CCの動向紹介

1. CC V3.0
2. システム評価 (ISO TR 19791)

注:

・いずれも検討中であり、確定した規格ではないことに留意願います。

・使用している用語は、規格として確定したものではないことに注意願います。

平成１８年２月

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

CC v3.0について

1．概要

2．ASE/APE

2．パート2

3．パート3

注：名称変更

コンポーネント：パート2，3で規定の要求事項

パート2　セキュリティ機能要件(CC 2.1)

→パート2　セキュリティ機能コンポーネント(CC 3.0)

要件：PP/STで規定の要求事項でコンポーネントの具体化

1. 概要

CC 2.1: 1999　以来の大規模な改訂

目的: 評価の冗長性改善

保証への貢献が高い評価に集中

パート1: 用語の一貫性、　ASE/APEの内容を変更

パート2　(TOEのセキュリティ機能を正確に理解):

・セキュリティ機能のモデル化:

TOE内部の管理 (アクセス管理など)、TOEへの接続 (認証など)、通信保護 (秘密保持など)、監査、TSFの保護

・スリム化:クラス (11⇒6)、ファミリー(67 ⇒45)

パート3　(TOEのセキュリティ保証の確保):

・保証要件の整理

・統合製品の保証

提供スケジュール

- 2005年7月4日
  - V3.0のパブリックレビューを開始
  - トライアルユースを開始
    （このトライアルユース はCCRAの対象とする）
- 2005年11月1日　パブリックレビュー終了
  レビュー結果を反映したCC V 3.1を作成。
- 2006年7月14日にCC　V3.1の適用をCCRAで承認。
- CCRAでは2008年1月よりCC3.1の使用が必須。
  これ以降、評価を開始するものが対象。

2006年7月には日本語版のCC V3.1を作成予定

2006年4月はじめまでにはCC V3.0の翻訳版（技術チェックは未）を公開

用語

製品

ハードウェア、ソフトウェア，及びファームウェア

ガイダンス（配付/導入、運用/管理/利用に係る記述）

CD-ROM

＋

マニュアル

ガイダンスにしたがって、導入され動作している製品（唯一の構成を持ち、セキュリティ機能を提供）

評価対象（TOE）

TOEセキュリティ機能（TSF）

TOEセキュリティポリシー(TSP:TOE Security Policy)を実現するために必要となる(*)全てのハードウェア、ソフトウェア，及びファームウェア

実装

セキュリティ目標（ST:Security Target）

-セキュリティ課題

-セキュリティ対策方針

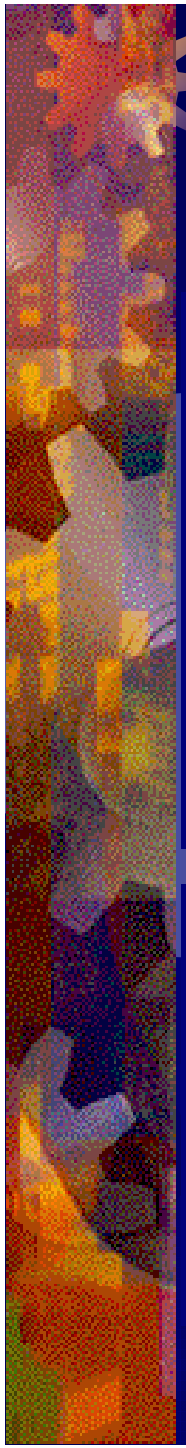
TOEセキュリティポリシー（TSP）

TOEに係るセキュリティ機能要件（SFR:Security Functional Requirements)のセット；

-セキュリティ保証要件

など

＊：TSP実現のための非バイパス性、ドメイン分離、非干渉性などのための機能もTSFに含まれる。



2. ASE/APE その1

STの構成

1.ST概説

- ST参照
- TOE参照
- TOE概要
- TOE記述

2.適合主張

- CC適合主張
- PP主張
- パッケージ主張

ASE/APE　その2

3.セキュリティ課題定義(Security problem definition)　(EAL1では不要)

- 脅威

  TOE、その運用環境、及びその開発環境に係る脅威を記述する。

  TSFのバイパスや干渉への脅威はADV_ARCで考慮する。

- 組織のセキュリティ方針
- 前提

4.セキュリティ対策方針

- TOEのためのセキュリティ対策方針 (EAL1では不要)
- 開発環境のためのセキュリティ対策方針 (EAL1では不要)

  例：　開発環境ではソースコードの完全性を確保する。

  　　ソースコードレベルでの信頼性を確保する。

- 運用環境のためのセキュリティ対策方針
- セキュリティ対策方針根拠 (EAL1では不要)

ASE/APE　その3

5.拡張コンポーネント定義

6.セキュリティ要件

- TOEセキュリティ機能要件
- TOEセキュリティ保証要件
- セキュリティ要件根拠(EAL1では不要)

7.TOE要約仕様(EAL1では不要)

ASE/APE　その4

TOEの説明として記載すべき事項⇒読者に必要な情報が提供できる。

項目	対象読者	伝えたい情報
TOE概要	一般利用者	TOEの機能
	購入者	TOEのセキュリティ機能（必要なセキュリティ事項は（例：データベースへのアクセス制御）装備されている。）
		TOEの動作に必要なハードウェア/ファームウェア/ソフトウェア
TOE記述	購入者	TOEの機能および物理的な範囲（TOE外との境界）
セキュリティ課題定義	購入者	対抗できる脅威、運用環境の前提、カバーできる規則や法律
運用環境のセキュリティ対策方針	購入者	TOE動作に際して、要求する運用環境のセキュリティ対策
TOE要約仕様	技術者	セキュリティ機能（動作/運用に与える影響が理解できる）
適合主張	調達者	適合するパッケージやPP
	購入者	保証パッケージ（TOEの信頼度）

