認　証　報　告　書

評価対象

申請受付年月日(受付番号)	**平成16年12月3日（IT認証4037）**
認証番号	C0028
認証申請者	**日本電信電話株式会社**
TOEの名称	Trust-CANP
TOEのバージョン	V8.0i
PP適合	**なし**
適合する保証要件	EAL2
TOE開発者	**日本電信電話株式会社**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成17年7月6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セキュリティ評価機関に対する要求事項」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-0407

評価結果：合格

「Trust-CANP V8.0i」は、独立行政法人情報処理推進機構が定めるIT製品等のセキュリティ認証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

この認証報告書は、「Trust-CANP V8.0i」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である日本電信電話株式会社情報流通プラットフォーム研究所に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）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。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。
名称: Trust-CANP
バージョン: V8.0i
開発者: 日本電信電話株式会社 情報流通プラットフォーム研究所

1.2.2 製品概要

本製品は、PKI (Public Key Infrastructure) における認証局 (Certification Authority/Certificate Authority; 以下、CAと記す。) を実現するソフトウェアである。CAは、登録局 (Registration Authority; 以下RAと記す。) と連携し、公開鍵暗号方式を基盤とする電子認証システムの業務を果たす。本製品は、CAを構成する各機器のうち、その中核となるCAサーバ上で動作するソフトウェアと、操作者が使用してCAサーバにアクセスするCAO端末上で動作するソフトウェアの二つからなる。

1.2.3 TOEの範囲と動作概要

本TOEは、いくつかの装置 (ハードウェア) とそれらで動作するソフトウェア群と組み合わされ、電子認証システムサービスを提供する。電子認証システムサービスにおいて、TOEの主たる機能は、外部のRAサーバからの申請書に基づき公開鍵証明書の発行・失効を行い、CRL(公開鍵証明書失効リスト）を生成し、これらの情報をディレ

クトリサーバに送付し公開することである。

電子認証システムを構成する基本的な装置とソフトウェアの全体を図1-1に示す。この図において、ハッチをかけた太枠の部分がTOEである。外側のボックスはハードウェアを含む装置全体を表し、内側のボックスはソフトウェアを表す。各装置をつなぐ線は、接続ケーブルあるいはネットワークを表す。CAサーバ、RAサーバ、及びディレクトリサーバは、ファイアウォールサーバを介して接続される。なお、CAサーバ、CAO端末、HSM、ICカードリーダライタ及びファイアウォールサーバは、セキュアルームに設置される。

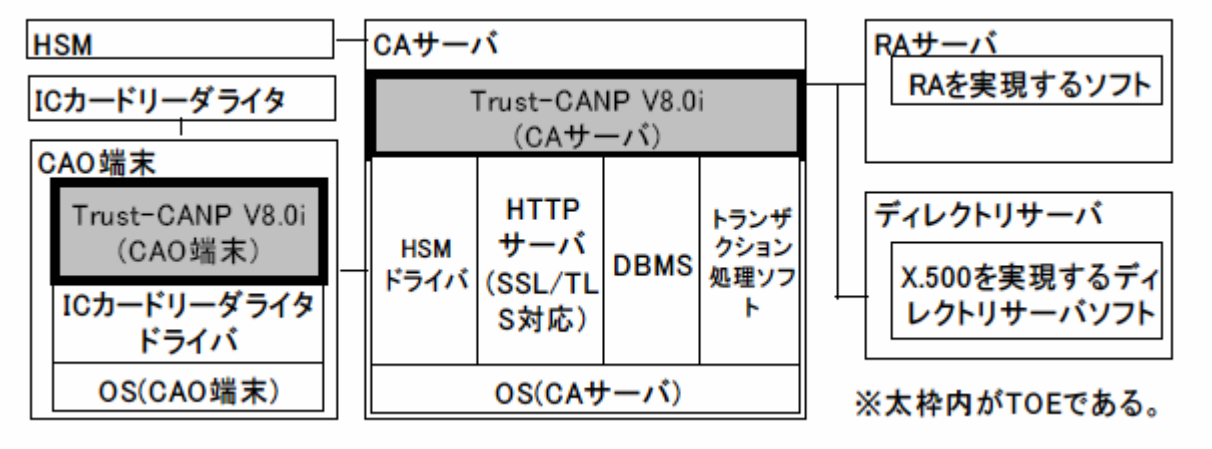

図1-1　TOEの範囲

図1-1に示された構成物は次のとおりである。

- CA サーバ
  Trust-CANP V8.0i(CA サーバ)、OS 、HTTP サーバ、DBMS、HSMドライバ、トランザクション処理ソフトがインストールされているサーバ。CAサーバには、HSM、CAO端末が接続され、RAサーバとディレクトリサーバには、ファイアウォールサーバを介して接続される。

