# ＳＴ確認報告書

評価対象

| | |
|---|---|
| **申請受付年月日（受付番号）** | **平成**15**年** 6**月**20**日**（ST**確認**3026） |
| **ＳＴ確認申請者** | **株式会社　日立製作所** |
| **ＳＴの名称** | PKI Management Program **セキュリティターゲット** |
| **ＳＴのバージョン** | **第1.1版** |
| **ＰＰ適合** | **なし** |
| **適合する保証要件** | ASE（ST**評価**）**クラス**<br>（TOE**の保証パッケージは**EAL3+ADV_SPM.1） |
| **ＳＴ開発者** | **株式会社　日立製作所　ソフトウェア事業部** |
| **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 7月21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 ISO/IEC 15408:1999 Information technology - Security techniques - Evaluation criteria for IT security
② JIS X 5070(2000) セキュリティ技術 ― 情報技術セキュリティの評価基準
③ Common Criteria for Information Technology Security Evaluation Version 2.1
④ 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
⑤ Common Methodology for Information Technology Security Evaluation Version1.0
⑥ 認証機関が公開する③及び⑤の翻訳文書

**評価結果：合格**

「PKI Management Program 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。

その他：なし

# 目次

# 1 全体要約

## 1.1 はじめに

このST確認報告書は、「PKI Management Program セキュリティターゲット第1.1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株式会社日立製作所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:　PKI Management Program
- バージョン:　Windows版：02-04-/A
  Solaris(TM) Operating Environment版：02-04
- 開発者:　株式会社日立製作所

