認　証　報　告　書

評価対象

申請受付年月日（受付番号）	**平成15年10月15日（IT認証3014）**
認証申請者	**株式会社日立製作所**
TOE**の名称**	Enterprise Certificate Server Set
TOE**のバージョン**	01-01-A
PP**適合**	**なし**
適合する保証要件	EAL3
TOE**開発者**	**株式会社日立製作所　ソフトウェア事業部**
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16年7月21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 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 Version 1.0
⑥ CCIMB Interpretation-0210
⑦ 認証機関が公開する③、⑤及び⑥の翻訳文書

評価結果：合格

「Enterprise Certificate Server Set 01-01-A」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、「Enterprise Certificate Server Set 01-01-A」（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株式会社日立製作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:	Enterprise Certificate Server Set
バージョン:	01-01-A
開発者:	株式会社日立製作所　ソフトウェア事業部

1.2.2 製品概要

Enterprise Certificate Server Set（以下ECS Setと記す）は、国際標準X.509に準拠した証明書の発行及び失効を管理する認証局（CA：Certificate Authority の略）ソフトウェア製品であり、証明書発行サーバ機能を提供するCAサーバとリモートから管理を行う管理端末を用いて、証明書の発行管理を行う。

1.2.3　　TOEの範囲と動作概要

(1) TOEの範囲

本TOEは認証局で使用されることを前提としたソフトウェア製品である。認証局を利用した、認証局システムの全体像を図1-1に示す。ECS Setは図1-1の網掛けの認証局（CA）内で動作し、国際標準X.509に準拠した証明書の発行及び証明書失効リストを生成、発行し、これの管理を行う。

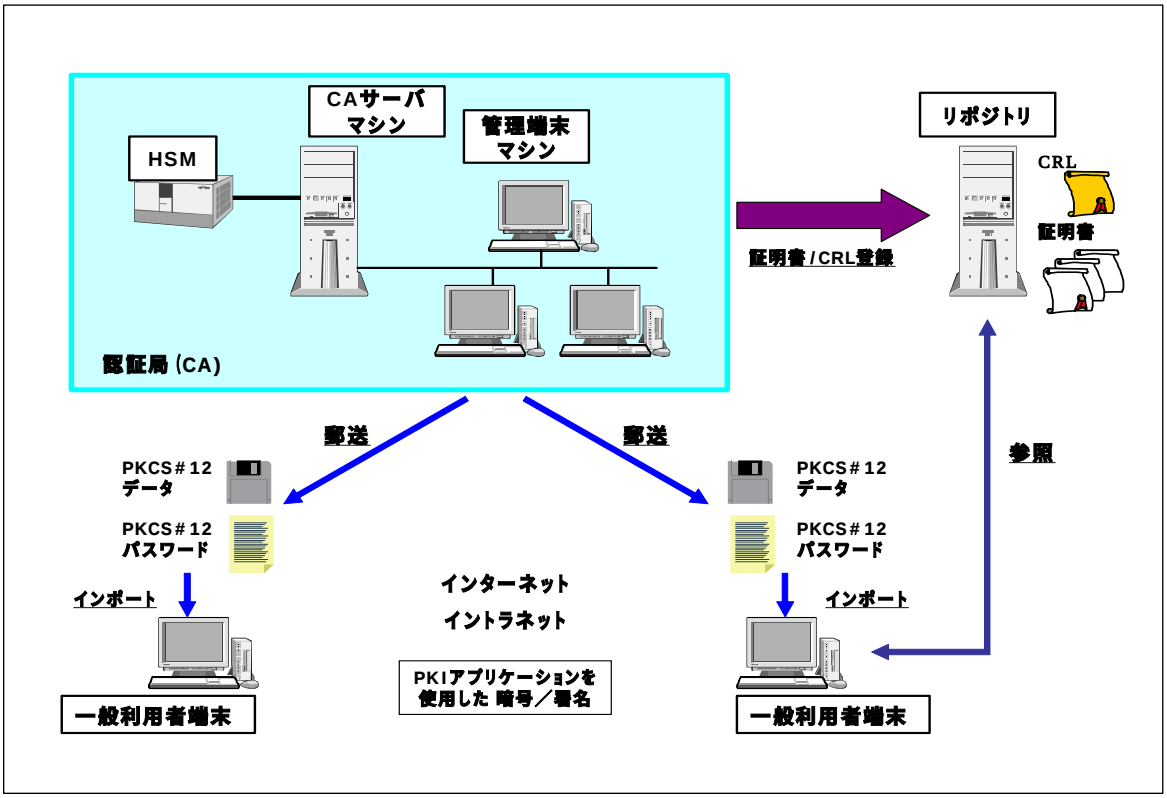

図1-1 認証局を利用した認証局システムの全体像

図1-1内の網掛けの認証局（CA）内で動作する、本TOEであるECS Setを用いた認証局のシステム構成例を図1-2に示す。図1-2では、「CAサーバマシン」中にTOEの「CAサーバ」ソフトウェアが位置し、「管理端末マシン」上にTOEの「管理端末」ソフトウェアが位置する。認証局システムを構成するには、本TOE以外に図1-2に示すような装置を必要とするが、TOEとして定義したソフトウェア以外のすべてのハードウェア、ソフトウェア、ファームウェアは、TOEに含まれない。TOEは、図1-2の網掛けにて示したCAサーバマシンと管理端末マシンにインストールされ動作する。

