Trust-CANP v6.1

Security Target バージョン 1.2.8

Document version control log

Version	Date	Author	Description
1.0	2002/2/18	金岡　文彦	―
1.1	2002/3/22	金岡　文彦	OR 番号： ACY-EORL-0001-00　～ ACY-EORL-0009-00　対応
1.1.1	2002/4/30	金岡　文彦	OR 番号： ACY-EORL-0010-00　～ ACY-EORL-0017-00　対応
1.2	2003/1/9	新井　聡	―
1.2.1	2003/1/22	新井　聡	OR 番号： ACY-EORL-0018-00　～ ACY-EORL-0048-00　対応
1.2.2	2003/1/31	新井　聡	―
1.2.3	2003/2/18	新井　聡	OR 番号： ACY-EORL-0049-00　～ ACY-EORL-0054-00　対応
1.2.4	2003/3/11	新井　聡	OR 番号： ACY-EORL-0050-00 ACY-EORL-0054-00 ACY-EORL-0055-00　対応
1.2.5	2003/6/2	新井　聡	OR 番号： ACY-EORL-0056-00　～ ACY-EORL-0063-00　対応
1.2.6	2003/8/25	新井　聡	OR 番号： ACY-EORL-0064-00 ACY-EORL-0065-00　対応
1.2.7	2004/1/21	新井　聡	OR 番号： ACY-EORL-0066-00　～ ACY-EORL-0068-00　対応
1.2.8	2004/2/6	新井　聡	―

Table of Contents

1 ST introduction

1.1 ST identification

ST 名称 Trust-CANP v6.1 Security Target

バージョン 1.2.8

日付 2004/2/6

著者 NTT Information Sharing Platform Laboratories
Information Security Project金岡　文彦
新井　　聡

キーワード PKI(Public Key Infrastructure)、CA(Certification Authority)、
Certificate(Public Key Certificate)、CRL(Certificate Revocation List)

CC のバージョン ISO/IEC 15408:1999(E) (CC Version 2.1)

注） 日本語訳は「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１－３（平成１３年１月翻訳第１．２版情報処理振興事業協会（IPA）セキュリティセンター)」を使用

1.2 TOE identification

TOE 名称: 「Trust-CANP v6.1」（以下 TOE という。）

1.3 CC conformance

この ST は以下の CC に適合している。

・Part 2 conformant

・Part 3 conformant

1.4 ST overview

本文書は、Trust-CANP v6.1 のセキュリティ仕様を定めたセキュリティターゲットである。TOE は PKI における認証局(CA=Certificate Authority、以下 CA と呼ぶ)を実現するソフトウェア製品である。登録局(RA=Registration Authority、以下 RA と呼ぶ)と連携することで、公開鍵暗号方式を基盤とした電子認証システムの業務を果たす。

電子認証システムはネットワークを介した電子政府及び電子商取引などの実現のために利用されている。

1.5 Evaluation Assurance Level

選択された保証レベルは EAL3 である。

1.6 Conformance to a PP

この ST が適合している PP はない。

2 TOE description

この章では対象となる TOE について、提供する機能、操作者とその業務、TOE が動作するために必要なハードウェア及びソフトウェア、Trust-CANP v6.1 のセキュリティ機能、TOE が送受信するデータについて記述する。

2.1 TOE概説

2.1.1 TOE が提供する機能

Trust-CANP v6.1 は、PKI における CA を実現するソフトウェア製品である。

なお、本文において公開鍵証明書とは、RFC2459 準拠の公開鍵証明書を指し、CRL とは、RFC2459 準拠の公開鍵証明書失効リストを指し、ディレクトリとは、X.500 で規定されたディレクトリを指すこととする。

Trust-CANP v6.1 の主な機能を以下に示す。

- 公開鍵を登録し、その公開鍵証明書を発行する（以下、公開鍵証明書発行と表す。）機能。
- 発行済みの公開鍵証明書を失効する（以下、公開鍵証明書失効と表す。）機能。
- 発行済みの公開鍵証明書を失効禁止にする（以下、公開鍵証明書失効禁止と表す。）機能。
- 発行済みの公開鍵証明書の失効禁止を解除する（以下、公開鍵証明書失効禁止解除と表す。）機能。
- 自らが発行した公開鍵証明書及び CRL をディレクトリサーバに送信する機能。

※以下、「公開鍵証明書発行」、「公開鍵証明書失効」、「公開証明書鍵失効禁止」、「公開鍵証明書失効禁止解除」を「公開鍵証明書発行等」と表す。

2.1.2 TOE を含む製品が提供する機能

Trust-CANP v6.1 を含む製品が CA として提供する機能を述べる。Trust-CANP v6.1 は RA と連携して PKI での CA としての業務を果たしていることから、CA サーバと RA サーバ間のサービスの流れをまず述べるとともに、CA サーバからディレクトリサーバへのサービスの流れと、Trust-CANP v6.1 の運用について触れる。Trust-CANP v6.1 では、連携する RA サーバは、Trust-CANP v6.1 に登録されていなければならない。

一般の利用者が RA に公開鍵証明書発行を申請すると、RA 操作者が RA サーバを操作し、その一般の利用者の公開鍵と秘密鍵を生成し、公開鍵証明書発行に関する RFC2510 及び RFC2797 準拠の申請書（以下、申請書と呼ぶ）を作成し、CA サーバに対し送信する。ここで申請書には、公開鍵証明書発行のコマンドおよび生成する公開鍵

証明書の内容が記され、この申請書を作成した RA の署名が付されている。CA サーバでは、申請書に記されている申請者の登録 ID と申請者の署名により RA を識別認証し、プロセスを立ち上げ、公開鍵証明書発行のコマンドのアクセス制御のチェックを行った後に、申請書の内容に従い、公開鍵を登録し公開鍵証明書を発行する。次に CA サーバから RA サーバに対し、RFC2510 及び RFC2797 準拠の報告書（以下、報告書と呼ぶ）が送信される。ここで報告書には、申請された公開鍵の公開鍵証明書が添付され、CA の署名（以下、CA 署名）が付されている。

RA では、RA 操作者が受け取った公開鍵証明書を先の一般の利用者に渡す。

一般の利用者が RA に公開鍵証明書失効を申請すると、RA 操作者が RA サーバを操作し、公開鍵証明書失効に関する申請書を作成し、CA サーバに対し送信する。ここで申請書には、公開鍵証明書失効のコマンドおよび失効する公開鍵証明書の内容が記され、この申請書を作成した RA の署名が付されている。CA では、申請書に記されている申請者の登録 ID と申請者の署名により RA を識別認証し、プロセスを立ち上げ、公開鍵証明書失効のコマンドのアクセス制御のチェックを行った後に、申請書が示す公開鍵証明書を失効させる。ついで CA サーバから RA サーバに対し、RFC2510 及び RFC2797 準拠の報告書が送信される。ここで報告書には、失効を行った情報が添付され、CA 署名が付されている。RA では、RA 操作者が受け取った結果を先の一般の利用者に渡す。

また、Trust-CANP v6.1 は、定期的に公開鍵証明書が失効しているかを検証し、失効している公開鍵証明書を抽出して、CRL を発行する。

一般の利用者が RA に公開鍵証明書失効禁止を申請すると、RA 操作者が RA サーバを操作し、公開鍵証明書失効禁止に関する申請書を作成し、CA サーバに対し送信する。ここで申請書には、公開鍵証明書失効禁止のコマンドおよび失効する公開鍵証明書の内容が記され、この申請書を作成した RA の署名が付されている。CA では、申請書に記されている申請者の登録 ID と申請者の署名により RA を識別認証し、プロセスを立ち上げ、公開鍵証明書失効禁止のコマンドのアクセス制御のチェックを行った後に、申請書が示す公開鍵証明書を失効禁止にさせる。ついで CA サーバから RA サーバに対し、RFC2510 及び RFC2797 準拠の報告書が送信される。ここで報告書には、失効禁止を行った情報が添付され、CA 署名が付されている。RA では、RA 操作者が受け取った結果を先の一般の利用者に渡す。

一般の利用者が RA に公開鍵証明書失効禁止解除を申請すると、RA 操作者が RA サーバを操作し、RFC2510 及び RFC2797 準拠の公開鍵証明書失効禁止解除に関する申請書を作成し、CA サーバに対し送信する。ここで申請書には、公開鍵証明書失効禁止解除コマンドおよび失効する公開鍵証明書の内容が記され、この申請書を作成した RA の

署名が付されている。CA では、申請書に記されている申請者の登録 ID と申請者の署名により RA を識別認証し、プロセスを立ち上げ、公開鍵証明書の失効禁止解除のコマンドのアクセス制御のチェックを行った後に、申請書が示す公開鍵証明書の失効禁止を解除させる。ついで CA から RA に対し、RFC2510 及び RFC2797 準拠の報告書が送信される。ここで報告書には、公開鍵証明書失効禁止解除を行った情報が添付され、CA 署名が付されている。RA では、RA 操作者が受け取った結果を先の一般の利用者に渡す。

CA サーバは、発行した公開鍵証明書及び発行した CRL を定期的にディレクトリサーバに送信する。

操作者は、CAO 端末から自身のユーザ ID もしくは自身が所属するグループ ID を入力しログインを試みる。（ユーザ ID 及びグループ ID については、後述の 2.3.3 項を参照）CAO 端末は、入力したユーザ ID もしくは入力したグループ ID に対して、操作者が保有する IC カードに格納された秘密鍵を用いて署名を付す(以下、IC カードの署名と表す)。IC カードの署名が付されたユーザ ID もしくは IC カードの署名が付されたグループ ID を CAO 端末から CA サーバに送信し CA サーバで識別認証されログインし操作権限を与えられる。操作者は、Trust-CANP v6.1 を管理する組織の責任者または CA 管理者の指示に基づき運用作業を行う。CA 操作者の運用作業には、申請書による他 CA 及び RA の公開鍵証明書発行等の作業、コマンド操作による CRL の発行およびコマンド操作による CA の鍵対の管理操作（CA の鍵対（秘密鍵及び公開鍵）の生成、削除、バックアップ及びリストア）が含まれる。コマンド操作は、コマンド入力後、コマンドのアクセス制御のチェックを行った後に、実行される。他 CA 及び RA の公開鍵証明書発行等の作業は、RA と同様に、CAO 端末から CA サーバへ申請書を送信し、おのおの、コマンドのアクセス制御のチェックを行った後に、CA サーバ内で公開鍵証明書発行、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処理を行い、CA サーバから CAO 端末へ報告書を送信することである。

2.1.3 補足説明

本 ST を説明する上で、以下に補足説明する。

- Trust-CANP　v6.1 での CA サーバ構築時に、CA の鍵対（秘密鍵及び公開鍵）は、HSM(ハードウェアセキュリティモジュール)内で HSM ドライバを用いて CA 管理者が生成する。CA 運用開始後、CA の鍵対の管理操作として、CA の鍵対の生成、削除、バックアップ及びリストアは、CA 管理者の指示のもと、CA 管理者及び CA 操作者によって、HSM ドライバを用いて行われる。ここで、HSM ドライバは TOE 外の製品である。

- 操作者の IC カードには、操作者の秘密鍵と公開鍵証明書と PIN が格納されている。本人確認のために PIN の入力が必要であるが、本 TOE の操作者の識別認証は IC カードの署名に基づいて行っており、IC カードの所有者が本人であるとの前提に立つ。

- 一つの CA サーバ内に複数の CA を論理的に構築することは可能だが、本 ST では一つの CA での構築を前提で記述する。

2.2 操作者とその業務

Trust-CANP v6.1 を管理する組織の責任者は、表 2-1 に示す業務を担う操作者を決定する。

表 2-1 操作者とその業務

操作者	業務
CA 管理者	CA の運用ポリシーの決定と運用の統括管理を行う。また、ハードウェア及びソフトウェアの管理を行うシステム管理者の業務を兼任する。 CA 管理者、CA 操作者、監査人を登録、削除を行い、TOE 内でのすべての操作を設定する。
CA 操作者	CA 管理者の指示のもと、CA を CAO 端末から運用操作する。 他 CA 及び RA の公開鍵証明書発行等を行い、CA の鍵対の管理操作も行う。 なお、CA の鍵対の管理操作の場合は、CA 操作者の鍵管理操作が CA の鍵対の管理操作に対する複数人操作の人数に達したとき、鍵管理操作が許可される。
監査人	ログ参照の操作権限が与えられ、CAO 端末を操作して CA の運用の検査・分析を行う。監査結果を監査依頼者に報告する。

2.3 TOEの構成及び機能

TOE を含む製品の構成について示す。

2.3.1 TOE が機能するために必要なハードウェア構成

図 2-1 に TOE を含む製品のハードウェアの構成を示す。

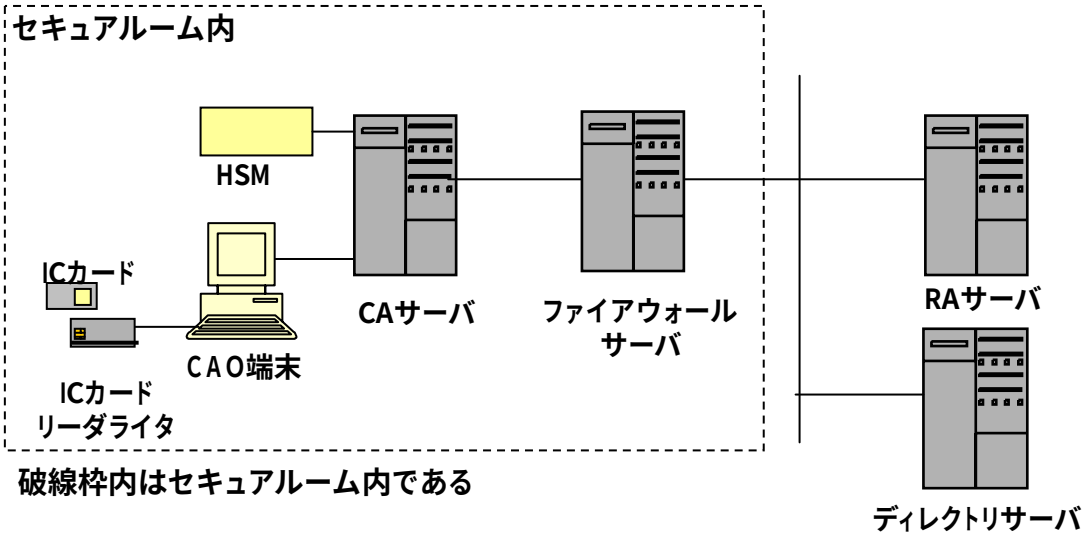


図 2-1 TOE が機能するために必要なハードウェア構成

CA サーバ

後述する Trust-CANP v6.1(CA サーバ)と OS と Web サーバとデータベース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。

