ST確認報告書

独立行政法人情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成23年9月21日（ST確認1060）
確認番号	V051
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 ver4.1
STの名称、バージョン	PKIサーバ/Carassuit 電子政府版 ver4.1 セキュリティターゲット バージョン1.7
PP適合	なし
適合する保証パッケージ	ASE(ST評価)クラス及びADV_FSP.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24年1月31日

技術本部
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　山里　拓己

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 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 バージョン3.1 リリース3
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース3

評価結果：合格

「PKIサーバ/Carassuit 電子政府版 ver4.1 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セキュリティ認証申請手続等に関する規程に従い、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 ver4.1 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の範囲と動作概要」で定義されている。

- 名称　　：　PKIサーバ/Carassuit 電子政府版
- バージョン　：　ver4.1
- 開発者　　：　日本電気株式会社

1.2.2 製品概要

本製品は、公開鍵基盤(PKI)における認証局(CA)機能および登録局(RA)機能を提供するソフトウェアシステムである。製品は、CAサーバ端末に搭載されるCAサーバ用アプリケーション、各CAクライアント端末に搭載されるCAクライアント用アプリケーション、各RA操作用端末からブラウザにより操作されるWEBアプリケーションという、3種類のソフトウェアで構成されており、それら全体でCA/RAの機能を提供する。

CAとしての主な機能は、エンドエンティティ(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の範囲と動作概要

TOEは、認証局(CA)機能のアプリケーションが搭載されたCAサーバ端末・CAクライアント端末と、登録局(RA)機能のWEBアプリケーション（WEBアプリケーション自体はCAサーバ端末内のWEB/APサーバ上に配置される）を操作するRA操作端末という構成になっており（図1-1の太破線で囲んだ部分がTOEに該当）、それぞれが連携してPKIのCA(認証局)/RA(登録局)サービスを提供する。