### 1.2.2 製品概要

本製品は、PKIシステムを構築するための基本製品であり、登録局（RA）の機能を提供するソフトウェア製品である。

また、本製品は認証局（CA）の機能を提供する製品と連携して、証明書の発行・失効申請を審査する等、一般利用者とCAの間において証明書の管理を行う。

### 1.2.3 TOEの範囲

本TOEは、図1で示される環境下で動作する。また、図中の太枠内で示される4つのコンポーネントがTOEである。

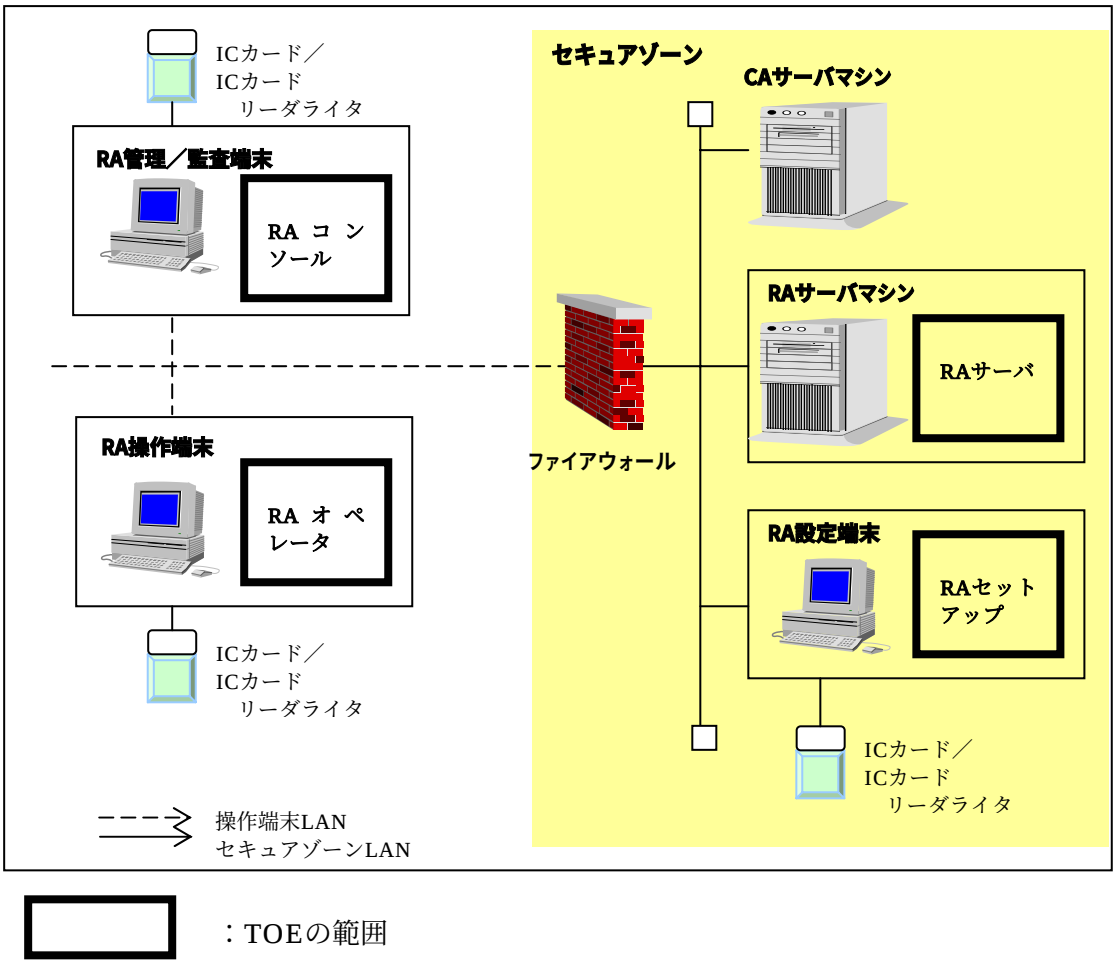


**図1　TOEの動作環境**

図中示される各エンティティは、以下に定義される。

- セキュアゾーン

  TOE の運用に関わるシステム管理者及び他のサーバマシン管理者だけが入室可能であり、外部とはファイアウォールを介してのみ接続される、物理的、接続的に隔離・管理された空間のこと。

- セキュアゾーン LAN

  セキュアゾーン内の LAN。RA サーバマシン、CA サーバマシン及び RA 設定端末が接続される。

- 操作端末 LAN

  セキュアゾーン外で運用に関わる操作端末が接続される LAN。
- RA サーバマシン

  PKI Management Program のサーバシステムであり、RA 管理／監査端末及び RA 操作端末からの要求を受け付け、それに対応した処理を行う。TOE のコンポーネントのうち RA サーバが動作するサーバであり、RDBMS といった RA サーバが稼動するために必要なソフトウェアも動作する。
- RA 設定端末

  システム管理者が操作する端末であり、RA サーバの初期設定、RA 管理者、監査者の登録を行う。RA サーバのシステム管理者が、RA サーバの設定等を行うための端末である。TOE のコンポーネントのうち RA セットアップが動作する。
- CA サーバマシン

  CA の機能を提供する製品のサーバシステムであり、RA サーバからの証明書の発行、失効要求を受け付け、証明書の発行及び失効を行う。
- RA 管理／監査端末

  RA 管理者、または監査者が操作する端末であり、RA サーバの運用環境の設定、監査を実施する。TOE のコンポーネントのうち RA コンソールが動作する。
- RA操作端末

  RA操作者が、RAサーバへアクセスし、RAサーバの操作を行うための端末である。一般利用者の証明書の発行、失効の操作を行う。また、発行された証明書の取得を行う。TOEのコンポーネントのうちRAオペレータが動作する。

