統合化プラットフォーム・セキュリティ評価ガイドライン

1.0 版

2006 年 3 月 17 日

NICT

電磁波計測部門 タイムアプリケーショングループ

※注意事項
本ガイドラインは確定したものではありません。随時変更が入る可能性があります。ご了承願います。

適用範囲

本ガイドは、「時刻認証基盤技術実験装置－統合化プラットフォームシステム（Experimental System of Time Stamping Based on the Japan Standard Time – Integrated Platform Systems - ）仕様書」（平成 17 年 4 月 1 日、独立行政法人　情報通信研究機構）に記載された「統合化プラットフォームシステム」に適用される。統合化プラットフォームシステム、及び構成要素となる各サブシステム（これらをセキュリティ評価対象システム、あるいは、評価対象システムと呼ぶ）のセキュリティを評価する際に適用する。

目的

本ガイドは、統合化プラットフォームシステム及び各サブシステムのセキュリティ評価を容易かつ正規化した形で実施できるようにするために、セキュリティ評価の手順を取り纏め、セキュリティ評価の手引きとなることを目的とする。

内容

本ガイドは、セキュリティ評価に関する国際標準 ISO/IEC 15408 の考えに従って、評価対象システムにおけるセキュリティ環境の導出作業、脅威分析、セキュリティ目標の決定、そして、セキュリティ機能の策定及び評価を行うための指針を取りまとめたものである。

改変履歴

項番	作成/変更年月日	変更番号	作番	枚数	作成/変更	審査	承認	変更内容
1	05.10.20				谷川			新規作成(0.9 版)
2	06.03.17				谷川			統合化プラットフォームシステムのセキュリティ評価作業を踏まえた修正・追加(1.0 版)
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

目次

1 セキュリティ評価の考え方

1.1 セキュリティ評価とは

本ガイドは、セキュリティ評価に関する国際標準 ISO/IEC 15408 の考え方に基づいている。そのため、セキュリティ評価とは、評価対象システム（Target of Evaluation: TOE）におけるセキュリティ環境の導出、脅威分析、セキュリティ目標の決定、そして、セキュリティ機能の策定及び評価を行うことを意味する。

1.2 統合化プラットフォームシステムのセキュリティ評価

統合化プラットフォームシステムは、複数のサブシステムから構成されたシステムである（図 1-1）。

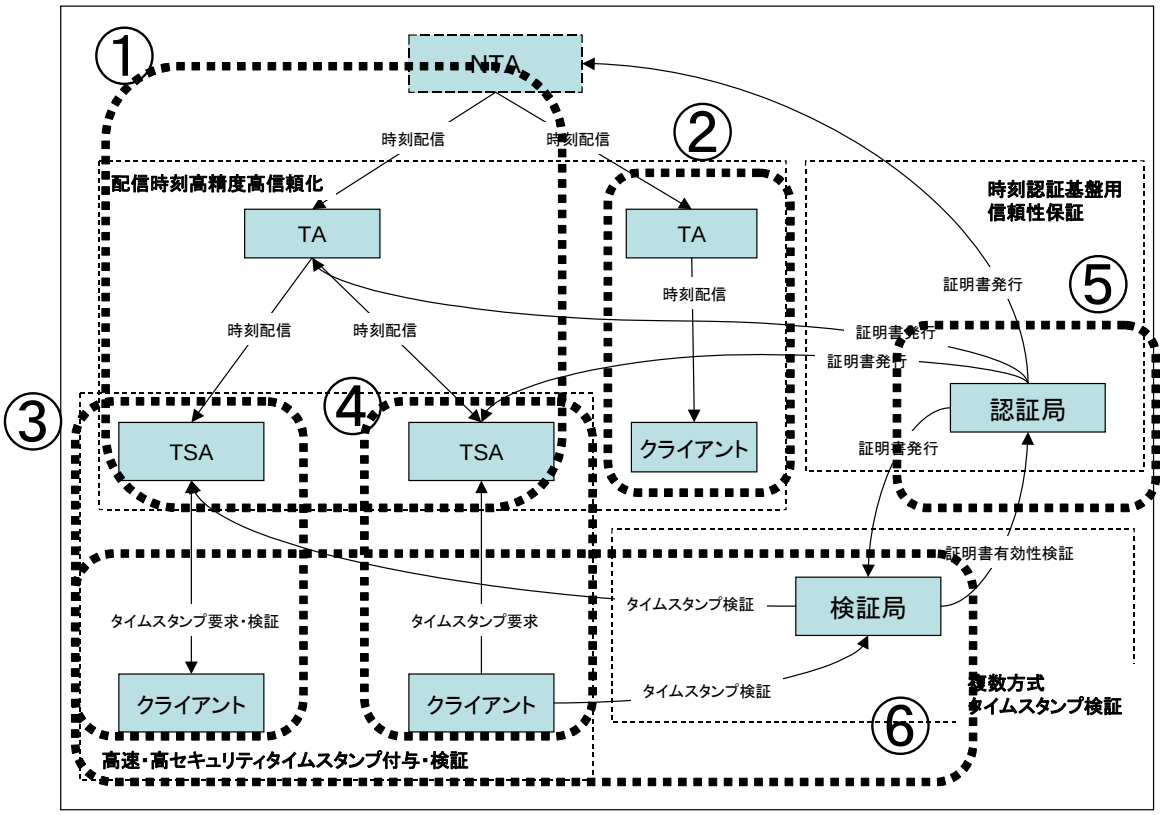

図 1-1：統合化プラットフォームシステム（出典：NICT：時刻認証基盤技術実験装置－統合化プロトタイプシステム－仕様書, 2004）

図 1-1に含まれる番号に対応するサブシステムの説明は、表 1-1の通りである。これらのサブシステムは、予め意図されたインタフェースを介して関係するサブシステムと通信を行う。

表 1-1：統合化プラットフォームシステムにおけるサブシステム

#	サブシステム名	説明

1	配信時刻高精度高信頼化サブシステム-2	配信時刻の高信頼化を実現するサブシステムである。 時刻配信のサービスを実施する主体は、TA(Time Authority)と呼ばれる。
2	配信時刻高精度高信頼化サブシステム-3	時刻情報のトレーサビリティを保証するサブシステムである。 時刻情報のトレーサビリティを保証する主体は、TA(Time Authority)と呼ばれる。
3	高速・高セキュリティタイムスタンプ付与・検証サブシステム-1	リンクトークン方式のタイムスタンプトークンを発行するサブシステムである。 タイムスタンプトークンを発行する主体は、TSA(Time-Stamping Authority)と呼ばれる。
4	高速・高セキュリティタイムスタンプ付与・検証サブシステム-2	独立トークン方式のタイムスタンプトークンを発行するサブシステムである。 タイムスタンプトークンを発行する主体は、TSA(Time-Stamping Authority)と呼ばれる。
5	時刻認証基盤用信頼性保証サブシステム	統合化プラットフォームシステムで使用される公開鍵証明書を発行するサブシステムである。 公開鍵証明書を発行する主体は、認証局（CA: Certification Authority）と呼ばれる。
6	複数方式タイムスタンプ検証サブシステム	独立トーク方式とリンクトークン方式のタイムスタンプを統一的に検証するサブシステムである。 検証サービスの主体は、検証局（VA: Validation Authority）と呼ばれる。

統合化プラットフォームシステムのセキュリティ評価とは、構成要素となる各サブシステムにおける外部とのインタフェースを明確にし、これらの各サブシステムに対してセキュリティ評価することと定義する。

また、通信ネットワークを用いないオフライン的な処理に関しては、セキュリティ評価対象外とする。例えば、CD-ROM などのメディアに格納されたデータの郵送、や、紙ベースの書面を用いた申請や通知などの手続きは、対象外となる。

2 セキュリティ評価手順の概要

2.1 セキュリティ評価作業内容

本ガイドが想定するセキュリティ評価作業内容は、以下の通りである(表 2-1)。

表 2-1:セキュリティ評価作業内容

#	項目	説明
1	評価システムの明確化	セキュリティ評価対象の物理配置構成、ネットワーク構成、システム構成、ソフトウェア構成、及び外部インタフェース(物理、論理、組織)を明確化する。
2	関与者の明確化	システムの関与者及び役割を明確化する。
3	資産の明確化	保護が必要な資産(一般的には、IT 環境の中の情報やリソース、あるいは、TOE 自体)を記述する。
4	セキュリティ環境の明確化	ISO/IEC 15408 や関係ドキュメントの考え方に基づき「セキュリティ環境(前提、脅威、組織のセキュリティポリシー)」を記述する。 ※ここで述べる「脅威」はあくまで、雛形をベースにカスタマイズしたものである。網羅性を高めるため、下記の「脅威分析」で、再度、脅威を抽出・検討する。
5	脅威分析	Microsoft 社のモデルを用いて、脅威抽出、リスク評価を行う。
6	セキュリティ目標の決定	ISO/IEC 15408 や関係ドキュメントの考え方に基づき「セキュリティ目標」を決定する。
7	セキュリティ機能の策定	ISO/IEC 15408 や関係ドキュメントの考え方に基づき「セキュリティ機能」を策定する。
8	セキュリティ機能の評価	実装されたセキュリティ機能を評価する。

セキュリティ評価手順及び各作業項目との関係性の模式図を示す(図 2-1)。ISO/IEC 15408 や関連ドキュメントを参照し、セキュリティ評価作業を実施する。

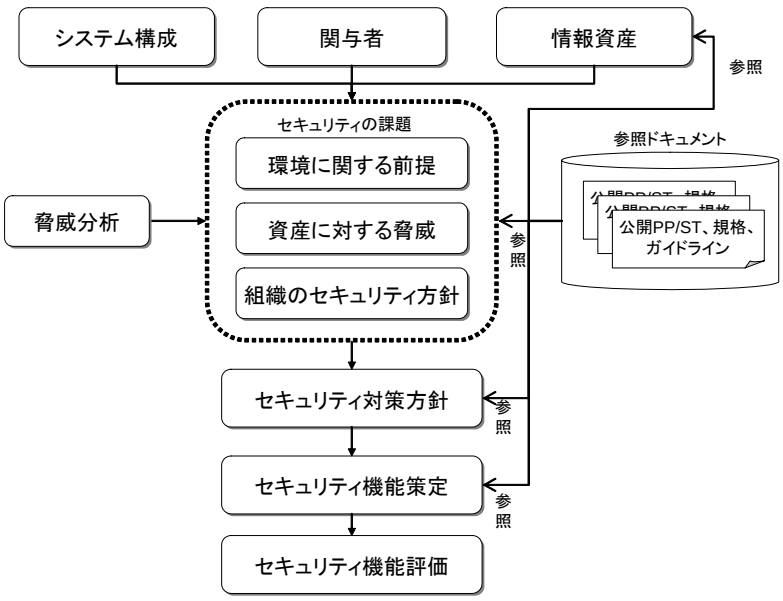

図 2-1:セキュリティ評価手順

なお、「セキュリティ機能の策定」フェーズでは、ISO/IEC 15408 で規定された「セキュリティ機能」の選定、あるいは、カスタマイズを想定するが、高いスキルを要する作業であるため、この作業を必須とはしない。作業を行わない場合は、「セキュリティ対策方針」フェーズにて、セキュリティ機能に関わる記述を含めるようにする。

2.2 参照ドキュメント一覧

本ガイドで参照するドキュメントは、以下の通りである(表 2-2)。セキュリティ評価に関わる国際規格、認定済みのST、セキュリティ評価に関するガイドブックを参照する。

表 2-2:参照ドキュメント

#	ドキュメント名	説明
1	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model January 2004 Version 2.2	IT製品やITシステムのセキュリティ評価基準。概要を示す。CC Ver.2.2 は、CC Ver.2.1(ISO/IEC 15408-1:1999 と同等)に補足版(CCIMB Interpretation-0407)を反映させたものである[1]。 セキュリティ評価のための概念及び内容を理解するために使用する。
2	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements January 2004 Version 2.2	IT 製品や IT システムのセキュリティ評価基準。評価対象のセキュリティ機能要件を示す。 統合化プラットフォームに含まれる各サブシステムにおけるセキュリティ機能要件のカタログとして参照する。
3	ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management	ISO/IEC 13335 シリーズは、情報通信技術のセキュリティ管理のガイドライン。パート1は、概念とモデルを示す。 セキュリティ評価のための概念及び内容を理解するために使用する。
4	ISO/IEC TR 15446:2004 Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets	PP/ST を作成するための標準規格(ISO/IEC 規格のテクニカル・レポート)。附属として、汎用システムと暗号機能などに関する「セキュリティ環境」の記述例が掲載されている。 統合化プラットフォームに含まれる全てのサブシステムに適用される。
5	Security Target for Baltimore Timestamp Server version 2.0.2 Patch 1(3rd Oct 2003)	Baltimore 社の PKI ベースのタイムスタンプサーバの ST 統合化プラットフォームにおけるTSA(特にPKIベースのTSA)に適用される。
6	Enterprise Certificate Server Set セキュリティターゲット Version 1.10 2004/06/24	日立製作所の認証局サーバの ST 統合化プラットフォームにおける CA に適用される。
7	脅威モデル セキュアなアプリケーション構築 Frank Swiderski、Window Snyder 著、日経 BP ソフトプレス(2005)	システム、アプリケーション、API を例とした脅威抽出や分析などの実践ガイドライン。Microsoft 社の脅威モデルを採用している。

[1] 国内では、IPA のセキュリティセンターが CC の日本語訳を提供している。「CC Ver.2.1 の日本語訳 第 1.2 版」、「補足-0407」、「補足-0201 第 2 版」から構成されるドキュメントは、CC Ver.2.2 と同等内容である。国内の IT セキュリティ評価及び認証制度(JISEC)は、CC Ver.2.2 に基づいている。なお、参考の位置づけで公開されている「CC Ver.2.1 の日本語訳 第 1.4 版」は、「CC Ver.2.1 の日本語訳 第 1.2 版」に「補足-0407」及び「補足-0201 第 2 版」の内容を反映させたものである。

		統合化プラットフォームにおける脅威分析のためのガイドライン。

2.3 用語の定義

本ガイドで使用されるセキュリティ評価に関する用語は、基本的に、ISO/IEC 15408、ISO/IEC 13335、ISO/IEC TR 15446 基づくものである。

ISO/IEC 15408 では、セキュリティ評価に係る用語が定義されている。重要な用語に関して以下に示す(表 2-3)。なお、日本語訳に関しては、IPAがWebサイト上で公開するCC V.2.1 の日本語訳に基づく[2]。

表 2-3:ISO/IEC 15408 で規定された用語

#	用語	説明
1	資産 (Assets)	TOE の対抗策が保護すべき情報または資源。 Information or resources to be protected by the countermeasures of a TOE.
2	割付 (Assignment)	コンポーネント内の識別されたパラメタの仕様。 The specification of an identified parameter in a component.
3	保証 (Assurance)	エンティティがそのセキュリティ対策方針を満たしていることを信頼するための根拠。 Grounds for confidence that an entity meets its security objectives.
4	攻撃能力 (Attack potential)	攻撃が開始された場合に、攻撃が成功すると認められる可能性を、攻撃者の技能、資源、及び動機の観点から表現したもの。 The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
5	認証データ (Authentication data)	要求される利用者の識別情報を検証する際に用いられる情報。 Information used to verify the claimed identity of a user.
6	許可された利用者[3] (Authorised user)	TSP に従って操作を実行することができる利用者。 A user who may, in accordance with the TSP, perform an operation.
7	クラス (Class)	共通の対象を共有するファミリのグループ。 A grouping of families that share a common focus.
8	コンポーネント (Component)	選択可能な最小のエレメントのセットで、PP、ST、またはパッケージに含まれる可能性がある。 The smallest selectable set of elements that may be included in a PP, an ST, or a package.
9	接続性 (Connectivity)	TOE と外部の IT エンティティとの対話を可能にする TOE の特性。これには、任意の環境または構成において任意の距離を介して、有線または無線手段によって行われるデータ交換が含まれる。 The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
10	依存性 (Dependency)	依存する側の要件の目的を達成できるようにするには、依存される側の要件を正常に満たさなければならないという要件間の関係。 A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

[2] 参考の位置づけとなる「CC Ver.2.1 の日本語訳 第1.4版」を参照した。
[3] 悪意者が「ある手段」を用いて、正当な利用者に成りすまし、システムにアクセスした場合、その状態の悪意者を「許可された利用者」と呼ぶのかどうかは、文脈に依存する。

11	エレメント (Element)	不可分のセキュリティ要件。 An indivisible security requirement.
12	外部 IT エンティティ (External IT entity)	信頼の如何にかかわらず、TOE の外部にあって TOE と対話する任意の IT 製品またはシステム。 Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
13	ファミリ (Family)	セキュリティ対策方針を共有するが、重点または厳密さが異なるコンポーネントのグループ。 A grouping of components that share security objectives but may differ in emphasis or rigour.
14	人間の利用者 (Human user)	TOE と対話する任意の人。 Any person who interacts with the TOE.
15	識別情報 (Identity)	許可された利用者を一意に識別する表現(例えば、文字列)で、その利用者のフルネームまたは略称、または仮名。 A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
16	内部通信チャネル (Internal communication channel)	TOE 内部の別々の部分間の通信チャネル。 Communicating data between separated parts of the TOE.
17	TOE 内転送 (Internal TOE transfer)	TOE 内部の別々の部分間でデータを通信すること。 Communicating data between separated parts of the TOE.
18	TSF 間転送 (Inter-TSF transfers)	TOE と他の信頼できる IT 製品のセキュリティ機能との間でデータを通信すること。 Communicating data between the TOE and the security functions of other trusted IT products.
19	繰返し (Iteration)	様々な操作で 2 回以上、コンポーネントを使用すること。 The use of a component more than once with varying operations.
20	オブジェクト (Object)	情報を内蔵または受信し、サブジェクトによる操作の実行対象となる TSC 内のエンティティ。 An entity within the TSC that contains or receives information and upon which subjects perform operations.
21	組織のセキュリティ方針 (Organisational security policies)	組織がその業務に対して課す 1 つまたは複数のセキュリティ規則、手続き、慣行、またはガイドライン。 One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.
22	プロテクションプロファイル (Protection Profile (PP))	ある TOE の分野に関して特定の消費者ニーズを満たす、実装に依存しないセキュリティ要件のセット。 An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
23	パッケージ (Package)	A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives. 識別されたセキュリティ対策方針を満たすために組み合わされた、再利用可能な機能コンポーネントまたは保証コンポーネント(例えば、EAL)のセット。
24	製品 (Product)	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. 様々なシステム内での使用、または組込みを目的に設計された機能性を提供する IT ソフトウェア、ファームウェア、及び/またはハードウェアのパッケージ。
25	プロテクションプロファイル	ある TOE の分野に関して特定の消費者ニーズを満たす、実装に依存しないセキュリティ要件のセット。

	(Protection Profile 、PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
26	リファレンスモニタ (Reference monitor)	TOE アクセス制御方針を実施する抽象機械の概念。 The concept of an abstract machine that enforces TOE access control policies.
27	リファレンス確認メカニズム (Reference validation mechanism)	改ざん不能であり、常に呼び出され、かつ詳細な分析とテストを受けるのに十分なほど簡潔であるという特性を有するリファレンスモニタ概念の実装。 An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.
28	詳細化 (Refinement)	コンポーネントに詳細を追加すること。 The addition of details to a component.
29	役割 (Role)	利用者と TOE との間に許可される対話を規定する定義済み規則のセット。 A predefined set of rules establishing the allowed interactions between a user and the TOE.
30	秘密 (Secret)	特定の SFP を実施するために許可された利用者、及び/または TSF にしか知らせてはならない情報。 Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.
31	セキュリティ属性 (Security attribute)	TSP の実施のために使用される、サブジェクト、ユーザ、オブジェクト、情報及び/または、資源の特性。 Characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP.
32	セキュリティ機能 (Security Function (SF))	TSP の密接に関連する規則のサブセットを実施するために、必要としなければならない TOE の一部分または複数の部分。 A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
33	セキュリティ機能方針 (Security Function Policy (SFP))	SF によって実施されるセキュリティ方針。 The security policy enforced by an SF.
34	セキュリティ対策方針 (Security objective)	識別された脅威への対抗、及び/または識別された組織のセキュリティ方針、及び前提条件を満たすことを目的とする方針。 A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.
35	セキュリティターゲット (Security Target (ST))	識別された TOE の評価の基礎として用いられるセキュリティ要件及び仕様のセット。 A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
36	選択 (Selection)	コンポーネント内のリストから 1 つまたは複数の項目を指定すること。 The specification of one or more items from a list in a component.
37	サブジェクト (Subject)	実行すべき操作の原因となる TSC 内のエンティティ。 An entity within the TSC that causes operations to be performed. サブジェクトの例としては、 • 許可されたユーザの代理として動作するプロセス(例:UNIX プロセス) • TOE 自体の一部として動作するもの(例:信頼されたプロセス)
38	システム (System)	特定の目的と運用環境を伴う特定の IT 設備。 A specific IT installation, with a particular purpose and operational environment.
39	評価対象 (Target of Evaluation (TOE))	評価の対象となる IT 製品またはシステム、及び関連する管理者/利用者ガイダンス文書。 An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

40	TOE 資源 (TOE resource)	TOE 内において使用可能または利用可能なもの。 Anything useable or consumable in the TOE.
41	TOE セキュリティ機能 (TOE Security Functions (TSF))	TSP の正しい実施のために必要としなければならない TOE のすべてのハードウェア、ソフトウェア、及びファームウェアからなるセット。 A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
42	TOE セキュリティ機能インタフェース (TOE Security Functions Interface、TSFI)	対話(マンマシンインタフェース)またはプログラミング(アプリケーションプログラミングインタフェース)の如何にかかわらず、それを介して TOE 資源にアクセスしたり、TSF が仲介したり、TSF から情報を取得したりするインタフェースのセット。 A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
	TOE セキュリティ方針 (TOE Security Policy (TSP))	TOE 内での資産の管理方法、保護方法、及び配付方法を規定する規則のセット。 A set of rules that regulate how assets are managed, protected and distributed within a TOE.
43	TSF 制御範囲外転送 (Transfers outside TSF control)	TSF の制御下にないエンティティとデータを通信すること。 Communicating data to entities not under control of the TSF.
44	高信頼チャネル (Trusted channel)	TSF と相手側の信頼できる IT 製品が、TSP をサポートするのに必要な信頼度を持って通信することができる手段。 A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.
45	高信頼パス (Trusted path)	利用者と TSF が TSP を支持するのに必要な信頼度を持って通信する手段。 A means by which a user and a TSF can communicate with necessary confidence to support the TSP.
46	TSFデータ[4] (TSF data)	TOE によって作成された及び TOE に関して作成されたデータであり、TOE の動作に影響を与える可能性のあるもの。 Data created by and for the TOE that might affect the operation of the TOE.
47	TSF 制御範囲 (TSF Scope of Control, TSC)	TOE に対してまたは TOE 内で発生することができ、かつ TSP の規則を条件とする制御のセット。 The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
48	利用者 (User)	TOE の外部にあって TOE と対話する任意のエンティティ(人間の利用者または外部 IT エンティティ)。 Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
49	利用者データ (User data)	利用者によって作成された及び利用者に関して作成されたデータであり、TSF の動作に影響を与えないもの。 Data created by and for the user, that does not affect the operation of the TSF.

ISO/IEC 13355 では、セキュリティの概念に係る重要な用語が定義されている。用語を以下に記す(表 2-4)。

表 2-4:ISO/IEC 13355 で規定された用語

#	用語	説明
1	責任追跡可能性 (Accountability)	エンティティの行為がそのエンティティによって行われたものであることを保証すること。そのエンティティに追跡できること。

[4] 「TSF データ」は、利用者からは見えないデータでもある。ISO/IEC 15408 では、セキュリティ評価で注目されたデータは、「TSF データ」、あるいは、「利用者データ」に区別される。

		The property that ensures that the actions of an entity may be traced uniquely to the entity [ISO/IEC 7498-2]
2	真正性(Authenticity)	サブジェクト、あるいはリソースのアイデンティティが、主張されたものであると保証すること。ユーザ、プロセス、システム、情報などのエンティティに適用される。 The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information
3	可用性(Availability)	許可されたエンティティの要求時に、アクセス・使用できること。 The property of being accessible and usable upon demand by an authorized entity [ISO/IEC 7498-2]
4	機密性(Confidentiality)	許可されない個人、エンティティ、プロセスに対して情報を利用できるようにしない、すなわち暴露しないこと。 The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 7498-2]
5	完全性(Integrity)	資産の正確性と完全性を保護すること。 The property of safeguarding the accuracy and completeness of assets
6	信頼性(Reliability)	一貫性のある意図された動作と結果。 The property of consistent intended behaviour and results

ISO/IEC TR 15446 の附属書Cにおいて、暗号機能に関するセキュリティ評価指針が記載されている。ここでは、暗号機能に関する用語が定義されている。重要な用語を以下に示す（表 2-5）。なお、日本語訳に関しては、IPAがWebサイト上で公開するISO/IEC TR 15446 WD N3374 の日本語訳に基づく。

表 2-5：ISO/IEC TR 15446 で規定された暗号機能に関する用語

#	用語	説明
1	暗号機能 (Cryptographic Function)	暗号アルゴリズムによって実行される計算の一つ。例: 暗号化、復号、デジタル署名生成、デジタル署名検証など。 One of the computations performed with a cryptographic algorithm. Examples: encryption, decryption, digital signature generation, digital signature verification, etc.
2	暗号変数 (Cryptographic Variable (CV))	アルゴリズム入力を出力へ変換するための暗号アルゴリズムの操作のために必要となる、一つのまたは連続した値。暗号変数の例は、暗号鍵 (共通、公開、秘密、その他)、公開鍵パラメタ、及び初期化ベクターである (平文、暗号文、及びハッシュ値は暗号変数とはみなされないことに注意)。 A value or series of values required for the operation of the cryptographic algorithm in order to transform the algorithm input to output. Examples of cryptographic variable are cryptographic keys (secret, public, private, etc.), public key parameters, and initialisation vectors. (Note that plaintext, cyphertext and hash values are not considered to be cryptographic variables.)
3	初期化ベクター (Initialisation Vector)	暗号アルゴリズムの中で、暗号化の出発点を定義するために暗号鍵に関連して用いられるベクター (ビットの連なり)。 A vector (series of bits) used in conjunction with a cryptographic key to define the starting point of encryption within a cryptographic algorithm.
4	呼び出しパラメタ	暗号機能にアクセスするため、TOE に供給される秘密 (例えば、パスワード、または個人識

	(Invocation Parameter)	別番号)。 A secret (e.g., a password or personal identification number) which is supplied to a TOE to access a cryptographic function.

「脅威モデル」では、脅威分析に関する用語が定義されている(表 2-6)。ISO/IEC 15408 で定義された用語も含まれる。これらの違いに関しては、備考に示される。

表 2-6:Microsoft 社の脅威モデルで規定された用語

#	用語	説明	備考
1	資産(asset)	攻撃者の不正使用からシステムが守られなければならない抽象的または具体的なリソース	ISO/IEC 15408(CC)の「資産(assets)」と同等の意味。
2	攻撃経路(attack path)	攻撃目標(脅威)に到達するために通過しなければならない脅威ツリーの中の一連の条件。有効な攻撃経路(条件に対する軽減策のないもの)	
3	条件(condition)	攻撃経路に存在し、脅威に対する軽減策がとられなければ脆弱性として攻撃に利用されうる単一のアクションまたは弱点。	
4	DREAD	条件や脆弱性に関するリスクのランク。潜在的損失(D: Damage potential)、再現性(R: Reproducibility)、攻撃利用可能性(E: Exploitability)、影響ユーザ(A: Affected users)、発見可能性(D: Discoverability)から成る。	
5	エントリポイント(entry point)	システムが外界に対して持つインタフェース、つまり、システムがコントロールする機能とコントロールできない機能との境界となるポイント。	
6	外部依存性(external dependency)	モデル化対象のシステムの潜在的脆弱性を防ぎ、セキュリティを守る上で、別システムに依存する度合い。	
7	外部エンティティ(external entity)	モデル化対象のシステム外にあり、1つ以上のエントリポイントを通して対象システムと相互作用できるシステム、ユーザ、または、他のコンポーネント。	
8	リスク(risk)	脆弱性またはコンディションの危険の特性	
9	セキュリティの強さ(security strength)	システムの脅威軽減の有効性	
10	セキュリティの弱さ(security weakness)	システムの脅威に対して軽減策が不十分なところ。通常は、これが脆弱性につながる。	
11	STRIDE	脅威の現れ方を示す分類体系。成りすまし(S: Spoofing)、改ざん(T: Tampering)、否認(R: Repudiation)、情報漏洩(I: Information disclosure)、DoS 攻撃(Denial of service)、権限昇格(E: Elevation of privilege)から成る。	
12	システム(system)	1つ以上のコンポーネント(機能領域)にまたがる機能の集合体。システムは、特定の機能を外部エンティティ(システムのコントロール外にあり相互作用を持つもの)に公開し、守るべき資産を持つ。	
13	脅威(threat)	攻撃者の目標、または、攻撃者がシステムに対して試みること(システムに対するすべての脅威の集合が脅威プロファイルとなる)。軽減策をとろうととるまいと、システムに対する脅威は常に存在する。	ISO/IEC 15408(CC)では、用語としては定義されていないが、脅威とは、情報資産の価値を下げる望ましくないイベントと説明されている。
14	脅威モデル(threat	システムの背景となる情報、システムの脅威プロファイル、そし	

	model)	てその脅威プロファイルに対する現行システムの分析結果を記したドキュメント。	
15	脅威プロファイル (threat profile)	システムに対する敵の全攻撃目標の特徴を記述したもの。脅威プロファイルは、攻撃者がシステム資産に対して、またはそれに関連して何かを試みるかという説明になる。脅威の一覧である。	
16	脅威ツリー (threat tree)	特定の脅威に対する攻撃経路を記述する解析ツール。脅威ツリーは、条件の階層から成り、脅威の軽減策（あるいはその欠如）の特徴を表す。脅威ツリーは、攻撃に対応する脅威をルートとする。	
17	信頼レベル (trust level)	通常は、認証方法と権限の種類に基づく外部エンティティの特定のこと。信頼レベルとエントリポイントが関連することがあるが、その場合の信頼レベルは、外部エンティティがエントリポイントとインタフェースを持つために備えなければならない最低限の信頼度を表す。また、信頼レベルと保護対象リソースが関連することもあり、その場合の信頼レベルは、外部エンティティがリソースに影響を及ぼすために備えなければならない最低限の信頼度を表す。	ISO/IEC 15408(CC)の「許可された利用者（Authorized user）」を更に分類したものとして解釈できる。
18	使用シナリオ (use scenario)	システムをどのように使用するか（あるいはしないか）という意図を表すもの。	
19	脆弱性 (vulnerability)	システムのセキュリティ不具合のこと。攻撃者が脅威を実現[5]するための有効な方法を示す。経路のリーフとなる条件からルートとなる脅威に至る脅威ツリーの中で、軽減策のない攻撃経路のある脅威が最終的に脆弱性となる。	

本ガイドで想定する改ざんと偽造の用語の定義を以下に示す（表 2-7）。

表 2-7:改ざんと偽造の定義

#	用語	定義
1	改ざん	悪意者が、自分にとって都合のよい形で、データの内容を修正すること。 修正対象のデータは、作成済みであり、本来の保管場所に存在している。悪意者は、そのデータをアクセスし、内容を変更する。その後、本来の保管場所へ格納する。 許可されたユーザが、運用規定に従って行う業務の中で、不注意により、データの内容を、あるべき形ではないように修正してしまうこと。例えば、設定ファイル内容の変更時に、”sha256”とすべきところを”sha1”として変更してしまう、など。
2	偽造	悪意者が、自分にとって都合のよい形で、データを新規作成すること。 基本的に、偽造されたデータは、ある格納場所に存在する本来のデータを模したものである。本来のデータは、改ざんされない。

[5] 文献「脅威モデル」の訳は、「認識」であったが、「実現」の誤訳だと思われる。原文の該当箇所は、”A security flaw in the system that represents a valid way for an adversary to realize a threat.”

