情報技術セキュリティ評価のための
コモンクライテリア

パート1：概説と一般モデル

2005年8月

バージョン2.3

CCMB-2005-08-001

平成 17 年 12 月翻訳第 1.0 版
独立行政法人情報処理推進機構
セキュリティセンター
情報セキュリティ認証室

IPA まえがき

はじめに

本書は、「IT セキュリティ評価及び認証制度」において、「認証機関が公開する評価基準」の規格として公開している Common Criteria(以下、CC という)を翻訳した文書である。

注：1.原文の CC で記載してある段落番号については、本書では段落番号が付与されていない。このため、段落番号については、CC の原文を参照のこと。
CC v2.3 では規格上の改定以外に、編集上、書式上、及びレイアウト上の体裁の変更がされているが、規格を改定する変更でないため、本書では反映していないものがある。
例えば：

- “the components of the FAU_GEN Security audit data generation family” の表記を “the components of the Security audit data generation (FAU_GEN) family”に変更
- “Dependencies:”の表記位置を“Hierarchical to:”の後に移動

2.本翻訳文書は、補足-0512 の解釈を反映済みである。

原文

Common Criteria for Information Technology Security Evaluation
Part1: Introduction and general model Version 2.3
August 2005 CCMB-2005-08-001
Part2: Security functional requirements Version 2.3
August 2005 CCMB-2005-08-002
Part3: Security assurance requirements Version 2.3
August 2005 CCMB-2005-08-003

まえがき

情報技術セキュリティ評価のためのコモンクライテリア(CC 2.3)の本バージョンは、国際標準のISO/IEC 15408:2005と合わせて、すべての最終的な解釈、編集上の修正、及びCC2.1の発表以来の合意した新しい資料を含んでいる。

CCバージョン2.3は、次のパートから構成される:

- パート1: 概説と一般モデル
- パート2: セキュリティ機能要件
- パート3: セキュリティ保証要件

法定通知

以下に示す政府組織は、情報技術セキュリティ評価のためのコモンクライテリアの本バージョンの開発に貢献した。情報技術セキュリティ評価ためのコモンクライテリアバージョン2.3のパート1から3(CC 2.3と呼ぶ)の著作権を共有したまま、これらの政府組織が、ISO/IEC 15408国際標準の継続的な開発/維持の中で、CC 2.3を使用するためにISO/IECに対し、排他的でないライセンスを許可している。ただし、適切と思われる場合にCC 2.3を使用、複製、配布、翻訳及び改変する権利は、これらの政府組織が保有する。

オーストラリア/ニュージーランド: *The Defence Signals Directorate and the Government Communications Security Bureau respectively;*
カナダ: *Communications Security Establishment;*
フランス: *Direction Central de la Sécurité des Systèmes d'Information;*
ドイツ: *Bundesamt für Sicherheit in der Informationstechnik;*
日本: *Information Technology Promotion Agency*
オランダ: *Netherlands National Communications Security Agency;*
スペイン: *Ministerio de Administraciones Públicas and Centro Criptológico Nacional;*
英国: *Communications-Electronics Security Group;*
米国: *The National Security Agency and the National Institute of Standards and Technology.*

目次

図一覧

表一覧

1 序説

CC は、独立したセキュリティ評価結果間の比較を可能にするものである。このため、IT 製品及びシステムのセキュリティ機能とセキュリティ評価の際にそれらに適用される保証手段に関する共通要件のセットを規定している。評価プロセスでは、そうした製品及びシステムのセキュリティ機能とそれらに適用される保証手段が、これらの要件を満たしていることの信頼のレベルを明らかにする。評価結果は、IT 製品またはシステムがその目的とする利用に十分セキュアであるかどうか、またその使用に当たって潜在的に含まれるセキュリティリスクが許容できるものであるかどうかについて、消費者が判定する際に役立つであろう。

CC は、IT セキュリティ機能を備えた製品またはシステムの開発、ならびにそうした機能を備えた市販製品及びシステムの調達のための指針として役立つ。評価においては、そうした IT 製品またはシステムを評価対象（TOE）と呼ぶ。TOE には、例えばオペレーティングシステム、コンピュータネットワーク、分散システム、アプリケーションが含まれる。

CC が扱うのは、許可されない暴露、改変、または利用不能からの情報の保護である。一般に、これら 3 種類のセキュリティ障害に関する保護のカテゴリはそれぞれ機密性、完全性、及び可用性と呼ばれる。CC はまた、これら 3 つ以外の IT セキュリティの側面にも適用してもよい。CC は、その情報に対する脅威のうち、悪意のあるものであろうとなかろうと人間の活動に起因するものを主な対象としているが、人間以外のものによる一部の脅威にも同様に適用してもよい。なお、CC は、その他の IT 分野にも適用してもよいが、厳密な IT セキュリティ領域以外に対する有効性は求めていない。

CC は、ハードウェア、ファームウェア、またはソフトウェアに実装される IT セキュリティ手段に適用される。評価の特定の側面が、特定の実装方法に適用することのみを目的とする場合には、関連する基準ステートメントにおいてこれを示すことになる。

2　適用範囲

複数のパートからなるこの標準、コモンクライテリア（Common Criteria：CC）は、IT 製品及びシステムのセキュリティ特性を評価する基盤として用いるためのものである。そうした共通の基準のベースを確立することにより、IT セキュリティ評価の結果はより広範な対象者にとって有意義なものとなろう。

いくつかの項目には、専門的な技法が必要であったり、IT セキュリティにとってあまり重要でなかったりすることから、CC の範囲外と見なされるものがある。以下にこれらの項目の一部を示す。

a) CC は、IT セキュリティ手段に直接関係しない管理上のセキュリティ手段に関するセキュリティ評価基準は含んでいない。しかし、多くの場合、TOE セキュリティのかなりの部分が組織的、人的、物理的、及び手続き的管理のような管理上の手段によって実現可能であると認められる。したがって、TOE の動作環境における管理上のセキュリティ手段は、識別された脅威に対抗するための IT セキュリティ手段の能力に影響を与える場合には、セキュアな使用法の前提として扱う。

b) 電磁波放射制御のような IT セキュリティの技術上の物理的側面の評価は、特に対象としていないが、扱われる概念の多くはその領域にも適用することができる。特に、CC は TOE の物理的保護のいくつかの側面を扱っている。

c) CC は、評価機関が基準を適用するうえでの評価方法と管理上・法律上の枠組みのいずれも扱っていない。しかし、そうした枠組みや方法の状況においても、評価を目的として CC を用いることが期待される。

d) 製品またはシステムの認定(accreditation)における評価結果を用いるための手続きは、CC の範囲外である。製品またはシステムの認定は、機関があらゆる運用環境における IT 製品またはシステムの運用を認めるための管理上のプロセスである。評価の中心となるのは、製品またはシステムの IT セキュリティ部分と、運用環境のうち IT エレメントのセキュアな使用に直接影響する可能性のある部分である。したがって、評価プロセスの結果は、認定プロセスへの貴重な入力となる。しかし、非 IT 関連の製品またはシステムのセキュリティ特性、及び IT セキュリティ部分とのそれらの関係のための評定には、他の技法の方がより適しているため、認定者(accreditor)はこれらの側面に対して個別に備えるべきである。

e) 暗号化アルゴリズム固有の品質評定のための基準は、CC では対象とされない。TOE に組み込まれる暗号の数学的特性に対する独立の評定が必要な場合、CC が適用される評価制度は、そうした評定に備えたものでなければならない。

3　用語と定義

本文書の目的について、以下の用語と定義があてはまる。

この 3 章では、CC 全体にわたって特別な意味で用いられる用語のみを示す。CC の用語の大部分は、認められた辞書の定義に従うか、または ISO セキュリティ用語やその他の周知のセキュリティ用語に記載されていると考えられる一般的に認められた定義に従って用いられる。CC に用いられる一般用語の一部の組合せのうち、この 3 章に含まれていないものについては、分かりやすくするためにそれぞれの文脈において説明している。CC パート 2 及びパート 3 で特別な意味で用いられている用語と概念の使用法の説明は、それぞれの使用個所(「　」で示す)の節に記載してある。

資産（Assets）－ TOE の対抗策が保護すべき情報または資源。

割付（Assignment）－ コンポーネント内の識別されたパラメタの仕様。

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。

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。

要件追加（Augmentation）－ CC パート 3 の 1 つまたは複数の保証コンポーネントを EAL または保証パッケージに追加すること。

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。

許可された利用者（Authorised user）－ TSP に従って操作を実行することができる利用者。

クラス（Class）－ 共通の対象を共有するファミリのグループ。

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。

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。

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。

エレメント（Element）－ 不可分のセキュリティ要件。

評価（Evaluation）－ 定義された基準に対する PP、ST、または TOE の評定。

評価保証レベル（Evaluation Assurance Level、EAL）－ CC の定義済み保証尺度での程度を表す、CC パート 3 の保証コンポーネントからなるパッケージ。

評価監督機関（Evaluation authority）－ 評価制度に基づき特定のコミュニティに対して CC を履行し、それによって、標準を定め、そのコミュニティ内の機関が実施する評価の品質を監視する機関。

評価制度（Evaluation scheme）― 評価監督機関が特定のコミュニティにおいて CC を適用する際の規範となる管理及び規制の枠組み。

要件拡張（Extension）― CC のパート 2 に含まれていない機能要件、及び/または CC のパート 3 に含まれていない保証要件を、ST または PP に追加すること。

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。

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。

形式的（Formal）― 確立した数学上の概念に基づいて、意味が定義された制限付き構文言語で表現すること。

ガイダンス証拠資料（Guidance Documentation）― 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。

人間の利用者（Human user）― TOE と対話する任意の人。

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。

非形式的（Informal）― 自然言語で表現すること。

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。

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。

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。

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。

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。

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。

パッケージ（Package）― 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。

製品（Product）― 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。

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。

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。

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。

詳細化（Refinement）― コンポーネントに詳細を追加すること。

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。

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。

セキュリティ属性（Security attribute）― 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/または資源の特性。

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。

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。

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ステートメント。

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。

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。

準形式的（Semiformal）― 意味が定義された制限付き構文言語で表現すること。

機能強度（Strength of Function、SOF）― 下位のセキュリティメカニズムを直接攻撃することにより、予測されるセキュリティのふるまいを無効にするのに必要と見なされる最小限の労力で表した TOE セキュリティ機能の能力。

SOF-**基本**（SOF-basic）― 分析により、低い攻撃能力を有する攻撃者による偶発的な TOE セキュリティ侵害に対して、その機能が十分な抵抗力を備えていると認められた TOE 機能強度のレベル。

SOF-**中位**（SOF-medium）― 分析により、中程度の攻撃能力を有する攻撃者による直接的または意図的な TOE セキュリティ侵害に対して、その機能が十分な抵抗力を備えていると認められた TOE 機能強度のレベル。

SOF-**高位**（SOF-high）― 分析により、高い攻撃能力を有する攻撃者による系統的または組織的な TOE セキュリティ侵害に対して、その機能が十分な抵抗力を備えていると認められた TOE 機能強度のレベル。

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。

システム（System）― 特定の目的と運用環境を伴う特定の IT 設備。

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、及び関連するガイダンス証拠資料。

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。

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。

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。

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。

TOE **セキュリティ方針モデル**（TOE security policy model）－ TOE が実施すべきセキュリティ方針の構造化表現。

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。

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。

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。

TSF **データ**（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。

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。

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）。

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。

規定（Normative）－ 規定テキストは、「文書の適用範囲を記述し、そして規定を提示する」ものである（ISO/IEC 専門業務用指針 第 2 部）。規定テキストにおいては、助動詞「しなければならない（shall）」、「するべきである（should）」、「することができる（may）」、及び「できる（can）」は、この章において記述される ISO 基準の意味を持つ、そして助動詞「ねばならない（must）」は使用しない。明確に「参考」と表示されていない場合、すべての CC テキストは規定である。要件を満たすことに関係するあらゆるテキストは、規定と考えられる。

参考（Informative）－ 参考テキストは、「文書の理解、または使用を援助することを意図する追加情報を提供する。」ものである（ISO/IEC 専門業務用指針 第 2 部）。参考テキストは、要件を満たすことに関連しない。

しなければならない（Shall）－ 規定テキストにおいて、「しなければならない（shall）」は、「文書に準拠し、そして逸脱を許さない厳格に従う要件」を示す。（ISO/IEC 専門業務用指針 第 2 部）

するべきである（Should）－ 規定テキストにおいて、するべきである（should）は、「いくつかの可能性の中で、他に言及することなくまたは他を排除することなく、特に適切であるとして 1

つを推奨すること、または一連のアクションが望ましいが、必ずしも必要ではないこと。」を示す（ISO/IEC 専門業務用指針 第 2 部）。CC は、「必ずしも必要ではない」は、他の可能性の選択はなぜ望ましい選択肢が選択されなかったのかの根拠を求めることを意味すると解釈する。

してもよい（May）ー 規定テキストにおいて、してもよい（may）は、「文書の制限内で許される一連のアクション」を示す。（ISO/IEC 専門業務用指針 第 2 部）

できる（Can）ー 規定テキストにおいて、できる（can）は、「有形的、物理的、または原因的な可能性と能力のステートメント」を示す。（ISO/IEC 専門業務用指針 第 2 部）

4　記号と略語

以下の略語は、CC の各パートに共通して用いられる。

CC	コモンクライテリア（Common Criteria)
EAL	評価保証レベル（Evaluation Assurance Level）
IT	情報技術（Information Technology）
PP	プロテクションプロファイル（Protection Profile）
SF	セキュリティ機能（Security Function）
SFP	セキュリティ機能方針（Security Function Policy）
SOF	機能強度（Strength of Function）
ST	セキュリティターゲット（Security Target）
TOE	評価対象（Target of Evaluation）
TSC	TSF 制御範囲（TSF Scope of Control）
TSF	TOE セキュリティ機能（TOE Security Functions）
TSFI	TSF インタフェース（TSF Interface）
TSP	TOE セキュリティ方針（TOE Security Policy）

5 概要

この章では、CC の主な概念について述べ、対象者、評価の枠組み、及び資料を提出するのに取られたアプローチを明らかにする。

5.1 序説

IT 製品またはシステムが保有する情報は、組織がその使命で成功できるようにする極めて重要な資源である。さらに、人々は、IT 製品またはシステムに格納されているそれぞれの個人情報が、秘匿され、必要に応じて利用でき、許可されない改変を受けない状態に留まることに相当な期待を抱いている。IT 製品またはシステムは、不要または不当なまき散らし、改ざん、損失などの危険から確実に保護できるように情報を適切に統制しながら、それぞれの機能を実行するべきである。IT セキュリティという用語は、これらの危険及びこれらと同様の危険の防止と軽減を対象として用いる。

IT 消費者の多くは、IT 製品またはシステムのセキュリティの信頼度が妥当なものかどうかを判断するのに必要な知識、技能、または資源を欠いているが、場合によっては開発者の主張だけに頼ることを望まないこともある。したがって、消費者はそのセキュリティの分析（すなわちセキュリティ評価）を依頼することにより、IT 製品またはシステムのセキュリティ手段(security measures)に対する信頼度を向上させることも可能である。

適切な IT セキュリティ手段を選定するために、CC を用いることができる。CC にはセキュリティ要件の評価のための基準が記載されている。

5.1.1 CC の対象読者

IT 製品及びシステムのセキュリティ特性の評価に一般的関心を有するのは、3 つのグループ、すなわち TOE 消費者、TOE 開発者、及び TOE 評価者である。この文書で示す基準は、3 つのグループすべてのニーズに対応できるように構成されている。これら 3 つのグループはすべて、この CC の主な利用者と見なされており、以下のパラグラフで説明するようにこの基準から利益を受けることができる。

5.1.1.1 消費者

CC は、消費者がそれぞれの組織ニーズを表す IT セキュリティ要件を選択する手法のサポートにおいて重要な役割を果たす。CC は、評価により消費者のニーズが確実に実現できるように記述されているが、それは、これが評価プロセスの基本的な目的であり、正当な理由だからである。

消費者は、評価対象の製品またはシステムがそれぞれのセキュリティニーズを満たしているかどうかを判定する一助として、評価結果を用いることができる。これらのセキュリティニーズは、リスク分析と方針の方向付けの結果として、通常識別される。消費者はまた、様々な製品またはシステムを比較する場合に評価結果を用いることもできる。このニーズは、階層化で保証要件を提示することによってサポートされる。

