Enterprise Certificate Server Set
セキュリティターゲット

2004/06/24

Version 1.10

株式会社 日立製作所

「Enterprise Certificate Server Set セキュリティターゲット」

― 変更歴 ―

変更番号	作成／変更年月日	バージョン	更新理由	作成者	承認者
1	2003/07/15	Version 1.00	**新規作成**	**恵南**	**高山**
2	2003/10/10	Version 1.01	2003/08/06 **版** DTW-ST **の内容を反映** 2003/09/17 **設計内レビューの内容を反映**	**恵南**	**高山**
3	2003/11/14	Version 1.02	2003/10/29 **版** DTW-ST **の内容を反映**	**恵南**	**高山**
4	2003/11/25	Version 1.03	DTT-EOR-0001〜0003 **の内容を反映** 2003/11/21 **設計内レビューの内容を反映**	**恵南**	**高山**
5	2003/11/27	Version 1.04	2003/11/27 **設計内レビューの内容を反映**	**恵南**	**高山**
6	2003/12/01	Version 1.05	2003/12/01 **設計内レビューの内容を反映**	**恵南**	**高山**
7	2003/12/19	Version 1.06	2003/12/10 **設計内レビューの内容を反映**	**恵南**	**高山**
8	2004/02/06	Version 1.07	2004/01/28 **設計内レビューの内容を反映**	**恵南**	**高山**
9	2004/02/13	Version 1.08	2004/02/09 **設計内レビューの内容を反映**	**恵南**	**高山**
10	2004/03/11	Version 1.09	2004/03/04 **設計内レビューの内容を反映** DTT-EOR-0021-00、DTT-EOR-0022-00 **の指摘内容を反映**	**恵南**	**高山**
11	2004/06/24	Version 1.10	2004/06/11 **設計内レビューの内容を反映**	**恵南**	**山口**

「Enterprise Certificate Server Set セキュリティターゲット」

― 変更書 ―

別紙「Enterprise Certificate Server Set セキュリティターゲット 変更書」参照。

商標類

Ethernet は，米国 Xerox Corp.の商品名称です。

Firewall-1 は，Check Point Software Technologies Ltd. およびその関連会社の商標または登録商標です。

Microsoft は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。

nShield は，英国 nCipher Corporation Ltd. の商標又は登録商標です。

PC/AT は，米国 International Business Machines Corp.の商品名称です。

RSA は，RSA Security, Inc.の商標です。

Solaris は，米国 Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

すべての SPARC 商標は，米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標がついた製品は，米国 Sun Microsystems, Inc. が開発したアーキテクチャに基づくものです。

Windows は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。

「Enterprise Certificate Server Set セキュリティターゲット」

― 目次 ―

― 図 目次 ―

― 表 目次 ―

1. ST 概説

1.1. ST 識別

1.1.1. ST 識別情報

本 ST（セキュリティターゲット）の識別情報を以下に示す。

名称：Enterprise Certificate Server Set セキュリティターゲット

バージョン：Version 1.10

識別名：ECS-ST-1.10

作成日：2004 年 6 月 24 日

作成者：株式会社 日立製作所

キーワード：PKI、公開鍵基盤、CA、認証局、合議

CC のバージョン：

- Common Criteria for Information Technology Security Evaluation, Ver. 2.1, Part 1-Introduction and general model (August 1999, CCIMB-99-031)
- Common Criteria for Information Technology Security Evaluation, Ver. 2.1, Part 2-Security functional requirements (August 1999, CCIMB-99-032)
- Common Criteria for Information Technology Security Evaluation, Ver. 2.1, Part 3-Security assurance requirements (August 1999, CCIMB-99-033)
- CCIMB Interpretations - 0210

1.1.2. TOE 識別情報

本 ST で評価する TOE（評価対象）の名称を以下に示す。

TOE 名称： Enterprise Certificate Server Set

識別名： P-9D44-72Z1

バージョン： 01

リビジョン： 01-A

作成者： 株式会社 日立製作所

1.2. ST 概要

1.2.1. TOE の概要

本 ST は、(株) 日立製作所のソフトウェア製品 「Enterprise Certificate Server Set （以降 ECS Set と略記)」 が提供する機能について記述する。ECS Set は、国際標準 X.509 に準拠した証明書の発行及び失効を管理する認証局製品であり、証明書発行サーバ機能を提供する CA サーバとリモートから管理を行う管理端末を用いて、証明書の発行管理を行うソフトウェアである。

ECS Set は、Enterprise Certificate Server(以降 ECS と略記)、PKI Runtime Library(以降 PRL と略記)、Keymate/Crypto Run Time（以降 Keymate と略記）のソフトウェアから構成されている。

ECS Set は、主に以下の機能を提供する。

- 証明書の発行及び管理機能
- 証明書失効リスト（CRL）の発行及び管理機能

ECS Set は、以下のセキュリティ機能を提供する。

- 監査機能
- 暗号機能
- アクセス制御機能
- 識別・認証機能
- CA 情報管理機能

1.2.2. 評価保証レベル

評価保証レベルは EAL 3 適合である。

1.2.3. 準拠する PP

PP（プロテクションプロファイル）は適用しない。

1.3. CC 適合の主張

本 ST は以下の CC に適合する。

- CC パート 2 適合
- CC パート 3 適合

1.4. 利用している文献

本 ST は以下の翻訳を利用している。

- 『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 情報処理振興事業協会 セキュリティセンター翻訳 第 1.2 版］
- 『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 情報処理振興事業協会 セキュリティセンター翻訳 第 1.2 版］
- 『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 情報処理振興事業協会 セキュリティセンター翻訳 第 1.2 版］
- 『補足-0210』
  ［独立行政法人製品評価技術基盤機構 適合性評価センター］

1.5. 用語の定義

表 1 に、本 ST で用いる用語の定義を示す。

表 1： 用語の定義

用語	意味
CA	（Certificate Authority の略）認証局のことをいう。
CA サーバ	認証局の機能を持つ ECS のサーバソフトウェアのことをいう。証明書や CRL の発行処理や、発行した証明書や CRL の管理を行う。
CA 情報設定合議	TOE のふるまいを決定する CA 情報設定に対する合議のことである。あらかじめ規定された複数の異なる CA 管理者がログインすることで、当該操作を行うことができる。
CA 証明書	認証局証明書のことをいう。
CA 秘密鍵	CA 証明書の公開鍵と対となる秘密鍵のことをいう。EE 証明書の署名に使用される。
CRL	（Certificate Revocation List の略）証明書に使用する鍵の漏洩などで鍵の信頼性が失われ、失効となった証明書のリストをいう。一般利用者は、CRL によって証明書が失効されていないかどうか確認する。
CRL 発行定義文	CRL を発行するために必要な情報が定義されたデータである。
DB データ暗号鍵	データベースを暗号化するときに必要な鍵のことをいう。
DES 暗号	共通鍵暗号の規格の一つである。
ECS	（Enterprise Certificate Server の略）認証局の機能を持つソフトウェア製品である。PRL や Keymate と共に、本 ST の TOE を構成する。TOE が提供する認証局機能のうちの、暗号処理以外の部分を提供する。
ECS Set	（Enterprise Certificate Server Set の略）本 ST の TOE である。ECS、PRL、Keymate から構成され、公開鍵暗号技術を用いて高度なセキュリティ基盤を構築する PKI システムの中で、認証局の機能を持つ製品である。
ECS 利用者	認証局において ECS Set を利用する利用者のことをいう。役職としては、CA 管理者、運用者、監査者が存在する。
EE 証明書	一般利用者に対して発行した証明書のことをいう。
FIPS 140-2	FIPS（Federal Information Processing Standard）は、米国

	の情報処理に関する規格であり、その中の 140-2 は暗号モジュールのセキュリティに関する規格である。
HSM	（Hardware Security Module の略）ハードウェア暗号装置のことをいう。認証局の秘密鍵を安全に管理し、また認証局の秘密鍵を使用した暗号処理を行う。
Keymate	（Keymate/Crypto Run Time の略）公開鍵暗号技術や共通鍵暗号技術を用いた、暗号機能を提供するソフトウェア製品である。ECS や PRL と共に、本 ST の TOE を構成する。TOE が提供する認証局機能のうちの、暗号処理部分の一部を提供する。
MD5	ハッシュアルゴリズムの一つである。
MULTI2 暗号	共通鍵暗号の一つである。
PBE	（Password Based Encryption の略）パスワード暗号方式のことをいう。
PKCS	（Public Key Cryptography Standard の略）RSA Security 社が開発した公開鍵暗号の規格のことをいう。
PKCS#1	RSA の公開鍵暗号システムに関する規格のことをいう。
PKCS#5	パスワードを基にした暗号方式をいう。
PKCS#7	メッセージやファイルを署名や暗号化する時に使用するデータ形式のことをいう。
PKCS#12	証明書と秘密鍵を暗号化するときに使用するデータ形式のことをいう。
PKCS#12 データ	EE 証明書と EE 証明書の対となる秘密鍵を PKCS#12 パスワードを基に PKCS#12 形式で暗号化したデータである。
PKCS#12 パスワード	PKCS#12 データを作成及び PKCS#12 データから EE 証明書と EE 証明書の対となる秘密鍵を取り出すために必要なパスワードである。
PKI	（Public Key Infrastructure の略）公開鍵暗号技術を使用したセキュリティ基盤技術の中で、証明書を利用する認証システムのことをいう。
PRL	（PKI Runtime Library の略）公開鍵暗号技術や共通鍵暗号技術を用いた、暗号機能を提供するソフトウェア製品である。ECS や Keymate と共に、本 ST の TOE を構成する。TOE が提供する認証局機能のうちの、暗号処理部分の一部を提供する。
SHA-1	ハッシュアルゴリズムの一つである。

X.509	OSI による証明書のフォーマットを規定した国際標準規格である。
暗号化	他の人から読み取れないような形式にデータを変換することをいう。
運用操作合議	運用者が管理端末から行う証明書操作に対する合議のことである。あらかじめ規定された複数の異なる運用者が合議承認を行うことで当該操作が有効になる。
監査ログ	運用時の操作やエラーを記録したログのことをいう。認証サーバの運用監視に利用できる。各監査ログは、監査ログ用証明書によって署名されており、認証サーバにファイルとして出力される。運用記録の盗聴や改竄を防止できるので、信頼性の高い運用監視ができる。
管理端末	ECS のクライアントソフトウェアのことをいう。証明書や CRL の発行や管理操作、認証サーバの運用・管理操作などの認証サーバに対する操作は、すべて管理端末から行う。
検定	署名を確認することをいう。
公開鍵	公開鍵暗号方式で、暗号化や復号化するために秘密鍵と対になっている鍵のことをいう。秘密鍵と公開鍵は対になっており、一方の鍵で暗号化したメッセージは、対となる他方の鍵でないと復号化できない。
合議	複数の異なる ECS 利用者が合意の上当該操作を行うことをいう。本 TOE では、CA 情報設定合議と運用操作合議がある。
合議承認	合議中の操作に対して承認することをいう。
合議否認	合議中の操作に対して否認することをいう。合議否認によって当該操作は無効となる。
セキュアエリア	入退室管理が行われ、不正な物理的アクセスから保護されたエリアのことをいう。セキュアエリアには、CA 管理者のみ入室することができる。
証明書	正当性を保証するための電子的な証明書のことをいう。認証局が署名するため、改竄や偽造はできないようになっている。
署名	当該ユーザ自身、あるいは当該認証局以外には作成できない情報のことをいう。署名を確認することで、不正なアクセスによる改竄や成りすましがないかを確認できる。
耐タンパ性	一般的に、悪意をもったユーザが不正な手段を用いて内部情報を獲得しようとした場合に、それを阻止するように働く機能や性質のことをいう。

内部セグメント	マシンエリア内に設置される。 ファイアウォールを介してインターネットに接続される。
認証局	証明書を発行する機関のことをいう。当該認証局が発行した認証局証明書を持っているかどうかで、通信相手が正当かどうかを判断する。
認証局証明書	認証局が自認証局の正当性を保証するために発行する証明書のことをいう。
認証局に属する者	TOE を運用する組織に属する者のことをいう。TOE へのアクセスを許可された ECS 利用者と TOE へのアクセスを許可されていない者がいる。いずれの者も認証局を運用する組織の管理者によって適切に管理される。
ハードウェア暗号装置	秘密鍵の管理、署名や検定などを処理する装置のことをいう。秘密鍵は、この装置の外に出ないため、秘密鍵に対する盗聴や改竄の心配がない。
半角記号	以下の「」で囲まれた記号をいう。 「 」(スペース)「!」「"」(ダブルクォーテーション)「#」「%」「&」 「'」(シングルクォーテーション)「(」「)」「*」「+」「,」(コンマ)「-」 「.」(ピリオド)「/」「:」「;」「<」「>」「=」「?」「[」「]」「\」「^」「_」「{」「}」「¦」
秘密鍵	公開鍵暗号方式で、暗号化や復号化するために公開鍵と対になっている鍵のことをいう。
秘密情報格納ディレクトリ	CA サーバ起動時に必要な設定情報などを保管する、暗号化された格納領域である。
復号化	暗号化されたデータを読めるようなデータに復元することをいう。
マシンエリア	認証局のマシンルームのことをいう。マシンエリアには、認証局に属する者のみ物理的にアクセスすることができる。
リポジトリ	証明書を利用する一般利用者に証明書や CRL を公開したり、発行した証明書や CRL を管理したりする。

2. TOE 記述

2.1. TOE の種別

TOE は、国際標準 X.509 に準拠した証明書の発行及び失効を管理する認証局（CA）の機能を提供する ECS Set というソフトウェア製品である。

2.2. TOE 概要

ECS Set は、認証局（CA）において、国際標準 X.509 に準拠した証明書の発行及び失効リスト（CRL）を生成、発行し、これの管理を行う。ECS Set が利用される認証局の位置付け及び発行されるデータの流れを図 1 に示す。

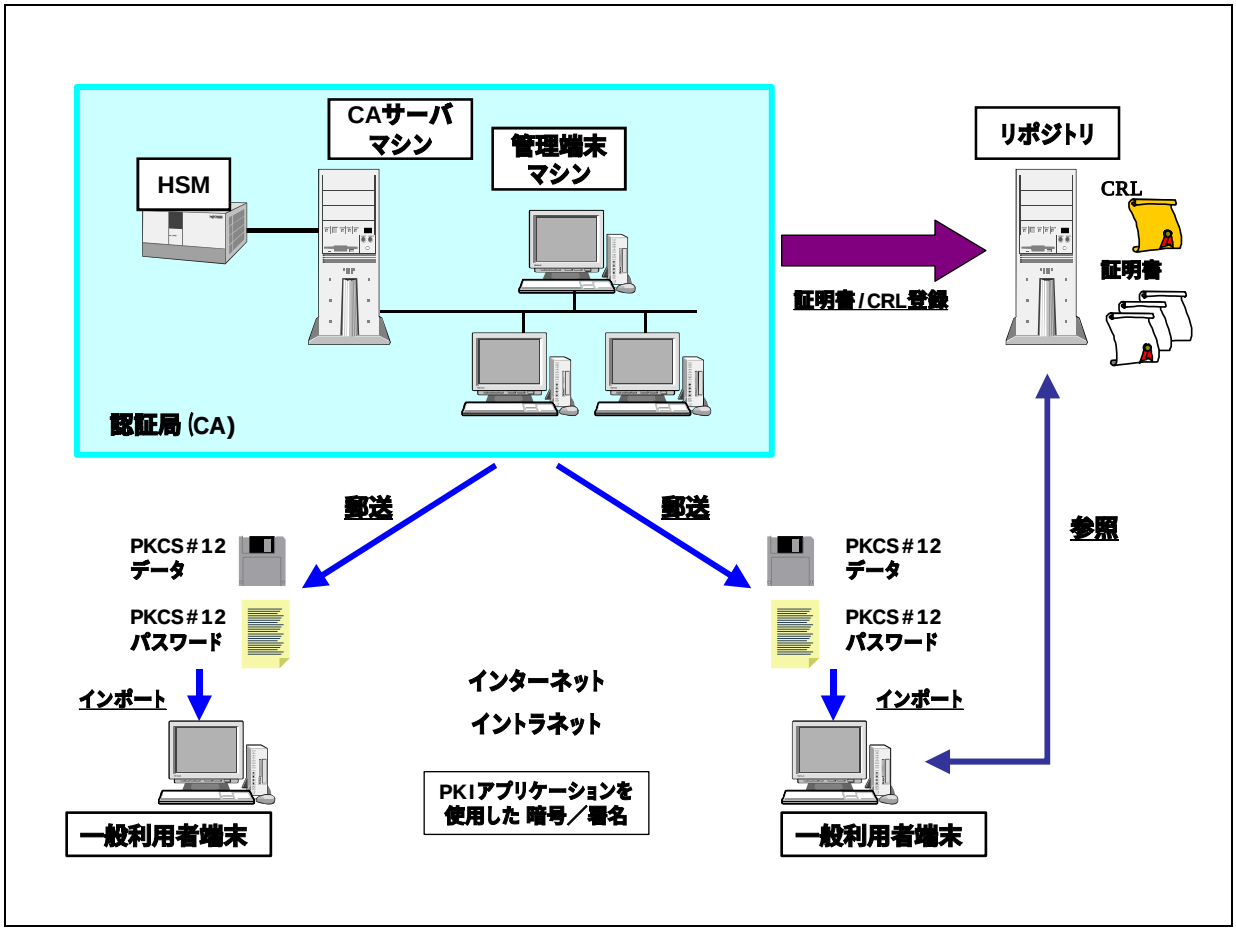

図 1： ECS Set が利用される認証局の位置付け及び発行されるデータの流れ

認証局（CA）は、ECS Set を使用して以下の業務を行う。

- 一般利用者（EE）の公開鍵／秘密鍵ペアを生成する。
- 一般利用者（EE）の公開鍵に対して電子署名を付与し、公開鍵証明書（EE 証明書）を発行する。
- 一般利用者（EE）の EE 証明書及び秘密鍵をペアにして、一般利用者（EE）の PKCS#12 パスワードを基に、PKCS#12 形式で暗号化した PKCS#12 データを生成する。
- 一般利用者の EE 秘密鍵の漏洩などで鍵の信頼性が失われた場合、証明書を失効し、失効リスト（CRL）を発行する。

認証局は、ECS Set を使用して発行したデータを以下のように登録及び送付する。

- 発行した EE 証明書及び CRL は、管理端末マシンから取得し、リポジトリに登録する。
- 生成した PKCS#12 データは、管理端末マシンから取得し、フロッピーディスクなどに格納して、郵送などのオフラインの手段により、一般利用者に送付する。
- 生成した PKCS#12 パスワードは、管理端末マシンから取得し、紙に印刷して、郵送などのオフラインの手段により一般利用者に送付する。

一般利用者は、ECS Set を使用して発行されたデータを以下の流れで利用する。以下は認証局の業務ではない。また、一般利用者は、ECS Set に直接アクセスすることはない。

- 一般利用者は、送付された PKCS#12 データを一般利用者端末にインポートする。その際、別途送付された PKCS#12 パスワードを使用する。
- 一般利用者は、インポートされた PKCS#12 データ（EE 証明書及び秘密鍵）を使用して、インターネットやイントラネットを介して PKI アプリケーションによる署名・暗号化を行う。
- 相手先の EE 証明書を取得したり、相手先の EE 証明書が失効していないかを確認するために、インターネットを介して リポジトリを参照する。