- Trust-CANP V8.0i(CA サーバ)
  CAの機能を実現するソフトウェアの一部で、CAサーバにインストールされるソフトウェアモジュールである。TOEである。
- CAO 端末
  CAを遠隔操作するためのハードウェアであり、OS 、Trust-CANP V8.0i(CAO端末)がインストールされている。CAサーバとICカードリーダライタに接続される。
- Trust-CANP V8.0i(CAO 端末)
  CAの機能を実現するソフトウェアの一部で、CAO端末にインストールされるソフトウェアモジュールである。TOEである。
- HSM

CAの鍵対を生成、削除、バックアップするために用いるハードウェア。FIPS 140-2 レベル3 相当のハードウェアセキュリティモジュールであり、CAの鍵対に対してハードウェアの直接攻撃による暴露もしくは改ざんに耐える構造をもつ。

- IC カードリーダライタ
  CAO端末の操作者のICカードを読み書きするためのハードウェア。
- RA サーバ
  RAの機能を実現するソフトウェアがインストールされているサーバ。
- ディレクトリサーバ
  公開鍵証明書及びCRL をLDAPv3 準拠のディレクトリサービスを通して提供するサーバ。
- OS（CA サーバ）
  CAサーバにインストールされているオペレーティングシステムである。
- OS（CAO 端末）
  CAO端末にインストールされているオペレーティングシステムである。
- DBMS
  CAサーバにインストールされているデータベース管理ソフトウェアである。
- トランザクション処理ソフト
  CAサーバにインストールされているトランザクションソフトウェアである。サーバ用ソフトとクライアント用ソフトを対で利用する。
- HTTP サーバ
  CAサーバにインストールされている、SSL及びTLS通信用ソフトウェアである。CAサーバとの通信は、HTTPサーバを介して行われる。
- HSM ドライバ
  CAサーバにインストールされているソフトウェアである。HSMを用いてCAの鍵対の更新、削除及びバックアップする機能を備えている。
- IC カードリーダライタドライバ
  CAO端末にインストールされているソフトウェアである。ICカードを用いてCA管理者、CA操作者、監査人の署名を生成する機能を備えている。

TOEを含む電子認証システムは、PKIにおける以下のような認証サービスを提供する。これらのうち、下線を施した部分が本TOEの提供する機能である。

(1) 公開鍵の登録及び公開鍵証明書の発行

- 一般利用者は、RAに対して公開鍵証明書発行を申請する。
- RAは、その利用者の公開鍵と秘密鍵のペアを生成し、公開鍵証明書発行の申請書と公開鍵をCAへ送る。
- <u>CAは、申請書に基づいて公開鍵を登録し、報告書 (CAの署名が付与された公開鍵証明書を含む) を作成しRAへ戻す。</u>

・ RAから一般利用者に公開鍵証明書が渡される。

(2) 発行済み公開鍵証明書の失効

・ 一般利用者は、RAに対して公開鍵証明書失効を申請する。

・ RAは、一般利用者の申請に基づく申請書を作成し、CAへ送る。

・ CAは、申請に基づく処理を行い 、報告書を作成しRAへ戻す。

・ RAは、CAの処理結果を申請元の一般利用者へ渡す。

・ CAは、定期的に公開鍵証明書を検証し、失効した公開鍵証明書のリスト (CRL) を作成・発行する。

(3) 発行済みの公開鍵証明書及び公開鍵証明書失効リスト (CRL) のディレクトリサーバへの送信

・ CAは、発行した公開鍵証明書及び公開鍵証明書失効リスト (CRL) をディレクトリサーバへ送信する。

1.2.4 TOEの機能

TOEの操作者には、「CA管理者」、「CA操作者」、「監査人」、「CA鍵対管理グループ」が存在する。操作者やRAの登録はCA管理者が行う。操作者は、あらかじめCAサーバに公開鍵が登録され、これに対応する秘密鍵がICカードに入っており、その署名により認証される。RAは、あらかじめCAサーバに公開鍵が登録され、これに対応する秘密鍵で申請書へ署名し、その検証により認証される。以下に機能別に説明する。