CC は、消費者、特に関心を持つ消費者のグループ及びコミュニティに対して、TOE における IT セキュリティ手段に関するそれぞれの特別な要件を表現するための、プロテクションプロファイル（PP）と呼ばれる実装に依存しない体系を提供する。

5.1.1.2 開発者

CC は、製品またはシステムの評価の準備と援助、及び各製品またはシステムが満たすべきセキュリティ要件の識別において、開発者をサポートすることを目的としている。さらに、評価結果に

対する相互承認協定に伴って合意された関連する評価方法によって、TOE 開発者以外の者が開発者の TOE 評価の準備と援助をサポートすることになることもあり得る。

また、評価されるべき特定のセキュリティの機能及び保証によって、TOE が識別された要件に適合していると主張するために、CC の構造を用いることができる。各 TOE の要件は、セキュリティターゲット（ST）と呼ばれる実装に依存する構造に含まれている。1 つまたは複数の PP は、広範な消費者ベースの要件を提供することができる。

CC は、開発者が TOE に含めることができるセキュリティ機能を記述している。CC は、TOE の評価を裏付けるのに必要な証拠を提供する責任及びアクションを決定するために用いることができる。また、その証拠の内容及び提示も定義されている。

5.1.1.3 評価者

CC は、セキュリティ要件に対する TOE の適合について判断を下す際に、評価者が用いる基準を含んでいる。CC は、評価者が実行すべき一般的なアクション、及びこれらのアクションの実行対象となるセキュリティ機能を記述している。CC は、それらのアクションの実行に当たって従うべき手続きを具体的に述べていないことに注意のこと。

5.1.1.4 その他の対象者

CC は、TOE の IT セキュリティ特性の仕様と評価に向かって志向しているが、IT セキュリティに関係または責任のあるすべての関係者のための参考資料としても役に立つことができる。以下に、CC に含まれている情報から利益を受けることができるその他の利益グループをいくつか示す。

a) 組織の IT セキュリティ方針と要件の決定及び実現に責任のある、システム管理者やシステムセキュリティ担当役員

b) システムのセキュリティの妥当性評定に責任のある、内部及び外部の監査員

c) IT システム及び製品のセキュリティ内容の仕様に責任のある、セキュリティ立案者及び設計者

d) 特定の環境内における IT システム使用の承認に責任のある、認定者

e) 評価の依頼及び支援に責任のある、評価のスポンサー

f) IT セキュリティ評価計画の管理及び監督に責任のある、評価監督機関

5.2 評価の枠組み

評価結果間の比較可能性を高めるには、標準を定め、評価の品質を監視し、評価設備と評価者が遵守しなければならない規則を管理する信頼すべき評価制度の枠組みの中で評価が実施されるべきである。

CC は、規制上の枠組みに関する要件を記述していない。しかしながら、こうした評価結果に対する相互承認の目標を達成するには、様々な評価監督機関の規制上の枠組み間の一貫性が必要になろう。図 1 に、評価の枠組みを形成する主なエレメントを示す。

共通評価方法を用いることは、結果の再現性と客観性に寄与するが、それだけでは十分とは言えない。評価基準の多くは、専門家の判断と予備知識の適用を必要とするため、一貫性の実現はいっそう困難なものとなる。評価結果の一貫性を高めるために、最終評価結果は認証(certification)プロセスにかけられることもある。認証プロセスは、最終的な認証書または承認書を提供する独立した評価結果の検査である。認証書は、通常、公開の場で利用することができる。認証プロセスは、IT セキュリティ基準の適用における一貫性を高める手段であることに注意のこと。

評価制度、方法、及び認証プロセスは、評価制度を実行する評価監督機関の責任であり、CC の範囲外である。

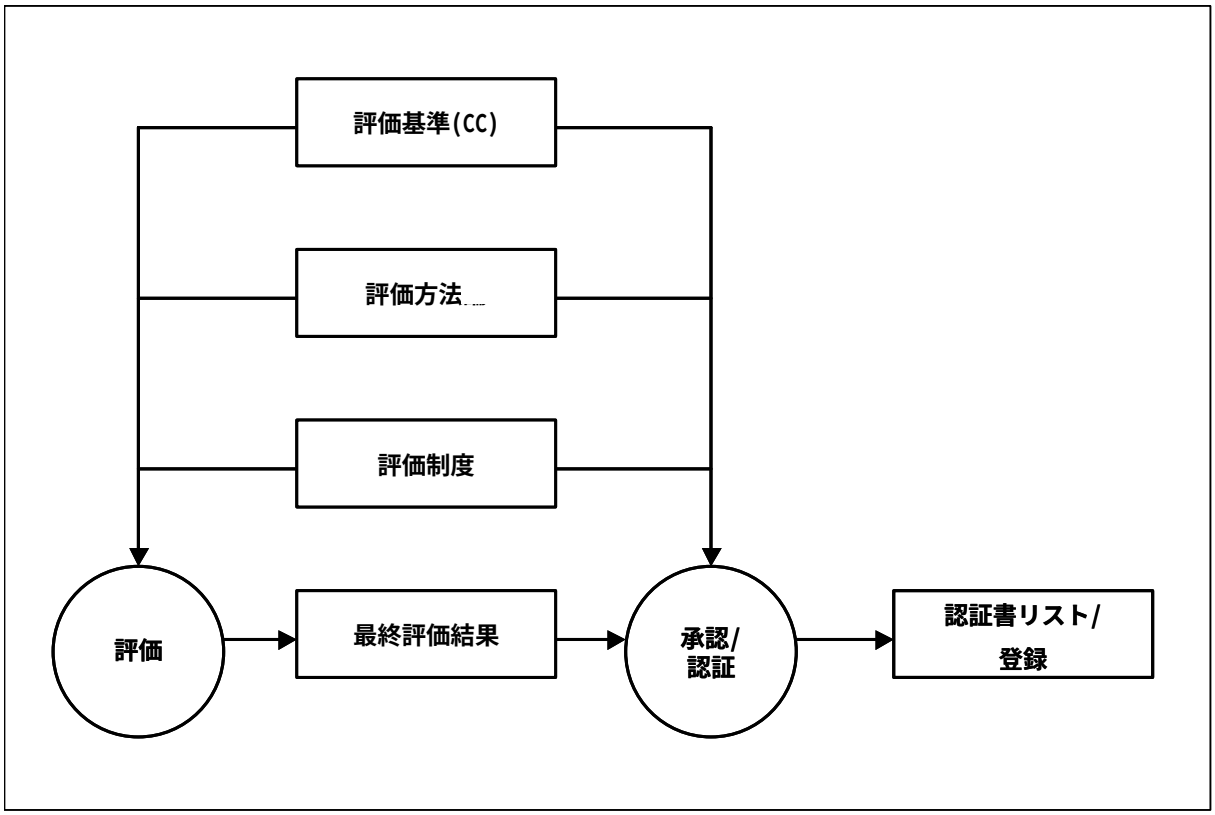

図 1　評価の枠組み

5.3　コモンクライテリアの構成

CC は、以下に示すように別のものではあるが、関連する 3 つのパートとして提供されている。各パートの記述に用いられている用語については、第 6 章で説明する。

a) **パート 1「概説と一般モデル」**は、CC の概説であり、IT セキュリティ評価の一般的概念と原則を定義し、評価の一般モデルを示している。パート 1 ではまた、IT セキュリティ対策方針の表現のための構造、IT セキュリティ要件の選択と定義のための構造、及び製品やシステムの上位レベル仕様記述のための構造も示している。さらに、CC の各パートの有用性について各対象読者の観点から述べている。

b) **パート 2「セキュリティ機能要件」**は、TOE の機能要件を表現する標準的な手段として、機能コンポーネントのセットを規定している。パート 2 は、機能コンポーネント、機能ファミリ、及び機能クラスのセットをカタログ化している。

c) **パート 3「セキュリティ保証要件」**は、TOE の保証要件を表現する標準的な手段として、保証コンポーネントのセットを規定している。パート 3 は、保証コンポーネント、保証ファミリ、及び保証クラスのセットをカタログ化している。また、PP 及び ST の評価基準も定義しており、評価保証レベル（EAL）と呼ばれる、TOE の保証をレート付けするための規定の CC 尺度を定義する評価保証レベルも示している。

上記の CC の 3 つのパートを支援するものとして、技術的根拠に関する資料やガイダンス文書を含め、その他のタイプの文書が出版されることが予想される。

以下の表に、3 つの主な対象読者グループが CC の各パートをどのように利用すべきかを示す。

表 1　コモンクライテリアのロードマップ

	消費者	開発者	評価者
パート 1	予備知識及び参照のために使用。PP に関するガイダンス構造。	TOE の要件の開発及びセキュリティ仕様の定式化に関する予備知識及び参考のために使用。	予備知識及び参考のために使用。PP 及び ST に関するガイダンス構造。
パート 2	セキュリティ機能の要件ステートメントを定式化する際のガイダンス及び参考資料として使用。	TOE の機能要件のステートメントを解釈する際、及び機能仕様を定式化する際の参考資料として使用。	TOE が要求されるセキュリティ機能を有効に実現しているかどうかを判定する際に不可欠な評価基準のステートメントとして使用。
パート 3	必要な保証レベルを決定する際のガイダンスとして使用。	TOE の保証要件のステートメントを解釈する際、及び TOE の保証アプローチを決定する際の参考資料として使用。	TOE の保証を確定する際、及び PP と ST を評価する際に不可欠な評価基準のステートメントとして使用。

6　一般モデル

この章は、概念が用いられるべき枠組み、CC における概念を適用するアプローチを含め、CC 全体にわたって用いられる一般的概念を示す。CC パート 2 と CC パート 3 では、これらの概念の使用について詳述しており、ここに述べるアプローチを用いることを前提としている。この章は、IT セキュリティについて相応の知識があることを前提としており、この領域に関する手引きの役割を果たすことは意図していない。

CC は、セキュリティについてセキュリティの概念と用語のセットを用いて論じている。これらの概念及び用語を理解していることが、CC を効果的に用いるための前提条件である。ただし、概念自体は極めて一般的なものであり、CC が適用される IT セキュリティの問題の種類を限定することを意図したものではない。

6.1　セキュリティの枠組み

6.1.1　一般的なセキュリティの枠組み

セキュリティは、脅威からの資産の保護に関係しているが、この場合の脅威とは、保護対象の資産が悪用される可能性として分類される。脅威のすべてのカテゴリについて考察されるべきであるが、セキュリティの領域においては、悪意のあるアクティビティやその他の人間のアクティビティに関連する脅威に特に注目する。図 2 に、上位レベルの概念と関係を示す。

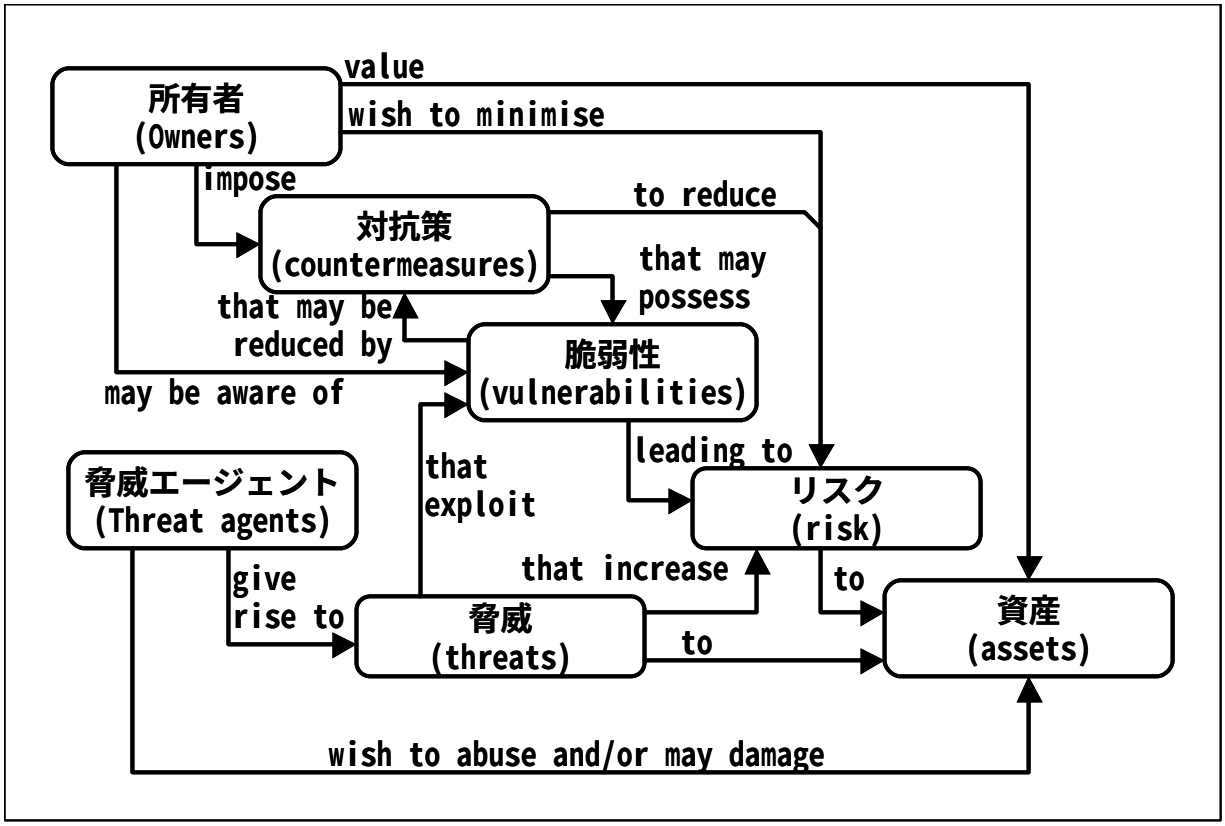

図 2　セキュリティの概念と関係

対象となる資産の保護手段は、それらの資産の価値を認識している所有者の責任である。実在するまたは想定の脅威エージェントもまたその資産の価値を認識しており、所有者の利益に反する

形で資産を悪用しようとする可能性がある。所有者は、そうした脅威を、所有者にとっての資産の価値が減少することになるような資産の侵害の可能性と捉えるであろう。一般に、セキュリティ固有の侵害には、許可されない受信者への資産の公開（機密性の損失）、許可されない改変による資産の損害（完全性の損失）、許可されない資産利用妨害（可用性の損失）などがあるが、これらだけではない。

資産の所有者は、関連するリスクを特定して、資産と環境にあてはまる脅威を分析することになる。この分析は、リスクに対抗し、そのリスクを許容できるレベルまで軽減するための対抗策選定の一助となり得る。

対抗策は、脆弱性を軽減することと資産の所有者のセキュリティ方針を満たすことを目的に実施される（直接的に、または他の関係者に指示することによって間接的に）。しかし、対抗策の実施後も、その他の脆弱性が残存する可能性がある。そうした脆弱性は脅威エージェントにつけ込まれる可能性があり、これは資産に対してあるレベルのリスクが残存することを意味する。その他の制約を考えると、所有者はそのリスクを最小限に抑えようと努めるであろう。

