IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

CC評価を理解するための開発者向け説明会

2012年6月25日

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

本講座の目標

①国際標準のセキュリティ評価の考え方を理解すること
（セキュリティ欠陥をなくすための観点）
②開発者に対するCC評価の要求資料を理解すること

- CC（Common Criteria）とは
  - ITセキュリティ評価の国際標準規格
  - ISO/IEC 15408としても知られる
- CCの用途
  - 米国をはじめ多くの国でIT製品の調達要件
  - 日本も採用（政府機関の情報セキュリティのための統一管理基準）
- CCの評価概要
  - セキュリティ機能が正しく実装され脆弱性がないことを評価者が評価
  - 開発プロセス全般についてセキュリティ欠陥がないことを評価
    - 開発者の設計書、テスト内容、マニュアル
    - 製品の完全性と機密性のために開発環境や配送手段も評価

目次

- CC評価の概要
- 開発
- テスト
- ガイダンス文書
- ライフサイクルサポート
- 脆弱性評定とセキュリティアーキテクチャ
- おわりに

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Common Criteria(CC)評価の概要

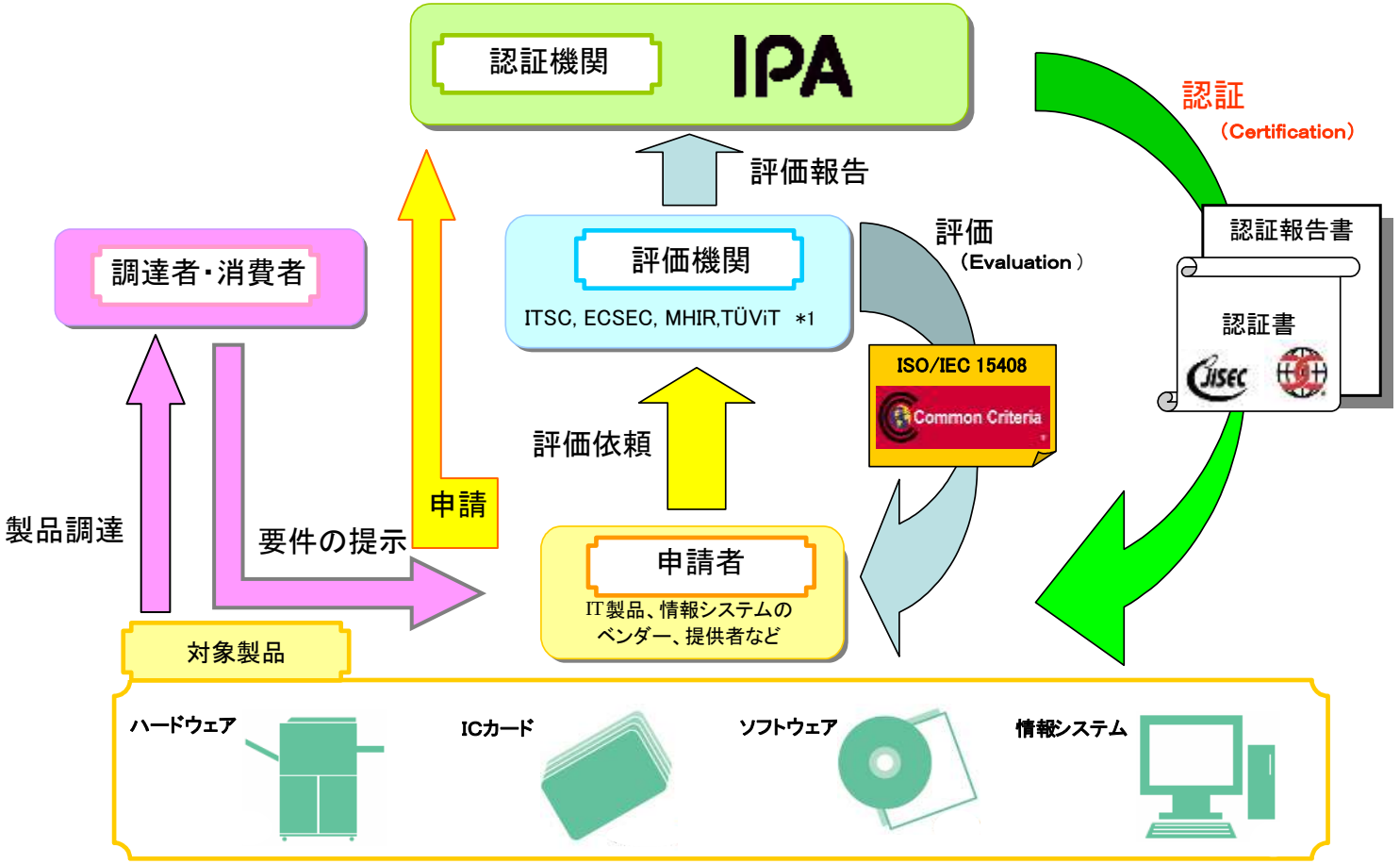
CC評価認証制度の概要

詳細は、
http://www.ipa.go.jp/security/jisec/

評価機関がCCに基づきIT製品を評価。
認証機関が評価結果を認証。

認証結果は、CCRA（CC承認アレンジメント）加盟国で有効

2012年5月時点で26カ国



*1 ITSC：一般社団法人ITセキュリティセンター、ECSEC：株式会社電子商取引安全技術研究所、MHIR：みずほ情報総研株式会社、TÜViT: TÜV Informationstechnik GmbH

CC評価の概要

セキュリティターゲットに達成すべき要件を記述。
セキュリティターゲットに従って評価対象（TOE）を評価。

開発者自身の要件

プロテクションプロファイル（PP）
- 製品のセキュリティに対する要求内容
- 通常、調達者が指定（存在しない場合もある）

PPは、これまで、各国個別に作成されていた。
最近、各国共通のPPが開発されつつある。

開発者

セキュリティターゲット（ST）
- 評価対象（TOE）の範囲
- 運用上の前提条件（運用環境のセキュリティ対策方針）
- TOEの構成条件
- 達成すべきセキュリティ機能要件 （SFR）
- 達成すべきセキュリティ保証要件
- その他

本講座の対象外（別途講座あり）

評価者による評価
①STの妥当性
②STに従ったTOE評価

評価対象（TOE）
- 評価対象製品およびマニュアル
- 評価に必要な証拠資料
  - TOEの開発資料（設計、ソースコード、テスト）
  - TOEの開発環境等のセキュリティ対策資料
- 開発、製造、出荷の現場

本講座の対象

- SFRの正確完全な設計実装
- 開発者テストの妥当性
- TOEの開発、製造、出荷環境のセキュリティ対策の妥当性（評価者による現地調査含む）
- 評価者によるテスト実施
- 評価者による脆弱性評定

CC評価規格

- 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（CC）
  - パート１　概説と一般モデル
    - セキュリティ評価の概要
    - 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）の内容
  - パート２　セキュリティ機能コンポーネント
    - セキュリティ機能要件のカタログ集
    - PPやSTの作成時に選択する
  - パート３　セキュリティ保証コンポーネント
    - セキュリティ保証要件のカタログ集
    - 評価保証レベル（EAL）の定義
- 情報技術セキュリティ評価のための共通方法（CEM）
    - CCパート３のセキュリティ保証要件に対する、具体的な評価方法

CC規格原文は以下のURLより入手可能。最新版は、バージョン3.1 リリース3
http://www.ipa.go.jp/security/jisec/cc/index.html

CCパート２の内容例

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*]。

CCパート2には、以下の11分野(クラス)のセキュリティ機能要件(SFR)が定義。

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

FIA_AFL.1	**認証失敗時の取り扱い**
	下位階層: なし
	依存性: FIA_UAU.1 認証のタイミング
FIA_AFL.1.1	**TSF** は、[割付: *認証事象のリスト*]に関して、[選択: *[割付: 正の整数値]*、*[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。
FIA_AFL.1.2	不成功の認証試行が定義した回数に達するか上回ったとき、**TSF** は、[割付: *アクションのリスト*]をしなければならない。

CCパート３の内容例

ADV_FSP.4	**完全な機能仕様**
	依存性: ADV_TDS.1 基本設計
	開発者アクションエレメント:
ADV_FSP.4.1D	開発者は、機能仕様を提供しなければならない。
ADV_FSP.4.2D	開発者は、機能仕様から SFR への追跡を提供しなければならない。
	内容・提示エレメント:
ADV_FSP.4.1C	機能仕様は、完全に TSF を表現しなければならない。
ADV_FSP.4.2C	機能仕様は、すべての TSFI の目的と使用方法を記述しなければならない。
ADV_FSP.4.3C	機能仕様は、各 TSFI に関連するすべてのパラメタを識別及び記述しなければならない。
ADV_FSP.4.4C	機能仕様は、各 TSFI に関連する**すべての**アクションを**記述**しなければならない。
ADV_FSP.4.5C	**機能仕様は、各 TSFI の呼び出しによって発生する可能性があるすべての直接的誤りメッセージを記述しなければならない。**
ADV_FSP.4.6C	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。
	評価者アクションエレメント:
ADV_FSP.4.1E	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。***
ADV_FSP.4.2E	評価者は、機能仕様が、SFR の正確かつ完全な具体化であることを***決定しなければならない。***

開発者への要求事項（提供すべき資料等）

提供すべき資料等に対する要求事項

評価者への要求事項

CEMの内容例

CCパート３の評価者アクションエレメントに対して、さらに詳細な評価内容を記述。
以下は、ADV_FSP.4に対する内容の一例。

ADV_FSP.4-6	評価者は、TSFI の提示がすべての TSFI に関連するすべてのパラメタを完全かつ正確に記述していることを決定するために、その提示を***検査しなければならない。***
644	すべてのパラメタが識別されたら、評価者は、それらが正確に記述されていること、及びパラメタの記述が完全であることを保証する必要がある。パラメタの記述は、そのパラメタが何であるかを意味のある形で伝える。例えば、インタフェース *foo(i)*について、「整数であるパラメタ i」を持つと記述されていた場合、この記述は、パラメタの記述としては受け入れられない。これが、「パラメタ i は、現在システムにログインしている利用者の数を示す整数である」などになると、はるかに受け入れられる記述となる。
645	パラメタの記述が完全であることを決定するには、評価者は、パラメタの記述が含まれているかどうかを決定するために、残りのインタフェース記述(目的、使用方法、アクション、誤りメッセージなど)を検査するべきである。評価者は、機能仕様に含まれていないふるまいや追加のパラメタが記述されていないかどうかを確認するために、提供されているその他の証拠(例えば、TOE 設計、アーキテクチャ設計、利用者操作ガイダンス、実装表現)もチェックするべきである。

～しなければならない（shall）
⇒必須

～するべきである（should）
⇒強い要請（原則必須）
除外には合理的理由必要

CEMには、CCパート３だけではわからない詳細な要求内容が記述されている。
従って、開発者もCEMの要求内容を理解しておく必要がある。

保証要件とEAL

EALは、保証コンポーネント（保証要件）をパッケージ化したもの。
EALが高いほど、より詳細な評価が実施される。
EALが高いほど、対抗すべき攻撃のレベルが上がる。

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	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
AGD 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	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	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
テスト ATE	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
AVA 脆弱性評定	AVA_VAN	1	2	2	3	4	5	5

CCパート3
表24 評価保証レベルの要約

（表の見方）
EAL4の「開発」には、以下の保証コンポーネント（保証要件）が含まれる。
ADV_ARC.1　セキュリティアーキテクチャ
ADV_FSP.4　機能仕様（インタフェース）
ADV_IMP.1　実装表現（ソースコード）
ADV_TDS.3　TOE設計（内部設計）

保証コンポーネントの詳細な評価内容は、CEMに記述されている。
例えば、ADV_FSP.4には、ADV_FSP.4-1～ADV_FSP.4-12の評価項目がある。

表中の数字が大きいほど、検査内容が増加し、より詳細な評価が実施される。
⇒開発者に要求される証拠資料増加。

CC評価で要求されるもの

評価対象製品に加えて、EALに応じた評価証拠資料が必要。
評価中の評価機関への対応も必要（サイト訪問や各種質問対応等）。

①製品開発に係る各種文書：評価証拠資料
（EALが上がるにつれ要求される情報が多くなる）

要件分析/定義 → 基本設計 → 詳細設計 → プログラム設計 → プログラム実装 → 各種テスト → 設置・運用

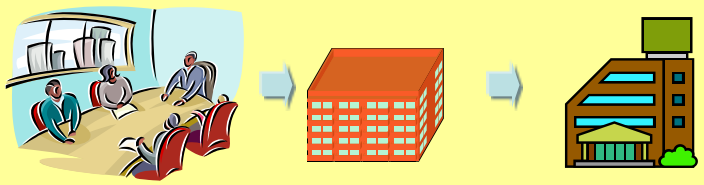
セキュリティターゲット（ASE）	機能仕様、内部設計、詳細設計（ADV）	ソースコード（ADV）	テスト文書（ATE）	各種マニュアル（AGD）

本講座の対象外

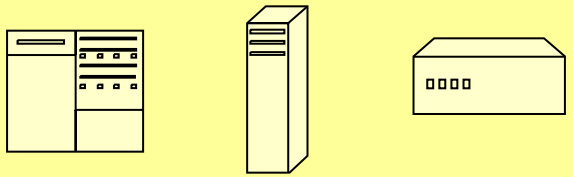
構成管理、配付、開発セキュリティ、ツール等に係る文書（ALC）

②サイト訪問対応
（EAL2より要求される）

開発現場 → 組立工場 → 出荷工場



③製品本体及びテスト環境
（評価者がEALに応じたテストを実施）



本講座の範囲

- 規格は、CC/CEMバージョン3.1 リリース3
- EAL4を対象に要求される証拠資料を解説
  - 多くは設計書など開発者が通常作成する資料
    （ただし、CC/CEMの要求を満足する必要がある）
  - CC評価特有の資料もある
    （セキュリティアーキテクチャ、SFRと仕様のマッピングなど）

①開発(ADV)	ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, ADV_ARC.1
②テスト(ATE)	ATE_FUN.1, ATE_COV.2, ATE_DPT.1 ATE_IND.2は評価者によるテストのため省略
③ガイダンス文書(AGD)	AGD_OPE.1, AGD_PRE.1
④ライフサイクルサポート(ALC)	ALC_LCD.1, ALC_CMC.4, ALC_CMS.4, ALC_TAT.1, ALC_DVS.1, ALC_DEL.1
⑤脆弱性評定(AVA)	AVA_VAN.3 （AVAと関係の深いADV_ARC.1の解説を含む）

※本講座にはセキュリティターゲットは含まない。

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

開発（ADV）

開発評価の目的（1）

セキュリティ機能要件（SFR）の達成

製品設計
（要件定義）

製品の目的
・・・・・
セキュリティ
機能要件
・・・・

ST（セキュリティ機能要件）

製品開発は、要件を変換するプロセス

多くの欠陥は、この変換の過程で発生

仕様設計

XXXコマンド仕様
・・・・・
YYYコマンド仕様
・・・・・
ZZZコマンド仕様
・・・・・
・・・・・
・・・・・
・・・・・

ADV_FSP（機能仕様） 外部インタフェース仕様
ADV_TDS（TOE設計） 内部設計仕様

プログラミング

```
module HelloApp
{
    interface Hello
    {
        {};
        exception exception cantWriteFile cantReadFile{};
        string sayHello(in string message)
                raises (cantWriteFile);
        string lastMessage()
                raises (cantReadFile);
    };
};
```

