IPA Information-technology Promotion Agency, Japan

ST作成講座

独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

- ST全体概要
  - STの位置付け
  - STの注意点
- STの構成要素
  - STの構成イメージ
  - 各章毎の概要、注意点
  - サンプルSTを用いた記述例の確認
- ST作成のポイント
  - ST作成時のポイント
  - Protection Profileに基づくST作成の流れ

ST全体概要

CC評価におけるSTの位置付け（1）

- 以下のことを実証するためのドキュメント
  - セキュリティ機能要件（SFR）が、セキュリティ対策方針を満たしていること
  - TOEのセキュリティ対策方針及び運用環境のセキュリティ対策方針が、脅威に対抗すること
  - したがって、SFR及び運用環境のセキュリティ対策方針が脅威に対抗すること

- 開発者によるセキュリティの目標を、調達者・消費者に対し主張するドキュメント

・SFR：Security Functional Requirement

CC評価におけるSTの位置付け (2)

ITシステム・製品が提供するセキュリティ機能要件が正確に規定され、その背景や実現方法が示される

STを読むと・・・

何をセキュリティの課題（脅威）として捉え、課題に対してどのような対抗策をとり、対抗策をどのように実現しようとしているITシステム・製品なのか理解できる

CC評価におけるSTの位置付け (3)

STの目的

- セキュリティ課題をどのような機能要件で解決するかを調達者・製品利用者に対して示す
- PPで要求されるセキュリティ要件をどのような機能で実現するかを調達者に対して示す
- 定義された機能要件が、以降のセキュリティ機能の評価（設計・実装・テスト・脆弱性検査）の拠り所となる

STに関する注意点

- **使用の容易さ**と、**理解の容易さ**が重要
  - セキュリティ機能性、利用環境について誤解無く伝える
  - 製品購入者が利用の可否を判断できる

一般読者がSTの内容を正確に理解できるように記述されていなければならない

- STは**製品の紹介資料ではない**
  - 何をどこまで、どうやって守るのかを明確に示す
  - 設計ポリシーの明確化

ITシステムや製品における全体の仕様を示すものではなく、セキュリティの機能性について記述する

STの構成要素

STの構成イメージ

第1章　ST概説

- ST参照
- TOE参照
- TOE概要
- TOE記述

第2章　適合主張

- CC適合主張
- PP主張
- パッケージ主張
- 適合根拠

第3章　セキュリティ課題定義

- 脅威
- 組織のセキュリティ方針（OSP）
- 前提条件

第4章　セキュリティ対策方針

- TOEのセキュリティ対策方針
- 運用環境のセキュリティ対策方針
- セキュリティ対策方針根拠

第5章　拡張コンポーネント定義

- 拡張コンポーネント定義

第6章　セキュリティ要件

- セキュリティ機能要件
- セキュリティ保証要件
- セキュリティ要件根拠

第7章　TOE要約仕様

- TOE要約仕様

「第1章 ST概説」（1）

TOEの全体概要について記述する

- ST参照
  - STを一意に識別するための情報
- TOE参照
  - TOEを一意に識別するための情報
- TOE概要
  - TOEの使用法、動作環境の記述と、主要なセキュリティ機能の特徴の要約
  - TOE種別
- TOE記述
  - TOEの範囲を明確にする情報

「第1章 ST概説」 (2)

- STとTOEを一意に識別する
  - ST参照：STの識別
    - バージョンや作成日などを用いて識別できること
    - 識別するための管理方法（構成管理の仕組み）が確立されていること
  - TOE参照：TOEの識別
    - TOEの名称
      - 評価範囲外のセキュリティ機能までを含む名称では、消費者に誤解を与える可能性があり不適切
    - バージョン/リリース/ビルド番号、リリース日などを用いて識別できること
    - TOEに、製品・ITシステムの主要な部分、主要なセキュリティ機能が含まれていない場合には、含まれる機能が明確にわかるような名称にすること

「第1章 ST概説」 (3)

- 消費者がTOEの概要を理解できる
  - TOE概要
    - TOEの使用法と、TOEの主要なセキュリティ機能の特徴に関する記述
      - 単なる機能の羅列ではなく、あくまでセキュリティ機能性としての特徴を記載
    - TOE種別として一般的な種別の識別
      - » ファイアウォール、スマートカード、ウェブサーバ、データベース、デジタル複合機、etc…
      - 一般的な消費者が期待する、機能性や運用環境での動作性について満たしているか？満たしていない場合、明確に説明すること
    - TOEを使用するために必要なハードウェア、ソフトウェア、ファームウェアの記述

「第1章 ST概説」 (4)

- TOEの範囲を明確に記述する
  - TOE記述
    - 「TOE概要」より詳細なセキュリティ機能の特徴に関する説明
      - TOEが提供しない機能について、TOEが提供するかのように消費者に誤解を与えないこと
    - 物理的範囲
      - TOEの構成要素をすべてリストする
        - » ハードウェア、ソフトウェア、ファームウェア
        - » ガイダンス
    - 論理的範囲
      - TOEが提供する、セキュリティ機能の特徴を説明する
      - TOE範囲を明確にするためにTOEが提供しない機能や、TOEが提供する非セキュリティ機能を記載する場合もあるが、それらの機能の必要以上の詳細な説明は、消費者に誤解を生じさせるため不適切

「第1章 ST概説」 (5)

消費者が、TOEを明確に認識できること

消費者が、TOEが提供するセキュリティ機能を正確に理解できること

消費者が、TOEを利用するために必要な環境を理解し、自分の運用環境に合致するかを判断できること

TOE参照、TOE概要、TOE記述が相互に一貫した内容であること

PP適合の場合は…

PPに記述されるTOE概要をベースに、具体化を行う

「第2章 適合主張」（1）

STの適合状況を記述する

- CC適合主張
  - 使用されたCCのバージョン、言語
  - CC Part2とPart3への適合/拡張
- パッケージ主張
  - EALの適合、または追加
- PP主張
  - PPの適合（正確適合、論証適合）※詳細は次ページ
- 適合主張根拠
  - STがPPと同等か、より制限的であることの論証

PP（Protection Profile）：
プロテクションプロファイル

PP適合

- PPは、TOE種別について作成される
  - ファイアウォール、データベース、複合機などの一般的な種別に対する、一般要件を示す
  - RFPのようなもの

- STがPPに適合する場合、以下の2種類の適合が認められる
  - 正確適合
    - PPを厳格に適用する（追加以外の変更は許可されない）
  - 論証適合
    - PPの適用において、同等またはより制限的とみなされる変更がなされる（その根拠を含む必要がある）

「第2章 適合主張」 (2)

- CCのバージョン

【記述例】　情報技術セキュリティ評価のためのコモンクライテリア
パート1:概説と一般モデル　2012年9月　バージョン3.1　改訂第4版　［翻訳第1.0版］
パート2:セキュリティ機能コンポーネント　2012年9月　バージョン3.1　改訂第4版　［翻訳第1.0版］
パート3:セキュリティ保証コンポーネント　2012年9月　バージョン3.1　改訂第4版　［翻訳第1.0版］

- CC パート2、パート3
  - パート２に定義されるセキュリティ**機能コンポーネントのみ**を利用
    - パート２**適合**
  - パート３に定義されるセキュリティ**保証コンポーネントのみ**を利用
    - パート３**適合**
  - パート２に定義されていないセキュリティ**機能コンポーネントを作成**
    - パート２**拡張**
  - パート３に定義されていないセキュリティ**保証コンポーネントを作成**
    - パート３**拡張**

「第５章　拡張コンポーネント定義」に
拡張コンポーネントが定義されていること

「第2章 適合主張」 (3)

- パッケージ
  - 保証パッケージ：EAL１～EAL７
    - EAL x 適合 / 追加
- PP
  - PPへの適合を主張する場合
    - PPのタイトル、バージョンなどの識別情報
    - 正確適合 / 論証適合
    - 「適合主張根拠」による裏付け
  - PPへの適合を主張しない場合
    - 例：PPへの適合を主張しない。
    - 「適合主張根拠」は不要

STとPPの一貫性を裏付ける
・セキュリティ課題定義、セキュリティ対策方針、セキュリティ機能要件の内容がPPと同等もしくは、より制限的である事を主張
（正確適合の場合は不要）

PP適合を主張する場合の記述例

2.2. PP主張

2.2.1 PP主張

本STは、「Protection Profile for xxxx，Version:1.0」への論証適合を主張する。

2.2.2 パッケージ主張

EAL3適合を主張する。

2.2.3 適合根拠

・本STはPPが規定する全ての脅威/OSP/前提条件を引用し、さらにOSP xxxxを追加している。これはTOEに対する制約であるため、課題定義に関して本STはPPより制限的であるといえる。

・本STはPPが規定するSFR FDP_xxxについて、下記の変更を行っている。

FDP_xxx　の割り付け x回 を y回に変更

この変更は、PPが規定するSFRより制限的なxxxを求めるものである。他のSFRについてはPPの規定内容を変更なく引用していることから、SFRに関して本STはPPより制限的であるといえる。

….