ハードウェア条件としては、Solaris 8 が動作可能であり、メモリは 1GB 以上、ハードディスクドライブの容量は 20GB 以上である。

HSM

CA の鍵対を生成、削除、バックアップ、リストアするために用いるハードウェア。

FIPS 140-1 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、ハードウェアの直接攻撃によって暴露もしくは改ざんされない。

CA サーバに SCSI ケーブルで接続されている。

動作保証環境は、nShield SCSI 300、ファームウェアのバージョンは 1.70.0 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 と後述の Trust-CANP v6.1(CAO 端末)がインストールされている。

CA サーバとはイーサネットを通して接続され、IC カードリーダライタとはシリアル

ケーブルで接続される。

端末のハードウェア条件としては、DOS/V マシンであり、メモリは 256MB 以上、ハードディクスドライブ 1GB 以上である。

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。

CAO 端末にシリアルケーブルで接続されている。

動作保証環境では、ActivCard 1.1 が読み書き可能な IC カードリーダライタを用いる。

IC カード

CAO 端末の操作者が所有する IC カード。操作者の秘密鍵、及び PIN の２つが格納されており、それらは暴露、改ざんされないものとする。

IC カードリーダライタに挿入して使用する。

動作保証環境では、ActivCard 1.1 を用いる。

ファイアウォールサーバ

CA サーバから、CAO 端末以外の外部機器との接続の間に構築するファイアウォールサービス機能を持ったハードウェア。

このファイアウォールサーバによって、外部からの CA サーバへの許可するプロトコルは、SSL 及び TLS に限定し、外部からの DOS(Deny of Service)攻撃を拒絶する能力もある。

検証時には FireWall-1 Version 4.0 がインストールされたサーバを用いる。

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。

CA サーバとは、 ファイアウォールを介して接続され、SSL により通信処理が行われる。

検証時には、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

公開鍵証明書及び CRL を LDAPv3 準拠のディレクトリサービスに基づいて、提供するサーバ。CA サーバとは ファイアウォールを介して接続され、SSL または TLS により通信処理が行われる。

検証時には、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。

また、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、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セキュアルームに設置される。

2.3.2 TOE が機能するために必要なソフトウェア

図 2-2 に TOE を含む製品のソフトウェア構成図を示し、以下に説明を行う。

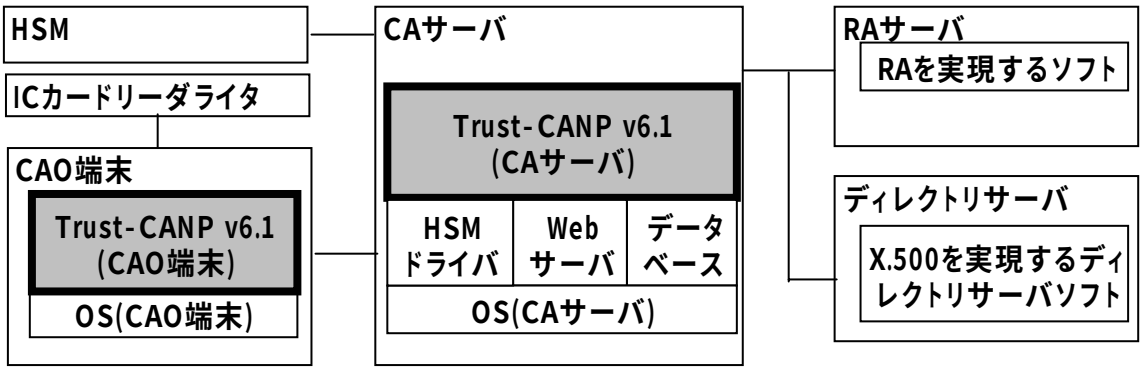


図 2-2 TOE が機能するために必要なソフトウェア構成図

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。

TOE の範囲外である。

使用する OS は、Solaris 8 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。

TOE の範囲外である。

使用する OS は、Microsoft Windows 2000 Professional Service Pack 2 である。

データベース

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。

TOE の範囲外である。

使用するデータベースソフトは、Oracle8*i* Enterprise Edition R8.1.7 である。

Web 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。

TOE の範囲外である。

使用する Web サーバは、Apache 1.3.21 である。

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 を用いた CA の鍵対の生成、削除、バックアップ及びリストアする機能を備えている。

使用するソフトは、nShield SCSI 300 のドライバである。

TOE の範囲外である。

Trust-CANP v6.1(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 の範囲内である。

Trust-CANP v6.1(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 の範囲内である。

2.3.3 Trust-CANP v6.1 のセキュリティ機能及びその周辺のセキュリティに関わる機能

以下に Trust-CANP v6.1 のセキュリティに関わる部分の機能を列挙し、各機能が CA サーバ及び CAO 端末にどのように機能分担されているかを図 2-3 に示す。

Trust-CANP v6.1 は、利用者情報テーブルとロールテーブルを有し、操作者は操作者ごとに、RA は RA ごとに登録 ID によって識別を行う。利用者情報テーブルは、ユーザ ID、グループ ID、登録 ID 及び操作者の公開鍵証明書か RA の公開鍵証明書の情報を有し、操作者と RA の登録 ID を決定できる。また、ロールテーブルは、登録 ID により決定するアクセス権限を有するロールを決定する。

端末操作機能 (CAO 端末)

CAO 端末上で作成した署名する前の申請書(以下、署名前の申請書と表す)に対して、またはユーザ ID またはグループ ID に対して、IC カードによって生成された署名付与する機能。この機能は、TOE の範囲内である。

操作者認証機能 (CA サーバ)

操作者に対して、識別認証する機能。また、CA 署名の検証、RA の署名の検証、及び IC カードの署名の検証を行う機能もそなえている。この機能は、TOE の範囲内である。

クライアント認証機能 (CA サーバ)

RA に対して、識別認証する機能。また、CA 署名の検証、RA の署名の検証、及び IC カードの署名の検証を行う機能もそなえている。この機能は、TOE の範囲内である。

アクセス制御機能 (CA サーバ)

保護資産である、申請書、報告書、公開鍵証明書、CRL に対して、アクセス制御を行う機能。詳細においては以下のような機能である。

- 公開鍵証明書発行、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 CA 操作者、CA 管理者及び RA に制限する機能。

・ CRL の作成を CA 操作者および CA 管理者に制限する機能。
・ CRL 作成するために、公開鍵証明書を参照、更新する機能。

また、公開鍵証明書発行等に関連し、以下の署名検証機能や署名を付す機能も有している。

・ 署名する前の報告書（以下、署名前の報告書と表す）に HSM が生成した CA 署名を付す機能。
・ 署名する前の公開鍵証明書（以下、署名前の公開鍵証明書と表す）に HSM が生成した CA 署名を付す機能。
・ 署名する前の CRL（以下、署名前の CRL と表す）に HSM が生成した CA 署名を付す機能。

この機能は、TOE の範囲内である。

運用支援機能 (CA サーバ)

操作者に対して、Trust-CANP v6.1 を運用するための操作を許可する機能。

Trust-CANP v6.1 を運用するための操作として、アーカイブ及びログに対しての CA 署名を行う周期の変更、CA の鍵対の管理操作に対する複数人操作の人数の変更、利用者情報テーブルのユーザ ID 及びグループ ID 及び登録 ID 及び操作者の公開鍵証明書か RA の公開鍵証明書の登録及び削除、ロールテーブルの登録 ID 及び登録 ID により決定するロールの登録及び削除、CA の鍵対の管理操作、アーカイブ及びログの閲覧がある。

この機能は、TOE の範囲内である。

履歴管理機能 (CA サーバ)

公開鍵証明書、CRL、申請書、報告書の履歴を日付、時刻とともに記録したアーカイブ(以下、アーカイブと表す)及び、CA サーバのサービス履歴ログ、運用ログ(以下、ログと表す)を生成し、アーカイブ及びログに対して署名を付して、許可された操作者のみ閲覧可能な状態として読み出す機能。

アーカイブ及びログに対しての署名は、Keyed-Chain-Hash を用いるハッシュ署名と CA 署名の２種類ある。アーカイブ及びログを記録するごとに行われる署名にはマシン負荷の少ないハッシュ署名を用い、管理者が定める周期ごとに行われる署名には CA 署名を用いる。

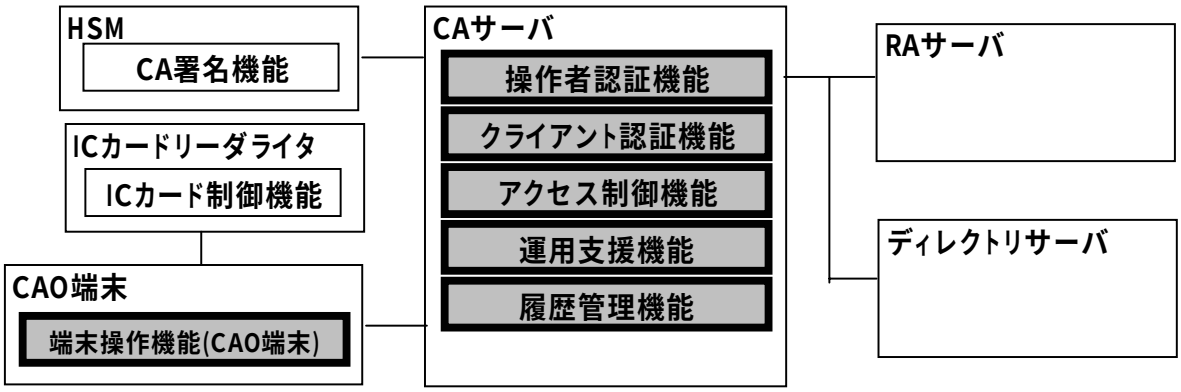
この機能は、TOE の範囲内である。

CA 署名機能 (HSM)

CA 署名を生成する機能。この機能は、TOE の範囲外である。

IC カード制御機能 (IC カードリーダライタ)

IC カードにアクセスおよび IC カードの署名を生成する機能。この機能は、TOE の範囲外である。

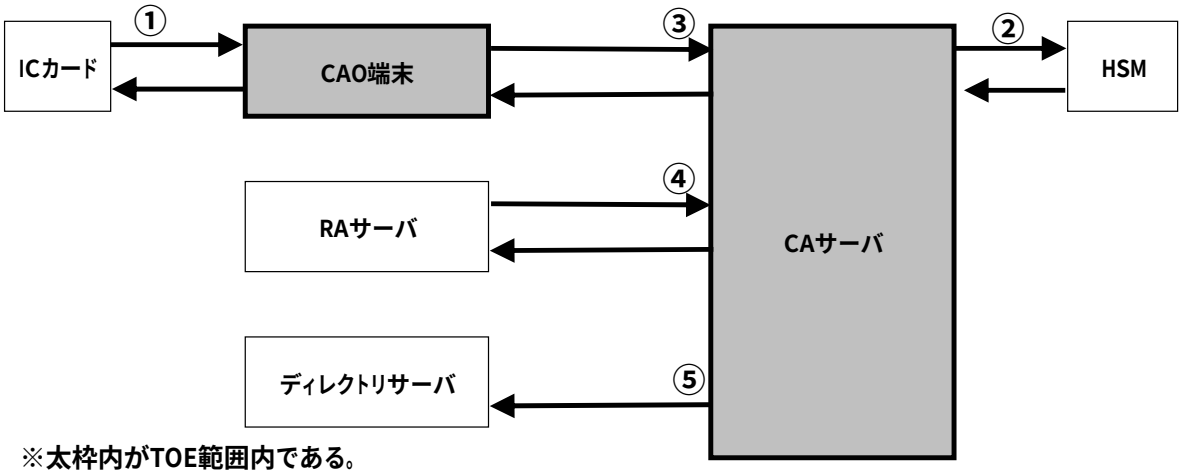


※太枠内がTOEのセキュリティ機能である。

図 2-3 TOE のセキュリティ機能について

2.4 TOEが送受信するデータ

TOE の理解を深めるために、TOE に関連する機器が送受信するデータの内容を図 2-4 に示す。



※太枠内がTOE範囲内である。

図 2-4 TOE に関連する機器が送受信するデータ

①IC カード→IC カードリーダライタ→CAO 端末(平文)

- IC カードの署名が付されたユーザ ID
- IC カードの署名が付されたグループ ID
- 申請書

CAO 端末→IC カードリーダライタ(平文)

- ユーザ ID
- グループ ID
- 署名前の申請書

②CA サーバ→HSM(平文)

- 署名前の報告書

HSM→CA サーバ(平文)

- 報告書

③CAO 端末→CA サーバ(SSL 通信)

- コマンド操作
- IC カードの署名が付されたユーザ ID
- IC カードの署名が付されたグループ ID
- 申請書

CA サーバ→CAO 端末(SSL 通信)

- コマンド操作の結果
- 報告書

④RA サーバ→CA サーバ(SSL 通信)

- 申請書

CA サーバ→RA サーバ(SSL 通信)

- 報告書（公開鍵証明書含む）

⑤CA サーバ→ディレクトリサーバ (SSL または TLS 通信)

- 公開鍵証明書
- CRL

3 TOE security environment

3.1 Assets

TOE では、以下を保護資産とする。保護資産は論理的にはすべて CA サーバの TOE 範囲内にある。

- 申請書
- 報告書
- 公開鍵証明書
- CRL
- ログ
- アーカイブ
- ユーザ ID
- グループ ID
- 登録 ID
- 登録 ID により決定するロール
- アーカイブ及びログに対しての CA 署名を行う周期
- CA の鍵対の管理操作に対する複数人操作の人数

3.2 Assumptions

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。

3.3 Threats

T.AUTH 1

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.AUTH 2

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。

3.4 Organisational security policies

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 が不正にアクセスされることのないようにしなければならない。

