

ガイダンス文書

# セキュリティターゲット作成の手引

平成17年3月

第1.2版

独立行政法人 情報処理推進機構

情報セキュリティ認証室

## 目次

### はじめに

- . 概説
- 1 . ST 作成
- 2 . 評価
  
- . ST 各論
- 1 . ST 概説
  - 1 . 1 ST 識別
  - 1 . 2 ST 概要
  - 1 . 3 CC 適合
- 2 . TOE 記述
- 3 . TOE セキュリティ環境
  - 3 . 1 前提条件
  - 3 . 2 脅威
  - 3 . 3 組織のセキュリティ方針
- 4 . セキュリティ対策方針
  - 4 . 1 TOE のセキュリティ対策方針
  - 4 . 2 環境のセキュリティ対策方針
- 8 . 1 セキュリティ対策方針根拠
- 5 . IT セキュリティ要件
  - 5 . 1 TOE セキュリティ要件
    - 5 . 1 . 1 TOE セキュリティ機能要件
    - 5 . 1 . 2 TOE セキュリティ保証要件
  - 5 . 2 IT 環境に対するセキュリティ要件
- 8 . 2 セキュリティ要件根拠
- 6 . TOE 要約仕様
  - 6 . 1 TOE セキュリティ機能
  - 6 . 2 保証手段
- 8 . 3 TOE 要約仕様根拠
- 7 . PP 主張
  - 7 . 1 PP 参照
  - 7 . 2 PP 修整
  - 7 . 3 PP 追加
- 8 . 4 PP 主張根拠

## はじめに

本書は、「ISO/IEC 15408(1999) Evaluation Criteria for IT Security (以下、「CC」という。)、および「JIS X5070(2000) 情報技術セキュリティの評価基準」に基づいて、セキュリティターゲット(以下、「ST」という。)を作成する際に注意すべき事項を記載したガイダンスである。新たな規格を定めたり、現規格である CC を補足するものでも、補完するものでもない。

本書は主に ST 作成者を対象にしているが、評価者が ST 評価時に参照することもできる。

本書は、CC の基礎的な解説を目的としたものではない。ST を作成する上で必要な知識は習得していることを前提にしている。このために、これから ST を作成する読者は、本書の前に、CC に関わる基礎知識を習得されることを勧める。

文書中、

【参考規格類】には、「IT セキュリティ評価・認証制度」において、規格として定められている CC (Common Criteria for Information Technology Security Evaluation) および CEM(Common Methodology for Information Technology Security Evaluation) を要約(正確な記載ではない)して記載してある。

CEM は評価方法を規定したものであるが、評価者はこれを規格として使用するため、ST の作成に際して、ST 作成者はこの規定内容についても把握しておかなければならない。なお、CC および CEM に記載してある事項については、内容が推奨に相当するものも、ここに記載してある。

【ガイダンス】は規格を解釈する上での考え方や作成時の推奨例を示す。ただし、規格ではない。

用語は JIS X5070(2000)で規定する定義による。

本書は、下記の文書を参照している。

- ・ ISO/IEC 15408-1(1999): Evaluation Criteria for IT Security Part1:Introduction and general model
- ・ ISO/IEC 15408-3(1999): Evaluation Criteria for IT Security Part2:Security functional requirements
- ・ ISO/IEC 15408-3(1999): Evaluation Criteria for IT Security Part3:Security assurance requirements
- ・ Common Methodology for Information Technology Security Evaluation Part2
- ・ CCIMB Interpretations-0407

- ・ ISO/IEC PDTR Guide for the production of PPs and STs, Version 0.93
- ・ 参考事例 「外務省 旅券申請審査システムセキュリティターゲット 第 1.05 版  
2004 年 11 月 18 日 外務省」
- ・ 参考事例 JISEC IC カードセキュリティターゲット バージョン 1.0

## ．概説

### 1．ST作成

#### 【参考規格類】

TOEの定義：評価の対象となるITの製品又はシステム、それに関連するガイダンス証拠資料。(CC)

製品の定義：単独での使用又は様々なシステム内への組み込みを目的に設計された機能性を提供するITのソフトウェア、ファームウェア、及び/又はハードウェアの集まり。(CC)

システムの定義：特定の目的及び運用動作環境を伴う特定のIT設備。(CC)

STは一連のセキュリティ要件を含む。このセキュリティ要件はPPを参照するか、CCの機能コンポーネント若しくは保証コンポーネントを直接参照するか、又は明示的に記述することによって作成が可能。(CC)

STは、セキュリティ要件及びセキュリティ対策方針、TOEの要約仕様、それぞれの根拠を含む。STは、TOEが提供するセキュリティに関して、すべての関係者間の合意の基礎となる。

記載内容と構成は利用者に理解できるものであること。(CEMワークユニット共通)

記載内容は内部的に一貫していること。(CEMワークユニット共通)

内部的に一貫しているとは；

- 記載事項に曖昧さが無い、
- 同一事項の説明に対して、異なった箇所に矛盾するような説明がない、

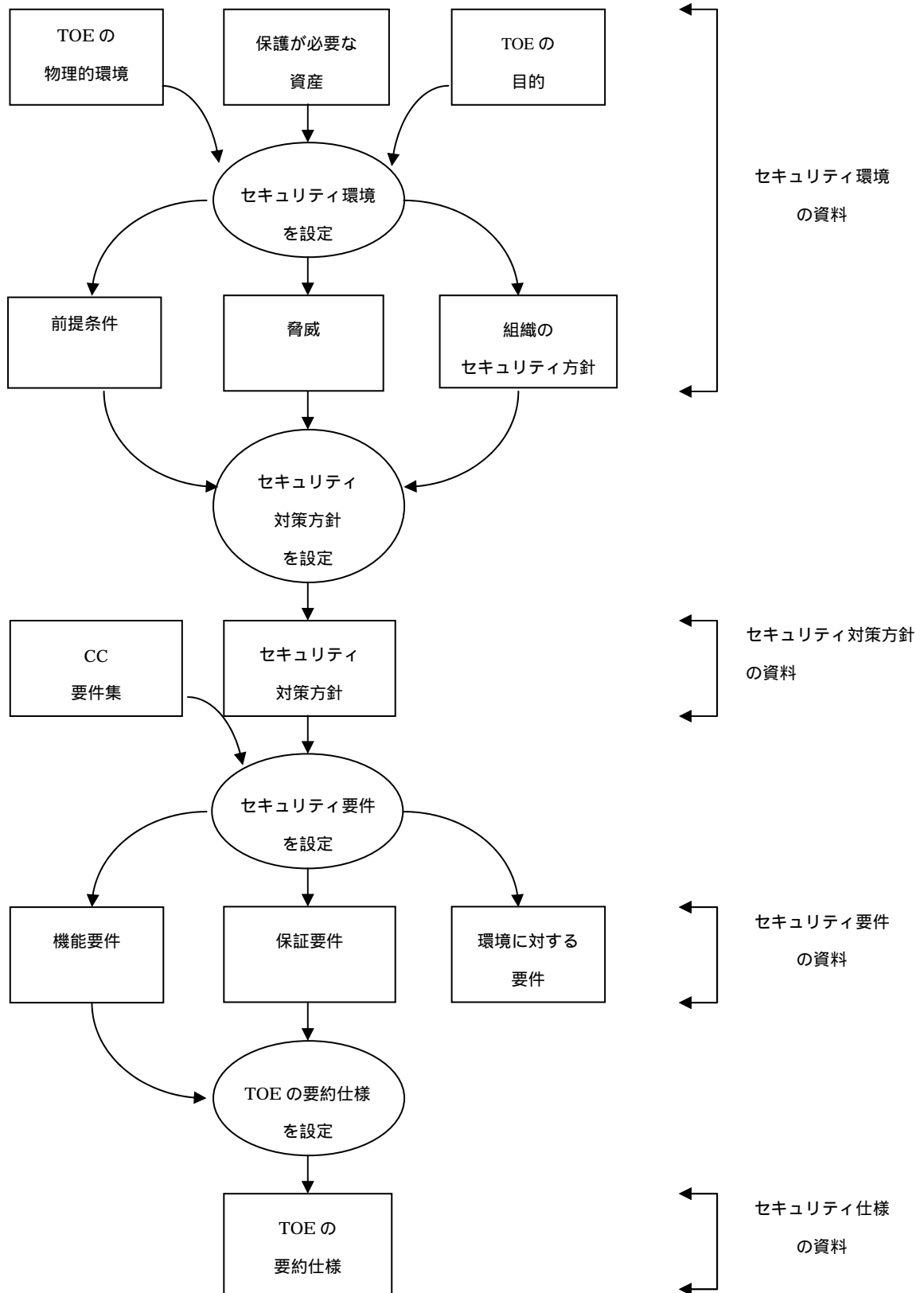
ことである。

セキュリティ属性の定義：TSPの実施を目的として用いられる、サブジェクト、利用者、オブジェクト、情報、及び/または情報の特性。(CC)

例として、利用者識別情報、サブジェクト識別情報、役割、作成時間、アクセス権(例：アクセス制御リスト(ACL))などがある。

ガイダンス証拠資料の定義：ガイダンス証拠資料は、TOEの配付、導入、構成、運用、管理及び利用を記述する。これらのアクティビティは、TOEの利用者、管理者及びインテグレータに適用される。ガイダンス文書の範囲と内容における要件は、PPまたはSTにおいて定義する。(CC)

STの枠組みは下記。(CC)



## 【ガイダンス】

ST は、読者が、

- TOE のセキュリティ機能を正確に理解する、
- TOE のセキュリティ機能が必要かつ十分なものであることを理解する、
- TOE のセキュリティ保証目標を理解する、

ことを目的とする。

規格は遵守する。

規格に要求されている事項を要求されている箇所（章、節）に記載する。

例：規格に準拠

CEM では、TOE 要約仕様において、確率的または順列的メカニズムによって実現されるすべての IT セキュリティ機能を識別していることを要求している。

TOE 要約仕様の説明の中で識別しないで、「TOE 要約仕様根拠の説明から読み取れ！」というのでは規格準拠にはならない。

ST の読者には、TOE の利用者や情報システム管理者が含まれる。したがって、ST はメモではない。記載内容は、技術文書として正確かつ簡潔でなければならない。

TOE の導入決定者/システム管理者/システムインテグレータ/システム運用者/開発者などの利用者それぞれに合わせて、ST 各章の記載内容と記載の詳細レベルを決める。

ST は技術文書である。ST の読者に、ST の行間を読むことや全体から類推することを強要してはならない。読者に理解させる必要がある事項は ST に明記する。図表についても、何を説明するためのものなのかを記載する。

ST は、利用者が「TOE の利用環境に求められている条件は何か」を理解できるものでなければならない。

利用者は、TOE の利用者（一般利用者/管理者）向けマニュアルを理解するのに必要なレベルの情報処理技術に関わる知識しか持っていないことを前提とする。この前提において自明でない用語は定義し、その用語を使用する（似て非なる用語を使用しない）。

ST は、利用者が「TOE に装備されているセキュリティ機能（要約仕様レベル）はいかなるもので、それらは必要最小限で、かつ、十分なものである。」ことを理解できるものでなければならない。このために、ST はトップダウン方式（セキュリティ要求仕様 セキュリティ対策方針 セキュリティ要件 要約仕様）で対応と詳細化、具体化を行うものである。“はじめに実装ありき”ではない（ST の作成方法としてはあり得るが）、前工程の記載内容から後工程の規定内容が必要かつ十分であることを、読者が理解できる（相互の工程でトレースが可能）ものでなければならない。

ST で記載すべき項目がワークユニットで規定されている場合は、その項目名を記載し、その後該当する内容を規定する形式を勧める（利用者の明確な理解を助けるため）。

章、節の構成および名称は JIS X5070 付属書 C に準拠（本ガイダンスはこれに準拠）

する。準拠しない場合には、その理由を明記する。

適したセキュリティ機能要件および保証要件が CC パート 2 およびパート 3 に無い場合には新規に規定する。既存の要件を無理して使用することは避ける。

必要な事項を簡潔に記載する。関係の無い、余分なことは記載しない。

## 2. 評価

評価者は ST の読者 (TOE の利用者、TOE の開発者など) の立場で記載内容の明確さや十分性や妥当性についてレビュー (本書に基づいて、機能設計を行うことが可能か? ガイダンス文書の執筆は可能か? などの観点からチェックする。) する。ST 作成者の代弁者であってはならない。客観性を高めるために、複数でレビューを行うことを勧める。特に、TOE を知りすぎてしまった場合には、既成の知識を持たない評価者に必ずレビューしてもらおう。

「ST 記載の表現には問題があり、正確な理解は困難かもしれないが、作成者が意図している内容には問題は無い。」というような判断は不適切。ST の読者は ST に記載してある内容から判断する。ST 作成者による解説を前提にしているわけではない。

評価報告書には CEM の要求内容、その検証方法と結果を記載する。検証方法の記載は、他の評価者が記載内容だけを参照して同等の検証が実施できる程度に具体的、かつ詳細なものでなければならない。(反復性、再現性)

悪い例: XX の説明に対して異なった箇所に矛盾するような説明がないことを検査し(これは CEM の要求そのまま) 矛盾するような説明は検出できなかった。

良い例: キーワード XX で ST の全箇所を検索し、該当する箇所の機能説明内容が、2.2 TOE 機能概要に記載してある XX に関わる説明の内容に反したものが無いことを確認した。

情報セキュリティの一般常識を評価に適用しなければならない (ST が機能開発の入力文書として妥当か? と自問自答するのと同義)。下記は事例。

- ・ 監査者と運用関連者の独立
- ・ 特権は必要最小限に
- ・ 公開は必要最小限に

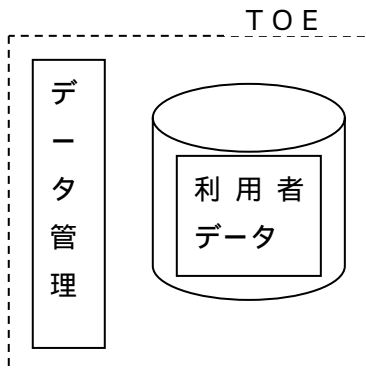
### 3 . 注意事項

#### セキュリティ製品と TOE のセキュリティ機能

CCではTOEの資産を保護するものとしてTOEのセキュリティ機能を位置づけている。このため、ファイアウォールなどのセキュリティ機能（パケットフィルタリングやアプリケーションゲートウェイなど）が必ずしも TOE のセキュリティ機能として定義できるわけではないことに注意が必要である。なぜなら、TOE の資産を保護するための機能ではなく、他の製品やシステムの資産（ファイアウォールの場合は内部ネットワークで管理されている資産）を保護するための機能（これはセキュリティ機能ではあるが、TOE からみれば提供するサービス機能の位置づけになる）であり、1. ST 作成の で述べた脅威から導かれる機能ではない。

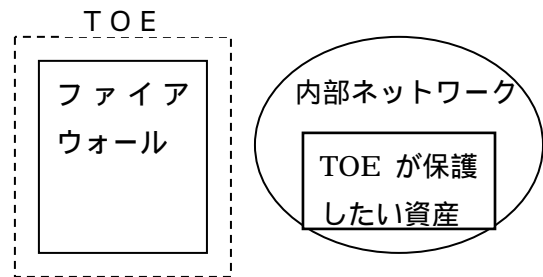


TOE がデータ管理機能の場合



この場合、保護資産である利用者データは、TOE であるデータ管理機能が直接処理の対象とすべきデータである。これを保護するためのアクセス管理機能などが TOE のセキュリティ機能になる。

TOE がファイアウォール機能の場合



ファイアウォール製品部分だけを TOE として識別した場合、保護資産はファイアウォールを通過する際のパケットデータなどとなり、内部ネットワーク内のホスト上のデータなどは保護資産にはならない( TOE が直接処理対象とする資産ではないという意味)。このため TOE のセキュリティ機能は、メモリー上のパケットデータの秘匿や改ざん防止などであり、パケットフィルタリングやアプリケーションゲートウェイが TOE のセキュリティ機能にはならない。パケットフィルタリングやアプリケーションゲートウェイをセキュリティ機能として、評価するためには、

- ・ セキュリティ製品の対象となる保護資産(この場合は内部ネットワーク)を TOE 保護資産とする(この場合、脅威の識別に注意のこと)

