PKI サーバ/Carassuit 電子政府版 Ver9.0
セキュリティターゲット

バージョン：1.6

発行日：2023 年 6 月 12 日

作成者：NEC ソリューションイノベータ株式会社

改版履歴

日付	バージョン	改版内容
2023/1/13	1.0	新規作成
2023/2/14	1.1	●1.4.2. TOE の物理的範囲 ・TOE のガイダンス文書の会社名を日本電気株式会社から NEC ソリューションイノベータ株式会社に変更 ●8.2. 参照 ・以下を削除 [6] 政府認証基盤（GPKI） 府省認証局 CP／CPS ガイドライン，平成 15 年 6 月 6 日改定，共通システム専門部会了承 ・[7] 政府認証基盤（GPKI）政府認証基盤相互運用性仕様書（移行完了編），平成２７年３月２７日改定，共通システム専門部会了承を[6] 政府認証基盤（GPKI）政府認証基盤相互運用性仕様書，令和 3 年 12 月 23 日改定，デジタル社会推進会議関係課長等連絡会議了承に修正 ・[8]を[7]に変更 ・[9] 電子政府推奨暗号リスト，令和 4 年 3 月改定を[8] 電子政府推奨暗号リスト，令和 4 年 3 月 30 日，デジタル庁・総務省・経済産業省に修正 ・上記参照ドキュメント番号の変更に合わせて本文中の番号を更新
2023/4/7	1.2	●6.1. セキュリティ機能要件 ・「LunaSA7」を「SafeNet LunaSA」に修正 ・ FMT_MOF.1 、 FMT_MTD.1a 、 FMT_MTD.1c 、 FMT_MTD.1d：許可された識別された役割の記載を変更 ・FMT_SMF.1：セキュリティ管理機能のリストの許可された識別された役割の記載を変更 ・FMT_SMR.2：許可された識別された役割の記載を変更、異なる役割に対する条件を追記 ●6.3.1. セキュリティ機能要件根拠

		・表 6.3.1 の FMT_SMF.1 と FMT_SMR.2 を更新 ・O.ISSUE_CONFIRMATION（発行確証）の記述を更新 ●6.3.2. セキュリティ機能要件依存性 ・表 6.3.2 の FCS_COP.1 を更新 ・FCS_COP.1 の依存関係の一部が不要であることの根拠を追記 ●7.1.4. SF.Crypto ・「LunaSA7」を「SafeNet LunaSA」に修正 ●7.1.2. SF.ACC ・FMT_SMR.2 の異なる役割に対する条件に関する記載を追記 ●8.2. 参照 ・以下を削除 [6] 政府認証基盤（GPKI）政府認証基盤相互運用性仕様書，令和 3 年 12 月 23 日改定，デジタル社会推進会議関係課長等連絡会議了承 ・[7]を[6]に変更 ・[8]を[7]に変更 ・上記参照ドキュメント番号の変更に合わせて本文中の番号を更新

2023/5/8	1.3	●3.2. 組織のセキュリティ方針 ・「P.CA_PRIVATE_KEY（認証局秘密鍵)」 を「P.CA_PAIRWISE_KEY（認証局鍵ペア)」 に修正　秘密鍵のみの記述から鍵ペアへの記述に変更 ●4.2.1. IT 環境のセキュリティ対策方針 ・ OE.CA_PRIVATE_KEY （認証局秘密鍵）を OE.CA_PAIRWISE_KEY（認証局鍵ペア）に修正 ●4.3. セキュリティ対策方針根拠 ・ 表 4.3.1 の P.CA_PRIVATE_KEY を P.CA_PAIRWISE_KEY に、OE.CA_PRIVATE_KEY を OE.CA_PAIRWISE_KEY に修正 ・○組織のセキュリティ方針の P.CA_PRIVATE_KEY を P.CA_PAIRWISE_KEY に修正　秘密鍵のみの記述から鍵ペアへの記述に変更 ●6.3.2. セキュリティ機能要件依存性 ・FCS_COP.1 の依存関係の一部が不要であることの根拠の一部を運用のセキュリティ対策方針で依存性を不要としている理由を追記
2023/5/29	1.4	●7.1.2. SF.ACC ・操作員と操作員種別の関連付けは、機能の実行を開始する場合に再取得し反映することを追記（FMT_SMR.2）
2023/6/2	1.5	●4.2.1. OE.CA_PAIRWISE_KEY（認証局鍵ペア） ・CA 秘密鍵は HSM で物理的に保護されることを明記
2023/6/12	1.6	●3.2. P.CA_PAIRWISE_KEY（認証局鍵ペア） ・CA 秘密鍵は HSM で物理的に保護されることを明記

目次

1. ST 概説

本章では、ST 参照、TOR 参照、TOE 概要、TOE 記述について述べる。

1.1. ST 参照

タイトル	: PKI サーバ/Carassuit 電子政府版 Ver9.0 セキュリティターゲット
バージョン	: 1.6
作成者	: NEC ソリューションイノベータ株式会社
発行日	: 2023 年 6 月 12 日

1.2. TOE 参照

TOE	: PKI サーバ/Carassuit 電子政府版
TOE のバージョン	: Ver9.0
キーワード	: PKI、公開鍵基盤、CA、認証局、RA、登録局
開発者	: NEC ソリューションイノベータ株式会社

1.3. TOE 概要

1.3.1. TOE 種別及び主要セキュリティ機能

TOE は、公開鍵基盤(PKI)における認証局(CA)機能および登録局(RA)機能を提供するアプリケーションソフトウェアであり、証明書発行・失効機能(公開鍵証明書、機関証明書、失効リストの発行及びこれらのデータのディレクトリへの保存)、登録局(RA)コンソール機能(証明書発行要求、証明書失効要求の受付処理、要求に対する資格審査処理)、及び共通で使用される基本機能(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)を提供する。

TOE が提供する主要なセキュリティ機能の概要を以下に示す。

- 証明書発行・失効機能：
  - エンドエンティティの公開鍵証明書を発行する。
  - 必要に応じて EE 鍵の鍵ペア生成、鍵保管を行う。EE の秘密鍵保管時には、暴露防止のため暗号化する。

- 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の２種類がある。
- 失効リスト(CRL、ARL)を発行する。
- 公開鍵証明書を LDAP ディレクトリへ保管する。
- 発行した公開鍵証明書を検証する為に、CA 自身の公開鍵証明書を公開する。
- TOE を利用して運用する CA が発行するすべての証明書および失効リストは、CA 自身の公開鍵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 自身の公開鍵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。
- 証明書の発行と失効時には、監査データを出力する。

・ 登録局(RA)コンソール機能：
- EE 証明書の発行における、申請、申請データ管理（検索、照会、削除等)、審査、出力の操作を行う。
- 発行された EE 証明書と秘密鍵を出力する。暴露防止のため出力形式に応じた暗号化を行う。
- EE 証明書の失効における、申請と失効リストの外部ファイル出力の操作を行う。
- EE の IC カードへ鍵・証明書を格納する形式のファイル（IC カード発行依頼ファイル）を生成する。
- IC カード発行依頼ファイルの生成時には、暴露防止のため暗号化する。
- IC カード発行依頼ファイルの生成時には、監査データを出力する。

・ 監査機能：
- 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を行う。
- 監査データの参照、検索、並べ替えや、外部ファイル出力の機能を提供する。
- 監査データには改ざん検知のためのハッシュ値を付加し、暴露防止のために暗号化する。
- 監査機能の起動と終了時には、監査データを出力する。

・ 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。
- バックアップ時には署名を付加し、リカバリ時に署名値を検証することで、バックアップデータの完全性を検証する。
- バックアップおよびリカバリ実行時には、監査データを出力する。

・ 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。
- アーカイブデータには改ざん検知のためのハッシュ値を付加し、暴露防止のために暗号化する。
- アーカイブデータの削除と外部出力時には、監査データを出力する。

・ アクセスコントロール（操作員管理）機能：
- 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操作員のみ可能であるよう制御する。
- TOE に対するアクセス権限を権限グループ単位で管理する。
- 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。
- アクセスコントロール情報には改ざん検知のためのハッシュ値を付加し、暴露防止のために暗号化する。
- 操作員の登録、削除等の管理実施時、および権限グループへのアクセス権限の設定時には、監査データを出力する。

・ ユーザ管理機能：
- EE の個人情報を管理する。
- EE の IC カードへ鍵・証明書を格納する形式のファイル（IC カード発行依頼ファイル）を生成する。
- IC カード発行依頼ファイルの生成時には、暴露防止のため暗号化する。
- IC カード発行依頼ファイルの生成時には、監査データを出力する。

・ システム環境設定機能：
- TOE の運用に必要な情報の設定、変更、参照等の管理機能を提供する。
- システム環境設定情報には改ざん検知のためのハッシュ値を付加し、暴露防止のために暗号化する。
- システム環境の設定、変更、参照等時には、監査データを出力する。

すべてのセキュリティ機能、および以下に示す一般機能の実行前には、登録された操作員として識別され、認証されなければならない。認証は、操作員 ID とパスワード、もしくは IC カードとその PIN を用いることができる。また機能によっては複数の操作員の認証を必要とする設定が可能である。

TOE が提供する一般機能の概要を以下に示す。

・ 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、変更、参照等の管理機能を提供する。
- ポリシー情報の設定、変更および参照時には、監査データを出力する。

・ 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。TOE はスケジュール設定された時間に、証明書失効リスト（CRL）、機関失効リスト（ARL）の発行を証明書発行・失効機能に依頼する機能を提供する。
- スケジュールの設定、変更、参照等の管理機能を提供する。
- スケジュール情報管理操作時には監査データを出力する。