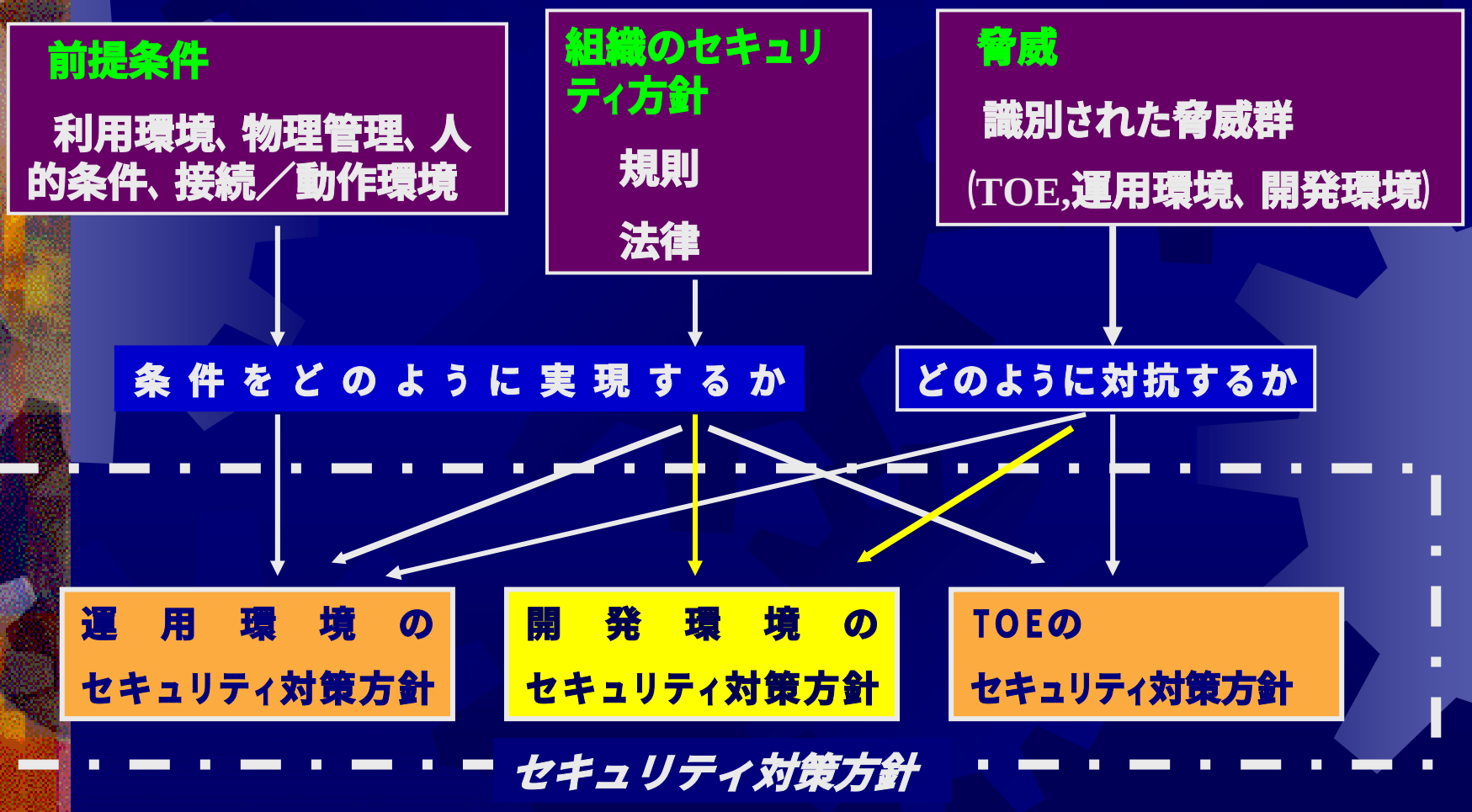
ASE/APE その5

PP適合について、下記の3つから選択可能

- **完全適合**(Exact conformance)：**PPと同一であること**
  - PPの記載に対して追加も修正も不可（基本的には操作の選択のみ）
  - 調達する部品用のPPなどに採用
- **正確適合**(Strict conformance)：**PPを包含していること**
  - PPの記載に対して追加のみ可（ただし、セキュリティを弱めるものは不可、TOEに合わせて操作を完成）
  - 製品やシステムに対する最低限のセキュリティ要件をPPに記載
- **要求適合**(Demonstrable conformance)：**PPの要求は満たすこと**
  - PPの記載に対して変更は可（ただし、PPの規定内容との矛盾が無いこと、保証要件はPP規定要件を含む、選択操作はPP指定範囲内）
  - 解決すべきセキュリティ課題と解決のためのガイダンスをPPに記載

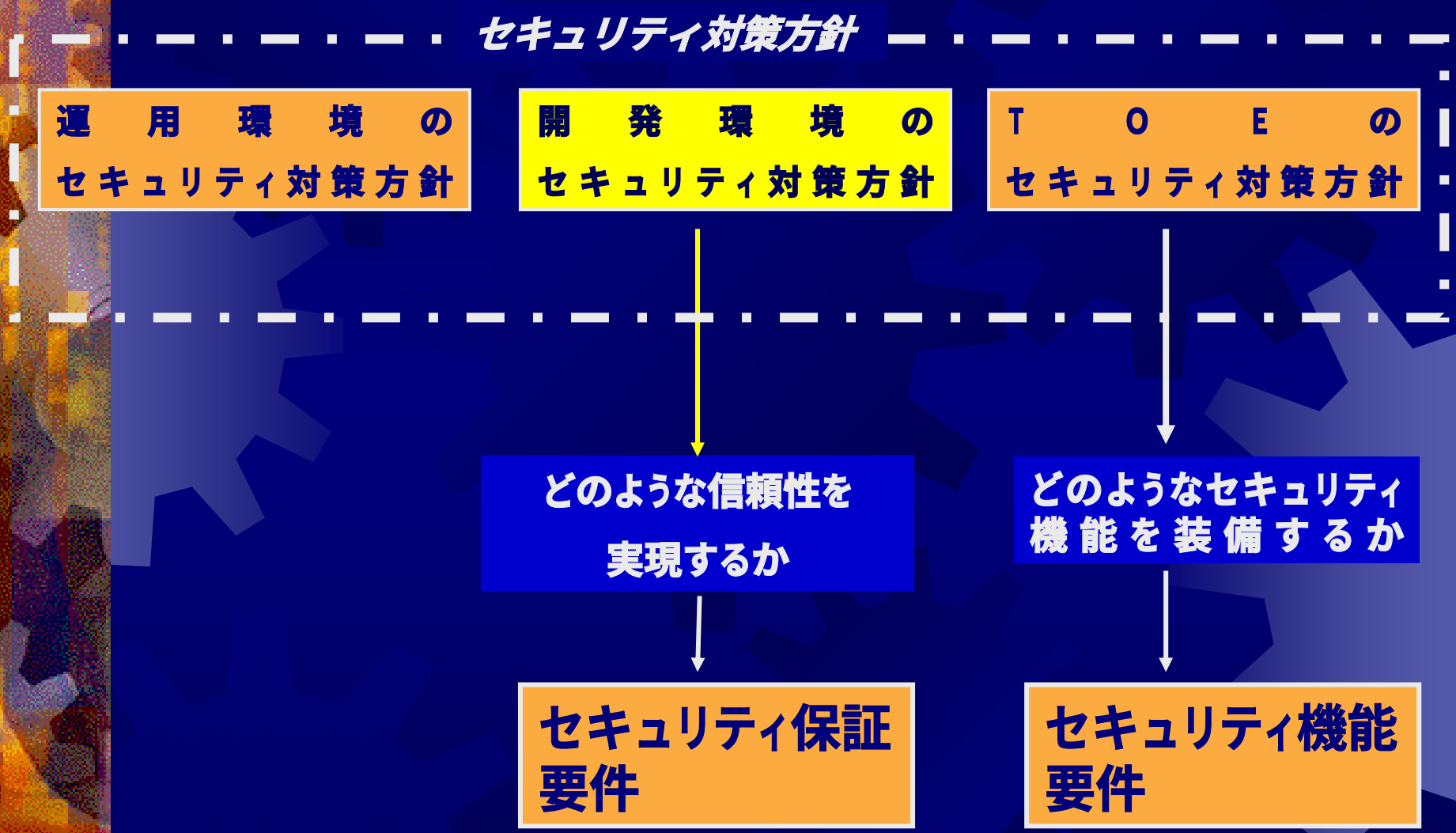
ASE/APE その6

セキュリティ対策方針の策定手順



ASE/APE その7

セキュリティ要件の策定手順



ASE/APE その8

簡易ST(Low assurance Security Targets)

・EAL1**に適用**

特徴

●**ST**概説、適合主張、運用環境のセキュリティ対策方針、拡張コンポーネント定義、**TOE**セキュリティ要件、**TOE**要約仕様のみを記載。

（セキュリティ課題定義、**TOE**及び開発環境のセキュリティ対策方針とそれらの根拠、及びセキュリティ要件根拠の記述は不要）

●**SFR**及び**SAR**は、それぞれの依存性を満たす必要はないし、そのことに対する根拠を記述する必要もない。

3. パート2

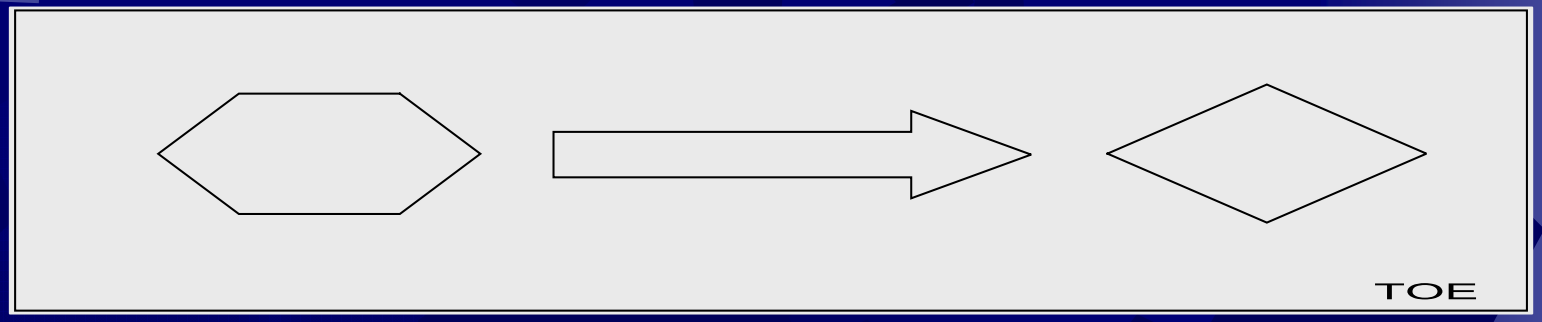
問題認識1：二者択一で多様性欠如

(1) 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、アプリケーション側で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。