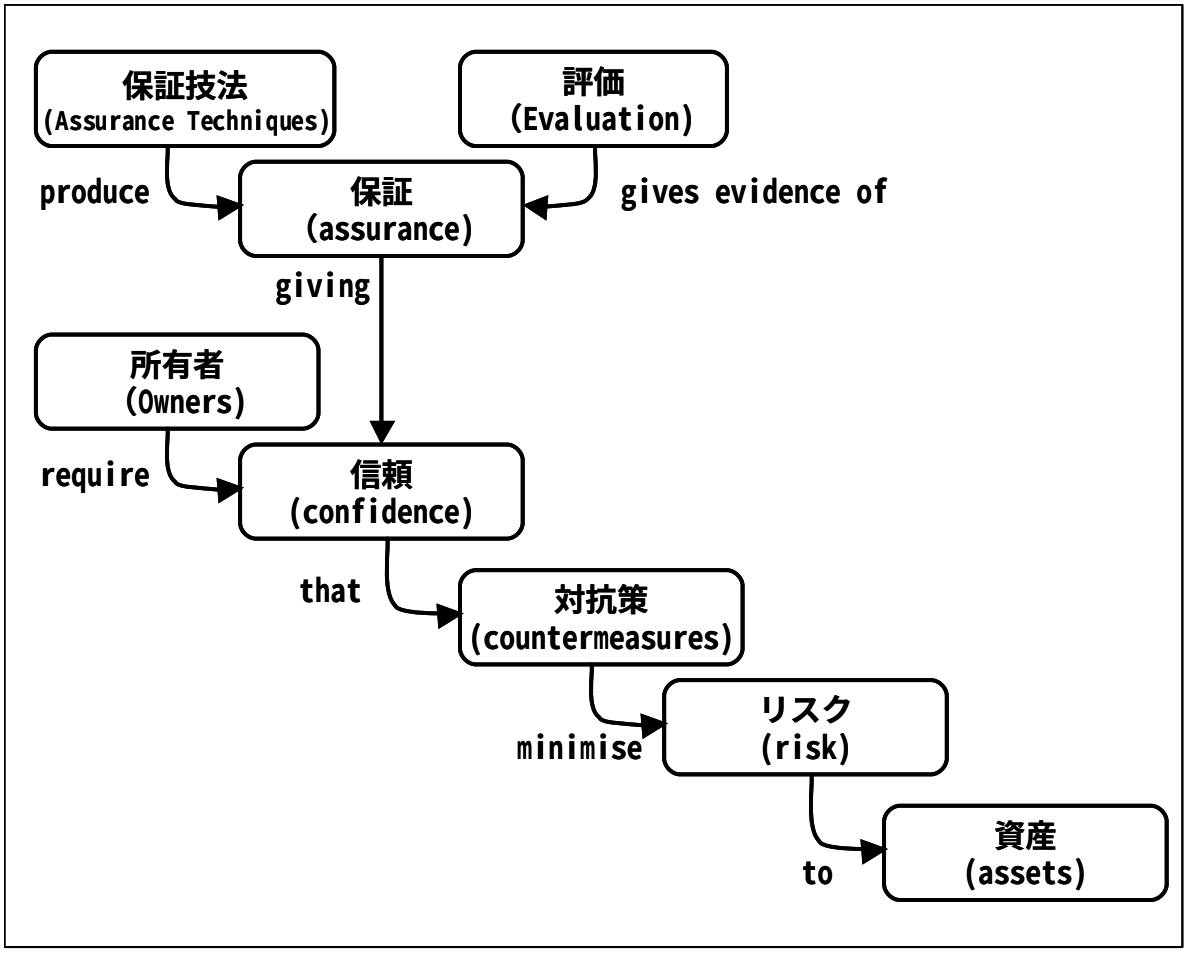

図３　評価の概念と関係

所有者は、対抗策が資産に対する脅威に対抗するのに十分なものであることを確認してから、その資産を脅威にさらすことを許可する必要がある。所有者自身は、対抗策のすべての側面を判断する能力を備えていない可能性があり、その結果、対抗策の評価を求めることになる。評価結果は、対抗策が保護対象の資産に対するリスクを減少させることの信頼性の保証が得られる度合いについてのステートメントである。保証は、対抗策についての、その適切な運用における信頼度の根拠となる特性なので、ステートメントでは対抗策の保証のレート付けを行う。このステート

メントは、資産の所有者が資産を脅威にさらすリスクを受け入れるかどうかを判断する際に用いることができる。これらの関係を図 3 に示す。

一般に、資産に対する責任は資産の所有者が負うことになり、所有者は資産を脅威にさらすリスクを受け入れる判断を立証できるべきである。このため、評価から得られるステートメントは、立証を可能にするものであることが求められる。したがって、評価は目的、ならびに証拠として挙げることができる再現性のある結果を導くものであるべきである。

6.1.2 情報技術セキュリティの枠組み

資産の多くは情報の形をとり、情報の所有者が規定した要件を満たす IT 製品またはシステムによって保存されたり、処理されたり、伝送されたりする。情報の所有者は、そうした情報の表現（データ）のまき散らし及び改変を厳密に制御することが必要になろう。また、データに対する脅威の抑制を目的として導入される総合的なセキュリティ対抗策の一環として、IT 製品またはシステムが IT 固有のセキュリティ制御を実装していることも必要になろう。

IT システムの調達及び構築は、特定の要件を満たすように行われるが、経済的な理由により、オペレーティングシステム、汎用アプリケーションコンポーネント、ハードウェアプラットフォームの既存の汎用 IT 製品が最大限に活用される可能性がある。場合によっては、システムに実装されている IT セキュリティ対抗策が、下位の IT 製品の機能を利用していることもあり、その場合、セキュリティ対抗策は IT 製品のセキュリティ機能の正しい動作に依存することになる。したがって、IT 製品もまた、IT システムのセキュリティ評価の一部として評価対象となろう。

IT 製品が複数の IT システムに統合されている場合、または統合が検討されている場合、そうした製品のセキュリティ面を独立して評価し、評価済み製品のカタログを作成する方がコスト的に有利である。そうした評価の結果は、製品のセキュリティ調査に必要な作業を無駄に繰り返すことなく、複数の IT システムへの製品統合を裏付けるような形で表現されるべきである。

IT システムの認定者は、IT 及び非 IT セキュリティ対抗策の組合せにより、データが十分に保護されるかどうかを判定するための情報を所有する権限を有しており、したがってシステムの運用を許可するかどうかを決定する権限も有している。認定者は、IT 対抗策が十分な保護を提供するかどうか、及び特定の対抗策が IT システムに適切に実装されているかどうかを判定するために、IT 対抗策の評価を要求する可能性がある。この評価は、認定者に課される規則または認定者が課す規則に応じて、様々な形と厳密さをとることになろう。

6.2 コモンクライテリアのアプローチ

IT セキュリティにおける信頼度は、開発、評価、及び運用の各プロセスにおいて取られるアクションによって高めることができる。

6.2.1 開発

CC は、特定の開発方法またはライフサイクルモデルを規定していない。図 4 に、セキュリティ要件と TOE との関係に関する基本的な前提条件を示す。この図は、検討の枠組みを規定するために用いるものであり、ある方法（例えば、ウォータフォール型）が別の方法（例えば、プロトタイプ型）に優先することを提唱するものと解釈するべきでない。

不可欠なのは、IT 開発に課されるセキュリティ要件が消費者のセキュリティ対策方針に有効に寄与することである。開発プロセスの開始時に適切な要件が規定されていなければ、得られる最終製品は、如何に適切に設計されているものであっても、期待する消費者の目的を満たすことはできないであろう。

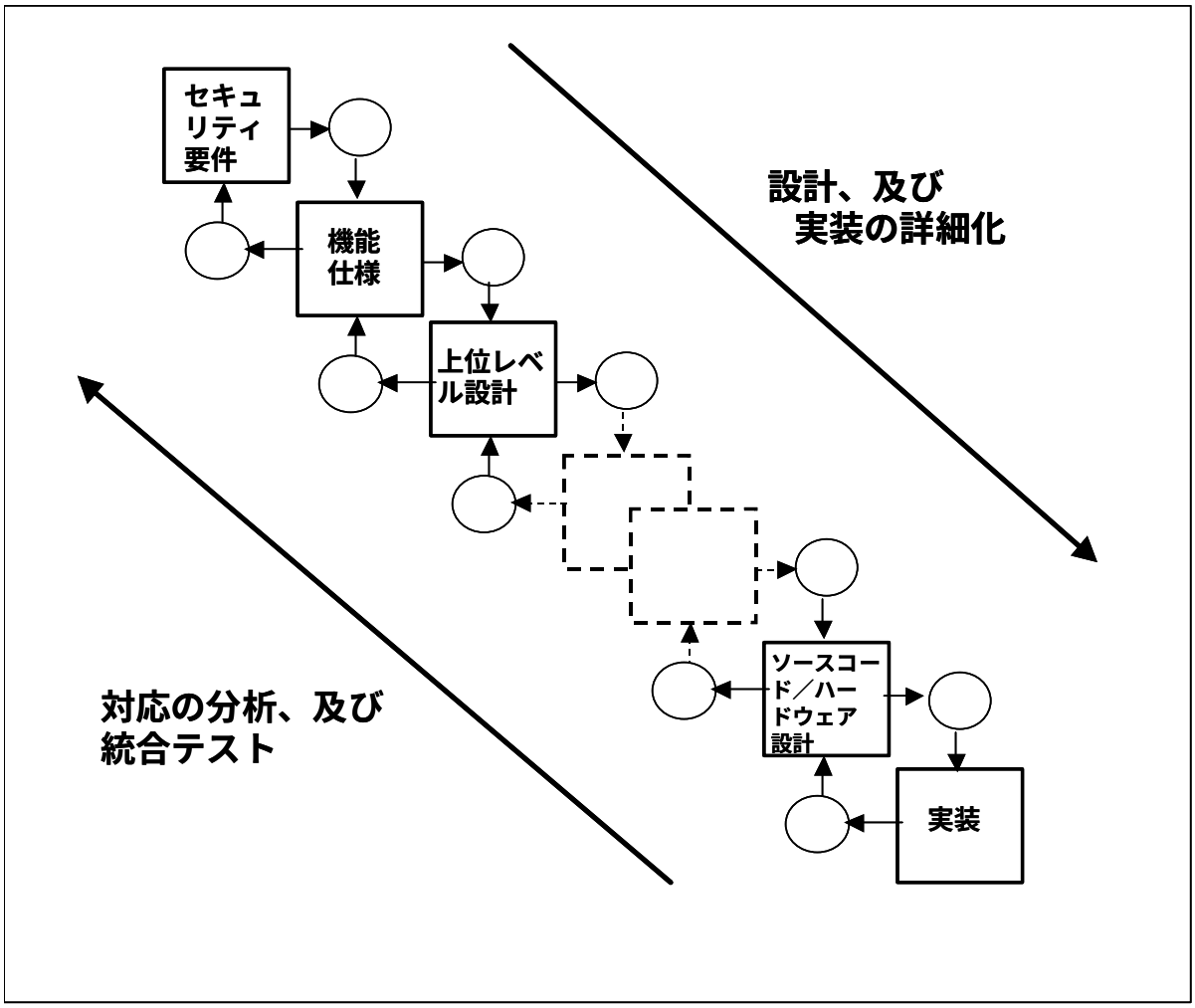

図 4　TOE 開発モデル

このプロセスは､セキュリティターゲットで表現した TOE 要約仕様へのセキュリティ要件の詳細化を基本とする。下位レベルの詳細化はそれぞれ、追加の設計詳細による設計への展開を表す。最も具体的な表現は TOE の実装自体である。

CC では、特定の設計表現を規定していない。CC において求めているのは、必要に応じて、以下のことを実証するのに十分な設計表現が十分な細かさで提示されるべきである。

a) 各詳細化のレベルは、上位レベルの完全な具体化であること（すなわち、より高い抽象度で定義されたすべての TOE セキュリティ機能、特性、及びふるまいが、下位レベルにおいて実証的に提示されていなければならない）

b) 各詳細化のレベルは、上位レベルの正確な具体化であること（すなわち、上位レベルにおいて必要のない TOE セキュリティ機能、特性、及びふるまいが、より低い抽象度で定義されるべきでない）

CC の保証基準では、機能仕様、上位レベル設計、下位レベル設計、及び実装の設計抽象度を明らかにする。指定された保証レベルに応じて、開発者は、開発方法が CC の保証要件をどのように満たしているかを示すことが要求されるであろう。

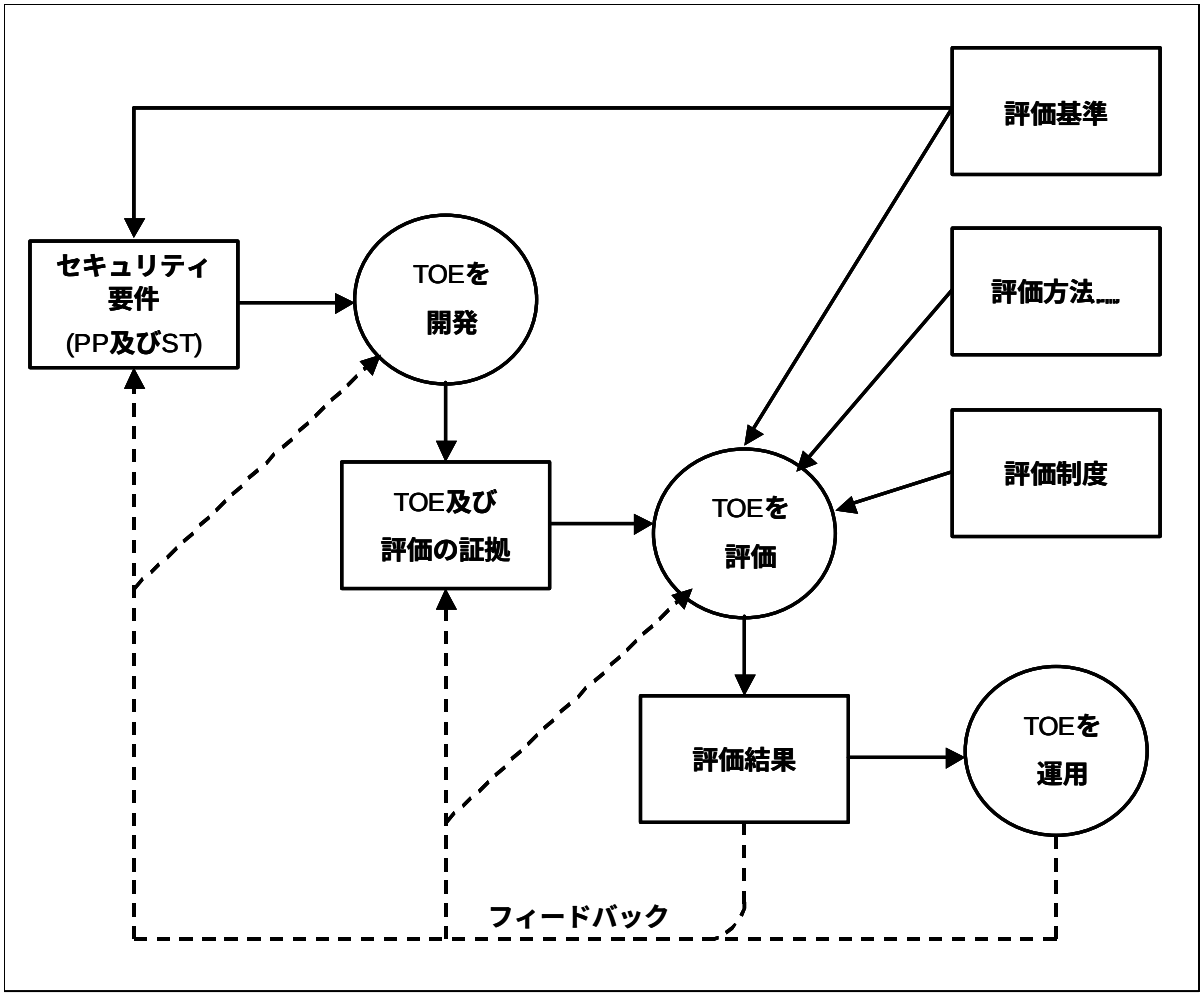

図 5　TOE の評価プロセス

6.2.2　TOE の評価

図 5 に示す TOE の評価プロセスは、開発と並行して、または開発の後に実施してもよい。TOE の評価への主な入力は、以下のとおりである。

a) TOE の証拠のセット、これは TOE 評価のための基準となる ST を含む

b) 評価が要求される TOE

c) 評価の基準、方法、及び制度

さらに、参考資料（CC の適用上の注釈のような）や、評価者及び評価コミュニティの IT セキュリティの専門的知識も、評価の入力として用いられる可能性が高い。

評価プロセスに期待される結果は、TOE に関する評価者の結論を評価基準によって決められたとおりに文書化した 1 つまたは複数の報告書により、TOE がそのセキュリティ要件を ST に記述されているとおりに満たしていることを確認することである。これらの報告書は、開発者のみならず、TOE によって表現される製品またはシステムの実際の消費者及び潜在的消費者にとっても役立つものとなろう。

評価によって得られる信頼度は、満たされる保証要件（例えば、評価保証レベル）に依存する。

評価は、2 つの形で IT セキュリティ製品の向上をもたらすことができる。評価は、開発者が修正可能な TOE の誤りまたは脆弱性を識別し、それによって将来の運用におけるセキュリティ障害の可能性を低減することを目的とする。また、評価の厳密さに備えて、開発者が TOE の設計及び開発に、より細心の注意を払うことが可能になる。したがって、評価プロセスは初期要件、開発プロセス、最終製品、及び運用環境に対して間接的ながら多大な効果を及ぼすことができる。

