ＳＴ確認報告書

評価対象

申請受付年月日(受付番号)	平成14年5月31日（ST確認2008）
ＳＴ確認申請者	日本電気株式会社
ＳＴの名称	PKI**サーバ**／Carassuit **電子政府版** Version2.0 **セキュリティターゲット バージョン** : 2.1
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EAL3）
ＳＴ開発者	NEC**ソリューションズインターネットソフトウェア事業部**
評価実施機関の名称	電子商取引安全技術研究組合研究所

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１４年１２月２０日

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管理課情報セキュリティ室
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.
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
⑥ 認証機関が公開する③および⑤の翻訳文書

評価結果：合格

PKIサーバ／Carassuit 電子政府版 Version2.0 セキュリティターゲット バージョン ：2.1は、独立行政法人製品評価技術基盤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サーバ／Carassuit 電子政府版 ver2.0 セキュリティターゲット バージョン 2.1」（以下「本ST」という。）について電子商取引安全技術研究組合研究所（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日本電気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ST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、STにおいて詳述されている。

本ST確認報告書は、当該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サーバ／Carassuit 電子政府版 ver2.0
- 開発者: 日本電気株式会社

1.2.2 製品概要

本製品は、PKI (公開鍵基盤) 用のCA (認証局) / RA (登録局)を構成するためのソフトウェアである。製品は、CAサーバ用、CAクライアント用、RA操作用の3種類のソフトウェアからなり、各々が異なったPC (パーソナルコンピュータ) に搭載され、全体として、CA/RAの機能を提供する。

CAとしての主な機能は、EE (一般利用者) の公開鍵に対する公開鍵証明書発行、失効リスト (証明書失効リスト/機関失効リスト) 発行、機関証明書 (下位CA証明書及び相互認証証明書) 発行、CA自身の公開鍵証明書公開、及び公開鍵証明書保管である。RAとしての主な機能は、証明書申請要求の受付、及び証明書発行・失効に伴う資格審査である。

1.2.3 TOEの範囲

TOEは、PKIサーバ／Carassuit 電子政府版 ver2.0 ソフトウェアであり、CAサーバ用、CAクライアント用、RA操作用の3種類からなる。3種類のソフトウェアは、各々異なったPCに搭載されるアプリケーションプログラムであり、所定のOS (オペレーティングシステム) 、DBMS (データベース管理システム) などのプログラム上で動作する。これらTOEソフトウェアを搭載したPCは、CAサーバ端末、CAクライアント端末、RA操作端末と呼ばれる。各端末には、必要に応じてICカードリーダ/ライタ (操作員証明書や秘密鍵を格納したICカード用) が接続され、さらに、CAサーバ端末には、

HSM (ハードウェアセキュリティモジュール; CA秘密鍵を生成・管理する装置) が接続される。各端末は、LANで相互接続され、全体として一つの製品としての機能を提供する。このように、本TOEは、物理的に分離された3つのパーツから構成される分散型TOEである。TOEとTOEに関わるソフトウェア、ハードウェアの構成を図1-1に示す。図中のハッチされた部分がTOEに相当する。TOEが提供する機能は、「0 1.2.2 製品概要」に概要が記載され、「0 1.2.4 TOEの動作概要」に詳細な説明が記載されている。

