NTT

Trust-CANP V8.0i

Security Target 第9版

変更履歴

バージョン	日付	著者	更新概要
第 1 版	2004/12/1	新井　聡	—
第 2 版	2004/12/28	新井　聡	識別認証に関する修正
第 3 版	2005/1/17	新井　聡	申請書の操作に関する修正
第 4 版	2005/2/8	新井　聡	アクセス制御に関する修正
第 5 版	2005/2/14	新井　聡	監査事象に関する修正
第 6 版	2005/2/17	新井　聡	セキュリティ属性に関する修正
第 7 版	2005/4/13	新井　聡	指摘に対する修正
第 8 版	2005/4/22	新井　聡	保証手段の表記の変更
第 9 版	2005/5/17	新井　聡	IT 環境記述の変更

目次

1 ST概説

1.1 ST識別

ST 名称 Trust-CANP V8.0i Security Target

バージョン 第 9 版

日付 2005/5/17

著者 NTT 情報流通プラットフォーム研究所　新井 聡

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

CC のバージョン Common Criteria for Information Technology Security Evaluation Version 2.1、CCIMB Interpretations-0407

1.2 TOE識別

TOE 名称: 「Trust-CANP」

バージョン: 「V8.0i」

1.3 CC適合

この ST は以下の CC に適合している。

・機能要件は CC Version 2.1 Part2 適合

・保証要件は CC Version 2.1 Part 3 適合

1.4 ST概要

本文書は、Trust-CANP V8.0i 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 評価保証レベル

評価保証レベルは EAL2 適合。

1.6 適合するPP

この ST が適合している PP はない。

2 TOE記述

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 V8.0i のセキュリティ機能について記述する。

2.1 TOE概説

2.1.1 TOE が提供する機能

Trust-CANP V8.0i 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、RFC3280 準拠の公開鍵証明書を指し、CRL とは、RFC3280 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 V8.0i の主な機能を以下に示す。

- 一般の利用者の公開鍵を登録し、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。
- 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」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 V8.0i を含む製品が CA として提供する機能を述べる。Trust-CANP V8.0i 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、CAO 端末を用いた Trust-CANP V8.0i の運用について触れる。Trust-CANP V8.0i では、連携する RA サーバは、Trust-CANP V8.0i に RA の DN に基づき公開鍵証明書発行等が可能な権限を持つクラス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 の操作者が 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申請種別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 RA 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。このときの報告書は公開鍵証明書そのものであり、RFC2510 及び RFC2797 に準拠している。報告書には、発行者署名として、CA の署名（以下、CA 署名）が付されている。

RA では、RA の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 の操作者が 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申請種別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 RA 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(以下、報告書と呼ぶ)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。

Trust-CANP V8.0i 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。

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。

CA サーバのアクセスは、CA サーバ自体の管理または HSM のトラブル時以外は CAO 端末から行われる。操作者には個別に固有のユーザ ID が付与され、CA の運用ポリシーに従い単数または複数のユーザに対してグループ ID が付与される。CA サーバへの操作は、ユーザ ID もしくはグループ ID の権限に従い許可される。

操作者が CAO 端末から CA サーバの操作を行う場合、識別認証を行う必要がある。ユーザ ID を利用したログインの場合、操作者は CAO 端末を用いて、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認証データを生成する。その後、ユーザ ID と認証データとともに CA サーバに送信することによって、ログインを試みる。グループ ID を利用したログインの場合、複数人の操作者がそれぞれ保有する IC カードに格納された秘密鍵を用いて一人ずつ認証データを生成する。その後、グループ ID と認証データとともに CA サーバに送信することによって、ログインを試みる。

CAO 端末を用いた操作は、Trust-CANP V8.0i を管理する組織の運用ポリシーに基づき運用作業が行われる。CA 管理者は組織の運用ポリシーに従い CA を管理し、CA 操作者は組織の運用ポリシーまたは CA 管理者の指示に基づき運用作業を行う。CA 管理者および CA 操作者の運用作業には、申請書による 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、削除及びバックアップ）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。

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 V8.0i 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 の鍵対の更新、削除及びバックアップは、CA 管理者の指示のもと、鍵対の管理グループによって、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 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。

- CAO 端末から操作者がログインする場合、認証のための操作者の公開鍵証明書を別途登録する必要がある。

- 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 V8.0i 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 内でのすべての管理を行う。
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。 RA 及び他 CA 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。
鍵対の管理グループ	CA の運用ポリシーのもと、CA の鍵対の管理操作を行う。 このグループは、監査人以外の操作者の複数人で構成され、グループ ID により識別される。
監査人	ログファイル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。

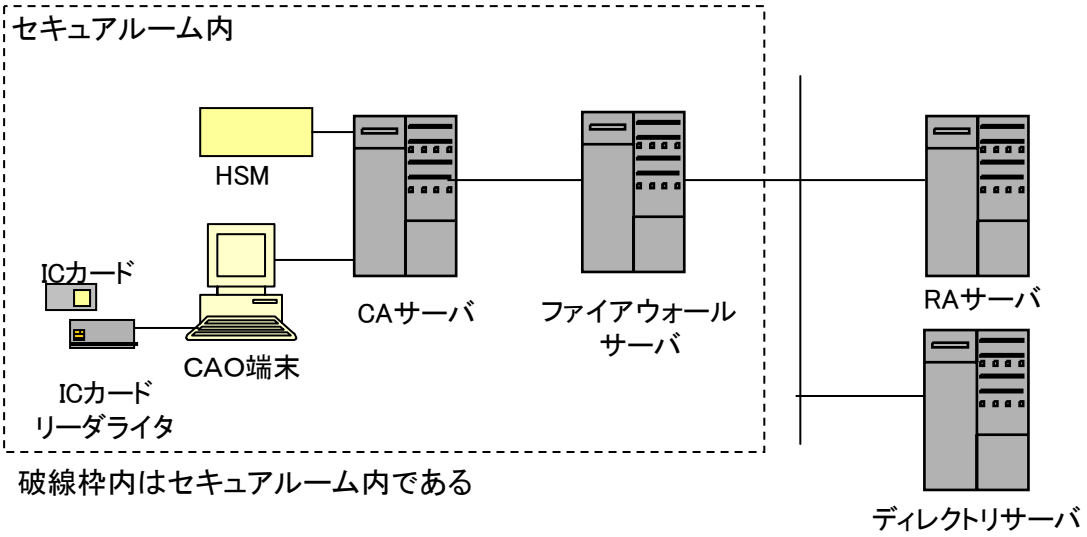

図 2-1 TOE が機能するために必要なハードウェア構成

CA サーバ

後述する Trust-CANP V8.0i(CA サーバ)と OS と HTTP サーバと DBMS 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。

使用する CA サーバのハードウェア条件は、Solaris 8 の要求条件を満たすものであり、メモリは 1GB 以上、ハードディスクドライブの容量は 10GB 以上である。

HSM

CA の鍵対を生成、削除、バックアップするために用いるハードウェア。

FIPS 140-2 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、CA の鍵対に対してハードウェアの直接攻撃による暴露もしくは改ざんに耐える構造をもつ。

CA サーバに SCSI ケーブルで接続されている。

使用する HSM は、nCipher 社の FIPS 140-2 レベル 3 相当である nShield 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 V8.0i(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 USB ケー

ブルで接続される。

使用する CAO 端末のハードウェア条件は、Windows 2000 Professional の要求条件を満たすものであり、メモリは 196MB 以上、ハードディスクドライブ 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 USB ケーブルで接続されている。

使用する IC カードリーダライタは、Cryptoflex 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。操作者の秘密鍵および PIN の２つが格納されており、それらは暴露、改ざんから保護されている。

IC カードリーダライタに挿入して使用する。

使用する IC カードは、Cryptoflex 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、また外部からの DOS(Denial of Service)攻撃を拒絶する能力もある。

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。

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を通して提供するサーバ。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。

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、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。

