外務省 旅券申請審査システム
セキュリティターゲット

第 1.05 版

2004 年 11 月 18 日

外務省

－ 更新履歴 －

日付	Version	更新箇所	更新内容	作成者
2004/6/29	1.0	－	－	外務省
2004/7/14	1.01	全般	所見指摘事項の反映	外務省
2004/7/29	1.02	全般	所見指摘事項の反映	外務省
2004/8/18	1.03	全般	所見指摘事項の反映	外務省
2004/9/15	1.04	全般	所見指摘事項の反映	外務省
2004/11/18	1.05	全般	認証指摘事項の反映	外務省

～ 目次 ～

1. ST概説 1
1.1. ST識別 1
1.1.1. STの識別と管理 1
1.1.2. TOE識別と管理 1
1.1.3. 適用するCCのバージョン 1
1.2. ST概要 1
1.3. CC適合 2
1.4. 参考資料 2
2. TOE記述 3
2.1. TOE種別 3
2.2. 用語定義 3
2.3. TOE概要 4
2.3.1. 業務サービス概要 4
2.3.2. TOEの利用環境 6
2.3.3. TOEの関連者 10
2.3.4. TOEの利用方法 13
2.4. TOE構成 23
2.4.1. TOEの構成 23
2.4.2. ハードウェア構成 24
2.4.3. TOEの構成 26
2.5. TOEの機能 27
2.5.1. 業務アプリケーションの機能 27
2.5.2. インフラの機能 31
2.6. 保護対象となる資産 32
3. TOEセキュリティ環境 35
3.1. 前提条件 35
3.2. 脅威 36
3.3. 組織のセキュリティ方針 37
4. セキュリティ対策方針 38

4.1. TOEのセキュリティ対策方針..... 38
4.2. 環境のセキュリティ対策方針..... 39
5. ITセキュリティ要件..... 42
5.1. TOEセキュリティ要件..... 42
5.1.1. TOEセキュリティ機能要件..... 42
5.1.2. TOEセキュリティ保証要件..... 103
5.2. IT環境に対するセキュリティ要件..... 103
5.3. 最小機能強度主張..... 103
6. TOE要約仕様..... 104
6.1. TOEセキュリティ機能..... 104
6.1.1. 業務利用制御機能（F.APLACTL）..... 104
6.1.2. セション管理機能（F.SESMAN）..... 108
6.1.3. 旅券事務担当職員管理機能（F.USEMAN）..... 109
6.1.4. 暗号化通信機能（F.CRYCOM）..... 110
6.1.5. 申請データ検証機能（F.SIGVER）..... 112
6.1.6. 監査機能（F.AUDIT）..... 113
6.1.7. インフラ利用管理機能（F.INFMAN）..... 117
6.2. セキュリティ機能強度..... 118
6.3. 保証手段 119
7. PP主張..... 120
8. 根拠..... 121
8.1. セキュリティ対策方針根拠..... 121
8.1.1. 前提条件に対するセキュリティ対策方針の適合性..... 122
8.1.2. 脅威に対するセキュリティ対策方針の適合性..... 124
8.1.3. 組織のセキュリティ方針に対するセキュリティ対策方針の適合性..... 127
8.2. セキュリティ要件根拠..... 128
8.2.1. セキュリティ対策方針に対するTOEセキュリティ機能要件の適合性..... 128
8.2.2. セキュリティ機能要件の相互支援について..... 136
8.2.3. TOEセキュリティ機能要件間の依存関係..... 137
8.2.4. TOEセキュリティ保証要件の選択根拠..... 144
8.2.5. セキュリティ対策方針に対するセキュリティ機能強度の一貫性..... 145
8.3. TOE要約仕様根拠..... 146

8.3.1. TOEセキュリティ機能要件に対するTOE要約仕様の適合性..... 146
8.3.2. セキュリティ機能強度根拠..... 159
8.3.3. 保証手段根拠..... 159

～ 図目次 ～

図 2.1 業務サービスの全体像..... 4
図 2.2 旅券申請システム全体像..... 6
図 2.3 旅券発給フロー..... 13
図 2.4 運用管理のユースケース..... 14
図 2.5 TOEの構成図..... 23

～ 表目次 ～

表 2.1 TOEに関係する人物..... 10
表 2.2 業務サービスにおいて関係する人物..... 12
表 2.3 ハードウェア構成..... 24
表 2.4 TOEの構成..... 26
表 2.5 保護対象資産一覧..... 32
表 5.1 TOEセキュリティ機能要件一覧..... 42
表 5.2 監査事象一覧..... 46
表 5.3 旅券事務担当職員アクセス制御方針が適用されるサブジェクト、オブジェクト及びサブジェクトとオブジェクト間の操作..... 63
表 5.4 管理項目一覧..... 90
表 5.5 TOEの保証要件コンポーネント一覧..... 103
表 6.1 パスワード規則..... 104
表 6.2 旅券事務担当職員アクセス制御方針..... 105
表 6.3 審査者端末とTOE間のSSL通信で使用するセキュリティメカニズム..... 111
表 6.4 汎用受付システムとTOE間のSSL通信で使用するセキュリティメカニズム.. 111
表 6.5 申請データ検証機能で使用するセキュリティメカニズム..... 113
表 6.6 監査ログに記録する内容..... 114
表 6.7 シグネチャとして選択可能な重要度 116
表 6.8 TOEの保証要件とエビデンス..... 119
表 8.1 前提条件、脅威、組織のセキュリティ方針とセキュリティ対策方針の対応 121
表 8.2 セキュリティ対策方針とTOEセキュリティ機能要件の対応..... 128
表 8.3 TOEセキュリティ機能要件間の依存関係..... 137
表 8.4 TOEセキュリティ機能要件とTOE要約仕様の対応..... 146

1. ST 概説

1.1. ST 識別

1.1.1. ST の識別と管理

名称：外務省 旅券申請審査システム セキュリティターゲット

バージョン：第 1.05 版

作成日：2004 年 11 月 18 日

作成者：外務省

1.1.2. TOE 識別と管理

名称：旅券申請審査システム

バージョン：1.0

作成者：外務省

1.1.3. 適用する CC のバージョン

JIS X 5070:2000

CCIMB Interpretations-0210 適用

注）日本語訳は「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1～3（平成13年1月翻訳第1.2版情報処理振興事業協会セキュリティセンター)」及び「補足-0210（独立行政法人製品評価技術基盤機構適合性評価センター翻訳）」を使用

1.2. ST 概要

旅券申請システムは、出入国に必要な旅券（パスポート）の発給処理をシステム化し、申請側に対してのサービス向上と旅券発給側に対しての業務効率化を図る。旅券申請システムは、申請側にインターネット経由のサービスを提供する汎用受付システム、旅券発給側に地方公共団体のネットワーク経由でサービスを提供する旅券申請審査システム、審査のために利用する審査者端末、リモート監視のために利用する監視端末から構成される。本 ST は、旅券申請システムに含まれている旅券申請審査システムを対象とする。旅券申請審査システムは、パッケージ製品として日本国内の様々な地方公共団体で使用される。

旅券申請審査システムは、申請の審査、審査結果の決裁及び公文書の発行を行う機能により、審査の効率化を図る。また、電子署名の検証を行う機能により、申請に対する正当性及び完全性の検証を行い、電子署名を付与する機能により、審査の結果に対する正当性及び完全性を保証する。

1.3. CC 適合

パート 2 適合

パート 3 適合

コンポーネント AVA_MSU.1 を用いた EAL2 追加

1.4. 参考資料

- JIS X 5070 セキュリティ技術―情報技術セキュリティの評価基準―第 1 部：総則及び一般モデル、第 2 部：セキュリティ機能要件、第 3 部：セキュリティ保証要件、平成 12 年 7 月 20 日
- 情報技術セキュリティ評価のためのコモンクライテリア パート 1:概説と一般モデル バージョン 2.1 1999 年 8 月 CCIMB-99-031
- 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:セキュリティ機能要件 バージョン 2.1 1999 年 8 月 CCIMB-99-032
- 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:セキュリティ保証要件 バージョン 2.1 1999 年 8 月 CCIMB-99-033
- Common Criteria 補足-0210
- Common Criteria for Information Technology Security Evaluation
  Part 1： Introduction and general model
  August 1999 Version 2.1 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation
  Part 2： Security functional requirements
  August 1999 Version 2.1 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation
  Part 3： Security assurance requirements
  August 1999 Version 2.1 CCIMB-99-033
- Common Criteria CCIMB Interpretations-0210
- ISO／IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part1, 99／12
- ISO／IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part2, 99／12
- ISO／IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part3, 99／12
- 外務省 旅券申請審査システム プロテクションプロファイル 第 1.1 版
  2003 年 12 月 24 日 外務省

2. TOE 記述

2.1. TOE 種別

本 TOE は、旅券の電子申請に関する審査の業務を Web サービスによって提供するパッケージ製品である。

2.2. 用語定義

本 ST で使用する用語の定義を以下に示す。

用語	定義内容
審査サービス	旅券に関する申請を審査及び検証する Web サービスである。審査サービスは、業務アプリケーション及びインフラによって提供される。
業務 アプリケーション	業務アプリケーションは、旅券に関する申請を審査及び検証するための機能を持つ。
インフラ	インフラは、業務アプリケーションの動作を支援するための機能を持つ、オペレーティングシステムやデータベースマネージメントシステムソフトウェアなどのソフトウェアを表す。
旅券申請システム	汎用受付システム、監視端末、旅券申請審査システム、審査者端末から構成されるシステムである。
旅券事務担当職員	地方公共団体旅券事務所職員のうち、TOE を利用して業務を行う、業務管理者、決裁者、審査者、旅券作成検査担当者、交付担当者の総称である。
総合行政 ネットワーク	各地方公共団体が接続しているネットワークである。本 ST 中は、LGWAN と称す。
庁内ネットワーク	地方公共団体のネットワークであり、LGWAN に接続している。
職責署名用 IC カード	地方公共団体の長が発行する電子証明書及び対になる秘密鍵を格納する媒体である。
公的個人認証 IC カード	地方公共団体が発行する電子証明書及び対になる秘密鍵を格納する媒体である。

2.3. TOE 概要

2.3.1. 業務サービス概要

本 TOE は、旅券の電子申請及び発給処理を行う業務サービスにおいて、中核を担う審査サービスを提供する旅券申請審査システムである。本項では、TOE を理解するために、旅券申請システム全体の業務サービス概要を説明する。図 2.1 に業務サービスの全体像を示す。

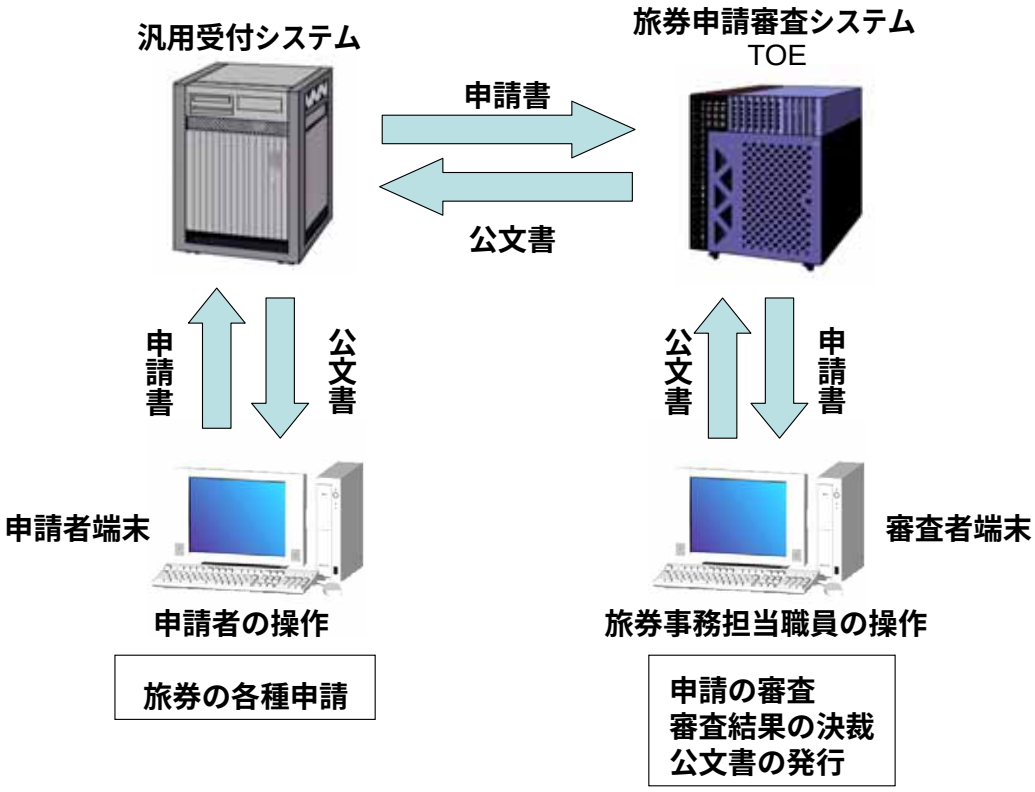

図 2.1 業務サービスの全体像

申請者は、申請者端末を介して、汎用受付システムにアクセスし、旅券に関する電子申請を行うことができる。申請者が申請可能な内容は以下の通りである。

- 旅券の新規発給申請
  旅券を新規に発給する際の申請
- 旅券の訂正新規発給申請
  旅券に訂正が生じた場合に新規発給する際の申請
- 旅券の記載事項の訂正
  旅券の記載事項に訂正が生じた際の申請
- 旅券の有効期間内の申請
  旅券の有効期間内に新規発給する際の申請
- 旅券の査証欄の増補
  査証欄を増補する際の申請
- 旅券紛失または焼失の届出
  旅券を紛失または焼失した際の届出

申請者は、テンプレート情報である申請者様式に基づいて申請書を作成し、汎用受付システムに送る。汎用受付システムは、旅券申請審査システムからの要求に応じて、申請書を旅券申請審査システムに送る。

旅券事務担当職員は、審査者端末を介して、旅券申請審査システムが提供している審査サービスを利用する。審査サービスの概要は、以下の通りである。

- 申請の審査
  申請者から送られる申請書を審査する。
- 審査結果の決裁
  審査した内容に対して決裁する。
- 公文書の発行
  決裁した内容を基に、申請受理、補正請求、応答（申請棄却）に係るいずれかの通知を発行する。

旅券事務担当職員は、申請の審査を行い、審査結果に基づき公文書を発行する。公文書は、旅券申請審査システムから汎用受付システムに送られる。

申請者は、申請者端末を介して、汎用受付システムにアクセスし、公文書を閲覧することで、審査結果を知ることができる。

2.3.2. TOE の利用環境

旅券申請システムには、図 2.2 で示したシステム構成が必要である。TOE は、地方公共団体旅券事務所に導入される旅券申請審査システムである。

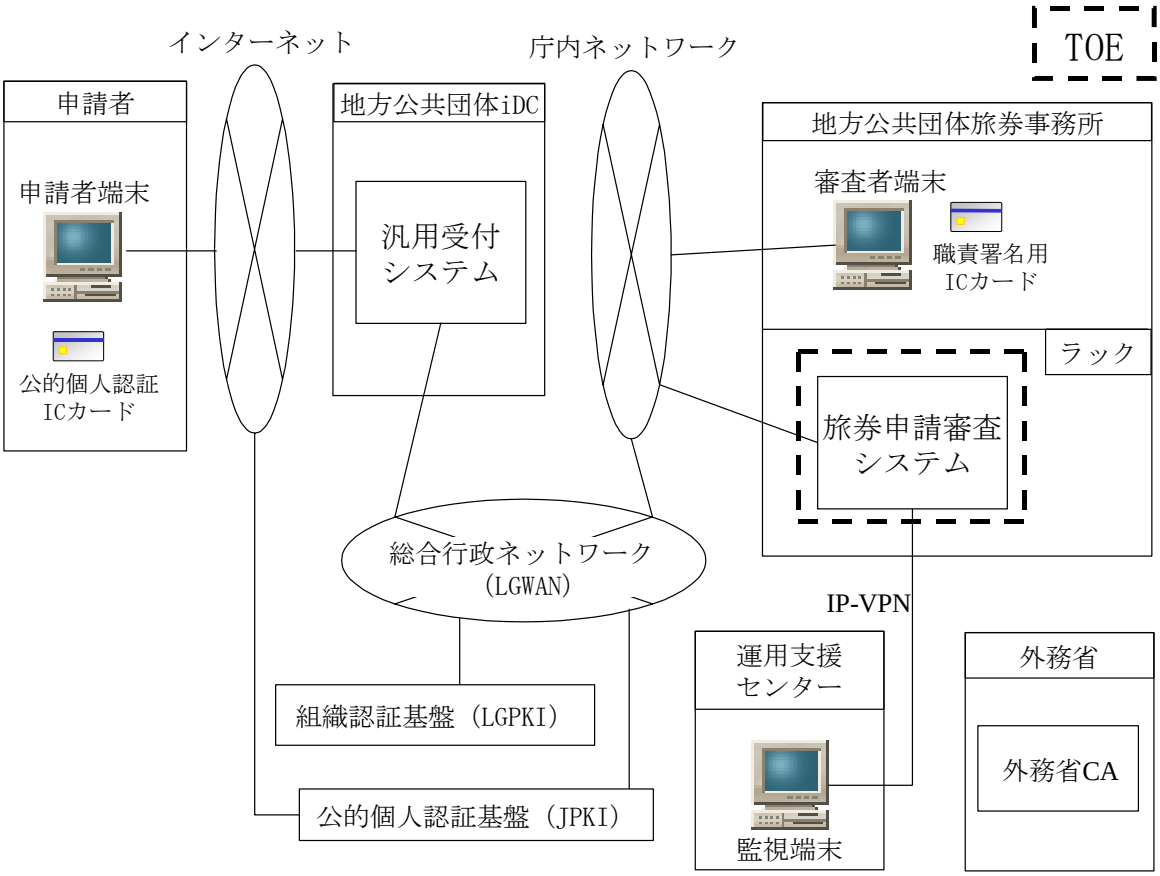

図 2.2 旅券申請システム全体像

以降では、旅券申請システム全体について説明する。

- 申請者（TOE 外）

  申請者は、申請者端末を介して、汎用受付システムにアクセスし、旅券の電子申請を含む各種業務サービスを利用する。

  - 申請者端末

    申請者端末は、インターネットに接続しており、以下に示すように、汎用受付システム及び JPKI と通信を行う。

    - 汎用受付システムとの通信
      - 電子申請を行うために、申請書様式を受信し、申請者自身の申請データを送信する。
      - 審査の結果を確認するために、公文書データ及び申請者自身の申請データ(申請が受理されない場合のみ)を受信する。
      - 審査状況を確認するために、状態通知情報を受信する。
    - JPKI との通信
      - 地方公共団体の電子証明書の有効性を検証するために、失効ステータスの確認要求を送信し、確認結果を受信する。

- 地方公共団体旅券事務所

  地方公共団体旅券事務所には、旅券申請審査システムと審査者端末が導入される。

  - 旅券申請審査システム（TOE）

    旅券申請審査システムは、庁内ネットワークに接続し、特定の役割を有する人物以外からの物理的なアクセスを禁止するため、施錠可能なラック内に設置される。

    旅券申請審査システムは、以下に示すように、汎用受付システム、審査者端末、LGPKI、JPKI 及び監視端末と通信を行う。

    - 汎用受付システムとの通信
      - 審査を行うために、申請データを受信する。
      - 審査の結果を通知するために、公文書データ、申請データ(申請が受理されない場合のみ)を送信する。
      - 審査状況を通知するために、状態通知情報を送信する。
    - 審査者端末との通信
      - 申請者から郵送された写真、自署を申請データとして取込むために、写真、自署を受信する
      - 審査を行うために、申請データ、審査データ、公文書を送信する。
      - 審査の内容を登録するために、審査データ、公文書データを受信

する。
- 業務アプリケーションを管理するために、管理データを送受信する。

・ LGPKI との通信
- 汎用受付システムのサーバ証明書の有効性を検証するために、失効ステータスの確認要求を送信し、確認結果を受信する。

・ JPKI との通信
- 申請者または法定代理人の電子証明書の有効性を検証するために、失効ステータスの確認要求を送信し、確認結果を受信する。

・ 監視端末との通信
- 異常の可能性を通知するために、監視端末へアラートを送信する。
- インフラを管理するために、運用管理に関するデータを受信する。

－ 審査者端末（TOE 外）

審査者端末は、庁内ネットワークに接続し、地方公共団体旅券事務所内の施錠管理された部屋に設置される。申請者は旅券受領のために地方公共団体旅券事務所へ出頭するが、審査者端末が設置される部屋への入室は禁止されている。旅券事務担当職員は、審査者端末を介して、旅券申請審査システムを利用する。

審査者端末は、以下に示すように、旅券申請審査システムと通信を行う。

・ 旅券申請審査システムとの通信
- 申請者から郵送された写真、自署を申請データとして取込むために、写真、自署を送信する
- 審査を行うために、申請データ、審査データ、公文書を受信する。
- 業務アプリケーションを管理するために、管理データを送受信する。
- 審査の内容を登録するために、審査データ、公文書データを送信する。

● 地方公共団体 iDC（TOE 外）

地方公共団体が管理する地方公共団体 iDC には、汎用受付システムが導入される。なお、汎用受付システムと申請者間の通信は「地方公共団体における申請・届出等手続きに関する汎用受付システムの基本仕様」に従って行われ、盗聴や改ざんから保護されている。

－ 汎用受付システム

汎用受付システムは、インターネット及び LGWAN に接続しており、以下に

示すように、申請者端末及び旅券申請審査システムとの通信を行う。

- 申請者端末との通信
  - 電子申請を行うために、申請書様式を送信し、申請データを受信する。
  - 審査の結果を通知するために、公文書データ、申請データ(申請が受理されない場合のみ)を送信する。
  - 審査状況を通知するために、状態通知情報を送信する。
- 旅券申請審査システムとの通信
  - 審査の結果を通知するために、公文書データ、申請データ(申請が受理されない場合のみ)を受信する。
  - 審査状況を通知するために、状態通知情報を受信する。
  - 審査を行わせるために、申請データを送信する。

- 運用支援センター（TOE 外）

外務省から監視業務を委託された運用支援センターには、旅券申請審査システム用の監視端末が設置される。

- 監視端末

監視端末は、IP-VPN を介して旅券申請審査システムに接続しており、以下に示すように、旅券申請審査システムとの通信を行う。

- 旅券申請審査システムとの通信
  - 異常の可能性を検知するために、アラートを受信する。
  - インフラを管理するために、運用管理に関するデータを送信する。

- LGPKI（TOE 外）

LGPKI は、公文書データの正当性及び完全性の確認と汎用受付システムの正当性を保証するために必要となる認証基盤である。LGPKI は、LGWAN に接続し、地方公共団体によって管理される。LGPKI は、汎用受付システムに対するサーバ証明書の発行及び電子証明書の失効ステータス管理、地方公共団体の電子証明書の発行及び電子証明書の失効ステータス管理を行う。また、地方公共団体の電子証明書及び対になる秘密鍵を格納した職責署名用 IC カードの発行を行う。

- 外務省 CA（TOE 外）

外務省 CA は、旅券申請審査システムの正当性を保証する認証局である。外務省 CA は、旅券申請システムとは独立しており、外務省によって管理される。外務省 CA は、旅券申請審査システムのサーバ証明書の発行及び失効ステータス管理を行う。

- JPKI（TOE 外）

  JPKI は、申請データの正当性及び完全性を確認するために必要となる認証基盤である。JPKI は、インターネット及び LGWAN に接続され、地方公共団体によって管理される。JPKI は、申請者及び法定代理人の電子証明書の発行及び電子証明書の失効ステータス管理を行う。

  なお、LGPKI と JPKI は相互認証を行っている。このため、申請者端末にて地方公共団体の電子証明書の有効性を検証する際には、LGPKI と相互認証を行っている JPKI に対して確認要求を行う。

2.3.3. TOE の関連者

TOE に関係する人物を表 2.1 に示す。

表 2.1 TOE に関係する人物

役割	説明
システム責任者	システム責任者は、TOE の運用管理全般における責任を持つ人物である。 TOE の利用は許可されておらず、旅券事務所システム管理者、業務管理者、決裁者及び監視者の任命を行う。また、旅券事務所システム管理者、業務管理者、決裁者、監視者に対して、システム運用管理に関する規則を遵守させる。さらに、旅券事務所システム管理者、監視者、旅券事務担当職員に対して、情報セキュリティ教育を実施し、セキュリティ意識の向上及び維持を図る。
旅券事務所システム管理者	旅券事務所システム管理者は、TOE のハードウェア／ソフトウェアを管理し、TOE の安定的な運用を行う人物である。 TOE のハードウェア／ソフトウェアに対する特権を有し、ハードウェア／ソフトウェアの管理を行う。また、審査者端末の利用管理、TOE の利用管理及び運用管理、TOE に存在する各種資源のバックアップ／リストア、監視者と連携して異常が発生した際の対処を行う。ただし、業務アプリケーションが提供する機能の利用は許可されていない。
交付担当者	交付担当者は、作成された旅券を申請者に交付する人物である。業務アプリケーションに対する利用権限を有し、審査者端末を介して、業務アプリケーションが提供する機能を利用する。交付担当者は、申請者が持参したはがき及び身元確認書類と審査者端末に表示される申請データの突合検査を行い、申請者に旅券を交付する。

役割	説明
旅券作成検査担当者	旅券作成検査担当者は、決裁により申請受理となった申請の旅券作成及び作成された旅券の検査を実施する人物である。 業務アプリケーションに対する利用権限を有し、審査者端末を介して、業務アプリケーションが提供する機能を利用する。旅券作成検査担当者は、申請受理となった申請データに基づいて旅券を作成する。
審査者	審査者は、申請者から電子申請された内容を審査する人物である。 業務アプリケーションに対する利用権限を有し、審査者端末を介して、業務アプリケーションが提供する機能を利用する。交付担当者及び旅券作成検査担当者の役割に加え、申請データの内容に対して、審査を行う。
決裁者	決裁者は、審査の内容を決裁する人物である。 業務アプリケーションに対する利用権限を有し、審査者端末を介して、業務アプリケーションが提供する機能を利用する。審査者の役割に加え、審査の内容に対する決裁及び公文書の発行を行う。
業務管理者	業務管理者は、業務アプリケーションにおける運用管理を行う人物である。 業務アプリケーションに対する特権を有し、審査者端末を介して、業務アプリケーションが提供する機能を利用する。決裁者の役割に加え、審査者端末から業務アプリケーションの運用管理を行う。 また、職責署名用 IC カードの貸出管理も行う
監視者	運用支援センターの監視端末から TOE の監視及び TOE のソフトウェア管理を行う人物である。 TOE のソフトウェア及び監視端末に対する利用権限を有する。TOE から通知されるアラートを監視し、TOE に異常が発生した場合は、旅券事務所システム管理者と連携し、異常への対処を実施する。
保守担当者	TOE を安全に運用するための保守作業を行う人物である。 TOE の利用は許可されていない。旅券事務所システム管理者の監視の下、ハードウェア／ソフトウェアの保守を行う。

また、旅券発給という業務サービス上、TOE に関係する人物を表 2.2 に示す。

表 2.2 業務サービスにおいて関係する人物

役割	説明
申請者	インターネットを介して、旅券に関する申請を行う人物である。 申請者が未成年もしくは成年被後見人である場合、法定代理人を伴う。 TOE の利用は許可されていないが、旅券に関する申請を行うために必要となる申請データを作成し、汎用受付システムに登録する。 また、汎用受付システムにアクセスし、地方公共団体旅券事務所から発行される公文書データの検証や自身の申請に対する審査状況の確認を行う。
法定代理人	法律により定められた代理人に該当する人物であり、以下の者を指す。 ・ 未成年者の親権者 ・ 未成年者の未成年後見人 ・ 成年被後見人の後見人 申請者が自らの意思で申請行為を行える場合、法定代理人は同意書の作成を行う。申請者が自らの意思で申請行為を行えない場合、法定代理人は申請の内容に同意した上で、申請者の代理として旅券に関する電子申請を行う。

2.3.4. TOE の利用方法

旅券に関する各種申請において、概ね、TOE の利用方法が同一の手順となるため、一般的によく利用される申請者の新規旅券申請から旅券交付までの旅券発給フローの概略を図 2.3 に示す。