または、

- ・ 組織のセキュリティ方針として製品のセキュリティ機能を規定する。

## セキュリティ機能

TOEの一部であって、TOE保護資産がTOE内でどのように保護されるかを規定する規則を実施するための機能がセキュリティ機能である。(CCパート1定義)

具体的には、通常下記の機能がセキュリティ機能と定義されている。(ISO/IEC TR Guidelines for Management of IT Security)

- ・ 機密性：許可されていない個人、エンティティ、またはプロセスに対して情報を使用不可または非開示にする特性
- ・ データ完全性：許可されていない方法でデータを改ざんまたは破壊されないようにする特性
- ・ システム完全性：システムが、意図的または偶発的な不正操作によって妨害されることなく、本来果たすべき機能を滞りなく実行する特性。
- ・ 可用性：許可されたエンティティによって要求されたときにアクセスと使用を可能にする特性
- ・ 責任追跡性：あるエンティティの動作が、そのエンティティに対して一意に追跡できることを保証する特性
- ・ 真正性：対象物またはリソースが要求されているものと同一であることを保証する特性
- ・ 信頼性：矛盾のない意図した動作と結果を確保する特性

これらを侵害するものが脅威になる。

## . ST 各論

### 1 . ST 概説

#### 【参考規格類】

ST概説はその他の部分と一貫していること。(ASE\_INT 1-6)

ST概説はTOEの正確な要約であり、TOE範囲外のセキュリティ機能について記載したり、その存在を暗示するような表現があってはならない。

### 1 . 1 ST 識別

#### 【参考規格類】

ST及び対象のTOE を管理及び識別するために必要なST 識別情報を記載すること。  
(ASE\_INT.1-1)

下記を記載；

ST の名称

本 ST を一意に識別できる情報（バージョン番号、発行日、作成者など）

TOE を管理および一意に識別するための情報（TOE の名称、そのバージョン番号など）

使用する CC のバージョン

#### 【ガイダンス】

下記を記載することが望ましい。

キーワード（TOE を特徴付ける提供機能やセキュリティ機能）

保証パッケージ（EAL など）

使用する CC のバージョンの箇所には、適用する規格とそのバージョンなどの識別情報を記載する。また、制度が要求する追加情報として適用した評価補足文書（補足-0210 第 2 版および補足-0407、CCIMB Interpretations-0407）について記載する。

TOE は製品全体なのかその一部なのかを明確に規定し、以降はこの規定で一貫する。

保証レベルの考え方（参考：PP Consistency Guidance for Medium Robustness）

TOE に関わる保護資産（TOE 自体やその処理データなど）の最大価値と資産利用エンティティ（利用者、運用者、他システムなど）の最小信頼度を指標にして最適な保証コンポーネントを選択する。

記述例

ST 名称：ABC スマートカードセキュリティターゲット

ST バージョン：1.03

ST 発行日：2004 年 10 月 21 日

作成者：ABC 株式会社

TOE 名称：ABC スマートカード

TOE バージョン：1.1

CC バージョン：CC V2.1 + 補足-0210 第 2 版および補足-0407

## 1.2 ST 概要

### 【参考規格類】

TOEが関心の対象となるかどうかを利用者が判断するのに十分に詳細であることが望ましい。また、認証製品リストに取り込める抄録として単独で利用可能であることが望ましい。(CC)

ST の内容の簡潔な要約（詳細な記述は、TOE 記述に記載される）を記載し、利用者がTOE（及び残りのST記載事項）に興味を示すことができる情報を提供すること。(ASE\_INT.1-2)

### 【ガイダンス】

TOE の機能と特徴、および提供するセキュリティ機能を簡潔に記載する。ST の読者の興味をひきつけられるか否かは、この箇所の記述内容で決まる。

記述例。(イギリス CESG 発行の認証製品リストより)

*Oracle 7 はリレーショナルデータベース管理システムであり、多様な利用者に対して、分散環境に適した高度なセキュリティやデータベース管理機能を提供する。EAL4 相当以上の OS の下で、Oracle 7 Release 7.2.2.4.13 は EAL4 相当のセキュリティを提供する。*

*主なセキュリティ機能は、*

- ・ 分散データベース間のセキュアな通信機能、
- ・ 最小特権の考え方に基づくきめ細かな単位でのデータベース管理機能、
- ・ 利用者に役割を付与し、この役割に基づくアクセス権限の管理機能、
- ・ 多様で柔軟な監査機能、
- ・ 警告機能、

*である。*

## 1.3 CC 適合

### 【参考規格類】

TOEのCC適合について評価可能なすべての主張を記述すること。(ASE\_INT.1-3)

PPへの適合が主張される場合、適合主張の対象となるPP(複数指定可能)を識別する。

CC 適合主張がパート 2 適合またはパート 2 拡張のいずれかである。また、パート 3 適合またはパート 3 拡張のいずれかである。

パート3 拡張が主張され、保証要件パッケージがパート3 の保証要件を含む場合、CC適

合主張がパート3 にあるどの保証要件が主張されているのかを述べているかを記載する。

パッケージ適合が主張される場合、CC 適合主張がどのパッケージに対して主張されているかを記載する。

パッケージ追加が主張される場合、CC 適合主張がどのパッケージに対して主張されており、そのパッケージに対してどの追加が主張されているかを記載する。

CC 適合主張がST の残りの部分の記載内容と矛盾していないこと。(ASE\_INT.1-5)

#### 【ガイダンス】

##### 記述例

- ・ CC バージョン 2.1 パート 2 適合
- ・ CC バージョン 2.1 パート 3 適合
- ・ 保証パッケージは EAL3 に ADV\_SPM.1, AVA\_VLA.2 を追加

## 2 . TOE 記述

### 【参考規格類】

TOE についてそのセキュリティ要件の理解の一助となることを目的に記載する。(CC) 製品またはシステムの種別 (例: ファイアウォール、スマートカード、暗号モデム、ウェブサーバ、イントラネット) を記載すること。(ASE\_DES.1-1)

TOEの機能概要を記載し、読者がTOEの利用に関して理解できる内容でなければならない。製品またはシステムの種別によって明らかにいくつかの機能がTOE に期待される場合がある。TOEにこの機能がない場合には、このことを明確に記載しなければならない。

TOE の物理的範囲及び境界を記載すること。(ASE\_DES.1-2)

TOEを構成するハードウェア、ファームウェア、及び/またはソフトウェアコンポーネント及び/またはモジュールについて説明する。

TOEが製品と同一でない場合、TOE と製品間の物理的関係を説明する。

TOEの論理範囲及び境界を記載すること。(ASE\_DES.1-3)

TOEの機能および、TOE によって提供されるセキュリティ機能について説明する。

TOE が製品と同一でない場合、TOE と製品間の論理的関係を説明する。

TOEの記述が理路整然としていること。(ASE\_DES.1-4)

記載内容が対象読者(すなわち、評価者及び消費者)に理解可能でなければならない。

TOEの記述が内部的に一貫していること。(ASE\_DES.1-5)

TOE記述はその他の部分と一貫していること。(ASE\_DES.1-6)

TOE記述には、STの他の箇所では考慮されていない脅威、セキュリティ機能またはTOEの構成についての記述が含まれていないこと。

### 【ガイダンス】

次章以降の、TOE セキュリティ環境やセキュリティ対策方針などの規定内容を理解する上で必要となる TOE 関連事項については、本 TOE 記述で記載する。読者はこの TOE 記述の記載内容によって TOE を理解する。

STは単独で完結した文書でなければならない。TOE 種別、TOE の物理的な範囲 (下記目次例の 2.3)、TOE の論理的な範囲(下記目次例の 2.5)の項に分けて明確に記載することを推奨する。

目次例 ;

#### 2 . 1 TOE の概要

TOE の種別を記載

#### 2 . 2 用語定義

TOE の機能および、TOE のセキュリティ機能に関する用語を定義する。

#### 2 . 3 TOE の機能 (論理的な範囲の記載を含む)

TOE の機能概要と TOE の保護資産概要を記載

#### 2.4 TOE の利用

利用目的、利用環境、利用方法を記載

#### 2.5 TOE の構成（物理的な範囲の記載を含む）

ハードウェア構成、ソフトウェア構成、ネットワーク環境を記載

#### 2.6 TOE のセキュリティ機能

TOE のセキュリティ機能についての簡潔な説明を記載

規格において、「製品」と「システム」は明確に識別されて、定義されている。ST で使用する用語も、正確にこの定義に従う。

注：CC で定義する「システム」とは、「特定の目的と運用環境を伴う特定の IT 設備」のことを意味する。

正確な TOE の範囲、すなわち、TOE に含まれるものと含まれないものを明確に識別する。

物理的な範囲（ハードウェア、ソフトウェアコンポーネント/モジュール）

注：TOE の動作構成図は物理的な範囲を直接に示すものではない。

論理的な範囲（TOE が提供する情報技術やセキュリティ特性）

TOE に含まれないものに対する説明は、TOE を理解する上で必要な範囲にとどめる。TOE がソフトウェア製品だけの場合、TOE としてハードウェアを規定してはならない。TOE セキュリティ機能については、「1.2 ST 概要」で説明した事項に簡潔な説明を加える。

TOE が製品（利用者に提供される単位）の一部の場合には、識別された TOE を利用者が認識できなければならない。利用者が認識できない機能や内部構造によって TOE を規定した場合には、その範囲を利用者が認識できないので、TOE としては不適切である。

TOE 記述で記載した事項は、必ず、セキュリティ環境やセキュリティ対策方針に反映されなければならない。例えば、TOE の関連者として異なった役割、権限を想定するのであれば、それはセキュリティ対策方針（識別と権限付与など）に規定されなければならない。

TOE が提供する機能の説明と TOE の運用手順の説明とで内容に矛盾が無いようにする。

TOE の保護資産の記載では、資産の識別、TOE の管理下に入るタイミング、利用される環境や条件、TOE の管理下から外れるタイミング、などを正確に述べる。

### 3 . TOE セキュリティ環境

#### 【参考規格類】

セキュリティ環境には、関連するすべての法規、組織のセキュリティ方針、慣行、技能及び知識が含まれる。(CC)

TOE が意図している使用方法を定義する。さらに、その環境に存在する又は存在すると考えられるセキュリティに対する脅威を含む。

ST の作成者は、次のことを考慮しなければならない。

- a) TOE のセキュリティに関連するすべての運用環境と物理的環境。これには、既知の物理的及び人的な構成が含まれる。
- b) TOE による保護が必要な資産。これには、ファイル、データベースなどのように、直接利用する資産だけでなく、証明書、IT の実装など、当該資産へのセキュリティ侵害によって、データベースなどの資産を侵害するような、間接的にセキュリティ要件の対象となる資産も含まれる。
- c) TOE の目的。これは、TOE の製品種別及び意図した用途を含む。

セキュリティ方針、脅威及びリスクに関するセキュリティ課題を次に示す事項にまとめる。(CC)

- a) TOE が安全であると見なされるために TOE の環境が満たすべき使用上の前提条件。
- b) TOE の処理資産に関わるすべての脅威。

CC は、脅威エージェント、推定される攻撃方法、攻撃のきっかけとなる脆弱性、及び攻撃対象となる資産の明確化によって脅威を特徴付ける。セキュリティに対するリスクの評定では、このような脅威が実際の攻撃に発展する可能性、このような攻撃が成功する可能性及びその結果生じるすべての損害を評定することによって、各脅威を分類する。

- c) 関連する方針及び規則を明らかにした組織のセキュリティ方針。

IT システムの場合、明に適用する方針を参照してもよい。これに対して、はん(汎)用の IT の製品又は製品群の場合、適用している実際的前提内容を記載することが必要となることもある。

TOE が物理的に分散しているときは、TOE の分散されたそれぞれの領域ごとにセキュリティ環境(前提条件、脅威及び組織のセキュリティ方針)の考察が必要な場合がある。(CC)

TOE が意図する使用環境のセキュリティ及び想定される使用方法を記述(利用者が理解可能な記載内容であること。)すること。(ASE\_ENV.1-4)

TOE セキュリティ環境の記述が内部的に一貫していること。(ASE\_ENV.1-5)

内部的に一貫していない記述の例；

- 攻撃方法が脅威エージェントの能力範囲内でない脅威を含む

- 「TOE をインターネットに接続してはならない」という組織のセキュリティ方針及び脅威エージェントがインターネットからの侵入者であるという脅威を含む

## 【ガイダンス】

TOE のセキュリティに関わる課題( 要求仕様、セキュリティ与件 )を明確に記載する。TOE にとって何がセキュリティ上の与件なのかを記載する。TOE がいかにこの与件を実装するかについての記載は不要。

このために、例えばTOEが保護すべき資産( 資産は「TOEの対抗策が保護すべき情報または資源」と定義されている )についても具体的な識別が必要である。「TOEが管理するデータ」との定義では、どのようなデータかが識別できないため、不十分な定義であると言わざるを得ない。

利用者は本章で記載の脅威や前提などの内容によって、TOE の動作/運用環境が実際の利用環境に適したものであるか否かを判断する。したがって、この目的が達せられる内容にする。

TOE が物理的に分散しているときは、TOE の分散されたそれぞれの領域ごとにセキュリティ環境(前提条件、脅威及び組織のセキュリティ方針)の考察が必要な場合がある。TOE がセキュリティ製品( 例として電子署名機能を例示する。 )である場合の考え方；

- ST で記載するセキュリティ機能は、あくまでも TOE が処理する資産( 例では署名のために入力されるデータ )を保護する機能( データに対するアクセス管理機能など )と考える。この場合は、電子署名機能は ST ではセキュリティ機能としては扱われないことになる。この箇所に対する保証要件も適用範囲には含まれないことになる。
- ST で記載するセキュリティ機能にセキュリティ製品としての機能( 例では電子署名 )も含めたい場合。セキュリティ機能に含めることによって、保証要件の適用範囲に含めることができ、セキュリティ評価の対象になるので利用者にとっても好ましい。

この場合は、セキュリティ機能( 例では電子署名 )を要求するために、本章の TOE セキュリティ環境では、次の 2 つのいずれかの方法で、その課題を規定する。

- a. 組織のセキュリティ方針で記載する。
- b. 電子署名の対象となるデータを保護資産とする。( この場合には、脅威の識別に注意する。データそのものに対する全ての脅威への対抗策をセキュリティ機能として提供するわけではない。このため、対抗する脅威の特定とその理由を明確にしなければならない。 )

前提条件で規定した事項と脅威で記載した事項が矛盾してはならない。下記は矛盾した例。

前提条件：運用端末は管理された部屋に設置し、非許可者が利用することはできない。  
脅威：運用端末が不正な利用者によって操作される。

前提条件：IC カードは所有者の責任で他人が使用することがないように管理する。  
脅威：IC カードが他人に盗用される。

### 3.1 前提条件

#### 【参考規格類】

下記の事項について記載すること。(ASE\_ENV.1-1)

意図されている TOE の利用環境

TOEの意図する利用方法、TOEによる保護を必要とする資産の潜在的な価値、及びTOEを使用する上での制限内容について記載する。利用者が意図する使用法が、本項で記載の前提条件と一致していることを判断するのに必要なレベルの詳細度で記載する。

TOE に対する物理的な環境による保護内容

TOEがセキュアな方法で動作するために、TOEまたは付属周辺機器の物理的場所についての条件（例：管理者コンソールは管理者にのみ利用を制限されている部屋に設置する）を記載する。利用者が意図する物理的環境が、本項で記載の前提条件と一致していることを判断するのに必要なレベルの詳細度で記載する。

接続に関わる条件（例えば、外部と内部ネットワークの接続はファイアウォールを仲介するなど）

TOEがセキュアな方法で機能するために、TOEとTOEの外部にある他のITシステムまたは製品（ハードウェア、ソフトウェア、ファームウェア、またはそれらの組み合わせ）との接続に関して、必要となる全ての前提条件（例：TOEが信頼できないネットワークに接続されないことを想定する。）を記載する。利用者が意図する接続環境が、本項で記載の前提条件と一致していることを判断するのに必要なレベルの詳細度で記載する。

