SystemWalker/PkiMGR CA

セキュリティターゲット

第1.8版

2004**年**4**月**9**日**

富士通株式会社

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	2002.10.18	初版	全般
第1.1版	2002.12.25	所見（ASE-001-01～ASE-017-01）に対する修正。	1章～3章
第1.2版	2003.01.15	所見（ASE-018-01～ASE-040-01、ASE-003-02、ASE-009-02～ASE-012-02）に対する修正。	1章～4章
第1.3版	2003.01.28	所見（ASE-041-01～ASE-063-01、ASE-010-03、ASE-030-02、ASE-033-02）に対する修正。	5章～8章
第1.4版	2003.05.23	所見（ASE-10-04、ASE-030-03、ASE-064-01～ASE-069-01、ASE-041-02 、 ASE-053-02 、 ASE-054-02 、 ASE-063-02 、ASE-070-01～ASE-073-01）に対する修正。	全般
第1.5版	2003.09.24	所見（ASE-074-01～ASE-083-01）に対する修正。	全般
第1.6版	2003.12.27	所見（ASE-084-01～ASE-089-01）に対する修正。	全般
第1.7版	2004.03.09	プラットフォーム依存の記述に対する修正。	全般
第1.8版	2004.04.09	所見（ASE-090-01～ASE-091-01）に対する修正。	全般

目次

図目次

表目次

1　ST概説

1.1　ST識別

(1)　ST識別

- 名称　：　「SystemWalker/PkiMGR CAセキュリティターゲット」
- バージョン　：　第1.8版
- 作成日　：　2004年04月09日
- 作成者　：　富士通株式会社

(2)　TOE識別

本STは、以下の製品に対応する。

- 製品名称　：　SystemWalker/PkiMGR
　　：　SystemWalker/PkiMGR Key Protection Option
- バージョン／リリース番号　：　Windows版：V10.0 L20
　　Solaris(TM) Operating Environment版：10.1
　　（以降、Solaris OEと記述）
- 作成者　：　富士通株式会社

1.2　ST概要

証明書を使用した認証システムを実現するPKIにおいて、その証明書を発行するCA（認証局, Certification Authority）は最も信頼されるべきものでなければならない。したがって、CAのセキュリティが保証されないものであれば、PKIシステム全体のセキュリティを低下させることになってしまう。そのためCAは、強固なセキュリティ環境とセキュリティ機能によって、様々な脅威から保護されることが要求される。

そこで本STでは、PKIシステムの基盤製品であるSystemWalker/PkiMGR（以降SW/PkiMGRと記述）を利用したCAについて、そのセキュリティの安全性、及び堅牢性を証明する。

本STは、SW/PkiMGRを利用したCAを運用するに当たってのセキュリティ環境の分析、セキュリティ問題への対策、ISO/IEC15408に基づく機能要件の適用、製品のセキュリティ機能の概説、またその必要性と十分性の証明について、以下のように構成した文書である。

1章　ST概説：本STについて概説する。

2章　TOE記述：セキュリティ評価の対象範囲をTOEとして定義し、その機能について解説する。

3章　TOEセキュリティ環境：セキュリティ前提条件、脅威について解説する。

4章　セキュリティ対策方針：3章で規定した脅威に対して、TOEとその環境で実現する対策方針について解説する。

5章　ITセキュリティ要件：4章で規定した対策方針を実現するために必要となるISO/IEC15408 パート2 セキュリティ機能要件を選択し、決定すべき事項を具体化する。また、評価保証

レベルとそれに対応するISO/IEC15408パート3 セキュリティ保証要件を示す。

6章　TOE要約仕様：TOEにおけるセキュリティ機能について解説する。

7章　PP主張：PPを適用していないため、記述しない。

8章　根拠：3章から6章で規定したセキュリティ対処により、TOEがセキュリティを維持できることを必要性と十分性の観点から実証する。

SW/PkiMGRが実現するCAは、以下のセキュリティ機能を持つ。

- 識別機能・識別認証機能
  TOE利用者を識別する機能、または識別認証する機能。
- アクセス制御機能・合議制アクセス制御機能
  操作権を持つTOE利用者だけに操作を許可するアクセス制御機能、及び複数人のTOE利用者の合意をアクセス許可条件とするアクセス制御機能。
- 監査機能
  監査ログを記録し、それを参照する機能。

1.3 CC適合

- 機能要件

・ 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 1999年8月 バージョン2.1 CCIMB-99-032（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュリティセンター）適合。

- 保証要件

・ 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 1999年8月 バージョン2.1 CCIMB-99-033（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュリティセンター）追加。

・ 評価保証レベルEAL3 追加。追加する要件はADV_SPM.1。

1.4 参照資料

- Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model Version 2.1 August 1999 CIMB-99-031
- Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements Version2.1 August 1999 CCIMB-99-033
- 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 1999年8月 バージョン2.1 CCIMB-99-031（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュリティセンター）
- 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 1999年8月 バージョン2.1 CCIMB-99-032（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュ

リティセンター）

- 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 1999年8月 バージョン2.1 CCIMB-99-033（平成13年1月翻訳第1.2版 情報処理振興事業協会 セキュリティセンター）
- JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部：総則及び一般モデル
- JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部：セキュリティ機能要件
- JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部：セキュリティ保証要件
- ISO/IEC 15408-1:1999 情報技術－セキュリティ技法－ITセキュリティのための評価基準 パート1：概説と一般モデル
- ISO/IEC 15408-2:1999 情報技術－セキュリティ技法－ITセキュリティのための評価基準 パート2：セキュリティ機能要件
- ISO/IEC 15408-3:1999 情報技術－セキュリティ技法－ITセキュリティのための評価基準 パート3：セキュリティ保証要件

1.5 用語

(1) CC略語・一般用語

公開鍵 ： 公開鍵暗号方式で使用する鍵ペアのうち、一般に公開される鍵。

証明書 ： X.509に従い発行した公開鍵証明書。公開鍵証明書は利用者の公開鍵を保証するために、CAがディジタル署名をしたもの。

申請書 ： 証明書の発行をCAに申請する時に使用するものであり、PKCS#10で規定された形式で作成される。証明書の利用者の名前、公開鍵、利用者のディジタル署名等の情報が格納されている。申請を受けたCAは、利用者のディジタル署名を検証し、有効であれば申請書の情報に基づき証明書を発行する。

相互認証証明書 ： 2つのCAが互いの信頼を証明するために認証し合うことを相互認証という。公開鍵を認証するために2つのCAは互いに相手の証明書（相互認証証明書）を発行する。相互認証証明書は証明書と同じ形式である。

ハッシュ ： 与えられた原文から固定長の疑似乱数を生成する演算手法。

秘密鍵 ： 公開鍵暗号方式で使用する鍵ペアのうち、一般に公開されない鍵。

ディジタル署名 ： メッセージの受信時に、そのメッセージの送信者を確認する手段。

ANSI ： American National Standards Institute：米国規格協会。工業分野での自発的な規格の統一と標準化を行なう。米国の各種団体が定めた規格を審議し、承認するのが主な目的。

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。
CC	：	Common Criteria：コモンクライテリア。
CM	：	Configuration Management：構成管理。
CMP	：	Certificate Management Protocol：証明書の発行や管理に関するRFC2510で定義されるプロトコル。証明書の発行や失効の要求、及びそれらに対する応答等を行う場合に送信するメッセージの形式を定義。
CRL	：	Certification Revocation List：証明書失効リスト。失効したX.509証明書のリストにCAがディジタル署名をしたもの。
EAL	：	Evaluation Assurance Level：評価保証レベル。
FIPS	：	Federal Information Processing Standard：米国連邦政府情報処理標準。
HSM	：	Hardware Security Module：秘密鍵を管理するために使用する物理的な攻撃に強い耐タンパー性ハードウェア。
HTTPS	：	WWWブラウザとWWWサーバ間のデータ送受信に使用するプロトコルであるHTTPに、SSLのデータ暗号化機能が付加されたプロトコル。
PCIバス	：	Peripheral Component Interconnect Bus。拡張スロットの規格のひとつであるローカルバス規格。
PIN	：	ICカードにアクセスするためのパスワード。
PKCS	：	Public Key Cryptography Standards：RSA Securityが開発した公開鍵暗号方式の業界標準。 ● PKCS#1は、「RSA暗号を使用した暗号化方法と署名方法」についての規格。 ● PKCS#5は、「パスワードから生成した秘密鍵を使用した暗号化方法」についての規格。 ● PKCS#10は、「証明書の申請構文に関する標準」（CAに証明書の発行を依頼する時の申請書の形式）についての規格。 ● PKCS#11は、「暗号インタフェース」についての規格。 ● PKCS#12は、「個人情報交換構文に関する標準」（証明書とその秘密鍵を暗号化して格納する形式）についての規格。
PKI	：	Public Key Infrastructure：公開鍵暗号方式によるセキュリティ基盤。証明書を使用して通信データ交換を暗号化したり、通信データにディジタル署名を付加したりする場合の基盤となるもの。
PP	：	Protection Profile：プロテクションプロファイル。
RA	：	Registration Authority：登録局。証明書の発行や失効の申請を審査する等、一般利用者とCAの間において証明書管理を行う。
RDBMS	：	Relational DataBase Management System：「リレーショナルデータモデル」によりデータを管理するデータベース管理システム。

RFC	：	Request for Comments：インターネットに関する技術情報や仕様、運用規則等を規定した文書。IETF（Internet Engineering Task Force）が管理。
RSA	：	Ron Rivest、Adi Shamir、Len Adlemanが提案した暗号化とディジタル署名に使用する公開鍵暗号アルゴリズム。
SFP	：	Security Function Policy：セキュリティ機能方針。
SHA-1	：	Secure Hash Algorithm：ハッシュ関数の一つ。
Shamir 閾値秘密分散法	：	Adi Shamirによる閾値秘密分散法。秘密分散法では秘密情報からn個の分散情報を作成し、n個のうち任意のk個を集めれば元の秘密情報を復元できる。
SOF	：	Strength of Function：機能強度。
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であり、サーバ・クライアント間における双方向の証明書による認証、暗号通信を可能にする。
ST	：	Security Target：セキュリティターゲット。
TOE	：	Target Of Evaluation：評価対象。
Triple-DES	：	DES（Data Encryption Standard：米国商務省／NIST（National Institute of Standards and Technology）で標準として採用される共通鍵暗号方式）を三重に適用する方式。同じ方式を三重に適用することでDESより強度が高められている。
TSF	：	TOE Security Functions：TOEセキュリティ機能。
X.509	：	ITU-Tが勧告した証明書とCRLの標準仕様。（ITU-T（International Telecommunication Union-Telecommunication sectorはITU（国際電気通信連合）の下部組織であり、通信関係の標準化を担当。）

(2)　ST**定義用語**

本STで定義する用語を以下に説明する。

合議制	：	操作毎に予め決められている必要最小人数（2～10人）分のCAオペレータの合意に基づいてCAサービスを操作する仕組み。
プロファイル	：	発行する証明書・CRLの形式についての情報で、利用目的に応じて決める。証明書プロファイルはディジタル署名のアルゴリズム、証明書の有効期間、拡張情報について、CRLプロファイルはCRLの発行間隔、ディジタル署名のアルゴリズム、拡張情報について各々決めたもの。
CA監査端末	：	監査者が監査作業を行う端末。
CAサーバマシン	：	CAサービスを運用するサーバマシン。
CAサービス	：	CAを実現するソフトウェア製品が提供するサービス。
CA操作端末	：	CAオペレータがCAサービスの運用を行う端末。

CMPサービス	：	CMPによりデータの送受信を行うCMPサーバが提供するサービス。CAサービスは本サービスを使用してRAサービスと通信する。
RA管理／監査端末	：	RA管理者やRAの監査者が操作する端末であり、RAサービスの運用環境の設定と監査を実施する。
RAサーバマシン	：	RAを実現するサービスを運用するサーバマシン。
RAサービス	：	RAを実現するソフトウェア製品が提供するサービス。
RA設定端末	：	RAのシステム管理者が操作する端末であり、RAサービスの初期設定、及びRA管理者やRAの監査者の登録を行う。
RA操作端末	：	一般利用者の証明書の発行や失効の操作を行う。また発行された証明書の取得を行う。
TOEクライアント操作端末	：	CA監査端末とCA操作端末の総称。
WWWサービス	：	WWWサーバが提供するサービス。

2　TOE記述

2.1　TOEの特定

2.1.1　TOEの種別

本STにおけるTOEは、CA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システムを構築するための基盤製品であるSW/PkiMGRは、CAサービスの基本機能を提供するSW/PkiMGRのCA機能（以降、SW/PkiMGR CAと記述）とRA（登録局, Registration Authority）サービスを提供するSW/PkiMGRのRA機能（以降、SW/PkiMGR RAと記述）から構成される。またCAサービスの拡張機能を提供するSW/PkiMGR Key Protection Option（以降、SW/PkiMGR KPOと記述）により、更に高度なセキュリティ環境での運用が可能となる。図2-1の太枠内で示すようにTOEは、SW/PkiMGR CAとSW/PkiMGR KPOにより実現するCAサービスである。

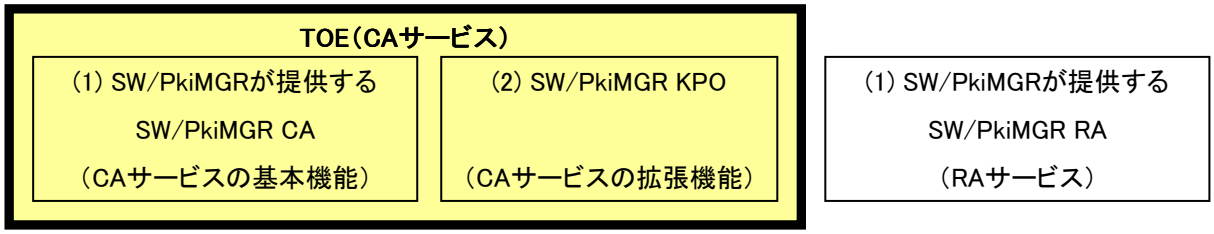

図 2-1：TOEの製品構成

(1)　SW/PkiMGRが提供する機能

- SW/PkiMGR CA（CAサービスの基本機能）
  証明書の発行・失効とそれらに付随するCAサービス。
- SW/PkiMGR RA（RAサービスの機能）
  証明書の発行・失効の申請窓口とそれらに付随するRAサービス。

(2)　SW/PkiMGR KPO（CAサービスの拡張機能）

- 合議制アクセス制御機能
  CAサービスの作業の中において、セキュリティ上非常に重要な作業に対して実施する合議制アクセス制御。
- CA秘密鍵管理機能
  ハードウェアセキュリティモジュール（Hardware Security Module：以降、HSMと記述）におけるCAサービスの秘密鍵（以降、CA秘密鍵と記述）の管理。

2.1.3　TOEの動作環境

TOEは図2-2の太枠内であり、図2-2に示す環境で動作する。点線内は1つの筐体（CAサーバマシン）、網掛けはセキュアゾーンを表す。また①～③はTOEのクライアントである。

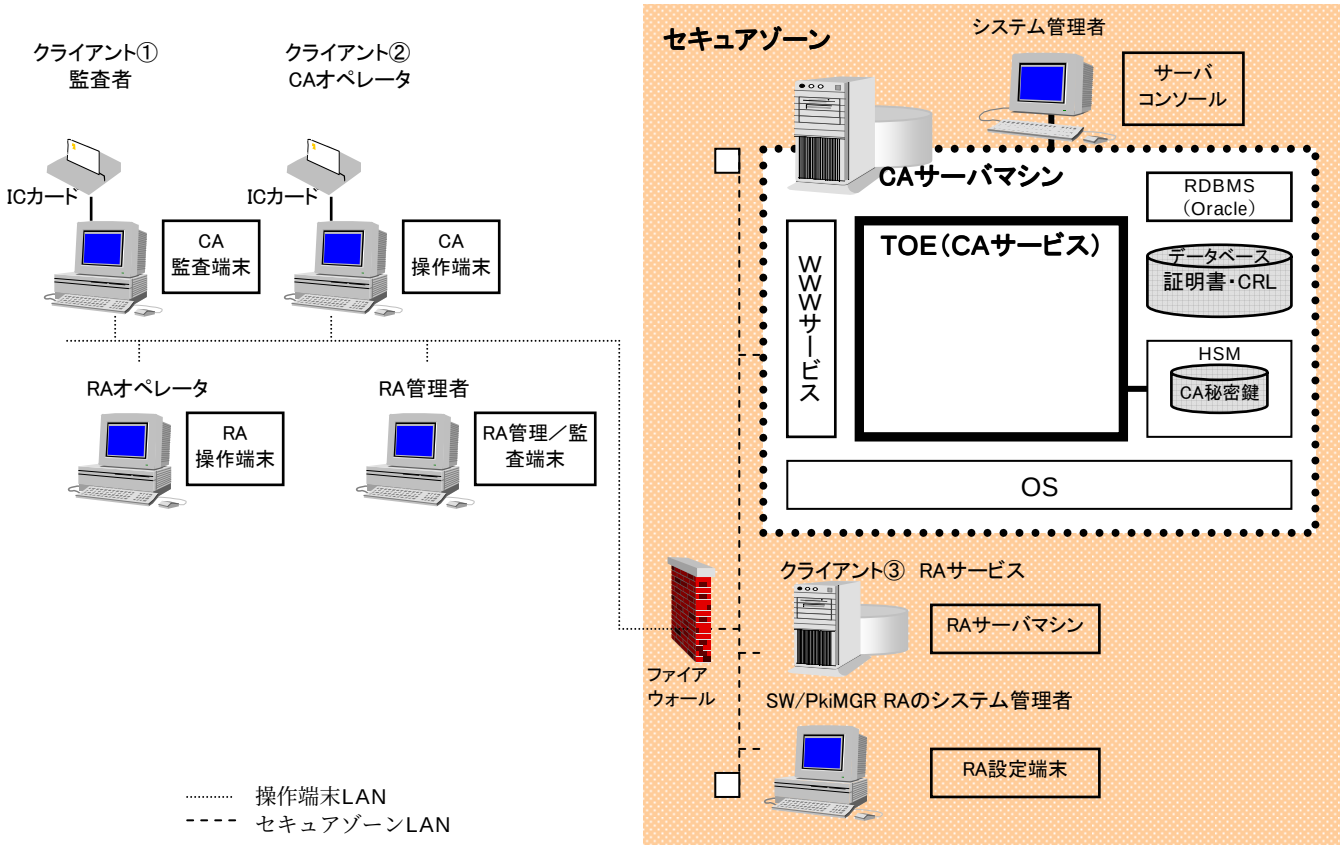

図 2-2：TOEの動作環境

監査者が作業する端末（以降、CA監査端末と記述）、CAオペレータが作業する端末（以降、CA操作端末と記述）の2つの端末を「TOEクライアント操作端末」と呼び、これらはTOEを運用する組織に属する者だけが物理的にアクセスすることができる場所に設置される。なお、CA監査端末、CA操作端末はそれぞれ1台ずつ配置し、監査者、CAオペレータは各々の役割に応じた端末を複数人で共用する。RA管理者が作業する端末（以降、RA管理／監査端末と記述）、RAオペレータが作業する端末（以降、RA操作端末と記述）はSW/PkiMGR RA操作端末であり、これらからの操作は必ずセキュアゾーン内のRAサービスに対して行われる。

セキュアゾーンはファイアウォールにより保護されたネットワークに接続され、かつ入退室管理により物理的に保護、隔離された専用区域であり、運用に必要となる機器以外の持込は制限されている。セキュアゾーンにはCAサーバマシン、RAサーバマシン、RA設定端末等が配置され、CAサーバマシンにはサーバコンソールが接続される。RAサービスはSW/PkiMGR RA操作端末からの一般利用者証明書の発行・失効の申請を中継、処理するサービスである。RA設定端末はRAサービスの設定を行うための端末であり、SW/PkiMGR RAのシステム管理者だけが操作することができる。サーバコンソールはCAサーバマシンに付属のキーボードとディスプレイであり、SW/PkiMGR CA

のシステム管理者（以降、システム管理者と記述）がCAサービスの運用環境の構築とバックアップを行うためのものである。

WWWサービス、RDBMSはCAサーバマシンにインストールされる。CAサーバマシン内のTOEを含むソフトウェアは、オペレーティングシステム（以降、OSと記述）上で動作する。HSMはCA秘密鍵を管理するための物理的な攻撃に強い耐タンパー性のハードウェアであり、CAサーバマシンにはPCIバスで接続される。図2-2はHSMに表2-1の富士通製 暗号プロセッサカードを使用した場合であり、CHRYSALIS-ITS Inc.製 LUNA(R) CA3を使用する場合は、HSM本体がCAサーバマシンの筐体外（セキュアゾーン内）に設置され、CAサーバマシンとは専用のケーブルで接続される。

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。特例としてHSMで管理するCA秘密鍵のバックアップ作業のため、CAオペレータがセキュアゾーンに入室することがあるが、その場合には必ずシステム管理者と共に入室し、システム管理者の監視の下、システム管理者と共同で作業を行う。システム管理者は、CAサーバマシンと同一筐体内の各構成要素とCAサーバマシンに接続されるセキュアゾーン内の機器に対して適切な設定、管理を行う。またCAサーバマシン以外の各サーバマシンの管理者（以降、他サーバマシン管理者と記述）はシステム管理者同様、各々のサーバマシンに対して適切な設定、管理を行う。

セキュアゾーン内のネットワーク（以降、セキュアゾーンLANと記述）はファイアウォールを介してTOEクライアント操作端末、SW/PkiMGR RA操作端末が接続されているセキュアゾーン外のネットワーク（以降、操作端末LANと記述）に接続される。操作端末LANからCAサービスへのアクセス要求に対しては、ファイアウォールにより特定のポートに対してTOEクライアント操作端末からのパケットだけが通過できるように保護されている。

(1)　動作条件

TOEは、表2-1のハードウェア、及び表2-2のソフトウェアに示す条件で動作する。

表 2-1：ハードウェア構成

種類	説明
CPU	Windows版：Intel® Pentium® III 500MHz相当以上。 Solaris OE版：Sun Microsystems, Inc.UltraSPARC® II 400MHz相当以上。
メモリ	512MB以上。
ディスク	証明書の発行枚数が100枚までの場合、200MB以上。 100枚を超える場合、上記に加え証明書1枚につき200KB必要。
HSM	PKCS#11v2.01に準拠したインタフェースを実装する以下の何れか。 ● 富士通製 暗号プロセッサカード ● CHRYSALIS-ITS Inc.製 LUNA(R) CA3

表 2-2：ソフトウェア構成

種類	説明
OS	Windows版：Microsoft® Windows® 2000 Server + Service Pack 3 Solaris OE版：Sun Microsystems, Inc Solaris (TM) 8 Operating Environment
WWWサービス	同梱されるWWWサービス（InfoProvider Pro）
データベース	Oracle Database 8i Release 8.1.7.0.0 または Oracle9i Database Release 2

2.1.4　利用目的と利用方法

(1)　利用目的

- TOEは、一般利用者のために証明書を発行する。
- TOEは、発行した証明書を失効し、CRLを発行する。
- TOEは、発行した証明書とCRLを管理する。

(2)　TOEの関連者及び関連サービス

TOEは、表2-3に示す関連者を想定する。

表 2-3：TOEの関連者

役割	人数	特性
TOEを運用する組織の責任者	特定少数	TOEを運用する組織に属し、TOEクライアント操作端末へのアクセス可。監査者とCAオペレータは、各々の操作端末を複数人で共用する。なおシステム管理者と他サーバマシン管理者は、サーバコンソールへのアクセスも可。
システム管理者	CAサーバマシンに1人	
監査者	CAサービスに複数人	
CAオペレータ	CAサービスに複数人	
他サーバマシン管理者	特定少数	
TOEを運用する組織に属する第三者 （以降、組織内第三者と記述）	特定多数	
RAサービス	運用に依存	TOEを運用する組織に属するが、TOEクライアント操作端末へアクセス不可。
一般利用者	特定多数	TOEを運用する組織に属さず、TOEクライアント操作端末へもアクセス不可。
TOEを運用する組織に属さない第三者 （以降、組織外第三者と記述）	不特定多数	

表2-3の「役割」について説明する。

- **TOEを運用する組織の責任者**

TOEのセキュアな運用に関する責任を持つ。

- **システム管理者**

TOEとそのセキュアな運用環境の管理に関する役割を持つ。OSの管理者でもある。CAサービスの運用環境の構築とバックアップを主業務とする。システム管理者が行う運用環境の構築作業とは、CAサーバマシンとその構成要素であるWWWサービス、RDBMS、HSMやCAサーバマシンに接続される機器（サーバコンソールやHSM本体）の適切な設定と管理であり、それにはSSLクライアント認証に必要なCA証明書をWWWサービスに登録する作業、TOEの識別認証に必要な監査者証明書やRA証明書をTOEに登録する作業も含まれる。システム管理者が行うバックアップ作業は、運用環境が壊れた場合の復旧手段の確保を目的としており、CAサーバマシンのソフトウェア環境をOSの機能レベルで定期的にバックアップするものである。但しCA秘密鍵のバックアップ作業についてだけは、CAオペレータと共同で実施する。またシステム管理者は、バックアップデータが格納された媒体の管理も行う。何らかの不具合により運用環境が壊れた場合には、この媒体を使用して運用環境を復旧する。

- **監査者**

TOEのCA監査端末から監査を実施する役割を持つ。監査者の主業務は以下であり、これらはOSの機能レベルでファイルに直接アクセスして行うものではなく、CA監査端末から2.1.5(2)⑦で説明する監査機能を利用して行うものである。

・TOEが記録した監査ログを追跡し、不正がないか確認する。
・監査ログは肥大化していくものであるため、古くなったログを長期的に保管しておくことを目的として、CAサーバマシン上から外部媒体へ移出し、移出したログをCAサーバマシン上から削除する。また外部媒体にしか存在しない監査ログを使用する必要がある場合には、ログを外部媒体からCAサーバマシン上へ移入する。

また監査者は、監査ログを移出した媒体の管理も行う。

- **CAオペレータ**

TOEの運用を管理する役割を持つ。CAオペレータの主業務は以下であり、これらはCA操作端末から2.1.5(2)①～④で説明するCA管理機能を利用して行うものである。ただし、CAオペレータの業務は、オペレーションが主であるため、TOEを含むソフトウェアの技術機構は熟知していない。

なおCAオペレータはTOEにとって重要な役割を担うため、その役割に関連する識別認証情報やアクセス制御情報はTOE内で秘匿される。

・証明書とCRLを発行する。
・発行した証明書とCRLをデータベースで管理する。
・CA秘密鍵を活性化・非活性化する。
・CA秘密鍵をバックアップする。

● **他サーバマシン管理者**

セキュアゾーンに設置されるCAサーバマシン以外のサーバマシンのシステム管理者（RAのシステム管理者等）。

● **組織内第三者**

TOEクライアント操作端末へアクセスできるが、TOEの管理・監査・運用に関する権限や役割を持たない。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いない。

なお、組織内第三者には、RAオペレータとRA管理者も含まれる。

- RAオペレータ：一般利用者からの証明書の発行・失効の申請を受け、RAサービスにそれを依頼する。
- RA管理者：RAサービスの運用環境の設定と監査を実施する。

● **RAサービス**

一般利用者からの証明書の発行や失効の申請に基づいてRAオペレータから行われる依頼を受け、TOEに対し証明書の発行や失効を要求する。

● **一般利用者**

RAオペレータからの依頼に基づいてTOEが発行した証明書の利用者。一般利用者証明書はRAオペレータから配付される。CA証明書とCRLはこれらが格納されているディレクトリサーバマシンに一般利用者自身がアクセスし取得する。

● **組織外第三者**

CA監査端末やCA操作端末等、TOEに関連するいかなる操作端末に対してもアクセスできない。CAサービスを享受しないため、TOEの運用に対して部外者である。

(3)　**利用方法**

TOEの構築と運用についての手順を説明する。

● **CAサーバマシンの構築手順**

1) CAサーバマシンの準備（システム管理者が実施）
   表2-1の必要機器を準備し、起動可能な状態にする。HSMの接続も行う。
2) OSのインストールとセットアップ（システム管理者が実施）
   表2-2のOSをインストールし、TOE利用者のIDとパスワードの設定、グループの登録、ネットワーク環境等の設定を行う。
3) CAサービスに必要なソフトウェアのインストール（システム管理者が実施）
   SW/PkiMGR、SW/PkiMGR KPO、Oracleをインストールする。
4) CAオペレータと監査者のアカウントをOSへ登録（システム管理者が実施）

OS上のTOE内部プロセスの実行権限やOSが管理するTOE資源の所有者の情報として使用するため、CAオペレータと監査者のアカウントをOSに登録する。

5) CAサービスのセットアップ（システム管理者が実施）
CAサービスを開始するため、及び監査ログを記録するためのセットアップを行う。これ以降、SSL通信でCAサービスが利用できるようになる。

6) CAオペレータのTOEへの登録と操作権の付与（システム管理者が実施）
2～10人のCAオペレータをTOEへ登録し、CAサービスの全ての操作権を設定する。

7) CAサービスの初期設定（6で登録されたCAオペレータが実施）
CA秘密鍵の生成やCA証明書の発行、またRAサービスと通信するためのCMPサービスの証明書とその秘密鍵の作成を行う。

8) SSLクライアント認証を行うためのCAオペレータ証明書の準備（6で登録されたCAオペレータが実施）
CA操作端末にICカードを装着し、PINを入力してICカードの認証を実施する。その後、合議操作に基づいて証明書・CRL管理機能を利用してCAオペレータ証明書の発行作業を行うと、ICカード内で鍵ペアが生成され、そのうちの公開鍵の情報を基にTOEがCAオペレータ証明書を発行する。（ICカード内で生成される鍵ペアのうち公開鍵の情報だけがCAサービスへ流通してCAオペレータ証明書が発行される。なお発行された証明書はICカードに格納され、発行時に自動的にTOEへも登録される。またCAオペレータ証明書の識別名にCAオペレータの役割を識別する情報が自動的に設定される。）

9) SSLクライアント認証を行うための監査者証明書の準備1（6で登録されたCAオペレータが実施）
監査者からのオフラインの証明書の発行依頼を受け、PKCS#12形式で監査者証明書とその秘密鍵を作成し、監査者に配付する。また、システム管理者に監査者証明書を配付する。

10) SSLクライアント認証を行うための監査者証明書の準備2（監査者が実施）
CAオペレータから渡された監査者証明書とその秘密鍵をICカードに格納する。

11) CAオペレータから渡された監査者証明書をTOEへ登録（システム管理者が実施）

12) SSLクライアント認証に必要なCA証明書をWWWサービスへ登録（システム管理者が実施）

13) RA証明書の準備（6で登録されたCAオペレータが実施）
RAのシステム管理者からのオフラインの証明書の発行依頼を受け、PKCS#12形式でRA証明書とその秘密鍵を作成し、RAのシステム管理者に配付する。また、システム管理者にRA証明書を配付する。

14) CAオペレータから渡されたRA証明書にRAサービスIDを付け、TOEへ登録（システム管理者が実施）

15) WWWサービスの設定変更（システム管理者が実施）
監査者証明書・CAオペレータ証明書を使用したSSLクライアント認証によってTOEを運用できるように、設定を変更する。この時、WWWサービスの環境にTOE（CA管理機能）へのアクセスをフィルタリングするための情報として、CAオペレータの役割を識別する情報が自動的に設定される。

16) CAサービスの運用を開始

- **CAサービスの運用手順**

① システム管理者の利用手順

1) サーバコンソールからOSにログオンする。
2) 運用環境のバックアップ作業または復旧作業を行う場合､CAサーバマシンに外部媒体を挿入する。
3) 運用環境の復旧作業を行う場合、起動中のプログラムを停止する。
4) 必要な作業を行う。
5) 運用環境の復旧作業を行った場合、3)で停止したプログラムを再開する。
6) 運用環境のバックアップ作業または復旧作業を行った場合、CAサーバマシンから外部媒体を排出する
7) OSからログオフし、作業を終了する。