上記の説明より、本STはPPより制限的であるため、PPに論証適合している。

単純な追記のみであれば正確適合の範疇

内容の変更が伴う場合は論証適合が必要

「第2章 適合主張」 (4)

定型の記述に注意すること

PP論証適合の場合、適合主張根拠を記述すること

「第3章 セキュリティ課題定義」（1）

TOEが対処する必要がある、セキュリティ上の課題を定義する

- 脅威
  - TOEやその運用環境によって対抗しなければならない脅威
- 組織のセキュリティ方針（OSP）
  - TOEの運用環境により課せられる、規則、手続き、ガイドラインなど
- 前提条件
  - TOEが機能するために、TOE利用者が満たす必要がある運用環境の条件

「第3章 セキュリティ課題定義」 (2)

- 脅威
  - 脅威エージェント
    - 資産に有害な影響を与える可能性があるものを、明確に記述する
      - » 人、プロセス、事故、etc…
    - 次の側面を考慮する
      - » 技能（ITやTOEに対する技術力、知識）
      - » 資源（費やすことが可能な費用、時間）
      - » 機会（TOEに接するタイミング、頻度）
      - » 動機（攻撃の目的、攻撃成功時の利点）
  - 資産
    - 存在する物理的環境や格納される媒体ごとに検討する
  - 有害なアクション
    - 脅威エージェントが、資産に対して行うアクション（攻撃）を具体的に記述する

「第3章 セキュリティ課題定義」 (3)

- 組織のセキュリティ方針（OSP）
  - TOEの運用環境において、課せられるセキュリティ規則、手続き、ガイドラインなど
    - TOE、TOEの運用環境、これらの組み合わせにより実施される
      - » TOEを利用する企業のセキュリティ規則として、パスワードの最低文字数を xx文字以上に制限することの義務付けが想定される場合
      - » 業界ガイドラインにより、DBの設置場所への入室を管理者のみに制限している場合
  - セキュリティ対策方針を策定し、SFRを定義するための、十分な説明、具体的な指示が必要
  - 暗に想定される脅威から導かれたものではないか？
    - 具体的な規則やガイドラインが示されない場合は、基本的に脅威として記述する

「第3章 セキュリティ課題定義」 (4)

- 前提条件
  - TOEがすべてのセキュリティ機能を提供するために必要な運用環境に対する条件の記述
    - ST作成時において、TOEの運用環境として想定する条件
    - 物理的な側面、人的な側面、接続の側面
    - 前提条件が満たされない場合、TSFが機能しない可能性がある
  - 消費者にとって、自身の運用環境が前提条件と一致していることを判断可能であること
    - 前提条件の記述から、TOEを利用するにあたり、どのような運用環境が必要なのか、具体的なアクションが理解できること
    - アクションを実施する目的が示され、複数のアクションが選択できる（解釈される）場合、それぞれが矛盾せず、すべてのアクションにおいて同等の結果をもたらすこと

「第3章 セキュリティ課題定義」 (5)

- セキュリティ課題定義の不適切な例
  - 前提条件と脅威、前提条件とOSP、脅威とOSPにおける矛盾が存在する
    - 前提条件：ICカードは、所有者が自らの責任で他人がそのICカードを使用することがないように管理されている。
    - 脅威：ICカードの非所有者が、ICカードを利用しDBにアクセスすることで、DBの内容を漏洩、破壊、改ざんする。
  - 前提条件の記述から、具体的なアクションを特定できない
    - 前提条件：管理者は、ファイアウォールを適切に管理する
      - » 適切な管理とは？
      - » ファイアウォールはどこに必要？
      - » どのような設定をする？

「第3章 セキュリティ課題定義」 (6)

前提条件は、消費者がSTを利用する際に何をする（準備する）必要があるのかを明確に理解できる記述とすること

脅威が存在しない場合は、必ずOSPが存在すること
OSPが存在しない場合は、必ず脅威が存在すること

脅威には、「脅威エージェント」、「資産」、「有害なアクション」を含めること

STの有用性を理解するために、セキュリティ課題定義の記述が重要であることに留意

PP適合の場合は…

PPの課題定義（脅威、OSP、前提条件）を引用する

「第4章 セキュリティ対策方針」（1）

セキュリティ課題定義によって定義される課題に対し、対抗する解決策を記述する

- TOEのセキュリティ対策方針
  - TOEが持つ機能で対抗、または実現する解決策
- 運用環境のセキュリティ対策方針
  - 運用環境において達成する必要があり、TOEを支援するために実装する技術・手続きに関する手段
- セキュリティ対策方針根拠
  - 脅威への対抗、OSPの実施、前提条件の充足について、すべてのセキュリティ対策方針の効果を分析

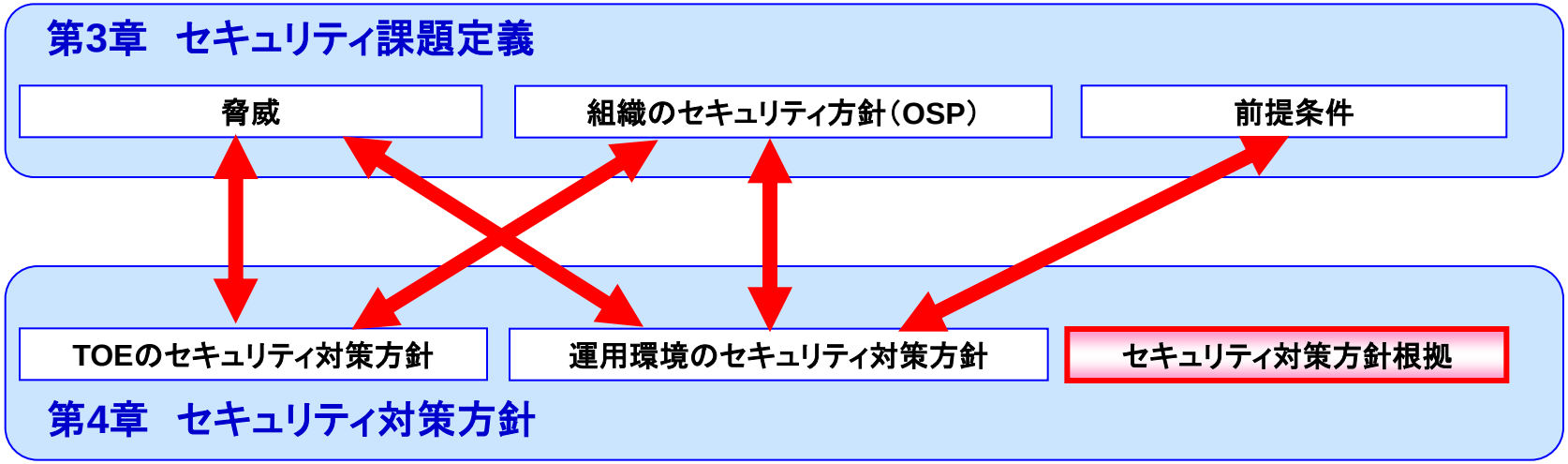
「第4章 セキュリティ対策方針」 (2)

- 脅威への対抗と、OSPの実施
  - TOEのセキュリティ対策方針、もしくは運用環境のセキュリティ対策方針、またはこれらの組み合わせにより対抗･実施される
- 前提条件の充足
  - 運用環境のセキュリティ対策方針により充足される

セキュリティ課題定義にさかのぼれない対策方針が存在する場合、その対策方針は不要な対策方針である可能性がある

「第4章 セキュリティ対策方針」 (3)

- セキュリティ対策方針根拠
  - 各セキュリティ課題に対抗･実施･充足するために、十分なセキュリティ対策方針が策定されているか？
  - 各セキュリティ対策方針は、セキュリティ課題に対抗･実施･充足するため必要なものか？



「第4章 セキュリティ対策方針」 (4)

対抗策や実施策の詳細な説明とならないこと
（セキュリティ機能要件が特定できるレベルで良い）

全ての脅威が対抗され、全てのOSPが実施され、全ての前提条件が充足されること

根拠の記述は、読者が必要・十分であることを納得できるものであること

PP適合の場合は…

PPのセキュリティ対策方針を引用する

「第6章 セキュリティ要件」（1）

TOEセキュリティ対策方針からCC Part2 / Part3を用いた書換えと、SFRを満たす保証の範囲を記述する

- セキュリティ機能要件（SFR）
  - 自然言語で作成されたTOEセキュリティ対策方針からの、TOEの機能性についてのより正確な記述
  - CCの標準言語を利用
- セキュリティ保証要件（SAR）
  - TOEの保証範囲についての正確な記述
  - CCの標準言語を利用
- セキュリティ要件根拠
  - すべてのTOEセキュリティ対策方針が、SFRによって効果的に対処されることの根拠
  - 選択されたSARが適切であることの説明

「第6章 セキュリティ要件」 (2)

- セキュリティ機能要件
  - 規定や定義に基づく、正確な記述であること
    - CC Part2、「拡張コンポーネント定義」、STが適合を主張するPPを参照し記述する
    - 曖昧な用語により、誤解が発生しないようにする
  - 運用環境のセキュリティ対策方針は書き換え不要