人的な条件（例えば、役割の種別、役割における責任、信頼できる度合い、など）

TOEがセキュアな方法で動作するために、TOE環境内のTOEの利用者及び管理者、またはその他の個人（潜在的な脅威エージェントを含む）についての条件（例：利用者が特定のスキルまたは専門知識を持っている。）を記載する。利用者が意図する人的条件が、本項で記載の前提条件と一致していることを判断するのに必要なレベルの詳細度で記載する。

#### 【ガイダンス】

TOE のセキュアな動作や運用に関連しない事項は記載しない

前提条件は、TOEの意図する使用法についての前提条件、またはTOEの使用環境についての前提条件のどちらかである。

TOEのセキュアな動作や運用に関わる事項のみを、前提条件として明示する。これによって、利用者は当該TOEのセキュアな動作や運用条件を把握できる。脅威として規定することもできる。この場合、これに対するセキュリティ対策は環境によって受けることになる。しかし、非IT環境のセキュリティ要件は明示されない場合もあり、利用者がセキュアな動作や運用条件を把握できないといった事態も発生する。

悪い例：

暗号鍵の管理がセキュアなプロトコルで実施されることを前提条件で記載。しかし、暗号鍵を利用した処理（データの暗号化など）自体はTOE外の処理。この場合、TOEの処理には関係しない事項を前提条件に記載すべきではない。

悪い例：

パーソナルコンピュータにインストールして使用するTOEについて、TOEはパーソナルコンピュータやオペレーティングシステムとセキュリティ機能の動作に関して何も関連性を持っていないにもかかわらず、「TOEを使用するためにTOEに対応した動作環境（パーソナルコンピュータ、オペレーティングシステム）を必要とする。」と記載。

TOEのセキュリティ機能を前提条件に記載してはならない。TOEの動作や運用のための条件を、前提条件として記載する。したがって、TOEのセキュリティ機能で、この条件に対処することは矛盾を生じることになる。

悪い例：

TOEが管理しているデータに対して、“不正アクセスから保護されていること”を前提条件にすると、TOEではなく、環境でこのための対処を行うことになる。

悪い例：

本人認証のためのパスワードはTOEが管理しているにもかかわらず、前提条件に、「一方向性の関数で暗号化して、パスワードファイルに格納する。」と記載。

前提条件を増大させることは、TOEの適用環境を制限することになることに注意しなければならない。この制限はTOEの市場価値を狭めることにつながる。

前提条件で規定された事項はTOEの動作や運用に際して、保証できるものでなければならない。保証できなければ、脆弱性を伴うことになる。このため、前提条件の内容の妥当性については、十分な配慮が必要である。

例えば、前提条件で「一般利用者が不正な行為はしない。」と規定した場合、TOEの利用者には不正な者が存在しないような動作環境でのみ、このTOEを使用できることを意味している。また、「LAN上の通信データの機密性と完全性は確保される。」と規定した場合には、LAN接続に関わる規制が必要になる。前提条件で「セキュアである」

と規定すれば、あとは「利用者が適切な条件のもとでセキュアな利用を保証する。」ことを期待するのは誤りである。利用者が何を実施すればセキュアな利用が保証できるかについての“何を”について、前提条件に記載しなければならない。

「TOE の利用者は、自分のパスワードを定期的に適切な内容で変更しなければならない。」といった記載も、“定期的に適切な”という表現から、利用者が具体的に“何を”すればよいのか読み取れない悪い例である。

ここでの記載事項は製品の利用関連マニュアルに記載することになる。利用者が妥当であると判断できる内容でなければならない。

前提条件で規定した事項は、それを実現するための対策方針を、次章で記載しなければならない。次章で記載できないような、あるいは、記載しても意味が無いような前提条件は規定しない。

TOE 自体や IT 環境がセキュリティ機能を装備することによっては対抗できない事項を前提条件として規定する。

例：TOE の運用に際して、すべての管理者は TOE をセキュアに管理するための必要な教育と訓練を受ける。

例：IT 環境が提供する物理的なセキュリティによって、データが格納された媒体を保護する。

悪い例：全ての利用者は TOE を利用するに先だって認証されているものとする。(TOE 自体や IT 環境がセキュリティ機能を装備することによって実現できるため、前提条件にすることは好ましくない。)

記述例

(ア) LOCATE

TOE の処理に関わる機器類は物理的なアクセスが管理された部屋に設置する。

A.ADMIN

TOE のセキュリティ管理は信頼できる管理者が行い、不正行為はしない。

A.FIREWALL

外部ネットワークと内部ネットワークの接続は、唯一、ファイアウォールを介してのみ可能になる。

注：A.LOCATE などのラベルは、文中の説明や根拠記載のための表中で使用するものであり、特定の ST でのみ意味を持つものである。また、必ずしもラベルを記載する必要は無い。

### 3.2 脅威

#### 【参考規格類】

資産の定義：“TOE の対抗策で保護する情報および資源”(CC)

資産は IT システムで保管、処理、転送される情報の場合が多い。

環境において直面すると考えられるすべての脅威を挙げる必要はなく、TOEの安全な運用に関連するものだけを挙げればよい。(CC)

存在する脅威について識別し、説明すること。(ASE\_ENV.1-2)

識別されたすべての脅威に対して、その脅威エージェント、攻撃、及び攻撃の対象となる資産に関して明確に説明する。

脅威の特性として、脅威エージェントの専門知識、資源、及び動機を記載する。また、攻撃に関しては、攻撃方法、悪用される脆弱性、及び機会を記載する。

TOE 及びその環境のセキュリティ対策方針が前提条件及び組織のセキュリティ方針からのみ派生するものである場合、脅威を識別する必要は無い。

### 【ガイダンス】

機密性、完全性、信頼性、真正性、責任追跡性、可用性が損なわれると TOE の正常な処理に影響を与える情報や資源が、保護対象資産である。TOE が処理の対象としているものを資産として識別する。

適切な脅威分析（保護すべき資産の識別、資産に対する脅威の抽出、資産価値に応じたセキュリティ対策）を行うことが必要である。脅威エージェントについては、技能、利用可能な資源及び動機を考慮して記述するのがよい。攻撃については、攻撃方法、つけ込まれる脆弱性及び機会を考慮して記述するのがよい。

攻撃レベル（高、中、低）も識別しておく。

セキュリティ機能をバイパスしたり干渉したりするような、資産から見ると間接的な脅威（セキュリティ機能自体への攻撃）については、セキュリティ機能が本章より後ろで言及されることもあり、この部分で規定することは読者に混乱を与えるので好ましくない。セキュリティ機能に対する動作の迂回、破壊、非稼働などの脅威は、本節で間接的な脅威として記載しないで、セキュリティ機能の動作に対する支援機能要件として配慮することを推奨する。

組織のセキュリティ方針及び前提条件だけからセキュリティ対策方針を導き出す場合、脅威の記述は省略してもよい。（ただし、脅威に関わる最新の状況が組織のセキュリティ方針及び前提条件に反映されているという保証がなければ、脅威の記述を省略することは危険である。）

TOE に対する特定の攻撃については脅威として規定し、一般的な脅威（TOE の動作・運用に関わるもので、TOE による対処を意図していない）については前提の項で記載するのが妥当である。

例えば、TOE の安全な動作/運用に関しては、脅威として記載してもいいし、前提として規定してもいい。どちらにしても、次節のセキュリティ対策方針で受けることになる。しかし、TOE のセキュアな運用条件が明白な場合には、その条件を前提条件として記載することを勧める。利用者は TOE を利用するための条件としての位置づけが、

明確に理解できる。

下記の事項を明瞭かつ簡潔(重複を避け、記載の詳細レベルを合わせる)に記載する。

#### TOE が保護しなければならない資産

一般的に、資産は IT システムで保管、処理、転送される情報の形態をとり、TOE の利用者に関わる利用者データ、及び TOE の動作に関わる TSF データが該当する。

#### 脅威となるエージェント

権限を付与されている人への成り代わり、外部インタフェースを利用した攻撃、操作ミスなど、人が脅威エージェントとなる場合が多いが、人以外の物がエージェントになることもある。

#### - 保護対象資産に対する攻撃方法または脅威となる事象

TOE のセキュリティ環境に対する脆弱性分析や前提条件を配慮することによって脅威となるエージェントが利用できる潜在的な脆弱性を抽出したり、TOE のセキュリティ環境にアクセスする攻撃者の能力を分析することによって、保護対象資産に対する攻撃方法を識別する。脅威への対策の妥当性を検証するためにも、具体的な攻撃方法を記載する。“不正な利用方法によって・・・”という抽象的な表現では、対策方針の立案も、その検証もできない。

例えば、攻撃については、資産に対する直接の攻撃方法(暴露、改ざん、破壊などを発生させる方法や手段)を識別する。

“攻撃者が物理的にデータを暴露する。”との記載では暴露するための攻撃方法が記載されていない。どのようにして暴露するかを識別しなければならない。

脅威の識別において、上記の項目の内容が異なる場合には、異なった脅威として識別することを勧める。この識別が不明瞭であると、対策方針の識別も不明瞭になる。

外部インタフェースが存在する場合、そのインタフェースを不正に利用する攻撃は、脅威として考慮すべきである。

ASE\_ENV.1-2 では「存在する脅威について識別し、説明すること」を要求している。本規格では、すべての脅威を識別することは要求していないが、必要十分なセキュリティ対策を策定するためには、存在すると想定される脅威は漏れなく識別しておくことを勧める。ST における脅威の識別に漏れが発生した場合、TOE にとって必要なセキュリティ機能が欠如することになる。セキュリティ機能の欠如が、後の脆弱性の分析で検出されたとしても、開発への手戻りが大きなものになる。

#### 記述例

- TOE が保護する資産は、TOE 利用者によって作成されたデータベースである。データベースは分散環境でも一元的に利用できるように、ネットワーク上を転送されることがある。
- 脅威

#### T.ACCESS

TOE の利用許可者（注：脅威エージェント）がデータベース所有者の許可を得ないで、SQL を使用して（注：攻撃方法）データベース（注：保護資産）にアクセス（注：脅威）する。

#### T.NETWORK

LAN 利用者（注：脅威エージェント）がプロトコルアナライザーを使用（注：攻撃方法）して、LAN 上を転送されているデータ（注：保護資産）を盗聴（注：脅威）する。

#### T.ADMIN

一般の TOE 利用者（注：脅威エージェント）が管理者のパスワードを推測（注：攻撃方法）し、管理者に成り代わってデータベースのアクセス権限リストを改ざん（注：攻撃方法）し、非許可者でもデータベース（注：保護資産）にアクセス（注：脅威）できるようにする。

### 3.3 組織のセキュリティ方針

#### 【参考規格類】

TOE または TOE が使用される環境を管理する組織によって規定された、その環境が従わなければならない規則、実践またはガイドラインを規定すること。

（ASE\_ENV.1-3）

組織のセキュリティ方針の例は、政府によって規定されている標準に従うためのパスワード生成及び暗号化要件などがある。

各組織のセキュリティ方針が明確に理解できるように、十分に詳細な説明及び/または解釈を記載する。

TOE のセキュリティ対策方針及び環境が前提条件及び脅威からのみ派生するものである場合、組織のセキュリティ方針をST に提示する必要はない。

#### 【ガイダンス】

脅威及び前提条件の変形による繰り返し記述は不要である。

一般的には、TOE が特定の環境（組織など）で利用されることを意図している、あるいは、脅威からは導出されないセキュリティ要求を TOE が実装する必要がある場合には、この組織のセキュリティ方針で規定する。

TOE がセキュリティ製品で、そのセキュリティ機能を TOE に含めたいが、脅威からは導出できない（脅威から導出しようとするとな煩雑になる）場合には、そのセキュリティ機能の提供を組織のセキュリティ方針として規定することによって、TOE のセキュリティ機能に含めることができる。

ただし、脅威に対抗することが明白なセキュリティ機能に対して、脅威ではなく組織

のセキュリティ方針で規定することは、TOE のセキュリティ機能を正確に理解する上で妨げになるため、避けること。

記述例

- ・ P.PRIVACY  
個人情報が保管されている xx データベースに対して、「個人情報の保護に関する法律（平成 15 年法律第 57 号）」に規程されている管理を適用する。
- ・ P.ACCESS  
指定のデータへのアクセスは下記の場合に制限する。  
データの所有者  
所有者が許可した利用者
- ・ P.AUDIT  
セキュリティ監査に関する XX 規則を適用する。XX 規則の中で、監査すべき事象を正確に規定する。監査者は監査データの監査を 1 ヶ月ごとに実施する。
- ・ P.SECREQ  
XX セキュリティ機能を実装する。

悪い例：

- ・ 「XX 技術標準を適用する。」  
これだけでは XX 技術標準のどの部分が TOE に関連するのかが不明であり、この規定が、セキュリティ対策方針に結びつかない。具体的な要求事項を規定しなければならない。
- ・ 「顧客データの不正利用に対処するために、適切なセキュリティ機能を装備する。」この例では下記の 2 つの問題がある。  
問題 1：本項はセキュリティに係わる要求事項を規定する。このため、規定内容は具体的でなければならない。この事例の、“適切なセキュリティ機能”だけでは、どのようなセキュリティ機能が要求されているのか把握できない。  
問題 2：“不正利用”という脅威に対する対抗としてのセキュリティ機能を要求しているのであるから、脅威の項に規定すべきである。脅威の項に、脅威エージェント、攻撃方法、保護資産、攻撃力などを規定することにより、要求されるセキュリティが正確に規定できる。

## 4 . セキュリティ対策方針

### 【参考規格類】

「3 . TOE セキュリティ環境」の分析結果は、脅威に対抗するためのセキュリティ対策方針の策定、並びに組織のセキュリティ方針及び使用上の前提条件を実現するためのセキュリティ対策方針の検討に使用する。(CC)

セキュリティ対策方針は、規定された運用目的又は TOE の製品目的が、その物理的環境についての認識と矛盾しないものであること。

セキュリティ対策方針を決定する目的は、セキュリティ上の問題をすべて検討すること及び TOE 又はその環境によってどのようなセキュリティが直接提供されるのかを明らかにすることにある。これは、技術的判断、セキュリティ方針、経済的要因及びリスクの受入れ判断を取り込んだ過程に基づく。

環境に対するセキュリティ対策方針は、IT の領域において、及び非技術的又は手続上の手段によって実現される。

TOE セキュリティ環境で規定したセキュリティ要求仕様への対応を簡潔に表現する。

(CC)

簡潔；

- 実装レベルの記述は不要(いかなる手段によって実現するかを記載する。その手段の実装方法の詳細を記述する必要は無い。)
- TOE セキュリティ環境における規定(脅威や組織のセキュリティ方針)の繰り返しは無用

セキュリティ対策方針が、TOE、あるいは、環境、またはその両方に適用するものであることが判断できるように明記すること。(ASE\_OBJ.1-1)

セキュリティ対策方針はすべての識別された脅威に対抗するために十分であり、すべての識別された組織のセキュリティ方針及び前提条件を満足するものであること。

(ASE\_OBJ.1-8)

これは、セキュリティ対策方針根拠でも説明される。

脅威または組織のセキュリティ方針が TOE で部分的に、またその環境で部分的にカバーされる場合、関連する対策方針を TOE および環境ごとに記述しなければならない。

### 【ガイダンス】

TOE または環境のどちらで対応するかは、対象資産の価値、実装コスト、利便性、市場の要請、実現可能性などに依存する。

例：TOE と環境の棲み分け

TOE では監査用ログデータの採取と記録をセキュリティ対策方針とし、環境では監査ログデータの解析をセキュリティ対策方針とする。

脅威又は組織のセキュリティ方針が TOE で一部、その環境で一部対処される場合は、関連する対策方針を、TOE のセキュリティ対策方針の項と、環境のセキュリティ対策方針の項とに分けて記述する。

TOE 及びその環境のセキュリティ対策方針を簡潔に定義しなければならない。対策は何かと、その目的を記載する。対策をどのように実現するかについての詳細な記載は不要。同時に、脅威に「対抗する」とか、組織のセキュリティ方針を「実現する」とか、「セキュアに管理する」、「適切に管理する」、「正しく管理する」、などの記載では、対策が何であるかが不明であるため、不十分である。セキュリティ対策方針の規定は、3章で記載した、脅威に対抗できる、あるいは、前提や組織のセキュリティ方針を満足させることができることが理解できる内容でなければならない。