2.3. TOE 範囲

2.3.1. TOE の動作及び関連するハードウェア構成

TOE を利用した認証局システムのハードウェア構成の一例を図 2 に示す。

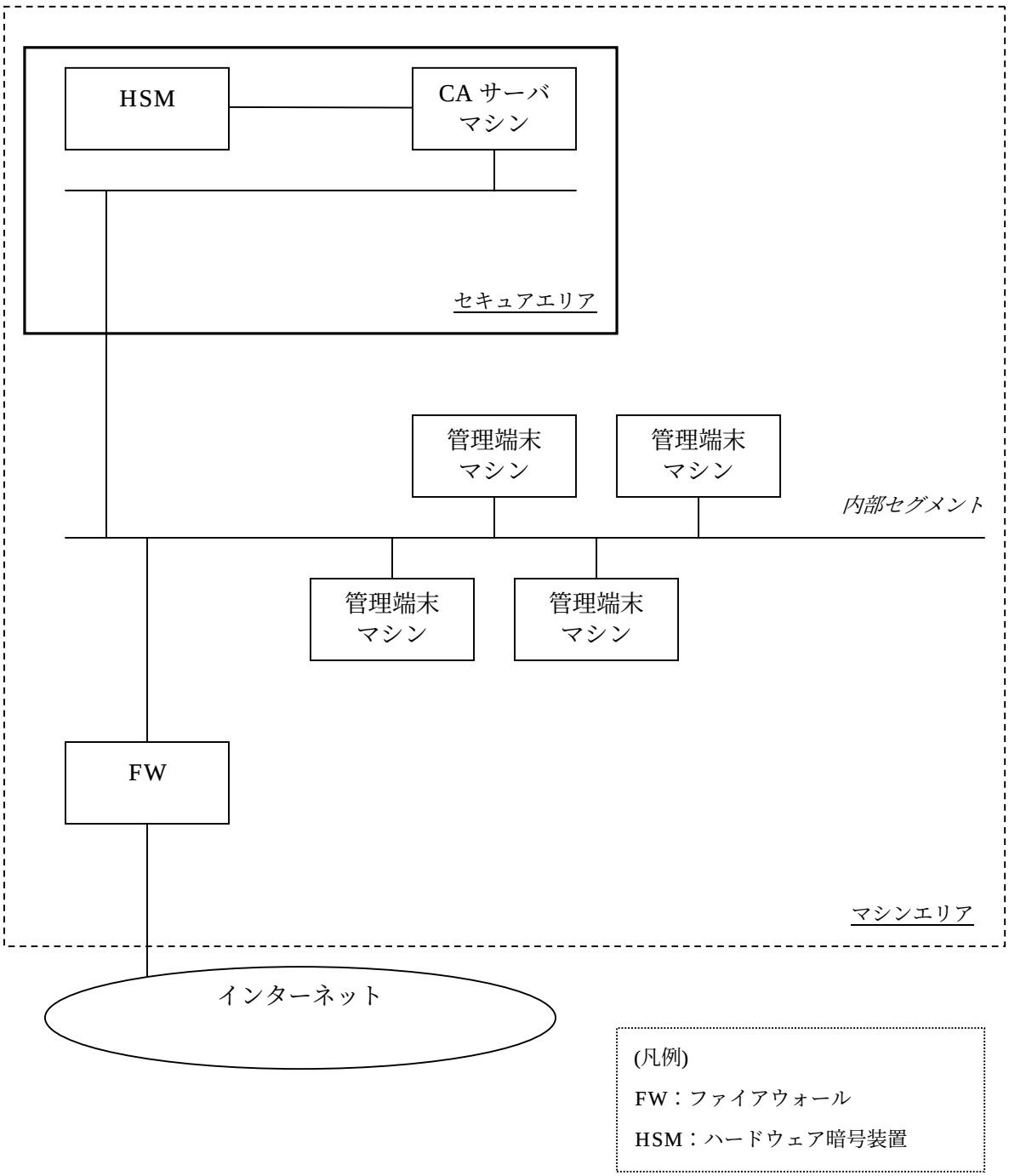

図 2： 認証局システムのハードウェア構成の例

以下に、図 2 に示した各々のハードウェアについて説明する。

＜TOE 及び IT 環境を構成するマシン＞

- **CA サーバマシン：**
  本 ST の TOE である ECS Set のサーバソフトウェア（CA サーバ）が動作する。
  認証局のサーバ機能を提供する。
  入退室管理が行われ、不正な物理的アクセスから保護されたセキュアエリア内に設置される。
  認証局のネットワークの内部セグメントに Ethernet を使用して接続される。
- **管理端末マシン：**
  本 ST の TOE である ECS Set のクライアントソフトウェア（管理端末）が動作する。
  認証局のマシンエリア内に設置される。
  CA サーバと通信することによって、EE 証明書及び CRL のリモート管理を行う。
  認証局のネットワークの内部セグメントに Ethernet を使用して接続される。
- **HSM：**
  CA 秘密鍵が格納されており、CA 秘密鍵を使用した署名などの暗号操作を行う。CA 秘密鍵が HSM 外に漏洩することはない。HSM は、FIPS 140-2 level3 相当の要件に準拠している。
  入退室管理が行われ、不正な物理的アクセスから保護されたセキュアエリア内に設置される。
  CA サーバマシンに SCSI を使用して接続される。
  本 ST の TOE 外であり、IT 環境として利用する。

＜TOE 及び IT 環境以外を構成するマシン＞

- **ファイアウォール：**
  認証局のマシンエリア内に設置される。
  認証局のネットワークのインターネット、内部セグメントを論理的に分離する。
  本 ST の TOE 外である。

＜論理エリア＞

- **内部セグメント：**
  マシンエリア内に設置され、CA サーバマシン、管理端末マシン、ファイアウォールが Ethernet を使用して接続される。内部セグメントは、ファイアウォールによって、インターネットからのアクセスは拒否されるように設定されている。

＜物理エリア＞

- **セキュアエリア:**
  CA サーバマシン、HSM が設置される。セキュアエリアには、TOE の動作に関係しない機器は設置されない。入退室管理が行われ、不正な物理的アクセスから保護されている。セキュアエリアには、CA 管理者のみ入室することができる。
- **マシンエリア:**
  認証局内に設置されたマシン室であり、管理端末マシン、ファイアウォールが設置される。マシンエリアには、認証局に属する者のみ物理的にアクセスすることができる。

以下に、図 2 に示した各々のハードウェアの仕様を記述する。

- **CA サーバマシン:**
  Solaris 8 が稼動する SPARC プラットフォームのマシン
- **管理端末マシン:**
  Windows2000 が搭載できる日立 FLORA シリーズのマシンまたは PC/AT 互換機
- **HSM:**
  nShield F3 SCSI 150 標準エンクロージャ（nCipher 社製 ハードウェア暗号装置）
- **ファイアウォール:**
  Windows2000 が搭載できる日立 FLORA シリーズのマシンまたは PC/AT 互換機

2.3.2. TOE の動作及び関連するソフトウェア構成

以下に、図 2 に示した各々のハードウェアが使用するソフトウェアについて記述する。

- **CA サーバマシン:**
  - Solaris 8
    CA サーバマシンのオペレーティングシステムである。
    本 ST の TOE 外であり、IT 環境である。
  - Enterprise Certificate Server Set 01-01-A（形名：P-9D44-72Z1）
    ECS Set のサーバソフトウェア（CA サーバ）である。
    本 ST の TOE である。
  - HiRDB/Single Server Version 6 (64) 06-01 以降（形名：P-9D62-1561）
    CA サーバが使用するデータベースのプログラムである。
    本 ST の TOE 外であり、IT 環境である。
  - SORT Version 6（型名：P-9321-1311）
    データベースを使用するためのプログラムである。
    本 ST の TOE 外であり、IT 環境である。
  - nCipher Support Software for Solaris

HSM を使用するためのプログラムである。

本 ST の TOE 外であり、IT 環境である。

- **管理端末マシン:**
  - Microsoft Windows 2000 Professional Service Pack 3 以降

    管理端末マシンのオペレーティングシステムである。

    本 ST の TOE 外であり、IT 環境である。
  - Enterprise Certificate Server Set 01-01-A（形名：P-9D44-72Z1）

    ECS Set のクライアントソフトウェア（管理端末）である。

    本 ST の TOE である。
- **ファイアウォール:**
  - Microsoft Windows 2000 Server Service Pack 1

    ファイアウォールのオペレーティングシステムである。

    本 ST の TOE 外である。
  - Check Point Firewall-1 Next Generation FP3

    ファイアウォールの機能を提供するプログラムである。

    本 ST の TOE 外である。

2.4. 保護対象資産

TOE の運用・管理において、以下の保護対象資産を想定する。一般的に証明書及びこれに対応する秘密鍵は、セキュリティ機能に関連するデータとして取り扱われるが、本 ST の TOE は証明書の発行及び失効を管理するソフトウェアであるため、本 ST では証明書申請者に対して発行する証明書に関連するデータ（EE 証明書、PKCS#12 データ、PKCS#12 パスワード、CRL、CRL 発行定義文）は利用者データとして扱う。

2.4.1. 利用者データ

(1) EE 証明書

認証局のサービスとして発行される一般利用者の証明書である。生成されるデータの性質上、改竄と削除からは保護されるべきであるが、公開して利用されるデータであるため、暴露から保護する必要はない。

(2) PKCS#12 データ (EE 証明書と秘密鍵)

EE 証明書と EE 証明書の対となる秘密鍵を PKCS#12 パスワードを基に PKCS#12 形式で暗号化したデータである。EE 証明書の対となる秘密鍵は PKI サービスの要であるため、暴露と改竄、削除から保護される必要がある。

(3) PKCS#12 パスワード (EE 証明書と秘密鍵のパスワード)

PKCS#12 データを作成するため、及び PKCS#12 データから EE 証明書と EE 証明書の対となる秘密鍵を取り出すために必要なパスワードである。暴露と改竄、削除から保護する必要がある。

(4) CRL (証明書失効リスト)

EE 証明書の対となる秘密鍵、あるいは CA 証明書の対となる秘密鍵が危殆化した場合に、当該証明書が失効したことを公開するために作成される。認証局のサービスとして発行される。生成されるデータの性質上、改竄と削除からは保護されるべきであるが、公開して利用されるデータであるため、暴露から保護する必要はない。

(5) CRL 発行定義文

CRL を発行するために必要な情報が定義されたデータである。CRL の性質上、改竄と削除からは保護されるべきであるが、暴露から保護する必要はない。

上記利用者データは、すべてデータベースに格納される。

2.4.2. TSF データ

(6) ECS 利用者 ID

TOE を操作する利用者の情報である。ECS 利用者の識別に使用される。
データベースに格納される。

(7) ECS 利用者パスワード

TOE を操作する利用者の情報である。ECS 利用者の認証に使用される。
暗号化されてデータベースに格納される。

(8) ECS 利用者権限リスト

TOE を操作する利用者の情報である。管理端末からの各操作を実施する権限があるかどうかが記載され、ECS 利用者が保護対象資産にアクセスする際のアクセス制御に使用される。
データベースに格納される。

(9) CA 設定情報

TOE が動作するために必要な設定情報である。CA 設定情報には、監査ログの署名に必要な情報、監査ログとデータベースの暗号化に必要な情報、合議操作を行うために必要な情報が含まれる。
秘密情報格納ディレクトリに格納される。

(10) DB データ暗号鍵

TOE で利用するデータベース内のデータを暗号化するための暗号鍵である。
秘密情報格納ディレクトリに格納される。

(11) 監査ログ

TOE 運用時の操作や エラーなどの事象が記録されたデータである。
CA サーバマシンの OS の管理下にあるファイルとして保管される。

(12) 監査ログ用証明書／監査ログ用秘密鍵

監査ログを署名するための秘密鍵及び公開鍵証明書である。
秘密情報格納ディレクトリに格納される。

以降の記述では、上記 ECS 利用者 ID、ECS 利用者パスワード、ECS 利用者権限リストの集合を、ECS 利用者情報と表記する。

2.5. TOE の関連者

本 ST では、TOE の構築・運用・管理に関連する者として、以下の役職を想定する。

2.5.1. システム構築者

CA サーバ、管理端末及び周辺機器など TOE 及び TOE の IT 環境のシステム構築を行う。具体的には、以下の作業を行う。

- CA サーバのインストール
- CA サーバを使用するためのセットアップ
- データベースの構築
- データベーステーブルの作成
- DB データ暗号鍵の設定
- HSM の設定
- CA サーバの起動
- ECS 利用者の登録

- 管理端末のインストール
- 管理端末のセットアップ

システム構築後は、CA 管理者が認証局システムの管理を行う。

システム構築者は、システムの構築時には、セキュアエリア、マシンエリアに立ち入ることができるが、システム構築後は、CA 管理者に引継ぎを行い、以降 TOE にアクセスすることはできない。

2.5.2. CA 管理者

CA 管理者は、システム構築直後、認証局のサービスを稼動させるために必要な以下の作業を管理端末から行う。

- CA 秘密鍵の作成
- CA 証明書の作成と登録
- 合議の設定

CA 管理者は、CA サーバマシンの OS に直接ログインして、以下の操作を行う。

- CA サーバの起動／停止
- HSM の管理

CA 管理者は、認証局の管理業務として必要に応じて、管理端末を利用して、以下の操作を行う。以下の操作を行うためには、CA 情報設定合議が必要である。

- DB 暗号化の設定
- 監査ログ用証明書名称の設定
- 監査ログ暗号化の設定
- ECS 利用者登録
- ECS 利用者削除
- ECS 利用者情報の改変
- 合議情報の改変

CA 証明書には、認証局が定めた有効期限が設定される。設定された有効期限が切れた後、CA 管理者は、新たな CA 証明書を作成するために、以下の操作を行う。

- CA 秘密鍵の更新
- CA 証明書の更新

CA 管理者が他の役職を兼務することはできない。
CA 管理者は、セキュアエリア、マシンエリアに立ち入ることを許可されている。

2.5.3. **運用者**

運用者は、管理端末を利用して、証明書の発行／失効等の運用業務を行う。
具体的には、以下の操作を行う。

- EE 証明書検索／取得／失効／削除
- PKCS#12 データ作成／取得
- PKCS#12 パスワード取得
- CRL 発行定義文登録／削除
- CRL 作成／検索／削除／取得

運用者が行う以下の操作には、運用操作合議が必要である。

- EE 証明書失効／削除
- PKCS#12 データ作成
- CRL 発行定義文登録／削除
- CRL 発行定義文削除合議
- CRL 作成／削除

運用者が他の役職を兼務することはできない。
運用者は、マシンエリアに立ち入ることは許可されているが、セキュアエリアに立ち入ることを許可されていない。

2.5.4. 監査者

TOE が生成する監査ログの分析等の監査業務を行う。監査者は、管理端末を使用して、以下の操作を行う。

- 監査ログファイル一覧の問い合わせ
- 監査ログファイルの参照
- 監査ログファイルの削除
- 監査ログファイルの取り出し

監査者が他の役職を兼務することはできない。

監査者は、マシンエリアに立ち入ることは許可されているが、セキュアエリアに立ち入ることを許可されていない。

2.5.5. 認証局に属する者

TOE を運用する組織に属する者のことである。上記に示した、CA 管理者、運用者、監査者は認証局に属しているが、システム構築者は、認証局には属していない。認証局に属する者には、TOE へのアクセスが許可された ECS 利用者と TOE へのアクセスが許可されていない者がいる。認証局に属する者のうち、TOE へのアクセスが許可されていない者も、マシンエリアへの入退室は行うことができる。認証局に属する者は、認証局を運用する組織の管理下にあり、特殊な機器を持ち込んだ攻撃や、管理端末マシンへの攻撃などの認証局の運用を妨害するような悪質な攻撃は行わない。

※ 本 ST の想定する利用者は上記であり、いわゆる一般利用者は、EE 証明書及び CRL の利用者であり、TOE の範囲外である。

2.6. TOE が提供する機能

本 ST の TOE は、国際標準 X.509 に準拠した証明書の発行及び失効を管理する機能を提供する CA サーバと、リモートから管理を行う管理端末を用いて、証明書の発行管理を行うことができる。

TOE は主に以下の機能を提供する。

- 証明書の発行及び管理機能
- 証明書失効リスト（CRL）の発行及び管理機能

2.7. TOE が提供するセキュリティ機能

TOE は、以下のセキュリティ機能を提供する。

2.7.1. 監査機能

TOE は、認証局が適切に運用されていることを監査するために必要な情報を監査ログとして記録し、監査ログの保護、表示及び管理を行う。

2.7.2. 暗号機能

TOE は、DB データ暗号鍵や、CA サーバ起動時に必要な設定情報などを保管するために、暗号化された格納領域である秘密情報格納ディレクトリを提供する。

TOE は、監査ログを暴露と改竄から保護するために、監査ログに署名・暗号化を行い、また検定・復号化を行う機能を提供する。

TOE は、データベースに格納されたデータのうち、暴露から保護すべき保護対象資産を暗号化する。

TOE は、管理端末と CA サーバの間の通信路を流れるデータを暗号化する。

2.7.3. アクセス制御機能

TOE は、あらかじめ定められた ECS 利用者の権限に基づき、ECS 利用者がアクセスできる利用者データを制御する。また、利用者データに関する操作については、複数の異なる ECS 利用者による合意の上で操作を許可するために、合議機能を提供する。

2.7.4. 識別・認証機能

TOE は、管理端末を通じて CA サーバにログインを試みる利用者に対して、識別・認証を行い、当該利用者が、TOE に登録された正当な ECS 利用者であることを確認する。

2.7.5. CA 情報管理機能

TOE は、認証局を適切に運用するための、CA サーバの動作に関する設定機能を提供する。また、ECS 利用者の登録、削除及び ECS 利用者情報の管理を行う機能を提供する。また、CA サーバの動

作に関する設定機能については、複数の異なる ECS 利用者による合意の上で操作を許可するために、合議機能を提供する。

2.8. TOE の範囲外である機能

以下の機能は、TOE の範囲外である。

2.8.1. HSM 機能

TOE の CA 秘密鍵に関連した暗号処理は、FIPS140-2 level3 相当の機能を持つ HSM を使用する。CA 秘密鍵は、HSM の外に露出することはない。また、HSM は、耐タンパ性を持ち、物理的な攻撃からデータを守る物理保護機能を持つ。

2.8.2. データベース機能

TOE が利用するデータを管理する処理は、HiRDB の機能を使用する。データを管理するデータベース機能は、TOE 外の機能であるが、HiRDB に格納される保護対象資産は、TOE の制御下にある。

2.8.3. オペレーティングシステム機能

TOE 及びその環境のソフトウェアが動作するための基盤となる機能は、オペレーティングシステムである Solaris 8 及び Microsoft Windows 2000 の機能を使用する。

2.8.4. ファイアウォール機能

インターネット、内部セグメントを論理的に分離する機能である。ファイアウォール機能は、TOE 範囲外である。

3. TOE セキュリティ環境

3.1. 前提条件

3.1.1. 利用環境

A.TOE_SEP (不正な干渉からの分離)

TOE が動作する CA サーバマシン、管理端末マシンには、TOE の動作に必要なソフトウェア以外はインストールされないものと仮定する。

A.ABSTRACT_ACCOUNT (下位抽象マシンのアカウント)

TOE が動作するために必要な OS 及び DB のアカウントは適切に管理されており、このアカウントを不正に利用した保護対象資産の改竄と削除はないものと仮定する。

A.PASSWORD (パスワードの管理)

ECS 利用者のパスワードは、ECS 利用者本人によって適切に管理され、本人以外に知られることはないものと仮定する。

A.IT_ENV (TOE の IT 環境)

TOE の IT 環境は、正常に動作するものと仮定する。

3.1.2. 物理管理

A.ABSTRACT (下位抽象マシンの動作)

TOE が動作するために必要な OS 及び DB は、不正な改変から保護され、正しく動作するものと仮定する。

A.SETTING (設置エリア)

CA サーバマシン及び HSM は、セキュアエリア内に設置され、管理端末マシンは、マシンエリア内に設置されるものと仮定する。

A.AREA (エリアの保護)

・セキュアエリアは、入退室管理が行われ、不正な物理的アクセスから保護されるものと仮定する。
・セキュアエリアには、CA 管理者のみ入室することができるものと仮定する。
・マシンエリアには、認証局に属する者のみ物理的にアクセスできるものと仮定する。

3.1.3. 接続・動作環境

A.FIREWALL (ファイアウォール)

内部セグメントは、ファイアウォールを経由してインターネットに接続され、インターネットから CA サーバマシン及び管理端末マシンへの直接のアクセスは存在しないものと仮定する。

3.2. 脅威

T.UNAUTH_ACCESS (不正なアクセス)

ECS 利用者が、管理端末マシンから TOE を使用して、与えられた権限外の操作を行うことにより、保護対象資産を暴露、改竄または削除するかもしれない。

T.IMPERSON (不正ログイン)

ECS 利用者でない認証局に属する者が、管理端末マシンから TOE に不正にログインすることにより、TOE を使用して、保護対象資産を暴露、改竄または削除するかもしれない。

