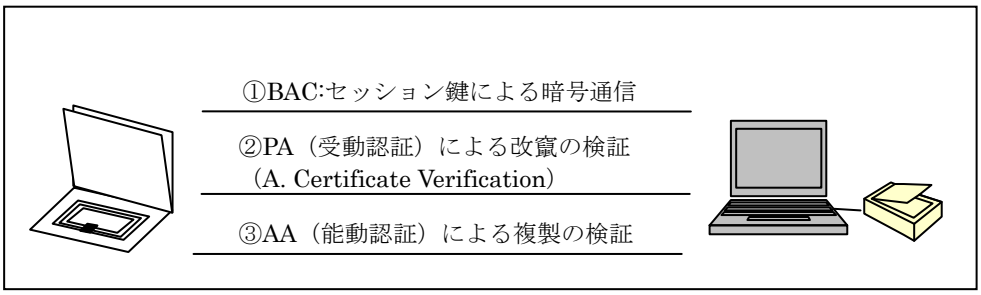

図 3 AIS（AA に対応した検査システム）

7.2. 脅威

本PPにおける脅威は12個である。

7.2.1. 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、個人化のためのデータの書き込み等がおこなわれることから、以下の２つの脅威を識別している。

表 3 個人化フェーズにおける脅威

脅威	解説
T. Application Program Interference	個人化フェーズにおいては、TOE へのデータの書き込みインタフェースが有効化されていることから、攻撃者が個人化担当者に代わって TOE に対して不正なプログラムをロードする可能性がある。 不正なプログラムとしては、運用時にセキュリティ機能をパイパスしたり、非活性化するなどの機能もったプログラムが考えられる。
T. TSF Data Modification	攻撃者が不正な検査システムを利用して TOE へ不正なプログラムをロードすることを脅威としている。 T. Application Program Interference が攻撃者が個人化担当者に代わって書き込みインタフェースを使用することを想定しているのに対し、この脅威

	は、TOE が検査システムと通信をおこなうことを悪用し、不正な検査システムから TOE にアクセスすることで、TOE が検査システムとの通信において想定していないような命令・要求を送信し、それにより、TOE に格納されているデータを改竄することを脅威としている。

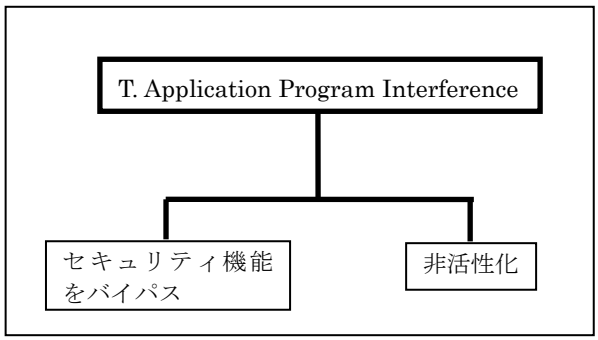

図 4 脅威（T. Application Program Interference）

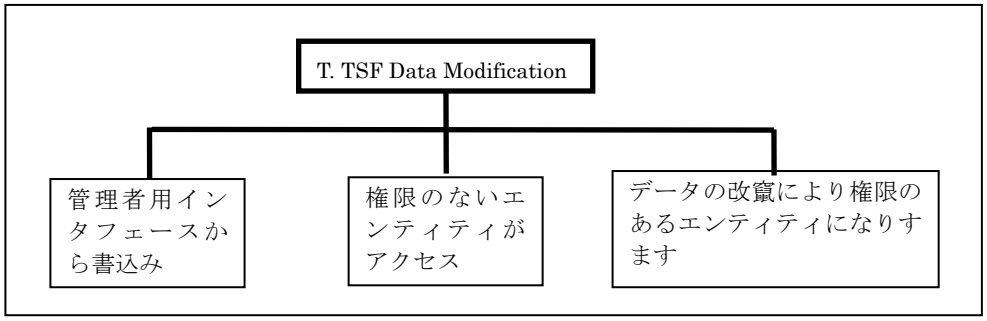

図 5 脅威（T. TSF Data Modification）

7.2.2. 運用フェーズにおける脅威

運用フェーズにおいては、TOEに対してデータを書き込むインタフェースが停止されていることから、TOEに書き込まれているデータの不正な読み取りに関係する脅威を識別している。

7.2.2.1. 運用フェーズにおける BAC 関連の脅威

BACはTOEに記録されているデータを保護するために、アクセス制御ならびに暗号通信をおこなう。BACの機能を侵害し、データが読み取られる脅威として、５つの脅威を識別している。

表 4 運用フェーズにおける BAC 関連の脅威

脅威	解説
T. BAC Authentication Key Disclose	BAC は認証に成功した場合のみ通信をおこなう機能であることから、TOE に書き込まれている BAC 認証鍵が不正に読み出されることを脅威としている。BAC 認証鍵を読み出した攻撃者はその鍵を使用して認証に成功し、TOE との通信をおこなうことができる。
T. BAC Replay Attack	認証をおこなう際に TOE と検査システムの間でやり取りされるデータを収集しておき、TOE に対して収集しておいたデータを送信することで、検査システムに成りすまされること、そして、その結果、TOE に書き込まれているデータが読み出されることを脅威としている。
T. Eavesdropping	TOE に記録されているデータは検査システムに対して送信されることから、このデータを盗聴することで、TOE に記録されているデータを取得されることを脅威としている。
T. Forgery and Corruption of Personal Data	TOE は検査システムと通信をおこなうことを想定している。そこで不正な検査システムを使用して TOE との通信がおこなわれ、TOE に書き込まれているデータが読み出されることを脅威としている。
T. Skimming	攻撃者が TOE が実装している通信インタフェースを使用せず、TOE から直接データを読み出すことを脅威としている。

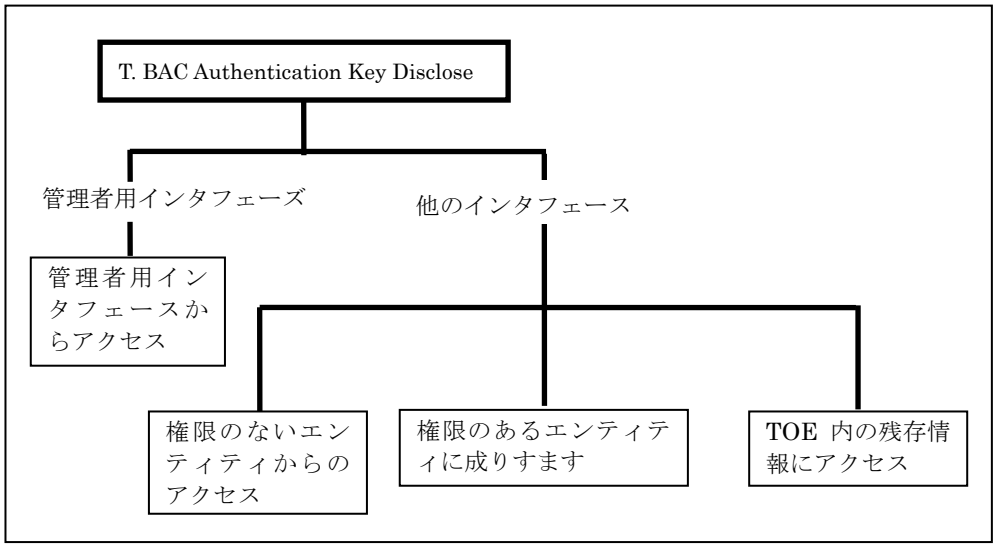

図 6 脅威（T. BAC Authentication Key Disclose）

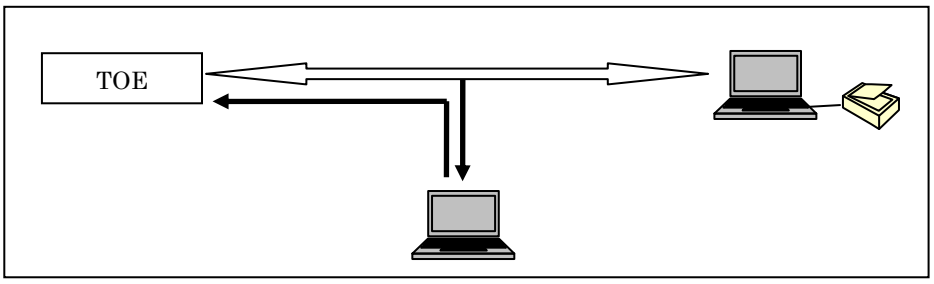

図 7 脅威（T. BAC Replay Attack）

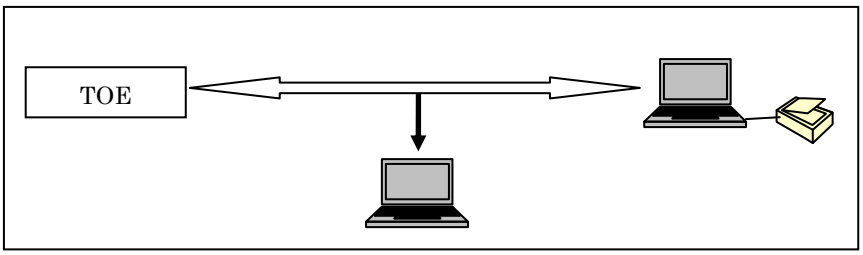

図 8 脅威（T. Eavesdropping）

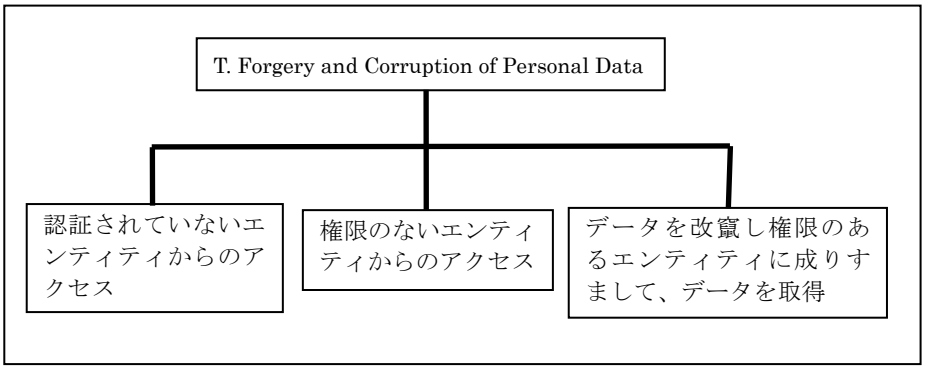

図 9 脅威（T. Forgery and Corruption of Personal Data）

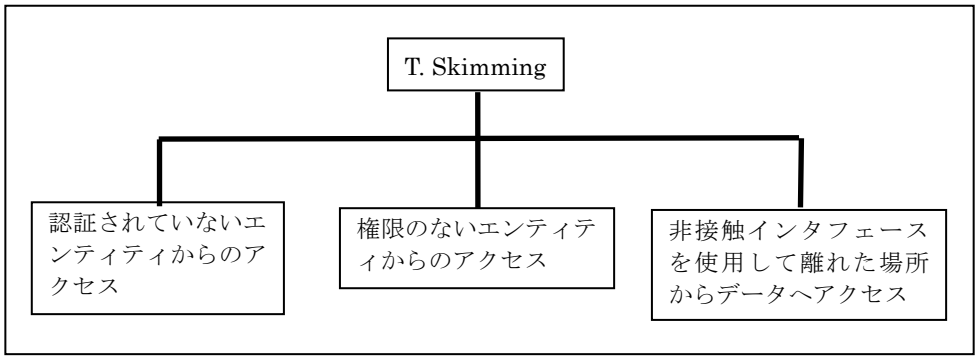

図 10 脅威（T. Skimming）

7.2.2.2. 運用フェーズにおける IC チップへの脅威

運用フェーズにおけるICチップへの直接の脅威として、１つの脅威を識別している。

表 5 運用フェーズにおける IC チップへの脅威

脅威	解説
T. Malfunction	TOE は IC チップである。そのため、物理的な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すことを脅威としている。