4 Security objectives

4.1 Security objectives for the TOE

SO.AUTH

TOE は、CAO 端末からログインしてきた操作者を識別認証しなければならない。

SO.PRIVILEGES

TOE は、正当な利用者に対して、役割ごとに許可された操作のみ行うことができることを保証する。

SO.LOG_GEN

TOE は、不正なアクセス行為などがあった場合に、後から正しく分析することができるようにするために、許可された操作者のみに閲覧可能なアーカイブ及びログを生成しなければならない。

SO.AUDIT_DATA

TOE は、アーカイブ及びログに対して改ざんまたは削除を検出することが可能でなければならない。

SO.RA_AUTH

TOE は、RA から申請書を受信した場合、RA を識別認証しなければならない。

SO.CA_SIGN

TOE は、改ざんの検知および CA の本人性が確認できるように、公開鍵証明書、CRL 及び報告書を作成しなければならない。

TOE は、申請書の改ざんを検知しなければならない。

4.2 Security objectives for the environment

4.2.1 Security objectives for the IT environment

SOE.CA_SIGN

HSM は、CA の秘密鍵を用いて署名を行なわなければならない。

SOE.CA_KEY

HSM に格納されている CA の秘密鍵は、セキュアに鍵管理操作されなければならない。

SOE.IC_CARD_SIGN

IC カードは、IC カードの署名を行なうために、IC カードの秘密鍵にて署名を行わなければならない。

SOE.SSL

CA サーバと CAO 端末間、CA サーバと RA 間は SSL を、CA サーバとディレクトリサーバ間は、SSL もしくは TLS を用いなければならない。

SOE.DB&OS

データベース及び OS は、TOE がセキュアに機能するように、信頼される動作を提供しないといけない。

4.2.2 Security objectives for the non-IT environment

SOE.PHYSICAL_PROTECT

CA サーバ及び CAO 端末及び HSM 及び 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なければならない。

SOE.HSM

CA の秘密鍵は、FIPS140-1 レベル 3 相当の HSM によって保護されなければならない。

SOE.IC_CARD

IC カードは、PIN によって操作者を認証できなければならない。

SOE.FIREWALL

CA サーバとセキュアルーム外との通信に対して、すべてファイアウォールサーバを通して行わなければならない。そのファイアウォールサーバには、SSL 及び TLS 以外の通信を排除し、DOS 攻撃から保護されるよう設定されなければならない。

SOE.UTILITY

TOE を管理する組織の責任者もしくは CA 管理者は、CA サーバ、HSM 、 CAO 端末、IC カードリーダライタ、IC カード、ファイアウォールサーバ、OS（CA サーバ)、OS（CAO 端末)、データベース及び Web サーバが製品仕様通りに動作していることを定期的に確認しなければならない。

SOE.ADMIN

TOEを管理する組織の責任者は、信頼される人物をCA管理者に任命し、セキュリティポリシーを教育しなければならない。

SOE.OPERATOR

CA管理者は、CA操作者がセキュリティポリシーに従って操作するように管理しなければならない。

SOE.MANAGEMENT

TOE を管理する組織の責任者は、組織内部セキュリティポリシーを作成し、そのポリシーに基づいたガイダンス文書を作成する。その上で CA 管理者、CA 操作者、監査人を適切に指導しポリシーを実施させなければならない。

SOE.PASSWORD

TOE を管理する組織の責任者及び CA 管理者は、パスワードの安全性を保てるように、TOE に関連するパスワードの運用規則を定めなければならない。

SOE.DB&OS_ADM

TOE を管理する組織の責任者及び CA 管理者は、TOE がセキュアに機能するように、データベース及び OS を管理しなければならない。

5 IT security requirements

以下に、CC からのセキュリティ要件の操作の方法について記述する。

選択の場合：［選択:*選択した内容*］のように表記する。

割付の場合：［割付:*割付した内容*］のように表記する。

繰返しの場合：機能要件を識別する名称の後に(　)で数値を記す。

詳細化の場合：［詳細化:*詳細化した内容*］のように表記する。

5.1 TOE security requirements

5.1.1 TOE security functional requirements

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択:*指定なし*]レベルのすべての監査対象事象; 及び

c) [割付:*表 5-1 で下線に示すもの*]。

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付:*なし*]

依存性: FPT_STM.1 高信頼タイムスタンプ

表 5-1 監査対象事象一覧

機能要件	CC で定義された監査対象	監査事象	生成される監査記録
FAU_GEN.1	監査対象とすべき識別されたアクションはない。	なし	－
FAU_GEN.2	監査対象とすべき識別されたアクションはない。	なし	－
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	a) アーカイブ及びログの閲覧を行うとき	ログ
FAU_SAR.2	a) 基本: 監査記録からの成功しなかった情報読み出し。	a) アーカイブ及びログの閲覧を行うとき	ログ
FAU_STG.1	監査すべき識別されたアクションはない。	なし	ログ
FAU_STG.3	a) 基本: 閾値を超えたためにとられるアクション。	a) アーカイブ及びログの合計容量が TOE 構築時に設定した量を超えたとき	ログ

FCS_COP.1(1)	a) 最小: 成功と失敗及び暗号操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	a)b) ハッシュ署名の生成及び検証したとき	ログ
FCS_COP.1(2)	a) 最小: 成功と失敗及び暗号操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	a)b) IC カードの署名の検証、RA の署名の検証または CA 署名の検証したとき	ログ
FDP_ACC.2	監査対象にすべき識別された事象はない。	なし	—
FDP_ACF.1	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	a)b)c) 申請書の書込、読出のとき a)b)c) 公開鍵証明書の書込、更新、読出のとき a)b)c) 報告書の書込、読出のとき a)b)c) CRL の書込、読出のとき	アーカイブ及びログ
FDP_ITT.1	a) 最小: 使用された保護方法の識別を含む、利用者データの成功した転送。 b) 基本: 使用された保護方法と生じたいかなる誤りも含む、利用者データを転送するためのすべての試み。	a) IC カードの署名の検証または CA 署名の検証したとき	ログ
FDP_UIT.1	a) 最小: データ交換メカニズムを使用する利用者あるいはサブジェクトの識別情報。 b) 基本: データ交換メカニズムの使用を試みる、不当な利用者あるいはサブジェクトの識別情報。 c) 基本: 送信あるいは受信された利用者データの識別に利用できる名前、あるいはそれ以外のインデックス情報の参照。これは利用者データに関連するセキュリティ属性を含むことができる。 d) 基本: 利用者データの送信を妨害する識別された試み。 e) 詳細: 送信された利用者データに対する、検出された改変の種別及び/あるいは影響。	a) CA 署名を生成し、それを付したとき a) RA の署名の検証または CA 署名の検証したとき	ログ
FIA_ATD.1	監査対象にすべき識別されたアクションはない。	なし	—
FIA_UAU.2	最小: 認証メカニズムの不成功になった使用; 基本: 認証メカニズムのすべての使用。	最小)基本) 操作者もしくは RA を識別認証するとき	ログ

FIA_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	a)b)操作者もしくは RA を識別認証するとき	ログ
FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功及び失敗)。	a)b)操作者もしくは RA を識別認証するとき	ログ
FMT_MOF.1	a) 基本: TSF の機能のふるまいにおけるすべての改変。	a) HSM ドライバを用いた CA の鍵対の生成、削除、バックアップ及びリストアのとき	ログ
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	a)利用者情報テーブルのユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書の登録または削除のとき a)ロールテーブルの登録 ID、登録 ID により決定するロールの登録または削除のとき	ログ
FMT_MSA.2	a) 最小: セキュリティ属性に対して提示され、拒否された値すべて; b) 詳細: セキュリティ属性に対して提示され、受け入れられたセキュアな値すべて。	a) IC カードの署名の検証、RA の署名の検証または CA 署名の検証したとき	ログ
FMT_MTD.1	a) 基本: TSF データの値のすべての改変。	a)アーカイブ及びログに対しての CA 署名を行う周期の改変のとき a)CA の鍵対の管理操作に対する複数人操作の人数の改変のとき a)アーカイブ及びログの改変のとき	ログ
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	a)CA の鍵対の管理操作に対する複数人操作の人数の改変のとき a)利用者情報テーブルのユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書の登録または削除のとき a) ロールテーブルの登録 ID、登録 ID により決定するロールの登録または削除のとき	ログ
FPT_RVM.1	監査対象にすべき識別されたアクションはない。	なし	―

FAU_GEN.2 利用者識別情報の関連付け

下位階層: なし

FAU_GEN.2.1 TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性: FAU_GEN.1 監査データ生成
FIA_UID.1 識別のタイミング

FAU_SAR.1 監査レビュー

下位階層: なし

FAU_SAR.1.1 TSF は、[割付: *CA 管理者、監査人*]が、[割付:*事象に日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)*]を監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.2 限定監査レビュー

下位階層: なし

FAU_SAR.2.1 TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

依存性: FAU_SAR.1 監査レビュー

FAU_STG.1 保護された監査証跡格納

下位階層: なし

FAU_STG.1.1 TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査記録の改変を[選択:*検出*]できねばならない。

依存性: FAU_GEN.1 監査データ生成

FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層: なし

FAU_STG.3.1 TSF は、監査証跡が[割付: *TOE 構築時に設定した量*]を超えた場合、[割付: *警告表示を出し、下記以外の TOE の機能の停止*]をとらなければならない。

＜停止しない機能＞

・監査レビュー機能

・ハッシュ署名の検証機能

依存性: FAU_STG.1 保護された監査証跡格納

FCS_COP.1(1) 暗号操作

下位階層: なし

FCS_COP.1(1).1 TSF は、[割付:*表 5-2 の標準*]に合致する、特定された暗号アルゴリズム[割付:*表 5-2 のアルゴリズム*]と暗号鍵長[割付:*なし*]に従って、[割付:*ハッシュ署名の生成、検証*]を実行しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 5-2 ハッシュ署名のアルゴリズム

アルゴリズム	暗号操作	標準
SHA-1	ハッシュ署名の生成、検証	FIPS 180-1

FCS_COP.1(2) 暗号操作

下位階層: なし

FCS_COP.1(2).1 TSF は、[割付:*表 5-3 の標準のいずれか*]に合致する、特定された暗号アルゴリズム[割付:*表5-3のアルゴリズム*]と暗号鍵長[割付:*表5-3のアルゴリズムの鍵長*]に従って、[割付:*IC カードの署名の検証、RA の署名の検証または CA 署名の検証*]を実行しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 5-3 署名アルゴリズムとその鍵長

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

FDP_ACC.2 完全アクセス制御

下位階層: FDP_ACC.1

FDP_ACC.2.1 TSF は、[割付: *CANP アクセス制御 SFP*]を[割付: *アクセス制御の対象となる以下のサブジェクト、オブジェクト*]及び SFP でカバーされるサブジェクトとオブジェクト間のすべての操作に対して実施しなければならない。

<アクセス制御の対象となるサブジェクト>

・CA 管理者プロセス

・CA 操作者プロセス

・監査人プロセス

・RA プロセス

<アクセス制御の対象となるオブジェクト>

・申請書テーブル
・報告書テーブル
・公開鍵証明書テーブル
・CAO 端末への送信ポート
・CAO 端末からの受信ポート
・RA への送信ポート
・RA からの受信ポート

FDP_ACC.2.2 TSF は、TSC 内の任意のサブジェクトと TSC 内の任意のオブジェクト間のすべての操作がアクセス制御 SFP でカバーされることを保証しなければならない。

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1 TSF は、[割付: *登録 ID により決定するロール*]に基づいて、オブジェクトに対して、[割付: *CANP アクセス制御 SFP*]を実施しなければならない。

FDP_ACF.1.2 TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付:*表 5-4 の規則*]。

FDP_ACF.1.3 TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付:*なし*]。

FDP_ACF.1.4 TSF は、[割付:*なし*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

表 5-4 CANP アクセス制御規則

登録 ID により決定するロールに基づく、制御されたサブジェクト	制御されたオブジェクト	許される操作
CA 管理者プロセス	申請書テーブル	書込、読出
	報告書テーブル	書込、読出
	公開鍵証明書テーブル	書込、読出、更新
	CRL テーブル	書込
	CAO 端末への送信ポート	送信
	CAO 端末からの受信ポート	受信
CA 操作者プロセス	申請書テーブル	書込、読出
	報告書テーブル	書込、読出
	公開鍵証明書テーブル	書込、読出、更新

	CRL テーブル	書込
	CAO 端末への送信ポート	送信
	CAO 端末からの受信ポート	受信
RA プロセス	申請書テーブル	書込、読出
	報告書テーブル	書込、読出
	公開鍵証明書テーブル	書込、読出、更新
	RA への送信ポート	送信
	RA からの受信ポート	受信
監査人プロセス	なし	なし

FDP_ITT.1 基本内部転送保護

下位階層: なし

FDP_ITT.1.1 TSF は、利用者データが TOE の物理的に分離されたパート間を転送される場合、その[選択:*改変*]を防ぐための[割付: ***CANP アクセス制御 SFP***]を実施しなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]

FDP_UIT.1 データ交換完全性

下位階層: なし

FDP_UIT.1.1 TSF は、利用者データを[選択:*改変*]誤りから保護した形で[選択:*送信*、*受信*]できるようにするために、[割付: ***CANP アクセス制御 SFP***]を実施しなければならない。

FDP_UIT.1.2 TSF は、利用者データ受信において、[選択:*改変*]が生じたかどうかを判定できなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
[FTP_ITC.1 TSF 間高信頼チャネル、または
FTP_TRP.1 高信頼パス]

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付*:* 以下のセキュリティ属性のリスト]を維持しなければならない。

＜セキュリティ属性のリスト＞

利用者情報テーブル｛ユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書｝
ロールテーブル｛登録 ID、登録 ID により決定するロール｝

依存性: なし

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1 TSFは、適切な利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。

依存性: FIA_ATD.1 利用者属性定義

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1 TSF は、機能[割付: *HSM ドライバを用いた CA の鍵対の生成、削除、バックアップ及びリストア*][選択:*を動作させる*]能力を[割付: *CA の鍵対管理用複数人操作者ロール*]に制限しなければならない。

