CC/CEM V3.1の紹介

平成18年10月4日

独立行政法人　情報処理推進機構

情報セキュリティ認証室

対象の規格

・Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model　September 2006 Version 3.1 Revision 1
CCMB-2006-09-001

・Common Criteria for Information Technology Security Evaluation
Part 2: Security functional components　September 2006 Version 3.1 Revision 1
CCMB-2006-09-002

・Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance components　September 2006 Version 3.1 Revision 1
CCMB-2006-09-003

以上をCCと呼称

・Common Methodology for Information Technology Security Evaluation
Evaluation methodology　September 2006 Version 3.1 Revision 1
CCMB-2006-09-004

以上をCEMと呼称

プログラム

1　CC/CEM V3.1の運用について

2　CC/CEM V3.1の規定内容について

CC/CEM V3.1**の運用について**

CC/CEM V3.1の運用に係わるCCRA(CC承認アレンジメント)決定事項

・2006年9月19日より、CC/CEM V3.1の使用を開始。

・2008年4月１日より、規格はCC/CEM V3.1を必須とする。

・2009年10月1日より、保証継続の再評価時の規格は
CC/CEM V3.1を必須とする。

・V2のCC認証書が無効になることは無い(注)。

注：V2のCC認証書の有効期限について

アメリカ、フランス、ドイツなどは、運用ルールとして、2年間を経過したものは、無効にしている。

(動作環境が変化するので、保証の意味を失うとの見解)

日本におけるCC/CEM V3.1の運用

・平成18年10月5日よりV3.1（英語版）の運用を開始する。

英語版：

規格そのものの記載が要求されている事項（ST内の章節タイトル：パート1のSecurity Target contentsで示されているものをコピー、STに記載の機能要件/保証要件：パート2機能コンポーネント/パート3保証コンポーネントをコピー）は英語を使用する。当該事項以外（要件の操作など）については、日本語で記述することができる。

・平成20年4月1日以降の認証申請は、評価規格としてV3.1を必須とする。（CCRA決定事項に基づく）

・平成21年10月1日以降の保証継続TOEの再評価（認証申請）は、評価規格としてV3.1を必須とする。（CCRA決定事項に基づく）

・V2の認証書は継続して有効とする。

セキュリティ評価規格（CC/CEM）で規定する要求事項について

shall が含まれる文は、例外なく実施しなければならない。

“shall” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).

shouldが含まれる文は、実施しない正当な理由を明記しない限り、shallに準ずる。

“should” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC) The CC interprets 'not necessarily required‘ to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

特に、CEMのワークユニット（サブタスク）に、mayやcanの文と一緒に混在しているので注意のこと。

例：ADV_ARC.1-4 The evaluator ***shall examine*** the security architecture description to ------

532 -----

533 ------

534 ------

535 All of the mechanisms contributing to the domain separation functions are described. The evaluator **should** use knowledge gained from other evidence --------.

CC/CEM V3.1翻訳版の作成について（予定）

- 平成19年1月：　CC/CEM V3.1の和文の参考資料を公開
- 平成19年4月：　CC/CEM V3.1の和文の規格を公開

CC/CEM V3.1の規定内容について

注：

- **実際に規格を利用する際には、必ず、ITセキュリティ評価及び認証制度（JISEC)が公開する規格を使用してください。本資料中には、理解を容易にするためにV3.1の規格を一時的に翻訳しているものも含まれるが、和文の規格に影響を与えるものではない。**
- **以降の説明には、V2で使用した翻訳用語はそのまま使用します。**
- **CCの基礎知識を前提としています。CCの基礎用語などの解説はありません。**
- **V2との比較（何が変更されたのか）を中心に説明しています。**

V 3.1の基本的な考え方

CC（CEMを含む）は情報セキュリティ機能(SFR)の“保証”を確保するための規格である。

TSFの定義：
“TSP（TOEが資産を管理、保護するための規定）を遂行するために必要なTOEの全てのソフトウェア/ファームウェア/ハードウェアのセット”（V2）⇒ “SFRを正確に遂行するために必要な - - - -”(V3)

評価の対象（TOE）はIT機能であること以外の制限はしない。

TOEの定義：
“IT製品またはシステム＋ガイダンス文書”（V2）⇒ “ソフトウェア/ファームウェア/ハードウェアのセット＋ガイダンス文書”（V3）
外部エンティティの定義：
“TOE外のIT製品やシステム”（V2）⇒“TOE外の実体（人またはIT）”（V3）

保証の対象とする情報セキュリティ機能は、TOEが決めるものであり、その決定を制限するようなことはしない。

例：
資産：“TOEのセキュリティ対策によって保護される情報あるいは資源”(V2)⇒“TOEが価値を認めた実体”（V3）

V2からの変更（共通）

・IT製品とシステムの区別がなくなった。

V2でシステムと呼称していたTOEがCCRAの対象（CC認証書の発行対象）になった。

CCRAにおいて確認した内容（骨子）：

In V3.1, TOEs with a particular purpose and operational environment are accepted as IT products, and Common Criteria certificates can be issued for them.

STについて

STの改善点

TOEのSFRを正確に記述することに集中

- Low assurance ST (ただし、EAL1のみ)
- SFRの規定はTOEのみを対象
- SOFの考慮は不要
- FPT_RVM、FPT_SEPは削除
- SARに関わる要約仕様は不要
- 要約仕様根拠は不要

STの目次

4 Security objectives

4.1 Security objectives for the TOE （EAL1では不要）

4.2 Security objectives for the operational environment

4.3 Security objectives rationale （EAL1では不要）

5 Extended components definition

6 Security requirements （TOEのみ、SOFの考慮は不要（脆弱性分析：直接攻撃で評価）、FPT_RVM/FPT_SEPは削除（ADV_ARCで評価））

6.1 Security functional requirements

6.2 Security assurance requirements

6.3 Security requirements rationale （EAL1では不要）

7 TOE summary specification（SARは不要、根拠は不要、TOE自体の保護を要約仕様レベルで記述（EAL1では不要））

「1.2 TOE reference」について

【TOEと製品の関係】

・TOEに製品名称を使用する場合は、TOEと製品の機能範囲は同じとする。（オプション機能を除外するのは許容範囲）

・TOEが製品のサブセットの場合は、利用者が導入時や使用時に認識できる名称をTOEに対して付与する。

・V3.1では、利用者に誤解を与えないことの検証が、明に規定されている。

(ASE_INT.1-4)：
TOE参照が利用者に誤解を与えるものであってはならない。
製品の一部のみがTOEであるにもかかわらず、TOE参照は製品となっており、評価範囲について利用者に誤解を与えることが懸念される場合には、製品を直接TOE参照に記述してはならない。