(1) 申請書認証機能

RAから受信した申請書の署名を検証し、申請書の完全性を確認するとともに、登録されていた送付元のRAを認証する。

(2) 操作者認証機能

CAO端末から操作者のユーザIDと、操作者の持つICカードによる署名がCAサーバに送付され、識別認証が行われる。

(3) 申請書アクセス制御機能

識別認証に成功したCA管理者、CA操作者またはRAに対して、申請書による公開鍵証明書の発行・失効を許可する。公開鍵証明書テーブルが更新された後、公開鍵証明書または報告書が申請書の送信元へ返却される。

(4) 操作者アクセス制御機能

識別認証に成功したCA管理者またはCA操作者に対して、CRLの発行を許可す

る。公開鍵証明書テーブルは対象の証明書に対してCRL発行済情報が付加され、CRLテーブルが更新される。

(5) 運用支援機能

CA管理者に対し、以下の管理機能を提供する。

・CA操作者の登録・削除・変更

・RAの登録・削除・変更

・ログ設定ファイルの変更

CA管理者または監査人に対して、ログの検証・閲覧を許可する。鍵対の管理グループに対してCA鍵対の変更・削除・バックアップを許可する。

(6) 履歴管理機能

セキュリティ関連イベントのログを生成する。カレントログファイルに対してHASH署名を付加する。ログ設定ファイルにて設定される契機で、カレントログファイルを非カレントログファイルに移行し、CA秘密鍵による署名を付加する。

1.3 評価の実施

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セキュリティ認証申請等の手引き」[2]、「ITセキュリティ評価機関に対する要求事項」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「Trust-CANP V8.0i セキュリティターゲット 第９版」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOE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）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13][16]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「Trust-CANP V8.0i セキュリティターゲット　第９版　評価報告書」（以下「本評価報告書」という。）[22]に示されている。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。また、CC及びCEMの各パートは補足（[20] [20]のいずれか ）の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、本評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証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17年6月の評価機関による本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TOE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認証報告書を作成し、認証作業を終了した。

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、EAL2適合である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、物理的及び接続的に安全に保たれた環境に置かれている。また、攻撃は高度な専門知識を持たない低レベルの脅威エージェントを想定している。従って、TOEとして考慮すべき最小機能強度はSOF-基本で適切と判断された。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

- **申請書認証機能** SF.AUTH

  RAから受信した申請書を識別認証する機能。

  RAから受信した「申請書」内の情報を元に、RAの「DN」を識別する。「申請書」に付された署名を検証して、識別情報が正しいことを確認する。検証の際、署名に付された公開鍵証明書に基づき、鍵の有効期間、鍵種別、公開鍵証明書の失効情報を確認する。確認できない場合には、認証は不成功とな

り、エラーを示す報告書を作成する。鍵種別は、表1-1に示す署名アルゴリズムと鍵長に従う。このセキュリティ機能によって、CAO端末以外の経路からのアクセスは、識別認証されるまで、CAサーバに対していかなる操作もできない。

表1-1 CAサーバ用署名アルゴリズム

アルゴリズム	鍵長（bit）	標準
SHA1 with RSA	512～2048	PKCS#1
SHA1 with DSA	512～1024	FIPS186-2
SHA1 with ESIGN	576～2304	ISO14888-3

- **操作者認証機能**　SF.CAO_AUTH

CAO端末からログインする操作者を識別認証する機能。

CAO端末からICカードの署名とユーザID（あるいはグループID）を受け取り、ユーザID（あるいはグループID）によって操作者を識別し、ICカードの署名の検証によって、その識別情報が正しいことを確認する。検証の際、操作者の公開鍵証明書に基づき、鍵の有効期間、鍵種別を確認する。確認できない場合には、認証は不成功となり、エラーを示すメッセージを返す。このセキュリティ機能によって､CAO端末からのアクセスに対して識別認証されるまで、CAサーバに対していかなる操作もできない。検証の署名は、表1-2 に示す暗号アルゴリズムに従う。

表1-2 CAO端末用署名アルゴリズム

アルゴリズム	鍵長（bit）	標準
SHA1 with RSA	512～2048	PKCS#1

- **申請書アクセス制御機能**　SF.ACCESS_CONTROL

識別認証されたCA管理者、CA操作者もしくは識別認証されたRAに対して、申請書による公開鍵証明書の発行または失効を許可する機能。

CAサーバによってCA管理者、CA操作者もしくはRAが識別認証されると、CA管理者、CA操作者もしくはRAを代行するプロセスが生成される。CA管理者、CA操作者もしくはRAを代行するプロセスは、権限設定ファイルあるいはクライアント認証テーブルによって、公開鍵証明書テーブルに対して、表1-3 に示す操作に制限される。