CC V3では、セキュリティ機能の概念を一般化することによってこの二重性を排除し、機能を単純明快なものにした。

「サブジェクト、オブジェクト、操作」によるセキュリティ機能の概念の共通化



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。

オブジェクト：サブジェクトによる操作の実行対象となる受動的なエンティティ。

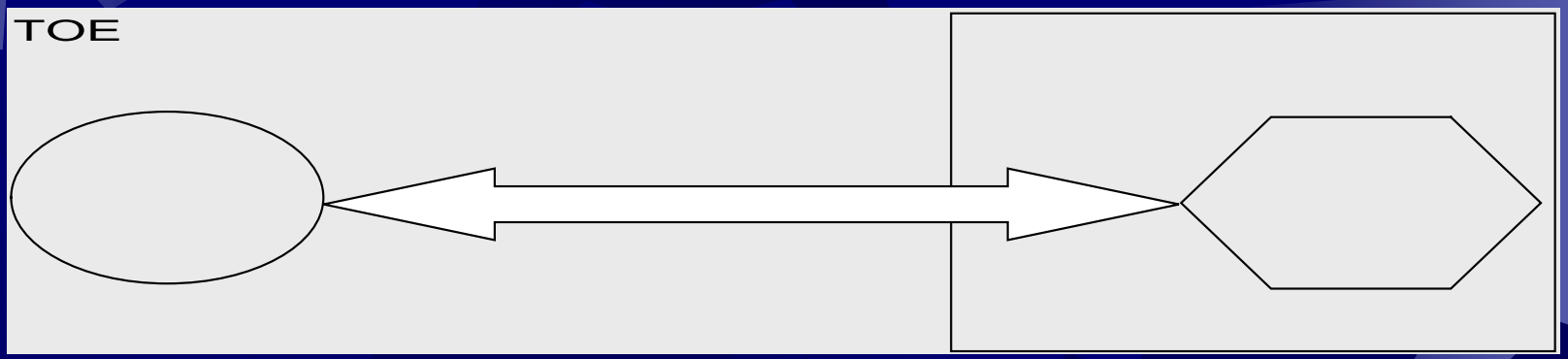
問題認識2：“利用者”の概念が不明確

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。さらに、利用者とサブジェクトが誤解。

V3では、利用者とサブジェクトの２語のみを使用し、明確に区別する。

利用者とは、TOEの外部の能動的なエンティティ（人間、アプリケーションプログラムなど）。

利用者がオブジェクトを利用する場合には、まず、サブジェクトに結合。サブジェクトは、利用者の代わりに、オブジェクトに対して操作を実行することにより、オブジェクトと通信する。



問題認識3： 完成系が不確定

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）で要求。

問題認識4： 要件の抽象度のレベルで要件を分離

V3では、抽象度を統一。

問題認識5： 実装に依存するような要件が存在

V3では、

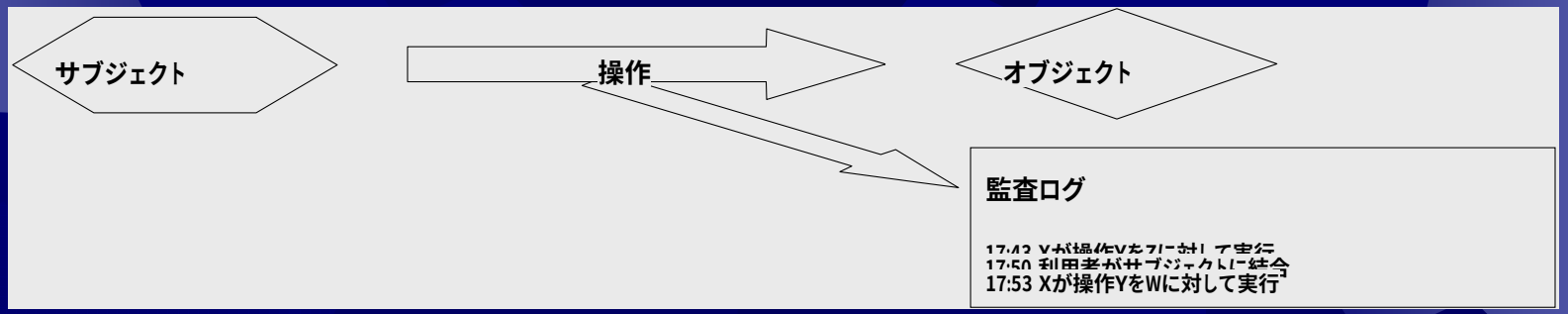
- 抽象エンティティ（オブジェクト、サブジェクトなど）を使用して期待されるふるまいを記述。
- 実装に依存する要件は削除（暗号機能：FCSなど）。

セキュリティ監査（FAU）

- 基本的には、CC V2のFAUクラスより構成した。

監査ログ情報はオブジェクトであるため、この保護はアクセス制御（FDP_ACC）を使用して行う。また、ログ格納領域のオーバフローは資源割当て（FPT_RSA）を使用して管理する。

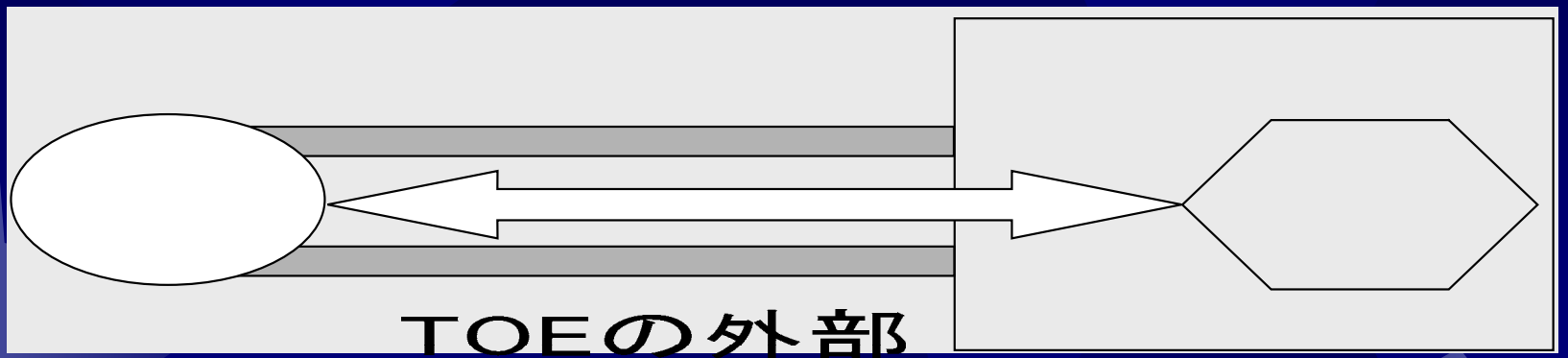
- 監査可能事象は、機能コンポーネントのファミリの「監査」で規定。
- 実際に選択された監査事象は、セキュリティ監査データ作成ファミリ（FAU_GEN）で規定。
- 結果としての監査事象の処理は、セキュリティ監査分析ファミリ（FAU_SAA）で規定。・



監査事象をログに記録し（FAU_GENファミリ）、ログを自動的に分析し（FAU_SAAファミリ）、この分析の結果に基づいて動作する（FAU_ARPファミリ）コンポーネントを定義する。

通信（FCO）

●基本的にはV2のFDP,FPT,FTP,FCOから構成した。



サブジェクトとそのサブジェクトに結合した利用者間の通信の保護（つまり、機密性、完全性、及び可用性の保証）に対処するコンポーネントを規定。

主なエクスポートファミリ

保護

・エクスポートされたデータの可用性（FCO_AED）

・エクスポートされたデータの機密性（FCO_CED）

・エクスポートされたデータの完全性（FCO_IED）

保護

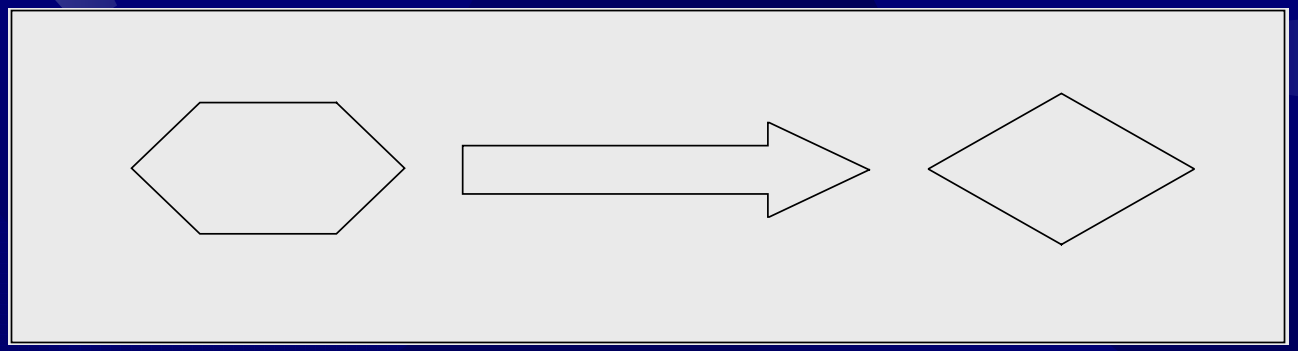
・エクスポートされたデータの否認拒否（FCO_NRE）

・エクスポートの観察不能性（FCO_UNE）

インポートファミリも同様・

データ保護とプライバシー（FDP）　その１

- 基本的に、CC V2のFDP,FMT,FPRクラスから構成。
- CC V2では、ポリシーの指定(ACC/IFC)と規則の指定(ACF/IFF)が別のファミリとして、不自然に分離されている。⇒規則の指定は、ポリシーの中で。
- CC V2では、アクセス制御(ACC/ACF)と情報フロー制御(IFC/IFF)との差異が不明確。⇒ACCは能動エンティティ（プロセスなど）が受動エンティティ(ファイルなど）にアクセスする際の制御、IFCは能動エンティティ間のアクセスにかかわる制御であることを明確化。
- CC V2では、ポリシー名称の規定を要求するが、この指定は不必要な場合　が多い。⇒FDP_ETC/ITC/ITT/ROL/UCT/UITの操作からポリシー名称の規定を削除。