② 監査者の利用手順

1) 予め配付されているICカードをCA監査端末に装着する。
2) CA監査端末からWWWブラウザを起動し、リモートでTOEへアクセスする。このとき、ICカードのPINを入力し、ICカードの認証を実施する。
3) 監査ログの移入・移出作業を行う場合は、CA監査端末に外部媒体を挿入する。
4) TOEを利用して必要な作業を行う。
5) 監査ログの移入・移出作業を行った場合は、CA監査端末から外部媒体を排出する。
6) WWWブラウザを閉じ、ICカードを抜いて作業を終了する。

CAオペレータが行う作業は、その内容の重要度により、単独で実施できるものと複数人の合意が必要なものとに分類される。CAオペレータが単独で行う作業を「通常操作」と呼び、主に証明書・CRLを扱う作業が該当する。複数人の合意により行う作業を「合議操作」と呼び、TOEにとってセキュリティ上非常に重要なCA秘密鍵を扱う作業やCAオペレータの操作権の設定作業が該当する。これらの作業については、表2-4に示す。

③ 通常操作を行うCAオペレータの利用手順

1) 予め配付されているICカードをCA操作端末に装着する。
2) CA操作端末からWWWブラウザを起動し、リモートでTOEへアクセスする。このとき、ICカードのPINを入力し、ICカードの認証を実施する。
3) TOEを利用して必要な作業を行う。
4) WWWブラウザを閉じ、ICカードを抜いて作業を終了する。

④ 合議操作を行うCAオペレータの利用手順

1) 操作権を持つCAオペレータがこれから行う作業に対して必要な人数分（2～10人）揃っているか

確認する。

2) 必要な人数のCAオペレータが揃っている場合、任意の者が代表として、予め配付されているICカードをCA操作端末に装着する。
3) CA操作端末からWWWブラウザを起動してリモートでTOEへアクセスする。このとき、ICカードのPINを入力し、ICカードの認証を実施する。
4) 実施する作業を選択する。
5) CAオペレータ全員が各々CAオペレータIDとパスワードを入力後、TOEを利用して必要な作業を行う。
6) WWWブラウザを閉じ、ICカードを抜いて作業を終了する。

⑤ RAからの利用手順

1) RAオペレータは、RA操作端末から一般利用者証明書の発行・失効をRAサービスに依頼する。
2) RAサービスはCMP通信を開設し、依頼をTOEに送信する。
3) RAサービスからCMP通信により、TOEが依頼を受け付ける。
4) TOEは依頼内容に応じて証明書を発行・失効し、その結果をRAサービスに送信する。
5) CMP通信を終了する。
6) 証明書を発行した場合、RAオペレータは一般利用者にそれを配付する。

監査者とCAオペレータは、運用開始後に追加登録が可能である。

⑥ 監査者の追加登録手順

1) 監査者証明書の準備1（証明書発行権限を持つCAオペレータが通常操作に基づき実施）
   PKCS#12形式で監査者証明書とその秘密鍵を作成し、監査者に配付する。
2) 監査者証明書の準備2（監査者が実施）
   CAオペレータから渡された監査者証明書とその秘密鍵をICカードに格納する。
3) 監査者をTOEへ登録（既に登録されている監査者が実施）
   監査者証明書をTOEへ登録する。

⑦ CAオペレータの追加登録手順

1) CAオペレータをTOEへ登録（登録権限を持つCAオペレータが通常操作に基づき実施）
2) CAオペレータの操作権設定（操作権の設定権限を持つCAオペレータが合議操作に基づき実施）
   追加登録されたCAオペレータが作業を実施できるように、必要な操作権を設定する。
3) SSLクライアント認証を行うためのCAオペレータ証明書の準備（証明書発行権限を持つCAオペレータが合議操作に基づき実施）
   CA操作端末にICカードを装着し、PINを入力してICカードの認証を実施する。その後、合議操作に基づいて証明書・CRL管理機能を利用すると、ICカード内で鍵ペアが生成され、そのうちの公開鍵の情報を基にTOEがCAオペレータ証明書の発行作業を行う。（ICカード内で生成される鍵ペアのうち公開鍵の情報だけがCAサービスへ流通してCAオペレータ証明書が発行される。

発行された証明書はICカードに格納され、発行時に自動的にTOEへも登録される。）

⑧ CA秘密鍵のバックアップ手順

TOEの運用環境のバックアップ作業は基本的にシステム管理者が単独で行うが、CA秘密鍵のバックアップ作業についてだけはシステム管理者とCAオペレータが共同で行う。

1) システム管理者とCA秘密鍵のバックアップ権限を持つ必要な人数分のCAオペレータが共にセキュアゾーンに入室する。
2) サーバコンソールからOSにログオン（システム管理者が実施）
3) バックアップ作業（CAオペレータが合議操作に基づき実施）
   CAオペレータIDとパスワードを入力し、作業を行う。
4) システム管理者はバックアップデータが格納された媒体をCAオペレータから受け取る。
5) OSからログオフ（システム管理者が実施）
6) システム管理者とCAオペレータが共にセキュアゾーンから退室する。

2.1.5　TOEの機能構成

TOEの構成を図2-3に示す。TOEは太枠内であり、①～⑦の機能とそれらが使用するファイルから構成される。点線内は1つの筐体（CAサーバマシン）、網掛けはセキュアゾーンを表す。

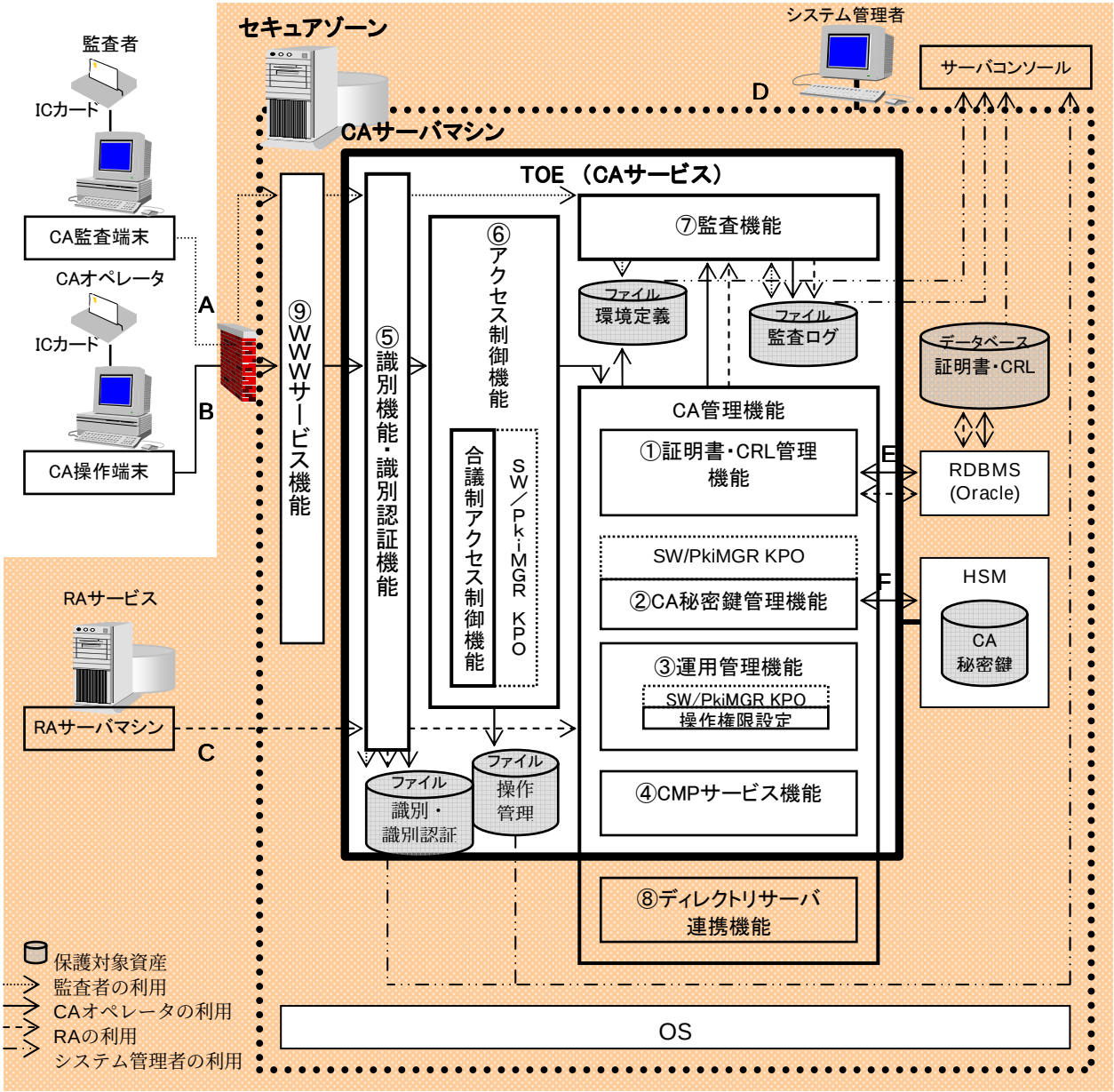

図 2-3：TOEの機能構成

(1)　外部インタフェース

TOEは、図2-3にA～Fで示す以下の外部インタフェースを持つ。

A) CA監査端末からTOEへアクセスするためのインタフェース

監査者からTOEへアクセスが要求される場合、CA監査端末から操作端末LAN、ファイアウォール、セキュアゾーンLANを介して、TOE外部機能であるWWWサービス機能で認証が行われ

る。監査者が保持するICカード内の監査者証明書とその秘密鍵を使用して監査者がWWWサービスで認証されると、TOEの⑤識別機能が動作し、⑦監査機能が利用可能になる。このインタフェースで使用する保護対象資産は、監査者クライアントデータ、監査者識別データ、環境定義データ、監査ログである。

B) CA操作端末からTOEへアクセスするためのインタフェース

CAオペレータからTOEへアクセスが要求される場合、CA操作端末から操作端末LAN、ファイアウォール、セキュアゾーンLANを介して、TOE外部機能であるWWWサービス機能で識別認証が行われる。CAオペレータが保持するICカード内のCAオペレータ証明書とその秘密鍵を使用してCAオペレータがWWWサービスで識別認証されると、通常操作のためのアクセスではTOEの⑤識別機能、⑥アクセス制御機能が動作し、①証明書・CRL管理機能、③運用管理機能（CAオペレータの登録・削除）が利用可能になる。この場合に使用する保護対象資産は、CAオペレータクライアントデータ（CAオペレータ証明書とその秘密鍵）、CAオペレータ識別データ、CAオペレータ操作管理データ、環境定義データ、証明書・CRLである。

また合議操作のためのアクセスでは、TOEの⑤識別認証機能、⑥アクセス制御機能、及び合議制アクセス制御機能が動作し、②CA秘密鍵管理機能、③運用管理機能（CAオペレータ操作権設定機能）が利用可能になる。この場合に使用する保護対象資産は、CAオペレータクライアントデータ（CAオペレータ証明書とその秘密鍵、及び各CAオペレータのIDとパスワード）、CAオペレータ識別認証データ、合議操作管理データ、環境定義データ、CA秘密鍵である。

なお、CAオペレータがWWWサービス機能で識別認証されると、TOEはCAオペレータプロセスを生成する。このCAオペレータプロセスは、OSに作成されたCAオペレータのアカウントに付与されているアクセス権の範囲でだけ動作する。

C) RAサービスからTOEへアクセスするためのインタフェース

RAサービスからTOEへアクセスが要求される場合、セキュアゾーンLANを介して、TOEの⑤識別認証機能で識別認証が行われる。識別認証されると④CMPサービス機能が動作し、RAサービスとのCMP通信が開始され、④CMPサービス機能から①証明書・CRL管理機能が利用される。このインタフェースで使用する保護対象資産は、RAサービスクライアントデータ、RA識別データ、CMPサービス証明書とその秘密鍵、RA証明書である。

D) サーバコンソールからTOEへアクセスするためのインタフェース

システム管理者がOSにログオンしてTOEへアクセスが要求される場合、OSで識別認証が行われる。システム管理者が識別認証されるとTOEに関連するデータをOSから直接操作することが可能となる。バックアップ作業で使用する保護対象資産は、証明書・CRL、CA秘密鍵、識別データ、識別認証データ、操作管理データ、環境定義データ、監査ログである。

E) RDBMSとTOEのインタフェース

①証明書・CRL管理機能がデータベースで管理する証明書・CRLにアクセスするためのインタフェースである。TOEはプロセス間通信によりRDBMSを利用する。

F) HSMとTOEのインタフェース

②CA秘密鍵管理機能がCA秘密鍵にアクセスするためのインタフェースである。TOEはプロセス間通信によりCA秘密鍵にアクセスする。

(2) TOEが提供する機能

TOEは、SW/PkiMGRにより提供される図2-3に①～⑦で示す以下のTSFから構成される。なお、CAサービスの運用に関する機能をCA管理機能と呼び、①～④、⑧が該当する。

① 証明書・CRL管理機能

- 既存の証明書プロファイルを変更する（設定されている証明書の形式を変更する）。
- 新しい証明書プロファイルを追加する（新しい証明書の形式を定義する）。
- 追加した証明書プロファイルを削除する（追加した証明書の形式を削除する）。
- 既存のCRLプロファイルを変更する（CRLのプロファイルは予め全形式が用意されているため、それを変更してCRLの形式を定義する）。
- CMPサービス証明書、CAオペレータ証明書、CA証明書を発行する。
- PKCS#10形式の申請書に基づき、CAオペレータが相互認証証明書等を発行する。
- 監査者・RAサービス等の証明書とその秘密鍵をCAオペレータがPKCS#12形式で作成する。
- 発行した証明書を失効する。
- 管理している証明書の内容を表示する。
- CRLを発行する。
- ④CMPサービス機能からの要求に基づき、一般利用者証明書を発行・失効する。
- 他のCAが発行した証明書・CRLをCA操作端末からインポートしてデータベースに登録し、管理する。
- データベースで管理する証明書・CRLを削除する。
- データベースで管理する証明書・CRLをCA操作端末に取り出す。

但し、上記のうちプロファイルに関連する操作以外は、CA秘密鍵が必要な操作であるため、CA秘密鍵の活性化後でなければ行うことができない。

② CA秘密鍵管理機能

HSMでCA秘密鍵を管理するための以下の機能である。

- CA秘密鍵を生成・削除する。
- CA秘密鍵を活性化・非活性化する。
- CA秘密鍵をバックアップ・リストアする。

③ 運用管理機能

- CAオペレータを追加・削除する。
- CAオペレータの操作権を設定する。

④ CMPサービス機能

CAサービスとRAサービス間の通信を制御するための以下の機能である。

- RAサービスからの一般利用者証明書の発行や失効の要求を受信する。
- 一般利用者証明書の発行や失効を①証明書・CRL管理機能に依頼する。
- ①証明書・CRL管理機能の処理結果をRAサービスに送信する。

⑤ 識別機能・識別認証機能

TOE利用者を識別または識別認証する以下の機能である。

- 監査者を識別する。
- 通常操作を行うCAオペレータを識別する。
- 合議操作を行うCAオペレータを識別認証する。
- RAサービスを識別認証する。

TOE外部機能である⑨WWWサービス機能において、CAオペレータに対するSSLクライアント認証、及びCAオペレータの役割についての識別が行われるため、通常操作を行うCAオペレータに対しては、TOEはオペレータ個人についての識別だけを行う。但し、合議操作を行うCAオペレータに対しては、TOEはオペレータ個人についての識別、及び認証を行う。

⑥ アクセス制御機能・合議制アクセス制御機能

表2-4で示すCAオペレータが行う操作は、操作毎に操作を行うCAオペレータを限定することができる。表2-4で「合議操作」に分類される操作を行う場合は更に、操作毎にその実施に必要となるCAオペレータの最小人数を2～10人の範囲で設定することができる。つまりCAオペレータという役割において、オペレータ毎あるいは操作毎に独自のセキュリティをきめ細かく設定することが可能である。そのため、以下のアクセス制御機能を提供する。

- CAオペレータが行う操作全てについて操作権を管理し、許可されない操作を制限するアクセス制御を行う。
- セキュリティ上非常に重要なCA秘密鍵を扱う操作やCAオペレータの操作権の設定操作について、操作の実施に必要な最小人数を管理し、その人数分の合意が得られなければ操作を制限する合議制アクセス制御機能を行う。

CAオペレータが行う操作は表2-4で示すように分類され、操作に応じたアクセス制御が実施される。

表 2-4：CAオペレータが行う操作

分類	内容
通常操作	・既存の証明書プロファイルの変更 ・新しい証明書プロファイルの追加 ・追加した証明書プロファイルの削除 ・既存のCRLプロファイルの変更 ・PKCS#10形式の申請書に基づく相互認証証明書等の発行 ・監査者・RAサービス等の証明書とその秘密鍵をPKCS#12形式で作成 ・発行した証明書の失効 ・CRLの発行 ・他のCAが発行した証明書・CRLの登録 ・データベースで管理する証明書・CRLの削除 ・CAオペレータの登録・削除
合議操作	・CA秘密鍵の生成・削除 ・CA秘密鍵の活性化・非活性化 ・CA秘密鍵のバックアップ・リストア ・CA証明書・CAオペレータ証明書の発行 ・CMPサービス証明書とその秘密鍵の更新 ・CAオペレータの操作権の設定

⑦ 監査機能

監査者がTOE利用者の操作について監査を実施できるようにするための以下の機能である。

- 監査者・CAオペレータ・RAサービスのセキュリティに関連する全ての操作について監査ログを記録する。
- 監査ログの完全性と連続性を保証する。
- 監査ログを検索して表示する。
- 監査ログをCAサーバマシンから外部媒体に移出する。
- 監査ログをCAサーバマシンから削除する。
- 監査ログを外部媒体からCAサーバマシンに移入する。

なお本機能はWindows版の場合はサービスプログラム、Solaris OE版の場合はデーモンプロセスとして動作するため、通常OSの起動と共に自動的に開始し、OSの停止の前に自動的に停止する。

(3) TOEの利用対象外機能

⑧ ディレクトリサーバ連携機能

一般利用者にCA証明書・CRLを配布することと、RAの申請により発行された一般利用者証明書をディレクトリサーバから一般利用者に配布することを目的として、CAサーバマシンとディレクト

リサーバマシンとをオンラインで連携するオプション機能である。本機能はCAサービスのCA管理機能に含まれるが、本STではCAサービスからディレクトリサーバへCA証明書・CRL・一般利用者証明書をオンラインで格納して公開する運用は想定しないため、TOE範囲外とする。

(4)　**TOEが提供しない機能**

⑨ WWWサービス機能

- 識別機能・認証機能

監査者・CAオペレータからのTOEアクセス要求時に、WWWサービスにおいてICカード内の監査者・CAオペレータの各々の証明書とその秘密鍵を使用したSSLクライアント認証が行われる。ICカード内の証明書は、SSL通信によってTOEクライアント操作端末を経由して操作端末LAN上に流通し、WWWサービスに渡る。WWWサービスは、その環境に登録されているCA証明書を使用して、渡された証明書のディジタル署名を検証することにより認証を行う。なお監査者は認証が終了した時点でTOEへのアクセスが可能となるが、CAオペレータについては更にWWWサービスによる識別が行われる。WWWサービスは、その環境に設定されているCAオペレータの役割を識別する情報が、渡されたCAオペレータ証明書に含まれているかを確認することにより、アクセス者であるCAオペレータがそのCAサービスに対し役割を持つかどうかを識別する。

- 高信頼パス機能

WWWサービスとTOEクライアント操作端末間の通信には高信頼パスが使用される。

2.1.6　TOEの運用パターン

TOEは、図2-4か図2-5の何れかのパターンで運用される。図2-4、図2-5はHSMに表2-1の富士通製 暗号プロセッサカードを使用した場合を示している。なおCHRYSALIS-ITS Inc.製 LUNA(R) CA3を使用する場合は、HSM本体がCAサーバマシンの筐体外に専用のケーブルで接続される。

(1)　**1CAサーバマシン上でCAサービスを1つだけ構築して運用するパターン**

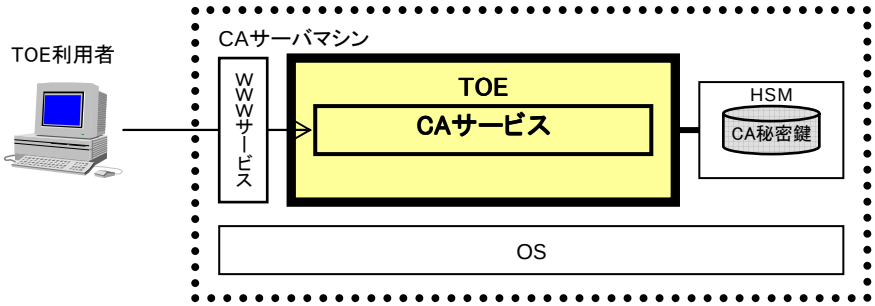

図 2-4：運用パターン[1]

(2)　1CAサーバマシン上で複数のCAサービスを構築して運用するパターン

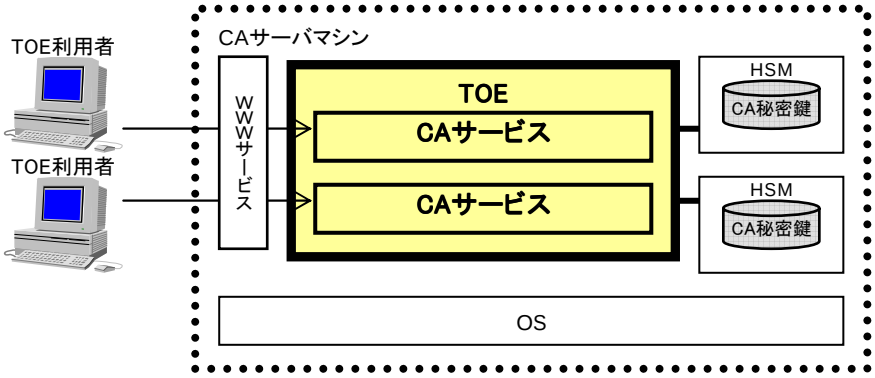

図 2-5：運用パターン[2]

1つのCAサーバマシン上で複数のCAサービスを構築し、運用することができる。その場合WWWサービスはシステムで1つだけ起動され共用されるが、CA秘密鍵を管理するHSMはCAサービスごとに用意する必要がある。また、CAサービス毎にTOEの管理する資源は区別され保管されており、同一CAサーバマシン上で動作するそれぞれのCAサービス同士が連携することはない。

TOE利用者はURLで区別される各CAサービスに対してアクセスし、各CAサービスは独立して動作する。またCAサービス毎に監査者とCAオペレータが決定され、各々異なるCAサービスへアクセスすることはできない。1CAサーバマシン上に複数のCAサービスを構築する場合のTOE利用者の人数を表2-5に示す。

表 2-5：1CAサーバマシン上に複数のCAサービスを構築した場合のTOE利用者

役割	人数
システム管理者	CAサーバマシンに1人
監査者	CAサービスに複数人
CAオペレータ	CAサービスに複数人

2.2　TOEとIT環境により保護するデータ

TOEとIT環境により保護するデータについて説明する。

- **証明書**

TOEは以下の①～④の発行／配付の形態を持つ。①～④で発行された証明書は全てデータベースに自動的に登録され、証明書・CRL管理機能を利用して削除しない限りデータベースで管理される。なお、TOEが発行する証明書のうち識別機能や識別認証機能で使用するものは、信頼できる証明書でなければならない。そのため証明書発行時にTOEがディジタル署名のために使用するCA秘密鍵は耐タンパー性のあるHSMで安全に管理される必要があり、発行は「証明書の発行」操作の権限を持つCAオペレータだけが行う。また監査者証明書やCAオペレータ証明書は発行後、耐タンパー性のあるICカードで安全に管理されている。

① 証明書に設定する利用者の名前や公開鍵の情報が含まれるRAサービスからのCMP要求メッセージに基づき、一般利用者証明書を発行する。本証明書はCMP応答メッセージに同梱され、セキュアゾーンLANを介してRAサーバマシンに送信され、配付される。
② CAオペレータが証明書の発行の申請元を確認した後、証明書に設定する利用者の名前や公開鍵の情報を含むPKCS#10形式の申請書に基づき、証明書を発行する。本証明書は証明書・CRL管理機能の取り出し機能により外部媒体へ取り出され、利用者にオフラインで配付される。
③ TOEが秘密鍵と公開鍵を生成し、証明書に設定する利用者の名前はCAオペレータが決めて、証明書とその秘密鍵を暗号化して格納するPKCS#12形式で作成する。本証明書は証明書・CRL管理機能の取り出し機能により外部媒体へ取り出され、利用者にオフラインで配付される。
④ 証明書・CRL管理機能の取り出し機能により外部媒体へ取り出したCA証明書をオフラインでディレクトリサーバマシンへ格納し、一般利用者にはディレクトリサーバマシンから配布される。
なお相互認証を行う場合は、以下の⑤を行う。
⑤ TOEを運用する組織の責任者が認証相手となる他のCAについてオフラインで身元を確認した後、CAオペレータが他のCAが発行した相互認証証明書を自CAサービスのデータベースに登録する。

- **CRL**

CAオペレータにより発行され、発行後は全てデータベースに自動的に登録される。相互認証を行う場合は、TOEを運用する組織の責任者が認証相手となる他のCAについてオフラインで身元を確認した後、CAオペレータが他のCAが発行したCRLを自CAサービスのデータベースに登録する。登録されたCRLは証明書・CRL管理機能を利用して削除しない限り、データベースで管理される。また証明書・CRL管理機能の取り出し機能により外部媒体へ取り出したものをオフラインでディレクトリサーバマシンへ格納し、一般利用者にはディレクトリサーバマシンから配布される

- **CA秘密鍵**

HSM内で生成され、管理される。新しい鍵を生成しない限り常にHSMに保持される。なおCA秘密鍵は次の状態でバックアップされている。HSMに富士通製 暗号プロセッサカードを使用する場合、バックアップデータはHSMにより暗号化、及び分割されたファイルとなる。またCHRYSALIS-ITS Inc.製 LUNA(R) CA3を使用する場合、バックアップはHSMからHSMへの複写となるため、バックアップデータは同じ耐タンパー性のHSMに格納される。

- **TOE動作環境ファイル**

各々TOE内のファイルとして保持される以下の①～④の総称。
① 識別データ：TOEの識別機能で使用する以下のデータの総称。
  - 監査者識別データ：アクセスを許可する監査者証明書と監査者IDを予め登録している。監査者管理ファイルとして管理する。
  - CAオペレータ識別データ：アクセスを許可するCAオペレータの情報として、CAオペレータ証明書のシリアル番号とCAオペレータIDの関連情報を定義している。CAオペレータ管理フ

ァイルとして管理する。

- RA識別データ：アクセスを許可するRAサービスの情報として、RA証明書とRAサービスIDを予め定義している。RA管理ファイルとして管理する。

② 識別認証データ：TOEの識別認証機能で使用する以下のデータの総称。

- CAオペレータ識別認証データ：アクセスを許可するCAオペレータの情報として、CAオペレータID、パスワードを照合するための秘密情報を定義している。CAオペレータ認証管理ファイルとして管理する。
- CMPサービス証明書とその秘密鍵：RAサービスと通信する際の認証に必要な情報を予め定義している。CMPサービス管理ファイルとして管理する。

③ 操作管理データ：TOEのアクセス制御機能で使用する以下のデータの総称。

- CAオペレータ操作管理データ：CAオペレータの操作全てについて、アクセス制御を行うための情報として、CAオペレータIDと操作ID（合議操作の場合は合議操作ID）の関連情報を定義している。CAオペレータ操作管理ファイルとして管理する。
- 合議操作管理データ：合議制アクセス制御を行うための情報として、合議操作ID、合議操作の必要最小人数、合議操作秘密情報を定義している。合議操作管理ファイルとして管理する。

④ 環境定義データ：TOEの環境を定義する以下のデータの総称。

- 監査環境定義データ：監査機能の動作環境についての情報を定義している。監査環境定義ファイルとして管理する。
- CA環境定義データ：CA管理機能の動作環境についての情報を定義している。CA環境定義ファイルとして管理する。
- データベース環境定義データ：データベースにアクセスするための情報を定義している。データベース環境定義ファイルとして管理する。

- **監査ログ**

TOEが記録した監査ログを監査ログファイルとして管理する。監査機能により削除しない限りTOE内のファイルとして保持する。監査ログファイルは肥大化していくものであるため、定期的に外部媒体に移出し、CAサービス上から削除する運用が推奨される。なお、外部媒体にしか存在しない監査ログは再度CAサービスに移入することができるが、この場合既にCAサービス上に存在する監査ログが上書きされることはない。また、外部媒体内の監査ログがCAサービスに既に存在する場合には、移入することはできない。

- **クライアントが保持するデータ**

TOEのクライアントである監査者、CAオペレータ、RAサービスが各々保持する以下の①～③のデータ。

① 監査者クライアントデータ：監査者からのアクセス要求時に必要な監査者証明書とその秘密鍵であり、監査者が管理するICカード内に格納されている。TOEへのアクセス開始時に、TOE外部機能であるWWWサービス機能で監査者証明書による認証が行われるため、ICカード内の証明書

はSSL通信によってCA監査端末を経由して操作端末LAN上に流通し、WWWサービスに渡される。なお秘密鍵は、操作端末LAN上に流通することはない。

② CAオペレータクライアントデータ：CAオペレータからのアクセス要求時に必要な以下のデータ。

- CAオペレータ証明書とその秘密鍵：CAオペレータが管理するICカード内に格納されている。TOEへのアクセス開始時に、TOE外部機能であるWWWサービス機能でCAオペレータ証明書による識別認証が行われるため、ICカード内の証明書はSSL通信によってCA操作端末を経由して操作端末LAN上に流通し、WWWサービスに渡される。なお秘密鍵は、操作端末LAN上に流通することはない。
- CAオペレータIDとパスワード：CAオペレータ自身が管理するデータであり、合議操作を行う場合にはCAオペレータ証明書とその秘密鍵に加えて必要となる。なお合議操作時は、TOEでCAオペレータIDとパスワードによる識別認証が行われるため、これらはCA操作端末を経由して操作端末LAN上に流通する。

③ RAサービスクライアントデータ：RAサービスからのアクセス要求時に必要なRA証明書であり、RAサービス自身が管理する。TOEでRA証明書による識別認証が行われるため、RA証明書はCMP要求メッセージに同梱され、RAサーバマシンからセキュアゾーンLANに流通する。

3　TOEセキュリティ環境

3.1　前提条件

3.1.1　物理的条件

- **ASM.CA-ACCESS（CAサーバマシンのアクセス制限）**
  CAサーバマシンはセキュアゾーンに設置され、セキュアゾーンへの入室時には物理鍵や認証システムを必要とする。入室する権限はシステム管理者とセキュアゾーンに設置されるその他のサーバマシンの管理者（他サーバマシン管理者）だけが持つ。HSMで管理するCA秘密鍵のバックアップ作業のためCAオペレータがセキュアゾーンに入室する特例では必ずシステム管理者と共に入室し、セキュアゾーンでの作業はシステム管理者の監視の下、共同で実施される。

- **ASM.TERMINAL-ACCESS（TOEクライアント操作端末へのアクセス制限）**
  TOEを運用する組織に属する者だけが物理的にTOEクライアント操作端末へアクセスできる。

- **ASM.CA-KEY（CA秘密鍵の保護）**
  CA秘密鍵は耐タンパー性のあるHSMで管理されており、物理的な攻撃を行われたとしてもCA秘密鍵が暴露されることはない。

- **ASM.AUDITOR-CAO-KEY（監査者とCAオペレータの秘密鍵の保護）**
  監査者、CAオペレータがTOEへアクセスする時に必要となる監査者、CAオペレータの各々の証明書とその秘密鍵は、耐タンパー性のあるICカードに格納されており、物理的な攻撃を行われたとしても秘密鍵が暴露されることはない。