1.3.2. TOE 利用環境

図 1.3-1 に、TOE が稼動する端末と、関連 IT 機器の構成例を示す。

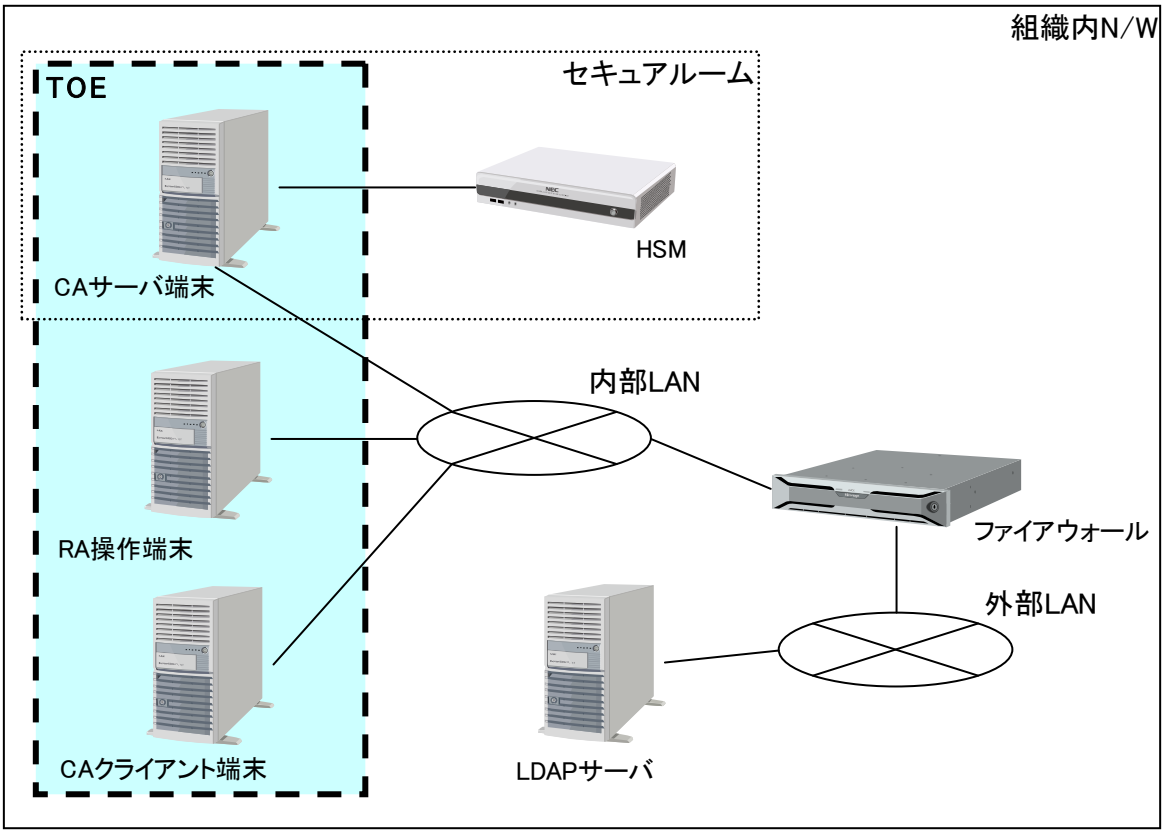

図 1.3-1：TOE の IT 構成図

組織内で TOE を稼動する場合、1 台以上の CA サーバ端末、1 台以上の RA 操作端末、1 台以上の CA クライアント端末、ファイアウォールを設置し、それぞれを LAN（ここでは、内部 LAN と呼称する）で接続する。内部 LAN はファイアウォールによって外部ネットワーク(ここでは、外部 LAN と呼称する)からのアクセスが制限されたセキュアなネットワークである。また、TOE により出力される証明書を保管する為の LDAP サーバを設置するが、本機は外部公開目的で設置する機器である為、外部 LAN 上に設置する。また、設置した端末のうち、CA サーバ端末は、TOE が使用する認証局鍵ペアをセキュアに管理する HSM (Hardware Security Module) と共に入退出管理されたセキュアルームに設置する。
TOE の物理的範囲内にある機器は、図 1.3-1 の太破線内にある CA サーバ端末、RA 操作端末、CA クライアント端末である。

・ CA サーバ端末：

CA サーバ端末は、セキュアルーム内に設置され、内部 LAN に接続される。また、HSM とはLAN ケーブルもしくはRS232C ケーブルと接続される。上級操作員が、CA サービスの起動／停止、システム環境設定、バックアップ／リカバリ、監査データ参照、上級／一般操作員管理、CA の秘密鍵管理を行う為に用いる。

- CA クライアント端末：

  CA クライアント端末は、内部 LAN に接続される。一般操作員が、CA サーバ端末で稼動している CA サービスの状態監視、証明書のポリシー設定、監査データ参照、ユーザ管理、一般操作員管理を行う為に用いる。

- RA 操作端末：

  RA 操作端末は、内部 LAN に接続される。一般操作員が、証明書発行要求、証明書失効要求、証明書取得、失効リスト取得、IC カード発行依頼ファイル取得を行う為に用いる。

- 内部 LAN：

  CA サーバ端末、CA クライアント端末、RA 操作端末が接続するネットワークである。通常、ファイアウォールによって組織内の外部 LAN からのアクセスが制限される。

- LDAP サーバ：

  CA サーバ端末で稼動する CA サービスにより発行された証明書及び失効リストが保管されるディレクトリサーバ。図 1.3-1 では組織内部に閉じたネットワーク上に設置されているが、インターネット上に証明書、失効リストを公開する場合は、インターネットに接続される事もある。

1.3.2.1. ハードウェア構成

表 1.3.1 に、TOE の動作環境としてのハードウェア構成を示す。TOE は、表に識別されたハードウェア構成または、同等構成の仮想化環境で正しく動作する。なお、表中の端末名については、図 1.3-1 を参照の事。

表 1.3.1：TOE 動作環境ハードウェア構成

端末名・装置名	説明
CA サーバ端末	
パーソナルコンピュータ	NEC Express5800 シリーズ または PC/AT 互換機 で以下を満たすもの。 ・ CPU：1.4GHz 以上の 64bit プロセッサ ・ メモリ：1GB 以上の RAM ・ HDD：10GB 以上の空き領域がある HDD
IC カードリーダ／ライタ	GemAlto PC USB-TR
IC カード	大日本印刷 Standard-9(NEC SecureWare 用 STD-9)
HSM	NEC CK-Guard V SafeNet LunaSA 7.4
CA クライアント端末	
パーソナルコンピュータ	NEC Express5800 シリーズ または PC/AT 互換機 で以下を満たすもの。 ・ CPU：1.4GHz 以上の 64bit または 32bit プロセッサ ・ メモリ：1GB 以上の RAM ・ HDD：10GB 以上の空き領域がある HDD
IC カードリーダ／ライタ	GemAlto PC USB-TR
IC カード	大日本印刷 Standard-9(NEC SecureWare 用 STD-9)
RA 操作端末	
パーソナルコンピュータ	NEC Express5800 シリーズ または PC/AT 互換機 で以下を満たすもの。 ・ CPU：1.4GHz 以上の 64bit または 32bit プロセッサ ・ メモリ：1GB 以上の RAM ・ HDD：10GB 以上の空き領域がある HDD
IC カードリーダ／ライタ	GemAlto PC USB-TR
IC カード	大日本印刷 Standard-9(NEC SecureWare 用 STD-9)

1.3.2.2. ソフトウェア構成

表 1.3.2 に TOE のソフトウェア構成を示す。TOE は表に識別されたソフトウェア構成によって、正しく動作する。なお、表中の端末名については、図 1.3-1 を参照の事。

表 1.3.2：TOE 動作環境ソフトウェア構成

ソフトウェア名(ベンダ名含む)	用途・説明
CA サーバ端末	
・Microsoft Windows Server 2019	オペレーティングシステム
・Oracle Database 19c 19.8.0.0 (64bit) ・Oracle Database Client 19c 19.8.0.0 (32bit)	DBMS 及び DBMS クライアント
Oracle Advanced Security 19c	Oracle Database セキュリティオプション
Microsoft Internet Information Service 10.0	WWW サーバ
NEC SecureWare/秘密鍵装置マネージャ Ver7.0	NEC CK-GuardV用インタフェース
Luna SA Client SoftWare 7.4	SafeNet LunaSA 用インタフェース
CA クライアント端末	
※以下の内、1 つが必要： ・Microsoft Windows 10 (64bit) ・Microsoft Windows 11	オペレーティングシステム
Oracle Database Client 19c 19.8.0.0 (32bit)	DBMS クライアント
RA 操作端末	
※以下の内、1 つが必要： ・Microsoft Windows 10 (64bit) ・Microsoft Windows 11	オペレーティングシステム
Microsoft Edge (Chromium)	WWW クライアント

1.4. TOE 記述

本章では、TOE の利用者役割、TOE の論理的範囲、及び TOE の物理的範囲について記述する。

1.4.1. TOE の利用者役割

TOE の役割を持つ利用者として、以下 3 種を定義する。

- 上級操作員
- 一般操作員
- 監査ログ検査者

上級操作員および一般操作員はシステム上の分類であり、それぞれ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。
監査ログ検査者は、システム上は上級操作員あるいは一般操作員であるが、所属する権限グループに付与されるアクセス権限が TOE の監査機能の操作に限定された特殊な作業者であり、他の上級操作員、および一般操作員と区別する。
上級操作員、一般操作員、および監査ログ検査者は、政府認証基盤の要求事項に準拠して「8.2　参照」[5]に示す文書中「5.2 手続き面の管理」で定める「(5)IA 操作員」「(6)RA 操作員」「(8)監査ログ検査者」に相当するものとして任命されるものとする。

TOE では、表 1.4.1 のアクセス権限が存在する。アクセス権限は、任意の権限グループにまとめることができる。一部の権限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。

表 1.4.1：TOE の権限一覧

アクセス権限	対応する TOE の機能	付与
ARL 出力	証明書発行・失効機能	○
CRL 出力	証明書発行・失効機能	○
アーカイブ管理(*注 1)	アーカイブ機能	○
アーカイブ参照(*注 2)	アーカイブ機能	○
システム環境設定	システム環境設定機能	○
スケジュール管理	スケジュール管理機能	○
ポリシ管理	ポリシー管理機能	○
監査ログ参照(*注 3)	監査機能	○
監査管理(*注 4)	監査機能	○
操作員管理	アクセスコントロール（操作員管理）機能	○
ユーザ管理	ユーザ管理機能	△
証明書情報参照	証明書発行・失効機能	○

機関証明書申請	証明書発行・失効機能	○
機関証明書取得	証明書発行・失効機能	○
機関証明書失効	証明書発行・失効機能	○
EE 証明書申請	証明書発行・失効機能	△
EE 証明書審査	登録局(RA)コンソール機能	△
EE 証明書取得	証明書発行・失効機能	△
EE 証明書失効	証明書発行・失効機能	△
EE IC カード発行	登録局(RA)コンソール機能	△
CA 鍵管理	システム環境設定機能	●
バックアップ・リカバリ	バックアップ／リカバリ機能	●
CA の起動・停止	証明書発行・失効機能	●

付与欄記号凡例：

●：上級操作員権限グループにのみ付与可能

○：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

△：一般操作員権限グループのみに付与可能

(*注 1)　アーカイブデータを外部出力して保管、および削除する操作を指す。

(*注 2)　アーカイブデータの参照、および検索を指す。

(*注 3)　監査ログの参照、および検索を指す。

(*注 4)　監査ログを印刷、外部出力して保管、および削除する操作を指す。

TOE のセットアップ時に、既定のアクセス権限が付与された上級操作員権限グループ、および一般操作員権限グループが各々 1 つずつ作成され、セットアップ時に登録する操作員が所属する。

TOE セットアップ時に作成される権限グループに既定値として付与されるアクセス権限を表 1.4.2 に示す。

表 1.4.2：TOE セットアップ時に生成される権限グループとアクセス権限

権限グループ種別	付与されるアクセス権限
上級操作員権限グループ	操作員管理
	CA 鍵管理
	バックアップ・リカバリ
	CA の起動・停止
一般操作員権限グループ	操作員管理

TOE の運用開始後は、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）、または一般操作員（操作員管理のアクセス権限を持つ権限グループに所属）によって、権限

