ＳＴ確認報告書

独立行政法人 情報処理推進機構
理事長　藤原　武平太

原紙押印済

評価対象

申請受付年月日（受付番号）	**平成**18年11月1日（ST**確認**6039）
確認番号	V030
ＳＴ確認申請者	**日本電気株式会社**
ＴＯＥの名称、バージョン	PKI**サーバ**／Carassuit **電子政府版** ver3.1
ＳＴの名称、バージョン	PKI**サーバ**／Carassuit **電子政府版** ver3.1 **セキュリティターゲット バージョン**1.13
ＰＰ適合	**なし**
適合する保証要件	ASE(ST**評価**)**クラス及び**ADV_FSP.1、ADV_RCR.1**保証コンポーネント** （TOE**の保証パッケージは**EAL3**適合**）
開発者	**日本電気株式会社**
評価機関の名称	**みずほ情報総研株式会社 情報セキュリティ評価室**

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19年2月22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：「ITセキュリティ評価及び認証制度の基本規程」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 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「PKIサーバ／Carassuit 電子政府版 ver3.1 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ITセキュリティ認証手続規程に従い、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、「PKIサーバ／Carassuit 電子政府版 ver3.1 セキュリティターゲット」[1]（以下「本ST」という。）についてみずほ情報総研株式会社 情報セキュリティ評価室（以下「評価機関」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、対応する本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、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 TOEの範囲」で定義される。

- 名称: PKIサーバ／Carassuit 電子政府版
- バージョン: ver3.1
- 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、一般利用者の公開鍵に対する公開鍵証明書発行、機関証明書発行、CA自身の公開鍵証明書発行、公開鍵証明書保管、及び失効リスト発行である。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 ver3.1を構成するCAサーバ用、CAクライアント用、RA用の各アプリケーション群をCAサーバ端末、CAクライアント端末、RA操作端末の各端末にインストールしたもの（図1の網掛け部分）であり、それぞれが連携してPKIのCA/RAサービスを提供する。