- **ASM.MEDIA-DATA（媒体の保護）**
  TOEの運用環境をバックアップしたデータを格納した媒体や監査ログを移出した媒体は、適切な手順に従い保管され、物理的な破壊・盗難から保護されている。

3.1.2　人的条件

- **ASM.ADMIN-AUDITOR-RELIABILITY（システム管理者、監査者、他サーバマシン管理者の信頼）**
  システム管理者、監査者、他サーバマシン管理者は、各自に課せられた役割に対して許可される一連の作業について、悪意を持った行為は行わず、TOEの運用に協力的に関わる。

- **ASM.SECURE-ENVIRONMENT（セキュアな運用環境の構築と管理）**
  システム管理者は、CAサーバマシンとその構成要素であるWWWサービス、RDBMS、HSMやCAサーバマシンに接続される機器（サーバコンソールやHSM本体）を適切にセットアップし、セキュアな状態を維持する。この時、システム管理者はSSLクライアント認証に必要なCA証明

書、及びTOEの識別認証に必要な監査者証明書やRA証明書を適切に設定する。また、運用環境の復旧のためにTOE内のデータの定期的なバックアップを行う。

3.1.3　接続条件

- **ASM.CA-CONNECT（CAサーバマシンへの接続制限）**
  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のみと接続され、CAサービスの特定のポートに対してTOEクライアント操作端末とだけ通信できるように設定されている。

- **ASM.OTHER-RELIABILITY（その他のサーバマシンの信頼）**
  セキュアゾーンに設置されるCAサーバマシン以外のサーバマシンは、他サーバマシン管理者が適切に設定し、管理するものである。

3.1.4　使用条件

- **ASM.IMPORT-DATA-RELIABILITY（インポートデータの信頼）**
  TOEにインポートされるデータは、TOEを運用する組織の責任者が予めその信頼性を確認したものである。

3.2　脅威

- **T.ADMIN-ERROR（システム管理者の誤操作）**
  システム管理者が誤操作により、以下のTOE内のデータを変更・削除する。
  ・証明書
  ・CRL
  ・TOE動作環境ファイル
    ・識別データ（監査者識別データ、CAオペレータ識別データ、RA識別データ）
    ・識別認証データ（CAオペレータ識別認証データ、CMPサービス証明書とその秘密鍵）
    ・操作管理データ（CAオペレータ操作管理データ、合議操作管理データ）
    ・環境定義データ（監査環境定義データ、CA環境定義データ、データベース環境定義データ）
  ・監査ログ

- **T.AUDITOR-ERROR（監査者の誤操作）**
  監査者が監査作業中の誤操作により、以下の行為を行う。
  ・移出していない有効な監査ログを削除する。
  ・登録されている監査者の証明書を削除する。

- **T.CAO-MALICE&ERROR-1（CAオペレータの悪意ある操作と誤操作-1）**
  悪意を持つCAオペレータがCAサービスの運用を妨害するために自分自身の役割に与えられる操作権の範囲を超えてTOEを利用するか、または悪意を持たないCAオペレータが運用作業中の

誤操作により、以下の行為を行う。
・発行すべきでない第三者に証明書を発行する。
・定義されているプロファイルとは異なる形式の証明書・CRLを発行する。
・データベースで管理する有効な証明書・CRLを削除する。
・データベースで管理する有効な証明書を失効し、CRLを発行する。
・操作権を持つ有効なCAオペレータを削除する。
・信頼性が確認されていない他のCAが発行した証明書・CRLを登録する。
・信頼性が確認されていない他のCAと相互認証を行う。

- **T.CAO-MALICE&ERROR-2（CAオペレータの悪意ある操作と誤操作-2）**
  悪意を持つCAオペレータがCAサービスの運用を妨害するために自分自身の役割に与えられる操作権の範囲を超えてTOEを利用するか、または悪意を持たないCAオペレータが運用作業中の誤操作により、以下の行為を行う。
  ・CA秘密鍵を新しく生成し、有効なCA秘密鍵を無効化する。また、CA証明書を新たに発行し、有効なCA証明書を無効化する。
  ・CMPサービス証明書とその秘密鍵を新しく生成し、有効なCMPサービス証明書およびその秘密鍵を無効化する。
  ・CAオペレータの操作権を変更する。

- **T.AUDITOR-PRETENDED（監査者へのなりすまし）**
  悪意を持つCAオペレータや悪意を持つ組織内第三者が監査者をなりすましてアクセスし、以下の行為を行う。
  ・監査ログの全てまたは一部を削除する。
  ・不正な監査者の証明書を登録する。
  ・登録されている監査者の証明書を削除する。

- **T.CAO-PRETENDED（CAオペレータへのなりすまし）**
  悪意を持つ組織内第三者がCAオペレータをなりすましてアクセスするか、または悪意を持つCAオペレータが他のCAオペレータをなりすまして、自CAサービスや同じCAサーバマシン内に構築されている他のCAサービスへアクセスし、以下の行為を行う。
  ・発行すべきでない第三者に証明書を発行する。
  ・定義されているプロファイルとは異なる形式の証明書・CRLを発行する。
  ・データベースで管理する有効な証明書・CRLを削除する。
  ・データベースで管理する有効な証明書を失効し、CRLを発行する。
  ・操作権を持つ有効なCAオペレータを削除する。
  ・CA秘密鍵を新しく生成し、有効なCA秘密鍵を無効化する。また、CA証明書を新たに発行し、有効なCA証明書を無効化する。

・CMPサービス証明書とその秘密鍵を新しく生成し、有効なCMPサービス証明書およびその秘密鍵を無効化する。
・CAオペレータの操作権を変更する。
・CAオペレータを追加し、不正な操作権を設定する。

- **T.INTERCEPTION（盗聴）**
  悪意を持つCAオペレータや悪意を持つ組織内第三者が、TOEクライアント操作端末とTOE間の操作端末LANを経由する送受信データを盗聴する。

3.3 組織のセキュリティ方針

- **P.SECUREZONE-CA（セキュアゾーン内のCAサーバマシン）**
  セキュアゾーンにおいてCAサーバマシンのOSにログオン可能な利用者は、システム管理者に限定されなければならない。

- **P.SECRET（秘匿）**
  CAサービスに対し重要な役割を有するCAオペレータがTOEへアクセスするために必要な情報、及び重要な操作を行う際に必要な情報は、システム管理者に対しても秘匿されなければならない。

- **P.RA-RELIABILITY（RAサービスの信頼性）**
  CAサービスは、RAサービスからのアクセス要求に対して識別認証を実施し、予め登録されている正当なRAサービスに対してだけアクセスを許可しなければならない。

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.I-AUDITOR（監査者の識別）**
  TOEは、WWWサービス機能から受け取った監査者証明書を使用して、監査者がTOEを利用する前に、複数人存在する監査者の中のどの監査者か特定するための識別を行い、識別した監査者の要求だけを受け付ける。

- **O.IA-CAO（CAオペレータの識別認証）**
  TOEは、CAオペレータIDとパスワード情報を使用して、合議操作を行うCAオペレータがTOEを利用する前に、複数人存在するCAオペレータの中のどのCAオペレータか特定するための識別認証を行い、識別認証したCAオペレータの要求だけを受け付ける。

- **O.I-CAO（CAオペレータの識別）**
  TOEは、WWWサービス機能から受け取ったCAオペレータ証明書を使用して、通常操作を行うCAオペレータがTOEを利用する前に、複数人存在するCAオペレータの中のどのCAオペレータか特定するための識別を行い、識別したCAオペレータの要求だけを受け付ける。

- **O.IA-RA（RAサービスの識別認証）**
  TOEは、RAサービスからのアクセス要求に対し識別認証を行い、識別認証したRAサービスのアクセス要求だけを受け付ける。

- **O.ACCESS-CONTROL-CAO（CAオペレータのアクセス制御）**
  TOEは、CAオペレータが実施できる操作を管理し、許可されない操作を制限する。

- **O.DUAL-CONTROL-CAO（CAオペレータの合議制アクセス制御）**
  TOEは、操作に必要な人数を管理し、その人数の操作権を持つCAオペレータの合意が得られなければ操作を制限する。

- **O.AUDIT（監査記録）**
  TOEは、監査者、CAオペレータ、RAサービスのセキュリティに関連する操作の全てを記録する手段、及び監査ログ表示時に不正な削除による漏れがないか、また改変されていないかを検出する手段を提供する。また監査者だけに監査を実施する機能を提供する。

- **O.CRYPTOGRAPHY（暗号）**
  TOEは、CAオペレータを特定するための情報について暗号化し、TOE内のファイルとして保持する。

4.2 環境のセキュリティ対策方針

(1)　IT環境セキュリティ対策方針

- **OE.OS-IA（OSの識別認証）**
  OSは、システム管理者を識別認証し、識別認証したシステム管理者の要求だけを受け付ける。

- **OE.OS-ACCESS-CONTROL（OSのアクセス制御）**
  OSは、OSが管理するファイルに対してアクセス制御を実施することにより、システム管理者の意図しないファイルの変更・削除を防止する。

- **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.BYPASS（OSのセキュリティドメインによる保護）**
  OSは、意図されないアクセスから保護するためのセキュリティドメインを各CAサービスにおけるCAオペレータ、監査者ごとに維持する。

- **OE.WWW-A（WWWサービスの認証）**
  WWWサービスは、TOEクライアント操作端末からのアクセス要求に対して、ICカード内の監査者・CAオペレータの各々の証明書とその秘密鍵による認証を行い、認証した監査者・CAオペレータの要求だけを受け付ける。

- **OE.WWW-I（WWWサービスの識別）**
  WWWサービスは、CA操作端末からのアクセス要求に対して、そのCAオペレータのCAオペレータ証明書に、CAオペレータの役割を識別する情報が含まれているかどうかについて識別を行い、識別したCAオペレータの要求だけを受け付ける。

- **OE.WWW-TRUST-PATH（WWWサービスの高信頼パス）**
  WWWサービスは、TOEクライアント操作端末との通信において、通信内容が盗聴されないよう高信頼パスを提供する。

- **OE.HSM（HSM）**
  HSMは、CA秘密鍵を生成し、それを使用して証明書の完全性を保証するための偽造不可能なディジタル署名を提供する。

- **OE.ICCARD-A（ICカードの認証）**
  ICカードは、利用者からのアクセス要求に対して認証を行ない、ICカードの正当な所有者以外の者による不正な利用を防止する。

(2)　**運用／管理セキュリティ対策方針**

- **OE.CA-ACCESS（CAサーバマシンのアクセス制限）**
  TOEを運用する組織の責任者は、CAサーバマシンを専用区域（セキュアゾーン）に設置し、セキュアゾーンへは許可されている管理者だけが入室できるよう入退室管理を行う。またCAオペレータがセキュアゾーンに入室する特例では、必ずシステム管理者と共に入室し、システム管理者の監視下、作業が共同で実施されるよう入退室管理、及び監視する。

- **OE.TERMINAL-ACCESS（TOEクライアント操作端末へのアクセス制限）**
  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を確保し、TOEクライアント操作端末を設置する。

- **OE.CA-KEY（CA秘密鍵の保護）**
  システム管理者は、耐タンパー性のあるHSMでCA秘密鍵を管理する。

- **OE.AUDITOR-CAO-KEY（監査者とCAオペレータの秘密鍵の保護）**
  監査者、CAオペレータは、各々が保持する耐タンパー性のあるICカードで自身の証明書とその秘密鍵を管理する。

- **OE.MEDIA-DATA（媒体の保護）**
  システム管理者と監査者は、破壊・盗難から保護される管理場所を確保し、運用環境をバックアップした媒体や監査ログを移出した媒体を各々保管する。

- **OE.ADMIN-AUDITOR-RELIABILITY（システム管理者、監査者、他サーバマシン管理者の信頼）**
  TOEを運用する組織の責任者は、システム管理者、監査者、他サーバマシン管理者が各自に課せられた役割に対して許可される一連の作業について、セキュリティ意識を向上させ悪意を持った行為を行わず、TOEの運用に協力的に関わるように、及びTOEの担当作業を指導し誤操作の可能性を低減するために、システム管理者と監査者に対してセキュリティ教育や訓練を実施する。

- **OE.SECURE-ENVIRONMENT（セキュアな運用環境の構築と管理）**
  システム管理者は、CAサービスの運用環境の構築としてCAサーバマシンとその構成要素であるWWWサービス、RDBMS、HSMやCAサーバマシンに接続される機器（サーバコンソールやHSM本体）を適切にセットアップし、セキュアな状態を維持できるようプログラムを管理（最新パッチの適用等）する。またシステム管理者は、SSLクライアント認証に必要なCA証明書、及びTOEの識別認証に必要な監査者証明書やRA証明書を適切に設定する。

- **OE.BACKUP（復旧のためのバックアップ）**
  システム管理者は運用環境を復旧できるように、定期的にTOE内のデータをバックアップする。

- **OE.CA-CONNECT（CAサーバマシンへの接続制限）**
  システム管理者は、セキュアゾーンLANと操作端末LANの間にファイアウォールを設置し、CAサービスの特定のポートに対してTOEクライアント操作端末とだけ通信できるようファイアウォールを設定する。

- **OE.OTHER-RELIABILITY（その他のサーバマシンの信頼）**
  TOEを運用する組織の責任者は、他サーバマシン管理者により適切に設定し、管理されるサーバマシンをセキュアゾーンに設置する。

- **OE.IMPORT-DATA-RELIABILITY（インポートデータの信頼）**
  TOEを運用する組織の責任者は、証明書発行の申請書や証明書・CRLをやりとりすることになる申請者や他のCAについて、事前にオフラインでその信頼性を確認し、TOEの運用を開始する。また運用開始後には、信頼性を確認した申請者や他のCAからのインポートデータだけが受け付けられていることを監査ログにより確認する。

5　ITセキュリティ要件

ここではTOEセキュリティ要件及びIT環境に対するセキュリティ要件について記述する。記述の中で、各コンポーネントの操作（割付、選択、繰り返し、詳細化）は以下のように識別する。

操作	識別方法
割付	割り付け内容をイタリック体、かつボールド体で記述する。 例えば「[割付：AAA]：***BBB***」と記載した場合、[ ]の括弧内の部分はCC パート2の内容を記述し、***BBB***の部分は割り付け内容を記述する。
選択	選択した要素をイタリック体、かつボールド体で記述する。 例えば「[選択：AAA、BBB、CCC]：***AAA***」と記載した場合、[ ]の括弧内の部分はCC パート2の内容を記述し、***AAA***の部分は選択した要素を記述する。
繰り返し	コンポーネントラベルの末尾に[a]、[b]といった識別子を付与する。また、IT環境のセキュリティ機能要件に対してはコンポーネントラベルの末尾に[E]を付与する。 例えば、コンポーネントラベルが「AAA_BBB」である機能要件を繰り返す場合、「AAA_BBB[a]」、「AAA_BBB[b]」と記述する。また、IT環境のセキュリティ機能要件のコンポーネントラベルが「AAA_BBB」である機能要件を繰り返す場合、「AAA_BBB[E][a]」、「AAA_BBB[E][b]」と記述する。
詳細化	詳細化したテキストをステートメント中に直接イタリック体、かつボールド体で記述する。

5.1　TOEセキュリティ要件

5.1.1　TOEセキュリティ機能要件

(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
	監査データ損失の恐れ発生時のアクション	FAU_STG.3
	監査データ損失の防止	FAU_STG.4

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*］。：

  個別の監査対象事象を表5-2に示す。なお、監査対象アクション中の下線部分は対応する監査レベルを示す。

表 5-2：個別の監査対象事象

コンポーネント	監査対象アクション	監査対象事象
FAU_GEN.1	なし。	なし。
FAU_GEN.2	なし。	なし。
FAU_SAR.1	a) 基本：監査記録からの情報の読み出し。	・監査ログの検索／表示
FAU_SAR.2	b) 基本：監査記録からの成功しなかった情報読み出し。	・監査ログの検索／表示
FAU_SAR.3	a) 詳細：閲覧に使用されるパラメタ。	・監査ログの検索／表示
FAU_STG.1	なし。	なし。
FAU_STG.3	a) 基本：閾値を超えたためにとられるアクション。	なし。
FAU_STG.4	a) 基本：監査格納失敗によってとられるアクション。	なし。
FCS_CKM.1[a1]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	なし。

（続く）

（続き）

コンポーネント	監査対象アクション	監査対象事象
FCS_CKM.1[b]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	・監査者・RAサービス等の秘密鍵の生成
FCS_CKM.1[h]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	・CAオペレータの登録 ・CAオペレータの識別認証
FCS_CKM.1[i]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	・CAオペレータの登録
FCS_CKM.1[j]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	・CAオペレータの操作権の変更
FCS_CKM.2	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	・証明書の発行
FCS_CKM.4[a1]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	なし。
FCS_CKM.4[h]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	なし。
FCS_CKM.4[i]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	・CAオペレータの削除。

（続く）

（続き）

コンポーネント	監査対象アクション	監査対象事象
FCS_CKM.4[j]	a) 最小：動作の成功と失敗。 b) 基本：オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	なし。
FCS_COP.1[a1]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	なし。
FCS_COP.1[a2]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	なし。
FCS_COP.1[e]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	・RAサービスからの要求の受信
FCS_COP.1[f]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	・RAサービスからの要求の受信
FCS_COP.1[g]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	・CAオペレータの識別認証 ・CAオペレータの登録
FCS_COP.1[h]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	・CAオペレータの識別認証 ・CAオペレータの登録
FCS_COP.1[i]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	・CAオペレータの識別認証 ・CAオペレータの操作権の変更

（続く）

（続き）

コンポーネント	監査対象アクション	監査対象事象
FCS_COP.1[j]	a) 最小：成功と失敗及び暗号操作の種別。 b) 基本：すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	・CAオペレータの識別認証 ・CAオペレータの操作権の変更
FDP_ACC.1[a1]	なし。	なし。
FDP_ACC.1[a2]	なし。	なし。
FDP_ACF.1[a1]	a) 最小：SFPで扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本：SFPで扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細：アクセスチェック時に用いられる特定のセキュリティ属性。	・CAオペレータの登録、削除 ・CAオペレータのパスワードの変更 ・CAオペレータの操作権の変更 ・既存の証明書プロファイルの変更、新しい証明書プロファイルの追加、追加した証明書プロファイルの削除 ・既存のCRLプロファイルの変更 ・CA秘密鍵の活性化・非活性化 ・証明書の発行 ・証明書の失効 ・CRLの発行 ・他のCAが発行した証明書・CRLの登録 ・データベースで管理する証明書・CRLの削除 ・CA秘密鍵の生成・削除 ・CA秘密鍵のバックアップ・リストア
FDP_ACF.1[a2]	a) 最小：SFPで扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本：SFPで扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細：アクセスチェック時に用いられる特定のセキュリティ属性。	・CAオペレータの操作権の変更 ・証明書の発行 ・CA秘密鍵の活性化・非活性化 ・CA秘密鍵の生成・削除 ・CA秘密鍵のバックアップ・リストア
FDP_ETC.2	a) 最小：情報エクスポート成功。 b) 基本：情報をエクスポートするすべての試み。	なし。

（続く）

（続き）

コンポーネント	監査対象アクション	監査対象事象
FDP_ITC.1	a) 最小：任意のセキュリティ属性を含む、利用者データの成功したインポート。 b) 基本：任意のセキュリティ属性を含む、利用者データをインポートするすべての試み。 c) 詳細：許可利用者によって提供される、インポートされる利用者データに対するセキュリティ属性の仕様。	・証明書の発行。
FIA_ATD.1	なし。	なし。
FIA_SOS.1	a) 最小：TSFによる、テストされた秘密の拒否; b) 基本：TSFによる、テストされた秘密の拒否または受け入れ; c) 詳細：定義された品質尺度に対する変更の識別。	・CAオペレータの登録 ・CAオペレータのパスワードの変更
FIA_UAU.2	a) 最小：認証メカニズムの不成功になった使用。 b) 基本: 認証メカニズムのすべての使用。	・CAオペレータの識別認証 ・RAサービスからの要求の受信
FIA_UAU.7	なし。	なし。
FIA_UID.2	a) 最小：提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本：提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	・CAオペレータの識別認証 ・監査者の識別 ・RAサービスからの要求の受信
FIA_USB.1	a) 最小：利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本：利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功及び失敗)。	・CAオペレータの識別認証 ・監査者の識別

（続く）

（続き）

コンポーネント	監査対象アクション	監査対象事象
FMT_MSA.1[a1-1]	a) 基本：セキュリティ属性の値の改変すべて。	・CAオペレータの登録、削除
FMT_MSA.1[a1-2]	a) 基本：セキュリティ属性の値の改変すべて。	・CAオペレータの操作権の変更
FMT_MSA.1[a1-3]	a) 基本：セキュリティ属性の値の改変すべて。	なし。
FMT_MSA.1[a2]	a) 基本：セキュリティ属性の値の改変すべて。	・CAオペレータの操作権の変更
FMT_MSA.2[b]	a) 最小：セキュリティ属性に対して提示され、拒否された値すべて; b) 詳細：セキュリティ属性に対して提示され、受け入れられたセキュアな値すべて。	なし。
FMT_MSA.2[e-f]	a) 最小：セキュリティ属性に対して提示され、拒否された値すべて; b) 詳細：セキュリティ属性に対して提示され、受け入れられたセキュアな値すべて。	なし。
FMT_MSA.2[h-i-j]	a) 最小：セキュリティ属性に対して提示され、拒否された値すべて; b) 詳細：セキュリティ属性に対して提示され、受け入れられたセキュアな値すべて。	・CAオペレータの登録
FMT_MSA.3[a1-1]	a) 基本：許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本：セキュリティ属性の初期値の改変すべて。	なし。
FMT_MSA.3[a1-2]	a) 基本：許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本：セキュリティ属性の初期値の改変すべて。	なし。

（続く）

（続き）

コンポーネント	監査対象アクション	監査対象事象
FMT_MSA.3[a2]	a) 基本：許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本：セキュリティ属性の初期値の改変すべて。	なし。
FMT_MTD.1	a) 基本：TSFデータの値のすべての改変。	・証明書の発行 ・CAオペレータの登録、削除 ・CAオペレータのパスワードの変更 ・監査ログの検索／表示 ・監査ログの移出・移入、削除 ・監査者証明書の登録・削除
FMT_SMR.1	a) 最小：役割の一部をなす利用者のグループに対する改変； b) 詳細：役割の権限の使用すべて。	・CAオペレータの操作権の変更 ・CAオペレータの登録、削除 ・監査者証明書の登録・削除
FPT_RVM.1	なし。	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、サブジェクト識別子、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シーケンス番号***

依存性：　FPT_STM.1 高信頼タイムスタンプ（FPT_STM.1[E]）

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（FIA_UID.2）

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***
- ［割付：*監査情報のリスト*］：***FAU_GEN.1で規定される全ての監査情報***

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*］：***日付／時刻、事象の結果、事象、利用者ID***
- ［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

FAU_STG.3	監査データ損失の恐れ発生時のアクション

下位階層：　なし

FAU_STG.3.1

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

- ［割付：*事前に定義された限界*］：***ディスクの空き容量が10%未満***
- ［割付：*監査格納失敗の恐れ発生時のアクション*］：
  一定時間（60分）経過毎に、監査警告メッセージをWindows版はイベントログ、Solaris OE版はシステムログに記録。

依存性：　FAU_STG.1 保護された監査証跡格納

FAU_STG.4	監査データ損失の防止

下位階層：　FAU_STG.3

FAU_STG.4.1

TSFは、監査証跡が満杯になった場合、［選択：*監査対称事象の無視*、*特権をもつ許可利用者にかかわるもの以外の監査対象事象の抑止*、*最も古くに格納された監査記録への上書き*］及び［割付：*監査格納失敗時にとられるその他のアクション*］を行わねばならない。

- ［選択：*監査対称事象の無視*、*特権をもつ許可利用者にかかわるもの以外の監査対象事象の抑止*、*最も古くに格納された監査記録への上書き*］：
  特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止

- ［割付：*監査格納失敗時にとられるその他のアクション*］：
  監査警告メッセージをWindows版はイベントログ、Solaris OE版はシステムログに記録

依存性：　　FAU_STG.1 保護された監査証跡格納

(2)　暗号サポート（FCS）

表 5-3：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[a1]
		FCS_CKM.1[b]
		FCS_CKM.1[h]
		FCS_CKM.1[i]
		FCS_CKM.1[j]
	暗号鍵配付	FCS_CKM.2
	暗号鍵破棄	FCS_CKM.4[a1]
		FCS_CKM.4[h]
		FCS_CKM.4[i]
		FCS_CKM.4[j]
暗号操作	暗号操作	FCS_COP.1[a1]
		FCS_COP.1[a2]
		FCS_COP.1[e]
		FCS_COP.1[f]
		FCS_COP.1[g]
		FCS_COP.1[h]
		FCS_COP.1[i]
		FCS_COP.1[j]

FCS_CKM.1[a1]　暗号鍵生成

下位階層：　なし

FCS_CKM.1.1[a1]

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*］：***PKCS#1 "RSA Cryptography Standard"***
- ［割付：*暗号鍵生成アルゴリズム*］：***RSA***
- ［割付：*暗号鍵長*］：***1024bit***

依存性：　[~~FCS_CKM.2 暗号鍵配付~~
または
FCS_COP.1 暗号操作（FCS_COP.1[a1]）]
FCS_CKM.4 暗号鍵破棄（FCS_CKM.4[a1]）
~~FMT_MSA.2 セキュアなセキュリティ属性~~

FCS_CKM.1[b]　暗号鍵生成

下位階層：　なし

FCS_CKM.1.1[b]

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

- ［割付：*標準のリスト*］：***PKCS#1 "RSA Cryptography Standard"***
- ［割付：*暗号鍵生成アルゴリズム*］：***RSA***
- ［割付：*暗号鍵長*］：***512, 768, 1024, 2048bit***

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.1[h]	暗号鍵生成

下位階層：　なし

FCS_CKM.1.1[h]

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*］：***PKCS#5 v2.0 "Password-Based Cryptography Standard"***
- ［割付：*暗号鍵生成アルゴリズム*］：***PBKDF2***
- ［割付：*暗号鍵長*］：***168bit***

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

FCS_CKM.1[i]	暗号鍵生成

下位階層：　なし

FCS_CKM.1.1[i]

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*］：***PKCS#1 "RSA Cryptography Standard"***
- ［割付：*暗号鍵生成アルゴリズム*］：***RSA***
- ［割付：*暗号鍵長*］：***2048bit***

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

FCS_CKM.1[j]	暗号鍵生成

下位階層：　なし

FCS_CKM.1.1[j]

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*］：***FIPS PUB 46-3 “Data Encryption Standard(DES)”***
- ［割付：*暗号鍵生成アルゴリズム*］：***Triple-DES***
- ［割付：*暗号鍵長*］：***168bit***

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

FCS_CKM.2	暗号鍵配付

下位階層：　なし

FCS_CKM.2.1

TSFは、以下の［割付：*標準のリスト*］に合致する、指定された暗号鍵配付方法［割付：*暗号鍵配付方法*］に従って、暗号鍵を配付しなければならない。

- ［割付：*標準のリスト*］：
  ***PKCS#12 Personal Information Exchange Syntax Standard*、**
  X.509 The Directory: Public-Key And Attribute Certificate Frameworks
- ［割付：*暗号鍵配付方法*］：***証明書ベース鍵管理***

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.1[b]）]
~~FCS_CKM.4 暗号鍵破棄~~
FMT_MSA.2 セキュアなセキュリティ属性（FMT_MSA.2[b]）

FCS_CKM.4[a1]	暗号鍵破棄

下位階層：　なし

FCS_CKM.4.1[a1]

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*］：
  FIPS PUB 140-1 Security Requirements for Cryptographic Modules
- ［割付：*暗号破棄方法*］：
  0で上書き削除

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（FCS_CKM.1[a1]）]
~~FMT_MSA.2 セキュアなセキュリティ属性~~

FCS_CKM.4[h]	暗号鍵破棄

下位階層：　なし

FCS_CKM.4.1[h]

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*］：
  FIPS PUB 140-1 Security Requirements for Cryptographic Modules
- ［割付：*暗号破棄方法*］：
  0で上書き削除

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（FCS_CKM.1[h]）]
FMT_MSA.2 セキュアなセキュリティ属性（FMT_MSA.2[h-i-j]）

FCS_CKM.4[i]	暗号鍵破棄

下位階層：　なし

FCS_CKM.4.1[i]

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*］：
  FIPS PUB 140-1 Security Requirements for Cryptographic Modules
- ［割付：*暗号破棄方法*］：
  0で上書き削除

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（FCS_CKM.1[i]）]
FMT_MSA.2 セキュアなセキュリティ属性（FMT_MSA.2[h-i-j]）

FCS_CKM.4[j]	暗号鍵破棄

下位階層：　なし

FCS_CKM.4.1[j]

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*］：
  FIPS PUB 140-1 Security Requirements for Cryptographic Modules
- ［割付：*暗号破棄方法*］：
  0で上書き削除

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（FCS_CKM.1[j]）]
FMT_MSA.2 セキュアなセキュリティ属性（FMT_MSA.2[h-i-j]）

FCS_COP.1[a1]	暗号操作

下位階層：　なし

FCS_COP.1.1[a1]

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 "RSA Cryptography Standard"***
- ［割付：*暗号アルゴリズム*］：***SHA-1、RSA***
- ［割付：*暗号鍵長*］：***1024bit***
- ［割付：*暗号操作のリスト*］：***監査ログの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.1[a1]）]
FCS_CKM.4 暗号鍵破棄（FCS_CKM.4[a1]）
~~FMT_MSA.2 セキュアなセキュリティ属性~~

FCS_COP.1[a2]	暗号操作

下位階層：　なし

FCS_COP.1.1[a2]

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*］：***FIPS PUB 180-1 Secure Hash Standard***
- ［割付：*暗号アルゴリズム*］：***SHA-1***
- ［割付：*暗号鍵長*］：***なし***
- ［割付：*暗号操作のリスト*］：***監査ログのハッシュ値の生成***

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[e]	暗号操作

下位階層：　なし

FCS_COP.1.1[e]

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 "RSA Cryptography Standard"***
- ［割付：*暗号アルゴリズム*］：***SHA-1、RSA***
- ［割付：*暗号鍵長*］：***512bit, 768bit, 1024bit, 2048bit***
- ［割付：*暗号操作のリスト*］：***RA証明書の検証***

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（FMT_MSA.2[e-f]）

FCS_COP.1[f]	暗号操作

下位階層：　なし

FCS_COP.1.1[f]

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 "RSA Cryptography Standard"***
- ［割付：*暗号アルゴリズム*］：***SHA-1、RSA***
- ［割付：*暗号鍵長*］：***512bit, 768bit, 1024bit, 2048bit***
- ［割付：*暗号操作のリスト*］：
  RA証明書の公開鍵に対する秘密鍵で生成された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（FMT_MSA.2[e-f]）

FCS_COP.1[g]	暗号操作

下位階層：　なし

FCS_COP.1.1[g]

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*］：***FIPS PUB 46-3 “Data Encryption Standard(DES)”***
- ［割付：*暗号アルゴリズム*］：***Triple-DES***
- ［割付：*暗号鍵長*］：***168bit***
- ［割付：*暗号操作のリスト*］：***CAオペレータ証明書のシリアル番号の暗号化・復号化***

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[h]	暗号操作

下位階層：　なし

FCS_COP.1.1[h]

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*］：***FIPS PUB 46-3 “Data Encryption Standard(DES)”***
- ［割付：*暗号アルゴリズム*］：***Triple-DES***
- ［割付：*暗号鍵長*］：***168bit***
- ［割付：*暗号操作のリスト*］：***CAオペレータ毎の秘密鍵（CAオペレータ識別認証データ）の暗号化・復号化***

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.1[h]）]
FCS_CKM.4 暗号鍵破棄（FCS_CKM.4[h]）
FMT_MSA.2 セキュアなセキュリティ属性（FMT_MSA.2[h-i-j]）

