PKI Management Program

セキュリティターゲット

第 1.1 **版**

2004 **年** 7 **月** 5 **日**

株式会社日立製作所

更新履歴

バージョン	作成・更新日	更新概要	更新箇所
第 1.0 版	2003.06.11	初版	全般
第 1.1 版	2004.07.05	所見報告書(2004 年 6 月 2 日発行)に対する修正。[ASE-001-01,ASE-002-01,ASE-003-01,ASE-004-01,ASE-005-01,ASE-006-01,ASE-007-01,ASE-008-01,ASE-009-01,ASE-010-01,ASE-011-01,ASE-012-01,ASE-013-01,ASE-014-01,ASE-015-01]	全般

目次

1 ST 概説 5
1.1 ST 識別 5
1.2 ST 概要 5
1.3 CC 適合 7
1.4 参照資料 7
1.5 用語説明 8
2 TOE 記述 11
2.1 TOE の特定 11
2.1.1 TOE の種別 11
2.1.2 TOE の製品構成 11
2.1.3 TOE の動作環境 13
2.1.4 TOE の関連者 21
2.1.5 TOE の構成と機能 23
2.1.6 利用目的と利用方法 36
2.2 保護対象資産 44
2.2.1 保護対象資産 44
2.2.2 保護対象資産に対する操作 50
3 TOE セキュリティ環境 51
3.1 前提条件 51
3.1.1 物理的な条件 51
3.1.2 人的な条件 52
3.1.3 接続条件 52
3.1.4 使用条件 53
3.2 脅威 54
3.3 組織のセキュリティ方針 55
4 セキュリティ対策方針 56
4.1 TOE のセキュリティ対策方針 56
4.2 環境のセキュリティ対策方針 57
4.2.1 IT 環境セキュリティ対策方針 57
4.2.2 運用／管理セキュリティ対策方針 58
5 IT セキュリティ要件 61
5.1 TOE セキュリティ要件 61

5.1.1 TOE セキュリティ機能要件 61
5.1.2 TOE セキュリティ機能強度 101
5.1.3 TOE セキュリティ保証要件 102
5.2 IT 環境に対するセキュリティ要件 103
6 TOE 要約仕様 117
6.1 TOE セキュリティ機能 117
6.1.1 F.AUDIT（監査機能） 121
6.1.2 F.OPERATOR_AUTH（オペレータ識別認証機能） 125
6.1.3 F.CA_AUTH（CA 識別認証機能） 127
6.1.4 F.ACCESS_CONTROL（アクセス制御機能） 128
6.1.5 F.STATUS_FLOW_CONTROL（状態フロー制御機能） 131
6.1.6 F.CIPHER（暗号化機能） 136
6.1.7 F.SSL（暗号通信機能） 141
6.1.8 F.ADMIN（管理機能） 142
6.2 セキュリティ機能強度 143
6.3 保証手段 144
7 PP 主張 145
8 根拠 146
8.1 セキュリティ対策方針根拠 146
8.1.1 前提条件に対するセキュリティ対策方針の検証 146
8.1.2 脅威に対するセキュリティ対策方針の検証 153
8.1.3 組織のセキュリティ方針に対するセキュリティ対策方針の検証 159
8.2 セキュリティ要件根拠 162
8.2.1 セキュリティ機能要件根拠 162
8.2.2 最小機能強度根拠 180
8.2.3 保証要件根拠 180
8.3 TOE 要約仕様根拠 181
8.3.1 TOE セキュリティ要件の根拠 181
8.3.2 セキュリティ機能強度主張の根拠 198
8.3.3 保証手段根拠 198
8.4 PP 主張根拠 198

1 ST 概説

1.1 ST 識別

(1) ST 識別

- 名称 : 「PKI Management Program セキュリティターゲット」
- バージョン : 第 1.1 版
- 作成者名 : 株式会社日立製作所
- 作成日 : 2004 年 7 月 5 日

(2) TOE 識別

本 ST は、以下の製品に対応する。

- 製品名称 : PKI Management Program
- バージョン／リリース番号 : Windows 版：02-04-/A
  Solaris(TM) Operating Environment（以降、Solaris OE と記述）版：02-04
- 作成者名 : 株式会社日立製作所

1.2 ST 概要

PKI Management Program は公開鍵基盤(Public Key Infrastructure：以降、PKI と記述)システムにおける登録局(Registration Authority：以降、RA と記述)の機能を提供するソフトウェア製品である。

PKI において、RA はユーザからの証明書発行または失効の申請を受け付ける。また、RA は、RA の運用に関わる者に対して、RA サーバが受け付けた申請が妥当なものであるかを審査する手段を提供する。RA の運用に関わる者によって妥当なものと判断された申請は CA に転送され、CA によって証明書が発行または失効される。

本 ST は、PKI Management Program を運用する上でのセキュリティ上の脅威を分析し、それらの脅威に対する対策として PKI Management Program が提供するセキュリティ機能について記述することにより、PKI Management Program の安全性及び堅牢性を証明することを目的としている。

PKI Management Program を運用する上でのセキュリティ上のおもな脅威としては、通信データの盗聴、TOE への不正アクセス、許可されない操作、不正操作を取り上げている。PKI Management Program では、これらの脅威への対策として、SSL 通信機能、TOE 利用者識別認証機能、アクセス制御機能、状態フロー

制御機能、監査機能、暗号化機能を提供している。

1.3 CC 適合

- CC パート 2 適合
- CC パート 3 追加：EAL3 に ADV_SPM.1 を追加する。

1.4 参照資料

- 情報技術セキュリティ評価のためのコモンクライテリア
  パート 1：概説と一般モデル バージョン 2.1 1999 年 8 月 CCIMB-99-031
- 情報技術セキュリティ評価のためのコモンクライテリア
  パート 2:セキュリティ機能要件 バージョン 2.1 1999 年 8 月 CCIMB-99-032
- 情報技術セキュリティ評価のためのコモンクライテリア
  パート 3:セキュリティ保証要件 バージョン 2.1 1999 年 8 月 CCIMB-99-033
- 情報技術セキュリティのための共通評価方法論 CEM-97/017
  パート１：概説と一般モデル バージョン 0.6 97/01/11
- 情報技術セキュリティ評価のための共通方法論 CEM-99/045
  パート２：評価方法論 バージョン 1.0 1999 年 8 月

1.5 用語説明

CA	：	Certification Authority：認証局。利用者の公開鍵に対してディジタル署名を行い、証明書を発行する。また、CRL を発行する。
CAID	：	RA サーバに登録される CA を識別するために CA に割り付けられる RA 内で一意な名前。
CMP	：	Certificate Management Protocol。電子証明書の発行や管理に関するプロトコル。X.509 証明書の要求や失効、それらの要求に対する応答などを行う際に、どういった形式でメッセージを送るべきかが定義されている。
CMP サーバ	：	CMP による証明書の発行・失効要求を受け付けるサーバ。CA により提供される。
CMP クライアント	：	CMP により CMP サーバに要求を行うクライアント。ERA サーバにより実装される。
ERA サーバ	：	Enterprise Registration Authority サーバ：RA を実現するサーバである。証明書(Certificate)の発行申請や失効申請を CA(Certification Authority)に渡すと同時に、それぞれの申請の詳細情報を管理する。
KeySafer	：	ERA サーバで生成された鍵の管理を行う機能である。
PKCS	：	Public Key Cryptography Standards：RSA Security が開発した公開鍵暗号の業界標準。 ● PKCS#7 は S/MIME 用にキーや証明書を扱えるようにした規格で、ASN.1 記述の証明書の格納や、署名、MIME 形式における記述法などを定めたものである。 ● PKCS#8 は、鍵の格納を定めたものである。 ● PKCS#12 は、PKCS#7 証明書と PKCS#8 秘密鍵のファイル化を行ったものである。
PIN	：	PKCS#12 ファイルにアクセスするためのパスワードである。
PKI	：	Public Key Infrastructure：公開鍵暗号方式によるセキュリティ基盤。
RA	：	Registration Authority：登録局。証明書の発行・失効申請を審査するなど、一般利用者と CA の間において証明書管理を行う。
RA サーバ	：	RA を構築するサーバである。 ERA サーバと KeySafer を総称するものである。
RMI	：	Remote Method Invocation。Java が提供する機能で、Java VM 上のオブジェクトに対して、他マシン上のオブジェクトの呼び出しを可能にする機構。

SCL	：	SecureCrypto Library の略で、TOE の前提製品である Securecrypto Library ランタイム V1.0L52 により提供される暗号ライブラリ。IC カードへのアクセス機能を提供する。
SSL	：	Secure Sockets Layer：TCP 層とアプリケーション層の間に位置する Netscape 社が開発したプロトコル層。証明書による認証機能と通信データの暗号化機能を持つ。
X.509	：	ITU-T が勧告した証明書、及び CRL リストの標準仕様。ITU-T（International Telecommunication Union-Telecommunication sector とは、ITU（国際電気通信連合）の下部組織であり、ITU の機能のうち、通信関係の標準化を担当。
オペレータ		TOE のうち、RA サーバのクライアントとして動作するコンポーネントを操作する者で、RA サーバに TOE の正当な操作者として登録された者。オペレータには RA 管理者、監査者、RA 操作者の種別がある。（「2.1.4 TOE の関連者」参照）
オペレータ ID		RA サーバに登録されるオペレータを識別するためにオペレータに割り付けられる RA 内で一意な名前。
オペレータ種別		オペレータの種別を規定するセキュリティ属性。通常のオペレータの種別としては以下のものがある。 ● CONSOLE (RA 管理者) ● AUDITOR (監査者) ● RAO1 (RA 操作者) ● RAO2 (RA 操作者) ● KRO1 (RA 操作者) ● KRO2 (RA 操作者) また、上記の他に、RA サーバプロセス自身を識別するための種別がある。 ● RA (RA サーバ)
鍵番号	：	RA サーバが管理する監査暗号鍵を識別するために、監査ログ暗号鍵に対して RA サーバが割り付ける RA 内で一意な番号。
鍵ペア	：	公開鍵暗号における、対となる公開鍵と秘密鍵の組のことである。
管理者 PIN	：	IC カードの管理者パスワード。
公開鍵	：	公開鍵暗号方式で使用される鍵ペアのうち、一般に公開される鍵。
公開鍵暗号	：	暗号化と復号に、対となる別の鍵(公開鍵、秘密鍵)を使用する暗号技術のことである。
合議制	：	証明書発行、証明書失効を行ううえで複数人の承認を得る仕組みである。
サイト	：	証明書を発行する CA、発行・失効審査を行うオペレータをひとまとまりにしたグループ。

サイト ID		RA サーバに登録されるサイトを識別するためにサイトに割り付けられる RA 内で一意な名前。
証明書	：	X.509 に従って発行された公開鍵証明書のことを表す。公開鍵証明書とは、公開鍵の所有者であることを保証したもので、CA がディジタル署名をしたもの。
証明書失効	：	鍵紛失や危殆化などの理由で、有効期限満了前に証明書を無効にすることである。
証明書発行	：	証明書発行要求(CSR)を受け、認証局が署名を施すことである。
署名	：	送信されたメッセージを受け取った際、そのメッセージが確かにそのメッセージの送信者からのものかを確認する手段。公開鍵暗号技法の応用例のひとつ。ディジタル署名は、秘密鍵を保持している本人しか作ることができないため、これが付加されているメッセージは、確かに本人が作成したことを証明する。
利用者 PIN	：	IC カードの利用者パスワード。
秘密鍵	：	公開鍵暗号方式で使用される鍵ペアのうち、一般に公開されない鍵。
要求番号	：	RA サーバが受け付けた証明書発行要求に対して RA サーバが割り付ける RA 内で一意な番号。

2 TOE 記述

本章では、TOE の種別、範囲及び境界を含む TOE 情報を記述する。

2.1 TOE の特定

2.1.1 TOE の種別

TOE は、RA を実現するソフトウェア製品である。

2.1.2 TOE の製品構成

PKI システムは、CA の機能を提供する製品と、RA の機能を提供する製品から構成される。

CA は証明書の発行・失効と、それに付随する CA サービスを提供する。RA は証明書の発行・失効の申請窓口と、それに付随する RA サービスを提供する。

本 ST は RA を実現するソフトウェア製品である PKI Management Program に含まれる機能を TOE としている。

なお、CA は本 ST における TOE の対象外であるが、図 2-1 の例では、CA 製品として日立製作所の Enterprise Certificate Server が使用されることを前提としている。

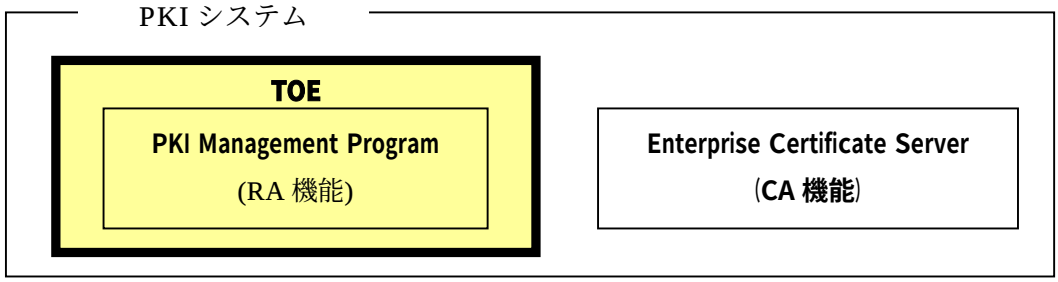

図 2-1：PKI システムの構成例

PKI Management Program は以下の４つのコンポーネントから構成される。

- RA サーバ
  RA オペレータからの証明書発行・失効申請を受け付けて CA に渡すと同時に、それぞれの申請の詳細情報を管理する。
- RA セットアップ
  RA サーバの動作環境設定を行う。
- RA コンソール
  RA サーバのクライアントとして動作し、RA サーバの運用管理等を行う。
- RA オペレータ
  RA サーバのクライアントとして動作し、RA サーバに対して証明書の発行・失効申請等を行う。

RA サーバには Windows 版と Solaris OE 版が存在するが、これらは IT 環境に依存する部分を除いて実装レベルで同一であり、RA サーバのこれら２つの実装は TOE に包含される。

2.1.3 TOE の動作環境

PKI Management Program は RA サーバ・RA セットアップ・RA コンソール・RA オペレータの４つのコンポーネントにより構成される。これらのコンポーネントは、それぞれ RA サーバマシン・RA 設定端末・RA 管理／監査端末・RA 操作端末上で動作する。「図 ２－２ PKI Management Program 動作環境」に TOE の動作環境を示す。

本 ST における TOE は、「図 ２－２ PKI Management Program 動作環境」の太枠内の RA サーバ、RA セットアップ、RA コンソール、及び RA オペレータである。

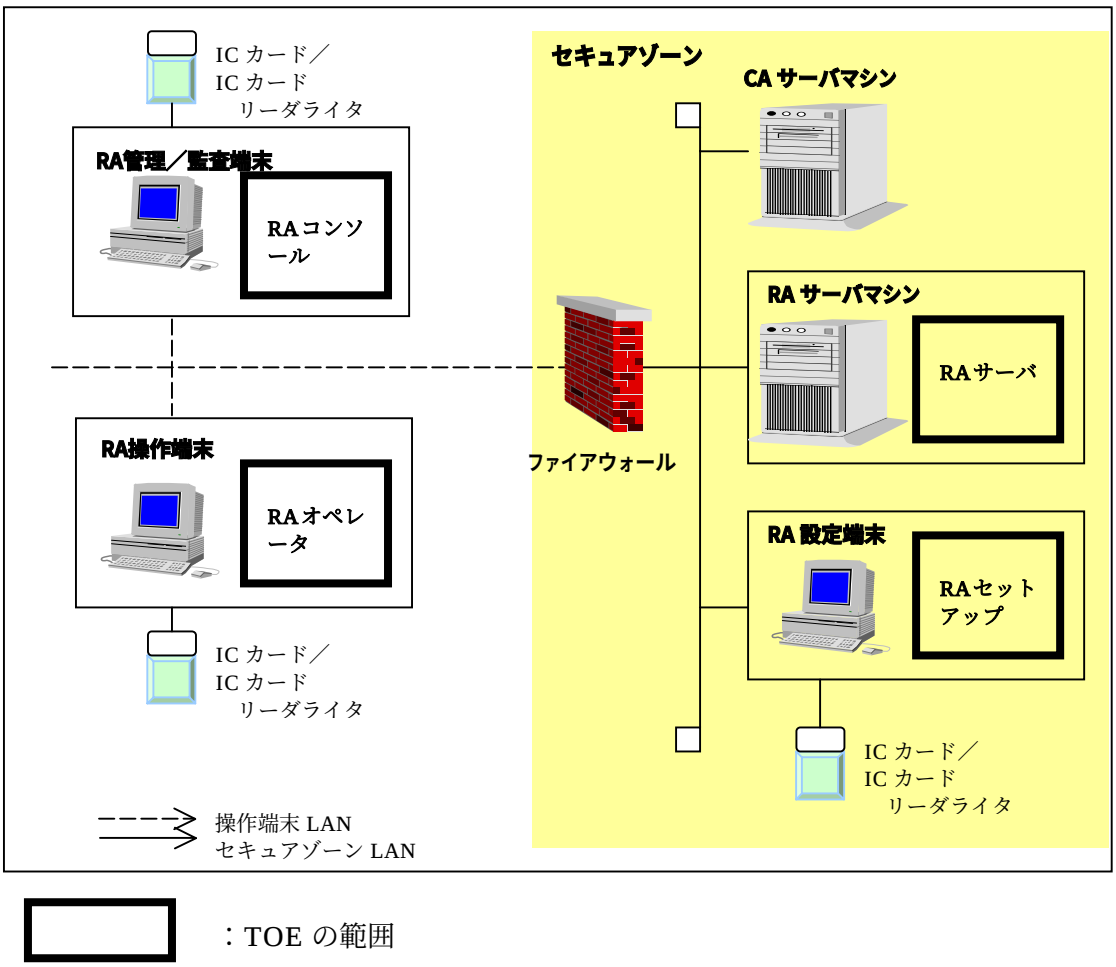

図 2-2 PKI Management Program 動作環境

(1)　物理的な環境

TOE の動作環境はセキュアゾーンとそれ以外のゾーンとから構成される。セキュアゾーンは入退室管理により物理的に保護された専用区域である。セキュアゾーンには RA サーバマシン、CA サーバマシン、RA 設定端末等が設置される。セキュアゾーン以外のゾーンは TOE を運用する組織内の任意の場所で、TOE を運用する組織に属する者だけが物理的にアクセスできる。セキュアゾーン以外のゾーンには RA 管理／監査端末、RA 操作端末等が設置される。

セキュアゾーンへの入室権限は、システム管理者等セキュアゾーンに設置される各サーバマシンの管理者が持つ。例外として各サーバマシン管理者に特に許可されたものがセキュアゾーンに入室することがあるが、その場合には必ず入室を許可した管理者と共に入室し、各サーバマシン管理者の監視下で作業を実施する。

(2)　ネットワーク環境

TOE の動作環境内のネットワークはセキュアゾーン LAN と操作端末 LAN から構成される。

セキュアゾーン LAN はファイアウォールによって保護されたセキュアゾーン内の LAN である。セキュアゾーン LAN はファイアウォールを介して RA 管理／監査端末及び RA 操作端末が接続されている操作端末 LAN に接続される。ファイアウォールは特定のポートに対する特定の端末からのパケットだけが通過できるように設定され、セキュアゾーン LAN を保護する。セキュアゾーン LAN には RA サーバマシン、CA サーバマシン、RA 設定端末等が接続される。

操作端末 LAN は TOE を運用する組織内の LAN で、操作端末 LAN には TOE を運用する組織に属する者だけがアクセスできる。操作端末 LAN には RA 管理／監査端末、RA 操作端末、及び TOE を運用する組織に属する任意のマシンが接続される。

(3) ハードウェア

TOE の動作環境には以下のハードウェアが存在する。

- RA サーバマシン
- CA サーバマシン
- RA 設定端末
- RA 管理／監査端末
- RA 操作端末
- IC カードリーダライタ／IC カード

RA サーバマシンは RA サーバが動作するマシンであり、RA サーバ、及び RA サーバ動作するのに必要なソフトウェアがインストールされる。

CA サーバマシンは CA が動作するマシンであり、CA、及び CA が動作するのに必要なソフトウェアがインストールされる。

RA 設定端末はシステム管理者が操作する端末であり、RA セットアップ、及び RA セットアップが動作するのに必要なソフトウェアがインストールされる。

RA 管理／監査端末は RA 管理者または、監査者が操作する端末であり、RA コンソール、及び RA コンソールが動作するのに必要なソフトウェアがインストールされる。

RA 操作端末は RA 操作者が操作する端末であり、RA オペレータ、及び RA オペレータが動作するのに必要なソフトウェアがインストールされる。

RA 設定端末、RA 管理／監査端末、及び RA 操作端末には IC カードリーダライタが接続される。IC カードにはオペレータの証明書・秘密鍵が格納される。IC カードリーダライタ及び IC カードは、オペレータの IC カード作成、及びオペレータが RA サーバにログインする際のユーザ認証等に使用される。

(4) 動作条件

TOE は、以下のハードウェア、及びソフトウェア上で動作する。

a) RA サーバ（Windows 版）

表 2-1 RA サーバハードウェア構成（Windows 版）

種類		説明
CPU		Intel PentiumIII 500MHz 相当以上
メモリ		256MB 以上
補助記憶装置	ディスク	250MB 以上

表 2-2 RA サーバソフトウェア構成（Windows 版）

種類	名称	修正レベル
OS	Microsoft® Windows® 2000 Server	サービスパック 3 以上を適用
データベース	Oracle Database 8i (8.1.7) または Oracle9i Database Release2(9.2.0)	Oracle Database 8i (8.1.7)の場合は 8.1.7.2 パッチを適用
その他	Securecrypto Library ランタイム V1.0L52	
	S/MIME & EE Certificate Management Package V3.1L16	

b) RA サーバ（Solaris OE 版）

表 2-3 RA サーバハードウェア構成（Solaris OE 版）

種類		説明
CPU		UltraSPARC-II 400MHz 相当以上
メモリ		512MB 以上
補助記憶装置	ディスク	250MB 以上

表 2-4 RA サーバソフトウェア構成（Solaris OE 版）

種類	名称	修正レベル
OS	Sun Microsystems,Inc Solaris(TM) 8 Operating Environment	106327-08 以上 106300-09 以上 107058-01 以上 106748-04 以上 108528-10 以上
データベース	Oracle Database 8i (8.1.7) または Oracle9i Database Release2(9.2.0)	Oracle Database 8i (8.1.7)の場合は 8.1.7.2 パッチを適用
その他	Securecrypto Library RunTime 1.4	
	S/MIME & EE Certificate Management Package 3.1.6	

c) RA セットアップ

表 2-5　RA セットアップハードウェア構成

種類		説明
CPU		Pentium プロセッサー200MHz　以上
メモリ		128MB 以上
補助記憶装置	ディスク	34MB 以上
	カード リーダライタ	HX-360MJ（RS-232C 手動挿入手動排出タイプ・カードリーダライタ） HX-500UJ（USB 手動挿入手動排出タイプ・カードリーダライタ）

表 2-6　RA セットアップソフトウェア構成

種類	名称	修正レベル
OS	Microsoft® Windows® 2000 Server	サービスパック 3 以上を適用
データベース	Oracle Database 8i (8.1.7) または Oracle9i Database Release2(9.2.0)	Oracle Database 8i (8.1.7)の場合は 8.1.7.2 パッチを適用
その他	Securecrypto Library ランタイム V1.0L52	
	S/MIME & EE Certificate Management Package　V3.1L16	

d) RA **コンソール**

表 2-7　RA コンソールハードウェア構成

種類		説明
CPU		Pentium プロセッサー200MHz　以上
メモリ		128MB 以上
補助記憶装置	ディスク	55MB 以上
	カード リーダライタ	HX-360MJ（RS-232C 手動挿入手動排出タイプ・カードリーダライタ） HX-500UJ（USB 手動挿入手動排出タイプ・カードリーダライタ）

表 2-8　RA コンソールソフトウェア構成

種類	名称	版数
OS	Microsoft® Windows® 2000 Professional	サービスパック 3 以上を適用
その他	Securecrypto Library ランタイム V1.0L52	
	S/MIME & EE Certificate Management Package　V3.1L16	

e) RA **オペレータ**

表 2-9　RA オペレータハードウェア構成

種類		**説明**
CPU		Pentium プロセッサー200MHz　以上
メモリ		256MB 以上
補助記憶装置	ディスク	56MB 以上
	カード リーダライタ	HX-360MJ（RS-232C 手動挿入手動排出タイプ・カードリーダライタ） HX-500UJ（USB 手動挿入手動排出タイプ・カードリーダライタ）

表 2-10　RA オペレータソフトウェア構成

種類	**説明**	**版数**
OS	Windows 2000 Professional	サービスパック 3 以上を適用
その他	Securecrypto Library ランタイム V1.0L52	
	S/MIME & EE Certificate Management Package V3.1L16	

2.1.4 TOE の関連者

本 ST では、以下の関連者を想定する。

- システム管理者

  TOE を運用する組織に属し、TOE を運用する組織の責任者により任命される。システム管理者は RA サーバ及び RA セットアップのインストールを行い、RA サーバの初期設定、起動、停止を行う。RA サーバマシン及び RA 設定端末のオペレーティングシステム、及びデータベースの管理者でもある。

- RA 管理者

  TOE を運用する組織に属し、TOE を運用する組織の責任者により任命される。RA 管理／監査端末への RA コンソールのインストール、RA コンソールの設定・管理、及び RA サーバの運用環境設定を行う。

- 監査者

  TOE を運用する組織に属し、TOE を運用する組織の責任者により任命される。RA 管理／監査端末への RA コンソールのインストール、RA コンソールの設定・管理、及び RA の監査を行う。

- RA 操作者

  TOE を運用する組織に属し、TOE を運用する組織の責任者により任命される。RA 操作端末への RA オペレータのインストール、RA オペレータの設定・管理、一般利用者の証明書の発行・失効の申請・審査、及び一般利用者の鍵・証明書の取得等の操作を行う。

  RA 操作者には RAO1、RAO2、KRO1、KRO2 の種別がある。RAO1・RAO2 は、証明書の発行・失効、及び発行された鍵・証明書の取得等に関わる操作を行う。KRO1・KRO2 は鍵紛失時等の鍵の回復に関わる操作を行う。

  RAO1 と RAO2、または KRO1 と KRO2 は、一般利用者の鍵・証明書の発行、失効、取得、削除に関わる一連の操作の権限を分担し、単独の RA 操作者だけでは重要な処理が行われないよう、RA サーバによって制御される。

- CA オペレータ

  TOE を運用する組織に属し、CA の運用を管理する。

- 一般利用者

  RA 操作者からの申請により TOE 及び CA により発行される鍵・証明書の利用者。鍵・証明書は、RA 操作者から配付される。

- TOE を運用する組織の責任者

  システム管理者、RA 管理者、RA 操作者、監査者が属する組織の責任者。TOE のセキュアな運用に対する責任を持つ。

- TOE を運用する組織に属する者

  RA 管理／監査端末、RA 操作端末にアクセスすることはできるが、TOE の操作に関する権限は持たない。また、TOE を含むソフトウェアの技術機構については熟知しておらず、攻撃力は高くない。

- システム管理者に許可された者

  システム管理者の監視下のもとでセキュアゾーンに入室し、作業を行う。

- 他サーバマシン管理者

  セキュアゾーンに設定される RA サーバマシン以外のサーバマシン管理者。

2.1.5 TOE の構成と機能

TOE の範囲を「図 2－3 TOE の範囲」に示す。本 ST における TOE の範囲は網がけ部分であり、①～⑨の機能で構成される。

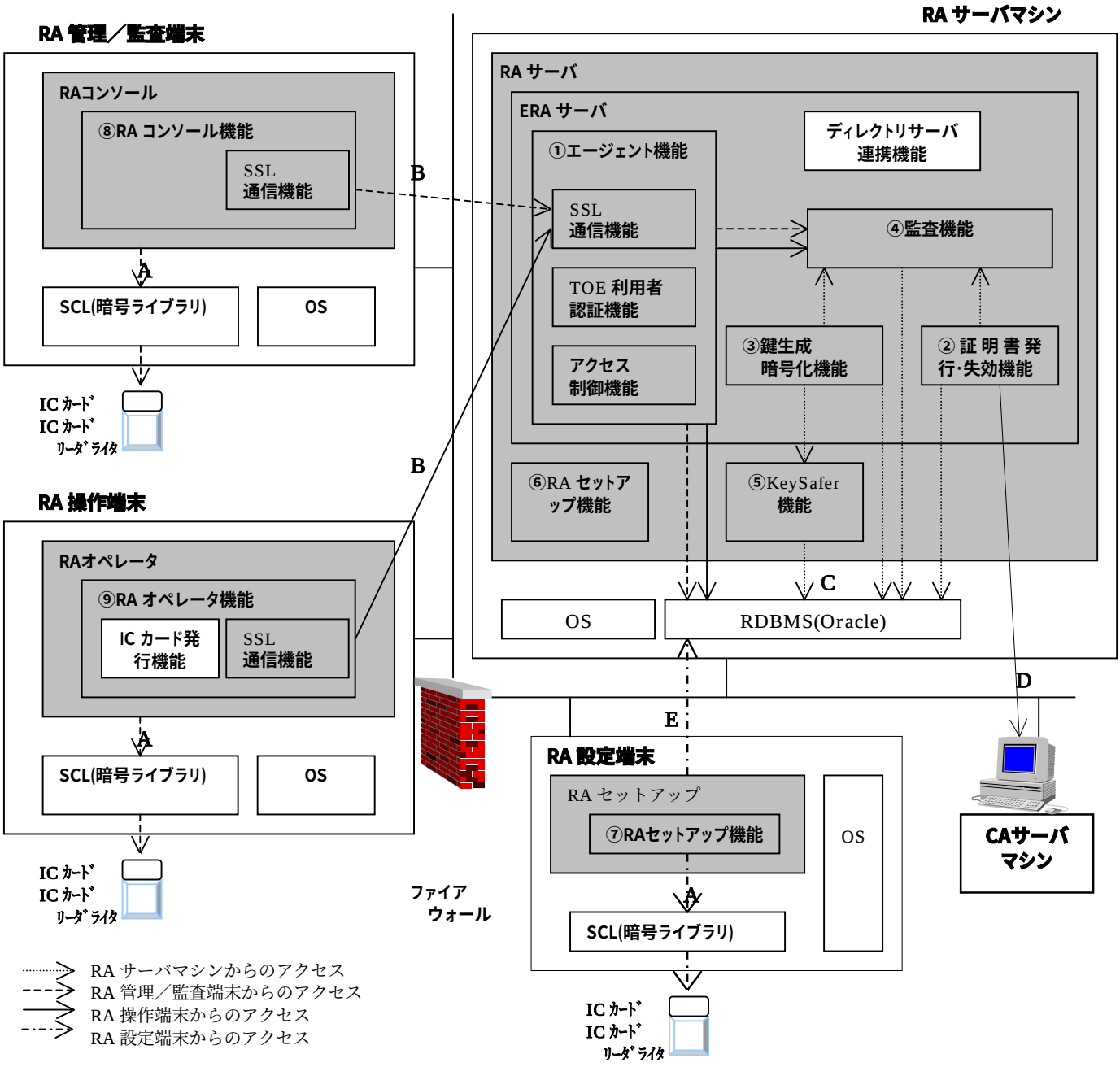

図 2-3 TOE の範囲

(1) TOE が提供する機能

TOE が提供する機能を以下に記述する。

①～⑨の説明は図 2-3 の①～⑨で示した機能に対応する。

a) RA **サーバ**

① エージェント機能

RA コンソール、及び RA オペレータ(以降、クライアントと記述)からの要求を受け付け、処理を代行する機能である。

クライアントは ERA サーバに対して処理の要求を行うのに先立ち、ERA サーバに対するログインを行う。ERA サーバがログイン要求を受け付けると、TOE 利用者識別認証機能によりクライアント利用者の識別認証が行われる。識別認証にはユーザ ID／パスワードによる認証と、証明書による認証がある。ユーザ ID／パスワードによる識別認証は、RA オペレータのオペレータ登録機能でのみ使用される識別認証方式であり、それ以外の場合は証明書による識別認証が行われる。識別認証機能によりログインを要求しているクライアント利用者が RA サーバに登録されたオペレータであることが確認されると、クライアントの ERA サーバへのログインが許可される。ログイン後、クライアントは ERA サーバに対して処理を要求することが可能となる。

