PKI サーバ／Carassuit 電子政府版 ver3.1
セキュリティターゲット

バージョン：1.13

発行日： 2007 年 2 月 7 日

作成者：日本電気株式会社

目次

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合の主張について記述する。

1.1. ST 識別

タイトル：PKI サーバ／Carassuit 電子政府版 ver3.1 セキュリティターゲット
バージョン：1.13
発行日：2007 年 2 月 7 日
作成者：日本電気株式会社
TOE：PKI サーバ／Carassuit 電子政府版 ver3.1
TOE のバージョン：3.1
キーワード：PKI、公開鍵基盤、CA、認証局、RA、登録局
CC のバージョン：Common Criteria for Information Technology Security Evaluation Ver2.3
補足-0512 適用

1.2. ST 概要

このドキュメントは PKI サーバ／Carassuit 電子政府版 ver3.1 と呼ばれる PKI（公開鍵基盤）ソフトウェア製品のセキュリティターゲットである。 PKI サーバ／Carassuit 電子政府版 ver3.1 は次の機能を提供する。

[CA（認証局）機能]

- 一般利用者（EE）の公開鍵に対して電子署名し、公開鍵証明書を発行する（申請者が公開鍵に対応した秘密鍵を持つことを保証する）。
- 発行した公開鍵証明書を検証するために CA 自身の公開鍵証明書を公開する。
- 失効リスト（CRL、ARL）を発行する。
- 機関証明書を発行する。 機関証明書には、下位 CA 証明書と相互認証証明書との二種類がある。
- 公開鍵証明書をディレクトリへ保管する。

[RA（登録局）機能]

- 証明書申請要求を受け付ける。
- 証明書発行・失効などの資格審査をする。

1.3. CC 適合の主張

この ST は以下の CC に適合している。
・CC パート２適合
・CC パート３適合
評価保証レベルは EAL３である。
この ST が適合している PP はない。

2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE 範囲、TOE 関連の利用者役割について記述する。

2.1. TOE 種別

TOE は、「PKI サーバ／Carassuit 電子政府版 ver3.1」というソフトウェア製品である。
「PKI サーバ／Carassuit 電子政府版 ver3.1」は、公開鍵基盤（PKI）における認証局（CA）機能および登録局 （RA）機能を提供するものである。

2.2. TOE 概要

PKI サーバ／Carassuit 電子政府版 ver3.1 は公開鍵証明書、失効リスト（CRL、ARL）を生成、発行し、LDAP ディレクトリで公開する。
PKIサーバ／Carassuit 電子政府版 ver3.1で提供される機能は大別すると以下のサービスに分類される。
1）メインサービス
CA（認証局）メイン機能、RA（登録局）メイン機能
2）他のサービス
監査機能、バックアップ／リカバリ機能、アーカイブ機能、アクセスコントロール（操作員管理）機能、ユーザ管理機能、ポリシー管理機能、スケジュール管理機能、システム環境設定機能

2.2.1. TOE によって提供されるメインサービス

（1） CA メイン機能

- 一般利用者（EE）の公開鍵に対して電子署名し、公開鍵証明書を発行する（申請者が公開鍵に対応した秘密鍵を持つことを保証する）。
- 発行した公開鍵証明書を検証するために CA 自身の公開鍵証明書を公開する。
- 失効リスト（CRL、ARL）を発行する。
- 機関証明書を発行する。 機関証明書には、下位 CA 証明書と相互認証証明書との二種類がある。
- 公開鍵証明書をディレクトリへ保管する。

（2） RA メイン機能

- 証明書申請要求を受け付ける。
- 証明書発行・失効などの資格審査を行う。

2.2.2. TOE によって提供されるほかのサービス

（1） 監査データ管理機能

TOE がセキュアに運用されていることを監査するために必要な情報の採取、および管理を行う。

（2）バックアップ／リカバリ機能

TOE の障害に備えて、システムの復旧に必要なデータのバックアップを行う。障害が発生した場合には、バックアップをリストアすることにより TOE を復旧する。バックアップにおいては、DB のイメージコピーが作成されるので、バックアップ媒体中のデータの完全性・機密性は DB 内のデータと同等である。

（3）アーカイブ機能

TOE が発行した証明書、鍵等の履歴を管理する。

（4）アクセスコントロール（操作員管理）機能

あらかじめ定められた TOE の運用に関する役割とセキュリティ要件に基づき、TOE へのアクセスを操作員 ID、証明書等を用いて制御する。制御情報として、上級操作員及び一般操作員の登録・削除・情報管理、および権限グループの管理を行う機能を提供する。

（5）ユーザ管理機能

EE の秘密鍵および個人情報を管理する。 必要に応じて EE 鍵の鍵ペア生成、鍵保管を行う。 EE の IC カードへ鍵・証明書を格納する形式のファイルを生成する機能を提供する。

（6）ポリシー管理機能

証明書プロファイルおよび証明書失効リストプロファイルの設定と変更を行う。

（7）スケジュール管理機能

TOE をあらかじめ定めたスケジュールで運用する。本バージョンでは、証明書失効リスト（CRL）、機関失効リスト（ARL）のスケジュール機能を提供する。

（8）システム環境設定機能

TOE の運用に必要な情報を設定する。

2.3. TOE 範囲

2.3.1. ハードウェア・ソフトウェアコンポーネント

TOE を含むハードウェア・ソフトウェアコンポーネント構成を図 2-1に示す。

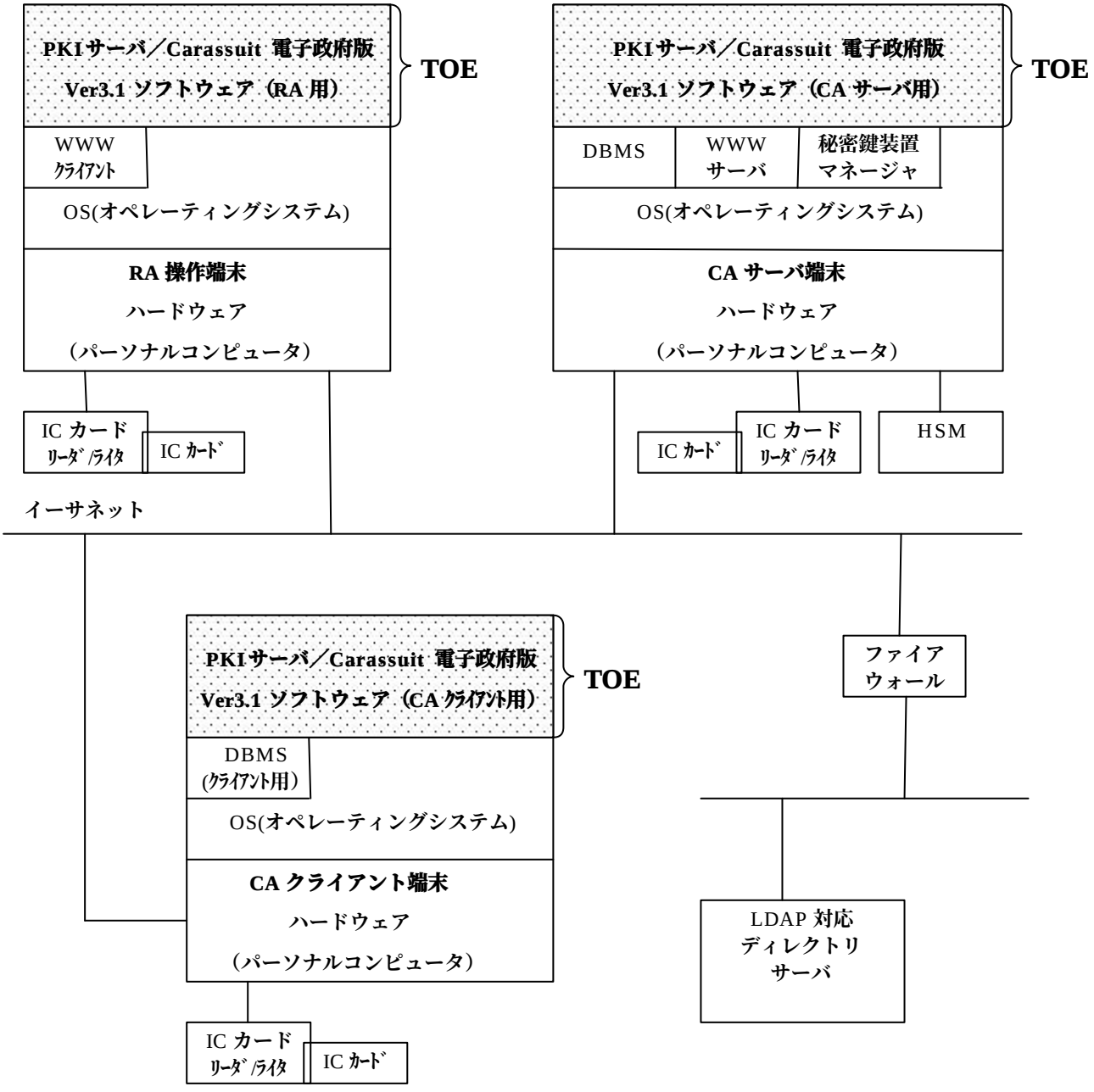

図 2-1 PKI サーバ／Carassuit 電子政府版 ver 3.1 アーキテクチャ

図 2-1に示すように、**TOE は、PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェア (CA サーバ用、CA クライアント用、RA 用)である**。PKI サーバ／Carassuit 電子政府版 ver3.1 は複数のハードウェア・ソフトウェアコンポーネントを利用するが、**PKI サーバ／**

Carassuit 電子政府版 ver3.1 ソフトウェア(CA サーバ用、CA クライアント用、RA 用)以外のハードウェア・ソフトウェアは TOE 外である。

以下に、PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェアを動作させるために必要なハードウェア・ソフトウェアコンポーネントについて説明する。最初にハードウェアについて記述する。

- **CA サーバ端末ハードウェア：**CA サービスが稼動するパーソナルコンピュータ。
- **HSM（Hardware Security Module）：**認証局秘密鍵を生成・管理するハードウェア装置で、FIPS PUB 140-1 または 140-2 レベル 3 またはレベル 3 相当である。 CA サーバ端末に接続される。秘密鍵へのアクセスは、秘密鍵装置マネージャから HSM へ処理を依頼し、HSM 内で秘密鍵を使用し、結果を秘密鍵装置マネージャへ返却する方式であり、HSM 自身のバックアップ操作以外で秘密鍵が HSM の外に出ることはない。また、耐タンパ性があり、解体などの物理的な不正操作を検知すると、HSM 内の秘密鍵を消去することによって、秘密鍵の暴露を防止する。
- **CA クライアント端末ハードウェア：**CA サービスに接続するパーソナルコンピュータ。
- **RA 操作端末ハードウェア：**RA 操作を実行するためのパーソナルコンピュータ。
- **IC カードリーダ／ライタ：**IC カードをリード／ライトするハードウェア装置。上記の各端末に接続される。
- **IC カード：**一般操作員の操作員証明書および秘密鍵を保持するハードウェア。IC カードリーダ／ライタ経由でアクセスする。IC カードに格納された操作員証明書および秘密鍵にアクセスするには、PIN による認証が必要である。IC カードは一般操作員の識別・認証用に用いられる。また、EE 用に EE 証明書および秘密鍵の保持にも使用される。この場合、一般操作員用のカード以外のものを用いる。
- **ファイアウォール：**CA サーバ端末・CA クライアント端末・RA 操作端末のつながっているネットワークとそれら以外の端末（外部端末）のつながっているネットワークを分離し、外部端末からの不正侵入を防止するハードウェア装置。

各端末の周辺機器（HSM、IC カードリーダ／ライタ）は、それぞれの端末付近に設置され、各端末と RS-232C ケーブル、SCSI ケーブルまたは USB ケーブルで直接接続される。
各端末はイーサネットケーブルで接続されている。また、上記以外に、証明書を蓄積・公開する LDAP 対応ディレクトリサーバがファイアウォールの外側に接続されている。その他のハードウェアとして、バックアップするデータを保存するバックアップ媒体がある。バックアップ媒体として、CD-R、MO などのリムーバブル媒体や TOE がインストールされた CA サーバ端末のハードディスクを利用する。

次に、PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェア、およびそのソフトウェアが利用するソフトウェアを説明する。

<CA サーバ端末>

- **PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェア（CA サーバ用）：**TOE であり、CA サーバ用の複数のアプリケーション。これらのアプリケーションの有する機能については後述する。
- **DBMS：**データベース管理システム。TOE データ(後述)を管理する。
- **WWW サーバ：**RA 操作端末の要求に応じる。
- **秘密鍵装置マネージャ：**HSM への低レベルアクセスインタフェースを提供する。
- **OS(オペレーティングシステム)：**上記のソフトウェアを動作させるための基盤となるソフトウェア。

<CA クライアント端末>

- **PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェア（CA クライアント用）：**TOE であり、CA クライアント用の複数のアプリケーション。これらのアプリケーションの有する機能については後述する。
- **DBMS(クライアント用)：**データベース管理システム。CA サーバ端末に保存された TOE データ(後述)にアクセスする手段を提供する。
- **OS(オペレーティングシステム)：**上記ソフトウェアを動作させるための基盤となるソフトウェア。

<RA 操作端末>

- **PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェア（RA 用）：**TOE であり、RA 用の複数のアプリケーション。これらのアプリケーションの有する機能については後述する。
- **WWW クライアント：**リモートで RA 操作を行うために用いる。
- **OS(オペレーティングシステム)：**上記ソフトウェアを動作させるための基盤となるソフトウェア。

上記の OS および DBMS は、識別認証機能、アクセス制御機能を有している。
TOE データとは、3.1 節 資産で説明する TOE の利用者データおよび TSF データである。本章で以降登場する TOE のデータも同様である。

次に、上記のハードウェア・ソフトウェアコンポーネントで、PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェア、秘密鍵装置マネージャ以外の製品名・仕様について示す。

ソフトウェア

<CA サーバ端末>

- **OS(オペレーティングシステム)：** Windows 2000 Server or Windows Server 2003
- **WWW サーバ：** Internet Information Service 5 or Internet Information Service 6
- **DBMS：**Oracle10g Release2 の Enterprise Edition 及び Oracle Advanced Security

<CA クライアント端末>

- **OS(オペレーティングシステム)：** Windows 2000 or Windows XP or Windows Server 2003
- **DBMS（クライアント用）：**Oracle10g Release2 の Enterprise Edition 及び Oracle Advanced Security（必要な製品コンポーネントは Oracle Database 10g と Oracle Net Services のみ）

<RA 操作端末>

- **OS(オペレーティングシステム)：** Windows 2000 or Windows XP or Windows Server 2003
- **WWW クライアント：**Microsoft Internet Explorer 6.0

ハードウェア

<CA サーバ端末>

- **本体：** Express5800 シリーズ
- **CPU：** PentiumⅢ 1GHz 以上
- **メモリー：**512MB 以上
- ハードディスク：2GB 以上

<CA クライアント端末>

- **本体：** Express5800 シリーズ、PC／AT 互換機
- **CPU：** PentiumⅢ 1GHz 以上
- **メモリー：**512MB 以上
- ハードディスク：2GB 以上

<RA 操作端末>

- **本体：** Express5800 シリーズ、PC／AT 互換機
- **CPU：** PentiumⅢ 1GHz 以上
- **メモリー：**256MB 以上（512MB 以上推奨）

<IC カードリーダ／ライタ>

- Gemplus 社製 GemPC410 (RS-232C 接続タイプ)、GemPCTwin(RS-232C 接続タイプまたは USB 接続タイプ)、NEC 製 CK1505-02(USB 接続タイプ)、または CK1506-02(USB 接続タイプ)

<IC カード>

- 大日本印刷社製 Standard-9 (NEC SecureWare 用 STD-9)

<HSM>

- NEC 製 CK-GuardⅡ、CK-GuardⅢまたは SafeNet 社製 Luna CA^3、Luna SA

2.3.2. TOE 機能

TOE およびその IT 環境が提供する機能を図 2-2に示す。各端末の太線で囲まれている機能が TOE 範囲内であり、PKI サーバ／Carassuit 電子政府版 ver3.1 ソフトウェア（CA サーバ用、CA クライアント用、RA 用）が提供する機能である。

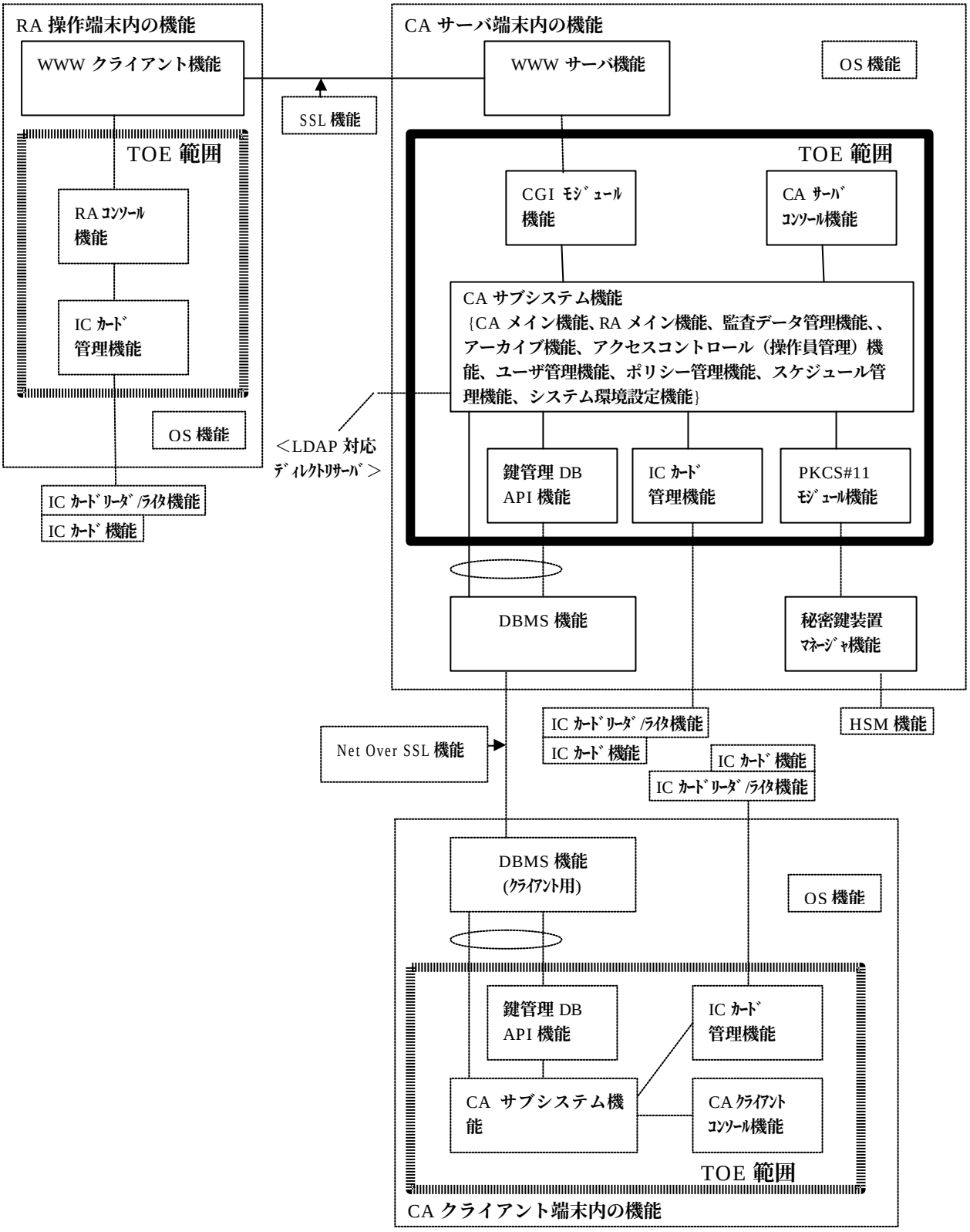

図 2-2 TOEとその IT 環境が提供する機能

図 2-2において、**TOE 範囲内**にある機能について端末ごとに説明する。

<CA サーバ端末>

CA サーバコンソール機能：PKI サーバ／Carassuit 電子政府版 ver3.1 を管理するために使われる GUI（グラフィカルユーザインタフェース）から構成される。システム管理 GUI、CA セットアップツール、CA 鍵・証明書更新ツール、自己署名証明書失効ツール、データベースセットアップツール、データベースパスワード変更ツール、バックアップツール、リカバリツール、ユーザ管理ツール、サービス監視ツール、CA サービス起動停止ツールがある。

システム管理 GUI: CA メイン機能、監査データ管理機能、アーカイブ機能、アクセスコントロール機能、ポリシー管理機能、スケジュール管理機能、システム環境設定機能についての GUI を提供する。

CA セットアップツール: 新規の認証局をセットアップする。認証局のセットアップでは、初期操作員（上級操作員二名および一般操作員一名）の登録や CA 証明書の発行などが行われる。

CA 鍵・証明書更新ツール: 認証局の秘密鍵および CA 証明書を更新する。

自己署名証明書失効ツール: 認証局の CA 証明書を失効する。これ以降、認証局は新たな証明書の発行や、証明書の失効などの操作が行えなくなる。

データベースセットアップツール: 認証局からアクセスする各種データベースを作成する。このツールは新たな認証局を構築する際に、CA セットアップに先立って実行される。

データベースパスワード変更ツール: 認証局からアクセスする各種データベースのパスワードを変更する。

バックアップツール: 認証局のセットアップ情報および各種データベース内のデータをバックアップする。

リカバリツール: バックアップツールによってバックアップしたデータを復元し、認証局を再構成する。

ユーザ管理ツール: ユーザ管理機能についての GUI を提供する。

サービス監視ツール: CA メイン機能が正常に動作しているかどうかを監視する。

CA サービス起動停止ツール：CA サービスを起動及び停止する GUI を提供する。

CA サブシステム機能：CA サービスを提供する以下の機能から構成される。

CA メイン機能、RA メイン機能、監査データ管理機能、アーカイブ機能、アクセスコントロール（操作員管理）機能、ユーザ管理機能、ポリシー管理機能、スケジュール管理機能、システム環境設定機能。また、これらの機能のほとんどは、TOE データが保存されたデータベースに直接アクセスする。

CGI モジュール機能：CA サブシステム機能を呼び出して、EE 証明書の申請、審査、検索、出力、失効などを行う。

鍵管理 DB-API 機能：CA サブシステム機能からの鍵アクセス要求に基づいて、鍵に関する TOE データを保存するデータベースへアクセスする。

IC カード管理機能：IC カードへのリード・ライトを管理する。

PKCS#11 モジュール機能：CA サブシステム機能からの PKCS#11 インタフェースによる HSM アクセス要求に基づいて、秘密鍵装置マネージャにアクセスする。

<CA クライアント端末>

CA クライアントコンソール機能：PKI サーバ／Carassuit 電子政府版 ver3.1 を管理するために使われる GUI（グラフィカルユーザインタフェース）。CA サーバ端末の GUI とは若干異なり、機能が制限されており、システム管理 GUI、データベースパスワード変更ツール、ユーザ管理ツール、サービス監視ツールから構成される。

システム管理 GUI: CA メイン機能、監査データ管理機能、アーカイブ機能、アクセスコントロール（操作員管理）機能、ポリシー管理機能、スケジュール管理機能、システム環境設定機能についての GUI を提供する。

データベースパスワード変更ツール: 認証局からアクセスする各種データベースのパスワードを変更する。

ユーザ管理ツール: ユーザ管理機能についての GUI を提供する。

サービス監視ツール: CA サーバ上の CA メイン機能が正常に動作しているかどうかを監視する。

CA サブシステム機能：上記の CA サーバ端末の CA サブシステム機能とまったく同じものである。これらの機能は、CA サーバ端末のデータベースに直接アクセスする。

鍵管理 DB-API 機能：CA サブシステム機能からの鍵アクセス要求に基づいて、鍵に関する TOE データを保存するデータベースへアクセスする。

IC カード管理機能：IC カードへのリード・ライトを管理する。

<RA 操作端末>

RA コンソール機能：リモートで EE 証明書申請要求を登録する。証明書受取、証明書検索、証明書生成要求、IC カードへの書込要求を行う。

IC カード管理機能：IC カードへのリード・ライトを管理する。

なお、3.1節 資産で説明する TOE の利用者データ及び TSF データは、DBMS を使ってデータベースに保存されているが、それらのデータ自身は TOE 保護対象資産である。
DBMS は、OS と同じように TOE の下位で動作するもので、DBMS 内にある TOE のデータには、TOE 以外のプロセスがアクセスすることはない。

次に、TOE の外部インタフェースおよび TOE の保護対象資産の利用と保管について説明する。

1) CA サーバ端末の CA サブシステム機能・鍵管理 DB API 機能－DBMS 機能間、CA クライアント端末の CA サブシステム機能・鍵管理 DB API 機能－DBMS(クライアント用)機能間

この間は 3.1 資産で挙げたすべての利用者データ、TSF データが受け渡される。TOE（CA サーバ端末の CA サブシステム機能・鍵管理 DB API 機能 CA クライアント端末の CA サブシステム機能・鍵管理 DB API 機能）が Oracle の提供する API を呼び出すことによりデータの受け渡しを行う。

2) CA サーバ端末の WWW サーバ機能－CGI モジュール機能間

CGI モジュール機能は、WWW サーバ機能の CGI 機能を基盤として利用している。この間は RA 操作員の識別・認証データ（ユーザ ID、パスワード、チャレンジ、証明書)、EE IC カード発行情報が受け渡される。この間のデータ受け渡しは OS によって保護される。

3) RA 操作端末の WWW クライアント機能－RA コンソール機能間

RA コンソール機能は、WWW クライアント機能を基盤として利用している。WWW クライアント機能が RA コンソール機能の GUI を提供し、CA サーバ端末の CGI モジュールによって生成された RA 操作画面を表示する。この間は RA 操作員の識別・認証データ（ユーザ ID、パスワード、チャレンジ、証明書)、EE IC カード発行情報が受け渡される。この間のデータ受け渡しは OS によって保護される。