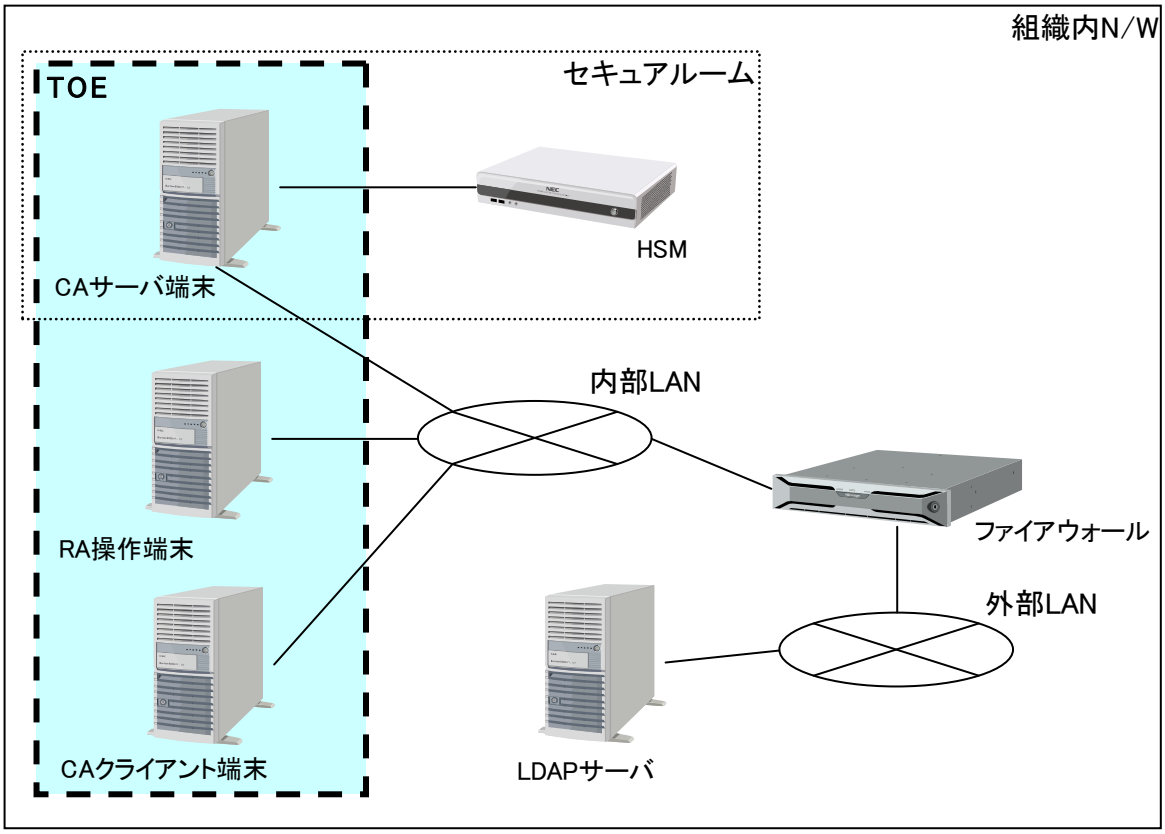

図1-1 PKIサーバ/Carassuit 電子政府版 ver4.1のIT構成図

組織内でTOEを稼動する場合、1台以上のCAサーバ端末、1台以上のRA操作端末、1台以上のCAクライアント端末を設置し、それぞれをファイアウォールによって外部ネットワークからのアクセスが制限されたセキュアなLAN（ここでは、内部LANと呼称する）で接続する。

図1-1にあるとおり、CAサーバ端末は入退出管理されたセキュアルームに設置され、HSM(ハードウェアセキュリティモジュール)が接続される。

次に、TOEに関わるIT機器と周辺装置の説明を表1-1に記す。

表1-1 TOEに関わるIT機器と周辺装置

名称	説明
CAサーバ端末	認証局(CA)機能が稼動するパーソナルコンピュータ。 CAサービスの起動/停止、システム環境設定、バックアップ/リカバリ、監査データ参照、上級/一般操作員管理、CAの秘密鍵管理を行う為に用いる。
HSM	認証局秘密鍵を生成・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。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内の秘密鍵を消去することによって、秘密鍵の暴露を防止する。CAサーバ端末に接続される。
CAクライアント端末	認証局(CA)機能に接続するパーソナルコンピュータ。 CAサーバ端末で稼動しているCAサービスの状態監視、証明書のポリシー設定、監査データ参照、ユーザ管理、一般操作員管理を行う為に用いる。
RA操作端末	登録局(RA)操作を実行するためのパーソナルコンピュータ。 証明書発行要求、証明書失効要求、証明書取得、失効リスト取得、ICカード発行依頼ファイル取得を行う為に用いる。
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。図1-1中には描かれていないが、CAサーバ端末、RA操作端末、CAクライアント端末の各端末に接続される。
ICカード	操作員証明書および秘密鍵を保持するハードウェア。図1-1中には描かれていないが、ICカードリーダ/ライタ経由でアクセスする。
内部LAN	CAサーバ端末、CAクライアント端末、RA操作端末が接続するネットワークである。通常、ファイアウォールによって組織内の外部LANからのアクセスが制限される。
LDAPサーバ	CAサーバ端末で稼動するCAサービスにより発行された証明書及び失効リストが保管されるディレクトリサーバ。図1-1では組織内部に閉じたネットワーク上に設置されているが、インターネット上に証明書、失効リストを公開する場合は、インターネットに接続される事もある。
ファイアウォール	CAサーバ端末・CAクライアント端末・RA操作端末が接続されているネットワークとそれら以外の端末（外部端末）が接続され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。

各端末の周辺装置（HSM、ICカードリーダ/ライタ）は、それぞれの端末付近に設置され、各端末とRS232Cケーブル、SCSIケーブルまたはUSBケーブルで直接接続される。

各端末はイーサネットケーブルで接続されている。また、証明書を蓄積・公開するLDAP対応ディレクトリサーバがファイアウォールの外側に接続されている。その他のハードウェアとして、バックアップするデータを保存するバックアップ媒体がある。