クライアントからの処理要求を受け付けると、エージェント機能は要求された処理を実行する。このとき、アクセス制御機能により、クライアントが許可されない操作を行うことを抑止する。

ERA サーバ-クライアント間の通信データは SSL 通信機能により SSL で保護される。

エージェント機能はクライアントに対して以下のサービスを提供する。

- CA 管理機能

  RA サーバが証明書の発行・失効申請を行う CA サーバに関する管理情報の登録、変更、削除を行う。
- サイト管理機能

  サイトの登録、変更、削除を行う。
- オペレータ管理機能

  RA 操作者の登録、変更、削除を行う。
- トラスト CA 管理機能

信頼する CA 証明書の登録、削除を行う。

- 監査機能

  監査ログの検索、表示、検証、削除を行う。

- 鍵・証明書操作機能

  証明書の発行・失効申請の受け付け、及び発行された鍵・証明書の取得などの操作を行う。提供される機能は以下のものがある。

  - 証明書発行申請
  - 証明書発行審査
  - 証明書失効申請
  - 証明書失効審査
  - 証明書取得
  - 証明書情報検索
  - 証明書情報取得
  - 証明書情報削除
  - PKCS#12 取得要求
  - PKCS#12 取得審査
  - PIN 取得審査
  - PKCS#12 取得
  - PIN 取得

  証明書の発行申請が受け付けられると、RA サーバのデータベースに証明書情報が追加される。証明書情報には証明書申請情報、証明書状態、証明書等が含まれ、ERA サーバによる証明書ライフサイクルの管理に使用される。

② 証明書発行／失効機能

証明書情報を検索し、証明書の発行・失効を行う必要がある証明書情報があれば、CA サーバに対して証明書の発行・失効を依頼する。発行された証明書はデータベースに保存される。

証明書発行処理の対象となる証明書発行申請が RA オペレータのオペレータ登録機能による証明書申請だった場合は、発行された証明書を RA 操作者の証明書としてデータベースに格納する。この証明書は RA 操作者のオペレータ登録情報と関連づけられ、RA 操作者の識別認証で使用される。

証明書発行／失効機能は CMP クライアントとして動作する。

③ 鍵生成／暗号化機能

証明書情報を検索し、鍵の生成を行う必要がある証明書情報があれば鍵ペアの生成を行う。生成された鍵ペアは暗号化され、KeySafer 機能を使用してデータベースに格納される。また、証明書発行済みの証明書情報があれば、鍵・証明書から PKCS#12 を生成する。生成された PKCS#12 はその PKCS#12 の PIN とともに暗号化され、KeySafer 機能を使用してデータベースに格納される。

④ 監査機能

ERA サーバで実行された操作を監査ログに記録し、管理する。監査ログには電子署名が付され、監査ログの改ざん、削除を検出することができる。

監査機能により採取された情報は、エージェント機能によってクライアントから操作することができる。

⑤ KeySafer 機能

鍵生成／暗号化機能で生成された鍵ペア、暗号化された PKCS#12、PIN をデータベースで管理する。

ERA サーバの起動時に実行可能状態になり、ERA サーバの停止で終了する。

⑥ RA セットアップ機能

RA サーバのセットアップを行う機能であり、システム管理者によって使用される。

RA セットアップ機能には以下の機能がある。

- RA 動作環境情報インポート機能

  RA 設定端末上の RA セットアップ機能によりエクスポートされた RA 動作環境情報を、RA サーバマシンにインポートする。

b) RA **セットアップ**

⑦ RA **セットアップ機能**

RA サーバのセットアップを行う機能であり、システム管理者によって使用される。

RA セットアップ機能には以下の機能がある。

- RA 動作環境情報設定機能

  RA サーバ鍵・証明書登録、ネットワーク環境設定、RA が使用するデータベースの環境設定、KeySafer 環境設定、監査ログ暗号化シードの設定を行う。設定された情報は RA 設定端末マシン上のファイルに保存される。

- 監査ログ暗号化鍵設定機能

  監査ログを暗号化するための鍵の登録、変更を行う。監査ログ暗号化鍵は RA サーバのデータベースに格納される。

- RA 動作環境情報エクスポート機能

  RA 動作環境情報をリムーバブル媒体にエクスポートする。エクスポートされたデータは RA サーバの RA セットアップ機能により RA サーバマシンにインポートされる。

- RA 管理者・監査者登録機能

  RA 管理者・監査者の登録、変更、削除を行う。RA 管理者・監査者の登録情報は、RA サーバのデータベースに格納される。RA 管理者・監査者の登録処理では、RA 管理者・監査者の IC カードが作成される。システム管理者は作成された IC カードを該当する担当者に配付する。

- RA 起動パスワード設定機能

  RA サーバ起動時に入力する起動パスワードを設定する。

c) RA **コンソール**

⑧ RA **コンソール機能**

RA コンソール機能は RA サーバのクライアントとして動作し、RA サーバのエージェント機能を使用して、RA の運用管理機能、及び監査機能を提供する。

RA コンソール機能には以下の機能がある。

- 環境設定機能

  RA コンソールの動作環境設定を行う。設定された情報は RA コンソール動作環境定義情報ファイルに格納される。

- オペレータ環境設定機能

  端末管理者情報を操作する機能を提供する。オペレータ環境設定機能には以下の機能がある。

  - 証明書表示

    IC カード内のオペレータの証明書を表示する。このとき、RA コンソールは、現在の利用者に対して IC カードの利用者 PIN 入力を求め、IC カードの機能を使用して、利用者 PIN による RA 管理者・監査者の本人確認を行う。

  - IC カードパスワード変更

    IC カードの利用者 PIN を変更する。このとき、RA コンソールは、現在の利用者に対して IC カードの利用者 PIN 入力を求め、IC カードの機能を使用して、利用者 PIN による RA 管理者・監査者の本人確認を行う。

- ログイン機能

  RA サーバに対するログインを行う。ログインを行うには、システム管理者から配付される IC カードが必要である。このとき、RA コンソールは、現在の利用者に対して IC カードの利用者 PIN 入力を求め、IC カードの機能を使用して、利用者 PIN による RA 管理者・監査者の本人確認を行う。ログインを行おうとする者が IC カードの正当な所有者であることが確認されると、RA コンソールは RA サーバに対してログイン要求を行う。RA サーバによってログインが受け付けられると、CA 管理機能、サイト管理機能、オペレータ管理機能、トラスト CA 管理機能、及び監査機能が使

用可能となる。

- CA 管理機能

  RA サーバが証明書の発行・失効申請を行う CA サーバに関する管理情報の登録、変更、削除を行う。

- サイト管理機能

  鍵・証明書発行ポリシー、鍵・証明書の状態フロー制御情報、サイトに関連づけられる CA の情報等、サイト管理情報の登録、変更、削除を行う。

- オペレータ管理機能

  RA 操作者の登録、変更、削除を行う。RA 操作者の登録を行うと、オペレータ登録情報ファイルが作成される。RA 管理者はオペレータ登録情報ファイルをオフラインで RA オペレータに配付する。

- トラスト CA 管理機能

  信頼する CA 証明書の登録、削除を行う。

- 監査機能

  監査ログの参照、検証、削除を行う。

- SSL 通信機能

  RA サーバと RA コンソール間の通信データを SSL で保護する。

d) RA **オペレータ**

⑨ RA **オペレータ機能**

RA オペレータ機能は RA サーバのクライアントとして動作し、RA サーバのエージェント機能を使用して、証明書操作機能、及び監査機能を提供する。

RA オペレータ機能には以下の機能がある。

- 環境設定機能

  RA オペレータの動作環境設定を行う。設定された情報は動作環境定義情報ファイルに格納される。

- オペレータ環境設定機能

  端末管理者情報を操作する機能を提供する。オペレータ環境設定機能には以下の機能がある。

  - オペレータ登録

    RA 操作者の鍵・証明書を IC カードに登録する。

    オペレータ登録を実行すると IC カードを初期化し、鍵ペアの生成を行う。このとき、RA オペレータは、現在の利用者に対して IC カードの管理者 PIN 入力を求め、IC カードの機能を使用して、管理者 PIN による RA 操作者の本人確認を行う。

    生成された鍵ペアと、RA コンソールのオペレータ管理機能で作成されたオペレータ登録情報を使用して、RA サーバに対して RA 操作者証明書の発行申請をおこなう。

    発行された RA 操作者の証明書を取得し、IC カードに格納する。

  - オペレータ削除

    IC カード内の RA 操作者の鍵・証明書を削除する。このとき、RA オペレータは、現在の利用者に対して IC カードの利用者 PIN 入力を求め、IC カードの機能を使用して、利用者 PIN による RA 操作者の本人確認を行う。

- 証明書表示

  IC カード内のオペレータの証明書、及び端末環境定義情報内の RA サーバ証明書・CA 証明書を表示する。このとき、RA オペレータは、現在の利用者に対して IC カードの利用者 PIN 入力を求め、IC カードの機能を使用して、利用者 PIN による RA 操作者の本人確認を行う。

- IC カードパスワード変更

  IC カードの利用者 PIN を変更する。このとき、RA オペレータは、現在の利用者に対して IC カードの利用者 PIN 入力を求め、IC カードの機能を使用して、利用者 PIN による RA 操作者の本人確認を行う。

- ログイン機能

  RA サーバに対するログインを行う。ログインを行うには、オペレータ登録機能で作成された IC カードが必要である。RA オペレータは、現在の利用者に対して IC カードの利用者 PIN 入力を求め、IC カードの機能を使用して、利用者 PIN による RA 操作者の本人確認を行う。ログインを行おうとする者が IC カードの正当な所有者であることが確認されると、RA オペレータは RA サーバに対してログイン要求を行う。RA サーバによってログインが受け付けられると、鍵・証明書操作機能、及び監査機能が使用可能となる。

- 鍵・証明書操作機能

  証明書の発行・失効申請、及び発行された鍵・証明書の取得などの操作を行う。提供される機能は以下のものがある。

  - 証明書発行申請
  - 証明書発行審査
  - 証明書失効申請
  - 証明書失効審査
  - 証明書取得
  - 証明書情報検索
  - 証明書情報取得
  - 証明書情報削除
  - PKCS#12 取得要求
  - PKCS#12 取得審査
  - PIN 取得審査
  - PKCS#12 取得
  - PIN 取得

  証明書の発行申請・発行審査・失効申請・失効審査には、単一の証明書を処理する個別発行・失効と、複数の証明書を同時に処理する一括発行・失効機能がある。

- 監査機能

  監査ログの参照を行う。RA オペレータで参照できる監査ログは、ログインしたオペレータが属するサイトのログのみに制限される。

- SSL 通信機能

  RA サーバと RA オペレータ間の通信データを SSL で保護する。

(2) TOE が提供しない機能

TOE が提供しない機能を以下に記述する。

a) **ディレクトリサーバ連携機能**

発行された証明書をディレクトリサーバに格納する機能である。

この機能は RA サーバの ERA サーバ機能に含まれるが、本 ST では ERA サーバからディレクトリサーバへ証明書を格納し、証明書の公開を行う運用は想定しないため、TOE の範囲外とする。

b) IC **カード発行機能**

鍵・証明書操作機能の PKCS#12 取得及び PIN 取得で取得された PKCS#12/PIN から、一般利用者の IC カードを発行する機能である。

この機能は RA オペレータの RA オペレータ機能に含まれるが、本 ST では一般利用者への鍵・証明書の配付を IC カードで行う運用は想定しないため、TOE の範囲外とする。

c) OS

TOE 及びその環境内のソフトウェアが動作するための基盤となる機能。

d) RDBMS

Oracle が提供する機能であり、TOE のデータを管理する。

e) SCL(**暗号ライブラリ**)

Securecrypto Library ランタイムが提供する機能である。TOE は SCL を介して IC カードにアクセスする。

(3) 外部インタフェース

TOE は、図 2-3 に A～E で示した以下の外部インタフェースを持つ。

A TOE－SCL 間インタフェース

TOE は SCL を介して IC カードにアクセスする。TOE－SCL 間では、PIN、証明書、署名・被署名データなどがやりとりされる。SCL の呼び出しはプロセス内の関数呼び出しであり、プロセス間通信等は発生しない。

B RA サーバ－RA コンソール・RA オペレータ間インタフェース

RA サーバとそのクライアントである RA コンソール、及び RA オペレータ間のインタフェースである。SSL 上で動作する Java の RMI(Remote Method Invocation)インタフェースにより、操作端末 LAN、及びセキュアゾーン LAN を介して接続される。RA サーバ－RA コンソール・RA オペレータ間では一般利用者鍵・証明書、RA 管理情報、監査ログが送受信される。RA コンソール・RA オペレータから RA サーバへの接続時には、SSL による証明書認証、及び RA サーバによるユーザ ID／パスワード、または証明書認証が行われる。

C RA サーバ－RDBMS 間インタフェース

RA サーバと RDBMS 間のインタフェースであり、RDBMS が提供するプロトコルにより、RA サーバ内部のプロセス間通信で接続される。RA サーバと RDBMS 間では一般利用者鍵・証明書、RA 管理情報、監査ログが送受信される。RA サーバから RDBMS への接続時には、ユーザ ID／パスワードによる認証が行われる。

D RA サーバ－CA 間インタフェース

RA サーバと CA とのインタフェースであり、CMP(Certificate Management Protocol)により、セキュアゾーン LAN を介して接続される。RA サーバ－CA 間では証明書発行・失効要求、及びそれに対する応答が送受信される。RA サーバから CA への接続時には、証明書による相互認証が行われる。

E　RA セットアップ－RDBMS 間インタフェース

RA セットアップと RDBMS 間のインタフェースであり、RDBMS が提供するプロトコルにより、セキュアゾーン LAN を介して接続される。RA セットアップと RDBMS 間では一般利用者鍵・証明書、RA 管理情報、監査ログが送受信される。RA セットアップから RDBMS への接続時には、ユーザ ID／パスワードによる認証が行われる。

2.1.6　利用目的と利用方法

(1)　利用目的

TOE は以下の目的で使用されることを意図している。

- 一般利用者の秘密鍵を生成し、それに対応する証明書を発行する。
- 一般利用者の証明書を失効する。
- 発行された鍵・証明書を取得する。

(2)　利用方法

A)　OS と TOE のインストール

TOE 動作環境内の各マシンに、OS、TOE、及び TOE が動作するうえで必要とするソフトウェアをインストールする。インストールは各マシンで直接操作し、ネットワーク経由では行わない。

各マシンは OS の識別･認証機能により決められた作業者のみログイン出来るように OS の設定を行う。

インストールする TOE のコンポーネント、インストールするマシン、インストール作業者は以下のとおりである。

表 2-11　TOE の利用環境

TOE のコンポーネント	インストールするマシン	作業者
RA サーバ	RA サーバマシン	システム管理者
RA セットアップ	RA 設定端末	システム管理者
RA コンソール	RA 管理／監査端末	RA 管理者または監査者
RA オペレータ	RA 操作端末	RA 操作者

B) 運用の準備

システム管理者は RA サーバの運用に必要な以下の鍵・証明書の発行を CA オペレータに依頼する。CA オペレータは発行された鍵・証明書をリムーバブル媒体に格納し、オフラインでシステム管理者に配付する。

- RA サーバ鍵・証明書
- RA 管理者鍵・証明書
- 監査者鍵・証明書

C) RA サーバの運用開始

システム管理者は OS の識別・認証機能により RA サーバマシン、RA 設定端末へのログインを行う。

システム管理者は RA サーバマシンで RA サーバが使用するデータベースを作成する。

システム管理者は RA 設定端末で RA セットアップを起動し、RA サーバの動作環境設定、監査ログ暗号化鍵の登録、RA 管理者・監査者の登録等の初期設定を行う。RA 管理者・監査者の登録では RA 管理者・監査者の IC カードが作成される。システム管理者は、IC カードと IC カードの管理者 PIN・利用者 PIN を、該当する担当者に配付する。

システム管理者は RA 設定端末上の RA セットアップ機能により RA 動作環境情報をエクスポートし、RA サーバマシン上の RA セットアップ機能によりインポートする。その後 RA サーバマシンで RA サーバの起動を行う。

D) RA 運用環境の設定

RA 管理者は CA オペレータに CMP クライアントの鍵・証明書の発行を依頼する。CA オペレータは発行された CMP クライアントの鍵・証明書と CMP サーバ証明書をリムーバブル媒体に格納し、オフラインで RA 管理者に配付する。

RA 管理者は RA 管理／監査端末で RA コンソールを起動し、システム管理者から配付された IC カードを使用して RA サーバにログインする。ログイン後、RA サーバの運用を行うための CA、サイト、オペレータを登録する。CMP サーバ証明書、及び CMP クライアントの鍵・証明書は、CA 管理情報として TSC 内にインポートされる。

オペレータの登録ではオペレータ登録情報ファイルが作成される。オペレータ登録情報ファイルはパスワードで保護されている。RA 管理者は、リムーバブル媒体に格納したオペレータ登録情報ファイルとオペレータ登録情報ファイルのパスワードを該当する担当者に配付する。

E) RA 操作者証明書の発行

RA 操作者は RA 運用端末で RA オペレータを起動し、RA 管理者より配付されるオペレータ登録情報を使用して、オペレータ環境設定機能によりオペレータの登録を行う。このとき、RA 操作者の IC カードが作成される。

F) 一般利用者証明書の発行

TOE を運用する組織の責任者からの依頼により、証明書発行操作が開始される。RA 操作者は RA 操作端末で RA オペレータを起動し、「RA 操作者証明書の発行」で作成された IC カードを使用して、RA サーバへのログインを行う。その後、RA オペレータの鍵・証明書操作機能を使用して、下記の各操作を実施する。操作が完了したら RA サーバからログアウトする。

a) 証明書申請

RAO2 は TOE を運用する組織の責任者から依頼を受けた一般利用者のための証明書の発行申請を行う。RA 発行申請が受け付けられると、証明書状態は RA 操作者による発行審査待ちとなる。

b) 証明書発行審査

RAO1、または RAO2 は、証明書の発行申請の内容を審査し、証明書発行を承認、または拒否する。発行が承認されると、証明書状態は RA サーバによる鍵・証明書発行処理待ちとなるか、あるいは他の RA 操作者による発行審査待ちとなる。発行が拒否されると証明書状態は発行拒否となり、この申請に対する証明書発行処理は行われない。

証明書発行申請のシーケンス(発行審査を誰が、どういう順序で行うか)は、RA 管理者が RA コンソールのサイト管理機能を使用して設定する。

G) 一般利用者の鍵・証明書の取得

RA サーバによる鍵・証明書の発行処理が完了すると、証明書状態は発行済みとなる。RA 操作者は RA 操作端末で RA オペレータを起動し、「RA 操作者証明書の発行」で作成された IC カードを使用して、RA サーバへのログインを行う。その後、RA 操作者は RA オペレータの証明書情報取得機能により証明書状態を確認し、鍵・証明書の取得を行う。操作が完了したら RA サーバからログアウトする。

a) PKCS#12 取得要求

RAO1 または RAO2 は、RA サーバに対して、PKCS#12 取得要求を行う。要求が受け付けられると、PKCS#12 及び PIN が取得可能な状態になる。

b) PKCS#12 取得

RAO1 は RA サーバに対して PKCS#12 取得要求を行い、取得された PKCS#12 を RA 操作端末のハードディスクに保存する。

RAO1 は、ハードディスクに格納された PKCS#12 を、一般利用者ごとに別のリムーバブル媒体に複写し、オフラインで一般利用者に配付する。RAO1 は、リムーバブル媒体への複写後、ハードディスク上の PKCS#12 を速やかに削除する。

c) PIN 取得

RAO2 は RA サーバに対して PIN 取得要求を行い、取得された PIN を RA 操作端末のハードディスクに保存する。

RAO2 は、ハードディスクに格納された PIN を、一般利用者ごとに別の用紙に印字し、オフラインで一般利用者に配付する。RAO2 は、用紙への印字後、ハードディスク上の PIN を速やかに削除する。

H) 一般利用者の証明書の失効

TOE を運用する組織の責任者からの依頼により、証明書失効操作が開始される。RA 操作者は RA 操作端末で RA オペレータを起動し、「RA 操作者証明書の発行」で作成された IC カードを使用して、RA サーバへのログインを行う。その後、RA オペレータの鍵・証明書操作機能を使用して、下記の各操作を実施する。操作が完了したら RA サーバからログアウトする。

a) 証明書失効要求

RAO1 または RAO2 は、TOE を運用する組織の責任者から依頼を受けた一般利用者の証明書の失効要求を行う。RA 失効要求が受け付けられると、証明書状態は RA 操作者による失効審査待ちとなる。
証明書失効のシーケンス(失効要求を誰が行うか、誰が失効審査を行うか)は、RA 管理者が RA コンソールのサイト管理機能を使用して設定する。

b) 証明書失効審査

RAO1 または RAO2 は、証明書の失効申請の内容を審査し、証明書失効を承認、または拒否する。失効が承認されると、証明書状態は RA サーバによる証明書失効処理待ちとなる。失効が拒否されると証明書状態は失効要求前の状態に戻る。

l) 一般利用者の鍵・証明書の回復

一般利用者が鍵・証明書を紛失するなどした場合、鍵・証明書を再取得することができる。これを鍵・証明書の回復という。鍵・証明書の回復は TOE を運用する組織の責任者からの依頼により開始される。RA 操作者は RA 操作端末で RA オペレータを起動し、「RA 操作者証明書の発行」で作成された IC カードを使用して、RA サーバへのログインを行う。その後、RA 操作者は RA オペレータの鍵・証明書操作機能により鍵・証明書の取得を行う。操作が完了したら RA サーバからログアウトする。

a) PKCS#12 取得要求

KRO1 または KRO2 は、RA サーバに対して、PKCS#12 取得要求を行う。要求が受け付けられると、PKCS#12 及び PIN は RA 操作者による取得審査待ち状態になる。

b) PKCS#12 取得審査

KRO2 は、PKCS#12 取得要求の内容を審査し、PKCS#12 の取得を承認、または拒否する。取得が承認されると、PKCS#12 状態は KRO1 による取得待ちとなる。取得が拒否されると PKCS#12 状態は取得要求前の状態に戻る。

c) PIN 取得審査

KRO1 は、PKCS#12 取得要求の内容を審査し、PIN の取得を承認、または拒否する。取得が承認されると、PIN 状態は KRO2 による取得待ちとなる。取得が拒否されると PIN 状態は取得要求前の状態に戻る。

d) PKCS#12 取得

KRO1 は RA サーバに対して PKCS#12 取得要求を行い、取得された PKCS#12 を RA 操作端末のハードディスクに保存する。

KRO1 は、ハードディスクに格納された PKCS#12 を、一般利用者ごとに別のリムーバブル媒体に複写し、オフラインで一般利用者に配付する。KRO1 は、リムーバブル媒体への複写後、ハードディスク上の PKCS#12 を速やかに削除する。

e) PIN 取得

KRO2 は RA サーバに対して PIN 取得要求を行い、取得された PIN を RA 操作端末のハードディスクに保存する。

KRO2 は、ハードディスクに格納された PIN を、一般利用者ごとに別の用紙に印字し、オフラインで一般利用者に配付する。KRO2 は、用紙への印

字後、ハードディスク上の PIN を速やかに削除する。

J) 監査

監査者は RA 管理／監査端末で RA コンソールを起動し、システム管理者から配付された IC カードを使用して RA サーバにログインする。ログイン後、RA コンソールの監査機能を使用して監査ログの検索、表示を行い、RA サーバが正しく運用されているか監査を実施する。また、TOE 外の機能を使用して監査ログに対する改ざん、及び不当な削除が行われていないことを確認するために、監査ログの検証を行う。

監査が完了して監査ログが不要となった場合には、監査機能により監査ログの削除を行う。

操作が完了したら RA サーバからログアウトする。

2.2 保護対象資産

2.2.1 保護対象資産

TOE、または環境により保護される資産について、その所在を「表 2-12 保護対象資産」に示す。

表 2-12 保護対象資産

保護対象資産 ＼ 所在 / 形式	データベース内のテーブル / レコード	RA サーバ内のハードディスク / ファイル	RA 設定端末内のハードディスク / ファイル	RA 操作端末内のハードディスク / ファイル	セキュアゾーン LAN / パケット	操作端末 LAN / パケット	IC カード / データ	リムーバブル媒体 / ファイル
RA 鍵・証明書								●
RA 管理者・監査者鍵・証明書								●
信頼する CA 証明書								●
CMP 鍵・証明書								●
RA 動作環境情報		●	●					●
RA 管理者・監査者認証情報							●	
RA 管理情報	●				●	●		
オペレータ登録情報								●
RA 操作者認証情報	●				●	●	●	
監査ログ	●				●	●		
一般利用者鍵・証明書	●			●	●	●		

※網がけ部分は TSC にインポートされる、または TSC からエクスポートされた TSC 外の資産

以下では「表 2-12 保護対象資産」で示された保護対象資産の使用方法、及びライフサイクルについて説明する。

(1)RA 鍵・証明書

RA サーバの鍵・証明書。システム管理者からの依頼により CA オペレータが発行する。

CA オペレータは CA の機能を使用して RA サーバの鍵・証明書を PKCS#12 形式で発行し、リムーバブル媒体に格納してシステム管理者に配付する。

RA 鍵・証明書は、RA 設定端末上の RA セットアップの RA 動作環境情報設定機能により TSC 内にインポートされ、RA 動作環境情報内の RA サーバ証明書・秘密鍵として保存される。

(2)RA 管理者・監査者鍵・証明書

RA 管理者・監査者の鍵・証明書。システム管理者からの依頼により CA オペレータが発行する。

CA オペレータは CA の機能を使用して RA 管理者・監査者の鍵・証明書を PKCS#12 形式で発行し、リムーバブル媒体に格納してシステム管理者に配付する。

RA 管理者・監査者鍵・証明書は、RA 設定端末上の RA セットアップの RA 管理者・監査者登録機能により TSC 内にインポートされ、IC カード内の RA 管理者・監査者認証情報として保存される。

(3)信頼する CA 証明書

RA と接続される CA、及びその上位 CA の証明書。RA 管理者からの依頼により CA オペレータが取得する。

CA オペレータは CA の機能を使用して CA、及びその上位 CA の証明書を取得し、リムーバブル媒体に格納してシステム管理者に配付する。

信頼する CA 証明書は、RA コンソールのトラスト CA 管理機能により TSC 内にインポートされ、RA 管理情報内の信頼する CA 証明書として保存される。

(4)CMP 鍵・証明書

CMP クライアントの鍵・証明書、及び CMP サーバの証明書。RA 管理者からの依頼により CA オペレータが発行する。

CA オペレータは CA の機能を使用して CMP クライアントの鍵・証明書を PKCS#12 形式で発行し、CA が管理する CMP サーバ証明書とともにリムーバブル媒体に格納して RA 管理者に配付する。

CMP 鍵・証明書は、RA コンソールの CA 管理機能により TSC 内にインポートされ、RA 管理情報内の CA 情報として保存される。

(5)RA 動作環境情報

RA サーバの動作に必要な以下のデータの総称である。

・データベースのネットワークアドレス
・データベースアクセス時の認証情報
・RA サーバ鍵・証明書
・RA サーバ鍵・証明書暗号化パスワード　等

システム管理者は、RA 設定端末上の RA セットアップの RA 動作環境情報設定機能により、RA の動作環境設定を行う。RA サーバ証明書・秘密鍵はあらかじめ用意されたリムーバブル媒体上の RA 鍵・証明書からインポートされる。その他の情報は、システム管理者が RA セットアップの画面から入力する。設定された情報は RA 設定端末のディスクに RA 動作環境情報として保存される。

システム管理者は、RA 設定端末上の RA セットアップの RA 動作環境情報エクスポート機能により、RA 動作環境情報をリムーバブル媒体にエクスポートする。

システム管理者は、RA サーバマシン上の RA セットアップの RA 動作環境情報インポート機能により、エクスポートされた RA 動作環境情報をインポートする。

(6)RA 管理者・監査者認証情報

RA 管理者・監査者の認証で使用される鍵・証明書。

システム管理者は、RA 設定端末上の RA セットアップの RA 管理者・監査者登録機能により、RA 管理者・監査者登録の登録を行う。このとき、あらかじめ用意されたリムーバブル媒体上の RA 管理者・監査者鍵・証明書が IC カードに格納される。

システム管理者は作成された IC カードを RA 管理者・監査者に配付する。

(7)RA 管理情報

RA サーバが管理する以下の情報の総称である。

・信頼する CA 証明書
・CA 情報
・サイト情報
・オペレータ情報
・証明書情報
・サイト鍵

信頼する CA 証明書は、RA コンソールのトラスト CA 管理機能により、あらかじめ用意されたリムーバブル媒体上の信頼する CA 証明書からインポートされる。

CA 情報は RA コンソールの CA 管理機能により登録、変更、削除される。CA 情報には CA サーバのネットワークアドレス､CRL の格納ディレクトリ情報､CMP サーバ・クライアントの鍵・証明書が含まれる。CMP サーバ・クライアントの鍵・証明書は、あらかじめ用意されたリムーバブル媒体上の CMP 鍵・証明書からインポートされる。

サイト情報は RA コンソールのサイト管理機能により登録、変更、削除される。サイト情報にはサイトに関連づけられる CA、証明書発行ポリシー、状態フロー制御情報などが含まれる。

オペレータ情報は RA セットアップの RA 管理者・監査者登録機能、及び RA コンソールのオペレータ管理機能により登録、変更、削除される。オペレータ情報には、オペレータが属するサイトの情報、RA 操作者証明書の発行申請データ、オペレータの証明書、オペレータの種別などが含まれる。RA 操作者証明書の発行申請データは RA 操作端末に接続された IC カードにより生成され、RA オペレータのオペレータ環境設定機能のオペレータ登録により RA サーバにインポートされる。RA サーバは発行申請データを用いて CA サーバに対して証明書の発行申請を行い、発行された証明書をオペレータの証明書として保存する。

証明書情報は RA が発行申請を受け付けた証明書に関する情報であり､証明書の申請情報、証明書の状態を管理する証明書状態属性、鍵の状態を管理する鍵状態属性、証明書の削除状態を管理する証明書削除状態属性などが含まれる。

サイト鍵は TOE に登録されたサイトの鍵で、そのサイト内で申請された一般利用者の鍵・証明書の暗号化に使用される。

CA 情報、サイト情報、オペレータ情報は、それぞれ RA コンソールの CA 管理

機能、サイト管理機能、オペレータ管理機能により設定される。証明書情報は、RA 操作者により証明書発行申請が行われたときに、RA サーバにより生成される。サイト鍵は、RA 管理者によりサイトの登録が行われたときに、RA サーバにより生成される。