3 評価システムの明確化に関するガイドライン

セキュリティ評価対象のシステム構成及び外部インタフェースを明確化する。また、セキュリティ評価対象を明確化する。具体的には、以下の項目を明確化する。

- 物理的配置構成
- ネットワーク構成
- システム構成
- ソフトウェアコンポーネント構成
- 外部接続

図 3-1は、複数方式タイムスタンプ検証サブシステムの例である。セキュリティ評価対象としては、タイムスタンプ検証サーバ装置となる。なお、意図されたインタフェースを介してタイムスタンプ検証サーバ装置と通信する外部システム、及びタイムスタンプ検証サーバ装置に含まれる周辺機器などのコンポーネントの一部は、セキュリティ評価対象外である。下記の例では、TSA1、TSA2、検証Client（検証クライアント）、Firewall（ファイアウォール）、Directory Server（ディレクトリサーバ）、CA Server（CAサーバ）、NTP Server（日本標準時と同期したNTPサーバ）、PKCS#11 モジュール及びハードウェア暗号モジュールは、評価対象外である。

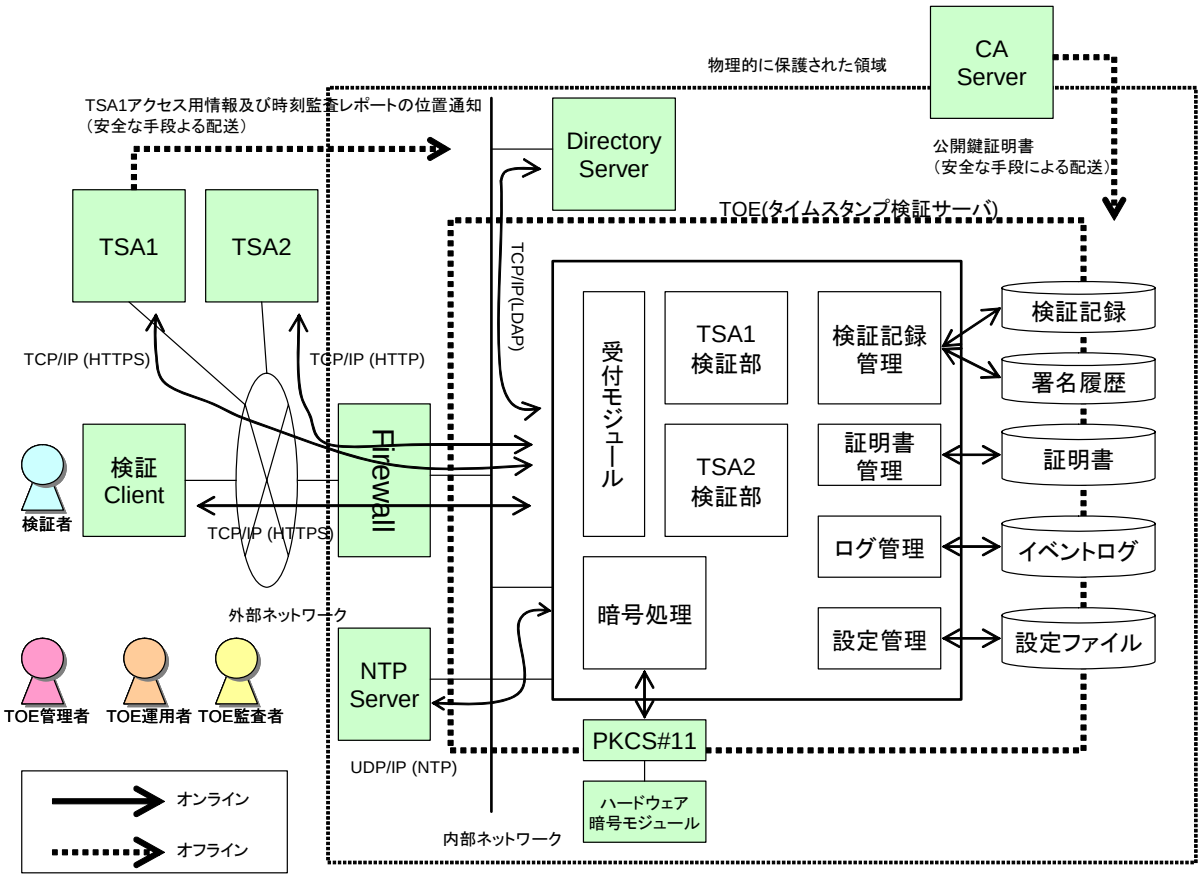

図 3-1:複数方式タイムスタンプ検証サブシステムのシステム構成図

上記の構成図を参考にして、各サブシステムにおけるシステム構成及び外部インタフェースを明確化する。

また、別途、暗号機能に係る部分を入出力、及び実装部分を明確にし、これらが評価対象、あるいは、評価対象外なのかを区別する。下記の例は、タイムスタンプ検証サーバが、検証結果に対して署名を作成する処理部分、及び、検証記録に対するヒステリシス署名検証処理部分を示す(図 3-2、図 3-3)。

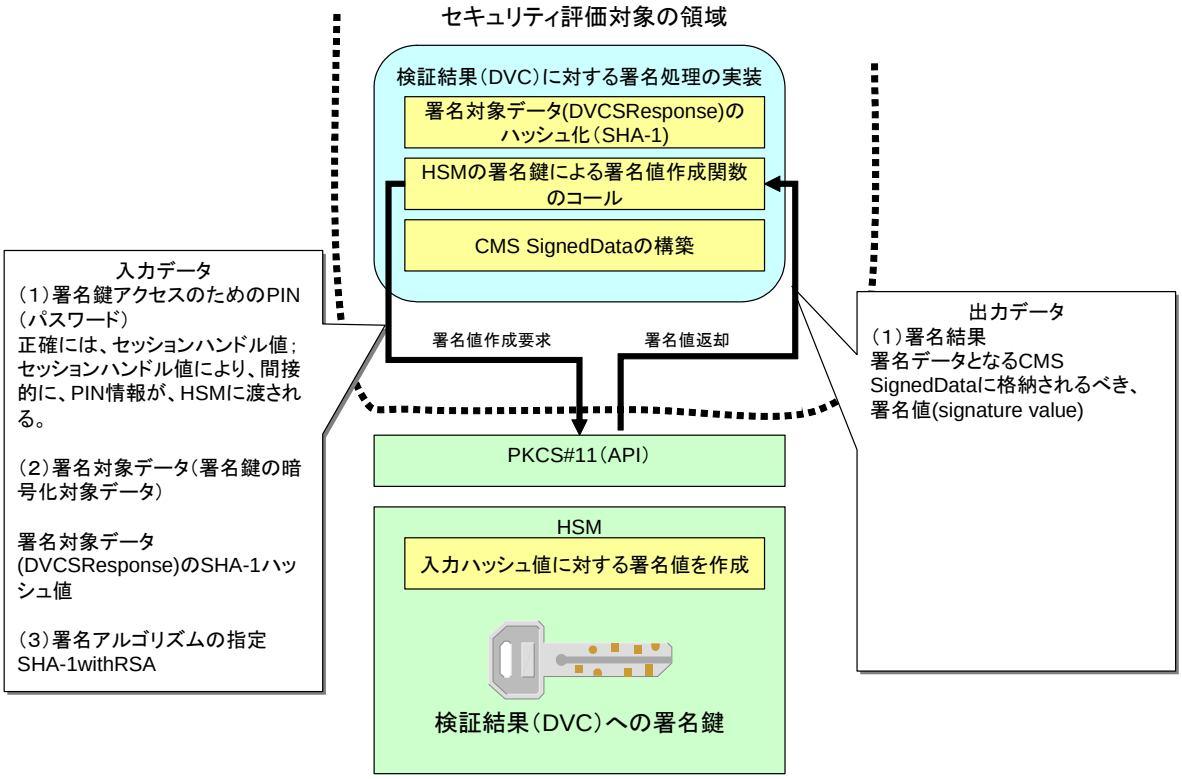

図 3-2:タイムスタンプ検証サーバの署名作成処理部分及びセキュリティ評価対象の領域

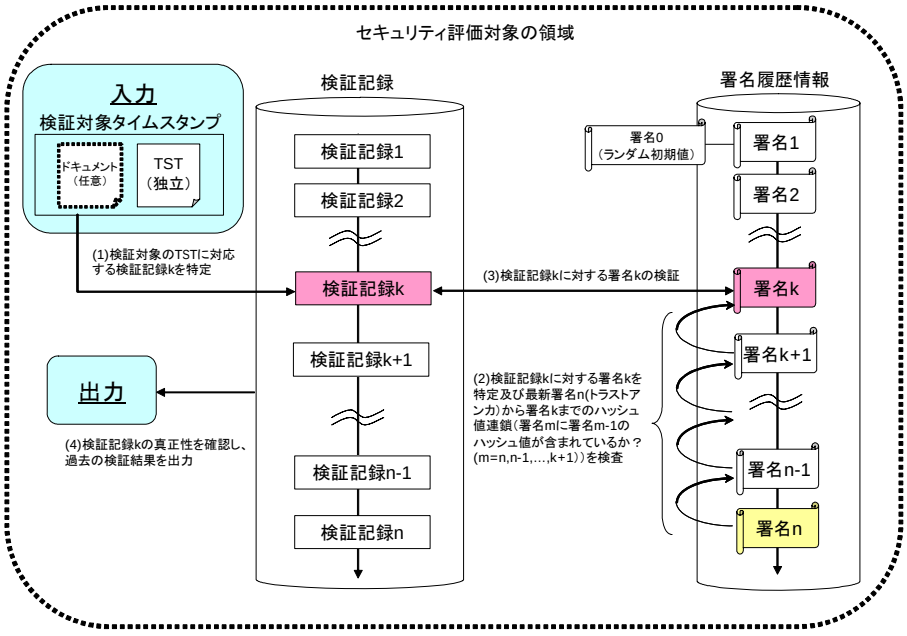

図 3-3:タイムスタンプ検証サーバのヒステリシス署名検証処理部分及びセキュリティ評価対象の領域

4 関与者の明確化に関するガイドライン

評価対象システムの意図した動作を実現するために必要となる関与者及びその役割を明確化する。
雛形となる関与者モデルは、以下の通りである(表 4-1)。

表 4-1:関与者モデル

#	関与者	説明
1	TOE 管理者	暗号機能に関わる初期化及び管理業務を行う。 TOE に関わるユーザ/役割を管理する。
2	TOE 運用者	TOE の起動・停止を実行する。 TOE 管理者の指示の元で各種設定など運用業務を行う。
3	TOE 監査者	TOE が生成する監査データの分析等の監査業務を行う。
4	TOE 利用者	TOE が提供するサービスを利用する。
5	外部の第 3 者機関	TOE がサービスを提供する上で、利用する外部の第 3 者機関(第 3 者機関が運用する装置/システム)

上記を雛形として、各評価システムにおける関与者モデルを明確化する。

5 資産の明確化に関するガイドライン

一般公開されている規格、及びガイドラインを参考にして、評価対象システムにおける保護すべき資産を明確化する。

ISO/IEC 15408 における資産(Assets)の定義は、以下の通りである。

資産 （Assets）	TOE（セキュリティ評価対象）の対抗策が保護すべき情報または資源 （Information or resources to be protected by the countermeasures of a TOE.）

ISO/IEC TR 15446 では、資産の特定に関するガイドラインを記述している。資産とは、個人、あるいは、組織が所有するものであり、重要な価値を持つものである。この資産は、脅威エージェント(攻撃者)にとっても価値がある。脅威エージェントは、資産が持つ価値を下げることを試みる。具体的には、資産の持つ「機密性」、「完全性」、「信頼性」、「真正性」、「責任追跡可能性」、「可用性」を損なわせる[6]。

ISO/IEC 15408 における脅威のフレームワークは、資産、脅威エージェント、攻撃の観点から記述可能である（図 5-1）。資産は、ISO/IEC 13335 で定義される 6 つのセキュリティ特性を持つ。具体的には、完全性、機密性、可用性、真正性、信頼性、責任追跡可能性、である。悪意者である脅威エージェントは、資産の持つ特性を低下させる攻撃を行う。脅威エージェントは、悪意を行う動機や悪意を実際に行うための能力、及び利用可能資源の観点から記述される。また、攻撃は、攻撃方法、攻撃機会、攻撃で利用する脆弱性の観点から見ることが可能である。

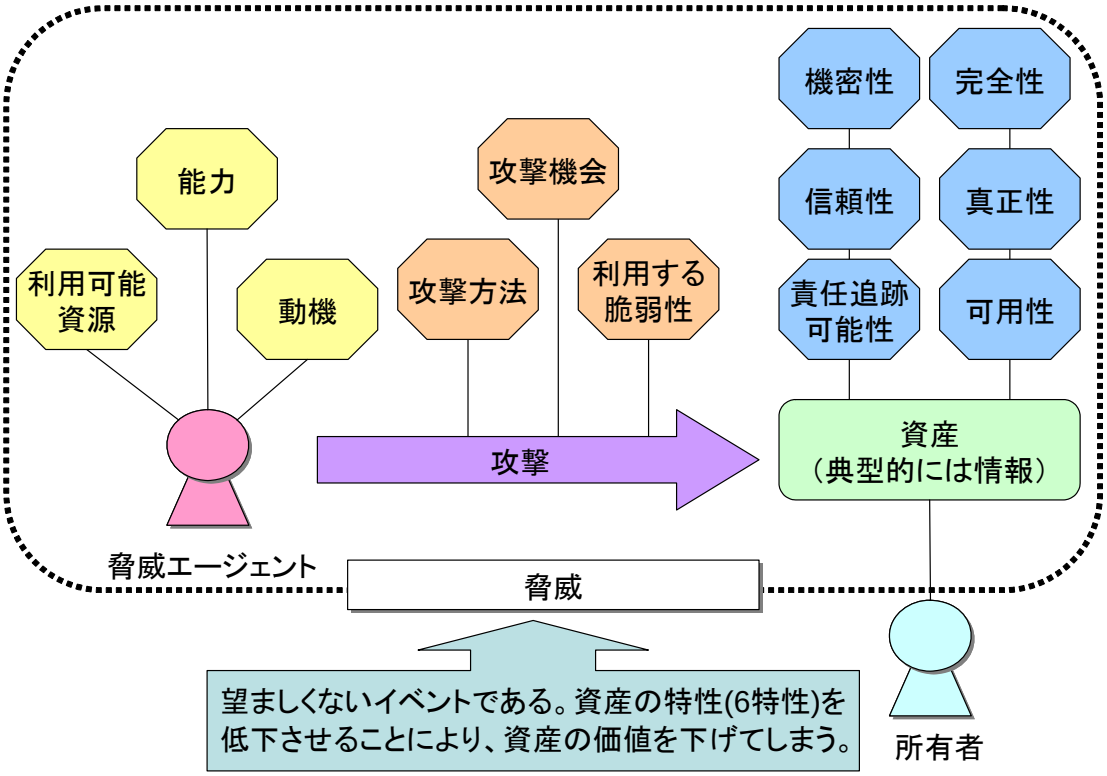

図 5-1：ISO/IEC 15408 における資産と脅威エージェントに注目した脅威のフレームワーク

[6] どれか一つでも損なえば、脅威とみなすことができる。

ISO/IEC 15408 では、資産とは、典型的には、情報の形態を持つ。この情報は、IT システムにより、格納、処理、あるいは、転送されるものである。例えば、ファイルやデータベースなどが典型的な情報資産である。また、資産は、TOE（セキュリティ評価対象）の外部に存在するかもしれない（ただし、IT 環境の中に存在する）。例えば、TOE としてファイアウォールや侵入検知システムを考えた場合、ファイアウォールや侵入検知システムによって保護される情報とリソースも資産として捉えられる。

なお、資産として、許可クレデンシャル(authorization credentials)や IT 実装などを含めてもよい。これらは、ファイルやデータベースなどの資産に対するセキュリティ対策を検討する上で、副次的に明らかになる資産とも言える。ISO/IEC TR 15446 では、ファイルなどの主要な資産（重要な資産）を守ることの目的があいまいになる可能性があるなどの理由から、この副次的な資産に関しては、セキュリティ環境で明文化することは勧めないとしているが、本ガイドでは、分かる範囲でこれらの資産を明確にすることを推奨する。理由は、以下の通りである。

- 統合化プラットフォームシステムのようなインターネットベースのシステムにおける典型的な「脅威」である「成りすまし」や「DoS 攻撃」などは、明らかに、ファイルやデータベースなどの情報に対する脅威ではなく、IT 実装（例えば、Web サーバなど）に対する脅威と言える。よって、セキュリティの課題を定義するための「セキュリティ環境」にてこれらの資産を明確化した方が好ましい。
- 統合化プラットフォームシステムは、ほとんど実装済みと見なせるため、実装に深く関係すると思われる副次的な資産がある程度具体的である。

本ガイドで想定する資産をまとめると以下の通りである（表 5-1）。

表 5-1：資産分類モデル

#	分類		説明
1	情報資産	利用者データ	利用者によって作成された及び利用者に関して作成されたデータ。TSF の動作に影響を与えないもの。 【例】 ● 電子メールのメッセージ内容
		TSF データ	TOE によって作成された及び TOE に関して作成されたデータであり、TOE の動作に影響を与える可能性のあるもの。 【例】 ● TSF 設定データ ● 認証データのデータベース ● 監査記録 ● サブジェクト/オブジェクトなどのセキュリティ属性 ● 認証データ ● アクセス制御リストエントリ ●「暗号処理に使用する鍵」（特別な配慮が必要なデータ）
2	IT 実装		ハードウェア/ソフトウェア/ファームウェアである。 このタイプの資産に対する典型的な攻撃は、「改変」、及び「DoS 攻撃」である。

ISO/IEC TR 15446 では、特に、暗号コンポーネントに係る資産の例を記述している。統合化プラットフォームシステムは、暗号技術を利用したサービスを提供するため、暗号技術の実装に関する資産を更に詳細化して検討する。これらのデータは、上記の分類で言う「TSF データ」と言える。

ISO/IEC TR 15446 で記載された資産例は以下の通りである（表 5-2）。

表 5-2：暗号コンポーネントに特化した資産モデル

#	項目	説明
1	暗号変数	アルゴリズム入力を出力へ変換するための暗号アルゴリズムの操作のために必要となる、一つのまたは連続した値。暗号変数の例は、暗号鍵 (共通、公開、秘密、その他)、

		公開鍵パラメタ、及び初期化ベクターである (平文、暗号文、及びハッシュ値は暗号変数とはみなされないことに注意)。
2	暗号機能の入出力	暗号機能への入力、及び出力(平文と暗号文)。
3	暗号アルゴリズム実装	ハードウェア、ソフトウェア、及び/またはファームウェア上での暗号アルゴリズムの実装。
4	呼び出しパラメータ	暗号機能にアクセスするため、TOE に供給される秘密 (例えば、パスワード、または個人識別番号)。

例えば、ハッシュ関数を実装したコンポーネントの場合の資産例は、以下の通りである(図 5-2)。

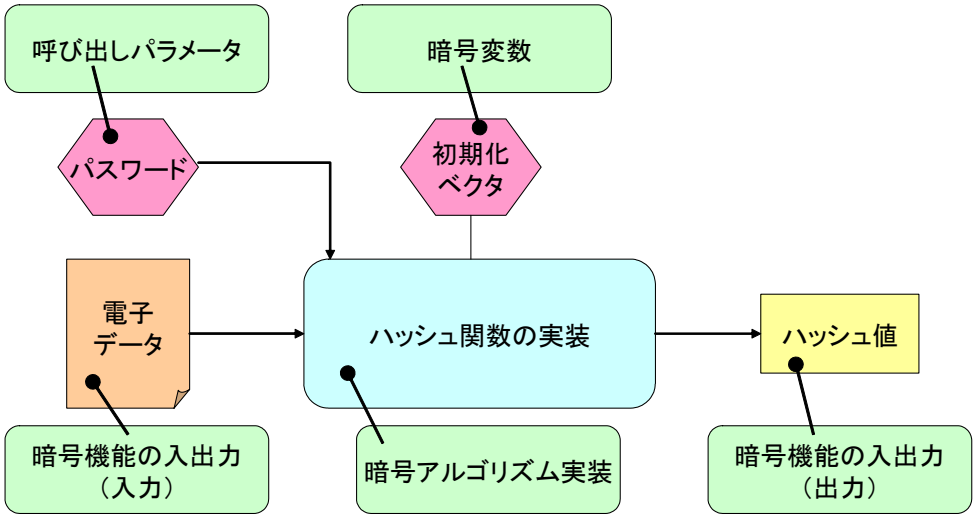

図 5-2:ハッシュ関数実装とその資産の例

また、複数方式タイムスタンプ検証サブシステムにおけるタイムスタンプ検証サーバの暗号実装の例を以下に示す(図 5-3)。検証結果に対する署名を作成するコンポーネントに関わる資産である[7]。

[7] 複数方式タイムスタンプ検証サブシステムにおけるタイムスタンプ検証サーバでは、PKCS#11 モジュール及び HSM そのものに対するセキュリティ評価は、スコープ外である。

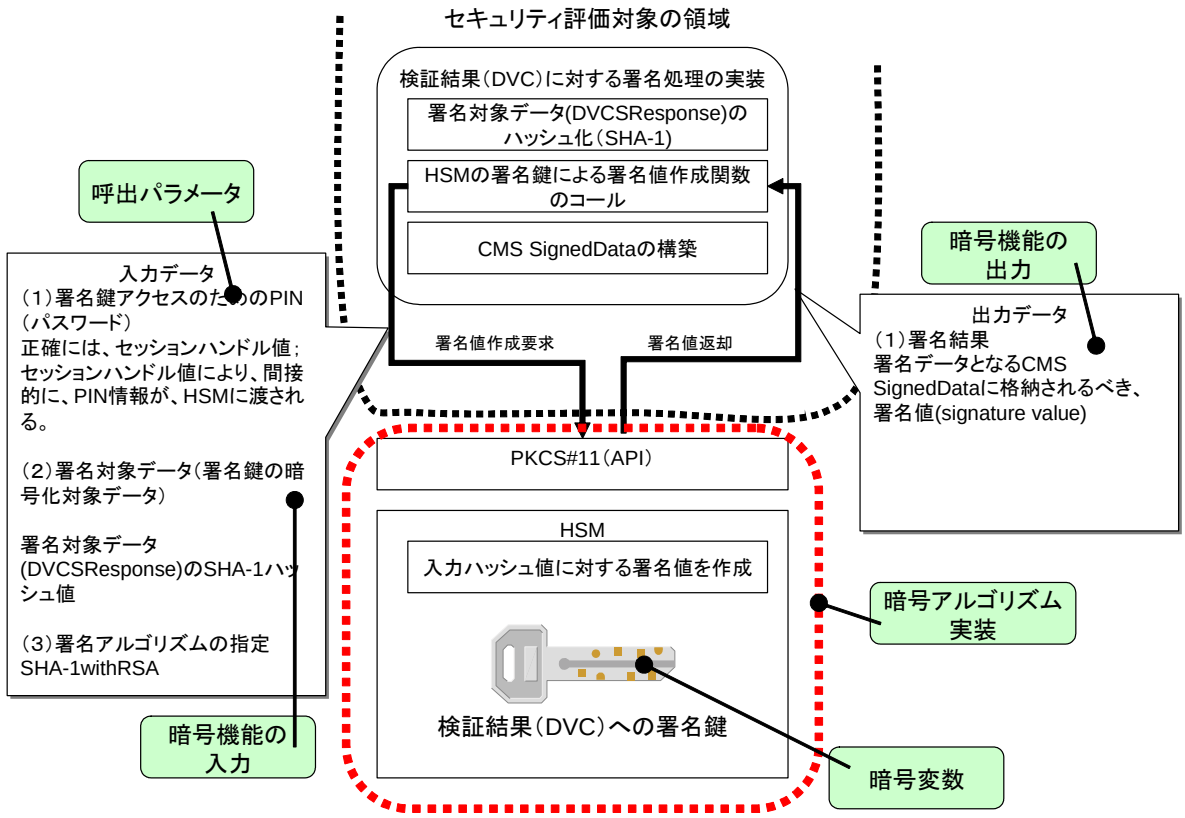

図 5-3:タイムスタンプ検証サーバの署名処理実装の例及びそれに関わる資産

6 セキュリティ環境の導出ガイドライン

セキュリティ評価を行う上で、評価対象システムの「セキュリティの課題（Security Concerns）」を明確化することが重要である。ISO/IEC 15408 では、「セキュリティ上の課題」を導出するために、「セキュリティ環境」を記述する必要がある。

ここでは、ISO/IEC 15408 で記載された「セキュリティ環境」の考え方を示し、次に、雛形となる「セキュリティ環境」を記述する。評価対象システムの「セキュリティ環境」は、この「セキュリティ環境」をカスタマイズすることで求められる。

6.1 セキュリティ環境

ISO/IEC 15408 では、セキュリティ評価対象システム（TOE）の「セキュリティ環境」を記述し、対象システムのセキュリティの課題を定義する。「セキュリティ環境」の記述では、「環境に関する前提」、「情報資産に対する脅威」、そして「組織のセキュリティポリシー」を明確化する必要がある（表 6-1）。これらの三つの視点から、「セキュリティの課題」が定義される（図 6-1）。

表 6-1：セキュリティ環境の構成要素

#	項目	説明
1	環境に関する前提	TOE セキュリティ環境に関する前提である。この前提は、セキュリティの課題の範囲を定義する。 プリフィックス(A.)から開始する識別ラベルで区別する。
2	情報資産に対する脅威	保護が必要な情報資産（一般的には、IT 環境の中の情報やリソース、あるいは、TOE 自体）、識別された脅威エージェント、脅威エージェントがその情報資産に対して及ぼす脅威、などを記述する。 脅威を分類してもよい[8]。たとえば、TOEに対する脅威と環境に対する脅威に分けることが出来る。TOEに対する脅威は、プリフィックス(T.)から開始する識別ラベルで区別する。また、環境に対する脅威は、プリフィックス(TE.)から開始する識別ラベルで区別する。
3	組織のセキュリティ方針 （組織のセキュリティポリシー）	組織のセキュリティポリシーやルールを記述する。TOE は、セキュリティの課題に取り組む上で、そのポリシーやルールに従わなければならない。 プリフィックス(P.)から開始する識別ラベルで区別する。

[8] TOE に対する脅威と環境に対する脅威との違いは、前者の場合、TOE 自体に実装されたセキュリティ機能により、脅威対策が可能である。一方、後者の場合、TOE を含む IT 環境（運用なども含む）により、対策されるものである。

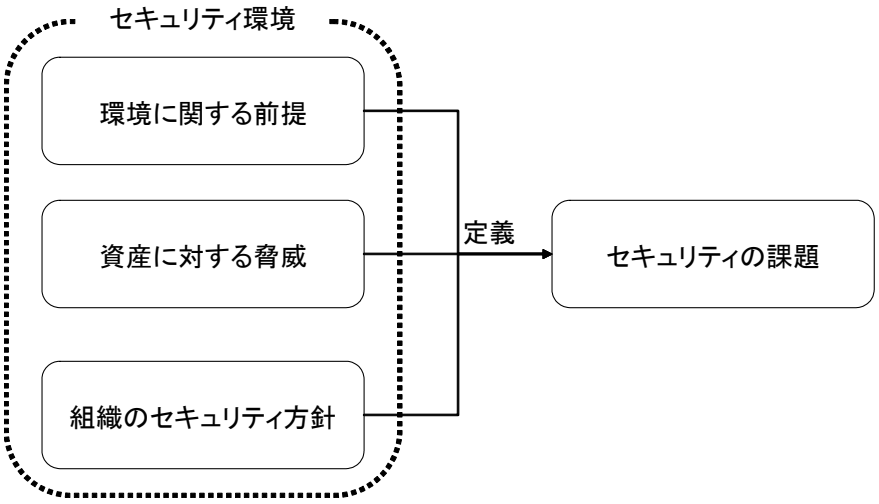

図 6-1:セキュリティ環境から定義されるセキュリティの課題

セキュリティ評価作業におけるセキュリティ目標及びセキュリティ機能要件の策定とは、このセキュリティの課題を解決するためのものとなる。図 6-2は、セキュリティ環境、セキュリティ目標、セキュリティ機能要件の関係性を示す。セキュリティ環境から導出されたセキュリティの課題を解決するための方針であるセキュリティの目標は、TOEのセキュリティ目標及び環境のセキュリティ目標に分類される。TOEのセキュリティ目標は、TOEのセキュリティ機能要件につながる。一方、環境のセキュリティ目標は、環境に対するITのセキュリティ機能要件、あるいは、環境に対するNon-ITのセキュリティ機能要件につながる。