4) CA サーバ端末の PKCS#11 モジュール機能－秘密鍵装置マネージャ機能間

この間では、CA 鍵による署名を要求するデータと署名値とが送受信される。 この間の通信はプロセス間通信であり、OS によって保護される。

5) CA サーバ端末の IC カード管理機能－IC カード機能間

この間では、一般操作員の IC カード発行情報が送受信される。

6) CA クライアント端末の IC カード管理機能－IC カード機能間

この間では、一般操作員の識別・認証データ（PIN、チャレンジ、証明書)、一般操作員の IC カード発行情報、EE IC カード発行情報が送受信される。

7) RA 操作端末の IC カード管理機能－IC カード機能間

この間では、一般操作員の識別・認証データ（PIN、チャレンジ、証明書)、EE IC カード発行情報が送受信される。

なお、5),6),7)の各端末の IC カード管理機能－IC カード機能間は、盗聴されないことを前提とする。

次に、**TOE 範囲内**にある上記各機能で実現される**セキュリティ機能**について端末ごとに説明する。

<CA サーバ端末、CA クライアント端末>

・監査機能

セキュリティ関連事象の監査記録生成、監査ログ検査者による監査レビュー、監査記録保護。

・アクセス制御機能

上級操作員および一般操作員の種別によるアクセス制御、上級操作員および一般操作員の権限による操作制限。

・識別認証機能

上級操作員および一般操作員による ID／パスワード認証、一般操作員による IC カード認証、複数認証メカニズムのサポート、パスワード・PIN の品質の検証、アカウントロック。

・暗号機能

TOE の資産の署名・署名検証、暗号化・復号、ダイジェスト生成。

・証明書発行

証明書・失効リストに対する発信元証拠生成、EE 鍵の有効性証拠生成。

<RA 操作端末>

・識別認証機能

一般操作員による ID／パスワード認証、一般操作員による IC カード認証、パスワード・PIN の品質の検証。

2.3.3. TOE 範囲外の機能

図 2-2において、**TOE 範囲外**にある機能について説明する。

○端末

<CA サーバ端末>

秘密鍵装置マネージャ機能：HSM への低レベルアクセスインタフェースを提供する。

WWW サーバ機能：RA 操作端末からの要求を処理する。

DBMS 機能：TOE データを管理する。

OS 機能：TOE 及びその環境のソフトウェアを動作させるための基盤となる機能。

<CA クライアント端末>

DBMS(クライアント用)機能：CA サーバ端末に保存された TOE データにアクセスする手段を提供する。

OS 機能：TOE 及びその環境のソフトウェアを動作させるための基盤となる機能。

<RA 操作端末>

WWW クライアント機能：RA コンソール機能を利用するために必要な WEB ユーザインタフェースを提供する。

OS 機能：TOE 及びその環境のソフトウェアを動作させるための基盤となる機能。

○その他ハードウェア

HSM 機能：認証局秘密鍵を生成・管理する機能。耐タンパ機能。

IC カードリーダ／ライタ機能：IC カードをリード・ライトする。

IC カード機能：一般操作員の PIN 認証を行う。

○通信パス

Net Over SSL 機能：DBMS(Oracle)が提供する機能で、以下の通信パスを暗号化する。

・CA サーバの DBMS 機能と CA クライアントの DBMS(クライアント用)機能の間

SSL 機能：WWW サーバと WWW クライアントの間の通信を暗号化する。

次に、**TOE 範囲外**にある上記各機能で実現されるセキュリティ機能について説明する。

＜IC カード＞

認証機能（PIN 認証）

＜HSM＞

暗号機能（認証局秘密鍵の生成など）、物理的保護機能

＜OS＞

識別認証機能、アクセス制御機能

＜DBMS・DBMS(クライアント用)＞

識別認証機能、アクセス制御機能、高信頼チャネル機能(Net Over SSL)

＜WWW サーバ・WWW クライアント＞

高信頼チャネル機能(SSL)

2.4. TOE 関連の利用者役割

PKIサーバ／Carassuit 電子政府版 ver3.1で使用される各端末における利用者の役割は以下のとおりである。上級操作員および一般操作員（RA 操作員を含む）は権限グループに所属し、所属する権限グループに付与されたアクセス権限の範囲の業務を行うことができる。なお、TOE は、上級操作員、一般操作員が TOE にログイン後、各権限グループに所属する上級操作員プロセス、一般操作員プロセスを生成する。これらのプロセスは権限グループに付与されたアクセス権限の範囲の動作を行う。利用者データである機関証明書、EE 証明書、ARL、CRL、EE IC カード発行情報はファイルオブジェクトとして扱われ、利用者データに関するアクセス制御の対象となる。

<CA サーバ端末>

（1）上級操作員

認証局秘密鍵管理者（後述）の指示の下に、認証局秘密鍵を用いた業務を行う。CA サーバに直接ログインして次の業務を行う権限を有する。

- CA メイン機能の起動／停止
- CA 鍵管理
- バックアップ／リカバリ
- 操作員管理

上級操作員の認証は、操作員 ID 及びパスワードによって行われる。

CA サーバのデータベースとは証明書及びその発行、失効などの履歴からなるデータベースをいう。

<CA クライアント端末>

（2）一般操作員

遠隔より認証局を操作する権限を与えられた操作員である。各一般操作員にどの権限を与えるかは、操作員登録において上級操作員によって決定される。権限によっては複数人の一般操作員の関与によって行われることを指定できる。一般操作員は登録時に操作にあたって行われる識別認証の方式が決定される。 識別認証の方式には、操作員 ID とパスワードを用いる方式と IC カードを用いる方式とがある。 IC カードを用いる方式では、当該一般操作員に対して公開鍵証明書が発行され、IC カード内に格納される。

TOE では、以下の権限が存在する。権限は、任意の権限グループにまとめることができる。

- ARL 出力
- CRL 出力
- アーカイブ管理
- アーカイブ参照

- システム環境設定
- スケジュール管理
- ポリシー管理
- 監査ログ参照
- 監査管理
- 操作員管理（一般操作員の登録、削除など）
- ユーザ管理
- 証明書情報参照
- 機関証明書申請
- 機関証明書取得
- 機関証明書失効
- EE 証明書申請
- EE 証明書審査
- EE 証明書取得
- EE 証明書失効
- EE IC カード発行

なお、ユーザ管理、EE 証明書申請、EE 証明書審査、EE 証明書取得、EE 証明書失効、EE IC カード発行を除く権限は、上級操作員にも割り当てることが可能である。

（3）監査ログ検査者

CA サーバが生成する監査データを検査する作業者である。監査ログ検査者は、上記の権限のうち「監査ログ参照」および「監査管理」の権限が付与された上級操作員もしくは一般操作員である。監査ログ検査者は他の権限を割り当てられない。

<RA 操作端末>

（4）RA 操作員

CA サーバに対して証明書申請要求、証明書申請要求の審査、証明書受取、証明書検索、証明書生成要求、証明書の IC カードへの書込などの RA 業務を行う作業者である。
RA 操作員は、システム上は一般操作員である。

<その他 >

（5）認証局秘密鍵管理者

認証局秘密鍵管理者は、認証局鍵の生成、バックアップ、バックアップからのリストアなど、認証局秘密鍵を使用した業務に関する責任者である。 認証局秘密鍵管理者は次の業務に携わる。なお、認証局秘密鍵は分散保管し、その操作は複数人によるものとする。

- 認証局鍵ペアの生成

- 認証局秘密鍵のバックアップ
- 認証局秘密鍵バックアップからのリストア

認証局鍵管理者には、認証局運用規定（CPS）において責任ある者が任命されるものとする。 これらの操作は HSM 上で行い、認証局秘密鍵管理者は TOE にアクセスしない。

（6）EE 証明書利用者（一般利用者）

EE 証明書利用者（一般利用者）は、一般操作員により EE 証明書を発行される。 EE 証明書の配付は、

- IC カードに格納した EE 秘密鍵および証明書
- PKCS#12 形式の EE 秘密鍵および証明書

があるが、配付は TOE の範囲外である。 EE 証明書利用者は、発行された EE 証明書を使用することができる。LDAP 対応ディレクトリサーバにある証明書にアクセスすることができる。ファイアウォールを設置しているため、EE 証明書利用者が TOE に直接アクセスすることはできない。

3. TOEセキュリティ環境

本章では、資産、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 資産

本 TOE の資産は利用者データ、TSF データである。
利用者データには、以下のようなデータがある。
・機関証明書
・EE 証明書
・EE 秘密鍵
・失効リスト（CRL、ARL）
・EE IC カード発行情報
TSF データには、以下のようなデータがある。
・操作員証明書
・識別・認証情報
・アクセスコントロール情報
・監査ログ
・アーカイブログ
・その他のシステム設定情報（システム環境設定、スケジュール設定など）
・暗号化用鍵（システム共通鍵、データベース共通鍵）
これらの資産は TOE による保護対象となる。
TOE による保護対象外のデータとしては、TOE プログラム（2.3.1 TOE 境界内で指定した機能のソフトウェアコンポーネント）、HSM のデータ（認証局秘密鍵（CA 鍵））、IC カードのデータ（操作員証明書、操作員秘密鍵）、バックアップデータ（上記利用者データ、上記 TSF データ、レジストリ情報でバックアップ媒体に保存される）がある。

以降、特に断りのない限り、利用者データ、TSF データ、TOE プログラム、IC カードのデータ、バックアップデータは上記で記述した内容を指すものとする。

3.2. 前提条件

3.2.1. TOE の意図する使用方法

A.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）
上級操作員および一般操作員が TOE にアクセスするために用いるパスワードは、他人に知られないように本人によって管理される。パスワードは推測・解析されにくいものが設定され、適正な間隔で変更される。

A.PIN_ICC_MANAGEMENT（一般操作員による PIN・IC カードの管理）
一般操作員が TOE にアクセスするために用いる IC カードは不正利用されないよう管理され、IC カード内のデータを使用するための PIN は他人に漏洩しないように本人によって管理される。PIN は推測・解析されにくいものが設定され、適正な間隔で変更される。

A.USER_RESTRICTION（利用者制限）
TOE に関連する権限・役割を持つ利用者は、管理者（上級操作員、一般操作員、監査ログ検査者、RA 操作員）のみとなるように利用者登録を行う。

3.2.2. 物理的前提

A.SAFE_PLACE（安全な場所）
TOE に関連するハードウェアは、許可された人員のみが入室できるよう制御された場所に設置される。

A.BACKUP_MEDIA（バックアップ媒体）
TOE のバックアップデータが保存されたリムーバブル媒体は、物理的に不正侵入できないように制御された場所に保管され、不正に持ち出せないように管理される。

3.2.3. 接続的前提

A.NETWORK（ネットワーク環境）
TOE の内部ネットワークはそれ以外のネットワークに直接接続されない。

A.HSM（HSM）
HSM で生成・管理される認証局秘密鍵は物理的に保護される。

A.HARDWARE（ハードウェア）
TOE に関連するハードウェアは、正確に動作する。

A.PERIPHERAL_INTERFACE（周辺装置）
TOE に接続する周辺機器は TOE の付近に設置される。TOE と周辺機器は、その間で盗聴されることがないように直接接続される。

3.3. 脅威

T.ILLEGAL_LOGON（不正なログオン）
高度な専門知識を持たない不正な利用者が、不正に TOE にログオンして TOE を利用することにより、利用者データ及び TSF データを破壊・改ざん・暴露するかもしれない。

T.UNAUTHORIZED_ACCESS（不正なアクセス）
TOE の正当な利用者が、許可されていない操作を行うことにより、利用者データ及び TSF データを破壊・改ざん・暴露するかもしれない。

T.MODIFY_DB_DATA（DB データ改ざん）
高度な専門知識を持たない不正な利用者が、利用者データおよび TSF データが保存されたデータベースに直接アクセスすることにより、その利用者データおよび TSF データを改ざん・暴露するかもしれない。

T.DISCLOSE_ICC_FILE（EE IC カード発行情報ファイル暴露）
高度な専門知識を持たない不正な利用者が、CA クライアント端末もしくは RA 操作端末に保管された EE IC カード発行情報ファイルに直接アクセスすることにより、EE IC カード発行情報ファイルを暴露するかもしれない。

T.DISCLOSE_NW_DATA（ネットワークデータ暴露）
高度な専門知識を持たない不正な利用者が、CA サブシステムとデータベース間及び WWW サーバと WWW クライアント間のネットワーク上でやりとりされる TSF データ及び利用者データを暴露するかもしれない。

3.4. 組織のセキュリティ方針

P.ISSUE（発行）
TOE により提供される認証局（CA）は、自らが発行するすべての証明書及び失効リストが確かに当該認証局から発行されたことを要求者が確認する手段を提供しなければならない。また自らが発行するすべての証明書及び失効リストの発行履歴を管理しなければならない。

P.AUTHORITY（権限付与）
利用者は、運用上必要な最小限の権限のみを与えられるものとする。

P.AUDITOR（監査ログ検査者）
監査ログ検査者は他の権限を持てない。

P.CA_PRIVATE_KEY（認証局秘密鍵）
TOE によって使われる認証局秘密鍵は、FIPS PUB 140-1 または 140-2、PKCS に従って生成・破棄・操作されるものとする。

P.OS_DB（信頼できる OS／DB）
TOE を動作させるために必要となる OS および DB は、識別認証機能を適切に実施できるもの、さらに OS は信頼できない利用者による干渉と改ざんから TOE を保護するためのセキュリティドメインを維持できるものを利用しなければならない。また OS は信頼できるタイムスタンプ情報を提供しなければならない。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境セキュリティ対策方針について記述する。

4.1. TOE セキュリティ対策方針

O.I&A（識別認証）
TOE は、利用者が TOE を利用する前に識別認証されることを保証する。

O.ACCESS_CONTROL（アクセスコントロール）
TOE は、権限のある利用者のみが TOE 及びそのリソースにアクセスを得ることを保証する。利用者またはプロセスは、対象となるリソースに対する権限を設定され、アクセスが制限される。TOE は、セキュリティ関連の役割と、利用者の関連を維持する。

O.AUDIT（監査）
TOE は、特定の事象が発生した場合これを監査記録として保管する。監査記録は、事象の日付・時刻、事象個所、および事象に責任を持つ主体を含む。監査記録によって、利用者の TOE 誤用を発見し、異常なユーザ動作を検出する。TOE は、これらの制御を回避することを試みるユーザを特定できる。ユーザ動作は監査事象として記録される。
TOE は、監査事象を保証するために監査記録に対する、権限のないアクセス、改ざん、または削除を防ぐ。

O.DATA_INTEGRITY（データの完全性）
TOE は、TSF データ（識別・認証情報、アクセスコントロール情報、その他のシステム設定情報）を TOE の IT 環境であるデータベースに格納する際にそれぞれのダイジェストを作成して添付する。 TOE は、データベースからそれらの TSF データを取得する際にダイジェストを再作成して添付されているダイジェストと比較し、当該 TSF データの完全性を確認する。

O.CRYPTOGRAPHY（暗号）
TOE は、利用者データ（EE 秘密鍵）および TSF データ（操作員証明書を除く）を暗号化してデータベースに格納する。TOE は、EE IC カード発行情報ファイルを暗号化する。TOE は、操作員証明書を用いる一般操作員識別・認証時に操作員証明書の署名検証を行う。TOE は、TSF データを TOE の IT 環境であるデータベースに格納する際にハッシュ値を添付し、当該データをデータベースから取得する際にハッシュ値の一致チェックを行う。

O.ISSUE_CONFIRMATION（発行確証）

すべての証明書および失効リストには、認証局秘密鍵(CA 鍵)による署名がされており、発行された証明書や失効リストが確かに本認証局から発行されたということを検証する手段を提供する。また自らが発行するすべての証明書及び失効リストの発行履歴を管理する。

4.2. 環境セキュリティ対策方針

4.2.1. IT 環境のセキュリティ対策方針

OE.ICC_PROTECTION（IC カードの保護）
一般操作員が TOE のアクセスに用いる IC カードは PIN によって保護されなければならない。また、IC カードの PIN 認証は TOE の一般操作員の識別認証プロセスの一部として利用される。

OE.CA_PRIVATE_KEY（認証局秘密鍵）
TOE によって使われる認証局秘密鍵は、HSM により FIPS PUB 140-1 または 140-2、PKCS に従って生成・破棄・操作されなければならない。

OE.TRUSTED_PATH（高信頼チャネル）
CA サブシステム－データベース間、および WWW サーバ－WWW クライアント間のネットワークは高信頼チャネルを用いなければならない。

OE.TRUSTED_OS_DB（信頼できる OS／DB）
TOE を動作させるオペレーティングシステムと TOE が使用するデータベースは、その利用者に対して適切な識別認証を行う機能を保証し、信頼できない利用者による干渉と改ざんから TOE 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。オペレーティングシステムは信頼できるタイムスタンプ情報を提供しなければならない。

4.2.2. Non-IT 環境のセキュリティ対策方針

OEN.AUTHORIZATION_SETTING（権限の設定）
TOE に関連する権限・役割をもつ利用者として認証局秘密鍵管理者、上級操作員、一般操作員、監査ログ検査者が任命され、それぞれが行える操作が割り当てられなければならない。監査ログ検査者は他の権限を割り当てられない。

OEN.AUTHORIZATION_DUTY（権限に関する責務）
TOE に関連する権限・役割をもつ利用者は、与えられた責務を果たし、TOE およびその環境を故意に破壊・改変してはならない。

OEN.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）
上級操作員及び一般操作員は TOE サービスを提供するシステムにアクセスするための認証情報（パスワード）を記憶し、他人に漏らしてはならない。 また推測・解析されやすい認証情報（パスワード）を設定してはならず、適正な間隔で変更しなければならない。

OEN.PIN_ICC_MANAGEMENT（一般操作員による PIN、IC カードの管理）
一般操作員は資格喪失時に IC カードを裁断して完全に破棄するなどして、IC カードが不正利用されないように管理されなければならない。また、一般操作員は IC カードにアクセスするための PIN を記憶し、他人に漏らしてはならない。 また推測・解析されやすい PIN を設定してはならず、適正な間隔で変更しなければならない。

OEN.SAFE_PLACE（安全な場所）
TOE に関連するハードウェア(CA サーバ端末とその周辺機器(IC カードリーダ／ライタ、HSM)、CA クライアント端末とその周辺機器（IC カードリーダ／ライタ)、RA 操作端末とその周辺機器（IC カードリーダ／ライタ)）は、物理的に不正侵入できないように制御された場所に設置されなければならない。

OEN.BACKUP_MEDIA（バックアップ媒体）
TOE のバックアップデータが保存されたリムーバブル媒体は、物理的に不正侵入できないように制御された場所に保管され、不正に持ち出せないように管理されなければならない。

OEN.NETWORK（ネットワーク環境）
TOE の内部ネットワーク（CA サーバ端末、CA クライアント端末および RA 操作端末などを含む内部ネットワーク）は、適切に設定されたファイアウォールにより LDAP ディレクトリサーバを含む EE 証明書利用者が利用するネットワークと隔離されており、外部ネットワークから保護されている。

OEN.HSM_PROTECTION（HSM の保護）
認証局秘密鍵の生成・管理に FIPS PUB 140-1 または 140-2 レベル 3 またはレベル 3 相当の HSM を用いることにより、認証局秘密鍵が物理的に保護されなければならない。

OEN.HARDWARE（ハードウェア）
TOE に関連するハードウェアは、正しく動作するものを使用しなければならない。

OEN.PERIPHERAL_INTERFACE（周辺装置）
TOE に接続する周辺機器は、TOE の付近に設置されなければならない。TOE と周辺機器は、その間で盗聴されることがないように短いケーブルで直接接続されなければならない。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件、IT 環境セキュリティ要件について記述する。

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

TOE が提供するセキュリティ機能の機能要件を記述する。すべての機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用する。

○セキュリティ監査（FAU）

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：最小、基本、詳細、指定なし：から一つのみ選択]レベルのすべての監査対象事象；及び
c) [割付：上記以外の個別に定義した監査対象事象]。

[選択：最小、基本、詳細、指定なし：から一つのみ選択]：指定なし

[割付：上記以外の個別に定義した監査対象事象]：以下の監査対象事象

- 操作員の識別と確認
- CA サーバコンソール機能および CA クライアントコンソール機能の起動／停止
- CA メイン機能の起動／停止
- 操作員の登録／削除／編集
- アクセス権限の設定
- ポリシーの設定
- バックアップ／リカバリの実行
- 証明書要求の発行
- 証明書の発行
- 証明書の失効
- 証明書の出力
- 証明書要求の審査
- CRL／ARL の発行
- CRL／ARL の出力
- EE IC カード発行情報ファイルの出力

・システム環境設定
・スケジュールの設定
・監査データの削除／外部出力
・アーカイブデータの削除／外部出力
・ユーザ情報の登録／削除／編集
・CA のセットアップ
・CA 鍵の変更
・CA 証明書の失効
・データベースパスワードの変更
・アクセスの拒否（操作員の識別と確認の失敗、アクセス権限のない操作の試み）

各機能要件を選択した場合に監査対象とすべきアクション（CC における規定）と、それに関連する TOE の監査対象事象を表 5-1に示す。下線は対応する監査レベルを表す。

表 5-1 監査対象とすべきアクション（CC における規定)と関連する監査対象事象

機能要件	監査対象とすべきアクション	監査対象事象
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	一部記録（後述）
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) アクセスの拒否
FAU_SAR.3a	a) 詳細: 閲覧に使用されるパラメタ。	なし（後述）
FAU_SAR.3b	a) 詳細: 閲覧に使用されるパラメタ。	なし（後述）
FAU_STG.1	なし	なし
FAU_STG.3	a) 基本: 閾値を超えたためにとられるアクション。	なし（後述）
FCO_NRO.2	a) 最小: 否認不可サービスの呼出。 b) 基本: 情報、宛先、提供された証拠のコピーの識別。 c) 詳細: 証拠の検証を要求した利用者の識別情報。	a) 証明書の発行 a) CRL／ARL の発行 a) CA のセットアップ a) CA 鍵の変更
FCS_CKM.1a	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	a) CA のセットアップ a)操作員の登録 a) EE IC カード発行情報ファイルの出力
FCS_CKM.4a	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	a) CA 鍵の変更 a) 操作員の削除
FCS_COP.1a	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) 操作員の識別と確認 a) アクセス権限の設定 a) バックアップ／リカバリの実行 a) 証明書要求の発行 a) EE IC カード発行情報ファイルの出力 a) システム環境設定 a) 監査データの外部出力 a) アーカイブデータの外部出力
FDP_ACC.1	なし	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	以下の操作についての情報 a), b), c) CA メイン機能 a), b), c) CA の鍵情報の参照機能 a), b), c)バックアップ、リカバリ機能 a), b), c)アクセスコントロール（操作員管

	キュリティ属性。	理）機能 a), b), c)ARL の外部出力機能 a), b), c) CRL の外部出力機能 a), b), c)アーカイブデータの外部出力機能 a), b), c)アーカイブデータの参照、検索機能 a), b), c)システムパラメータの設定機能 a), b), c)スケジュール管理の設定機能 a), b), c)証明書プロファイルの新規登録、 a), b), c)変更、削除機能 a), b), c)監査データの参照及び検索機能 a), b), c)監査データの外部ファイル出力、印刷機能 a), b), c)発行済みの証明書および処理中の証明書要求の一覧表示機能 a), b), c)機関証明書プロファイルでの証明書の申請機能 a), b), c)機関証明書プロファイルで発行された証明書の出力機能 a), b), c)機関証明書プロファイルで発行された証明書の失効機能 a), b), c)ユーザ管理機能 a), b), c) EE証明書プロファイルでの証明書の申請機能 a), b), c) EE証明書プロファイルで申請された証明書の審査機能 a), b), c) EE証明書プロファイルで発行された証明書の出力機能 a), b), c) EE証明書プロファイルで発行された証明書の失効機能 a), b), c) EE鍵／証明書を IC カードへ格納する形式のファイルの生成機能
FIA_AFL.1a	a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	a) 認証試行の不成功が規定回数を超えたこと及びそれに伴うアカウントのロック
FIA_ATD.1	なし	なし
FIA_SOS.1a	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	a) なし（後述） b) 操作員の登録／編集
FIA_SOS.1b	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	a) なし（後述） b) 操作員の登録／編集
FIA_SOS.1c	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	a) なし（後述） b) データベースパスワードの変更
FIA_UAU.2a	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	a), b) 操作員の識別と確認 a), b) アクセスの拒否
FIA_UAU.5	a) 最小: 認証の最終決定; b) 基本: 最終決定で共に用いられた、各々の稼動したメカニズムの結果。	a), b) 操作員の識別と確認

FIA_UID.2a	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) 操作員の識別と確認
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) 操作員の識別と確認
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) アクセス権限の設定 a) 操作員の登録／削除／編集
FMT_MTD.1a	a) 基本: TSF データの値のすべての改変。	a) 操作員の登録／削除／編集 a) CA のセットアップ
FMT_MTD.1b	a) 基本: TSF データの値のすべての改変。	a) 操作員の編集（ﾊﾟｽﾜｰﾄﾞ、PIN 変更）
FMT_MTD.1 c	a) 基本: TSF データの値のすべての改変。	a) 操作員グループの登録／削除 a) 操作員グループへのアクセス権限の割当
FMT_MTD.1d	a) 基本: TSF データの値のすべての改変。	a) システム環境設定 a) CA のセットアップ
FMT_SMF.1	a) 最小：管理機能の使用	a) 操作員の登録／削除／編集 a) アクセス権限の設定 a) システム環境設定 a) CA のセットアップ a) 監査データの削除、外部出力 a) アーカイブデータの削除、外部出力
FMT_SMR.2	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) 最小: 役割に対して与えられた条件のために成功しなかった、その役割を使用する試み; c) 詳細: 役割の権限の使用すべて。	a) 操作員の登録／削除／編集 a) 操作員グループの登録／削除 a) 操作員グループへのアクセス権限の割当 b) アクセスの拒否
FPT_RVM.1	なし	なし