「1.3　TOE概要」について

利用者にTOEが興味あるものであるか否かの判断（セキュリティに対する要求、サポートされるハードウェア/ソフトウェア/ファームウェア、など）に必要な情報を与える。TOEの利用と主なセキュリティ機能、TOE種別、TOEが必要とする主な非TOEのハードウェア/ソフトウェア/ファームウェアを数段落程度で記述する。

「1.4　TOE記述」について

TOEの機能とセキュリティ機能の詳細を数ページで記述する。TOEの物理的、論理的な範囲を明確に記述する。

「2.2　PP claim」について　（その１）

【strict conformance】

STにはPPで規定のすべての要求を含むが、**PP**規定内容に矛盾しない限り、要求の追加は可能。最小限のセキュリティ要求を規定する場合にこの適合を規定する。

例えば、セキュリティ対策方針に対して、次の条件を満足しなければならない。

・STで規定のセキュリティ対策方針には適合が主張されているPPで規定されているセキュリティ対策方針をすべて含む。STでさらに追加することは可能。

・STで規定の運用環境のセキュリティ対策方針は、適合が主張されているPPで規定されている運用環境のセキュリティ対策方針を正確に全て含む、あるいは、一部を含む。PPで規定されていない運用環境のセキュリティ対策方針を含んではならない。

「2.2　PP claim」について　（その２）

【demonstrable conformance】

STとPPには包含などの関係はないが、**ST**は**PP**の要求事項を満足しなければならない。満足している理由を**ST**の根拠（「2.4 Conformance rationale」）に記述する。**PP**はガイダンス的な存在である。

例えば、セキュリティ対策方針に対して、次の条件を満足しなければならい。

・STで規定のセキュリティ対策方針は、PPで規定のセキュリティ対策方針と同等、または、より制限的であることを適合主張根拠で記述する。

制限的とは、PPのTOEセキュリティ対策方針は全て含み、追加は許可、運用環境のセキュリティ対策方針は全て含み、追加は非許可を意味する。

同等とは、STに規定のTOEセキュリティ対策方針を満足するTOEは、PPに規定のセキュリティ対策方針を満足する、さらに、PPに規定のセキュリティ対策方針を満足する運用環境は、STに規定のセキュリティ対策方針を満足することを意味する。

「3 Security problem definition」について

- 与件（axiomatic：公理の、自明の）であるから、導出の過程や内容自体の妥当性（脅威の十分性など）は評価しない。（security objectivesとの関連で矛盾がなければ問題なしとの意）
- OSPとthreatsの記述については、threatsに記述できる（脅威として認識できる）ものは、OSP（TOEの運用管理組織や立法機関からの要請）には記述しないことを原則とする。ただし、PPには、要求するセキュリティ機能をOSPで記述（政府調達の立場）したものがあるので、これに適合するSTでは、そのままOSPに記述することは可である。

以下は、CEMの規定。

3.2 組織のセキュリティ方針

【組織のセキュリティ方針に対する要求事項】

セキュリティ課題定義に組織のセキュリティ方針を記述しなければならない。(ASE_SPD.1-3)

ガイダンス：

・組織のセキュリティ方針とは、規則、慣行、またはガイドラインである。TOEの運用環境を管理する組織、または立法機関などが組織のセキュリティ方針を規定できる。

パート2について

V2に対する問題認識

二者択一で多様性に欠ける。

一般利用者か管理者、利用者データかTSFデータ、運用機能か管理機能、など。

例えば、業務アプリケーションでTSFデータでもOSから見れば利用者データ。これでは、複数のTOEを統合する際には適用が困難。

“利用者”の概念が不明確である。

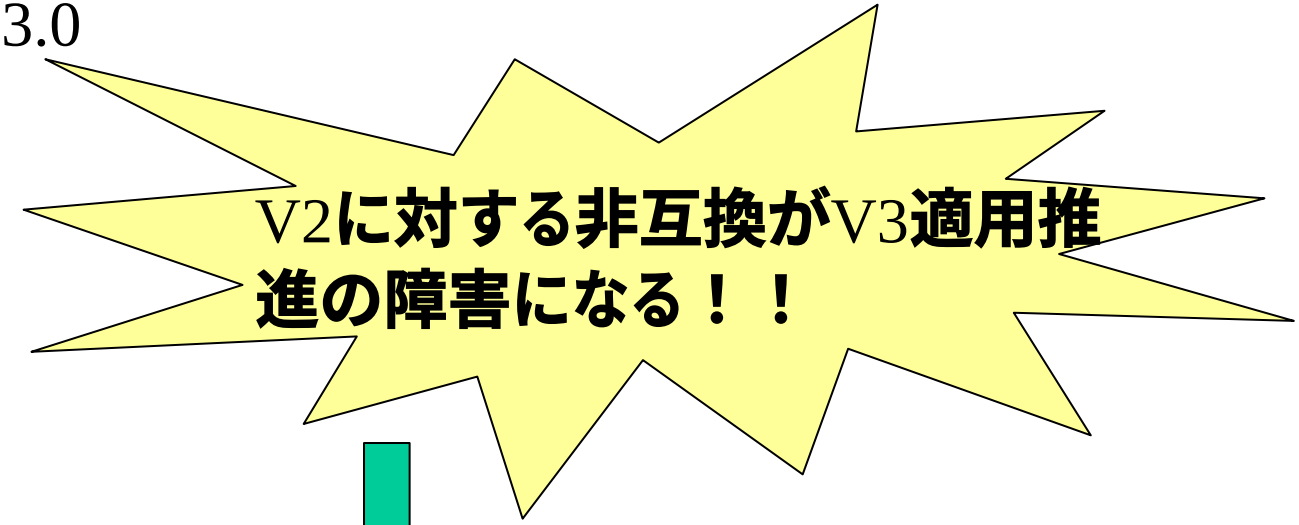
利用者、許可利用者、信頼できる利用者、信頼できるIT製品、抽象マシンなどとの通信に係わる要件が存在する。さらに、利用者とサブジェクトが誤解されたまま使用されていることがある。

要件の抽象度のレベルが異なる。(高い抽象度、適切な抽象度、実装レベルの記載)

実装に依存するような要件が存在している。要件は抽象的で、実装に依存しないものにする。

抽象的とは、ディスク、データバスなどのエンティティではなく、抽象エンティティ(オブジェクト、サブジェクトなど)を使用して期待されるふるまいを記述することである。実装に依存しないとは、SFRを満たす多くのTOEが存在することができ、これらのTOEはまったく異なる方法で実装することができることである。

V2の解決⇒V 3.0



V 2.3に対して、

- パート3でカバーする、FPT_RVM/ FPT_SEPを削除。
- パート3で変更したADV_SPM.1への依存性を削除。
- V3で使用を中止した用語（TSP,TSC,システム、など）を変更。
- 既に修正を決定していた事項（エディトリアル的なものが主）を反映。