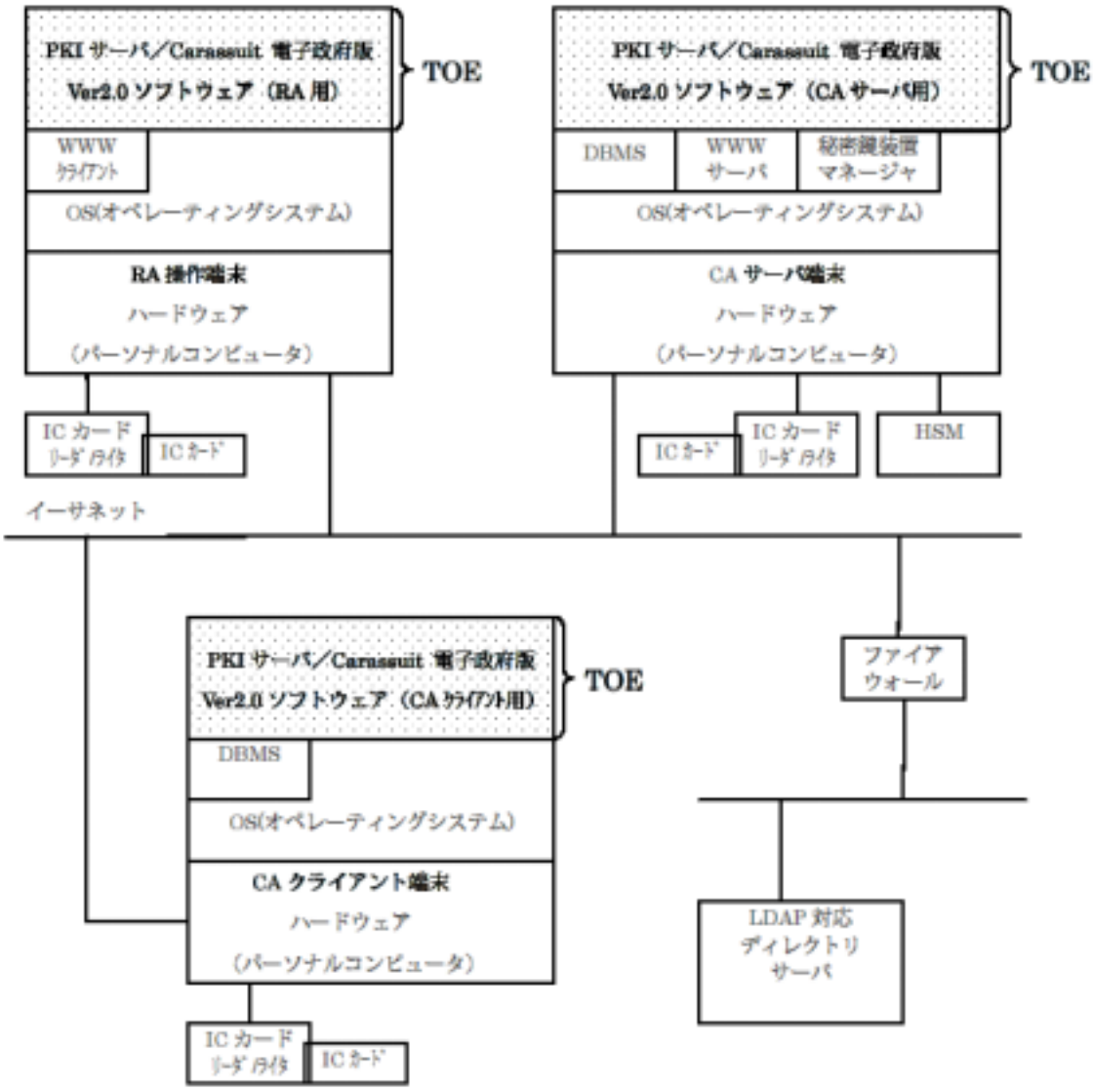

図1-1　　PKIサーバ／Carassuit 電子政府版 ver2.0 アーキテクチャ

1.2.4 TOEの動作概要

TOEは、CA/RAとしての機能を提供する。具体的には、一般利用者から証明書申請要求を受け、公開鍵証明書、失効リスト、機関証明書を生成・発行・保管し、LDAPディレクトリで公開する。また、証明書発行・失効に伴う資格審査を行う。これらの機能を果たすため、管理運用に関わる以下の機能を併せ持つ: 監査機能、バックアップ/リカバリ機能、アーカイブ機能、アクセスコントロール機能、操作員管理機能、ユーザ管理機能、ポリシー管理機能、スケジュール管理機能、システム環境設定機能。

以下、機能の詳細リストを示す。

【CA/RAの主な機能】

CA:

・EEの公開鍵に対する公開鍵証明書発行
・失効リスト発行
・機関証明書 (下位CA証明書及び相互認証証明書) 発行
・CA自身の公開鍵証明書公開
・公開鍵証明書保管

RA:

・証明書申請要求の受付
・証明書発行・失効に伴う資格審査

【TOEの管理運用に関わる機能】

・監査機能

セキュリティ保持上必要となる監査情報の採取と管理を行う。具体的な監査対象データは、ST[1]に詳述されている。

・バックアップ/リカバリ機能

DB (データベース) 内データのバックアップ及びリカバリを行う。TOE障害時のデータ損失に対応する。

・アーカイブ機能

TOEが発行した証明書、鍵の履歴を管理する。

・アクセスコントロール機能

操作員のTOEへのアクセスを管理する。管理の第一段階は、TOEへのログイン管理、第二段階は、操作員が属する権限グループ[1]に付与された属性に基づくTOE内オブジェクトへのア