注釈：（後述）となっているものに関しては、8.2.6 監査対象事象根拠において、監査対象とすべき最小レベルのアクション（CC における規定の内)、本 TOE における監査対象に含まれない根拠を説明する。

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) 各監査事象の種別に対して、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：その他の監査関連情報]

[詳細化：サブジェクト識別情報]：操作員 ID

[割付：その他の監査関連情報]：以下の監査関連情報

・順次番号。監査データ 1 件ごとに割り当てられる番号。

・メッセージ。事象の詳細な内容を表すもの。

・拡張情報。メッセージに付随するコード、具体的な対象名、ステータスなどに類する補足情報。
・ハッシュ値。監査データの改ざんチェックに使用する内部データ。

依存性： FPT_STM.1 高信頼タイムスタンプ

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：許可利用者]が、[割付：監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付：許可利用者]：監査ログ検査者
[割付：監査情報のリスト]：
・順次番号
・操作員 ID
・事象の種別
・メッセージ
・事象の結果（成功または失敗）
・事象の日付・時刻
・拡張情報
・ハッシュ値

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_SAR.3a 選択可能監査レビュー
下位階層： なし

FAU_SAR.3.1.a TSF は、[割付：論理的な関連の基準]に基づいて、監査データを[選択：検索、分類、並べ替え]する能力を提供しなければならない。

[割付：論理的な関連の基準]：以下の検索条件の任意の組み合わせ
- 操作員 ID
- 事象の種別
- 事象の日付・時刻
- 事象の結果（成功および／または失敗）

[選択：検索、分類、並べ替え]：検索

依存性： FAU_SAR.1 監査レビュー

FAU_SAR.3b 選択可能監査レビュー
下位階層： なし

FAU_SAR.3.1.b TSF は、[割付：論理的な関連の基準]に基づいて、監査データを[選択：検索、分類、並べ替え]する能力を提供しなければならない。

[割付：論理的な関連の基準]：以下の指定可能な並べ替え条件のうちの１つ
- 順次番号
- 操作員 ID
- 事象の種別
- メッセージ
- 事象の日付・時刻

・事象の結果（成功または失敗）
・拡張情報
[選択：検索、分類、並べ替え]：並べ替え

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、監査証跡内の格納された監査記録への不正な改変を[選択：防止、検出：から一つのみ選択]できねばならない。

[選択：防止、検出：から一つのみ選択]：検出

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：事前に定義された限界]を超えた場合、[割付：監査格納失敗の恐れ発生時のアクション]をとらなければならない。

[割付：事前に定義された限界]：上級操作員が CA のセットアップ時に指定した容量
[割付：監査格納失敗の恐れ発生時のアクション]：サービス停止のアクション

依存性： FAU_STG.1 保護された監査証跡格納

○通信（FCO）
FCO_NRO.2 発信の強制的証明
下位階層： FCO_NRO.1

FCO_NRO.2.1 TSF は、送信された[割付：情報種別のリスト]に対する発信元の証拠の生成を常に実施しなければならない。

[割付：情報種別のリスト]：以下の証明書及び失効リスト

- CA 証明書
- 機関証明書
- 操作員証明書
- EE 証明書
- CRL
- ARL

FCO_NRO.2.2 TSF は、情報の発信者の[割付：属性リスト]を証拠が適用される情報の[割付：情報フィールドのリスト]に関係付けることができなければならない。

[割付：属性リスト]：CA 証明書のサブジェクト名、CA 公開鍵
[割付：情報フィールドのリスト]：発行者名、CA による署名値

FCO_NRO.2.3 TSF は、[選択：発信者、受信者、[割付：第三者のリスト]]へ、[割付：発信元の証拠における制限]の範囲で、情報の発信元の証拠を検証する能力を提供しなければならない。

[選択：発信者、受信者、[割付：第三者のリスト]]：検証者
[割付：発信元の証拠における制限]：CA 証明書の有効期間

依存性： FIA_UID.1 識別のタイミング

○暗号サポート（FCS）

FCS_CKM.1a 暗号鍵生成

下位階層： なし

FCS_CKM.1.1.a TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付：暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付：標準のリスト]：以下の標準のリスト
[割付：暗号鍵生成アルゴリズム]：以下の暗号鍵生成アルゴリズム
[割付：暗号鍵長]：以下の暗号鍵長

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
EE 鍵ペア	・ ANSI X9.31	・疑似乱数生成ア	512bit,

(RSA)	Appendix A.2.4 Using AES(注1) ・PKCS #1	ルゴリズム ・PKCS#1	768bit, 1024bit, 2048bit から選択
操作員鍵ペア (RSA)	・ANSI X9.31 Appendix A.2.4 Using AES(注1) ・PKCS #1	・疑似乱数生成アルゴリズム ・PKCS#1	512bit, 768bit, 1024bit, 2048bit から選択
システム共通鍵 (Triple DES)	ANSI X9.31 Appendix A.2.4 Using AES(注1)	疑似乱数生成アルゴリズム	168bit
データベース共通鍵 (Triple DES)	ANSI X9.31 Appendix A.2.4 Using AES(注1)	疑似乱数生成アルゴリズム	168bit
共通鍵保護鍵	なし（注２）	非公開独自方式(注２)	168bit
EE IC カード発行情報ファイル保護鍵 (Triple DES)	FIPS PUB 180-1	SHA-1 (元データをハッシュ演算で加工することで鍵としている)	168bit

（注１） これは、独立行政法人 情報処理推進機構、独立行政法人 情報通信研究機構の暗号モジュール評価基準(米国 NIST が発行する”FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE (12-03-2002)”の翻訳版)の”Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules “で承認された疑似乱数生成アルゴリズムとされているものである。

（注２） 共通鍵保護鍵は、この鍵自体を機密性を保って保存できないため、固有の元データを非公開方式で加工して使用時に毎回生成を行っている。元データ及び生成方法が非公開であることで安全性を確保するものである。

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.4a 暗号鍵破棄

下位階層： なし

FCS_CKM.4.1.a TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵破棄方法[割付：暗号鍵破棄方法]に従って、暗号鍵を破棄しなければならない。

[割付：標準のリスト]：なし
[割付：暗号鍵破棄方法]：耐タンパ性のない格納領域に保管されている暗号鍵は、ダミーデータ（乱数やゼロデータなどの実質的な意味のないデータ）で上書きしてから削除する

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
FDP_ITC.2 セキュリティ属性付き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.1a 暗号操作
下位階層： なし

FCS_COP.1.1.a TSF は、[割付：標準のリスト]に合致する、特定された暗号アルゴリズム[割付：暗号アルゴリズム]と暗号鍵長[割付：暗号鍵長]に従って、[割付：暗号操作のリスト]を実行しなければならない。

[割付：標準のリスト]：以下の標準のリスト
[割付：暗号アルゴリズム]：以下の暗号アルゴリズム
[割付：暗号鍵長]：以下の暗号鍵長
[割付：暗号操作のリスト]：以下の暗号操作のリスト

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
CA 公開鍵	PKCS#1	RSA	512bit, 768bit, 1024bit, 2048bit から選択	・操作員証明書の署名検証 ・CRL の署名検証
操作員秘密鍵／公開鍵	PKCS#1	RSA	512bit, 768bit, 1024bit, 2048bit から選択	認証用のチャレンジの署名および署名検証
システム共通鍵	FIPS PUB 46-3	Triple DES	168bit	・アクセスコントロール情報の登録時の暗号化と参照時の復号 ・監査データ(1 レコードづつ)の登録時の暗号化と参照時の復号

				・アーカイブデータ(1 レコードづつ)の登録時の暗号化と参照時の復号 ・データベース用パスワードの保管時の暗号化と参照時の復号
データベース共通鍵	FIPS PUB 46-3	Triple DES	168bit	・EE 秘密鍵の保管時の暗号化と取り出し時の復号
共通鍵保護鍵	FIPS PUB 46-3	Triple DES	168bit	システム共通鍵、データベース共通鍵の保管時の暗号化と参照時の復号
EE IC カード発行情報ファイル保護鍵	FIPS PUB 46-3	Triple DES	168bit	EE IC カード発行情報ファイルの暗号化
パスフレーズから生成する共通鍵	FIPS PUB 46-3	Triple DES	168bit	・機関証明書と秘密鍵の PKCS#12 出力時の秘密鍵暗号化 ・EE 証明書と秘密鍵の PKCS#12 出力時の秘密鍵暗号化
なし	FIPS PUB 180-1	SHA-1	―	識別・認証情報のハッシュ操作 アクセスコントロール情報のハッシュ操作 システム設定情報のハッシュ操作 監査ログのハッシュ操作 アーカイブデータのハッシュ操作 注) ハッシュ操作とは、ハッシュ値生成および比較である
なし	RFC1321	MD5 (注1)	―	

(注1)MD5は電子政府推奨暗号リストに記載のないハッシュアルゴリズムであるが、用途として、他の TOE セキュリティ機能や前提条件等により改ざんのリスクを最小限に低減した上での内部的なデータの改ざん検知用であるため、アルゴリズム強度は許容範囲とみなしている。

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
FDP_ITC.2 セキュリティ属性付き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

○利用者データ保護（FDP）

FDP_ACC.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：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：アクセス制御 SFP]を実施しなければならない。

[割付：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]：アクセス制御の対象となるサブジェクトとして以下のプロセス、オブジェクトとして以下の TOE の機能、サブジェクトとオブジェクトの操作

サブジェクト	オブジェクト	操作
操作員プロセス	CA メイン機能	実行
	CA の鍵情報の参照機能	
	バックアップ、リカバリ機能	
	アクセスコントロール（操作員管理）機能	
	ユーザ管理	
	ARL の外部出力機能	
	CRL の外部出力機能	
	アーカイブデータの外部出力機能	
	アーカイブデータの参照、検索機能	
	システムパラメータの設定機能	
	スケジュール管理の設定機能	
	証明書プロファイルの新規登録、変更、削除機能	
	監査データの参照、検索機能	
	監査データの外部ファイル出力、印刷機能	
	発行済みの証明書および処理中の証明書要求の一覧表示機能	
	機関証明書プロファイルでの証明書の申請機能	
	機関証明書プロファイルで発行された証明書の出力機能	
	機関証明書プロファイルで発行された証明書の失効機能	
	EE 証明書プロファイルでの証明書の申請機能	
	EE 証明書プロファイルで申請された証明書の審査機能	
	EE 証明書プロファイルで発行された証明書の出力機能	
	EE 証明書プロファイルで発行された証明書の失効機能	
	EE 鍵／証明書を IC カードへ格納する形式のファイルの生成機能	

[割付：アクセス制御 SFP]：以下の Carassuit 電子政府版 ver3.1 アクセス制御方針

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、以下の[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付：アクセス制御 SFP]を実施しなければならない。

[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]：

サブジェクト	セキュリティ属性
操作員プロセス	・ 操作員種別 ・ 所属する権限グループ
オブジェクト	**セキュリティ属性**
CA メイン機能	なし
CA の鍵情報の参照機能	
バックアップ、リカバリ機能	
アクセスコントロール（操作員管理）機能	
ARL の外部出力機能	
CRL の外部出力機能	
アーカイブデータの外部出力機能	
アーカイブデータの参照、検索機能	
システムパラメータの設定機能	
スケジュール管理の設定機能	
証明書プロファイルの新規登録、変更、削除機能	
監査データの参照及び検索機能	
監査データの外部ファイル出力、印刷機能	
発行済みの証明書および処理中の証明書要求の一覧表示機能	
機関証明書プロファイルでの証明書の申請機能	
機関証明書プロファイルで発行された証明書の出力機能	
機関証明書プロファイルで発行された証明書の失効機能	
ユーザ管理機能	
EE 証明書プロファイルでの証明書の申請機能	
EE 証明書プロファイルで申請された証明書の審査機能	
EE 証明書プロファイルで発行された証明書の出力機能	
EE 証明書プロファイルで発行された証明書の失効機能	

EE 鍵／証明書を IC カードへ格納する形式のファイルの生成機能	

[割付：アクセス制御 SFP]：Carassuit 電子政府版 ver3.1 アクセス制御方針

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：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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

[割付：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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]：以下のアクセスを管理する規則

制御されたサブジェクト	制御されたオブジェクト	制御された操作
CA メイン機能の起動／停止のアクセス権限が付与された権限グループに所属する上級操作員プロセス	CA メイン機能	実行
CA 鍵管理のアクセス権限が付与された権限グループに所属する上級操作員プロセス	CA の鍵情報の参照機能	
バックアップ／リカバリのアクセス権限が付与された権限グループに所属する上級操作員プロセス	バックアップ、リカバリ機能	
操作員管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	アクセスコントロール（操作員管理）機能	
ARL 出力のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	ARL の外部出力機能	
CRL 出力のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	CRL の外部出力機能	
アーカイブ管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	アーカイブデータの外部出力機能	
アーカイブ参照のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	アーカイブデータの参照、検索機能	
システム環境設定のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	システムパラメータの設定機能	
スケジュール管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	スケジュール管理の設定機能	
ポリシー管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	証明書プロファイルの新規登録、変更、削除機能	
監査ログ参照のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	監査データの参照及び検索機能	
監査管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	監査データの外部ファイル出力、印刷機能	
証明書情報参照のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	発行済みの証明書および処理中の証明書要求の一覧表示機能	
機関証明書申請のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	機関証明書プロファイルでの証明書の申請機能	
機関証明書取得のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	機関証明書プロファイルで発行された証明書の出力機能	

機関証明書失効のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	機関証明書プロファイルで発行された証明書の失効機能	
ユーザ管理のアクセス権限が付与された権限グループに所属する一般操作員プロセス	ユーザ管理機能	
EE 証明書申請のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルでの証明書の申請機能	
EE 証明書審査のアクセス制限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルで申請された証明書の審査機能	
EE 証明書取得のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルで発行された証明書の出力機能	
EE 証明書失効のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルで発行された証明書の失効機能	
EE IC カード発行のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE 鍵／証明書を IC カードへ格納する形式のファイルの生成機能	

制御されたサブジェクト（上級操作員プロセス、一般操作員プロセス）は、表で対応している制御されたオブジェクトに対して、表で対応している制御された操作を行うことができる。

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：セキュリティ属性に基づいてオブジェクトのサブジェクトに対するアクセスを明示的に承認する規則]

[割付：セキュリティ属性に基づいてオブジェクトのサブジェクトに対するアクセスを明示的に承認する規則]：なし

FDP_ACF.1.4 TSF は、[割付：セキュリティ属性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拒否する規則]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。

[割付：セキュリティ属性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拒否する規則]：なし

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

○識別と認証（FIA）

FIA_AFL.1a 認証失敗時の取り扱い

下位階層： なし

FIA_AFL.1.1.a TSF は、[割付：認証事象のリスト]に関して、[選択：[割付：正の整数値], 「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」] 回の不成功認証試行が生じたときを検出しなければならない。

[割付：認証事象のリスト]：

・操作員 ID とパスワードを用いた操作員のログイン

[選択：[割付：正の整数値], 「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]：パスワード試行可能回数(3～16)(既定値(8)または運用開始後に操作員管理のアクセス権限を持つ上級操作員および／または一般操作員によって変更可能)

FIA_AFL.1.2.a 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：アクションのリスト]をしなければならない。

[割付：アクションのリスト]：

・アカウントをロックし、解除不可能にする

注釈：ロックされたアカウントを復旧する場合は、「操作員管理」のアクセス権限を有する上級操作員／一般操作員が当該アカウントを削除し、再度アカウントを作成する。

依存性： FIA_UAU.1 認証のタイミング

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：セキュリティ属性のリスト]を維持しなければならない。

[割付：セキュリティ属性のリスト]：

・操作員種別（上級操作員、一般操作員）

・所属する権限グループ

依存性： なし

FIA_SOS.1a 秘密の検証
下位階層：　なし

FIA_SOS.1.1.a TSF は、秘密が[割付：定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[詳細化：秘密]：上級操作員、および操作員 ID とパスワードを用いる一般操作員の認証パスワード
[割付：定義された品質尺度]：6 文字以上 32 文字以下の半角英数記号文字

依存性：　なし

FIA_SOS.1b 秘密の検証
下位階層：　なし

FIA_SOS.1.1.b TSF は、秘密が[割付：定義されたの品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[詳細化：秘密]：データベースにアクセスするためのパスワード
[割付：定義された品質尺度]：6 文字以上 16 文字以下の半角英数記号文字

依存性：　なし

FIA_SOS.1c 秘密の検証
下位階層：　なし

FIA_SOS.1.1.c TSF は、秘密が[割付：定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[詳細化：秘密]：IC カードにアクセスするための一般操作員の PIN
[割付：定義された品質尺度]：6 文字以上 16 文字以下の半角英数記号文字

依存性：　なし

注釈：本 TSF は IC カード管理機能(TOE)である。

FIA_UAU.2a アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1.a 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_UAU.5 複数の認証メカニズム

下位階層： なし

FIA_UAU.5.1 TSFは、利用者認証をサポートするため、[割付：複数の認証メカニズムのリスト]を提供しなければならない。

[割付：複数の認証メカニズムのリスト]：以下の認証メカニズムのリスト

- 操作員IDとパスワードによる認証
- ICカードに格納された秘密鍵を使用したチャレンジ&レスポンス認証
- ICカードに格納された証明書の正当性確認による認証
- 複数操作員認証

FIA_UAU.5.2 TSFは、[割付：複数の認証メカニズムがどのように認証を提供するかを記述する規則]に従って、利用者が主張する識別情報を認証しなければならない。

[割付：複数の認証メカニズムがどのように認証を提供するかを記述する規則]：

項番	適用場面（いつ使われるか）	使用する認証メカニズムと認証内容
1	・CAサーバ端末において、上級操作員を識別認証する場合 ・CAクライアント端末において、一般操作員の識別認証方式として「操作員IDとパスワード」を設定している場合	・操作員IDとパスワードによる認証を行う。TOEは入力されたパスワードとTOEの管理するパスワードとが一致することを確認する

2	・CA クライアント端末において、一般操作員の識別認証方式として「IC カードと PIN による方式」を設定している場合	・IC カードに格納された秘密鍵を使用したチャレンジ＆レスポンス認証を行う。 ・チャレンジ＆レスポンス認証成功後、操作員証明書の正当性確認（当該 CA から発行されたものであること、有効期間内であること、CRL に含まれないこと）を行う。 両方が成功した場合だけ成功となる。 注) チャレンジ＆レスポンス認証に用いられる操作員証明書および操作員秘密鍵は IC カードに格納されており、チャレンジ＆レスポンス認証は、TOE 外の IC カードによる PIN 認証が成功した場合にのみ行われる。
3	・RA 操作端末において、一般操作員の識別認証方式として「IC カードと PIN による方式」を設定している場合	・操作員証明書の正当性確認（当該 CA から発行されたものであること、有効期間内であること、CRL に含まれないこと）を行う。 注) 操作員証明書は IC カードに格納されており、その正当性の確認は、TOE 外の IC カードによる PIN 認証および WWW サーバによる SSL 認証が成功した場合にのみ行われる。
4	・RA 操作端末において、一般操作員の識別認証方式として「操作員 ID とパスワード」を設定している場合	・操作員 ID とパスワードによる認証を行う。TOE は入力されたパスワードと TOE の管理するパスワードとが一致することを確認する
5	・項番１および２で、機能の実行に必要な操作員人数が二人に設定されている場合	・対象機能の実行開始時に、第 2 操作員の認証を行う。認証の内容は項番１もしくは２と同様。第 1 操作員、第 2 操作員両方の認証が成功した場合だけ成功となる。

依存性： なし

FIA_UID.2a アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1.a 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、次の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：[割付：利用者セキュリティ属性のリスト]

[割付：利用者セキュリティ属性のリスト]：

・操作員種別（上級操作員、一般操作員）
・所属する権限グループ

FIA_USB.1.2 TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない：[割付：属性の最初の関連付けに関する規則]

[割付：属性の最初の関連付けに関する規則]：
- 上級操作員、あるいは一般操作員が TOE にログインすると、以降生成される操作員プロセスは、操作員種別に応じて上級操作員プロセス、あるいは一般操作員プロセスとして生成される。上級操作員プロセスあるいは一般操作員プロセスは、操作員が所属する権限グループと、権限グループに付与されているアクセス権限の一覧を照らし合わせることで、プロセスの保持するアクセス権限を決定する。
- 上級操作員、および一般操作員を登録する際、デフォルトでは上級操作員は CA メイン機能の起動／停止、CA 鍵管理、バックアップ／リカバリ、操作員管理、の４つのアクセス権限を付与された上級操作員グループ「administrator」に所属する。一般操作員は、操作員管理、の１つのアクセス権限を付与された一般操作員グループ「operator」に所属する。この２つの権限グループは TOE によって初めから作成されている。

FIA_USB.1.3 TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない：[割付：属性の変更に関する規則]

[割付：属性の変更に関する規則]：上級操作員プロセス、及び一般操作員プロセスは、アクセス制御されるオブジェクトの操作を開始する場合に、自己の操作員種別と所属する権限グループ、および権限グループの保持するアクセス権限を再取得することで、プロセス動作中の利用者セキュリティ属性の変更を既存プロセスに反映する。

依存性： FIA_ATD.1 利用者属性定義

○セキュリティ管理（FMT）

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：以下の機能のリスト][選択：のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を[割付：許可され

た識別された役割]に制限しなければならない。

[割付：機能のリスト]：以下の機能のリスト
[選択：のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]：以下のふるまいの管理
[割付：許可された識別された役割]：以下の役割

機能	ふるまいの管理	役割
アクセス制御機能	改変する（操作員人数）	操作員管理のアクセス権限を持つ権限グループに所属する上級操作員
識別認証機能	決定する（認証方式）	操作員管理のアクセス権限を持つ権限グループに所属する上級操作員、操作員管理のアクセス権限を持つ権限グループに所属する一般操作員

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_MTD.1a TSF データの管理
下位階層：　なし

FMT_MTD.1.1.a TSF は、[割付：TSF データのリスト]を[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]する能力を[割付：許可された識別された役割]に制限しなければならない。

[割付：TSF データのリスト]：以下の TFS データ
[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]：以下の操作
[割付：許可された識別された役割]：以下の役割

TSF データ		操作	許可された識別された役割
上級操作員データ		-	上級操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
	操作員種別（上級操作員）	[その他の操作：割付]	
	操作員 ID	削除、[その他の操作：登録]	
	パスワード	削除、改変、[その他の操作：登録]	
	所属する権限グループ（上級操作員権限グループから選択）	[その他の操作：割付]	
一般操作員データ		-	上級操作員、および一般操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
	操作員種別（一般操作員）	[その他の操作：割付]	
	操作員 ID	削除、[その他の操作：登録]	
	パスワードまたは PIN	削除、改変、[その他の操作：	

	登録]	
秘密鍵	削除、改変、[その他の操作：生成]	
証明書	改変、[その他の操作：生成、失効]	
所属する権限グループ（一般操作員権限グループから選択）	[その他の操作：割付]	

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_MTD.1b TSF データの管理
下位階層： なし

FMT_MTD.1.1.b TSF は、 [割付：TSF データのリスト]を[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]する能力を[割付：許可された識別された役割]に制限しなければならない。

[割付：TSF データのリスト]：
・自分自身のパスワードまたは PIN
[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]：改変
[割付：許可された識別された役割]：上級操作員、一般操作員

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_MTD.1c TSF データの管理
下位階層： なし

FMT_MTD.1.1.c TSF は、[割付：TSF データのリスト]を[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]する能力を[割付：許可された識別された役割]に制限しなければならない。

[割付：TSF データのリスト]：以下の TFS データ
[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]：以下の操作
[割付：許可された識別された役割]：以下の役割

TSF データ	操作	許可された識別され

			た役割
上級操作員グループデータ		-	上級操作員(ただし、操作員管理のアクセス権限を持つ場合のみ許可される)
	権限グループ(上級操作員のみ所属できる上級操作員グループ)	削除、[その他の操作：登録]	
	権限グループが保持するアクセス権限	改変	
一般操作員グループデータ		-	上級操作員、および一般操作員(ただし、操作員管理のアクセス権限を持つ場合のみ許可される)
	権限グループ(一般操作員のみ所属できる一般操作員グループ)	削除、[その他の操作：登録]	
	権限グループが保持するアクセス権限	改変	

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_MTD.1d TSF データの管理

下位階層： なし

FMT_MTD.1.1d TSF は、[割付：TSF データのリスト]を[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]する能力を[割付：許可された識別された役割]に制限しなければならない。

[割付：TSF データのリスト]：以下の TFS データ

[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]：以下の操作

[割付：許可された識別された役割]：以下の役割

TSF データ	操作	役割
監査ログ	問い合わせ（参照）、削除、外部ファイルへの保管	上級操作員、および一般操作員（ただし、監査ログ参照、および／または監査管理のアクセス権限を持つ場合のみ許可される）
アーカイブログ	問い合わせ（参照）、削除、外部ファイルへの保管	上級操作員、および一般操作員（ただし、アーカイブ管理、および／またはアーカイブ参照のアクセス権限を持つ場合のみ許可される）
システム設定情報	削除、改変、登録	上級操作員、および一般操作員（ただし、システム環境設定、および／またはスケジュール管理アクセス権限を持つ場合のみ許可される）

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：TSF によって提供されるセキュリティ管理機能のリスト]。

[割付：TSF によって提供されるセキュリティ管理機能のリスト]：以下のセキュリティ管理機能のリスト

- 権限グループの登録、削除
- 権限グループの保持するアクセス権限の改変
- 操作員 ID の登録、削除
- 操作員のパスワードまたは PIN の登録、改変
- 操作員の秘密鍵の生成
- 操作員の証明書の生成、失効
- 操作員種別の割付
- 操作員の所属する権限グループへの割付
- 認証方式の決定
- 機能の要求する操作員人数の改変
- 監査ログの削除、外部ファイルへの保管
- アーカイブデータの削除、外部ファイルへの保管
- システム設定情報の登録、改変、削除
- 以下の表に示す機能要件の管理項目（上記リストと重複あり）