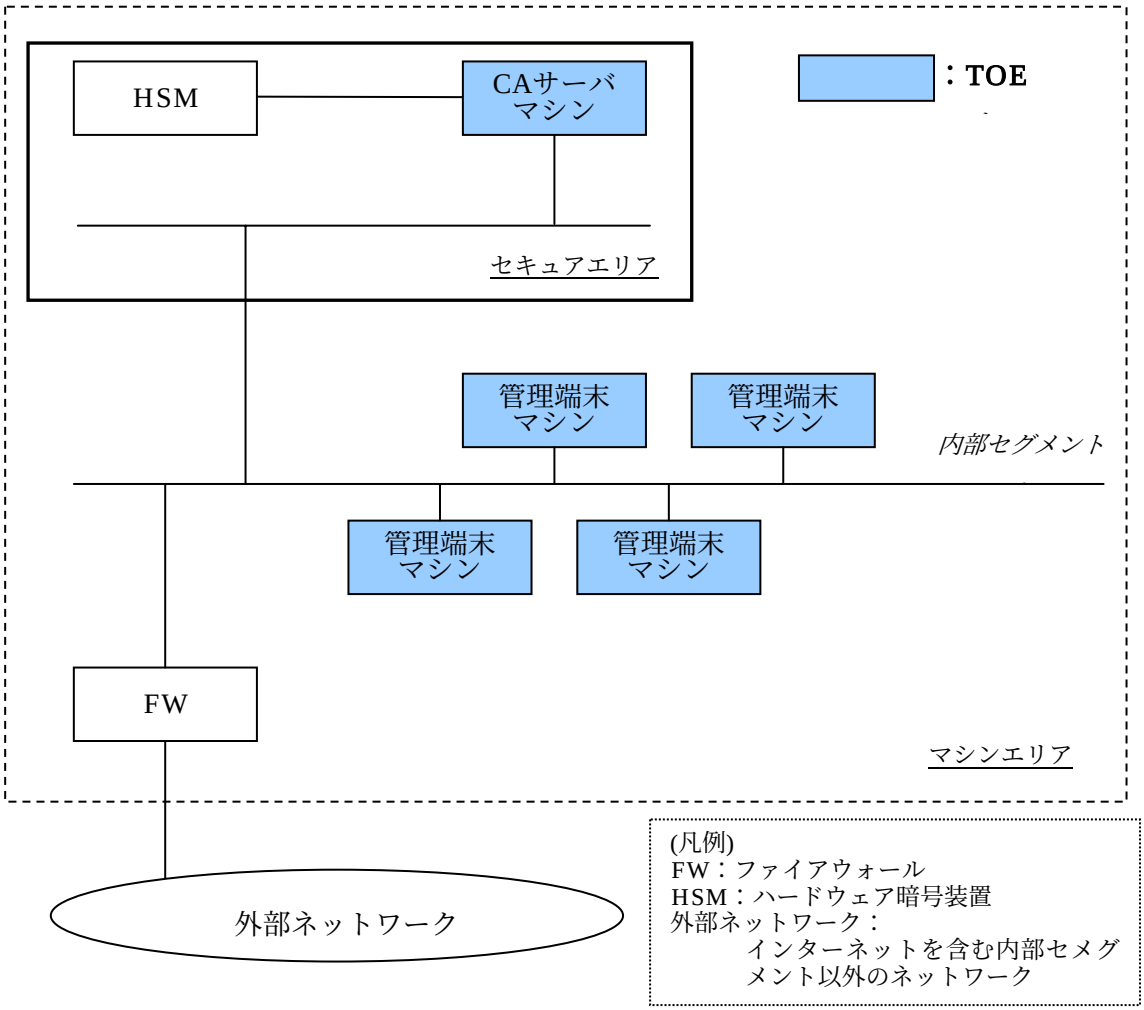

図1-2 ECS Setを用いた認証局のシステム構成例

図1-2における、機器やエリア等を以下に説明する。

1) CAサーバマシン

TOEであるECS Setのサーバソフトウェア（CAサーバ）が動作する。

2) 管理端末マシン

TOEであるECS Setのクライアントソフトウェア（管理端末）が動作する。

3) HSM

CA秘密鍵が格納されており、CA秘密鍵を使用した署名などの暗号操作を行う。CAサーバマシンに接続される。TOE外であり、IT環境として利用する。

4) 内部セグメント

マシンエリア内に設置され、CAサーバマシン、管理端末マシン、ファイアウォールがEthernetを使用して接続されるネットワーク。内部セグメントは、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は拒否されるように設定されている。

5) セキュアエリア

CAサーバマシン、HSMが設置される。セキュアエリアには、TOEの動作に関係しない機器は設置されない。入退室管理が行われ、不正な物理的アクセスから保護されている。セキュアエリアには、CA管理者のみ入室することができる。