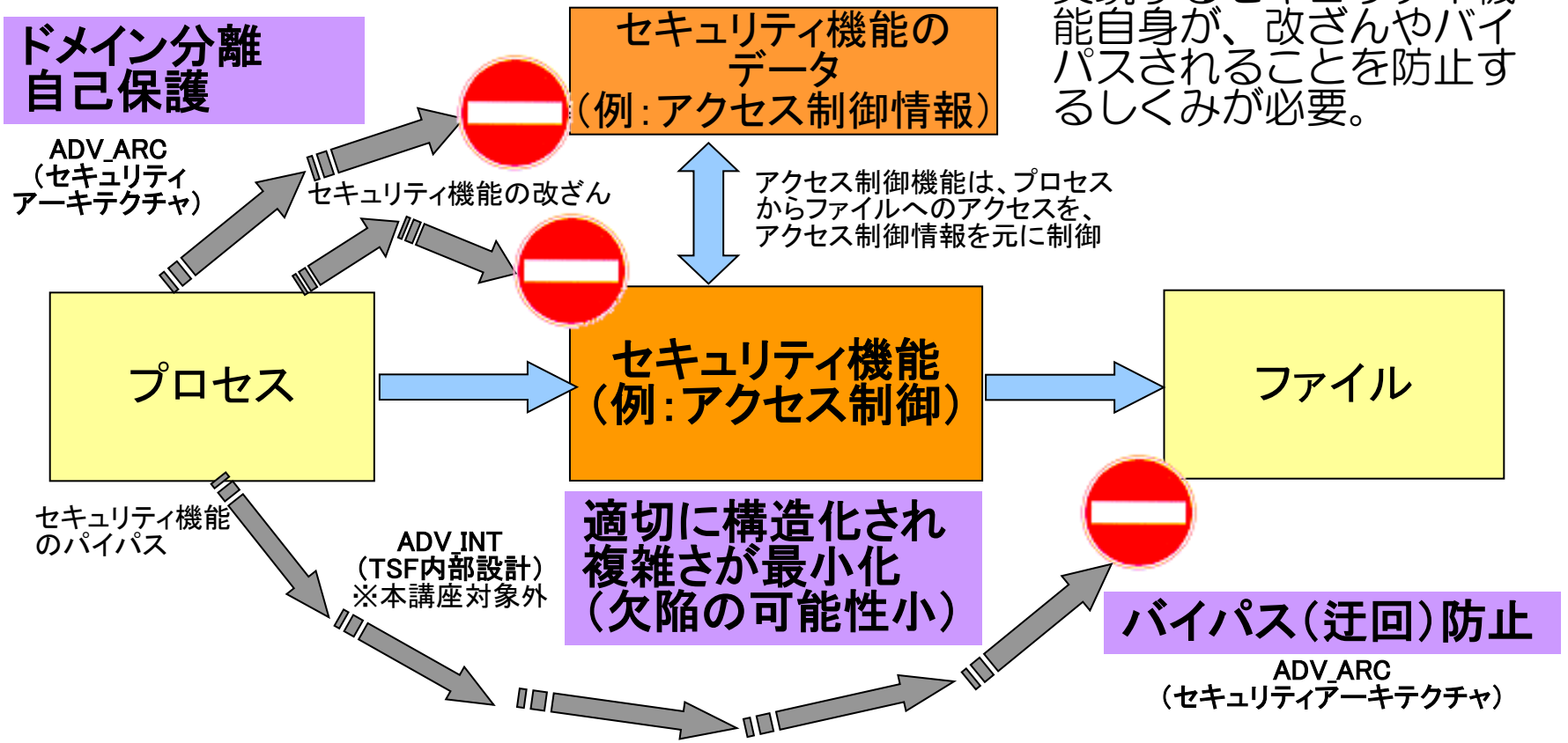
ADV_IMP（実装表現）

セキュリティ機能要件から設計・実装への変換が、正確かつ完全に行われているかを評価

開発評価の目的（2）

セキュリティ機能の保護

セキュリティ機能要件を実現するセキュリティ機能自身が、改ざんやバイパスされることを防止するしくみが必要。



セキュリティ機能自身が保護され、バイパスされないことを評価

※EAL5以上では、内部的に適切に構成されていることも評価される

開発評価の理解に必要な概念

- TSF（TOEセキュリティ機能）
- TSFI（TSFインタフェース）
- TSFとTSFIの分類
  - SFR実施、SFR支援、SFR非干渉
    （セキュリティ機能要件（SFR）との関連度合い）

TSF（TOEセキュリティ機能）とは

TSFはSFRが正しく動作するために必要なすべてのサブシステムやモジュール。
SFRとの関連性に応じてSFR実施/支援/非干渉に分類される。

SFRとの関連性に応じて、評価者が検査する情報量が異なる。
・SFR実施が最も詳細。
・セキュリティアーキテクチャはSFR実施と同じく最も詳細。

セキュリティ機能要件（SFR）

直接的に対応

（例）FDP_ACC.1
TSFは、[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御SFP]を実施しなければならない。

開発者はSFR実施/支援/非干渉を識別する必要はない。（EAL5以上では必要）

ただし、TSF/Non-TSFの区別は重要。特に、SFR非干渉は間違えやすいので注意が必要。

TOE（評価対象製品）

TSF

セキュリティ機能の保護を実現する部分（セキュリティアーキテクチャ(ADV_ARC)）も含まれる。

（例）
利用者のファイル操作に対して、アクセス制御情報を元に、許可・不許可を制御。

SFR実施

機能提供（SFRを実現するために、機能を利用）

（SFR実施のために誤りなく動作することが要求される）

SFR支援

SFR実施をサポート

（例）
アクセス制御情報を格納した設定ファイルの読み込み。

SFR非干渉

機能的にはSFRに無関係

SFRを実現する機能の動作に影響を与えることが可能

（SFRの動作のために、干渉しないことが要求される）

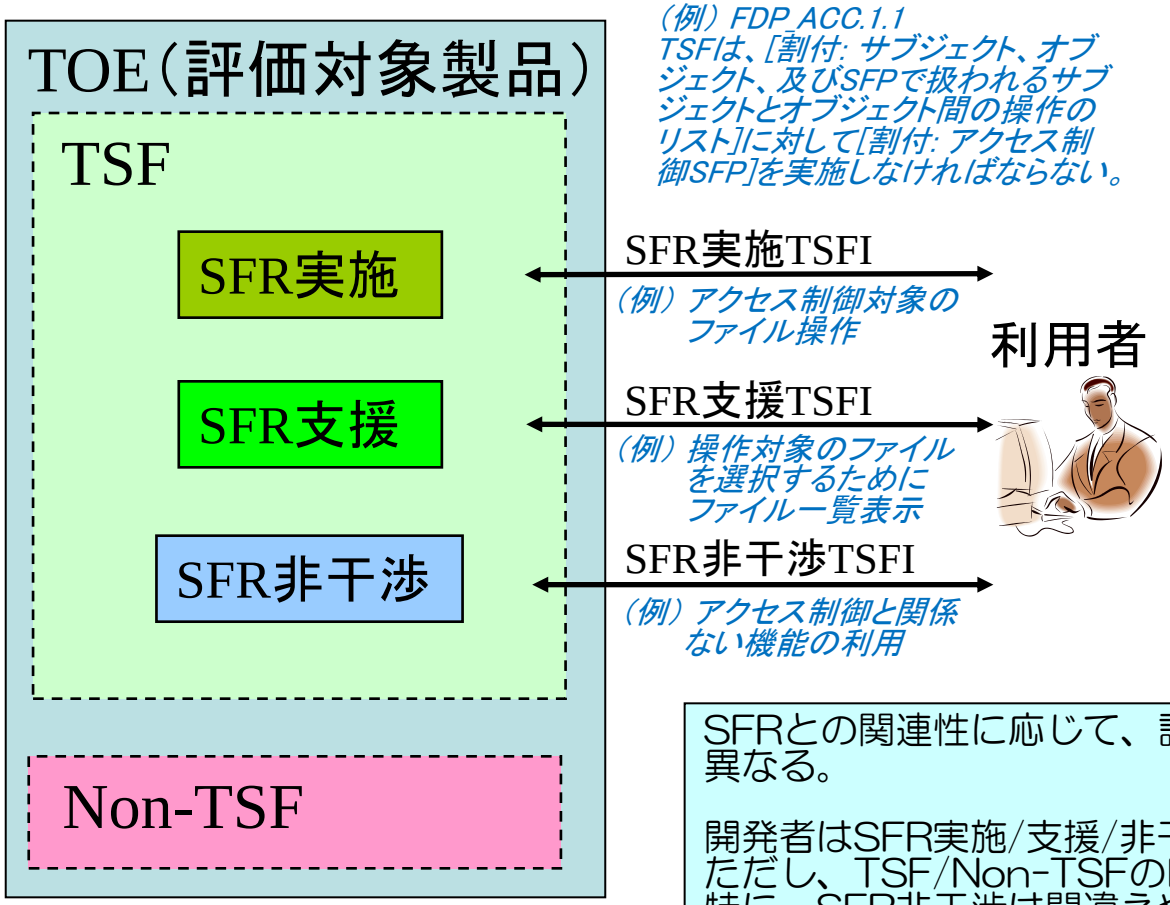
（例）
アクセス制御と関係のない機能。

Non-TSF

セキュリティアーキテクチャにより、セキュリティ機能（TSF）がNon-TSFから影響を受けないように保護されていれば、Non-TSFは評価をする必要がない

TSFI（TSFインタフェース）とは

TSFIは、利用者がTSFに対して、データを供給・入手したり、サービスを呼び出したりするインタフェース。
SFRとの関連性に応じて、SFR実施/支援/非干渉に分類される。



（例）FDP_ACC.1.1
TSFは、[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御SFP]を実施しなければならない。

SFR実施TSFIによって実行されるTSFの機能には、必ずSFR実施の機能を含む。

SFR支援TSFIによって実行されるTSFの機能には、SFR実施の機能を含まない。

SFR非干渉TSFIによって実行されるTSFの機能には、SFR実施やSFR支援の機能を含まない。

SFRとの関連性に応じて、評価者が検査する情報量が異なる。

開発者はSFR実施/支援/非干渉を識別する必要はない。
ただし、TSF/Non-TSFの区別は重要。
特に、SFR非干渉は間違えやすいので注意が必要。

機能仕様
(ADV_FSP)

機能仕様評価の目的と証拠資料

目的

- STに記載されたSFRが、外部のインタフェース仕様に、漏れなく正確に仕様化されていること

要求される証拠資料

- CCの要求事項を満たした機能仕様書
- TSFIとSFRの対応表

TSFI \ SFR	FCS_CKM.1	FCS_CKM.3	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_RIP.1
TSFI_1	×				×	×	
TSFI_2		×					
TSFI_3			×	×			

TSFI_xは、機能仕様書の中で、TSFIに該当するインタフェースの名称。

SFRの動作が、外部インタフェースから実行される機能に含まれない場合は、空欄にする。

※FDP_RIP.1（残存情報保護）は、製品内部で資源が解放/割当てされた際に、以前の情報が参照できないことを要求する機能要件。

※仕様として記述されるべきSFRを空欄にすることはできない。
（例えば、監査ログの生成など）

機能仕様評価の概要

①必要なインターフェース（TSFI）が全て記載されているか？

ADV_FSP.4-1 評価者は、TSFが完全に表現されていることを決定するために、機能仕様を検査しなければならない。

②個々のインタフェース仕様にCCで要求される情報が記載されているか？

ADV_FSP.4-2 評価者は、機能仕様が各TSFIの目的を記述していることを決定するために、その仕様を検査しなければならない。

ADV_FSP.4-2～9

- 目的：　インタフェースの全般的な説明
- 使用方法：　インタフェースがどのように使用されるかの記述
- パラメタ：　インタフェースの入力・出力パラメタ
- パラメタの記述：パラメタの説明
- アクション：　インタフェースにより実施される処理
- 誤りメッセージ：　エラーメッセージの説明

要求される情報量は、EALにより異なる。

③インタフェース仕様はSFRを正確･完全に実現しているか？

ADV_FSP.4-11 評価者は、機能仕様がSFRの完全な具体化であることを決定するために、その仕様を検査しなければならない。

ADV_FSP.4-11～12

評価者は、②の情報と、TSFIとSFRの対応表を元に、SFRが漏れなく誤りなく仕様化されているかを評価する。

機能仕様書の例

暗号化ディスクの生成インタフェースの機能仕様の例

ディスクの作成 （目的）

このセキュリティ機能は、「暗号化ディスク」の作成を可能にする。暗号化ディスクは、物理パーティション、またはコンテナ・ファイルから作成される。この機能により、暗号化ディスクのヘッダが生成され暗号化される。暗号化されたヘッダの最初から512バイトのみがコンテナ・ファイル、または物理パーティションにコピーされ、このディスクの残りのデータはフォーマットされる。
（省略）

入力インタフェース	入力データ （パラメタ）
TrueCrypt HMI （TrueCrypt暗号化ディスク作成ウィザード）	暗号化ディスクのアクセス・パス 暗号アルゴリズム ハッシュ・アルゴリズム ボリューム・サイズ ユーザ・パスワード （省略） （暗号化ディスク作成ウィザードにおいて入力するパラメタ）

実際には、パラメタを羅列するだけでなく、パラメタの説明も記述

使用方法 （暗号化ディスク作成ウィザードの起動方法）

メイン・プログラム・メニューでは：
1. 「Create volume」ボタンをクリック、
2. 「Volume」メニューをクリックし、次に「Create new volume」をクリック、または
3. 「Tools」メニューをクリックし、次に「Volume Creation Wizard」を使用。

「TrueCrypt format.exe」をダブル・クリックし、ウイザードを開始できる。

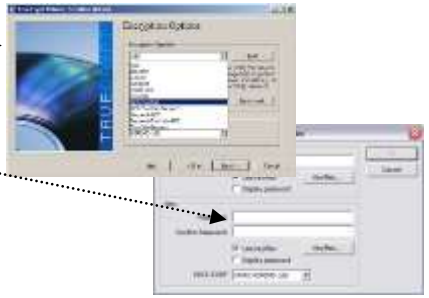
アクション （このインタフェースで行われるSFR関連の処理内容）

ランダムデータからのシード生成
ユーザ・パスワードと鍵ファイルによる修正パスワードの生成
シードと修正パスワードによるヘッダ鍵の生成
マスタ鍵の生成
暗号化ディスクの（マスタ鍵とシードが含まれる）ヘッダの作成
（シードを除く）ヘッダ鍵によるヘッダの暗号化
暗号化ディスク上への暗号化ヘッダの格納
暗号化ディスクのフォーマッティング

実際には、詳細な処理内容を記述

左記はオープンソースのTrueCryptをベースに教育用に作成されたもの。機能仕様書がこのフォーマットに従う必要はない。

TrueCrypt暗号化ディスク作成ウィザード



開発者はSFR実施やSFR支援を分類する必要はない（分類は評価者のタスク）。
左記では、
太字斜体→SFR実施＋支援アクション
太字→SFR実施アクション

機能仕様書の例（続き）

暗号化ディスクの生成インタフェースの機能仕様の例（前ページの続き）

出力インタフェース	出力データ
TrueCrypt HMI （ディスクフォーマット画面）	乱数プールの最初のバイト ヘッダ鍵の最初のバイト マスタ鍵の最初のバイト フォーマッティングの進捗 暗号化ディスクの概要 （ディスクフォーマット画面において出力されるデータ）
SFR （このインタフェースで実現されるSFR一覧）	
FCS_CKM.1／ヘッダ鍵： 暗号鍵生成 FCS_CKM.1／マスタ鍵： 暗号鍵生成 FCS_CKM.3／ヘッダ鍵： 暗号鍵アクセス FCS_CKM.3／マスタ鍵： 暗号鍵アクセス FCS_CKM.4： 暗号鍵破壊 FCS_COP.1： 暗号操作 FIA_SOS.1／パスワード： 秘密の検証 FMT_MOF.1／ディスク所有者： セキュリティ機能のふるまいの管理 FMT_MSA.2： セキュアなセキュリティ属性 FMT_MSA.3： 静的属性初期化 FMT_MTD.1／マスタ鍵： TSFデータの管理 FMT_MTD.1／ヘッダ鍵： TSFデータの管理 FMT_MTD.2／認証データ： TSFデータにおける限界値の管理 FMT_MTD.3： セキュアなTSFデータ FMT_SMF.1： 管理機能の特定 FMT_SMR.1： セキュリティの役割	

ディスクフォーマット画面

TSFIとSFRとの対応は、開発者が評価者に提示する必要がある。

※左記の形式でなくても良い。（TSFIとSFRの対応表など）

上記の他に、例外（エラー）の記述もあり

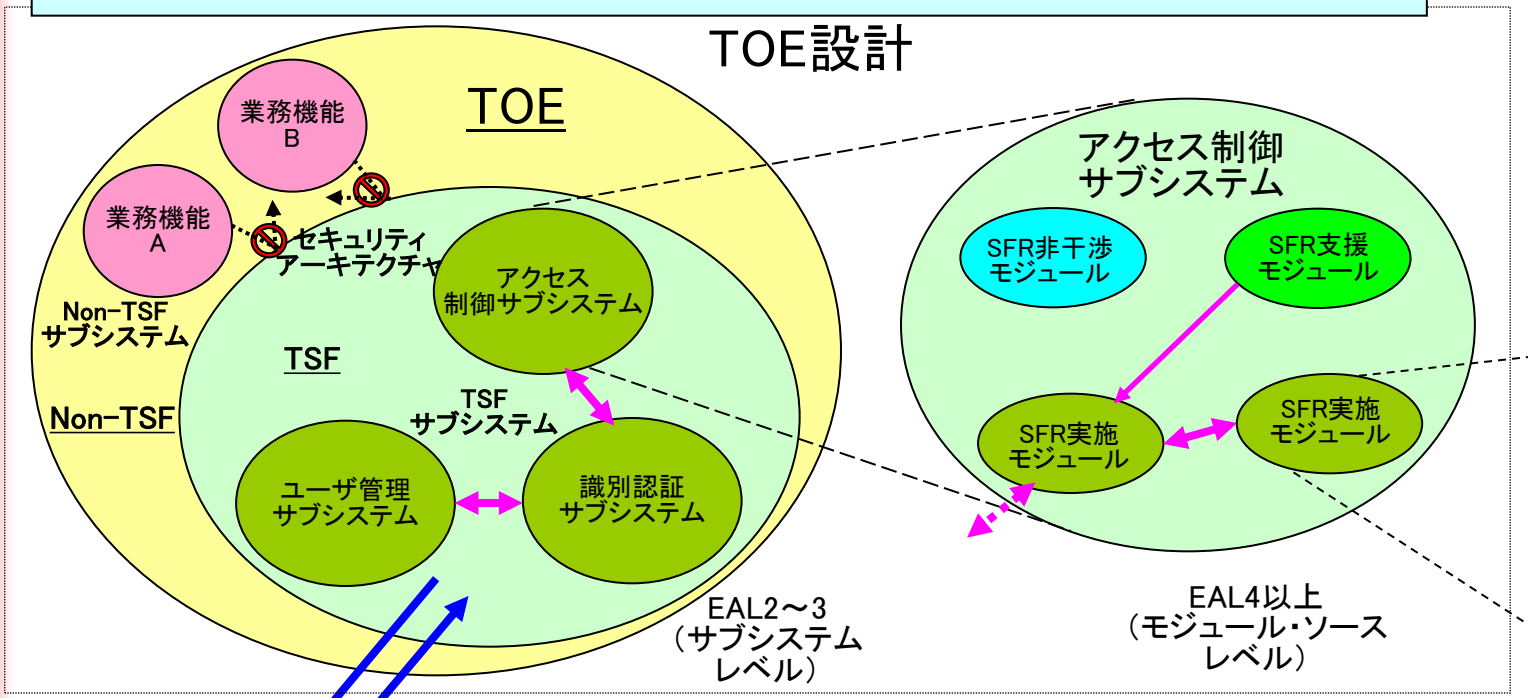
機能仕様の注意事項

- SFRを正確に漏れなく実現すること
- 仕様書からSFRの実現内容が読み取れること
- 第三者が理解できるように曖昧なく記述すること
  - 明確に定義されていない用語、一貫性のない用語、説明不足はNG（実装誤りや脆弱性の要因になりがち）
  - 例えば、パラメタが単に「整数」と書かれているだけでは不適切。「ｘｘの数を示す整数」などの記述が必要
- 各種資料間（仕様書内部、ガイダンス、TOE設計等）で一貫していること
  - 例えば、誤りメッセージの要因となる処理が、アクションとして記述されていること
  - その他、相互に記述漏れがないこと