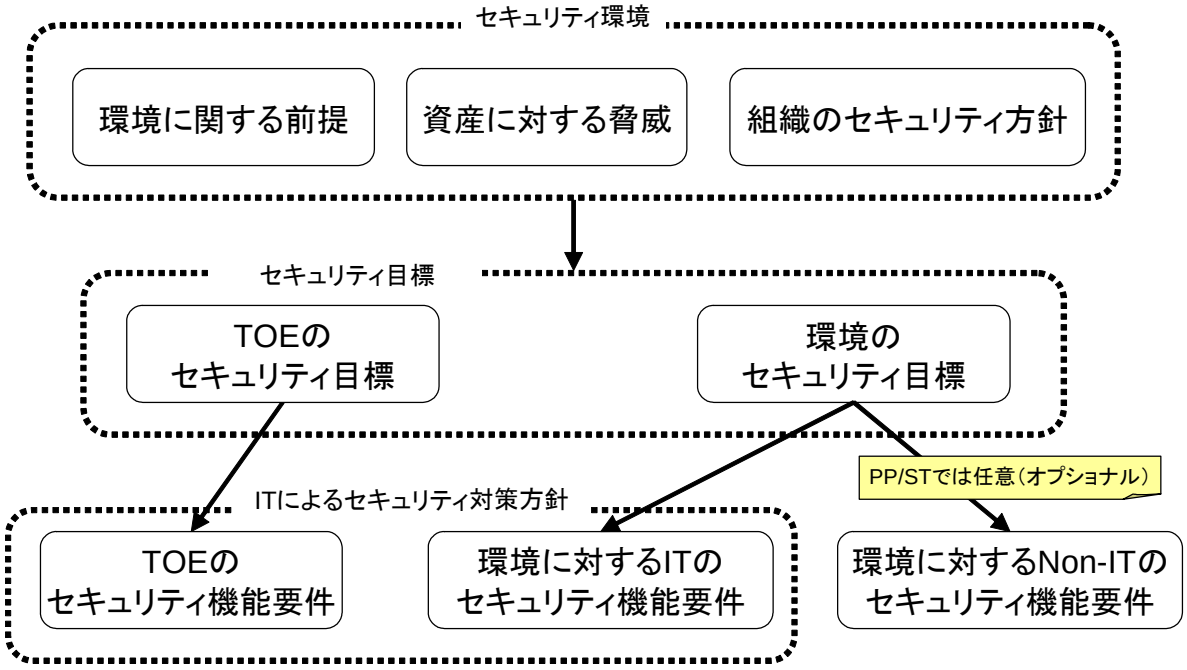

図 6-2:セキュリティ環境、セキュリティ目標、セキュリティ対策の関係

セキュリティ環境に対応するセキュリティ機能要件の対応を 表 6-2に示す。環境に関する前提は、環境に対するセキュリティ要件で実現させる必要がある。情報資産に対する脅威及び組織のセキュリティ方針で定義されるセキュリティの課題は、TOEのセキュリティ機能要件、あるいは、環境に対する機能要件で対抗する必要がある。

表 6-2:セキュリテ環境の構成要素とそれらに対応するセキュリティ機能要件

#	セキュリティ環境要素	セキュリティ機能要件		
		TOE セキュリティ機能要件	環境に対するセキュリティ要件	
			IT のセキュリティ機能要件	Non-IT セキュリティ要件
1	環境に関する前提	―	○	○
2	情報資産に対する脅威	○	○	○
3	組織のセキュリティ方針（組織のセキュリティポリシー）	○	○	○

○:該当する、ー:該当せず。

以降で、ISO/IEC TR 15446 に基づき、前提、脅威、そして組織のセキュリティポリシーを識別するためのガイドラインを記述する。

6.1.1 前提を識別し記述する方法

前提とは、TOE セキュリティ環境に関するものである。意図された TOE の使用方法(the intended usage of the TOE)に関するもの、物理的な環境、人的な環境、などについて記述する。前提のリストを作成するために、まず、以下を自問する必要がある。

「TOE セキュリティ環境」と「セキュリティの課題の範囲」に関してどのような前提をつくるのか？ (What assumptions am I making about the TOE security environment and the scope of the security concerns?)

例えば、ある資産に対する潜在的な脅威は、実際のところ、その TOE セキュリティ環境においては、関係がないことを保証するための「前提」をつくる必要がある場合もある。

前提を分類すると以下のようになる（表 6-3）。

表 6-3:前提の分類

#	分類	説明
1	想定された使用方法	TOE の想定された使用方法に関する前提である。 【例】 • 一般事務用に使われることを想定している • 保護資産として価値の極めて高いもの(国家機密)を守るようにはできていない • 平日日中のみの利用を想定している
2	物理的環境	TOE の物理的な環境に関する前提である。例えば、TOE が物理的に保護されている、など。
3	人的環境	TOE に関わる人的な前提である。期待されるユーザロールのタイプ、ユーザロールの責任、ユーザロールに対する信頼性の程度。
4	その他	TOE が依存する OS/ソフトウェア/ハードウェアなどに関する前提である。 【例】 • TOE が依存する OS は、安全に導入・運用されている。 • TOE が依存する OS により、データベースファイルやディレクトリは、許可のないアクセスから保護

6.1.2 脅威を識別し記述する方法

ISO/IEC 15408 は、PP や ST の中に脅威に関する記述を含めることを要求している。しかしながら、セキュリティの目標が、組織のセキュリティポリシー(OSPs)と前提だけから導出されるのであれば、脅威に関する記述は省略できると言っている。違う言い方をすれば、OSPs と前提により、セキュリティの課題(security concerns)を定義できるのであれば、脅威の記述は不要である。

その一方で、OSPs よりも脅威の方が、「セキュリティの課題」をより明確化するため、可能であれば含めることが好ましいと述べられている。本ガイドでは、脅威を積極的に識別し記述することを推奨する。

また、ISO/IEC 15408 の PP や ST では、前提に矛盾する脅威を含めてはならないとしている。例えば、物理的にアクセスすることが許可されない場所に TOE が配置されている場合、権限を持たない悪意者が、TOE に物理的アクセスすることは想定されない。そのため、このような前提においては、「悪意者が、物理的に TOE にアクセスする」というような脅威は不要である。

しかしながら、本ガイドでは、PP や ST の記述に求められる無矛盾性を追求しない。そのため、前提の実現化により対策可能であるものも脅威として含めてもよい。

なお、ISO/IEC 15408 は、脅威分析のフレームワークを提供していない。また、PP/ST作成ガイドラインであるISO/IEC TR 15446 でも脅威分析の方法については、スコープ外である。あくまで一般的な原則を記述しているのに過ぎない。具体的な脅威の捉え方に関する一般的な原則は、以下の通り(表 6-4)。

表 6-4:脅威の捉え方

#	項目	説明
1	何が脅威か？ (What is a threat?)	脅威とは、望ましくないイベントである。これは、脅威エージェント、攻撃方法、攻撃に際して利用される脆弱性、攻撃対象となる情報資産の特定などにより特徴付けられる。何が脅威であるのかを特定するために、以下の質問に答えること。 a) 保護が必要な情報資産は何か？ b) 誰、あるいは、何が脅威エージェントか？ c) 攻撃方法、望ましくないイベントは？
2	資産の特定 (Identifying the assets)	ISO/IEC 15408 では、資産とは、TOE の対抗手段によって保護された情報、あるいは、リソースであると定義している。 脅威エージェントは、情報資産が持つ以下のいずれかの特性を損失させることで、これらの資産の価値を脆弱化することを試みる。 • 完全性 • 機密性 • 可用性 • 真正性 • 信頼性 • 責任追跡可能性

より実践的な脅威分析のガイドラインは、「7章 脅威分析ガイドライン」にて紹介する。

6.1.3 組織のセキュリティポリシーを識別し記述する方法

ISO/IEC 15408 では、セキュリティの課題が、脅威と前提からだけから定義されるのであれば、組織のセキュリティポリシーを省略してもよいとされている。

組織のセキュリティポリシーが脅威の言い換えであれば、含める必要はない。例えば、脅威として、「許可されない人物が、TOEに対して論理的なアクセスをおこなうかもしれない」を述べた場合、組織のセキュリティポリシーとして、「TOEの正当な使用者は、TOEに対するアクセスが許可される前に、識別されなければならない」を含める必要性はない(図 6-3)。

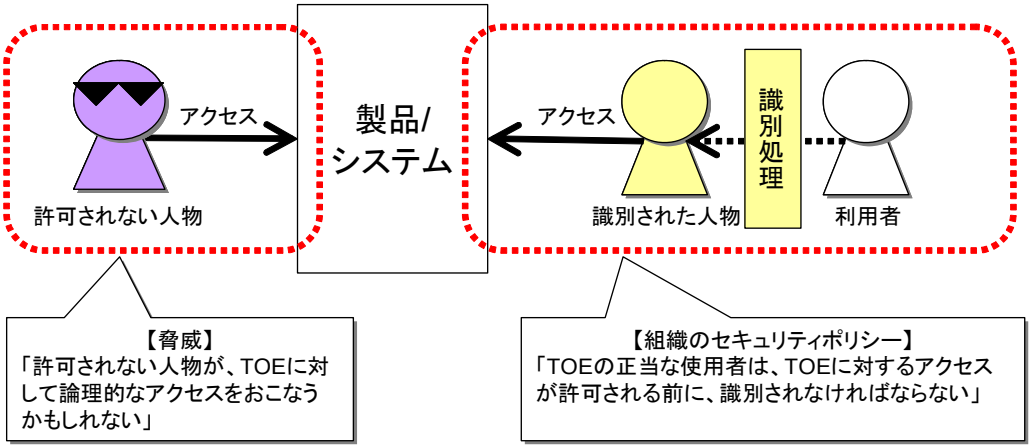

図 6-3:「脅威」の言い換えとなる「組織のセキュリティポリシー」の例

原則として、脅威として明示的、あるいは、暗黙的に示すことができないルールを実装する必要性がある場合、組織のセキュリティポリシーとして記述するのが適切である。例は、以下の通り(表 6-5)。

表 6-5:組織のセキュリティポリシーの例

#	例
1	情報フローの制御ルール 例:あるコンポーネント間の通信は許可する。
2	アクセス・コントロール 例:あるオブジェクトを閲覧するためには、ある権限が必要。
3	セキュリティ監査に関する組織のセキュリティポリシー 例:監査ログの暴露、改ざんに対する防止措置をとる。
4	組織が採用する解決方法。 例えば、特定の承認済みの暗号アルゴリズムの使用、あるいは、特定の標準への準拠、など。

本ガイドでは、TOE を用いる組織が採用する『運用管理規定』を想定し、組織のセキュリティポリシーを策定することを推奨する。

6.2 セキュリティ環境記述方針

統合化プラットフォームシステムに対して、「セキュリティ環境」の記述をゼロの状態から作成するのは、非常に工数のかかる作業である。また、ゼロから作成した場合、記述内容の網羅性や重複を確認することも大変な作業となる。場合によっては、記載内容の品質が落ちる可能性もある。

よって、これまでに作成/公開されている関連する PP/ST、標準規格、ガイドラインに記載された内容を雛形とし、これをカスタマイズする(修正や追加する)というアプローチにより、「セキュリティ環境」を規定する。これにより、「セキュリティ環境」の記述工数の削減及び記載内容の品質を高めることが期待される。

なお、セキュリティ環境における「脅威」に関しては、脅威の網羅性を確実にするために、7章にて、後述する「脅威分析ガイドライン」に従い、再度、脅威抽出を行うことが望ましい。

参照するPP/ST、標準規格、ガイドラインは、以下の通りである(表 6-6)。

表 6-6:セキュリティ環境を検討する上で参照するドキュメント

#	ドキュメント名	説明
1	ISO/IEC TR 15446:2004	PP/ST を作成するための標準規格(ISO/IEC 規格のテクニカル・レポート)。附属として、汎用システム(Generic system)と暗号機能などに関する「セキュリティ環境」の記述例が掲載されている。 統合化プラットフォームに含まれる全てのサブシステムに適用される。
2	Security Target for Baltimore Timestamp Server version 2.0.2 Patch 1(3rd Oct 2003)	Baltimore 社の PKI ベースのタイムスタンプサーバの ST 統合化プラットフォームにおけるTSA(特にPKIベースのTSA)に適用される。
3	Enterprise Certificate Server Set セキュリティターゲット Version 1.10 2004/06/24	日立製作所の認証局サーバの ST 統合化プラットフォームにおける CA に適用される。

これらのドキュメントを参照する際、評価対象(TOE)の定義を把握することが重要である。これらのドキュメントで定義されたTOE と統合化プラットフォームシステムにおける TOE との違いを明確にすることで、雛形となる「セキュリティ環境」のカスタマイズ方針が定まる。

(1)ISO/IEC TR 15446 の汎用システムの TOE

システム構成に関する具体的な説明は存在しない。ただし、「環境に関する前提」、「脅威」、「組織のセキュリティポリシー」の記述内容を踏まえると、図 6-4のようなシステム構成例が考えられる。

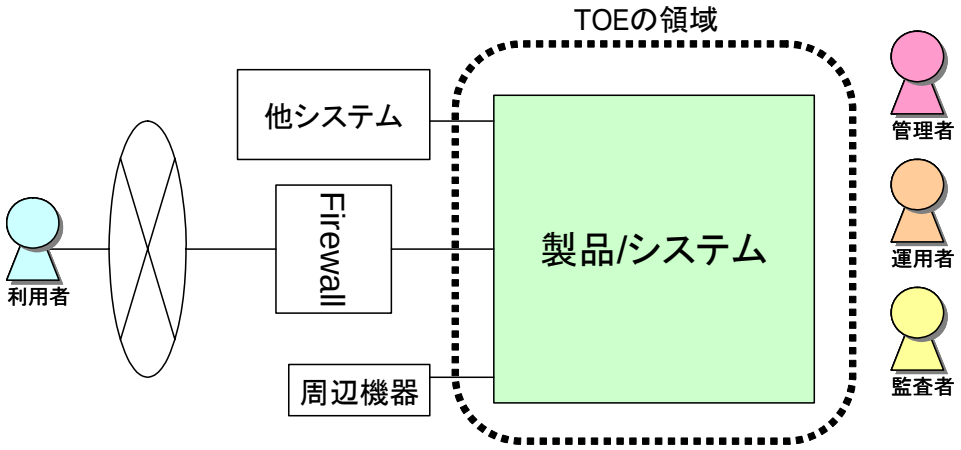

図 6-4:汎用システムのシステム構成例(ISO/IEC TR 15446 の記載内容から想定)

(2)Security Target for Baltimore Timestamp Server version 2.0.2 Patch 1(3rd Oct 2003)の TOE
独立トークン方式(PKI方式)のタイムスタンプトークンを発行するタイムスタンプサーバのSTにおけるTOEを以下に示す(図6-5)。

評価対象は、白地のコンポーネントである。強調表示されたコンポーネントは、評価対象外である。評価対象は、タイムスタンプサービスを提供する TSS Server の一部、及び、TSS Server の動作を制御する管理者ツールである Administration Utility である。評価対象外としては、タイムスタンプ要求者が操作する TSS Client や TSS Server が使用する PKCS#11 インターフェイスデバイスや Oracle データベースなどである。また、タイムスタンプトークンに含まれる時刻情報の正確性や信頼性に直結する時刻ソース(システムクロック)も評価対象外である。

なお、本ガイドラインの適用対象である統合化プラットフォームシステムでは、時刻情報の正確性や信頼性は、重要な要件であるため、時刻情報に関する要素を評価対象の中に含めることを推奨する。

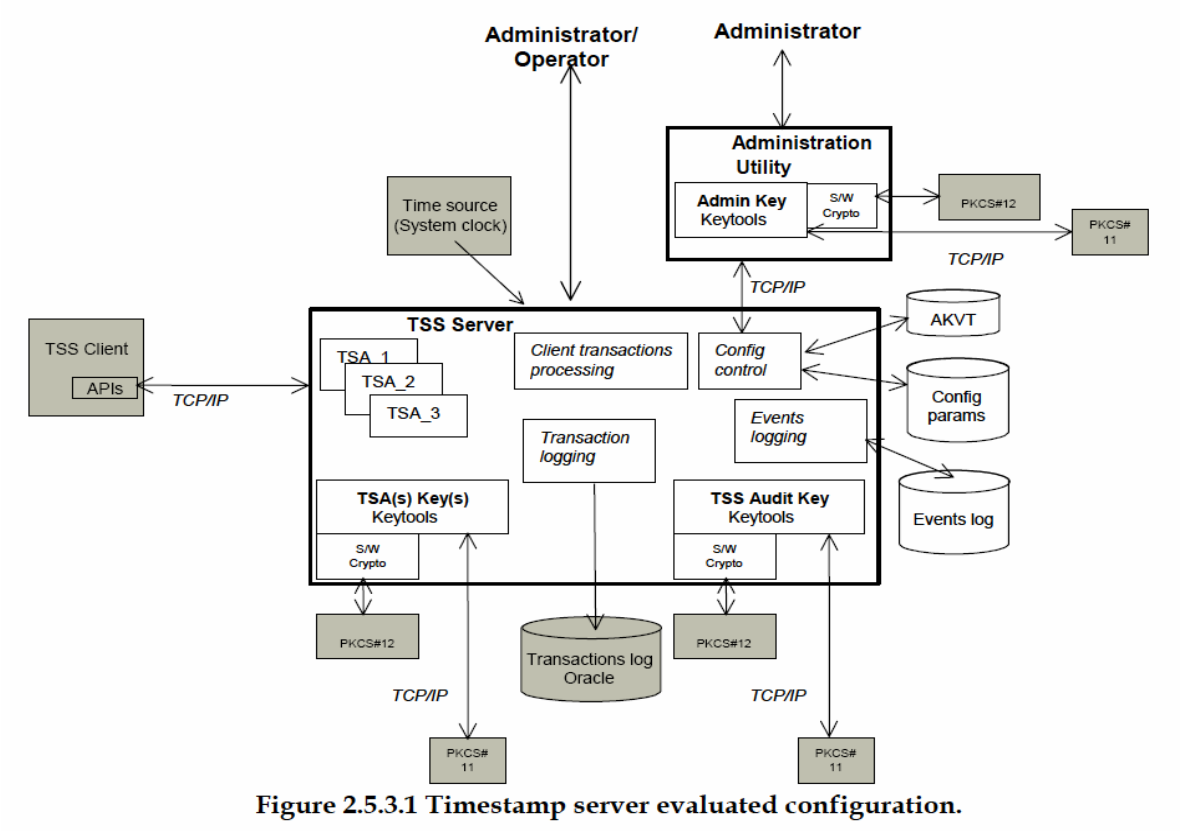

Figure 2.5.3.1 Timestamp server evaluated configuration.

図 6-5：Baltimore Timestamp Server に関わるシステム構成

(3) Enterprise Certificate Server Set セキュリティターゲット Version 1.10 2004/06/24 の TOE
認証局ソフトウェアのSTにおけるTOEを以下に示す（図 6-6）。

評価対象は、点線で囲った領域で示したソフトウェアコンポーネントである。CA サーバマシン上で稼動する ECSSet のサーバソフトウェア（CA サーバ）及び ECSSet のクライアントソフトウェア（管理端末）である。CA サーバマシンと接続する HSM やインターネットとの接点となる FW(ファイアウォール)は評価対象外である。

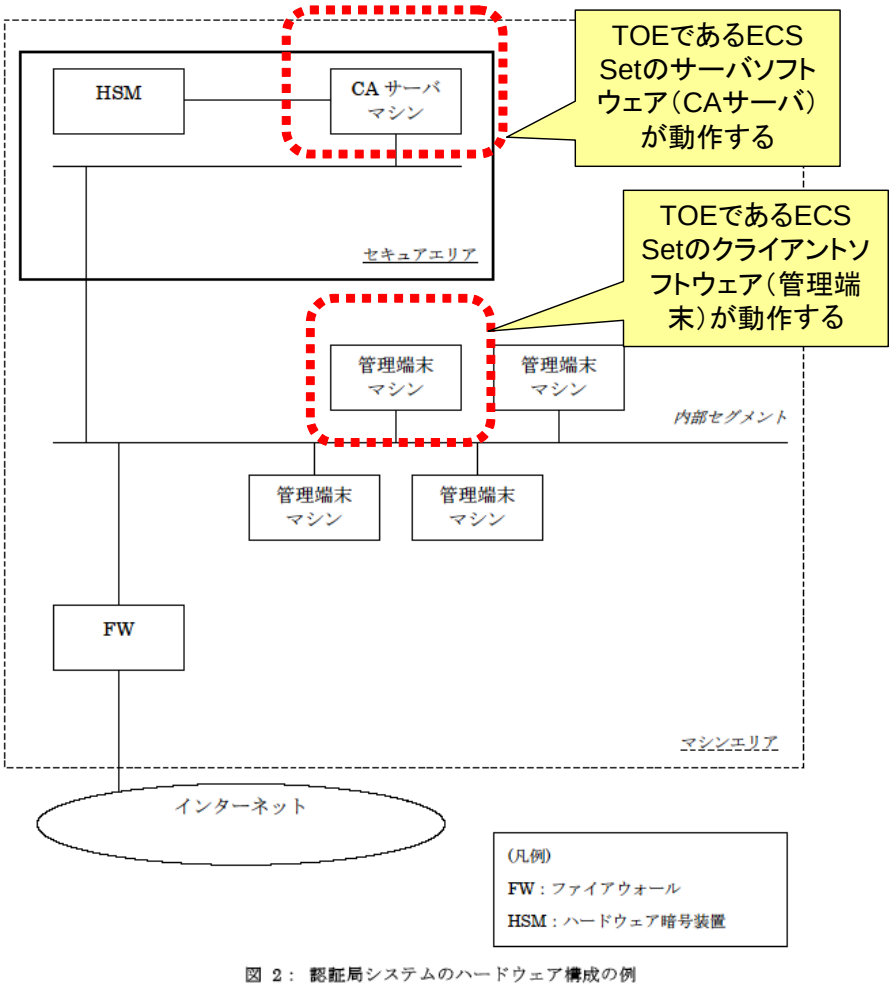

図 2： 認証局システムのハードウェア構成の例

図 6-6: 日立の Enterprise Certificate Server Set に関わるシステム構成

6.3 セキュリティ環境の雛形

本ガイドで、想定するセキュリティ環境の雛形を記す。

6.3.1 前提の例

6.3.1.1 ISO/IEC TR 15446 の汎用システムの前提

ISO/IEC TR 15446 の汎用システムにおける前提は、物理的な前提、人的な前提、接続に関する前提に分類される（図 6-7）。

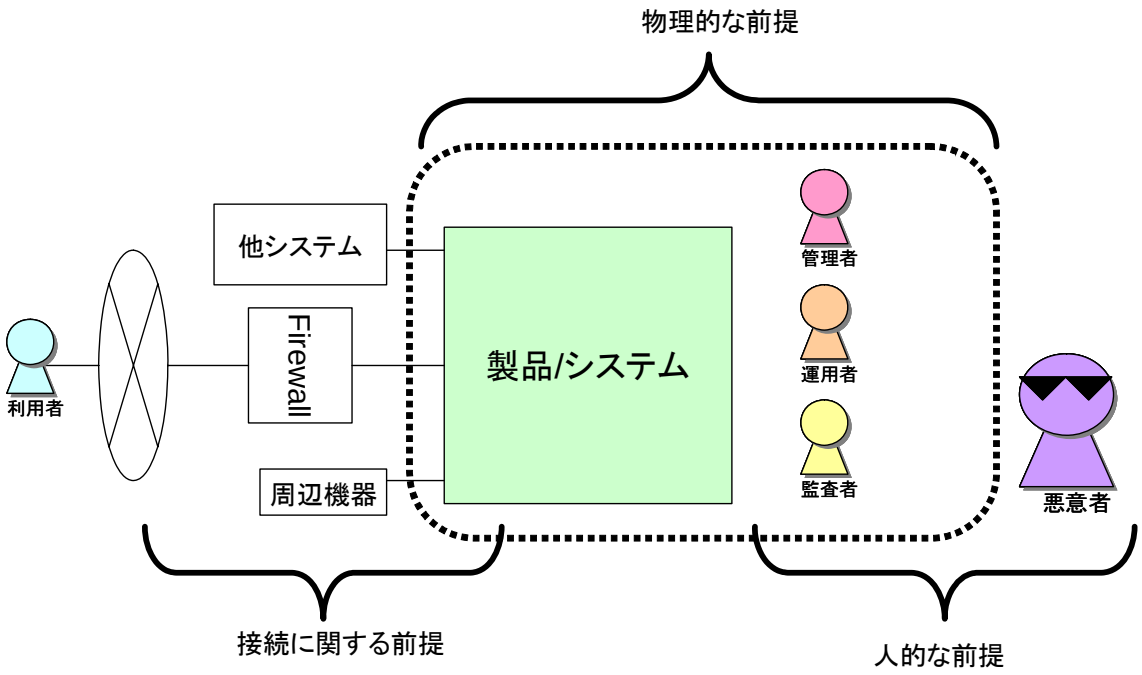

図 6-7:ISO/IEC TR 15446 の汎用システムにおける「前提」の分類

具体的な前提を以下に示す(表 6-7)。

表 6-7:ISO/IEC TR 15446 の汎用システムにおける「前提」

#	分類	項目	説明
1	物理的な前提(Physical assumptions)	A.LOCATE	TOE の処理リソースは、コントロールされたアクセス・ファシリティの中に配置される。これにより、権限のないユーザからの物理アクセスを防ぐ。
2		A.PROTECT	セキュリティポリシーの実施にとって重要な TOE ハードウェアとソフトウェアは、物理的に保護されている。そのため、悪意のある外部ユーザによる権限のない修正を防ぐ。
3	人的な前提(Personnel assumptions)	A.ADMIN	一人以上の許可された管理者が、割り当てられる。彼らは、TOE と TOE に含まれる情報のセキュリティを管理する資格を持つ。さらに彼らは、信用できる。そのため、彼らは、権限を濫用し、故意にセキュリティを低めることはしない。
4		A.ATTACK	攻撃者は、高いレベルの能力を持つ、さらに、高度なリソースと、大きな動機を持つ。 ※個々の TOE セキュリティ環境で適切に解釈され扱われなければならない。この前提は、脅威の定義の中でも利用される。例えば、あるレベルの能力、動機、利用可能なリソースを持つ脅威エージェントからの攻撃の可能性を除くことが可能。
5		A.USER	TOE の利用者は、TOE によって管理される情報にアクセスするために適切に許可されている。
6	接続に関する前提(Connectivity assumptions)	A.DEVICE	周辺機器への全接続は、コントロールされたアクセス・ファシリティ内に存在する。
7		A.FIREWALL	ファイアウォールは、プライベートネットワークと外部ネットワークを結

			ぶ唯一のネットワーク接続である。
8		A.PEER	TOE と通信する全ての他システムは、同じ管理コントロールの元にあり、同じセキュリティポリシーの制約の中で運用される。

6.3.1.2 ISO/IEC TR 15446 の暗号機能の前提

前提としての記載は無い。

6.3.1.3 Baltimore 社のタイムスタンプサーバの前提

Baltimore社のPKIベースのタイムスタンプサーバのSTにおける前提は以下の通りである(表 6-8)。

表 6-8:Baltimore 社のタイムスタンプサーバの前提

#	分類	項目	説明
1	その他	A.Time_Source	TOE 所有者は、タイムスタンプの時刻ソースがアベイラブルであることを保証する。また、時刻ソースの信頼性と正確性は、TOE 所有者にとって受容可能である。
2	その他	A.PKI	安全に管理された PKI の中で、TOE は運用される。 全ての鍵と証明書は、安全に発行、失効される。 全ての鍵と証明書の状態は、使用前にチェックされる。
3	その他	A.Key_Storage	全ての私有鍵は、安全に保管される。許可された TOE 管理者以外の人間からのアクセスを防ぐ。
4	物理的な前提	A.Location	TOE(及び関連するコンポーネント)は、コントロールされたアクセス・ファシリティに設定される。許可されない物理的アクセスを防ぐ。
5	接続に関する前提	A.Connectivity	TOE(及び関連するコンポーネント)は、専用のネットワークに設置される。外部ネットワークからのネットワークに対する攻撃を防ぐ装置が設置される。
6	人的な前提	A.System_Administrator	一つ以上の許可された人物が、次の責務に割り当てられる。 ・ 評価対象の設定において、TOE を安全に導入、管理する ただし、これらの人物は、TOE に係る鍵をアクセスすることは許されない。鍵に対してアクセスできるのは、システム管理者。 システム管理者の責務は、以下の通り。 ・ TOE 上で悪意のあるソフトウェアが動作しないようにする ・ TOE の要件を満たす適切なディスクスペースを用意する ・ TOE のデータベースを適切に管理する
7	人的な前提	A.TOE_Administrator	一人以上の許可された人物が、割り当てられ、TOE を安全に設定、管理する。 TOE 管理者には、以下のクラスがある(一人の人物は、複数のロールを兼ねることかもしれない) ・ Bootstrap Administrator ・ TSS Administrator ・ TSS Operator
8	人的な前提	A.TS_Requestor	タイムスタンプユーザ(タイムスタンプ要求者)は、タイムスタンプトークンを検証及び保持する。

