参考資料

# ISO/IEC DTR 15446
# N6645

# PP/ST作成のためのガイド

2008-06-19

2009年 6月仮訳
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

## 本書の目的

本書は、ISO/IEC DTR 15446: N6645「Guide for the Production of Protection profiles and Security Targets 2008-06-19」を日本語訳したもので、独立行政法人 情報処理推進機構セキュリティセンターにてPP/ST作成の注意点、評価方法等の調査を行うための補助資料として作成したものです。

## 使用上の注意

本書の原書のステータスは、ISO/IEC SC27 WG3において審議中のものです。
本書は、用語及び体裁の統一、記述内容などに不備がある可能性がある。疑問点については 原書で確認していただきたい。本書の改変、及び他への転載は禁止する。

## 原書

ISO/IEC DTR 15446: N6645
TITLE: Guide for the Production of Protection profiles and Security Targets
DATE: 2008-06-19

# 目次

ページ

# はじめに

ISO（the International Organization for Standardization）、国際標準化機構は、世界中に活動の拠点を置き、国際的な標準化を推進する機関（ISO メンバ機関）である。国際的な標準化を策定する作業は、通常、ISO 技術委員会によって実施される。技術委員会が提案する案件に関心を持つ機関は、当該委員会に参加する権利を持つ。海外の組織、行政（政府）機関、民間企業、ISO のリエゾン（関連機関）もその策定作業に参加することができる。ISO は、電子的な技術の標準化に関するあらゆる分野でも IEC（International Electrotechnical Commission）、国際電気技術委員会と緊密な協力体制を保っている。

国際的な標準は、ISO/IEC 指示（ISO/IEC Directive）第 2 部の定めに従い、ドラフト化されている。

（国際的な標準化策定）技術委員会の主な役割は、国際的な標準化の策定を推進することである。よって、この技術委員会が可決した国際的な標準のドラフト版は、投票用にメンバ機関に配布される。このドラフト版が国際的な標準として公開されるためには、メンバ機関による全投票数の最低でも 75%の承認票を獲得する必要がある。

例外として、技術委員会が、国際的な標準として通常公開されるものとは異種の集合的なデータを提供する場合（例えば、「最先端技術」など）は、技術報告書（TR）の作成メンバの多数決で単純に決定されることがある。技術報告書は、全体的に参考情報として考えられているため、その TR の中で提供されているデータが有効、または有用ではないと判断されるまで見直す必要はない。

本書の内容には、特許権の対象となる記述が含まれている可能性がある、という点に注意する必要がある。ISO は、そのような特許権の一部、またはすべてを明示する義務は負わない。

ISO/IEC TR 15446 は、セキュリティ技術の ISO/IEC JTC 1 小委員会 27 との共同技術委員会によって作成された。

技術面で改訂があった第 1 版（ISO/IEC TR 15446:2004）は無効とし、以降、本書改訂第 2 版を有効とする。

# 序説

本技術評価報告書は、ISO/IEC 15408 情報技術－セキュリティ技術－IT セキュリティの評価基準を補足する文書である。ISO/IEC 15408 では、プロテクションプロファイル（PP: Protection Profile）とセキュリティターゲット（ST: Security Target）の考え方を導入している。プロテクションプロファイルは実装とは関係なく IT 製品の種類に応じ、必要なセキュリティについて記述された文書であり、ISO/IEC 15408 の評価の対象となる一方、セキュリティターゲットは、ISO/IEC 15408 の特定の評価対象（TOE: Target of Evaluation）に適合するセキュリティについて記述された文書である。

改訂前のバージョンとは異なり、ISO/IEC 15408: 2008 では、PP、または ST を記述するには何が必要かの包括的な説明を提供している。ただし、PP や ST の作成方法やセキュリティが確保されたシステムの仕様を定めたり、設計や実装の段階で PP や ST を実践的に用いたりする方法については、いかなる説明やガイダンスも提供していない。

本技術報告書は、こういった格差を補うことを目的としている。本報告書は、ISO/IEC 15408 の評価や適切なセキュリティが確保された IT 製品の開発に長年、携わってきた先人専門家諸氏の経験から得た知識を集約したものである。

# 情報技術－セキュリティ技術－プロテクションプロファイル（PP）とセキュリティターゲット（ST）開発のためのガイド

## 1. 目的

本書では、ISO/IEC 15408: 2008 に適合したプロテクションプロファイル（PP）とセキュリティターゲット（ST）を作成するためのガイダンスを提供する。本書は、情報セキュリティの評価と認証に関与する政府機関のコンソーシアムである、コモンクライテリア管理委員会（Common Criteria Management Board）発行の技術的に同一の標準である、コモンクライテリア バージョン 3.1（Common Criteria Version 3.1）[1]に準拠して作成される PP や ST に対しても適用することができる。

このように、PP や ST の開発担当者を対象に作成されたのが本書である。本書は、第三者が開発した PP や ST の内容を理解したいと考えている、あるいは PP や ST に記載されている情報の関連性や正確性を確認したいと考えている、PP や ST の読者にとっても無視できない内容となっている。本書は、PP や ST の評価者や PP や ST の評価を監視する責任のある認証者にとっても有用である。

本技術報告書は、読者が、ISO/IEC 15408-1 の中でも、特に ST と PP について説明している附属書 A と附属書 B を理解していることを前提に作成されている。PP と ST の作成者は（むろんのこと）、本報告書でも説明しているように、ISO/IEC 15408-2 の第 5 章「機能要件のパラダイム」など、PP や ST の入門書的な資料集を含め、ISO/IEC 15408 の他の章についても理解を深める必要がある。

本書は、PP や ST のガイダンスに関する情報の提供のみを目的とした、ISO の技術報告書である。従って、本書は PP や ST の内容と構造の標準として評価に引用されるべきではない。本書は、ISO/IEC 15408 へ一貫性を持たせることを目的としている。ただし、本技術報告書と ISO/IEC 15408 との間に矛盾が生じた場合は、規範的な標準として後者が優先される。

本技術報告書は、PP の登録や保護されている知的財産権への対応など、PP や ST の仕様以上の関連作業には対応していない。

## 2. 規定の参照

次の規定文書は、本書には必要不可欠なものである。日付入りの規定を参照する際には、編集時の日付のみを記載する。日付のない規定については、最後に編集された日付（文書の修正を含む）を記載する。

ISO/IEC 15408: 2008 （全章）、情報技術－セキュリティ技術－IT セキュリティの評価基準（Information technology-Security techniques-Evaluation criteria for IT security）

ISO/IEC 18045: 2008、情報技術－セキュリティ技術－IT セキュリティ評価方法（Information technology-Security techniques-Methodology for IT security evaluation）

## 3. 用語と定義

本書においては、ISO/IEC 15408-1 で用いられている用語や定義が適用される。

# 4. 略語

本書においては、ISO/IEC 15408-1 で用いられている略語に加え、次の略語が適用される。

COTS　民生品（Commercial Off the Shelf）

SPD　セキュリティ課題定義（Security Problem Definition）

# 5. 本技術報告書の目的と構成

本技術報告書は、国際的な標準である ISO/IEC 15408: 2008 に適合した評価の対象として用いられる PP、または ST を作成する者への助言を目的としている。本書は、PP、または ST の各部分の詳細と、それらの相関関係のガイダンスである。本技術報告書は、ISO/IEC 15408 による評価の入門書としての機能はない。よって、評価用の入門書をお探しの読者諸氏は、ISO/IEC 15408-1 を読まれることを進言する。

本技術報告書は、国際的な標準である ISO/IEC 15408: 2008 のみに対応している。ISO/IEC 15408 の以前のバージョンは異なるものであり技術的要件は一貫していない。ただし、本技術報告書で提案されている方法の大半は、これまでのバージョンの ISO/IEC 15408 にも適用可能である。

第 1 章から第 4 章は、本書の入門編であり、PP や ST についての参考文献が掲載されている。第 5 章の本書の概要がこれに続いている。

第 6 章では、PP と ST の入門編である。PP や ST とは何か、どのような時に、なぜ用いるのか、が記載されている。この章では、PP と ST の関係のほか、PP/ST の開発プロセスに関する問題点についても論じている。

第 7 章から第 13 章では、ISO/IEC 15408-1 の附属書 A.2 と附属書 B.2 の概要に続き、PP、または ST に必須の 7 つの記載事項を特定する方法を提供する。

第 14 章では、統合 TOE の PP や ST(つまり、TOE は 2 つ以上のコンポーネント TOE で構成されていて、それぞれの TOE に対応する PP、または ST がある)に特化した問題点を検証する。

第 15 章では、PP/ST の内容を削減した低保証、国家レベルでの制限や解釈への適合、及び機能や保証パッケージの利用、といった特例を扱っている。

第 16 章では、PP/ST の自動開発ツールの利用法について論じる。

# 6. PP と ST の概要

## 6.1. 序説

本章では、ISO/IEC 15408 に適合する情報セキュリティ評価における PP と ST の役割の概要を説明する。

## 6.2. 対象読者

本書は、次のように 2 つに大別される読者による利用を目的に作成された。

a) セキュリティの知識（例えば、セキュリティ要件を理解しているセキュリティ担当者や設計者など）に長けているが、情報セキュリティ評価の熟練者ではなく、ISO/IEC 15408 の基礎的な知識がない IT 専門家。

b) ISO/IEC 15408 の知識に精通しており、職務の一貫として PP や ST の開発に携わっている情報セキュリティの専門家。

読者が前者のカテゴリに属する場合、本章は、PP や ST を理解／構築する上で必要な情報を提供することだろう。また、本章では、PP や ST を理解する上で必要であり、読者に特化した環境に適合し、適切な PP や ST を識別するためのバックグラウンド情報についても提供している。以下の章では、PP や ST の構成パートについて詳述しているが、これらの文書は、ISO/IEC 15408 に基づいたものであり、読者はその知識があることを前提としている。

読者が IT セキュリティの専門家の場合、本章に記載されている内容には既に精通しているはずである。次章以降では、効率的に、かつ適合性に即した方法で PP や ST を作成するための方法、技法や秘訣などを提供する。

情報セキュリティの専門家ではないが、PP や ST を作成しなければならない読者の場合は、この技術報告書が役に立つことだろう。ただし、既に公開されている、読者のセキュリティ要件に類似の PP や ST の例を探し、理解を深める必要がある。また、PP や ST の作成に必要な専門的な知識や経験を持つ、第三者によるサービスの要求を検討することも一案である。

## 6.3. PP と ST の利用法

### 6.3.1. 序説

ISO/IEC 15408 は、主に、IT 製品のセキュリティを評価するために用いられる。「IT 製品」という用語は、ISO/IEC 15408 の中では実際に定義されたことはない。しかし、1 つの組織が排他的に使用する IT システム全体であれ、製造者が多様な消費者に販売するために開発する COTS パッケージであれ、IT 技術を利用して構築したあらゆるタイプのものをカバーすると理解できる。本技術報告書の中で、「IT 製品」、または単に「製品」と記述されている場合、本書の内容は、これらすべてのものを対象に記述されたものである。本書では、システムについて、COTS 製品について、あるいはその他特定的な用語を明示的に用いている場合、その内容は、特定の種類の製品に限定したものである。

IT 製品は多岐多様に、かつさまざまな環境で用いられているため、セキュリティの考え方は通常各 IT 製品により異なる。従って、ISO/IEC15408 の最終的な評価結果は、「この IT 製品はセキュアである」ではなく、必ず「この IT 製品はセキュリティ仕様を満足する」といった内容になる。

ISO/IEC 15408 は、（特に）次のようなセキュリティ仕様の標準について定めている：

- 製品のセキュリティ仕様を評価する際に必須の、具体的な内容。
- 個々の製品のセキュリティ仕様の比較が可能。

ISO/IEC 15408 では、PP と ST といった、異なる 2 通りのセキュリティ仕様を認めている。この 2 通りのセキュリティ仕様で異なる点は、一般的な製品購入プロセスにおいて、消費者が開発者からの購入製品を探索する際に果たす役割の違いを用いて、よく説明される。

消費者、開発者や製品の概念は、意図して抽象的な表現にとどめている。消費者は、製品を調達したいと思う者である。消費者は、個人を指す場合もあれば、ある組織、組織グループ、政府機関のある省庁などさまざまである。開発者は、製品を売りたいと思う者である。開発者は、個人のプログラマの場合もあれば、小規模の企業、大企業、提携企業グループなどさまざまである。そして、製品とは、小さなソフトウェアアプリケーションやスマートカードから大規模なオペレーティングシステム、あるいは多数の異なるコンポーネントで構成されているコンピュータシステム全体を指すこともある。

消費者が製品を調達する際には、次のような 2 通りの可能性がある：

- 消費者が、開発者に連絡を取って必要な機能を指定し、開発者がその消費者用に具体的な製品をしつらえることによって、その消費者の要望を完全に満たすことである。これには多額の資金が必要だが、消費者は、自身が思い描いた通りの製品を調達することができる。これより以降、こういった調達方法を、仕様ベースの調達プロセス（specification-based purchasing process）と呼ぶことにする。

- 消費者が、数ある既存の製品の中から製品を選択する場合。この調達方法は、前者に比べると多額の資金を必要とはしないが、消費者が必要とする機能を備えた製品かどうかは確実ではない。これより以降、こういった調達方法を、選択ベースの調達プロセス（selection-based purchasing process）と呼ぶことにする。

IT セキュリティが重要になるに従い、こういった調達プロセスは、困難を呈する。従って、一般的な消費者は：

ー どのような IT セキュリティが必要なのかを判断するのが難しい。

ー 製品に記載されている通りの IT セキュリティが、その消費者にとって有効か、または必要とするセキュリティ要件を十分に満たしているかを判断することさえ難しい。

ー もし製品がセキュリティの特性を持っていると宣言していても、それが正しいかどうかを判断することは更に難しい。

調達プロセスを通じて消費者を支援し、上述のような問題点に対応するために、ISO/IEC 15408 と照らし合わせ、製品を評価することが有効であり、このような場合、PP と ST が重要な役割を果たしている。次の 2 つのサブセクションでは、仕様ベースと選択ベースの調達プロセスで、評価がどのように関わってくるかを説明する。

もちろん、IT 製品は単独で動作しない。製品は固有のセキュリティ手段を含むかもしれない運用環境で消費者に使用される。時には製品が運用環境にある種のセキュリティ特性があることを前提としている場合があり、これらの前提条件もまた PP や ST の一部を構成する。

### 6.3.2. 仕様ベースの調達プロセス

#### 6.3.2.1. 概要

仕様ベースの調達プロセスでは、消費者が仕様書を作成し、開発者に提出することによって、その仕様書をベースにした製品が開発される。具体的には、次のような手順を実施しなければならない：

a) 消費者が非形式的なセキュリティ要件を決定しなければならない。

b) 消費者が非形式的なセキュリティ要件を、開発者が理解できるような標準的な形式にする。

c) 開発者は、この仕様に基づいた製品を開発しなければならない。

最終的に、消費者は、「この製品は、自身の役に立つか」を知りたいと思うだろう。そのために、これらの手順の 1 つ 1 つの質が重要なのである。

#### 6.3.2.2. 非形式的に表現されたセキュリティ要件

非形式的なセキュリティ要件の決定プロセスでは、「私のセキュリティに関する問題は何か？それをどう述べるべきか？」を決定することだが、それは ISO/IEC15408 の対象外であり本書の対象ではない。しかし、これを対象外とすることは、このプロセスが簡単で重要ではないと判断したという意味ではない。

しかしながら、ISO/IEC 15408 は、消費者が、非形式的なセキュリティ要件を定義することができることを前提に規定されている。非形式的なセキュリティ要件が不適切であれば、調達した製品も最終的には、実際のセキュリティ要件とは適合しない可能性がある。

従って、一旦、消費者がそれらの要件を洗い出すことによって、セキュリティに関する分野では特に、それらに関連の問題が浮かび上がってくることが多い。セキュリティに関する消費者の要件の問題点には、通常、次のようなものがある。

a) 不完全（すべての要件が記載されていない）。例えば、製品にもたらされる可能性が高い重大な脅威の記述がない。

b) 組み込めない。製品が機能すべき特定の環境に適合できない、またはこの環境について十分な説明がされていない。

c) 黙示的。製品の要件の中には、既に結論が出ているものがあるが、これらの結論そのものが含まれていない。開発者が、これらの黙示的な要件を考慮していないことがある。

d) 検証ができない。要件があいまいに記載されているため、製品が要件を満たしているのか、いないのか確認することができない。

e) 詳述過ぎる。実装については、実際に記載されているが、それが選択された理由については記載されていない。後に、要件を変更する場合、どのように変更すべきかが不明になることが多い。

f) あいまいな用語ばかり用いられている。例えば、「通信は、安全に行われなければならない。」が、「安全」な状態が定義付けされていない。

g) 一貫性の欠如。要件が内部的に自己矛盾している。

これら消費者側の要件をそのまま開発者に提供すれば、誤解が生じることもあり、それが問題に発展するのが常である。セキュリティ評価では、評価者が消費者と開発者双方の要件の見解をさらに異なった解釈をすることによって、問題の争点がさらに拡大することもある。

このような理由で、仕様ベースの調達プロセスにおける重要な手順は、消費者の要件を所定の形式にすることである。ISO/IEC 15408 をベースにしたセキュリティ要件では、こういった場合に PP と呼ばれる形式が適用される。PP とは、消費者のセキュリティ要件を所定の形式で標準化した、基本的な文書のことである。

#### 6.3.2.3. 仕様としての PP を用いる場合

PP 作成には多大な工数をつぎ込む必要があるため、大きな組織、グループ組織、政府部門が作成することが一般的である。

PP は、さまざまな節に分けられているが、セキュリティ仕様としては、「セキュリティ機能要件」が最も重要である。ISO/IEC 15408 に照らし合わせ、その国際的な標準の中で定めている特別な言語を用いて、これらの要件を記述することが必須となっている。その特別な言語を用いると、PP は以下であることが保証される:

a) 明確さ。特別な言語では、要件を記述するための用語が詳述に定義されているため、開発者は、要件を正しく理解し、解釈することができる。

b) 検証が可能。特別な言語には、検証可能な用語のみが含まれるように定義されている。よって、後に、その製品が実際に PP と適合しているかどうかを評価することができる。

c) 詳述過ぎない。特別な言語では、ある程度抽象的な表現をするよう要求している。これによって、後に、消費者の要件を詳しく補足することができる。消費者は要件がどのように実現されるかについてまでは気にしていない。

d) 完全さ。特別な言語には、黙示的な要件が確実に含まれるようにするために複数の構文(「ある機能性が要求された場合には、その他の機能性も要求される」、など)が含まれている。

#### 6.3.2.4. PP による製品の構築

これで、消費者は、所定の形式化された PP を開発者に提供することができる。開発者は、この PP を製品開発の開始点として用いる。このプロセスの最初の段階で、開発者は、ST を作成する。

こういった目的で用いられる ST は、PP と非常に類似しているが、PP は消費者側の要件を定義し、原則として消費者側で作成されるのに対し、ST は製品の仕様であり、開発者によって作成される。

むろん、消費者の PP に対しては任意の ST ではなく、PP に適合した ST を開発者は提供しなければならない。すなわち、製品は消費者のすべての要求をカバーしなければならない:ただし、

- ST は、PP よりも多くを規定する場合がある:開発された製品は、消費者が指定した要件よりも多くのセキュリティ機能を提供する(注:この追加された機能性は、PP と不適合であってはならない)。なぜならば、例えば、その製品が複数の消費者に販売された場合、それぞれの製品は類似しているにも関わらず、若干、異なった要件が必要だったり、または、その製品が、既存の、標準的な製品から導出されたものだったりするためである。
- ST の内容は、PP のそれよりも詳述である。PP が、「何」に対してセキュリティを確保しているかについて説明しているのに対し、ST では、「どのように」セキュリティを確保するのかを説明している。通常は、開発者が消費者の要件をいかに実装するかを指定する。

PP では、ST の作成者が、PP 記述の中で用いられているセキュリティ機能に関し、同様の意味ではあるが、別の表現方法で記述する柔軟性を許可している－詳しくは、6.5.6 項を参照。

ST には、開発者による以降の開発プロセスのために、開発者による「セキュリティ要件の仕様」としてその製品に搭載され、かつ機能すべきセキュリティ機能が明示されている。

開発プロセスの最終段階は、製品が消費者に配布され、製品をインストールして利用できなければならない。当然のことながら、この製品は ST に記載されている通りの機能を実行できなければならない。

#### 6.3.2.5. 仕様ベースの調達プロセスにおける評価の役割

これまでは、仕様ベースの調達プロセスにおける消費者の役割と開発者の役割についてのみ説明してきた。このプロセスでは、開発者は消費者に対し、（さらなる証拠を提出しなくても）次のような説明をすることができる。

a） 開発者の ST は、消費者の PP に適合している。

b） 開発者の製品は、開発者の ST に適合している。

c） 従って、開発者の製品は、消費者の PP に適合するので、消費者の要件にも合致している。

消費者が、これらの説明を承認した場合、本プロセスはここで終了する。

ただし、消費者がこれらの説明に対し、独立した検証を要求する場合、開発者が主張する適合性を ISO/IEC 15408 を適用したセキュリティ評価によって確認するために、第三者機関（評価機関）に協力を求めることができる。このプロセスでは、2 種類の文書を評価するために、消費者の PP、開発者の ST と製品に ISO/IEC 15408 を照らし合わせる。

a） 開発者の ST は、消費者の PP に適合しているか。

b） 開発者の製品は、その ST に適合しているか。

次の 2 つの点は、評価の対象外であることに注意する。

a） *消費者の非形式的なセキュリティ要件から PP への翻訳。*既に説明したように、このプロセスは、ISO/IEC 15408 の目的には含まれていないが、このプロセスが適切に実施されなければ、この PP が消費者の要件に適合するとは言えず、従って、製品も消費者の要件に適合するとは言えなくなる可能性がある。

b） *評価は、適合性を「証明」するものではない。*ISO/IEC 15408 による評価は、その製品が PP に適合するという絶対的な保証を提供するものではなく、PP、または ST に記載されている通り、評価の深度や目的に応じ、所定の保証が提供されるだけのものである。

### 6.3.3. 選択ベースの調達プロセス

#### 6.3.3.1. 概要

前節では、消費者が仕様書を作成し、その仕様書を基に開発者が製品を開発するプロセスを論じた。本節では、消費者が自身の製品に特別な機能を欲していない場合、すなわち、既存の製品から選択する場合について論じる。従って、この調達プロセスでは、消費者の要件の形式的な文書（すなわち、PP）に適合した調達方法である必要はないが、消費者が、既存の製品を比較し、選択する。

IT 製品の選択ベースの調達プロセスでは：

a) 開発者が、製品とその製品の仕様を開発し、消費者にその仕様を提供する。

b) 消費者が、自身に最も適切な製品を調達するために、その製品が適切かどうかを（他の開発者の仕様と比較する場合もある）仕様から判断しなければならない。

最終的には、消費者が「この製品は自身に適している」ことを納得するために、上述のプロセスの中で実施される内容が重要である。

#### 6.3.3.2. 開発者が提供する仕様を用いる場合

選択ベースの調達プロセスでは、消費者は、開発者が提供した仕様を用いなければならない。

この仕様が非形式的であれば、第 6.3.2.2.項でも論じているが、消費者の非形式的な要件にありがちな欠点がそのまま維持されることになる。このような理由で、開発者が提供する仕様についても形式的である必要がある。従って、ST を記述する場合は、第 6.3.2.4.項でも述べたように、ISO/IEC 15408 を適用する。ここで言う ST とは、第 6.3.2.4.項で論じた ST と同一のものであるが、1 つだけ明らかに違っている点がある。つまり、この ST は、消費者の PP をベースにしたものではないため、その PP に対し、適合性を主張することができない（別の種類の PP に対し、適合性を主張できることがある－第 6.3.4.項以下を参照）。

開発者は、消費者の具体的な要件を知らないため、開発者は、市場ではどのような仕様が欲せられているのかを推測して、ST を記述する。従って、消費者の特有の要件に適合するとは限らない。

開発者は、ST に従って自身の製品を構築する。このプロセスは、仕様をベースにした調達プロセスの記述と同様である。

#### 6.3.3.3. 開発者の ST の比較

消費者は、複数の製品の ST を比較し、自身の要件に最適な製品を選択することができる（価格などセキュリティには直接関係のない要件も検討の対象になるだろう）。つまり、消費者は、何らかの方法で自身に必要な非形式的なセキュリティ要件（第 6.3.2.2.参照）を見いだし、ST の中で提供されているセキュリティ要件を比較検討しなければならない。複数の製品の中に消費者が必要とするセキュリティ要件と適合するものがあれば、このプロセスは完了である。必要とするセキュリティ要件と適合する製品がなかった場合、消費者は、自身の要件に最も近い要件を備えた製品を選択するか、別のソリューションを見いださなければならない（つまり、消費者の要件を変更しなければならない）。

第 6.3.2.項でも既に述べたことだが、消費者の非形式的なセキュリティ要件を導出するプロセスは、ISO/IEC 15408、及び本技術報告書の対象外である。この技術報告書の後半の章にこの件に関するガイダンスを提供しているが、消費者の要件や開発者の ST を比較するプロセスも ISO/IEC 15408 の対象外である。

#### 6.3.3.4. 選択ベースの調達プロセスにおける評価の役割

仕様ベースの調達プロセスと同様に、開発者は自身の製品が ST に合致すると主張することができ、消費者がこの主張を受け入れた場合、このプロセスはここで終了する。

ただし、慣習として、開発者は、独立した第三者機関(評価機関)が ST を検証し、その製品が実際に ST に合致していることを確認するために ISO/IEC 15408 を適用したセキュリティ評価を実施した確証として認証書を提供する。この評価プロセスを開発者にゆだねることなく自身で実施すべきと考える消費者は、自身で評価を実施することができる。

評価された製品であっても、次のような点が解決されているとは限らない点に留意する。

a) *消費者が必要とする非形式的なセキュリティ要件と ST の内容が同じであるという証明。*既に説明したように、このプロセスは、ISO/IEC 15408 の対象外ではあるが、これが適切に実施されなかった場合、開発者の ST は消費者の要件と適合しないこともあるため、その製品もまた消費者の要件に適合しない場合がある。

b) *評価は、適合性を「証明」するものではない。*ISO/IEC 15408 による評価は、その製品が完全に ST に適合するという保証を提供するものではなく、ST に記載されている通り、評価の深度や目的に応じ、所定の保証が提供されるだけのものである。

### 6.3.4. PP のその他の利用法

PP には、その他の利用法がある。例えば、標準化団体やベンダ協会が、最適な実施例として、特定種類のアプリケーションに対する PP を最小限度のセキュリティ基準として指定することがある。政府機関や事業団体の中には、アプリケーションを用いる際の必須基準にするところがある。そのような場合、消費者と開発者が追加のセキュリティ機能を要求、あるいは提供することに加えて、その PP に適合する必要があるであろう。

そういった目的で PP を指定したり、必須基準としたりする組織は、その PP が最低限のセキュリティ機能を備えており(それ以上のセキュリティ機能が必要にならないように)、現実に即している(開発者が提供できないような機能要件や保証要件を要求することがないように)ことを確かめるといった、煩わしい責任を負うことになる。

PP は、それが公開された時点で、そのようなセキュリティ要件を備えた製品がまだ市場に存在しなくても、特定種類のセキュリティ製品の必要性を表現するために作成されるかもしれない。あなたが製品の開発者であるなら、そういった PP には注意を払わなければならない。あなたが相応しい製品を開発する前に要件が古くなったり、PP のスポンサーが要件を満たす別の方法を発見したりして、もうあなたの製品を買おうとはしないかもしれない。

結論を言えば、PP とは *セキュリティ*要件の仕様である。明示的に表現すると受け入れられない別の種別の要件を誤って指定することがないようにしなければならない。

### 6.4. PP/ST の開発プロセス

ISO/IEC 15408-1 の附属書 A と B、及び本章の前半部分でも PP と ST の要件を記述する手順を説明しているが、PP と ST は常に論理的に「上から下へ(top-down)」の法則で記述されるのが望ましい。例えば、ST の場合は:

a) セキュリティ課題を明らかにする。

b) 明らかにしたセキュリティ課題に対応するためのセキュリティ対策方針を識別する。

c) 次いで、TOE に対応するセキュリティ対策方針を満足させるセキュリティ要件を特定する。

d) さらに、セキュリティ要件を満足させるような、セキュリティ機能を実際に選択する。

こういった要件を無視していると、再度同様のプロセスを反復する必要性が高くなる。例えば、セキュリティ要件を定義付けすることによって、セキュリティ対策方針、場合によってはセキュリティ課題をも明確にする必要性が強調されてしまう。脅威、組織のセキュリティ方針、セキュリティ対策方針、セキュリティ要件、及びセキュリティ機能の関係の詳細な検査は繰り返し行う必要があるかもしれない。根拠が作成される際には特に必要であろう。これらの根拠で明らかにされた格差がすべて満足された場合に限り、PP、または ST が完全であると考えることができる。

PP、または ST 開発時の反復プロセスにおいて、現在明らかになっているセキュリティ課題を対象とした新たな情報が浮上した場合は、外的な環境の変化を反映する記述箇所に対する変更が導かれる場合がある。例えば:

a) 新たな脅威が明らかになった。

b) 組織のセキュリティ方針が変更になった。

c) 資金や開発までの時間に制限が設けられ、TOE や TOE を適用した環境で対応できると考えられていた役割（機能）の分担の変更が余儀なくされた。

d) 想定する攻撃能力の変更は、TOE セキュリティ課題定義に影響が及ぶ可能性がある。

（TOE が既に開発済みの製品である場合は特に）PP、または ST の作成者は、TOE が提供するセキュリティ機能（仮にその機能がまだ、ISO/IEC 15408 でセキュリティ機能要件として明らかにされていなくても）について、明確なアイディアを考えることもできる。このような場合、考慮すべきセキュリティやセキュリティ対策方針の定義には、TOE によって提供されるセキュリティソリューションの情報形態がいやおうなしに含まれることとなる。PP/ST の開発プロセスには、ある程度、こういったボトムアップのケースが生じる。

## 6.5. PP と ST の読み方と理解

### 6.5.1. 序説

本項は、既に ISO/IEC 15408 の知識を持っている専門家は対象として*いない*。本項は、PP や ST について僅かな知識を持っているが、これらに関連する製品のセキュリティ機能を理解するために、複数の PP や ST を読破する必要のある、本技術報告書の読者の一部を対象としている。この技術報告書では、省略／欠落箇所など、特に評価目的で明示していない記述について説明する。

PP や ST を細部まで理解するには、ISO/IEC 15408-1 の、特に附属書 A と B に記載されている、ST と PP それぞれの詳細を読破するより他の手立てはない。既に公開されたり、一般的に利用されている他の PP や ST を研究したりするのも良いアイディアである。また、登録されている多彩な PP や ST をダウンロードすることもできる。Common Criteria Portal は、これらが最も多く登録されているサイトである[2]。ここに登録されているものは、ISO/IEC 15408 を適用して構成された PP やそのパッケージの正式な JTC 1 による登録として ISO、及び IEC の審議会によって認められたものである。この審議会は、国際的な標準に関連の、ISO/IEC 15292[3]に基づいて運営されている。

残念ながら、PP、または ST は、単独のものとして、または単独の機能として要約することはできない。PP や ST は、セキュリティ機能の複合的な集合として説明されているため、注意して読まなければ、製品を調達したり、利用した場合、予期しない動作をしたりすることがある。一方、PP や ST の記述箇所（特にセキュリティ機能要件）には、ISO/IEC 15408 を完全に理解していなければ、到底理解することができない、ISO/IEC 15408 と同等、あるいはそれ以上に重要な記述が含まれている。従って、本項以降の各項では、PP や ST をこれから習得しようと思われている読者用に PP や ST の重要な記述箇所を紹介する。それぞれの項目は、比較的理解し易いと思うが、PP、または ST の記述に基づき開発された製品として、セキュリティ機能要件を理解するために重要な情報が記述されている。

これに関し、読破しておくべき項目は:

a) TOE 概要。

b） TOE 記述。

c） 運用環境のセキュリティ対策方針。

d） 適合主張。

以下の各項で、これらの内容についてさらに詳しく説明する。

### 6.5.2. TOE 概要の読み方

TOE 概要は、一般的に PP や ST の最初に読む項目であり、「セキュリティニーズを満たし、使用するハードウェア、ソフトウェア、及びファームウェアによってサポートされている TOE を見つけるために、評価済み TOE/製品のリストに目を通している TOE の潜在的な消費者」を対象としている。（ISO/IEC 15408-1、附属書 A.4.2.節）。TOE 概要には、次のような 3 つの項目が含まれている：

a） TOE の使用法及びその主要なセキュリティ機能の特徴。

b） TOE 種別。

c） 必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア。

これらの各項目を、順を追って説明する。ISO/IEC 15408 の附属書 A.4.2.節には、各項目に対応する簡単な例が記載されている。

TOE の使用法及び主要なセキュリティ機能の特徴に関する記述は、セキュリティ面から見た TOE の機能とセキュリティに関する TOE の用途について、ごく一般的な概念を提供することを目的としている。