(8)オペレータ登録情報

RA 操作者の識別情報、及び RA サーバへの接続情報であり、RA 操作者によるオペレータ登録時に使用される。

RA 管理者は RA コンソールのオペレータ管理機能により RA 操作者の登録を行う。このときオペレータ管理機能によりオペレータ登録情報がリムーバブル媒体に格納される。

RA 操作者は、オペレータ登録情報を使用して RA オペレータのオペレータ環境設定機能によりオペレータの登録を行う。

(9)RA 操作者認証情報

RA 操作者の認証で使用される鍵・証明書、及び RA 操作者証明書の発行申請データ。

RA 操作者は RA オペレータのオペレータ管理機能により RA 操作者の登録を行う。このとき、IC カードに RA 操作者の秘密鍵、及び証明書発行申請データが作成される。また、RA サーバに対して証明書の発行申請が行われ、発行された証明書が IC カードに格納される。

(10)監査ログ

RA サーバの操作の履歴であり、RA サーバの監査機能により、RA サーバ上のデータベースに作成される。RA コンソールの監査機能により表示、検証、削除が行われ、RA オペレータの監査機能により表示が行われる。

(11) 一般利用者鍵・証明書

一般利用者の鍵・証明書。

RA オペレータから証明書の発行申請・審査が行われると、RA サーバで鍵ペアの生成が行われる。生成された鍵は KeySafer 機能によりデータベースに格納される。

RA サーバは生成された鍵ペアを使用して CA に対して証明書発行申請を行う。発行された証明書は秘密鍵とともに PKCS#12 形式にエンコードされ、PKCS#12 の PIN とともに暗号化されて KeySafer 機能によりデータベースに格納される。

RAO1 及び RAO2 は、一般利用者の PKCS#12 及び PIN をそれぞれ取得する。RAO1 は取得した PKCS#12 をリムーバブル媒体に格納し、オフラインで該当する一般利用者に配付する。また、RAO2 は PIN を用紙に印字し、オフラインで該当する一般利用者に配付する。KRO1 及び KRO2 により鍵回復が行われる場合は、同様の鍵・証明書の取得と配付が KRO1 及び KRO2 によって行われる。

2.2.2 保護対象資産に対する操作

保護対象資産のうちデータベース上に存在するものは RA サーバにより保護され、RA サーバ以外では、特定の権限を有するものだけが RA サーバのエージェント機能を介してこれにアクセスすることができる。このとき、RA サーバ、及び RA サーバに対して要求を行う主体をサブジェクト、サブジェクトにより操作される資産をオブジェクトという。

サブジェクトには以下のものがある。

RA サーバプロセス	：	RA サーバ自身のプロセス
RA 管理者プロセス	：	RA 管理者の権限でログインを行った RA コンソールのプロセス
監査者プロセス	：	監査者の権限でログインを行った RA コンソールのプロセス
RA 操作者プロセス	：	RA 操作者の権限でログインを行った RA オペレータのプロセス

上記のサブジェクトは、RA サーバのエージェント機能が提供する機能を使用して、以下のオブジェクトに対する操作を行うことができる。

一般利用者証明書オブジェクト	：一般利用者鍵・証明書に含まれる一般利用者の証明書
一般利用者 PKCS#12 オブジェクト	：一般利用者鍵・証明書に含まれる一般利用者の PKCS#12
一般利用者 PIN オブジェクト	：一般利用者鍵・証明書に含まれる一般利用者の PIN
監査ログオブジェクト	：監査ログ
CA 情報オブジェクト	：RA 管理情報に含まれる CA 情報
サイト情報オブジェクト	：RA 管理情報に含まれるサイト情報
オペレータ情報オブジェクト	：RA 管理情報に含まれるオペレータ情報
信頼する CA 証明書オブジェクト	：RA 管理情報に含まれる信頼する CA 証明書

どのサブジェクトがどのオブジェクトに対してどのような操作を行うことができるかは、サブジェクトのオペレータ種別に従って RA サーバにより決定される。

3 TOE セキュリティ環境

3.1 前提条件

3.1.1 物理的な条件

ASM.ACCESS（アクセスの物理的制限）
RA サーバ、RA 設定端末はセキュアゾーンに設置される。セキュアゾーンの入室時には物理鍵や認証システムを必要とし、セキュアゾーンへの入室はセキュアゾーンに設置される各マシンの管理者だけが許可される。各マシン管理者に許可された者がメンテナンス等のためにセキュアゾーンに入室する場合もあるが、必ず各マシン管理者の監視下で作業を行う。

ASM.CLIENT_ACCESS（クライアントアクセスの物理的制限）
RA 管理／監査端末、RA 操作端末には、TOE を運用する組織に属する者だけが物理的にアクセスできる。

ASM.MEDIA_PROTECT（媒体の物理的保護）
TOE 内にあるデータのバックアップが保管された媒体は、適切な手順に従って管理、保管され、物理的な破壊、及び盗難から保護されている。

ASM.OPERATOR_PROTECT（オペレータ秘密鍵の物理的保護）
オペレータの鍵・証明書は耐タンパー性のある IC カードに格納され、IC カード盗難時にも物理的な攻撃による秘密鍵の暴露、不正使用から保護される。

3.1.2 人的な条件

ASM.ADMIN（システム管理者・RA 管理者・監査者・他サーバの管理者の信頼性）

システム管理者、RA 管理者、監査者は TOE を運用する組織に属し、TOE を運用する組織の責任者によって任命される。
システム管理者、RA 管理者、監査者、他サーバの管理者は、それぞれの役割を果たす上で必要となる知識を習得するための教育を施される。
システム管理者、RA 管理者、監査者、他サーバの管理者は、それぞれに課せられた役割に対して、許可された一連の行為に関する悪意を持った行為は行わず、システムの運用に協力的に関わる。

ASM.OPERATOR（RA 操作者の信頼性）

RA 操作者は TOE を運用する組織に属し、TOE を運用する組織の責任者によって任命される。
RA 操作者は RA 操作者としての役割を果たす上で必要となる知識を習得するための教育を施される。

3.1.3 接続条件

ASM.CONNECT（接続制限）

セキュアゾーン LAN はファイアウォールを介して操作端末 LAN にのみ接続される。
操作端末 LAN には TOE を運用する組織に属する者だけがアクセスできるよう物理的に保護される。また、操作端末 LAN が TOE を運用する組織外のネットワークに接続される場合は、TOE を運用する組織外のネットワークから操作端末 LAN に対してアクセスできないよう、操作端末 LAN はファイアウォールにより保護される。
操作端末 LAN から RA サーバへのアクセスは、RA 管理・監査端末及び RA 操作端末から RA サーバの特定のポートに対してのみ接続可能であるよう、セキュアゾーン LAN－操作端末 LAN 間のファイアウォールにより制限される。

3.1.4　使用条件

ASM.RELIABILITY（TOE 構成要素の信頼性）
TOE が動作する上で必要となるハードウェア及びソフトウェアは、システム管理者、RA 管理者、監査者、RA 操作者により適切にインストール、設定し管理される。

ASM.CA_RELIABILITY（CA の信頼性）
TOE が証明書の発行・失効要求を行う CA は信頼できる CA のみであり、これらの CA はセキュアゾーン LAN に接続される。

ASM.OTHER_RELIABILITY（その他のマシンの信頼性）
セキュアゾーンに設置される TOE 構成要素外のハードウェア及びソフトウェアは、他サーバマシン管理者により適切に設定し管理される。

ASM.IMPORTED（インポートデータの信頼性）
TSC にインポートされる鍵・証明書は、セキュアゾーン LAN に接続された CA により発行されたものである。
TSC にインポートされる利用者データは、暴露・盗難・改ざんから保護するため、関連者により適切に管理される。

ASM.EXPORTED（エクスポートデータの保護）
TSC からエクスポートされた鍵・証明書を含む利用者データは、暴露・盗難・改ざんから保護するため、関連者により適切に管理される。

ASM.CLIENT_RESTORE（クライアント環境の復元）
RA 管理・監査端末、または RA 操作端末上の TSC 内データが毀損され、RA コンソール、または RA オペレータが正常に動作しなくなった場合、各端末を使用するオペレータは、自身の責任で TOE の再インストール、及び再設定を行う。

ASM.PASSWORD（パスワード及び PIN の管理）
TOE 利用者が TOE を使用する際に必要となるパスワード及び PIN は、TOE 利用者本人によって適切に管理され、本人以外のものに知られることはない。
パスワード及び PIN は類推が困難であり、適切な頻度で変更される。

3.2 脅威

T.DATA_CORRUPTED（TOE データの毀損）
システム管理者による TOE 外の機能の誤操作で、RA 動作環境情報が削除、または変更される。

T.DATA_REMOVED（TOE データの削除）
RA 管理者、または監査者による TOE の機能の誤操作で、RA 管理情報、監査ログが削除される。

T.UNAUTH_TOE_ACCESS（TOE への不正アクセス）
TOE に登録されたオペレータ以外の者が、RA コンソール、または RA オペレータを使用し、TOE が提供する機能で RA 管理情報、監査ログ、一般利用者鍵・証明書を利用する。

T. UNAUTH _OPERATION（許可されない操作）
オペレータが自らに与えられた権限外の操作を行うことにより、TOE の運用上許可されない TSC 内データの作成、変更、削除、エクスポートが行われる。

T.INVALID_OPERATION（不正操作）
RA 操作者が故意、または誤操作により、自らの権限内で、TOE の運用上許可されない鍵・証明書の発行、取得、失効、削除を行う。

T. INVALID_TERMINAL_ACCESS（端末への不正アクセス）
TOE を運用する組織に属する者のうち、悪意を持つ者が、直接または操作端末 LAN を介して RA 管理／監査端末、RA 操作端末にアクセスし、以下の行為を行う。
・TSC 内のデータを削除、または変更する。
・TSC からエクスポートされ、RA 操作端末からアクセス可能な状態にある一般利用者鍵・証明書を不正に利用する。

T.INTERCEPTION（盗聴）
TOE を運用する組織に属する者のうち、悪意を持つ者により、RA 管理／監査端末、RA 操作端末と RA サーバ間の送受信データが盗聴される。

3.3 組織のセキュリティ方針

- **P.OS_IA（OS による識別認証）**
  TOE が動作する上で必要となるすべてのマシンの OS は識別認証機能を持ち、あらかじめ登録された利用者のログインのみを許可する。

- **P.OS_ACCESS_CONTROL（OS によるアクセス制御）**
  TOE が動作する上で必要となるすべてのマシンの OS はアクセス制御機能を持ち、識別された利用者による OS が管理する資源への許可されないアクセスを抑止する。

- **P.DOMAIN_SEPARATION（OS によるドメイン分離）**
  TOE が動作する上で必要となるすべてのマシンの OS はドメイン分離機能を持ち、TSF、及び IT 環境により提供される全てのセキュリティ機能が他の機能の干渉（破壊）を受けないことを保証する。

- **P.CA_RELIABILITY（CA の信頼性）**
  TOE は、CA への証明書発行・失効要求に際して CA の識別認証を行い、要求先の CA があらかじめ登録された信頼できる CA であることを確認する。

- **P.CIPHER（秘密データの暗号化）**
  TSC 内に存在する鍵、パスワード等の秘密データを暗号化する。

- **P.AUDIT_INVISIBLE（監査ログの不可視性）**
  監査ログの内容は、TOE 外の機能による参照を不可能にする。

4 セキュリティ対策方針

4.1 TOE のセキュリティ対策方針

O.AUTH（TOE 利用者識別認証）
TOE は、RA サーバにおいて、RA サーバに登録されたオペレータのログインのみを許可するよう、RA コンソール、及び RA オペレータからのログイン要求に際して識別認証を行う。

O. NETWORK _ENCRYPT（暗号通信）
TOE は、RA サーバ－RA コンソール・RA オペレータ間で送受信されるデータが盗聴され、暴露、改変、不正使用されることを防止するため、RA サーバ－RA コンソール・RA オペレータ間の通信データを暗号化する。

O.PERMISSION（実行権限管理）
TOE は、RA サーバにおいて、オペレータによる許可されない操作の実行を抑止するため、オペレータの実行権限を管理する。

O.STATUS_FLOW_CONTROL（一般利用者鍵・証明書の状態フロー制御）
TOE は、RA サーバにおいて、単独の RA 操作者によって一般利用者鍵・証明書の発行、失効、取得、削除が行われることを抑止するため、一般利用者鍵・証明書の状態フロー制御を行う。

O.AUDIT（監査記録）
TOE はオペレータによる全操作の履歴を監査ログとして記録する。また、TOE は、監査ログにアクセスするための以下の機能を提供する。
・監査ログを参照する
・監査ログ内のレコードが TOE 外の機能により改ざん、及び削除されていないことを検証する
・監査ログを削除する
監査は監査者が行うものとし、監査者に対しては上記のすべての機能を許可する。RA 操作者には監査ログの参照のみを許可する。

O.CA_AUTH（CA の識別認証）
TOE は、RA サーバにおいて、CA に対して証明書の発行・失効要求を行うとき、要求先の CA があらかじめ RA サーバに証明書を登録された信頼できる CA であることを確認するため、CA の識別認証を行う。

O.CIPHER（データの暗号化）
TOE は、TSC 内に存在する秘密鍵、認証情報、パスワード、PIN、監査ログ、オペレータ登録情報を暗号化する。

4.2 環境のセキュリティ対策方針

4.2.1 IT 環境セキュリティ対策方針

OE.IC_IA（IC カードによる識別認証）
IC カードは、IC カードの正当な所有者以外の者からのアクセスを抑止するため、利用者からのアクセス要求に対して識別認証を行う。

OE.OS_IA（OS による識別認証）
OS は、あらかじめ登録された利用者以外の者のログインを抑止するため、利用者からのログイン要求に際して識別認証を行う。

OE.OS_ACCESS_CONTROL（OS によるアクセス制御）
OS は、OS が管理する資源への識別された利用者による許可されないアクセスを抑止するため、OS が管理する資源へのアクセスに対してアクセス制御を実施する。

OE.OS_CORRECT_TIME（OS が提供する時刻）
OS は、正確な日付／時刻を提供する。

OE.DOMAIN_SEPARATION（OS によるドメイン分離）
OS は、TSF、及び IT 環境により提供される全てのセキュリティ機能が他の機能の干渉（破壊）を受けることを抑止するドメイン分離機能を提供する。

4.2.2　運用／管理セキュリティ対策方針

OE.ACCESS（アクセスの物理的制限）

TOE を運用する組織の責任者は、RA サーバマシン、及び RA 設定端末がセキュアゾーンに設置されることに責任を持つ。

TOE を運用する組織の責任者は、セキュアゾーンにはセキュアゾーンに設置された各マシンのマシン管理者、及び各マシン管理者に特に許可された者だけが入室できるよう、入退室管理を実施する。

各マシン管理者に許可された者がセキュアゾーンに入室する場合、入室を許可した各マシン管理者は、各マシン管理者に許可された者とともに入退室し、各マシン管理者に許可された者が許可された操作以外の操作を行わないよう監視する。

OE.CLIENT_ACCESS（クライアントアクセスの物理的制限）

TOE を運用する組織の責任者は、TOE を運用する組織に属する者だけが物理的にアクセスできる場所が確保され、その場所に RA 管理／監査端末、RA 操作端末が設置されることに責任を持つ。

OE.MEDIA_PROTECT（媒体の物理的保護）

TOE を運用する組織の責任者は、破壊、及び盗難から保護される物理的に強固な管理場所が確保され、その場所に TSC 内のデータをバックアップした媒体が保管されることに責任を持つ。

OE.OPERATOR_PROTECT（オペレータの秘密鍵の物理的保護）

オペレータは、鍵・証明書を耐タンパー性のある IC カードに格納し、本人以外が使用できないように管理する。

OE.ADMIN（システム管理者・RA 管理者・監査者・他サーバの管理者の信頼性）

TOE を運用する組織の責任者は、TOE を運用する組織に属する者の中から適した者を選別し、システム管理者、RA 管理者、監査者に任命する。

TOE が正常に動作しない場合、システム管理者、RA 管理者、監査者は TOE の再インストール、再セットアップを行う。

また、TOE を運用する組織の責任者は、システム管理者、RA 管理者、監査者、他サーバの管理者に対して以下の教育、及び訓練を実施する。

・課せられた役割を果たす上で必要となる知識を習得するための技術教育
・課せられた役割に対して、セキュリティ意識を向上させ、悪意を持った行為を行わないようにするためのセキュリティ教育
・課せられた役割を果たす上で、誤操作により TOE データを毀損する可能性を低減させるための技術教育、及び訓練

OE.OPERATOR（RA 操作者の信頼性）

TOE を運用する組織の責任者は、TOE を運用する組織に属する者の中から適した者を選別し、RA 操作者に任命する。

TOE が正常に動作しない場合、RA 操作者は TOE の再インストール、再セットアップを行う。

また、TOE を運用する組織の責任者は、RA 操作者に対して、RA 操作者としての役割を果たす上で必要となる知識を習得するための技術教育を実施する。

OE.CONNECT（接続制限）

TOE を運用する組織の責任者は、セキュアゾーン LAN がファイアウォールを介して操作端末 LAN のみに接続されるように LAN が設置されることに責任を持つ。

TOE を運用する組織の責任者は、操作端末 LAN から RA サーバへのアクセスについて、RA 管理／監査端末、RA 操作端末から RA サーバが使用するポートへのパケットだけを通過させるようにファイアウォールが設定されることに責任を持つ。

TOE を運用する組織の責任者は、TOE を運用する組織に属する者だけがアクセスできる物理的に保護された場所を確保し、その場所に操作端末 LAN を設置することに責任を持つ。

TOE を運用する組織の責任者は、操作端末 LAN が TOE を運用する組織外のネットワークに接続される場合、TOE を運用する組織外のネットワークから操作端末 LAN に対してアクセスできないよう、操作端末 LAN がファイアウォールにより保護されることを保証する。

OE.RELIABILITY（TOE 構成要素の信頼性）

システム管理者、RA 管理者、監査者、RA 操作者は、TOE が動作する上で必要となるハードウェア及びソフトウェアを適切にインストール、設定し管理する。また、OS の日付／時刻の設定を適切に行う。

システム管理者は監査ログ等を格納する RDBMS を適切に設定し、ディスク領域が不足しないように管理を行う。

OE.OTHER_RELIABILITY（その他のマシンの信頼性）

他サーバマシン管理者は、それぞれが管理するマシンについて、ハードウェア及びソフトウェアを適切に設定し管理する。

OE.CA_RELIABILITY（CA の信頼性）

TOE を運用する組織の責任者は、信頼する CA のみがセキュアゾーン LAN に接続されることに責任を持つ。また、RA 管理者は、セキュアゾーン LAN に接続された信頼する CA のみを、信頼する CA として TOE に登録する。

OE. IMPORTED（インポートデータの信頼性）

TSC に鍵・証明書をインポートする者は、インポートされる鍵・証明書がセキュアゾーン LAN に接続された CA により発行されたものであることを確認し、インポートされる鍵・証明書の信頼性を確保する。

TSC に利用者データをインポートする者は、インポートされる利用者データを暴露・盗難・改ざんから保護するために適切に管理し、インポートされる利用者データの信頼性を確保する。

OE. EXPORTED（エクスポートデータの保護）

TSC から鍵・証明書を含む利用者データをエクスポートする者は、暴露・盗難・改ざん等から保護するために、エクスポートされた鍵・証明書を含む利用者データを適切に管理する。

OE. PASSWORD（パスワード及び PIN の管理）

TOE 利用者は､TOE を使用する際に必要となるパスワード及び PIN が本人以外の者に知られることがないよう、パスワード及び PIN を適切に管理する。

TOE 利用者は、類推が困難であるパスワード及び PIN を設定する。

TOE 利用者は、パスワード及び PIN を適切な頻度で変更する。

OE.BACKUP（バックアップ）

システム管理者は、TOE の運用環境を復旧できるよう、RA サーバマシン上の保護資産のバックアップを定期的に実施する。

OE.STATUS_FLOW_MANAGEMENT（状態フロー制御管理）

RA 管理者は、単独の RA 操作者が一般利用者鍵・証明書の発行、失効、取得、削除を行うことがないよう、RA コンソールのサイト管理機能を使用して、状態フロー制御情報を適切に管理する。

5 IT セキュリティ要件

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

(1) セキュリティ監査（FAU）

表 5-1：FAU 機能要件

セキュリティ機能要件		コンポーネント
セキュリティ監査データ生成	監査データ生成	FAU_GEN.1
	利用者識別情報の関連付け	FAU_GEN.2
セキュリティ監査レビュー	監査レビュー	FAU_SAR.1
	限定監査レビュー	FAU_SAR.2
	選択可能監査レビュー	FAU_SAR.3
セキュリティ監査事象格納	保護された監査証跡格納	FAU_STG.1

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*］レベルのすべての監査対象事象；及び

- ［選択：*最小*、*基本*、*詳細*、*指定なし*］：***指定なし***

c) ［割付：*上記以外の個別に定義した監査対象事象*］

- ［割付：*上記以外の個別に定義した監査対象事象*］

個別に定義された監査対象事象を表 5-2 に、監査対象事象と機能コンポーネントの対応を表 5-3 に示す。

表 5-2：監査対象事象

番号	事象	番号	事象
1	起動 ※1	２１	証明書発行拒否
2	停止 ※1	２２	鍵暗号化
3	CA 追加	２３	鍵暗号化失敗
4	CA 更新	２４	証明書失効
5	CA 削除	２５	証明書失効拒否
6	サイト追加	２６	鍵回復要求
7	サイト更新	２７	一括鍵回復要求
8	サイト削除	２８	鍵取得承認
9	オペレータ追加	２９	鍵取得拒否
１０	オペレータ更新	３０	鍵取得準備
１１	オペレータ削除	３１	PKCS#12 取得
１２	信頼する証明書の追加・削除	３２	PIN 取得
１３	オペレータ証明書申請	３３	削除要求
１４	ログイン	３４	削除審査
１５	ログアウト	３５	削除拒否
１６	証明書申請	３６	削除実行
１７	一括証明書申請	３７	監査ログ取得
１８	鍵生成	３８	監査ログ検証 ※1
１９	鍵生成失敗	３９	監査ログ削除
２０	証明書発行	４０	CRL 取得 ※1

※1 これらの監査対象事象は機能要件に対応するものではなく、独自に追加された監査対象事象である。

表 5-3：個別の監査対象事象

コンポーネント	監査対象事象	コンポーネント	監査対象事象
FAU_GEN.1	なし	FIA_SOS.1[1]	なし
FAU_GEN.2	なし	FIA_SOS.1[2]	なし
FAU_SAR.1	37	FIA_SOS.1[3]	なし
FAU_SAR.2	37	FIA_SOS.2	なし
FAU_SAR.3	37	FIA_UAU.1	14,15
FAU_STG.1	なし	FIA_UAU.2	14,15
FCS_CKM.1	なし	FIA_UID.1	14,15
FCS_CKM.4	なし	FIA_UID.2	14,15
FCS_COP.1[1]	38	FMT_MSA.1[1]	3～11
FCS_COP.1[2]	なし	FMT_MSA.1[2]	14～36
FCS_COP.1[3]	なし	FMT_MSA.2	なし
FCS_COP.1[4]	なし	FMT_MSA.3[1]	3～11
FDP_ACC.1	なし	FMT_MSA.3[2]	14～36
FDP_ACF.1	3～11	FMT_MSA.3[3]	なし
FDP_IFC.1	なし	FMT_MSA.3[4]	なし
FDP_IFF.1	14～36	FMT_MTD.1	39
FDP_ITC.1	3,4,9,10	FMT_SMR.1	6～11
FDP_ITT.1	なし	FPT_ITT.1	なし

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) 各監査対象事象種別に対して、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*］

- ［割付：*その他の監査関連情報*］：
  監査ログのレコードに割り振られる一意な連続した番号

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*]：***監査者、RA 操作者***
- [割付：*監査情報のリスト*]：
  監査者に対しては FAU_GEN.1 で規定されるすべての監査情報
  RA 操作者に対しては、表 5-2 の監査対象事象のうち、自身が属するサイトに関する 14～36 の事象の監査情報

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.3	（選択可能監査レビュー）

下位階層： なし

FAU_SAR.3.1
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*］：
  事象の日付・時刻、事象の種別、事象の結果、サイト ID、オペレータ種別、オペレータ ID、
  要求番号
- ［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_STG.1	（保護された監査証跡格納）

下位階層： なし

FAU_STG.1.1
TSF は、格納された監査記録を不正な削除から保護しなければならない。
FAU_STG.1.2
TSF は、監査記録の改変を［選択：*防止、検出*］できねばならない。

- ［選択：*防止、検出*］：***検出***

依存性： FAU_GEN.1 監査データ生成

(2) 暗号サポート（FCS）

表 5-4：FCS 機能要件

セキュリティ機能要件		コンポーネント
暗号鍵管理	暗号鍵生成	FCS_CKM.1
	暗号鍵破棄	FCS_CKM.4
暗号操作	暗号操作	FCS_COP.1[1]
		FCS_COP.1[2]
		FCS_COP.1[3]
		FCS_COP.1[4]

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*］：***表 5-5 の「標準」***
- ［割付：*暗号鍵生成アルゴリズム*］：***表 5-5 の「アルゴリズム」***
- ［割付：*暗号鍵長*］：***表 5-5 の「鍵長」***

表 5-5：暗号鍵生成

アルゴリズム	標準	鍵長（bit）
RC2	PKCS#5	128
RC4	PKCS#5	128
RSA	PKCS#1	RA サーバの鍵長

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

FCS_CKM.4	（暗号鍵破棄）

下位階層： なし

FCS_CKM.4.1

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*］：***メモリから削除、RDBMS から DELETE 文で削除***

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

FCS_COP.1[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*］：***RFC2104、PKCS#5***
- ［割付：*暗号アルゴリズム*］：***HMAC-SHA1-1、RC2***
- ［割付：*暗号鍵長*］：***128bit***
- ［割付：*暗号操作のリスト*］：***監査ログデータの鍵付きハッシュの生成、及び検証***

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

FCS_COP.1[2]	**（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*］：***PKCS#1, RFC3174***
- ［割付：*暗号アルゴリズム*］：***RSAwithSHA-1***
- ［割付：*暗号鍵長*］：***512,1024,2048***
- ［割付：*暗号操作のリスト*］：***ディジタル署名の検証***

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

FCS_COP.1[3]	**（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*］：***PKCS#1, RFC3174***
- ［割付：*暗号アルゴリズム*］：***RSAwithSHA-1***
- ［割付：*暗号鍵長*］：***512,768,1024,2048***
- ［割付：*暗号操作のリスト*］：***ディジタル署名の生成、及び検証***

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

FCS_COP.1[4]	**（暗号操作）**

下位階層： なし

FCS_COP.1.1
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*］：***表 5-6 の「標準」***
- ［割付：*暗号アルゴリズム*］：***表 5-6 の「アルゴリズム」***
- ［割付：*暗号鍵長*］：***表 5-6 の「鍵長」***
- ［割付：*暗号操作のリスト*］：***表 5-6 の「暗号操作」***

表 5-6：暗号操作

アルゴリズム	標準	鍵長（bit）	暗号操作
RC2	PKCS#5	128	データの暗号化、及び復号
RC4	PKCS#5	128	データの暗号化、及び復号
RSA	PKCS#1	RA サーバの鍵長	データの暗号化、及び復号

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

(3)　利用者データ保護（FDP）

表 5-7：FDP 機能要件

セキュリティ機能要件		コンポーネント
アクセス制御方針	サブセットアクセス制御	FDP_ACC.1
アクセス制御機能	セキュリティ属性によるアクセス制御	FDP_ACF.1
情報フロー制御方針	サブセット情報フロー制御	FDP_IFC.1
情報フロー制御機能	単純セキュリティ属性	FDP_IFF.1
TSF 制御外からのインポート	セキュリティ属性無しの利用者データのインポート	FDP_ITC.1
TOE 内転送	基本内部転送保護	FDP_ITT.1

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*]：

  サブジェクト
  RA 操作者プロセス
  RA 管理者プロセス

  オブジェクト
  オペレータ情報オブジェクト
  一般利用者証明書オブジェクト
  一般利用者 PKCS#12 オブジェクト
  一般利用者 PIN オブジェクト
  CA 情報オブジェクト

  サブジェクトとオブジェクト間の操作
  オペレータ情報オブジェクトへの RA 操作者証明書の発行申請データの読み込み
  証明書発行申請、発行審査、取得
  証明書失効要求、失効審査
  証明書削除要求、削除審査
  PKCS#12 取得要求、取得審査、取得
  PIN 取得要求、取得審査、取得
  CA 情報オブジェクトへの CMP サーバ・クライアントの鍵・証明書の読み込み

- [割付：*アクセス制御 **SFP***]：***オペレータアクセス制御 SFP***

依存性： FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1	**（セキュリティ属性によるアクセス制御）**

下位階層： なし

FDP_ACF.1.1

TSF は、[割付：*セキュリティ属性、名前付けされたセキュリティ属性のグループ*] 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：*セキュリティ属性、名前付けされたセキュリティ属性のグループ*]：
  オペレータ種別
  オペレータ ID
  サイト ID
  CAID

- [割付：*アクセス制御 SFP*]：***オペレータアクセス制御 SFP***

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*]：***表 5-8 の制御されたサブジェクトが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。***

表 5-8：オペレータアクセス規則

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*
オペレータ種別が RAO1 の RA 操作者プロセス	サブジェクトと同じオペレータ ID によって識別されるオペレータ情報オブジェクト	RA 操作者証明書の発行申請データの読み込み
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者証明書オブジェクト	発行審査
		失効要求
		失効審査
		削除要求
		削除審査
		取得
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PKCS#12/PIN オブジェクト	取得要求
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PKCS#12 オブジェクト	取得
オペレータ種別が RAO2 の RA 操作者プロセス	サブジェクトと同じオペレータ ID によって識別されるオペレータ情報オブジェクト	RA 操作者証明書の発行申請データの読み込み
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者証明書オブジェクト	発行申請
		発行審査
		失効要求
		失効審査
		削除要求
		削除審査
		取得
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PKCS#12/PIN オブジェクト	取得要求
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PIN オブジェクト	取得

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*
オペレータ種別が KRO1 の RA 操作者プロセス	サブジェクトと同じオペレータ ID によって識別されるオペレータ情報オブジェクト	RA 操作者証明書の発行申請データの読み込み
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PKCS#12/PIN オブジェクト。	取得要求
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PKCS#12 オブジェクト。	取得
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PIN オブジェクト	取得審査
オペレータ種別が KRO2 の RA 操作者プロセス	サブジェクトと同じオペレータ ID によって識別されるオペレータ情報オブジェクト	RA 操作者証明書の発行申請データの読み込み
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PKCS#12/PIN オブジェクト	取得要求
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PIN オブジェクト	取得
	サブジェクトと同じサイト ID によって識別されるサイトに属する一般利用者 PKCS#12 オブジェクト	取得審査
オペレータ種別が CONSOLE の RA 管理者プロセス	RA コンソールの CA 管理機能で操作中の CA と同じ CAID で識別される CA 情報オブジェクト	CMP サーバ・クライアントの鍵・証明書の読み込み

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に対するサブジェクトの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に対するサブジェクトの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*］：

  RA 操作者がユーザ ID／パスワードにより識別認証されている場合、自身のオペレータ証明書の発行申請、取得以外の操作は拒否される。

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

FDP_IFC.1　　（サブセット情報フロー制御）

下位階層： なし

FDP_IFC.1.1

TSFは、［割付：サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト］に対して[割付：情報フロー制御SFP] を実施しなければならない。

- [割付：サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト]：***表 5-9***
- ［割付：情報フロー制御 SFP］：***状態フロー制御 SFP***