7.2.2.3. 運用フェーズにおけるその他の脅威

運用フェーズにおけるその他の脅威として、１つの脅威を識別している。

表 6 運用フェーズにおける IC チップへの脅威

脅威	解説

T. ePassport Reproduction	IC 旅券の偽造である。 IC 旅券は TOE である IC チップと冊子部分から構成されているが、この IC 旅券が偽造されることを脅威としている。TOE が偽造に対抗することで、TOE を含む IC 旅券の偽造に対抗する。
T. Leakage of Cryptographic Key Information	TOE に対して電力解析を行い、TOE 内でおこなわれている演算等を特定し、暗号鍵の解読がおこなわれることを脅威としている。
T. Residual Information	一時的な記憶に残るデータが読み取られ悪用されることを脅威としている。 一時的な記憶としては一般にメモリ等が考えられる。TOE が処理をおこなうために TOE に書き込まれているデータを作業領域に読出し、その作業領域上で演算をおこなうといったケースが考えられる。このような場合において、当該メモリ上に残存しているデータが読み出され悪用されることを脅威としている。
T. Phys Tamper	TOE に対するプローブ解析を脅威としている。 T. Leakage of Cryptographic Key Information との違いは、T. Leakage of Cryptographic Key Information が TOE から漏れる情報をもとに解析を試みるのに対して、本脅威は TOE に対して物理的な処理（探針を刺す、改変を加える等）を伴うことである。

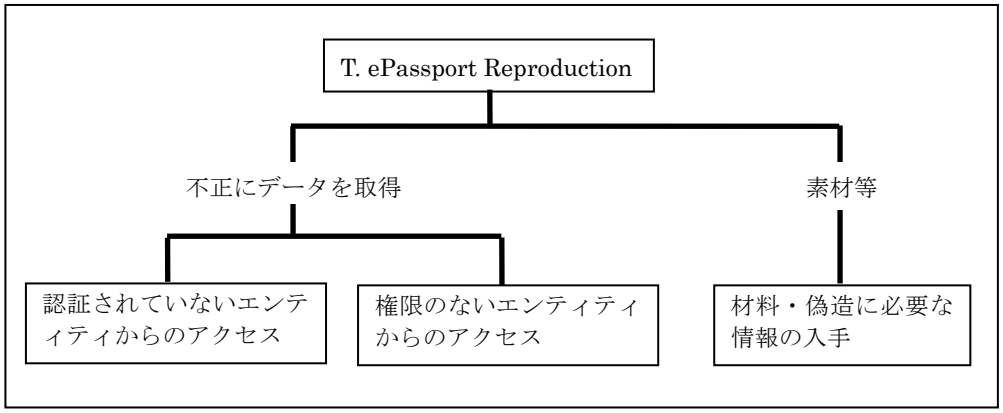

図 11 脅威（T. ePassport Reproduction）

7.3. 組織のセキュリティ方針

本PPにおける組織のセキュリティ方針は7個である。

表 7 組織のセキュリティ方針

方針	解説
P. ePassport Access Control	アクセス制御ポリシーの構築を組織のセキュリティ方針にしている。 アクセス制御ポリシーは IC 旅券の運用主体によって決定されるべきものであるが、旅券が多国間で利用されるものであることを踏まえ、ここで定義することによりアクセス制御ポリシーの統一的な設定を求めている。 注意）本 PP は個人化担当者がアクセス制御ポリシーを設定することを想定しているが、アクセス制御ポリシーを固定することも考えられる。この場合、アクセス制御ポリシーは TOE の製造時に設定・固定され、以後、設定や変更といったフェーズは存在しないことになる。
P. International Compatibility	TOE のセキュリティメカニズムは､検査システムが当該メカニズムに対応していなければ効果が期待できない。そのため､TOE に対して設定を行う個人化担当者が検査システムとの整合性を保証することを求めている。 注意）個人化担当者が整合性を保証する手段については､TOE の運用環境に合わせて検討されるべきである。TOE を搭載した IC 旅券の運用は多国間にまたがることが考えられ、このような対策方針を設定することが現実にそぐわない場合は、この対策方針を定義しないことも考えられる。
P. PKI	TOE のセキュリティメカニズムは PKI を使用する。そのため、IC 旅券の発行国が、CPS に準拠した電子署名鍵、証明書の管理を行うことを求めている。また、証明書には有効期限が設定されることを考慮し､IC 旅券の発行国が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求めている。

	注意）PKI の仕組みは、IC 旅券の運用に関わる各国が参加することにより可能となるものである。しがたって、TOE の運用主体が単独で実現できるものではなく、実態に応じて、この対策方針を定義しないことも考えられる。
P. Personalization Agent	IC 旅券の運用フェーズへの移行について個人化担当者が責任を持つことを求めている。 TOE はデータの書き込みインタフェースを実装するとともに、当該インタフェースを停止する機能を実装する。これらのインタフェース、機能は個人化担当者に対して提供されるものであり、これらを有効に機能させるため、個人化担当者に対して、運用フェーズへの移行にあたり、書き込みインタフェースを停止することを求めている。
P. Range of RF Communication	TOE が非接触インタフェースを持つことに基づく方針である。通信できる距離を制限するとともに、冊子を開かなければ通信できないようにすることで、遠隔地からの TOE の追跡をできないようにする。 注意）本 PP では、TOE が通信できる距離を 5cm 未満とすることで遠隔地からの TOE の追跡を防止することを想定しているが、このような方針を設けるかどうかは ST の開発者が決定すべきである。また、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するということは、IC 旅券冊子に電波を遮断する材質の板を入れるなどして、冊子を開かない限り通信ができないようにすることを想定したものであるが、このような方針が必要かどうかは ST の開発者が決定すべきである。
P. Security Mechanism Application Procedures	TOE が提供するセキュリティメカニズムは個人化担当者のアクセス制御ポリシーに反しないものでなければならない。これは個人化担当者のアクセス制御ポリシーに反してデータを送信したりデータへのアクセスを許可するようなメカニズムの実装を防止する目的がある。

	また、TOE のセキュリティメカニズムは検査システムと整合が取れていない場合、実効が期待できなくなることから、検査システムとの整合をとらなければならない。 注意）検査システムの運用主体は TOE の運用主体と異なることが考えられ、検査システムが提供するセキュリティメカニズムを保証できないケースが考えられる。そのような場合、この対策方針は定義すべきではない。
P. Manufact	IC 製造者ならびに旅券製造者に関する方針である。 注意）TOE の品質、一意な識別、初期データ等に関する方針であるが、IC 製造者、旅券製造者、個人化担当者の役割分担については、IC 旅券を運用する運用主体によって異なることが考えられることから、それぞれの運用主体（国等）の実態にあわせて定義されるべきである。

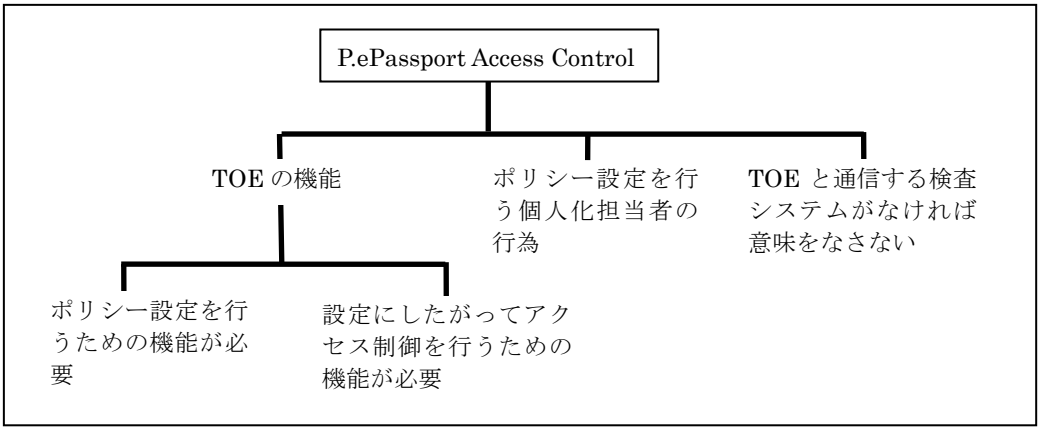

図 12 組織のセキュリティ方針（P.ePassport Access Control）

7.4. セキュリティ対策方針

本PPにおけるセキュリティ対策方針はTOEのセキュリティ対策方針、運用の環境のセキュリティ対策方針をあわせて21個である。

7.4.1. TOE のセキュリティ対策方針

本PPにおけるTOEのセキュリティ対策方針は13個である。

表 8 TOE のセキュリティ対策方針

No.	方針	解説
1	O.Access Control	個人化担当者のアクセス制御方針を実現するために、TOE がアクセス制御機能を提供することを求めている。 注意）P. ePassport Access Control との整合性に注意する必要がある。本 PP では個人化担当者がアクセス制御ポリシーを設定するという想定のもとに本対策方針を定義していることから、P. ePassport Access Control に対する修正は、この対策方針にも及ぶ。
2	O.BAC	BAC の実装を求める対策方針である。BAC については PP に記述されている通りである。
3	O.Certificate Verification	証明書の自動更新に関する対策方針である。TOE に書き込まれている証明書を更新するために TOE を都度個人化担当者に戻すということは非現実的であることから、TOE に書き込まれている証明書の更新は自動化する必要がある。 注意）P. PKI との整合性に注意して定義する。P.PKI が定義されない場合、この対策方針も定義されない。
4	O.Deleting Residual Information	TOE のセキュリティに関する情報が残存することを防止することを求める対策方針である。 メモリなどの作業領域にセキュリティに関する情報が残存し、それが読み取られて悪用されることを防止する。これは処理終了時に確実に消去をおこなうことで達成される。
5	O.Handling Information Leakage	TOE が暗号処理を実行中に漏出する情報（電力など）が利用されることを防止することを求める対策方針である。 暗号処理の分野では、電力解析による暗号鍵取得の可能性などが研究されており、それらを防止することを意図している。
6	O.Management	個人化担当者が TOE にデータを書き込むための機能を提供するとともに、個人化担当者が書き込み用インタフェースを停止する機能を提供することを求める対策方針である。 書き込みインタフェースが有効になっている場合は、

		書き込みを個人化担当者のみに制限することで不正なデータ等が書き込まれることを防止し、運用フェーズなど、TOE が個人化担当者の管理下を離れる場合においては、書き込みインタフェースを停止することで、より強く不正な書き込みを防止する。 注意）本 PP では、TOE が書き込みのための外部インタフェースを持ち、個人化担当者のみがその外部インタフェースの起動・停止を制御できることを想定しているが、TOE の書き込みインタフェースの停止を永久的なものとし、一度停止したら 2 度と起動できないようにすることも考えられる。この場合、TOE は、なんらかの操作によって書き込み不可にすることができることを保証すればよく、場合によっては、書き込み不可にする操作を個人化担当者などの特定の役割に制限する必要もないかもしれない。 この方針は、TOE の運用フェーズへの移行に責任をもつ役割を明確にすること、ならびに、運用フェーズにおいては TOE に対するデータの書き込みを禁止することを主張しているものであり、詳細は ST の開発者が定義すべきである。
7	O.Replay Prevention	BAC によって暗号通信をおこなう際に、セッションごとに異なる鍵が生成されることを求める対策方針である。
8	O.Secure Messaging	TOE が送信データの完全性と機密性を保証することを求める対策方針である。 TOE から送信されるデータには保護資産であるデータが含まれる場合があり保護する必要がある。また、TOE が受信するデータは保護資産へのアクセスを許可するか否かの判断に使用されるデータが含まれるため、こちらもまた保護する必要がある。
9	O.Security Mechanism Application Procedures	TOE に IC 旅券検査手順の実行を求める対策方針である。 TOE は確実に IC 旅券検査手順を実行しなければならない。 注意）IC 旅券検査手順は検査システムが該当する機能を実装し、実施することが必要で、TOE だけで実