V 3.1の作成

資料参照

ただし、

完成系が不確定である。
全てのオブジェクトをリストさせないで、「全てのオブジェクトを保持」と要求していたので完全な検証ができなかった。

V3.1では、機能要件の指定時に、全てのサブジェクトとそのセキュリティ属性、全てのオブジェクトとそのセキュリティ属性、全ての操作、全ての利用者を指定しなければならないことを明確にする。
ASE_REQ.1.1C (ワークユニットASE_REQ.1-3)で、
“セキュリティ要件（SFR, SAR）で使用する、全ての、サブジェクト、オブジェクト、操作、セキュリティ属性、外部エンティティ、その他の用語をSTで定義しなければならない。”

パート3について

保証の基本的な考え方（V3の作成に当たっての確認事項）

セキュリティに対する脅威と、**TOE**を運用する組織が遵守を必要とする規則や法律などを明らかにする。ただし、その内容の十分性や妥当性を保証するものではない。⇒**ST**のセキュリティ課題の規定

TOEが装備するセキュリティ機能と、**TOE**の運用環境のセキュリティ対策方針が、**ST**で規定のセキュリティ課題を解決または実現するために十分（正確性、有効性）であることを、実際に**TOE**を検査することによって実証する。⇒**SAR**に基づく評価の実施

TOEに残存する脆弱性が、**TOE**の動作・運用において問題とならないことを、実際に**TOE**を検査することによって実証する。

問題とならないとは：

- 発生し得る脅威に残存脆弱性が利用されたとしても、顕在化する問題は許容の範囲である。
- 発生し得る脅威に脆弱性が利用されたとしても、顕在化する問題が許容の範囲を超えるような脆弱性は残存していない。
- 残存する脆弱性を利用しようとする攻撃は検出でき、許容の範囲を超えるような問題の発生時の被害を最小限に抑えることができる。

⇒**AVA**に基づく脆弱性評価の実施

脆弱性が作りこまれる危険性は、**TOE**の機能設計、**TOE**の実装、**TOE**の動作・運用にわたって存在する。

⇒**TOE**のライフサイクル、および、**TOE**のガイダンス文書に対する脆弱性評価

TOEに対するセキュリティ保証は、**TOE**が**ST**で規定のセキュリティ対策方針を満たしていることに対する確からしさを、実際の**TOE**を検査することによって検証する。

⇒確からしさは、**SAR**に規定の多様な保証クラスと保証の程度（評価の範囲、評価の深さ、評価の厳密さ）に基づく

セキュリティ保証の程度に応じて、効率的な評価を行う。

⇒開発者がエビデンス情報の内容を分類できる。（SFR- enforcing, SFR-supporting, SFR-non-interferingの導入）

分類を強要するものではない。

V2からの主な変更

- **ADV_RCR削除**

各エビデンス作成要求の中で、開発者が対応についても表示。

例：ADV_FSP.1.2D/1.4C:開発者はSFRからTSFIに対する対応を記述（tracing)しなければならない。

- **Informal/ semiformal SPM削除**

STで規定するセキュリティ機能要件以外の何か（Informal/ semiformal SPM）が保証のために必要であるとは考えられないために削除。セキュリティポリシーモデルとして、確立した数学的概念に基づき意味が定義された構文言語で表現する公式モデルのみが存在。

- **TSP削除**

TSPはSFRと同等であると考える。

・用語“Security Function”削除

TSFはTOE Security Functionality（セキュリティ機能）のことを意味し、セキュリティ機能要件（SFRs: Security Functional Requirements）にのみ依存する。