次に、TOEの物理的範囲を図1-2に記す。

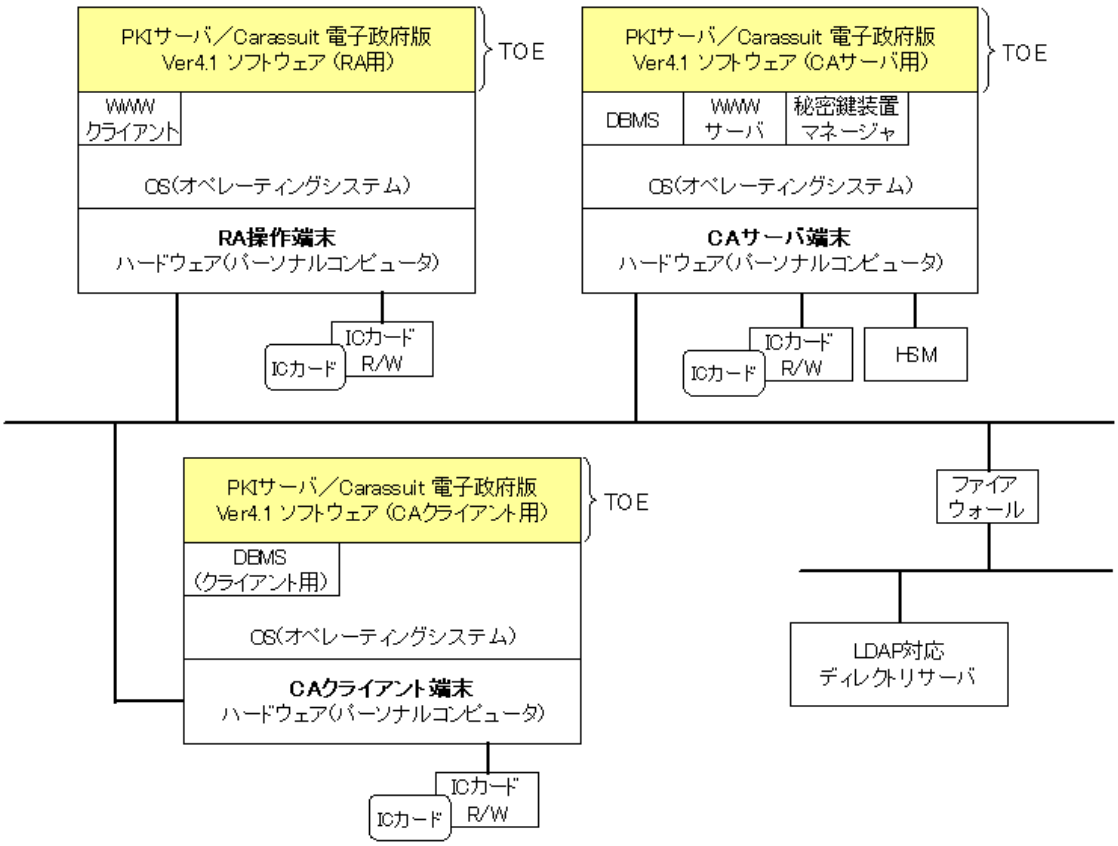

図1-2 PKIサーバ/Carassuit 電子政府版 ver4.1の構成図

図1-2が示すように、TOEはPKIサーバ/Carassuit 電子政府版 ver4.1ソフトウェア(CAサーバ用、CAクライアント用、RA操作用)であり、それ以外のハードウェア・ソフトウェアはTOE外となる。

次に、TOE及びTOEを動作させる為に必要なソフトウェアについて端末ごとに、表1-2に記述する。

表1-2 TOEに関わるソフトウェア

端末	ソフトウェア	
CAサーバ端末	PKIサーバ/Carassuit 電子政府版 ver4.1 ソフトウェア(CAサーバ用)	TOEであり、CAサーバ用の複数のアプリケーション。CAサーバコンソール機能、CAサブシステム機能、CGIモジュール機能、鍵管理DB-API機能、ICカード管理機能、PKCS#11モジュール機能がある。
	DBMS	データベース管理システム。TOEデータを管理する。
	WWWサーバ	WEBサーバ。RA操作端末の要求に応じる。
	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ソフトウェア。
	OS	上記ソフトウェアを動作させる為の基盤となるソフトウェア。
CAクライアント端末	PKIサーバ/Carassuit 電子政府版 ver4.1 ソフトウェア(CAクライアント用)	TOEであり、CAクライアント用の複数のアプリケーション。CAクライアントコンソール機能、CAサブシステム機能、鍵管理DB-API機能、ICカード管理機能がある。
	DBMS(クライアント用)	データベース管理システム。CAサーバ端末に保存されたTOEデータにアクセスする手段を提供する。
	OS	上記ソフトウェアを動作させる為の基盤となるソフトウェア。
RA操作端末	PKIサーバ/Carassuit 電子政府版 ver4.1 ソフトウェア(RA用)	TOEであり、RA用の複数のWEBアプリケーション。RAコンソール機能、ICカード管理機能がある。
	WWWクライアント	WEBブラウザ。CAサーバ端末上のWEBアプリケーションへリモートアクセスしてRA操作を行う。
	OS	上記ソフトウェアを動作させる為の基盤となるソフトウェア。

