CC Version 3.1 トピックス紹介

ー V2に対して何が変更されたのか ー

平成19年5月9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

CC V3.1の基本的な考え方

CC/CEMは“セキュリティ機能要件（SFR）の保証”を確保するための規格である。

“保証(assurance)”とは、

V2の定義：エンティティがそのセキュリティ対策方針を満たしていることを信頼するための根拠。

V3の定義：TOEがSFRを満たしていることを信頼するための根拠。

- **“SFRの保証”にかかわる概念、定義、アクションの明確化**
- **より実質論へ（STはセキュリティ目標（SFR)の記述、脆弱性の評定が信頼の根拠の主要な要素）**

目次

- V3.1全般
- ST
- 機能コンポーネント
- 保証コンポーネント
- 運用

V3.1 全般

- 評価規格
- TOE
- TSF
- セキュリティ機能の記述

評価規格

評価要件を満足（評価合格）するためには、**評価方法**（CEM）に規定の必須および強い要請を満足しなければならない。

◆必須は、「**評価者は・・・しなければならない** (The evaluator shall)。」と記述されている。この記述は、CEMの各ワークユニットの最初のセクション部分である。

◆強い要請は、「**評価者は・・・すべきである** (The evaluator should)。」と記述されている。この記述は、CEMの各ワークユニットのセクションに混在しているので、注意が必要である。

注：必須および強い要請は、「評価者は・・・しなければならない/するべきである。」で記述されているものとする。

TOE

【定義】

V2:評価の対象となるIT 製品またはシステム、及び関連する管理者/利用者ガイダンス文書。

V3:ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び/またはハードウェアのセット。

【背景（考え方）】

◆ IT機能であることだけがTOEの条件（IT機能であること以外の制限はしない）

◆ V2定義の製品もシステムも、評価の上で差が無い（V2定義のシステムもCC認証の対象）

TSF

【定義】

V2：TSP（TOEセキュリティ方針：TOE 内での資産の管理方法、保護方法、及び配付方法を規定する規則のセット）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

V3：SFRを正確に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

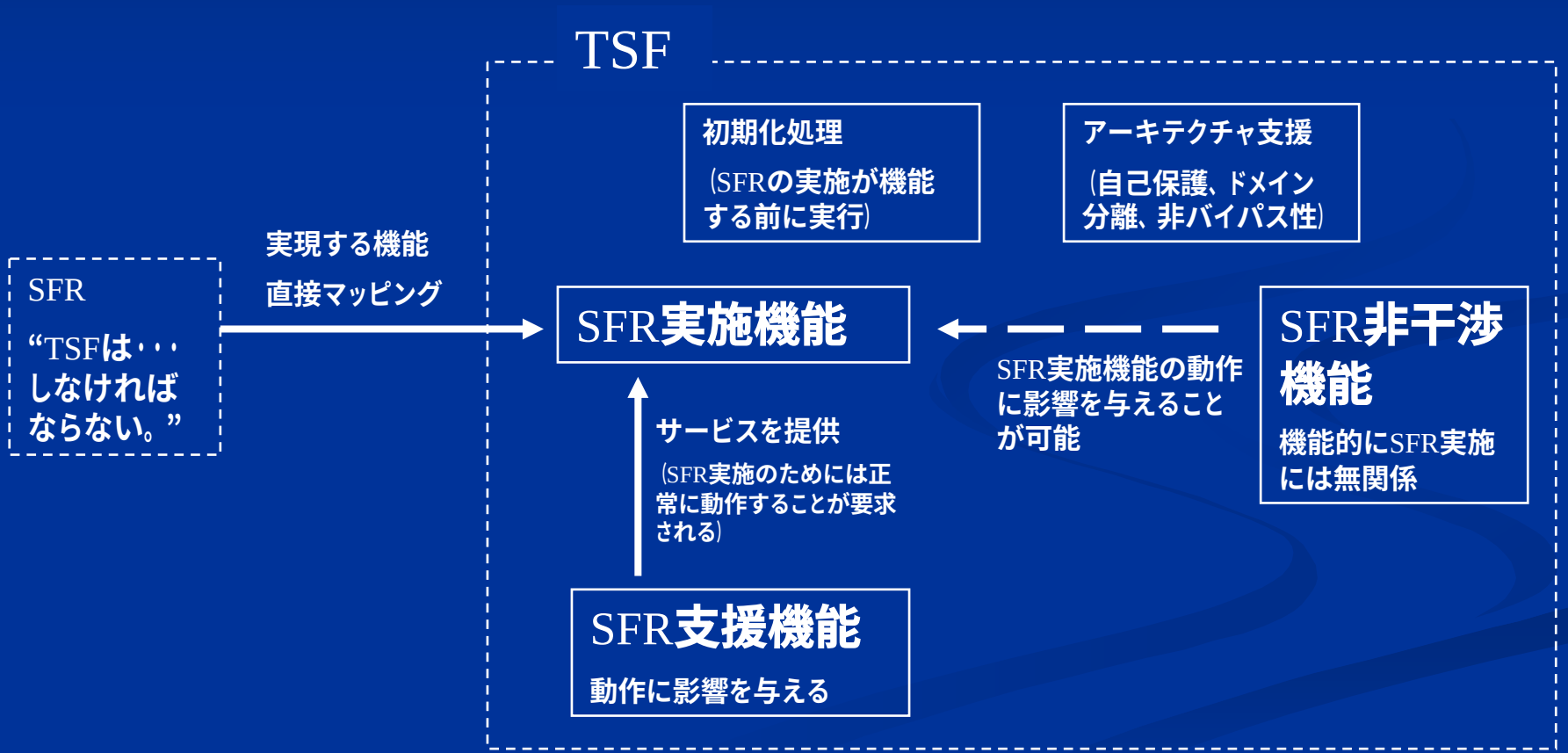
【背景（考え方）】

“SFRの保証”の明確化

TSFの構成要素（ SFRを正確に遂行するために必要なすべての部分）

◆ **SFRを直接実施する機能**

◆ **SFRを侵害する可能性のある機能も含めた、SFRを直接実施しないが間接的にSFRの実施に寄与する機能（立ち上げ時に呼び出され、TSFをそのセキュアな初期状態にする　TOEの各部分を含む）**



開発者は仕様書に記述する情報量を軽減したい場合のみ、SFR実施、支援などの識別をすることができる。

セキュリティ機能の記述

V2：セキュリティ機能(security function)

V3:　セキュリティ機能性（security functionality）
SFRを実施するセキュリティ機能が、TOEにおいてどのように全体としてSFRを実現しているかに関する特性。

セキュリティ機能性を記述：SFRをTOEでどのようにして実現しているか（どのように機能するか）について記述（SFRは何であるかを機能面から記述するものではない）

注：

・自己保護機能を記述：TSF自体の保護をTOEでどのようにして実現しているかについて記述（自己保護は何であるかを機能面から記述するものではない）

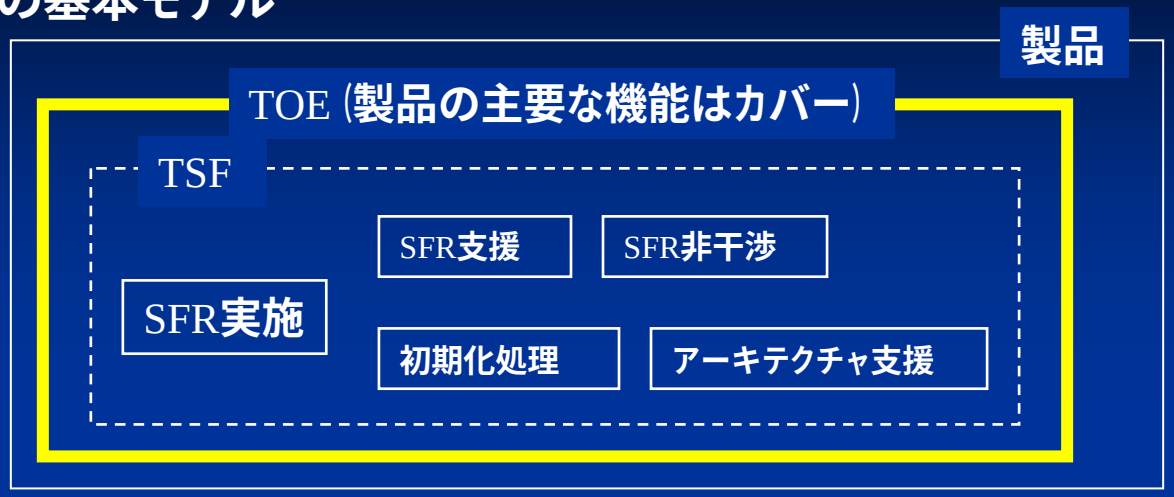
・TOE要約仕様（ASE_TSS)：TOE 要約仕様は、TOE がどのように各SFR を満たすかを記述しなければならない