依存性: FMT_SMR.1 セキュリティ役割

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1 TSF は、セキュリティ属性[割付: 以下のセキュリティ属性のリスト]に対し[選択:*削除*、[割付:*登録*]]をする能力を[割付:*CA 管理者ロール*]に制限するために[割付: *CANP アクセス制御 SFP*]を実施しなければならない。

＜セキュリティ属性のリスト＞

利用者情報テーブル｛ユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書｝

ロールテーブル｛登録 ID、登録 ID により決定するロール｝

依存性: [FDP_ACC.1 サブセットアクセス制御または

FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.2 セキュアなセキュリティ属性

下位階層: なし

FMT_MSA.2.1 TSF は、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性: ADV_SPM.1 非形式的 TOE セキュリティ方針モデル
[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

FMT_MTD.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[割付:*表 5-5 の TSF データ*]を[選択:*改変*、 [割付: *なし*]]する能力を[割付:*表 5-5 に示したロール*]に制限しなければならない。

依存性: FMT_SMR.1 セキュリティ役割

表 5-5 TSF データとロールによる許可された動作

TSF データ	ロール	許可される操作
アーカイブ及びログに対しての CA 署名を行う周期	CA 管理者ロール	改変
CA の鍵対の管理操作に対する複数人操作の人数	CA 管理者ロール	改変

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割[割付:*CA 管理者ロール*、*CA 操作者ロール*、*監査人ロール*、*RA ロール*、*CA の鍵対管理用複数人操作者ロール*]を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

適用上の注釈：「CA の鍵対管理用複数人操作者ロール」は、CA の鍵対管理操作を行う CA 操作者の人数が「CA の鍵対の管理操作に対する複数人操作の人数」に達したときに、与えられるロールである。

FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

5.1.2 TOE security assurance requirements

本 TOE の保証要件は EAL3 からなる。これらは CC part3 から選択されている。

5.2 Security requirements for the IT environment

FCS_CKM.1 暗号鍵生成

下位階層: なし

FCS_CKM.1.1 [詳細化:*HSM*]は、以下の[割付: *表 5-3 の標準のいずれか*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *表 5-3 のアルゴリズム*]と指定された暗号鍵長[割付: *表 5-3 のアルゴリズムの鍵長*]に従って、暗号鍵を生成しなければならない。

依存性: [FCS_CKM.2 暗号鍵配付
または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4 暗号鍵破棄

下位階層: なし

FCS_CKM.4.1 [詳細化:*HSM*]は、以下の[割付: *表 5-3 の標準のいずれか*]に合致する、指定された暗号鍵破棄方法[割付: *HSM の鍵の廃棄方法*]に従って、暗号鍵を破棄しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1(3) 暗号操作

下位階層: なし

FCS_COP.1(3).1 TSF は、[割付:*表 5-3 の標準のいずれか*]に合致する、特定された暗号アルゴリズム[割付:*表 5-3 のアルゴリズム*]と暗号鍵長[割付:*表 5-3 のアルゴリズムの鍵長*]に従って、[割付:*CA 署名の生成*]を実行しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1(4) 暗号操作

下位階層: なし

FCS_COP.1(4).1 TSF は、[割付:*表 5-3 の標準のいずれか*]に合致する、特定された暗号アルゴリズム[割付:*表5-3のアルゴリズム*]と暗号鍵長[割付:*表5-3のアルゴリズムの鍵長*]に従って、[割付:*IC カードの署名の生成*]を実行しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FPT_SEP.1 TSFドメイン分離

下位階層: なし

FPT_SEP.1.1 [詳細化: *データベース及びOS*]は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2 [詳細化: *データベース及びOS*]は、[詳細化: *データベース及びOSコントロール範囲*]内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性: なし

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1 [詳細化: *CAサーバのOS*]は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性: なし

FTP_ITC.1 TSF間高信頼チャネル

下位階層: なし

FTP_ITC.1.1 [詳細化: *Web サーバ*]は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露か

らのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2[詳細化: *Web サーバ*]は、[選択: *TSF*、*リモート高信頼 IT 製品*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3 [詳細化: *Web サーバ*]は、[割付: *申請書の受信*、*報告書の送信*、*公開鍵証明書の送信*、*CRL の送信*]のために、高信頼チャネルを介して通信を開始しなければならない。

依存性: なし

5.3 Minimum strength of function (SOF) claim

本 TOE における Minimum strength of function レベルを、SOF-basic としてクレームする。確率的または順列的メカニズムを利用する機能要件は、FCS_COP.1(1)、FCS_COP.1(2)であり、Minimum strength of function として、ハッシュ暗号アルゴリズムのみである FCS_COP.1(1)及び、署名アルゴリズムの一部としてハッシュ暗号アルゴリズムを用いている FCS_COP.1(2)のハッシュ暗号アルゴリズム部分を対象とする。

6 TOE summary specification

6.1 TOE security functions

SF.CAO_OPERATE 端末操作機能

SF.CAO_OPERATE は、次のように、CAO 端末を用いて、CA サーバにログイン、もしくは CAO 端末上で「申請書」作成の処理を行う。

(ア) CAO 端末を用いて、CA サーバにログインするとき

① CAO 端末にて入力された「ユーザ ID またはグループ ID」に対して、IT 環境の IC カードによって生成された（IT 環境の IC カードの FCS_COP.1(4)）署名を付す。署名は、認証および改ざんの検知に用いる。(FDP_ITT.1、FIA_UAU.2) 使用できる署名アルゴリズムは表 6-1 に示す標準に従ったいずれかのアルゴリズム及び鍵長を選択できる。

② ①を CA サーバへ送信する。

③ CA サーバより、識別認証の成功、失敗の情報を受信し、成功の場合は、CA サーバに対して、「申請書」送信や TSF データの更新（改変）などのオペレーションを行う。

(イ) CAO 端末を用いて、「申請書」を作成するとき

CAO 端末にて作成された「署名前の申請書」に対して、IT 環境の IC カードによって生成された（IT 環境の IC カードの FCS_COP.1(4)）署名を付して、改ざんが検知できるような「申請書」を作成する(FDP_ITT.1)。使用できる署名アルゴリズムは表 6-1 に示す標準に従ったいずれかのアルゴリズム及び鍵長を選択できる。

表 6-1 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

対応する機能要件： FDP_ITT.1、FIA_UAU.2

SF.CAO_AUTH 操作者認証機能

SF.CAO_AUTH は、次のように操作者の識別認証を行う。

① CAO 端末から「ユーザ ID またはグループ ID＋IT 環境の IC カードの署名」を受信する。

② 受信した「ユーザ ID またはグループ ID」を元に、操作者を識別する。

③ IC カードの署名を検証（FCS_COP.1(2)）することによって、認証を行い、識別認証が成功したことを CAO 端末に送信する。

IC カードの署名の検証時には、検証に使う公開鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。
・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）
このチェックにより、有効でない場合はエラーを返す。

④ CA サーバから「ユーザ ID 及びグループ ID」を含んだ操作者の登録 ID が決定される（FIA_UAU.2、FIA_UID.2）。

⑤ 識別認証された操作者に対するプロセスが立ち上がる。

また、SF.CAO_AUTH は、次のような機能を持つ。

- CAO 端末からの経路のアクセスで、識別認証されるまで、CA サーバに対して、いかなる操作も行うことができない（FIA_UAU.2、FIA_UID.2、FPT_RVM.1）
- IC カードの署名を検証する際に使用できる署名アルゴリズムは表 6-1 に示す標準に従ったいずれかのアルゴリズム及び鍵長を選択できる（FCS_COP.1(2)）。ここで選択したアルゴリズム及び鍵長は、公開鍵のセキュリティ属性である鍵種別となる。

対応する機能要件：FCS_COP.1(2)、FIA_UAU.2、FIA_UID.2、FMT_MSA.2、FPT_RVM.1

SF.RA_AUTH クライアント認証機能

SF.RA_AUTH は、次のように RA の識別認証を行う。

① CAO 端末以外から受信した「申請書」内の RA の識別情報を元に、RA を識別する。ここでの RA の識別は、CA は RA 操作者として識別せず、RA として識別する。受信した「申請書」の署名を検証することにより（FCS_COP.1(2)）、認証する。
RA の署名の検証時には、検証に使う公開鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。
・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）
このチェックにより、有効でない場合はエラーを返す。

② RA に対して登録 ID が決定される（FIA_UAU.2、FIA_UID.2）。

③ 識別認証された RA に対するプロセスが立ち上がる。

また、SF.RA_AUTH は、次のような機能を持つ。

- CAO 端末以外の経路からのアクセスで、識別認証されるまで、CA サーバに対していかなる操作も行うことができない（FIA_UAU.2、FIA_UID.2、FPT_RVM.1）。

・ 使用できる署名アルゴリズムは表 6-1 に示す標準に従ったいずれかのアルゴリズム及び鍵長を選択できる（FCS_COP.1(2)）。ここで選択したアルゴリズム及び鍵長は、検証に使う公開鍵のセキュリティ属性である鍵種別となる。

対応する機能要件：FCS_COP.1(2)、FIA_UAU.2、FIA_UID.2、FMT_MSA.2、FPT_RVM.1

SF.ACCESS_CONTROL アクセス制御機能

SF.ACCESS_CONTROL は、識別認証された操作者もしくは識別認証された RA に対して、役割に基づき、操作を許可する機能である。具体的には、下に示す。また、それぞれのユーザデータに対して、表 6-2 のように操作を制限する（FDP_ACC.2、FDP_ACF.1)。また、SF.ACCESS_CONTROL を介さずユーザデータを操作することはできない（FPT_RVM.1）。

識別認証された操作者もしくは識別認証された RA に対するアクセス制御を行う場合、識別認証された操作者もしくは識別認証された RA の登録 ID と、許可される操作の権限を有するロールとを結びつける(FIA_USB.1、FIA_ATD.1、FMT_SMR.1) 。

操作は、「直接のコマンド」によるものと「申請書」によるものがある。TSF は「直接のコマンド」による操作はコマンドをそのまま操作を理解し、「申請書」による操作はその「申請書」内のコマンドを読み取ることによって操作を理解する。以下に、コマンドによる手順をそれぞれ A)～E)に示す。

A) コマンドが「公開鍵証明書発行」の場合

① アクセス制御のチェックを行う（FDP_ACC.2、FDP_ACF.1)。

② 「申請書」の署名検証を行う。改ざんを検知した場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する（FCS_COP.1(2)、FDP_ITT.1、FDP_UIT.1）。

「申請書」の署名検証時には、検証に使う公開鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）

・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）

・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

このチェックにより、有効でない場合はエラーを返す。

③ 「申請書」を読出、「申請書」の内容の正当性の検証を行い、正当性が満たされていない場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する。

④ 「申請書」を読出、「申請書」の内容に従い、「公開鍵証明書」を書込する。

「公開鍵証明書」には、「申請書」で指定された表 6-1 に示す標準のいずれかの署名アルゴリズム及び鍵長をもとに、IT 環境の HSM に CA 署名を生成させ、この CA 署名が付してある（FDP_ITT.1、FDP_UIT.1、 IT 環境の HSM の

FCS_COP.1(3))。

CA 署名の生成に使う CA の秘密鍵のセキュリティ属性は、対となる公開鍵のセキュリティ属性と同じである。よって、CA の秘密鍵のセキュリティ属性として、CA の秘密鍵と対となる公開鍵の公開鍵証明書に記述してある以下の３つを、CA 署名の生成時に、チェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

このチェックにより、有効でない場合はエラーを返す。

⑤ ④にて書込された、「公開鍵証明書」を「申請書」の送信元へ送信するために、「公開鍵証明書」を読出、④にて書込した「公開鍵証明書」を含む「報告書」を書込する。「報告書」には、「申請書」で指定された表 6-1 に示す標準のいずれかの署名アルゴリズム及び鍵長をもとに、IT 環境の HSM に CA 署名を生成させ、この CA 署名が付してある（FDP_ITT.1、FDP_UIT.1、 IT 環境の HSM の FCS_COP.1(3))。

CA 署名の生成に使う CA の秘密鍵のセキュリティ属性は、対となる公開鍵のセキュリティ属性と同じである。よって、CA の秘密鍵のセキュリティ属性として、CA の秘密鍵と対となる公開鍵の公開鍵証明書に記述してある以下の３つを、CA 署名の生成時に、チェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

このチェックにより、有効でない場合はエラーを返す。

⑥ ⑤にて書込した「報告書」を読出、「申請書」の送信元へ送信する。

B) コマンドが「公開鍵証明書失効」の場合

① アクセス制御のチェックを行う（FDP_ACC.2、FDP_ACF.1)。

② 「申請書」の署名検証を行う。改ざんを検知した場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する（FCS_COP.1(2)、FDP_ITT.1、FDP_UIT.1)。

「申請書」の署名検証時には、検証に使う公開鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

このチェックにより、有効でない場合はエラーを返す。

③ 「申請書」を読出、「申請書」の内容の正当性の検証を行い、正当性が満たされ

ていない場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する。

④　「申請書」を読出、「申請書」の内容に従い、「公開鍵証明書」を失効し、「公開鍵証明書」の状態を更新する。

⑤　「公開鍵証明書失効」に関する「報告書」を書込する。「報告書」には、「申請書」で指定された表 6-1 に示す標準のいずれかの署名アルゴリズム及び鍵長をもとに、IT 環境の HSM に CA 署名を生成させ、この CA 署名が付してある（FDP_ITT.1、FDP_UIT.1、IT 環境の HSM の FCS_COP.1(3)）。

CA 署名の生成に使う CA の秘密鍵のセキュリティ属性は、対となる公開鍵のセキュリティ属性と同じである。よって、CA の秘密鍵のセキュリティ属性として、CA の秘密鍵と対となる公開鍵の公開鍵証明書に記述してある以下の３つを、CA 署名の生成時に、チェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

このチェックにより、有効でない場合はエラーを返す。

⑥　⑤にて書込した「報告書」を読出、「申請書」の送信元へ送信する。

C) コマンドが「公開鍵証明書失効禁止」の場合

①　アクセス制御のチェックを行う（FDP_ACC.2、FDP_ACF.1)。

②　「申請書」の署名検証を行う。改ざんを検知した場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する。（FCS_COP.1(2)、FDP_ITT.1、FDP_UIT.1）

