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 4 月 10日 (ST確認2003)
ＳＴ確認申請者	株式会社　日立製作所
ＳＴの名称	Enterprise Certificate Server セキュリティターゲット Version1.7
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	株式会社　日立製作所　ソフトウェア事業部
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2月26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
⑦ 補足文書（補足-0210, CCIMB Interpretations-0210）

評価結果：合格

Enterprise Certificate Serverセキュリティターゲット Version1.7　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、「Enterprise Certificate Serverセキュリティターゲット Version1.7」（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株式会社　日立製作所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:　　Enterprise Certificate Server (P-2465-9214)
- バージョン:　02-00
- 開発者:　　株式会社 日立製作所

1.2.2 製品概要

本製品は、Enterprise Certificate Server (以下、ECSと記す) という名称のソフトウェア製品であり、国際標準X.509に準拠した証明書の発行を管理する認証局機能を提供する。証明書発行機能を提供する「CAサーバ」と、リモートから管理を行う「管理端末」の二つのパーツから構成される。

1.2.3 TOEの範囲

本TOEは認証局（Certification Authority; 以下「CA」と記す。）システムに使われるソフトウェア製品である。本TOEを用いたCAシステム構成例を図1-1に示す。図1-1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。CAシステムを構成するには、本TOE以外に図1-1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に含まれず、ST確認の対象外である。