			この中には、アウト・オブ・バンドの方法を用いて、TSA 証明書が失効していないかどうかの確認、タイムスタンプトークンの署名は、正当な TSA によって行われたものかどうかの確認、が含まれる。
9	その他	A.P11_Device	TSS 所有者は、以下の仕様を持つハードウェア暗号デバイスを選択する。 ・ RSA(1024/2048 ビット)、DSA(1024 ビット)の署名と検証 ・ SHA-1 ハッシュの生成 ・ PKCS#11 準拠 ・ 国家機関によって認定、あるいは、CC EAL3 相当として評価

6.3.1.4 日立製作所の認証局サーバの前提

日立製作所の認証局サーバのSTにおける前提は、以下の通りである(表 6-9)。

表 6-9: 日立製作所の認証局サーバの前提

#	分類	項目	説明
1	人的な前提	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。
2	人的な前提	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。
3	人的な前提	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。
4	接続に関する前提	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。
5	その他	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。
6	物理的な前提	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。
7	物理的な前提	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。
8	接続に関する前提	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。

6.3.2 脅威の例

6.3.2.1　ISO/IEC TR 15446 の汎用システムの脅威

ISO/IEC TR 15446 の汎用システムにおける脅威は、製品/システム（TOE）に対する脅威と環境に対する脅威に分類される（図 6-8）。

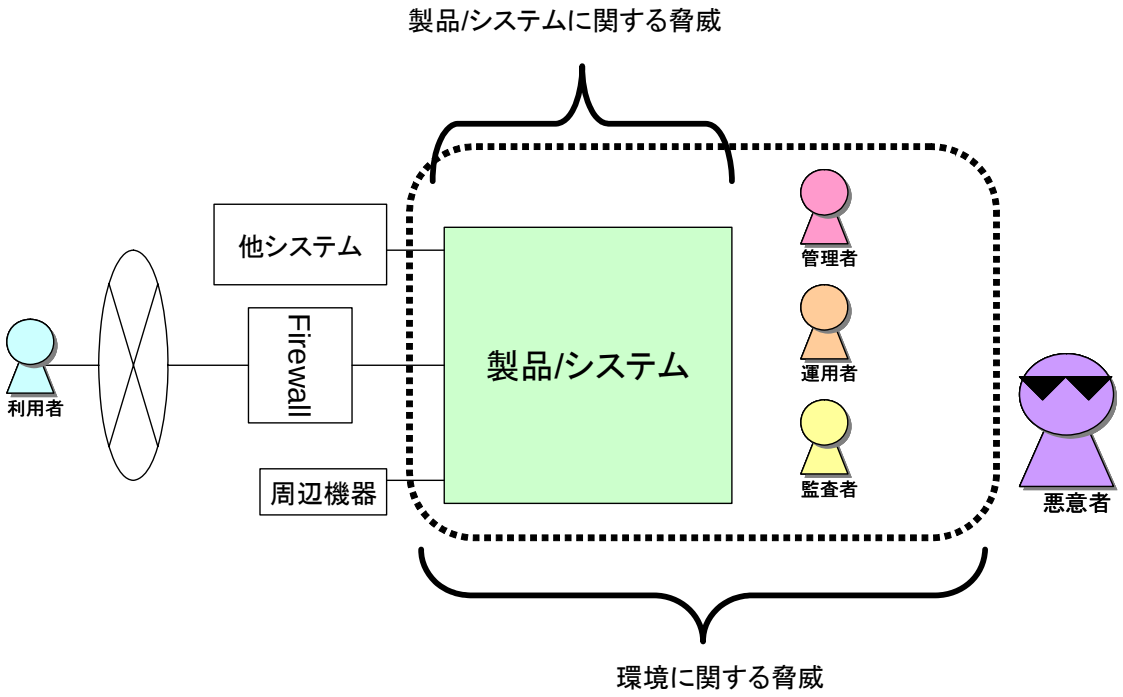

図 6-8：ISO/IEC TR 15446 の汎用システムの「脅威」の分類

具体的な脅威を以下に示す（表 6-10）。

表 6-10：ISO/IEC TR 15446 の汎用システムの脅威

#	分類	項目	説明
1	TOE	T.ABUSE	IT 資産に対する検知されない脆弱化。許可されたユーザが、（故意、あるいは、不注意で）アクションを実行した結果によってもたらされた脆弱化。 その個人は、アクションの実行を許可されている。
2		T.ACCESS	その情報やリソースの所有者あるいは管理者に許可を得ずに、その情報やリソースにアクセスする。
3		T.ATTACK	IT 資産に対する検知されない脆弱化。攻撃者（内部者あるいは外部者）のアクション実行によってもたらされた脆弱化。 その個人は、アクションの実行許可を得ていない。
4		T.CAPTURE	攻撃者は、ネットワーク上のデータを盗み見、あるいは、捕捉する。
5		T.CONSUME	許可されたユーザが、グローバル・リソースを消費する。消費の方法は、他の許可されたユーザがリソースにアクセス、あるいは、使用を妨げてしまうほど。

6		T.COVERT	許可されたユーザが、故意にあるいは不注意で、機密情報を含む情報を「隠れチャネル（covert channel）」を介して、その情報を見ることを許可されていない人に送信する。
7		T.DENY	情報転送にユーザが参加する（送信者、あるいは、受信者として）。その後、その参加行為を否認する。
8		T.ENTRY	IT 資産の脆弱化が発生。許可されたユーザによる TOE の使用の結果として。不適切な時間、あるいは、不適切な場所で、TOE を使用。
9		T.EXPORT	許可されたユーザが、TOE から情報をエクスポート。ソフト複写、あるいは、ハード複写。受信者は、機密レベル（sensitivity designation）と不一致となる方法で処理する。
10		T.IMPERSON	攻撃者（外部者、あるいは、内部者）は、情報やリソースに対する許可されないアクセスを取得。許可されないアクセスを取得することで。
11		T.INTEGRITY	情報の一貫性が脆弱化。ユーザエラー、ハードウェアエラー、伝送エラーなどのよって。
12		T.LINK	攻撃者は、リソースやサービスの複数の使用を見つけることができる。一人のエンティティ、そして、これらの使用を結びつける。エンティティが機密にしておきたい情報を推論する。
13		T.MODIFY	情報の一貫性が脆弱化。攻撃者は、許可を得ずに、情報を改変、破壊する。
14		T.OBSERVE	攻撃者は、リソースとサービスの正当な使用法を観察している。それは、ユーザがリソースやサービスの使用を秘密にしておきたい時。
15		T.SECRET	許可されたユーザが、故意、あるいは不注意で、TOE に格納された情報を観察する。そのユーザは、見ることを許可されていない。
16	環境	TE.CRASH	ヒューマン・エラー、あるいは、ソフトウェア、ハードウェア、電源のエラーのより、TOE の運用が突然停止する。その結果、セキュリティの重要なデータが損失、あるいは、破壊される。
17		TE.BADMEDIA	ストレージ・メディアの経年劣化、不適切なストレージ、すなわち、リムーバルメディアのハンドリング、はセキュリティの重要なデータが損失、あるいは、破壊につながる。
18		TE.PHYSICAL	TOE のセキュリティ上で重要な部分が、物理的な攻撃を受けやすい。その攻撃は、セキュリティ脆弱化を引き起こす。
19		TE.PRIVILEGE	IT 資産の脆弱化が起こる。管理者、あるいは、他の特権ユーザによる不注意、あるいは、悪意による行動の結果として。
20		TE.VIRUS	IT 資産の一貫性やアベイラビリティが脆弱化する。許可されたたユーザが、知らずに、コンピュータ・ウイルスをシステムに導入したため。

6.3.2.2 ISO/IEC TR 15446 の暗号機能の脅威

ISO/IEC TR 15446 の附属書(C.4.2.5 Typical threats)で述べられた暗号機能に係る脅威は、以下の通り（表 6-11）。

表 6-11：ISO/IEC TR 15446 の暗号機能の脅威

#	分類	項目	説明
1		T.EMI	TOE から放射される電磁波を介して、許可されないユーザに IT 資産が暴露される。 Cryptography-related IT assets may be disclosed to an unauthorised individual or user via the electromagnetic emanations from the TOE.
2		T.IMPERSON	攻撃者は、許可されたユーザに成りすます。

			An attacker (outsider or insider) may impersonate an authorised user of the TOE.
3		T.ERROR	許可されないユーザは、TOE における動作不良を引き起こし、許可されないユーザに IT 資産を暴露、あるいは、IT 資産を改変する。 An unauthorised individual or user of the TOE may cause unauthorised disclosure or modification of cryptography-related IT assets by inducing errors in the TOE.
4		T.MODIFY	攻撃者は、許可を得ないで、情報の改変や破壊を実施。その結果、情報の完全性がなくなる。 The integrity of information may be compromised due to the unauthorized modification or destruction of the information by an attacker.
5		T.ATTACK	検出できない IT 資産の脆弱化。内部者、あるいは、外部者であろうとも、その個人にとって許可されてない活動を実施。 An undetected compromise of the cryptography-related IT assets may occur as a result of an attacker (whether an insider or outsider) attempting to perform actions that the individual is not authorised to perform.
6		T.ABUSE	検出できない IT 資産の脆弱化。TOE に対する許可されたたユーザ、内部者、あるいは、外部者であろうとも、その個人にとって許可された行為を実施。 An undetected compromise of the cryptography-related IT assets may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.
7		T.MAL	TOE の動作不良を介して、許可されていないユーザなどに IT 資産が暴露される。 Cryptography-related IT assets may be modified or disclosed to an unauthorized individual or user of the TOE, through malfunction of the TOE.
8		T.PHSICAL	セキュリティ上重要な部分が、物理的な攻撃を受ける。 Security-critical parts of the TOE may be subject to physical attack which may compromise security.

6.3.2.3 Baltimore 社のタイムスタンプサーバの脅威

Baltimore社のSTにおける「脅威」は、以下の通りである(表 6-12)。

表 6-12:Baltimore 社のタイムスタンプサーバの脅威

#	分類	項目	説明
1		T.Hack_Imperson_Admin	ハッカーが、TOE 管理者に成りすまし、管理者ユーティリティをアクセスする。 ・ 実現方法:アイデンティティの偽造、盗みが必要 ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する

2		T.Hack_Imperson_TOE	外部のネットワークに位置するハッカーが、TOE に成りすまし、偽のタイムスタンプトークンを発行する。 ・ 実現方法: ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する
3		T.Hack_Mod_Timestamp	TOE によって生成されたタイムスタンプトークンの内容を変更する。変更するのは、タイムスタンプの意図された受信者、あるいは、受信者へのタイムスタンプをインターセプトしたハッカー。 ・ 実現方法: ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する
4		T.Client_Refute_Origin	タイムスタンプの意図された受信者が、タイムスタンプ生成元に関して異議を唱える。TOE から送信されたものではないと主張することにより。 ・ 実現方法:クライアントが、タイムスタンプトークンの署名を修正する。 ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する
5		T.Config_Mod_Undetect	TOE 管理者が、TOE の設定を変更する。その変更は、TOE によって検出されない。その結果、ある時点における TOE の設定を知ることができなくなる。 ・ 実現方法: ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する
6		T.Log_Mod_Undetect	TOE 管理者が、「不注意で」、イベントログを修正する。ログの完全性を検証することができなくなる。変更を隠す場合、以下の要件が必要。 ・ 実現方法: ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する
7		T.Mod_Config_Data	設定パラメータ・ファイルに対する変更。TOE 管理者による「不注意」から、あるいは、攻撃者による「悪意」から。変更は、イベントログに記録されない。変更を隠す場合、以下の要件が必要。 ・ 実現方法: ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する
8		T.Replace_Audit_Key	監査キーの取替え、TOE 管理者による「不注意」から、あるいは、攻撃者による「悪意」から。 ・ 実現方法: ・ 必要とする能力:高い ・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する
9		T.Replace_TSA_Key	TSA キーの取替え、TOE 管理者による「不注意」から、あるいは、攻撃者による「悪意」から。 ・ 実現方法: ・ 必要とする能力:高い

			・ 必要とするリソース:高い ・ 動機:タイムスタンプ付与対象の電子データの価値に依存する

6.3.2.4 日立製作所の認証局サーバの脅威

日立製作所の認証局サーバのSTにおける脅威は、以下の通りである(表 6-13)。

表 6-13: 日立製作所の認証局サーバの脅威

#	分類	項目	説明
1		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。
2		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。
3		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。
4		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。
5		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。

6.3.3 組織のセキュリティポリシーの例

6.3.3.1 ISO/IEC TR 15446 の汎用システムの組織のセキュリティポリシー

ISO/IEC TR 15446 における一般的な組織のセキュリティポリシーは、以下の通り(図 6-9、表 6-14)。

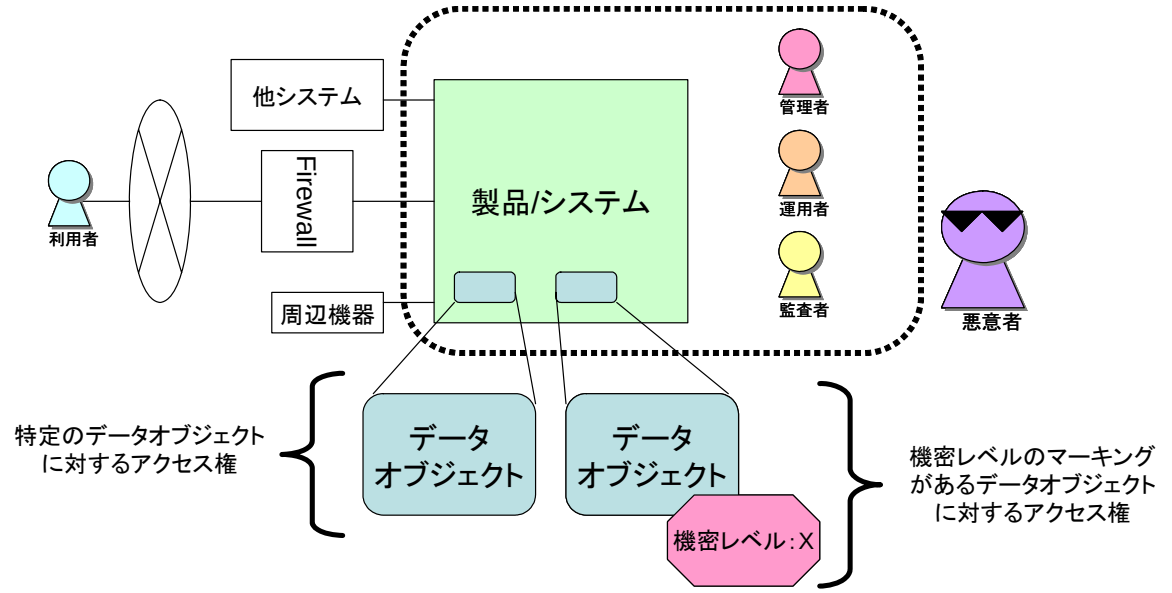

図 6-9：ISO/IEC TR 15446 の汎用システムの「組織のセキュリティポリシー」の分類

表 6-14：ISO/IEC TR 15446 の汎用システムの組織のセキュリティポリシー

#	分類	項目	説明
1		P.DAC	任意アクセス制御（Discretionary Access Control）に関するポリシー。 特定のデータオブジェクトに対するアクセス権は、以下の情報に基づき、決定される。 a) オブジェクトの所有者 b) アクセスを試みる主体者アイデンティティ c) オブジェクト所有者によって、その主体者に認められた暗黙的、あるいは、明示的なアクセス権、オブジェクトに対するアクセス権。
2		P.MAC	強制アクセス制御（Mandatory Access control）に関するポリシー。 情報に対するアクセス権は、以下のように決定。 The information is marked with a sensitivity designation. a) 見る権限を得れば、その個人は、情報を見ることを許可される。 b) 明示的な許可されない限り、その個人は、情報の sensitivity designation をダウングレードしてはならない。

6.3.3.2 ISO/IEC TR 15446 の暗号機能の組織のセキュリティポリシー

ISO/IEC TR 15446 の「C.4.3 Organizational security policies」において、TOEの暗号機能に係る組織のセキュリティポリシーの例が述べられている（表 6-15）。

表 6-15：SO/IEC TR 15446 の暗号機能の組織のセキュリティポリシー

#	ポリシー	
1	Identification and authentication policy	識別と認証に関するポリシー

2	User access control policy	ユーザアクセスコントロールに関するポリシー
3	Audit and accountability policy	監査と説明責任に関するポリシー
4	Cryptographic key management policy	暗号鍵の管理に関するポリシー
5	Physical security policy	物理的なセキュリティポリシー
6	Emanations policy	電磁波に関するポリシー

6.3.3.3 Baltimore 社のタイムスタンプサーバの組織のセキュリティポリシー

Baltimore社のSTにおける「組織ポリシー」は、以下の通りである(表 6-16)。

表 6-16:Baltimore 社のタイムスタンプサーバの組織のセキュリティポリシー

#	分類	項目	説明
1		P.Cryptography	全ての暗号処理(署名と検証)は、国家機関により認証されたアルゴリズムによって実装されなければならない。
2		P.Key_Generation_Destruction	全ての暗号キー、証明書(TOE 管理者とシステムに係るもの)は、国家機関により認定された方法を用いて、生成、破壊されなければならない。
3		P.Passphrases_PINs	全てのパスフレーズやPIN、これらは、TOEに係る私有鍵にアクセスするために必要となる、は、機密情報として管理されなければならない。また、国家機関の要件に従って、定期的に変更されなければならない。

6.3.3.4 日立製作所の認証局サーバの組織のセキュリティポリシー

日立製作所の認証局サーバのSTにおける組織のセキュリティポリシーは、以下の通りである(表 6-17)。

表 6-17:日立製作所の認証局サーバの組織のセキュリティポリシー

#	分類	項目	説明
1		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。
2		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。
3		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。
4		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。
5		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。
6		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。

7		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。
8		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。

7 脅威分析ガイドライン

本ガイドで推奨する Microsof 社の脅威分析モデルとリスク評価モデルを記述する。

7.1 脅威分析モデル

本ガイドでは、Microsoft 社の脅威分析モデルを採用する。脅威分析の手順例は、以下の通り。
(1)攻撃されやすいと思われるポイントを特定する
ポイントを特定後、以下の質問に関して、考察する。

- 各資産を保護するために、どのような「セキュリティ機構」が備わっているのか？
- 全ての遷移とインタフェースが適切に「セキュリティ」で保護されているのか？
- 機能を不適切に使用することにより、「セキュリティ」が意図せず脅かされる可能性はあるのか？
- 悪意をもって機能を使用することにより、「セキュリティ」が脅かされる可能性はあるか？
- 規定の設定で十分な「セキュリティ」を実現できるか？

(2) STRIDE モデルの脅威分類毎に脅威を抽出する
Microsoft社は、脅威分類モデルであるSTRIDEモデルを提唱している。STRIDEとは、以下の脅威項目の頭文字を連結したものである（表 7-1）。STRIDEの観点から脅威を分類する。

これらの脅威は関連性を持つ可能性がある。例えば、「権限の昇格」の脅威を利用した攻撃が、「情報漏洩」や「サービス拒否」を引き起こす可能性がある。

表 7-1：STRIDE の説明

#	脅威項目	説明
1	成りすまし （Spoofing）	偽のアイデンティティを使用し、システムへのアクセスを試みること。この脅威は、「盗まれたユーザ情報（ユーザ・クレデンシャル）」、あるいは、「偽の IP アドレス」により、現実化。 攻撃者は、正当なユーザあるいは、ホストとしてアクセス権を取得すると、その後、その権限を使用することによる、「権限の昇格」、つまり、「不正使用」が開始。
2	改ざん （Tampering）	許可されていないデータ改変を示す。例えば、二つのコンピュータ間の通信ネットワーク上を伝送するデータを改ざん。
3	否認 （Repudiation）	ユーザ（正当なユーザ、あるいは、悪意を持つユーザ）が、特定のアクションやトランザクションを実行した事実を否認できる可能性を示す。 適切な監査機能が無ければ、「否認」攻撃を証明することは難しい。
4	情報漏えい （Information disclosure）	プライベートデータが望まれていない暴露状態になること。例えば、許可されない人が、ファイルの内容を閲覧すること、あるいは、ネットワーク上を伝送する平文データをモニタリングすること。 「情報漏えい」の「脆弱性」の例は、(1)Web ページで hidden フォームタグを使用すること、また、(2)Web ページにコメントを含め、そのコメントに、データベース接続文字列や接続の詳細情報を記載すること、また、(3)例外処理結果をそのままクライアントに返すこと、例えば、内部的なシステムレベルエラーをクライアントに提供すること。どんな情報でも攻撃者にとっては役立つ。

5	サービス拒否（サービス妨害）、DoS 攻撃 （Denial of service）	システムやアプリケーションを使用できないようにするプロセスである。例えば、(1)サーバの全システムリソースを消費する要求を大量に送信することで、また、(2)アプリケーションプロセスをクラッシュさせる不正な入力データを渡すことで、現実化。
6	権限の昇格 （Elevation of privilege）	この攻撃は、制限された許可されたユーザが、許可されたユーザに成りすまし、アプリケーションに対するアクセス権限を取得するときに発生。

なお、列挙された脅威が、STRIDE に、完全にマッピングされるわけではないことに注意を要する。例えば、「暗号技術の脆弱化により、情報資産の信頼性が乏しくなる」という脅威は、STRIDE には直接当てはまらない。この脅威は、「当初想定された暗号技術の使用有効年限などに基づく情報資産の信頼性の保証期間が、暗号技術の脆弱化により、その保証期間が満たされない」という脅威として解釈できる。つまり、STRIDE の分類ではなく、ISO/IEC 13355 における「信頼性(Reliability)：The property of consistent intended behavior and results」の低下に関する脅威と言える。このように、STRIDE に直接マッピングできないと思われる脅威は、分類としては、「その他」などとする。

また、TOE毎に適切なSTRIDE内容に再解釈してもよい。例えば、以下は、資産に注目し、カスタマイズしたSTRIDE定義となる（表 7-2）。

表 7-2:カスタマイズした STRIDE 定義

#	項目	資産分類		解釈
1	Spoofing（成りすまし）	情報	相手に渡す情報	基本的に本カテゴリの脅威を考慮しない。 ただし、例外として、下記の観点から Spoofing（成りすまし）を捉えてもよい。 悪意者が、「情報資産」を偽造することで発生する脅威の一つとして捉える。 【脅威例】 悪意者が、「情報資産」を偽造し、正当なものだと偽って、流通させる（TOE の信頼性の低下、TOE を使ったサービスに関する風評の低下）。
2			相手から受け取る情報	基本的に本カテゴリの脅威を考慮しない。 ただし、例外として、下記の観点から Spoofing（成りすまし）を捉えてもよい。 悪意者が、「情報資産」を偽造することで発生する脅威の一つとして捉える。 【脅威例】 悪意者が、「情報資産」を偽造し、正当なものだと偽って、使用させる（TOE の信頼性の低下、TOE を使ったサービスに関する風評の低下）。
3			TOE 内で作成・利用する情報	基本的に本カテゴリの脅威を考慮しない。 ただし、例外として、下記の観点から Spoofing（成りすまし）を捉えてもよい。 悪意者が、「情報資産」を偽造することで発生する脅威の一

				つとして捉える。 【脅威例】 悪意者が、「情報資産」を偽造し、正当なものだと偽って、使用させる(TOE の信頼性の低下、TOE を使ったサービスに関する風評の低下)。
4		実装		悪意者が「IT 実装」にアクセスするときの脅威の一つとして捉える。 【脅威例】 正当なユーザ、あるいは、正当なコンポーネントに成りすまして「IT 実装」にアクセスする。
5	Tampering(改ざん)	情報	相手に渡す情報	「情報資産」の内容を修正・改変・改ざんすることに関する脅威である。 この脅威のカテゴリの中に、「情報資産」の「偽造」、「消去」に関わる脅威を含めてもよい。 また、脅威エージェントとして、悪意者だけでなく、内部者(不注意)も含めてもよい。
6			相手から受け取る情報	
7			TOE 内で作成・利用する情報	
8		実装		「IT 実装(CPU に依存したバイナリデータ、見読性のあるスクリプトデータ、など)」の内容を修正・改変・改ざんすることに関する脅威である。 この脅威のカテゴリの中に、「IT 実装」の全体の差し替え、あるいは、部分的な入れ替えによる「偽造」、あるいは、「IT 実装」の「消去」に関わる脅威を含めてもよい。
9	Repudiation(否認)	情報	相手に渡す情報	基本的に本カテゴリの脅威を考慮しない。 なお、例外として、「情報資産」を相手に渡した事実を否認できることに関する脅威を含めてもよい。
10			相手から受け取る情報	基本的に本カテゴリの脅威を考慮しない。 なお、例外として、「情報資産」を受け取った事実を否認できることに関する脅威を含めてもよい。
11			TOE 内で作成・利用する情報	基本的に本カテゴリの脅威を考慮しない。 なお、例外として、「情報資産」が作成された事実、修正された事実、利用された事実が、否認できることに関する脅威を含めてもよい。
12		実装		基本的に本カテゴリの脅威を考慮しない。 なお、例外として、IT 実装にアクセスすることに関わる否認行為を含めてもよい。
13	Information Disclosure (情報漏洩)	情報	相手に渡す情報	主に「通信路上」における情報漏えい、盗聴、などに関する脅威である。 本ガイドでは、オフラインでのデータ送受信時の情報漏洩はスコープ外である。
14			相手から受け取る情報	

15			TOE 内で作成・利用する情報	TOE 内から情報漏えいすることに関する脅威である。
16		実装		TOE 内から情報漏えいすることに関する脅威である。
17	Denial of Service（サービス妨害）	情報	相手に渡す情報	基本的に本カテゴリの脅威を考慮しない。
18			相手から受け取る情報	
19			TOE 内で作成・利用する情報	
20		実装		外部ネットワークを介した DoS 攻撃に関する脅威である。
21	Elevation of Privilege（権限の昇格）	情報	相手に渡す情報	基本的に本カテゴリの脅威を考慮しない。
22			相手から受け取る情報	
23			TOE 内で作成・利用する情報	
24		実装		

(3)抽出した脅威毎に「攻撃シナリオ」を記述する

潜在的に脆弱なすべてのポイントで、脅威の可能性を調査する。脆弱な各ポイントで、成りすまし、改ざん、否認、情報漏洩、サービス拒否、および権限の昇格、などの可能性のある脅威のカテゴリを特定する。脅威に対して、1つまたは複数の攻撃シナリオを作成する。

攻撃シナリオのモデリングには、「脅威ツリー」が役立つ。本ガイドでは、「脅威ツリー」を用いて、脅威分析することを推奨する。「脅威ツリー」とは、脅威、または、脆弱性の階層構造を示した図（図 7-1参照）である。悪意のあるユーザが攻撃を仕掛ける際に行う各手順を模擬的に示す。攻撃の最終的な目標は、「ツリーの最上部」に配置する。下位の各レベルは、攻撃を実行するために必要な手順や条件を示す。下位の複数のノードの条件が同時に満たされないと上位のノードが実現されない場合（AND関係）、または、下位の複数のノードのどれか一つが満たされれば、上位のノードが実現される場合(OR関係)がある。暗黙的には、OR関係である。

なお、本ガイドラインでは、悪意のあるユーザが明確ではない脅威に対する脅威ツリーも検討する。この場合、ルートノードは、脅威としてのイベント内容であり、下位のノードは、その脅威、あるいは、その上位ノードが実現するための条件である。

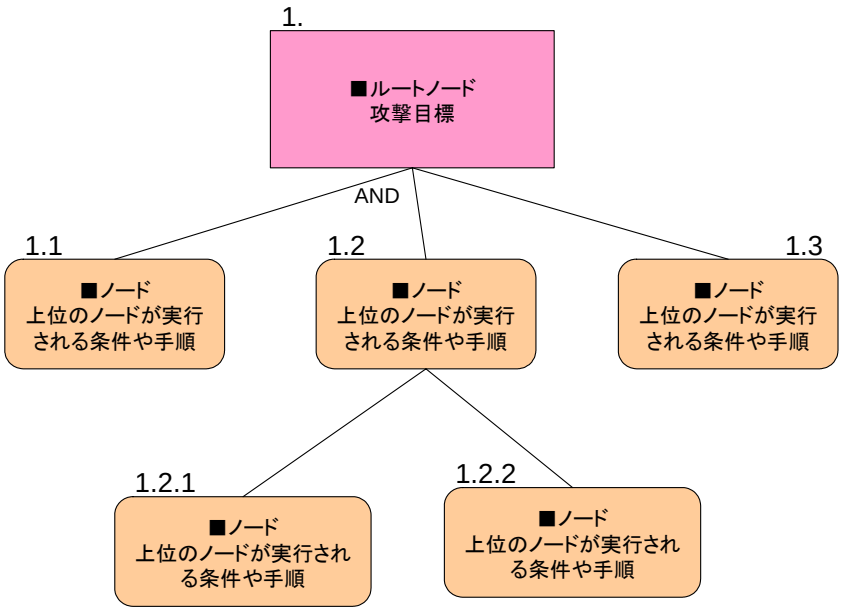

図 7-1:脅威ツリー

脅威ツリーは、テキストで表現することも可能である。上記の例をテキストで表現した例を以下に示す。

1 なになに脅威
  1.1 (AND)なになに条件
  1.2 (AND)なになに条件
    1.2.1 なになに条件
    1.2.2 なになに条件
  1.3 なになに条件