6) マシンエリア

認証局内に設置されたマシン室であり、管理端末マシン、ファイアウォールが設置される。マシンエリアには、認証局に属する者のみ物理的にアクセスすることができる。

※）CA管理者、認証局に属する者については、項番1.2.4を参照。

(2) TOEの動作概要

TOEは、図1-1の認証局（CA）内においてCAのサービスの中核となる機能を提供する。TOEが提供する機能を以下に示す。

・一般利用者 (以下EEと記す) の公開鍵・秘密鍵のペアを生成する。
・EEの公開鍵にCAの秘密鍵で電子署名を施し、公開鍵証明書 (EE証明書) として発行する。
・EE証明書及びEEの秘密鍵をペアとして、EEのPKCS#12パスワードをもとに、PKCS#12形式で暗号化したPKCS#12データを生成する。
・EE証明書を失効させ、EE証明書失効リスト(以下CRLと記す) を発行する。

また、TOEは上記で生成、発行されたデータを一般利用者へ送付及びリポジトリへの登録をするために、以下の機能を提供する。

・EE証明書及びCRLをリポジトリに登録するために、EE証明書及びCRLを取得する。
・PKCS#12データを一般利用者に送付するために、PKCS#12データを取得する。
・PKCS#12パスワードを一般利用者に送付するために、PKCS#12パスワードを取得する。

※）一般利用者（EE）は、EE証明書及びCRLを利用する者のことをいう。一般利用者は、本TOEに直接アクセスすることはないため、TOE外である。

1.2.4 TOEの機能

証明書の発行管理は、国際標準X.509に準拠した証明書の発行及び失効を管理する機能を提供するCAサーバと、リモートから管理を行う管理端末を用いて行われる。

TOEが提供する機能及びセキュリティ機能を表1-1に示す。

TOEのセキュリティ機能は、利用者データの保護が主目的である。保護対象資産となる利用者データを以下に示す。なお、保護対象資産となる利用者データは、図1-2に示したCAサーバおよび管理端末の利用者データが対象となる。

・EE証明書: EEの公開鍵に**認証局**が署名を施したもの
・PKCS#12データ: EE証明書とEE秘密鍵をPKCS#12パスワードをもとにPKCS#12形式で暗号化したもの
・PKCS#12パスワード
・CRL
・CRL発行定義文: CRL発行に必要な情報を定義したもの

表1-1 TOEが提供する機能及びセキュリティ機能

機能名称	機能内容
証明書発行及び管理機能	EE証明書の発行と管理
CRL発行及び管理機能	CRLの発行と管理
監査機能 （セキュリティ機能）	認証局の監査に必要な監査ログ情報の記録、保護、表示、管理機能
暗号機能 （セキュリティ機能）	次の暗号処理機能 ・秘密情報格納ディレクトリ暗号化 以下の情報を暗号化して保管する。 CA設定情報 DBデータ暗号鍵 監査ログ用証明書・監査ログ用秘密鍵 秘密情報暗号鍵 ・監査ログへの署名・暗号化及び検定・復号 ・DB暗号化 DBに格納されたデータのうち、以下の情報を暗号化して保管する。 PKCS#12データ PKCS#12パスワード ECS利用者パスワード ・通信路暗号化 管理端末とCAサーバの間の通信路を流れるデータを暗号化する。
アクセス制御機能 （セキュリティ機能）	利用者データに対するアクセス制御及び利用者データに関する操作における合議機能
識別・認証機能 （セキュリティ機能）	ECS利用者の識別・認証機能
CA情報管理機能 （セキュリティ機能）	CAサーバの動作設定機能及びECS利用者情報管理機能(合議機能が適用される)

本TOEにおける、TOEを構築、運用、管理に関連する、TOEの関連者は以下の者を想定する。

(1) システム構築者

CAサーバ、管理端末及び周辺機器などTOE及びTOEのIT環境のシステム構築を行う。システム構築後は、CA管理者がTOEの管理を行う。システム構築者は、システムの構築時には、セキュアエリア、マシンエリアに立ち入ることができるが、システム構築後は、CA管理者に引継ぎを行い、以降TOEにアクセスすることはできない。

(2) CA管理者

CA管理者は、システム構築直後、認証局のサービスを稼動させるために、認証局サービスにおける、TOEの各機能の設定や管理を行う。CA管理者は、セキュアエリア、マシンエリアに立ち入ることを許可されている。

(3) 運用者

運用者は、管理端末を利用して、証明書の発行／失効等の運用業務を行う。運用者は、マシンエリアに立ち入ることは許可されているが、セキュアエリアに立ち入ることを許可されていない。

(4) 監査者

TOEが生成する監査ログの分析等の監査業務を行う。監査者は、マシンエリアに立ち入ることは許可されているが、セキュアエリアに立ち入ることを許可されていない。

(5) 認証局に属する者

TOEを運用する組織に属する者。CA管理者、運用者、監査者は認証局に属しているが、システム構築者は、認証局には属していない。認証局に属する者には、TOEへのアクセスが許可されたECS利用者とTOEへのアクセスが許可されていない者がいる。認証局に属する者のうち、TOEへのアクセスが許可されていない者も、マシンエリアへの入退室は行うことができる。