機能要件	管理要件	管理項目
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
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)。	監査ログ参照権限ありの権限グループの管理
FAU_SAR.2	なし	なし
FAU_SAR.3a	なし	なし
FAU_SAR.3b	なし	なし
FAU_STG.1	なし	なし
FAU_STG.3	a) 閾値の維持; b) 監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)。	a) 監査ログ格納用 DB 容量の設定(セットアップ時に指定) b) なし（アクションは固定であり、管理対象とならない）
FCO_NRO.2	a) 情報種別、フィールド、発信者属性及び証拠の受信者に対する変更の管理。	
FCS_CKM.1a	a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、デ	なし（アクションは固定であり、管理対象とならない）

機能要件	管理要件	管理項目
	ータ暗号化)などがある。	
FCS_CKM.4a	a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし（アクションは固定であり、管理対象とならない）
FCS_COP.1a	なし	なし
FDP_ACC.1	なし	なし
FDP_ACF.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。	なし（属性は固定であり、管理対象とならない）
FIA_AFL.1a	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) 不成功の認証試行に対する閾値の管理 b) なし（アクションは固定であり、管理対象とならない）
FIA_ATD.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。	なし（アクションは固定であり、管理対象とならない）
FIA_SOS.1a	a) 秘密の検証に使用される尺度の管理。	なし（尺度は固定であり、管理対象とならない）
FIA_SOS.1b	a) 秘密の検証に使用される尺度の管理。	なし（尺度は固定であり、管理対象とならない）
FIA_SOS.1c	a) 秘密の検証に使用される尺度の管理。	なし（尺度は固定であり、管理対象とならない）
FIA_UAU.2a	管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	上級操作員及び一般操作員のパスワードあるいは PIN の登録 上級操作員及び一般操作員のパスワードあるいは PIN の改変
FIA_UAU.5	認証メカニズムの管理; 認証に対する規則の管理。	なし(認証メカニズム及び認証に対する規則は固定であり、管理対象とならない)
FIA_UID.2a	a) 利用者識別情報の管理。	a) 上級操作員及び一般操作員の登録
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。	a) なし（サブジェクトのセキュリティ属性定義は固定であり、管理対象とならない）
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;	a) なし（TSF の機能と相互に影響を及ぼし得る役割のグループは固定であり、管理対象とならない）
FMT_MTD.1a	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定であり、管理対象とならない）
FMT_MTD.1b	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。	a) なし（TSF データと相互に影響を及ぼし得る役割のグループは固定であり、管理対象とならない）
FMT_MTD.1c	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定であり、管理対象とならない）
FMT_MTD.1d	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。	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定であり、管理対象とならない）
FMT_SMF.1	なし	なし
FMT_SMR.2	a) 役割の一部をなす利用者のグループを管理すること; b) 役割が満たさなければならない条件を管理すること。	a) 権限グループの管理 b) なし(役割が満たさなければならない条件は固定)
FPT_RVM.1	なし	なし

依存性： なし

FMT_SMR.2 セキュリティ役割における制限
下位階層： FMT_SMR.1

FMT_SMR.2.1 TSF は、役割[割付：許可された識別された役割]を維持しなければならない。

[割付：許可された識別された役割]：上級操作員、一般操作員

FMT_SMR.2.2 TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.2.3 TSF は、条件[割付：異なる役割に対する条件]が満たされていることを保証しなければならない。

[割付：異なる役割に対する条件]：一つの操作員アカウントは、上級操作員と一般操作員の両方を持てない。

依存性： FIA_UID.1 識別のタイミング

○TSF の保護（FPT）

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. 最小機能強度レベル

この TOE の最小機能強度レベルは、低程度（SOF-基本）である。 確率的または順列的メカニズムを利用する機能要件は、上述の FIA_SOS.1a、FIA_SOS.1b、FIA_SOS.1c、FCO_NRO.2、FCS_CKM.1a、FCS_COP.1a であるが、これらの機能要件のうち、最小機能強度レベルに関連する機能要件は、FIA_SOS.1a、FIA_SOS.1b、FIA_SOS.1c である。FIA_AFL.1 により FIA_SOS.1a の機能強度を適正化する。また、FCO_NRO.2、

FCS_CKM.1a、FCS_COP.1a は暗号アルゴリズムを利用した機能要件であるので、本機能強度レベルの対象としない。

5.1.3. TOE セキュリティ保証要件

TOE セキュリティ保証要件を記述する。

本 TOE の評価保証レベルは EAL3 である。すべての保証要件コンポーネントは、CC パート 3 で規定されている EAL3 のコンポーネントを直接使用する。

[EAL3 規定コンポーネント]

(1) 構成管理

ACM_CAP.3：許可の管理

ACM_SCP.1：TOE の CM 範囲

(2) 配付と運用

ADO_DEL.1：配付手続き

ADO_IGS.1：設置、生成、及び立上げ手順

(3) 開発

ADV_FSP.1：非形式的機能仕様

ADV_HLD.2： セキュリティ実施上位レベル設計

ADV_RCR.1： 非形式的対応の実証

(4) ガイダンス文書

AGD_ADM.1：管理者ガイダンス

AGD_USR.1：利用者ガイダンス

(5) ライフサイクルサポート

ALC_DVS.1：セキュリティ手段の識別

(6) テスト

ATE_COV.2： カバレージの分析

ATE_DPT.1： テスト：上位レベル設計

ATE_FUN.1： 機能テスト

ATE_IND.2： 独立テスト－サンプル

(7) 脆弱性評定

AVA_MSU.1：ガイダンスの検査

AVA_SOF.1：TOE セキュリティ機能強度評価

AVA_VLA.1：開発者脆弱性分析

5.2. IT 環境セキュリティ要件

5.2.1. IT 環境セキュリティ機能要件

IT 環境が提供するセキュリティ機能の機能要件を記述する。すべての機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用する。本節で機能要件を満たすのは TOE ではなく IT 環境であるため、機能要件コンポーネントのステートメント中の「TSF」は詳細化を行い主体である IT 環境を明示する。

○暗号サポート（FCS）

FCS_CKM.1b 暗号鍵生成

下位階層： なし

FCS_CKM.1.1.b TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付：暗号鍵長]に従って、暗号鍵を生成しなければならない。

[詳細化：TSF]：HSM

[割付：標準のリスト]：

・FIPS PUB 140-1 または 140-2

[割付：暗号鍵生成アルゴリズム]：ANSI X9.31、PKCS#1

[割付：暗号鍵長]：512bit、768bit、1024bit、1280bit、1536bit、1792bit、2048bit から選択

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.4b 暗号鍵破棄

下位階層： なし

FCS_CKM.4.1.b TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵破棄方法[割付：暗号鍵破棄方法]に従って、暗号鍵を破棄しなければならない。

[詳細化：TSF]：HSM

[割付：標準のリスト]：

・FIPS PUB 140-1 または 140-2

[割付：暗号鍵破棄方法]：zeroization

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
FDP_ITC.2 セキュリティ属性付き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.1b 暗号操作

下位階層： なし

FCS_COP.1.1.b TSF は、[割付：標準のリスト]に合致する、特定された暗号アルゴリズム[割付：暗号アルゴリズム]と暗号鍵長[割付：以下の暗号鍵長]に従って、[割付：暗号操作のリスト]を実行しなければならない。

[詳細化：TSF]：HSM

[割付：標準のリスト]：以下の標準のリスト

[割付：暗号アルゴリズム]：以下の暗号アルゴリズム

[割付：暗号鍵長]：以下の暗号鍵長

[割付：暗号操作のリスト]：以下の暗号操作のリスト

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
CA 鍵	PKCS#1	RSA	512bit, 768bit, 1024bit, 1280bit, 1536bit, 1792bit, 2048bit から選択	EE 証明書の署名 機関証明書の署名 操作員証明書の署名 CRL／ARL の署名

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
FDP_ITC.2 セキュリティ属性付き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

○識別と認証（FIA）

FIA_AFL.1b 認証失敗時の取り扱い

下位階層： なし

FIA_AFL.1.1.b TSF は、[割付：認証事象のリスト]に関して、[選択：[割付：正の整数値],「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]回の不成功認証試行が生じたときを検出しなければならない。

[詳細化：TSF]：IC カード
[割付：認証事象のリスト]：
・IC カードを用いた一般操作員のログイン
[選択：[割付：正の整数値],「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]：8

FIA_AFL.1.2.b 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付:アクションのリスト]をしなければならない。

[割付：アクションのリスト]：
・当該 IC カードでの PIN 入力のブロック

注釈：使用不可能になった IC カードを使用可能にする手段は提供されない。

依存性： FIA_UAU.1 認証のタイミング

FIA_UAU.2b アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1.b 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。

[詳細化：TSF]：データベース

依存性： FIA_UID.1 識別のタイミング

FIA_UAU.2c アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1.c 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。

[詳細化：TSF]：IC カード

依存性： FIA_UID.1 識別のタイミング

FIA_UAU.2d アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1.d 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。

[詳細化：TSF]：オペレーティングシステム

依存性： FIA_UID.1 識別のタイミング

FIA_UID.2b アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1.b 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。

[詳細化：TSF]：データベース

依存性： なし

FIA_UID.2c アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1.c 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。

[詳細化：TSF]：IC カード

依存性： なし

FIA_UID.2d アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1.d 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。

[詳細化：TSF]：オペレーティングシステム

依存性： なし

○TSF の保護（FPT）

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や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。

[詳細化：TSF]：オペレーティングシステムおよびデータベースのセキュリティ機能

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。

[詳細化：TSF]：オペレーティングシステムおよびデータベースのセキュリティ機能

依存性： なし

○高信頼パス／チャネル（FTP）

FTP_ITC.1a TSF 間高信頼チャネル

下位階層： なし

FTP_ITC.1.1.a TSF 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。

[詳細化：TSF]：データベース
[詳細化：リモート高信頼 IT 製品]：TOE

FTP_ITC.1.2.a TSF 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。

[詳細化：TSF]：データベース
[選択: TSF、リモート高信頼 IT 製品]：リモート高信頼 IT 製品
[詳細化：リモート高信頼 IT 製品]：TOE
[詳細化：高信頼チャネル]：CA サーバ端末内の CA サブシステム及び CA クライアント端末内の CA サブシステムと、CA サーバ端末内のデータベースとの間の、データベース機能である Oracle Advanced Security の Net Over SSL を利用したパス

FTP_ITC.1.3.a TSF は、[割付: 高信頼チャネルが要求される機能のリスト]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。

[詳細化：TSF]：データベース
[割付：高信頼チャネルが要求される機能のリスト]：
・高信頼チャネルが要求される CA 操作
[詳細化：高信頼チャネル]：CA サーバ端末内の CA サブシステム及び CA クライアント端末内の CA サブシステムと、CA サーバ端末内のデータベースとの間の、データベース機能である Oracle Advanced Security の Net Over SSL を利用したパス

依存性: なし

FTP_ITC.1b TSF 間高信頼チャネル
下位階層： なし

FTP_ITC.1.1.b TSF 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。

[詳細化：TSF]：CA サーバ端末のWWWサーバ
[詳細化：リモート高信頼 IT 製品]：RA 操作端末の WWW クライアント

FTP_ITC.1.2.b TSF 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。

[詳細化：TSF]：CA サーバ端末のWWWサーバ
[選択：TSF、リモート高信頼 IT 製品]：リモート高信頼 IT 製品
[詳細化：リモート高信頼 IT 製品]：RA 操作端末の WWW クライアント
[詳細化：高信頼チャネル]：RA 操作端末内のWWWクライアントと、CA サーバ端末内のWWWサーバとの間の、WWW サーバの機能である SSL を利用して、サーバ認証、クライアント認証、暗号化が行われるパス

FTP_ITC.1.3.b TSF は、[割付: 高信頼チャネルが要求される機能のリスト]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。

[詳細化：TSF]：RA 操作端末の WWW クライアント
[割付：高信頼チャネルが要求される機能のリスト]：
・高信頼チャネルが要求される CA 操作
[詳細化：高信頼チャネル]：RA 操作端末内のWWWクライアントと、CA サーバ端末内のWWWサーバとの間の、WWW サーバの機能である SSL を利用して、サーバ認証、クライアント認証、暗号化が行われるパス

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

[詳細化：TSF]： OS
注釈：OS は TOE が使用する高信頼タイムスタンプ情報を提供する。

6. TOE要約仕様

この章では、TOEの要約仕様を記述する。

6.1. TOEセキュリティ機能

この節では、TOEのセキュリティ機能を説明する。 表 6-1に示すように、本節で説明するセキュリティ機能は、5.1.1節で記述したTOEセキュリティ機能要件を満たすものである。

表 6-1 TOEセキュリティ機能とセキュリティ機能要件の対応関係

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3a	FAU_SAR.3b	FAU_STG.1	FAU_STG.3	FCO_NRO.2	FCS_CKM.1a	FCS_CKM.4a	FCS_COP.1a	FDP_ACC.1	FDP_ACF.1	FIA_AFL.1a	FIA_ATD.1	FIA_SOS.1a	FIA_SOS.1b	FIA_SOS.1c	FIA_UAU.2a	FIA_UAU.5	FIA_UID.2a	FIA_USB.1	FMT_MOF.1	FMT_MTD.1a	FMT_MTD.1b	FMT_MTD.1c	FMT_MTD.1d	FMT_SMF.1	FMT_SMR.2	FPT_RVM.1
SF.Audit	×	×	×		×	×	×	×																							
SF.I&A															×		×	×	×	×	×	×									×
SF.ACC			×	×			×						×	×		×							×	×	×	×	×	×	×	×	×
SF.Crypto							×			×	×	×																	×		
SF. Cer_Issue									×																				×		

6.1.1. SF.Audit

TOEは、TOEがセキュアに運用されていることを監査するために必要な情報の採取、および管理を行うために、監査の対象となる事象が発生した場合に、当該事象を監査データとして採取する。 TOEは、監査データを記録するのに必要なタイムスタンプ情報をIT環境であるOSから取得する。

監査データは以下の項目で構成される。

- 順次番号。監査データ1件ごとに割り当てられる番号。
- 操作員ID。システムに登録されている上級操作員、一般操作員のID。
- 事象の種別。事象の分類を表すもの。” システム起動 ”、” 証明書発行 ” など。
- メッセージ。事象の詳細な内容を表すもの。
- 事象の結果。成功、失敗（警告）、失敗（エラー）の３種類。
- 事象の日付・時刻。OSから取得したタイムスタンプ情報を使用する。
- 拡張情報。メッセージに付随するコード、具体的な対象名、ステータスなどに類する補足情報。
- ハッシュ値。監査データの改ざんチェックに使用する内部データ。

監査データを生成する主体となるプロセスは全て操作員が関連している。各プロセス（サブジェクト）は関連する操作員IDで一意に識別可能である。従って、本TOEではサブジェクト識別情報と操作員IDを同一のものとして、監査データを生成している。

監査データは以下の監査対象事象の発生時に採取する。

- 監査機能の起動と終了
- 操作員の識別と確認
- CA サーバコンソール機能および CA クライアントコンソール機能の起動／停止
- CA メイン機能の起動／停止
- 操作員の登録／削除／編集
- アクセス権限の設定
- ポリシー設定
- バックアップ／リカバリの実行
- 証明書要求の発行
- 証明書の発行
- 証明書の失効
- 証明書の出力
- 証明書要求の審査
- CRL／ARL の発行
- CRL／ARL の出力
- EE IC カード発行情報ファイルの出力
- システム環境設定
- スケジュールの設定
- 監査データの削除／外部出力
- アーカイブデータの削除／外部出力
- ユーザ情報の登録／削除／編集
- CA のセットアップ
- CA 鍵の変更
- CA 証明書の失効
- データベースパスワードの変更
- アクセスの拒否（操作員の識別と確認の失敗、アクセス権限のない操作の試み）

TOE は、以下の監査データ保護機能を提供する。

- 現在 TOE 内に存在するはずの監査データの順次番号（開始番号と終了番号）を管理する。また、順次番号の開始番号と終了番号との間で、監査データが連続していることを検証する。
- 監査データは、SF.Cryptoによって導出したハッシュ値を保持する。このハッシュ値は、監査データを参照、外部出力する際に検証される。
- 監査データは、順次番号と事象の日付・時刻を除くすべての項目が SF.Crypto によって

暗号化されて保管される。これによって、監査データの暴露を防ぐ。

- 監査データの連続性の確認。TOE に存在する最初の監査データの順次番号が管理している開始番号と一致しない場合や、最後の監査データの順次番号が管理している終了番号と一致しない場合、また、監査データの順次番号が連続していない場合には、監査データが消失していることを操作員に知らせる。
- 監査データの完全性の確認。SF.Crypto によって監査データのハッシュ値を計算し、監査データの完全性を検証する。監査データの改ざんを検知した場合には、これを操作員に知らせる。

TOE は、以下の監査データ参照機能を提供する。

- 監査データは、CA サーバコンソールもしくは CA クライアントコンソールで参照できる。また、紙に印刷することが可能である。
- 監査データの検索。検索条件には、操作員 ID、事象の種別、事象の日付・時刻、事象の結果（成功または失敗）の任意の組み合わせが指定可能である。
- 監査データの並べ替え。並べ替え条件に指定できる項目には、順次番号、操作員 ID、事象の種別、メッセージ、事象の結果（成功または失敗）、事象の日付・時刻、拡張情報のうちのひとつが指定可能である。監査データの参照機能は、SF.ACC による「監査ログ参照」アクセス権限を付与された操作員だけが実行できる。

上級操作員が CA のセットアップ時に、監査データを保持するための専用のデータベース領域が確保される。この領域のサイズは、CA のセットアップ時のパラメータによって決定される。

この領域に空き領域がなくなるなどの理由で監査データの出力に失敗した場合には、TOE の運用を停止し、監査データが採取できない状況において、監査対象となる事象が発生することを防止する。TOE は、監査データを保持するためのデータベース領域を確保するため、採取済みの監査データをデータベース上から削除し、外部ファイルに保管する機能を提供する。この機能は、SF.ACC による「監査管理」アクセス権限を付与された操作員だけが実行できる。

6.1.2. SF.ACC

TOE は、TOE に対するすべての操作が、TOE に対するアクセス権限を付与された上級操作員および一般操作員によってのみ可能である。

TOE に対するアクセス権限は、権限グループ単位で管理される。各操作員は、TOE で定義されている 1 つの権限グループに所属することにより、TOE に対するアクセス権限を獲得

する。
TOE は、後述する SF.I&A で識別認証が終了した後、操作員 ID を利用者を代行して動作するサブジェクトである上級操作員プロセスまたは一般操作員プロセスに関連付ける。

TOE は、SF.I&A によって識別および認証された上級操作員もしくは一般操作員の操作員 ID から、当該操作員の操作員種別および所属する権限グループを認識する。これと、所属する権限グループに付与されているアクセス権限の一覧を照らし合わせることにより、当該操作員のアクセス制御を実施する。このアクセス制御は、Carassuit 電子政府版 ver3.1 アクセス制御方針に従う。

TOE は、以下の 2 種類の操作員種別を定義する。
- 上級操作員
- 一般操作員

すべての操作員は、登録時点において、上記いずれか一方の操作員種別に分類される。

上級操作員は、登録時に以下のセキュリティ属性を持つ。
- 操作員種別（上級操作員）
- 所属する権限グループ

一般操作員は、登録時に以下のセキュリティ属性を持つ
- 操作員種別（一般操作員）
- 所属する権限グループ

セキュリティ属性のうち、所属する権限グループは、登録後に、操作員管理のアクセス権限を持つ上級操作員および一般操作員によって変更可能である。

TOE は、以下の 2 種類の権限グループ種別を定義する。
- 上級操作員権限グループ。上級操作員だけが所属することができる。
- 一般操作員権限グループ。一般操作員だけが所属することができる。

CA のセットアップ時において、権限グループとして上級操作員権限グループに属する「Administrator」、一般操作員権限グループに属する「Operator」が定義される。デフォルトで付与されているアクセス権限（後述）は以下のとおりである。

権限グループ名	権限グループ種別	付与されているアクセス権限
Administrator	上級操作員権限グループ	CA メイン機能の起動／停止 CA 鍵管理 バックアップ／リカバリ

		操作員管理
Operator	一般操作員権限グループ	操作員管理

必要に応じて、上記権限グループに対してアクセス権限を追加または削除することが可能である。ただし、Administrator 権限グループは、自身の「操作員管理」アクセス権限を削除できない。
また、新たな権限グループを作成することができる。この場合、デフォルトで付与されるアクセス権限はなく、必要に応じてアクセス権限を追加する。

各操作員が所属する権限グループは、デフォルトでは上級操作員は Administrator 権限グループ、一般操作員は Operator 権限グループが選択される。但し、別の権限グループが作成されていればそれを選択することもできる。

TOE が定義できるアクセス権限の表を以下に示す。アクセス権限は以下の表で定義されたものがすべてであり、新たなアクセス権限を定義することはできない。

アクセス権限	機能	権限グループ種別	操作員人数
ARL 出力	ARL の外部出力	上級操作員 一般操作員	複数可
CA メイン機能の起動／停止	CA メイン機能の起動、および停止	上級操作員	複数可
CA 鍵管理	CA の鍵情報の参照	上級操作員	複数可
CRL 出力	CRL の外部出力	上級操作員 一般操作員	複数可
アーカイブ管理	アーカイブデータの外部ファイル出力	上級操作員 一般操作員	複数可
アーカイブ参照	アーカイブデータの参照および検索	上級操作員 一般操作員	複数可
システム環境設定	システムパラメータの設定	上級操作員 一般操作員	複数可
スケジュール管理	スケジュール管理の設定	上級操作員 一般操作員	複数可
バックアップ／リカバリ	バックアップおよびリカバリの実行	上級操作員	複数可
ポリシー管理	証明書プロファイルの新規登録、変更、削除	上級操作員 一般操作員	複数可
監査ログ参照	監査データの参照および検索	上級操作員 一般操作員	複数可
監査管理	監査データの外部ファイル出力および印刷	上級操作員 一般操作員	複数可
操作員管理	操作員の登録、削除 権限グループの作成 操作員の所属する権限グループの変更 権限グループに付与するアクセス権限の変更	上級操作員 一般操作員	複数可
	機能を実行する操作員人数の設定・変更	上級操作員	複数可
ユーザ管理	ユーザ情報の登録／削除／編集	一般操作員	複数可
証明書情報参照	発行済みの証明書および現在処理中の証明書要求の一覧参照	上級操作員 一般操作員	複数可
機関証明書申請	指定した機関証明書プロファイルでの証明書の	上級操作員	複数可

	申請	一般操作員	
機関証明書取得	指定した機関証明書プロファイルで発行された証明書の出力	上級操作員 一般操作員	複数可
機関証明書失効	指定した機関証明書プロファイルで発行された証明書の失効	上級操作員 一般操作員	複数可
EE 証明書申請	指定した EE 証明書プロファイルでの証明書の申請	一般操作員	複数可
EE 証明書審査	指定した EE 証明書プロファイルで申請された証明書の審査	一般操作員	単数のみ
EE 証明書取得	指定した EE 証明書プロファイルで発行された証明書の出力	一般操作員	複数可
EE 証明書失効	指定した EE 証明書プロファイルで発行された証明書の失効	一般操作員	複数可
EE IC カード発行	EE 鍵／証明書を IC カードへ格納する形式のファイルの生成	一般操作員	単数のみ

二列目に記述した機能を実行することができるのは、その機能を実施するアクセス権限が付与された権限グループ種別の権限グループに属する上級操作員および／または一般操作員のみである。
各アクセス権限は、権限グループ種別（「上級操作員」または「上級操作員と一般操作員」または「一般操作員」）ごとに付与できるアクセス権限が異なる。上の表の権限グループ種別の欄で、「上級操作員」となっているアクセス権限は上級操作員権限グループにのみ付与可能。「上級操作員」と「一般操作員」が併記されているアクセス権限は上級操作員権限グループ、一般操作員権限グループの両方に付与可能。「一般操作員」となっているアクセス権限は一般操作員権限グループにのみ付与可能である。

また、一部のアクセス権限は、その機能を実行する操作員人数を一人もしくは二人に設定することができる。上記の表の操作員人数の欄で、「複数可」となっているアクセス権限が該当する。「単数のみ」となっているアクセス権限は操作員人数が一人固定である。

アクセス権限の中で「操作員管理」のアクセス権限は、アクセス権限自体の管理権限である。
必要なアクセス権限を獲得している上級操作員、一般操作員が管理できるセキュリティ属性を含む TSF データは以下の通りである。

TSF データ	許可された識別された役割
上級操作員データ	上級操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
操作員種別（上級操作員）	
操作員 ID	
パスワード	
所属する権限グループ（上級操作員権限グループから選択）	
一般操作員データ	上級操作員、および一般操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
操作員種別（一般操作員）	
操作員 ID	

パスワードまたは PIN	
秘密鍵	
証明書	
所属する権限グループ（一般操作員権限グループから選択）	
上級操作員グループデータ	上級操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
権限グループ(上級操作員のみ所属できる上級操作員グループ)	
権限グループが保持するアクセス権限	
一般操作員グループデータ	上級操作員、および一般操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
権限グループ(一般操作員のみ所属できる一般操作員グループ)	
権限グループが保持するアクセス権限	
監査ログ	上級操作員、および一般操作員（ただし、監査ログ参照､および／または監査管理のアクセス権限を持つ場合のみ許可される）
アーカイブログ	上級操作員、および一般操作員（ただし、アーカイブ管理､および／またはアーカイブ参照のアクセス権限を持つ場合のみ許可される）
システム設定情報	上級操作員、および一般操作員（ただし、システム環境設定､および／またはスケジュール管理アクセス権限を持つ場合のみ許可される）

