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 6 月13日（ST確認2009）
ＳＴ確認申請者	日本電信電話株式会社
ＳＴの名称	Trust-CANP v6.1 Security Target バージョン1.2.8
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	日本電信電話株式会社
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16年3月16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 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
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

Trust-CANP v6.1 Security Target バージョン1.2.8 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、「Trust-CANP v6.1 Security Target バージョン1.2.8」（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信電話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［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: Trust-CANP
- バージョン: 6.1
- 開発者: 日本電信電話株式会社

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サービスを提供する。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 (Certification Authority Operation) 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

本製品は、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。

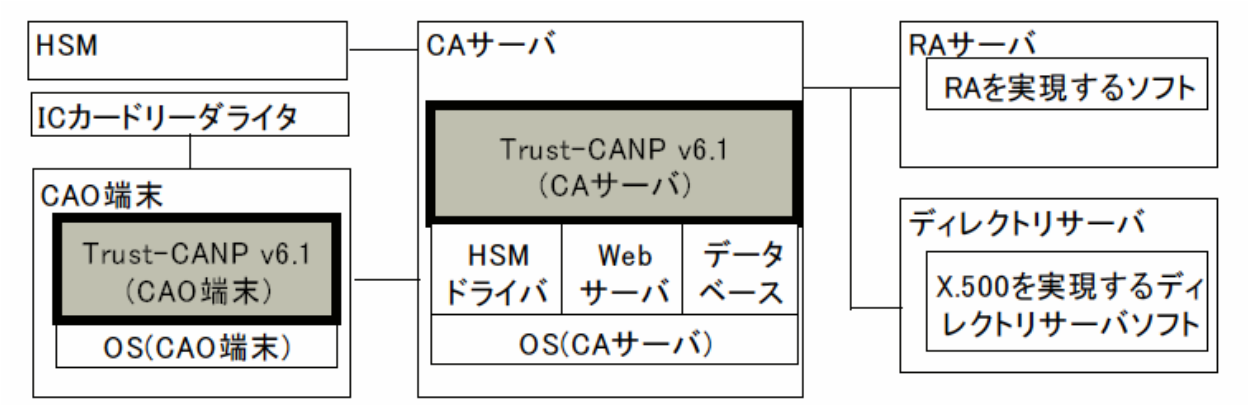

図1-1　　TOEの範囲

1.2.4 TOEの動作概要

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 (RFC2510/RFC2797準拠) 」と公開鍵をCAへ送る。
- CAは、申請書に基づいて「報告書 (RFC2510/RFC2797準拠) 」 (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。
- RAから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、失効禁止、失効禁止解除

- 一般利用者は、RAに対して公開鍵証明書失効・公開鍵証明書失効禁止・公開鍵証明書失効禁止解除のいずれかを申請する。
- RAは、一般利用者の申請に基づく「申請書 (RFC2510/RFC2797準拠) 」を作成し、CAへ送る。
- CAは、申請に基づく処理を行い 、「報告書 (RFC2510/RFC2797準拠) 」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。

1.3 評価実施

Trust-CANP v6.1 Security Target 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。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16年2月の評価実施機関による「ST評価報告書 2版 2004年2月17日」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TOEに要求される最小機能強度レベルは、SOF-基本である。最小機能強度レベルは、TOEの確率的・順列的メカニズム部分に対して適用される。本TOEにおいて確率的・順列的メカニズムに相当するものは、署名アルゴリズムの一部で用いられるハッシュ暗号アルゴリズムである。

1.4.4 セキュリティ機能

本TOEは、以下に示すTOEセキュリティ機能 (以下、TSFと記す。) を持つ。このTSFによって、STの第5章に記載されたセキュリティ機能要件が実現される。

- **SF.CAO_OPERATE 端末操作機能**

  CAO端末を操作してCAサーバのサービスを利用する際のTOEセキュリティ機能。以下の二つの機能がある。

  - CAサーバログイン: CAO端末に入力したユーザID (あるいはグループID) に、利用者のICカードが生成する署名を付してCAサーバへ送る。このICカードは、TOEには含まれない。CAサーバは、送られたデータによって利用者の識別・認証を行う。署名アルゴリズムは、表1-1に示すもののいずれかを選択できる。
  - 「申請書」作成: CAO端末上で申請書を作成した場合、利用者のICカードによって署名を生成し、申請書に付与してCAサーバへ送る。CAサーバは、この署名を用いて申請書データの伝送途中での改ざんを検出できる。署名アルゴリズムは、表1-1に示すもののいずれかを選択できる。