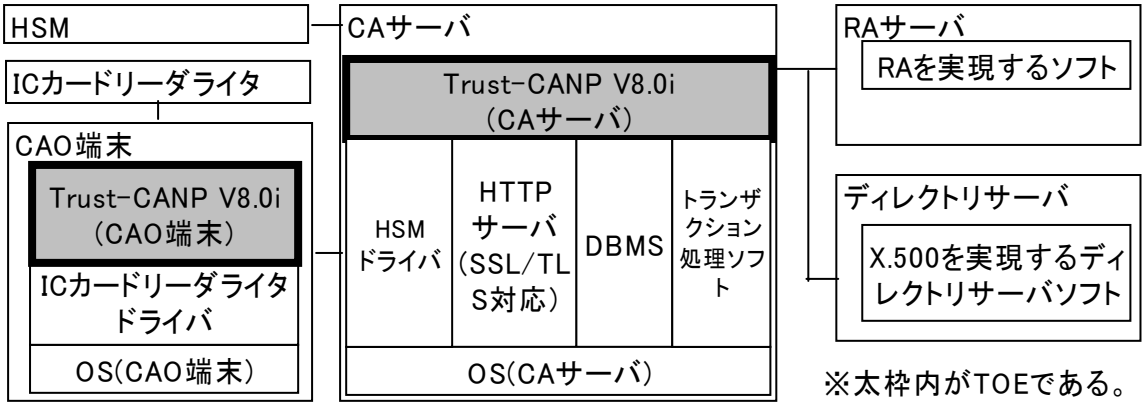

図 2-2 TOE が機能するために必要なソフトウェア構成図

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 の製品名は、Sun 社が提供する 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 の製品名は、Microsoft Windows 2000 Professional であり、 適用されているのは、ServicePack4 である。

DBMS

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 DBMS の製品名は、Oracle8i R8.1.7 である。

トランザクション処理ソフト

CA サーバにインストールされているトランザクションソフトウェアである。サーバ用ソフトとクライアント用ソフトを対で利用する。

TOE 範囲外である。

使用するトランザクションソフトは、サーバ用ソフトとして OpenTP1 Server Base 05-00、クライアント用ソフトとして OpenTP1 Client/W 05-00 である。

HTTP 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。CA サーバとの通信は、HTTP サーバを介して行われる。

TOE の範囲外である。

使用する HTTP サーバは、フリーウェアである Apache 1.3 であり、これに対応した HTTP サーバ用暗号プロトコル接続モジュール(フリーウェアである mod_SSL)と

HTTP サーバ用暗号プロトコルソフト(OpenSSL 0.9.6)と共に用いられる。

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 を用いて CA の鍵対の更新、削除及びバックアップする機能を備えている。

使用するソフトは、nShield のドライバである。

TOE の範囲外である。

IC カードリーダライタドライバ

CAO 端末にインストールされているソフトウェアである。IC カードを用いて CA 管理者、CA 操作者、監査人の署名を生成する機能を備えている。

使用するソフトは、Cryptoflex のドライバである。

TOE の範囲外である。

Trust-CANP V8.0i(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 V8.0i(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 V8.0i 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 V8.0i 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 V8.0i は、権限設定ファイルとクライアント認証テーブルを有する。CAO 端末からの識別認証時には、TOE は、操作者ごとに付与されているユーザ ID を用いて、もしくは単数または複数の操作者ごとに付与されているグループ ID を用いて識別を行う。申請書による識別認証時には、TOE は、CA 管理者、CA 操作者、RA はおのおののユーザ ID もしくは DN を用いて識別を行う。権限設定ファイルは、ユーザ ID、グループ ID によるコマンドの権限が記述されている。クライアント認証テーブルは、DN とクラスによる公開鍵証明書発行および公開鍵証明書失効の権限が記述されている。

申請書認証機能(CA サーバ)

RA に対して、申請書による識別認証する機能。また、認証については、申請書の署名の検証を行うことで実現される。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。認証については、CAO 端末にて認証データとして IC カードの署名の生成を行うこと、IC カードの署名の検証を行い、認証を行うことで実現されている。この機能は、TOE の範囲内である。

申請書アクセス制御機能(CA サーバ)

公開鍵証明書テーブルに対してアクセス制御を行う機能､および公開鍵証明書または報告書を作成する機能。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、公開鍵証明書失効を CA 操作者、CA 管理者及び RA に制限する機能。
- 署名する前の報告書（以下、報告書元データと表す）に HSM が生成した CA 署名を付す機能。
- 公開鍵証明書テーブルを更新する機能

この機能は、TOE の範囲内である。

操作者アクセス制御機能(CA サーバ)

公開鍵証明書テーブルと CRL テーブルに対してアクセス制御を行う機能､CRL を作成する機能。詳細においては以下のような機能である。

- CRL の作成を CA 操作者および CA 管理者に制限する機能。
- CRL を作成するために、公開鍵証明書テーブルを更新する機能。
- 署名する前の CRL（以下、CRL の元データと表す）に HSM が生成した CA 署名を付す機能。
- CRL テーブルを更新する機能

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 V8.0i を運用するための操作を許可する機能である。

Trust-CANP V8.0i を運用するための操作として、ログ設定ファイルの変更、CA の鍵対の管理グループの変更、権限設定ファイルのユーザ ID 及びグループ ID 及び許可される操作の追加と変更と削除、クライアント認証テーブルの DN 及びクラスの追加と変更と削除、CA の鍵対の管理操作、ログファイルの閲覧がある。

この機能は、TOE の範囲内である。

履歴管理機能(CA サーバ)

日付、時刻とともに記録した 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、ログもしくはログファイルに対して署名を付す機能。

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。ログファイルは操作ごとにログが書き込まれるカレントログファイルと、ログ設定ファイルに記述される契機ごとにカレントログファイルから移行される非カレントログファイルがある。カレントログファイルにはログを記録するごとに署名を行うので、マシン負荷の少ないハッシュ署名を用い、非カレントログファイルには CA 署名を用いる。

この機能は、TOE の範囲内である。

また、TOE の範囲外ではあるが、非カレントログファイルのバックアップおよび削除は CA 管理者が行う。

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。

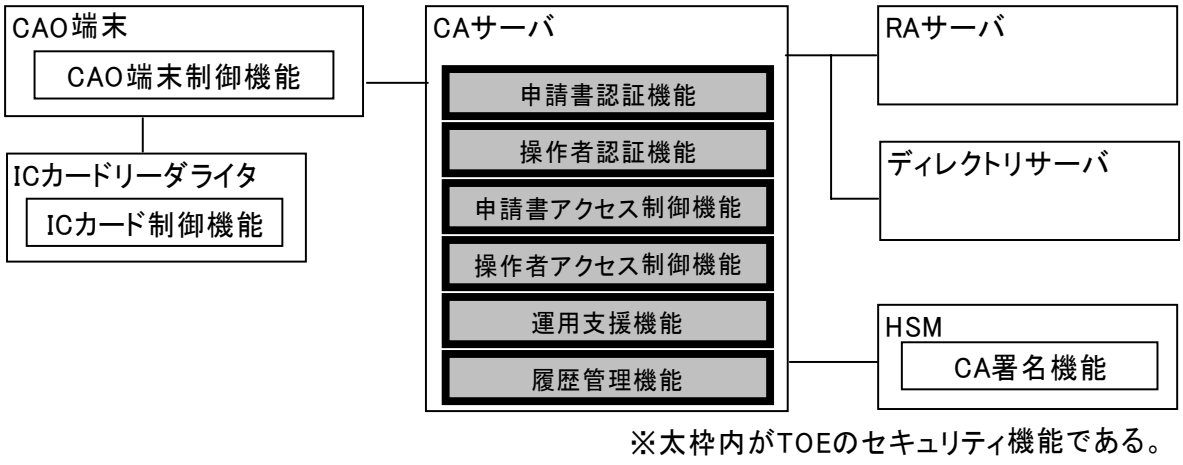

図 2-3 TOE のセキュリティ機能について

3 TOEセキュリティ環境

3.1 資産

TOE では、以下を保護資産とする。

- 申請書
- 報告書
- 発行された公開鍵証明書
- 公開鍵証明書テーブル
- 発行された CRL
- CRL テーブル
- ログ
- ログファイル
- クライアント認証テーブル
- 権限設定ファイル
- ログ設定ファイル