※）ECS利用者

CA管理者、運用者、監査者を総称してECS利用者という。

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 (平成14年4月)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「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14年4月)」[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「Enterprise Certificate Server Set セキュリティターゲット Version 1.10」（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、「2004年7月5日評価報告書 DTT-ETR-0001-02」（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][21]）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16年7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、EAL3である。

1.5.3 セキュリティ機能強度

本TOEは、最小機能強度としてSOF-基本を主張する。

CAサーバマシン及びHSMは、セキュアエリア内に設置され、入退室管理が行われており、また、管理端末マシンは、認証局内のマシンエリア内に設置されているため、外部の者が侵入して行う物理的な攻撃からは、保護されている。CAサーバマシン、管理端末マシンが接続される内部セグメントは、ファイアウォールによりインターネットからのアクセスを禁止しているため、不特定の利用者から攻撃される可能性はない。攻撃者としては、認証局を運用する組織の管理下にある、認証局に属する者を想定しているため、攻撃に対する動機及び機会が少ない脅威エージェントである。従って、最小機能強度レベルは、SOF-基本が妥当であるといえる。

1.5.4 セキュリティ機能

本TOEは、以下に示すセキュリティ機能を持つ。

(1) 監査機能 (SF.AUDIT)

セキュリティ機能の動作を監査ログとして記録する。記録された監査ログは、権限を持つECS利用者 (すなわち監査者) が読み出せる。

(2) 暗号機能 (SF.CRYPTO)

利用者データやTSFデータを保護するため、それらデータの暗号化/復号を行う。対象とするデータによって、各種の暗号機能を使い分ける。対象となるデータとそれに適用される暗号の種類と適用場面を表1-2に示す。

表1-2 対象となるデータとそれに適用される暗号の種類と適用場面

対象データ	データの種別	暗号アルゴリズム	適用場面
PKCS#12データ	利用者データ	MULTI2(ISO/IEC 9979/0009)	DBアクセス時
PKCS#12 パスワード			
ECS利用者 パスワード	TSFデータ	SHA-1 (FIPS 180-1)	

CAサーバ・管理端末間通信データ	利用者データ/TSFデータ	MULTI2(ISO/IEC 9979/0009)	CAサーバ･管理端末間通信時 (LAN経由)
CAサーバ・管理端末間通信データ暗号化の通信路暗号鍵	TSFデータ	RSA (PKCS#1)	通信路暗号鍵交換時
CA設定情報	TSFデータ	Triple-DES (FIPS 46-3)	秘密情報格納ディレクトリへ格納時に「秘密情報暗号鍵」で暗号化/復号。(鍵は、TOE運用開始時にCA管理者が生成。)
DBデータ暗号鍵			
監査ログ用証明書			
監査ログ用秘密鍵			
秘密情報暗号鍵	TSFデータ	PBE (PKCS#5)	秘密情報格納ディレクトリアクセスに使用する「秘密情報暗号鍵」の暗号化/復号。(ECS起動時に使われるECS起動パスワードを鍵として暗号化。)
監査ログ	TSFデータ	Triple-DES (FIPS 46-3)	監査ログ暗号化/復号
		RSA (PKCS#7)	監査ログ署名/検定
		SHA-1 (FIPS 180-1)	監査ログ署名/検定(ハッシュ)

(3) アクセス制御機能 (SF.AC)

利用者データに対するECS利用者のアクセスを管理する。以下の操作に関して、複数のECS利用者による合議操作が必要となる。 (合議操作に必要な人数の設定は、以下の(5)で説明する。)

- EE証明書削除
- EE証明書失効
- PKCS#12データ作成
- CRL作成
- CRL削除
- CRL発行定義文登録
- CRL発行定義文削除

(4) 識別・認証機能 (SF.I&A)

ECS利用者の正当性を確認するため、利用者の識別・認証を行う。利用者の識別は利用者IDで、認証はパスワードによって行う。利用者IDとパスワードの初期登録はCA管理者が行う。登録後、ECS利用者は、自身のパスワードを変更することができる。

(5) CA情報管理機能 (SF.CA_MGT)

CA管理者は、以下のセキュリティ機能に関する設定を行う。設定には、2名以上のCA管理者による合議を適用することもできる。合議の人数変更、合議操作の停止も可能である。合議操作が設定されている場合、合議操作の人数条件を満たすCA管理者がTOEにログインする必要がある。

【セキュリティ機能の設定】

・DB暗号化の有無
・監査ログ署名の有無及び署名用証明書の設定
・監査ログ暗号化の有無
・合議操作の有無及び合議人数設定
・ECS利用者の登録・変更・削除

1.5.5 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3 想定する脅威

識別子	脅 威
T.UNAUTH_ACCESS（不正なアクセス）	ECS利用者が、管理端末マシンからTOEを使用して、与えられた権限外の操作を行うことにより、保護対象資産を暴露、改竄または削除するかもしれない。
T.IMPERSON（不正ログイン）	ECS利用者でない認証局に属する者が、管理端末マシンからTOEに不正にログインすることにより、TOEを使用して、保護対象資産を暴露、改竄または削除するかもしれない。
T.TOE_SECRET（秘密情報の暴露）	ECS利用者でない認証局に属する者が、CAサーバマシンのOSやDBにアクセスすることによって、暴露から保護する必要がある保護対象資産を暴露するかもしれない。
T.LINE_SECRET（通信回線上の秘密情報の暴露／改竄）	ECS利用者でない認証局に属する者が、管理端末とCAサーバの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改竄するかもしれない。
T.MISS（操作ミスによるデータ改竄／削除）	CA管理者及び運用者が、操作ミスによって、アクセスが許可されている保護対象資産を改竄または削除してしまうかもしれない。