その他：

・high level description：CCに定義は無いが、機能の説明（何）を意味する。機能をどのように実現するかについての処理の説明ではない。

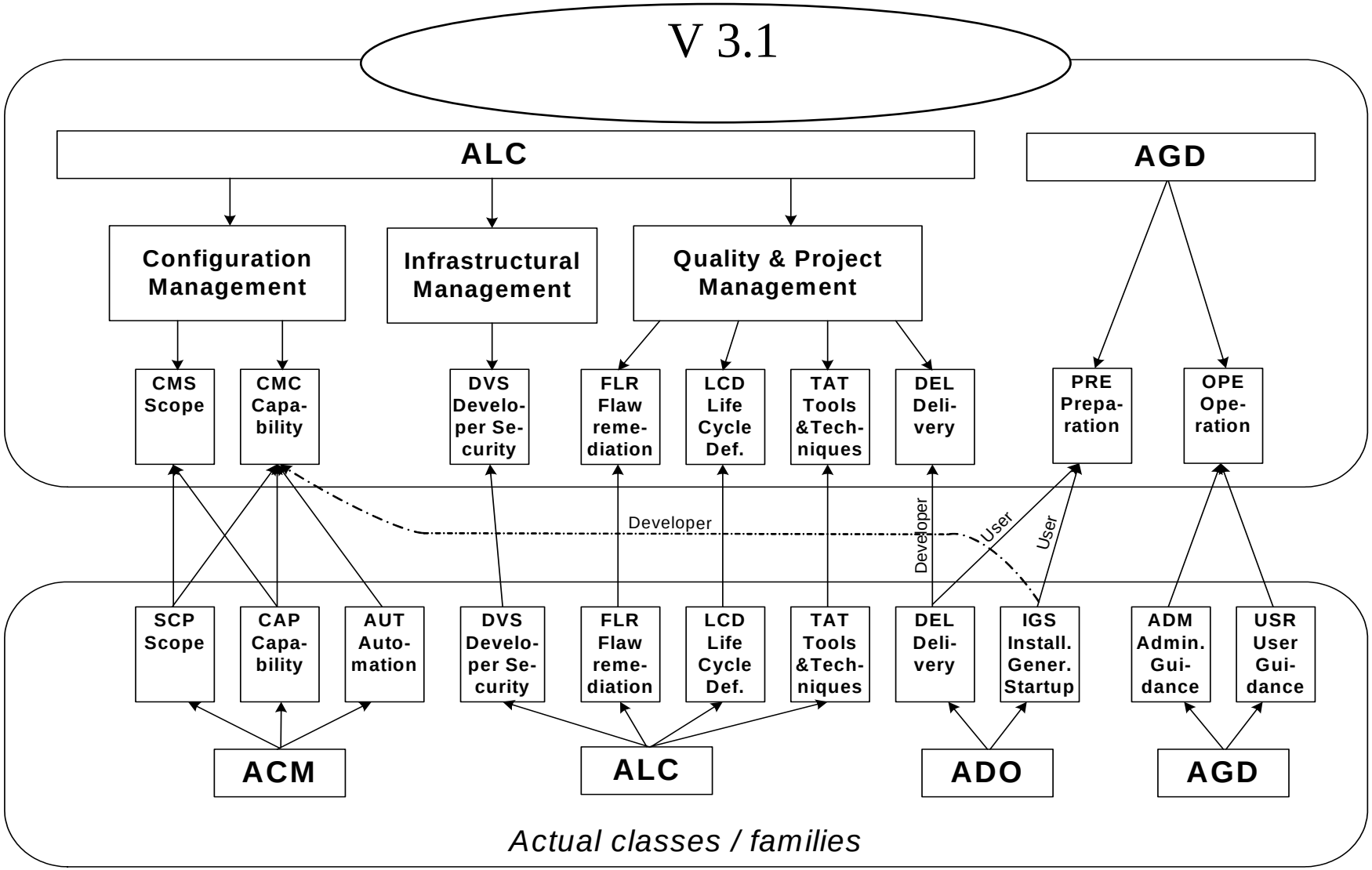
【ALC/AGD】

・基本的なライフサイクルモデルとして、開発、配付、導入、生成、起動、運用を規定。

・要件内容は、基本的には、CC V2を変更しないで、重複した要件を整理。また、要件を適切なクラスに移動させ、クラスとしての保証に係わる要求内容を明確化。

・要件内容の整理
- 利用者に対する要件と開発者に対する要件の明確化
- 管理機能に対する要件と管理対象に関する要件の明確化
- TOEの運用とその環境に係わる要件の明確化

例：ガイダンス文書は、評価時の構成下で、TOEの運用中に実行する必要があるすべての操作、つまり運用と管理に係わる事項を記載した利用者操作ガイダンス(AGD_OPE)と、STに記述された環境で配付されたTOEを評価時の構成(認証された運用環境)に変換するために実行する必要があるすべての操作、つまりTOEの受入と設置に係わる事項を記載した利用者準備ガイダンス(AGD_PRE)に分ける。


V 3.1
ALC
AGD
Configuration Management
Infrastructural Management
Quality & Project Management
CMS Scope
CMC Capa-bility
DVS Develo-per Se-curity
FLR Flaw reme-diation
LCD Life Cycle Def.
TAT Tools &Tech-niques
DEL Deli-very
PRE Prepa-ration
OPE Ope-ration
Developer
Developer
User
User
SCP Scope
CAP Capa-bility
AUT Auto-mation
DVS Develo-per Se-curity
FLR Flaw reme-diation
LCD Life Cycle Def.
TAT Tools &Tech-niques
DEL Deli-very
IGS Install. Gener. Startup
ADM Admin. Gui-dance
USR User Gui-dance
ACM
ALC
ADO
AGD
Actual classes / families
V 2.3

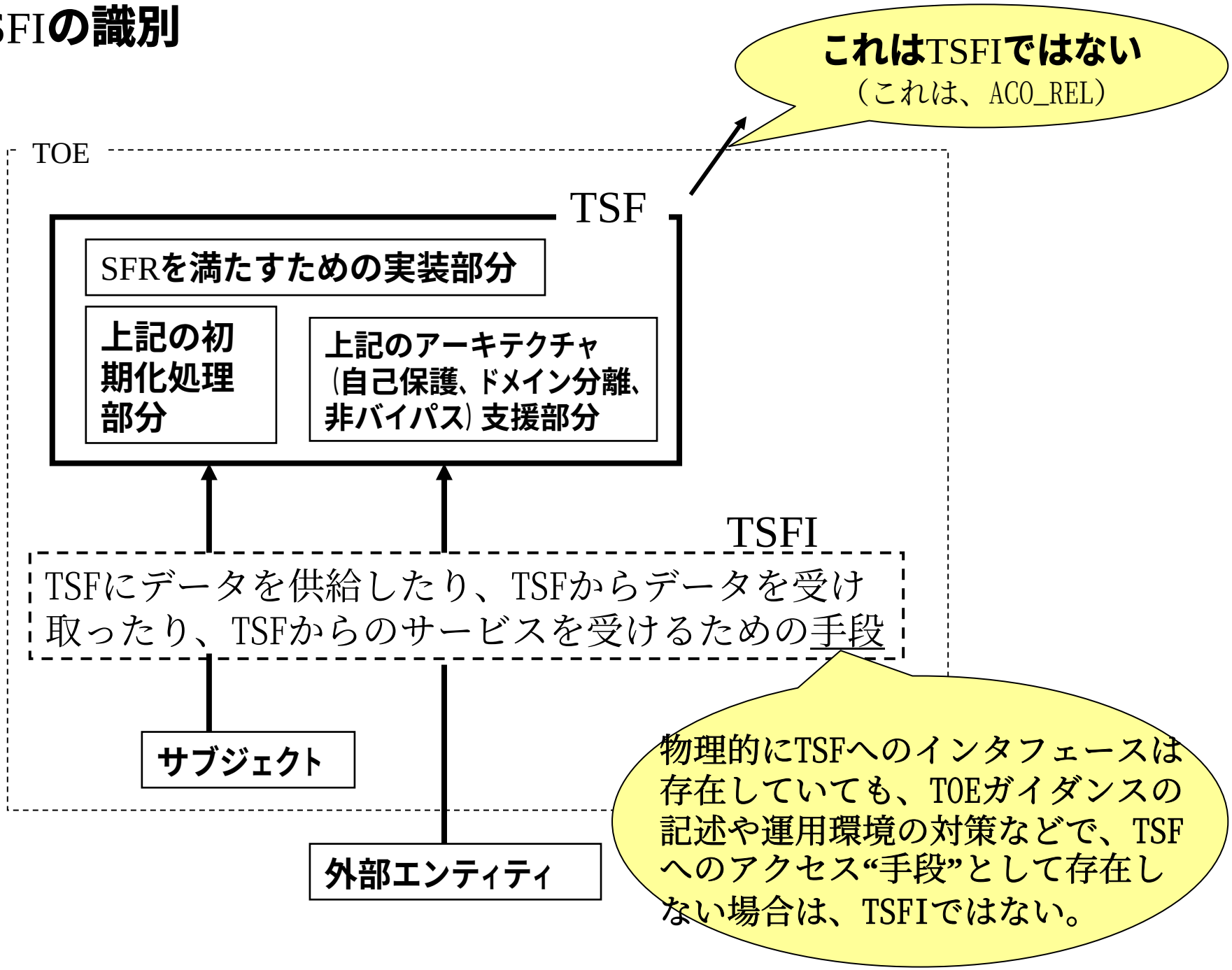
【機能仕様(FSP)】

“外部エンティティ（あるいはTSF外のTOE内のサブジェクト）がTSFにデータを供給したり、TSFからデータを受け取ったり、TSFからのサービスを受けるための手段(means)”（TSFI)を記述する。