#### 4.1 TOE のセキュリティ対策方針

##### 【参考規格類】

TOE の各セキュリティ対策方針は最低でも1 つのTOEが対抗すべきと識別された脅威及び/又はTOEが満たすべき組織のセキュリティ方針にまでさかのぼれること。

( ASE\_OBJ.1-2 )

脅威に対抗するセキュリティ対策方針は、そのセキュリティ対策方針が実施された場合、脅威が取り除かれ、脅威が受入れ可能なレベルに軽減されるか、または脅威の影響が十分に緩和されることを実証すること。( ASE\_OBJ.1-4 )

脅威の除去の例は、次のとおりである。

- エージェントから攻撃方法を使用する能力を除去する。
- 抑止によって脅威エージェントの動機を除去する。
- 脅威エージェントを除去する。(例えば、頻繁にネットワークをクラッシュさせるマシンをネットワークから取り外す。)

脅威の軽減の例は、次のとおりである。

- 脅威エージェントの攻撃方法を制限する。
- 脅威エージェントの機会を制限する。
- 行われた攻撃が成功する可能性を減少させる。
- 脅威エージェントに対してより多くの専門知識または資源を要求する。

脅威の影響の緩和の例は、次のとおりである。

- 資産のバックアップを頻繁に行う。
- TOE のコピーを取っておく。
- 通信セッションで使用されるキーを頻繁に変更し、1 つのキーが破られた場合の影響を相対的に少なくする。

##### 【ガイダンス】

セキュリティ対策方針と脅威及び組織のセキュリティ方針との対応については根拠の項で記載するが、本項でもこの対応関係を明確に記載しておけば、読者の理解を助けるのに役立つ。

一般的に、セキュリティ対策方針として、予防対策（脅威の影響を阻止または軽減する）、検出対策（セキュリティ問題の発生を検出または監視）、復旧対策（セキュアな状態への復旧）がある。TOEのセキュリティ対策は、導入や運用コスト面で、保護対象資産の価値に見合うものにする。

記述例

O.ACCESS

データベースへのアクセスは所有者および、所有者が許可した利用者のみを可能にする。

O.AUTHENTICATE

TOEへのアクセス時には、利用者を一意に識別し、本人の確認を行う。

O.AUDIT

資産の利用に関わる記録を採取し、記録する。

#### 4.2 環境のセキュリティ対策方針

##### 【参考規格類】

環境のセキュリティ対策方針は、TOEセキュリティ環境における前提条件の記述の全部又は一部を再掲してもよい。(CC)

環境の各セキュリティ対策方針が最低でも1つのTOEが完全には対抗できない識別された脅威及び/又はTOEが完全に満たしていない組織のセキュリティ方針又は前提条件にまでさかのぼれること。(ASE\_OBJ.1-3)

##### 【ガイダンス】

環境のセキュリティ対策は、TOE利用者に不当な制限を与えたり、実施が困難なものであってはならない。

環境のセキュリティ対策方針は、IT環境または管理・手続きによる対策などの非IT対策を含む。

記述例

OE.PASSWORD

利用者がパスワードを秘密に保持できるように、その管理手続きを規定する。

OE.EDUCATE

業務担当者がアクセスしたデータを不当に扱わないように、従業員規則にその旨を規程し、教育を行う。

OE.SROOM

TOE の処理に関わる情報機器を入退出が管理された部屋に設置する。

OE.USER

TOE の動作の前提となる OS により利用者の識別と認証を行う。

## 8.1 セキュリティ対策方針根拠

### 【参考規格類】

記述されたセキュリティ対策方針が、TOE セキュリティ環境において識別されたすべてについて追跡することができ、かつ、それらを満足するのに適していることを説明しなければならない。(CC)

TOE のすべてのセキュリティ対策方針が対抗されるべき識別された脅威、及び/または TOE が満たす必要がある組織のセキュリティ方針にまでさかのぼれることを検証すること。(ASE\_OBJ.1-2)

環境のセキュリティ対策方針が TOE 環境によって対抗されるべき識別された脅威、及び/または TOE 環境によって満たされるべき組織のセキュリティ方針、及び/または TOE の環境で満たされるべき前提条件にまでさかのぼれることを検証すること。

(ASE\_OBJ.1-3)

各脅威に対して、セキュリティ対策方針がその脅威に対抗するために適していることを示す適切な正当化を、セキュリティ対策方針根拠に含めること。(ASE\_OBJ.1-4)

セキュリティ対策方針が脅威にまでさかのぼれなければならない。脅威に対する正当化が、脅威にまでさかのぼるすべてのセキュリティ対策方針が達成された場合、脅威が取り除かれるか、脅威が受入れ可能なレベルに軽減されるか、または脅威の影響が十分に緩和されることを実証すること。

脅威にまでさかのぼる各セキュリティ対策方針が達成されると、実際に脅威の除去、軽減または緩和に寄与すること。

各組織のセキュリティ方針に対して、セキュリティ対策方針がその組織のセキュリティ方針をカバーするのに適していることを示す適切な正当化を、セキュリティ対策方針根拠に含めること。(ASE\_OBJ.1-5)

セキュリティ対策方針が組織のセキュリティ方針にまでさかのぼれなければならない。組織のセキュリティ方針が、組織のセキュリティ方針にまでさかのぼるすべてのセキュリティ対策方針が達成された場合、組織のセキュリティ方針が実装されることを実証すること。

組織のセキュリティ方針にまでさかのぼる各セキュリティ対策方針が達成されると、実際に組織のセキュリティ方針の実装に寄与すること。

各前提条件に対して、環境に対するセキュリティ対策方針がその前提条件をカバーするのに適していることを示す適切な正当化を、セキュリティ対策方針根拠に含めること。(ASE\_OBJ.1-6)

環境に対するセキュリティ対策方針が前提条件にまでたどれなければならない。

TOE の意図する使用法について、その前提条件にまでさかのぼる環境に対するすべてのセキュリティ対策方針が達成された場合、意図する使用法がサポートされることを実証すること。

TOE の使用環境について、その前提条件にまでさかのぼる環境に対するすべてのセキュリティ対策方針が達成された場合、意図する使用環境が達成されることを実証すること。

セキュリティ対策方針が TOE セキュリティ環境に対して十分であり、かつ、必要であることを示すこと。(ASE\_OBJ.1-8)

### 【ガイダンス】

セキュリティ対策方針と TOE セキュリティ環境（脅威、前提、組織のセキュリティ方針）との対応表を作成する。各セキュリティ対策方針は少なくとも一つの TOE セキュリティ環境と対応を持つ。各 TOE セキュリティ環境は少なくとも一つの各セキュリティ対策方針によって実現される。この検証により、不必要なセキュリティ対策方針は含まれていないことが確認できる。

この場合、脅威・前提条件・組織のセキュリティ方針とセキュリティ対策方針との対応表を記載するだけでなく、それによって何を説明しているのかを記載する。

セキュリティ対策方針が十分であることを示すために、

- 各脅威に対して、セキュリティ対策方針が有効な対策（脅威の項で示した事項に対して、脅威が取り除かれるか、脅威が受入れ可能なレベルに軽減されるか、または脅威の影響が十分に緩和される、検出 / 回復 / 軽減 / 予防が可能）となることを、また、
- 各前提、組織のセキュリティ方針に対して、セキュリティ対策方針がその要求を実現（実装）できることを、

説明する。

各脅威・前提条件・組織のセキュリティ方針ごとに、関連するセキュリティ対策方針によって、その脅威・前提条件・組織のセキュリティ方針に対抗、または、対応できることを説明する。

記述例

セキュリティ対策方針の必要性について

各セキュリティ対策方針は、必ず、TOE セキュリティ環境（脅威、組織のセキュリティ方針）に対応しており、対応しないセキュリティ対策方針は存在しないことを下記の表で示す。

セキュリティ環境 セキュリティ対策方針	T.P_Probe	T.Forcd_Rst	T.Reuse	T.Brute-Force	T.Link	T.Inv_Inp	T.Access	T.P_Load	T.Sec_Com	T.LC_Ftn	T.I_Leak	T.Env_Strs	P.Crypt_Std	A.Data_Store	A.Key_Supp	A.Priv	A.Shipping_System
<b>TOE</b>																	
O.Phys Prot																	
O.Init																	
O.Reuse																	
O.Brute-Force																	
O.Unlink																	
O.Log Prot																	
O.I&A																	
O.DAC																	
O.P Load																	
O.Sec Com																	
O.Life Cycle																	
O.I Leak																	
O.Env Strs																	
O.Crypt Std																	
<b>TOE環境</b>																	
OE.CAD Sec Com																	
OE.Data Store																	
OE.Key Supp																	
OE.Priv																	
OE.Shipping System																	
OE.Secure AP																	

セキュリティ対策方針の十分性について

脅威に対するセキュリティ対策方針の十分性

**T.Reuse** (攻撃者は、利用者の認証処理を行っている最中の IC カードとカード端末間の通信データ (認証データ) を入手し、それを再利用して認証に成功することにより、IC カードを不正使用する。):

**O.Reuse** によって、認証処理中の認証データを暗号化することにより、認証データの暴露を防止することができる。認証処理毎に生成される公開鍵・秘密鍵ペアを用いた暗号化を行うことにより、過去の認証処理で使用された暗号化された認証データの再利用を防止することができる。

## 5 . IT セキュリティ要件

### 【参考規格類】

IT セキュリティ要件は、セキュリティ対策方針を、TOE に対する一連のセキュリティ要件及び環境に対するセキュリティ要件に詳細化したものである。(CC)

機能要件及び保証要件に分けてセキュリティ要件を提示する。

TOE が確率的又は順列的な機構によって実現されるセキュリティ機能（例えば、パスワード及びハッシュ関数）を含む場合、保証要件は、セキュリティ対策方針に整合する最小限の強度レベルを要求するように規定してもよい。この場合、規定するレベルは、SOF-基本、SOF-中位、又はSOF-高位のいずれかとなる。このような機能は、それぞれ最小限のレベル又は少なくとも任意に定義された特定の値を満たさなければならない。

保証の程度は、一連の機能要件ごとに異なる可能性がある。したがって、保証の程度は、通常、保証コンポーネントの組み合わせで決まる厳密さのレベルによって表現される。

セキュリティ対策方針が、選択されたセキュリティ機能によって達成される保証は、次の二つの要因から導出される。

- a) セキュリティ機能の実装の正確さに対する信頼性。すなわち、セキュリティ機能が正しく実装されているかどうかの評定。
- b) セキュリティ機能の有効性に対する信頼性。すなわち、セキュリティ機能が実際に規定したセキュリティ対策方針を満たしているかどうかの評定。

一般的に、セキュリティ要件は、要求された振る舞いが存在するという要件及び要求されていない振る舞いが存在しないという要件を共に含む。

TOE のセキュリティ要件は、次に示す情報を基に構築することができる。(CC)

- a) 既存の PP：ST に含める TOE のセキュリティ要件は、既存の PP に含まれている要件を用いて適切に表現してもよいし、又はこれらの要件に完全に適合するように意図してもよい。
- b) 既存のパッケージ：ST に含める TOE セキュリティ要件の一部は、使用できるパッケージ内で既に表現されていてもよい。  
一連の既定のパッケージは、CC パート 3 で定義する EAL とする。PP 又は ST に含める TOE の保証要件として、パート 3 の EAL を記述することが望ましい。
- c) 既存の機能要件コンポーネント又は保証要件コンポーネント：ST に含める  
TOE の機能要件又は保証要件は、CC パート 2 又はパート 3 に含まれているコンポーネントを用いて直接表現してもよい。
- d) 拡張要件：ST においては、パート 2 に含まれていない機能要件及び / 又はパート

3に含まれていない保証要件を追加して用いてもよい。

利用できるならば、CC パート2及びパート3の既存の要件を用いることが望ましい。既存のPPを用いることによって、TOEが周知の有用性の要求を満たしていることを容易に保証することができ、したがって、そのTOEがより広く認められる。

次の共通条件は、TOE及びそのIT環境に対するセキュリティ機能要件及びセキュリティ保証要件の表現に等しく適用しなければならない。(CC)

- 1) 適用可能ならば、すべてのITセキュリティ要件は、CCパート2又はパート3の該当するセキュリティ要件コンポーネントを参照して記述するのがよい。そのセキュリティ要件の全部又は一部に、直ちに適用できるパート2又はパート3の要件コンポーネントがない場合、STは、CCを参照せずに、それらの要件を明示的に記述してもよい。
- 2) 明示的に記述するTOEセキュリティ機能要件又はTOEセキュリティ保証要件は、満足していることの評価及び説明ができるように明確で、かつ、あいまいさなく表現しなければならない。その表現の詳細度及び方法は、既存のCC機能要件又はCC保証要件をモデルとして用いなければならない。
- 3) 要求された操作は、セキュリティ対策方針が満たされていることを説明するのに必要な詳細度で表現しなければならない。すべての要件コンポーネントに指定された操作については、具体的に規定しなければならない。
- 4) ITセキュリティ要件間のすべての依存性は、満たすことが望ましい。依存性は、関係が深い要件をTOEセキュリティ要件に含めるか又は環境に対する要件として規定してもよい。

CCのコンポーネントは、CCに定義されているとおりに用いてもよいし、特定のセキュリティ方針を満たし、又は特定の脅威に対抗するために、許容される操作を行って修整してもよい。(CC)

CC機能及び保証コンポーネントは、CCに定義されているとおりに用いてもよいし、セキュリティ対策方針を満たすために許可された操作の使用を通して修整することもできる。コンポーネント内のエレメントに詳細化を施す場合には、そのような詳細化がなされたことを明確に識別しなければならない。また、この要件に依存する他の要件への依存性の必要性が満たされていることにも注意しなければならない。許可された操作は、以下のとおりである。

繰返し：種々の操作で2回以上コンポーネントを使用する。

割付：パラメタを特定する。

選択：リストから、一つあるいはそれ以上の項目を選択する。

詳細化：詳細を追加する。

STではすべての操作を完成しなければならない。

ITセキュリティ要件におけるすべての操作が識別(活字印刷上の区別、周辺の文章内

での明示的な識別、またはその他の特徴的な手段による) されていること。  
( ASE\_REQ.1-10 )

CCパート2 およびパート3 コンポーネントに許可されている操作は、割付、繰返し、選択、及び詳細化である。割付及び選択操作は、コンポーネント内で特に示されている場合のみ許可される。繰返し及び詳細化は、すべてのコンポーネントに対して許可されている。

すべてのコンポーネント内でのすべての割付及び選択を完全に決定(コンポーネント内で行う選択が残っていない) すること。( ASE\_REQ.1-11 )

完全に決定できない場合には、その理由を明記する。操作が完全に決定できない例には、FTA\_MCS.1 (複数同時セッションの基本制限) で同じ利用者に属する同時セッションの数に対する割付操作を実行するとき値の範囲を特定することがある。これに対する適切な正当化は、TOE 設置時に管理者によって値が特定範囲内の値から選択されることである。

すべての操作に関して、下記を満足すること。( ASE\_REQ.1-12 )

- a) 割付の場合、選択されたパラメタまたは変数の値が、割付で要求される指定された型に従っている。
- b) 選択の場合、選択された要素(複数可) がエレメントの選択部分内で指定された1 つまたは複数の要素であること。選択された要素の数が要件に適切であること。
- c) 詳細化の場合、コンポーネントは、詳細化された要件を満たすTOE が詳細化されていない要件も満たすような方法で詳細化されること。詳細化された要件がこの境界を越えた場合、拡張要件とみなされる。詳細化は明確に識別できること。  
例：ADV\_SPM.1.2C TSP モデルは、モデル化が可能なTSP のすべての方針の規則及び特性を記述しなければならない。  
詳細化：TSP モデルは、アクセス制御のみを扱う必要がある。
- d) 繰返しの場合、コンポーネントの各繰返しがそのコンポーネントの別の繰返しとはそれぞれ異なること(最低でもコンポーネントの1 つのエレメントが別のコンポーネントの対応するエレメントと異なっていること)、またはコンポーネントがTOE の異なる部分に適用されること。

IT セキュリティ要件ステートメントで使用されるコンポーネントに要求される依存性を満足すること。( ASE\_REQ.1-13 )