ST

- TOE範囲の規定
- SFR
- 資産
- PP適合

TOE範囲の規定

TOE範囲の基本モデル



どのように考えるか

TOE範囲の規定は自由裁量、しかし

アーキテクチャ記述によって存在が明らかになる

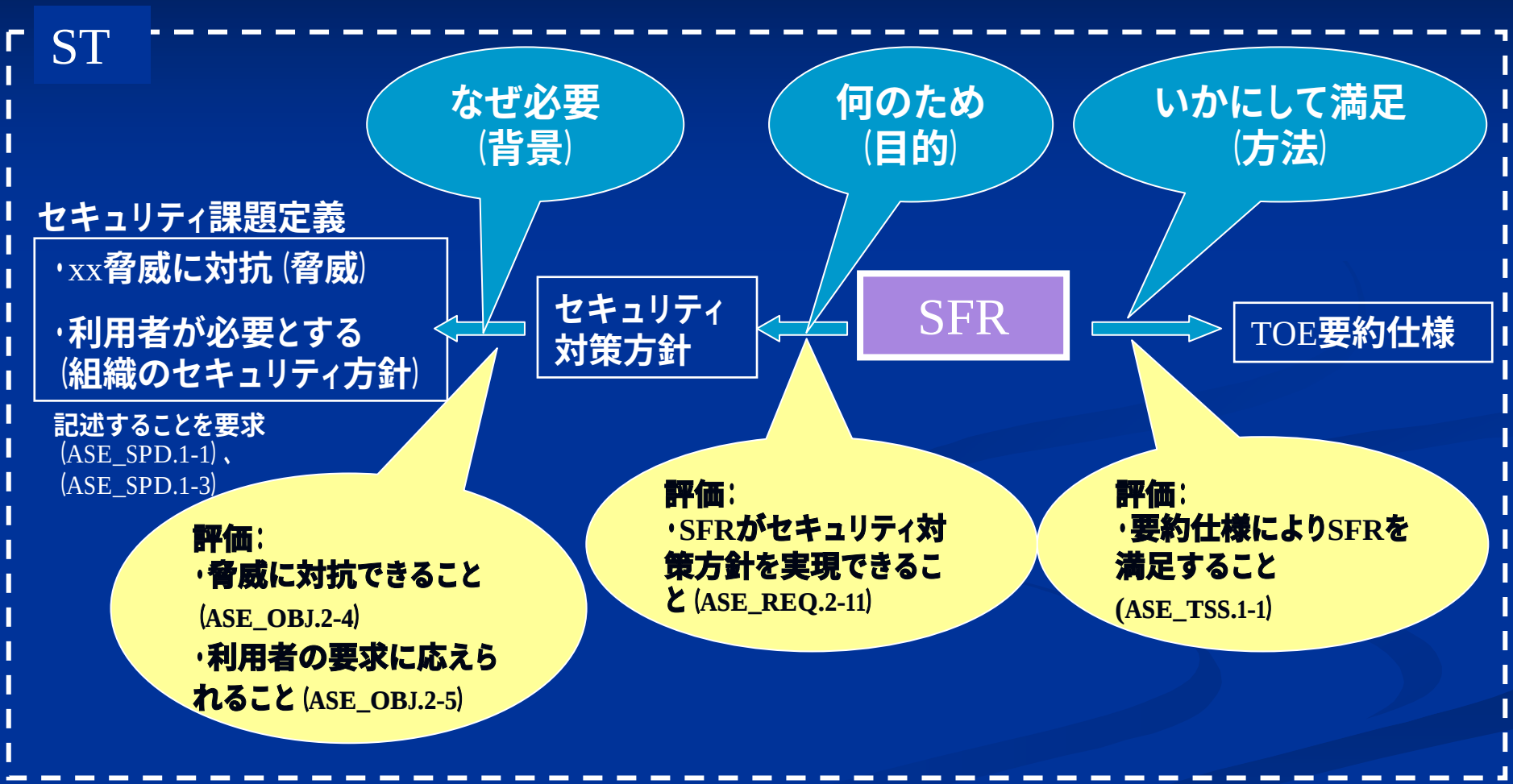
・ベース製品のSFR支援機能の保証は前提とする。

◆当該製品のSFR支援などの機能保証はTOE外（運用環境）なので前提⇒SFR支援などの機能の保証が必要（自己矛盾）⇒TOEの範囲を拡大（SFR非干渉を考慮すると、TOE＝製品となる）

セキュリティ機能の保証から見ても、SFR実施部分のみの評価では、その有益性を損なう。

SFR

STはSFRを正確に規定し、その背景や実現方法を記述する。



セキュリティ課題定義は与件（axiomatic：公理）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。（セキュリティ対策方針との関連で矛盾がなければ問題なしとの意）

TOEにとって適切なSFRの規定

TOE≠製品の場合、TOE名称≠製品名称にする (ASE_INT.1-4)

TOEおよびそのセキュリティ機能の特徴はTOE種別から想定されるものにする (ASE_INT.1-7)

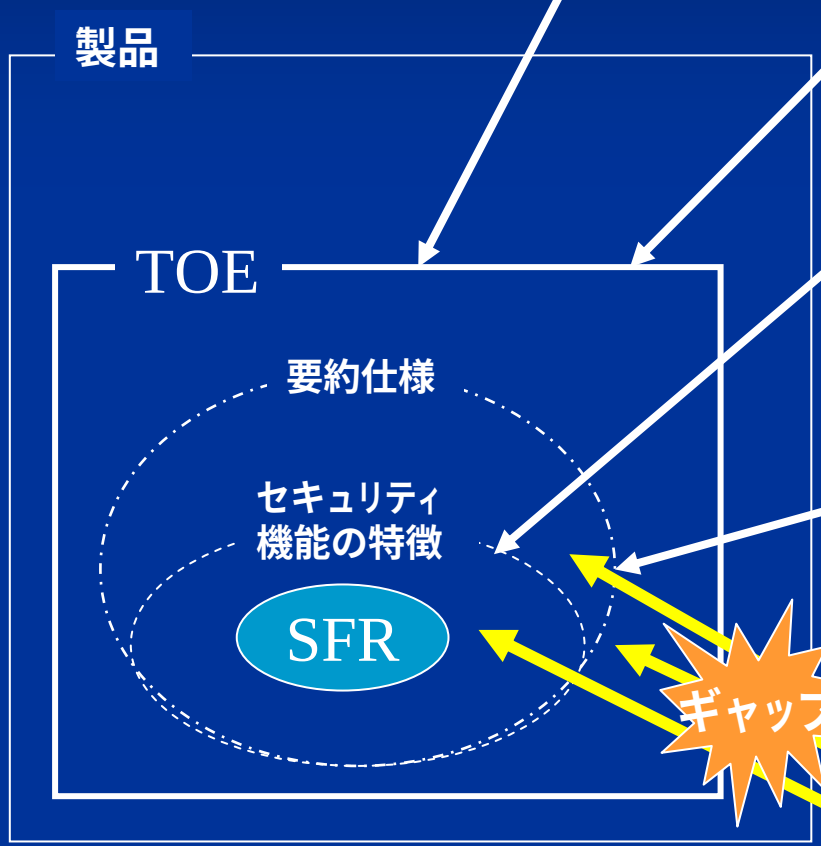
TOE種別に対する客観的な判断基準は無い

TOEのセキュリティ機能の特徴に係わる記述は、TOE概要、TOE記述、TOE要約仕様で順次、詳細化し、矛盾が無い記述にする (ASE_INT.1-5), (ASE_INT.1-10), (ASE_INT.1-11), (ASE_TSS.1-2)

セキュリティ機能の特徴の詳細化に対する一貫性

TOE要約仕様はSFRをどのように実現するかを記述する (ASE_TSS.1-1)

SFR⇒要約仕様への対応のみ



問題と対策

- TOE記述とSFR（要約仕様）との一貫性
- TOE要約仕様とSFRとの一貫性

⇒ASE_OBJに要求を追加（V2.3　ASE_DES.1-6相当）

V2.3：ASE_DES.1-6 評価者は、TOE 記述がST のその他の部分と一貫していることを決定するために、ST を検査しなければならない。

解釈を適用

ASE_TSS.1-2 評価者は、TOE要約仕様がTOE概要及びTOE記述と一貫していることを決定するために、そのTOE要約仕様を検査しなければならない。

TOE概要に記述のセキュリティ機能の特徴がTOE記述、TOE要約仕様で矛盾なく詳細化されていることの検査に加えて、TOE記述に記載のTOE機能から消費者が期待するセキュリティ機能がTOE要約仕様に記述されていることも検査する。

ASE_TSS.1-1 評価者は、TOEがどのように各SFRを満たすかをTOE要約仕様が記述することを決定するために、そのTOE要約仕様を検査しなければならない。

SFRをTOE要約仕様が満足していることの検査に加えて、SFR に対応しない記述がTOE要約仕様に存在しないことも検査する。

資産

定義

V2:TOE の対抗策が保護すべき情報または資源。

V3:TOEの所有者が一般に価値を認めるエンティティ。

CCは資産を攻撃から護るために、セキュリティ機能が適切であること（リスク管理）を検証するための規格ではない。

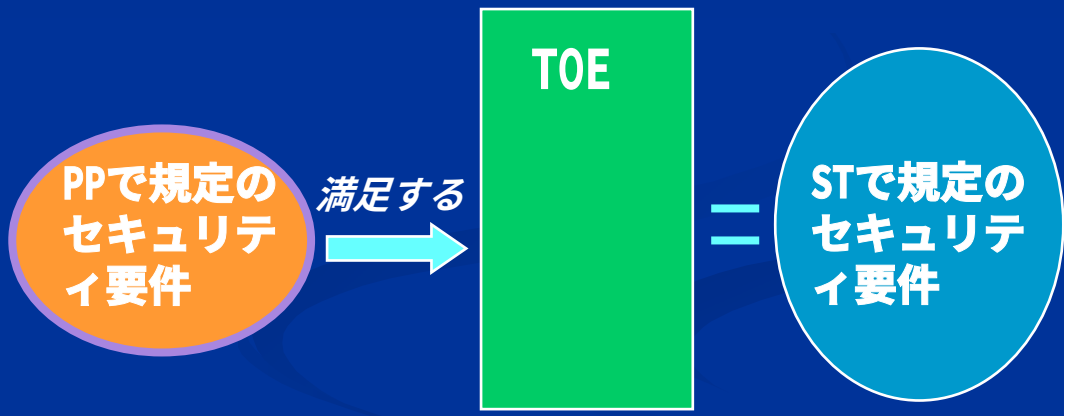
PP適合

正確適合

利用例：PPに必要最小限のSFRを規定して、製品調達時に適合を要求

論証適合

利用例：PPにセキュリティ対策方針を規定して、ガイダンスとして使用



STの規定内容を満足するTOEはPPの要求内容も満足する

適合対象PPのPP適合ステートメントに矛盾しないこと

機能コンポーネント

- V2からの主な変更点
- サブジェクトとオブジェクト
- ユーザデータとTSFデータ
- 翻訳版の利用

V2からの主な変更点

・FAU_STG:**保護対象の監査レコードは監査証跡のレコードであり、一次ファイル上の監査レコードではないことを明確化。**

・TSC（TSF**制御範囲**）⇒TOE、TSF（**で管理される**）

・FPT_RVM、FPT_SEP**が削除**

・**変更した保証コンポーネント**（ADV_SPM.1、AVA_CCA.1、AGD_ADM)**への依存性が削除、または、変更**

サブジェクトとオブジェクト

【定義】

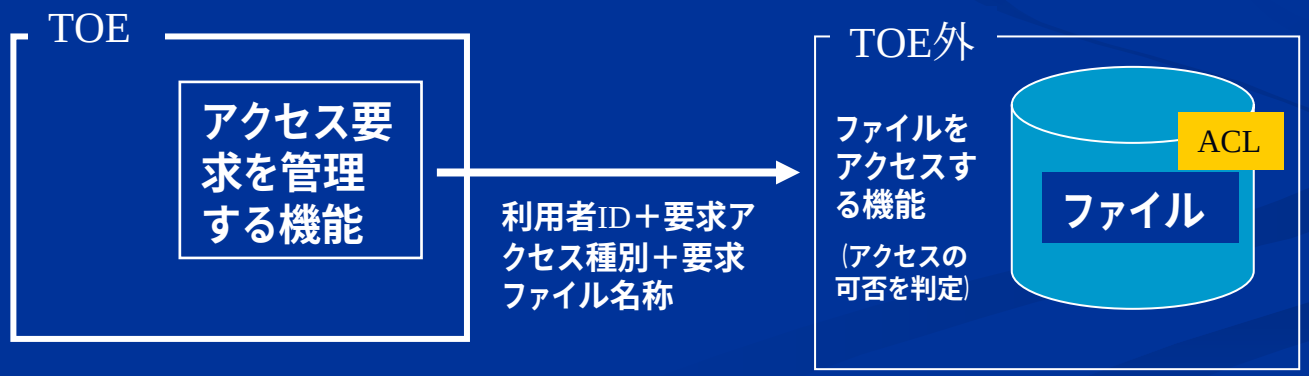
V2

サブジェクト：実行すべき操作の原因となるTSC 内のエンティティ。
オブジェクト：情報を内蔵または受信し、サブジェクトによる操作の実行対象となるTSC 内のエンティティ。