3.2 前提条件

A.PHYSICAL_PROTECT

TOE が動作するために必要なハードウェアは、入退管理されている場所に設置され、直接的な物理攻撃から保護されているものとする。また、サーバおよび HSM は施錠可能なサーバラックに配置し、直接的な操作から保護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とする。

A.IC_CARD

正当な操作者が所有する IC カードは、所有者が正当であることを確認できる情報を提供するものとする。

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 攻撃からも保護されているものとする。

A.NETWORK

CA サーバと CAO 端末間の通信路の情報は、改ざんの無いものとする。

A.OPERATOR

操作者は、信頼されるものであり、ガイダンス文書に従って CA の運用を行い、
・自己の所有する IC カードを他人に使わせない
・操作の途中、認められた操作者以外の者に CAO 端末を操作させない
ものとする。

A.ADMIN

CA 管理者は、細心の注意を払って CA の運用を行い、誤った操作を行わないという点でも信頼できるものとする。

3.3 脅威

T.AUTH

TOE に登録されていないものが、IT 機器を用いて、セキュアルーム外からネットワークを通して、TOE へ申請書を送信し、不正に資産を改ざんするかもしれない。

T.CAO_AUTH

セキュアルームに入室が可能な者が、CAO 端末から不正にログインして公開鍵証明書発行等を行うかもしれない。

T.ACCESS_CONTROL

TOE に公開鍵証明書を発行、失効の許可をされていないものが、申請書を用いて、不正に公開鍵証明書を発行、失効するかもしれない。

T.CAO_ACCESS_CONTROL

CA 操作者または監査人が、ログイン後、誤操作により権限外の操作を行うかもしれない。

T.COMMUNICATE

TOE の保護資産を改ざんしようとするものが、IT 機器を用いて、次の通信路上の、次の保護資産に対して改ざんを行うかもしれない。
・CA サーバとディレクトリサーバ間の通信路上の、公開鍵証明書あるいは CRL
・CA サーバと RA サーバの通信路上の、申請書あるいは報告書

3.4 組織のセキュリティ方針

P.AUDIT_DATA

TOE の生成するログは、改ざんや消去の検出が可能な状態で記録されなければならな

い。

P.MANAGEMENT

TOE を管理する組織の責任者は、予め組織内部セキュリティポリシーを決定し、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、パスワードの運用規則を定め、実施すること。

4 セキュリティ対策方針

4.1 TOEのセキュリティ対策方針

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.CAO_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、正当な操作者に対して、役割ごとに許可された操作のみ行うことができなければならない。

SO.LOG_GEN

TOE は、不正なアクセス行為を分析し追跡できるようなログを生成し、CA 管理者、監査人に読出を制限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。

SO.AUDIT_DATA

TOE は、ログファイル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。

4.2 環境のセキュリティ対策方針

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.SSL

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.PHYSICAL_PROTECT

TOE が動作するハードウェアは、TOE を管理する組織の責任者によって入退管理が可能な安全な場所に設置、管理されなければならない。また、サーバおよび HSM は施錠可能なサーバラックに配置し、直接的な操作から保護されなければならない。

SOE.HSM

CA の秘密鍵は、FIPS140-2 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 によって操作者が所有することを確認後、正当である証拠を提供しなければならない。

SOE.FIREWALL

CA サーバとセキュアルーム外との通信は、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 攻撃からも保護されるよう設定されなければならない。

SOE.NETWORK

CA サーバと CAO 端末間の通信は SSL を用いなければならない。

SOE.OPERATOR

TOEを管理する組織の責任者は、操作者に信頼される人を選定し、ガイダンス文書に従うことを周知しなければならない。操作者は、自己の所有するICカードの紛失、ICカードのPINの漏洩に注意し、操作の途中、認められた操作者以外の者にCAO端末を操作させないようにしなければならない。

SOE.ADMIN

TOEを管理する組織の責任者は、細心の注意を払ってCAの運用を行い、誤った操作を行わないという点でも信頼できるCA管理者を選定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、RA を登録する際もポリシーに従わなければならない。

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 の運用に関連するパスワードの運用規則を定め、実施しなければならない。

5 ITセキュリティ要件

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セキュリティ要件

5.1.1 TOE セキュリティ機能要件

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
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)ログの読出を行うとき
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)ログの読出を行うとき
FAU_STG.1	監査すべき識別されたアクションはない。	なし
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

機能要件	CC で定義された監査対象	監査事象
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) 操作者の署名の検証、RA の署名の検証または CA 署名を検証したとき
FDP_ACC.1(1)	監査対象にすべき識別された事象はない。	なし
FDP_ACC.1(2)	監査対象にすべき識別された事象はない。	なし
FDP_ACF.1(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) 公開鍵証明書テーブルの書込、失効情報の更新のとき
FDP_ACF.1(2)	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) 公開鍵証明書テーブルの読出、CRL 発行情報の更新のとき a)b)c) CRL テーブルの書込のとき
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 の署名の検証したとき
FIA_ATD.1(1)	監査対象にすべき識別されたアクションはない。	なし

機能要件	CC で定義された監査対象	監査事象
FIA_ATD.1(2)	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.1	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。 詳細: 利用者認証以前に行われたすべての TSF 調停アクション	最小)基本) 操作者もしくは RA を識別認証するとき
FIA_UID.1	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
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
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 の鍵対の更新、削除、バックアップのとき
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	a)クライアント認証テーブルの DN およびクラスの登録、削除、改変のとき a)権限設定ファイルのユーザ ID およびグループ ID および許可される操作の登録、削除、改変のとき a) 操作者の公開鍵証明書の登録
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) CA 署名を生成し、それを付したとき a) 操作者の署名の検証、RA の署名の検証または CA 署名を検証したとき
FMT_MTD.1	a) 基本: TSF データの値のすべての改変。	a)ログ設定ファイルの改変のとき

機能要件	CC で定義された監査対象	監査事象
FMT_SMF.1	a) 最小：管理機能の使用	a) クライアント認証テーブルの DN およびクラスの登録、削除、改変のとき a) 権限設定ファイルのユーザ ID、グループ ID、許可される操作の登録、削除、改変のとき a) HSM ドライバを用いた CA の鍵対の更新、削除、バックアップのとき a) 操作者の公開鍵証明書の登録
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) クライアント認証テーブルの DN およびクラスの登録、削除、改変のとき a) 権限設定ファイルのユーザ ID、グループ ID、許可される操作の登録、削除、改変のとき a) 操作者の公開鍵証明書の登録
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
FPT_SEP.1	監査対象にすべき識別されたアクションはない。	なし
FPT_STM.1	a) 最小: 時間の変更; b) 詳細: タイムスタンプの提供。	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、監査証跡内の監査記録への不正な改変を[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

FCS_COP.1(1) 暗号操作

下位階層: なし

FCS_COP.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.1.1 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 CA サーバ用の署名アルゴリズムとその鍵長

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

FDP_ACC.1(1) サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1 TSF は、[割付: *以下に示すサブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *申請書アクセス制御 SFP*]を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 管理者用申請書プロセス

・CA 操作者用申請書プロセス

・RA 用申請書プロセス

<アクセス制御の対象となるオブジェクト>

・公開鍵証明書テーブル

<SFP で扱われるサブジェクトとオブジェクト間の操作のリスト>

・書込

・失効情報の更新

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1(2) サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1 TSF は、[割付: *以下に示すサブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *操作者アクセス制御 SFP*]を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 管理者用操作プロセス

・CA 操作者用操作プロセス

・監査人用操作プロセス

<アクセス制御の対象となるオブジェクト>

・公開鍵証明書テーブル

・CRL テーブル

<SFP で扱われるサブジェクトとオブジェクト間の操作のリスト>

・読出

・書込

・CRL 発行情報の更新

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(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、以下の[割付: *表 5-4 に示すサブジェクトとオブジェクト、及び各々に対応する、クライアント認証テーブルおよび権限設定ファイル*]に基づいて、オブジェクトに対して、[割付: *申請書アクセス制御 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 申請書アクセス制御規則