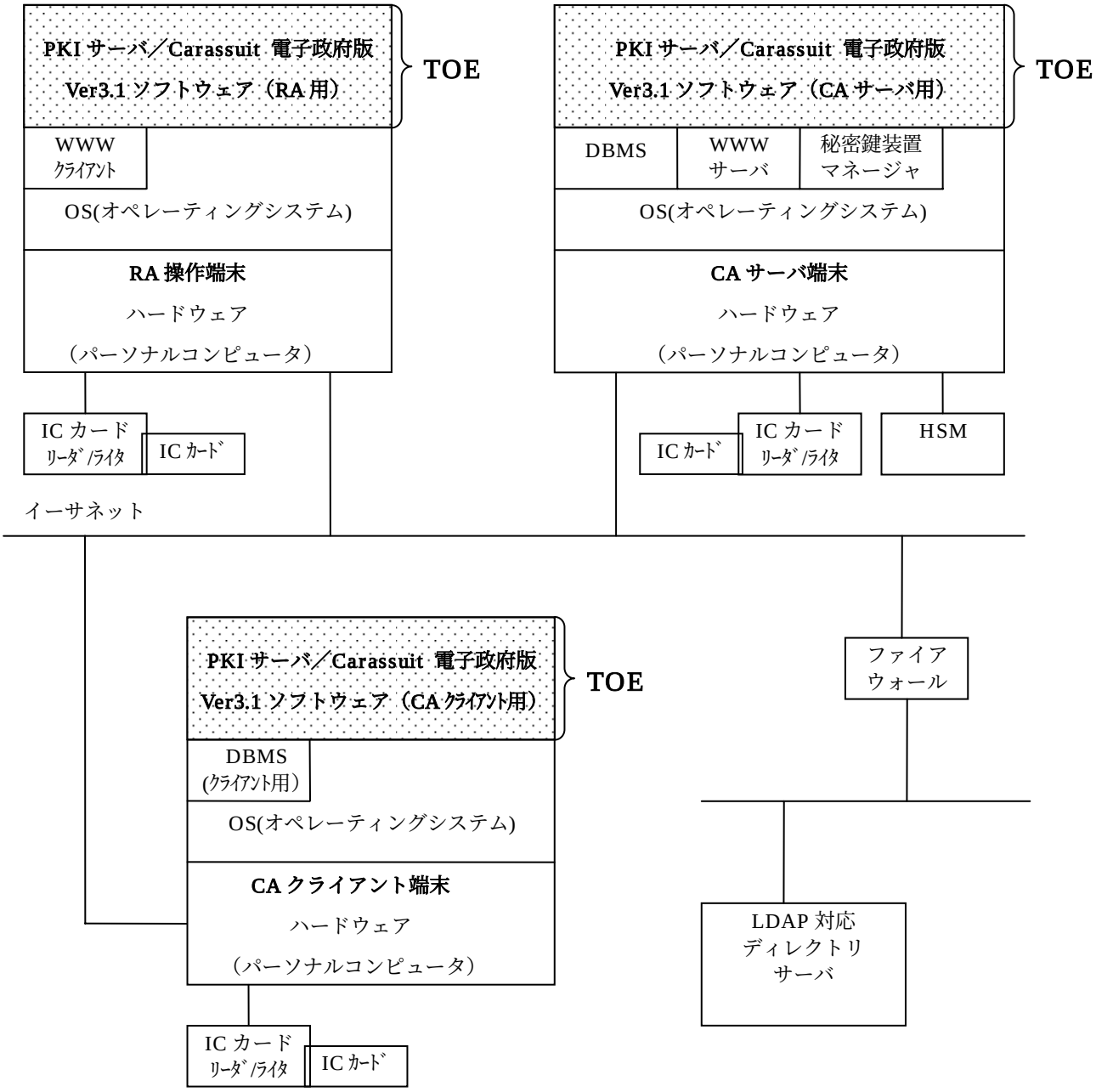

図1　PKIサーバ／Carassuit 電子政府版 ver3.1の構成

TOEを構成する各アプリケーションプログラムは、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)上で動作する。

各端末にはICカードリーダ/ライタが接続され、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)が接続される。また各端末はイーサネットで相互接続される。

なお、図1中のTOE以外のソフトウェア及びハードウェアの各用語の定義については「5. 用語」を参照のこと。

1.2.4 TOE**の動作概要**

TOEは、以下のCA(認証局)/RA(登録局)としてのサービスを提供するための機能とCA/RAの運用管理に関わる機能を提供する。

(1) CAメイン機能

- 一般利用者の公開鍵に対する公開鍵証明書の発行
  一般利用者(EE)の公開鍵に対して電子署名し、公開鍵証明書を発行する（申請者が公開鍵に対応した秘密鍵を持つことを保証する)。
- 機関証明書の発行
  機関証明書を発行する。機関証明書には、下位CA証明書と相互認証証明書との二種類がある。
- CA自身の公開鍵証明書の公開
  発行した公開鍵証明書を検証するためにCA自身の公開鍵証明書を発行する。
- 失効リストの発行
  証明書失効リスト(CRL)及び機関失効リスト(ARL)を発行する。
- 公開鍵証明書の保管
  公開鍵証明書をディレクトリへ保管する。

(2) RAメイン機能

- 証明書申請要求の受付
  RA操作端末からの証明書申請要求を受け付ける。
- 証明書発行・失効に伴う資格審査
  申請された証明書発行･失効などの要求に対して資格審査を行うための機能を提供する。

(3) 運用管理に関わる機能

- 監査データ管理機能
  TOEがセキュアに運用されていることを監査するために必要な情報の採取、及び管理を行う。
- バックアップ／リカバリ機能
  TOEの障害に備えて、システムの復旧に必要なデータのバックアップを行う。障害が発生した場合には、バックアップをリストアすることによりTOEを復旧する。
- アーカイブ機能
  TOEが発行した証明書、鍵等の履歴を管理する。
- アクセスコントロール（操作員管理）機能
  あらかじめ定められたTOEの運用に関する役割とセキュリティ要件に基づき、TOEへのアクセスを操作員ID､証明書等を用いて制御する｡制御情報として、