6.2.3 運用

消費者は、自らの環境において評価済み TOE を使用することを選ぶことができる。TOE の運用が開始されることになれば、これまで分からなかった誤りや脆弱性が表面化したり、環境の前提条件の変更が必要になったりする可能性がある。運用の結果、開発者が TOE を修正したり、セキュリティ要件または環境の前提条件を再定義したりするのに必要になるフィードバックが得られるであろう。こうした変更を行う場合、TOE の再評価、またはその運用環境のセキュリティの強化が必要になる可能性がある。場合によっては、TOE の信頼を回復するために必要な更新部分を評価するだけでよいこともある。CC は、評価結果の再利用を含め、詳細な再評価手続きは、CC の範囲外である。

6.3 セキュリティの概念

評価基準は、安全な TOE の開発及び評価の支えとなる工学的プロセス及び規制上の枠組みの範囲において最も役立つ。この節は、説明及びガイダンスのみを目的としており、CC を採用することができる分析プロセス、開発手法、または評価制度を限定することは意図していない。

CC は、IT が用いられており、かつ IT 要素の資産の保護手段に関心がある場合に適用される。資産がセキュアであることを明らかにするには、セキュリティの問題を、最も抽象的なレベルからその運用環境への最終的な IT の実装に至るまで、すべてのレベルで検討しなければならない。次節以降で述べるこうしたレベルの表現は、セキュリティの問題や課題の明確化や検討を可能にするが、それだけでは最終的な IT の実装が必要なセキュリティのふるまいを示し、その結果、信頼することができるということの実証にはならない。

CC は、あるレベルの表現にそのレベルにおける TOE の表現に対する根拠が含まれていることを要求する。すなわち、そうしたレベルには、上位レベルに適合しており、かつそれ自体が完全であり、正確であり、内部的に一貫していることを示す、理路整然とし、かつ説得力のある論拠が含まれていなければならない。隣接する上位レベル表現との適合を実証する根拠のステートメントは、TOE の正確さを主張する場合の一助となる。セキュリティ対策方針への適合を直接的に実証する根拠は、TOE が脅威への対抗及び組織のセキュリティ方針の履行において有効であるという主張の裏付けとなる。

CC は、図 6 に示す様々なレベルの表現で階層化されている。この図は、PP または ST の開発時に、セキュリティ要件及びセキュリティ仕様を導き出す方法を示すものである。最終的に、TOE のすべてのセキュリティ要件は、TOE の目的及び枠組みを検討することから生じる。この図は、PP 及び ST を開発する方法を限定することを意図したものではなく、いくつかの分析的アプローチの結果が、PP 及び ST の内容とどのように関連するかを示すものである。

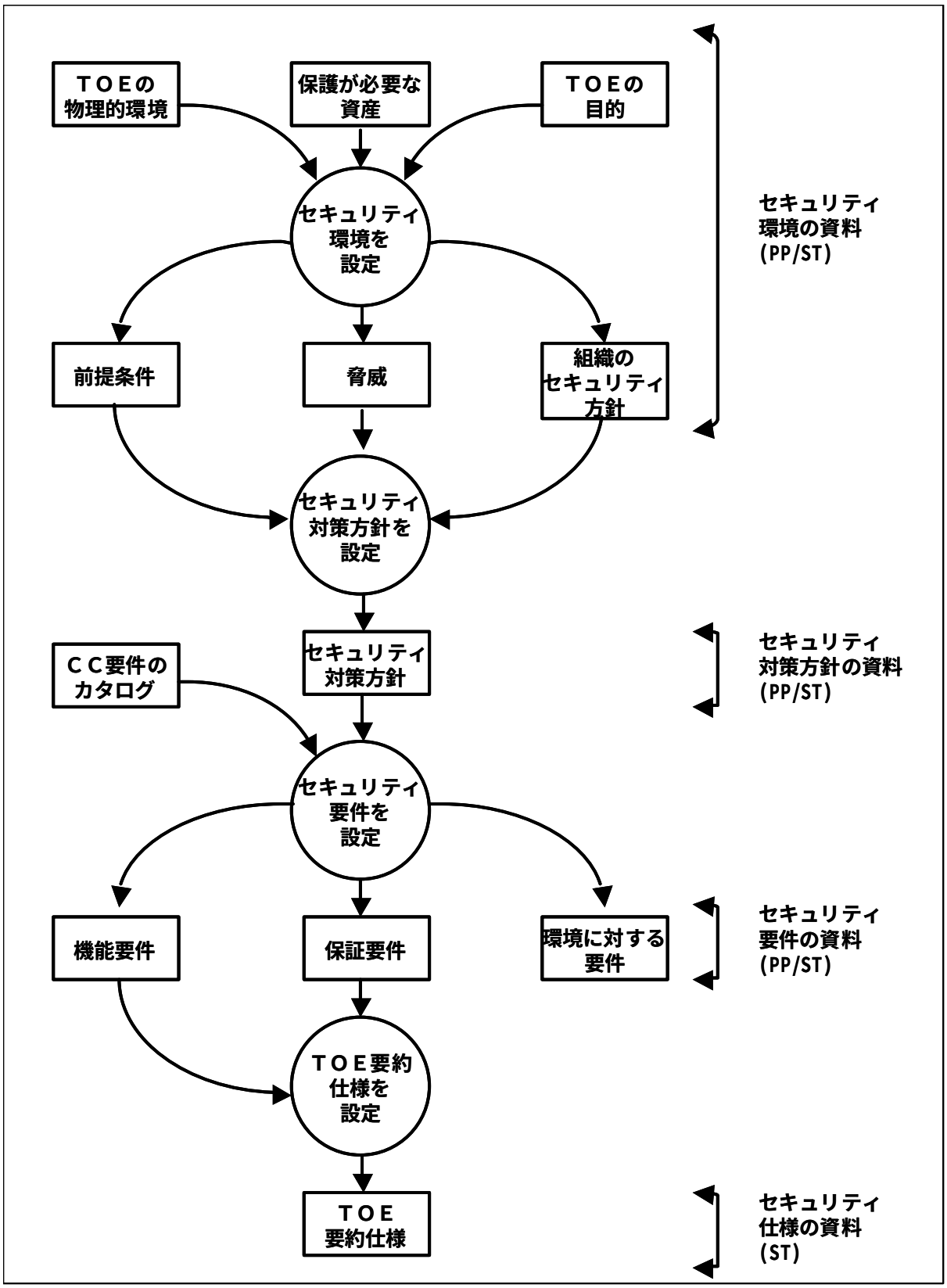

図６　要件及び仕様の導出

6.3.1 セキュリティ環境

セキュリティ環境には、関連性があると判定されたすべての法規、組織のセキュリティ方針、慣行、技能、及び知識が含まれる。したがって、それは、TOE の使用対象となる範囲を定義する。また、セキュリティ環境には、その環境内に存在する、または存在すると考えられるセキュリティに対する脅威も含まれる。

セキュリティ環境を設定する場合、PP または ST の作成者は以下のことを考慮しなければならない。

a) 既知の物理的及び人的セキュリティ構成を含め、TOE のセキュリティに関連する TOE の運用環境の側面すべてを識別する TOE の物理的環境。

b) セキュリティ要件またはセキュリティ方針の適用対象となる、TOE の要素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、直接的に参照される資産のみならず、公認の証明書や IT の実装自体など、間接的にセキュリティ要件の対象となる資産も含むことができる。

c) TOE の目的。これは TOE の製品種別及び意図した使用法が対象となる。

セキュリティ方針、脅威、及びリスクの調査は、以下の TOE に関するセキュリティ固有のステートメントの作成を可能にするべきである。

a) TOE がセキュアと見なされるために TOE の環境が満たすべき前提条件のステートメント。このステートメントは、TOE の評価に対する公理として受け入れることができる。

b) 資産のセキュリティに対する脅威のステートメントは、セキュリティ分析によって TOE に関連するものとして認められたすべての脅威を識別することが求められる。CC では、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、及び攻撃を受ける資産の識別の点から脅威を特徴付けている。セキュリティに対するリスクの評定では、そうした脅威が実際の攻撃に発展する可能性、そうした攻撃が成功する可能性、及びその結果として生じる損害を評定することにより、各脅威を分類する。

c) 適用される組織のセキュリティ方針のステートメントで、関連する方針及び規則を識別する。IT システムの場合、こうした方針を明示的に記載することができるが、汎用の IT 製品または製品群の場合、組織のセキュリティ方針についての実用的な前提条件の作成が必要になることもある。

6.3.2 セキュリティ対策方針

次いで、セキュリティ環境の分析結果は、識別された脅威に対抗するためのセキュリティ対策方針を規定したり、識別された組織のセキュリティ方針及び前提条件を検討したりすることに使用できる。セキュリティ対策方針は、規定された TOE の運用上の目的または製品目的、及びその物理的環境についての認識と一貫しているべきである。

セキュリティ対策方針を決定する意味は、セキュリティの問題をすべて検討すること、及びセキュリティの側面が TOE またはその環境によって直接扱われるどうかを明らかにすることにある。この分類は、技術的判断、セキュリティ方針、経済的要因、及びリスク受入れの判断を組み入れたプロセスに基づく。

環境に対するセキュリティ対策方針は、IT の領域内において非技術的手段または手続上の手段によって実現されるであろう。

TOE 及びその IT 環境に対するセキュリティ対策方針だけは、IT セキュリティ要件によって扱われる。

6.3.3 IT セキュリティ要件

IT セキュリティ要件は、TOE に対するセキュリティ要件及び環境に対するセキュリティ要件のセットに、セキュリティ対策方針を詳細化したものであり、それらのセキュリティ要件が満たされると、TOE がそのセキュリティ対策方針を満たすことを保証する。

CC は、機能要件と保証要件という別の分類に分けてセキュリティ要件を提示している。

機能要件は、特に IT セキュリティをサポートする TOE の機能に対して課されるもので、要求されたセキュリティのふるまいを定義している。CC パート 2 は、機能要件を定義している。機能要件の例として、識別、認証、セキュリティ監査、発信の否認不可に関する要件が挙げられる。

TOE が確率的または順列的メカニズム（例えば、パスワードやハッシュ関数）によって実現されるセキュリティ機能を含む場合、保証要件はセキュリティ対策方針と一致する最小限の強度レベルを求めるように規定することができる。この場合、規定されるレベルは SOF-基本、SOF-中位、SOF-高位のいずれかとなる。そうした機能はそれぞれ、その最小限のレベルを満たすか、または任意に定義された特定の数値尺度を少なくとも満たすことが必要になる。

保証の度合いは、機能要件のセットごとに異なる可能性がある。したがって、通常は保証コンポーネントによって高められる厳密さのレベルという形で表現される。CC パート 3 は、保証要件と評価保証レベル（EAL）の尺度を定義している。保証要件は、開発者のアクション、提出される証拠、及び評価者のアクションに対して課される。保証要件の例としては、開発プロセスの厳密さに対する制約、セキュリティの脆弱性の可能性の探索、及びその影響の分析を行うための要件などが挙げられる。

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、以下の 2 つの要素から導き出される。

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適切に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規定されたセキュリティ対策方針を実際に満たしているかどうかの評定。

一般に、セキュリティ要件は、望ましいふるまいが存在するという要件、及び望ましくないふるまいが存在しないという要件を共に含む。通常は、使用またはテストにより、望ましいふるまいが存在することを実証するのは可能である。しかし、望ましくないふるまいが存在しないことを明確に実証するのは必ずしも可能ではない。テスト、設計レビュー、及び実装レビューは、そうした望ましくないふるまいが存在するリスクの削減に大きく寄与する。根拠のステートメントは、そうした望ましくないふるまいが存在していないことの主張をさらに裏付ける。

6.3.4 TOE 要約仕様

ST において規定される TOE 要約仕様は、TOE のセキュリティ要件の具体例をあげて定義する。これにより、機能要件を満たすために要求されるセキュリティ機能の上位レベルの定義、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。

6.3.5 TOE の実装

TOE の実装は、ST に含まれるそのセキュリティ機能要件、及び TOE 要約仕様に基づいて TOE を実現することである。TOE の実装は、セキュリティを適用するプロセス、及び IT に関する工学的スキルや知識を用いて実現される。TOE は、ST に記述されているすべてのセキュリティ要件を正確かつ有効に実装していれば、セキュリティ対策方針を満たしていることになる。

6.4 CC の記述資料

CC は、評価を行うための枠組みを提示している。証拠及び分析に関する要件を提示することにより、より客観的な、ひいては有効な評価結果を実現することができる。CC は、関連する IT セキュリティの側面を表現したり、伝達したりするための構造の共通セット及び共通言語を具体化しており、IT セキュリティに責任のある者が他者の経験や専門知識から利益を受けることを可能にする。

6.4.1 セキュリティ要件の表現

CC は、有効性が判明している意味のあるセキュリティ要件の集合体に統合された構造のセットを定義しており、これは開発予定の製品及びシステムのセキュリティ要件の規定に際して用いることができる。以下、要件を表現する様々な構造間の関係について述べ、それを図 7 に示す。

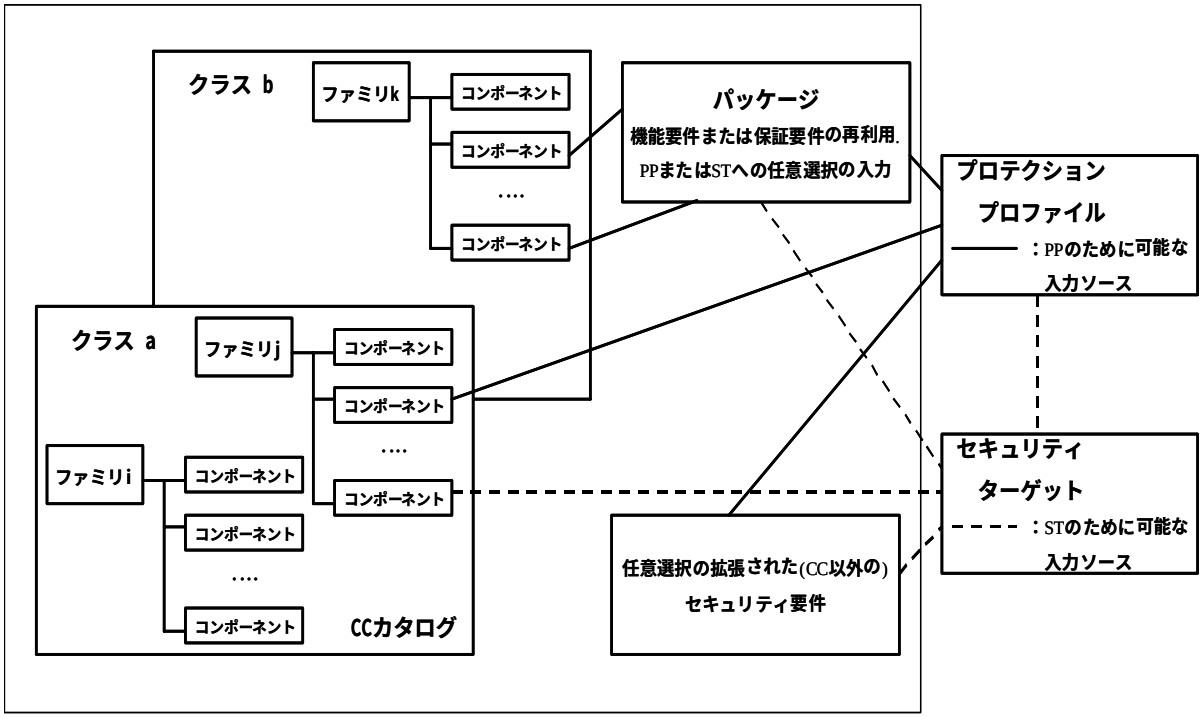

図 7　要件の編成及び構造

CC のセキュリティ要件が、クラス ― ファミリ ― コンポーネントという階層で編成されているため、消費者は特定のセキュリティ要件を簡単に見つけることができる。

CC は、機能面と保証面の要件を同じ一般様式で提示しており、またそれぞれに対して同じ編成及び用語を用いている。

6.4.1.1 クラス

クラスという用語は、セキュリティ要件の最も概括的なグループを表す場合に用いる。クラスのメンバは、すべて共通の対象を共有するが、セキュリティ対策方針のカバレージは異なる。