FCS_COP.1[i]	暗号操作

下位階層：　なし

FCS_COP.1.1[i]

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 "RSA Cryptography Standard"***
- ［割付：*暗号アルゴリズム*］：***RSA***
- ［割付：*暗号鍵長*］：***2048bit***
- ［割付：*暗号操作のリスト*］：
  合議操作秘密情報の暗号化用TripleDES暗号鍵の暗号化・復号化

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.1[i]）]
FCS_CKM.4 暗号鍵破棄（FCS_CKM.4[i]）
FMT_MSA.2 セキュアなセキュリティ属性（FMT_MSA.2[h-i-j]）

FCS_COP.1[j]	暗号操作

下位階層：　なし

FCS_COP.1.1[j]

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*］：***FIPS PUB 46-3 "Data Encryption Standard(DES)"***
- ［割付：*暗号アルゴリズム*］：***Triple-DES***
- ［割付：*暗号鍵長*］：***168bit***
- ［割付：*暗号操作のリスト*］：***合議操作秘密情報の暗号化・復号化***

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.1[j]）]
FCS_CKM.4 暗号鍵破棄（FCS_CKM.4[j]）
FMT_MSA.2 セキュアなセキュリティ属性（FMT_MSA.2[h-i-j]）

(3)　利用者データ保護（FDP）

表 5-4：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[a1]
		FDP_ACC.1[a2]
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[a1]
		FDP_ACF.1[a2]
TSF制御外へのエクスポート	セキュリティ属性付き利用者データのエクスポート	FDP_ETC.2
TSF制御外からのインポート	セキュリティ属性なし利用者データのインポート	FDP_ITC.1

FDP_ACC.1[a1]　サブセットアクセス制御

下位階層：　なし

FDP_ACC.1.1[a1]

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*］：***表5-5***
- ［割付：*アクセス制御SFP*］：***CAオペレータアクセス制御SFP***

表 5-5：CAオペレータの全操作

サブジェクト	オブジェクト	操作
CAオペレータのプロセス	「PKCS#10形式の申請書に基づく相互認証証明書等の発行機能」実行オブジェクト	実行
	「監査者・RAサービス等の証明書とその秘密鍵をPKCS#12形式で作成機能」実行オブジェクト	実行
	「CA証明書の発行機能」実行オブジェクト	実行
	「CMPサービス証明書の発行機能」実行オブジェクト	実行
	「CAオペレータ証明書の発行機能」実行オブジェクト	実行
	「発行した証明書の失効機能」実行オブジェクト	実行
	「データベースで管理する証明書の削除機能」実行オブジェクト	実行
	「他のCAが発行した証明書のTOE外からの登録機能」実行オブジェクト	実行
	「CRLの発行機能」実行オブジェクト	実行
	「データベースで管理するCRLの削除機能」実行オブジェクト	実行
	「他のCAが発行したCRLのTOE外からの登録機能」実行オブジェクト	実行
	「CA秘密鍵の生成・削除機能」実行オブジェクト	実行
	「CA秘密鍵の活性化・非活性化機能」実行オブジェクト	実行
	「CA秘密鍵のバックアップ・リストア機能」実行オブジェクト	実行
	証明書プロファイル設定ファイル	読み込み、上書き、削除
	CRLプロファイル設定ファイル	読み込み、上書き
	CAオペレータ管理ファイル	読み込み、上書き、消去
	CAオペレータ認証管理ファイル	読み込み、上書き、削除
	CAオペレータ操作管理ファイル	読み込み、上書き
	合議操作管理ファイル	読み込み、上書き

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[a1]）

FDP_ACC.1[a2]　　サブセットアクセス制御

下位階層：　　なし

FDP_ACC.1.1[a2]

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*］：***表5-6***
- ［割付：*アクセス制御SFP*］：***合議操作アクセス制御SFP***

表 5-6：CAオペレータの合議操作

サブジェクト	オブジェクト	操作
CAオペレータのプロセス	「CA証明書の発行機能」実行オブジェクト	実行
	「CAオペレータ証明書の発行機能」実行オブジェクト	実行
	「CMPサービス証明書の発行機能」実行オブジェクト	実行
	「CA秘密鍵の生成・削除機能」実行オブジェクト	実行
	「CA秘密鍵のバックアップ・リストア機能」実行オブジェクト	実行
	「CA秘密鍵の活性化・非活性化機能」実行オブジェクト	実行
	CAオペレータ操作管理ファイル	読み込み、上書き
	合議操作管理ファイル	読み込み、上書き

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[a2]）

FDP_ACF.1[a1]　　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[a1]

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*］：
  CAオペレータID、実行オブジェクトIDおよびファイルの種類
- ［割付：*アクセス制御SFP*］：***CAオペレータアクセス制御SFP***

FDP_ACF.1.2[a1]

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*］：
  制御されたサブジェクトであるCAオペレータのプロセスは、各CAオペレータに対して登録されるCAオペレータIDという属性を持つ。
  実行オブジェクトは実行オブジェクトIDを属性として持ち、サブジェクト属性であるCAオペレータIDと関連付けられる。CAオペレータのプロセスは各実行オブジェクトの実行に際してCAオペレータIDと関連付けられた実行オブジェクトIDに実行オブジェクトの「実行」操作だけが許可される。
  各ファイルに対する操作はサブジェクト属性であるCAオペレータIDと関連付けられる。CAオペレータのプロセスは各ファイルに対する操作に対してCAオペレータIDと関連付けられた操作だけが許可される。

FDP_ACF.1.3[a1]

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[a1]

TSFは、［割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*］に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

- ［割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*］：***なし***

依存性：　FDP_ACC.1 サブセットアクセス制御（FDP_ACC.1[a1]）
FMT_MSA.3 静的属性初期化（FMT_MSA.3[a1-1]、FMT_MSA.3[a1-2]）

FDP_ACF.1[a2]　　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[a2]

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*］：
  CAオペレータID、実行オブジェクトIDおよびファイルの種類、実行が許可されるCAオペレータの必要最小人数
- ［割付：*アクセス制御SFP*］：***合議操作アクセス制御SFP***

FDP_ACF.1.2[a2]

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*］：
  制御された実行オブジェクトの実行オブジェクトIDおよび各ファイル毎に、操作の実行が許可されるCAオペレータの必要最小人数が関連付けられる。各オブジェクトの操作に対し、実行権限を持つCAオペレータが設定された最小人数が集まった場合、操作の実行が許可される。

FDP_ACF.1.3[a2]

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[a2]

TSFは、［割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*］に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

- ［割付：*セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*］：***なし***

依存性：　　FDP_ACC.1 サブセットアクセス制御（FDP_ACC.1[a2]）
FMT_MSA.3 静的属性初期化（FMT_MSA.3[a2]）

FDP_ETC.2	**セキュリティ属性付き利用者データのエクスポート**

下位階層：　　なし

FDP_ETC.2.1

TSFは、SFP(s)制御下にある利用者データをTSCの外部にエクスポートするとき、［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。

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

FDP_ETC.2.2

TSFは、利用者データに関係したセキュリティ属性と共に利用者データをエクスポートしなければならない。

FDP_ETC.2.3

TSFは、セキュリティ属性がTSCの外部にエクスポートされるとき、それがエクスポートされる利用者データに曖昧さなく関係付けられることを保証しなければならない。

FDP_ETC.2.4

TSFは、利用者データがTSCからエクスポートされるとき、以下の規則を実施しなければならない：［割付：*追加エクスポート制御規則*］。

- ［割付：*追加エクスポート制御規則*］：***なし***

依存性：　　[FDP_ACC.1 サブセットアクセス制御（FDP_ACC.1[a1]）、または
~~FDP_IFC.1 サブセット情報フロー制御~~]

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外から利用者データ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*］：
  CA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、利用者データ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

TSFは、SFPに従って制御され、TSC外から利用者データ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（FDP_ACC.1[a1]）、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~~

(4)　識別と認証（FIA）

表 5-7：FIA機能要件

セキュリティ機能要件		コンポーネント
利用者属性定義	利用者属性定義	FIA_ATD.1
秘密についての仕様	秘密の検証	FIA_SOS.1
利用者認証	アクション前の利用者認証	FIA_UAU.2
	保護された認証フィードバック	FIA_UAU.7
利用者識別	アクション前の利用者識別	FIA_UID.2
利用者・サブジェクト結合	利用者サブジェクト結合	FIA_USB.1

FIA_ATD.1	**利用者属性定義**

下位階層：　なし

FIA_ATD.1.1

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

- ［割付：*セキュリティ属性のリスト*］：***CAオペレータID、監査者ID***

依存性：　なし

FIA_SOS.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*］：***パスワードは6文字以上***

依存性：　なし

FIA_UAU.2	アクション前の利用者認証

下位階層：　FIA_UAU.1

FIA_UAU.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に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.2）

FIA_UAU.7	保護された認証フィードバック

下位階層：　なし

FIA_UAU.7.1

TSFは、認証を行っている間、［割付：*フィードバックのリスト*］だけを利用者に提供しなければならない。

- ［割付：*フィードバックのリスト*］：***入力されたパスワードの文字列を“＊”で表示***

依存性：　FIA_UID.1 識別のタイミング（FIA_UID.2）

FIA_UID.2	アクション前の利用者識別

下位階層：　FIA_UID.1

FIA_UID.2.1

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

依存性：　なし

FIA_USB.1	利用者・サブジェクト結合

下位階層：　なし

FIA_USB.1.1

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

依存性：　FIA_ATD.1 利用者属性定義

(5)　セキュリティ管理（FMT）

表 5-8：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[a1-1]
		FMT_MSA.1[a1-2]
		FMT_MSA.1[a1-3]
		FMT_MSA.1[a2]
	セキュアなセキュリティ属性	FMT_MSA.2[b]
		FMT_MSA.2[e-f]
		FMT_MSA.2[h-i-j]
	静的属性初期化	FMT_MSA.3[a1-1]
		FMT_MSA.3[a1-2]
		FMT_MSA.3[a2]
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[a1-1]　セキュリティ属性の管理

下位階層：　なし

FMT_MSA.1.1[a1-1]

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*］：***CA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*］］：
  問い合わせ、削除、［割付：その他の操作］：登録
- ［割付：*許可された識別された役割*］：
  「CAオペレータの登録・削除」操作の権限を持つCAオペレータ
- ［割付：*アクセス制御SFP*、*情報フロー制御SFP*］：***CA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（FDP_ACC.1[a1]）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[a1-2]　セキュリティ属性の管理

下位階層：　なし

FMT_MSA.1.1[a1-2]

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*］：
  CAオペレータID、操作ID（合議操作の場合は、合議操作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*］］：
  ［割付：その他の操作］：CAオペレータIDに対して操作IDを関連付ける操作、
  CAオペレータIDと操作IDの関連付けを問い合わせる操作
- ［割付：*許可された識別された役割*］：
  「CAオペレータの操作権の設定」操作の権限を持つCAオペレータ
- ［割付：*アクセス制御SFP*、*情報フロー制御SFP*］：***CA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（FDP_ACC.1[a1]）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[a1-3]　セキュリティ属性の管理

下位階層：　なし

FMT_MSA.1.1[a1-3]

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*］：
  CAオペレータ証明書の有効期限、CAオペレータ証明書の所有者、監査者証明書の有効期限、監査者証明書の所有者、RA証明書の有効期限、RA証明書の所有者
- ［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
- ［割付：*許可された識別された役割*］：
  CAオペレータ
- ［割付：*アクセス制御SFP*、*情報フロー制御SFP*］：***CA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（FDP_ACC.1[a1]）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[a2]　セキュリティ属性の管理

下位階層：　なし

FMT_MSA.1.1[a2]

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*］：
  合議操作の実行が許可されるCAオペレータの必要最小人数

- ［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*］］：
  デフォルト値変更、問い合わせ、改変
- ［割付：*許可された識別された役割*］：
  「CAオペレータの操作権の設定」操作の権限を持つCAオペレータ
- ［割付：*アクセス制御SFP、情報フロー制御SFP*］：***合議操作アクセス制御SFP***

依存性：　[FDP_ACC.1 サブセットアクセス制御（FDP_ACC.1[a2]）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[b]	**セキュアなセキュリティ属性**

下位階層：　なし

FMT_MSA.2.1[b]

TSFは、セキュアな値だけが***CA、CAオペレータ、監査者、RAサービスの公開鍵の有効期間及び所有者***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（FDP_ACC.1[a1]）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_MSA.1[a1-3]）
FMT_SMR.1 セキュリティ役割

FMT_MSA.2[e-f]	**セキュアなセキュリティ属性**

下位階層：　なし

FMT_MSA.2.1[e-f]

TSFは、セキュアな値だけが***CA、RAサービスの公開鍵の有効期間***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.2[h-i-j]　セキュアなセキュリティ属性

下位階層：　なし

FMT_MSA.2.1[h-i-j]

TSFは、セキュアな値だけが***合議操作時に必要となる暗号鍵の利用者（CAオペレータ）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[a1-1]　静的属性初期化

下位階層：　なし

FMT_MSA.3.1[a1-1]

TSF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*］：
  許可的
- ［割付：*アクセス制御SFP、情報フロー制御SFP*］：***CAオペレータアクセス制御SFP***

FMT_MSA.3.2[a1-1]

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_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.1[a1-3]）
FMT_SMR.1 セキュリティの役割

FMT_MSA.3[a1-2]　静的属性初期化

下位階層：　なし

FMT_MSA.3.1[a1-2]

TSF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*］：***CAオペレータアクセス制御SFP***

FMT_MSA.3.2[a1-2]

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_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.1[a1-3]）
FMT_SMR.1 セキュリティの役割

FMT_MSA.3[a2]　静的属性初期化

下位階層：　なし

FMT_MSA.3.1[a2]

TSF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*］：***合議操作アクセス制御SFP***

FMT_MSA.3.2[a2]

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_MSA.1[a2]）
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5-9「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5-9「操作」***
- ［割付：*許可された識別された役割*］：***表5-9「役割」***

表 5-9：TSF**データの管理**

TSFデータ	操作	役割
監査者証明書、 RA証明書	[割付：*その他の操作*]：発行	「PKCS#12形式の証明書の発行」操作の権限を持つCAオペレータ
CAオペレータ証明書	[割付：*その他の操作*]：発行	「CAオペレータ証明書の発行」操作の権限を持つCAオペレータ
CA証明書	[割付：*その他の操作*]：発行	「CA証明書の発行」操作の権限を持つCAオペレータ
CAオペレータパスワード	改変、 [割付：*その他の操作*]：登録	CAオペレータ
監査ログ	[割付：*その他の操作*]：インポート、エクスポート、削除、検証	監査者
監査者識別データ （監査者証明書）	[割付：*その他の操作*]：インポート（登録）、削除	既にTOEに対して登録されている監査者

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*］：　***CAオペレータ、監査者***

FMT_SMR.1.2

TSFは、利用者を役割に関連づけなければならない。

依存性：　　FIA_UID.1 識別のタイミング（FIA_UID.2）

(6)　TSFの保護（FPT）

表 5-10：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

FPT_RVM.1	**TSPの非バイパス性**

下位階層：　　なし

FPT_RVM.1.1

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

依存性：　　なし

5.1.2　TOEセキュリティ機能強度主張

TOEは、商用システムとして低レベルの攻撃能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-基本を提供する。確率的または順列的メカニズムを適用するのはFIA_SOS.1、FCS_CKM.1[a1]、FCS_CKM.1[b]、FCS_CKM.1[h]、FCS_CKM.1[i]、FCS_CKM.1[j]、FCS_CKM.2、FCS_CKM.4[a1]、FCS_CKM.4[h]、FCS_CKM.4[i]、FCS_CKM.4[j]、FCS_COP.1[a1]、FCS_COP.1[a2]、FCS_COP.1[e]、FCS_COP.1[f]、FCS_COP.1[g]、FCS_COP.1[h]、FCS_COP.1[i]、FCS_COP.1[j]である。このうちTOE機能強度が対象とするものはパスワードメカニズムと合議制メカニズムであり、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_CKM.1[a1]、FCS_CKM.1[b]、FCS_CKM.1[h]、FCS_CKM.1[i]、FCS_CKM.1[j]、FCS_CKM.2、FCS_CKM.4[a1]、FCS_CKM.4[h]、FCS_CKM.4[i]、FCS_CKM.4[j]、FCS_COP.1[a1]、FCS_COP.1[a2]、FCS_COP.1[e]、FCS_COP.1[f]、FCS_COP.1[g]、FCS_COP.1[h]、FCS_COP.1[i]、FCS_COP.1[j]は、TOE機能強度の対象外である。

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を評価保証レベルとする。本STでは表5-11に示すようにEAL3で規定さ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 5-11：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

(1)　暗号サポート（FCS）

表 5-12：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[E]
	暗号鍵破棄	FCS_CKM.4[E]
暗号操作	暗号操作	FCS_COP.1[E][b]
		FCS_COP.1[E][c]
		FCS_COP.1[E][d]

FCS_CKM.1[E]　　暗号鍵生成

下位階層：　　なし

FCS_CKM.1.1[E]

HSM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*］：***PKCS#1 "RSA Cryptography Standard"***
- ［割付：*暗号鍵生成アルゴリズム*］：***RSA***
- ［割付：*暗号鍵長*］：***512, 768, 1024, 2048bit***

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

FCS_CKM.4[E]　　暗号鍵破棄

下位階層：　　なし

FCS_CKM.4.1[E]

HSM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*］：
  FIPS PUB 140-1 Security Requirements for Cryptographic Modules
- ［割付：*暗号破棄方法*］：***0で上書き削除***

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（FCS_CKM.1[E]）]
~~FMT_MSA.2 セキュアなセキュリティ属性~~

FCS_COP.1[E][b]　暗号操作

下位階層：　なし

FCS_COP.1.1[E][b]

HSM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 "RSA Cryptography Standard"***
- ［割付：*暗号アルゴリズム*］：***SHA-1、RSA***
- ［割付：*暗号鍵長*］：***512, 768, 1024, 2048bit***
- ［割付：*暗号操作のリスト*］：
  CAオペレータ証明書、監査者証明書、RA証明書、CA証明書の発行におけるディジタル署名の生成

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.1[E]）]
FCS_CKM.4 暗号鍵破棄（FCS_CKM.4[E]）
~~FMT_MSA.2 セキュアなセキュリティ属性~~

FCS_COP.1[E][c]　暗号操作

下位階層：　　なし

FCS_COP.1.1[E][c]

WWWサービスは、［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 "RSA Cryptography Standard"***
- ［割付：*暗号アルゴリズム*］：***SHA-1、RSA***
- ［割付：*暗号鍵長*］：***512, 768, 1024, 2048bit***
- ［割付：*暗号操作のリスト*］：***CAオペレータ証明書、監査者証明書の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（FMT_MSA.2[E]）

FCS_COP.1[E][d]　暗号操作

下位階層：　　なし

FCS_COP.1.1[E][d]

WWWサービスは、［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 "RSA Cryptography Standard"***
- ［割付：*暗号アルゴリズム*］：***SHA-1、RSA***
- ［割付：*暗号鍵長*］：***512, 768, 1024, 2048bit***
- ［割付：*暗号操作のリスト*］：
  CAオペレータ証明書、監査者証明書中の公開鍵のペアである秘密鍵により生成された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（FMT_MSA.2[E]）

(2)　**利用者データ保護**（FDP）

表 5-13：FDP**機能要件** [IT**環境**]

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[E]

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*］：***表5-14***
- ［割付：*アクセス制御SFP*］：***OSアクセス制御SFP***

表 5-14：**サブジェクトのオブジェクトに対する操作** [IT**環境**]

サブジェクト	**オブジェクト**	**操作**
OS利用者のプロセス	TOEが扱うファイル、TOEが扱うファイルが保管されるディレクトリ	ファイルの読み込み、 ファイルの書き込み、 ディレクトリの読み込み、 ディレクトリの書き込み

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]）

FDP_ACF.1[E]　　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[E]

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[E]

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の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*]：
  制御されたオブジェクトであるTOEが扱うファイルおよびそのファイルが保管されるディレクトリに対し、制御された操作（ファイル及びディレクトリに対する読み込み、書き込み）を行なうことは、OSの利用者属性であるアドミニストレータグループに関連付けられるOS利用者IDをもつ制御されたサブジェクトであるOS利用者のプロセスにだけ許可される。

FDP_ACF.1.3[E]

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[E]

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（FDP_ACC.1[E]）
　　FMT_MSA.3 静的属性初期化（FMT_MSA.3[E]）

(3)　識別と認証（FIA）

表 5-15：FIA機能要件 [IT環境]

セキュリティ機能要件		コンポーネント
利用者認証	アクション前の利用者認証	FIA_UAU.2[E][d1]
		FIA_UAU.2[E][d2]
		FIA_UAU.2[E][d3]
利用者識別	アクション前の利用者識別	FIA_UID.2[E][d1]
		FIA_UID.2[E][d2]

FIA_UAU.2[E][d1]　アクション前の利用者認証

下位階層：　FIA_UAU.1

FIA_UAU.2.1[E][d1]

WWWサービスは、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.2[E][d1]、FIA_UID.2）

FIA_UAU.2[E][d2]　アクション前の利用者認証

下位階層：　FIA_UAU.1

FIA_UAU.2.1[E][d2]

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.2[E][d2]）

FIA_UAU.2[E][d3]　　アクション前の利用者認証

下位階層：　　FIA_UAU.1

FIA_UAU.2.1[E][d3]

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.2[E][d1]　　アクション前の利用者識別

下位階層：　　FIA_UID.1

FIA_UID.2.1[E][d1]

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

依存性：　　なし

FIA_UID.2[E][d2]　　アクション前の利用者識別

下位階層：　　FIA_UID.1

FIA_UID.2.1[E][d2]

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

(4)　セキュリティ管理（FMT）

TOEはOS上で動作する。OSは、TOE内のファイル（TOE動作環境ファイルと監査ログファイル）の管理に関係し、これらに不当にアクセスされることを防止する機能を提供する。

表 5-16：FMT機能要件 [IT環境]

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[E]
	セキュアなセキュリティ属性	FMT_MSA.2[E]
	静的属性初期化	FMT_MSA.3[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[E]　セキュリティ属性の管理

下位階層：　なし

FMT_MSA.1.1[E]

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*］：
  ファイル及びディレクトリの属性（読み込み、書き込み）
- ［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、［割付：*その他の操作*］：***有効化、無効化***
- ［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（FDP_ACC.1[E]）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_SMR.1[E]）

FMT_MSA.2[E]	セキュアなセキュリティ属性

下位階層：　なし

FMT_MSA.2.1[E]

WWWサーバは、セキュアな値だけが***CA、CAオペレータ、監査者の公開鍵の有効期間***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[E]	静的属性初期化

下位階層：　なし

FMT_MSA.3.1[E]

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*］：***許可的***
- ［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[E]

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_MSA.1[E]）
FMT_SMR.1 セキュリティの役割（FMT_SMR.1[E]）

FMT_SMR.1[E]	**セキュリティ役割**

下位階層：　　なし

FMT_SMR.1.1[E]

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*］：

  システム管理者

FMT_SMR.1.2[E]

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（FIA_UID.2[E][d2]）

(5)　TSF**の保護**（FPT）

表 5-17：FPT**機能要件** [IT**環境**]

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

FPT_SEP.1[E]	**TSFドメイン分離**

下位階層：　　なし

FPT_SEP.1.1[E]

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[E]

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

FPT_STM.1[E]　　高信頼タイムスタンプ

下位階層：　　なし

FPT_STM.1.1[E]

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

(6)　**高信頼パス／チャネル**（FTP）

表 5-18：FTP**機能要件** [IT**環境**]

セキュリティ機能要件		コンポーネント
高信頼パス／チャネル	高信頼パス	FTP_TRP.1[E]

FTP_TRP.1[E]　　高信頼パス

下位階層：　　なし

FTP_TRP.1.1[E]

WWWサービスは、それ自身と［選択：*リモート*、*ローカル*］利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスを提供しなければならない。

- ［選択：*リモート*、*ローカル*］：***リモート***

FTP_TRP.1.2[E]

WWWサービスは、［選択：*TSF*、*ローカル利用者*、*リモート利用者*］が、高信頼パスを介して通信を開始することを許可しなければならない。

- ［選択：*TSF*、*ローカル利用者*、*リモート利用者*］：***リモート利用者***

FTP_TRP.1.3[E]

WWWサービスは、［選択：*最初の利用者認証*、［割付：*高信頼パスが要求される他のサービス*］］に対して、高信頼パスの使用を要求しなければならない。

- ［選択：*最初の利用者認証*、［割付：*高信頼パスが要求される他のサービス*］］：
  最初の利用者認証

依存性：　　なし

6　TOE要約仕様

6.1　TOEセキュリティ機能

ここでは、TOEのセキュリティ機能について記述する。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

TOEセキュリティ機能		ID
識別／アクセス制御機能	CAオペレータ証明書による識別、及びアクセス制御機能	F.I&ACCESS.1
識別認証／アクセス制御機能	CAオペレータIDとパスワードによる識別認証、及びアクセス制御機能	F.IA&ACCESS.2
識別機能	監査者証明書による識別機能	F.I.3
識別認証機能	RA証明書による識別認証機能	F.IA.4
監査機能	監査ロギング機能	F.AUDIT.1
	監査ログ完全性・連続性検証機能	F.AUDIT.2
	監査ログ操作機能	F.AUDIT.3
	監査ログ損失防止機能	F.AUDIT.4

TOEのセキュリティ機能とセキュリティ機能要件の関係を表6-2に示す。これらでセキュリティ機能要件がTOEのセキュリティ機能によって全て満たされる。

表 6-2：セキュリティ機能要件とTOE要約仕様の関係

TOE要約仕様 / セキュリティ機能要件	F.I&ACCESS.1	F.IA&ACCESS.2	F.I.3	F.IA.4	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4
FAU_GEN.1					●			
FAU_GEN.2					●			
FAU_SAR.1							●	
FAU_SAR.2							●	
FAU_SAR.3							●	
FAU_STG.1					●	●		
FAU_STG.3								●
FAU_STG.4								●
FCS_CKM.1[a1]					●			
FCS_CKM.1[b]	●							
FCS_CKM.1[h]		●						
FCS_CKM.1[i]		●						
FCS_CKM.1[j]		●						
FCS_CKM.2	●							
FCS_CKM.4[a1]					●			
FCS_CKM.4[h]		●						
FCS_CKM.4[i]		●						
FCS_CKM.4[j]		●						
FCS_COP.1[a1]					●	●		
FCS_COP.1[a2]					●	●		
FCS_COP.1[e]				●				
FCS_COP.1[f]				●				

（続く）

（続き）

TOE要約仕様 / セキュリティ機能要件	F.I&ACCESS.1	F.IA&ACCESS.2	F.I.3	F.IA.4	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4
FCS_COP.1[g]	●							
FCS_COP.1[h]		●						
FCS_COP.1[i]		●						
FCS_COP.1[j]		●						
FDP_ACC.1[a1]	●							
FDP_ACC.1[a2]		●						
FDP_ACF.1[a1]	●							
FDP_ACF.1[a2]		●						
FDP_ETC.2	●							
FDP_ITC.1	●							
FIA_ATD.1	●						●	
FIA_SOS.1		●						
FIA_UAU.2		●		●				
FIA_UAU.7		●						
FIA_UID.2	●	●	●	●				
FIA_USB.1	●						●	
FMT_MSA.1[a1-1]	●							
FMT_MSA.1[a1-2]	●							
FMT_MSA.1[a1-3]	●							
FMT_MSA.1[a2]		●						
FMT_MSA.2[b]	●							
FMT_MSA.2[e-f]				●				
FMT_MSA.2[h-i-j]		●						
FMT_MSA.3[a1-1]	●							
FMT_MSA.3[a1-2]	●							

（続く）

（続き）

TOE要約仕様 ＼ セキュリティ機能要件	F.I&ACCESS.1	F.IA&ACCESS.2	F.I.3	F.IA.4	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4
FMT_MSA.3[a2]		●						
FMT_MTD.1	●						●	
FMT_SMR.1	●	●	●				●	
FPT_RVM.1	●	●	●	●				

6.1.1　識別・識別認証／アクセス制御機能

(1)　F.I&ACCESS.1（CAオペレータ証明書による識別／アクセス制御機能）

F.I&ACCESS.1は、表6-3の操作を行うTOE利用者をCAオペレータに限定するため、WWWサービス機能から受け取ったCAオペレータ証明書を使用したTOEの識別機能、及び識別されたCAオペレータが操作権を持つ場合にだけ表6-3の操作を許可するためのTOEのアクセス制御機能である。

表 6-3：CAオペレータの操作

分類	内容
証明書・CRL管理機能	・ 既存の証明書プロファイルの変更 ・ 新しい証明書プロファイルの追加 ・ 追加した証明書プロファイルの削除 ・ 既存のCRLプロファイルの変更 ・ CA証明書・CAオペレータ証明書・CMPサービス証明書の発行 ・ PKCS#10形式の申請書に基づく相互認証証明書等の発行 ・ 監査者・RAサービス等の証明書とその秘密鍵をPKCS#12形式で作成 ・ 発行した証明書の失効 ・ CRLの発行 ・ 他のCAが発行した証明書・CRLの登録 ・データベースで管理する証明書・CRLの削除
CA秘密鍵管理機能	・CA秘密鍵の生成・削除 ・CA秘密鍵のバックアップ・リストア ・CA秘密鍵の活性化・非活性化

運用管理機能	・CAオペレータの操作権の設定 ・CAオペレータの登録・削除

TOEは、各操作を示す操作IDに対して、操作権限を持つCAオペレータのCAオペレータIDを関連付けて管理する。1つの操作IDに対しては、複数人のCAオペレータIDを関連付けることができる。なお、この情報は、「CAオペレータの操作権限の設定」操作を許可されたCAオペレータだけが管理できるようにF.IA&ACCESS.2「CAオペレータIDとパスワードによる識別認証／アクセス制御機能」により制御される。

TOEは、初期セットアップ時には、各操作IDに対して、登録されている全てのCAオペレータIDを関連付ける。運用中に、新たに登録されたCAオペレータIDは、デフォルトでは全ての操作を実行する権限を持たない。

TOEは、次のようにCAオペレータ証明書を用いて、CAオペレータを識別し、操作権限を持っているかどうか確認する。

① TOEは、CAオペレータからのアクセスに対して、TOE外部機能であるWWWサービス機能からCAオペレータ証明書を取得する。このCAオペレータ証明書は、TOE自身がHSMを利用して発行したものであり、そのCAオペレータ証明書はWWWサービス機能によって証明書が検証され、証明書の正当性が確認される。

② TOEはこの証明書のシリアル番号を「CAオペレータ識別データ（CAオペレータ管理ファイル）」から検索する。「CAオペレータ識別データ（CAオペレータ管理ファイル）」は、アクセスを許可するCAオペレータの情報として、CAオペレータ証明書のシリアル番号とCAオペレータIDの関連情報を定義するデータである。なお、シリアル番号は、Triple-DES暗号アルゴリズムに従い168bitの鍵で暗号化した状態であるため、復号化を行い検索する。

③ 一致するシリアル番号が見つかった場合、それに対し定義されているCAオペレータIDを検索する。シリアル番号が一致するCAオペレータを特定することでCAオペレータを識別する。

④ CAオペレータが行う操作のIDを「CAオペレータ操作管理データ（CAオペレータ操作管理ファイル）」から検索する。「CAオペレータ操作管理データ（CAオペレータ操作管理ファイル）」は、アクセス制御を行うための情報として、CAオペレータの操作全てについて各々権限を持つCAオペレータIDを定義しているデータである。

⑤ 一致する操作IDが見つかった場合、それに対し登録されているCAオペレータIDの中から、識別時に特定したCAオペレータIDを検索する。CAオペレータがその操作に対して操作権を持つ者として登録されている場合には操作の実行を許可し、登録されていない場合には操作の実行を拒否する。