		行することはできない。したがって、検査システムでこれらの機能が実装・実施されることが保証されない場合、TOE はこれらの機能を実装し、検査システムが対応している場合、確実に実施しなければならないといった定義に変更することが考えられる。
10	O.Self protection	TOE に自分自身を改竄から保護する機能を実装することを求める対策方針である。 TOE は自分自身を改竄から保護し、セキュアな状態を維持しなければならない。
11	O.Session Termination	アンセキュアな状態が生じることを防止するための対策方針である。 認証が失敗した場合、データの改竄を検知した場合などは直ちにセッションを終了し、不正な通信がおこなわれないようにしなければならない。
12	O.Prot Phys Tamper	TOE に書き込まれているソフトウェアやデータを物理的な攻撃から保護することをもとめる対策方針である。
13	O.Range of RF Communication	TOE の非接触インタフェースが悪用されることを防止するための対策方針である。 遠隔地から TOE を追跡されたり、遠隔地から不正なアクセスを受けたりすることを防止することを求めている。 注意）P. Range of RF Communication との整合性に注意して定義する。P. Range of RF Communication が定義されない場合、この対策方針も定義されない。

7.4.2. 運用環境のセキュリティ対策方針

本PPにおける運用環境のセキュリティ対策方針は8個である。

表 9 運用環境のセキュリティ対策方針

No.	方針	解説
1	OD.Assurance	TOE の設計・製造において求められる対策方針である。 TOE の設計・製造においてセキュリティを考慮することを求めている。 また、設計・製造過程において必要なデータの書き込みについても記述している。

		注意）TOE の設計・製造における対策方針であるが、IC 製造者、旅券製造者などの役割ならびにその役割に関する対策方針は、TOE のライフサイクルに合わせて ST の開発者によって具体的に決定されるべきである。 製造フェーズから個人化フェーズに移行した時点において TOE は個人化担当者のみが書き込み可能な状態になっており、製造フェーズにおいて脆弱性が入り込まないことを求めている。
2	OD.Material	TOE の製造者に求められる対策方針である。 TOE は IC チップであり、旅券冊子に組み込まれるが、偽造を防止するために、その材料・製造工程等を管理することを求めている。
3	OE. Personalization Agent	個人化担当者に求められる対策方針である。 個人化担当者がセキュリティに関する役割を果たす上で実行しなければならない行為を記述している。 注意）A. Personalization Agent との整合性に注意して定義する必要がある。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、A. Personalization Agent に対する変更は、この対策方針にも及ぶ。
4	OE. Certificate Verification	検査システムに求められる対策方針である。 検査システムに対して証明書の検証ならびに SOD の検証をおこなうことを求めている。証明書ならびに SOD は TOE に書き込まれているがその検証をおこなうのは検査システムである。 注意）A. Certificate Verification との整合性に注意して定義する必要がある。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、A. Certificate Verification に対する変更は、この対策方針にも及ぶ。
5	OE. Inspection System	検査システムに求められる対策方針である。 TOE のセキュリティ機能が実効性をともなったものとなるためには、PA、BAC、AA において TOE の通信相手が実装すべき機能を検査システムが実装している必要がある。そこで、検査システムに求められる機能を記述している。 注意）P. Security Mechanism Application Procedures と

		の整合性に注意して定義する必要がある。検査システムの運用主体は TOE の運用主体と異なることが考えられ、P. Security Mechanism Application Procedures に対する修正は本対策方針にも及ぶ。
6	OE. MRZ Entropy	BAC 認証鍵の種のエントロピーに関する対策方針である。 BAC の認証鍵は旅券冊子に印刷されている OCR 文字を種にすることから、この種（OCR 文字）は十分なエントロピーを持つ必要がある。 注意）A. MRZ Entropy との整合性に注意して定義する必要がある。A. MRZ Entropy に対する修正は本体策方針にも及ぶ。
7	OE. PKI	TOE のセキュリティメカニズムに関わる鍵、証明書に関する対策方針である。 この鍵や証明書は TOE の運用主体によってセキュアに管理されなければならない。 注意）A. Certificate Verification との整合性に注意して定義する必要がある。A. Certificate Verification に対する修正は本体策方針にも及ぶ。
8	OE. Procedures of ePassport holder Check	検査システムの運用者に求められる対策方針である。 検査システムを利用し検査をおこなう者（検査者）に求められる行為を記述している。 注意）これは検査システムの運用者に求められる対策方針である。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、このような対策方針を定義することが現実にそぐわない場合、この対策方針を定義しないケースも考えられる。