クラスのメンバは、ファミリと呼ばれる。

6.4.1.2 ファミリ

ファミリは、セキュリティ対策方針は共有するが、重点または厳密さが異なる可能性のあるセキュリティ要件の集合のグループである。

ファミリのメンバは、コンポーネントと呼ばれる。

6.4.1.3 コンポーネント

コンポーネントは、特定のセキュリティ要件の集合を表すもので、CC に定義されている構造に含めることができる、最小の選択可能なセキュリティ要件セットである。ファミリ内のコンポーネントセットは、共通の目的を持つセキュリティ要件の強度または能力の増加を表現するように順序付けすることができる。また、関連する非階層セットを表現するように部分的に順序付けすることもできる。場合によっては、ファミリ内に 1 つのコンポーネントしか含まれていないこともあり、その場合には順序付けは適用されない。

コンポーネントは、個々のエレメントから構成される。エレメントは、セキュリティ要件の最下位レベル表現であり、評価によって検証することができる不可分のセキュリティ要件である。

6.4.1.3.1 コンポーネント間の依存性

コンポーネント間には、依存性が存在する可能性がある。依存性は、あるコンポーネントが自立的ではなく、別のコンポーネントの存在に依存する場合に生じる。依存性は、機能コンポーネント間、保証コンポーネント間、及び機能コンポーネントと保証コンポーネント間に存在する可能性がある。

コンポーネントの依存性の記述は、CC コンポーネント定義の一部となっている。TOE 要件の完全性を保証するには、必要に応じてコンポーネントを PP 及び ST に取り入れるときに依存性が満たされるべきである。

6.4.1.3.2 コンポーネントに対して許容される操作

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ることもでき、あるいは、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が施されたとき、PP/ST 作成者は、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。PP/ST 作成者は、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、以下のセットから選択される。

a) 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ことを許す。
b) 割付：パラメタの特定を許す。
c) 選択：リストから、一つあるいはそれ以上の項目の特定を許す。
d) 詳細化：詳細の追加を許す。

繰返し

同一の要件の異なる側面をカバーすることが必要な場合(例えば、2 種類以上の利用者の識別)、各側面をカバーするために、同一のコンポーネントの繰返し使用が許可される。

繰返しは、要件コンポーネントのレベルに向けたものであるが、常にコンポーネントの各繰返しの全文を反復する必要があるのではない。もし、繰返しを常に行うと、コンポーネント内のエレメントの中には、変更されることなく何回も反復されるものが出てくるだろう。PP またはST では、詳細化、あるいは割付の完了、または選択操作によって、その都度、変更される要件エレメントだけを反復することが許されている。(詳細化された要件の繰返しに関するさらなるガイダンスについては、詳細化を参照)。

割付

コンポーネントの中には、セキュリティ対策方針を満たすために、PP またはSTに組み込む値のセットをPP/ST の作成者が特定することを可能にするパラメタを含むエレメントを持つものがある。これらのエレメントは、各パラメタとそのパラメタに割り付け得る値への制約を明確に識別する。

受け入れ得る値をあいまいさなく記述、あるいは列挙できるエレメントのあらゆる側面は、パラメタによって表現することができる。パラメタは、属性であってもよく、あるいは要件を特定の値あるいは値の範囲に狭める規則であってもよい。例えば、セキュリティ対策方針に基づき、コンポーネント内のエレメントは、定められた操作が何度か実行されるべきであることを述べられる。この場合、割付は、そのパラメタで使用されるべき数あるいは数の範囲を規定することになる。

選択

これは、コンポーネント内のエレメントの範囲を狭めるために、リストから一つあるいはそれ以上の項目を取り上げる操作である。

詳細化

すべてのコンポーネントについて、PP/ST 作成者は、セキュリティ対策方針を満たすために、追加の詳細を特定することによって、受け入れられる実装のセットを制限することが許可されている。コンポーネント内のエレメントの詳細化は、これらの技術的詳細を付加することからなる。コンポーネントへの変更が有効な詳細化であると見なされるために、その変更は、以下のすべての条件を満たさねばならない。

a) 詳細化された要件を満たすTOE は、PP/ST の文脈で解釈されるように、本来の要件もみたす。
b) 詳細化された要件が繰り返される場合、各繰返しは、要件の範囲のサブセットだけに対応することが許される。しかしながら、繰返しをすべて合わせたものを一緒にして、本来の要件の全体の範囲が満たされねばならない
c) 詳細化された要件は、本来の要件の範囲を拡張しない。
d) 詳細化された要件は、本来の要件の依存性のリストを変更しない。

有効な詳細化の例を示す。

a) 完了した割付の内容を理解しやすくするための、あるいは文法的正確さに対応するための変更など、単なる編集上の変更。

b) PP/ST で使われる際の文脈によるもので、要件の範囲を置き換えることのない変更。例えば、「TOE 利用者」と述べた要件を「TOE telnet 利用者」に変更することは、TOE の利

用者がtelnet 利用者だけの場合に有効な詳細化となろう。

c) 要件の範囲を拡張せずに、実装に関する許容できるアプローチの情報を提供する変更。有効な詳細化の一例は、要件を「検証する能力を提供する」から「暗号チェックサムを実装することにより、検証する能力を提供する」に変更することである。この変更は、既存の要件の実装に用いられるメカニズムの性質に制限を与えるが、本来の範囲を拡張しない。

CC パート 2 附属書は、選択と割付の有効な完了のガイダンスを提示する。このガイダンスは、いかに操作を完了させるかについて規定となる指示を提供し、PP/ST 作成者が、逸脱を正当としない場合、この指示に従わなければならない。

a) 「なし」は、明示的に示される場合のみ、選択の完了として選ぶことができる。

選択の完全性に係わり提示されるリストは、空白であってはならない。もし「なし」の選択肢が選ばれた場合、追加の選択肢は選ばなくてもよい。「なし」が選択における選択肢として与えられない場合、選択において、「及び」及び「または」の組み合わせが「から一つのみ選択」という明確な記述がない場合に限り許される。

選択操作は、必要な箇所の繰返しにより、組み合わせられることがある。この場合、各々の繰返しの選択肢の適用可能性は、排他的であることを目的とするので、他の繰返し選択の対象と重複しない。

b) 割付の完了について、CC パート 2 附属書では、「なし」を有効な完了であると指示する。

必要な操作には、PPにおいて（すべてまたは一部）完成すればよいものもあれば、STにおいて完了すればよいものもある。ただし、STではすべての操作が完成しなければならない。

6.4.1.4 セキュリティ要件の使用

CC は、パッケージ、PP、及び ST という 3 種類の要件構造を定義している。CC は、多くのコミュニティのニーズに対処することができる IT セキュリティ基準のセットもさらに定義しており、そのためこれらの構造の作成に対する主な専門的入力の役割を果たす。CC は、CC に定義されているセキュリティ要件コンポーネントを可能な限り用いるという考えを中心に開発されているが、それらのコンポーネントはよく知られ、理解されている範囲を表している。図 8 に、これらの様々な構造間の関係を示す。

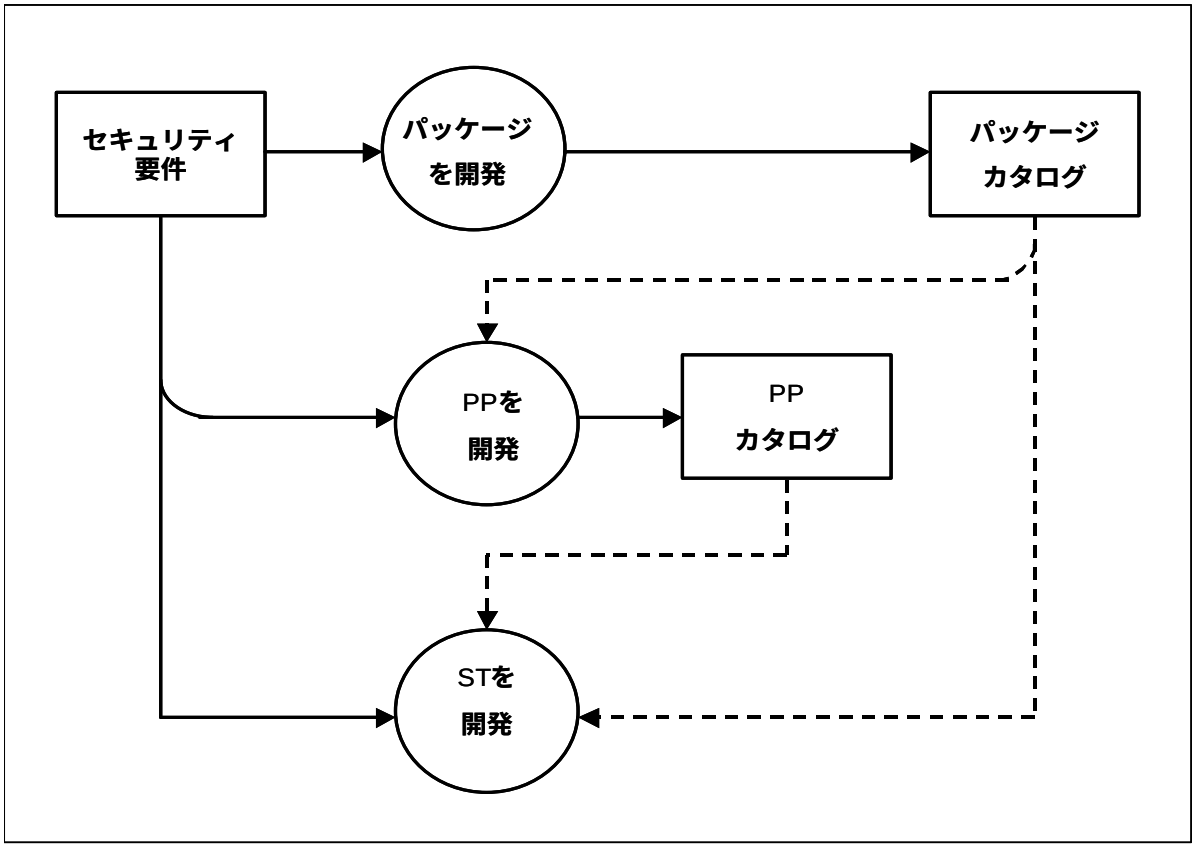

図 8　セキュリティ要件の使用

6.4.1.4.1　パッケージ

コンポーネントの組合せは、パッケージと呼ばれる。パッケージは、セキュリティ対策方針のうちの同一と見なし得るサブセットを満たす機能要件または保証要件のセットの表現を可能にする。パッケージは、再利用可能であること、及び識別された対策方針を満たすために有用かつ有効であることが分かっている要件を定義することを目的としている。パッケージは、より大きなパッケージ、PP、及び ST の構造内で用いることができる。

評価保証レベル（EAL）は、CC パート 3 に記述されている既定の保証パッケージである。EAL は、評価のための保証要件の基準セットである。各 EAL は、保証要件の一貫したセットを定義している。全体として、EAL は、CC の順序付けられた既定の保証尺度を形作っている。

6.4.1.1.2　プロテクションプロファイル

PP は、CC からのセキュリティ要件のセット、または明示的に規定されたセキュリティ要件のセットを含んでいるが、これには EAL（付加的に保証コンポーネントによって追加することも可能）を含めるべきである。PP は、セキュリティ対策方針のセットに完全に従う、TOE のセットに対するセキュリティ要件の実装に依存しない表現を可能にする。PP の目的は、再利用可能であること、及び機能と保証のいずれについても識別された対策方針を満たすために有用かつ有効であることが分かっている TOE 要件を定義することである。PP はまた、セキュリティ対策方針とセキュリティ要件の根拠も記述する。

PP は、利用者のコミュニティ、IT 製品開発者、またはそうした共通要件のセットの定義に関係のあるその他の関係者によって作成される可能性がある。PP は、特定のセキュリティニーズを参照する手段を消費者に提供し、そのニーズに照らしたさらに詳細な評価を容易にする。

6.4.1.4.3 セキュリティターゲット

ST は、セキュリティ要件のセットを含んでおり、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または保証コンポーネントを直接参照するか、または明示的に記述することによって作成することができる。ST は、識別された対策方針を満たすために有用かつ有効であると、評価によって認められた特定の TOE に対するセキュリティ要件の表現を可能にする。

ST は、セキュリティ要件とセキュリティ対策方針、及びそれぞれの根拠と併せて、TOE 要約仕様を含んでいる。ST は、TOE が提供するセキュリティに関するすべての関係者間の合意の基礎となる。

6.4.1.5 セキュリティ要件のソース

TOE のセキュリティ要件は、以下の入力を用いて構築することができる。

a) 既存の PP

ST に含める TOE セキュリティ要件は、既存の PP に含まれている要件の既存ステートメントによって適切に表現することもできるし、またはそのステートメントに従うことを目的とする。

既存の PP は、新規の PP の基礎として用いることができる。

b) 既存のパッケージ

PP または ST に含める TOE セキュリティ要件の一部は、使用可能なパッケージ内に既に表現されている可能性がある。

既定のパッケージのセットは、CC パート 3 で定義されている EAL である。PP または ST に含める TOE 保証要件は、CC パート 3 からの EAL を含めるべきである。

c) 既存の機能要件コンポーネントまたは保証要件コンポーネント

PP または ST に含める TOE 機能要件または TOE 保証要件は、CC パート 2 または CC 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することができる。

d) 拡張要件

PP または ST においては、CC パート 2 に含まれていない追加の機能要件、及び/または CC パート 3 に含まれていない追加の保証要件を用いることができる。

可能であれば、CC パート 2 及び CC パート 3 からの既存の要件資料を用いるべきである。既存の PP を用いることは、TOE が周知の有用性のニーズを満たし、それによってより広く受け入れられることを確実にする一助となろう。

6.4.2 評価の種類

6.4.2.1 PP の評価

PP の評価は、CC パート 3 に含まれている PP 評価基準に照らして実施する。この評価の目標は、PP が完全で一貫しており、かつ技術的にしっかりしており、評価対象の TOE に対する要件のステートメントとして用いるのに適していることを実証することである。

6.4.2.2 ST の評価

TOE に対する ST の評価は、パート 3 に含まれている ST 評価基準に照らして実施する。この評価の目標は 2 つある。まず 1 つは、ST が完全で一貫しており、かつ技術的にしっかりしており、したがって対応する TOE の評価の基礎として用いるのに適していることを実証することである。もう 1 つは、ST が PP への適合を主張している場合に、ST が PP の要件を適切に満たしていることを実証することである。

6.4.2.3 TOE の評価

TOE 評価は、実質的に完成した ST に基づいて、CC パート 3 に含まれている評価基準に照らして実施する。実質的に完成した ST とは、その後の評価プロセスにおける問題によるリスクを削減するものであり、評価スキームで受け入れ可能な程度で、かつ評価上の重大な問題が全く予見されない程度に、全ての節が完成している状態のものである。TOE 評価の結果は、TOE が評価済み ST に含まれているセキュリティ要件を満たしていることを実証することである。

7 コモンクライテリアの要件と評価結果

7.1 序説

この章は、PP 及び TOE の評価からの期待される結果を示す。PP または TOE の評価は、それぞれ評価済みの PP または TOE のカタログとなる。ST の評価は、TOE の評価の枠内で用いられる中間の結果となる。