グループに付与されたアクセス権限の変更、任意のアクセス権限を付与した権限グループの新規作成、削除、および所属する操作員の登録、削除が可能である。

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。

以下、TOE の利用者の役割を、端末ごとに記述する。

(1) CA サーバ端末

① 上級操作員：
付与されたアクセス権限に従って、CA サーバ端末上で認証局を操作する作業員である
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。

② 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、表 1.4.1 に示す権限のうち「監査ログ参照」および「監査管理」の権限のみが付与された上級操作員権限グループに所属する上級操作員である。監査ログ検査者は他の権限を割り当てられない。

(2) CA クライアント端末

① 一般操作員：
付与されたアクセス権限に従って、CA クライアント端末上で認証局を操作する作業員である。
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。

② 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、表 1.4.1 に示す権限のうち「監査ログ参照」および「監査管理」の権限のみが付与された一般操作員権限グループに所属する一般操作員である。監査ログ検査者は他

の権限を割り当てられない。

(3) RA 操作端末

① 一般操作員：

CA サーバに対して証明書発行要求、証明書発行要求の審査、証明書受取、証明書検索、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。

TOE の役割を持つ利用者の他に、TOE に直接アクセスしないことから役割を持つ利用者ではないが、TOE に関係する主体として以下２種を定義する。

① 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

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。認証局秘密鍵管理者は、政府認証基盤の要求事項に準拠して「8.2　参照」[5]に示す文書中「5.2 手続き面の管理」で定める「(2)IA 鍵管理者」に相当するものとして任命されるものとする。

② EE 証明書利用者：

EE 証明書利用者は、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。

1.4.2. TOE の物理的範囲

図 1.4-1 に、TOE を含むハードウェア・ソフトウェアの物理的なコンポーネント構成図を示す。

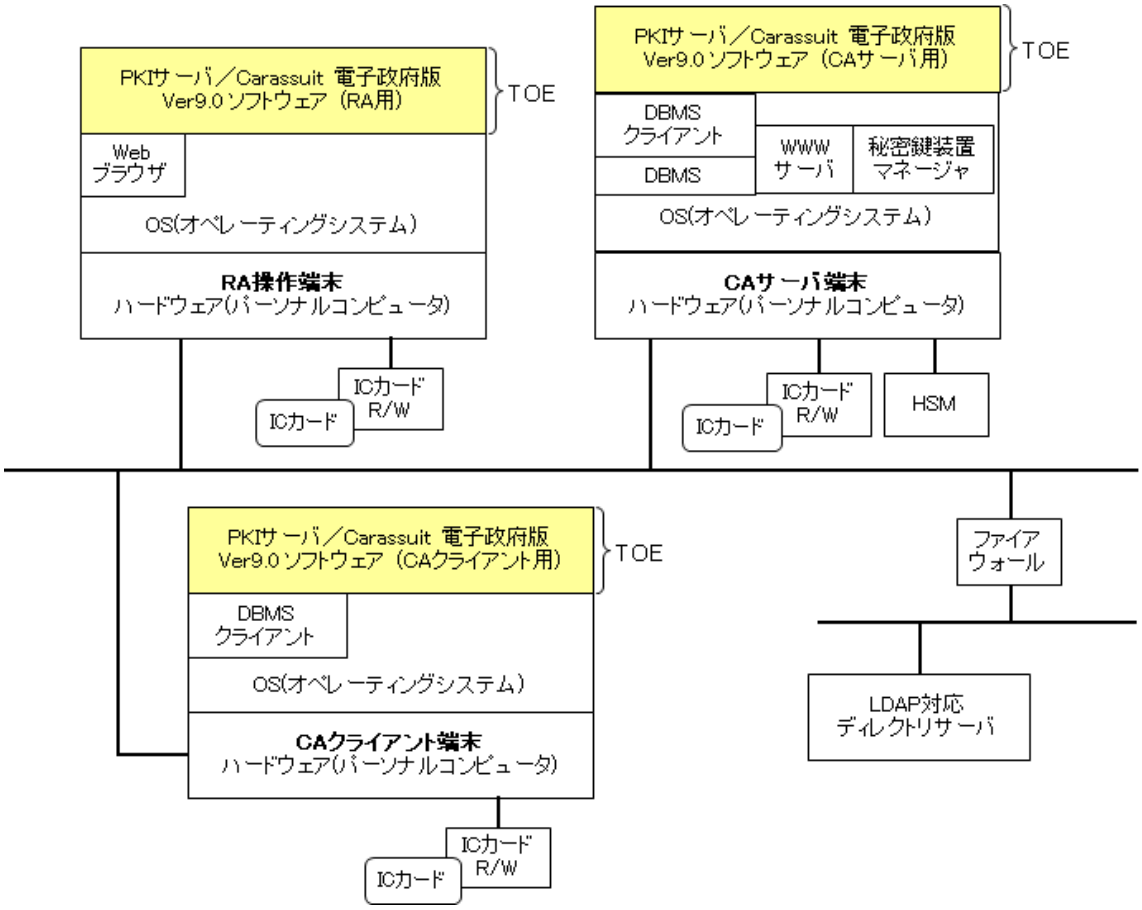

図 1.4-1：PKI サーバ/Carassuit 電子政府版 構成図

図 1.4-1 に示すように、TOE は PKI サーバ/Carassuit 電子政府版 Ver9.0 ソフトウェア(CA サーバ用、RA 用、CA クライアント用)であり、それ以外のハードウェア・ソフトウェアは TOE 外となる。
以下に TOE を動作させる為に必要なハードウェアについて記述する。

(1) **CA サーバ端末ハードウェア：**
認証局(CA)機能が稼動するパーソナルコンピュータ。

(2) **CA クライアント端末ハードウェア：**
認証局(CA)機能に接続するパーソナルコンピュータ。

(3) **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。

(4) **HSM(Hardware Security Module)：**

認証局鍵ペアを生成・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。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 サーバ端末に接続される。

(5) **IC カードリーダ/ライタ（R/W：Reader/Writer)：**

IC カードをリード／ライトするハードウェア装置。CA サーバ端末、RA 操作端末、CA クライアント端末の各端末に接続される。

(6) **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 R/W 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。

(7) **ファイアウォール：**

CA サーバ端末・CA クライアント端末・RA 操作端末が接続されているネットワークとそれら以外の端末（外部端末）が接続され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。

各端末の周辺装置（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 RS232C 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。

次に TOE 及び TOE を動作させる為に必要なソフトウェアについて、端末ごとに記述する。

(1) **CA サーバ端末**

① PKI サーバ/Carassuit 電子政府版 Ver9.0 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。CA サーバコンソール機能、CA サブシステム機能、CGI モジュール機能、鍵管理 DB-API 機能、IC カード管理機能、PKCS#11 モジュール機能がある。これらの機能説明については 1.4.3 節に記述する。

② DBMS：
データベース管理システム。TOE データ(後述)を管理する。

③ DBMS クライアント：
データベース管理システムクライアント。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。

④ WWW サーバ：
Web サーバ。RA 操作端末の要求に応じる。

⑤ 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ソフトウェア。

⑥ 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為の基盤となるソフトウェア。

⑵ CA クライアント端末

① PKI サーバ/Carassuit 電子政府版 Ver9.0 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。CA クライアントコンソール機能、CA サブシステム機能、鍵管理 DB-API 機能、IC カード管理機能がある。これらの機能説明については 1.4.3 節に記述する。

② DBMS クライアント：
データベース管理システムクライアント。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。

③ 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為の基盤となるソフトウェア。

⑶ RA 操作端末

① PKI サーバ/Carassuit 電子政府版 Ver9.0 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。RA コンソール機能、IC カード管理機能がある。これらの機能説明については 1.4.3 節に記述する。

② WWW クライアント：
Web ブラウザ。リモートで RA 操作を行う。

③ 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為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、3.1.1 節 TOE 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。

PKI サーバ/Carassuit 電子政府版 Ver9.0 ソフトウェアは、製品を購入した TOE 消費者が、通知されたウェブサイトからダウンロードすることで入手できる。通知された ID/パスワードを指定してウェブサイトにログインすると、購入した製品情報が表示されるため、目的の TOE 名称とバージョン情報が表示されているものを選択してダウンロードする。ソフトウェアは、インストーラ（exe 形式の binary）とガイダンス文書(pdf）から構成される。インストーラ実行時の指定により、CA サーバ用、RA 用、CA クライアント用の各ソフトウェアがインストールされる。

ガイダンス文書は以下の通りである。

(1) PKI サーバ/Carassuit 電子政府版 Ver9.0 取扱説明書
2023 年 4 月 NEC ソリューションイノベータ株式会社

(2) PKI サーバ/Carassuit 電子政府版 Ver9.0 セットアップガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(3) PKI サーバ/Carassuit 電子政府版 Ver9.0 Oracle Net over SSL セットアップガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(4) PKI サーバ/Carassuit 電子政府版 Ver9.0 Oracle Database チューニングガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(5) PKI サーバ/Carassuit 電子政府版 Ver9.0 ライセンス管理ツール操作ガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(6) PKI サーバ/Carassuit 電子政府版 Ver9.0 ユーザ管理サブシステム操作ガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(7) PKI サーバ/Carassuit 電子政府版 Ver9.0 バックアップ／リカバリ操作ガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(8) PKI サーバ/Carassuit 電子政府版 Ver9.0 自己署名証明書・リンク証明書失効機能操作ガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(9) PKI サーバ/Carassuit 電子政府版 Ver9.0 サービス監視操作ガイド
2023 年 4 月 NEC ソリューションイノベータ株式会社

(10) PKI サーバ/Carassuit 電子政府版 Ver9.0 エラーメッセージ・エラーコード一覧
2023 年 4 月 NEC ソリューションイノベータ株式会社

(11) PKI サーバ/Carassuit 電子政府版 Ver9.0 注意制限事項一覧
2023 年 4 月 NEC ソリューションイノベータ株式会社

(12) PKI サーバ/Carassuit 電子政府版 Ver9.0 Carassuit API リファレンス
2023 年 4 月 NEC ソリューションイノベータ株式会社

1.4.3. TOE の論理的範囲

図 1.4-2 に、TOE 及びその IT 環境が提供する機能を示す。各端末の太破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 Ver9.0 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。