- セキュリティ保証要件
  - 規定や定義に基づく、正確な記述であること
    - CC Part3、「拡張コンポーネント定義」、STが適合を主張するPP、保証パッケージ(EAL)を参照し記述する
    - 曖昧な用語により、誤解が発生しないようにする

「第6章 セキュリティ要件」 (3)

- CC Part2、Part3などに記述されたとおり、そのままを再現する
- CC Part2、Part3の再現の他に、コンポーネントに対する「操作」を実施する
  - 全ての操作を正しく実行すること
    - 割　付：指定された項目を具体化する
    - 選　択：指定された項目の中から選択する
    - 繰返し：同じコンポーネントを複数の要件で使用する
    - 詳細化：必要に応じて、要件を具体化する
- 全てのコンポーネントの依存性を満たす
  - 正当な理由があれば、依存性を除外することができる（セキュリティ要件根拠に記述する）

「第6章 セキュリティ要件」 (4)

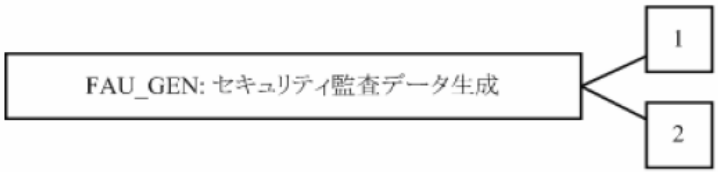
- 機能コンポーネントの具体例

8.2 セキュリティ監査データ生成(FAU_GEN)

ファミリのふるまい

86 このファミリでは、TSF の制御下で発生するセキュリティ関連事象を記録するための要件を定義している。このファミリは、監査レベルを識別し、TSF による監査対象としなければならない事象の種別を列挙し、様々な監査記録種別の中で規定されるべき監査関連情報の最小セットを識別する。

コンポーネントのレベル付け



87 FAU_GEN.1 監査データ生成は、監査対象事象のレベルを定義し、記録ごとに記録されねばならないデータのリストを規定する。

88 FAU_GEN.2 利用者識別情報の関連付けでは、TSF は、監査対象事象を個々の利用者識別情報に関連付けなければならない。

管理: FAU_GEN.1、FAU_GEN.2

89 予見される管理アクティビティはない。

監査: FAU_GEN.1、FAU_GEN.2

90 予見される監査対象事象はない。

FAU_GEN.1 監査データ生成

下位階層: なし

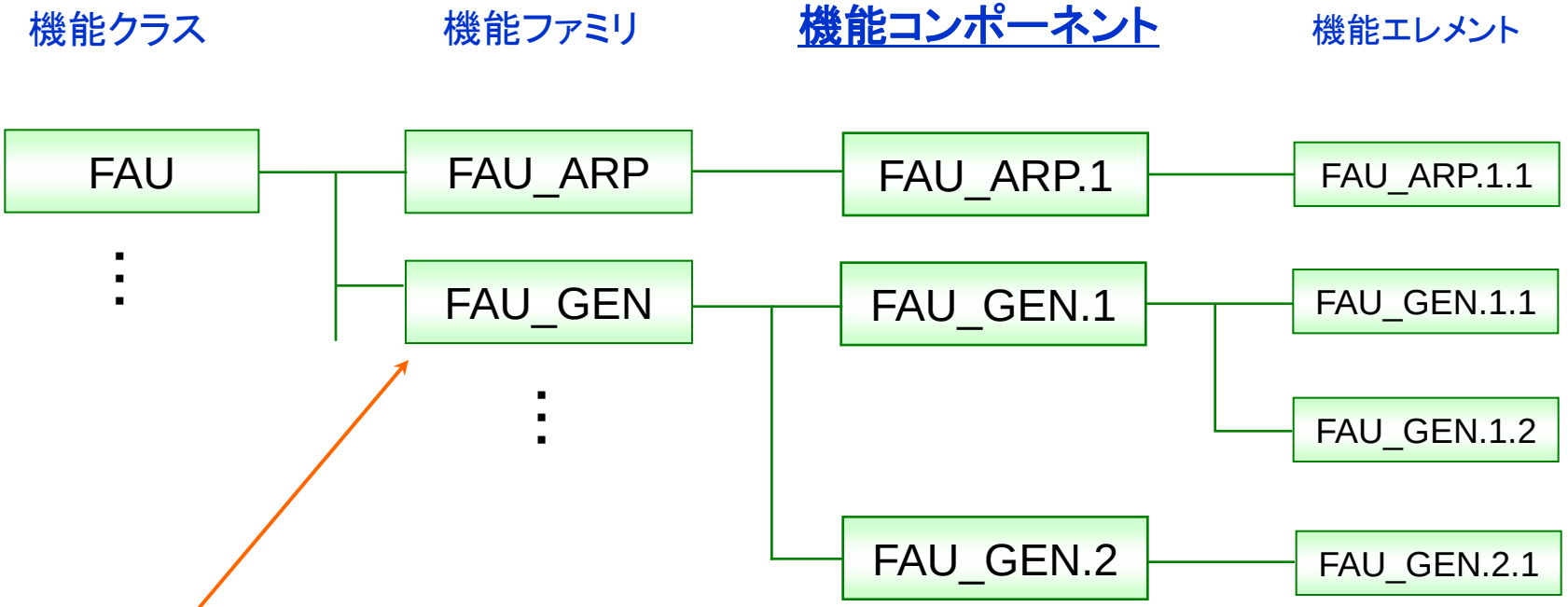
依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない:

- 監査機能の起動と終了;
- 監査の[選択: *最小*、*基本*、*詳細*、*指定なし*: から1つのみ選択]レベルのすべての監査対象事象;及び
- [割付: *上記以外の個別に定義した監査対象事象*]。

「第6章 セキュリティ要件」 (5)

- 機能コンポーネントの構造



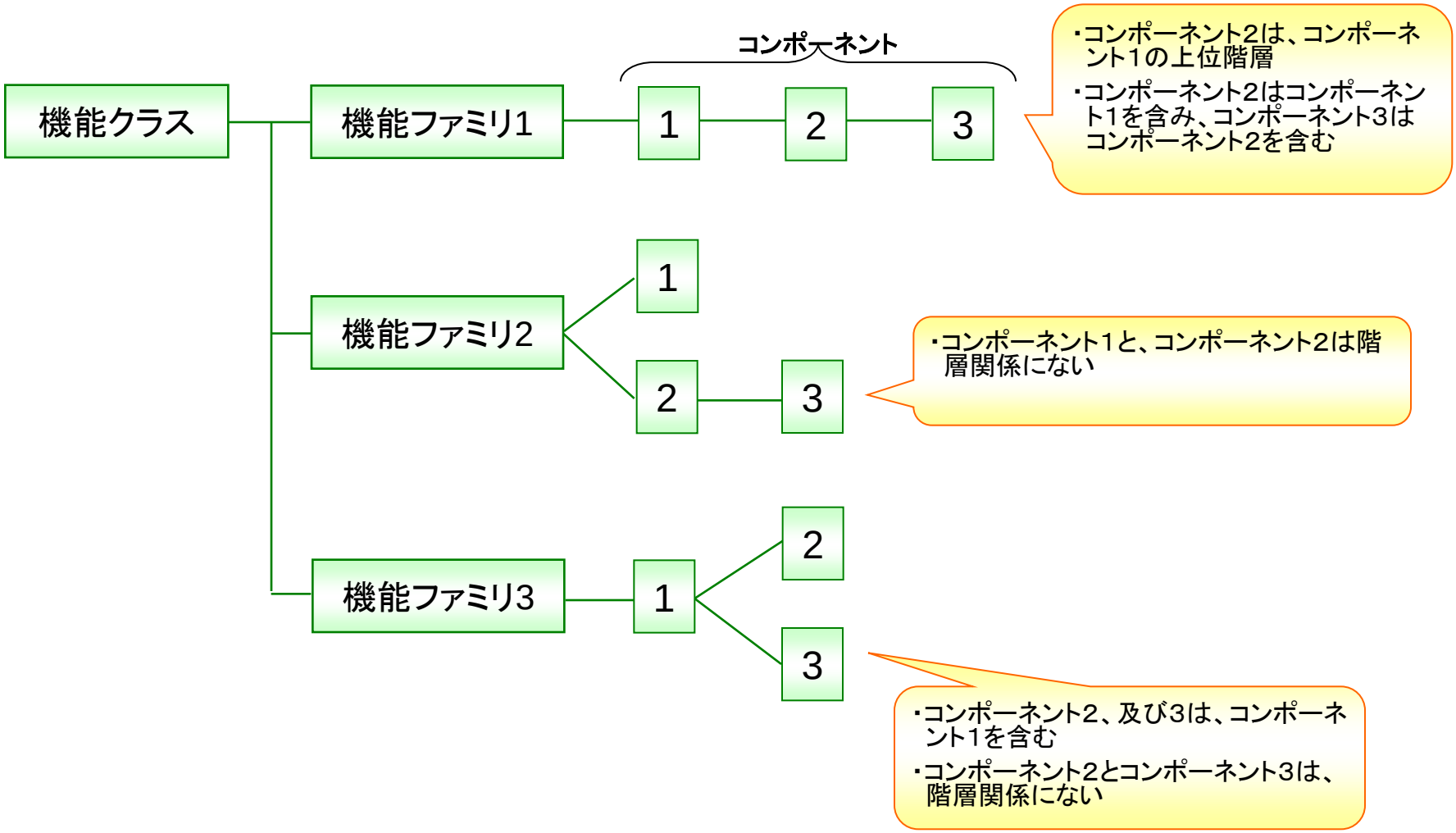
【管理要件】
コンポーネントに対する管理機能の参考情報を示す。
管理クラスのコンポーネントに詳細に記述されており、必要に応じて選択される。