表 5-9：制御された情報の流れを引き起こす操作のリスト

サブジェクト	情報	操作
RA 操作者プロセス	証明書情報	発行申請
		発行承認
		発行拒否
		失効要求
		失効承認
		失効拒否
		削除要求
		削除承認
		削除拒否
	鍵情報(PKCS#12)	取得要求
		取得承認
		取得拒否
		取得
	鍵情報(PIN)	取得要求
		取得承認
		取得拒否
		取得
RA サーバプロセス	証明書情報	発行
		失効
		削除
	鍵情報(PKCS#12)	生成
	鍵情報(PIN)	生成

依存性： FDP_IFF.1 単純セキュリティ属性

FDP_IFF.1	（単純セキュリティ属性）

下位階層： なし

FDP_IFF.1.1

TSFは、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付：*情報フロー制御**SFP***]を実施しなければならない：[割付：*セキュリティ属性の最小数及び種別*] 。

- ［割付：*情報フロー制御 SFP*］：***状態フロー制御 SFP***
- ［割付：セキュリティ属性の最小数及び種別］：***少なくとも表 5-10 のセキュリティ属性と種別に従い実施する。***

表 5-10：セキュリティ属性の種別

セキュリティ属性	種別
オペレータ種別	サブジェクトのセキュリティ属性
証明書状態属性	証明書情報のセキュリティ属性
鍵状態属性	鍵情報(PKCS#12)のセキュリティ属性
	鍵情報(PIN)のセキュリティ属性
証明書削除状態属性	証明書情報のセキュリティ属性

FDP_IFF.1.2

TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない：[割付：*各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*] 。

- [割付：*各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]：***表 5-11 に示すサブジェクトの操作において、情報のセキュリティ属性及び許可されるサブジェクトのセキュリティ属性が表 5-11 に示すものである場合、表 5-11 に示す情報の許可されるサブジェクトへの情報フローを許可する。***

表 5-11：許可される情報フロー規則

操作するサブジェクト	操作するサブジェクトのセキュリティ属性	情報	情報のセキュリティ属性	操作前の情報のセキュリティ属性の状態	操作	操作後の情報のセキュリティ属性の状態	許可されるサブジェクト	許可されるサブジェクトのセキュリティ属性
RA 操作者プロセス	オペレータ種別が RAO1	証明書情報	証明書状態	RAO1 発行審査待ち	発行承認	RAO2 発行審査待ち	RA 操作者プロセス	オペレータ種別が RAO2
						CA 発行審査待ち	RA サーバプロセス	オペレータ種別が RA
					発行拒否	RAO1 発行拒否	なし ※1	なし
				RAO1 失効審査待ち	失効承認	RAO2 失効審査待ち	RA 操作者プロセス	オペレータ種別が RAO2
						CA 失効審査待ち	RA サーバプロセス	オペレータ種別が RA
					失効拒否	発行	RA 操作者プロセス	オペレータ種別が RAO2
			証明書削除状態	削除要求前	削除要求	RAO1 削除審査待ち	RA 操作者プロセス	オペレータ種別が RAO1
						RAO2 削除審査待ち	RA 操作者プロセス	オペレータ種別が RAO2
						削除待ち	RA サーバプロセス	オペレータ種別が RA
				RAO1 削除審査待ち	削除承認	RAO2 削除審査待ち	RA 操作者プロセス	オペレータ種別が RAO2
						削除待ち	RA サーバプロセス	オペレータ種別が RA
					削除拒否	削除要求前	RA 操作者プロセス	オペレータ種別が RAO1
								オペレータ種別が RAO2
		鍵状態情報 (PKCS#12)	鍵状態	鍵取得要求前	取得要求	RAO1 取得待ち	RA 操作者プロセス	オペレータ種別が RAO1
				RAO1 取得待ち	取得	鍵取得済み	RA 操作者プロセス	オペレータ種別が KRO1
								オペレータ種別が KRO2
		鍵状態情報 (PIN)	鍵状態	鍵取得要求前	取得要求	RAO2 取得待ち	RA 操作者プロセス	オペレータ種別が RAO2

操作するサブジェクト	操作するサブジェクトのセキュリティ属性	情報	情報のセキュリティ属性	操作前の情報のセキュリティ属性の状態	操作	操作後の情報のセキュリティ属性の状態	許可されるサブジェクト	許可されるサブジェクトのセキュリティ属性
RA 操作者プロセス	オペレータ種別がRAO2	証明書情報	証明書状態	発行申請前	発行申請	RAO1発行審査待ち	RA 操作者プロセス	オペレータ種別がRAO1
						RAO2発行審査待ち	RA 操作者プロセス	オペレータ種別がRAO2
						CA 発行審査待ち	RA サーバプロセス	オペレータ種別がRA
				RAO2発行審査待ち	発行承認	RAO1発行審査待ち	RA 操作者プロセス	オペレータ種別がRAO1
						CA 発行審査待ち	RA サーバプロセス	オペレータ種別がRA
					発行拒否	RAO2発行拒否	なし ※1	なし
				発行	失効要求	RAO1失効審査待ち	RA 操作者プロセス	オペレータ種別がRAO1
						CA 失効審査待ち	RA サーバプロセス	オペレータ種別がRA
				RAO2失効審査待ち	失効承認	RAO1失効審査待ち	RA 操作者プロセス	オペレータ種別がRAO1
						CA 失効審査待ち	RA サーバプロセス	オペレータ種別がRA
					失効拒否	発行	RA 操作者プロセス	オペレータ種別がRAO2
			証明書削除状態	削除要求前	削除要求	RAO1削除審査待ち	RA 操作者プロセス	オペレータ種別がRAO1
						RAO2削除審査待ち	RA 操作者プロセス	オペレータ種別がRAO2
						削除待ち	RA サーバプロセス	オペレータ種別がRA
				RAO2削除審査待ち	削除承認	RAO1削除審査待ち	RA 操作者プロセス	オペレータ種別がRAO1
						削除待ち	RA サーバプロセス	オペレータ種別がRA
					削除拒否	削除要求前	RA 操作者プロセス	オペレータ種別がRAO1
								オペレータ種別がRAO1
		鍵状態情報(PKCS#12)	鍵状態	鍵取得要求前	取得要求	RAO1取得待ち	RA 操作者プロセス	オペレータ種別がRAO1
		鍵状態情報(PIN)	鍵状態	鍵取得要求前	取得要求	RAO2取得待ち	RA 操作者プロセス	オペレータ種別がRAO2
				RAO2取得待ち	取得	鍵取得済み	RA 操作者プロセス	オペレータ種別がKRO1
								オペレータ種別がKRO2

操作するサブジェクト	操作するサブジェクトのセキュリティ属性	情報	情報のセキュリティ属性	操作前の情報のセキュリティ属性の状態	操作	操作後の情報のセキュリティ属性の状態	許可されるサブジェクト	許可されるサブジェクトのセキュリティ属性
RA 操作者プロセス	オペレータ種別が KRO1	鍵状態情報(PKCS#12)	鍵状態	鍵取得済み	取得要求	KRO1 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO1
						KRO2 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO2
				KRO1 取得審査待ち	取得承認	KRO1 取得待ち	RA 操作者プロセス	オペレータ種別が KRO1
						KRO2 審査取得待ち	RA 操作者プロセス	オペレータ種別が KRO2
					取得拒否	鍵取得済み	RA 操作者プロセス	オペレータ種別が KRO1
								オペレータ種別が KRO2
				KRO1 取得待ち	取得	鍵取得済み	RA 操作者プロセス	オペレータ種別が KRO1
								オペレータ種別が KRO2
		鍵状態情報(PIN)	鍵状態	鍵取得済み	取得要求	KRO1 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO1
						KRO2 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO2
				KRO1 取得審査待ち	取得承認	KRO2 取得待ち	RA 操作者プロセス	オペレータ種別が KRO2
					取得拒否	鍵取得済み	RA 操作者プロセス	オペレータ種別が KRO1
								オペレータ種別が KRO2
RA 操作者プロセス	オペレータ種別が KRO2	鍵状態情報(PKCS#12)	鍵状態	鍵取得済み	取得要求	KRO1 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO1
						KRO2 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO2
				KRO2 取得審査待ち	取得承認	KRO1 取得待ち	RA 操作者プロセス	オペレータ種別が KRO1
					取得拒否	鍵取得済み	RA 操作者プロセス	オペレータ種別が KRO1
								オペレータ種別が KRO2
		鍵状態情報(PIN)	鍵状態	鍵取得済み	取得要求	KRO1 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO1
						KRO2 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO2
				KRO2 取得審査待ち	取得承認	KRO2 取得待ち	RA 操作者プロセス	オペレータ種別が KRO2
						KRO1 取得審査待ち	RA 操作者プロセス	オペレータ種別が KRO1
					取得拒否	取得済み	RA 操作者プロセス	オペレータ種別が KRO1
								オペレータ種別が KRO2
				KRO2 取得待ち	取得	取得済み	RA 操作者プロセス	オペレータ種別が KRO1
								オペレータ種別が KRO2

操作するサブジェクト	操作するサブジェクトのセキュリティ属性	情報	情報のセキュリティ属性	操作前の情報のセキュリティ属性の状態	操作	操作後の情報のセキュリティ属性の状態	許可されるサブジェクト	許可されるサブジェクトのセキュリティ属性
RA サーバプロセス	オペレータ種別が RA	証明書情報	証明書状態	CA 発行審査待ち	発行	発行	RA 操作者プロセス	オペレータ種別が RAO1
								オペレータ種別が RAO2
						発行失敗	なし ※1	なし
				CA 失効待ち	失効	失効	なし ※1	なし
						CA 失効拒否	なし ※1	なし
			証明書削除状態	削除待ち	削除	なし	なし ※1	なし
		鍵状態情報 (PKCS#12)	鍵状態	なし	生成	鍵取得要求前	RA 操作者プロセス	オペレータ種別が RAO1
								オペレータ種別が RAO2
		鍵状態情報 (PIN)	鍵状態	なし	生成	鍵取得要求前	RA 操作者プロセス	オペレータ種別が RAO1
								オペレータ種別が RAO2

(※1) 証明書状態が「RAO1 発行拒否」、「RAO2 発行拒否」、「発行失敗」、「失効」、「CA 失効拒否」のいずれかの場合、証明書状態は他の状態に遷移せず、証明書状態の更新はどのサブジェクトに対しても許可されない。

FDP_IFF.1.3
TSFは、[割付:*追加の情報フロー制御SFP 規則*]を実施しなければならない。

- [割付：*追加の情報フロー制御 SFP 規則*]：***なし***

FDP_IFF.1.4
TSFは、以下の [割付：*追加のSFP 能力のリスト*] を提供しなければならない。

- [割付：*追加の SFP 能力のリスト*]：***なし***

FDP_IFF.1.5
TSF は、以下の規則に基づいて、情報フロー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、明示的に情報フローを承認する規則*] 。

- [割付：*セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]：***なし***

FDP_IFF.1.6
TSF は、次の規則に基づいて、情報フロー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、明示的に情報フローを拒否する規則*] 。

- [割付：*セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]：***なし***

依存性： FDP_IFC.1 サブセット情報フロー制御
FMT_MSA.3 静的属性初期化

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）

下位階層： なし

FDP_ITC.1.1

TSF は、SFP に従って制御され、TSC 外から***RA操作者証明書の発行申請データ、及びCMPサーバ・クライアントの鍵・証明書***をインポートするときは、[割付：*アクセス制御**SFP** 及び/または情報フロー制御**SFP***]を実施しなければならない。

- [割付：*アクセス制御 **SFP** 及び/または情報フロー制御 **SFP***]：***オペレータアクセス制御 SFP***

FDP_ITC.1.2

TSF は、TSC 外からインポートされるとき、***RA操作者証明書の発行申請データ、及びCMPサーバ・クライアントの鍵・証明書***に関連付けられたいかなるセキュリティ属性も無視しなければならない。

FDP_ITC1.3

TSF は、SFP に従って制御され、TSC 外から***RA操作者証明書の発行申請データ、及びCMPサーバ・クライアントの鍵・証明書***をインポートするときは、以下の規則を実施しなければならない：[割付： *追加のインポート制御規則*]。

- [割付：*追加のインポート制御規則*]：***なし***

依存性： [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.3 静的属性初期化

FDP_ITT.1	（基本内部転送保護）

下位階層： なし

FDP_ITT.1.1

TSF は、利用者データがTOEの物理的に分離されたパート間を転送される場合、その［選択：*暴露、改変、使用不可*］を防ぐための [割付：*アクセス制御 SFP(s) 及び/または情報フロー制御SFP(s)*]を実施しなければならない。

- ［選択：*暴露、改変、使用不可*］：***暴露、改変***
- [割付：*アクセス制御 SFP(s) 及び/または情報フロー制御 SFP(s)*]：***オペレータアクセス制御 SFP***

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

(4) 識別と認証（FIA）

表 5-12：FIA 機能要件

セキュリティ機能要件		コンポーネント
秘密についての仕様	秘密の検証	FIA_SOS.1[1]
		FIA_SOS.1[2]
		FIA_SOS.1[3]
	TSF 秘密生成	FIA_SOS.2
利用者認証	認証のタイミング	FIA_UAU.1
	アクション前の利用者認証	FIA_UAU.2
利用者識別	識別のタイミング	FIA_UID.1
	アクション前の利用者識別	FIA_UID.2

FIA_SOS.1[1] （秘密の検証）

下位階層： なし

FIA_SOS.1.1

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。

- ［割付：*定義された品質尺度*］：***パスワード、シードは ASCII コードの 0x20～0x7E を 4 文字以上 8 文字以下***

依存性： なし

FIA_SOS.1[2]	（秘密の検証）

下位階層： なし

FIA_SOS.1.1

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。

- ［割付：*定義された品質尺度*］：***パスワードは ASCII コードの 0x20～0x7E を 6 文字以上 14 文字以下***

依存性： なし

FIA_SOS.1[3]	（秘密の検証）

下位階層： なし

FIA_SOS.1.1

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。

［割付：*定義された品質尺度*］：***パスワードは 10 バイトの乱数***

-

依存性： なし

FIA_SOS.2　　（TSF 秘密生成）

下位階層：　　なし

FIA_SOS.2.1

TSF は、［割付：*定義された品質尺度*］に合致する秘密を生成するメカニズムを提供しなければならない。

［割付：*定義された品質尺度*］：***15 バイトの乱数***

FIA_SOS.2.2

TSF は、［割付：*TSF 機能のリスト*］に対し、TSF 生成の秘密の使用を実施できなければならない。

- ［割付：*TSF 機能のリスト*］：
  RA セットアップ機能の RA 動作環境情報設定機能

依存性：　　なし

FIA_UAU.1　　（認証のタイミング）

下位階層：　　なし

FIA_UAU.1.1

TSF は、利用者が認証される前に利用者を代行して行われる[割付：*TSF 調停アクションのリスト*]を許可しなければならない。

- ［割付：*TSF 調停アクションのリスト*］：
  RA オペレータ機能の環境設定機能

FIA_UAU.1.2

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

依存性：　　FIA_UID.1 識別のタイミング

FIA_UAU.2	（アクション前の利用者認証）

下位階層： FIA_UAU.1

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

依存性： FIA_UID.1 識別のタイミング

FIA_UID.1	（識別のタイミング）

下位階層： なし

FIA_UID.1.1
TSF は、利用者が識別される前に利用者を代行して実行される[割付：*TSF 調停アクションのリスト*]を許可しなければならない。

- ［割付：*TSF 調停アクションのリスト*］：
  RA オペレータ機能の環境設定機能

FIA_UID.1.2
TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

依存性： なし

FIA_UID.2	（アクション前の利用者識別）

下位階層： FIA_UID.1

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

依存性： なし

(5)　セキュリティ管理（FMT）

表 5-13：FMT 機能要件

セキュリティ機能要件		コンポーネント
セキュリティ属性の管理	セキュリティ属性の管理	FMT_MSA.1[1]
		FMT_MSA.1[2]
	セキュアなセキュリティ属性	FMT_MSA.2
	静的属性初期化	FMT_MSA.3[1]
		FMT_MSA.3[2]
		FMT_MSA.3[3]
		FMT_MSA.3[4]
TSF データの管理	TSF データの管理	FMT_MTD.1
セキュリティ管理役割	セキュリティ役割	FMT_SMR.1

FMT_MSA.1[1]　　（セキュリティ属性の管理）

下位階層：　　なし

FMT_MSA.1.1

TSF は、セキュリティ属性［割付：*セキュリティ属性のリスト*］に対し［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］をする能力を［割付：*許可された識別された役割*］に制限するために［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］を実施しなければならない。

- ［割付：*セキュリティ属性のリスト*］：***RA 操作者のオペレータ種別、RA 操作者のオペレータ ID、サイト ID、CAID***
- ［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］：***改変、削除***、［割付：*その他の操作*］：***作成、設定***
- ［割付：*許可された識別された役割*］：***RA 管理者***
- ［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］：***オペレータアクセス制御 SFP***

依存性：　　[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.1[2]　　（セキュリティ属性の管理）

下位階層：　　なし

FMT_MSA.1.1

TSF は、セキュリティ属性［割付：*セキュリティ属性のリスト*］に対し［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］をする能力を［割付：*許可された識別された役割*］に制限するために［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］を実施しなければならない。

- ［割付：*セキュリティ属性のリスト*］：***証明書状態属性、鍵状態属性、証明書削除状態属性***
- ［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］：***改変、削除***、［割付：*その他の操作*］：***作成***
- ［割付：*許可された識別された役割*］：***RA 操作者***
- ［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］：***状態フロー制御 SFP***

依存性：　　[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.2	（セキュアなセキュリティ属性）

下位階層： なし

FMT_MSA.2.1

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

依存性：

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

FMT_MSA.3[1]　　（静的属性初期化）

下位階層：　　なし

FMT_MSA.3.1

TSF は、その SFP を実施するために使われる***オペレータ種別・サイト ID***として、［選択：*制限的、許可的、その他の特性*］デフォルト値を与える［割付：*アクセス制御 **SFP**、情報フロー制御 **SFP***］を実施しなければならない。

- ［選択：*制限的、許可的、その他の特性*］：***制限的***
- ［割付：*アクセス制御 **SFP**、情報フロー制御 **SFP***］：***オペレータアクセス制御 SFP***

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、［割付：*許可された識別された役割*］が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

- ［割付：*許可された識別された役割*］：***なし***

依存性：　　FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MSA.3[2]　　（静的属性初期化）

下位階層：　　なし

FMT_MSA.3.1

TSF は、その SFP を実施するために使われる***証明書状態属性・鍵状態属性・証明書削除状態属性***として、［選択：*制限的、許可的、その他の特性*］デフォルト値を与える［割付：*アクセス制御 **SFP**、情報フロー制御 **SFP***］を実施しなければならない。

- ［選択：*制限的、許可的、その他の特性*］：***制限的***
- ［割付：*アクセス制御 **SFP**、情報フロー制御 **SFP***］：***状態フロー制御 SFP***

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、［割付：*許可された識別された役割*］が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

- ［割付：*許可された識別された役割*］：***なし***

依存性：　　FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MSA.3[3]	（静的属性初期化）

下位階層： なし

FMT_MSA.3.1

TSF は、その SFP を実施するために使われる***鍵番号***として、［選択：*制限的、許可的、その他の特性*］***1 から始まるシーケンシャルな番号***を与える［割付：*アクセス制御 SFP、情報フロー制御 SFP*］を実施しなければならない。

- ［選択：*制限的、許可的、その他の特性*］：***その他の特性***
- ［割付：*アクセス制御 SFP、情報フロー制御 SFP*］：***オペレータアクセス制御 SFP***

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、［割付：*許可された識別された役割*］が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

- ［割付：*許可された識別された役割*］：***なし***

依存性： FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MSA.3[4]	（静的属性初期化）

下位階層： なし

FMT_MSA.3.1

TSF は、その SFP を実施するために使われる***オペレータ種別***として、［選択：*制限的*、*許可的*、*その他の特性*］デフォルト値を与える［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］を実施しなければならない。

- ［選択：*制限的*、*許可的*、*その他の特性*］：***制限的***
- ［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］：***オペレータアクセス制御 SFP***

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、［割付：*許可された識別された役割*］が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

- ［割付：*許可された識別された役割*］：***なし***

依存性： FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MTD.1　　（TSF データの管理）

下位階層：　　なし

FMT_MTD.1.1

TSF は、［割付：*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*］：***表 5-14 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*］］：***表 5-14 の「操作」***
- ［割付：*許可された識別された役割*］：***表 5-14 の「役割」***

表 5-14：TSF データの管理

TSF データ	操作	役割
オペレータ証明書	その他の操作：取得	RA 操作者((RAO1、RAO2、KRO1、KRO2))
監査ログ	削除、問い合わせ、その他の操作：検証	監査者(AUDITOR)
	問い合わせ	RA 操作者(RAO1、RAO2、KRO1、KRO2)
CA 情報	改変、削除、その他の操作：登録	RA 管理者(CONSOLE)
サイト情報	改変、削除、その他の操作：登録	RA 管理者(CONSOLE)
オペレータ情報	改変、削除、その他の操作：登録	RA 管理者(CONSOLE)
信頼する CA 証明書	削除、その他の操作：登録	RA 管理者(CONSOLE)

依存性：　　FMT_SMR.1 セキュリティ役割

FMT_SMR.1　　（セキュリティ役割）

下位階層： なし

FMT_SMR.1.1
TSF は、役割［割付：*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*］：**RA 管理者(CONSOLE)、RA 操作者（RAO1,RAO2,KRO1,KRO2）、監査者(AUDITOR)**

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

依存性： FMT_UID.1 識別のタイミング

(6) TSF の保護（FPT）

表 5-15：FPT 機能要件

セキュリティ機能要件		コンポーネント
リファレンス調停	TSP の非バイパス性	FPT_RVM.1
TSF の保護	TOE 内 TSF データ転送	FPT_ITT.1

FPT_RVM.1　（TSP の非バイパス性）

下位階層： なし

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

依存性： なし

FPT_ITT.1　（基本 TSF 内データ転送保護）

下位階層： なし

FPT_ITT.1.1
TSF は、TSF データがTOE の別々のパーツ間で送られる場合、TSFデータを［選択：*暴露*、*改変*］から保護しなければならない。

- ［選択：*暴露*、*改変*］：***暴露、改変***

依存性： なし

5.1.2 TOE セキュリティ機能強度

この TOE の最小機能強度レベルは SOF-基本である。確率的または順列的メカニズムを適用するのは、FIA_SOS.1[1]、FIA_SOS.1[2]、FIA_SOS.1[3]、FCS_COP.1[1]、FCS_COP.1[2]、FCS_COP.1[3]、FCS_COP.1[4]である。このうち TOE 機能強度主張が対象とするものはパスワードメカニズム、暗号化シードメカニズムであり、本 ST における対象コンポーネントは FIA_SOS.1[1]、FIA_SOS.1[2]、FIA_SOS.1[3]である。なお、暗号アルゴリズムを利用するコンポーネントの FCS_COP.1[1]、FCS_COP.1[2]、FCS_COP.1[3]、FCS_COP.1[4]は、TOE 機能強度主張の対象外である。

5.1.3 TOE セキュリティ保証要件

TOE は、商用システムの中で利用される。商用システムとして十分なレベルである EAL3 を品質保証レベルとする。

本 ST では表 5-16 に示すように EAL3 で定められた保証要件のセット、及び暗号サポートの機能要件の依存性を満たすために追加する ADV_SPM.1 に従う。

表 5-16：EAL3 追加の保証要件コンポーネント

TOE セキュリティ保証要件		コンポーネント	EAL3	追加
構成管理	CM 能力	ACM_CAP.3	●	
	CM 範囲	ACM_SCP.1	●	
配付と運用	配付	ADO_DEL.1	●	
	設置・生成・及び立上げ	ADO_IGS.1	●	
開発	機能仕様	ADV_FSP.1	●	
	上位レベル設計	ADV_HLD.2	●	
	表現対応	ADV_RCR.1	●	
	セキュリティ方針モデル化	ADV_SPM.1		●
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	●	
	利用者ガイダンス	AGD_USR.1	●	
ライフサイクルサポート	開発セキュリティ	ALC_DVS.1	●	
テスト	カバレージ	ATE_COV.2	●	
	深さ	ATE_DPT.1	●	
	機能テスト	ATE_FUN.1	●	
	独立テスト	ATE_IND.2	●	
脆弱性評定	誤使用	AVA_MSU.1	●	
	TOE セキュリティ機能強度	AVA_SOF.1	●	
	脆弱性分析	AVA_VLA.1	●	

5.2 IT 環境に対するセキュリティ要件

IT 環境のセキュリティ機能要件は、以下に分類される。

(1) 利用者データ保護 （FDP クラス）
(2) 識別と認証 （FIA クラス）
(3) セキュリティ管理 （FMT クラス）
(4) TSF の保護 （FPT クラス）

(1) 利用者データ保護（FDP）

表 5-17：FDP 機能要件

セキュリティ機能要件		コンポーネント
アクセス制御方針	サブセットアクセス制御	FDP_ACC.1[E]
アクセス制御機能	セキュリティ属性による アクセス制御	FDP_ACF.1[E]

FDP_ACC.1[E]　　（サブセットアクセス制御）

下位階層：　　なし

FDP_ACC.1.1

OS 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*］：

  サブジェクト
  OS の利用者プロセス

  オブジェクト
  ファイル

  サブジェクトとオブジェクト間の操作
  改変
  削除
  読み込み

- ［割付：*アクセス制御 **SFP***］：***OS アクセス制御 SFP***

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[E]　　（サブセットアクセス制御）

下位階層：　　なし

FDP_ACF.1.1

OS は、[割付：*セキュリティ属性、名前付けされたセキュリティ属性のグループ*] 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：*セキュリティ属性、名前付けされたセキュリティ属性のグループ*]
  ：***OS の利用者 ID***
- [割付：*アクセス制御 **SFP***]：***OS アクセス制御 SFP***

FDP_ACF.1.2

OS 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*]：
  表 5-18 の制御されたサブジェクトが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。

表 5-18：OS アクセス規則

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
TOE 内のファイルへのアクセス権を持つ OS の利用者プロセス	OS が管理する TOE 内のファイル	改変
		削除
		読み込み

FDP_ACF.1.3

OS 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に対するサブジェクトの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に対するサブジェクトのアクセスを明示的に承認する規則*］：***なし***

FDP_ACF.1.4

OS 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

(2) 識別と認証（FIA）

表 5-19：FIA 機能要件

セキュリティ機能要件		コンポーネント
秘密についての仕様	秘密の検証	FIA_SOS.1[E1]
		FIA_SOS.1[E2]
利用者認証	認証のタイミング	FIA_UAU.1[E]
	アクション前の利用者認証	FIA_UAU.2[E]
利用者識別	識別のタイミング	FIA_UID.1[E]
	アクション前の利用者識別	FIA_UID.2[E]

FIA_SOS.1[E1]　（秘密の検証）

下位階層：　なし

FIA_SOS.1.1

IC カードは、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。

- ［割付：*定義された品質尺度*］：***パスワードは 4 文字以上***

依存性：　なし

FIA_SOS.1[E2]　（秘密の検証）

下位階層：　なし

FIA_SOS.1.1

OS 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。

- ［割付：*定義された品質尺度*］：***Windows、Solaris OE ともパスワードは 6 文字以上***

依存性：　なし

FIA_UAU.1[E]	（認証のタイミング）

下位階層： なし

FIA_UAU.1.1

OS は、利用者が認証される前に利用者を代行して行われる[割付：*TSF 調停アクションのリスト*]を許可しなければならない。

- ［割付：*TSF 調停アクションのリスト*］：
  Windows：ヘルプ表示
  Solaris OE：言語選択、セッション選択、ログイン方法の選択、ヘルプ表示

FIA_UAU.1.2

OS 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.2[E]	（アクション前の利用者認証）

下位階層： FIA_UAU.1

FIA_UAU.2.1

IC カードは、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認証することを要求しなければならない。

依存性： FIA_UID.1 識別のタイミング

FIA_UID.1[E]	（識別のタイミング）

下位階層： なし

FIA_UID.1.1

OS は、利用者が識別される前に利用者を代行して実行される[割付:*TSF 調停アクションのリスト*]を許可しなければならない。

- ［割付：*TSF 調停アクションのリスト*］：
  Windows：ヘルプ表示
  Solaris OE：言語選択、セッション選択、ログイン方法の選択、ヘルプ表示

FIA_UID.1.2

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

依存性： なし

FIA_UID.2[E]	（アクション前の利用者識別）

下位階層： FIA_UID.1

FIA_UID.2.1

IC カードは、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

(3) セキュリティ管理（FMT）

表 5-20：FMT 機能要件

セキュリティ機能要件		コンポーネント
セキュリティ属性の管理	セキュリティ属性の管理	FMT_MSA.1[E1]
		FMT_MSA.1[E2]
		FMT_MSA.1[E3]
	静的属性初期化	FMT_MSA.3[E]
TSF データの管理	TSF データの管理	FMT_MTD.1[E]
セキュリティ管理役割	セキュリティ役割	FMT_SMR.1[E]

FMT_MSA.1[E1]　（セキュリティ属性の管理）

下位階層：　なし

FMT_MSA.1.1

OS は、セキュリティ属性［割付：*セキュリティ属性のリスト*］に対し［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］をする能力を［割付：*許可された識別された役割*］に制限するために［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］を実施しなければならない。

- ［割付：*セキュリティ属性のリスト*］：***OS の利用者 ID***
- ［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］：***問い合わせ、改変、削除***、［割付：*その他の操作*］：***なし***
- ［割付：*許可された識別された役割*］：***TOE 内のファイルに対するアクセス権を持つ OS の利用者***
- ［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］：***OS アクセス制御 SFP***

依存性：　[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.1[E2]　　（セキュリティ属性の管理）

下位階層：　　なし

FMT_MSA.1.1

OS は、セキュリティ属性［割付：*セキュリティ属性のリスト*］に対し［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］をする能力を［割付：*許可された識別された役割*］に制限するために［割付：*アクセス制御 **SFP***、*情報フロー制御 **SFP***］を実施しなければならない。

- ［割付：*セキュリティ属性のリスト*］：***鍵番号***
- ［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］：［割付：*その他の操作*］：***作成***
- ［割付：*許可された識別された役割*］：***システム管理者***
- ［割付：*アクセス制御 **SFP***、*情報フロー制御 **SFP***］：***OS アクセス制御 SFP***

依存性：　　[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.1[E3]　　（セキュリティ属性の管理）

下位階層：　　なし

FMT_MSA.1.1

OS は、セキュリティ属性［割付：*セキュリティ属性のリスト*］に対し［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］をする能力を［割付：*許可された識別された役割*］に制限するために［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］を実施しなければならない。

- ［割付：*セキュリティ属性のリスト*］：***RA 管理者・監査者のオペレータ種別、RA 管理者・監査者のオペレータ ID***
- ［選択：*デフォルト値変更*、*問い合わせ*、*改変*、*削除*、［割付：*その他の操作*］］：***改変、削除***、［割付：*その他の操作*］：***作成***
- ［割付：*許可された識別された役割*］：***システム管理者***
- ［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］：***OS アクセス制御 SFP***

依存性：　　[FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティ役割

FMT_MSA.3[E]　　（静的属性初期化）

下位階層：　　なし

FMT_MSA.3.1

OS は、その SFP を実施するために使われるセキュリティ属性として、［選択：*制限的*、*許可的*、*その他の特性*］デフォルト値を与える［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］を実施しなければならない。

- ［選択：*制限的*、*許可的*、*その他の特性*］：***制限的***
- ［割付：*アクセス制御 SFP*、*情報フロー制御 SFP*］：***OS アクセス制御 SFP***