1.2.4 TOEの機能

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。

次に、各機能の説明を記す。

(1) CAメイン機能

- エンドエンティティ(一般利用者)の公開鍵に対する公開鍵証明書の発行
  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)。
- CA鍵ペア生成、鍵保管
  必要に応じてEE鍵の鍵ペア生成、鍵保管を行う。EEの秘密鍵保管時には、暴露防止のため暗号化する。
- 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2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LDAP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
  エンドエンティティ(一般利用者)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。エンドエンティティ(一般利用者)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。

次に、TOEの役割を持つ利用者として、以下3種が定義されている。

- ✧ 上級操作員
- ✧ 一般操作員
- ✧ 監査ログ検査者

表1-3に、TOEの利用者役割を、各利用者が操作する端末ごとに記す。

表1-3 TOE利用者の役割

操作端末	役割		
CAサーバ端末	上級操作員	上級操作員（監査ログ検査者除く）	CAサーバ端末上で、付与されたアクセス権限に従って、認証局を操作する作業員。「監査ログ参照」および「監査管理」権限は割り当てられない。
		監査ログ検査者	CAサーバ端末上で、監査データを検査する作業員。当作業員は上級操作員ではあるが、「監査ログ参照」および「監査管理」の権限のみが付与され、他の権限を割り当てられないため、認証局の操作はできない。

操作端末	役割		
CAクライアント端末	一般操作員	一般操作員（監査ログ検査者除く）	CAクライアント端末上で、付与されたアクセス権限に従って、認証局を操作する作業員。「監査ログ参照」および「監査管理」権限は割り当てられない。
		監査ログ検査者	CAクライアント端末上で、監査データを検査する作業員。当作業員は一般操作員ではあるが、「監査ログ参照」および「監査管理」の権限のみが付与され、他の権限を割り当てられないため、認証局の操作はできない。
RA操作端末	一般操作員		RA操作端末上で、CAサーバに対して証明書発行要求、証明書発行要求の審査、証明書受取、証明書検索、証明書のICカードへの書込などのRA業務を行う作業員。

次に、本TOEの保護対象となる資産である利用者データ、TSFデータを以下に記す。

【利用者データ】

- ✧ 機関証明書
- ✧ EE証明書
- ✧ EE秘密鍵
- ✧ 失効リスト(CRL、ARL)
- ✧ EE ICカード発行情報

【TSFデータ】

- ✧ 操作員証明書
- ✧ 識別・認証情報
- ✧ アクセスコントロール情報
- ✧ 監査ログ
- ✧ アーカイブログ
- ✧ その他のシステム設定情報
- ✧ 暗号化用鍵(システム共通鍵、データベース共通鍵)

他に、TOEによる保護対象外のデータとして、TOEプログラム(図1-2のTOE範囲内で指定した機能のソフトウェアコンポーネント)、HSMのデータ(認証局秘密鍵(CA鍵))、ICカードのデータ(一般操作員証明書、一般操作員秘密鍵)、バックアップデータ(上記利用者データ、上記TSFデータ、レジストリ情報でバックアップ媒体に保存される）がある。

1.3 評価の実施

PKIサーバ/Carassuit 電子政府版 ver4.1 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、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セキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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ST及び機能仕様が、CCパート1 ([5][8]のいずれか) 附属書A、CCパート2 ([6][9]のいずれか) の機能要件及びCCパート3 ([7][10]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 ([11][12]のいずれか) に準拠する。

1.4 評価の確認

認証機関は、評価機関が作成した評価報告書[16]、所見報告書、及び関連する評価証拠資料を検証し、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。確認の過程において発見された問題については、認証レビューを作成した。評価は、平成24年1月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本ST確認報告書を作成し、確認作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

本STが規定するTOEの評価保証レベルは、EAL3適合である。

1.5.3 パッケージ適合

本STにおいて適合するパッケージ主張はなし。ただし、本STにて適用される保証コンポーネントは、調達者の要請により以下のとおりである。

ASE_CCL.1、ASE_ECD.1、ASE_INT.1、ASE_OBJ.2、 ASE_REQ.2、 ASE_SPD.1、ASE_TSS.1、ADV_FSP.1

1.5.4 セキュリティ機能

TOEは、業務に関連する利用者データに対して、誤使用や改ざん、消失等から保護するため、以下のセキュリティ機能を提供する。

(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。

1.5.5 脅威

TOEは、次の表1-4に示す脅威を想定し、これに対抗する機能を備える。

表1-4 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カード発行依頼ファイル暴露）	高度な専門知識を持たない不正な利用者が、CAサーバ端末、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カード発行依頼ファイルに直接アクセスすることにより、EE ICカード発行依頼ファイルを暴露するかもしれない。