「申請書」の署名検証時には、検証に使う公開鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

このチェックにより、有効でない場合はエラーを返す。

③　「申請書」を読出、「申請書」の内容の正当性の検証を行い、正当性が満たされていない場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する。

④　「申請書」の内容に従い、「公開鍵証明書」を失効禁止にし、「公開鍵証明書」の状態を更新する。

⑤　「公開鍵証明書失効禁止」に関する「報告書」を書込する。「報告書」には、「申請書」で指定された表 6-1 に示す標準のいずれかの署名アルゴリズム及び鍵長をもとに、IT 環境の HSM に CA 署名を生成させ、この CA 署名が付して

ある（FDP_ITT.1、FDP_UIT.1、IT 環境の HSM の FCS_COP.1(3)）。
CA 署名の生成に使う CA の秘密鍵のセキュリティ属性は、対となる公開鍵のセキュリティ属性と同じである。よって、CA の秘密鍵のセキュリティ属性として、CA の秘密鍵と対となる公開鍵の公開鍵証明書に記述してある以下の３つを、CA 署名の生成時に、チェックしている(FMT_MSA.2)。
・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）
このチェックにより、有効でない場合はエラーを返す。

⑥ ⑤にて書込した「報告書」を読出、「申請書」の送信元へ送信する。

D) コマンドが「公開鍵証明書失効禁止解除」の場合

① アクセス制御のチェックを行う（FDP_ACC.2、FDP_ACF.1)。

② 「申請書」の署名検証を行う。改ざんを検知した場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する。（FCS_COP.1(2)、FDP_ITT.1、FDP_UIT.1）
「申請書」の署名検証時には、検証に使う公開鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。
・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）
このチェックにより、有効でない場合はエラーを返す。

③ 「申請書」を読出、「申請書」の内容の正当性の検証を行い、正当性が満たされていない場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信する。

④ 「申請書」の内容に従い、「公開鍵証明書」の失効禁止を解除し、「公開鍵証明書」の状態を更新する。

⑤ 「公開鍵証明書失効禁止」に関する「報告書」を書込する。「報告書」には、「申請書」で指定された表 6-1 に示す標準のいずれかの署名アルゴリズム及び鍵長をもとに、IT 環境の HSM に CA 署名を生成させ、この CA 署名が付してある（FDP_ITT.1、FDP_UIT.1、IT 環境の HSM の FCS_COP.1(3)）。
CA 署名の生成に使う CA の秘密鍵のセキュリティ属性は、対となる公開鍵のセキュリティ属性と同じである。よって、CA の秘密鍵のセキュリティ属性として、CA の秘密鍵と対となる公開鍵の公開鍵証明書に記述してある以下の３つを、CA 署名の生成時に、チェックしている(FMT_MSA.2)。
・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）

・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）
このチェックにより、有効でない場合はエラーを返す。

⑥ ⑤にて書込した「報告書」を読出、「申請書」の送信元へ送信する。

E) コマンドが「CRL 発行」の場合

① コマンドのアクセス制御のチェックを行う（FDP_ACC.2、FDP_ACF.1)。

② 「公開鍵証明書」を読出の後、失効になっているものを検索し、「CRL」を書込する。「CRL」には、HSM を用いて、「申請書」で指定された表 6-1 に示す標準のいずれかの署名アルゴリズム及び鍵長をもとに、IT 環境の HSM に CA 署名を生成させ、この CA 署名が付してある（FDP_ITT.1、IT 環境の HSM の FCS_COP.1(3)）

CA 署名の生成に使う CA の秘密鍵のセキュリティ属性は、対となる公開鍵のセキュリティ属性と同じである。よって、CA の秘密鍵のセキュリティ属性として、CA の秘密鍵と対となる公開鍵の公開鍵証明書に記述してある以下の３つを、CA 署名の生成時に、チェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）
このチェックにより、有効でない場合はエラーを返す。

表 6-2 ユーザデータのアクセス制御

操作者のロール	機能	操作対象	操作
CA 管理者	公開鍵証明書発行	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	書込、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）

	公開鍵証明書失効禁止	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効禁止解除	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）
	CRL 発行	公開鍵証明書テーブル	読出、更新（FDP_ACF.1）
		CRL テーブル	書込（FDP_ACF.1）
CA 操作者	公開鍵証明書発行	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	書込、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効禁止	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）

		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効禁止解除	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		CAO 端末への送信ポート	送信（FDP_ACF.1）
		CAO 端末からの受信ポート	受信（FDP_ACF.1）
	CRL 発行	公開鍵証明書テーブル	読出、更新（FDP_ACF.1）
		CRL テーブル	書込（FDP_ACF.1）
RA	公開鍵証明書発行	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	書込、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		RA への送信ポート	送信（FDP_ACF.1）
		RA からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		RA への送信ポート	送信（FDP_ACF.1）
		RA からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効禁止	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		RA への送信ポート	送信（FDP_ACF.1）

		RA からの受信ポート	受信（FDP_ACF.1）
	公開鍵証明書失効禁止解除	申請書テーブル	書込、読出（FDP_ACF.1）
		公開鍵証明書テーブル	更新、読出（FDP_ACF.1）
		報告書テーブル	書込、読出（FDP_ACF.1）
		RA への送信ポート	送信（FDP_ACF.1）
		RA からの受信ポート	受信（FDP_ACF.1）

対応する機能要件：FCS_COP.1(2)、FDP_ACC.2、FDP_ACF.1、FDP_ITT.1、FDP_UIT.1、FIA_ATD.1、FIA_USB.1、FMT_MSA.2、FMT_SMR.1、FPT_RVM.1

SF. PRIVILEGE 運用支援機能

SF. PRIVILEGE は、識別認証された操作者の登録 ID と許可される操作の権限を有するロールとを結びつけ (FIA_USB.1、FIA_ATD.1、FMT_SMR.1) 、CA サーバを運用するための TSF データ管理を、表 6-3 のように行う。また、SF. PRIVILEGE を介さず TSF データ管理を行うことはできない（FPT_RVM.1）。

表 6-3　CA サーバを運用するための操作

ロール	機能	操作対象	操作
CA 管理者	アーカイブ及びログに対しての CA 署名を行う周期の変更	アーカイブ及びログに対しての CA 署名を行う周期	改変（FMT_MTD.1)
	CA の鍵対の管理操作に対する複数人操作の人数の変更	CA の鍵対の管理操作に対する複数人操作の人数	改変（FMT_MTD.1)
	利用者情報テーブルのユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書の登録及び削除	利用者情報テーブルのユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書	登録、削除（FMT_MSA.1)
	ロールテーブルの登録 ID 及び登録 ID により決定するロールの登録及び削除	ロールテーブルの登録 ID 及び登録 ID により決定するロール	登録、削除（FMT_MSA.1)
	アーカイブ及びログの閲覧	アーカイブ及びログ	閲覧（FAU_SAR.1、FAU_SAR.2)

CA の鍵対管理用複数人操作者	CA の鍵対の管理操作（注）	HSM 内の CA の鍵対	生成、削除、バックアップ、リストア（FMT_MOF.1)
監査人	アーカイブ及びログの閲覧	アーカイブ及びログ	閲覧（FAU_SAR.1、FAU_SAR.2)

（注）「CA の鍵対の管理操作」は、CA の鍵対管理操作を行う CA 操作者の人数が「CA の鍵対の管理操作に対する複数人操作の人数」に達したときに「CA の鍵対管理用複数人操作者」として実行される。

対応する機能要件：FAU_SAR.1、FAU_SAR.2、FIA_ATD.1、FIA_USB.1、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1、FMT_SMR.1、FPT_RVM.1

SF.AUDIT 履歴管理機能

SF.AUDIT は、次のように履歴を生成、管理している。

・ SF.AUDIT は、アーカイブ及びログを、日付・時刻（CA サーバの OS のタイムスタンプによる、FPT_STM.1）とともに、表 6-5 に示す事象の種別、利用者の識別情報（FAU_GEN.2)、実行されたプロセス及び事象の結果（成功や失敗）に対して生成する（FAU_GEN.1)。

表 6-4 監査事象

監査事象	監査事象に関連する機能要件	生成される監査記録
監査の起動と終了のとき	FAU_GEN.1	ログ
アーカイブ及びログの閲覧を行うとき	FAU_SAR.1、FAU_SAR.2	ログ
アーカイブ及びログの合計容量が TOE 構築時に設定した量を超えたとき	FAU_STG.3	ログ
CA 署名を生成し、それを付したとき	FDP_UIT.1	ログ
IC カードによる署名の検証､RA の署名の検証または CA 署名の検証したとき	FCS_COP.1(2)、FDP_UIT.1、FDP_ITT.1、FMT_MSA.2	ログ
申請書の書込、読出のとき	FDP_ACF.1	アーカイブ及びログ
公開鍵証明書の書込、更新、読出のとき	FDP_ACF.1	アーカイブ及びログ
CRL の書込、読出のとき	FDP_ACF.1	アーカイブ及びログ
報告書の書込、読出のとき	FDP_ACF.1	アーカイブ及びログ
操作者もしくは RA を識別認証するとき	FIA_UAU.2、FIA_UID.2、FIA_USB.1	ログ
HSM ドライバを用いた CA の鍵対の生成、削除、バックアップ及びリストアのとき	FMT_MOF.1	ログ
利用者情報テーブルのユーザ ID 及びグループ ID 及び登録 ID 及び操作者の公開鍵証明書か RA の公開鍵証明書の登録または削除のとき	FMT_MSA.1 、FMT_SMR.1	ログ
ロールテーブルの登録 ID 及び登録 ID により決定するロール登録または削除のとき	FMT_MSA.1 、FMT_SMR.1	ログ
アーカイブ及びログに対しての CA 署名を行う周期の変更のとき	FMT_MTD.1	ログ
CA の鍵対の管理操作に対する複数人操作の人数の変更のとき	FMT_MTD.1、FMT_SMR.1	ログ

・ 動作中に生成されるすべてのアーカイブや CA サーバで生成されるログに対して署名生成し、それを付す。それにより、アーカイブ及びログに対して、改ざんまたは削除が行われたとき、事後検出を可能にする（FAU_STG.1）。使用する署名の方法は以下の 2 種類である。

① ハッシュ署名（FCS_COP.1(1)）は、アーカイブやログが更新されるたびに付される署名であり、更新されるたびにハッシュを取ることで、少ないマシン負荷で改ざんを検出可能とすることを目的としている。アーカイブ及びログが生成されるたびに、TOE の機能によってこの署名を行う。また、閲覧の際には、ハッシュ署名を検証することにより（FCS_COP.1(1)）、アーカイブ及びログの改ざんの検知を行う。また、ハッシュ署名の生成及び検証は、表 6-6 のアルゴリズムを使用する。

表 6-5　ハッシュ署名のアルゴリズム

アルゴリズム	暗号操作	標準
SHA-1	ハッシュ署名の生成、検証	FIPS 180-1

② アーカイブ及びログに対して、IT 環境の HSM に CA 署名を生成させ（IT 環境の HSM の FCS_COP.1(3)）、それを付すことで、改ざんを検出可能とすることを目的としている。

CA 署名の生成に使う CA の秘密鍵のセキュリティ属性は、対となる公開鍵のセキュリティ属性と同じである。よって、CA の秘密鍵のセキュリティ属性として、CA の秘密鍵と対となる公開鍵の公開鍵証明書に記述してある以下の３つを、CA 署名の生成時に、チェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

アーカイブ及びログに対しての CA 署名を行う周期毎に、HSM によってこの署名を行う。また、閲覧の際には、CA 署名を検証することにより（FCS_COP.1(2)）、アーカイブ及びログの改ざんの検知を行う。また、CA 署名の生成及び検証は、表 6-1 のいずれかの署名アルゴリズム及び鍵長を使用する。

FCS_COP.1(2)の署名の検証時には、検証に使う公開鍵のセキュリティ属性として公開鍵証明書に記述してある以下の３つをチェックしている(FMT_MSA.2)。

・鍵の有効期間（検証日時が鍵の有効期間内かどうか）
・鍵種別（CA が許可する鍵のアルゴリズムと鍵長が一致するかどうか）
・公開鍵証明書の失効情報（公開鍵証明書が失効されているかどうか）

・ アーカイブ及びログに対しては、CA 管理者、監査人が閲覧可能な状態のテキストフ

ァイルとして読み出せる（FAU_SAR.1）。

・ 運用中にアーカイブ及びログの合計容量が TOE 構築時に設定した量を超えた場合には、警告表示を出し、監査レビュー機能及びハッシュ署名の検証機能以外の TOE の機能を停止する（FAU_STG.3）。

対応する機能要件：FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_STG.1、FAU_STG.3、FCS_COP.1(1)、FCS_COP.1(2)、FMT_MSA.2

6.2 Strength of function claims

確率的または順列的メカニズムとして、SF.CAO_AUTH、SF.RA_AUTH、SF.ACCESS_CONTROL および SF.AUDIT の CA 署名の検証、IT 環境の IC カードの署名の検証、RA の署名の検証、ハッシュ署名の生成および検証がある。このうちハッシュ署名の生成及び検証は、ハッシュ暗号アルゴリズムのみであり、その Strength of function レベルは、SOF-basic である。また、CA 署名の検証、IT 環境の IC カードの署名の検証、RA の署名の検証は、ハッシュ暗号アルゴリズムを含んだ署名アルゴリズムであり、そのハッシュ暗号アルゴリズムの Strength of function レベルは、SOF-basic である。署名アルゴリズムは、ハッシュ暗号アルゴリズム及び公開鍵暗号アルゴリズムからなり、公開鍵暗号アルゴリズムに対しては、CC に基づく評価対象外であるため、機能強度の対象としない。

6.3 Assurance measures

ASE クラス及び EAL3 からなる保証要件と、それぞれのコンポーネントに対応する保証手段とを表 6-7 に示す。

表 6-6 保証要件と保証手段

保証クラス	保証要件コンポーネント	保証手段
ASE：ST 評価	ASE_INT.1 ASE_DES.1 ASE_ENV.1 ASE_OBJ.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1 ASE_PPC.1	Trust-CANP v6.1 Security Target バージョン 1.2.8 日付 2004/2/6
ACM：構成管理	ACM_CAP.3 ACM_SCP.1	Trust-CANP v6.1 構成管理仕様書
ADO：配布と運用	ADO_DEL.1 ADO_IGS.1	Trust-CANP v6.1 配布マニュアル Trust-CANP v6.1 構築マニュアル
ADV：開発	ADV_FSP.1 ADV_HLD.2	Trust-CANP v6.1 機能仕様書 Trust-CANP v6.1 外部インタフェース仕様書

