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11月29日（ST確認2016）
ＳＴ確認申請者	富士通株式会社
ＳＴの名称	SystemWalker/PkiMGR CA セキュリティターゲット
ＳＴのバージョン	第1.8版
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+ADV_SPM.1）
ＳＴ開発者	富士通株式会社 運用管理ソフトウェア事業部 第4開発部
評価実施機関の名称	社団法人　電子情報技術産業協会　ITセキュリティセンター

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 6月18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：「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 Version 1.0
⑥ 認証機関が公開する③及び⑤の翻訳文書

評価結果：合格

「SystemWalker/PkiMGR CA 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、「SystemWalker/PkiMGR CA セキュリティターゲット第1.8版」（以下「本ST」という。）について社団法人　電子情報技術産業協会　ITセキュリティセンター（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富士通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:　SystemWalker/PkiMGR、及び
  SystemWalker/PkiMGR Key Protection Option
- バージョン:　Windows版：V10.0 L20
  Solaris(TM) Operating Environment版：10.1
- 開発者:　富士通株式会社

1.2.2 製品概要

本製品は、認証局（CA）や登録局（RA）といったPKIシステムを構築するためのソフトウェア製品であるSystemWalker/PkiMGRのCA機能（以降、SW/PkiMGR CAと記述）とSystemWalker/PkiMGRのセキュリティ機能を拡張するための附属製品にあたるSystemWalker/PkiMGR Key Protection Option（以降、SW/PkiMGR KPOと記述）によって実現するCAサービスである。

主な機能は、RAサービス[1]と連携して一般利用者に対し、公開鍵証明書、CRL、相互認証証明書、自身の公開鍵証明書（CA証明書）等の発行を行い、それらの管理を行う。

---

[1] SystemWalker/PkiMGRによって提供されるRA機能（以降、SW/PkiMGR RAと記述）。RAサーバマシンにインストールされるもので、本評価の対象ではない。