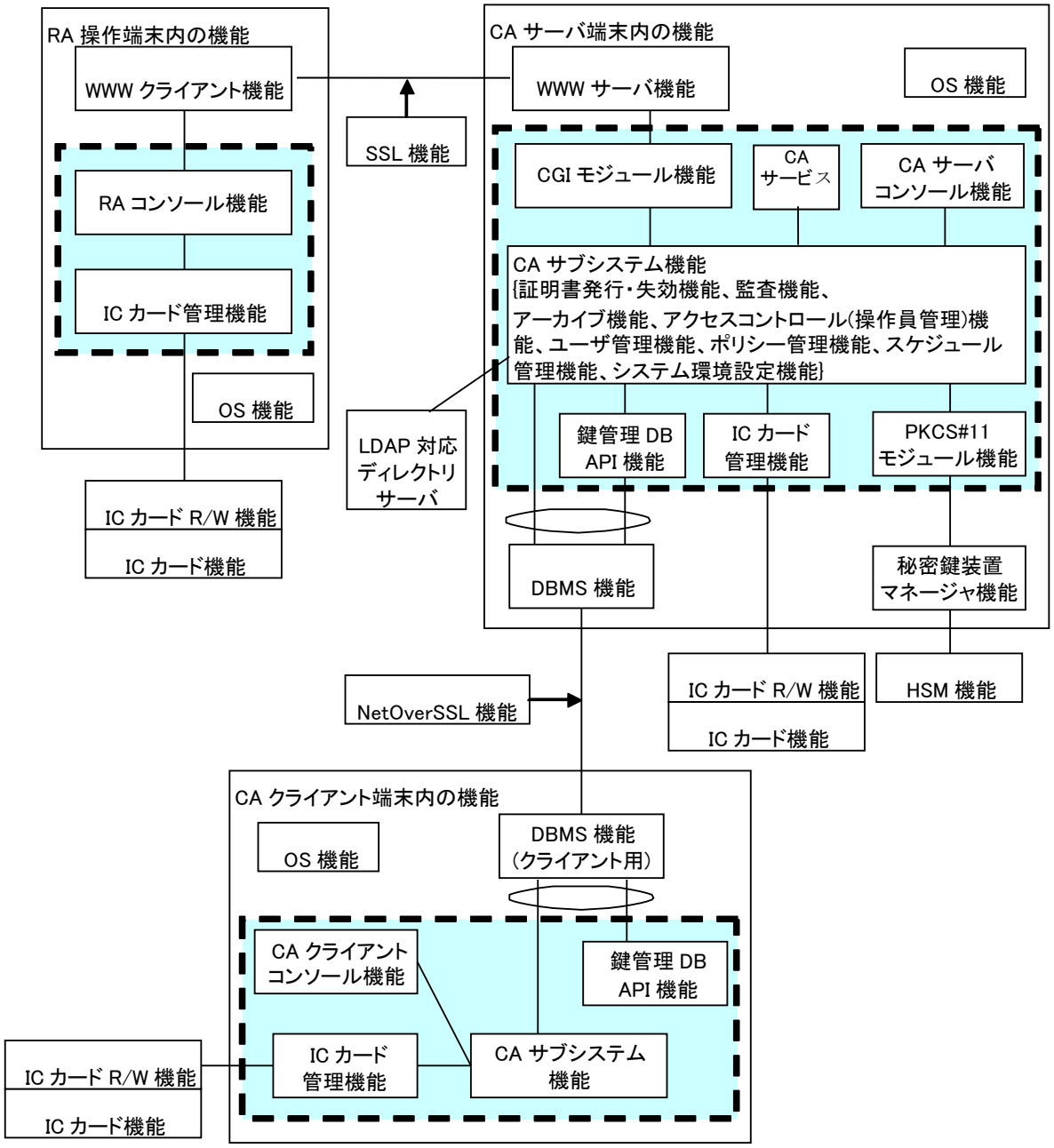

図 1.4-2：TOE とその IT 環境が提供する機能

1.4.3.1. TOE 範囲内の機能

図 1.4-2 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。

(1) **CA サーバ端末**

① CA サーバコンソール機能：

TOE 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、旧世代自己署名証明書・リンク証明書失効ツール、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。

(ア) システム管理 GUI：

証明書発行・失効機能、監査機能、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。

(イ) 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。

(ウ) CA 鍵・証明書更新ツール：

認証局の秘密鍵及び CA 証明書を更新する。

(エ) 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。CA 証明書失効以降、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。

(オ) 旧世代自己署名証明書・リンク証明書失効ツール：

CA 鍵・証明書更新ツールによって更新された更新前の CA 証明書、更新時に発行されたリンク証明書を失効する。

(カ) 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。

(キ) 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。

(ク) 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。

(ケ) 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。
(コ) 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) サービス監視ツール：
CA サービスが正常に動作しているかどうかを監視する。
(シ) 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。

② CA サブシステム機能：
認証局としての機能を提供する以下の機能から構成される。
証明書発行・失効機能、監査機能、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。

③ CA サービス機能：
Windows サービスプログラムとして動作し、証明書、および失効リストの発行処理を行う。

④ 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。

⑤ 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。

⑥ 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。

⑦ 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。

⑵ CA クライアント端末

① CA クライアントコンソール機能：

PKI サーバ/Carassuit 電子政府版 Ver9.0 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。

(ア) システム管理 GUI：

証明書発行・失効機能、監査機能、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。

(イ) 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。

(ウ) 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。

(エ) サービス監視ツール：

CA サーバ上の CA サービスが正常に動作しているかどうかを監視する。

② 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。

③ 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。

④ 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。

⑶ RA 操作端末

① RA コンソール機能：

リモートで EE 証明書発行要求を登録する。証明書受取、証明書検索、IC カード発行依頼ファイルの取得を行う。

② 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、3.1.1 節 TOE 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。

⑴ **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。

⑵ **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。この間は一般操作員の識別・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。

⑶ **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。この間は一般操作員の識別・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。

⑷ **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。

⑸ **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）が送受信される。

(8) **CA サーバ端末の CA サーバコンソール機能、CA クライアント端末の CA クライアントコンソール機能、RA 操作端末の RA コンソール機能：**

これら機能から､機関もしくは EE の秘密鍵と証明書が PKCS#12 ファイルとして出力される。PKCS#12 ファイル内の秘密鍵と証明書は、改ざん検知のための HMAC 付加と暴露防止のための暗号化により保護される。

EE IC カード発行情報は､IC カード発行依頼ファイルとしてファイル出力される。IC カード発行依頼ファイルは IC カードへ情報を書き込み（TOE 範囲外の機能）EE へ配布するために一時的に作成されるものであり、暴露防止のための暗号化によって保護される。IC カード書き込み前の IC カード発行依頼ファイルの削除、もしくは改ざんが発生した場合には、IC カード発行依頼ファイルを再取得することで回復できる。

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。

(1) **CA サーバ端末**

① 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。

② 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。

③ 識別認証機能：

上級操作員による ID／パスワード認証、複数認証メカニズムのサポート、パスワ

ードの品質の検証、アカウントロック。

④ 暗号機能：

TOE の資産の署名・署名検証、暗号化・復号、ハッシュ値生成。

⑤ 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。

⑵ CA サーバ端末、CA クライアント端末

① 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。

② 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。

③ 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、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。

④ 暗号機能：

TOE の資産の署名・署名検証、暗号化・復号、ハッシュ値生成。

⑤ 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。

⑶ RA 操作端末

① 監査機能：

セキュリティ関連事象の監査記録生成。

② アクセス制御機能：

一般操作員の種別によるアクセス制御。

③ 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。

④ 暗号機能：

TOE の資産の暗号化・復号、ハッシュ値生成。

1.4.3.2. TOE 範囲外の機能

図 1.4-2 において、TOE 範囲外にある機能について説明する。

(1) CA サーバ端末

① 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。

② WWW サーバ機能：
RA 操作端末からの要求を処理する。

③ DBMS 機能：
TOE データを管理する。

④ 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。

(2) CA クライアント端末

① 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。

② 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。

(3) RA 操作端末

① 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。

② 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。

(4) その他ハードウェア

① HSM 機能：
認証局鍵ペアを生成・管理する機能。耐タンパ機能。

② 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。

③ IC カード機能：
一般操作員の PIN 認証を行う。

(5) 通信パス

① Net Over SSL 機能：
DBMS(Oracle)が提供する機能で、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)機能間の通信パスを暗号化する。

② 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。

(1) IC カード：

認証機能(PIN 認証)

(2) HSM：

暗号機能(認証局鍵ペアの生成など)、物理的保護機能

(3) OS：

識別認証機能、アクセス制御機能

(4) 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)

(5) WWW サーバ・WWW クライアント：

高信頼性チャネル機能(SSL)

2. 適合主張

本章では、CC 適合主張、PP 主張、パッケージ主張について記述する。

2.1. CC 適合主張

本 ST 及び TOE の CC 適合主張は、以下のとおりである。

ST と TOE が適合を主張する CC のバージョン：

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 2017 年 4 月 バージョン 3.1 改訂第 5 版 翻訳第 1.0 版
パート 2：セキュリティ機能コンポーネント 2017 年 4 月 バージョン 3.1 改訂第 5 版 翻訳第 1.0 版
パート 3：セキュリティ保証コンポーネント 2017 年 4 月 バージョン 3.1 改訂第 5 版 翻訳第 1.0 版

CC パート 2 に対する ST の適合：CC パート 2 適合
CC パート 3 に対する ST の適合：CC パート 3 適合

2.2. PP 主張

本 ST が適合している PP はない。

2.3. パッケージ主張

本 ST は EAL3 適合である。

2.4. 適合根拠

本 ST は PP 適合を主張していないので、PP 適合根拠はない。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威

3.1.1. TOE 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
- 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(1.4.3 節の 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(一般操作員証明書、一般操作員秘密鍵)、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。

3.1.2. 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 カード発行依頼ファイル暴露）
高度な専門知識を持たない不正な利用者が、CA サーバ端末、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 カード発行依頼ファイルに直接アクセスすることにより、EE IC カード発行依頼ファイルを暴露するかもしれない。

3.2. 組織のセキュリティ方針

各項を、政府認証基盤の要求事項に準拠して定める。参照した政府認証基盤の規定は「8.2. 参照」[4][5]である。

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。本方針は、[5]の「4.6 アーカイブ」に準拠する。

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。本方針は[4]の「6.1.3 権限の管理」に準拠する。

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。本方針は[5]の「5.2 手続き面の管理 (8)監査ログ検査者」に準拠する。

P.CA_PAIRWISE_KEY（認証局鍵ペア）
TOE によって使われる認証局鍵ペアは、FIPS PUB 140-1 または 140-2 レベル３またはレベル３相当の HSM、PKCS に従って生成・破棄・操作されるものとする。また認証局秘密鍵は HSM により物理的に保護されなければならない。本方針は[5]の「6.1 鍵ペア生成とインストール」及び「6.2 秘密鍵の保護」に準拠する。

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。本項目は[4]の「6.1 情報システムのセキュリティ機能」及び「7.1 端末・サーバ装置等」に準拠する。

3.3. 前提条件

3.3.1. 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 に関連する権限を持つ利用者として、職務上 TOE の操作が必要な主体のみが上級操作員、一般操作員、監査ログ検査者となるように利用者登録を行う。TOE を利用する必要がなくなった場合には、当該利用者の登録を削除する。

3.3.2. 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である CA サーバ端末は、端末に接続される周辺装置（IC カードリーダ／ライタ及び、HSM）と共に、入退出管理されたセキュアルームに設置される。RA 操作端末、CA クライアント端末は、各端末に接続される周辺装置（IC カードリーダ／ライタ）と共に、不正侵入できないよう制御された場所に設置される。設置場所の物理的セキュリティレベルは政府認証基盤の要求事項に準拠して「8.2　参照」[5]に示す文書中「5.1.2 物理的アクセス」によって規定される。