各アクセス権限が付与された権限グループに所属する上級操作員プロセスおよび一般操作員プロセスが実行できる機能とその操作対象となる TOE の資産は以下のとおりである。

機能	資産
機関証明書プロファイルで発行された証明書の出力機能	機関証明書ファイル
機関証明書プロファイルで発行された証明書の失効機能	ARL ファイル
EE 証明書プロファイルでの証明書の出力機能	EE 証明書ファイル
EE 証明書プロファイルで発行された証明書の失効機能	CRL ファイル
EE 鍵／証明書を IC カードへ格納する形式のファイルの生成機能	EE IC カード発行情報ファイル
アクセスコントロール（操作員管理）機能	操作員証明書
	識別・認証情報
	アクセスコントロール情報
監査データの参照、検索機能 監査データの外部ファイル出力、印刷機能	監査ログ
アーカイブデータの外部出力機能 アーカイブデータの参照、検索機能	アーカイブログ
システムパラメータの設定機能 スケジュール管理の設定機能	システム設定情報

TOE は、TSC 内の各機能の動作が許可される前に、SF.ACC を呼び出す。
本節で述べた設定情報すべて（識別認証に関する情報やアクセス権限に関する情報など）はデータベースのファイルに保存される。

6.1.3. SF.I&A

TOE は、TOE にアクセスする上級操作員および一般操作員を識別し、識別した操作員が登録されている上級操作員および一般操作員本人であることを確認する。

識別認証方式は、以下のように複数の認証メカニズムと認証を提供する規則がある。

認証方式	認証を提供する規則
操作員 ID とパスワードによる認証	CA サーバ端末において、上級操作員を識別認証する場合、および CA クライアント端末、もしくは RA 操作端末において、一般操作員の識別認証方式が操作員 ID とパスワードによる方式の場合、 TOE が入力されたパスワードと TOE の管理するパスワードとが一致することを確認する。
IC カードに格納された秘密鍵と証明書による認証	CA クライアント端末において、一般操作員の識別認証方式が IC カードと PIN による方式の場合、TOE はチャレンジ＆レスポンス認証を行う。 チャレンジ＆レスポンス認証成功後、TOE は操作員証明書の正当性（当該 CA から発行されたものであること、有効期間内であること、CRL に含まれないこと）を確認する。 注) チャレンジ＆レスポンス認証に用いられる操作員証明書および操作員秘密鍵は IC カードに格納されており、チャレンジ＆レスポンス認証は、IC カードによる PIN 認証が成功した場合にのみ行われる。
IC カードに格納された証明書による認証	RA 操作端末において、一般操作員の識別認証方式が IC カードと PIN による方式の場合、TOE は操作員証明書の正当性（当該 CA から発行されたものであること、有効期間内であること、CRL に含まれないこと）を確認する。 注) 操作員証明書は IC カードに格納されており、その正当性の確認は、IC カードによる PIN 認証および WWW サーバによる SSL 認証が成功した場合にのみ行われる。
複数操作員認証	第１操作員、第２操作員の両者の認証が成功した場合に成功となる。

PIN 認証は IC カードの機能を使うので、TOE 外である。
上級操作員および一般操作員の認証にあたっては、TOE は各操作員に識別認証前のいかなる操作も許可しない。
一般操作員は、登録時に、操作員認証に操作員 ID とパスワードを用いるか、もしくは IC カードとその PIN を用いるかのどちらかを選択する。パスワードもしくは PIN は、登録後に、操作員管理のアクセス権限を持つ上級操作員および一般操作員によって変更可能である。また、上級操作員および一般操作員は、自分自身のパスワードもしくは PIN を変更可能である。

それぞれの方式において、TOE は、以下のように上級操作員および一般操作員を一意に識別、認証する。

1.操作員 ID とパスワードによる認証

1) CA サーバコンソール／CA クライアント端末から CA サーバコンソール／CA クライアントコンソールを起動して操作員認証画面を表示させる。RA 操作員は、RA 操作端末からブラウザを起動し、CA サーバ端末の WWW サーバにアクセスし操作

員認証画面を表示させる。

2) ID、パスワードを入力すると、それに基づきデータベースから該当する情報を読み込む。
3) 入力したパスワードのハッシュ値を生成し、ID と DB 内に保存されたパスワードのハッシュ値と同じであることを確認することにより認証する。
パスワードが正しくない場合、パスワード誤り回数がカウントされる。パスワード誤り回数が、パスワード試行可能回数(3～16)（既定値(8)または運用開始後にアクセスコントロールで指定）に達すると、アカウントをロックする。
4) ロックされたアカウントを復旧する場合は、「操作員管理」のアクセス権限を有する上級操作員／一般操作員が当該アカウントを削除し、再度アカウントを作成する。

2.CA クライアント端末における IC カードと PIN による認証

一般操作員は、あらかじめ登録され、証明書を保存し PIN を設定した IC カードが発行されている必要がある。

1) CA クライアント端末上で CA クライアントコンソールを起動して操作員認証画面を表示させる。
2) CA クライアント端末に接続された IC カードリーダに当該操作員の IC カードを差し込み、PIN を入力する。
3) PIN を IC カード管理機能に渡し、IC カード管理機能が IC カードにアクセスして PIN を IC カードに送る。
4) IC カードは PIN 認証を実行する。PIN が正しい場合、IC カードに保存されたその操作員の証明書、および CA サーバから送られたチャレンジを IC カードに保存されたその操作員の秘密鍵を用いて署名したものが TOE に送信される。TOE は、その証明書とチャレンジの署名を検証し、両者が有効な場合に当該操作員を認証する。
5) PIN が正しくない場合、IC カードの PIN 誤り回数がカウントされる。PIN 誤り回数が 8 回に達すると、PIN の入力をブロックする。
6) PIN の入力がブロックされた IC カードは、ブロック解除用の PIN を入力することにより解除可能であるが、TOE はブロック解除用 PIN を知る手段、および、ブロック解除用 PIN の入力ユーザインタフェースを提供しない。

注： IC カード、IC カードリーダは TOE 外であり、上記 4)、5)の PIN 認証は TOE 範囲外の機能である。

3.RA 操作端末における IC カードと PIN による認証

RA 操作員は、あらかじめ登録され、証明書を保存し PIN を設定した IC カードが発行されている必要がある。

1) RA 操作端末からブラウザを起動し、CA サーバ端末の WWW サーバにアクセスし操作員認証画面を表示させる。
2) RA 操作端末に接続された IC カードリーダに当該操作員の IC カードを差し込み、PIN を入力する。
3) PIN を IC カード管理機能に渡し、IC カード管理機能が IC カードにアクセスして PIN を IC カードに送る。
4) IC カードは PIN 認証を実行する。PIN が正しい場合、IC カードに保存されたその操作員の証明書、および CA サーバから送られたチャレンジを IC カードに保存されたその操作員の秘密鍵を用いて署名したものが WWW サーバに送信される。WWW サーバは、その証明書とチャレンジの署名を検証し、SSL のクライアント認証を行う。
5) SSL のクライアント認証が成功した場合、WWW サーバは TOE に当該操作員の証明書を渡す。
6) TOE は WWW サーバから渡された当該操作員の証明書を検証し、正しい証明書であることを確認することにより、当該操作員を認証する。
7) PIN が正しくない場合、IC カードの PIN 誤り回数がカウントされる。PIN 誤り回数が 8 回に達すると、PIN の入力をブロックする。
8) PIN の入力がブロックされた IC カードは、ブロック解除用の PIN を入力することにより解除可能であるが、TOE はブロック解除用 PIN を知る手段、および、ブロック解除用 PIN の入力ユーザインタフェースを提供しない。

注： WWW サーバ、IC カード、IC カードリーダは TOE 外であり、上記 4)、5)、7)は TOE 範囲外の機能である。

機能の実行に必要な操作員人数が二人に設定されている場合、第 2 操作員の認証が必要である。（ただし第２操作員認証は RA 操作端末からの操作は対象外である。機能の実行に必要な操作員人数が二人に設定されている場合でも RA 操作端末からの操作では一人の操作員認証しか行わない。）第 2 操作員の 認証は以下のように行う。

4.第 2 操作員の認証

1) 操作員人数が二人に設定されている機能を実行した時点で第 2 操作員のための操作員認証画面を表示する。
2) 第 2 操作員として提示された ID もしくは IC カードが、第 1 操作員と同じでないことを確認する。
3) 第 1 操作員と同じ方法（上述の 1.操作員 ID とパスワードによる認証、あるいは 2.CA クライアント端末における IC カードと PIN による認証の、操作員認証画面の表示以降で示した認証メカニズム）で、第 2 操作員の認証を行う。

パスワードは、以下の条件を満たすものが設定可能である。

- 長さ: 6 文字～32 文字
- 使用可能な文字: 半角英数記号文字
- 大文字・小文字の区別がある

上級操作員および一般操作員の登録時、および、パスワードの変更時において、当該操作員が指定したパスワードが上記を満たさない場合には、パスワードの再入力を要求する。

TOE は、利用者データ及び TSF データの保存にデータベースを使用するので、そのパスワードの条件を検証する。データベースへアクセスするパスワードは、以下の条件を満たすものが設定可能である。

- 長さ: 6 文字～16 文字
- 使用可能な文字: 半角英数記号文字

PIN は、以下の条件を満たすもののみを設定可能とする。

- 長さ: 6 文字～16 文字
- 使用可能な文字: 半角英数記号文字

一般操作員の登録時、および、PIN の変更時において、当該操作員が指定した PIN が上記を満たさない場合には、IC カード管理機能が PIN の再入力を要求する。

TOE は、TSC 内の各機能の動作が許可される前に、SF.I&A を呼び出す。

6.1.4. SF.Crypto

TOE は、以下の鍵を生成する。

鍵の種類	アルゴリズム	暗号鍵長
EE 鍵ペア （RSA）	・疑似乱数生成アルゴリズム ・PKCS#1	512bit, 768bit, 1024bit, 2048bit から選択
操作員鍵ペア （RSA）	・疑似乱数生成アルゴリズム ・PKCS#1	512bit, 768bit, 1024bit, 2048bit から選択
システム共通鍵 （Triple DES）	疑似乱数生成アルゴリズム	168bit
データベース共通鍵 （Triple DES）	疑似乱数生成アルゴリズム	168bit
共通鍵保護鍵	非公開独自方式	168bit

（Triple DES）		
EE IC カード発行情報ファイル保護鍵（Triple DES）	SHA-1 (元データをハッシュ演算で加工することで鍵としている)	168bit

TOE は、以下の暗号操作を行う。
表中の CA 公開鍵は TOE 外である HSM により生成されるが、CA 証明書として取り出されたものを使用して TOE 内で署名検証の操作を行うものである。

鍵の種類	アルゴリズム	暗号鍵長	暗号操作
CA 公開鍵	RSA	512bit, 768bit, 1024bit, 2048bit から選択	・操作員証明書の署名検証 ・CRL の署名検証
操作員秘密鍵／公開鍵	RSA	512bit, 768bit, 1024bit, 2048bit から選択	認証用のチャレンジの署名および署名検証
システム共通鍵	Triple DES	168bit	・アクセスコントロール情報の登録時の暗号化と参照時の復号 ・監査データ(1 レコードづつ)の登録時の暗号化と参照時の復号 ・アーカイブデータ(1 レコードづつ)の登録時の暗号化と参照時の復号 ・データベース用パスワードの保管時の暗号化と参照時の復号
データベース共通鍵	Triple DES	168bit	EE 秘密鍵の保管時の暗号化と取り出し時の復号
共通鍵保護鍵	Triple DES	168bit	システム共通鍵、データベース共通鍵の保管時の暗号化と参照時の復号
EE IC カード発行情報ファイル保護鍵	Triple DES	168bit	EE IC カード発行情報ファイルの暗号化
パスフレーズから生成する共通鍵	Triple DES	168bit	・機関証明書と秘密鍵の PKCS#12 出力時の秘密鍵暗号化 ・EE 証明書と秘密鍵の PKCS#12 出力時の秘密鍵暗号化
なし	SHA-1	—	・識別認証情報のハッシュ操作 ・アクセスコントロール情報のハッシュ操作 ・システム設定情報のハッシュ操作 ・監査ログのハッシュ操作 ・アーカイブデータのハッシュ操作 注) ハッシュ操作とは、ハッシュ値生成および比較である
なし	MD5	—	

補足：CA 鍵ペアの生成は、TOE の運用開始前に認証局秘密鍵管理者が TOE 外の HSM を直接操作することで行われる。また CA 秘密鍵による署名（EE 証明書、機関証明書、操作員証明書、CRL,ARL）は、TOE からの API 呼び出しで TOE 外の HSM によって行われる。EE 証明書と機関証明書は TOE で署名検証することはない。システム共通鍵及びデータベ

ース共通鍵は CA セットアップ時に生成し、同じくその場で生成した共通鍵保護鍵で暗号化してデータベースに保存する。以降の TOE 運用中はこれらの鍵を更新することはない。共通鍵保護鍵は、システム共通鍵及びデータベース共通鍵の参照が必要である都度、初回と同様の元データと加工手順により生成する。共通鍵保護鍵は使用後すぐに破棄し、TOE 内外に保存することはない。

TOE は、データベースに格納している暗号鍵を破棄する場合には、暗号鍵を格納していた領域をダミーデータ（乱数やゼロデータなどの意味のないデータ）で上書きした後、領域を解放する。

6.1.5. SF.Cer_Issue

TOE は、生成された証明書および失効リスト（CRL、ARL）を発行（出力）する機能を提供する。
生成される証明書は、CA 証明書、機関証明書、操作員証明書、EE 証明書である。 機関証明書には、下位 CA 証明書と相互認証証明書との二種類がある。

証明書は、証明書プロファイルに基づいて発行される。証明書プロファイルとは、証明書に含めるフィールド（共通名や電子メールアドレスなど）の集合であり、証明書発行に先だって、上級操作員もしくは一般操作員が作成する。証明書プロファイルは、複数作成することができる。
証明書プロファイルには機関証明書を発行するための機関証明書用プロファイルと、EE 証明書を発行するための EE 証明書用プロファイルとがあり、証明書プロファイル作成時にどちらかが指定される。

証明書の出力は以下の形式で行われる。

- データベースへの登録
- リポジトリへの登録
- 上級操作員および一般操作員からの要求により証明書をバイナリファイル（DER、BASE64 エンコード、PKCS#7、PKCS#12）出力

登録先となるデータベース、及びリポジトリはシステム環境設定機能で設定される。

すべての証明書および失効リストは、CA 証明書のサブジェクト名と同じ値である発行者名と、CA 秘密鍵を用いて生成された署名値が格納されており、CA 証明書の有効期間の範囲で、発行された証明書や失効リストが確かに本認証局から発行されたということを検証者が検証することができる。

また、TOE は自らが発行するすべての証明書及び失効リストの発行履歴をアーカイブログとして管理する。

6.2. セキュリティ機能強度

確率的または順列的メカニズムに基づくセキュリティ機能は、上述の SF.I&A 及び SF.Crypto、SF.Cer_Issue である。これらのセキュリティ機能のうち、SF.I&A が機能強度レベル SOF-基本を持つ。SF.Crypto、SF.Cer_Issue は、暗号アルゴリズムを利用したセキュリティ機能であるので、本機能強度レベルの対象としない。

6.3. 保証手段

この章では、TOE のセキュリティ保証手段を説明する。 表 6-2に示すように、以下のセキュリティ保証手段は、5.1.3 節で記述した TOE セキュリティ保証要件を満たすものである。

表 6-2 保証手段と保証要件コンポーネントの対応関係

保証手段	保証要件クラス	保証要件コンポーネント
PKIサーバ／Carassuit 電子政府版 ver3.1 構成管理文書	ACM 構成管理	ACM_CAP.3
		ACM_SCP.1
PKIサーバ／Carassuit 電子政府版 ver3.1 配付手続文書	ADO 配付と運用	ADO_DEL.1
PKIサーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス		ADO_IGS.1
PKIサーバ／Carassuit 電子政府版 ver3.1 機能仕様書	ADV 開発	ADV_FSP.1
PKIサーバ／Carassuit 電子政府版 ver3.1 上位レベル設計書		ADV_HLD.2
PKIサーバ／Carassuit 電子政府版 ver3.1 表現対応分析書		ADV_RCR.1
PKIサーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス	AGD ガイダンス文書	AGD_ADM.1
本 TOE は管理者のみが利用し、一般利用者は利用しないので、利用者ガイダンスは提供しない。		AGD_USR.1
PKIサーバ／Carassuit 電子政府版 ver3.1 開発セキュリティ文書	ALC ライフサイクルサポート	ALC_DVS.1
PKIサーバ／Carassuit 電子政府版 ver3.1 テストカバレージ分析書	ATE テスト	ATE_COV.2
PKIサーバ／Carassuit 電子政府版 ver3.1 テスト深さ分析書		ATE_DPT.1
PKIサーバ／Carassuit 電子政府版 ver3.1 テスト手順書・報告書		ATE_FUN.1
PKIサーバ／Carassuit 電子政府版 ver3.1 TOE		ATE_IND.2
PKIサーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス	AVA 脆弱性評定	AVA_MSU.1
PKIサーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス		AVA_MSU.1
PKIサーバ／Carassuit 電子政府版 ver3.1 セキュリティ強度分析書		AVA_SOF.1
PKIサーバ／Carassuit 電子政府版 ver3.1 脆弱性分析書		AVA_VLA.1

次に、各保証手段の内容を説明する。

（1）構成管理

構成管理文書として、以下の文書を作成する。

a） PKI サーバ／Carassuit 電子政府版 ver3.1 構成管理文書
＜記述内容＞
・TOE のバージョンのリファレンス
（バージョンの付け方、TOE のバージョン表示方法）
・構成リスト
（構成要素）
・構成管理計画
（構成要素作成・変更・削除方法、構成要素の操作に必要な個人の役割と責任、
構成要素へのアクセス権、構成要素同時変更防止方法、構成要素管理記録、
TOE バージョン管理方法）
・構成要素識別
（保証手段文書、テストソフトウェア、TOE ソースコード）
・構成要素識別方法
（一意の識別情報を割り付ける方法、構成管理システムに組み入れる方法、
TOE の置き換えバージョンを識別する方法、開発保守ライフサイクルにおいて
構成要素を識別する方法、構成要素間の対応識別）

（2）配付と運用

配付と運用文書として、以下の文書を作成する
b） PKI サーバ／Carassuit 電子政府版 ver3.1 配付手続文書
＜記述内容＞
・TOE を利用者サイトへ配送するときのセキュリティを維持するために必要な手続き
（配付する TOE 識別（型番、バージョン）、TOE 配付手段、TOE パッケージ方法）

c） PKI サーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス
＜記述内容＞
・セキュアな設置、生成及び立上げに必要な手順
（設置、インストール方法）

（3）開発

開発文書として、以下の文書を作成する。
d） PKI サーバ／Carassuit 電子政府版 ver3.1 機能仕様書
＜記述内容＞
・TOE セキュリティ機能内容
・外部 TOE セキュリティ機能インタフェース識別
・外部 TOE セキュリティ機能インタフェース内容

（効果、例外および誤りメッセージ）
・外部 TOE セキュリティ機能インタフェースのふるまい
（利用者入力パラメータ、モード）

e） PKI サーバ／Carassuit 電子政府版 ver3.1 上位レベル設計書
＜記述内容＞
・サブシステム識別
・サブシステム内容
（セキュリティ機能）
・TSF で必要とする IT 環境であるハードウェア、ソフトウェア識別
・IT 環境のハードウェア、ソフトウェアで実装される補助的な保護メカニズムが提供する機能
・サブシステム内部インタフェース識別
・サブシステム外部インタフェース識別
・サブシステムインタフェース内容
（目的、使用方法、効果、例外及び誤りメッセージ）
・TSP 実施サブシステム識別

f） PKI サーバ／Carassuit 電子政府版 ver3.1 表現対応分析書
＜記述内容＞
・ST の TOE セキュリティ機能と上記機能仕様書の TOE セキュリティ機能間の関係
・ST の TOE セキュリティ機能と上記機能仕様書の外部 TOE セキュリティ機能インタフェース間の関係
・上記機能仕様書の TOE セキュリティ機能と上記上位レベル設計書のサブシステム間の関係
・上記機能仕様書の外部 TOE セキュリティ機能と上記上位レベル設計書のサブシステム間の関係

（4）ガイダンス
ガイダンス文書として、以下の文書を作成する。
g） PKI サーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス
＜記述内容＞
・管理セキュリティ機能とインタフェース
（目的、ふるまい、相互関係、インタフェース起動方法、パラメータとそのデフォルト値、リターンコード）
・IT 環境の利用方法、IT セキュリティ要件

・TOE の管理機能・権限
・TOE 操作のすべての可能なモード
（故障または操作誤りの後の操作も含む）
・ST で記述した前提条件
（TOE の意図する使用方法、物理的、人的及び接続的前提条件）

（5）ライフサイクルサポート

ライフサイクルサポート文書として、以下の文書を作成する。

h） PKI サーバ／Carassuit 電子政府版 ver3.1 開発セキュリティ文書

＜記述内容＞

・開発環境で使用されるセキュリティ手段
（TOE 開発環境への物理的アクセス制御、開発マシンへのアクセス制御、部外者のアクセス制限、セキュリティ適用役割と責任、開発スタッフ管理）
・開発環境セキュリティ記録
（入退室管理ログ）

（6）テスト

テスト文書として、以下の文書を作成し、TOE を提供する。

i） PKI サーバ／Carassuit 電子政府版 ver3.1 テストカバレージ分析書

＜記述内容＞

・上記機能仕様書のセキュリティ機能と下記テスト手順書・報告書 k）のテスト項目名との間の関係

j） PKI サーバ／Carassuit 電子政府版 ver3.1 テスト深さ分析書

＜記述内容＞

・上記上位レベル設計書のサブシステムと下記テスト手順書・報告書 k）のテスト項目名との間の関係

k） PKI サーバ／Carassuit 電子政府版 ver3.1 テスト手順書・報告書

＜記述内容＞

・テスト計画
（テストされるセキュリティ機能識別、テスト目標、テスト構成）
・テスト手順記述
（セキュリティ機能ふるまい識別、順序の依存性、再現可能性、テスト手順）
・期待されるテスト結果及び実際のテスト結果

l） PKI サーバ／Carassuit 電子政府版 ver3.1 TOE
評価者が TOE のテストを行う際、l）に関し、上記のテスト手順書・報告書に記述したテストで使用されたものと同等の一連の資源を提供する。

（7）脆弱性評定
脆弱性評定文書として、以下の文書を作成する。
g） PKI サーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス
＜記述内容＞
既述。

c） PKI サーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス
＜記述内容＞
既述。

m）PKI サーバ／Carassuit 電子政府版 ver3.1 セキュリティ強度分析書
＜記述内容＞
・ST でレート付けした SOF 主張に対するセキュリティメカニズムに関する SOF 分析
（前提条件、正しいパスワードの入力確率計算、攻撃潜在性計算、考察）

n）PKI サーバ／Carassuit 電子政府版 ver3.1 脆弱性分析書
＜記述内容＞
・上記の保証手段文書ごと含まれる脆弱性の内容
・明らかな脆弱性の内容
・上記で識別された脆弱性の分析
（公知の有無、知識の有無、対抗手段、悪用可能性）

7. PP 主張

この章では、PP 主張について記述する。

7.1. PP 参照

参照した PP はない。

7.2. PP 修整

修整した PP はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠、PP 主張根拠について記述する。

8.1. セキュリティ対策方針根拠

セキュリティ対策は、TOE セキュリティ環境で規定した脅威に対抗するためのものである。あるいは、TOE の前提条件と組織セキュリティ方針を実現するためのものである。 セキュリティ対策方針と対抗する脅威及び対応する組織セキュリティ方針及び前提条件の対応関係を表 8-1に示す。

表 8-1セキュリティ対策方針と対抗する脅威、組織セキュリティ方針及び前提条件

	T.ILLEGAL_LOGON	T.UNAUTHORIZED_ACCESS	T.MODIFY_DB_DATA	T.DISCLOSE_ICC_FILE	T.DISCLOSE_NW_DATA	P.ISSUE	P.AUTHORITY	P.AUDITOR	P.CA_PRIVATE_KEY	P.OS_DB	A.PASSWORD_MANAGEMENT	A.PIN_ICC_MANAGEMENT	A.SAFE_PLACE	A.BACKUP_MEDIA	A.USER_RESTRICTION	A.NETWORK	A.HSM	A.HARDWARE	A.PRIPHERAL_INTERFACE
O.I&A	×						×												
O.ACCESS_CONTROL		×					×												
O.AUDIT	×	×																	
O.DATA_INTEGRITY			×																
O.CRYPTOGRAPHY	×		×	×															
O.ISSUE_CONFIRMATION						×													
OE.ICC_PROTECTION	×																		
OE.CA_PRIVATE_KEY									**x**										
OE.TRUSTED_PATH					×														
OE.TRUSTED_OS_DB										**x**									
OEN.AUTHORIZATION_SETTING	×	×					×	×							×				
OEN.AUTHORIZATION_DUTY	×	×					×												
OEN.PASSWORD_MANAGEMENT											×								
OEN.PIN_ICC_MANAGEMENT												×							
OEN.SAFE_PLACE													×						
OEN.BACKUP_MEDIA														×					
OEN.NETWORK																×			
OEN.HSM_PROTECTION																	×		
OEN.HARDWARE																		×	
OEN.PERIPHERAL_INTERFACE																			×