[1] **操作員には、上級操作員と一般操作員の二つの種別があり、それぞれ、上級操作員権限グループ、一般操作員権限グループに所属する。**

クセス管理である。

ログイン管理: 操作員は、あらかじめTOEに登録された操作員IDによって識別される。識別された操作員の認証メカニズムとして、パスワード方式あるいはICカード方式が使用される。パスワードとICカードの使い分けは、TOEを使用する組織の管理運用方針に依存する。TOEは、CAサーバ、CAクライアント、RA操作の3つのパーツに分かれており、各パーツごとに、操作員の種別と適用される認証メカニズムが異なっている。それぞれの対応関係を表1-1に示す。

表1-1　　TOEのパーツ・操作員種別・認証メカニズムの対応関係

TOEのパーツ	操作員種別	認証メカニズム
CAサーバ	上級操作員	パスワード
CAクライアント	一般操作員	パスワードあるいはICカードに格納された秘密鍵と証明書(PIN認証を併用)
RA	一般操作員	パスワードあるいはICカードに格納された証明書(PIN認証とWWWサーバによるSSL認証を併用)

アクセス管理: TOEにログインした操作員がどのデータにアクセスできるかは、操作員が属する権限グループに付与されるアクセス権限によって決まる。権限グループへのアクセス権限付与の権限も同じメカニズムによって制御されるので、この権限は、十分に信頼できる権限グループに与えられねばならない。下位の権限グループに属する操作員は、アクセス権限を上位の権限グループに変更する権限を持たない。セキュリティ上重要ないくつかのアクセス権限の設定・変更については、2名の操作員の協働を必要とする操作方法設定も可能で、操作員のミスや不正の抑止効果が期待できる。

・操作員管理機能

操作員 (上級及び一般) の登録、削除、情報管理及び権限グループの管理を行う。権限グループには、上級操作員権限グループ及び一般操作員権限グループの2種類の権限グループ種別が定義されており、各々、上級操作員、一般操作員が所属する。上級操作員は、上級操作員と一般操作員両方の権限の管理が可能だが、一般操作員は、一般操作員の権限に対してだけ、管理が可能である。

・ユーザ管理機能

EEの秘密鍵、個人情報を管理する。EE鍵の鍵ペア生成、保管も行う。

・ポリシー管理機能

証明書プロファイル、証明書失効リストプロファイルの設定、変更を行う。

・スケジュール管理機能

失効リスト発行に関わるスケジュール管理を行う。

・システム環境設定機能
TOEの運用に必要な情報を設定する。

1.3 評価実施

PKIサーバ／Carassuit 電子政府版 Version2.0 セキュリティターゲット バージョン : 2.1のセキュリティ評価は、独立行政法人製品評価技術基盤機構が独立した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って実施された。

本評価の目的は、申請者によって提出された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。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、評価実施機関である電子商取引安全技術研究組合研究所が実施する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14年10月31日の評価実施機関によるST評価報告書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である。

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。

・SF.Audit

TOEがセキュアに運用されていることを監査するため、あらかじめ定めた監査対象事象を監査データとして採取し、保存する。

本STの機能要件には、FAU_GEN.1 (監査データ生成) が含まれているが、CCの監査要件として機能要件コンポーネントごとに規定された監査対象事象の一部が除外されている。CCの監査要件に含まれているが本STで監査対象から除外された事象は、以下のものである。

- FAU_SAR.1 [監査記録からの情報の読み出し]
- FAU_SAR.3 [閲覧に使用されるパラメタ]
- FAU_STG.3 [閾値を超えたためにとられるアクション]
- FIA_SOS.1 [TSFによる、テストされた秘密の拒否]
- FPT_STM.1 [時間の変更]

これらの事象について、監査対象に含めずともセキュリティ上の問題が生じない理由がST[1]の「8.2.6 監査対象事象根拠」に説明されている。しかしながら、これらの事象が監査データから除外されることで、例えば、監査ログ検査者が監査記録を端末画面上で閲覧したり、監査記録をあるパラメタに基づいてソートしたりしても、そのふるまいが監査記録に残らない。あるいは、パスワードやPIN設定時に、規定された品質尺度を満たさないためにTSFが拒否した場合のふるまいが記録に残らない。TOEの管理運用に責任を持つ者は、監査データに関し、このような内容を理解しておくべきである。