公開鍵証明書発行の場合は、申請書の内容に従い公開鍵証明書を作成し、表1-１に示す署名アルゴリズム及び鍵長を元にHSMで生成されたCA署名を付す。公開鍵証明書失効の場合は、公開鍵証明書の状態を失効に更新し、失効が成功したことを示す報告書を作成する。その報告書には、上述と同様にCA署名を付す。

表1-3 申請者アクセス制御機能による公開鍵証明書テーブルのアクセス制御

役割	機能	操作対象	許可される操作
CA管理者	公開鍵証明書発行	公開鍵証明書テーブル	書込
	公開鍵証明書失効	公開鍵証明書テーブル	失効情報の更新
CA操作者	公開鍵証明書発行	公開鍵証明書テーブル	書込
	公開鍵証明書失効	公開鍵証明書テーブル	失効情報の更新
RA	公開鍵証明書発行	公開鍵証明書テーブル	書込
	公開鍵証明書失効	公開鍵証明書テーブル	失効情報の更新

- **操作者アクセス制御機能**　SF.CAO_ACCESS_CONTROL

  識別認証されたCA管理者、CA操作者に対してCRLの発行を許可する機能。

  CAサーバによって、操作者が識別認証されると、操作者を代行するプロセスが生成される。そのプロセスは、権限設定ファイルによって、公開鍵証明書テーブル、及びCRLテーブルに対して、表1-4に示す操作に制限される。

表1-4 操作者アクセス制御機能による公開鍵証明書テーブル、及びCRLテーブルのアクセス制御

役割	機能	操作対象	許可される操作
CA管理者	CRL発行	公開鍵証明書テーブル	読出、CRL発行情報の更新
		CRLテーブル	書込
CA操作者	CRL発行	公開鍵証明書テーブル	読出、CRL発行情報の更新
		CRLテーブル	書込

- **運用支援機能**　SF.PRIVILEGE

  TOEを運用するための操作を許可する機能。表1-5に示すとおり、役割に応じて操作を制限する。

表1-5　　役割ごとの管理権限範囲

役割	機能	操作対象	操作
CA管理者	ログ設定ファイルの変更	ログ設定ファイル	改変
	クライアント認証テーブルのDN、クラスの変更のとき	クライアント認証テーブル	登録、削除、改変
	権限設定ファイルのユーザID、グループID、許可される操作の変更のとき	権限設定ファイル	登録、削除、改変
	操作者の公開鍵証明書の登録	操作者の公開鍵証明書	登録
	ログの読出	ログ	読出
鍵対の管理グループ	CAの鍵対の管理操作	HSM内のCAの鍵対	更新、削除、バックアップ
監査人	ログの読出	ログ	読出

- **履歴管理機能**　SF.AUDIT

  履歴管理機能によって、TOEのセキュリティ事象に関わるログを記録し、CA管理者、監査人が必要に応じて記録した情報を閲覧することができる。記録対象となる事象詳細は、ST〔1〕の表6-6を参照のこと。

  記録された情報は、改ざんや削除を防ぐため、TOEによって2種類の署名が付与される。一つは、ハッシュ署名 (SHA-1) を用いログが生成されるごとにハッシュ署名が生成・付与される。他の一つは、IT環境のHSMを用いるCA署名である。HSMによってCA署名を行う契機毎に署名を行う。

1.5.5 脅威

本TOEは、表1-6に示す脅威を想定し、これに対抗する機能を備える。

表1-6 想定する脅威

識別子	脅 威
T.AUTH	TOEに登録されていないものが、IT機器を用いて、セキュアルーム外からネットワークを通して、TOEへ申請書を送信し、不正に資産を改ざんするかもしれない。
T.CAO_AUTH	セキュアルームに入室が可能な者が、CAO端末から不正にログインして公開鍵証明書発行等を行うかもしれない。
T.ACCESS_CONTROL	TOEに公開鍵証明書を発行、失効の許可をされていないものが、申請書を用いて、不正に公開鍵証明書を発行、失効するかもしれない。
T.CAO_ACCESS_CONTROL	CA操作者または監査人が、ログイン後、誤操作により権限外の操作を行うかもしれない。
T.COMMUNICATE	TOEの保護資産を改ざんしようとするものが、IT機器を用いて、次の通信路上の、次の保護資産に対して改ざんを行うかもしれない。 ・CAサーバとディレクトリサーバ間の通信路上の、公開鍵証明書あるいはCRL ・CAサーバとRA サーバの通信路上の、申請書あるいは報告書