1.2.3 TOEの範囲

本TOEは、図中の太線で示されるソフトウェア（SW/PkiMGR CA 、SW/PkiMGR KPO）であり、以下の環境で動作する。

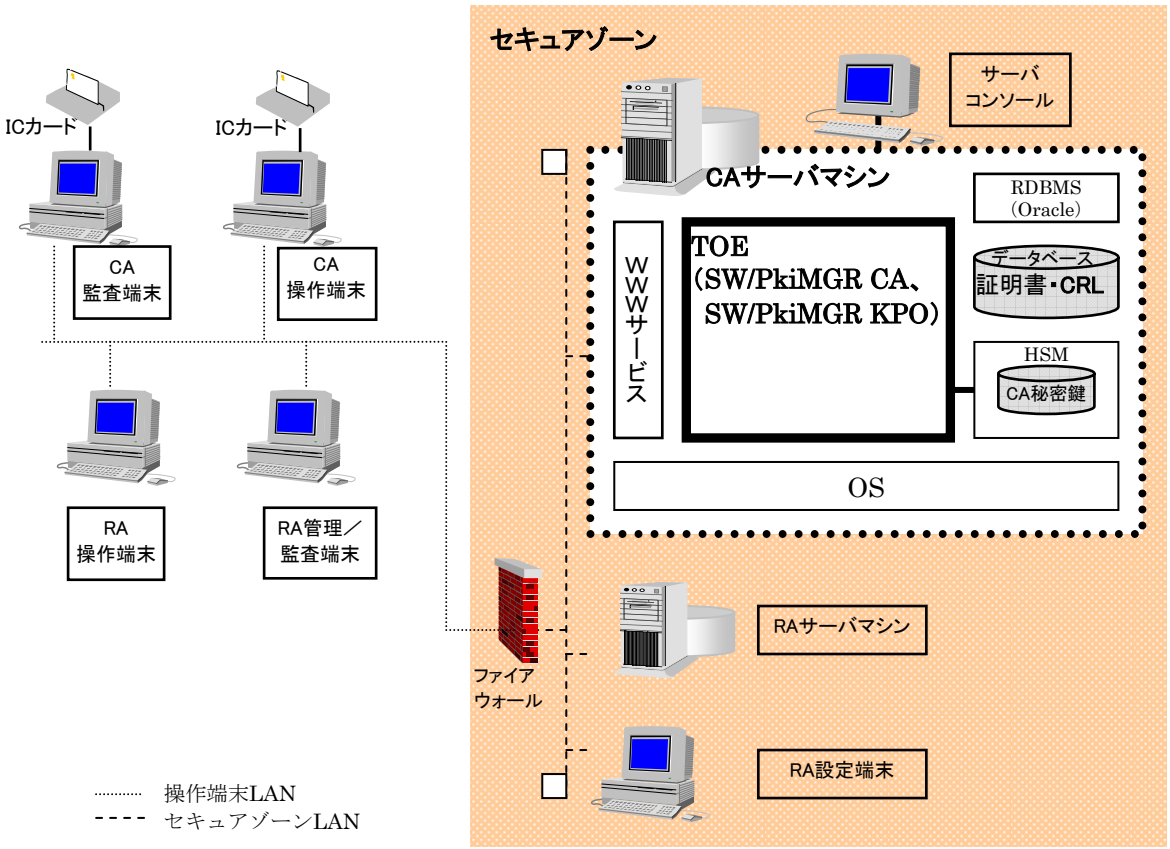

図1　TOEの動作環境

また、図中で示される各エンティティは以下に定義される。

- セキュアゾーン
  TOE の運用に関わるシステム管理者及び他のサーバマシン管理者だけが入室可能であり、外部とはファイアウォールを介してのみ接続される、物理的、接続的に隔離・管理された空間のこと。
- セキュアゾーン LAN
  セキュアゾーン内の LAN。サーバマシンが接続される。
- 操作端末 LAN
  セキュアゾーン外で運用に関わる操作端末が接続される LAN。

- CA サーバマシン
  TOE が設置され、動作するサーバマシン。WWW サーバ、RDBMS といったソフトウェアも動作する。CA サーバ内の TOE を含む各ソフトウェアは、サーバマシンで稼動する OS（オペレーションシステム）上で動作する。
- サーバコンソール
  CA サーバマシンに直接接続されたディスプレイ・キーボード。
- HSM（ハードウェア セキュリティ モジュール）
  CA秘密鍵が格納されるハードウェア。
- RAサーバマシン
  SW/PkiMGR RAが動作するサーバマシン。一般利用者の証明書発行・失効依頼をRA操作端末から受信し、TOEであるCAサービスに申請する。また、証明書発行処理結果をTOEから受信し、RA操作端末に送信することも実施する。
- RA設定端末
  RAサーバマシンのシステム管理者が、RAサービスの設定等を行うために使用する端末。
- CA操作端末
  CAオペレータが、TOEにアクセスし、CAサービスで提供される機能を操作するための端末。
- CA監査端末
  監査者が、TOEにアクセスし、監査機能を操作するための端末。
- RA管理／監査端末
  RAサーバの管理者が、RAサービスへアクセスし、RAサービスの設定を行う。また、RAサーバの監査者が、RAサービスへアクセスし、監査を行うための端末。
- RA操作端末
  RAサーバのオペレータが、RAサービスへアクセスし、RAサービスで提供される機能を操作するための端末。