⑥ TOEは、許可されたCAオペレータを、CAオペレータを代行して動作するCAオペレータプロセスに結合する。

TOEを利用するCAオペレータは、TOEにCAオペレータとして登録され、予め証明書が格納されたICカードが配付されている必要がある。CAオペレータ証明書の発行時には「CAオペレータ証明書の発行」操作権限を持つCAオペレータによって操作され、ICカード内で生成されたRSA公開鍵ペアのうち公開鍵がTOEにインポートされ、それに対して証明書が発行される。発行された証明書はCAオペレータ証明書としてTOEからエクスポートされ、ICカードに格納される。このとき、TOEは、発行した証明書のシリアル番号をTriple-DES暗号アルゴリズムを用いて暗号化し、CAオペレータ識別データ（CAオペレータ管理ファイル）にCAオペレータIDと関連付けて格納する。

本機能で許可されたCAオペレータのうち、「PKCS#12形式の証明書の発行」操作権限を持つCAオペレータによって、監査者及びRAサービスに対するRSA公開鍵ペアを生成、証明書を発行し、監査者及びRAサービスに対してPKCS#12形式のデータによってRSA秘密鍵と証明書が配付される。

また、本機能によって識別されたCAオペレータのみが、データベースで管理している証明書の内容を表示する操作、及び、データベースで管理する証明書・CRLをCA操作端末に取り出す操作が許可される。

(2)　F.IA&ACCESS.2（CA**オペレータ**ID**とパスワードによる識別認証／アクセス制御機能）**

F.IA&ACCESS.2は、表6-4の操作を行うTOE利用者をCAオペレータに限定するためのCAオペレータIDとパスワードによる識別認証機能、及び識別認証されたCAオペレータが操作権を持つ場合にだけ表6-4の操作を許可するアクセス制御機能かつ操作権を持つCAオペレータが当該操作に決められた必要最小人数揃っている場合にだけ操作を許可する合議制アクセス制御機能である。

表 6-4：CA**オペレータの合議操作**

分類	内容
証明書・CRL管理機能	・CA証明書・CAオペレータ証明書・CMPサービス証明書の発行
CA秘密鍵管理機能	・CA秘密鍵の生成・削除 ・CA秘密鍵の活性化・非活性化 ・CA秘密鍵のバックアップ・リストア
運用管理機能	・CAオペレータの操作権の設定

TOEは、CAオペレータを以下のように登録する。なお、本操作は初期セットアップ時にはシステム管理者によって実施されるが、運用中は「CAオペレータの登録」操作の実行権を持つCAオペレータによってのみ実施することができるようにF.I&ACCESS.1によって制御する。また、パスワードは運用中にはCAオペレータ自身によってのみ変更可能である。

① 操作権限を持つCAオペレータによって、CAオペレータIDとパスワードが入力される。このとき、パスワードは6文字以上でなければならない。

② TOEはCAオペレータ用のRSA公開鍵ペア（2048ビット）を生成する。次に入力されたパスワードからPKCS#5 PBKDF2方式に従ってTriple-DES暗号鍵を生成し、そのTriple-DES暗号鍵によってRSA秘密鍵が暗号化され、「CAオペレータ識別認証データ（CAオペレータ認証管理ファイル）」とする。「CAオペレータ識別認証データ（CAオペレータ認証管理ファイル）」は、ファイル名にCAオペレータIDを用いてファイルとして保管される。なお、Triple-DES暗号鍵は0で上書きし、メモリ上から削除する。

③ TOEは、CAオペレータIDを「CAオペレータ識別データ（CAオペレータ管理ファイル）」として格納する。

TOEは、CAオペレータの操作権限は以下のように設定する。なお、本操作は初期セットアップ時にはシステム管理者によって実施されるが、運用中は「CAオペレータの操作権限の設定」操作の実行権を持つCAオペレータによってのみ実施することができる。

① CAオペレータは、それぞれの操作に対して実行時に必要となる必要最小人数と、操作権限を持つCAオペレータを必要最小人数以上選択する。

② TOEは、合議操作IDに対する秘密情報を実行権限を持つCAオペレータ全人数と必要最小人数を使ってShamir閾値秘密分散法にしたがって分散する。

③ TOEは、CAオペレータ毎に、実行権限を持つ合議操作ID毎の分散された秘密情報をまとめて、一時的に生成したTriple-DES暗号鍵によって暗号化し、さらにそのTriple-DES暗号鍵をそれぞれのCAオペレータに対応する「CAオペレータ識別認証データ（CAオペレータ認証管理ファイル）」中のRSA公開鍵で暗号化し合議操作秘密情報とする。TOEは、登録されているCAオペレータ全員に対応する合議操作秘密情報を生成し、ファイル名にそれぞれのCAオペレータIDを用いて合議操作管理ファイルとして保管する。一時的に生成したTriple-DES暗号鍵は0で上書きし、メモリ上から削除する。

④ TOEは、各操作IDに対して操作権限を持つCAオペレータIDと必要最小人数を関連付け、「CAオペレータ操作管理データ（CAオペレータ操作管理ファイル）」として格納する。

TOEは、表6-4に示した操作実行時には当該操作の実行権限を持つCAオペレータが必要最小人数揃っている場合のみ、以下のように許可する。

① それぞれのCAオペレータはTOEに登録されている各自のCAオペレータIDとパスワードを入力する。このとき、入力されたパスワードは“＊”として表示される。

② TOEは、それぞれのCAオペレータIDを「CAオペレータ識別データ（CAオペレータ管理ファイル）」から検索し、CAオペレータIDをファイル名として持つ「CAオペレータ識別認証データ（CAオペレータ認証管理ファイル）」を検索する。入力されたパスワードからPKCS#5 PBKDF2方式に従ってTriple-DES鍵を導出し、そのTriple-DES鍵によってCAオペレータ識別認証データ中のRSA秘密鍵を復号化する。正しいパスワードが入力されている場合には、正しくRSA秘密鍵が復号化されるが、誤ったパスワードが入力されている場合にはRSA秘密鍵は復号化されない。Triple-DES暗号鍵は、0で上書きし、メモリ

上から削除する。

③ CAオペレータのRSA秘密鍵が復号化された場合、TOEはそのRSA秘密鍵を用いて、それぞれのCAオペレータが操作の実行権限を持つ合議操作IDが格納された合議操作秘密情報（合議操作管理ファイル）を暗号化したTriple-DES暗号鍵を復号化し、復号したTriple-DES暗号鍵を用いて合議操作秘密情報を復号化する。

④ TOEは、それぞれのCAオペレータの合議操作秘密情報（合議操作管理ファイル）から当該操作に対する秘密情報を取り出し、それらをShamir閾値秘密分散法により復元することにより、正しく実行権を持つCAオペレータが必要最小人数分、揃っているかどうかを確認する。

なお、CAオペレータを削除する際には、「CAオペレータ識別認証データ（CAオペレータ認証管理ファイル）」に含まれるRSA秘密鍵は0で上書きされ削除される。また、合議操作管理ファイルとして管理されている該当するCAオペレータに対する合議操作秘密情報も削除される。

また、CAオペレータ識別認証データ及び合議操作秘密情報は、それぞれファイル名に設定されたCAオペレータIDがセキュリティ属性であり、CAオペレータIDとそれぞれのファイル名が一致してなければならない。これらのファイルはOSのアクセス制御によってセキュアな状態が維持されている。

6.1.2 識別・識別認証機能

(1) F.I.3（監査者証明書による識別機能）

F.I.3は、表6-5の操作を行うTOE利用者を監査者に限定するため、WWWサービス機能から受け取った監査者証明書を使用したTOEの識別機能である。

表 6-5：監査者の操作

分類	内容
監査機能	・監査ログの検索／表示 ・監査ログの移出・移入、削除 ・監査者証明書の登録・削除

TOEは、以下のように監査者を識別する。

① TOEは、TOE外部機能であるWWWサービス機能から監査者証明書を取得する。監査者証明書は、TOEがHSMを利用して発行したものであり、その監査者証明書はWWWサービス機能によって証明書が検証され、証明書の正当性が確認される。

② TOEはWWWサービス機能から取得した監査者証明書と一致する証明書を「監査者識別デ

ータ（監査者管理ファイル）」から検索する。「監査者識別データ（監査者管理ファイル）」は、アクセスを許可する監査者証明書と監査者IDを予め定義するデータである。

③　一致する証明書が登録されていることを確認することにより、監査者IDを識別する。識別された監査者だけが表6-5に示す操作を実行することができる。

本セキュリティ機能で使用する「監査者識別データ（監査者管理ファイル）」に対する登録、改変、削除の操作は、構築時はシステム管理者、運用開始後は監査者に限定されている。

(2)　F.IA.4（RA**証明書による識別認証機能**）

F.IA.4は、CAサービスとの通信を許可するRAサービスからの要求だけを受理するための識別認証機能である。

TOEは以下のようにRAサービスを識別認証する。なお、一般利用者証明書の発行・失効の要求時にRAサービスから送信されるCMP要求メッセージには、RAサービスのRSA秘密鍵を用いたディジタル署名とそのRSA秘密鍵に対応するRA証明書が含まれる。

①　TOEは、CMP要求メッセージに含まれるRA証明書をCA証明書のRSA公開鍵を用いて検証し、正しい証明書であることを確認する。

②　TOEは、RA証明書中のRSA公開鍵を用いて、CMP要求メッセージに含まれるRAサービスのRSA秘密鍵によるディジタル署名を検証し、正しくRAサービスから送信されたメッセージであることを確認する。

③　TOEは、CMP要求メッセージに含まれるRA証明書を「RA識別データ（RA管理ファイル）」から検索し、そのRA証明書のRAサービスIDを特定する。RAサービスIDが特定できるかどうかにより、許可されているRAサービスであることを確認する。

「RA識別データ（RA管理ファイル）」は、アクセスを許可するRAサービスの情報として、RA証明書とRAサービスIDを予め登録されるデータである。この「RA識別データ（RA管理ファイル）」に対する登録、改変、削除の操作、及び識別認証に使用するCA証明書の登録は、システム管理者に限定される。

6.1.3　監査機能

(1)　F.AUDIT.1（監査ロギング機能）

F.AUDIT.1は、CA管理機能、監査機能、RAサービスのセキュリティに関連する操作で発生する全ての事象を、表6-6に示す情報で構成する監査ログレコードとして記録する機能である。本機能により誰が、いつ、どのような操作を行ったか等のTOEの操作履歴を管理することができる。

表 6-6：監査ログに記録する情報

記録する情報	説明
番号	レコードに割り振られるシーケンス番号。
日付／時刻	監査ログを記録した日付と時刻。
事象の結果	“ 成功 ” または “ 失敗 ”
事象	操作事象を示す文字列。
利用者ID	事象の操作を行なった監査者、CAオペレータ、RAサービスの識別情報。
詳細情報	追加詳細情報。例えば、以下の情報を記録する。 “ 理由 ”（事象の結果が「失敗」の場合、その理由）

TOEは、監査ログレコードの完全性と連続性を保証するために、図6-1に示すように監査ログデータを保護する。なお、図6-1中のH(S(D))はS(D)のハッシュ値を、S(D)はディジタル署名を意味する。

① SHA-1アルゴリズムを用いて1つ前の監査ログレコードに付加されているディジタル署名のハッシュ値を生成する。そのハッシュ値を監査ログレコードに含めることにより、前監査ログレコードとの連鎖を生成する。これにより、監査ログレコードの連続性を検証することで、不正に削除されたかどうかを検出できる。

② 監査ログレコードには、1つ前のレコードのSHA-1によるハッシュ値を含めデータに対して、RSA秘密鍵によるディジタル署名を生成し、付加する。これにより、監査ログレコードの完全性を検証できる。

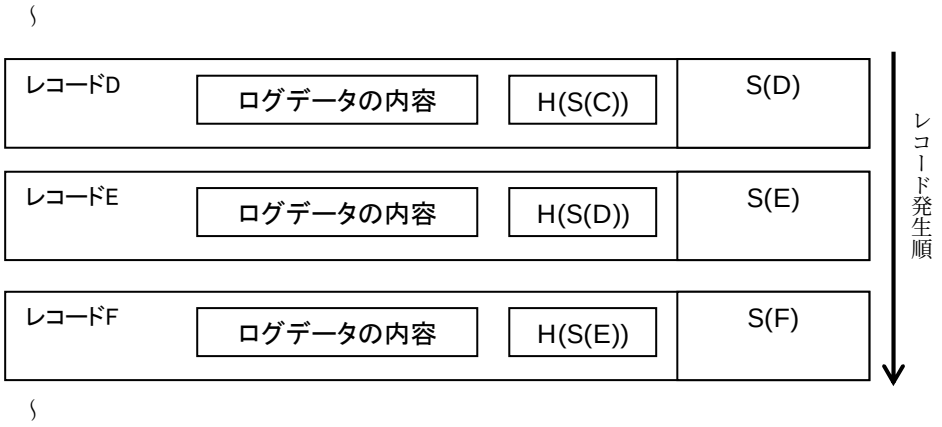

図 6-1：監査ログレコードの構造

TOEは、監査ログデータは日付単位にファイルとして保存する。なお、先頭の監査ログレコードには前監査ログレコードが存在しないため、ハッシュ値（H(S(D))）として0（ゼロ）を設定する。また、それぞれの監査ログファイルの先頭の監査ログレコードは前日の監査ログファイルの最終レコード（前監査ログレコード）のハッシュ値を含めて連鎖を生成する。

TOEは、監査ログレコードに対するディジタル署名の生成に用いるRSA秘密鍵を初期セットアップ時に生成する。監査ログの運用中は常にこのRSA秘密鍵を用いて監査ログレコードに対するディジタル署名を生成する。このRSA秘密鍵は監査ログの運用終結時、すなわち、CA自体が運用を終結しCAサービスがアンセットアップするときに削除する。

TOEは、監査ログを以下の事象発生時に記録する。

- CAオペレータの識別認証
- CAオペレータの登録、削除
- CAオペレータのパスワードの変更
- CAオペレータの操作権の変更
- 既存の証明書プロファイルの変更、新しい証明書プロファイルの追加、追加した証明書プロファイルの削除
- 既存のCRLプロファイルの変更
- CA秘密鍵の活性化・非活性化
- 証明書の発行
- 証明書の失効
- CRLの発行
- 他のCAが発行した証明書・CRLの登録
- データベースで管理する証明書・CRLの削除

- 監査者・RAサービス等の秘密鍵の生成
- CA秘密鍵の生成・削除
- CA秘密鍵のバックアップ・リストア
- 監査ログの検索／表示
- 監査ログの移出・移入、削除
- 監査者の識別
- 監査者証明書の登録・削除
- 監査ログ機能の起動・停止
- RAサービスからの要求の受信

(2)　F.AUDIT.2**（監査ログ完全性・連続性検証機能）**

F.AUDIT.１で記録した監査ログの完全性、及び連続性を以下のように検証する機能である。

- 各レコードの完全性の検証：
  監査ログレコードに付加されているディジタル署名をRSA公開鍵を用いて検証する。検証が成功する場合にだけレコードの完全性が保証される。
- レコードの連続性の検証：
  ディジタル署名が正しく検証されたものに対して、1つ前の監査ログレコードのディジタル署名のハッシュ値をSHA-1アルゴリズムを用いて生成し、現在の監査ログレコードに含まれている前監査ログレコードのハッシュ値と比較する。これにより、前レコードと現在のレコードの連続性を確認する。本操作を全ての監査ログレコードに対して実施し、それが成功する場合にだけ連続性が保証される。
  なお、最終の監査ログファイルが削除操作の当日ではない場合、監査ログデータの最終レコードを削除することが可能であるが、その際、本操作は「監査ログの削除」事象として監査ログレコードに記録される。そのため、最終レコードが削除された場合においても前監査ログレコードとのハッシュ値が一致しなくなるため連続性が不正であることを検出することができる。

上記の検証結果に応じた以下の何れかのメッセージを画面に表示することで、監査者は監査ログの改変や削除の有無を検出することができる。

- 監査ログの完全性・連続性がともに確認できた場合：「問題ありません」
- 監査ログの完全性が確認できなかった場合（改変を検出）:「ログデータの署名検証に失敗しました。ログデータが改ざんされている可能性があります。」また、該当レコードを赤色で表示する。
- 監査ログの連続性が確認できない場合（削除を検出）:「前のレコードとの連続性が確認できません。」

(3)　F.AUDIT.3**（監査ログ操作機能）**

F.AUDIT.3は、F.AUDIT.1で記録した監査ログファイルを操作するための以下の機能である。これらの機能は、操作対象の監査ログの期間を指定し、日付毎に保存されている監査ログファイル単位に対して操作することができる。

① 監査ログを検索し、表示する。
② 監査ログをTOE外部に移出する。
③ 監査ログをTOE外部から移入する。
④ 監査ログを削除する。
⑤ 監査者証明書を登録、削除する。

これらの全ての操作は既にTOEに監査者の役割として証明書が登録されている監査者だけが実行することができる。監査者は、F.I.3「監査者証明書による識別機能」により監査者IDとして識別された後、監査者を代行して動作する監査者プロセスに結合する。

① 監査ログを検索し、表示する

監査者が監査ログを参照する際には、F.AUDIT.2による監査ログの完全性・連続性の検証後に、指定された条件に従って監査ログを検索し、検索結果に応じて以下の何れかを表示する。

・検索条件に一致する監査ログがある場合：図6-2に示す内容の監査ログ
・検索条件に一致する監査ログがない場合：「指定された条件のログはありません。」

nnnnnn yyyy/mm/dd hh:mm:ss 成功 証明書の発行 CAオペレータ=aaaaa,追加詳細情報				
番号	①	②	③	④

図中の丸付き番号は、表6-7の「検索条件」の丸番号に対応する。

図 6-2**：監査ログの表示形式例**

監査者は表6-7に示す項目を監査ログの検索条件として指定することができる。

表 6-7：監査ログの検索条件

検索条件		検索結果
①	日付／時刻	指定した期間の監査ログが表示される。
②	事象の結果	指定した以下の何れかの条件の監査ログが表示される。 “ 全て ” または “ 成功のみ ” または “ 失敗のみ ”
③	事象	表5-2の何れかの「事象」についての監査ログが表示される。
④	利用者ID	指定した以下の何れかのIDを含む監査ログが表示される。 “ CAオペレータID ” または “ 監査者ID ” または “ RAサービスID ”

② 監査ログをTOE外部に移出する

監査ログは長期的な保管のために、日付毎に保存された監査ログファイルをTOE外部に対して移出することができる。

③ 監査ログをTOE外部から移入する

外部媒体などTOE外部で保管されていた監査ログファイルを参照する必要がある場合には、TOE外部から監査ログファイルを移入する。移入後、その監査ログデータを参照することができる。

④ 監査ログを削除する

TOE外部に移出し外部媒体などに保管した監査ログは、日付毎に保存された監査ログファイルをCAサーバマシン上から削除することができる。なお、削除操作を実施する日付と同じ日付の監査ログファイルは削除することはできない。

⑤ 監査者証明書を登録、削除する

新たに監査者をTOEに登録する場合、その監査者の識別データとして証明書をTOEに登録する。また、既に登録されている監査者から監査者としての役割を削除する場合、TOEに登録されている当該監査者の証明書を削除する。

(4) F.AUDIT.4（監査ログ損失防止機能）

F.AUDIT.4は監査ログの記録漏れが発生しないようにするための機能である。

監査対象の操作が行われる前にディスクの空き容量を確認し、空き容量が10%未満になった場合は以下の何れかを行う。

- Windows版：表6-8の「容量不足」の監査警告メッセージをイベントログに記録する。
- Solaris OE版：表6-9の「容量不足」の監査警告メッセージをシステムログに記録する。

但し空き容量が10%未満となっている間中、監査ログを記録する度にメッセージを記録することがないように一定時間（60分）経過毎にメッセージを記録し、前回の記録時から一定時間が経過しない間は記録しない。

また、空き容量が不足した場合等で監査ログが記録できない場合は、TOEの運用を停止して監査対象事象となる全ての操作を抑止し、以下の何れかを行う。

- Windows版：表6-8の「記録不可」の監査警告メッセージをイベントログに記録する。
- Solaris OE版：表6-9の「記録不可」の監査警告メッセージをシステムログに記録する。

なお監査ログをF.AUDIT.3を用いてTOE外部へ移出し、CAサーバマシン上から削除することで、空き容量不足を解消することができる。

表 6-8：監査警告メッセージ [Windows**版**]

種類	分類	メッセージ
エラー	容量不足	ディスクの空き容量が少なくなっています。
エラー	記録不可	作業メモリが不足しているため、監査ログサービスでログを書き込みできませんでした。
エラー	記録不可	ディスクの空き容量が不足しているため、監査ログサービスでログを書き込みできませんでした。

表 6-9：監査警告メッセージ [Solaris OE**版**]

種類	分類	メッセージ
ERROR	容量不足	Available disk space is running low.
ERROR	記録不可	Audit-logging daemon process could not write log data because of memory shortage.
ERROR	記録不可	Audit-logging daemon process could not write log data because of insufficient disk space.

6.2　TOE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.IA&ACCESS.2の認証処理である。F.IA&ACCESS.2は機能強度レベルSOF-基本を持つ。F.I&ACCESS.1、F.IA&ACCESS.2の暗号処理、F.IA4、F.AUDIT.1、F.AUDIT.2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。

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6-10に示す。なお追加の保証要件はADV_SPM.1である。

表 6-10：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		ｺﾝﾎﾟｰﾈﾝﾄ	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	Windows版： ソフトウェア説明書 Solaris OE版： インストールガイド
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	Windows版： Systemwalker PkiMGR V10.0 説明書 CA編 Systemwalker PkiMGR Key Protection Option V10.0 説明書 Solaris OE版： Systemwalker PkiMGR 10.1 説明書 CA編 Systemwalker PkiMGR Key Protection Option 10.1 説明書
	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	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PPはない。

8　根拠

本STで規定した内容の正当性について検証する。

8.1　セキュリティ対策方針根拠

(1)　必要性

前提条件、脅威、組織のセキュリティ方針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、脅威、組織のセキュリティ方針の各々について１つ以上のセキュリティ対策方針により対応することを表している。

表 8-1：前提条件、脅威、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

前提条件／脅威／組織のセキュリティ方針 ＼ セキュリティ対策方針	ASM.CA-ACCESS	ASM.TERMINAL-ACCESS	ASM.CA-KEY	ASM.AUDITOR-CAO-KEY	ASM.MEDIA-DATA	ASM.ADMIN-AUDITOR-RELIABILITY	ASM.SECURE-ENVIRONMENT	ASM.CA-CONNECT	ASM.OTHER-RELIABILITY	ASM.IMPORT-DATA-RELIABILITY	T.ADMIN-ERROR	T.AUDITOR-ERROR	T.CAO-MALICE&ERROR-1	T.CAO-MALICE&ERROR-2	T.AUDITOR-PRETENDED	T.CAO-PRETENDED	T.INTERCEPTION	P.SECUREZONE-CA	P.SECRET	P.RA-RELIABILITY
O.I-AUDITOR															●					
O.IA-CAO																●				
O.I-CAO																●				
O.IA-RA																				●
O.ACCESS-CONTROL-CAO													●	●						
O.DUAL-CONTROL-CAO														●						
O.AUDIT												●	●	●						
O.CRYPTOGRAPHY																			●	
OE.OS-IA																		●		
OE.OS-ACCESS-CONTROL											●									
OE.OS-CORRECT-TIME												●	●	●						
OE.BYPASS													●	●	●	●				
OE.WWW-A															●	●				

（続く）

（続き）

前提条件 脅威 組織のセキュリティ方針 セキュリティ対策方針	ASM.CA-ACCESS	ASM.TERMINAL-ACCESS	ASM.CA-KEY	ASM.AUDITOR-CAO-KEY	ASM.MEDIA-DATA	ASM.ADMIN-AUDITOR-RELIABILITY	ASM.SECURE-ENVIRONMENT	ASM.CA-CONNECT	ASM.OTHER-RELIABILITY	ASM.IMPORT-DATA-RELIABILITY	T.ADMIN-ERROR	T.AUDITOR-ERROR	T.CAO-MALICE&ERROR-1	T.CAO-MALICE&ERROR-2	T.AUDITOR-PRETENDED	T.CAO-PRETENDED	T.INTERCEPTION	P.SECUREZONE-CA	P.SECRET	P.RA-RELIABILITY
OE.WWW-I																●				
OE.WWW-TRUST-PATH																	●			
OE.HSM															●	●				●
OE.ICCARD-A															●	●				
OE.CA-ACCESS	●																			
OE.TERMINAL-ACCESS		●																		
OE.CA-KEY			●																	
OE.AUDITOR-CAO-KEY				●																
OE.MEDIA-DATA					●															
OE.ADMIN-AUDITOR-RELIABILITY						●					●	●								
OE.SECURE-ENVIRONMENT							●													
OE.BACKUP							●				●	●	●	●						
OE.CA-CONNECT								●												
OE.OTHER-RELIABILITY									●											
OE.IMPORT-DATA-RELIABILITY										●			●							

(2)　十分性

①　前提条件

前提条件に対するセキュリティ対策方針を以下に説明する。

- **ASM.CA-ACCESS（CAサーバマシンのアクセス制限）**

本前提条件は、CAサーバマシンはセキュアゾーンに設置されること、及びセキュアゾーンに入室できる権限はシステム管理者とセキュアゾーンに設置されるその他のサーバマシンの各管理者（他サーバマシン管理者）だけが持ち、CAオペレータがセキュアゾーンに入室する特例においては必ずシステム管理者と共に入室し、作業はシステム管理者の監視の下、共同で実施されることを想定している。

OE.CA-ACCESSによりTOEを運用する組織の責任者は、CAサーバマシンを専用区域（セキュアゾーン）に設置し、セキュアゾーンへは許可されている管理者だけが入室できるよう入退室管理を行っている。またCAオペレータがセキュアゾーンに入室する特例においても必ずシステム管理者と共に入室し、作業はシステム管理者の監視の下、共同で実施されるよう入退室管理、及び監視している。これにより本前提条件を実現する。

- **ASM.TERMINAL-ACCESS（TOEクライアント操作端末へのアクセス制限）**

本前提条件は、TOEクライアント操作端末へ物理的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ことを想定している。

OE.TERMINAL-ACCESS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だけが物理的にアクセスできる場所を確保し、TOEクライアント操作端末を設置している。これにより本前提条件を実現する。

- **ASM.CA-KEY（CA秘密鍵の保護）**

本前提条件は、CA秘密鍵は耐タンパー性のあるHSMで管理されることによって、物理的な攻撃により暴露されることはないと想定している。

OE.CA-KEYによりシステム管理者は、CA秘密鍵を耐タンパー性のあるHSMで管理している。これにより本前提条件を実現する。

- **ASM.AUDITOR-CAO-KEY（監査者とCAオペレータの秘密鍵の保護）**

本前提条件は、監査者、CAオペレータがTOEへアクセスする時に必要となる監査者とCAオペレータの各々の証明書とその秘密鍵は耐タンパー性のあるICカードに格納されることによって、物理的な攻撃により秘密鍵が暴露されることはないと想定している。

OE.AUDITOR-CAO-KEYにより監査者とCAオペレータは、各々耐タンパー性のあるICカードを持ち、自身の証明書とその秘密鍵をICカードで管理している。これにより本前提条件を実現する。

- **ASM.MEDIA-DATA（媒体の保護）**

本前提条件は、TOEの運用環境をバックアップした媒体や監査ログを移出した媒体が適切な手順に従って保管され、物理的な破壊・盗難から保護されていることを想定している。

OE.MEDIA-DATAにより、システム管理者や監査者は、破壊・盗難から保護される管理場所を確保し、運用環境をバックアップした媒体や監査ログを移出した媒体を各々保管している。これにより本前提条件を実現する。

- **ASM.ADMIN-AUDITOR-RELIABILITY（システム管理者、監査者、他サーバマシン管理者の信頼）**

本前提条件は、システム管理者、監査者、他サーバマシン管理者が各自に課せられた役割に対して許可される一連の作業について、悪意を持った行為を行わず、TOEの運用に協力的に関わることを想定している。

OE.ADMIN-AUDITOR-RELIABILITYによりTOEを運用する組織の責任者は、システム管理者、監査者、他サーバマシン管理者が各自に課せられた役割に対して許可される一連の作業につい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ず、TOEの運用に協力的に関わるようにするために、及びTOEの担当作業を指導し誤操作の可能性を低減するために、システム管理者、監査者、他サーバマシン管理者に対してセキュリティ教育や訓練を実施している。これにより本前提条件を実現する。

- **ASM.SECURE-ENVIRONMENT（セキュアな運用環境の構築と管理）**

本前提条件は、システム管理者がCAサーバマシンとその構成要素であるWWWサービス、RDBMS、HSMやCAサーバマシンに接続される機器（サーバコンソールやHSM本体）を適切にセットアップし、SSLクライアント認証に必要なCA証明書、及びTOEの識別認証に必要な監査者証明書やRA証明書を適切に設定すること、及び運用環境の復旧のためにTOE内のデータの定期的なバックアップを行うことを想定している。

OE.SECURE-ENVIRONMENTによりシステム管理者は、CAサービスの運用環境の構築としてCAサーバマシンとその構成要素であるWWWサービス、RDBMS、HSMやCAサーバマシンに接続される機器（サーバコンソールやHSM本体）を適切にセットアップし、セキュアな状態を維持できるようプログラムを管理（最新パッチの適用等）することによって、CAサービスの運用環境を構築している。更にシステム管理者は、SSLクライアント認証に必要なCA証明書、及びTOEの識別認証に必要な監査者証明書やRA証明書を適切に設定している。また、OE.BACKUPによりシステム管理者は、運用環境を復旧できるように、定期的にTOE内のデータのバックアップを実施している。これにより本前提条件を実現する。

- **ASM.CA-CONNECT（CAサーバマシンへの接続制限）**

本前提条件は、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のみと接続され、CAサービスの特定のポートに対してTOEクライアント操作端末とだけ通信できるように設定されていることを想定している。

OE.CA-CONNECTによりシステム管理者は、セキュアゾーンLANと操作端末LANの間にファイアウォール設置し、CAサービスの特定のポートに対してTOEクライアント操作端末とだけ通信できるようファイアウォールを設定している。これにより本前提条件を実現する。

- **ASM.OTHER-RELIABILITY（その他のサーバマシンの信頼）**

本前提条件は、セキュアゾーンに設置するCAサーバマシン以外のサーバマシンは、各他サーバマシン管理者が適切に設定し、管理するものであることを想定している。

OE.OTHER-RELIABILITYによりTOEを運用する組織の責任者は、各他サーバマシン管理者により適切に設定／管理されるサーバマシンをセキュアゾーンに設置している。これにより本前提条件を実現する。

- **ASM.IMPORT-DATA-RELIABILITY（インポートデータの信頼）**

本前提条件は、TOEにインポートされるデータは、TOEを運用する組織の責任者が予めその信頼性を確認したものであることを想定している。

OE.IMPORT-DATA-RELIABILITYによりTOEを運用する組織の責任者は、証明書発行の申請書や証明書・CRLをやりとりすることになる申請者や他のCAについて、事前にオフラインでその信頼性を確認し、TOEの運用を開始している。また運用開始後には、信頼性を確認した申請者や他のCAからのインポートデータだけが受け付けられていることを監査ログにより確認している。これにより本前提条件を実現する。

② 脅威

脅威に対するセキュリティ対策方針を以下に説明する。

- **T.ADMIN-ERROR（システム管理者の誤操作）**

システム管理者が誤操作によりTOEのデータを変更・削除してしまうかもしれない。本脅威に対抗するためには、誤操作を予防できるようにすること、また誤操作が行われたとしても復旧できるようにすることが効果的である。

OE.ADMIN-AUDITOR-RELIABILITY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容易な誤操作を予防する。またOSが管理するTOE内のファイルについては、OE.OS-ACCESS-CONTROLによりシステム管理者であっても安易に変更・削除できないアクセス権を事前に設定しておくことで誤操作を防止する。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により定期的に実施されているバックアップによる媒体を使用して復旧可能である。