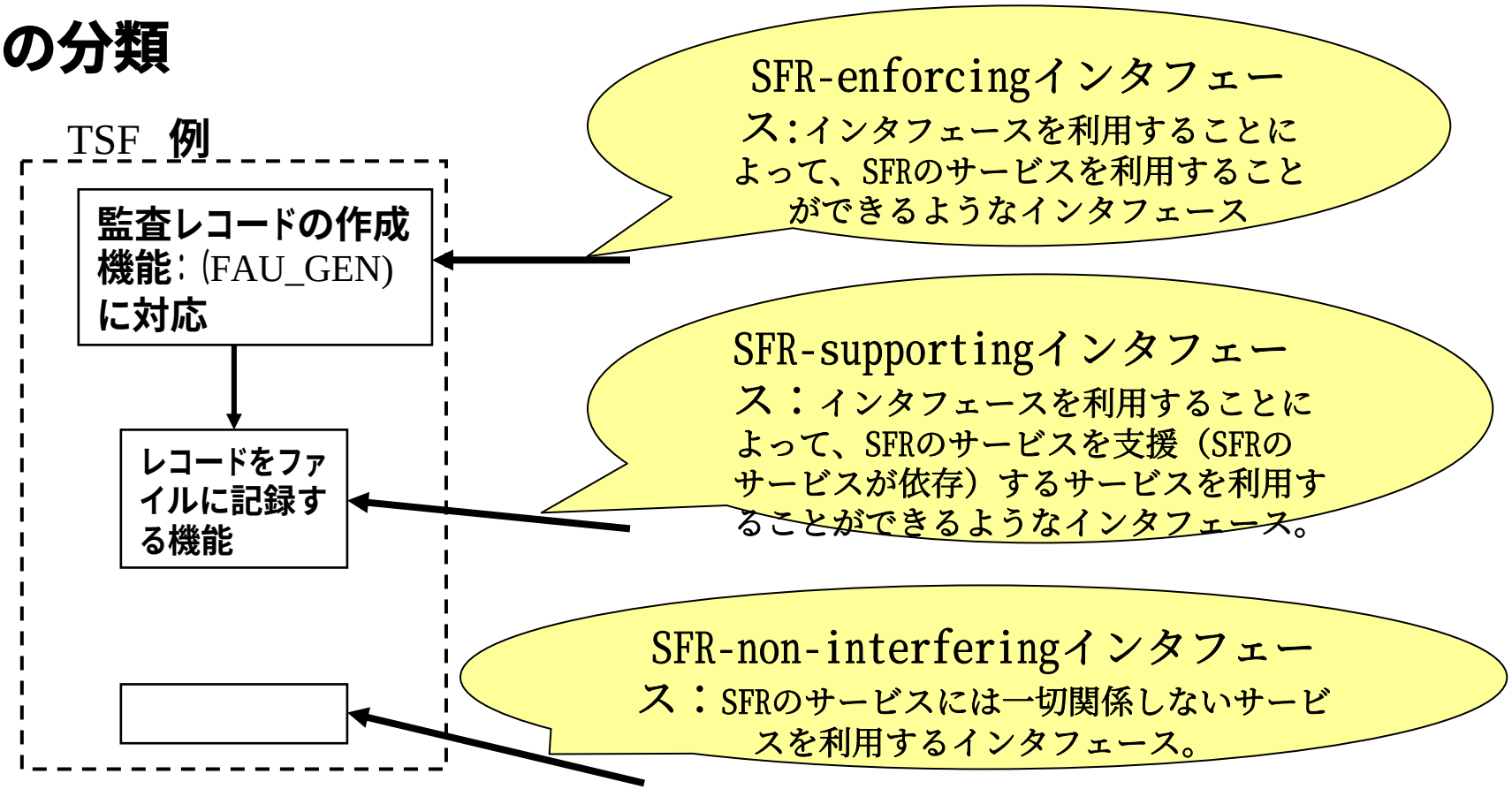
・TSFのサービス処理内容を記述（これは、ADV_TDS）するものではない。

・TSFがその運用環境からサービスを受けるためのインタフェースを記述するものでもない。

TSFIの識別


これはTSFIではない
（これは、ACO_REL）
TOE
TSF
SFRを満たすための実装部分
上記の初期化処理部分
上記のアーキテクチャ（自己保護、ドメイン分離、非バイパス）支援部分
TSFI
TSFにデータを供給したり、TSFからデータを受け取ったり、TSFからのサービスを受けるための手段
サブジェクト
外部エンティティ
物理的にTSFへのインタフェースは存在していても、TOEガイダンスの記述や運用環境の対策などで、TSFへのアクセス“手段”として存在しない場合は、TSFIではない。

TSFIの分類



注：評価を効果的に行うために、TSFIをSFRへの関連度合いから分類し、低い保証レベルでは、SFRそのもののサービスに直接関係しないインタフェース（ 例：**SFR-non-interfering**) に関わるエビデンスの作成負荷を軽減するためのものである。したがって、開発者が、エビデンス内容を区別する必要が無いと判断すれば、TSFIを分類する必要も無い。

TSFIの記述

インタフェースの*目的*：インタフェースの全般的な目標を上位レベルで記述。

インタフェースの*使用方法*：どのように使用されることが期待されているかを記述。

パラメタ：インタフェースへ（から）の明示的な入力、及び出力であり、そのインタフェースのふるまいを制御する事項の識別と、それが何であるかについて簡単な説明。

パラメタの記述：そのパラメタがどのような意味をもつかについて説明する。

インタフェースの*ふるまい*：インタフェースが何を行うかを記述。

エラーメッセージの記述：それが作製される条件、メッセージの内容、エラーコードの意味を記述。

機能仕様の記述例：管理者コマンド　Passwdの例

インタフェースの*目的*：管理者用のパスワードを設定する。

インタフェースの*使用方法*：　Passwd〈パスワード〉

パラメタ：パスワード

パラメタの記述：新パスワードの文字列。文字は、数字、英文字および、特殊記号を必ず１つ以上含む、８文字以上である。

インタフェースの*ふるまい*：旧パスワードを、入力された新パスワードで置き換える。

エラーメッセージの記述：入力されたパスワードが「パラメタ」の記述の項で述べた規則に反していた場合は、“入力されたパスワードは間違っています。再度、入力してください。”とのエラーメッセージを表示する。