【監査要件】
FAUクラス（セキュリティ監査）が要件として含まれる場合、選択すべき監査対象事象を示す。

【依存性】
他のコンポーネントの機能性や、他のコンポーネントとの相互作用に対する依存関係を示す。
依存性が示される場合、それに従いコンポーネントを選択する。
不要の場合、その根拠を示す必要がある。

「第6章 セキュリティ要件」 (6)

- 機能コンポーネントの構造例



「第6章 セキュリティ要件」（7）

- 機能コンポーネントの選択の仕方
  - TOEセキュリティ対策方針に対応する機能クラスから必要な要件を選ぶ
    - 当該クラスにおける全てのファミリを確認し、関連するコンポーネントを洗い出す
  - 定義した要件群が、TOEセキュリティ対策方針を十分に満足するかどうかを検討する
  - 選んだコンポーネントと依存関係にあるコンポーネントを加える

- 次スライド以降で具体例を用いて、機能コンポーネント選択の流れ（の一例）を紹介

機能コンポーネントの選択の仕方 (1)

- セキュリティ対策方針【O.I&A】
  （識別認証）の場合

TOEは、操作員がTOEを利用する時は必ず識別認証されることを保証し、指定された回数以内に識別認証に成功した操作員のみTOEの利用を許可しなければならない。

また、認証情報の推測を防止するために、設定する認証情報の品質を保証しなければならない。

(サンプルST P.20)

機能コンポーネントの選択の仕方 (2)

- CC Part2には11個の機能クラスが存在

【O.I&A】（識別認証）に対応するクラスを選択

- FAU　：セキュリティ監査
- FCO　：通信
- FCS　：暗号サポート
- FDP　：利用者データ保護
- FIA　：識別と認証
- FMT　：セキュリティ管理
- FPR　：プライバシー
- FPT　：TSFの保護
- FRU　：資源利用
- FTA　：TOEアクセス
- FTP　：高信頼パス/チャネル

機能コンポーネントの選択の仕方 (3)

- 各クラスには機能要件の概括的記述である機能ファミリが存在

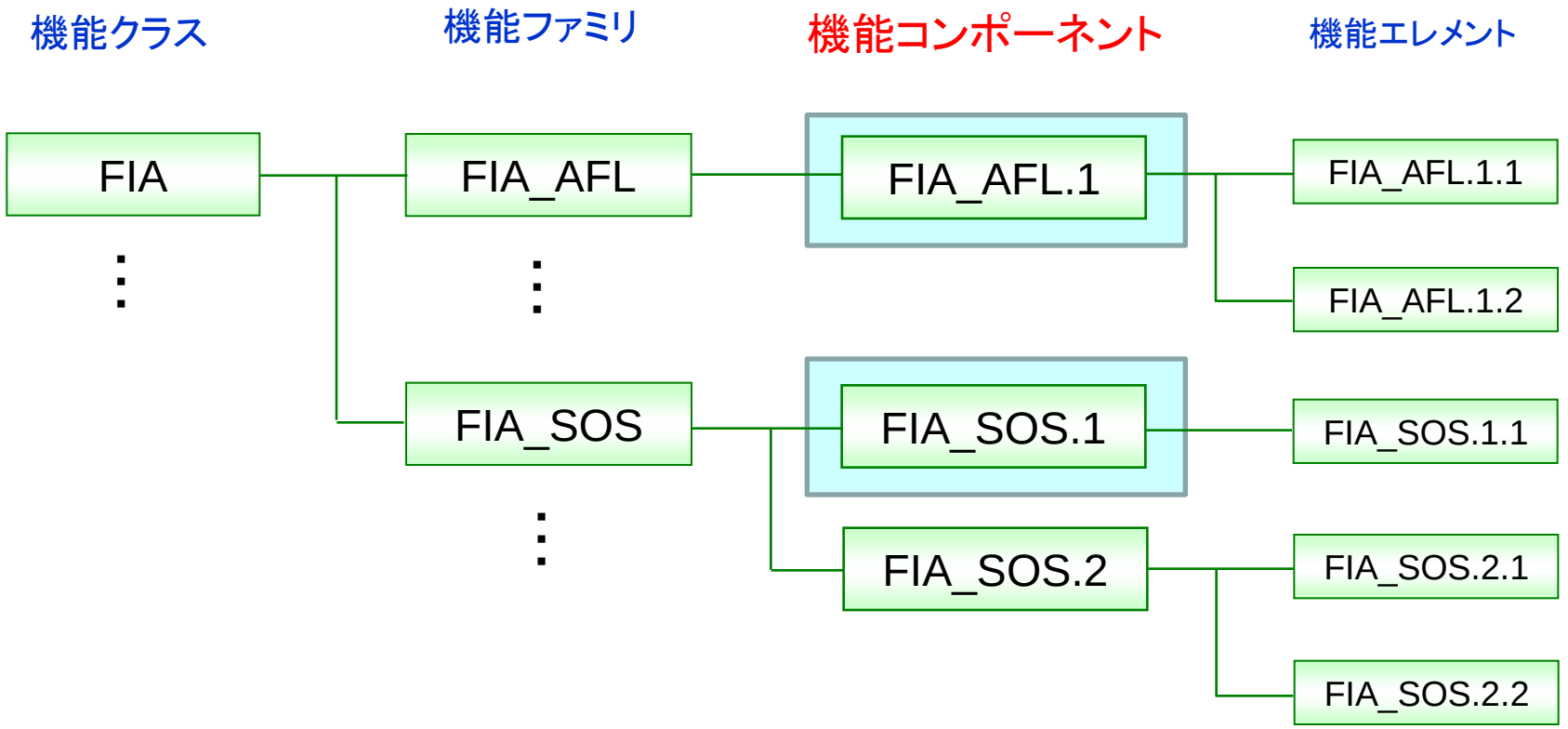
【クラスFIA：識別と認証】には6個のファミリが存在（必要なファミリを選択）

- 認証失敗 (FIA_AFL)
- 利用者属性定義 (FIA_ATD)
- 秘密についての仕様 (FIA_SOS)
- 利用者認証 (FIA_UAU)
- 利用者識別 (FIA_UID)
- 利用者-サブジェクト結合 (FIA_USB)

機能コンポーネントの選択の仕方 (4)