当該項は、比較的短いため（2～3 程度のパラグラフ）、読んで理解するまでにさほど多くの時間を要することはないだろう。また、この項は、一般消費者を対象としているため、技術的に高度な内容にはなっていない。本項は、ごく一般的な知識が体得できることを目的にしているため、読者が徒労を感じることもないだろう。

TOE 種別は、TOE が対応する IT 製品の一般的な種別の説明である（例：ファイアウォール、スマートカード、イントラネット、LAN など）。ISO/IEC 15408 は、TOE 種別から有することが期待されている機能が TOE によってサポートされない場合、TOE 概要がその合理的な根拠を提供するよう義務付けている。特に：

a） TOE が特定のセキュリティ機能性を備えていないにもかかわらず、その TOE 種別のために TOE がそれを備えるものと期待される場合、TOE 概要にはその機能性が備わっていない旨を記載しなければならない。

b） TOE が特定の環境で動作できないにもかかわらず、その TOE 種別のために TOE がその環境で動作するものと期待される場合、TOE 概要にはその旨を記載しなければならない。

PP や ST で、こういった注意事項の表示を義務付けているのは、TOE 概要のみである点に、留意されたい。PP や ST の作成者は、留意事項として、後に、然るべき場所で、本件に関する情報を再度公開することもできるが、ISO/IEC 15408 ではこれを義務付けてはいない。

こういった注意事項が該当し、消費者が目的とする TOE の利用法にも影響が及ぶ可能性がある場合は、このような制限があってもこの TOE を使用するかどうかを真剣に検討しなければならない。

TOE の中でも、ソフトウェアタイプの TOE は、ハードウェア、ファームウェアやその他のソフトウェアコンポーネントに依存せざるをえないものがある。このような場合には、TOE 概要で、TOE 以外のハードウェア/ソフトウェア/ファームウェアを識別する必要がある。

PP や ST では、すべてのハードウェア/ソフトウェア/ファームウェアについて完全、かつ詳述に識別する必要はないが、TOE を利用する際に必要な外部の主なハードウェア/ソフトウェア/ファームウェアコンポーネントを判断するために十分な完全かつ詳細な識別を行うべきである。

また、消費者は、TOE が動作する一般的ではないコンポーネントが存在し、これらのコンポーネントが消費者の既存のインフラストラクチャ、予算、組織の方針、その他に適合するかどうかを慎重に評価しなければならない。

### 6.5.3. TOE 記述の読み方

ISO/IEC 15408 の評価を理解する上で重要な点は、周知の製品 XYZ であっても、その製品のすべてのセキュリティ機能（または、主要なセキュリティ機能であっても）がすべて評価されているとは限らないということである。そのセキュリティ機能のいくつかだけが実際に検査される場合がありえ、その場合、残りのセキュリティ機能は、評価されたセキュリティ機能の一部であると考えられない。ISO/IEC 15408-1 の従属節 A.4.1.では、誤解を招くTOE 参照を禁じているが、開発者は単に製品名を使用することによってこの規定を回避することが常にできる。評価された機能性が、あなたが必要とするものと合致しているか確認する必要がある。もし、あなたの必要とするセキュリティ機能性が除外されていた場合には、その理由を考える必要がある。

TOE 記述の重要な役割の 1 つは、ST の読者が、（ある）製品のどの機能が評価の対象なのかを理解できるようにすることである。これによって TOE の物理的、かつ論理的な範囲を詳細に規定することができる。

物理的な範囲は、ISO/IEC 15408 では、「TOE 記述は、TOE の物理的な範囲、つまり TOE を構成するすべてのハードウェア、ファームウェア、ソフトウェア、及びガイダンスの各部分のリストを記述する。このリストは、各部分の包括的な理解を読者に与えるために十分な詳細レベルで記述するべきである」と規定されている（ISO/IEC 15408-1、附属書 A.4.3.の従属節より）。

予想に反する奇妙と思える記述があったり、存在すると予想していたパーツが欠落したりしていないか、リストを確認する必要がある。もし、リストに何か欠落していた場合、評価ではそのパーツが無視され、存在しないものとして扱われている。あなたがそのパーツを使用したいのであれば、評価結果からそのパーツのセキュリティの能力を知ることはできない。

論理的な範囲は、ISO/IEC 15408 では、「TOE 記述は、TOE の論理的な範囲、つまり TOE によって提供される論理セキュリティ機能の特徴についても、包括的な理解を読者に与えるために十分な詳細レベルで説明するべきである。この記述は、TOE 概要で記述される主要なセキュリティ機能の特徴よりも詳細にすることが求められる」と規定されている（ISO/IEC 15408-1、附属書 A.4.3.の従属節より）。

TOE の物理的な範囲では TOE を構成する各部分のリストを規定する傍ら、TOE の論理的な範囲では、TOE が何をするかを記述しなければならない。このことについては、TOE の主要なセキュリティ機能（6.5.2.節参照）でもざっと論じているが、実際は、数パラグラフではなく、数ページを割いて規定すべきものである。本章で最も重要なことは、もしあなたが例えばリモート管理(例えば業界紙の製品広告でその特性が触れられている)を予想していたのに、論理的範囲がリモート管理を含んでいない場合には、リモート管理は評価されていないため、評価された構成でその製品を使用したい場合には、リモート管理を停止しなければならないということである。

よって、消費者が実際に必要なセキュリティ機能がすべて評価されていることを慎重に判断することが重要である、ということを述べているのが本章である。評価されていない場合は、その特性の運用については保証されていない。

### 6.5.4. 運用環境のセキュリティ対策方針

運用環境は、TOE が一般的に設置される場所のことである。TOE で評価された機能が適切に動作するために、この運用環境は所定の制約（事項）を満たしていなければならない。例えば、TOE が可用性の高いサーバである場合、この TOE は、ねじ回しを持ってサーバにアクセスしようとする攻撃者からサーバを保護する必要がある。この保護は TOE によって提供することができるが（耐タンパ性サーバはごく稀ではある）、一般的にはセキュアなサーバルームに設置するという運用環境で対処する。

運用環境での、上で述べたような要件や類似の要件については、PP、または ST の運用環境のセキュリティ対策方針の項目に記載されている。これらの項目には、TOE 記述にあるようなセキュリティ要件に適合するために、TOE 以外に必要なすべての要件が記載されていなければならない。ISO/IEC 15408-1、附属書 A7.2.2 の従属節がこの運用環境のセキュリティ対策方針についての事例に当たる。

ここで最も重要な点は、これらはガイドラインではなく、TOE が記述されたと通りに動くために必要な条件であるということである。これらのすべての対策方針は、あなたやあなたの組織が満たすか、対応しなければならず、TOE が実施するわけではない。項目の中の 1 つが適合しなくても、TOE の評価対象となっている機能が安全に機能しないかも知れない。従って、TOE の評価対象となっている機能が、消費者組織にとって有効かどうかを判断し、そのうちの

1 つでも有効ではないということが判った場合、その TOE は、読者（消費者）に適しているとは言えない。

### 6.5.5. 適合主張の読み方

適合主張は、PP、または ST の最も重要な箇所、すなわち一際目を引く箇所に、箇条書きで記載されるのが普通である。

ここで言う PP/ST が主張する適合性とは：

- ISO/IEC 15408:2008。ここで言う主張箇所とは、適合主張の確認に用いられた ISO/IEC 15408 のバージョンを示している。2008 年バージョン、またはそれ以降のバージョン(つまり、コモンクライテリアのバージョン 3.1 と同等かそれ以上)でない場合、その PP/ST は、本技術報告書で規定している仕様とは適合しないため、本書を直接適用することはできない。
- ISO/IEC 15408 Part2 拡張、または Part2 適合。本主張箇所では、セキュリティ機能要件の構成方法について定めており、消費者の視点から、どちらが選択されても構わない。
- ISO/IEC 15408 Part3 拡張、または Part3 適合。本主張箇所では、セキュリティ保証要件の構成方法について定めている。もし「Part3 拡張」が選択されている場合は、PP と ST の開発者は独自の保証テストを企画している。消費者の視点からはその理由を問う必要がある。
- TOE が適合するパッケージのすべてのリスト。パッケージは、EAL1、EAL2、・・・EAL7 と名付けられた単一のパッケージが一般的だが、場合によって「追加」が付属する場合がある。ここで紹介した EAL については、6.5.7.で詳しく説明する。これ以外のパッケージを主張することは稀であるが、消費者の視点から、再度、なぜそういったパッケージが必要だったのかを疑問に思うべきである。
- PP、または ST が適合する、PP リスト。これについては、6.5.6.で詳しく説明する。

### 6.5.6. PP への適合

6.3.2.4.で既に説明したように、ST は、PP への適合性を主張することができる（必ずしも主張する必要はない）。また、PP は、他の PP との適合性を主張することもできる。適合性を主張する場合、その PP は適合主張の箇所にリストされる。ISO/IEC 15408 では、如何なる場合でも部分的な適合については認めていない。従って、ここでリストされる場合、PP、または ST は、それに対応する PP に完全に適合していなければならない。

PP への適合とは、PP、または ST（及び、ST が既に評価された製品である場合は、その製品についても）が、対象となる PP のすべての要件を満たすことである。

PP を読んでいる間に、消費者（読者）は、ST、または他の PP が「正確適合」、または「論証適合」のいずれかの方法で適合しているという文言を目にすることだろう。通常は論証適合を要求しているであろう。これは、PP への適合性を主張する ST は、PP で記述されている一般的なセキュリティ課題の解決のために必要な要件を提供しなければならないが、PP に記載されている解決のための要件と同等またはより制限的な要件を提供することができる、という意味である。「同等またはより制限的」については、ISO/IEC 15408 の中で詳しく定義されているが、基本的に、PP と ST には、異なったエンティティについて論じられていたり、異なった概念が用いられていたりするなど、全く異なった文言が含まれているという意味である。ただし、全体的に ST には、TOE に対して PP と同等、またはそれ以上の制限が課されているが、TOE の運用環境に対して PP と同等、またはそれ以下の制限が課されている。

正確適合は、例えば、選択ベースの調達（6.3.3.項参照）など、PP と ST に寸分の誤差も許可できないものに限り、用いられる。むろん、必要であれば、ST の中で補足的な制約事項を設けることもできる。PP が正確適合を求めているにも関わらず、あなたやあなたの組織がそれを望まないのであれば、その PP は全く利用できない。

### 6.5.7. EAL とその他の保証に関する課題

TOE 概要と TOE 記述では、TOE によって実際に実現される機能、すなわち、TOE によって提供される機能性について規定している。ただし、機能性が、IT 製品のすべてではない。同様の一般的な機能性を備えた製品でも異なる設定で利用されうる。例えば、同じデザインのスマートカードでも、次のような利用方法がある。

- 小額の「交通費」前納型バスチケット。
- €10.000 を上限とするクレジットカード。
- 最高機密軍事施設への立ち入りを許可するアクセス管理策、など。

最初に紹介したケースの場合は、「あまり品質（セキュリティ）の高くない」スマートカードで十分である。仮にハッカーが、このバスチケットのセキュリティを破ったとしても、せいぜい、このカードのパラメタが変更されるまで、バスへの乗り降りが自由になるというだけである。見込まれていた収入の損失も、このバス会社にとってあまり大きなものではない（ただし、これ以外にもカードが同じような方法でハッキングされていなければ、だが）。

2 番目に紹介したケースと、むろんのことだが 3 番目のケースでは、カード 1 枚が破られただけでも重大な損失に発展する恐れがあるため、カードのセキュリティ機能性が正しく実装されていることをより深く確信する必要がある。

ISO/IEC 15408 では、こういった品質を「保証」と呼ぶ。ISO/IEC 15408 では、開発と製造プロセス、設計、マニュアル、製品の開発者が実施した（製品に対する）試験の量など、製品の開発をさまざまな角度から確認する方法で、保証に所定の基準を設けている。

ISO/IEC 15408 では、保証を（保証ファミリと呼ばれる）27 のカテゴリに分類している。また、カテゴリごとに、ISO/IEC 15408 によって、異なったレベルの適合性が定められているが、高いレベルの適合性を満たしているほど、保証レベルも高い。

例えば、ある製品について、開発者が作成した試験のカテゴリのレベル付けは、次のとおりである。

- 0：開発者が、製品について試験を実施したかどうかも不明。
- 1：開発者が、製品の一部であるインタフェースについて、若干の試験を実施した。
- 2：開発者が、製品に備わっているすべてのインタフェースについて、若干の試験を実施した。
- 3：開発者が、製品に備わっているすべてのインタフェースについて、あらゆる角度からさまざまな試験を実施した。

この例からも判るように、レベルに応じどの程度の試験を実施したかによって保証の度合いが高くなると同時に、不確かさが減少する。

残念なことに、専門家でなければ 27 に分類された全カテゴリの、個々の得点が記されているスコアカードを判読することは不可能である。従って、専門家以外の消費者が保証を評価する場合は、評価保証レベル（EAL：Evaluation Assurance Level）と呼ばれる ISO/IEC 15408 であらかじめ定めている 7 通りの得点配分を適用することができる。これらは、EAL1 から EAL7 まであり、EAL1 が最低限の保証レベルであるのに対し、EAL7 が最高の保証レベルとなっている。

各 EAL は、27 の要件で構成されており、その 1 つ 1 つがサブカテゴリと考えることができる。例えば、EAL1 では、13 のサブカテゴリの得点配分を 1 とし、それ以外の 14 のサブカテゴリの得点配分は 0 とする。EAL2 では、7 のサブカテゴリの得点配分を 2 とし、11 のサブカテゴリには 1 を、残り 9 のサブカテゴリの得点配分は 0 にする、といった具合である。

EAL は厳密な階層型を呈しているため、EALn のあるカテゴリで、ある得点が配されると、EALn+1 では、そのサブカテゴリに同等、またはそれ以上の得点を配すことになる。つまり、EALn+1 では、EALn よりも全体的により厳密な保証が提供される。

高度な保証の欠点は、やはり、費用の問題である。既に説明したように、保証に関する試験では、レベル付けが 0 の場合、費用は必要ないが、レベル付けが 1 以上の保証の試験では、開発者が試験を実施し、終了した試験について文書を作成し、評価者が、保証に関する試験が適切に実施され、それが文書にまとめられているかなどを判断しなければならない。保証のレベルが高くなれば、より多額の費用が必要である。むろん、保証のレベルが高くなれば、主張されていた機能性が適切に動作しない、または悪用されがちな脆弱性が含まれているといったリスクを低減することもできる。

各 EAL のリストとその EAL に関する説明、及びその EAL によって提供される保証の内容については、ISO/IEC 15408-3 の第 8 章に記載されている。

EAL は、保証について大まかなメカニズムを定義したものであり、他のメカニズムよりも特定種類の製品を評価するのに適している。ただし、現時点では、ISO/IEC 15408 の保証に携わる専門家ではない消費者でも理解できるという点で、広く適用されている保証のメカニズムは EAL のみである。

### 6.5.8. サマリ

本章では、次の 2 つの内容について説明してきた。

a) ST は、各章を読み進めるに従って、ある程度のレベルまで理解することができる（ことがはっきりしている）が、

b) （はっきり示されているわけではないが、）各章には重要な注意が含まれていることもあるため、評価に関する制限を理解するためには重要である。

過去にはファイアウォールであれ何であれ、EAL4 のものを購入したいと消費者が宣言するケースもあった。ISO/IEC15408 で EAL4 認証されたファイアウォールであっても、あなたに全く適さない制限があったり、あなたが必要とするセキュリティを全て提供しなかったりすることを、本章が説明できたことを望む。

例えば、ファイアウォールにパケットルーティングとHTTP/FTP プロキシサービスの双方が必要な場合を考えてみよう。そのルータは、TOE 種別がファイアウォールであり、EAL4 の評価がされている。ただし、ルータとして利用する場合は、パケットのルーティング管理しか提供することができない。悪条件が重なり、EAL4 として評価されたファイアウォールは、プロキシサービスを提供することはできるが、その論理的な範囲は、パケットルーティングのみに制限されている場合、消費者はその理由を考えてみるべきである。

ISO/IEC 15408 のように大掛かりな標準さえ、そのような事例に対する解答にはならない。消費者がどんなにがんばったところで、IT セキュリティのように複雑な事案の説明を単一にまとめるのはとうてい無理であろう。

### 6.5.9. 知識を深めるために

これまで説明してきた PP、または ST についての各章は、PP、及び ST の最も基本となる章であり、PP や ST に携わる専門家ではない消費者が読むのに最適である。製品についてもっと知りたいと思うなら、TOE の実装方法が詳しく説明されている、TOE 要約仕様も併せて読んでみるとよい。ただし、この章は、簡単に理解することはできないだろう。なぜならば、この章は、FIA_UID.2.1.のように、説明のない略語がたくさん登場するからである。多くの開発者は評価者からの修正要求に対応し、消費者に対しても理解しやすいような TOE 要約仕様を提供できるように努力している。

PP や ST のその他の部分も読んでみたいと思うなら、本技術報告書の後半部分が役にたつことだろう。本書は、PP や ST を細部まで設計する専門家が利用することを目的として作成されたものではあるが、PP や ST に関連の内容を把握したいと思っている一般消費者にとっても有効な情報が含まれている。

## 7. PP/ST 概説の規定

本章では、PP、または ST に関する、PP/ST 概説の規定に関するガイダンスを提供する。これらは、ISO/IEC 15408-1 の附属書 A.4 と B.4 でも詳しく説明されているため、本技術報告書では、ガイダンスに追加が必要な項目を若干説明するにとどめる。

PP 概説には、次のような内容を含めること:

- PP 参照。
- TOE 概要。

ST 概説には、次のような内容を含めること:

- ST 及び TOE 参照。
- TOE 概要。
- TOE 記述。

唯一はっきりしないパートが、TOE 概要の「TOE の使用法及び主要なセキュリティ機能の特徴」の章である。使用法に関しては、PP、または ST についてのセキュリティ課題を明らかにし、それをまとめることによって最善策が導出される（詳しくは、第 9 章を参照）が、主要なセキュリティ機能の特徴は、TOE のセキュリティ対策方針をまとめることで適切に説明することができる場合が多い。これは、すなわち、概説が、それをさらに詳細に記述している PP または ST の箇所と一貫していることを裏付けることになる。

大抵の概説と同様に、PP、または ST の後半部分(の記述)を完了させ、最後に概説を記載するほうがより簡単であろう。

# 8. 適合主張の規定

本章では、PP、または ST の適合主張に関する規定のガイダンスを提供する。ST の適合主張については、ISO/IEC 15408-1 の附属書 A.5 で説明しており、PP の適合主張については、ISO/IEC 15408-1 の附属書 B.5 で提供する。

PP、または ST の適合主張では、PP、または ST がどのように適合するかについて説明している：

a) *ISO/IEC 15408 適合主張*。これには、PP、または ST を実際に記述する（と共に、おそらく評価時にも）際に用いられた ISO/IEC 15408 の正確なバージョンのリストが含まれる。英語以外の言語で正式に翻訳されたものではない ISO/IEC 15408 が用いられている場合は、その旨が明記されていなければならない。正誤表、CC の解釈、及びそれを裏付ける文書を利用した場合も同様に、その旨をリストに明記しなければならない。

b) *PP主張*。これには、この PP、または ST が適合性を主張するすべての PP のリストが含まれる。簡単なリストで十分であり、ここには必要以上の情報を含める必要はない。

c) *パッケージ主張*。これには、PP、または ST が参照するすべてのパッケージのリストが含まれる。ISO/IEC 15408-3 で定めている保証要件のパッケージ（EAL）レベルのうちのいずれか 1 つ（場合によっては追加保証コンポーネントもあり）との適合性を主張するのが一般的である。パッケージの利用方法については、15.3 節で詳しく説明する。繰り返しになるが、ここも簡単なリストで十分であり、必要以上の情報を含める必要はない。

むろんのこと、本適合性は、その PP、または ST をベースにした任意の TOE にも適用される。

従って、PP を規定する場合、消費者は、他の PP と ST がその消費者の PP に適合する方法を明らかにしなければならず、それには、次のような 2 通りの方法がある：

a) 正確適合。基本的に、この PP に記載されているすべての要件が、適合性を主張する PP/ST に含まれていなければならない。詳しい要件については、ISO/IEC 15408-1 の第 8.3 節を参照。

b) 論証適合。基本的に、この PP に記載されているすべての要件は、適合性を主張する PP/ST と「同等」でなければならない。繰り返しになるが、詳しい要件については、ISO/IEC 15408-1 の第 8.3 節を参照。

ガイドラインでは、消費者が個人で利用する製品を購入、または構築の目的で詳しく完全な PP を記述する場合は、「正確適合」が要求される。自身で利用する以外の目的で PP の仕様を決定するならば、「論証適合」を用いればよい。

機能要件のパッケージ、または別の PP に対する適合性を主張する場合、消費者自身のセキュリティ課題定義、セキュリティ対策方針、及びセキュリティ要件が、その PP、またはパッケージに適合していなければならない。

PP、または ST の記述時に、参照している PP に含まれている要件からさらに要件を追加する際には、TOE がすべての要件を実装することができない、またはすべての要件を同時に実装することができないといった矛盾するような要件を記述しないよう、慎重を期さなければならない。

# 9. セキュリティ課題定義に関する規定

## 9.1. 序説

本章では、PP、または ST の*セキュリティ課題定義*（SPD： Security Problem Definition）節の仕様のガイダンスを提供する。ISO/IEC 15408-1 の附属書 A.6、及び附属書 B.6 で、PP、及び ST の SPD についてそれぞれ説明している。PP を説明している ISO/IEC 15408-1 の附属書 B.6 は、附属書 A.6 の単なる参照ではあるが、セキュリティ課題定義節で PP と ST の要件に相違点がないことを確認するために用いることができる。まさに、ISO/IEC 15408-3 の検証基準に関する語法が寸分違いないことを裏付けている。

セキュリティ課題定義の目的は、TOE が対応すべきセキュリティ課題の形式的な特徴やその範囲を定めることである。そのメカニズムを図 1 に示す。

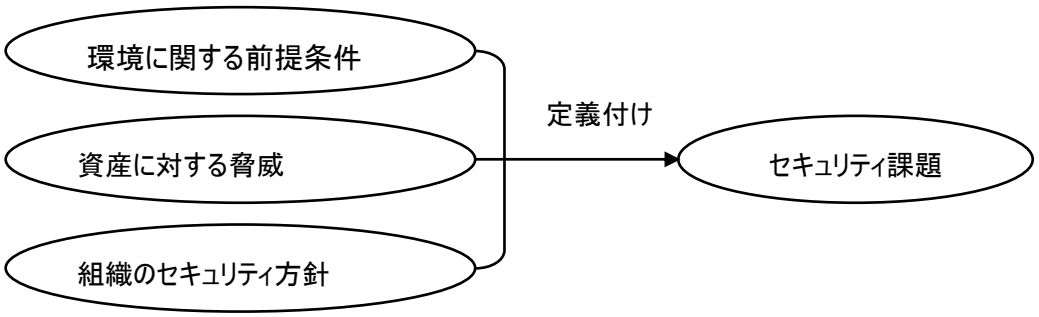


**図 1：セキュリティ課題定義付けのメカニズム**

PP や ST すべてに、セキュリティ課題定義が含まれているわけではないが（第 15 章参照）、セキュリティ課題定義は、PP や ST の中でも最も重要な箇所であるため、部外者にそういったセキュリティ課題定義を委託するのは最も危険な行為である。ここで ISO/IEC 15408 から、次のような要件を引用する：

「評価結果の有用性は ST に大きく依存し、ST の有用性はセキュリティ課題定義の質に大きく依存することに注意するべきである。したがって、良好なセキュリティ課題定義を引き出すために、多くの資源を費やし、明確に定義されたプロセス及び分析を使用するに値することがある（ISO/IEC 15408-1 の附属書 A.6.1）。」

指摘した課題が誤りであったり、その記述にあいまいな点があったりする場合は、PP、または ST の残りの部分が不適切になるだろう。また、有効ではあるが、不適切な仕様に基づいて、製品を選択、または調達した場合には事態はさらに悪化する。従って、本章では、ISO/IEC 15408 でも僅か数ページしか割いて説明していない標準ではあるが、本技術報告書の中で最も重要であると考える要件についてさらに詳しく説明する。本書の読者が開発者なのか一般消費者なのかに関わらず、または PP、または ST を記述する際に仕様、または選択をベースにしたプロセスを用いたのかどうかには関わらず、*セキュリティ課題定義を適切な方法で得ることが最も重要である。*

PP、及び ST の後半部分では、運用環境と共に TOE によってセキュリティ課題に対応する方法を提供する。従って、セキュリティ課題定義を明らかにする方法を明確にすると共に、簡潔でありながら、矛盾が生じない方法を確保することが重要である。

ISO/IEC 15408 では、セキュリティ課題定義を用意するための特定のプロセスや方法は提供していない。つまり、如何なる方法を用いてもかまわない。むろん、PP や ST の開発プロセスに新たに携わる者にとっては不親切としか言いようがない。そのため、本章では、実際に試用/テスト済みであり、さまざまな組織や環境で、その有効性が認められた（セキュリティ課題を明らかにする）簡単な方法を詳しく説明する。この方法は、一連の手続きを、順番どおりに実施するものである：

a） 非形式的なセキュリティ要件を識別し、確認する。

b） 形式的な脅威分析を実施し、それに対応する脅威を明らかにし、指定する。

c） それに適用可能な方針を文書化する。

d） それに適用可能な前提条件を文書化する。

e） 完結した SPD の仕様をまとめ、最終確認する。

どの方法を用いたかに関わらず、本技術報告書では、存在する非形式的なセキュリティ要件がセキュリティ課題定義に形式的に記述されているものと想定する。むろん、実際は、非形式的な要件を都合よく 1 つにまとめた文書などないかもしれないし、文書化すらされていないかもしれない。そのため最初の手続きとして推奨する方法は、まず非形式的な要件を識別して確認することである。それらがたとえ PP や ST に表現されることにならなくても構わない。非形式的な要件は自明であったり、既に定義済みであったりするかもしれない。あるいは SPD を作成する過程の殆どが単に非形式的な要件を識別することであるかもしれない。そして、マネジメントや関係者にそれが彼らのセキュリティニーズを正しく網羅した表現になっていることを確認する。

ISO/IEC 15408 では要求されていないが、この方法には、PP/ST 開発の最終段階で混乱や疑問が生じるのを防ぐことによって全体的な時間を確保するために実際に利用されている、2 通りの方法がある：

a） 重要視しなかった脅威の文書化。

b） 非形式的なセキュリティ要件に SPD を関連付ける際の根拠の明示化。

これらの方法については、方法の要所ごとに詳しく説明しているが、ざっと説明するならば、重要視しなかった脅威は製品に関係するかもしれないし、関係しないかもしれない脅威である。もし関係する場合は、他の理由で TOE に用意されたセキュリティ機能性で対抗される脅威である。こういった脅威が SPD で文書化されていないと、PP/ST を（参照用に）確認した消費者から質問が殺到するおそれがある。さらに深刻な事態になると、セキュリティ要件を変更した際に重要視しなかった脅威にも対応しているセキュリティ機能の重要性を無視し、削除されるおそれがある。

評価では、SPD は自明のこととして扱われるため、実際のセキュリティニーズを確認し直すものはいない。つまり、SPD の根拠が提供されなければ、SPD を作成するプロセスで非形式的なセキュリティ要件の一部が消失するかも知れないというリスクが常に付きまとい、製品が利用されたときにその製品の当初の目的と合致していないことが判明するまで、セキュリティ要件の一部が消失したことに気付く者はいない。従って、根拠は、適合性と完全であることを確認するための重要な手がかりとなる。

原則として、セキュリティ課題定義では、例えば TOE のセキュリティ機能に関する詳細な内容など、そのセキュリティ要件に合致する TOE の対応を形成するいかなる議論も、可能であれば避けるべきである。こういった原則を念頭に置くことで、（PP/ST の開発者は、）読者がセキュリティ課題を解決する際に重要なことは何かを考えることができるように導くことができる。TOE を利用してセキュリティ課題を解消する方法を論じることは、PP、または ST の後半の記述まで温存しておくこととする。むろん、非形式的なセキュリティ要件の一部として特定のソリューションが必須となっている場合には、SPD の一部としてそのソリューションを記載することになると思うが、確実にするために文書化しておくことと、後の設計に課す制約を正当化しておかなければならない。

### 9.2. 非形式的なセキュリティ要件の特定

#### 9.2.1. 序説

セキュリティ課題には、実にさまざまなものがあるーそして、そのソリューションについても同様で、セキュリティ課題定義という態勢がとられるより以前からソリューションとして確立されているものや既知のものもある。これらの要件や制約によって、非形式的なセキュリティ要件が形成されている。難しいのは、それらを洗い出し、文書にまとめることである。よって、この作業が、本技術報告書で推奨する方法の最初の手続きとなる。

#### 9.2.2. 情報源

##### 9.2.2.1. 概要

非形式的なセキュリティ要件の概要を確認する方法は、さまざまである。次項では、それらの方法の中からいくつかを選んで紹介する。組織の中には、本技術報告書の中で一般的な方法としては紹介していない、別な方法が用いられている場合もある。従って、（非形式的なセキュリティ要件）を特定するためには、セキュリティニーズを慎重、かつ包括的に考慮しなければならない。ただし、本節で提供している情報源が、非形式的なセキュリティ要件を特定する際に役に立つことだろう。

#### 9.2.2.2. 必要な機能性

セキュリティ機能性は、製品検討時の目的の一部である。そのことは、COTS 製品に特にあてはまる。なぜなら、アプリケーションプログラムインタフェース（API: application program interface）やヒューマンコンピュータインタフェース（HCI: human-computer interface）を通して調達者（購入者）が利用できるようになっているセキュリティサービスが、製品の仕様の重要な部分となることがあるからである。

ただし、セキュリティ機能性が、消費者のセキュリティ要件の一部として文書化されている場合は、SPD で対応すべき課題の一部と見なされる。

#### 9.2.2.3. リスク評定

セキュリティのリスク評定が、COTS 製品であっても提示されたシステムをカバーする範囲で既に実施されており、IT セキュリティ制御による軽減を要するリスクが識別されている場合がある。これらのリスクが、すなわち、セキュリティ課題である。

リスク評定を実施するには、さまざまな方法がある。ただし、これらの方法は一般的にリスクには 3 つの項目が存在することを受け入れている。何らかの方法で価値を侵害される資産、資産を侵害する何かあるいは誰かである脅威、及び資産が侵害される方法である脆弱性である。これらのいずれか 1 つでも存在しなければ、リスクは存在しないといっても過言ではない。このモデルの形式は、ISO/IEC 15408 で想定しているものである。実際のリスク評定がリスクのモデルと不適合であれば、SPD で適切な形式を用いるために、その評定結果を対応付けする際に課題が生じることだろう。

#### 9.2.2.4. 脅威評定

脅威評定とは、脅威が明らかになった場合、資産に損害がもたらされ、結果としてリスクが生じるという脆弱箇所のリスクを評定することである。この場合、明らかになった脅威は、セキュリティ課題の一部であることを示している。

脅威評定は、セキュリティ課題を特定/指定しようとしている人物が、保護される資産の所有者ではない、またはリスク評定や資産の価値を判断する立場にない場合に、特に望ましい方法である。

#### 9.2.2.5. マネジメント方針

セキュリティ要件は、例えば、特定組織のすべてのシステムには所定の標準を満たした IT セキュリティ制御が実装されている、といったマネジメントによって決定された方針をまとめたものである。このプロセスは、「最低限の標準」、あるいは「リスク回避策」と呼ばれることもある。方針には、例えば、「以下は、同業種の組織がすべきことである」といったように漠然としたものもあれば、「顧客によって課される法的な要件や契約時の諸条件と照らし合わせることができる」といった、論理的なものもある。

むろん、方針が法律や契約のように論理的な考え方に基づいたものであっても、必須のセキュリティ制御の中には特定のシステムや組織に相応しいものではなかったり、ごく一部しか適用できなかったりすることもある。

#### 9.2.2.6. 表現的な方針

セキュリティ要件は、しかるべき IT セキュリティ制御を実装していることを立証したいと思う組織、または COTS 製品によって生じたものである。また、方針は、市場のニーズによって、あるいは成功事例を見習おうとする消費者によって生じたものである。

承認されている評価機関によって所定の基準を満たしていると評価された製品やシステムに交付される正式な認証であり、しかるべき管理が実装されているという独立した証明にもなるという点で、セキュリティ課題は、ISO/IEC 15408 による評価に非常に適しているといえる。公開された PP は、適切な管理を明らかにするために用いることができる。

この種の方針の欠点は、既に認証されている、あるいは適合性が立証されているセキュリティ制御をベースにしており、実際に評価中の製品に関連するセキュリティ制御を選択することができないことである。これが仇となり、セキュリティ制御に必要な根拠となる SPD に十分な理由を提供することができないという課題が生じる。セキュリティ制御は方針として扱うこともできるが、セキュリティ制御の起案者がこれを嫌がるだろうというのが、管理を選択できない真の理由であろう。