・SF.ACC

データを格納したTOE内オブジェクトに対してアクセス制御を行う機能であるが、ユーザデータに対するアクセス制御機能だけでなく、TSFデータであるセキュリティ属性に対する管理機能も含まれる。 (CC機能要件で定めるアクセス制御よりも広い機能範囲を含む。) 管理機能の詳細は、ST[1]第6章を参照のこと。

・SF.I&A

上級操作員、一般操作員に対して、個人の識別及びパスワードあるいはICカードによる認証を行う。ログインする端末の種類、操作員種別によって異なる識別・認証メカニズムが適用される。各々の対応関係は、表1-1に示すとおりである。

・SF.Crypto

TOEは、セキュリティ上の目的を達成するため、種々の暗号機能を使用する。使用する暗号名称 (アルゴリズム) と用途を表1-2に示す。

・SF.Cer_Issue

TOEは、発行する証明書及び失効リストに対して、自らが発行したことの証拠情報を付与する。そのために、対象となる証明書及び失効リストのCA署名フィールドに、TOEのCA鍵を用いて作成した署名を格納する。

表1-2　　使用する暗号機能

暗号アルゴリズム	鍵長	用途
RSA (PKCS#1)	2048bit	CA鍵（鍵ペア） • EE証明書、機関証明書、失効リストの署名 • 操作員証明書及びデータ保護証明書の署名及び署名検証
RSA (PKCS#1)	1024bit	操作員秘密鍵（鍵ペア）
RSA (PKCS#1)	1024bit	EE鍵（鍵ペア）
RSA (PKCS#1)	1024bit	データ保護鍵（鍵ペア） • 監査データ、アーカイブデータの署名及び署名検証
Triple DES (FIPS PUB 46-3)	168bit	システム共通鍵 • アクセス制御に関わるセキュリティ属性、監査データ、アーカイブデータ、鍵管理DB用パスワード、LDAPサーバパスワードの暗号化・復号
Triple DES (FIPS PUB 46-3)	168bit	鍵管理DB共通鍵（共通鍵） • EE証明書に対応する秘密鍵、データ保護鍵の暗号化・復号
Triple DES (FIPS PUB 46-3)	168bit	EE ICカード発行情報ファイル保護鍵（共通鍵） • EE ICカード発行情報ファイルの暗号化・復号
SHA-1 MD5	160bit 128bit	ハッシュ値の生成・検証 • 識別・認証情報 • アクセス制御に関わるセキュリティ属性 • システムパラメータ

1.4.5 脅威

TOEが想定する脅威は、以下に示すとおりである。これらの脅威によって生じる資産へのリスクは、TOEによる対抗手段によって、安全なレベルまで軽減される。

・T.ILLEGAL_LOGON（不正なログオン）

高度な専門知識を持たない不正な利用者が不正にTOEにログオンしてTOEを利用することにより、利用者データ及びTSFデータを破壊・改ざん・暴露するかもしれない。

・T.UNAUTHORIZED_ACCESS（不正なアクセス）

TOEの正当な利用者が許可されていない操作を行うことにより、利用者データ及びTSFデータを破壊・改ざん・暴露するかもしれない。

・T.MODIFY_DB_DATA（DBデータ改ざん）

高度な専門知識を持たない不正な利用者が利用者データ及びTSFデータを保存したデータベースに直接アクセスすることにより、その利用者データ及びTSFデータを改ざん・暴露するかもしれない。

・T.DISCLOSE_ICC_FILE（EE ICカード発行情報ファイル暴露）

高度な専門知識を持たない不正な利用者がCAクライアント端末もしくはRA操作端末に保管さ

れたEE ICカード発行情報ファイルに直接アクセスすることにより、EE ICカード発行情報ファイルを暴露するかもしれない。

・T.DISCLOSE_NW_DATA（ネットワークデータ暴露）
　高度な専門知識を持たない不正な利用者がCAサブシステムとデータベース間及びWWWサーバとWWWクライアント間のネットワーク上でやりとりされるTSFデータ及び利用者データを暴露するかもしれない。

1.4.6 組織のセキュリティ方針

TOEに適用される組織のセキュリティ方針は、以下のとおりである。これら組織のセキュリティ方針のうち、P.ISSUEとP.AUTHORITYは、TOEによって対処される (P.AUTHORITYは、管理運用上の手続きによる対処も併用)。P.AUDITORは、管理運用上の手続きによって対処される。P.CA_PRIVATE_KEYとP.OS_DBは、IT環境の機能によって対処される。

・P.ISSUE（発行）
　TOEにより提供されるCAは、自らが発行する証明書（EE証明書、機関証明書、失効リスト）が確かに当該認証局から発行されたことを要求者が確認する手段を提供しなければならない。