依存性は、適切なコンポーネント(またはそれに対して上位階層のコンポーネント) がTOE セキュリティ要件のステートメントに含められることにより、またはTOE のIT 環境によって満たされていると主張される要件として、満たすことができる。CC が依存性を含めることによって依存性分析のサポートを提供していても、これはその他の依存性が存在しない正当化ではない。その他の依存性の例には、「すべてのオブ

ジェクト」または「すべてのサブジェクト」を参照するエレメントがある。

この場合、依存性はオブジェクトまたはサブジェクトが列挙される別のエレメントまたはエレメントのセット内の詳細化で存在可能である。

IT 環境内で必要なセキュリティ要件の依存性は、ST に記述し、満足すべきである。CCで指定されている依存性を満足する必要が無い場合は、その理由を明確に説明すること。(ASE\_REQ.1-14)

例えば、TOE がセキュリティ対策方針として「失敗した認証は利用者の識別情報及び日時とともにログに記録しなければならない」を規定し、FAU\_GEN.1( 監査データ生成 ) をこのセキュリティ対策方針を満たす機能要件として使用する場合を想定する。この場合、FAU\_GEN.1 は、FPT\_STM.1( 高信頼タイムスタンプ ) への依存性を含む。しかし、TOE が時計メカニズムを含んでいないため、FPT\_STM.1はST 作成者によってIT 環境の要件として定義される。ST 作成者は、以下の正当化によって、この要件が満たさないことを示すことができる。「この特定の環境においてタイムスタンプメカニズムに対する攻撃が可能であるため、環境は高信頼タイプスタンプを提供できない。ただし、脅威エージェントの中には、タイプスタンプメカニズムに対して攻撃を実行できないものもあり、これらの脅威エージェントによるいくつかの攻撃は、攻撃の日時をログに記録することによって分析することができる。」

IT セキュリティ要件のステートメントは完全であること。(ASE\_REQ.1-25)

セキュリティ要件のステートメントは、要件に対するすべての操作が完了し、セキュリティ要件がTOE のすべてのセキュリティ対策方針が満たされていることを保証するのに十分でなければならない。

IT セキュリティ要件のステートメントは内部的に一貫していること。

(ASE\_REQ.1-26)

セキュリティ要件がほかのセキュリティ要件と競合し、セキュリティ対策方針が満たされなくなるといふことが発生しない場合、内部的に一貫している。

## 【ガイダンス】

セキュリティ要件の規定は、TOE のセキュリティ機能を TOE の利用者やセキュリティ評価の関連者が正確に理解することを目的にしたものである。したがって、割付などの操作は、誤解を招くことなく、理解しやすく、具体的かつ正確に規定することが要求される。

例：

・TSF は、[割付：AA]・・・[割付：BB]・・・

割付：aa

割付：bb

上記の表現では、対応が不明瞭になる危険性があるので、

AA=aa, BB=bb

と記載する。

セキュリティ機能要件は、クラス ファミリー コンポーネント エレメントからなる階層構造で構成されている。TOE 又はその環境によって満たさなければならないITセキュリティ要件を、コンポーネントを用いて定義する。

定義に際して、内容の理解を容易にすることが重要である。このために、要件の名前やエレメント名に、必ずしも、CC 規定のものを使用する必要は無い(添付として対応表を載せておけばいい)。ST として理解しやすい命名方法を採用することができる。

## 5.1 TOE セキュリティ要件

### 5.1.1 TOE セキュリティ機能要件

#### 【参考規格類】

同じ要件を異なる場合に使用する必要があるとき(例えば、2種類以上の使用者の識別)は、CC パート2の同じコンポーネントの繰返し利用(例えば、繰返し操作の適用)が可能である。(CC)

TOE セキュリティ機能要件のステートメントはCC パート2 機能要件コンポーネントから抽出し、個別のコンポーネントの参照、またはST が適合を主張するPP 内の個別のコンポーネントの参照、あるいは、内容の複写によって識別すること。

(ASE\_REQ.1-1)

CCパート2 のTOE セキュリティ機能要件コンポーネントを参照する場合は、参照したコンポーネントがCC パート2 に存在すること。PP 内のTOE セキュリティ機能要件コンポーネントを参照する場合、参照したコンポーネントがそのPP に存在すること。

(ASE\_REQ.1-2)

パート2 から抽出した各TOE セキュリティ機能要件コンポーネントは正しく記載すること。(ASE\_REQ.1-3)

TOE セキュリティ保証要件にAVA\_SOF.1 が含まれている場合、TOE セキュリティ機能要件に対する最小機能強度レベルのステートメントを含み、このレベルがSOF-基本、SOF-中位またはSOF-高位のいずれかであること。(ASE\_REQ.1-15)

TOE セキュリティ機能要件には確率的または順列的な機構(例えば、ハッシュ関数、パスワードなど)によって実現されるTOE セキュリティ機能の最小機能強度レベルを記述すること。暗号化アルゴリズムの強度は、CC の適用範囲外である。機能強度は、非暗号である確率的または順列的メカニズムにのみ適用する。したがって、ST が最小限のSOF 主張を含む場合、この主張はCC 評価に関連する暗号メカニズムにも適用しない。そのような暗号メカニズムがTOE に含まれる場合、アルゴリズム強度は機能強度に適用されないことを明言すること。

各ドメインに対して最小機能強度レベルを持つ方がTOE 全体に対して1 つの包括的な最小機能強度レベルを持つよりも適切である場合、TOEを複数の別々のドメインに分割できる。この場合、TOE セキュリティ機能要件を別々のセットに分け、それぞれのセットに関連する機能レベルに異なる最低強度を持たせることができる。この例としては、公の場所にある利用者端末、及び物理的にセキュアな場所にある管理者端末を持つ分散端末システムがある。この場合、TOE を利用者ドメインと管理者ドメインに分けてTOEセキュリティ機能要件をそれらのドメインに属するセットに分割し、最低強度のSOF-基本の機能レベルを管理者ドメインに属するセットに割り付け、最小機能強度のSOF-中位の機能レベルを利用者ドメインに属するセットに割り付ける。

TOE セキュリティ保証要件にAVA\_SOF.1 が含まれている場合、明示された機能強度が適用される全てのTOE セキュリティ機能要件を、特定の機能強度または数値尺度とともに識別すること。(ASE\_REQ.1-16)

明示された機能強度主張は、SOF-基本、SOF-中位、SOF-高位、または定義された特定の数値尺度のいずれかになる。特定の数値尺度を使用する場合は、これらが特定された機能要件のタイプに適切であること、及び特定された数値尺度が強度主張として測定可能であること。

## 【ガイダンス】

### 要件定義

機能要件の定義に際しては、CC パート 2 の附属書 (規格) に各セキュリティ機能要件の適用上の注釈や操作について規定されている。

例：

FDP\_IFF.1.1 TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: 情報フロー制御SFP]を実施しなければならない：  
[ 割付:セキュリティ属性の最小数及び種別]。

セキュリティ属性の最小数について附属書には、下記の説明がある。

「FDP\_IFF.1.1 において、PP/ST 作成者は、その機能が規則を特定するために使用するセキュリティ属性の最少数と種別を特定すべきである。例えば、そのような属性には、サブジェクト識別子、サブジェクトの機密(sensitivity) レベル、サブジェクトの取扱許可(clearance) レベル、情報の機密レベルなどがある。セキュリティ属性の各種別の最少数は、適用する環境の要求を満たすために十分な数でなければならない。」

機能要件の定義に際しては、セキュリティ対策方針を実現するために必要な機能要件と、これらの機能要件を支援するための機能要件の 2 種類を考慮 (ST の記載でこれらを明示的に区別する必要はないが、機能要件の定義手順において考慮) しなければならない。

らない。

支援のための機能要件には；

- ・セキュリティ対策方針を実現する機能要件に対して、依存性を持つ機能要件として指定されているもの、ならびに、関連する機能要件（例：FAU\_GEN.1（監査データの生成）が規定されている場合には、監査データを TOE 外で処理するのでなければ、FAU\_STG（セキュリティ監査事象格納）ファミリや FAU\_SAR（セキュリティ監査レビュー）も関連機能として必要になる。なお、FAU\_GEN.1 で指定の直接の依存性は FPT\_STM.1（高信頼タイムスタンプ）のみである。）
- ・セキュリティ機能への攻撃に対抗するためのもの（当該セキュリティ機能のセキュアな動作保証や干渉からの保護、TSF データの機密性、完全性や可用性確保、当該セキュリティ機能の管理 FMT FMT\_REV.1 などがある）
- ・上記 2 つの機能要件の依存性を持つ機能要件として指定されているもの、

がある。これらの支援のための機能要件も、セキュリティ対策方針を遂行する上で必要が無い場合には指定しない。

セキュリティ機能の保護のための要件（上記の 2 番目の支援機能要件）

セキュリティ機能に対する攻撃から保護するための機能要件を考慮しなければならない。

- ・セキュリティ機能のバイパス防止

FPT\_RVM.1(Non-bypassability of the TSP)で対応する。アクセス管理要件に対しては識別認証はバイパス防止機能と考えられる。

- ・セキュリティ機能への干渉阻止

FPT\_SEP(Domain separation) 不当な干渉を阻止

FPT\_PHP(TSF Physical Protection) 物理的な干渉の検出や防止

FMT\_MSA.1(Management of Security Attribute) セキュリティ属性の改ざんの抑止

FMT\_MTD.1(Management of TSF data), FAU\_STG.1(Protected Audit Trail Storage), FPT\_AMT.1(Abstract machine testing) セキュリティ関連データの安全性保証

FPT\_TRP(Trusted Path) 偽造 TSF による干渉（パスワードの盗聴など）阻止

- ・セキュリティ機能の動作不能防止

FAU\_STG(Security Audit Event Storage)ファミリには監査ログ用バッファがフルになった場合に監査機能が動作不能にならないことを要求する要件がある。

FMT\_MOF.1(Management of Security Functions Behaviour)の利用も有益である。

- ・セキュリティ機能の構成ミスの検出またはセキュリティ機能破壊のための攻撃の検出

監査機能、FDP\_SDI(Stored Data Integrity),FPT\_PHP(TSF Physical Protection)

など

操作（割付、選択、詳細化、繰り返し）

- ・ 繰り返しは、異なったコンポーネントでそれぞれ依存性が要求され、それぞれの場合を満足させるために、割付や選択内容が異なるとの理由でセキュリティ管理クラス FMT（例：FMT\_MSA.1）が使用される場合が多い。
- ・ 割付の場合はパラメタ値の指定が空のこともあり得る。  
しかし、選択の場合は、複数選択が可能である。パラメタを選択しなくてももいい場合や、一つだけ選択する場合には、その旨が選択のパラメタとして表示されている。（補足-0410）
- ・ 割付では記載する詳細レベルは、当該機能要件が対応するセキュリティ対策方針を実現する上で妥当であることが判断できる（説明できる）程度のもので、あいまいさが残らないものにする。
- ・ 詳細化では、セキュリティ対策方針を満足するために、エレメントの要求事項に対して、さらに詳細な条件を付加することによって実現手段を制限する。詳細化の内容は、元の要件の内容に矛盾してはならない。さらに、依存性を変更してはならない。

例 1：

エレメントの内容：TSF は、xx データの改変を検出する能力をもたなければならない。

詳細化： TSF は、チェックサムの確認によって、xx データの改変を検出する能力をもたなければならない。

例 2：

エレメントの内容：TSF はユーザのために TSF によって行われる他のアクションが実行される前に、各ユーザが認証に成功することを要求しなければならない。

詳細化：TSF はユーザのために TSF によって行われる他のアクションが実行される前に、各ユーザがバイオメトリクス照合装置を使用した認証に成功することを要求しなければならない。

監査要件

- ・ 監査に関わる要件が規定されている場合には、FAU\_GEN.1 の指定（最小：重要な行為や事象、基本：関連する全ての行為や事象、詳細：基本への追加、指定なし：FAU\_GEN.1.1 c で対象とする監査事象を個別に明示する）に基づいて、最小限の監査事象や最小限の監査記録情報を規定する。この規定は組織のセキュリティ方針、セキュリティ対策方針の実現における監査の役割や監査事象の関連性、オーバーヘッドへの影響などを考慮して妥当なものを選択する。記録しても監査の役に立たなかったり、分析ができないような事象や情報は規定しない。

なお、監査事象を個別に明示することを選択した場合には、必要な監査事象はすべてリストしておかなければならない。

監査事象や監査記録情報をテーブル形式で記載しておくとう理解しやすい。

例

機能要件	監査レベル	監査事象	監査記録情報
FCS_CKM.1	最小	動作の成功と失敗	TOE とデータベースサーバ間の SSL 通信における成功と失敗に係わる発生日時、利用者データ
FCS_CKM.4 (a)	最小	動作の成功と失敗	同上

#### 管理要件

- ・管理セクションで考慮すべき管理行為として規定している内容は、あくまでも、参考であり、必須要件ではない。(依存関係で規定してある管理要件は必須である。)
- ・管理しなければならない TSF データが存在する場合には、関連する管理要件の識別は必要である。
- ・セキュリティ属性を扱うセキュリティ機能要件が指定されている場合、そのセキュリティ属性を抹消するための管理要件 FMT\_REV.1 が必要になる。

#### サブジェクト、オブジェクトの定義

オブジェクト：TSF 範囲内の実体。情報を内蔵、包含又は受信し、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。(CC パート 1)

受動エンティティ(例えば、情報コンテナ)は、パート2セキュリティ機能要件ではオブジェクトと呼ばれる。オブジェクトは、サブジェクトが実行する操作の対象である。サブジェクト(能動エンティティ)が操作(例えば、プロセス間通信)の対象である場合、サブジェクトは、オブジェクトの働きもする。オブジェクトは、情報を含むことができる。この概念は、FDPクラスで記述されている情報フロー制御方針を指定するために必要となる。利用者、サブジェクト、情報及びオブジェクトは、TOEが正しくふるまうことができるようにする情報が含まれるある種の属性を所有する。(以上、CCパート2)

実際に管理の対象となる単位を規定する。

#### 【事例】

通常、データは操作(アクセス管理など)の実施単位にはならない。ファイルやテーブルがオブジェクトである。

サブジェクト：実行すべき操作を行う原因となる TSF 制御範囲内の実体エンティティ。所定のタスクを実行するために、あるサブジェクトが利用者によって存在を与えられるか起動されて、その利用者の代わりとなって動作する。

能動的なエンティティはサブジェクトと呼ばれる。TOEには、次に示すようないくつかのタイプのサブジェクトが存在する可能性がある。

- a) 許可利用者を代行して働く、TSPのすべての規則に従うサブジェクト(例えば、プロセス)
- b) 複数の利用者を代行してアクションを行う、特定の機能プロセスの働きをするサブジェクト(例えば、クライアント/サーバアーキテクチャに見られる機能)
- c) TOE自体の一部として働くサブジェクト(例えば、高信頼プロセス)

(以上、CCパート2)

パート2の説明においても、「受信の証拠の確認を要求するサブジェクト(例: 受信者や、調停者などの第三者)」、「サブジェクト(利用者またはアプリケーションを表している)」などのように、利用者もサブジェクトに含めるような表現を用いている箇所があり、情報フロー制御のサブジェクトについては、一般的な意味でのサブジェクトを含むと解説されているなど、必ずしも一貫した定義がなされていない。要件の内容にしたがって、正確にサブジェクトを定義しなければならない。アクセス制御要件で使用するサブジェクトはTOE内のエンティティを示し、TOE外のユーザはサブジェクトにはできない。

利用者データ、TSFデータの定義

TOEのデータは、利用者データまたはTSFデータのいずれかに分類される。

利用者データ：TSPに従って利用者が操作し、TSFに対して特別の意味を持たない、TOE資源に蓄積される情報である。例えば、電子メールメッセージの内容は、利用者データである。

TSFデータ：TOEの動作のために使用されるデータ。TSPの決定を行うときに、TSFが使用する情報である。セキュリティ属性(利用者属性、オブジェクト属性、サブジェクト属性、情報属性)、認証データ及びアクセス制御リストエントリは、TSFデータの例である。

事例：アクセス制御について；

TOE内のサブジェクトとオブジェクトに対して、それぞれのセキュリティ属性に従って、どのような操作が許されるかを規定する。利用者データに対して適用するものであり、TSFデータに適用するものではない。