7.4.3. セキュリティ対策方針と脅威、組織のセキュリティ方針の関係

セキュリティ対策方針と脅威、組織のセキュリティ方針の関係を以下に図で示す。

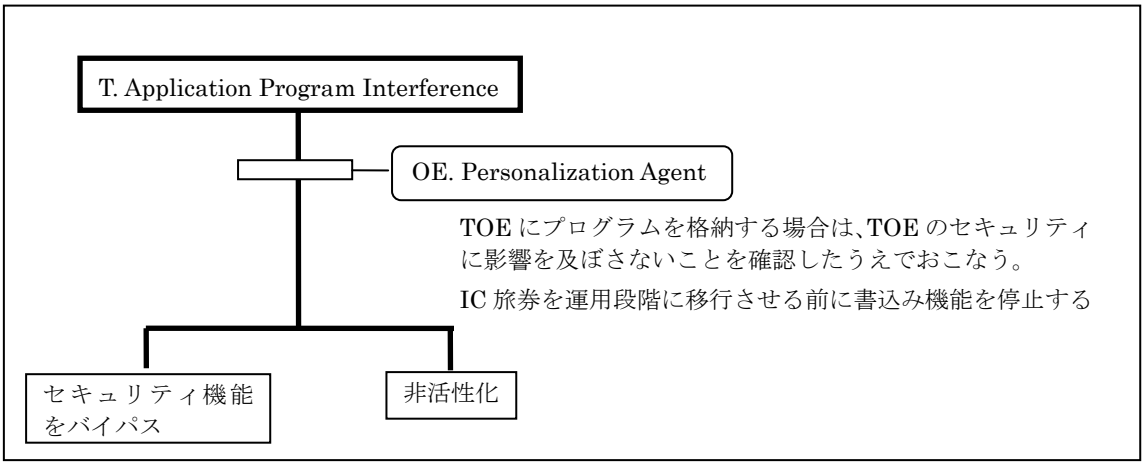

図 13　脅威（T. Application Program Interference）と対策方針の関係

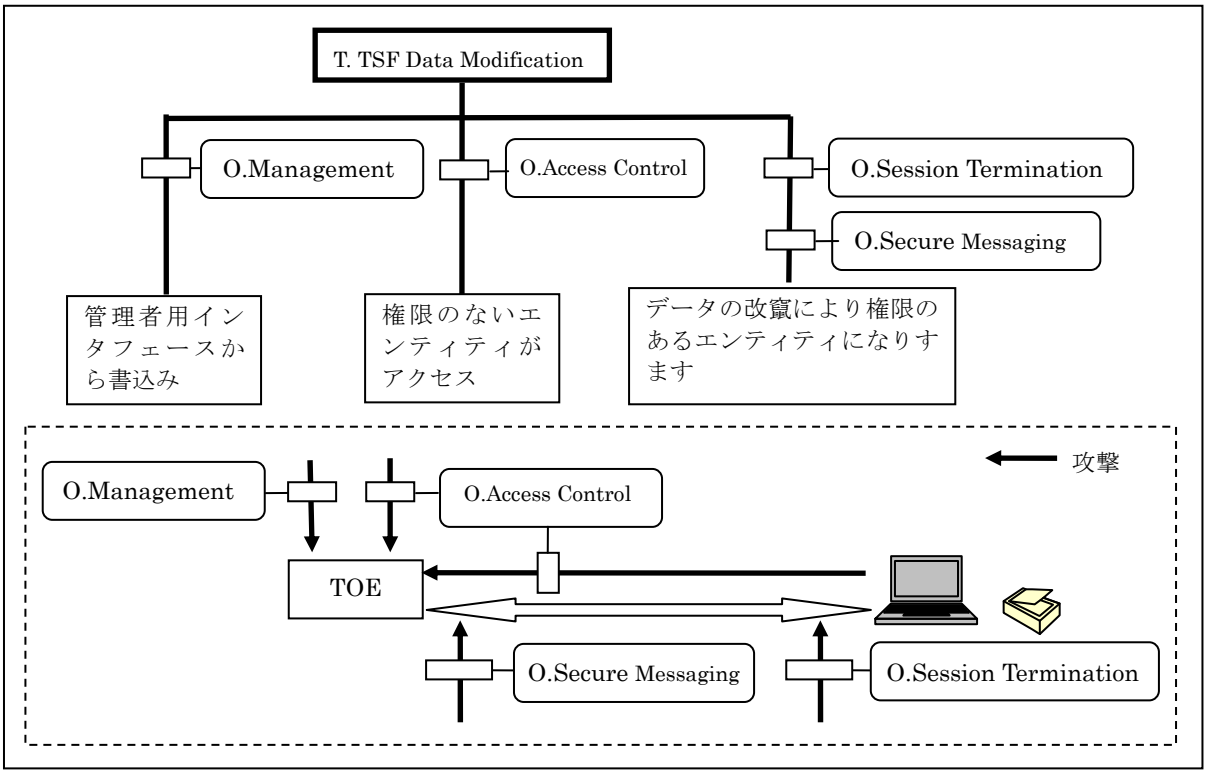

図 14　脅威（T. TSF Data Modification）と対策方針の関係

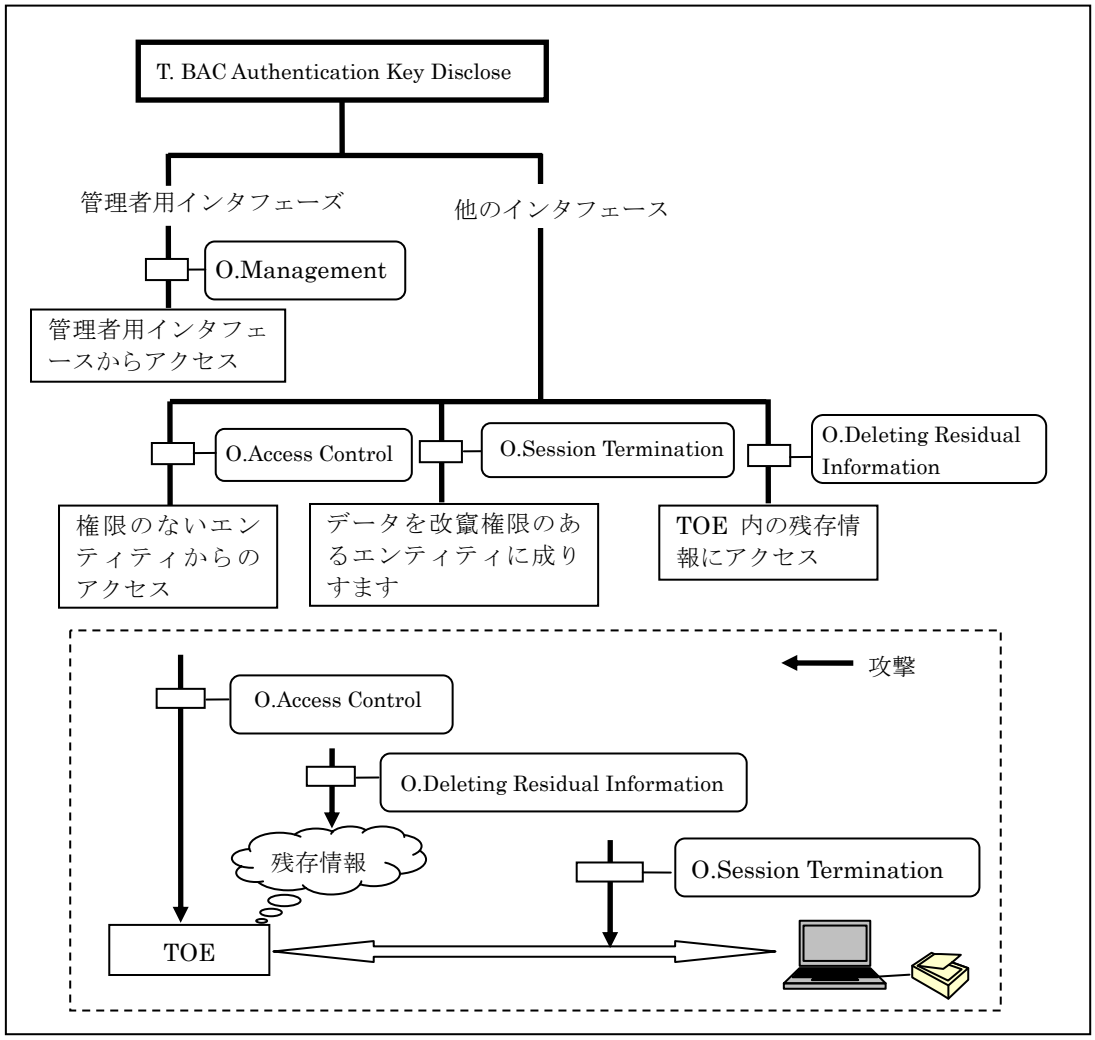

図 15　脅威（T. BAC Authentication Key Disclose）と対策方針の関係

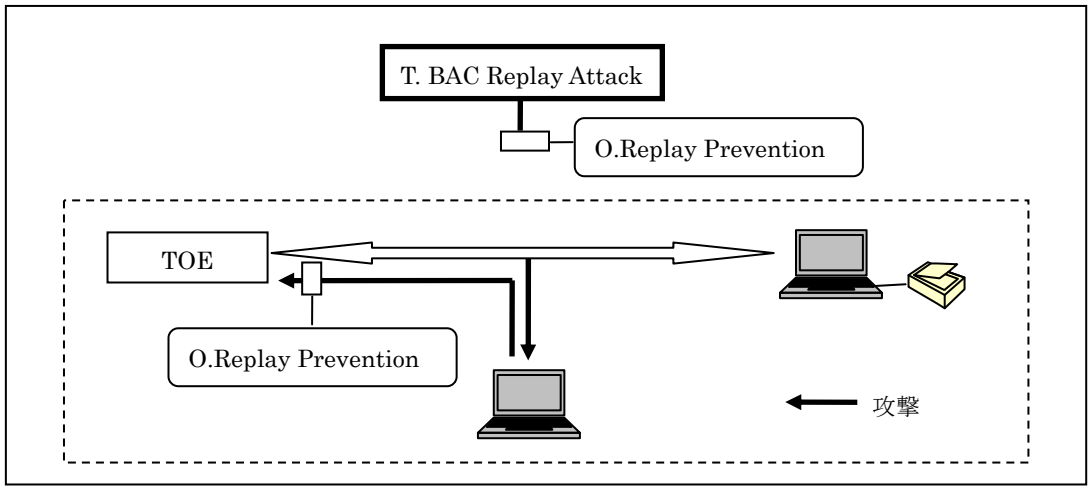

図 16　脅威（T. BAC Replay Attack）と対策方針の関係

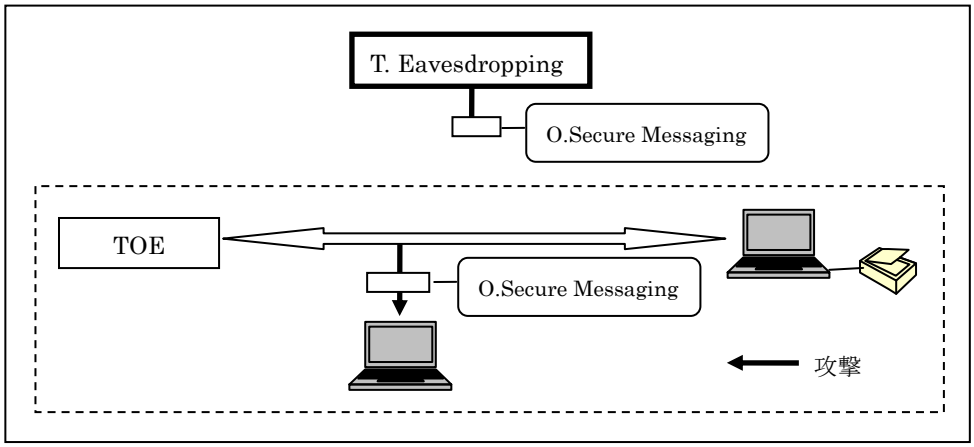

図 17　脅威（T. Eavesdropping）と対策方針の関係

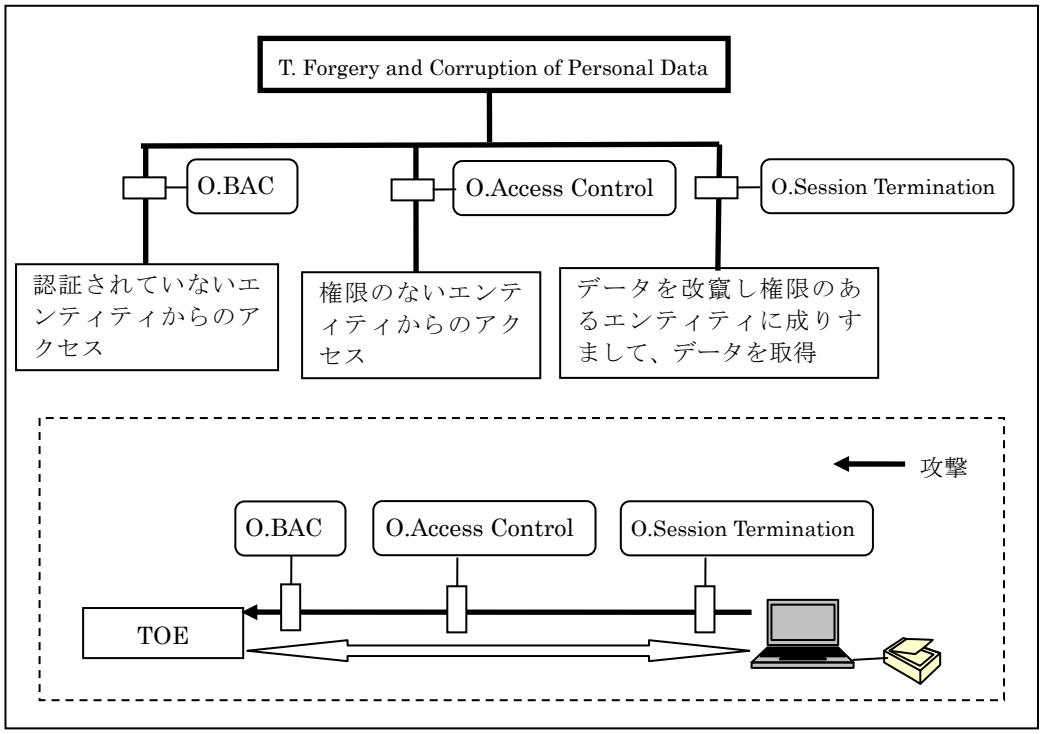

図 18　脅威（T. Forgery and Corruption of Personal Data）と対策方針の関係

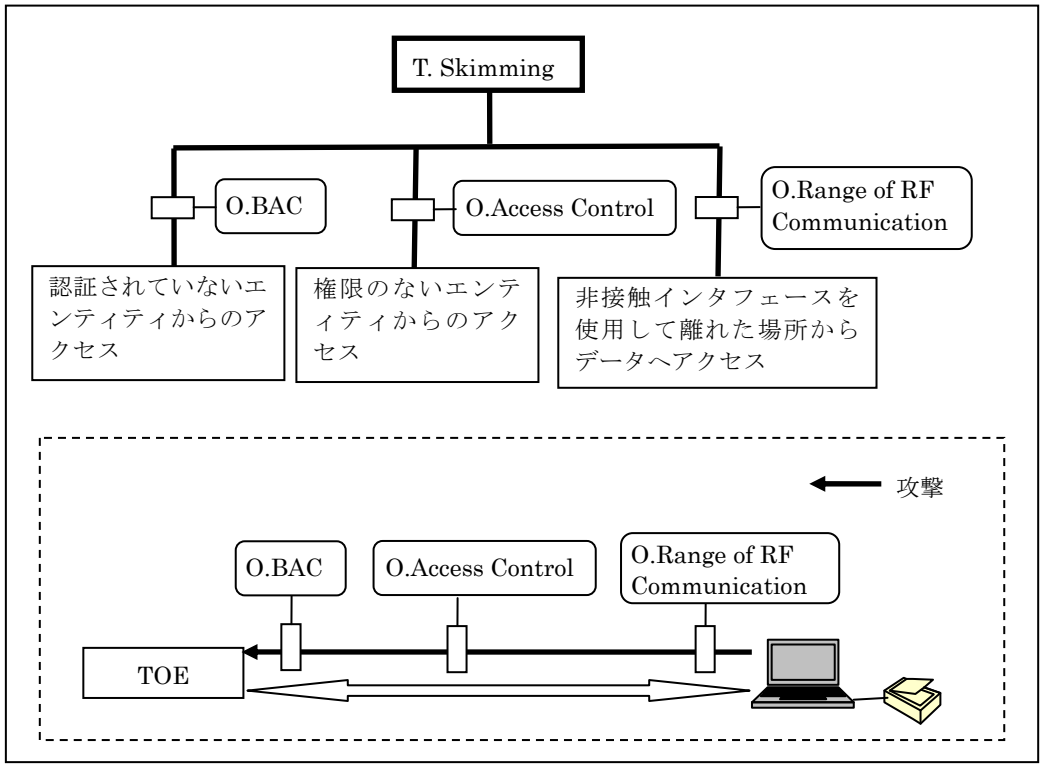

図 19　脅威（T. Skimming）と対策方針の関係

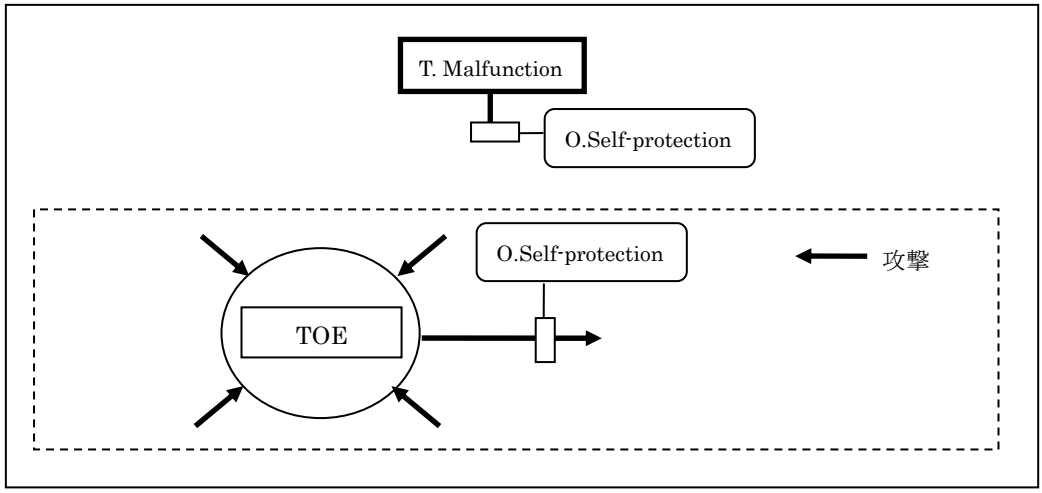

図 20　脅威（T. Malfunction）と対策方針の関係

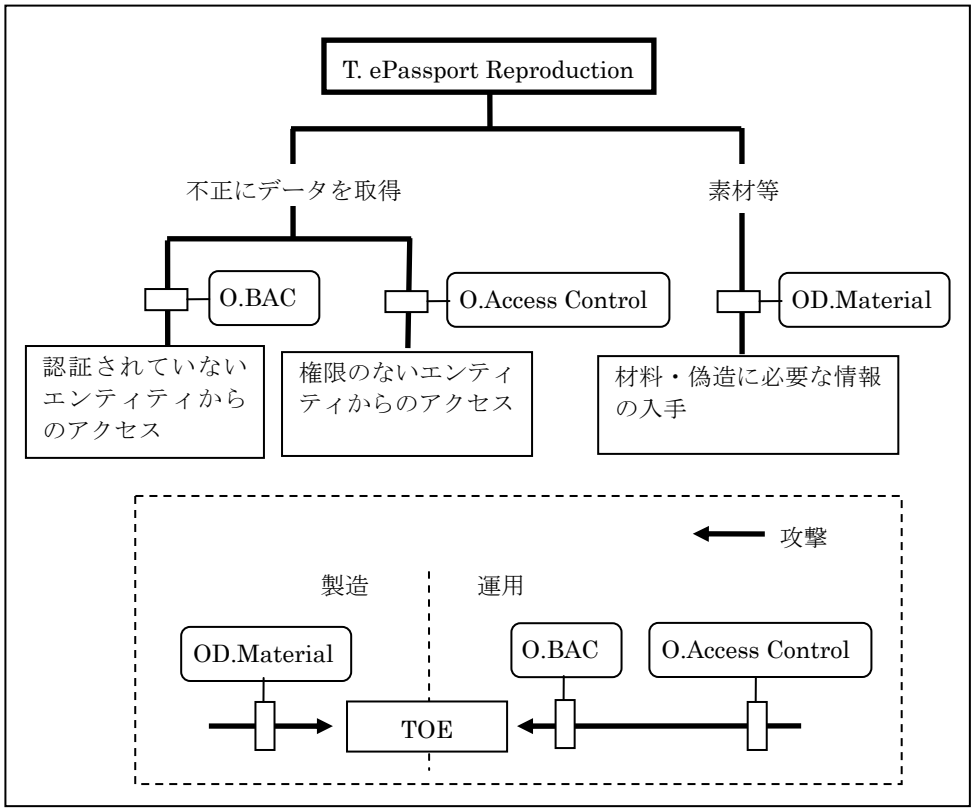

図 21　脅威（T. ePassport Reproduction）と対策方針の関係

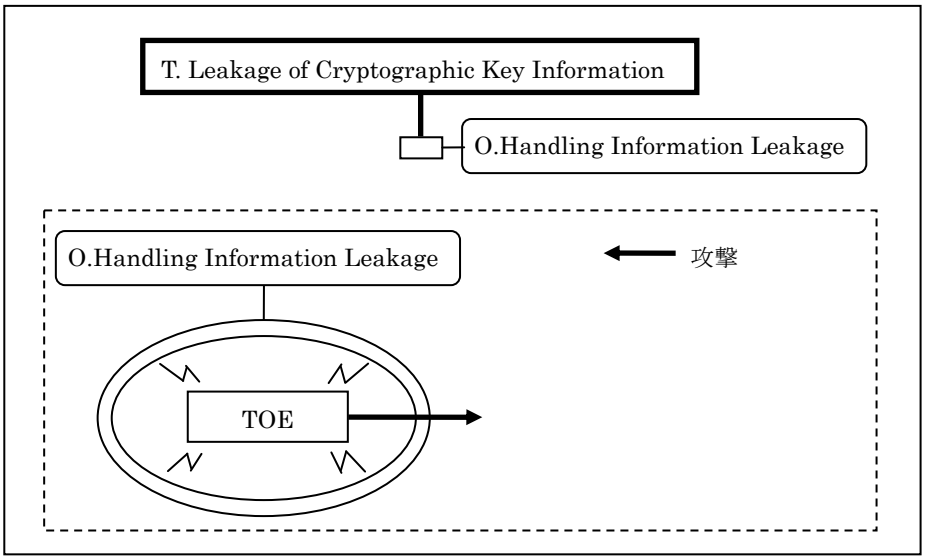

図 22　脅威（T. Leakage of Cryptographic Key Information）と対策方針の関係

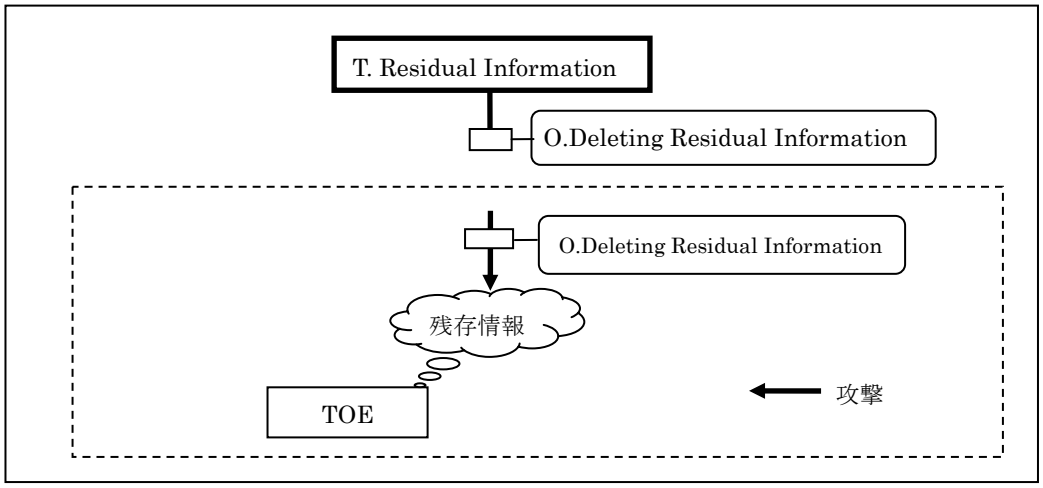

図 23　脅威（T. Residual Information）と対策方針の関係

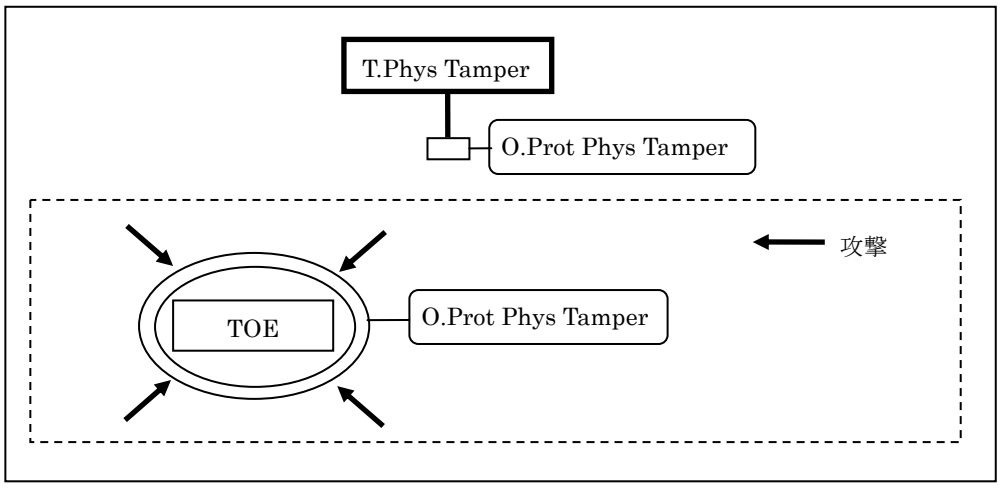

図 24　脅威（T.Phys Tamper）と対策方針の関係

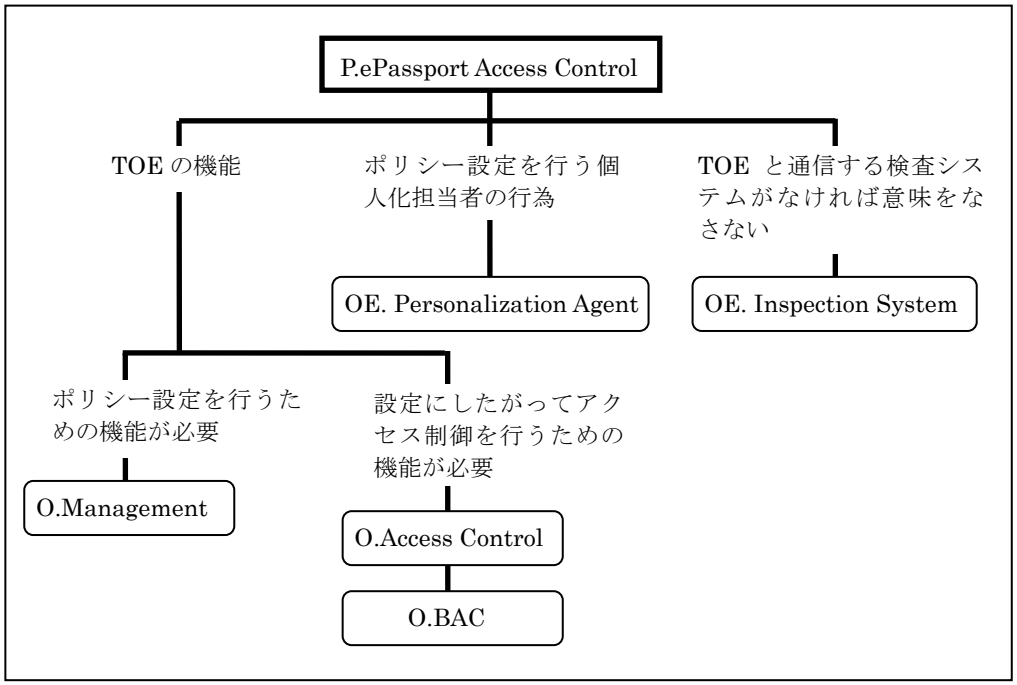

図 25　組織のセキュリティ方針（P.ePassport Access Control）と対策方針の関係

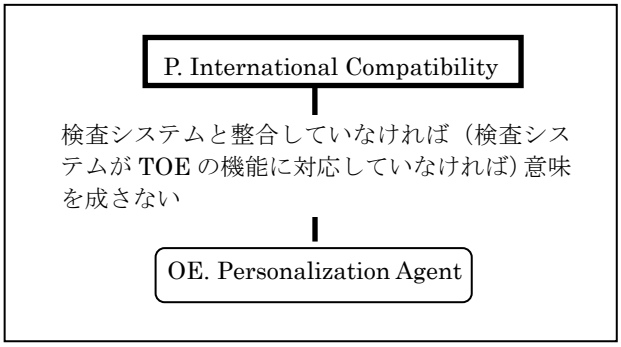

図 26　組織のセキュリティ方針（P. International Compatibility）と対策方針の関係

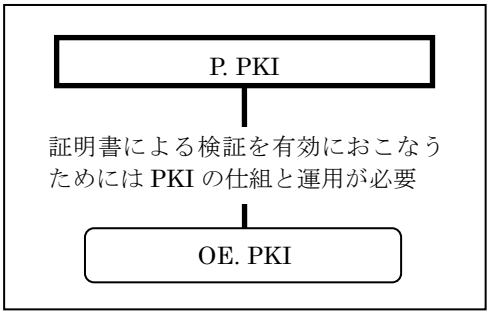

図 27　組織のセキュリティ方針（P. PKI）と対策方針の関係

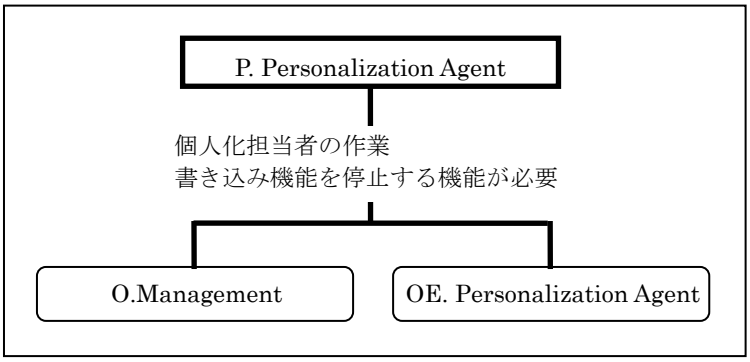

図 28　組織のセキュリティ方針（P. Personalization Agent）と対策方針の関係

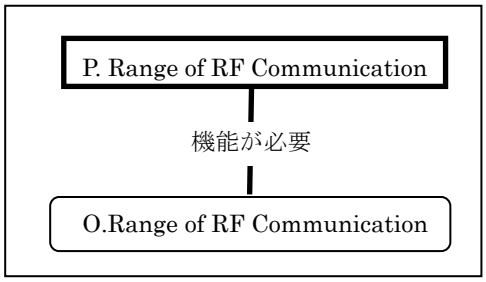

図 29　組織のセキュリティ方針（P. Range of RF Communication）と対策方針の関係

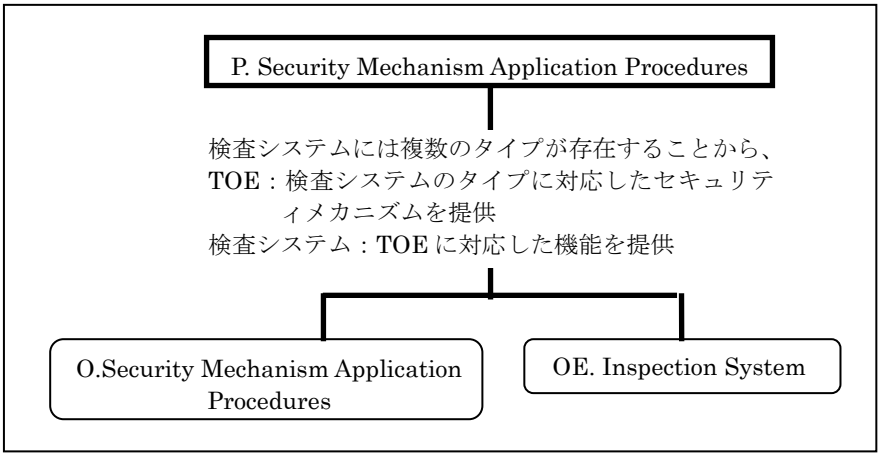

図 30　組織のセキュリティ方針（P. Security Mechanism Application Procedures）と対策方針の関係

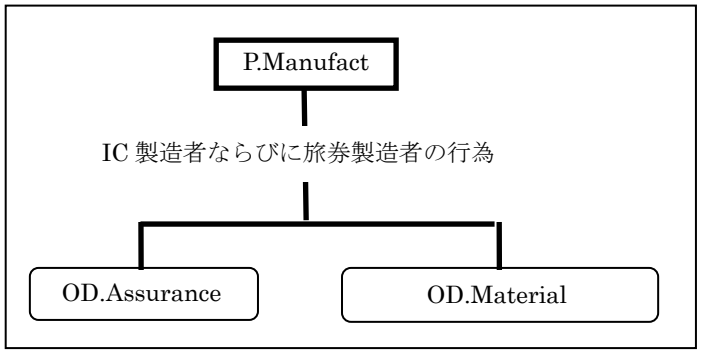

図 31　組織のセキュリティ方針（P.Manufact）と対策方針の関係

8. セキュリティ機能要件

本PPで選択している機能要件は以下の通りである。

クラス		機能要件	解説
FCS	暗号サポート	FCS_CKM.1	TOEのセキュリティメカニズムが使用する鍵に関する要件である。
		FCS_CKM.2	TOEのセキュリティメカニズムが使用する暗号鍵配付に関する要件である。
		FCS_CKM.4	TOEのセキュリティメカニズムが使用する鍵の破棄に関する要件である。 破棄した鍵が不正使用されることを防止する。