1.2.4 TOEの動作概要

(1) TOEの論理的構成

以下の『図2　TOE論理的構成』に、TOEの論理的な構成を示す。

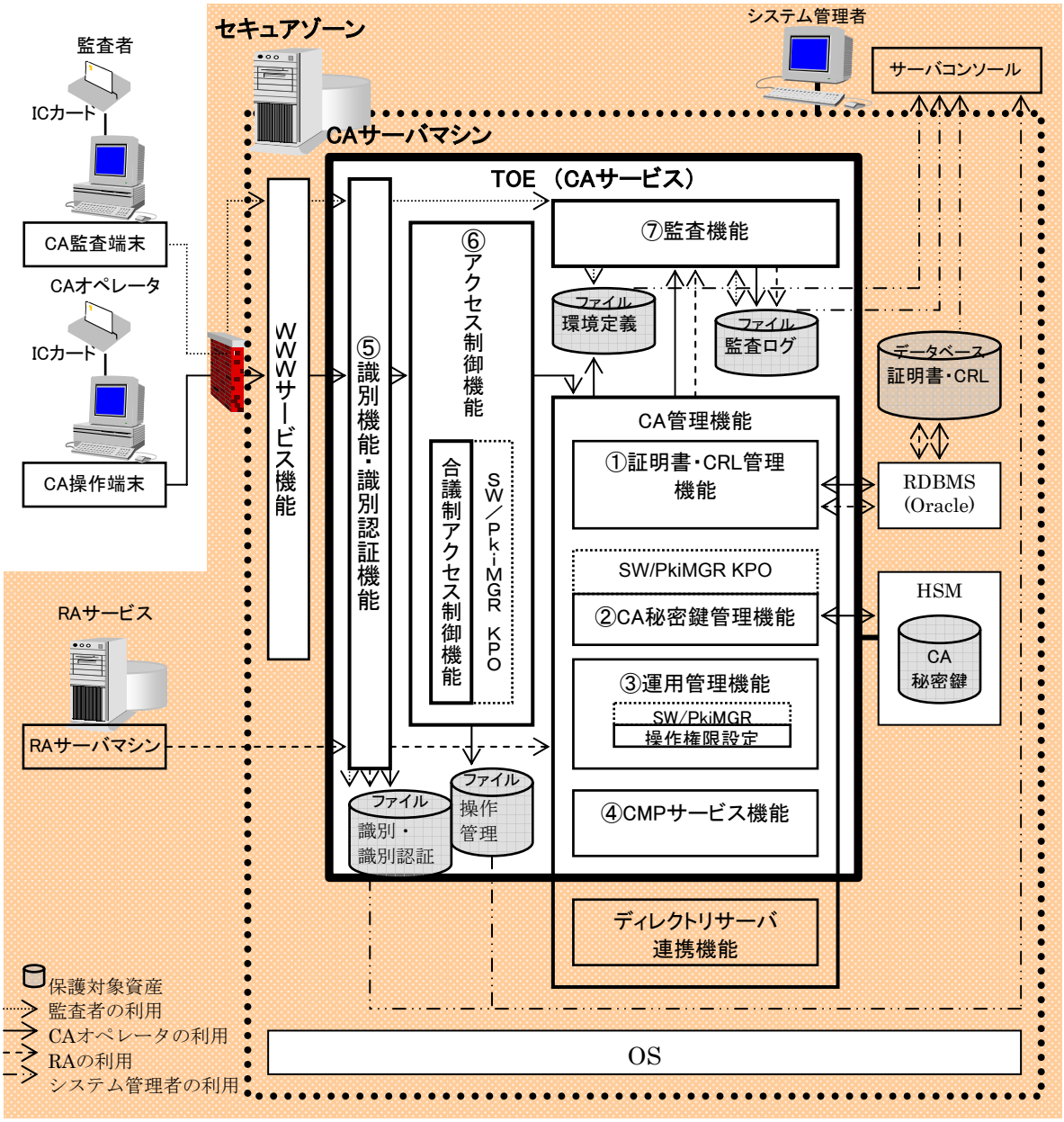

図2　TOE論理的構成

① 証明書・CRL 管理機能

- 証明書、CRL のプロファイルを設定する機能。
- PKCS#10 形式の申請書より、一般利用者、相互認証のための証明書を発行する機能。
- PKCS#12 形式で、TOE 利用者である監査者、RA サービスのための証明書を発行する機能。
- CMP サーバ証明書、CA オペレータ証明書、CA 証明書を発行する機能。

・ 発行した証明書・CRL をデータベース（以降、DB）で管理（検索、閲覧、削除）する機能。
・ 発行した証明書を失効する機能。
・ CMP サーバによって RA サーバからの申請を受け付け、一般利用者の証明書を発行・失効する機能。
・ CRL を発行する機能。
・ 他の CA によって発行された証明書・CRL を CA 操作端末からインポートして、DB に登録し、管理する機能。
・ 証明書・CRL を CA 操作端末に取り出す機能。

② CA 秘密鍵管理機能
・ CA 秘密鍵を HSM で管理（生成・削除、活性化・非活性化、バックアップ・リストア）する機能。

③ CMP サービス機能
・ RA サービスから一般利用者証明書の発行申請を受信する機能。
・ 一般利用者証明書の発行申請に基づき、証明書・CRL 管理機能に処理を依頼する機能。
・ RA サービスから発行依頼された証明書の発行後処理結果を RA サービスに送信する機能。

④ 運用管理機能
・ CA オペレータを追加・削除する機能。
・ CA オペレータの操作権限を設定する機能。

⑤ 識別機能・識別認証機能
・ WWW サーバの SSL クライアント認証機能と連携し、TOE の利用者である CA オペレータや監査者の TOE へのアクセスを許可するための識別機能。
・ RA サービスが CA サービスに対するアクセスを許可するための識別認証機能。