FDP\_ACF.1.1：サブジェクト、オブジェクトのアクセス制御に関わるセキュリティ属性を規定する。

FDP\_ACF.1.2：操作に関わる規則を規定する。FDP\_ACF.1.1で規定したセキュリティ属性を使用する。

記述例：

**FDP\_ACF.1.1** TSFは、以下の[割付: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ

属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 SFP]を実施しなければならない。

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]: **表に示すサブジェクト、オブジェクト、セキュリティ属性に分けられたグループ**

[割付: アクセス制御SFP]: **JISEC ICカードアクセス制御方針**

セキュリティ属性		オブジェクト											
		OS			本人確認アプリケーション				追加のアプリケーション				
カードのモード	ステータス	OS用DF	セキュリティ環境ファイル	鍵ファイル	アプリケーション用DF	セキュリティ環境ファイル	鍵ファイル	情報ファイル	アプリケーション用DF	セキュリティ環境ファイル	鍵ファイル	情報ファイル	
サブジェクト	発行モード	状態-1	-	読出、書込、変更、削除	書込、変更、削除	-	読出、書込、変更、削除	書込、変更、削除	読出、書込、変更、削除	書込	読出、書込、変更、削除	書込、変更、削除	読出、書込、変更、削除
	通常利用モード	状態-2	-	-	-	-	-	読出	-	-	-	-	-
		状態-3	-	読出、書込、変更、削除	-	-	読出、書込、変更、削除	書込、変更、削除	読出、書込、変更、削除	書込、削除	読出、書込、変更、削除	書込、変更、削除	読出、書込、変更、削除
	ロックモード	状態-4	-	-	-	-	-	-	-	-	-	-	-
	クォーミネットモード	状態-4	-	-	-	-	-	-	-	-	-	-	-

・上表は、TOE のサブジェクト、セキュリティ属性、オブジェクト、操作の関係を示す。

・サブジェクトは、カードのモードとステータス(下に示す状態)で定義されたプロセスであり、オブジェクトに対して、操作を行う。

状態-1: 発行者認証鍵による認証が完了した後の状態。

状態-2: 暗証番号、及び端末認証鍵による認証が完了した後の状態。

状態-3: 暗証番号、端末認証鍵、及びアプリケーション利用鍵による認証が完了した後の状態。

状態-4: 暗証番号、端末認証鍵、及びアプリケーション利用鍵の一つ、または、いずれかの組み合わせによる認証が完了した後の状態。

[表の読み方の例] 発行モードで、状態-1(発行者認証鍵による認証が完了した後の状態)で定義されたサブジェクト(プロセス)は、OSのセキュリティ環境ファイルに対しては、読出、書込、変更、削除が可能である。

## 機能強度

- ・TOE セキュリティ保証要件に AVA\_SOF.1 が含まれている場合(例えば、EAL 2 以上)、TOE セキュリティ機能要件には、確率的又は順列的な機構(例えば、パスワード又はハッシュ関数)によって実現される、TOE セキュリティ機能の最小限の強度レベルを記述しなければならない。このような機能は、すべて、この最小限のレベルを満たさなければならない。このレベルは、SOF-基本(低レベルの攻撃力に対抗できる)、SOF-中位(中レベルの攻撃力に対抗できる)又はSOF-高位(高レベルの攻撃力に対抗できる)のいずれかでなければならない。レベルの選択は、識別された TOE のセキュリティ対策方針(対抗すべき攻撃力)に矛盾してはならない。

#### 記述例

本 TOE の機能強度は SOF-中位である。

- ・TOE の特定のセキュリティ対策方針を満たすために、選択した機能要件に対して SOF-基本/SOF-中位/SOF-高位という指定方法に代わって、特定の機能強度の測定方法を定義することもできる。
- ・機能強度レベルは脅威エージェントの攻撃力( TOE に対する知識、TOE へのアクセス、技術力、攻撃所要時間、ツールの装備などによって決まる )に基づいて決める。
- ・TOE セキュリティ機能強度の評価(AVA\_SOF.1)の一環として、個別の TOE セキュリティ機能に対して規定された強度主張及び全体として、最低限の強度レベルが TOE によって満たされているようにする。
- ・TOE セキュリティ機能要件に、確率的又は順列的な機構によって実現される TOE セキュリティ機能が存在しない場合には、下記のいずれかの記載を行う。
  - 最小機能強度は SOF-xx (これは想定 of 攻撃力により決まる) とする。ただし、該当する機能は存在しない。
  - 最小機能強度の指定に関わる機能は存在しない。

#### PP 適合時の指定

- ・PP の規定とは異なる機能要件のみを ST に規定することが望ましい。
- ・PP で不完全な操作が存在する場合には、ST では完全な操作を規定し、その箇所が判別できる(イタリック文字にするなどして)ようにしておく。
- ・PP で指定されていない機能要件を追加する場合には、追加の要件が既存の PP 指定要件と矛盾しないことを確認し、根拠の項で説明しなければならない。

#### 新規の規定

- ・CC で規定の形式、具体性レベル(各エレメントは単独で理解できる、要求事項の評価ができる、など)用語体系に合わせて、新規のコンポーネントを規定する。
- ・当該 ST のみで使用することを目的にしている場合には、要件の規定に操作を含める必要は無い。

#### セキュアなセキュリティ属性

##### FMT\_MSA.2 セキュアなセキュリティ属性

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

依存性として ADV\_SPM.1 非形式的TOEセキュリティ方針モデルが規定されている。

FMT\_MSA.2は、セキュリティ属性の妥当とみなされるすべての組み合わせがセキュアな状態の範囲内にあることを保証するのに使用できる。「セキュア」が何を意味するかの定義は、TOEのガイダンス文書及びTSPモデルに委ねられている。セキュアな値の明確な定義と、なぜそれらがセキュアと見なされるべきかの理由を開発者が提供すれば、

FMT\_MSA.2のADV\_SPM.1への依存性は、論証して取り除くことができる。(以上CC Part2)

FMT\_MSA.2.1ではセキュアな値を定義できない。ADV\_SPM.1に対応のポリシーモデルが提供できない場合は、STにセキュアな値の明確な定義と、なぜそれらがセキュアと見なされるべきかの理由を記載する。

事例：

FMT\_MSA.2が対象とするセキュリティ属性は、セッション確立時に生成される共通鍵の暗号方式や鍵長である。これらのセキュリティ属性は、暗号操作に必要なセキュリティ属性であるが、暗号操作では暗号化/復号化の操作のみであり、暗号する/しないとといったセキュリティに関する制御はない。

したがって、TOE のセキュリティ方針モデルを表現するセキュリティ保証要件 ADV\_SPM.1 は不要である。

コンポーネントの正確な再現

依存性や下位階層が指定されている場合には、それを省略しないで、正確に再現する。「適用上の注釈」などの名目で、要件の内容を補っても、規定としての意味は無い。

セキュリティに関わる管理機能

FMT\_SMR.1 はセキュリティに関わる管理機能の使用のための役割を識別するものである。利用者データへのアクセス権限はこの役割に該当するものではない。なお、役割が何をするかについては、FMT\_MOF,FMT\_MSA,FMT\_MTDなどで定義する。

事例：

FMT\_SMR.1 セキュリティ役割

FMT\_SMR.1.1

TSF は、役割[割付： 識別された役割]を維持しなければならない。

[割付： 識別された役割]

業務管理者

## 5.1.2 TOE セキュリティ保証要件

### 【参考規格類】

TOE セキュリティ保証要件の記述では、CC パート3の保証コンポーネントを用いて作成された EAL のうちから一つ選んで保証要件として記述するのがよい。ST では、また、パート3に規定していない保証要件を明確に記述して、EAL を拡張してもよい。(CC)

CC パート3 保証要件コンポーネントから抽出したすべてのTOE セキュリティ保証

要件コンポーネントは、EAL の参照、パート3 の個別のコンポーネントの参照、ST が適合を主張するPP の参照、あるいは、内容の複写によって識別すること。

(ASE\_REQ.1-4)

CC パート3 のTOE セキュリティ保証要件コンポーネントの各参照について、参照されたコンポーネントがCC パート3 に存在すること。PP 内のTOE セキュリティ保証要件コンポーネントの各参照について、参照されたコンポーネントがそのPP に存在すること。(ASE\_REQ.1-5)

パート3 から抽出した各TOE セキュリティ保証要件コンポーネントは正しく記載すること。(ASE\_REQ.1-6)

TOE セキュリティ保証要件のステートメントは、CC パート3 に定義されているEAL を含んでいるか、またはEAL を含んでいないことを適切に正当化すること。

(ASE\_REQ.1-7)

この正当化は、EAL を含めることが不可能、望ましくない、または不適切である理由について明記すること。

#### 【ガイダンス】

資産の価値、市場の要請、技術的な背景、保証のための所要コスト、想定される攻撃者の攻撃能力、隠れチャンネルへの懸念、開発環境への懸念、などが保証要件を決める要因となる。これらはセキュリティ対策方針として記載する。

セキュリティ対策方針での記載内容によって、必要な保証要件が決まる場合がある。

下記はその一例である。

(ア) “ TOE は高位レベルの攻撃力に対抗する ” AVA\_VLA.4

(イ) “ 隠れチャンネルへの対応が必要である ” AVA\_CCA

(ウ) “ 開発環境への配慮が必要である ” ALC\_DVS

保証パッケージに保証要件を追加する場合 (EAL<sub>n</sub> に保証コンポーネント を追加する) には、追加要件で指定されている保証コンポーネント に対して、依存性を持つコンポーネントも配慮しなければならない。

操作

- ・現在の CC 規定の保証コンポーネントには割付と選択は存在しない。
- ・繰り返しと詳細化 ( 特定の開発ツールや開発手法使用の要請、評価対象に含めるべきソースコード箇所の特定、明白な脆弱性として考慮すべき事象の識別などに利用される。) は指定可能である。TOE の異なった箇所に保証要件を指定する際に、異なった詳細化が必要になる場合に、繰り返しを使用する。

新規の規定

CC で規定の形式、具体性レベル ( 各エレメントは単独で理解できる、可能な限り客観的に評価ができる、など )、用語体系に合わせて、新規のコンポーネントを規定する。

### 保証パッケージ (EAL1~5) の考え方の例

EAL	主な評価対象物	想定する攻撃力	保証する内容
EAL1	機能仕様	公開の外部インタフェースを使用した攻撃 (例: 辞書攻撃、IPアドレススプーフィング)	公開の外部インタフェースを使用した攻撃によって利用される脆弱性は無い
EAL2	構造設計だが機能仕様の補完	全ての外部インタフェースを使用した攻撃 (例: DoS攻撃)	全ての外部インタフェースを使用した攻撃によって利用される脆弱性は無い
EAL3	構造設計	処理機能の不備を利用した攻撃 (例: リプレイアタック)	処理機能の不備を利用した攻撃によって利用される脆弱性は無い
EAL4	論理設計	処理論理の欠陥を利用した攻撃 (例: バッファオーバーフロー)	処理論理の欠陥を利用した攻撃によって利用される脆弱性は無い
EAL5	ソースコード	全ての処理論理の欠陥を利用した攻撃 (例: 隠れチャネル)	全ての処理論理の欠陥を利用した攻撃によって利用される脆弱性は無い

## 5.2 IT環境に対するセキュリティ要件

### 【参考規格類】

IT環境に対するセキュリティ要件が含まれている場合は、IT環境に対するセキュリティ要件を識別すること。(ASE\_REQ.1-9)

TOEがそのセキュリティ対策方針を達成するために、必要なセキュリティ機能をTOE以外のIT環境に依存する場合、そのIT環境に対するセキュリティ要件として明確に識別すること。

TOEがファイアウォールの場合、管理者の認証及び監査データの保存のために下層のオペレーティングシステムの機能を利用することがある。この場合、IT環境(下層のオペレーティングシステム)に対するセキュリティ要件にFAU及びFIAクラスからのコンポーネントが含まれる。

また、TOEが、定期的に自身のコードを検証して、コードが改ざんされた場合に自分自身を使用不可能にする機能を装備している場合、自身を回復するためには、IT環境に依存する必要がある。このため、IT環境の要件として、FPT\_RCV.2(自動回復)を持つ。FPT\_RCV.2の依存性の1つにAGD\_ADM.1(管理者ガイダンス)があるが、この保証要件は、IT環境の保証要件となる。

IT 環境のセキュリティ要件には機能要件及び保証要件の両方を含めることができる。

#### 【ガイダンス】

IT 環境に対するセキュリティ要件もパート 2 及びパート 3 のセキュリティ要件コンポーネントを参照し（拡張は除く）規定の操作を実施しなければならない。

非 IT 環境に対するセキュリティ要件は、実際には有用である場合が多いが、TOE の実装には直接関連しないことから、必ずしも、ST に記述する必要はない。しかし、非 IT 環境に対するセキュリティ要件の識別は、ガイダンス文書の記載内容を確認する上で有益であるため、特別の理由が無ければ、非 IT 環境に対するセキュリティ要件も記載することを勧める。

### 8.2 セキュリティ要件根拠

#### 【参考規格類】

一連のセキュリティ要件(TOE 及び環境)が、セキュリティ対策方針を満たすのに適し、かつ、セキュリティ対策方針を追跡できることを説明しなければならない。

下記の事項を説明しなければならない。(CC)

- ・ TOE の個々の機能要件コンポーネント及び保証要件コンポーネントと、その IT 環境との組合せが一体となって、記述されたセキュリティ対策方針を満たすこと。
- ・ 一連のセキュリティ要件が一体となって、互いに補完し、かつ、相互に矛盾しないこと。
- ・ セキュリティ要件の選択を正当化すること。次のいずれかの場合は、明確に正当化しなければならない。
  - パート 2 又はパート 3 に含まれない要件を選択した場合
  - EAL に含まれていない保証要件を選択した場合
  - 依存性を満足していない場合
- ・ ST において選択した機能強度のレベル及び明確に規定した機能強度の主張が、TOE のセキュリティ対策方針と矛盾していないこと。

TOE セキュリティ保証要件のステートメントが適切であることを、セキュリティ要件根拠で十分に正当化すること。(ASE\_REQ.1-8)

保証要件にEAL を含む場合、正当化は、そのEAL のすべての個々のコンポーネントを取り扱うというよりは、EAL 全体として取り扱うことができる。保証要件にそのEAL への追加コンポーネントを含む場合、各追加を個別に正当化すること。保証要件に明示された保証要件を含む場合、各々の明示された保証要件の使用を個別に正当化すること。セキュリティ要件根拠が、セキュリティ環境及びセキュリティ対策方針のステートメントを与えられた場合、保証要件が十分であることを十分に正当化すること。

例えば、知識のある攻撃者に対する防御が必要な場合、明白なセキュリティの弱点以外

を検出しないAVA\_VLA.1 を選択することは不適切である。

正当化には、以下のような理由も含まれる。

- a) ST が適合を主張するPP に示されている保証要件
- b) 制度、政府、またはその他の組織によって要求される特定要件
- c) TOE セキュリティ機能要件からの依存性として指定される保証要件
- d) TOE とともに使用されるシステム及び/または製品の保証要件
- e) 市場からの要求

各EAL の意図の概要及び目標は、CC パート3 の6.2 節に記述されている。

保証要件が適切であるかどうかの決定は主観的である。したがって正当化が十分であることの分析を過度に厳密に行う必要は無い。

TOE セキュリティ保証要件にAVA\_SOF.1 を含む場合、最小機能強度レベルが明示された機能強度主張とともにTOE のセキュリティ対策方針と一貫していることを、セキュリティ要件根拠で実証すること。(ASE\_REQ.1-17)

TOE セキュリティ環境のステートメントで記述されているように、攻撃者の持ちうる専門知識、資源、動機に関する詳細を考慮すること。例えば、TOE が高い攻撃能力を持っている攻撃者に対する防御を提供する必要がある場合、SOF-基本主張は不適切である。

セキュリティ対策方針の特定の強度関連特性を考慮すること。該当する場合には、対策方針に対する要件からの追跡を使用して、特定の強度関連特性を持つ対策方針に対応する機能要件が適切な機能強度の主張を持っていること。

TOE セキュリティ要件がTOE に対するセキュリティ対策方針にまでさかのぼれること。(ASE\_REQ.1-18)