### 1.2.4 TOEの動作概要

(1) TOEの論理的構成

図 2 に、TOE の論理的な構成を示す。

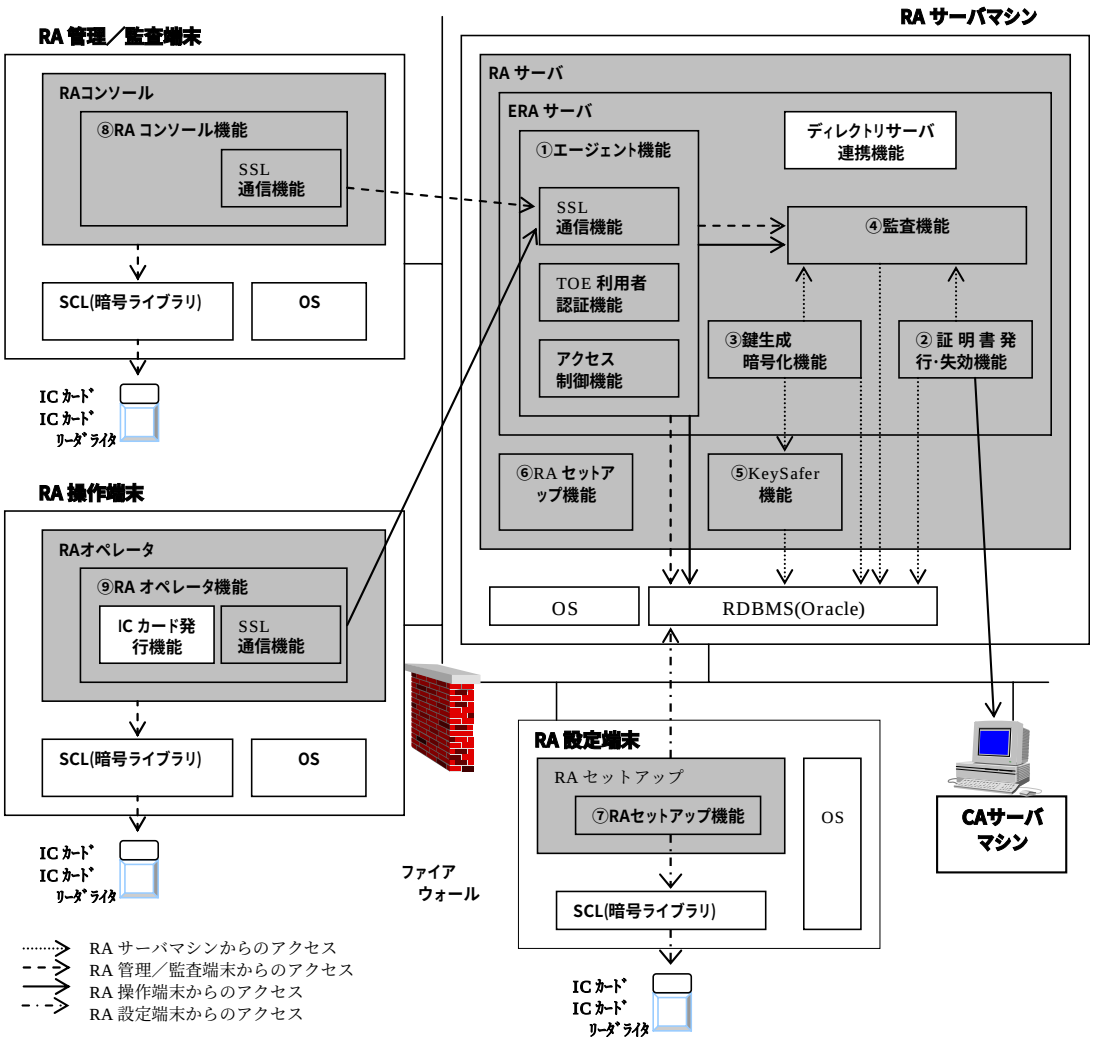


**図2　TOEの論理的構成**

**① エージェント機能**

RA コンソール、RA オペレータからの操作要求（運用環境の設定／証明書発行申請・失効申請等）を受け付ける機能。各端末の操作者（オペレータ）の識別認証、各端末との暗号通信（SSL）、操作者毎の操作の制御も行う。

**② 証明書発行／失効機能**

CA サーバに証明書の発行・失効を依頼する機能。発行された証明書のデータベースへの格納も行う。

**③ 鍵生成／暗号化機能**

鍵ペアの生成、PKCS#12・PIN の暗号化を行う機能。

④ **監査機能**

RA サーバで実行された操作を記録し、管理する機能。

⑤ KeySafer **機能**

鍵生成／暗号化機能で生成された鍵ペア、暗号化された PKCS#12、PIN をデータベースで管理する機能。

⑥ RA **セットアップ機能（**RA **サーバ）**

RA セットアップにて生成された RA 動作環境情報をインポートする機能。

⑦ RA **セットアップ機能（**RA **セットアップ）**

RA サーバの各種設定、環境情報を生成する機能。生成された設定等をエクスポートする機能も有する。

⑧ RA **コンソール機能**

RA サーバのクライアントとして機能し、RA サーバのエージェント機能を通じて RA の運用管理機能、監査機能を提供する。

⑨ RA **オペレータ機能**

RA サーバのクライアントとして機能し、RA サーバのエージェント機能を通じて RA の証明書操作機能（証明書の発行申請、発行審査、失効申請、失効審等)、監査機能を提供する。