⑥ アクセス制御機能・合議制アクセス制御機能
・ TOE へのアクセスを許可された CA オペレータに対し、各 CA オペレータに設定された操作権限情報に基づいて操作を制限するアクセス制御機能。
・ セキュリティ上、重要とされる操作に対して、操作権限を持つ複数の CA オペレータが設定された必要人数以上に達しない場合、その操作の実行を許可しない合議制アクセス制御機能。

⑦ 監査機能
・ TOE の運用に関する操作履歴（監査ログ）を記録する機能。

・ 監査ログを検索・表示・削除する機能する機能。
・ 監査ログの完全性・連続性を検証する機能。
・ 監査ログを長期保管するため、TOE から外部媒体に監査ログを移出する機能。またそれを元に戻す（移入する）機能。

(2) TOEの利用方法

本TOEは、システム管理者、CAオペレータ及び監査者によって利用される。それぞれの利用方法について以下に示す。

- システム管理者

  TOE及びTOEの運用環境を管理する権限を持つ者。CAサーバマシンに対して１人しか存在しない。CAサーバマシンにOSのインストールを行い、TOEのインストール、セットアップ、設定・管理、及びOS、WWWサーバ機能、RDBMS、HSM等の運用環境の設定・管理を行う。またDBに管理される証明書・CRL等やTOE運用環境に関するデータのバックアップを行い、何らかの不具合が生じた場合やセキュリティ侵害が生じた場合、リストアを行う。

- CA オペレータ

  TOEを運用操作する権限を持つ者。CAサービス毎に複数人存在する。CA操作端末からTOEにアクセスし、CA管理機能を使用して証明書の発行及び失効、CRLの発行、CA秘密鍵の管理操作等を行う。またCA秘密鍵のバックアップ及びリストアの作業を行う役割があり、システム管理者の監視下においてセキュアゾーン内に入ることも許可されている。

- 監査者

  TOEの監査に関する権限を持つ者。CAサービス毎に複数人存在する。監査機能を使用し、監査ログの検索・表示・削除、監査ログの完全性・連続性の検証、及び監査ログの移出・移入の操作を行う。

1.3 評価実施

SystemWalker/PkiMGR CA 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、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社団法人　電子情報技術産業協会　ITセキュリティセンターが実施する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5月の評価実施機関による「ST評価報告書 第1.0版 2004.5.11」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追加である。
追加する要件はADV_SPM.1。

1.4.3 セキュリティ機能強度

本STにおいてTOEに要求される最小機能強度レベルは、SOF-基本である。

1.4.4 セキュリティ機能

TOEは、以下のセキュリティ機能を有する。

- CAオペレータ証明書による識別／アクセス制御機能
  表1の操作を行うTOE利用者をCAオペレータに限定するため、WWWサービス機能から受け取ったCAオペレータ証明書を使用したTOEの識別機能、及び識別されたCAオペレータが操作権を持つ場合にだけ表1の操作を許可するための

TOEのアクセス制御機能である。

表1　CAオペレータの操作

分類	内容
証明書・CRL管理機能	・既存の証明書プロファイルの変更 ・新しい証明書プロファイルの追加 ・追加した証明書プロファイルの削除 ・既存のCRLプロファイルの変更 ・CA証明書・CAオペレータ証明書・CMPサービス証明書の発行 ・PKCS#10形式の申請書に基づく相互認証証明書等の発行 ・監査者・RAサービス等の証明書とその秘密鍵をPKCS#12形式で作成 ・発行した証明書の失効 ・CRLの発行 ・他のCAが発行した証明書・CRLの登録 ・データベースで管理する証明書・CRLの削除
CA秘密鍵管理機能	・CA秘密鍵の生成・削除 ・CA秘密鍵のバックアップ・リストア ・CA秘密鍵の活性化・非活性化
運用管理機能	・CAオペレータの操作権の設定 ・CAオペレータの登録・削除

- **CAオペレータIDとパスワードによる識別認証／アクセス制御機能**

  表2の操作を行うTOE利用者をCAオペレータに限定するためのCAオペレータIDとパスワードによる識別認証機能、及び識別認証されたCAオペレータが操作権を持つ場合にだけ表2の操作を許可するアクセス制御機能かつ操作権を持つCAオペレータが当該操作に決められた必要最小人数揃っている場合にだけ操作を許可する合議制アクセス制御機能である。

