ＳＴ確認報告書

評価対象

申請受付年月日(受付番号)	平成16年7月14日（ST確認4033）
確認番号	V022
ＳＴ確認申請者	エヌ・ティ・ティ・コミュニケーションズ株式会社
ＳＴの名称	外務省　旅券申請審査システムセキュリティターゲット
ＳＴのバージョン	第1.05版
ＰＰ適合	なし
適合する保証要件	ASE（ST評価）クラス （TOEの保証パッケージはEAL2＋AVA_MSU.1）
ＳＴ開発者	エヌ・ティ・ティ・コミュニケーションズ株式会社
評価実施機関の名称	社団法人　電子情報技術産業協会　ITセキュリティセンター

上記のSTについての評価は、以下のとおりであることを確認したので報告します。
平成16年12月10日

独立行政法人 情報処理推進機構
セキュリティセンター情報セキュリティ認証室
技術管理者　田渕　治樹

評価基準等：「セキュリティターゲットの確認業務実施規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0210

評価結果：合格

「外務省　旅券申請審査システムセキュリティターゲット」は、独立行政法人 情報処理推進機構が定めるセキュリティターゲットの確認業務実施規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

このST確認報告書は、「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」（以下「本ST」という。）について社団法人　電子情報技術産業協会　ITセキュリティセンター（以下「評価実施機関」という。）が行ったセキュリティ評価に対し、その内容の確認結果を申請者であるエヌ・ティ・ティコミュニケーションズ株式会社に報告するものである。

本ST確認報告書の読者は、本書とともに、対応する本ST[1]を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、本STにおいて詳述されている。

本ST確認報告書は、本STに対する確認結果を示すものであり、対応するTOEのいかなる実装についても言及していないことに留意されたい。

1.2 評価製品

1.2.1 製品名称

本STが対象とする製品は、以下のとおりである。なお、TOEの正確な範囲は、1.2.3節で定義される。

- 名称:　　旅券申請審査システム
- バージョン　1.0
- 開発者:　　外務省

1.2.2 製品概要

TOE(旅券申請審査システム)は、地方公共団体における旅券申請の審査サービス（申請の審査、審査結果の決裁及び公文書の発行）を行うソフトウェアのパッケージ製品である。

本製品は、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。

1.2.3 TOEの範囲

旅券申請及び発給に係わるシステムの全体は、「図1 旅券の申請及び発給に係わる全体のシステム構成」に示すとおり、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。

TOEは旅券申請及び発給に係わるシステムに含まれる旅券申請審査システムであり、TOE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。