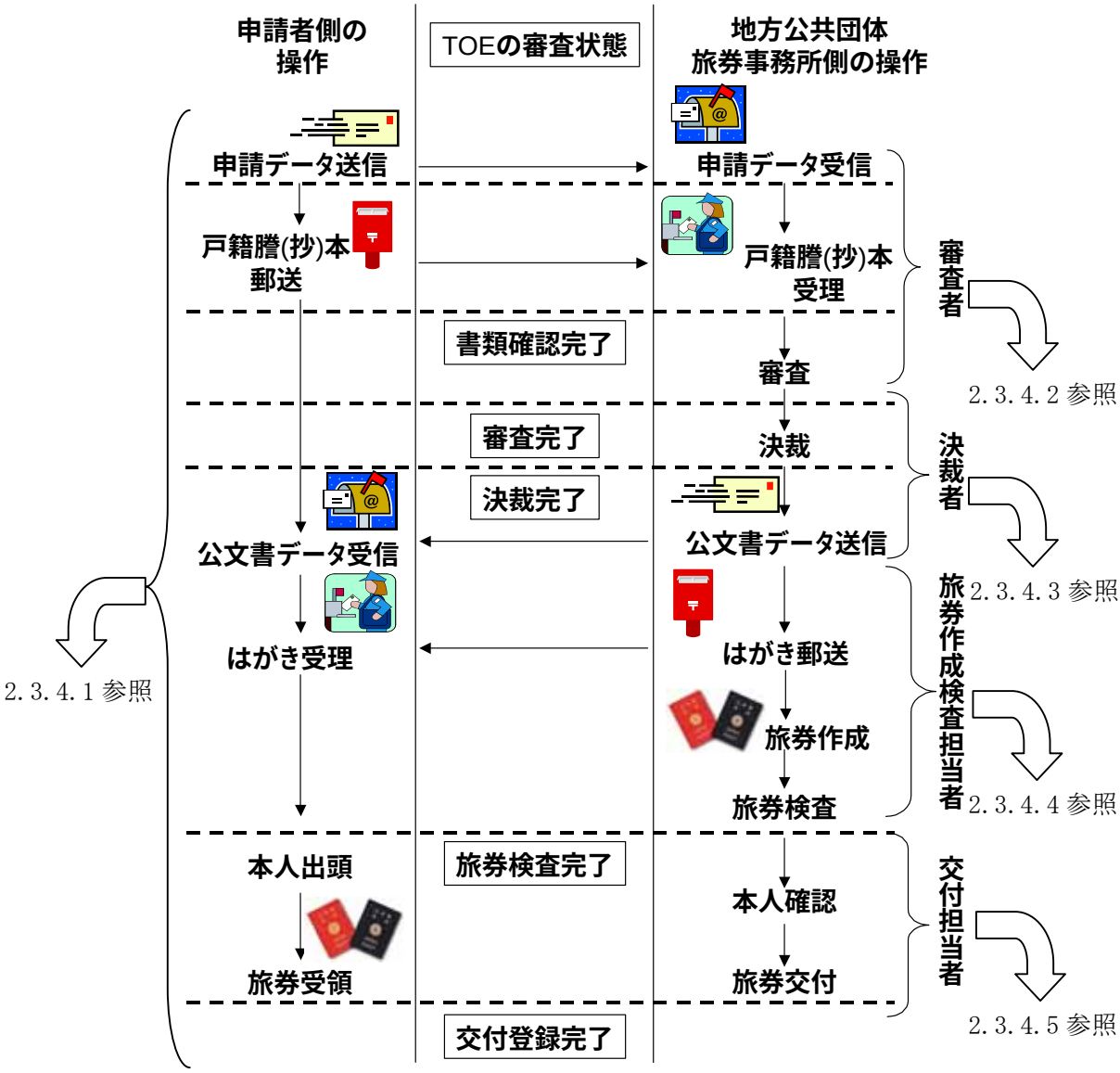

図 2.3 旅券発給フロー

なお、『2.3.4.1 申請者側の利用』に関しては、TOE の利用方法ではないが、全体フローの理解は、TOE の理解に繋がるため、本項で説明する。地方公共団体旅券事務所側の操作である審査は、審査者による審査フェーズ、決裁者による決裁フェーズ、旅券作成検査担当者による旅券作成検査フェーズ及び交付担当者による交付フェーズの順に実施される。

また、本 TOE に対する運用管理のユースケースを図 2.4 に示す。

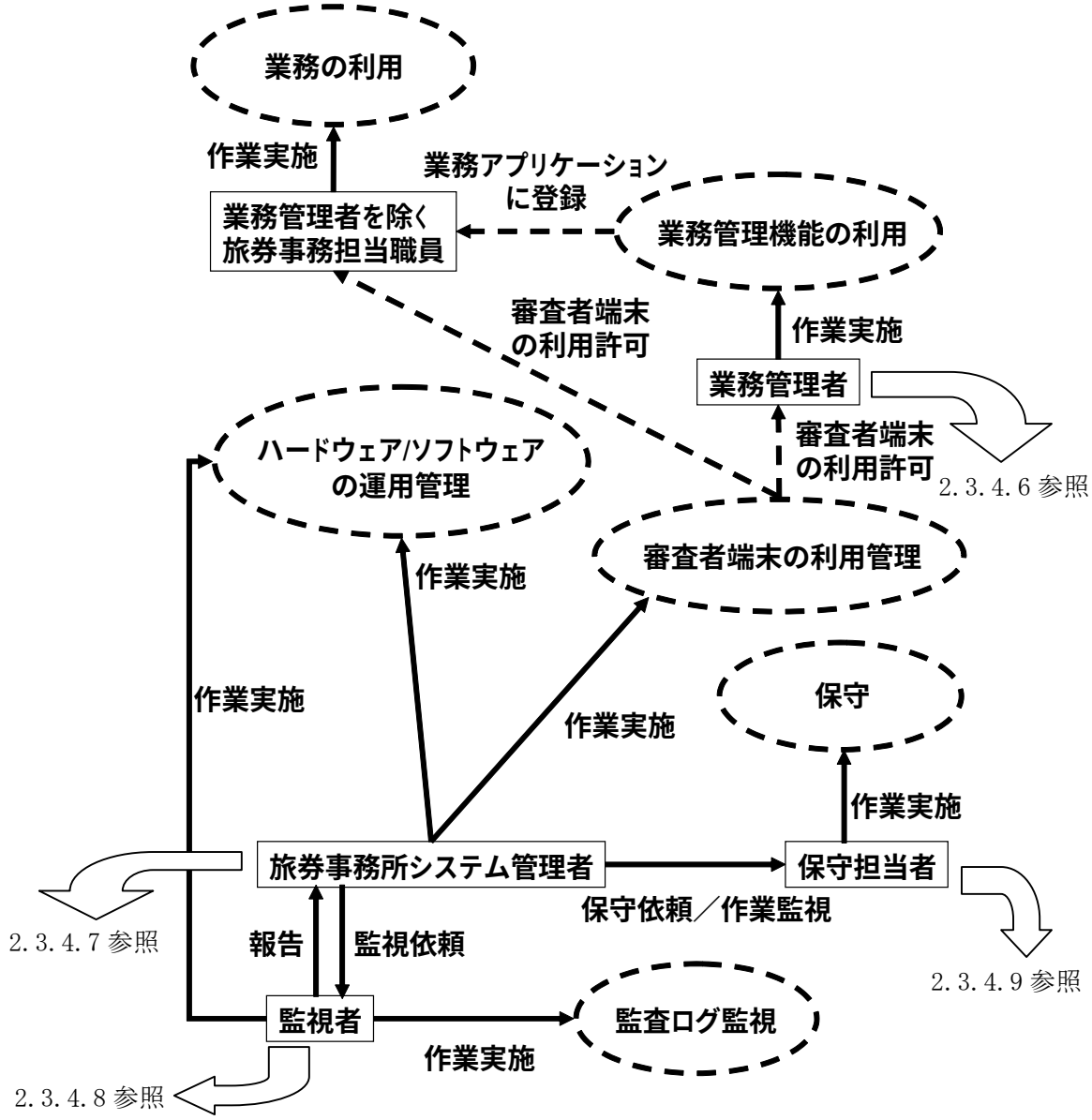

図 2.4 運用管理のユースケース

実線の矢印(⟶)は役割が行う運用行為を表す。また、点線の矢印(⇢)は役割が運用行為を行うために、事前に必要となる条件を表す。なお、四角(□)は役割を、点線楕円(◌)は運用行為の作業内容を表す。

2.3.4.1.　申請者側の利用

申請者または法定代理人は、旅券に関する申請を行う際に、申請者端末の Web ブラウザを介して、汎用受付システムにのみアクセスするため、TOE を直接操作できない。

- 事前準備

  旅券申請システムを利用するために、申請者は、汎用受付システムの利用が許可されており、公的個人認証 IC カードを所有している必要がある。また、必要に応じて、法定代理人は、公的個人認証 IC カードを所有している必要がある。

- 申請方法

  1. 申請書様式の取得

     申請者または法定代理人は、汎用受付システムで提供される申請書様式を取得する。

  2. 申請データの作成

     (A) 申請者が申請する場合

     申請者は、取得した申請書様式に、申請に必要となる情報を入力し、申請書を作成する。その後、申請書、写真、自署から申請データを作成する。ただし、写真及び自署を郵送する場合、申請データに写真及び自署は含まれない。

     (B) 法定代理人を伴って申請する場合

     以下のいずれかの方法で電子申請を行う。

     (ア)申請者及び法定代理人が公的個人認証 IC カードを所持している場合

     法定代理人は、申請者の電子申請に同意した内容、法定代理人の電子署名及び法定代理人の電子証明書から、同意書を作成する。申請者は、取得した申請書様式に、申請に必要となる情報を入力し、申請書を作成する。その後、申請書、写真、自署、同意書から申請データを作成する。ただし、写真及び自署を郵送する場合、申請データに写真及び自署は含まれない。

     また、同意書を郵送する場合、同意書は、申請データに含まれず、法定代理人によって紙媒体で作成される。

     (イ)申請者のみが公的個人認証 IC カードを所持している場合

     申請者は、取得した申請書様式に、申請に必要となる情報を入力し、申請書を作成する。その後、申請書、写真、自署、同意書から申請データを作成する。ただし、写真及び自署を郵送する場合、申請データに写真及び自署は含まれない。

     法定代理人は、紙媒体で同意書を作成し、地方公共団体旅券事務所へ郵送する。

(ウ)法定代理人のみが公的個人認証 IC カードを所持している場合

法定代理人は、取得した申請書様式に、申請に必要となる申請者の情報を入力し、申請書を作成する。その後、申請書、写真、自署から申請データを作成する。ただし、写真及び自署を郵送する場合に、申請データに写真及び自署は含まれない。

3. 申請データへ電子署名の付与

(A) 申請者が申請する場合

申請者は、申請データに対して、申請者の電子署名を付与する。電子署名の付与では、申請者の公的個人認証 IC カードに格納されている秘密鍵を使用する。

(B) 法定代理人を伴って申請する場合

以下のいずれかの方法で電子申請を行う。

(ア)申請者及び法定代理人が公的個人認証 IC カードを所持している場合

法定代理人は、同意書に対して、法定代理人の電子署名を付与する。電子署名の付与では、法定代理人の公的個人認証 IC カードに格納されている秘密鍵を使用する。

申請者は、申請データに対して、申請者の電子署名を付与する。電子署名の付与では、申請者の公的個人認証 IC カードに格納されている秘密鍵を使用する。

(イ)申請者のみが公的個人認証 IC カードを所持している場合

申請者は、申請データに対して、申請者の電子署名を付与する。電子署名の付与では、申請者の公的個人認証 IC カードに格納されている秘密鍵を使用する。

(ウ)法定代理人のみが公的個人認証 IC カードを所持している場合

法定代理人は、申請データに対して、法定代理人の電子署名を付与する。電子署名の付与では、法定代理人の公的個人認証 IC カードに格納されている秘密鍵を使用する。

4. 申請データの送信

(A) 申請者が申請する場合

申請者は、申請者の公的個人認証 IC カードに格納されている電子証明書を申請データに添付し、汎用受付システムへ送信する。

(B) 法定代理人を伴って申請する場合

以下のいずれかの方法で電子申請を行う。

(ア)申請者及び法定代理人が公的個人認証 IC カードを所持している場合

法定代理人は、法定代理人の公的個人認証 IC カードに格納されている電子証明書を同意書に添付し、申請データに添付する。

申請者は、申請者の公的個人認証 IC カードに格納されている電子証明書を申請データに添付し、汎用受付システムへ送信する。

(イ)申請者のみが公的個人認証 IC カードを所持している場合

申請者は、申請者の公的個人認証 IC カードに格納されている電子証明書を申請データに添付し、汎用受付システムへ送信する。

(ウ)法定代理人のみが公的個人認証 IC カードを所持している場合

法定代理人は、法定代理人の公的個人認証 IC カードに格納されている電子証明書を申請データに添付し、汎用受付システムへ送信する。

5. 戸籍謄(抄)本の郵送

申請者または法定代理人は、汎用受付システムで付与された受付番号を戸籍謄(抄)本に記載し、地方公共団体旅券事務所に郵送する。申請データに写真、自署、同意書を含めない場合は、併せて、写真、自署、同意書も地方公共団体旅券事務所に郵送する。

6. 審査状況の確認

申請者または法定代理人は、汎用受付システムから提供される状態通知情報を確認する。また、審査が完了し、公文書が発行されると、メールによる通知を希望する申請者または法定代理人には、汎用受付システムからメール通知される。

7. 公文書データの取得

申請者または法定代理人は、汎用受付システムから提供される公文書データを取得する。

8. 公文書データの検証

申請者または法定代理人は、取得した公文書データの検証を行い、正当性及び完全性を確認する。公文書データを検証する際には、職責証明書を使用して電子署名の検証を行う。併せて、職責証明書の有効性確認も行う。

9. 旅券の受領

申請者または法定代理人は、地方公共団体旅券事務所から郵送されたはがき及び身元確認書類を持参し、地方公共団体旅券事務所で旅券を受領する。

2.3.4.2. 審査者の利用

審査者は、審査者端末の Web ブラウザを介して、TOE を利用し、申請データの審査を行う。

- 事前準備

審査者端末及び TOE の利用が許可されている必要がある。

- 審査方法

1. 申請データの取得

審査者は、汎用受付システムから申請データを取得する。申請データの取得完

了により、申請取得完了通知が生成され、汎用受付システムに通知される。

2. 郵送書類の確認

審査者は、申請者または法定代理人から郵送された書類として、戸籍謄(抄)本、写真、自署、同意書を受領する。ただし、写真、自署、同意書に関しては、電子送付された場合、郵送書類として必要ではない。

審査者は、戸籍謄(抄)本に記載されている受付番号を基に、対象となる申請データを検索し、受領した書類の確認を行う。その際、郵送された写真及び自署を電子的に取り込む。書類の確認において、不備がなければ、審査状態情報に書類確認結果を登録し、書類確認作業の完了とする。書類確認結果の登録により、書類確認完了通知が生成され、汎用受付システムに通知される。

3. 申請データの署名検証

(A) 申請者が申請する場合

審査者は、申請データの正当性と完全性を検証するために、申請者の電子証明書を用いて、申請者の電子署名を検証する。

(B) 法定代理人を伴って申請する場合

以下のいずれかの方法で電子申請を行う。

(ア)申請者及び法定代理人が公的個人認証 IC カードを所持している場合

審査者は、申請データの正当性と完全性を検証するために、申請者の電子証明書を用いて、申請者の電子署名を検証する。また、同意書の正当性と完全性を検証するために、法定代理人の電子証明書を用いて、法定代理人の電子署名を検証する。

(イ)申請者のみが公的個人認証 IC カードを所持している場合

審査者は、申請データの正当性と完全性を検証するために、申請者の電子証明書を用いて、申請者の電子署名を検証する。

(ウ)法定代理人のみが公的個人認証 IC カードを所持している場合

審査者は、申請データの正当性と完全性を検証するために、法定代理人の電子証明書を用いて、法定代理人の電子署名を検証する。

4. 申請データの証明書検証

(A) 申請者が申請する場合

審査者は、申請データを検証する際に必要となる申請者の電子証明書の有効性を確認する。

(B) 法定代理人を伴って申請する場合

以下のいずれかの方法で電子申請を行う。

(ア)申請者及び法定代理人が公的個人認証 IC カードを所持している場合

審査者は、申請データを検証する際に必要となる申請者の電子証明書の有効性を確認する。また、同意書を検証する際に必要となる法定代

理人の電子証明書の有効性を確認する。

(イ)申請者のみが公的個人認証 IC カードを所持している場合

審査者は、申請データを検証する際に必要となる申請者の電子証明書の有効性を確認する。

(ウ)法定代理人のみが公的個人認証 IC カードを所持している場合

審査者は、申請データを検証する際に必要となる法定代理人の電子証明書の有効性を確認する。

5. 申請データの本人性確認

審査者は、対象となる申請データの本人性確認を行う。

(A) 申請者が申請する場合

審査者は、申請データに含まれている申請者の個人情報と申請者の電子証明書に含まれている個人情報を比較し、本人性を確認する。加えて、郵送された戸籍謄(抄)本による本人性を確認する。

(B) 法定代理人を伴って申請する場合

以下のいずれかの方法で電子申請を行う。

(ア)申請者及び法定代理人が公的個人認証 IC カードを所持している場合

審査者は、申請データに含まれている申請者の個人情報と申請者の電子証明書に含まれている個人情報を比較し、本人性を確認する。加えて、郵送された戸籍謄(抄)本による本人性を確認する。また、同意書に含まれている法定代理人の個人情報と法定代理人の電子証明書に含まれている個人情報を比較し、本人性を確認する。

(イ)申請者のみが公的個人認証 IC カードを所持している場合

審査者は、申請データに含まれている申請者の個人情報と申請者の電子証明書に含まれている個人情報を比較し、本人性を確認する。加えて、郵送された戸籍謄(抄)本による本人性を確認する。

(ウ)法定代理人のみが公的個人認証 IC カードを所持している場合

審査者は、申請データに含まれている法定代理人の個人情報と法定代理人の電子証明書に含まれている個人情報を比較し、本人性を確認する。加えて、郵送された戸籍謄(抄)本による本人性を確認する。

6. 審査

審査者は、申請データに対して審査を行い、審査情報を入力する。審査は、先の本人性確認に加え、申請内容の不備、申請者の適格性（渡航先への入国可否や刑罰など）の観点で行われる。

7. 審査結果の登録

審査者は、審査状態情報に審査結果を登録し、審査作業の完了とする。審査結果の登録により、審査完了通知が生成され、汎用受付システムに通知される。

2.3.4.3.　決裁者の利用

決裁者は、審査者端末の Web ブラウザを介して、TOE を利用し、審査が完了した申請に対して決裁を行う。なお、決裁者は、審査者、交付担当者、旅券作成検査担当者の操作権限も有する。

- 事前準備

  審査者端末及び TOE の利用が許可されている必要がある。また、職責署名が行えるように、職責証明書及び対となる秘密鍵が格納された職責署名用 IC カードを用意する必要がある。

- 決裁方法

  1. 申請データの閲覧

     決裁者は、審査が完了した申請データを対象に検索し、閲覧する。

  2. 決裁

     決裁者は、審査の内容を確認し、必要があれば審査情報を入力する。

  3. 職責署名の付与

     決裁者は、申請データ及び審査データから必要となる情報を抽出し、公文書データを作成する。決裁者は、作成された公文書データに対して、職責署名を付与し、汎用受付システムに通知する。ただし、審査結果が申請受理以外の場合、公文書データと併せて申請データも汎用受付システムに通知する。

  4. 決裁結果の登録

     決裁者は、審査状態情報に決裁結果を登録し、決裁作業の完了とする。決裁結果の登録により、決裁完了通知が生成され、汎用受付システムに通知される。

2.3.4.4.　旅券作成検査担当者の利用

旅券作成検査担当者は、審査者端末の Web ブラウザを介して、TOE を利用し、審査結果が申請受理となった申請の旅券を発行する。

- 事前準備

  審査者端末及び TOE の利用が許可されている必要がある。

- 旅券作成検査方法

  1. 申請データの閲覧

     旅券作成検査担当者は、決裁が完了した申請データから審査結果が申請受理である申請データを検索し、閲覧する。また、対象となる公文書を閲覧することも可能である。

  2. 受領はがきの郵送

     旅券作成検査担当者は、申請者の居住確認を行うためのはがきを作成し、申請者へ郵送する。

3. 旅券発行
   旅券作成検査担当者は、申請データ及び審査データに基づき、旅券を発行する。
4. 申請書との突合確認
   旅券作成検査担当者は、発行した旅券に印刷上の不備がないか確認する。
5. 旅券検査結果の登録
   旅券作成検査担当者は、旅券に印刷上の不備がない場合、審査状態情報に旅券検査結果を登録し、旅券検査作業の完了とする。仮に、旅券に不備があった場合、旅券の再作成を行う。

2.3.4.5. 交付担当者の利用

交付担当者は、審査者端末の Web ブラウザを介して、TOE を利用し、申請者を確認した後、発行された旅券を申請者に交付する。

- 事前準備
  審査者端末及び TOE の利用が許可されている必要がある。
- 旅券交付方法
  1. 申請データの閲覧
     交付担当者は、旅券検査が完了した申請データを対象に検索し、閲覧する。また、対象となる公文書を閲覧することも可能である。
  2. 旅券交付
     交付担当者は、地方公共団体旅券事務所の受付窓口で旅券を交付する際に、申請者が持参するはがき及び身元確認書類と申請データの突合確認を行う。記載内容や写真を基に本人であることを確認した後、申請者に旅券を交付する。
  3. 交付結果の登録
     交付担当者は、審査状態情報に交付結果を登録し、交付登録作業の完了とする。

2.3.4.6. 業務管理者の利用

業務管理者は、審査者端末の Web ブラウザを介して、TOE を利用し、業務アプリケーションの業務管理機能を利用する。決裁者と同様の操作が可能であり、決裁者の操作に加えて、以下の運用管理を行う。

- 申請データの削除を行う。
- 確立中のセション一覧表示／切断を行う。
- 担当者情報の登録／削除／変更を行う。
- 事務所情報の登録／変更を行う。

2.3.4.7.　旅券事務所システム管理者の利用

旅券事務所システム管理者は、地方公共団体旅券事務所に設置されたラック内のコンソールを利用して、TOE に対して以下の運用管理を行う。

- TOE の利用管理のため、旅券事務所システム管理者や監視者のパスワード変更を行う。
- TOE に存在する各種資源のバックアップ／リストアを含むシステム運用管理を、日常的に行う。
- 異常が発生した場合に、監視者と連携して TOE のソフトウェアに対する運用管理を行う。
- 定期的な運用管理のため、保守担当者に TOE のハードウェア／ソフトウェアの保守作業を依頼する。また、保守担当者の作業中は不正な行為が行われないように監視する。

また、TOE に対する運用管理以外に、審査者端末の管理を行う。

- 審査者端末の利用管理のため、旅券事務担当職員を審査者端末に登録し、審査者端末の利用を許可する。

＜審査業務とバックアップについて＞

・ 保護対象資産のバックアップは、地方公共団体旅券事務所のすべての開庁日に取得する。
・ 審査業務の手続き上、申請データの受理から１日以内で処理が終了する審査業務はない

2.3.4.8.　監視者の利用

監視者は、運用支援センター内の監視端末をモニタリングし、TOE が通知するアラートの監視を行う。検出したアラートは旅券事務所システム管理者に報告する。監視者は、TOE のソフトウェアに対する利用権限を持ち、異常が発生した場合は、旅券事務所システム管理者と連携し、利用権限の範囲内で異常に対する対処を実施する。

2.3.4.9.　保守担当者の利用

保守担当者は、旅券事務所システム管理者からの依頼を受け、TOE のハードウェア／ソフトウェアに対する保守作業を行う。なお、保守作業は、旅券事務所システム管理者の監視下で行われる。

2.4. TOE 構成

TOE の物理的な配置構成、動作環境としてのハードウェア構成、TOE のソフトウェア構成を示す。

2.4.1. TOE の構成

「図 2.5 TOE の構成図」に TOE が稼動する旅券申請審査サーバ及び旅券申請審査 DB サーバと、関連する IT 機器の構成を示す。

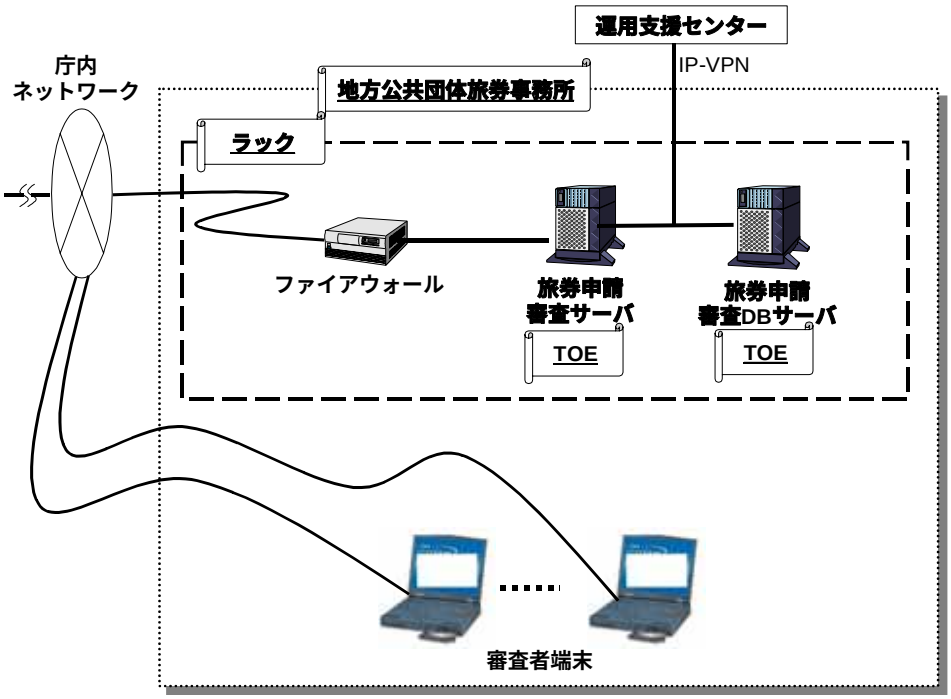

図 2.5 TOE の構成図

– 物理配置及びネットワーク

地方公共団体旅券事務所内には、複数台の審査者端末と施錠可能なラック内に収納されているファイアウォール、旅券申請審査サーバ及び旅券申請審査 DB サーバが設置される。TOE は、旅券申請審査サーバ及び旅券申請審査 DB サーバにて稼動する旅券申請審査システムである。旅券申請審査サーバと旅券申請審査 DB サーバは、相互に接続されている。また、旅券申請審査サーバ及び旅券申請審査 DB サーバは IP-VPN によって運用支援センターに接続されている。

- 旅券申請審査サーバ
  旅券申請審査サーバは、審査を提供するシステムとして、フロントエンドを担当する。汎用受付システムまたは審査者端末との通信においては、要求に応じて旅券申請審査 DB サーバのテーブルにアクセスし、結果を返す。また、監査ログに異常が発生した場合に、運用支援センターに対してアラートを通知する。
- 旅券申請審査 DB サーバ
  旅券申請審査 DB サーバは、審査を提供するシステムとして、バックエンドを担当し、審査に関わる申請データ、審査データ及び管理データを管理する。旅券申請審査サーバからの要求に応じて、テーブルの操作を行う。また、監査ログに異常が発生した場合に、運用支援センターに対してアラートを通知する。
- ファイアウォール
  ファイアウォールは、庁内ネットワークと旅券申請審査サーバの間に接続される。ファイアウォールは、庁内ネットワークから TOE へ流れる通信を制御する。
- 審査者端末
  審査者端末は、庁内ネットワークに接続される。旅券事務担当職員が審査を行う際に、審査者端末から庁内ネットワークを介して旅券申請審査サーバにアクセスを行う。
  また、業務に応じて旅券事務担当職員がローカルプリンタを接続することもある。