表2　CAオペレータの合議操作

分類	内容
証明書・CRL管理機能	・CA証明書・CAオペレータ証明書・CMPサービス証明書の発行
CA秘密鍵管理機能	・CA秘密鍵の生成・削除 ・CA秘密鍵のバックアップ・リストア ・CA秘密鍵の活性化・非活性化
運用管理機能	・CAオペレータの操作権の設定

- **監査者証明書による識別機能**

  表3の操作を行うTOE利用者を監査者に限定するため、WWWサービス機能から受け取った監査者証明書を使用したTOEの識別機能である。

表3 監査者の操作

分類	内容
監査機能	・監査ログの検索・表示 ・監査ログの移出・移入、削除 ・監査者証明書の登録・削除

- **RA証明書による識別認証機能**

  CAサービスとの通信を許可するRAサービスからの要求だけを受理するための識別認証機能である。

- **監査ロギング機能**

  CA管理機能、監査機能、RAサービスのセキュリティに関連する操作で発生する全ての事象を、監査ログレコードとして記録する機能である。

- **監査ログ完全性・連続性検証機能**

  監査ロギング機能で記録した監査ログの完全性、及び連続性を検証する機能である。

- **監査ログ操作機能**

  監査ロギング機能で記録した監査ログファイルを操作するための機能である。

- **監査ログ損失防止機能**

  監査ログの記録漏れが発生しないようにするための機能である。監査対象の操作が行われる前にディスクの空き容量を確認し、空き容量が10%未満になった場合は以下の何れかを行う。

  Windows版：「容量不足」の監査警告メッセージをイベントログに記録。

  Solaris OE版：「容量不足」の監査警告メッセージをシステムログに記録。

1.4.5 脅威

TOEは表4に示す脅威を想定し、本システムは、これに対抗する機能を備える。

表4　想定する脅威

識別子	脅威
T.ADMIN-ERROR（システム管理者の誤操作）	システム管理者が誤操作により、以下のTOE内のデータを変更・削除する。 ・証明書 ・CRL ・TOE動作環境ファイル －識別データ（監査者識別データ、CAオペレータ識別データ、RA識別データ） －識別認証データ（CAオペレータ識別認証データ、CMPサービス証明書とその秘密鍵） －操作管理データ（CAオペレータ操作管理データ、合議操作管理データ） －環境定義データ（監査環境定義データ、CA環境定義データ、データベース環境定義データ） ・監査ログ
T.AUDITOR-ERROR （監査者の誤操作）	監査者が監査作業中の誤操作により、以下の行為を行う。 ・移出していない有効な監査ログを削除する。 ・登録されている監査者の証明書を削除する。

T.CAO-MALICE&ERROR-1（CAオペレータの悪意ある操作と誤操作-1）	悪意を持つCAオペレータがCAサービスの運用を妨害するために自分自身の役割に与えられる操作権の範囲を超えてTOEを利用するか、または悪意を持たないCAオペレータが運用作業中の誤操作により、以下の行為を行う。 ・発行すべきでない第三者に証明書を発行する。 ・定義されているプロファイルとは異なる形式の証明書・CRLを発行する。 ・データベースで管理する有効な証明書・CRLを削除する。 ・データベースで管理する有効な証明書を失効し、CRLを発行する。 ・操作権を持つ有効なCAオペレータを削除する。 ・信頼性が確認されていない他のCAが発行した証明書・CRLを登録する。 ・信頼性が確認されていない他のCAと相互認証を行う。
T.CAO-MALICE&ERROR-2（CAオペレータの悪意ある操作と誤操作-2）	悪意を持つCAオペレータがCAサービスの運用を妨害するために自分自身の役割に与えられる操作権の範囲を超えてTOEを利用するか、または悪意を持たないCAオペレータが運用作業中の誤操作により、以下の行為を行う。 ・CA秘密鍵を新しく生成し、有効なCA秘密鍵を無効化する。また、CA証明書を新たに発行し、有効なCA証明書を無効化する。 ・CMPサービス証明書とその秘密鍵を新しく生成し、有効なCMPサービス証明書及びその秘密鍵を無効化する。 ・CAオペレータの操作権を変更する。
T.AUDITOR-PRETENDED（監査者へのなりすまし）	悪意を持つCAオペレータや悪意を持つ組織内第三者が監査者になりすましてアクセスし、以下の行為を行う。 ・監査ログの全てまたは一部を削除する。 ・不正な監査者の証明書を登録する。 ・登録されている監査者の証明書を削除する。
T.CAO-PRETENDED （CAオペレータへのなりすまし）	悪意を持つ組織内第三者がCAオペレータになりすましてアクセスするか、または悪意を持つCAオペレータが他のCAオペレータになりすまして、自CAサービスや同じCAサーバマシン内に構築されている他のCAサービスへアクセスし、以下の行為を行う。 ・発行すべきでない第三者に証明書を発行する。 ・定義されているプロファイルとは異なる形式の証明書・CRLを発行する。 ・データベースで管理する有効な証明書・CRLを削除する。 ・データベースで管理する有効な証明書を失効し、CRLを発行する。 ・操作権を持つ有効なCAオペレータを削除する。 ・CA秘密鍵を新しく生成し、有効なCA秘密鍵を無効化する。また、CA証明書を新たに発行し、有効なCA証明書を無効化する。 ・CMPサービス証明書とその秘密鍵を新しく生成し、有効なCMPサービス証明書及びその秘密鍵を無効化する。 ・CAオペレータの操作権を変更する。 ・CAオペレータを追加し、不正な操作権を設定する。
T.INTERCEPTION（盗聴）	悪意を持つCAオペレータや悪意を持つ組織内第三者が、TOEクライアント操作端末とTOE間の操作端末LANを経由する送受信データを盗聴する。