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。

3.3.3. 接続的前提

A.NETWORK（ネットワーク環境）
TOE の CA サーバ端末、CA クライアント端末、および RA 操作端末が接続されている内部ネットワークは、それら以外の外部端末が接続されているネットワークからファイアウォールで分離され直接接続されない。

A.TRUSTED_PATH（高信頼チャネル）
CA サブシステムとデータベース間、および WWW サーバと WWW クライアント間のネットワーク上は、TSF データ及び利用者データがその間で盗聴されることがないように、高信頼チャネルを用いて通信が行われる。

A.PERIPHERAL_INTERFACE（周辺装置）
TOE に接続する周辺装置（HSM、IC カードリーダ／ライタ）は TOE の付近に設置される。TOE と周辺装置（HSM、IC カードリーダ／ライタ）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。

4. セキュリティ対策方針

本章では、TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針、セキュリティ対策方針根拠について記述する。

4.1. TOE の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。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。

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ハッシュ値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ハッシュ値を再作成して添付されているハッシュ値と比較し、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。

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。

O.ICC_FILE_CRYPT（EE IC カード発行依頼ファイルの暗号）
TOE は、EE IC カード発行依頼ファイルを暗号化する。

4.2. 運用環境の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_PAIRWISE_KEY（認証局鍵ペア）
TOE によって使われる認証局鍵ペアは、FIPS PUB 140-1 または 140-2 レベル 3 またはレベル 3 相当の HSM、PKCS に従って生成・破棄・操作されなければならない。また認証局秘密鍵は HSM により物理的に保護されなければならない。

OE.TRUSTED_PATH（高信頼チャネル）
CA サブシステムーデータベース間のネットワークは DBMS(Oracle)が提供する Net Over SSL 機能による高信頼チャネル、および WWW サーバーWWW クライアント間のネットワークは SSL 機能による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なければならない。オペレーティングシステムが信頼できるタイムスタンプ情報を提供するよう、上級操作員が管理しなければならない。

OE.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。

OE.PERIPHERAL_INTERFACE（周辺装置）
TOE に接続する周辺装置（IC カードリーダ／ライタ、HSM）は、TOE の付近に設置されなければならない。TOE と周辺装置（IC カードリーダ／ライタ、HSM）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。

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）
職務上 TOE の操作が必要な主体のみが TOE に関連する権限・役割をもつ利用者である上級操作員、一般操作員、監査ログ検査者として任命され、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。TOE の操作の必要がなくなった場合には、当該利用者の登録は削除されなければならない。

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装置（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装置（IC カードリーダ／ライタ）、RA 操作端末とその周辺装置（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。

4.3. 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 4.3.1 に示す。

表 4.3.1：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	P.ISSUE	P.AUTHORITY	P.AUDITOR	P.CA_PAIRWISE_KEY	P.OS_DB	A.PASSWORD_MANAGEMENT	A.PIN_ICC_MANAGEMENT	A.SAFE_PLACE	A.BACKUP_MEDIA	A.USER_RESTRICTION	A.NETWORK	A.TRUSTED_PATH	A.PERIPHERAL_INTERFACE
O.I&A	×																
O.ACCESS_CONTROL		×				×											
O.AUDIT	×	×															
O.DATA_INTEGRITY			×														
O.CRYPTOGRAPHY			×														
O.ISSUE_CONFIRMATION					×												
O.ICC_FILE_CRYPT				×													
OE.ICC_PROTECTION	×																
OE.CA_PAIRWISE_KEY								x									
OE.TRUSTED_PATH																x	
OE.TRUSTED_OS_DB									x								
OE.NETWORK															×		
OE.PERIPHERAL_INTERFACE																	×
OEN.AUTHORIZATION_SETTING	×	×				×	×							×			
OEN.AUTHORIZATION_DUTY	×	×				×											
OEN.PASSWORD_MANAGEMENT										×							
OEN.PIN_ICC_MANAGEMENT											×						
OEN.SAFE_PLACE												×					
OEN.BACKUP_MEDIA													×				

表 4.3.1 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、OE.ICC_PROTECTION、OEN.AUTHORIZATION_SETTING、OEN.AUTHORIZATION_DUTY によって対抗される。

TOE は、以下のように識別認証、不正ログイン察知を行うことにより、脅威を軽減する。

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)。また、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。O.AUDIT により、TOE はログオンの失敗を監査ログに記録する。

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。

TOE は、以下のようにアクセス管理、不正操作の察知を行うことにより、脅威を軽減する。

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.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。

TOE は、以下のように暗号化による暴露防止、改ざん検出により、脅威を軽減する。

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。
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 カード発行依頼ファイル暴露）
この脅威は、O.ICC_FILE_CRYPT によって対抗される。
TOE は、以下のように暗号化による暴露防止により、脅威を軽減する。
O.ICC_FILE_CRYPT により、TOE は EE IC カード発行依頼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 カード発行依頼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。

○組織のセキュリティ方針
組織のセキュリティ方針は、TOE を利用した PKI における認証局および登録局の機能を利用する組織において、政府認証基盤の要求事項に準拠することを想定している。参照した政府認証基盤の規定は「8.2. 参照」[4][5]である。

P.ISSUE（発行）
この組織のセキュリティ方針は、参照文書[5]の、アーカイブデータに対する項目を遵守することを想定している。
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。
上述のことより、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。

P.AUTHORITY（権限付与）
この組織のセキュリティ方針は、参照文書[4]のうち情報システムのセキュリティ機能に関わる項目の中で、権限管理に対する項目を遵守することを想定している。
OEN.AUTHORIZATION_SETTING により、TOE を利用する組織において、上級操作員、一般操作員、監査ログ検査者が任命される。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.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。
上述のことより、この組織のセキュリティ方針は、OEN.AUTHORIZATION_SETTING、OEN.AUTHORIZATION_DUTY、O.ACCESS_CONTROL によって実現できる。

P.AUDITOR（監査ログ検査者）
この組織のセキュリティ方針は、参照文書[5]の、監査ログ検査者に対する項目を遵守することを想定している。
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。
上述のことより、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。

P.CA_PAIRWISE_KEY（認証局鍵ペア）
この組織のセキュリティ方針は、参照文書[5]の、認証局秘密鍵の管理に対する項目を遵守し、認証局鍵ペアを管理することを想定している。
OE.CA_PAIRWISE_KEY により、認証局鍵ペアは、FIPS PUB 140-1 または 140-2 レベル３またはレベル３相当の HSM、PKCS に従って生成・破棄・操作され、認証局秘密鍵は HSM により物理的に保護される。
上述のことより、この組織のセキュリティ方針は OE.CA_PAIRWISE_KEY によって実現される。

P.OS_DB（信頼できる OS／DB）f
この組織のセキュリティ方針は、参照文書[4]のうち情報システムのセキュリティ機能に関わる項目の中で、主体認証、および端末・サーバ装置等に対する項目を遵守することを想定している。
OE.TRUSTED_OS_DB により、OS・DB による適切な識別認証がなされるので、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。OS により信頼できるタイムスタンプ情報が提供されるよう、上級操作員が管理する。
上述のことより、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。

○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重要度に応じたセキュリティレベルで入退室が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 の利用者として登録される上級操作員、一般操作員、監査ログ検査者は許可された主体のみであり、また不要となった利用者は削除される。

A.NETWORK（ネットワーク環境）
この前提条件は OE.NETWORK によって実現できる。
OE.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.TRUSTED_PATH（高信頼チャネル）
この前提条件は OE.TRUSTED_PATH によって対抗される。
OE.TRUSTED_PATH により、CA サブシステムーデータベース間の通信には高信頼チャネルを用い、WWW サーバー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、その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。

A.PERIPHERAL_INTERFACE（周辺装置）
この前提条件は、OE.PERIPHERAL_INTERFACE により実現できる。
OE.PERIPHERAL_INTERFACE により、TOE に接続する周辺装置（HSM、IC カードリーダ／ライタ）は TOE の付近に設置され、TOE と周辺装置（HSM、IC カードリーダ／ライタ）の間で盗聴されないように接続される。

5. 拡張コンポーネント定義

本 ST で定義される拡張コンポーネントはない。

6. セキュリティ要件

本章では、セキュリティ要件を記述する。

6.1. セキュリティ機能要件

TOE が提供するセキュリティ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。
なお、以下の機能エレメントの記述において、「割付」、「選択」及び「詳細化」は、エレメントとは別に示す。「繰返し」は、コンポーネントラベルの後に英小文字、エレメントラベルの後に ドットと英小文字を付与して示す。

○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 サービスの起動／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 カード発行依頼ファイルの出力
・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
・パスワード試行可能回数の変更
・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 6.1.1 に示す。下線は対応する監査レベルを表す。

表 6.1.1：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（注釈１）
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ータ。	なし（注釈２）
FAU_SAR.3b	a) 詳細：閲覧に使用されるパラメータ。	なし（注釈２）
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（注釈３）
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.1	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 カード発行依頼ファイルの出力

FCS_CKM.4	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.1	a) 最小: 成功と失敗及び暗号操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	a) 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 カード発行依頼ファイルの出力 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キュリティ属性。	以下の操作についての情報 a), b), c) 証明書発行・失効機能の実行 a), b), c) CA の鍵情報の参照 a), b), c)バックアップ、リカバリの実行 a), b), c)アクセスコントロール（操作員管理）機能の実行 a), b), c) ARL の外部出力 a), b), c) CRL の外部出力 a), b), c)アーカイブデータの外部出力 a), b), c)アーカイブデータの参照、検索 a), b), c)システムパラメータの設定 a), b), c)スケジュール管理の設定 a), b), c)証明書プロファイルの新規登録、変更、削除 a), b), c)監査データの参照及び検索 a), b), c)監査データの外部ファイル出力、印刷 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 a), b), c)機関証明書プロファイルでの証明書の申請 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 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 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 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 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 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 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
FIA_AFL.1	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（注釈４） 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（注釈４） 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（注釈４） b) データベースパスワードの変更
FIA_UAU.2	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.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用;	a), b) 操作員の識別と確認

	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。	
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)パスワード試行可能回数の変更
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

注釈１： 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。

注釈２：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。

注釈３：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。

注釈４：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。

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(該当する場合)、事象の結果（成功または失敗）；及び

b) 各監査事象種別に対して、PP／ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付：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　識別された利用者のアクションがもたらした監査事象に対し、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、監査データの[割付:選択方法、及び/または 並べ替え方法]を適用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]：以下の指定可能な検索条件の任意の組み合わせ(論理積)

・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）

[割付:選択方法、及び/または 並べ替え方法]：条件検索

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、監査データの[割付:選択方法、及び/または 並べ替え方法]を適用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

[割付:選択方法、及び/または 並べ替え方法]：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、監査証跡に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、監査証跡に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]：CA 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 発信の選択的証明