・P.AUTHORITY（権限付与）
　権限を与えられたもののみが与えられた権限の範囲でシステム操作を行うことができる。

・P.AUDITOR (監査ログ検査者)
　監査ログ検査者は、他の権限を持てない。

・P.CA_PRIVATE_KEY（認証局秘密鍵）
　TOEによって使われる認証局秘密鍵は、FIPS PUB 140-1、PKCSに従って生成・破棄・操作される。

・P.OS_DB（信頼できるOS/DB）
　TOEのソフトウェアコンポーネント (TOEプログラム、DBMS、WWW サーバ、秘密鍵装置マネージャ) の盗難・破壊・改ざんを防ぐため、TOEの動作に必要となるOS・DBは、識別認証機能を適切に実施できるものでなければならない。さらに、OSは、信頼できない利用者による干渉と改ざんからTOEを保護するためのセキュリティドメインを維持できなければならない。

1.4.7 構成条件

TOEは、CAサーバ、CAクライアント、RA操作の3つのパーツからなり、それぞれが異なるハードウェア (パーソナルコンピュータ: PC) に搭載される。TOE各パーツが搭載されたPCは、それぞれ、CAサーバ端末、CAクライアント端末、RA操作端末と呼ばれる。各端末のソフトウェア/ハードウェアに対する構成条件は、表1-3のとおりである。

表1-3　TOE**の構成条件**

TOE/**端末**	**ソフトウェア条件**	**ハードウェア条件**
CA**サーバ端末**	• OS: Microsoft Windows NT 4.0 Server Service Pack 6**あるいは**Windows 2000 Server • WWW**サーバ**: Microsoft Internet Information Server Version 4 (Option Pack) **あるいは**Version 5 • DBMS: Oracle8i (R8.1.7)	• **本体**: Express5800**シリーズ** • CPU: Pentium II 200MHz**以上** • **メモリー**: 128MB**以上** • **ハードディスク**: 2GB**以上**
CA**クライアント端末**	• OS: Microsoft Windows NT 4.0 Server Service Pack 6**あるいは**Windows 2000 Server • DBMS：Oracle8i (R8.1.7)	• **本体**: Express5800:**シリーズ** • CPU: Pentium III 500MHz**以上** • **メモリー**:128MB**以上** • **ハードディスク**: 2GB**以上**
RA**操作端末**	• OS: Microsoft Windows NT 4.0 Workstation Service Pack 6**あるいは**Windows 2000 Professional • WWW **クライアント**: Microsoft Internet Explorer 5.5 **あるいは**6.0	• **本体**: Express5800**シリーズ、**PC/AT**互換機** • CPU: Pentium II 200MHz**以上** • **メモリー**: 96MB**以上** (128MB **以上推奨**)

各端末には、ICカードリーダ/ライタが接続され、CAサーバ端末には、さらにHSMが接続される。ICカードリーダ/ライタ、HSMの構成条件、及びICカードリーダ/ライタで使用するICカードの構成条件は、以下のとおりである。

・ICカードリーダ/ライタ

GemPC410 (RC-232C接続タイプ; Gemplus製)

・HSM

CK-Guard IIあるいはCK-Guard III (NEC製)

・ICカード

Standard-9 (NEC SecureWare用STD-9; 大日本印刷製)

1.4.8 **動作環境の前提条件**

TOEの使用方法、使用環境に関わる前提条件を以下に示す。TOEのセキュリティ機能が有効に動作するためには、これらの前提条件が満たされていなければならない。

・A.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）：

上級操作員及び一般操作員がTOEにアクセスするために用いるパスワードは、他人に知られないように本人によって管理される。パスワードは推測・解析されにくいものが設定され、適正な間隔で変更される。

・A.PIN_ICC_MANAGEMENT（一般操作員によるPIN・ICカードの管理）：
　一般操作員がTOEにアクセスするために用いるICカードは不正利用されないよう管理され、ICカード内のデータを使用するためのPINは他人に漏洩しないように本人によって管理される。PINは推測・解析されにくいものが設定され、適正な間隔で変更される。

・A.SAFE_PLACE（安全な場所）：
　TOEに関連するハードウェアは、物理的に不正侵入できないように制御された場所に設置される。

・A.BACKUP_MEDIA（バックアップ媒体）：
　TOEのバックアップデータが保存されたリムーバブル媒体は、物理的に不正侵入できないように制御された場所に保管され、不正に持ち出せないように管理される。