1.5.6 組織のセキュリティ方針

TOEの利用にあたって要求される組織のセキュリティ方針を以下表1-5に示す。

表1-5 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。本方針は、[14]および[15]の「4.6 アーカイブ」に準拠する。
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。本方針は[13]の「2.1.1.3 権限管理機能」に準拠する。

識別子	組織のセキュリティ方針
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。本方針は[14]および[15]の「5.2 手続き面の管理 (8)監査ログ検査者」に準拠する。
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。これにより認証局秘密鍵が物理的に保護されなければならない。本方針は[14]および[15]の「6.1 鍵ペア生成とインストール」に準拠する。
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。本項目は[13]の「2.1.1 情報セキュリティについての機能」および「2.2.2 電子計算機」に準拠する。

1.5.7 構成条件

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表1-6に記すソフトウェアによって構成されているとするTOEが評価対象となる。

表1-6 ソフトウェア構成

端末	ソフトウェア	
CAサーバ端末	OS	Microsoft Windows Server 2003 R2 SP2(32bit) または Microsoft Windows Server 2008 SP2(32bit) または Microsoft Windows Server 2008 R2 SP1
	DBMS	Oracle Database 11g R2(32bit/64bit) 及び Oracle Advanced Security 11g(有償オプション)
	WWWサーバ	Microsoft Internet Information Service 6.0 または Microsoft Internet Information Service 7.0 または Microsoft Internet Information Service 7.5
	HSMインタフェース	NEC SecureWare/秘密鍵装置マネージャ Ver4.0 または Luna SA Client SoftWare 4.5
CAクライアント端末	OS	Microsoft Windows Server 2003 R2 SP2(32bit) または Microsoft Windows Server 2008 SP2(32bit) または Microsoft Windows Server 2008 R2 SP1
	DBMS	Oracle Client 11g R2(32bit/64bit)

端末	ソフトウェア	
RA操作端末	OS	Microsoft Windows Server 2003 R2 SP2(32bit) または Microsoft Windows Server 2008 SP2(32bit) または Microsoft Windows Server 2008 R2 SP1 または Microsoft Windows XP SP3(32bit) または Microsoft Windows Vista SP2(32bit) または Microsoft Windows 7 SP1(32bit/64bit)
	WWWクライアント	Microsoft Internet Explorer 7.0 または Microsoft Internet Explorer 8.0 または Microsoft Internet Explorer 9.0

次に、TOEの動作に必要なハードウェアを表1-7に示す。

表1-7 ハードウェア構成

端末	ハードウェア	
CAサーバ端末	パーソナルコンピュータ	NEC Express5800シリーズまたはPC/AT互換機で、以下の条件を満たすもの。 CPU：Intel PentiumⅣ 1.5GHz以上 メモリ：1GB以上のRAM HDD：10GB以上の空き領域
	ICカードリーダ/ライタ	GemAlto GemPCTwin または NEC CK-1506-02
	ICカード	大日本印刷 Standard-9(NEC SecureWare用 STD-9)
	HSM	NEC CK-GuardⅣ または SafeNet LunaSA 4.8.1
CAクライアント端末	パーソナルコンピュータ	NEC Express5800シリーズまたはPC/AT互換機で、以下の条件を満たすもの。 CPU：Intel PentiumⅣ 1.5GHz以上 メモリ：1GB以上のRAM HDD：10GB以上の空き領域があるHDD
	ICカードリーダ/ライタ	GemAlto GemPCTwin または NEC CK-1506-02
	ICカード	大日本印刷 Standard-9(NEC SecureWare用 STD-9)
RA操作端末	パーソナルコンピュータ	NEC Express5800シリーズまたはPC/AT互換機で、以下の条件を満たすもの。 CPU：Intel PentiumⅣ 1.5GHz以上 メモリ：1GB以上のRAM HDD：10GB以上の空き領域があるHDD

端末	ハードウェア	
	ICカードリーダ/ライタ	GemAlto GemPCTwin または NEC CK-1506-02
	ICカード	大日本印刷 Standard-9(NEC SecureWare用 STD-9)