(2) TOEの利用方法

本TOEの運用に関連する利用者として以下が定義されている。それぞれの利用方法について以下に示す。

- TOE を運用する組織の責任者
  システム管理者、RA管理者、RA操作者、監査者が属する組織の責任者。TOEのセキュアな運用に対する責任を持つ。
- システム管理者
  TOEを運用する組織に属し、RAサーバの環境を構築する。RAサーバのインストール、初期設定、起動、停止を行う。オペレーティングシステム、データベースの管理者でもある。
- RA 管理者
  TOEを運用する組織に属し、RA管理／監査端末を使用してRAサーバの運用環境設定を行う。
- 監査者
  TOEを運用する組織に属し、RA管理／監査端末を使用してRAサーバの監査機能を利用し、監査ログの表示、検索、検証、削除を行う。
- RA 操作者
  TOEを運用する組織に属し、RA操作端末を使用して証明書の発行、失効の申請、審査、証明書の取得等の操作を行う。RA操作者は複数人存在し、複数のRA操作者の合議に基づいて申請、審査を行う。

## 1.3 評価実施

PKI Management Program セキュリティターゲットのセキュリティ評価は、認証機関として運営するITセキュリティ評価・認証プログラムに基づき、公表文書「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14年4月)」[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 (平成14年4月)」[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 (平成14年4月)」[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][8][11][14]のいずれか)附属書C、CCパート2（[6][9][12][15]のいずれか）の機能要件及びCCパート3（[7][10][13][16]のいずれか）のASEクラスの規定を満たし、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][18][19]のいずれか）に準拠する。

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7月の評価実施機関による「ST評価報告書 第1.0版 2004.7.7」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、EAL3追加である。
追加する要件はADV_SPM.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

TOEは、以下のセキュリティ機能を有する。

- **監査ロギング機能**
  RAサーバで実行された操作の記録を監査ログとして記録する機能である。

- **監査ログ参照機能**
  監査ロギング機能で記録した監査ログの内容を参照する機能である。

- **監査ログ検証機能**
  監査ロギング機能で記録した監査ログの完全性と連続性を検証する機能である。

- **監査ログ削除機能**
  監査ロギング機能で記録した監査ログを削除する機能である。

- **オペレータ識別認証機能**
  RAコンソール、及びRAオペレータからのログイン要求受け付け時に、RAサーバより実施されるオペレータの識別認証機能である。識別認証の方式は、ユーザID／パスワードによる識別認証と、証明書による識別認証がある。

- CA**識別認証機能**
  RAサーバからCAへの証明書の発行、失効要求時に、あらかじめRAサーバに登録されたCAとの接続だけを許可するための識別認証機能である。

- **アクセス制御機能**
  オペレータ（RA管理者、監査者、RA操作者）のアクセス権限を管理する機能である。

- **状態フロー制御機能**
  鍵･証明書の状態遷移を管理する機能である。RA操作者からの鍵･証明書の発行、失効、取得、削除要求を受け、鍵・証明書の状態を適切に遷移させる。

- **暗号化機能（暗号化）**
  TSC内のデータを暗号化するための鍵を生成し、データの暗号化を行う機能である。また、使用済みとなった鍵の廃棄を行う。

- **暗号化機能（パスワードメカニズム）**
  パスワードを表1のパスワード仕様により検証する機能である。

**表1　パスワードメカニズム**

| パスワード名 | パスワード仕様 |
|---|---|
| RAサーバの起動パスワード | ASCIIコードの0x20～0x07Eを６文字以上14文字以下 |
| オペレータ登録情報のパスワード | ASCIIコードの0x20～0x07Eを4文字以上8文字以下 |
| オペレータ登録用ログインパスワード | 10バイトの乱数 |

- **暗号化機能（暗号鍵シードメカニズム）**
  暗号鍵シードを表2のシード仕様により生成または検証する機能である。

**表2　鍵生成時に使用するシード**

| シード名 | シード仕様 |
|---|---|
| 監査ログ暗号化シード | ASCIIコードの0x20～0x07Eを4文字以上8文字以下 |
| RAサーバの鍵・証明書暗号化シード | 15バイトの乱数 |

- **暗号通信機能**
  TOEを構成するコンポーネント間の通信データを暗号化及びアクセス制御で保護する機能である。SSLを使用して通信データの暗号化、復号及び通信データの改ざん検出を行う。