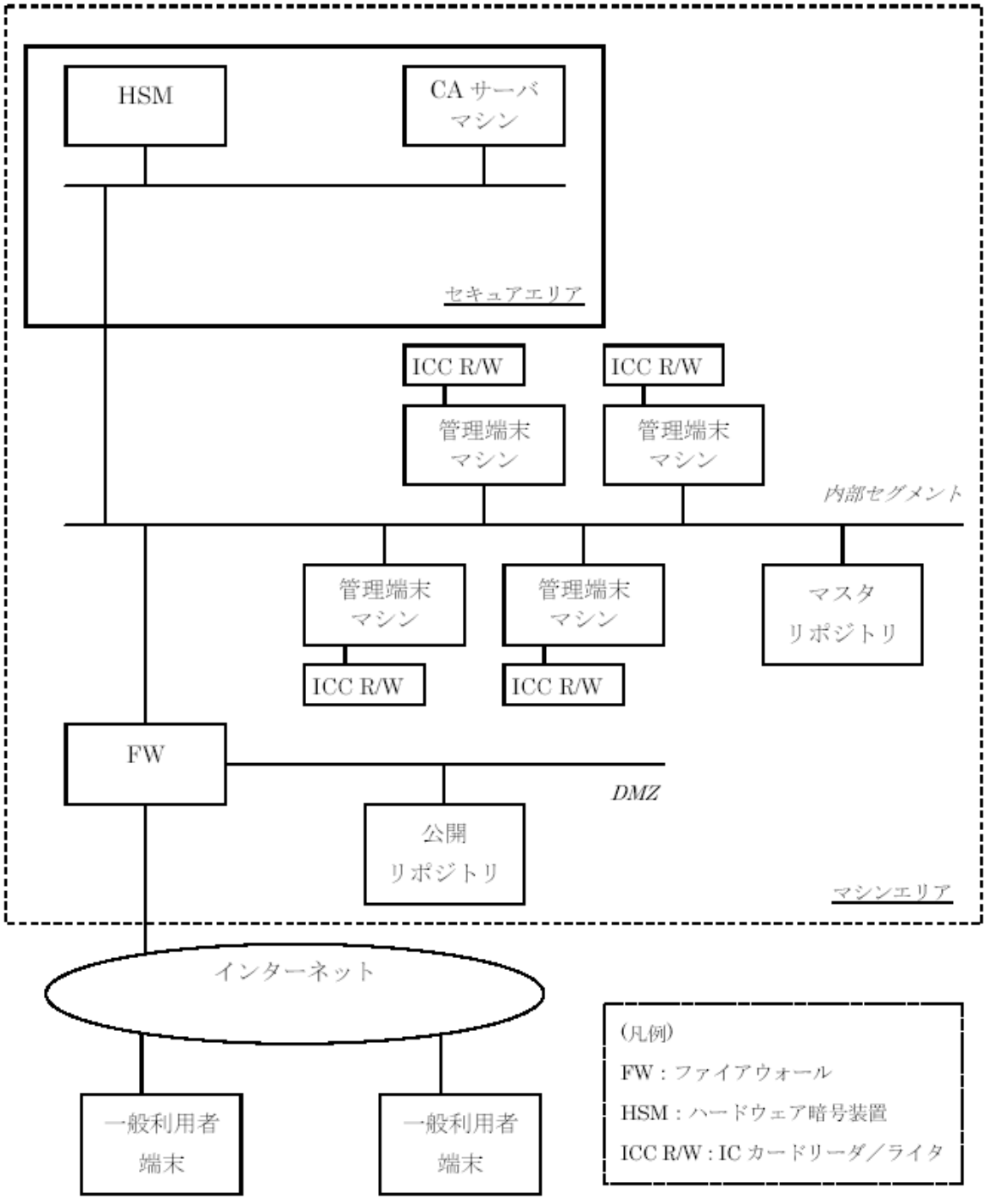

図1-1　　CAシステム構成例

TOEを構成する「CAサーバ」と「管理端末」の各ソフトウェアが共同して提供する機能は、表1-1のとおりである。

表1-1　　TOEの機能範囲

機能名称	機能内容
証明書発行及び管理機能	一般利用者（EE）証明書の発行と管理
証明書失効リスト（CRL）発行及び管理機能	証明書失効リスト（CRL）の発行と管理
監査機能	CAの監査に必要な監査ログ情報の記録と表示
暗号機能	以下のデータ暗号操作機能 - PKCS#12データ（EE証明書及び秘密鍵をPKCS#12形式で暗号化したもの）の暗号化 - PKCS#12パスワード（PKCS#12データからEE証明書及び秘密鍵を取り出すためのパスワード）の暗号化 - ECS利用者パスワードの暗号化 - CA設定情報の暗号化 - DBデータ暗号鍵の暗号化 - 監査ログの暗号化/復号及び署名付与 - 監査ログ用証明書・監査ログ用秘密鍵の暗号化 - 秘密情報暗号鍵の暗号化 - CAサーバ・管理端末間通信データの暗号化 - CAサーバ・管理端末間通信データ暗号化用暗号鍵の交換
アクセス制御機能	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	ECS利用者の識別・認証機能
CA情報管理機能	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)

1.2.4 TOEの動作概要

(1)　　TOEのサービス機能

TOEは、CAが提供するサービスの中核となる部分の機能を提供する。機能範囲は前節に示したが、ここでは、TOEが提供するサービス機能を詳細に説明する。

- 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、失効リスト（以下、CRLと記す）を発行する。

(2)　　EEに対するサービス提供形式

TOEのサービスは、CAの組織に属する「運用者」がCA内に置かれた「管理端末マシン」を介して操作し、以下のような手段によってEEへ提供される。これらの手段は、TOE外のIT環境によって提供されるものであるが、TOE動作に関連するものとして知っておく必要がある。

- EE証明書とCRLは、公開リポジトリ（図1-1参照）を介してネットワーク経由でEEへ提供される。EEは、CAの公開リポジトリから、確認したい相手のEE証明書あるいはCRLを参照できる。
- PKCS#12データ（前項参照）をフロッピーディスクなどのメディアに格納し、郵送などのオフライン手段でEEへ送付する。
- PKCS#12データを復号するためのパスワードを紙に印刷し、郵送などのオフライン手段でEEへ送付する。

(3) TOEのセキュリティ機能

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。保護対象となる利用者データを以下に示す。

- EE証明書: EEの公開鍵にCAが署名を施したもの
- EE秘密鍵
- 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