1.5.6 組織のセキュリティ方針

組織のセキュリティ方針を表1-4に示す。

表1-4 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.CA_ADMIN（CA管理者）	CA 管理者は､TOE 及び TOE の IT 環境を管理する管理業務を適切に行うこととする。 また CA 管理者は、認証局の運用管理に対する知識を有する者が担当し、指定された以外の手段で TOE の構成を変更しないものとする。 CA管理者は、他の役職を兼務することはできないものとする。
P.OPERATOR（運用者）	運用者は、TOE の運用業務を適切に行うこととする。 運用者は、他の役職を兼務することはできないものとする。
P.AUDITOR（監査者）	監査者は、TOE の監査業務を適切に行うこととする。 監査者は、他の役職を兼務することはできないものとする。
P.SIER（認証局の構築者）	システム構築者は、TOE及びTOEのIT環境のマニュアルを熟読し、設置・生成・立上げを適切に行うこととする。
P.DUALCTL（合議）	TOE の管理業務における重要な操作は､複数の CA 管理者による合議の上で行うこととする。 またTOEの運用業務における重要な操作は､複数の運用者による合議の上で行うこととする。
P.HSM（HSM）	TOEを利用する認証局は、FIPS 140-2 level3相当の機能を持つHSMにより、物理的に保護されたCA秘密鍵を利用した、暗号操作及びCA秘密鍵のライフサイクル管理を行うこととする。
P.PERSONNEL（認証局に属する者）	認証局に属する者は、認証局を運用する組織の管理下にあり、特殊な機器を持ち込んだ攻撃や、管理端末マシンへの攻撃などの認証局の運用を妨害するような悪質な攻撃は行わないこととする。
P.PROTECT_LOG（監査ログの保護）	TOEを利用する認証局は、監査ログの暴露、改竄または削除の防止のために必要な措置をとることとする。

1.5.7 構成条件

本TOEはCAサーバマシンと管理端末マシンに搭載されるソフトウェア製品であり、TOEの構成に関して、前提となるハードウェアとしてHSMが必要となる。

TOEの外部環境に関して、構成条件を以下に示す

・CAサーバマシン：
本体：Solaris 8が稼動するSPARCプラットフォームのマシン
OS : Solaris 8
DB : HiRDB/Single Server Version 6 (64) 06-01以降
DBを使用するためのプログラム：SORT Version 6
HSMを使用するためのプログラム：nCipher Support Software for Solaris

・管理端末マシン
本体：Windows2000が搭載できる日立FLORAシリーズのマシンまたはPC/AT互換機
OS : Microsoft Windows 2000 Professional Service Pack 3以降

・HSM
本体：nShield F3 SCSI 150 標準エンクロージャ
（nCipher社製 ハードウェア暗号装置）

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1-5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1-5 TOE使用の前提条件

識別子	前提条件
A.TOE_SEP（不正な干渉からの分離）	TOEが動作するCAサーバマシン、管理端末マシンには、TOEの動作に必要なソフトウェア以外はインストールされないものと仮定する。
A.ABSTRACT_ACCOUNT（下位抽象マシンのアカウント）	TOEが動作するために必要なOS及びDBのアカウントは適切に管理されており、このアカウントを不正に利用した保護対象資産の改竄と削除はないものと仮定する。

A.PASSWORD（パスワードの管理）	ECS利用者のパスワードは、ECS利用者本人によって適切に管理され、本人以外に知られることはないものと仮定する。
A.IT_ENV（TOEのIT環境）	TOEのIT環境は、正常に動作するものと仮定する。
A.ABSTRACT（下位抽象マシンの動作）	TOEが動作するために必要なOS及びDBは、不正な改変から保護され、正しく動作するものと仮定する。
A.SETTING（設置エリア）	CAサーバマシン及びHSMは、セキュアエリア内に設置され、管理端末マシンは、マシンエリア内に設置されるものと仮定する。
A.AREA（エリアの保護）	・セキュアエリアは、入退室管理が行われ、不正な物理的アクセスから保護されるものと仮定する。 ・セキュアエリアには、CA 管理者のみ入室することができるものと仮定する。 ・マシンエリアには、認証局に属する者のみ物理的にアクセスできるものと仮定する。
A.FIREWALL（ファイアウォール）	内部セグメントは、ファイアウォールを経由してインターネットに接続され、インターネットからCAサーバマシン及び管理端末マシンへの直接のアクセスは存在しないものと仮定する。

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。

- Enterprise Certificate Server Set システムセキュリティガイド
  3000-3-494-20(D) 第3版　2004年7月

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15年10月に始まり、平成16年7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、セキュリティ機能が仕様どおりに機能することを実証するために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