FMT_MSA.3.2

OS は、オブジェクトや情報が生成されるとき、［割付：*許可された識別された役割*］が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

- ［割付：*許可された識別された役割*］：***なし***

依存性： FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MTD.1[E]	（TSF データの管理）

下位階層： なし

FMT_MTD.1.1

OS 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*］：***表 5-21 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*］］：***表 5-21 の「操作」***
- ［割付：*許可された識別された役割*］：***表 5-21 の「役割」***

表 5-21：TSF データの管理 [IT 環境]

TSF データ	操作	役割
RA 動作環境情報	改変、削除、消去、読み込み	TOE 内のファイルに対するアクセス権を持つ OS の利用者

依存性： FMT_SMR.1 セキュリティ役割

FMT_SMR.1[E]　　（セキュリティ役割）

下位階層：　　なし

FMT_SMR.1.1

OS 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*］
  ：***TOE 内のファイルに対するアクセス権を持つ OS の利用者***

FMT_SMR.1.2

OS は、利用者を役割に関連づけなければならない。

依存性：　　FIA_UID.1 識別のタイミング

(4) TSF の保護（FPT）

表 5-22：FPT 機能要件

セキュリティ機能要件		コンポーネント
タイムスタンプ	高信頼タイムスタンプ	FPT_STM.1[E]
ドメイン分離	TSF ドメイン分離	FPT_SEP.1[E]

FPT_STM.1[E]	高信頼タイムスタンプ

下位階層： なし

FPT_STM.1.1
OS は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性： なし

FPT_SEP.1[E]	TSF ドメイン分離

下位階層： なし

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

FPT_SEP.1.2
OS は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性： なし

6 TOE 要約仕様

TOE のセキュリティ機能、及び保証手段について記述する。

6.1 TOE セキュリティ機能

TOE のセキュリティ機能の一覧を表 6-1 に示す。

表 6-1：TOE セキュリティ機能

機能	説明	コンポーネント
監査機能	監査ロギング機能	F.AUDIT.1
	監査ログ参照機能	F.AUDIT.2
	監査ログ検証機能	F.AUDIT.3
	監査ログ削除機能	F.AUDIT.4
オペレータ識別認証機能	証明書、またはユーザ ID／パスワードによりオペレータを識別認証する機能	F.OPERATOR_AUTH
CA 識別認証機能	TOE が CA に対して証明書要求を行うとき、証明書による識別認証を行う機能	F.CA_AUTH
アクセス制御機能	オペレータのアクセス権限を管理する機能	F.ACCESS_CONTROL
状態フロー制御機能	鍵・証明書の状態遷移を管理する機能	F.STATUS_FLOW_CONTORL
暗号化機能	TSC 内の鍵、パスワード、監査ログ等を暗号化する機能	F.CIPHER.1
	パスワードのメカニズムに関する機能	F.CIPHER.2
	暗号鍵シードのメカニズムに関する機能	F.CIPHER.3
暗号通信機能	TOE を構成するコンポーネント間の通信を暗号化する機能	F.SSL
管理機能	セキュリティ属性を管理する機能	F.ADMIN

TOE のセキュリティ機能と TOE セキュリティ機能要件との適合性を表 6-2 に示す。TOE 要約仕様により、各機能要件が採用されることを表している。

表 6-2：TOE 要約仕様の関係

TOE 要約仕様 / セキュリティ機能要件	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4	F.OPERATOR_AUTH	F.CA_AUTH	F.ACCESS_CONTROL	F.STATUS_FLOW_CONTROL	F.CIPHER.1	F.CIPHER.2	F.CIPHER.3	F.SSL	F.ADMIN
FAU_GEN.1	●												
FAU_GEN.2	●												
FAU_SAR.1		●											
FAU_SAR.2		●											
FAU_SAR.3		●											
FAU_STG.1			●										
FCS_CKM.1									●			●	
FCS_CKM.4					●	●			●			●	
FCS_COP.1[1]	●		●										
FCS_COP.1[2]					●								
FCS_COP.1[3]						●							
FCS_COP.1[4]									●			●	
FDP_ACC.1							●						
FDP_ACF.1							●						
FDP_IFC.1								●					
FDP_IFF.1								●					
FDP_ITC.1					●	●							
FDP_ITT.1												●	

TOE 要約仕様 / セキュリティ機能要件	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4	F.OPERATOR_AUTH	F.CA_AUTH	F.ACCESS_CONTROL	F.STATUS_FLOW_CONTROL	F.CIPHER.1	F.CIPHER.2	F.CIPHER.3	F.SSL	F.ADMIN
FIA_SOS.1[1]										●	●		
FIA_SOS.1[2]										●			
FIA_SOS.1[3]										●			
FIA_SOS.2											●		
FIA_UAU.1					●								
FIA_UAU.2						●							
FIA_UID.1					●								
FIA_UID.2						●						●	
FMT_MSA.1[1]													●
FMT_MSA.1[2]								●					
FMT_MSA.2	●		●		●	●			●				
FMT_MSA.3[1]													●
FMT_MSA.3[2]								●					
FMT_MSA.3[3]													●
FMT_MSA.3[4]													●
FMT_MTD.1		●	●	●									
FMT_SMR.1					●		●						
FPT_ITT.1												●	

TOE 要約仕様 / セキュリティ機能要件	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4	F.OPERATOR_AUTH	F.CA_AUTH	F.ACCESS_CONTROL	F.STATUS_FLOW_CONTROL	F.CIPHER.1	F.CIPHER.2	F.CIPHER.3	F.SSL	F.ADMIN
FDP_ACC.1[E]	IT 環境の機能要件により実現される。												
FDP_ACF.1[E]													
FIA_SOS.1[E1]													
FIA_SOS.1[E2]													
FIA_UAU.1[E]													
FIA_UAU.2[E]													
FIA_UID.1[E]													
FIA_UID.2[E]													
FMT_MSA.1[E1]													
FMT_MSA.1[E2]													
FMT_MSA.1[E3]													
FMT_MSA.3[E]													
FMT_MTD.1[E]													
FMT_SMR.1[E]													
FPT_SEP.1[E]													
FPT_STM.1[E]													

6.1.1 F.AUDIT（監査機能）

(1) F.AUDIT.1（監査ロギング機能）

F. AUDIT.1 は、RA サーバで実行された操作の記録を監査ログとして記録する機能である。監査ログの記録は RA サーバの起動時に開始され、停止時に終了する。監査ログの対象事象が発生すると、RA サーバは要求された処理を実行するとともに、監査ログに適切なレコードを出力する。要求に対する処理と監査ログの出力は同一のトランザクション内でアトミックに実行されるため、処理の実行時の監査ログの記録が保証される。なお、監査ログレコードは改変、削除を検出できるように鍵付きハッシュ値を付加する。ハッシュに使用するデータは監査ログに記録されるデータを使用する。鍵付きハッシュのハッシュアルゴリズムは HMAC-SHA1 で、使用する鍵は **F.CIPHER.1** で生成された監査ログ暗号化鍵で鍵のアルゴリズムは RC2、鍵長は 128 ビットである。監査ログ暗号化鍵は鍵番号で管理されており、RA サーバのみアクセスすることができる。

監査ログレコードは表 6-3 に示す情報から構成される。また、監査ログの対象となる事象を表 6-4 に示す。

表 6-3：監査ログに記録される情報

記録される情報	説明
日時	監査ログを記録した日付と時刻
サイト ID	操作が行われたサイトの識別情報
要求番号	操作の対象となった証明書情報の識別番号
オペレータ ID	操作を行ったオペレータ
オペレータ種別	操作を行ったオペレータの種別
結果	操作の結果（成功、または失敗）
アクションコード	行われた操作を示すコード
詳細情報	行われた操作の詳細情報
ログ ID	監査ログ内で一意な連続した番号
署名	日時からログ ID までのデータに対する鍵付きハッシュ値
鍵番号	監査ログ暗号化鍵の番号

表 6-4：監査ログ対象事象

事象	意味
起動	RA サーバが起動された（監査ログ記録開始）
停止	RA サーバが停止された（監査ログ記録終了）
CA 追加	CA 管理情報が追加された
CA 更新	CA 管理情報が更新された
CA 削除	CA 管理情報が削除された
サイト追加	サイト管理情報が追加された
サイト更新	サイト管理情報が更新された
サイト削除	サイト管理情報が削除された
オペレータ追加	オペレータ管理情報が追加された
オペレータ更新	オペレータ管理情報が更新された
オペレータ削除	オペレータ管理情報が削除された
信頼する証明書の追加・削除	信頼する CA 証明書の追加、削除が行われた
オペレータ証明書申請	RA 操作者の証明書の発行申請が行われた
ログイン	オペレータのログインが行われた
ログアウト	オペレータのログアウトが行われた
証明書申請	一般利用者証明書の個別発行申請が行われた
一括証明書申請	一般利用者証明書の一括発行申請が行われた
鍵生成	一般利用者の鍵が生成された
鍵生成失敗	一般利用者の鍵生成に失敗した
証明書発行	証明書の発行が承認された、または証明書が発行された
証明書発行拒否	証明書の発行が拒否された、または証明書の発行に失敗した
鍵暗号化	一般利用者の鍵が暗号化された
鍵暗号化失敗	一般利用者の鍵の暗号化に失敗した
証明書失効	証明書の失効が申請された、証明書の失効が承認された、または証明書が失効された
証明書失効拒否	証明書の失効が拒否された、または証明書の失効に失敗した
鍵回復要求	個別申請された鍵・証明書の取得が要求された
一括鍵回復要求	一括申請された鍵・証明書の取得が要求された
鍵取得承認	PKCS#12 または PIN の取得が承認された
鍵取得拒否	PKCS#12 または PIN の取得が拒否された
鍵取得準備	取得する PKCS#12 または PIN のリストが作成された
PKCS#12 取得	PKCS#12 が取得された
PIN 取得	PIN が取得された

事象	意味
削除要求	鍵・証明書の削除が要求された
削除審査	鍵・証明書の削除が承認された
削除拒否	鍵・証明書の削除が拒否された
削除実行	鍵・証明書が削除された
監査ログ取得	監査ログが取得された
監査ログ検証	監査ログの検証が行われた
監査ログ削除	監査ログが削除された
CRL 取得	CRL が取得された

(2) F.AUDIT.2**（監査ログ参照機能）**

F. AUDIT.2 は、**F. AUDIT.1** で記録された監査ログの内容を参照する機能である。監査ログの参照は、RA コンソール、及び RA オペレータの監査機能を使用して、監査者、及び RA 操作者が行うことができる。監査者は TOE により記録されたすべての監査ログを参照することができ、RA 操作者は自身が属するサイトの監査ログのみ参照できる。また、**F. AUDIT.2** は、監査ログの参照時に、日付・時刻、サイト ID、オペレータ種別、オペレータ ID、要求番号、事象、処理結果により、参照する監査ログを検索する機能を提供する。

(3) F.AUDIT.3**（監査ログ検証機能）**

F. AUDIT.3 は、**F. AUDIT.1** で記録された監査ログの完全性と連続性を検証する機能である。監査ログの検証は、RA コンソールの監査機能を使用して、監査者のみが行うことができる。

監査ログのレコードには、レコード生成時に鍵付きハッシュ値が付加される。これを現在のレコードの鍵付きハッシュ値と比較することにより、レコードの改ざんを検出することができる。鍵付きハッシュのハッシュアルゴリズムは HMAC-SHA1 で、鍵のアルゴリズムは RC2、鍵長は 128 ビットである。使用する鍵は **F.CIPHER.1** で生成された監査ログ暗号化鍵で鍵のアルゴリズムは RC2、鍵長は 128 ビットである。監査ログ暗号化鍵は鍵番号で管理されており、RA サーバのみアクセスすることができる。

これにより監査ログの完全性が検証される。

また、監査ログのレコードには、レコード記録時に監査ログ内で一意な、連続したログ ID が付けられる。監査ログレコードのログ ID の連続性を検査することにより、TOE 外の機能を使用して行われたログレコードの削除を検出することができる。これにより監査ログの連続性が検証される。

(4) F.AUDIT.4**（監査ログ削除機能）**

F. AUDIT.4 は、**F. AUDIT.1** で記録された監査ログを削除する機能である。監査ログの削除は、RA コンソールの監査機能を使用して、監査者のみが行うことができる。

6.1.2 F.OPERATOR_AUTH（オペレータ識別認証機能）

F.OPERATOR_AUTH は、RA コンソール、及び RA オペレータからのログイン要求受け付け時に、RA サーバにより実施されるオペレータの識別認証機能である。識別認証にはユーザ ID／パスワードによる識別認証と、証明書による識別認証とがある。ユーザ ID／パスワードによる識別認証は、RA オペレータのオペレータ登録機能でのみ使用される識別認証方式である。

RA オペレータのオペレータ登録機能を行うには事前に RA コンソールのオペレータ管理機能を実行する必要がある。RA コンソールのオペレータ管理機能を実行することによりオペレータ登録情報が RA 操作者に配付される。RA 操作者は配付されたオペレータ登録情報のユーザ ID／パスワードを使用して RA オペレータのオペレータ登録機能を実行する。RA オペレータのオペレータ登録機能により IC カードで生成された鍵ペアを使用し、RA 操作者の証明書発行申請が行われ、証明書が正常に発行されると、RA サーバはこの証明書をオペレータ証明書として RDBMS にインポートする。この証明書は RA オペレータのオペレータ登録機能の証明書取得要求により、RA オペレータに配付される。オペレータ登録が完了して、RA 操作者の証明書が IC カードに格納されると、それ以降のログイン要求は証明書による識別認証が行われる。

インポートしたオペレータ証明書は、RA コンソール機能のオペレータ管理機能で削除を行うことにより、RDBMS から削除される。オペレータ証明書の鍵はアルゴリズムが RSAwithSHA-1、鍵長は 512,1024,2048bit である。また、オペレータ証明書はオペレータ ID によって識別され **F.ACCESS_CONTROL** によってセキュアに管理される。

オペレータの識別認証を行う前に可能な操作として環境設定機能、オペレータ環境設定機能がある。

ユーザ ID／パスワード、及び証明書による識別認証は、それぞれ以下の方法で行われる。

(1) ユーザ ID／パスワードによる識別認証

- TOE を構成するコンポーネント間の通信は **F.SSL** により SSL で行われるが、ユーザ ID／パスワードによるログインの場合、クライアント認証は行われない。SSL の接続確立時に RA オペレータからユーザ ID／パスワードが RA サーバに送られる。パスワードは **F.CIPHER.2** のオペレータ登録用ログインパスワードを使用する。このパスワードは RA オペレータのオペレータ登録機能により自動的に読み込まれるため、入力する必要はない。RA サーバは、受信したユーザ ID／パスワードを登録されているオペレータのユーザ ID／パスワードと比較し、オペレータの識別認証を行う。一致するユーザ ID／パスワードが登録されている場合、接続要求は受け付けられる。一致するユーザ ID／パスワードが見つからない場合、接続要求は拒絶される。

(2) 証明書による識別認証

- TOE を構成するコンポーネント間の通信は **F.SSL** により SSL で行われる。SSL の接続確立時に証明書が交換されるが、このとき取得される利用者の証明書が RA サーバに登録されているオペレータ証明書と比較される。これにより利用者の識別が行われる。
  一致するオペレータ証明書が登録されている場合、接続要求は受け付けられる。一致する証明書が見つからない場合、接続要求は拒絶される。
- RA サーバは RA サーバで生成された乱数を RA コンソール、または RA オペレータに送信する。
- RA コンソール、または RA オペレータは、RA サーバから送信された乱数に IC カードの機能を使用して署名を行い、署名データを RA サーバに送信する。
- RA サーバは RA コンソール、または RA オペレータから送られた署名データに対して利用者の証明書で検証を行い、利用者が証明書に対応する秘密鍵を所有していることを確認する。これにより利用者の認証が行われる。
  署名の検証に成功すると、RA サーバへのログインが受け付けられる。署名の検証に失敗すると RA サーバへのログインは拒絶される。

6.1.3 F.CA_AUTH（CA 識別認証機能）

F.CA_AUTH は、RA サーバから CA への証明書の発行、失効要求時に、あらかじめ RA サーバに登録された CA との接続だけを許可するための識別認証機能である。CA への証明書の発行・失効の要求時に CA から送信される CMP 応答メッセージに同梱される CMP サーバ証明書が、RA サーバに登録されている CMP サーバ証明書と一致することを確認することにより、CMP サーバを識別する。また、CMP 応答メッセージに付加される署名を CMP サーバの証明書で検証することにより CA を認証する。

CMP サーバの証明書は RA コンソール機能の CA 管理機能でインポートされることにより RDBMS に登録される。インポートは **F. ACCESS_CONTROL** によりアクセス制御された RA 管理者によって行われる。インポートされた CMP サーバの証明書は RA コンソール機能の CA 管理機能の削除により RDBMS から削除される。CMP サーバ証明書の鍵はアルゴリズムが RSAwithSHA-1、鍵長は 512,768,1024,2048bit である。また、CMP サーバ証明書は CAID によって識別され **F.ACCESS_CONTROL** によってセキュアに管理される。

6.1.4 F.ACCESS_CONTROL（アクセス制御機能）

F.ACCESS_CONTROL は、オペレータのアクセス権限を管理する機能である。各オペレータは表 6-5 のオペレータ登録者によって登録される。登録時に指定するオペレータ種別、サイト ID によりデフォルトのアクセス権限が設定される。RA 操作者のサイト ID は登録後に変更可能である。

表 6-5：オペレーター一覧

オペレータ（操作者）	オペレータ種別	サイト ID	オペレータ登録者
RA 管理者	CONSOLE	ADMIN(全サイト)	システム管理者
監査者	AUDITOR		
RA 操作者	RAO1	任意のサイト ID	RA 管理者
	RAO2		
	KRO1		
	KRO2		

RA サーバはオペレータからの要求受け付けに際して、要求を行ったオペレータのオペレータ種別、サイト ID とオペレータアクセス権限テーブルのデータから、要求された操作が許可されるか否かをチェックする。

各オペレータが実行可能な操作を表 6-6 で示す。

表 6-6：オペレータが実行可能な操作

オペレータ種別	実行可能な操作
RA 管理者 (CONSOLE)	CA 情報の登録、改変、削除（CA 情報は CAID により管理する）
	サイト情報の登録、改変、削除（サイト情報はサイト ID により管理する）
	オペレータ情報の登録、改変、削除（オペレータ情報はオペレータ ID により管理する）
	信頼する CA 証明書の登録、削除
	CMP サーバ・クライアントの鍵・証明書の読み込み
監査者 (AUDITOR)	全サイトの監査ログ問い合わせ
	全サイトの監査ログ検証
	全サイトの監査ログ削除
RA 操作者 （RAO1）	自サイトの証明書発行審査
	自サイトの証明書失効要求
	自サイトの証明書失効審査
	自サイトの証明書情報削除要求
	自サイトの証明書情報削除審査
	自サイトの証明書取得
	自サイトの PKCS#12 取得要求
	自サイトの PKCS#12 取得
	自サイトの監査ログ問い合わせ
	自身の RA 操作者証明書発行申請データの読み込み
	自身のオペレータ証明書取得
RA 操作者 （RAO2）	証明書発行申請
	自サイトの証明書発行審査
	自サイトの証明書失効要求
	自サイトの証明書失効審査
	自サイトの証明書情報削除要求
	自サイトの証明書情報削除審査
	自サイトの証明書取得
	自サイトの PKCS#12 取得要求
	自サイトの PIN 取得
	自サイトの監査ログ問い合わせ
	自身の RA 操作者証明書発行申請データの読み込み
	自身のオペレータ証明書取得

オペレータ種別	実行可能な操作
RA 操作者 （KRO1）	自サイトの PKCS#12 取得要求
	自サイトの PKCS#12 取得
	自サイトの PIN 取得審査
	自サイトの監査ログ問い合わせ
	自身の RA 操作者証明書発行申請データの読み込み
	自身のオペレータ証明書取得
RA 操作者 （KRO2）	自サイトの PKCS#12 取得要求
	自サイトの PIN 取得
	自サイトの PKCS#12 取得審査
	自サイトの監査ログ問い合わせ
	自身の RA 操作者証明書発行申請データの読み込み
	自身のオペレータ証明書取得

6.1.5 F.STATUS_FLOW_CONTROL（状態フロー制御機能）

F. STATUS_FLOW_CONTROL は、鍵・証明書の状態遷移を管理する機能である。RA サーバは RA 操作者からの鍵・証明書発行、失効、取得、削除要求を受け、鍵・証明書状態を適切に推移させる。

鍵・証明書状態には証明書状態、鍵状態、証明書削除状態の３つがある。表 6-7 に RA 操作者が状態を遷移させる操作と状態の遷移を示す。操作者は表 6-5 のオペレータ種別で役割を識別される。

状態遷移のライフサイクルは、表 6-7 の状態フロー制御情報に従って制御される。RA 管理者が RA コンソールのサイト管理機能でサイトを登録したときのデフォルトの状態遷移を表 6-8 に示す。状態フロー制御情報は RA 管理者により RA コンソールのサイト管理機能で変更可能である。

表 6-7：状態フロー制御情報

オペレータ種別	状態種別	操作	状態	遷移可能な状態
RAO1	証明書状態	発行承認	RAO1 発行審査待ち	RAO2 発行審査待ち
		発行承認	RAO1 発行審査待ち	CA 発行審査待ち
			CA 発行審査待ち	発行
			CA 発行審査待ち	発行失敗
		発行拒否	RAO1 発行審査待ち	RAO1 発行拒否
		失効承認	RAO1 失効審査待ち	RAO2 失効審査待ち
		失効承認	RAO1 失効審査待ち	CA 失効審査待ち
			CA 失効審査待ち	失効
			CA 失効審査待ち	発行
		失効拒否	RAO1 失効審査待ち	発行
	証明書削除状態	削除要求	削除要求前	RAO1 削除審査待ち
		削除要求	削除要求前	RAO2 削除審査待ち
		削除要求	削除要求前	削除待ち
		削除承認	RAO1 削除審査待ち	RAO2 削除審査待ち
		削除承認	RAO1 削除審査待ち	削除待ち
		削除拒否	RAO1 削除審査待ち	削除要求前
	鍵状態：PKCS#12	取得要求	鍵取得要求前	RAO1 取得待ち
		取得	RAO1 取得待ち	鍵取得済み
	鍵状態：PIN	取得要求	鍵取得要求前	RAO2 取得待ち

オペレータ種別	状態種別	操作	状態	遷移可能な状態
RAO2	証明書状態	個別申請	発行申請前	RAO1 発行審査待ち
		一括申請	発行申請前	RAO1 発行審査待ち
		個別申請	発行申請前	RAO2 発行審査待ち
		一括申請	発行申請前	RAO2 発行審査待ち
		個別申請	発行申請前	CA 発行審査待ち
			CA 発行審査待ち	発行
			CA 発行審査待ち	発行失敗
		一括申請	発行申請前	CA 発行審査待ち
			CA 発行審査待ち	発行
			CA 発行審査待ち	発行失敗
		発行承認	RAO2 発行審査待ち	RAO1 発行審査待ち
		発行承認	RAO2 発行審査待ち	CA 発行審査待ち
			CA 発行審査待ち	発行
			CA 発行審査待ち	発行失敗
		発行拒否	RAO2 発行審査待ち	RAO2 発行拒否
		失効要求	発行	RAO1 失効審査待ち
		失効要求	発行	CA 失効審査待ち
			CA 失効審査待ち	失効
			CA 失効審査待ち	発行
	証明書削除状態	削除要求	削除要求前	RAO1 削除審査待ち
		削除要求	削除要求前	RAO2 削除審査待ち
		削除要求	削除要求前	削除待ち
		削除承認	RAO2 削除審査待ち	RAO1 削除審査待ち
		削除承認	RAO2 削除審査待ち	削除待ち
		削除拒否	RAO2 削除審査待ち	削除要求前
	鍵状態：PKCS#12	取得要求	鍵取得要求前	RAO1 取得待ち
	鍵状態：PIN	取得要求	鍵取得要求前	RAO2 取得待ち
		取得	RAO2 取得待ち	鍵取得済み
KRO1	鍵状態：PKCS#12	取得要求	鍵取得済み	KRO1 取得審査待ち
		取得要求	鍵取得済み	KRO2 取得審査待ち
		取得要求	鍵取得済み	KRO1 取得待ち
		取得承認	KRO1 取得審査待ち	KRO2 取得審査待ち
		取得承認	KRO1 取得審査待ち	KRO1 取得待ち
		取得拒否	KRO1 取得審査待ち	KRO1 取得拒否
		取得	KRO1 取得待ち	鍵取得済み

オペレータ種別	状態種別	操作	状態	遷移可能な状態
	鍵状態：PIN	取得要求	鍵取得済み	KRO1 取得審査待ち
		取得要求	鍵取得済み	KRO2 取得審査待ち
		取得要求	鍵取得済み	KRO2 取得待ち
		取得承認	KRO1 取得審査待ち	KRO2 取得審査待ち
		取得承認	KRO1 取得審査待ち	KRO2 取得待ち
		取得拒否	KRO1 取得審査待ち	KRO1 取得拒否
KRO2	鍵状態：PKCS#12	取得要求	鍵取得済み	KRO1 取得審査待ち
		取得要求	鍵取得済み	KRO2 取得審査待ち
		取得要求	鍵取得済み	KRO1 取得待ち
		取得承認	KRO2 取得審査待ち	KRO1 取得審査待ち
		取得承認	KRO2 取得審査待ち	KRO1 取得待ち
		取得拒否	KRO2 取得審査待ち	KRO2 取得拒否
	鍵状態：PIN	取得要求	鍵取得済み	KRO1 取得審査待ち
		取得要求	鍵取得済み	KRO2 取得審査待ち
		取得要求	鍵取得済み	KRO2 取得待ち
		取得承認	KRO2 取得審査待ち	KRO1 取得審査待ち
		取得承認	KRO2 取得審査待ち	KRO2 取得待ち
		取得拒否	KRO2 取得審査待ち	KRO2 取得拒否
		取得	KRO2 取得待ち	鍵取得済み
RA	証明書状態	発行	CA 発行審査待ち	発行
		発行	CA 発行審査待ち	発行失敗
		失効	CA 失効審査待ち	失効
		失効	CA 失効審査待ち	CA 失効拒否
	証明書削除状態	削除	削除待ち	－
	鍵状態：PKCS#12	鍵生成	－	鍵取得要求前
	鍵状態：PIN	鍵生成	－	鍵取得要求前

表 6-8：デフォルトの状態遷移

RA 操作者	状態種別	操作	状態	遷移可能な状態
RAO1	証明書状態	発行承認	RAO1 発行審査待ち	CA 発行審査待ち
			CA 発行審査待ち	発行
			CA 発行審査待ち	発行失敗
		発行拒否	RAO1 発行審査待ち	RAO1 発行拒否
		失効承認	RAO1 失効審査待ち	CA 失効審査待ち
			CA 失効審査待ち	失効
			CA 失効審査待ち	発行
		失効拒否	RAO1 失効審査待ち	発行
	証明書削除状態	削除要求	削除要求前	RAO2 削除審査待ち
		削除承認	RAO1 削除審査待ち	削除待ち
		削除拒否	RAO1 削除審査待ち	削除要求前
	鍵状態：PKCS#12	取得要求	鍵取得前	RAO1 取得待ち
		取得	RAO1 取得待ち	鍵取得済み
	鍵状態：PIN	取得要求	鍵取得前	RAO2 取得待ち
RAO2	証明書状態	一括申請	発行申請前	RAO1 発行審査待ち
		個別申請	発行申請前	RAO2 発行審査待ち
		発行承認	RAO2 発行審査待ち	RAO1 発行審査待ち
		発行拒否	RAO2 発行審査待ち	RAO2 発行拒否
		失効要求	発行	RAO1 失効審査待ち
	証明書削除状態	削除要求	削除要求前	RAO2 削除審査待ち
		削除承認	RAO2 削除審査待ち	RAO1 削除審査待ち
		削除拒否	RAO2 削除審査待ち	削除要求前
	鍵状態：PKCS#12	取得要求	鍵取得前	RAO1 取得待ち
	鍵状態：PIN	取得要求	鍵取得前	RAO2 取得待ち
		取得	RAO2 取得待ち	鍵取得済み
KRO1	鍵状態：PKCS#12	取得要求	鍵取得済み	KRO2 取得審査待ち
		取得	KRO1 取得待ち	鍵取得済み
	鍵状態：PIN	取得要求	鍵取得済み	KRO1 取得審査待ち
		取得承認	KRO1 取得審査待ち	KRO2 取得待ち
		取得拒否	KRO1 取得審査待ち	KRO1 取得拒否
KRO2	鍵状態：PKCS#12	取得要求	鍵取得済み	KRO2 取得審査待ち
		取得承認	KRO2 取得審査待ち	KRO1 取得待ち
		取得拒否	KRO2 取得審査待ち	KRO2 取得拒否
	鍵状態：PIN	取得要求	鍵取得済み	KRO1 取得審査待ち
		取得	KRO2 取得待ち	鍵取得済み

RA 操作者は鍵・証明書操作機能を操作することにより鍵、証明書の状態を変更する。鍵・証明書操作機能で実行可能なセキュリティ属性の操作を表 6-9 に示す。

表 6-9：実行可能なセキュリティ属性の操作

オペレータ種別	機能	セキュリティ属性	実行可能な操作
RA 操作者（RAO1)	鍵・証明書操作機能	証明書状態	改変、削除
		鍵状態	改変、削除
		証明書削除状態	改変、削除
RA 操作者（RAO2）	鍵・証明書操作機能	証明書状態	作成、改変、削除
		鍵状態	作成、改変、削除
		証明書削除状態	作成、改変、削除
RA 操作者（KRO1）	鍵・証明書操作機能	鍵状態	改変
RA 操作者（KRO2）	鍵・証明書操作機能	鍵状態	改変

6.1.6 F.CIPHER（暗号化機能）

(1) F.CIPHER.1（暗号操作メカニズム）

F.CIPHER.1 は、TSC 内のデータを暗号化するための鍵を生成し、データの暗号化を行う機能である。また、使用済みとなった鍵の破棄も行う。

暗号化及び復号に使用される鍵の情報を表 6-10 に示す。

表 6-10：暗号化及び復号に使用される鍵情報

鍵名 （ ）内の情報で鍵を生成する	標準	アルゴリズム	鍵長（bit）
鍵名なし （RA サーバの鍵・証明書暗号化シード）	PKCS#5	RC2	128
鍵名なし （RA サーバの起動パスワード）	PKCS#5	RC2	128
監査ログ暗号化鍵 （監査ログ暗号化シード）	PKCS#5	RC2	128
鍵名なし （オペレータ登録情報のパスワード）	PKCS#5	RC2	128
サイト鍵（乱数）	PKCS#5	RC4	128
RA 鍵	PKCS#1	RSA	RA サーバの鍵長

暗号化及び復号に使用される鍵の暗号操作と鍵生成・破棄方法について表 6-11 に示す。

表 6-11：暗号化及び復号に使用される鍵の暗号操作と鍵生成・破棄方法

鍵名 （ ）内の情報で鍵を生成する	暗号操作	鍵生成・破棄
鍵名なし（RA サーバの鍵・証明書暗号化シード）	RA サーバの鍵・証明書の暗号化及び復号。	メモリ上で生成、削除。
鍵名なし（RA サーバの起動パスワード）	RA サーバの鍵・証明書暗号化シード、RDBMS にアクセスするための認証情報、監査ログ暗号化シードの暗号化及び復号。	メモリ上で生成、削除。
監査ログ暗号化鍵（監査ログ暗号化シード）	監査ログの暗号化及び復号。	監査ログ暗号化鍵設定機能で RDBMS に登録。 RDBMS からの削除は行われない。
鍵名なし（オペレータ登録情報のパスワード）	オペレータ登録情報の暗号化及び復号。	メモリ上で生成、削除。
サイト鍵（乱数）	一般利用者の鍵・証明書、PKCS#12、PIN の暗号化及び復号。	サイト管理機能で RDBMS に登録、削除。
RA 鍵	CMP クライアントの鍵・証明書、サイト鍵、監査ログを暗号化するための鍵の暗号化及び復号。	RA 動作環境情報設定機能でインポート。 削除は行われない。