T.TOE_SECRET (秘密情報の暴露)

ECS 利用者でない認証局に属する者が、CA サーバマシンの OS や DB にアクセスすることによって、暴露から保護する必要がある保護対象資産を暴露するかもしれない。

T.LINE_SECRET (通信回線上の秘密情報の暴露／改竄)

ECS 利用者でない認証局に属する者が、管理端末と CA サーバの間のネットワーク上を流れるデータを傍受することによって、これを暴露または改竄するかもしれない。

T.MISS (操作ミスによるデータ改竄／削除)

CA 管理者及び運用者が、操作ミスによって、アクセスが許可されている保護対象資産を改竄または削除してしまうかもしれない。

3.3. 組織のセキュリティ方針

P.CA_ADMIN (CA 管理者)

CA 管理者は、TOE 及び TOE の IT 環境を管理する管理業務を適切に行うこととする。
また CA 管理者は、認証局の運用管理に対する知識を有する者が担当し、指定された以外の手段で TOE の構成を変更しないものとする。
CA 管理者は、他の役職を兼務することはできないものとする。

P.OPERATOR (運用者)

運用者は、TOE の運用業務を適切に行うこととする。
運用者は、他の役職を兼務することはできないものとする。

P.AUDITOR (監査者)

監査者は、TOE の監査業務を適切に行うこととする。
監査者は、他の役職を兼務することはできないものとする。

P.SIER (認証局の構築者)

システム構築者は、TOE 及び TOE の IT 環境のマニュアルを熟読し、設置・生成・立上げを適切に行うこととする。

P.DUALCTL (合議)

TOE の管理業務における重要な操作は、複数の CA 管理者による合議の上で行うこととする。
また TOE の運用業務における重要な操作は、複数の運用者による合議の上で行うこととする。

P.HSM (HSM)

TOE を利用する認証局は、FIPS 140-2 level3 相当の機能を持つ HSM により、物理的に保護された CA 秘密鍵を利用した、暗号操作及び CA 秘密鍵のライフサイクル管理を行うこととする。

P.PERSONNEL (認証局に属する者)

認証局に属する者は、認証局を運用する組織の管理下にあり、特殊な機器を持ち込んだ攻撃や、管理端末マシンへの攻撃などの認証局の運用を妨害するような悪質な攻撃は行わないこととする。

P.PROTECT_LOG (監査ログの保護)

TOE を利用する認証局は、監査ログの暴露、改竄または削除の防止のために必要な措置をとる

こととする。

4. セキュリティ対策方針

4.1. TOE セキュリティ対策方針

4.1.1. TOE 管理

O.ADMIN (TOE の管理)

TOE は、正当な CA 管理者に対して、TOE 及びそのセキュリティ機能を適切に管理できるようにする。

4.1.2. アクセス制御

O.AC_DATA (保護対象資産のアクセス権限)

TOE は、保護対象資産を暴露、改竄または削除から保護するために、適切な権限を持つ者だけが保護対象資産にアクセスできるように制限する。

4.1.3. 識別・認証

O.I&A (TOE での識別･認証)

TOE は、TOE の保護対象資産へのアクセスを許可する前に、全ての利用者に対して識別・認証情報の入力を要求し、識別・認証を実施する。

4.1.4. データ保護

O.ENC_DATA (保管データの保護)

TOE は、暴露から保護する必要がある以下の保護対象資産を暗号化して保管する。

- PKCS#12 データ
- PKCS#12 パスワード
- ECS 利用者パスワード
- CA 設定情報
- DB データ暗号鍵
- 監査ログ用証明書
- 監査ログ用秘密鍵

O.ENC_LINE (通信データの保護)

TOE は、管理端末と CA サーバの間の通信を暗号化して行う。

4.1.5. 監査ログ

O.AUDIT (監査ログの記録･追跡･管理)

TOE は、運用・管理操作やエラーなどセキュリティに関連する事象を記録し、発生した事象を監査者が追跡・管理できるようにする。

O.PROTECT_LOG (監査ログの保護)

TOE は、監査ログを暴露から保護し、監査ログが改竄または削除された場合、検出できるようにする。

4.1.6. 合議

O.COUNCIL (合議に基づいた操作)

TOE は、運用時に行われる運用・管理操作に対して複数人による合議を要求する。

4.2. IT 環境セキュリティ対策方針

4.2.1. CA 秘密鍵の保護

OE.HSM (HSM での鍵生成／破棄)

CA 秘密鍵のライフサイクル管理及び CA 秘密鍵を利用した暗号操作は、IT 環境として提供される FIPS 140-2 level3 相当の機能を持つ HSM を使用する。

4.3. 運用・管理的セキュリティ対策方針

4.3.1. 設置・生成・立上げ規定

OM.SI (システム構築手順)

システム構築者は、ECS Set のガイダンス文書が定める手順に従って、TOE 及び TOE の IT 環境のマニュアルを熟読した上で、TOE 及び TOE の IT 環境を構築しなければならない。この際、CA サーバマシン、管理端末マシンには、TOE の動作に関係ないソフトウェアをインストールしてはならない。

OM.SETTING (設置規定)

・CA サーバマシン及び HSM は、セキュアエリア内に設置しなければならない。
・管理端末マシンは、マシンエリア内に設置しなければならない。

OM.CONNECT (接続規定)

・内部セグメントは、ファイアウォールを介してインターネットに接続しなければならない。
・ファイアウォールは、インターネットから CA サーバマシン、管理端末マシンへのアクセスを拒否するように、設定しなければならない。

4.3.2. 運用・管理規定

OM.AREA_CONTROL (入退室制限)

・セキュアエリアは、CA 管理者のみ入室できるよう入退室管理を行い、不正な物理的アクセスから保護しなければならない。

・マシンエリアは、認証局に属する者のみ物理的にアクセスできるように制限しなければならない。

OM.MACHINE_MGT (マシンの管理)

・CA 管理者は、TOE が動作する OS 及び DB が不正な改変から保護され、正しく動作するよう適切に管理しなければならない。
・CA 管理者は、TOE が動作する CA サーバマシン、管理端末マシンに、TOE の動作を干渉するようなソフトウェアがインストールされないように、適切に管理しなければならない。
・CA 管理者は、TOE 及び TOE の IT 環境が正常な動作を維持するように、適切に管理しなければならない。
・ファイアウォールの設定は、適切に維持・管理されなければならない。

OM.ACCOUNT_MGT (アカウントの管理)

CA 管理者は、保護対象資産を不正に改竄または削除されないよう、TOE が動作する OS 及び DB のアカウントを適切に管理しなければならない。

OM.PASSWORD_MGT (パスワードの管理)

ECS 利用者は、自分自身のパスワードを記憶し、他人に漏らしてはならない。また、ECS Set のガイダンス文書に従って、適切なパスワードを設定し、適切な頻度でパスワードを変更しなければならない。

OM.CA_ADMIN (CA 管理手順)

・CA 管理者は、ECS Set のガイダンス文書が定める手順に従って、TOE 及び TOE の IT 環境の管理業務を行わなければならない。
・CA 管理者は、認証局の運用管理に対する知識を有する者が担当しなければならない。
・CA 管理者は、ECS Set のガイダンス文書にて指定された以外の手段で、TOE の構成を変更してはならない。
・CA 管理者は、他の役職を兼務してはならない。

OM.OPERATION (運用手順)

・運用者は、ECS Set のガイダンス文書が定める手順に従って、TOE の運用業務を行わなければならない。
・運用者は、他の役職を兼務してはならない。

OM.AUDIT (監査手順)

・監査者は、ECS Set のガイダンス文書が定める手順に従って、TOE の監査業務を行わなけれ

ばならない。

・監査者は、他の役職を兼務してはならない。

OM.PERSONNEL (認証局に属する者の管理)

認証局を運用する組織の管理者は、認証局の運用を妨害するような、特殊な機器を持ち込んだ攻撃や、管理端末マシンへの攻撃などの悪質な攻撃が行われないよう、認証局に属する者を適切に管理しなければならない。

5. IT セキュリティ要件

本章では、セキュリティ要件の許可された機能コンポーネントの割付及び選択に関する操作部分を 下線かつ太字 で示す。また、”＜”、”＞”及び”(”、”)”で囲まれた部分は、割付の内容を示す。

詳細化に関する操作部分は *斜体かつ下線* で示す。繰返しに関しては、コンポーネント及びエレメントに対してアルファベットを付与して記述する。

5.1. TOE セキュリティ機能要件

5.1.1. セキュリティ監査

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**指定なし**レベルのすべての監査対象事象； 及び

c) **上記以外の個別に定義した監査対象事象**。

＜個別に定義した監査対象事象＞

なし

本節であげる各機能要件を選択した場合に、CC Part2 で規定された、監査対象とすべきアクションを以下に示す。また、TOE で監査対象事象としているアクションを下線で示す。

機能要件	監査対象とすべきアクション
セキュリティ監査	
FAU_GEN.1	監査対象とすべき識別されたアクションはない。
FAU_GEN.2	監査対象とすべき識別されたアクションはない。
FAU_SAR.1	基本: 監査記録からの情報の読み出し。
FAU_SAR.2	基本: 監査記録からの成功しなかった情報読み出し。
FAU_STG.1	監査対象とすべき識別されたアクションはない。
FAU_STG.4	基本: 監査格納失敗によってとられるアクション。
暗号サポート	
FCS_CKM.1a	最小: 動作の成功と失敗。 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。
FCS_CKM.1b	
FCS_CKM.1c	
FCS_COP.1a	最小: 成功と失敗及び暗号操作の種別。 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
FCS_COP.1b	

FCS_COP.1c	属性。
FCS_COP.1d	
FCS_CKM.2b	最小: 動作の成功と失敗。 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。
利用者データ保護	
FDP_ACC.1	監査対象にすべき識別された事象はない。
FDP_ACF.1	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。 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。 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。
識別と認証	
FIA_AFL.1	最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション（例えば端末の停止）、もし適切であれば、正常状態への復帰（例えば端末の再稼動）。
FIA_ATD.1	監査対象にすべき識別されたアクションはない。
FIA_SOS.1	最小: TSF による、テストされた秘密の拒否; 基本: TSF による、テストされた秘密の拒否または受け入れ; 詳細: 定義された品質尺度に対する変更の識別。
FIA_UAU.1	最小: 認証メカニズムの不成功になった使用; 基本: 認証メカニズムのすべての使用。 詳細: 利用者認証以前に行われたすべての TSF 調停アクション
FIA_UID.1	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; 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。
FIA_USB.1	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）。 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）。
セキュリティ管理	
FMT_MOF.1	基本: TSF の機能のふるまいにおけるすべての改変。
FMT_MSA.1a **FMT_MSA.1b** **FMT_MSA.1c** **FMT_MSA.1d**	基本: セキュリティ属性の値の改変すべて。
FMT_MSA.2c	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; 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。
FMT_MSA.3	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。

	基本: セキュリティ属性の初期値の改変すべて。
FMT_MTD.1a **FMT_MTD.1b**	基本: TSF データの値のすべての改変。
FMT_SMR.1	最小: 役割の一部をなす利用者のグループに対する改変; 詳細: 役割の権限の使用すべて。
FMT_SMF.1	最小: 管理機能の使用
TSF の保護	
FPT_RVM.1	監査対象にすべき識別されたアクションはない。
FPT_SEP.1	監査対象にすべき識別されたアクションはない。
FPT_STM.1	最小: 時間の変更; 詳細: タイムスタンプの提供

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗）；及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、**以下の監査関連情報**。

＜監査関連情報＞

- 事象の通番
- 事象が発生した TOE のモジュール名
- 各事象固有の情報
- メッセージの識別情報

依存性：FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.2 利用者識別情報の関連付け

下位階層：なし

FAU_GEN.2.1 TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性：FAU_GEN.1 監査データ生成

FIA_UID.1 識別のタイミング

FAU_SAR.1 監査レビュー

下位階層：なし

FAU_SAR.1.1 TSF は、**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、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性：FAU_GEN.1 監査データ生成

FAU_SAR.2 限定監査レビュー

下位階層：なし

FAU_SAR.2.1 TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

依存性：FAU_SAR.1 監査レビュー

FAU_STG.1 保護された監査証跡格納

下位階層：なし

FAU_STG.1.1 TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査記録の改変を**検出**できねばならない。

依存性：FAU_GEN.1 監査データ生成

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、**監査対象事象の無視**、及び **CA サーバの停止、OS への下記の事象の出力**を行わねばならない。

＜OS に出力する事象＞

- 監査ログの出力に失敗した事象。
- CA サーバを停止した事象。

依存性：FAU_STG.1 保護された監査証跡格納

5.1.2. **暗号サポート**

暗号サポートの機能要件に関して、以下の 4 つに分けて繰返しを適用する。

a) DB の暗号化
b) 通信路の暗号化
c) 監査ログの署名・暗号化
d) 秘密情報格納ディレクトリの暗号化

【DB の暗号化】

FCS_CKM.1a　暗号鍵生成

下位階層：なし

FCS_CKM.1.1a　TSF は、以下の**暗号鍵生成に関する標準**に合致する、指定された暗号鍵生成アルゴリズム（**鍵生成アルゴリズム**）と指定された暗号鍵長（**鍵長**）に従って、暗号鍵を生成しなければならない。

＜暗号鍵生成に関する標準＞

暗号鍵名称	標準	鍵生成アルゴリズム	鍵長
DB データ暗号鍵	ISO/IEC 9979/0009	MULTI2	256 bit

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_COP.1a　暗号操作

下位階層：なし

FCS_COP.1.1a　TSF は、**以下の暗号操作に関する標準**に合致する、特定された暗号アルゴリズム（**暗号アルゴリズム**）と暗号鍵長（**鍵長**）に従って、**暗号操作**を実行しなければならない。

＜暗号操作に関する標準＞

暗号操作名称	標準	暗号アルゴリズム	鍵長
DB データ暗号化／復号化	ISO/IEC 9979/0009	MULTI2	256 bit
ECS 利用者パスワード格納で使用するハッシュ	FIPS 180-1	SHA-1	----

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

【通信路の暗号化】

FCS_CKM.1b　暗号鍵生成

下位階層：なし

FCS_CKM.1.1b　TSF は、以下の**暗号鍵生成に関する標準**に合致する、指定された暗号鍵生成アルゴリズム（**鍵生成アルゴリズム**）と指定された暗号鍵長（**鍵長**）に従って、暗号鍵を生成しなければならない。

＜暗号鍵生成に関する標準＞

暗号鍵名称	標準	鍵生成アルゴリズム	鍵長
通信路暗号鍵	ISO/IEC 9979/0009	MULTI2	256 bit
通信路公開鍵／秘密鍵	PKCS#1	RSA	1024 bit

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.2b　暗号鍵配付

下位階層：なし

FCS_CKM.2.1b　TSF は、以下の**暗号鍵配付方法に関する標準**に合致する、指定された暗号鍵配付方法（**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。

＜暗号鍵配付方法に関する標準＞

暗号鍵名称	標準	鍵配付方法
通信路暗号鍵	ISO/IEC 9798	ISO/IEC 9798 通信路暗号鍵の共有

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.1b 暗号操作

下位階層：なし

FCS_COP.1.1b TSF は、**以下の暗号操作に関する標準**に合致する、特定された暗号アルゴリズム（**暗号アルゴリズム**）と暗号鍵長（**鍵長**）に従って、**暗号操作**を実行しなければならない。

＜暗号操作に関する標準＞

暗号操作名称	標準	暗号アルゴリズム	鍵長
通信路暗号化／復号化	ISO/IEC 9979/0009	MULTI2	256 bit
通信路暗号鍵の暗号化	PKCS#1	RSA	1024 bit

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

【監査ログの署名・暗号化】

FCS_CKM.1c 暗号鍵生成

下位階層：なし

FCS_CKM.1.1c TSF は、以下の**暗号鍵生成に関する標準**に合致する、指定された暗号鍵生成アルゴリズム（**鍵生成アルゴリズム**）と指定された暗号鍵長（**鍵長**）に従って、暗号鍵を生成しなければならない。

＜暗号鍵生成に関する標準＞

暗号鍵名称	標準	鍵生成アルゴリズム	鍵長
監査ログ暗号鍵	FIPS 46-3	Triple-DES	168 bit
監査ログ署名公開鍵／秘密鍵	PKCS#1	RSA	512 bit

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_COP.1c　暗号操作

下位階層：なし

FCS_COP.1.1c　TSF は、**以下の暗号操作に関する標準**に合致する、特定された暗号アルゴリズム（**暗号アルゴリズム**）と暗号鍵長（**鍵長**）に従って、**暗号操作**を実行しなければならない。

＜暗号操作に関する標準＞

暗号操作名称	標準	暗号アルゴリズム	鍵長
監査ログ署名／検定	PKCS#7	RSA	512 bit
監査ログ暗号化／復号化	FIPS 46-3	Triple-DES	168 bit
監査ログ署名で使用するハッシュ	FIPS 180-1	SHA-1	----

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

【秘密情報格納ディレクトリの暗号化】

FCS_COP.1d　暗号操作

下位階層：なし

FCS_COP.1.1d　TSF は、**以下の暗号操作に関する標準**に合致する、特定された暗号アルゴリズム（**暗号アルゴリズム**）と暗号鍵長（**鍵長**）に従って、**暗号操作**を実行しなければならない。

＜暗号操作に関する標準＞

暗号操作名称	標準	暗号アルゴリズム	鍵長
秘密情報暗号化／復号化	FIPS 46-2	DES	56 bit
秘密情報暗号鍵暗号化／復号化	PKCS#5	PBE	64 bit

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

5.1.3. 利用者データ保護

FDP_ACC.1　サブセットアクセス制御

下位階層：なし

FDP_ACC.1.1　TSF は、**以下のサブジェクト、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 **ECS 利用者データアクセス制御 SFP** を実施しなければならない。

＜サブジェクト＞

- ECS 利用者の代行スレッド

＜オブジェクト＞

- EE 証明書 オブジェクト
- PKCS#12 データ オブジェクト
- PKCS#12 パスワード オブジェクト
- CRL オブジェクト
- CRL 発行定義文 オブジェクト

＜サブジェクトーオブジェクト間操作＞

- 作成
- 削除
- 読み出し
- 改変

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1　セキュリティ属性によるアクセス制御

下位階層：なし

FDP_ACF.1.1　TSF は、**権限及び合議人数**に基づいて、オブジェクトに対して、**ECS 利用者データアクセス制御 SFP** を実施しなければならない。

FDP_ACF.1.2　TSF は、制御されたサブジェクトと制御されたオブジェクト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。**制御されたサブジェクトと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以下の規則**

＜制御されたサブジェクトと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	制御された操作	制御されたオブジェクト

EE 証明書検索権限を持つ ECS 利用者の代行スレッド	読み出し	EE 証明書 オブジェクト
EE 証明書削除権限を持つ ECS 利用者の代行スレッド	削除	合議状態が成立した EE 証明書 オブジェクト
EE 証明書失効権限を持つ ECS 利用者の代行スレッド	改変	合議状態が成立した EE 証明書 オブジェクト
EE 証明書取得権限を持つ ECS 利用者の代行スレッド	読み出し	EE 証明書 オブジェクト
PKCS#12 データ作成権限を持つ ECS 利用者の代行スレッド	作成	合議状態が成立した以下のオブジェクト ・EE 証明書 オブジェクト ・PKCS#12 データ オブジェクト ・PKCS#12 パスワード オブジェクト
PKCS#12 データ取得権限を持つ ECS 利用者の代行スレッド	読み出し	PKCS#12 データ オブジェクト
PKCS#12 パスワード取得権限を持つ ECS 利用者の代行スレッド	読み出し	PKCS#12 パスワード オブジェクト
CRL 定義文登録権限を持つ ECS 利用者の代行スレッド	作成／改変	合議状態が成立した CRL 発行定義文 オブジェクト
CRL 定義文削除権限を持つ ECS 利用者の代行スレッド	削除	合議状態が成立した CRL 発行定義文 オブジェクト
CRL 作成権限を持つ ECS 利用者の代行スレッド	作成／改変	合議状態が成立した CRL オブジェクト
CRL 検索権限を持つ ECS 利用者の代行スレッド	読み出し	CRL オブジェクト
CRL 削除権限を持つ ECS 利用者の代行スレッド	削除	合議状態が成立した CRL オブジェクト
CRL 取得権限を持つ ECS 利用者の代行スレッド	読み出し	CRL オブジェクト