本TOEの開発者テストでは、以下のような環境が構築される。

1)ハードウェア構成

・CAサーバマシン　1台：Sun Microsystems　sun4u Sun Blade 2000/1000 (2 X UltraSPARC-III+)

・HSM　1台：nShield F3 SCSI 150

・管理端末マシン1台：Hitachi FLORA

・侵入テスト用およびネットワークキャプチャ用のPCを一台設置し、ネットワーク内に接続。

2)ソフトウェア構成

・CAサーバ側ソフトウェア：

Solaris8 HW 7/03 s28s_hw3wos_05a SPARC Generic-108528-22

HiRDB/Single Server Version 6(64) 06-02-/B

SORT Version 6 06-00/A

nCipher Support Software for Solaris

Enterprise Certificate Server Set 01-01-A

・管理端末側ソフトウェア：

Windows2000 5.00.2195 Service Pack 4

Enterprise Certificate Server Set 01-01-A

3)適用しない前提条件

・マシンルームは設置しない

設置環境に対する前提条件はテスト結果に影響しないため。

・セキュアルームは設置しない

設置環境に対する前提条件はテスト結果に影響しないため。

・テスト実施者は、TOEのすべての利用者の役割で操作を行う

利用者に対する役割は、兼任してもテスト結果には影響しないため。

・ファイアウォールは設置しない。

テスト環境においては、外部ネットワークに接続せず、前提条件と同等の環境であるため。

(2) 開発者テスト概説

1)テスト構成

2.3.1節 1) の開発者テスト環境に記載された各装置をネットワーク接続し、ソフトウェアをCAサーバマシン及び管理端末マシンにインストールしテストを実施する。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。

2)テスト手法

開発者はテストを実施するにあたり、TSFIを刺激し、そのふるまいを観察することによってテストを実施し、一部のテストにおいては、TSFIを刺激し、そのふるまいを観察するツールを用いるなどしてテストを実施している。

3)実施テストの範囲

開発者テストは、以下の観点で設定され、結果として、実施されたテスト範囲が適切であると評価されている。

① 大項目として35項目のテストが実施されている。各テスト項目には１つ以上のテストパターンが存在する。

②すべてのTSF及び、すべてのTSFIが1つ以上のテスト項目によってテストが実施されており、セキュリティ機能に対するカバレージの範囲は十分である。

③すべてのサブシステム、そしてすべてのサブシステムインターフェイスは、1つ以上のテスト項目によってテストが実施されており、上位レベル設計のセキュリティ機能に対する深さの範囲も十分である。

4)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システムの構成。

1)ハードウェア構成

・CAサーバマシン　1台：Sun Microsystems　sun4u Sun Blade 2000/1000
(2 X UltraSPARC-III+)

・HSM　1台：nShield F3 SCSI 150

・管理端末マシン1台：Hitachi FLORA

・侵入テスト用及びネットワークキャプチャ用のPCを一台設置し、ネットワーク内に接続。

2)ソフトウェア構成

・サーバ側ソフトウェア：

Solaris8 HW 7/03 s28s_hw3wos_05a SPARC Generic-108528-22
HiRDB/Single Server Version 6(64) 06-02-/B
SORT Version 6 06-00/A
nCipher Support Software for Solaris
Enterprise Certificate Server Set 01-01-A

・管理端末側ソフトウェア：

Windows2000 5.00.2195 Service Pack 4
Enterprise Certificate Server Set 01-01-A

3)適用しない前提条件

・マシンルームは設置しない

設置環境に対する前提条件はテスト結果に影響しないため。

・セキュアルームは設置しない

設置環境に対する前提条件はテスト結果に影響しないため。

・テスト実施者は、TOEのすべての利用者の役割で操作を行う
利用者に対する役割は、兼任してもテスト結果には影響しないため。
・ファイアウォールは設置しない。
テスト環境においては、外部ネットワークに接続せず、前提条件と同等の環境であるため。

(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。

1)テスト構成

評価者が実施したテストの構成は、開発者のテスト環境を借用し、評価者が開発者テストと同様のテスト環境を構築して構成している。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テスト環境で実施している。

2)テスト手法

評価者は以下のテスト方針を設定し、TSFIを刺激し、そのふるまいを観察することによってテストを実施し、一部のテストにおいては、TSFIを刺激し、そのふるまいを観察するツールを用いるなどしてテストを実施するテスト手法により評価者テストを実施している。

① サンプリングテスト

TOE のセキュリティにとって重要であると評価者が判断した、識別・認証機能、アクセス制御機能、CA 情報管理機能に関するテストのうち主なものを選択し、なお、合議操作に関しては、合議承認と合議否認のテストパターンのうち半数ずつを選択する。残るテスト項目に関しては、既に選択したアクセス制御機能（運用操作合議）の中でテストされる項目を除外して、ランダムに６項目を選択する。サンプリングテストでは、重要なセキュリティ機能を重点的にテストし、また、それ以外のテスト項目に関しても、ランダムでサンプルし、テストを実施する。