暗号化及び復号に使用される鍵のセキュアな状態とセキュリティ属性について表 6-12 に示す。

表 6-12：暗号化及び復号に使用される鍵のセキュアな状態とセキュリティ属性

鍵名 （ ）内の情報で鍵を生成する	セキュリティ属性	セキュアな状態
鍵名なし（RA サーバの鍵・証明書暗号化シード）	なし	RA サーバが固定の鍵で暗号化及び復号するため、セキュリティ属性はない。
鍵名なし（RA サーバの起動パスワード）	なし	RA サーバが固定の鍵で暗号化及び復号するため、セキュリティ属性はない。
監査ログ暗号化鍵（監査ログ暗号化シード）	鍵番号	監査ログ暗号化鍵は鍵番号によって管理され、セキュアな状態を保持する。 鍵番号はシステム管理者により RA セットアップ機能の監査ログ暗号化鍵設定機能でのみ登録、変更が行える。RA セットアップ機能はシステム管理者がセキュアゾーンでしか使用しないためアクセス制御はない。
鍵名なし（オペレータ登録情報のパスワード）	なし	鍵は RA コンソール機能のオペレータ管理機能により RA 管理者からオフラインで RA 操作者に渡され、TOE では管理しないため、セキュリティ属性はない。
サイト鍵（乱数）	サイト ID	サイト鍵はサイト ID によって管理され、セキュアな状態を保持する。 サイト ID は RA 管理者により RA コンソール機能のサイト管理機能でのみ追加、削除が行える。サイト ID は F.ACCESS_CONTROL によりアクセス制御される。
RA 鍵	なし	RA サーバが固定の鍵で暗号化及び復号するため、セキュリティ属性はない。

(2) F.CIPHER.2（パスワードメカニズム）

パスワードメカニズムではパスワードを表 6-13 のパスワード仕様により検証する機能を提供する。

パスワードメカニズムについて表 6-13 に示す。

表 6-13：パスワードメカニズム

パスワード名	パスワード仕様	生成	使用
RA サーバの起動パスワード	ASCII コードの 0x20～0x07E を 6 文字以上 14 文字以下	システム管理者が RA セットアップの RA 起動パスワード設定機能を使用してパスワードを設定する。 設定したパスワードで RA 動作環境情報を暗号化する。	システム管理者が RA サーバ起動時に入力する。 入力したパスワードで RA 動作環境情報を復号し、RA サーバを起動する。
オペレータ登録情報のパスワード	ASCII コードの 0x20～0x7E を 4 文字以上 8 文字以下	RA 管理者が RA コンソールのオペレータ管理機能でオペレータ登録時に設定する。 設定したパスワードでオペレータ登録情報を暗号化する。	RA 操作者が RA オペレータのオペレータ環境設定機能のオペレータ登録でオペレータ登録情報を復号し、オペレータ登録を行う。
オペレータ登録用ログインパスワード	10 バイトの乱数	RA 管理者が RA コンソールのオペレータ管理機能でオペレータ登録時に自動生成される。	RA 操作者が RA オペレータのオペレータ環境設定機能のオペレータ登録で識別認証を行うときにプログラム内部で使用する。

(3) F.CIPHER.3（暗号鍵シードメカニズム）

暗号鍵シードメカニズムでは暗号鍵シードを表 6-14 のシード仕様により生成または検証する機能を提供する。

鍵生成時に使用するシードについて表 6-14 に示す。

表 6-14：鍵生成時に使用するシード

シード名	シード仕様	生成	使用
監査ログ暗号化シード	ASCII コードの 0x20～0x07E を 4 文字以上 8 文字以下	システム管理者が RA セットアップの監査ログ暗号化鍵設定機能を使用してシードを設定する。	RA サーバが監査ログの暗号化、検証時に使用する。
RA サーバの鍵・証明書暗号化シード	15 バイトの乱数	システム管理者が RA セットアップの RA 動作環境情報設定機能を使用時に自動的に生成され、RA サーバの鍵・証明書を暗号化する。	RA サーバが起動時に RA サーバの鍵・証明書を復号するときに使用する。

6.1.7 F.SSL（暗号通信機能）

F.SSL は、TOE を構成するコンポーネント間の通信データを暗号化及びアクセス制御で保護する機能である。SSL を使用して通信データの暗号化、復号及び通信データの改ざんの検出を行う。SSL で使用する鍵の暗号アルゴリズムは RC4、鍵長は 128 ビットである。鍵は使用後にメモリ上から削除する。

通信データの検証はオペレータ証明書を使用してオペレータを識別し、署名検証が行われる。オペレータ証明書は **F.OPERATOR_AUTH** により取り込まれる。

6.1.8 F.ADMIN（管理機能）

F.ADMIN は各情報にアクセスするために使用するセキュリティ属性を管理する機能である。管理するセキュリティ属性を表 6-15 に示す。

表 6-15：実行可能なセキュリティ属性の操作

オペレータ（操作者）	機能		セキュリティ属性	実行可能な操作
システム管理者	RA セットアップ機能	RA 管理者・監査者登録機能	RA 管理者・監査者のオペレータ ID	作成、改変、削除
			RA 管理者・監査者のオペレータ種別	作成、改変、削除
		監査ログ暗号化鍵設定機能	鍵番号	作成
RA 管理者	RA コンソール機能	CA 管理機能	CAID	作成、改変、削除
		サイト管理機能	サイト ID	作成、改変、削除
			CAID	設定
		オペレータ管理機能	RA 操作者のオペレータ ID	作成、改変、削除
			RA 操作者のオペレータ種別	作成、改変、削除
			サイト ID	設定

オペレータの登録には「RA セットアップ機能」の「RA 管理者・監査者登録機能」と「RA コンソール機能」の「オペレータ管理機能」がある。
各機能で登録可能なオペレータ種別を表 6-16 に示す。

表 6-16：登録可能なオペレータ

オペレータ登録者	機能		サイト ID	操作可能なオペレータ種別
システム管理者	RA セットアップ機能	RA 管理者・監査者登録機能	ADMIN	CONSOLE（RA 管理者）
				AUDITOR（監査者）
RA 管理者	RA コンソール機能	オペレータ管理機能	任意のサイト ID	RAO1（RA 操作者）
				RAO2（RA 操作者）
				KRO1（RA 操作者）
				KRO2（RA 操作者）

鍵番号は 1 から始まる数字で暗号鍵の更新をした場合、現在の数字に 1 足された数字で暗号鍵を登録する。

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を適用するセキュリティ機能は、F.OPERATOR_AUTH、F.SSL、F.CA_AUTH、F.AUDIT.1、F.AUDIT.3、F.CIPHER.1、F.CIPHER.2 である。これらのセキュリティ機能のうち、F.OPERATOR_AUTH、F.SSL、F.CA_AUTH、F.AUDIT.1、F.AUDIT.3、F.CIPHER.1 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ため、本機能強度の対象外である。F.CIPHER.2 は表 6-13 の機能強度として、SOF-基本を満たしている。

6.3 保証手段

5.1.3 で記述した EAL3 追加の TOE セキュリティ保証要件のコンポーネントを満たす保証手段を表 6-17 に示す。なお追加の保証要件は ADV_SPM.1 である。

表 6-17：EAL3 追加の保証要件コンポーネントと保証手段

TOE セキュリティ保証要件		コンポーネント	保証手段
構成管理	CM 能力	ACM_CAP.3	構成管理手順書
	CM 範囲	ACM_SCP.1	
配付と運用	配付	ADO_DEL.1	配付規定書
	設置・生成・及び立上げ	ADO_IGS.1	PKI Management Program サーバパッケージ README、PKI Management Program クライアントパッケージ README、PKI Management Program ソフトウェア添付資料
開発	機能仕様	ADV_FSP.1	機能仕様書
	上位レベル設計	ADV_HLD.2	構成仕様書
	表現対応	ADV_RCR.1	表現対応書
	セキュリティ方針モデル化	ADV_SPM.1	機能仕様書
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	日立公開鍵認証基盤 PKI Management Program Server 編、
	利用者ガイダンス	AGD_USR.1	日立公開鍵認証基盤 PKI Management Program Operator 編
ライフサイクルサポート	開発セキュリティ	ALC_DVS.1	開発環境管理規定書
テスト	カバレージ	ATE_COV.2	テスト仕様書
	深さ	ATE_DPT.1	
	機能テスト	ATE_FUN.1	
	独立テスト	ATE_IND.2	
脆弱性評定	誤使用	AVA_MSU.1	脆弱性評定書
	TOE セキュリティ機能強度	AVA_SOF.1	
	脆弱性分析	AVA_VLA.1	

7 PP 主張

本 ST には、適合するプロテクションプロファイルはない。

8 根拠

本 ST で規定した内容についての正当性の検証について記述する。

8.1 セキュリティ対策方針根拠

8.1.1 前提条件に対するセキュリティ対策方針の検証

(1)　必要性

前提条件とセキュリティ対策方針の対応を表 8-1 に示す。前提条件について、1 つ以上のセキュリティ対策方針により対応していることを表している。

表 8-1：前提条件に対するセキュリティ対策方針の適合性

セキュリティ対策方針 / 前提条件	OE.ACCESS	OE.CLIENT_ACCESS	OE.MEDIA_PROTECT	OE.OPERATOR_PROTECT	OE.ADMIN	OE.OPERATOR	OE.CONNECT	OE.RELIABILITY	OE.CA_RELIABILITY	OE.OTHER_RELIABILITY	OE.IMPORTED	OE.EXPORTED	OE.PASSWORD
ASM.ACCESS	●												
ASM.CLIENT_ACCESS		●											
ASM.MEDIA_PROTECT			●										
ASM.OPERATOR_PROTECT				●									
ASM.ADMIN					●								
ASM.OPERATOR						●							
ASM.CONNECT							●						
ASM.RELIABILITY								●					
ASM.CA_RELIABILITY									●				
ASM.OTHER_RELIABILITY										●			
ASM.IMPORTED											●		
ASM.EXPORTED												●	
ASM.CLIENT_RESTORE					●	●							
ASM.PASSWORD													●

(2) 十分性

前提条件に対する、セキュリティ対策方針の説明を以下に記述する。

ASM.ACCESS（アクセスの物理的制限）

ASM.ACCESS は、RA サーバ、及び RA 設定端末がセキュアゾーンに設置され、セキュアゾーンにはセキュアゾーンに設置された各マシンの管理者、及び各マシン管理者に許可された者だけが入室できるよう入退室管理が実施され、システム管理者に許可された者がセキュアゾーンに入室する場合には、必ずシステム管理者の監視下に置かれるということを想定している。

OE.ACCESS により、RA サーバ、及び RA 設定端末がセキュアゾーンに設置され、セキュアゾーンにはセキュアゾーンに設置された各マシンの管理者、及び各マシン管理者に許可された者だけが入室できるよう入退室管理が実施されている。また、各マシンの管理者に特に許可された者が入室する場合には、必ず各マシンの管理者が共に入室し、各マシンの管理者が各マシンの管理者に特に許可された者の作業を監視している。これにより **ASM.ACCESS** が実現される。

ASM.CLIENT_ACCESS（クライアントアクセスの物理的制限）

ASM.CLIENT_ACCESS は、RA 管理／監査端末、RA 操作端末にアクセスできるのは、TOE を運用する組織に属する者だけであるとういうことを想定している。

OE.CLIENT_ACCESS により、TOE を運用する組織に属する者だけが物理的にアクセスできる場所が確保され、その場所に RA 管理／監査端末、RA 操作端末を設置されている。これにより、**ASM.CLIENT_ACCESS** が実現される。

ASM.MEDIA_PROTECT（媒体の物理的保護）

ASM.MEDIA_PROTECT は、TSC 内にあるデータのバックアップが保管された媒体が適切な手順に従って保管され、物理的な破壊、及び盗難から保護されていることを想定している。

OE.MEDIA_PROTECT により、破壊、及び盗難から保護される場所が確保され、その場所に TSC 内にあるデータのバックアップした媒体が保管されている。これにより、**ASM. MEDIA_PROTECT** が実現される。

ASM.OPERATOR_PROTECT（クライアント秘密鍵の物理的保護）

ASM.OPERATOR_PROTECT は、オペレータの秘密鍵と証明書が耐タンパー性のある IC カードに格納され、IC カード盗難時にも物理的な攻撃による秘密鍵の盗難から保護されることを想定している。

OE.OPERATOR_PROTECT により、オペレータは耐タンパー性のある IC カードを持ち、自身の秘密鍵と証明書を IC カードで管理している。これにより、**ASM.OPERATOR_PROTECT** が実現される。

ASM.ADMIN（システム管理者・RA 管理者・監査者・他サーバの管理者の信頼性）

ASM.ADMIN は以下のことを想定している。

・ システム管理者、RA 管理者、監査者は TOE を運用する組織に属し、TOE を運用する組織の責任者によって任命される

・ システム管理者、RA 管理者、監査者、他サーバの管理者は、それぞれの役割を果たす上で必要となる知識を習得するための教育を施される

・ システム管理者、RA 管理者、監査者、他サーバの管理者は、それぞれに課せられた役割に対して、許可された一連の行為に関する悪意を持った行為は行わず、システムの運用に協力的に関わる

・ システム管理者、RA 管理者、監査者、他サーバの管理者は、それぞれに課せられた役割に対して、許可された一連の行為に関する悪意を持った行為は行わず、システムの運用に協力的に関わる

OE.ADMIN により、TOE を運用する組織の責任者は、TOE を運用する組織に属する者の中から適した者を選別し、システム管理者、RA 管理者、及び監査者に任命している。また、TOE を運用する組織の責任者は、システム管理者、RA 管理者、監査者、他サーバの管理者に対して以下の教育、及び訓練を実施されている。

・課せられた役割を果たす上で必要となる知識を習得するための技術教育

・課せられた役割に対して、セキュリティ意識を向上させ、悪意を持った行為を行わないようにするためのセキュリティ教育

・TOE が正常に動作しなくなった場合、TOE の再インストール、再セットアップを行う。

これにより、**ASM.ADMIN** が実現される。

ASM.OPERATOR（RA 操作者の信頼性）

ASM. OPERATOR は、RA 操作者が TOE を運用する組織に属し、TOE を運用する組織の責任者によって任命され、RA 操作者としての役割を果たす上で必要となる知識を習得するための教育を施されることを想定している。

OE.OPERATOR により、TOE を運用する組織の責任者は、TOE を運用する組織に属する者の中から適した者を選別し、RA 操作者に任命している。また、TOE を運用する組織の責任者は、RA 操作者に対して、RA 操作者としての役割を果たす上で必要となる知識を習得するための技術教育を実施している。TOE が正常に動作しなくなった場合、TOE の再インストール、再セットアップを行う。

これにより、**ASM.OPERATOR** が実現される。

ASM.CONNECT（接続制限）

ASM.CONNECT は以下のことを想定している。

・ セキュアゾーン LAN はファイアウォールを介して操作端末 LAN にのみ接続される
・ 操作端末 LAN には TOE を運用する組織に属する者だけがアクセスできるよう物理的に保護される
・ 操作端末 LAN が TOE を運用する組織外のネットワークに接続される場合は、TOE を運用する組織外のネットワークから操作端末 LAN に対してアクセスできないよう、操作端末 LAN はファイアウォールにより保護される
・ 操作端末 LAN から RA サーバへのアクセスは、RA 管理・監査端末及び RA 操作端末から RA サーバの特定のポートに対してのみ接続可能であるよう、セキュアゾーン LAN－操作端末 LAN 間のファイアウォールにより制限される

OE.CONNECT により以下のことが実施されている。

・ セキュアゾーン LAN はファイアウォールを介して操作端末 LAN にのみ接続されている
・ 操作端末 LAN には TOE を運用する組織に属する者だけがアクセスできるよう物理的に保護されている
・ 操作端末 LAN が TOE を運用する組織外のネットワークに接続される場合は、TOE を運用する組織外のネットワークから操作端末 LAN に対してアクセスできないよう、操作端末 LAN はファイアウォールにより保護されている
・ 操作端末 LAN から RA サーバへのアクセスは、RA 管理・監査端末及び RA 操作端末から RA サーバの特定のポートに対してのみ接続可能であるよう、セキュアゾーン LAN－操作端末 LAN 間のファイアウォールにより制限されている

これにより、**ASM.CONNECT** が実現される。

ASM.RELIABILITY（TOE 構成要素の信頼性）

ASM.RELIABILITY は、TOE が動作する上で必要となるハードウェア及びソフトウェアが、システム管理者、RA 管理者、監査者、及び RA 操作者により適切に設定され管理されることを想定している。

OE.RELIABILITY により、システム管理者、RA 管理者、監査者、及び RA 操作者は、TOE が動作する上で必要となるハードウェア及びソフトウェアを適切に設定・管理している。これにより、**ASM.RELIABILITY** が実現される。

ASM.CA_RELIABILITY（CA の信頼性）

ASM.CA_RELIABILITY は、TOE がセキュアゾーン LAN に接続された信頼できる CA に対してのみ証明書の発行・失効要求を行うことを想定している。

OE.CA_RELIABILITY により、TOE を運用する組織の責任者は信頼する CA のみがセキュアゾーン LAN に接続されるよう管理を行い、RA 管理者はセキュアゾーン LAN に接続された信頼する CA のみを信頼する CA として TOE に登録している。これにより、**ASM.CA_RELIABILITY** が実現される。

ASM.OTHER_RELIABILITY（その他のマシンの信頼性）

ASM.RELIABILITY は、セキュアゾーンに設置される TOE 構成要素外のハードウェア及びソフトウェアが、他サーバマシン管理者により適切に設定・管理されることを想定している。

OE.OTHER_RELIABILITY により、他サーバマシン管理者はセキュアゾーンに設置される TOE 構成要素外のハードウェア及びソフトウェアを適切に設定・管理している。これにより、**ASM.OTHER_RELIABILITY** が実現される。

ASM.IMPORTED（インポートデータの信頼性）

ASM.IMPORTED は、TSC にインポートされる鍵・証明書は、セキュアゾーン LAN に接続された CA により発行されたものであり、また、TSC にインポートされる利用者データは、暴露・盗難・改ざんから保護するため、関連者により適切に管理されていることを想定している。

OE.IMPORTED により、TSC に鍵・証明書をインポートする者は、インポートされる鍵・証明書がセキュアゾーン LAN に接続された CA により発行されたものであることを確認しており、また、TSC に利用者データをインポートする者は、インポートされる利用者データを暴露・盗難・改ざんから保護するために適切に管理している。これにより、**ASM.IMPORTED** が実現される。

ASM.EXPORTED（エクスポートデータの信頼性）

ASM.EXPORTED は、TSC からエクスポートされた鍵・証明書を含む利用者データが、暴露・盗難・改ざんから保護するため、関連者により適切に管理されていることを想定している。

OE.EXPORTED により、TSC から鍵・証明書を含む利用者データをエクスポートする者は、暴露・盗難・改ざん等から保護するために、エクスポートされた鍵・証明書を含む利用者データを適切に管理している。これにより、**ASM.EXPORTED** が実現される。

ASM.CLIENT_RESTORE（クライアント環境の復元）

ASM.CLIENT_RESTORE は、RA 管理・監査端末、または RA 操作端末上の TSC 内データが毀損され、RA コンソール、または RA オペレータが正常に動作しなくなった場合、各端末を使用するオペレータは、自身の責任で TOE の再インストール、及び再設定を行うことを想定している。

OE.ADMIN 及び **OE. OPERATOR** により、RA 管理・監査端末、及び RA 操作端末を使用するオペレータは TOE が正常に動作しない場合、TOE のインストール、及び設定を行う。

これにより、**ASM.CLIENT_RESTORE** が実現される。

ASM.PASSWORD（パスワード及び PIN の管理）

ASM.PASSWORD は、TOE を運用する際に必要となるパスワード及び PIN について、以下のことを想定している。

・ パスワード及び PIN が TOE 利用者本人により適切に管理され、本人以外の者に知られることがないこと
・ TOE 利用者によって設定されるパスワード及び PIN は類推が困難であること
・ パスワード及び PIN が適切な頻度で変更されること

OE.PASSWORD により、TOE 利用者は以下のことが実施されている。

・ パスワード及び PIN が本人以外の者に知られることがないよう適切に管理している
・ 類推が困難であるパスワード及び PIN を設定している
・ パスワード及び PIN を適切な頻度で変更している

これにより、**ASM.PASSWORD** が実現される。

8.1.2　脅威に対するセキュリティ対策方針の検証

(1)　必要性

脅威とセキュリティ対策方針の対応を表 8-2 に示す。脅威に対して、1 つ以上のセキュリティ対策方針により対抗していることを表している。

表 8-2：脅威に対するセキュリティ対策方針の適合性

セキュリティ対策方針 / 脅威	TOE					環境								
	O.AUTH	O.NETWORK_ENCRYPT	O.PERMISSION	O.STATUS_FLOW_CONTROL	O.AUDIT	OE.OS_CORRECT_TIME	OE.OS_IA	OE.IC_IA	OE.OS_ACCESS_CONTROL	OE.RELIABILITY	OE.PASSWORD	OE.BACKUP	OE.ADMIN	OE.STATUS_FLOW_MANAGEMENT
T.DATA_CORRUPTED									●	●		●	●	
T.DATA_REMOVED					●	●						●	●	
T.UNAUTH_TOE_ACCESS	●				●	●		●						
T.UNAUTH_OPERATION			●		●	●								
T.INVALID_OPERATION				●	●	●								●
T.INVALID_TERMINAL_ACCESS							●		●	●	●			
T.INTERCEPTION		●												

(2) 十分性

脅威に対する、セキュリティ対策方針の説明を以下に記述する。

T.DATA_CORRUPTED（TOE データの毀損）

システム管理者が、OS 等 TOE 外の機能の誤使用により、RA サーバマシン上の保護対象資産が変更･削除されることが考えられる。**T.DATA_CORRUPTED** の脅威に対抗するためには、事前に自身の誤操作を予防できるようにすること、誤操作を行っても変更・削除が容易には行われないようファイルのアクセス権限を設定しておくこと、変更・削除してしまった TOE のデータを元の状態に戻せるようにすることが効果的である。

OE.ADMIN により、誤操作の可能性を低減するためにシステム管理者へセキュリティ教育や訓練を実施し、慎重な操作の自覚を促すことで誤操作を予防する。

また、誤操作が行われた場合にも、**OE. RELIABILITY** により、システム管理者であっても容易に変更、削除できないようファイルのアクセス権を事前に設定しておくことで、**OE.OS_ACCESS_CONTROL** によりファイルの変更・削除が抑止される。

以上のセキュリティ対策方針を実施することで本脅威に対抗できるが、対抗しきれず変更･削除が行われたとしても、**OE.BACKUP** によって定期的に実施されているバックアップで作成されるバックアップデータから、元の状態に復旧することができる。

以上のセキュリティ対策方針を実施することで、**T.DATA_CORRUPTED** に対抗できる。

T.DATA_REMOVED（TOE データの削除）

RA 管理者、及び監査者による TOE の機能の誤使用により、RA サーバマシン上の RA 管理情報、監査ログが削除されることが考えられる。**T.DATA_REMOVED** の脅威に対抗するためには、事前に自身の誤操作を予防できるようにすること、削除してしまった TOE のデータを元の状態に戻せるようにすることが効果的である。

OE.ADMIN により、誤操作の可能性を低減するために RA 管理者、及び監査者へセキュリティ教育や訓練を実施し、慎重な操作の自覚を促すことで誤操作を予防する。誤って削除が行われたとしても、**O.AUDIT** 及び **OE.OS_CORRECT_TIME** によって監査ログが正確な日付／時刻を伴って記録されているため、誤操作を検出することができ、削除されたデータは **OE.BACKUP** によって定期的に実施されているバックアップで作成されるバックアップデータから復元することができる。

以上のセキュリティ対策方針を実施することで、**T.DATA_REMOVED** に対抗できる。

T.UNAUTH_TOE_ACCESS（TOE への不正アクセス）

TOE 利用者の識別認証が正確に行われなければ、TOE を利用する権限を持たない者が RA コンソールにログインし、RA 管理情報の登録、変更、削除、監査ログの削除、及び RA オペレータを使用して RA サーバにログインし、鍵・証明書の発行、失効、取得、削除を行い、その結果として TOE の適切な運用が妨げられる。

T.UNAUTH_TOE_ACCESS の脅威に対抗するためには、TOE を利用する権限を持たない者が RA コンソール、及び RA オペレータを使用して RA サーバにログインすることができないように制御することが効果的である。

RA コンソール、及び RA オペレータでのログイン操作時、RA コンソール、及び RA オペレータは利用者に対して IC カードの利用者 PIN の入力を求める。このとき、**OE.IC_IA** により、現在の利用者が IC カードの正当な所有者であるかの認証が行われ、認証されない利用者のログインは抑止される。

OE.IC_IA による識別が成功すると RA サーバへのログイン要求が行われる。このとき、**O.AUTH** により、RA サーバに登録されたオペレータだけが RA サーバにログインすることができるよう証明書による識別認証が行われ、識別認証されない利用者のログインは抑止される。

また、**O.AUDIT** 及び **OE.OS_CORRECT_TIME** によって TOE 利用者のログイン、ログアウトの履歴が監査ログに正確な日付／時刻を伴って記録されているため、TOE を利用する権限を持たない者が RA サーバへのログインを試みた場合、これを検出することができる。

以上のセキュリティ対策方針を実施することで、**T.UNAUTH_ACCESS** に対抗できる。

T.UNAUTH_OPERATION（許可されない操作）

オペレータに与えられる権限が適切に管理されなければ、オペレータが故意、または誤操作で自身に許可されていない操作を行い、その結果として TOE の適切な運用が妨げられる。

T.UNAUTH_OPERATION の脅威に対抗するためには、オペレータが自身に許可されていない操作を行えないように制御することが効果的である。

O.PERMISSION により、RA サーバはオペレータの実行権限を管理し、許可されない操作の実行を抑止する。

以上のセキュリティ対策方針を実施することで本脅威に対抗できるが、対抗しきれず許可されない操作が行われた場合には、**O.AUDIT** 及び **OE.OS_CORRECT_TIME** によって監査ログが正確な日付／時刻を伴って記録されているため、許可されない操作を抑止する効果があり、かつ許可されない操作が行われたことを検出することができる。

以上のセキュリティ対策方針を実施することで、**T.UNAUTH_OPERATION** に対抗できる。

T.INVALID_OPERATION（不正操作）

RA 操作者が故意、または誤操作で、自らに与えられた権限内で TOE の運用上適当でない操作を行うかもしれない。

T.INVALID_OPERATION の脅威に対抗するためには、単独の RA 操作者の操作では、証明書の発行、失効、取得などが行えないようにすることが効果的である。

O.STATUS_FLOW_CONTROL により、RA サーバは、RA 操作者からの証明書発行申請、失効申請、鍵・証明書取得申請等を受け付けたとき、申請者以外の RA 操作者による承認が行われるまで、証明書の発行、失効、鍵・証明書取得取得が行われないように制御する。**OE.STATUS_FLOW_MANAGEMENT** により、RA 管理者は、単独の RA 操作者が一般利用者鍵・証明書の発行、失効、取得、削除を行うことがないよう、状態フロー制御情報を適切に管理している。

また、**O.AUDIT** 及び **OE.OS_CORRECT_TIME** によって RA 操作者の操作の履歴が監査ログに正確な日付／時刻を伴って記録されているため、許可される権限内で行われる悪意ある操作を抑止する効果があり、かつ誤操作を検出することもできる。

以上のセキュリティ対策方針を実施することで、**T. INVALID_OPERATION** に対抗できる。

T.INVALID_TERMINAL_ACCESS（端末への不正アクセス）

TOE を運用する組織に属するもののうち悪意を持つ者が、直接、または操作端末 LAN から RA 管理／監査端末、RA 操作端末にアクセスし、TSC 内のデータ、及び TSC からエクスポートされたデータを不正利用、削除、または変更するかもしれない。

T.INVALID_TERMINAL_ACCESS の脅威に対抗するためには、RA 管理／監査端末、及び RA 操作端末を利用しようとするものの識別認証を行い、TOE を運用する組織に属するもののうち悪意を持つ者が操作を行えないように制御し、また、TSC 内のデータ、及び TSC からエクスポートされたデータに対して適切なアクセス権限を設定することにより、操作端末 LAN からアクセスできないようにすることが効果的である。

OE.RELIABILITY により、RA 管理／監査端末、及び RA 操作端末の OS には TOE の動作、及び管理のために必要なユーザアカウントのみが登録されている。**OE.OS_IA** により、OS は利用者からのログイン要求に対して識別認証を行い、識別認証されない者のログインを抑止する。また、**OE.PASSWORD** により、OS にログインするためのパスワードは適切に管理されており、パスワードが他者に知られることはない。これにより、TOE を運用する組織に属するもののうち悪意を持つ者が RA 管理／監査端末、または RA 操作端末に直接ログインすることにより、TSC 内のデータ、及び TSC からエクスポートされたデータを不正利用、削除、または変更することを防止する。

OE.RELIABILITY により、ネットワークを介して TSC 内のデータ、及び TSC からエクスポートされたデータにアクセスされることがないよう、アクセス権限が適切に設定されている。このため、**OE.ACCESS_CONTROL** によりネットワークを介しての TSC 内のデータ、及び TSC からエクスポートされたデータへアクセスは抑止される。

以上のセキュリティ対策方針を実施することより、**T.INVALID_TERMINAL_ACCESS** に対抗できる。

T.INTERCEPTION（盗聴）

RA コンソール･RA オペレータと RA サーバ間の通信が保護されていなければ、操作端末 LAN を経由する送受信データが容易に盗聴される。

T.INTERCEPTION の脅威に対抗するためには、RA コンソール・RA オペレータと RA サーバ間で送受信されるデータを暗号化することが効果的である。

O.NETWORK_ENCRYPT により、TOE は RA コンソール・RA オペレータと RA サーバ間で送受信されるデータを暗号化する。これにより、送受信データが盗聴されることを防止する。

以上のセキュリティ対策方針を実施することより、**T.INTERCEPTION** に対抗できる。

8.1.3　組織のセキュリティ方針に対するセキュリティ対策方針の検証

(1)　必要性

組織のセキュリティ方針に対するセキュリティ対策方針の対応を表 8-3 に示す。組織のセキュリティ方針に対して、１つ以上のセキュリティ対策方針により対抗していることを表している。

表 8-3：組織のセキュリティ方針に対するセキュリティ対策方針の適合性

セキュリティ対策方針 ＼ 組織のセキュリティ方針	TOE		環境				
	O.CA_AUTH	O.CIPHER	OE.RELIABILITY	OE.OS_IA	OE.OS_ACCESS_CONTROL	OE.DOMAIN_SEPARATION	OE.IMPORTED
P.OS_IA			●	●			
P.OS_ACCESS_CONTROL			●		●		
P.DOMAIN_SEPARATION						●	
P.CA_RELIABILITY	●						●
P.CIPHER		●					
P.AUDIT_INVISIBLE		●					