V3

オブジェクト：情報を格納または受信し、サブジェクトによる操作の実行対象となるTOE内の受動的なエンティティ
サブジェクト：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

TOEが管理の対象とするエンティティをサブジェクト、オブジェクトとして正確に定義する。



TOEではファイルを管理していないため、オブジェクトにファイルを規定することはできない。

(そもそも、アクセス制御SFRの機能ではないという問題はあるが)

サブジェクトとオブジェクトの指定

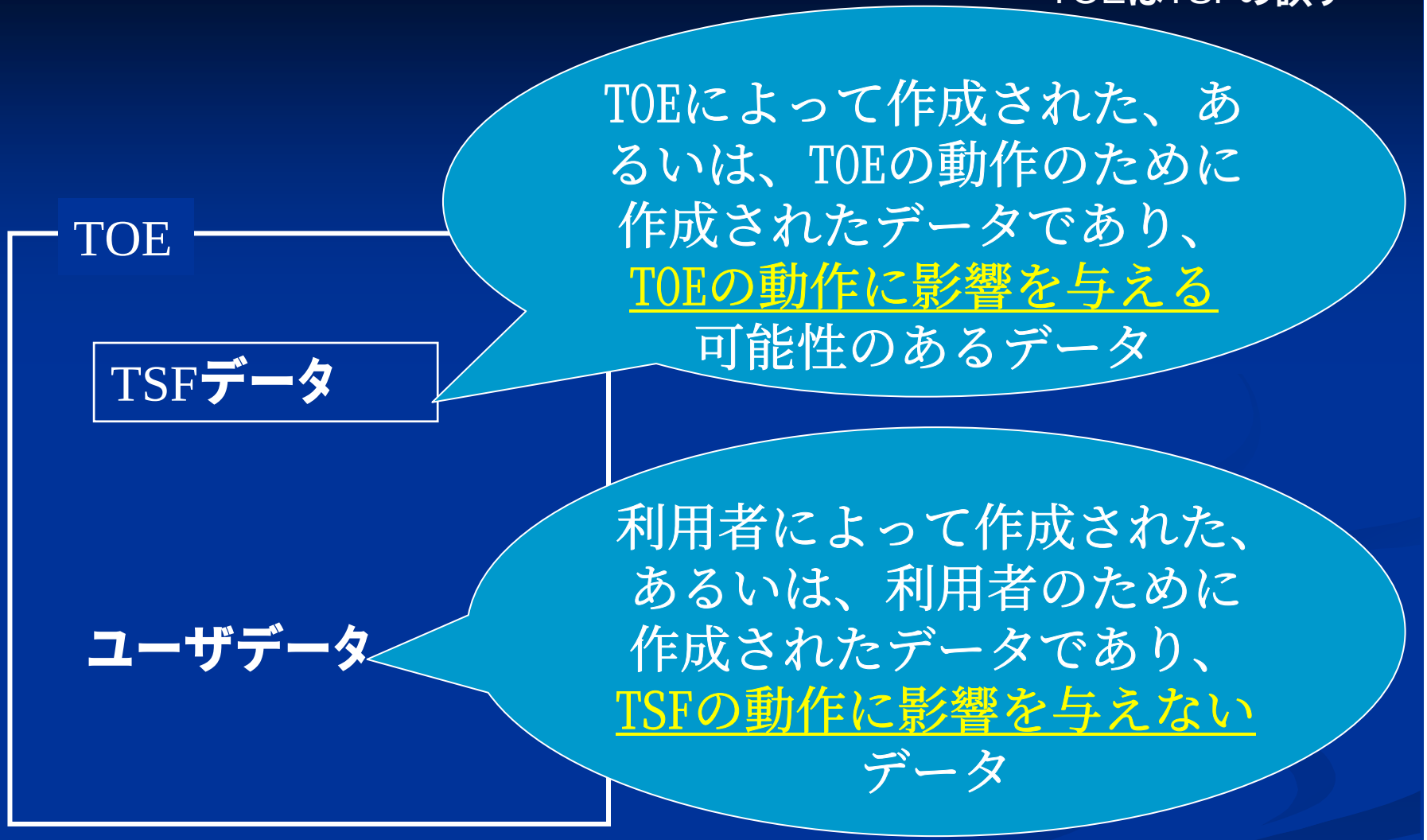
【問題認識】
全てのオブジェクトやサブジェクトなどを指定させないで、一貫性の評価を要求していたので完全な検証ができなかった。

【改善】
V3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）
評価者は、SFR及びSARで使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語が定義されていることを決定するために、STを検査しなければならない。
（ASE_REQ.1-3）

ユーザデータとTSFデータ

TOEはTSFの誤り



定義はV2と同じ

TSFデータは、SFRの要求に応じて決定を下すときにTSFが使用する情報である。
TSFデータの例として、監査情報、クロック、及びその他のTSF構成パラメタがある。

TSFデータは、例えば、パスワード、キー、監査データ、TSF実行コードなどのTSFに重要なデータである。

TSFデータと実行可能コードの完全性

（パート2）

翻訳版の利用について

翻訳版のV3.1を規格として使用する場合には、必ず、V3.1用のパート２（V2.3に対して用語や表現を変更している）から機能コンポーネントをコピーする。

（**ASE_REQ.1-1**：評価者は、セキュリティ要件のステートメントが**SFR**を記述していることをチェックしなければならない。）

保証コンポーネント

- V2からの主な変更点
- TSFI
- アーキテクチャ
- TOE設計
- 脆弱性評定
- ライフサイクル/ガイダンス
- コンポジション

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　機能仕様からSFRへの追跡を提供しなければならない。
　　追跡は、機能仕様でのTSFIに対するSFRの追跡を実証するものでなければならない。

・非形式的/ 準形式的 SPM削除

STで規定するセキュリティ機能要件以外の何か（非形式的/準形式的 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。