	ADV_RCR.1	Trust-CANP v6.1 構成設計書 Trust-CANP v6.1 機能仕様及び上位レベル設計間対応分析書 Trust-CANP v6.1 TOE 要約仕様及び機能仕様間対応分析書
AGD：ガイダンス文書	**AGD_ADM.1** **AGD_USR.1**	Trust-CANP v6.1 管理者マニュアル Trust-CANP v6.1 利用者マニュアル
ALC：ライフサイクルサポート	**ALC_DVS.1**	Trust-CANP v6.1 開発セキュリティに関する開発文書 Trust-CANP v6.1 保守マニュアル
ATE：テスト	**ATE_COV.2** **ATE_DPT.1** **ATE_FUN.1** **ATE_IND.2**	Trust-CANP v6.1 テストカバレージ分析書 Trust-CANP v6.1 テスト深さ分析書 Trust-CANP v6.1 テスト手順書 Trust-CANP v6.1 テスト結果一覧
AVA：脆弱性評定	**AVA_MSU.1** **AVA_SOF.1** **AVA_VLA.1**	Trust-CANP v6.1 セキュリティ機能強度分析書 Trust-CANP v6.1 脆弱性分析書

7 PP claims

この ST で参照される PP はない。

8 Rationale

8.1 Security objectives rationale

表 8-1 Security objectives rationale

	SO.AUTH	SO.PRIVILEGES	SO.LOG_GEN	SO.AUDIT_DATA	SO.RA_AUTH	SO.CA_SIGN	SOE.CA_SIGN	SOE.CA_KEY	SOE.IC_CARD_SIGN	SOE.SSL	SOE.DB&OS	SOE.PHYSICAL_PROTECT	SOE.HSM	SOE.IC_CARD	SOE.FIREWALL	SOE.UTILITY	SOE.ADMIN	SOE.OPERATOR	SOE.MANAGEMENT	SOE.PASSWORD	SOE.DB&OS_ADM
T.AUTH1	○		○						○												
T.AUTH2	○		○						○												
T.ACCESS_CONTROL1		○	○																		
T.ACCESS_CONTROL2		○	○																		
T.AUDIT_DATA				○			○	○													
T.RA			○		○																
T.COMMUNICATE						○	○	○	○	○											
A.PHYSICAL_PROTECT												○									
A.HSM								○				○	○								
A.IC_CARD												○		○							
A.FIREWALL															○						
A.UTILITY																○					
A.ADMIN																	○				
A.OPERATOR																		○			
P.MANAGEMENT																			○		
P.RA_TRUST																			○		
P.PASSWORD																				○	
P.DB&OS											○										○

T.AUTH1 は SO.AUTH と SO.LOG_GEN と SOE.IC_CARD_SIGN によって対抗される。

なぜなら、TOE は、TOE を利用する前に、CAO 端末上で SOE.IC_CARD_SIGN によって、識別認証のための IT 環境の IC カードの署名を行い、SO.AUTH によって、CAO 端末からログインしてきた操作者を識別認証するからである。また、SO.LOG_GEN によって、操作者の識別認証の事象が検知できるからである。

T.AUTH2 は SO.AUTH と SO.LOG_GEN と SOE.IC_CARD_SIGN によって対抗される。

なぜなら、TOE は、TOE を利用する前に、CAO 端末上で SOE.IC_CARD_SIGN によって、識別認証のための IT 環境の IC カードの署名を行い、SO.AUTH によって、CAO 端末からログインしてきた操作者を識別認証するからである。また、SO.LOG_GEN によって、識別認証の事象が検知できるからである。

T.ACCESS_CONTROL1 は SO.PRIVILEGES と SO.LOG_GEN によって対抗される。

なぜなら、SO.PRIVILEGES によって、TOE は、正当な利用者に対して、ロールごとに許可された操作のみ行うことができるからである。また、SO.LOG_GEN によって、TOE は、ロールごとに許可されていない操作を行おうとした場合、その操作をログに記録するからである。

T.ACCESS_CONTROL2 は SO.PRIVILEGES と SO.LOG_GEN によって対抗される。

なぜなら、SO.PRIVILEGES によって、TOE は、正当な利用者に対して、ロールごとに許可された操作のみ行うことができるからである。また、SO.LOG_GEN によって、TOE は、ロールごとに許可されていない操作を行おうとした場合、その操作をログに記録するからである。

T.AUDIT_DATA は SO.AUDIT_DATA と SOE.CA_SIGN と SOE.CA_KEY によって対抗される。

なぜなら、SO.AUDIT_DATA によって、TOE は、アーカイブまたはログに対して改ざんまたは削除などの不正な加工が行われた場合、そのような不正な加工が行われたことを事後に検出することが可能であるからである。また、SOE.CA_SIGN によって、アーカイブまたはログに対して改ざんまたは削除などの不正な加工を事後に検出するための CA の署名を行なうからである。また、SOE.CA_KEY によって、CA 署名に使用される CA の秘密鍵は、セキュアに鍵管理操作されるからである。

T.RA は、SO.RA_AUTH、SO.LOG_GEN によって対抗される。

なぜなら、SO.RA.AUTH によって、TOE は、RA から申請書を受信した際、RA を識別認証するからである。また、TOE は、SO.LOG_GEN によって、RA の識別認証の事象が検知できるからである。

T. COMMUNICATE は、SO.CA_SIGN と SOE.CA_SIGN と SOE.CA_KEY と SOE.IC_CARD_SIGN と SOE.SSL で対抗される。

なぜなら、SO.CA_SIGN によって、TOE は、TOE 外で改ざんの検知または CA の本人

性が確認できるように、公開鍵証明書、CRL 及び報告書を作成するからであり、TOE 外からの申請書の改ざんを検知するからである。また、SOE.CA_SIGN によって、公開鍵証明書、CRL 及び報告書の改ざんを検知または CA の本人性が確認のための CA の署名を行なうからである。また、SOE.CA_KEY によって、公開鍵証明書、CRL 及び報告書の改ざんを検知または CA の本人性が確認できるようにするために必要な CA の秘密鍵は、セキュアに鍵管理操作されるからである。また、SOE.IC_CARD_SIGN によって、申請書の改ざんを検知または操作者の本人性が確認のための IT 環境の IC カードの署名を行なうからである。また、SOE.SSL によって、CAO 端末と CA サーバ間、CA サーバと RA 間は SSL で、CA サーバとディレクトリサーバ間は SSL もしくは TLS で通信するので、公開鍵証明書及び CRL 及び申請書及び報告書の暴露及び改ざんを防ぐからである。

A.PHYSICAL_PROTECT は、SOE.PHYSICAL_PROTECT で実現できる。

なぜなら、SOE.PHYSICAL_PROTECT によって、CA サーバ及び CAO 端末及び HSM 及び 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１つのセキュアルームに設置されていることが明示されているからである。

A.HSM は、SOE.HSM と SOE.CA_KEY と SOE.PHYSICAL_PROTECT で実現できる。

なぜなら、SOE.HSM によって、CA の秘密鍵は、FIPS140-1 レベル 3 相当の HSM によって保護されるため、ハードウェアの直接攻撃によって暴露、改ざんされないからである。また、SOE.CA_KEY によって、HSM の中にある CA の秘密鍵は、セキュアに鍵管理操作されるからである。また、SOE.PHYSICAL_PROTECT によって、HSM 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ため、HSM から TOE に送られてくる情報は、改ざんされないからである。

A.IC_CARD は、SOE.IC_CARD と SOE.PHYSICAL_PROTECT で実現できる。

なぜなら、SOE.IC_CARD によって、IT 環境の IC カードは、PIN によって操作者を認証し、IC カードの所有者が本人であることを確認できるからである。また、SOE.PHYSICAL_PROTECT によって、IC カードリーダライタは、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ため、IT 環境の IC カードから IC カードリーダライタを通して TOE に送られてくる情報は、改ざんされないからである。

A.FIREWALL は、SOE.FIREWALL で実現できる。

なぜなら、CA サーバとセキュアルーム外との通信は、すべてファイアウォールを通して行い、SSL 及び TLS 以外の通信を排除し、DOS 攻撃から保護されることが明示されて

いるからである。

A.UTILITY は、SOE.UTILITY で実現できる。
なぜなら、SOE.UTILITY によって、TOE を管理する組織の責任者もしくは CA 管理者は、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が、製品仕様通りに機能することを運用時に定期的に確認することによって、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からである。

A.ADMIN は、SOE.ADMIN で実現できる。
なぜなら、SOE.ADMIN によって、TOE を管理する組織の責任者は、信頼される人物を CA 管理者に任命し、セキュリティポリシーを教育するからである。

A.OPERATOR は、SOE.OPERATOR 実現できる。
なぜなら、SOE.OPERATOR によって、CA 管理者は、CA 操作者がセキュリティポリシーに従って操作するように管理するからである。

P.MANAGEMENT は、SOE.MANAGEMENT で実現できる。
なぜなら、SOE.MANAGEMENT によって、TOE を管理する組織の責任者は、組織内部セキュリティポリシーを作成し、そのポリシーに基づいたガイダンス文書を作成する。その上で CA 管理者、CA 操作者、監査人を適切に管理し、TOE を運用させるからである。

P.RA_TRUST は、SOE.MANAGEMENT で実現できる。
なぜなら、SOE.MANAGEMENT によって、TOE を管理する組織の責任者は、組織内部セキュリティ指針及び運用ポリシーに基づいたガイダンス文書を作成しそれを RA 登録時においても適用することを求めているからである。その上で CA 管理者、CA 操作者、監査人を適切に指導し組織内部セキュリティポリシーを実施させるからである

P.PASSWORD は、SOE.PASSWORD で実現できる。
なぜなら、SOE.PASSWORD によって、TOE を管理する組織の責任者及び CA 管理者は、TOE に関連するパスワードの運用規則を定めるため、パスワードの安全性が保たれるからである。

P.DB＆OS は、SOE.DB&OS と SOE.DB&OS_ADM で実現できる。
なぜなら、SOE.DB&OS によって、データベース及び OS は、TOE がセキュアに機能するように、信頼される動作を提供するからである。また、SOE.DB&OS_ADM によって、

TOE を管理する組織の責任者及び CA 管理者は、TOE がセキュアに機能するように、データベース及び OS を管理するからである。

8.2 Security requirements rationale

8.2.1 Security requirements rationale

表 8-2　Security requirements rationale

	TOE の機能要件																					IT 環境の機能要件						
	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_STG.1	FAU_STG.3	FCS_COP.1(1)	FCS_COP.1(2)	FDP_ACC2	FDP_ACF.1	FDP_ITT.1	FDP_UIT.1	FIA_ATD.1	FIA_UAU.2	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MTD.1	FMT_SMR.1	FPT_RVM.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1(3)	FCS_COP.1(4)	FPT_SEP.1	FPT_STM.1	FTP_ITC.1
SO.AUTH								○						○	○				○			○				○			
SO.PRIVILEGES									○	○			○			○	○	○		○	○	○							
SO.LOG_GEN	○	○	○	○																								○	
SO.AUDIT_DATA					○	○	○	○											○										
SO.RA_AUTH								○						○	○				○			○							
SO.CA_SIGN								○	○	○	○	○							○						○				
SOE.CA_SIGN																									○				
SOE.CA_KEY																							○	○					
SOE.IC_CARD_SIGN																										○			
SOE.SSL																													○
SOE.DB&OS																											○	○	

SO.AUTH は、FCS_COP.1(2)、FIA_UAU.2、FIA_UID.2 、FMT_MSA.2、FPT_RVM.1 及び IT 環境の FCS_COP.1(4)で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

- IC カードの署名を FCS_COP.1(2)によって、署名検証することで、認証する。また、FMT_MSA.2 によって、使用される鍵のセキュリティ属性をチェックする。なお、IC カードの署名は IT 環境の FCS_COP.1(4)により生成される。
- FIA_UID.2 によって、利用者が TOE にアクセスしてアクションを行う前に利用者を識別する。
- FIA_UAU.2 によって、利用者が TOE にアクセスしてアクションを行う前に利用者の認証を正しく行う。
- FIA_RVM.1 によって、利用者が TOE にアクセスする際に必ず FIA_UAU.2 を呼び出し、他の機能要件がバイパスされることを防ぐ。

SO.PRIVILEGES は、FDP_ACC.2 、FDP_ACF.1 、 FIA_ATD.1 、 FIA_USB.1 、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1、FMT_SMR.1、FPT_RVM.1 で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

- FIA_USB.1 によって、利用者セキュリティ属性を代行のサブジェクトに関連付けら

れる。

- FMT_SMR.1 によって、TOE が認識する利用者のセキュリティに関するロールを特定する。
- FIA_ATD.1 によって、利用者セキュリティ属性であるユーザ ID、グループ ID、登録 ID、登録 ID により決定するロールを維持する。
- FDP_ACC.2 によって、サブジェクトとオブジェクトについての操作が、CANP アクセス制御 SFP で制御される。
- FDP_ACF.1 によって、CANP アクセス制御 SFP に基づくアクセスを実施する。
- FMT_MOF.1 によって、HSM ドライバを用いた CA の鍵対の生成、削除、バックアップ及びリストアを CA の鍵対管理用複数人操作者のみに制限する。
- FMT_MSA.1 によって、利用者情報テーブルのユーザ ID 及びグループ ID 及び登録 ID 及び操作者の公開鍵証明書か RA の公開鍵証明書の登録及び削除、及びロールテーブルの登録 ID、登録 ID により決定するロールの登録及び削除が CA 管理者のみに限定される。
- FMT_MTD.1 によって、TSF データの改変を表 5-5 のように許可する。
- FPT_RVM.1 によって、利用者が TOE にアクセスする際に必ず FDP_ACC.2、FDP_ACF.1 を呼び出し、他の機能要件がバイパスされることを防ぐ。

SO.LOG_GEN は、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2 及び IT 環境の FPT_STM.1 で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