		FCS_COP.1	TOEのセキュリティメカニズムが使用する暗号アルゴリズムに関する要件である。
FDP	利用者データ保護	FDP_ACC.1	TOEの保護資産に対するアクセス制御に関する要件である。
		FDP_ACF.1	TOEの保護資産に対するアクセス制御の規則を定義する機能要件である。 FDP_ACC.1は本機能要件で定義した規則にしたがってアクセス制御を実施する。
		FDP_RIP.1	BACで使用する鍵が残存することを防止するための機能要件である。 鍵が一時的な記憶領域等に残存し、読み取られることを防止する。
		FDP_UCT.1	TOEとTOE外のエンティティの間における

			セキュアなデータ交換を実現するための機能要件である。 TOEとTOE外のエンティティの間のデータのやり取りは、製造者や個人化担当者がTOEにデータを書き込む際、TOEと検査システムがデータのやり取りをおこなう際等に発生すると考えられる。 これらは、本PPを参照するSTにおいて特定されるべきである。
		FDP_UIT.1	TOEとTOE外のエンティティの間におけるセキュアなデータ交換を実現するために実施する規則を定義する機能要件である。 FDP_UCT.1は本機能要件で定義した規則にしたがって機能を実施する。
FIA	識別と認証	FIA_AFL.1	BACにおいて相互認証が失敗した場合の処理を定義する機能要件である。 相互認証が失敗した場合にどのような処理をおこなうかについては、本PPを参照するSTにおいて特定されるべきである。
		FIA_UAU.1	BACにおいて認証に先立っておこなわれる前処理の存在を定義している。 また、前処理を除いて、認証が成功しなければアクションがおこなわれないことを定義している。
		FIA_UAU.4	BAC相互認証に関係するデータの再使用を防止することを定義している。 BAC相互認証に関係するデータが再利用されることで、認証機能が危殆化することを防止するためのものである。
		FIA_UID.1	TOEが必ず識別が成功することを要求することを定義している要件である。
FMT	セキュリティ管理	FMT_MOF.1	TOEに対するデータの書き込み機能を個人化担当者が停止できるようにすることを定義している機能要件である。 この機能を実装することにより、運用フェーズではデータの書き込み機能を停止してお

			くことで、TOEに対するデータの書き込みを防止することができる。
		FMT_MSA.1	TOEのセキュリティ機能に関係するサブジェクトのセキュリティ属性の初期化をTSFに制限することを定義している機能要件である。これによりTSFによらず（TSF以外の不正な機能・手段で）セキュリティ属性を初期化することはできない。
		FMT_MSA.3	セキュリティ属性のデフォルト値を制限的とし、デフォルト値を上書きする代替の初期値を特定できるのは個人化担当者のみに制限することを定義している。
		FMT_MTD.1	セキュリティ機能の振る舞いに影響をあたえるTSFデータの管理を個人化担当者に制限することを定義している。
		FMT_SMF.1	TOEが提供する管理機能を特定している。
		FMT_SMR.1	個人化担当者の役割を維持することを定義している。
FPR	プライバシー	FPR_UNO.1	TOEの処理が観察されないことを定義している。 観察されることにより暗号鍵などが特定されることを防止するためである。
FPT	TSFの保護	FPT_FLS.1	TOEに障害が発生した場合にセキュアな状態が維持されることを定義している。
		FPT_ITI.1	TSF間でTSFデータの改竄が発生した場合にセキュアな状態が維持されることを定義している。
		FPT_TST.1	TOEが自己テストを実施し、完全性を保証することを定義している。 詳細は、本PPを参照するSTにおいて特定されるべきである。
		FPT_PHP.3	TOEが物理的な攻撃に対抗することを定義している。

9. その他

ここではPPを作成するにあたっておこなった調査結果をまとめる。

9.1. 次期 IC 旅券システムの概要

IC旅券の所有者は、受入国の管理下にある検査システムにてIC旅券の正当性を検証される。検証は、「基本アクセス制御（BAC）⇒受動認証（PA）⇒能動認証（AA)」という３つのセキュリティメカニズムによるフェーズからなる。