1.5.8 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1-8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1-8 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に関連する権限を持つ利用者として、職務上TOEの操作が必要な主体のみが上級操作員、一般操作員、監査ログ検査者となるように利用者登録を行う。TOEを利用する必要がなくなった場合には、当該利用者の登録を削除する。
A.SAFE_PLACE （安全な場所）	TOEに関連するハードウェアであるCAサーバ端末は、HSMと共に、入退出管理されたセキュアルームに設置される。RA操作端末、CAクライアント端末は、不正侵入できないよう制御された場所に設置される。設置場所の物理的セキュリティレベルは政府認証基盤の要求事項に準拠して[14]および[15]に示す文書中「5.1.2 物理的アクセス」によって規定される。
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。

識別子	前提条件
A.NETWORK （ネットワーク環境）	TOEのCAサーバ端末、CAクライアント端末、およびRA操作端末が接続されている内部ネットワークは、それら以外の外部端末が接続されているネットワークからファイアウォールで分離され直接接続されない。
A.TRUSTED_PATH （高信頼チャネル）	CAサブシステムとデータベース間、およびWWWサーバとWWWクライアント間のネットワーク上は、TSFデータ及び利用者データがその間で盗聴されることがないように、高信頼チャネルを用いて通信が行われる。
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に接続する周辺装置（HSM、ICカードリーダ/ライタ）はTOEの付近に設置される。TOEと周辺装置（HSM、ICカードリーダ/ライタ）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。

1.6 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等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ST確認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 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3のASEクラス及びADV_FSP.1の保証要件について、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[16]において報告されている。評価報告書では、TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成23年9月に始まり、平成24年1月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、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。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 評価結果

評価報告書をもって、評価者はST及び機能仕様がCEMのワークユニットすべてを満たしていると判断した。

3 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当該所見報告書でなされた指摘内容が妥当であること。
②当該所見報告書でなされた指摘内容が正しく反映されていること。
③提出された証拠資料の内容を検査し、関連するワークユニッ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に適合していること。

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 結論

4.1 確認結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、STがCCパート3に規定されたASEクラス及びADV_FSP.1に対する保証要件を満たしていることを確認した。

4.2 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関連略語】

CC (Common Criteria):
　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
CEM (Common Evaluation Methodology):
　情報技術セキュリティ評価のための共通方法
EAL (Evaluation Assurance Level):
　評価保証レベル
IT (Information Technology):
　情報技術
PP (Protection Profile):
　プロテクションプロファイル
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

【TOE関連略語】

ARL (Authority Revocation List):
　機関失効リスト
CA (Certificate Authority):
　認証局
CPS (Certification Practice Statement):
　認証局運用規定
CRL (Certificate Revocation List):
　証明書失効リスト
DBMS (Database Management System):
　データベースマネジメントシステム
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
PKI (Public Key Infrastructure):
　公開鍵基盤
RA (Registration Authority):
　登録局
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
WWW (World Wide Web):
　ワールドワイドウェブ

【TOE関連用語】
スケジュール:
　本報告書では、失効リストの更新処理の実行スケジュールを指す。
ポリシー:
　本報告書では、セキュリティ機能ポリシー、およびTOEセキュリティポリシー以外で出現する場合、証明書プロファイル、および失効リストプロファイルの定義を指す。

6 参照

[1] PKIサーバ/Carassuit 電子政府版 ver4.1 セキュリティターゲット
バージョン1.7 2011年12月13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23年2月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成23年2月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成23年2月 独立行政法人 情報処理推進機構 CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[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3.1 改訂第3版 2009年7月 CCMB-2009-07-001（平成21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3.1 改訂第3版 2009年7月 CCMB-2009-07-002（平成21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3.1 改訂第3版 2009年7月 CCMB-2009-07-003（平成21年12月翻訳第1.0版）

[11] Common Methodology for Information Technology Security Evaluation：Evaluation methodology Version 3.1 Revision 3 July 2009 CCMB-2009-07-004

[12] 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3.1 改訂第3版 2009年7月 CCMB-2009-07-004（平成21年12月翻訳第1.0版）

[13] 政府機関の情報セキュリティ対策のための統一基準（第4版） 2009年2月3日 情報セキュリティ政策会議

[14] 政府認証基盤（GPKI） 行政機関等認証局CP／CPSガイドライン 平成20年9月30日改定 共通システム専門部会了承

[15] 政府認証基盤（GPKI） 府省認証局CP／CPSガイドライン 平成15年6月6日改定 共通システム専門部会了承

[16] PKIサーバ/Carassuit 電子政府版 ver4.1 評価報告書 2012年1月16日
みずほ情報総研株式会社 情報セキュリティ評価室