- **管理機能**
  各情報にアクセスするために使用するセキュリティ属性を管理する機能である。

### 1.4.5 脅威

TOEは表3に示す脅威を想定し、これに対抗する機能を備える。

**表3　想定する脅威**

| 識別子 | 脅威 |
|---|---|
| T.DATA_CORRUPTED（TOEデータの毀損） | システム管理者によるTOE外の機能の誤操作で、RA動作環境情報が削除、または変更される。 |
| T.DATA_REMOVED（TOEデータの削除） | RA管理者、または監査者によるTOEの機能の誤操作で、RA管理情報、監査ログが削除される。 |
| T.UNAUTH_TOE_ACCESS（TOEへの不正アクセス） | TOEに登録されたオペレータ以外の者が、RAコンソール、またはRAオペレータを使用し、TOEが提供する機能でRA管理情報、監査ログ、一般利用者鍵・証明書を利用する。 |
| T. UNAUTH _OPERATION（許可されない操作） | オペレータが自らに与えられた権限外の操作を行うことにより、TOEの運用上許可されないTSC内データの作成、変更、削除、エクスポートが行われる。 |
| T.INVALID_OPERATION（不正操作） | RA操作者が故意、または誤操作により、自らの権限内で、TOEの運用上許可されない鍵・証明書の発行、取得、失効、削除を行う。 |
| T. INVALID_TERMINAL _ACCESS（端末への不正アクセス） | TOEを運用する組織に属する者のうち、悪意を持つ者が、直接または操作端末LANを介してRA管理／監査端末、RA操作端末にアクセスし、以下の行為を行う。<br>・TSC内のデータを削除、または変更する。<br>・TSCからエクスポートされ、RA操作端末からアクセス可能な状態にある一般利用者鍵・証明書を不正に利用する。 |
| T.INTERCEPTION（盗聴） | TOEを運用する組織に属する者のうち、悪意を持つ者により、RA管理／監査端末、RA操作端末とRAサーバ間の送受信データが盗聴される。 |

### 1.4.6 組織のセキュリティ方針

本TOEは、表4に示す組織のセキュリティ方針に従う機能を備える。

**表4　組織のセキュリティ方針**

| 識別子 | 組織のセキュリティ方針 |
|---|---|
| P.OS_IA（OSによる識別認証） | TOEが動作する上で必要となるすべてのマシンのOSは識別認証機能を持ち、あらかじめ登録された利用者のログインのみを許可する。 |
| P.OS_ACCESS_CONTROL（OS によるアクセス制御） | TOEが動作する上で必要となるすべてのマシンのOSはアクセス制御機能を持ち、識別された利用者によるOSが管理する資源への許可されないアクセスを抑止する。 |
| P.DOMAIN_SEPARATION（OSによるドメイン分離） | TOEが動作する上で必要となるすべてのマシンのOSはドメイン分離機能を持ち、TSF、及びIT環境により提供される全てのセキュリティ機能が他の機能の干渉（破壊）を受けないことを保証する。 |
| P.CA_RELIABILITY（CAの信頼性） | TOEは、CAへの証明書発行・失効要求に際してCAの識別認証を行い、要求先のCAがあらかじめ登録された信頼できるCAであることを確認する。 |
| P.CIPHER（秘密データの暗号化） | TSC内に存在する鍵、パスワード等の秘密データを暗号化する。 |
| P.AUDIT_INVISIBLE（監査ログの不可視性） | 監査ログの内容は、TOE外の機能による参照を不可能にする。 |

### 1.4.7 構成条件

本TOEは、表5～表8で示されるハードウェア、OS上で動作する。また同表に示されるソフトウェアとともに動作する。

**表5　TOE（RAサーバ）の動作に必要なハードウェア、ソフトウェアの諸条件**

| | 種類 | 説明 |
|---|---|---|
| Windows版 | CPU | Intel PentiumIII 500MHz相当以上 |
| | メモリ | 256MB以上 |
| | ディスク | 250MB以上 |
| | OS | Microsoft® Windows® 2000 Server（サービスパック3以上を適用） |
| | データベース | Oracle8i Release 8.1.7（Oracle8.1.7.2パッチを適用）またはOracle9i Release 9.2.0 |
| | その他ソフトウェア | Securecrypto Libraryランタイム V1.0L52 |
| | | S/MIME&EE Certificate Management Package V3.1L16 |
| Solaris OE版 | CPU | UltraSPARC-II 400MHz相当以上 |
| | メモリ | 512MB以上 |
| | ディスク | 250MB以上 |
| | OS | Sun Microsystems, Inc.Solaris (TM) 8 Operating Environment（106327-08以上、106300-09以上、107058-01以上、106748-04以上、108528-10以上） |

| | 種類 | 説明 |
|---|---|---|
| | データベース | Oracle8i Release 8.1.7（Oracle8.1.7.2パッチを適用）またはOracle9i Release 9.2.0 |
| | その他ソフトウェア | Securecrypto Library RunTime 1.4 |
| | | S/MIME & EE Certificate Management Package 3.1.6 |