TOE設計
(ADV_TDS)

TOE設計評価の目的

STに記載されたSFRが、製品内部の設計に、漏れなく正確に仕様化されていること



機能仕様（インタフェース仕様）は外部からみてTOEが“何（What）“をするのかを記述する

TOE設計はTOEをより小さなコンポーネント（サブシステム・モジュール）に分割し、“どのように（How）”内部的に機能するのかを記述する

コーディング（ADV_IMP）

要件定義（STのSFR）

EAL1はTOE設計は要求されない。EAL2～3はサブシステム設計、EAL4以上はサブシステム設計に加えモジュール設計が要求される。

TOE設計評価の証拠資料

- 要求される証拠資料
  - CCの要求事項を満たしたTOE設計書
  - サブシステムとモジュールの対応表
  - TSFIとモジュールの対応表

サブシステム	サブシステムに含まれるモジュール
Subsystem_X	Module_A, Module_B, Module_C
Subsystem_Y	Module_D
Subsystem_Z	Module_E, Module_F

TSFI	TSFIから呼び出されるモジュール （最初）	（呼び出される一連のモジュール）
TSFI_1	Module_A	Module_B
TSFI_2	Module_A	Module_B, Module_C
TSFI_3	Module_D	ー

TOE設計評価の概要（１）

①TOE全体がサブシステムに記述され、TSFサブシステムが識別されているか？

ADV_TDS.3-3 評価者は、TSFのすべてのサブシステムが識別されることを決定するために、そのTOE設計を検査しなければならない。

②TSFのサブシステム仕様にCCで要求される情報が記載されているか？

ADV_TDS.3-4 評価者は、TSFの各サブシステムがSTで記述されたSFRの実施におけるそれぞれの役割を記述することを決定するために、そのTOE設計を検査しなければならない。

ADV_TDS.3-1

ADV_TDS.3-4～6

- 構造：　サブシステムの観点でのTOE全体構造
- 記述：　サブシステム内のSFRを実現するメカニズム（ふるまい）
- 相互作用：サブシステム間の機能の依存関係（やりとりする目的とデータ）

要求される情報量は、EALにより異なる。

サブシステムレベルの記述には、実装レベルの詳細な仕様は求められない。
サブシステムに含まれるモジュールの概要が理解できる程度の記述が必要。

相互作用の目的は、SFRを実現するセキュリティ機能の間の関係を明確にすることであり、その目的に合った詳細度の記述が求められる。
例えば、識別認証機能（ログイン）とアクセス制御機能との間や、アクセス制御規則を設定する機能とその規則を使うアクセス制御機能との間の、主要データのやりとりや依存関係の記述が求められる。

TOE設計評価の概要（2）

③TSFサブシステムとモジュールの対応関係が記載されているか？（EAL4以上）

ADV_TDS.3-7 評価者は、TSFのサブシステムとTSFのモジュールの間のマッピングが完全であることを決定するために、そのTOE設計を検査しなければならない。

ADV_TDS.3-7～8

④モジュール仕様にCCで要求される情報が記載されているか？（EAL4以上）

ADV_TDS.3-9 評価者は、各SFR 実施モジュールの目的と他のモジュールとの関係の記述が完全で正確であることを決定するために、そのTOE設計を検査しなければならない。

ADV_TDS.3-2

ADV_TDS.3-9～13

- 目的：　モジュールが実現する機能の説明
- 相互作用：モジュール間の機能の依存関係（やりとりする目的とデータ）
- インタフェース仕様：モジュールのインタフェースの説明（入出力パラメタ、呼び出し規則、戻り値）

要求される情報量は、EALにより異なる。

モジュール仕様には、実装表現のレビューが可能な程度の記述が必要。

EAL4では、以下の詳細度で評価される。
- SFR実施モジュールは、インタフェース仕様を含めて詳細に評価される。
- SFR支援/非干渉モジュールは、目的と相互作用だけが評価される。

TOE設計評価の概要（3）

⑤サブシステム仕様やモジュール仕様はSFRを正確･完全に実現しているか？

ADV_TDS.3-16 評価者は、TOE設計がすべてのセキュリティ機能要件の正確な具体化であることを決定するために、そのTOE設計を検査しなければならない。

ADV_TDS.3-15～16

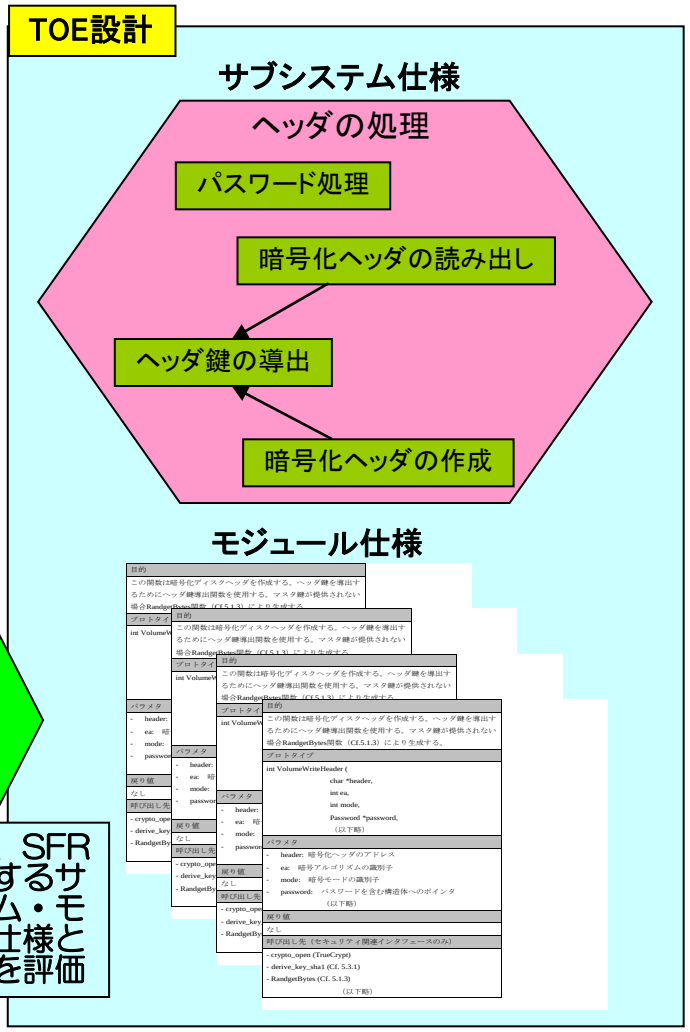
評価者は、以下の情報からTOE設計とSFRの対応を評価
- SFRとインタフェース仕様(TSFI)との対応
- TSFIとモジュールとの対応
- サブシステムとモジュールとの対応

モジュールとSFRとの対応表（評価者が作成）

サブシステム / モジュール	SFR	FCS_CKM.1／ヘッダ鍵	FCS_CKM.1／マスタ鍵	FCS_CKM.3／ヘッダ鍵	FCS_CKM.3／マスタ鍵	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_RIP.1	FIA_UID.1／ディスク所有者	FIA_UAU.1／ディスク所有者	FIA_SOS.1／パスワード	FMT_MOF.1／ディスク所有者
ヘッダの処理	パスワード処理						X						X	X
	ヘッダ鍵の導出	X		X										○
	暗号化ヘッダの作成		X	X			X							X
	暗号化ヘッダの読み出し	X		X	X		X	X	X		X	X	X	X

オープンソースのTrueCryptの例

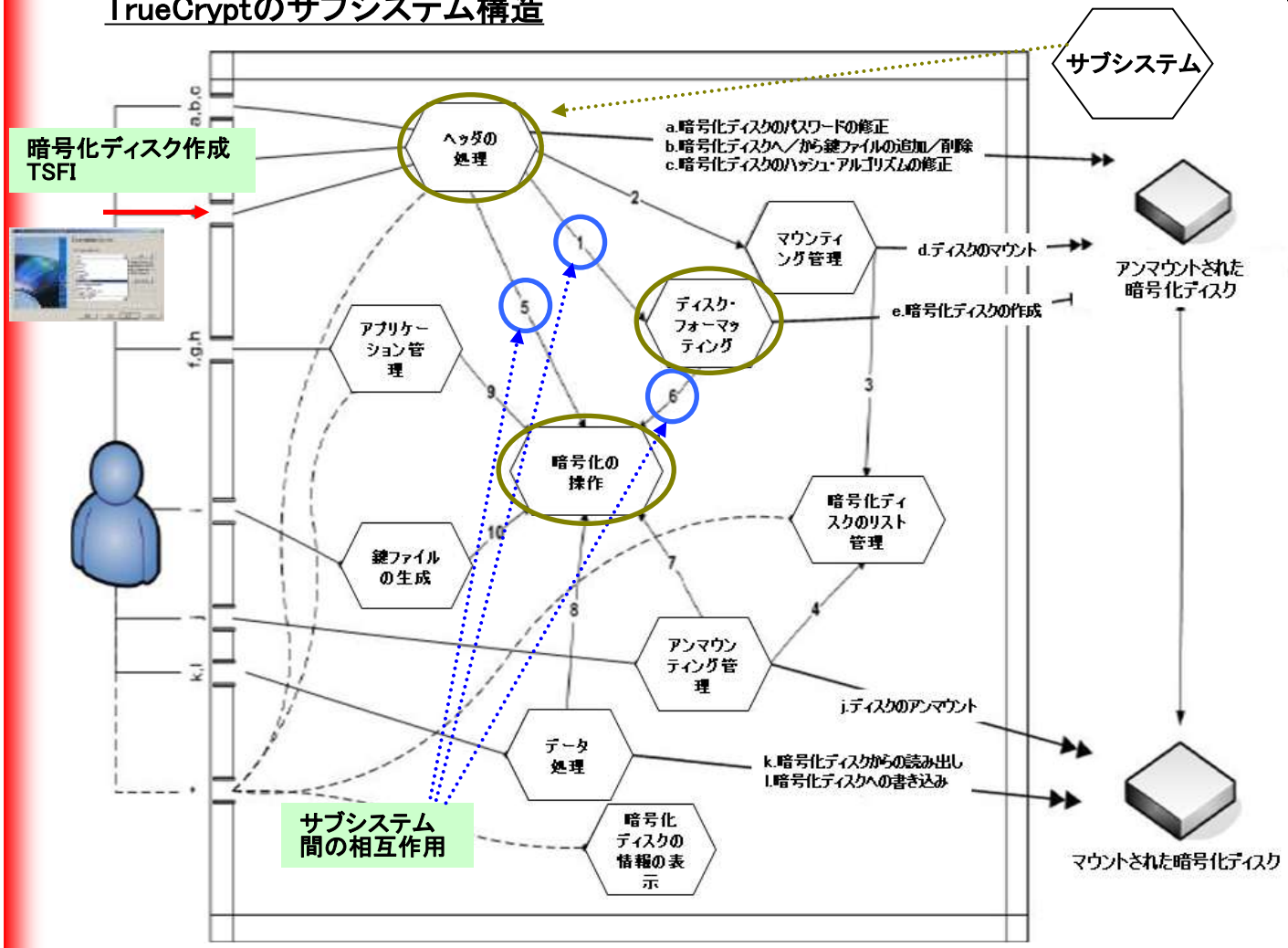
評価者は、SFRと、該当するサブシステム・モジュール仕様との一貫性を評価



オープンソースのTrueCryptの例

TOE設計の例1（全体の構造）

TrueCryptのサブシステム構造



暗号化ディスク作成の流れは以下の通り。

①暗号化ディスクの生成TSFIより「ヘッダの処理」サブシステムが呼び出される

②「ヘッダの処理」サブシステムがマスタ鍵の作成、入力パスワードからのヘッダ鍵の作成、ヘッダの暗号化等を実施する。暗号・復号化、乱数生成を実施する際は、「暗号化の操作」サブシステムを呼び出し処理を依頼する。

③「ヘッダの処理」サブシステムは、最後に「ディスク・フォーマッティング」サブシステムにディスクのフォーマットを依頼する。

④「ディスク・フォーマッティング」サブシステムは「暗号化の操作」サブシステムから得た乱数によりディスクを上書きし、暗号化ディスクの作成が完了する。

TOE設計の例2（サブシステム）

サブシステムの記述（概要説明）

2	ヘッダの処理	SFR 実施
このサブシステムは、ヘッダに関する全ての操作を実施する：暗号化ディスク作成時のディスク・ヘッダの作成、ディスクマウント時のディスク・ヘッダの読み出し、ヘッダのバックアップやリストアである。また、認証手法が変更された場合のヘッダの読み書きも実施する（旧パスワード／鍵ファイル・ペアの読み出し検証し、変更された認証手法に応じた新ヘッダを書き込む）。		

3	ディスク・フォーマッティング	SFR 実施
このサブシステムは、暗号化ディスク作成時に使用される。ヘッダを作成し（ディスクの最初の 512 バイトに）書き込まれると、TrueCrypt は「TrueCrypt Format.exe」実行ファイルにより実施されるディスクのフォーマッティングを開始する。このフォーマッティングは、ファイル・システムごとに異なる（FAT、または NTFS）。		

9	暗号化の操作	SFR 実施
これが、TrueCrypt の主要システムである。このサブシステムは、乱数の生成、暗号化、復号、ハッシュ化操作などの暗号化の機能を提供する。		

開発者はSFR実施や支援サブシステムを分類する必要はない。

ただし、評価者がSFRとの関連度合いを判別できるだけの情報が必要。

サブシステム間の相互作用

1「ヘッダの処理」と「ディスク・フォーマッティング」サブシステム間の相互作用
暗号化ディスクの作成プロセスでは、はじめに「ヘッダの処理」サブシステムによって管理されている暗号化ヘッダの生成が要求される。ヘッダの生成には、暗号化ディスクのデータを暗号化・復号するために使用する暗号鍵が含まれる。このヘッダ自体は、パスワードと鍵ファイル・リストから導出された鍵によって暗号化されている。次にこのヘッダが暗号化ディスクの最初のバイトに書き込まれると、このディスクのその他のセクタは、上記で生成された鍵以外のランダムな鍵で暗号化された、ランダムなデータで満たされる（フォーマッティングは、「TrueCrypt Format.exe」で実行される）。

5「ヘッダの処理」と「暗号化の操作」サブシステム間の相互作用
「ヘッダの処理」サブシステムは、（例えばヘッダの暗号化、乱数の生成などの）処理に必要な暗号化の操作を実行するために「暗号化の操作」サブシステムを使用する。

6「ディスク・フォーマッティング」と「暗号化の操作」サブシステム間の相互作用
ディスクのフォーマッティングは、ランダムな鍵を使用して暗号化された乱数データで満たすことである。これが、「ディスク・フォーマッティング」サブシステムが「暗号化の操作」サブシステムによって提供される機能を使用しなければならない理由である

TOE設計の例３（モジュール）

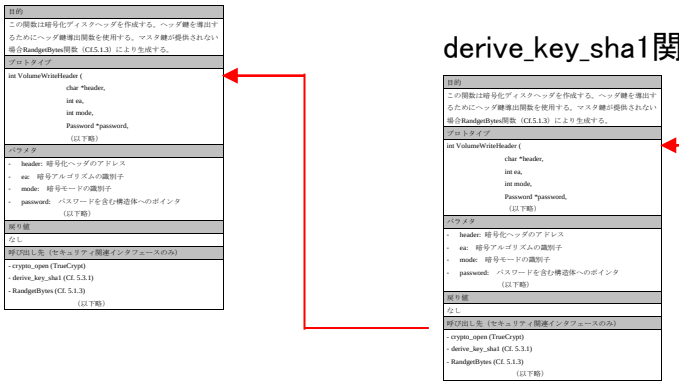
SFR実施モジュールに要求される仕様情報(EAL4)