① 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。

② 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。

③ 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

④ 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。

⑤ 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。

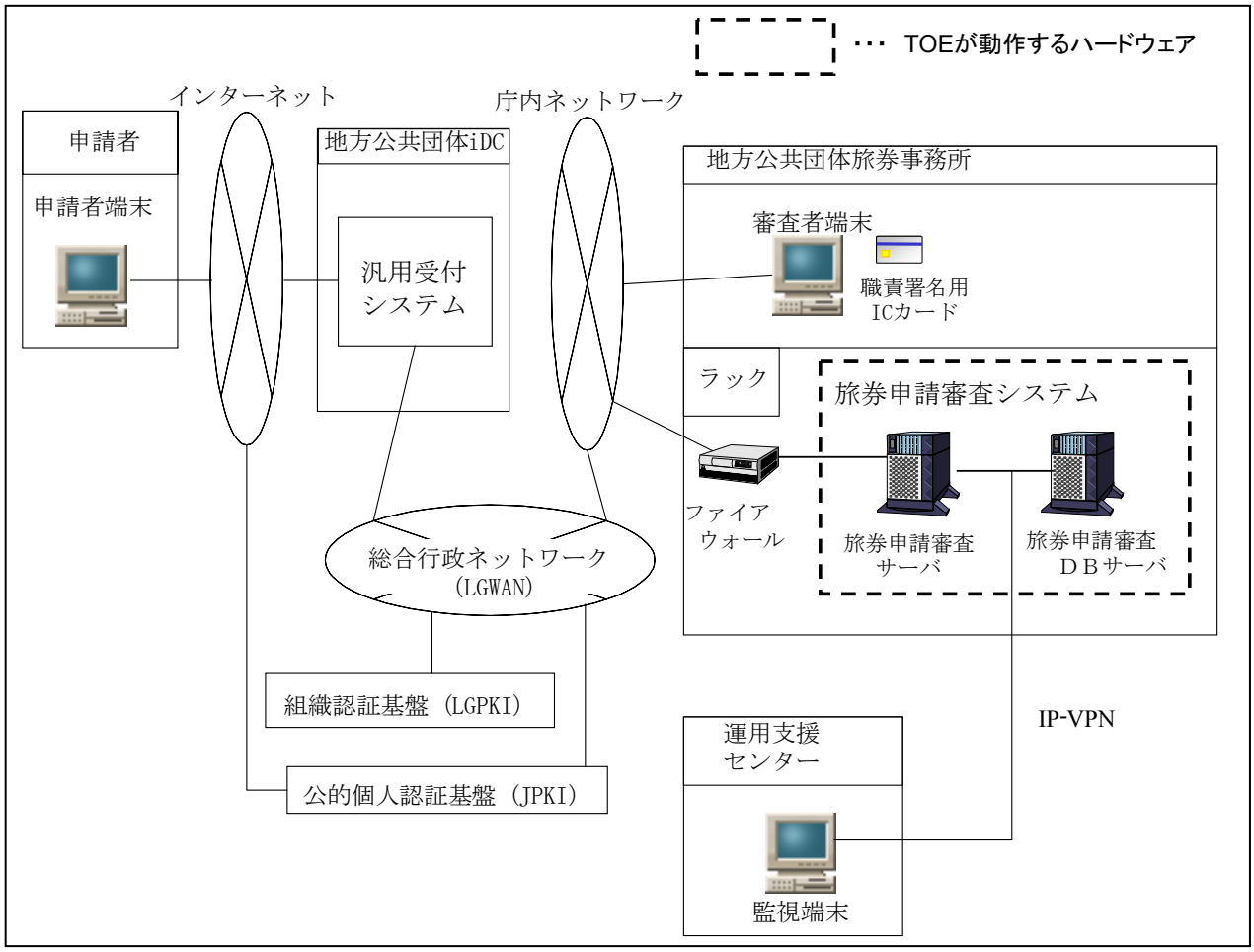

図1　旅券の申請及び発給に関わる全体のシステム構成

図1の全体のシステムの構成に関する説明を以下に示す。

- 申請者
  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。

- 地方公共団体iDC（インターネットデータセンター）
  地方公共団体が管理し、汎用受付システムが導入されている。

- 汎用受付システム
  住民や企業からインターネットを通して提出される電子的な申請届出等の受付や行政機関からの電子的結果通知等、複数の手続きができるシステム。

- 庁内ネットワーク
  地方公共団体のネットワークであり、総合行政ネットワーク に接続している。

- 総合行政ネットワーク（LGWAN）
  各地方公共団体が接続しているネットワーク。

- 地方公共団体旅券事務所
  TOEとTOEを利用するための審査者端末が導入されている。

- 旅券申請審査システム
  TOE。旅券審査サーバ、旅券審査DBサーバ上で稼動するソフトウェアであり、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の物理的なアクセスを禁止するため、施錠可能なラック（図中、「ラック」）内に設置される。