制御されたサブジェクト	制御されたオブジェクト	許可される操作
CA 管理者用申請書プロセス	公開鍵証明書テーブル	書込、失効情報の更新
CA 操作者用申請書プロセス	公開鍵証明書テーブル	書込、失効情報の更新
RA 用申請書プロセス	公開鍵証明書テーブル	書込、失効情報の更新

FDP_ACF.1(2) 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、以下の[割付: *表 5-5 に示すサブジェクトとオブジェクト、及び各々に対応する、権限設定ファイル*]に基づいて、オブジェクトに対して、[割付: *操作者アクセス制御 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 5-5 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 5-5 操作者アクセス制御規則

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	公開鍵証明書テーブル	読出、CRL 発行情報の更新
	CRL テーブル	書込
CA 操作者プロセス	公開鍵証明書テーブル	読出、CRL 発行情報の更新
	CRL テーブル	書込
監査人プロセス	なし	なし

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: *申請書アクセス制御 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(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*:* クライアント認証テーブルの DN およびクラス、権限設定ファイルのユーザ ID およびグループ ID および許可される操作]を維持しなければならない。

依存性: なし

FIA_ATD.1(2) 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*:* 権限設定ファイルのユーザ ID およびグループ ID および許可される操作]を維持しなければならない。

依存性: なし

FIA_UAU.1 認証のタイミング

下位階層: なし

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる[割付: *識別認証失敗時のエラーの報告*]を許可しなければならない。

FIA_UAU.1.2 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.1 識別のタイミング

下位階層: なし

FIA_UID.1.1 TSF は、利用者が識別される前に利用者を代行して実行される[割付:*識別認証失敗時のエラーの報告*]を許可しなければならない。

FIA_UID.1.2 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、各利用者に識別が成功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 の鍵対の更新、削除、バックアップ*][選択:*を動作させる*]能力を[割付: *鍵対の管理グループ*]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定
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: 以下のリストのセキュリティ属性]に対し[詳細化:*以下のリストに従った*][選択:*改変*、*削除*、[割付:*登録*]]をする能力を[割付:*CA 管理者*]に制限するために[割付: *操作者アクセス制御 SFP*]を実施しなければならない。

＜セキュリティ属性と能力の制限のリスト＞

・クライアント認証テーブル｛DN、クラス｝に対して改変と削除と登録

・権限設定ファイル｛ユーザ ID、グループ ID、許可される操作｝に対して改変と削除と登録

・操作者の公開鍵証明書に対して登録

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_SMF.1 管理機能の特定
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: *ログ設定ファイル*]を[選択:*改変*、 [割付: *なし*]]する能力を[割付:*CA 管理者*]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層： なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付: *表 5-6 の下線に示したもの*]。

依存性： なし

表 5-6CANP セキュリティ管理

機能要件	管理アクティビティ	対応する機能要件とデータ
FAU_GEN.1	予見される管理アクティビティはない。	－
FAU_GEN.2	予見される管理アクティビティはない。	－
FAU_SAR.1	a) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	FMT_MSA.1、権限設定ファイル
FAU_SAR.2	予見される管理アクティビティはない。	－
FAU_STG.1	予見される管理アクティビティはない。	－
FCS_COP.1(1)	予見される管理アクティビティはない。	－

機能要件	管理アクティビティ	対応する機能要件とデータ
FCS_COP.1(2)	予見される管理アクティビティはない。	－
FDP_ACC.1(1)	予見される管理アクティビティはない。	－
FDP_ACC.1(2)	予見される管理アクティビティはない。	－
FDP_ACF.1(1)	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	－
FDP_ACF.1(2)	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	－
FDP_UIT.1	予見される管理アクティビティはない。	－
FIA_ATD.1(1)	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	－
FIA_ATD.1(2)	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	－
FIA_UAU.1	管理者による認証データの管理; 関係する利用者による認証データの管理; 利用者が認証される前にとられるアクションのリストを管理すること。	FMT_MSA.1、操作者の公開鍵証明書
FIA_UID.1	a) 利用者識別情報の管理; b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。	FMT_MSA.1、クライアント認証テーブル FMT_MSA.1、権限設定ファイル
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。	－
FMT_MOF.1	a) TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること;	FMT_MSA.1、権限設定ファイル
FMT_MSA.1	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	FMT_MSA.1、権限設定ファイル
FMT_MSA.2	予見される管理アクティビティはない。	－
FMT_MTD.1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	FMT_MSA.1、権限設定ファイル
FMT_SMF.1	予見される管理アクティビティはない。	－
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	FMT_MSA.1、権限設定ファイル
FPT_RVM.1	予見される管理アクティビティはない。	－
FPT_SEP.1	予見される管理アクティビティはない。	－
FPT_STM.1	a) 時間の管理。	－

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*、*CA 操作者*、*監査人*、*RA*、*鍵対の管理グループ*]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

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

FPT_SEP.1 TSFドメイン分離

下位階層: なし

FPT_SEP.1.1 TSF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 TSFは、TSC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 TSF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

5.1.2 TOE セキュリティ保証要件

本 TOE の保証要件は EAL2 からなる。これらは CC part3 から選択されている。

5.2 IT環境に対するセキュリティ機能要件

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: *なし*]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.1.1 [詳細化:*HSM*]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

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:*HTTP 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:*HTTP 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:*HTTP 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 最小機能強度(SOF)主張

本 TOE における最小機能強度レベルを、SOF-基本として主張する。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、最小機能強度として、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要約仕様

6.1 TOEセキュリティ機能

SF. AUTH 申請書認証機能

SF. AUTH は、次のように RA の識別認証を行う。

RA から受信した「申請書」内の情報を元に、RA の「DN」を識別する（FIA_UID.1）。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（FIA_UAU.1）および「申請書」の完全性を確認する(FDP_UIT.1)。

「申請書」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、有効でない場合は署名の検証は成功しない。

以上の確認および検証の結果、認証に成功しない場合は、エラーを示す報告書を作成する。

また、SF. 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（FPT_RVM.1、FPT_SEP.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)、FDP_UIT.1、FIA_UAU.1、FIA_UID.1、FMT_MSA.2、FPT_RVM.1、FPT_SEP.1

表 6-1 CA サーバ用署名アルゴリズム

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

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 端末上にて、IT 環境の IC カードによって署名を生成する。署名は、CA サーバに送信後、CA サーバ上にて認証に用いる。使用できる署名アルゴリズムは表 6-2 に示す標準に従ったアルゴリズムを使用し、表 6-2 に従った鍵長を選択できる。

② CAO 端末から「IT 環境の IC カードの署名」と「ユーザ ID」、または「IT 環境の IC カードの署名」と「グループ ID」を CA サーバへ送信する。

③ CA サーバが、CAO 端末から「ユーザ ID またはグループ ID」および「IT 環境の IC カードの署名」を受信する。

④ 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（FIA_UID.1）する。

⑤ CAO 端末から受信した「IC カードの署名」を操作者の公開鍵証明書を用いて検証（FCS_COP.1(2)）することによって、認証（FIA_UAU.1）を行い、識別認証の結果を CAO 端末に送信する。

CAO 端末からの認証データの検証時には、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 2 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）

このチェックにより、有効でない場合、認証は成功しない。

認証が、成功しない場合は、エラーを示すメッセージを返却する。

⑥ 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、RA の公開鍵証明書発行や失効、CRL の発行、表 6-5 に示すオペレーションなどを行う。

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（FPT_RVM.1、FPT_SEP.1）
-

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

表 6-2　CAO 端末用署名アルゴリズム

アルゴリズム	鍵長(bit)	標準
SHA1 with RSA	512～2048	PKCS#1

SF.ACCESS_CONTROL　申請書アクセス制御機能

SF.ACCESS_CONTROL は、識別認証された CA 管理者、CA 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機能である。(FIA_USB.1、FIA_ATD.1(1)、FMT_SMR.1）。CA 管理者、CA 操作者を代行するプロセスは、権限設定ファイルによって、公開鍵証明書テーブルに対して表 6-3 のように操作を制限され、RA を代行するプロセスは、クライアント認証テーブルによって公開鍵証明書テーブルに対して表 6-3 のように操作を制限される(FDP_ACC.1(1)、FDP_ACF.1(1))。