【目的】
モジュールの機能の説明
【SFR関連インタフェース記述】
SFR関連インタフェースの呼び出し方法と戻り値、パラメタの説明(グローバル変数含む)
【呼び出し関係】
その他のSFR実施モジュールから呼び出されるSFR関連インタフェース

ヘッダ鍵の導出

derive_u_sha1関数

derive_key_sha1関数



単に必要な情報が記載されているだけでなく、モジュール仕様として誤りがないかも評価される（例えばモジュールの目的と、インタフェース記述や呼び出し関係との一貫性等）

SFR実施モジュールに要求される仕様情報(EAL4)の例

暗号化ヘッダの作成

VolumeWriteHeader関数

目的
この関数は暗号化ディスクヘッダを作成する。ヘッダ鍵を導出するためにヘッダ鍵導出関数を使用する。マスタ鍵が提供されない場合RandgetBytes関数（Cf.5.1.3）により生成する。
プロトタイプ
int VolumeWriteHeader (char *header, int ea, int mode, Password *password, （以下略）
パラメタ
- header: 暗号化ヘッダのアドレス - ea: 暗号アルゴリズムの識別子 - mode: 暗号モードの識別子 - password: パスワードを含む構造体へのポインタ （以下略）
戻り値
なし
呼び出し先（セキュリティ関連インタフェースのみ）
- crypto_open (TrueCrypt) - derive_key_sha1 (Cf. 5.3.1) - RandgetBytes (Cf. 5.1.3) （以下略）

「TrueCrypt cryptographic specifications」より抜粋し翻訳(一部改変)

TOE設計の注意事項

- SFRを正確に漏れなく実現すること
- 設計書からSFRの実現内容が読み取れること
- 第三者が理解できるように曖昧なく記述すること
- 各種資料間（設計書内部、ガイダンス、機能仕様等）で一貫していること
  - 例えば、機能の実現内容と相互作用や入出力パラメタ
  - 例えば、モジュールのインタフェース仕様と機能仕様
- CCで要求されている詳細度が必要
  - サブシステム/モジュールの役割（SFR実施/支援/非干渉）が理解できる
  - サブシステム/モジュール間の相互作用（やりとりする目的とデータ、依存関係）が理解できる
  - SFR実施モジュールについては特に詳細な情報が必要（インタフェース仕様、処理内容、グローバルデータの扱い）

実装表現
(ADV_IMP)

実装表現評価の目的と証拠資料

目的

- モジュール仕様どおりに実装されていること

要求される証拠資料

- TSF全体の実装表現（ソースコードや回路図）
- モジュールと実装表現の対応表

モジュール名	対応するファイル名	対応する関数名
Module_A	File_A.c	Func_A1(), Func_A2()
Module_B	File_B.c	Func_B1(), Func_B2(), Func_B3()
Module_C	File_C.c	Func_C1()

実装表現評価の概要

①実装表現が、開発者と同じように参照できるか？

ADV_IMP.1-2 評価者は、実装表現の形式が、開発要員が使用する形式であることをチェックしなければならない。

②実装表現がモジュール仕様の通りに開発されているか？

ADV_IMP.1-3 評価者は、正確であることを決定するために、TOE設計記述と実装表現のサンプルの間のマッピングを検査しなければならない。

開発者はTSF全体のソースコード提示が必要。
評価者は、評価者の判断で、必要なソースコードをサンプリングして確認。
また、実装表現評価に加えて、脆弱性分析にも使用される。

ソースコード生成ツールや、難読化ツールを使用している場合、
ツール適用前の開発者が参照している形式の提供が必要。

評価者が、ソースコードを参照し、コンパイルできるだけの情報提供が必要。
・コンパイルオプション（例えば、ソース中の「#ifdef」など、実際にどの条件が適用されるのかが理解できること。）
・コンパイル自動化ツールのための設定ファイル（Makefileなど）
・ソースコードの表示やコンパイル等に、特殊なツールが必要な場合には、ツールの貸与が必要な場合もある（評価者と整合が必要）

最終的なオブジェクトコードの生成に影響するツール（コンパイラ、ソースコード生成、難読化など）の妥当性は、ツールと技法（ALC_TAT）で評価される。
また、コンパイル自動化手続きは、構成管理（ALC_CMC）で評価される。

セキュリティ
アーキテクチャ
(ADV_ARC)

セキュリティアーキテクチャ評価

目的

- セキュリティ機能が、改ざんやバイパスされないように設計実装されていること

要求される証拠資料

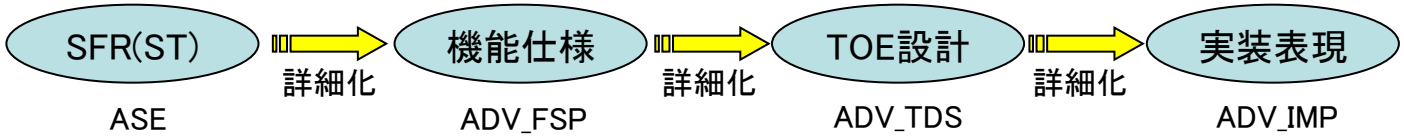
- セキュリティアーキテクチャ記述
  - セキュリティドメインの維持
  - TSF自身の改ざん防止
  - TSFのバイパス防止
  - セキュアな初期化

脆弱性評定に大きく影響⇒脆弱性評定の後で詳細を説明

開発（ADV）評価証拠資料に関する留意点

TOE範囲と開発証拠資料

評価者は、STに記載された全てのセキュリティ機能要件が、正確に漏れなくTOEに実現されることを評価する。



CC評価によって、有意な保証が得られるためには、

TOEの範囲内でSFRを実現していること

SFRの主要な部分をTOEの範囲外で実現している場合、TOEの開発証拠資料を評価しても、SFRを満たしていることの保証が得られない。

開発証拠資料がTSF全体を正しく表現していること

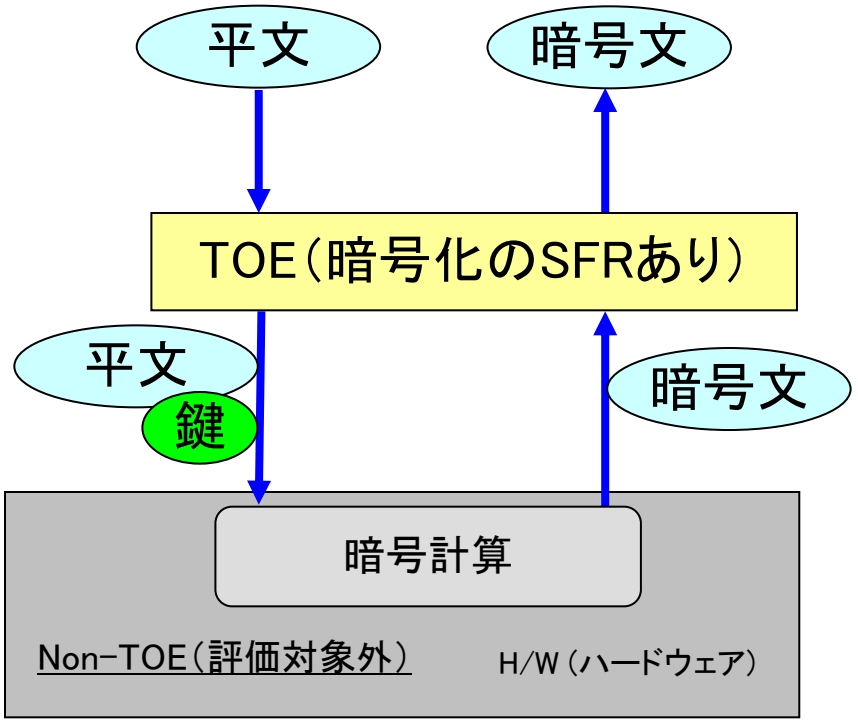
実際の開発で使用された設計書とは別に、CC評価に合格するように新規に資料を作成すると、実際の設計情報が隠ぺいされ、評価の信頼性が損なわれる

適切でないTOE範囲の例

TOEの範囲内に、SFRに記述された暗号アルゴリズムを実現する部分がない。

TOEは単にNon-TOEに処理を依頼し、平文を暗号化する。

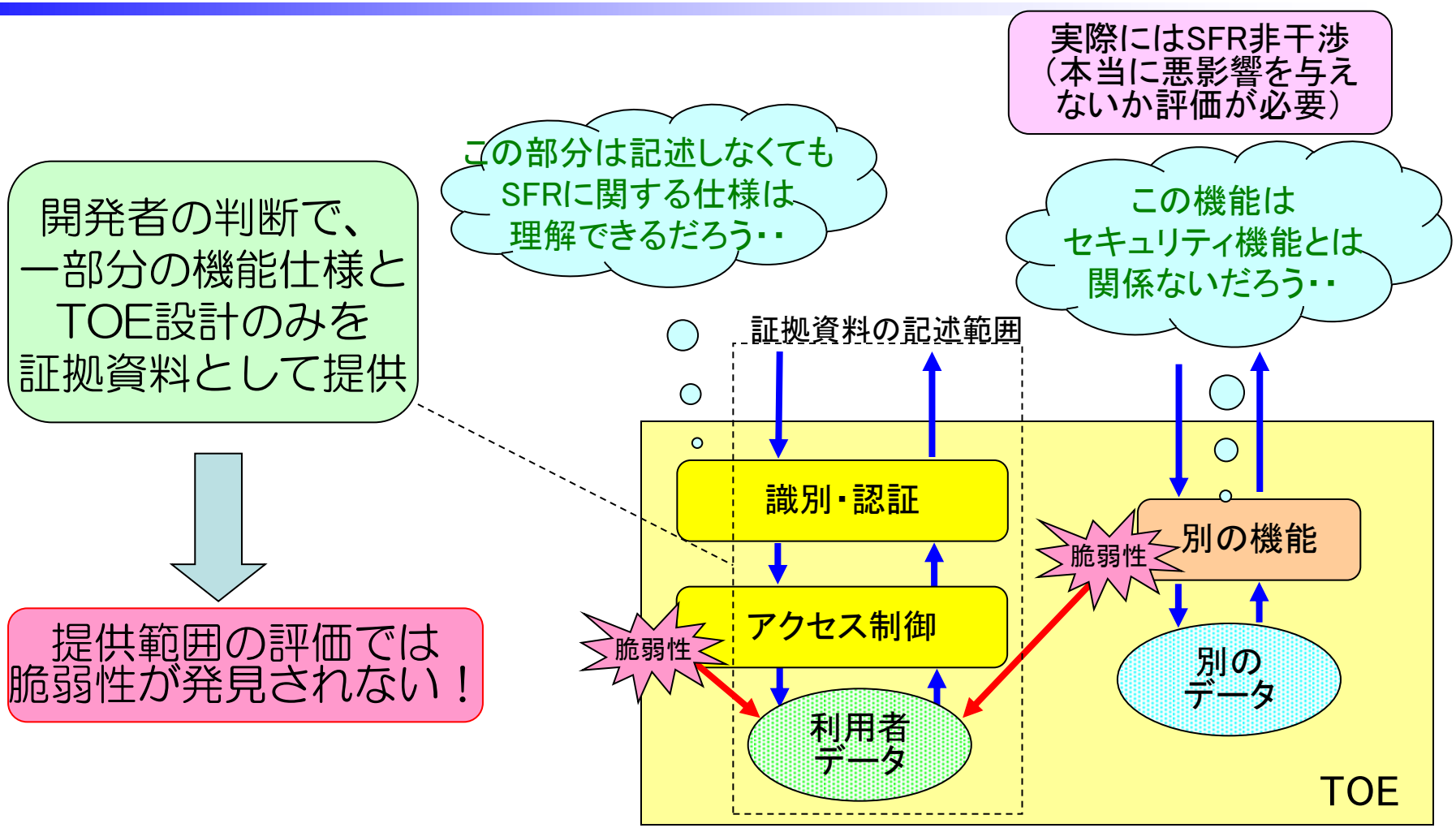
暗号処理自体はNon-TOEにより実施される。



一般的に以下のような回避策が考えられる。
①H/WもTOEに含め、必要な証拠資料を提供する
　（EAL4の場合、H/Wの仕様書や回路図も必要）
②暗号の機能要件をSTより外し、暗号処理を評価対象外にする

ただし、TOEのSFRを実現する程度に依存して、TOEがSFRの実現に責任を持っていると判断できる場合もある⇒早めに評価機関に相談

適切でない開発証拠資料の例



開発者はセキュリティ機能に関連する評価証拠資料を抜粋し提供するのではなく、TSF全体の実際の仕様を証拠資料として提供する必要がある

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

テスト(ATE)

テスト評価の目的と証拠資料

目的

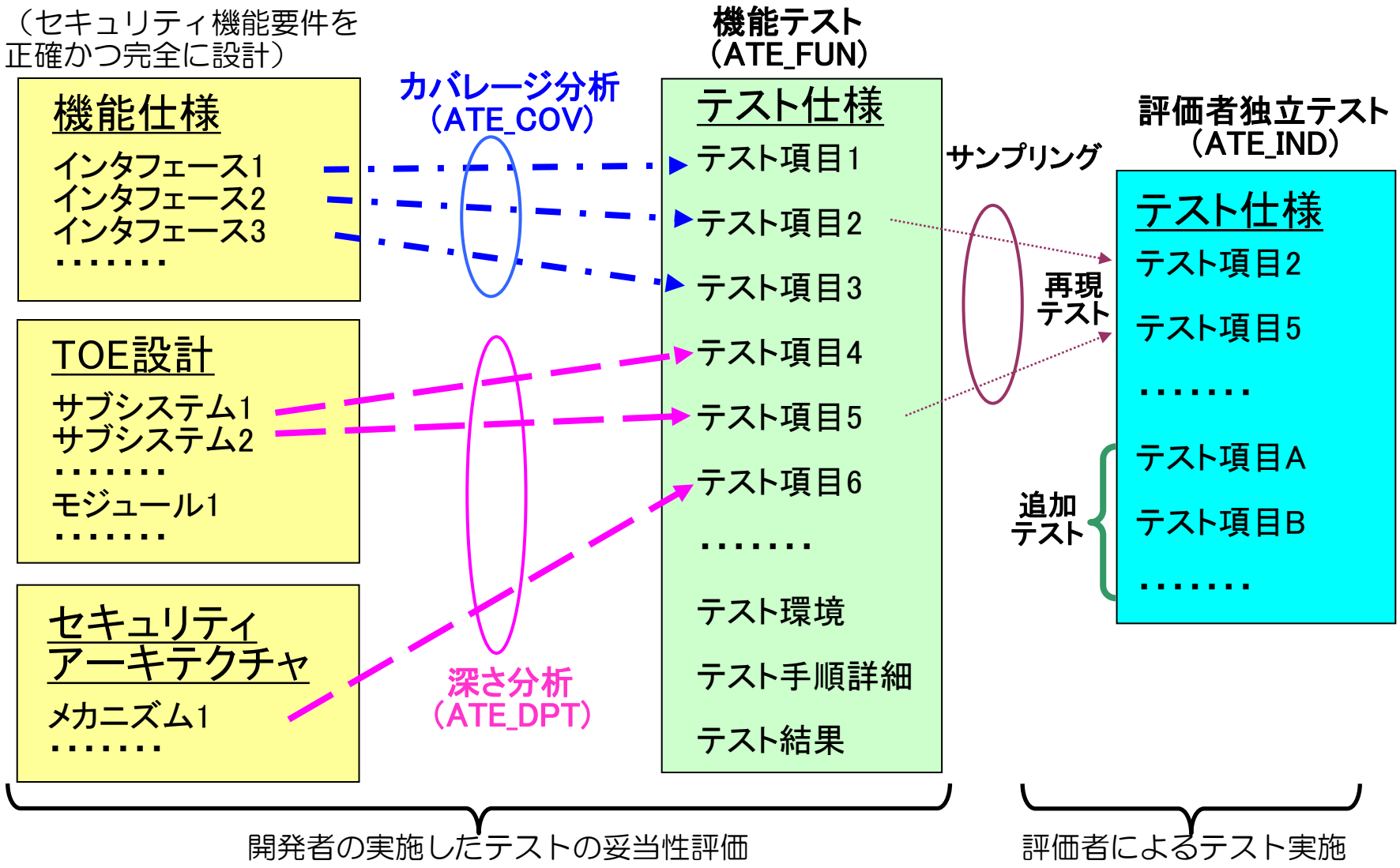
- セキュリティ機能が設計どおりに動作すること

（セキュリティ機能要件とセキュリティアーキテクチャの動作）

要求される証拠資料

- テスト証拠資料
  - テスト計画（テスト手順など）、期待される結果、実際の結果
- テストカバレージ分析、テストの深さ分析
  - テストとセキュリティ機能との対応関係の分析
- TOEとテスト環境
  - 評価者がテストを実施するための環境を貸与する必要がある

テスト評価の概要



機能テスト
(ATE_FUN)

テスト証拠資料の記載事項（1）

テスト計画

- テスト識別（テスト番号など）
- テストの実行シナリオ
  - テスト実施方法の詳細
    - テスト構成、セットアップ手順、クリーンアップ手順
    - テストの入力値、入力の方法、出力の取得方法
  - 再現可能であるように充分に詳細であること