- 運用支援センター
  外務省から監視業務を委託されている。TOEから通知されるアラートを監視するための監視端末が設置されている。

- 組織認証基盤（LGPKI）
  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。

- 公的個人認証基盤（JPKI）
  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。

1.2.4 TOEの動作概要

(1) 業務サービスの概要

旅券申請システム全体の業務サービスの概要を以下に示す。

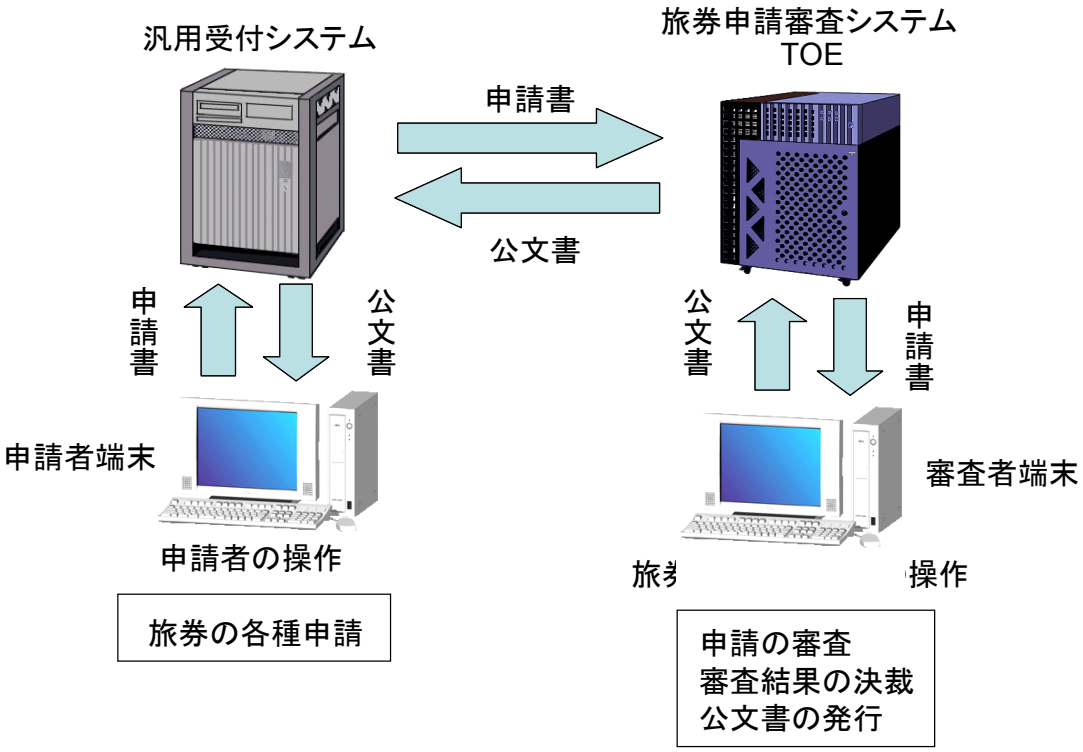

図2　旅券の申請システム全体のサービスの概要

旅券事務担当職員は、審査者端末を介してTOEが提供する以下のサービスを利用する。

- 申請の審査
  申請者から送られてくる申請書を審査する。
- 審査結果の決裁
  審査した内容について決裁する。
- 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）に係るいずれかを発行する。

(2) TOEの機能

TOE は、以下に示す業務アプリケーションの機能と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ソフトウェアなどのソフトウェア（以下、「インフラ」）の機能によって、審査サービスを提供する。ソフトウェアの構成については、「2　TOE構成」を参照。

(A) 業務アプリケーションの機能

(a) 申請の審査、審査結果の決裁に関する機能

- 申請データ取得機能
  汎用受付システムに格納されている申請データを取得する。
- 申請データ表示機能
  指定された申請データを検索し、審査者端末に表示する。
- 申請データ削除機能
  指定された申請データを検索し、削除する。
- 結果登録機能
  作成された審査情報を登録する。
- 署名検証機能
  申請データの正当性及び完全性を検査するため、署名を検証する。
- 証明書検証機能
  申請者証明書及び法定代理人証明書の有効性を検査する。
- 本人性確認機能
  本人性を確認するために証明書の情報と申請書の情報とを比較し、その比較結果を審査者端末に表示する。
- 写真／自署取込み機能
  申請者から写真及び自署が郵送された場合、申請データとして登録する。
- 状態通知機能
  各審査業務に応じて生成された状態情報を汎用受付システムに通知する。

(b) 公文書の発行に関する機能

- 公文書表示機能
  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内容を表示する。
- 署名付与機能
  公文書データを生成し、署名（職責署名用IC カードで生成された職責署名）を付与する。
- 公文書データ通知機能
  署名機能により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。