(2) 十分性

脅威に対する、セキュリティ対策方針の説明を以下に記述する。

P.OS_IA（OS による識別認証）

P.OS_IA は TOE が動作する上で必要となるすべてのマシンの OS は識別認証機能を持ち、あらかじめ登録された利用者だけが OS へのログインを許可されることを想定する。

OE.OS_IA により、OS は利用者からのログイン要求に対して識別認証を行い、識別認証されない者のログインを抑止する。また、**OE.RELIABILITY** により, TOE が動作する上で必要となるすべてのマシンの管理者は、それぞれのマシンに TOE の動作、及び管理のために必要なユーザアカウントのみが登録されるよう、ユーザアカウントの設定、管理を行っている。

これにより **P.OS_IA** が実現される。

P.OS_ACCESS_CONTROL（OS によるアクセス制御）

P.OS_ACCESS_CONTROL は、TOE が動作する上で必要となるすべてのマシンの OS はアクセス制御機能を持ち、識別された利用者による OS が管理する資源への許可されないアクセスを抑止することを想定する。

OE.OS_ACCESS_CONTROL により、OS は識別された利用者による OS が管理する資源へのアクセスに対してアクセス制御を実施し、OS が管理する資源への許可されないアクセスを抑止する。また、**OE.RELIABILITY** により, TOE が動作する上で必要となるすべてのマシンの管理者は、OS のアクセス制御機能を使用して OS が管理する TOE の保護対象資産に対して適切なアクセス権限は設定している。

これにより **P.OS_ACCESS_CONTROL** が実現される。

P.DOMAIN_SEPARATION（OS によるドメイン分離）

P. DOMAIN_SEPARATION は、TOE が動作する上で必要となるすべてのマシンの OS がドメイン分離機能を持ち、TSF、及び IT 環境により提供されるすべてのセキュリティ機能が他の機能の干渉を受けないことを想定する。

OE. DOMAIN_SEPARATION により、OS はセキュリティドメインを維持し、TSF、及び IT 環境により提供されるすべてのセキュリティ機能が他の機能の干渉を受けることを抑止する。

これにより **P. DOMAIN_SEPARATION** が実現される。

P. CA_RELIABILITY（CA の信頼性）

P.CA_RELIABILITY は、RA が接続する CA はセキュアゾーン LAN に接続された CA のみであることを想定する。

O.CA_AUTH により、TOE は RA サーバにおいて、CA に対して証明書の発行、失効要求を行うとき、証明書による相互認証を行い、要求先の CA があらかじめ RA サーバに証明書を登録された信頼できる CA であることを確認する。また、**OE.IMPORTED** により、TOE に登録された CA 証明書は、セキュアゾーン LAN に接続された CA により発行されたものである。

これにより **P. CA_RELIABILITY** が実現される。

P. CIPHER（秘密データの暗号化）

P.CIPHER は、TSC 内に存在する鍵、パスワード等の秘密データが暗号化されることを想定する。

O.CIPHER により、TOE は、TSC 内に存在する秘密鍵、認証情報、パスワード、PIN、オペレータ登録情報を暗号化する。

これにより **P. CIPHER** が実現される。

P. AUDIT_INVISIBLE（監査ログの不可視性）

P.AUDIT_INVISIBLE は、監査ログの内容が TOE 外の機能によって参照されないことを想定する。

O.CIPHER により、TOE は監査ログデータを暗号化する。

これにより **P. AUDIT_INVISIBLE** が実現される。

8.2　セキュリティ要件根拠

8.2.1　セキュリティ機能要件根拠

(1)　必要性

セキュリティ対策方針とセキュリティ機能要件の対応を表 8-4 に示す。セキュリティ機能要件が１つ以上のセキュリティ対策方針を満たしていることを表している。

表 8-4：セキュリティ対策方針に対する機能要件の適合性

セキュリティ対策方針 ＼ セキュリティ機能要件	TOE							環境				
	O.AUDIT	O.AUTH	O.CA_AUTH	O.PERMISSION	O.STATUS_FLOW_CONTROL	O.CIPHER	O.NETWORK_ENCRYPT	OE.OS_CORRECT_TIME	OE.DOMAIN_SEPARATION	OE.IC_IA	OE.OS_IA	OE.OS_ACCESS_CONTROL
FAU_GEN.1	●											
FAU_GEN.2	●											
FAU_SAR.1	●											
FAU_SAR.2	●											
FAU_SAR.3	●											
FAU_STG.1	●											

セキュリティ対策方針 / セキュリティ機能要件	TOE							環境				
	O.AUDIT	O.AUTH	O.CA_AUTH	O.PERMISSION	O.STATUS_FLOW_CONTROL	O.CIPHER	O.NETWORK_ENCRYPT	OE.OS_CORRECT_TIME	OE.DOMAIN_SEPARATION	OE.IC_IA	OE.OS_IA	OE.OS_ACCESS_CONTROL
FCS_CKM.1						●	●					
FCS_CKM.4		●	●			●	●					
FCS_COP.1[1]	●											
FCS_COP.1[2]		●					●					
FCS_COP.1[3]			●									
FCS_COP.1[4]						●	●					
FDP_ACC.1				●		●						
FDP_ACF.1				●		●						
FDP_IFC.1					●							
FDP_IFF.1					●							
FDP_ITC.1		●	●				●					
FDP_ITT.1							●					
FIA_SOS.1[1]						●						
FIA_SOS.1[2]						●						
FIA_SOS.1[3]		●										
FIA_SOS.2						●						
FIA_UAU.1		●										
FIA_UAU.2			●									

セキュリティ対策方針 / セキュリティ機能要件	TOE							環境				
	O.AUDIT	O.AUTH	O.CA_AUTH	O.PERMISSION	O.STATUS_FLOW_CONTROL	O.CIPHER	O.NETWORK_ENCRYPT	OE.OS_CORRECT_TIME	OE.DOMAIN_SEPARATION	OE.IC_IA	OE.OS_IA	OE.OS_ACCESS_CONTROL
FIA_UID.1	●	●		●	●	●						
FIA_UID.2			●				●					
FMT_MSA.1[1]		●	●	●		●	●					
FMT_MSA.1[2]					●							
FMT_MSA.2	●	●	●			●	●					
FMT_MSA.3[1]		●	●	●		●	●					
FMT_MSA.3[2]					●							
FMT_MSA.3[3]	●											
FMT_MSA.3[4]		●		●			●					
FMT_MTD.1	●	●	●	●			●					
FMT_SMR.1	●	●	●	●	●	●	●					
FPT_ITT.1							●					
FPT_RVM.1	●	●	●	●	●	●	●					

セキュリティ対策方針 / セキュリティ機能要件	TOE							環境				
	O.AUDIT	O.AUTH	O.CA_AUTH	O.PERMISSION	O.STATUS_FLOW_CONTROL	O.CIPHER	O.NETWORK_ENCRYPT	OE.OS_CORRECT_TIME	OE.DOMAIN_SEPARATION	OE.IC_IA	OE.OS_IA	OE.OS_ACCESS_CONTROL
FDP_ACC.1[E]												●
FDP_ACF.1[E]												●
FIA_SOS.1[E1]										●		
FIA_SOS.1[E2]											●	
FIA_UAU.1[E]											●	
FIA_UAU.2[E]										●		
FIA_UID.1[E]											●	●
FIA_UID.2[E]										●		
FMT_MSA.1[E1]												●
FMT_MSA.1[E2]												●
FMT_MSA.1[E3]												●
FMT_MSA.3[E]												●
FMT_MTD.1[E]												●
FMT_SMR.1[E]												●
FPT_SEP.1[E]									●			
FPT_STM.1[E]								●				

(2) 十分性

セキュリティ対策方針を実現するセキュリティ機能要件の説明を以下に記述する。

O.AUDIT（監査記録）

O.AUDIT は、以下のセキュリティ機能要件で実現される。

FAU_GEN.1、FAU_GEN.2 により RA 管理者、監査者、RA 操作者によるセキュリティに関連するすべての操作が監査ログに記録され、監査ログには事象の種別、操作者の識別情報、操作の結果、及び操作が行われた日時が含まれる。

FAU_STG.1 により、監査ログの完全性を保証する。これを実現するために、**FCS_COP.1[1]**により監査ログレコードの鍵付きハッシュを生成し、監査ログレコードとともに保存する。これにより、監査ログの改ざんが検出できる。また、監査ログレコードに連続する番号を付加することにより、監査ログレコードの不正な削除を検出する。監査ログのハッシュ生成、暗号化に使用する鍵は**FMT_MSA.3[3]**により鍵番号で管理され **FMT_MSA.2** により鍵番号はセキュアな値だけが受け入れられる。

FAU_SAR.1、FAU_SAR.2、FMT_MTD.1 により、監査者、及び RA 操作者に対してのみ、監査ログを参照する手段が提供される。RA 操作者に対しては、監査ログの参照を行う RA 操作者が属するサイトに関連した監査ログの参照のみが許可される。また、**FAU_SAR.3、FMT_MTD.1** により、一定の条件による監査ログの検索・参照・削除する機能を提供する。**FMT_SMR.1、FIA.UID.1** により監査者であることを識別し、その役割を維持する。

FPT_RVM.1 は監査記録機能が必ず動作することを保証する。なお、妥当性の詳細については補完性にて述べる。

O.AUTH（TOE 利用者識別認証）

FIA_UAU.1、**FIA_UID.1** により、RA コンソール、及び RA オペレータからのログイン要求時に RA サーバによる利用者の識別認証が行われ、識別認証された利用者からのログイン要求のみが受け付けられる。
利用者の識別認証は、証明書、またはユーザ ID／パスワードにより行われる。証明書による認証は、**FCS_COP.1[2]**により、利用者の秘密鍵によるディジタル署名を、利用者の証明書で検証することにより行われる。ユーザ ID／パスワードによる識別認証は、**FIA_SOS.1[3]**のパスワードを使用し TOE が保持するオペレータ認証情報とログイン要求に含まれるオペレータ認証情報を照合することで行われる。
FCS_COP.1[2]で使用されるオペレータの証明書は、**FDP_ITC.1** により TSC 内にインポートされ、**FCS_CKM.4** により削除される。オペレータの証明書はオペレータ ID によって管理され **FMT_MSA.2** によりオペレータ ID はセキュアな値だけが受け入れられる。
FDP_ITC.1 により鍵がインポートされる操作、インポートされた鍵で認証する操作は **FDP_ACC.1**、**FDP_ACF.1** によりオペレータアクセス制御 SFP を実施する。
FMT_MSA.1[1]により、使用するセキュリティ属性の管理を可能とし、**FMT_SMR.1**、**FIA.UID.1** によりオペレータを識別し、その役割を維持する。また、**FMT_MSA.3[1]** 、**FMT_MSA.3[4]**により使用するセキュリティ属性のデフォルト値を制限的とする。
FPT_RVM.1 は TOE 利用者識別認証機能が必ず動作することを保証する。なお、妥当性の詳細については補完性にて述べる。

O.CA_AUTH（CA の識別認証）

FIA_UAU.2、**FIA_UID.2** により、CA サーバに対する証明書発行要求・失効要求時に RA サーバによる CA サーバの識別認証が行われ、あらかじめ RA サーバに登録された CA サーバからの応答のみが受け付けられる。

CA サーバの識別認証は、証明書により行われる。CA への証明書の発行・失効の要求時に CA から送信される CMP 応答メッセージに同梱される CMP サーバ証明書が、RA サーバに登録されている CMP サーバ証明書と一致することを確認することにより、CMP サーバを識別する。また、CMP 応答メッセージに付加されるディジタル署名を、**FCS_COP.1[3]**により CMP サーバの証明書で検証することで、CA を認証する。

FCS_COP.1[3]で使用される CMP サーバの証明書は、**FDP_ITC.1** により TSC 内にインポートされ、**FCS_CKM.4** により削除される。CMP サーバの証明書は CAID によって管理されるため **FMT_MSA.2** により CAID はセキュアな値だけが受け入れられる。

FDP_ITC.1 により鍵がインポートされる操作、インポートされた鍵で認証する操作は **FDP_ACC.1**、**FDP_ACF.1** によりオペレータアクセス制御 SFP を実施する。

FMT_MSA.1[1]により、使用するセキュリティ属性の管理を可能とし、**FMT_SMR.1**、**FIA.UID.2** により CA を識別し、その役割を維持する。また、**FMT_MSA.3[1]**により、使用するセキュリティ属性のデフォルト値を制限的とする。

FPT_RVM.1 は CA の識別認証機能が必ず動作することを保証する。なお、妥当性の詳細については補完性にて述べる。

O.PERMISSION（実行権限管理）

FDP_ACC.1、**FDP_ACF.1** により、RA 管理者、監査者、RA 操作者からの操作要求に対してオペレータアクセス制御 SFP を実施し、RA 管理者、監査者、RA 操作者が権限外の操作を行えないように制御する。

FMT_MSA.1[1]により、使用するセキュリティ属性の管理を可能とし、**FMT_SMR.1**、**FIA_UID.1** によりオペレータを識別し、その役割を維持する。また、**FMT_MSA.3[1]**、**FMT_MSA.3[4]**により、使用するセキュリティ属性のデフォルト値を制限される。

FPT_RVM.1 は実行権限管理機能が必ず動作することを保証する。なお、妥当性の詳細については補完性にて述べる。

O.STATUS_FLOW_CONTROL（一般利用者鍵・証明書の状態フロー制御）

FDP_IFC.1、**FDP_IFF.1** により、RA 操作者からの操作要求に対して状態フロー制御 SFP を実施し、一般利用者鍵・証明書の状態を適切に遷移させ、情報の流れを制御する。
FMT_MSA.1[2]により、使用するセキュリティ属性の管理を可能とし、**FMT_SMR.1**、**FIA_UID.1** によりオペレータを識別し、その役割を維持する。また、**FMT_MSA.3[2]**により、使用するセキュリティ属性のデフォルト値を制限的とする。
FPT_RVM.1 は一般利用者鍵・証明書の状態フロー制御機能が必ず動作することを保証する。なお、妥当性の詳細については補完性にて述べる。

O.CIPHER（データの暗号化）
FCS_COP.1[4]により、TSC 内の秘密データが暗号化される。**FCS_COP.1[4]**で使用される鍵は **FCS_CKM.1** により生成され、**FCS_CKM.4** により破棄される。サイト鍵、監査ログ暗号化鍵に関してはセキュリティ属性がサイト ID、鍵番号になるため **FMT_MSA.2** によりサイト ID、鍵番号にセキュアな値だけが受け入れられるよう管理している。
サイト鍵による一般利用者の鍵・証明書、PKCS#12、PIN の暗号操作は **FDP_ACC.1**、**FDP_ACF.1** によりオペレータアクセス制御 SFP を実施する。
FMT_MSA.1[1]により、使用するセキュリティ属性の管理を可能とし、**FMT_SMR.1**、**FIA.UID.1** によりオペレータを識別し、その役割を維持する。また、**FMT_MSA.3[1]**により、使用するセキュリティ属性のデフォルト値を制限的とする。
暗号化に使用するパスワードは **FIA_SOS.1[1]**、**FIA_SOS.1[2]** によりパスワード、シードの強度が十分であることが保証されている。**FIA_SOS.2** によりパスワード生成のメカニズムを提供する。
FPT_RVM.1 はデータの暗号化機能が必ず動作することを保証する。なお、妥当性の詳細については補完性にて述べる。

O.NETWORK_ENCRYPT（暗号通信）

FPT_ITT.1、FDP_ITT.1 により、TOE を構成する各コンポーネント間の通信データを、暴露、及び改変から保護する。データを暗号化するために使用される鍵は **FCS_CKM.1** により生成され、**FCS_CKM.4** により破棄される。通信データは **FCS_COP.1[4]**により暗号化される。

通信データの署名検証は **FCS_COP.1[2]**で行なわれる。署名検証で使用するオペレータの証明書は、**FDP_ITC.1** により TSC 内にインポートされ、**FCS_CKM.4** により削除される。オペレータの証明書はオペレータ ID によって管理され **FMT_MSA.2** によりオペレータ ID はセキュアな値だけが受け入れられる。

FDP_ITC.1 により鍵がインポートされる操作、インポートされた鍵で認証する操作は **FDP_ACC.1、FDP_ACF.1** によりオペレータアクセス制御 SFP を実施する。

FMT_MSA.1[1]により、使用するセキュリティ属性の管理を可能とし、**FMT_SMR.1、FIA.UID.2** によりオペレータを識別し、その役割を維持する。また、**FMT_MSA.3[1]、FMT_MSA.3[4]**により、使用するセキュリティ属性のデフォルト値を制限的とする。

FPT_RVM.1 は**暗号通信**機能が必ず動作することを保証する。なお、妥当性の詳細については補完性にて述べる。

OE.OS_ CORRECT _TIME (OS が提供する時刻)

FPT_STM.1[E]により OS は高信頼タイムスタンプを提供する。以上のセキュリティ機能要件により本セキュリティ対策方針を実現する。

OE.DOMAIN_SEPARATION(OS によるドメイン分離)

FPT_SEP.1[E] により OS はセキュリティドメインを維持し、TSF、及び IT 環境により提供される全てのセキュリティ機能が他の機能の干渉（破壊）を受けることを抑止する。

OE.IC_IA (IC カードによる識別認証)

IC カードは、利用者からのアクセス要求に際して、**FIA_UAU.2[E]**、**FIA_UID.2[E]**によりが識別認証を行い、IC カードの正当な所有者の要求のみを受け付ける。認証の手段としてはパスワードが用いられ、パスワードの強度が十分であることは **FIA_SOS.1[E1]**により保証される。

OE.OS_IA (OS による識別認証)

TOE が動作する上で必要となるマシンの OS は、利用者からのアクセス要求に際して、**FIA_UAU.1[E]**、**FIA_UID.1[E]**により識別認証を行い、正当な所有者の要求のみを受け付ける。認証の手段としてはパスワードが用いられ、パスワードの強度が十分であることは **FIA_SOS.1[E2]**により保証される。

OE.OS_ACCESS _CONTROL(OS によるアクセス制御)

FDP_ACC.1[E]、**FDP_ACF.1[E]**により、OS は利用者からの OS が管理する資源へのアクセス要求に際して、OS アクセス制御を実施する。

FMT_MSA.1[E1]、**FMT_MSA.1[E2]**、**FMT_MSA.1[E3]**により、OS アクセス制御 SFP で使用するセキュリティ属性について操作権限を持つ OS の利用者が、そのセキュリティ属性を管理することを可能とする。また、**FMT_MSA.3[E]**により OS アクセス制御 SFP で使用するセキュリティ属性のデフォルト値を制限的とする。

FMT_MTD.1[E]により、識別された OS の利用者だけに OS が管理するファイルに対する操作を許可し、**FMT_SMR.1[E]**、**FIA_UID.1[E]** によりその役割を維持する。以上のセキュリティ機能要件により本セキュリティ対策方針を実現する。

(3) 補完性

他のセキュリティ機能要件を有効に動作させるための機能要件を表 8-5 に示す。

表 8-5：セキュリティ機能要件の相互支援

コンポーネント	防御を提供するセキュリティ機能要件	
	①迂回	②干渉または破壊
FAU_GEN.1	FPT_RVM.1	FPT_SEP.1[E]
FAU_GEN.2	FPT_RVM.1	FPT_SEP.1[E]
FAU_SAR.1	N/A	FPT_SEP.1[E]
FAU_SAR.2	N/A	FPT_SEP.1[E]
FAU_SAR.3	N/A	FPT_SEP.1[E]
FAU_STG.1	FPT_RVM.1	FPT_SEP.1[E]
FCS_CKM.1	N/A	FPT_SEP.1[E]
FCS_CKM.4	N/A	FPT_SEP.1[E]
FCS_COP.1[1]	N/A	FPT_SEP.1[E]
FCS_COP.1[2]	N/A	FPT_SEP.1[E]
FCS_COP.1[3]	N/A	FPT_SEP.1[E]
FCS_COP.1[4]	N/A	FPT_SEP.1[E]
FDP_ACC.1	FPT_RVM.1	FPT_SEP.1[E]
FDP_ACF.1	FPT_RVM.1	FPT_SEP.1[E]
FDP_IFC.1	FPT_RVM.1	FPT_SEP.1[E]
FDP_IFF.1	FPT_RVM.1	FPT_SEP.1[E]
FDP_ITC.1	FPT_RVM.1	FPT_SEP.1[E]
FDP_ITT.1	FPT_RVM.1	FPT_SEP.1[E]
FIA_SOS.1[1]	N/A	FPT_SEP.1[E]
FIA_SOS.1[2]	N/A	FPT_SEP.1[E]
FIA_SOS.1[3]	N/A	FPT_SEP.1[E]
FIA_SOS.2	N/A	FPT_SEP.1[E]
FIA_UAU.1	FPT_RVM.1	FPT_SEP.1[E]
FIA_UAU.2	FPT_RVM.1	FPT_SEP.1[E]
FIA_UID.1	FPT_RVM.1	FPT_SEP.1[E]
FIA_UID.2	FPT_RVM.1	FPT_SEP.1[E]

コンポーネント	防御を提供するセキュリティ機能要件	
	①迂回	②干渉または破壊
FMT_MSA.1[1]	N/A	FPT_SEP.1[E]
FMT_MSA.1[2]	N/A	FPT_SEP.1[E]
FMT_MSA.2	N/A	FPT_SEP.1[E]
FMT_MSA.3[1]	N/A	FPT_SEP.1[E]
FMT_MSA.3[2]	N/A	FPT_SEP.1[E]
FMT_MSA.3[3]	N/A	FPT_SEP.1[E]
FMT_MSA.3[4]	N/A	FPT_SEP.1[E]
FMT_SMR.1	N/A	FPT_SEP.1[E]
FMT_MTD.1	N/A	FPT_SEP.1[E]
FPT_ITT.1	N/A	FPT_SEP.1[E]
FPT_RVM.1	N/A	FPT_SEP.1[E]
FDP_ACC.1[E]	N/A	FPT_SEP.1[E]
FDP_ACF.1[E]	N/A	FPT_SEP.1[E]
FIA_SOS.1[E1]	N/A	FPT_SEP.1[E]
FIA_SOS.1[E2]	N/A	FPT_SEP.1[E]
FIA_UAU.1[E]	N/A	FPT_SEP.1[E]
FIA_UAU.2[E]	N/A	FPT_SEP.1[E]
FIA_UID.1[E]	N/A	FPT_SEP.1[E]
FIA_UID.2[E]	N/A	FPT_SEP.1[E]
FMT_MSA.1[E1]	N/A	FPT_SEP.1[E]
FMT_MSA.1[E2]	N/A	FPT_SEP.1[E]
FMT_MSA.1[E3]	N/A	FPT_SEP.1[E]
FMT_MSA.3[E]	N/A	FPT_SEP.1[E]
FMT_MTD.1[E]	N/A	FPT_SEP.1[E]
FMT_SMR.1[E]	N/A	FPT_SEP.1[E]
FPT_SEP.1[E]	N/A	FPT_SEP.1[E]
FPT_STM.1[E]	N/A	FPT_SEP.1[E]

N/A：Not Applicable

① 迂回阻止

FPT_RVM.1

FAU_GEN.1、**FAU_GEN.2**、**FAU_STG.1**、**FDP_ACC.1**、**FDP_ACF.1**、**FDP_IFC.1** 、 **FDP_IFF.1** 、 **FDP_ITT.1** 、 **FIA_UAU.1** 、 **FIA_UAU.2** 、**FIA_UID.1**、**FIA_UID.2** の各機能要件は **FPT_RVM.1** により、TOE の各機能の動作進行が許可される前にセキュリティ機構の実施機能（識別機能・識別認証機能である **FIA_UAU.1**・**FIA_UID.1**、アクセス制御機能である **FDP_ACC.1**・**FDP_ACF.1**、状態フロー制御機能である **FDP_IFC.1**・**FDP_IFF.1**）が呼び出され成功することを保証する。

② 干渉または破壊の拒否

FPT_SEP.1 [E]
セキュリティドメインが分離されることにより、全てのセキュリティ機能が他の機能の干渉（破壊）を受けないことを保証する。

(4)　セキュリティ機能要件間の依存関係の検証

セキュリティ機能要件の依存性を表 8-6 に示す。

表 8-6：コンポーネントの依存関係

コンポーネント	依存関係	備考
FAU_GEN.1	FPT_STM.1[E]	
FAU_GEN.2	FAU_GEN.1	
	FIA_UID.1	
FAU_SAR.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	
FAU_SAR.3	FAU_SAR.1	
FAU_STG.1	FAU_GEN.1	
FCS_CKM.1	FCS_COP.1[4]	FMT_MSA.2の依存性に関しては表8-7の１～7参照
	FCS_CKM.4	
	FMT_MSA.2	
FCS_CKM.4	FCS_CKM.1	
	FDP_ITC.1	
	FMT_MSA.2	FMT_MSA.2の依存性に関しては表8-7参照
FCS_COP.1[1]	FCS_CKM.1	使用する鍵はO.CIPHERで生成するため依存性なし
	FCS_CKM.4	使用する鍵はO.CIPHERで破棄するため依存性なし
	FMT_MSA.2	FMT_MSA.2の依存性に関しては表8-7の8参照
FCS_COP.1[2]	FDP_ITC.1	
	FCS_CKM.4	
	FMT_MSA.2	FMT_MSA.2の依存性に関しては表8-7の9,12参照
FCS_COP.1[3]	FDP_ITC.1	
	FCS_CKM.4	
	FMT_MSA.2	FMT_MSA.2の依存性に関しては表8-7の10,11参照
FCS_COP.1[4]	FCS_CKM.1	
	FCS_CKM.4	
	FMT_MSA.2	FMT_MSA.2の依存性に関しては表8-7の１～7参照

コンポーネント	依存関係	備考
FDP_ACC.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1	
	FMT_MSA.3[1] FMT_MSA.3[4]	
FDP_IFC.1	FDP_IFF.1	
FDP_IFF.1	FDP_IFC.1	
	FMT_MSA.3[2]	
FDP_ITC.1	FDP_ACC.1	
	FMT_MSA.3[1] FMT_MSA.3[4]	
FDP_ITT.1	FDP_ACC.1	
FIA_SOS.1[1]	なし。	
FIA_SOS.1[2]	なし。	
FIA_SOS.1[3]	なし。	
FIA_SOS.2	なし。	
FIA_UAU.1	FIA_UID.1	
FIA_UAU.2	FIA_UID.2	上位コンポーネントである
FIA_UID.1	なし。	
FIA_UID.2	なし。	
FMT_MSA.1[1]	FDP_ACC.1	
	FMT_SMR.1	
FMT_MSA.1[2]	FDP_IFC.1	
	FMT_SMR.1	
	FMT_SMR.1	
FMT_MSA.2	FDP_ACC.1	FMT_MSA.2の依存性に関しては表8-7の5,9,10,11,12が対象
	FMT_MSA.1[1] FMT_MSA.1[E3]	
	FMT_SMR.1	
	ADV_SPM.1	

コンポーネント	依存関係	備考
FMT_MSA.3[1]	FMT_MSA.1[1]	
	FMT_SMR.1	
FMT_MSA.3[2]	FMT_MSA.1[2]	
	FMT_SMR.1	
FMT_MSA.3[3]	FMT_MSA.1[E2]	
	FMT_SMR.1	
FMT_MSA.3[4]	FMT_MSA.1[E3]	
	FMT_SMR.1	
FMT_MTD.1	FMT_SMR.1	
FMT_SMR.1	FIA_UID.1 FIA_UID.2	O.CA_AUTH, O.NETWORK_ENCRYPTは FIA_UID.2で代替
FPT_ITT.1	なし。	
FPT_RVM.1	なし。	
FDP_ACC.1[E]	FDP_ACF.1[E]	
FDP_ACF.1[E]	FDP_ACC.1[E] FMT_MSA.3[E]	
FIA_SOS.1[E1]	なし。	
FIA_SOS.1[E2]	なし。	
FIA_UAU.1[E]	FIA_UID.1[E]	
FIA_UAU.2[E]	FIA_UID.2[E]	上位コンポーネントである
FIA_UID.1[E]	なし。	
FIA_UID.2[E]	なし。	
FMT_MSA.1[E1]	FDP_ACC.1[E] FMT_SMR.1[E]	
FMT_MSA.1[E2]	FDP_ACC.1[E]	
	FMT_SMR.1[E]	
FMT_MSA.1[E3]	FDP_ACC.1[E]	
	FMT_SMR.1[E]	
FMT_MSA.3[E]	FMT_MSA.1[E1] FMT_SMR.1[E]	
FMT_MTD.1[E]	FMT_SMR.1[E]	
FMT_SMR.1[E]	FIA_UID.1[E]	
FPT_STM.1[E]	なし。	
FPT_SEP.1[E]	なし。	

表 8-7：FMT_MSA.2 の依存関係の詳細

番号	鍵名　（ ）内の情報で鍵を生成する	対象／目的	セキュリティ属性	説明
1	鍵名なし(RA サーバの鍵・証明書暗号化シード)	RA サーバの鍵・証明書の暗号化及び復号 (F.CIPHER)	なし	RA サーバが固定の鍵で暗号化及び復号するためセキュリティ属性は存在しない。このため FMT_MSA.2 は選択しない。
2	鍵名なし(RA サーバの起動パスワード)	RA サーバの鍵・証明書暗号化シード、RDBMS にアクセスするための認証情報、監査ログ暗号化シードの暗号化及び復号 (F.CIPHER)	なし	RA サーバが固定の鍵で暗号化及び復号するためセキュリティ属性は存在しない。このため FMT_MSA.2 は選択しない。
3	監査ログ暗号化鍵（監査ログ暗号化シード）	監査ログの暗号化及び復号 (F.CIPHER)	鍵番号	RA サーバが鍵番号で管理されている鍵で暗号化及び復号するため、セキュリティ属性は鍵番号である。鍵番号へは RA サーバ、RA セットアップしかアクセスできないため FMT_MSA.2 の依存性は選択しない。
4	鍵名なし（オペレータ登録情報のパスワード）	オペレータ登録情報の暗号化及び復号 (F.CIPHER)	なし	鍵はオペレータ登録時に RA 管理者からオフラインで RA 操作者に渡されるため、TOE では鍵の管理を行わない。このため、セキュリティ属性が存在せず FMT_MSA.2 は選択しない。
5	サイト鍵（乱数）	一般利用者の鍵・証明書、PKCS#12、PIN の暗号化及び復号 (F.CIPHER)	サイト ID	サイト ID で管理されている鍵で暗号化及び復号するためセキュリティ属性はサイト ID である。サイト ID へのアクセスはオペレータアクセス制御 SFP により管理される。
6	RA 鍵	CMP クライアントの鍵・証明書、サイト鍵、監査ログを暗号化するための鍵の暗号化及び復号(F.CIPHER)	なし	RA サーバが固定の鍵で暗号化及び復号するためセキュリティ属性は存在しない。このため FMT_MSA.2 は選択しない。
7	鍵名なし（乱数）	SSL 通信データの暗号化及び復号 (F.CIPHER)	なし	RA サーバと RA コンソール、RA オペレータ間をセッション内でのみ有効な鍵をメモリ上に生成し暗号化及び復号するため、セキュリティ属性は存在しない。このため FMT_MSA.2 は選択しない。