(凡例)：
上記規則では、TSF は、制御されたサブジェクト（例：EE 証明書検索権限を持つ ECS 利用者の代行スレッド）が、制御されたオブジェクト（例：EE 証明書 オブジェクト）に対して、制御された操作（例：読み出し）を許可することを示している。

FDP_ACF.1.3 TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない。

＜アクセスを明示的に承認する追加規則＞
なし

FDP_ACF.1.4 TSF は、**以下の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追加規則**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。

＜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追加規則＞
なし

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

5.1.4. 識別と認証

FIA_AFL.1 認証失敗時の取り扱い

下位階層：なし

FIA_AFL.1.1 TSF は、管理端末からの接続における認証に関して、1回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、以下のアクションをしなければならない。

＜アクション＞

- 当該コネクションの切断
- 監査ログへのイベントの出力
- 10 秒間の再認証試行拒否

依存性：FIA_UAU.1 認証のタイミング

FIA_ATD.1 利用者属性定義

下位階層：なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト（セキュリティ属性のリスト）を維持しなければならない。

＜セキュリティ属性のリスト＞

- ECS 利用者 ID
- ECS 利用者パスワード
- ECS 利用者権限リスト

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、秘密が以下の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。

＜定義された品質尺度＞

アカウントの種類	秘密	品質尺度
ECS 利用者パスワード	パスワード	長さ：8～64 文字

		使用可能な文字：半角英数字または半角記号 必要な文字： 半角大文字英字、半角小文字英字、半角数字及び半角記号

依存性：なし

FIA_UAU.1　　認証のタイミング

下位階層：なし

FIA_UAU.1.1　TSF は、利用者が認証される前に利用者を代行して行われる**暗号化通信路の使用**を許可しなければならない。

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

依存性：FIA_UID.1 識別のタイミング

FIA_UID.1　　識別のタイミング

下位階層：なし

FIA_UID.1.1　TSF は、利用者が識別される前に利用者を代行して実行される**暗号化通信路の使用**を許可しなければならない。

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

依存性：なし

FIA_USB.1　　利用者･サブジェクト結合

下位階層：なし

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

依存性：FIA_ATD.1 利用者属性定義

5.1.5. セキュリティ管理

FMT_MOF.1　セキュリティ機能のふるまいの管理

下位階層：なし

FMT_MOF.1.1　TSF は、**合議機能、DB 暗号化機能、監査ログ署名機能、監査ログ暗号化機能を動作／停止する**能力を**規定の合議人数に達した CA 管理者**に制限しなければならない。

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

FMT_MSA.1a　セキュリティ属性の管理

下位階層：なし

FMT_MSA.1.1a　TSF は、セキュリティ属性（**各サブジェクトに対する以下のセキュリティ属性**）に対し**作成、削除**をする能力を**規定の合議人数に達した CA 管理者**に制限するために **ECS 利用者データアクセス制御 SFP** を実施しなければならない。

＜各サブジェクトに対するセキュリティ属性＞

- ECS 利用者 ID
- ECS 利用者パスワード
- ECS 利用者権限リスト

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

FMT_MSA.1b　セキュリティ属性の管理

下位階層：なし

FMT_MSA.1.1b　TSF は、セキュリティ属性（**各サブジェクトに対する ECS 利用者パスワードのうち、自分自身のもの**）に対し**改変**する能力を **CA 管理者、監査者、運用者**に制限するために **ECS 利用者データアクセス制御 SFP** を実施しなければならない。

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

FMT_MSA.1c　セキュリティ属性の管理

下位階層：なし

FMT_MSA.1.1c　TSF は、セキュリティ属性（**各サブジェクトに対する ECS 利用者権限リスト**）に対し**改変**をする能力を**規定の合議人数に達した CA 管理者**に制限するために**ECS 利用者データアクセス制御 SFP** を実施しなければならない。

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

FMT_MSA.1d　セキュリティ属性の管理

下位階層：なし

FMT_MSA.1.1d　TSF は、セキュリティ属性（**各オブジェクトに対する以下のセキュリティ属性**）に対し**改変、クリア**をする能力を**運用者**に制限するために **ECS 利用者データアクセス制御 SFP** を実施しなければならない。

＜各オブジェクトに対するセキュリティ属性＞

- 操作種別
- 操作要求者と合議者の ECS 利用者 ID
- 操作に必要な残りの合議人数

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

【監査ログの署名】

FMT_MSA.2c　セキュアなセキュリティ属性

下位階層：なし

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

依存性：ADV_SPM.1 非形式的 TOE セキュリティ方針モデル
　　[FDP_ACC.1 サブセットアクセス制御

または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

FMT_MSA.3 静的属性初期化

下位階層：なし

FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性として、許可的デフォルト値を与える **ECS 利用者データアクセス制御 SFP** を実施しなければならない。

FMT_MSA.3.2 TSF は、オブジェクトや情報が生成されるとき、**規定の合議人数に達した CA 管理者**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。

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

FMT_MTD.1a TSF データの管理

下位階層：なし

FMT_MTD.1.1a TSF は、**監査ログ用証明書の設定、合議人数の設定**を**問い合わせ、改変**する能力を**規定の合議人数に達した CA 管理者**に制限しなければならない。

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

FMT_MTD.1b TSF データの管理

下位階層：なし

FMT_MTD.1.1b TSF は、**監査ログ**を**問い合わせ、削除、取得**する能力を**監査者**に制限しなければならない。

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

FMT_SMR.1 セキュリティ役割

下位階層:なし

FMT_SMR.1.1 TSF は、役割（**以下の役割**）を維持しなければならない。

＜役割＞

- CA 管理者
- 監査者
- 運用者

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

FMT_SMF.1 管理機能の特定
下位階層：なし
FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：

本節であげる各機能要件を選択した場合に、CC Part2 で規定された、管理対象とすべきアクティビティを以下に示す。また、TOE でセキュリティ管理機能を持つアクティビティを下線で示す。

機能要件	管理アクティビティ
セキュリティ監査	
FAU_GEN.1	予見される管理アクティビティはない。
FAU_GEN.2	予見される管理アクティビティはない。
FAU_SAR.1	監査記録に対して読み出し権のある利用者グループの維持（削除、改変、追加）。
FAU_SAR.2	予見される管理アクティビティはない。
FAU_STG.1	予見される管理アクティビティはない。
FAU_STG.4	監査格納失敗時にとられるアクションの維持（削除、改変、追加）。
暗号サポート	
FCS_CKM.1a **FCS_CKM.1b** **FCS_CKM.1c**	暗号鍵属性の変更の管理。
FCS_COP.1a **FCS_COP.1b** **FCS_COP.1c** **FCS_COP.1d**	予見される管理アクティビティはない。
FCS_CKM.2b	暗号鍵属性の変更の管理。
利用者データ保護	
FDP_ACC.1	予見される管理アクティビティはない。
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。
識別と認証	
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。

FIA_SOS.1	秘密の検証に使用される尺度の管理。
FIA_UAU.1	a) 管理者による認証データの管理; b) 関係する利用者による認証データの管理; c) 利用者が認証される前にとられるアクションのリストを管理すること。
FIA_UID.1	a) 利用者識別情報の管理; b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。
FIA_USB.1	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。
セキュリティ管理	
FMT_MOF.1	TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること。
FMT_MSA.1a **FMT_MSA.1b** **FMT_MSA.1c** **FMT_MSA.1d**	セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。
FMT_MSA.2c	予見される管理アクティビティはない。
FMT_MSA.3	a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。
FMT_MTD.1a **FMT_MTD.1b**	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。
FMT_SMR.1	役割の一部をなす利用者のグループの管理。
FMT_SMF.1	予見される管理アクティビティはない。
TSF の保護	
FPT_RVM.1	予見される管理アクティビティはない。
FPT_SEP.1	予見される管理アクティビティはない。
FPT_STM.1	a) 時間の管理

依存性：なし

5.1.6. TSF の保護

FPT_RVM.1 TSP の非バイパス性

下位階層：なし

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

依存性：なし

FPT_SEP.1 TSF ドメイン分離

下位階層：なし

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

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

依存性：なし

FPT_STM.1 高信頼タイムスタンプ

下位階層：なし

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

依存性：なし

5.2. IT 環境に対するセキュリティ機能要件

5.2.1. 暗号サポート

IT 環境における暗号サポートの機能要件に関して、以下の繰返しを適用する。

e) CA 署名とその検定

【CA 署名とその検定】

FCS_CKM.1e　暗号鍵生成

下位階層：なし

FCS_CKM.1.1e　*TSF*は、以下の**暗号鍵生成に関する標準**に合致する、指定された暗号鍵生成アルゴリズム（**鍵生成アルゴリズム**）と指定された暗号鍵長（**鍵長**）に従って、暗号鍵を生成しなければならない。

＜暗号鍵生成に関する標準＞

暗号鍵名称	標準	鍵生成アルゴリズム	鍵長
CA 公開鍵／秘密鍵	PKCS#1	RSA	512/1024/2048 bit

適用上の注釈：

- 上記要件において、*TSF* は、HSM の機能を示す。

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.4e　暗号鍵破棄

下位階層：なし

FCS_CKM.4.1e　*TSF*は、以下の**暗号鍵破棄方法に関する標準**に合致する、指定された暗号鍵破棄方法（**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。

＜暗号鍵破棄に関する標準＞

暗号鍵名称	標準	鍵破棄方法
CA 秘密鍵	FIPS 140-2	FIPS 140-2 level3 準拠

適用上の注釈：

- 上記要件において、***TSF*** は、HSM の機能を示す。
- CA 秘密鍵は、作成から破棄までの全てのライフサイクルにおいて、FIPS 140-2 level3 準拠の HSM 内で操作される。

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

FCS_COP.1e 暗号操作

下位階層：なし

FCS_COP.1.1e ***TSF*** は、**以下の暗号操作に関する標準**に合致する、特定された暗号アルゴリズム（**暗号アルゴリズム**）と暗号鍵長（**鍵長**）に従って、**暗号操作**を実行しなければならない。

＜暗号操作に関する標準＞

暗号操作名称	標準	暗号アルゴリズム	鍵長
署名／検定	PKCS#7	RSA	512/1024/2048 bit
CA 署名で使用するハッシュ	FIPS 180-1	SHA-1	----

適用上の注釈：

- 上記要件において、***TSF*** は、HSM の機能を示す。

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

5.2.2. セキュリティ管理

【CA 署名とその検定】

FMT_MSA.2e セキュアなセキュリティ属性

下位階層：なし

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

適用上の注釈：

- 上記要件において、***TSF*** は、HSM の機能を示す。

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

5.3. セキュリティ機能強度の指定

本 TOE の最小機能強度レベルは、**SOF**-基本である。

5.4. TOE セキュリティ保証要件

5.4.1. 評価保証レベル

評価保証レベルは「Common Criteria for Information Technology Security Evaluation, Ver. 2.1, Part 3- Security assurance requirements (August 1999, CCIMB-99-033) 」で規定された EAL3 を適用する。

5.4.2. 基本コンポーネント

EAL3 の基本コンポーネントを表 2 に示す。

表 2： EAL3 基本コンポーネント一覧

保証クラス	保証コンポーネント	
ACM (機成管理)	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOE の CM 範囲
ADO (配付と運用)	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
ADV (開発)	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_RCR.1	非形式的対応の実証
AGD (ガイダンス文書)	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ALC (ライフサイクル サポート)	ALC_DVS.1	セキュリティ手段の識別
ATE (テスト)	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト:上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
AVA (脆弱性評定)	AVA_MSU.1	ガイダンスの検査
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.4.3. 追加コンポーネント

本 ST で追加する保証コンポーネントはない。

6. TOE 要約仕様

6.1. TOE セキュリティ機能

TOE のセキュリティ機能要件と TOE のセキュリティ機能の対応を表 3 に示す。

表 3： TOE セキュリティ機能要件と TOE セキュリティ機能の対応表

TOE セキュリティ機能 / TOE セキュリティ機能要件	SF.AUDIT	SF.CRYPTO	SF.AC	SF.I&A	SF.CA_MGT
FAU_GEN.1	○				
FAU_GEN.2	○				
FAU_SAR.1	○				
FAU_SAR.2	○				
FAU_STG.1	○	○			
FAU_STG.4	○				
FCS_CKM.1a		○			
FCS_COP.1a		○			
FCS_CKM.1b		○			
FCS_CKM.2b		○			
FCS_COP.1b		○			
FCS_CKM.1c		○			
FCS_COP.1c		○			
FCS_COP.1d		○			
FDP_ACC.1			○		
FDP_ACF.1			○		
FIA_AFL.1				○	
FIA_ATD.1					○
FIA_SOS.1					○
FIA_UAU.1				○	
FIA_UID.1				○	
FIA_USB.1			○		
FMT_MOF.1					○

FMT_MSA.1a					○
FMT_MSA.1b					○
FMT_MSA.1c					○
FMT_MSA.1d			○		
FMT_MSA.2c		○			
FMT_MSA.3					○
FMT_MTD.1a					○
FMT_MTD.1b	○				
FMT_SMR.1					○
FMT_SMF.1					○
FPT_RVM.1			○	○	
FPT_SEP.1	○	○	○	○	○
FPT_STM.1	○				

6.1.1. **監査機能（SF.AUDIT）**

(監査ログ生成)

TOE は、監査の対象となる事象が発生した場合に、当該事象を監査ログとして記録する。
TOE は、監査ログに以下の監査情報を記録する。

項目	説明
通番	監査事象毎に割り振られる 6 桁の 10 進数の通番
日付／時刻	事象が発生した年月日 時分秒を示すタイムスタンプ情報
モジュール名	当該事象が発生したモジュール名またはコマンド名
ユーザ名	発生事象に関連する操作を行った ECS 利用者 ID
事象種別	発生事象の種別（標準：INFO、警告：WARN、エラー：ERR）
LogID	発生事象を示すメッセージにつけられている 4 桁の 16 進数の識別情報
メッセージ	LogID に対応した当該事象のメッセージ
拡張情報	メッセージ毎に固有なコード、ステータスなどの補足情報。なお、この情報は、メッセージ内に埋め込まれて記録される。

TOE は、監査ログに必要なタイムスタンプを OS から取得し、提供する。

TOE は、監査ログのサブジェクト識別情報として、ECS 利用者 ID を記録する。

TOE は、発生事象の成功及び失敗を、メッセージの内容に記述する。当該事象の成功及び失敗は、

LogID が異なるため、LogID で識別することが可能である。さらに、発生事象が失敗の場合、TOE は、事象種別の項目を警告（WARN）またはエラー（ERR）として記録する。

TOE は、以下の事象が発生した際に、監査ログを記録する。

表 4： TOE が記録する監査対象事象

#	監査対象事象
1	監査ログの表示要求／表示成功／表示失敗
2	監査ログの削除要求／削除成功／削除失敗
3	CA サーバの起動／停止
4	EE 証明書の検索要求／検索成功
5	EE 証明書の削除要求／削除成功
6	EE 証明書の失効要求／失効成功
7	EE 証明書の取得要求／取得成功
8	PKCS#12 データの作成要求／作成成功
9	PKCS#12 データの取得要求／取得成功
10	PKCS#12 パスワードの取得要求／取得成功
11	CRL 発行定義文の登録要求／登録成功
12	CRL 発行定義文の削除要求／削除成功
13	CRL の発行要求／発行成功
14	CRL の検索要求／検索成功
15	CRL の削除要求／削除成功
16	CRL の取得要求／取得成功
17	合議承認／合議否認
18	ECS 利用者が権限外の操作を行った場合のエラー
19	ECS 利用者のログインの要求／成功／失敗
20	ECS 利用者パスワードの品質尺度不正
21	サブジェクト代行スレッドの生成失敗
22	CA 設定情報の設定／変更
23	ECS 利用者情報の追加／削除／変更
24	エラーイベント（エラー内容）

適用上の注釈：

- 監査ログの記録機能は、CA サーバの起動とともに開始し、CA サーバの停止とともに終了

する。

(監査ログ保護)

TOE は、監査ログに対して署名を付与し、暗号化して格納する。
署名・暗号化には、**SF.CRYPTO** に示す暗号方式を使用する。

TOE は、監査ログを読み出す際に、監査ログの検定・復号化を行う。
検定を行うことにより、監査ログの改竄を検出することができる。
検定・復号化には **SF.CRYPTO** に示す暗号方式を使用する。

監査ログは、監査者だけが参照及び削除することができる。

TOE は、CA サーバマシンのディスク容量不足により、監査ログファイルが出力できない場合、CA サーバを停止し、以下の事象を OS に出力する。

- 監査ログの出力に失敗した事象。
- CA サーバを停止した事象。

(監査ログ表示)

TOE は、監査者だけに対して、管理端末から監査ログを参照する機能を提供する。
監査ログの参照に先立って、TOE は、監査者だけに対して、署名・暗号化された監査ログファイルのリストを表示する。
監査者が、提示された監査ログファイルのリストから監査ログファイルを選択することによって、TOE は、当該監査ログを表示する。
監査ログの表示に際して、記録した情報を 日付と時刻順に表形式で表示する。

また、TOE は、監査者だけに対して、管理端末から監査ログを署名つきのファイル形式で取得する機能を提供する。

6.1.2. 暗号機能（SF.CRYPTO）

（秘密情報格納ディレクトリ暗号化）

TOE は、DB データ暗号鍵や、CA サーバ起動時に必要な設定情報などを暴露から保護するために、暗号化された格納領域である秘密情報格納ディレクトリを使用する。
TOE は、以下の情報を秘密情報格納ディレクトリに格納する。

- CA 設定情報
- DB データ暗号鍵
- 監査ログ用証明書
- 監査ログ用秘密鍵

TOE は、PBE（PKCS#5）暗号アルゴリズムに従って、秘密情報暗号鍵を ECS 起動パスワードで暗号化／復号化する機能を提供する。
適用上の注釈：

- ECS 起動パスワードは CA サーバ起動時に CA 管理者が入力する。

TOE は、DES（FIPS 46-2）暗号アルゴリズムに従って、秘密情報格納ディレクトリ内のデータを秘密情報暗号鍵で暗号化／復号化する機能を提供する。

TOE は、秘密情報格納ディレクトリにデータが格納される時、データを暗号化する。また、データが取り出される時、データを復号化する。

（監査ログ署名／暗号化）

TOE は、監査ログを暴露／改竄から保護するために、監査ログに署名を付与し、暗号化する機能を提供する。

TOE は、監査ログ暗号化のために、Triple-DES（FIPS 46-3）暗号アルゴリズムに従って、鍵長 168bit の監査ログ暗号鍵（共通鍵）を生成する。
適用上の注釈：

- 監査ログ暗号鍵は、**SF.AUDIT** で示した監査ログを暗号化する際に生成され、監査ログファイル内に、RSA（PKCS#7）暗号アルゴリズムに従って埋め込まれる。

TOE は、監査ログに署名を付与するために、RSA（PKCS#1）暗号アルゴリズムに従って、鍵長 512bit の監査ログ署名公開鍵／秘密鍵（鍵ペア）を生成する。
生成された監査ログ署名公開鍵は、監査ログ用証明書として秘密情報格納ディレクトリに格納される。

生成された監査ログ署名秘密鍵は、監査ログ用秘密鍵として秘密情報格納ディレクトリに格納される。
適用上の注釈：

- 監査ログ用証明書／監査ログ用秘密鍵は、TOE の運用開始時に生成される。

TOE は、監査ログ暗号鍵、監査ログ署名公開鍵／秘密鍵を使用して対象となる監査ログを暗号化／復号化、署名／検定する機能を提供する。
TOE は、署名／検定に使用するハッシュとして SHA-1（FIPS180-1）を使用する。

TOE は、監査ログ署名秘密鍵を使用する前に、対応する監査ログ用証明書の有効期限を確認し、有効期限切れの場合、事象を OS に出力する。

(DB 暗号化)