上級操作員と一般操作員の登録・削除・情報管理、及び権限グループの管理を行う機能を提供する。

- ユーザ管理機能
  一般利用者(EE)の秘密鍵及び個人情報を管理する。要求に応じてEE鍵の鍵ペア生成、鍵保管を行う。一般利用者(EE)のICカードへ鍵・証明書を格納する形式のファイルを生成する機能を提供する。
- ポリシー管理機能
  証明書プロファイル及び証明書失効リストプロファイルの設定と変更を行う。
- スケジュール管理機能
  TOEをあらかじめ定めたスケジュールで運用する。また、証明書失効リスト(CRL)、機関失効リスト(ARL)のスケジュール機能を提供する。
- 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 ver3.1 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「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[4]に規定された内容に従い、評価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及び機能仕様が、CCパート1([5][8][11]のいずれか)附属書C、CCパート2（[6][9][12]のいずれか）の機能要件及びCCパート3（[7][10][13]のいずれか）のASEクラス及びADV_FSP.1の規定を満たし、STに対しては目標とするセキュリティ機能の妥当性を評価し、また機能仕様に対しては目標のセキュリティ機能が正確に設計されていることを評価することである。ただし、ASEクラス及びADV_FSP.1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（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

認証機関は、評価機関が実施するST及び機能仕様の評価を監督し、ST及び機能仕様の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19年2月の評価機関による「評価報告書」[18]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適合である。

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。

(1) 監査機能
セキュリティ関連事象の監査記録の生成、生成された監査記録の提示、及び生成された監査記録の保護を行う。

(2) アクセス制御機能
上級操作員と一般操作員の種別とアクセス権限に基づく操作制限、及び各操作員のアクセス権限の管理を行う。

(3) 識別認証機能
ログインする端末と操作員種別に応じて、ID／パスワード認証、ICカード内の操作員証明書を使用した認証などの複数の認証メカニズムを提供する。また、パスワード・PINの品質の検証、認証失敗時のアカウントロックの各機能を提供する。

(4) 暗号機能
TOEが取り扱う各種データに対して、署名検証、暗号化・復号、及びダイジェスト生成を行う。また、その際に使用する暗号鍵の生成・廃棄を行う。
（注：CA鍵ペアの生成、及びCA秘密鍵によるEE証明書、機関証明書、操作員証明書、及び失効リストの署名はHSMが行う。）

(5) 証明書発行機能
発行する証明書と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。また、発行するすべての証明書及び失効リストの発行履歴を管理する。

1.4.5 脅威

TOEは、表1に示す脅威を想定し、これに対抗する機能を備える。

表1　想定する脅威

識別子	脅威
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、利用者データおよびTSFデータが保存されたデータベースに直接アクセスすることにより、その利用者データおよび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	組織のセキュリティ方針
P.ISSUE （発行）	TOEにより提供される認証局（CA）は、自らが発行するすべての証明書及び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。また自らが発行するすべての証明書及び失効リストの発行履歴を管理しなければならない。
P.AUTHORITY （権限付与）	利用者は、運用上必要な最小限の権限のみを与えられるものとする。

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または140-2、PKCSに従って生成・破棄・操作されるものとする。
P.OS_DB （信頼できるOS／DB）	TOEを動作させるために必要となるOSおよびDBは、識別認証機能を適切に実施できるもの、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るものを利用しなければならない。またOSは信頼できるタイムスタンプ情報を提供しなければならない。