- FAU_GEN.1 によって、事象の日時、事象の種別、事象の成功や失敗を関連付けた形で生成、格納される。このときの日時については CA サーバの OS の FPT_STM.1 によって CA サーバの OS から時刻を取得し、その時刻をもってタイムスタンプがなされる。
- FAU_GEN.2 によって、各監査対象事象を、その原因となった利用者の識別情報に関連付けられる。
- FAU_SAR.1 によって、閲覧に適した形で読み出しが可能になり、FAU_SAR.2 によって、許可された者以外の閲覧は禁止される。

SO.AUDIT_DATA は、FAU_STG.1、FAU_STG.3、FCS_COP.1(1)、FCS_COP.1(2)、FMT_MSA.2 で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

- FCS_COP.1(1)によって、アーカイブ及びログに対してハッシュ署名を生成し、それを付し、事後の改ざんを検知可能とする。
- FCS_COP.1(2)によって、アーカイブ及びログに対して生成された CA 署名を検証で

き、改ざんを検知可能とする。また、FMT_MSA.2 によって、使用される鍵のセキュリティ属性をチェックする。

- FAU_STG.1 によって、格納された監査記録を不正な削除から保護するために、監査記録の改変を検出できる。
- FAU_STG.3 によって、監査証跡が TOE 構築時に設定した量を超えた場合、警告表示を出し、監査レビュー機能及びハッシュ署名の検証機能以外の TOE の機能を停止する。

SO.RA_AUTH は、FCS_COP.1(2)、FIA_UAU.2、FIA_UID.2、FMT_MSA.2、FPT_RVM.1 で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

- FCS_COP.1(2)によって、RA の署名の検証を行う。また、FMT_MSA.2 によって、使用される鍵のセキュリティ属性をチェックする。
- FIA_UID.2 によって、利用者が TOE にアクセスしてアクションを行う前に利用者を識別する。
- FIA_UAU.2 によって、利用者が TOE にアクセスしてアクションを行う前に利用者の認証を正しく行う。
- FIA_RVM.1 によって、利用者が TOE にアクセスする際に必ず FIA_UAU.2 を呼び出し、他の機能要件がバイパスされることを防ぐ。

SO.CA_SIGN は、FCS_COP.1(2)、FDP_ACC.2、FDP_ACF.1、FDP_ACF.1、FDP_ITT.1、FDP_UIT.1、FMT_MSA.2 で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

- FCS_COP.1(2)によって、IC カードの署名、RA の署名、または CA 署名の検証を行う。また、FMT_MSA.2 によって、使用される鍵のセキュリティ属性をチェックする。
- FDP_ACC.2 によって、サブジェクトとオブジェクトについての操作が、CANP アクセス制御 SFP で制御される。
- FDP_ACF.1 によって、CANP アクセス制御 SFP に基づくアクセスを実施する。
- FDP_ITT.1 と FCS_COP.1(2)、FDP_ACC.2、FDP_ACF.1 によって、利用者データが TOE の物理的に分離されたパート間を転送される場合、その改変を防ぐ。
- FDP_UIT.1 と FDP_ACC.2、FDP_ACF.1 によって、利用者データを改変誤りから保護した形で送信、受信が行われる。

SOE.CA_SIGN は、IT 環境の FCS_COP.1(3)で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

・ FCS_COP.1(3)によって、IT 環境の HSM を用いて CA 署名を生成する。

SOE.CA_KEY は、IT 環境の FCS_CKM.1 及び FCS_CKM.4 で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

・ IT 環境の HSM を用いて CA 署名を生成するための暗号鍵は、HSM の FCS_CKM.1 によって生成され、HSM の FCS_CKM.4 によって破棄される。

SOE.IC_CARD_SIGN は、IT 環境の FCS_COP.1(4)で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

・ TOE が操作者の識別認証を行うために、FCS_COP.1(4)によって、CAO 端末でユーザ ID あるいはグループ ID に対して IT 環境の IC カードの署名を生成する。

SOE.SSL は、IT 環境の FTP_ITC.1 で実現される。なぜなら、この機能要件によって以下が保証されるからである。

・ FTP_ITC.1 によって、CA サーバと CAO 端末間、CA サーバと RA サーバ間、CA サーバとディレクトリサーバ間の通信に対して、他の通信チャネルと論理的に区別され、その端点の保証された識別、改変あるいは暴露からのチャネルデータの保護を提供する通信チャネルを提供する。

SOE.DB&OS は、IT 環境の FPT_SEP.1 及び FPT_STM.1 で実現される。なぜなら、これらの機能要件によって以下が保証されるからである。

・ FPT_SEP.1 によって、データベース及び OS は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持し、OS コントロール範囲内でサブジェクトのセキュリティドメイン間の分離を実施することが保証されるからである。
・ FPT_STM.1 によって、CA サーバの OS は、TOE が使用するための高信頼タイムスタンプを提供できるからである。

8.2.2 Demonstration of mutual support between security requirements

セキュリティ機能要件とその依存性の関係を表 8-3 にまとめる。
IT 環境で依存性を満たしている機能要件は斜体で、満たしていない機能要件は下線で表記する。なお、IT 環境の機能要件を選択した理由と依存性を満たしていない機能要件に対する理由については表の後で述べている。

表 8-3 セキュリティ機能要件のコンポーネントの依存性

機能要件	ST で選択した依存する機能	満たしていない機能要件

		要件	
TOE	FAU_GEN.1	*FPT_STM.1*	—
	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	—
	FAU_SAR.1	FAU_GEN.1	—
	FAU_SAR.2	FAU_SAR.1	—
	FAU_STG.1	FAU_GEN.1	—
	FAU_STG.3	FAU_STG.1	—
	FCS_COP.1(1)	—	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**
	FCS_COP.1(2)	FMT_MSA.2	**FCS_CKM.1** **FCS_CKM.4**
	FDP_ACC.2	FDP_ACF.1	—
	FDP_ACF.1	FDP_ACC.2	**FMT_MSA.3**
	FDP_ITT.1	FDP_ACC.2	—
	FDP_UIT.1	FDP_ACC.2 *FTP_ITC.1*	—
	FIA_ATD.1	—	—
	FIA_UAU.2	FIA_UID.1	—
	FIA_UID.2	—	—
	FIA_USB.1	FIA_ATD.1	—
	FMT_MOF.1	FMT_SMR.1	—
	FMT_MSA.1	FDP_ACC.2 FMT_SMR.1	—
	FMT_MSA.2	FDP_ACC.2 FMT_MSA.1 FMT_SMR.1	**ADV_SPM.1**
	FMT_MTD.1	FMT_SMR.1	—
	FMT_SMR.1	FIA_UID.1	—
	FPT_RVM.1	—	—
IT 環境	FCS_CKM.1	*FCS_COP.1(3)* FMT_MSA.2 *FCS_CKM.4*	—
	FCS_CKM.4	FMT_MSA.2 *FCS_CKM.1*	—
	FCS_COP.1(3)	FMT_MSA.2 *FCS_CKM.1* *FCS_CKM.4*	—
	FCS_COP.1(4)	—	**FCS_CKM.1** **FCS_CKM.4** **FMT_MSA.2**
	FPT_SEP.1	—	—
	FPT_STM.1	—	—
	FTP_ITC.1	—	—

表 8-3 にて、IT 環境の機能要件を選択した理由を以下に示す。

- FPT_STM.1

アーカイブ及びログ生成の時刻は、信頼されている IT 環境上の CA サーバの OS の時間を利用して、依存性を満たしている。

・ FTP_ITC.1
TSF 及びリモート高信頼 IT 製品間の通信は、信頼されている IT 環境上の Web サーバの SSL 及び TLS を用い、依存性を満たしている。

表 8-3 にて、依存性を満たしていない機能要件に対する理由を以下に示す。

・FCS_COP.1(1)から依存する FCS_CKM.1、FCS_CKM.4 及び FMT_MSA.2
ハッシュ署名には、アルゴリズムは 1 種類であり、暗号鍵自体がないため、有効期間等のセキュリティ属性もない。そのため、生成及び破棄する必要がなく、セキュアな値だけをセキュリティ属性として、受け入れる必要もない。よって、FCS_COP.1(1)から依存する FCS_CKM.1、FCS_CKM.4 及び FMT_MSA.2 は必要ない。

・FCS_COP.1(2)から依存する FCS_CKM.1 及び FCS_CKM.4
IC カードの署名の検証、RA の署名の検証及び CA 署名の検証は、検証のために利用する鍵はそれぞれの公開鍵を使用するため、鍵の生成及び廃棄は行わない。よって、FCS_COP.1(2)から依存する FCS_CKM.1 及び FCS_CKM.4 は必要ない。

・FDP_ACF.1 から依存する FMT_MSA.3
TOE は、利用者のセキュリティ属性の改変を許していない。そのため、静的属性初期化は必要ない。よって、FDP_ACF.1 から依存する FMT_MSA.3 は必要ない。

・FMT_MSA.2 から依存する ADV_SPM.1
この機能要件に対する TOE セキュリティ方針モデルは、本 ST の第 6 章の SF.RA_AUTH、 SF.CAO_AUTH、SF.ACCESS_CONTROL 及び SF.AUDIT に示している。よって、FMT_MSA.2 から依存する ADV_SPM.1 は本 ST 内で満たしている。

・IT 環境の FCS_COP.1(4)から依存する FCS_CKM.1、FCS_CKM.4 及び FMT_MSA.2
TOE として必要な機能は、IT 環境の IC カードの署名の生成機能のみであり、IT 環境の IC カードの鍵管理には TSF は依存していないので、鍵の生成および廃棄は不要である。また、鍵には有効期間等のセキュリティ属性はない。よって、FCS_COP.1(4)から依存する FCS_CKM.1、FCS_CKM.4 及び FMT_MSA.2 は必要ない。

よって、表 8-3 で示した依存関係は満足しているといえる。

また、以下に記述する通り、本 ST で選択された機能要件は相互にサポートしあっている。

＜バイパス防止＞
FPT_RVM.1 により、TOE の他の機能要件がバイパスされないことを保証する。

＜改ざん防止＞
IT 環境である OS 及びデータベース の実施機能である FPT_SEP.1 により、OS 及びデータベース のアカウントを有しない信頼できないサブジェクトによるセキュリティドメインの改ざんを防止する。従って、その OS 及びデータベース 上で動作する TOE のセキュリティ機能（すべての TOE 機能要件）の改ざんも防止する。

＜非活性化防止＞
FMT_MOF.1 により、TOE のセキュリティに関する機能を非活性化する能力は、CA の鍵対の生成、削除、バックアップ及びリストアに関してだけであるため、他のセキュリティ機能を非活性化することはない。

＜改ざん検出＞
CA 管理者、CA 操作者、監査人、RA の識別情報と共に監査記録を生成し、(FAU_GEN.1, FAU_GEN.2)、定められたロールである CA 管理者、監査人が監査記録をレビュー(FAU_SAR.1, FAU_SAR.2)することによって、攻撃の事象を検出することが可能である。また、監査記録は不正な改ざんを事後に検出することが可能である。(FAU_STG.1)。

8.2.3 Audit Event rationale

表 5-1 より、各機能要件の監査対象とすべきアクションは、本 TOE の監査対象事象と対応している。

8.2.4 Appropriateness of assurance requirements

本製品は、PKI の中で公開鍵証明書の発行及び失効を担当する製品であり、開発環境及び構成管理の評価を通じて製品の一定以上の品質が要求されるものである。

セキュリティ環境と対策方針にて、主なターゲットである一般的な民間企業または一般的な公的機関を考えている。また、TOE はセキュアルーム内へ設置し、入室を操作者に限定することで物理的に安全性を確保している。ネットワークの外部の接続部分にはファイアウォールを設置することで、DOS 攻撃、SSL あるいは TLS 以外の通信の攻撃を防いでいる。

このような環境条件を踏まえ、攻撃者の資産にアクセスする方法は、物理的手段を除外し、TOE とのインタフェースが利用されるという想定は TOE の利用者に納得されると考えられる。さらに、インタフェースを利用する攻撃者は既にセキュアルームで入室が制限されており低レベルの手段すなわち攻撃者による不正アクセスによる脅威を想定

することを妥当であると考える。

TOE のインタフェースは、ADV_HLD.2 の保証要件で保証され、また、ATE_FUN.1 、ATE_COV.2 及び ATE_DPT.1 においてテストされる。さらに AVA_VLA.1 にて想定される明白な脅威に対する分析がなされる。

以上を考慮し保証レベルとして EAL3 が妥当と考える。

8.2.5 Minimum strength of function (SOF) claim rationale

TOE は 3.2 Assumptions で述べたように物理的および接続的に安全に保たれているため、過度に保護される必要はない。このためセキュリティ機能は攻撃に対し低レベルの防御を備えればよい。本 TOE では 3.3 Threats で述べたように、攻撃レベルが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に対するセキュリティ対策方針で施している。従って、Minimum strength of function レベルは SOF-basic が妥当であるといえる。

8.3 TOE summary specification rationale

8.3.1 Security functions rationale

表 8-4　Security functions rationale

	SF.CAO_OPERATE	SF.CAO_AUTH	SF.RA_AUTH	SF.ACCESS_CONTROL	SF. PRIVILEGE	SF.AUDIT
FAU_GEN.1						○
FAU_GEN.2						○
FAU_SAR.1					○	○
FAU_SAR.2					○	
FAU_STG.1						○
FAU_STG.3						○
FCS_COP.1(1)						○
FCS_COP.1(2)		○	○	○		○
FDP_ACC.2				○		
FDP_ACF.1				○		
FDP_ITT.1	○			○		
FDP_UIT.1				○		
FIA_ATD.1				○	○	
FIA_UAU.2	○	○	○			
FIA_UID.2		○	○			
FIA_USB.1				○	○	
FMT_MOF.1					○	
FMT_MSA.1					○	
FMT_MSA.2		○	○	○		○
FMT_MTD.1					○	
FMT_SMR.1				○	○	
FPT_RVM.1		○	○	○	○	

FAU_GEN.1 監査データ生成(SF.AUDIT)

操作した者の識別情報、事象の日時、事象の種別、事象の結果を関連付けた、表 6-4 に基づくアーカイブ及びログの生成を行うことで実現している。

FAU_GEN.2 利用者識別情報の関連付け(SF.AUDIT)