1.4.6 組織のセキュリティ方針

本TOEは、表5に示す組織のセキュリティ方針に従う機能を備える。

表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.SECUREZONE-CA（セキュアゾーン内のCAサーバマシン）	セキュアゾーンにおいてCAサーバマシンのOSにログオン可能な利用者は、システム管理者に限定されなければならない。
P.SECRET（秘匿）	CAサービスに対し重要な役割を有するCAオペレータがTOEへアクセスするために必要な情報、及び重要な操作を行う際に必要な情報は、システム管理者に対しても秘匿されなければならない。
P.RA-RELIABILITY（RAサービスの信頼性）	CAサービスは、RAサービスからのアクセス要求に対して識別認証を実施し、予め登録されている正当なRAサービスに対してだけアクセスを許可しなければならない。

1.4.7 構成条件

本TOEは、表6で示されるハードウェア、OS上で動作する。また同表に示されるソフトウェアとともに動作する。

表6　TOEの動作に必要なハードウェア、ソフトウェアの諸条件

種類	説明
CPU	Windows版：Intel® Pentium® III 500MHz相当以上。 Solaris OE版：Sun Microsystems, Inc.UltraSPARC® II 400MHz相当以上。
メモリ	512MB以上。
ディスク	証明書発行枚数が100枚までの場合、200MB以上。 100枚を超える場合は、上記に加えて証明書1枚につき200KB必要。
HSM	PKCS#11v2.01に準拠したインタフェースを実装する以下のいずれかのハードウェアセキュリティモジュール。（CA秘密鍵を管理するために使用する） ・　富士通製 暗号プロセッサカード ・　CHRYSALIS-ITS Inc.製 LUNA(R) CA3
OS	Windows版：Microsoft® Windows® 2000 Server + Service Pack 3 Solaris OE版：Sun Microsystems, Inc Solaris (TM) 8 Operating Environment
WWWサーバ	同梱されるWWWサーバ。（InfoProvider Pro）
RDBMS	Oracle Database 8i Release 8.1.7.0.0 またはOracle9i Database Release 2

1.4.8 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7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7　TOE使用の前提条件