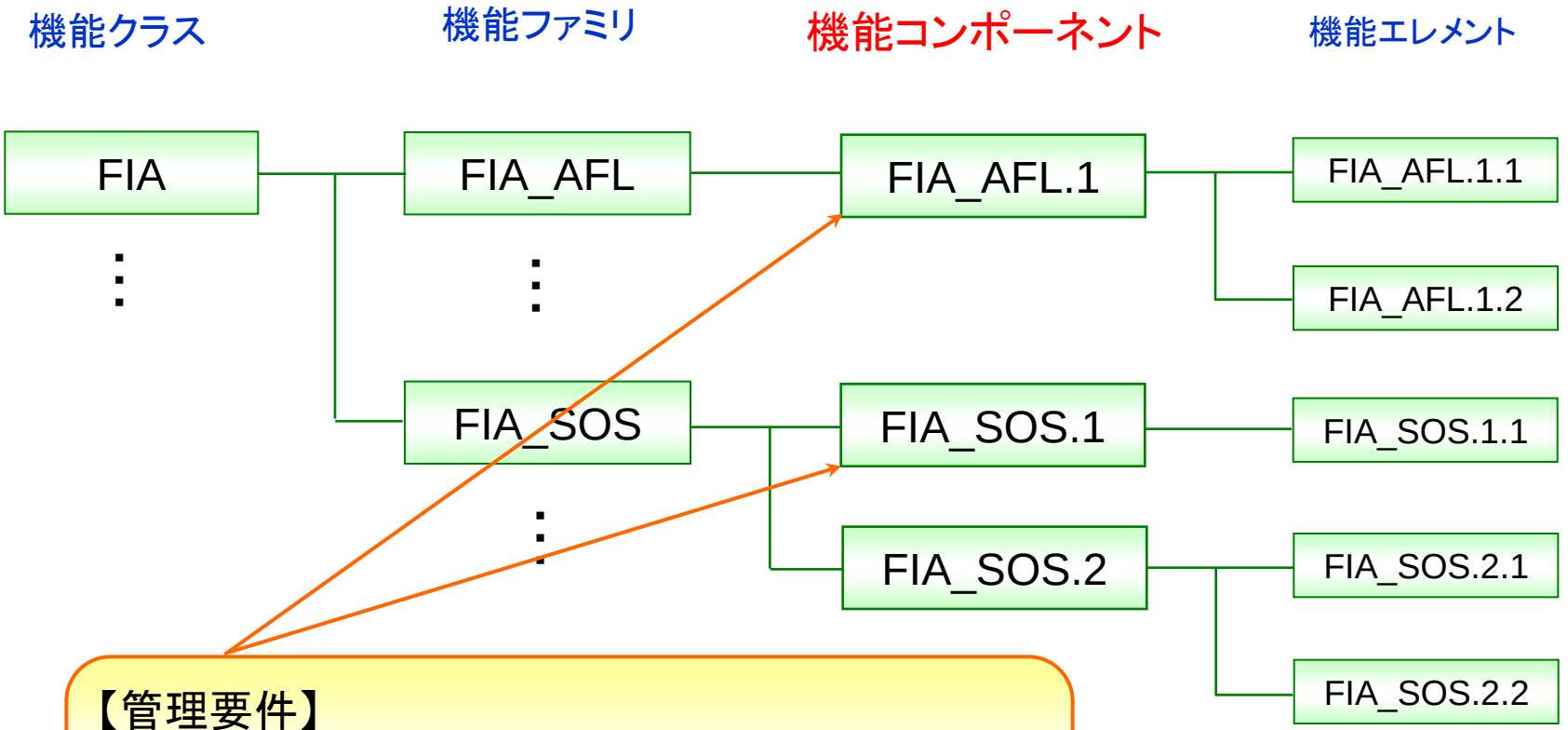
- 機能コンポーネントの決定

選択した機能ファミリから適切な機能コンポーネントを選択



機能コンポーネントの選択の仕方 (5)

- 管理機能（管理要件）の必要性を検討



【管理要件】
機能要件に定義されたセキュリティ機能を適切に動作させるために必要となる要件（参考情報）。
必要に応じてFMTクラスで定義。

機能コンポーネントの選択の仕方 (6)

管理要件の例(CC Part2 P88)

FIA_UAU.1	**認証のタイミング**
	下位階層: なし
	依存性: FIA_UID.1 識別のタイミング
FIA_UAU.1.1	**TSF** は、利用者が認証される前に利用者を代行して行われる[割付: *TSF 仲介アクションのリスト*]を許可しなければならない。
FIA_UAU.1.2	**TSF** は、その利用者を代行する他のすべての **TSF** 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

管理: FIA_UAU.1

263 以下のアクションは FMT における管理機能と考えられる:

a) 管理者による認証データの管理;

b) 関係する利用者による認証データの管理;

c) 利用者が認証される前にとられるアクションのリストを管理すること。

機能コンポーネントの選択の仕方 (7)

- CC Part2には11個の機能クラスが存在

【O.I&A】（識別認証）に対応するクラスを選択

- FAU　：セキュリティ監査
- FCO　：通信
- FCS　：暗号サポート
- FDP　：利用者データ保護
- FIA　：識別と認証
- FMT　：セキュリティ管理
- FPR　：プライバシー
- FPT　：TSFの保護
- FRU　：資源利用
- FTA　：TOEアクセス
- FTP　：高信頼パス/チャネル

機能コンポーネントの選択の仕方 (8)

- FMT_SMF　：必要な管理機能を特定
  （各機能コンポーネントの【管理】を参考に）

  (サンプルST P.35)
- 特定された管理機能をより詳細に定義する
  （主なコンポーネント）
  - FMT_MOF：機能の管理
  - FMT_MSA：セキュリティ属性の管理
  - FMT_MTD：TSFデータの管理
  - FMT_SMR：役割の管理

機能コンポーネントの選択の仕方 (9)

- 【O.I&A】に必要な要件として選択された機能コンポーネント

  - TOE利用前に、操作員が許可された者であることを識別する。
    FIA_UID.1　：識別のタイミング
  - TOE利用前に、操作員が許可された者であることを認証する。
    FIA_UAU.1　：認証のタイミング
  - 認証情報の品質（予測が困難なこと）を検証する。
    FIA_SOS.1　：秘密の検証
  - 識別認証に成功した時に、TOEの利用を許可する。
    FIA_ATD.1　：利用者属性定義
    FIA_USB.1　：利用者-サブジェクト結合
  - 指定回数以内に識別・認証に成功しない場合、TOEの利用を無効とする。
    FIA_AFL.1　：認証失敗時の取り扱い
  - 識別・認証の可否を決定するTSFデータの管理者を制限する。
    FMT_MTD.1：TSF データの管理
    FMT_SMF.1：管理機能の特定
    FMT_SMR.2：セキュリティ役割における制限

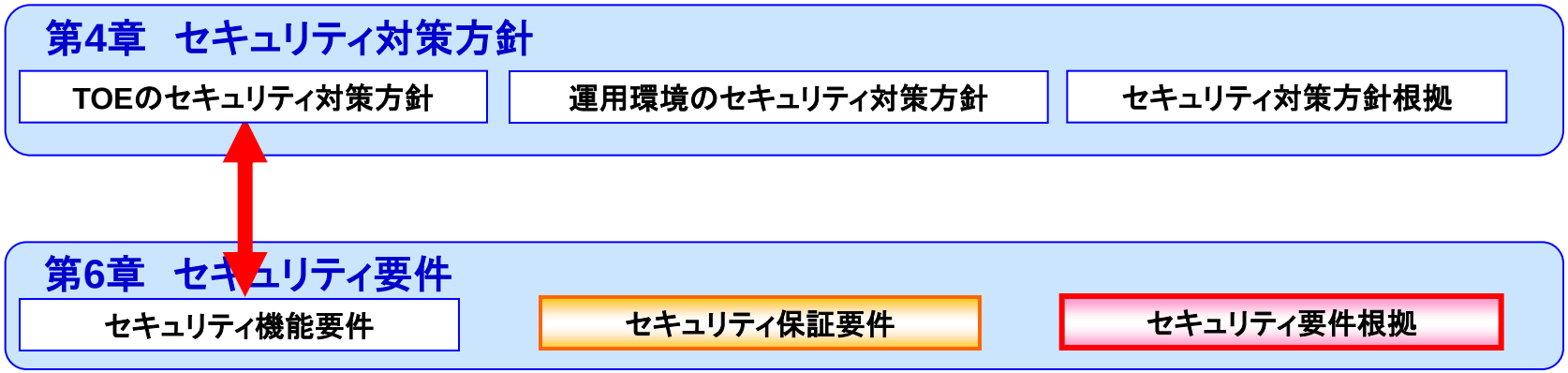
機能コンポーネントの選択の仕方 (10)

- 選択した機能（及び保証）コンポーネントは、許可された【操作】により必要な操作を実施し具体化する（機能要件の定義）
  - 繰返し：種々の操作で2 回以上コンポーネントを使用することができる
  - 割付　：パラメタを特定する
  - 選択　：リストから、1つまたは複数の項目を特定する
  - 詳細化：詳細を追加することができる

（機能要件の依存性が満たされていることも確認する）

「第6章 セキュリティ要件」 (8)

- セキュリティ要件根拠
  - セキュリティ機能要件の実現が、TOEのセキュリティ対策方針を達成するために、必要・十分であるか？
  - 選択されたセキュリティ保証要件について、その選択された理由は想定する攻撃力と一貫しているか？攻撃力、理由ともに明確か？
  - 満たされない依存性が存在する場合、その理由は妥当なものであるか？



「第6章 セキュリティ要件」 (9)

– EAL別の保証コンポーネント

保証クラス	保証ファミリ	評価保証レベル別の保証コンポーネント						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
開発	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
ガイダンス文書	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
ライフサイクルサポート	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
セキュリティターゲット評価	ASE_CCL	1	1	1	1	1		
	ASE_ECD	1	1	1	1			
	ASE_INT	1	1	1	1			
	ASE_OBJ	1	2	2	2			
	ASE_REQ	1	2	2	2			
	ASE_SPD		1	1	1			
	ASE_TSS	1	1	1	1			
テスト	ATE_COV		1	2	2			
	ATE_DPT			1	2	3		
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
脆弱性評定	AVA_VAN	1	2	2	3	4	5	5

・脅威の性質
（攻撃者の攻撃レベル、攻撃方法、動機、etc...）
・保護資産の価値
・保証に要する費用と時間
・PPや、外部からの要求

「第6章 セキュリティ要件」（10）

- コンポーネント間の依存性
  - あるコンポーネントAがセキュリティ機能性または保証を提供するために別のコンポーネントBの存在に依存

- コンポーネント間の依存性が生じる場合、STには以下の内容を含まなければならない
  - 依存関係にあるコンポーネント（もしくは上位階層関係にあるコンポーネント）の追加
  - 依存性が満たされていない（必要ない）ことを正当化するセキュリティ要件根拠