・A.USER_RESTRICTION（利用者制限）：
　TOEに直接アクセスする利用者は、管理者（上級操作員、一般操作員、監査ログ検査者、RA 操作員）だけである。

・A.NETWORK (ネットワーク環境) :
　TOEの内部ネットワークは、それ以外のネットワークに直接接続されない。

・A.HSM（HSM）：
　HSMで生成・管理される認証局秘密鍵は、物理的に保護される。

・A.HARDWARE (ハードウェア) :
　TOEに関連するハードウェアは、正確に動作する。

・A.PERIPHERAL_INTERFACE（周辺装置）：
　TOEに接続する周辺機器は、TOEの付近に設置される。TOEと周辺機器は、その間で盗聴されることがないように直接接続される。

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どうかなども評価範囲外である。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

TOEの全体構成と、TOEを構成するコンポーネントについて詳細に説明する。TOEは、CAサーバ、CAクライアント、RA操作の3つのソフトウェアパーツから構成され、全体としてCA/RAサービスを提供する。以下に、各パーツの構成と機能を述べる。

【CAサーバ】

CAサーバは、以下のサブ機能からなる。

・CAサーバコンソール機能:

管理者がCAサーバを操作するためのインタフェースであるGUI (グラフィカルユーザインタフェース) を提供する。これには、以下のツールが含まれる。

- CAセットアップツール
- CA鍵・証明書更新ツール
- 自己署名証明書失効ツール
- DBセットアップツール
- DBパスワード変更ツール
- バックアップツール
- リカバリツール
- ユーザ管理ツール
- サービス監視ツール

・CAサブシステム機能:

CAサービスを提供する機能群である。これを構成する個々の機能は、以下のとおりである。

- CAメイン機能
- RAメイン機能
- 監査データ管理機能
- バックアップ/リカバリ機能
- アーカイブ機能
- アクセスコントロール機能
- 操作員管理機能
- ユーザ管理機能
- ポリシー管理機能
- スケジュール管理機能
- システム環境設定機能

・CGIモジュール機能:

CAサブシステム機能を呼び出し、EE証明書申請・審査・検索・出力・失効処理を行う。

・鍵管理DB API機能:

DB内の鍵データにアクセスする。

・ICカード管理機能:
ICカードのリード/ライトを行う。

・PKCS#11モジュール機能:
HSMを利用するため、TOE外機能である秘密鍵装置マネージャにアクセスする。

【CAクライアント】

CAクライアントの構成は、以下のサブ機能からなる。

・CAクライアントコンソール機能:
CAクライアントのGUIを提供する。

・CAサブシステム機能:
CAサーバで説明したCAサブシステム機能と同じである。

・鍵管理DB API機能:
DB内の鍵データにアクセスする。

・ICカード管理機能:
ICカードのリード/ライトを行う。

【RA操作】

RA操作は、以下のサブ機能からなる。

・RAコンソール機能:
EE証明書申請要求登録、証明書受取、証明書検索、証明書生成要求、ICカード書込要求を行う。

・ICカード管理機能:
ICカードのリード/ライトを行う。

以上のTOE構成を図2-1に示す。太線で囲まれた部分がTOEに相当し、それ以外のものは、TOEの動作に関わるTOE外機能である。

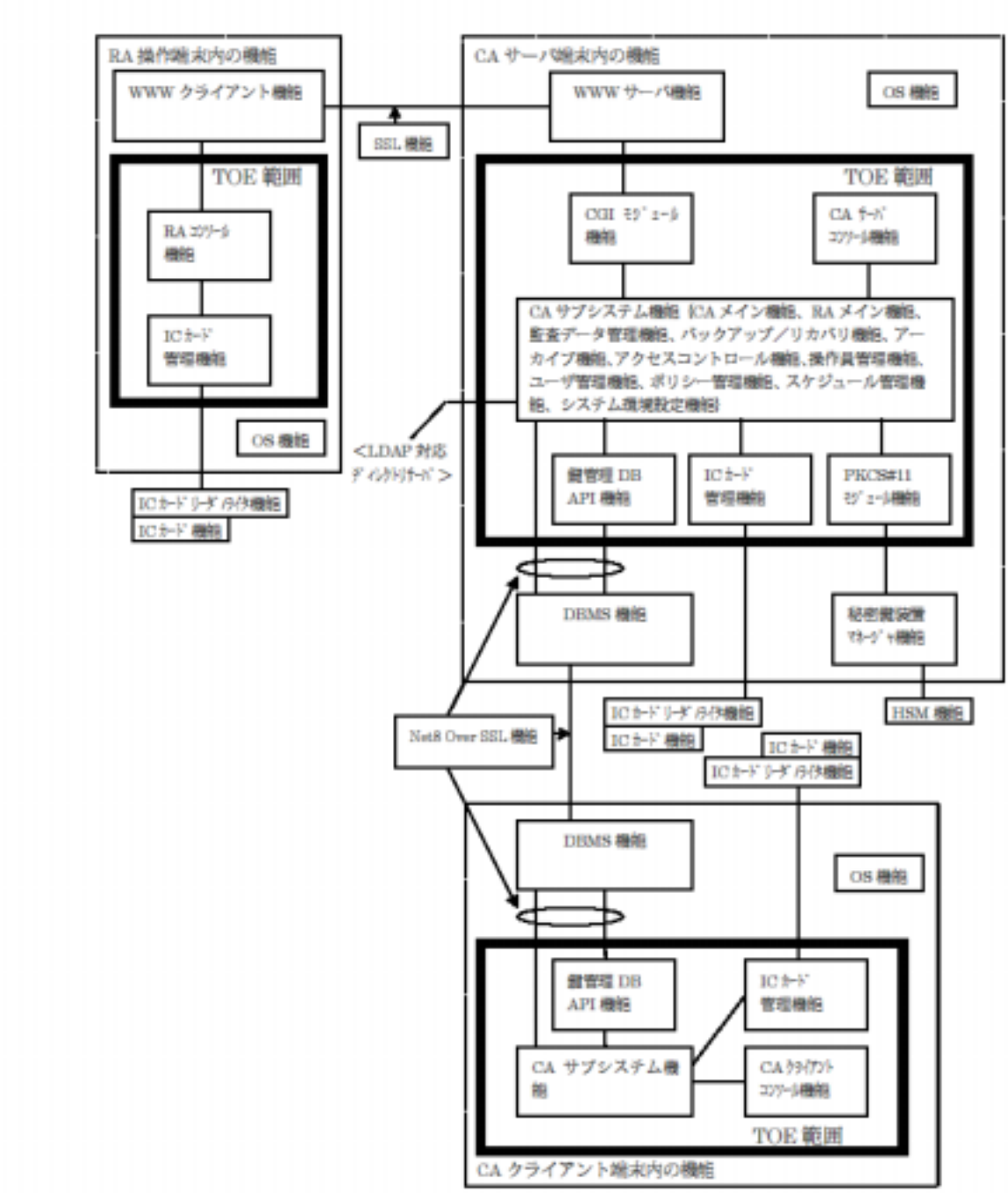

図2-1　　TOEとIT環境の構成

TOE各パーツの相互関係、及びTOE各パーツとTOE外の機能との相互関係は、以下に示すとおりである。

・CAサーバ端末とRA操作端末間の通信:

CAサーバ端末とRA操作端末は、WWWサーバとWWWクライアント機能を介して相互に通信する。WWWサーバ・WWWクライアント間の通信データは、SSLで暗号化されたセキュアなチャネルを介して送受される。

・CAサーバ端末、CAクライアント端末におけるTOEとDBMS機能間、及びCAサーバ端末、

CAクライアント端末各々のDBMS間の通信:
TOE機能及びDBMS機能の下位プログラムが提供するNet8 Over SSLを介して通信する。Net8は、Oracle社が提供するミドルウェアで、クライアントとDBMS、あるいはDBMS間のトランスペアレントなコネクションを提供する。SSLを介することによって、セキュアな通信が実現される。

・CAサーバ端末のTOE部分と秘密鍵装置マネージャ機能:
CA自身の秘密鍵は、HSM機能内に格納されている。CAは、秘密鍵を使用する処理を行う際、秘密鍵装置マネージャへアクセスして必要な処理を依頼する。秘密鍵を使用する処理は、HSM機能内で行われ、秘密鍵は、HSM機能内で安全に保持される。

・各端末のTOE部分とICカードリーダ/ライタ機能:
ICカード内情報に関わる処理が必要なとき、TOEは、ICカードリーダ/ライタ機能を介してICカード内情報にアクセスする。なお、端末とICカードリーダ/ライタ間の通信は、特に暗号化されない。双方の装置は、物理的アクセスが管理された室内で、操作者の目が届くごく近い距離で相互接続されており、タッピング等の物理的な盗聴が事実上困難な環境で使用される。