#### 9.2.2.7. 評価方針

組織によっては、実装されているセキュリティ制御に関わらず、ISO/IEC 15408、またはコモンクライテリアに則った評価方法を用いて IT 製品が評価されるという方針がある。

この要件も問題含みである。対応すべきセキュリティ課題については、方針が作成されていないため、課題そのものが明らかになっていない。しかし、こういった方針は、実際にセキュリティ課題が検出されてから作成されるため、結果的には、ST を作成する際に、セキュリティ要件の中に含まれる。

### 9.2.3. 非形式的な要件の文書化

セキュリティ課題に関する最適な情報源は、セキュリティリスク評定の結果である。幸運にも、リスク評定の結果にアクセスすることができれば、その評定結果が包括的であることが判るばかりか、リスク評定方法の大半には、どの程度のリスクを容認することができるか、といった比例ベースの考え方が取り入れられており、被害による損失の割合が非常に低い、または損害によって被った損失があまり重大ではないという公算が見えてくる。容認できるリスクと容認できないリスクの両者を明らかにすることで、将来、PP や ST を設計する際にセキュリティ課題を修正することもできる。また、特定のリスクを排除するために必要な制御を実装したり、評価することが困難であることが判明したりする場合でも、別の潜在的なリスク用の異なったセキュリティ制御を用いることによって、システム全体で容認できるリスクレベルを維持することもできる。

第三者機関が彼ら自身の目的で作成したリスク評定では、上述と同様の方法でリスクを判断することができないことはいうまでもない。そういった場合には、評定結果を利用する際に注意が必要である。

リスクに関する問題が記載されていない場合は、修正や訂正ができないように漠然と記述されていることが多い。このような場合は、非形式的な記述で明記することが重要である。

関連情報の中には、開発すべき IT 製品のみならずその運用環境とも関連しているものがある。運用環境は、配置される要員、手続きや物理的な管理との関連でそのレベルが決定される。公共のスペースは、セキュリティニーズという点で、鍵付きのサーバルームとは趣を異にする。仮にしかるべき要員、手続きや物理的な管理が規定されていると考えることができるならば、それは、セキュリティ課題の一部を明らかにしたことに他ならない。

リスクや管理についての情報でも同様で、例えば、パスワードよりも生体認証を利用する、またはセキュリティ機能として定義されている http/https といった特定の通信用プロトコルを利用すると決定されているなど、特定のセキュリティ機能を実装する方法を、PP/ST の設計時に作成することができる。

ただし、セキュリティ課題の中には技術的な方法では解決できないものもある。これらは、要員、手続きや物理的な管理によってしか対応することができない。それらは、依然としてセキュリティ課題のまま、文書にまとめる必要がある。すなわち、さまざまな角度からセキュリティ課題であると判断されたものは、非形式的なセキュリティ要件の一部として文書にまとめなければならない。

（セキュリティ課題に関する）すべての情報を明らかにし、収集された情報について矛盾点がないことを確認したのちに、その情報は次のような 3 つのクラスに分類される：

a） 製品がほぼ間違いなく直面する潜在的な攻撃。

b） 製品が保持していなければならないセキュリティ特性、または特徴。

c） 製品が保持する必要がないセキュリティ特性、または特徴。

これらの情報は、次の手続きに進んだときの対処のしかたが異なるため、区分けをすることが重要である。潜在的な攻撃は、TOE に対する脅威として扱われ、対処しなければならない。必須のセキュリティソリューションを含め、製品が保持していなければならないセキュリティ特性や特徴は、組織のセキュリティ方針（OSP）に対応していなければならない。製品が保持する必要がないセキュリティ特性や特徴は、前提条件に含まれる。本書では、次項から順番に 3 つのクラスに区分けされた情報を説明する。

異なった情報源から導出された非形式的なセキュリティ要件は、別な箇所であっても重複していたり、矛盾していたりすることもある。識別された潜在的な攻撃に対し、潜在的に対応するセキュリティ特性や特徴を義務づけることは珍しいことではない。同様に攻撃の種類によっても、効果的に対処するのが非常に困難であったり、あるいは非常に高額であったりするために、明言されている関連のセキュリティ機能が必要ないものとして潜在的に考えられる

ことがある。こういった矛盾点は、非形式的な仕様を先に進める前に整理しておく必要がある。よってこの手続きでは、非形式的なセキュリティ要件をさまざまな角度から 1 つずつ表現することに集中すべきである。

## 9.3. 脅威の識別と特定方法

### 9.3.1. 序説

非形式的セキュリティ要件を文書にまとめることによって、攻撃やその属性が明らかになったならば、セキュリティ課題定義のための次なる論理的な手続きは、潜在的な攻撃によってもたらされる脅威を特定するための脅威分析を実施することである。ISO/IEC 15408 では、対象とする脅威を特定するための特定の方法については何ら規定していない。しかし、課題があると思われる TOE に関連すると思われるすべての脅威を特定しなければならない。

一般的に、脅威を分析したり、詳述したりすることは、方針や前提条件を定義するよりも複雑、かつ困難なケースが多いため、手続きの初期段階で対処しておくのが望ましい。一方、非形式的な要件が主に方針の決定や必須要件（前節 9.2 を参照）から導出されている場合は、最初に方針やセキュリティ課題定義の前提条件箇所（第 9.4 節と 9.5 節参照）の草案を作成し、本節で説明した脅威分析を実施すると共に、最終的に方針や前提条件を再度検討した上で完成させることも容易である。方針や前提条件を確認することが容易であれば、それらを利用して想定される脅威を直接軽減したり、排除したりすることができるため、脅威分析も簡素化することができる。

脅威分析を実施するには、次のような 3 つの手順を踏む必要がある：

a） 利用する（脅威の）分析方法を決定する。

b） この方法に必要な要員を特定する。

c） 方法を適用する。

これらの手順については、本章の次節以降で順番に説明する。

### 9.3.2. 脅威の分析方法の決定

対象とする脅威を特定するために最適な方法は、非形式的なセキュリティ要件を導出する際に用いられた方法によるところが大きい。その要件がリスク評定の結果に関連して特定されている場合は、リスク評定の結果の 1 つとして脅威のリストが既に利用可能なはずである。リスク評定を実施していない場合でも、既に存在するその他の情報から関連する脅威を特定することも可能である。

残念なことに、（脅威を特定するために）十分な情報が得られないケースが多いため、追加で脅威分析を実施しなければならない。

脅威分析に利用することができる方法には、実に多くの種類がある。ただし、ST や PP の開発者の大半が利用する方法は、次の 3 通りである：

a） 脅威ツリー分析。

b） 脅威データベースの検索。

c） アドホックな識別。

脅威ツリー分析が、適切な方法で文書にまとめられ、確立された技術であることは言うまでもない。これは、リスクの管理や信頼性工学（事例については、[4]、及び[5]を参照）で広く用いられている問題解析技術である、意思決定ツリーの構成をベースにしたものである。セキュリティの脅威分析に、最初にこの方法を適用した事例を記録したものが[6]である。

脅威ツリー分析は確立された技術であり、適切な方法で既に文書にまとめられているため、本技術報告書の中ではあまり詳しく説明しない。簡単に説明すると、一般的にこの脅威ツリー分析には、IT 製品の種別に対応した潜在的な脅威の完全なセットのおおまかな説明が含まれており、手続きの段階ごとに脅威を確認できるよう、反復的な方法でさらに詳しく説明されている。この技術では、最初の要約された（脅威の）説明を木の根と考えると、その根に関連するノードを新たに追加してより詳しく説明を加えることで新たなレベルが作成される。これらが、次なるノードの新たな木の根となる。最終的な木の葉となる（脅威の）説明は、十分な裏づけができるようさらに詳細化する

ことによって、PP や ST で特定される実際の脅威として利用することができる。このツリーは、PP や ST に内在する脅威を抽出する際の根拠を提供すると共に、これに関連する脅威が除外されていないという裏づけにもなる。

昨今では、Bruce Schneier[7]やマイクロソフト社の Trustworthy Computing Initiative という考え方の中で脅威のツリー分析の利用が提唱されている。まさに、マイクロソフト社発刊の最新書の中でさまざまなソフトウェア製品（[8]、第 22 章）に対応する脅威ツリーの事例が紹介されており、それぞれのソフトウェア製品に対応する TOE の分析作業を最小限度に抑えるためのモデルとして利用することができる。この方法は、正確、かつ適合性のある脅威ツリー（ibid、128 ページの囲みを参照）を構築することが困難なセキュリティの専門家ではない消費者に、マイクロソフトから注意を促すよりも効果的である。

2 番目の方法、すなわち脅威データベースの検索は、どの項目が対象の IT 製品に対して識別された攻撃にあてはまるかを調べるために、既に明らかになっている一つ、または複数の一般的な脅威のデータベースを徹底的に調査するという手法である。脅威に関するデータベースについては、さまざまな情報源を利用することができる。最も一般的な評価方法では、必要に応じて一般的な脅威と考えることができる情報が提供されるが、これには、検索可能なデータベースの形式が取られるのが一般的である。

データベースによる検索には多くのメリットと共に、それに相反するデメリットも存在する。メリットとしては、多岐に渡り、脅威と考えることができるさまざまな情報が提供され、それらが共通の方式で表示、または規定されていることである。デメリットの 1 つとして、特定の製品のみに対応する脅威があり、そのデータベースには含まれていないために、認識されないという点が挙げられる。また、データベースにおける脅威の記述が、当該製品への適用が可能か、容易に判断できないくらい一般的すぎるかもしれない。従って、対応すると思われる脅威が複数表示されたり、検索の仕方によっては漠然とした結果が導出されたりすることがあるという点に注意しなければならない。

3 番目の方法は、問題があると思われる IT 製品のみをベースとして、体系化されていない方法で脅威を特定する方法である。この方法は利用しないほうが良い。これは開発者や問題孕みの(製品の)所有者には、既成概念に捕らわれず物事を考えることは困難だからである。なぜならば攻撃者のほうが対応する脅威を特定するための経験や知識が豊富なこともあるためである。

セキュリティ課題やそれを取り囲んでいる環境の双方が適切に定義されている場合は、脅威ツリーの構築が、一般的には最も効果的な方法である。問題点がごく一般的なレベルでしか明らかにされていなかったり、それを取り囲んでいる環境が明瞭ではなかったり漠然としか定義されていない場合は、脅威データベースを単純に逐次検索するほうが、何がしかの方法論に基づいて包括的な分析を実施するよりもよほど効果的に対象となる脅威が提供されることだろう。この方法は、製品が利用される実際の環境についてあまり多くの知識がない、COTS 製品の開発者に適している。

要求されたセキュリティ分析によって対象となる脅威がまだ対処されていないことが脅威分析の結果で明らかになったとしても、方針や必須のセキュリティ機能によって非形式的セキュリティな要件があらかじめ導出されていれば、驚かされることはない。

利用した脅威分析方法や非形式的なセキュリティ要件の情報源によっては、識別されたものの、その後に軽減される脅威や、その他の要件（例えば方針）が重複して識別されるものもある。ISO/IEC 15408 では、SPD を包括的に理解し、特に変更箇所を反映させることが非常に難しくても、これらの脅威を*すべて*文書にまとめることは要求していない。本技術報告書においても、軽減された脅威のみを文書にまとめることを強く推奨する。通常、この作業は、SPD の前提条件の一部として実施する（9.5 項参照）。

### 9.3.3. 参加者の識別

#### 9.3.3.1. 序説

ISO/IEC 15408 の以前のバージョンでは、脅威を特定した上で説明することのみが要求されていたが、ISO/IEC 15408:2008 では、それぞれの脅威に付き、その脅威エージェント、（脅威を受けることが想定される）資産、や有害なアクションについても説明することを要求している－資産には、COTS 製品の場合、PP や ST の開発者は実際に保護すべき資産を知り得ないという点で、さまざまな資産が含まれるという解釈が成り立つ。

残念なことに、リスクや脅威分析の結果、及びその他の攻撃や攻撃方法の説明については、脅威エージェント、資産や有害なアクションの中で説明されていることはごく稀である：従って、利用可能な脅威や攻撃に関する情報を用いて、ISO/IEC 15408 で大原則として要求されるそれらの特徴を明らかにする必要がある。

#### 9.3.3.2. 脅威エージェント

ISO/IEC 15408 では、脅威エージェントを「資産に有害な影響を与える可能性があるエンティティ」として定義している。脅威エージェントを特定するためのガイダンスや、どの程度詳しく、正確に説明しなければならないかといった基準は設けられていない。PP や ST の脅威について説明する際には、その脅威エージェントをできる限りシンプルに説明するのが最適である。この方法で推奨する一般的な方法は、5 つの脅威エージェントについて特定しているリストを利用することである:

a) 攻撃者。

b) 承認された利用者。

c) 特権を持つ利用者。

d) 管理者。

e) システムの所有者と開発者。

*攻撃者*とは、IT 製品によって保護されている資産に不正な手段を講じてアクセスする者である。攻撃者には、承認された利用者ではあるが、その正体を隠してアクセスする者も含まれる。システム所有者にとって彼らは身元が確認されていない人物であるため、電話の逆探知や警備員による目視等によって、彼らによる攻撃の検知や人物の身元が特定できなければ、その対処に遅れが出てしまう。

*承認された利用者*とは、IT 製品のセキュリティ方針に則り、その利用を認められた人物で、資産の所有者の許可を得て、その製品によって保護されている資産にアクセスすることができる。承認された利用者はシステム所有者に知られている者であり、自らの活動に責任を負い、資産に被害が及ばないように保護する。

*特権を持つ利用者*とは、IT 製品のセキュリティ方針と相反し、資産の所有者による明示的な許可がなくても資産にアクセスすることができる者のことである。システム管理者の大半は、特権を持つ利用者である。ただし、特権を持つ利用者には、ハードウェアやソフトウェアなどの、メンテナンス技術者といった別な意味の特権を持つ利用者も存在する。特権を持つ利用者は、自らの行為に責任を持たなければならないが、IT 製品によって彼らによる攻撃を止めることはできない。

*管理者*とは、運用環境にインストールされた IT 製品が適切に動作することに責任をもつ者を指す。従って、管理者は資産に対する被害を防ぎ、被害を被っている資産を検知するための管理策を講じることに責任を負う。管理者の活動には制限が設けられているが、不適切な活動を実施した場合には、資産が第三者によって損害がもたらされるおそれがある。

*システム所有者と開発者*とは、システムや COTS 製品の仕様、設計、及び実装に責任を持つ者を指すが、それらによって保護される資産に必要以上にアクセスすることはない。システム所有者や開発者の行為によって資産に直接的な被害がもたらされることはないが、(仕様、設計、及び実装に)不適切な判断があった場合には、その製品が資産を適切に保護することができなくなるおそれがある。

こういった役割を理解した上で、個々の消費者は場面に応じ、時に複数の(実際にはすべての)これらの職務に携わることになる。脅威は、脅威エージェントの種別毎の行為によって、脅威の種別が区別される。

上述のリストには、複数のセキュリティ課題を持っていると思われる脅威エージェントが 1 つ除外されている。すなわち、人的行為が入り込む隙がない、例えば地震などの自然災害(「神の為せる業」と呼ばれることもある)である。システム所有者と開発者は、攻撃方法を画策したり、実行したりすることはないが、こういった脅威は、彼らの責任で対応されるのが一般的である。場合によっては、脅威エージェントとして「なし」、または「自然災害」と説明を加えることによって、脅威がより明確になり、問題を抱えている消費者が受け入れ易くなることがある。

#### 9.3.3.3. 資産の種別

脅威分析には資産が重要であり、資産を適切な方法で特定する必要がある。大半の脅威分析方法では、脅威エージェントや有害なアクションをあいまい、または重複して扱うことができるが、資産については明確、かつ適切な説明がされていなければならない。従って、本項では、特定の IT 製品を用いて保護すべき資産や資産の種別を特定する方法を詳しく紹介する。

システムの中には保護すべき資産を詳しく特定することができるものもあり、そのことがシステムの特性の一部となる。

COTS 製品の場合、その製品が実際にはどのような使われ方をするのかがはっきりしていないことが多いため、そういった製品では保護の対象となっている資産の種別を特定することしかできない。

IT システムに関連する資産は、通常、次のような 3 つのクラスに分類される:

a) 情報に属する資産。

b) プロセスに関する資産。

c) 物理的な資産。

*情報に属する資産*とは、それを所有する組織にとって価値があるデータのことである。情報に属する資産として分類されるものの例は:

- 一般的なデータ。
- システムに関するデータ。
- 専任者用のデータベース。
- 顧客データ。

専任者用のデータベースとは、ごく少数の消費者にとってのみ価値がある情報のことである。例えば、従業員のデータベース(人事部のみに価値がある)や顧客のデータベース(受注業務やマーケティング部門のみに価値がある)などがこれにあたる。顧客データとは、システムの所有者が保持することはないデータで、顧客に関する守秘義務が付随する特別なデータである。

システムでは、保護の対象となる実際のデータベースやその他の情報に属する資産の名称やその特徴を識別することができるのが一般的である。

ごく単純な事例では、同等の価値と攻撃に対するリスクを持ち、単独の情報に属する資産として扱うことができるすべてのデータを「利用者データ」などと呼ぶ。

ただし、情報に属する資産は、常にシステムデータ、つまり TOE の TOE セキュリティ機能(TSF)によって用いられるデータと他のデータを区別する必要がある。システムデータが改変されたり、削除されたりすると、TSF による機能が不適切に動作し、さまざまな攻撃を受けることがあるが、他のデータが改変された場合は、直接的な被害はそのデータが破壊されるだけで、TSF は動作を継続し、他の資産も継続して保護される。つまり、IT 製品によって保護される情報に属する資産は、TSF データとこれ以外のすべてのデータ(利用者データ)の 2 通りで構成されることが一般的である。

TSF データの種類により異なる攻撃に影響される場合や、侵害された場合の影響が異なる場合がある。このような場合は TSF データを区別する必要が生じる。例として、TSF データの種別には次のようなものがある:

- TSF 構成データ。
- 認証データのデータベース。
- 監査記録。

例えば暗号鍵など、ごく限られた特殊な形態を持つデータは、ある機能に特化した攻撃の影響を受け易いため、他のデータと区別しておく必要がある場合がある。

*プロセスに関する資産*とは、データを変換したり、分析したりする際に用いられるアプリケーションのことである。情報に属する資産との違いは、そのアプリケーションにデータの処理能力がなければ、それに関連するデータにはあまり価値がないという点である。例として、プロセスに関する資産には次のようなものがある:

- 金融/財務。
- 通信。
- 物流。

- 製造。
- オフィスオートメーション。

金融/財務関係のアプリケーションには、給与計算、投資管理、または会計管理などが含まれる。通信システムには、電子メールやイントラネット/エクストラネットの情報管理などがある。物流システムには、受注処理、倉庫管理や物流要員計画などが含まれる。製造関係のアプリケーションには、実作業処理管理システムなどがあり、オフィスオートメーションには、構造化テキストによるプロセシングなどが含まれる。

システムでは、保護の対象となる実際のデータベースやその他の情報に属する資産の名称やその特徴を識別することができるのが一般的である。

一般的にプロセスに関する資産は、改ざんや DoS 攻撃などによってのみ影響を受け易い。例えば、認証機能が削除されたり、金融/財務に関するプロセスが改変されたりするなどアプリケーションソフトウェアに関連の主要な機能が改変され易い。通常、「アプリケーションソフトウェア」やこれと同種の資産には、すべてのプロセスに十分対応することができる機能が備わっている。

*物理的な資産*(physical assets)とは、情報やプロセスに関する資産の支援に用いられる、実際の情報処理設備のことである。物理的な資産には、次のようなものがある:

- ネットワークの主要なインフラストラクチャ。
- ノートパソコン。
- データセンター。

TOE では、セキュリティ課題の一部として物理的な資産の保護を提案することはあまりない。物理的な保護は、除外されているか、運用環境で提供されるため、前提条件として扱われている。従って、物理的な資産が PP や ST で記述されることは稀である。ただし、電力の供給に不具合が生じた場合に、システムを自動的にシャットダウンすることで物理的な資産に保護を提供することができる場合は、適用可能な技術として PP や ST に記述されることがある。

ここで重要なことは、あまり多くの資産や資産の種別を特定しないことである。例えば、2 通りの資産や資産の種別に対して、同種の攻撃を受ける可能性があり、その攻撃の被害が同種のものである場合は、1 つの資産の種別としてグループ化すべきである。TOE の大半は、TSF データと利用者データといった 2 通りの資産しか保護することができない。また 6 種類以上の資産になると、非常に複合的な、あるいは個別的な保護機能を備えた TOE を除き、適切な保護を提供するには不適切である。

セキュリティ課題を明らかにする箇所では、所定の資産や資産の種別に必要な保護が削除されていることがある。このような場合には、これらの資産や資産の種別を別個にリストすべきである:なぜならば、こういった情報は、後に、脅威分析から削除された理由を説明する際に必要になるためである。

#### 9.3.3.4. 有害なアクション

ISO/IEC 15408 では、有害なアクションの記述方法については何ら定義していない。脅威エージェントとして、この規定で提供することができる最適な方法は、一連の活動をできるだけシンプルに記録することである。シンプルでありながら、包括的な一連の記録とは次のようなものである:

- 不正アクセス。
- アクセス権の不正な譲渡。
- 正当なアクセスの否認。
- 責任追跡性が伴わない活動。

こういったシンプルな一連の記録が、実際に見つかりそうなあらゆる脅威をカバーしていることがわかっているが、たまに特定の有害なアクションには、明確さを期すために個別に説明が必要な、異なった結果をもたらすことがある。その中には、上述のいずれのグループにも属さない、その他の、ある機能に対してのみ脅威となる有害なアクションが

含まれていることもある。このことは、非形式的なセキュリティ要件によって明らかにされるべきであり、これについても別個に対応する必要がある。

これに替わる方法には、例えば、機密性の消失というように攻撃によってもたらされた結果によって有害なアクションを説明することである。これは、以前、よく用いられていた方法で、非常に具体的に記述しなければならなかったが、それを利用することができる範囲が限られていたために、現在ではあまり利用されていない。

### 9.3.4. 選択した脅威分析方法の適用

脅威分析の方法が選択され、その方法の適用に必要な情報が集まったならば、次なる手続きは、対象となる脅威のリストを作成し、その情報に対応付けることである。

事実、脅威となる可能性がある要因の多くは即座に軽減することができる。この方法には、非常に有効な 2 つの技術がある－脅威には含まれないもの、あるいは容認できる脅威を特定することと、方針によって既に対処されている脅威を特定することである。

脅威の大半は、非形式的なセキュリティ用件の定義の一部によってすでに軽減されているか、その IT 製品の範囲(TOE)から除外されていたり、関連リスクによる影響が低い、あるいは第三者(例えば、保険業者)に委託されているなどの理由で、それらを容認することを決定していたりする。

これは、COTS 製品についても例外ではない－例えば、あるオペレーティングシステムのベンダが、調達/購入者が優秀なウイルス対策（AV）製品を追加で購入したり、その製品が感染しないように隔離された環境で利用されたりすることを想定して、その COTS 製品にはウイルス対策（AV）による保護を組み込まない決定をする場合である。

脅威の容認は、たいていシステムコンテキストにみられる。－これには、上述のような COTS 製品の製造者には不可能な、何か別の方法で資産を評価する必要がある。

脅威を軽減するための情報は、その製品には必要のない機能をリストにまとめることによって明らかになることが多い。明らかになっていない場合は、再度その製品には必要のない機能を見直し、リストに追加する。製品に必要のない機能は、前提条件としても記録しておくべきである（第 9.5.項参照）。

多くの IT 製品は、実際の脅威の分析には関係なく、既にセキュリティ機能を組み込むことが決定されている。これは COTS 製品についても例外ではない－例えば、ある製品が特定の消費者向けに設計されたものであっても、オペレーティングシステムのベンダが、その製品に識別認証機能を組み込む場合である。

こうしたデフォルトで組み込まれる機能が特定の種類の脅威に対抗する場合、必ず保護が提供されるので、その脅威に対してデフォルト機能が実際に適用可能かどうかを判断するための追加調査は必要ない。

存在しないものとして扱うことができる脅威についての情報は、IT 製品が保持していなければならない性質をリストにまとめることによって明らかになることが多い。明らかになっていない場合は、再度その製品には必要のない機能を見直し、リストに追加する。製品は必要のない機能は、方針文書としても記録しておくべきである（第 9.4.項参照）。

これ以外にもすべての脅威を特定し、検討した上で、脅威ごとにその脅威エージェント、対象となる資産や有害なアクションについて詳しく記述した資産の脅威による保護対象リストを作成しなければならない。

脅威の中には、特定のシステムのみに適用されるものがあるが、これは既にセキュリティ課題の対象となっており、運用環境のセキュリティ対策方針によって対処される。脅威の中には、環境的な対策よってのみ対処できるものもある（例えば、物理的な保護が必要な場合）。こういった脅威についてもリストにまとめる必要があり、これらは環境的な対策を講じる際のエントリと共に貴重な記録としても有効である。こういった情報は、後に、非常に役に立つ。

ただし、これらの情報が TOE やその環境のどちらでも対処することができるのならば、脅威を対処する方法を先入観で判断してはならない。これは、後に管理策を選択し設計する際に、設計の選択の余地がなくなるためである。

ISO/IEC 15408 の以前のバージョンでは、IT 製品（すなわち、その開発環境）の開発時における脅威は、脅威分析に含めることが規定されていた。しかし、ISO/IEC 15408:2008 では、何も規定されていない。従って、評価者を混乱させないためにも、脅威の分析には、こういった不必要な情報を含めてはならない。

### 9.3.5. 実践的な勧告

脅威は、IT 製品が攻撃され得る方法を示す手がかりとなる。従って、脅威を説明する場合は、そのような言葉を用いるべきである。最適な方法は、「～かもしれない、～となることがある（may）」のような動詞を利用することである。例えば:

*T.UNAUTH 許可されていない人物が不正アクセスを試み、TOE リソースを搾取するかもしれない。*

脅威についての説明を記述する場合は、対象となる脅威の名称から始めると判り易い。慣習として、PP や ST の作者の大半は、識別し易くするために脅威に関連する記述には識別子として T（threat）を用いている。説明は、短めに、要点のみを記述すべきである。

本章で説明されているものであっても、消費者自身で選択したものであっても、方法は無分別に利用してはならない。方法は、セキュリティ課題の要件に対応するよう調整した上で解釈されなければならない。あるカテゴリに分類した方法によって実際にはあまり良い結果が得られなかったとしても、問題に立ち返り、別な方法を用いてその問題を対処することに躊躇してはならない。

脅威エージェント、脅威の対象となっている資産や有害なアクションが類似の脅威は、まとめて記述することができる。類似の脅威には同じ管理策が用いられることが多いため、脅威についてまとめたリストのサイズを低減することができるため、後に、それを対処するための時間を節約することができる。同様に、脅威エージェントや脅威が対象とする資産など要素によって顕著に異なる脅威の場合は、その脅威を複数に分割し、より具体的な言葉を用いて明確に記述することで、後に、それを対処するための時間を節約することができる。

脅威を軽減するための情報は、間接的な表現で記述されることが多い。次のような文言を例に挙げてみよう:

*管理者は、悪意のない、信頼のおける十分な能力を持つ人物であると想定される。*

この文言は、脅威エージェントについて述べたものであるが、通常、こういった脅威エージェントと関連する脅威の種類の大半が効果的に軽減されるような表現方法が用いられている。こういった種類の脅威は、管理者に特化したものであり、これらを全面的に軽減することができる。その他の脅威も当てはまらないわけではないが、例えば、一般利用者など、管理者の他にも適用可能な脅威エージェントのみに限定される。前提条件のリストに、これら脅威の範囲を減少させた前提条件を加えることを忘れてはならない。

中には、脅威エージェントや有害なアクションを特定できないことがある。関連するリスクは黙認できないだけである。例えば、それに関連するセキュリティモデルを実装している下層の抽象マシンの不具合である。こういった場合は、推測や想像力を働かせて、その脅威の特徴を捉えることは無意味である。従ってそういった脅威は、セキュリティ課題として明らかにすることはできないため、そのようなものであることが正当な理由と共に識別すべきである。

脅威についてまとめたリストの作成が終了したら、常に完全性と、矛盾点はないかを確認すべきである。脅威が、対象とする資産や脅威エージェントなどで分割されている場合は、その脅威によってもたらされるすべての影響が網羅されているか？類似点の多い脅威には、同様の方法で対処されているか？そうでない場合は、裏づけとなる十分な根拠があるか？PP や ST の作成時には、後に、矛盾点や脱落箇所が見つかる場合が多いため、この段階で確認することで時間を節約できるばかりではなく、後戻りすることもない。

脅威分析では、TOE で対応することができる脅威として、リストにまとめるべき脅威が特定できないこともある。例えば、一般企業や政府の方針以外には対応しないように設計されている PP がこれに相当する。こういった PP は、間違いなく、ISO/IEC 15408 による評価において支障なく受け入れられる。そういった場合は、脅威について記述する箇所は空白のままとし、特定の脅威が認識されていない旨を明示しなければならない。

過去を見ても、受け入れられている一般的な PP は、適用する脅威を少数特定しているか、または適用する脅威を特定していない。例えば、読者がさまざまな目的に使えるような PP を作成した際に、それらを対象とする複数の脅威が特定された場合、現実的ではない状況や、必要以上の制限のある状況を、無意識のうちに想定していないだろうか？

## 9.4. 方針の識別と特定方法

セキュリティ課題定義には、TOE が対応する組織のセキュリティ方針（OSP）のリストも含まれていなければならない。脅威に比べると、方針は、それを特定することも記述することも容易な場合が多い。本書が推奨する方法を用い

ている場合、読者は、IT 製品が必ず備えていなければならないセキュリティ属性、または機能のリストが既に手元にあるはずである。それらを書き換えることで、OSP を作成することができる。

方針とは、脅威やその他の問題点を考慮することとは別に、IT 製品によって必ず実行されなければならない項目を文書にまとめたものである。従って、方針はそのような言葉で表現すべきである。英語で書かれている基準にはこういった要件を示す際に「しなければならない（shall）」という助動詞が用いられる。英語が母国語の人々には不自然と思う方のほうが多く、「するだろう、できる（will）」という助動詞のほうを好まれる方が多いのではないだろうか。従って、方針を明確、かつ適切に表現するには：

*P.IDAUTH 管理者は、TOE の機能やデータにアクセスする前に、自身を認証できる。*

脅威と同様、目的の対象となっている方針の名称から始めると判り易い。方針の説明は、短めに、要点のみを記述すべきである。慣習として、PP や ST の作者の大半は、識別し易くするために方針に関連する記述には識別子として P（policy）を用いている。

ISO/IEC 15408 では、方針とは、通常、組織のセキュリティ方針を指し、OSP と省略される。これが混乱を招くことがあるーなぜならば、OSP の中には、組織が所有するすべてのシステムというよりも、PP、または ST が対象としている特定のシステムのみに適用できるものがあるためである。本技術報告書では、単純に「方針」という用語が用いられている。

対象となる方針の大半は、非形式的なセキュリティ要件の特定時、または脅威分析時には特定されているべきである。ただし、セキュリティ課題に関連の方針がすべて特定されているかを最終的に確認すべきである。

方針では、次のような項目が定められる：

- TOE に組み込むべき必須のセキュリティ機能。
- （組み込むべき機能を黙示的に要求する）特定のセキュリティ機能の実装に用いられる必須の技術/技法。

方針は、次の各項目に該当する場合、脅威を置き換えるときにも利用することができる。

- 特定の脅威が存在するかどうかは明らかではないが、以下にかかわりなく、その脅威から保護するための方針が定められている。
- 特定の脅威に対し、例えば次のような活動を指定するなど、その対処方法が方針に組み込まれている：
  - どのような管理策が、攻撃で損害を受けることを防ぐか、または
  - 攻撃を受けた場合には、どのようなことをすべきか？
- 方針には、複数の関連する脅威を対処することができる、特定の方法が組み込まれているか？

ただし、脅威について説明している文書の中で、方針に（脅威に関する）情報が追加されていることが明示的に示されていない場合は、方針の中で脅威を置き換えることは何ら価値がない。

このように最終的な確認の段階で認識された方針では、例えば、現在はその方針で対処している脅威を削除するなど、既に明らかになっていたセキュリティ課題の説明の記述の変更や書き換えが必要になることがある。

事実、大半の方針は認識することも明示的に示すことも容易である。ただし、こういった方針の中にも注意すべき共通の問題点がある。

時に、方針では、TOE の運用環境で実行しなければならないことの替わりに、TOE の運用環境でしてはならない、または実行することができない要件を示すために誤って用いられることがある。TOE がある要件を実装することができなかった場合、それを適切に特定する方法が、運用環境に関する前提条件（第 9.5.項参照）である。TOE と運用環境、またはその双方で策定中の方針を実行することができない場合は、その方針のステートメントが意味を成さない、目的の達成が不可能なものになる。