1.5.6 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1-7に示す。

表1-7 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.AUDIT_DATA	TOEの生成するログは、改ざんや消去の検出が可能な状態で記録されなければならない。
P.MANAGEMENT	TOEを管理する組織の責任者は、予め組織内部セキュリティポリシーを決定し、実施すること。
P.RA_TRUST	TOEを管理する組織の責任者は、CA と同等のセキュリティポリシーを実施しているRA を登録すること。
P.PASSWORD	TOEを管理する組織の責任者及びCA 管理者は、CA に関するパスワードの安全性を保てるように、パスワードの運用規

	則を定め、実施すること。

1.5.7 構成条件

本TOEは、PKIにおけるCAを実現するソフトウェア製品である。本TOEが必要とするハードウェア／ソフトウェア環境の構成は、以下のとおりである。

ハードウェア: メモリ 1GB以上

ハードディスク 10GB以上

OS: Solaris8

1.5.8 操作環境の前提条件

本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、本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.PHYSICAL_PROTECT	TOEが動作するために必要なハードウェアは、入退管理されている場所に設置され、直接的な物理攻撃から保護されているものとする。また、サーバ及びHSMは施錠可能なサーバラックに配置し、直接的な操作から保護されているものとする。
A.HSM	HSMにてセキュアに管理されるCAの秘密鍵は、ハードウェアの直接的な物理攻撃によって暴露､改ざんされないものとする。
A.IC_CARD	正当な操作者が所有するICカードは、所有者が正当であることを確認できる情報を提供するものとする。
A.FIREWALL	CAサーバとセキュアルーム外との通信は、SSLもしくはTLS以外の通信を排除でき、DOS攻撃からも保護されているものとする。
A.NETWORK	CAサーバとCAO端末間の通信路の情報は、改ざんの無いものとする。
A.OPERATOR	操作者は､信頼されるものであり､ガイダンス文書に従ってCAの運用を行い、 ・自己の所有するICカードを他人に使わせない ・操作の途中、認められた操作者以外の者にCAO端末を操作させないものとする。
A.ADMIN	CA管理者は、細心の注意を払ってCAの運用を行い、誤った

	操作を行わないという点でも信頼できるものとする。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

- Trust-CANP V8.0i 運用マニュアル　第６版
- Trust-CANP V8.0i 構築マニュアル　第４版
- Trust-CANP V8.0i 概要書　第４版

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の保証要件について、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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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、本評価報告書による評価実施の履歴を示す。

評価は、平成16年12月に始まり、平成17年6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。また、平成17年3月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成17年4月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

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 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を表2-1に示す。

表2-1　開発者テストの構成

構成要素		テスト環境
ハードウェア構成		
	CA サーバ	GP500S Model1000 Memory：1GB、HDD：16GB
	HSM	nShield F3 UltraSign
	CAO 端末	IBM ThinkPad Memory：196Mbyte、HDD：20GB
	IC カードリーダライタ	Reflex USB V2.0
	IC カード	Cryptoflex
ソフトウェア構成		
	OS（CA サーバ）	Solaris8 2/02
	OS（CAO 端末）	Windows2000 Professional SP4
	DBMS	Oracle Enterprise Edition8.1.7.3
	トランザクション処理ソフト	OpenTP1 Server Base 05-00 OpenTP1 Client/W 05-00
	HTTP サーバ	Apache 1.3.33 (CANP 用) Apache 1.3.33 (NOAA 用)
	HTTP サーバ用暗号プロトコル接続モジュール	mod_SSL 2.8.22-1.3.33
	HTTP サーバ用暗号プロトコルソフト	OpenSSL 0.9.6m
	HSM ドライバ	HSMソフトウェアDevelopmentkit S5.30
	IC カードR/W ドライバ	Cyberflex Access Software Developmentkit 4.4
	IC カードR/W ドライバ	Cyberflex Access Software Developmentkit 4.4
周辺機器		
	ファイアウォールサーバ	TOEの動作に影響を与えるものではなく、また、今回は外部からの攻撃はないものとしてテストを行う為、今回の試験環境では構築しない。
	RA サーバ	Sun Blade100 Memory：1GB、HDD：16GB、Trust-KMS V8.0が動作可能
	ディレクトリサーバ	RAサーバと同居。LDAP V3 に準拠しているソフトウェアが動作可能である。