1.4.7 構成条件

TOEの構成条件を表3に示す。

本評価では、CAサーバ端末、CAクライアント端末、RA操作端末の各端末が以下のソフトウェアによって構成されているときのTOEが評価対象である。

表3　TOEの構成条件

端末	ソフトウェア
CAサーバ端末	• OS Windows 2000 Server または Windows Server 2003 • DBMS Oracle10g Release2 の Enterprise Edition 及び Oracle Advanced Security • WWWサーバ Internet Information Service 5 または Internet Information Service 6
CAクライアント端末	• OS Windows 2000 または Windows XP または Windows Server 2003 • DBMS(クライアント用) Oracle10g Release2 の Enterprise Edition 及び Oracle Advanced Security (必要な製品コンポーネントは Oracle Database 10gとOracle Net Servicesのみ)
RA操作端末	• OS Windows 2000 または Windows XP または Windows Server 2003 • WWWクライアント Microsoft Internet Explorer 6.0

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4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4　TOE使用の前提条件

識別子	前提条件
A.PASSWORD_MANAGEMENT （操作員によるパスワードの管理）	上級操作員および一般操作員が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.USER_RESTRICTION （利用者制限）	TOEに関連する権限・役割を持つ利用者は、管理者（上級操作員、一般操作員、監査ログ検査者、RA操作員）のみとなるように利用者登録を行う。
A.SAFE_PLACE （安全な場所）	TOEに関連するハードウェアは、許可された人員のみが入室できるよう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.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及び機能仕様の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及び機能仕様の評価を規定したASEクラス及びADV_FSP.1の要件の中で、TOE評価と関連する事項については評価の対象になっていない。また、ASEクラス及びADV_FSP.1以外の保証要件に属する事項、例えば、STの記載事項がそのとおりに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

2.1 TOEの動作に必要なハードウェア

TOEの動作に必要なハードウェアを表5に示す。

表5　ハードウェア構成

端末	ハードウェア
CAサーバ端末	• 本体 Express5800シリーズ • CPU PentiumⅢ 1GHz 以上 • メモリ 512MB 以上 • ハードディスク 2GB 以上
CAクライアント端末	• 本体 Express5800シリーズ、PC／AT互換機 • CPU PentiumⅢ 1GHz 以上 • メモリ 512MB 以上 • ハードディスク 2GB 以上
RA操作端末	• 本体 Express5800シリーズ、PC／AT互換機 • CPU PentiumⅢ 1GHz 以上 • メモリ 256MB 以上 (512MB 以上推奨)

各端末間はイーサネットでネットワーク接続される。また、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、及び使用されるICカードは以下のとおりである。

- ICカードリーダ／ライタ
  Gemplus社製 GemPC410 (RS-232C接続タイプ)、GemPCTwin (RS-232C接続タイプまたはUSB接続タイプ)
  NEC製 CK1505-02 (USB接続タイプ)、CK1506-02 (USB接続タイプ)
- HSM
  NEC製 CK-GuardⅡ、CK-GuardⅢ、
  SafeNet社製 Luna CA^3、Luna SA
- ICカード
  大日本印刷社製 Standard-9 (NEC SecureWare用 STD-9)

3 評価機関による評価結果

評価は、CCパート3のASEクラス及びADV_FSP.1の規定に基づき、CEM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、評価報告書[18]において報告されている。評価報告書には、TOEの概要説明、CEM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

認証機関は、評価の過程で評価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及び機能仕様に反映されていること。

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

④ 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 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クラス及びADV_FSP.1の保証要件を満たしていることを確認した。

評価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、確認結果を表6にまとめる。

表6　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記述が理路整然とし一貫してい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。
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。
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。
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、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。
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完全で、理路整然としていて、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完全で、理路整然としていて、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。

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全で、理路整然としていて、かつ一貫していることを確認している。
開発	**適切な評価が実施された。**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んで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所見報告書も適切と判断される。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化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所見報告書も適切と判断される。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であることを、それらの対応分析により確認している。

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を以下に示す。

【CC関連用語】

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】（）内に日本語訳または一般的な意味を示す。

ARL	Authority Revocation List（機関失効リスト）
CA	Certificate Authority（認証局）
CRL	Certificate Revocation List（証明書失効リスト）
DB	Database（データベース）
EE	End Entity（エンドエンティティ）
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（暗号鍵を生成・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 Data Security社(現RSA Security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）
WWW	World Wide Web（ワールドワイドウェブ）