**表6　TOE（RAセットアップ）の動作に必要なハードウェア、ソフトウェアの諸条件**

| 種類 | 説明 |
|---|---|
| CPU | Pentiumプロセッサー200MHz　以上 |
| メモリ | 128MB以上 |
| ディスク | 34MB以上 |
| カードリーダライタ | HX-360MJ（RS-232C手動挿入手動排出タイプ・カードリーダライタ）<br>HX-500UJ（USB 手動挿入手動排出タイプ・カードリーダライタ） |
| OS | Microsoft® Windows® 2000 Professional（サービスパック3以上を適用） |
| データベース | Oracle8i Release 8.1.7（Oracle8.1.7.2パッチを適用）またはOracle9i Release 9.2.0 |
| その他ソフトウェア | Securecrypto Libraryランタイム V1.0L52 |
| | S/MIME & EE Certificate Management Package V3.1L16 |

**表7　TOE（RAコンソール）の動作に必要なハードウェア、ソフトウェアの諸条件**

| 種類 | 説明 |
|---|---|
| CPU | Pentiumプロセッサー200MHz　以上 |
| メモリ | 128MB以上 |
| ディスク | 55MB以上 |
| カードリーダライタ | HX-360MJ（RS-232C手動挿入手動排出タイプ・カードリーダライタ）<br>HX-500UJ（USB 手動挿入手動排出タイプ・カードリーダライタ） |
| OS | Microsoft® Windows® 2000 Professional（サービスパック3以上を適用） |
| その他ソフトウェア | Securecrypto Libraryランタイム V1.0L52 |
| | S/MIME & EE Certificate Management Package　V3.1L16 |

**表8　TOE（RAオペレータ）の動作に必要なハードウェア、ソフトウェアの諸条件**

| 種類 | 説明 |
|---|---|
| CPU | Pentiumプロセッサー200MHz　以上 |
| メモリ | 256MB以上 |
| ディスク | 56MB以上 |
| カードリーダライタ | HX-360MJ（RS-232C手動挿入手動排出タイプ・カードリーダライタ）<br>HX-500UJ（USB 手動挿入手動排出タイプ・カードリーダライタ） |
| OS | Microsoft® Windows® 2000 Professional（サービスパック3以上を適用） |
| その他ソフトウェア | Securecrypto Libraryランタイム V1.0L52 |
| | S/MIME & EE Certificate Management Package　V3.1L16 |

### 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9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9　TOE使用の前提条件**