番号	鍵名　（ ）内の情報で鍵を生成する	対象／目的	セキュリティ属性	説明
8	監査ログ暗号化鍵（監査ログ暗号化シード）	監査ログのハッシュ生成・検証 (F.AUDIT.1,F.AUDIT.3)	鍵番号	RA サーバが鍵番号で管理されている鍵で暗号化及び復号するため、セキュリティ属性は鍵番号である。鍵番号へは RA サーバ、RA セットアップしかアクセスできないため FMT_MSA.2 の依存性は選択しない。
9	オペレータ鍵	SSL 通信時の認証 (F.OPERATOR_AUTH)	オペレータ ID	オペレータ ID で管理されている鍵で署名及び署名検証を行うため、セキュリティ属性はオペレータ ID である。オペレータ ID へのアクセスはオペレータアクセス制御 SFP により管理される。
10	CMP サーバ鍵	CA の認証 (F.CA_AUTH)	CAID	CAID で管理されている鍵で署名検証を行うため、セキュリティ属性は CAID である。CAID へのアクセスはオペレータアクセス制御 SFP により管理される。
11	CMP クライアント鍵	CA に対する認証 (F.CA_AUTH)	CAID	CAID で管理されている鍵で署名を行うため、セキュリティ属性は CAID である。CAID へのアクセスはオペレータアクセス制御 SFP により管理される。
12	オペレータ鍵	クライアントの認証 (F.OPERATOR_AUTH)	オペレータ ID	オペレータ ID で管理されている鍵で署名及び署名検証を行うため、セキュリティ属性はオペレータ ID である。オペレータ ID へのアクセスはオペレータアクセス制御 SFP により管理される。

8.2.2 最小機能強度根拠

本 TOE は PKI システムの RA としての役割を果たす。RA では一般利用者の証明書を発行するために鍵ペアを生成し、CA に証明書の発行依頼を行う。発行された証明書と秘密鍵は、その鍵を証明書の申請書以外の者に不正使用されないよう厳重に管理する必要がある。TOE は前提条件に記述されているとおり物理的及び接続的保護されており、不特定のユーザが TOE に対して直接攻撃を行う可能性はなく、TOE を運用する組織に属する者からだけ攻撃される可能性がある。TOE を運用する組織に属する者は TOE を含むソフトウェアの技術機構については熟知していないため、攻撃力は低レベルである。このため、本 TOE は低レベルの攻撃者に対するセキュリティ対策方針を規定しており、最小機能強度レベルは対策方針と一貫している。

8.2.3 保証要件根拠

本 TOE は商用システムの中で利用され、PKI システムの RA を実現するための製品である。RA としてセキュリティ機能には高い信頼性が要求されるが、TOE の運用／管理面からも厳重に保護されたセキュリティが確保されるため、商用システムとして十分なレベルの品質保証レベルが必要である。また、TOE の暗号サポートに関する機能要件からの依存性によって、ADV_SPM.1 が必要である。以上のことから、品質保証レベルを EAL3、ADV_SPM.1 追加とすることは妥当である。

8.3 TOE 要約仕様根拠

8.3.1 TOE セキュリティ要件の根拠

(1) 必要性

TOE のセキュリティ機能と TOE セキュリティ機能要件との適合性を表 8-8 に示す。TOE 要約仕様により、各機能要件が採用されることを表している。

表 8-8：TOE 要約仕様の検証

TOE 要約仕様 / セキュリティ機能要件	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4	F.OPERATOR_AUTH	F.CA_AUTH	F.ACCESS_CONTROL	F.STATUS_FLOW_CONTROL	F.CIPHER.1	F.CIPHER.2	F.CIPHER.3	F.SSL	F.ADMIN
FAU_GEN.1	●												
FAU_GEN.2	●												
FAU_SAR.1		●											
FAU_SAR.2		●											
FAU_SAR.3		●											
FAU_STG.1			●										
FCS_CKM.1									●			●	
FCS_CKM.4					●	●			●			●	
FCS_COP.1[1]	●		●										
FCS_COP.1[2]					●								
FCS_COP.1[3]						●							
FCS_COP.1[4]									●			●	
FDP_ACC.1							●						
FDP_ACF.1							●						
FDP_IFC.1								●					
FDP_IFF.1								●					
FDP_ITC.1					●	●							
FDP_ITT.1												●	

TOE 要約仕様 / セキュリティ機能要件	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4	F.OPERATOR_AUTH	F.CA_AUTH	F.ACCESS_CONTROL	F.STATUS_FLOW_CONTROL	F.CIPHER.1	F.CIPHER.2	F.CIPHER.3	F.SSL	F.ADMIN
FIA_SOS.1[1]										●	●		
FIA_SOS.1[2]										●			
FIA_SOS.1[3]										●			
FIA_SOS.2											●		
FIA_UAU.1					●								
FIA_UAU.2						●							
FIA_UID.1					●								
FIA_UID.2						●						●	
FMT_MSA.1[1]													●
FMT_MSA.1[2]								●					
FMT_MSA.2	●		●		●	●			●				
FMT_MSA.3[1]													●
FMT_MSA.3[2]								●					
FMT_MTD.1		●	●	●			●						
FMT_SMR.1					●		●						
FPT_ITT.1												●	

TOE 要約仕様 / セキュリティ機能要件	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4	F.OPERATOR_AUTH	F.CA_AUTH	F.ACCESS_CONTROL	F.STATUS_FLOW_CONTROL	F.CIPHER.1	F.CIPHER.2	F.CIPHER.3	F.SSL	F.ADMIN
FDP_ACC.1[E]	IT 環境の機能要件により実現される。												
FDP_ACF.1[E]													
FIA_SOS.1[E1]													
FIA_SOS.1[E2]													
FIA_UAU.1[E]													
FIA_UAU.2[E]													
FIA_UID.1[E]													
FIA_UID.2[E]													
FMT_MSA.1[E1]													
FMT_MSA.1[E2]													
FMT_MSA.1[E3]													
FMT_MSA.3[E]													
FMT_MTD.1[E]													
FMT_SMR.1[E]													
FPT_SEP.1[E]													
FPT_STM.1[E]													

(2) 十分性

要約仕様に対応する機能要件を実現する根拠を以下に説明する。なお、SFR のうち機能を定義していないものについては、N/A（Not Applicable）としている。

FAU_GEN.1

FAU_GEN.1.1：TSF は、表 5-2 の監査記録を生成できなければならない。
FAU_GEN.1.2：TSF は監査記録に事象の日付・時刻、事象、事象の結果、サブジェクト識別情報、監査ログレコードの鍵付きハッシュ値、監査ログレコードに割り振られるシーケンス番号を記録しなければならない。

F.AUDIT.1 により、各機能要件で必要な監査要件の日時、詳細情報、結果、オペレータ ID、署名が表 8-9 に示すとおりに記録される。また、表 8-9 で示される各コンポーネントの監査レベルを表 8-10 に示す。監査レベルが CC で要求される最小の監査レベルを満たさないものについては、その正当性の根拠を表 8-10 に示す。
これらの事象が監査ログに書き込まれるとき、**F.AUDIT.1** により監査ログにログ ID が割り付けられる。これにより **FAU_GEN.1** が満たされる。

表 8-9：監査要件を実現する TOE 要約仕様

コンポーネント	要約仕様	コンポーネント	要約仕様
FAU_GEN.1	－	FIA_SOS.1[1]	－
FAU_GEN.2	－	FIA_SOS.1[2]	－
FAU_SAR.1	F.AUDIT.1	FIA_SOS.1[3]	－
FAU_SAR.2	F.AUDIT.1	FIA_SOS.2	－
FAU_SAR.3	－	FIA_UAU.1	F.AUDIT.1
FAU_STG.1	－	FIA_UAU.2	F.AUDIT.1
FCS_CKM.1	－	FIA_UID.1	F.AUDIT.1
FCS_CKM.4	－	FIA_UID.2	F.AUDIT.1
FCS_COP.1[1]	F.AUDIT.1	FMT_MSA.1[1]	F.AUDIT.1
FCS_COP.1[2]	F.AUDIT.1	FMT_MSA.1[2]	F.AUDIT.1
FCS_COP.1[3]	F.AUDIT.1	FMT_MSA.2	－
FCS_COP.1[4]	F.AUDIT.1	FMT_MSA.3[1]	F.AUDIT.1
FDP_ACC.1	－	FMT_MSA.3[2]	F.AUDIT.1
FDP_ACF.1	F.AUDIT.1	FMT_MSA.3[3]	－
FDP_IFC.1	－	FMT_MSA.3[4]	－
FDP_IFF.1	F.AUDIT.1	FMT_MTD.1	F.AUDIT.1
FDP_ITC.1	F.AUDIT.1	FMT_SMR.1	F.AUDIT.1
FDP_ITT.1	－	FPT_ITT.1	－

表 8-10：監査対象事象と監査レベルの対応

コンポーネント	対応する監査レベル	最小レベルを満たさない場合の正当性根拠
FAU_GEN.1	―	―
FAU_GEN.2	―	―
FAU_SAR.1	基本	―
FAU_SAR.2	基本	―
FAU_SAR.3	(最小レベルを満たさない)	監査ログの閲覧は、オペレータ種別、及びサイト ID で制限される。このためオペレータ種別、及びサイト ID は監査対象であるが、その他の閲覧パラメタの監査は不要である。
FAU_STG.1	―	―
FCS_CKM.1	(なし)	鍵の生成は以下の理由のいずれかにより監査は不要である。 ・TOE 内部で暗黙に生成される鍵である ・TOE の運用の前提となる RA セットアップ機能で生成される鍵である ・TOE が提供する他の機能の延長で自動的に生成される鍵であり、他の監査記録に包含される
FCS_CKM.4	(なし)	鍵の廃棄は以下の理由のいずれかにより監査は不要である。 ・TOE 内部で暗黙に破棄される鍵である ・TOE が提供する他の機能の延長で自動的に破棄される鍵であり、他の監査記録に包含される
FCS_COP.1[1]	(なし)	監査ログに対する署名は監査ログの一部であり、監査ログに対する署名の監査は監査ログの採取自体に包含される。
FCS_COP.1[2]	(なし)	オペレータの署名の検証はオペレータのログインの記録に包含される。
FCS_COP.1[3]	(なし)	CMP の署名検証は CA に対する証明書発行・失効要求の成功・失敗の記録に包含される。
FCS_COP.1[4]	(なし)	TOE 内部で暗黙に行われる暗号操作である。
FDP_ACC.1	―	―
FDP_ACF.1	詳細	―
FDP_IFC.1	―	―
FDP_IFF.1	詳細	―

コンポーネント	対応する監査レベル	最小レベルを満たさない場合の正当性根拠
FDP_ITC.1	最小	－
FDP_ITT.1	(なし)	TOE 内での利用者データ転送は、利用者証明書等の取得としてログに記録される。また、保護の方法は常に一定であるため監査は不要である。
FIA_SOS.1[1]	(なし)	TOEが提供する他の機能の延長で使用される機能であり、他の監査記録に包含される。
FIA_SOS.1[2]	(なし)	TOEの運用の前提となるRAセットアップ機能で提供する機能であるため。
FIA_SOS.1[3]	(なし)	TSF が固定の品質尺度で自動的に生成するものであるため不要。
FIA_SOS.2	(なし)	秘密の品質尺度は常に一定であるため監査は不要である。
FIA_UAU.1	最小（注）	－
FIA_UAU.2	(なし)	CA サーバ認証の記録は CA に対する証明書発行・失効要求の成功・失敗の記録に包含される。
FIA_UID.1	最小（注）	－
FIA_UID.2	(なし)	CA サーバ識別の記録は CA に対する証明書発行・失効要求の成功・失敗の記録に包含される。
FMT_MSA.1[1]	基本	－
FMT_MSA.1[2]	基本	－
FMT_MSA.2	(なし)	鍵番号は TOE により内部的に生成される。オペレータ ID、CAID はアクセス制御で保護されるため、セキュアでない値が提示されることはない。
FMT_MSA.3[1]	基本	－
FMT_MSA.3[2]	基本	－
FMT_MSA.3[3]	(なし)	TOE の運用の前提となる RA セットアップ機能で提供する機能であるため。
FMT_MSA.3[4]	(なし)	TOE の運用の前提となる RA セットアップ機能で提供する機能であるため。
FMT_MTD.1	基本	－
FMT_SMR.1	詳細	－
FPT_ITT.1	－	－

（注）これらのログは監査ログではなくエラーログに記録される。

FAU_GEN.2

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なければならない。

F.AUDIT.1 で、当該操作を行った利用者の識別情報として、オペレータ ID、オペレータ種別、サイト ID が監査ログに記録される。これにより **FAU_GEN.2** が満たされる。

FAU_SAR.1

FAU_SAR.1.1：TSF は、監査者に対しては全ての監査情報を、RA 操作者に対しては RA 操作者が属するサイトに関する監査情報を監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2：TSF は、監査者に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。

F.AUDIT.2 により、監査者、及び RA 操作者に対して監査ログを読み出す機能が提供される。読み出された情報は RA コンソール、及び RA オペレータで整列し表示される。これにより **FAU_SAR.1** が満たされる。

FAU_SAR.2

FAU_SAR.2.1：TSF は、明示的に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。

F.AUDIT.2 により、監査者、及び RA 操作者以外のものによる監査ログの参照は抑止される。これにより **FAU_SAR.2** が満たされる。

FAU_SAR.3

FAU_SAR.3.1：TSF は、以下の検索条件を１つまたは複数指定して監査データを検索する機能を提供しなければならない。

- 日付・時刻
- サイト ID
- オペレータ種別
- オペレータ ID
- 要求番号
- 事象
- 処理結果

F.AUDIT.2 には、利用者によって指定される検索条件に従って、監査ログレコードを選択的に取得する機能を提供する。これにより **FAU_SAR.3** が満たされる。

FAU_STG.1

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、格納された監査記録の改変を検出できなければならない。

F.AUDIT.3 は、**F.AUDIT.1** により監査ログレコードに割り付けられた番号の連続性を検査することで、監査ログの不正な削除を検出する。また、**F.AUDIT.3** は、**F.AUDIT.1** により生成された監査ログの鍵付きハッシュ値を検証することにより、監査ログレコードの改変を検出する。これにより **FAU_STG.1** が満たされる。

FCS_CKM.1

FCS_CKM.1.1：TSF は、表 5-5 で示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を生成しなければならない。

F.CIPHER.1 は表 6-12 に示された鍵を生成する機能を提供する。**F.SSL** は暗号アルゴリズムが RC4、鍵長は 128 ビットの鍵を生成する機能を提供する。これにより **FCS_CKM.1** が満たされる。

FCS_CKM.4

FCS_CKM.4.1：TSF は、5.1.1 章の **FCS_CKM.4** で示された暗号破棄方法に従って、暗号鍵を破棄しなければならない。

F.OPERATOR_AUTH はインポートしたオペレータ証明書が不要になった場合、RDBMS から削除する機能を提供する。**F.CA_AUTH** はインポートした CMP サーバ証明書が不要になった場合、RDBMS から削除する機能を提供する。**F.CIPHER.1** は表 6-13 で示される鍵を削除する機能を提供する。**F.SSL** は、使用済みとなった暗号鍵をメモリ上から削除する機能を提供する。これにより **FCS_CKM.4** が満たされる。

FCS_COP.1[1]

FCS_COP.1.1：TSF は、以下に示す鍵により、監査ログデータの鍵付きハッシュを生成、検証しなければならない。

- 暗号アルゴリズム HMAC-SHA1-1,RC2
- 暗号鍵長：128bit

F.AUDIT.1 は、監査ログレコードの格納時に、上記の鍵によりレコードの鍵付きハッシュを生成し、監査ログレコードに付加する機能を提供する。**F.AUDIT.3** は、格納されたログレコードの鍵付きハッシュと現在のログレコードの鍵付きハッシュを検証する機能を提供する。これにより **FCS_COP.1[1]**が満たされる。

FCS_COP.1[2]

FCS_COP.1.1：TSF は、以下に示す鍵により、ディジタル署名の検証を行わなければならない。

- 暗号アルゴリズム：RSAwithSHA-1
- 暗号鍵長：512,1024,2048bit

F.OPERATOR_AUTH は、上記の鍵により、RA コンソール、及び RA オペレータからのログイン要求時に利用者の秘密鍵によるディジタル署名の検証を行う機能を提供する。これにより **FCS_COP.1[2]**が満たされる。

FCS_COP.1[3]

FCS_COP.1.1：TSF は、以下に示す鍵により、ディジタル署名の生成、検証を行わなければならない。

- 暗号アルゴリズム：RSAwithSHA-1
- 暗号鍵長：512,768,1024,2048bit

F.CA_AUTH は、上記の鍵により、CA サーバへの証明書発行要求、及び失効要求時に、CMP サーバからの応答に含まれる CMP サーバの秘密鍵によるディジタル署名の生成、検証を行う機能を提供する。これにより **FCS_COP.1[3]**が満たされる。

FCS_COP.1[4]

FCS_COP.1.1：TSF は、表 5-6 示された鍵により、データの暗号化、及び復号を行わなければならない。

F.CIPHER.1 は表 6-13 に示された暗号操作を行う機能を提供する。**F.SSL** は、暗号アルゴリズムが RC4、鍵長が 128 ビットで通信データの暗号化及び復号を行う機能を提供する。これにより **FCS_COP.1[4]**が満たされる。

FDP_ACC.1

FDP_ACC.1.1：TSF は、5.1.1 章の FDP_ACC.1 で示されたサブジェクト、オブジェクト、サブジェクトとオブジェクト間の操作のリスト対して、オペレータアクセス制御 SFP を実施しなければならない。

F.ACCESS_CONTROL は、表 6-6 で示されたオペレータが表の実行可能な操作のみ実行する機能を提供する。これにより **FDP_ACC.1** が満たされる。

FDP_ACF.1

FDP_ACF.1.1：TSF は、RA 管理者、監査者、RA 操作者からのすべての操作の要求に対して、オペレータ種別、及びサイト ID に基づいてオペレータアクセス制御 SFP を実施しなければならない。

FDP_ACF.1.2：TSF は、制御されたサブジェクトと制御されたオブジェクトの間での操作が許されるかどうか決定するために、表 5-8 のオペレータアクセス規則を実施しなければならない。

FDP_ACF.1.3、FDP_ACF.1.4：N/A

F.ACCESS_CONTROL は、表 6-5 で示されたオペレータを表のオペレータ種別とサイト ID によって管理する。表 6-6 で示されたオペレータ種別が表の実行可能な操作のみ受け付ける機能を提供する。これにより **FDP_ACF.1** が満たされる。

FDP_IFC.1

FDP_IFC.1.1：TSF は、表 5-9 で示されたすべての操作に対して、状態フロー制御 SFP を実施しなければならない。

F.STATUS_FLOW_CONTROL は、**F.ADMIN** で示された RA 操作者が表の状態種別に対して表の操作を行う機能を提供する。これにより **FDP_IFC.1** が満たされる。

FDP_IFF.1

FDP_IFF.1.1：TSF は、表 5-10 で示されたセキュリティ属性に基づいて、状態フロー制御 SFP を実施しなければならない。

FDP_IFF.1.2：TSF は、表 5-11 で示された規則に基づいて、情報の状態遷移を制御しなければならない。

FDP_IFF.1.3、FDP_IFF.1.4、FDP_IFF.1.5、FDP_IFF.1.6：N/A

F.STATUS_FLOW_CONTROL は、**F.ADMIN** で示された RA 操作者が表の状態種別に対して表の操作を行うことにより、表の状態が遷移可能な状態に遷移する機能を提供する。これにより **FDP_IFF.1** が満たされる。

FDP_ITC.1

FDP_ITC.1.1：TSF は、SFP に従って制御され、TSC 外から RA 操作者証明書の発行申請データ、及び CMP サーバ・クライアントの鍵・証明書をインポートするときはオペレータアクセス制御 SFP を実施しなければならない。

FDP_ITC.1.2：TSF は、TSC 外からインポートされるとき、RA 操作者証明書の発行申請データ、及び CMP サーバ・クライアントの鍵・証明書に関連付けられたいかなるセキュリティ属性も無視しなければならない。

FDP_ITC.1.3：N/A

F.CA_AUTH は CMP サーバ・クライアントの鍵・証明書をインポートするときにオペレータアクセス制御 SFP を実施する機能を提供する。

F.OPERATOR_AUTH は RA 操作者証明書の発行申請データをインポートするときにオペレータアクセス制御 SFP を実施する機能を提供する。インポートするときはセキュリティ属性を無視する。これにより **FDP_ITC.1** が満たされる。

FDP_ITT.1

FDP_ITT.1.1：TSF は、利用者データが TOE の分離されたパート間で送られる場合、暴露、改変を防ぐためにオペレータアクセス制御 SFP を実施しなければならない。

F.SSL は RA サーバと RA コンソール及び RA オペレータ間で送られるデータを保護する機能を提供する。これにより **FDP_ITT.1** が満たされる。

FIA_SOS.1[1]

FIA_SOS.1.1：TSF は、パスワード、シードが ASCII コードの 0x20～0x7E で 4 文字以上 8 文字以下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。

F.CHIPER.2 は表 6-13 のオペレータ登録情報のパスワードが ASCII コード 0x20～0x7E の範囲で 4 文字以上 8 文字以下のパスワードで検証する機能を提供する。

F.CHIPER.3 は表 6-14 の監査ログ暗号化シードが ASCII コード 0x20～0x7E の範囲で 4 文字以上 8 文字以下のシードで検証する機能を提供する。

これにより **FIA_SOS.1[1]**が満たされる。

FIA_SOS.1[2]

FIA_SOS.1.1：TSF は、パスワードが ASCII コードの 0x20～0x7E で 6 文字以上 14 文字以下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。

F.CHIPER.2 は表 6-13 の RA サーバの起動パスワードが ASCII コード 0x20～0x7E の範囲で 6 文字以上 14 文字以下のパスワードで検証する機能を提供する。

これにより **FIA_SOS.1[2]**が満たされる。

FIA_SOS.1[3]

FIA_SOS.1.1：TSF は、パスワードが 10 バイトの乱数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。

F.CHIPER.2 は表 6-13 のオペレータ登録用ログインパスワードが 10 バイトの乱数で検証する機能を提供する。これにより **FIA_SOS.1[3]**が満たされる。

FIA_SOS.2

FIA_SOS.2.1：TSF は、15 バイトの乱数で秘密を生成するメカニズムを提供しなければならない。

F.CHIPER.3 は表 6-14 の RA サーバの鍵・証明書暗号化シードを 15 バイトの乱数で生成する機能を提供する。これにより **FIA_SOS.2** が満たされる。

FIA_UAU.1

FIA_UAU.1.1：TSF は、利用者が認証される前に環境設定を許可しなければならない。

FIA_UAU.1.2：TSF は、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認証することを要求しなければならない。

F.OPERATOR_AUTH は、認証を行う前に環境設定及びオペレータ環境設定を行う機能を提供する。RA コンソール、及び RA オペレータからの RA サーバへのログイン要求に際して利用者の認証を実施し、認証された利用者のログインのみを許可する機能を提供する。これにより **FIA_UAU.1** が満たされる。

FIA_UAU.2

FIA_UAU.2.1：TSF は、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認証することを要求しなければならない。

F.CA_AUTH は、CA サーバへの証明書発行・失効要求に際して CA サーバの認証を実施し、認証された CA サーバからの応答のみを受け付ける機能を提供する。これにより **FIA_UAU.2** が満たされる。

FIA_UID.1

FIA_UID.1.1：TSFは、利用者が識別される前に環境設定を許可しなければならない。

FIA_UID.1.2：TSFは、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。

F.OPERATOR_AUTHは、識別を行う前に環境設定及びオペレータ環境設定を行う機能を提供する。RAコンソール、及びRAオペレータからのRAサーバへのログイン要求に際して利用者の識別を実施し、識別された利用者のログインのみを許可する機能を提供する。これにより**FIA_UID.1**が満たされる。

FIA_UID.2

FIA_UID.2.1：TSFは、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。

F.CA_AUTHは、CAサーバへの証明書発行・失効要求に際してCAサーバの識別を実施し、あらかじめRAサーバに登録されたCAサーバからの応答のみを受け付ける機能を提供する。**F.SSL**は、RAサーバとRAコンソール及びRAオペレータ間の通信時にオペレータの識別を実施し、あらかじめRAサーバに登録されたオペレータからの応答のみを受け付ける機能を提供する。これにより**FIA_UID.2**が満たされる。

FMT_MSA.1 [1]

FMT_MSA.1.1：TSF は、オペレータアクセス制御 SFP を実施して、以下のセキュリティ属性に対し改変、削除、作成、設定できる能力を RA 管理者に制限しなければならない。

- RA 操作者のオペレータ種別
- RA 操作者のオペレータ ID
- サイト ID
- CAID

F.ADMIN は表 6-15 で示された RA 操作者のオペレータ種別、RA 操作者のオペレータ ID、サイト ID、CAID に対して RA 管理者だけが改変、削除、作成、設定できる機能を提供する。これにより **FMT_MSA.1 [1]**が満たされる。

FMT_MSA.1 [2]

FMT_MSA.1.1：TSF は、状態フロー制御 SFP を実施して、以下のセキュリティ属性に対し改変、削除、作成できる能力を RA 操作者に制限しなければならない。

- 証明書状態属性
- 鍵状態属性
- 証明書削除状態属性

F.STATUS_FLOW_CONTROL は表 6-11 で示されたセキュリティ属性に対して RA 操作者だけが表の実行可能な操作を行うことができる機能を提供する。これにより **FMT_MSA.1 [2]**が満たされる。

FMT_MSA.2

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

F.AUDIT.1 は監査ログ暗号化鍵が鍵番号で管理されており、RA サーバのみアクセスすることにより、セキュアな値のみ与える機能を提供する。

F_OPERATOR_AUTH はオペレータ証明書を識別するオペレータ ID をアクセス制御で管理することにより、セキュアな値のみ与える機能を提供する。

F_CA.AUTH は CMP サーバ証明書を識別する CAID をアクセス制御で管理することにより、セキュアな値のみ与える機能を提供する。**F.CIPHER.1** は表 6-14 で示すセキュリティ属性を管理することにより、セキュアな値のみ与える機能を提供する。これにより **FMT_MSA.2** が満たされる。

FMT_MSA.3 [1]

FMT_MSA.3.1：TSF は、オペレータアクセス制御 SFP を実施するセキュリティ属性に対して、制限的なデフォルト値を許可しなければならない。

FMT_MSA.3.2：N/A

F.ACCESS_CONTROL はオペレータ登録時に表 6-5 で示されるオペレータ種別、サイト ID に対して制限的なデフォルト値を与える機能を提供する。これにより **FMT_MSA.3[1]**が満たされる。

FMT_MSA.3 [2]

FMT_MSA.3.1：TSF は、状態フロー制御 SFP を実施するセキュリティ属性に対して、制限的なデフォルト値を許可しなければならない。

FMT_MSA.3.2：N/A

F.STATUS_FLOW_CONTROL はサイト登録時に表 6-8 で示される制限的なデフォルトの状態フロー制御情報を与える機能を提供する。これにより **FMT_MSA.3[2]**が満たされる。

FMT_MSA.3 [3]

FMT_MSA.3.1：TSF は、オペレータアクセス制御 SFP を実施するセキュリティ属性に対して、1 から始まるシーケンシャルな番号を許可しなければならない。

FMT_MSA.3.2：N/A

F.ADMIN は暗号鍵登録時に鍵番号が 1 から始まる数字を与える機能を提供する。これにより **FMT_MSA.3[3]**が満たされる。

FMT_MSA.3 [4]

FMT_MSA.3.1：TSF は、オペレータアクセス制御 SFP を実施するセキュリティ属性に対して、制限的なデフォルト値を許可しなければならない。

FMT_MSA.3.2：N/A

F.ADMIN はオペレータ登録時に表 6-16 で示されるオペレータ種別に対して制限的なデフォルト値を与える機能を提供する。これにより **FMT_MSA.3[4]**が満たされる。

FMT_MTD.1

FMT_MTD.1.1：TSF は、RA 管理者、RA 操作者、監査者が、「表 5-14：TSF データの管理」で示された操作のみを実行できるように制限しなければならない。

F.AUDIT.2 は監査者、RA 操作者のみが監査ログを参照できる機能を提供する。**F.AUDIT.3** は監査者のみが監査ログの検証を行う機能を提供する。**F.AUDIT.4** は監査者のみが監査ログの削除を行う機能を提供する。**F.ACCESS_CONTROL** は RA 管理者、RA 操作者、監査者が実行可能な操作を「表 6-6：オペレータが実行可能な操作」に示されたもののみに制限する。これにより **FMT_MTD.1** が満たされる。

FMT_SMR.1

FMT_SMR.1.1：TSF は、RA 管理者、RA 操作者、監査者の役割を維持しなければならない。

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

F.OPERATOR_AUTH,F.ACCESS_CONTROL は RA 管理者、RA 操作者､監査者という役割を識別する機能を提供する。これにより **FMT_SMR.1** が満たされる。

FPT_RVM.1

FPT_RVM.1.1：TSF は以下の①～④について、どの TOE 外部インタフェースからアクセスが要求されたとしても、必ず識別認証のセキュリティ機能が動作することを保証しなければならない。

① RA コンソール、RA オペレータが IC カードにアクセスするインタフェース
② RA コンソール､RA オペレータが RA サーバにアクセスするインタフェース
③ RA サーバが RDBMS にアクセスするインタフェース
④ RA サーバが CA サーバにアクセスするインタフェース

②では、RA コンソール、及び RA オペレータからのログイン要求に際して、**F.OPERATOR_AUTH** による TOE 利用者の識別認証が行われる。

④では、RA サーバから CA サーバへの証明書発行・失効要求に対する応答受信時に、**F.CA_AUTH** による CA サーバの識別認証が行われる。

①の IC カード､③の RDBMS は信頼できるサブジェクトであり､これらから TOE を利用するアクセス経路はないため、利用者を識別認証する必要はない。これにより **FPT_RVM.1** が満たされる。

FPT_ITT.1

FPT_ITT.1.1：TSF は、TSF データが TOE の別々のパーツ間で送られる場合、TSF データを暴露、改変から保護しなければならない。

F.SSL は SSL を使用し、TOE の別々のパーツ間で送られる TSF データを改変、暴露から保護する機能を提供する。これにより **FPT_ITT.1** が満たされる。

8.3.2 セキュリティ機能強度主張の根拠

本 ST のセキュリティ機能強度については、低レベルの攻撃力を持つ攻撃者による侵害に対して適切に対抗できる SOF-基本を 5.1.2 で規定し、これに基づく TOE セキュリティ機能を 6.2 で F.CIPHER.2 のパスワードメカニズムであると記述している。攻撃力は低レベルであるため、セキュリティ機能としても低レベルな防御を備えている必要がある。セキュリティ機能強度のレベルの主張は、確率的または順列的メカニズムを適用するセキュリティ機能に適用される。

F.CIPHER.2 の「RA サーバの起動パスワード」はセキュリティルーム内でシステム管理者が設定し、RA サーバが使用するため TOE が実装する強度で対抗できる。F.CIPHER.2 の「オペレータ登録情報のパスワード」はオペレータ登録情報にアクセスするためのパスワードである。オペレータ登録情報は OE.EXPORTED により適切に管理されているため、パスワードの強度は TOE が実装する強度で対抗できる。以上の理由により、セキュリティ機能強度主張は満たされる。

8.3.3 保証手段根拠

表 6-17 に示すように、セキュリティ保証要件は全て保証手段により示されたドキュメントのセットによって対応づけられる。また保証手段に示されたドキュメントによって、本 ST が規定したセキュリティ保証要件が要求する証拠を網羅している。TOE の外部インタフェース、及び内部インタフェースを識別するための機能仕様書や構成仕様書、PKI Management Program サーバパッケージ README、PKI Management Program クライアントパッケージ README や PKI Management Program ソフトウェア添付資料によるセキュリティ機能の分析を行うことによって保証を提供する。また配付規定書によるセキュアな配付手続きを通して保証を提供する。以上の理由により、保証手段は満たされる。

8.4 PP 主張根拠

本 ST では、準拠する PP はない。