セキュリティ課題やそのソリューションを明らかにする段階では、策定中の TOE の境界を変更する必要が生じたり、TOE からその運用環境、または運用環境から TOE に機能を移動したりしなければならないことがある。方針が前提条件になったり、前提条件が方針になったり、あるいは、新たな TOE の境界を考慮するために、方針や前提条件をあらためて明示化する必要が生じる原因となることがある。同様に、複数のセキュリティ課題に対処するために複数のコンポーネントに分割された統合 TOE では、あるコンポーネントを対象にした、ある前提条件が、別のコンポーネントでは方針要件として実装されることが多い。このような場合は、方針のステートメントの表現方法を慎重に検討することによって、コンポーネント間の適合性や整合性を容易に確保する手段を講じると共に、その他の SPD に対応する前提条件として再度利用することができる。

時に、セキュリティ課題定義を明らかにする段階では、方針は TOE の実装、または運用環境のどちらによって対応されるのかははっきりしていない。これは、セキュリティ機能要件が明らかになれば、セキュリティ対策方針を明らかにする段階ではっきりするため、現時点ではこのままでかまわない。TOE の対策方針と環境の対策方針の双方は、方針に立ち帰る(link back)することができる。方針は、部分的にであっても TOE とその環境に実装されることがある。

すべてのセキュリティ課題に方針が必要なわけではない。こういったセキュリティ課題は、間違いなく、ISO/IEC 15408 による評価の対象となる。この場合、方針について記述する箇所は空白のままとし、特定の方針が認識されていない旨を明示しなければならない。

### 9.5. 前提条件の識別と特定方法

最後に、セキュリティ課題定義には、TOE の中で要求されているセキュリティ機能を制限、または排除する前提条件のリストが含まれていなければならない。本書が推奨する方法を用いている場合、IT 製品が備えていなくてもよいセキュリティ属性、または特性のリストが既に手元にあるはずである。これらは、TOE の環境、または利用法に関する前提条件にするために表現を書き換えることができる。

前提条件とは、脅威やその他の問題点を考慮することとは別に、IT 製品が実行しなくてもよい項目を文書にまとめたものである。従って、前提条件では事実が伝わるような表現方法にすべきである。前提条件を明確、かつ適切に表現する例は次の通りである:

*A.PHYSICAL TOE は、物理的に安全な場所に設置される。*

前提条件には、2 通りの利用法がある:

- 運用環境によって提供されるが、TOE によって提供されない特定の管理策、または管理策の種類を示すこと。
- 想定された運用環境には存在しないか、あまり重要ではないために、軽減することができる特定の脅威、または脅威の種類を示すこと。

上で紹介した最初の前提条件は、TOE によってではないが、管理策が必ず提供されなければならないという意味が含まれているため、「するだろう、できる(will)」という助動詞を用いた最適な表現である。2 番目の前提条件は、「である(is)」のような能動態の、現在形の動詞を用いた最適な表現である。

環境によって提供された管理策に関する前提条件と軽減された脅威に関する前提条件は、前者が ISO/IEC 15408 によって要求され、後者は本技術報告書が推奨する、対象となるすべての脅威が含まれるセキュリティ対策方針を簡単に示すことを目的として追加されたものである、という点で区別している。これについては、後に、説明する(第 10.2.項参照)。

前提条件には、後に、容易に参照することができるように、短い名前を付すべきである。前提条件は、短めに、要点のみを記述すべきである。慣習として、識別し易くするために、前提条件の名前には識別子として、「A(assumption)」を用いている。

実際は、前提条件を明確、かつ肯定的に表現するほうが、方針や脅威を同様に表現するより難しい。従って、「してもよい(may)」や「するべきである(should)」のような助動詞を衝動的に用いてはならない:前提条件は、事実を記述する文書である。

運用環境に関する前提条件は、次のような 3 つのクラスに分類する必要がある:

- 物理的な保護。

－ 人的、及び手続き的な保護。

－ TOE 外の技術的な機能。

ISO/IEC 15408 では、「運用環境の物理的条件、人的条件及び接続に関する条件（ISO/IEC15408-1、附属書 A.6.4）」と規定されている。ただし、これだけでは十分ではないことが実践で明らかになっている。外的な技術的管理策に関する前提条件の大半は、当然のことながら接続に関する条件に分類される。例えば：

*A.INTERNET TOE は、インターネットから隔離される。*

ただし、技術的な管理策に関するその他の前提条件が必要になることが多い。例えば：

*A.NO_DEV_TOOLS TOE の運用環境では、一般利用者に利用を許可したり、システムに新たな機能性を追加したりするようなツールは提供されない。*

方針や脅威は、部分的に TOE と環境で対処される場合が多い。例えば、TOE の技術的な管理策では、効率の良い運用を提供するために、支援的な手続きや物理的な対策が必要になることがある。環境での、そういった支援策の必要性は、前提条件として認識し、表現しなければならない。

前提条件は、常に有効、かつ真実であるとして、評価時に試験されることはない。前提条件は、一貫性や完全性を示す際に有効である。方法論的なアプローチにより、脅威が識別された場合、前提条件はその根拠で完全にカバーされている必要がある。それによって、部分的にではあるが、脅威を軽減し、対処することができる。この場合、セキュリティ対策方針によって対策された脅威箇所にさかのぼる際に、前提条件は、その根拠に完全に含まれていることを示す必要がある。

前提条件は、非形式的なセキュリティ要件を定める場合、または脅威分析時に認識されるものが多い。ただし、その他にも関連する前提条件を認識するため、セキュリティ課題を明らかにする手続きの一貫として全体的な確認をすべきである。方針を実装するか、または運用環境によって脅威に対処するかという決定は、常に前提条件として記録しておかなければならない。こういった前提条件は、方針や問題のある脅威が反映されるような表現をすべきである。なぜならば、前提条件は、こういった方針や脅威を対象とする運用環境の対策方針となるためである。

1 つの前提条件は、どこかが関連している複数の脅威を対処するために用いられることが多い。もし脅威ツリーのアプローチが用いられるなら、複数の詳細な脅威、全て環境によって対抗され、共通の階層ノードをさらにのぼっていき、前提条件は共有ノードのレベルで表示されるべきである。例えば、管理者の悪影響をもたらす活動の結果生じたすべての脅威は軽減される場合、これは単一の前提条件として次のように表現することができる：

*A.NO_POOR_ADMINISTRATION 管理者には、自身に割り当てられたすべての管理機能を実行するための技術、訓練、時間、及びリソースが提供されており、これらすべての機能を正確に実行する。*

適切、かつ必要な前提条件を作成するには、文言が不正確だと、TOE が間違いなく攻撃されてしまうことを考慮することである。

前提条件をその種類ごとに分類することによって、セキュリティ対策方針の認識や明示化がし易くなる。人的、手続き的、及び物理的なセキュリティに関する前提条件は、初期段階で分類すべきである。次に、IT の運用環境で提供されるセキュリティ機能に関する前提条件を対象とし、最終的に、軽減された脅威に関する前提条件を対象とすべきである。これらは、セキュリティ対策方針には関連しないため、分離させておくべきである。

セキュリティ課題の中にも、前提条件を全く必要としないものがある場合がある。これは、間違いなく、ISO/IEC 15408 による評価の対象である。そういった場合は、前提条件について記述する箇所は空白のままとし、特定の前提条件が認識されていない旨を明示しなければならない。

### 9.6. セキュリティ課題定義のまとめ

SPD 作成の最終段階が、SPD の仕様のまとめである。これには、次のような 2 通りの作業が必要である:

- 脅威、方針、及び前提条件のすべてを網羅したリストの作成。
- SPD の仕様が、セキュリティ課題や非形式的なセキュリティ要件が対処する問題を正しく表現しているかを確認する適合性、及び完全性チェック(欠落検査)の実施。

ISO/IEC 15408 では、SPD の根拠に関する要件については、何ら規定していない。SPD に記載される脅威、方針、及び前提条件の記述は、自明のこととして扱われる(SPD を引き出すプロセスは評価の範囲外である)。ただし、SPD の要素ごとに対応する非形式的なセキュリティ要件と相互参照することで、重複箇所や冗長箇所がないこと、及び網羅的に対処されていることを示す根拠を提供することを強く推奨する。後に、要件に変更があったり、複合箇所が検出されたりする場合は、SPD を簡潔にし、エラーの原因となるリスクを低減するために、根拠の改訂作業を実施する。

同様に、ISO/IEC 15408 では、軽減、もしくは無視された脅威を認識するための要件も何ら規定していない。繰り返しになるが、環境に変化があったり、SPD がやり直しになったりする場合には、こういった情報が非常に有効である。本技術報告書では、こういった脅威に関する前提条件を常軌的に含めることを推奨する。ただし、これらの前提条件は、運用環境に関する前提条件と区別し、SPD の独立した項目であることが判る箇所に記載する。これによって、セキュリティ対策方針と相互参照する際に無視されがちな SPD を検証する評価者へ注意を促すことができる。

適合性と完全性チェック(欠落検査)には、対象とするセキュリティ課題が方針や前提条件に反映されていると同時にすべての制約や要件が含まれており、認識されたすべての脅威が何らかの方法で対処、もしくは軽減されているかの確認が含まれる。また、SPD でリストにまとめられたすべての方針、脅威や前提条件は、非形式的なセキュリティ要件の草案ともさまざまな角度から相互参照すべきである。相互参照表を作成することで、適合性や完全性チェック(欠落検査)を効果的、かつ容易になる。

時に、前提条件や方針は、矛盾しているように見えることがある。すなわち、ある会社の方針要件では「X を実行する。」とあるが、これに反し、前提条件では「X を実行する必要はない。」と表現されている場合である。調べたところでは、TOE は、認識されたセキュリティ課題のすべてではなく、その中の一部に対応することが求められている、という点で実際には何ら矛盾点は見つかっていない。実際のセキュリティ要件を記述する場合には、詳述な説明と共に的確な表現を用い、明らかな矛盾点を解消する必要がある。実際に矛盾点がある場合は、実際にはどのような非形式的なセキュリティ要件を確立したかったのかを再確認し、この矛盾点を解消しなければならない。

## 10. セキュリティ対策方針の特定

### 10.1. 序説

本章では、ST、または PP におけるセキュリティ対策方針を識別、及び明示化すると共に、ISO/IEC 15408-1 の附属書 A.7、及び附属書 B.7 でそれぞれ説明されている要件のガイダンスを提供する。セキュリティ課題定義として、附属書 B.7 は、附属書 A.7 の単純な指針に過ぎないが、いずれの場合も想定される(セキュリティ課題の)内容が同一であることを強調している。セキュリティ課題定義に関しては、ISO/IEC 15408-3 では、検証する要件が同一の内容となっている。

*セキュリティ対策方針*では、*セキュリティ課題を対象とした対応方法が簡潔に*定められている(ISO/IEC 15408-3、第 9.4.1.従属節、及び第 10.4.1.従属節)。セキュリティ機能要件(第 11 章参照)の本当の仕様がこの対応であると誤解すべきではない。詳細な SFR と抽象的な SPD を関係付けて、必要となるセキュリティ機能の概要や構造を表現することがセキュリティ対策方針の最良の役目である。言い換えれば、SPD において何がセキュリティ事項であるかが記述された後には、それらを TOE やその環境にどのように対応させるかを方向付ける必要がある。

ISO/IEC 15408 では、次のような 2 通りの異なった種類のセキュリティ対策方針を定める必要がある:

a) TOE によって実装された技術的な(IT)(セキュリティ)対策を満足させる TOE のセキュリティ対策方針。

b) IT 環境、または IT 環境以外の(例えば、手続き的な)(セキュリティ)対策のいずれかによって実装された技術的な(セキュリティ)対策を満足させる運用環境のセキュリティ対策方針。

以下の図 2 を参照。

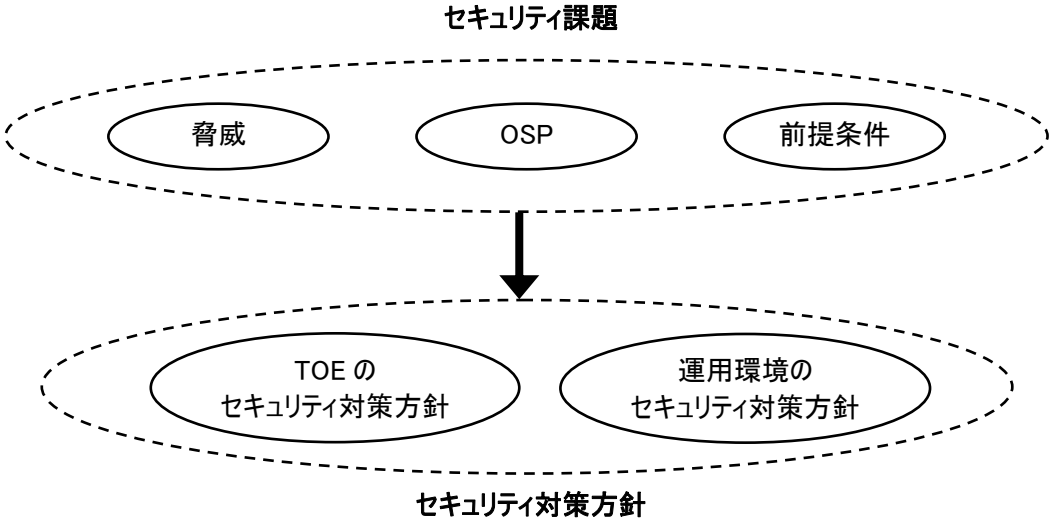


**図 2:セキュリティ対策方針の役割**

すべての ST と PP には、運用環境のセキュリティ対策方針を定めなければならない。低保証の PP や ST(第 15 章参照)では、TOE のセキュリティ対策方針を定める必要はないが、運用環境のセキュリティ対策方針は自明として扱われる。すなわち、運用環境のセキュリティ対策方針は、セキュリティ課題定義へさかのぼる必要がない。

本章の後半部分は、双方のセキュリティ対策方針が要求されており、セキュリティ課題定義へさかのぼるという前提で説明を続ける。

セキュリティ対策方針は、要件として表すべきである。セキュリティ対策方針は、簡潔、かつ明瞭に記述すると共に、それに関連の SPD で認識されたセキュリティ課題に対する高次なソリューションの定義が含まれるべきである。英語では、助動詞「ねばならない(must)」が、セキュリティ対策方針を表現するのに適切である。

ISO/IEC 15408 では、セキュリティ対策方針を作成するための特定のプロセスや方法を前提としたり、必須としたりしていない。自身が好きな方法を用いることができる。むろん、PP や ST の開発プロセスに新たに携わる者には、これでは役に立たない。本章には、従って、実際の現場で試され、試験され、さまざまな組織や環境で正常に機能することが確認された簡単な方法を詳しく説明する。この方法では、以下の手順を順番通りに実施するだけである:

a) セキュリティ対策方針に含まれるすべての脅威、方針、前提条件のリストの作成。

b) IT 運用環境以外の対策方針の特定。

c) IT 運用環境の対策方針の特定。

d) TOE の対策方針の特定。

e) 認識された脅威、方針、及び前提条件へさかのぼる対策方針根拠の作成。

以下の各項で、これらの手順を説明する。この方法では、上述の手順を順番に実施するのが最も効果的である。

むろん、これは、対策方針を特定する方法の 1 つに過ぎない。これ以外にも、同じように有効な方法があるが、状況によっては、簡単で、即座に、あるいは容易に実施可能な方法ではないこともある。躊躇せずに、さまざまな方法を試すのも一案である。

セキュリティ対策方針は、PP や ST で重要な役割を担っているため、セキュリティ対策方針を記述する際は、どの程

度のレベルまで詳しく説明するのが適切かを考えることが重要である。ISO/IEC 15408 では、セキュリティ対策方針が、（上でも指摘している通り）*簡明*でなければならない旨が述べられており、これがセキュリティ対策方針の作成に優秀な着想を提供している。事実、次の 2 つの関連項目のバランスを保つ必要がある：

a)セキュリティ対策方針は、SPD で必須となっているセキュリティ対策方針を除き、その実装内容に踏み込まずに、TOE によって対処すべきセキュリティ課題定義で認識されたセキュリティ関連の課題を読者がどのように理解するかを支援すべきである。理想的には、TOE のセキュリティ対策方針は、実装－独立型であるべきである。従って、セキュリティ対策方針では、それを確立する*方法*ではなく、それを確立するためのソリューションは*何か*が中心になる。

b) それと同時に、定義されたセキュリティ対策方針が、例え僅かに異なっているだけであっても、脅威や OSP のセキュリティ課題定義の中で同じ情報の繰り返しの終始にならないようにすべきである。

セキュリティ対策方針の根拠やセキュリティ要件を作成する場合には、セキュリティ課題をどの程度まで適切なレベルで詳しく説明しているかが 1 つの目安となる。一方がごく平凡な根拠であるのに対し、もう一方が誇張しすぎで、複雑になり理解しにくい場合は、いずれかの手順が複雑すぎるために、セキュリティ対策方針が詳しすぎたり、漠然となりすぎたりしていることが多い。

本技術報告書の次の章ではっきりすると思うが、TOE で明確にされた一連のセキュリティ対策方針によって、それらに対応するよう選択されたセキュリティ機能要件が過剰ではないことを確認する目安となる。これによって TOE の評価に必要な費用や時間を最小限に抑えることができる。

### 10.2. 脅威、方針、及び前提条件のしくみ

最初の作業は、SPD から対象となるすべての脅威、方針、及び前提条件の完全なリストを作成することである。

脅威の中には TOE と関連するものがあるという説明をしたと思うが、リスク分析や環境を考慮することによってそれらの脅威が軽減することができる、あるいは無視することができると判断されていることがある。本技術報告書で推奨する方法に従うのであれば、こういった脅威を SPD に含めると共に、脅威には当てはまらない旨を明示し、前提条件としても記録する。こういった脅威についてはセキュリティ対策方針を作成しないため、最初の作業は脅威とそれに関連の前提条件を識別し、今後の検討事項からこれらの脅威や前提条件を除外することである。この方法で、SPD から TOE と関連する脅威が除外されていることを確認する。

潜在的な脅威、方針、及び前提条件は種類ごとに分類すべきである：

- IT 運用環境以外に関連するもの。
- IT運用環境に関連するもの。
- TOE の機能性に関連するもの。

これは、見た目よりも容易なことが多い。物理的な管理策に必要な方針は、IT 運用環境以外のみに適用することができる。TOE を直接攻撃する可能性を示す脅威は、TOE の機能性に含まれる。すなわち、前提条件は、運用環境に関連する脅威のみに適用することができる。方針や要件が複数箇所に及んでいる場合は、それらを分割し、それぞれが種類ごとに割り当てられるようにすべきである。

例えば、脅威 T.EAVESDROP は、次の 2 つに分割することができる：

- T.EAVESDROP IT 運用環境に割り当てられた（通信）。
- T.EAVESDROP TOE の機能性に割り当てられた（内部）。

確信がもてない場合には、対応する方針や脅威を分割してみるとよい。不必要なものは、後に、容易に削除することができる。一方、必要なものが欠落している場合には、対策方針が欠落する原因となることがあり、PP/ST 確認時に検出することが困難である。

### 10.3. IT 運用環境以外の対策方針の識別

一般的に、TOE よりも運用環境の対策方針の定義のほうが容易であり、IT 環境の対策方針よりも IT 運用環境以外の対策方針の定義のほうが容易である。IT 運用環境以外の対策方針から着手するのはこのためである。

これらの対策方針を識別するための最初の手順は、IT 運用環境以外で割り当てられたすべての前提条件を対象に、1 つずつ対策方針と適合するように表現方法を書き換えることである（本項の後半に、その方法のガイダンスを提供している）。運用環境の対策方針は、PP や ST、または評価中にさらに分析されることはないため、共通点や一般的な表現や重複箇所などを識別することに意味がなく、記述される対策方針が、はっきりと理解し易いように記述されていればよい。

次に IT 運用環境以外の対策方針に割り当てられた脅威や方針をさまざまな角度から適合させることができるように検討が重ねられ、さらに目的が追加される。繰り返しになるが、関連する脅威や方針を対策方針として表現し直す場合でも、拡張したり、説明を追加したりしてはならない。適切な表現方法は、簡単に見つかることが多い。そうでない場合は、分類のテクニックは 10.5 項で説明されている TOE の対策方針の表現方法を流用することができる。

IT 運用環境以外のセキュリティ対策方針には、次のようなものが含まれることがある：

a） TOE が、安全な方法で使用されることを保証する手順(及び、特に環境的な前提条件にしたがって)の確立と導入。

b） 管理者や一般利用者が健全なセキュリティを実践するための教育やトレーニング。

これらは、TOE のセキュリティ対策方針に対応しているため、この段階で識別するのはまだ困難である。それらが明らかになっているのであれば、この段階で追加する。そうでない場合は、この方法の最終段階で運用環境の対策方針を再確認し、それらを追加する。

運用環境の対策方針では、認識し易くするために「OE.」で始まる名前が付されることが多い。これによって、通常「O」で始まる TOE のセキュリティ対策方針とはっきり区別することができる。運用環境の対策方針では、その目的の対象となっている（セキュリティ）対策が手続き的なものか物理的なものかを示すために、はっきりと表示すべきである。必要に応じて、明確に「IT 運用環境以外」の対策方針の記述である旨を記載する。

前提条件から導出された運用環境の対策方針は、前提条件の表現を変えずに、つまり事例として、適切に表示される。例えば：

*OE.RESIDUAL 磁気メディアは、最終的に廃棄する前に消磁、または断片化する。*

脅威や方針から導出された対策方針は、要件に適合するように表現すべきである。例えば：

*OE.AUD_REVIEW オペレーション要員は、例外的な監査痕跡や異常な活動証跡を定期的に確認する。*

IT 運用環境以外の対策方針の大半は、前提条件から導出される。脅威の検討事項から導出された対策方針だけの場合は、セキュリティ課題定義から前提条件が欠落している場合があるため、SPD を確認し、必要に応じて訂正する。

便宜的に、関連する前提条件が複数含まれている場合、前提条件とそれに関連の脅威が含まれている場合、あるいは方針とそれに関連の脅威が含まれている場合は、単一の対策方針を定義することができる。最終的にセキュリティ対策方針が明確になるのであれば、これらの要素を組み合わせるほうが賢明である。明確にならない場合は、単一の対策方針のままで構わない。

IT 運用環境以外の対策方針を満足させることは、評価を受ける IT 製品を用いる組織の責任となる。したがって、この段階で、システム運用に携わる者（COTS 製品の場合は、マーケティング部門）がこれらの対策方針が、現実的、かつ達成可能であることを確認することが非常に重要である。そうでないことが判明したならば、後にではなく、対策方針をまだ変更することができ、脅威や方針を別な方法で扱うことができる今の段階でその問題点を報告することが望ましい。

### 10.4. IT 運用環境の対策方針の識別

IT 運用環境の対策方針を特定し、明示化する方法は、上述の第 10.3 項で説明した IT 運用環境以外の対策方針を特定し、明示化する方法と同一である。ただし、TOE の仕様や設計の段階に TOE 境界が変更されたことによって、TOE の対策方針が IT 環境の対策方針となることがあるため、IT 運用環境以外の対策方針とは区別しておくことが重要である。

便宜的に、IT 運用環境の対策方針も、「OE」で始まる名前を付すことによって認識される。同様に、対策方針の説明に「IT 運用環境」という言葉を含めるか、あるいは、技術的な手段で TOE 外に実装されていることを明確にすべきである。

ISO/IEC 15408 の以前のバージョンでは、IT 運用環境の対策方針が達成されるべきかを定義し、正確に説明するためのセキュリティ要件を定めることが許可されていた。これは、ISO/IEC 15408:2008 では許可されていない。ただし、対策方針オブジェクトの実装時に制約される事項を記録するアプリケーションノートといった別な方法がある。

複合型の製品では、1 つのドメインの IT 運用環境の対策方針は、他のドメインの TOE の対策方針となる。こういった対策方針は、対応箇所を容易に認識することができるよう、さらに慎重に表現すべきである。

### 10.5. TOE の対策方針の識別

TOE のセキュリティ対策方針は、最も重要で、精緻に表現することが最も困難な対策方針である。運用環境の対策方針とは異なり、TOE の対策方針は、セキュリティ機能要件を裏付けるために用いられる。したがって、対策方針の意図を明らかにすると共に詳述なセキュリティ要件とセキュリティ課題に適切な追跡可能性を提供するために、精緻に表現することが重要である。セキュリティ課題を単純に書き直したり、セキュリティ要件を網羅したリストを作成したりするだけでは十分とは言えない。

本章で提供する方法では、ISO/IEC 15408-2 のファミリやクラスを構成する機能コンポーネントとの関連で選択された、広範囲なセキュリティ要件をベースにした TOE の対策方針を構成することができる。(セキュリティ要件の)範囲や深度は、セキュリティ要件の分類ごとに主たる概念とその従属的な目的に基づいて扱われる。主たる概念には、さまざまな角度からセキュリティを考えることができるように、「最適な実践」を対象とした広範な戦略が備わっている。従属的な目的では、セキュリティ課題にありがちな点について詳しく扱っているが、適切に扱われなかった場合は、「より大きな問題」が見失われてしまう。

こういった TOE の対策方針を明らかにするために、この方法による最初の手順では、TOE に関連の脅威や方針をまとめるために、TOE の機能性が対象とする脅威や方針のリストを整理しなければならない。前提条件は、(TOE の)運用環境からのみ構成されるため、TOE の機能性に関する前提条件は存在しない。TOE の機能性のヘディング(項)に前提条件が指定されていることがあれば、それに対する行為は、単純に調べ直し、解決することである。

特定の PP、または ST の理想的なグルーピングは、それに対応する TOE の機能性によるところが大きい。ただし、そのグルーピングが ISO/IEC 15408-2 の内部構造に関連性がある場合には、後に、SFR を作成する際に訳に立つことが多い。

本章で紹介している方法では、すべての脅威と方針をグループ化に、次のような 7 通りのヘディング(項)を提案している。この方法は、実際に試用/試験済みであり、さまざまな TOE に対し、その有効性が認められたものである。以下が、そのヘディング(項)である:

a) アクセス制御(目的、属性、操作、アクセス規則)。

b) 利用者管理(利用者タイプ、利用者の識別情報、利用者の認証)。

c) TOE による自己保護(異常の検知、信頼のおける回復など)。

d) セキュリティが確保された通信(通信リンク、リンク特性、規則の確立など)。

e) 監査(イベントのログ、イベントに対する反応、インシデント管理、分析)。

f) アーキテクチャ要件(必要な特性や制約)。

g) その他の機能(例えば、信頼のおけるタイムソース、乱数生成など、容易にこれらのヘディング(項)に分類できないもの)。

セキュリティ機能要件を特定し、明示化するために、本技術報告書の第 12 章で提案するヘディング（項）と推奨する構成には意図的に密接な関係を持たせている。セキュリティ対策方針は、開発者の好みでさまざまな構造や構成手法を用いることもできるが、上述で推奨するヘディング（項）は、後に、相互参照をしたり、完全性と一貫性に関する拡張要件を簡略化したりするためのものである。むろん、構成が異なれば、後の作業を明確、かつ容易にするために特定の TOE が存在する。この段階では、（セキュリティ対策方針の）構造を考慮し、適切な手法を選択することが重要である。

次なる段階は、全体的なセキュリティ課題に適合するように、開発者が選択したセキュリティ要件それぞれのクラスごとに必要なセキュリティサービスやセキュリティによる保護機能を単純に書き留めることである。セキュリティ課題を明らかにするための分析や一般論を述べるよりも、SPD によって導出された非形式的なセキュリティ要件に戻るほうが適切である。広範なクラスごとにどのようなセキュリティ機能を主軸とすべきかについては、非形式的なセキュリティ要件から導きだされるのは言うまでもない。クラスによっては、どのようなセキュリティ要件を主軸とすべきかについて述べていないものや関連性がないものとして明確に識別されているものもあり、この段階では、これらは無視して構わない。

このセキュリティサービスのリストを、脅威や方針をグループ化したリストと比較し、それぞれのセキュリティサービスがどの脅威や方針と関連性があるかを判断する。最終的には、脅威や方針との関連性がないものが「その他」のセキュリティサービスに振り分けられる。

次にそれぞれのセキュリティサービスに関連する脅威や方針を、一般的な要件とセキュリティに特化した要件とに分割する。一般的な要件は、セキュリティサービスを明らかにする際にすべての要素に適用すべきは言うまでもないが、セキュリティに特化した要件は、特別な事例に適用すべきである。

最終的に、セキュリティサービスを、一般的な要件に対応するよう、肯定的な表現で書き直す。これが、セキュリティサービスの主な対策方針となる。セキュリティに特化したそれぞれの要件を、そのセキュリティサービスに対して関連のある、従属的な対策方針ごとに表現し直す。

脅威は、その脅威を阻止する対策方針が、脅威を構成するのに必要な要素の 1 つを削除、または阻止することで対処される。有害なアクションを実行する脅威エージェントの機能を取り除き、資産を移動させたり、変更、もしくは保護させたりすることで、有害なアクションを実行不可能にすることや、（例えば、物理的なアクセス制御のために環境の対策方針を導入するなど）脅威エージェントの排除がこの例である。脅威は、間接的にも対応することができる。監査機能による責任追跡性の実行や、消費者による偶発的なエラーを阻止するための適切なトレーニング、損失や被害をこうむった資産を容易に復元させるために頻繁にバックアップを取ることなどが、間接的な対応の例である。

すべての脅威に保護を提供できるわけではない。関連するインシデントを検出し、警告を発する、監査ログのエントリが最適な活動となることもある。こういった（TOE 仕様の）設計は、この時点で判断しなければならない。その対応としてインシデントの検出が選択された場合には、そのインシデントに対応する監査サービスの必要性が生じる。

この仕様設計プロセスでは、脅威や方針を指定し直す必要が生じることがある。セキュリティサービスが適切に定義されれば、脅威や方針の中にも主要な対策方針に対してよりも従属的な対策方針、またはその逆のほうが容易に適合する、あるいは別なセキュリティサービスの一部としてのほうがより適合するということもある。このプロセスでは、当初、見逃されていた運用環境の対策方針が認識されることが多い。例えば、ある脅威への対応として警告が選択されている場合、管理者は、その警告に応答する必要性が生じる。TOE の設計上の決定の場合、特定の脅威に対する保護が解消されたり、方針が TOE の対策方針から運用環境の対策方針に変更されたり、またはその逆が生じることもある。こういった変更点は予期されているものである。したがって、すべてのセキュリティサービスを網羅した目的がはっきりとしたリストが完成するまで何度でもこの作業を繰り返す必要がある。

一般的な（主たる対策方針と直接関連する）保護要件の表現と同様に、方針の中にもそれに関連の技術的なソリューションの性質を制約する用いられるものがある。こういった類の制約は、一般的な要件に関連する従属的な対策方針として表現されるべきである。

脅威の中には、その脅威のみを対処する、特定の従属的な対策方針と直接関連するものがある。この場合は、その対策方針がその情報源に直接反映されるように表現する。これは、後に、SPD との相互参照によって関連性のある対策方針や読者の理解を深めるための根拠の 2 つについてその追跡性を容易にするためのものである。

従属的な対策方針では、複数の脅威や方針を扱うことがある。例えば、リソース管理クラスの従属的な対策方針

として、PP や ST の大半に対策方針を再利用するオブジェクトを持っている。一般的に、脅威として対処される際の重複箇所はごく僅かなため、(再利用は)その他のリソース管理と切り離して考えることが賢明である。ただし、例えば RAM に対する脅威が磁気媒体には適用されないなど、異なった方法で対処することができるなど、リソースの種類が異なる場合でも、その対策方針を、明らかにすべきリソースごとにさらに分割する必要はない。異なったリソースのメカニズムとして異なった SFR が選択される際に、セキュリティ要件の仕様を設計する段階でその違いが明らかになる。

必要な管理策の種類によって、従属的な対策方針の有効性による違いをさらに明らかにすることができる。管理策では、予防的措置(発生するインシデントの阻止)、検知(発生したインシデントの認知)、または是正措置(インシデントによってもたらされた結果の修正)が可能である。脅威や方針に対処するために、こういった措置を複数実施する必要がある場合は、管理策ごとに異なった従属的な対策方針を備えるほうが賢明である。セキュリティ課題でその防御策を所定の深度まで説明する必要がある場合、またはセキュリティサービスの主な対策方針が、脅威の阻止ではなく削減、または緩和のみを目的としている場合は、この方法がよく使われる。

TOE の利用者の個人識別情報や認証情報を識別する必要がある場合の、*予防的措置*に関するセキュリティ対策方針の例が以下である:

*TOE は、それぞれの利用者が TOE の機能へのアクセスの許可を得る前に、それぞれの利用者が一意的に認識されており、主張する身元情報が認証されていることを確認する。*

アクセス制御と情報フロー制御に関するセキュリティ対策方針も*予防的*なカテゴリに属する。セキュリティの視点から TOE が複数のアクセス制御や情報フロー制御方針を実装すべきであることが示されている箇所では、それぞれの方針ごとに異なったセキュリティ対策方針を識別することが推奨される。こういった方法を取ることによってセキュリティ要件の根拠を簡潔にすることができる。