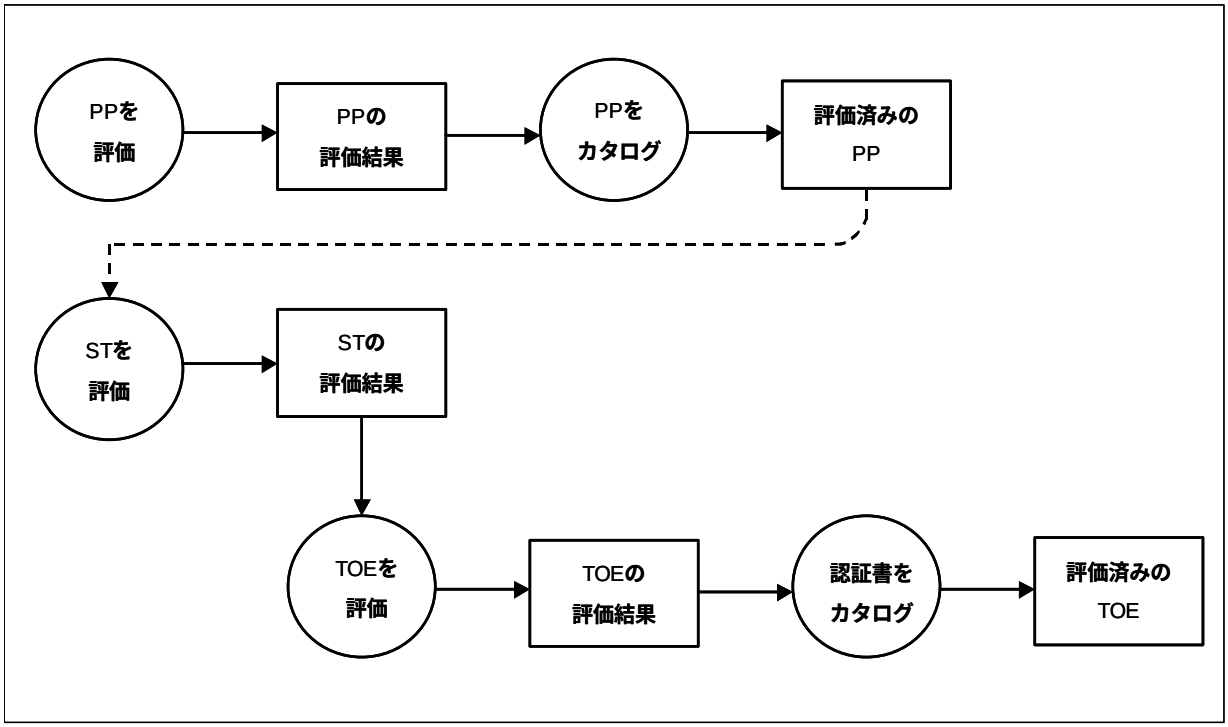

図 9 評価結果

評価は、IT セキュリティ評価の結果を表現するための完全に客観的な尺度がない場合でも、証拠と見なすことができる客観的で再現性のある結果をもたらすべきである。評価基準のセットが存在するということは、評価が意味のある結果をもたらし、評価監督機関間での評価結果に対する相互承認の技術的基礎を提供するのに必要な前提条件である。しかし、基準の適用は、客観的要素と主観的要素を共に含んでおり、したがって IT セキュリティの厳密かつ普遍的なレート付けは、無理である。

CC を基準にして行われるレート付けは、TOE のセキュリティ特性についての特定の種類の調査の成果を意味する。そうしたレート付けでは、特定の適用環境における使用への適合を保証するものでない。特定の適用環境への TOE の使用を承認するかどうかの判断は、評価結果を含め、多くのセキュリティ上の課題の検討に基づかれる。

7.2 PP 及び ST における要件

CC は、多くのコミュニティのニーズに対処することができる IT セキュリティ基準のセットを定義している。CC パート 2 に含まれているセキュリティ機能コンポーネント、及び CC パート 3 に含まれている EAL と保証コンポーネントは、よく知られ、理解されている範囲を表していることから、これらを用いることは、PP 及び ST において TOE に対する要件を表現するのに好ましい行動方針を意味するという考えを中心に、CC は作成されている。

CC は、完全な IT セキュリティ要件を表現するためには、規定されたカタログに含まれていない機能要件や保証要件が必要になるという可能性を認めている。こうした拡張した機能要件または保証要件を含める場合、以下の事項を適用するものとする。

a) PP または ST に含める拡張した機能要件または保証要件のすべては、適合性の評価及び実証が可能なように、明確かつ一意に表現しなければならない。モデルとして、既存の CC の機能コンポーネントまたは保証コンポーネントの表現の詳細度及び様式を用いなければならない。

b) 拡張した機能要件または保証要件を用いて得られた評価結果は、そのように注記しなければならない。

c) 拡張した機能要件または保証要件を PP または ST に組み込む場合、必要に応じて、CC パート 3 の APE クラスまたは ASE クラスに従わなければならない。

7.2.1 PP の評価結果

CC は、PP が完全で一貫しており、かつ技術的にしっかりしているため、評価対象の TOE に対する要件のステートメントとして用いるのに適していることを評価者が記述することを可能にする評価基準を含んでいる。

PP の評価の結果として、合否ステートメントを記述しなければならない。評価の結果、合格ステートメントを記述された PP は、登録簿に登録される資格が与えられなければならない。

7.3 TOE に対する要件

CC は、TOE が ST に示されているセキュリティ要件を満たしているかどうかを評価者が決定することを可能にする評価基準を含んでいる。TOE の評価に際して CC を用いることにより、評価者は以下のことをステートメントすることが可能になる。

a) 明記された TOE のセキュリティ機能が機能要件を満たしており、その結果、TOE のセキュリティ対策方針を満たすのに有効であるかどうか

b) 明記された TOE のセキュリティ機能が適切に実装されているかどうか

CC に示されているセキュリティ要件は、IT セキュリティ評価基準の有効と認められた適用範囲を定義する。そのセキュリティ要件が CC から抜粋された機能要件と保証要件のみによって示される TOE は、CC に照らして評価することができる。EAL に含まれていない保証パッケージを用いる場合は、正当性を示さなければならない。

ただし、場合によっては、TOE は、CC に直接示されていないセキュリティ要件を満たすことが必要なこともある。CC ではそうした TOE を評価する必要性を認めているが、追加の要件は、CC の認められた適用範囲外であることから、そうした評価の結果には必要に応じて注記しなければならない。そうした注記は、関与する評価監督機関による評価結果の普遍的な承認は、得られない可能性がある。

TOE 評価の結果は、CC への適合についてのステートメントを含めなければならない。TOE のセキュリティを記述するために、CC の用語を用いれば、一般的に TOE のセキュリティ特性の比較が可能になる。

7.3.1 TOE の評価結果

TOE 評価の結果は、TOE がその要件に適合していることの信頼の範囲を記述するステートメントをしなければならない。

TOE の評価の結果として、合否ステートメントを記述しなければならない。評価の結果、合格ステートメントを記述された TOE は、登録簿に登録される資格が与えられなければならない。評価の結果には、「適合結果」も含まれなければならない。

7.4 適合結果

適合結果は、評価に合格したTOEまたはPP によって満たされる要件の集合の源を識別する。この適合結果には、CCパート2（機能要件）、CCパート3（保証要件）及びもし該当するならば、あらかじめ定義された一連の要件（例えば、EAL、プロテクションプロファイル）に関して示される。

適合結果は、以下のうちの1つからなる。

a) CC**パート2 適合**－ PP またはTOE は、その機能要件がCCパート2 の機能コンポーネントのみに基づく場合、CCパート2 適合となる。

b) CC**パート2 拡張**－ PP またはTOE は、その機能要件がCCパート2 にない機能コンポーネントを含む場合、CCパート2 拡張となる。

これに、下記のうちの1 つが加えられる。

a) CC**パート3 適合**－ PP またはTOE は、その保証要件がCCパート3 の保証コンポーネントのみに基づく場合、CCパート3 適合となる。

b) CC**パート3 拡張**－ PP またはTOE は、その保証要件がCCパート3 にない保証要件を含む場合、CCパート3 拡張となる。

さらに、適合結果には、一連の定義された要件に関して作成されたステートメントが含まれるかもしれない。そのような場合には以下のうちの1 つからなる。

a) ***パッケージ名*適合**－ PP またはTOE は、その要件（機能または保証）が適合結果に記載されているパッケージにあるすべてのコンポーネントを含む場合、あらかじめ定義され、名前を付けられた機能及び/または保証パッケージ（例えば、EAL）に適合している。

b) ***パッケージ名*追加**－ PP またはTOE は、その要件（機能または保証）が適合結果に記載されているパッケージにあるすべてのコンポーネントの適切なスーパーセットであるならば、あらかじめ定義され、名前を付けられた機能及び/または保証パッケージ（例えば、EAL）に関する追加となる。

最後に、適合結果には、プロテクションプロファイルに関して作成されたステートメントが含まれるかもしれない。その場合には下記が含まれる。

a) ***PP*適合**－ TOE は、適合結果の一部として記載されている特定のPP(s)を満たしている。

7.5 TOE の評価結果の使用

IT 製品及びシステムは、評価結果の使用に関して異なる。図 10 に、評価結果の処理オプションを示す。製品は、運用システムが実現されるまで、完成度を逐次高めながら、評価及びカタログ化を行うことができ、運用システムが実現された時点で、システムの認定として評価を受けることができる。

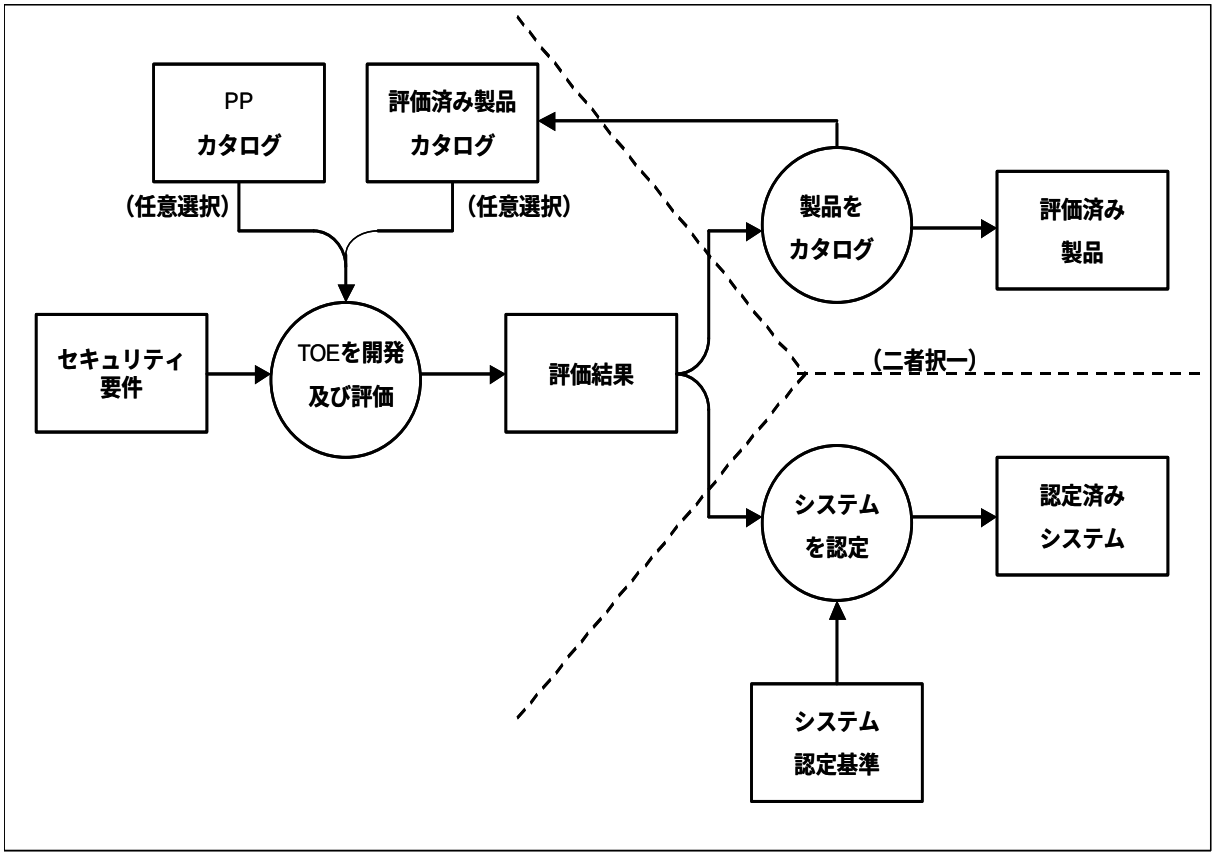

図 10 TOE の評価結果の使用

TOE は、組み込まれるすべての評価済み製品のセキュリティ特性、及び参照される PP を考慮に入れた要件に即して開発される。その後の TOE の評価により、評価の結論を文書化した評価結果のセットに至る。

より汎用的な使用を目的とする IT 製品を評価した後は、評価の結論の要約を評価済み製品のカタログに記載し、それによってセキュアな IT 製品の使用を求めるより広範な市場がその要約を利用できるようにする。

TOE が、評価対象の導入済み IT システムに組み込まれているか、または組み込まれる予定である場合、TOE の評価結果は、システム認定者が利用できるであろう。それにより認定者は、CC の評価を必要とする組織固有の認定基準を適用する場合、CC の評価結果を検討することができる。CC の評価結果は、システム運用のリスクを受け入れるかどうかの判断をもたらす認定プロセスへの 1 つの入力となる。

A　プロテクションプロファイルの仕様

(規定)

A.1　概要

PP は、TOE のカテゴリに関する実装に依存しない IT セキュリティ要件のセットを定義するものである。そうした TOE は、IT セキュリティに対する消費者共通のニーズを満たすことを目的とする。したがって、消費者は PP の作成または参照を行うことにより、特定の TOE を参照せずに IT セキュリティのニーズを表現することができる。

この附属書は、PP の記述形式に対する要件を記載する。これらの要件は、CC パート 3 の第 9 章に記載されている保証クラス APE に、PP の評価に用いられる保証コンポーネントの形で含まれている。

A.2　プロテクションプロファイルの内容

A.2.1　内容と提示

PP は、この附属書に記述されている内容要件に従っていなければならない。PP は、PP 利用者が容易に入手できない可能性のある他の資料の参照を極力抑えた利用者用文書として提示する必要がある。根拠は、必要に応じて別々に提示することができる。

PP の内容を図 11 に示すが、PP 文書の構造のアウトラインを構成するときには、これを用いるべきである。

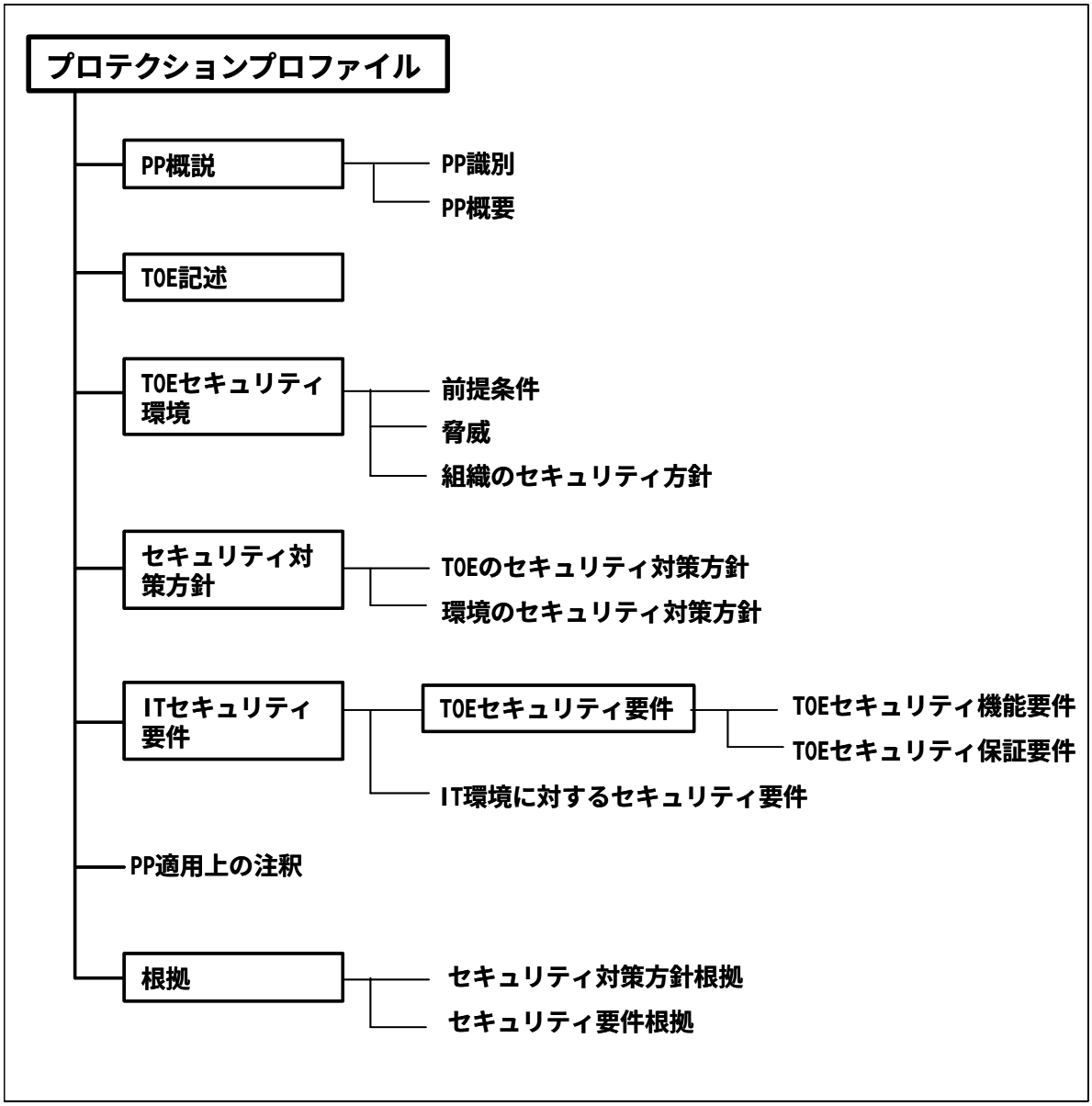

図 11　プロテクションプロファイルの内容

A.2.2　PP 概説

PP 概説は、PP 登録を行うのに必要な以下の文書管理情報及び概要情報を含めなければならない。

a) PP **識別**は、PP を識別、カタログ化、登録、及び相互参照を行うのに必要なラベル情報及び記述的情報を含めなければならない。

b) PP **概要**は、PP について叙述的形式で要約しなければならない。この概要は、その PP が関心の対象となるかどうかを PP の潜在的利用者が判断するのに十分に詳細であるべきである。また、概要は、PP カタログ及び登録で用いる抄録として単独に利用可能であるべきである。