表1-1　　署名アルゴリズム

アルゴリズム	鍵長（bit）	標準
SHA1 with ESIGN	576〜2304	FIPS 186-2 + ISO14888-3
SHA1 with RSA	512〜2048	PKCS#1
MD5 with RSA	512〜2048	PKCS#1
SHA1 with DSA	512〜1024	FIPS 186-2

- **SF.CAO_AUTH 操作者認証機能**

  CAサーバがCAO端末からログインする操作者を識別・認証する機能。CAサーバは、以下のような機能を提供する。

  ・ CAO端末から署名が施されたユーザID (あるいはグループID) を受け取り、IDによって操作者を識別し、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、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、CRLとの対応を併せて確認する。

  ・ このセキュリティ機能は、セキュリティ機能要件FIA_UID.2、FIA_UAU.2を満たすものなので、RAの識別・認証が成功するまで、RAは、このセキュリティ機能を除き、TSFが介在する一切のTOE機能を利用できない。

- **SF.RA_AUTH クライアント認証機能**

  CAサーバがRAからサービス要求を受け付けるときに相手を識別・認証する機能。CAサーバは、CAO端末以外から「申請書」を受信したとき、以下のようにして送信した相手がRAであることを識別し、認証する。

  ・ CAO端末以外で「申請書」をCAサーバへ送信するのは、RAである。CAサーバは、「申請書」内の識別情報情報から、相手がRAであることを識別し、「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、CRLとの対応を併せて確認する。

  ・ このセキュリティ機能は、セキュリティ機能要件FIA_UID.2、FIA_UAU.2を満たすものなので、操作者の識別・認証が成功するまで、利用者は、このセキュリティ機能を除き、TSFが介在する一切のTOE機能を利用できない。

- **SF.ACCESS_CONTROL アクセス制御機能**

  TOEのセキュリティ機能SF.CAO_AUTH (操作者認証機能)、SF.RA_AUTH (クライアント認証機能) によってCAサーバに利用者が識別・認証されると、CAサーバ中にその利用者を代行するプロセスが生成さ

れる。そのプロセスは、TOEでユーザデータが出入りする以下のオブジェクトにアクセスする。アクセスの可否は、利用者及びオブジェクトの種別に対応するセキュリティ属性に基づいて決定される。SF.ACCESS_CONTROLにおけるアクセス制御規則は、表1-2に示すとおりである。

表1-2　　アクセス制御の規則

<table>
<tr><th>オブジェクト＼利用者</th><th>CA管理者・操作者</th><th>RA</th><th>監査人</th></tr>
<tr><td>申請書テーブル</td><td colspan="2" rowspan="3">書込み[*1]・読出し許可</td><td rowspan="6">アクセス不可</td></tr>
<tr><td>公開鍵証明書テーブル</td></tr>
<tr><td>報告書テーブル</td></tr>
<tr><td>CRLテーブル</td><td>書込許可</td><td rowspan="3">アクセス不可</td></tr>
<tr><td>CAO端末への送信ポート</td><td>送信許可</td></tr>
<tr><td>CAO端末からの受信ポート</td><td>受信許可</td></tr>
<tr><td>RAへの送信ポート</td><td rowspan="2">アクセス不可</td><td>送信許可</td></tr>
<tr><td>RAからの受信ポート</td><td>受信許可</td></tr>
</table>