TOE は、データベースに格納するデータのうち、以下に示す暴露から保護すべきデータを暗号化する。

- PKCS#12 データ
- PKCS#12 パスワード

TOE は、PKCS#12 データ及び PKCS#12 パスワードの暗号化のために、MULTI2（ISO/IEC 9979/0009）暗号アルゴリズムに従った、鍵長 256bit の DB データ暗号鍵（共通鍵）を生成する。
生成された DB データ暗号鍵は、秘密情報格納ディレクトリに格納する。
適用上の注釈：

- DB データ暗号鍵は、TOE 生成時にシステム構築者によって生成される。

TOE は、DB データ暗号鍵を使用して対象となるデータを暗号化／復号化する機能を提供する。

また TOE は、データベースに格納するデータのうち、以下に示す暴露から保護すべきデータをハッシュ変換する。

- ECS 利用者パスワード

TOE は、ECS 利用者パスワード格納で使用するハッシュとして SHA-1（FIPS180-1）を使用する。

(通信路暗号化)

TOE は、管理端末と CA サーバの間の通信路を流れるデータを暗号化する。

TOE は、管理端末と CA サーバの間の通信路を暗号化するために、MULTI2（ISO/IEC 9979/0009）

暗号アルゴリズムに従った、鍵長 256bit の通信路暗号鍵（共通鍵）を生成する。

TOE は、CA サーバと管理端末の間で通信路暗号鍵を共有するために、RSA（PKCS#1）暗号アルゴリズムに従った、鍵長 1024bit の通信路公開鍵／秘密鍵（鍵ペア）を生成する。

TOE は、CA サーバと管理端末の間で通信路暗号鍵を共有するために、通信路公開鍵／秘密鍵を使用し、標準：ISO/IEC 9798 に従って、通信路暗号鍵の配付を行う。

TOE は、通信路暗号鍵を使用して通信路を流れるデータを暗号化／復号化する機能を提供する。

6.1.3. アクセス制御機能（SF.AC）

（アクセス制御）

TOE は、**SF.I&A** で示す識別・認証処理が終了した後、ECS 利用者を代行して動作するサブジェクトである代行スレッドに ECS 利用者 ID を関連付ける。

TOE は、代行スレッドに関連付けられた ECS 利用者 ID から、当該 ECS 利用者の ECS 利用者権限リストを取得する。
TOE は、代行スレッドがオブジェクトにアクセスする際に、代行スレッドが当該操作に対する ECS 利用者権限を持っているか、また合議が必要な操作に関しては、合議人数が規定された人数に達しているかを判定することにより、アクセス制御を実施する。このアクセス制御は、「ECS 利用者データアクセス制御 SFP」に従う。

TOE が提供する操作と TOE が実施する「ECS 利用者データアクセス制御 SFP」の一覧を以下に示す。

TOE が提供する操作	サブジェクト	操作	オブジェクト
EE 証明書検索	OT1	読み出し	EEC
EE 証明書削除	OT2	削除	GEEC
EE 証明書失効	OT3	改変	GEEC
EE 証明書取得	OT4	読み出し	EEC
PKCS#12 データ作成	OT5	作成	GEEC
			GP12D
			GP12P
PKCS#12 データ取得	OT6	読み出し	P12D
PKCS#12 パスワード取得	OT7	読み出し	P12P
CRL 定義文登録	OT8	作成／改変	GCRLD
CRL 定義文削除	OT9	削除	GCRLD
CRL 作成	OT10	作成／改変	GCRL
CRL 検索	OT11	読み出し	CRL
CRL 削除	OT12	削除	GCRL
CRL 取得	OT13	読み出し	CRL

（凡例）：
OT1：EE 証明書検索権限を持つ ECS 利用者の代行スレッド
OT2：EE 証明書削除権限を持つ ECS 利用者の代行スレッド

OT3：EE 証明書失効権限を持つ ECS 利用者の代行スレッド
OT4：EE 証明書取得権限を持つ ECS 利用者の代行スレッド
OT5：PKCS#12 データ作成権限を持つ ECS 利用者の代行スレッド
OT6：PKCS#12 データ取得権限を持つ ECS 利用者の代行スレッド
OT7：PKCS#12 パスワード取得権限を持つ ECS 利用者の代行スレッド
OT8：CRL 定義文登録権限を持つ ECS 利用者の代行スレッド
OT9：CRL 定義文削除権限を持つ ECS 利用者の代行スレッド
OT10：CRL 作成権限を持つ ECS 利用者の代行スレッド
OT11：CRL 検索権限を持つ ECS 利用者の代行スレッド
OT12：CRL 削除権限を持つ ECS 利用者の代行スレッド
OT13：CRL 取得権限を持つ ECS 利用者の代行スレッド

EEC：EE 証明書 オブジェクト
P12D：PKCS#12 データ オブジェクト
P12P：PKCS#12 パスワード オブジェクト
CRLD：CRL 発行定義文 オブジェクト
CRL：CRL オブジェクト
GEEC：合議状態が成立した EE 証明書 オブジェクト
GP12D：合議状態が成立した PKCS#12 データ オブジェクト
GP12P：合議状態が成立した PKCS#12 パスワード オブジェクト
GCRLD：合議状態が成立した CRL 発行定義文 オブジェクト
GCRL：合議状態が成立した CRL オブジェクト

適用上の注釈：

- ”TOE が提供する操作”とは、TOE が ECS 利用者に提供する”オブジェクト”に対する操作を示す。
- 上記「ECS 利用者データアクセス制御 SFP」では、”TOE が提供する操作”によって、”サブジェクト”が”オブジェクト”に対する”操作”が行われることを TOE が許可することを示す。
- EE 証明書及び PKCS#12 パスワードは、PKCS#12 データ作成操作によって作成される。

(運用操作合議)

TOE は、管理端末から行う操作に対して、あらかじめ規定された人数の、当該操作に対する権限を持つ複数の運用者による合議を要求する。以下の操作に対して、運用操作合議が必要である。

- EE 証明書削除

- EE 証明書失効
- PKCS#12 データ作成
- CRL 作成
- CRL 削除
- CRL 発行定義文登録
- CRL 発行定義文削除

当該操作に対する権限を持つ運用者に対して、TOE は、以下の操作要求、合議承認、合議否認の操作を受け付けることにより、運用操作合議を実施する。

操作要求 ：
TOE は、当該操作に対する権限を持つ運用者が操作要求を行うと、操作対象となるデータに対して、｛操作種別、操作要求者の ECS 利用者 ID、操作に必要な残りの合議人数｝から構成される管理情報を作成する。

合議承認 ：
TOE は、当該操作に対する権限を持つ運用者が合議承認を行うと、新規の合議者である場合に限り、操作対象となるデータに対して、{操作種別、操作要求者と合議者の ECS 利用者 ID、操作に必要な残りの合議人数｝の管理情報を更新する。
更新に際しては、合議者の ECS 利用者 ID を追記し、操作に必要な残りの合議人数を 1 減らす。

合議否認 ：
TOE は、当該操作に対する権限を持つ運用者が合議否認を行うと、新規の合議者である場合に限り、操作対象となるデータに対して、管理情報をリセットする。

上記合議承認操作を繰返し、操作に必要な残りの合議人数が 1 になった時点で、操作対象となるデータの合議状態が成立する。
TOE は、当該操作に対する権限を持つ運用者が、合議状態が成立したデータに対して合議承認を行うと、当該操作を実行し管理情報をリセットする。

6.1.4. **識別・認証機能（SF.I&A）**

TOE は、正当な ECS 利用者を確認するために、**SF.CA_MGT** によって TOE に登録した ECS 利用者 ID、ECS 利用者パスワードを利用する。

TOE は、管理端末を通じて CA サーバにログインを試みる利用者に対して、識別・認証を行い、識別・認証に成功した場合、正当な ECS 利用者として取り扱う。

TOE は、ECS 利用者の識別・認証が成功するまで、**SF.CRYPTO** の通信路暗号化以外のセキュリティ機能を使用しない。

TOE は、ECS 利用者の識別・認証のため、ECS 利用者 ID と ECS 利用者パスワードが、ECS 利用者情報と一致することの確認を行う。

TOE は、識別・認証に 1 回でも失敗した場合、管理端末と CA サーバの間の通信路のコネクションを切断し、当該事象を監査ログに出力する。また、認証の再試行を 10 秒間受け付けない。

6.1.5. CA 情報管理機能（SF.CA_MGT）

(CA 情報設定)

TOE は、CA 情報設定機能を使用して、CA 設定情報を表示及び設定することで、以下のセキュリティ機能を管理する機能を、規定の合議人数に達した CA 管理者に提供する。

- DB 暗号化の設定
  - ・ DB に格納するデータのうち、PKCS#12 データと PKCS#12 パスワードの暗号化を行うか行わないかを設定する。
- 監査ログ署名の設定
  - ・ 監査ログ用証明書を設定する場合、当該証明書を使用して監査ログに署名を付与する。
  - ・ 監査ログ用証明書を設定しない場合、監査ログに署名を付与しない。
- 監査ログ暗号化の設定
  - ・ 監査ログの暗号化を行うか行わないかを設定する。
- 合議情報の設定
  - ・ 合議を設定できる各操作に対して、合議機能を必須とするかしないかを設定する。
  - ・ 合議を設定できる各操作に対して、必要な合議者の人数を設定する。

TOE は、ECS 利用者 ID、ECS 利用者パスワード、ECS 利用者権限リストを設定することで、以下の ECS 利用者の管理機能を規定の合議人数に達した CA 管理者に提供する。

- ECS 利用者の登録
- ECS 利用者の削除
- ECS 利用者権限リストの改変

TOE は、ECS 利用者の登録の際、ECS 利用者パスワードとして以下の品質尺度を満たすことを検証するメカニズムを提供する

項目	品質尺度
長さ	8~64 文字
使用可能な文字	半角英数字または半角記号
必要な文字	半角大文字英字、半角小文字英字、半角数字及び半角記号

TOE は、上記品質尺度に満たない ECS 利用者パスワードは、許可しない。

TOE は、CA 情報設定権限を持つ ECS 利用者を CA 管理者という役割、監査権限を持つ ECS 利用者を監査者という役割、これら以外の ECS 利用者権限を持つ ECS 利用者を運用者という役割として維持する。

TOE は、ECS 利用者権限リストのすべての ECS 利用者権限が、権限ありとなるようにデフォルト

値を設定する。

CA 管理者のみが、CA 情報設定機能の起動を要求することができる。
CA 情報設定機能は、CA 情報設定合議が成功した後、使用することができる。
CA 情報設定合議が成功した後は、CA 情報設定機能を終了するまで、これを使用し続けることができる。

＜TOE をセキュアに運用するための管理に関する補足＞
CA 管理者は、以下に示す 本 ST で前提としている ”役職”と”ECS 利用者権限”に基づいて、ECS 利用者権限リストの設定を行った後、ECS 利用者の登録を終了しなければならない。

CA 管理者は、CA 設定情報を以下に示す値に維持する必要がある。

項目	設定値
DB 暗号化	暗号化を行う
監査ログ署名	署名を行う（監査ログ用証明書を設定する）
監査ログ暗号化	暗号化を行う
合議機能	必須とする
合議人数	

合議の必要な機能	合議人数
CA 情報設定機能	１人以上
EE 証明書削除機能	１人以上
EE 証明書失効機能	１人以上
PKCS#12 データ作成機能	１人以上
CRL 定義文登録機能	１人以上
CRL 定義文削除機能	１人以上
CRL 作成機能	１人以上
CRL 削除機能	１人以上

以下に ECS 利用者権限の一覧及び本 ST が前提としている ”役職”に対する ECS 利用者権限の設定値を以下に示す。CA 管理者は、以下に基づいて ECS 利用者権限を与えなければならない。

ECS 利用者権限	本 ST が想定する役職		
	CA 管理者	運用者	監査者
CA 情報設定権限	○	×	×

EE 証明書検索権限	×	○	×
EE 証明書削除権限	×	○	×
EE 証明書失効権限	×	○	×
EE 証明書取得権限	×	○	×
PKCS#12 データ作成権限	×	○	×
PKCS#12 データ取得権限	×	○	×
PKCS#12 パスワード取得権限	×	○	×
CRL 定義文登録権限	×	○	×
CRL 定義文削除権限	×	○	×
CRL 作成権限	×	○	×
CRL 検索権限	×	○	×
CRL 削除権限	×	○	×
CRL 取得権限	×	○	×
監査権限	×	×	○

（凡例）：
○：権限あり
×：権限なし（ECS 利用者権限の設定値として、これら以外の値はない）

(CA 情報設定合議)

TOE は、TOE のふるまいを決定する CA 情報設定機能に対して、あらかじめ規定された人数の、CA 管理者による合議を要求する。
CA 管理者からの CA 情報設定機能の起動要求に対して、TOE は、別の CA 管理者の識別・認証が成功することを要求する。
TOE は、あらかじめ規定された人数に達するまで、別々の CA 管理者の識別・認証が成功することを要求する。
TOE は、上記識別・認証の成功があらかじめ規定された人数に達して初めて、CA 情報設定機能を起動する。

適用上の注釈：
あらかじめ規定された合議人数が１人とは、1 人が起動要求を行い、1 人が合議した結果、2 人の同意の下に操作が行われることを示す。

(パスワード変更)

TOE は、ログインしている自分自身の ECS 利用者パスワードを変更する機能を CA 管理者、監査者、運用者に対して提供する。

TOE は、ECS 利用者パスワードの変更の際、ECS 利用者パスワードとして以下の品質尺度を満たすことを検証するメカニズムを提供する

項目	品質尺度
長さ	8~64 文字
使用可能な文字	半角英数字または半角記号
必要な文字	半角大文字英字、半角小文字英字、半角数字 及び半角記号

TOE は、上記品質尺度に満たない ECS 利用者パスワードは、許可しない。

6.2. セキュリティ機能強度

確率的かつ順列的メカニズムを使用したセキュリティ機能は、**SF.CA_MGT**、**SF.I&A** 及び **SF.CRYPTO** である。これらのセキュリティ機能のうち、**SF.CA_MGT**、**SF.I&A** で実現する ECS 利用者のパスワードに関する機能が、機能強度レベル **SOF**-基本を持つ。また、**SF.CRYPTO** のうち、ハッシュアルゴリズムを用いた暗号機能については、アルゴリズムとして 160bit の SHA-1 を使用しており、機能強度レベル **SOF**-基本を持つ。その他の **SF.CRYPTO** の暗号機能は、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、本機能強度レベルの対象としない。

6.3. 保証手段

本 ST で適用するセキュリティ保証要件とセキュリティの保証手段の対応を表 5 に示す。

本 ST で適用するセキュリティ保証手段として、以下に示すドキュメントを提供する。

表 5： セキュリティ保証要件（EAL3）とセキュリティ保証手段の対応表

セキュリティ保証要件 (EAL3)		セキュリティ保証手段
ACM (構成管理)	ACM_CAP.3	Enterprise Certificate Server Set 構成管理文書
	ACM_SCP.1	
ADO (配付と運用)	ADO_DEL.1	Enterprise Certificate Server Set 配付文書
	ADO_IGS.1	Enterprise Certificate Server Set システムセキュリティガイド
ADV (開発)	ADV_FSP.1	Enterprise Certificate Server Set 機能仕様書
	ADV_HLD.2	Enterprise Certificate Server Set 構造設計書
	ADV_RCR.1	Enterprise Certificate Server Set 対応分析書
AGD (ガイダンス文書)	AGD_ADM.1	Enterprise Certificate Server Set システムセキュリティガイド
	AGD_USR.1	本 TOE は、一般利用者は利用しないので、 利用者ガイダンスは提供しない。
ALC (ライフサイクルサポート)	ALC_DVS.1	Enterprise Certificate Server Set 開発セキュリティ規程書
ATE (テスト)	ATE_COV.2	Enterprise Certificate Server Set テスト分析書
	ATE_DPT.1	
	ATE_FUN.1	Enterprise Certificate Server Set テスト仕様書／報告書
	ATE_IND.2	Enterprise Certificate Server Set

AVA **(脆弱性評定)**	**AVA_MSU.1**	Enterprise Certificate Server Set システムセキュリティガイド
	AVA_SOF.1	Enterprise Certificate Server Set セキュリティ機能強度分析書
	AVA_VLA.1	Enterprise Certificate Server Set 脆弱性分析書

本 ST で適用する保証手段を以下に示す。

(1) Enterprise Certificate Server Set 構成管理文書

＜記述内容＞

- TOE のバージョン識別とバージョン命名規則
- TOE の構成要素リスト
- TOE の構成管理計画

(2) Enterprise Certificate Server Set 配付文書

＜記述内容＞

- TOE を利用者サイトへ配送するときのセキュリティを維持するために必要な手続き

(3) Enterprise Certificate Server Set システムセキュリティガイド

＜記述内容＞

- TOE のセキュアな設置・生成・立上げに必要な手順
- TOE の前提環境
- TOE 管理におけるセキュリティ上の注意事項
- 管理者が利用できる TOE のセキュリティ機能とインタフェース
- TOE のセキュアな管理方法

(4) Enterprise Certificate Server Set 機能仕様書

＜記述内容＞

- TOE セキュリティ機能の識別と仕様
- TSF インタフェースの識別と仕様

(5) Enterprise Certificate Server Set 構造設計書

＜記述内容＞

- TSP を実施するサブシステムの識別と仕様
- サブシステム間インタフェースの識別と仕様

- 前提 IT 環境（ハードウェア、ソフトウェア）の識別
- 前提 IT 環境で実装される補助的な保護メカニズムの仕様

(6) Enterprise Certificate Server Set 対応分析書

＜記述内容＞

- ST の TOE セキュリティ機能と、上記機能仕様書の TSF インタフェースとの対応関係
- 上記機能仕様書の TSF インタフェースと、上記構造設計書のサブシステム間インタフェースとの対応関係

(7) Enterprise Certificate Server Set 開発セキュリティ規程書

＜記述内容＞

- 開発環境において、TOE に関連する資産を保護するための手続き
- 上記手続きを実施した際の証跡

(8) Enterprise Certificate Server Set テスト仕様書／報告書

＜記述内容＞

- テスト計画
- テスト項目
- テスト手順
- 期待されるテスト結果及び実際のテスト結果

(9) Enterprise Certificate Server Set テスト分析書

＜記述内容＞

- 上記機能仕様書の TSF インタフェースと、上記テスト仕様書／報告書のテスト項目との対応関係
- 上記構造設計書のサブシステム間インタフェースと、上記テスト仕様書／報告書のテスト項目との対応関係

(10) Enterprise Certificate Server Set セキュリティ機能強度分析書

＜記述内容＞

- ST で記述したセキュリティ機能強度に対する分析

(11) Enterprise Certificate Server Set 脆弱性分析書

＜記述内容＞

- TOE が持つ脆弱性の識別
- 識別した脆弱性が TOE の想定した運用環境では顕在化しないこと

(12) Enterprise Certificate Server Set

評価者が TOE のテストを行う際、上記テスト仕様書／報告書で実施されたものと同等のテスト環境を提供する。

7. PP 主張

7.1. PP 参照

参照した PP はない。

7.2. PP 修整

PP への修整はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

8.1. セキュリティ対策方針根拠

本章では、セキュリティ対策方針が TOE セキュリティ環境に対して必要かつ十分であることを記述する。

セキュリティ対策方針と対応する前提条件及び組織のセキュリティ方針の対応関係を表 6に示す。

またセキュリティ対策方針と対抗する脅威及び組織のセキュリティ方針の対応関係を表 7に示す。

表 6： セキュリティ対策方針と前提条件及び組織のセキュリティ方針の対応表

前提条件及び組織のセキュリティ方針 / セキュリティ対策方針	A.TOE_SEP	A.ABSTRACT_ACCOUNT	A.PASSWORD	A.IT_ENV	A.ABSTRACT	A.SETTING	A.AREA	A.FIREWALL	P.CA_ADMIN	P.OPERATOR	P.AUDITOR	P.SIER	P.HSM	P.PERSONNEL
OE.HSM													○	
OM.SI	○			○								○		
OM.SETTING						○								
OM.CONNECT								○						
OM.AREA_CONTROL							○							
OM.MACHINE_MGT	○			○	○			○						
OM.ACCOUNT_MGT		○												
OM.PASSWORD_MGT			○											
OM.CA_ADMIN									○					
OM.OPERATION										○				
OM.AUDIT											○			
OM.PERSONNEL														○