FSPコンポーネント

コンポーネント	名称	エビデンスへの要求内容
ADV_FSP.1 (EAL1)	Basic functional specification	SFR-enforcing 及びSFR-supporting TSFIの目的、使用方法、及びパラメタ。SFR-non-interfering TSFIを分類している場合には、その根拠。SFRとTSFIとの対応。
ADV_FSP.2 (EAL2)	Security-enforcing functional specification	TSFの識別に基づいて（TOE設計）、すべてのTSFIの目的、使用方法、パラメタ、及びパラメタ記述。 さらに、SFR-enforcing TSFIに対して、インタフェースのふるまいと、TSFIの呼び出しに起因するエラーメッセージ識別。 SFRとTSFIとの対応。
ADV_FSP.3 (EAL3)	Functional specification with complete summary	ADV_FSP.2 に加えて、 SFR-supporting と SFR-non-interfering TSFIに対して、インタフェースのふるまいとTSFIの呼び出しに起因するエラーメッセージ識別。（それらがSFR-enforcing TSFIではないことを示すために)
ADV_FSP.4 (EAL4)	Complete functional specification	ADV_FSP.3に加えて、すべてのTSFI に対して、インタフェースの完全なふるまい。 TSFIの呼び出しに起因するエラーメッセージの意味。
ADV_FSP.5 (EAL5/6)	Complete semi-formal functional specification with additional error information	ADV_FSP.4に加えて、すべてのTSFIを準形式的スタイルで表現。TSFの呼び出しに起因しないすべてのエラーメッセージ識別。
ADV_FSP.6 (EAL7)	Complete semi-formal functional specification with additional formal specification	規定なし。

【アーキテクチャ(ADV_ARC)】 EAL2から

・セキュリティアーキテクチャ記述の詳細レベルと内容は、要求のADVと同等。

・TSFの特性（実現のための仕組）と正確な実装（実装規約など）に関わる記述。

・脆弱性分析とテストで、アーキテクチャーを確認。（モニタリング、TSFへの直接攻撃など）

セキュリティドメイン（有害なエンティティ用の環境）分離

・ドメイン分離の実現方法（他のエンティティ利用の場合は利用しているメカニズムと役割分担）
例：

ソフトウェアドメイン分離の実装のために、TSFはソフトウェア保護命令やコーディング規約を実装する。

・ドメイン分離が不要な場合はその理由（有害なエンティティとのインタフェース無しなど）を記述。

TSF自己保護

・TSF（実行コードやオブジェクトを含む）への干渉や改ざんからの保護方法

例：システムアドレス空間から利用者アドレス空間を分離

・入力データの処理（特権モード、特権レベル、コーディング規約など）

・初期化処理（セキュアな初期状態、処理コードの保護）

TSFの非バイパス性

・SFR-enforcing TSFIを使用してTSFをバイパスできる操作やモードが存在しないことの説明（なぜを）

・非SFR-enforcing TSFIを使用してTSFをバイパスできる操作やモードが存在しないことの説明（なぜを）

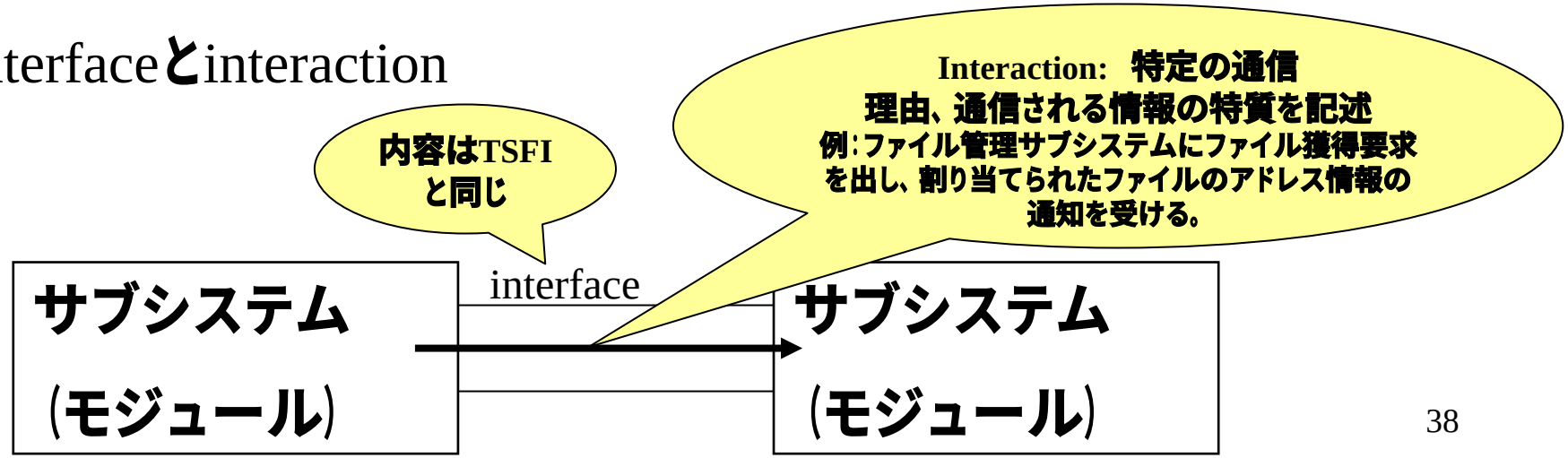
・非バイパス性は、すべてのSFR（機能と保護資産）に等しく適用

例：サイドチャネル攻撃が可能な場合、内部のランダム時計、二重化配線など、このサイドチャネル攻撃を防止するメカニズムを説明する。

【TOE設計（ADV_TDS)】

- **TOE設計記述の目的：**
  - **TSFの境界を明確にする。**
  - **TSFがどのようにSFRを実装しているかを説明する。**
- **TOEの開発（保守）に必要な情報のみをTOE設計記述に記載する。**
  - **複雑なTOE（多数のSFR)では、サブシステム/モジュールの階層構造**
  - **単純なTOE（少数のSFR)では、モジュールのみ**
    （サブシステム要求は満足しているとみなす）

- interfaceとinteraction



サブシステム

・TSF境界を識別する。

SFRの動作に関係するサブシステムはTSFの一部。

・TSFの構成を明確にする。

SFRに対して、TSFがどのように機能するかを記述

- SFR enforcing：SFRに関わる処理を実施する部分を含むサブシステム

SFR処理のためのメカニズムを記述、SFR-enforcing TSFIの実装部分を含む

- SFR-supporting：SFRの処理には直接関係しないが、その処理には必要な部分を含むサブシステム

- SFR-non-interfering：SFRの処理には無関係

モジュール

・実装表現の内容を説明した最下位層（モジュールと実装表現の間に他の設計記述は存在しない）の設計単位

・ADV_TDS.1: Basic design, TDS.2: Architecture designではサブシステムに関わる情報の提供を要求しているが、TOEの特質によって、サブシステムの記述が不要であれば、モジュールの情報によって、これらコンポーネントの要求は満足しているものとみなす。