*1: 公開鍵証明書テーブルに関しては、公開鍵証明書失効、公開鍵証明書失効禁止、公開鍵証明書失効禁止解除を行う場合、「更新」と読み替える。

- **SF.PRIVILEGE 運用支援機能**

TOEの管理権限を持つ役割の権限範囲を表1-3のように規定する。

表1-3　　役割ごとの管理権限範囲

役割	操作対象	許可される操作
CA管理者	アーカイブ及びログに対してCA署名を行う周期	改変
	複数人操作が必要なCA鍵対の管理操作に必要な人数	改変
	利用者情報テーブルのユーザID、グループID、登録ID、操作者/RAの公開鍵証明書	登録、削除
	ロールテーブルのロールと登録ID	登録、削除
CAの鍵対管理用複数人操作者	HSM内のCAの鍵対	生成、削除、バックアップ、リストア
監査人	アーカイブ、ログ	閲覧

- **SF.AUDIT 履歴管理機能**

SF.AUDIT機能によって、TOEのセキュリティ事象に関わるアーカイブ、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の表6-4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) を用いるもので、アーカイブ、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。これは、ハッシュ署名にくらべて処理上の負荷が大きいため、事象の発生ごとでなく定期的なスケジュールで実行される。

1.4.5 脅威

本TOEは、以下の脅威に対して対抗策を講じている。

- **T.AUTH1**

  操作者が、自分以外のユーザIDもしくは自分が属さないグループIDを用いて、自身の所有するICカードによって署名し、CAO端末からTOEに不正ログインして、TOEの保護資産を改ざんまたは暴露するかもしれない。

- **T.AUTH2**

  外部の専門知識のない悪意をもった者が、操作者のユーザIDもしくは操作者の属するグループIDを用いて、TOEに登録外のIC カードによって署名し、CAO端末からTOEに不正にログインして、TOEの保護資産を改ざんまたは暴露するかもしれない。

- **T.ACCESS_CONTROL1**

  正当な監査人が、申請書を用いて、不正に証明書を発行、失効するかもしれない。

- **T.ACCESS_CONTROL2**

  正当な監査人が、コマンド操作を用いて、CRLを更新するかもしれない。

- **T.AUDIT_DATA**

  CA管理者が、誤操作によりアーカイブまたはログに対して改ざんもしくは削除を行うかもしれない。

- **T.RA**

  外部の専門知識のない悪意ある者が、IT機器を用いて、セキュアルーム外からTOEへ申請書を送信し、不正にTOEに侵入するかもしれない。

- **T.COMMUNICATE**

  外部の専門知識のない悪意ある者が、IT機器を用いて、下記の通信路上で、下記の保護資産に対して改ざんまたは暴露を行うかもしれない。

  ・ CAサーバとCAO端末間の通信路上で、申請書あるいは報告書に対して。

・ CAサーバとディレクトリサーバ間の通信路上で、公開鍵証明書あるいはCRLに対して。
・ CAサーバとRAサーバの通信路上で、申請書あるいは報告書に対して。

1.4.6 組織のセキュリティ方針

本TOEに関連する組織のセキュリティ方針を以下に示す。これらのセキュリティ方針には、TOEによる対処が必要なものは含まれていず、すべて運用・管理手段によって対処されるものである。本TOEをセキュアに運用・管理するには、これらの組織のセキュリティ方針がすべて正しく実行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、セキュリティポリシーを実施すること。

- **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、パスワード運用規則を定めること。

- **P.DB＆OS**

  TOE を管理する組織の責任者及びCA 管理者は、データベース及びOS が不正にアセスされることのないようにしなければならない。

1.4.7 構成条件

本TOEをセキュアに使用するためには、TOE (ソフトウェア) をインストールするコンピュータ、TOEに接続される各種機器、ネットワーク、協働するサーバの構成などが特定の条件を満たしたものでなければならない。詳細については、2.1章を参照のこと。

1.4.8 動作環境の前提条件

本TOEの使用環境に関わる前提条件を以下に示す。TOEのセキュアな運用・管理の

ため、これらの前提条件がすべて満たされねばならない。

- **A.PHYSICAL_PROTECT**

  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のすべては、操作者のみに入出が制限され、かつ入出記録が残せるように管理された同一のセキュアルームに設置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であり、HSM からTOE に送られてくる情報は信頼できるものとする。

- **A.IC_CARD**

  正当な操作者はPIN 認証機能を持ったIC カードを所有し、PIN によって本人であることを確認でき、そのIC カードからIC カードリーダライタを介して、TOE に送られてくる情報は信頼できるものとする。