② 評価者テスト

開発者のテストに対して、評価者が別のテスト方策を検討した機能に対して、開発者テストとテスト方策を変えて評価者テストを実施する。またセキュリティにとって重要であると、評価者が判断した機能に関しては、開発者とは異なる観点からテストを行うため、テストパターンを増加させ実施する。

③ 侵入テスト

脆弱性分析において開発者の主張した明白な脆弱性に対する根拠が正しいことを実証するために侵入テストを実施する。また開発者が考慮していない明白な公知の脆弱性が無いことを検証するために、評価者が明白な公知の脆弱性だと判断する項目に対して、侵入テストを実施する。

3)実施テストの範囲

・サンプリングテストとして、上記2)のテスト方針の下、14項目の開発者テスト

を選択しテストを実施している。合議操作のテストについては、合議承認と合議否認のテストパターンのうち半分（７項目）選択しテストを実施している。サンプリングしたテスト数は、開発者テスト項目の40％に相当し、サンプリングテストして、十分な量をテストしている。

・評価者テストとして、上記2)のテスト方針の下、11個のテストケースを作成・実施している。テストサブセットにおいては、すべてのセキュリティ機能に対して、1つ以上のテストを実施している。テストサブセットのテスト数は、開発者テスト項目35項目の約1/3に相当し、すべてのセキュリティ機能に対して実施している。

・侵入テストとして、上記2)のテスト方針の下、開発者の脆弱性分析に基づき、8項目の侵入テストを立案し、テストを実施している。加えて、IT環境に対して前提条件が確実に実施されていることを確認するために、2項目の補助的なテストを立案し、テストを実施している。これらの、立案した侵入テスト項目は、妥当なものである。

(4)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

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EAL3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、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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。
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.3.1E	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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んで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。また、当評価に至るまでなされた所見報告書による指摘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による指摘も適切と判断される。
ADV_HLD.2.1E	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.2.2E	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。また、当評価に至るまでなされた所見報告書による指摘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り、上位レベル設計が機能仕様の正しく完全な表現であり、下位レベル設計が上位レベル設計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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、管理機能のみであり、利用者ガイダンスが無いため非適用であることを確認している
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	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かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするもの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による指摘も適切と判断される。
ATE_DPT.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上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであ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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。
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、当評価に至るまでなされた所見報告書による指摘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。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンス及びインストールガイドがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法が記述され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の指摘も適切と判断される。

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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでなされた所見報告書による指摘も適切と判断される。

注意事項

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
CM	Configuration Management
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

本報告書で使用された用語の定義を以下に示す。

用語	意味
CA	（Certificate Authority の略）認証局のことをいう。
CAサーバ	認証局の機能を持つECSのサーバソフトウェアのことをいう。証明書やCRLの発行処理や、発行した証明書やCRLの管理を行う。
CA情報設定合議	TOEのふるまいを決定するCA情報設定に対する合議のことである。あらかじめ規定された複数の異なるCA管理者がログインすることで、当該操作を行うことができる。
CA証明書	認証局証明書のことをいう。
CA秘密鍵	CA証明書の公開鍵と対となる秘密鍵のことをいう。EE証明書の署名に使用される。
CRL	（Certificate Revocation List の略）証明書に使用する鍵の漏洩などで鍵の信頼性が失われ、失効となった証明書のリストをいう。一般利用者は、CRLによって証明書が失効されていないかどうか確認する。

CRL発行定義文	CRLを発行するために必要な情報が定義されたデータである。
DBデータ暗号鍵	データベースを暗号化するときに必要な鍵のことをいう。
ECS	（Enterprise Certificate Server の略）認証局の機能を持つソフトウェア製品である。
ECS Set	（Enterprise Certificate Server Set の略）TOEである。ECS、暗号ライブラリから構成され、公開鍵暗号技術を用いて高度なセキュリティ基盤を構築するPKIシステムの中で、認証局の機能を持つ製品である。
ECS利用者	認証局においてECS Setを利用する利用者のことをいう。役割としては、CA管理者、運用者、監査者が存在する。
EE	（End Entityの略）本TOEでは一般利用者のことをいう。
EE証明書	一般利用者に対して発行した証明書のことをいう。
FIPS 140-2	FIPS（Federal Information Processing Standard）は、米国の情報処理に関する規格であり、その中の 140-2 は暗号モジュールのセキュリティに関する規格である。
HSM	（Hardware Security Module の略）ハードウェア暗号装置のことをいう。認証局の秘密鍵を安全に管理し、また認証局の秘密鍵を使用した暗号処理を行う。
PBE	（Password Based Encryption の略）パスワード暗号方式のことをいう。
PKCS	（Public Key Cryptography Standard の略）RSA Security 社が開発した公開鍵暗号の規格のことをいう。
PKCS#1	RSAの公開鍵暗号システムに関する規格のことをいう。
PKCS#5	パスワードを基にした暗号方式をいう。
PKCS#7	メッセージやファイルを署名や暗号化する時に使用するデータ形式のことをいう。
PKCS#12	証明書と秘密鍵を暗号化するときに使用するデータ形式のことをいう。
PKCS#12データ	EE証明書と EE証明書の対となる秘密鍵をPKCS#12パスワードを基にPKCS#12形式で暗号化したデータである。
PKCS#12パスワード	PKCS#12データを作成及びPKCS#12データからEE証明書とEE証明書の対となる秘密鍵を取り出すために必要なパスワードである。
PKI	（Public Key Infrastructure の略）公開鍵暗号技術を使用したセキュリティ基盤技術の中で、証明書を利用する認証システムのことをいう。
SHA-1	ハッシュアルゴリズムの一つである。