A.2.3 TOE 記述

PP のこの部分は、TOE についてそのセキュリティ要件の理解の一助となるように記述しなければならない、また TOE の製品種別及び一般的 IT 機能についても示さなければならない。

TOE 記述では、その評価の範囲を規定する。TOE 記述に提示された情報は、評価過程において矛盾を識別するために用いられることになる。PP では通常、特定の実装については言及しないので、記述する TOE 機能は想定でよい。TOE が、その主な機能がセキュリティである製品またはシステムの場合、PP のこの部分を用いて、そうした TOE がふさわしいような広範な適用範囲を記述することができる。

A.2.4 TOE セキュリティ環境

TOE **セキュリティ環境**のステートメントは、TOE が意図する使用環境セキュリティの側面、及び期待される使用方法を記述しなければならない。このステートメントには、以下のことを含めなければならない。

a) **前提条件**の記述は、TOE が使用される環境、または意図されている使用環境についてのセキュリティの側面を記述しなければならない。これには、以下の情報を含めなければならない。

   意図される利用、潜在的な資産価値、考えられる使用制限などの側面を含む、TOE の使用目的に関する情報

   物理的、人的、及び接続性の側面を含む、TOE の使用環境に関する情報

b) **脅威**の記述は、TOE またはその環境において固有の保護が必要な資産に対する脅威をすべて含めなければならない。その環境において直面すると考えられるすべての脅威をリストする必要はなく、TOE のセキュアな運用に関連するもののみをリストすることができることに注意のこと。

   脅威は、識別された脅威エージェント、攻撃、及び攻撃対象の資産の観点から記述されなければならない。脅威エージェントは、技能、利用可能資源、及び動機のような側面を扱うことによって記述されなければならない。攻撃は、攻撃方法、つけ込まれる脆弱性、及び機会のような側面を扱うことによって記述されなければならない。

   組織のセキュリティ方針及び前提条件のみからセキュリティ対策方針を導き出す場合、脅威の記述は省略することができる。

c) **組織のセキュリティ方針**の記述では、TOE が従わなければならない組織のセキュリティ方針ステートメントまたは規則を識別し、また必要に応じて説明を加えなければならない。明確なセキュリティ対策方針を定める際に用いることができるような形で個々の方針ステートメントを提示するには、説明や解説が必要になろう。

   脅威及び前提条件のみからセキュリティ対策方針を導き出す場合は、組織のセキュリティ方針の記述を省略することができる。

TOE が物理的に分散している場合は、TOE 環境の個別領域ごとにセキュリティ環境の側面（前提条件、脅威、組織のセキュリティ方針）を考察する必要があろう。

A.2.5 セキュリティ対策方針

セキュリティ対策方針のステートメントは、TOE及びその環境に対するセキュリティ対策方針を定義しなければならない。セキュリティ対策方針は、識別されたセキュリティ環境の側面にすべ

て対処したものでなければならない。セキュリティ対策方針は、記述された意図を反映したものでなければならず、また識別されたすべての脅威に対抗し、識別されたすべての組織のセキュリティ方針及び前提条件をカバーするのに適したものでなければならない。脅威は1つまたはそれ以上のTOEの対策方針、1つまたはそれ以上の環境の対策方針、またはこれらの組み合わせによって対抗される。以下のカテゴリの対策方針が識別されなければならない。注： 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する場合は、関連する対策方針をカテゴリごとに記述しなければならない。

a) TOE **のセキュリティ対策方針**は、明確に記述する必要があり、また TOE が対抗すべき識別された脅威、及び/または TOE が満たすべき組織のセキュリティ方針の側面にまでさかのぼれなければならない。

b) **環境のセキュリティ対策方針**は、明確に記述する必要があり、また TOE が完全には対抗できない識別された脅威、及び/または TOE が完全には満たしていない組織のセキュリティ方針または前提条件の側面にまでさかのぼれなければならない。

ただし、環境のセキュリティ対策方針は、TOE セキュリティ環境のステートメントの前提条件の全部または一部を再掲することができる。

A.2.6 IT **セキュリティ要件**

PP のこの部分は、TOE またはその環境が満たしていなければならない詳細な IT セキュリティ要件を定義する。IT セキュリティ要件は、以下のとおりに記述しなければならない。

a) 同一要件の異なる側面をカバーする必要があるとき(例えば、2 種類以上の利用者の識別)、各側面をカバーする同一のCCパート2 コンポーネントの反復使用(すなわち、繰返し操作を適用すること)が可能である。**TOE セキュリティ要件**のステートメントは、TOE に対するセキュリティ対策方針を満たすために、TOE 及びその評価の裏づけとなる証拠が満たす必要があるセキュリティ機能要件及びセキュリティ保証要件を定義しなければならない。TOE セキュリティ要件は、以下のとおりに記述しなければならない。

1) 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 から該当する機能コンポーネントを抜き出して、TOE に対する機能要件を定義するべきである。

TOE セキュリティ保証要件に AVA_SOF.1 が含まれている場合（例えば、EAL2 以上）、TOE セキュリティ機能要件のステートメントには、確率的または順列的メカニズム（例えば、パスワードやハッシュ関数）によって実現される TOE セキュリティ機能の最低限の強度レベルを含めなければならない。そうした機能は、すべて、この最低限のレベルを満たしていなければならない。このレベルは、SOF-基本、SOF-中位、SOF-高位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と一致するものでなければならない。任意選択で、特定の TOE 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特定の機能強度の数値尺度を定義することができる。

TOE セキュリティ機能強度評価（AVA_SOF.1）の一環として、TOE が個別の TOE セキュリティ機能に対する強度主張、及び全体として最低限の強度レベルを満たしているかどうかが評定される。

2) TOE **セキュリティ保証要件**のステートメントでは、CC パート 3 の保証コンポーネントにて用意された EAL のうちから 1 つの保証要件を記述すべきである。PP はまた、CC パート 3 からのものでない追加の保証要件を明示的に記述することにより、EAL を拡張することもできる。

b) **IT 環境に対するセキュリティ要件**の任意選択のステートメントは、TOE の IT 環境が満たすべき IT セキュリティ要件を識別しなければならない。PP のこの部分における要件は、CC パート 2 及び CC パート 3 から引き出すことができ、もし、そうならば TOE ではなく、IT 環境が要件を満たさねばならないと明確に指摘するために、言い直すべきである。このような言い直しは、詳細化の特別なケースであり、修正された CC コンポーネントに関連する評定要件に関わるサブジェクトではない。TOE が IT 環境に対して仮定された依存性を持たない場合、PP のこの部分は省略することができる。

c) 以下の**一般条件**を、TOE 及びその IT 環境に対するセキュリティ機能要件と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。

1) すべての IT セキュリティ要件は、CC パート 2 または CC パート 3 からの適用可能な部分から抜き出したセキュリティ要件コンポーネントを参照して記述されるべきである。そのセキュリティ要件の全部または一部に対して、どれも容易に適用できる CC パート 2 または CC パート 3 の要件コンポーネントがない場合、PP はそれらの要件を、CC を参照することなしに明示的に記述することができる。

2) TOE セキュリティ機能要件または TOE セキュリティ保証要件の明示的なステートメントは、準拠性の評価及び実証が可能な形で、明確かつ一意に表現しなければならない。モデルとして、既存の CC 機能要件または CC 保証要件の表現の詳細度及び様式を用いなければならない。

3) 必要な操作（割付または選択）を指定する要件コンポーネントを選択する場合、PP は、セキュリティ対策方針が満たされていることを実証するのに必要な詳細度まで要件を拡充するために、それらの要件を使用しなければならない。すべての必要な操作のうち、PP において実行しないものは、そのように示さなければならない。

4) 要件コンポーネントに対して操作を行うことにより、TOE セキュリティ要件ステートメントは、特定のセキュリティメカニズムの使用の規定または禁止を、必要に応じて任意に行うことができる。

5) IT セキュリティ要件間のすべての依存性は、満たされるべきである。依存性は、関連する要件を TOE セキュリティ要件に含めることにより、または環境に対する要件として、満たすことができる。

A.2.7 適用上の注釈

PP のこの任意選択部分は、TOE の構築、評価、または使用に関連する、または有用と考えられる追加の補足情報を含めることができる。

A.2.8 根拠

PP のこの部分は、PP 評価に用いる証拠を提示する。この証拠は、PP が完全で理路整然とした要件のセットであるということと、適合した TOE がセキュリティ環境において有効な IT セキュリティ対抗策のセットを提供するということの主張の裏付けとなる。根拠には、以下のことを含めなければならない。

a) **セキュリティ対策方針根拠**は、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の側面にまでたどれることができ、かつそれらをカバーするのに適していることを実証しなければならない。

b) **セキュリティ要件根拠**は、セキュリティ要件（TOE 及び環境）のセット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にまでたどれることを実証しなければならない。以下のことが実証されなければならない。

1) TOE 及び IT 環境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

2) セキュリティ要件のセットが一体となって、互いに補完し、かつ内部的に一貫した全体を形成すること

3) セキュリティ要件の選択が正当化されていること。以下のいずれかの条件に当てはまる場合は必ず、明確に正当化しなければならない。

   ⅰ) CC パート 2 または CC パート 3 に含まれていない要件の選択
   ⅱ) EAL を含んでいない保証要件の選択
   ⅲ) 依存性を満たしていない

4) PP において選択した機能強度レベルが、明示された機能強度の主張と共に、TOE のセキュリティ対策方針と一貫していること

この膨大となる可能性のある資料は、すべての PP 利用者にとって適切または有用であるとは限らないことから、別々に分割することができる。

B　セキュリティターゲットの仕様

(規定)

B.1　概要

ST は、識別された TOE の IT セキュリティ要件を記載するものであり、また記述された要件を満たすためにその TOE が提供する機能及び保証のセキュリティ手段を明記するものである。

TOE の ST は、TOE のセキュリティ特性及び評価範囲に関する開発者、評価者、及び該当する場合は消費者間での合意の基礎となる。ST の対象読者は、TOE の製造及び評価に責任を持つ者に限定されず、場合によって TOE の管理、販売、購入、導入、設定、運用、及び利用に責任を持つ者も含まれることがある。

ST は、1 つまたは複数の PP の要件、またはそれに対する適合の主張を組み込むことができる。B.2 節の最初に必要な ST 内容を定義しているが、そうした PP 適合の主張の影響を考慮に入れていない。必要な ST 内容に対する PP 適合の主張の影響については、B.2.8 節で扱う。

この附属書は、ST の記述形式に対する要件を記載する。これらの要件は、CC パート 3 の第 10 章に記載されている保証クラス ASE に、ST の評価に用いられる保証コンポーネントの形で含まれている。

B.2　セキュリティターゲットの内容

B.2.1　内容と提示

ST は、この附属書に記述されている内容要件に従っていなければならない。ST は、ST 利用者が容易に入手できない可能性のある他の資料の参照を極力抑えた利用者用文書として提示する必要がある。根拠は、必要に応じて別々に提示することができる。

ST の内容を図 10 に示すが、ST の構造のアウトラインを構成するときには、これを用いるべきである。

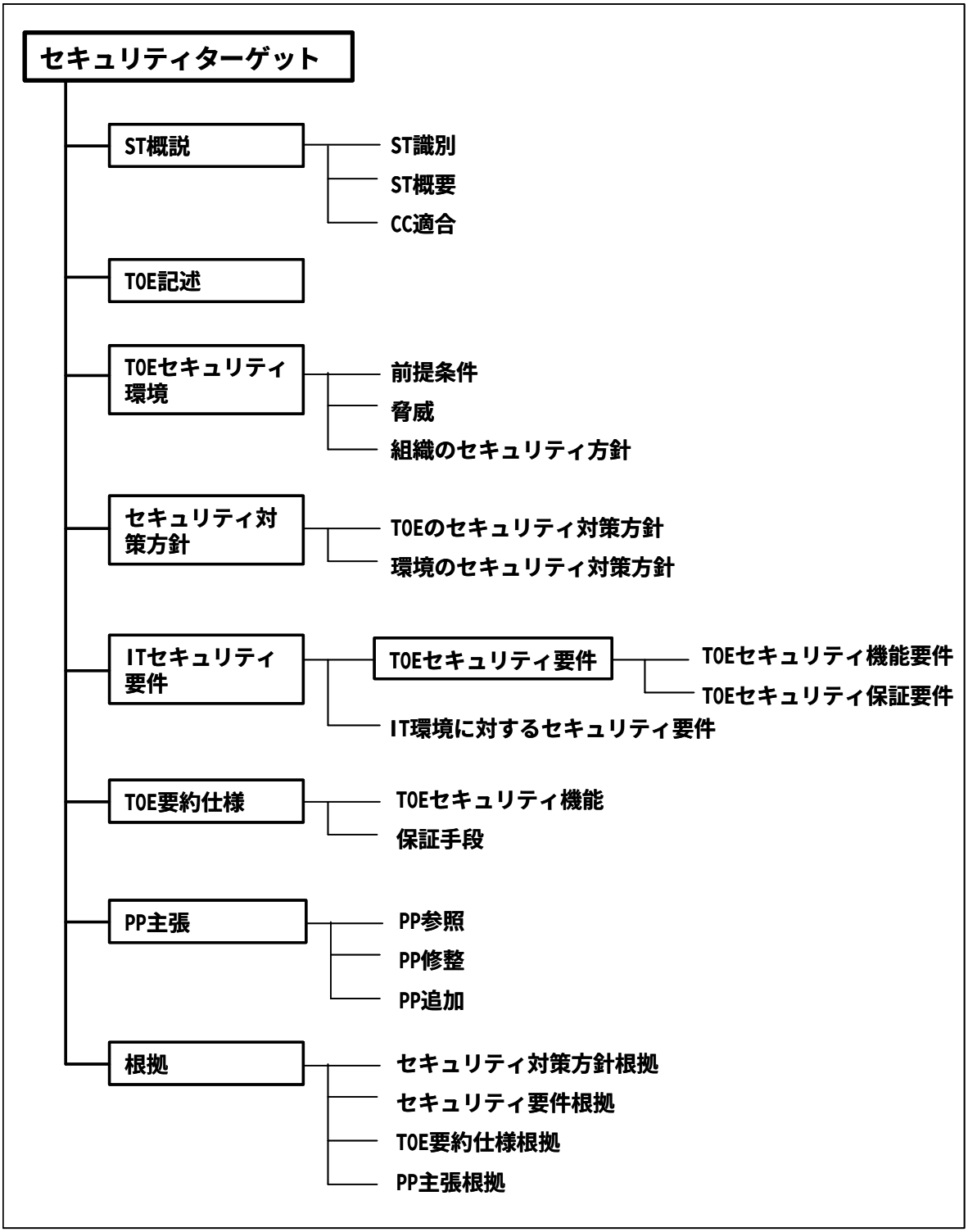

図 12　セキュリティターゲットの内容

B.2.2 ST 概説

ST 概説は、以下の文書管理情報及び概要情報を含めなければならない。

a) ST **識別**は、ST 及びその対象となる TOE の管理及び識別に必要なラベル情報及び記述的情報を含めなければならない。

b) ST **概要**は、ST について叙述的形式で要約しなければならない。この概要は、その TOE が関心の対象となるかどうかを TOE の潜在的消費者が判断するのに十分に詳細であるべきである。また、概要は、評価済み製品リストに記載するための抄録として単独に利用可能であるべきである。

c) CC **適合の主張**は、このパート 1 の 7.4 節で明らかにしているとおり、TOE の CC 適合について、あらゆる評価可能な主張を記述しなければならない。