データ保護とプライバシー（FDP）その２

操作

●アクセス制御（FDP_ACC）：セキュリティ属性に基づいてサブジェクトがオブジェクト上で操作を実行するための規則を規定。

●ロールバック（FDP_ROL）：これらの操作を元に戻すための規則を規定。

●観察不能性（FDP_UNO）：サブジェクトが操作を実行している他のサブジェクトを観察できないようにするための機能を規定。

●リンク不能性（FDP_UNL）：サブジェクトが何らかの方法で異なるサブジェクト、オブジェクトや操作にリンクできないようにするための機能を規定。

セキュリティ属性

●セキュリティ属性の初期化（FDP_ISA）：新しいオブジェクトまたはサブジェクトの作成時にセキュリティ属性を初期化するための規則を規定。

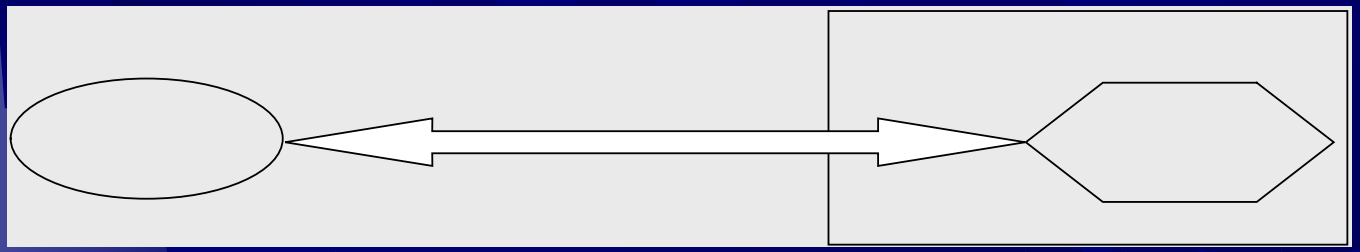
●セキュリティ属性の管理（FDP_MSA）：既存のサブジェクト及びオブジェクトのセキュリティ属性の値を変更するための規則を規定。

識別、認証及び結合（FIA）

●基本的には、CC V2のFIA,FTAクラスから構成した。

●TSFが識別や認証を実施することを要求していることを明確化。

●利用者識別の単位（利用者個人、グループなど）を規定。



- 利用者登録（セキュリティ特性、認証データなど）（FIA_URE）
- 認証データの品質（推測不可性など）（FIA_QAD）
- 利用者識別（FIA_UID）
- 利用者認証（FIA_UAU）
- 認証失敗時の処置（FIA_AFL）
- TSF結合規則（利用時間帯制限など）（FIA_TBR）
- 利用者-サブジェクトの結合（FIA_USB）
- サブジェクト/TSFの認証（FIA_SUA）
- TSF情報（アクセス履歴の通知など）（FIA_TIN）
- 結合のロックアウト（FIA_LOB）
- 結合の終了（FIA_TOB）

TOEの外部

利用者

通信

TSFの保護（FPT）

●基本的に、CC V2のFPTクラス、PHPの修正、FRU_FLTより構成。

●タイムスタンプ機能については、別のクラス（FMI_TIM）で規定する。

●AMTとTSTの区別が不明確。⇒TSTはTSFのテストであることの明確化。
TOE外のテストはファミリ名を変更（機械利用者のテスト：FPT_TOU）

●SEPとRVMは保証要件（ADV_ARC）で対応。

３つのファミリのグループから構成。

a)TSFが以下の条件を満たす場合のテスト、障害、及び回復

TSF自己テスト（FPT_TST)、機械利用者のテスト（FPT_TOU)、耐障害性（FPT_FLT)、フェールセキュア（FPT_FLS），高信頼回復FPT_RCV））

b)物理的保護

TSF物理的保護（FPT_PHP）

c)資源の使用

優先度処理（FPT_PRI)、資源割当て（FPT_RSA)、残存情報保護（FPT_RIP）

その他（FMI）

・乱数発生（FMI_RND）

・タイムスタンプ（FMI_TIM）

・選択（FMI_CHO）

　PPが機能要件としてFMI_CHO.1（**SFR**の**2**つのセットからの選択を可能にする）を含む場合、STでは適切な**SFR**のセットを選択できる。

4. パート3

認証製品の統合に対する評価 (ACO)

ハードウェアに対する評価 (PLT)

インタフェース仕様、テスト範囲、プラットフォームの定義

HLDとLLDを統合してTDS （TSF/TOE Design)

実装とアーキテクチャーに分析を分類

実装： FSP, TDS, IMP

アーキテクチャー：ARC, INT

統合 (ACO)

既に評価されている製品を含む統合製品の評価に関わる要件を規定。

統合の根拠 (ACO_COR)

正常な統合のために、基本**TOE**に適切な保証手段が適用されていることを検証。

統合TOE

依存TOE

基本TOE

依存**TOE**の依存性（**ACO_REL**）：基本**TOE**の**機能の十分性を検証。**

下記の依存情報を記述

・基本**TOE**のハードウェア、ファームウェアやソフトウェアの機能

・基本**TOE**のセキュリティ機能：依存**TOE**の**ST**の運用環境の記載事項と矛盾しないことも検証する。

・基本**TOE** のインタフェース情報：

ADV_FSPで要求の詳細度レベルで記述。

基本TOEのテスト (ACO_TBT)

依存情報、基本TOE情報で識別のインタフェースのテスト。

開発証拠（**ACO_DEV**）：基本**TOE**の**セキュリティ機能の検証。**

下記の基本TOE情報を作成

・インタフェース仕様：基本**TOE**のインタフェース（機能仕様）を記述。記述は**ADV_FSP**と**同程度。**

・構造：基本**TOE**の構造を記述。記述は**ADV_TDS.3**と同程度。

・ アーキテクチャ：基本**TOE**のアーキテクチャを記述。記述は**ADV_ARC.1**と**同程度。**

統合の脆弱性分析 (ACO_VUL)

・基本TOEと依存TOEに残存する脆弱性が、統合TOEの運用環境でも悪用不可能であること。

・統合TOEが、所定のレベルの攻撃能力を持つ攻撃者に対して抵抗力を持っている。

開発(ADV)　その1

1　ハードウェアの評価を可能にする。

●ハードウェア特性（インタフェース仕様、テストによる確認）を利用して保証を確保する。

●プラットフォームの定義（ソフトウェアTOEはハードウェアプラットフォームで動作、信頼が保証されないエンティティとの外部インタフェース/TOEセキュリティ機能との内部インタフェース、既存の情報の利用）を明確にする。

2　HLDとLLDを統合して TOE設計（TDS)とする。

3　セキュリティ機能の評価対象を絞り込む。

TOEをセキュリティ機能の観点から次の3つに分類する。

・SFR Enforcing:　SFRを直接実現する。

・SFR Supporting:　SFR Enforcing機能の動作には必要である機能。

・SFR Non-Interfering:　SFR Enforcing機能の動作には影響しない。

開発(ADV)　その2

４　セキュリティ機能の実装の確認とアーキテクチャに係わる確認は分離する。

・設計の評価　FSP，　TDS，　IMP

・アーキテクチャの評価　ARC，INT

ドメイン分離（FPT_SEP）を検証する。

迂回不可（FPT_RVM）を検証する。

５　保証の程度に係わる考え方を明確にする。

●セキュリティ機能の分類（SFR Enforcing、SFR Supporting、SFR Non-Interfering）により要求する保証に応じた適切な資材を提供できる。

●低レベルの保証では、開発者の分類による、一部の開発関連資材によって評価。高レベルの保証では、全ての開発関連資材を、評価者が検証。

開発（ADV） その3

ADV_FSP

利用者へのインタフェースに関してセキュリティ機能（ Enforcing と supportingを識別）は何を行なうか（目的、利用方法、パラメタ、効果、例外、エラーメッセージ）の明確化をより鮮明に要求。