2.4.2. ハードウェア構成

「表 2.3 ハードウェア構成」に、TOE の動作環境としてのハードウェア構成を示す。TOE は、表 2.3 を満たす動作環境で、正しく確実に動作する。

表 2.3 ハードウェア構成

サーバ名	種別	説明
旅券申請審査サーバ	CPU	SPARC 64V 1.1GHz/1MB 以上
	メモリ	1GB 以上
	HDD	36.4GB 以上 10,000rpm 以上
	ディスク装置	DVD-ROM （CD-ROM 読み取り最大 24 倍速以上）

サーバ名	種別	説明
	ネットワークカード	10/100 Ethernet カード 3 ポート 100/1000 Ethernet カード 1 ポート
	PGX64 フレームバッファ	ディスプレイ接続用
	DAT 装置	内蔵 DAT 装置、DDS-4 対応、40GB/巻(圧縮時)
	SSL アクセラレータ	SSL-R
旅券申請審査 DB サーバ	CPU	SPARC 64V 1.1GHz/1MB 以上
	メモリ	1GB 以上
	HDD	36.4GB 以上 10,000rpm 以上
	ディスク装置	DVD-ROM (CD-ROM 読み取り最大 24 倍速以上)
	ネットワークカード	10/100 Ethernet カード 1 ポート 100/1000 Ethernet カード 1 ポート
	PGX64 フレームバッファ	ディスプレイ接続用
	DAT オートローダ装置	DAT 装置、DAT テープを最大 6 巻まで搭載可能、DDS-4 対応、40GB/巻(圧縮時)
	デュアルチャネル UltraSCSI カード	DAT オートローダ装置用
	ファイバーチャネルカード	DB サーバ共用ディスク接続用
	ストレージ装置 (RAID5)	ETURNUS3000 モデル 50 165GB 10,000rpm
その他	KVM スイッチ付共用ディスプレイ	コンソール

2.4.3. TOE の構成

「表 2.4 TOE の構成」に、TOE の構成を示す。TOE は表 2.4 に識別されたソフトウェアから構成される。

表 2.4 TOE の構成

サーバ名	製品名	備考
旅券申請審査サーバ	Solaris 9 8/03 OE	オペレーティングシステム
	SafeDISK 2.1	ミラーリングソフト
	INTERSTAGE Application Server Enterprise Edition V5.1.1	アプリケーションサーバソフトウェア
	NetWorker WorkGroup Edition 6.1.3.Build.428	バックアップソフトウェアクライアント機能
	Enhanced Support Facility 2.3,REV=2003.02.1400	システム監視ソフトウェア
	INTERSTAGE Charset Manager Standard Edition Web 入力 Agent V6.0	外字コード管理ソフトウェア
	INTERSTAGE Charset Manager Web 入力 マルチ文字コードオプション V6.0	外字コード管理ソフトウェアのオプション
	OpenView Operations for Windows Agent version A.07.23	統合サービス管理ソフトウェア
	Tripwire for Server 4.0.2	整合性チェックツール
	業務アプリケーション V1.0	旅券に関する申請の審査に必要となるアプリケーションパッケージ
旅券申請審査 DB サーバ	Solaris 9 8/03 OE	オペレーティングシステム
	SafeDISK 2.1	ミラーリングソフト
	Oracle9i Database Release2(9.2.0.1.0)	データベースマネージメントシステムソフトウェア
	NetWorker WorkGroup Edition 6.1.3.Build.428	バックアップソフトウェアサーバ機能

サーバ名	製品名	備考
	NetWorker Auto Changer Software Module 6.1.3.Build.428	バックアップソフトウェア
	Enhanced Support Facility 2.3,REV=2003.02.1400	システム監視ソフトウェア
	OpenView Operations for Windows Agent version A.07.23	統合サービス管理ソフトウェア
	Tripwire for Server 4.0.2	整合性チェックツール

2.5. TOE の機能

TOEは、業務アプリケーションの機能とインフラの機能によって、審査サービスを提供する。以下では、業務アプリケーションの機能とインフラの機能について述べる。なお、機能説明のうち、下線（＿＿＿）で識別されたものがTOEのセキュリティ機能である。

2.5.1. 業務アプリケーションの機能

業務アプリケーションでは、以下の機能を提供する。

- 業務利用者制御機能

  TOEは、旅券事務担当職員の正当性を確認するために、識別及び認証を行う。また、TOEは、識別された人物に対する業務アプリケーションの利用を制限するため、役割に基づいてアクセス制御を行う。

  なお、役割は、業務管理機能から旅券事務担当職員を登録する際に、旅券事務担当職員に付与される。

- 業務管理機能

  TOEは、本機能の使用を業務管理者のみに制限し、旅券申請審査DBサーバのテーブルに対して、担当者情報及び事務所情報を登録及び変更、担当者情報の削除を行う。

  TOEは、業務管理者の要求に従い、旅券申請審査DBサーバのテーブルにアクセスし、業務利用者制御機能に関わる情報であるユーザID、パスワード、役割情報の登録及び削除を行う。ただし、本機能を使用する業務管理者自身に関する情報の削除はできない。

  また、旅券申請審査DBサーバのテーブルに登録されているパスワード及び役割情報に対して、旅券事務担当職員のパスワード変更、交付担当者、旅券作成検査担当者、審査者及び決裁者の役割情報の変更を行う。

  なお、最初の業務管理者の登録に関しては、TOE 導入時に行われる。

- 申請データ取得機能

  TOE は、定められた時間あるいは業務管理者、決裁者または審査者の要求に従って、汎用受付システムに格納されている申請データを旅券申請審査 DB サーバのテーブルに登録する。

- 申請データ表示機能

  TOE は、旅券事務担当職員が入力した検索条件を基に、旅券申請審査 DB サーバに登録されている申請データを検索し、対象となる申請書、写真、自署、同意書の表示データを返す。また、表示された申請データを、審査者端末に接続されたローカルプリンタを利用して印刷することも可能である。

- 申請データ削除機能

  TOE は、業務管理者が入力した検索条件を基に、旅券申請審査 DB サーバに登録されている申請データを検索し、選択された申請データを旅券申請審査 DB サーバのテーブルから削除する。なお、申請データ削除機能は、一定期間が過ぎた申請データの削除や旅券申請審査 DB サーバのデータベースをメンテナンスする際のみ利用される。

- 結果登録機能

  TOE は、審査者、決裁者及び業務管理者が入力した審査情報を、旅券申請審査 DB サーバのテーブルに登録する。

  TOE は、旅券事務担当職員が登録した審査状態情報及び入力した官公庁記載欄情報を旅券申請審査 DB サーバのテーブルに登録する。情報は、審査の履歴として残すため、情報は追記形式で登録される。また、旅券事務担当職員の操作に応じて、旅券申請審査 DB サーバのテーブルを検索し、審査情報、審査状態情報または官公庁記載欄情報の表示データを返す。

  審査状態情報の登録では、以下に示すように、役割毎に登録可能な情報が異なる。

  ◆ 交付担当者の場合
    交付結果の登録
  ◆ 旅券作成検査担当者の場合
    旅券検査結果の登録
  ◆ 審査者の場合
    書類確認結果、審査結果、旅券検査結果、交付結果の登録
  ◆ 決裁者及び業務管理者の場合
    書類確認結果、審査結果、決裁結果、旅券検査結果、交付結果の登録

- 署名検証機能

TOEは、審査者、決裁者または業務管理者の操作に応じて、申請データの正当性及び完全性を検査するために、申請者証明書を用いて申請者署名の検証を行う。なお、同意書が含まれる場合は、法定代理人証明書を用いて法定代理人署名の検証も行う。

- 証明書検証機能

TOEは、審査者、決裁者または業務管理者の操作に応じて、申請者証明書の有効性を検証するために、申請者証明書の有効期間を検査する。ただし、申請者証明書の失効ステータスの確認については、JPKIによって失効ステータスの確認が行われ、TOEは、その結果のみを受け取る。失効ステータスにより、失効が確認された場合、無効な申請者証明書であると判断し、申請を棄却する。なお、同意書が含まれる場合は、同様に法定代理人証明書の有効性検査も行う。

- 本人性確認機能

TOE は、審査者、決裁者または業務管理者の操作に応じて、申請者証明書に格納されている情報と申請書の情報を比較し、本人性を確認する。また、申請者証明書に格納されている情報と申請書の比較結果を審査者端末に返す。なお、同意書が含まれる場合は、同様に法定代理人の本人性確認も行う。

- 写真／自署取込み機能

TOE は、審査者、決裁者または業務管理者の操作に応じて、写真及び自署を取込み、旅券申請審査 DB サーバのテーブルに登録する。情報は、審査の履歴として残すため、情報は追記形式で登録される。ただし、申請者または法定代理人から、写真及び自署が郵送された場合に限る。

- 状態通知機能

TOE は、以下に示すように、審査者、決裁者及び業務管理者が行う審査業務に応じて、状態通知情報を生成し、汎用受付システムに通知する。

◆ 申請データ取得完了後
　申請取得完了通知の生成
◆ 書類確認結果の登録後
　書類確認完了通知の生成
◆ 審査結果の登録後
　審査完了通知の生成
◆ 決裁結果の登録後
　決裁完了通知の生成

状態通知機能は、汎用受付システムに状態通知情報を通知するだけであり、実際

に申請者が審査の進捗状況を確認するには、汎用受付システムにアクセスする必要がある。

- 公文書表示機能

  TOE は、旅券事務担当職員の操作に応じて、旅券申請審査 DB サーバのテーブルに登録されている申請データ及び審査データから必要な情報を抽出し､審査者端末に公文書の表示データを返す。

- 署名付与機能

  TOE は、決裁者または業務管理者の操作に応じて、公文書データを生成し、職責署名付与を行う。ただし、職責署名の生成については、職責署名用 IC カードによって行われ、TOE は、生成された職責署名を用いて署名付与を行う。

- 公文書データ通知機能

  TOE は、署名付与機能にて公文書データが作成された後、公文書データを汎用受付システムに通知する。なお、審査結果が申請受理以外の場合、併せて、申請データも汎用受付システムに通知する。

- セション管理機能

  TOEは、TOEと審査者端末間のセション管理を行う。セション管理機能は、セション一覧表示、セション手動切断及びセション自動切断が可能である。セション一覧表示は、業務管理者に対して、現在確立されているセション一覧を表示する。セション手動切断は、業務管理者が指定するセションを強制的に切断する。セション自動切断は、セションが確立された状態において、定められた時間内に審査者端末から応答がない場合、TOEがセションを強制的に切断する。

2.5.2. インフラの機能

インフラでは、以下の機能を提供する。

- 管理作業の識別認証及びアクセス制御機能

  TOEは、TOEを構成するサーバを利用する旅券事務所システム管理者及び監視者の正当性を確認するために、識別及び認証を行う。また、TOEは、識別された人物に対するインフラの機能の利用を制限するために、アクセス制御を行う。

- システム管理機能

  TOEは、旅券事務所システム管理者の操作に応じて、旅券事務所システム管理者または監視者のパスワード変更、TOEの時刻変更及び参照、セキュリティ侵害を検知するための規則変更及び参照を行う。また、監視者の要求に基づき、監視者のパスワード変更、セキュリティ侵害を検知するための規則変更及び参照を行う。なお、旅券事務所システム管理者及び監視者の登録に関しては、TOE導入時に行われる。

- 暗号化通信機能

  TOEは、汎用受付システムとTOE間または審査者端末とTOE間の通信データを、改ざん及び盗聴から保護するためにSSLを利用した通信を行う。

- 監査機能

  TOEは、安定的な稼動維持及びセキュリティ侵害を検知するために、TOEを構成するサーバの監査ログを記録する。監査ログを記録する監査ログ格納領域を管理するため、一定の閾値を越えた場合、監査ログに閾値超えの事象を記録する。記録した監査ログは、旅券事務所システム管理者及び監視者のみが参照できるよう制限する。また、セキュリティ侵害を検知するための規則に基づき、監査ログをリアルタイムで分析し、セキュリティ侵害の可能性の検出を行う。セキュリティ侵害の可能性を検出すると、監視端末にアラートを通知する。

2.6. 保護対象となる資産

本 TOE が提供する審査サービスを不正な申請によって不当に利用され、その結果、不適切な旅券を発給し、不正申請者に取得されることは、TOE にとって大きな問題である。この問題に対抗するため、TOE の審査サービスにおける入出力情報及び審査サービスを正しく遂行するために必要な管理情報を保護する。保護対象資産の一覧を表 2.5 に示す。

表 2.5 保護対象資産一覧

資源名	内容
申請データ	申請データは、申請書構成管理情報、申請書、写真、自署及び同意書の総称である。 申請データは、汎用受付システムから旅券申請審査サーバを経由し、旅券申請審査 DB サーバに登録される。また、旅券事務担当職員の操作に応じて、旅券申請審査 DB サーバから旅券申請審査サーバを経由し、審査者端末に通知される。加えて、審査の結果、申請受理以外になった場合、公文書データと併せて旅券申請審査サーバから汎用受付システムに通知される。 なお、写真及び自署に関して、申請者が申請する際に、電子的に送付する場合と郵送する場合があり、郵送する場合には、審査者端末から TOE に登録される。
申請書構成管理情報	申請書管理情報、申請書署名情報、申請者署名及び申請者証明書の総称である。
申請書管理情報	受付番号、申請種別、申請データの構成を示した情報である。
申請書署名情報	申請書管理情報、申請書、写真、自署及び同意書(法定代理人を伴う申請かつ同意書が電子送付される場合のみ)に関する、署名生成に必要な情報である。
申請者署名	申請者が申請する場合は、申請者の公的個人認証 IC カードに格納される秘密鍵を用いて、申請書署名情報のハッシュ値を暗号化した署名値となる。 法定代理人が代理申請する場合は、法定代理人の公的個人認証 IC カードに格納される秘密鍵を用いて、申請書署名情報のハッシュ値を暗号化した署名値となる。

資源名	内容
申請者証明書	申請者が申請する場合は、申請者の公的個人認証 IC カードから取り出された電子証明書となる。 法定代理人が代理申請する場合は、法定代理人の公的個人認証 IC カードから取り出された電子証明書となる。
申請書	申請者が旅券に関する申請を行うために、申請者または法定代理人が入力した個人情報を含む電子文書である。
写真	申請者を被写体とした画像データである。
自署	申請者のサインを電子化した画像データである。
同意書	同意書管理情報、同意書署名情報、法定代理人署名及び法定代理人証明書の総称である。同意書は、法定代理人を伴う申請かつ同意書が電子送付される場合のみ存在する。
同意書管理情報	法定代理人の個人情報及び申請者の申請書に対して、同意した内容が含まれた情報である。
同意書署名情報	同意書管理情報に関する、署名生成に必要な情報である。
法定代理人署名	法定代理人の公的個人認証 IC カードに格納される秘密鍵を用いて、同意書署名情報のハッシュ値を暗号化した署名値である。
法定代理人証明書	法定代理人の公的個人認証 IC カードにから取り出された電子証明書である。
審査データ	審査データは、審査情報、官公庁記載欄情報、審査状態情報及び状態通知情報の総称である。 審査情報、官公庁記載欄情報及び審査状態情報は、審査者端末から旅券申請審査サーバを経由して、旅券申請審査 DB サーバに登録される。また、必要に応じて旅券申請審査サーバを介して旅券申請審査 DB サーバにアクセスし、審査者端末に通知される。状態通知情報は、旅券申請審査サーバから汎用受付システムに通知される。
審査情報	審査者または決裁者が、申請書に対して、審査した内容を記載する情報である。
官公庁記載欄情報	旅券事務担当職員が、必要に応じて、メモや注意事項として入力する情報である。
審査状態情報	旅券事務担当職員が実施する審査における各作業の完了状態を識別する情報である。
状態通知情報	申請者に審査の進捗状況を通知するための情報である。

資源名	内容
公文書データ	公文書データは、公文書構成管理情報及び公文書の総称である。公文書データは、旅券申請審査サーバで生成され、汎用受付システムへ通知される。ただし、公文書に関しては、必要に応じて、旅券申請審査サーバを介して旅券申請審査 DB サーバにアクセスし、審査者端末に通知される。
公文書構成管理情報	公文書管理情報、公文書署名情報、職責署名及び職責証明書の総称である。
公文書管理情報	公文書データの構成を示した情報である。ただし、審査結果が申請受理以外の場合、申請書、写真(申請者から電子送付された場合のみ)、自署(申請者から電子送付された場合のみ)及び同意書の構成(申請者から電子送付された場合のみ)が含まれる。
公文書署名情報	公文書管理情報、公文書に関する、署名生成に必要な情報である。ただし、審査結果が申請受理以外の場合、申請書、写真(申請者から電子送付された場合のみ)、自署(申請者から電子送付された場合のみ)及び同意書(申請者から電子送付された場合のみ)に関する、署名生成に必要な情報も含まれる。
職責署名	職責署名用 IC カードに格納される秘密鍵を用いて、公文書署名情報のハッシュ値を暗号化した署名値である。
職責証明書	職責署名用 IC カードから取り出された電子証明書である。
公文書	申請データ及び審査データから必要な情報を抽出した審査の結果となる情報である。
管理データ	管理データは、担当者情報及び事務所情報の総称である。管理データは、業務サービスが正常に動作するために必要なデータであり、業務管理者の操作に応じて、審査者端末から旅券申請審査サーバを経由し、旅券申請審査 DB サーバに登録される。また、旅券申請審査 DB サーバから旅券申請審査サーバを経由し、審査者端末に通知される。
担当者情報	旅券事務担当職員に関する情報である。旅券事務担当職員の人事情報が含まれる。
事務所情報	地方公共団体旅券事務所に関する情報である。事務所名、申請者へのメールフォーム、受領証情報、手数料情報が含まれる

以降では、表 2.5 で識別された保護資源をまとめて「保護対象資産」とする。

3. TOE セキュリティ環境

3.1. 前提条件

A.TRUST_ROLE

旅券事務所システム管理者、業務管理者、決裁者及び監視者は、信用できる人物であり、各々に許可された行為において不正は行わない。

A.SECRECY

審査者、旅券作成検査担当者及び交付担当者は、パスワード及び審査者端末に表示される保護対象資産の情報を他人に漏らすことはない。

A.MAINTAIN

保守担当者による作業は、旅券事務所システム管理者の監視のもとで実施され、不正な操作は行われない。

A.PHYSICAL_ACCESS

TOE が設置される筐体及び保護対象資産の複製物は、旅券事務所システム管理者以外の物理的アクセスが禁止されている。また、審査者端末が設置される部屋は、TOE に関係する人物以外の入室が禁止されている。

A.SUPPORT_CENTER

監視端末が設置される部屋は、監視者以外の入室が禁止されている。

A.CONNECT_NETWORK

TOE が設置されるネットワークと庁内ネットワークは、TOE の業務アプリケーションの機能に必要な通信以外の通過を禁止された特定個所で接続される。また、TOE と運用支援センター間は、TOE と運用支援センターのみが通信可能な閉域ネットワークで接続される。

A.TRUST_PKI

TOE が申請データの検証に利用する申請者証明書もしくは法定代理人証明書及び電子証明書の失効ステータスは信頼できる機関によって発行され、電子証明書の正しい失効ステータスが TOE に提供される。

A.TRUST_CRYPT

TOE が汎用受付システムもしくは審査者端末との暗号化通信に利用する、TOE 及び汎用受

付システムの電子証明書、TOE 及び汎用受付システムの秘密鍵、TOE 及び汎用受付システムの電子証明書の失効ステータスは信頼できる機関によって発行され、電子証明書の正しい失効ステータスが TOE に提供される。

A.IC_CARD

申請データの署名には、正当な IC カードが利用される。

3.2. 脅威

表 2.1 及び表 2.2 で識別された人物以外の者を「攻撃者」とする。

T.TAP

攻撃者により汎用受付システムあるいは審査者端末との通信データが盗聴または改ざんされ、保護対象資産の漏洩や破壊が起こる。

T.ID_SPOOF

旅券事務担当職員以外の地方公共団体旅券事務所職員が TOE の機能を利用することで、保護対象資産の漏洩や破壊が起こる。

T.EXCEED_ACCESS

審査者、旅券作成検査担当者及び交付担当者が担当する審査業務以外の操作を行うことで、保護対象資産の破壊が起こる。

T.MISTAKE

業務管理者による TOE 機能の誤操作により保護対象資産の削除が起こる。

T.FAKE_APPLICATION

攻撃者による不正な申請データを基に意図しない旅券が発給される。

不正な申請データとは以下を指す。

- 電子署名の付与後に修正された申請内容を含んだ申請データ
- 他人を装って申請された申請データ
- 申請内容に偽りを含む申請データ

T.ABUSE

申請棄却すべき申請データに対し審査者が正しい審査を行わないことにより、不適切な旅券が発給される。

T.FAKE_PHOTO&SIGN

攻撃者により郵送された、もしくは、審査者が持ち込んだ、申請者と異なる人物の写真または自署を基に意図しない旅券が発給される。

3.3. 組織のセキュリティ方針

P.OFFICIAL_DOCUMENT

TOE は、公文書が正当かつ有効なものであることを申請者に検証させるため、公文書に対する公的な電子署名を提供しなければならない。

P.INFRA

TOEは、インフラにおいて、特定の役割の正当性を確認できなければならない。また、システム運用管理を特定の役割に制限しなければならない。

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

O.CRYPT_MESSAGE

TOE は、汎用受付システム及び審査者端末との通信において、SSL 通信により通信データの保護を行う。

O.ID_AUTH

TOE は、業務アプリケーションが提供する機能を旅券事務担当職員のみに利用させるため、旅券事務担当職員に対してユーザ ID／パスワードを付与した上で、利用者とのセションの確立から終了までの間、以下のような制御を行う。

- 業務アプリケーションが提供する機能の利用前には、識別認証により必ず正当な利用者であることを確認する
- 業務アプリケーションが提供する機能の利用時には、審査者端末から無応答が続いた場合、該当するセションを切断する。

O.ACCESS_CONTROL

TOE は、審査業務をフェーズ毎に分割して役割を定義し、役割を割り当てられた旅券事務担当職員だけに各フェーズに対応する必要最小限の機能を提供する。

O.VERIFICATION

TOE は、電子署名を検証することにより、申請者から送られる申請データの完全性を検証する。また、電子証明書の有効性を確認することにより、申請データの正当性を検証する。

O.AUDIT

TOE は、セキュリティ関連事象を記録し、記録した監査情報格納領域を管理する。また、旅券事務所システム管理者及び監視者のみに監査記録を表示する。加えて、セキュリティ侵害を監視し、セキュリティ侵害発生時には、アラートを監視端末に通知する。

O.APP_ADMIN

TOE は、業務アプリケーションにおける旅券事務担当職員の識別認証、セション管理及びアクセス制御に関する運用管理を業務管理者のみに制限する。

O.INFRA_ADMIN

TOE は、インフラにおけるシステム運用管理を旅券事務所システム管理者及び監視者のみに制限する。

O.INFRA_I&A

TOE は、インフラの機能を利用する前に、旅券事務所システム管理者または監視者の正当性を必ず確認する。

4.2. 環境のセキュリティ対策方針

OE.TRUST_ROLE

システム責任者は TOE に関わる特権利用者として適切な人物を以下の役割に任命する。

- 旅券事務所システム管理者
- 業務管理者
- 決裁者
- 監視者

また、任命した人物に対して情報セキュリティ教育及び啓蒙を実施し、システム運用管理に関する規則を遵守することに同意させる。

OE.SECRECY

システム責任者は、審査者、旅券作成検査担当者及び交付担当者に対して、情報セキュリティ教育及び啓蒙を実施する。情報セキュリティ教育及び啓蒙によって、地方公務員法を遵守し、業務上必要な情報や知り得た情報の扱いにおいて不正は行わないことに同意させる。

OE.MAINTAIN

旅券事務所システム管理者は保守担当者が正しく保守作業を行うことを監視する。

OE.PHYSICAL_ACCESS

旅券事務所システム管理者は、自身以外の物理的アクセスを禁止できる施錠可能なラック内に TOE を設置する。また、保護対象資産の複製物は旅券事務所システム管理者により施錠管理された場所で保管される。更に、審査者端末が設置される部屋は、施錠管理により TOE に関係する人物以外の入室を禁止する。

OE.SUPPORT_CENTER

監視端末が設置される部屋への入室管理として、バイオ認証システムによる監視者の本人確認を行う。

OE.CONNECT_NETWORK

旅券事務所システム管理者は、庁内ネットワークと TOE が設置されるネットワーク間にファイアウォールを設置し、TOE の業務アプリケーションの機能に必要な通信以外の通過を禁止する。また、TOE と運用支援センターは IP-VPN を介して接続する。

OE.TRUST_PKI

TOE が申請データの検証に利用する電子証明書及び電子証明書の失効ステータスは、地方公共団体によって運営される JPKI によって発行される。また、電子証明書の失効ステータスは、正当性や完全性が保証された JPKI の手続きに従って TOE に提供される。

OE.TRUST_CRYPT

TOE が汎用受付システムもしくは審査者端末との暗号化通信に利用する、TOE 及び汎用受付システムの電子証明書、TOE 及び汎用受付システムの秘密鍵、TOE 及び汎用受付システムの電子証明書の失効ステータスは、地方公共団体によって運用される LGPKI 及び外務省 CA によって発行される。また、汎用受付システムの電子証明書の失効ステータスは、正当性や完全性が保証された LGPKI の手続きに従って TOE に提供される。TOE の電子証明書が失効した場合には、外務省 CA より電子証明書が失効した旨が連絡される。

OE.DATA_PROTECT

旅券事務所システム管理者は毎日保護対象資産のバックアップ作業を行い、誤操作によって保護対象資産が削除された場合でも、直前のバックアップ完了状態までの復旧を可能にする。

OE.OFFICIAL_DOCUMENT

決裁者及び業務管理者は、公文書へ公的な電子署名を提供するために、地方公共団体によって運用される LGPKI の職責署名用 IC カードを利用して、職責署名の生成と付与を行う。

OE.VERIFICATION

審査者、決裁者及び業務管理者は、申請者から送付される電子証明書の有効性の確認を行うために、JPKI を利用する。

OE.TRUST_EXAMINATION

決裁者は、審査者が行った審査内容の正当性を検証する。

OE.FAKE_PHOTO&SIGN

交付担当者は、申請者への旅券交付時に、申請者が持参するはがき及び身元確認書類と申請データの突合確認を行い、記載内容や写真を基に申請者本人であることを確認した後に旅券を交付する。交付担当者による本人確認は、業務管理者による監視もしくは複数の交付担当者による相互確認によって十分な確認を行う。

OE.IC_CARD

申請データへの署名は、本人に対して発行された公的個人認証 IC カードで行う。

OE.ROLE_ASSIGN

システム責任者は、審査業務を各フェーズに区切り、旅券事務担当職員を、各フェーズを担当する役割及び審査業務を管理する役割として割り当てる。旅券事務担当職員は、担当するフェーズ順に審査業務を実施し、申請内容が正しいことを確認し、TOE へ結果を登録する。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

TOE セキュリティ機能要件を表 5.1 に示す。

表 5.1 TOE セキュリティ機能要件一覧

セキュリティ機能要件			コンポーネント
セキュリティ監査	セキュリティ監査自動応答	セキュリティアラーム	FAU_ARP.1
	セキュリティ監査データ生成	監査データ生成	FAU_GEN.1
	セキュリティ監査分析	侵害の可能性の分析	FAU_SAA.1
	セキュリティ監査レビュー	監査レビュー	FAU_SAR.1
	セキュリティ監査事象格納	保護された監査証跡格納	FAU_STG.1
		監査データ損失の恐れ発生時のアクション	FAU_STG.3
暗号サポート	暗号鍵管理	暗号鍵生成	FCS_CKM.1
		暗号鍵破棄	FCS_CKM.4(a)
			FCS_CKM.4(b)
	暗号操作	暗号操作	FCS_COP.1(a)
			FCS_COP.1(b)
			FCS_COP.1(c)
利用者データ保護	アクセス制御方針	サブセットアクセス制御	FDP_ACC.1
	アクセス制御機能	セキュリティ属性によるアクセス制御	FDP_ACF.1
	TSF 間利用者データ完全性転送保護	データ交換完全性	FDP_UIT.1
識別と認証	利用者属性定義	利用者属性定義	FIA_ATD.1
	秘密についての仕様	秘密の検証	FIA_SOS.1
	利用者認証	認証のタイミング	FIA_UAU.1