・アーキテクチャ記述（ADV_ARC)追加

・統合TOE（ACOクラス)追加

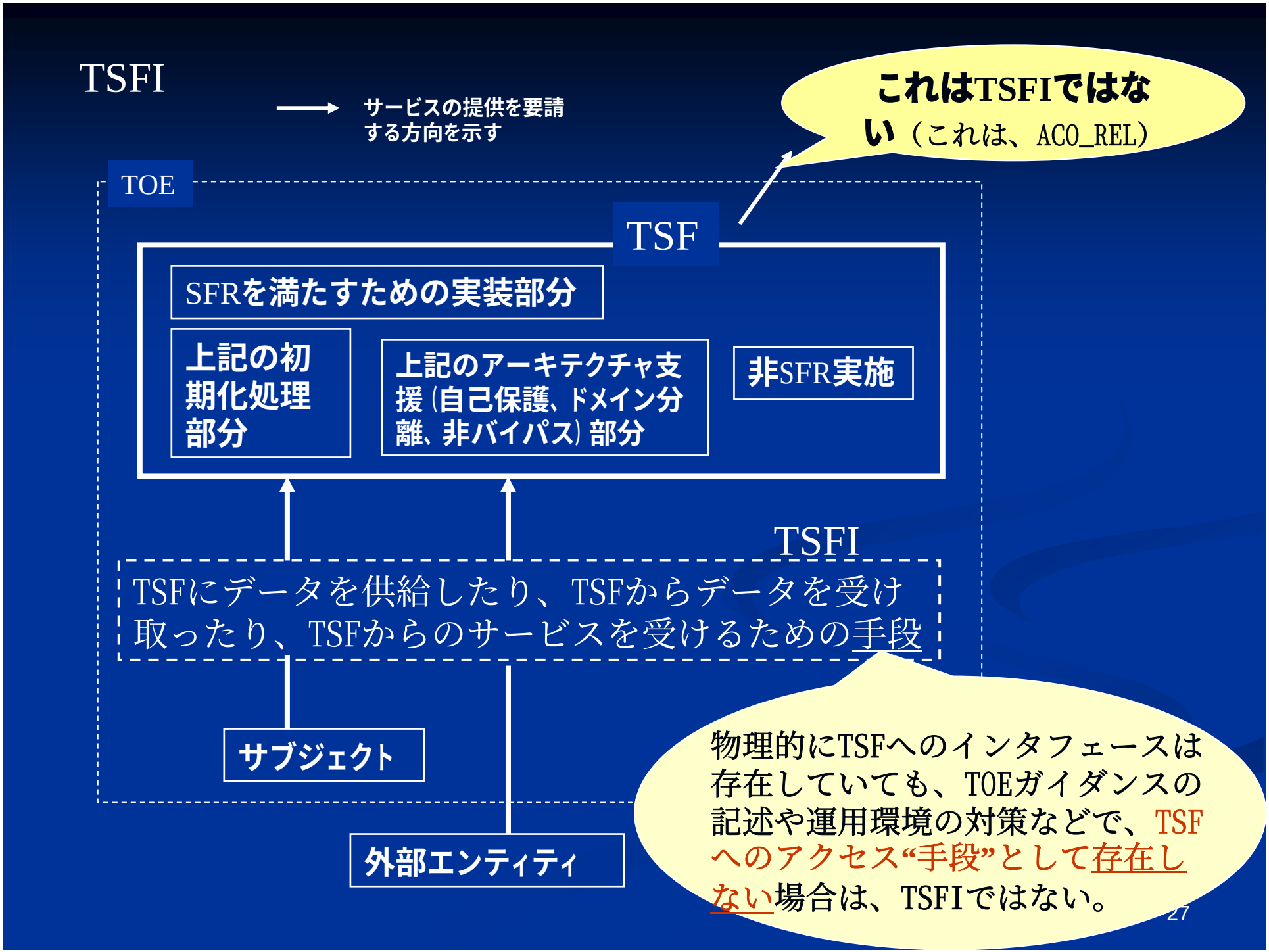
TSFI

【定義】

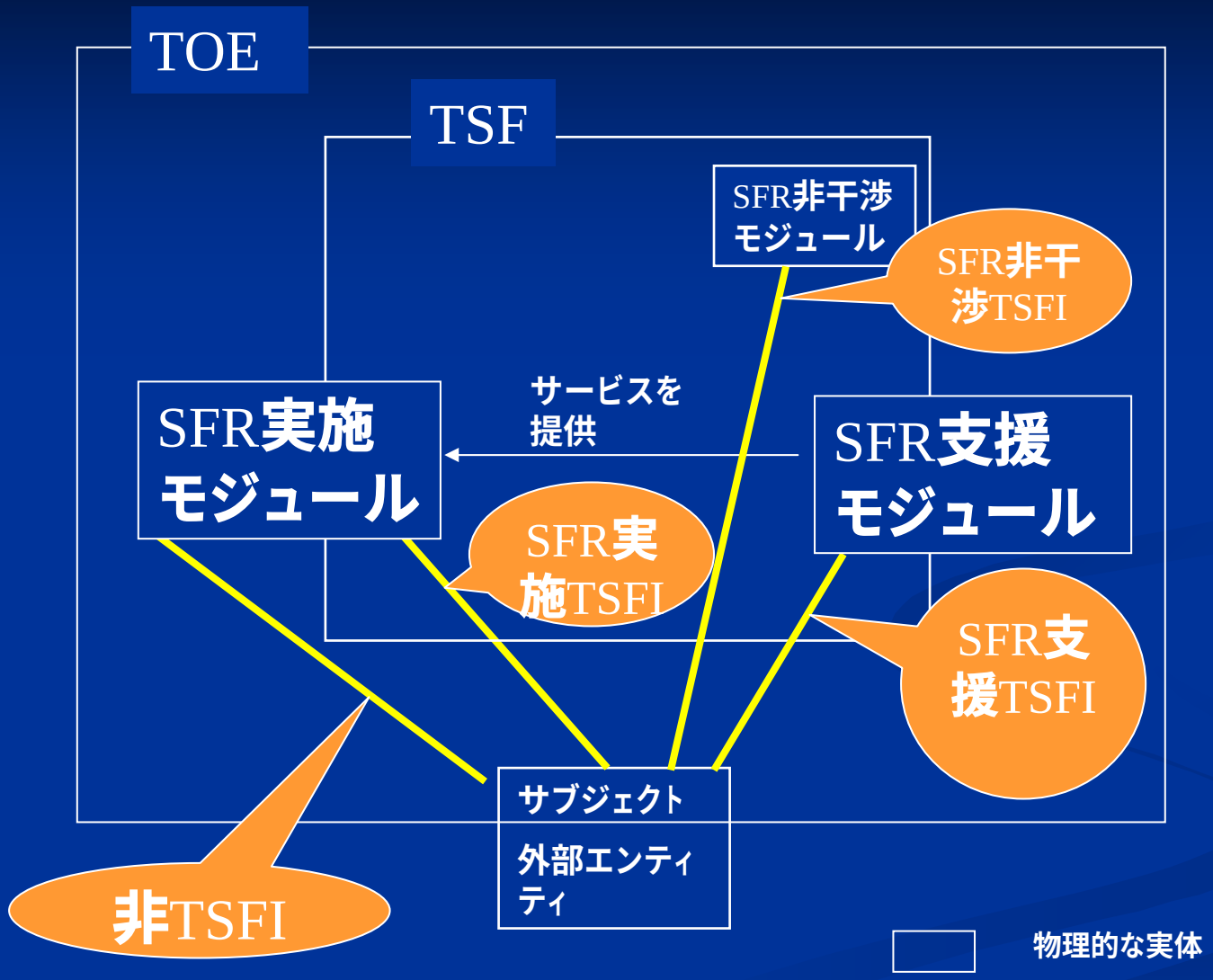
V2：対話（マンマシンインタフェース）またはプログラミング（アプリケーションプログラミングインタフェース）の如何にかかわらず、それを介してTOE 資源にアクセスしたり、TSF が仲介したり、TSF から情報を取得したりするインタフェースのセット。

V3: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

外部エンティティの定義：
V2:TOE外のIT製品やシステム
V3: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)。


TSFI
サービスの提供を要請する方向を示す
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支援（自己保護、ドメイン分離、非バイパス）部分
非SFR実施
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の種別


TOE
TSF
SFR非干渉モジュール
SFR非干渉TSFI
サービスを提供
SFR実施モジュール
SFR支援モジュール
SFR実施TSFI
SFR支援TSFI
サブジェクト
外部エンティティ
非TSFI
物理的な実体