「第6章 セキュリティ要件」（11）

一貫した要件であり、競合する要件がないこと

曖昧な記述を残さないこと

根拠の記述は、読者が納得できるものであること

TOEが提供する機能要件のみが、正確に記述されること

PP適合の場合は…

PPに定義されたセキュリティ要件を引用し、必要に応じて操作を完了させる

「第5章 拡張コンポーネント定義」（1）

CCに規定されていない、セキュリティ機能コンポーネントまたはセキュリティ保証コンポーネントを定義する

- 拡張コンポーネント定義
  - CC Part2に規定されていない、ST/PP作成者が定義したセキュリティ機能コンポーネントの定義
  - CC Part3に規定されていない、ST/PP作成者が定義したセキュリティ保証コンポーネントの定義
  - 拡張コンポーネントが存在する場合、「第2章 CC適合主張」において、「拡張」と記述する
    - CC Part2 拡張
    - CC Part3 拡張

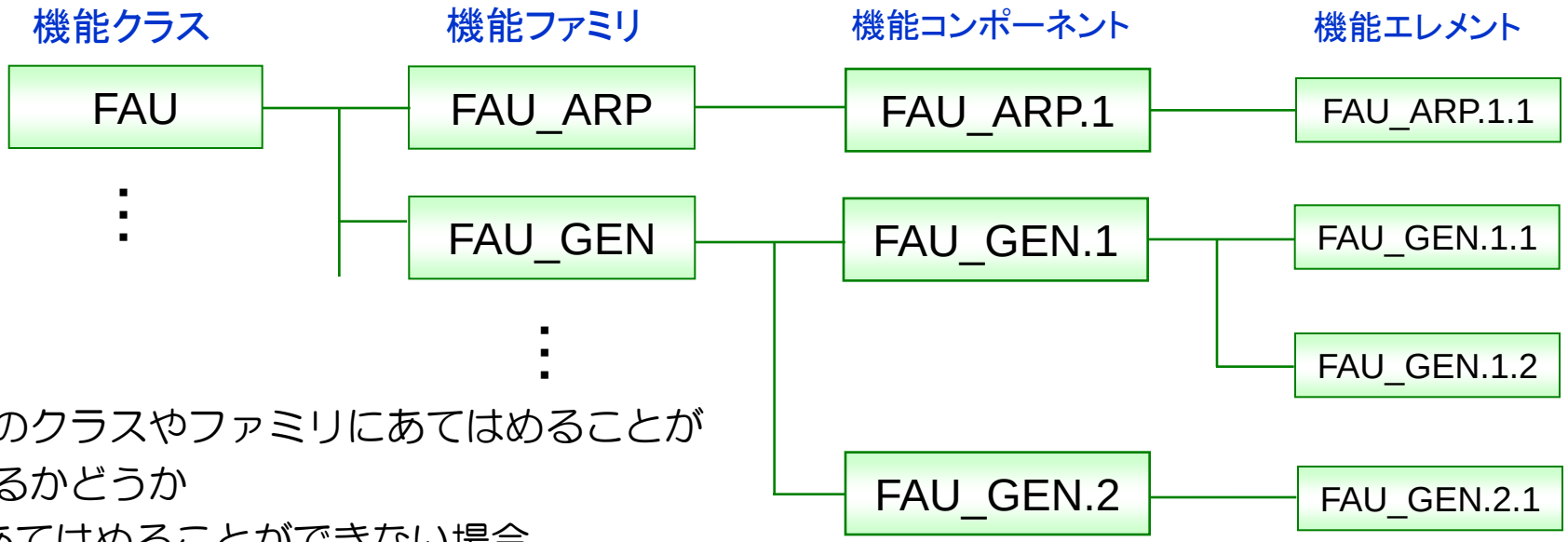
・SFR：Security Functional Requirement
・SAR：Security Assurance Requirement

「第5章 拡張コンポーネント定義」 (2)

- Part2に定義されていない機能コンポーネントを定義する
  - 拡張コンポーネントは、既存のコンポーネントでは明確に表現できない時に用いる
  - ここで定義するのはコンポーネント
    - 要件は、（CC Part2,3の代わりに）本章の定義内容をベースに次章「セキュリティ要件」で定義される

「第5章 拡張コンポーネント定義」 (3)

- 定義した拡張機能コンポーネントは、CC Part2のクラス、ファミリ、コンポーネントにどのようにあてはまるのか？



- 既存のクラスやファミリにあてはめることができるかどうか
  - あてはめることができない場合
    - » 既存のクラス/ファミリにあてはまらない理由
  - あてはめることができる場合
    - » 関連性や、そこにあるべき理由
    - » 同一のクラス/ファミリにある既存のコンポーネントにあてはまらない理由

「第5章 拡張コンポーネント定義」 (4)

CC Part2、Part3に規定されている既存のコンポーネントをモデルとし、規定される構造と一貫するよう定義すること

客観的な記述であり、明確な定義であること

既存のコンポーネントを用いることでは明確に表現できないコンポーネントであること

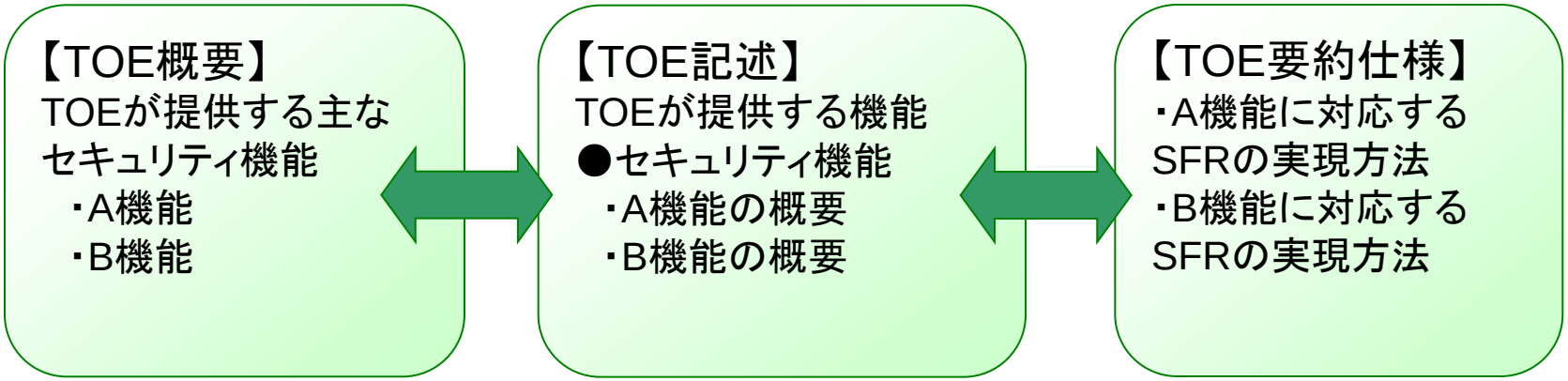
「第7章 TOE要約仕様」（1）

TOEがどのようにしてすべてのSFRを満たすのかを記述する

- TOE要約仕様
  - TOEが提供するセキュリティ機能の技術的メカニズム
    - TOEの一般的な形態、及び実装を理解できる程度の詳細レベル
      - » 認証：パスワード、トークン、虹彩スキャン、etc...
  - TOE概要、TOE記述と一貫した記述、及び詳細度の増加
    - TOE概要 ＜ TOE記述 ＜ TOE要約仕様

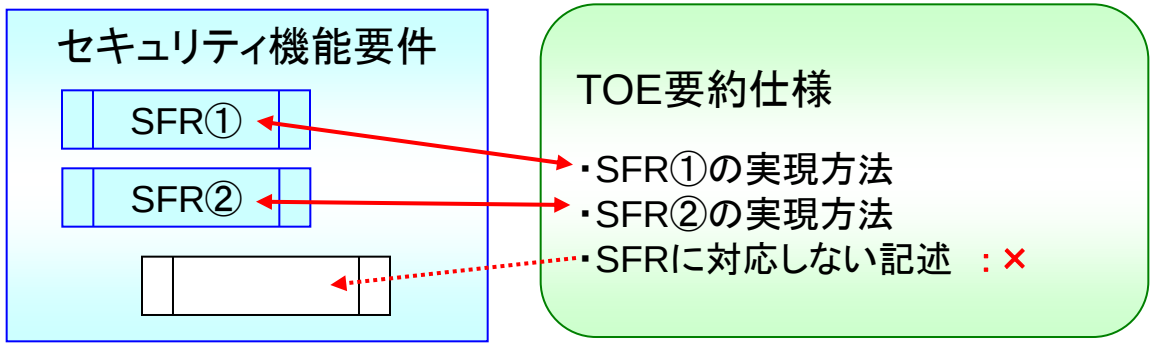
「第7章 TOE要約仕様」 (2)

- TOE概要、TOE記述との一貫性
  - TOEが提供するセキュリティ機能以外は記述しない
    - 説明のために必要となる最低限の記述を除く
    - ただし、TOE外の機能や非セキュリティ機能を記述する時は、それらがTOE外、または非セキュリティ機能であることを明記すること
  - TOE概要、TOE記述に記載されるセキュリティ機能が、もれなくTOE要約仕様に詳細化されていること