セキュリティ機能要件			コンポーネント
		アクション前の利用者認証	FIA_UAU.2(a)
		アクション前の利用者認証	FIA_UAU.2(b)
		保護された認証フィードバック	FIA_UAU.7
	利用者識別	識別のタイミング	FIA_UID.1
		アクション前の利用者識別	FIA_UID.2(a)
		アクション前の利用者識別	FIA_UID.2(b)
	利用者･サブジェクト結合	利用者・サブジェクト結合	FIA_USB.1
セキュリティ管理	TSF における機能の管理	セキュリティ機能のふるまいの管理	FMT_MOF.1
	セキュリティ属性の管理	セキュアなセキュリティ属性	FMT_MSA.2(a)
		セキュアなセキュリティ属性	FMT_MSA.2(b)
		セキュアなセキュリティ属性	FMT_MSA.2(c)
	TSF データの管理	TSF データの管理	FMT_MTD.1(a)
			FMT_MTD.1(b)
			FMT_MTD.1(c)
			FMT_MTD.1(d)
			FMT_MTD.1(e)
			FMT_MTD.1(f)
	管理機能の特定	管理機能の特定	FMT_SMF.1
	セキュリティ管理役割	セキュリティ役割	FMT_SMR.1(a)
			FMT_SMR.1(b)
TSF の保護	リファレンス調停	TSP の非バイパス性	FPT_RVM.1
	ドメイン分離	TSF ドメイン分離	FPT_SEP.1
	タイムスタンプ	高信頼タイムスタンプ	FPT_STM.1
TOE アクセス	セションロック	TSF 起動による終了	FTA_SSL.3

セキュリティ機能要件			コンポーネント
高信頼パス／チャネル	TSF 間高信頼チャネル	TSF 間高信頼チャネル	FTP_ITC.1
	高信頼パス	高信頼パス	FTP_TRP.1

FAU_ARP.1　　セキュリティアラーム

下位階層：なし

FAU_ARP.1.1

TSF は、セキュリティ侵害の可能性が検出された場合、[割付: 混乱を最小にする*アクションのリスト*]を実行しなければならない。

[割付: 混乱を最小にする*アクションのリスト*]
監視端末へのアラート通知

依存性：FAU_SAA.1 侵害の可能性の分析

FAU_GEN.1　　監査データの生成

下位階層：なし

FAU_GEN.1.1

TSFは、以下の監査対象事象の監査記録を生成できなければならない：

a) 監査機能の起動と終了;

b) 監査の[選択：*最小*、*基本*、*詳細*、*指定なし*]レベルのすべての監査対象事象;及び

c) [割付：*上記以外の個別に定義した監査対象事象*]。

[選択：*最小*、*基本*、*詳細*、*指定なし*]

最小

表 5.2 監査事象一覧

セキュリティ機能要件	監査レベル	監査の要件	実際の監査項目
FAU_ARP.1	最小	切迫したセキュリティ侵害によってとられるアクション	監視端末へのアラート通知事象
FAU_GEN.1	－	－	－
FAU_SAR.1	－	－	－
FAU_SAA.1	最小	すべての分析メカニズムの活性化/非活性化	監査ログ監視エージェントの起動事象／停止事象
	最小	ツールによって実行される自動応答	監視端末へのアラート通知事象
FAU_STG.1	－	－	－
FAU_STG.3	－	－	－
FCS_CKM.1	最小	動作の成功と失敗	汎用受付システムと TOE 間の SSL 通信における成功事象／失敗事象
FCS_CKM.4(a)	最小	動作の成功と失敗	審査者端末と TOE 間の SSL 通信における成功事象／失敗事象
FCS_CKM.4(b)	最小	動作の成功と失敗	汎用受付システムと TOE 間の SSL 通信における成功事象／失敗事象

セキュリティ機能要件	監査レベル	監査の要件	実際の監査項目
FCS_COP.1(a)	最小	成功と失敗及び暗号操作の種別	・ 申請者署名の検証における成功事象／失敗事象 ・ 法定代理人署名の検証における成功事象／失敗事象
FCS_COP.1(b)	最小	成功と失敗及び暗号操作の種別	審査者端末と TOE 間の SSL 通信における成功事象／失敗事象
FCS_COP.1(c)	最小	成功と失敗及び暗号操作の種別	汎用受付システムと TOE 間の SSL 通信における成功事象／失敗事象
FDP_ACC.1	－	－	－
FDP_ACF.1	最小	SFP で扱われるオブジェクトに対する操作の実行における成功した要求	・ 申請者署名の検証における成功事象 ・ 申請者証明書の有効性確認における成功事象 ・ 申請データの登録における成功事象 ・ 申請データの削除における成功事象 ・ 申請書、写真、自署、同意書の閲覧における成功事象 ・ 法定代理人署名の検証における成功事象 ・ 法定代理人証明書の有効性確認における成功事象 ・ 審査情報、官公庁記載欄情報、審査状態情報の閲覧における成功事象 ・ 審査情報、官公庁記載欄情報の入力における成功事象 ・ 書類確認結果、決裁結果、審査結果、旅券検査結果、交付結果の登録における成功事象 ・ 申請取得完了通知、書類確認完了通知、審査完了通知、決裁完了通知の生成における成功事象 ・ 職責署名の付与における成功事象 ・ 公文書データの生成における成功事象

セキュリティ機能要件	監査レベル	監査の要件	実際の監査項目
			・ 公文書の閲覧における成功事象 ・ 担当者情報、事務所情報の登録における成功事象 ・ 担当者情報、事務所情報の変更における成功事象 ・ 担当者情報の削除における成功事象
FDP_UIT.1	最小	データ交換メカニズムを使用する利用者あるいはサブジェクトの識別情報	・ 申請者署名の検証における成功事象／失敗事象 ・ 法定代理人署名の検証における成功事象／失敗事象
FIA_ATD.1	－	－	－
FIA_SOS.1	最小	TSF による、テストされた秘密の拒否	業務アプリケーションのパスワード規則における不適合事象
FIA_UAU.1	最小	認証メカニズムの不成功になった使用	旅券事務所システム管理者の識別認証における失敗事象
FIA_UAU.2(a)	最小	認証メカニズムの不成功になった使用	旅券事務担当職員の識別認証における失敗事象
FIA_UAU.2(b)	最小	認証メカニズムの不成功になった使用	監視者の識別認証における失敗事象
FIA_UAU.7	－	－	－
FIA_UID.1	最小	提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用	旅券事務所システム管理者の識別認証における失敗事象
FIA_UID.2(a)	最小	提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用	旅券事務担当職員の識別認証における失敗事象
FIA_UID.2(b)	最小	提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用	監視者の識別認証における失敗事象

セキュリティ機能要件	監査レベル	監査の要件	実際の監査項目
FIA_USB.1	最小	利用者セキュリティ属性のサブジェクトに対する不成功結合	旅券事務担当職員の役割情報取得における失敗事象
FMT_MOF.1	－	－	－
FMT_MSA.2(a)	最小	セキュリティ属性に対して提示され、拒否された値すべて	申請者証明書もしくは法定代理人証明書の有効期間確認における有効期間外事象
FMT_MSA.2(b)	最小	セキュリティ属性に対して提示され、拒否された値すべて	審査者端末と TOE 間の SSL 通信における失敗事象
FMT_MSA.2(c)	最小	セキュリティ属性に対して提示され、拒否された値すべて	汎用受付システムと TOE 間の SSL 通信における失敗事象
FMT_MTD.1(a)	－	－	－
FMT_MTD.1(b)	－	－	－
FMT_MTD.1(c)	－	－	－
FMT_MTD.1(d)	－	－	－
FMT_MTD.1(e)	－	－	－
FMT_MTD.1(f)	－	－	－
FMT_SMF.1	最小	管理機能の使用	・ 旅券事務担当職員の登録事象 ・ 旅券事務担当職員の削除事象 ・ 旅券事務担当職員のパスワード変更事象 ・ 決裁者、審査者、旅券作成検査担当者及び交付担当者の役割情報変更事象 ・ 旅券事務所システム管理者及び監視者のパスワード変更事象 ・ シグネチャ、システム内時刻の問い合わせ事象及び変更事象
FMT_SMR.1(a)	最小	役割の一部をなす利用者のグループに対する改変	・ 旅券事務担当職員の削除事象 ・ 決裁者、審査者、旅券作成検査担当者、交付担当者の役割情報変更事象

セキュリティ機能要件	監査レベル	監査の要件	実際の監査項目
FMT_SMR.1(b)	最小	役割の一部をなす利用者のグループに対する改変	旅券事務所システム管理者及び監視者の役割を付与された利用者は固定であるため、監査対象とならない
FPT_RVM.1	－	－	－
FPT_SEP.1	－	－	－
FPT_STM.1	最小	時間の変更	システム内時刻の変更事象
FTA_SSL.3	最小	セションロックメカニズムによる対話セションの終了	タイムアウトによるセション切断事象
FTP_ITC.1	最小	高信頼チャネル機能の失敗	汎用受付システムと TOE 間の通信確立における失敗事象
	最小	失敗した高信頼チャネル機能の開始者とターゲットの識別	汎用受付システム-TOE 間の通信確立を失敗した利用者のユーザ ID、ターゲットの IP アドレス
FTP_TRP.1	最小	高信頼パス機能の失敗	審査者端末と TOE 間の通信確立における失敗事象
	最小	もし得られれば、すべての高信頼パス失敗に関係する利用者の識別情報	審査者端末-TOE 間の通信確立を失敗した利用者のユーザ ID

[割付：*上記以外の個別に定義した監査対象事象*]

- 監査ログ格納領域の閾値越え事象
- 旅券事務所担当職員の識別認証成功事象
- 申請者証明書の有効性確認における失敗事象
- 法定代理人証明書の有効性確認における失敗事象
- 申請データの登録における失敗事象
- 申請データの削除における失敗事象
- 申請書、写真、自署、同意書の閲覧における失敗事象
- 審査情報、官公庁記載欄情報、審査状態情報の閲覧における失敗事象
- 審査情報、官公庁記載欄情報の入力における失敗事象
- 書類確認結果、決裁結果、審査結果、旅券検査結果、交付結果の登録における失敗事象
- 申請取得完了通知、書類確認完了通知、審査完了通知、決裁完了通知の生成に

おける失敗事象
- 職責署名の付与における失敗事象
- 公文書データの生成における失敗事象
- 公文書の閲覧における失敗事象
- 担当者情報、事務所情報の登録における失敗事象
- 担当者情報、事務所情報の変更における失敗事象
- 担当者情報の削除における失敗事象
- 申請データの取得における成功事象と失敗事象
- 公文書データの登録における成功事象と失敗事象
- 状態通知情報の通知における成功事象と失敗事象
- ログインユーザ一覧表示事象
- 業務管理者による手動セション切断事象

FAU_GEN.1.2

TSFは、各監査記録において少なくとも以下の情報を記録しなければならない：

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)；及び

b) 各監査事象種別に対して、PP／STの機能コンポーネントの監査対象事象の定義に基づいた、[割付：*その他の監査関連情報*]

[割付：*その他の監査関連情報*]

重要度（emerg、alert、crit、err、exception、TNS-、ORA-、warning、notice、infoのいずれか）

依存性：FPT_STM.1 高信頼タイムスタンプ

FAU_SAA.1　　侵害の可能性の分析

下位階層：なし

FAU_SAA.1.1

TSF は、監査事象のモニタに規則のセットを適用し、これらの規則に基づき TSP 侵害の可能性を示すことができなければならない。

FAU_SAA.1.2

TSF は、監査事象をモニタするための以下の規則を実施しなければならない;

a) セキュリティ侵害の可能性を示すものとして知られている[割付: *定義された監査対象事象のサブセット*]をすべて合わせた、あるいは組み合わせたもの;

b) [割付: *その他の規則*]。

[割付: *定義された監査対象事象のサブセット*]

すべての監査対象事象に関して、シグネチャ（注）として選択された重要度のいずれかと共に監査ログが生成された場合に、セキュリティ侵害の可能性があると判断する。シグネチャとして選択可能な重要度のリストは以下である。

- emerg
- alert
- crit
- err
- exception
- TNS-
- ORA-
- Warning

（注）シグネチャとは、セキュリティ侵害の可能性を判断する基準である重要度を意味し、上記リストの中から１つ選択される

[割付: *その他の規則*]

なし

依存性：FAU_GEN.1 監査データ生成

FAU_SAR.1　　監査レビュー

下位階層：なし

FAU_SAR.1.1

TSF は、[割付：許可利用者]が、[割付：監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付：許可利用者]
旅券事務所システム管理者
監視者

[割付：監査情報のリスト]
すべての監査情報

FAU_SAR.1.2

TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性：FAU_GEN.1 監査データ生成

FAU_STG.1　　保護された監査証跡格納

下位階層：なし

FAU_STG.1.1

TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2

TSF は、監査記録の改変を[選択：*防止*、*検出*]できねばならない。

[選択：*防止*、*検出*]
防止

依存性：FAU_GEN.1 監査データ生成

FAU_STG.3　　監査データ損失恐れ発生時のアクション

下位階層：なし

FAU_STG.3.1

TSF は、監査証跡が[割付：*事前に定義された限界*]を超えた場合、[割付：*監査格納失敗の恐れ発生時のアクション*]をとらなければならない。

[割付：*事前に定義された限界*]
監査ログ格納領域の 80%

[割付：*監査格納失敗の恐れ発生時のアクション*]
監査ログの生成（その後、当該監査ログ情報は、セキュリティ侵害の可能性ありと判断され、監視端末へのアラート通知が行われる）

依存性：FAU_STG.1 保護された監査証跡格納

FCS_CKM.1　　暗号鍵生成

下位階層：なし

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、暗号鍵を生成しなければならない。

[割付：*標準のリスト*]
DES：FIPS PUB 46-3
3DES：FIPS PUB 46-3
RSA：PKCS#1
RC4：仕様公開されていないが、ISO/IEC9979 に登録されている国際標準である

[割付：*暗号鍵生成アルゴリズム*]
DES、3DES、RSA、RC4

[割付：*暗号鍵長*]
DES：56bit
3DES：168bit
RSA：1024bit
RC4：128bit

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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4(a)　暗号鍵破棄

下位階層：なし

FCS_CKM.4.1(a)

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、暗号鍵を破棄しなければならない。

[割付：*標準のリスト*]
SSL プロトコル仕様

[割付：*暗号鍵破棄方法*]
SSL プロトコルに従った破棄方法

依存性：~~[FDP_ITC.1 セキュリティ属性なし利用者データのインポート または FCS_CKM.1 暗号鍵生成]~~
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4(b)　暗号鍵破棄

下位階層：なし

FCS_CKM.4.1(b)

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、暗号鍵を破棄しなければならない。

[割付：*標準のリスト*]
SSL プロトコル仕様

[割付：*暗号鍵破棄方法*]
SSL プロトコルに従った破棄方法

依存性：[FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1(a)　暗号操作

下位階層：なし

FCS_COP.1.1(a)

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*]
SHA-1：FIPS PUB 180-2
RSA：PKCS#1

[割付：*暗号アルゴリズム*]
SHA-1、RSA

[割付：*暗号鍵長*]
RSA：1024bit、2048bit

[割付：*暗号操作のリスト*]
申請書構成管理情報の申請者署名に対する署名検証
同意書の法定代理人署名に対する署名検証

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 FCS_CKM.1 暗号鍵生成]~~
~~FCS_CKM.4 暗号鍵破棄~~
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1(b)　暗号操作

下位階層：なし

FCS_COP.1.1(b)

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*]
DES：FIPS PUB 46-3
3DES：FIPS PUB 46-3
RSA：PKCS#1
RC4：仕様公開されていないが、ISO/IEC9979 に登録されている国際標準である
MD5：RFC1321
SHA-1：FIPS 180-2

[割付：*暗号アルゴリズム*]
DES、3DES、RSA、RC4、MD5、SHA-1

[割付：*暗号鍵長*]
DES：56bit
3DES：168bit
RSA：1024bit
RC4：128bit

[割付：*暗号操作のリスト*]
審査者端末-TOE 間の通信データの SSL を利用した暗号化
審査者端末-TOE 間の通信データの SSL を利用した復号化

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 FCS_CKM.1 暗号鍵生成]~~
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1(c)　暗号操作

下位階層：なし

FCS_COP.1.1(c)

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*]
DES：FIPS PUB 46-3
3DES：FIPS PUB 46-3
RSA：PKCS#1
RC4：仕様公開されていないが、ISO/IEC9979 に登録されている国際標準である
MD5：RFC1321
SHA-1：FIPS 180-2

[割付：*暗号アルゴリズム*]
DES、3DES、RSA、RC4、MD5、SHA-1

[割付：*暗号鍵長*]
DES：56bit
3DES：168bit
RSA：1024bit
RC4：128bit

[割付：*暗号操作のリスト*]
汎用受付システム-TOE 間の通信データの SSL を利用した暗号化
汎用受付システム-TOE 間の通信データの SSL を利用した復号化

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 FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FDP_ACC.1　　サブセットアクセス制御方針

下位階層：なし

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。

[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*]
サブジェクト：
表 5.3 によって識別される役割を付与された旅券事務担当職員を代行するプロセス

オブジェクト：
表 5.3 によって識別される資源を含むファイル

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：
表 5.3 において役割と資源が対応するセルに識別される操作

表 5.3 旅券事務担当職員アクセス制御方針が適用されるサブジェクト、オブジェクト及びサブジェクトとオブジェクト間の操作

役割 / 資源	業務管理者	決裁者	審査者	旅券作成検査担当者	交付担当者
申請書構成管理情報	・申請者署名検証 ・申請者証明書有効性確認 ・登録 ・削除	・申請者署名検証 ・申請者証明書有効性確認 ・登録	・申請者署名検証 ・申請者証明書有効性確認 ・登録	－	－

役割 / 資源	業務管理者	決裁者	審査者	旅券作成検査担当者	交付担当者
申請書	・閲覧 ・登録 ・削除	・閲覧 ・登録	・閲覧 ・登録	・閲覧	・閲覧
写真	・閲覧 ・登録 ・削除	・閲覧 ・登録	・閲覧 ・登録	・閲覧	・閲覧
自署	・閲覧 ・登録 ・削除	・閲覧 ・登録	・閲覧 ・登録	・閲覧	・閲覧
同意書	・閲覧 ・法定代理人署名検証 ・法定代理人証明書有効性確認 ・登録 ・削除	・閲覧 ・法定代理人署名検証 ・法定代理人証明書有効性確認 ・登録	・閲覧 ・法定代理人署名検証 ・法定代理人証明書有効性確認 ・登録	・閲覧	・閲覧
審査情報	・閲覧 ・入力	・閲覧 ・入力	・閲覧 ・入力	・閲覧	・閲覧
官公庁記載欄情報	・閲覧 ・入力	・閲覧 ・入力	・閲覧 ・入力	・閲覧 ・入力	・閲覧 ・入力
審査状態情報	・閲覧 ・交付結果登録 ・旅券検査結果登録 ・書類確認結果登録 ・審査結果登録 ・決裁結果登録	・閲覧 ・交付結果登録 ・旅券検査結果登録 ・書類確認結果登録 ・審査結果登録 ・決裁結果登録	・閲覧 ・交付結果登録 ・旅券検査結果登録 ・書類確認結果登録 ・審査結果登録	・閲覧 ・旅券検査結果登録	・閲覧 ・交付結果登録

役割 / 資源	業務管理者	決裁者	審査者	旅券作成検査担当者	交付担当者
状態通知情報	・申請取得完了通知生成 ・書類確認完了通知生成 ・審査完了通知生成 ・決裁完了通知生成	・申請取得完了通知生成 ・書類確認完了通知生成 ・審査完了通知生成 ・決裁完了通知生成	・申請取得完了通知生成 ・書類確認完了通知生成 ・審査完了通知生成	－	－
公文書構成管理情報	・職責署名付与 ・生成	・職責署名付与 ・生成	－	－	－
公文書	・閲覧 ・生成	・閲覧 ・生成	・閲覧	・閲覧	・閲覧
担当者情報	・登録 ・変更 ・削除	－	－	－	－
事務所情報	・登録 ・変更	－	－	－	－

[割付：*アクセス制御 SFP*]
旅券事務担当職員アクセス制御方針

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

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

FDP_ACF.1.1

TSF は、[割付：*セキュリティ属性、名前付けされたセキュリティ属性のグループ*]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：*セキュリティ属性、名前付けされたセキュリティ属性のグループ*]
役割情報（表 5.3 で識別される役割を表すセキュリティ属性）
資源情報（表 5.3 で識別される資源を表すセキュリティ属性）
操作情報（表 5.3 で識別される操作を表すセキュリティ属性）

[割付：*アクセス制御 SFP*]
旅券事務担当職員アクセス制御方針

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*]
制御されたサブジェクト（役割情報で識別される役割権限を付与された旅券事務担当職員を代行するプロセス）から制御されたオブジェクト（資源情報で識別される資源）へのアクセスは、そのアクセスの内容（操作情報で識別される操作）が表 5.3 にて特定された当該サブジェクトとオブジェクトが対応するセルに識別された操作に一致した場合、許可される。それ以外の場合は拒否される。

FDP_ACF.1.3

TSF は、以下の追加規則に基づいて、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承認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承認する規則*]。

[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承認する規則*]
なし

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*]
なし

依存性：FDP_ACC.1 サブセットアクセス制御
~~FMT_MSA.3 静的属性の初期化~~

FDP_UIT.1　　データ交換完全性

下位階層：なし

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(s)及び／あるいは情報フロー制御 SFP(s)]を実施しなければならない。

[選択：改変、消去、挿入、リプレイ]
改変

[選択：送信、受信]
受信

[割付：アクセス制御 SFP(s)及び／あるいは情報フロー制御]
旅券事務担当職員アクセス制御方針

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]

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]

FIA_ATD.1　　利用者属性定義

下位階層：なし

FIA_ATD.1.1

TSF は個々の利用者に属する以下のセキュリティ属性のリスト[割付：*セキュリティ属性のリスト*]を維持しなければならない。

[割付：*セキュリティ属性のリスト*]
役割情報（取り扱う役割情報は、業務管理者、決裁者、審査者、旅券作成検査担当者、交付担当者）

詳細化：TSF→業務アプリケーションの TSF

依存性：なし

FIA_SOS.1　　秘密の検証

下位階層：なし

FIA_SOS.1.1

TSF は、秘密が[割付：*定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。

[割付：*定義された品質尺度*]
パスワード文字長：6 バイト以上 12 バイト以下
使用可能な文字種：半角数字　0～9
半角英文字　a～z A～Z
記号　＃＄’（）＊＋，－．／：＝？@［￥］_｀｛｝~！

依存性：なし

FIA_UAU.1　　認証のタイミング

下位階層：なし

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調停アクションのリスト*]を許可しなければならない。

[割付：*TSF調停アクションのリスト*]

- 言語の選択
- GUIでのログイン、コマンドラインからのログインの選択
- ログインサーバの選択
- ヘルプの参照

詳細化：TSF→インフラの TSF
　　利用者→旅券事務所システム管理者

FIA_UAU.1.2

TSF は、その利用者を代行する他の TSF 調停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。

詳細化：TSF→インフラの TSF
　　利用者→旅券事務所システム管理者

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.2(a)　アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1(a)

TSFは、その利用者を代行する他のTSF調停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。

詳細化：TSF→業務アプリケーションの TSF
利用者→業務管理者、決裁者、審査者、旅券作成検査担当者、
交付担当者

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.2(b)　アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1(b)

TSFは、その利用者を代行する他のTSF調停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。

詳細化：TSF→インフラの TSF
利用者→監視者

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.7　　保護された認証フィードバック

下位階層：なし

FIA_UAU.7.1

TSFは、認証を行っている間、[割付：*フィードバックのリスト*]だけを利用者に提供しなければならない。

[割付：*フィードバックのリスト*]
パスワード入力文字数分のダミー文字(アスタリスク：*)

依存性：FIA_UAU.1 認証のタイミング

FIA_UID.1　　識別のタイミング

下位階層：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 調停アクションのリスト*]を許可しなければならない。

[割付：*TSF 調停アクションのリスト*]
言語の選択
GUI でのログイン、コマンドラインからのログインの選択
ログインサーバの選択
ヘルプの参照

詳細化：TSF→インフラの TSF
利用者→旅券事務所システム管理者

FIA_UID.1.2

TSF は、その利用者を代行する他の TSF 調停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。

詳細化：TSF→インフラの TSF
　　利用者→旅券事務所システム管理者

依存性：なし

FIA_UID.2(a)　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1(a)

TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化：TSF→業務アプリケーションの TSF
利用者→業務管理者、決裁者、審査者、旅券作成検査担当者、
交付担当者

依存性：なし

FIA_UID.2(b)　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1(b)

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化：TSF→インフラの TSF
利用者→監視者

依存性：なし

FIA_USB.1　　利用者・サブジェクトの結合

下位階層：なし

FIA_USB.1.1(a)

TSF は、適切な利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。

詳細化：TSF→業務アプリケーションの TSF

依存性：FIA_ATD.1 利用者属性定義

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

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*]
- セション管理機能

[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*]
のふるまいを決定する、のふるまいを改変する

[割付：*許可された識別された役割*]
業務管理者

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_MSA.2(a)　セキュアなセキュリティ属性

下位階層：なし

FMT_MSA.2.1(a)

TSFは、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性：~~ADV_SPM.1 非形式的TOEセキュリティ方針モデル~~

[FDP_ACC.1 サブセットアクセス制御　または

FDP_IFC.1 サブセット情報フロー制御]

~~FMT_MSA.1 セキュリティ属性の管理~~

~~FMT_SMR.1 セキュリティ役割~~

FMT_MSA.2(b)　セキュアなセキュリティ属性

下位階層：なし

FMT_MSA.2.1(b)

TSFは、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性：~~ADV_SPM.1 非形式的TOEセキュリティ方針モデル~~
~~[FDP_ACC.1 サブセットアクセス制御　または~~
~~FDP_IFC.1 サブセット情報フロー制御]~~
~~FMT_MSA.1 セキュリティ属性の管理~~
~~FMT_SMR.1 セキュリティ役割~~

FMT_MSA.2(c)　セキュアなセキュリティ属性

下位階層：なし

FMT_MSA.2.1(c)

TSFは、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性：~~ADV_SPM.1 非形式的TOEセキュリティ方針モデル~~
~~[FDP_ACC.1 サブセットアクセス制御　または~~
~~FDP_IFC.1 サブセット情報フロー制御]~~
~~FMT_MSA.1 セキュリティ属性の管理~~
~~FMT_SMR.1 セキュリティ役割~~

FMT_MTD.1(a)　TSF データの管理

下位階層：なし

FMT_MTD.1.1(a)

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*]

- 業務管理者のパスワード
- 決裁者のパスワード
- 決裁者の役割情報
- 審査者のパスワード
- 審査者の役割情報
- 旅券作成検査担当者のパスワード
- 旅券作成検査担当者の役割情報
- 交付担当者のパスワード
- 交付担当者の役割情報

[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*]]
改変

[割付：*その他の操作*]
なし

[割付：*許可された識別された役割*]
業務管理者

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(b)　TSF データの管理

下位階層：なし

FMT_MTD.1.1(b)

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*]

- 業務管理者のユーザ ID
- 業務管理者のパスワード
- 業務管理者の役割情報
- 決裁者のユーザ ID
- 決裁者のパスワード
- 決裁者の役割情報
- 審査者のユーザ ID
- 審査者のパスワード
- 審査者の役割情報
- 旅券作成検査担当者のユーザ ID
- 旅券作成検査担当者のパスワード
- 旅券作成検査担当者の役割情報
- 交付担当者のユーザ ID
- 交付担当者のパスワード
- 交付担当者の役割情報

[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*]]

削除（ただし、削除操作を行う業務管理者自身のユーザ ID、パスワード、役割情報を削除することはできない）

[割付：*その他の操作*]

登録

[割付：*許可された識別された役割*]

業務管理者

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(c)　TSF データの管理

下位階層：なし

FMT_MTD.1.1(c)

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*]

- セキュリティ侵害の可能性ありと判断するシグネチャ

[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*]]

問い合わせ、改変

[割付：*その他の操作*]

なし

[割付：*許可された識別された役割*]

旅券事務所システム管理者

監視者

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(d)　TSF データの管理

下位階層：なし

FMT_MTD.1.1(d)