アーキテクチャ

TSFがセキュリティ機能を提供できる保証基盤

TOE開発に際して利用できる（必要となる）情報に基づいて記述する。

自己保護

・外部エンティティの操作によるTSF破壊から保護する特性

他のITエンティティに依存する場合には、TSFとITエンティティの役割を明確にする

・利用者入力の処理ミスによるTSF破壊からの保護

・初期化時のTSF保護メカニズム

ドメイン分離

・信頼できない能動的なエンティティをドメイン分離して相互に干渉できなくする特性

他のITエンティティに依存する場合には、TSFとITエンティティの役割を明確にする

信頼できないエンティティドメインが存在しない場合は不要（理由を記述）

非バイパス性

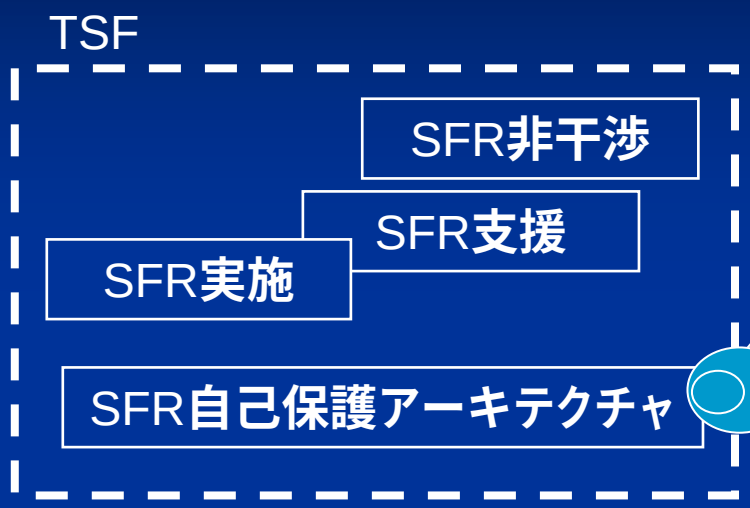
・TSFが適切なタイミングで常に呼び出され、回避できない特性

・SFR実施インタフェースにはTSFをバイパスする操作やモードは存在しないことの論証

・非SFR実施インタフェースによって、TSFのバイパスは不可能であることを論証

「できないこと」の論証であることに注意

自己保護



TSFを保護するための仕組み

例

機能/サブシステムレベル：

・ドメイン分離、プロセス分離

モジュール/実装レベル：

・コーディング規約（バッファオーバフロー対策、入力パラメタチェックなど）

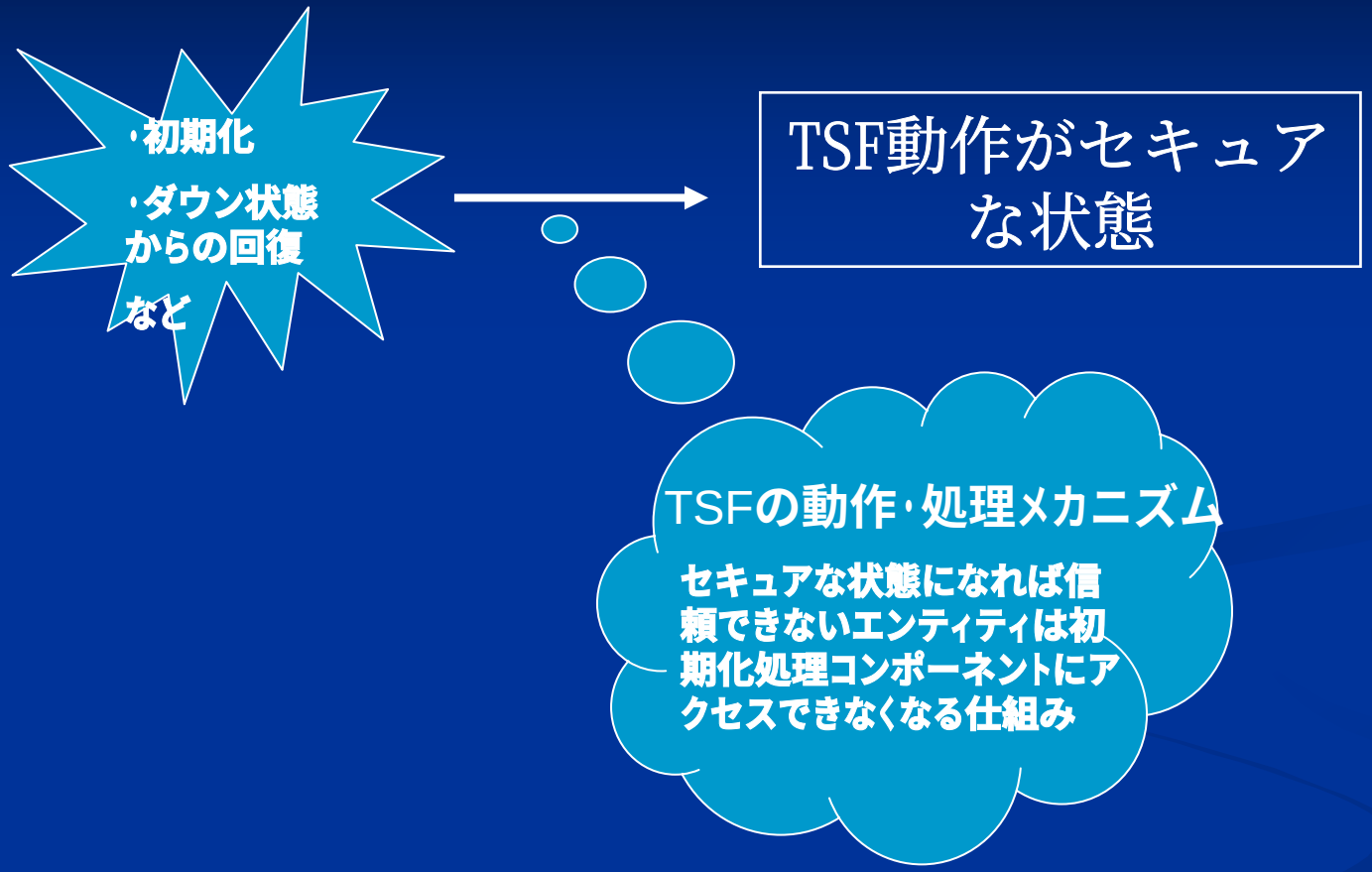
IT環境の機構を利用

例

メモリ保護機構

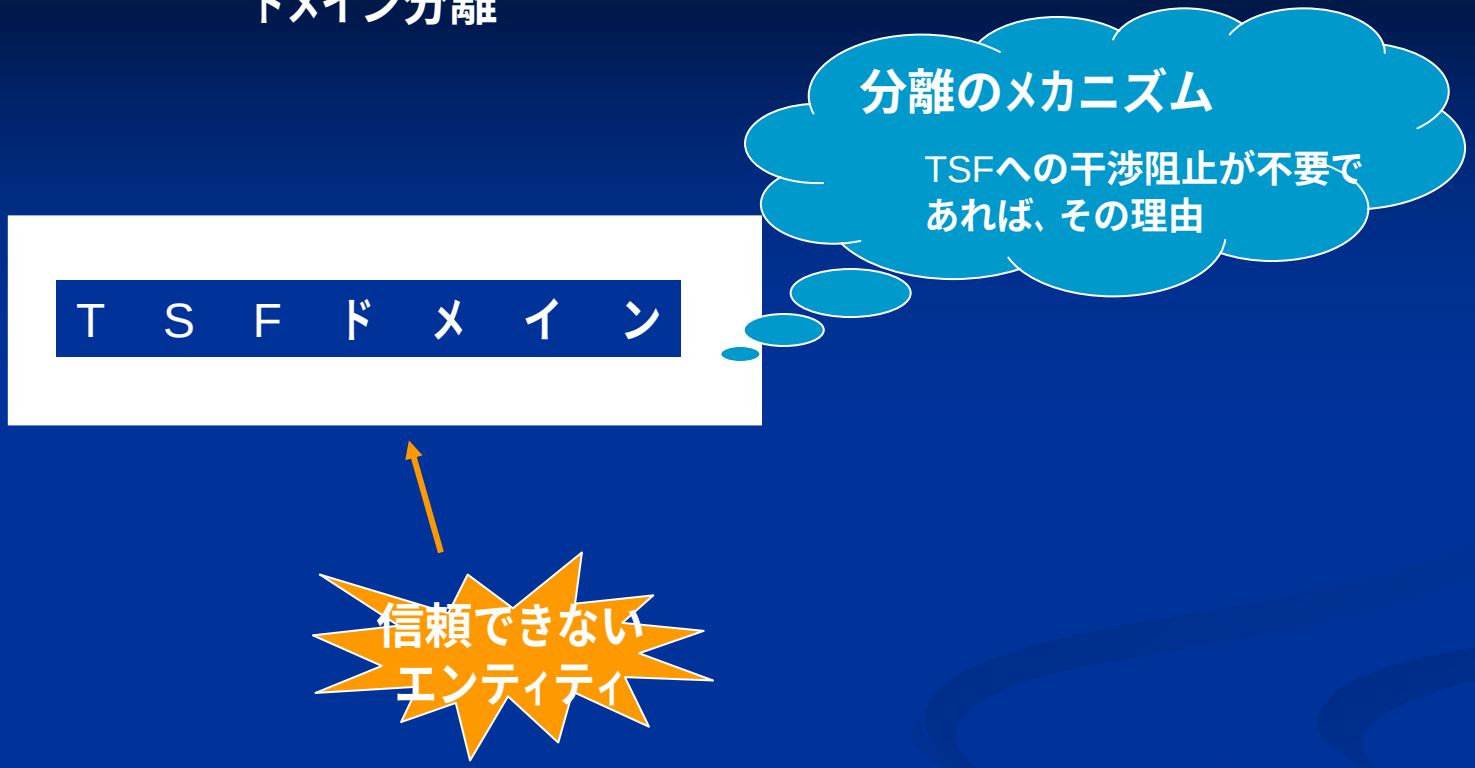
ADV_ARC.1-4 評価者は、セキュリティアーキテクチャ記述が、信頼できない能動的なエンティティによる改ざんからTSFが自分自身を保護できるという決定を支持するのに十分な情報を含んでいることを決定するために、その記述を検査しなければならない。

初期化



ADV_ARC.1-3 評価者は、初期化プロセスのセキュリティが保持されていることを決定するために、セキュリティアーキテクチャ記述を検査しなければならない。

ドメイン分離



ADV_ARC.1-2 評価者は、TSFによって維持されるセキュリティドメインをセキュリティアーキテクチャ記述が記述していることを決定するために、その記述を検査しなければならない。

非バイパス性

論証1 TSF:**資産保護のための機能**

このルートが無いことを検証

資産を利用するために可能なすべてのインタフェースを抽出

↓

すべてのインタフェースにTSFが介在することを論証

論証2 TSF:**資産保護以外の機能**

TSFは資産の利用には関与しない。

↓

TSFの呼び出し条件の記述に問題が無いことを論証。

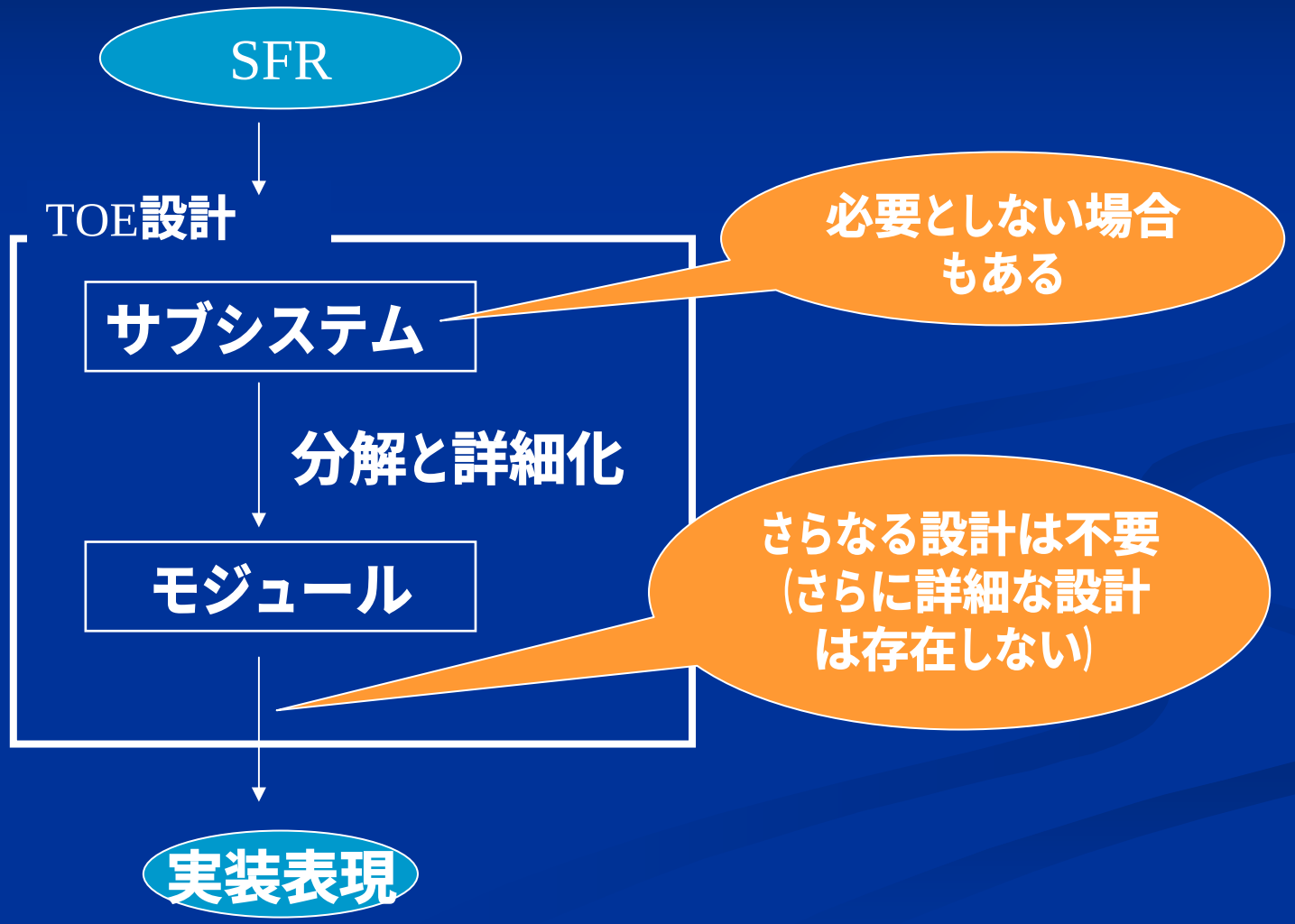
↓

呼び出し条件が整えば必ず動作する。

ADV_ARC.1-5 評価者は、SFR実施メカニズムをバイパスできないようにするしくみを適切に説明する分析をセキュリティアーキテクチャ記述が提示していることを決定するために、その記述を検査しなければならない。