第１フェーズの基本アクセス制御とは、検査システムにMRZ[1]情報以外の領域に対する読み出しを禁止するセキュリティメカニズムである。IC旅券所有者が受入国側の検査システのリーダライタにIC旅券冊子のICチップ（以下、「MRTD[2]チップ」と呼ぶ）が格納されたプラスチックカードのページを開いてかざすことにより、受け入れ国側の検査システムは受入国側の検査システムはMRTDチップに格納された特定領域のMRZ情報を読み出し、リーダライタとMRTDチップの間のチャレンジレスポンスを経てセキュアメッセージングが実現する。この時点で、MRTDチップは検査システムに対し、内部基礎ファイル（IEF: Internal Elementary File）[3]以外の全領域への読出し権限を付与する。MRZ情報読出しのイメージは次の図のようになる。開いた旅券冊子の下にあるものがIC旅券読出し装置であり、左のディスプレイにはMRTDチップから読み出した顔写真や旅券番号、氏名等が表示されている。

図 32 検査システムのリーダライタによる MRZ 情報の読出し（外務省 HP より抜粋）

[1] Machine Readable Zone の略
[2] Machine Readable Travel Document の略
[3] 不可視領域のこと。本稿では、JIS X 6306 の表記法に準拠した。尚、韓国の PP[5]では“Secure Memory”と表記されている。

第２フェーズの受動認証とは、CSCA証明書とDS証明書の証明書チェーンを利用したIC旅券の正当性の検証するセキュリティメカニズムである。DS証明書は、CSCAのもつ秘密鍵でデジタル署名が施されていて、CSCA証明書によって改ざんの有無を検証する。また、DS証明書が格納されているDocument Security Objectは、DSのもつ秘密鍵でデジタル署名が施されていて、DS証明書を用いてその正当性検証を行う。これらの処理が正常に行われれば、MRTDチップの格納データが偽造・改ざんされていないことが保証される。

第3フェーズの能動認証とは、基本アクセス制御や受動認証では検知できなかった「MRTDチップの複製」を検出するセキュリティメカニズムである。能動認証では、公開鍵暗号方式に基づいて生成されたAA鍵ペアを内部基礎ファイルに格納し、検査システムから送信されたチャレンジコードに内部基礎ファイルに格納されたAA秘密鍵でデジタル署名する。検査システムは、MRTDチップの読み取り可能な領域に格納されたAA公開鍵を読出し、デジタル署名付きのチャレンジコードを復号し、正常に復号処理できるかどうかを検証する。

9.2. 次期 IC 旅券の論理データ構造

ICAO document[1]のFigure III-2 (Data group reference numbers assigned to LDS)によると、IC旅券冊子に添付されているMRTDチップの論理データ構造（LDS: Logical Data Structure）は、EF.DG1-19というデータグループから構成される。データグループへの格納がMandatoryとなっているEF(Elementary File)は4種類存在し、それぞれIC旅券のMRZ[4]情報(EF.DG1)、IC旅券所有者の顔データ(EF.DG2)、バージョンやタグリストを含むEF.COM、及び格納データの完全性を保証するデータを含むEF.SODである。これらのEFに格納される主なコンテンツは以下のとおりである。

表 10 IC 旅券発行国のデータ要素(Mandatory)

格納先	コンテンツ
EF.DG1 （MRZ 情報）	Document Type
	Issuing State or organization
	Name (of Holder)
	Document Number
	Check Digit – Doc Number
	Nationality
	Date of Birth
	Check Digit – DOB
	Sex
	Data of Expiry or Valid Until Date

[4] Machine Readable Zone

	Check Digit DOE / VUD
	Optional Data
	Check Digit – Optional Data Field
	Composite Check Digit
EF.DG2	Encoded Face
EF.SOD	Hash(DG1-15)[5]
EF.COM	Version information, Tag list etc.