表 7： セキュリティ対策方針と脅威及び組織のセキュリティ方針の対応表

脅威及び組織のセキュリティ方針 / セキュリティ対策方針	T.UNAUTH_ACCESS	T.IMPERSON	T.TOE_SECRET	T.LINE_SECRET	T.MISS	P.DUALCTL	P.PROTECT_LOG
O.ADMIN	○	○					
O.AC_DATA	○						
O.I&A		○					
O.ENC_DATA			○				
O.ENC_LINE				○			
O.AUDIT	○	○			○		
O.PROTECT_LOG							○
O.COUNCIL		○				○	

次に、各前提条件及び組織のセキュリティ方針がセキュリティ対策方針で実現できること、並びに各脅威がセキュリティ対策方針で対抗できることを示す。

＜前提条件＞

A.TOE_SEP (不正な干渉からの分離)

OM.SI により、システム構築者は、CA サーバマシン及び管理端末マシンに、TOE の動作に関係ないソフトウェアはインストールしない。また、**OM.MACHINE_MGT** により、CA 管理者は、TOE の動作を干渉するようなソフトウェアが CA サーバマシン及び管理端末マシンにインストールされないよう適切に管理を行う。

これらの対策によって **A.TOP_SEP** は実現される。

A.ABSTRACT_ACCOUNT (下位抽象マシンのアカウント)

OM.ACCOUNT_MGT により、TOE が動作する OS 及び DB のアカウントは、CA 管理者によって適切に管理される。これにより、OS 及び DB のアカウントを不正に利用した保護対象資産の改竄、削除を防ぐことができる。

この対策によって **A.ABSTRACT_ACCOUNT** は実現される。

A.PASSWORD (パスワードの管理)

OM.PASSWORD_MGT により、TOE を利用するためのパスワードは、ECS 利用者が記憶しており、本人以外に知られないように管理される。また、ECS 利用者は、ECS Set のガイダンス文書に従って、適切なパスワードを設定し、適切な頻度でパスワード変更を行う。
この対策によって **A.PASSWORD** は実現される。

A.IT_ENV (TOE の IT 環境)

OM.SI により、システム構築者は、ECS Set のガイダンス文書が定める手順に従って、TOE 及び TOE の IT 環境のマニュアルを熟読した上で、TOE 及び TOE の IT 環境を構築する。また、**OM.MACHINE_MGT** により、CA 管理者は、TOE 及び TOE の IT 環境が正常な動作を維持するように、適切に管理を行う。
これらの対策によって **A.IT_ENV** は実現される。

A.ABSTRACT (下位抽象マシンの動作)

OM.MACHINE_MGT により、TOE が動作する OS 及び DB は、CA 管理者によって不正な改変から保護され、正しく動作するよう適切に管理される。
この対策によって **A.ABSTRACT** は実現される。

A.SETTING (設置エリア)

OM.SETTING により、CA サーバマシン及び HSM は、セキュアエリア内に設置され、管理端末マシンは、マシンエリア内に設置される。
この対策によって **A.SETTING** は実現される。

A.AREA (エリアの保護)

OM.AREA_CONTROL により、セキュアエリアは、CA 管理者のみ入室できるよう入退室管理が行われ、不正な物理的アクセスから保護される。また、マシンエリアは、認証局に属する者のみ物理的にアクセスできるように制限される。
この対策によって **A.AREA** は実現される。

A.FIREWALL (ファイアウォール)

OM.CONNECT により、内部セグメントは、ファイアウォールを介してインターネットに接続される。また、ファイアウォールは、インターネットから CA サーバマシン、管理端末マシンへのアクセスを拒否するように設定される。
また、**OM.MACHINE_MGT** により、ファイアウォールの設定は、適切に管理・維持される。

これらの対策によって **A.FIREWALL** は実現される。

以上より、全ての前提条件に対して、何らかのセキュリティ対策方針が十分に実現していることが示される。

＜組織のセキュリティ方針＞

P.CA_ADMIN (CA 管理者)

OM.CA_ADMIN により、CA 管理者は、ECS Set のガイダンス文書が定める手順に従って、TOE 及び TOE の IT 環境の管理業務を行う。また、CA 管理者は、認証局に対する知識が要求され、指定された以外の手段で TOE の構成を変更することを禁止され、他の役職を兼務することができない。
この対策によって **P.CA_ADMIN** は実現される。

P.OPERATOR (運用者)

OM.OPERATION により、運用者は、ECS Set のガイダンス文書が定める手順に従って、TOE の運用業務を行う。また、運用者は他の役職を兼務することができない。
この対策によって **P.OPERATION** は実現される。

P.AUDITOR (監査者)

OM.AUDIT により、監査者は、ECS Set のガイダンス文書が定める手順に従って、TOE の監査業務を行う。また、監査者は他の役職を兼務することができない。
この対策によって **P.AUDITOR** は実現される。

P.SIER (認証局の構築者)

OM.SI により、システム構築者は、ECS Set のガイダンス文書が定める手順に従って、TOE 及び TOE の IT 環境のマニュアルを熟読した上で、TOE 及び TOE の IT 環境の設置・生成・立上げを行う。
この対策によって **P.SIER** は実現される。

P.DUALCTL (合議)

O.COUNCIL により、TOE の管理操作に対しては複数の CA 管理者による合議が要求され、運用操作に対しては複数の運用者による合議が要求される。
この対策によって **P.DUALCTL** は実現される。

P.HSM (HSM)

OE.HSM により、認証局の CA 秘密鍵のライフサイクル管理及び CA 秘密鍵を利用した暗号操作は、FIPS 140-2 level3 相当の HSM を使用して行われる。

この対策によって **P.HSM** は実現される。

P.PERSONNEL (認証局に属する者)
OM.PERSONNEL により、認証局に属する者は、認証局を運用する組織の管理者によって適切に管理され、認証局の運用を妨害するような、特殊な機器を持ち込んだ攻撃や、管理端末マシンへの攻撃は行わない。
この対策によって **P.PERSONNEL** は実現される。

P.PROTECT_LOG (監査ログの保護)
監査ログは、**O.PROTECT_LOG** により暴露から保護され、改竄または削除された場合に検出することができる。
この対策によって **P.PROTECT_LOG** は実現される。

以上より、全ての組織のセキュリティ方針に対して、何らかのセキュリティ対策方針が十分に実現していることが示される。

＜脅威＞
T.UNAUTH_ACCESS (不正なアクセス)
O.AC_DATA により、適切な権限を持った者だけが TOE を使用して、利用者データ、TSF データにアクセスすることができる。また、**O.ADMIN** により、アクセスに関する管理は CA 管理者によって適切に行われる。以上のセキュリティ対策方針により、TOE を使用したデータの不正改変を防止することができる。
O.AUDIT によりデータの不正改変というセキュリティ事象を記録・追跡・管理することができ、またセキュリティ事象を記録・追跡・管理することにより、このような予兆を検出することができる。
これらの対策によって **T.UNAUTH_ACCESS** に対抗できる。

T.IMPERSON (不正ログイン)
O.I&A により、TOE は、管理端末を通じて CA サーバにログインを試みる利用者に対して識別・認証を行い、正当な ECS 利用者であることの確認を行う。また、**O.ADMIN** により、識別・認証に関する管理は、CA 管理者によって適切に行われる。以上のセキュリティ対策方針により、正当なアカウントを持たない利用者による TOE への不正なログインを防止することができる。
O.AUDIT により、TOE は、ログインの失敗を監査ログに記録する。連続したログイン失敗の事象を記録・追跡・監査することで、この脅威を検出することができる。
ECS 利用者でない利用者が識別・認証情報の不正入手を通じて、CA サーバへのログインに成功しても、**O.COUNCIL** により、他の正当な ECS 利用者による合議がなければ、重要な操作を実行できない。

これらの対策によって **T.IMPERSON** に対抗できる。

T.TOE_SECRET (秘密情報の暴露)
暴露から保護する必要がある保護対象資産は、**O.ENC_DATA** により暗号化した状態で保管される。
この対策によって **T.TOE_SECRET** に対抗できる。

T.LINE_SECRET (通信回線上の秘密情報の暴露／改竄)
管理端末と CA サーバの間の通信路を流れるデータは、**O.ENC_LINE** により暗号化した状態で送受信される。
この対策によって **T.LINE_SECRET** に対抗できる。

T.MISS (操作ミスによるデータ改竄／削除)
O.AUDIT により、どのような操作を行ったかというセキュリティ事象を記録・追跡・管理することができ、またセキュリティ事象を記録・追跡・管理することにより、このような操作ミスを検出することができる。
この対策によって **T.MISS** に対抗できる。

以上より、全ての脅威に対して、何らかのセキュリティ対策方針が十分に対策していることが示される。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

本章では、セキュリティ機能要件がセキュリティ対策方針に対して必要かつ十分であることを記述する。セキュリティ機能要件とセキュリティ対策方針の対応関係を表 8 に示す。

表 8： セキュリティ機能要件とセキュリティ対策方針の対応表

セキュリティ対策方針 / セキュリティ機能要件	O.ADMIN	O.AC_DATA	O.I&A	O.ENC_DATA	O.ENC_LINE	O.AUDIT	O.PROTECT_LOG	O.COUNCIL	OE.HSM
FAU_GEN.1						○			
FAU_GEN.2						○			
FAU_SAR.1						○			
FAU_SAR.2						○			
FAU_STG.1							○		
FAU_STG.4							○		
FCS_CKM.1a				○					
FCS_COP.1a				○					
FCS_CKM.1b					○				
FCS_CKM.2b					○				
FCS_COP.1b					○				
FCS_CKM.1c							○		
FCS_COP.1c							○		
FCS_COP.1d				○					
FDP_ACC.1		○						○	
FDP_ACF.1		○						○	
FIA_AFL.1			○						
FIA_ATD.1			○						
FIA_SOS.1	○								
FIA_UAU.1			○						
FIA_UID.1			○						

FIA_USB.1			○						
FMT_MOF.1	○							○	
FMT_MSA.1a	○							○	
FMT_MSA.1b		○							
FMT_MSA.1c	○							○	
FMT_MSA.1d								○	
FMT_MSA.2c							○		
FMT_MSA.3	○								
FMT_MTD.1a		○						○	
FMT_MTD.1b						○			
FMT_SMR.1	○								
FMT_SMF.1	○								
FPT_RVM.1		○	○						
FPT_SEP.1	○	○	○	○	○	○	○	○	
FPT_STM.1						○			
IT 環境									
FCS_CKM.1e									○
FCS_CKM.4e									○
FCS_COP.1e									○
FMT_MSA.2e									○

「表 8： セキュリティ機能要件とセキュリティ対策方針の対応表」より、全てのセキュリティ機能要件が、何らかのセキュリティ対策方針の実現のために必要であることが示される。

次に、セキュリティ対策方針がセキュリティ機能要件で実現できることを以下に説明する。

＜TOE セキュリティ対策方針＞

O.ADMIN（TOE の管理）：

FMT_SMR.1 により、役割が定義され、ECS 利用者に関連付けられ、維持される。**FMT_MSA.1a**、**FMT_MSA.1c**、**FMT_MSA.3** により、ECS 利用者のセキュリティ属性は、規定の合議人数に達した CA 管理者によって管理される。また **FMT_MOF.1** により、規定の合議人数に達した CA 管理者だけが TOE に関わるセキュリティ機能の起動と停止を行う。**FIA_SOS.1** により、ECS 利用者の秘密（ECS 利用者パスワード）を設定する際に、秘密が品質尺度に合致することを TSF が検証することを要求する。**FMT_SMF.1** により、TOE はセキュリティ機能を管理する能力をもつ。

O.AC_DATA (保護対象資産のアクセス権限)：

FDP_ACC.1 により、利用者データのアクセス制御ポリシーが定義される。アクセス制御ポリシーは **FDP_ACF.1** により具体化され、TOE は、権限及び合議人数に基づいて利用者データに対する操作を制御する。また **FMT_MTD.1a** により、TOE は、TSF データ（監査ログ用証明書の設定、合議人数の設定）に対する操作を、規定の合議人数に達した CA 管理者に制限する。また **FMT_MSA.1b** により、TOE は、ECS 利用者パスワードに対する操作を、ログインしている ECS 利用者に制限する。

O.I&A (TOE での識別･認証)：

FIA_UAU.1、**FIA_UID.1** により、TOE は、利用者が TOE の保護対象資産にアクセスする前に、ECS 利用者 ID と ECS 利用者パスワードの入力を要求し、識別・認証が成功することを要求する。**FIA_AFL.1** により、TOE は、識別・認証が失敗した場合、当該管理端末からのコネクションを終了する。さらに **FIA_ATD.1** より、TOE は、ECS 利用者のセキュリティ属性を維持する。**FIA_USB.1** により、TOE は、ECS 利用者のセキュリティ属性をその代行サブジェクトに関連付ける。

O.ENC_DATA (保管データの保護)：

TOE は、保護対象資産のうち、PKCS#12 データ、PKCS#12 パスワード、ECS 利用者パスワードを暗号化してデータベースに格納する。また、TOE は、CA 設定情報、DB データ暗号鍵、監査ログ用証明書／監査ログ用秘密鍵を暗号化された格納領域である秘密情報格納ディレクトリに格納する。**FCS_CKM.1a** により、TOE は、指定された標準に基づく特定のアルゴリズムと鍵長に従って、DB データ暗号鍵を生成する。**FCS_COP.1a、FCS_COP.1d** により、TOE は、指定されたアルゴリズムと指定された鍵長に従って、暗号操作を実施する。

O.ENC_LINE (通信データの保護)：

TOE は、管理端末と CA サーバの間の通信路を暗号化する。**FCS_CKM.1b** により、TOE は、指定された標準に基づく特定のアルゴリズムと鍵長に従って、通信路暗号鍵を生成する。**FCS_CKM.2b** により、TOE は、生成した鍵を指定された特定の方法に従って配付し、CA サーバと管理端末の間で共有する。また、生成された鍵は、CA サーバと管理端末の間のコネクションの確立とともに生成され、コネクション終了により揮発する。**FCS_COP.1b** により、TOE は、指定されたアルゴリズムと指定された鍵長に従って、暗号操作を実施する。

O.AUDIT (監査ログの記録･追跡･管理)：

FAU_GEN.1 により、TOE は、監査対象事象の監査ログを生成する。また **FAU_GEN.2** により、監査対象事象の原因となった利用者を監査ログに記録する。**FAU_SAR.1** により、監査者が監査ログから監査情報を読み出すことができる。**FAU_SAR.2** により、監査者のみが監査ログを読み出すことができる。また **FMT_MTD.1b** により、監査者のみが監査ログを問い合わせ、削除、取得するこ

とができる。**FPT_STM.1** により、TOE は、監査ログに必要なタイムスタンプを提供する。

O.PROTECT_LOG (監査ログの保護)：
TOE は、監査ログに対して、署名・暗号化及び検定・復号化を行う。**FAU_STG.1** により、監査ログに対する改変を検知することを要求される。また、監査ログを不正な削除から保護することを要求される。**FAU_STG.4** により、監査ログが満杯になった場合、CA サーバの停止などのアクションをとる。**FCS_COP.1c** により、TOE は、監査ログに対して指定されたアルゴリズムと指定された鍵長に従って、暗号操作を実施する。**FCS_CKM.1c** により、TOE は、指定された標準に基づく特定のアルゴリズムと鍵長に従って、監査ログ暗号鍵、監査ログ署名公開鍵／秘密鍵を生成する。**FMT_MSA.2c** により、使用される鍵のセキュリティ属性はセキュアなものだけが使用される。

O.COUNCIL (合議に基づいた操作)：
FDP_ACC.1、FDP_ACF.1 により、TOE は、利用者データへのアクセスに対する合議を実施する。**FMT_MOF.1** により、TOE は、セキュリティ機能のふるまいの変更に対する合議を実施する。**FMT_MSA.1a、FMT_MSA.1c** により、TOE は、サブジェクトのセキュリティ属性（ECS 利用者 ID、ECS 利用者パスワード、ECS 利用者権限リスト）の作成、改変及び削除に対する合議を実施する。**FMT_MSA.1d** により、TOE は、オブジェクトのセキュリティ属性（操作種別、操作要求者と合議者の ECS 利用者 ID、操作に必要な残りの合議人数）の改変及びクリアに対する合議を実施する。また **FMT_MTD.1a** により、TOE は、TSF データ（監査ログ用証明書の設定、合議人数の設定）に対する問い合わせ及び改変に対する合議を実施する。

以上より、全ての TOE セキュリティ対策方針に対して、何らかのセキュリティ機能要件が十分に実現していることが示される。

＜IT 環境セキュリティ対策方針＞
OE.HSM (HSM での暗号操作)：
FCS_CKM.1e により、HSM が FIPS 140-2 に基づいた特定のアルゴリズムと鍵長に従って CA 秘密鍵が生成されることを要求する。**FCS_CKM.4e** により、HSM が FIPS 140-2 に基づいた特定の破棄方法に従って CA 秘密鍵が破棄されることを要求する。
FCS_COP.1e により、HSM が指定されたアルゴリズムと指定された鍵長に従って、暗号操作を実施することを要求する。また、**FMT_MSA.2e** により、使用される鍵のセキュリティ属性はセキュアなものだけが使用される。

以上より、全ての IT 環境セキュリティ対策方針に対して、何らかのセキュリティ機能要件が十分に実現していることが示される。

8.2.2. セキュリティ機能要件の相互支援

セキュリティ機能の迂回防止、干渉または破壊防止の観点から、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以下に示す。

○ FPT_RVM.1（TSP の非バイパス性）

FDP_ACC.1、FDP_ACF.1、FIA_UAU.1、FIA_UID.1 の各機能要件は、**FPT_RVM.1** により、本 TOE のセキュリティ機能要件が迂回されずに確実に実施されることを保証する。

○ FPT_SEP.1（TSF ドメイン分離）

FPT_SEP.1 により、TSF のセキュリティドメインが分離されることによって、TOE 内の他のサブジェクトから TSF への干渉または破壊が防御されることを保証する。

8.2.3. セキュリティ機能要件依存性

本 ST で選択した TOE 及び IT 環境のセキュリティ機能要件と、本 ST で選択した依存コンポーネント及び本 ST で除去した依存コンポーネントを表 9 に示す。

表 9： セキュリティ機能要件間の依存関係対応表

本 ST で選択した セキュリティ機能要件	本 ST で選択した依存コンポーネント	本 ST で除去した 依存コンポーネント
TOE 機能要件		
FAU_GEN.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	
FAU_SAR.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	
FAU_STG.1	FAU_GEN.1	
FAU_STG.4	FAU_STG.1	
FCS_CKM.1a	FCS_COP.1a	FMT_MSA.2a (※3) FCS_CKM.4a (※1)
FCS_COP.1a	FCS_CKM.1a	FMT_MSA.2a (※3) FCS_CKM.4a (※1)
FCS_CKM.1b	FCS_COP.1b	FMT_MSA.2b (※3) FCS_CKM.4b (※2)
FCS_CKM.2b	FCS_CKM.1b	FMT_MSA.2b (※3) FCS_CKM.4b (※2)
FCS_COP.1b	FCS_CKM.1b	FMT_MSA.2b (※3) FCS_CKM.4b (※2)
FCS_CKM.1c	FCS_COP.1c FMT_MSA.2c	FCS_CKM.4c (※1)
FCS_COP.1c	FCS_CKM.1c FMT_MSA.2c	FCS_CKM.4c (※1)
FCS_COP.1d		FMT_MSA.2d (※3) FCS_CKM.1d (※5) FCS_CKM.4d (※1)
FDP_ACC.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	
FIA_AFL.1	FIA_UAU.1	
FIA_ATD.1	なし	