識別子	前提条件
ASM.CA-ACCESS（CAサーバマシンのアクセス制限）	CAサーバマシンはセキュアゾーンに設置され、セキュアゾーンへの入室時には物理鍵や認証システムを必要とする。入室する権限はシステム管理者とセキュアゾーンに設置されるその他のサーバマシンの管理者（他サーバマシン管理者）だけが持つ。HSMで管理するCA秘密鍵のバックアップ作業のためCAオペレータがセキュアゾーンに入室する特例では必ずシステム管理者と共に入室し、セキュアゾーンでの作業はシステム管理者の監視の下、共同で実施される。
ASM.TERMINAL-ACCESS（TOEクライアント操作端末へのアクセス制限）	TOEを運用する組織に属する者だけが物理的にTOEクライアント操作端末へアクセスできる。
ASM.CA-KEY（CA秘密鍵の保護）	CA秘密鍵は耐タンパー性のあるHSMで管理されており、物理的な攻撃を行われたとしてもCA秘密鍵が暴露されることはない。
ASM.AUDITOR-CAO-KEY（監査者とCAオペレータの秘密鍵の保護）	監査者、CAオペレータがTOEへアクセスする時に必要となる監査者、CAオペレータの各々の証明書とその秘密鍵は、耐タンパー性のあるICカードに格納されており、物理的な攻撃を行われたとしても秘密鍵が暴露されることはない。
ASM.MEDIA-DATA（媒体の保護）	TOEの運用環境をバックアップしたデータを格納した媒体や監査ログを移出した媒体は、適切な手順に従い保管され、物理的な破壊・盗難から保護されている。
ASM.ADMIN-AUDITOR-RELIABILITY（システム管理者、監査者、他サーバマシン管理者の信頼）	システム管理者、監査者、他サーバマシン管理者は、各自に課せられた役割に対して許可される一連の作業について、悪意を持った行為は行わず、TOEの運用に協力的に関わる。
ASM.SECURE-ENVIRONMENT（セキュアな運用環境の構築と管理）	システム管理者は、CAサーバマシンとその構成要素であるWWWサービス、RDBMS、HSMやCAサーバマシンに接続される機器（サーバコンソールやHSM本体）を適切にセットアップし、セキュアな状態を維持する。この時、システム管理者はSSLクライアント認証に必要なCA証明書、及びTOEの識別認証に必要な監査者証明書やRA証明書を適切に設定する。また、運用環境の復旧のためにTOE内のデータの定期的なバックアップを行う。
ASM.CA-CONNECT（CAサーバマシンへの接続制限）	セキュアゾーンLANはファイアウォールを介して操作端末LANのみと接続され、CAサービスの特定のポートに対してTOEクライアント操作端末とだけ通信できるように設定されている。
ASM.OTHER-RELIABILITY（その他のサーバマシンの信頼）	セキュアゾーンに設置されるCAサーバマシン以外のサーバマシンは、他サーバマシン管理者が適切に設定し、管理するものである。
ASM.IMPORT-DATA-RELIABILITY（インポートデータの信頼	TOEにインポートされるデータは、TOEを運用する組織の責任者が予めその信頼性を確認したものである。

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

以下の『図3　TOEの構成』に示すとおり、本TOEはSW/PkiMGRが提供するCAサービスの基本機能であるSW/PkiMGR CAと、CAサービスの拡張機能を提供するSW/PkiMGR KPOにより構成される。

またTOEは、SW/PkiMGRが提供するRAサービスであるSW/PkiMGR RAと連携して動作する。

図3　TOEの構成

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

認証機関は、評価の過程で評価実施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。

4.2 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アクションエレメントについての確認結果を表8にまとめる。

表8　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。また、当評価に至るまでなされた指摘(所見報告書)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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また､当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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指摘(所見報告書)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。

4.3 注意事項

特になし。

5 用語

本報告書で使用された略語・一般用語を以下に示す。

公開鍵	:	公開鍵暗号方式で使用する鍵ペアのうち、一般に公開される鍵。
証明書	:	X.509に従い発行した公開鍵証明書。公開鍵証明書は利用者の公開鍵を保証するために、CAがディジタル署名をしたもの。
申請書	:	証明書の発行をCAに申請する時に使用するものであり、PKCS#10で規定された形式で作成される。証明書の利用者の名前、公開鍵、利用者のディジタル署名等の情報が格納されている。申請を受けたCAは、利用者のディジタル署名を検証し、有効であれば申請書の情報に基づき証明書を発行する。
相互認証証明書	:	2つのCAが互いの信頼を証明するために認証し合うことを相互認証という。公開鍵を認証するために2つのCAは互いに相手の証明書（相互認証証明書）を発行する。相互認証証明書は証明書と同じ形式である。
秘密鍵	:	公開鍵暗号方式で使用する鍵ペアのうち、一般に公開されない鍵。
ディジタル署名	:	メッセージの受信時に、そのメッセージの送信者を確認する手段。
CA	:	Certification Authority：認証局。利用者の公開鍵に対してディジタル署名を行い、証明書を発行する。またCRLを発行する。
CC	:	Common Criteria：コモンクライテリア。
CMP	:	Certificate Management Protocol：証明書の発行や管理に関するRFC2510で定義されるプロトコル。証明書の発行や失効の要求、及びそれらに対する応答等を行う場合に送信するメッセージの形式を定義。
CRL	:	Certification Revocation List：証明書失効リスト。失効したX.509証明書のリストにCAがディジタル署名をしたもの。
EAL	:	Evaluation Assurance Level：評価保証レベル。
HSM	:	Hardware Security Module：秘密鍵を管理するために使用する物理的な攻撃に強い耐タンパー性ハードウェア。
PKCS	:	Public Key Cryptography Standards：RSA Securityが開発した公開鍵暗号方式の業界標準。 ● PKCS#1は、「RSA暗号を使用した暗号化方法と署名方法」についての規格。 ● PKCS#5は、「パスワードから生成した秘密鍵を使用した暗号化方法」についての規格。 ● PKCS#10は、「証明書の申請構文に関する標準」（CAに証明書の発行を依頼する時の申請書の形式）についての規格。 ● PKCS#11は、「暗号インタフェース」についての規格。 ● PKCS#12は、「個人情報交換構文に関する標準」（証明書とその秘密鍵を暗号化して格納する形式）についての規格。