ATE_FUN.1-2

- テストの順序依存性
  - 初期条件のための実行ステップ
  - 依存性の指示（テスト結果を後で使用する場合）

ATE_FUN.1-4

テスト構成は、セキュリティターゲットと一貫していること。
- 運用環境のセキュリティ対策方針の充足
- セキュリティターゲットに記載されたすべての構成の考慮

ATE_FUN.1-3

テスト証拠資料の記載事項（2）

期待されるテスト結果

ATE_FUN.1-5

- 期待される結果を曖昧さがないように記述
  - 第三者(評価者)が結果の一致／不一致を正確に判定できること
  - 例えば、複数のエラーが発生する可能性がある場合、単に「失敗すること」「エラーメッセージが出ること」は不適切。具体的な出力文字列など、どのエラーであるかが間違いなく判別できる記述が必要。

実際のテスト結果

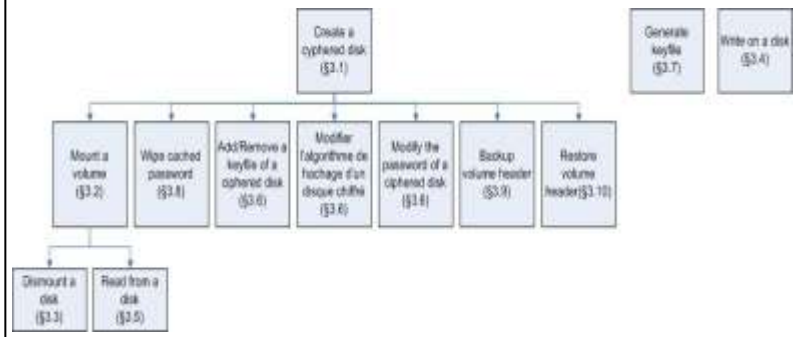
ATE_FUN.1-6

- 実際に得られた結果を記述
- 実際の結果と期待される結果の比較が単純ではない場合その比較方法も記述（バイナリデータのデコードなど）
  - 評価者が実際の結果と期待される結果の一致を確認できること

テスト証拠資料の例

テスト構成

テストプラットフォーム
Windows XP SP2 (32bit)。設定は導入時のまま。なおフリーツールのddコマンド（version 0.4 beta 5）を使用。
ハードウェア設定
ADM 3800+ Athlon 64 X2 デュアルプロセッサ＋1 GB RAM
ソフトウェア構成
TrueCrypt 4.2aを導入済（デフォルト構成）。
テスト順序



TrueCryptのサンプル証拠資料(Eng – AQL – TRUECRYPT – ATE – 2.00.pdf)を一部改変し翻訳抜粋

テスト手順（Tests CREATE_01）

目的
Non-rootユーザがコンテナファイル内に暗号化ディスクを作成できることを検証する。
前提
TrueCrypt ドライバがメモリ内にロードされていること - 設定によりシステムブート時に自動開始されている - ユーザにより TrueCrypt が開始されている
手順（テストシナリオ）
<暗号化ディスク生成ウィザード>の開始 - <TrueCtypt Format.exe>を開始する - <Next>をクリック - <Select File>よりコンテナファイルへのパスを選択 （以下略）
期待されるテスト結果
暗号化ディスクの作成が終了しましたというメッセージの表示
実際のテスト結果
暗号化ディスクの作成が終了しましたというメッセージの表示

一部のテストは、評価者により再度テストされ、テスト資料通りの結果が得られるか確認される。
従って記述内容は、評価者がマニュアルを参照しつつ、独自にテストを再現できるレベルの詳細度が必要。

カバレージ/深さ分析
(ATE_COV・ATE_DPT)

テストカバレージ分析の記載事項

ATE_COV.2-1～4

- テスト証拠資料のテスト識別と機能仕様のインタフェース（TSFI）の対応を記述
- TSFIに対応付けられるセキュリティ機能要件について期待される動作がテストされていること
- すべてのTSFIがテストされていること

機能仕様のTSFI名	該当するテスト名
TSFI_1	テスト#1, テスト#2, テスト#3
TSFI_2	テスト#11
TSFI_3	テスト#12, テスト#13

セキュリティ機能要件に暗号アルゴリズム等が含まれている場合、
指定されたアルゴリズムどおりの実装かどうかのテストも含まれる。
（一般に、既知解テストが実施される。）

テストの深さ分析の記載事項

ATE_DPT.1-1～4

- テスト証拠資料のテスト識別とTOE設計の対応を記述
  - 対象は、サブシステムのふるまいとサブシステム間の相互作用
  - セキュリティアーキテクチャのメカニズムを含む
- サブシステムのふるまいとサブシステム間の相互作用がすべてテストされていること
  - 製品でのテストが困難な場合は、代替のテスト可
    （製品組込み前のモジュールテストなど）

TOE設計のサブシステム		該当するテスト名
Subsystem_X	ふるまいx1	テスト#1, テスト#2
	ふるまいx2	テスト#1, テスト#3, テスト#4
	相互作用a	テスト#5
Subsystem_Y	ふるまいy1	テスト#11
	相互作用b	テスト#12, テスト#13
	…	

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ガイダンス文書(AGD)

ガイダンス文書評価の目的と証拠資料

目的

- TOEのセキュリティ機能の利用方法や注意事項が適切に記述されていること
  - TOEの理解不足や誤使用などによって、セキュリティが保証されない状態に陥ることを防止する

要求される証拠資料

- 利用者操作ガイダンス（操作マニュアル）
  - TOEセキュリティ機能とその操作方法の説明
- 準備手続き（インストールマニュアル）
  - 購入・受領したTOEを導入・設定する手順

評価者は、実際に準備手続きを使用してTOEをインストールし、テスト環境を構築する。

ガイダンス文書の概要

TOEの運用に影響を与える要因

機能仕様（インタフェース仕様）
- 使用方法
- パラメタ
- エラー

セキュリティターゲット
- 運用環境のセキュリティ対策方針（前提条件）

配付証拠資料
- 配付手段に対応した、購入者が実施すべき手続き

TOEをセキュアに運用するための解説
（合理的で誤解されない内容であること）

AGD_OPE.1-7　AGD_OPE1-8

利用者操作ガイダンス
- 機能と操作方法、管理方法
- 障害等のメッセージと対処方法
- 使用上や動作環境の条件

準備手続き
- 受領したTOEの確認（改変の有無、バージョン等）
- 動作環境の条件
- 構築設定の手順と設定条件

ガイダンス文書は、機能仕様やセキュリティターゲット等と一貫していること

利用者操作ガイダンス
(AGD_OPE)

利用者操作ガイダンスの記載事項

- 利用者役割毎に記述（すべての項目） AGD_OPE.1-1 AGD_OPE.1-6
- セキュリティ機能と利用者権限、管理すべき内容と警告（セキュリティ対策方針の充足を含む） AGD_OPE.1-2
- インタフェースのセキュアな使用法 AGD_OPE.1-3
  - インタフェースで認識できるセキュリティ機能の概要、目的、ふるまい、相互関係
  - 起動方法、パラメタ（目的、取りうる値、デフォルト値、セキュアな値）、結果の応答、メッセージ、エラーコード等
  - 効果的な使用方法のアドバイス
- 発生事象とセキュリティ維持のための対処方法 AGD_OPE.1-4
  - 監査ログ満杯、障害、利用者登録の変更や抹消等、の対処方法
- 操作のすべてのモードの記述 AGD_OPE.1-5
  - すべての可能な操作に対する、セキュアな運用手続き
  - 操作には、障害発生時や操作誤り後を含む

準備手続き
(AGD_PRE)

準備手続きの記載事項

- セキュアな受け入れに必要な手続き　AGD_PRE.1-1
  - TOE（ガイダンス含むすべての部分）が正しいバージョンであることの確認
  - 配付手続きに対応して、利用者が実施しなければならない手続き（受領したTOEの改変の確認など）
- セキュアな準備に必要な手続き　AGD_PRE.1-2
  - システム要件
  - セキュリティ対策方針に従った運用環境の要件
  - 構築・設定のステップ（成功・失敗など次ステップを実施するための条件が明確になっていること）
  - 例外や問題発生時の扱い

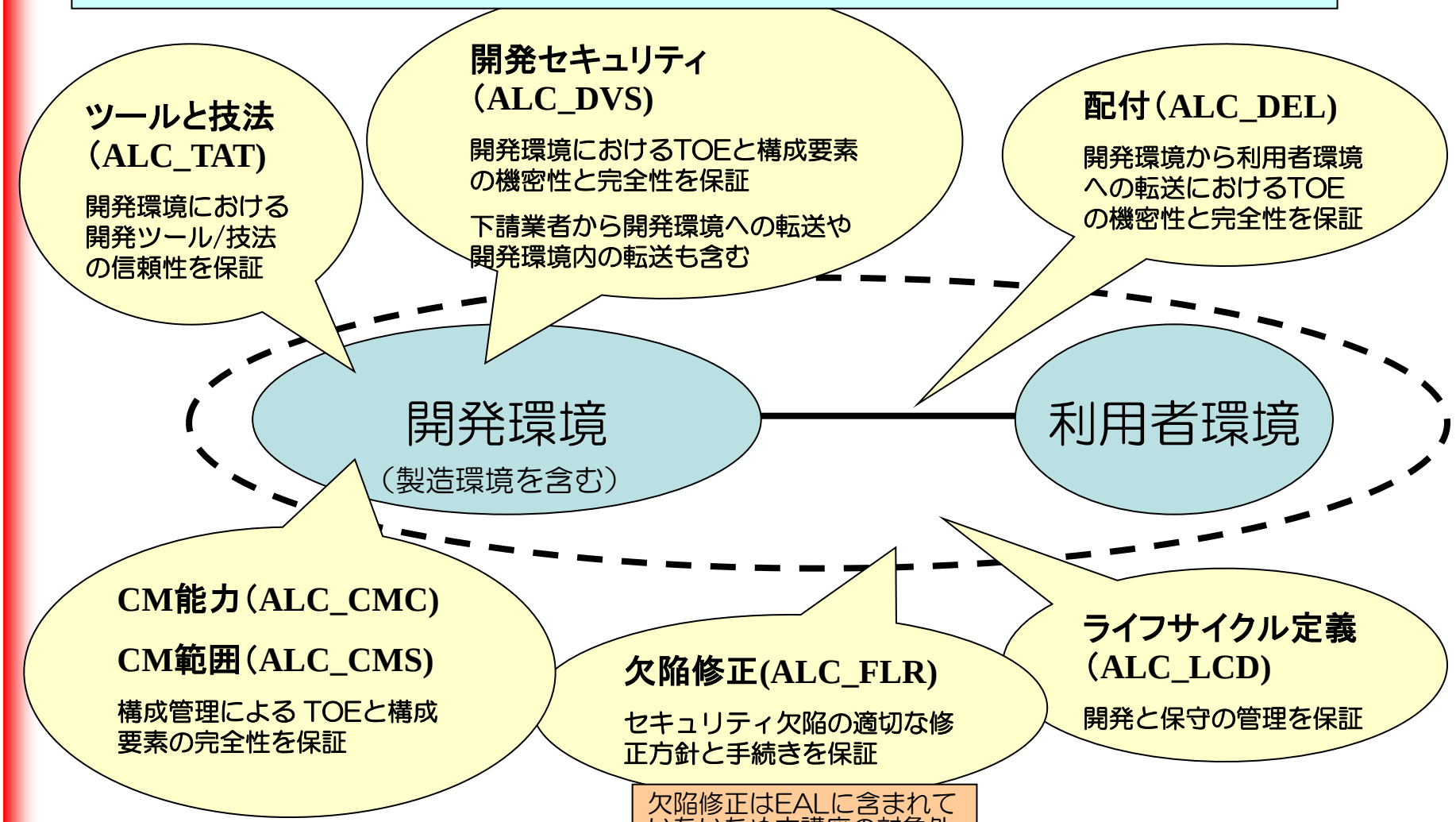
評価者が、ガイダンスの記述だけを使用して、手続きが実行できるように、明確に記述されていること。　AGD_PRE.1-3

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ライフサイクルサポート(ALC)

ライフサイクルサポート評価の目的

開発の各プロセスにおいて、セキュリティ確保に必要な手続きや方法が明文化され、実際に実施されていること



欠陥修正はEALに含まれていないため本講座の対象外

ライフサイクル定義
(ALC_LCD)

ライフサイクル定義評価

目的

- TOEの開発から保守までの手続きが適切に定義され、TOEの品質向上に寄与すること
  - 定義された手続きを使用することは、セキュリティ欠陥が入り込む可能性が小さくなることに貢献する

要求される証拠資料

- ライフサイクル定義評価証拠資料
  - 開発から保守までの工程で使用する手続きや手法

ライフサイクル定義証拠資料の記載事項

- TOEの開発から保守までの工程で使用されるモデル。以下の内容が含まれていること　ALC_LCD.1-1
  - a) TOEの工程やフェーズの定義（境界が理解できること）
  - b) 開発者が使用する手続き、ツール、技法
  - c) 全体的な管理構造(管理や承認の体制、各手続きにおける個人の責任や役割等)
  - d) サブコントラクタ（下請け業者）が開発したTOEの部分と、その受け入れに関する情報

- 上記の手続き、ツール、技法は、（セキュリティ上の）欠陥が入り込む可能性を減じる効果があること

ALC_LCD.1-2

CCでは特定の開発標準を要求していない

CM能力・範囲
(ALC_CMC/CMS)

構成管理評価の目的

目的

- TOEと構成要素（実装表現、各種評価証拠資料等）が、完全性を維持するように管理されていること

✓ TOEや構成要素の一意の識別
  - なんらかの変更がされた場合、識別が変わる

✓ 許可されていない変更の防止

✓ 構成要素の変更やTOE製造の自動化
  - 可能な限り人為的ミスをなくす

✓ 評価者の評価したTOEと、実際の製品が同一

構成管理評価の証拠資料

CM証拠資料（以下の資料の総称）

- 構成リスト
  - TOE開発時に生成された構成要素（ソースコード、各仕様書など）のリスト。リストされた構成要素は構成管理の対象。
- 構成管理計画
  - 構成管理の手続きを規定した社内基準・規定・ガイドライン。
- 構成管理の記録
  - 構成管理計画とおりに手続きが実施されたことを示す証拠。ソースコード変更などの構成管理の際に出力される記録やツールのログ、変更要求指示書、作業報告書など。
- その他
  - 構成要素の一意の識別方法など、構成管理評価で必要な情報。

構成管理評価の方法

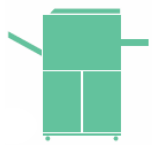
- 証拠資料の確認（適切な管理規則や手続き）
- 証拠資料の確認（管理規則や手続きが適用されたエビデンス）
- 構成要素の現物の確認（名称やバージョンの記載）
- 開発現場の訪問による確認
  - 構成要素の管理状況
  - 構成要素に対するアクセス制御
  - 構成管理ツール

構成管理の対象

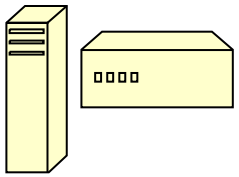
構成管理の対象となるべき構成要素はEALにより異なる。
EAL4の場合は①～⑤の全てが対象となる。

ALC_CMS.4-1

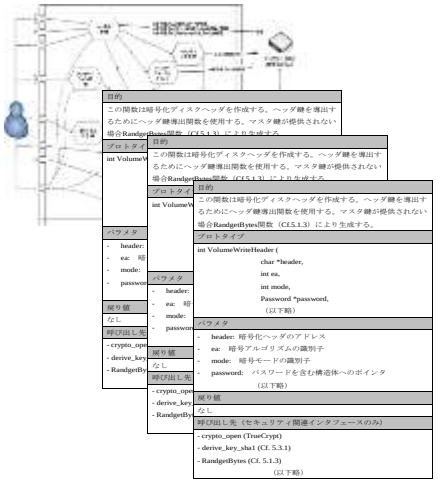
①TOE本体



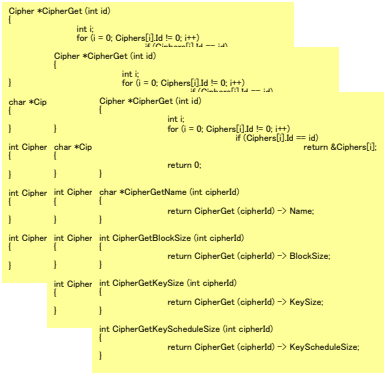
②TOEを構成する各パーツ



③全ての評価証拠資料（モジュール仕様書、テスト手順書、サブシステム仕様書等々）

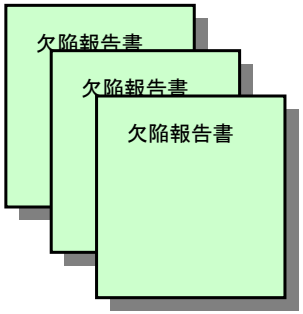


④TOEの実装表現（ソースコード、回路図等）



```
Cipher *CipherGet (int id)
{
        int i;
        for (i = 0; Ciphers[i].Id != 0; i++)
                if (Ciphers[i].Id == id)
                        return &Ciphers[i];
        return 0;
}

int CipherGetName (int cipherId)
{
        return CipherGet (cipherId) -> Name;
}

int CipherGetBlockSize (int cipherId)
{
        return CipherGet (cipherId) -> BlockSize;
}

int CipherGetKeySize (int cipherId)
{
        return CipherGet (cipherId) -> KeySize;
}

int CipherGetKeyScheduleSize (int cipherId)
{
        return CipherGet (cipherId) -> KeyScheduleSize;
}
```