また、MRTDチップのLDS以外にも「内部基礎ファイル（IEF: Internal Elementary File）」と呼ばれるデータ格納領域があり、外部インタフェースを通じてここに格納されたデータに対する読出し・書込みはできない設計になっている。格納データは暗号鍵等のTSFデータである。

9.3. 受動認証 (Passive Authentication)

受動認証とは、公開鍵基盤による証明書チェーンを利用した認証スキームであり、受入国側の検査システムが旅行者の所有する旅券本体及び旅券発行国の正当性を検証する。本節では、受動認証使用されるCSCA証明書とDS証明書に対するセキュリティ要件、またこれらの証明書チェーンを用いた認証スキームの概念図を解説する。

9.3.1. CSCA 証明書

CSCAは旅券発行国にあるIC旅券専用のルート認証局であり、CSCA秘密鍵・公開鍵のペア （KPr_CSCA, KPu_CSCA） を管理し、CSCA公開鍵を格納したCSCA証明書（C_CSCA）の発行を自分自身が行う[6]。また、CSCA秘密鍵（KPr_CSCA）を用いて、後述のDS証明書（C_DS）に対する、デジタル署名を施す[7]。

文献[2] Annex G1.1によると、CSCA証明書のための秘密鍵と公開鍵のペアは、発行国の安全なオフライン環境で生成されること、サイドチャネル攻撃や乱数生成器に対する攻撃から秘密鍵を適切に管理できるようにEAL4+SOF-High[8]のCC認証を取得しているSSCD(Secure Signature Creation Device)を使用することが推奨されている。また、CSCA証明書の管理方法に対する要求事項は、厳重に守られた安全な外交手段で配送すべきと記載されている。ヒアリング調査の結果、CSCA証明書はインターネット上に公開せず[9]、IC

[5] ICAO document[1]の III-30 頁 A.10.4 節 Security を参照のこと。
[6] ICAO document[1] の IV-5 頁「Country Signing CA」によると、”（C_CSCA） shall be self-signed and issued by the CSCA.”と記載されている。
[7] ICAO document[1] の IV-2 頁「Country Signing CA Private Key」の定義を参照のこと。
[8] SOF-High という概念は、CCv2.3 に登場する。CCv3.1 では、AVA_VAN.5 に対応する。
[9] ICAO document[1] の IV-6 頁「Country Signing CA Certificates」によると、CSCA 証明書は ICAO PKD サービスの対象外である。

旅券発行国と受入国の旅券発給当局又は出入国管理当局等で共有されることが確認できた。また、HSM(Hardware Security Module)等の安全なデバイスに格納したCSCA証明書を安全に読み出すために、EAL4+SOF-HighのCC認証を取得しているCAD(Card Acceptor Device)に格納することが推奨されている。

9.3.2. DS 証明書

DS(Document Signer)とは、旅券発行国に存在する認証局であり、CSCA証明書（自国のルート認証局であるCSCAが発行する公開鍵証明書)を用いてIC旅券本体の正当性を保証する。ここでは、ICAO document[1] の第IV章5.5.1節及び5.5.2節に記載された要求事項を概説する。

DSは発行国の厳重に守られた環境のもとでDS秘密鍵・公開鍵のペア（KPr_DS, KPu_DS）を生成し、HSM[10]等の安全なデバイスに格納して管理する。その後、DS公開鍵をDS証明書（C_DS）に格納し てICAOに送付する。或いは、IC旅券のICチップ（以下、「MRTDチップ」と呼ぶ）に直接格納してもよい。また、MRTDチップのデータ要素であるEF.SOD[11]に対して、DS秘密鍵 （KPr_DS） によるデジタル署名を施し、Document Security Object（SO_D）を生成する。（SO_D）に格納される詳細情報は、ICAO document[1]のIV-28頁A3.1節「Signed Data Type」を参照されたい。特に、Document Security Objectは、signature(以後、「DS署名」と呼ぶ)の保持が必須(mandatory)、certificate (DS証明書（C_DS）を保持することが可能（optional）である。

ICAOでは、旅券発行国間で効率的にDS証明書を共有できるように、ICAO PKD (ICAO Public Key Directory)が開発された。ICAO PKD参加国は、自国のDS証明書をPKDにアップロードする。検査システムはその国がICAO PKD参加国であるか否かを問わず、ICAO PKD参加国のDS証明書を随時無料でダウンロードできる。IC旅券発行国はDS証明書が失効した場合、48時間以内にCRLを発行し、各国に配布しなければならない。その国がICAO PKD参加国である場合は、配布方法としてICAO PKDへのCRL登録を選択してもよい。IC旅券発行国はたとえDS証明書に関するセキュリティインシデントが起きていない場合でも、定期的に、少なくとも90日周期で証明書のCRLを発行することが義務付けられている。

9.3.3. 正当性検証の流れ

ICAO document[1]の第IV章5.5.1節によると、検証の流れはIC旅券発行国の正当性検証と、IC旅券本体の正当性検証の2つのフェーズからなる。各フェーズの詳細、及び概念図は以下のとおりである。

- **第１フェーズ.** 受入国側の検査システムは、事前に入手している IC 旅券発行国

[10] HSM の CC 認証取得の推奨に関しては、特に記載されていない。
[11] ICAO document[1] の IV-12 頁によると、EF.SOD は（SO_D）を包含する。

の CSCA 証明書を使って、事前に入手した、或いは MRTD チップに格納された DS 証明書に施された CSCA 秘密鍵によるデジタル署名を検証する。この処理が正常に行われれば、DS 証明書の正当性が保証される。

- **第 2 フェーズ.**　受入国側の検査システムは、事前に入手した、或いは MRTD チップに格納された DS 証明書を使って SOD に施された DS 秘密鍵によるデジタル署名（DS 署名）を検証する。この処理が正常に行われれば、IC 旅券本体の正当性が保証される。

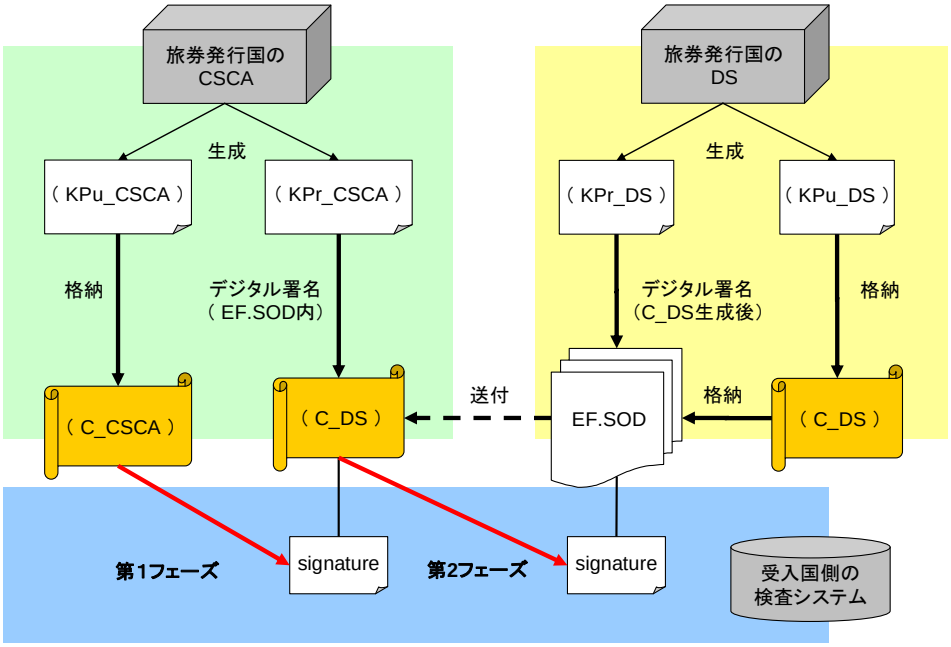

図 33 ICAO PKI による認証スキーム

9.4. 基本アクセス制御(Basic Access Control)

BAC（Basic Access Control）とは、IC旅券とリーダライタ間の通信内容を攻撃者からの盗聴及び改ざんから保護するセキュリティ機能である。使用する鍵はBAC認証鍵[12]とBACセッション鍵である。本節では、検査システムとIC旅券間での暗号通信であるセキュアメッセージングが実現する過程について、文献[1] (NORMATIVE APPENDIX 5)及び[2]（Annex E）をもとに解説する。

[12]韓国の PP[5]では“BAC Authentication Key”と表記されていて、ICAO document[1](Annex E)では、 Document Basic Access Key に対応する。ここでは、韓国の PP[5]に準拠して表記する。

9.4.1. BAC 認証鍵の生成

BAC認証鍵[7]は、受入国側の検査システム端末がIC旅券から読み出したMRZ情報を鍵のシードK_seedとして、KDM(Key Derivation System)と呼ばれる鍵生成のメカニズムにより作成される。

鍵のシードとなるMRZ情報とは、「旅券番号」、「生年月日」、「有効期限」及びそれぞれの検査桁から構成される。より安全な鍵のシードを作成するには、MRZ情報のエントロピー（情報量及びその拡散度合い）が高い方が望ましい。[13]

9.4.2. BAC セッション鍵の確立

BACセッション鍵は、IC旅券とリーダライタ間で2key3DESによる暗号通信を実現するための共通鍵であり、暗号鍵（KS_ENC）とメッセージ認証鍵（KS_MAC）が存在する。BACセッション鍵による暗号通信をセキュアメッセージングという。受入国側のリーダライタによるMRZ情報の読出しからセキュアメッセージングまでのセッション鍵確立過程の概念図は以下のとおりである。