上記利用者データを保護するためのTOEの主要なセキュリティ機能は、以下のようなものである。

- 監査機能: セキュリティ機能の動作に関わる監査ログを記録する。
- 暗号機能: 保護すべき利用者データ、TSFデータを暗号化して格納する。監査ログについては、暗号化し署名を施す。また、LANで接続されたCAサーバと管理端末間のデータを暗号化する。
- アクセス制御機能: TOEを運用・管理する利用者に対して、利用者の権限に応じてデータのアクセスを制御する。重要な利用者データに対しては、複数の利用者が合意したときだけデータに対する操作を可能にする「合議機能」を備えている。合議に必要な人数は、運用環境に応じて設定できる。

- TOEのセキュリティ機能自身（TOEのセキュリティ機能全体をTSFと呼ぶ。以下、セキュリティ機能全体を指す場合にTSFと記す。）、及びTSFが使用するデータ（以下、TSFデータと記す。）を保護するためのセキュリティ機能。TSF/TSFデータを保護するセキュリティ機能は、間接的に利用者データの保護に貢献する。

1.3 評価実施

Enterprise Certificate Serverセキュリティターゲット Version1.7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][9][13][16]のいずれか）附属書C、CCパート2（[6][10][14][17]のいずれか）の機能要件及びCCパート3（[7][11][15][18]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（[19][20][21]のいずれか）に準拠する。また、これらの基準には、補足文書（[8][12]のいずれか）の内容を反映するものとする。

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15年11月5日の評価実施機関による「ST評価報告書 2.2版 2003.11.05 DTW-ETRST-0002-02」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確認報告書案を作成した。

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。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、ECS利用者に対するパスワード機能（後述するセキュリティ機能SF.CA_MGTに含まれる）と、セキュリティ機能SF.CRYPTO（後述）のハッシュアルゴリズムに関わる部分である。パスワードに使用されるメカニズムは、パスワード文字長を4～64文字としている。この条件だと、ECS利用者は、4文字のパスワードを使用するかもしれない。通常、4文字程度のパスワードでSOF-基本を満たすことはできないが、本TOEでは、5回の誤ったパスワード入力でその利用者を閉塞するようなICカードを補助手段として併用すること、全利用者に対して、簡単に推定できるようなパスワードを使用しない教育を施すことなど、管理・運用面での補強策によって、総合的にSOF-基本の要件を満たすようにしている。

1.4.4 セキュリティ機能

本TOEは、以下に示すTSF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満たされる。

(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。（詳細は、ST 6.1.1参照）

(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。詳細を2.2に示す。

(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。

ECS利用者は、自身の利用者IDとパスワードを記録したICカードを保持する。TOEへのログインに先立ち、管理端末に接続されたICカードリーダを使用して、ICカードに記録された利用者ID・パスワードによる識別・認証が行われる。この識別・認証が不成功だと、その不成功回数がICカードに記録され、累積が5回になるとICカードが閉塞され、そのICカードで識別・認証が行えなくなる。このICカードによる利用者の識別・認証は、TOE外の機能ではあるが、TOEの認証メカニズムのセキュリティ機能強度を支援する役割を持っており、TOEのセキュアな運用のために必要な前提条件となっている。

このICカードに記録される利用者ID・パスワードは、TOE内に記録された利用者ID・パスワードと同一である。本TOEによるパスワード設定時のチェックは、パスワードの文字種と桁数確認（4～64文字）だけであり、「弱い」パスワードを排除するには不十分である。従って、利用者は、自らの管理によって安全なパスワードを選択しなければならない。また、併用するICカードは、ICカード内のデータを不正に読み出されたり改ざんされたりしないよう、十分なセキュリティ機能を備えたものでなければならない。これらの条件が満たされないと、TOEのセキュリティに弱点が生じる。

(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

1.4.5 脅威

本TOEが対策を講じている脅威は、以下のとおりである。T.IMPERSONに対しては、

環境によるセキュリティ対策が併用される。

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・改ざん・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・改ざん・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・改ざん）