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を表2-1に示す。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

・機能仕様書に記述されている機能を網羅的に確認する。ただし、個々の機能を単独で確認できないものは、一連の流れ（例えば、公開鍵登録申請など）で、最終的に正しい結果が得られることで、確認できたものと判断する。

・対応する全てのテストが完了したとき、確認項目の完了を意味する。確認する項目がTSFI の場合は、確認項目以外にメッセージとログを確認する。また、公開鍵証明書発行及び公開鍵証明書失効の場合は、申請書と報告書（または公開鍵証明書）の署名と、署名と対応する公開鍵証明書を確認する。

c.実施テストの範囲

テストは開発者によって13種類69件実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を表2-1に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

セキュリティ機能毎にTSFI を操作することにより、あるいはセキュリティ機能に関する一連の流れを実行し、対応するふるまいを直接観察、あるいはログによって間接的に観察し、期待とおりの動作であることを確認する。

c.実施テストの範囲

評価者が独自に考案したテストを1項目、開発者テストのサンプリングによるテストを13項目、計14項目のテストを実施した。テスト項目の選択基準として、

下記を考慮している。

① 開発者が実施した13項目のシナリオは全て網羅する

② 履歴管理機能に関する追加のテスト

侵入テストは、開発者が考慮していない明白な脆弱性が存在しないかの確認のため、5項目のTOEとTOEの環境全体を対象とするテストが実施された。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

本評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断した。

3 認証実施

評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

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をサンプリングし、その内容を検査し、関連するワークユニッ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に適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、本ST及び本評価報告書において、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 **認証結果**

提出された本評価報告書、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、本TOEがCCパート3 ([7][10][13][16]のいずれか) のEAL2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エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
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種別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘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。
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明記され、それらが脅威、組織のセキュリティ方針、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。
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。
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。
構成管理	**適切な評価が実施された**
ACM_CAP.2.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。

配付と運用	適切な評価が実施された
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであ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。
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。
ADV_HLD.1.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.1.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。

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り、上位レベル設計が機能仕様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。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確に対応していることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果が含まれておりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。

ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

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	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

本報告書で使用された用語を以下に示す。

CA	Certificate Authority の略。認証局と訳され、公開鍵証明書を発行する。
CAO 端末	Certificate Authority Operator 端末の略。CAを操作するために用いられる端末。
CRL	Certificate Revocation List の略。公開鍵証明書失効リストとも表す。失効された一般利用者の公開鍵証明書をまとめたリストに、発行したCA署名が付与されているもの。登録されている公開鍵証明書は有効でないことを示す。
DN	Distinguished Name の略。ディレクトリ・ツリー上でエントリを一意に識別するための名前である。
HSM	Hardware Security Module の略。鍵対を保存するために用い、保存されている鍵対を守るために耐タンパ性である。
LDAP	The Lightweight Directory Access Protocol の略。ディレクトリサーバに情報を通知するためのプロトコル。

PKI	Public Key Infrastructure の略。公開鍵インフラと呼ばれ、おもにX.509 及びPKIX が定めるRFC文書によるものをさす。
RA	Registration Authority の略。登録局と呼ばれ、一般利用者の公開鍵をCAに登録する業務を担う。
クラス	公開鍵証明書の発行及び失効などの権限を記述したもの。そのクラスに属するDNは、そのクラスに記述され権限を実行できる。
公開鍵証明書	X.509v3 で定義された公開鍵を含む証明書。
セキュアルーム	許可された人のみが入退できる物理的制限を設けかつ入退記録を残せる部屋
ディレクトリサーバ	X.509 形式の公開鍵証明書を含む、X.500 で定義された誰でも利用可能なディレクトリ。
パスワード	OS(CAサーバ及びCAO 端末)及びDBに対しての識別認証のためのパスワード。

6 参照

[1] Trust-CANP V8.0i セキュリティターゲット　第９版（2005年5月17日）日本電信電話株式会社 情報流通プラットフォーム研究所

[2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人情報処理推進機構 ITQM-23

[3] ITセキュリティ評価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-07

[4] ITセキュリティ認証申請者・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-08

[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] CCIMB Interpretations-0407

[21] 補足-0210　第２版、補足-0407

[22] Trust-CANP V8.0i 評価報告書 第2.1版 2005年6月3日
株式会社電子商取引安全技術研究所　評価センター