(c) その他

- 業務利用者制御機能
  利用者である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。また業務アプリケーションの利用制限を行うために役割に基づくアクセス制御を行う。
- 業務管理機能
  ユーザID、パスワード、役割情報の登録、変更及び削除を行う。これらの操作を業務管理者のみに制限する。
- セション管理機能
  審査者端末との間のセションを管理し、定められた時間内に審査者端末から応答がない場合に切断する。

(B)インフラの機能

・管理作業の識別認証及びアクセス制御機能
利用者であ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。

・システム管理機能
時刻変更及び参照を旅券事務所システム管理者に制限する。また、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旅券事務所システム管理者及び監視者に制限する。

・暗号化通信機能
汎用受付システム間及び審査者端末間の通信データの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
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監査ログを記録し、閾値越えの事象も記録する。記録された監査ログは、その参照を制限する。また、セキュリティ侵害の可能性を検出し、監視端末にアラートを通知する。

なお、TOEは上記機能のうち「署名検証機能」、「証明書検証機能」、「業務利用者制御機能」、「業務管理機能」、「セション管理機能」、「管理作業の識別認証及びアクセス制御機能」、「システム管理機能」、「暗号化通信機能」及び「監査機能」は、セキュリティ機能を保有し、TOEの入出力情報である申請データ、審査データ、公文書データ、及び審査サービスを遂行するために必要な管理データを保護する。

(3) TOEの利用方法

本TOEの関係者を以下に示す。

・ 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。

・ 旅券事務所システム管理者

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。

・ 交付担当者

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。

・ 旅券作成検査担当者

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

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

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。
- 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。

1.3 評価実施

「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」のセキュリティ評価は、認証機関が運営するITセキュリティ評価・認証プログラムに基づき、「セキュリティターゲットの評価・確認申請等の手引き」[2]、「セキュリティターゲット 評価実施機関に対する要求事項」[3]、「セキュリティターゲットの確認申請者・登録者に対する要求事項」[4]に規定された内容に従い、評価実施機関によって実施された。

本評価の目的は、申請者から提出された本ST[1]が、CCパート1([5])附属書C、CCパート2([6])の機能要件及びCCパート3([7])のASEクラスの規定を満たしており、セキュリティ機能設計の基本文書として技術的に妥当なものであるかどうかを評価することである。ただし、ASEクラスの規定の中で、TOE評価と関連する要求事項については、評価の項目に含まれていない。なお、評価方法は、CEMパート2([17])に準拠する。また、CC及びCEMの各パートは補足（[21]）の内容を含む。

認証機関は、評価実施機関が実施するSTの評価を監督し、ST評価が所定の手続きに沿って行われたことを確認した。評価は、平成16年11月の評価実施機関による「外務省　旅券申請審査システムセキュリティターゲット　評価報告書 第1.2版 2004年11月26日」の提出をもって完了し、同報告書に基づき、認証機関は本ST確認報告書を作成した。

1.4 報告概要

1.4.1 PP適合

適合するPPはない。

1.4.2 EAL

本STが規定するTOEの評価保証レベルは、EAL2追加である。
追加する要件は、AVA_MSU.1。

1.4.3 セキュリティ機能強度

本STにおいてTOEに要求される最小機能強度レベルは、SOF-基本である。

1.4.4 セキュリティ機能

本STで扱うTOEのセキュリティ機能は以下のとおりである。

- 業務利用制御機能
  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。

- セション管理機能
  TOE と審査者端末間で確立されたセション状態を管理し、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。

- 旅券事務担当職員管理機能
  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。

- 暗号化通信機能
  汎用受付システムとTOE 間、審査者端末とTOE 間の通信データに対し、HTTPSを用いた通信を行い、盗聴及び改ざんから保護する。
  （暗号化通信機能として、DES、3DES、RC4、RSA、MD5、SHA-1の暗号アルゴリズムを利用する。）