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*]
- 監視者のパスワード

[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*]]
改変

[割付：*その他の操作*]
なし

[割付：*許可された識別された役割*]
旅券事務所システム管理者
監視者

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(e)　TSF データの管理

下位階層：なし

FMT_MTD.1.1(e)

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*]

- システム内時刻

[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*]]

問い合わせ、改変

[割付：*その他の操作*]

なし

[割付：*許可された識別された役割*]

旅券事務所システム管理者

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(f)　TSF データの管理

下位階層：なし

FMT_MTD.1.1(f)

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*]
- 旅券事務所システム管理者のパスワード

[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*]]
改変

[割付：*その他の操作*]
なし

[割付：*許可された識別された役割*]
旅券事務所システム管理者

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_SMF.1　　管理機能の特定

下位階層：なし

FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]

[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]
「表 5.4 管理項目一覧」にて識別された「実際の確認項目」を管理する機能

表 5.4 管理項目一覧

セキュリティ機能要件	管理の要件（参考情報）	実際の管理項目
FAU_ARP.1	アクションの管理(追加、除去、改変)	なし（アクションは固定であり、管理対象とならない）
FAU_GEN.1	－	－
FAU_SAA.1	規則のセットから規則を(追加、改変、削除)することによる規則の維持	セキュリティ侵害の可能性ありと判断するシグネチャの管理
FAU_SAR.1	監査記録に対して読み出し権のある利用者グループの維持（削除、改変、追加）	なし（旅券事務所システム管理者、監視者は固定であり、管理対象とならない）
FAU_STG.1	－	－
FAU_STG.3	閾値の維持	なし（閾値は固定であり、管理対象とならない）
	監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)	なし（アクションは固定であり、管理対象とならない）
FCS_CKM.1	暗号鍵属性の変更の管理	なし（対象となる暗号鍵は暗号化通信に利用する共通鍵のみであり、管理対象とならない）

セキュリティ機能要件	管理の要件（参考情報）	実際の管理項目
FCS_CKM.4(a)	暗号鍵属性の変更の管理	なし（対象となる暗号鍵は暗号化通信に利用する共通鍵のみであり、管理対象とならない）
FCS_CKM.4(b)	暗号鍵属性の変更の管理	なし（対象となる暗号鍵は暗号化通信に利用する共通鍵のみであり、管理対象とならない）
FCS_COP.1(a)	－	－
FCS_COP.1(b)	－	－
FCS_COP.1(c)	－	－
FDP_ACC.1	－	－
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	なし（アクセス制御の方針は固定であり、管理対象とならない）
FDP_UIT.1	—	—
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる	役割情報（業務管理者、決裁者、審査者、旅券作成検査担当者、交付担当者）
FIA_SOS.1	秘密の検証に使用される尺度の管理	なし（パスワードの基準は固定であり、管理対象とならない）
FIA_UAU.1	管理者による認証データの管理	旅券事務所システム管理者のパスワード
	関係する利用者による認証データの管理	旅券事務所システム管理者のパスワード
	利用者が認証される前にとられるアクションのリストを管理すること	なし（アクションは固定であり、管理対象とならない）
FIA_UAU.2(a)	管理者による認証データの管理	審査者、決裁者、旅券作成検査担当者、交付担当者、業務管理者のパスワード
	このデータに関係する利用者による認証データの管理	なし（パスワードの管理は業務管理者のみに制限されているため、管理対象とならない）

セキュリティ機能要件	管理の要件（参考情報）	実際の管理項目
FIA_UAU.2(b)	管理者による認証データの管理	監視者のパスワード
	このデータに関係する利用者による認証データの管理	監視者のパスワード
FIA_UAU.7	－	－
FIA_UID.1	利用者識別情報の管理	なし（旅券事務所システム管理者のユーザ ID は固定であり、管理対象とならない）
	許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること	なし（識別前に利用可能なアクションリストは固定であり、管理対象とならない）
FIA_UID.2(a)	利用者識別情報の管理	審査者、決裁者、旅券作成検査担当者、交付担当者、業務管理者のユーザ ID
FIA_UID.2(b)	利用者識別情報の管理	なし（監視者のユーザ ID は固定であり、管理対象とならない）
FIA_USB.1	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる	役割情報（業務管理者、決裁者、審査者、旅券作成検査担当者、交付担当者）
FMT_MOF.1	TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること	なし（役割は固定であり、管理対象とならない）
FMT_MSA.2(a)	－	－
FMT_MSA.2(b)	－	－
FMT_MSA.2(c)	－	－
FMT_MTD.1(a)	TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし（役割は固定であり、管理対象とならない）
FMT_MTD.1(b)	TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし（役割は固定であり、管理対象とならない）

セキュリティ機能要件	管理の要件（参考情報）	実際の管理項目
FMT_MTD.1(c)	TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし（役割は固定であり、管理対象とならない）
FMT_MTD.1(d)	TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし（役割は固定であり、管理対象とならない）
FMT_MTD.1(e)	TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし（役割は固定であり、管理対象とならない）
FMT_MTD.1(f)	TSF データと相互に影響を及ぼし得る役割のグループを管理すること	なし（役割は固定であり、管理対象とならない）
FMT_SMF.1	－	－
FMT_SMR.1(a)	役割の一部をなす利用者のグループの管理	役割情報（審査者、決裁者、旅券作成検査担当者、交付担当者、業務管理者）
FMT_SMR.1(b)	役割の一部をなす利用者のグループの管理	なし（旅券事務所システム管理者、監視者は固定であり、管理対象とならない）
FPT_RVM.1	－	－
FPT_SEP.1	－	－
FPT_STM.1	時間の管理	システム内時刻
FTA_SSL.3	個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定	なし（個々の利用者毎の設定はなく、時間は固定であるため、管理対象とならない）
	対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定	なし（時間は固定であり、管理対象とならない）
FTP_ITC.1	もしサポートされていれば、高信頼チャネルを要求するアクションの設定	なし（サポートしていないため、管理対象とならない）

セキュリティ機能要件	管理の要件（参考情報）	実際の管理項目
FTP_TRP.1	もしサポートされていれば、高信頼パスを要求するアクションの設定	なし（サポートしていないため、管理対象とならない）

依存性：なし

FMT_SMR.1(a)　セキュリティ役割

下位階層：なし

FMT_SMR.1.1(a)

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*]
業務管理者

詳細化：TSF→業務アプリケーションの TSF

FMT_SMR.1.2(a)

TSF は、利用者を役割に関連づけなければならない。

詳細化：TSF→業務アプリケーションの TSF

依存性：FIA_UID.1 識別のタイミング

FMT_SMR.1(b)　セキュリティ役割

下位階層：なし

FMT_SMR.1.1(b)

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*]
旅券事務所システム管理者
監視者

詳細化：TSF→インフラの TSF

FMT_SMR.1.2(b)

TSF は、利用者を役割に関連づけなければならない。

詳細化：TSF→インフラの TSF

依存性：FIA_UID.1 識別のタイミング

FPT_RVM.1　　TSP の非バイパス性

下位階層：なし

FPT_RVM.1.1

TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性：なし

FPT_SEP.1　　TSF ドメイン分離

下位階層：なし

FPT_SEP.1.1

TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2

TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性：なし

FPT_STM.1　　高信頼タイムスタンプ

下位階層：なし

FPT_STM.1.1

TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性：なし

FTA_SSL.3　　TSF 起動による終了

下位階層：なし

FTA_SSL.3.1

TSF は、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。

[割付: *利用者が非アクティブである時間間隔*]
10 分間

依存性：なし

FTP_ITC.1　　TSF 間高信頼チャネル

下位階層：なし

FTP_ITC.1.1

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

FTP_ITC.1.2

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

[選択: *TSF、リモート高信頼 IT 製品*]
TSF

FTP_ITC.1.3

TSF は、[割付: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。

[割付: *高信頼チャネルが要求される機能のリスト*]
申請データ取得機能
状態通知機能
公文書データ通知機能

依存性：なし

FTP_TRP.1　　高信頼パス

下位階層：なし

FTP_TRP.1.1

TSF は、それ自身と[選択：*リモート*、*ローカル*]利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスを提供しなければならない。

[選択：*リモート*、*ローカル*]
リモート

FTP_TRP.1.2

TSF は、[選択：*TSF*、*ローカル利用者*、*リモート利用者*]が、高信頼パスを介して通信を開始することを許可しなければならない。

[選択：*TSF*、*ローカル利用者*、*リモート利用者*]
リモート利用者

FTP_TRP.1.3

TSF は、[選択：*最初の利用者認証*、[割付：*高信頼パスが要求される他のサービス*]]に対して、高信頼パスの使用を要求しなければならない。

[選択：*最初の利用者認証*、[割付：*高信頼パスが要求される他のサービス*]]
最初の利用者認証

依存性：なし

5.1.2. TOE セキュリティ保証要件

本 ST にて要求する、TOE に対する保証レベルは EAL2 追加である。保証コンポーネント構成を表 5.5 に示す。

表 5.5 の[EAL2]欄のチェック「○」は、EAL2 の保証コンポーネントであることを示す。また、[追加要件]欄のチェック「●」は、EAL2 の保証に追加した保証コンポーネントであることを示す。要求する各保証コンポーネントの保証エレメントは、CC Part3 の要求通りである。

表 5.5 TOE の保証要件コンポーネント一覧

TOE セキュリティ保証要件		コンポーネント	EAL2	追加要件
構成管理	CM 能力	ACM_CAP.2	○	
配付と運用	配付	ADO_DEL.1	○	
	設置、生成、及び立上げ	ADO_IGS.1	○	
開発	機能仕様	ADV_FSP.1	○	
	上位レベル設計	ADV_HLD.1	○	
	表現対応	ADV_RCR.1	○	
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	○	
	利用者ガイダンス	AGD_USR.1	○	
テスト	カバレージ	ATE_COV.1	○	
	機能テスト	ATE_FUN.1	○	
	独立テスト	ATE_IND.2	○	
脆弱性評定	誤使用	AVA_MSU.1		●
	TOE セキュリティ機能強度	AVA_SOF.1	○	
	脆弱性分析	AVA_VLA.1	○	

5.2. IT 環境に対するセキュリティ要件

本 TOE が必要とする IT 環境に対するセキュリティ要件はない。

5.3. 最小機能強度主張

TOE セキュリティ機能要件に対する最小機能強度は、SOF-基本であり、確率的または順列的メカニズムを適用する TOE セキュリティ機能要件は FIA_SOS.1 である。なお、採用する暗号アルゴリズムは、TOE セキュリティ機能強度の対象外である。

6. TOE 要約仕様

6.1. TOE セキュリティ機能

6.1.1. 業務利用制御機能（F.APLACTL）

【セキュリティ機能の概要】

業務利用制御機能は、旅券事務担当職員の正当性を確認するための識別認証、役割に基づいたアクセス制御を実施する機能である。

【セキュリティ機能の仕様】

業務利用制御機能は、業務アプリケーションを利用する際に、ユーザ ID 及びパスワードの入力を促す画面を必ず表示し、その画面を迂回させないようにしている。そのため、業務アプリケーションを利用するには、必ず識別認証が行われることになる。なお、識別認証前における操作で、ユーザ ID、パスワードの入力以外に許可されている操作はない。

業務利用制御機能は、旅券事務担当職員によって入力されたユーザ ID 及びパスワードと予め「旅券事務担当職員管理機能」にて登録されているユーザ ID 及びパスワードを照合し、本人の正当性を確認する。また、パスワード入力の際は、入力された文字数分“*”表示を行う。パスワードに関する規則は、表 6.1 に示す通りである。

表 6.1 パスワード規則

パスワード長	6 バイト～12 バイト
使用可能文字	数字（0～9） 英文字（a～z、A～Z） 記号（# $ ’ ( ) * + , - . / : = ? @ [¥] _ ` { } ~ !）

本人の正当性が確認されると、業務アプリケーションにログインすることになる。業務利用制御機能は、ログイン時に、各旅券事務担当職員を代行するプロセスを割り当てる。プロセスは、旅券事務担当職員毎に割り当てられ、分離されている。そのため、他プロセスからの干渉及び改ざんから保護される。

業務利用制御機能は、「旅券事務担当職員管理機能」にて設定された役割情報をプロセスに関連付ける。プロセスに関連付けられた役割情報は、ログアウトされるまで、その情報が維持される。

また、業務利用制御機能は、旅券事務担当職員アクセス制御方針を実施する。旅券事務担当職員アクセス制御方針は、プロセスに関連付けられた役割情報、アクセス資源を識別するための資源情報、操作内容を識別するための操作情報に基づき、表 6.2 の規則に従ったアクセスを許可し、それ以外のアクセスは拒否する。

表 6.2 旅券事務担当職員アクセス制御方針

役割	アクセス制御内容
業務管理者	－申請書構成管理情報の申請者署名検証 －申請者証明書有効性確認 －同意書の法定代理人署名検証(※) －法定代理人証明書有効性確認(※) －申請書構成管理情報、申請書、写真、自署、同意書(※)の登録 －申請書構成管理情報、申請書、写真、自署、同意書(※)の削除 －申請書、写真、自署、同意書(※)の閲覧 －審査情報、官公庁記載欄情報、審査状態情報の閲覧 －審査情報、官公庁記載欄情報の入力 －審査状態情報へ書類確認結果の登録 －審査状態情報へ審査結果の登録 －審査状態情報へ決裁結果の登録 －審査状態情報へ旅券検査結果の登録 －審査状態情報へ交付結果の登録 －申請取得完了通知の状態通知情報生成 －書類確認完了通知の状態通知情報生成 －審査完了通知の状態通知情報生成 －決裁完了通知の状態通知情報生成 －公文書構成管理情報へ職責署名付与 －公文書構成管理情報、公文書の生成 －公文書の閲覧 －担当者情報、事務所情報の登録 －担当者情報、事務所情報の変更 －担当者情報の削除 ※：申請者から電子送付された場合に限る。

役割	アクセス制御内容
決裁者	－申請書構成管理情報の申請者署名検証 －申請者証明書有効性確認 －同意書の法定代理人署名検証(※) －法定代理人証明書有効性確認(※) －申請書構成管理情報、申請書、写真、自署、同意書(※)の登録 －申請書、写真、自署、同意書(※)の閲覧 －審査情報、官公庁記載欄情報、審査状態情報の閲覧 －審査情報、官公庁記載欄情報の入力 －審査状態情報へ書類確認結果の登録 －審査状態情報へ審査結果の登録 －審査状態情報へ決裁結果の登録 －審査状態情報へ旅券検査結果の登録 －審査状態情報へ交付結果の登録 －申請取得完了通知の状態通知情報生成 －書類確認完了通知の状態通知情報生成 －審査完了通知の状態通知情報生成 －決裁完了通知の状態通知情報生成 －公文書構成管理情報へ職責署名付与 －公文書構成管理情報、公文書の生成 －公文書の閲覧 ※：申請者から電子送付された場合に限る。

役割	アクセス制御内容
審査者	－申請書構成管理情報の申請者署名検証 －申請者証明書有効性確認 －同意書の法定代理人署名検証(※) －法定代理人証明書有効性確認(※) －申請書構成管理情報、申請書、写真、自署、同意書(※)の登録 －申請書、写真、自署、同意書(※)の閲覧 －審査情報、官公庁記載欄情報、審査状態情報の閲覧 －審査情報、官公庁記載欄情報の入力 －審査状態情報へ書類確認結果の登録 －審査状態情報へ審査結果の登録 －審査状態情報へ旅券検査結果の登録 －審査状態情報へ交付結果の登録 －申請取得完了通知の状態通知情報生成 －書類確認完了通知の状態通知情報生成 －審査完了通知の状態通知情報生成 －公文書の閲覧 ※：申請者から電子送付された場合に限る。
旅券作成検査担当者	－申請書、写真、自署、同意書(※)の閲覧 －審査情報、官公庁記載欄情報、審査状態情報の閲覧 －官公庁記載欄情報の入力 －審査状態情報へ旅券検査結果の登録 －公文書の閲覧 ※：申請者から電子送付された場合に限る。
交付担当者	－申請書、写真、自署、同意書(※)の閲覧 －審査情報、官公庁記載欄情報、審査状態情報の閲覧 －官公庁記載欄情報の入力 －審査状態情報へ交付結果の登録 －公文書の閲覧 ※：申請者から電子送付された場合に限る。

【TOE セキュリティ機能要件】

FIA_ATD.1、FIA_SOS.1、FIA_UAU.2(a)、FIA_UAU.7、FIA_UID.2(a)、FIA_USB.1、FDP_ACC.1、FDP_ACF.1、FPT_RVM.1、FPT_SEP.1

6.1.2. セション管理機能（F.SESMAN）

【セキュリティ機能の概要】

セション管理機能は、TOE と審査者端末間で確立されるセションを管理する機能である。

【セキュリティ機能の仕様】

旅券事務担当職員が審査者端末を介して TOE にアクセスした場合、TOE と審査者端末間にセションが確立される。

セション管理機能は、確立されたセションの状態を管理し、旅券事務担当職員との対話で無応答時間が１０分間に達した場合、旅券事務担当職員とのセションを強制的に切断する。なお、１０分間という時間設定は変更不可である。

セションは、その特性上、旅券事務担当職員がログアウト操作を実施しなかった場合、１０分間のタイムアウトによるセション切断まで、セションが切断されず残存してしまい、セキュリティ上好ましくない状態となる。そのため、セション管理機能は、業務管理者に対して、以下の管理操作を提供する。

－ログインユーザ一覧表示

TOE にログインしている旅券事務担当職員の一覧を表示する。ログインユーザ一覧を表示させることによって、TOE にアクセスしている旅券事務担当職員を確認することができ、セション状況の管理が可能である。セション状況の確認により、TOE を利用していない旅券事務担当職員のセションが検出された場合、下記、手動によるセション切断機能により、セションの切断が可能である。

－手動によるセション切断

「ログインユーザ一覧」から該当する旅券事務担当職員のセションを手動で切断する。手動によるセション切断によって、１０分間のタイムアウトを待たずにセションを切断でき、セションを残存させないことが可能である。

【TOE セキュリティ機能要件】

FTA_SSL.3、FMT_MOF.1

6.1.3. 旅券事務担当職員管理機能 (F.USEMAN)

【セキュリティ機能の概要】

旅券事務担当職員管理機能は、業務アプリケーションへのアクセスを管理にするために、旅券事務担当職員の登録、変更、削除を実施する機能である。

【セキュリティ機能の仕様】

TOE へアクセスするには、事前にアクセスを行う人物を登録する必要がある。また、様々な事象により、登録した人物の削除や変更を行う必要が生じる可能性がある。そのため、旅券事務担当職員管理機能では、業務管理者に対して、旅券事務担当職員の登録、変更、削除を行う管理操作を提供する。

旅券事務担当職員管理機能では、識別認証及びアクセス制御で必要となる以下の情報を管理対象としている。

・ユーザ ID

「業務利用制御機能」にて、旅券事務担当職員を識別する際に使用する識別情報である。

・パスワード

「業務利用制御機能」にて、旅券事務担当職員を認証する際に使用する認証情報である。

・役割情報

「業務利用制御機能」にて、アクセス制御を実施する際に使用する権限情報である。

旅券事務担当職員管理機能は、業務管理者によって設定されたユーザ ID、パスワード、役割情報を格納し、その状態を維持する。

旅券事務担当職員管理機能が提供する各管理操作を、以下で説明する。

－旅券事務担当職員の登録

旅券事務担当職員の登録では、ユーザ ID、パスワード、役割情報を設定することが可能である。なお、システム運用開始時は、TOE 導入時に予め登録されている業務管理者によって行われる。

－旅券事務担当職員の変更

旅券事務担当職員の変更では、パスワード、役割情報の設定を変更することが可能である。なお、業務管理者の役割情報を変更することはできない。

－旅券事務担当職員の削除

旅券事務担当職員の削除では、削除対象である旅券事務担当職員に関する全ての情報を削除する。なお、本操作を行っている業務管理者自身を削除することはできない。

【TOE セキュリティ機能要件】

FMT_MTD.1(a)、FMT_MTD.1(b)、FMT_SMF.1、FMT_SMR.1(a)

6.1.4. 暗号化通信機能（F.CRYCOM）

【セキュリティ機能の概要】

暗号化通信機能は、汎用受付システムと TOE 間、審査者端末と TOE 間の通信データを盗聴及び改ざんから保護する機能である。

【セキュリティ機能の仕様】

TOE は、ネットワークを介して汎用受付システムまたは審査者端末と通信データの送受信を行う。そのため、暗号化通信機能は、SSL を利用し、ネットワークを介して送受信される通信データを盗聴及び改ざんから保護する。

汎用受付システムと TOE 間、審査者端末と TOE 間の各ケースにおける、SSL 通信の確立及び維持に関して以下で説明する。

－審査者端末と TOE 間のケース

旅券事務担当職員は、審査者端末の Web ブラウザを利用して TOE にアクセスを行う。Web ブラウザと TOE 間は、SSL を実現するプロトコルである HTTPS を用いて接続される。TOE は、Web ブラウザを利用している旅券事務担当職員の接続要求を受け、SSL に従ったハンドシェイクを開始し、共通鍵を交換する。Web ブラウザと TOE は、SSL によるハンドシェイクが完了した後、HTTPS 通信を確立する。SSL ハンドシェイクの完了時には、終了メッセージによりセションが成功したことを確認するため、安全に HTTPS 通信を行うことができる。また、HTTPS 通信は、ユーザ ID 及びパスワードを入力する画面から TOE との接続を切断するまで適用される。すなわち、ログイン要求からログアウトまで HTTPS 通信が維持されることになる。TOE は、SSL プロトコルに従い、HTTPS 通信の完了もしくはエラーの発生を契機に共通鍵を廃棄する。

－汎用受付システムと TOE 間のケース

汎用受付システムと TOE 間も、「審査者端末と TOE 間のケース」と同様に、HTTPS を用いて接続を行う。TOE は、汎用受付システムに対して接続要求を行い、SSL に従ったハンドシェイクを開始し、表 6.4 にて（※）印で識別された暗号鍵生成ア

ルゴリズムによって共通鍵を生成する。汎用受付システムと TOE は、SSL プロトコルによるハンドシェイクが完了した後、HTTPS 通信を確立する。SSL ハンドシェイクの完了時には、終了メッセージによりセションが成功したことを確認するため、安全に HTTPS 通信を行うことができる。また、HTTPS 通信は、以下の機能によって接続要求が行われ、通信確立後に送受信される通信データは保護されることになる。

・申請データ取得機能
・状態通知機能
・公文書データ通知機能

TOE は、SSL プロトコルに従い、HTTPS 通信の完了もしくはエラーの発生を契機に共通鍵を廃棄する。

暗号化通信機能で採用している SSL は、表 6.3 及び表 6.4 に示すセキュリティメカニズムが利用できる。

表 6.3 審査者端末と TOE 間の SSL 通信で使用するセキュリティメカニズム

暗号アルゴリズム	鍵長	仕様
DES	56bit	FIPS PUB 46-3,Data Encryption Standard
3DES	168bit	FIPS PUB 46-3,Data Encryption Standard
RC4	128bit	仕様は公開されていない。ただし、ISO/IEC9979 に登録されている国際標準
RSA	1024bit	PKCS#1,RSA Cryptography Standard
MD5	－	RFC1321,Message-Digest Algorithm
SHA-1	－	FIPS PUB 180-2,Secure Hash Standard

表 6.4 汎用受付システムと TOE 間の SSL 通信で使用するセキュリティメカニズム

暗号アルゴリズム	鍵長	仕様
DES（※）	56bit	FIPS PUB 46-3,Data Encryption Standard
3DES（※）	168bit	FIPS PUB 46-3,Data Encryption Standard
RC4（※）	128bit	仕様は公開されていない。ただし、ISO/IEC9979 に登録されている国際標準
RSA（※）	1024bit	PKCS#1,RSA Cryptography Standard
MD5	－	RFC1321,Message-Digest Algorithm
SHA-1	－	FIPS PUB 180-2,Secure Hash Standard

（※）は暗号鍵生成アルゴリズム

【TOE セキュリティ機能要件】

FCS_CKM.1、FCS_CKM.4(a)、FCS_CKM.4(b)、FCS_COP.1(b)、FCS_COP.1(c)、FMT_MSA.2(b)、FMT_MSA.2(c)、FTP_TRP.1、FTP_ITC.1

6.1.5. 申請データ検証機能（F.SIGVER）

【セキュリティ機能の概要】

申請データ検証機能は、申請者証明書を用いて申請者署名を検証する機能である。また、同意書が含まれている場合は、法定代理人証明書を用いて法定代理人署名も検証する。

申請者証明書が有効である場合、申請データは正当な申請者より送られたことが確認できる。また、申請者署名が検証できた場合、申請データが改変されていないことが確認できる。

【セキュリティ機能の仕様】

申請データ検証機能では、以下に示す仕組みで、申請者署名を検証している。

1. 申請者証明書に含まれている申請者の公開鍵または法定代理人の公開鍵で、申請者署名を復号し、ハッシュ値を求める。
2. 申請書署名情報から、ハッシュ値を生成する。
3. 申請者署名から復号されたハッシュ値と申請書署名情報から生成したハッシュ値を比較し、申請者署名を検証する。これにより、申請データに改変が生じたかどうかを判定することができる。

また、申請データ検証機能では、以下に示す仕組みで法定代理人署名を検証している。

1. 法定代理人証明書に含まれている法定代理人の公開鍵で、法定代理人署名を復号し、ハッシュ値を求める。
2. 同意書署名情報から、ハッシュ値を生成する。
3. 法定代理人署名から復号されたハッシュ値と同意書署名情報から生成したハッシュ値を比較し、法定代理人署名を検証する。これにより、申請データに改変が生じたかどうかを判定することができる。

申請データ検証機能は、表 6.5 に示すセキュリティメカニズムを使用している。

表 6.5 申請データ検証機能で使用するセキュリティメカニズム

暗号アルゴリズム	鍵長	仕様
RSA	1024bit	PKCS#1,RSA Cryptography Standard
	2048bit	
SHA-1	－	FIPS PUB 180-2,Secure Hash Standard

なお、申請データ検証機能は、申請者証明書及び法定代理人証明書の有効性を確認する機能も有している。

申請者証明書及び法定代理人証明書の有効性の確認は以下によって行われる。

- 電子証明書に登録された有効期間（開始と終了）と現在時刻を比較して、有効期間内であるかどうかを確認する
- JPKI が確認した失効ステータス結果より、電子証明書が失効しているかどうかを確認する

電子証明書が有効期間内であり、かつ、失効していないことが確認された場合、有効な電子証明書であると判断する。

【TOE セキュリティ機能要件】

FCS_COP.1(a)、FDP_UIT.1、FMT_MSA.2(a)

6.1.6. 監査機能（F.AUDIT）

【セキュリティ機能の概要】

監査機能は、業務アプリケーション機能及びインフラ機能の操作内容を監査ログに記録し、記録された情報からセキュリティ侵害の可能性をリアルタイムで分析する機能である。また、記録された監査事象及び監査ログ格納領域の管理も行う。

【セキュリティ機能の仕様】

監査機能は、脅威の早期検出、TOE に対する操作を分析するために、業務アプリケーション機能及びインフラ機能の操作に関して、表 6.6 に示す監査事象を監査ログに記録する。また、監査ログの性質上、正確な日付・時刻が必要であるため、信頼できる時間を提供する。