TOE 元来の機能の否認防止性を提供する TOE を識別する必要がある場合の、*検知*に関するセキュリティ対策方針の例が以下である:

*TOE は、情報の受信者がその情報の出典元の証明としてその証拠を生成することができる方法を提供する。*

検知された侵入に対処する TOE を識別する必要がある場合の、*是正措置*に関するセキュリティ対策方針の例が以下である:

*差し迫っているセキュリティ侵害を示すイベントが検出された場合、TOE は、他の利用者に提供されているサービスを最小限に中断することで攻撃を抑止する適切な手段を講じる。*

この段階では、TOE が提供するセキュリティサービスが有効であることを確認するために追加すべき管理アクティビティに関するセキュリティ対策方針が存在することを確認するために、運用環境のセキュリティ対策方針の記述を再確認する必要がある。その中には、必要な管理アクティビティが明らかであり、(IT 以外の)セキュリティ対策方針として直接表現できるものがある。一方、必要な管理アクティビティが、TOE のセキュリティ対策方針を実装するために用いられているセキュリティ要件の内容に依存している場合もある。例えば、利用者の「個人識別情報や認証情報」と関連付けられているセキュリティ対策方針は、利用者のパスワードに実装されているかも知れない。これは、利用者が自身のパスワードを他の利用者に知られないようにすることを意味すると共に、IT 以外の環境におけるセキュリティ要件としても適切に表現されている。こういった黙示的な要件を見落としてしまっても、混乱したり、驚いたりしてはならない。なぜならば、SFR を定義することによってそういった要件が明らかになり、その時点でセキュリティ対策方針の記述も更新することができるからである。

可能であれば、PP や ST の根拠ではどの程度の有効性を証明しなければならないかという点について、ごく僅かな懸念を残すにとどめるために、セキュリティ対策方針では、予期される最小限の有効性を(非形式的に)定量化することを目的にすべきである。量は、次のように記述することができる:

a) 例えば、環境的な条件や以前の状態に関する相対的な用語。

b) 絶対的な数値を示す用語。

絶対的な数値を用いるのが最も正確な選択肢であるのは間違いないが、有効性を数値で示すことが最も困難であることも明らかである。

対策方針と脅威、または方針が 1 つに対し 1 つが対応することを望んではならない。方針を扱うために必要な主た

る対策方針では、セキュリティサービスに関する複数の脅威にも対処することが多いためである。また、脅威や方針は資産の種類によって異なった対処をしなければならず、資産の種類ごとに異なった従属的な対策方針が必要になることがある。

これ以外にもセキュリティ対策方針の識別に用いることができる技術がある。セキュリティ対策方針が、SPD に記載の関連する脅威や方針で明確に表現されていない場合には、小規模の SPD と好相性の簡潔な手法として、単純に脅威、または方針ごとに 1 つの対策方針を作成し、具体的な資産や脅威エージェント等が反映されるような表現に置き換えることである。

TOE の対策方針には、運用環境の対策方針と区別するために「OE」ではなく、「O」で識別することができる名前が付与されているのが一般的である。TOE の対策方針では、実装する対策が TOE の一部として、TOE によって実行されることがはっきりと判るような表現にすべきである。

時に TOE の対策方針では、「TSF は～ねばならない（The TSF must…）」、または「システムは～ねばならない（The system must…）」という表現で始まるものがある。TSF は、SFR を実装する TOE の一部である。この違いは、評価時に確認しなければならない TOE の範囲を低減するという、実践的な理由によるものである。したがって、どの対策方針の場合も、TOE の一部として TSF を実装する場合は、TSF の一部でなければならないという点で、「TSF」という用語を用いる場合には、正確さを期さなければならない。ただし、TSF にはどこか循環論法的なところがあり、こういった対策方針は通常、「TSF の対策方針」ではなく、「TOE の対策方針」として考えられていることも誤解を招く元になっている。「システムは、～」という表現も誤解を招く元である。この表現では、運用環境で実装される対策方針が含まれるように解釈することができるためである。運用環境で実装される対策方針が含まれることを意図する場合は、「TOE、またはその環境では」という表現のほうが適切である。運用環境の対策方針を TOE の対策方針と区別することが決まっている場合は、 対策方針をまとめる前に TOE の設計の段階で分離しなければならないという点に注意が必要である。

### 10.6. 対策方針根拠の作成

対策方針を明らかにするための最終的な段階では、対策方針を SPD で記述した脅威、方針、及び前提条件と相互参照し、これらがすべて必要であり、SPD で記述した脅威、方針、及び前提条件をさまざまな角度から確認した結果、対策方針で対処されているか、今後の検討事項から除外されていることを示す根拠を作成することである。低保証以外のすべての評価では、ISO/IEC 15408 で根拠の作成が定められており、PP/ST の有効性の評価でも確認される。

根拠の作成の簡潔な方法は、SPD の要素と対策方針との関連性が相互に交わるような表を作成し、矛盾箇所、格差、あるいは重複箇所がないかを確認することである。脅威、方針、または前提条件が複数の対策方針に対応している箇所には、どの部分がどの対策方針に対応しているかを示す、簡単な識別子を SPD の要素に追加することができる－上述の第 10.2 項の例を参照のこと。こういった例を表に組み込むことによって、明確な対応付けをすることができ、確認が容易になることだろう。

それぞれの対策方針が最低でも 1 つの脅威、方針、または前提条件と相互参照が可能な場合は、その表が、それぞれの対策方針が*必要である*ことを示すべきである。これ以外の対策方針が同じ脅威、方針、または前提条件と相互に対応しており、既に適切な措置が取られていることもあるため、セキュリティ対策方針に全く冗長性がないという保証がないことは言うまでもない。ただし、これは、第 2 の有効性要件である十分性を確立するための要件の一部と判断することができる。

十分性は、相互参照用の情報を補完する、非形式的な根拠を提供することによって示さなければならない。軽減されていない脅威ごとに、関連のあるセキュリティ対策方針が脅威に効果的に対処されるのはなぜかを考える必要がある。こういった脅威をベースにした攻撃は、必ずしも完全に排除する必要はないという点に留意してほしい。つまり、攻撃を検知したり、攻撃を受けた場合でも回復が可能であったり、あるいは攻撃される可能性を容認可能なレベルまで低減するだけで十分な場合がある。これらはすべて、効果的な対策となっていることが SPD の記述には必要不可欠である。

同様に、識別された OSP、あるいは環境における前提条件では、関連のあるセキュリティ対策方針が OSP のセキュリティ要件をすべて満たしているか、または前提条件を裏付ける非形式的な論証を提供していることを証明しなければならない。

軽減、もしくは無視できるレベルの脅威を認識するために SPD で記述された前提条件は、対策方針を作成することはなく、したがって、対策方針根拠にも含める必要がないことを記憶にとどめていただきたい。

PP、または ST が、他の PP との適合性を主張する場合、その根拠では、TOE のセキュリティ対策方針が対象とする PP のセキュリティ対策方針の記述と適合していることを示さなければならない。このように、セキュリティ対策方針に同じ表現方法が用いられている場合、その対策方針は、簡単なマッピングですべての対策方針に適合していることを示すことができる場合がある。つまり、PP に正確適合であることが要求されている場合、その表現方法は、寸分も違っていてはならず、したがって、評価者は、そこに記載されているその他の情報をすべて無視する。

ただし、PP の対策方針に単純に対応するものがない場合は、対象とする PP の対策方針を全く別なものとして構築したり、表現したりできることがある。このような場合は、TOE のセキュリティ対策方針が、対象とする PP の SPD に記載されているセキュリティ要件にも適合していることを示さなければならない。これによって、TOE のセキュリティ対策方針が PP の対策方針にも含まれており、したがって、双方の対策方針が適合することを主張することができる。

PP、または ST が他の PP との適合性を主張する際に、適合すべき他の PP の SPD があなたの SPD のすべての脅威に明示的に対応していない場合、主張を十分に満足するだけの根拠の作成が不可能な場合がある。これに対するソリューションはない。その場合、対象とする PP に適合する COTS 製品が読者の目的に完全に合致しているとしても、COTS 製品の PP 適合性の主張は読者の目的に合致していることの証明にはならない。そういった COTS 製品であっても、読者は ST の脅威について記載されている箇所を参照し、その製品が読者の関心があるすべての脅威を考慮していることを確認することによって、その製品が読者の要求の合致することの確証を得ることができる。

# 11. 拡張コンポーネントの定義

セキュリティ機能要件や保証要件の仕様を定めようとする場合、ISO/IEC 15408 の Part2 や Part3 で規定されている既存のコンポーネントを詳細化する自在性が与えられていても、PP や ST の作成者がそれらの要件の適切な仕様を作成できないことがある。こういった場合には、拡張コンポーネントを定義することができる。本章では、拡張コンポーネントの仕様に関するガイダンスを提供する。

ガイダンスを提供する前に、1 つだけ一般的なアドバイスをする：それは、拡張コンポーネントを定義することは、できる限り避けるべきである、という点である。なぜならば、拡張コンポーネントを用いることによって、その製品を満足させるセキュリティ機能と保証要件をベースにした別の製品との比較が困難になるためである。その替わりに、まず、ISO/IEC 15408 で規定されている既存のコンポーネントを利用することを試すべきである。こういった手段を取ることができない場合に限り、拡張コンポーネントを利用すべきである。

ISO/IEC 15408 のコンポーネントに PP、または ST に記述したいと思う具体的な要件に対応するものがないと思われる場合には、コンポーネントを詳細化することで問題を解決できることが多い。例えば、利用者認証の要件が利用者のタイプによって異なる場合には、特定の要件が適用される利用者タイプを特徴付けるために FIA クラスのコンポーネントを詳細化し、さらに複数のコンポーネントを具現化することによって異なった消費者タイプすべてに対応するように表現することもできる。同様に、異なるタイプの利用者、サブジェクト、オブジェクト、またはセキュリティ属性を管理するための異なった要件も詳細化を用いて表現することができる場合が多い。

ISO/IEC 15408-1 では、詳細化に関する例と共に、それらを利用して詳細化をより正確に表現する方法を提供している。

ISO/IEC 15408-1 には、拡張コンポーネントを定義する方法に関するガイダンスも若干提供されている。以下の各項では、このガイダンスを補足している。

拡張コンポーネントを定義する前に、評価が既に完了し、公開されている ST、または PP の中に、セキュリティ機能、または保証要件に具体的に追加したいと思う拡張コンポーネントが既に定義されているかについて詳しく調査すべきである。評価済みの ST や PP で既に定義されている拡張されたコンポーネントを利用することによって、そのコンポーネントが既に ISO/IEC 15408 で要求されている ST、または PP の評価の一部として、その整合性や適合性が確認されていることを容易に判断することができる。

拡張要件を定義する場合、ISO/IEC 15408-1 では、ISO/IEC 15408 の既存コンポーネントと同様の方法で定義

されていることが必要である。拡張コンポーネントに名前を付ける場合にも、ISO/IEC 15408 の既存のコンポーネントと同様の詳述さのレベルが適用される。したがって、拡張コンポーネントについても、ISO/IEC 15408 と同様の構造を用いて記述するよう勧める。拡張コンポーネントに名前を付ける場合には、ISO/IEC 15408 のクラス、またはファミリの中で既に定義されているコンポーネントに対応していることを確認し、クラスの名前と（基本的には）ファミリの名前に、このコンポーネントが拡張コンポーネントであることを示す識別子を追加するだけで名前が作成されるようにすべきである。拡張コンポーネントは、割付、及び/または選択などの操作ができるよう、可能な限り、一般的な方法で定義すべきである。これによって ST、または PP の別な作成者が拡張コンポーネントを抽出し、それらを自らの要件に適合するような方法で容易にインスタンス化することができる。

ISO/IEC 15408-2 の機能コンポーネントを用いて、拡張 SFR コンポーネントをモデルとして表現する場合の仕様には、次のような条件が含まれる：

a） 拡張 SFR が、ISO/IEC 15408-2 のコンポーネントと同様の詳述さのレベルで定義されていること。

b） ISO/IEC 15408-2 のコンポーネントと同様の書式と表現方法が用いられていること。

c） コンポーネントには ISO/IEC 15408-2 としてのトポロジと用語が用いられていること。

新たな SFR が、クラス、またはファミリに含まれている既存の SFR と同じ特徴があることが判れば、新たな SFR だけでまとめることが容易になり、クラス、またはファミリ全体が対象としている共通の内容を具体的に表現することにも役立つ。

ISO/IEC 15408-2 の機能コンポーネントとして表現される書式には次のような特徴がある：

a） 機能要件の大半は、*TSFは～しなければならない*」、または「*TSFは～ができなければならない*」という言い回しを用い、「可能にする」、「検知する」、「実行する」、「保証する」、「制限する」、「監視する」、「認める」、「回避する」、「保護する」、「提供する」、または「限定する」といった動詞が用いられる。

b） セキュリティ属性や認証された利用者といった標準的な用語の利用。

c） 個々のエレメントそれ自体で意味を持ち、1 つ前のエレメントを参照しなくても理解することができる。

d） セキュリティ要件が TOE に適合しているかどうかを判断することができるなど、それぞれのセキュリティ要件が評価可能でなければならない。

拡張コンポーネントを作成する場合は、SFR に関し、次のような条件を考慮すべきである：

a） ST、または PP の作成者によって割付、または選択などの操作ができるように構成されている。

b） PP、または ST に含まれていなければならない、他の SFR に依存性を持っている。

c） 監査対象のイベントが説明されており、イベントについてどのような情報が記録されるべきかに関する内容が含まれている。

d） 管理すべきセキュリティ属性に対応するなど、セキュリティ管理に関する内容が含まれている。

ISO/IEC 15408-2 には含まれておらず、またこれとは全く異なる SFR を適切に構築し、その内容が著しく向上されていると確信できるならば、国際的な標準である ISO/IEC 15408 の既存の機能コンポーネントの次期バージョンにその SFR を提出することを進言する。

SFR が ST のみで用いられる場合、つまり、SFR が他の PP、ST または機能パッケージのコンポーネントとして再利用されない場合は、SFR の割付や選択方法を ISO/IEC 15408 の操作として規定する必要はないことがある点に注意すべきである。

ISO/IEC 15408-2 に含まれていない拡張 SFR に名前を付ける場合は、標準と同様の書式となるように、ISO/IEC 15408-2 で規定されているトポロジと命名規則に従うべきである。拡張 SFR には、機能要件を示す「F」を用い、続けてクラスやファミリに指定された適切なコンポーネント番号を用いるべきである。次に、既存のクラスをベースに拡張されたコンポーネントを所定の場所に挿入する。既存のクラスとは関連性のない拡張コンポーネントの場合は、例えば、コンポーネント「EX」のクラスを作成する、あるいはコンポーネントの名前の後に EX を追加するといった方法

で、拡張されたセキュリティ要件が新たに作成されたものであることがはっきりと判るようにすることも可能である。拡張コンポーネントをどのように表示すべきかについては、PP、または ST の適用時の注意事項で説明すべきである。用いられた命名規則については、ISO/IEC 15408-2 で規定されているものとの矛盾が生じないように注意すべきである。

付録 A では、拡張コンポーネントを ISO/IEC 15408-2 で定義しているのと同様の方法で説明している。これによって評価者は、拡張コンポーネントを定義する ST や PP の評価時に、拡張コンポーネントを ISO/IEC 15408-2 で規定されているものと同様に扱うことが可能になる。

付録 A で説明している拡張 SFR の例と同様に、拡張セキュリティ保証要件も定義することができる。これは、ST や PP に製品に共通のセキュリティに関する保証アクティビティが説明されており、この保証アクティビティが ISO/IEC 15408-3 で規定されている既存のコンポーネントに含まれていない場合に納得の行く話である。また、ISO/IEC 15408-3 で規定されている既存のコンポーネントに利用されているものと同様の書式でセキュリティ保証コンポーネントが定義されている場合、拡張されたセキュリティ保証要件には、評価者が、製品が拡張セキュリティ保証要件に適合していることを検証する活動を裏付ける評価方法を明らかにする必要がある。こういったアクティビティは、ISO/IEC 15408-3 で定義している保証コンポーネントを、ISO/IEC 18045 で定義している程度の内容の詳述さで定義しなければならない。

拡張された保証コンポーネントでは、次のような要素（詳しくは、ISO/IEC 15408-1 の附属書 C.5 を参照）について定義すべきである：

a) 開発者のアクション。

b) 開発者が規定しなければならない証拠の内容・提示に対する要件。

c) 評価者のアクション。

ISO/IEC 15408-3 を詳しく見てみると、保証コンポーネントに関する要素は、次のような特徴を持っていることが判る：

a) 開発者のアクションに関する要素には、開発者が実行しなければならないアクション、一般的には評価証拠の提供を示すことを目的としている。

b) 内容や表示法に関する要素には、要求されている内容と共に、開発者が提供しなければならない評価証拠をさまざまな角度から質的に特徴づけることを目的としている。

c) 評価者のアクションに関する要素には、次のような 2 通りの様式がある：

   ― 評価者の最初のアクションは、一般的に次のような様式である：

   *評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。*

   ― その他の評価者アクション要素については、一般的に独立したステートメントの様式を取るが、これは評価の一貫として判断される。

したがって、証拠の内容・提示に対するすべての要件は、はっきりと曖昧な表現にならないようにするだけではなく、（できる限り）評価者の評価者アクションの一部として主観的な判断が必要とならないような表現にすべきである。むしろ、拡張 SAR に関しては、評価者が判断し易いように対象とする基準をはっきりと定義すべきである。セキュリティ対策方針を判断する際、それに対応する拡張 SAR を明らかにする必要がある場合は、適用時の注意事項の追加を検討すべきである。

拡張 SAR が ISO/IEC 15408 で規定するコンポーネントと同様の様式で確実に定められるように、分離可能な要件が独立した要件の要素として記述されるようにすべきである。また、拡張 SAR に適切な表現を選択する方法は、ISO/IEC 15408-3 で詳しく説明しているが、ISO/IEC 15408-1 の第 3 章で説明している一般的な用語の定義のしかたを参考にすべきである。

ISO/IEC 15408-3 には含まれておらず、またこれとは全く異なる SAR を適切に構築し、その内容が著しく向上されていると確信できるならば、国際的な標準である ISO/IEC 15408 の既存の保証コンポーネントの次期バージョンに

その SAR を提出することを進言する。

拡張された保証コンポーネントを定義する場合には、評価時に、拡張された保証コンポーネントとの適合性を示す際に必要な評価者のワークユニットについても定義する必要がある。これは、例えば、ISO/IEC 18045 で規定されているワークユニットの内容を用いて定義することができる。ワークユニットは、拡張された保証コンポーネントをさまざまな角度から捉えることで、評価者による評価の実施方法についての明確な見解を提供する。

# 12. セキュリティ要件

## 12.1.序説

本章では、PP、または ST の IT セキュリティ要件の仕様を定める際のガイダンスを提供する。このガイダンスは、TOE のセキュリティ要件にも適用される。

PP、または ST では次のようなタイプの IT セキュリティ要件が規定される:

a) TOE のセキュリティ機能要件(SFR)。これらセキュリティ機能要件は、TOE のセキュリティ対策方針が網羅されるように、TOE が提供しなければならないセキュリティ機能要件を識別することである。

b) TOE のセキュリティ保証要件(SAR)。これらセキュリティ保証要件は、SFR の実装時に必要な保証のレベルを認識することである。

これを示したものが、次の図 3 である。

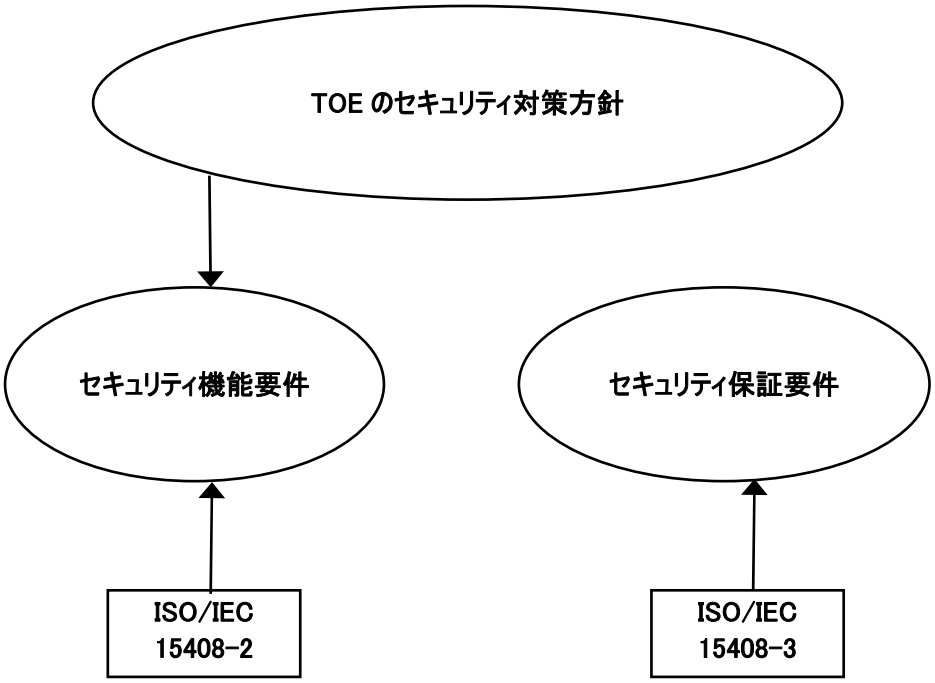


**図 3: IT セキュリティ要件の導出**

図 3 でも示しているように、IT セキュリティ要件の主たる特徴は、できる限り、ISO/IEC 15408-2 で定義されている機能コンポーネントの一覧と ISO/IEC 15408-3 で定義されている保証コンポーネントの一覧を用いて構成することを目的としていることである。ここでの ISO/IEC 15408 の目的は、IT セキュリティ要件が提供されている方法で、標準化のレベルが確保されるようにすることである。つまり、IT セキュリティ要件を示すために、「共通の言語」を用いることによって、PP と ST の比較を容易にすることである。ISO/IEC 15408 の機能パラダイムを用いて、セキュリティ機能要件を導出するためのガイダンスを第 12.2.項で提供する。

ただし、ISO/IEC 15408 では、ISO/IEC 15408-2 と ISO/IEC 15408-3 に適切な機能、または保証コンポーネント

がない場合があることも認めている。このような場合は、IT セキュリティ要件に対応する要件が ISO/IEC 15408 には規定されていないことをはっきりと記述することができる。ただし、こういった IT セキュリティ要件は既存の ISO/IEC 15408 で規定されているコンポーネントと同様に、確実に評価の対象となるように表現しなければならない。第 12.3.7.項に、ISO/IEC 15408-2 で識別することができる適切な機能コンポーネントが存在しない場合のガイダンスを提供する。第 12.4.3.項では、同様に ISO/IEC 15408-3 で識別することができる適切な保証コンポーネントが存在しない場合のガイダンスを提供する。

ISO/IEC 15408 では、セキュリティ要件、すなわち割付、繰返し、選択、及び詳細化を適切に調整するための、SFR や SAR を対象に実行されるべき一連の操作を可能にすることで SFR や SAR に所定の自在性を持たせた方法で規定することを認めている。次の第 12.3.3 項では、ISO/IEC 15408 で規定されている機能コンポーネントに対する操作の利用法に関するガイダンスを提供する。第 12.4.2.項では、ISO/IEC 15408 で規定されている保証コンポーネントに対する操作の利用法に関するガイダンスを提供する。

ISO/IEC 15408-2 と ISO/IEC 15408-3 で規定されているそれぞれのセキュリティ要件は、ISO/IEC 15408 で定義されている分類法をベースにした一意な識別子が、個々に割り当てられる:

a) ISO/IEC 15408-2 では、例えば、コンポーネント FAU_GEN.1.2.は、次のような意味を持つ。
   - 「F」は、機能要件であることを示す。
   - 「AU」は、SFR のセキュリティ監査クラスに属すことを示す。
   - 「GEN」は、セキュリティ監査クラスのセキュリティ監査データ生成ファミリに属すことを示す。
   - 「1」は、セキュリティ監査データ生成ファミリの監査データ生成コンポーネントであることを示す。
   - 「2」は、監査データ生成コンポーネントの第 2 エレメントであることを示す。

b) ISO/IEC 15408-3 にも同様の分類法を用いるが、それぞれの要素が 3 つの保証要素のいずれか 1 つに属すことが判るように、アルファベットを 1 文字追加する:
   - アルファベット「D」は、開発者アクションエレメントに属し、そのアクティビティが開発者によって実行されることを示す。
   - アルファベット「C」は、証拠の内容・提示エレメントに属し、証拠が伝えなければならない内容を示す。
   - アルファベット「E」は、評価者アクションエレメントに属し、そのアクティビティが評価者によって実行されることを示す。

c) ISO/IEC 15408-3 では、例えば、コンポーネント ADV_TDS.1.2C は、次のような意味を持つ。
   - 「A」は、保証要件であることを示す。
   - 「DV」は、SAR の開発クラスに属すことを示す。
   - 「TDS」は、開発クラスの TOE 設計ファミリに属すことを示す。
   - 「1」は、TOE 設計ファミリの基本設計コンポーネントであることを示す。
   - 「2」は、保証エレメントの第 2 エレメントであることを示す。
   - 「C」は、証拠の内容・提示エレメントの 1 つであることを示す。

SFR と SAR は*コンポーネント*のレベルで選択される。コンポーネントが PP や ST に含まれる場合は、コンポーネントの中で定義されたすべてのエレメントも PP や ST に含まれる。コンポーネント間の関連性には IT セキュリティ要件選択時の手順も含まれているため、こういったコンポーネント間における 2 通りの関連性を認識しておく必要がある:

a) ファミリの中のコンポーネントは、1 つのコンポーネントにそのファミリの中の別なコンポーネントで定められているすべての要件が含まれていることを示す、階層的な関係にあるものがある。例えば、FAU_STG.4 は、FAU_STG.3 で定められたすべての機能エレメントが前者にも含まれているという点で、後者との階層的な関係にある。ただ

し、FAU_STG.4 は、FAU_STG.1 とは階層的な関係にはないため、双方のコンポーネントが同じ PP と ST に含まれる可能性がある。

b) コンポーネントは、それ自体で要件を満足させることができず、自身が適切に機能するために、他の機能コンポーネントに依存している、あるいは相互的な関係にあるなど、別なファミリのコンポーネントの依存関係にあるコンポーネントとして定義されるものがある。例えば、FIA_UAU.1（利用者が主張する識別情報の認証を要求する）は、FIA_UID.1（利用者の識別を要求する）の依存関係にあるコンポーネントである。こういったコンポーネントは、脅威やセキュリティ対策方針と関連性がないことを示すことができない限り、PP や ST に含まれなければならない。

## 12.2.ISO/IEC 15408 におけるセキュリティパラダイム

### 12.2.1. セキュリティ機能のモデリングのためのセキュリティパラダイムとその利用法について

ISO/IEC 15408-2 で規定されているセキュリティ機能要件のクラス、ファミリ、及びコンポーネントの構造を理解し易くするために、本ガイドでは、ISO/IEC 15408-2、第 5 章に記載のセキュリティ機能のパラダイムにも触れておく。

ISO/IEC 15408 のセキュリティパラダイムの目的は、TOE のセキュリティ機能をモデリングする際のベースを定めるために、そのモデルに適合するセキュリティ対策方針がどの程度まで要求されるのかを示すことである。前項で説明したパラダイムは、ここでセキュリティ機能の概要的なモデルの開発に利用することができ、後に、ISO/IEC 15408-2 で定められた SFR という形で表現される。以下の各項では、こういったモデルを開発する方法のガイダンスを提供すると共に、SFR を用いてモデルを説明する。

### 12.2.2. リソースやオブジェクトへのアクセスとその利用法

#### 12.2.2.1. 説明

ISO/IEC 15408-2 で規定されているセキュリティ機能のパラダイムでは、TOE によって保護されているリソースの利用法を制御すると共に規定している。リソースは、TOE の内部（メインメモリ、CPU 時間、ディスクスペース、サービス、など）にあることもあれば、それ自体は TOE の外部にあるが、TOE の機能（例えば、その他のシステムからのネットワークサービス）によって管理されているもの（限られた数のエンティティ）のみがアクセスできることもある。ファイアウォールは、リソースの利用法を管理しているが、それ自体は TOE の一部ではないものの一般的な例である。

セキュリティ対策方針を達成するために、制御される必要のあるリソースの例は、次の通りである：

- メモリ（メインメモリとディスクスペース双方）。
- CPU 時間。
- 周辺装置、またはネットワークリンク。
- 機能。

ISO/IEC 15408-1 では、利用者は、「TOE の外部にあって TOE と対話する(または対話することができる)任意のエンティティ（人間、または IT）」として定義されている。また、ISO/IEC 15408-1 では、サブジェクト（subject）は、「オブジェクトに対して操作を実行する TOE の能動的なエンティティ」として定義されている。利用者とサブジェクトは、TOE によるサービスを要求する能動的なエンティティであり、それにしたがってオブジェクトとリソースが運用される。

セキュリティ対策方針を達成するために、リソースの利用は、TOE が実行する必要がある規則に基づき、TOE の内部で規定される。こういった規則は、リソースの利用にも適用することができ、リソースの利用を記録することもできる。

A－こういった規則の一部として評価されることがある、意図的に不完全なままにしてあるパラメタには：

- リクエストを開始したエンティティの種類と識別。
- リクエストを開始したエンティティのその他の属性。
- リクエストの対象であるリソースの種類と識別。

- リクエストの対象であるリソースのその他の属性。
- リクエストの種類。
- 時間と日付。
- TOE の内部状態。

これらのパラメタがベースとなっている規則を実行するには、TOE がこれらのパラメタを維持し、管理する必要がある:

- 外部のエンティティ(「利用者」とも呼ばれる)の場合、TOE はそれらを認識すると共に、少なくてもその規則の実行に必要な程度まで、外部のエンティティを認証する。その規則が、TOE 外部の特定的な一連のエンティティ、またはエンティティグループに属する外部のエンティティのみを対象にしている場合、TOE が一連のエンティティやエンティティグループを認識し、認証するのに十分である。
- TOE は、TSF によって管理されているサービスの利用を許可された(潜在的にセキュリティ属性を備えた)外部エンティティのリストを維持している場合が多い。このような場合、(セキュリティ)機能では、外部のエンティティやそのセキュリティ属性(ただし、そのリストは静的なものではない)のリストを管理する必要がある。

セキュリティ対策方針を満足させるために用いられるセキュリティ機能を実装する TOE の一部とセキュリティ機能を修正、もしくはバイパスする可能性がある TOE のその他の部分は、「TOE セキュリティ機能(TOE security functionality、TSF)」と呼ばれる。TOE のアーキテクチャによって、TSF が TOE 全体になることもあれば、TOE として定義された一部となることもある。TSF が、TOE の一部である場合、TOE の TSF ではない部分が、セキュリティ対策方針を妨害するような方法で TSF を操作したり、バイパスすることができないようにしたりすることが重要である。

外部エンティティはもとより、(TSF によって)管理されているリソースによるサービスを要求するサブジェクトは、TSFI と呼ばれる、TSF に対応するインタフェースを利用する。

時にサブジェクトは、外部エンティティの代わりに動作する。こういった場合、外部エンティティ(あるいは、利用者)は、サブジェクトと「関連付け」される。この関連付けの手順の一部として、サブジェクトのセキュリティ属性は、この関連性が反映するように修正されることが多い。その一例が、TOE のサブジェクトが外部エンティティのセキュリティ属性を継承している場合だが、関連付けの一部として導出されたサブジェクトをどのようにセキュリティ属性と定義付けするかを定める、さらに複雑な規則が存在することがある。

リソースは、「オブジェクト」としてグループ化されることがあり、TOE は、リソースをグループ化してオブジェクトにする際に用いられる規則とは別のオブジェクトに用いるための規則を特定の用途のために取っておくことがある。この一般的な例が、TOE が、最大量のディスクスペース(リソース)を確保するための規則を実行し、ディスクスペースのリソースによって作成されたファイル(オブジェクト)へアクセスするための規則を定めることである。これは、一連の規則によってリソースの利用法を規定し、もう一方の一連の規則がリソースによって作成されるオブジェクトを規定することで、単一のリソースを対象とし、異なった規則が TOE によって実行されることを示す例である。