脅威ツリーの具体例を示す(図 7-2)。下記は、「悪意者が、評価対象システムが参照する時刻情報をずらす」という脅威に基づく、脅威ツリーの例である。

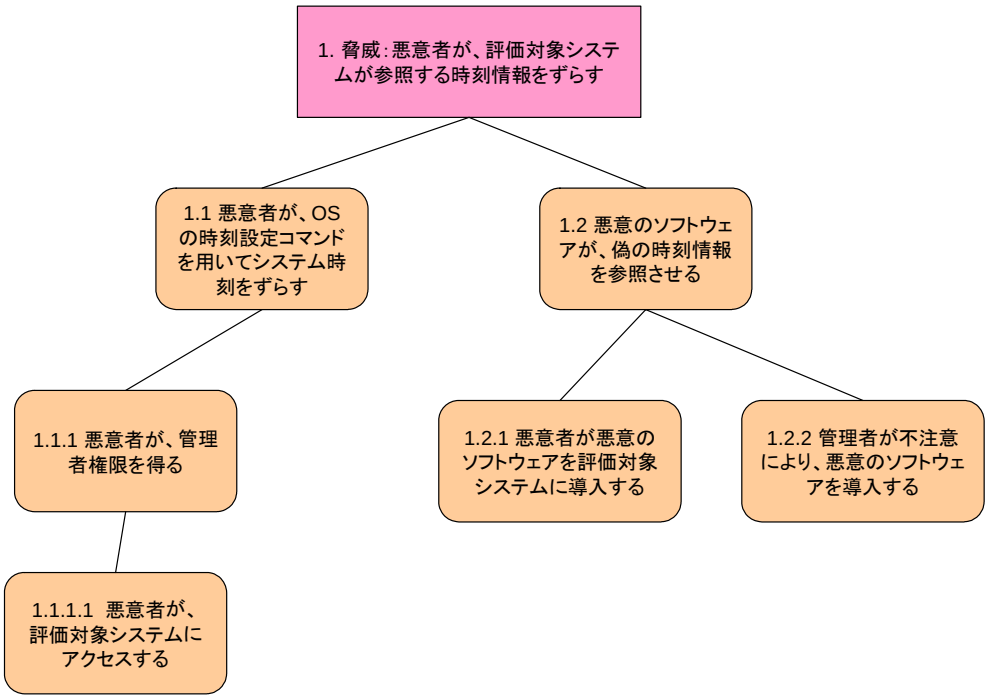

図 7-2:「時刻情報をずらす」脅威に対する脅威ツリーの例

上記で述べたMicrosoft社の脅威モデルに基づき、脅威を抽出し、以下の情報から構成される脅威情報をまとめる[9](表 7-3)。

表 7-3:脅威情報の構成要素

#	項目	説明
1	ID	脅威の識別情報。ISO/IEC 15408 の考え方に基づき、プリフィックス(T.)から始まる英語表現とする。
2	資産	脅威の対象となる「資産」を記述する。
3	STRIDE 分類	Microsoft 社の STRIDE モデルに基づき、脅威がどのように分類されるのかを記す。
4	ISO/IEC 15408 のセキュリティ特性への影響	資産に対する「責任追跡可能性」、「認証」、「可用性」、「機密性」、「完全性」、「信頼性」のどの特性が脅かされるのかを記す。
6	脅威エージェントの情報	脅威エージェント、及びその脅威エージェントの持つ「能力」、「動機[10]」、「利用可能資源」を記す。
7	攻撃の情報	攻撃に関する情報を記す。攻撃に関する「攻撃方法」、「攻撃機会」、「攻撃で利用される脆弱性」を明確化する。

例えば、「悪意者が、評価対象システムが参照する時刻情報をずらす」という脅威(脅威ツリーの 1.1、1.1.1、1.1.1.1 に該当)を例に脅威情報をまとめると以下の通りである(表 7-4)。

[9] 分かる範囲で記述する。
[10] 動機は、大きく二つに分類される；悪意と不注意に分類される。

表 7-4:「時刻情報をずらす」ことに関する脅威情報

#	項目		説明
1	ID		T.MODIFY_TIME_SOURCE
2	資産		システム時計
3	STRIDE 分類		改ざん(Tampering)
4	ISO/IEC 15408 のセキュリティ特性への影響	完全性	○(改ざんされた時刻情報)
		機密性	-
		可用性	-
		責任追跡可能性	-
		認証	-
		信頼性	○(正確な時刻を供給するという意図した動作から逸脱)
6	脅威エージェント	脅威エージェントの概要	外部の悪意者
		動機	悪意(悪戯、あるいは、システムの信頼性を低下させることにより、サービス提供者の評判を落とすこと)
		能力	-
		利用可能資源	-
7	攻撃	攻撃の概要	時刻変更コマンドを利用する。
		攻撃方法	システムに物理的にアクセスし、偽造、あるいは、取得した管理者パスワードを用いて、システムにログインし、OS が提供する時刻変更コマンドを実行する。
		攻撃機会	-
		利用する脆弱性	-

7.2 リスク評価モデル

抽出した脅威に対してリスク評価を行う。本ガイドでは、Microsoft 社の DREAD モデルにより、リスク評価することを推奨する。

一般的なリスク定義は、以下の通り。

Risk = Probability * Damage Potential リスク = 発生確率 * 損失額(潜在的)

リスクを厳密に見積もりことは困難である。そこで、上記のリスク定義を扱い易い形に加工して使用する。

【再スケール】
発生確率は、1 から 10 のスケールで表現:1 は、発生する可能性はほとんどない、10 は、ほぼ発生。
損失は、1 から 10 のスケールで表現:1 は、最小限の損失、10 は壊滅的。

リスクは、1 から 100 までのスケールを持つ。これらを High、Medium、Low の 3 レベルに格付けする。

【DREAD モデル】
セキュリティ評価メンバの全てが合意する形で格付けすることは困難である。DREAD モデルを導入し、リスクを計算する。

- 潜在的損失(Damage potential): 脆弱性を利用されたときに発生する損害はどの程度か(How great is the damage if the vulnerability is exploited?)
- 再現性(Reproducibility): 何度でも攻撃することが可能か(How easy is it to reproduce the attack?)

- 攻撃利用可能性(Exploitability): 攻撃をすることが容易か(How easy is it to launch an attack?)
- 影響ユーザ(Affected users): 攻撃により影響を受けるユーザはどの程度か(As a rough percentage, how many users are affected?)
- 発見可能性(Discoverability): 脆弱性が容易に発見されるか？(How easy is it to find the vulnerability?)

格付けのための簡易スキームを使用する。高(3)、中(2)、低(1)とする。以下は、典型的な脅威格付け表である(表 7-5)。この場合、5 から 15 のスケールを持つ。

表 7-5: 脅威格付けの簡易スキーム

	格付け	高(3)	中(2)	低(1)
D	潜在的損失 (Damage potential)	攻撃者は、セキュリティシステムを破ることが可能; 全ての権限を取得; 管理者として動作させることが可能、コンテンツをアップロード可能。 The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	機密情報が漏洩する。 Leaking sensitive information	機密性の低い情報が漏洩する。 Leaking trivial information
R	再現性 (Reproducibility)	いつでも攻撃を再現することが可能である。 The attack can be reproduced every time and does not require a timing window.	ある時間帯、かつ、特定の条件において、攻撃を再現することが可能である。 The attack can be reproduced, but only with a timing window and a particular race situation.	セキュリティホールの知識があったとしても、攻撃を再現することは非常に困難である。 The attack is very difficult to reproduce, even with knowledge of the security hole.
E	攻撃利用可能性 (Exploitability)	初心者のプログラマーであったとしても短時間で攻撃可能である。 A novice programmer could make the attack in a short time.	習熟したプログラマーであれば、攻撃可能である。攻撃が成功すれば繰り返すことが可能。 A skilled programmer could make the attack, then repeat the steps.	非常に習熟したプログラマーであれば攻撃可能。攻撃の度に高度な知識が必要。 The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	影響ユーザ (Affected users)	全てのユーザ、デフォルトの設定、重要な顧客。 All users, default configuration, key customers	一部のユーザ、デフォルトからカスタマイズした設定。 Some users, non-default configuration	非常に少数のユーザ。 Very small percentage of users, obscure feature; affects anonymous users
D	発見可能性 (Discoverability)	攻撃に関する公開情報がある。脆弱性は一般的であり、気付かれやすい。	製品のほとんど使用されない部分に脆弱性がある。少数のユーザがその脆弱性を見つける。	そのバグは、知られていない。ユーザは潜在的損失を分析できない。

		Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

なお、この簡易スキームをベースに、TOE毎に、DREADの内容を再解釈し、脅威格付けスキームを作成してもよい。例えば、以下のようなカスタマイズした脅威格付けスキームが考えられる(表 7-6)。

DREAD の項目毎に複数の視点が存在する。そのため、複数の視点毎にそれぞれの格付けが異なる（例：再現性において、悪意を持った内部者(高)が、ある時間帯のみに攻撃できる(中)、など。）場合が想定される。この時の「総合評価」を導出する方法に関しては、基本的に、最悪のケースに合わせるようにする。

表 7-6:カスタマイズした脅威格付けスキームの例

#	DREAD 分類	視点	高 (3)	中 (2)	低 (1)
1	Damage potential（潜在的損失）	サービス継続性	異常なサービス提供	異常なサービス提供をすることはないが、正常なサービス継続不可能	正常なサービス継続可能
		資産の流出		機密情報が漏洩する	重要情報が漏洩する
		資産の信頼性		機密情報の改ざん、偽造、消去	重要情報の改ざん、偽造、消去
2	Reproducibility（再現性）	攻撃時間帯	任意の時間に脅威が発生	ある時間帯のみ脅威が発生	ある限られた条件において脅威が発生
		脅威エージェント	悪意を持った内部者	外部者、あるいは利用者 自然(ある程度予知可能な要因による脅威発生)	不注意な内部者 自然や偶然(予知不可能な要因による脅威発生)
3	Exploitability(攻撃利用可能性)	脅威エージェント	悪意を持った内部者	外部者、あるいは利用者	不注意な内部者、あるいは、自然や偶然(予知不可能な要因による脅威発生)
		脅威エージェントが使用する攻撃ツールの入手・使用の容易性	TOE、あるいは、TOE の下位抽象マシンなどに標準的に備わる機能を直接利用	TOE、あるいは、TOE の下位抽象マシンに比較的入手可能な攻撃用のツールを導入要	TOE、あるいは、TOE の下位抽象マシンに攻撃者が新規に作成した独自の攻撃用ツールが必要
4	Affected users（影響ユーザ）	影響を受ける利用者の範囲	全ての利用者に影響が出る	一部の利用者に影響が出る	ごく少数の利用者に影響が出る 管理者/運用者/監査者の業務に影響が出る
5	Discoverability（発見可能性）	攻撃方法の公知性	脅威エージェントが外部者、あるいは、利用者である場合、攻撃方	脅威エージェントが外部者、あるいは、利用者である場合、攻撃方法は、	脅威エージェントが外部者、あるいは、利用者である場合、攻撃方法は、

			法は公知である 脅威エージェントが内部者(悪意)の場合、正規の運用方法で攻撃可能である。	少数のユーザに知られている 脅威エージェントが内部者(悪意)である場合、攻撃を行う際、正規の運用方法以外の手法も用いる必要がある	ほとんど未知である 脅威エージェントが内部者(不注意)である場合、正規の運用方法で脅威が発生する

統合化プラットフォームのセキュリティ評価においては、このDREADモデルに従い、抽出した脅威に関するリスクを評価する[11]。

簡易スキームの脅威格付け表に従い、「悪意者が、評価対象システムが参照する時刻情報をずらす」という脅威(脅威ツリーの1.1、1.1.1、1.1.1.1 に該当)に対するリスク評価を行うと以下の通りである(表 7-7)。

表 7-7:「時刻情報をずらす」ことに関する脅威に対するリスク評価

#	脅威 ID	潜在的損失	再現性	攻撃利用可能性	影響ユーザ	発見可能性	合計点
1	T.MODIFY_TIME_SOURCE	高(3)	低(1) ※入退出管理を突破すること困難	中(2)	高(3)	高(3)	12

11 全てのリスクを対策する(セキュリティ目標の策定、セキュリティ機能の策定)のではなく、「ある閾値」以上のリスクに対して対策するという方針とする。「閾値」に関しては、リスク評価プロセスを介して、決定する予定。

8 セキュリティ目標決定ガイドライン

評価対象システムにおけるセキュリティ環境に係る「セキュリティの課題」を踏まえて、評価対象システムにおけるセキュリティ目標を決定する。セキュリティ目標とは、セキュリティの課題を解決するための方針(What)である。具体的な対策 (How)に依存しないセキュリティ目標を策定する。なお、具体的な対策は、セキュリティ機能の策定に係る。

なお、セキュリティ目標決定作業の後に実施する ISO/IEC 15408 に厳格に基づいたセキュリティ機能要件の導出を行わない場合は、このセキュリティ目標策定において、具体的な対策を検討してもよい。

8.1 セキュリティ目標

ISO/IEC 15408 では、セキュリティ目標は、大きく二つに分類される(表 8-1)。一つは、評価対象システム(TOE)に対するセキュリティ目標であり、もう一つは、環境に対するセキュリティ目標である。TOEに対するセキュリティ目標は、TOEシステムのセキュリティ要件/機能によって実現化される。また、環境に対するセキュリティ目標は、IT(情報技術)によるセキュリティ要件、あるいは、Non-IT(非情報技術)によるセキュリティ要件につながる。

表 8-1:セキュリティ目標とその対策

セキュリティ目標	目標を実現するための対策
評価対象システムに対するセキュリティ目標	評価対象システムのセキュリティ要件/機能
環境に対するセキュリティ目標	IT(情報技術)によるセキュリティ要件/機能
	Non-IT(非情報技術)によるセキュリティ要件/機能

ISO/IEC TR 15446 や公開ドキュメントで記載された「セキュリティ目標」」の例を参照し、統合化プラットフォームシステムにおけるセキュリティ目標を決定する。

統合化プラットフォームシステムにおけるセキュリティ目標の識別子の命名規則は以下の通りである(表 8-2)。

表 8-2:セキュリティ目標の命名規則

セキュリティ目標	命名規則
評価対象システムに対するセキュリティ目標	プリフィックス(O.)をつける。
環境に対するセキュリティ目標	プリフィックス(OE.)をつける。

8.2 セキュリティ目標の例

8.2.1 ISO/IEC TR 15446 の汎用システムのセキュリティ目標

ISO/IEC TR 15446 で記載された汎用システムにおけるセキュリティ目標を以下に記す(表 8-3)。

表 8-3:ISO/IEC TR 15446 の汎用システムにおける「セキュリティ目標」

#	分類	項目	説明

1	TOE	O.ADMIN	TOE は許可された管理者が、TOE とそのセキュリティ機能を効果的に管理できるようにするための設備を提供し、許可された管理者のみがそのような機能性にアクセスできることを保証する。
2		O.ANON	TOE は利用者識別情報が他のエンティティに暴露されることなしに、サブジェクトが資源及びサービスを利用することを許す手段を提供する。
3		O.AUDIT	TOE はセキュリティに関連する事象を記録する手段を提供し、管理者が攻撃の可能性または、TOE が攻撃を受けやすい状態なるようなセキュリティ機構(feature)の設定ミスを検出することで管理者を助け、そして利用者がセキュリティに関連して遂行するいかなるアクションに対しても責任をもたせる状態を維持する。
4		O.DAC	TOE はその利用者に対して、個人利用者または識別された利用者のグループに基づき、また P.DAC セキュリティ方針で定義される規則のセットに従い、利用者が所有するまたは責任をもつオブジェクトや資源に対するアクセスを、制御及び制限する手段を提供する。
5		O.ENCRYPT	TOE は、ネットワークを介した2つのエンドシステム間での転送時に、情報の機密性を保護する手段を提供する。
6		O.ENTRY	TOE は、時間とエントリーするデバイスの場所を基に、利用者のエントリーを制限する能力をもつ。
7		O.I&A	TOE は、すべての利用者を一意に識別し、利用者が TOE の設備にアクセスすることを許可する前に、主張された識別情報を認証する。
8		O.INTEGRITY	TOE は、情報に及ぼされる完全性の損失を検出する手段を提供する。
9		O.LABEL	TOE は、TOE が保存及び処理する情報の秘匿ラベルの完全性を、保持及び維持する。TOE による(エクスポートされる)データ出力は、内部秘匿ラベルの正確な表現である秘匿ラベルをもつ。
10		O.MAC	TOE は、情報に対する個人の取扱許可(clearance)または許可(authorisation)と、その情報の秘匿指定との比較に直接基づき、P.MAC セキュリティ方針に従って、TOE が管理する責任をもつ情報の機密性を保護する。 ※このセキュリティ対策方針はもちろんあらゆる特定の情報フロー制御方針の対策方針に対して適切に訂正することができる。
11		O.NOREPUD	TOE は、情報の発信者が情報を送信したことをまんまと否定することを防ぐための証拠、及び情報の受信者が情報を受信したことをまんまと否定することを防ぐための証拠を生成するための手段を提供する。
12		O.PROTECT	TOE は、信頼できないサブジェクトによる外部からの妨害または改ざん、または信頼できないサブジェクトによるセキュリティ機能迂回の試みから自分自身を保護する。
13		O.PSEUD	TOE は、利用者識別情報が他のエンティティに暴露されることなく、サブジェクトが資源またはサービスを利用することを可能にし、さらにその利用に対するエンティティの責任を維持する手段を提供する。
14		O.RBAC	TOE は、利用者が、その利用者の役割に対して明示的な許可がない資源に対してアクセスを得ること、及び操作を実行することを防ぐ。
15		O.RESOURCE	TOE は、その利用者及びサブジェクトによる資源の利用を制御し、不当なサービス拒否を防ぐ手段を提供する。
16		O.ROLLBACK	TOE は、トランザクションの系列が不完全な場合、利用者にトランザクションを取り消すことを許可することにより、明瞭に定義された有効な状態に戻る手段を提供する。
17		O.UNLINK	TOE は一つのエンティティに資源またはサービスの複数利用を許し、他のエンティティがそれらの利用を結びつけることができないようにする手段を提

			供する。
18		O.UNOBS	TOE は利用者が資源またはサービスを利用し、他のエンティティがその資源またはサービスが利用されていることを観察することができないようにする手段を提供する。
19	環境	OE.AUDITLOG	TOE の管理者は監査設備が有効に利用及び管理されていることを保証しなければならない。とりわけ以下のように: a) 連続的な監査ログ収集を保証するために、適切なアクションが取られなければならない。例えば、監査証跡が枯渇する前に、十分な空き容量を保証する規則正しいログのアーカイブにより。 b) 監査ログは一定の基準で検査されるべきであり、そしてセキュリティ違反または将来セキュリティ違反を導きそうな事象を検出した場合、適切なアクションが取られなければならない。
20		OE.AUTHDATA	TOE に対して責任をもつ者は、各利用者の TOE に対する利用者アカウントの認証データが、セキュアに保持され、そのアカウントの利用を許可されていない利用者に対して暴露されないよう、保証しなければならない。
21		OE.CONNECT	TOE に対して責任をもつ者は、セキュリティを蝕もうとする外部システムまたは利用者との接続が、提供されないことを保証しなければならない。
22		OE.INSTALL	TOE に対して責任をもつ者は、IT セキュリティを維持するようなやり方で、TOE が配付され、インストールされ、管理され、そして運用されることを保証しなければならない。
23		OE.PHYSICAL	TOE に対して責任をもつ者は、IT セキュリティを危険にさらす恐れのある物理的攻撃から、TOE のセキュリティ方針の実施に重大な TOE のパーツが保護されることを保証しなければならない。
24		OE.RECOVERY	TOE に責任をもつ者はシステムの故障またはその他の中断の後、IT セキュリティが危険にさらされることなく回復できることを保証するための、手続き及びまたはメカニズムが適当であることを保証しなければならない

8.2.2 ISO/IEC TR 15446 の暗号機能のセキュリティ目標

ISO/IEC TR 15446 では、暗号機能に対するセキュリティ目標を以下のように掲げている(表 8-4)。

表 8-4:ISO/IEC TR 15446 の暗号機能における「セキュリティ目標」

#	分類	項目	説明
1	TOE	O.I&A	TOE は、すべての利用者を一意に識別しなければならず、TOE の機能にアクセスしようとする利用者に許可を与える前に、その主張する識別情報を認証しなければならない。
2		O.DAC	TOE は、TOE の利用者に対して、個別の利用者または識別された利用者グループに基づき、かつ裁量によるセキュリティ方針によって定義された規則のセットに沿って、利用者の所有する、または責任を持つオブジェクト及び資源へのアクセスを制御する、及び制限する手段を提供しなければならない。
3		O.PHP	TOE は、自分自身及びその中の暗号関連の IT 資産を、許可されない物理的アクセス、改変、または使用から保護すべきである。
4		O.INTEGRITY	TOE は、情報に影響を及ぼす完全性の喪失を検出する手段を提供しなければならない。
5		O.FAILSAFE	誤りの発生する事象において、TOE はセキュアな状態を保たねばならない。
6		O.ADMIN	TOE は、許可された管理者が TOE 及びそのセキュリティ機能を効果的に管理できるようにする機能性を提供しなければならず、かつ、許可された管理者だけがその機能性にアクセスできることを保証しなければならない。

7	環境	OE.EMI	TOE の電磁波放射によって、許可されない者または利用者に暗号関連の IT 資産が暴露されることを防ぐため、手続き的及び物理的手段がとられるべきである。
8		OE.PHYSICAL	TOE に責任を持つ者は、セキュリティ方針の実施において重要となる部分が、IT セキュリティを脅かす恐れのある物理的攻撃から保護されることを保証しなければならない。

8.2.3 Baltimore 社のタイムスタンプサーバのセキュリティ目標

Baltimore社のSTにおいて記載されたセキュリティ目標は、以下の通り(表 8-5)。

表 8-5:Baltimore 社のタイムスタンプサーバにおける「セキュリティ目標」

#	分類	項目	説明
1	TOE	O.Ident_Authent	TOE の管理者を固有に特定することを保証すること。 さらに、TOE 管理者が、TOE のセキュリティ関連データにアクセスすることを許可される前に、その TOE 管理者を認証することを保証すること。
2		O.Timestamp	タイムスタンプトークンの生成・発行を行う手段を提供する。タイムスタンプトークンは、TOE のアイデンティティと関連付けられることを保証する手段を提供する。
3		O.Audit	セキュリティに関連するイベントを記録する手段を提供する。 TOE の管理者が、イベント記録を格納したログの完全性を確認できること。 TOE は、直前の記録に対する改変・削除を検出する手段を提供。ただし、新しい記録が追加される前の最新の記録に対する改変・削除は検知できない。
4		O.Integrity_Config	TOE の設定の完全性を確保する手段を提供する。設定とは、Configuration Parameters File に格納された設定情報。Audit 鍵と TSA 鍵の保護も含む。
5	環境	OE_Time_Source	タイムスタンプに使用する時刻ソースの可用性を保証する。また、時刻ソースの信頼性と正確性は、TOE 所有者にとって受容可能であることを保証する。
6		OE.PKI	TOE は、安全に管理された PKI の中で運用されることを保証する。鍵/証明書は、安全に発行・失効される。鍵/証明書を使用する前には、鍵/証明書のステータスが確認される。
7		OE.Cryptography	国家機関によって認定されたアルゴリズムを実装して暗号処理(署名・検証)が行われることを保証する。
8		OE.P11_Device	以下の仕様を持つハードウェア装置を使用することを保証する。 ・ RSA(1024 ビット、あるいは、2048 ビット)と DSA(1024 ビット)の署名・検証の実装 ・ SHA-1 のハッシュ関数の実装 ・ PKCS#11 規格に準拠 また、国家機関に認定、あるいは、CC EAL3 相当の装置であること。
9		OE.Key_Generation_Destruction	国家機関によって認定された方法で、鍵の生成・破棄を行うこと。
10		OE.Passphrases_PINs	国家機関の要件に合致するように、パスフレーズと PINs の管理を行うこと。

11		OE.Key_Storage	秘密鍵は安全に管理し、TOE 管理者以外からアクセスできないようにすること。
12		OE.Physical	TOE に対する物理的な攻撃から保護すること。
13		OE.Connectivity	TOE から IT セキュリティを低下させる外部システムへの接続を許可しないこと。
14		OE.System_Administrator	システム管理者は、責務を実行できるように、必要な知識を持ち十分な訓練を受けるようになっていること。 システム管理者は、IT セキュリティを維持するように TOE を導入し、管理することを保証する。
15		OE.TOE_Administrator	TOE 管理者は、責務を実行できるように、必要な知識を持ち十分な訓練を受けるようになっていること。 TOE 管理者は、IT セキュリティを維持するように TOE を設定し、動作させることを保証すること。
16		OE.TS_Requestor	タイムスタンプ要求者は、受け取ったタイムスタンプトークンを検証・保持する責任を持つ。アウト・オブ・バウンド方法により、TSA 証明書が失効していないこと、また、正当な TSA の署名がタイムスタンプトークンに付与されていることを確認すること。 タイムスタンプ要求者は、否認防止の証拠として、タイムスタンプトークンを保持する。
17		OE.Audit_Log	Audit ログの管理と保護手段を提供する。 ・ ログ保管のための十分なスペースを確保すること。 ・ TOE 自体が Audit ログの保護手段を提供しているが、環境もある保護手段を提供する。何故ならば、最新の記録が削除されてしまうとそれを検知できないため。

8.2.4 日立製作所の認証局サーバのセキュリティ目標

日立製作所の認証局サーバのセキュリティ目標は、以下の通りである(表 8-6)。

表 8-6: 日立製作所の認証局サーバの「セキュリティ目標」

#	分類	項目	説明
1	TOE	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。
2		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。
3		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		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
5		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。
6		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。
7		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。
8		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。
9	環境	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。
10		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。
11		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。
12		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。
13		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。
14		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。
15		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。
16		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。
17		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。
18		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。
19		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。
20		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。

8.3 脅威とセキュリティ目標のマッピング例

ISO/IEC TR 15446 では、汎用システムに対する脅威とそれに対するセキュリティ目標（TOE、あるいは、環境における）の例を記している（表 8-7）。セキュリティ目標としては、「防止」、「検出」、「回復」に分類して記載している[12]。

表 8-7：ISO/IEC TR 15446 における脅威とセキュリティ目標の対応例

#	資産	脅威	セキュリティ目標	
1	ストレージ・メディア上のデータ	不正にメディアを抜き出しデータが暴露。	防止	メディアの抜き出しを制御/管理。 データ暴露を防止（例：暗号化など）。
			検出	メディア・ストレージの制御/管理
			回復	-
2		許可を得ていない人物によりデータが参照、改変、削除。また、アプリケーションからデータが追加、あるいは、アプリケーションへデータを追加。	防止	運用管理（例：アプリケーションプログラムや端末などの使用を制限）。 データアクセスに対する権限制御/管理。
			検出	操作ログの監査、データ改ざんの検知、データのシークエンス番号の管理。
			回復	バックアップ/リストア
3		許可を得ていない人物によりデータがストレージ・メディア上にダンプ化。データが暴露	防止	運用管理（例：アプリケーションプログラムや端末などの使用を制限）。 データアクセスに対する権限制御/管理。
			検出	操作ログの監査
			防止	-
4		メディア上に残ったデータが参照される	防止	データ削除上にデータ領域をクリア。 データ暴露の防止（例：暗号化など）
			検出	-
			回復	-
5		不正にデータがコピーされる	防止	操作管理（例：コピー機能操作の制限、アプリケーションや端末の操作制限）。 データアクセスの権限制御/管理。

[12] ISO/IEC 15408 では、セキュリティ目標として、「防止」、「検出」、「回復」のどれを選択すべきかなどの規定はない。PP/ST 作成者に選択は委ねられている。そのため、ある脅威の対策として、「防止」の目標を定め、他の脅威の対策として、「検出」の目標を設定することは可能である。

				データ暴露の防止(例:暗号化など)
			検出	操作ログの監査。 オリジナルデータの制御/管理(例:電子透かし)
			回復	-
6		許可されない人物により、不正にデータが使用、あるいは、データアクセス属性が変更され、使用が妨害される。	防止	操作管理(例:データ属性の変更機能の使用制限、アプリケーションや端末の操作制限)。 属性のレジストリデータへのアクセス権限の制御/管理。
			検出	操作ログ監査。
			回復	バックアップ/リストア
7		ファイルが偽造されることにより、データが不正になる	防止	運用管理(例:ファイル作成/削除機能の使用制限、アプリケーションや端末の操作制限)。 データの暴露の防止(例:暗号化など)
			検出	ファイル所有者の監査。
			回復	-
8		メディアが破壊されることによりデータが損失。	防止	メディア・ストレージ場所の物理的な管理と入退室の管理。 ストレージ・メディアに対する二重化構成の採用。
			検出	メディア・ストレージの制御/管理
			回復	バックアップ/リストア。
9		メディアの I/O 装置のハードウェア故障により、データが破壊、あるいは、使用が妨害。	防止	I/O 装置の品質管理。 ストレージ・メディアの二重化構成の採用。
			検出	故障の検出(OS)。 プログラム実行ログの監査。
			回復	バックアップ/リストア
10		許可を得ていない人物があるコマンドを用いて、データを参照、改変、削除、追加。	防止	運用管理(例:コマンドの使用の制限、端末の使用の制限)。 データアクセスの権限の制御/管理。
			検出	操作ログの監査。 データ改変の検出。 データのシークエンス番号の管理。
			回復	バックアップ/リストア
11		秘密鍵の損失により、暗号化されたデータが、復号化できない。	防止	厳密な管理の下で秘密鍵を保持。
			検出	-
			回復	秘密鍵のリカバリ。
12		許可された人物が不注意でデータを削除。	防止	高品質な運用マニュアルの提供、運用の自動化。 運用エラーの防止(例:データ削除の再確認、削除権限をシークエンスに登録)。
			検出	操作ログの監査。
			回復	バックアップ/リストア。
13	通信路上のデータ	データの盗聴と破壊。	防止	通信路を物理的に保護、通信路に接続する装置の管理。 データの暴露の防止、データ破壊の検出(例:通信路の暗号化:VPN、SSL、IPSec など)。
			検出	データの破壊の検出。
			回復	データの再送。
14		中継システム上で、データが盗聴、改ざん、削除される。	防止	中継システムの運用管理(例:LAN プロトコルアナライザーの使用制限)。