- FSP.1：基本機能仕様　EAL1

  SFR実施と支援のTSFIの目的、利用方法、パラメタ

- FSP.2: SFR実施機能仕様　EAL2

  TSFの仕様、SFR実施TSFIの処理とエラーメッセージ

- FSP.3: 要約機能仕様　EAL3

  全てのTSFIに対して、SFRに関係しない処理の要約

開発 (ADV)　その4

・FSP.4: 完全な機能仕様　EAL4

　すべてのTSFIの処理、TSFIの呼び出しにともなうすべてのエラー　メッセージ

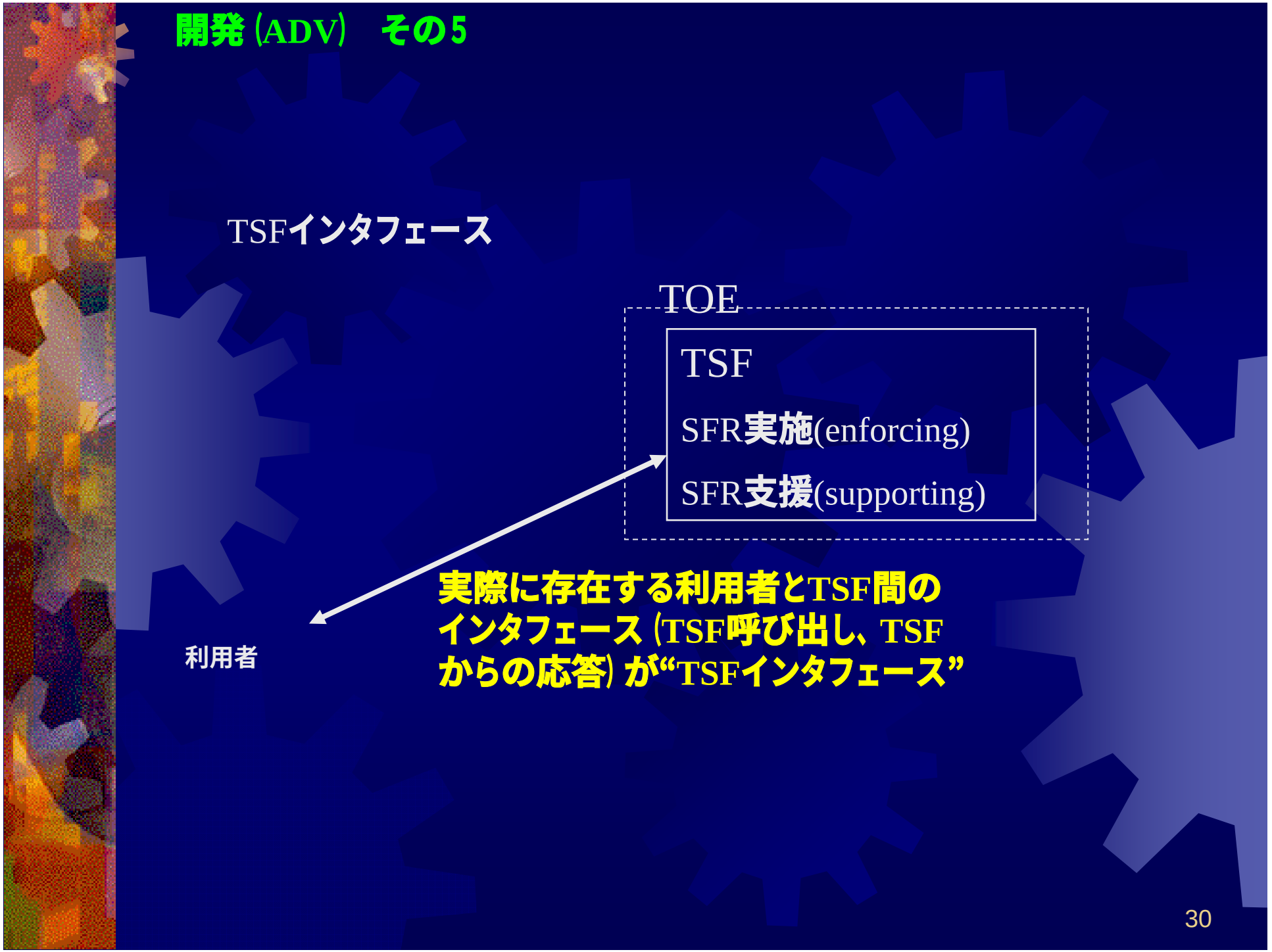
・FSP.5: 追加のエラー情報を伴う準公式的表現　EAL5/6

　TSFIを準公式的表現で記述、TSFの実装に伴うすべてのエラーメッセージとTSFIの処理に無関係である理由

・FSP.6:追加の公式的表現を伴う準公式的表現　EAL7

　TSFの機能仕様の公式的な表現

開発（ADV） その5


TSFインタフェース
TOE
TSF
SFR実施(enforcing)
SFR支援(supporting)
利用者
実際に存在する利用者とTSF間のインタフェース（TSF呼び出し、TSFからの応答）が“TSFインタフェース”

ライフサイクルサポート(ALC)/ ガイダンス(AGD) その1

重複した作業要求の削除

・AGDクラスの再構成：AGD_PRE(Preparation:利用者に関わる配付とIGS関連を含める)、AGD_OPE(Operation:現在のAGD_ADM,_USRを統合)

・ADO_IGS（利用者の責任に関する事項）⇒ AGD_PREへ移す

・ADO_IGS（開発者の責任に関する事項）⇒ ALC_CMCへ移す

・ADO_DEL（利用者に関する事項）⇒ AGD_PREへ移す

・ADO_DEL（開発者に関する事項）⇒ALC_DELへ移す

・構成管理のSCPとCAPの重複箇所を削除して、scope（ALC_CMS:構成リストに含める内容）とcapability（ALC_CMC:構成管理システムへの要求事項）に関わる要求内容を明確に区別した。これに合わせて、AUTに関わる要求をALC_CMCに含める。

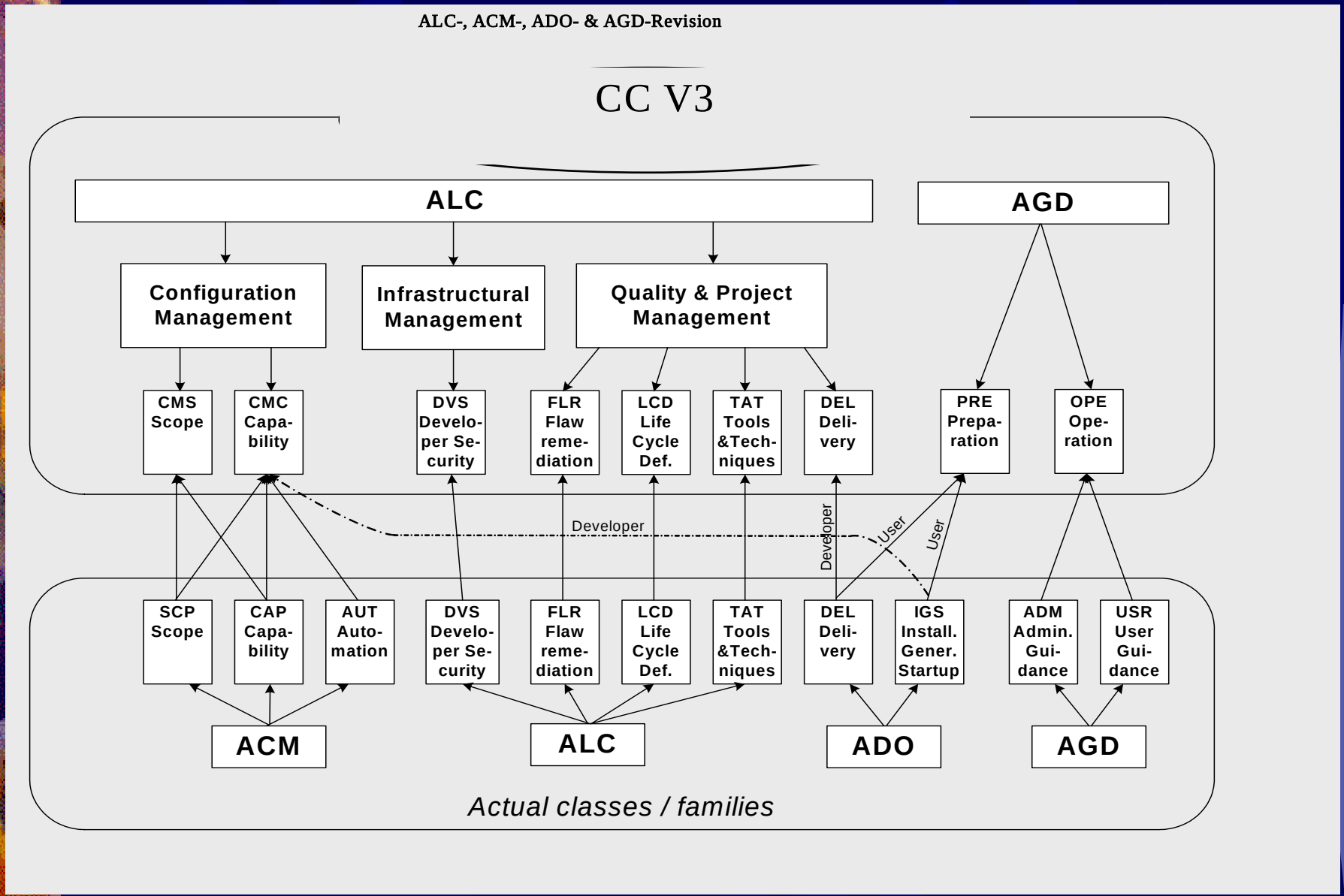
クラス/ ファミリー構成は以下。

AGDクラス：AGD_PRE, AGD_OPE

ALCクラス：

ALC_CMS, ALC_CMC, ALC_DVS, ALC_FLR, ALC_LCD, ALC_TAT, ALC_DEL

ライフサイクルサポート(ALC)/ ガイダンス(AGD) その2



脆弱性分析（AVA）　その1

●脆弱性分析は、TOEの動作環境において、存在する脆弱性が攻撃を受けるような脅威が存在しないことを検証する。

●EAL１評価に脆弱性分析を導入

　評価者が公開情報を　探索して脆弱性分析を実施。

●開発者分析と評価者分析

　脆弱性評価は評価者が主導するように変更。ただし、上位の脆弱性分析では、開発者による潜在している脆弱性に係わる分析を要求。

脆弱性分析(AVA)　その2

●明白な脆弱性

- 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

- 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。

●ファミリ名称

AVA_VAN (Vulnerability Analysis：脆弱性分析)