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・改ざんするかもしれない。

T.MISS（操作ミスによるデータ改ざん・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ざん・削除してしまうかもしれない。

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は、以下のようなものである。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ない。IT環境に関係するP.HSMを除き、すべて運用・管理手段による対処が必要なものである。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.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。なお、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。なお、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。なお、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環境を適切に設置・生成・立上げることとする。

P.HSM (HSM)

TOEを利用する認証局は、FIPS 140-1 level3相当のHSMにて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、改ざん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。

1.4.7 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、特段の条件はない。

TOEの外部環境に関して、具体的な構成例を2.1に示す。

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。

【利用環境】

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.ICC_MGT (ICカードの管理)

TOEの運用に使用するICカードは、閉塞機能を持つ規定のICカードを使用し、正当なECS利用者にのみ発行され、ECS利用者によって、適切に管理されるものと仮定する。

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ざん、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。

【物理管理】

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、不正な改ざんから保護され、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。

【接続・動作環境】

A.DEVICE（周辺機器）

ICカードリーダ/ライタは、管理端末マシンの付近に設置され、USBでローカルに接続される。これらの間で盗聴されることがないものと仮定する。

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、HSM、管理端末マシンへのアクセスは存在しないものと仮定する。

1.4.9 特記事項

本TOEをセキュアに使用するために、STの前提条件及び組織のセキュリティ方針に記述された内容を遵守することが必要である。特に、組織のセキュリティ方針に記述された7項目は、P.HSMを除きすべて運用・管理手段によって対処しなければならない

ものである。これらの条件が満たされないと、TOEの脆弱性が悪用される危険が生じる。

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

2.1 TOEの外部環境構成

STに記述されたTOEの外部環境構成を以下に示す。この中には、TOEのセキュリティ環境（前提条件や組織のセキュリティ方針）に明示されているものも含まれており、それらを適切に構成することがTOEのセキュアな運用・管理のために必要である。

(参照: 1.4.6 組織のセキュリティ方針、1.4.8 動作環境の前提条件)

- CAサーバマシン：
  本体：FLORAシリーズ IBM PC/AT互換機
  CPU：Pentium4　1GHz以上
  メモリ：512MB以上
  ハードディスク：4GB以上
  OS：Microsoft Windows 2000 Server Service Pack 3
  DB：HiRDB Single Server 5.0 05-04 (形名：P-2462-7154)
  HSM使用のためのソフトウェア：ハードウェア暗号装置 アクセスライブラリ 01-01/B (形名：P-2444-8214)
- 管理端末マシン：
  本体：FLORAシリーズ IBM PC/AT互換機
  CPU：PentiumIII 500MHz以上
  メモリ：256MB以上
  ハードディスク：4GB以上
  OS：Microsoft Windows 2000 Professional Service Pack 3
  ICカードリーダ使用のためのソフトウェア：ICカードアクセスライブラリ 02-00 (形名：P-F2465-9214１)
- HSM：
  本体：日立ディジタル署名装置（タイプBX)
  形名：HN-S9342-10
- ICカードリーダ/ライタ：
  本体：ICカードリーダライタ
  形名：HX-500UJ
- IC カード：
  本体：MULTOSカード（バージョン3.4以降)

2.2 TOEが使用する暗号機能

本TOEは、利用者データ、TSFデータ保護のために各種暗号機能を使用している。対象となるデータとそれに適用される暗号の種類を表2-1に示す。

表2-1　　暗号機能の適用形態

対象データ	データの種別	暗号アルゴリズム	適用形態
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		
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	DES (FIPS 46-2)	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。 (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。 (ECS起動時に使われるCA管理者パスワードを鍵として暗号化。)
監査ログ	TSFデータ	DES (FIPS 46-2)	監査ログ暗号化
		RSA (PKCS#1)	監査ログ署名
		SHA-1 (FIPS 180-1)	監査ログ署名/検定（ハッシュ)

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[22]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。