- **T.AUDITOR-ERROR（監査者の誤操作）**

監査者は監査中の誤操作により監査ログを改変・削除してしまうかもしれない。本脅威に対抗するためには、誤操作を予防できるようにすること、また誤操作が行われた場合はそれを即検出でき、かつ復旧できるようにすることが効果的である。

OE.ADMIN-AUDITOR-RELIABILITYにより誤操作の可能性を低減するために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して容易な誤操作を予防する。また、O.AUDIT及びOE.OS-CORRECT-TIMEにより監査ログは正確な日付／時刻を伴って記録されており、その完全性（改変の有無）と連続性（削除の有無）の検証結果もログと共に表示されるため、誤操作が行われたかどうかを即検出することが可能である。更に改変・削除を行ったという事象自体も記録されるため、監査ログの追跡による誤操作の検出も可能である。なお誤操作を検出したとしても、OE.BACKUPによって定期的に実施されているバックアップによる媒体を使用して復旧可能である。以上のセキュリティ対策方針を実施することで十分に本脅威に対抗できる。

- **T.CAO-MALICE&ERROR-1（CAオペレータの悪意ある操作と誤操作-1）**

CAオペレータは悪意ある操作や誤操作を行うかもしれない。本脅威に対抗するためには、容易に悪意ある操作や誤操作を行えないようにすることが効果的である。

O.ACCESS-CONTROL-CAOにより権限を持たないオペレータが悪意ある操作や誤操作によってCAオペレータという役割の中において、そのオペレータに与えられた操作権を超えた許可されない操作を行うことを防止する。またO.AUDIT及びOE.OS-CORRECT-TIMEにより監査ログは正確な日付／時刻を伴ってCAオペレータの全ての操作を記録しているため、CAオペレータが許可される権限内で行おうとする悪意ある操作自体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。

OE.IMPORT-DATA-RELIABILITYによりTOEを運用する組織の責任者は、証明書発行の申請書や証明書・CRLをやりとりすることになる申請者や他のCAについて、事前にオフラインでその信頼性を確認してからTOEの運用を開始することにより、信頼性が確認されていないデータがTOEにインポートされることを防止する。

CAサービスは同一サーバ内で複数起動し、また複数の利用者からのアクセスを受け付けるが、OE.BYPASSによって各セキュリティドメインが維持されるため、意図されない不正なアクセスを防止する。

以上のセキュリティ対策方針を実施することで十分に本脅威に対抗できるが、対抗しきれず運用開始後に、信頼性を確認した申請者や他のCAからのインポートデータ以外が受け付けられている等の悪意ある操作や誤操作を検出した場合にも、OE.BACKUPにより定期的に実施されているバックアップによる媒体を使用して復旧可能である。

- **T.CAO-MALICE&ERROR-2（CAオペレータの悪意ある操作と誤操作-2）**

CAオペレータは悪意ある操作や誤操作を行うかもしれない。本脅威に対抗するためには、複数人のCAオペレータが確認し合い、その合意に基づいた操作を行うよう制御することが効果的である。

O.ACCESS-CONTROL-CAOにより、権限を持たないオペレータが悪意ある操作や誤操作によって、CAオペレータという役割の中においてそのオペレータに与えられた操作権を超え許可されない操作を行うことを防止する。またO.DUAL-CONTROL-CAOにより操作権を持つ必要最小人数のオペレータの合意が得られなければ操作を許可しないことでCAオペレータが互いに確認し合うことになり、一人のCAオペレータの操作権を超える悪意ある操作、及び操作権の範囲内で行う悪意ある操作の両方と誤操作を防止する。なおO.AUDIT及びOE.OS-CORRECT-TIMEにより正確な日付／時刻を伴ってCAオペレータの全ての操作を記録しているため、CAオペレータが許可される権限内で行おうとする悪意ある操作自体を抑止する効果があり、また誤操作を検出することもできる。

CAサービスは同一サーバ内で複数起動し、また複数の利用者からのアクセスを受け付けるが、OE.BYPASSによって各セキュリティドメインが維持されるため、意図されない不正なアクセスを防止する。

なお誤操作を検出したとしても、OE.BACKUPによって定期的に実施されているバックアップによる媒体を使用して復旧可能である。以上のセキュリティ対策方針を実施することで十分に本脅威に対抗できる。

- **T.AUDITOR-PRETENDED（監査者へのなりすまし）**

TOE利用者が正確に識別認証されなければ、容易に監査者へのなりすましが発生する。本脅威に対抗するためには、監査者をなりすました悪意を持つCAオペレータや悪意を持つ組織内第三者が容易に操作を行うことがないよう制御することが効果的である。

TOE外部機能であるWWWサービス機能の認証機能であるOE.WWW-Aにより、ICカード内の監査者証明書を使用したSSLクライアント認証が行われる。ICカード内の証明書は、SSL通信によってTOEクライアント操作端末を経由して操作端末LAN上に流通し、WWWサービスに渡る。WWW

サービスは、その環境に登録されている監査者証明書を使用して、渡された証明書のディジタル署名を検証することにより、監査者を認証する。証明書による認証で使用する秘密鍵は、耐タンパー性のあるICカードで安全に管理されているため盗難することができない。また、ICカードにアクセスする際には、OE.ICCARD-AによりPINの入力によって監査者が正当な利用者であるかの認証が行なわれ、ICカード内の秘密鍵及び証明書を不正に利用することはできない。その後TOEでは、WWWサービスから受け取った監査者証明書を基に、O.I-AUDITORにより監査者を特定するための識別を行う。このように監査者については、OE.ICCARD-AでICカードによる認証、OE.WWW-Aで証明書による認証、O.I-ADUITORで監査者の識別を行っている。これらが補完し合うことによって、識別認証を行い、識別認証された監査者の要求だけを受け付けることができるようになる。

また、識別認証で使用するこの監査者証明書は、「監査者証明書とその秘密鍵のPKCS#12形式での作成」操作の権限を持つCAオペレータにだけが発行でき、OE.HSMにより生成したCA秘密鍵を使って偽造不可能なディジタル署名が付加されている信頼できる証明書である。

CAサービスは同一サーバ内で複数起動し、また複数の利用者からのアクセスを受け付けるが、OE.BYPASSによって各セキュリティドメインが維持されるため、意図されない不正なアクセスを防止する。

以上のセキュリティ対策方針を実施することで十分に本脅威に対抗できる。

- **T.CAO-PRETENDED（CAオペレータへのなりすまし）**

TOE利用者が正確に識別認証されなければ、容易にCAオペレータへのなりすましや他のCAオペレータへのなりすましが発生する。本脅威に対抗するためには、CAオペレータをなりすました悪意を持つ組織内第三者が自CAサービスへアクセスし、または他のCAオペレータをなりすました悪意を持つCAオペレータが自CAサービスや同じCAサーバマシン内に構築されている他のCAサービスへアクセスし、容易に操作を行うことがないように制御することが効果的である。

TOE外部機能であるWWWサービス機能の認証機能であるOE.WWW-Aにより、ICカード内のCAオペレータ証明書を使用したSSLクライアント認証が行われる。ICカード内の証明書は、SSL通信によってTOEクライアント操作端末を経由して操作端末LAN上に流通し、WWWサービスに渡る。WWWサービスは、その環境に登録されているCA証明書を使用して、渡された証明書のディジタル署名を検証することにより、CAオペレータを認証する。証明書による認証で使用する秘密鍵は、耐タンパー性のあるICカードで安全に管理されており盗難することができない。また、ICカードにアクセスする際には、OE.ICCARD-AによりPINの入力によってCAオペレータが正当な利用者であるかの認証が行なわれ、ICカード内の秘密鍵及び証明書を不正に利用することはできない。また、WWWサービス機能の識別機能であるOE.WWW-Iにより、WWWサービスの環境に設定されているCAオペレータの役割を識別する情報がCAオペレータ証明書に含まれているかを確認することにより、アクセス者であるCAオペレータがそのCAサービスに対し役割を持つかどうかを識別する。その後TOEでは、WWWサービスから受け取ったCAオペレータ証明書を基に、CAオペレータをなりすました者が行おうとする操作に応じてO.I-CAOまたはO.IA-CAOにより、そのCAオペレータが役割を持つCAオペレータの中の誰であるかを特定して、CAオペレータ個人を識別または識別認証する。

このようにCAオペレータについては、OE.ICCARD-AでICカードによる認証、OE.WWW-Aで証明書による認証、OE.WWW-IでそのCAオペレータが役割を持つかどうかについての識別、更にO.IA-CAOまたはO.I-CAOでCAオペレータ個人の識別を行っている。これらが補完し合うことによって、役割及び個人の識別認証を行い、識別認証されたCAオペレータの要求だけを受け付けることができるようになる。また、識別認証で使用するこのCAオペレータ証明書は、「CAオペレータ証明書の発行」操作の権限を持つCAオペレータだけが発行でき、OE.HSMにより生成したCA秘密鍵を使って偽造不可能なディジタル署名が付加されている信頼できる証明書である。

CAサービスは同一サーバ内で複数起動し、また複数の利用者からのアクセスを受け付けるが、OE.BYPASSによって各セキュリティドメインが維持されるため、意図されない不正なアクセスを防止する。

以上のセキュリティ対策方針を実施することで十分に本脅威に対抗できる。

- **T.INTERCEPTION（盗聴）**

TOEクライアント操作端末とTOE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を盗聴することは容易である。本脅威に対抗するためには、TOEが送受信するデータを高信頼パスにより保護することが効果的である。

TOEクライアント操作端末とTOE間のデータの送受信に高信頼パスを提供するOE.WWW-TRUST-PATHにより通信内容の盗聴を防止する。以上のセキュリティ対策方針を実施することで十分に本脅威に対抗できる。

③　組織のセキュリティ方針

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を以下に説明する。

- **P.SECUREZONE-CA（セキュアゾーン内のCAサーバマシン）**

本組織のセキュリティ方針は、セキュアゾーンのCAサーバマシンのOSにログオン可能な利用者は、システム管理者に限定されることを想定している。

OE.OS-IAによりOSは、システム管理者を識別認証し、識別認証したシステム管理者の要求だけを受け付けている。これにより本組織のセキュリティ方針を実現する。

- **P.SECRET（秘匿）**

本組織のセキュリティ方針は、システム管理者であっても、CAサービスにとって重要な操作を行うCAオペレータをなりすまして不正アクセスすることができないように、CAオペレータ、及びそのアクセス権を特定する情報は秘匿されることを想定している。

O.CRYPTOGRAPHYによりTOEは、CAオペレータを特定するための情報について暗号化し、TOE内のファイルとして保持している。これにより本組織のセキュリティ方針を実現する。

- **P.RA-RELIABILITY（RAサービスの信頼性）**

本組織のセキュリティ方針は、セキュアゾーン内に設置されているRAサービスであっても、CAサービスに対して不正に要求できないように、RAサービスに対して識別認証を実施することを想定している。

システム管理者が登録したRA証明書とそのRAサービスIDを基に、O.IA-RAによりTOEはRAサービスの識別と認証を行い、識別認証したRAサービスからの要求だけを受け付ける。RA証明書は、OE.HSMにより生成したCA秘密鍵を使って偽造不可能なディジタル署名が付加されている信頼できる証明書である。これにより本組織のセキュリティ方針を実現する。

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関係を表8-2に示す。セキュリティ対策方針が１つ以上のセキュリティ機能要件を満たすことを表している。

表 8-2：セキュリティ対策方針に対するセキュリティ機能要件の適合性

セキュリティ機能要件 ＼ セキュリティ対策方針	O.I-AUDITOR	O.IA-CAO	O.I-CAO	O.IA-RA	O.ACCESS-CONTROL-CAO	O.DUAL-CONTROL-CAO	O.AUDIT	O.CRYPTOGRAPHY	OE.OS-IA	OE.OS-ACCESS-CONTROL	OE.OS-CORRECT-TIME	OE.BYPASS	OE.WWW-TRUST-PATH	OE.WWW-I	OE.WWW-A	OE.HSM	OE.ICCARD-A
FAU_GEN.1							●										
FAU_GEN.2							●										
FAU_SAR.1							●										
FAU_SAR.2							●										
FAU_SAR.3							●										
FAU_STG.1							●										
FAU_STG.3							●										
FAU_STG.4							●										
FCS_CKM.1[a1]							●										
FCS_CKM.1[b]	●			●													
FCS_CKM.1[h]								●									
FCS_CKM.1[i]								●									
FCS_CKM.1[j]								●									
FCS_CKM.2	●		●	●													
FCS_CKM.4[a1]							●										

（続く）

（続き）

セキュリティ対策方針 / セキュリティ機能要件	O.I-AUDITOR	O.IA-CAO	O.I-CAO	O.IA-RA	O.ACCESS-CONTROL-CAO	O.DUAL-CONTROL-CAO	O.AUDIT	O.CRYPTOGRAPHY	OE.OS-IA	OE.OS-ACCESS-CONTROL	OE.OS-CORRECT-TIME	OE.BYPASS	OE.WWW-TRUST-PATH	OE.WWW-I	OE.WWW-A	OE.HSM	OE.ICCARD-A
FCS_CKM.4[h]								●									
FCS_CKM.4[i]								●									
FCS_CKM.4[j]								●									
FCS_COP.1[a1]							●										
FCS_COP.1[a2]							●										
FCS_COP.1[e]				●													
FCS_COP.1[f]				●													
FCS_COP.1[g]								●									
FCS_COP.1[h]								●									
FCS_COP.1[i]								●									
FCS_COP.1[j]								●									
FDP_ACC.1[a1]	●	●	●	●	●												
FDP_ACC.1[a2]						●											
FDP_ACF.1[a1]	●	●	●	●	●												
FDP_ACF.1[a2]						●											
FDP_ETC.2	●		●	●	●												
FDP_ITC.1			●		●												
FIA_ATD.1					●		●										
FIA_SOS.1		●															
FIA_UAU.2		●		●													
FIA_UAU.7		●															
FIA_UID.2	●	●	●	●	●	●	●										
FIA_USB.1					●		●										

（続く）

（続き）

セキュリティ対策方針 / セキュリティ機能要件	O.I-AUDITOR	O.IA-CAO	O.I-CAO	O.IA-RA	O.ACCESS-CONTROL-CAO	O.DUAL-CONTROL-CAO	O.AUDIT	O.CRYPTOGRAPHY	OE.OS-IA	OE.OS-ACCESS-CONTROL	OE.OS-CORRECT-TIME	OE.BYPASS	OE.WWW-TRUST-PATH	OE.WWW-I	OE.WWW-A	OE.HSM	OE.ICCARD-A
FMT_MSA.1[a1-1]	●	●	●	●	●												
FMT_MSA.1[a1-2]	●	●	●	●	●												
FMT_MSA.1[a1-3]	●		●	●	●												
FMT_MSA.1[a2]						●											
FMT_MSA.2[b]	●		●	●													
FMT_MSA.2[e-f]				●													
FMT_MSA.2[h-i-j]								●									
FMT_MSA.3[a1-1]	●	●	●	●	●												
FMT_MSA.3[a1-2]	●	●	●	●	●												
FMT_MSA.3[a2]						●											
FMT_MTD.1	●	●	●	●	●		●										
FMT_SMR.1	●	●	●	●	●	●	●										
FPT_RVM.1	●	●	●	●	●	●	●										
FCS_CKM.1[E]																●	
FCS_CKM.4[E]																●	
FCS_COP.1[E][b]																●	
FCS_COP.1[E][c]															●		
FCS_COP.1[E][d]															●		
FDP_ACC.1[E]										●							
FDP_ACF.1[E]										●							

（続く）

（続き）

セキュリティ対策方針 / セキュリティ機能要件	O.I-AUDITOR	O.IA-CAO	O.I-CAO	O.IA-RA	O.ACCESS-CONTROL-CAO	O.DUAL-CONTROL-CAO	O.AUDIT	O.CRYPTOGRAPHY	OE.OS-IA	OE.OS-ACCESS-CONTROL	OE.OS-CORRECT-TIME	OE.BYPASS	OE.WWW-TRUST-PATH	OE.WWW-I	OE.WWW-A	OE.HSM	OE.ICCARD-A
FIA_UAU.2[E][d1]															●		
FIA_UAU.2[E][d2]									●								
FIA_UAU.2[E][d3]																	●
FIA_UID.2[E][d1]														●			
FIA_UID.2[E][d2]									●								
FMT_MSA.1[E]										●							
FMT_MSA.2[E]															●		
FMT_MSA.3[E]										●							
FMT_SMR.1[E]									●	●							
FPT_SEP.1[E]												●					
FPT_STM.1[E]											●						
FTP_TRP.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を以下に説明する。

- **O.I-AUDITOR（監査者の識別）**

FIA_UID.2は、WWWサービス機能から受け取った監査者証明書を監査者管理ファイルから検索して、複数人存在する監査者のうちの誰であるかを識別する。FMT_MTD.1及びFMT_SMR.1は、監査者を識別するための監査者証明書を「監査者証明書とその秘密鍵のPKCS#12形式での作成」操作の権限を持つCAオペレータにだけが発行できるように制限し、さらに監査者を新たに登録する際にその監査者証明書を登録する操作を、既に登録されている監査者だけに制限する。FCS_CKM.1[b]、FCS_CKM.2、FDP_ETC.2は、監査者の秘密鍵生成、PKCS#12形式データの配付が標準に従って実施される。FDP_ACC.1[a1]、FDP_ACF.1[a1]は、操作権限を持つCAオペレータだけが監査者証明書を発行し、PKCS#12データを配付するよう制限する。FMT_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.1[a1-3]、FMT_MSA.3[a1-1]、FMT_MSA.3[a1-2]、FMT_SMR.1は、監査者証明書の発行・配付・内容の表示を制限するCAオペレータのアクセス制御で使用するセキュリティ属性を、CAオペレータとしての役割に関連付けられた正当なCAオペレータだけが管理できるようにする。FMT_MSA.2[b]は監査者の証明書配付時に、証明書の有効期間や所有者という属性がセキュアな値であることを保証する。FPT_RVM.1は、監査者を識別する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。

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。

- **O.IA-CAO（CAオペレータの識別認証）**

FIA_UID.2は、CAオペレータが入力したCAオペレータIDから複数人存在するCAオペレータのうちの誰であるかを識別する。FIA_UAU.2は、CAオペレータが入力したパスワードとCAオペレータIDを検証し、CAオペレータを検証する。FIA_UAU.7は、CAオペレータのパスワード入力時に“＊”をフィードバックして表示する。FIA_SOS.1は、CAオペレータのパスワードが6文字以上であることを検証する。FDP_ACC.1[a1]、FDP_ACF.1[a1]は、操作権限を持つCAオペレータだけが、CAオペレータの新規登録、パスワードの変更ができるように制限する。FMT_MTD.1は、CAオペレータのパスワードをそのCAオペレータ本人だけが登録・変更できるように制限する。FMT_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.3[a1-1]、FMT_MSA.3[a1-2]、FMT_SMR.1は、CAオペレータの新規登録及びパスワードの変更を制限するCAオペレータのアクセス制御で使用するセキュリティ属性を、CAオペレータとしての役割に関連付けられた正当なCAオペレータだけが管理できるようにする。FPT_RVM.1は、CAオペレータを識別認証する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。

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。

- **O.I-CAO（CAオペレータの識別）**

FIA_UID.2は、WWWサービス機能から受け取ったCAオペレータ証明書のシリアル番号をCAオペレータ管理ファイルから検索し、複数人存在するCAオペレータのうちの誰であるかを識別する。FMT_MTD.1及びFMT_SMR.1は、CAオペレータを識別するためのCAオペレータ証明書を「CAオペレータ証明書の発行」操作の権限を持つCAオペレータにだけが発行できるように制限する。FCS_CKM.2、FDP_ETC.2は、CAオペレータの公開鍵が格納された証明書の配付が標準に従って実施される。FDP_ITC.1は、CAオペレータ証明書の発行時にCAオペレータのICカード内で生成された公開鍵がインポートされるとき許可されたCAオペレータだけに制限する。FDP_ACC.1[a1]、FDP_ACF.1[a1]は、操作権限を持つCAオペレータだけがCAオペレータ証明書を証明書を発行し配付するよう制限する。FMT_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.1[a1-3]、FMT_MSA.3[a1-1]、FMT_MSA.3[a1-2]、FMT_SMR.1は、CAオペレータ証明書の発行・配付・内容の表示を制限するCAオペレータのアクセス制御で使用するセキュリティ属性を、CAオペレータとしての役割に関連付けられた正当なCAオペレータだけが管理できるようにする。FMT_MSA.2[b]は、CAオペレータ証明書の配付時に、証明書の有効期間や所有者という属性がセキュアな値であることを保証する。FPT_RVM.1は、CAオペレータを識別する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。

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。

- **O.IA-RA（RAサービスの識別認証）**

FIA_UID.2は、CMP要求メッセージに含まれるRA証明書のRAサービスIDをRA管理ファイルから検索してRAサービスを識別する。FIA_UAU.2は、RA証明書のディジタル署名をCA公開鍵を用いて署名し、そのRA証明書中の公開鍵を用いてCMP要求メッセージに付加されているRAサービスのディジタル署名を検証して、RAサービスを認証する。FCS_COP.1[e]は、RA証明書のディジタル署名をCA公開鍵を用いて検証する。FCS_COP.1[f]は、CMP要求メッセージに付加されているRAサービスのディジタル署名を検証する。FMT_MSA.2[e-f]は、RAサービスの識別認証で使用するRA証明書及びCA証明書の有効期間という属性がセキュアな値であることを保証する。FMT_MTD.1及びFMT_SMR.1は、RAサービスを識別するためのRA証明書を「証明書と秘密鍵のPKCS#12形式での作成」操作の権限を持つCAオペレータにだけが発行できるように制限する。FCS_CKM.1[b]、FCS_CKM.2、FDP_ETC.2は、RAサービスの秘密鍵生成、PKCS#12形式データの配付が標準に従って実施される。FDP_ACC.1[a1]、FDP_ACF.1[a1]は、操作権限を持つCAオペレータだけがRA証明書を発行し、PKCS#12データを配付するよう制限する。FMT_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.1[a1-3]、FMT_MSA.3[a1-1]、FMT_MSA.3[a1-2]、FMT_SMR.1は、RA証明書の発行・配付・内容の表示を制限するCAオペレータのアクセス制御で使用するセキュリティ属性を、CAオペレータとしての役割に関連付けられた正当なCAオペレータだけが管理できるようにする。FPT_RVM.1は、RAサービスを識別認証する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。

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。

- **O.ACCESS-CONTROL-CAO（CAオペレータのアクセス制御）**

FIA_UID.2は、アクセス制御に先立ってCAオペレータIDまたはCAオペレータ証明書によってCAオペレータを識別する。FDP_ACC.1[a1]、FDP_ACF.1[a1]は、CAオペレータの役割の中においても当該操作の権限を持つCAオペレータだけに操作を許可するようにCAオペレータアクセス制御SFPに従って制限する。FMT_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.1[a1-3]、FMT_MSA.3[a1-1]、FMT_MSA.3[a1-2]、FMT_SMR.1は、CAオペレータのアクセス制御で使用するセキュリティ属性に適切なデフォルト値を設定し、CAオペレータとしての役割に関連付けられ、かつ許可されたCAオペレータだけが管理できるようにする。FIA_ATD.1、FIA_USB.1は、識別認証されたCAオペレータをCAオペレータIDからCAオペレータを代行して動作するサブジェクトであるCAオペレータプロセスに関連付ける。FDP_ITC.1は、CAオペレータの識別に使用するCAオペレータ証明書の発行時にCAオペレータのICカード内で生成された公開鍵がインポートされるとき許可されたCAオペレータだけに制限する。FDP_ETC.2は、CAオペレータの公開鍵が格納された証明書がTOE外部へエクスポートされるとき、許可されたCAオペレータだけが行なうことができるよう制限する。FMT_MTD.1及びFMT_SMR.1は、CAオペレータの識別に使用するCAオペレータ証明書を「CAオペレータ証明書の発行」操作の権限を持つCAオペレータにだけが発行できるように制限する。FPT_RVM.1は、CAオペレータアクセス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。

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。

- **O.DUAL-CONTROL-CAO（CAオペレータの合議制アクセス制御）**

FIA_UID.2は、アクセス制御に先立ってCAオペレータIDによってCAオペレータを識別する。FDP_ACC.1[a2]、FDP_ACF.1[a2]は、重要な操作を実施する際に、当該操作の権限を持つCAオペレータが設定された必要最少人数を満たしている場合だけ操作の実行を許可するように合議操作タアクセス制御SFPに従って制限する。FMT_MSA.1[a2]、FMT_MSA.3[a2]、FMT_SMR.1は、合議操作アクセス制御SFPで使用するセキュリティ属性に適切なデフォルト値を設定し、CAオペレータとしての役割に関連付けられ、かつ許可されたCAオペレータだけが管理できるように制限する。FPT_RVM.1は、CAオペレータの合議制アクセス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。

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。

- **O.AUDIT（監査記録）**

FAU_GEN.1、FAU_GEN.2は、監査者、CAオペレータ、RAサービスのセキュリティに関連する操作、また当該操作を行った利用者のID（CAオペレータID、監査者ID、RAサービスID）を伴って監査ログに記録する。FAU_SAR.1は、監査ログを監査者が参照できるように読み出す。FAU_SAR.2は、監査者だけが監査ログを読み出せるように制限する。FAU_SAR.3は、監査ログの読み出し時に、日付／時刻、事象の結果、事象、利用者IDの条件を用いて検索できるようにする。FAU_STG.1は、監査ログの不正な削除を防止し、監査ログに付加されたディジタル署名によって監査ログの不正な改変を検出する。FAU_STG.3は、監査ログを記録するディスクの空き容量が10%未満となった場合にはイベントログまたはシステムログを記録し、監査ログの格納失敗の恐れを通知する。FAU_STG.4は、監査ログを記録するディスクが満杯になった場合に、監査対象事象を抑止し、イベントログまたはシステムログに記録する。FCS_CKM.1[a1]、FCS_CKM.4[a1]は、監査ログの完全性を保証するための秘密鍵の生成及び破棄を標準に従って実施する。FCS_COP.1[a1]、FCS_COP.1[a2]は、1つ前の監査ログレコードのハッシュ値を生成し、そのハッシュ値を含めて監査ログレコードのディジタル署名を生成する。FIA_ATD.1、FIA_UID.2、FIA_USB.1は、監査者を識別し監査者IDから監査者代行して動作するサブジェクトである監査者プロセスに関連付ける。FMT_MTD.1及びFMT_SMR.1は、監査ログのインポート、エクスポート、削除、検証を、監査者としての役割に関連付けられた正当な監査者だけが操作できるように制限する。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。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。

- **O.CRYPTOGRAPHY（暗号）**

FCS_COP.1[g]は、CAオペレータ証明書のシリアル番号をCAオペレータ識別データに格納する際に暗号化し、CAオペレータを識別する際にCAオペレータ識別データから暗号化されたシリアル番号を復号化する。FCS_COP.1[h]は、CAオペレータの新規登録時にパスワードから導出した暗号鍵を用いてそのCAオペレータのRSA秘密鍵を暗号化し、CAオペレータの識別認証時に入力されたパスワードから導出した暗号鍵を用いてそのCAオペレータのRSA秘密鍵を復号化する。FCS_COP.1[i]は、CAオペレータの操作権限の設定時に各CAオペレータに対する合議操作秘密情報を暗号化した暗号鍵を暗号化し、合議操作の実行時に合議操作秘密情報を暗号化した暗号鍵を復号化する。FCS_CKM.1[j]は、CAオペレータの操作権限の設定時に各CAオペレータに対する合議操作秘密情報を暗号化し、合議操作の実行時に合議操作秘密情報を暗号化する。FCS_CKM.1[h]、FCS_CKM.1[i]、FCS_CKM.1[j]は、標準に従って暗号鍵を生成する。FCS_CKM.4[h]、FCS_CKM.4[i]、FCS_CKM.4[j]は、標準に従って暗号鍵を破棄する。FMT_MSA.2[h-i-j]は、CAオペレータに対するRSA秘密鍵やTriple-DES暗号鍵のCAオペレータIDという属性がセキュリアな値であることを保証する。

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.OS-IA（OSの識別認証）**

FIA_UAU.2E][d2]、FIA_UID.2[E][d2]は、サーバコンソールからのアクセス要求時にはOSで識別認証が実施し、識別認証されたシステム管理者だけの要求が受け付けられる。FMT_SMR.1[E]は、OSは識別認証されたシステム管理者の役割を維持する。

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。

- **OE.OS-ACCESS-CONTROL（OSのアクセス制御）**

FDP_ACC.1[E]とFDP_ACF.1[E]は、OSがTOEの扱うファイル及びディレクトリに対してアクセス制御を実施する。FMT_MSA.1[E]、FMT_MSA.3[E]、FMT_SMR.1[E]は、ファイル及びディレクトリに対するアクセス制御に利用する属性に適切なデフォルト値を設定し、システム管理者としての役割を維持された正当なシステム管理者だけが管理できるようにする。

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.OS-CORRECT-TIME（OSが提供する時刻）**

FPT_STM.1[E]は、OSが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.BYPASS（OSのセキュリティドメインによる保護）**

FPT_SEP.1[E]は、OSがCAサービス、各利用者のセキュリティドメインを維持し、他からの干渉および破壊を保護する。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.WWW-TRUST-PATH（WWWサービスの高信頼パス）**

FPT_TRP.1[E]は、監査者やCAオペレータからのアクセス要求に高信頼パスが使用され、CA監査端末とWWWサービス間、及びCA操作端末とWWWサービス間の通信がWWWサービス機能により盗聴から保護する。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.WWW-I（WWWサービスの識別）**

FIA_UID.2[E][d1]は、WWWサービス機能ではその環境に設定されているCAオペレータの役割を識別する情報が、CA操作端末から送信された証明書に含まれるかを確認することにより、アクセス者であるCAオペレータがCAオペレータとしての役割を持つかどうかを識別する。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.WWW-A（WWWサービスの認証）**

FIA_USU.2[E][d1]は、WWWサービス機能において、CAオペレータ証明書・監査者証明書のディジタル署名を検証し、CAオペレータ・監査者の秘密鍵によるディジタル署名を検証することにより認証する。なお、CAオペレータ証明書及び監査者証明書はHSMで安全に管理されたCA秘密鍵によりディジタル署名され、またその証明書中の公開鍵に対する秘密鍵はICカード内で安全に管理されている。FCS_COP.1[E][c]は、CAオペレータ証明書・監査者証明書のディジタル署名をCA公開鍵を用いて検証する。FCS_COP.1[E][d]は、CAオペレータ・監査者の秘密鍵に生成されたディジタル署名をCAオペレータ証明書・監査者証明書中の公開鍵を用いて検証する。FMT_MSA.2[E]は、ディジタル署名の検証に用いる公開鍵の有効期間というセキュリティ属性がセキュアな値であることを保証する。

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.HSM（HSM）**

FCS_COP.1[E][b]は、HSMに管理されたCA秘密鍵を用いてTOEが発行する証明書のディジタル署名を生成する。FCS_CKM.1[E]は、標準に従ってCA鍵ペアを生成する。FCS_CKM.4[E]は、標準に従ってCA鍵ペアを破棄する。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.ICCARD-A（ICカードの認証）**

ICカードはFIA_UAU.2[E][d3]により認証を行い、ICカードの正当な所有者からのアクセス要求だけを受け付ける。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8-3に示す。

表 8-3：セキュリティ機能要件の相互支援

セキュリティ機能要件	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	③非活性化	④無効化
FAU_GEN.1	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FAU_GEN.2	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FAU_SAR.1	N/A	FPT_SEP.1[E]	N/A	N/A
FAU_SAR.2	N/A	FPT_SEP.1[E]	N/A	N/A
FAU_SAR.3	N/A	FPT_SEP.1[E]	N/A	N/A
FAU_STG.1	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FAU_STG.3	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FAU_STG.4	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FCS_CKM.1[a1]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_CKM.1[b]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_CKM.1[h]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_CKM.1[i]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1