表 6.6 監査ログに記録する内容

記録する情報	説明
日付／時刻	事象が発生した日付及び時刻を記録する。
事象の重要度	各事象において、以下に示すいずれかの重要度を記録する。 ・ emerg：システムの緊急事態 ・ alert：すぐに修正が必要なエラー ・ crit：致命的なエラー ・ err：その他のエラー ・ exception：アプリケーション例外 ・ TNS-：データベースのコネクションエラー ・ ORA-：その他のデータベースエラー ・ warning：警告メッセージ ・ notice：エラーではないが、処置を必要とする状態 ・ info：情報メッセージ
事象の発生元	事象を発生させたユーザ ID、IP アドレスまたはその両方を記録する。
事象の内容	以下に示す事象の種別及び結果を記録する。 ・ 監査ログ生成デーモンの起動事象 ・ 監査ログ生成デーモンの停止事象 ・ 監査ログ監視エージェントの起動事象 ・ 監査ログ監視エージェントの停止事象 ・ 監視端末へのアラート通知事象 ・ 監査ログ格納領域の閾値越え事象 ・ 審査者端末と TOE 間の通信確立における失敗事象 ・ 審査者端末と TOE 間の SSL 通信における成功事象または失敗事象 ・ 汎用受付システムと TOE 間の通信確立における失敗事象 ・ 汎用受付システムと TOE 間の SSL 通信における成功事象または失敗事象 ・ 旅券事務担当職員の識別認証における成功事象または失敗事象 ・ 旅券事務担当職員の役割情報取得における失敗事象 ・ 業務アプリケーションのパスワード規則における不適合事象 ・ 申請データの取得における成功事象または失敗事象 ・ 公文書データの登録における成功事象または失敗事象 ・ 状態通知情報の通知における成功事象または失敗事象 ・ 申請者署名の検証における成功事象または失敗事象 ・ 申請者証明書の有効性確認における成功事象または失敗事象

記録する情報	説明
	・ 法定代理人署名の検証における成功事象または失敗事象 ・ 法定代理人証明書の有効性確認における成功事象または失敗事象 ・ 申請書、写真、自署、同意書(※)の閲覧における成功事象または失敗事象 ・ 申請データの登録における成功事象または失敗事象 ・ 申請データの削除における成功事象または失敗事象 ・ 審査情報、官公庁記載欄情報、審査状態情報の閲覧における成功事象または失敗事象 ・ 審査情報、官公庁記載欄情報の入力における成功事象または失敗事象 ・ 書類確認結果、決裁結果、審査結果、旅券検査結果、交付結果の登録における成功事象または失敗事象 ・ 申請取得完了通知、書類確認完了通知、審査完了通知、決裁完了通知の生成における成功事象または失敗事象 ・ 職責署名の付与における成功事象または失敗事象 ・ 公文書データの生成における成功事象または失敗事象 ・ 公文書の閲覧における成功事象または失敗事象 ・ 担当者情報、事務所情報の登録における成功事象または失敗事象 ・ 担当者情報、事務所情報の変更における成功事象または失敗事象 ・ 担当者情報の削除における成功事象または失敗事象 ・ タイムアウトによるセション切断事象 ・ 業務管理者による手動セション切断事象 ・ ログインユーザの一覧表示事象 ・ 旅券事務担当職員の登録事象 ・ 旅券事務担当職員の削除事象 ・ 旅券事務担当職員のパスワード変更事象 ・ 決裁者、審査者、旅券作成検査担当者、交付担当者の役割情報変更事象 ・ 旅券事務所システム管理者及び監視者の識別認証における失敗事象 ・ 申請者証明書もしくは法定代理人証明書の有効期間確認における有効期間外事象 ・ 旅券事務所システム管理者及び監視者のパスワード変更事象 ・ システム内時刻の問い合わせ事象及び変更事象 ・ シグネチャの問い合わせ事象及び変更事象

記録する情報	説明
	※：申請者から電子送付された場合に限る。

監査機能は、記録された監査ログをリアルタイムで分析する。分析時に、セキュリティ侵害の可能性を検知した場合、監査機能は、監視端末にアラートを通知する。セキュリティ侵害の可能性検知では、シグネチャが用いられる。シグネチャは、セキュリティ侵害の可能性を判断する基準であり、表 6.7 に示された重要度の中から選択することができる。シグネチャは、監査ログに記録される表 6.6 の中で、シグネチャに示された重要度と合致した重要度を含む事象が発生した場合、その事象をセキュリティ侵害の可能性があると判断する。

表 6.7 シグネチャとして選択可能な重要度

事象の重要度
・ emerg：システムの緊急事態
・ alert：すぐに修正が必要なエラー
・ crit：致命的なエラー
・ err：その他のエラー
・ exception：アプリケーション例外
・ TNS-：データベースのコネクションエラー
・ ORA-：その他のデータベースエラー
・ warning：警告メッセージ

リアルタイムで分析される監査事象は、緊急性を要する事象に限定される。そこで、監査機能は、詳細な監査ログ分析を行うために、記録された監査事象の表示を提供する。また、監査事象の表示は、旅券事務所システム管理者及び監視者のみが実施できるように制御する。

監査機能は、監査事象の表示制御だけではなく、記録された監査事象の不正な削除及び改変を防止するため、監査ログ格納領域の保護も行う。

監査機能は、監査ログ格納領域を枯渇させないために、閾値を設ける。閾値は、監査ログ格納領域の 80%としており、固定値である。監査機能は、閾値を超えた場合、その旨を監査ログに記録し、監視端末にアラート通知を行う。

【TOE セキュリティ機能要件】

FAU_ARP.1、FAU_GEN.1、FAU_SAA.1、FAU_SAR.1、FAU_STG.1、FAU_STG.3、FPT_STM.1

6.1.7. インフラ利用管理機能（F.INFMAN）

【セキュリティ機能の概要】

インフラ利用管理機能は、インフラを利用する旅券事務所システム管理者／監視者の正当性を確認するために識別認証を行い、旅券事務所システム管理者／監視者のパスワード、セキュリティ侵害の可能性を示すシグネチャ、システム内時刻の管理を実施する機能である。

【セキュリティ機能の仕様】

インフラ利用管理機能は、インフラを利用する際に、ユーザ ID 及びパスワードの入力を促す画面を必ず表示し、その画面を迂回させないようにしている。そのため、インフラを利用するには、必ず識別認証が行われることになる。なお、識別認証前に操作できる内容は、役割によって異なっており、以下にその内容を示す。

・旅券事務所システム管理者

ユーザ ID、パスワード入力の他に、「言語の選択」、「GUI でのログイン、コマンドラインからのログインの選択」、「ログインサーバの選択」、「ヘルプの参照」が許可されている。

・監視者

ユーザ ID、パスワード入力の以外に、許可されている操作はない。

インフラ利用管理機能は、旅券事務所システム管理者または監視者によって入力されたユーザ ID 及びパスワードと予め登録されているユーザ ID 及びパスワードを照合し、本人の正当性を確認する。なお、ユーザ ID 及びユーザ ID に関連付ける役割情報は、TOE 導入時に登録されており、それらの値は固定値として維持されている。

本人の正当性が確認されると、インフラにログインすることになる。インフラ利用管理機能は、ログイン時に、旅券事務所システム管理者または監視者を代行するプロセスを割り当てる。プロセスは、旅券事務所システム管理者または監視者に割り当てられ、独立している。そのため、他プロセスからの干渉及び改ざんから保護される。

インフラ利用管理機能は、TOE 導入時に登録されている役割情報をプロセスに関連付ける。プロセスに関連付けられた役割情報は、ログアウトされるまで、その情報が維持される。

インフラ利用管理機能は、旅券事務所システム管理者／監視者のパスワード、セキュリティ侵害の可能性を示すシグネチャ、システム内時刻の管理を行うために、旅券事務所システム管理者／監視者に対して、以下の管理操作を提供する。

－パスワード管理

パスワードを危殆化させないため、旅券事務所システム管理者または監視者は、自身のパスワードを変更することが可能である。なお、旅券事務所システム管理者は、監視者のパスワードも変更することが可能である。

－シグネチャ管理

監査ログを柔軟に監視するため、旅券事務所システム管理者または監視者は、シグネチャの問い合わせまたは変更を行うことが可能である。

－システム内時刻管理

不測の事態発生に備え、旅券事務所システム管理者は、システム内時刻の問い合わせまたは変更を行うことが可能である。

【TOE セキュリティ機能要件】

FIA_UAU.1、FIA_UAU.2(b)、FIA_UID.1、FIA_UID.2(b)、FMT_MTD.1(c)、FMT_MTD.1(d)、FMT_MTD.1(e)、FMT_MTD.1(f)、FMT_SMF.1、FMT_SMR.1(b)、FPT_RVM.1、FPT_SEP.1

6.2. セキュリティ機能強度

TOE セキュリティ機能要件に対する最小機能強度は、SOF-基本である。セキュリティ機能強度の対象となる機能は、業務利用制御機能であり、セキュリティ機能強度は SOF-基本である。

6.3. 保証手段

TOE セキュリティ保証要件のコンポーネントに対応するエビデンスを表 6.8 に示す。

表 6.8 TOE の保証要件とエビデンス

TOE セキュリティ保証要件		コンポーネント	エビデンス
構成管理	CM 能力	ACM_CAP.2	構成管理仕様書
配付と運用	配付	ADO_DEL.1	配付手順書
	設置、生成、及び立上げ	ADO_IGS.1	運用環境移行手順書
開発	機能仕様	ADV_FSP.1	基本設計書
	上位レベル設計	ADV_HLD.1	詳細設計書
	表現対応	ADV_RCR.1	基本設計書
			詳細設計書
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	システム基本仕様書
			データセンタ内環境設定書
	利用者ガイダンス	AGD_USR.1	審査手引書
			審査者端末マニュアル
テスト	カバレージ	ATE_COV.1	テスト仕様書
	機能テスト	ATE_FUN.1	テスト仕様書
	独立テスト	ATE_IND.2	テスト仕様書
脆弱性評定	誤使用	AVA_MSU.1	システム基本仕様書
			データセンタ内環境設定書
			審査手引書
			審査者端末マニュアル
	TOE セキュリティ機能強度	AVA_SOF.1	脆弱性分析書
	脆弱性分析	AVA_VLA.1	脆弱性分析書

7. PP 主張

本 ST が適合する PP は存在しない。

8. 根拠

8.1. セキュリティ対策方針根拠

TOE セキュリティ環境に対するセキュリティ対策方針の対応を表 8.1 に示す。

表 8.1 前提条件、脅威、組織のセキュリティ方針とセキュリティ対策方針の対応

TOE セキュリティ環境 / セキュリティ対策方針	A. TRUST_ROLE	A. SECRECY	A. MAINTAIN	A. PHYSICAL_ACCESS	A. SUPPORT_CENTER	A. CONNECT_NETWORK	A. TRUST_PKI	A. TRUST_CRYPT	A. IC_CARD	T. TAP	T. EXCEED_ACCESS	T. ID_SPOOF	T. MISTAKE	T. FAKE_APPLICATION	T. ABUSE	T. FAKE_PHOTO&SIGN	P. OFFICIAL_DOCUMENT	P. INFRA
O.CRYPT_MESSAGE										○								
O.ID_AUTH												○						
O.ACCESS_CONTROL											○			○	○			
O.VERIFICATION														○				
O.AUDIT											○	○		○	○			
O.APP_ADMIN											○	○		○	○			
O.INFRA_ADMIN																		○
O.INFRA_I&A																		○
OE.TRUST_ROLE	○																	
OE.SECRECY		○																
OE.MAINTAIN			○															
OE.PHYSICAL_ACCESS				○														
OE.SUPPORT_CENTER					○													
OE.CONNECT_NETWORK						○												
OE.TRUST_PKI							○											
OE.TRUST_CRYPT								○										
OE.DATA_PROTECT													○					
OE.OFFICIAL_DOCUMENT																	○	
OE.VERIFICATION														○				
OE.TRUST_EXAMINATION															○			
OE.FAKE_PHOTO&SIGN																○		

OE.IC_CARD									○								
OE.ROLE_ASSIGN														○			

以下に、『4.1.TOE のセキュリティ対策方針』及び『4.2.環境のセキュリティ対策方針』で識別したセキュリティ対策方針が必要かつ十分であることの根拠を示す。

表 8.1 により、すべてのセキュリティ対策方針は１つ以上の前提条件、脅威もしくは組織のセキュリティ方針に対応しているため、識別されたセキュリティ対策方針は必要である。

8.1.1. 前提条件に対するセキュリティ対策方針の適合性

・ A.TRUST_ROLE

OE.TRUST_ROLE により、システム責任者の権限において適切であると判断される人物が旅券事務所システム管理者、業務管理者、決裁者及び監視者として任命される。加えて、任命した人物に対してセキュリティ教育及び啓蒙を実施し、システム運用管理に関する規則を遵守することに同意させる。

これにより、旅券事務所システム管理者、業務管理者、決裁者及び監視者は信用できる人物であり、不正行為は行わないとした前提条件を実現することができる。

・ A.SECRECY

OE.SECRECY により、システム責任者は、審査者、旅券作成検査担当者及び交付担当者に対して、情報セキュリティ教育及び啓蒙を実施する。情報セキュリティ教育及び啓蒙によって、地方公務員法を遵守し、業務上必要な情報や知り得た情報の扱いにおいて不正は行わないことに同意させる。なお、業務アプリケーションは一度に複数の申請データの内容を画面表示することができないため、多くの情報を収集するまでに時間と労力を要する。そのため、申請データを始めとする保護対象資産へのアクセス履歴の記録宣言や罰則の実施による抑止力は、不正の動機に対し、十分な効果を有するものと考える。

これにより、審査者、旅券作成検査担当者及び交付担当者は、パスワード及び審査者端末に表示される保護対象資産の情報を他人に漏らすことはないとした前提条件を実現することができる。

・ A.MAINTAIN

OE.MAINTAIN により、旅券事務所システム管理者は、保守担当者が正しく保守作業を行うことを監視する。

これにより、保守担当者による作業は、旅券事務所システム管理者の監視のもと実施され、不正な操作は行われないとした前提条件を実現することができる。

・ A.PHYSICAL_ACCESS

OE.PHYSICAL_ACCESS により、旅券事務所システム管理者は、自身以外の物理的アクセスを禁止できる施錠可能なラック内に TOE を設置し、保護対象資産の複製物も施錠管理された場所で保管する。更に、審査者端末が設置される部屋を施錠管理により TOE に関係する人物以外の入室を禁止する。

これにより、TOE が設置される筐体及び保護対象資産の複製物は、旅券事務所システム管理者以外の物理的アクセスが禁止されており、審査者端末が設置される部屋は、TOE に関係する人物以外の入室が禁止されているとした前提条件を実現することができる。

・ A.SUPPORT_CENTER

OE.SUPPORT_CENTER により、監視端末が設置される部屋への入室管理として、バイオ認証システムを利用して監視者の本人確認を行い、本人であることを確認できなかった場合には入室を禁止する。

これにより、監視端末が設置される部屋は、監視者以外の入室が禁止されているとした前提条件を実現することができる。

・ A.CONNECT_NETWORK

OE.CONNECT_NETWORK により、旅券事務所システム管理者は、庁内ネットワークと TOE が設置されるネットワークの接続点にファイアウォールを設置して、TOE の業務アプリケーションの機能に必要な通信以外の通過を禁止する。また、TOE と運用支援センター間は、IP-VPN によって接続され、改ざん及び盗聴から保護される。

これにより、TOE が設置されるネットワークと庁内ネットワークは、TOE の業務アプリケーションの機能に必要な通信以外の通過を禁止された特定個所で接続され、また、TOE と運用支援センター間は、TOE と運用支援センターのみが通信可能な閉域ネットワークで接続されるとした前提条件を実現することができる。

・ A.TRUST_PKI

OE.TRUST_PKI により、TOE が申請データの検証に利用する電子証明書及び電子証明書の失効ステータスは、地方公共団体によって運営される JPKI によって発行され、電子証明書の失効ステータスは、正当性や完全性が保証された JPKI の手続きに従って TOE に提供される。

これにより、TOE が申請データの検証に利用する申請者証明書もしくは法定代理人証明書及び電子証明書の失効ステータスは信頼できる機関によって発行され、電子証明書の正しい失効ステータスが TOE に提供される、とした前提条件を実現することができる。

・ A.TRUST_CRYPT

OE.TRUST_CRYPT により、TOE が汎用受付システムもしくは審査者端末との暗号化通信に利用する、TOE 及び汎用受付システムの電子証明書、TOE 及び汎用受付システムの秘密鍵、TOE 及び汎用受付システムの電子証明書の失効ステータスは、地方公共団体によって運用される LGPKI 及び外務省 CA によって発行される。また、汎用受付システムの電子証明書の失効ステータスは、正当性や完全性が保証された LGPKI の手続きに従って TOE に提供される。TOE の電子証明書が失効した場合には、外務省 CA より電子証明書が失効した旨が連絡されるため、電子証明書の失効を正しく知ることができる。

これにより、TOE が汎用受付システムもしくは審査者端末との暗号化通信に利用する、TOE 及び汎用受付システムの電子証明書、TOE 及び汎用受付システムの秘密鍵、TOE 及び汎用受付システムの電子証明書の失効ステータスは信頼できる機関によって発行され、電子証明書の正しい失効ステータスが TOE に提供されるとした前提条件を実現できる。

・ A.IC_CARD

OE.IC_CARD により、申請データへの署名は、本人に対して発行された公的個人認証 IC カードを用いて行われる。

これにより、申請データの署名には、正当な IC カードが利用されるとした前提条件を実現できる。

8.1.2. 脅威に対するセキュリティ対策方針の適合性

・ T.TAP

O.CRYPT_MESSAGE により、汎用受付システム及び審査者端末との通信において、SSL 通信による通信データの保護を行うことにより、脅威に対抗する。

これにより、攻撃者による TOE と汎用受付システム間あるいは TOE と審査者端末間の通信データにおける盗聴、改ざんの脅威に対抗できる。

・ T.ID_SPOOF

O.ID_AUTH により、TOE は業務アプリケーションが提供する機能へのアクセス要求を受けた場合に識別認証を行い正当な旅券事務担当職員であることを確認し、業務アプリケーションが提供する機能の利用時に審査者端末から無応答状態が続いた場合に該当セションを切断する。

O.APP_ADMIN により、業務アプリケーションにおける旅券事務担当職員の識別認証及びセション管理の運用管理を業務管理者のみに制限する。業務管理者が旅券事務担当職員に関わる情報を管理することにより、O.ID_AUTH の実施が可能となる。

O.AUDIT により、識別認証に関連するセキュリティ事象を監査記録として採取し、採取した監査記録を管理する。更に、アラート通知を行うことで、脅威の早期検出を行う。O.AUDIT によって、脅威の影響範囲を抑える。

これらにより、旅券事務担当職員以外の地方公共団体旅券事務所職員による TOE の不正利用の脅威に対抗できる。

・ T.EXCEED_ACCESS

O.ACCESS_CONTROL により、TOE は、審査業務をフェーズ毎に分割して役割を定義し、役割を割り当てられた旅券事務担当職員だけに各フェーズに対応する必要最小限の機能を提供する。よって、旅券事務担当職員は担当するフェーズ以外の審査業務を行うことができない。

O.APP_ADMIN により、業務アプリケーションに関して旅券事務担当職員のアクセス制御に関わる運用管理を業務管理者のみに制限する。業務管理者が旅券事務担当職員のアクセス制御に関わる情報を管理することにより、O.ACCESS_CONTROL の実施が可能となる。

O.AUDIT により、アクセス制御に関連するセキュリティ事象を監査記録として採取し、採取した監査記録を管理する。更に、アラート通知を行うことで、脅威の早期検出を行う。O.AUDIT によって、脅威の影響範囲を抑える。

これらにより、担当する審査業務以外の操作による脅威に対抗できる。

・ T.MISTAKE

OE.DATA_PROTECTにより、旅券事務所システム管理者は毎日保護対象資産のバックアップ作業を行い、直前のバックアップ完了状態への復旧を可能にする。

なお、審査業務は複数人による厳密な審査が行われるため、１日で処理が完了することはない。このため、毎日保護対象資産のバックアップを取得することで、資産の消失を最大でも直前バックアップからの１日分の作業内容に留めることができる。

これにより、業務管理者による TOE 機能の誤操作の脅威に対抗できる。

・ T.FAKE_APPLICATION

O.VERIFICATIONにより、TOEは申請者から送られる申請データの完全性を署名検証により確認することで、電子署名の付与後に修正された申請内容を含んだ申請データを検出することができる。

OE.VERIFICATION により、決裁者及び業務管理者が JPKI を利用して、申請者から送られる申請データの正当性を電子証明書検証により確認することで、他人を装って申請された申請データを検出することができる。

O.ACCESS_CONTROL により、TOE は、審査業務をフェーズ毎に分割して役割を定義し、役割を割り当てられた旅券事務担当職員だけに各フェーズに対応する必要最小限の機

能を提供する。これにより、TOE は、複数の審査のフェーズにより実施される審査業務を行うための業務アプリケーション機能及び審査業務を正しく遂行するための審査業務を管理するための業務アプリケーション機能を提供することができるため、旅券事務担当職員は審査業務を確実に実施することができる。よって、偽りを含む申請データを検出することができる。

OE.ROLE_ASSIGN により、システム責任者は、審査業務を各フェーズに区切り、旅券事務担当職員を、各フェーズを担当する役割及び審査業務を管理する役割として割り当てる。役割を割り当てられた旅券事務担当職員は、担当するフェーズ順に審査業務を実施し、申請内容が正しいことを確認し、TOE へ結果を登録する。よって、審査業務は O.ACCESS_CONTROL に従って、各フェーズを担当する役割の責任の下、フェーズ単位で順番に実施されるため、偽りを含む申請データを検出することができる。

O.APP_ADMIN により、業務アプリケーションに関して旅券事務担当職員のアクセス制御に関わる運用管理を業務管理者のみに制限する。業務管理者が旅券事務担当職員のアクセス制御に関わる情報を管理することにより、O.ACCESS_CONTROL の実施が可能となる。

O.AUDIT により、アクセス制御に関連するセキュリティ事象を監査記録として採取し、採取した監査記録を管理する。更に、アラート通知を行うことで、脅威の早期検出を行う。O.AUDIT によって、脅威の影響範囲を抑える。

これらにより、不正な申請データを基にした旅券発給の脅威に対抗できる。

・ T.ABUSE

OE.TRUST_EXAMINATION により、決裁者は、審査者が行った審査内容の正当性を検証する。すなわち、旅券発給には決裁者の決裁が必要であり、審査者の審査のみで発給されることはない。

O.ACCESS_CONTROL により、TOE は、審査業務をフェーズ毎に分割して役割を定義し、役割を割り当てられた旅券事務担当職員だけに各フェーズに対応する必要最小限の機能を提供する。よって、審査者は決裁を行う機能は利用できず、決裁者による決裁が必要となる。

O.APP_ADMIN により、業務アプリケーションに関して旅券事務担当職員のアクセス制御に関わる運用管理を業務管理者のみに制限する。業務管理者が旅券事務担当職員のアクセス制御に関わる情報を管理することにより、O.ACCESS_CONTROL の実施が可能となる。

O.AUDIT により、アクセス制御に関連するセキュリティ事象を監査記録として採取し、採取した監査記録を管理する。更に、アラート通知を行うことで、脅威の早期検出を行う。O.AUDIT によって、脅威の影響範囲を抑える。

これらにより、申請棄却すべき申請データに対し審査者が正しい審査を行わないことにより、不適切な旅券が発給される脅威に対抗できる。

・ T.FAKE_PHOTO&SIGN

OE.FAKE_PHOTO&SIGN により、交付担当者は、申請者への旅券交付時に、申請者が持参するはがき及び身元確認書類と申請データの突合確認を行い、記載内容や写真を基に申請者本人であることを確認した後に旅券を交付する。交付担当者による本人確認は、業務管理者による監視もしくは複数の交付担当者による相互確認によって十分な確認を行えるため、申請者と異なる人物の写真や自署に基づき生成された申請を検出することができる。

これにより、申請者と異なる人物の写真または自署に基にした旅券発給の脅威に対抗できる。

8.1.3. 組織のセキュリティ方針に対するセキュリティ対策方針の適合性

・ P.OFFICIAL_DOCUMENT

OE.OFFICIAL_DOCUMENT により、決裁者及び業務管理者は、公文書へ公的な電子署名を提供するために、地方公共団体によって運用される LGPKI の職責署名用 IC カードを利用して、職責署名の生成と付与を行う。

これにより、TOE は公文書が正当かつ有効なものであることを申請者に検証させるため、公文書に対する公的な電子署名を提供しなければならないとした組織のセキュリティ方針を満足することができる。

・ P.INFRA

O.INFRA_ADMIN により、TOE は、インフラにおけるシステム運用管理を旅券事務所システム管理者及び監視者に制限する。

O.INFRA_I&A により、TOE は、インフラの機能を利用する前には、旅券事務所システム管理者または監視者の正当性を必ず確認する。

これらにより、TOE は、管理行為を特定の役割に制限し、また、特定の役割の正当性を確認できなければならないとした組織のセキュリティ方針を満足することができる。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ対策方針に対する TOE セキュリティ機能要件の適合性

セキュリティ対策方針に対する TOE セキュリティ機能要件の対応を表 8.2 に示す。

表 8.2 セキュリティ対策方針と TOE セキュリティ機能要件の対応

TOE セキュリティ機能要件 ＼ セキュリティ対策方針	O.CRYPT_MESSAGE	O.ID_AUTH	O.ACCESS_CONTROL	O.VERIFICATION	O.AUDIT	O.APP_ADMIN	O.INFRA_ADMIN	O.INFRA_I&A
FAU_ARP.1					○			
FAU_GEN.1					○			
FAU_SAA.1					○			
FAU_SAR.1					○			
FAU_STG.1					○			
FAU_STG.3					○			
FCS_CKM.1	○							
FCS_CKM.4(a)	○							
FCS_CKM.4(b)	○							
FCS_COP.1(a)				○				
FCS_COP.1(b)	○							
FCS_COP.1(c)	○							
FDP_ACC.1			○					
FDP_ACF.1			○					
FDP_UIT.1				○				
FIA_ATD.1			○					
FIA_SOS.1		○						
FIA_UAU.1								○
FIA_UAU.2(a)		○						
FIA_UAU.2(b)								○
FIA_UAU.7		○						
FIA_UID.1								○

セキュリティ対策方針 / TOE セキュリティ機能要件	O.CRYPT_MESSAGE	O.ID_AUTH	O.ACCESS_CONTROL	O.VERIFICATION	O.AUDIT	O.APP_ADMIN	O.INFRA_ADMIN	O.INFRA_I&A
FIA_UID.2(a)		○						
FIA_UID.2(b)								○
FIA_USB.1			○					
FMT_MOF.1		○				○		
FMT_MSA.2(a)				○				
FMT_MSA.2(b)	○							
FMT_MSA.2(c)	○							
FMT_MTD.1(a)						○		
FMT_MTD.1(b)						○		
FMT_MTD.1(c)							○	
FMT_MTD.1(d)							○	
FMT_MTD.1(e)							○	
FMT_MTD.1(f)							○	
FMT_SMF.1						○	○	
FMT_SMR.1(a)						○		
FMT_SMR.1(b)							○	
FPT_RVM.1		○	○					○
FPT_SEP.1		○						○
FPT_STM.1					○			
FTA_SSL.3		○						
FTP_ITC.1	○							
FTP_TRP.1	○							

以下に、『5.1.1.TOE セキュリティ機能要件』で識別したセキュリティ機能要件が必要かつ十分であることの根拠を示す。

表 8.2 により、すべてのセキュリティ機能要件は 1 つ以上の TOE セキュリティ対策方針に対応しているため、識別されたセキュリティ機能要件は必要である。

・ O.CRYPT_MESSAGE

FCS_CKM.1により、国際標準として規格化された暗号鍵生成メカニズム(DES:56bit、3DES:168bit、RSA:1024bit、RC4:128bit)により、TOEと汎用受付システム間で利用される共通鍵が生成される。

FCS_CKM.4(a)により、TOEと審査者端末間で利用された共通鍵がSSLプロトコル仕様に従って破棄される。

FCS_CKM.4(b)により、TOEと汎用受付システム間で利用される共通鍵がSSLプロトコル仕様に従って破棄される。

FMT_MSA.2(b)により、TOEと審査者端末間で共通鍵が交換され、安全に暗号化通信を行う準備が完了したことが確認されるため、セキュアな暗号鍵が準備されることが保証される。

FMT_MSA.2(c)により、TOEと汎用受付システム間で利用される共通鍵がFCS_CKM.1にて規定された標準のリストや暗号鍵生成メカニズムに従って生成され安全に暗号化通信を行う準備が完了したことが確認されるため、セキュアな暗号鍵が生成されることが保証される。

FCS_COP.1(b)により、TOEと審査者端末間で送受信される通信データに対して、国際標準として規格化された暗号メカニズム(DES:56bit、3DES:168bit、RSA:1024bit、RC4:128bit、MD5、SHA-1)により、SSLを利用した通信データの暗号化／復号化処理が行われる。