4.3 勧告

本TOEの認証機能は、十分なセキュリティ機能強度を得るために、ECS利用者識別・認証用のICカード（TOEに含まれない）の併用が必要であり、さらに、ECS利用者の

パスワードが他人に簡単に推測されないよう、利用者個人の裁量によって適切なパスワードを選択することが前提になっている。使用するICカード及びパスワード選択方法については、TOEに含まれるガイダンスに明示されることになるので、それに沿った適切な管理・運用を行わないと、TOEのセキュリティ機能が十分な効果を発揮できない危険のあることに注意が必要である。

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
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

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) 認証局のことをいう。
CAサーバ	認証局の機能を持つEC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。
DES	暗号共通鍵暗号の規格の一つである。
DMZ	(De Militarized Zoneの略) 公開サーバをインターネット側からの不正な攻撃から守るため、ファイアウォールにより設けられたセグメント。
ECS	(Enterprise Certificate Serverの略) 本STのTOEであ

	る。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を利用する利用者のことをいう。役職としては、CA管理者・運用者・監査者が存在する。
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。
FIP140-1	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140-1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。
ICカード	秘密情報を格納するための媒体である。耐タンパ性を持っている。格納されている情報にアクセスする前に識別と認証が実施されるため、フロッピーディスクなどの媒体に比べ安全である。
LDAP	(Lightweight Directory Access Protocolの略) X.500ディレクトリサービスをInternet向けに軽量、簡素化したサービスプロトコル。Webブラウザやメーラなどの LDAPクライアントからは、LDAPに対応したディレクトリサービスを直接検索・参照することができる。
MD5	ハッシュアルゴリズムの一つである。
MULTI2暗号	共通鍵暗号の一つである。
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暗号化や署名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。
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ざんを防止できるので、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・復号の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化できない。
公開リポジトリ	認証局で発行したEE証明書及CRLが格納される。ファイアウォールを介してインターネットに接続されており、一般利用者に対してEE証明書及CRLを公開するために利用される。
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。
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。
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、改ざん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ざんや成りすましがないかを確認できる。
耐タンパ性	一般的に、悪意をもったユーザが不正な手段を用いて内部情報を獲得しようとした場合に、それを阻止するように働く機能や性質のことをいう。ICカードは決められた回数のパスワードの入力に失敗した場合、閉塞し、ICカード自体を使えなくしたり、複製の作成を困難にしたりするなどの耐タンパ性を持っている。
ディレクトリサーバ	リポジトリの役目を果たすLDAPに対応しているプログラムのことをいう。
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インターネットに接続される。
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、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ざんの心配がない。また、鍵に対する権限の管理や複数ユーザの同時利用、分割バックアップなどの機能を備え、認証局の秘密鍵を扱うのに適している。
半角記号	以下の「」で囲まれた記号をいう。 「!」「"」 (ダブルクォーテーション)「#」「$」「%」「&」「'」(シングルクォーテーション)「(」「)」「*」「+」「,」(コンマ)「-」「.」(ピリオド)「/」「:」「;」「<」「>」「=」「?」「@」「[」「]」「¥」「^」「_」「`」「{」「}」「¦」
秘密鍵	公開鍵暗号方式で、暗号化・復号の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。
閉塞	ICカードが使用できなくなる状態のことをいう。

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。
マスタリポジトリ	認証局で発行したEE証明書及CRLが格納される。マスタリポジトリの内容は、ディレクトリサーバのリプリケーション機能を使用して公開リポジトリにコピーされる。
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セキュリティターゲット Version 1.7 株式会社日立製作所

[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] CCIMB Interpretations-0210

[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1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031

[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

[11] 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

[12] 補足－0210

[13] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[14] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[15] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[16] 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

[17] 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

[18] 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

[19] Common Methodology for Information Technology Security Evaluation
CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999
[20] 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
[21] 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
[22] ST評価報告書 2.2版 2003年11月5日 DTW-ETRST-0002-02/個別評価報告書
Security Target ASE 3.2版 2003年11月5日 DTW-EST-0003-02