FIA_SOS.1	**なし**		
FIA_UAU.1	**FIA_UID.1**		
FIA_UID.1	**なし**		
FIA_USB.1	**FIA_ATD.1**		
FMT_MOF.1	**FMT_SMR.1**	**FMT_SMF.1**	
FMT_MSA.1a	**FDP_ACC.1** **FMT_SMF.1**	**FMT_SMR.1**	
FMT_MSA.1b	**FDP_ACC.1** **FMT_SMF.1**	**FMT_SMR.1**	
FMT_MSA.1c	**FDP_ACC.1** **FMT_SMF.1**	**FMT_SMR.1**	
FMT_MSA.1d	**FDP_ACC.1** **FMT_SMF.1**	**FMT_SMR.1**	
FMT_MSA.2c	**FMT_MSA.1** **FMT_SMR.1**	**FDP_ACC.1**	**ADV_SPM.1c (※4)**
FMT_MSA.3	**FMT_MSA.1**	**FMT_SMR.1**	
FMT_MTD.1a	**FMT_SMR.1**	**FMT_SMF.1**	
FMT_MTD.1b	**FMT_SMR.1**	**FMT_SMF.1**	
FMT_SMR.1	**FIA_UID.1**		
FMT_SMF.1	**なし**		
FPT_RVM.1	**なし**		
FPT_SEP.1	**なし**		
FPT_STM.1	**なし**		
IT 環境機能要件			
FCS_CKM.1e	**FCS_CKM.4e** **FMT_MSA.2e**	**FCS_COP.1e**	
FCS_CKM.4e	**FCS_CKM.1e**	**FMT_MSA.2e**	
FCS_COP.1e	**FCS_CKM.1e** **FMT_MSA.2e**	**FCS_CKM.4e**	
FMT_MSA.2e	**FMT_MSA.1** **FMT_SMR.1**	**FDP_ACC.1**	**ADV_SPM.1e (※4)**

（※1）本 ST では、**FCS_CKM.1a、FCS_COP.1a、FCS_CKM.1c、FCS_COP.1c、FCS_COP.1d** の鍵破棄の依存コンポーネントとして、それぞれ **FCS_CKM.4a**、**FCS_CKM.4c、FCS_CKM.4d** を取り扱わない。**FCS_CKM.1a、FCS_CKM.1c** によって生成される鍵は、秘密情報格納ディレクトリに

格納される。秘密情報格納ディレクトリに格納されるこれらの鍵は、システム構築時に生成した鍵を TOE が破棄されるまで使用し続けるため、破棄する必要はない。従って、鍵破棄に関する機能要件を取り扱う必要がない。

（※２）本 ST では、**FCS_CKM.1b、FCS_CKM.2b、FCS_COP.1b** の鍵破棄の依存コンポーネントとして、**FCS_CKM.4b** を取り扱わない。**FCS_CKM.1b** によって生成される鍵は、管理端末と CA サーバの間のコネクション毎に生成され、コネクションの切断とともに破棄される。従って、鍵破棄に関する機能要件を取り扱う必要がない。

（※３）本 ST では、**FCS_CKM.1a、FCS_COP.1a、FCS_CKM.1b、FCS_CKM.2b、FCS_COP.1b、FCS_COP.1d** のセキュアなセキュリティ属性の依存コンポーネントとして、**FMT_MSA.2a、FMT_MSA.2b、FMT_MSA.2d** を取り扱わない。
以下 各々説明する。

【DB データ暗号鍵】	**FMT_MSA.2a**
説明	DB データ暗号鍵は、TOE の生成時にシステム構築者によって生成される。以降、生成された鍵は変更されずに使用されるため、暗号鍵のセキュリティ属性は、セキュアな値が維持される。そのため、**FMT_MSA.2a** がなくとも、DB データ暗号鍵は常にセキュアな状態で使用できる。このため、**FMT_MSA.2a** は取り扱わない。
【通信路の暗号化】	**FMT_MSA.2b**
説明	TOE は、管理端末と CA サーバ間の接続時に通信路暗号鍵及び通信路公開鍵／秘密鍵を生成する。これらの鍵は管理端末と CA サーバ間のコネクション毎に生成され、コネクションの切断と伴に破棄される。従って、**FMT_MSA.2b** がなくとも通信路暗号鍵及び通信路公開鍵／秘密鍵は常にセキュアな状態で使用できる。このため、**FMT_MSA.2b** は取り扱わない。
【秘密情報暗号鍵】	**FMT_MSA.2d**
説明	秘密情報暗号鍵は、TOE の生成時にシステム構築者によって生成される。以降、生成された鍵は変更されずに使用されるため、暗号鍵のセキュリティ属性は、セキュアな値が維持される。そのため、**FMT_MSA.2d** がなくとも、秘密情報暗号鍵は常にセキュアな状態で使用できる。このため、**FMT_MSA.2d** は取り扱わない。

（※４）本 ST では、**FMT_MSA.2c、FMT_MSA.2e** のセキュリティ方針モデルの依存コンポーネントとして、**ADV_SPM.1c、ADV_SPM.1e** を取り扱わない。
以下 各々説明する。

表 10： セキュリティ方針モデルの説明

【監査ログの署名】	**FMT_MSA.2c**
対象／目的	監査ログに署名を付与する。
セキュリティ属性	監査ログ署名公開鍵／秘密鍵の有効期限
説明	ADV_SPM.1 にて要求されるセキュリティ方針は、本 ST では FDP_ACC.1 にて規定された ECS 利用者データアクセス制御 SFP に相当する。この SFP は、監査ログ署名公開鍵／秘密鍵をアクセス制御の対象としていない。このため、ADV_SPM.1c は取り扱わない。
【CA 署名とその検定】	**FMT_MSA.2e**
対象／目的	EE 証明書に署名を付与する。
セキュリティ属性	CA 公開鍵／秘密鍵の有効期限
説明	ADV_SPM.1 にて要求されるセキュリティ方針は、本 ST では FDP_ACC.1 にて規定された ECS 利用者データアクセス制御 SFP に相当する。この SFP は、CA 公開鍵／秘密鍵をアクセス制御の対象としていない。このため、ADV_SPM.1e は取り扱わない。

（※５）本 ST では、**FCS_COP.1d** の鍵生成の依存コンポーネントとして、**FCS_CKM.1d** を取り扱わない。**FCS_COP.1d** によって使用される鍵は、システム構築時に生成し、TOE が破棄されるまで使用し続けるため、TOE の運用時に生成する必要はない。従って、鍵生成に関する機能要件を取り扱う必要がない。

8.2.4. **監査対象事象根拠**

「5.1TOE セキュリティ機能要件」であげた各機能要件を選択した場合に、CC Part2 で規定された、監査対象とすべきアクションを表 11 に示す。また、TOE で監査対象事象としているアクションを下線で示す。さらに、「6.1.1 監査機能（**SF.AUDIT**)」で示した TOE が記録する監査対象事象の対応する番号を示す。

表 11： CC Part2 で規定された監査対象とすべきアクションと関連する TOE の監査対象事象

機能要件	監査対象とすべきアクション	TOE の監査対象事象
セキュリティ監査		
FAU_GEN.1	監査対象とすべき識別されたアクションはない。	なし
FAU_GEN.2	監査対象とすべき識別されたアクションはない。	なし
FAU_SAR.1	基本: 監査記録からの情報の読み出し。	#1
FAU_SAR.2	基本: 監査記録からの成功しなかった情報読み出し。	#1
FAU_STG.1	監査対象とすべき識別されたアクションはない。	なし
FAU_STG.4	基本: 監査格納失敗によってとられるアクション。	なし（後述）
暗号サポート		
FCS_CKM.1a	最小: 動作の成功と失敗。 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。	#22, #24
FCS_CKM.1b		#19, #24
FCS_CKM.1c		#22, #24
FCS_COP.1a	最小: 成功と失敗及び暗号操作の種別。 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。	#8, #9, #10, #24
FCS_COP.1b		#19, #24
FCS_COP.1c		#1, #24
FCS_COP.1d		#3, #24
FCS_CKM.2b	最小: 動作の成功と失敗。 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。	#19, #24
利用者データ保護		
FDP_ACC.1	監査対象にすべき識別された事象はない。	なし
FDP_ACF.1	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。 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。 詳細: アクセスチェック時に用いられる特定のセキュ	#4, #5, #6, #7, #8, #9, #10, #11, #12, #13, #14, #15, #16, #18

	リティ属性。	
識別と認証		
FIA_AFL.1	最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション（例えば端末の停止）、もし適切であれば、正常状態への復帰（例えば端末の再稼動）。	#19
FIA_ATD.1	監査対象にすべき識別されたアクションはない。	なし
FIA_SOS.1	最小: TSF による、テストされた秘密の拒否; 基本: TSF による、テストされた秘密の拒否または受け入れ; 詳細: 定義された品質尺度に対する変更の識別。	#20
FIA_UAU.1	最小: 認証メカニズムの不成功になった使用; 基本: 認証メカニズムのすべての使用。 詳細: 利用者認証以前に行われたすべての TSF 調停アクション	#19
FIA_UID.1	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; 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。	#19
FIA_USB.1	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）。 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）。	#21
セキュリティ管理		
FMT_MOF.1	基本: TSF の機能のふるまいにおけるすべての改変。	#22
FMT_MSA.1a	基本: セキュリティ属性の値の改変すべて。	#23
FMT_MSA.1b		#23
FMT_MSA.1c		#23
FMT_MSA.1d		#17
FMT_MSA.2c	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; 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（後述）
FMT_MSA.3	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。 基本: セキュリティ属性の初期値の改変すべて。	#23

FMT_MTD.1a	基本: TSF データの値のすべての改変。	#22
FMT_MTD.1b		#2
FMT_SMR.1	最小: 役割の一部をなす利用者のグループに対する改変; 詳細: 役割の権限の使用すべて。	#23
FMT_SMF.1	最小: 管理機能の使用	#22
TSF の保護		
FPT_RVM.1	監査対象にすべき識別されたアクションはない。	なし
FPT_SEP.1	監査対象にすべき識別されたアクションはない。	なし
FPT_STM.1	最小: 時間の変更; 詳細: タイムスタンプの提供	なし（後述）

表 11 に示した通り、各機能要件の監査対象とすべきアクションは、後述の例外を除いて、本 TOE の監査対象事象として記録している。

以下では、CC Part2 で規定された監査対象とすべき最小レベルのアクションのうち、本 TOE において監査対象事象に含まれない根拠を説明する。

FAU_STG.4	基本: 監査格納失敗によってとられるアクション。
根拠	本機能要件の監査対象とすべき最小レベルのアクションはない。 また、TOE は、監査格納失敗時のアクションとして以下の事象を OS に出力する。 ● 監査ログの出力に失敗した事象 ● CA サーバを停止した事象。 上記事象により、監査格納失敗によって取られたアクションを確認することは可能である。従って、本アクションが監査対象事象に含まれていなくても、TOE セキュリティ対策方針上問題ない。
FMT_MSA.2c	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; 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。
根拠	TOE は、監査ログ用証明書の有効期限が切れる 3 日前から、有効期限切れが迫る旨の事象を OS に出力するため、監査ログ用証明書の有効期限が切れ、セキュリティ属性がセキュアな値でなくなることを確認することは可能である。従って、本アクションが監査対象事象に含まれていなくても、TOE セキュリティ対策方針上問題ない。
FPT_STM.1	最小: 時間の変更; 詳細: タイムスタンプの提供
根拠	TOE は、時間を変更する機能を提供しない。従って、本アクションが監査対象事象に含まれていなくても、TOE セキュリティ対策方針上問題ない。

8.2.5. セキュリティ管理機能根拠

「5.1 TOE セキュリティ機能要件」であげた各機能要件を選択した場合に、CC Part2 で規定された、管理対象とすべきアクティビティを表 12 に示す。TOE でセキュリティ管理機能を持つアクティビティを下線で示す。さらに、TOE が持つセキュリティ管理機能を示す。

表 12： CC Part2 で規定された管理対象とすべきアクティビティと関連する TOE の管理機能

機能要件	管理アクティビティ	TOE の管理機能
セキュリティ監査		
FAU_GEN.1	予見される管理アクティビティはない。	なし
FAU_GEN.2	予見される管理アクティビティはない。	なし
FAU_SAR.1	監査記録に対して読み出し権のある利用者グループの維持（削除、改変、追加)。	**SF.CA_MGT**
FAU_SAR.2	予見される管理アクティビティはない。	なし
FAU_STG.1	予見される管理アクティビティはない。	なし
FAU_STG.4	監査格納失敗時にとられるアクションの維持（削除、改変、追加)。	なし（後述）
暗号サポート		
FCS_CKM.1a **FCS_CKM.1b** **FCS_CKM.1c**	暗号鍵属性の変更の管理。	なし（後述）
FCS_COP.1a **FCS_COP.1b** **FCS_COP.1c** **FCS_COP.1d**	予見される管理アクティビティはない。	なし
FCS_CKM.2b	暗号鍵属性の変更の管理。	なし（後述）
利用者データ保護		
FDP_ACC.1	予見される管理アクティビティはない。	なし
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	なし（後述）
識別と認証		
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) なし（後述） b) なし（後述）
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし（後述）

FIA_SOS.1	秘密の検証に使用される尺度の管理。	なし（後述）
FIA_UAU.1	a) 管理者による認証データの管理; b) 関係する利用者による認証データの管理; c) 利用者が認証される前にとられるアクションのリストを管理すること。	a), b) **SF.CA_MGT** c) なし（後述）
FIA_UID.1	a) 利用者識別情報の管理; b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。	a) **SF.CA_MGT** b) なし（後述）
FIA_USB.1	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。	なし（後述）
セキュリティ管理		
FMT_MOF.1	TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること。	**SF.CA_MGT**
FMT_MSA.1a **FMT_MSA.1b** **FMT_MSA.1c** **FMT_MSA.1d**	セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	**SF.CA_MGT**
FMT_MSA.2c	予見される管理アクティビティはない。	なし
FMT_MSA.3	a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	a) **SF.CA_MGT** b) なし（後述）
FMT_MTD.1a **FMT_MTD.1b**	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	**SF.CA_MGT**
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	**SF.CA_MGT**
FMT_SMF.1	予見される管理アクティビティはない。	なし
TSF の保護		
FPT_RVM.1	予見される管理アクティビティはない。	なし
FPT_SEP.1	予見される管理アクティビティはない。	なし
FPT_STM.1	a) 時間の管理	なし（後述）

表 12 に示した通り、各機能要件の管理対象とすべきアクティビティは、後述の例外を除いて、本 TOE の管理機能で管理している。

以下では、CC Part2 で規定された管理対象とすべきアクティビティのうち、本 TOE の管理機能に含まれない根拠を説明する。

FAU_STG.4	監査格納失敗時にとられるアクションの維持（削除、改変、追加）。

根拠	監査格納失敗時のアクションは CA サーバの停止であり、このアクションは不変であり、管理の対象ではない。
FCS_CKM.1a **FCS_CKM.1b** **FCS_CKM.1c**	暗号鍵属性の変更の管理。
根拠	いずれの暗号鍵に対しても、生成した鍵の属性は不変であるため、管理の対象ではない。
FCS_CKM.2b	暗号鍵属性の変更の管理。
根拠	通信路暗号鍵、通信路公開鍵／秘密鍵のいずれの鍵に対しても、鍵のセキュリティ属性は存在しないため、管理の対象ではない。
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。
根拠	本コンポーネントでは、明示的なアクセスまたは拒否に対する割付を行っていない。従って、明示的なアクセスまたは拒否に関する属性はない。
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理
根拠	a) 不成功の認証試行に対する閾値は、1 回であり、これは不変である。従って管理の対象ではない。 b) 認証失敗の事象において取られるアクションは、管理端末と CA サーバ間のコネクションの切断であり、これは不変である。従って管理の対象ではない。
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。
根拠	本コンポーネントに関するセキュリティ属性の追加はない。従って管理の対象ではない。
FIA_SOS.1	秘密の検証に使用される尺度の管理。
根拠	本 TOE で秘密の検証に使用される尺度は、不変であり、管理の対象ではない。
FIA_UAU.1	c) 利用者が認証される前にとられるアクションのリストを管理すること。
根拠	識別前に許可される暗号通信路の使用はアクションを変更できない。従って管理の対象ではない。
FIA_UID.1	b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。
根拠	識別前に許可される暗号通信路の使用はアクションを変更できない。従って管理の対象ではない。
FIA_USB.1	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。
根拠	サブジェクトのセキュリティ属性は ECS 利用者 ID であり、この属性が変更されることはない。従って管理の対象ではない。

FMT_MSA.3	b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。
根拠	b) 本コンポーネントのデフォルト値は、許可的であり、この設定は不変である。従って管理の対象ではない。
FPT_STM.1	a) 時間の管理。
根拠	a) 本 TOE では、時刻は変更しない。従って時刻の管理は管理の対象ではない。

8.2.6. 最小機能強度レベル根拠

本 ST の TOE は、国際標準 X.509 に準拠した証明書の発行及び失効を管理する認証局（CA）の機能を提供する。本 TOE の保護対象資産である利用者データ、TSF データは安全に保護される必要がある。

「3.1 前提条件」で述べたように、CA サーバマシン及び HSM はセキュアエリア内に設置され、入退室管理が行われているため、また、管理端末マシンは、認証局内のマシンエリア内に設置されているため、外部の者が侵入して行う物理的な攻撃からは、保護されている。CA サーバマシン、管理端末マシンが接続される内部セグメントは、ファイアウォールによりインターネットからのアクセスを禁止しているため、不特定の利用者から攻撃される可能性はない。攻撃者としては、認証局を運用する組織の管理下にある、認証局に属する者を想定しているため、攻撃に対する動機及び機会が少ない脅威エージェントである。

従って、最小機能強度レベルは、**SOF-**基本が妥当であるといえる。

8.2.7. セキュリティ保証要件根拠

本 ST の TOE は、国際標準 X.509 に準拠した証明書の発行及び失効の管理業務を行うために使用される。発行される証明書は、公開鍵の所有者の身元を証明するために使用され、他の PKI アプリケーションにおける正当な利用者の根拠となるものである。そのため、TOE の動作には高い信頼性が求められる。

しかしながら、本 TOE は、外部ネットワークからのアクセスから保護され、また物理的にも不正なアクセスから保護された状態での使用が前提とされる、製品価格を考慮した商用目的の製品であるため、EAL4 ほどの高い評価保証レベルは要求されない。

従って、TOE の評価保証レベルは EAL3 を適用する。本 ST では、EAL３の保証要件の基本コンポーネントのみを適用する。追加コンポーネントは適用しない。

基本コンポーネントの記述は「Common Criteria for Information Technology Security Evaluation, Ver. 2.1, Part 3- Security assurance requirements (August 1999, CCIMB-99-033)」の定義に従う。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

本章では、TOE セキュリティ機能が TOE セキュリティ機能要件に対して必要かつ十分であることを記述する。TOE セキュリティ機能要件と TOE セキュリティ機能の対応関係を表 3 に示す。

「表 3： TOE セキュリティ機能要件と TOE セキュリティ機能の対応表」より、全ての TOE セキュリティ機能が､何らかの TOE セキュリティ機能要件の実現のために必要であることが示される。

FAU_GEN.1　　監査データ生成

＜根拠＞

SF.AUDIT は、表 4 に示した監査対象事象の監査ログを生成する。

「8.2.4 監査対象事象根拠」で述べた通り、各機能要件の監査対象とすべきアクションは、例外を除いて、本 TOE の監査対象事象として記録している。

また、例外に関しても CC Part2 で規定された監査対象とすべき最小レベルのアクションのうち、本 TOE において監査対象事象に含まれない根拠を説明している。

また、監査機能の起動と終了は、CA サーバの起動と停止に同期しているため、これらの事象により代用することができる。

従って **SF.AUDIT** により、**FAU_GEN.1** を実現できる。

FAU_GEN.2　　利用者識別情報の関連付け

＜根拠＞

SF.AUDIT は、監査記録時に、ECS 利用者 ID を記録することによって、当該事象をその原因となった ECS 利用者の識別情報に関連付けている。

従って **SF.AUDIT** により、**FAU_GEN.2** を実現できる。

FAU_SAR.1　　監査レビュー

＜根拠＞

SF.AUDIT は、監査者に監査ログの参照を許可する。また、**SF.AUDIT** は、通番、日付／時刻、コンポーネント名、ECS 利用者 ID、事象の種別、LogID、メッセージ、拡張情報を、表形式で表示する機能を提供する。