また、SF.ACCESS_CONTROL もしくは SF.CAO_ACCESS_CONTROL を介さず公開鍵証明書テーブルを操作することはできない（FPT_RVM.1、FPT_SEP.1）。

TOE は、「申請書」内の申請種別を読み取ることによって操作を理解する。

A) 申請種別が「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.1(1)、FDP_ACF.1(1)）。

② 「申請書」の内容に従い、「公開鍵証明書」を作成する。「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_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２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）このチェックにより、有効でない場合、CA 署名は生成されない。生成されない場合は、エラーを示す報告書を作成する。

③ 作成した「公開鍵証明書」を「公開鍵証明書テーブル」に書込を行い、さらに「申請書」の送信元へ送信する。

B) 申請種別が「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.1(1)、FDP_ACF.1(1)）。

② 「申請書」の内容に従い、「公開鍵証明書テーブル」の中の当該の「公開鍵証明書」の状態を失効に更新する。

③ 「公開鍵証明書失効」が成功したことを示す「報告書」を作成する。「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_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２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）このチェックにより、有効でない場合、CA 署名は生成されない。生成されない場合は、エラーを示す報告書を作成する。

④ 作成した「報告書」を「申請書」の送信元へ送信する。

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

表 6-3　申請書アクセス制御機能による公開鍵証明書テーブルのアクセス制御

役割	機能	操作対象	操作
CA 管理者	公開鍵証明書発行	公開鍵証明書テーブル	書込（FDP_ACF.1(1)）
	公開鍵証明書失効	公開鍵証明書テーブル	失効情報の更新（FDP_ACF.1(1)）
CA 操作者	公開鍵証明書発行	公開鍵証明書テーブル	書込（FDP_ACF.1(1)）
	公開鍵証明書失効	公開鍵証明書テーブル	失効情報の更新（FDP_ACF.1(1)）
RA	公開鍵証明書発行	公開鍵証明書テーブル	書込（FDP_ACF.1(1)）
	公開鍵証明書失効	公開鍵証明書テーブル	失効情報の更新（FDP_ACF.1(1)）

SF.CAO_ACCESS_CONTROL 操作者アクセス制御機能

SF.CAO_ACCESS_CONTROL は、識別認証された操作者に対するアクセス制御を行う機能である（FIA_USB.1、FIA_ATD.1(2)、FMT_SMR.1)。操作者を代行するプロセスは、権限設定ファイルによって公開鍵証明書テーブルおよび CRL テーブルに対して、表 6-4 のように制限される（FDP_ACC.1(2)、FDP_ACF.1(2)）。

また、SF.ACCESS_CONTROL もしくは SF.CAO_ACCESS_CONTROL を介さず公開鍵証明書テーブルおよび CRL テーブルを操作することはできない（FPT_RVM.1、FPT_SEP.1)。

操作は、CUI ベースで行われ、CRL 発行は以下の手順で行われる。

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

② 「公開鍵証明書テーブル」の中から失効状態の「公開鍵証明書」検索し、「CRL」を作成する。「CRL」には、HSM を用いて、コマンドで指定された表 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（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２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)

このチェックにより、有効でない場合、CA 署名は生成されない。生成しない場

合は、エラーを示すメッセージを返却する。

③ 作成した「CRL」は、「CRL テーブル」に書込を行う。

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

表 6-4 公開鍵証明書テーブルおよび CRL テーブルのアクセス制御

操作者の役割	機能	操作対象	操作
CA 管理者	CRL 発行	公開鍵証明書テーブル	読出、CRL 発行情報の更新（FDP_ACF.1(2)）
		CRL テーブル	書込（FDP_ACF.1(2)）
CA 操作者	CRL 発行	公開鍵証明書テーブル	読出、CRL 発行情報の更新（FDP_ACF.1(2)）
		CRL テーブル	書込（FDP_ACF.1(2)）

SF. PRIVILEGE 運用支援機能

SF. PRIVILEGE は、識別認証された操作者に対する運用支援に関する機能であり、識別認証された操作者のユーザ ID もしくはグループ ID と権限設定ファイルによって管理する(FIA_USB.1、FIA_ATD.1(2)、FMT_SMF.1、FMT_SMR.1) 。また、カレントログおよび非カレントログの署名の検証を行う（FCS_COP.1(1)、FCS_COP.1(2)）。CA サーバを運用するための管理を、表 6-5 のように行う。また、SF. PRIVILEGE を介さず表 6-5 の管理を行うことはできない（FPT_RVM.1）。

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

表 6-5 CA サーバを運用するための操作

役割	機能	操作対象	操作
CA 管理者	ログ設定ファイルの変更	ログ設定ファイル	改変（FMT_MTD.1）
	クライアント認証テーブルの DN、クラスの変更のとき	クライアント認証テーブル	登録、削除、改変（FMT_MSA.1）
	権限設定ファイルのユーザ ID、グループ ID、許可される操作の変更のとき	権限設定ファイル	登録、削除、改変（FMT_MSA.1）
	操作者の公開鍵証明書の登録	操作者の公開鍵証明書	登録（FMT_MSA.1）
	ログの読出	ログ	読出（FAU_SAR.1、FAU_SAR.2、FCS_COP.1(1)、FCS_COP.1(2)）
鍵対の管	CA の鍵対の管理操作	HSM 内の CA の	更新、削除、バックアップ

役割	機能	操作対象	操作
理グループ	（注）	鍵対	（FMT_MOF.1）
監査人	ログの読出	ログ	読出（FAU_SAR.1、FAU_SAR.2、FCS_COP.1(1)、FCS_COP.1(2)）

(注)「CA の鍵対の管理操作」は、鍵対の管理グループに属する操作者がすべて認証に成功した場合に「鍵対の管理グループ」の操作として実行される。

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、ログを、日付・時刻（FPT_STM.1）とともに、表 6-6 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）。

ログに対して、削除する手段を提供していないことと、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。

ログファイルは操作ごとにログが書き込まれるカレントログファイルと、ログ設定ファイルに記述される契機ごとにカレントログファイルから移行される非カレントログファイルがある。カレントログファイルにはログを記録するごとに署名を行うので、マシン負荷の少ないハッシュ署名を用い、非カレントログファイルには CA 署名を用いる。

① ハッシュ署名（FCS_COP.1(1)）は、ログが更新されるたびに付される署名であり、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。また、ハッシュ署名の生成及び検証は、表 6-7 のアルゴリズムを使用する。

② ログファイルに対して、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。ログファイルに対しての CA 署名を行う契機毎に、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、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をチェックしている(FMT_MSA.2)。

・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）

・ 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ようログを生成する（FAU_SAR.1）。

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

表 6-6 監査事象

監査事象	監査事象に関連する機能要件
ログの読出を行うとき	FAU_SAR.1、FAU_SAR.2
CA 署名を生成し、それを付したとき	FDP_UIT.1、FMT_MSA.2
ハッシュ署名の生成及び検証のとき	FCS_COP.1(1)
操作者の署名の検証、RA の署名の検証または CA 署名を検証したとき	FCS_COP.1(2) 、 FDP_UIT.1 、FMT_MSA.2
公開鍵証明書テーブルの書込、失効情報の更新のとき	FDP_ACF.1(1)
公開鍵証明書テーブルの読出、CRL 発行情報の更新のとき	FDP_ACF.1(2)
CRL テーブルの書込のとき	FDP_ACF.1(2)
操作者もしくは RA を識別認証するとき	FIA_UAU.1 、 FIA_UID.1 、FIA_USB.1
HSM ドライバを用いた CA の鍵対の更新、削除、バックアップのとき	FMT_MOF.1、FMT_SMF.1
クライアント認証テーブルの DN およびクラスの登録、削除、改変のとき	FMT_MSA.1 、 FMT_SMR.1 、FMT_SMF.1
権限設定ファイルのユーザ ID、グループ ID、許可される操作の登録、削除、改変のとき	FMT_MSA.1 、 FMT_SMR.1 、FMT_SMF.1
操作者の公開鍵証明書の登録	FMT_MSA.1 、 FMT_SMF.1 、FMT_SMR.1
ログ設定ファイルの変更のとき	FMT_MTD.1