PKI	:	Public Key Infrastructure：公開鍵暗号方式によるセキュリティ基盤。証明書を使用して通信データ交換を暗号化したり、通信データにディジタル署名を付加したりする場合の基盤となるもの。
PP	:	Protection Profile：プロテクションプロファイル。
RA	:	Registration Authority : 登録局。証明書の発行や失効の申請を審査する等、一般利用者とCAの間において証明書管理を行う。
RDBMS	:	Relational DataBase Management System :「リレーショナルデータモデル」によりデータを管理するデータベース管理システム。
RFC	:	Request for Comments:インターネットに関する技術情報や仕様、運用規則等を規定した文書。IETF（Internet Engineering Task Force）が管理。
RSA	:	Ron Rivest、Adi Shamir、Len Adlemanが提案した暗号化とディジタル署名に使用する公開鍵暗号アルゴリズム。
SOF	:	Strength of Function：機能強度。
SSL	:	Secure Sockets Layer：TCP層とアプリケーション層の間に位置するNetscape社が開発したプロトコル層であり、サーバ・クライアント間における双方向の証明書による認証、暗号通信を可能にする。
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。
X.509	:	ITU-T（International Telecommunication Union-Telecommunication sector）が勧告した証明書とCRLの標準仕様。（ITU-TはITU（国際電気通信連合）の下部組織であり、通信関係の標準化を担当。）

本報告書で使用された用語の定義を以下に示す。

合議制	:	操作毎に予め決められている必要最小人数（2～10人）分のCAオペレータの合意に基づいてCAサービスを操作する仕組み。
プロファイル	:	発行する証明書・CRLの形式についての情報で、利用目的に応じて決める。証明書プロファイルはディジタル署名のアルゴリズム、証明書の有効期間、拡張情報について、CRLプロファイルはCRLの発行間隔、ディジタル署名のアルゴリズム、拡張情報について各々決めたもの。
CA監査端末	:	監査者が監査作業を行う端末。
CAサーバマシン	:	CAサービスを運用するサーバマシン。
CAサービス	:	CAを実現するソフトウェア製品が提供するサービス。
CA操作端末	:	CAオペレータがCAサービスの運用を行う端末。
CMPサービス	:	CMPによりデータの送受信を行うCMPサーバが提供するサービス。CAサービスは本サービスを使用してRAサービスと通信する。
RA管理／監査端末	:	RA管理者やRAの監査者が操作する端末であり、RAサービスの運用環境の設定と監査を実施する。
RAサーバマシン	:	RAサービスを運用するサーバマシン。

RAサービス	：	RAを実現するソフトウェア製品が提供するサービス。
RA設定端末	：	RAのシステム管理者が操作する端末であり、RAサービスの初期設定、及びRA管理者やRAの監査者の登録を行う。
RA操作端末	：	一般利用者の証明書の発行や失効の操作を行う。また発行された証明書の取得を行う。
TOEクライアント操作端末	：	CA監査端末とCA操作端末の総称。
WWWサービス	：	WWWサーバが提供するサービス。

6 参照

[1] SystemWalker/PkiMGR CA セキュリティターゲット　第1.8版　2004年4月9日 富士通株式会社

[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] SystemWalker/PkiMGR CA セキュリティターゲット（第1.8版） 評価報告書 2004年5月11日 第1.0版 02ITSC-E016 社団法人 電子情報技術産業協会 ITセキュリティセンター