TOE設計

目的、ふるまい（SFRとの関連性）、相互作用を記述



・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。

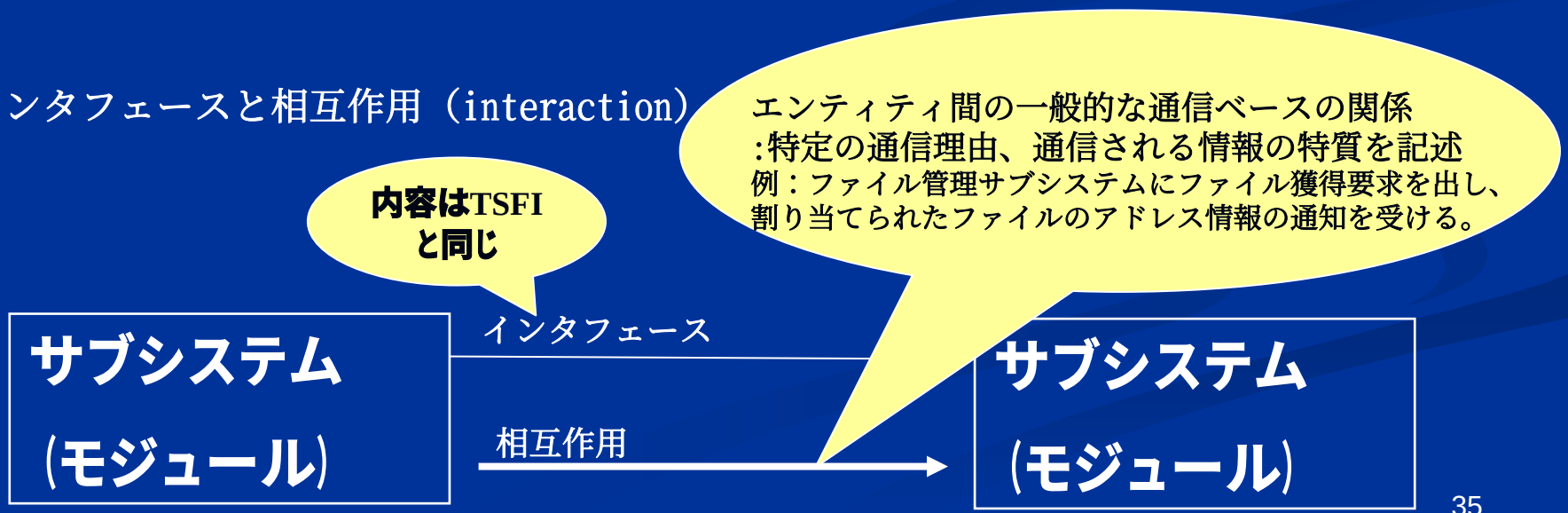
・TOEの開発（保守）に必要な情報のみをTOE設計記述に記載する。

　— 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）

・インタフェースと相互作用（interaction）



脆弱性評定

【定義】

V2:定義なし

ただし、以下のような記述があり、TOE全体の侵害に係わる弱点を対象にしていた。

AVAクラスは、悪用されうる隠れチャネルの存在、TOEの誤使用や設定誤りの可能性、確率的または順列的メカニズムが破られる可能性、及びTOEの開発または運用で入り込む悪用されうる脆弱性の可能性を扱う。

開発者分析の意図は、意図したTOEの環境において、識別されたどの脆弱性も悪用できないこと、TOEが明白な侵入攻撃に耐えることを確認することである。

V3：ある環境のSFR を侵害するために使用されることがあるTOE の弱点。

残存脆弱性(residual vulnerability) - TOE の運用環境では悪用できないが、TOE の運用環境において予想を超える攻撃が可能な攻撃者が、SFR を侵害するために使用することがある弱点。

悪用可能脆弱性(exploitable vulnerability) - TOE の運用環境でSFR を侵害するために使用されることがあるTOE の弱点。

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実施するように変更した。

一番低い脆弱性分析レベル（EAL1:AVA_VAN.1)では、公知の潜在的な 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。

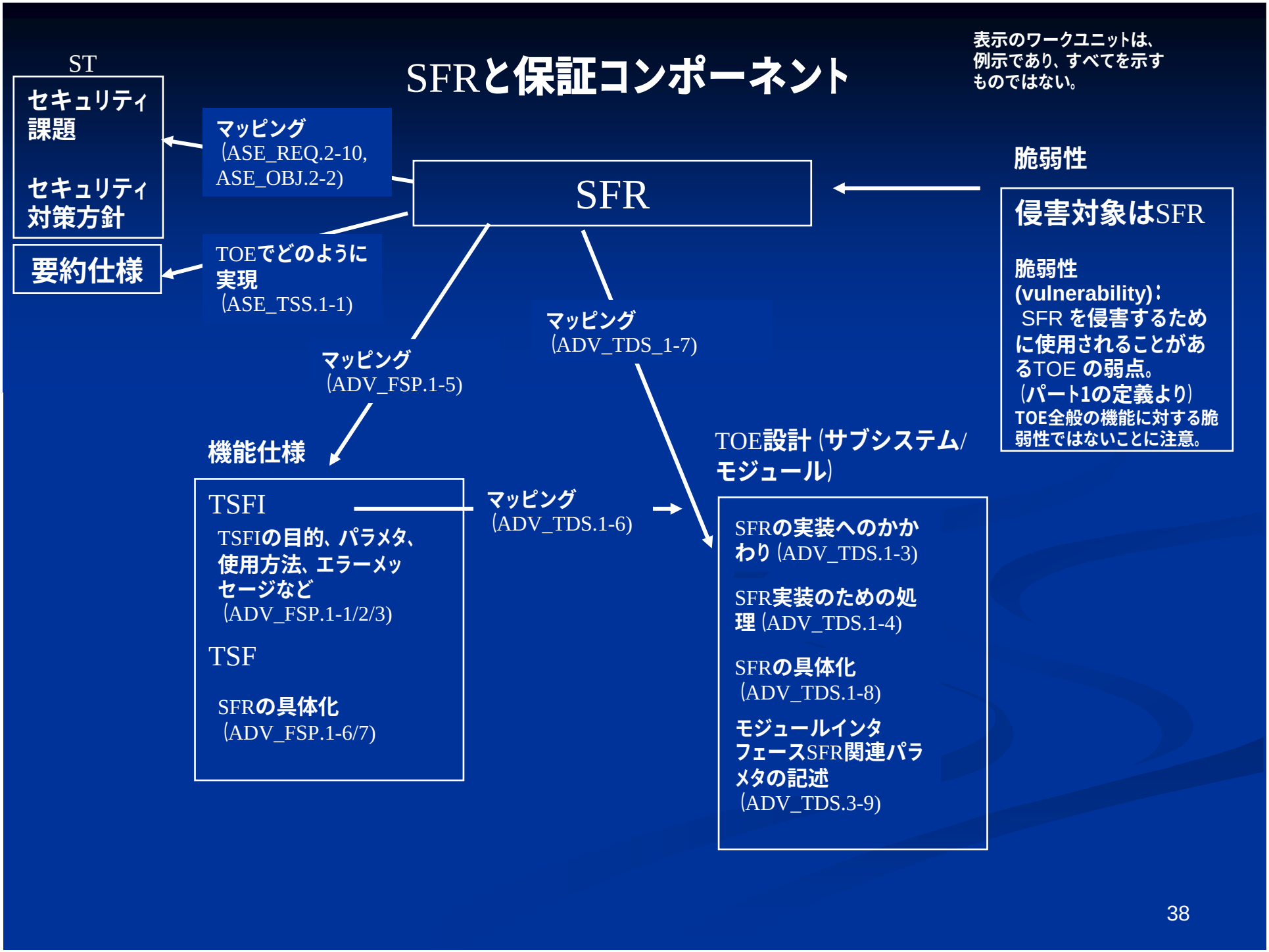
評価者は、TOEへの侵入テストを実施する際に、基本（AVA_VAN.1及びAVA_VAN.2）、拡張された基本（AVA_VAN.3）、中（AVA_VAN.4）、または高（AVA_VAN.5）レベルの攻撃能力を持つ攻撃者の役割を想定しなければならない。

ワークユニットの例:

AVA_VAN.2-4 評価者は、TOEに存在する可能性がある潜在的な脆弱性を識別するために、ST、ガイダンス証拠資料、機能仕様、TOE設計、及びセキュリティアーキテクチャ記述の証拠の探索を実施しなければならない。

AVA_VAN.2-11 評価者は、TOEが、運用環境において、基本的な攻撃能力を持つ攻撃者に耐えられることを決定するために、すべての侵入テストの結果を検査しなければならない。

SFRと保証コンポーネント



ライフサイクル/ガイダンス

◆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

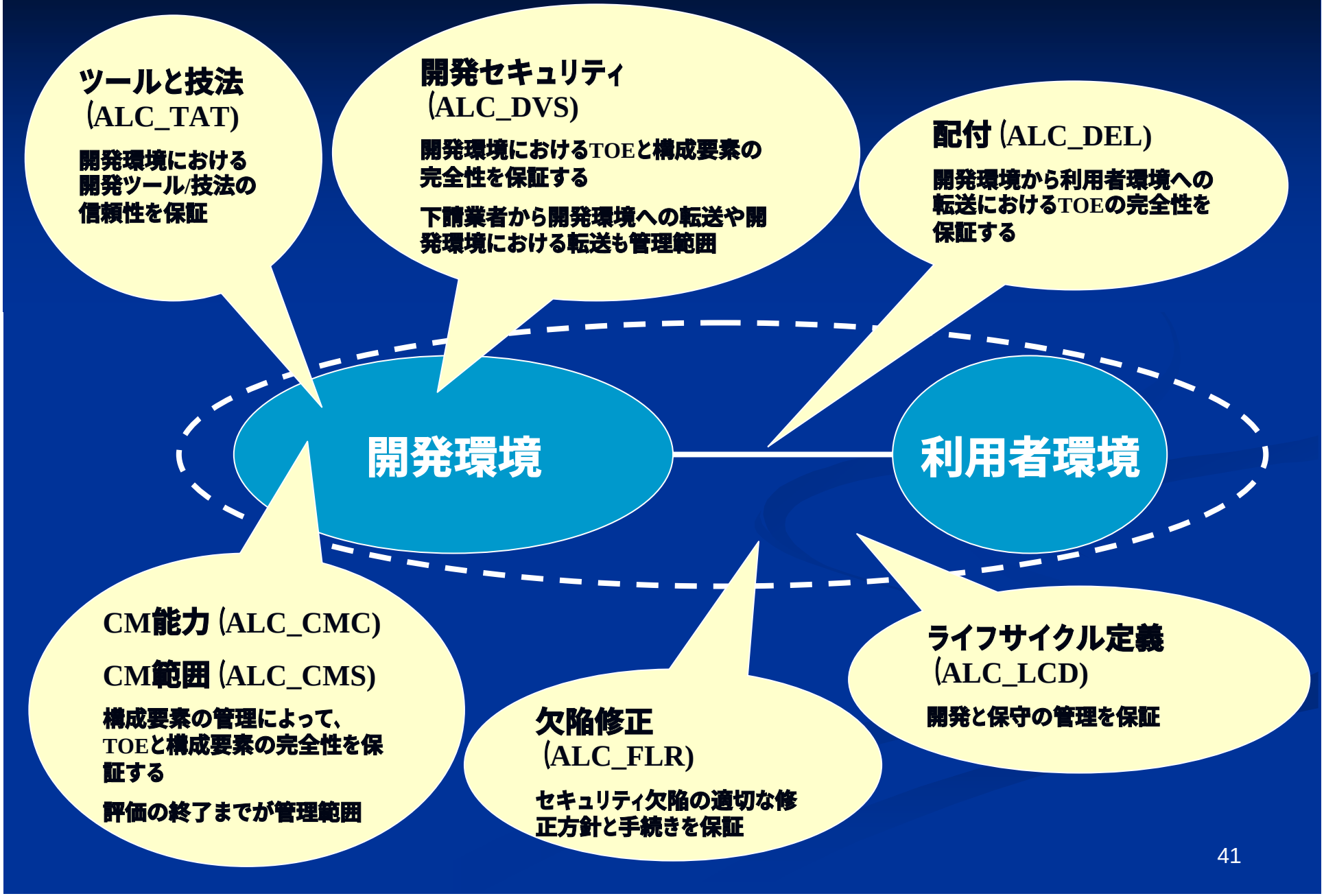
- 利用者に対する要件と開発者に対する要件の明確化
- 管理機能に対する要件と管理対象に関する要件の明確化
- TOEの運用とその環境に係わる要件の明確化