表 6-7 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

6.2 機能強度(SOF)主張

確率的または順列的メカニズムとして、SF.AUTH、SF.CAO_AUTH、SF.ACCESS_CONTROL、SF.CAO_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、その機能強度レベルは、SOF-基本である。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機能強度レベルは、SOF-基本である。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 保証手段

ASE クラス及び EAL2 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 6-8 に示す。

表 6-8 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 V8.0i Security Target
ACM:構成管理	ACM_CAP.2	Trust-CANP V8.0i 構成管理仕様書
ADO:配付と運用	ADO_DEL.1 ADO_IGS.1	Trust-CANP V8.0i 配付マニュアル Trust-CANP V8.0i 構築マニュアル
ADV:開発	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1	Trust-CANP V8.0i 機能仕様書
AGD:ガイダンス文書	AGD_ADM.1 AGD_USR.1	Trust-CANP V8.0i 概要書 Trust-CANP V8.0i 運用マニュアル
ATE:テスト	ATE_COV.1 ATE_FUN.1 ATE_IND.2	Trust-CANP V8.0i テスト仕様書 Trust-CANP V8.0i テスト結果一覧 Trust-CANP V8.0i (TOE)
AVA:脆弱性評定	AVA_SOF.1 AVA_VLA.1	Trust-CANP V8.0i SOF 分析書 Trust-CANP V8.0i 脆弱性分析書

7 PP主張

この ST で参照される PP はない。

8 根拠

8.1 セキュリティ対策方針根拠

表 8-1 セキュリティ対策方針根拠

	SO.RA_AUTH	SO.CAO_AUTH	SO.PRIVILEGES	SO.LOG_GEN	SO.CA_SIGN	SO.AUDIT_DATA	SOE.CA_SIGN	SOE.CA_KEY	SOE.SSL	SOE.PHYSICAL_PROTECT	SOE.HSM	SOE.IC_CRAD	SOE.FIREWALL	SOE.NETWORK	SOE.OPERATOR	SOE.ADMIN	SOE.MANAGEMANT	SOE.PASSWORD
T.AUTH	○			○														
T.CAO_AUTH		○		○								○						
T.ACCESS_CONTROL			○	○														
T.CAO_ACCESS_CONTROL			○	○														
T.COMMUNICATE					○		○	○	○									
A.PHYSICAL_PROTECT										○								
A.HSM											○							
A.IC_CARD												○						
A.FIREWALL													○					
A.NETWORK														○				
A.OPERATOR															○			
A.ADMIN																○		
P.AUDIT_DATA						○												
P.MANAGEMENT																	○	
P.RA_TRUST																	○	
P.PASSWORD																		○

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

なぜなら、TOE は、SO.RA_AUTH によって、外部のネットワーク上にある RA から申請書を受信した場合、RA を識別認証するからである。また、SO.LOG_GEN によって、不正なアクセス行為を分析し追跡できるようなログを生成することによって､不正なアクセス行為を事後に検知できるからである。

T.CAO_AUTH は SO.CAO_AUTH と SO.LOG_GEN と SOE.IC_CARD によって対抗される。

なぜなら、TOE は、SO.CAO_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。その際の認証データは、SOE.IC_CARD によって、PIN によって操作者が所有することを確認後、正当であることを確認して作られるものである。また、SO.LOG_GEN によって、不正なアクセス行為を分析し追跡できるようなログを生成することによって、不正なアクセス行為を事後に検知できるからである。

T.ACCESS_CONTROL 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、正当な操作者に対して、役割ごとに許可された操作のみ行うことができるからである。また、SO.LOG_GEN によって、不正なアクセス行為を分析し追跡できるようなログを生成することによって、不正なアクセス行為を事後に検知できるからである。

T.CAO_ACCESS_CONTROL 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、正当な操作者に対して、役割ごとに許可された操作のみ行うことができるからである。また、SO.LOG_GEN によって、不正なアクセス行為を分析し追跡できるようなログを生成することによって、不正なアクセス行為を事後に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.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 の本人性の確認のための 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 の本人性の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.SSL によって、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、TOE が動作するハードウェアは、TOE を管理する組織の責任者によって入退管理が可能な安全な場所に設置、管理されているからであり、また、サーバおよび HSM は施錠可能なサーバラックに配置し、直接的な操作から保護されているからである。

A.HSM は、SOE.HSM で実現できる。
なぜなら、SOE.HSM によって、CA の秘密鍵は、FIPS140-2 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。

A.IC_CARD は、SOE.IC_CARD で実現できる。
なぜなら、SOE.IC_CARD によって、IC カードは、PIN によって操作者が所有することを確認後、正当である証拠を提供するからである。

A.FIREWALL は、SOE.FIREWALL で実現できる。
なぜなら、SOE.FIREWALL によって、CA サーバとセキュアルーム外との通信には、すべてファイアウォールサーバを通して行われているからであり、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 攻撃からも保護されるよう設定されているからである。

A.NETWORK は、SOE.NETWORK で実現できる。
なぜなら、SOE.NETWORK によって、CA サーバと CAO 端末間の通信は SSL を用いているからである。

A.OPERATOR は、SOE.OPERATOR で実現できる。
なぜなら、SOE.OPERATOR によって、操作者は、信頼される人を選定されており、ガイダンス文書に従うからである。また、操作者は、自己の所有する IC カードの紛失、IC カードの PIN の漏洩に注意し、操作の途中、認められた操作者以外の者に CAO 端末を操作させないように CA を運用するからである。

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、細心の注意を払って CA の運用を行い、誤った操作を行わないという点でも信頼できる CA 管理者を選定するからである。

P. AUDIT_DATA は、SO. AUDIT_DATA で実現できる。
なぜなら、TOE は、ログファイルに対して改ざんまたは削除を検出することができるからである。

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し、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ポリシーに基づいたガイダンス文書を作成し、RA 登録時においてもそれを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、実施するため、パスワードの安全性が保たれるからである。

8.2 セキュリティ要件根拠

8.2.1 セキュリティ要件根拠

表 8-2　セキュリティ要件根拠 その 1

	TOE の機能要件														
	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_STG.1	FCS_COP.1(1)	FCS_COP.1(2)	FDP_ACC.1(1)	FDP_ACC.1(2)	FDP_ACF.1(1)	FDP_ACF.1(2)	FDP_UIT.1	FIA_ATD.1(1)	FIA_ATD.1(2)	FIA_UAU.1
SO.RA_AUTH							○								○
SO.CAO_AUTH							○								○
SO.PRIVILEGES								○	○	○	○		○	○	
SO.LOG_GEN	○	○	○	○											
SO.CA_SIGN							○					○			
SO.AUDIT_DATA					○	○	○								
SOE.CA_SIGN															
SOE.CA_KEY															
SOE.SSL															

表 8-2　セキュリティ要件根拠 その 2

	TOE の機能要件											IT 環境の機能要件			
	FIA_UID.1	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FCS_CKM.1	FCS_CKM.4	FCS_COP.1(3)	FTP_ITC.1
SO.RA_AUTH	○				○				○	○					
SO.CAO_AUTH	○				○				○	○					

SO.PRIVILEGES		○	○	○		○	○	○	○	○					
SO.LOG_GEN											○				
SO.CA_SIGN					○										
SO.AUDIT_DATA					○										
SOE.CA_SIGN														○	
SOE.CA_KEY												○	○		
SOE.SSL															○

SO.RA_AUTH は、FCS_COP.1(2)、FIA_UAU.1、FIA_UID.1、FMT_MSA.2、FPT_RVM.1 と FPT_SEP.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、TOE は、RA の署名の検証を行う。また、TOE は、検証のを行うときに 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.1 によって、TOE は、RA に対して TOE にアクセスして識別認証に関わるアクション以外を許可する前に、RA の識別を行う。
- FIA_UAU.1 によって、TOE は、RA に対して TOE にアクセスして識別認証に関わるアクション以外を許可する前に、RA の認証を正しく行う。
- FPT_RVM.1 によって、TOE は、RA に対して、TOE の識別認証に関する機能以外にアクセスする際に必ず FIA_UAU.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。また、FPT_SEP.1 によって、TOE 以外のサブジェクトによる干渉や改ざんを保護している。