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.1 暗号鍵生成

下位階層：　なし

FCS_CKM.1.1　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 (RSA)	・SP800-90A ・PKCS #1	・疑似乱数生成アルゴリズム ・PKCS#1	2048bit 3072bit 4096bit から選択
操作員鍵ペア (RSA)	・SP800-90A ・PKCS #1	・疑似乱数生成アルゴリズム ・PKCS#1	2048bit
バックアップデータ署名用鍵ペア (RSA)	・SP800-90A ・PKCS #1	・疑似乱数生成アルゴリズム ・PKCS#1	2048bit
システム共通鍵 (AES)	SP800-90A	疑似乱数生成アルゴリズム	256bit
データベース共通鍵 (AES)	SP800-90A	疑似乱数生成アルゴリズム	256bit
共通鍵保護鍵	なし（注１）	非公開独自方式(注１)	256bit
PKCS#12 ファイル内秘密鍵保護鍵 (3Key Triple DES)	PKCS#5	SHA-1（注２） (パスフレーズをハッシュ演算で加工することで鍵とし	168bit

		ている)	
PKCS#12 ファイル内証明書保護鍵 (3Key Triple DES)	PKCS#12	SHA-1（注２） (パスフレーズをハッシュ演算で加工することで鍵としている)	168bit
PKCS#12 ファイル HMAC 鍵	PKCS#12	SHA-1（注３） (パスフレーズをハッシュ演算で加工することで鍵としている)	160bit
EE IC カード発行依頼ファイル保護鍵 (3Key Triple DES)	FIPS PUB 180-4	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） 共通鍵保護鍵は、この鍵自体の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。

（注２） PKCS#5 の規格上、PKCS#12 データに含める暗号鍵及び、証明書を暗号化する為の鍵として、パスフレーズを SHA-1 ハッシュ演算した値を用いるよう定められている為、SHA-1 の使用は許容される。

（注３） PKCS#12 の規格上、PKCS#12 データを暗号化する為に使用する暗号アルゴリズムとして HMAC を使用すると定められている。また、HMAC は、パスフレーズを SHA-1 ハッシュ演算して求めた値から鍵を生成する仕組みである。規格に定められた仕様である為、SHA-1 の使用は許容される。

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

FCS_CKM.4 暗号鍵破棄

下位階層： なし

FCS_CKM.4.1 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]

FCS_COP.1 暗号操作

下位階層：　　なし

FCS_COP.1.1　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	HSM が SafeNet LunaSA の場合 2048bit, 3072bit, 4096bit から選択 HSM が CK-Guard の場合 2048bit	・操作員証明書の署名検証 ・CRL の署名検証
		ECDSA	HSM が SafeNet LunaSA の場合 256bit(P-256), 384bit(P-384), 512bit(P-521) から選択	
操作員秘密鍵／公開鍵	PKCS#1	RSA	2048bit	認証用のチャレンジの署名および署名検証
バックアップデータ署名用秘密鍵／公開鍵	PKCS#1	RSA	2048bit	バックアップデータの署名およびリカバリ時の署名検証
システム共通鍵	FIPS PUB 197	AES	256bit	・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 197	AES	256bit	・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 197	AES	256bit	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 カード発行依頼ファイル保護鍵	SP 800-67	Triple DES	168bit	EE IC カード発行依頼ファイルの暗号化
PKCS#12 ファイル内秘密鍵保護鍵	SP 800-67	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
PKCS#12 ファイル内証明書保護鍵	SP 800-67	Triple DES	168bit	・機関証明書と秘密鍵の PKCS#12 出力時の証明書暗号化 ・EE 証明書と秘密鍵の PKCS#12 出力時の証明書暗号化
PKCS#12 ファイル HMAC 鍵	RFC2104	HMAC-SHA-1	160bit	・機関証明書と秘密鍵の PKCS#12 出力時の鍵付きハッシング ・EE 証明書と秘密鍵の PKCS#12 出力時の鍵付きハッシング
なし	FIPS PUB 180-2 (Change Notice1)	SHA-224 SHA-256 SHA-384 SHA-512	－	機関証明書、操作員証明書、EE 証明書、失効リスト発行のハッシュ生成
なし	FIPS PUB 180-1	SHA-1 (注 1)	－	識別・認証情報のハッシュ比較 アクセスコントロール情報のハッシュ比較 システム設定情報のハッシュ比較 監査ログのハッシュ比較 アーカイブデータのハッシュ比較 バックアップデータのハッシュ比較
なし	FIPS PUB 180-2	SHA-256	－	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 バックアップ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

(注 1)SHA-1 は、本バージョンの TOE へ移行する以前のバージョンの TOE で生成された SHA-1 ハッシュ値を対象とした比較検証においてのみ使用し、本バージョンの TOE 内で新たに SHA-1 ハッシュ値を生成しない。また、CRYPTOREC 暗号リストにおいて、互換性維持の為に継続利用を容認する旨が記述されている。本 TOE での SHA-1 の利用は互換性維持用途である事から、SHA-1 の利用は許容される。

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 セキュリティ属性を伴う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

○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	証明書発行・失効機能	実行
	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	
	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	
	ユーザ管理機能	
	RA コンソール機能	

[割付：アクセス制御 SFP]：Carassuit 電子政府版 Ver9.0 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
証明書発行・失効機能	なし
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	
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	
ユーザ管理機能	
RA コンソール機能	

[割付：アクセス制御 SFP]：Carassuit 電子政府版 Ver9.0 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 サービスの起動／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	証明書発行・失効機能	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	システム環境設定機能	
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	証明書発行・失効機能	

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	証明書発行・失効機能	
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	システム環境設定機能	
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	ポリシー管理機能	
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	証明書発行・失効機能	
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	証明書発行・失効機能	
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	証明書発行・失効機能	
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	証明書発行・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	証明書発行・失効機能	
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	RA コンソール機能	
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	証明書発行・失効機能	
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	証明書発行・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	証明書発行・失効機能	

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、次の追加規則、[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許可する規則]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許可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許可する規則]：なし

FDP_ACF.1.4　TSF は、次の追加規則、[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.1 認証失敗時の取り扱い

下位階層：　なし

FIA_AFL.1.1　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によって変更可能)

FIA_AFL.1.2　不成功の認証試行が定義した回数[選択：に達する、を上回った]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。

[選択：に達する、を上回った]：に達する

[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]

[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.2 アクション前の利用者認証
下位階層：　　FIA_UAU.1

FIA_UAU.2.1　TSF は、その利用者を代行する他の TSF 仲介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.2 アクション前の利用者識別

下位階層：　FIA_UID.1

FIA_UID.2.1　TSF は、その利用者を代行する他の TSF 仲介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、以下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、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に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 サービスの起動／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、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付：属性の変更の規則]

[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：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	許可された識別された役割
アクセス制御機能	改変する（操作員人数）	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)
識別認証機能	決定する（一般操作員の認証方式）	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)、一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)

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

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 TSF 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

表 6.1.2：FMT_MTD.1a TSF データの管理

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(操作員管理のアクセス権限を持つ権限グループに所属)
	操作員 ID	削除、[その他の操作：登録]	
	操作員種別	[その他の操作：登録済みデータから選択]	
	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：登録済みデータから選択]	
	パスワード	削除、改変、[その他の操作：登録]	
		改変	TSF へログイン中の上級操作員(自分自身のパスワードについてのみ許可される)
一般操作員データ		-	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)、一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)
	操作員 ID	削除、[その他の操作：登録]	
	操作員種別	[その他の操作：登録済みデータから選択]	
	秘密鍵	[その他の操作：生成]	
	証明書	[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：登録済みデータから選択]	
	パスワードまたは PIN	削除、改変、[その他の操作：登録]	
		改変	TSF へログイン中の一般操作員(自分自身のパスワードまたは PIN についてのみ許可される)

依存性：　　FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MTD.1 b 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]：

・パスワード試行可能回数

[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

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

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 TSF 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

表 6.1.3：FMT_MTD.1c TSF データの管理

TSF データ		操作	許可された識別された役割
上級操作員権限グループデータ		-	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)
	権限グループ ID(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	
一般操作員権限グループデータ		-	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)、一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)
	権限グループ ID(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_SMR.1 セキュリティの役割
　　FMT_SMF.1 管理機能の特定

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 TSF 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

表 6.1.4：FMT_MTD.1d TSF データの管理

TSF データ	操作	許可された識別された役割
アーカイブログ	問い合わせ（参照・検索）	上級操作員(アーカイブ参照のアクセス権限を持つ権限グループに所属)、一般操作員(アーカイブ参照のアクセス権限を持つ権限グループに所属)
	削除、外部ファイルへの保管	上級操作員(アーカイブ管理のアクセス権限を持つ権限グループに所属)、一般操作員(アーカイブ管理のアクセス権限を持つ権限グループに所属)
	エクスポート	上級操作員(アーカイブ参照とアーカイブ管理のアクセス権限を持つ権限グループに所属)、一般操作員(アーカイブ参照とアーカイブ管理のアクセス権限を持つ権限グループに所属)
システム設定情報	削除、改変、登録	上級操作員(システム環境設定のアクセス権限を持つ権限グループに所属)、一般操作員(システム環境設定のアクセス権限を持つ権限グループに所属)

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

FMT_SMF.1 管理機能の特定

下位階層：　なし

FMT_SMF.1.1　TSF は、以下の管理機能を実行することができなければならない。：[割付：TSF によって提供される管理機能のリスト]

[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

・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)による上級操作員または一般操作員権限グループ ID の登録、削除

・一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による一般操作員権限グループ ID の登録、削除

・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)または一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による権限グループが保持するアクセス権限の改変

・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)による上級操作員または一般操作員 ID の登録、削除

・一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による一般操作員

ID の登録、削除
・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)による上級操作員のパスワードの登録、改変、削除
・上級操作員による自身のパスワードの改変
・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)または一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による一般操作員のパスワードまたは PIN の登録、改変、削除
・一般操作員による自身のパスワードの改変
・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)または一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による一般操作員の秘密鍵の生成
・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)または一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による一般操作員の証明書の生成、失効
・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)による操作員種別(上級操作員)の登録済みデータからの選択
・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)または一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による操作員種別(一般操作員)の登録済みデータからの選択
・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)による上級操作員の所属する権限グループの登録済みデータからの選択
・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)または一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による一般操作員の所属する権限グループの登録済みデータからの選択
・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)または一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)による一般操作員の認証方式の決定
・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)による機能の要求する操作員人数の改変
・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)によるパスワード試行可能回数の改変
・上級操作員(アーカイブ参照のアクセス権限を持つ権限グループに所属)または一般操作員(アーカイブ参照のアクセス権限を持つ権限グループに所属)によるアーカイブデータの参照
・上級操作員(アーカイブ管理のアクセス権限を持つ権限グループに所属)、または一般操作員(アーカイブ管理のアクセス権限を持つ権限グループに所属)によるアーカイブデー

タの削除、外部ファイルへの保管

・上級操作員(アーカイブ参照とアーカイブ管理のアクセス権限を持つ権限グループに所属)、または一般操作員(アーカイブ参照とアーカイブ管理のアクセス権限を持つ権限グループに所属)によるアーカイブデータのエクスポート