- **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 攻撃から保護されているものとする。

- **A.UTILITY**

  TOE が機能するために必要なハードウェア製品及びソフトウェア製品は、製品仕様通りに機能するものとする。

- **A.ADMIN**

  CA 管理者は、TOE を管理する組織のセキュリティポリシーに従って操作することとし、信頼されているものとする。

- **A.OPERATOR**

  CA 操作者は、TOE を管理する組織のセキュリティポリシーに従ってTOE を操作するものとする。

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

1.1 TOE及び外部環境構成

本TOEは、CAサーバとCAO端末に搭載されるソフトウェア (アプリケーションプログラム) であり、前述の図1-1に示すIT環境のコンポーネント及び他の装置と共に使用される。TOEを構成するコンポーネント、IT環境のコンポーネント、及び関連する他の装置のリストと構成条件を以下に示す。

- TOEを構成するソフトウェアコンポーネント
  - Trust-CANP v6.1 (CAサーバ内)
  - Trust-CANP v6.1 (CAO端末内)
- IT環境のソフトウェア/ハードウェアコンポーネント
  - データベース: データベース管理ソフトウェア (Oracle8iEnterprise Edition R8.17) で、CAサーバにインストールされる。
  - Webサーバ: SSL/TLS通信ソフトウェア (Apache 1.3.21) で、CAサーバにインストールされる。
  - HSMドライバ: HSMを使用するためのソフトウェア (nShield SCSI 300用ドライバ) で、CAサーバにインストールされる。
  - OS: CAサーバのOS (Solaris 8) 及びCAO端末のOS (Microsoft Windows 2000 Professional Service Pack 2)。
  - CAサーバハードウェア: Solaris 8が動作するコンピュータで、主メモリ1GB以上、ハードディスクドライブ容量20GB以上のもの。
  - CAO端末ハードウェア: DOS/Vマシンで、主メモリ256MB以上、ハードディスクドライブ容量1GB以上のもの。
  - HSM: CA鍵の生成、削除、バックアップ、リストアを行うハードウェアで、CAサーバに接続される。
  - ICカードリーダライタ: CAO端末操作者のICカードを読み書きするハードウェアで、CAO端末に接続される。
  - ICカード: CAO端末操作者の秘密鍵、PINを格納するICカード。
  - ファイアウォールサーバ: TOE及びIT環境を構成する装置と外部ネットワークとの接続点に置かれ、SSL/TLSプロトコルのパケットだけを通過させる。

- 関連する他の装置

  - RAサーバ: RA機能を提供するサーバで、ネットワークを介してTOEと接続される。TOE評価を行う際には、Trust-KMS v6.1がインストールされたサーバを用いる。

  - ディレクトリサーバ: ネットワークを介してTOEに接続され、TOEが発行する公開鍵証明書及びCRLをLDAP v3準拠のディレクトリサービスに基づいて提供する。TOE評価を行う際には、Critical Path InJoin Directory Server version 4.0がインストールされたサーバを用いる。

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[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、所見報告書およ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調査した結果、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エレメントについての確認結果を表4-1にまとめる。

表4-1　評価者アクションエレメント調査結果

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。

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適合を明確に述べ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、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。

注意事項

本TOEは、スタンドアロン型ではなく、RAサーバやディレクトリサーバなどの外部装置と共に使用され、かつ、設置環境の物理的セキュリティも重要である。TOEの管理

者は、IT環境を含め、全体としてのセキュリティを確保できる運用管理を行うよう配慮すべきである。

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

本報告書で使用された用語の定義を以下に示す。

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	Certification 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。
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。
PIN	Personal Identification Numberの略。利用者を識別するために必要な番号パスワード。
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。
公開鍵証明書	X.509v3で定義された公開鍵を含む証明書。
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 v6.1, Security Target バージョン1.2.8 日本電信電話株式会社

[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 2版 2004年2月17日 ACY-ETRST-0002-00/個別評価報告書 Security Target ASE 2版 2004年2月17日 ACY-EST-0002-00