SO.CAO_AUTH は、FCS_COP.1(2)、FIA_UAU.1、FIA_UID.1 、FMT_MSA.2、FPT_RVM.1 と FPT_SEP.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、TOE は、IC カードの署名の検証を行う。また、TOE は、検証のを行うときに 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.1 によって、TOE は、操作者に対して TOE の識別認証に関する機能以外にアクセスしてアクションを許可する前に、操作者の識別を行う。
- FIA_UAU.1 によって、TOE は、操作者に対して TOE の識別認証に関する機能以外にアクセスしてアクションを許可する前に、操作者の認証を正しく行う。
- FPT_RVM.1 によって、TOE は、操作者に対して、TOE の識別認証に関する機能以外にアクセスする際に必ず FIA_UAU.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。また、FPT_SEP.1 によって、TOE 以外のサブジェクトによる干渉や改ざんを保護している。

SO.PRIVILEGES は、FDP_ACC.1(1)、FDP_ACC.1(2)、FDP_ACF.1(1)、FDP_ACF.1(2)、FIA_ATD.1(1)、FIA_ATD.1(2)、FIA_USB.1、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1 と FPT_SEP.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役割を維持し、関連付けている。
- FIA_ATD.1(1)によって、クライアント認証テーブルの DN およびクラス、権限設定ファイルのユーザ ID およびグループ ID および許可される操作を維持する。
- FDP_ACC.1(1)によって、サブジェクトとオブジェクトについての公開鍵証明書テーブルに対する書込、失効情報の更新の操作が、申請書アクセス制御 SFP で制御される。
- FDP_ACF.1(1)によって、申請書アクセス制御 SFP に基づくアクセスを実施する。
- FIA_ATD.1(2)によって、権限設定ファイルのユーザ ID およびグループ ID および許可される操作を維持する。
- FDP_ACC.1(2)によって、サブジェクトとオブジェクトについての公開鍵証明書テーブルに対する読出と CRL 発行情報の更新、CRL テーブルに対する書込の操作が、操作者アクセス制御 SFP で制御される。
- FDP_ACF.1(2)によって、操作者アクセス制御 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 の鍵対の更新、削除、バックアップを鍵対の管理グループのみに制限する。
- FMT_MSA.1 によって、クライアント認証テーブルの DN およびクラスの登録、削除改変が CA 管理者のみに限定される。また、権限設定ファイルのユーザ ID およびグループ ID および許可される操作の登録と削除と改変が CA 管理者のみに限定される。
- FMT_MTD.1 によって、ログ設定ファイルの改変を CA 管理者に制限する。
- FMT_SMF.1 によって、権限設定ファイルおよびクライアント認証テーブルを管理する。
- FPT_RVM.1 によって、RA が TOE にアクセスする際に必ず FDP_ACC.1(1)、FDP_ACF.1(1)を呼び出し、操作者が TOE にアクセスする際に必ず FDP_ACC.1(2)、FDP_ACF.1(2)を呼び出すことによって、他の機能要件がバイパスされることを防ぐ。また、FPT_SEP.1 によって、TOE 以外のサブジェクトによる干渉や改ざんを保護している。

SO.LOG_GEN は、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2 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。

- 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 FPT_STM.1 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.CA_SIGN は、FCS_COP.1(2)、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_UIT.1 によって、申請書、報告書、公開鍵証明書、CRL を改変誤りから保護した形で送信、受信が行われる。

SO.AUDIT_DATA は、FAU_STG.1、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、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、ログファイル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。

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.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 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。

8.2.2 セキュリティ要件の依存性の根拠

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、依存性を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要件	満たしていない機能要件
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	―
	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.1(1)	FDP_ACF.1(1)	―
	FDP_ACC.1(2)	FDP_ACF.1(2)	―
	FDP_ACF.1(1)	FDP_ACC.1(1)	FMT_MSA.3
	FDP_ACF.1(2)	FDP_ACC.1(2)	FMT_MSA.3
	FDP_UIT.1	FDP_ACC.1(1) *FTP_ITC.1*	―
	FIA_ATD.1(1)	―	―
	FIA_ATD.1(2)	―	―
	FIA_UAU.1	FIA_UID.1	―
	FIA_UID.1	―	―
	FIA_USB.1	FIA_ATD.1(1) FIA_ATD.1(2)	―
	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	―
	FMT_MSA.1	FDP_ACC.1(1) FDP_ACC.1(2) FMT_SMF.1 FMT_SMR.1	―
	FMT_MSA.2	FDP_ACC.1(1) FDP_ACC.1(2) FMT_MSA.1 FMT_SMR.1	ADV_SPM.1
	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	―
	FMT_SMF.1	―	―
	FMT_SMR.1	FIA_UID.1	―

	FPT_RVM.1	－	－
	FPT_SEP.1	－	－
	FPT_STM.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*	－
	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。

・ 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 HTTP 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(1)、FDP_ACF.1(2)から依存する FMT_MSA.3

TOE は、セキュリティ属性の初期値を信頼される CA 管理者にゆだねる為、デフォルト値を設定する必要はない。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.AUTH、SF.CAO_AUTH、SF.ACCESS_CONTROL、SF.CAO_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＞
FPT_SEP.1 により、セキュリティドメインの干渉および改ざんを防止する。

＜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 の鍵対の更新、削除、バックアップ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)、定められた役割である 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 監査事象の根拠

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 保証要件の根拠

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.1 の保証要件で保証され、また、ATE_FUN.1 、ATE_COV.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 EAL2 が妥当と考える。

8.2.5 最小機能強度(SOF)主張根拠

TOE は 3.2 前提条件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 脅威で述べたように、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、最小機能強度レベルは SOF-基本が妥当であるといえる。

8.3 TOE要約仕様根拠

8.3.1 セキュリティ機能根拠

表 8-4　セキュリティ機能根拠

	SF. AUTH	SF. CAO_AUTH	SF.ACCESS_CONTROL	SF. CAO_ACCESS_CONTROL	SF. PRIVILEGE	SF.AUDIT
FAU_GEN.1						○
FAU_GEN.2						○
FAU_SAR.1					○	○
FAU_SAR.2					○	
FAU_STG.1						○
FCS_COP.1(1)					○	○
FCS_COP.1(2)	○	○			○	
FDP_ACC.1(1)			○			
FDP_ACC.1(2)				○		
FDP_ACF.1(1)			○			
FDP_ACF.1(2)				○		
FDP_UIT.1	○		○	○		
FIA_ATD.1(1)			○			
FIA_ATD.1(2)				○	○	
FIA_UAU.1	○	○				
FIA_UID.1	○	○				
FIA_USB.1			○	○	○	
FMT_MOF.1					○	
FMT_MSA.1					○	
FMT_MSA.2	○	○	○	○		○
FMT_MTD.1					○	
FMT_SMF.1					○	
FMT_SMR.1			○	○	○	
FPT_RVM.1	○	○	○	○	○	
FPT_SEP.1	○	○	○	○	○	
FPT_STM.1						○

FAU_GEN.1 監査データ生成(SF.AUDIT)

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 6-6

に基づく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)

SF.AUDIT

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

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、ユーザ ID とグループ ID と権限設定ファイルを元に、表 6-5 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)

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、ユーザ ID とグループ ID と権限設定意ファイルを元に、表 6-5 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)

SF.AUDIT

動作中に生成されるすべてのログに対して署名生成し、それを付す。それにより、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。また、ログの削除する手段を提供していないことで実現している。

FCS_COP.1(1) 暗号操作(SF.AUDIT、SF. PRIVILEGE)

SF.AUDIT

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。

SF. PRIVILEGE

ハッシュ署名が付されたログに対しての読出の際には､ハッシュ署名を検証することにより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.AUTH、SF.CAO_AUTH、SF. PRIVILEGE)

SF.AUTH

RA からの認証を行う際、「申請書」の署名検証することで実現している。

SF.CAO_AUTH

CAO 端末からの認証を行う際、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. PRIVILEGE

CA 署名が付されたログに対しての読出の際には、CA 署名を検証することによりログの改ざんの検知を行うことで実現している。

FDP_ACC.1(1) サブセットアクセス制御(SF.ACCESS_CONTROL)