●V2の機能強度(AVA_SOF)は脆弱性分析(VAN)に移した。

●V2に存在している誤使用分析(AVA_MSU)はガイダンス（AGD_OPE）に移した。

脆弱性分析(AVA)　その3

AVA_VAN.1

公開情報に基づいて、潜在する脆弱性を探索する。EAL1で要求。

AVA_VAN.2

ガイダンス文書、機能仕様書、構造設計に基づいて、潜在する脆弱性を探索する。基本レベルの攻撃力に対抗できることを検証する。EAL2,3で要求。

AVA_VAN.3

ガイダンス文書、アーキテクチャ文書、機能仕様書、構造設計、論理設計、ソースコードの一部に基づいて、潜在する脆弱性を探索する。拡張された基本レベルの攻撃力に対抗できることを検証する。EAL4で要求。

脆弱性分析(AVA)　その4

AVA_VAN.4

ガイダンス文書、アーキテクチャ文書、機能仕様書、構造設計、論理設計、ソースコードの一部に基づいて、潜在する脆弱性を探索する。中レベルの攻撃力に対抗できることを検証する。EAL5で要求。

AVA_VAN.5

ガイダンス文書、詳細なアーキテクチャ文書、機能仕様書、構造設計、論理設計、ソースコードの一部に基づいて、潜在する脆弱性を探索する。高レベルの攻撃力に対抗できることを検証する。EAL6,7で要求。

システム評価について

運用システムのセキュリティ評価

ISOで運用システム評価のための評価基準と評価方法を作成中

TR：19791

タイトル：Security assessment of operational systems

スケジュール：2006．5に規格化予定

CCのサポート文書として登録される予定（2006．5）。

システム評価をより有効に、正確に、簡便に行うために、CC/CEMを拡張するもの。

現在のISO 15408/18045で運用システムの評価は可能だが？

運用システムを評価する際の主要課題

Ⅰ.異なるセキュリティポリシー（目標とする保証内容や許容リスクなど）を持つサブシステムの複合体に対する評価

Ⅱ.日々運用環境が変化するシステムに対する評価と維持

Ⅲ.非ITセキュリティ対策（手続きや規則などの規定による管理など）に対する評価

システム評価の位置づけ

ライフサイクル

リスク評価
-リスク識別
-許容リスク

→

開発/インテグレーション
- 開発
- インテグレーション
- 構成管理
- テスト
- 組織化

→

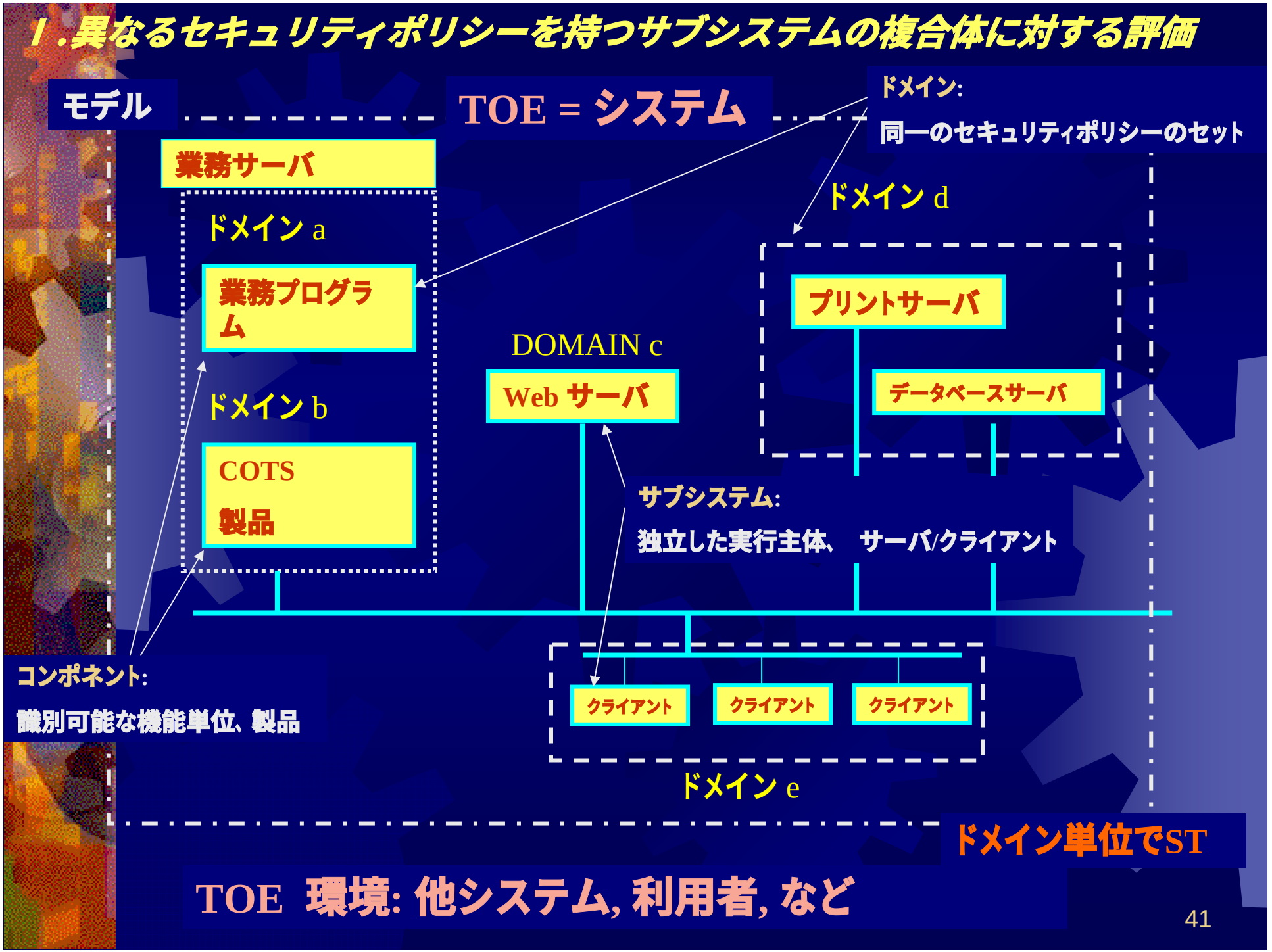
認定
潜在リスクの許容

→

運用/保守
セキュリティ制御に関わる記録採取
- 変更レビューとテスト

評価
- 運用システムに対するセキュリティ目標の規定 (ST作成)と評価
- 脆弱性分析の評価
- 運用システムがSTに準拠していることを検証 (運用実績も検証)