- 申請データ検証機能
  申請証明書、法定代理証明書に対し、含まれている公開鍵を用いた、申請証明書、法定代理証明書の署名の検証と、証明書有効性を確認するため、有効期限と失効されていないことの確認をする。

- 監査機能
  業務アプリケーション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。また、記録された監査事象及び監査ログ領域の管理を行う。

- インフラ利用管理機能
  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う。また、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判断する基準である重要度（シグネチャ）、システム内時刻の管理を行う。

1.4.5 脅威

TOEは、表1に示す脅威を想定し、本製品は、これに対抗する機能を備える。

表1　想定する脅威

識別子	内容
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。

1.4.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表2に示す。

表2　組織のセキュリティ方針

識別子	内容
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、インフラの使用において、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。

1.4.7 構成条件

本TOEが必要とする各サーバの構成条件は、以下のとおりである。

表3　旅券申請審査サーバのハードウェア構成

種別	説明
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 3ポート 100/1000　Ethernetカード　1ポート
ディスプレイ接続用グラフィックカード	PGX64フレームバッファ
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	SonicWALL　SSL-R

表4　旅券申請審査DBサーバのハードウェア構成

種別	説明
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
ディスプレイ接続用グラフィックカード	PGX64フレームバッファ
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)
DATオートローダ装置用カード	デュアルチャネルUltraSCSIカード
DBサーバ共用ディスク接続用カード	ファイバーチャネルカード
ストレージ装置（RAID5）	ETERNUS3000モデル50 165GB 10,000rpm

1.4.8 動作環境の前提条件

TOEを使用する環境において有する前提条件を表5に示す。

これらの前提条件が満たされない場合、TOEのセキュリティ機能が有効に動作することは保証されない。

表5　TOE使用の前提条件

識別子	内容
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。

1.5 ST確認に関わる注意事項

ST確認は、CCで規定された評価の全過程から、ST評価の部分だけを抜き出した評価に基づいて行われるものである。したがって、ST評価を規定したASEクラスの要件の中で、TOE評価と関連する事項についてはST評価の対象になっていない。また、ASEクラス以外の保証クラスに属する事項、例えば、STの記載事項がそのとおりに設計されTOEに実装されているかどうか、TOEに悪用可能な脆弱性が残っていないかどうか、あるいはTOEの製造・配付が安全な手続きに基づいて行われているかなども評価の範囲外である。これら評価対象外の事項については確認も行われていないことに、本報告書の読者は留意すべきである。

ST確認は、TOEに対する、潜在的なものを含めたあらゆるセキュリティ上の脅威が完全に対策されていることを保証するものではない。評価完了後にTOEやそのIT環境にあらたな脅威が発見される可能性は常に考慮されるべきであり、TOE利用者は、TOEに関わる最新のセキュリティ関連情報に継続的な注意を払うことが必要である。

STの中で前提条件として記述されたものは、TOEを安全に使用する上での必須事項である。これらの条件が満たされないと、TOEのセキュリティ機能は、期待される効果を発揮することができない。前提条件を満たすためのTOEの安全な運用管理は、TOE利用者の責務である。

本ST確認報告書は、認証機関が該当するTOEを保証し、その使用を推奨することを意図したものではない。

2 TOE構成

旅券申請審査サーバ及び旅券申請審査DBサーバ上で稼動するTOEを構成する業務アプリケーション及びインフラについて、ソフトウェアの詳細を以下に示す。

表6　旅券申請審査サーバ上で稼動するソフトウェア

製品名	備考
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

表7　旅券申請審査DBサーバ上で稼動するソフトウェア

製品名	備考
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
NetWorker Auto Changer Software	バックアップソフトウェア

Module 6.1.3.Build.428	
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

3 評価実施機関による評価結果

評価は、CCパート3のASEクラスの規定に基づき、CEMパート2に規定された評価方法を用いて行われた。評価作業の詳細は、ST評価報告書[20]において報告されている。ST評価報告書には、TOEの概要説明、CEMパート2のワークユニットごとの評価内容及び判断が記載されている。各ワークユニットの評価作業において発見された問題点及びその対処の経過・結果も記載されている。