従って **SF.AUDIT** により、**FAU_SAR.1** を実現できる。

FAU_SAR.2　　限定監査レビュー

＜根拠＞

SF.AUDIT は、監査者にのみ監査ログの参照を許可し、監査者以外が監査ログを参照することはで

きない。
従って **SF.AUDIT** により、**FAU_SAR.2** を実現できる。

FAU_STG.1 保護された監査証跡格納

＜根拠＞
SF.AUDIT は、監査者にのみ監査ログの参照及び削除を許可し、監査者以外が監査ログを参照及び削除することはできない。また、**SF.AUDIT** は、**SF.CRYPTO** を使用して保存された監査ログに対する改竄を検知する。さらに、**SF.AUDIT** により監査事象に通番が割り振られるため、通番の抜けから監査ログの不正な削除を検出できる。
従って **SF.AUDIT**、**SF.CRYPTO** により **FAU_STG.1** を実現できる。

FAU_STG.4 監査データ損失の防止

＜根拠＞
SF.AUDIT は、ディスク容量不足が原因で監査ログの出力が不可能な場合、CA サーバを停止し、監査ログの出力に失敗した事象と CA サーバを停止した事象を OS に出力する。
従って **SF.AUDIT** により、**FAU_STG.4** は実現できる。

FCS_CKM.1a 暗号鍵生成

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

暗号鍵名称	標準	鍵生成アルゴリズム	鍵長
DB データ暗号鍵	ISO/IEC 9979/0009	MULTI2	256 bit

従って **SF.CRYPTO** により、**FCS_CKM.1a** を実現できる。

FCS_COP.1a 暗号操作

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

暗号操作名称	標準	暗号アルゴリズム	鍵長
DB データ暗号化／復号化	ISO/IEC 9979/0009	MULTI2	256 bit
ECS 利用者パスワード格納で使用するハッシュ	FIPS 180-1	SHA-1	----

従って **SF.CRYPTO** により、**FCS_COP.1a** を実現できる。

FCS_CKM.1b 暗号鍵生成

＜根拠＞

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

暗号鍵名称	標準	鍵生成アルゴリズム	鍵長
通信路暗号鍵	ISO/IEC 9979/0009	MULTI2	256 bit
通信路公開鍵／秘密鍵	PKCS#1	RSA	1024 bit

従って **SF.CRYPTO** により、**FCS_CKM.1b** を実現できる。

FCS_CKM.2b 暗号鍵配付

＜根拠＞

SF.CRYPTO は、以下の暗号鍵配付方法に関する標準に合致する、指定された暗号鍵配付方法に従って、暗号鍵の配付を行う。

暗号鍵名称	標準	鍵配付方法
通信路暗号鍵	ISO/IEC 9798	ISO/IEC 9798 通信路暗号鍵の共有

従って **SF.CRYPTO** により、**FCS_CKM.2b** を実現できる。

FCS_COP.1b 暗号操作

＜根拠＞

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

暗号操作名称	標準	暗号アルゴリズム	鍵長
通信路暗号化／復号化	ISO/IEC 9979/0009	MULTI2	256 bit
通信路暗号鍵の暗号化	PKCS#1	RSA	1024 bit

従って **SF.CRYPTO** により、**FCS_COP.1b** を実現できる。

FCS_CKM.1c 暗号鍵生成

＜根拠＞

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

暗号鍵名称	標準	鍵生成アルゴリズム	鍵長
監査ログ暗号鍵	FIPS 46-3	Triple-DES	168 bit
監査ログ署名公開鍵／秘密鍵	PKCS#1	RSA	512 bit

従って **SF.CRYPTO** により、**FCS_CKM.1c** を実現できる。

FCS_COP.1c　　暗号操作

＜根拠＞

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

暗号操作名称	標準	暗号アルゴリズム	鍵長
監査ログ署名／検定	PKCS#7	RSA	512 bit
監査ログ暗号化／復号化	FIPS 46-3	Triple-DES	168 bit
監査ログ署名で使用するハッシュ	FIPS 180-1	SHA-1	----

従って **SF.CRYPTO** により、**FCS_COP.1c** を実現できる。

FCS_COP.1d　　暗号操作

＜根拠＞

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

暗号操作名称	標準	暗号アルゴリズム	鍵長
秘密情報暗号化／復号化	FIPS 46-2	DES	56 bit
秘密情報暗号鍵暗号化／復号化	PKCS#5	PBE	64 bit

従って **SF.CRYPTO** により、**FCS_COP.1d** を実現できる。

FDP_ACC.1　　サブセットアクセス制御

FDP_ACF.1　　セキュリティ属性によるアクセス制御

＜根拠＞

SF.AC は、以下の規則に基づいてアクセス制御を実施する。

制御されたサブジェクト	制御された操作	制御されたオブジェクト
EE 証明書検索権限を持つ ECS 利用者の代行スレッド	読み出し	EE 証明書 オブジェクト
EE 証明書削除権限を持つ ECS 利用者の代行スレッド	削除	合議状態が成立した EE 証明書 オブジェクト
EE 証明書失効権限を持つ ECS 利用者の代行スレッド	改変	合議状態が成立した EE 証明書 オブジェクト
EE 証明書取得権限を持つ ECS 利用者の代行スレッド	読み出し	EE 証明書 オブジェクト
PKCS#12 データ作成権限を持つ ECS 利用者の代行スレッド	作成	合議状態が成立した以下のオブジェクト ・EE 証明書 オブジェクト ・PKCS#12 データ オブジェクト ・PKCS#12 パスワード オブジェクト
PKCS#12 データ取得権限を持つ ECS 利用者の代行スレッド	読み出し	PKCS#12 データ オブジェクト
PKCS#12 パスワード取得権限を持つ ECS 利用者の代行スレッド	読み出し	PKCS#12 パスワード オブジェクト
CRL 定義文登録権限を持つ ECS 利用者の代行スレッド	作成／改変	合議状態が成立した CRL 発行定義文 オブジェクト
CRL 定義文削除権限を持つ ECS 利用者の代行スレッド	削除	合議状態が成立した CRL 発行定義文 オブジェクト
CRL 作成権限を持つ ECS 利用者の代行スレッド	作成／改変	合議状態が成立した CRL オブジェクト
CRL 検索権限を持つ ECS 利用者の代行スレッド	読み出し	CRL オブジェクト
CRL 削除権限を持つ ECS 利用者の代行スレッド	削除	合議状態が成立した CRL オブジェクト
CRL 取得権限を持つ ECS 利用者の代行スレッド	読み出し	CRL オブジェクト

従って、**SF.AC** により、**FDP_ACC.1**、**FDP_ACF.1** を実現できる。

FIA_AFL.1　　認証失敗時の取り扱い

＜根拠＞

SF.I&A は、CA サーバでの ECS 利用者 ID と ECS 利用者パスワードの確認に 1 回でも失敗した場合、管理端末と CA サーバの間の当該コネクションを切断し、当該事象を監査ログに出力する。また、認証の再試行を 10 秒間受け付けない。
従って **SF.I&A** により、**FIA_AFL.1** を実現できる。

FIA_ATD.1　　利用者属性定義

＜根拠＞
SF.CA_MGT は、ECS 利用者に属するセキュリティ属性である ECS 利用者 ID、ECS 利用者パスワード、ECS 利用者権限リストを維持し、適切に管理する。
従って **SF.CA_MGT** により、**FIA_ATD.1** は実現できる。

FIA_SOS.1　　秘密の検証

＜根拠＞
SF.CA_MGT は、ECS 利用者の認証に使用するパスワードが以下の品質尺度を満たすことを検証するメカニズムを提供する。

項目	品質尺度
長さ	8~64 文字
使用可能な文字	半角英数字または半角記号
必要な文字	半角大文字英字、半角小文字英字、半角数字 及び半角記号

従って **SF.CA_MGT** により、**FIA_SOS.1** を実現できる。

FIA_UAU.1　　認証のタイミング
FIA_UID.1　　識別のタイミング

＜根拠＞
SF.I&A は、ECS 利用者の識別・認証を行う。TOE は、ECS 利用者の識別・認証が成功するまで、**SF.CRYPTO** の通信路暗号化以外のセキュリティ機能を使用しない。
従って **SF.I&A** により、**FIA_UAU.1**、**FIA_UID.1** を実現できる。

FIA_USB.1　　利用者･サブジェクト結合

＜根拠＞
SF.AC は、ECS 利用者の識別・認証が成功した後に、ECS 利用者の動作を代行するサブジェクトとして、代行スレッドを生成し、当該 ECS 利用者 ID を代行スレッドに関連付ける。
従って **SF.AC** により、**FIA_USB.1** を実現できる。

FMT_MOF.1　セキュリティ機能のふるまいの管理

＜根拠＞

SF.CA_MGT は、以下のセキュリティ機能のふるまいを管理する。

- DB 暗号化機能の動作／停止
- 監査ログ署名機能の動作／停止
- 監査ログ暗号化機能の動作／停止
- 合議機能の動作／停止

また、CA 管理者のみが、**SF.CA_MGT** の CA 情報設定機能の起動を要求でき、さらに CA 情報設定機能は、CA 情報設定合議を行った後に使用することができる。

従って **SF.CA_MGT** により、**FMT_MOF.1** を実現できる。

FMT_MSA.1a　セキュリティ属性の管理

FMT_MSA.1c　セキュリティ属性の管理

＜根拠＞

SF.CA_MGT は、以下の ECS 利用者のセキュリティ属性を管理する。

- ECS 利用者 ID
- ECS 利用者パスワード
- ECS 利用者権限リスト

また、CA 管理者のみが、**SF.CA_MGT** の CA 情報設定機能の起動を要求でき、さらに CA 情報設定機能は、CA 情報設定合議を行った後に使用することができる。

従って **SF.CA_MGT** により、**FMT_MSA.1a、FMT_MSA.1c** を実現できる。

FMT_MSA.1b　セキュリティ属性の管理

＜根拠＞

SF.CA_MGT は、ログインしている自分自身の ECS 利用者のパスワードを変更する機能を CA 管理者、監査者、運用者に提供する。

従って **SF.CA_MGT** により、**FMT_MSA.1b** を実現できる。

FMT_MSA.1d　セキュリティ属性の管理

＜根拠＞

SF.AC は、操作要求者と合議者の ECS 利用者 ID と、操作に必要な残りの合議人数を管理し、これらを変更する合議承認操作または合議否認操作を運用者に提供する。

従って **SF.AC** により、**FMT_MSA.1d** を実現できる。

FMT_MSA.2c　セキュアなセキュリティ属性

＜根拠＞
SF.CRYPTO は、監査ログ署名秘密鍵を使用する前に、対応する監査ログ用証明書の有効期限を確認し、有効期限切れの場合、事象を OS に出力する。
従って **SF.CRYPTO** により、**FMT_MSA.2c** を実現できる。

FMT_MSA.3　　静的属性初期化
＜根拠＞
SF.CA_MGT は、ECS 利用者を新規に登録した直後は、ECS 利用者権限リストのデフォルト値は、すべての操作に対する権限を持つように設定されている。また、CA 管理者だけが、**SF.CA_MGT** の CA 情報設定機能を使用して ECS 利用者権限リストを変更することができる。
CA 管理者のみが、**SF.CA_MGT** の CA 情報設定機能の起動を要求でき、さらに CA 情報設定機能は、CA 情報設定合議を行った後に使用することができる。
従って **SF.CA_MGT** により、**FMT_MSA.3** を実現できる。

FMT_MTD.1a　　TSF データの管理
＜根拠＞
SF.CA_MGT は、CA 設定情報及び ECS 利用者情報を管理する。また、CA 管理者のみが、**SF.CA_MGT** の CA 情報設定機能の起動を要求でき、さらに CA 情報設定機能は、CA 情報設定合議を行った後に表示され、使用することができる。
従って **SF.CA_MGT** により、**FMT_MTD.1a** を実現できる。

FMT_MTD.1b　　TSF データの管理
＜根拠＞
SF.AUDIT は、監査者にのみ監査ログの参照、削除及び取得を許可し、監査者以外が監査ログを参照、削除及び取得することはできない。すなわち、監査ログを問い合わせ、削除、取得する機能は、監査者に制限されている。
従って **SF.AUDIT** により、**FMT_MTD.1b** を実現できる。

FMT_SMR.1　　セキュリティ役割
＜根拠＞
SF.CA_MGT は、CA 情報設定権限を持つ ECS 利用者を CA 管理者という役割、監査権限を持つ ECS 利用者を監査者という役割、これら以外の ECS 利用者権限を持つ ECS 利用者を運用者として維持する。
従って **SF.CA_MGT** により、**FMT_SMR.1** を実現できる。

FMT_SMF.1　　管理機能の特定

＜根拠＞
SF.CA_MGT は、CA 設定情報の管理機能及び ECS 利用者情報の管理機能を提供する。
「8.2.5 セキュリティ管理機能根拠」で述べた通り、各機能要件の管理対象とすべきアクティビティは、例外を除いて、本 TOE の管理機能で管理している。また、例外に関しても CC Part2 で規定された管理対象とすべきアクティビティのうち、本 TOE において管理対象事象に含まれない根拠を説明している。
従って **SF.CA_MGT** により、**FMT_SMF.1** を実現できる。

FPT_RVM.1　　TSP の非バイパス性
＜根拠＞
SF.I&A と **SF.AC** は、TSC 内の各機能の動作が許可される前に、TSP 実施機能が呼び出され成功することを保証する。
従って **SF.I&A**、**SF.AC** により、**FPT_RVM.1** を実現できる。

FPT_SEP.1　　TSF ドメイン分離
＜根拠＞
本要件は、全てのセキュリティ機能によって、実現されることが保証される。
従って全てのセキュリティ機能により、**FPT_SEP.1** を実現できる。

FPT_STM.1　　高信頼タイムスタンプ
＜根拠＞
SF.AUDIT は、監査ログの記録に必要なタイムスタンプ情報を提供する。
従って **SF.AUDIT** により、**FPT_STM.1** を実現できる。

以上より、全ての TOE セキュリティ機能要件が必要とする機能を、TOE セキュリティ機能が提供していることが示される。

8.3.2. セキュリティ機能強度根拠

本 TOE において、確率的かつ順列的メカニズムに基づくセキュリティ機能は、**SF.CA_MGT**、**SF.I&A** で実現する ECS 利用者のパスワードに関する機能、及び **SF.CRYPTO** のハッシュアルゴリズムを用いた暗号機能がある。このセキュリティ機能強度は、6.2 節において、機能強度レベル **SOF-**基本を指定している。また、本 TOE の最小機能強度は、5.3 節において、**SOF-**基本を指定している。従って両者は一貫している。

8.3.3. 保証手段根拠

本章では、セキュリティ保証手段がセキュリティ保証要件（EAL3）の評価コンポーネントに対して必要かつ十分であることを記述する。セキュリティ保証要件とセキュリティ保証手段の対応関係を表 5 に示す。

「表 5： セキュリティ保証要件（EAL3）とセキュリティ保証手段の対応表」より、全てのセキュリティ保証手段が、何らかの保証コンポーネントの実現のために必要であることが示される。

ACM_CAP.3 (許可の管理)：

(1) Enterprise Certificate Server Set 構成管理文書 は以下の内容を含む。

- TOE のバージョン識別とバージョン命名規則
- TOE の構成要素リスト
- TOE の構成管理計画

従って、上記（1）により **ACM_CAP.3** を実現できる。

ACM_SCP.1 (TOE の CM 範囲)：

(1) Enterprise Certificate Server Set 構成管理文書 は以下の内容を含む。

- TOE のバージョン識別とバージョン命名規則
- TOE の構成要素リスト

従って、上記（1）により **ACM_SCP.1** を実現できる。

ADO_DEL.1 (配付手続き)：

(2) Enterprise Certificate Server Set 配付文書 は以下の内容を含む。

- TOE を利用者サイトへ配送するときのセキュリティを維持するために必要な手続き

従って、上記（2）により **ADO_DEL.1** を実現できる。

ADO_IGS.1 (設置、生成及び立上げ手順)：

(3) Enterprise Certificate Server Set システムセキュリティガイド は以下の内容を含む。

- TOE のセキュアな設置・生成・立上げに必要な手順

従って、上記（3）により **ADO_IGS.1** を実現できる。

ADV_FSP.1 (非形式的機能仕様)：

(4) Enterprise Certificate Server Set 機能仕様書 は以下の内容を含む。

- TOE セキュリティ機能の識別と仕様
- TSF インタフェースの識別と仕様

従って、上記（4）により **ADV_FSP.1** を実現できる。

ADV_HLD.2 (セキュリティ実施上位レベル設計)：

(5) Enterprise Certificate Server Set 構造設計書 は以下の内容を含む。

- TSP を実施するサブシステムの識別と仕様
- サブシステム間インタフェースの識別と仕様
- 前提 IT 環境（ハードウェア、ソフトウェア）の識別
- 前提 IT 環境で実装される補助的な保護メカニズムの仕様

従って、上記（5）により **ADV_HLD.2** を実現できる。

ADV_RCR.1 (非形式的対応の実証)：

(6) Enterprise Certificate Server Set 対応分析書 は以下の内容を含む。

- ST の TOE セキュリティ機能と、上記機能仕様書の TSF インタフェースとの対応関係
- 上記機能仕様書の TSF インタフェースと、上記構造設計書のサブシステム間インタフェースとの対応関係

従って、上記（6）により **ADV_RCR.1** を実現できる。

AGD_ADM.1 (管理者ガイダンス)：

(3) Enterprise Certificate Server Set システムセキュリティガイド は以下の内容を含む。

- TOE の前提環境
- TOE 管理におけるセキュリティ上の注意事項
- 管理者が利用できる TOE のセキュリティ機能とインタフェース
- TOE のセキュアな管理方法

従って、上記（3）により **AGD_ADM.1** を実現できる。

AGD_USR.1 (利用者ガイダンス)：

本 TOE は、一般利用者は利用しないので、利用者ガイダンスは提供しない。

従って、**AGD_USR.1** は満たしている。

ALC_DVS.1 (セキュリティ手段の識別)：

(7) Enterprise Certificate Server Set 開発セキュリティ規程書 は以下の内容を含む。

- 開発環境において、TOE に関連する資産を保護するための手続き
- 上記手続きを実施した際の証跡

従って、上記（7）により **ALC_DVS.1** を実現できる。

ATE_COV.2 (カバレージの分析)：

(9) Enterprise Certificate Server Set テスト分析書 は以下の内容を含む。

- 上記機能仕様書の TSF インタフェースと、上記テスト仕様書／報告書のテスト項目との対応関係

従って、上記（9）により **ATE_COV.2** を実現できる。

ATE_DPT.1 (テスト：上位レベル設計)：

(9) Enterprise Certificate Server Set テスト分析書 は以下の内容を含む。

- 上記構造設計書のサブシステム間インタフェースと、上記テスト仕様書／報告書のテスト項目との対応関係

従って、上記（9）により **ATE_DPT.1** を実現できる。

ATE_FUN.1 (機能テスト)：

(8) Enterprise Certificate Server Set テスト仕様書／報告書 は以下の内容を含む。

- テスト計画
- テスト項目
- テスト手順
- 期待されるテスト結果及び実際のテスト結果

従って、上記（8）により **ATE_FUN.1** を実現できる。

ATE_IND.2 (独立テスト - サンプル)：

(12) Enterprise Certificate Server Set により、評価者が TOE のテストを行う際、上記テスト仕様書／報告書で実施されたものと同等のテスト環境を提供する。

従って、上記（１２）により **ATE_IND.2** を実現できる。

AVA_MSU.1 (ガイダンスの検査)：

(3) Enterprise Certificate Server Set システムセキュリティガイド は以下の内容を含む。

- TOE の前提環境
- TOE 管理におけるセキュリティ上の注意事項

従って、上記（3）により **AVA_MSU.1** を実現できる。

AVA_SOF.1 (TOE セキュリティ機能強度評価)：

(10) Enterprise Certificate Server Set セキュリティ機能強度分析書 は以下の内容を含む。

- ST で記述したセキュリティ機能強度に対する分析

従って、上記（１０）により **AVA_SOF.1** を実現できる。

AVA_VLA.1 (開発者脆弱性分析)：

(11) Enterprise Certificate Server Set 脆弱性分析書 は以下の内容を含む。

- TOE が持つ脆弱性の識別
- 識別した脆弱性が TOE の想定した運用環境では顕在化しないこと

従って、上記（１１）により **AVA_VLA.1** を実現できる。

以上より、全ての評価コンポーネントが必要とする評価証拠を、セキュリティ保証手段が提供していることが示される。

8.4. PP 主張根拠

参照した PP はない。