Ⅰ.異なるセキュリティポリシーを持つサブシステムの複合体に対する評価



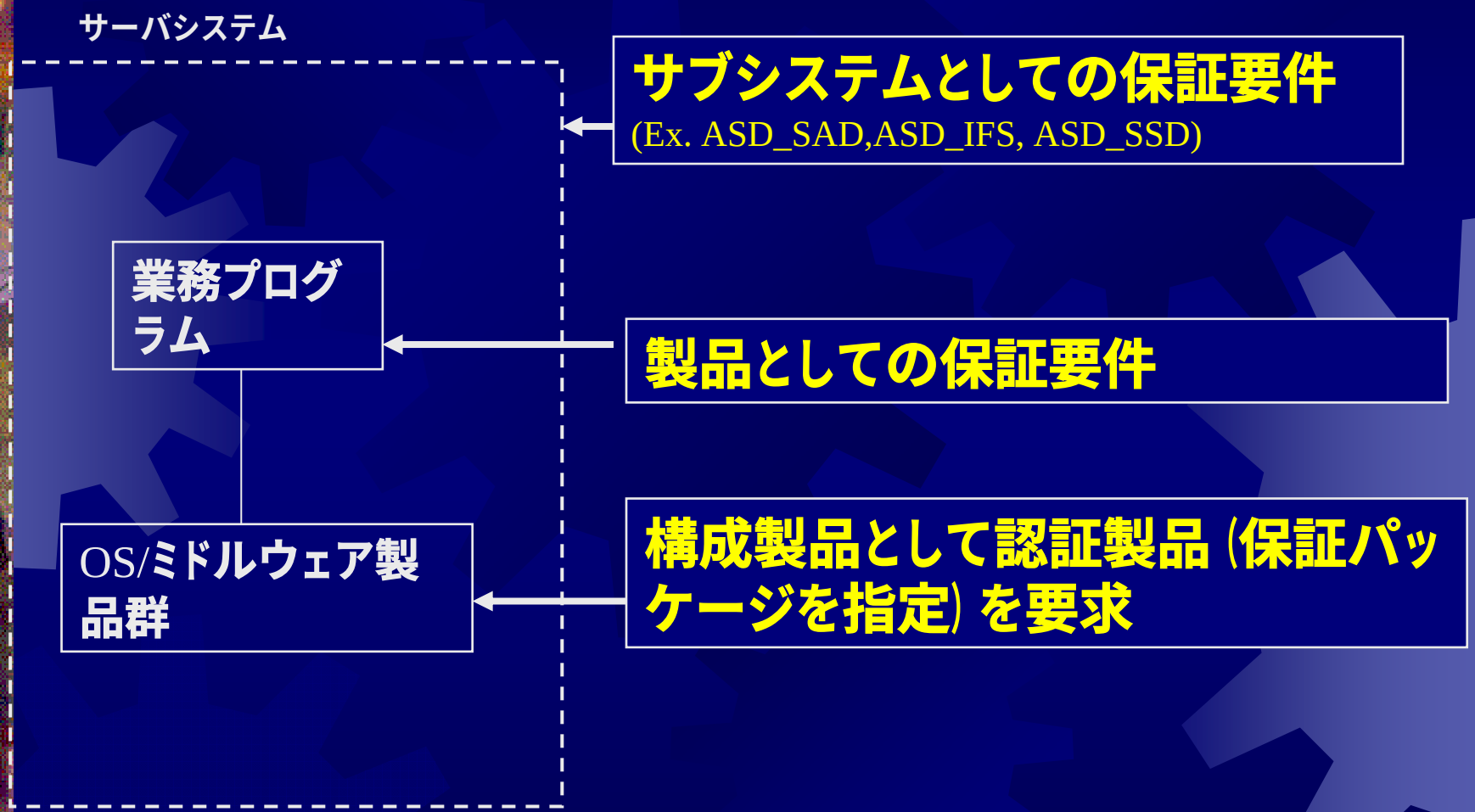
保証要件： 有効性

ライフサイクル	保証の対象	保証ファミリー
開発	リスクへの対抗性	SST/SPP評価 (AST/ASP)
	アーキテクチャー	アーキテクチャー設計 (ASD_SAD
		サブシステム設計 (ASD_SSD)
		コポネント設計 (ASD_CMP)
		実装 (ASD_IMP)
		インタフェース (ASD_IFS)
		運用 (ASD_COM)
	開発環境	セキュアー開発環境 (AOL_DVS)
導入	メカニズム強度	セキュリティ機能強度 (AOV_SOF)
		脆弱性分析 (AOV_VLA)
	広報と認識	広報の確認 (ASI_CMM)
		認識の確認 (ASI_AWA)
運用	監視と検証	状態の検出 (AOV_MSU)
		機能の動作確認 (AOD, ASI, ASC
修正	リグレッションテス	リグレッションテスト (AOT_REG)
	侵入テスト	侵入テスト (AOV_VLA)

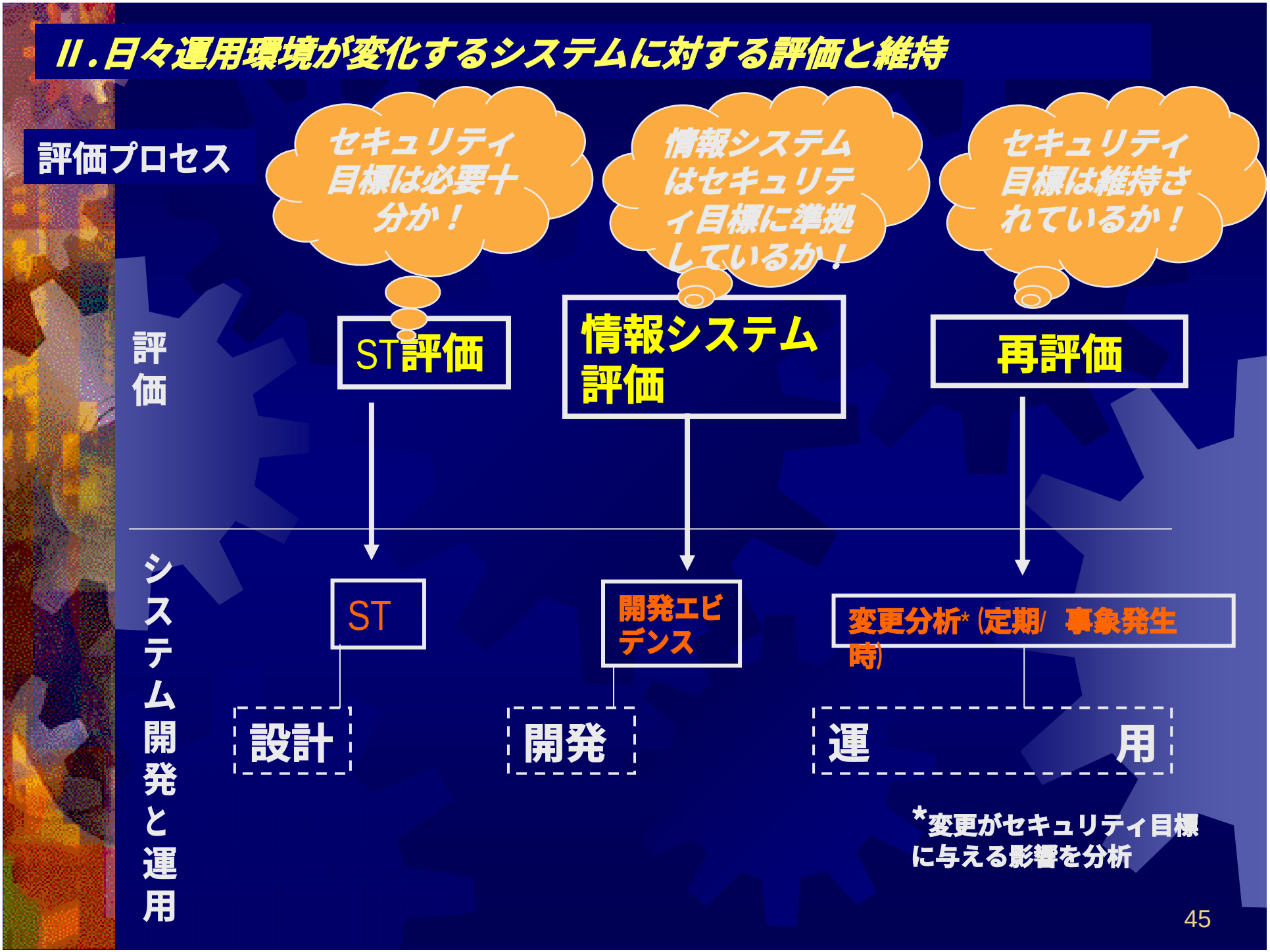
保証要件：正確性

ライフサイクル	保証の対象	保証ファミリー
開発	上流←→下流	SST/SPP評価 (AST/ASP)
	開発作業	アーキテクチャー設計 (ASD_SAD)
		サブシステム設計 (ASD_SSD)
		コポネント設計 (ASD_CMP)
		実装 (ASD_IMP)
		インタフェース (ASD_IFS)
		テスト (AOT)
		運用 (ASD_COM)
	構成管理	構成管理 (AOD_OCD)
	ガイダンス文書	ガイダンス表現 (AOD)
導入	準拠	ガイダンス表現 (AOV_MSU)
	構成管理	構成管理 (AOC)
		テスト (AOT)
	起動	起動 (ASI_SIC)
運用	監視と検証	監視 (ASO_MON)
		機能の動作検証 (AOD, ASO)
修正	リグレッションテス	リグレッションテスト (AOT_REG)
	設計の検証	設計の検証 (AOD_GVR, ASD_GVR)