B.2.3 TOE 記述

ST のこの部分は、TOE についてそのセキュリティ要件の理解の一助となるように記述しなければならない、また製品またはシステムの種別についても示さなければならない。TOE の範囲及び境界は、物理面（ハードウェア、及び/またはソフトウェアコンポーネント/モジュール）と論理面（TOE が提供する IT 及びセキュリティ機能）の両方について、一般的な表現で記述しなければならない。

TOE 記述では、その評価の範囲を規定する。TOE 記述に提示された情報は、評価過程において矛盾を識別するために用いられることになる。TOE が、その主な機能がセキュリティである製品またはシステムの場合、ST のこの部分を用いて、そうした TOE がふさわしいような広範な適用範囲を記述することができる。

B.2.4 TOE セキュリティ環境

TOE **セキュリティ環境**のステートメントは、TOE が意図する使用環境のセキュリティの側面、及び期待される使用方法を記述しなければならない。このステートメントには、以下のことを含めなければならない。

a) **前提条件**の記述は、TOE が使用される環境、または意図されている使用環境についてのセキュリティの側面を記述しなければならない。これには、以下の情報を含めなければならない。

意図される利用、潜在的な資産価値、考えられる使用制限などの側面を含む、TOE の使用目的に関する情報

物理的、人的、及び接続性の側面を含む、TOE の使用環境に関する情報

b) **脅威**の記述は、TOE またはその環境において固有の保護が必要な資産に対する脅威をすべて含めなければならない。その環境において直面すると考えられるすべての脅威をリストする必要はなく、TOE のセキュアな運用に関連するもののみをリストすることができることに注意のこと。

脅威は、識別された脅威エージェント、攻撃、及び攻撃対象の資産の観点から記述されなければならない。脅威エージェントは、技能、利用可能資源、及び動機のような側面を扱うことによって記述されなければならない。攻撃は、攻撃方法、つけ込まれる脆弱性、及び機会のような側面を扱うことによって記述されなければならない。

組織のセキュリティ方針及び前提条件のみからセキュリティ対策方針を導き出す場合、脅威の記述は省略することができる。

c) **組織のセキュリティ方針**の記述は、TOE が従わなければならない組織のセキュリティ方針ステートメントまたは規則を識別し、また必要に応じて説明を加えなければならない。明確なセキュリティ対策方針を定める際に用いることができるような形で個々の方針ステートメントを提示するには、説明や解説が必要になろう。

脅威及び前提条件のみからセキュリティ対策方針を導き出す場合は、組織のセキュリティ方針の記述を省略することができる。

TOE が物理的に分散している場合は、TOE 環境の個別領域ごとにセキュリティ環境の側面（前提条件、脅威、組織のセキュリティ方針）を考察する必要があろう。

B.2.5 セキュリティ対策方針

セキュリティ対策方針のステートメントは、TOE及びその環境に対するセキュリティ対策方針を定義しなければならない。セキュリティ対策方針は、識別されたセキュリティ環境の側面にすべて対処したものでなければならない。セキュリティ対策方針は、記述された意図を反映したものでなければならず、また識別されたすべての脅威に対抗し、識別されたすべての組織のセキュリティ方針及び前提条件をカバーするのに適したものでなければならない。脅威は1つまたはそれ以上のTOEの対策方針、1つまたはそれ以上の環境の対策方針、またはこれらの組み合わせによって対抗される。以下のカテゴリの対策方針が識別されなければならない。注： 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する場合、関連する対策方針をカテゴリごとに記述しなければならない。

a) TOE **のセキュリティ対策方針**は、明確に記述する必要があり、また TOE が対抗すべき識別された脅威、及び/または TOE が満たすべき組織のセキュリティ方針の側面にまでさかのぼれなければならない。

b) **環境のセキュリティ対策方針**は、明確に記述する必要があり、また TOE が完全には対抗できない識別された脅威、及び/または TOE が完全には満たしていない組織のセキュリティ方針または前提条件の側面にまでさかのぼれなければならない。

ただし、環境のセキュリティ対策方針は、TOE セキュリティ環境のステートメントの前提条件の全部または一部を再掲することができる。

B.2.6 IT セキュリティ要件

ST のこの部分は、TOE またはその環境が満たしていなければならない詳細な IT セキュリティ要件を定義する。IT セキュリティ要件は、以下のとおりに記述しなければならない。

a) 同一要件の異なる側面をカバーする必要があるとき(例えば、2 種類以上の利用者の識別)、各側面をカバーする同一のパート 2 コンポーネントの反復使用(すなわち、繰返し操作を適用すること)が可能である。TOE **セキュリティ要件**のステートメントは、TOE に対するセキュリティ対策方針を満たすために、TOE 及びその評価の裏付けとなる証拠が満たす必要があるセキュリティ機能要件及びセキュリティ保証要件を定義しなければならない。TOE セキュリティ要件は、以下のとおりに記述しなければならない。

1) TOE **セキュリティ機能要件**のステートメントは、パート 2 から該当する機能コンポーネントを抜き出して、TOE に対する機能要件を定義するすべきである。

TOE セキュリティ保証要件に AVA_SOF.1 が含まれている場合（例えば、EAL2 以上）、TOE セキュリティ機能要件のステートメントには、確率的または順列的メカニズム（例えば、パスワードやハッシュ関数）によって実現される TOE セキュリティ機能の最低限の強度レベルを含めなければならない。そうした機能は、すべて、この最低限のレベルを満たしていなければならない。このレベルは、SOF-基本、SOF-中位、SOF-高位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と一致するものでなければならない。任意選択で、特定の TOE 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特定の機能強度の数値尺度を定義することができる。

TOE セキュリティ機能強度評価（AVA_SOF.1）の一環として、TOE が個別の TOE セキュリティ機能に対する強度主張、及び全体として最低限の強度レベルを満たしているかどうかが評定される。

2) TOE **セキュリティ保証要件**のステートメントは、パート 3 の保証コンポーネントにて用意された EAL のうちから 1 つの保証要件を記述すべきである。ST はまた、パート 3 からのものでない追加の保証要件を明示的に記述することにより、EAL を拡張することもできる。

b) **IT 環境に対するセキュリティ要件**の任意選択のステートメントは、TOE の IT 環境が満たすべき IT セキュリティ要件を識別しなければならない。ST のこの部分における要件は CC パート 2 及びパート 3 から引き出すことができ、もし、そうならば TOE ではなく、IT 環境が要件を満たさねばならないと明確に指摘するために、言い直すべきである。このような言い直しは、詳細化の特別なケースであり、修正された CC コンポーネントに関連する評定要件に関わるサブジェクトではない。TOE が IT 環境に対して仮定された依存性を持たない場合、ST のこの部分は省略することができる。

c) 以下の**一般条件**を、TOE 及びその IT 環境に対するセキュリティ機能要件と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。

1) すべての IT セキュリティ要件は、CC パート 2 または CC パート 3 からの適用可能な部分から抜き出したセキュリティ要件コンポーネントを参照して記述されるべきである。そのセキュリティ要件の全部または一部に対して、どれも容易に適用できる CC パート 2 または CC パート 3 の要件コンポーネントがない場合、ST はそれらの要件を、CC を参照することなしに明示的に記述することができる。

2) TOE セキュリティ機能要件または TOE セキュリティ保証要件の明示的なステートメントは、準拠性の評価及び実証が可能な形で、明確かつ一意に表現しなければならない。モデルとして、既存の CC 機能要件または CC 保証要件の表現の詳細度及び様式を用いなければならない。

3) 必要な操作は、セキュリティ対策方針が満たされていることを実証するのに必要な詳細度まで要件を拡充しなければならない。すべての要件コンポーネントに対して指定された操作は、実行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、満たされるべきである。依存性は、関連する要件を TOE セキュリティ要件に含めることにより、または環境に対する要件として、満たすことができる。

B.2.7 TOE **要約仕様**

TOE 要約仕様は、TOE に対するセキュリティ要件を具体的に定義しなければならない。この仕様は、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しなければならない。場合によっては、TOE 要約仕様の一部として提供される機能情報は、ADV_FSP 要件の一部として TOE に関して提供される情報とまったく同じになる可能性があることに注意のこと。

TOE 要約仕様は、以下のことを含めなければならない。

a) TOE**セキュリティ機能のステートメント**は、ITセキュリティ機能をカバーしていなければならず、その機能がTOEセキュリティ機能要件をどのように満たしているかを明示しなければならない。このステートメントには、どの機能がどの要件を満たしているか、ならびにすべての要件が満たされていることを明確に示す、機能と要件の双方向の対応関係を含めなければならない。各セキュリティ機能は、少なくとも1つのTOEセキュリティ機能要件に寄与していなければならない。

   1) IT セキュリティ機能は、その目的を理解するのに必要最小限の詳細度をもって非形式的に定義しなければならない。

   2) ST に含めるセキュリティメカニズムへのすべての参照は、各機能の実装にどのセキュリティメカニズムが用いられるかが分かるように、関連するセキュリティ機能にまでたどれなければならない。

   3) TOE 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（例えば、パスワードやハッシュ関数）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なければならない。そうした機能のメカニズムが故意の攻撃、または偶発的な攻撃によって侵害される可能性は、TOE のセキュリティに関連するものとする。これらの機能のそれぞれについて TOE セキュリティ機能強度主張を行わなければならない。識別された各機能の強度は、SOF-基本、SOF-中位、SOF-高位として、または任意に定義した特定の数値尺度として決定し、主張しなければならない。

b) **保証手段のステートメント**は、記述された保証要件を満たしていると主張する TOE の保証手段を明示する。保証手段は、どの対策がどの要件の満足に寄与しているかが分かるように、保証要件にまでたどれなければならない。

   適切な場合には、保証手段の定義は、関連する品質計画、ライフサイクル計画、または管理計画を参照して行うことができる。

B.2.8 PP **主張**

ST は、TOE が 1 つ（または複数）の PP の要件に適合していることを任意に主張することができる。PP への適合を主張する場合、その主張を実証するのに必要な説明、根拠、及び裏付けとなるその他の資料を記述した PP **主張**ステートメントを ST に含めなければならない。

ST における TOE の対策方針及び要件のステートメントの内容と提示は、TOE に関して行う PP 主張に影響される可能性がある。ST に対する影響は、主張する各 PP ごとに以下のケースを検討することにより、その要約を示すことができる。

a) PP への適合を主張しない場合は、この附属書に記述されているとおりに、TOE の対策方針及び要件の完全な提示がされるべきである。この場合、PP 主張は含めない。

b) ST において、さらに必要条件を必要とすることなく PP の要件への適合のみを主張する場合、TOE の対策方針及び要件の定義や正当化を行うには、PP を参照するだけで十分である。PP の内容を再掲する必要はない。

c) ST において、PP の要件への適合を主張するものの、その PP にさらに必要条件を要求する場合、必要条件のための PP の要件が満たされていることを ST で明らかにしなければならない。そうした状況は通常、PP に未完結の操作が含まれている場合に生じる。このような状況では、ST において特定の要件を参照することはできるが、操作は ST において完了しなければならない。状況によって、操作を行うべき要件がかなりの数に上る場合は、分かりやすくするために PP の内容を改めて ST に記述する方が望ましいこともある。

d) ST において、PP の要件への適合を主張するものの、対策方針及び要件をさらに追加することによってその PP を拡張する場合、ST においてそれらの追加を定義しなければならないが、PP の対策方針及び要件を定義するには PP 参照を行うだけで十分である。状況によって、追加がかなりの数に上る場合は、分かりやすくするために PP の内容を改めて ST に記述する方が望ましいこともある。

e) ST において、PP への部分的な適合を主張するケースは、CC の評価では認められない。

CC は、PP の対策方針及び要件の再記述、または参照の選択に関して規定していない。基本的な要件は、ST の評価が可能であり、ST が TOE 評価の許容し得る基礎となり、しかも主張される PP に対する追跡性を明確にするような完全で、明白で、及び曖昧さがないことを、ST の内容が備えていることである。

PP への適合を主張する場合、PP 主張ステートメントには主張する各 PP ごとに以下の資料を含めなければならない。

a) PP **参照**ステートメントは、適合を主張する PP を識別し、その主張に関して必要と思われる追加説明をしなければならない。正当な主張は、TOE が PP の要件をすべて満たしているということを意味する。

b) PP **修整**ステートメントは、PP に対して許容された操作を満たすか、そうでなければ PP の要件をさらに適させる IT セキュリティ要件ステートメントを識別しなければならない。

c) PP **追加**ステートメントは、PP の対策方針及び要件に追加する TOE の対策方針及び要件ステートメントを識別しなければならない。

B.2.9 適用上の注釈

ST のこのオプション部分には、ST の理解に関連がある、または有用だと考えられる追加の情報が含まれている。ST がPP の要件に準拠することを主張する場合、PP適用上の注釈節に含まれているある情報を、ST の他の章に記載することが、適切である場合があることに留意する。例えば、TOE の構造に関する情報は、おそらく分離した適用上の注釈節よりも、TOE 要約仕様またはST 根拠に、より適切に提示される。ST の評価をより容易にするために、この附属書に概説されているST の提示の構造は規定ではないので、評価に関連する要素を含む適用上の注釈は、その評価の証拠を提供するST の節の一部として提供することを推奨する。

B.2.10 根拠

ST のこの部分は、ST 評価に用いる証拠を提示する。この証拠は、ST が完全で理路整然とした要件のセットであるということ、適合したTOE がセキュリティ環境において有効なIT セキュリティ

対抗策のセットを提供するということ、ならびに TOE 要約仕様がその要件に対処したものであるということの主張の裏付けとなる。また、PP 適合の主張が正当であることの実証にもなる。根拠には、以下のことを含めなければならない。

a) **セキュリティ対策方針根拠**は、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の側面にまでたどれることができ、かつそれらをカバーするのに適していることを実証しなければならない。

b) **セキュリティ要件根拠**は、セキュリティ要件（TOE 及び環境）のセット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にまでたどれることを実証しなければならない。以下のことが実証されなければならない。

   1) TOE 及び IT 環境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

   2) セキュリティ要件のセットが一体となって、互いに補完し、かつ内部的に一貫した全体を形成すること

   3) セキュリティ要件の選択が正当化されていること。以下のいずれかの条件に当てはまる場合は必ず、明確に正当化しなければならない。

      ⅰ) CC パート 2 または CC パート 3 に含まれていない要件の選択
      ⅱ) EAL に含まれていない保証要件の選択
      ⅲ) 依存性を満たしていない

   4) ST において選択した機能強度レベルが、明示された機能強度の主張と共に、TOE のセキュリティ対策方針と一貫していること

c) TOE **要約仕様根拠**は、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。以下のことが実証されなければならない。

   1) 明記された TOE の IT セキュリティ機能の組合せが、TOE セキュリティ機能要件を満たすために一体となって働くこと

   2) TOE 機能強度の主張が正当であること、またはそうした主張が不要であるという主張が正当であること

   3) 記述された保証手段が保証要件に従っているという主張が正当化されていること

   根拠のステートメントは、セキュリティ機能の定義の詳細度と一致する詳細度で提示しなければならない。

d) PP **主張根拠**ステートメントは、ST と適合を主張する 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 への適合を主張しない場合、または ST のセキュリティ対策方針及びセキュリティ要件が、主張する PP のそれらとまったく同じである場合、ST のこの部分は省略することができる。

この膨大となる可能性のある資料は、すべての ST 利用者にとって適切または有用であるとは限らないことから、別々に分割することができる。

C 参考文献

(参考)

BL Bell, D. E. and LaPadula, L. J., Secure Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-75-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

Biba Biba, K. J., Integrity Considerations for Secure Computer Systems, ESD-TR-372, ESD/AFSC, Hanscom AFB, Bedford MA., April 1977.

CTCPEC Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.

FC Federal Criteria for Information Technology Security, Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.

GOGU1 Goguen, J. A. and Meseguer, J., “Security Policies and Security Models,” 1982 Symposium on Security and Privacy, pp.11-20, IEEE, April 1982.

GOGU2 Goguen, J. A. and Meseguer, J., “Unwinding and Inference Control,” 1984 Symposium on Security and Privacy, pp.75-85, IEEE, May 1984.

ITSEC Information Technology Security Evaluation Criteria, Version 1.2, Office for Official Publications of the European Communities, June 1991.

OSI ISO/IEC 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model , Part 2: Security Architecture.

PPRP ISO/IEC 15292:2001 Information technology – Security techniques – Protection Profile registration procedures.

TCSEC Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985.