⑤今迄に発生した欠陥に関する記録



各構成要素が正しく識別され、変更管理され、その管理が可能な限り自動化されていなければならない。

TOEの識別情報

TOE名称・バージョン番号の表記

購入者が評価されたTOEを正しく認識できるように、一意の識別情報（TOE名称とバージョン等）を表示しなければならない。

（例）
- コマンドによるバージョン表示
- 起動メッセージによるバージョン表示
- TOE本体への印字やラベル貼付
- 出荷時に同梱する文書(マニュアル等)への記載
- CD-ROMなどの記録媒体への印字やラベル貼付

ALC_CMC.4-1

複数表示がある場合は一貫している必要がある。
セキュリティターゲットと一貫している必要がある。

ALC_CMC.4-2

購入者は、TOE名称とバージョンが、すべて一致していることにより、認証済製品の正しい組合せであることを確認できる。
- セキュリティターゲットの記載
- 購入製品の表示
- マニュアルの記載

CM証拠資料の記載事項（１）

構成リスト

- TOEの構成要素の正しいバージョンのリスト
- 構成要素の一意の識別と開発者名を含む

IPAソフトウェア開発文書リスト V1.1 2011年3月1日

ALC_CMS.4-2　ALC_CMS.4-3

構成要素名	バージョン番号	作成日	開発者
IPAソフトウェアST	1.08	2011.3.1	開発部A
IPAソフトウェア機能仕様書	1.0	2010.6.20	開発部A
IPAソフトウェア詳細設計書	1.0	2010.8.10	開発部A
IPAソフトウェア利用者マニュアル	1.2	2010.12.10	ドキュメント部門B
IPAソフトウェア管理者マニュアル	1.2	2010.12.10	ドキュメント部門B
IPAソフトウェアインストール手順書	1.01	2010.11.20	開発部A
…			

※ソースコードをはじめ、ALC_CMS.4-1で規定された構成要素をすべて含むこと

ソースコードや開発証拠資料等のバージョン管理がされ、変更がトラッキングできるようにする必要がある
（CVSやSubversion等の構成管理ソフトで構成要素を管理しておけば問題はない）

CM証拠資料の記載事項（2）

構成要素の一意の識別方法

ALC_CMC.4-2

- 構成要素を一意に識別する命名規則
- 一意の識別を構成要素に付与する方法
- 一意の識別を構成管理に登録する方法
- 変更された構成要素を識別する方法

各構成要素のそれぞれには、実際に、一意の識別方法に従って、識別情報（名称、バージョン等）が付けられていることが必要。

ALC_CMC.4-1

ALC_CMC.4-4

CM証拠資料の記載事項（3）

構成管理計画

ALC_CMC.4-8　ALC_CMC.4-9　ALC_CMC.4-10

- 構成管理対象の開発作業（ソースへの変更等）
- 構成管理の手段、使用ツールと利用法（CVS等）
- 各構成要素の管理体制と個人の役割
- 構成要素への変更管理
- 構成要素のアクセス制御や同時更新管理
- 手続きの適用結果、生成される記録（承認記録、ログ等）
- 構成要素の受入れ手続き（他社の製造物、開発フェーズ遷移、開発サイト間の転送後）

開発者は、構成管理及び構成要素受入れの手続き・方法・手順を定めた文書を作成し、それに従って開発を行わなければならない。

構成管理計画の記述例

- 構成要素の変更管理

プロジェクトリーダ（PL）は、変更の要求があった場合、両GLを含めたレビューチームを召集し、その変更要求のレビューを行い、承認または却下の判断を行う。レビューでは、変更の理由、重要性、及び変更に伴う影響範囲・概算工数について検証する。なお、これらの検証結果はレビュー日時とレビュー番号を付して変更要求記録簿に残す。

変更要求が承認された場合、各GLは、担当者に変更作業に必要な情報を連絡する。

担当者は、・・・（略）・・・

構成管理計画として、まったく新しい文書を作成する必要はない。
開発プロセスに関して規定されている各種社内基準・規定・ガイドラインなどの複数のドキュメントが、全体として構成管理の要件を満足していればよい。

CM証拠資料の記載事項（4）

構成管理計画（自動化手段）

ALC_CMC.4-5

- 構成要素の許可されない変更の自動化された防止手段

（例）
- OSのログイン機能及びアクセス制御機能
- 構成管理ツールのログイン機能及びアクセス制御機能

ALC_CMC.4-6

- TOE製造の自動化された手段

（例）
- “make” ツールと構成管理下にある “Makefile”
- ROM書き込み装置と構成管理下にある書き込みパラメータ

開発者は、不注意などによる人為的なミスを軽減するために、自動化ツールを使用しなければならない。

CM証拠資料の記載事項（5）

構成管理の記録（エビデンス）

ALC_CMC.4-12

- 構成管理計画に従って手続きを実施した際に生成される記録
  - ツールのログ、操作の履歴、変更管理の記録など
- すべての構成要素が構成管理計画の手続きに従って運用されていることを示す情報が必要

構成管理証拠資料のとおりに構成管理が実施されているかどうか、上記のエビデンスの確認に加えて、開発者へのインタビュー、構成管理の実演、実際のツールの使用や操作履歴の有無によって確認される。

ALC_CMC.4-13

ツールと技法
(ALC_TAT)

ツールと技法評価の目的と証拠資料

目的

- 開発ツールが明確に定義されていること
  （コンパイラやCADシステムが予測可能な結果をもたらすこと）

要求される証拠資料

EAL４では実装表現を評価するため、実装表現の文法・構文の定義が要求される

- 開発ツール証拠資料
  - プログラミング言語仕様書など
  - コンパイラ等の利用者マニュアル
  - 開発時に使用した開発ツールのオプション指定

開発ツール証拠資料の記載事項

- 実装表現の文法・構文の定義

ALC_TAT.1-1
ALC_TAT.1-2

  - すべてのステートメント、規則、指示文を曖昧なく定義する
  - プログラミング言語等の場合、準拠する標準（ISO標準等）や標準との差異を示せばよい
  - 処理系依存の構文は要注意（意図と異なる動作の可能性）
    （例えば、C言語のchar型の符号、各種型のサイズ、アラインメント等）

ALC_TAT.1-3

- 開発ツールの使用方法
  - 出力コードに影響を与えるオプションの定義と使用法
  - 例えば、オプションによる開発ツールの動作の違いや、コンパイルやリンクのオプション指定の意味など

ALC_TAT.1-3

- 開発時に使用したオプション指定

評価者は、実装表現の検査時に、開発ツールに起因する脆弱性が存在しないかどうか評価する。例えば、コンパイラの最適化オプションによっては、必要部分のコードが省略されてしまう可能性がある。

開発セキュリティ
(ALC_DVS)

開発セキュリティ評価の目的と証拠資料

目的

開発には、製造を含む

- 開発環境において、TOE設計と実装の機密性と完全性が保護されるように管理されていること

要求される証拠資料

- 開発セキュリティ証拠資料
  - 開発の機密性と完全性の方針
  - 方針の達成に必要なすべてのセキュリティ手段
  - セキュリティ手段が適用された証拠

ALC_DVS.1-3

証拠資料の検査に加えて、実際の開発環境の訪問検査が実施される

開発セキュリティ証拠資料の記載事項

- 開発の機密性と完全性の方針　ALC_DVS.1-2
  - TOEの機密情報を含む対象物、アクセス可能者
  - TOEの完全性維持に必要な対象物、変更可能者　ALC_DVS.1-1
- 方針を達成するために必要なセキュリティ対策
  - 物理的手段（建物やマシン室の保安・施錠等）
  - 手続的手段（入退出管理、アクセス承認と取り消し、情報の持出しや転送時の承認と保護対策、管理体制等）
  - 人的手段（規則、従業員教育、守秘義務等）
  - その他手段（マシンやネットワークのアクセス制御等）

開発サイト毎に記述が必要。以下の情報も含む。
- 開発サイトの場所
- 開発サイトで実施される開発の局面（設計、テスト、製造、出荷等）
- 開発サイト間でやりとりされる対象物や情報

TOEや開発サイトによっては、機密性を必要としない場合もある。

配付
(ALC_DEL)

配付評価の目的と証拠資料

目的

- TOE配付中にセキュリティが維持されること

（TOE出荷後、購入者に渡されるまでの間）

購入者が受け取ったTOEが、開発者の作成したTOEと同一であること。
TOEの秘密情報が漏えいしないこと。（TOEに秘密情報が存在する場合）

要求される証拠資料

- 配付証拠資料
  - 配付中のセキュリティ維持に必要な手続き

評価者は、以下の評価を行う。
- 証拠資料に必要な手続きが記述されていること
- 配付の現場において、必要な手続きが実際に使用されていること（サイト訪問などで確認）

ALC_DEL.1-2

配付証拠資料の記載事項

ALC_DEL.1-1

- 配付対象
  - TOE全体（ガイダンスを含む）
- 配付の工程と手段

開発サイト間の転送は、開発セキュリティ（ALC_DVS）で評価

  - 製造環境から設置環境までの全フェーズ（パッケージング、保管、配送）
  - 配送手段（運送、手渡し、電子的ダウンロード）
- セキュリティに必要な手続き
  - セキュリティ要件（機密性、完全性）はTOEに依存
  - セキュリティ要件に対して必要な手続き
    - 作業ミス（誤バージョンの混入等）防止、なりすまし防止、TOEの改ざん防止、TOEの改ざん検出、TOEの漏えい防止など
    - 具体例：配送／受領確認、開封検出可能なセキュリティシール、電子署名や暗号化

購入者が実施すべき手続き（電子署名の確認など）は、準備手続き（AGD_PRE）で評価

ライフサイクルサポート（ALC）の留意点

サイト訪問による検査

- ALC評価は、開発や製造現場のサイト訪問による検査を伴う
- サイト訪問の対象は、TOEに応じて決定され、別会社かどうかや場所には関係しない
  - 例えば、以下が含まれる
    - 別会社に委託しているパッケージング（出荷）工場
    - 海外の製造工場
    - TOEの構成要素を保管しているデータセンター
- CC評価認証を申請する場合、とりまとめ者は関連部門の調整が必要

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

脆弱性評定とセキュリティアーキテクチャ

脆弱性評定の目的

目的

- TOEの運用環境において、TOEに、想定される攻撃能力で悪用可能な脆弱性がないことを評価する。

＝ CC評価の最終目的

※想定される攻撃能力はEALで異なる。
攻撃能力の詳細は、後で説明。

脆弱性評定の目的

開発者に求められること

- 想定される攻撃能力の攻撃に耐えられるように、TOEを設計・実装すること。

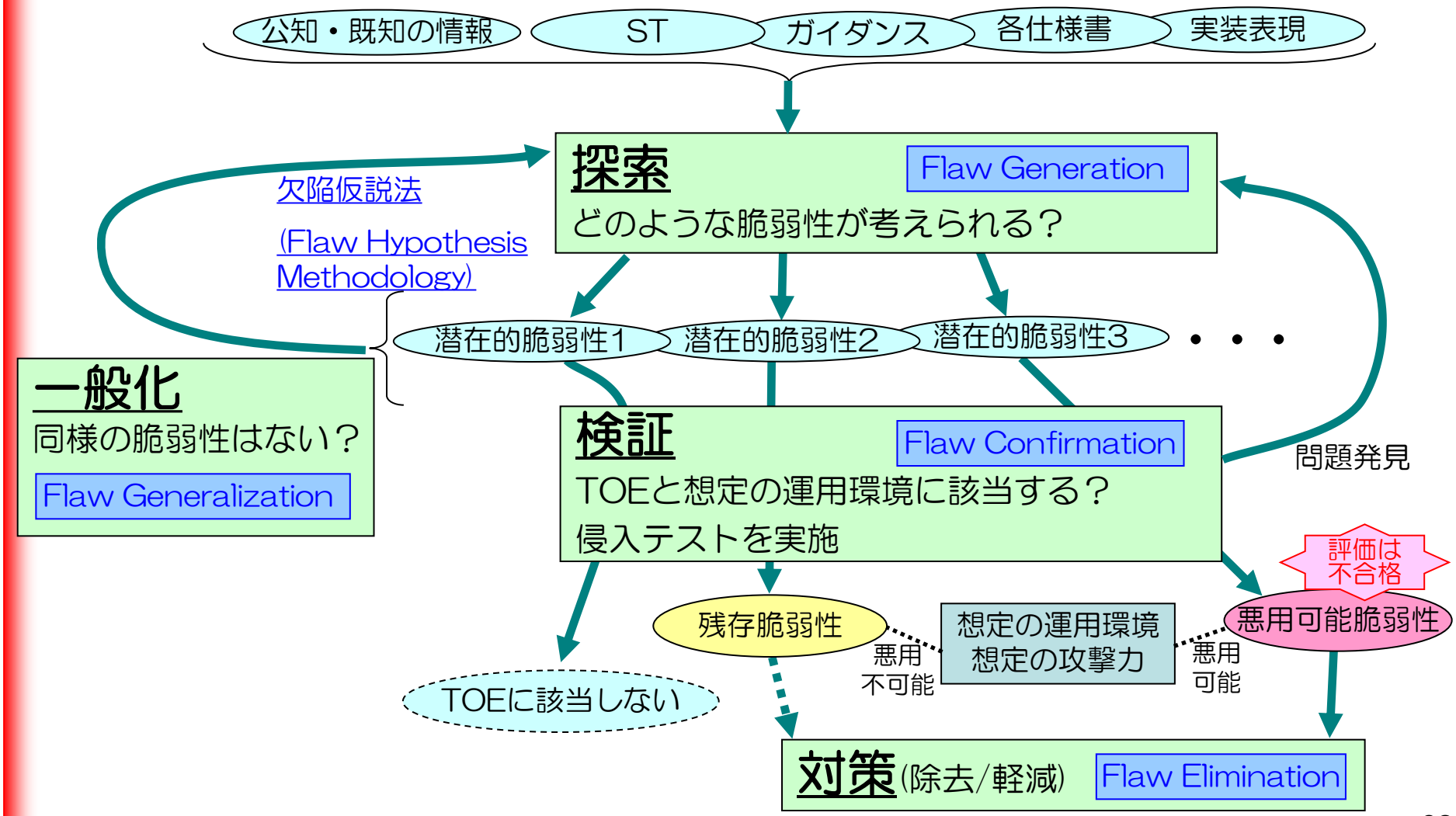
「セキュリティアーキテクチャ」を意識して
設計・実装することで、
脆弱性を作りこまないように！