アーカイブ及びログは、操作者または RA の識別情報に対して生成されることで実現されている。

FAU_SAR.1 監査レビュー(SF.AUDIT、SF. PRIVILEGE)

SF.AUDIT

アーカイブ及びログに対しては、閲覧可能な状態のテキストファイルとして読み出せることで実現している。

SF. PRIVILEGE

識別認証された操作者から TOE に対して操作が行われた場合、登録 ID により決定するロールを元に、表 6-3 に従った操作を許可することで実現している。

FAU_SAR.2 限定監査レビュー(SF. PRIVILEGE)

識別認証された操作者から TOE に対して操作が行われた場合、登録 ID により決定するロールを元に、表 6-3 に従った操作を許可することで実現している。

FAU_STG.1 保護された監査証跡格納(SF.AUDIT)

動作中に生成されるすべてのアーカイブ及びログに対して署名生成し、それを付す。それにより、アーカイブ及びログに対して、改ざんまたは削除が行われたとき、事後検出を可能にすることで実現している。

FAU_STG.3 監査データ損失の恐れ発生時のアクション(SF.AUDIT)

運用中にアーカイブ及びログの合計容量が、TOE 構築時に設定した量を超えた場合、警告表示を出し、監査レビュー機能及びハッシュ署名の検証機能以外の TOE の機能を停止することで実現している。

FCS_COP.1(1) 暗号操作(SF.AUDIT)

アーカイブ及びログに対して、ハッシュ署名を生成し、それを付すことで実現している。また、ハッシュ署名が付されたアーカイブ及びログに対しての閲覧の際には、ハッシュ署名を検証することによりアーカイブ及びログの改ざんの検知を行うことで実現している。

FCS_COP.1(2) 暗号操作　(SF.CAO_AUTH、SF.RA_AUTH、SF.ACCESS_CONTROL、SF.AUDIT)

SF.CAO_AUTH

操作者の認証を行う際、操作者からの IC カードの署名を検証することで実現している。

SF.RA_AUTH

RA の認証を行う際、RA からの「申請書」の署名検証することで実現している。

SF.ACCESS_CONTROL

識別認証された操作者もしくは識別認証された RA から、「申請書」を読出、「申請書」の署名検証を行うことで実現している。

SF.AUDIT

CA 署名が付されたアーカイブ及びログに対しての閲覧の際には、CA 署名を検証することによりアーカイブ及びログの改ざんの検知を行うことで実現している。

FDP_ACC.2 完全アクセス制御(SF.ACCESS_CONTROL)

識別認証された操作者もしくは識別認証された RA から TOE に対して申請書による操作が行われた場合、登録 ID により決定するロールに基づいて、表 6-2 に従った操作を許可することで実現している。

FDP_ACF.1 セキュリティ属性によるアクセス制御(SF.ACCESS_CONTROL)

識別認証された操作者もしくは識別認証された RA から TOE に対して申請書による操作が行われた場合、登録 ID により決定するロールに基づいて、表 6-2 に従った操作を許可することで実現している。

FDP_ITT.1 基本内部転送保護(SF.ACCESS_CONTROL)

識別認証された操作者から、「申請書」を読出、「申請書」の署名検証を行い、改ざんを検知した場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信することで実現している。また、事後に改ざんの検知及び CA の本人性の確認が可能なように、「公開鍵証明書」及び「報告書」に対して、IT 環境の HSM に CA 署名を生成させ、この CA 署名を付すことで実現している。また、事後に改ざんの検知及び CA の本人性の確認が可能なように、「CRL」に対して、IT 環境の HSM に CA 署名を生成させ、この CA 署名を付すことで実現している。

FDP_UIT.1 データ交換完全性(SF.ACCESS_CONTROL)

識別認証された RA から、「申請書」を読出、「申請書」の署名検証を行い、改ざんを検知した場合は、エラーを示す「報告書」を書込し、「報告書」を読出、「申請書」の送信元へ送信することで実現している。また、事後に改ざんの検知及び CA の本人性の確認が可能なように、公開鍵証明書及び報告書に対して、IT 環境の HSM を用いて CA 署名を生成し、それが付されることで実現している。

FIA_ATD.1 利用者属性定義(SF.ACCESS_CONTROL、SF. PRIVILEGE)

SF.ACCESS_CONTROL

利用者に属するセキュリティ属性のリストである、利用者情報テーブル｛ユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書｝及びロールテー

ブル｛登録 ID、登録 ID により決定するロール｝を維持することで実現している。

SF. PRIVILEGE

利用者に属するセキュリティ属性のリストである、利用者情報テーブル｛ユーザ ID、グループ ID、登録 ID、操作者の公開鍵証明書か RA の公開鍵証明書｝及びロールテーブル｛登録 ID、登録 ID により決定するロール｝を維持することで実現している。

FIA_UAU.2 アクション前の利用者認証(SF.CAO_AUTH、SF.RA_AUTH)

SF.CAO_AUTH

識別認証されるまで、TOE に対して、CAO 端末からのいかなる操作も行うことができないことで実現している。

SF.RA_AUTH

また、CAO 端末以外の経路からのアクセスで、識別認証されるまで、TOE に対していかなる操作も行うことができないことで実現している。

FIA_UID.2 アクション前の利用者識別(SF.CAO_AUTH、SF.RA_AUTH)

SF.CAO_AUTH

識別認証されるまで、TOE に対して、CAO 端末からのいかなる操作も行うことができないことで実現している。

SF.RA_AUTH

また、CAO 端末以外の経路からのアクセスで、識別認証されるまで、TOE に対していかなる操作も行うことができないことで実現している。

FIA_USB.1 利用者・サブジェクト結合(SF.ACCESS_CONTROL、SF. PRIVILEGE)

SF.ACCESS_CONTROL

識別認証された操作者もしくは識別認証された RA の登録 ID と、許可される操作の権限を有するロールとを結びつけることで実現している。

SF. PRIVILEGE

識別認証された操作者の登録 ID と許可される操作の権限を有するロールとを結びつけることで実現している。

FMT_MOF.1 セキュリティ機能のふるまいの管理(SF. PRIVILEGE)

HSM ドライバを用いた CA の鍵対の生成、削除、バックアップ及びリストアを CA の鍵対管理用複数人操作者に制限することで実現している。

FMT_MSA.1 セキュリティ属性の管理(SF. PRIVILEGE)

利用者情報テーブルのユーザ ID 及びグループ ID 及び登録 ID 及び操作者の公開鍵証明書か RA の公開鍵証明書の登録または削除、及びロールテーブルの登録 ID 及び登録

IDにより決定するロールの登録または削除をCA管理者に制限することで実現している。

FMT_MSA.2 セキュアなセキュリティ属性(SF.CAO_AUTH、SF.RA_AUTH、SF.ACCESS_CONTROL、SF.AUDIT)

SF.CAO_AUTH

操作者の認証を行う際、操作者からの IC カードの署名を検証する際に、公開鍵証明書に記述してある、鍵の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

SF.RA_AUTH

RA の認証を行う際、RA からの「申請書」の署名検証する際に、公開鍵証明書に記述してある、鍵の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

SF.ACCESS_CONTROL

識別認証された操作者もしくは識別認証された RA から、「申請書」を読出、「申請書」の署名検証する際に、「公開鍵証明書」に記述してある、鍵の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。また、「公開鍵証明書」及び「報告書」に含む CA の署名を生成する際に、CA の秘密鍵と対を成す公開鍵証明書に記述してある、鍵の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。また、「CRL」に含む CA の署名を生成する際に、CA の秘密鍵と対を成す公開鍵証明書に記述してある、鍵の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

SF.AUDIT

アーカイブ及びログに対して CA 署名の生成の時、CA の秘密鍵と対を成す公開鍵証明書に記述してある、鍵の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。また、CA 署名が付されたアーカイブ及びログに対しての閲覧の時、CA 署名を検証する際に、公開鍵証明書に記述してある、鍵の有効期間、鍵種別及び公開鍵証明書の失効情報をチェックすることで実現している。

FMT_MTD.1 TSF データの管理(SF. PRIVILEGE)

TSF データに対して、表 6-3 に従って操作が可能であることで実現している。

FMT_SMR.1 セキュリティ役割(SF.ACCESS_CONTROL、SF. PRIVILEGE)

SF.ACCESS_CONTROL

CA 管理者ロール、CA 操作者ロール、監査人ロール、RA ロールを維持し、CA の鍵対管理用複数人操作者ロール、利用者に関連付けることで実現している。

SF. PRIVILEGE

CA 管理者ロール、CA 操作者ロール、監査人ロール、CA の鍵対管理用複数人操作者

ロールを維持し、利用者に関連付けることで実現している。

FPT_RVM.1 TSP の非バイパス性 (SF.CAO_AUTH 、 SF.RA_AUTH 、 SF.ACCESS_CONTROL、SF. PRIVILEGE)

SF.CAO_AUTH

CAO 端末からの経路のアクセスで、識別認証されるまで、TOE に対して、いかなる操作も行うことができないことで実現している。

SF.RA_AUTH

CAO 端末以外の経路からのアクセスで、識別認証されるまで、TOE に対していかなる操作も行うことができないことで実現している。

SF.ACCESS_CONTROL

SF.ACCESS_CONTROL を介さずユーザデータの操作ができないことで実現している。

SF. PRIVILEGE

SF. PRIVILEGE を介さずCAサーバを運用するためのTSFデータ管理ができないことで実現している。

以上、これらの SF が確実に呼び出され、識別認証や TSF データ管理機能が実行され、これらの機能をバイパスすることが出来ないことにより、FPT_RVM.1 が実現されている。

8.3.2 Demonstration of mutual support between security functions

表 8-4 に示すとおり、セキュリティ機能は全てのセキュリティ機能要件をもれなく実現している。

SF.CAO_OPERATE と SF.CAO_AUTH は密接に関連して機能している。これは、SF.CAO_OPERATE によって、操作者のユーザ ID もしくはグループ ID に IT 環境による IC カードの署名の署名を付すことで、操作者の識別認証するための情報を生成する。SF.CAO_AUTH によって、その情報を識別認証に用いているからである（FIA_UAU.2、FIA_UID.2)。

しかし、この情報はそれぞれの機能を具体的に説明したに過ぎず、これらの追加情報がセキュリティ上の弱点を発生させる要因とはなりえない。

すなわち、Security Function Reqirements を満たすために、Security Function 全体が一体となって機能しているといえる。

8.3.3 Strength of function claims rationale

本 TOE において、ハッシュ暗号アルゴリズムである、ハッシュ署名の生成と検証及び CA 署名の検証、IT 環境の IC カードの署名の検証、RA の署名の検証のハッシュ暗号アル

ゴリズムの部分が確率的または順列的メカニズムに含まれる。strength of function は 6.2 節では「SOF-basic」と宣言している。一方、5.3 節において「SOF-basic」と宣言している。これらが矛盾しないことは明らかである。

8.3.4 Assurance measures rationale

表 6-6 に示すように、すべての TOE セキュリティ保証要件は、保証手段により示された文書により対応付けられ、TOE セキュリティ保証要件を満たしている。

8.4 PP claims rationale

この ST で参照される PP はない。

＜付録A＞ 用語説明

用語	意味
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 にを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。

＜付録B＞ 参考文献

＜DES＞ *NIST FIPS PUB 47 Data Encryption Standard, November 23, 1976*

＜DSA＞ *Federal Information Processing Standards Publication 186 Digital Signature Algorithm, 19 May 1994*

＜ESIGN＞ *ISO/IEC14888-3,Information technology - Security techniques - Digital signatures with appendix - Part3:Certificate-based mechanisms*

＜LDAPv3＞ Lightweight Directory Access Protocol, *RFC2511*

＜MD5＞ *R.L.Rivest The MD5 Message Digest Algorithm, RFC 1321 April 1992,*

＜FIPS140-1＞ *NIST FIPS PUB 140-1, Security Requirements for Cryptographic Modules, 1994 January 11*

＜FIPS180-1＞ *NIST FIPS PUB 180-1, Secure Hash Standard, 1995 April 17*

＜FIPS186-2＞ *NIST FIPS PUB 186-2, Digital Signature Standard (DSS), 2000 January 27*

＜FIPS140-1＞ *NIST FIPS PUB 140-1, Security Requirements for Cryptographic Modules, 1994 January 11*

＜ISO14888-3＞ *ISO/IEC 14888-3, Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms, (1997)*

＜PKCS#1＞ RSA Laboratories, *PKCS #1: RSA Encryption Standard, Version 1.5 Revised November 1, 1993*

＜PKCS#７＞ RSA Laboratories, *PKCS#7 – Cryptographic Message Syntax Standard, Version 1.5,November 1993*

＜PKCS#8＞ RSA Laboratories, *PKCS#8 – Private-Key Information Syntax Standard, Version 1.2,November 1993*

＜PKCS#10＞ RSA Laboratories, *PKCS#10 – Certification Request Syntax Standard, Version 1.5,November 1993*

＜PKIX＞ S. Farrell and C. Adams, *Internet Public Key Infrastructure, Part III: Certificate Management Protocols, Internet Draft, December 1996.*

＜RSA＞ RSA Laboratories, *PKCS #1: RSA Encryption Standard, Version 1.5 Revised November 1, 1993*

＜RFC2459＞ *Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999*

＜RFC2510＞ *Internet X.509 Public Key Infrastructure Certificate Management Protocols, March 1999*

＜RFC2511＞ *Internet X.509 Certificate Request Message Format, March 1999*

＜RFC2797＞ *Certificate Management Messages over CMS ,April 2000*

＜SHA-1＞ *NIST FIPS PUB 180-1, Secure Hash Standard, 1995 April 17.*

＜SSLv2＞ *Hickman, Kipp, "The SSL Protocol", Netscape Communications Corp., Feb 9, 1995.*

＜ SSLv3 ＞ *A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.*

＜TLS＞ *RFC2246, The TLS Protocol Version 1.0, January 1999*

＜X.509v3＞ *Final Text of Draft Amendments DAM 1 to ITU Rec. X.509 (1993) | ISO/IEC 9594-8 : 1995 Information Technology — Open Systems Interconnection —The Directory: Authentication Framework.*