			検出	-
			回復	-
15		中継システム上で、送信先の変更、送信者の変更、アクセス属性の変更などによりデータが不正に使用される	防止	通信データの保護管理(例:暗号化など)。 中継システムの運用管理(例:でバック機能の使用制限など)
			検出	制御/管理データの改ざんの検出。 デバックツール操作ログの監査。
			回復	データの再送。
16		通信路の故障により、通信が不能になる	防止	通信回線の二重化。 通信路の品質管理。
			検出	故障の検出(OS)
			回復	データの再送。
17		通信回線の異常により、通信が不能になる。	防止	通信回線の二重化。 通信路の品質管理。
			検出	故障の検出(OS)
			回復	データの再送。
18		データが不正に再送される。	防止	中継システムの運用管理(例:プログラム登録を制限)
			検出	再送の防止(シークエンス番号の割り当て、タイムスタンプの割り当て)
			回復	-
19	アプリケーションプログラム	許可されていない人物により、アプリケーションが実行。	防止	プログラム実行権限の制御/管理。 中継システムの運用管理(不要なプログラムの表示を制限)。 実行場所と実行ルートの管理。 オペレータ不在時の対策の提供。 アプリケーション端末の使用を制限。
			検出	アプリケーション実行ログの監査。
			回復	関連するデータのバックアップ/リストア。
20		許可されていない人物により、プログラムライブラリに含まれるデータが参照、改ざん、削除。	防止	プログラムライブラリへのアクセス権限の制御/管理。 運用管理(修正コマンドの使用を制限)。 端末の使用の制限。
			検出	操作ログの監査。
			回復	プログラムのバックアップ/リストア
21		許可されていない人物により、アクセス属性が変更されることで、プログラムが不正に使用、あるいは、使用が妨害される。	防止	プログラム実行権限の制御/管理。 プログラムライブラリのディレクトリのアクセス権限の制御/コントロール。 運用管理(修正コマンドの使用を制限)。
			検出	操作ログの監査。
			回復	-
22		コンピュータのハードウェア故障により、プログラム実行上に異常が発生する。	防止	ハードウェアの二重化構成の採用。 ハードウェアの品質管理。
			検出	故障の検出(OS)。
			回復	ハードウェアのリカバリ。
23	アプリケーションの処理及びデータ	不正なアプリケーション処理が実行される(Telnet や FTP など)	防止	プログラム実行の権限の制御/管理。 ファイアウォールの設置(アプリケーション・フィルタリング)。 操作規定の明確化。
			検出	プログラム実行ログの監査。

			回復	-
24		処理が妨害される（DoS 攻撃）	防止	プロセス処理に対して優先度を与える。 メール中継機能の禁止。
			検出	ネットワークアクセスログの監査。
			回復	-
25		データ交換やデータ内容が否認される。	防止	否認防止手段（例えば、TTP を使用し、証拠を蓄積、あるいは、暗号化機能）。 運用規定の明確化。
			検出	-
			回復	-
26		データのオリジナルが拒否される	防止	信頼のできるサービスを利用（データのオリジナリティを保証する） 運用規定の明確化。
			検出	-
			回復	-
27		データが不正に送信される。	防止	データフローの制御/管理（ファイアウォールやルール DB の制御/管理）。 アプリケーションプログラムの品質管理。 運用管理（例:プログラム登録の制限）。
			検出	データアクセスの監査。
			回復	-
28		デバック機能を用いてデータやプログラムを不正に使用。	防止	データアクセス権限、アプリケーション実行権限の制御/管理。 運用管理（デバック機能の使用制限）。
			検出	アプリケーション実行ログの監査。
			回復	-
29		サービス機能が不適切に拒否される。	防止	プロセス処理に対して優先度を与える。 アプリケーションプログラムの品質管理。 アプリケーションのスタッフに対して教育と規定を与える。 処理ハードウェアの品質管理。 処理リソースの容量の見積もり。
			検出	アプリケーション実行ログの監査。
			回復	-
30		コンテンツが改ざんされる、あるいは、破壊される。	防止	コンテンツの使用権限の制御/管理。 コンテンツの作成やダウンロードの管理。
			検出	コンテンツの改ざん検出。
			回復	コンテンツのバックアップ/リストア。
31		不正な操作。	防止	実行操作の権限の制御/管理。 操作場所と操作ルートの管理（リモート、インターネット経由、など）。
			検出	操作ログの監査。
			回復	-
32		プライバシーの侵害。	防止	プライバシー情報の使用権限の制御/管理。 匿名性の使用。 実名へリンクしないことを保証。
			検出	-
			回復	-

33	表示データ	許可されていない人物によりデータが閲覧。	防止	ディスプレイを物理的に隔離。 運用規定の強制。
			検出	-
			回復	-
34		不正なコピーとプリントアウト。	防止	許可された人物が不在時の対策を提供。 コピーやプリントアウト機能の使用権限の制御/管理。 運用規定の強制。
			検出	オリジナルデータの制御/管理(例:電子透かし)
			回復	-
35	入力データ	入力時にデータが暴露。	防止	入力端末室へのアクセス制御/管理。 運用規定の強制。
			検出	-
			回復	-
36		入力データが不正に持ち出される。	防止	入力データ保管場所の管理。 運用規定の強制。
			検出	-
			回復	-
37	出力データ(プリントアウトデータ)	許可されていない人物が、データを参照、取得。	防止	出力データを物理的に制御/管理。 運用規定の強制。
			検出	-
			回復	-
38		不正なコピー。	防止	コピーに対する対策を提供。 運用規定の強制。
			検出	オリジナルデータの制御/管理(例:電子透かし)
			回復	-
39	ユーザデータ	ユーザ(個人、システム、端末)が、識別できない。	防止	アクセス時に識別。 識別情報(各ユーザにIDを付与、IPアドレス)。 場所の制限(フィルタリング)。
			検出	識別処理ログの監査。
			回復	-
40		暴露したユーザ(個人、システム、端末)識別情報を用いて、成りすます。	防止	ユーザ認証。 識別情報の制御/管理。
			検出	識別処理の監査。
			回復	-
41		ユーザが識別されない。	防止	認証画面の表示。 信頼のできる識別。 認証(秘密鍵の暗号化、パスワード、所有物、物理的な特徴)。 コールバック。
			検出	認証処理の監査。
			回復	-
42		不正に暴露された認証情報を用いて成りすまし。	防止	複数の認証メカニズムを採用。 サーバのアクセス管理(被害の早期検出;認証処理情報の通知)。 機密性のあるメディア内に認証情報を保存。 認証情報の保護(一方向性の暗号化)。 アクセス・ルートの制限(例:公衆通信路やインターネット)

				ワンタイム・パスワード
			検出	システムアクセスの監査。
			回復	ユーザ単位での処理停止。
43		不正に推論された認証情報を用いて成りすまし。	防止	認証(推論の予防;リトライ回数の制限) サーバのアクセス管理(被害の早期検出;サーバを長期間使用していないユーザへの対策)。 複数の認証メカニズムの採用。 認証情報の制御/管理(推論の予防、長い秘密暗号鍵、シンタックスルール、初期値の変更、生成管理)。
			検出	システムアクセスのログ監査。
			回復	ユーザ単位での処理停止。 影響の最小限化(有効期間)。
44		不正な認証情報を用いて成りすまし。	防止	認証情報の妥当性を確認。 認証情報の制御/管理(無効情報の制御/管理)。
			検出	システムアクセスのログ管理。
			回復	-
45		ユーザ権限の修正登録に失敗し、不正な権限が使用される。	防止	ユーザ制御/管理(ユーザ権限の修正を即座に反映)。
			検出	システムアクセスのログ管理。
			回復	-
46		ユーザの行為が不正に暴露(プライバシーの侵害)	防止	ユーザに関わるログ情報へのアクセス権限の管理。 匿名性の使用。 実名との関連性をなくす。
			検出	システムアクセスのログ管理。
			回復	-
47		データ送信の否認。	防止	送信の否認を予防。 運用規定。
			検出	データ交換ログの監査。
			回復	-
48		データ所有を否認。	防止	データ作成時に、自動的に所有者を登録。
			検出	システムアクセスのログ監査。
			回復	-
49		データ受信の否認	防止	受信の否認を予防。 運用規定。
			検出	データ交換ログの監査。
			回復	-
50		成りすましや仕様不良により、間違った受信者へデータを送信。	防止	送信先の認証。 運用規定。
			検出	データ交換ログの監査。
			回復	-
51		認証情報を偽造し、成りすまし。	防止	認証情報へのアクセス権限の管理。 認証情報の妥当性を確認。 認証情報の制御/管理(偽造の予防、信頼のできる認証組織、所有物の物理的な保護)。
			検出	サーバのアクセス管理(被害の初期検出)。
			回復	-
52	システムサービスとデータ	秘密の暗号化鍵が、復号化し、システムセキュリティが低	防止	十分な強度と長さを持つ暗号化鍵を生成し、標準的な鍵配送プロトコルを採用。

		下。	検出	システム運用ログの監査。
			回復	新しい鍵の設定。
53		操作者が不在時に成りすましのユーザが不正にシステムを使用。	防止	操作者が不在時の対策の提供(一時停止、セッションの切断、再認証)
			検出	-
			回復	-
54		許可されたユーザが悪意、あるいは、不注意からシステムセキュリティを低下。	防止	許可されたユーザの誤りを予防(例:再確認)。 ユーザ権限の制御/管理(必要最小限の権限)。 監査管理、規定、教育、罰則。
			検出	システム操作ログの監査。
			回復	-
55		コンピュータウィルスの侵入	防止	ダウンロードしたプログラムやメールの添付ファイルに対するウィルスチェック。 アクセス制御/管理(適切なアクセス権限とファイルの保護)。 外部から得たデータやプログラムの使用及び実行の禁止。 ソフトウェア導入の制御/管理。
			検出	システム操作ログの監査。
			回復	必要な行為の実行(例:システムの停止。外部システムとの接続を切断)。
56		システムに対する不正な侵入	防止	ユーザ識別、認証、権限の確認(保護対象セグメントへのアクセス時、あるいは、ログイン時)。 システム構成の管理(例:接続された装置、外部への接続)。 ユーザ管理。
			検出	システム運用ログの監査。
			回復	-
57		既知のプロトコル欠陥(例:IPプロトコルや Sendmail)を悪用し、システムに侵入。	防止	ファイアウォール(フィルタリング)。 システムリソースへのアクセス制限/管理。 プログラムやプロトコルへのアクセスの制限。
			検出	システム運用ログの監査。
			回復	-
58		システムプログラムの不正な入れ替えによるシステムセキュリティの低下。	防止	システムプログラムライブラリへのアクセス制御/管理。 運用管理(システムプログラムの維持の規定)。
			検出	プログラムライブラリへのアクセスログの監査。
			回復	プログラムのバックアップ。
59		システムプログラムの破壊によるサービスの停止。	防止	システムプログラムライブラリの二重構成化。 メディア管理と運用管理(システムプログラムライブラリ)
			検出	-
			回復	-
60		不正なシステム運用	防止	操作コマンドの実行権限の制御/管理。 運用管理(操作コマンドの使用制限)。
			検出	運用ログの監査。
			回復	-
61	情報装置	破壊、あるいは、持ち出され	防止	二重化構成。

		る。		装置の設置場所へのアクセス制御/管理。 装置を管理下に置く。
			検出	-
			回復	-
62		電源が落とされる	防止	電源のバックアップ。 UPS。
			検出	-
			回復	電源のリカバリ。

9 セキュリティ機能策定ガイドライン

セキュリティ目標[13]を実現化するためのセキュリティ要件及びセキュリティ機能を明確化する。ISO/IEC 15408-2 に記載された「セキュリティ要件」カタログや公開ドキュメント(例えば、IPAが参考資料としてWeb公開/PDF入手可能な「CC Ver.2.1 の日本語訳 第1.4版」)を参照し、統合化プラットフォームシステムにおけるセキュリティ要件/機能を策定する。

ここでは、ISO/IEC 15408-2 におけるセキュリティ機能要件の概要を示し、さらに、公開ドキュメント(SO/IEC TR 15446、タイムスタンプ検証サーバの ST、認証サーバの ST)で記されたセキュリティ要件の例について記す。

なお、ISO/IEC 15408-2 で定義されたセキュリティ機能要件は、抽象的な記述も含まれるため、その意味を正しく理解することは容易ではない。また、139 種類のコンポーネントの内容と TOE の機能をマッピングする作業もスキルが必要な作業となる。本ガイドでは、セキュリティ要件とセキュリティ機能の策定までは必須とはしない。

9.1 セキュリティ機能要件のカタログ

ISO/IEC 15408-2 では、評価対象システム(TOE)及び環境の IT 機能として備えるべきセキュリティ要件のカタログが記載されている。セキュリティ要件は、クラス、ファミリ、コンポーネント、エレメントの順番に分類されている。ISO/IEC 15408-2 では、クラスは、11 種類、ファミリは、67 種類、コンポーネントは、137 種類存在する。

9.1.1 セキュリティ機能要件の命名規則

セキュリティ要件は、固有の識別子が割り当てられている。例えば、「TSF(TOEのセキュリティ機能)は、各監査記録において少なくとも以下の情報(※省略)を記録しなければならない」というセキュリティ要件は、「FAU_GEN.1.2」と表現される。ここで、「FAU_GEN.1.2」の意味は、以下の通りである(表 9-1、図 9-1)。

表 9-1:FAU_GEN.1.2 の意味

#	文字列要素	説明
1	F	機能要件を示す。
2	AU	セキュリティ機能要件における「セキュリティ監査」クラスに所属する。
3	GEN	「セキュリティ監査」クラスにおける「セキュリティ監査データ生成」ファミリに所属する。
4	1	「セキュリティ監査データ生成」ファミリに含まれる「監査データ生成」コンポーネントを示す。
5	2	「監査データ生成」コンポーネントに含まれる第2番目のエレメントを示す。

[13] TOE のセキュリティ目標である。環境に対するセキュリティ目標に関しては、基本的にスコープ外である。

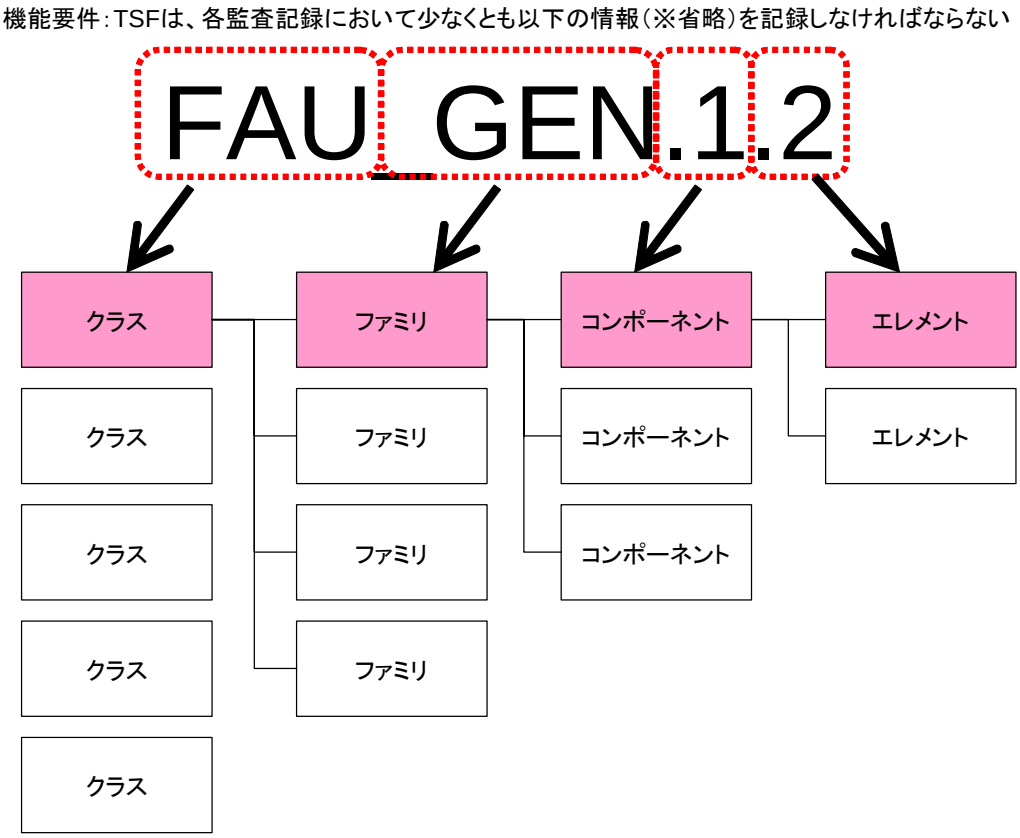

図 9-1：FAU_GEN.1.2 で示されるセキュリティ機能要件

統合化プラットフォームシステムのセキュリティ評価においては、ISO/IEC 15408 Part2 のセキュリティ機能要件のカタログを以下のように利用する。

（1）前章にて明確化した「セキュリティ目標」に対応すると思われる「セキュリティ機能要件のファミリレベル」を選択

（2）引き続き、該当するファミリ内の適当な「機能コンポーネント」を選択

（3）次に、時間/コストの許す限り、「機能コンポーネント」の詳細内容の適合性を検討

- 機能コンポーネントの依存関係を確認し、必要かどうかを判断する（保証要件「Axx_」に関しては、考慮しない）。
- 各ファミリの「管理」の項に記載されていることは管理機能として考慮すべきか否か。
- 「最小」レベルの監査対象事象が記録できるかどうかの確認（例えば、FAU_GEN.1 など）。

9.1.2 分散システムにおけるセキュリティ機能の重要な概念

ISO/IEC 15408 Part2 では、分散システムをTOEとした場合のセキュリティ機能の概要図を示している。セキュリティ機能要件を正しく選択するためには、データ交換や通信に関する用語の意味を深く理解する必要がある。図 9-2は、分散TOEにおけるデータ交換や通信に関する用語を整理したものである。

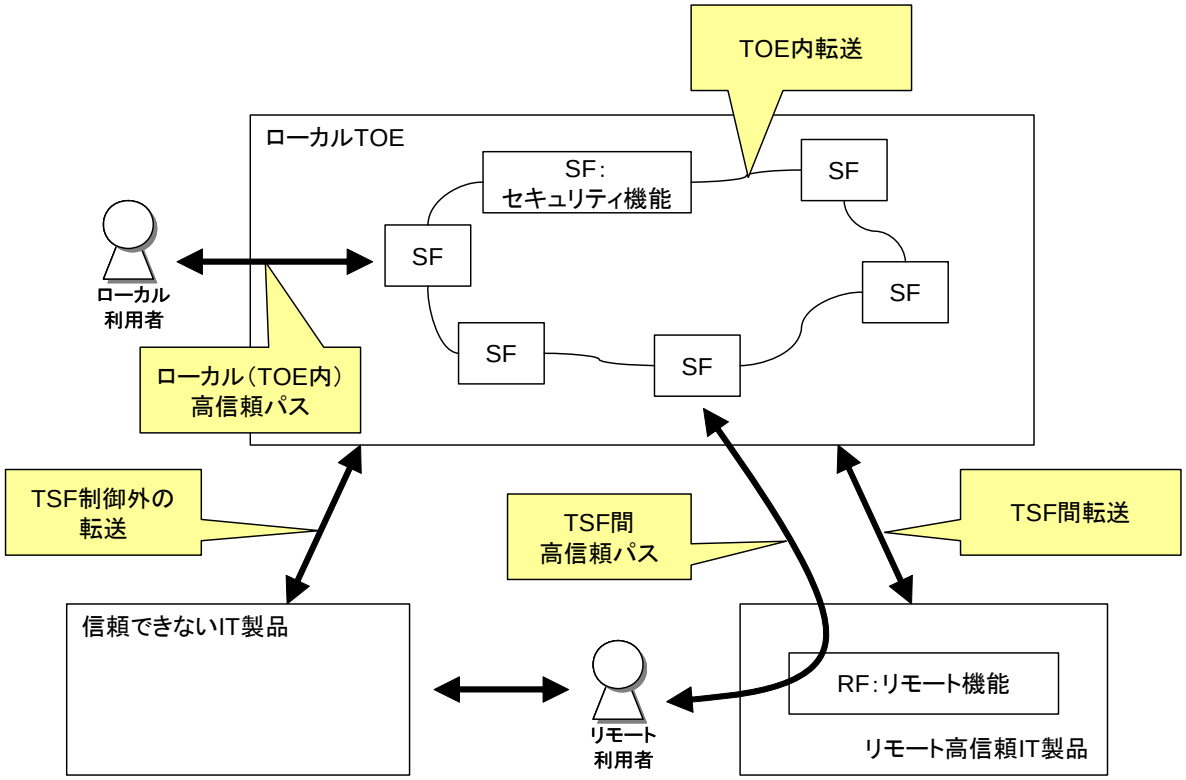

図 9-2:分散 TOE におけるセキュリティ機能の図(ISO/IEC 15408-2 の図を元に作成)

9.1.3 セキュリティ機能要件のクラス・ファミリ・コンポーネント

ISO/IEC 15408-2 で示されるクラス・ファミリ・コンポーネントは、以下の通りである（表 9-2）。

表 9-2:セキュリティ機能要件のクラス

#	クラス名	説明
1	FAU	セキュリティ監査(Security audit)を示す。セキュリティ監査は、セキュリティ関連のアクティビティ（つまり、TSP によって制御/管理されたアクティビティ）に関係する情報の認識、記録、格納、分析から構成される。
2	FCO	通信(Communication)を示す。データ交換に関与する参加者の識別情報を保証する。
3	FCS	暗号サポート(Cryptographic support)である。識別と認証、否認防止、高信頼パス/チャネル、データ分離などを実現/補助するための暗号機能。TOE が暗号機能を実装する時に使用。
4	FDP	利用者データ保護(User data protection)を示す。
5	FIA	識別と認証(Identification and authentication)を示す。主張してきたユーザの本人性を確かめる。識別と認証は、ユーザが、適切なセキュリティ属性（例:本人性、グループ、役割、セキュリティあるいは完全性のレベル）と関係付けられていることを保証することが要求される。
6	FMT	セキュリティ管理(Security management)である。TSF のいくつかの側面（セキュリティ属性、TSF データ、機能）の管理を明確化する。
7	FPR	プライバシー(Privacy)を示す。他の利用者による識別情報の露見と悪用から利用者を保護する。
8	FPT	TSF の保護(Protection of the TSF)である。TSF（特定の TSP から独立したもの）を提供するメカニズムの完全性と管理に関わる要件。また、TSF データの完全性に関わる要件。
9	FRU	資源利用(Resource utilization)である。処理能力及び/または格納容量など、必要な資源の可用性をサ

		ポートする。
10	FTA	TOE アクセス(TOE access)である。ユーザとのセッション確立を制御/管理する要件。
11	FTP	高信頼パス/チャネル(Trusted path/channels)を示す。ユーザとTSF 間の高信頼通信パス、及びTSF と他の高信頼 IT 製品間の高信頼通信チャネルのための要件。

9.1.4 FAU（セキュリティ監査）

FAUクラスのファミリは、以下の通りである（表 9-3）。

表 9-3：FAU クラスのファミリ

#	ファミリ	説明
1	FAU_ARP セキュリティ監査自動応答 (Security audit automatic response)	このファミリでは、セキュリティ侵害の可能性が検出された場合、自動的に応答するようなTSF における要件を定義している。
2	FAU_GEN セキュリティ監査データ生成 (Security audit data generation)	このファミリでは、TSF の制御下で発生するセキュリティ関連事象を記録するための要件を定義している。このファミリは、監査レベルを識別し、TSF による監査対象としなければならない事象の種別を列挙し、さまざまな監査記録種別の中で規定されるべき監査関連情報の最小セットを識別する。
3	FAU_SAA セキュリティ監査分析 (Security audit analysis)	このファミリでは、実際のセキュリティ侵害あるいはその可能性を探す、システムアクティビティや監査データを分析する自動化された手段に対する要件を定義している。 この検出に基づいてとられるアクションは、それが必要とするようにFAU_ARP ファミリを用いて特定することができる。
4	FAU_SAR セキュリティ監査レビュー (Security audit review)	このファミリでは、権限のある利用者が監査データをレビューする際の助けとなる監査ツールのための要件を定義している。
5	FAU_SEL セキュリティ監査事象選択 (Security audit event selection)	このファミリでは、TOE の動作中に監査される事象を選択するための要件を定義している。このファミリは監査対象事象のセットから、事象を含めたり除外したりするための要件を定義している。
6	FAU_STG セキュリティ監査事象格納 (Security audit event storage)	このファミリでは、セキュアな監査証跡を生成あるいは維持するための要件を定義している。

FAUクラスのコンポーネントは、以下の通りである（表 9-4）。

表 9-4：FAU クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FAU_ARP.1	セキュリティアラーム • セキュリティ侵害の可能性が検出された場合、あるアクションを実行する。	FAU_SAA.1 侵害の可能性の分析
2	FAU_GEN.1	監査データ生成 • 監査対象事象の監査記録を生成する。	FPT_STM.1 高信頼タイムスタンプ
3	FAU_GEN.2	利用者識別情報の関連付け • 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る。	FAU_GEN.1 監査データ生成 FIA_UID.1 識別のタイミング
4	FAU_SAA.1	侵害の可能性の分析 • 規則セットに基づいて侵害を検出する。	FAU_GEN.1 監査データ生成

5	FAU_SAA.2	プロファイルに基づく異常検出 • システム利用者の利用履歴パターンに基づいて侵害を検出する。	FAU_UID.1 識別のタイミング
6	FAU_SAA.3	単純攻撃の発見 • 重大な脅威を表す特徴的事象の発生を検出する。	
7	FAU_SAA.4	複合攻撃の発見 • 事象シーケンスに基づき侵害を検出する。	
8	FAU_SAR.1	監査レビュー • を利用者（人間、あるいは、システム）に対して監査記録を提供する。	FAU_GEN.1 監査データ生成
9	FAU_SAR.2	限定監査レビュー • 限られた利用者に対して監査記録を提供する。	FAU_SAR.1 監査レビュー
10	FAU_SAR.3	選択可能監査レビュー • 監査データの検索・分類・並び替えの機能を提供する。	FAU_SAR.1 監査レビュー
11	FAU_SEL.1	選択的監査 • ある属性に基づいて監査事象のセットから監査対象事象を含めたり、除外したりする機能を提供する。	FAU_GEN.1 監査データ生成 FMT_MTD.1 TSF データの管理
12	FAU_STG.1	保護された監査証跡格納 • 格納された監査記録を不正な削除から保護する。	FAU_GEN.1 監査データ生成
13	FAU_STG.2	監査データ可用性の保証 • 格納された監査記録を不正な削除から保護する。	FAU_GEN.1 監査データ生成
14	FAU_STG.3	監査データ損失の恐れ発生時のアクション • 監査証跡が、ある条件の閾値を超えた場合、あるアクションをとる。	FAU_STG.1 保護された監査証跡格納
15	FAU_STG.4	監査データ損失の防止 • 監査証跡が満杯になった場合、あるアクションをとる。	FAU_STG.1 保護された監査証跡格納

9.1.5 FCO（通信）

FCOクラスのファミリは、以下の通りである（表 9-5）。

表 9-5：FCO クラスのファミリ

#	ファミリ	説明
1	FCO_NRO 発信の否認不可 (Non-repudiation of origin)	発信の否認不可は、情報の発信者が情報を送ったことを否定できないようにする。このファミリは、データ交換中に情報を受け取るサブジェクトに対して、TSF が、情報の発信元の証拠が提供されることを保証する方法を提供することを要求する。この証拠は、このサブジェクトまたは他のサブジェクトのいずれかによって検証され得る。
2	FCO_NRR 受信の否認不可 (Non-repudiation of receipt)	受信の否認不可は、情報の受信者が情報の受信を否定できないようにする。このファミリは、データ交換中に情報を送信するザブジェクトに対して、TSF が、情報の受信先の証拠が提供されることを保証する方法を提供することを要求する。この証拠は、このサブジェクトまたは他のサブジェクトによって検証され得る。

FCOクラスのコンポーネントは、以下の通りである(表 9-6)。

表 9-6:FCO クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FCO_NRO.1	発信の選択的証明 • 発信者/受信者/第3者の要求を受け付けて発信元の証拠情報を提供する。	FIA_UID.1 識別のタイミング
2	FCO_NRO.2	発信の強制的証明 • 発信元の証拠情報を常に生成する。	FIA_UID.1 識別のタイミング
3	FCO_NRR.1	受信の選択的証明 • 発信者/受信者/第3者の要求を受け付けて受信元の証拠情報を提供する。	FIA_UID.1 識別のタイミング
4	FCO_NRR.2	受信の強制的証明 • 受信元の証拠情報を常に生成する。	FIA_UID.1 識別のタイミング

9.1.6 FCS(暗号)

FCSクラスのファミリは、以下の通りである(表 9-7)。

表 9-7:FCS クラスのファミリ

#	ファミリ	説明
1	FCS_CKM 暗号鍵管理 (Cryptographic key management)	暗号鍵は、そのライフサイクルを通して管理されねばならない。このファミリは、このライフサイクルをサポートするためのものであり、結果的に以下の行為のための要求を定義する:暗号鍵生成、暗号鍵配付、暗号鍵アクセス、暗号鍵破棄。このファミリは、暗号鍵の管理に対する機能要件があるときは、常に含められるべきである。
2	FCS_COP 暗号操作 (Cryptographic operation)	暗号操作が正しく機能するためには、操作は指定されたアルゴリズムと指定された長さの暗号鍵に従って実行されねばならない。暗号操作を実行する要求があるときは、いつでもこのファミリが含まれねばならない。 典型的な暗号操作は、データの暗号化/復号、デジタル署名の生成と検証、完全性のための暗号的チェックサムの生成と検証、セキュアハッシュ(メッセージダイジェスト)、暗号鍵の暗号化及び/または復号、暗号鍵交換などである。

FCSクラスのコンポーネントは、以下の通りである(表 9-8)。

表 9-8:FCS クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FCS_CKM.1	暗号鍵生成 • 指定された標準に基づく特定のアルゴリズムと鍵長に従って、暗号鍵が生成される。	[FCS_CKM.2 暗号鍵配布、または、FCS_COP.1 暗号操作] FCS_CKM.4 暗号鍵廃棄 FMT_MSA.2 セキュアなセキュリティ属性