それぞれのTOE セキュリティ機能要件がTOE に対する最低でも1 つのセキュリティ対策方針にまでさかのぼれること。

必須ではないが、いくつかまたはすべてのTOE セキュリティ保証要件がTOE のセキュリティ対策方針にまでさかのぼることもできる。

IT 環境に対するセキュリティ要件がその環境に対するセキュリティ対策方針にまでさかのぼれること。(ASE\_REQ.1-19)

IT 環境のそれぞれのセキュリティ機能要件がその環境に対する最低でも1 つのセキュリティ対策方針にまでさかのぼれること。

必須ではないが、いくつかまたはIT 環境のすべてのセキュリティ保証要件がその環境のセキュリティ対策方針にまでさかのぼることもできる。

TOE の各セキュリティ対策方針に対して、TOE セキュリティ要件が、そのTOEのセキュリティ対策方針を満たすのに適しているという適切な正当化を、セキュリティ要件根拠に含めること。(ASE\_REQ.1-20)

TOE セキュリティ要件がTOE のセキュリティ対策方針にまでさかのぼれなければな

らない。TOE のセキュリティ対策方針にまでさかのぼるすべてのTOE セキュリティ要件が満たされた場合、TOE のセキュリティ対策方針が達成されることを実証すること。

TOE のセキュリティ対策方針にまでさかのぼる各TOE セキュリティ要件が満たされると、実際にセキュリティ対策方針の達成に寄与すること。

IT 環境の各セキュリティ対策方針に対して、IT 環境に対するセキュリティ要件が、そのIT 環境のセキュリティ対策方針を満たすのに適していることを示す適切な正当化を、セキュリティ要件根拠に含めること。(ASE\_REQ.1-21)

IT 環境のセキュリティ要件がIT 環境のセキュリティ対策方針にまでさかのぼれなければならない。IT 環境のセキュリティ対策方針にまでさかのぼるIT 環境に対するすべてのセキュリティ要件が満たされた場合、IT 環境のセキュリティ対策方針が達成されることを実証すること。

IT 環境のセキュリティ対策方針にまでさかのぼる各IT 環境に対するセキュリティ要件が満たされると、実際にセキュリティ対策方針の達成に寄与すること。

IT セキュリティ要件のセットが内部的に一貫していることを、セキュリティ要件根拠が実証していること。(ASE\_REQ.1-22)

異なるIT セキュリティ要件が、実行される同じタイプの事象、操作、データ、テストに適用され、これらの要件が競合する可能性があるすべての場合において、相互に競合したり、矛盾が発生したりしないことを説明すること。例えば、ST に利用者の個別の責任に対する要件が利用者の匿名要件とともに含まれている場合、これらの要件が矛盾しないことを示す必要がある。これには「監査可能事象に、利用者の匿名が要求される操作に関しては、個々の利用者の責任が要求されない。」ことを示すことが含まれる場合がある。

IT セキュリティ要件のセットが全体として相互サポート可能な構造を構成することを、セキュリティ要件根拠で実証すること。(ASE\_REQ.1-23)

IT セキュリティ要件からセキュリティ対策方針への追跡を検査するワークユニット ASE\_REQ.1-18 及びASE\_REQ.1-19、及びIT セキュリティ要件がセキュリティ対策方針を満たすために適切であるかどうかを検査する

ワークユニットASE\_REQ.1-20 及びASE\_REQ.1-21 内で実行される決定に基づく。他のIT セキュリティ要件からのサポートがないためにセキュリティ対策方針が達成できない場合がある危険性を考慮すること。

機能要件がこれらの要件の間に依存関係がないことが示されている場合であっても、必要に応じて相互に支援することを実証すること。この実証では、以下のセキュリティ機能要件を取り扱うこと。

- a) FPT\_RVM.1 など、ほかのセキュリティ機能要件のバイパスを防ぐ
- b) FPT\_SEP など、ほかのセキュリティ機能要件の改ざんを防ぐ

- c) FMT\_MOF.1 など、ほかのセキュリティ機能要件の非活性化を防ぐ
- d) FAU クラスのコンポーネントなど、ほかのセキュリティ機能要件の無効化を狙った攻撃の検出を可能にする

分析の際に実行された操作を考慮に入れ、セキュリティ機能要件間の相互サポートに影響するかどうかを検証する。

セキュリティ要件の依存性が満たされないそれぞれの場合に、適切な正当化を提供すること。(ASE\_REQ.1-14)

識別されたセキュリティ対策方針がある場合に、依存性の必要がない理由を説明する。依存性を満たさないことは、セキュリティ要件のセットがセキュリティ対策方針を適切に取り扱う妨げにならないことを確認する。

## 【ガイダンス】

### 機能要件

セキュリティ機能要件がセキュリティ対策方針に対して十分であり、かつ、必要であることを示さなければならない。このために、下記に示すような方法がある。

- ・セキュリティ機能要件が必要であることを示すために、セキュリティ機能要件とセキュリティ対策方針との対応表を作成する。各セキュリティ機能要件は少なくとも一つのセキュリティ対策方針と対応を持つ。セキュリティ対策方針と対応しないセキュリティ機能要件は存在しない。この検証により、セキュリティ機能要件が必要なものであることを確認することができる。すなわち、セキュリティ対策方針の実現に無用な、セキュリティ機能要件は存在しないことが検証できる。
- ・セキュリティ機能要件が十分であることを示すために、各セキュリティ対策方針に対して、該当のセキュリティ機能要件の適用によって、意図したセキュリティ対策方針を実現できるとことを、文章で説明する。

### 保証要件

セキュリティ保証要件がセキュリティ対策方針に対して十分であり、想定されている攻撃者に対抗でき、過剰な保証内容でなく、現実的に実現可能であることを示さなければならない。

保証要件にEALが含まれている場合、そのEALが適切であることを示さなければならない。追加コンポーネントが含まれている場合には、個々の追加コンポーネントが適切であることを示さなければならない。ただし、適切であることの理由を客観的に述べることには困難が伴う。適切であることの理由として以下の事項が想定される。

- ・セキュリティ環境及びセキュリティ対策方針で規定された保証要件関連事項を満足している。(知識のある攻撃者に対する防御を行うことを規定したならば、明白な脆弱性への対抗性しか要求しないAVA\_VLA.1 の指定は不適切である。)
- ・ST が適合を主張するPP に示されている保証要件である。

- ・制度、政府、またはその他の組織によって指定された保証要件である。
- ・TOE セキュリティ機能要件からの依存性を持つ保証要件である。
- ・TOE とともに使用されるシステム及び/または製品の保証要件である。
- ・利用者が要求する保証要件である。

#### 機能強度

AVA\_SOF.1 が指定されている場合、指定の最小機能強度がセキュリティ対策方針に対して、妥当であり、矛盾しない(セキュリティ対策方針またはセキュリティ環境で述べられている攻撃者の技術力、攻撃ツール、動機、などに対抗できる)ものであることを示さなければならない。

#### 相互支援

セキュリティ要件は相互に協力しあい、統一された有効性を実現していることを示すことによって、完結されており、内部的に一貫性があることを説明する。このために、下記を説明する。

- ・機能及び保証コンポーネントの依存性は満足されている。

保証要件がパッケージを利用している場合は、基本的には、パッケージとしてこの依存性は完結しているので、機能要件のみを対象にする。

機能コンポーネントのレベルで、繰り返しなどの操作を含めて、依存性を満足していることを示す。依存性を満足しない要件がある場合には、必要でない理由を明確にする。

依存性は必ずしも TOE によって満足される必要は無く、内容によって、IT 環境や非 IT 環境によって満足されることもある。

全機能コンポーネントに対する依存コンポーネントをリストし、それらが満足している (TOE セキュリティコンポーネントとしてリストアップ) か、満足していない (不要な理由を明記) かを説明する方法で示すことができる。

機能要件と保証要件との間の依存性 (例: FPT\_RCV.1 は依存性として AGD\_ADM.1 と ADV\_SPM.1 を要求) もあるので注意する。

- ・IT セキュリティ要件間の一貫性は確保されている。

セキュリティ対策方針のある事項を実現するためのセキュリティ機能要件に矛盾や競合する (利用者保護のために責任追跡性とプライバシー保護が要請された場合など) ものが存在しないことを検証する。

同一の事象、操作やデータに対して異なった機能要件が適用されている場合、その間に矛盾 (例: 責任追跡性と匿名性が要求されている) が無いことを明記する。

- ・セキュリティ機能に対するバイパス、干渉や非稼働などの攻撃から保護するためのセキュリティ要件が含まれている。

セキュリティ対策方針と機能要件との対応表を記載するだけでなく、それによって何を説明しているのかを記載する。

各セキュリティ対策方針ごとに、関連する機能要件（TOE 固有の用語で記載）によって、そのセキュリティ対策方針を満足することを説明する。

記述例 （機能要件の例）

セキュリティ機能要件の必要性について

各セキュリティ機能要件は、必ず、1つ以上のセキュリティ対策方針に対応しており、すべてのセキュリティ機能要件は、セキュリティ対策方針を実現する上で必要となるものであることが検証できる。

TOE セキュリティ機能要件とセキュリティ対策方針との対応関係を下表に示す。

表 TOE セキュリティ機能要件と対応するセキュリティ対策方針

セキュリティ 対策方針	0. Phys_Prot	0. Init	0. Reuse	0. Brute-Force	0. UnInik	0. Log_Prot	0. I&A	0. DAC	0. P_Load	0. Sec_Com	0. Life_Cycle	0. I_Leak	0. Env_Strs	0. Crypt_Std	0E. CAD_Sec_Com
<b>TOE</b>															
FCS CKM.1(1)															
FCS CKM.1(2)															
FCS CKM.2(1)															
FCS CKM.2(2)															
FCS CKM.4(1)															
FCS CKM.4(2)															
FCS COP.1(1)															
FCS COP.1(2)															
FDP ACC.1															
FDP ACF.1															
FDP ITC.1															
FIA AFL.1															
FIA SOS.1															
FIA UAU.2															
FIA UAU.5															
FIA UAU.6															
FIA UAU.7															
FIA UID.2															
FMT MSA.1															
FMT MSA.3															
FMT MTD.1															
FMT SMF.1															
FMT SMR.1															
FPT FLS.1															
FPT PHP.3															
FPT RCV.4															
FPT RPL.1															
FPT RVM.1															
FPT SEP.1															
FPT TST.1															
FTP ITC.1															
<b>IT環境</b>															
FCS CKM.1(3)															
FCS CKM.2(3)															
FCS CKM.4(3)															
FCS CKM.4(4)															
FCS COP.1(3)															
FCS COP.1(4)															

## セキュリティ機能要件の十分性について

**O.Reuse** (リプレイ攻撃からの保護: TOE は、不正利用者が、認証処理中に入手した情報を再利用することによるなりすましを防ぐために、TOE・カード端末間を流れる秘密情報(認証情報)を暗号化するとともに、暗号化された秘密情報の再利用を検出・防止しなければならない。)

FCS\_CKM.1(1)、FCS\_CKM.1(2)、FCS\_CKM.2(1)、FCS\_CKM.2(2)、FCS\_CKM.4(1)、FCS\_CKM.4(2)、FCS\_COP.1(1)、FCS\_COP.1(2)、FPT\_RPL.1、FPT\_RVM.1、FTP\_ITC.1 によって実現できる。

TOE・カード端末間の秘密情報の盗聴を防止するために以下のように暗号通信路を確保する。まず FCS\_CKM.1(1)により公開鍵・秘密鍵ペアを生成し、FCS\_CKM.2(1)によりカード端末に公開鍵を配付する。一方、カード端末が生成・送信するテンポラリ公開鍵を TOE が受信する。このように相互に公開鍵を交換した後で、FCS\_CKM.1(2)によりセッション鍵を生成して、FCS\_CKM.2(2)によりカード端末に配付する。このとき、FCS\_COP.1(1)によりテンポラリ公開鍵でセッション鍵を暗号化する。最後に、FCS\_COP.1(2)において、前述のセッション鍵を使用して、TOE・カード端末間のセッションで送受信するデータを暗号化及び復号化を行う。さらに FCS\_CKM.4(1)及び FCS\_CKM.4(2)において、カード端末とのセッション終了時に前述の公開鍵・秘密鍵ペア及びセッション鍵を破棄する。以上の暗号通信機能により、TOE と信頼できるカード端末との間に FTP\_ITC.1 による高信頼チャネルを確保する。また、前回実施した認証処理で暗号化した秘密情報をそのまま再利用されることを防ぐために、FPT\_RPL.1 により前回と同じテンポラリ公開鍵によって秘密情報を復号できた場合は IC カードをロックする。さらに、通信データの暗号化に関する機能が迂回されるのを防止するために、FPT\_RVM.1 によって、通信を開始する前に必ず暗号処理に使用する鍵を共有しておく構造にする。

### 記述例 (セキュリティ機能要件の依存性)

TOE セキュリティ機能要件が依存するセキュリティ要件とそれをカバーする TOE セキュリティ機能要件を示すことにより、TOE セキュリティ機能要件の依存性が満たされている範囲を明確にする。さらに、満たされていない依存性についてはそれが正当である根拠を示す。

### セキュリティ機能要件の依存性

項番	TOE セキュリティ機能要件	依存するセキュリティ要件	該当する本書の項番
1	FCS_CKM.1(1)	FCS_CKM.2 または FCS_COP.1	3, 7
		FCS_CKM.4	5
		FMT_MSA.2	不要: 下記(1)参照
2	FCS_CKM.1(2)	FCS_CKM.2 または FCS_COP.1	4, 8
		FCS_CKM.4	6
		FMT_MSA.2	不要: 下記(1)参照

3	FCS_CKM.2(1)	FDP_ITC.1 または FCS_CKM.1	1
		FCS_CKM.4	5
		FMT_MSA.2	不要：下記(1)参照
4	FCS_CKM.2(2)	FDP_ITC.1 または FCS_CKM.1	2

以下、表は省略

(1) FCS\_CKM.1(1)、FCS\_CKM.1(2)、FCS\_CKM.2(1)、FCS\_CKM.2(2)、FCS\_CKM.4(1)、FCS\_CKM.4(2)、FCS\_COP.1(1)、及び FCS\_COP.1(2) から FMT\_MSA.2 への依存性が満たされないことが正当である根拠

国際標準に準拠した所定の仕様に基づいて、TOE が暗号鍵を生成するため、暗号鍵の属性はセキュアな状態にあることが保証される。さらに、破棄するまで暗号鍵に対する変更操作を行わないため、暗号鍵生成時のセキュアな状態が暗号鍵破棄時まで維持されている。以上より、FMT\_MSA.2 によるセキュアなセキュリティ属性の保証は不要である。

記述例（相互サポート）

セキュリティ要件全体が相互に補完し、内部的に一貫している根拠として、セキュリティ機能が迂回、干渉、非活性化の攻撃から保護されることを説明する。

【迂回防止の根拠】

FPT\_RVM.1 は、セキュリティ機能が適切なタイミング及び順序で実行されるような構造を実装する。これによって、FPT\_RVM.1、FPT\_SEP.1、FMT\_SMF.1 及び FMT\_SMR.1 を除くすべてのセキュリティ機能要件の迂回を防止することができる。

【干渉防止の根拠】

FPT\_SEP.1 は、TSF 及び各サブジェクトのドメイン分離を維持する。これによって、FDP クラス、FIA クラス、及び FMT クラスのセキュリティ機能要件が不正なサブジェクトから干渉されるのを防止することができる。

【非活性化防止の根拠】

TOE のセキュリティ機能は常に動作しており停止する機能を持たないため、セキュリティ機能を単独で非活性化させることはできない。また、セキュリティ機能に動作異常が発生した場合には、システム自体を停止させる。

記述例（機能強度）

TOE は、一般的な社外秘情報のある部屋から企業経営の存続に関わるような極秘情報を保管した部屋まで、一般企業のさまざまな資産を格納する部屋への入退出を管理できる入室

管理システムで利用されることを想定している。このため、TOE への脅威が成功すると、最悪の場合、企業の存続に影響するような高い価値を持つ情報にアクセスされ、多大な損害を与えられる恐れがある。本 ST では、このような損害を与えることを意図する攻撃者として、高度な専門知識・技術や特注の攻撃設備・ツールを使用できる人物を想定している。しかし、この入退室管理システムは国防に関わる国家機密のようなきわめて重要な情報を保護することまでは想定していないため、攻撃者は国家機密を脅かそうとするほどの強い動機は持ち合わせていない。