表 8-1により、各セキュリティ対策方針は１つ以上の脅威、組織のセキュリティ方針および前提条件に対応している。

次に、各脅威がセキュリティ対策方針で対抗できること、また各組織のセキュリティ方針・前提条件がセキュリティ対策方針で実現できることを説明する。

○脅威

T.ILLEGAL_LOGON（不正なログオン）

この脅威は、O.I&A、O.AUDIT、O.CRYPTOGRAPHY、OE.ICC_PROTECTION 、OEN.AUTHORIZATION_SETTING、OEN.AUTHORIZATION_DUTY によって対抗される。

O.I&A により、TOE は、利用者が TOE を利用する前に識別認証されることを保証する(PIN 認証以外)。O.AUDIT により、TOE はログオンの失敗を監査ログに記録する。O.CRYPTOGRAPHY は、操作員証明書を用いる一般操作員の識別・認証にあたり当該操作員証明書の検証を行う。OE.ICC_PROTECTION は、一般操作員の PIN 認証を保証する。OEN.AUTHORIZATION_SETTING により、監査ログ検査者が割り当てられる。 監査ログ検査者は、OEN.AUTHORIZATION_DUTY により与えられた責務を果たすので、監査ログを検査して不正なログオンの試みを察知できる。

T.UNAUTHORIZED_ACCESS（不正なアクセス）

この脅威は、O.ACCESS_CONTROL、O.AUDIT、OEN.AUTHORIZATION_SETTING、OEN.AUTHORIZATION_DUTY によって対抗される。

O.ACCESS_CONTROL により、TOE は利用者とプロセスに権限があるかどうかを判断し、権限があれば利用者とプロセスはリソースにアクセスできるが、権限がなければリソースにアクセスできない。

O.AUDIT により、利用者の TOE 誤用を発見し、異常なユーザ動作を検出する。OEN.AUTHORI ZATION_SETTING により、監査ログ検査者が割り当てられる。 監査ログ検査者は、OEN.AUTHORIZATION_DUTY により与えられた責務を果たすので、監査ログを検査して不正な操作の試みを察知できる。

T.MODIFY_DB_DATA（DB データ改ざん）

この脅威は、O.CRYPTOGRAPHY、O.DATA_INTEGRITY によって対抗される。

O.CRYPTOGRAPHY により、TOE は TSF データ（識別・認証情報、アクセスコントロール情報、監査ログ、アーカイブログ、システム共通鍵、データベース共通鍵）および利用者データ（EE 秘密鍵）を暗号化した上で TOE の IT 環境であるデータベースに格納するので、データベースアクセスによるこれらの TSF データおよび利用者データの暴露を防ぐことができる。O.CRYPTOGRAPHY により、TOE は TSF データ(監査ログ、アーカイブログ)の改ざんを検出する。

また、O.DATA_INTEGRITY により、TOE は、TOE の IT 環境であるデータベースに格納されていた TSF データ（識別・認証情報、アクセスコントロール情報、その他のシステム設定情報）の完全性を確認する手段を提供するので、データベースアクセスによるこれらの TSF データの改ざんを検出できる。

T.DISCLOSE_ICC_FILE（EE IC カード発行情報ファイル暴露）
この脅威は、O.CRYPTOGRAPHY によって対抗される。
O.CRYPTOGRAPHY により、TOE は EE IC カード発行情報ファイルを暗号化するので、CA クライアント端末もしくはRA操作端末に保管されたEE ICカード発行情報ファイルへの直接アクセスによるファイルの暴露を防ぐことができる。

T.DISCLOSE_NW_DATA（ネットワークデータ暴露）
この脅威は OE.TRUSTED_PATH によって対抗される。
OE.TRUSTED_PATH により、CA サブシステム－データベース間の通信には高信頼チャネルを用いるので、CA サブシステム－データベース間のネットワークを流れる TSF データ及び利用者データは暴露から保護される。また、OE.TRUSTED_PATH により、WWW サーバ－WWW クライアント間の通信には高信頼チャネルを用いるので、WWW サーバ－WWW クライアント間のネットワークを流れる TSF データ及び利用者データは暴露から保護される。

○組織のセキュリティ方針

P.ISSUE（発行）
この組織のセキュリティ方針は、O.ISSUE_CONFIRMATION によって実現できる。
O.ISSUE_CONFIRMATION により、すべての証明書、失効リストは認証局秘密鍵(CA 鍵)で署名され、発行された証明書、失効リストが本 TOE で構築された認証局から発行されたということの検証を可能にする。また TOE が発行するすべての証明書及び失効リストの発行履歴を管理する。

P.AUTHORITY（権限付与）
この組織のセキュリティ方針は、OEN.AUTHORIZATION_SETTING、OEN.AUTHORIZATION_DUTY、O.I&A、O.ACCESS_CONTROL によって実現できる。
TOE に関連する権限・役割をもつ利用者（認証局秘密鍵管理者、上級操作員、一般操作員、監査ログ検査者）は OEN.AUTHORIZATION_SETTING により任命される。
OEN.AUTHORIZATION_DUTY により、正当な利用者は与えられた責務を果たし、故意の破壊を行わない。O.I&A により、TOE は上級操作員、一般操作員、監査ログ検査者を識別・認証する。 O.ACCESS_CONTROL は識別・認証された上級操作員、一般操作員、監査ログ検査者が実行しようとする操作に関する権限を有するかどうかを判断し、権限があれば操作を許可し、権限がなければ操作を拒否するので、正当な利用者が権限を持たない操作を行うことを防ぐ。

P.AUDITOR（監査ログ検査者）
この組織のセキュリティ方針は、OEN.AUTHORIZATION_SETTING **によって実現できる。**OEN.AUTHORIZATION_SETTING **により、監査ログ検査者は他の権限を割り当てられない。**

P.CA_PRIVATE_KEY（認証局秘密鍵）
この組織のセキュリティ方針は OE.CA_PRIVATE_KEY **によって実現される。**
OE.CA_PRIVATE_KEY **により、認証局秘密鍵は、**FIPS PUB 140-1 **または** 140-2**、**PKCS **に従って生成・破棄・操作される。**

P.OS_DB（信頼できる OS／DB**）**
この組織のセキュリティ方針は、OE.TRUSTED_OS_DB **により実現できる。**
OE.TRUSTED_OS_DB **により、**OS**・**DB **による適切な識別認証と** OS **によるセキュリティドメインの維持がなされるので、**TOE **のソフトウェアコンポーネントは盗難・破壊・改ざんから保護される。**

○前提条件

A.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）
この前提条件は OEN.PASSWORD_MANAGEMENT **によって実現できる。**
OEN.PASSWORD_MANAGEMENT **により、上級操作員および一般操作員は** TOE **にアクセスするために用いるパスワードを他人に漏洩せず、推測・解析されにくいパスワードを設定し、パスワードを適切な間隔で変更する。**

A.PIN_ICC_MANAGEMENT（一般操作員による PIN**・**IC **カードの管理）**
この前提条件は OEN.PIN_ICC_MANAGEMENT **によって実現できる。**
OEN.PIN_ICC_MANAGEMENT **により、一般操作員は資格喪失時に** IC **カードを裁断して完全に破棄するなどして、**IC **カードが不正利用されないように管理される。また、**OEN.PIN_ICC_MANAGEMENT **により、一般操作員は** IC **カードにアクセスするための** PIN **を他人に漏らさず、推測・解析されにくい** PIN **を設定し、**PIN **を適正な間隔で変更する。**

A.SAFE_PLACE（安全な場所）
この前提条件は、OEN.SAFE_PLACE **によって実現できる。**
OEN.SAFE_PLACE **により、**TOE **に関連するハードウェアは許可された人員のみが入室できるに制御された場所に設置される。**

A.BACKUP_MEDIA（バックアップ媒体）
この前提条件は、OEN.BACKUP_MEDIA **によって実現できる。**
OEN.BACKUP_MEDIA **により、**TOE **のバックアップデータが保存されたリムーバブル媒体は物理的に不正侵入できないように制御された場所に保管され、不正に持ち出せないように管理される。**

A.USER_RESTRICTION（利用者制限）
この前提条件は、OEN.AUTHORIZATION_SETTING **によって実現できる。**
OEN.AUTHORIZATION_SETTING **により、**TOE **の利用者は管理者のみ（上級操作員、一般操作員、監査ログ検査者、**RA **操作員）である。**

A.NETWORK（ネットワーク環境）
この前提条件は OEN.NETWORK **によって実現できる。**
OEN.NETWORK **により、**TOE **の内部ネットワーク（**CA **サーバ端末、**CA **クライアント端末および** RA **操作端末などを含む内部ネットワーク）とそれ以外のネットワークは、適切に設定されたファイアウォールにより隔離されているので、**TOE **は外部ネットワークから保護されている。**

A.HSM（HSM）
この脅威は、OEN.HSM_PROTECTION **によって対抗される。**
OEN.HSM_PROTECTION **により、認証局秘密鍵の生成・管理に** FIPS PUB 140-1 **または** 140-2 **レベル３またはレベル** 3 **相当の** HSM **を用いられ、認証局秘密鍵が物理的に保護される。**

A.HARDWARE（ハードウェア）
この前提条件は、OEN.HARDWARE **により実現できる。**
OEN.HARDWARE **により、**TOE **に関連するハードウェアは正しく動作するものを使用する。**

A.PERIPHERAL_INTERFACE（周辺装置）
この前提条件は、OEN.PERIPHERAL_INTERFACE **により実現できる。**
OEN.PERIPHERAL_INTERFACE **により、**TOE **に接続する周辺装置は** TOE **の付近に設置され、**TOE **と周辺装置の間で盗聴されないように接続される。**

8.2. セキュリティ要件根拠

8.2.1. TOE セキュリティ機能要件根拠

TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 8-2に示す。

表 8-2 TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係

	O.I&A	O.ACCESS_CONTROL	O.AUDIT	O.DATA_INTEGRITY	O.CRYPTOGRAPHY	O.ISSUE_CONFIRMATION
FAU_GEN.1			×			
FAU_GEN.2			×			
FAU_SAR.1			×			
FAU_SAR.2			×			
FAU_SAR.3a			×			
FAU_SAR.3b			×			
FAU_STG.1			×			
FAU_STG.3			×			
FCO_NRO.2						×
FCS_CKM.1a					×	
FCS_CKM.4a					×	
FCS_COP.1a				×	×	
FDP_ACC.1		×				
FDP_ACF.1		×				
FIA_AFL.1a	×					
FIA_ATD.1		×				
FIA_SOS.1a	×					
FIA_SOS.1b	×					
FIA_SOS.1c	×					
FIA_UAU.2a	×					
FIA_UAU.5	×					
FIA_UID.2a	×					
FIA_USB.1		×				
FMT_MOF.1	×	×				
FMT_MTD.1a	×	×				
FMT_MTD.1b	×					
FMT_MTD.1c		×				
FMT_MTD.1d			×			×
FMT_SMF.1		×				
FMT_SMR.2		×				
FPT_RVM.1	×	×				

表 8-2より、各 TOE セキュリティ機能要件が１つ以上の TOE セキュリティ対策方針に対応している。

次に、各 TOE セキュリティ対策方針が、TOE のセキュリティ機能要件及び IT 環境のセキュリティ機能要件で実現できることを説明する。

O.I&A（利用者またはプロセスの確認）

このセキュリティ対策方針は、FIA_AFL.1a、FIA_SOS.1a、FIA_SOS.1b、FIA_SOS.1c、FIA_UAU.2a、FIA_UAU.5、FIA_UID.2a、FMT_MOF.1、FMT_MTD.1a、FMT_MTD.1b、FPT_RVM.1 で実現できる。

FIA_AFL.1a は、利用者認証の失敗を検出し、失敗が一定回数を上回ったとき、当該利用者のアカウントを非活性化する。FIA_SOS.1a、FIA_SOS.1b、FIA_SOS.1c は、秘密（上級操作員および一般操作員のパスワード、データベースにアクセスするためのパスワード、IC カードの PIN）を設定する際、秘密が品質尺度にあっていることを TSF が検証することを要求する。FIA_SOS.1b、FIA_SOS.1c は、IT 環境の秘密（FIA_UAU.2b、FIA_UAU.2c に関わるデータベースにアクセスするためのパスワード、IC カードの PIN）が TOE の求める品質尺度にあっていることを、TOE が当該 IT 環境を使用するにあたって保証するために検証する補完的な機能要件である。FIA_UAU.2a は、上級操作員および一部の一般操作員の利用者認証において、TSF が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する。FIA_UAU.5 は、利用者認証をサポートするため、①操作員 ID とパスワードによる認証、②IC カードに格納された秘密鍵を使用したチャレンジ＆レスポンス認証、③IC カードに格納された証明書の正当性確認による認証、④複数操作員認証の４つの認証メカニズムを持つ。FIA_UID.2a は、上級操作員および一部の一般操作員の利用者識別において、TSF が何らかのアクションを許す前に、各利用者に識別が成功することを要求する。FMT_MOF.1 は、認証方式を決定し、識別認証機能のふるまいを管理する。FMT_MTD.1a、FMT_MTD.1ｂは、正当な役割を有する利用者が識別認証に用いる TSF データ（操作員 ID）、および認証データ（パスワード、PIN、秘密鍵と証明書）を管理することを許す。FPT_RVM.1 は、TOE の機能を動作させる前に、識別認証機能が呼び出され成功することを保証する。

O. ACCESS_CONTROL （アクセスコントロール）

このセキュリティ対策方針は、FIA_ATD.1、FIA_USB.1、FDP_ACC.1、FDP_ACF.1、FMT_MOF.1、FMT_MTD.1a、FMT_MTD.1c、FMT_SMF.1、FMT_SMR.2、FPT_RVM.1 で実現できる。

FIA_ATD.1 は、利用者属性定義、各利用者に対する利用者セキュリティ属性を個別に管理できるようにする。 FIA_USB.1 は、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る。FDP_ACC.1 は、上級操作員および一般操作員と操作対象のリストに従ってアクセス制御を実施する。FDP_ACF.1 は、セキュリティ属性に基づいてアクセス制御されることを規定する。 FMT_MOF.1 はアクセス制御に関するセキュリティ機能のふるまいを管理する。FMT_MTD.1a および FMT_MTD.1c はアクセス制御で用

いるセキュリティ属性に関連するTSFデータを正当な利用者が適切に管理できるようにする。FMT_SMF.1はアクセス制御に関連するセキュリティ管理機能を提供する。FMT_SMR.2でセキュリティ役割を維持し、セキュリティ役割に制限をかける。FPT_RVM.1は、TOEの機能を動作させる前に、アクセス制御機能が呼び出され成功することを保証する。

O.AUDIT（監査）

このセキュリティ対策方針は、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_SAR.3a、FAU_SAR.3b、FAU_STG.1、FAU_STG.3、FMT_MTD.1d 、FPT_STM.1で実現できる。

FAU_GEN.1は、監査対象事象の監査記録を生成する。FAU_GEN.2は各監査対象事象をその原因となった識別情報に関連付ける。FAU_SAR.1は監査記録を読み出せるようにする。FAU_SAR.2は、明示的に読み出しアクセスを許可した利用者を除き、すべての利用者に監査記録の読み出しアクセスを禁止しなければならない。FAU_SAR.3aは、監査データを検索する能力を提供する。 FAU_SAR.3bは、監査データを並べ替えする能力を提供する。FAU_STG.1は、保管された監査記録が不正に削除されないように保護し、また監査記録の改変を検出する。FAU_STG.3は、監査証跡が事前に定義された限界値を超えた場合、TOE停止のアクションをとるようにする。FMT_MTD.1dは、監査ログをTSFデータとして管理する。FPT_STM.1は、監査データ記録に必要な高信頼タイムスタンプを提供する。

O.DATA_INTEGRITY（データの完全性）

このセキュリティ対策方針は、FCS_COP.1aで実現できる。

FCS_COP.1aは、TSFデータ（識別・認証情報、アクセスコントロール情報、その他のシステム設定情報）に対してハッシュ操作（ハッシュ値生成・比較）を行う。

O.CRYPTOGRAPHY（暗号）

このセキュリティ対策方針は、FCS_CKM.1a、FCS_CKM.4a、FCS_COP.1aで実現できる。

FCS_CKM.1aは、指定された標準に基づく特定のアルゴリズムと鍵長に従って暗号鍵が生成されることを要求する。FCS_CKM.4aは指定された特定の破棄方法に従って暗号鍵が破棄されることを要求する。FCS_COP.1aは、指定されたアルゴリズムと指定された鍵長に従って暗号操作がなされることを要求し、利用者データ及びTSFデータのデータベース保管時の暗号化、EE ICカード発行情報の暗号化、及びTSFデータのハッシュ操作を行う。

O.ISSUE_CONFIRMATION（発行確証）

このセキュリティ対策方針は、FCO_NRO.2とFMT_MTD.1dで実現できる。

FCO_NRO.2は、TSFが情報の発信元の証拠を要求する能力を提供する。

FMT_MTD.1d は、証明書および失効リストの発行履歴であるアーカイブログ、さらに証明書および失効リストの発行時に使用するシステム設定情報を TSF データとして管理する。

8.2.2. IT 環境セキュリティ機能要件根拠

IT 環境セキュリティ機能要件と IT 環境セキュリティ対策方針の対応関係を表 8-3に示す。

表 8-3 IT 環境セキュリティ機能要件と IT 環境セキュリティ対策方針の対応関係

	OE.ICC_PROTECTION	OE.CA_PRIVATE_KEY	OE.TRUSTED_PATH	OE.TRUSTED_OS_DB
FCS_CKM.1b		×		
FCS_CKM.4b		×		
FCS_COP.1b		×		
FIA_AFL.1b	×			
FIA_UAU.2b				×
FIA_UAU.2c	×			
FIA_UAU.2d				×
FIA_UID.2b				×
FIA_UID.2c	×			
FIA_UID.2d				×
FPT_SEP.1				×
FTP_ITC.1a			×	
FTP_ITC.1b			×	
FPT_STM.1				×

表 8-3より、各 IT 環境セキュリティ機能要件が１つ以上の IT 環境セキュリティ対策方針に対応している。

次に、各 IT 環境セキュリティ対策方針が、IT 環境セキュリティ機能要件で実現できることを説明する。

OE.ICC_PROTECTION（IC カードの保護）

このセキュリティ対策方針は、FIA_AFL.1b、FIA_UAU.2c、FIA_UID.2c で実現できる。FIA_AFL.1b は、利用者認証の失敗を検出し、失敗が一定回数を上回ったとき、当該利用者の IC カードへの PIN 入力インタフェースを非活性化する。 FIA_UAU.2c は、アクション前の利用者認証において、IC カードがアクションを許可する前に、当該利用者に認証が成

功することを要求する。FIA_UID.2c は、アクション前の利用者識別において、IC カードが何らかのアクションを許す前に、当該利用者に識別が成功することを要求する。

OE.CA_PRIVATE_KEY（認証局秘密鍵）
このセキュリティ対策方針は、FCS_COP.1b、FCS_CKM.1b、FCS_CKM.4b で実現できる。
FCS_COP.1b は、標準である PKCS#1 で指定されたアルゴリズムと指定された鍵長に従って暗号操作がなされることを要求する。FCS_CKM.1b は、FIPS PUB 140-1 または 140-2 に基づく特定のアルゴリズムと鍵長に従って暗号鍵が生成されることを要求する。FCS_CKM.4b は FIPS PUB 140-1 または 140-2 に基づく特定の破棄方法に従って暗号鍵が破棄されることを要求する。

OE.TRUSTED_PATH（高信頼チャネル）
このセキュリティ対策方針は、FTP_ITC.1a、FTP_ITC.1b で実現できる。
FTP_ITC.1a は、データベースと TOE（CA サブシステム）の間で送信されるデータを送信中の不当な改変や暴露からチャンネルデータの保護を提供する通信チャンネルを提供する。FTP_ITC.1b は、WWW クライアントと WWW サーバの間で送信されるデータを送信中の不当な改変や暴露からチャンネルデータの保護を提供する通信チャンネルを提供する。

OE.TRUSTED_OS_DB（信頼できる OS／DB）
このセキュリティ対策方針は、FIA_UAU.2b、FIA_UAU.2d、FIA_UID.2b、FIA_UID.2d、FPT_SEP.1、FPT_SMT.1 で実現できる。
FIA_UAU.2b は、アクション前の利用者認証において、データベースがアクションを許可する前に、利用者に認証が成功することを要求する。FIA_UAU.2d は、アクション前の利用者認証において、オペレーティングシステムが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する。FIA_UID.2b は、アクション前の利用者識別において、データベースが何らかのアクションを許す前に、利用者に識別が成功することを要求する。FIA_UID.2d は、アクション前の利用者識別において、オペレーティングシステムが何らかのアクションを許す前に、各利用者に識別が成功することを要求する。FPT_SEP.1 は、TSF の実行のため、信頼できないサブジェクトによる妨害と改ざんから TSF を保護するためのセキュリティドメインを維持する。FPT_SMT.1 はオペレーティングシステムが TOE の監査ログ出力に必要な信頼できるタイムスタンプ情報を提供する。

8.2.3. 最小機能強度レベル根拠

EE 証明書は、EE の秘密鍵と対になる公開鍵に CA 局の秘密鍵で署名したものである。CA 局自身の信頼性が失われた場合は、その CA 局が発行した EE 証明書を用いた公開鍵認証システム自体が正常に機能しなくなる。しかし、TOE は 3.2 前提条件で述べたように物理的・

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程度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」つまり低レベルの脅威エージェントに対する対策を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。

8.2.4. セキュリティ機能要件依存性

セキュリティ要件のコンポーネントの依存性を表 8-4に示す。依存するコンポーネントは「×」、選択可能なコンポーネントで選択した直接依存するコンポーネントは「○」で表している。CC パート２で規定されている依存コンポーネントの上位階層になっているコンポーネントには「^」、除去されたコンポーネントには「*」、一部だけ対応するコンポーネントには「$」をつけている。

表 8-4　セキュリティ要件のコンポーネントの依存性

	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1a	FCS_CKM.1b	FCS_CKM.4a	FCS_CKM.4b	FCS_COP.1a	FCS_COP.1b	FDP_ACC.1	FDP_ACF.1	FIA_ATD.1	FIA_UAU.2a	FIA_UAU.2c	FIA_UID.2a	FIA_UID.2b	FIA_UID.2c	FIA_UID.2d	FMT_MSA.2(※1)	FMT_MSA.2(※2)	FMT_MSA.3	FMT_MTD.1a	FMT_MTD.1b	FMT_MTD.1c	FMT_MTD.1d	FMT_SMF.1	FMT_SMR.2	FPT_STM.1
FAU_GEN.1																												×
FAU_GEN.2	×														× ^													
FAU_SAR.1	×																											
FAU_SAR.2		×																										
FAU_SAR.3a		×																										
FAU_SAR.3b		×																										
FAU_STG.1	×																											
FAU_STG.3			×																									
FCO_NRO.2															× ^													
FCS_CKM.1a						○		○ $											× *									
FCS_CKM.1b							○		○											× *								
FCS_CKM.4a				○															× *									
FCS_CKM.4b					○															× *								
FCS_COP.1a				○ $	× $	○	× $												× *									
FCS_COP.1b					○		○													× *								
FDP_ACC.1											×																	
FDP_ACF.1										×											× *							
FIA_AFL.1a													× ^															
FIA_AFL.1b														× ^														
FIA_ATD.1																												

FIA_SOS.1a																											
FIA_SOS.1b																											
FIA_SOS.1c																											
FIA_UAU.2a														× ^													
FIA_UAU.2b															× ^												
FIA_UAU.2c																× ^											
FIA_UAU.2d																	× ^										
FIA_UAU.5																											
FIA_UID.2a																											
FIA_UID.2b																											
FIA_UID.2c																											
FIA_UID.2d																											
FIA_USB.1												×															
FMT_MOF.1																									×	× ^	
FMT_MTD.1a																									×	× ^	
FMT_MTD.1b																									×	× ^	
FMT_MTD.1c																									×	× ^	
FMT_MTD.1d																									×	× ^	
FMT_SMF.1																									×	× ^	
FMT_SMR.2														× ^													
FPT_RVM.1																											
FPT_SEP.1																											
FPT_STM.1																											
FTP_ITC.1a																											
FTP_ITC.1b																											

注釈：網掛部分 は IT 環境セキュリティ機能要件の依存性、それ以外の部分は TOE セキュリティ機能要件の依存性を示す。FMT_MSA.2(※1)／FMT_MSA.2(※2)、および FMT_MSA.3 は TOE／IT 環境セキュリティ機能要件としては挙げられていないが、除去されたコンポーネントとして示すために記述した。

表 8-4より、TOE セキュリティ機能要件及び IT 環境セキュリティ機能要件は後述する例外を除きそれぞれの必要な依存関係をすべて満たしている(FCS_COP.1a から FCS_CKM.1 への依存関係は、CA 公開鍵以外は FCS_CKM.1a、CA 公開鍵は FCS_CKM.1b によって満たされる)。一部の依存するコンポーネントは、CC パート２で規定されている依存コンポーネントの上位階層になっている。

FCS_CKM.1a の依存関係は一部満たされていないが、問題がない根拠を以下に示す。 また、FCS_CKM.1a、FCS_CKM.4a、FCS_COP.1a 、FCS_CKM.1b、FCS_CKM.4b、FCS_COP.1b から FMT_MSA.2(※1)、FMT_MSA.2(※2)への依存関係、FDP_ACF.1 から FMT_MSA.3 への依存関係は満たされないが、問題がない根拠を以下に示す。

・FCS_CKM.1a → FCS_COP.1a

EE 鍵は EE 証明書利用者（一般利用者）による暗号操作で用いられるものなので、この依存関係は不要である。操作員秘密鍵は一般操作員による暗号操作で用いられるものなので、この依存関係は不要である。

・FCS_CKM.1a、FCS_CKM.4a、FCS_COP.1a → FMT_MSA.2(※1)
FCS_CKM.1b、FCS_CKM.4b、FCS_COP.1b → FMT_MSA.2(※2)

暗号鍵は管理されるセキュリティ属性を持たないため、セキュリティ属性がセキュアな状態に関して有効であることを保証する必要はない。FCS_COP.1a におけるハッシュ（SHA-1、MD5）では、暗号鍵自体がないため、セキュリティ属性もないので FMT_MSA.2(※1)は不要である。

・FDP_ACF.1 → FMT_MSA.3

アクセス制御に使用するセキュリティ属性である操作員種別と所属する権限グループは、FIA_ATD.1 で維持され、FIA_USB.1 によりサブジェクトに値が割り当てられる。このため静的属性初期化の要件は不要である。