「第7章 TOE要約仕様」 (3)

- SFRとの一貫性
  - TOE要約仕様において、SFRの実現方法がもれなく説明されていること
  - SFRに対応しないセキュリティ機能に関する記述が存在しないこと



TOE要約仕様では、TOEが提供しないセキュリティ機能については記載しない

「第7章 TOE要約仕様」 (4)

セキュリティ機能の仕様ではなく、SFRの実現方法を示すこと

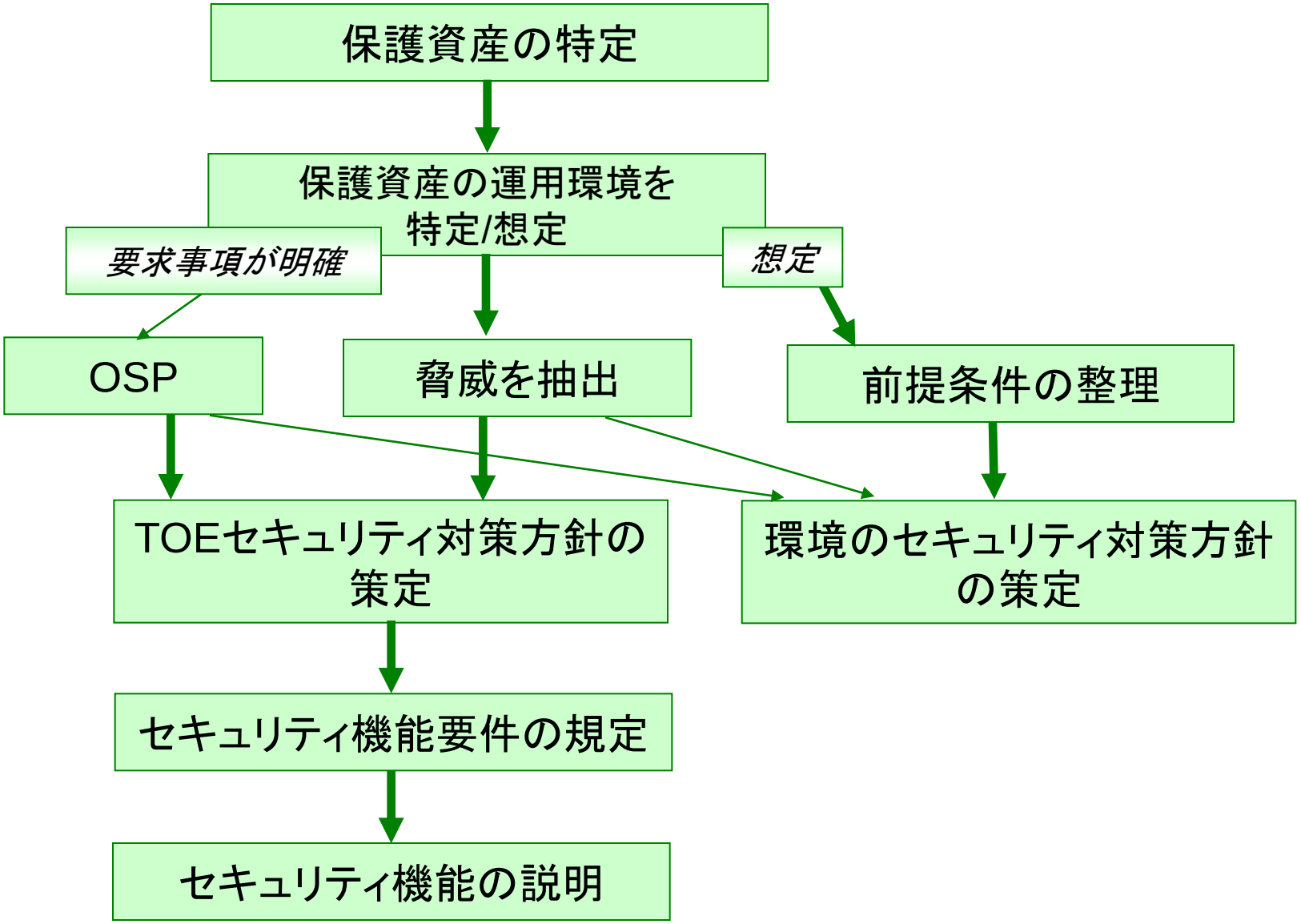
SFRに定義されたセキュリティ機能要件のみ、その実現方法が記載されること

TOE概要、及びTOE記述に示されたセキュリティ機能についてのみ対象とすること

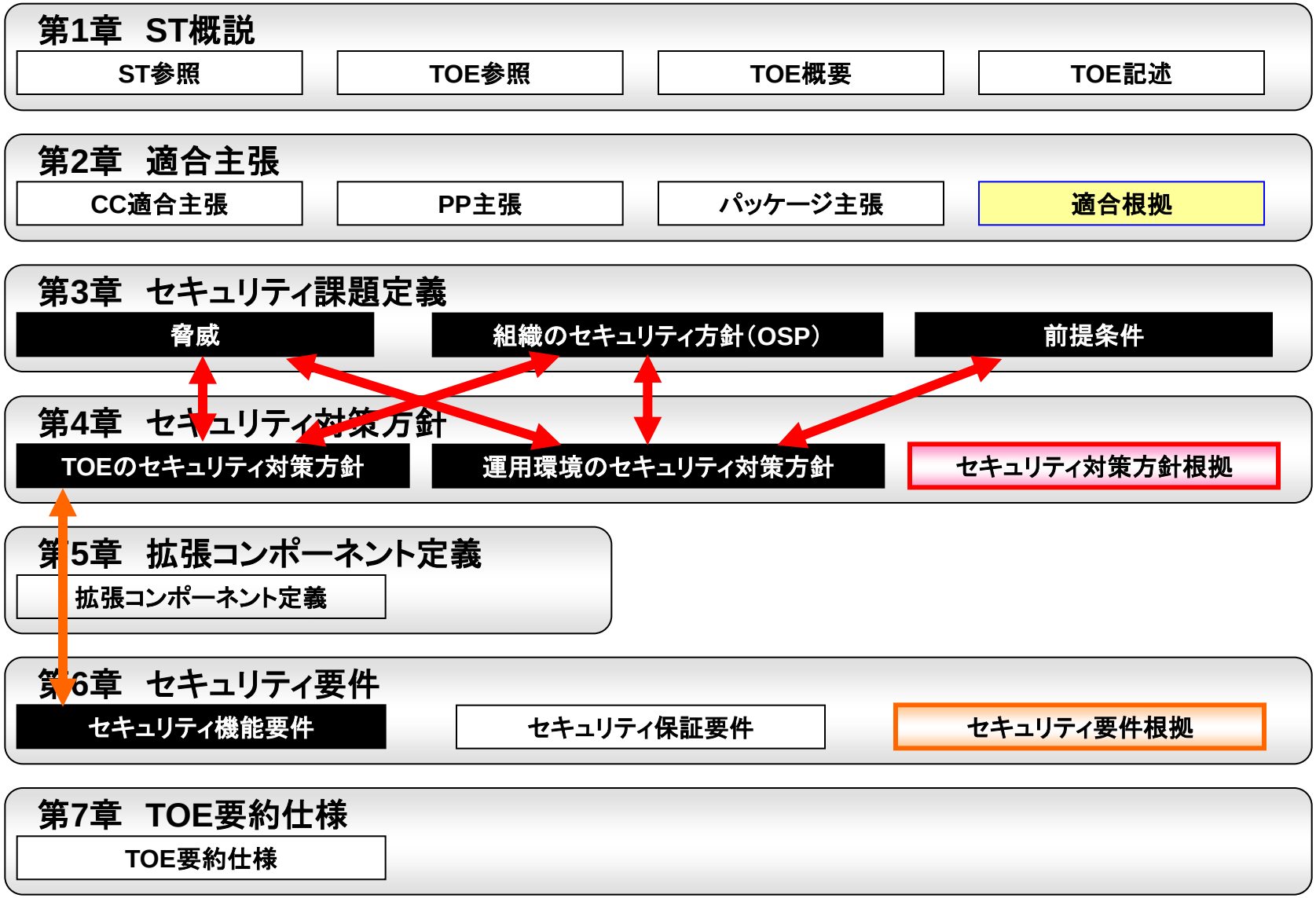
TOEが提供するセキュリティ機能以外の記述はしないこと

ST作成のポイント

STの基本的な論理展開



ST構成要素の関連性


第1章　ST概説
ST参照
TOE参照
TOE概要
TOE記述
第2章　適合主張
CC適合主張
PP主張
パッケージ主張
適合根拠
第3章　セキュリティ課題定義
脅威
組織のセキュリティ方針（OSP）
前提条件
第4章　セキュリティ対策方針
TOEのセキュリティ対策方針
運用環境のセキュリティ対策方針
セキュリティ対策方針根拠
第5章　拡張コンポーネント定義
拡張コンポーネント定義
第6章　セキュリティ要件
セキュリティ機能要件
セキュリティ保証要件
セキュリティ要件根拠
第7章　TOE要約仕様
TOE要約仕様