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 (ST評価報告書と個別報告書のセット) [20]において報告されている。ST評価報告書には、TOEの一般情報とST評価の総合判定が記されている。総合判定は、「合格」である。個別評価報告書では、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。

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。

評価者は、本STがASEクラスの要件を満たしていると判断した。

4 結論

4.1 ST確認結果

提出されたST評価報告書[20]及び所見報告書の検査、及び評価実施機関に対する評価作業の監督・確認の結果、本STは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が確認された。ただし、TOE評価は実施されていないために、ASEクラスの要件の中で、TOE評価と関連する事項は確認の対象外である。

4.2 勧告

日本電気株式会社のPKIサーバ／Carassuit 電子政府版 ver2.0　を使用する者は、本ST確認報告書に該当するST[1]と併せ読むことで、ST確認の範囲を明確に理解すべきである。

本ST確認報告書の内容は、1.4.7節に示された構成条件の下においてのみ有効である。同時に、1.4.8節に記載された動作環境の前提条件が満たされていなければならない。

5 ST確認者補記

TOEのIT環境に関わる留意点を述べる。本STに記載されたTOEは、分散型TOEである。CAサーバ端末、CAクライアント端末、RA操作端末と呼ばれる3種類の装置にTOEが分散している。分散した各TOEパーツの下位で動作するソフトウェア、ハードウェアには、「表1-3 TOEの構成条件」に示されるいくつかのバリエーションが想定されている。各TOEパーツごとに下位ソフトウェア、ハードウェアのバリエーションを組み合わせると、TOE全体として、多くのバリエーションが生じる。しかも、TOE下位のソフトウェア、ハードウェアのふるまいは、TSFに影響を及ぼす場合がある。このため、TOEの評価に際しては、TSFの動作に関係するこれら下位のハードウェア、ソフトウェアのふるまいについて、セキュリティ上の観点から十分な吟味を行わなくてはならない。特に、TSFのテストにおいて、下位のソフトウェア、ハードウェアのふるまいを含めた評価が必要となる。

6 用語

【CC関連用語】

本報告書で使用されたCC関連の略語を以下に示す。

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
TSF	TOE Security Functions

【TOE関連用語】

本報告書で使用されたTOE関連の略語・用語の定義を以下に示す。

API	Application Programming Interface
ARL	Authority Revocation List ： 機関失効リスト
BASE64	エンコード方式の一つ
CA	Certificate Authority ： 認証局
CGI	Common Gateway Interface : Web サーバが、Web ブラウザからの要求に応じて、プログラムを起動するための仕組み
CPS	Certification Practice Statement ： 認証局運用規定
CRL	Certificate Revocation List ： 証明書失効リスト
DB	Database ： データベース
DER	Distinguished Encoding Rules ： 区別化エンコード規則
DES	Data Encryption Standard：IBM社によって開発された秘密鍵暗号化アルゴリズム
EE	End Entity ： エンドエンティティ (一般利用者)
FIPS	Federal Information Processing Standard ： 米国政府調達基準; 暗号モジュールの安全性に関する標準を含む
HSM	Hardware Security Module ： 認証局秘密鍵を生成管理するハードウェア
IC	Integrated Circuit ： 集積回路
ID	Identification ： 識別番号
LDAP	Lightweight Directory Access Protocol ： TCP/IP ネットワークで、ディレクトリデータベースにアクセスするためのプロトコル
PIN	Personal Identification Number ： 個人識別番号
PKCS	Public Key Cryptography Standards ： RSA DSI社が定める公開鍵暗号技術をベー

	スとした各種の規格群
PKI	Public Key Infrastructure ： 公開鍵基盤
RA	Registration Authority ： 登録局
RSA	Rivest Shamir Adleman ： Ronald Rivest氏、Adi Shamir氏、Leonard Adleman氏の3 人が1978 年に開発した公開鍵暗号方式の一つ
WWW	World Wide Web
Net8	Oracle DBのネットワークコンポーネント
SSL	Secure Socket Layer：Netscape Communications社が開発した、インターネット上で情報を暗号化して送受信するプロトコル

7 参照

[1] PKIサーバ／Carassuit 電子政府版 ver2.0 セキュリティターゲット バージョン 2.1 日本電気株式会社

[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] ST評価報告書 1.2版 2002年11月1日 CLE-ETRST-0001-02 / 個別評価報告書 1.2版 2002年11月1日 CLE-EST-0001-02 / 電子商取引安全技術研究組合研究所

(白紙)