2	FCS_CKM.2	暗号鍵配布 • 指定された標準に基づく特定の配付方法に従って暗号鍵が配付される。	[FDP_ITC.1 セキュリティ属性なし利用者データのインポート、または、FCS_CKM.1 暗号鍵生成] FCS_CKM.4 暗号鍵破棄 FMT_MSA.2 セキュアなセキュリティ属性
3	FCS_CKM.3	暗号鍵アクセス • 指定された標準に基づく特定のアクセス方法に従って暗号鍵がアクセス(暗号鍵バックアップ、暗号鍵アーカイブ、暗号鍵エスクロー、暗号鍵回復、など)される。	[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
4	FCS_CKM.4	暗号鍵破棄 • 指定された標準に基づく特定の破棄方法に従って暗号鍵が破棄される。	[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
5	FCS_COP.1	暗号操作 • ある標準に合致する、ある暗号アルゴリズムと暗号鍵長さに従って、ある暗号操作を実行する。	[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

9.1.7 FDP(利用者データ保護)

FDPクラスのファミリは、以下の通りである(表 9-9)。

表 9-9:FDP クラスのファミリ

#	分類	ファミリ	説明
1	利用者データ保護におけるセキュリティ機能方針	FDP_ACC アクセス制御方針 (Access control policy)	このファミリは、アクセス制御 SFP を(名前で)識別し、TSP の識別されたアクセス制御部分を形成する方針の制御範囲を定義する。この制御範囲は、三つのセットによって特徴付けられる:方針の制御下にあるサブジェクト、方針の制御下にあるオブジェクト、及び、方針でカバーされた、制御されたサブジェクトと制御されたオブジェクト間の操作である。

			本基準は、複数の方針が、各々一意の名前を持って存在することを許している。これは、各々の名前を付けたアクセス制御方針に対して、このファミリのコンポーネントを一つずつ繰り返すことで実現できる。アクセス制御 SFP の機能を定義する規則は、FDP_ACF や FDP_SDI といった他のファミリによって定義される。FDP_ACC において識別されたアクセス制御 SFP の名前は、「アクセス制御 SFP」の割付または選択が必要な操作を有する残りの機能コンポーネント全体を通して使われることになる。
2		FDP_IFC 情報フロー制御方針 (Information flow control policy)	このファミリは、情報フロー制御 SFP を(名前で)識別し、TSP の識別された情報フロー制御部分を形成する方針の制御範囲を定義する。この制御範囲は、以下の三つのセットによって特徴付けられる:方針の制御下のサブジェクト、方針の制御下の情報、及び制御された情報を、方針によってカバーされる制御されたサブジェクトへ(あるいはサブジェクトから)流れさせる操作。本基準は、複数の方針が、各々一意の名前を持って存在することを許している。これは、各々の名前を付けた情報フロー制御方針に対し、このファミリからのコンポーネントを一つずつ繰り返すことで実現できる。情報フロー制御 SFP の機能を定義する規則は、FDP_IFF や FDP_SDI といった他のファミリによって定義される。 FDP_IFC において識別された情報フロー制御 SFP の名前は、「情報フロー制御 SFP」の割付または選択が必要な操作を有する残りの機能コンポーネント全体を通して使われることになる。 TSF のメカニズムは、情報フロー制御 SFP に従って情報の流れを制御する。情報のセキュリティ属性を変更する操作は情報フロー制御 SFP に違反するので、通常は許可されない。 しかしながら、明示的に特定される場合、このような操作が情報フロー制御 SFP の例外として許可されることがある。
3	利用者データ保護の形態	FDP_ACF アクセス制御機能 (Access control functions)	このファミリでは、FDP_ACC で名前を付けられたアクセス制御方針を実装することができる特定の機能に対する規則を記述する。FDP_ACC は、方針の制御範囲を特定する。
4		FDP_IFF 情報フロー制御機能 (Information flow control functions)	このファミリは、FDP_IFC で名前付された(また方針の制御範囲も特定しているが、)情報フロー制御 SFP を履行できる特定の機能についての規則を述べる。これは、二種類の要件からなる:一つは共通の情報フロー機能の問題を扱い、他方は不正な情報フロー(すなわち隠れチャネル)を扱う。この区別は、不正な情報フローに関係する問題が、ある意味で、情報フロー制御 SFP の残りの部分と直交しているために生じたものである。この性質によって、不正な情報フローは情報フロー制御 SFP を回避し、その結果として方針を侵害することになる。そのようなわけで、この発生を制限あるいは防止するための特別な機能が必要になる。
5		FDP_ITT TOE 内転送 (Internal TOE transfer)	このファミリは、利用者データが内部チャネルを通って TOE のパーツ間で転送される場合の利用者データの保護に対応する要件を提供する。これは、利用者データが外部チャネルを通って異なる TSF 間を転送されるときの利用者データ保護を提供する FDP_UCT 及び FDP_UIT ファミリ、TSF の制御外へまたは制御外からのデータ転送に対応する FDP_ETC 及び FDP_ITC と対照的と言えよう。
6		FDP_RIP 残存情報保護 (Residual information protection)	このファミリは、削除された情報が再びアクセスできないこと、及び新たに生成されたオブジェクトがアクセスされるべきでない情報を含まないことを保証するための必要性に対応する。このファミリは、論理的

			に削除されたり解放されたが、TOE 中にまだ存在するかもしれない情報の保護を要求する。
7		FDP_ROL ロールバック (Rollback)	ロールバック操作とは、時間間隔など、なんらかの制限によって境界を決められた、最後の操作あるいは一連の操作をもとどおりにし、以前の分かっている状態へ戻すことを意味する。ロールバックは、利用者データの完全性を保持するために一つの操作または一連の操作の影響を元に戻す能力を提供する。
8		FDP_SDI 蓄積データ完全性 (Stored data integrity)	このファミリは、TSC(TSF Scope of Control)内部で蓄積されている間の利用者データ保護に対応する要件を提供する。完全性誤りは、メモリや記憶装置の利用者データに影響を及ぼすかもしれない。 このファミリは、TOE 内転送時の完全性誤りから利用者データを保護する FDP_ITT TOE 内転送とは異なるものである。
9	オフライン格納、インポート及びエクスポート	FDP_DAU データ認証 (Data authentication)	データ認証は、あるエンティティが情報の真正性についての責任を持つ(例えば、デジタル署名によって)ことを許可する。このファミリは、特定のデータユニットの有効性を保証する方法を提供する。このデータユニットは、情報の内容が捏造されたり欺瞞的に改変されたりしていないことを検証するのに使える。FAU クラスと異なり、このファミリは、転送中のデータよりもむしろ「静的」なデータに適用されることを意図している。
10		FDP_ETC TSF 制御外へのエクスポート (Export to outside TSF control)	このファミリは、セキュリティ属性と保護の両方が、明示的に保持されるかあるいはいったんエクスポートされたあとでは無視できるよう、TOE から利用者データをエクスポートする機能を定義する。このファミリは、エクスポートにおける制約及びエクスポートされた利用者データとセキュリティ属性の関連に関係する。
11		FDP_ITC TSF 制御外からのインポート (Import from outside TSF control)	このファミリは、適切なセキュリティ属性を持ちかつ適切に保護された利用者データを TOE に導入するためのメカニズムを規定する。ここでは、インポート時の制限、望ましいセキュリティ属性の決定、及び利用者データに関連付けられたセキュリティ属性の解釈について述べる。
12	TSF 間通信	FDP_UCT TSF 間利用者データ機密転送保護 (Inter-TSF user data confidentiality transfer protection)	このファミリは、利用者データが外部チャネルを用いて別の TOE あるいは別の TOE の利用者間で転送されるとき、その利用者データの機密を保証する要件を定義する。
13		FDP_UIT TSF 間利用者データ完全性転送保護 (Inter-TSF user data integrity transfer protection)	このファミリは、TSF と他の高信頼 IT 製品間を通過する利用者データに対し、完全性を提供し、かつ検出可能な誤りから回復するための要件を定義する。最低限、このファミリは、改変に対する利用者データの完全性を監視する。さらに、このファミリは、検出された完全性誤りを訂正する各種の方法をサポートする。

FDPクラスのコンポーネントは、以下の通りである(表 9-10)。

表 9-10:FDP クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FDP_ACC.1	サブセットアクセス制御 • 操作のサブセットに対する制御方針名前付け機能を提供する。	FDP_ACF.1 セキュリティ属性によるアクセス制御
2	FDP_ACC.2	完全アクセス制御 • 全ての操作に対する制御方針名前付け機能を提供する。	FDP_ACF.1 セキュリティ属性によるアクセス制御

3	FDP_IFC.1	サブセット情報フロー制御 • 情報フローのサブセットに対する制御方針名前付け機能を提供する。	FDP_IFF.1 単純セキュリティ属性
4	FDP_IFC.2	完全アクセス制御 • 全ての情報フローに対する制御方針名前付け機能を提供する。	FDP_IFF.1 単純セキュリティ属性
5	FDP_ACF.1	セキュリティ属性によるアクセス制御 • セキュリティ属性に基づいたアクセス制御機能を提供する。	FDP_ACC.1 サブセットアクセス制御 FMT_MSA.3 静的属性初期化
6	FDP_IFF.1	単純セキュリティ属性 • セキュリティ属性に基づいた情報フロー制御機能を提供する。	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
7	FDP_IFF.2	階層的セキュリティ属性 • 送信元/送信先のセキュリティレベルを踏まえ、セキュリティ属性に基づいた情報フロー制御機能を提供する。	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
8	FDP_IFF.3	制限付き不正情報フロー • 不正情報フローの容量を制限する情報フロー制御機能を提供する。	AVA_CCA.1 隠れチャネル分析 FDP_IFC.1 サブセット情報フロー制御
9	FDP_IFF.4	不正情報フローの部分的排除 • 不正情報フローの容量を制限し、かつ、ある特定の情報フローを防止する情報フロー制御機能を提供する。	AVA_CCA.1 隠れチャネル分析 FDP_IFC.1 サブセット情報フロー制御
10	FDP_IFF.5	不正情報フローなし • 情報フロー制御機能を回避する不正情報フローが存在しないことを保証する機能を提供する。	AVA_CCA.3 徹底的隠れチャネル分析 FDP_IFC.1 サブセット情報フロー制御
11	FDP_IFF.6	不正情報フロー監視 • 不正情報フローの容量が閾値を超えた場合に検出する。	AVA_CCA.1 隠れチャネル分析 FDP_IFC.1 サブセット情報フロー制御
12	FDP_ITT.1	基本内部転送保護 • 利用者データが、TOE のパーツ間で転送されるときに保護する機能を提供する。	[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]
13	FDP_ITT.2	属性による転送分離 • 利用者データ、TOE のパーツ間で転送されるときに保護する機能を提供し、さらに、セキュリティ属性に基づいて、データを分離して転送する。	[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]
14	FDP_ITT.3	完全性監視 • 転送中に、利用者データの完全性誤りを検出し、アクションを実行する。	[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] FDP_ITT.1 基本内部転送保護
15	FDP_ITT.4	属性に基づく完全性監視 • セキュリティ属性に基づいて、転送中における利用者データの	[FDP_ACC.1 サブセットアクセス制御、または、

		完全性誤りを検出し、アクションを実行する。	FDP_IFC.1 サブセット情報フロー制御] FDP_ITT.2 属性による転送分離
16	FDP_RIP.1	サブセット残存情報保護 • 選択されたあるオブジェクトにおいて、削除された後は、再度読み出しなどができないようにする機能を提供する。	
17	FDP_RIP.2	全残存情報保護 • 全てのオブジェクトにおいて、削除された後は、再度読み出しなどができないようにする機能を提供する。	
18	FDP_ROL.1	基本ロールバック • あるオブジェクトに対する選択された操作をロールバックする。	[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]
19	FDP_ROL.2	高度ロールバック • あるオブジェクトに対する全ての操作をロールバックする。	[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]
20	FDP_SDI.1	蓄積データ完全性監視 • 蓄積された利用者データの完全性誤りを検出する。	
21	FDP_SDI.2	蓄積データ完全性監視及びアクション • 蓄積された利用者データの完全性誤りを検出し、アクションを実行する。	
22	FDP_DAU.1	基本データ認証 • オブジェクトの真正性を保証する。	
23	FDP_DAU.2	保証人識別情報付きデータ認証 • オブジェクトの真正性を保証し、さらに、保証人の識別情報を提供する。	FIA_UID.1 識別のタイミング
24	FDP_ETC.1	セキュリティ属性なし利用者データのエクスポート • 利用者データのセキュリティ属性を含めないで利用者データをエクスポートする。	[FDP_ACC.1 サブセットアクセス制御、あるいは、FDP_IFC.1 サブセット情報フロー制御]
25	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 • 利用者データのセキュリティ属性を含めて利用者データをエクスポートする。	[FDP_ACC.1 サブセットアクセス制御、あるいは、FDP_IFC.1 サブセット情報フロー制御]
26	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 • 利用者データのセキュリティ属性を含めないで利用者データをインポートする。	[FDP_ACC.1 サブセットアクセス制御、あるいは、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
27	FDP_ITC.2	セキュリティ属性付き利用者データのインポート • 利用者データのセキュリティ属性を含めて利用者データをインポートする。	[FDP_ACC.1 サブセットアクセス制御、あるいは、FDP_IFC.1 サブセット情報フロー制御] [FTP_ITC.1 TSF 間高信頼チャネル、または、FTP_TRP.1 高信頼パ

			ス] FPT_TDC.1 TSF 間基本 TSF データ一貫性
28	FDP_UCT.1	基本データ交換機密 • 別の TOE あるいは、別の TOE の利用者間で、利用者データが転送されるとき、その利用者データの機密性を保証する。	[FDP_ACC.1 サブセットアクセス制御、あるいは、FDP_IFC.1 サブセット情報フロー制御] [FTP_ITC.1 TSF 間高信頼チャネル、または、FTP_TRP.1 高信頼パス]
29	FDP_UIT.1	データ交換完全性 • 送信される利用者データの、改変、削除、挿入、及びリプレイ誤りを検出する。	[FDP_ACC.1 サブセットアクセス制御、あるいは、FDP_IFC.1 サブセット情報フロー制御] [FTP_ITC.1 TSF 間高信頼チャネル、または、FTP_TRP.1 高信頼パス]
30	FDP_UIT.2	発信側データ交換回復 • 発信側の高信頼 IT 製品の助けを借りて、誤りから回復する。	[FDP_ACC.1 サブセットアクセス制御、あるいは、FDP_IFC.1 サブセット情報フロー制御] FDP_UIT.1 データ交換完全性 FTP_ITC.1 TSF 間高信頼チャネル
31	FDP_UIT.3	着信側データ交換回復 • 発信側の高信頼 IT 製品の助けを借りずに、誤りから回復する。	[FDP_ACC.1 サブセットアクセス制御、あるいは、FDP_IFC.1 サブセット情報フロー制御] FDP_UIT.1 データ交換完全性 FTP_ITC.1 TSF 間高信頼チャネル

9.1.8 FIA（識別と認証）

FIAクラスのファミリは以下の通りである（表 9-11）。

表 9-11：FIA クラスのファミリ

#	ファミリ	説明
1	FIA_AFL 認証失敗 (Authentication failures)	このファミリは、不成功の認証試行数についての値と、認証試行の失敗における TSF アクションの定義に対する要件を含む。パラメタは、失敗した認証の数と時間の閾値を含むが、それだけに限定されない。
2	FIA_ATD 利用者属性定義 (User attribute definition)	すべての許可利用者は、利用者識別情報以外に、TSP を実施するために使われるセキュリティ属性のセットを持つかもしれない。このファミ

		リはセキュリティ属性を利用者に関連付けるための要件を定義するものであり、TSP を支えるものとして必要とされる。
3	FIA_SOS 秘密についての仕様 (Specification of secrets)	このファミリは、定義された尺度を満たすため、提供された秘密と生成された秘密について定義される品質尺度を実施するメカニズムに対する要件を定義する。
4	FIA_UAU 利用者認証 (User authentication)	このファミリは、TSF がサポートされる利用者認証メカニズムの種別を定義する。またこのファミリは、利用者認証メカニズムが基づくべき要求された属性も定義する。
5	FIA_UID 利用者識別 (User identification)	このファミリは、利用者が自分自身を識別することが要求されねばならない条件を定義するものであり、この識別は、TSF が調停しかつ利用者認証を必要とする他のすべてのアクションの前に行われる。
6	FIA_USB 利用者・サブジェクト結合 (User-subject binding)	認証された利用者は、TOE を使用するため、通常はサブジェクトを動作させる。利用者のセキュリティ属性は(全面的または部分的に)このサブジェクトに関連付けられる。このファミリは、利用者のセキュリティ属性と利用者を代行して動作するサブジェクトとの関連付けを生成し維持するための要件を定義する。

FIAクラスのコンポーネントは、以下の通りである(表 9-12)。

表 9-12:FIA クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FIA_AFL.1	認証失敗時の取り扱い • 認証失敗の検出、及び、検出後のアクションを実行する。	FIA_UAU.1 認証のタイミング
2	FIA_ATD.1	利用者属性定義 • 利用者に対してセキュリティ属性を定義・維持する。	
3	FIA_SOS.1	秘密の検証 • 秘密がある品質尺度に合致することを検証する。	
4	FIA_SOS.2	TSF 秘密生成 • ある品質尺度に合致する秘密を生成する。	
5	FIA_UAU.1	認証のタイミング • 利用者認証前に、利用者があるアクションを実行することを許可する。	FIA_UID.1 識別のタイミング
6	FIA_UAU.2	アクション前の利用者認証 • アクションを許可する前に利用者認証を行う。	FIA_UID.1 識別のタイミング
7	FIA_UAU.3	偽造されない認証 • 偽造やコピーされたことのある認証データの使用を検出・防止する。	
8	FIA_UAU.4	単一使用認証メカニズム • 単一使用の認証メカニズムを提供する(例:ワンタイム・パスワード)。	
9	FIA_UAU.5	複数の認証メカニズム • 複数の認証メカニズムを提供する。	
10	FIA_UAU.6	再認証 • ある条件のもとで利用者を再認証する。	
11	FIA_UAU.7	保護された認証フィードバック • 認証処理時にあるフィードバックのみ利用者に提供する。	FIA_UAU.1 認証のタイミング
12	FIA_UID.1	識別のタイミング • 利用者識別前に、利用者があるアクションを実行することを許可	

		する。	
13	FIA_UID.2	アクション前の利用者識別 ● アクションを許可する前に利用者識別を行う。	
14	FIA_USB.1	利用者・サブジェクト結合 ● 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る。	FIA_ATD.1 利用者属性定義

9.1.9 FMT（セキュリティ管理）

FMTクラスのファミリは、以下の通りである（表 9-13）。

表 9-13：FMT クラスのファミリ

#	ファミリ	説明
1	FMT_MOF TSF における機能の管理 (Management of functions in TSF)	このファミリは、許可利用者が TSF における機能の管理を統括できるようにする。TSF における機能の例として、監査機能、多重認証機能がある。
2	FMT_MSA セキュリティ属性の管理 (Management of security attributes)	このファミリは、許可利用者がセキュリティ属性の管理を統括することを許可する。この管理には、セキュリティ属性を見たり改変したりする実施権限を含められる。
3	FMT_MTD TSF データの管理 (Management of TSF data)	このファミリは、許可利用者(役割)が TSF データの管理を統括することを許可する。TSF データの例として、監査情報、クロック、システム構成、その他の TSF 設定パラメタがある。
4	FMT_REV 取消し (Revocation)	このファミリは、TOE 内のいろいろなエンティティのセキュリティ属性の取消しに対応する。
5	FMT_SMF 管理機能の特定 (Specification of Management Functions)	このファミリは、TOE によって管理機能が提供されるための仕様を記す。
6	FMT_SAE セキュリティ属性有効期限 (Security attribute expiration)	このファミリは、セキュリティ属性の有効性に対して時間制限を実施する能力に対応する。
7	FMT_SMR セキュリティ管理役割 (Security management roles)	このファミリは、利用者への異なる役割の割付けの管理を意図している。セキュリティ管理に関するこれらの役割の実施権限は、このクラスの他のファミリで記述される。

FMTクラスのコンポーネントは、以下の通りである（表 9-14）。

表 9-14：FMT クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FMT_MOF.1	セキュリティ機能の振る舞いの管理 ● 許可された利用者だけが、セキュリティ機能の振る舞いを管理する。	FMT_SMF.1 管理機能の特定 FMT_SMR.1 セキュリティ役割
2	FMT_MSA.1	セキュリティ属性の管理 ● 許可された利用者だけが、セキュリティ属性を管理する。	[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
3	FMT_MSA.2	セキュアなセキュリティ属性 • 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する。	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
4	FMT_MSA.3	静的属性初期化 • セキュリティ属性のデフォルト値を設定する。	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
5	FMT_MTD.1	TSF データの管理 • 許可された利用者だけが、TSF データを管理する。	FMT_SMF.1 管理機能の特定 FMT_SMR.1 セキュリティ役割
6	FMT_MTD.2	TSF データにおける限界値の管理 • 許可された利用者だけが、TSF データにおける限界値を管理する。	FMT_MTD.1 TSF データの管理 FMT_SMR.1 セキュリティ役割
7	FMT_MTD.3	セキュアな TSF データ • セキュアな値だけが TSF データとして受け入れられる。	ADV_SPM.1 非形式的 TOE セキュリティ方針モデル FMT_MTD.1 TSF データの管理
8	FMT_REV.1	取消し • 許可された利用者だけが、セキュリティ属性を取り消す。	FMT_SMR.1 セキュリティ役割
9	FMT_SAE.1	時限付き許可 • 許可された利用者だけが、セキュリティ属性に対する有効期限を設定する。	FMT_SMR.1 セキュリティ役割 FPT_STM.1 高信頼タイムスタンプ
10	FMT_SMF.1	管理機能の特定 • セキュリティ管理機能を定義する。	
11	FMT_SMR.1	セキュリティ役割 • セキュリティ役割を定義し、特定する。	FIA_UID.1 識別のタイミング
12	FMT_SMR.2	セキュリティ役割における制限 • セキュリティ役割の定義、特定、さらに、役割間の関係を制御する規則がある。	FIA_UID.1 識別のタイミング
13	FMT_SMR.3	負わせる役割 • TSF は、ある役割を負わせるために、明示的な要求をする。	FMT_SMR.1 セキュリティ役割

9.1.10 FPR（プライバシー）

FPRクラスのファミリは、以下の通りである（表 9-15）。

表 9-15：FPR クラスのファミリ

#	ファミリ	説明
1	FPR_ANO 匿名性 (Anonymity)	このファミリは、利用者が利用者の識別情報を暴露することなく、資源やサービスを使用できるようにする。匿名性に対する要件は、利用者識別情報の保護を提供することである。 匿名性は、サブジェクト識別情報の保護を意図したものではない。
2	FPR_PSE 偽名性 (Pseudonymity)	このファミリは、利用者がその利用者識別情報を暴露することなく資源やサービスを使用できるが、その使用に対しては責任を取り得ることを保証する。
3	FPR_UNL リンク不能性 (Unlinkability)	このファミリは、一人の利用者が資源やサービスを複数使用できるが、他人はこれらの使用を一緒にリンクすることができないことを保証する。
4	FPR_UNO 管理不能性 (Unobservability)	このファミリは、利用者が資源やサービスを使用でき、その際に他の利用者、特に第三者は、その資源やサービスが使用されていることを観察できないことを保証する。

FPRクラスのコンポーネントは、以下の通りである（表 9-16）。

表 9-16：FPR クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FPR_ANO.1	匿名性 • あるサブジェクトまたは操作に結び付けられた利用者の識別情報を、他の利用者やサブジェクトが判別できないことを保証する。	
2	FPR_ANO.2	情報を請求しない匿名性 • TSF が利用者識別情報を要求しないことを保証することにより、FPR_ANO.1 を強化する。	
3	FPR_PSE.1	偽名性 • あるサブジェクトあるいは操作に結び付けられたある利用者の識別情報について、利用者及び/またはサブジェクトのセットはそれを判別することができないが、この利用者はそのアクションに対して責任を取り得ることを要求する。	
4	FPR_PSE.2	可逆偽名性 • 提供された別名に基づき、TSF が元の利用者識別情報を判別する能力を備えることを要求する。	
5	FPR_PSE.3	別名偽名性 • 利用者識別情報の別名に対するある構成規則に TSF が従うことを要求する。	
6	FPR_UNL.1	リンク不能性 • そのシステムにおいて、同一の利用者がある特定の操作(複数形)の原因になっているかどうかを、利用者及び/またはサブジェクトが判別できないことを要求する。	
7	FPR_UNO.1	観察不能性 • 利用者及び/またはサブジェクトが、ある操作が実行されていることを判別できないことを要求する。	

8	FPR_UNO.2	観察不能性に影響する情報の配置 • TOE 内の情報に関係するプライバシーの集中化を避ける特定のメカニズムを TSF が提供することを要求する。	
9	FPR_UNO.3	情報を請求しない観察不能性 • 観察不能性の弱体化に利用されるかもしれない情報に関係するプライバシーを TSF が取得しようとしないことを要求する。	
10	FPR_UNO.4	許可利用者観察可能性 • 資源及び/またはサービスの利用を観察する権限を、一人またはそれ以上の許可利用者に TSF が提供することを要求する。	

9.1.11 FPT（TSF の保護）

FPTクラスのファミリは、以下の通りである（表 9-17）。

表 9-17：FPT クラスのファミリ

#	ファミリ	説明
1	FPT_AMT 下層の抽象マシンテスト (Underlying abstract machine test)	このファミリは、TSF が依存する下層抽象マシンについて作られたセキュリティ想定を実証するテストを TSF が実行するための要件を定義する。この「抽象」マシンは、ハードウェア/ファームウェアプラットフォームでも、仮想マシンとして動作する、内容がわかりかつ査定された、何らかのハードウェア/ソフトウェアの組み合わせでもよい。
2	FPT_FLS フェールセキュア (Fail secure)	このファミリの要件は、TSF 中の識別された障害のカテゴリの事象において、TOE がその TSP を侵害しないことを保証する。
3	FPT_ITA エクスポートされた TSF データの可用性 (Availability of exported TSF data)	このファミリは TSF とリモート高信頼 IT 製品間を流れる TSF データの可用性の損失を防ぐ規則を定義する。このデータは、例えば、パスワード、キー、監査データ、あるいは TSF 実行コードなどの TSF に重要なデータである。
4	FPT_ITC エクスポートされた TSF データの機密性 (Confidentiality of exported TSF data)	このファミリは、TSF とリモート高信頼 IT 製品間の送信中の、不正な暴露からの TSF データの保護に対する規則を定義する。このデータは、例えば、パスワード、キー、監査データ、あるいは TSF 実行コードなどの TSF に重要なデータである。
5	FPT_ITI エクスポートされた TSF データの完全性 (Integrity of exported TSF data)	このファミリは、TSF とリモート高信頼 IT 製品間で送信中の TSF データの、不正な改変からの保護に対する規則を定義する。このデータは、例えば、パスワード、キー、監査データ、TSF 実行コードなどの TSF に重要なデータである。
6	FPT_ITT TOE 内 TSF データ転送 (Internal TOE TSF data transfer)	このファミリは、TSF データが内部チャネルを通して一つの TOE の分離したパーツ間を転送されるときの TSF データの保護に対応する要件を提供する。
7	FPT_PHP TSF 物理的保護 (physical protection)	TSF 物理的保護コンポーネントは、TSF に対する不正な物理的アクセスの制限、及び TSF の不正な物理的改変あるいは置き換えに対する阻止と抵抗に言及する。 このファミリのコンポーネントの要件は、物理的な改ざんと干渉から TSF が保護されることを保証する。これらのコンポーネントの要件を満たすことは、結果として、TSF がパッケージ化され、かつ、物理的改ざんを検出可能な、あるいは物理的改ざんへの抵抗が強制されるような形で使われることになる。これらのコンポーネントがなければ、物理的損害を防ぎ得ない環境において、TSF の保護機能はその有効性を失

		う。このファミリはまた、TSF がどのようにして物理的な改ざんの試みに対応しなければならないかに関する要件を提供する。
8	FPT_RCV 高信頼回復 (Trusted recovery)	このファミリの要件は、保護の弱体化なくTOEが立ち上がることを決定できること、かつ操作の中断後、保護の弱体化なく回復できることを保証する。TSF の立ち上がりの状態がそれに続く状態の保護を決定するので、このファミリは重要である。
9	FPT_RPL リプレイ検出 (Replay detection)	このファミリは、さまざまな種別のエンティティ(例えば、メッセージ、サービス要求、サービス応答)に対するリプレイの検出と、それに続く訂正のためのアクションに対応する。リプレイが検出できるような場合は、このファミリは効果的にリプレイを防止する。
10	FPT_RVM リファレンス調停 (Reference mediation)	このファミリの要件は、伝統的なリファレンスモニタの「いつでも呼び出せる」側面に対応する。このファミリの目標は、与えられた SFP に関して、方針の実施を要求するすべてのアクションが、SFP に対する TSF によって有効性を確認されることを保証することである。もし、SFP を実施する TSF の部分も FPT_SEP(ドメイン分離)と ADV_INT(TSF 内部)の適切なコンポーネントの要件に合致するならば、TSF のその部分は、その SFP に対する「リファレンスモニタ」を提供する。
11	FPT_SEP ドメイン分離 (Domain separation)	このファミリのコンポーネントは、少なくとも一つのセキュリティドメインが TSF 自身の実行のために利用でき、かつ信頼できないサブジェクトによる外部の干渉と改ざん(例えば、TSFコードやデータ構造の改変による)から TSF が保護されることを保証する。このファミリの要件を満たすことで TSF は自己保護型になり、これは、信頼できないサブジェクトは TSF を改変したり損害を与えたりできないことを意味する。
12	FPT_SSP 状態同期プロトコル (State synchrony protocol)	分散システムは、システムのパーツ間の状態において潜在的な差異が生じること、通信における遅延があることによって、一体化したシステムよりも複雑さを増すかもしれない。 ほとんどの場合、分散した機能間の状態の同期は、単純なアクションでなく、交換プロトコルを必要とする。これらのプロトコルの分散環境に悪意が存在すれば、さらに複雑な防御的プロトコルが要求される。FPT_SSP は、この信頼できるプロトコルを使用する TSF のある重要なセキュリティ機能についての要件を制定する。FPT_SSP は、TOE(例えば、ホスト)の二つの分散したパーツが、あるセキュリティ関連のアクションのあとで、同期した状態を持つことを保証する。
13	FPT_STM タイムスタンプ (Time stamps)	このファミリは、TOE での高信頼タイムスタンプ機能に対する要件に対応する。
14	FPT_TDC TSF 間 TSF データ一貫性 (Inter-TSF data consistency)	分散あるいは複合システム環境において、TOE は TSF データ(例えば、データに関連した SFP 属性、監査情報、識別情報)を他の高信頼 IT 製品と交換するする必要があるかもしれない。このファミリは、TOE の TSF と他の高信頼 IT 製品間で、これらの属性の共有及び一貫した解釈のための要件を定義する。
15	FPT_TRC TOE 内 TSF データ複製一貫性 (Internal TOE TSF data replication consistency)	このファミリの要件は、TSF データが TOE 内で複製される場合、TSF データの一貫性を保証することを求めている。もし、TOE のパート間の内部チャネルが運用不能になると、そのようなデータは一貫性を失うかもしれない。もし、TOE の内部構造がネットワーク化されており、TOE ネットワーク接続のパーツが切断されると、パーツが非活性状態になるときにこのようなことが生じるかもしれない。
16	FPT_TST TSF 自己テスト (TSF self test)	このファミリは、ある期待される正しい運用に関する、TSF の自己テストのための要件を定義する。例として、実施機能に対するインタフェースや、TOE の重要なパーツにおける抜き取りの計算的操作がある。こ