オブジェクトへのアクセスとその利用法を定める規定は、オブジェクトごとに異なるのが一般的である。混乱を防ぐために、ISO/IEC 15408 では、オブジェクト、サブジェクト、操作を異なった「セキュリティ機能方針(security function policy、SFP)」として一連の規則をグループ化し、個々の SFR を対象とする SFP が、SFR が属すセキュリティ機能方針を示すことを許可している。セキュリティ機能方針では、方針が適用する一連のサブジェクト、利用者、オブジェクト、リソース、及び操作を定義することにより、SFP の適用範囲を明確にしなければならない。次いで、利用者、またはサブジェクトが SFP の一部として定義したオブジェクト、またはリソースを用いる際に、サブジェクト、または利用者に対する規則が操作によって実行される。上でも説明したが、こういった規則は、通常、サブジェクト、利用者、オブジェクト、またはリソースに関する具体的な属性がベースになっている。SFP の規則に反映されるこういった属性は、「セキュリティ属性」と呼ばれる。セキュリティ属性の管理要件は、SFP の中で機能すると共に、SFP に対するエンティティのサブジェクトが作成され、(利用者用に)取り込まれ、あるいは登録される場合、セキュリティ属性がどのように初期化されるかの定義を含め、SFP の一部としても機能する。まとめると、SFP とは、定義された一連の能動的なエンティティ(利用者、またはサブジェクト)が用いる定義された一連の操作へのアクセスと、定義された一連のオブジェクトやリソースの利用を定めた規則とこれらの規則で用いられるセキュリティ属性を管理する機能を説明するものである。

この一般的な例が、オペレーティングシステムのファイルシステムのオブジェクトについて定めたアクセス制御方針であ

る。能動的なエンティティには、利用者に替わって動作するプロセスもあるため、利用者のセキュリティ属性と関連付けする際に、導出されるセキュリティ属性が備わっているものもある。操作とは、読み込み、書き込み、更新のためにファイルを開き、ファイルの属性を確認したり、変更する、ファイルを作成したり、削除するなどファイルシステムのオブジェクト上で動作するシステムコールのことである。また、セキュリティ属性のプロセスやファイルシステムのオブジェクトを管理する操作もある。セキュリティ属性の一般的な例には、次のような機能を果たす SFP がある:

- オブジェクトのセキュリティ属性:アクセス制御リスト、ファイルの種類。
- 利用者のセキュリティ属性:利用者の識別情報、利用者の役割。
- プロセスのセキュリティ属性:プロセスの識別情報、プロセスの信頼レベル。

その他の SFP は、中間的なサブジェクトがなくても、外部エンティティが直接実行することができる操作について規定することができる。その例が、外部システムが利用することができるネットワークサービスや機能について定めているファイアウォールシステムである。これには、能動的なエンティティ(リクエストを開始する外部システム)、オブジェクト(リクエストに対応する外部システム)や操作(ネットワークサービス)なども含まれる。こういった SFP に対する規則は、操作に関与する外部システムの同一性、実行された操作の種類(例えば、ポートの利用など)、操作の内容(例えば、特定ポートへの接続があらかじめ確立されている場合など)、及び/またはネットワークパッケージの内容がベースになっていることがある。

一連の利用者、サブジェクト、オブジェクト、及び操作が同一であっても、複数の SFP を定義するのはよくあることである。この例が、1 つの SFP とする任意アクセス制御方針や追加的な SFP とする必須アクセス制御方針である。SFP によって対処される一連の利用者、サブジェクト、オブジェクト、及び操作が同一であっても、SFP の規則とこういった規則に用いられる一連のセキュリティ属性は異なるものであり、2 通りの SFP を定義する対象となる。

#### 12.2.2.2. 利用法

アクセス制御方針とは、リソースやオブジェクトに関する TOE の基本的なモデルと TOE によって、または、TOE を経由して動作する能動的なエンティティ(TOE 内部、または外部)に対し、許可されたこれらのリソースやオブジェクトに対する操作について定めたものである。したがって、アクセス制御用の SFR を特定するために、TOE モデルを導出する最初の手続きは、TOE によって提供されるリソース、オブジェクト、操作とその操作の対象となるサブジェクトと利用者を識別することである。この初期の段階では、PP、または ST の冒頭部分に記載されている一般的な TOE 機能及びオブジェクトから直接導出することができるリソース、オブジェクト、操作、サブジェクトや利用者の種類のみがこのモデルに含まれるべきである。既存の製品、またはシステムについて ST を作成する場合、このモデルで定義されたエンティティは、TOE にも存在すべきである。こういった最初のセットへエンティティを追加する場合には、整合性や欠落箇所がないことを確認する目的で SFR を定義する際に必要になることがある。

ISO/IEC 15408 では、SFR で述べているエンティティと SFR は、TOE に存在しているエンティティの概要であり、TOE の設計と実装部分に精緻に述べられているエンティティと適合すると見なされるため、TOE のモデルに記載されていないエンティティを定義すると、評価時に問題が生じてしまう。

次なる段階では、セキュリティ対策方針を満足させるように、アクセスの制限、サブジェクト及び/または消費者をモデルの中で定義する操作によってリソースやオブジェクトの利用法についての規則を定める必要がある。繰り返しになるが、既存の TOE から ST を定義する場合、TOE が実装する規則は、モデルに適用された規則を厳密に反映させたものでなければならず、モデルの中で定義されたエンティティは、TOE の実際の動作の概要を捉えたものであることは言うまでもない。

規則の中には、こういった規則の中で用いられるパラメタの識別情報が含まれている。その中でも定義しなければならない確率の高いものがリソース、利用者、サブジェクトとオブジェクトのセキュリティ属性である。初期化と管理用の規則が必要になることがあるため、こういったセキュリティ属性は、リストにまとめておくべきである。

こういった規則を定める場合は、リソース、オブジェクト、利用者、サブジェクト、または操作の異なったセットの規則との相違点を識別しなければならないことが多い。このモデルの記述を簡易化するには、セキュリティ機能方針(または、類似の規則)で同一のリソース、オブジェクト、利用者、サブジェクトと操作のセット(「種類」)をグループ化すべきである。次にそれらを識別するためにそれぞれの「セキュリティ機能方針」に名前を付す。

サブジェクトとオブジェクトの作成や削除に関する規則を定める。こういった規則は、サブジェクトやオブジェクトの種類ごとに異なる場合がある。こういった規則では、サブジェクトとオブジェクトのセキュリティ属性を初期化する方法も

定める必要がある。

サブジェクトとオブジェクトのセキュリティ属性が静的ではなかった場合のセキュリティ属性の管理に関する規則を定める。こういった規則にはTSFIを経由し外部エンティティによって着手される操作やTSFによって実行される操作の一部としてセキュリティ属性の修正方法についての規則が含まれるという点に留意する。

利用者を TOE に登録する必要がある場合は、利用者の登録方法(「作成」)と登録の抹消方法(「削除」)の規則を定める。利用者登録の規則は、利用者のセキュリティ属性を初期化する際の規則にも含まれる。利用者を登録する必要がない場合もある点に留意する。その場合、利用者は、サービスを要求し、自身が提供する電子証明書を用いて自らを識別認証することができる。こういった電子証明書には、利用者のセキュリティ属性も含まれている場合がある。このような場合は、容認される電子証明書とその電子証明書を確認する方法についての規則を定める必要がある。

利用者を識別し、(必要に応じて)認証する規則を定める。こういった規則では、利用者が提供しなければならない電子証明書(電子証明書の種類、最短、または最長の電子証明書の有効期間、最短、または最長の製品寿命などに設けられた基本的な制限)と共に適切ではない電子証明書が提供された場合の TSF の反応などに関する電子証明書を定める。

利用者のセキュリティ属性を管理するための規則を定める。これは、サブジェクトとオブジェクトを定義するのと同様の方法で定められる。

TOE が利用者とサブジェクトの関連付け機能をサポートしている場合には、この関連付けに関する規則についても定義する。こういった規則には、次のような内容が含まれている場合がある:

- 関連付けを許可する際に満足する必要がある条件/状態。
- 関連付けがされた後にセキュリティ属性のサブジェクトを設定。

規則を定義し終わったならば、追加的な管理規則が必要かどうかを確認しなければならない。セキュリティ属性を管理する方法(すなわち、利用者が役割の一部として取得する利用者のセキュリティ属性のセットの定義)の規則を用いて、新たなセキュリティ属性(すなわち、新たな利用者の役割)の作成を許可する追加的な規則が、この例である。

### 12.2.3. 利用者の管理

#### 12.2.3.1. 説明

ISO/IEC 15408-2 のパラダイムでは、利用者は TOE のインタフェースを用いて TOE からサービスを要求する、TOE 外部エンティティであると定義されている。利用者は、TOE のサービスを利用する前や、登録されていない利用者によってリクエストされたサービスを許可する場合には利用者を「登録する」必要がある。リクエストされたサービスが TOE によって提供されるかどうかは、利用者のセキュリティ属性によって決定されることが多い。利用者のセキュリティ属性は、リクエスト、利用者について保存されている TOE、または利用者が属するグループから導出されたデータのいずれかと共に提供することができる。

1 番目のケースの場合は、TOE は、利用者によって提供されたセキュリティ属性を信頼することができるということを保証する必要がある。これは、TOE がセキュリティ属性の評価方法について定めた規則を実装しており、(出所が不明の)利用者がセキュリティ属性を合法的に利用しているという信頼を確立することを意味する。

2 番目のケースでは、TOE は、利用者の識別情報、または利用者が属するグループの識別情報を知る必要がある。また、この場合、TOE は、主張された利用者の識別情報、または利用者が属するグループのメンバーシップが正しいことを確認する方法を定める規則を実装する必要がある。この手続きは認証と呼ばれ、利用者は、主張する識別情報やグループのメンバーシップが正確であるという信頼を確立するために、TOE によって用いられた電子証明書を提出する必要がある。したがって、ここでは認証手続きを実施する方法と認証手続きのパラメタを管理する方法を定める必要がある。

TOE が、利用者に登録するよう要求した場合には、利用者を登録する規則とそのセキュリティ属性を管理する方法についての規則を定める必要が生じる。

時に、TOE は、利用者に替わって動作するために、その利用者のサブジェクトの 1 つを利用する。この場合、そのサ

ブジェクトは、TSF によって利用者と関連付けられる。つまり、TSF では、そのサブジェクトを利用者と関連付ける際にサブジェクトのセキュリティ属性を導出する方法が定められる。実際のアクセスが、サブジェクトによって実施される場合であっても、そのサブジェクトは、アクセス管理方針をベースにした利用者のセキュリティ属性の実施を許可する利用者のセキュリティ属性の一部を継承することが多い。

#### 12.2.3.2. 利用法

利用者の管理機能を定義するには、次のような手順を実施する必要がある:

- TOE へアクセスする利用者の種別(と共に、それぞれの利用者種別に備わっているセキュリティ属性のセット)を識別し、定義する。
- 利用者が、TOE の機能を利用する前に登録する必要がある場合は、その利用者種別を識別する。
- 登録する必要がある利用者については、利用者を登録するための規則(方法)と共に、登録時に設定する必要がある利用者のセキュリティ属性に関する規則を明らかにする。
- 利用者の識別情報が要求される場合は、すべての利用者種別を特定する。その場合には、利用者を特定する方法を明らかにする。利用者を認証するために必要な条件を明らかにする。
- 認証手続きを管理する方法(認証時に用いられる電子証明書の管理も含め)を明らかにする。
- それぞれの利用者種別について、利用者のセキュリティ属性を管理する方法を明らかにする。
- 利用者とサブジェクトの関連付けが可能な場合、または必要な場合には、その関連付けに関する規則を明らかにする。特に、サブジェクトのセキュリティ属性が、関連付けの手続き時に設定される方法を明らかにする。

### 12.2.4. TOE の自己保護

#### 12.2.4.1.説明

次の条件が 1 つでも当てはまる場合には、セキュリティ機能そのものを保護する必要がある:

- セキュリティ対策方針を実現することができないような TOE の環境を対象としてセキュリティ機能を攻撃するような脅威エージェントが存在する可能性がある場合。
- TOE 環境の要素に不具合があり、セキュリティ対策方針を実現することができない可能性がある場合。
- TSF の要素に不具合があり、セキュリティ対策方針を実現することができない可能性がある場合。

このような事態を検知し、対応するための条件と共にこのような事態にセキュリティ対策方針を実現するための条件も TSF の自己保護機能の一部として定める必要がある。

機能性モデルで TOE の自己保護を定義する場合は、次のような条件が必要である:

- 可能性のある攻撃シナリオとセキュリティ対策方針を侵害する TOE の誤動作を特定する。
- 攻撃や誤動作を回避することができる機能を特定する。そういった機能の例として、特定の物理的な攻撃を回避する TOE の先端的な物理的保護がある。
- 回避策が可能ではない場合(一般的には、可能ではない場合が大半である)、攻撃や誤動作を検知し、適切に対処することができる機能を特定する。

外部からの攻撃や TOE 環境におけるシステムの誤動作の検知には、TSFI による監視と攻撃を受ける原因となる状態の確認、攻撃を受ける原因となるコミュニケーションリンクの状態や攻撃を検知するために、TOE が特別に備えているセンサによる監視が必要になる場合がある。

#### 12.2.4.2. 利用法

TOE の自己保護機能を明らかにするには、セキュリティ対策方針を満足させるためにそういった機能が要求されているかを SPD から特定する必要がある。TOE の自己保護機能を明らかにしなければならない場合は、外部からの

攻撃を（例えば、物理的な保護を強化することによって）回避する必要があるか、攻撃、または誤動作を検知し、対処する必要があるのかを選択しなければならない。

TOE の環境を意図している場合、どの攻撃、または不具合をどの時点で対処しないとセキュリティ対策方針に侵害する可能性があるかについてのリストの作成から着手する。それぞれのリストごとに、対象となる攻撃や誤動作に対処する方法を明らかにすべきである。つまり、TOE のセキュリティ機能によって回避されるのか、あるいは TOE のセキュリティ機能が、攻撃、または誤動作を検知し、それに対処する必要があるのかを明らかにする必要がある。

TOE のセキュリティ機能によって攻撃が回避される場合は、その機能性によって対抗される攻撃の種類を特定すると共にその根拠を説明する必要がある。

TOE のセキュリティ機能によって攻撃、または誤動作を検知し（こういった場合、TOE がどのような機能を実行しなければならないかについて、要約レベルの規則で述べられているように）、（要約レベルで）検知時、及び対処時の基準や規則を明らかにする必要がある。

TSF は、テストを実行する内部状態の変数値、TOE 内部の機能の監視、または機能やデータの冗長性や矛盾点の確認によって誤動作を検知する。

こういった対処には、次のようなものがある：

- 攻撃や誤動作による影響を排除する修正アクション。この修正アクションの例として、データ、または機能性の冗長性をベースにして、不具合を検知し、自動的に修正することができる機能が挙げられる。
- 攻撃や誤動作による影響を部分的に排除するが、（TOE のセキュリティ対策方針に適合する必要がある）TOE の機能性を結果として若干低減させる修正アクション。この修正アクションの例として、不具合や攻撃から回復させる機能があるが、その回復には時間を要し、完全ではないことがある。このような場合は、機能の実施に遅延が生じたり、回復が完全ではないデータによってセキュリティ対策方針に違反したりすることがないように確実さを期す必要がある。
- 修正アクションマニュアルの作成（例えば、攻撃や誤動作による影響を受けるTOEの一部、またはTOE全体の停止、停止された TOE の一部、または TOE 全体をセキュアモードで再開するための要求）。
- 安全に再開するために、TSF 内部では何ら対策されていないTOEの不具合箇所、またはTOE全体の停止。この例には、攻撃や誤動作を検知した場合、そのセキュリティ対策方針に違反しないように、重要な機能やデータを破壊してしまう TOE がある。

上述のような修正アクションのリストは、TOE 全体の機能性で影響度の高い順に分類される。

### 12.2.5. セキュリティが確保された通信

#### 12.2.5.1. 説明

外部エンティティ、または信頼/信用できない通信チャネルを用いて配布された TOE の一部のいずれかと通信する際にデータを保護する機能が、追加的なモデルを要求する機能のもう 1 つの例である。

通信をモデル化するには、通信チャネルのセキュリティ特性を明らかにする必要がある。こういったセキュリティ特性には次のようなものがある：

- 通信相手の認証。
- 通信チャネルを介して転送されるデータの完全性の保護（これには、メッセージのリプレイ保護、及び/またはメッセージシーケンスの変更の防止が含まれる）。
- 通信チャネルを介して転送されるデータの機密性の保護。
- データの喪失に対する保護。
- メッセージの送信、及び/または受信時の否認防止対策。

通信チャネルをモデル化するには、通信のピア（通信を行うエンティティ）はもとより、通信チャネルのセキュリティ特性を明らかにする必要がある。これは、オンラインの通信、オフラインの通信の双方に当てはまる。

#### 12.2.5.2. 利用法

セキュリティが確保された通信に要求される機能を認識するには、次のような手続きが必要である:

- 通信リンクの特定。
- 通信リンクごとに要求されるセキュリティ特性の定義。こういったセキュリティ特性の例には、次のようなものがある:
  - 通信を行うピアの認証(authentication)。
  - 完全性の保護(リプレイの保護、メッセージシーケンスの保護などが含まれることがある)。
  - 機密性の保護(トラフィックフロー分析の保護が含まれることがある)。
  - 否認防止対策(メッセージの送信時/受信時、または双方)。
  - 通信時のデータ喪失防止対策。

要求されるセキュリティ特性は、通信リンクごとに明らかにしなければならない。ST でもこういったセキュリティ特性を実装するためのメカニズム(特に暗号メカニズムについて)が定義されている。PP では、要求されている程度の詳述さで定義すべきである。TOE に適合する PP が相互運用性要件も満足させることが想定される場合、この詳述さのレベルは非常に高位になることがあるという点に留意する。このような場合は、PP であっても特定のプロトコルのレベルと共に相互運用性を確保するために必要なプロトコルオプション(例えば、暗号アルゴリズム)のメカニズムを詳しく明記することができる。

通信リンクのリストを確認する場合は、物理的な通信リンクだけではなく、具体的な保護を要求する(例えば、アプリケーションプロトコルレベルなど)論理的なリンクについても確認すべきである。こういった通信リンクでは、個々のレベルごとに異なった種類の保護が提供されている場合、異なったプロトコルのレベルが積み重ねられることがある。例えば、IP レベルの IPsec がピアエンティティを認証すると共に、(システムの場合には)完全性と機密性の保護も提供している場合がある。(また、別の論理的な通信リンクである)IPsec の最上部にあるアプリケーションプロトコルでは、(例えば、利用者(人間)やアプリケーション)に追加的な認証と共に否認防止機能も提供されることがある。このような場合、IPsec とそのアプリケーションプロトコルは、それぞれのセキュリティ特性と共に別個の通信リンクとしてリストされるべきである。

セキュリティを確保する通信リンク機能の大半には、こういった状態を検知する機能によって、完全性を保護すると共にデータ喪失に対する保護が実施されるという点に留意する必要がある。TOE の自己保護の項で説明した検知機能と同様に、こういった状態が検知された場合には、TOE の対処法を明らかにする必要がある。

また、認証の試みが失敗した場合や無効な否認防止の対処法についても明らかにする必要がある。

通信を行うピアの身元が不明の通信では、TOE が管理する TSF データや、利用者データのエクスポート、及び TOE への TSF データや利用者データのインポートは、特別なケースと考えることができる。エクスポートやインポートを実施する場合には、次のような(セキュリティ)特性を考慮することができる:

- 完全性の保護(リプレイ防止や有効期限なども含まれることがある)。
- 機密性の保護。
- 否認防止対策(エクスポート、インポート、または双方について)。

### 12.2.6. セキュリティ監査

#### 12.2.6.1. 説明

明らかにされたセキュリティ関連の重要なイベントの監視、及びこういったイベントに自動的に応答する機能を今後の分析や評価用に記録として残すことは、セキュリティ対策方針を満足させるために TOE に要求される別なセキュリティ機能である。セキュリティ関連の重要なイベントとは、能動的なエンティティがセキュリティに関連のサービスの利用を直接 TOE に要求する場合やセキュリティについて検知された重要な状態やイベントがこういったリクエストに直接対応することができないことを指す。

セキュリティ関連の重要なイベントには、次のようなものがある:

- TSF によって提供されたサービスを利用することの試みの成功、および/または失敗。
- 予期していなかった不具合の発生。
- リモートで信頼のおける IT 製品の予期していなかった、または欠陥がともなった動作。
- 自己テスト機能によって検知された不具合。
- 詳述すぎるセキュリティの重要な閾値に関する定義。
- 重要な TSF データの変更。
- 個々のイベントについて監査に値するほど重要ではないと考えられていたイベントの集積。

#### 12.2.6.2. 利用法

セキュリティ監査をモデル化するには、次のような手続きが必要である:

- 監査が必要なイベントをリスト化する。
- イベントを監査する場合の規則を明らかにする(例えば、リクエストが拒否された場合に限る、など)。
- イベントごとの収集する必要のあるデータを明らかにする。
- 収集した監査用のデータを処理し、分析する方法を明らかにする。

監査の必要性があるセキュリティ機能に関連のイベントが発生した場合は、個々のセキュリティ機能を分析することが適切な実践となる。また、セキュリティ機能のモデルでは、セキュリティ機能に関連のイベントが発生した場合、監査記録を作成する必要がある重要な内部状態を把握するために分析すべきである。

### 12.2.7. アーキテクチャ要件

#### 12.2.7.1. 説明

前項でリストした要件に加え、TOE アーキテクチャに関する要件を定める必要性もある。こういった要件は、TOE のアーキテクチャ分析を実施することができ、読者が容易に TOE アーキテクチャを理解するために必要になることがある。こういった TOE アーキテクチャに関連のセキュリティ要件は、TOE が実行しなければならないセキュリティに特化した特性と関連しているのが通常である。こういった特性の一般的な例には、次のようなものがある:

- 耐障害性。
- 情報フロー制御。
- プライバシー特性。
- リアルタイム特性。

アーキテクチャ要件は、前項のセキュリティ要件に対応していることが多い。例えば、情報フロー制御やプライバシー特性は、通常、オブジェクトにアクセスする際に定められている規則が伴い、耐障害性は、欠陥を検知する際に用いられるセキュリティ監査要件が伴うのが一般的である。こういったアクセス制御に関する規則の中でも、特にセキュリティ監査に関する規則は、必要なものではあるが、通常、セキュリティに特化した要件を実施するには十分とは言えない。

アーキテクチャ要件は、他の SFR を特定し、その仕様を定めるよりも困難である。それにも関わらず、アーキテクチャ要件の中には、セキュリティ対策方針と完全に適合することが要求されるものがあるため、PP、または ST の中で、SFR の一部として定義する必要がある。

#### 12.2.7.2. 利用法

アーキテクチャ要件を特定し、モデル化するには、次のような手続きを実施する:

- 対処されていないセキュリティ対策方針、または前項でセキュリティ要件によって全面的に対処されていないセキュリティ対策方針を特定する。
- 対策方針を満足するために要求されるアーキテクチャ要件を識別する。
- こういったアーキテクチャ要件を提供するための規則を明らかにする。

このガイドでは、アーキテクチャ要件を選択する方法について、僅かな助言を提供するにとどめている。ST の場合、こういった要件は、ST を作成する際に TOE を構築するための要件によってあらかじめ定義されている場合が多いためである。例えば、TOE が配布されるものであることが判明している場合、セキュリティ対策方針を明らかにするために、TOE の配布される拠点間で受け渡しされるデータの整合性を維持するための要件や TOE の配布される拠点間でデータを受け渡しする際に不正アクセスからデータを保護するための要件が必要になることがある。TOE が TSFI におけるセキュリティ対策方針に対応し続けるかぎり、TOE 内部の TSF に対応する内部機能が支援すべきであるという意見もあるが、セキュリティ対策方針に対応する必須の内部機能を特定することによって、評価時に TOE を把握し、分析するのに有効である。

## 12.3. PP、または ST で SFR を特定する方法

### 12.3.1. SFR はどのように選択すべきか？

SPD の一貫として TOE のセキュリティ対策方針を定義したならば、次なる段階は、こういったセキュリティ対策方針と適合させる方法を詳述する必要がある。これは、上述の通り、コンポーネントのレベルで SFR の適切なセットを選択することによって実施する。むろん、あらかじめ定義されている TOE のセキュリティ対策方針に関連の機能パッケージが利用可能な場合は、SFR の選択手続きはことのほか容易である。

SFR は、TOE の全体的な機能性モデルをベースにして選択される。この機能性のモデルでは、リソース、利用者、

サブジェクト、オブジェクト、及び操作について定めている。次に SFR では、セキュリティ対策方針が、TOE の機能要件のモデルの範囲内で適合するものとして、セキュリティの機能性を定義する。すべてのモデルと同様に、TOE の機能要件のモデルは、TOE の実際の機能要件を要約したものだが、TOE の主要な機能性を理解するのに十分な詳述さのレベルでなければならない。セキュリティ対策方針に適合させるために制御する必要のないリソース、利用者、サブジェクト、オブジェクト、及び操作は、SFR を定める際に無視することができる。例えば、TOE のセキュリティ対策方針がデータへのアクセス制御のみである場合、リソースである「CPU 時間」は、SFR を定める際に考慮する必要がない。

PP、または ST 用に SFR を選択する手順には数通りの段階がある。選択手順では、次のような 2 通りの SFR の違いを明らかにすることが有効である:

a) TOE で識別されたセキュリティ対策方針を*直接*満足させる SFR 実施。

b) TOE で識別されたセキュリティ対策方針を直接満足させることはないが、*SFR 実施*への支援を提供するばかりではなく、TOE に関連するセキュリティ対策方針を*間接的に*満足させるのに有効な SFR 支援。

ISO/IEC 15408 では、こういった 2 通りの SFR の違いを*明確に*区別してはいないが、この相違点は機能コンポーネント間の依存性のようなものとして、SFR が相互に対応していることを証明するために、*黙示的に*考慮される。したがって、PP、または ST では、*SFR 実施*か、*SFR 支援*かを明確に区別する必要はなく、PP、または ST を作成する際は、SFR に 2 通りの種類があることを認識することが非常に有効である。

よって、SFR を選択する際の最初の段階は、TOE のセキュリティ対策方針ごとに、TOE を直接満足させる機能性モデルの *SFR 実施*を認識することである。*SFR 実施*の完全なセットが確立されれば、次なる手続きは *SFR 支援*の完全なセットによる反復的な手順の認識である。上述のように、(*SFR 実施*、*SFR 支援*に関係なく)すべての SFR は、可能であれば、ISO/IEC 15408-2 の適切な機能要件を用いて表現すべきである。第 12.3.2.項では、一般的な SFR を示すには、どの機能要件を用いるべきかを特定するためのガイダンスを提供している。ISO/IEC 15408-2 から機能コンポーネントを選択する際は、そのコンポーネントが適切かどうか、またそのコンポーネントをどのように解釈すべきかについて、ISO/IEC 15408-2 の付録に記載されているガイダンスも参考にすべきである。

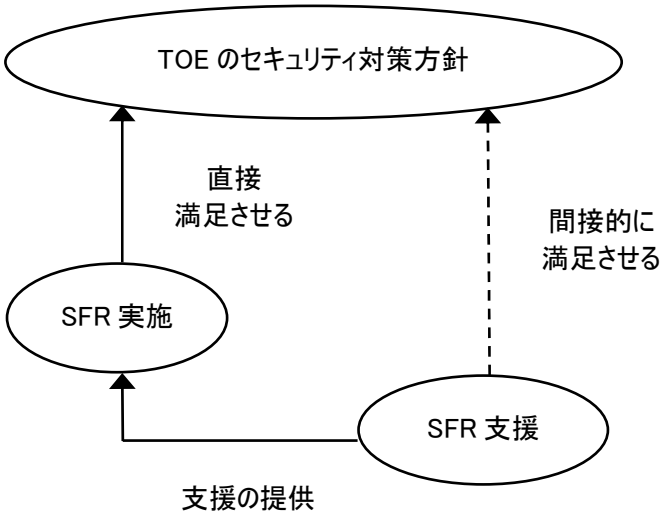


**図 4:SFR 実施と SFR 支援の役割**

こういった 2 通りの SFR の関係は、上の図 4 に示したとおりである。この関係は、PP、または ST の根拠とも関連性を持っており、*とりわけ*、SFR 間が相互に支援していることを証明するために必要であるという点に留意する。このことは、TOE のセキュリティ対策方針と確実に適合するために有効な SFR 支援によって提供される支援の内容とも関連がある。

*SFR 支援*の完全なセットを特定するには次のような 3 つの段階がある:

a) すべての *SFR 実施*の(機能コンポーネントの関連で ISO/IEC 15408-2 で定義されている)依存性を(適切であると考えるレベルまで)満足させるために必要な、追加的な SFR を特定する。これには、この段階で *SFR 支援*として特定されたすべての依存性が含まれる。

b) TOE のセキュリティ対策方針を達成するのに必要な追加的な SFR を特定する。これには、TOE のセキュリティ機能を破る複合型の攻撃に対して、*SFR 実施*を保護し、その脅威を対象とする TOE のセキュリティ機能を搭載するのに必要な SFR が含まれる。

c) 第 2、第 3 段階で選択された *SFR 支援*の依存性を(適切であると考えるレベルまで)満足させるために必要な追加的な SFR を特定する。

ISO/IEC 15408-2 で認識されているような依存性を満足させる SFR 支援の特定は、反復的な手順のようなものである。例えば:

a) PP、または ST に、差し迫ったセキュリティ侵害を示すイベントの検知に具体的な応答を返すために、TOE に必要なセキュリティ対策方針が含まれる場合を想定する。この場合、TOE に、FAU_ARP.1(セキュリティアラーム)に関するコンポーネントをベースにした *SFR 実施*を包含するという結論が導出される。

b) ISO/IEC 15408-2 では、FAU_ARP.1 には、*SFR 支援*として含まれるべき FAU_SAA.1(侵害の可能性の分析)に関する依存性が含まれている。

c) FAU_SAA.1 には、FAU_GEN.1(監査データ生成)に関する依存性が含まれている。

d) FAU_GEN.1 には、FPT_STM.1(高信頼タイムスタンプ)に関する依存性が含まれている。

e) FPT_STM.1 には、追加的な機能コンポーネントを導入する要件はない。

ISO/IEC 15408 では、依存性の中に「満足されていない」ものがあっても、そのままで構わないとしている。ただし、その関連のある SFR が、なぜセキュリティ対策方針を満足させる必要がないのかを説明しなければならないという点に留意すべきである。(したがって、セキュリティの考慮事項を解決すべきである。)

依存性には、一貫性のある方法が適用されるべきである。例えば、FAU_ARP.1 の場合、一貫性は、要件の内容に取り入れられている(FAU_ARP.1 は、FAU_SAA.1.2.で定義されている潜在的なセキュリティ侵害の説明を適用すること依存している)。

その他のコンポーネントの場合、一貫性を理解するのはさらに難しい。例えば、FDP_ACC.1 の場合、PP、または ST では、特定のアクセス制御 SFP を認識しなければならない。FDP_ACC.1 の依存性である FDP_ACF.1 を満足させるには、FDP_ACF.1 は、FDP_ACC.1 で用いられていたアクセス制御 SFP に対応していなければならない。異なるアクセス制御 SFP を用いるために、FDP_ACC.1 に繰返し操作が適用されている場合、FDP_ACF.1 の依存性は、ぞれぞれのアクセス制御 SFP を満足させる必要がある。

追加的な *SFR 支援*(すなわち、ISO/IEC 15408-2 では、依存性として認識されていないもの)を特定する手順には、TOE のセキュリティ対策方針の達成を支援するために必要な、その他の SFR の特定が含まれる。こういった SFR では、攻撃者が利用できそうな機会を低減したり、攻撃を成功させるために攻撃者側が搭載しなければならない技能やリソースのレベルを上昇させる(攻撃者の技能やリソースを無駄に費やさせる目的)ための支援を提供したりするのが一般的である。以下は、セキュリティに関する考慮事項やセキュリティ対策方針を踏まえて、検討すべき事柄である:

a) ISO/IEC 15408-2 の同じクラスの関連コンポーネントをベースにした SFR。例えば、FAU_GEN.1(監査データ生成)が含まれている場合、(FAU_STG ファミリの中から 1 つ以上の機能コンポーネントを要求し)生成されたデータを保存するにはセキュリティが確保された監査証跡を作成し、維持する必要があり、(FAU_SAR ファミリの中から 1 つ以上の機能コンポーネントを要求し)生成された監査データを確認するためのツールが必要になることがあるという意味が含まれている。言い換えれば、生成されたデータは、レビューのために別のシステムにエクスポートすることができる。

b) FPT(TSF の保護)クラスに関連のコンポーネントをベースにした SFR。こういった SFR では、他の SFR の機能

性も保護することができるが、その SFR に対応している TSF や、TSF データの完全性、及び/または可用性も保護されるのが一般的である。この例には、FPT_TEE.1（外部エンティティのテスト）に関する要件や（悪質な手口などによって）TSF にもたらされた不具合、破損、改ざんなどに対し、明らかに TSF を保護する必要性が生じた場合に、セキュリティ対策方針に対応するために必要な FPT_PHP（TSF 物理的保護）関連のファミリのコンポーネントが含まれる。

c) FMT（セキュリティ管理）クラスに関連のコンポーネントをベースにした SFR。こういったコンポーネントは、セキュリティ管理用 SFR の支援に必要な要件を定めるために用いられる。この例には、セキュリティ属性の取り消しに対応する FMT_REV.1 があり、セキュリティ属性（例えば、アクセス制御）を扱う SFR に関連の要件が含まれる。