SF.ACCESS_CONTROL

識別認証された CA 管理者もしくは CA 操作者から TOE に対して申請書による操作が行われた場合、権限設定ファイルとクライアント認証テーブルに基づいて表 6-3 に従った操作を許可することで実現している。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、クライアント認証テーブルに基づいて、表 6-3 に従った操作を許可することで実現している。

FDP_ACC.1(2) サブセットアクセス制御(SF.CAO_ACCESS_CONTROL)

SF.CAO_ACCESS_CONTROL

識別認証された操作者から TOE に対してコマンドによる操作が行われた場合、権限設定ファイルに基づいて、表 6-4 に従った操作を許可することで実現している。

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

SF.ACCESS_CONTROL

識別認証された CA 管理者もしくは CA 操作者から TOE に対して申請書による操作が行われた場合、権限設定ファイルとクライアント認証テーブルに基づいて表 6-3 に従った操作を許可することで実現している。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、クライアント認証テーブルに基づいて、表 6-3 に従った操作を許可することで実現している。

FDP_ACF.1(2) セキュリティ属性によるアクセス制御(SF.CAO_ACCESS_CONTROL)

SF.CAO_ACCESS_CONTROL

識別認証された操作者から TOE に対してコマンドによる操作が行われた場合、権限設定ファイルに基づいて、表 6-4 に従った操作を許可することで実現している。

FDP_UIT.1 データ交換完全性(SF.AUTH、SF.ACCESS_CONTROL、SF.CAO_ACCESS_CONTROL)

SF.AUTH

RA からの認証を行う際、「申請書」の署名検証することで、申請書の完全性を確認す

ることで実現している。

SF.ACCESS_CONTROL

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。

SF.CAO_ACCESS_CONTROL

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 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(1) 利用者属性定義(SF.ACCESS_CONTROL)

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、クライアント認証テーブルの DN およびクラス、権限設定ファイルのユーザ ID およびグループ ID および許可される操作を維持することで実現している。

FIA_ATD.1(2) 利用者属性定義(SF.CAO_ACCESS_CONTROL、SF.PRIVILEGE)

SF.CAO_ACCESS_CONTROL

利用者に属するセキュリティ属性のリストである、権限設定ファイルのユーザ ID およびグループ ID および許可される操作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、権限設定ファイルのユーザ ID およびグループ ID および許可される操作を維持することで実現している。

FIA_UAU.1 認証のタイミング(SF.AUTH、SF.CAO_AUTH)

SF.AUTH

識別認証されるまで、TOE に対して CAO 端末以外の経路からのアクセスからの識別認証以外の操作を行うことができないことで実現している。

SF.CAO_AUTH

識別認証されるまで、TOE に対して CAO 端末からの識別認証以外の操作を行うことができないことで実現している。

FIA_UID.1 識別のタイミング(SF.AUTH、SF.CAO_AUTH)

SF.AUTH

識別認証されるまで、TOE に対して CAO 端末以外の経路からのアクセスからの識別認証以外の操作を行うことができないことで実現している。

SF.CAO_AUTH

識別認証されるまで、TOE に対して CAO 端末からの識別認証以外の操作を行うこと

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.CAO_ACCESS_CONTROL、SF.PRIVILEGE)

SF.ACCESS_CONTROL

識別認証された CA 管理者もしくは CA 操作者のユーザ ID もしくはグループ ID と許可される操作を結びつけることと、識別認証された RA の DN とクラスを結びつけることで実現している。

SF.CAO_ACCESS_CONTROL

識別認証された操作者のユーザ ID もしくはグループ ID と許可される操作の権限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ユーザ ID もしくはグループ ID と許可される操作の権限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)

SF.PRIVILEGE

HSM ドライバを用いた CA の鍵対の更新、削除、バックアップを鍵対の管理グループ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)

SF.PRIVILEGE

権限設定ファイルのユーザ ID およびグループ ID および許可される操作と、クライアント認証テーブルの DN およびクラスの各々の登録、改変、削除と、公開鍵証明書の登録を 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.AUTH 、 SF.CAO_AUTH 、SF.ACCESS_CONTROL、SF.CAO_ACCESS_CONTROL、SF.AUDIT)

SF.AUTH

「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.CAO_AUTH

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、鍵の有効期間及び鍵種別をチェックすることで実現している。

SF.ACCESS_CONTROL

「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､鍵の有効期間及び鍵種別をチェックすることで実現している。

SF.CAO_ACCESS_CONTROL

「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、鍵の有効期間及び鍵種別をチェックすることで実現している。

SF.AUDIT

ログに対して CA 署名の検証の時、CA の秘密鍵と対を成す公開鍵証明書に記述してある、鍵種別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)

SF.PRIVILEGE

ログ設定ファイルに対して、改変を CA 管理者のみに限定していることで実現している。

FMT_SMF.1 TSF データの管理(SF. PRIVILEGE)

SF.PRIVILEGE

TSF データに対して、表 6-5 の操作を管理してい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.CAO_ACCESS_CONTROL、SF.PRIVILEGES)

SF.ACCESS_CONTROL

CA 管理者および CA 操作者および RA の許可される操作を維持することで実現している。

SF.CAO_ACCESS_CONTROL

CA 管理者および CA 操作者および監査人の許可される操作を維持すことで実現している。

SF. PRIVILEGE

CA 管理者および CA 操作者および監査人の許可される操作を維持し、CA の鍵対の管理グループを維持して操作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.AUTH 、SF.CAO_AUTH、SF.ACCESS_CONTROL、SF.CAO_ACCESS_CONTROL、SF. PRIVILEGE)

SF. AUTH

識別認証されるまで、TOE に対して CAO 端末以外の経路からのアクセス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.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.ACCESS_CONTROL

SF.ACCESS_CONTROL および SF.CAO_ACCESS_CONTROL を介さず公開鍵証明書テーブルの操作ができないことで実現している。

SF.CAO_ACCESS_CONTROL

SF.ACCESS_CONTROL および SF.CAO_ACCESS_CONTROL を介さず公開鍵証明書テーブルおよび CRL テーブル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表 6-5 の操作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。

FPT_SEP.1 TSF ドメイン分離(SF.AUTH 、SF.CAO_AUTH、SF.ACCESS_CONTROL、SF.CAO_ACCESS_CONTROL、SF. PRIVILEGE)

SF. AUTH

SF. AUTH は、干渉と改ざんから守られていることで実現している。

SF.CAO_AUTH

SF.CAO_AUTH は、干渉と改ざんから守られていることで実現している。

SF. ACCESS_CONTROL

SF. ACCESS_CONTROL は、干渉と改ざんから守られていることで実現している。

SF.CAO_ACCESS_CONTROL

SF.CAO_ACCESS_CONTROL は、干渉と改ざんから守られていることで実現している。

SF. PRIVILEGE

SF. PRIVILEGE は、干渉と改ざんから守られていることで実現している。

FPT_STM.1 高信頼タイムスタンプ(SF.AUDIT)

SF.AUDIT

ログを生成するための日付・時刻を提供することによって実現している。

8.3.2 機能強度(SOF)主張根拠

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。機能強度は 6.2 節では「SOF-基本」と宣言している。一方、5.3 節において「SOF-基本」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。

8.3.3 保証手段根拠

表 6-8 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主張根拠

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	Certificate 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。
DN	Distinguished Name の略。 ディレクトリ・ツリー上でエントリを一意に識別するための名前である。
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。 利用者を認証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。
クラス	公開鍵証明書の発行および失効などの権限を記述したもの。そのクラスに属する DN は、そのクラスに記述され権限を実行できる。
公開鍵証明書	X.509v3 で定義された公開鍵を含む証明書。
セキュアルーム	許可された人のみが入退できる物理的制限を設けかつ入退記録を残せる部屋
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

＜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*

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

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

＜LDAPv3＞ Lightweight Directory Access Protocol, *RFC2251*

＜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.*

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

＜RFC3280＞ *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002*

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

＜ FIPS140-2 ＞ *NIST FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 25 May, 2001*

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

1999

＜RFC2251＞ *Internet X.509 Certificate Request Message Format, March 1999*

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