・上級操作員(システム環境設定のアクセス権限を持つ権限グループに所属)または一般操作員(システム環境設定のアクセス権限を持つ権限グループに所属)による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)。	a) 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。	a) 各種証明書の発行、失効、および失効リストの発行
FCS_CKM.1	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。	a) なし（アクションは固定であり、管理対象とならない）
FCS_CKM.4	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。	a) なし（アクションは固定であり、管理対象とならない）
FCS_COP.1	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。	a) なし（属性は固定であり、管理対象とならない）
FIA_AFL.1	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。	a) 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の管理
FIA_SOS.1a	a) 秘密の検証に使用される尺度の管理。	a) 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。	a) 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。	a) なし（尺度は固定であり、管理対象とならない）
FIA_UAU.2	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	a) 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、削除、改変 b) 上級操作員及び一般操作員のパスワー

機能要件	管理要件	管理項目
		ドあるいは PIN の改変
FIA_UAU.5	a) 認証メカニズムの管理; b) 認証に対する規則の管理。	a) および b) 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.2	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、削除
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。 b) 許可管理者は、サブジェクトのセキュリティ属性を変更できる。	a) なし（デフォルトの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) b) 権限グループの保持するアクセス権限の改変、操作員の所属する権限グループの変更
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。	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.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) パスワード試行可能回数の管理
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。	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.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。	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_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)

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
- 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)
- 上級操作員(アーカイブ管理のアクセス権限を持つ権限グループに所属)
- 上級操作員(アーカイブ参照のアクセス権限を持つ権限グループに所属)

・上級操作員(アーカイブ参照とアーカイブ管理のアクセス権限を持つ権限グループに所属)
・上級操作員(システム環境設定のアクセス権限を持つ権限グループに所属)
・一般操作員
・一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)
・一般操作員(アーカイブ管理のアクセス権限を持つ権限グループに所属)
・一般操作員(アーカイブ参照のアクセス権限を持つ権限グループに所属)
・一般操作員(アーカイブ参照とアーカイブ管理のアクセス権限を持つ権限グループに所属)
・一般操作員(システム環境設定のアクセス権限を持つ権限グループに所属)

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。
・上級操作員は上級操作員権限グループに付与可能なアクセス権を同時に担うことができる。
・一般操作員は一般操作員権限グループに付与可能なアクセス権を同時に担うことができる。

依存性：　FIA_UID.1 識別のタイミング

6.2. セキュリティ保証要件

TOE セキュリティ要件を示す。
本 TOE の評価保証レベルは EAL3 である。全てのセキュリティ保証要件は CC パート 3 に既定されているセキュリティ保証コンポーネントを直接適用する。

(1) 開発（ADV）

ADV_ARC.1	: セキュリティアーキテクチャ記述
ADV_FSP.3	: 完全な要約を伴う機能仕様
ADV_TDS.2	: アーキテクチャ設計

(2) ガイダンス文書（AGD）

AGD_OPE.1	: 利用者操作ガイダンス
AGD_PRE.1	: 準備手続き

(3) ライフサイクルサポート（ALC）

ALC_CMC.3	: 許可の管理
ALC_CMS.3	: 実装表現の CM 範囲
ALC_DEL.1	: 配付手続き
ALC_DVS.1	: セキュリティ手段の識別
ALC_LCD.1	: 開発者によるライフサイクルモデルの定義

(4) セキュリティターゲット評価（ASE）

ASE_CCL.1	: 適合主張
ASE_ECD.1	: 拡張コンポーネント定義
ASE_INT.1	: ST 概説
ASE_OBJ.2	: セキュリティ対策方針
ASE_REQ.2	: 派生したセキュリティ要件
ASE_SPD.1	: セキュリティ課題定義
ASE_TSS.1	: TOE 要約仕様

(5) テスト（ATE）

ATE_COV.2	: カバレージの分析
ATE_DPT.1	: テスト：基本設計
ATE_FUN.1	: 機能テスト
ATE_IND.2	: 独立テスト – サンプル

(6) 脆弱性評定（AVA）

AVA_VAN.2	: 脆弱性分析

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

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 6.3.1 に示す。この表で示すとおり、各セキュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対応している。

表 6.3.1：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	O.ICC_FILE_CRYPT
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.1					×		×
FCS_CKM.4					×		×
FCS_COP.1	×			×	×		×
FDP_ACC.1		×					
FDP_ACF.1		×					
FIA_AFL.1	×						
FIA_ATD.1		×					
FIA_SOS.1a	×						
FIA_SOS.1b	×						
FIA_SOS.1c	×						
FIA_UAU.2	×						
FIA_UAU.5	×						
FIA_UID.2	×						
FIA_USB.1		×					
FMT_MOF.1	×	×					
FMT_MTD.1a	×	×					
FMT_MTD.1b		×					
FMT_MTD.1c		×					
FMT_MTD.1d						×	
FMT_SMF.1		×				×	
FMT_SMR.2		×				×	

次に、各 TOE セキュリティ対策方針が、セキュリティ機能要件により実現できる事を説明する。

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、FCS_COP.1、FIA_AFL.1、FIA_SOS.1a、FIA_SOS.1b、FIA_SOS.1c、FIA_UAU.2、FIA_UAU.5、FIA_UID.2、FMT_MOF.1、FMT_MTD.1a で実現できる。

FCS_COP.1 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署名検証を行う。FIA_AFL.1 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（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.2 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.2 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 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。

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.1b、FMT_MTD.1c、FMT_SMF.1、FMT_SMR.2 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、FMT_MTD.1b 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。

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 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、CA サービス停止のアクションをとるようにする。

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.1 で実現できる。

FCS_COP.1 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.1、FCS_CKM.4、FCS_COP.1 で実現できる。

FCS_CKM.1 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.4 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.1 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、及び TSF データのハッシュ操作を行う。アルゴリズムと鍵長の指定は、[7]、および情報セキュリティ政策会議決定である[6]に準拠している。

O.ISSUE_CONFIRMATION（発行確証）

このセキュリティ対策方針は、FCO_NRO.2、FMT_MTD.1d、FMT_SMF.1、FMT_SMR.2 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。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。

O.ICC_FILE_CRYPT（EE IC カード発行依頼ファイルの暗号）
このセキュリティ対策方針は、FCS_CKM.1、FCS_CKM.4、FCS_COP.1 で実現できる。FCS_CKM.1 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.4 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_CKM.1 は、FCS_COP.1 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、EE IC カード発行情報の暗号化を行う。
アルゴリズムと鍵長の指定は、[7]および情報セキュリティ政策会議決定である[6]に準拠している。

更に補足として、セキュリティ機能要件 FMT_MOF.1、および FAU_GEN.1 が、明示的な依存関係は持たないが、以下の観点から TOE セキュリティ対策方針の実現を相互補完することを説明する。

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。

無効化抑止
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.2、 FIA_UID.2、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。

6.3.2. 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 6.3.2 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 6.3.2：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.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FIA_ATD.1	FIA_UAU.2	FIA_UID.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.1					×	○ $													
FCS_CKM.4				○															
FCS_COP.1				○ $	× $														
FDP_ACC.1								×											
FDP_ACF.1							×					× *							
FIA_AFL.1										× ^									

FIA_ATD.1																		
FIA_SOS.1a																		
FIA_SOS.1b																		
FIA_SOS.1c																		
FIA_UAU.2											× ^							
FIA_UAU.5																		
FIA_UID.2																		
FIA_USB.1									×									
FMT_MOF.1																	×	×
FMT_MTD.1a																	×	×
FMT_MTD.1b																	×	×
FMT_MTD.1c																	×	×
FMT_MTD.1d																	×	×
FMT_SMF.1																		
FMT_SMR.2											× ^							

表 6.3.2 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。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。

FAU_GEN.1 の依存関係、FCS_CKM.1 の依存関係の一部、FCS_COP.1 の依存関係の一部、および FDP_ACF.1 の依存関係は満たされていないが、問題がない根拠を以下に示す。

・FAU_GEN.1 → FPT_STM.1：
信頼できるタイムスタンプは、IT 環境であるオペレーティングシステムより提供されるため、TOE の提供するセキュリティ機能コンポーネントとしての依存関係は不要である。

・FCS_CKM.1 → FCS_COP.1：
EE 鍵は EE 証明書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_COP.1 → FDP_ITC.1、FDP_ITC.2 または FCS_CKM.1
利用者データのインポートでは操作員証明書の署名検証と CRL の署名検証は行われな

い。また、CA 公開鍵は運用環境の対策方針 OE.CA_PAIRWISE_KEY で TOE 外である HSM にて生成されたものを使用するため、この依存関係は不要である。SHA(SHA-1、SHA-224、SHA-256、SHA384、SHA-512)によるハッシュ操作には鍵を使用しないため、この依存関係は不要である。

・FCS_COP.1 → FCS_CKM.4
CA 公開鍵は公開用の鍵で機密情報ではなく削除されなくても問題がないため、この依存関係は不要である。SHA(SHA-1、SHA-224、SHA-256、SHA384、SHA-512)によるハッシュ操作には鍵を使用しないため、この依存関係は不要である。

・FDP_ACF.1 → FMT_MSA.3：
FDP_ACF.1.1 にてセキュリティ属性なしとしているオブジェクトに対するアクセス制御は、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によってのみ行われる。ゆえに、オブジェクトはセキュリティ属性を持たない。また、サブジェクト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必ず値が割り当てられ、オブジェクトに対するアクセス制御が実現する。このため静的属性初期化の要件は不要である。

6.3.3. セキュリティ保証要件根拠

PKI サーバ/Carassuit 電子政府版 Ver9.0 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。

7. TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について述べる。

7.1. TOE セキュリティ機能

本節では、TOE のセキュリティ機能を説明する。表 7.1.1 に示すように、本節で説明するセキュリティ機能は、6.1 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 7.1.1：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.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1a	FIA_SOS.1b	FIA_SOS.1c	FIA_UAU.2	FIA_UAU.5	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MTD.1a	FMT_MTD.1b	FMT_MTD.1c	FMT_MTD.1d	FMT_SMF.1	FMT_SMR.2
SF.Audit	×	×	×		×	×	×	×																						
SF.I&A															×		×	×	×	×	×	×								
SF.ACC			×	×			×						×	×		×							×	×	×	×	×	×	×	×
SF.Crypto							×			×	×	×																	×	
SF. Cer_Issue									×																				×	

7.1.1. 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。(FAU_GEN.1)

- 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。(FAU_GEN.2)

監査データは以下の監査対象事象の発生時に採取する。(FAU_GEN.1)

- 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 サービスの起動／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 カード発行依頼ファイルの出力
- 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。(FAU_STG.1)

- 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。(FAU_SAR.1)
- 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(論理積)が指定可能である。(FAU_SAR.3a)
- 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。(FAU_SAR.3b)
- 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。(FAU_SAR.１、FAU_SAR.2)

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、CA サービスの運用を停止し、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(FAU_STG.3)。
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。(FAU_SAR.１、FAU_SAR.2)

7.1.2. 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。(FDP_ACC.1)

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。上級操作員プロセス、及び一般操作員プロセスは、機能の実行を開始する場合に、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。(FIA_USB.1)