こういった *SFR 支援*は、セキュリティ対策方針や機能性モデルなど、特に、相互的な支援ができ、統合的、かつ効果的な SFR のセットを完成させる必要性を常に考慮し、選択すべきである。PP、または ST の根拠を組み立てる手続きは、したがって、この選択手続きに大きな影響を及ぼすことがある。セキュリティ対策方針の達成に必要のない *SFR 支援*を含めることは、PP、または ST で定めた内容に次のような制約を加えてしまうため、断じて進言できない:

a) TOE の中にはこういった SFR に適合しないものがある。

b) SFR の数を増やすことによって、評価時の費用や不必要な要件を維持するための費用がかさむ。

PP、または ST が、関連のある PP をベースに用いて作成されている場合、SFR を選択する手順が大幅に単純化される。作成された PP、または ST は、適宜、TOE のセキュリティ課題定義、及び/またはセキュリティ対策方針との違いを考慮し、別の SFR を含めて作成すべきである。

### 12.3.2. ISO/IEC 15408-2 の中から SFR を選択する場合

以下は、前項で説明したパラダイムと ISO/IEC 15408-2 で定義されている SFR コンポーネントとの対象表である。コンポーネントの中には 1 つ以上の角度から捉えたパラダイムが含まれているものもあるため、1 回以上リストされているコンポーネントもある。

**表 1－アクセス制御**

| 要件 | 対応コンポーネント |
|---|---|
| サブジェクト、オブジェクト、操作の定義 | FDP_ACC.1、FDP_ACC.2、FDP_IFC.1、FDP_IFC.2、FMT_SMF.1 |
| セキュリティ属性の定義 | FDP_DAU.1 、FDP_DAU.2 、FDP_IFF.1 、FDP_IFF.2 、FRU_PRS.1 、FRU_PRS.2、FRU_RSA.1、FRU_RSA.2 |
| サブジェクト、オブジェクトの作成 | FDP_ITC.1、FDP_ITC.2、FMT_SMF.1 |
| オブジェクトのエクスポート | FDP_ETC.1、FDP_ETC.2 |
| セキュリティ属性の管理 | FDP_ITC.2 、FIA_USB.1 、FMT_MSA.1 、FMT_MSA.2 、FMT_MSA.3 、FMT_MTD.1、FMT_MTD.2、FMT_MTD.3、FMT_REV.1、FMT_REV.2、FMT_SAE.1、FTA_LSA.1 |
| アクセス規則の定義 | FDP_ACF.1 、FDP_IFF.1 、FDP_IFF.2 、FDP_ROL.1 、FDP_ROL.2 、FRU_PRS.1、FRU_PRS.2、FRU_RSA.1、FRU_RSA.2 |
| アクセス制御規則の管理 | FMT_MOF.1、FMT_SMF.1 |

表 2－利用者管理

| 要件 | 対応コンポーネント |
|---|---|
| 利用者種別の定義 | FMT_SMF.1 |
| セキュリティ属性の定義 | FIA_ATD.1 |
| 利用者識別の規則 | FIA_UID.1、FIA_UID.2 |
| 利用者認証の規則 | FIA_AFL.1 、FIA_SOS.1 、FIA_SOS.2 、FIA_UAU.1 、FIA_UAU.2 、FIA_UAU.3、FIA_UAU.4、FIA_UAU.5、FIA_UAU.6、FIA_UAU.7 |
| 利用者電子証明書と<br>セキュリティ属性の管理 | FMT_MSA.1 、FMT_MSA.2 、FMT_MSA.3 、FMT_MSA.4 、FMT_MTD.1、FMT_MTD.2、FMT_MTD.3、FMT_REV.1、FMT_REV.2、FMT_SAE.1、FMT_SMR.1、FMT_SMR.2、FMT_SMR.3、FTA_LSA.1、FTA_MCS.1、FTA_MCS.2 |
| 識別認証規則の管理 | FMT_MOF.1、FMT_MTD.1、FMT_MTD.2、FMT_MTD.3、FMT_SMF.1 |
| 利用者とサブジェクトの関連付けの管理 | FIA_USB.1 |

表 3－TOE の自己保護

| 要件 | 対応コンポーネント |
|---|---|
| 欠陥の検知 | FPT_TEE.1 、FPT_ITI2 、FPT_ITT.3 、FPT_PHP.1 、FPT_PHP.2 、FPT_PHP.3、FPT_RPL.1、FPT_TST.1、FRU_FLT.1、FRU_FLT.2 |
| 欠陥への対応 | FPT_ITT.3 、FPT_PHP.2 、FPT_PHP.3 、FPT_RCV.1 、FPT_RCV.2 、FPT_RCV.3、FPT_RCV.4、FPT_RPL.1、FRU_FLT.1、FRU_FLT.2 |
| 欠陥と対応規則の管理 | FMT_MOF.1、FMT_MTD.1、MFT_MTD.2、MFT_MTD.3、FMT_SMF.1 |

表 4－セキュリティが確保される通信

| 要件 | 対応コンポーネント |
|---|---|
| 通信リンクの確立 | FMT_SMF.1、FTP_ITC.1、FTP_TRP.1 |
| 通信リンク特性（セキュリティ属性）の定義 | FCO_NRO.1 、FCO_NRO.2 、FCO_NRR.1 、FCO_NRR.2 、FDP_UTC.1 、FDP_UID.1 、FDP_UID.2 、FDP_UID.3 、FPT_ITC.1 、FPT_ITI.1、FPT_ITI.2、FPT_RPL.1、FTP_ITC.1、FTP_TRP.1 |
| 通信リンク特性の管理 | FMT_MSA.1 、FMT_MSA.2 、FMT_MSA.3 、FMT_MTD.1 、FMT_MTD.2、FMT_MTD.3、FMT_REV.1、FMT_REV.2、FMT_SAE.1 |
| リンク確立規則の管理 | FMT_MOF.1 、FMT_MTD.1 、FMT_MTD.2 、FMT_MTD.3 、FMT_SMF.1 、FTA_SSL.1 、FTA_SSL.2 、FTA_SSL.3 、FTA_SSL.4 、FTA_TAB.1、FTA_TAH.1、FTA_TSE.1 |

表 5－監査

| 要件 | 対応コンポーネント |
|---|---|
| 監査すべきイベントの定義 | FAU_GEN.1、FAU_GEN.2、FAU_SEL.1 |
| イベントに対する対応の定義 | FAU_ARP.1、FAU_SAA.1、FAU_SAA.2、FAU_SAA.3、FAU_SAA.4 |
| イベントの管理の定義 | FAU_SAR.1、FAU_SAR.2、FAU_SAR.3 |
| 監査証跡の管理の定義 | FAU_STG.1 |
| 監査規則の管理 | FMT_MOF.1、FMT_MTD.1、FMT_MTD.2、FMT_MTD.3 |

表 6ーアーキテクチャ要件

| 要件 | 対応コンポーネント |
|---|---|
| 監査証跡の保護 | FAU_STG.2、FAU_STG.3、FAU_STG.4 |
| 暗号機能 | FCS_CKM.1、FCS_CKM.2、FCS_CKM.3、FCS_CKM.4、FCS_COP.1 |
| 情報フロー制御 | FDP_IFF.3、FDP_IFF.4、FDP_IFF.5、FDP_IFF.6 |
| TOE 内転送 | FDP_ITT.1、FDP_ITT.2、FDP_ITT.3、FDP_ITT.4 |
| 残存情報の護 | FDP_RIP.1、FDP_RIP.2 |
| 蓄積データ完全性 | FDP_SDI.1、FDP_SDI.2、 |
| 管理 | FMT_MTD.1 |
| プライバシー保護 | FPR_ANO.1、FPR_ANO.2、FPR_PSE.1、FPR_PSE.2、FPR_PSE.3、FPR_UNL.1、FPR_UNO.1、FPR_UNO.2、FPR_UNO.3、FPR_UNO.4 |
| フェールセキュア | FPT_FLS.1 |
| 可用性 | FPT_ITA.1、FPT_ITT.1、FPT_ITT.2 |
| 状態の同期 | FPT_SSP.1、FPT_SSP.2 |
| セキュリティが確保されたタイムスタンプ | FPT_STM.1 |
| データー貫性 | FPT_TDC.1、FPT_TRC.1 |

この表は、第 12.2 項と第 12.3.1.項のガイダンスにもとづいて定められたセキュリティの機能性モデルに対応する、適切な SFR コンポーネントを特定し易くするために作成されたものである。どのコンポーネントを選択し、そのコンポーネントに対し許可された操作を用いて、セキュリティの機能性モデルをさまざまな角度からどのように表現するかは、ST、または PP の作者の判断にゆだねられている。

アーキテクチャ要件では、ISO/IEC 15408-2 の SFR コンポーネントに対応するアーキテクチャの課題についてまとめたリストが提供される。

### 12.3.3. SFR を操作する方法

#### 12.3.3.1. 許可された操作

上述第 10.1.項（ISO/IEC 15408-2 の第 2.1.4.項も参照）でも説明したように、機能コンポーネントの中には、PP、またはSTの内容に応じて、PP、またはSTの作成者に対しセキュリティ要件を調節するような要求を許可する操作が含まれているものがある。そういった操作には、次のようなものがある：

a) *割付*。認識されたパラメタの特定を許可する。

b) *繰返し*。異なった要件を表現するために、同じ機能コンポーネントの複数回の利用を許可する。

c) *選択*。所定のリストの中から 1 つ、または複数の項目の特定を許可する。

d) *詳細化*。他の SFR の中から新たに別の依存性を導入せずに、容認されたソリューションのセットをより厳格にすることによってセキュリティ要件に詳述さを追加することを許可する。

#### 12.3.3.2.繰返し

*繰返し*の操作は、ISO/IEC 15408-2 のさまざまな機能コンポーネントの依存性として要求される FMT(セキュリティ管理)クラスのコンポーネントを用いて SFR を表現するために必要になることが多い。これらの依存性を満足させるには、*割付*と*選択*操作を個々に満足させる、同じコンポーネントが必要になるのが一般的である。例えば、FMT_MSA.1 では、異なった種類のセキュリティ属性の管理に関連する異なった SFR を定義するために、複数回繰返されることがある。同様に、TOE が異なったアクセス制御方針を実行するよう要求された場合には(例えば、任意アクセス制御(DAC)とロールベースアクセス制御(RBAC))、FDP_ACC と FDP_ACF ファミリの中からコンポーネントを複数回用いるのが望ましい。

例えば、複雑で大きすぎて扱いにくい SFR を明確かつ管理しやすい機能要件に細分化する場合など、PP、または ST の明確さを期すために、繰返しの操作を用いることが推奨される。ただし、繰返しの操作によって、PP、または ST に記載された SFR を表示する際に、別の潜在的な問題点がもたらされる。

#### 12.3.3.3. 割付と選択

*割付*の操作では、パラメタの値がヌル(空値)である可能性があるのに対し、*選択*の操作では、最低でも 1 つのパラメタの値が常に特定される。PP で、*割付*、または*選択*の操作が完了することによって、ST の作者が、(詳細化の操作以外で)セキュリティ対策方針と適合させるために、機能コンポーネントの調整方法を決定する必要がなくなる。言い換えれば、(割付や選択の操作が適用される範囲では)ST の作者が「決定すべき」事柄がない、ということである。

通常、個々の*割付*や*選択*の操作は、ST の作者によって完成される必要がある。PP の場合は、操作を満足させるために、内容の充実さを期す(つまり詳述過ぎる)ことで、PP との適合性を主張することができる TOE の数が限られてしまうことにもなりかねない。したがって、操作が満足されるように上手くバランスを取るには、次のような項目をベースに PP を作成する必要がある:

a) 作者の要件のセット一式。

b) 実装に依存しないこと。

c) 対策方針に適合していることが証明できるように詳しく説明されていること。

したがって、割付と選択の操作を完成させるために必要な範囲でセキュリティ対策方針と適合させることが必要である。セキュリティ要件の根拠を構築する場合は、厳しい試験が実施される:IT セキュリティ要件がセキュリティ対策方針に適合することを証明するために提出される根拠は、SFR で特定されていない内容に基づいてはならない。例えば、FDP_ACF.1 をベースにしたアクセス制御要件の SFR で、OSP で既に定義されている規則に関連の(この場合は、アクセス制御)セキュリティ対策方針と適合することを目的としている場合、そのアクセス制御規則は、全面的に ST の作者の手にゆだねられているのが適切であると考えることができる。この場合、PP の作者は、TOE で実装されるアクセス制御規則の詳細を決定し、PP との整合性を主張する ST の作者に十分な裁量をゆだね、自身は、一般的なセキュリティ対策方針を満足させるために必要な割付と選択の操作のみを完成させるべきである。

上述のような問題を解消するために利用できる技術の 1 つが、操作を*部分的に*完成させることである。この方法を取り入れることによって、ST の作者に最大の自在性を提供することができると共に、TOE のセキュリティ対策方針とは一致していない割付や選択の操作が選ばれる可能性を排除することができる。

例えば、(FAU_STG.4.1.をベースにした)次のような SFR では、PP の作者が、TOE のセキュリティ対策方針とは不適合であると判断した「監査可能なイベントを無視する」という選択肢を排除することによって、選択の部分的な操作が完成される。したがって、SFR は、ST の作者に対し、(3 つではなく)2 つの選択肢を提供することができる:

*TSF は、監査証跡が満杯になった場合、[選択:「特別な権限をもつ許可利用者に係わるもの以外の監査事象の抑止、」、「最も古くに格納された監査記録への上書き」]、及び[割付:「監査格納失敗時にとられるその他のアクション」]を行わなければならない。*

割付操作では、PP の作者は、ST の作者に、TOE の環境に適している選択肢のセットの選択の幅を狭めてもらうことができる。この場合、PP の作者は、ST の作者の代わりに、適切な選択肢が含まれている選択の操作に替わり、割付の操作を完成させることができる。

一般的に、選択操作がベースとなっている機能コンポーネントによって許可されている選択肢のサブセットである場合には、*部分的に*完成された選択操作が有効である。同様に、許可された値で満足される割付操作がベースとなる機能コンポーネントに関し有効な割付の操作である場合も、*部分的に*完成された割付操作が有効である。何らかの理由でこれらの条件が満足されない場合には、別の割付、または選択操作を定義した拡張機能コンポーネント要件を実行することになる。

割付と選択の操作を完成させることは、直接的で合理的である。割付操作の場合は、単純に、パラメタが明確に特定していることを確認する必要がある。選択操作の場合は、単純に、TOE のセキュリティ対策方針の考慮事項をベースにした適切な項目を選択する必要がある。ただし、迷いが生じた場合には、ISO/IEC 15408-2 の附属書で提供されているガイダンスを参照すべきである。

割付、または選択操作が PP の段階で実施される場合は、それについて触れている箇所をハイライトしなければならない(これは、読者や ISO/IEC 15408 に対する適合性を確認する PP の評価者の役に立つ)。ハイライトの一般的な方法は、イタリック体を用いることだが、太字体や別のフォントセットを利用することもできる。

例えば、FMT_SAE.1.1.は、次のように表示することができる:

*TSF は、**利用者のパスワード**に対する有効期限の時間を特定する能力を、**許可された管理者**に制限しなければならない。*

この場合、要件の文章は既にイタリック体になっているため、ハイライトには太字体が用いられている。

操作が未完状態の場合は、ST の作者がこれを完成させなければならない。

未完の(または、部分的に完成した)操作の場合は、対応する ST の作者が、(例えば、注釈などの形で)適宜、どのようにして操作を完成させるかの説明をすべきである。これは、操作の 内容を明記することによって、ST の作者の義務/責任を明らかにするのに役に立つ。例えば、FDP_RIP.1.1.は、PP では、次のように記述することができる:

*TSF は、[割付:**ST の作者によって指定されたオブジェクトのリスト**]のオブジェクト**への資源の割り当て**において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。*

PP に含まれるそれぞれの SFR では、SFR を表現するための機能コンポーネントに含まれる割付、または選択操作が完成しているかどうかを判断する必要がある。ST では、すべての割付、及び選択操作が完成している必要がある。

#### 12.3.3.4. 詳細化

PP、または ST に含まれるそれぞれの SFR では、SFR に詳細化が指定されているかどうかを判断する必要がある。

詳細化操作は、いずれの機能コンポーネントの中の要件についても実施することができ、容認可能な実装のセットをより厳格にすることで、新たな要件を課していない SFR に技術的な内容を追加的に明記することができる。詳細化操作は、詳細化された要件が、詳細化前の要件にも適合することを意味している場合に、有効である。詳細化操作は、次のような場合に適切である:

a) PP が、対応する ISO/IEC 15408-2 のコンポーネントには含まれていない組織の方針情報など、追加の技術的な詳細を保有する組織によって記述される場合。

b) 選択された機能コンポーネントが、詳細化操作を行わないと、(例えば相互運用性の根拠が意味を為さなくなるなど)検討中の TOE のタイプとの矛盾や、不適切な点がある実装を許可してしまう場合。

c) SFR の可読性を向上させることができる場合。

割付と選択操作では、読者(と特に PP の評価者)が容易に理解することができるように、詳細化した要件の文章をハイライトしておくことを推奨する。

(FMT_MTD.3.1.を)詳細化した例が以下である:

*TSF は、TSF データとしてセキュアな値だけが受け入れられることを保証しなければならない。****詳細化:TSF は、TOE によって実行される最小のパスワード長が、最低でも 6 文字の値で構成されることを保証しなければならない。***

### 12.3.4. 監査要件はどのように特定すべきか?

PP、または ST に監査要件(すなわち、FAU_GEN.1 をベースにした要件)が含まれる場合、ISO/IEC 15408 では、監査対象の最小限のイベントのセットと記録しなければならない最小限の情報が要求されており、PP、または ST に記載されている他のすべての機能要件を検討する際にも特定されている必要がある。

この選択は、次の項目を含む条件の数によって決定する:

a) OSP で定義されている、セキュリティ監査に関するセキュリティ方針の要件。

b) セキュリティ対策方針の達成に関する監査の重要性。

c) セキュリティ対策方針に対する潜在的なイベントとその特性との関連性。

d) 費用/利益分析。

例えば、TOE が悪意のある利用者やハッカーのアクションに対する保護を目的としており、PP、または ST にそれに関連の SFR が含まれる場合、ログイン、またはアクセス制御の侵害に関連するイベントには、監査対象として必要になることが多い。ただし、管理者への信頼性が前提条件として記述されている、管理機能に関連のイベントについては、管理者がどの程度信頼されている(またはどの程度信頼すべき)かによって、監査の必要がない場合がある。

費用/利益分析では、次のような課題が残されることがある:

a) 情報収集は、(コスト)パフォーマンスにプラスの影響をもたらすか?

b) 情報が収集された場合、管理者は、データを効果的に分析するに足るリソース(例えば、ツールサポート)を得ることができるか?

c) 収集されたデータの管理、または構築に係るコストにはどのようなものがあるか?

ISO/IEC 15408 では、*最小*、*基本*、または*詳細として*監査要件の 3 つのレベルが、あらかじめ定義されている(ISO/IEC 15408-2 の 2.1.2.5.を参照)。ISO/IEC 15408-2 では、それぞれのレベルごとに、PP、または ST (ISO/IEC 15408-2 の附属書 C.2 も参照)に含まれている機能コンポーネントに基づき、記録すべき最小限の情報と共にどのイベントが(最小限の)監査対象となるかが記述されている。この 3 つのレベルは、次のように大別することができる。

a) *最小*レベルでは、通常、監査対象となる所定の機能コンポーネントについて定義されている一部の操作、またはイベントのサブセットのみが要求される。このサブセットは、もっとも関心を引くイベントや重要な種類のイベントとして定義されているのが一般的である。

b) *基本*レベルでは、例えば、ログインの成功/失敗など、通常、監査対象となる所定の機能コンポーネントについて定義されているすべての操作、またはイベントが要求される。

c) *詳述*レベルでは、通常、記録すべき関心のある追加すべき情報を要求する点が、*基本*レベルと異なっている。このレベルでは、生成された監査データの量が僅かであると予想される場合に限り、適切である可能性が高く、そうでない場合は、高度な監査分析ツールや侵入検知装置による分析の対象となる。

これらのレベルに当てはまるものがない場合は、FAU_GEN.1.1.で明示的に要求されている監査対象のすべてのイベントをリストにまとめ、「*指定なし*」を選択すべきである。例えば、ガイダンスには最小レベルを用いるが、FDP_ACF.1 が、PP、または ST に含まれているなど、別の操作やイベントのサブセットが、セキュリティ対策方針よりも関連性が高い場合には、特定的な事例として最小の要件の選択はせずに、(ISO/IEC 15408-2 の最小レベルで要求されている)成功した試みよりも不成功に終わったアクセスの試みを監査対象とすることを考慮することができる。

それぞれの機能コンポーネントを検討する替わりに、監査対象のイベントのリストを完成させる必要がある。あらかじめ定義されたレベルが*最小*、*基本*、または*詳細*レベルの場合には、*監査*項目に含まれるコンポーネントのファミリごとに、こういったレベルが特定される。FAU_GEN.1.1.と FAU_GEN.1.2.で適宜、参照することができるように、記録すべきイベントと(適宜)追加的な情報を識別するための表の作成を推奨する。

### 12.3.5. 管理要件はどのように特定すべきか？

ISO/IEC 15408-2 では、コンポーネント用に考慮すべき管理アクティビティのリストを、各コンポーネントのファミリごとに管理項目として特定している。これには、FMT クラス(セキュリティ管理)のクラスから特定のコンポーネントを含める必要性も提案している。ただし、この項目は、*参考情報*にとどめておくのが重要である。したがって、(むろん、ISO/IEC 15408-2 の依存性の項で明確に示されていない場合)PP、または ST の特別な管理コンポーネントに含めることを判断するための理由は必要ない。

一般的に、管理アクティビティは、機能コンポーネントが参照すべき、管理や制御が必要な、構成対象の TSF データが存在する箇所で特定される。例えば、TOE のセキュリティ対策方針では、こういったデータを修正する機能が、TOE の管理者によって制限されていない場合、TOE がこの機能を無効化していることがある。したがって、FMT のコンポーネントは、TOE のセキュリティ対策方針と適合していることを確認し、SFR 全体が相互に参照されるように、SFR 支援を定義するために含まれることが多い。

管理アクティビティは、TOE の機能性モデルから導出することができる。一般的に、必要であると考えられる管理アクティビティには:

- 利用者の登録、または登録の解除。
- オブジェクトの作成。
- 利用者、オブジェクト、セッションなどのセキュリティ属性の修正。
- セキュリティ機能の動作に関する変更(TOE 機能のすべて、または一部の開始/停止を含む)。
- 監査用パラメタの修正。
- セキュリティ関連の(例えば、メンテナンスモードの変更など)TSF の内部状態の変数値の変更。

このクラスから機能コンポーネントを選択する場合は、ISO/IEC 15408-2 の附属書 H で提供されている FMT クラスのガイダンスを参照すべきである。

### 12.3.6. PP の中からどのように SFR を特定すべきか？

ST が 1 つ以上の PP との適合性を主張する箇所では、PP によって SFR が完全に、またはほぼ全面的に指定されていることが多い。このような場合、ST の作者は、（要件の文章がすべて 1 箇所にまとまっているかを確認するために）PP の機能要件をすべて指定するか、PP を単純に参照し、さらに PP とは異なる SFR を指定するかを決定しなければならない。

後者の場合は、ST を簡略化することができるが、読者は PP と ST 双方について全体的なイメージを把握することが必要である。ST の読者は、SFR よりも IT のセキュリティ機能のほうにより関心を寄せていることが多い。これには、（設計、テスト文書、ガイダンス文書といった評価証拠の内容が、SFR よりも TOE 要約仕様での IT セキュリティ機能に関連付けしやすいことが多いため）TOE の評価者も含まれる。ST で SFR を指定することの主な目的は、ISO/IEC 15408-2 で定義されているように、対象となる PP と SFR の追跡可能性の実証を可能とすることである。ST のセキュリティ機能の仕様に両者を指定する際には、読者が混乱しないように PP を参照することによって省略された SFR のステートメントを付録で説明するという方法もある。

ただし、PP に含まれている SFR の中には、（割付、または選択操作など）ST の作者に委ねられている操作がある。このような場合には、適切な文字設定（例えば、イタリック体を用いるなど）で完成された操作を強調するなどして、すべての SFR を指定するよう推奨する。必要な説明があれば、それも同様の文字設定で追加すべきである。これは ST の読者（及び、特に ST の評価者）がどの操作が、どんな方法で実装されているかを容易に確認できるようにするためのものである。また、ST の根拠の構築も容易になる。

### 12.3.7. PP に含まれていない SFR はどのように特定すべきか？

時に PP に対応していない箇所を、ST の SFR として指定する必要が生じる場合がある。こういった対応が必要になる箇所は：

a) TOE との適合性を主張する、適切な PP が存在しない場合。

b) スポンサーが、PP で要求される機能要件、または保証要件から追加することによって、発生すると思われる追加的な費用に見合うだけの十分な利益が得られると考える場合。

場合によっては、SFR を指定する方法が、前項で説明したものと同じになることがある。SFR が、PP が必要なものに追加される箇所では、ST の作者は、追加された SFR が PP で記述した SFR と矛盾しないことを確認しなければならない（ST の根拠では、こういった矛盾が生じないことを証明する必要がある）。

### 12.3.8. ISO/IEC 15408 の Part2 に含まれていない SFR はどのように特定すべきか？

ISO/IEC 15408 では、PP、または ST の作者が、機能要件に含めたいと思う適切な機能コンポーネントが ISO/IEC 15408-2 で定義されていない場合、最終的な SFR を表示するためのモデルとして Part2 のコンポーネントの利用を要求している。

これには、ISO/IEC 15408-2 に精通していることが必要となるため、ISO/IEC 15408-2 に利用することができる適切な機能要件があるかどうかを判断するのは困難である。したがって、ISO/IEC 15408 の中に、一般的な SFR を示す適切な機能コンポーネントを特定するには、ガイダンスの第 12.3.2.項を参照することを推奨する。目的とする SFR は、詳細化操作を適切に適用したり、許可された割付や、選択操作によって取得できたりするケースが大半である。ただし、不必要な SFR によって、SFR の本来の意味合いや意図することが読者に伝わらなかったり、（不適切なコンポーネントを用いることによって）論争に発展するような不適切な依存性を導入したりしないためにも、機能コンポーネントに、SFR を単純に「押し込む」ことを試みないことを進言する。

拡張コンポーネントを適切に定義するためのガイダンスは、第 11 章で提供している。

### 12.3.9. SFR はどのように提示すべきか？

ISO/IEC 15408 の要件への適合が明確な SFR を記述することは、(むろん)PP や ST の作者*のみの*目的ではない。セキュリティ要件がどのような意味を持つかを一般の読者が理解し易いように、最適な SFR を提供し、表現する方法についても考慮すべきである。ISO/IEC 15408 への適合性を理解していなくても、可読性を高める方法はいくらでもある。

まず PP、または ST の適切な表題ごとに SFR をグループ化する。ISO/IEC 15408-2 で用いられているクラス、ファミリ、またはコンポーネントの表題を無理やり採用しようと考える必要はない。

次に、PP、または ST で SFR にラベルを付すために、ISO/IEC 15408-2 で用いられている機能エレメントのラベリング方式を無理やり採用しようと考える必要はない。スポンサー自身が、より意味のあるラベリングを目指すことができるように、独自のラベリングシステムを採用してもまったく差し支えないが、SFR と ISO/IEC 15408-2 の機能コンポーネントとの対応付けを(例えば、付録などで)証明しなければならない。実際、こういった方法は、複数回呼び出しされる機能コンポーネントを含む PP、または ST で記述されていることが多い。これは、SFR に一意的なラベルが付されないための別な方法がないためである。SFR に適切さを欠いた一意的なラベリングが付された場合には、セキュリティ要件の根拠を構築する際に重大な問題が生じる。

第 3 に、詳細化操作を慎重に扱うことによって、一般的な用語(セキュリティ属性など)を TOE 種別、または目的としているセキュリティ機能に関連するより具体的な用語に置き換えたりすることで、SFR の可読性を向上させることができる。FMT_MSA.3.1.をベースにした次の SFR がその例である:

*TSF は、**オブジェクトのアクセス権**に対して**制限的な**デフォルトの値を与える、**DAC 方針**を実施しなければならない。*

この例では、一般的な用語である「SFP を実施するために使われるセキュリティ属性」を方針に特化した「オブジェクトのアクセス権」と置き換えるために、詳細化操作が用いられている。

こういった詳細化操作を用いた場合は、(PP、または ST の評価を支援するために)PP、または ST の根拠でその旨をハイライトし、明確に説明すべきである。

### 12.3.10. セキュリティ要件根拠を作成する方法

ST、または PP が低保証(これについては、第 15.1 章で詳しく説明している)のものでない限り、セキュリティ対策方針が SFR とどのように適合しているかを説明する根拠が要求される。この根拠を作成するには、オブジェクトを扱うべき SFR に対応するすべてのセキュリティ対策方針を追跡する必要がある。この追跡では、それぞれの SFR が最低でも 1 つのセキュリティ対策方針を参照しており、それぞれのセキュリティ対策方針が最低でも 1 つの SFR を追跡していることを示す必要がある。

多くは、1 つのセキュリティ対策方針が 1 つ以上の SFR を追跡し、1 つの SFR が 1 つ以上のセキュリティ対策方針と対応していることが多い。大半の ST と PP では、セキュリティ対策方針は SFR に比べると一般的であるという点で、SFR の数のほうが、セキュリティ対策方針の数よりも多い。セキュリティ対策方針の例には:

*TOE は、それぞれの利用者が一意的に識別されており、その利用者が TOE 設備へのアクセスを許可される前に主張されている識別情報が認証されていることを保証する。*

上述のようなセキュリティ対策方針には、具体的には次のような SFR が対応していることが多い:

- 利用者を認識する方法。
- 利用者を認証する方法。
- 認証が失敗するとどうなるか？
- 利用者とその認証データを作成し、管理する方法。
- 利用者をサブジェクトと関連付ける方法。

単純にセキュリティ対策方針が SFR と対応していることを追跡するよりも、SFR のセットが、追跡されるセキュリティ対策方針がその目的を完全に満足させていることを証明することがより重要である。例えば、こういった証明を導出するのは容易かも知れないが、それがすべてのセキュリティ対策方針に当てはまるわけではない。特に、セキュリティ対策方針で TOE のセキュリティ特性の仕様を定めている場合は、そのセキュリティ対策方針を包括的に扱う SFR を証明するのは並大抵のことではない。セキュリティ対策方針の例には：

*TOE は、特定のセキュリティラベルにあるサブジェクトの操作から、階層的に低位のセキュリティラベル、または互換性のないセキュリティラベルにあるサブジェクトの操作へ情報が流れていないことを保証しなければならない。*

ラティスに基づく必須アクセス制御方針に対して、SFR が完全にセキュリティ対策方針に対応していることを証明するのは困難である。したがって、例えば、情報フロー制御に対してサポートを提供するアーキテクチャなど補足的な SFR を追加することはできるが、それでも SFR のセットが、セキュリティ対策方針に完全に対応していることを証明するのは不可能である。上の例では、すべての SFR が適切に実装されていても、隠れチャネルが存在し、セキュリティ対策方針に違反する方法で情報フローが許可されることがある。セキュリティ要件根拠の一部として提供される、完全であることを示す証明では、これを認識し、SFR のセットによって構成される TOE のモデルでは、例えば、セキュリティ対策方針に相反する SFR が存在しないという証明を提供するなど、セキュリティ対策方針に完全に対応していることを示すべきである。

通常、セキュリティ対策方針がセキュリティ特性よりもセキュリティ機能を表現しており、SFR と同程度の詳述さで記述されている場合、セキュリティ対策方針や SFR の追跡、及び完全性の証明は容易である。したがって、この時点でセキュリティ対策方針は、できる限り明確さを期すべきである。ST や PP を記述する際は、セキュリティ対策方針を再考し、万が一の場合に備えてセキュリティ対策方針が SFR に対応していること、または SFR がセキュリティ対策方針に完全に対応しているという証明ができるよう、より正確さを期すのが賢明である。

## 12.4. PP、または ST で保証要件を特定する方法

### 12.4.1. SAR はどのように選択すべきか？

保証要件を選択する場合は、次のような項目を含め、その他の要素とのバランスを取る必要がある：

a) 保護すべき資産の価値とこれらの資産を脅かす恐れのあるリスク。

b) 技術的な可能性。

c) 開発や評価に発生し得る費用。

d) TOE の開発や評価に必要なタイムスケール。

e) （製品の場合）市場で必要と思われること。

f) 保証コンポーネントの中で、機能コンポーネントの依存性として認識されているもの。

保護の対象となる資産の価値とこれらの資産に対するリスクが大きくなるほど、これらの資産を保護するために用いられるセキュリティ機能には、より高位なレベルの保証が要求される。これは、セキュリティ対策方針の記述に反映させるべきである。組織は、自身の資産に対するリスクが容認できるレベルまで低減させるために必要な保証レベルを決定するために方針や規則を定めることができる。言い換えれば、製品に必要なレベルの保証は、組織の中で定めることができるということである。