8.2.5. セキュリティ機能要件相互補完性

前節より、TOE セキュリティ機能要件及び IT 環境セキュリティ機能要件は、一部の例外を除き、それぞれと依存関係のある機能要件と相互補完している。
これらの機能要件以外で、明示的な依存関係はないが、以下の観点から相互補完する機能要件について記述する。

＜バイパス防止＞
FPT_RVM.1 により、TSC 内の各機能の動作進行が許可される前に、識別認証機能（FIA_UAU.2a、FIA_UID.2a）、アクセス制御機能（FDP_ACC.1、FDP_ACF.1）が呼び出され成功することが保証される。
<改ざん防止>
IT 環境である OS/DB の実施機能である FPT_SEP.1 により、OS/DB 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/DB 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権限が付与された上級操作員または一般操作員に制限され、信頼できないサブジェクトによる TSF の非活性化を防止する。
＜無効化＞
FAU_GEN.1 により、証明書発行、アクセス権限設定、アクセス拒否など監査データ生成

に関わるセキュリティ機能要件（FCO_NRO.2、FDP_ACF.1、FIA_UAU.2a、FIA_UID.2a、FMT_MOF.1、FMT_SMR.2）の無効化を狙った攻撃の検出が可能になる。FAU_GEN.1 がこれらの機能に関する監査データを記録することにより、TSF の無効化に対する監視の能力を高め、セキュリティ侵害につながる不正行為を抑止する。

8.2.6. 監査対象事象根拠

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後述の例外を除き、本 TOE の監査対象事象と対応している。

次に、監査対象とすべき最小レベルのアクション（CC における規定)のうち、本 TOE における監査対象に含まれない根拠を説明する。

表 8-5 最小レベルのアクション除外の根拠

機能要件	監査対象とすべき最小レベルのアクション	根拠
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	TOE は、CA サーバコンソール・CA クライアントコンソール上での監査ログ参照を記録しないが、監査管理（監査データの外部ファイル出力および印刷）に関わる監査記録からの情報読み出しを記録する。コンソール上の監査ログ参照は、監査ログ参照のアクセス権限を付与された上級操作員・一般操作員のみに許可されており、コンソール上の監査ログ参照が監査対象事象に含まれなくても TOE セキュリティ対策方針上問題ない。
FAU_SAR.3a FAU_SAR.3b	a) 詳細: 閲覧に使用されるパラメータ。	TOE は、限られた利用者（監査ログ参照のアクセス権限を付与された上級操作員・一般操作員）のみに監査ログ参照を許可しており、検索・並べ替えに使用するパラメータを監査対象事象とする必要はない。
FAU_STG.3	a) 基本: 閾値を超えたためにとられるアクション。	TOE は、監査証跡が CA セットアップ時に指定した容量を超えた場合、TOE の運用を停止するので、監査対象事象に含まれなくても TOE セキュリティ対策方針上問題ない。
FIA_SOS.1a FIA_SOS.1b FIA_SOS.1c	a) 最小: TSF による、テストされた秘密の拒否;	TOE は、TOE の定める品質尺度を満たさない秘密を拒否する（すなわち、TOE 上受入れられたパスワード/PIN はすべて品質尺度を満足している）ので、本アクションが監査対象事象に含まれなくても、TOE セキュリティ対策方針上問題ない。

8.2.7. セキュリティ保証要件根拠

PKI サーバ／Carassuit 電子政府版 ver3.1 は、PKI（公開鍵基盤）システムを実現するための認証局、登録局機能を提供し、利用者へ公開鍵証明書を発行する製品であるので、セキュリティ機能には高い信頼性が要求される。 一方で、高い保証レベルの評価にはそれなりのコストがかかるため、製品の価格に影響を及ぼすことも事実である。 それらを考慮すると、EAL3 は TOE の開発段階のセキュリティ対策の分析（系統だったテストの実施と分析、開発環境や開発生産物の管理状況の評価）を含むという点で妥当な選択であるといえる。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係を表 8-6に示す。

表 8-6 TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3a	FAU_SAR.3b	FAU_STG.1	FAU_STG.3	FCO_NRO.2	FCS_CKM.1a	FCS_CKM.4a	FCS_COP.1a	FDP_ACC.1	FDP_ACF.1	FIA_AFL.1a	FIA_ATD.1	FIA_SOS.1a	FIA_SOS.1b	FIA_SOS.1c	FIA_UAU.2a	FIA_UAU.5	FIA_UID.2a	FIA_USB.1	FMT_MOF.1	FMT_MTD.1a	FMT_MTD.1b	FMT_MTD.1c	FMT_MTD.1d	FMT_SMF.1	FMT_SMR.2	FPT_RVM.1
SF.Audit	×	×	×		×	×	×	×																							
SF.I&A															×		×	×	×	×	×	×									×
SF.ACC			×	×			×						×	×		×							×	×	×	×	×	×	×	×	×
SF.Crypto							×			×	×	×																	×		
SF. Cer_Issue									×																				×		

表 8-6より、各 TOE セキュリティ機能が１つ以上の TOE セキュリティ機能要件に対応している。

次に、各 TOE セキュリティ機能要件が、TOE セキュリティ機能で実現できることを説明する。

FAU_GEN.1 監査データ生成

SF.Audit は、以下の監査対象事象の監査記録を生成する。

- 監査機能の起動と終了
- 操作員の識別と確認
- CA サーバコンソール機能および CA クライアントコンソール機能の起動／停止
- CA メイン機能の起動／停止
- 操作員の登録／削除／編集
- アクセス権限の設定
- ポリシーの設定
- バックアップ／リカバリの実行
- 証明書要求の発行
- 証明書の発行
- 証明書の失効
- 証明書の出力
- 証明書要求の審査
- CRL／ARL の発行
- CRL／ARL の出力

- EE IC カード発行情報ファイルの出力
- システム環境設定
- スケジュールの設定
- 監査データの削除／外部出力
- アーカイブデータの削除／外部出力
- ユーザ情報の登録／削除／編集
- CA のセットアップ
- CA 鍵の変更
- CA 証明書の失効
- データベースパスワードの変更
- アクセスの拒否（操作員の識別と確認の失敗、アクセス権限のない操作の試み）

表 8-7は、各機能要件を選択した場合に監査対象とすべきアクション(CC における規定)と、それに関連する監査対象事象とを示す。

表 8-7 監査対象とすべきアクション（CC における規定)と関連する監査対象事象

機能要件	監査対象とすべきアクション	監査対象事象
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	一部記録（後述）
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) アクセスの拒否
FAU_SAR.3a	a) 詳細: 閲覧に使用されるパラメタ。	なし（後述）
FAU_SAR.3b	a) 詳細: 閲覧に使用されるパラメタ。	なし（後述）
FAU_STG.1	なし	なし
FAU_STG.3	a) 基本: 閾値を超えたためにとられるアクション。	なし（後述）
FCO_NRO.2	a) 最小: 否認不可サービスの呼出。 b) 基本: 情報、宛先、提供された証拠のコピーの識別。 c) 詳細: 証拠の検証を要求した利用者の識別情報。	a) 証明書の発行 a) CRL／ARL の発行 a) CA のセットアップ a) CA 鍵の変更
FCS_CKM.1a	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	a) CA のセットアップ a)操作員の登録 a) EE IC カード発行情報ファイルの出力
FCS_CKM.4a	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	a) CA 鍵の変更 a) 操作員の削除
FCS_COP.1a	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) 操作員の識別と確認 a) アクセス権限の設定 a) バックアップ／リカバリの実行 a) 証明書要求の発行 a) EE IC カード発行情報ファイルの出力 a) システム環境設定 a) 監査データの外部出力 a) アーカイブデータの外部出力
FDP_ACC.1	なし	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。	以下の操作についての情報 a), b), c) CA メイン機能 a), b), c) CA の鍵情報の参照機能 a), b), c)バックアップ、リカバリ機能

	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)アクセスコントロール（操作員管理）機能 a), b), c)ARL の外部出力機能 a), b), c) CRL の外部出力機能 a), b), c)アーカイブデータの外部出力機能 a), b), c)アーカイブデータの参照、検索機能 a), b), c)システムパラメータの設定機能 a), b), c)スケジュール管理の設定機能 a), b), c)証明書プロファイルの新規登録、 a), b), c)変更、削除機能 a), b), c)監査データの参照及び検索機能 a), b), c)監査データの外部ファイル出力、印刷機能 a), b), c)発行済みの証明書および処理中の証明書要求の一覧表示機能 a), b), c)機関証明書プロファイルでの証明書の申請機能 a), b), c)機関証明書プロファイルで発行された証明書の出力機能 a), b), c)機関証明書プロファイルで発行された証明書の失効機能 a), b), c)ユーザ管理機能 a), b), c) EE 証明書プロファイルでの証明書の申請機能 a), b), c) EE 証明書プロファイルで申請された証明書の審査機能 a), b), c) EE 証明書プロファイルで発行された証明書の出力機能 a), b), c) EE 証明書プロファイルで発行された証明書の失効機能 a), b), c) EE 鍵／証明書を IC カードへ格納する形式のファイルの生成機能
FIA_AFL.1a	a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	a) 認証試行の不成功が規定回数を超えたこと及びそれに伴うアカウントのロック
FIA_ATD.1	なし	なし
FIA_SOS.1a	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	a) なし（後述） b) 操作員の登録／編集
FIA_SOS.1b	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	a) なし（後述） b) 操作員の登録／編集
FIA_SOS.1c	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	a) なし（後述） b) データベースパスワードの変更
FIA_UAU.2a	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	a), b) 操作員の識別と確認 a), b) アクセスの拒否
FIA_UAU.5	a) 最小: 認証の最終決定; b) 基本: 最終決定で共に用いられた、各々の稼動し	a), b) 操作員の識別と確認

	たメカニズムの結果。	
FIA_UID.2a	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) 操作員の識別と確認
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) 操作員の識別と確認
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) アクセス権限の設定 a) 操作員の登録／削除／編集
FMT_MTD.1a	a) 基本: TSF データの値のすべての改変。	a) 操作員の登録／削除／編集 a) CA のセットアップ
FMT_MTD.1b	a) 基本: TSF データの値のすべての改変。	a) 操作員の編集（ﾊﾟｽﾜｰﾄﾞ、PIN 変更）
FMT_MTD.1c	a) 基本: TSF データの値のすべての改変。	a) 操作員グループの登録／削除 a) 操作員グループへのアクセス権限の割当
FMT_MTD.1d	a) 基本: TSF データの値のすべての改変。	a) システム環境設定 a) CA のセットアップ
FMT_SMF.1	a) 最小：管理機能の使用	a) 操作員の登録／削除／編集 a) アクセス権限の設定 a) システム環境設定 a) CA のセットアップ a) 監査データの削除、外部出力 a) アーカイブデータの削除、外部出力
FMT_SMR.2	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) 最小: 役割に対して与えられた条件のために成功しなかった、その役割を使用する試み; c) 詳細: 役割の権限の使用すべて。	a) 操作員の登録／削除／編集 a) 操作員グループの登録／削除 a) 操作員グループへのアクセス権限の割当 b) アクセスの拒否
FPT_RVM.1	なし	なし

次に、各機能要件を選択した場合に、監査対象とすべき最小レベルのアクション(CC における規定)の内、本 TOE における監査対象事象に含まれないものとその根拠を示す。

機能要件	監査対象とすべき最小レベルのアクション	根拠
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	TOE は、CA サーバコンソール・CA クライアントコンソール上での監査ログ参照を記録しないが、監査管理（監査データの外部ファイル出力および印刷）に関わる監査記録からの情報読み出しを記録する。コンソール上の監査ログ参照は、監査ログ参照のアクセス権限を付与された上級操作員・一般操作員のみに許可されており、コンソール上の監査ログ参照が監査対象事象に含まれなくても TOE セキュリティ対策方針上問題ない。
FAU_SAR.3a FAU_SAR.3b	a) 詳細: 閲覧に使用されるパラメタ。	TOE は、限られた利用者（監査ログ参照のアクセス権限を付与された上級操作員・一般操作員）のみに監査ログ参照を許可しており、検索・並べ替えに使用するパラメタを監査対象事象とする必要はない。
FAU_STG.3	a) 基本: 閾値を超えたためにとられるアクション。	TOE は、監査証跡が CA セットアップ時に指定した容量を超えた場合、TOE の運用を停止するので、監査対象事象に含まれなくても TOE セキュリティ対策方針上問題ない。
FIA_SOS.1a FIA_SOS.1b FIA_SOS.1c	a) 最小: TSF による、テストされた秘密の拒否;	TOE は、TOE の定める品質尺度を満たさない秘密を拒否する（すなわち、TOE 上受入れられたパスワード/PIN はすべて品質尺度を満足している）ので、本アクションが監査対象事象に含まれなくても、TOE

		セキュリティ対策方針上問題ない。

以下は、機能要件毎の監査対象とすべきアクション(CC における規定)との対応はないが、TOE セキュリティ対策方針を実現するために必要な監査対象事象である。

- CA サーバコンソール機能および CA クライアントコンソール機能の起動／停止
- ポリシーの設定
- 証明書要求の審査
- スケジュールの設定
- 監査データの削除
- アーカイブデータの削除
- CA 証明書の失効

また、SF.Audit は、各監査記録において少なくとも以下の情報を記録する。

- 順次番号。監査データ 1 件ごとに割り当てられる番号。
- 操作員 ID。システムに登録されている上級操作員、一般操作員の ID。
- 事象の種別。事象の分類を表すもの。” システム起動 ”、” 証明書発行 ” など。
- メッセージ。事象の詳細な内容を表すもの。
- 事象の結果。成功、失敗（警告）、失敗（エラー）の３種類。
- 事象の日付・時刻。OS から取得したタイムスタンプ情報を使用する。
- 拡張情報。メッセージに付随するコード、具体的な対象名、ステータスなどに類する補足情報。
- ハッシュ値。監査データの改ざんチェックに使用する内部データ。

監査データを生成する主体となるプロセスは全て操作員が関連している。各プロセスのサブジェクトは関連する操作員 ID で一意に識別可能である。従って、本 TOE ではサブジェクト識別情報と操作員 ID を同一のものとして、監査データを生成している。

従って、SF.Audit により、FAU_GEN.1 を実現できる。

FAU_GEN.2 利用者識別情報の関連付け

SF.Audit は、監査記録時に操作員 ID を記録することによって、各監査対象事象をその原因となった上級操作員もしくは一般操作員の識別情報に関連づけている。

従って、SF.Audit により、FAU_GEN.2 を実現できる。

FAU_SAR.1 監査レビュー

SF.ACC により、監査ログ検査者として許可された特定の上級操作員及び一般操作員に監査ログ参照権限を付与する。また、SF.Audit は監査ログ参照権限を付与された上級操作員及

び一般操作員が監査情報リスト（順次番号、操作員 ID、事象の種別、メッセージ、事象の結果（成功または失敗）、事象の日付・時刻、拡張情報、ハッシュ値）を監査記録から CA サーバコンソールもしくは CA クライアントコンソールを用いて読み出せるようにしている。
従って、SF.ACC と SF.Audit により、FAU_SAR.1 を実現できる。

FAU_SAR.2 限定監査レビュー
SF.ACC は、特定の上級操作員もしくは一般操作員に監査ログ参照権限を付与し、明示的に監査記録の読み出しアクセスを許可する。
従って、SF.ACC により、FAU_SAR.2 を実現できる。

FAU_SAR.3a 選択可能監査レビュー
SF.Audit は、操作員 ID・事象の種別・事象の日付・時刻・事象の結果（成功および／または失敗）という条件で監査データを検索する能力を提供する。
従って、SF.Audit により、FAU_SAR.3a を実現できる。

FAU_SAR.3b 選択可能監査レビュー
SF.Audit は、順次番号、操作員 ID、事象の種別、メッセージ、事象の結果（成功または失敗）、事象の日付・時刻、拡張情報という条件で監査データを並べ替えする能力を提供する。
従って、SF.Audit により、FAU_SAR.3b を実現できる。

FAU_STG.1 保護された監査証跡保管
SF.Audit は、SF.ACC を用いて、特定の上級操作員もしくは一般操作員に監査管理権限を付与し、明示的に監査記録の削除を許可し、保管された監査記録が不正に削除されないように保護する。SF.Audit は、以下の監査データ保護機能により、保管された監査記録に対する改変を検知する。
<監査データ保護機能>

- 現在 TOE 内に存在するはずの監査データの順次番号（開始番号と終了番号）を管理する。また、順次番号の開始番号と終了番号との間で、監査データが連続していることを検証する。
- 監査データは、SF.Crypto によって導出したハッシュ値を保持する。このハッシュ値は、監査データを参照、外部出力する際に検証される。
- 監査データは、順次番号と事象の日付・時刻を除くすべての項目が暗号化されて保管される。これによって、監査データの暴露を防ぐ。
- 監査データの連続性の確認。TOE に存在する最初の監査データの順次番号が管理している開始番号と一致しない場合や、最後の監査データの順次番号が管理している終了番

号と一致しない場合、また、監査データの順次番号が連続していない場合には、監査データが消失していることを監査ログ検査者に知らせる。

- 監査データの完全性の確認。SF.Crypto によって監査データのハッシュ値を計算し、監査データの完全性を検証する。監査データの改ざんを検知した場合には、これを操作員に知らせる。

従って、SF.ACC と SF.Audit、および SF.Crypto により、FAU_STG.1 を実現できる。

FAU_STG.3 監査データ損失の恐れ発生時のアクション

SF.Audit は、監査証跡が、上級操作員が CA のセットアップ時に指定したパラメータに基づいて決定された監査データ格納用の領域サイズを超えた場合、TOE の運用を停止する。

従って、SF.Audit により、FAU_STG.3 を実現できる。

FCO_NRO.2 発信の強制的証明

SF.Cer_Issue は、送信された以下の証明書リスト及び失効リストの発信元の証拠の生成を常に実施する。

<証明書リスト・失効リスト>

{CA 証明書、機関証明書、操作員証明書、EE 証明書、CRL、ARL}

SF.Cer_Issue は、情報の発信者の CA 証明書のサブジェクト名と CA 公開鍵を、証拠が適用される情報の発行者名と CA の署名値に関係付けることができる。

SF.Cer_Issue は、検証者へ、CA 証明書の有効期間の範囲で、情報の発信元の証拠を検証する能力を提供する。

従って、SF.Cer_Issue は、FCO_NRO.2 を実現できる。

FCS_CKM.1a 暗号鍵生成

SF.Crypto は、以下の標準のリストに合致する、指定された暗号鍵生成アルゴリズムと指定された暗号鍵長に従って、暗号鍵を生成する。

＜標準のリスト＞

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
EE 鍵ペア（RSA）	・ ANSI X9.31 Appendix A.2.4 Using AES(注 1) ・PKCS #1	・疑似乱数生成アルゴリズム ・PKCS#1	512bit, 768bit, 1024bit, 2048bit から選択
操作員鍵ペア（RSA）	・ ANSI X9.31 Appendix A.2.4 Using AES(注 1) ・PKCS #1	・疑似乱数生成アルゴリズム ・PKCS#1	512bit, 768bit, 1024bit, 2048bit から選択

システム共通鍵 （Triple DES）	ANSI X9.31 Appendix A.2.4 Using AES(注 1)	疑似乱数生成アルゴリズム	168bit
データベース共通鍵 （Triple DES）	ANSI X9.31 Appendix A.2.4 Using AES(注 1)	疑似乱数生成アルゴリズム	168bit
共通鍵保護鍵	なし（注２）	非公開独自方式(注２)	168bit
EE IC カード発行情報ファイル保護鍵 （Triple DES）	FIPS PUB 180-1	SHA-1 (元データをハッシュ演算で加工することで鍵としている)	168bit

（注１） これは、独立行政法人 情報処理推進機構、独立行政法人 情報通信研究機構の暗号モジュール評価基準(米国 NIST が発行する”FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE (12-03-2002)”の翻訳版)の”Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules “で承認された疑似乱数生成アルゴリズムとされているものである。

（注２） 固有の元データを加工する非公開独自方式を採用している。

従って、SF.Crypto により、FCS_CKM.1a を実現できる。

FCS_CKM.４a 暗号鍵破棄

SF.Crypto は、データベースなどに格納している暗号鍵を破棄する場合には、暗号鍵を格納していた領域をダミーデータ（乱数やゼロデータなどの意味のないデータ）で上書きした後、領域を解放する。

従って、SF.Crypto により、FCS_CKM.4a を実現できる。

FCS_COP.1a 暗号操作

SF.Crypto は、以下の暗号操作のリストに合致する、特定された暗号アルゴリズムと指定された暗号鍵長に従って、暗号操作を行う。

<暗号操作のリスト>

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
CA 公開鍵	PKCS#1	RSA	512bit, 768bit, 1024bit, 2048bit から選択	・操作員証明書の署名検証 ・CRL の署名検証
操作員秘密鍵／公開	PKCS#1	RSA	512bit,	認証用のチャレンジの署名および署名検証

鍵			768bit, 1024bit, 2048bit から選択	
システム共通鍵	FIPS PUB 46-3	Triple DES	168bit	・アクセスコントロール情報の登録時の暗号化と参照時の復号 ・監査データ(1 レコードづつ)の登録時の暗号化と参照時の復号 ・アーカイブデータ(1 レコードづつ)の登録時の暗号化と参照時の復号 ・データベース用パスワードの保管時の暗号化と参照時の復号
データベース共通鍵	FIPS PUB 46-3	Triple DES	168bit	EE 秘密鍵の保管時の暗号化取り出し時の復号
共通鍵保護鍵	FIPS PUB 46-3	Triple DES	168bit	システム共通鍵、データベース共通鍵の保管時の暗号化と参照時の復号
EE IC カード発行情報ファイル保護鍵	FIPS PUB 46-3	Triple DES	168bit	EE IC カード発行情報ファイルの暗号化
パスフレーズから生成する共通鍵	FIPS PUB 46-3	Triple DES	168bit	・機関証明書と秘密鍵の PKCS#12 出力時の秘密鍵暗号化 ・EE 証明書と秘密鍵の PKCS#12 出力時の秘密鍵暗号化
なし	FIPS PUB 180-1	SHA-1	―	識別・認証情報のハッシュ操作 アクセスコントロール情報のハッシュ操作 システム設定情報のハッシュ操作 監査ログのハッシュ操作 アーカイブデータのハッシュ操作 注) ハッシュ操作とは、ハッシュ値生成および比較である
なし	RFC1321	MD5	―	

従って、SF.Crypto により、FCS_COP.1a を実現できる。

FDP_ACC.1 サブセットアクセス制御

SF.ACC は、上級操作員プロセスと一般操作員プロセスによる以下の機能の実行をアクセス制御する。

サブジェクト	機能	操作
操作員プロセス	CA メイン機能	実行
	CA の鍵情報の参照機能	
	バックアップ、リカバリ機能	
	アクセスコントロール（操作員管理）機能	
	ユーザ管理	
	ARL の外部出力機能	
	CRL の外部出力機能	
	アーカイブデータの外部出力機能	
	アーカイブデータの参照、検索機能	
	システムパラメータの設定機能	
	スケジュール管理の設定機能	
	証明書プロファイルの新規登録、変更、削除機能	
	監査データの参照、検索機能	
	監査データの外部ファイル出力、印刷機能	

	発行済みの証明書および処理中の証明書要求の一覧表示機能	
	機関証明書プロファイルでの証明書の申請機能	
	機関証明書プロファイルで発行された証明書の出力機能	
	機関証明書プロファイルで発行された証明書の失効機能	
	EE 証明書プロファイルでの証明書の申請機能	
	EE 証明書プロファイルで申請された証明書の審査機能	
	EE 証明書プロファイルで発行された証明書の出力機能	
	EE 証明書プロファイルで発行された証明書の失効機能	
	EE 鍵／証明書を IC カードへ格納する形式のファイルの生成機能	

従って、SF.ACC により、FDP_ACC.1 を実現できる。

FDP_ACF.1 セキュリティ属性によるアクセス制御

SF.ACC は、権限グループに付与されたアクセス権限を確認することにより、各アクセス権限が付与された権限グループに所属する上級操作員プロセスおよび一般操作員プロセスに対する以下のアクセス制御を実施する。

制御されたサブジェクト	制御されたオブジェクト	制御された操作
CA メイン機能の起動／停止のアクセス権限が付与された権限グループに所属する上級操作員プロセス	CA メイン機能	実行
CA 鍵管理のアクセス権限が付与された権限グループに所属する上級操作員プロセス	CA の鍵情報の参照機能	
バックアップ／リカバリのアクセス権限が付与された権限グループに所属する上級操作員プロセス	バックアップ、リカバリ機能	
操作員管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	アクセスコントロール（操作員管理）機能	
ARL 出力のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	ARL の外部出力機能	
CRL 出力のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	CRL の外部出力機能	
アーカイブ管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	アーカイブデータの外部出力機能	
アーカイブ参照のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	アーカイブデータの参照、検索機能	
システム環境設定のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	システムパラメータの設定機能	
スケジュール管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	スケジュール管理の設定機能	
ポリシー管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	証明書プロファイルの新規登録、変更、削除機能	

監査ログ参照のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	監査データの参照及び検索機能	
監査管理のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	監査データの外部ファイル出力、印刷機能	
証明書情報参照のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	発行済みの証明書および処理中の証明書要求の一覧表示機能	
機関証明書申請のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	機関証明書プロファイルでの証明書の申請機能	
機関証明書取得のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	機関証明書プロファイルで発行された証明書の出力機能	
機関証明書失効のアクセス権限が付与された権限グループに所属する上級操作員／一般操作員プロセス	機関証明書プロファイルで発行された証明書の失効機能	
ユーザ管理のアクセス権限が付与された権限グループに所属する一般操作員プロセス	ユーザ管理機能	
EE 証明書申請のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルでの証明書の申請機能	
EE 証明書審査のアクセス制限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルで申請された証明書の審査機能	
EE 証明書取得のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルで発行された証明書の出力機能	
EE 証明書失効のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE 証明書プロファイルで発行された証明書の失効機能	
EE IC カード発行のアクセス権限が付与された権限グループに所属する一般操作員プロセス	EE鍵／証明書をICカードへ格納する形式のファイルの生成機能	