以上より、想定する攻撃力は中程度であり、TOE の最小機能強度レベルは、中程度の攻撃力に対抗できる「SOF-中位」が妥当である。

#### 記述例（保証要件）

TOE は、一般的な社外秘情報のある部屋から企業経営の存続に関わるような極秘情報を保管した部屋まで、さまざまな資産を格納する部屋への入退出を管理できる入退室管理システムで利用される IC カードである。TOE のセキュリティが破壊されると、このシステムを導入した企業が莫大な損害を受ける可能性があるため、ビジネス上妥当なコスト・期間をかけて、セキュリティ機能に対する高い信頼性を確保することが必要である。想定する攻撃力は中程度を想定している。

以上より、既存の開発・製造工程に対して、高度な手法や過度のコスト・期間を追加することなく適用可能な最高の保証レベルであるとともに、中程度の攻撃力への対抗を考慮した「EAL4+AVA\_VLA.3」が妥当である。

## 6 . TOE 要約仕様

### 【参考規格類】

TOE セキュリティ要件を満たす TOE のセキュリティ機能及び保証手段を記述する。これによって、機能要件を満たすために求められるセキュリティ機能の上位のレベルの定義及び保証要件を満たすために取られる保証手段を規定する。場合によっては、TOE 要約仕様の一部として記述する機能の情報は、その TOE の ADV\_FSP 要件の一部として提供される情報と一致することがある。(CC)

TOE セキュリティ機能要件を満たすためのセキュリティ機能、及び TOE セキュリティ保証要件を満たすための保証手段のハイレベルな定義を提供すること。(ASE\_TSS.1-1)

保証手段は、明示的に述べられるか、またはセキュリティ保証要件を満たす文書の参照によって定義することができる(例えば、関連する品質計画、ライフサイクル計画、管理計画)。

IT セキュリティ機能及び保証手段が、すべての特定された TOE のセキュリティ要件が満たされることを保証するのに十分であること。(ASE\_TSS.1-12)

IT セキュリティ機能または保証手段間で TOE のセキュリティ要件が完全には満たされないなどの競合がないこと。(ASE\_TSS.1-14)

### 6 . 1 TOE セキュリティ機能

#### 【参考規格類】

IT セキュリティ機能を網羅し、これらの機能がどのように TOE セキュリティ機能要件を満たすかを明記しなければならない。この記述は、どの機能がどの要件を満たし、全体として、すべての要件が満たされていることを明確に示すために、機能と要件との間の双方向の対応付けを含まなければならない。それぞれのセキュリティ機能は、少なくとも一つの TOE セキュリティ機能要件を満たすのに寄与していなければならない。(CC)

まず最初に、機能要件と要約仕様との対応を表示することを勧める。

各 IT セキュリティ機能が少なくとも 1 つの TOE セキュリティ機能要件にまでたどれること。(ASE\_TSS.1-2)

注：本ワークユニットは、8章の根拠ではなく6章の記載に対する要求であることに注意すること。

各 IT セキュリティ機能は、その目的を理解するために必要な詳細レベルで、非形式的スタイルで記述すること。(ASE\_TSS.1-3)

いくつかの場合では、IT セキュリティ機能が提供する詳細は、対応する TOE セキュリティ機能要件(複数可)で提供されている詳細と同じ程度である。その他の場合は、

ST 作成者は、例えば「セキュリティ属性」など一般的な用語の代わりにTOE特定の用語を使用して、TOE 特定の詳細を含めている場合がある。

ITセキュリティ機能を記述する準形式的または形式的スタイルは、同じ機能の非形式的なスタイルの記述が併記されていない限り、ここでは許可されていないことに注意すること。

セキュリティメカニズムへの参照が含まれている場合、それらの全ての参照がIT セキュリティ機能にまでさかのぼれること。(ASE\_TSS.1-4)

セキュリティメカニズムの参照は、ST では任意であるが、特定のプロトコルまたはアルゴリズムを実装する必要がある場合(例えば、特定のパスワード生成または暗号化アルゴリズム)には、そのプロトコルまたはアルゴリズムを明示すること。

機能強度の主張は適切(対応する機能要件の機能強度と等しいか、または高いことを示す。ただし、認証(例えば、バイオメトリクスなどを利用した認証機能)用のSOF-中位を実装するために、複数の低位機能強度の機能を組み合わせて使用するなどの例外もある。)で、かつ、正確であること。(ASE\_TSS.1-6)

TOE セキュリティ保証要件にAVA\_SOF.1 が含まれている場合、確率的または順列的メカニズムによって実現されるすべてのIT セキュリティ機能を識別すること。

(ASE\_TSS.1-10)

TOE セキュリティ保証要件にAVA\_SOF.1 が含まれている場合、各IT セキュリティ機能に対して、機能強度主張を特定の数値尺度、またはSOF-基本、SOF-中位またはSOF-高位として述べること。(ASE\_TSS.1-11)

## 【ガイダンス】

IT セキュリティ機能(要約仕様)は、その目的を理解するのに必要な詳細度(機能要件で規定した事項を満足するためにいかなる機能を提供するかを記載する。如何に実現するかや実装方法などは不要。)で非形式的(TOE の言葉を使用する。)に定義する。

ST に記述されているセキュリティ機構または技術(暗号アルゴリズム、パスワード生成アルゴリズム、準拠する国内/国際標準、など)は、セキュリティ機能の実装にどのセキュリティ機構または技術が使われているかが分かるように、アルゴリズムやメカニズムを明示しておく。

例：暗号鍵生成要件(FCS\_CKM.1)で、暗号鍵生成アルゴリズムとして、トリプルDES,RSA を規定してあれば、要約仕様の説明で、明確に記載する。

セキュリティ機能要件で規定してある内容は機能仕様を含める。

例：監査要件で収集する事象を規定している場合、要約仕様の説明では、これらの収集事象を含める。

## 6.2 保証手段

#### 【参考規格類】

保証要件を満たすための TOE の保証手段を指定する。保証手段は、どの要件を満たすのにどの手段を用いているのかがわかるように、保証要件を追跡できなければならない。保証手段の定義は、適切な場合には、関係する品質計画、ライフサイクル計画又は管理計画を参照して行ってもよい。(CC)

各保証手段が少なくとも1 つのTOE セキュリティ保証要件にまでたどれること。

(ASE\_TSS.1-8)

開発者が保証要件を取り扱う方法を記述すること。(ASE\_TSS.1-9)

#### 【ガイダンス】

EAL4 くらいまでは、開発者が提供する文書類やエビデンス(CC パート3 開発者アクションエレメントを参照)とその規定概要から保証要件へのマップを記載することで本節の対応ができる。

EAL5 以上に対しては、開発者が適用する具体的な設計手法、構成管理のためのツール、テスト項目の充分性検証ツール、隠れチャンネル分析手法、などを記載する。

### 8.3 TOE 要約仕様根拠

#### 【参考規格類】

TOE のセキュリティ機能及び保証手段が TOE セキュリティ要件を満たすのに適していることを示さなければならない。(CC)

次のことを説明しなければならない。

- ・ 明記された TOE の IT セキュリティ機能の組合せが、TOE のセキュリティ機能要件を満たすために一体となって動作すること。
- ・ 支援機能が他のセキュリティ機能をバイパス、改ざん、または非活性化するなどの潜在的なセキュリティの弱点を取り込まないこと。
- ・ TOE機能強度の主張が正当であること又はこのような主張が不要であるとの宣言が正当であること。機能強度の主張が対応する機能要件の機能強度と等しいか、または高いことを説明する。
- ・ 記述された保証手段が保証要件に対応したものであることの正当化が主張されていること。

根拠の記述は、セキュリティ機能の定義の詳細度に見合う程度で提示しなければならない。保証要件と保証手段とのマップにもとづいて、保証手段が保証要件を満足することを説明する。さらに詳細な正当性の説明は不要。

各TOE セキュリティ機能要件に対して、IT セキュリティ機能とそのTOE セキュリティ機能要件を満たすのに適していることを示す適切な正当化を、TOE 要約仕様根拠に含めること。(ASE\_TSS.1-5)

IT セキュリティ機能がTOE セキュリティ機能要件にまでさかのぼれなければならない。TOE セキュリティ機能要件のための正当化が、要件にまでさかのぼるすべてのIT セキュリティ機能が実装された場合、TOE セキュリティ機能要件が満たされることを実証すること。

TOE セキュリティ機能要件にまでさかのぼる各IT セキュリティ機能が実装されると、実際にその要件を満たすことに寄与すること。

IT セキュリティ機能に対する機能強度主張が、TOE セキュリティ機能要件に対する機能強度と一貫していること。(ASE\_TSS.1-6)

機能強度主張が適切である各IT セキュリティ機能に対して、それがさかのぼるすべてのTOE セキュリティ機能要件に対しこの主張が適していることをTOE要約仕様根拠で実証する。通常、適切性はIT セキュリティ機能の機能強度主張がたどるすべてのTOE セキュリティ機能要件の機能強度と等しいか、または高いことを意味するが、例外もある。そのような例外には、認証(例えば、バイオメトリ及びPIN)用の中程度の強度認証要件を実装するために、複数の低強度機能が連続して使用される場合がある。特定したIT セキュリティ機能の組み合わせが、TOE セキュリティ機能要件を満たすために一緒に機能することを、TOE 要約仕様根拠で実証すること。(ASE\_TSS.1-7)

IT セキュリティ機能に含まれる追加情報がほかのIT セキュリティ機能をバイパス、改ざん、または非活性化するなどの潜在的なセキュリティの弱点を取り込まないこと。各TOE セキュリティ保証要件に対して、保証手段がそのTOE セキュリティ保証要件を満たすことの適切な正当化を、TOE 要約仕様根拠に含めること。(ASE\_TSS.1-9)

保証手段がTOE セキュリティ保証要件にまでさかのぼれなければならない。TOE セキュリティ保証要件のための正当化が、要件にまでさかのぼるすべての保証手段が実装された場合、TOE セキュリティ保証要件が満たされることを実証していること。

TOE セキュリティ保証要件にまでさかのぼる各保証手段が実装されると、実際にその要件を満たすことに寄与すること。

保証手段は、開発者が保証要件を取り扱う方法を記述する。特定された保証手段が保証要件を満たすのに適切であること。

機能要件と要約仕様との対応表を記載するだけでなく、それによって何を説明しているのかを記載する。

機能要件ごとに、関連する要約仕様の実装された場合、その機能要件を満足することを説明する。

## 【ガイダンス】

セキュリティ機能の必要性について

各セキュリティ機能は、必ず、1つ以上のセキュリティ機能要件に対応しており、対

応しないセキュリティ機能は存在しないことを表で示す（セキュリティ対策方針やセキュリティ要件の場合と同じ）。

セキュリティ機能の十分性について

各セキュリティ機能要件の規定事項（割付内容や選択内容など）がどのようなセキュリティ機能によって実現できるかについて説明する（セキュリティ対策方針やセキュリティ要件の場合と同じ）。

## 7 . PP 主張

### 【参考規格類】

STは、TOEが一つ（又は一つ以上の場合もある）のPPの要件に適合していることを主張（適合対象のPPを名称、バージョン、PP概説の識別情報などによって識別。PPへの部分的な適合主張は不可（ASE\_PPC.1-1））してもよい。（CC）

どのようなPPの適合主張に対しても、STには、適合主張を実証するのに必要な説明、理由、その他の裏付けとなる資料からなるPP主張の記述を含まなければならない。

TOEのセキュリティ対策方針及び要件を記述するSTの内容及び表現は、TOEに対するPP主張に影響される可能性がある。STへの影響は、PP主張方法に応じて、次のように要約できる。

- ・PPへの適合を主張しない場合には、TOEのセキュリティ対策方針及び要件を完全に提示するのがよい。PP主張は含めない。
- ・STがPPの要件だけに適合することを主張し、追加を必要としない場合には、TOEのセキュリティ対策方針及び要件の定義及び正当化は、PPの参照だけで十分とする。PPの内容を再度記述する必要はない。
- ・STがPPの要件に対する適合を主張し、かつ、PPに追加が必要な場合には、STは、そのPPが必要とした追加に適合していることを示さなければならない。  
このような状況は、PPが未完結の操作を含んでいる場合に起こることが多い。このような状況では、STは、特定の要件を参照してもよいが、ST中でその操作を完結しなければならない。操作を完結するための要件が多数ある場合に、明確化の一助として、ST中でPPの内容を再度記述するのが望ましい。
- ・STがPPの要件へ適合することを主張するが、別のセキュリティ対策方針及び要件を追加してそのPPを拡張する場合は、PPへの参照がPPのセキュリティ対策方針及び要件を定義するのに十分であっても、STは、それらの追加事項を定義しなければならない。追加が多数ある場合には、明確化の一助として、ST中でPPの内容を再度記述するのが望ましい。
- ・STがPPへの部分的な適合を主張するのは、CCの評価では認めない。

PPのセキュリティ対策方針及び要件を再記述するか又は参照するかのいずれを選択するかについて、CCは規定しない。基本的要件は、STの評価が可能であり、STがTOE評価のために利用できる基礎となり、適合が主張されたPPへの追跡が可能であるように、STの内容が完全で、明解で、かつ、あいまいさがなくとする。

各々のPP主張に対して、PPからITセキュリティ要件に実施されたすべての操作が、PPによって設定された境界内にあること。（ASE\_PPC.1-4）

これは、PPにおける未完結の割付または選択操作だけでなく、PPから取り出されたセキュリティ要件に対する詳細化操作の適用もカバーする。

## 【ガイダンス】

PP への部分的な適合の主張は CC の下では許可されないことに留意する。

PP への適合の宣言が無い場合、適合する PP が無い旨を記載する。

### 7.1 PP 参照

#### 【参考規格類】

各々のPP 主張が適合を主張されているPP を曖昧なく識別すること（例えば、タイトル及びバージョン番号、またはPP の概説に含まれている識別によって）。

(ASE\_PPC.1-1)

## 【ガイダンス】

適合を主張する PP を識別し、その主張に関して、必要な追加説明をしなければならない。正当な主張は、TOE が PP のすべての要件を満たすことを意味する。

### 7.2 PP 修整

#### 【参考規格類】

PPで許容された操作を満たす場合の、又はPPの要件に対して追加が必要な場合の、IT セキュリティ要件の記述を識別しなければならない。（CC）

各々のPP 主張が、PP の許可された操作を満たす、またはPP 要件をさらに適正化するようなIT セキュリティ要件ステートメントを識別すること。（ASE\_PPC.1-2）

STでは、そのST に対して未修正のPP に含まれるセキュリティ要件のステートメントを繰り返す必要はない。しかし、PP のセキュリティ機能要件が未完了の操作を含む場合、またはST の作成者が任意のPP のセキュリティ要件に詳細化操作を適用した場合は、ST におけるこれらの要件を明確に識別しなければならない。

### 7.3 PP 追加

#### 【参考規格類】

PP のセキュリティ対策方針及び要件に追加される TOE のセキュリティ対策方針及び要件を識別しなければならない。（CC）

各々のPP 主張が、PP に含まれるセキュリティ対策方針及びIT セキュリティ要件に追加されるセキュリティ対策方針及びIT セキュリティ要件を識別すること。

(ASE\_PPC.1-3)

ST に含まれるが、PP には含まれていないすべてのセキュリティ対策方針及びセキュリティ要件が明確に識別すること。

### 8.4 PP 主張根拠

**【参考規格類】**

ST との適合を主張する PP との間のセキュリティ対策方針及び要件の相違をすべて説明しなければならない。PP との適合を主張しない場合、又は ST のセキュリティ対策方針及び要件が主張する PP のものと同じである場合、ST のこの部分は省略してもよい。(CC)

この膨大となる可能性のある資料は、必ずしも、すべての ST 使用者にとって適切又は有用であるとは限らないので、分冊にして配布してもよい。

- ・ PP で記載の全てのセキュリティ対策方針が含まれていることを示す。
- ・ PP で記載の全てのセキュリティ要件が含まれていることを示す。詳細化や他の操作は妥当であることを示す。
- ・ PP がない追加のセキュリティ対策方針や IT セキュリティ要件は PP と競合しないことを示す。
- ・ PP で不完全な操作が全て完全に指定されていることを確認する。

以上