費用やタイムスケールなどその他の要素は、実際に達成することができる保証レベルに制限を加える要素としての役割を果たす傾向がある。b)の技術的な可能性とは、特定の保証コンポーネントが要求する証拠の生成が実践的ではないと考えられる場合の判断基準となる。これは、すなわち高位の保証レベルが要求される、または設計文書が利用できない旧式のシステムとの関連性が高いことがあるが、容認されているタイムスケールの範囲内で、準形式的な、あるいは形式的な証拠を生成するのは技術的に不可能である。達成できそうな保証要件の中に実践的な制約事項が盛り込まれている場合は常に、達成できそうな最大の保証要件を理想的な保証要件に優先し容認する必要がある。こういったリスクを容認することは、繰り返しになるが、セキュリティ対策方針の文書に反映させるべきである。

セキュリティ対策方針の文書では、SAR に含めるべき特定の保証要件の必要性も示すことができる。例えば:

a) TOE のセキュリティ対策方針では、TOE が、高い攻撃力を持つ攻撃者に対する抵抗力を保持すべきであることを記述することができる。この場合、こういった抵抗力の実証を要求する AVA_VAN.5 を含めるための明確な指針となる。

b) セキュリティ対策方針では、自己保護、ドメイン分離、または非バイパス性を考慮事項として示すことができる。この場合は、ADV_ARC.1 コンポーネントに含める必要がある。ADV_ARC クラスにはコンポーネントが 1 つしかないが、アーキテクチャ記述レベルの説明は、ADV_TDS クラスから選択されたコンポーネントに依存していることに留意する。

c) セキュリティ対策方針では、TOE のセキュリティが、開発環境のセキュリティに大きく依存している点に注意することができる。この場合、SAR には、開発環境のセキュリティが保証されるように ALC_DVS ファミリを含めることを強く推奨する。

SAR の選択は、ISO/IEC 15408 の EAL といった、適切な保証パッケージを単純に選択するといった比較的直接的な方法である。保証パッケージの定義や説明については、そのパッケージに所定のセキュリティ対策方針の文書(例えば、EAL の場合は、ISO/IEC 15408-3 の第 6 章を参照)が適切に含まれるように、ISO/IEC 15408 の EAL の項を参考にすべきである。保証パッケージでは、必要な保証のレベルが広範囲に提供されているが、セキュリティ対策方針に対応する特定の分野を扱っているものは少ない。こういった場合には、セキュリティ対策方針が確実に満足されるように追加の保証要件(すなわち、パッケージに必須とされているものに追加される要件)を含めることが適切である。

追加の保証要件を特定した箇所では、PP、または ST の作者は、保証要件の依存性が、追加した要件に対して満足されることを保証しなければならない。例えば、PP、または ST の追加の保証要件が EAL3 に AVA_VAN.3 を追加する場合、EAL3 に含まれていない ADV_TDS.3 や ADV_IMP.1 も保証要件に追加すべきである。ADV_TDS.3 には ADV_FSP.4 にという依存性保証要件があるため、ADV_FSP.4 も追加する必要がある。

### 12.4.2. SAR を実際に運用する方法

SAR では、次のような操作が可能である:

a) *繰返し*。同じ保証コンポーネントの複数回の利用を許可する。

b) *詳細化*。他の SAR に新たな依存性を導入せずに、保証要件に詳述な説明の追加を許可する。

c) *割付*。SAR の要素に割付用のパラメタを用いた値の割付を許可する。

実際は、繰返し操作は、TOE の別な部分で、同じ保証コンポーネントに異なった詳細化を適用する必要がある場合、または PP、または ST で、統合 TOE の別な部分で異なった保証要件のセットを指定する必要のある場合に限り用いられる(第 14.1 章を参照)。後者の場合、(詳細化されている、いないに関わらず)1 つ以上の部分で構成された TOE に適用される保証要件には、繰返し操作が必要である。

SAR における詳細化操作は、次のように用いられる:

a) 具体的な開発用ツール、方法、ライフサイクルモデル、分析技術、表現方法、特定の基準への適合などの利用を義務付けることによって開発者アクションを制限する。

b) 評価者アクションを、例えば、次のような項目を実施することによって制限する:

   — ADV_IMP.1 の場合、TOE の実装表現を示す部分が検査されたサブセットに含まれるべきかを特定する。

   — AVA_VAN.1 の場合、TOE の内容に関連する脆弱性は、公共の情報源から説明されるのが一般的であるため、考慮する必要のある公共の情報源の最小限のセットを特定する。

割付操作が許可されている ISO/IEC 15408-3 の SAR のリストには、ADV_INT.1.1D と ADV_SPM.1.1.D の 2 通りの事例しか存在しない。1 番目のクラスの場合、PP、または ST の作者は、TSF のサブセットに適用される割付操作を定義する必要がある。2 番目のクラスの場合、PP、または ST の作者は、形式的にモデル化された方針のリス

トに用いられる割付操作を定義する必要がある。

### 12.4.3. ISO/IEC 15408 Part3 に含まれていない SAR は PP/ST でどのように特定すべきか？

ISO/IEC 15408 では、PP、または ST の作者が ISO/IEC 15408-3 で定義している保証コンポーネントの中に適切なものがない場合は、拡張 SAR を含めることを要求しており、拡張 SAR を含めた結果は、ISO/IEC 15408-3 のコンポーネントを用いた提示モデルとして明記すべきである。第 11 章では、PP、または ST の中でこういった拡大保証コンポーネントを定義するためのガイダンスを提供している。

### 12.4.4. SAR 根拠

PP と ST の構造では（第 15.1 章でも説明したように、低保証でない限りは）、SAR のセットが選択された根拠も必要である。図 3 の SAR では、SPD、またはセキュリティ対策方針から導出することは要求されていないため、他のソースから導出することもできる。したがって,ISO/IEC 15408-1 では、SAR が導出された方法の説明や特定の SAR のセットを要求する具体的な規則を指摘しなくてもかまわない。

脅威エージェントによってもたらされた攻撃に対する抵抗力を想定し、TOE の SAR を選択することを目的としてセキュリティ課題定義の中で識別された脅威や脅威エージェントをベースにして導出された SAR は、SPD に含まれることが多い。このような場合には、SAR を選択した根拠として、SPD を表現すべきである。

## 13. TOE 要約仕様

TOE 要約仕様は、ST で要求されるが、PP では必要ない。したがって、この章は、ST のみに適用される。

TOE 要約仕様の目的は、一般の消費者に、TOE のセキュリティ機能がどのように SFR に適合するかについての説明を提供することである。したがって、TOE 要約仕様では、TOE が提供することができる全体的な機能性の中からセキュリティに関する機能と TOE アーキテクチャについて説明すると共に、TOE の全体像を十分に捉え、TOE が SFR を実装する方法を提供すべきである。

したがって、TOE 要約仕様では、TOE のアーキテクチャと一般的な機能性に含まれる SFR で定義されるサブジェクト、オブジェクト、セキュリティ属性や規則がなど全体的な TOE のセキュリティを中心とした概要的なモデルとして説明する。このモデルは、TOE が実装するセキュリティ機能と関連性のない機能がある限り、TOE が提供するセキュリティ以外の機能性の大半は、概要的な機能のままである。TOE 要約仕様で提供される詳述さのレベルは、TOE 記述よりも詳しくなければならず、どのように SFR に適合するかについても重点が置かれる。TOE 要約仕様で説明したセキュリティ機能が SFR に適合する方法を示す対応付けが必要である。

TOE 要約仕様を構築するには、TSF の境界を含め TOE アーキテクチャの概要を提供する TOE の全体像から着手するのが適切である。この方法は、ASE_TSS.2 への適合性が要求されていなくても、TSF が自身をタンパリングやバイパスから保護する方法を説明する場合にも有効である。次に SFR を導出するために用いた機能性のモデルをベースにしてセキュリティ機能を説明すべきである。これは、TOE 要約仕様を記述すると同時に SFR をクラスごとに説明することで、導出されたそれぞれの SFR が機能性モデルと適合し、それによって TOE 要約仕様で記述されているセキュリティ機能と SFR への対応付けをするための適切な実践方法である。TOE 要約仕様には（第 12.2 章のガイダンスを用いて導出されるように）、基本的に、TOE のすべての機能とそのアーキテクチャを全体的な TOE に組み込むことによって実行される機能性モデルが含まれるべきである。これによって読者は、特定の機能要件、またはセキュリティ機能の詳細が選択された理由と、それら（特定の機能要件やセキュリティ機能の詳細）が TOE の全体的な機能とどのように対応しているかについても理解することができる。SFR と TOE 要約仕様の双方は、同じモデルから導出されているため、SFR への TOE 要約仕様の対応付けの追加は自動的に提供される。

統合 TOE の場合、その要約仕様では、個々のコンポーネントが SFR を定めるために、どのように相互に関連があるかを説明する必要がある。この説明によって読者は、統合 TOE の SFR とコンポーネントの SFR を対応付ける方法とこれらの SFR が相互運用される方法を理解することができる。統合 TOE の ST の詳細なガイダンスに付いては、第 14.1 を参照のこと。

# 14. 統合 TOE とコンポーネント TOE の PP/ST を特定する方法

## 14.1. 統合 TOE

TOE の運用環境では、大半の TOE が他の IT 製品やシステムと相互作用する。こういった TOE は、SFR を満足させる IT 製品やシステムによるサポートが必要な場合が多い。この簡単な例が、下位層のオペレーティングシステムをベースにしたファイルの保護、アドレス空間の分割や利用者認証機能に依存するデータベースシステムの TOE である。もう 1 つの例は、認証用にデジタル認証や証明書失効リストを保存する外部の LDAP サーバに依存するオペレーティングシステムである。このオペレーティングシステムは、こういったデジタル認証や証明書失効リストを生成し、LDAP サーバを通じて時機的な方法でこれらを公開する外部の PKI（システム）にも依存している。この 2 つの例を組み合わせて、（利用者を認証する場合、実際に TOE が依存するのはオペレーティングシステムであっても）データベース管理システムも、利用者の認証時には LDAP サーバと PKI システムに依存することになる。また、この例は、利用者の認証手続きの中で用いられるスマートカードにも簡単に応用することができる。この場合、上の例のような TOE との依存関係はスマートカード上に存在するが、スマートカードを個別化するシステム上にも存在する。

これらの例は、一見したところ単純な SFR（この場合は、利用者認証）が、個別に評価することができる多くの IT 製品による正しくセキュアな協調を必要とすることを示すものである。本章では、TOE の SFR を定める際に生ずる問題点との関連で、IT 製品を組み合わせることによって満足される SFR の問題点を扱うための TOE 環境のセキュリティ対策方針について説明する。

上述の例には、次のような依存性が確認できる：

- データベースの管理システムは、利用者認証、ファイルの保護やアドレス空間の分割に依存している。
- オペレーティングシステムは、アドレス空間の分割や、特権が付与されていないプログラムに付加されている I/O デバイスやプロセッサ専用構成レジスタによる直接的なアクセスから保護するハードウェアに依存している。
- オペレーティングシステムは、利用者認証に用いられる情報を不正なアクセスから保護する LDAP サーバに依存している。また、このシステムでは、LDAP サーバが、リクエストに応じて時機的な方法で情報を提供する場合にも、LDAP サーバとオペレーティングシステムとの間で転送される情報が検知できない方法で改ざんされないように保護している。
- オペレーティングシステムは、認証に関連のある利用者の適切な情報に基づいてデジタル認証を生成し、（LDAP サーバ上の証明書と証明書失効リストの時機的な公開も含め）これらの認証を適切に管理するために、PKI（システム）に依存している。
- オペレーティングシステムは、利用者のプライベート鍵を保護し、正しい認証情報（例えば、PIN）を受信したのちにその鍵のみを用いることができるスマートカードに依存している。
- スマートカードは、利用者が PIN を入力してから、スマートカードに転送され、オペレーティングシステムのメモリから PIN が安全に消去されるまで、利用者の PIN を保護するためにオペレーティングシステムに依存している。スマートカードは、例えば、許可されていない利用者が PIN を入力した場合など、PIN が悪用されないようにオペレーティングシステムに依存している。

これらは単に、PP、または ST で上述の例にあった依存性をどのように対処することができるかを示すリストとして用いたに過ぎない。

依存性を特定するための簡単な方法が以下である：

- データベースが、自身にセキュリティ機能を提供するために、オペレーティングシステムに依存している。
- オペレーティングシステムが、ハードウェアに依存している。
- オペレーティングシステムが、LDAP サーバに依存している。
- オペレーティングシステムが、PKI システムに依存している。
- オペレーティングシステムが、スマートカードに依存している。
- スマートカードが、オペレーティングシステムに依存している。

1 つのコンポーネントが、別のコンポーネントに依存している場合、ISO/IEC 15408 では、前者は「依存コンポーネント」、後者は「基本コンポーネント」と呼ぶ。データベースとオペレーティングシステムを組み合わせた上述の例では、データベースが依存コンポーネントであり、オペレーティングシステムが基本コンポーネントに当たる。同様に、オペレーティングシステムとハードウェアの組み合わせでは、オペレーティングシステムが依存コンポーネントであり、ハードウェアが基本コンポーネントである。スマートカードとオペレーティングシステムの場合は、双方のコンポーネントが相互に依存しているため、双方が依存コンポーネントと基本コンポーネントである。

依存コンポーネント用に ST、または PP を作成する場合は、基本コンポーネントに依存する依存コンポーネントは、前提条件とこれらの前提条件から導出される運用環境のセキュリティ対策方針として扱われなければならない。DBMS を例にした前提条件は、次のようなものである:

- *前提条件 1*
  *運用環境は、DBMS として同じシステム上で実行される他のアプリケーションソフトウェアによる DBMS ソフトウェアへの妨害や改ざんから保護する。*
- *前提条件 2*
  *運用環境は、DBMS の利用者データや TSF データの保存に用いられるファイルを不正なアクセスから保護する。*
- *前提条件 3*
  *運用環境は、個々の利用者を識別、及び認証し、DBMS によるリクエストの中から、DBMS が消費者の識別情報を取得する方法を提供する。*

こういった前提条件は、運用環境の一部としてオペレーティングシステムにとって非常に明確な対策方針を特定するために用いることができる。こういった対策方針の詳述さのレベルは、DBMS に対する要求がどの程度具体的かによって大きく左右される。例えば、監査が DBMS の SFR の場合、DBMS が依存するオペレーティングシステムのセキュリティ機能をバイパス、または改ざんさせる試みを検知するためにオペレーティングシステムの中からある程度の監査レベルを要求することも役に立つことがある。上述のような前提条件から導出されるセキュリティ対策方針の例には、次のようなものがある:

- *オペレーティングシステムは、そのシステムの制御下で実行される他のアプリケーションプログラムによる妨害や改ざんから自身の実行ドメインを保護するために、そのドメインの中で DBMS に実行を許可するメカニズムを提供しなければならない。*
- *オペレーティングシステムは、DBMS に属す実行型プログラムを不正なアクセスから保護しなければならない。*
- *オペレーティングシステムは、DBMS のソフトウェアに完全性を侵害する脅威や攻撃を検知するメカニズムを提供し、修正することができない完全性の侵害が検知された場合には DBMS の実行を禁止しなければならない。*
- *オペレーティングシステムは、少なくても読み取りと書き込み/更新用のアクセスの違いを認識するファイルに、アクセス制御メカニズムを提供し、個々の利用者に合わせた詳述さで(「アクセスなし」の場合も含め)それぞれのアクセスレベルの定義を許可しなければならない。*
- *オペレーティングシステムは、個々の利用者、または所定の利用者グループのファイルへのアクセス権の管理の制限を許可しなければならない。*
- *オペレーティングシステムは、DBMS の機能を呼び出す前に、個々の利用者を識別、及び認証しなければならない。*
- *オペレーティングシステムは、利用者を誤認証する確率が 1,000,000 分の 1 以下で認証する保護メカニズムを用いなければならない。*
- *オペレーティングシステムは、監査記録に利用者の識別情報や認証を試みた際の日時が含む認証試行の成功、または失敗を監査する機能を備えていなければならない。*
- *オペレーティングシステムは、呼び出されたデータベースの機能の代わりに DBMS が利用者の識別情報を適切に取得することができるインタフェースを提供しなければならない。*

ISO/IEC 15408-2 で示されているように、セキュリティ対策方針の大半は、SFR との対応付けが容易であることがお判りいただけたことだろう。1 番目のセキュリティ対策方針だけは、ドメイン分離の構造的な特性を扱っているという点が他と異なっている。セキュリティアーキテクチャに関する文書では、この特性がオペレーティングシステムでどのように実装されるかを説明する必要がある。セキュリティアーキテクチャに関する文書は、保証レベルが EAL2 以上の TOE には必須である。

前述の例のように、DBMS が依存コンポーネントでオペレーティングシステムが基本コンポーネントの場合、オペレーティングシステムのセキュリティ対策方針は、SFR の詳細レベルに近い非常に高位な詳細レベルで定義することができ、可能な場合は、常に高位な詳細レベルを提供すべきである。

前提条件とそこから導出された運用環境のセキュリティ対策方針が、包括的でなければならない場合もある。オペレーティングシステムを依存コンポーネントとし、LDAP サーバを基本コンポーネントとした場合に、作成する必要がある前提条件の例を取り上げる:

— *運用環境は、利用者の認証にオペレーティングシステムが要求するデジタル認証と証明書失効リストを、不正な修正や不正な手段で証明書や証明書失効リストに追加する行為から保護しなければならない。*

この場合、ST、または PP は、この前提条件に別な方法で適合するために、この保護メカニズムの一部が動作しないようにしておくことができる。この前提条件から導出される運用環境のセキュリティ対策方針には:

— LDAP サーバは、オペレーティングシステムが利用者認証に用いる証明書や CRL(証明書失効リスト)への修正、及び/または追加を許可する前に、利用者を識別し、認証しなければならない。

— 運用環境は、LDAP サーバとオペレーティングシステムとの間でやり取りされるデータを、(追加や繰返しを含め)検知されない方法で改ざんされないように保護しなければならない。

運用環境のセキュリティ対策方針を達成するために、異なる方法で対策することを許容するために、運用環境のセキュリティ対策方針をどのように達成するべきかについてまでは特定しない。例えば、上記の 2 番目のセキュリティ対策方針については、暗号によって保護された通信プロトコルを用いて構築する、または物理的に保護されているネットワークによって構築する等によって、対策方針を達成させることができる。

依存コンポーネント用に ST、または PP を作成する場合は、基本コンポーネントが評価されており、その評価結果を依存コンポーネントの評価に利用することができる場合と基本コンポーネントが評価されていないか基本コンポーネントの評価結果を利用することができない場合には、その違いを区別しなければならない。

前者の場合、ISO/IEC 15408-3 には、評価済みのコンポーネント用に評価基準を定義する ACO 保証クラスが含まれる。統合 TOE の ST、または PP の作者は、ACO クラスの中から保証レベルに相応しいと思われるコンポーネントをその TOE に含めなければならない。これを裏付けるために、ISO/IEC 15408-3 では、統合 TOE の ST、または PP に含まれる 3 通りの「統合保証パッケージ」を定義している。こういったあらかじめ定義されているパッケージとは異なるコンポーネントを ACO クラスから選択する場合は、依存関係が満足されていることを確認しなければならない。

### 14.2. コンポーネント TOE

TOE の環境には、別の IT コンポーネントとの明確な依存性がない自己完成型の TOE があるが、これには当てはまらない TOE も数多く存在する。こういった TOE は、ST、または PP の中では「コンポーネント TOE」と見なされている。この一般的な例には:

— ソフトウェアのパッケージに明確なセキュリティ機能が提供されているが、これらの機能は、さまざまな数多くの製品に組み込むことを目的としている。このソフトウェアパッケージは、それが組み込まれた製品の TSF や TSF データを保護すると共に一部の TSF データを管理するためにその製品に依存する。

— アプリケーションが自身のオブジェクトのためにアクセス制御機能を実装しているが、そのアプリケーション環境によって提供される利用者の身分識別や認証にも依存している。

— アプリケーション、またはオペレーティングシステムが、暗号化の機能や暗号鍵の管理を提供する暗号化コプロセッサに依存している。

これらはすべて、1 つ以上のセキュリティ対策方針が TOE の SFR や TOE の環境と部分的にのみ対応していることを示す例である。したがって、TOE は、自身が対応することができないセキュリティ対策方針の一部を満足させる SFR をその環境に正しく実装する前提条件によってのみ評価することができる。

コンポーネント TOE の ST、または PP は、TOE 搭載型の製品とさほど大きな違いはない。唯一異なる点は、TOE のセキュリティ対策方針によって扱われ、満足させることが要求される IT 環境のセキュリティ対策方針は、その対策方針を満足させることを目的とする環境の IT 製品の種類についても（可能な場合は）非常に詳しく記述されていることが多いということである。第 14.1 章で説明しているオペレーティングシステムの ST の例は、満足されるべきセキュリティ対策方針が、ベースとなるハードウェア、LDAP サーバ、PKI システムやスマートカードごとに明確に定義されている。こういったセキュリティ対策方針は、コンポーネント TOE の ST で明記されているように、SFR と容易に対応付けができるように、できるだけ詳しく定義すべきである。この方法でコンポーネント TOE の集合を統合 TOE として評価する際にも対応付けを容易にすることができる。

# 15. 特別なケース

## 15.1.低保証 PP と低保証 ST

保証要件が EAL1 の保証レベルで定められているよりも低位の PP、または ST の場合、ISO/IEC 15408 では、PP、または ST を簡略化することを許可している。ST、または PP の場合、次のような項目を省略することができる:

- SPD。
- セキュリティ対策方針。
- セキュリティ対策方針根拠。
- ISO/IEC 15408 で定義されているセキュリティ要件の中で、依存性を満たさない理由を除去したセキュリティ要件根拠。

これは、低保証の製品を対象に、ST や PP を簡略化するための手段である。その他の項目については、既に説明したように、すべてを扱う必要がある。

低保証 ST、または低保証 PP の場合は、低保証 PP との適合を主張するのみでよいが、低保証以外の PP、または ST が、低保証 PP との適合性を主張することもある。こういった低保証以外の PP、または ST には、低保証以外の PP、または ST のすべての必須項目が含まれていなければならない。したがって、低保証以外の PP、または ST との適合性を主張する場合には、低保証 PP で割愛された項目も含めなければならない。

## 15.2.国内解釈への適合

PP や ST について、ISO/IEC 15408 で定めている要件のほかに、国が定める制度で PP や ST の評価に対応することができるように、ISO/IEC 15408 では、国内の個々の制度を、特定の国内解釈として定義してもよい。通常、こういった国内解釈は、国のスキームによって公開されるため、この基準によって評価を得たいと思う PP や ST の作者は、この解釈を利用する旨をその制度に伝えるべきである。

国内解釈に加え、認証の相互認証に合意している国々によって容認されている ISO/IEC 15408 の修正を含め、共有の解釈もある。こういった解釈は、PP や ST の作成時に考慮する必要があり、その作者が、ST、または PP の構造や内容に関して共有の解釈を得るために、この協定に参加しているスキームにその旨を伝えるように進言する。

## 15.3.機能パッケージと保証パッケージ

PP に加え、ISO/IEC 15408 では、機能パッケージと保証パッケージを定義することについても許可している。機能パッケージには、SFR のセットが含まれており、保証パッケージには、SAR のセットが含まれている。SFR と SAR の双方が混在するパッケージは許可されない。

こういったパッケージには、そのパッケージを識別し易くするために、名前を付すべきであり、有効、かつ効果的な要件のセットを含むべきである。例えば、監査に関連する角度以外からは捉えることのできない監査に関連の機能（監査対象のイベントの最小限のセット、監査証跡の保護、監査時確認要件、監査管理）を定義する機能パッケージがこの例である。こういった機能パッケージは、別な種類のセキュリティ製品（例えば、オペレーティングシステム、データベース管理システム、ファイアウォールシステムなど）用に再利用することができる。こういった機能パッケージや保証パッケージを定義する際は、そのパッケージに含まれている依存性を直接扱うか、パッケージを利用する際に、未決の依存性を対処する方法をアドバイスするのが賢明である。

# 16. 自動化ツールの利用

ISO/IEC 15408 の構造や PP/ST に必須の項目のために、PP や ST など ISO/IEC 15408 の主要な文書の作成や評価にどの程度まで自動化ツールを利用することができるか、という疑問がもたらされる。

こういったツールを利用しようとする場合の動機は、開発者が、PP や ST の内容に重点を置くことができ、評価用に PP/ST を提出しなければならないという重圧から解き放たれるばかりではなく、リソースを消費させるタスクの中でも、関連性と根拠の整理、機能の依存性のチェックなど、PP/ST の評価の中でも時間を要するが、あまり成果が現れない活動から評価者を解放する、など実に広範である。

「The CCToolBox」[9]のように PP/ST のセキュリティ課題を分析し、セキュリティ要件を導出することができるものや、その逆で、「PPhelper」[10]のように、TOE のセキュリティ特性から SPD を導出する方法など、PP/ST を作成する一般の利用者向けのツールを公開しようという動きがあった。いずれの方法も相関的なセキュリティ概念のデータベースによって対応されるものである。

こういった動きは、あまり良い成果がもたらされなかったため、現在では行われていない。

一般的に入手できるツールの中には、そのセキュリティ概念を始めて、一般利用者が利用できるようにしたことを裏付けたという方式をベースにした製品が登場している。

ISO/IEC 15408 の新たな制度や CC の XML フォーマットは、PP/ST 開発の自動化、開発者の製品開発用のライフサイクルやツールにも、新たな可能性を広げている。これらは、外部ツールや一般向けのツールに依存する必要がなく、TOE 専門の開発者も利用することができる。

評価証拠の作成時に、特に PP や ST を作成する際に、このツールはどの程度まで対応できるか、あるいは対応すべきだろうか？

この時点ではっきりと言えることは、まず、PP や ST を作成するために必要な知識や概念を習得することである。次に、自動化ツールを利用して、ISO/IEC 15408 の最新バージョンの中から抽出した文章をコピーし、内容や表現方法に関連の要件を自動化する、といった手順で PP や ST を容易に作成することができる。逆もまた真なりと、有効な PP や ST を提供する自動化ツールに望みを託すばかりでも、大抵はがっかりする結末に至るものである。

# 付録 A

## （参考）

## 拡張コンポーネントの定義の例

次の項では、TSF データの回復に関する要件を扱う拡張型セキュリティ機能コンポーネントの例を提供する。この例は、拡張コンポーネントの定義はもとより ST、または PP で定義すべきコンポーネントの根拠を定義し、組み立てる方法を示したものである。

### TSF データの回復（FPT_REC_EXT）

#### ファミリのふるまい

TSF データの回復は、定義された TSF データのチェックポイントを明らかにし、後に、このチェックポイントが設定された時間の、この TSF データに回復させることを許可する。この機能によって、例えば、管理者のエラー、ハードウェアの一部が破損した場合やソフトウェアに不具合が生じたことで変更されてしまった TSF データを元の状態に回復することができる。

#### コンポーネントのレベル付け

FPT_REC_EXT.1：基本的な TSF データの回復では、チェックポイントの設定と管理者の明確なアクションによってチェックポイントが設定された時点の TSF データへの回復を扱う必要がある。

FPT_REC_EXT.2：高度な TSF データの回復では、チェックポイントの設定と自動的な、あるいは管理者の明確なアクション活動のいずれかによって、チェックポイントが設定された時点の TSF データへの回復を扱う必要がある。

#### 管理：FPT_REC_EXT.1、FPT_REC_EXT.2

以下のアクションは FMT における管理機能と考えられる：

- チェックポイント、及び/または回復の開始を定義することを要求する特権の管理。
- チェックポイントが設定された時間に格納されたデータに含まれる TSF データの管理。

#### 監査：FPT_REC_EXT.1、FPT_REC_EXT.2

セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである：

- 最小：すべての成功回復操作。
- 基本：回復操作をしようとするすべての試み。
- 詳細：すべてのチェックポイントの操作、回復操作をしようとするすべての試み。

#### FPT_REC_EXT.1（基本的な TSF データの回復）

下位階層：なし

依存性：FMT_SMR.1 セキュリティの役割

FMT_MOF.1 セキュリティ機能のふるまいの管理

FPT_REC_EXT.1.1：TSF は、[割付：TSF データのリスト]用にチェックポイントを定義することを、[割付：役割のリスト]の役割の利用者に許可しなければならない。TSF は、後に、TSF データを回復することができる場所にチェックポイントを設定しなければならない。

FPT_REC_EXT.1.2：TSF は、チェックポイントが持つ値から TSF データを回復することを、[割付：役割のリスト]の役割の利用者に許可しなければならない。

FPT_REC_EXT.1.3：TSF は、TSF データの回復後、以下のアクション[割付：一貫性と完全性確認のためのアクションのリスト]を実行し、データの一貫性と完全性を保証しなければならない。

FPT_REC_EXT.1.4：TSF は、回復時に TSF データが一貫していないことや完全性に違反していることを検知した場合は、以下のアクション[割付：アクションのリスト]を実行しなければならない。

**FPT_REC_EXT.2（TSF データの自動回復）**

下位階層：FPT_REC_EXT.1

依存性：FMT_SMR.1 セキュリティの役割

FMT_MOF.1 セキュリティ機能のふるまいの管理

FPT_REC_EXT.2.1：TSF は、以下の条件[選択：[ [割付：条件のリスト]、[割付：その他の基準]] が満足された場合、管理者が定めた時間間隔で[割付：TSF データのリスト]のチェックポイントを定義しなければならない。TSF は、後に、TSF データを回復することができる場所にチェックポイントを設定しなければならない。

FPT_REC_EXT.2.2：TSF は、以下の条件[割付：条件のリスト]で設定したチェックポイントが持つ値から TSF データを回復しなければならない。

FPT_REC_EXT.2.3：TSF は、TSF データの回復後、以下のアクション[割付：一貫性と完全性確認のためのアクションのリスト]を実行し、データの一貫性と完全性を保証しなければならない。

FPT_REC_EXT.2.4：TSF は、回復時に TSF データが一貫していないことや完全性に違反していることを検知した場合は、以下のアクション[割付：アクションのリスト]を実行しなければならない。

FPT_REC_EXT.2.5：TSF は、TSF データの一貫性と完全性が保証された場合に限り、回復されたデータを利用することができる。

**拡張コンポーネントの定義の根拠**

ISO/IEC 15408-2 では、設定されたチェックポイントの時点に格納された TSF データを回復させるための SFR は定められていない。こういった回復機能は、TOE のセキュアな操作を確実に実行するために、重要である。機能要件は、定義された TSF データのが「チェックポイント」の操作の一部として「格納されて」いるという前提で定められており、後に、この TSF データは、格納された値に基づいて回復される。単純に TSF データのセットを回復しようとすると、結果として TSF が不適合（となり、潜在的にセキュリティが確保されない）の状態に陥ることが多い。格納された TSF データの完全性についても確保しなければならない。したがって、回復後の TSF 全体に一貫性やセキュリティが確保されており、回復された TSF データが改ざんされていないことを保証するために確認を行う必要がある。したがって、SFR では、TSF データの回復後と TOE による通常の操作を継続する前に一貫性と完全性を確認する仕様を許可している。

こういった一貫性の確認が失敗した場合、TOE が自動的に修正アクションを実行する、管理者権限を持つ利用者が手動で修正アクションを実行できるようにメンテナンスモードに移る、またはセキュリティが確保されていない TOE を制止するために別のアクションを実行する、などを判断することができる。FPT_REC_EXT.2 は、TSF の一貫性や完全性が保証されない限り、回復された TSF の利用を許可しない。

この SFR のコンポーネントは、ISO/IEC 15408 で定められている、セキュリティ機能コンポーネントの中の FPT クラスの拡張コンポーネントである。

# 参考文献

[1] *Common Criteria for Information Technology Security Evaluation (3 parts)*, Version 3.1, Common Criteria Management Board, 2007. Downloadable from http://www.commoncriteriaportal.org/ (link valid May 2008).

[2] *List of PPs*, Downloadable from http://www.commoncriteriaportal.org/ (link valid May 2008).

[3] *ISO/IEC 15292, Information Technology – Security Techniques – Protection Profile registration procedures*.

[4] *Software Reliability Measurement, Prediction and Application*, J. Musa, A. Lanino and K. Okumotu, MacGrow-Hill, 1987, ISBN: 9780070441194.

[5] *Software Risk Management: Principals and Practices*, B. W. Boehm, IEEE Software, January 1991.

[6] *Security Engineering Process*, J. D. Weiss, Proceedings of the 14th National Computer Security Conference, Washington D. C., USA, October 1991.

[7] *Secrets and Lies*, B. Schneier, John Wiley & Sons, 2000, ISBN: 9780471253112.

[8] *The Security Development Lifecycle*, M. Howard and S. Lipner, Microsoft Press, 2006, ISBN: 9780735622142.

[9] The CC Toolbox. Downloadable from http://www.cctoolbox.sparta.com/ (link valid May 2008).

[10] The PP Helper. Presented at the Third International Common Criteria Conference, Ottawa, Canada, 13 – 14 May 2002.

# 索引

U