FCS_COP.1(c)により、TOEと汎用受付システム間で送受信される通信データに対して、国際標準として規格化された暗号メカニズム(DES:56bit、3DES:168bit、RSA:1024bit、RC4:128bit、MD5、SHA-1)により、SSLを利用した通信データの暗号化／復号化処理が行われる。

FTP_ITC.1により、TOEと汎用受付システム間の通信は、TSFによる申請データ取得機能、状態通知機能もしくは公文書データ通知機能の利用時に高信頼チャネルの開始が保証される。

FTP_TRP.1により、TOEと審査者端末間の通信は、リモート利用者である旅券事務担当職員による最初の利用者認証時に高信頼パスの開始が保証される。

これらにより、TOEと審査者端末間及びTOEと汎用受付システム間の通信において、SSL通信により通信データの保護を行うとした対策方針を満たすことができる。

・ O.ID_AUTH

FIA_SOS.1 により、業務アプリケーションが提供する機能へのアクセス時に求められるパスワードに一定の品質尺度を設定し、その品質尺度を基にしたパスワードの検証を行うことができる。

FIA_UAU.2(a)により、業務アプリケーションが提供する機能へのアクセス時に、先ずアクセス者が業務アプリケーションの利用権限を有した旅券事務担当職員であることの認証を行うことで、認証前には業務アプリケーションが提供する機能を利用できないことを保証できる。

FIA_UAU.7 により、パスワードの入力時にフィードバック情報「*」が画面に表示され、パスワードの漏洩を防止できる。

FIA_UID.2(a)により、業務アプリケーションが提供する機能へのアクセス時に、先ずアクセス者が誰であるかの識別を行うことで、識別前には業務アプリケーションが提供する機能を利用できないことを保証できる。

FTA_SSL.3 により、審査者端末から 10 分間 TOE への操作要求がない場合に、当該セションを自動的に切断することができる。

FMT_MOF.1 により、審査者端末から 10 分間 TOE への操作要求がない場合に当該セションを自動的に切断する機能を、10 分間待たずに任意のタイミングで実行することができる。

FPT_RVM.1 及び FPT_SEP.1 はセキュリティ対策方針の達成に必要なセキュリティ機能要件であり、『8.2.2.セキュリティ機能要件の相互支援について』にて説明する。

これらにより、業務アプリケーションが提供する機能の利用前には、識別認証により必ず正当な利用者であることを確認するとした対策方針及び業務アプリケーションが提供する機能の利用時には、審査者端末から無応答が続いた場合、該当するセションを切断するとした対策方針を満たすことができる。

・ O.ACCESS_CONTROL

FIA_ATD.1 により、業務アプリケーションが提供する機能へのアクセス時に必要な、旅券事務担当職員に属するセキュリティ属性として、役割情報が維持される。

FIA_USB.1 により、業務アプリケーションが提供する機能へのアクセス時に旅券事務担当職員を代行するサブジェクトにセキュリティ属性として役割情報を関連付けることができる。

FDP_ACC.1 により、アクセス制御 SFP を決定するために必要なサブジェクト、オブジェクト、操作を定義することで、業務アプリケーションが提供する機能利用に関するアクセス制御 SFP として旅券事務担当職員アクセス制御方針を識別することができる。

FDP_ACF.1 により、審査の各フェーズにおいて業務アプリケーションが提供する機能の利用可否を旅券事務担当職員アクセス制御方針に従って制御することができる。

FPT_RVM.1 はセキュリティ対策方針の達成に必要なセキュリティ機能要件であり、『8.2.2.セキュリティ機能要件の相互支援について』にて説明する。

これらにより、TOE が審査業務をフェーズ毎に分割して役割を定義し、役割を割り当てられた旅券事務担当職員だけに各フェーズに対応する必要最小限の機能を提供するとした対策方針を満たすことができる。

・ O.VERIFICATION

FCS_COP.1(a)により、取得した申請データに含まれる申請者署名及び法定代理人署名に対して、国際標準として規格化された暗号メカニズム（RSA:1024bit、2048bit、SHA-1）に従って、電子署名の検証を行う。

FDP_UIT.1 により、受け取った申請データに改変が生じたか否か判定することで、申請データの完全性を検証する。

FMT_MSA.2(a)により、申請データに含まれる申請者証明書もしくは法定代理人証明書の有効期間、及び、JPKI が確認した失効ステータスの結果による電子証明書の失効状態を確認することで、有効期間内かつ有効な電子証明書であることを確認する。

これにより、電子署名を検証することにより申請者から送られる申請データの完全性を検証し、また、電子証明書の有効性を確認することにより申請データの正当性を検証するとした対策方針を満たすことができる。

・ O.AUDIT

FAU_ARP.1 により、セキュリティ侵害の可能性が検出された際に、監視端末へアラートを通知する。

FAU_SAA.1 により、特定の重要度と共に記録された監査ログをセキュリティ侵害の可能性があると判断する基準を定義し、その基準に基づいた監査ログの分析を行う。

FAU_SAR.1 により、旅券事務所システム管理者及び監視者に対して、すべての監査ログを閲覧可能な形式で閲覧させることができる。

FAU_GEN.1 により、監査機能の起動と終了事象、FAU_GEN.1.1c)にて識別された事象、及び、表 5.2 にて識別された監査対象事象についての監査ログを、事象の日付・時刻、事象種別、サブジェクト識別情報、事象の結果及び重要度と共に生成することができる。

FAU_STG.1 により、生成された監査ログを不正な削除及び改変から保護することができる。

FAU_STG.3 により、監査ログが監査ログ格納領域の 80%に達した場合に、セキュリティ侵害の可能性ありとして、監査ログに記録することができる。

FPT_STM.1 により、監査ログに記録する時刻情報を取得するためにタイムスタンプを維持する。

これらにより、セキュリティ関連事象を記録するとした対策方針、記録した監査情報格納領域を管理するとした対策方針、監査記録を旅券事務所システム管理者及び監視者のみに表示するとした対策方針及びセキュリティ侵害発生時には、監査アラートを監視端末へ通知するとした対策方針を満たすことができる。

・ O.APP_ADMIN

FMT_MOF.1 により、セション管理機能のふるまいの決定や改変に影響を与える任意のタイミングによる手動セション切断の実行を業務管理者のみに制限することができる。

FMT_MTD.1(a)により、旅券事務担当職員の識別認証及びアクセス制御に関わる情報である業務管理者のパスワード、決裁者のパスワード、決裁者の役割情報、審査者のパスワード、審査者の役割情報、旅券作成検査担当者のパスワード、旅券作成検査担当者の役割情報、交付担当者のパスワード、交付担当者の役割情報の改変を業務管理者のみに制限することができる。

FMT_MTD.1(b)により、旅券事務担当職員の識別認証及びアクセス制御に関わる情報である業務管理者のユーザ ID、業務管理者のパスワード、業務管理者の役割情報、決裁者のユーザ ID、決裁者のパスワード、決裁者の役割情報、審査者のユーザ ID、審査者のパスワード、審査者の役割情報、旅券作成検査担当者のユーザ ID、旅券作成検査担当者のパスワード、旅券作成検査担当者の役割情報、交付担当者のユーザ ID、交付担当者のパスワード、交付担当者の役割情報の登録と削除を業務管理者のみに制限することができる。

FMT_SMR.1(a)により、業務管理者という役割が維持され、その役割を特定の人物に関連付けることができる。

FMT_SMF.1 により、業務管理者は与えられたセキュリティ機能の管理を行うことができる。

これらにより、業務アプリケーションにおける旅券事務担当職員の識別認証、セション管理及びアクセス制御の運用管理を業務管理者のみに制限するとした対策方針を満たすことができる。

・ O.INFRA_ADMIN

FMT_MTD.1(c)により、セキュリティ侵害の可能性ありと判断するシグネチャに対する問い合わせ、改変を旅券事務所システム管理者及び監視者のみに制限することができる。

FMT_MTD.1(d)により、監視者のパスワードに対する改変を旅券事務所システム管理者及び監視者のみに制限することができる。

FMT_MTD.1(e)により、システム内時刻に対する問い合わせ、改変を旅券事務所システム管理者のみに制限することができる。

FMT_MTD.1(f)により、旅券事務所システム管理者のパスワードに対する改変を旅券事務所システム管理者のみに制限することができる。

FMT_SMR.1(b)により、旅券事務所システム管理者、監視者という役割が維持され、その役割を特定の人物に関連付けることができる。

FMT_SMF.1 により、旅券事務所システム管理者及び監視者は与えられた TSF データの

管理を行うことができる。

これらにより、インフラにおけるシステム運用管理を旅券事務所システム管理者及び監視者に制限するとした対策方針を満たすことができる。

・ O.INFRA_I&A

FIA_UAU.1により、旅券事務所システム管理者による特定の機能（言語の選択、GUIでのログイン／コマンドラインからのログインの選択、ログインサーバの選択、ヘルプの参照）以外のインフラが提供する機能へのアクセス時に、先ずアクセス者がインフラ機能の利用権限を有した旅券事務所システム管理者であることの認証を行うことで、認証前には特定の機能（言語の選択、GUI でのログイン／コマンドラインからのログインの選択、ログインサーバの選択、ヘルプの参照）以外のインフラが提供する機能を利用できないことを保証できる。

FIA_UAU.2(b)により、監視者によるインフラが提供する機能へのアクセス時に、先ずアクセス者がインフラ機能の利用権限を有した監視者であることの認証を行うことで、認証前にはインフラが提供する機能を利用できないことを保証できる。

FIA_UID.1により、旅券事務所システム管理者による特定の機能（言語の選択、GUIでのログイン／コマンドラインからのログインの選択、ログインサーバの選択、ヘルプの参照）以外のインフラが提供する機能へのアクセス時に、先ずアクセス者が誰であるかの識別を行うことで、識別前には特定の機能（言語の選択、GUI でのログイン／コマンドラインからのログインの選択、ログインサーバの選択、ヘルプの参照）以外のインフラが提供する機能を利用できないことを保証できる。

FIA_UID.2(b)により、監視者によるインフラが提供する機能へのアクセス時に、先ずアクセス者が誰であるかの識別を行うことで、識別前にはインフラが提供する機能を利用できないことを保証できる。

FPT_RVM.1 及び FPT_SEP.1 はセキュリティ対策方針の達成に必要なセキュリティ機能要件であり、『8.2.2.セキュリティ機能要件の相互支援について』にて説明する。

これらにより、インフラが提供する機能の利用前には、旅券事務所システム管理者または監視者の正当性を必ず確認するとした対策方針を満たすことができる。

8.2.2. セキュリティ機能要件の相互支援について

本項では、明示的な依存関係は要求されないが、相互支援を目的として選択されたセキュリティ機能要件について記述する。

【迂回防止】

FPT_RVM.1により、TSC内の各機能の動作進行が許可される前に、識別認証に関するセキュリティ機能要件及びオブジェクトに対するアクセスの制御に関するセキュリティ機能要件が呼び出され成功することが保証される。対象となるセキュリティ機能要件は、FIA_ATD.1、FIA_UAU.1、FIA_UAU.2(a)、FIA_UAU.2(b)、FIA_UID.1、FIA_UID.2(a)、FIA_UID.2(b)、FIA_UAU.7、FIA_SOS.1、FIA_USB.1、FDP_ACC.1、FDP_ACF.1である。

【干渉防止】

FPT_SEP.1により、識別認証に関するセキュリティ機能要件が呼び出されることで各サブジェクトが識別され、信頼できないサブジェクトによる干渉及び改ざんを防止することが保証される。対象となるセキュリティ機能要件は、FIA_UAU.1、FIA_UAU.2(a)、FIA_UAU.2(b)、FIA_UID.1、FIA_UID.2(a)、FIA_UID.2(b)、FIA_UAU.7、FIA_SOS.1である。

【非活性化防止】

FMT_MOF.1により、セキュリティ機能を管理する能力を業務管理者のみに制限するため、信頼できない役割によるセキュリティ機能の非活性化攻撃を防止できる。

【無効化検出】

FAU_GEN.1により、セキュリティ機能の無効化を目的とした攻撃の検出が可能となる。

8.2.3. TOE セキュリティ機能要件間の依存関係

TOE セキュリティ機能要件間の依存関係を表 8.3 に示す。

表 8.3 TOE セキュリティ機能要件間の依存関係

No	TOE セキュリティ機能要件	下位階層	依存関係	参照 No	備考
1	FAU_ARP.1	－	FAU_SAA.1	3	
2	FAU_GEN.1	－	FPT_STM.1	41	
3	FAU_SAA.1	－	FAU_GEN.1	2	
4	FAU_SAR.1	－	FAU_GEN.1	2	
5	FAU_STG.1	－	FAU_GEN.1	2	
6	FAU_STG.3	－	FAU_STG.1	5	
7	FCS_CKM.1	－	FCS_COP.1(c)	12	
			FCS_CKM.4(b)	9	
			FMT_MSA.2(c)	29	
8	FCS_CKM.4(a)	－	[FDP_ITC.1 または FCS_CKM.1]	－	※1
			FMT_MSA.2(b)	28	
9	FCS_CKM.4(b)	－	FCS_CKM.1	7	
			FMT_MSA.2(b)	28	
10	FCS_COP.1(a)		[FDP_ITC.1 または FCS_CKM.1]	－	※2
			FCS_CKM.4	－	※3
			FMT_MSA.2(a)	27	
11	FCS_COP.1(b)	－	[FDP_ITC.1 または FCS_CKM.1]	－	※4
			FCS_CKM.4(a)	8	※5
			FMT_MSA.2(b)	28	※6
12	FCS_COP.1(c)	－	FCS_CKM.1	7	※7
			FCS_CKM.4(b)	9	※8

No	TOE セキュリティ機能要件	下位階層	依存関係	参照 No	備考
			FMT_MSA.2(c)	29	※9
13	FDP_ACC.1	－	FDP_ACF.1	14	
14	FDP_ACF.1	－	FDP_ACC.1	13	
			FMT_MSA.3	－	※10
15	FDP_UIT.1	－	FDP_ACC.1	13	
			FTP_ITC.1	43	
16	FIA_ATD.1	－	－	－	
17	FIA_SOS.1	－	－	－	
18	FIA_UAU.1	－	FIA_UID.1	22	
19	FIA_UAU.2(a)	FIA_UAU.1	FIA_UID.1	23	FIA_UID.2(a)はFIA_UID.1の上位階層コンポーネントである
20	FIA_UAU.2(b)	FIA_UAU.1	FIA_UID.1	24	FIA_UID.2(b)はFIA_UID.1の上位階層コンポーネントである
21	FIA_UAU.7	－	FIA_UAU.1	19	FIA_UAU.2(a)はFIA_UAU.1の上位階層コンポーネントである
22	FIA_UID.1	－	－	－	
23	FIA_UID.2(a)	FIA_UID.1	－	－	
24	FIA_UID.2(b)	FIA_UID.1	－	－	
25	FIA_USB.1	－	FIA_ATD.1	16	
26	FMT_MOF.1	－	FMT_SMF.1	36	
			FMT_SMR.1(a)	37	
27	FMT_MSA.2(a)	－	ADV_SPM.1	－	※11
			FDP_ACC.1	13	
			FMT_MSA.1	－	※12
			FMT_SMR.1	－	※13
28	FMT_MSA.2(b)	－	ADV_SPM.1	－	※14
			FDP_ACC.1 または FDP_IFC.1	－	※15
			FMT_MSA.1	－	※16
			FMT_SMR.1	－	※17
29	FMT_MSA.2(c)	－	ADV_SPM.1	－	※18

No	TOE セキュリティ機能要件	下位階層	依存関係	参照 No	備考
			FDP_ACC.1 または FDP_IFC.1	－	※19
			FMT_MSA.1	－	※20
			FMT_SMR.1	－	※21
30	FMT_MTD.1(a)	－	FMT_SMF.1	36	
			FMT_SMR.1(a)	37	
31	FMT_MTD.1(b)	－	FMT_SMF.1	36	
			FMT_SMR.1(a)	37	
32	FMT_MTD.1(c)	－	FMT_SMF.1	36	
			FMT_SMR.1(b)	38	
33	FMT_MTD.1(d)	－	FMT_SMF.1	36	
			FMT_SMR.1(b)	38	
34	FMT_MTD.1(e)	－	FMT_SMF.1	36	
			FMT_SMR.1(b)	38	
35	FMT_MTD.1(f)	－	FMT_SMF.1	36	
			FMT_SMR.1(b)	38	
36	FMT_SMF.1	－	－	－	
37	FMT_SMR.1(a)	－	FIA_UID.1	23	FIA_UID.2(a)はFIA_UID.1の上位階層コンポーネントである
38	FMT_SMR.1(b)	－	FIA_UID.1	22 24	FIA_UID.2(b)はFIA_UID.1の上位階層コンポーネントである
39	FPT_RVM.1	－	－	－	
40	FPT_SEP.1	－	－	－	
41	FPT_STM.1	－	－	－	
42	FTA_SSL.3	－	－	－	
43	FTP_ITC.1	－	－	－	
44	FTP_TRP.1	－	－	－	

※1 ：FCS_CKM.4(a)にて廃棄対象となる暗号鍵は、セション確立時に生成される共通鍵である。この共通鍵の生成／インポートは、審査者端末が SSL として標準化されたプロトコルによって実現する。SSL では、共通鍵の交換が成功したことを確認する処理

も含まれており、また、エラー時のふるまいも規定されている。このため、暗号鍵の生成／インポートが失敗した状態で SSL 通信が継続することはない。よって、暗号鍵の生成／インポートに関する安全性は保証されている。したがって、安全な暗号鍵の生成、導入に関するセキュリティ機能要件 FCS_CKM.1 及び FDP_ITC.1 は不要である。

※2 ：FCS_COP.1(a)にて使用する暗号鍵は、申請者証明書及び法定代理人証明書に含まれる公開鍵である。公開鍵は、申請者による電子申請時に申請データとして取得されるため、暗号鍵の生成やインポートは行われない。なお、FCS_COP.1(a)では、セキュアハッシュも使用しているが、セキュアハッシュは暗号鍵ではないため、その生成は不要である。したがって、安全な暗号鍵の生成、導入に関するセキュリティ機能要件 FDP_ITC.1 及び FCS_CKM.1 は不要である。

※3 ：FCS_COP.1(a)にて使用する暗号鍵は、申請者証明書及び法定代理人証明書に含まれる公開鍵である。公開鍵は、申請者証明書及び法定代理人証明書に含まれる公開情報であるため、明示的に破棄を実施する必要はない。なお、FCS_COP.1(a)では、セキュアハッシュも使用しているが、セキュアハッシュは暗号鍵ではないため、その破棄は不要である。したがって、安全な暗号鍵の破棄に関するセキュリティ機能要件 FCS_CKM.4 は不要である。

※4 ：FCS_COP.1(b)にて使用する暗号鍵は、TOE の秘密鍵、電子証明書に含まれる公開鍵及びセション確立時に生成される共通鍵である。このうち、TOE の秘密鍵及び電子証明書に含まれる公開鍵の信頼性は、A.TRUST_CRYPT 及び OE.TRUST_CRYPT によって、地方公共団体が運用する外務省 CA が保証するため、暗号鍵の生成に関する安全性は保証されている。さらに、TOE の秘密鍵及び電子証明書に含まれる公開鍵は、TOE の構築時に運用環境移行手順書（ADO_IGS.1 を満たす手順書）に従って格納されるため、暗号鍵のインポートに関する手順は保証されている。また、共通鍵の生成／インポートは、審査者端末が SSL として標準化されたプロトコルによって実現する。SSL では、共通鍵の交換が成功したことを確認する処理も含まれており、また、エラー時のふるまいも規定されている。このため、暗号鍵の生成／インポートが失敗した状態で SSL 通信が継続することはない。よって、暗号鍵の生成／インポートに関する安全性は保証されている。なお、FCS_COP.1(b)では、セキュアハッシュも使用しているが、セキュアハッシュは暗号鍵ではないため、その生成は不要である。したがって、安全な暗号鍵の生成、導入に関するセキュリティ機能要件 FCS_CKM.1 及び FDP_ITC.1 は不要である。

※5 ：FCS_COP.1(b)にて使用する暗号鍵は、TOE の秘密鍵、電子証明書に含まれる公開鍵及びセション確立時に生成される共通鍵である。このうち、TOE の秘密鍵及び電子証明書に含まれる公開鍵は、TOE の構築時に格納された後、TOE が破棄されるまで使用し続けるため、破棄する必要はない。したがって、TOE の秘密鍵、電子証明書に含まれる公開鍵に対して、安全な暗号鍵の破棄に関するセキュリティ機能要件 FCS_CKM.4 は不要である。ただし、セション確立時に生成される共通鍵については、FCS_CKM.4(a)によって安全に破棄される必要がある。

※6 ：FCS_COP.1(b)にて使用する暗号鍵は、TOE の秘密鍵、電子証明書に含まれる公開鍵及びセション確立時に生成される共通鍵である。このうち、TOE の秘密鍵及び電子証明書に含まれる公開鍵の信頼性は、A.TRUST_CRYPT 及び OE.TRUST_CRYPT によって、地方公共団体が運用する外務省 CA が保証するため、暗号鍵に関するセキュリティ属性の安全性は保証されている。したがって、TOE の秘密鍵、電子証明書に含まれる公開鍵に対して、セキュアなセキュリティ属性の受け入れに関するセキュリティ機能要件 FMT_MSA.2 は不要である。ただし、セション確立時に生成される共通鍵に関するセキュリティ属性については、FMT_MSA.2(b)によって保証される必要がある。

※7 ：FCS_COP.1(c)にて規定された暗号操作に関連する暗号鍵は、汎用受付システムの秘密鍵、電子証明書に含まれる公開鍵及びセション確立時に生成される共通鍵である。このうち、汎用受付システムの秘密鍵及び電子証明書に含まれる公開鍵の信頼性は、A.TRUST_CRYPT 及び OE.TRUST_CRYPT によって、地方公共団体が運用する LGPKI が保証するため、暗号鍵の生成に関する安全性は保証されている。さらに、汎用受付システムの秘密鍵及び電子証明書に含まれる公開鍵は、TOE 構築前に導入されるため、暗号鍵のインポートに関する手順は保証されている。したがって、汎用受付システムの秘密鍵、電子証明書に含まれる公開鍵に対して、安全な暗号鍵の生成、導入に関するセキュリティ機能要件 FCS_CKM.1 及び FDP_ITC.1 は不要である。ただし、セション確立時に生成される共通鍵については、FCS_CKM.1 によって安全に生成される必要がある。

※8 ：FCS_COP.1(c)にて規定された暗号操作に関連する暗号鍵は、汎用受付システムの秘密鍵、電子証明書に含まれる公開鍵及びセション確立時に生成される共通鍵である。このうち、汎用受付システムの秘密鍵及び電子証明書に含まれる公開鍵は、安全に維持される必要があるため、破棄する必要はない。したがって、汎用受付システムの秘密鍵、電子証明書に含まれる公開鍵に対して、安全な暗号鍵の破棄に関するセキュリティ機能要件 FCS_CKM.4 は不要である。ただし、セション確立時に生成される共通鍵については、FCS_CKM.4(b)によって安全に破棄される必要がある。

※9 ：FCS_COP.1(c)にて規定された暗号操作に関連する暗号鍵は、汎用受付システムの秘密鍵、電子証明書に含まれる公開鍵及びセション確立時に生成される共通鍵である。このうち、汎用受付システムの秘密鍵及び電子証明書に含まれる公開鍵の信頼性は、A.TRUST_CRYPT 及び OE.TRUST_CRYPT によって、地方公共団体が運用する LGPKI が保証するため、暗号鍵に関するセキュリティ属性の安全性は保証されている。したがって、汎用受付システムの秘密鍵、電子証明書に含まれる公開鍵に対して、セキュアなセキュリティ属性の受け入れに関するセキュリティ機能要件 FMT_MSA.2 は不要である。ただし、セション確立時に生成される共通鍵に関するセキュリティ属性については、FMT_MSA.2(c)によって保証される必要がある。

※10：アクセス制御の対象となる保護対象資産は、データベースに格納される。データベースに格納された保護対象資産は、業務アプリケーションによるアクセス制御によって、テーブル操作が行われる。また、データベースは、TOE 導入時に予めセキュリティ属性が付与された状態で構築され、その状態が維持される。すなわち、運用時に新たなデータベースの追加、生成は行われず、アクセス制御を実施するためのセキュリティ属性も固定値である。したがって、保護対象資産に関するセキュリティ属性のデフォルト値や初期値の管理は不要であり、FMT_MSA.3 は必要ない。

※11：FMT_MSA.2(a)が対象とするセキュリティ属性は申請者もしくは法定代理人の公開鍵を含む、申請者証明書もしくは法定代理人証明書の有効性である。この申請者証明書及び法定代理人証明書は A.TRUST_PKI 及び OE.TRUST_PKI によって、JPKI が発行、管理しており、TOE はこれを信頼している。したがって、TOE のセキュリティ方針モデルを表現するセキュリティ保証要件 ADV_SPM.1 は不要である。

※12：FMT_MSA.2(a)が対象とするセキュリティ属性は申請者もしくは法定代理人の公開鍵を含む、申請者証明書もしくは法定代理人証明書の有効性である。この申請者証明書及び法定代理人証明書は A.TRUST_PKI 及び OE.TRUST_PKI によって、JPKI が発行、管理しており、TOE はこれを信頼している。したがって、セキュリティ属性の管理に関するセキュリティ機能要件 FMT_MSA.1 は不要である。

※13：FMT_MSA.2(a)が対象とするセキュリティ属性は申請者もしくは法定代理人の公開鍵を含む、申請者証明書もしくは法定代理人証明書の有効性である。この申請者証明書及び法定代理人証明書は A.TRUST_PKI 及び OE.TRUST_PKI によって、JPKI が発行、管理しており、TOE はこれを信頼している。したがって、セキュリティ役割に関するセキュリティ機能要件 FMT_SMR.1 は不要である。

※14：FMT_MSA.2(b)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、暗号操作に必要なセキュリティ属性であるが、暗号操作では暗号化／復号化の操作のみであり、暗号する／しないといったセキュリティに関する制御はない。したがって、TOE のセキュリティ方針モデルを表現するセキュリティ保証要件 ADV_SPM.1 は不要である。

※15：FMT_MSA.2(b)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、暗号操作に必要なセキュリティ属性であり、利用者データの保護を目的としたアクセス制御方針や情報フロー制御方針に関するセキュリティ属性ではない。したがって、利用者データの保護に関する FDP_ACC.1 及び FDP_IFC.1 は不要である。

※16：FMT_MSA.2(b)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、プログラムとして定められた属性の中から最適のものが選択されるため、セキュリティ役割によるセキュリティ属性の管理は行えない。したがって、セキュリティ属性の管理に関するセキュリティ機能要件 FMT_MSA.1 は不要である。

※17：FMT_MSA.2(b)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、プログラムとして定められた属性の中から最適のものが選択されるため、セキュリティ役割によるセキュリティ属性の管理は行えない。したがって、セキュリティ役割に関するセキュリティ機能要件 FMT_SMR.1 は不要である。

※18：FMT_MSA.2(c)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、暗号操作に必要なセキュリティ属性であるが、暗号操作では暗号化／復号化の操作のみであり、暗号する／しないといったセキュリティに関する制御はない。したがって、TOE のセキュリティ方針モデルを表現するセキュリティ保証要件 ADV_SPM.1 は不要である。

※19：FMT_MSA.2(c)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、暗号操作に必要なセキュリティ属性であり、利用者データの保護を目的としたアクセス制御方針や情報フロー制御方針に関するセキュリティ属性ではない。したがって、利用者データの保護に関する FDP_ACC.1 及び FDP_IFC.1 は不要である。

※20：FMT_MSA.2(c)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、プログラムとして定められた属性の中から最適のものが選択されるため、セキュリティ役割によるセキュリティ属性の管理は行えない。したがって、セキュリティ属性の管理に関するセキュリティ機能要件 FMT_MSA.1 は不要である。

※21：FMT_MSA.2(c)が対象とするセキュリティ属性は、セション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、プログラムとして定められた属性の中から最適のものが選択されるため、セキュリティ役割によるセキュリティ属性の管理は行えない。したがって、セキュリティ役割に関するセキュリティ機能要件 FMT_SMR.1 は不要である。