- 想定される攻撃能力で悪用可能の場合、何らかの対策が必要。（そのままでは評価は不合格）

脆弱性評定の概要

評価者は脆弱性分析と侵入テストを実施

開発者は、悪用可能脆弱性がないように
TOEを設計・実装する



悪用可能な脆弱性の判定基準

攻撃能力

脆弱性を悪用するためにはどの程度の攻撃能力が必要かの判断に、

可能な範囲で客観的な基準を適用することにより、

TOEが想定する環境で必要な対抗能力を持つことの根拠を与える。

攻撃能力の計算方法

◆各要因ごとに、以下の表を目安に攻撃能力を定量分析する。

所要時間

条件	評定値
～1日	0
～1週間	1
～2週間	2
～1ヶ月	4
～2ヶ月	7
～3ヶ月	10
～4ヶ月	13
～5ヶ月	15
～6ヶ月	17
6ヶ月～	19

専門知識

条件	評定値
しろうと	0
熟練者	3
エキスパート	6
複数の エキスパート	8

機会

条件	評定値
不必要/無制限	0
容易	1
中	4
困難	10
なし	∞

TOEの知識

条件	評定値
公開	0
限定的	3
機密	7
危機的	11

機器

条件	評定値
標準	0
特殊	4
特別注文	7
複数の特別注文	9

合計

攻撃能力

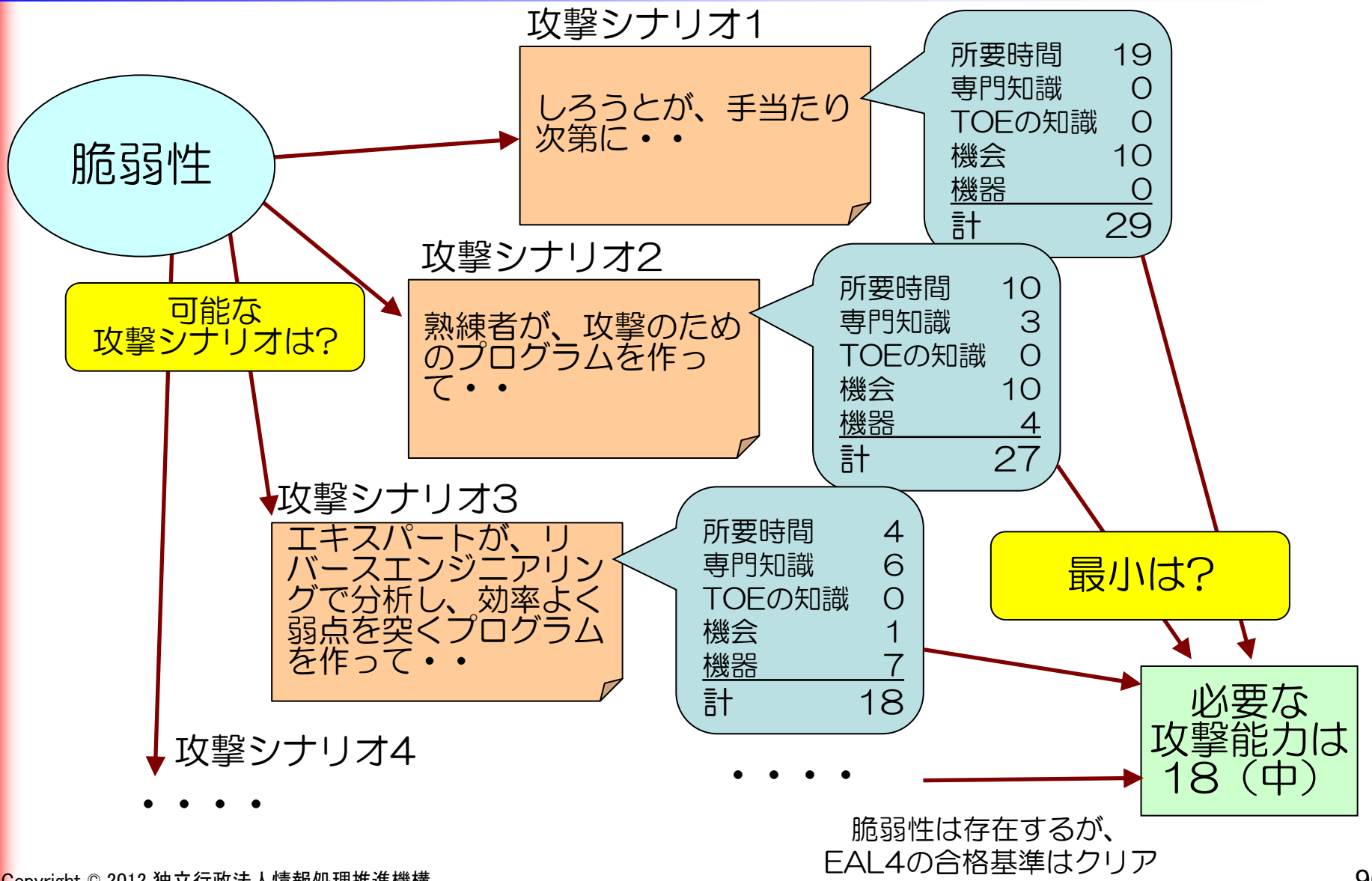
- 25～ 高より上
- 20～24 高
- 14～19 中
- 10～13 強化基本
- 0～9 基本

脆弱性が存在してもEAL4では合格

EAL4で対抗必要

CEM 附属書 B.4.2.3

攻撃能力の計算例

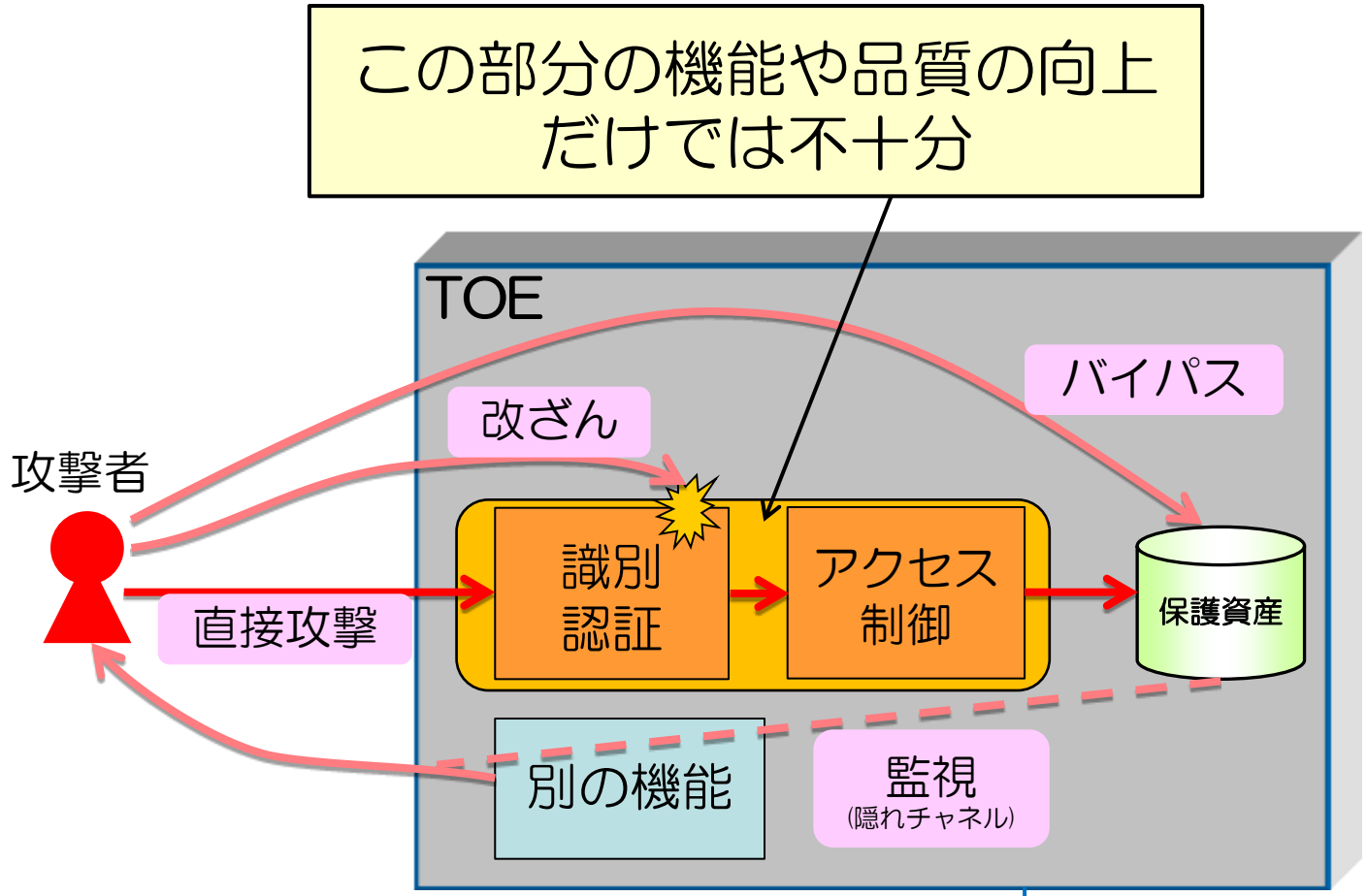


脆弱性の一般的カテゴリ

- バイパス
  - セキュリティ機能の実施を回避
- 改ざん
  - セキュリティ機能の動作を変更（破壊、妨害など）
- 直接攻撃
  - パスワード、暗号鍵、セッション情報などの推測や総当たり
    (正しく実装しても、CCでは「脆弱性は存在する」ことになる)
- 監視
  - 盗聴、隠れチャネル（電気信号や応答時間等の分析）
- 誤使用
  - セキュリティ機能に関する表示やガイダンスの記述が不適切

CEM 附属書 B.2.1

脆弱性とセキュリティアーキテクチャ



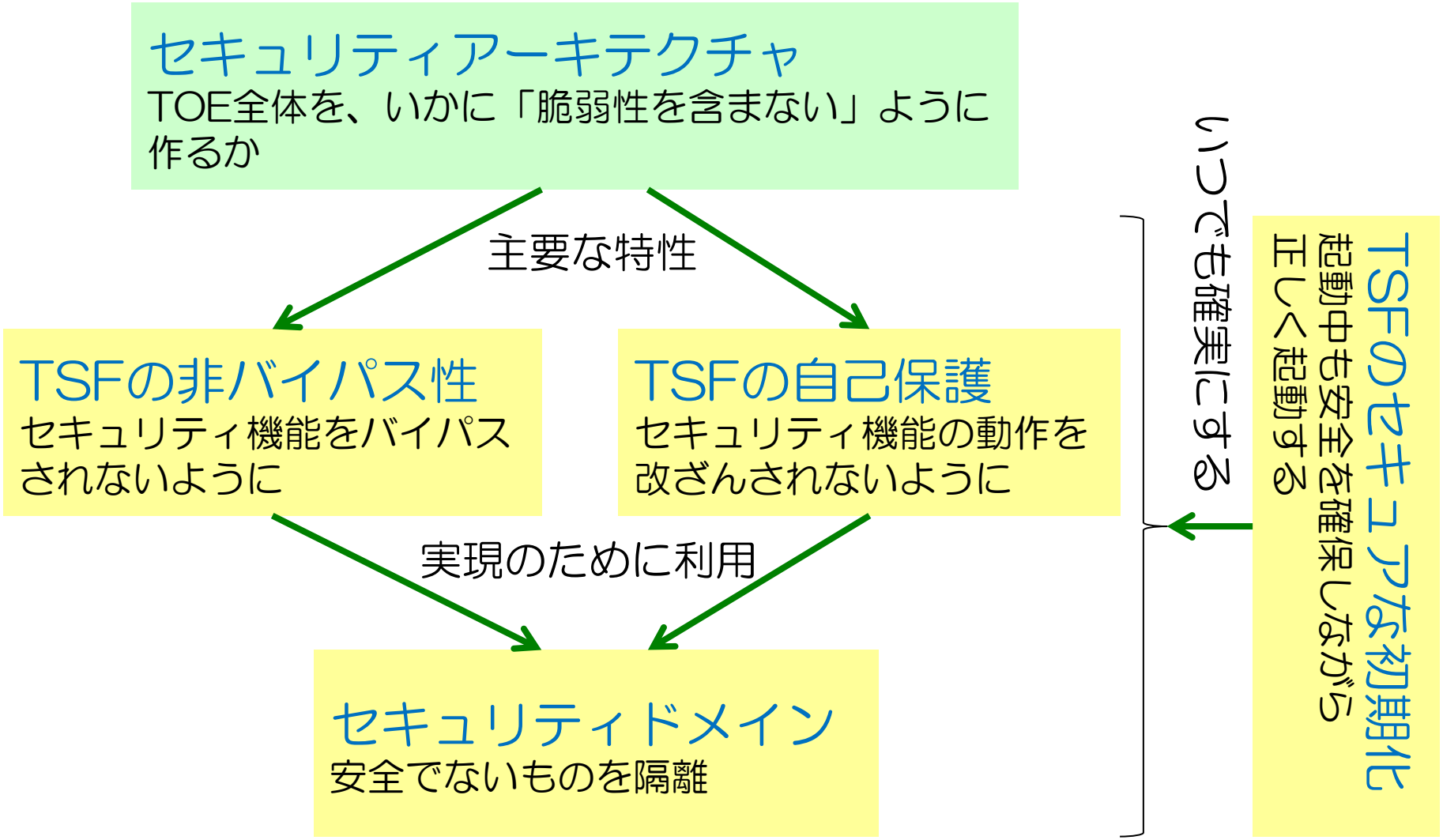
TOE全体を、攻撃に強い作りに = セキュリティアーキテクチャ

セキュリティアーキテクチャとは

開発者にとっては、セキュリティアーキテクチャの適切な設計と実装が特に重要。

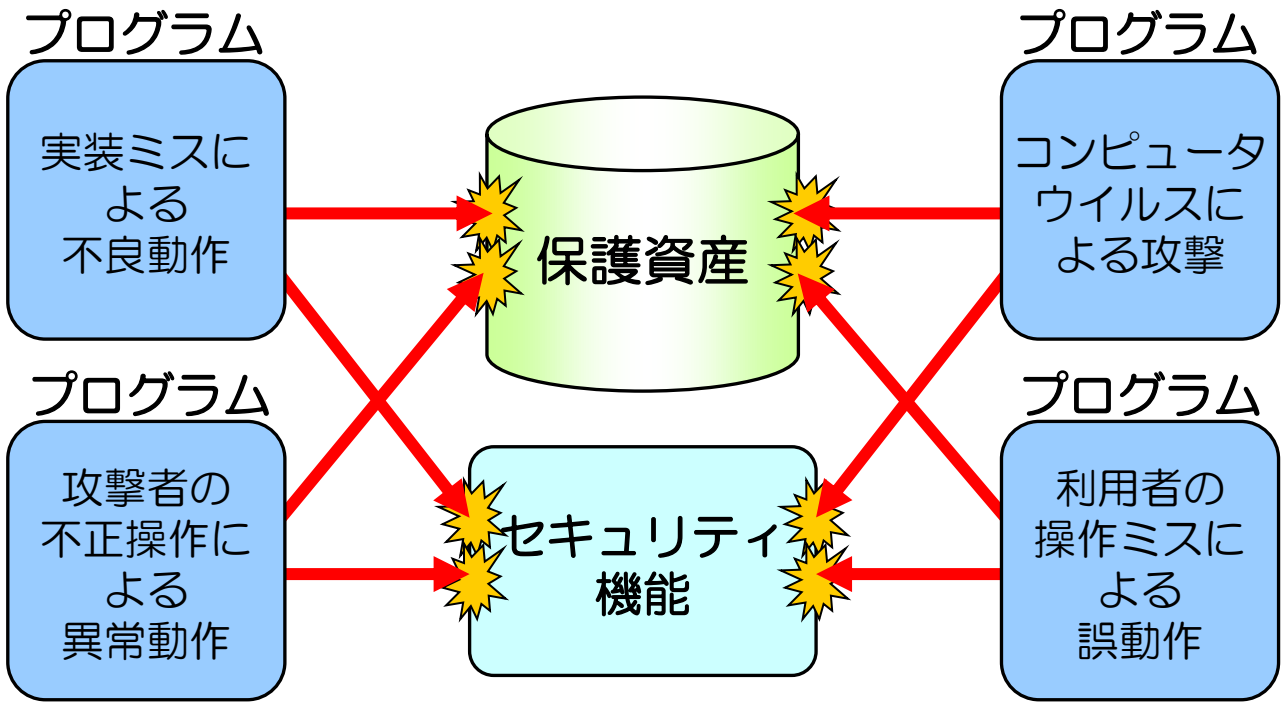
ADV_ARC.1.1D	開発者は、TSFのセキュリティ特性がバイパスされないようにTOEを設計及び実装しなければならない。
ADV_ARC.1.2D	開発者は、TSFが信頼できない能動的なエンティティによって改ざんされるのを防ぐことができるようにTSFを設計及び実装しなければならない。
ADV_ARC.1.3D	開発者は、TSFのセキュリティアーキテクチャ記述を提供しなければならない。