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。

ガイダンス


運用環境のセキュリティ対策方針
セキュリティ手段を記述
(AGD_OPE.1-6)
手順を記述
(AGD_PRE.1-4)
利用者操作ガイダンス
準備手続きガイダンス

ライフサイクルサポート



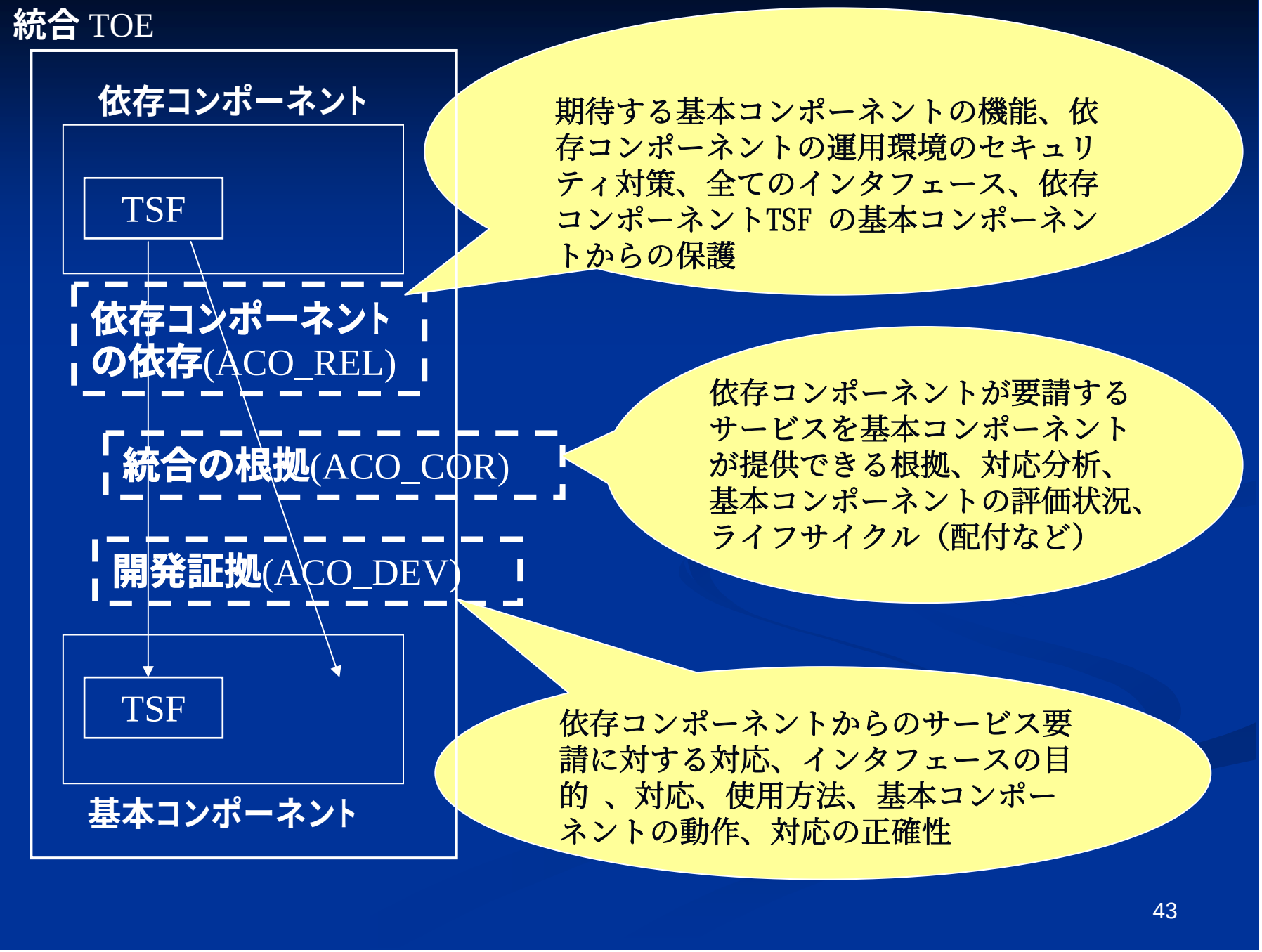
コンポジション

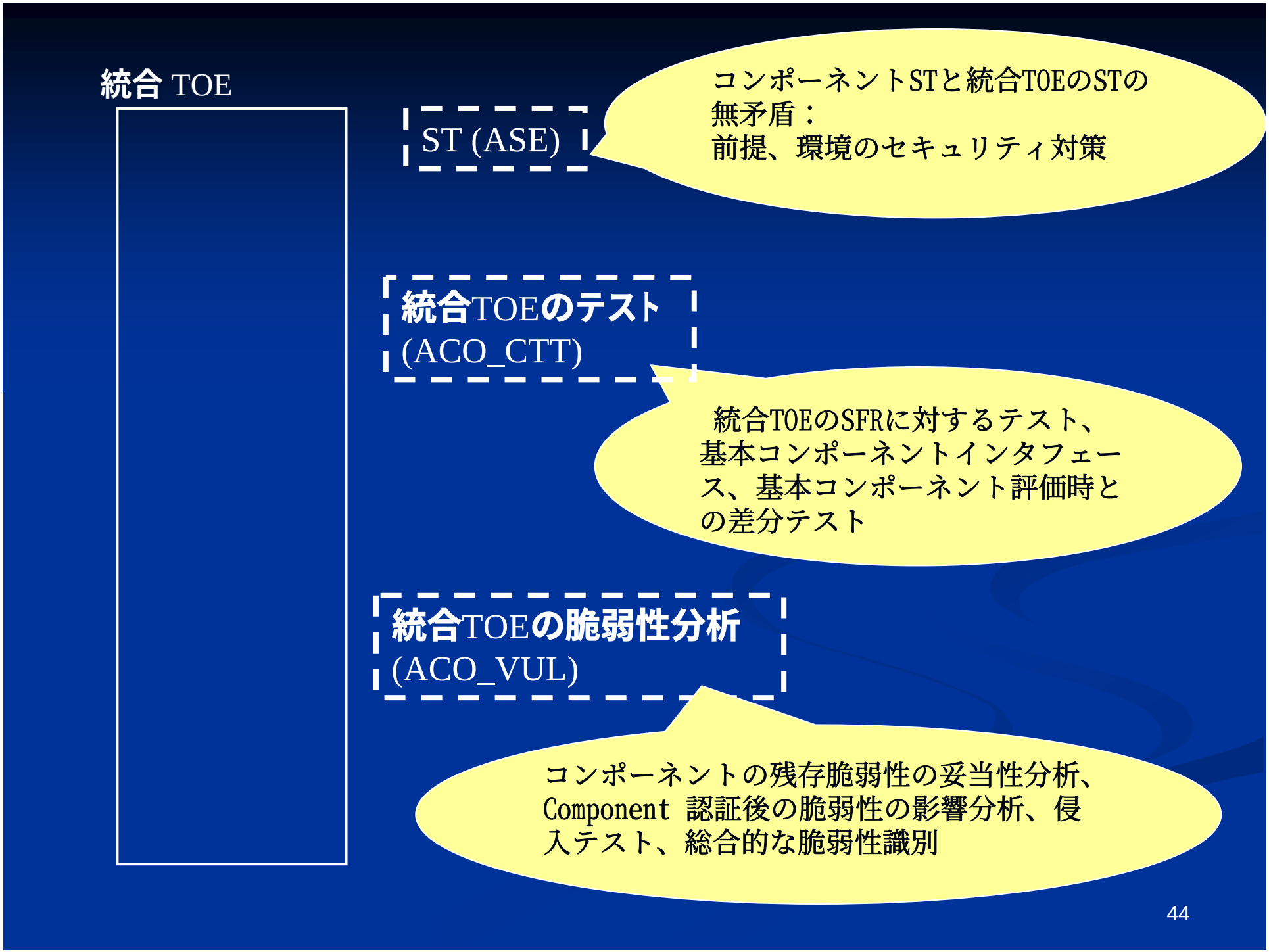
◆個別に評価された複数のTOE(基本/ 依存コンポーネント)を結合して、1つのTOE (統合 TOE)を作成した際の保証に係わる要件。(コンポーネント TOEの再評価は行わない)

◆保証は結合によって各コンポーネントの評価結果と統合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。

◆依存コンポーネントの開発者は、統合TOEの評価のためにエビデンスを提供。


統合 TOE
依存コンポーネント
TSF
依存コンポーネントの依存(ACO_REL)
統合の根拠(ACO_COR)
開発証拠(ACO_DEV)
TSF
基本コンポーネント
期待する基本コンポーネントの機能、依存コンポーネントの運用環境のセキュリティ対策、全てのインタフェース、依存コンポーネントTSF の基本コンポーネントからの保護
依存コンポーネントが要請するサービスを基本コンポーネントが提供できる根拠、対応分析、基本コンポーネントの評価状況、ライフサイクル（配付など）
依存コンポーネントからのサービス要請に対する対応、インタフェースの目的 、対応、使用方法、基本コンポーネントの動作、対応の正確性