（続く）

（続き）

セキュリティ機能要件	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	③非活性化	④無効化
FCS_CKM.1[j]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_CKM.2	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_CKM.4[a1]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_CKM.4[h]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_CKM.4[i]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_CKM.4[j]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_COP.1[a1]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_COP.1[a2]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_COP.1[e]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_COP.1[f]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_COP.1[g]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_COP.1[h]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_COP.1[i]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FCS_COP.1[j]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FDP_ACC.1[a1]	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FDP_ACC.1[a2]	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FDP_ACF.1[a1]	FPT_RVM.1	FPT_SEP.1[E]	N/A	FAU_GEN.1
FDP_ACF.1[a2]	FPT_RVM.1	FPT_SEP.1[E]	N/A	FAU_GEN.1
FDP_ETC.2	N/A	FPT_SEP.1[E]	N/A	N/A
FDP_ITC.1	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FIA_ATD.1	N/A	FPT_SEP.1[E]	N/A	N/A
FIA_SOS.1	FPT_RVM.1	FPT_SEP.1[E]	N/A	FAU_GEN.1
FIA_UAU.2	FPT_RVM.1	FPT_SEP.1[E]	N/A	FAU_GEN.1
FIA_UAU.7	FPT_RVM.1	FPT_SEP.1[E]	N/A	N/A
FIA_UID.2	FPT_RVM.1	FPT_SEP.1[E]	N/A	FAU_GEN.1
FIA_USB.1	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.1[a1-1]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FMT_MSA.1[a1-2]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FMT_MSA.1[a1-3]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.1[a2]	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1

（続く）

（続き）

セキュリティ機能要件	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	③非活性化	④無効化
FMT_MSA.2[b]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.2[e-f]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.2[h-i-j]	N/A	FPT_SEP.1[E]	N/A	F.AUDIT.1
FMT_MSA.3[a1-1]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.3[a1-2]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.3[a2]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MTD.1	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FMT_SMR.1	N/A	FPT_SEP.1[E]	N/A	FAU_GEN.1
FPT_RVM.1	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_CKM.1[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_CKM.4[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_COP.1[E][b]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_COP.1[E][c]	N/A	FPT_SEP.1[E]	N/A	N/A
FCS_COP.1[E][d]	N/A	FPT_SEP.1[E]	N/A	N/A
FDP_ACC.1[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FDP_ACF.1[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FIA_UAU.2[E][d1]	N/A	FPT_SEP.1[E]	N/A	N/A
FIA_UAU.2[E][d2]	N/A	FPT_SEP.1[E]	N/A	N/A
FIA_UAU.2[E][d3]	N/A	FPT_SEP.1[E]	N/A	N/A
FIA_UID.2[E][d1]	N/A	FPT_SEP.1[E]	N/A	N/A
FIA_UID.2[E][d2]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.1[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.2[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_MSA.3[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FMT_SMR.1[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FPT_SEP.1[E]	N/A	N/A	N/A	N/A
FPT_STM.1[E]	N/A	FPT_SEP.1[E]	N/A	N/A
FTP_TRP.1[E]	N/A	FPT_SEP.1[E]	N/A	N/A

N/A：Not Applicable

① 迂回阻止

- **FPT_RVM.1**

  FAU_GEN.1、FAU_GEN.2、FAU_STG.1、FAU_STG.3、FAU_STG.4、FDP_ACC.1[a1]、FDP_ACC[a2]、FDP_ACF.1[a1]、FDP_ACF.1[a2]、FIA_SOS.1、FIA_UAU.2、FIA_UAU.7、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.2、FIA_UID.2、アクセス制御機能であるFDP_ACC.1[a1]、FDP_ACC.1[a2]、FDP_ACF.1[a1]、FDP_ACF.1[a2]）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。

③ 非活性化防止

迂回防止やドメイン分離など他の相互サポート要件が実現されることにより、本STで求められるセキュリティ対策方針を十分に満たす要件構造となっているため、特に非活性化に対する直接的な防御を行うための相互サポート機能要件を適用していない。

④ 無効化防止

- **FAU_GEN.1**

  FAU_GEN.1により、FCS_CKM.1[b]、FCS_CKM.1[h]、FCS_CKM.1[i]、FCS_CKM.1[j]、FCS_CKM.2、FCS_CKM.4[i]、FCS_COP.1[e]、FCS_COP.1[f]、FCS_COP.1[g]、FCS_COP.1[h]、FCS_COP.1[i]、FCS_COP.1[j]、FDP_ACF.1[a1]、FDP_ACF.1[a2]、FDP_ITC.1、FIA_SOS.1、FIA_UAU.2、FIA_UID.2、FIA_USB.1、FMT_MSA.1[a1-1]、FMT_MSA.1[a1-2]、FMT_MSA.1[a2]、FMT_MSA.2[h-i-j]、FMT_MTD.1、FMT_SMR.1の無効化を狙った攻撃の検出を可能にする。

(4)　セキュリティ機能要件の依存性

セキュリティ機能要件の依存性を表8-4に示す。なお、依存関係が満たされないコンポーネントについては、依存関係を満たされなくても問題がない理由を「依存関係を満たさない理由」に示す。

表 8-4：コンポーネントの依存関係

コンポーネント	依存関係	依存関係を満たさない理由
FAU_GEN.1	FPT_STM.1[E]	全ての依存関係は満たしている。
FAU_GEN.2	FAU_GEN.1 FIA_UID.2	本来の依存関係はFIA_UID.1であるが、その上位コンポーネントであるFIA_UID.2を必要とする。
FAU_SAR.1	FAU_GEN.1	全ての依存関係は満たしている。
FAU_SAR.2	FAU_SAR.1	全ての依存関係は満たしている。
FAU_SAR.3	FAU_SAR.1	全ての依存関係は満たしている。
FAU_STG.1	FAU_GEN.1	全ての依存関係は満たしている。
FAU_STG.3	FAU_STG.1	全ての依存関係は満たしている。
FAU_STG.4	FAU_STG.1	全ての依存関係は満たしている。
FCS_CKM.1[a1]	FCS_COP.1[a1] FCS_CKM.4[a1]	監査ログのディジタル署名を生成するために必要となる鍵ペアの生成において必要となるセキュリティ属性が存在しないため、FMT_MSA.2は必要ない。
FCS_CKM.1[b]	FCS_CKM.2	監査者及びRAサービスが識別認証で使用する鍵ペアの生成において、TOEでは公開鍵を証明書の形式として保持する。公開鍵であるため、暗号鍵破棄が標準に従って実施される必要はないため、FCS_CKM.4は必要ない。また、この鍵ペア生成において必要となるセキュリティ属性は存在しないため、FMT_MSA.2は必要ない。
FCS_CKM.1[h]	FCS_COP.1[h] FCS_CKM.4[h] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FCS_CKM.1[i]	FCS_COP.1[i] FCS_CKM.4[i] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FCS_CKM.1[j]	FCS_COP.1[j] FCS_CKM.4[j] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。

（続く）

（続き）

コンポーネント	依存関係	依存関係を満たさない理由
FCS_CKM.2[b1]	FCS_CKM.1[b] FDP_ITC.1 FMT_MSA.2[b]	CAオペレータ、監査者、RAサービスが識別認証で証明書の配付において、公開鍵を証明書の形式として配付する。公開鍵であるため、暗号鍵破棄が標準に従って実施される必要はないため、FCS_CKM.4は必要ない。
FCS_CKM.4[a1]	FCS_CKM.1[a1]	監査ログのディジタル署名を生成するための鍵ペアの破棄において必要となるセキュリティ属性が存在しないため、FMT_MSA.2は必要ない。
FCS_CKM.4[h]	FCS_CKM.1[h] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FCS_CKM.4[i]	FCS_CKM.1[i] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FCS_CKM.4[j]	FCS_CKM.1[j] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FCS_COP.1[a1]	FCS_CKM.1[a1] FCS_CKM.4[a1]	監査ログのディジタル署名の生成においては必要となるセキュリティ属性が存在しないため、FMT_MSA.2は必要ない。
FCS_COP.1[a2]	－	監査ログのハッシュ値の生成操作であり、ハッシュにおいては暗号鍵が存在しないため、FCS_CKM.1、FDP_ITC.1、FCS_CKM.4、FMT_MSA.2は必要ない。
FCS_COP.1[e]	FMT_MSA.2[e-f]	RAサービスの識別認証のためのRA証明書の検証においては、セッション接続時に一時的にCA証明書中の公開鍵が使用されるため、FDP_ITC.1及びFCS_CKM.1は必要ない。また、CAの公開鍵であるためその暗号鍵が標準に従って実施される必要はないため、FCS_CKM.4は必要ない。

（続く）

（続き）

コンポーネント	依存関係	依存関係を満たさない理由
FCS_COP.1[f]	FMT_MSA.2[e-f]	RAサービスの識別認証のためのRAサービスのディジタル署名の検証においては、セッション接続時に一時的にRA証明書中の公開鍵が使用されるため、FDP_ITC.1及びFCS_CKM.1は必要ない。また、RAサービスの公開鍵であるためその暗号鍵が標準に従って実施される必要はないため、FCS_CKM.4は必要ない。
FCS_COP.1[g]	－	CAオペレータ識別認証データの暗号化・復号化においては、固定の暗号鍵が使用されるため、FCS_CKM.1、FDP_ITC.1、FCS_CKM.4は必要ない。また、このとき必要となるセキュリティ属性が存在しないため、FMT_MSA.2は必要ない。
FCS_COP.1[h]	FCS_CKM.1[h] FCS_CKM.4[h] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FCS_COP.1[i]	FCS_CKM.1[i] FCS_CKM.4[i] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FCS_COP.1[j]	FCS_CKM.1[j] FCS_CKM.4[j] FMT_MSA.2[h-i-j]	全ての依存関係は満たしている。
FDP_ACC.1[a1]	FDP_ACF.1[a1]	全ての依存関係は満たしている。
FDP_ACC.1[a2]	FDP_ACF.1[a2]	全ての依存関係は満たしている。
FDP_ACF.1[a1]	FDP_ACC.1[a1] FMT_MSA.3[a1-1] FMT_MSA.3[a1-2]	全ての依存関係は満たしている。
FDP_ACF.1[a2]	FDP_ACC.1[a2] FMT_MSA.3[a2]	全ての依存関係は満たしている。
FDP_ETC.2	FDP_ACC.1[a1]	全ての依存関係は満たしている。
FDP_ITC.1	FDP_ACC.1[a1]	CAオペレータ証明書の公開鍵がTOEにインポートされるとき、公開鍵にはセキュリティ属性は存在しないため、FMT_MSA.3は必要ない。

（続く）

（続き）

コンポーネント	依存関係	依存関係を満たさない理由
FIA_ATD.1	なし	N/A
FIA_SOS.1	なし	N/A
FIA_UAU.2	FIA_UID.2	本来の依存関係はFIA_UID.1であるが、その上位コンポーネントであるFIA_UID.2を必要とする。
FIA_UAU.7	FIA_UID.2	本来の依存関係はFIA_UID.1であるが、その上位コンポーネントであるFIA_UID.2を必要とする。
FIA_UID.2	なし	N/A
FIA_USB.1	FIA_ATD.1	全ての依存関係は満たしている。
FMT_MSA.1[a1-1]	FDP_ACC.1[a1] FMT_SMR.1	全ての依存関係は満たしている。
FMT_MSA.1[a1-2]	FDP_ACC.1[a1] FMT_SMR.1	全ての依存関係は満たしている。
FMT_MSA.1[a1-3]	FDP_ACC.1[a1] FMT_SMR.1	全ての依存関係は満たしている。
FMT_MSA.1[a2]	FDP_ACC.1[a2] FMT_SMR.1	全ての依存関係は満たしている。
FMT_MSA.2[b]	ADV_SPM.1 FDP_ACC.1[a1] FMT_MSA.1[a1-3] FMT_SMR.1	全ての依存関係は満たしている。
FMT_MSA.2[e-f]	ADV_SPM.1	RAサービスの識別認証で利用するRA証明書はシステム管理者によって適切に設定・管理されるため、FDP_ACC.1、FMT_MSA.1、FMT_SMR.1は必要ない。
FMT_MSA.2[h-i-j]	ADV_SPM.1	合議操作時に使用される暗号鍵のセキュリティ属性は特定の役割によって管理される必要はないため、FDP_ACC.1、FMT_MSA.1、FMT_SMR.1は必要ない。
FMT_MSA.3[a1-1]	FMT_MSA.1[a1-1] FMT_MSA.1[a1-2] FMT_MSA.1[a1-3] FMT_SMR.1	全ての依存関係は満たしている。

（続く）

（続き）

コンポーネント	依存関係	依存関係を満たさない理由
FMT_MSA.3[a1-2]	FMT_MSA.1[a1-1] FMT_MSA.1[a1-2] FMT_MSA.1[a1-3] FMT_SMR.1	全ての依存関係は満たしている。
FMT_MSA.3[a2]	FMT_MSA.1[a2] FMT_SMR.1	全ての依存関係は満たしている。
FMT_MTD.1	FMT_SMR.1	全ての依存関係は満たしている。
FMT_SMR.1	FIA_UID.2	本来の依存関係はFIA_UID.1であるが、その上位コンポーネントであるFIA_UID.2を必要とする。
FPT_RVM.1	なし	N/A
FCS_CKM.1[E]	FCS_COP.1[E][b] FCS_CKM.4[E]	HSMにおける証明書発行時にディジタル署名を生成するために必要となる鍵ペアの生成において必要となるセキュリティ属性が存在しないため、FMT_MSA.2は必要ない。
FCS_CKM.4[E]	FCS_CKM.1[E]	HSMにおける証明書発行時にディジタル署名を生成するために必要となる鍵ペアの破棄において必要となるセキュリティ属性が存在しないため、FMT_MSA.2は必要ない。
FCS_COP.1[E][b]	FCS_CKM.1[E] FCS_CKM.4[E]	HSMにおける証明書発行時にディジタル署名の生成において、必要となるセキュリティ属性が存在しないため、FMT_MSA.2は必要ない。
FCS_COP.1[E][c]	FMT_MSA.2[E]	WWWサービスにおけるCAオペレータ及び監査者の識別認証のための証明書の検証においては、セッション接続時に一時的にCA証明書中の公開鍵が使用されるため、FDP_ITC.1及びFCS_CKM.1は必要ない。また、CAの公開鍵であるためその暗号鍵が標準に従って実施される必要はないため、FCS_CKM.4は必要ない。

（続く）

（続き）

コンポーネント	依存関係	依存関係を満たさない理由
FCS_COP.1[E][d]	FMT_MSA.2[E]	WWWサービスにおけるCAオペレータ及び監査者の識別認証のためのディジタル署名の検証においては、セッション接続時に一時的にCAオペレータ証明書及び監査者証明書中の公開鍵が使用されるため、FDP_ITC.1及びFCS_CKM.1は必要ない。また、公開鍵であるためその暗号鍵が標準に従って実施される必要はないため、FCS_CKM.4は必要ない。
FDP_ACC.1[E]	FDP_ACF.1[E]	全ての依存関係は満たしている。
FDP_ACF.1[E]	FDP_ACC.1[E] FMT_MSA.3[E]	全ての依存関係は満たしている。
FIA_UAU.2[E][d1]	FIA_UID.2[E][d1] FIA_UID.2	本来の依存関係はFIA_UID.1であるが、その上位コンポーネントであるFIA_UID.2、FIA_UID.2[E][d1]を必要とする。
FIA_UAU.2[E][d2]	FIA_UID.2[E][d2]	本来の依存関係はFIA_UID.1であるが、その上位コンポーネントであるFIA_UID.2[E][d2]を必要とする。
FIA_UAU.2[E][d3]	－	ICカードにおいては所有していることが利用者を識別することに相当するため、FIA_UID.1は必要ない。
FIA_UID.2[E][d1]	なし	N/A
FIA_UID.2[E][d2]	なし	N/A
FMT_MSA.1[E]	FDP_ACC.1[E] FMT_SMR.1[E]	全ての依存関係は満たしている。
FMT_MSA.2[E]	－	WWWサービスにおいてCAオペレータ及び監査者を識別認証するために必要となるCA証明書はシステム管理者によって適切に設定・管理されるため、FDP_ACC.1、FMT_MSA.1、FMT_SMR.1は必要ない。また、CAオペレータ及び監査者の秘密鍵はICカードによって適切に管理されるため、FDP_ACC.1、FMT_MSA.1、FMT_SMR.1は必要ない。
FMT_MSA.3[E]	FMT_MSA.1[E] FMT_SMR.1[E]	全ての依存関係は満たしている。

（続く）

（続き）

コンポーネント	依存関係	依存関係を満たさない理由
FMT_SMR.1[E]	FIA_UID.2[E][d2]	本来の依存関係はFIA_UID.1であるが、その上位コンポーネントであるFIA_UID.2[E][d2]を必要とする。
FPT_SEP.1[E]	なし	N/A
FPT_STM.1[E]	なし	N/A
FPT_TRP.1[E]	なし	N/A

N/A：Not Applicable

8.2.2　最小機能強度根拠

本TOEは、PKIシステムの中核を担うCAとしての役割を果たす。PKIシステムは証明書に付与されたCAの秘密鍵によるディジタル署名の信頼性によって維持されており、CAにはその秘密鍵や操作が厳重に管理されることが要求される。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に保護されており、不特定のユーザからTOEに対して直接攻撃が行なわれる可能性はない。

ただし、TOEを含むソフトウェアの技術機構を熟知していないCAオペレータや組織内第三者などの低レベルの攻撃能力を持った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。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SOF-基本が妥当である。

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システムの中核であるCAを実現するための製品である。CA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評価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、評価保証レベルを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8-5に示す。TOEのセキュリティ機能により各機能要件が採用されることを表している。

表 8-5：TOE要約仕様の検証

TOE要約仕様 / セキュリティ機能要件	F.I&ACCESS.1	F.IA&ACCESS.2	F.I.3	F.IA.4	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4
FAU_GEN.1					●			
FAU_GEN.2					●			
FAU_SAR.1							●	
FAU_SAR.2							●	
FAU_SAR.3							●	
FAU_STG.1					●	●		
FAU_STG.3								●
FAU_STG.4								●
FCS_CKM.1[a1]					●			
FCS_CKM.1[b]	●							
FCS_CKM.1[h]		●						
FCS_CKM.1[i]		●						
FCS_CKM.1[j]		●						
FCS_CKM.2	●							
FCS_CKM.4[a1]					●			
FCS_CKM.4[h]		●						
FCS_CKM.4[i]		●						
FCS_CKM.4[j]		●						
FCS_COP.1[a1]					●	●		

（続く）

（続き）

TOE要約仕様 / セキュリティ機能要件	F.I&ACCESS.1	F.IA&ACCESS.2	F.I.3	F.IA.4	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4
FCS_COP.1[a2]					●	●		
FCS_COP.1[e]				●				
FCS_COP.1[f]				●				
FCS_COP.1[g]	●							
FCS_COP.1[h]		●						
FCS_COP.1[i]		●						
FCS_COP.1[j]		●						
FDP_ACC.1[a1]	●							
FDP_ACC.1[a2]		●						
FDP_ACF.1[a1]	●							
FDP_ACF.1[a2]		●						
FDP_ETC.2	●							
FDP_ITC.1	●							
FIA_ATD.1	●						●	
FIA_SOS.1		●						
FIA_UAU.2		●		●				
FIA_UAU.7		●						
FIA_UID.2	●	●	●	●				
FIA_USB.1	●						●	
FMT_MSA.1[a1-1]	●							
FMT_MSA.1[a1-2]	●							
FMT_MSA.1[a1-3]	●							
FMT_MSA.1[a2]		●						
FMT_MSA.2[b]	●							
FMT_MSA.2[e-f]				●				
FMT_MSA.2[h-i-j]		●						

（続く）

（続き）

TOE要約仕様 / セキュリティ機能要件	F.I&ACCESS.1	F.IA&ACCESS.2	F.I.3	F.IA.4	F.AUDIT.1	F.AUDIT.2	F.AUDIT.3	F.AUDIT.4
FMT_MSA.3[a1-1]	●							
FMT_MSA.3[a1-2]	●							
FMT_MSA.3[a2]		●						
FMT_MTD.1	●		●				●	
FMT_SMR.1	●	●	●				●	
FPT_RVM.1	●	●	●	●				
FCS_CKM.1[E]	IT環境の機能要件により実現される。							
FCS_CKM.4[E]								
FCS_COP.1[E][b]								
FCS_COP.1[E][c]								
FCS_COP.1[E][d]								
FDP_ACC.1[E]								
FDP_ACF.1[E]								
FIA_UAU.2[E][d1]								
FIA_UAU.2[E][d2]								
FIA_UAU.2[E][d3]								
FIA_UID.2[E][d1]								
FIA_UID.2[E][d2]								
FMT_MSA.1[E]								
FMT_MSA.2[E]								
FMT_MSA.3[E]								
FMT_SMR.1[E]								
FPT_SEP.1[E]								
FPT_STM.1[E]								
FTP_TRP.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、機能要件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、事象の結果、事象、利用者ID、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。

監査機能、CA管理機能,、RAサービスのセキュリティに関連する操作全てを記録するF.AUDIT.1「監査ロギング機能」により、各コンポーネントで必要となる監査要件が表8-6に示すとおり記録される。これによりFAU_GEN.1が満たされる。

表 8-6：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	－	FDP_ACC.1[a1]	－
FAU_GEN.2	－	FDP_ACC.1[a2]	－
FAU_SAR.1	F.AUDIT.1	FDP_ACF.1[a1]	F.AUDIT.1
FAU_SAR.2	F.AUDIT.1	FDP_ACF.1[a2]	F.AUDIT.1
FAU_SAR.3	F.AUDIT.1	FDP_ETC.2	－
FAU_STG.1	－	FDP_ITC.1	F.AUDIT.1
FAU_STG.3	－	FIA_ATD.1	－
FAU_STG.4	－	FIA_SOS.1	F.AUDIT.1
FCS_CKM.1[a1]	－	FIA_UAU.2	F.AUDIT.1
FCS_CKM.1[b]	F.AUDIT.1	FIA_UAU.7	－
FCS_CKM.1[h]	F.AUDIT.1	FIA_UID.2	F.AUDIT.1
FCS_CKM.1[i]	F.AUDIT.1	FIA_USB.1	F.AUDIT.1
FCS_CKM.1[j]	F.AUDIT.1	FMT_MSA.1[a1-1]	F.AUDIT.1
FCS_CKM.2	F.AUDIT.1	FMT_MSA.1[a1-2]	F.AUDIT.1
FCS_CKM.4[a1]	－	FMT_MSA.1[a1-3]	－
FCS_CKM.4[h]	－	FMT_MSA.1[a2]	F.AUDIT.1
FCS_CKM.4[i]	F.AUDIT.1	FMT_MSA.2[b]	－
FCS_CKM.4[j]	－	FMT_MSA.2[e-f]	－
FCS_COP.1[a1]	－	FMT_MSA.2[h-i-j]	F.AUDIT.1
FCS_COP.1[a2]	－	FMT_MSA.3[a1-1]	－
FCS_COP.1[e]	F.AUDIT.1	FMT_MSA.3[a1-2]	－

FCS_COP.1[f]	F.AUDIT.1	FMT_MSA.3[a2]	－
FCS_COP.1[g]	F.AUDIT.1	FMT_MTD.1	F.AUDIT.1
FCS_COP.1[h]	F.AUDIT.1	FMT_SMR.1	F.AUDIT.1
FCS_COP.1[i]	F.AUDIT.1	FPT_RVM.1	－
FCS_COP.1[j]	F.AUDIT.1		

- **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「監査ロギング機能」において、当該操作を行った監査者、CAオペレータ、RAサービスの何れかのID（利用者ID）を監査ログの事象と共に記録する。従って、F.AUDIT.1によりFAU_GEN.2が満たされる。

- **FAU_SAR.1**

FAU_SAR.1.1：TSFは、監査者が全ての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.3「監査ログ操作機能」において、許可された監査者のみが日付／時刻、事象の結果、事象、利用者IDの何れかの検索条件に応じた検索を行い、監査者が解釈するのに適した形式で監査記録が読み出される。従って、F.AUDIT.3によりことでFAU_SAR.1が満たされる。

- **FAU_SAR.2**

FAU_SAR.2.1：TSFは監査者を除き、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.3「監査ログ操作機能」において、許可された監査者によってのみ、日付／時刻、事象の結果、事象、利用者IDといった検索条件に応じた検索を行って監査記録が読み出される。従って、F.AUDIT.3によりFAU_SAR.2が満たされる。

- **FAU_SAR.3**

FAU_SAR.3.1：TSFは、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、事象の結果、事象、利用者IDといった検索条件を１つまたは複数指定して検索を実施する。

F.AUDIT.3「監査ログ操作機能」で、許可された監査者のみが、監査者が指定する日付／時刻、事象の結果、事象、利用者IDの何れかの検索条件に応じた検索を行うことができ、その結果に応じた監査記録を表示する。従って、F.AUDIT.3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.1「監査ロギング機能」は、監査ログデータに対して1つ前の監査ログレコードのハッシュ値を含めたディジタル署名を付加する。また、F.AUDIT.2「監査ログ完全性・連続性検証機能」は監査ログデータのディジタル署名の検証及び1つ前の監査ログレコードのハッシュ値を比較するこよにより、各レコードの完全性及び全レコードの連続性を検証する。従って、F.AUDIT.1及びF.AUDIT.2により、FAU_STG.1が満たされる。

- **FAU_STG.3**

FAU_STG.3.1：TSFは、監査証跡がディスクの空き容量が10%未満を超えた場合、一定時間（60分）経過毎に警告メッセージをイベントログ（Windows版）かシステムログ（Solaris OE版）に記録しなければならない。

F.AUDIT.4「監査ログ損失防止機能」は、空き容量を監視し、それが10%未満を超えた場合には表6-8か表6-9の「容量不足」の監査警告メッセージをイベントログ（Windows版）かシステムログ（Solaris OE版）に一定時間（60分）経過毎に記録する。従って、F.AuDIT.4によりFAU_STG.3が満たされる。

また、TOEは本事象を監査ログに記録しないが、ディスクの空き容量の閾値を超えた場合にイベントログ（Windows版）かシステムログ（Solaris OE版）に記録されており、閾値を超えたためにとられるアクションが監査ログに記録されていなくてもセキュリティ対策方針上の問題はない。

- **FAU_STG.4**

FAU_STG.4.1：TSFは、監査証跡が満杯になった場合、特権を持つ許可利用者に関わるもの以外の監査対象事象を抑止しなければならない。また監査格納失敗時には警告メッセージをイベントログ（Windows版）かシステムログ（Solaris OE版）に記録しなければならない。

F.AUDIT.4「監査ログ損失防止機能」は、空き容量の不足等で監査ログを記録できない場合、TOEの運用を停止して監査対象事象となる操作の全てを抑止し、表6-8か表6-9の「記録不可」の監査警告メッセージをイベントログ（Windows版）かシステムログ（Solaris OE版）に記録する。従って、F.AUDIT.4により、FAU_STG.4が満たされる。

また、TOEは本事象を監査ログに記録しないが、監査ログを記録できない場合にはイベントログ（Windows版）かシステムログ（Solaris OE版）に記録し、監査対象事象となる操作を全て抑止するため、監査格納失敗によってとられるアクションが監査ログに記録されていなくてもセキュリティ対策方針上の問題はない。

- **FCS_CKM.1[a1]**

FCS_CKM.1.1[a1]：TSFは、以下の標準に合致する暗号鍵を生成しなければならない。

標準のリスト	暗号鍵生成アルゴリズム	暗号鍵長
PKCS#1 “RSA Cryptography Standard”	RSA	1024bit

F.AUDIT.1「監査ロギング機能」において、監査ログデータのディジタル署名を生成するための暗号鍵を上記の表に合致するように生成する。従って、FCS_CKM.1[a1]が満たされる。

また、FCS_CKM.1[a1]は監査ログデータへのディジタル署名のための暗号鍵生成を示し、監査ログ記録の運用に先立って行なわれるものである。そのため、FCS_CKM.1[a1]の動作の成功と失敗は監査ログに記録する必要はない。

- **FCS_CKM.1[b]**

FCS_CKM.1.1[b]：TSFは、以下の標準に合致する暗号鍵を生成しなければならない。

標準のリスト	暗号鍵生成アルゴリズム	暗号鍵長
PKCS#1 “RSA Cryptography Standard”	RSA	512, 768, 1024, 2048bit

F.I&ACCESS.1「CAオペレータ証明書による識別／アクセス制御機能」において、アクセス制御により許可されたCAオペレータが監査者及びRAサービスに対して証明書を発行するために、上記の表に合致するように暗号鍵を生成する。従って、FCS_CKM.1[b]が満たされる。

- **FCS_CKM.1[h]**

FCS_CKM.1.1[h]：TSFは、以下の標準に合致する暗号鍵を生成しなければならない。

標準のリスト	暗号鍵生成アルゴリズム	暗号鍵長
PKCS#5 v2.0 “Password-Based Cryptography Standard”	PBKDF2	168bit

F.IA&ACCESS.2「CAオペレータIDとパスワードにによる識別／アクセス制御機能」において、CAオペレータが入力したパスワードから、上記の表に合致するように暗号鍵を生成する。従って、FCS_CKM.1[h]が満たされる。

- **FCS_CKM.1[i]**

FCS_CKM.1.1[i]：TSFは、以下の標準に合致する暗号鍵を生成しなければならない。

標準のリスト	暗号鍵生成アルゴリズム	暗号鍵長
PKCS#1 “RSA Cryptography Standard”	RSA	2048bit

F.IA&ACCESS.2「CAオペレータIDとパスワードにによる識別／アクセス制御機能」において、CAオペレータ毎の合議操作秘密情報を暗号化するTriple-DES暗号鍵を暗号化するための暗号鍵を上記の表に合致するように生成する。従って、FCS_CKM.1[i]が満たされる。

- **FCS_CKM.1[j]**

FCS_CKM.1.1[j]：TSFは、以下の標準に合致する暗号鍵を生成しなければならない。

標準のリスト	暗号鍵生成アルゴリズム	暗号鍵長
FIPS PUB 46-3 “Data Encryption Standard(DES)”	Triple-DES	168bit

F.IA&ACCESS.2「CAオペレータIDとパスワードにによる識別／アクセス制御機能」において、CAオペレータ毎の合議操作秘密情報を暗号化するための暗号鍵を上記の表に合致するように生成する。従って、FCS_CKM.1[j]が満たされる。

- **FCS_CKM.2**

FCS_CKM.2.1：TSFは、以下の標準に合致する方法に従って、暗号鍵を配付しなければならない。

標準のリスト	暗号鍵配付方法
PKCS#12 Personal Information Exchange Syntax Standard、 X.509 The Directory: Public-Key And Attribute Certificate Frameworks	証明書ベース鍵管理

F.IA&ACCESS.1「CAオペレータIDとパスワードにによる識別／アクセス制御機能」において、アクセス制御により許可されたCAオペレータが、上記の表に合致した標準に従って監査者及びRAサービスに鍵ペア及び証明書を配付する。従って、FCS_CKM.2が満たされる。

- **FCS_CKM.4[a1]**

FCS_CKM.4.1[a1]：TSFは、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って、暗号鍵を破棄しなければならない。

F.AUDIT.1「監査ロギング機能」において、監査ログレコードにディジタル署名を付加するために使用した暗号鍵を、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って破棄する。これにより、FCS_CKM.4[a1]が満たされる。

また、FCS_CKM.4[a1]は監査ログデータへのディジタル署名のための暗号鍵の破棄を示し、監査ログ記録の運用を終結するときに行なわれるものである。そのため、FCS_CKM.4[a1]の動作の成功と失敗は監査ログに記録する必要はない。

- **FCS_CKM.4[h]**

FCS_CKM.4.1[h]：TSFは、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って、暗号鍵を破棄しなければならない。