X.509	OSIによる証明書のフォーマットを規定した国際標準規格である。
暗号化	他の人から読み取れないような形式にデータを変換することをいう。
一般利用者	EE証明書及びCRLの利用者であり、TOEの範囲外である。
運用操作合議	運用者が管理端末から行う証明書操作に対する合議のことである。あらかじめ規定された複数の異なる運用者が合議承認を行うことで当該操作が有効になる。
監査ログ	運用時の操作やエラーを記録したログのことをいう。認証サーバの運用監視に利用できる。各監査ログは、監査ログ用証明書によって署名されており、認証サーバにファイルとして出力される。運用記録の盗聴や改竄を防止できるので、信頼性の高い運用監視ができる。
管理端末	ECSのクライアントソフトウェアのことをいう。証明書やCRLの発行や管理操作、認証サーバの運用・管理操作などの認証サーバに対する操作は、すべて管理端末から行う。
検定	署名を確認することをいう。
公開鍵	公開鍵暗号方式で、暗号化や復号するために秘密鍵と対になっている鍵のことをいう。秘密鍵と公開鍵は対になっており、一方の鍵で暗号化したメッセージは、対となる他方の鍵でないと復号できない。
合議	複数の異なるECS利用者が合意の上当該操作を行うことをいう。本TOEでは、CA情報設定合議と運用操作合議がある。
合議承認	合議中の操作に対して承認することをいう。
合議否認	合議中の操作に対して否認することをいう。合議否認によって当該操作は無効となる。
証明書	正当性を保証するための電子的な証明書のことをいう。認証局が署名するため、改竄や偽造はできないようになっている。
署名	当該ユーザ自身、あるいは当該認証局以外には作成できない情報のことをいう。署名を確認することで、不正なアクセスによる改竄や成りすましがないかを確認できる。
セキュアエリア	入退室管理が行われ、不正な物理的アクセスから保護されたエリアのことをいう。セキュアエリアには、CA管理者のみ入室することができる。
内部セグメント	マシンエリア内に設置される。 ファイアウォールを介して外部ネットワークに接続される。

認証局	証明書を発行する機関のことをいう。当該認証局が発行した認証局証明書を持っているかどうかで、通信相手が正当かどうかを判断する。
認証局証明書	認証局が自認証局の正当性を保証するために発行する証明書のことをいう。
認証局に属する者	TOEを運用する組織に属する者のことをいう。TOEへのアクセスを許可されたECS利用者と TOEへのアクセスを許可されていない者がいる。いずれの者も認証局を運用する組織の管理者によって適切に管理される。
ハードウェア暗号装置	秘密鍵の管理、署名や検定などを処理する装置のことをいう。秘密鍵は、この装置の外に出ないため、秘密鍵に対する盗聴や改竄の心配がない。
秘密鍵	公開鍵暗号方式で、暗号化や復号するために公開鍵と対になっている鍵のことをいう。
秘密情報格納ディレクトリ	CAサーバ起動時に必要な設定情報などを保管する、暗号化された格納領域である。
復号	暗号化されたデータを読めるようなデータに復元することをいう。
マシンエリア	認証局のマシンルームのことをいう。マシンエリアには、認証局に属する者のみ物理的にアクセスすることができる。
リポジトリ	証明書を利用する一般利用者に証明書やCRLを公開したり、発行した証明書やCRLを管理したりする。

6 参照

[1] Enterprise Certificate Server Set セキュリティターゲット Version 1.10 2004/6/24 株式会社日立製作所

[2] ITセキュリティ認証申請等の手引き 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] ITセキュリティ評価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－IT機関要求－02

[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－IT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] CCIMB Interpretations-0210

[21] 補足-0210

[22] 2004年7月5日　評価報告書 DTT-ETR-0001-02　株式会社電子商取引安全技術研究所評価センター：評価報告書別冊となる個別評価報告書は、以下のリストに示す16点。

DTT-ECM-0001-02	Configuration Management
DTT-EDO-0001-03	Delivery and Operation
DTT-EDVS-0001-02	Development Security
DTT-EFSP-0001-04	Functional Specification
DTT-EGD-0001-02	Guidance Documents
DTT-EHLD-0001-03	High-Level Design
DTT-EIMP-0001-01	Implementation Representation
DTT-EIND-0001-02	Independent Testing
DTT-EMSU-0001-02	Misuse
DTT-ERCR-0001-03	Representation Correspondence
DTT-ESOF-0001-02	Strength of TOE Security Function
DTT-EST-0001-03	Security Target
DTT-ETD-0001-02	Test Documentation
DTT-EVLA-0001-03	Developer Vulnerability Analysis
DTT-ETEST-0001-04	独立テストおよび侵入テスト報告書
DTT-ESITE-0001-03	サイト訪問実施報告書