本報告書で使用された用語の定義を以下に示す。

CAクライアント端末ハードウェア	CAサーバが提供するCAサービスに接続するパーソナルコンピュータ。
CAサーバ端末ハードウェア	CAサービスが稼動するパーソナルコンピュータ。

DBMS	TOEが処理する各種データを管理するためのデータベース管理システム。識別認証機能とアクセス制御機能を有する。
DBMS(クライアント用)	CAサーバ端末に保存されたデータにアクセスする手段を提供するデータベース管理システムのクライアント機能。
HSM	認証局(CA)秘密鍵を生成・管理するハードウェア装置で、FIPS PUB 140-1 または140-2 レベル3またはレベル3相当である。CAサーバ端末に接続される。秘密鍵へのアクセスは、秘密鍵装置マネージャからHSMへ処理を依頼し、HSM内で秘密鍵を使用し、結果を秘密鍵装置マネージャへ返却する方式であり、HSM自身のバックアップ操作以外でCA秘密鍵がHSMの外に出ることはない。また、耐タンパ性があり、解体などの物理的な不正操作を検知すると、HSM内のCA秘密鍵を消去することによって、CA秘密鍵の暴露を防止する。
ICカード	一般操作員の操作員証明書及び操作員秘密鍵を保持するハードウェア。ICカードリーダ／ライタ経由でアクセスする。ICカードに格納された操作員証明書及び操作員秘密鍵にアクセスするには、PINによる認証が必要である。ICカードは一般操作員の識別・認証用に用いられる。また、EE用にEE証明書及びEE秘密鍵の保持にも使用される。ただし、EE用ICカードと一般操作員用ICカードは兼用できない。
ICカードリーダ／ライタ	ICカードをリード／ライトするハードウェア装置。
LDAP対応ディレクトリサーバ	証明書を蓄積・公開するためのLDAPプロトコルをサポートするサーバ。
OS(オペレーティングシステム)	アプリケーションソフトウェアを動作させるための基盤となるソフトウェア。識別認証機能とアクセス制御機能を有する。
RA操作端末ハードウェア	CAサーバに接続して、RA操作を実行するためのパーソナルコンピュータ。
WWWクライアント	RA操作端末からCAサーバ端末（WWWサーバ）に対して、RA操作のための要求を行うためのクライアントプログラム。
WWWサーバ	RA操作端末からの要求に応じるためのサーバプログラム。
秘密鍵装置マネージャ	HSMへの低レベルアクセスインタフェースを提供する。
ファイアウォール	CAサーバ端末・CAクライアント端末・RA操作端末のつながっているネットワークとそれら以外の端末（外部端末）のつながっているネットワークを分離し、外部端末からの不正侵入を防止するハードウェア装置。

6 参照

[1] PKIサーバ／Carassuit 電子政府版 ver3.1 セキュリティターゲット
バージョン1.13 2007年2月7日 日本電気株式会社

[2] ITセキュリティ評価及び認証制度の基本規程 平成18年9月 独立行政法人 情報処理推進機構 EC-01

[3] ITセキュリティ認証手続規程 平成18年9月 独立行政法人 情報処理推進機構 EC-03

[4] 評価機関承認手続規程 平成18年9月 独立行政法人 情報処理推進機構 EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[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2.3 2005年8月 CCMB-2005-08-001 (平成17年12月翻訳第1.0版)

[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2.3 2005年8月 CCMB-2005-08-002 (平成17年12月翻訳第1.0版)

[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2.3 2005年8月 CCMB-2005-08-003 (平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月 (平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512 平成17年12月

[18] PKIサーバ/Carassuit 電子政府版 ver3.1 評価報告書 第3版 2007年2月7日
みずほ情報総研株式会社 情報セキュリティ評価室