評価実施機関が評価中に発見した問題点は、すべて、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

総合判定は、「合格」である。

4 結論

4.1 ST確認実施

認証機関は、評価の過程で評価実施機関より提出される各資料をもとに、以下の確認を実施した。

① 評価実施機関が評価作業中に指摘した所見報告書の内容が妥当であること。

② 所見報告書でなされた指摘内容が正しくSTに反映されていること。

③ 提出されたSTの内容を確認し、関連する評価者アクションエレメントが本評価報告書で示されたように評価されていること。

④ 本評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 本評価報告書に示された評価者の評価方法がCEMに準拠していること。

これらの確認において発見された問題事項を認証レビューとして記載し、評価実施機関に送付した。

認証機関は、本STにおいて、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4.2 ST確認結果

提出されたST評価報告書及び所見報告書を調査した結果、認証機関は、本STがCCパート3に規定されたASEクラスの保証要件を満たしていることを確認した。

評価実施機関の実施した各評価者アクションエレメントについての調査結果を表4にまとめる。

表8　評価者アクションエレメント調査結果

評価者アクションエレメント	調査結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が明記され、それらが脅威、組織のセキュリティ、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が理路整然とし、完結しており、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。

ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が理路整然とし、完結しており、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完結しており、理路整然とし、かつ一貫していることを確認している。

4.3 注意事項

SSLを用いた暗号化通信は、TOEがサポートする暗号アルゴリズム（DES、3DES、RC4、RSA、MD5、SHA-1）と、クライアント側がサポートする暗号アルゴリズムによって決定される。従って、TOEと通信するHTTPSのクライアント間において、電子政府推奨暗号リスト[23]にないDES、MD5が選択されることがあるため、注意が必要である。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation

本報告書で使用された用語の定義を以下に示す。

HTTPS	Hypertext Transfer Protocol Security : Webサーバとクライアントがデータを送受信するのに使用されるHTTPにSSLによるデータの暗号化機能を付加したプロトコル。
SSL	Secure Sockets Layer：TCP層とアプリケーション層の間に位置するNetscape社が開発したプロトコル層。証明書による認証機能と通信データの暗号化機能を持つ。
申請データ	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審査サーバを経由し、旅券審査DBサーバに登録される。
審査データ	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（審査情報）、旅券事務担当者がメモや注意事項として入力する情報（官公庁記載情報）、旅券担当事務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（審査状態情報）、及び申請に対する審査の進捗を管理する情報（状態通知情報）の総称である。
公文書データ	公文書構成管理情報及び公文書の総称である。公文書構成管理情報とは、公文書データの構成を示した情報（公文書管理情報）、公文書管理情報、公文書に関する署名に必要な情報（公文書署名情報）、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（署名情報）及び職責署名用IC カードから取り出された電子証明書（職責証明書）の総称である。また公文書とは、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	担当者情報及び事務所情報の総称。業務サービスが正常に動作するために必要なデータ。
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	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	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。
汎用受付システム	住民や企業からインターネットを通して提出される電子的な申請届出等の受付や行政機関からの電子的結果通知等についての複数の手続きができるシステムである。
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。
庁内ネットワーク	地方公共団体のネットワークであり、総合行政ネットワークに接続している。
組織認証基盤（LGPKI）	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。
公的個人認証基盤（JPKI）	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。
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。

6 参照

[1] 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

[2] セキュリティターゲットの評価・確認申請等の手引き 平成16年4月 独立行政法人 情報処理推進機構 ITQM-21

[3] セキュリティターゲット 評価実施機関に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-13

[4] セキュリティターゲットの確認申請者・登録者に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-12

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] 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

[9] 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

[10] 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

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 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

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] 外務省　旅券申請審査システムセキュリティターゲット　評価報告書 第1.2版 2004年11月26日 04ITSC-E039-02　社団法人 電子情報技術産業協会 ITセキュリティセンター

[21] CCIMB Interpretations-0210

[22] 補足-0210

[23] 電子政府推奨暗号リスト 平成15年2月20日　総務省／経済産業省