| 識別子 | 前提条件 |
|---|---|
| ASM.ACCESS（アクセスの物理的制限） | RAサーバ、RA設定端末はセキュアゾーンに設置される。セキュアゾーンの入室時には物理鍵や認証システムを必要とし、セキュアゾーンへの入室はセキュアゾーンに設置される各マシンの管理者だけが許可される。各マシン管理者に許可された者がメンテナンス等のためにセキュアゾーンに入室する場合もあるが、必ず各マシン管理者の監視下で作業を行う。 |
| ASM.CLIENT_ACCESS（クライアントアクセスの物理的制限） | RA管理／監査端末、RA操作端末には、TOEを運用する組織に属する者だけが物理的にアクセスできる。 |
| ASM.MEDIA_PROTECT（媒体の物理的保護） | TOE内にあるデータのバックアップが保管された媒体は、適切な手順に従って管理、保管され、物理的な破壊、及び盗難から保護されている。 |
| ASM.OPERATOR_PROTECT（オペレータ秘密鍵の物理的保護） | オペレータの鍵・証明書は耐タンパー性のあるICカードに格納され、ICカード盗難時にも物理的な攻撃による秘密鍵の暴露、不正使用から保護される。 |
| ASM.ADMIN（システム管理者・RA管理者・監査者・他サーバの管理者の信頼性） | システム管理者、RA管理者、監査者はTOEを運用する組織に属し、TOEを運用する組織の責任者によって任命される。<br>システム管理者、RA管理者、監査者、他サーバの管理者は、それぞれの役割を果たす上で必要となる知識を習得するための教育を施される。<br>システム管理者、RA管理者、監査者、他サーバの管理者は、それぞれに課せられた役割に対して、許可された一連の行為に関する悪意を持った行為は行わず、システムの運用に協力的に関わる。 |
| ASM.OPERATOR（RA操作者の信頼性） | RA操作者はTOEを運用する組織に属し、TOEを運用する組織の責任者によって任命される。<br>RA操作者はRA操作者としての役割を果たす上で必要となる知識を習得するための教育を施される。 |
| ASM.CONNECT（接続制限） | セキュアゾーンLANはファイアウォールを介して操作端末LANにのみ接続される。<br>操作端末LANにはTOEを運用する組織に属する者だけがアクセスできるよう物理的に保護される。また、操作端末LANがTOEを運用する組織外のネットワークに接続される場合は、TOEを運用する組織外のネットワークから操作端末LANに対してアクセスできないよう、操作端末LANはファイアウォールにより保護される。<br>操作端末LANからRAサーバへのアクセスは、RA管理・監査端末及びRA操作端末からRAサーバの特定のポートに対してのみ接続可能であるよう、セキュアゾーンLAN－操作端末LAN間のファイアウォールにより制限される。 |
| ASM.RELIABILITY（TOE構成要素の信頼性） | TOEが動作する上で必要となるハードウェア及びソフトウェアは、システム管理者、RA管理者、監査者、RA操作者により適切にインストール、設定し管理される。 |
| ASM.CA_RELIABILITY（CAの信頼性） | TOEが証明書の発行・失効要求を行うCAは信頼できるCAのみであり、これらのCAはセキュアゾーンLANに接続される。 |

| | |
|---|---|
| ASM.OTHER_RELIABILITY（その他のマシンの信頼性） | セキュアゾーンに設置されるTOE構成要素外のハードウェア及びソフトウェアは、他サーバマシン管理者により適切に設定し管理される。 |
| ASM.IMPORTED（インポートデータの信頼性） | TSCにインポートされる鍵・証明書は、セキュアゾーンLANに接続されたCAにより発行されたものである。<br>TSCにインポートされる利用者データは、暴露・盗難・改ざんから保護するため、関連者により適切に管理される。 |
| ASM.EXPORTED（エクスポートデータの保護） | TSCからエクスポートされた鍵・証明書を含む利用者データは、暴露・盗難・改ざんから保護するため、関連者により適切に管理される。 |
| ASM.CLIENT_RESTORE（クライアント環境の復元） | RA管理・監査端末、またはRA操作端末上のTSC内データが毀損され、RAコンソール、またはRAオペレータが正常に動作しなくなった場合、各端末を使用するオペレータは、自身の責任でTOEの再インストール、及び再設定を行う。 |
| ASM.PASSWORD（パスワード及びPINの管理） | TOE利用者がTOEを使用する際に必要となるパスワード及びPINは、TOE利用者本人によって適切に管理され、本人以外のものに知られることはない。<br>パスワード及びPINは類推が困難であり、適切な頻度で変更される。 |

## 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

PKIシステムは図3に示すとおり、RAの機能を提供する製品(TOE)であるPKI Management Programと、CAの機能を提供する製品から構成される。

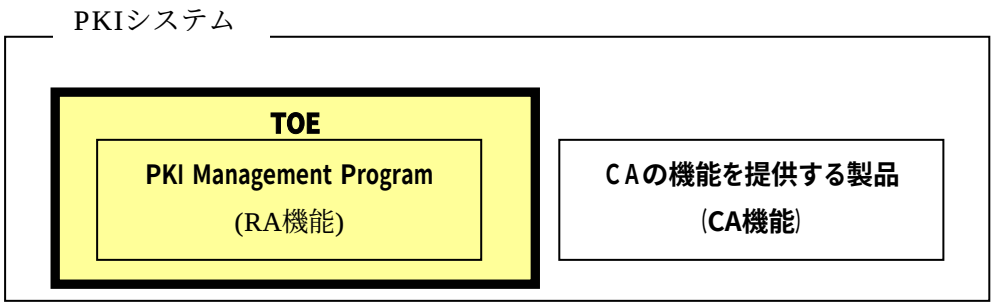


**図3　PKIシステムの構成**

またPKI Management Programは、RAサーバ、RAセットアップ、RAコンソール、RAオペレータの４つのコンポーネントにより構成される。これらのコンポーネントは、それぞれRAサーバマシン、RA設定端末、RA管理／監査端末、RA操作端末上で動作する。（『図１　TOEの動作環境』参照）