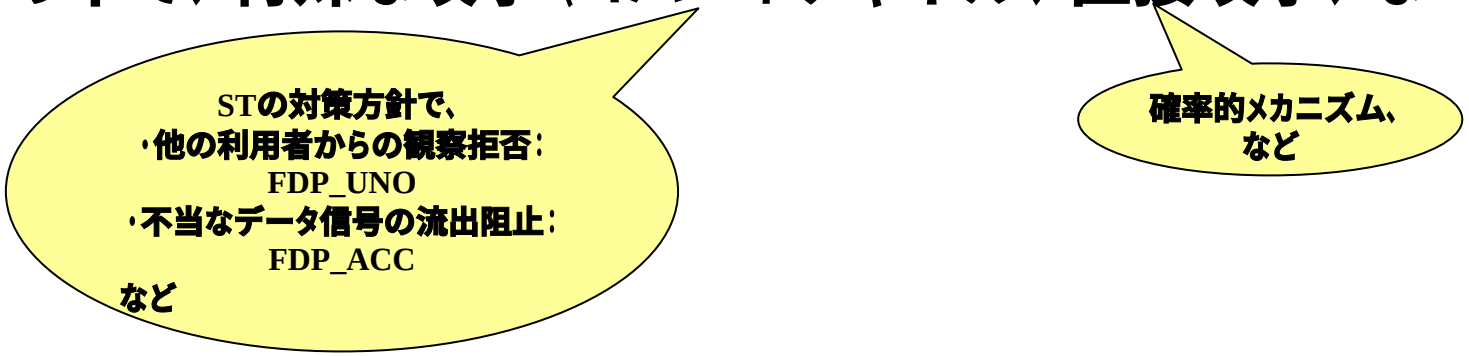
・SFR enforcing、SFR-supporting、SFR-non-interferingの考え方はサブシステムと同じ。

・ソースコードに記述されるコメント（ボックスコメント）は、モジュールに要求される情報が含まれていれば、モジュール記述とみなせる。ただし、コードに対応したコメントだけでは、まとまった説明ではないため、モジュール記述としては不適切。

【Vulnerability Assessment (AVA)】

・特定の攻撃方法に依存しない、一般的（幅広い）評定を要求。

　その評定の中で、特殊な攻撃（コバートチャネル、直接攻撃、など）も考慮。



開発に関わる（機能、構造、実装）脆弱性

　　TSF自己保護の破壊、TSFへの直接攻撃、TSFドメイン分離の破壊、TSFバイパス、など

運用に関わる脆弱性

　　TOE構成の不備、TOE誤使用、など

開発者分析と評価者分析について

・CC V2の脆弱性分析は、開発者が脆弱性分析を行って、その証拠資料を評価者に提供し、評価者はその証拠資料の内容が要件の要求事項を満足していることを確認するという、開発者主導のものであった。

・CC V3では、実際の評価に即して、脆弱性評価は評価者が主導するように変更した。

・一番低い脆弱性分析レベルでは、明白な脆弱性を検出するために、評価者は公開されている脆弱性に係る情報を分析して、侵入テストのための入力にする。

・上位の脆弱性分析では、開発者による、潜在脆弱性分析を要求している。

・評価者は、TOEへの侵入テストを実施する際に、基本（AVA_VAN.1及びAVA_VAN.2）、拡張された基本（AVA_VAN.3）、中（AVA_VAN.4）、または高（AVA_VAN.5）レベルの攻撃能力を持つ攻撃者の役割を想定しなければならない。

明白な脆弱性について

V3では、“公開情報（パブリックドメイン）に基づいて攻撃を受ける脆弱性、および、脆弱性分析評価以外のために、評価用提供物を評価している中で、評価者が検出する脆弱性。”

「一般的な脆弱性に関するガイダンス」を規定（CEMのAnnex)