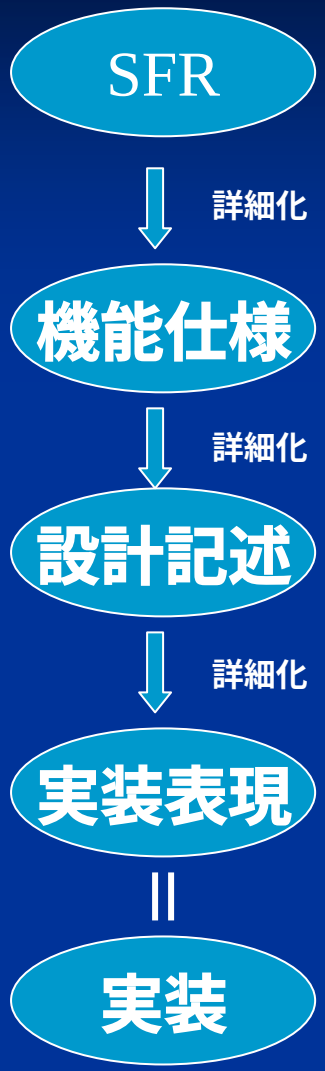

統合 TOE
ST (ASE)
コンポーネントSTと統合TOEのSTの無矛盾：
前提、環境のセキュリティ対策
統合TOEのテスト
(ACO_CTT)
統合TOEのSFRに対するテスト、基本コンポーネントインタフェース、基本コンポーネント評価時との差分テスト
統合TOEの脆弱性分析
(ACO_VUL)
コンポーネントの残存脆弱性の妥当性分析、Component 認証後の脆弱性の影響分析、侵入テスト、総合的な脆弱性識別

運用

- 証拠資料
- 低位ST
- 差分評価
- 評価規格

証拠資料

「証拠資料及び結果としてのIT製品の有効性を測定・・・」（保証のパラダイム記述より）



開発過程において、実装は機能仕様、設計記述や実装表現を正確に詳細化したものであることを検証。

機能仕様、設計記述や実装表現は実装を正確に記述していることが証明される。

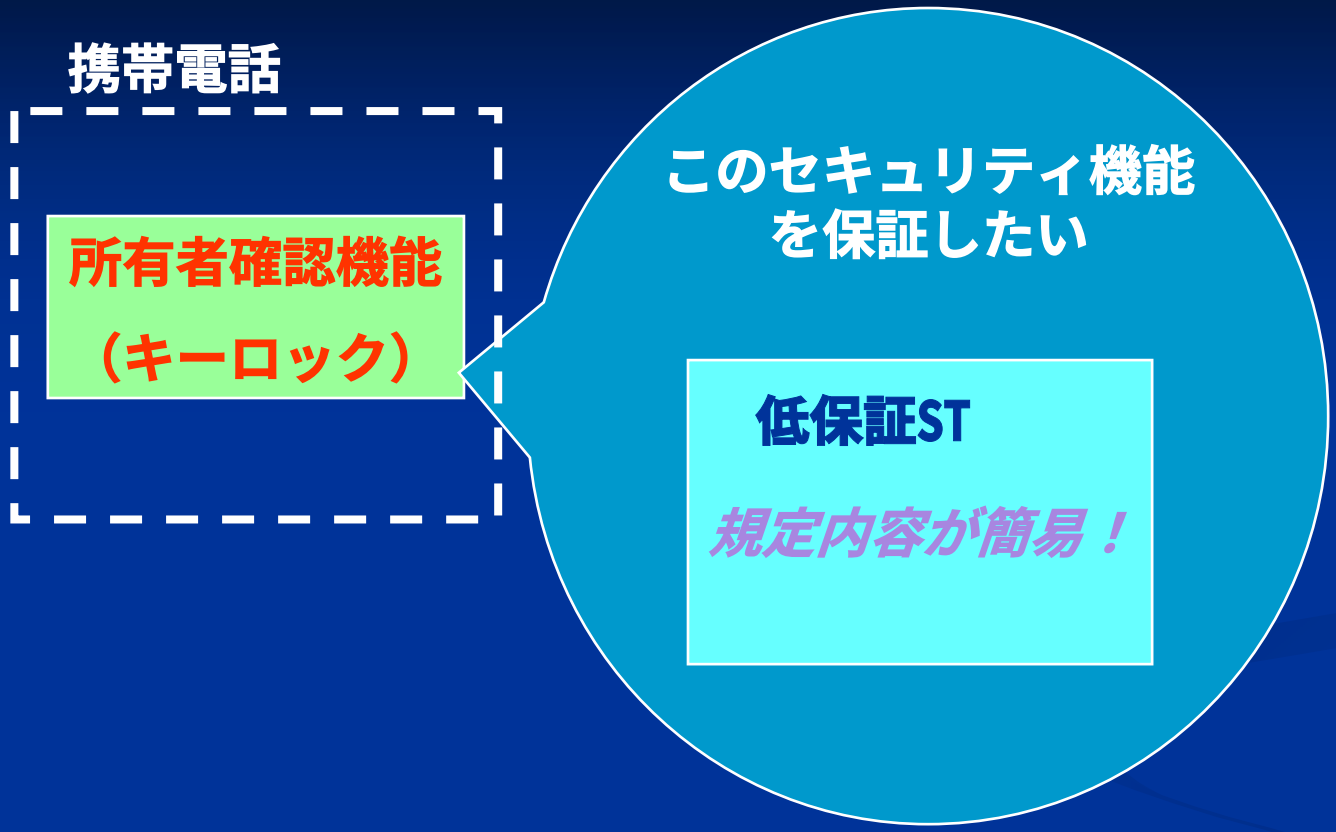
この前提で、機能仕様、設計記述や実装表現にセキュリティ上の問題（バイパス、侵害など）が無いことを検証。

実装に機能、設計や実装に係わるセキュリティ上の問題が無いことを検証。

証拠資料を開発とは別に作成した場合、実装と同一であることの証明が必要！

開発生産物以外に評価用にエビデンス作成は、原則、禁止。例外の場合は、作成エビデンスがTOEと同等（エビデンスに基づいてTOEが作成されたとみなせる）である理由を提示する。（評価の開始にあたって）

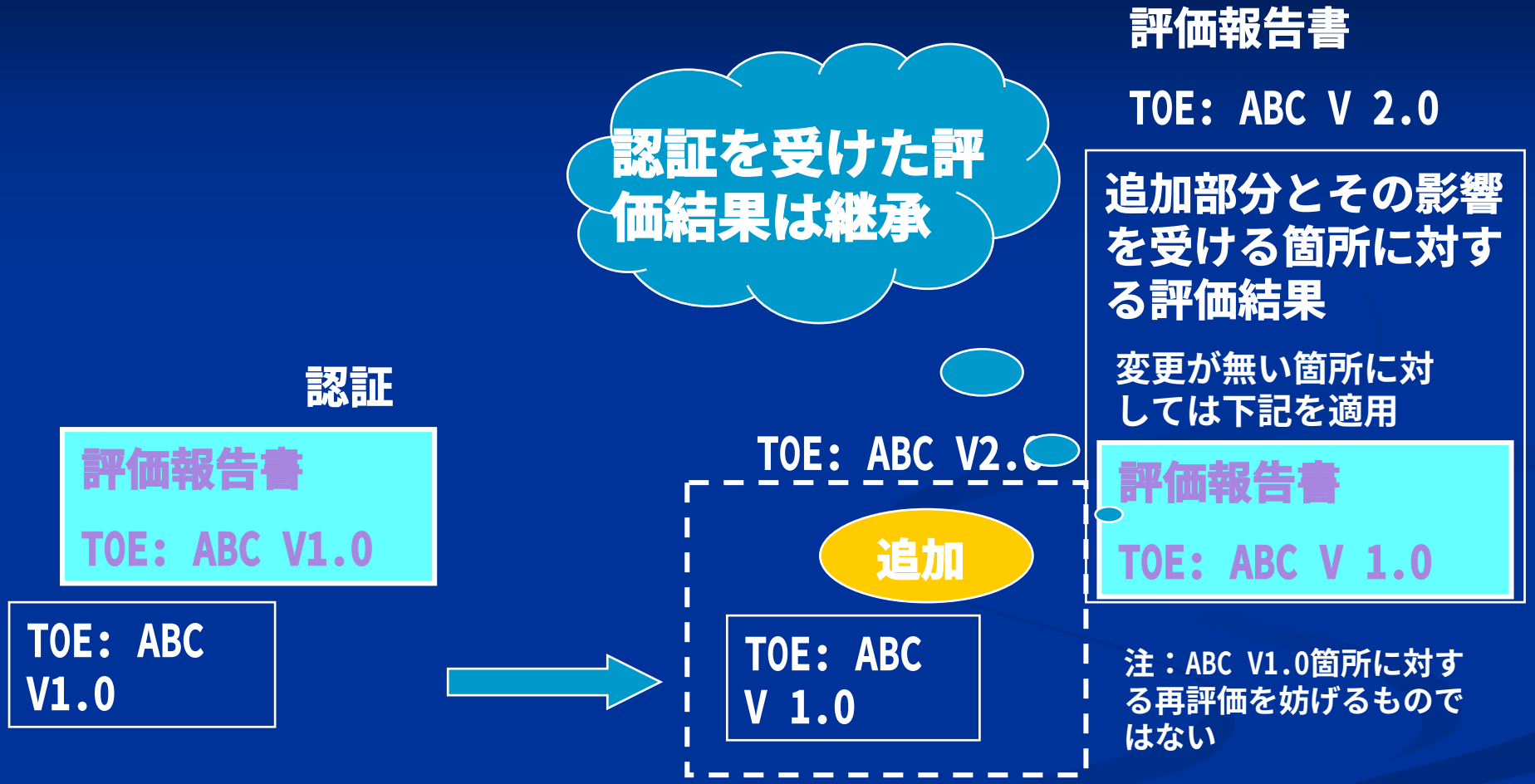
低保証ST



「プロトタイプ型機能特定保証（V3.1　EAL1）」の適用推進

差分評価

認証（＝評価結果は正当）した事実は他TOEの評価結果でも継承する。



V2からの評価および認証結果の継承は行わない。

V3.1では新規の評価および認証となる。

評価規格

平成18年10月5日に下記のV3.1規格を公開

Common Criteria for Information Technology Security Evaluation Version 3.1

- Part 1: Introduction and general model (CCMB-2006-09-001)
- Part 2: Security functional components (CCMB-2006-09-002)
- Part 3: Security assurance components (CCMB-2006-09-003)

Common Methodology for Information Technology Security Evaluation

- Evaluation methodology (CCMB-2006-09-004)

平成19年4月16日に下記のV3.1翻訳版規格を公開

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 バージョン3.1

- パート1: 概説と一般モデル [翻訳第 1.2 版]
- パート2: セキュリティ機能コンポーネント [翻訳第 1.2 版]
- パート3: セキュリティ保証コンポーネント [翻訳第 1.2 版]

情報技術セキュリティ評価のための共通方法　バージョン3.1

- 評価方法 [翻訳第 1.2 版]

V3.1の適用

◆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9月30日までに保証継続として認証されているTOEについて、平成21年10月1日以降の再評価（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。

◆最初の「認証書」の発行日から5年以上経過したTOEの保証継続の認証は受け付けない。