従って、SF.ACC により、FDP_ACF.1 を実現できる。

FIA_AFL.1a 認証失敗時の取り扱い

SF.I&A は、操作員 ID とパスワードを用いる操作員の認証失敗が定められた試行可能回数に達すると、当該操作員のアカウントをロックし、解除不可能にする。

従って、SF.I&A により、FIA_AFL.1a を実現できる。

FIA_ATD.1 利用者属性定義

SF.ACC は、個々の利用者に属する以下のセキュリティ属性リストを維持する。

- 操作員種別（上級操作員、一般操作員）
- 所属する権限グループ

従って、SF.ACC により、FIA_ATD.1 を実現できる。

FIA_SOS.1a 秘密の検証

SF.I&A は、上級操作員および一部の一般操作員の操作員認証に使用するパスワードが以下

の品質尺度を満たすことを検証するメカニズムを提供する。

- 長さ: 6 文字～32 文字
- 使用可能な文字: 半角英数記号文字

従って、SF.I&A により、FIA_SOS.1a を実現できる。

FIA_SOS.1b 秘密の検証

SF.I&A は、データベースの操作員認証に使用するパスワードが以下の品質尺度を満たすことを検証するメカニズムを提供する。

- 長さ: 6 文字～16 文字
- 使用可能な文字: 半角英数記号文字

従って、SF.I&A により、FIA_SOS.1b を実現できる。

FIA_SOS.1c 秘密の検証

SF.I&A は、IC カードにアクセスするための一般操作員の PIN が以下の品質尺度を満たすことを検証するメカニズムを提供する。

- 長さ: 6 文字～16 文字
- 使用可能な文字: 半角英数記号文字

従って、SF.I&A により、FIA_SOS.1c を実現できる。

FIA_UAU.2a アクション前の利用者認証

SF.I&A は、上級操作員および一部の一般操作員の識別認証にあたっては、TOE は各操作員に識別認証前のいかなる操作も許可しない。

従って、SF.I&A により、FIA_UAU.2a を実現できる。

FIA_UAU.5 複数の認証メカニズム

SF.I&A は、利用者認証をサポートするため以下の複数の認証メカニズムと認証を提供する規則を提供する。

項番	適用場面（いつ使われるか）	使用する認証メカニズムと認証内容
1	・CA サーバ端末において、上級操作員を識別認証する場合 ・CA クライアント端末において、一般操作員の識別認証方式として「操作員 ID とパスワード」を設定している場合	・操作員 ID とパスワードによる認証を行う。TOE は入力されたパスワードと TOE の管理するパスワードとが一致することを確認する

2	・CA クライアント端末において、一般操作員の識別認証方式として「IC カードと PIN による方式」を設定している場合	・IC カードに格納された秘密鍵を使用したチャレンジ＆レスポンス認証を行う。 ・チャレンジ＆レスポンス認証成功後、操作員証明書の正当性確認（当該 CA から発行されたものであること、有効期間内であること、CRL に含まれないこと）を行う。 両方が成功した場合だけ成功となる。 注) チャレンジ＆レスポンス認証に用いられる操作員証明書および操作員秘密鍵は IC カードに格納されており、チャレンジ＆レスポンス認証は、TOE 外の IC カードによる PIN 認証が成功した場合にのみ行われる。
3	・RA 操作端末において、一般操作員の識別認証方式として「IC カードと PIN による方式」を設定している場合	・操作員証明書の正当性確認（当該 CA から発行されたものであること、有効期間内であること、CRL に含まれないこと）を行う。 注) 操作員証明書は IC カードに格納されており、その正当性の確認は、TOE 外の IC カードによる PIN 認証および WWW サーバによる SSL 認証が成功した場合にのみ行われる。
4	・RA 操作端末において、一般操作員の識別認証方式として「操作員 ID とパスワード」を設定している場合	・操作員 ID とパスワードによる認証を行う。TOE は入力されたパスワードと TOE の管理するパスワードとが一致することを確認する
5	・項番１および２で、機能の実行に必要な操作員人数が二人に設定されている場合	・対象機能の実行開始時に、第 2 操作員の認証を行う。認証の内容は項番１もしくは２と同様。第 1 操作員、第 2 操作員両方の認証が成功した場合だけ成功となる。

従って、SF.I&A により、FIA_UAU.5 を実現できる。

FIA_UID.2a アクション前の利用者識別

SF.I&A は、上級操作員および一般操作員の識別認証にあたっては、TOE は各操作員に識別認証前のいかなる操作も許可しない。複数操作員認証が必要な機能の実行においては、２人の操作員認証が成功しなければ、操作を許可しない。

従って、SF.I&A により、FIA_UID.2a を実現できる。

FIA_USB.1 利用者・サブジェクト結合

SF.ACC は、SF.I&A で識別認証が終了した後、操作員種別と所属する権限グループを利用者を代行して動作するサブジェクトである上級操作員プロセスまたは一般操作員プロセスに関連付ける。

従って、SF.ACC により、FIA_USB.1 を実現できる。

FMT_MOF.1 セキュリティ機能のふるまいの管理

SF.ACC は、アクセス制御機能の操作員人数を改変する能力、および識別認証機能の使用する認証方式を決定する能力を以下の役割に制限する。

機能	ふるまいの管理	役割

アクセス制御機能	改変する（操作員人数）	操作員管理のアクセス権限を持つ権限グループに所属する上級操作員
識別認証機能	決定する（認証方式）	操作員管理のアクセス権限を持つ権限グループに所属する上級操作員、操作員管理のアクセス権限を持つ権限グループに所属する一般操作員

従って、SF.ACC により、FMT_MOF.1 を実現できる。

FMT_MTD.1a TSF データの管理

SF.ACC は、以下の役割（必要なアクセス権限を持つ上級操作員および一般操作員）が以下のセキュリティ属性を含む TSF データを管理することを可能にする。

TSF データ		操作	許可された識別された役割
上級操作員データ		-	上級操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
	操作員種別（上級操作員）	[その他の操作：割付]	
	操作員 ID	削除、[その他の操作：登録]	
	パスワード	削除、改変、[その他の操作：登録]	
	所属する権限グループ（上級操作員権限グループから選択）	[その他の操作：割付]	
一般操作員データ		-	上級操作員、および一般操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
	操作員種別（一般操作員）	[その他の操作：割付]	
	操作員 ID	削除、[その他の操作：登録]	
	パスワードまたは PIN	削除、改変、[その他の操作：登録]	
	秘密鍵	削除、改変、[その他の操作：生成]	
	証明書	改変、[その他の操作：生成、失効]	
	所属する権限グループ（一般操作員権限グループから選択）	[その他の操作：割付]	

従って、SF.ACC により、FMT_MTD.1a を実現できる。

FMT_MTD.1b TSF データの管理

SF.ACC は、上級操作員および一般操作員が自身のパスワード（もしくは PIN）を変更することを可能にする。

従って、SF.ACC により、FMT_MTD.1b を実現できる。

FMT_MTD.1c TSF データの管理

SF.ACC は、以下の役割（必要なアクセス権限を持つ上級操作員および一般操作員）が以下の TSF データを管理することを可能にする。

TSF データ		操作	許可された識別された役割
上級操作員グループデータ		-	上級操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
	権限グループ(上級操作員のみ所属できる上級操作員グループ)	削除、[その他の操作：登録]	
	権限グループが保持するアクセス権限	改変	
一般操作員グループデータ		-	上級操作員、および一般操作員（ただし、操作員管理のアクセス権限を持つ場合のみ許可される）
	権限グループ(一般操作員のみ所属できる一般操作員グループ)	削除、[その他の操作：登録]	
	権限グループが保持するアクセス権限	改変	

従って、SF.ACC により、FMT_MTD.1c を実現できる。

FMT_MTD.1d TSF データの管理

SF.ACC は、以下の役割（必要なアクセス権限を持つ上級操作員および一般操作員）が以下の TSF データを管理することを可能にする。

TSF データ	操作	役割
監査ログ	問い合わせ（参照）、削除、外部ファイルへの保管	上級操作員、および一般操作員（ただし、監査ログ参照、および／または監査管理のアクセス権限を持つ場合のみ許可される）
アーカイブログ	問い合わせ（参照）、削除、外部ファイルへの保管	上級操作員、および一般操作員（ただし、アーカイブ管理、および／またはアーカイブ参照のアクセス権限を持つ場合のみ許可される）
システム設定情報	削除、改変、登録	上級操作員、および一般操作員（ただし、システム環境設定、および／またはスケジュール管理アクセス権限を持つ場合のみ許可される）

従って、SF.ACC により、FMT_MTD.1d を実現できる。

FMT_SMF.1 管理機能の特定

SF.ACC は以下の管理機能を提供する。

・権限グループの登録、削除
・権限グループの保持するアクセス権限の改変
・操作員 ID の登録、削除
・操作員のパスワードまたは PIN の登録、改変
・SF.Crypto によって生成される操作員の秘密鍵の登録

・SF.Cer_Issue によって生成、失効される操作員の証明書の登録
・操作員種別意の割付
・操作員の所属する権限グループへの割付
・認証方式の決定
・機能の要求する操作員人数の改変
SF.Crypto は、以下の管理機能を提供する。
・システム設定情報のハッシュ値生成、比較
・監査ログデータのハッシュ値生成、比較
・アーカイブデータのハッシュ値生成、比較
SF.Cer_Issue は、以下の管理機能を提供する。
・ 操作員証明書の生成、失効
従って、SF.ACC、SF.Crypto、および SF.Cer_Issue により FMT_SMF.1 を実現できる。

FMT_SMR.2 セキュリティ役割における制限
SF.ACC は、以下の 2 種類の操作員種別を定義する。
・上級操作員
・一般操作員
また、SF.ACC は、一人の操作員を一つの操作員種別にしか分類しない。
従って、SF.ACC により、FIA_SMR.2 を実現できる。

FPT_RVM.1 TSP の非バイパス性
SF.I&A は、TSC 内の各機能の動作が許可される前に、識別認証機能が呼び出され成功することを保証する。SF.ACC は、ログイン後の操作員が操作を行う際に、アクセス制御機能が実施され成功することを保証する。
従って、SF.I&A と SF.ACC の組み合わせにより、FPT_RVM.1 を実現できる。
従って、SF.I&A と SF.ACC により、FPT_RVM.1 を実現できる。

8.3.2. セキュリティ機能強度根拠
この TOE において、確率的または順列的メカニズムに基づくセキュリティ機能は、SF.I&A である。これらのセキュリティ機能強度は、6.2節において、SOF-基本を指定している。一方、この TOE の最小機能強度レベルは、5.1.2節において SOF-基本を指定している。従って、両者は一貫している。

8.3.3. セキュリティ機能組合せ根拠
セキュリティ機能 SF.I&A、SF.ACC の組み合わせが、TOE セキュリティ機能要件 FPT_RVM.1 を満たすために一緒に機能することを以下に示す。
TOE を利用する場合、SF.I&A による利用者の識別認証と、SF.ACC によるアクセス権限の

確認が完了しないと、アクセス権限を必要とする TOE 操作ができない。従って、FPT_RVM.1 を満たすためには、SF.I&A と SF.ACC が一緒に機能しなければならない。

8.3.4. セキュリティ保証手段根拠

各保証手段と、EAL3 の保証要件クラス・保証要件コンポーネントの対応関係を表 8-8に示す。

表 8-8 保証手段

保証手段	保証要件クラス	保証要件コンポーネント
PKIサーバ／Carassuit 電子政府版 ver3.1 構成管理文書	ACM 構成管理	ACM_CAP.3
		ACM_SCP.1
PKIサーバ／Carassuit 電子政府版 ver3.1 配付手続文書	ADO 配付と運用	ADO_DEL.1
PKIサーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス		ADO_IGS.1
PKIサーバ／Carassuit 電子政府版 ver3.1 機能仕様書	ADV 開発	ADV_FSP.1
PKIサーバ／Carassuit 電子政府版 ver3.1 上位レベル設計書		ADV_HLD.2
PKIサーバ／Carassuit 電子政府版 ver3.1 表現対応分析書		ADV_RCR.1
PKIサーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス	AGD ガイダンス文書	AGD_ADM.1
本 TOE は管理者のみが利用し、一般利用者は利用しないので、利用者ガイダンスは提供しない。		AGD_USR.1
PKIサーバ／Carassuit 電子政府版 ver3.1 開発セキュリティ文書	ALC ライフサイクルサポート	ALC_DVS.1
PKIサーバ／Carassuit 電子政府版 ver3.1 テストカバレージ分析書	ATE テスト	ATE_COV.2
PKIサーバ／Carassuit 電子政府版 ver3.1 テスト深さ分析書		ATE_DPT.1
PKIサーバ／Carassuit 電子政府版 ver3.1 テスト手順書・報告書		ATE_FUN.1
PKIサーバ／Carassuit 電子政府版 ver3.1 TOE		ATE_IND.2
PKIサーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス	AVA 脆弱性評定	AVA_MSU.1
PKIサーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス		AVA_MSU.1
PKIサーバ／Carassuit 電子政府版 ver3.1 セキュリティ強度分析書		AVA_SOF.1
PKIサーバ／Carassuit 電子政府版 ver3.1 脆弱性分析書		AVA_VLA.1

表 8-8にある各保証手段により、それぞれ対応する保証要件が満たされる。

次に、各保証要件が、保証手段で実現できることを説明する。

（1）ACM：構成管理

ACM_CAP.3：許可の管理

a） PKI サーバ／Carassuit 電子政府版 ver3.1 構成管理文書

は、以下の内容を記述している。

・TOE のバージョンのリファレンス

（バージョンの付け方、TOE のバージョン表示方法）

・構成リスト

（構成要素）

・構成管理計画

（構成要素作成・変更・削除方法、構成要素の操作に必要な個人の役割と責任、

構成要素へのアクセス権、構成要素同時変更防止方法、構成要素管理記録、
TOE バージョン管理方法）
・構成要素識別
（保証手段文書、テストソフトウェア、TOE ソースコード）
・構成要素識別方法
（一意の識別情報を割り付ける方法、構成管理システムに組み入れる方法、
TOE の置き換えバージョンを識別する方法、開発保守ライフサイクルにおいて
構成要素を識別する方法、構成要素間の対応識別）
従って、上記構成管理文書 a）により ACM_CAP.3 を実現できる。

ACM_SCP.1：TOE の CM 範囲
b） PKI サーバ／Carassuit 電子政府版 ver3.1 構成管理文書
は、以下の内容を記述している。
・TOE のバージョンのリファレンス
（バージョンの付け方、TOE のバージョン表示方法）
・構成要素識別
（保証手段文書、テストソフトウェア、TOE ソースコード）
・構成要素識別方法
（一意の識別情報を割り付ける方法、構成管理システムに組み入れる方法、
TOE の置き換えバージョンを識別する方法、開発保守ライフサイクルにおいて
構成要素を識別する方法、構成要素間の対応識別）
従って、上記構成管理文書 b）により ACM_SCP.1 を実現できる。

（2）ADO：配付と運用
ADO_DEL.1：配付手続き
c） PKI サーバ／Carassuit 電子政府版 ver3.1 配付手続文書
は、以下の内容を記述している。
・TOE を利用者サイトへ配送するときのセキュリティを維持するために必要な手続き
（配付する TOE 識別（型番、バージョン）、TOE 配付手段、TOE パッケージ方法）
従って、上記配付手続き文書 c）により ADO_DEL.1 を実現できる。

ADO_IGS.1：設置、生成、及び立上げ手順
d） PKI サーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス
は、以下の内容を記述している。
・セキュアな設置、生成及び立上げに必要な手順すべて
（設置、インストール方法）

従って、上記設置、生成、及び立上げ手順文書 d）により ADO_IGS.1 を実現できる。

（3）ADV：開発

ADV_FSP.1：非形式的機能仕様

e） PKI サーバ／Carassuit 電子政府版 ver3.1 機能仕様書
は、以下の内容を記述している。
・TOE セキュリティ機能内容
・外部 TOE セキュリティ機能インタフェース識別
・外部 TOE セキュリティ機能インタフェース内容
（効果、例外および誤りメッセージ）
・外部 TOE セキュリティ機能インタフェースのふるまい
（利用者入力パラメータ、モード）
従って、上記非形式的機能仕様文書 e）により ADV_FSP.1 を実現できる。

ADV_HLD.2： セキュリティ実施上位レベル設計

f） PKI サーバ／Carassuit 電子政府版 ver3.1 上位レベル設計書
は、以下の内容を記述している。
・サブシステム識別
・サブシステム内容
（セキュリティ機能）
・TSF で必要とする IT 環境であるハードウェア、ソフトウェア識別
・IT 環境のハードウェア、ソフトウェアで実装される補助的な保護メカニズムが提供する機能
・サブシステム内部インタフェース識別
・サブシステム外部インタフェース識別
・サブシステムインタフェース内容
（目的、使用方法、効果、例外及び誤りメッセージ）
・TSP 実施サブシステム識別
従って、上記セキュリティ実施上位レベル設計文書 f）により ADV_HLD.2 を実現できる。

ADV_RCR.1： 非形式的対応の実証

g） PKI サーバ／Carassuit 電子政府版 ver3.1 表現対応分析書
は、以下の内容を記述している。
・ST の TOE セキュリティ機能と上記機能仕様書の TOE セキュリティ機能間の関係
・ST の TOE セキュリティ機能と上記機能仕様書の外部 TOE セキュリティ機能インタフェース間の関係

・上記機能仕様書の TOE セキュリティ機能と上記上位レベル設計書のサブシステム間の関係
・上記機能仕様書の外部 TOE セキュリティ機能と上記上位レベル設計書のサブシステム間の関係
従って、上記非形式的対応の実証 g）により ADV_RCR.1 を実現できる。

（4）AGD：ガイダンス文書

AGD_ADM.1：管理者ガイダンス

h） PKI サーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス
は、以下の内容を記述している。
・管理セキュリティ機能とインタフェース
（目的、ふるまい、相互関係、インタフェース起動方法、パラメータとそのデフォルト値、リターンコード）
・IT 環境の利用方法、IT セキュリティ要件
・TOE の管理機能・権限
・TOE 操作のすべての可能なモード
（故障または操作誤りの後の操作も含む）
・ST で記述した前提条件
（TOE の意図する使用方法、物理的、人的及び接続的前提条件）
従って、上記管理者ガイダンス文書 h）により AGD_ADM.1 を実現できる。

AGD_USR.1：利用者ガイダンス

本 TOE では、一般利用者は存在しないので、利用者ガイダンスは提供しない。
従って、AGD_USR.1 を削除する。

（5）ALC：ライフサイクルサポート

ALC_DVS.1：セキュリティ手段の識別

i） PKI サーバ／Carassuit 電子政府版 ver3.1 開発セキュリティ文書
は、以下の内容を記述している。
・開発環境で使用されるセキュリティ手段
（TOE 開発環境への物理的アクセス制御、開発マシンへのアクセス制御、部外者のアクセス制限、セキュリティ適用役割と責任、開発スタッフ管理）
・開発環境セキュリティ記録
（入退室管理ログ）
従って、上記セキュリティ手段の識別文書 i)により ALC_DVS.1 を実現できる。

（6）ATE：テスト

ATE_COV.2： カバレージの分析

j） PKI サーバ／Carassuit 電子政府版 ver3.1 テストカバレージ分析書
は、以下の内容を記述している。
・上記機能仕様書のセキュリティ機能と下記テスト手順書・報告書 l）のテスト項目名との間の関係
従って、上記カバレージの分析文書 j）により ATE_COV.2 を実現できる。

ATE_DPT.1： テスト：上位レベル設計

k） PKI サーバ／Carassuit 電子政府版 ver3.1 テスト深さ分析書
は、以下の内容を記述している。
・上記上位レベル設計書のサブシステムと下記テスト手順書・報告書 l）のテスト項目名との間の関係
従って、上位レベル設計のテスト深さ分析書 k）により ATE_DPT.1 を実現できる。

ATE_FUN.1： 機能テスト

l） PKI サーバ／Carassuit 電子政府版 ver3.1 テスト手順書・報告書
は、以下の内容を記述している。
・テスト計画
（テストされるセキュリティ機能識別、テスト目標、テスト構成、）
・テスト手順記述
（セキュリティ機能ふるまい識別、順序の依存性、再現可能性、テスト手順、）
・期待されるテスト結果及び実際のテスト結果
従って、上記機能テスト文書 l）により ATE_FUN.1 を実現できる。

ATE_IND.2： 独立テスト－サンプル

評価者が TOE のテストを行う際、
m） PKI サーバ／Carassuit 電子政府版 ver3.1 TOE
に関し、上記のテスト手順書・報告書 l）に記述したテストで使用されたものと同等の一連の資源を提供する。
従って、上記独立テスト－サンプルの手段 m）で ATE_IND.2 を実現できる。

（7）脆弱性評定

AVA_MSU.1：ガイダンスの検査

n） PKI サーバ／Carassuit 電子政府版 ver3.1 管理者ガイダンス
o） PKI サーバ／Carassuit 電子政府版 ver3.1 インストールガイダンス

は、以下の内容を記述している。
・TOE 操作のすべての可能なモード
（故障または操作誤りの後の操作も含む）
・ST で記述した前提条件
（TOE の意図する使用方法、物理的、人的及び接続的前提条件）
従って、上記ガイダンスの検査文書 n）および o)により AVA_MSU.1 を実現できる。

AVA_SOF.1：TOE セキュリティ機能強度評価
p） PKI サーバ／Carassuit 電子政府版 ver3.1 セキュリティ強度分析書
は、以下の内容を記述している。
・ST でレート付けした SOF 主張に対するセキュリティメカニズムに関する SOF 分析
（前提条件、正しいパスワードの入力確率計算、攻撃潜在性計算、考察）
従って、上記 TOE セキュリティ機能強度評価 p）により AVA_SOF.1 を実現できる。

AVA_VLA.1：開発者脆弱性分析
q） PKI サーバ／Carassuit 電子政府版 ver3.1 脆弱性分析書
は、以下の内容を記述している。
・上記の保証手段文書ごと含まれる脆弱性の内容
・明らかな脆弱性の内容
・上記で識別された脆弱性の分析
（公知の有無、知識の有無、対抗手段、悪用可能性）
従って、上記開発者脆弱性分析文書 q）により AVA_VLA.1 を実現できる。

9. 付録

9.1. 略語・用語

<CC 関連略語>
CC（Common Criteria）：コモンクライテリア
EAL（Evaluation Assurance Level）：評価保証レベル
IT（Information Technology）：情報技術
PP（Protection Profile）：プロテクションプロファイル
SFP（Security Function Policy）：セキュリティ機能ポリシー
ST（Security Target）：セキュリティターゲット
SOF（Strength Of Function）：機能強度
TOE（Target Of Evaluation）：評価対象
TSF（TOE Security Functions）：TOE セキュリティ機能
TSP（TOE Security Policy）：TOE セキュリティポリシー

<TOE 関連略語>
API（Application Programming Interface）：アプリケーションプログラミングインタフェース
ARL（Authority Revocation List）：機関失効リスト
BASE64：エンコード方式の一つ
CA（Certificate Authority）：認証局
CGI（Common Gateway Interface）：Web サーバが、Web ブラウザからの要求に応じて、プログラムを起動するための仕組み
CPS（Certification Practice Statement）：認証局運用規定
CRL（Certificate Revocation List）：証明書失効リスト
DB（Database）：データベース
DER（Distinguished Encoding Rules）：区別化エンコード規則
DES（Data Encryption Standard）：IBM 社によって開発された秘密鍵暗号化アルゴリズム
EE（End Entity）：エンドエンティティ（一般利用者）
FIPS（Federal Information Processing Standard）：米国政府調達基準。暗号モジュールの安全性に関する標準を含む。
HSM（Hardware Security Module）：認証局秘密鍵を生成管理するハードウェア
IC（Integrated Circuit）：集積回路
ID（IDentification）：識別番号

LDAP（Lightweight Directory Access Protocol）：TCP／IP ネットワークで、ディレクトリデータベースにアクセスするためのプロトコル
PIN（Personal Identification Number）：個人識別番号
PKCS（Public Key Cryptography Standards）：RSADSI 社が定める、公開鍵暗号技術をベースとした各種の規格群
PKI（Public Key Infrastructure）：公開鍵基盤
RA（Registration Authority）：登録局
RSA（Rivest Shamir Adleman）：Ronald Rivest 氏、Adi Shamir 氏、Leonard Adleman 氏の 3 人が 1978 年に開発した公開鍵暗号方式の一つ
WWW（World Wide Web）：ワールドワイドウェブ
SSL（Secure Socket Layer）：Netscape Communications 社が開発した、インターネット上で情報を暗号化して送受信するプロトコル。

9.2. 参照

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August 2005 Version 2.3
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements August 2005 Version 2.3
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements August 2005 Version 2.3
- Common Methodology for Information Technology Security Evaluation Evaluation Methodology August 2005 Version 2.3
- 情報技術セキュリティ評価のためのコモンクライテリア　パート１：概説と一般モデル　平成１７年１２月翻訳第１．０版　独立行政法人情報処理推進機構（IPA）セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア　パート２：セキュリティ機能要件　平成１７年１２月翻訳第１．０版　独立行政法人情報処理推進機構（IPA）セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア　パート３：セキュリティ保証要件　平成１７年１２月翻訳第１．０版　情報処理振興事業協会（IPA）セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のための共通方法　評価方法　平成１７年１２月翻訳第１．０版　独立行政法人情報処理推進機構（IPA）セキュリティセンター情報セキュリティ認証室
- 補足-0512　平成１７年１２月　独立行政法人情報処理推進機構（IPA）セキュリティセンター情報セキュリティ認証室