製品の集合体に対する保証の考え方

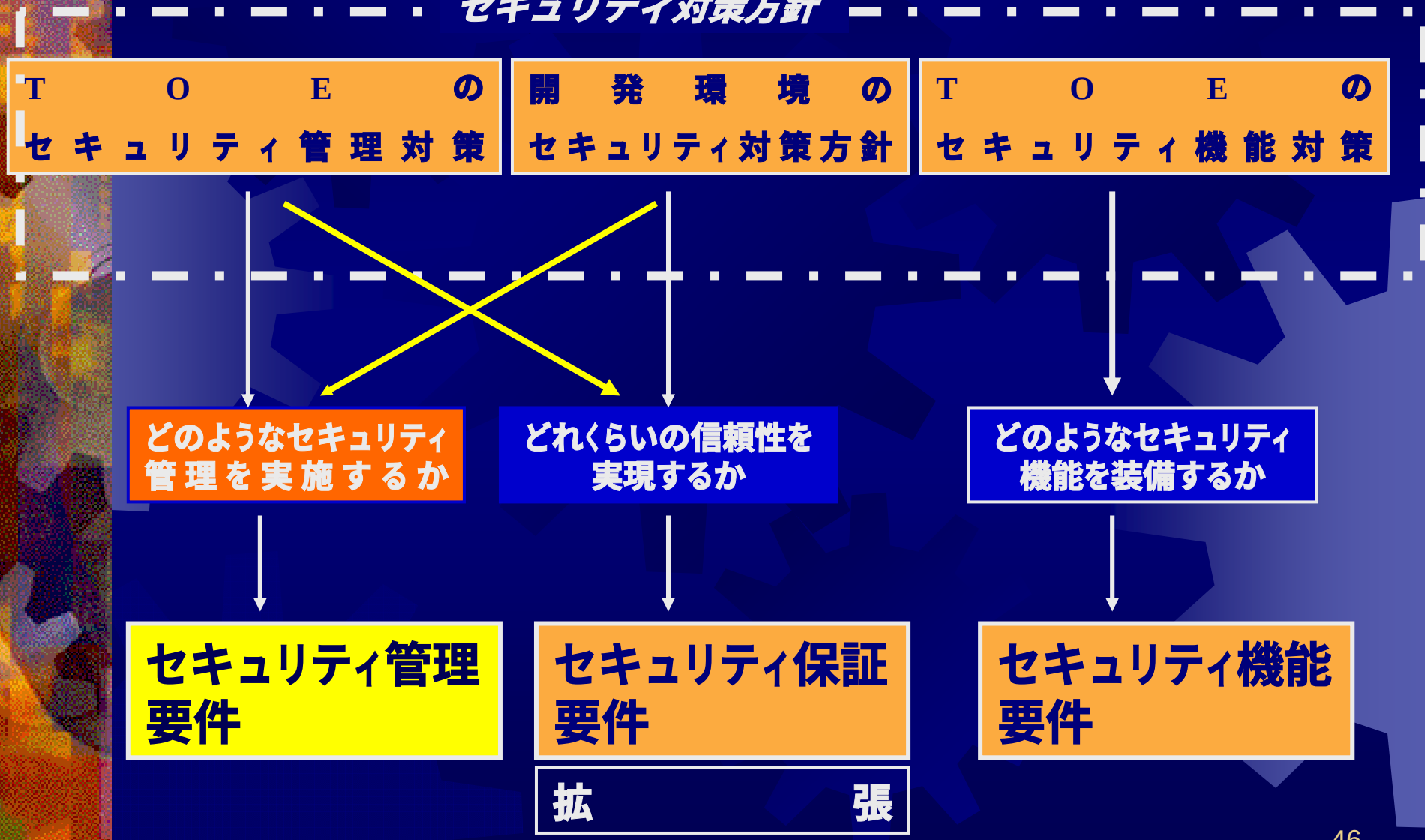


II.日々運用環境が変化するシステムに対する評価と維持

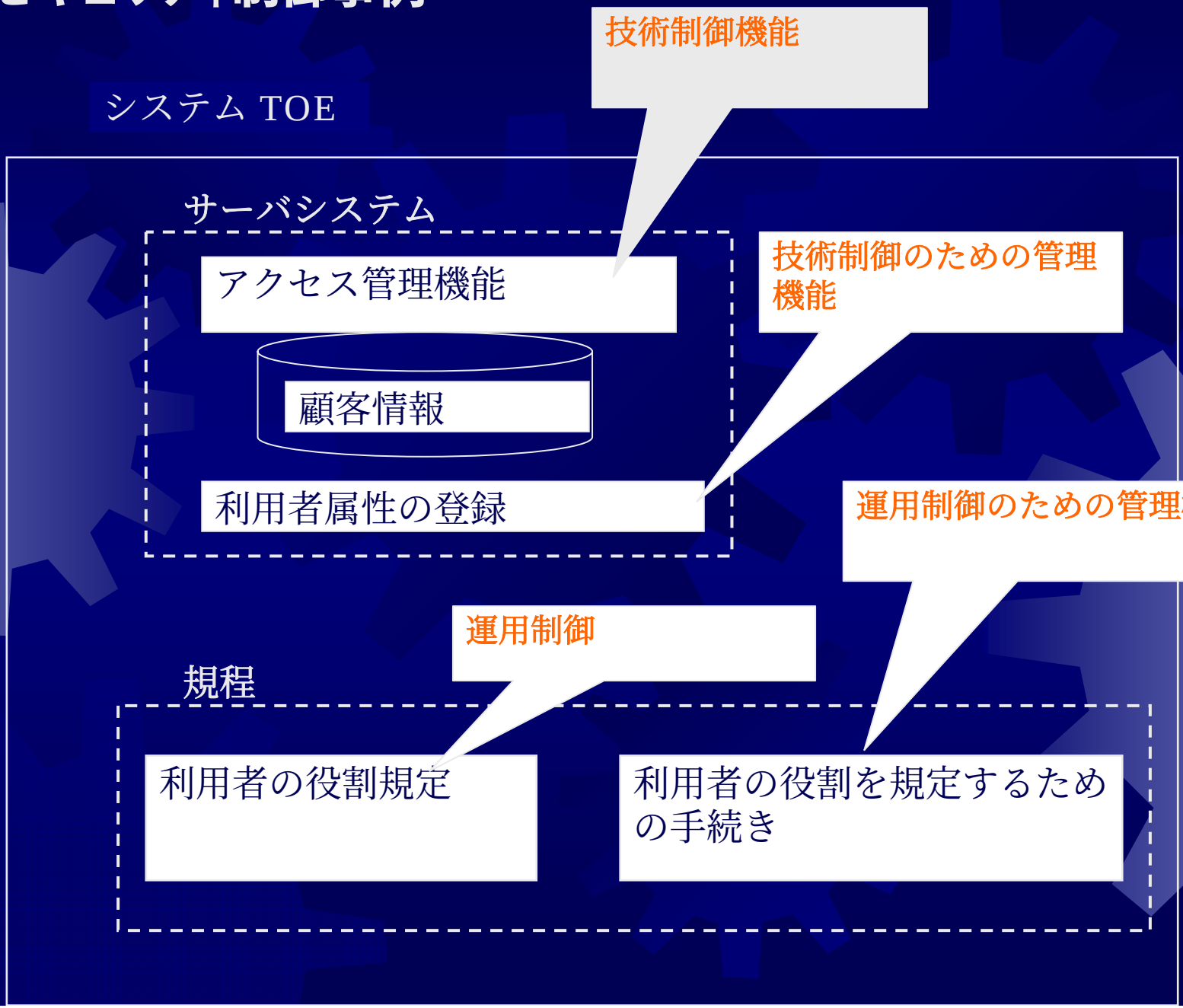


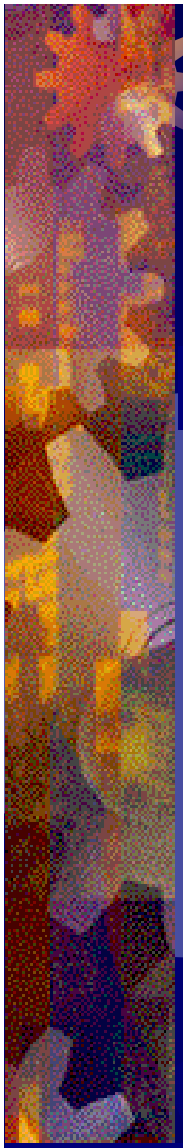
III.非ITセキュリティ対策に対する評価

非ITセキュリティ機能要件・保証要件の追加



セキュリティ制御事例


技術制御機能
システム TOE
サーバシステム
アクセス管理機能
顧客情報
技術制御のための管理機能
利用者属性の登録
運用制御のための管理機能
運用制御
規程
利用者の役割規定
利用者の役割を規定するための手続き



機能要件の概要

技術制御のための機能要件

CCパート2＋修整

運用制御のための機能要件

運用システム管理(FODクラス)

ITシステム管理(FOSクラス)

利用者資産管理(FOAクラス)

業務管理(FOBクラス)

施設･機器管理(FOPクラス)

第三者機関管理(FOTクラス)

一般管理(FOMクラス)

参照規格

-ISO 17799: Code of Practice for Information Security Management

-ISO TR 13335: Guidelines for the Management of IT Security

-NIST SP 800-53: Recommended Security Controls for Federal Information Systems