F.IA&ACCESS.2「CAオペレータIDとパスワードにによる識別／アクセス制御機能」において、CAオペレータが入力したパスワードを元に生成した暗号鍵を、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って破棄する。これにより、FCS_CKM.4[h]が満たされる。

また、FCS_CKM.4[h]はメモリ上に生成した暗号鍵の破棄を示すものであり、必ず成功するものである。そのため、FCS_CKM.4[h]の動作の成功と失敗は監査ログに記録する必要はない。

- **FCS_CKM.4[i]**

FCS_CKM.4.1[i]：TSFは、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って、暗号鍵を破棄しなければならない。

F.IA&ACCESS.2「CAオペレータIDとパスワードにによる識別／アクセス制御機能」において、CAオペレータ毎の合議操作秘密情報を暗号化するTriple-DES暗号鍵をさらに暗号化するための暗号鍵を、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って破棄する。これにより、FCS_CKM.4[i]が満たされる。

- **FCS_CKM.4[j]**

FCS_CKM.4.1[j]：TSFは、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って、暗号鍵を破棄しなければならない。

F.IA&ACCESS.2「CAオペレータIDとパスワードにによる識別／アクセス制御機能」において、CAオペレータ毎の合議操作秘密情報を暗号化するための暗号鍵を、FIPS PUB 140-1 Security Requirements for Cryptographic Modulesに合致する暗号鍵破棄方法（0で上書き削除）に従って破棄する。これによりFCS_CKM.4[i]が満たされる。

また、FCS_CKM.4[i]はメモリ上に生成した暗号鍵の破棄を示すものであり、必ず成功するものである。そのため、FCS_CKM.4[i]の動作の成功と失敗は監査ログに記録する必要はない。

- **FCS_COP.1[a1]**

FCS_COP.1.1[a1]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
PKCS#1 “RSA Cryptography Standard”	SHA-1、RSA	2048bit	監査ログのディジタル署名の生成及び検証

F.AUDIT.1「監査ロギング機能」において、1つの前の監査ログデータのハッシュ値を含めた監査ログデータに対してディジタル署名を生成する。F.AUDIT.2「監査ログ完全性・連続性検証機能」において監査ログデータのディジタル署名を検証する。従って、F.AUDIT.1及びF.AUDIT.2により、FCS_COP.1[a1]が満たされる。

また、FCS_COP.1[a1]は監査ログデータへのディジタル署名操作を示すものであるため、FCS_COP.1[a1]の動作の成功と失敗及び暗号操作の種別は監査ログに記録する必要はない。

- **FCS_COP.1[a2]**

FCS_COP.1.1[a2]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
FIPS PUB 180-1 Secure Hash Standard	SHA-1	なし	監査ログのハッシュ値の生成

F.AUDIT.1「監査ロギング機能」において、監査ログの連続性保証のために、1つの前の監査ログデータのハッシュ値を生成し、監査ログデータに含める。F.AUDIT.2「監査ログ完全性・連続性検証機能」においては、監査ログの連続性の検証のために、1つ前の監査ログデータのハッシュ値を生成し、監査ログデータ中のハッシュ値と比較する。F.AUDIT.1及びF.AUDIT.2により、FCS_COP.1[a2]が満たされる。

また、FCS_COP.1[a2]は監査ログデータのハッシュ値の生成を示すものであるため、FCS_COP.1[a2]の動作の成功と失敗及び暗号操作の種別は監査ログに記録する必要はない。

- **FCS_COP.1[e]**

FCS_COP.1.1[e]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
PKCS#1 “RSA Cryptography Standard”	SHA-1、RSA	512、768、 1024、2048bit	RA証明書の検証

F.IA.4「RA証明書による識別認証機能」において、RAサービスの識別認証のためにCA公開鍵を用いてRA証明書のディジタル署名を検証する。従って、F.IA.4により、FCS_COP.1[e]が満たされる。

また、FCS_COP.1[e]の動作の成功と失敗は、「RAサービスからの要求の受信」事象として監査ログに記録される。このとき暗号操作の種別は固定であるため、FCS_COP.1[e]の暗号操作の種別は監査ログに記録する必要はない。

- **FCS_COP.1[f]**

FCS_COP.1.1[f]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
PKCS#1 “RSA Cryptography Standard”	SHA-1、RSA	512、768、1024、2048bit	RA証明書の公開鍵に対する秘密鍵で生成されたディジタル署名の検証

F.IA.4「RA証明書による識別認証機能」において、RAサービスの識別認証のためにCMP要求メッセージに付与されたディジタル署名をRA証明書中の公開鍵を用いて検証する。従って、F.IA.4により、FCS_COP.1[f]が満たされる。

また、FCS_COP.1[f]の動作の成功と失敗は、「RAサービスからの要求の受信」事象として監査ログに記録される。このとき、暗号操作の種別は固定であるため、FCS_COP.1[f]の暗号操作の種別は監査ログに記録する必要はない。

- **FCS_COP.1[g]**

FCS_COP.1.1[g]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
FIPS PUB 46-3 “Data Encryption Standard(DES)”	Triple-DES	168bit	CAオペレータ証明書のシリアル番号の暗号化・復号化

F.I&ACCESS.1「CAオペレータ証明書による識別／アクセス制御機能」において、CAオペレータ識別認証データ中にCAオペレータ証明書のシリアル番号を上記の表に従って暗号化して保存する。また、識別認証時にはCAオペレータ識別認証データ中の暗号化されたCAオペレータ証明書のシリアル番号を上記の表に従って復号化し、比較する。従って、F.I&ACCESS.1により、FCS_COP.1[g]が満たされる。

また、FCS_COP.1[g]の動作の成功と失敗は、「CAオペレータの識別認証」及び「CAオペレータの登録」事象として監査ログに記録される。このとき、暗号操作の種別は固定であるため、FCS_COP.1[g]の暗号操作の種別は監査ログに記録する必要はない。

- **FCS_COP.1[h]**

FCS_COP.1.1[h]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
FIPS PUB 46-3 “Data Encryption Standard(DES)”	Triple-DES	168bit	CAオペレータ毎の秘密鍵（CAオペレータ識別認証データ）の暗号化・復号化

F.IA&ACCESS.2「CAオペレータIDとパスワードによる識別認証／アクセス制御機能」において、CAオペレータの登録時にCAオペレータが入力したパスワードから導出した暗号鍵を用いて、上記の表に従ってCAオペレータ毎に存在するRSA秘密鍵を暗号化する。また、CAオペレータの識別認証時にCAオペレータが入力したパスワードから導出した暗号鍵を用いて上記の表に従ってRSA秘密鍵を復号化し、正しく復号化されることでCAオペレータを識別認証する。従って、F.IA&ACCESS.2により、FCS_COP.1[h]が満たされる。

また、FCS_COP.1[h]の動作の成功と失敗は、「CAオペレータの識別認証」及び「CAオペレータの登録」事象として監査ログに記録される。このとき暗号操作の種別は固定であるため、FCS_COP.1[h]の暗号操作の種別は監査ログに記録する必要はない。

- **FCS_COP.1[i]**

FCS_COP.1.1[i]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
PKCS#1 “RSA Cryptography Standard”	RSA	2048bit	合議操作秘密情報の暗号化用Triple-DES暗号鍵の暗号化・復号化

F.IA&ACCESS.2「CAオペレータIDとパスワードによる識別認証／アクセス制御機能」において、「CAオペレータの操作権限の設定」実行時に、各CAオペレータ毎に操作権を持つ操作情報をTriple-DESで暗号化し、そのTriple-DES暗号鍵を各CAオペレータのRSA公開鍵で暗号化し、合議操作秘密情報として保管する。また、合議操作実行時には、合議操作秘密情報からCAオペレータが持つ操作情報を復号化するために暗号化されているTriple-DES暗号鍵を当該CAオペレータのRSA

秘密鍵で復号化する。従って、F.IA&ACCESS.2により、FCS_COP.1[i]が満たされる。

また、FCS_COP.1[i]の動作の成功と失敗は、「CAオペレータの識別認証」及び「CAオペレータの操作権の変更」事象として監査ログに記録される。このとき暗号操作の種別は固定であるため、FCS_COP.1[i]の暗号操作の種別は監査ログに記録する必要はない。

- **FCS_COP.1[j]**

FCS_COP.1.1[j]：TSFは、以下の表に合致する暗号操作を実行できなければならない。

標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
FIPS PUB 46-3 “Data Encryption Standard(DES)”	Triple-DES	168bit	合議操作秘密情報の暗号化・復号化

F.IA&ACCESS.2「CAオペレータIDとパスワードによる識別認証／アクセス制御機能」において、「CAオペレータの操作権限の設定」実行時に、各CAオペレータ毎に操作権を持つ操作情報を上記の表に従って暗号化し、合議操作秘密情報として保管する。また、合議操作実行時には、CAオペレータが持つ操作情報を得るために合議操作秘密情報を上記の表に従って復号化する。従って、F.IA&ACCESS.2により、FCS_COP.1[j]が満たされる。

また、FCS_COP.1[j]の動作の成功と失敗は、「CAオペレータの識別認証」及び「CAオペレータの操作権の変更」事象として監査ログに記録される。さらに、暗号操作の種別は固定であるため、FCS_COP.1[j]の動作の成功と失敗及び暗号操作の種別は監査ログに記録する必要はない。

- **FDP_ACC.1[a1]**

FDP_ACC.1.1[a1]：TSFは、CAオペレータが行う操作全てについて、権限を持つCAオペレータだけに操作を許可するようCA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.I&ACCESS.1「識別／アクセス制御機能」は、操作を行おうとするCAオペレータが当該操作に対して権限を持つ者として登録されている場合にだけ操作を許可する。従って、F.I&ACCESS.1によりFDP_ACC.1[a1]が満たされる。

- **FDP_ACC.1[a2]**

FDP_ACC.1.1[a2]：TSFは、操作権を持つCAオペレータが必要最小人数揃った場合だけ、操作を許可する合議操作アクセス制御SFPを実施しなければならない。

F.IA&ACCESS.2「識別認証／アクセス制御機能」において、セキュリティ上非常に重要なCA秘密鍵を扱う操作やCAオペレータの操作権の設定操作については、必要最小人数を満たす複数人のCAオペレータが揃った場合にその合意に基づいて操作を許可する。従って、F.IA&ACCESS.2により、FDP_ACC.1[a2]が満たされる。

- **FDP_ACF.1[a1]**

FDP_ACF.1.1[a1]：TSFは、CAオペレータIDと実行オブジェクトIDおよびファイルの種類に基づいて、CAオペレータが行う操作全てについて、権限を持つCAオペレータだけに許可するようCA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[a1]：TSFが実施するアクセス制御の規則は、F.I&ACCESS.1で定義することにより満たされる。

FDP_ACF.1.3[a1]、FDP_ACF.1.4[a1]：N/A

F.I&ACCESS.1「識別／アクセス制御機能」は、CAオペレータが当該操作に対して権限を持つ者として登録されている場合にだけ操作を許可する。従って、F.I&ACCESS.1及びF.IA&ACCESS.2により、FDP_ACC.1[a1]が満たされる。

- **FDP_ACF.1[a2]**

FDP_ACF.1.1[a2]：TSFは以下のセキュリティ属性に基づいて、必要最小人数のCAオペレータが揃った場合にその合意に基づいてだけ表6-4に示す操作を許可するよう合議操作アクセス制御SFPを実施しなければならない。

・CAオペレータID
・実行オブジェクトIDおよびファイルの種類
・操作の実行が許可されるCAオペレータの必要最小人数

FDP_ACF.1.2[a2]：TSFが実施するアクセス制御の規則は、F.IA&ACCESS.2で定義することにより満たされる。

FDP_ACF.1.3[a2]、FDP_ACF.1.4[a2]：N/A

F.IA&ACCESS.2「識別認証／アクセス制御機能」のアクセス制御機能で、必要最小人数を満たす複数人のCAオペレータが揃った場合にのみ操作を許可する。従って、F.IA&ACCESS.2により、FDP_ACF.1[a2]が満たされる。

- **FDP_ETC.2**

FDP_ETC.2.1：TSFは、SFP(s)制御下にある利用者データをTSCの外部にエクスポートするとき、CA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_ETC.2.2：TSFは、利用者データに関係したセキュリティ属性と共に利用者データをエクスポートしなければならない。

FDP_ETC.2.3：TSFは、セキュリティ属性がTSCの外部にエクスポートされるとき、それがエクスポートされる利用者データに曖昧さなく関連付けられることを保証しなければならない。

FDP_ETC.2.4：N/A

F.I&ACCESS.1「識別／アクセス制御機能」において、許可されたCAオペレータのみが監査者証明書及びRA証明書の発行後、監査者及びRAサービスに対して証明書を配付するためにTSC外部にエクスポートできるように制限される。従って、F.I&ACCESS.1により、FDP_ETC.2は満たされる。

また、TOEはCAオペレータ及び監査者の証明書のエクスポートを監査ログに記録しない。ただし、

これらの証明書の発行及び登録操作が監査ログに記録されることにより、不正な証明書が発行され、流出し、悪用される可能性に対し、発行及び登録に関する監査ログが事後分析に利用可能である。さらに、許可されたCAオペレータのみがTSC外部に証明書をエクスポートできるように制限されているため、当該証明書のエクスポートを監査ログに記録しなくてもセキュリティ対策方針上の問題はない。

- **FDP_ITC.1**

FDP_ITC.1.1：TSFは、SFPに従って制御され、TSC外から利用者データをインポートするとき、CA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、利用者データ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.I&ACCESS.1「識別／アクセス制御機能」において、許可されたCAオペレータのみがCAオペレータ証明書を発行するために、ICカード内で生成された公開鍵をTOE内にインポートできるよう制限される。従って、F.I&ACCESS.1により、FDP_ITC.2[a]は満たされる。

- **FIA_ATD.1**

FIA_ATD.1.1：TSFは、個々の利用者に属するセキュリティ属性のリスト[CAオペレータID、監査者ID]を維持しなければならない。

F.I&ACCESS.1「識別／アクセス制御機能」において、CAオペレータは必ずCAオペレータIDに関連付けられる。また、F.AUDIT.3「監査ログ操作機能」において、監査者は必ず監査者IDに関連付けられる。従って、F.I&ACCESS.1及びF.AUDIT.3により、FIA_ATD.1は満たされる。

- **FIA_SOS.1**

FIA_SOS.1.1：TSFは、パスワードは6文字以上であ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.IA&ACCESS.2「識別認証／アクセス制御機能」の識別認証機能は、CAオペレータパスワードは6文字以上であることを検証する。従って、F.IA&ACCESS.2により、FIA_SOS.1が満たされる。

- **FIA_UAU.2**

FIA_UAU.2.1：TSFは以下のTOE外部インタフェースに対し、他の機能が動作する前に必ず認証機能を動作させ、CAオペレータとRAサービスを各々認証しなければならない。

① CA操作端末からTOE外部機能であるWWWサービス機能を経てTOEへアクセスするインタフェース

② RAサービスからTOEへアクセスするインタフェース

①はF.IA&ACCESS.2「識別認証／アクセス制御機能」の識別認証機能で、CAオペレータが入力したCAオペレータパスワードを検証することでCAオペレータを識別認証する。②はF.IA.4「識別認

証機能」で、RAサービスから送信されるCMP要求メッセージに付加されているディジタル署名、及びCMP要求メッセージに同梱されるRA証明書について検証することで、RAサービスを認証する。従って、F.IA&ACCESS.2及びF.IA.4により、FIA_UAU.2は満たされる。

なお以下に示すその他の外部インタフェースに対する認証はIT環境で行う。

③ CA監査端末からTOE外部機能であるWWWサービス機能を経てTOEへアクセスするインタフェース

④ サーバコンソールからTOEへアクセスするインタフェース

⑤ RDBMSがTOEとプロセス間通信を行うインタフェース

⑥ HSMがTOEとPCIバスを介してプロセス間通信を行うインタフェース

①はWWWサービス機能が証明書による識別認証、③はWWWサービス機能が証明書による認証を行う。④はOSが認証を行う。また⑤⑥からTOEを利用するアクセス経路はないため、利用者を認証する必要はない。

- **FIA_UAU.7**

FIA_UAU.7.1：TSFは認証を行っている間、入力されたパスワードの文字列を“＊”で表示しなければならない。

F.IA&ACCESS.2「識別認証／アクセス制御機能」の識別認証機能において、認証中のパスワードの文字列を“＊”で表示して暴露から保護する。従って、F.IA&ACCESS.2によりFIA_UAU.7が満たされる。

- **FIA_UID.2**

FIA_UID.2.1：TSFは、以下の①～⑥の外部インタフェースに対し、他の機能が動作する前に必ず識別機能を動作させ、監査者、CAオペレータ、RAサービスを各々識別しなければならない。

① CA監査端末からTOE外部機能であるWWWサービス機能を経てTOEへアクセスするインタフェース

② CA操作端末からTOE外部機能であるWWWサービス機能を経てTOEへアクセスするインタフェース

③ RAサービスがTOEへアクセスするインタフェース

④ サーバコンソールからTOEへアクセスするインタフェース

⑤ RDBMSがTOEとプロセス間通信を行うインタフェース

⑥ HSMがTOEとPCIバスを介してプロセス間通信を行うインタフェース

FIA_UID.2は次のセキュリティ機能により満たされる。

①はF.I.3「識別機能」で、監査者証明書を使用して監査者を識別する。②はF.IA&ACCESS.2「識別認証／アクセス制御機能」の識別認証機能で、「CAオペレータ管理データ」からCAオペレータが各自入力したCAオペレータIDを検索し、CAオペレータを特定することにより識別する。またF.I&ACCESS.1「識別／アクセス制御機能」の識別機能で、「CAオペレータ識別データ」からCAオペレータ証明書のシリアル番号を検索し、CAオペレータを特定することにより識別する。③はF.IA.4

「識別認証機能」で、RAサービスから送信されるCMP要求メッセージに同梱されるRA証明書とそれを識別するRAサービスIDが「RA識別データ」に登録されていることを確認することにより、RAサービスを識別する。④はOSが識別を行う。①②③で各々使用する監査者証明書、CAオペレータ証明書、RA証明書は、識別認証やアクセス制御を経た「証明書の発行」操作の権限を持つCAオペレータの通常操作に基づきTOEの証明書・CRL管理機能を利用して発行したものであり、また耐タンパー性のあるHSMで管理するCA秘密鍵を使用したディジタル署名が付加された信頼できる証明書である。更に監査者証明書とCAオペレータ証明書は発行後、監査者とCAオペレータが各々耐タンパー性のあるICカードで安全に管理するものである。なお⑤⑥からTOEを利用するアクセス経路はないため、利用者を識別する必要はない。

- **FIA_USB.1**

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

F.I&ACCESS.1「識別／アクセス制御機能」において、CAオペレータIDをCAオペレータプロセスに関連付ける。F.AUDIT.3「監査ログ操作機能」において、監査者IDを監査者プロセスに関連付ける。従って、F.I&ACCESS.1及びF.AUDIT.3により、FIA_USB.1は満たされる。

- **FMT_MSA.1[a1-1]**

FMT_MSA.1.1[a1-1]：TSFはCAオペレータアクセス制御SFPを実施して、CAオペレータID（「CAオペレータ識別データ」）に対し問い合わせ、削除、登録できる能力を「CAオペレータの登録・削除」操作の操作権を持つCAオペレータに制限しなければならない。

F.I&ACCESS.1「識別／アクセス制御機能」は、アクセス制御機能で使用するCAオペレータIDにに対して、「CAオペレータの登録・削除」操作の権限を持つCAオペレータだけが操作を実行できるように制限する。従って、F.I&ACCESS.1により、FMT_MSA.1[a1-1]が満たされる。

- **FMT_MSA.1[a1-2]**

FMT_MSA.1.1[a1-2]：TSFはCAオペレータアクセス制御SFPを実施して、CAオペレータIDに対して操作IDを関連付ける、及びCAオペレータIDと操作IDの関連付けを問い合わせる能力を「CAオペレータの操作権の設定」操作の権限を持つCAオペレータに制限しなければならない。

F.I&ACCESS.1「識別／アクセス制御機能」は、CAオペレータIDに対して操作IDを関連付ける操作、及びCAオペレータIDと操作IDの関連付けを問い合わせ操作を、「CAオペレータの操作権の設定」操作の権限を持つCAオペレータだけが操作できるように制限する。従って、F.I&ACCESS.1により、FMT_MSA.1[a1-2]が満たされる。

- **FMT_MSA.1[a1-3]**

FMT_MSA.1.1[a1-3]：TSFはCAオペレータアクセス制御SFPを実施して、CAオペレータ証明書の有効期限、CAオペレータ証明書の所有者、監査者証明書の有効期限、監査者証明書の所有者、RA証明書の有効期限、RA証明書の所有者に対して、問い合わせる能力を「証明書の内容を表示する」操作の権限を持つCAオペレータに制限しなければならない。

F.I&ACCESS.1「識別／アクセス制御機能」は、CAオペレータ証明書の有効期限、CAオペレータ証明書の所有者、監査者証明書の有効期限、監査者証明書の所有者、RA証明書の有効期限、RA証明書の所有者に対して問い合わせる操作を、「証明書の内容を表示する」操作の権限を持つCAオペレータだけが操作できるように制限する。従って、F.I&ACCESS.1により、FMT_MSA.1[a1-3]が満たされる。

また、FMT_MSA.1[a1-3]はセキュリティ属性の問い合わせ操作だけであり、セキュリティ属性を改変することはない。そのため、本事象を監査ログに記録する必要はない。

- **FMT_MSA.1[a2]**

FMT_MSA.1.1[a2]：TSFは合議操作アクセス制御SFPを実施して、合議操作の実行が許可されるCAオペレータの必要最小人数に対し、デフォルト値の変更、問い合わせ、改変できる能力を「CAオペレータの操作権の設定」操作の権限を持つCAオペレータに制限しなければならない。

F.IA&ACCESS.2の「識別認証／アクセス制御機能」のアクセス制御機能で使用する合議操作の実行が許可されるCAオペレータの必要最小人のデフォルト値変更、問い合わせ、改変を、「CAオペレータの操作権の設定」操作の権限を持つCAオペレータだけが操作できるように制限する。従って、F.IA&ACCESS.2により、FMT_MSA.1[a2]が満たされる。

- **FMT_MSA.2[b]**

FMT_MSA.2.1[b]：TSFは、セキュアな値だけがCA、CAオペレータ、監査者、RAサービスの公開鍵の有効期間及び所有者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.IA&ACCESS.1「識別認証／アクセス制御機能」は、CA、CAオペレータ、監査者、RAサービスの公開鍵の有効期間及び所有者を、許可されたCAオペレータだけが証明書として発行し配付できるように制限する。従って、F.IA&ACCESS.1により、FMT_MSA.2[b]が満たされる。

また、本事象の操作は許可されたCAオペレータのみに制限され、かつ許可されたCAオペレータが指定した有効期間及び所有者を受け入れる。そのため、セキュリティ属性に対して提示され拒否された値を監査ログに記録する必要はない。

- **FMT_MSA.2[e-f]**

FMT_MSA.2.1[e-f]：TSFは、セキュアな値だけがCA、RAサービスの公開鍵の有効期間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.IA.4「識別認証機能」は、CA及びRAサービスの公開鍵の有効期間を証明書として管理する。従

って、F.IA.4によりFMT_MSA.2[e-f]が満たされる。

　また、セキュリティ属性であるCA、RAサービスの公開鍵の有効期間は証明書として管理されているため、提示された有効期間を拒否することはない。そのため、セキュリティ属性に対して提示され拒否された値を監査ログに記録する必要はない。

- **FMT_MSA.2[h-i-j]**

FMT_MSA.2.1[h-i-j]：TSFは、セキュアな値だけが合議操作時に必要となる暗号鍵の利用者（CAオペレータ）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.IA&ACCESS.2「識別認証／アクセス制御機能」は、合議操作時に必要となる暗号鍵の利用者（CAオペレータ）属性を管理する。従って、F.IA&ACCESS.2により、FMT_MSA.2.1[h-i-j]が満たされる。

- **FMT_MSA.3[a1-1]**

FMT_MSA.3.1[a1-1]：TSF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、セットアップ時にはCAオペレータIDに対して全ての操作IDが関連付けられるという許可的なデフォルト値を与えるCAオペレータアクセス制御SFPを実施しなければならない。

FMT_MSA.3.2[a1-1]：N/A

　F.I&ACCESS.1「識別／アクセス制御機能」は、セットアップ時に登録されたCAオペレータに対して、全ての操作権限が与えられるという許可的なデフォルト値を与える。従って、F.I&ACCESS.1により、FMT_MSA.3[a1-1]が満たされる。

　また、FMT_MSA.3[a1-1]が管理する許可的なデフォルト設定を変更することはできないため、デフォルト設定の改変を監査ログに記録する必要はない。

- **FMT_MSA.3[a1-2]**

FMT_MSA.3.1[a1-2]：TSF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、運用中に新たに登録されるCAオペレータIDに対して関連付けられる操作IDは1つもないという制限的なデフォルト値を与えるCAオペレータアクセス制御SFPを実施しなければならない。

FMT_MSA.3.2[a1-2]：N/A

　F.I&ACCESS.1「識別／アクセス制御機能」は、運用中に新規に登録されるCAオペレータに対して、全ての操作に対する操作権限がないという制限的なデフォルト値を与える。従って、F.I&ACCESS.1により、FMT_MSA.3[a1-2]が満たされる。

　また、FMT_MSA.3[a1-2]が管理する制限的なデフォルト設定を変更することはできないため、デフォルト設定の改変を監査ログに記録する必要はない。

- **FMT_MSA.3[a2]**

FMT_MSA.3.1[a2]：TSFは、そのSFPを実施するために使われる各合議操作の実行が許可されるCAオペレータの必要最小人数として、セットアップ時に登録されているCAオペレータ全員の数という

制限的なデフォルト値を与える合議操作アクセス制御SFPを実施しなければならない。

FMT_MSA.3.2[a2]：N/A

F.IA&ACCESS.2「識別認証／アクセス制御機能」は、全ての合議操作の実行が許可されるCAオペレータの必要最小人数に対して、セットアップ時に登録されているCAオペレータの総数という制限的なデフォルト値を与える。従って、F.IA&ACCESS.2により、FMT_MSA.3[a2]が満たされる。

また、FMT_MSA.3[a2]が管理する制限的なデフォルト設定を変更することはできないため、デフォルト設定の改変を監査ログに記録する必要はない。

- **FMT_MTD.1**

FMT_MTD.1.1：TSFは、監査者証明書及びRA証明書を発行する能力を「PKCS#12形式の証明書の発行」操作の権限を持つCAオペレータに制限しなければならない。CAオペレータ証明書を発行する能力を「CAオペレータ証明書の発行」操作の権限を持つCAオペレータに制限しなければならない。CA証明書を発行する能力を「CA証明書の発行」操作の権限を持つCAオペレータに制限しなければならない。CAオペレータパスワードを改変、登録する能力をCAオペレータに制限しなければならない。監査ログをインポート、エクスポート、削除、検証する能力を監査者に制限しなければならない。監査者識別データ（監査者証明書）を登録、削除する能力を既にTOEに対して登録されている監査者に制限しなければならない。

F.I&ACCESS.1「識別／アクセス制御機能」は、監査者証明書、RA証明書、CA証明書、CAオペレータ証明書の発行操作を、それぞれの操作権限を持ったCAオペレータだけに制限する。また、F.I&ACCESS.1はCAオペレータのパスワードの改変、登録操作をCAオペレータだけに制限する。F.I.3「識別機能」は、監査ログの移入、移出、削除、検証操作を監査者だけに制限する。F.AUDIT.3「監査ログ操作機能」は、新規に監査者を登録する際の監査者証明書の登録操作を、既に登録されている監査者だけに制限する。従って、F.I&ACCESS.1、F.I.3、F.AUDIT.3により、FMT_MTD.1が満たされる。

- **FMT_SMR.1**

FMT_SMR.1.1：TSFは、監査者、CAオペレータ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.I&ACCESS.1「識別／アクセス制御機能」及びF.IA&ACCESS.2「識別認証／アクセス制御機能」は、CAオペレータという役割を維持する。F.I.3「識別機能」及びF.AUDIT.3「監査ログ操作機能」は、監査者という役割を維持する。従って、F.I&ACCESS.1、F.IA&ACCESS.2、F.I.3、F.AUDIT.3により、FMT_SMR.1が満たされる。

- **FPT_RVM.1**

FPT_RVM.1.1：TSFは以下の①～⑥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 CA監査端末からTOE外部機能であるWWWサービス機能を経てTOEへアクセスするインタフェース
② CA操作端末からTOE外部機能であるWWWサービス機能を経てTOEへアクセスするインタフェース
③ RAサービスからTOEへアクセスするインタフェース
④ サーバコンソールからTOEへアクセスするインタフェース
⑤ RDBMSがTOEとプロセス間通信を行うインタフェース
⑥ HSMがTOEとPCIバスを介してプロセス間通信を行うインタフェース

②ではWWWサービス機能による識別認証後、合議操作を行うためのアクセス要求に対してはF.IA&ACCESS.2「識別認証／アクセス制御機能」でTOEがCAオペレータの識別認証を行い、通常操作を行うためのアクセス要求に対してはF.I&ACCESS.1「識別／アクセス制御機能」でTOEがCAオペレータを識別する。WWWサービスは信頼できるサブジェクトであり、F.I&ACCESS.1でWWWサービス機能から流通する受け取ったCAオペレータ証明書もまた信頼できるものである。③ではF.IA.4「識別認証機能」でCMP要求メッセージに同梱されるRA証明書のRAサービスIDを基にRAサービスの識別を行い、CMP要求メッセージに付加されているディジタル署名、及びCMP要求メッセージに同梱されるRA証明書のディジタル署名について検証することによってRAサービスを認証する。④はOSが識別認証を行う。システム管理者は悪意を持たないためOSの識別認証で十分であり、またOSは信頼できるサブジェクトである。つまりOSから得られる識別情報もまた信頼できるものである。①ではWWWサービス機能による認証後、F.I.3「識別機能」でTOEが監査者を識別する。監査者は悪意を持たないためWWWサービス機能の識別認証で十分であり、またWWWサービスは信頼できるサブジェクトである。つまりF.I.3でWWWサービス機能から得られる識別情報もまた信頼できるものである。⑤のRDBMS、⑥のHSM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。従って、F.I&ACCES.1、F.IA&ACCESS.2、F.I.3、F.IA.4により、FPT_RVM.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.IA&ACCESS.2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。

本STではパスワードメカニズムと合議制メカニズムがこれに該当する。F.IA&ACCESS.2で記述したとおりパスワード入力を行う操作は必ず合議操作であることから、この二つは連動するものである。パスワードの入力はTOE外部機能であるWWWサービス機能の認証を完了したCAオペレータ（許可された利用者）に限定されるため、TOEが実装するパスワード強度で対抗できている。またこのパスワード認証は単独で実施するのではなく、操作に必要な複数人のCAオペレータの人数分だけ実施している。これにより専門的な知識を持つ許可されない利用者による技術的な攻撃と識別したエラーや許可された利用者による悪意のないアクションの両方の脅威に対抗できる。これは低レベルの攻撃の可能性を持つ攻撃者によるTOEセキュリティの直接的、及び意図的な攻撃からの適切な保護を行っていることになる。また、TOEは前提条件により物理的、及び接続的に保護されており、不特定のユーザからTOEへ直接攻撃が行われる可能性はない。可能性があるのはTOEに関連する操作端末からの攻撃だけである。以上の理由により、セキュリティ機能強度はF.IA&ACCESS.2により満たされるSOF-基本が妥当である。

8.3.3　保証手段根拠

表6-10に示すように、「TOEセキュリティ保証要件」は全て「保証手段」に示されたドキュメントのセットにより対応づけられる。また、「保証手段」に示されたドキュメントにより、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。これらのドキュメントを「TOEセキュリティ保証要件」に従って組織的に開発を実施することにより、保証要件が満たされる。

8.4　PP主張根拠

本STでは、準拠するPPはない。