- RA サーバ
  RAオペレータからの証明書発行・失効申請を受け付けてCAに渡すと同時に、それぞれの申請の詳細情報を管理する。

- RA セットアップ
  RAサーバの動作環境設定を行う。

- RA コンソール
  RAサーバのクライアントとして動作し、RAサーバの運用管理等を行う。

- RA オペレータ
  RA サーバのクライアントとして動作し、RA サーバに対して証明書の発行・失効申請等を行う。

# 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、全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

確認は、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検証した結果、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確認結果を表10にまとめる。

**表10　評価者アクションエレメント確認結果**

| 評価者アクションエレメント | 確認結果 |
|---|---|
| **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。 |
| 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。 |
| 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。 |

| | |
|---|---|
| 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概説が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。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。 |

## 4.3 注意事項

特になし。

# 5 用語

本報告書で使用された略語・一般用語を以下に示す。

| | | |
|---|---|---|
| **鍵ペア** | ： | 公開鍵暗号における、対となる公開鍵と秘密鍵の組のことである。 |
| **公開鍵** | ： | 公開鍵暗号方式で使用される鍵ペアのうち、一般に公開される鍵。 |
| **公開鍵暗号** | ： | 暗号化と復号に、対となる別の鍵(公開鍵、秘密鍵)を使用する暗号技術のことである。 |
| **証明書** | ： | X.509に従い発行した公開鍵証明書。公開鍵証明書は利用者の公開鍵を保証するために、CAがディジタル署名をしたもの。 |
| **秘密鍵** | ： | 公開鍵暗号方式で使用される鍵ペアのうち、一般に公開されない鍵。 |
| **CA** | ： | Certification Authority：認証局。利用者の公開鍵に対してディジタル署名を行い、証明書を発行する。またCRLを発行する。 |
| **CC** | ： | Common Criteria：コモンクライテリア。 |
| **EAL** | ： | Evaluation Assurance Level：評価保証レベル。 |
| **PKCS** | ： | Public Key Cryptography Standards：RSA Securityが開発した公開鍵暗号方式の業界標準。<br>● PKCS#7 は S/MIME 用にキーや証明書を扱えるようにした規格で、ASN.1 記述の証明書の格納や、署名、MIME 形式における記述法などを定めたものである。<br>● PKCS#8 は、鍵の格納を定めたものである。<br>● PKCS#12 は、PKCS#7 証明書と PKCS#8 秘密鍵のファイル化を行ったものである。 |
| **PIN** | ： | PKCS#12ファイルにアクセスするためのパスワードである。 |
| **PKI** | ： | Public Key Infrastructure：公開鍵暗号方式によるセキュリティ基盤。 |
| **PP** | ： | Protection Profile：プロテクションプロファイル。 |
| **RA** | ： | Registration Authority：登録局。証明書の発行や失効の申請を審査する等、一般利用者とCAの間において証明書管理を行う。 |
| **RDBMS** | ： | Relational DataBase Management System：「リレーショナルデータモデル」によりデータを管理するデータベース管理システム。 |
| **SOF** | ： | Strength of Function：機能強度。 |
| **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であり、サーバ・クライアント間における双方向の証明書による認証、暗号通信を可能にする。 |
| **ST** | ： | Security Target：セキュリティターゲット。 |
| **TOE** | ： | Target Of Evaluation：評価対象。 |
| **TSF** | ： | TOE Security Functions：TOEセキュリティ機能。 |
| **X.509** | ： | ITU-T （ International Telecommunication Union-Telecommunication sector）が勧告した証明書とCRLの標準仕様。（ITU-TはITU（国際電気通信連合）の下部組織であり、通信関係の標準化を担当。） |

# 6 参照


[1] PKI Management Program セキュリティターゲット　第1.1版　2004年7月5日 株式会社日立製作所

[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14年4月 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

[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14年4月 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 適合－部門－ST評価要求－02

[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14年4月 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 適合－部門－ST申請要求－02

[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] PKI Management Program セキュリティターゲット（第1.1版） 評価報告書 2004年7月7日 第1.0版 03ITSC-E023 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