ST作成時のポイント

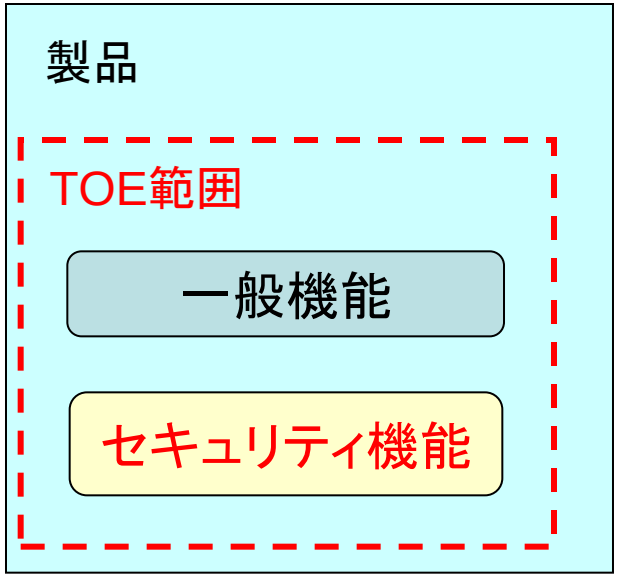
- 評価対象（TOE）の特定
  - 一般的にはProtection Profileで規定
  - TOE範囲と製品の関係の明確化
    - 利用者にとって意味のあるTOE範囲を考える
    - TOEを誤解無く読者に伝える

- 保護資産の特定
  - 所有者にとって価値のあるもの
    - 何を守りたいのか考える
    - 物理的に、どこにある資産なのか特定する

TOE：Target Of Evaluation

TOEを特定する際の注意点

- 評価対象（TOE）の特定
  - 提供者として保証できる範囲の明確化
    - 利用者にとって意味のあるTOE範囲を考える
    - TOEを誤解無く読者に伝える



製品　＝　TOE

＊Protection Profileでは製品全体の保証が一般的

＊調達者、製品利用者は製品の内部構成、部分的な保証範囲を認識できないケースがほとんど

⇨ 製品全体の保証が基本

製品の一部　＝　TOE（製品≠TOE）

＊最低限、調達者が認識できる範囲で

＊全部が保証されている訳ではない事を誤解無く利用者に伝える

JISEC発行文書「TOE決定に係る指針」を参照
(http://www.ipa.go.jp/security/jisec/apdx/documents/guideforTOEscopeVer2.0.pdf)

保護資産を特定する際のポイント

- 守りたい対象の特定
  - どの業務で利用するデータなのか？
  - どのようなサービスなのか？
  - ファイル名、プロセス名は何か？
  - 攻撃を受けた際の影響（資産価値）は？　　etc…

「守りたい」というのは、何から守りたいのかを考える
（機密性、完全性、可用性、真正性、信頼性、責任追跡性、などを考慮する）

同じ対象でも、考慮する必要がない脅威も存在する

PP(Protection Profile)

- 特定の製品分野のために用意されるセキュリティ要件
- 想定されるセキュリティ課題、機能要件を規定
  （セキュリティターゲットのテンプレート）
- 調達者、業界団体等が開発し、調達要件として活用

各技術分野毎に
世界共通となるPPの開発

調達要件、ST開発の中で
PPの積極的な活用が期待

これまでは…

開発者：
独自に要件を定義し、STを作成
STに基づき製品を開発、認証取得

製品調達者：
公開されたST、認証報告書を見て
自分のニーズに合う製品かを判断
（調達要件とのミスマッチ発生のリスク）

Protection Profileを活用した製品調達

製品調達者：
自分のニーズに合うPPをベースに
調達要件を提示

開発者：
提示されたPPに適合したSTの作成
STに基づく製品開発、認証取得

⇨ 要件にマッチした製品の提供

公開されているPPの例

分野	PP名称	発行日
ネットワーク基盤	PP_ND_V1.1	2012/6/8
ファイアウォール	PP_ND_TFFW_EP_V1.0	2011/12/19
VPNゲートウェイ	PP_ND_VPN_GW_EP_V1.1	2013/4/15
IPsec VPNクライアント	PP_VPN_IPSEC_CLIENT_V1.4	2013/10/23
SIPサーバー	PP_ND_SIP_EP_V1.0	2013/2/6
無線LANアクセスポイント	PP_WLAN_AS_V1.0	2011/12/1
無線LANクライアント	PP_WLAN_CLI_V1.0	2011/12/19
汎用OS	PP_GPOS_V3.9	2013/1/15
モバイルデバイス基盤	PP_MD_V1.1	2014/2/18
モバイルデバイス管理	PP_MDM_V1.1	2014/3/7
USBフラッシュドライブ	PP_USB_FD_V1.0	2011/12/1
ソフトウェアフルディスク暗号化	PP_SWFDE_V1.1	2014/3/31
認証局	PP_CA_V1.0	2014/5/16

分野	PP名称	発行日
VOIPアプリ	PP_VOIP_V1.2	2013/10/23
Emailクライアント	PP_EMAILCLIENT_V1.0	2014/4/1
Webブラウザ	PP_WEBBROWSER_V1.0	2014/3/31
BIOSアップデート	PP_BIOS_V1.0	2013/2/13
企業セキュリティ管理ポリシー管理	PP_ESM_PM_V2.1	2013/11/21
企業セキュリティ管理アクセス制御	PP_ESM_AC_V2.1	2013/11/12
企業セキュリティ管理ID・クレデンシャル管理	PP_ESM_ICM_V2.1	2013/11/21
データベース管理システム	PP_DBMS_V1.3	2010/12/24
デジタル複合機	PP_HCD_EAL2_V1.0	2010/2/26
デジタル複合機	PP_HCD_BR_V1.0	2009/6/12
IDS(侵入検知システム)	pp_ids_sys_br_v1.7	2007/7/25

PPの構成イメージ

第1章　PP~~ST~~概説

- PP~~ST~~参照
- ~~TOE参照~~
- TOE概要
- ~~TOE記述~~

第2章　適合主張

- CC適合主張
- PP主張
- パッケージ主張
- 適合根拠

第3章　セキュリティ課題定義

- 脅威
- 組織のセキュリティ方針（OSP）
- 前提条件

第4章　セキュリティ対策方針

- TOEのセキュリティ対策方針
- 運用環境のセキュリティ対策方針
- セキュリティ対策方針根拠

第5章　拡張コンポーネント定義

- 拡張コンポーネント定義

第6章　セキュリティ要件

- セキュリティ機能要件
- セキュリティ保証要件
- セキュリティ要件根拠

~~第x章　TOE要約仕様~~

- ~~TOE要約仕様~~

PP適合STの作成イメージ

STが適合を主張するPP

第1章　PP概説

第2章　適合主張

第3章　セキュリティ課題定義

第4章　セキュリティ対策方針

第5章　拡張コンポーネント定義

第6章　セキュリティ要件

第1章　ST概説
- PPに規定されたTOE概要をベースに、TOE記述（評価範囲、評価対象となる機能の内容等）を具体化

第2章　適合主張
- PP識別名をコピー
- PPの規定内容をベースに適合種別を記述
- 論証適合の場合はPPと同等または、より制限的であると見なせる根拠を記述

第3章　セキュリティ課題定義
第4章　セキュリティ対策方針
- 基本的にPPからそのままコピー（追加の要件がある場合は脅威・対策方針を定義）

第5章　拡張コンポーネント定義
第6章　セキュリティ要件
- 基本的にPPからそのままコピー（追加の要件がある場合は要件を新たに定義）
- 操作が未完了の機能要件について操作を完了する

第7章　TOE要約仕様
- この製品では定義された機能要件をどのように実現しているのか具体的に記載する

PP活用のメリット

ST開発、ST評価に要する労力の軽減

- 一貫した論理展開（課題定義 → 対策方針 → 要件定義）の記述の難しさ
- 適切な機能要件（SFR）定義のむずかしさ
- 記述（表現）内容に対する解釈等に起因するST評価に要するコスト

⇒ PP適合のST作成による上記課題の最小化

認証取得のメリットの最大化

- 調達要件適合に対する客観的な裏付け
- 調達要件を満たす製品の効率的な開発

⇒ PPに適合するSTに基づいた製品設計・開発

効率的・効果的な調達要件の策定

- 調達要件に合致するPP（新規作成、既存PPのリユース）に基づく製品調達

⇒ 調達者が求めるセキュリティ要件を満たした製品の調達
客観的な裏付け（認証取得製品）による受け入れ検査の簡略化

ご清聴ありがとうございました。

ST、認証制度に関するさらに詳しい情報は以下をご確認ください。
http://www.ipa.go.jp/security/jisec/index.html

ご質問、ご相談等ございましたら下記にご連絡ください。
（電子メール）
jisec@ipa.go.jp