バイパス、不正改ざん、直接攻撃、監視、誤使用、などについて、チェックリスト的に使用できるガイダンスを規定。

例：【バイパス】

(1)TOEのインタフェースの悪用、またはTOEと相互作用することができるユーティリティの悪用

①事前に定義されたTSFIの呼出し順序の変更

②追加のTSFIの呼出し

③想定されていない状況または目的でのコンポーネント使用

④実装表現の不正挿入

⑤チェックと使用の時間差の悪用

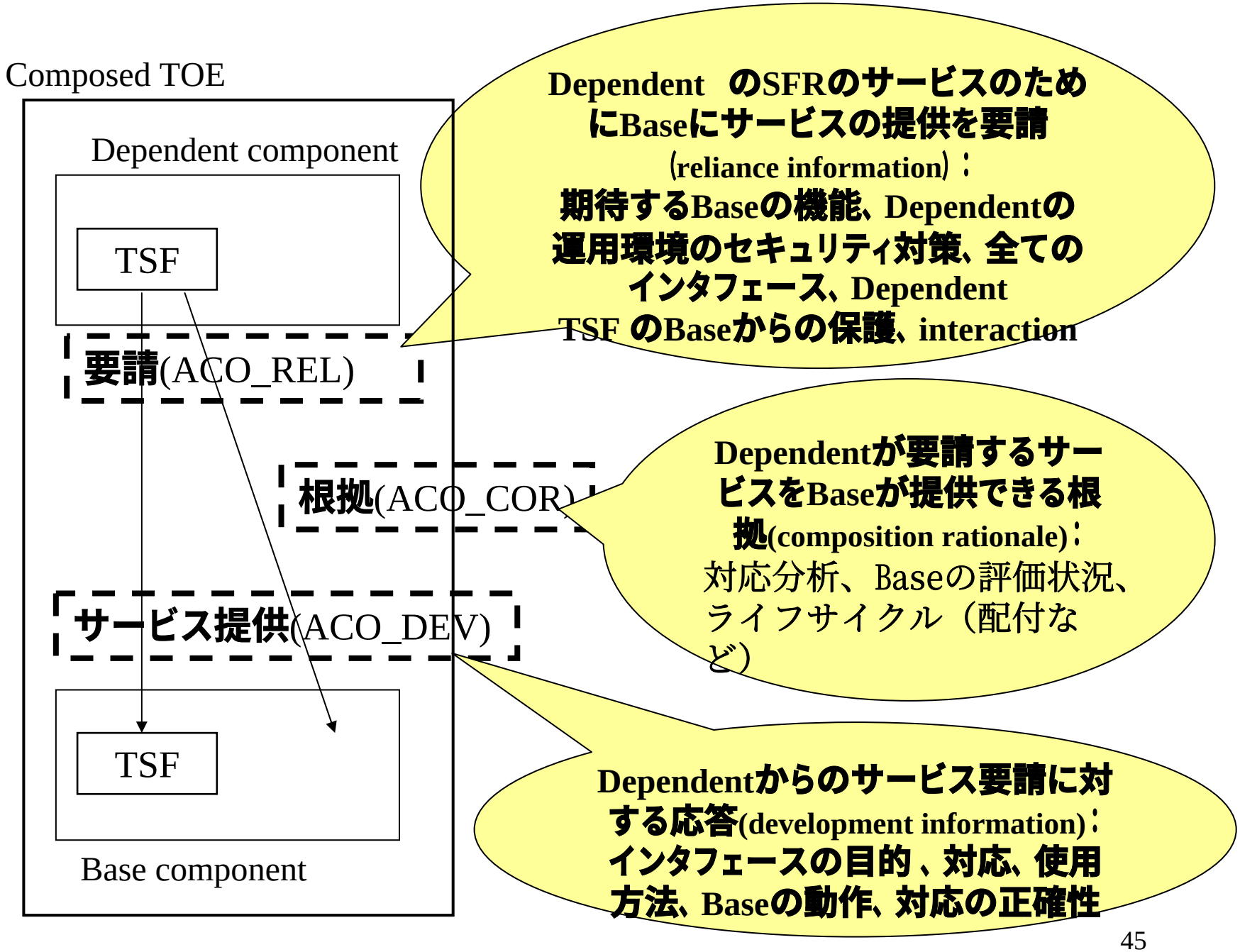
【コンポジション　ACO】

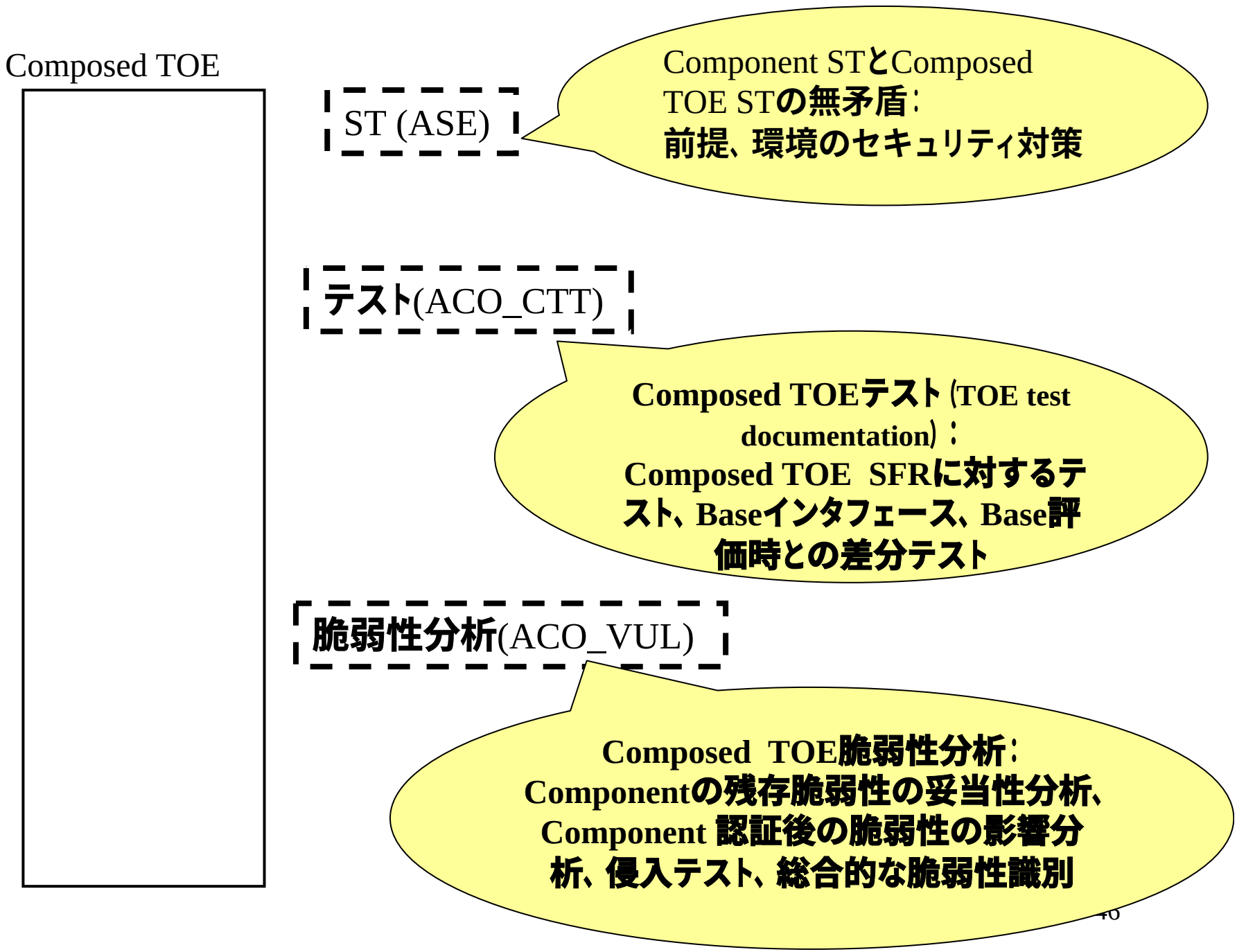
・個別に評価された複数のTOE(dependent/ base component)を結合して、1つのTOE (composed TOE)を作成した際の保証に係わる要件。（構成するTOE：component TOEの再評価は行わない）

・保証は結合によって各componentの評価結果とcomposed TOEとに矛盾（STの環境のセキュリティ対策、TSFI,など）が無いことの検証。

・保証にかかわる基本的な要求内容は、単一のTOEに対するADV，ATE，AVAの考え方を適用。

・Dependent componentの開発者は、composed TOEの評価のためにエビデンスを提供。


Composed TOE
Dependent component
TSF
要請(ACO_REL)
根拠(ACO_COR)
サービス提供(ACO_DEV)
TSF
Base component
Dependent のSFRのサービスのためにBaseにサービスの提供を要請(reliance information)：期待するBaseの機能、Dependentの運用環境のセキュリティ対策、全てのインタフェース、Dependent TSF のBaseからの保護、interaction
Dependentが要請するサービスをBaseが提供できる根拠(composition rationale)：対応分析、Baseの評価状況、ライフサイクル（配付など）
Dependentからのサービス要請に対する応答(development information)：インタフェースの目的 、対応、使用方法、Baseの動作、対応の正確性


Composed TOE
ST (ASE)
Component STとComposed TOE STの無矛盾：
前提、環境のセキュリティ対策
テスト(ACO_CTT)
Composed TOEテスト（TOE test documentation）：
Composed TOE SFRに対するテスト、Baseインタフェース、Base評価時との差分テスト
脆弱性分析(ACO_VUL)
Composed TOE脆弱性分析：
Componentの残存脆弱性の妥当性分析、
Component 認証後の脆弱性の影響分析、侵入テスト、総合的な脆弱性識別