		れらのテストは、立ち上げ時、定期的、許可利用者の要求によって、あるいはその他の条件が合致したときに実行される。自己テストの結果として TOE によって取られるアクションは、別のファミリで定義される。

FPTクラスのコンポーネントは、以下の通りである(表 9-18)。

表 9-18:FPT クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FPT_ATM.1	抽象マシンテスト • TSF の下層にある抽象マシンのテストを起動する。	
2	FPT_FLS.1	セキュアな状態を保持する障害 • 障害が生じたときにセキュアな状態を保持することを保証する。	ADV_SPM.1 非形式的 TOE セキュリティ方針モデル
3	FPT_ITA.1	定義された可用性尺度内の TSF 間可用性 • TSF とリモート高信頼IT 製品間を流れるTSF データの可用性を保証する。	
4	FPT_ITC.1	送信中の TSF 間機密性 • TSF とリモート高信頼IT 製品間を流れるTSF データの機密性を保証する。	
5	FPT_ITI.1	TSF 間改変の検出 • TSF とリモート高信頼 IT 製品間を流れる TSF データの改変を検出する。	
6	FPT_ITI.2	TSF 間改変の検出と訂正 • TSF とリモート高信頼 IT 製品間を流れる TSF データの改変を検出し、訂正する。	
7	FPT_ITT.1	基本 TSF 内データ転送保護 • TOE の分離したパーツ間で送信されるときにTSF データが保護される。	
8	FPT_ITT.2	TSF データ転送分離 • TSF が、利用者データを送信中の TSF データから分離する。	
9	FPT_ITT.3	TSF データ完全性監視 • TOE の分離したパーツ間で送信される TSF データの完全性誤りを検出し、アクションを実行する。	FPT_ITT.1 基本 TFS 内データ転送保護
10	FPT_PHP.1	物理的攻撃の受動的検出 • TSF の装置や TSF のエレメントに対する物理的干渉を検出できるようにする。	
11	FPT_PHP.2	物理的攻撃の通知 • TSF の装置や TSF のエレメントに対する物理的干渉を検出し、自動的に通知する。	FMT_MOF.1 セキュリティ機能のふるまいの管理
12	FPT_PHP.3	物理的攻撃への抵抗 • TSF の装置や TSF のエレメントに対する物理的干渉を防止・抵抗する。	
13	FPT_RCV.1	手動回復 • 障害/サービス中断後、セキュアな状態に戻す能力が提供される面手ナスモードに移る。	AGD_ADM.1 管理者ガイダンス ADV_SPM.1 非形式的 TOE セキュリティ方針モデル

14	FPT_RCV.2	自動回復 • 障害/サービス中断後、セキュアな状態に戻す能力が提供される面手ナスモードに移り、自動的に回復する。	AGD_ADM.1 管理者ガイダンス ADV_SPM.1 非形式的 TOE セキュリティ方針モデル
15	FPT_RCV.3	過度の損失のない自動回復 • 障害/サービス中断後、セキュアな状態に戻す能力が提供される面手ナスモードに移り、過度な損失がない範囲で自動的に回復する。	FPT_TST.1 TSF テスト AGD_ADM.1 管理者ガイダンス ADV_SPM.1 非形式的 TOE セキュリティ方針モデル
16	FPT_RCV.4	機能回復 • TSF データのセキュアな状態への成功裏の完了、あるいは、以前の状態へのロールバックを提供。	ADV_SPM.1 非形式的 TOE セキュリティ方針モデル
17	FPT_RPL.1	リプレイ検出 • さまざまな種別のエンティティ(例えば、メッセージ、サービス要求、サービス応答)に対するリプレイの検出とその後のアクションを実施する。	
18	FPT_RVM.1	TSP の非バイパス性 • 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する。	
19	FPT_SEP.1	TSF ドメイン分離 • TSF ドメイン分離は、TSF のための区分された保護ドメインを提供し、かつ TSC 内のサブジェクト間の分離を提供する。	
20	FPT_SEP.2	SFP ドメイン分離 • SFP の方針に対してリファレンスモニタとして動作する、識別された SFP のセットのための区分されたドメイン(複数形)と、TSF の残りの部分に対する一つのドメインに、TSF がさらに小分割。	
21	FPT_SEP.3	完全リファレンスモニタ • TSP 実施のための区分されたドメイン(複数形)と、TSF の残りの部分に対する一つのドメインを要求する。	
22	FPT_SSP.1	単純信頼肯定応答 • TSF は、データ受信時に改変されていないデータを受け取ったことを通知する。	FPT_ITT.1 基本 TSF 内データ転送保護
23	FPT_SSP.2	相互信頼肯定応答 • TSF は、データ受信時に改変されていないデータを受け取ったことを通知する。さらに、、TSF の関連するパーツが、肯定応答を使って、異なるパーツ間で送信されたデータの正確な状態を知ることを保証する。	FPT_ITT.1 基本 TSF 内データ転送保護
24	FPT_STM.1	高信頼タイムスタンプ • 高信頼タイムスタンプを提供する。	
25	FPT_TDC.1	TSF 間基本 TSF データ一貫性 • SF が TSF 間の属性の一貫性を保証する能力を提供する。データ解釈の一貫性を保証する。	
26	FPT_TRC.1	TSF 内一貫性 • 複数の場所で複製される TSF データの一貫性を保証する。	FPT_ITT.1 基本 TSF 内データ転送保護
27	FPT_TST.1	TSF テスト	FPT_ATM.1 抽象

		• TSF の正しい運用をテストする能力を提供する。	マシンテスト

9.1.12 FRU（資源利用）

FRUクラスのファミリは、以下の通りである（表 9-19）。

表 9-19：FRU クラスのファミリ

#	ファミリ	説明
1	FRU_FLT 耐障害性 (Fault tolerance)	このファミリの要件は、障害発生時においても、TOE が正しい運用を維持することを保証することである。
2	FRU_PRS サービス優先度 (Priority of service)	このファミリの要件は、低優先度アクティビティによって引き起こされる過度の干渉や遅延を受けることなく、TSC 内の高優先度アクティビティが常にその動作を完遂できるよう、利用者とサブジェクトによる TSC 内の資源利用を TSF が管理することを認める。
3	FRU_RSA 資源割当て (Resource allocation)	このファミリの要件は、不正な資源専有のためにサービス拒否が生じないよう、利用者とサブジェクトによる資源利用を TSF が管理することを認める。

FRUクラスのコンポーネントは、以下の通りである（表 9-20）。

表 9-20：FRU クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FRU_FLT.1	機能削減された耐障害性 • 識別した障害発生時に、TOE が、識別した能力の正しい運用を続けることを要求する。	FPT_FLS.1 セキュアな状態を保持する障害
2	FRU_FLT.2	制限付き耐障害性 • 識別した障害発生時に、TOE がすべての能力の正しい運用を続けることを要求する。	FPT_FLS.1 セキュアな状態を保持する障害
3	FRU_PRS.1	制限付きサービス優先度 • サブジェクトによる TSC 内の資源のサブセットの利用に対して優先度を提供する。	
4	FRU_PRS.2	完全サービス優先度 • サブジェクトによる TSC 内の全資源の利用に対して優先度を提供する。	
5	FRU_RSA.1	最大割当て • 利用者及びサブジェクトが制御下にある資源を専有しないことを保証する、割当てメカニズムのための要件を提供する。	
6	FRU_RSA.2	最小及び最大割当て • 利用者及びサブジェクトが、少なくとも最小限の特定された資源を常に持ち、かつ制御下にある資源を専有できないことを保証する、割当てメカニズムのための要件を提供する。	

9.1.13 FTA（TOE アクセス）

FTAクラスのファミリは、以下の通りである（表 9-21）。

表 9-21:FTA クラスのファミリ

#	ファミリ	説明
1	FTA_LSA 選択可能属性の範囲制限 (Limitation on scope of selectable attributes)	このファミリは、利用者がセションのため選択できるセションセキュリティ属性の範囲を制限する要件を定義する。
2	FTA_MCS 複数同時セッションの制限 (Limitation on multiple concurrent sessions)	このファミリは、同一利用者に属する同時セションの数に対する制限を設ける要件を定義する。
3	FTA_SSL セッションロック (Session locking)	このファミリは、TSF 起動及び利用者起動の、対話セションのロック及びロック解除のための能力を TSF が提供するための要件を定義する。
4	FTA_TAB TOE アクセスバナー (TOE access banners)	このファミリは、利用者に対し、TOE の適切な利用に関する、設定可能な勧告的警告メッセージを表示する要件を定義する。
5	FTA_TAH TOE アクセス履歴 (TOE access history)	このファミリは、セション確立の成功時に、利用者のアカウントにアクセスした成功及び不成功の試みの履歴を、TSF が利用者に対して表示するための要件を定義する。
6	FTA_TSE TOE セッション確立 (TOE session establishment)	このファミリは、TOE とセションを確立するための利用者許可を拒否する要件を定義する。

FTAクラスのコンポーネントは、以下の通りである(表 9-22)。

表 9-22:FTA クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FTA_LSA.1	選択可能属性の範囲制限 • セション確立中のセションセキュリティ属性の範囲を TOE が制限するための要件を提供する。	
2	FTA_MCS.1	複数同時セッションの基本制限 • TSF のすべての利用者に適用する制限を提供する。	FIA_UID.1 識別のタイミング
3	FTA_MCS.2	複数同時セッションの利用者属性ごと制限 • 関連したセキュリティ属性に基づく同時セション数の制限を特定する能力を要求することによって、FTA_MCS.1 を強化する。	FIA_UID.1 識別のタイミング
4	FTA_SSL.1	TSF 起動セッションロック • 利用者の動作がない特定した時間後の、システム起動の対話セションロックを含む。	FIA_UAU.1 認証のタイミング
5	FTA_SSL.2	利用者起動ロック • 利用者が、利用者自身の対話セションのロックとロック解除するための能力を提供する。	FIA_UAU.1 認証のタイミング
6	FTA_SSL.3	TSF 起動による終了 • TSF が、利用者の動作がない特定した時間後にセションを終了するための要件を提供する。	
7	FTA_TAB.1	デフォルト TOE アクセスバナー • TOE アクセスバナーに対する要件を提供する。このバナーは、セションの確立のための対話に先立って表示される。	
8	FTA_TAH.1	TOE アクセス履歴 • セションを確立するための以前の試みに関連する情報を TOE が表示するための要件を提供する。	
9	FTA_TSE.1	TOE セッション確立 • 属性に基づき、利用者が TOE にアクセスするのを拒否する要	

		件を提供する。	

9.1.14 FTP(高信頼パス/チャネル)

FTPクラスのファミリは、以下の通りである(表 9-23)。

表 9-23:FTP クラスのファミリ

#	ファミリ	説明
1	FTP_ITC TSF 間高信頼チャネル (Inter-TSF trusted channel)	このファミリは、セキュリティ上の重要な操作のために、TSF と他の高信頼 IT 製品間に高信頼チャネルを生成するための要件を定義する。このファミリは、TOE と他の高信頼 IT 製品間で利用者あるいは TSF データのセキュアな通信に対する要求があるときは、常に含まれるべきである。
2	FTP_TRP 高信頼パス (Trusted path)	このファミリは、利用者と TSF 間に高信頼通信を確立し維持するための要件を定義する。高信頼パスは、どのようなセキュリティ関連の対話に対しても要求されるかも知れない。高信頼パス交換は、TSF との対話の間に利用者によって開始されることもあり、高信頼パスを介して TSF が利用者との通信を確立することもある。

FTPクラスのコンポーネントは、以下の通りである(表 9-24)。

表 9-24:FTP クラスのファミリに含まれるコンポーネント

#	コンポーネント	説明	依存性
1	FTP_ITC.1	TSF 間高信頼チャネル • TSF が、それ自身と他の高信頼IT製品間に高信頼通信チャネルを提供することを要求する。	
2	FTP_TRP.1	高信頼パス • PP/ST 作成者により定義された事象のセットに対して、TSF と利用者間に高信頼パスが提供されることを要求する。	

9.2 セキュリティ機能要件の例

9.2.1 ISO/IEC TR 15446 の汎用システムのセキュリティ機能要件

ISO/IEC 15408-2 において定義された共通的な汎用セキュリティ機能は、以下のように分類される。

- 識別と認証(Identification and authentication)
- アクセス制御(Access control)
- 監査(Audit)
- 完全性(Integrity)
- 可用性(Availability)
- プライバシー(Privacy)
- データ交換(Data Exchage)

9.2.1.1 識別と認証

識別と認証に分類されるセキュリティ機能要件は、以下の通りである(表 9-25)。

表 9-25:識別と認証に分類されるセキュリティ機能要件

#	セキュリティ要件		ISO/IEC 15408 Part2 における機能コンポーネント
1	ログオン制御/管理	ユーザの識別	FIA_UID.1-2
2		ユーザの認証	FIA_UAU.1-2
3		ログイン失敗数の制限(ログイン失敗数がある閾値を超えるとロックアウトする)	FIA_AFL.1
4		ログインのための信頼されたパス	FTP_TRP.1-2
5		TOE アクセス時間の制限	FTA_TSE.1
6	パスワード選択	ユーザ生成パスワードの選択に関する制御/管理	FIA_SOS.1
7		TOE によるパスワード自動生成	FIA_SOS.2
8		パスワード有効期限の実施	FMT_SAE.1
9	認証データ保護	パスワード入力中にエコー表示しない	FIA_UAU.7
10		不正な修正や観察からの保護	FMT_MTD.1
11		リプレイ攻撃からの保護	FPT_RPL.1
12	リプレイ/再利用	偽造や複製に対する保護	FIA_UAU.3
13		再利用からの保護(例:ワンタイムパスワード)	FIA_UAU.4
14		パスワード変更のための信頼されたパス	FTP_TRP.1
15	セッションの一時停止	ユーザ不使用に基づくセッションの一時停止	FTA_SSL.1
16		ユーザ要求に基づくセッションの一時停止	FTA_SSL.2
17		ユーザ不使用に基づく停止	FTA_SSL.3
18	ユーザアカウントとプロファイル	ユーザアカウントの生成、削除、有効化、無効化に関する制御/管理	FMT_MTD.1
19		ユーザプロファイルに含まれるユーザセキュリティ属性の定義	FIA_ATD.1
20		ユーザプロファイルの修正に関する制御/管理(ユーザセキュリティ属性の修正)	FMT_MTD.1

9.2.1.2 アクセス制御

アクセス制御に分類されるセキュリティ機能要件は、以下の通りである(表 9-26)。

表 9-26:アクセス制御に分類されるセキュリティ機能要件

#	セキュリティ要件		ISO/IEC 15408 Part2 における機能コンポーネント
1	随意アクセス制御/管理(DAC)	ポリシーの範囲(サブジェクト、オブジェクト、ポリシーでカバーされる操作)	FDP_ACC.1-2

2		主体によるオブジェクトへのアクセスに関するルール	FDP_ACF.1
3		DAC ポリシーを上書きする権限	FDP_ACF.1
4	DAC 属性の制御/管理	オブジェクトに対するパーミション/ACLs の変更	FMT_MSA.1
5		新規に作成されたオブジェクトに対するデフォルトの保護	FMT_MSA.3
6		オブジェクト所有者の変更	FMT_MSA.1
7		ユーザグループの変更	FMT_MSA.1
8	強制アクセス制御/管理（MAC）	ポリシーの範囲（サブジェクト、オブジェクト、ポリシーでカバーされる操作）	FDP_IFC.1-2
9		アクセスフロー/情報フローに対するルール	FDP_IFF.2
10		MAC ポリシー上書きの権限	FDP_IFF.7-8
11		隠れチャネルの制限	FDP_IFF.3-6
12	MAC 属性に対する制御/管理	オブジェクトのラベル変更	FMT_MSA.1
13		新規に作成されたオブジェクトに対するデフォルトのラベル	FMT_MSA.3
14		ユーザのクリアランスの変更	FMT_MSA.1
15		ログイン時のセッション・クリアランスの選択	FTA_LSA.1
16	エクスポート/インポート	ラベルの無いデータのインポート	FDP_ITC.1
17		通信チャネル/装置を介したエクスポート	FDP_ETC.1-2
18		プリント出力に対するラベル付け	FDP_ETC.2
19	情報ラベル	情報ラベルの値に対する制約	FDP_IFF.2.3
20		Floating ラベルのルール	FDP_IFF.2.3
21	オブジェクトの再利用	ファイル、メモリなどに残存する情報の保護	FDP_RIP.1-2
22	ロールに基づくアクセス制御/管理（RBAC）	ポリシーの範囲（ロールや操作の観点）	FDP_ACC.1-2
23		操作の性能を制御/管理するルール	FDP_ACF.1(※1)
24		ロールの識別	FMT_SMR.1-2
25		Two-man ルールの実施	FDP_ACF.1(※2) FMT_SMR.2.3
26	RBAC 属性の制御/管理	ユーザ権限/許可の変更	FMT_MSA.1
27		ロール能力の定義の変更	FMT_MSA.1
28		ロールに対するユーザ割り当ての変更	FMT_MSA.1
29	ファイアウォールのアクセス制御/管理	サブジェクト-オブジェクト情報フローのビュー（例：送信元/送信先アドレスやポートに基づく）	FDP_IFC.1-2 FDP_IFF.1
30		セッションに基づくビュー（例：アプリケーション・プロキシー）	FTA_TSE.1(※3)

※ 1：他のコンポーネントもある。例えば、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1 など。特定のロールに対する特定の操作の性能に制限を与えるもの。

※ 2：FDP_ACF.1 も使える；特定の操作は、二つの区分されたロールによって許可されなければならない。また、FMT_SMR.2.3 は、ユーザアカウントは二つのロールに割り当てることはできないことを保証。

※ 3：代替として、FDP_IFC.1 と FDP_IFF.1 が利用できる。

9.2.1.3 監査

監査に分類されるセキュリティ機能要件は、以下の通りである（表 9-27）。

表 9-27:監査に分類されるセキュリティ機能要件

#	セキュリティ要件		ISO/IEC 15408 Part2 における機能コンポーネント
1	監査イベント	監査対応のイベントや情報の明確化	FAU_GEN.1
2		監査すべきイベントの選択に関する制御/管理	FMT_MTD.1
3		監査すべきイベントの選択に関する根拠	FAU_SEL.1
4		ユーザの責任追跡可能性	FAU_GEN.2
5	侵入検知と応答	緊急のセキュリティ違反に対する警告と応答の生成	FAU_ARP.1
6		潜在的、あるいは、緊急のセキュリティ違反を示すルール、イベント、イベント順序、システム使用のパターンの定義。	FAU_SAA.1-4
7	監査証跡の保護	データ損失に対する保護(例:監査証跡のあふれ、操作/運用に対する割り込み)	FAU_STG.2-4
8		不正な修正/アクセスに対する保護	FAU_STG.1
9	監査証跡の分析とレビュー	監査証跡分析ツール/レビューツールの提供	FAU_SAR.1-3

9.2.1.4 完全性

完全性に分類されるセキュリティ機能要件は、以下の通りである(表 9-28)。

表 9-28:完全性に分類されるセキュリティ機能要件

#	セキュリティ要件		ISO/IEC 15408 Part2 における機能コンポーネント
1	データ完全性	格納されたデータにおけるエラーの検知	FDP_SDI.2
2		チェックサム、一方向性ハッシュ、メッセージダイジェスト、などの生成と検証	FDP_DAU.1
3		トランザクションのロールバック(例:データベース)	FDP_ROL.1-2
4	TOE の完全性	タンパリングの検知	FPT_PHP.1-2
5		耐タンパー	FPT_PHP.3
6	データ認証	デジタル署名の生成と検証	FDP_DAU.2
7		証明書の生成と検証(例:公開鍵証明書)	FDP_DAU.2

9.2.1.5 可用性

可用性に分類されるセキュリティ機能要件は、以下の通りである(表 9-29)。

表 9-29:可用性に分類されるセキュリティ機能要件

#	セキュリティ要件		ISO/IEC 15408 Part2 における

			機能コンポーネント
1	リソースの消費	ユーザによるグローバル・リソースの消費に関する制限/クォータの実施	FRU_RSA.1-2
2		同一ユーザによるログイン・セッション数の制限	FTA_MCS.1-2
3	エラーの処理	故障時の TOE 操作の維持管理(フォールト・トレランス)	FRU_FLT.1-2
4		エラー検知	FPT_TST.1
5		エラー回復	FPT_RCV.1-4
6	スケジューリング	確立した優先度に応じて、アクティビティ/プロセスをスケジューリング	FRU_PRS.1-2

9.2.1.6 プライバシー

プライバシーに分類されるセキュリティ機能要件は、以下の通りである(表 9-30)。

表 9-30:プライバシーに分類されるセキュリティ機能要件

#	セキュリティ要件		ISO/IEC 15408 Part2 における機能コンポーネント
1	ユーザ・アイデンティティに基づくプライバシー	サービスやリソースを使用する際のユーザ・アイデンティティの暴露から保護	FPR_ANO.1-2
2		保護されたユーザ別名により匿名であるがサービスやリソースの使用に関して責任追跡可能性がある	FPR_PSE.1-3
3	リソース/サービスに基づくプライバシー	同一ユーザとサービスやリソースに対する複数の使用の間の関連性の暴露からの保護	FPR_UNL.1
4		特定のリソースやサービスの使用に関して観察できない	FPR_UNO.1-4

9.2.1.7 データ交換の要件

データ交換に分類されるセキュリティ機能要件は、以下の通りである(表 9-31)。

表 9-31:データ交換に分類されるセキュリティ機能要件

#	セキュリティ要件		ISO/IEC 15408 Part2 における機能コンポーネント
1	データ交換の機密性	ユーザデータ	FDP_UCT.1
2		セキュリティの観点から重要なデータ(例:鍵、パスワード)	FPT_ITC.1
3	データ交換の完全性	ユーザデータ	FDP_UCT.1-3
4		セキュリティの観点から重要なデータ(例:鍵、パスワード)	FPT_ITI.1-2
5	否認防止	送信者の証明	FCO_NRO.1-2
6		受信者の証明	FCO_NRR.1-2

9.2.2 ISO/IEC TR 15446 の暗号機能のセキュリティ機能要件

ISO/IEC TR 15446 では、暗号機能におけるセキュリティ目標とセキュリティ機能要件のマッピング例を示している（表 9-32）。

表 9-32：暗号機能におけるセキュリティ目標とセキュリティ機能要件

#	O.Type	セキュリティ目標	ISO/IEC 15408 の機能コンポーネント
1	O.I&A	TOE は、すべての利用者を一意に識別しなければならず、TOE 及びその中の暗号関連の IT 資産にアクセスしようとする利用者に許可を与える前に、その主張する識別情報を認証しなければならない。	FIA_UID.1-2 FIA_UAU.1-5
2	O.DAC	TOE は、TOE の利用者に対して、特定されたアクセス制御方針に沿って、暗号関連の IT 資産へのアクセスを制御する、かつ制限する手段を提供しなければならない。	FDP_ACC.1-2 FDP_ADF.1
3	O.PHP	TOE は、自分自身及びその中の暗号関連の IT 資産を、許可されない物理的アクセス、改変、または使用から保護すべきである。	FPT_PHP.1-3
4	O.INTEGRITY	TOE は、情報に影響を及ぼす完全性の喪失を検出する手段を提供しなければならない。	FPT_AMT.1 FPT_TST.1
5	O.FAILSFE	誤りの発生する事象において、TOE はセキュアな状態を保たねばならない。	FPT_FLS.1-4
6	O.ADMIN	TOE は、許可された管理者が、特定された暗号鍵管理方針に沿って暗号鍵を管理できるようにする機能性を提供しなければならない。	FCS_CKM.1-4 FCS_COP.1
7	O.EMI	TOE の電磁波放射によって、許可されない者または利用者に暗号関連の IT 資産が暴露されることを防ぐため、手続き的及び物理的手段がとられるべきである。	AGD_ADM.1 AGD_USR.1 セキュリティ運用手続き
8	O.PHYSICAL	TOE に責任を持つ者は、セキュリティ方針の実施において重要となる部分が、IT セキュリティを脅かす恐れのある物理的攻撃から保護されることを保証しなければならない。	セキュリティ運用手続き

9.2.3 Baltimore 社のタイムスタンプサーバのセキュリティ機能要件

Baltimore社のSTに記載されたセキュリティ機能要件を以下に示す（表 9-33）。

表 9-33：Baltimore 社のタイムスタンプサーバにおけるセキュリティ機能要件

#	ISO/IEC 15408 Part2 の機能クラス	機能コンポーネント	
1	セキュリティ監査	FAU_GEN.1	監査データの生成
2	通信	FCO_NRO.2	送信元の証明

3	暗号サポート	FCS_CKM.3	暗号鍵アクセス
4		FCS_COP.1	暗号オペレーション
5	識別と認証	FIA_UAU.1	認証のタイミング
6		FIA_UID.1	識別のタイミング
7	TSF の保護	FPT_ITT.1	基本 TSF 内データ転送保護
8		FPT_ITT.3	TSF データ完全性監視

9.2.4 日立製作所の認証局サーバのセキュリティ機能要件

日立製作所のSTに記載されたセキュリティ機能要件を以下に示す(表 9-34)。

表 9-34: 日立製作所の認証局サーバにおけるセキュリティ機能要件

#	ISO/IEC 15408 Part2 の機能クラス	機能コンポーネント	
1	セキュリティ監査	FAU_GEN.1	監査データの生成
2		FAU_GEN.2	利用者識別情報の関連付け
3		FAU_SAR.1	監査レビュー
4		FAU_SAR.2	限定監査レビュー
5		FAU_STG.1	保護された監査証跡格納
6		FAU_STG.4	監査データ損失の防止
7	暗号サポート	FCS_CKM.1a	暗号鍵生成
8		FCS_COP.1a	暗号操作
9		FCS_CKM.2b	暗号鍵配布
10	利用者データ保護	FDP_ACC.1	サブセットアクセス制御
11		FDP_ACF.1	セキュリティ属性によるアクセス制御
12	識別と認証	FIA_AFL.1	認証失敗時の取り扱い
13		FIA_ATD.1	利用者属性定義
14		FIA_SOS.1	秘密の検証
15		FIA_UAU.1	認証のタイミング
16		FIA_UID.1	識別のタイミング
17		FIA_USB.1	利用者・サブジェクト結合
18	セキュリティ管理	FMT_MOF.1	セキュリティ機能の振る舞いの管理
19		FMT_MSA.1a	セキュリティ属性の管理
20		FMT_MSA.2c	セキュアなセキュリティ属性
21		FMT_MSA.3	静的属性初期化
22		FMT_MTD.1b	TSF データの管理
23		FMT_SMR.1	セキュリティ役割
24		FMT_SMF.1	管理機能の特定
25	TSF の保護	FPT_RVM.1	TSP の非バイパス性
26		FPT_SEP.1	TSF ドメイン分離
27		FPT_STM.1	高信頼タイムスタンプ

10 セキュリティ機能評価ガイドライン

明確化したセキュリティ目標・対策（可能であれば、セキュリティ要件/機能）と統合化プラットフォームシステムの実装を比較し、統合化プラットフォームにおけるセキュリティ機能を評価する。

セキュリティ機能評価を取りまとめた一覧表の例は、下記の通りである。

脅威のセキュリティ目標・対策に対する統合化プラットフォームシステムの評価では、実際に、TOEが対策機能を実装している場合は、「なになに機能（～を行う）」などと記述する。また、TOEでは未実装の場合、想定される対策に関して、「なになにすることで実現可能」と記す（表 10-1）。

表 10-1：脅威のセキュリティ目標・対策及び実装システムに対する評価の記述例

#	脅威名	セキュリティ目標・対策		統合化システムにおける実現
1	T.ABUSE	防止	なになに	なになにすることで実現可能
		検出	なになに	なになに機能（～を行う）
		回復	なになに	なになに
…	…	…	…	…

セキュリティ環境における前提では、実現例を記載する（表 10-2）。

表 10-2：前提の実現例の記述例

#	前提名	実現例
1	A.LOCATE	TOE の設置場所は、ID カードを用いた入退出管理が施された居室である。 ID カードは、TOE にアクセスすることを許可されたユーザにのみ配布される。
…	…	…

セキュリティ環境における組織のセキュリティポリシーでは、想定される実現例を記す（表 10-3）。

表 10-3：組織のセキュリティポリシーの実現例の記述例

#	前提名	実現例
1	P.PROTECT_LOG（監査ログの保護）	監査ログに電子署名を施すとともに、監査ログを別システム上で保管することで、監査ログの暴露、改竄または削除を防止する。
…	…	…