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 Ver9.0 アクセス制御方針に従う。(FDP_ACF.1、FIA_USB.1)

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、両方の操作員種別を持つことはできない。(FMT_SMR.2、FMT_SMF.1)

上級操作員は、登録時に以下のセキュリティ属性を持つ。(FIA_ATD.1、FMT_SMF.1)
- 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。(FIA_ATD.1、FMT_SMF.1)
- 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。(FMT_SMF.1)

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。(FIA_USB.1)

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 メサービス機能の起動／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。(FMT_SMF.1)

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。(FIA_ATD.1、FIA__USB.1、FMT_SMF.1)

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	対応する TOE の機能	権限グループ種別	操作員 人数
ARL 出力	証明書発行・失効機能	上級操作員 一般操作員	複数可
CA サービスの起動／停止	証明書発行・失効機能	上級操作員	複数可
CA 鍵管理	システム環境設定機能	上級操作員	複数可
CRL 出力	証明書発行・失効機能	上級操作員 一般操作員	複数可
アーカイブ管理	アーカイブ機能	上級操作員 一般操作員	複数可
アーカイブ参照	アーカイブ機能	上級操作員 一般操作員	複数可
システム環境設定	システム環境設定機能	上級操作員 一般操作員	複数可

スケジュール管理	スケジュール管理機能	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／リカバリ機能	上級操作員	複数可
ポリシー管理	ポリシー管理機能	上級操作員 一般操作員	複数可
監査ログ参照	監査機能	上級操作員 一般操作員	複数可
監査管理	監査機能	上級操作員 一般操作員	複数可
操作員管理	アクセスコントロール（操作員管理）機能	上級操作員 一般操作員	複数可
ユーザ管理	ユーザ管理機能	一般操作員	複数可
証明書情報参照	証明書発行・失効機能	上級操作員 一般操作員	複数可
機関証明書申請	証明書発行・失効機能	上級操作員 一般操作員	複数可
機関証明書取得	証明書発行・失効機能	上級操作員 一般操作員	複数可
機関証明書失効	証明書発行・失効機能	上級操作員 一般操作員	複数可
EE 証明書申請	証明書発行・失効機能	一般操作員	複数可
EE 証明書審査	登録局(RA)コンソール機能	一般操作員	単数のみ
EE 証明書取得	証明書発行・失効機能	一般操作員	複数可
EE 証明書失効	証明書発行・失効機能	一般操作員	複数可
EE IC カード発行	登録局(RA)コンソール機能	一般操作員	単数のみ

二列目に記述した機能をさらに細分化した単位でアクセス権限の範囲が設定されている。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。

上級操作員は上級操作員権限グループに付与可能なアクセス権を同時に担うことができる。また、一般操作員は一般操作員権限グループに付与可能なアクセス権を同時に担うことができる。 上級操作員権限グループと一般操作員権限グループに付与されたアクセス権は操作員管理にて維持される。また、識別認証に成功した操作員に対して、対応する操作員種別を関連付けて維持する。操作員と操作員種別の関連付けは、機能の実行を開始する場合に再取得し反映する。(FMT_SMR.2)

また、一部のアクセス権限は、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)によって、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。(FMT_MOF.1、FMT_SMF.1)

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 データと操作、および許可された役割は以下の通りである。

・「表 6.1.2 : FMT_MTD.1a TSF データの管理」に示すもの。一般操作員の認証方式は、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)、および一般操作員(操作員管理のアクセス権限を持つ権限グループに所属)により決定される。(FMT_MTD.1a、FMT_MOF.1、FMT_SMF.1)

・パスワード試行可能回数(FMT_MTD.1b、FMT_SMF.1)

・「表 6.1.3:FMT_MTD.1c TSF データの管理」に示すもの(FMT_MTD.1c、FMT_SMF.1)

・「表 6.1.4:FMT_MTD.1d TSF データの管理」に示すもの(FMT_MTD.1d、FMT_SMF.1、FAU_SAR.1、FAU_SAR.2、FAU_STG.1)

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 カード発行依頼ファイル
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(FAU_SAR.1、FAU_SAR.2、FAU_STG.1)
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	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。

7.1.3. 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。(FIA_UAU.5)

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。(FIA_UAU.2、FIA_UID.2)

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。(FIA_UAU.5)

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。(FIA_UAU.5)

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。一般操作員は、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。(FIA_AFL.1)

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 IC カード毎に設定された閾値に達すると、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。

注：PIN 誤り回数の閾値は、IC カード毎に IC カード内で管理される情報であり、TOE 範囲外の機能で変更可能である。

3. RA 操作端末における IC カードと PIN による認証

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) 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 IC カード毎に設定された閾値に達すると、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。

注：PIN 誤り回数の閾値は、IC カード毎に IC カード内で管理される情報であり、TOE 範囲外の機能で変更可能である。

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。(FIA_SOS.1a)
- 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。(FIA_SOS.1b)
- 長さ: 6 文字～16 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

PIN は、以下の条件を満たすもののみを設定可能とする。(FIA_SOS.1c)
- 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。

7.1.4. SF.Crypto

TOE は、以下の鍵を生成する。(FCS_CKM.1、FMT_SMF.1)

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	2048bit, 3072bit, 4096bit 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	2048bit
バックアップデータ署名用鍵ペア （RSA）	・疑似乱数生成アルゴリズム ・PKCS#1	2048bit
システム共通鍵 （AES）	疑似乱数生成アルゴリズム	256bit
データベース共通鍵 （AES）	疑似乱数生成アルゴリズム	256bit
共通鍵保護鍵 （AES）	非公開独自方式	256bit
PKCS#12 ファイル内秘密鍵保護鍵 （3Key Triple DES）	SHA-1 (パスフレーズをハッシュ演算で加工することで鍵としている)	168bit
PKCS#12 ファイル内証明書保護鍵 （3Key Triple DES）	SHA-1 (パスフレーズをハッシュ演算で加工することで鍵としている)	168bit
PKCS#12 ファイル HMAC 鍵	SHA-1 (パスフレーズをハッシュ演算で加工することで鍵としている)	160bit
EE IC カード発行依頼ファイル保護鍵 （3Key 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。(FCS_COP.1)
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	HSM が SafeNet LunaSA の場合 2048bit 3072bit, 4096bit から選択 HSM が CK-Guard の場合 2048bit	・操作員証明書の署名検証 ・CRL の署名検証
	ECDSA	HSM が SafeNet LunaSA の場合 256bit(P-256) 384bit(P-384), 512bit(P-521) から選択	
操作員秘密鍵／公開鍵	RSA	2048bit	認証用のチャレンジの署名および署名検証
バックアップデータ署名用秘密鍵／公開鍵	RSA	2048bit	バックアップデータの署名および署名検証
システム共通鍵	AES	256bit	・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	AES	256bit	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	AES	256bit	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 カード発行依頼ファイル保護鍵	Triple DES	168bit	EE IC カード発行依頼ファイルの暗号化
PKCS#12 ファイル内秘密鍵保護鍵	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
PKCS#12 ファイル内証明書保護鍵	Triple DES	168bit	・機関証明書と秘密鍵の PKCS#12 出力時の証明書暗号化 ・EE 証明書と秘密鍵の PKCS#12 出力時の証明書暗号化
PKCS#12 ファイル HMAC 鍵	HMAC-SHA-1	160bit	・機関証明書と秘密鍵の PKCS#12 出力時の鍵付きハッシング ・EE 証明書と秘密鍵の PKCS#12 出力時の鍵付きハッシング
なし	SHA-224 SHA-256 SHA-384 SHA-512	－	機関証明書、操作員証明書、EE 証明書、失効リスト発行のハッシュ生成
なし	SHA-1 (注 1)	－	・識別認証情報のハッシュ比較 ・アクセスコントロール情報のハッシュ比較 ・システム設定情報のハッシュ比較 ・監査ログのハッシュ比較(FAU_STG.1) ・アーカイブデータのハッシュ比較 ・バックアップデータのハッシュ比較
なし	SHA-256	－	・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(FAU_STG.1) ・アーカイブデータのハッシュ操作 ・バックアップ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

(注 1)SHA-1 は、本バージョンの TOE へ移行する以前のバージョンの TOE で生成された SHA-1 ハッシュ値を対象とした検証においてのみ使用し、本バージョンの TOE 内で新た

に SHA-1 ハッシュ値を生成しない。また、CRYPTOREC 暗号リストにおいて、互換性維持の為に継続利用を容認する旨が記述されている。本 TOE での SHA-1 の利用は互換性維持用途である事から、SHA-1 の利用は許容される。

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、およびバックアップデータ署名用鍵ペアは 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。(FCS_CKM.4)

7.1.5. 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。(FCO_NRO.2)

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(FMT_SMF.1)。 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（DERBASE64 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。(FMT_SMF.1)

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。(FCO_NRO.2)
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。(FMT_SMF.1)

8. 付録

8.1. 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

TOE（Target Of Evaluation）:
　評価対象

TSF（TOE Security Functions）:
　TOE セキュリティ機能

<TOE 関連略語>

AES（Advanced Encryption Standard）
　共通鍵暗号アルゴリズム

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

ECDSA（Elliptic Curve Digital Signature Algorithm）:

楕円曲線上の離散対数問題と呼ばれる数学上の問題を安全性の根拠とするデジタル署名方式

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）:

認証局鍵ペア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。

<TOE 関連用語>

スケジュール：

本 ST 中では、失効リストの更新処理の実行スケジュールを指す。

ポリシー：

本 ST 中では、セキュリティ機能ポリシー、および TOE セキュリティポリシー以外で出現する場合、証明書プロファイル、および失効リストプロファイルの定義を指す。

破壊：

データに対する加工、消去等の行為により、ソフトウェアがデータを参照できない状態、つまりデータの消失・削除状態に陥らせる事を指す。

改ざん：

データを元の内容とは異なる内容に作り変える行為により、ソフトウェアがデータを参照できるが、そのデータを基に意図した動作を行えない状態に陥らせる事を指す。

8.2. 参照

[1] 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，2017 年 4 月 バージョン 3.1 改訂第 5 版 平成 29 年 7 月翻訳 1.0 版，独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室

[2] 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：セキュリティ機能コンポーネント，2017 年 4 月 バージョン 3.1 改訂第 5 版 平成 29 年 7 月翻訳 1.0 版，独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室

[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 3：セキュリティ保証コンポーネント，2017 年 4 月 バージョン 3.1 改訂第 5 版 平成 29 年 7 月翻訳 1.0 版，独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室

[4] 政府機関等のサイバーセキュリティ対策のための統一基準（令和 3 年度版），令和 3

年 7 月 7 日，サイバーセキュリティ戦略本部

[5] 政府認証基盤（GPKI） 行政機関等認証局 CP／CPS ガイドライン，令和 3 年 12 月 9 日改定，デジタル社会推進会議関係課長等連絡会議了承

[6] 政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針，平成 24 年 10 月 26 日改定，情報セキュリティ対策推進会議決定

[7] 電子政府推奨暗号リスト，令和 4 年 3 月 30 日 最終更新，デジタル庁・総務省・経済産業省