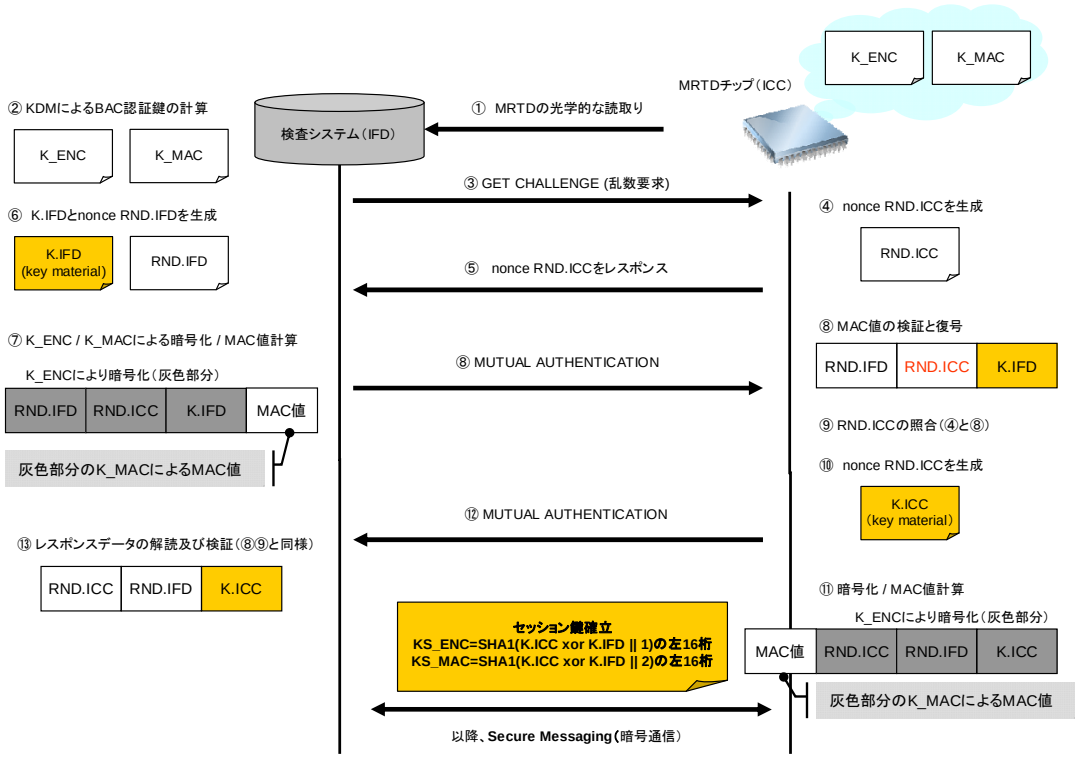

図 34 基本アクセス制御のおけるセッション鍵の確立過程

[13]韓国の PP[5]では前提条件として、MRZ 情報のエントロピーに対する要件（A. MRZ Entropy）を定めている。

認証と鍵確立は、ISO/IEC 11770-2[14]に準拠したチャレンジレスポンス形式の通信プロトコルにより実現される。セキュアメッセージングで使用される2key-3DESの暗号モードは、ISO11568-2に準拠した、8byteの初期ベクトル0 （0x 00 00 00 00 00 00 00 00）のCBC(cipher block chaining)である。一方、暗号チェックサムは、ISO/IEC 9797-1[15]に準拠して、8byteの初期ベクトル0による8byte MAC値である。MAC値によるデータの認証は、SSC（Send Sequence Counter）によってカウントされる。SSCの値は、MAC値が計算される前に一度カウントして+1、初めてのレスポンス段階で+2となる。SSCのデータ形式は、MRTDチップが生成する乱数RND.ICCと受入国側のリーダライタが生成する乱数RND.IFDの連結であり、それぞれのデータの大きさは4byteである。” MUTUAL AUTHENTICATE”に関しては、暗号化の際に入力データに対するパディングは行わない。また、メッセージ認証の際には初期値を0 （0x 00 00 00 00 00 00 00 00）に設定する。

9.4.3. セキュアメッセージング

MRTDチップと受入国側のリーダライタ間でBACセッション鍵が確立されたとき、2key3DESによる暗号通信が実現する。これ以降の通信内容は、セキュアメッセージングによってデータ保護される。

セキュアメッセージング（SM: Secure Message）には4種類のデータオブジェクトDO’87’、DO’97’、 DO’99’、DO’8E’が存在し、これらはISO/IEC 7816-4の中で詳細化されたBER TLVによって符号化される。データオブジェクトの概要は、DO’87’：暗号データに付加するISOパディングのインジケータ、DO’97’：Le、DO’99’：処理状態、DO’8E’：MACによる暗号チェックサムである。各データオブジェクトは、コマンドAPDU[16]とレスポンスAPDUにおいて、以下のように使用される。

表 11 セキュアメッセージング・データオブジェクトの利用用途

	Command APDU	Response APDU
DO’87’	データが送信される場合は Mandatory、そうでなければ使用しない	データが返される場合は Mandatory、そうでなければ使用しない
DO’97’	データが要求される場合は Mandatory、そうでなければ使用しない	使用しない
DO’99’	使用しない	Mandatory、ただし、セキュアメッセージングのエラーが発生した場合のみ使用しない
DO’8E’	Mandatory	DO’87’ and / or DO’99’を使用している場合は Mandatory

[14] Key Establishment Mechanism 6 using 3DES as block cipher
[15] MAC algorithm 3 及び padding method 2
[16] Application Protocol Data Unit

9.5. 能動認証(Active Authentication)

能動認証とは、基本アクセス制御や受動認証では検知できなかった「MRTDチップの複製」を検出するセキュリティ機能である。本節では、能動認証の手順、複写防止の根拠及び能動認証で使用されるデジタル署名の作成手順について解説する。

9.5.1. 能動認証の手順

次期IC旅券システムでは、MRTDチップと検査システム間でセキュアメッセージングが成立した後、能動認証の処理が実施される。その手順は以下のようになる。

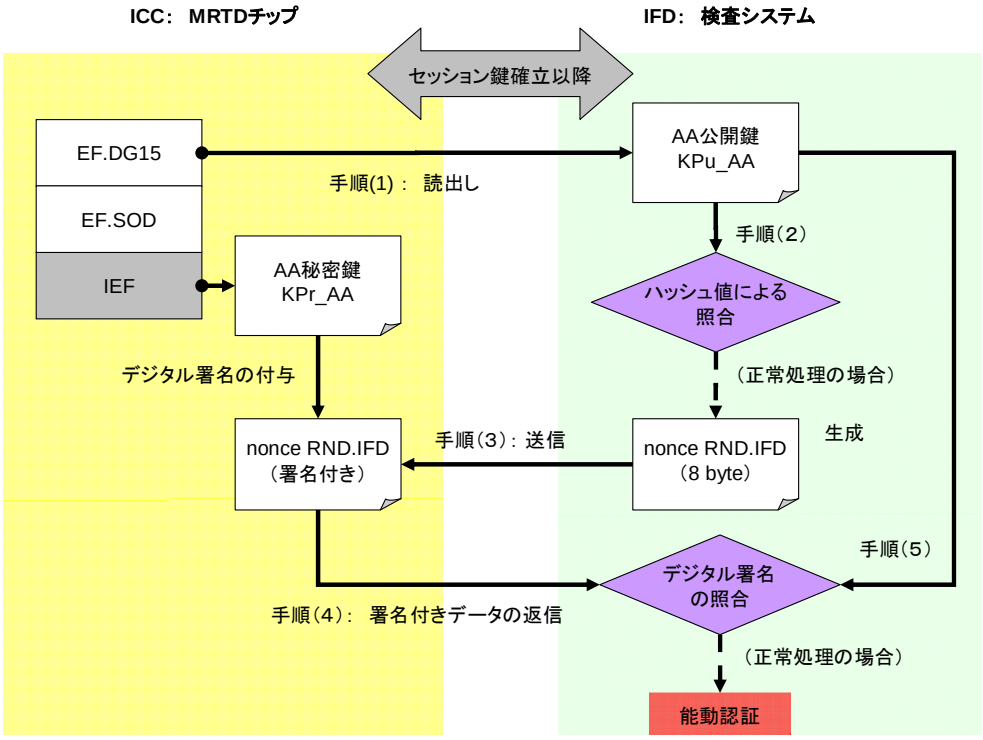

図 35 能動認証のメカニズム

(1) セキュアメッセージングを適用したデータ読み出しで、ファイル EF.DG15 から AA 公開鍵（KPu_AA）を取得する。

(2) セッション鍵確立以前の段階で読み出した IC 旅券の Document Security Object(SO_D)に含まれる DF.G15 に対応するハッシュ値を使って、AA 公開鍵（KPu_AA）を照合する。

(3) 端末は nonce RND.IFD（8byte の乱数）を生成し、これを「INTERNAL AUTHENTICATION」コマンドで IC 旅券に提示する。

(4) IC 旅券は、端末から提示された上記乱数にデジタル署名を施して端末に返信する。

（5）端末は、取得済みの AA 公開鍵（KPu_AA）を使って IC 旅券から提示されたデジタル署名を検証することで能動認証を実施する。

9.5.2. 複製防止の根拠

能動認証は、IC旅券内に保持された能動認証用の公開鍵暗号秘密鍵の安全性が十分確保され、IC旅券から取り出される（複写される）可能性が極めて低いことで、IC旅券データを別のIC旅券に複写することを防止している。したがって、IC旅券には、この秘密鍵が安全に保持され、外部に取り出されることを防ぐ機能が要求される。

9.5.3. デジタル署名作成手順

能動認証で使用されるデジタル署名は、ISO/IEC 9796-2:2002「Digital signature scheme 1」 に準拠したものであり、具体的には下記の４種類のデータを結合したデータを能動認証用の公開鍵暗号秘密鍵で暗号化することにより生成される。

- Header（1024bit の RSA 暗号鍵と SHA-1 を使用する場合は、‘6A’）
- IC 旅券で生成した乱数
- IC 旅券、端末双方で生成した乱数を結合したデータのハッシュ値
- ハッシュ関数に対応した１バイト又は２バイトの値

ICAO document[1]のIV 8節「Algorithm」によると、公開鍵暗号としてRSA、DSA、並びにECDSAが記載されているが、能動認証で使用されるデジタル署名は復号してデータを検証する必要があることから、暗号化・複号化機能をもつRSA暗号が使用される。また、ハッシュ関数としては、SHA-1、SHA-224、SHA-256、SHA-384、並びにSHA-512が規定されている。

次期IC旅券は、能動認証で使用する署名アルゴリズムとして、欧州の大手IC旅券及び端末メーカが使用しているRSA暗号（鍵長1024bit）とSHA-1を採用する。デジタル署名の手順の概略は以下のとおりである。

（1）INTERNAL AUTHENTICATION コマンドを受信し、8byte 端末生成乱数を入手する。
（2）848bit（106byte）IC 旅券乱数 M1 を生成する。尚、IC 旅券乱数長(L_M1)は、公開鍵の鍵長(k)、ハッシュ長(L_h)、並びにハッシュアルゴリズム(t)を元に、ISO/IEC 9796-2 及び ICAO document[1]の仕様に従って計算される。
（3）IC 旅券用乱数 M1 と端末乱数 M2 を結合させたデータ(M = M1 | M2)のハッシュ値 H を計算する。

（4）[Header | IC 旅券用乱数 M1 | ハッシュ値 H | Trailer] で構成される k bit 長（公開鍵鍵長）のデータ F を生成する。

（5）データ F を能動認証用公開鍵暗号秘密鍵で暗号化したデータ G を使用することにより、デジタル署名 S を生成する。

以下、デジタル署名作成手順に係る幾つかの注意事項を述べる。

- 段階（2）について
  - IC 旅券乱数長　　L_M1 = c－4 (Doc9303 規定)
  - c = k － L_h － 8＊t －4 (ISO/IEC 9796-2 規定)
  - 公開鍵鍵長 k=1024bit (鍵長 1024bit の RSA 暗号を使用)
  - L_h=160bit (SHA-1)
  - Trailer Option t = 1 if SHA-1; = 2 otherwise (Doc9303[1]により、ISO/IEC9796-2 Trailer Option 1 (t=1)or 2(t=2)を選択する)

- 段階（4）について
  - ISO/IEC 9796-2 の 8.2.2 Formatting より、Header の値は‘6A’
  - Doc9303[1]の A4.2 及び ISO/IEC 9796-2:2002 の 8.1.2 Trailer field options より、Trailer の値は以下のようになる。尚、SHA-256、SHA-384、並びに SHA-512 に関しては、ISO/IEC 10118-3 の hash-function identifier を参照のこと。

表 12 ハッシュ関数と Trailer の対応関係

ハッシュ関数	Trailer	ISO/IEC 10118-3:2004 の参照元
SHA-1	‘BC’	—
SHA-224	‘38CC’	—
SHA-256	‘34CC’	10. Dedicated Hash-Function 4
SHA-384	‘36CC’	11. Dedicated Hash-Function 5
SHA-512	‘35CC’	12. Dedicated Hash-Function 6

- 段階（5）について
  - ISO/IEC 9796-2:2002 A.4 又は A.6 より、データ G および公開鍵暗号モジュラス n を使ってデジタル署名を、S=min{G, n-G}、若しくは S=G 与える。

10. 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