8.2.4. TOE セキュリティ保証要件の選択根拠

本 ST にて要求する TOE に対する保証レベルは EAL2 に AVA_MSU.1 を追加した EAL2 追加である。

本 TOE は、不特定多数の人間に対して公開しているシステムではないが、庁内ネットワークに接続され、特定の外部インタフェースを利用した外部アクセスを受ける。このため、外部インタフェースの識別、機能の内部構造の特定、テストによるセキュリティ機能の確認、脆弱性分析といった開発プロセスにおけるセキュリティ確保への取組みが求められる。これらの要求を満たす保証レベルとして EAL2 が適切である。

また、TOE はその特性上、複数の IT 製品から構成され運用される。そのため、TOE をセキュアに利用するには、各 IT 製品に対して正しい利用、適切な運用管理が必要である。したがって、誤使用の可能性及び非セキュアな状態への遷移の可能性を低減するための保証として AVA_MSU.1 を追加する。

なお、追加した保証要件コンポーネントである AVA_MSU.1 と依存関係にある以下の保証要件コンポーネントも EAL2 のセットに含まれており、選択された保証要件のセットにおいて依存性も満たされている。

- ADO_IGS.1
- ADV_FSP.1
- AGD_ADM.1
- AGD_USR.1

8.2.5. セキュリティ対策方針に対するセキュリティ機能強度の一貫性

本 ST にて主張する TOE に対する最小機能強度は SOF-基本である。

TOE は、以下のような環境にて運用されることが想定されている。

- TOE が設置される筐体及び保護対象資産の複製物は、旅券事務所システム管理者以外の物理的アクセスが禁止されている。
- 審査者端末が設置される部屋は、施錠管理により TOE に関係する人物以外の入室を禁止されている。
- 監視端末が設置される部屋は、監視者以外の入室が禁止されている。
- TOE が設置されるネットワークと庁内ネットワークは、TOE の業務アプリケーションの機能に必要な通信以外の通過を禁止された特定個所で接続される。
- TOE と運用支援センター間は、TOE と運用支援センターのみが通信可能な閉域ネットワークで接続される。

更に、TOE に関連する役割については以下のような条件を想定している

- 旅券事務所システム管理者、業務管理者、決裁者及び監視者は信用できる人物であり、各々に許可された行為において不正は行わない。
- 審査者、旅券作成検査担当者及び交付担当者は、パスワード及び審査者端末に表示される保護対象資産の情報を他人に漏らすことはない。
- 保守担当者による作業は旅券事務所システム管理者の監視のもと実施され、不正な操作は行われない。

このため、TOE に対して論理的／物理的にアクセスし、攻撃を行うことができる脅威エージェントとして以下を特定することができる。

攻撃レベル：低レベル

攻撃頻度：低

よって、セキュリティ対策方針として低レベルの攻撃者に対抗できることが求められる。一方、セキュリティ機能要件に対する最小機能強度主張は SOF-基本であり、セキュリティ対策方針に求められるレベルと一貫している。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能要件に対する TOE 要約仕様の適合性

TOE セキュリティ機能要件に対する TOE 要約仕様の関係を表 8.4 に示す。

表 8.4 TOE セキュリティ機能要件と TOE 要約仕様の対応

TOE 要約仕様 / TOE セキュリティ機能要件	F. APLACTL	F. SESMAN	F. USEMAN	F. CRYCOM	F. SIGVER	F. AUDIT	F. INFMAN
FAU_ARP.1						○	
FAU_GEN.1						○	
FAU_SAA.1						○	
FAU_SAR.1						○	
FAU_STG.1						○	
FAU_STG.3						○	
FCS_CKM.1				○			
FCS_CKM.4(a)				○			
FCS_CKM.4(b)				○			
FCS_COP.1(a)					○		
FCS_COP.1(b)				○			
FCS_COP.1(c)				○			
FDP_ACC.1	○						
FDP_ACF.1	○						
FDP_UIT.1					○		
FIA_ATD.1	○						
FIA_SOS.1	○						
FIA_UAU.1							○
FIA_UAU.2(a)	○						
FIA_UAU.2(b)							○
FIA_UAU.7	○						
FIA_UID.1							○
FIA_UID.2(a)	○						

TOE 要約仕様 / TOE セキュリティ機能要件	F.APLACTL	F.SESMAN	F.USEMAN	F.CRYCOM	F.SIGVER	F.AUDIT	F.INFMAN
FIA_UID.2(b)							○
FIA_USB.1	○						
FMT_MOF.1		○					
FMT_MSA.2(a)					○		
FMT_MSA.2(b)				○			
FMT_MSA.2(c)				○			
FMT_MTD.1(a)			○				
FMT_MTD.1(b)			○				
FMT_MTD.1(c)							○
FMT_MTD.1(d)							○
FMT_MTD.1(e)							○
FMT_MTD.1(f)							○
FMT_SMF.1			○				○
FMT_SMR.1(a)			○				
FMT_SMR.1(b)							○
FPT_RVM.1	○						○
FPT_SEP.1	○						○
FPT_STM.1						○	
FTA_SSL.3		○					
FTP_ITC.1				○			
FTP_TRP.1				○			

以下に、『6.TOE 要約仕様』で識別した TOE 要約仕様が必要かつ十分であることの根拠を示す。

表 8.4 により、すべての TOE 要約仕様は 1 つ以上の TOE セキュリティ機能要件に対応しているため、識別された TOE 要約仕様は必要である。

・ FAU_ARP.1

FAU_ARP.1 では、セキュリティ侵害の可能性を検出した場合に実行されるアクションとして、監視端末へのアラート通知を規定している。

F.AUDIT では、セキュリティ侵害の可能性を検出した場合、監視端末にアラート通知を行う。

したがって、FAU_ARP.1 は、F.AUDIT によって満たされる。

・ FAU_GEN.1

FAU_GEN.1 では、監査機能の起動と終了、表 5.2 に示されている一覧を、生成する監査記録として規定している。また、各監査記録において、事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗)、事象の重要度を記録することを規定している。

F.AUDIT では、表 6.6 に示された監査事象発生の日時・時刻／事象発生者／事象の結果／事象の重要度を監査ログに記録する。また、表 6.6 で示されている監査事象の内容は、FAU_GEN.1 で規定した各監査記録を過不足なく再現している。

したがって、FAU_GEN.1 は、F.AUDIT によって満たされる。

・ FAU_SAA.1

FAU_SAA.1 では、監査事象をモニタリングする規則として、すべての監査対象事象に関して、特定の重要度と共に監査ログが生成された場合に、セキュリティ侵害の可能性があると判断することを規定している。

F.AUDIT では、監査ログのリアルタイム監視を行い、シグネチャに示された特定の重要度を含む事象が発生した場合、その事象をセキュリティ侵害の可能性があると判断する。

したがって、FAU_SAA.1 は、F.AUDIT によって満たされる。

・ FAU_SAR.1

FAU_SAR.1 では、旅券事務所システム管理者または監視者に、監査記録を読み出させることを規定している。

F.AUDIT では、旅券事務所システム管理者または監視者に、監査ログに記録されている情報を参照させることが可能である。

したがって、FAU_SAR.1 は、F.AUDIT によって満たされる。

・ FAU_STG.1

FAU_STG.1 では、監査記録が不正な削除から保護されることを規定している。また、監査記録の改変が防止されることを規定している。

F.AUDIT では、監査記録を不正な削除から保護するために、監査ログ格納領域を保護している。また、監査ログ格納領域の保護によって、監査記録の改変が防止できる。

したがって、FAU_STG.1 は、F.AUDIT によって満たされる。

・ FAU_STG.3

FAU_STG.3 では、監査証跡が 80%の閾値を超えた場合、監査ログを生成することを規定している。

F.AUDIT では、監査ログ格納領域の 80%を閾値として設定し、閾値を超えた場合、その旨を監査ログに記録する。

したがって、FAU_STG.3 は、F.AUDIT によって満たされる。

・ FCS_CKM.1

FCS_CKM.1 では、汎用受付システムと TOE 間の SSL 通信に利用する共通鍵を生成する暗号鍵生成アルゴリズム、鍵長、標準のリストを規定している。

F.CRYCOM では、表 6.4 にて（※）印で識別された暗号鍵生成アルゴリズムを用いて、識別された鍵長の共通鍵を生成しており、その内容は FCS_CKM.1 で規定した暗号鍵生成アルゴリズム及び鍵長と一貫している。また、表 6.4 では、暗号鍵生成アルゴリズムの仕様についても言及しており、その内容は、FCS_CKM.1 で規定した標準リストと一貫している。

したがって、FCS_CKM.1 は、F.CRYCOM によって満たされる。

・ FCS_CKM.4(a)

FCS_CKM.4(a)では、審査者端末と TOE 間の SSL 通信に利用する共通鍵を破棄する暗号鍵破棄方法、標準のリストを規定している。

F.CRYCOM では、SSL プロトコル仕様に従って暗号鍵を破棄しており、その内容は FCS_CKM.4(a)で規定した暗号鍵破棄方法、標準リストと一貫している。

したがって、FCS_CKM.4(a)は、F.CRYCOM によって満たされる。

・ FCS_CKM.4(b)

FCS_CKM.4(b)では、汎用受付システムと TOE 間の SSL 通信に利用する共通鍵を破棄する暗号鍵破棄方法、標準のリストを規定している。

F.CRYCOM では、SSL プロトコル仕様に従って暗号鍵を破棄しており、その内容は FCS_CKM.4(b)で規定した暗号鍵破棄方法、標準リストと一貫している。

したがって、FCS_CKM.4(b)は、F.CRYCOM によって満たされる。

・ FCS_COP.1(a)

FCS_COP.1(a)では、申請者署名及び法定代理人署名の検証で使用する暗号アルゴリズム、鍵長、標準のリストを規定している。

F.SIGVER では、表 6.5 に示された暗号アルゴリズム、鍵長の暗号鍵を用いて、申請者署名及び法定代理人署名の検証を実施しており、その内容は、FCS_COP.1(a)で規定した暗号アルゴリズム及び鍵長と一貫している。また、表 6.5 では、暗号アルゴリズムの仕様についても言及しており、その内容は、FCS_COP.1(a)で規定した標準リストと一貫している。

したがって、FCS_COP.1(a)は、F.SIGVER によって満たされる。

・ FCS_COP.1(b)

FCS_COP.1(b)では、審査者端末と TOE 間において、SSL を利用した通信データの暗号化／復号化処理に使用する暗号アルゴリズム、鍵長、標準のリストを規定している。

F.CRYCOM では、表 6.3 に示された暗号アルゴリズム、鍵長の暗号鍵を用いて、審査者端末と TOE 間の HTTPS による通信を実施しており、その内容は、FCS_COP.1(b)で規定した暗号アルゴリズム及び鍵長と一貫している。また、表 6.3 では、暗号アルゴリズムの仕様についても言及しており、その内容は、FCS_COP.1(b)で規定した標準リストと一貫している。

したがって、FCS_COP.1(b)は、F.CRYCOM によって満たされる。

・ FCS_COP.1(c)

FCS_COP.1(c)では、汎用受付システムと TOE 間において、SSL を利用した通信データの暗号化／復号化処理に使用する暗号アルゴリズム、鍵長、標準のリストを規定している。

F.CRYCOM では、表 6.4 に示された暗号アルゴリズム、鍵長の暗号鍵を用いて、汎用受付システムと TOE 間の HTTPS による通信を実施しており、その内容は、FCS_COP.1(c)で規定した暗号アルゴリズム及び鍵長と一貫している。また、表 6.4 では、暗号アルゴリズムの仕様についても言及しており、その内容は、FCS_COP.1(c)で規定した標準リストと一貫している。

したがって、FCS_COP.1(c)は、F.CRYCOM によって満たされる。

・ FDP_ACC.1

FDP_ACC.1 では、表 5.3 に示されている一覧を、旅券事務担当職員アクセス制御方針で形成されるサブジェクト、オブジェクト、操作リストとして規定している。

F.APLACTL では、表 6.2 に示された旅券事務担当職員アクセス制御方針を実施している。表 6.2 で示されている制御内容は、FDP_ACC.1 で規定したサブジェクト、オブジェ

クト及び操作リストを過不足なく再現している。また、サブジェクトは、役割情報を関連付けた旅券事務担当職員を代行するプロセスであることも示されている。

したがって、FDP_ACC.1 は、F.APLACTL によって満たされる。

・ FDP_ACF.1

FDP_ACF.1 では、役割情報、資源情報、操作情報に基づいて、旅券事務担当職員アクセス制御方針が実施されることを規定している。また、アクセス制御規則は、表 5.3 に示されている一覧と一致した場合、許可され、それ以外の場合は拒否されることを規定している。

F.APLACTL では、プロセスに関連付けられた役割情報、アクセス資源を識別するための資源情報、操作内容を識別するための操作情報に基づき、旅券事務担当職員アクセス制御方針を実施している。また、アクセス制御規則は、表 6.2 の規則に従ったアクセスを許可し、それ以外のアクセスは拒否している。

したがって、FDP_ACF.1 は、F.APLACTL によって満たされる。

・ FDP_UIT.1

FDP_UIT.1 では、受け取った申請データに改変が生じたことを判定できることを規定している。

F.SIGVER では、申請者署名もしくは法定代理人署名の検証により、申請データに改変が生じたか否か判定している。

したがって、FDP_UIT.1 は、F.SIGVER によって満たされる。

・ FIA_ATD.1

FAU_ATD.1 では、業務アプリケーションにおいて、個々の利用者に関連付けられる役割情報の維持を規定している。

F.APLACTL では、業務アプリケーションにおいて、個々の旅券事務担当職員に関連付けられる役割情報が、ログアウトされるまで維持されている。

したがって、FIA_ATD.1 は、F.APLACTL によって満たされる。

・ FIA_SOS.1

FIA_SOS.1 では、秘密を検証するための品質尺度を規定している。

F.APLACTL では、表 6.1 に示されたパスワード長、使用可能文字を用いてパスワード検証を実施しており、その内容は、FIA_SOS.1 で規定した品質尺度と一貫している。

したがって、FIA_SOS.1 は、F.APLACTL によって満たされる。

・ FIA_UAU.1

FIA_UAU.1 では、インフラにおける旅券事務所システム管理者の認証に関して、認証前に許可されるアクションを規定している。

F.INFMAN では、インフラを利用する際に、必ずユーザ ID 及びパスワードの入力を促し、旅券事務所システム管理者の認証を行っている。また、旅券事務所システム管理者に関して、認証前に許可している操作を識別しており、その内容は、FIA_UAU.1 で規定したアクションと一貫している。

したがって、FAU_UAU.1 は、F.INFMAN によって満たされる。

・ FIA_UAU.2(a)

FIA_UAU.2(a)では、業務アプリケーションにおいて、アクションを許可する前に、旅券事務担当職員自身の認証を行うことを規定している。

F.APLACTL では、業務アプリケーションを利用する際に、必ずユーザ ID 及びパスワードの入力を促し、旅券事務担当職員の認証を行っている。また、ユーザ ID 及びパスワードの入力以外に操作できることは何もない。

したがって、FAU_UAU.2(a)は、F.APLACTL によって満たされる。

・ FIA_UAU.2(b)

FIA_UAU.2(b)では、インフラにおいて、アクションを許可する前に、監視者自身の認証を行うことを規定している。

F.INFMAN では、インフラを利用する際に、必ずユーザ ID 及びパスワードの入力を促し、監視者の認証を行っている。また、ユーザ ID 及びパスワードの入力以外に操作できることは何もない。

したがって、FAU_UAU.2(b)は、F.INFMAN によって満たされる。

・ FIA_UAU.7

FIA_UAU.7 では、認証の間に、利用者へ提供するフィードバックリストを規定している。

F.APLACTL では、パスワード入力の際、入力された文字数分だけ”*”表示を行っている。

したがって、FAU_UAU.7 は、F.APLACTL によって満たされる。

・ FIA_UID.1

FIA_UID.1 では、インフラにおける旅券事務所システム管理者の識別に関して、識別前に許可されるアクションを規定している。

F.INFMAN では、インフラを利用する際に、必ずユーザ ID 及びパスワードの入力を促

し、旅券事務所システム管理者の識別を行っている。また、旅券事務所システム管理者に関して、識別認証前に許可している操作を識別しており、その内容は、FIA_UID.1 で規定したアクションと一貫している。

したがって、FAU_UID.1 は、F.INFMAN によって満たされる。

・ FIA_UID.2(a)

FIA_UID.2(a)では、業務アプリケーションにおいて、アクションを許可する前に、利用者自身の識別を行うことを規定している。

F.APLACTL では、業務アプリケーションを利用する際に、必ずユーザ ID 及びパスワードの入力を促し、旅券事務担当職員の識別を行っている。また、ユーザ ID 及びパスワードの入力以外に操作できることは何もない。

したがって、FAU_UID.2(a)は、F.APLACTL によって満たされる。

・ FIA_UID.2(b)

FIA_UID.2(b)では、インフラにおいて、アクションを許可する前に、利用者自身の識別を行うことを規定している。

F.INFMAN では、インフラを利用する際に、必ずユーザ ID 及びパスワードの入力を促し、監視者の識別を行っている。また、ユーザ ID 及びパスワードの入力以外に操作できることは何もない。

したがって、FAU_UID.2(b)は、F.INFMAN によって満たされる。

・ FIA_USB.1

FIA_USB.1 では、業務アプリケーションにおいて、利用者のセキュリティ属性と利用者を代行して動作するサブジェクトとの関連付けを規定している。

F.APLACTL では、業務アプリケーションにおいて、旅券事務担当職員を代行するプロセスに役割情報を関連付けている。

したがって、FIA_USB.1 は、F.APLACTL によって満たされる。

・ FMT_MOF.1

FMT_MOF.1 では、セション管理機能のふるまいの決定や改変に影響を与える任意のタイミングによる手動セション切断管理を業務管理者に制限することを規定している。

F.SESMAN では、ログインユーザ一覧表示、セション切断の操作を、業務管理者に許可している。手動によるセション切断を行うことで、本来 10 分間の無応答状態により動作するセション切断機能を、10 分間待たずに任意のタイミングで利用することができ、セション管理機能のふるまいの決定や改変を行うことができる。

したがって、FMT_MOF.1 は、F.SESMAN によって満たされる。

・ FMT_MSA.2(a)

FMT_MSA.2(a)では、セキュアなセキュリティ属性を受け入れることを保証することを規定している。

F.SIGVER では、申請データに含まれる申請者電子証明書及び法定代理人証明書の有効期間、及び、JPKI が確認した失効ステータスの結果による電子証明書の失効状態の確認を行い、有効期間内かつ有効な電子証明書であることをチェックしている。

したがって、FMT_MSA.2(a)は、F.SIGVER によって満たされる。

・ FMT_MSA.2(b)

FMT_MSA.2(b)では、セキュアなセキュリティ属性を受け入れることを保証することを規定している。

F.CRYCOM では、SSL ハンドシェイクの完了時に、終了メッセージによりセションが成功したことを確認しているため、安全に HTTPS 通信を行うことができる。

したがって、FMT_MSA.2(b)は、F.CRYCOM によって満たされる。

・ FMT_MSA.2(c)

FMT_MSA.2(c)では、セキュアなセキュリティ属性を受け入れることを保証することを規定している。

F.CRYCOM では、SSL ハンドシェイクの完了時に、終了メッセージによりセションが成功したことを確認しているため、安全に HTTPS 通信を行うことができる。

したがって、FMT_MSA.2(c)は、F.CRYCOM によって満たされる。

・ FMT_MTD.1(a)

FMT_MTD.1(a)では、旅券事務担当職員のパスワード及び業務管理者を除く旅券事務担当職員の役割情報の改変を業務管理者に制限することを規定している。

F.USEMAN では、旅券事務担当職員のパスワード及び業務管理者を除く旅券事務担当職員の役割情報の変更操作を、業務管理者に許可している。

したがって、FMT_MTD.1(a)は、F.USEMAN によって満たされる。

・ FMT_MTD.1(b)

FMT_MTD.1(b)では、旅券事務担当職員のユーザ ID 及び役割情報の登録と削除を業務管理者に制限することを規定している。

F.USEMAN では、旅券事務担当職員のユーザ ID 及び役割情報の登録操作と削除操作を、業務管理者に許可している。

したがって、FMT_MTD.1(b)は、F.USEMAN によって満たされる。

・ FMT_MTD.1(c)

FMT_MTD.1(c)では、シグネチャの問い合わせ、改変を、旅券事務所システム管理者及び監視者に制限することを規定している。

F.INFMAN では、シグネチャの問い合わせ、変更操作を、旅券事務所システム管理者及び監視者に許可している。

したがって、FMT_MTD.1(c)は、F.INFMAN によって満たされる。

・ FMT_MTD.1(d)

FMT_MTD.1(d)では、監視者パスワードの改変を、旅券事務所システム管理者及び監視者に制限することを規定している。

F.INFMAN では、監視者パスワードの変更操作を、旅券事務所システム管理者及び監視者に許可している。

したがって、FMT_MTD.1(d)は、F.INFMAN によって満たされる。

・ FMT_MTD.1(e)

FMT_MTD.1(e)では、システム内時刻の問い合わせ、改変を、旅券事務所システム管理者に制限することを規定している。

F.INFMAN では、システム内時刻の問い合わせ、変更操作を、旅券事務所システム管理者に許可している。

したがって、FMT_MTD.1(e)は、F.INFMAN によって満たされる。

・ FMT_MTD.1(f)

FMT_MTD.1(f)では、旅券事務所システム管理者パスワードの改変を、旅券事務所システム管理者に制限することを規定している。

F.INFMAN では、旅券事務所システム管理者パスワードの変更操作を、旅券事務所システム管理者に許可している。

したがって、FMT_MTD.1(f)は、F.INFMAN によって満たされる。

・ FMT_SMF.1

FMT_SMF.1 では、表 5.4 に示されている一覧を管理する管理機能を規定している。

F.USEMAN では、旅券事務担当職員のユーザ ID、パスワード、役割情報を管理する管理操作を有している。

F.INFMAN では、シグネチャ、システム内時刻、旅券事務所システム管理者／監視者のパスワードを管理する管理操作を有している。

F.USEMAN 及び F.INFMAN の管理項目は、FMT_SMF.1 で規定した管理項目を過不足なく

再現している。

したがって、FMT_SMF.1 は、F.USEMAN 及び F.INFMAN によって満たされる。

・ FMT_SMR.1(a)

FMT_SMR.1(a)では、業務アプリケーションにおいて、業務管理者の役割を維持し、利用者を、その役割に関連付けることを規定している。

F.USEMAN では、業務アプリケーションにおける業務管理者の役割を、ユーザ ID に関連付けている。また、業務管理者の役割は、F.USEMAN によって維持されている。

したがって、FMT_SMR.1(a)は、F.USEMAN によって満たされる。

・ FMT_SMR.1(b)

FMT_SMR.1(b)では、インフラにおいて、旅券事務所システム管理者、監視者の役割を維持し、利用者を、その役割に関連付けることを規定している。

F.INFMAN では、インフラにおける旅券事務所システム管理者または監視者の役割を、ユーザ ID に関連付けている。また、旅券事務所システム管理者または監視者の役割は、F.INFMAN によって維持されている。

したがって、FMT_SMR.1(b)は、F.INFMAN によって満たされる。

・ FPT_RVM.1

FPT_RVM.1 では、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを規定している。

F.APLACTL では、業務アプリケーションを利用する際、ユーザ ID 及びパスワードの入力を促す画面を必ず表示し、その画面を迂回させないようにしている。そのため、業務アプリケーションを利用するには、旅券事務担当職員の識別認証が必ず行われる。また、識別認証後は、旅券事務担当職員を代行するプロセスに役割情報を割り当て、旅券事務担当職員アクセス制御方針を必ず実施する。割り当てられた役割情報は、ログアウトされるまで維持されている。

F.INFMAN では、インフラを利用する際、ユーザ ID 及びパスワードの入力を促す画面を必ず表示し、その画面を迂回させないようにしている。そのため、インフラを利用するには、旅券事務所システム管理者または監視者の識別認証が必ず行われる。また、識別認証後は、旅券事務所システム管理者または監視者を代行するプロセスに役割情報を必ず割り当てる。その情報は、ログアウトされるまで維持されている。

したがって、FPT_RVM.1 は、F.APLACTL 及び F.INFMAN によって満たされる。

・ FPT_SEP.1

FPT_SEP.1 では、信頼できないサブジェクトによる干渉及び改ざんから保護し、TSC 内のサブジェクト間分離を規定している。

F.APLACTL では、業務アプリケーションにログインすると、各旅券事務担当職員を代行するプロセスを割り当てる。割り当てられたプロセスは、他プロセスと分離しており、他プロセスからの干渉及び改ざんから保護される。

F.INFMAN では、インフラにログインすると、旅券事務所システム管理者または監視者を代行するプロセスを割り当てる。割り当てられたプロセスは、他プロセスと分離しており、他プロセスからの干渉及び改ざんから保護される。

したがって、FPT_SEP.1 は、F.APLACTL 及び F.INFMAN によって満たされる。

・ FPT_STM.1

FPT_STM.1 では、TSF が TSF 機能のために高信頼性タイムスタンプを提供することを規定している。

F.AUDIT では、監査事象を監査ログに記録するため、信頼できる時間を提供する。

したがって、FPT_STM.1 は、F.AUDIT によって満たされる。

・ FTA_SSL.3

FTA_SSL.3 では、利用者の動作がない時間が 10 分間に達した時、利用者との対話セションを終了することを規定している。

F.SESMAN では、旅券事務担当職員との対話で無応答時間が 10 分間に達した場合、旅券事務担当職員とのセションを強制的に切断する。

したがって、FTA_SSL.3 は、F.SESMAN によって満たされる。

・ FTP_ITC.1

FTP_ITC.1 では、TSF 自身と高信頼性 IT 製品間のチャネルデータを保護する高信頼性チャネルの提供を規定している。また、高信頼性チャネルは、申請データ取得機能、審査状態通知機能、公文書データ通知機能に適用され、TSF が通信を開始することを規定している。

F.CRYCOM では、HTTPS を用いることによって、汎用受付システムと TOE 間の通信データを盗聴及び改ざんから保護する。また、HTTPS 通信は、ユーザ ID 及びパスワード入力から接続が切断されるまで適用され申請データ取得機能、審査状態通知機能、公文書データ通知機能が汎用受付システムに接続要求を行うことによって確立され、通信確立後に送受信される通信データは保護される。

したがって、FTP_ITC.1 は、F.CRYCOM によって満たされる。

・ FTP_TRP.1

FTP_TRP.1 では、利用者と TSF 間の通信データを保護する高信頼性パスの提供を規定している。また、高信頼性パスは、最初の利用者認証から適用され、利用者が通信を開始することを規定している。

F.CRYCOM では、HTTPS を用いることによって、審査者端末と TOE 間の通信データを盗聴及び改ざんから保護する。また、HTTPS 通信は、ユーザ ID 及びパスワード入力から接続が切断されるまで適用され、審査者端末を介して旅券事務担当職員が TOE に接続要求を行うことによって確立される。

したがって、FTP_TRP.1 は、F.CRYCOM によって満たされる。

8.3.2. セキュリティ機能強度根拠

TOE は、業務利用制御機能で、パスワードによる認証を採用している。業務利用制御機能では、パスワード規則として、以下の内容を制御することで、強固なセキュリティを保証している。

パスワード長：６バイト～１２バイト

使用可能文字：数字（0～9)、英文字（a～z、A～Z)、記号（# $ ’ ( ) * + , - . / : = ? @ [¥] _ ` { } ~ !)

したがって、セキュリティ機能の強度は、低レベルの攻撃能力を持つ攻撃者に対して十分に対抗することができるため、SOF-基本が妥当であると判断できる。また、IT セキュリティ要件で主張した SOF-基本と一貫している。

8.3.3. 保証手段根拠

TOE セキュリティ保証要件のコンポーネントに対するエビデンスを表 6.8 に示す。

表 6.8 に示すように、「TOE セキュリティ保証要件」は全て「保証手段」に示されたドキュメントのセットにより対応づけられる。また、「保証手段」に示されたドキュメントにより、本 ST が規定したセキュリティ保証要件が要求する証拠を網羅している。これらのドキュメントを「TOE セキュリティ保証要件」に従って組織的に開発を実施することにより、保証要件が満たされる。

（　最終ページ　）