セキュリティアーキテクチャとは



セキュリティドメインとは

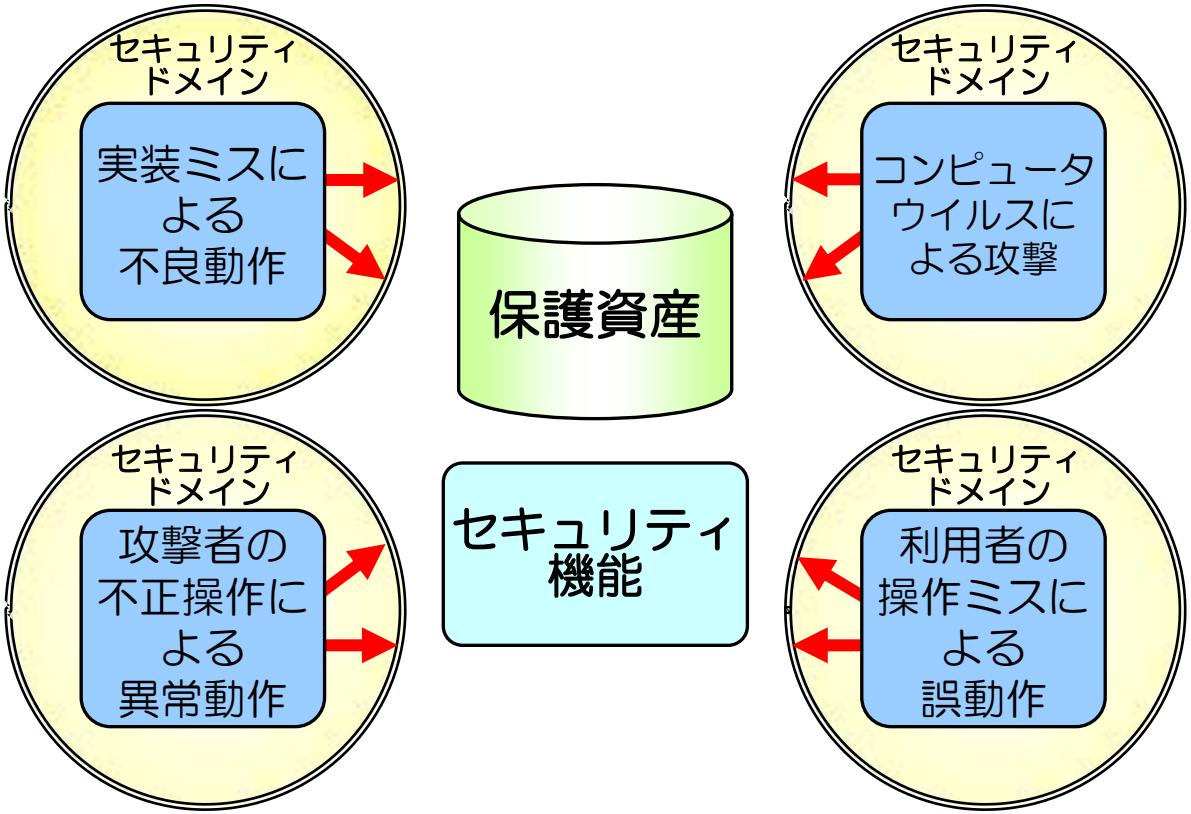
セキュリティ機能の周囲からのセキュリティの侵害には様々な要因がある。



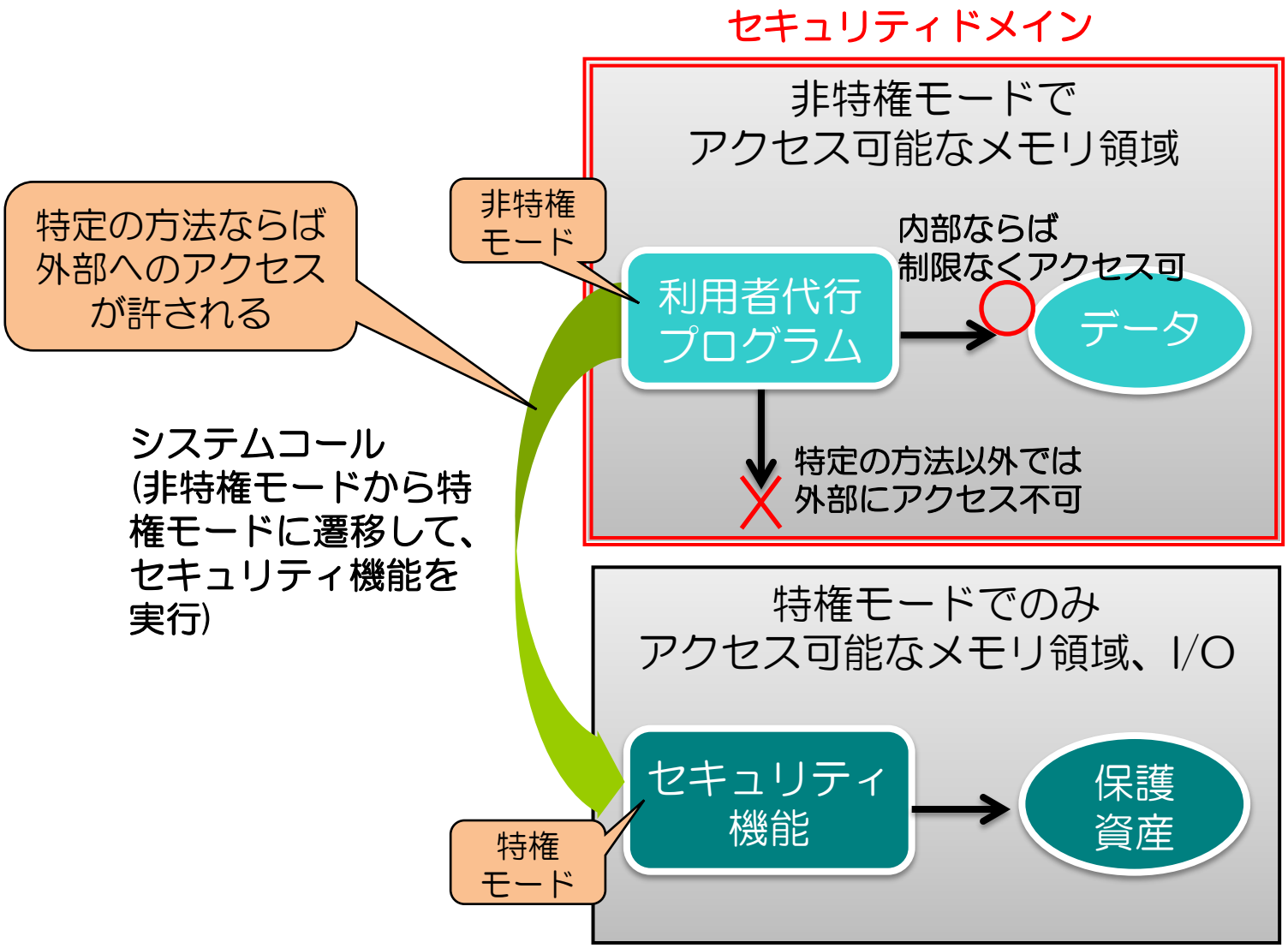
開発段階ですべてを予期することは難しい。

セキュリティドメインとは

信頼できない部分を、
余計な権限を与えずに閉じ込めて、
重要な部分に不正に影響しないように。



セキュリティドメインとは

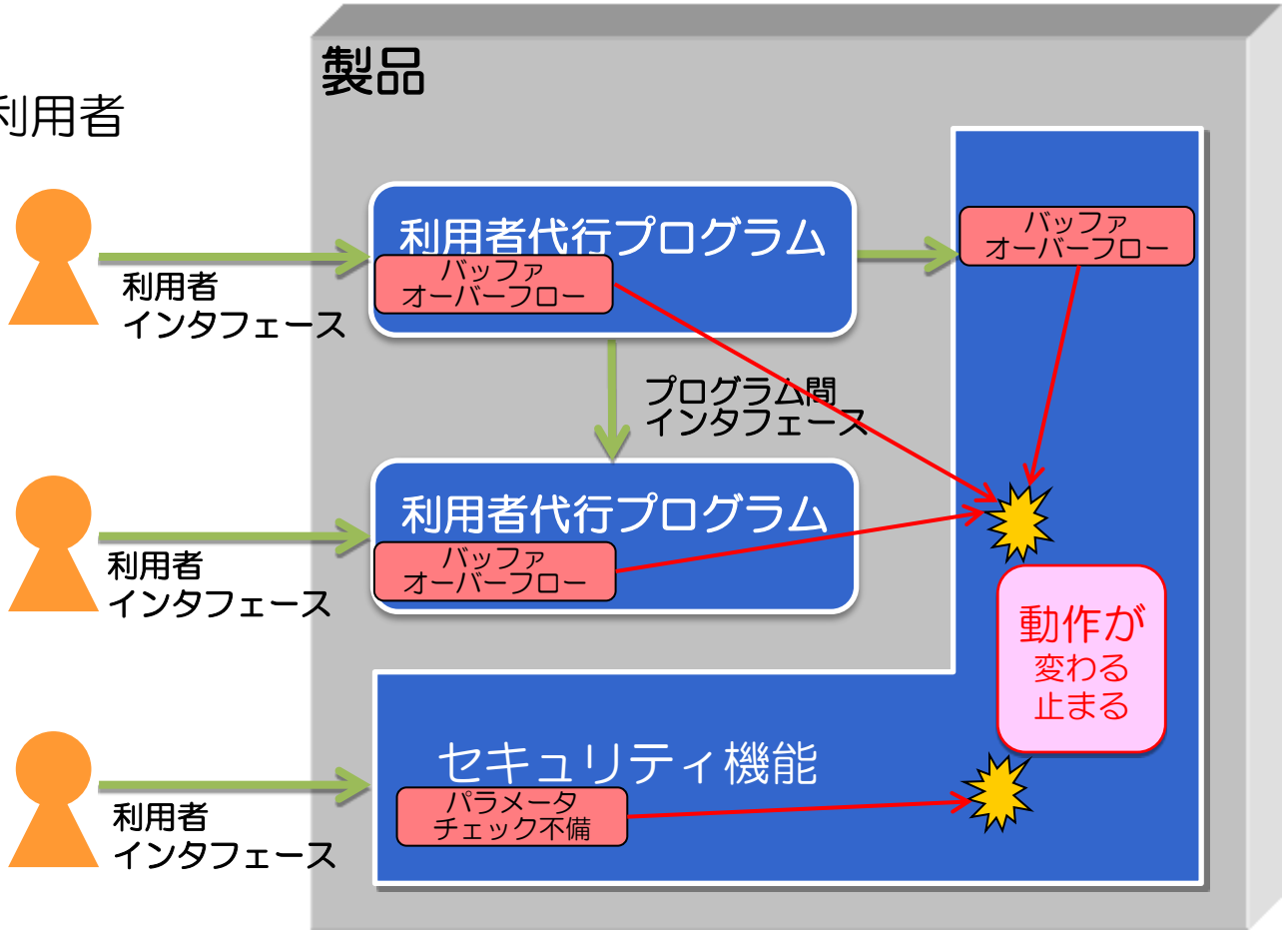


セキュリティドメインの記載事項

- セキュリティドメインの定義
  - 内部で何が動作するのか
  - 内部で自由に使える資源は何か
- ドメイン分離のメカニズム
  - 内部から外部への不正な干渉を防ぐためのメカニズム
    (TOEとTOE外の分担を明確に)
- セキュリティドメインが不要である根拠
  (セキュリティドメインがない場合、
  または不十分な場合)
  - セキュリティドメインがなくても、セキュリティ機能が正しく動作できる理由

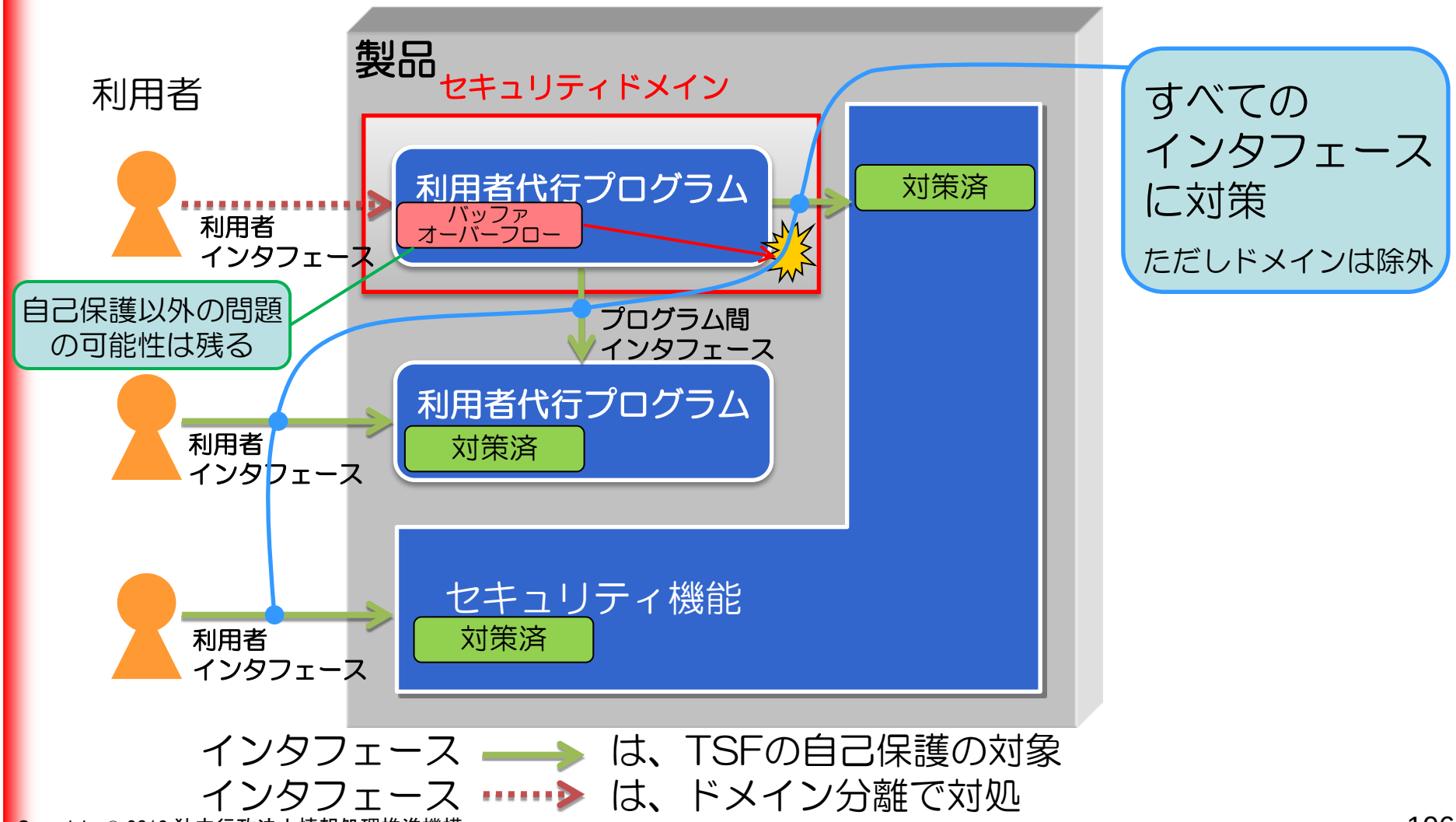
TSFの自己保護とは

自己保護が不十分な状態



TSFの自己保護とは

自己保護が十分な状態



TSFの自己保護の実現

想定外の動作となる要因を消していく。例えば・・

入力の長さチェック / 入力の一定長以降切り捨て / 動的なメモリ確保
(バッファオーバーフロー対策)

無害化(サニタイズ) / バインド機構
(SQL等のインジェクション対策)

パラメータの値、入力の形式のチェック
(想定外の入力対策)

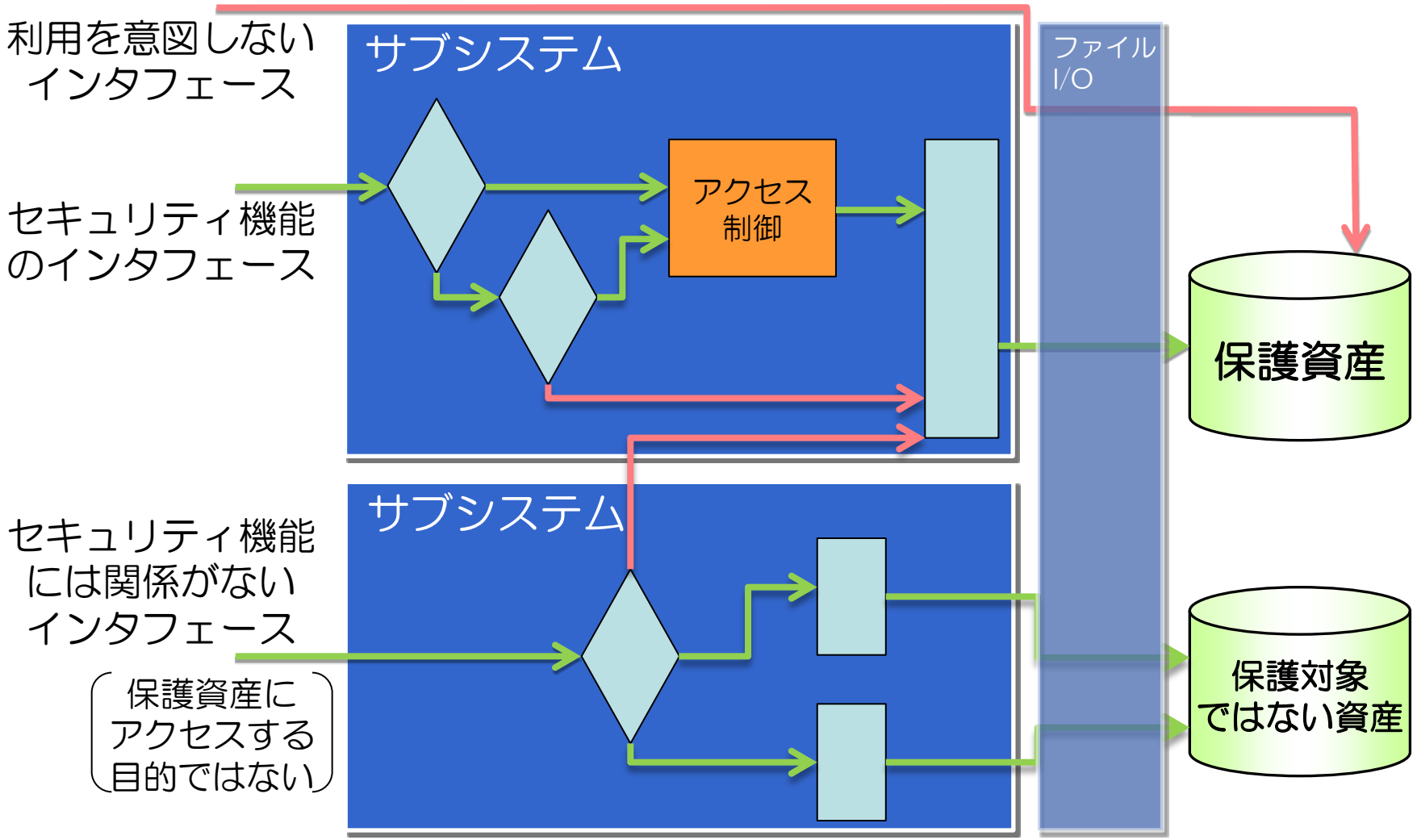
TSFの自己保護の記載事項

- ドメイン分離による自己保護
  - TOE自身のメカニズムの説明
  - TOE外のメカニズムをTOEがどのように利用するかを説明

- ドメイン分離以外による自己保護
  - セキュリティドメインの外部にあるすべてのインタフェースに対して、セキュリティ機能を保護するメカニズムを説明

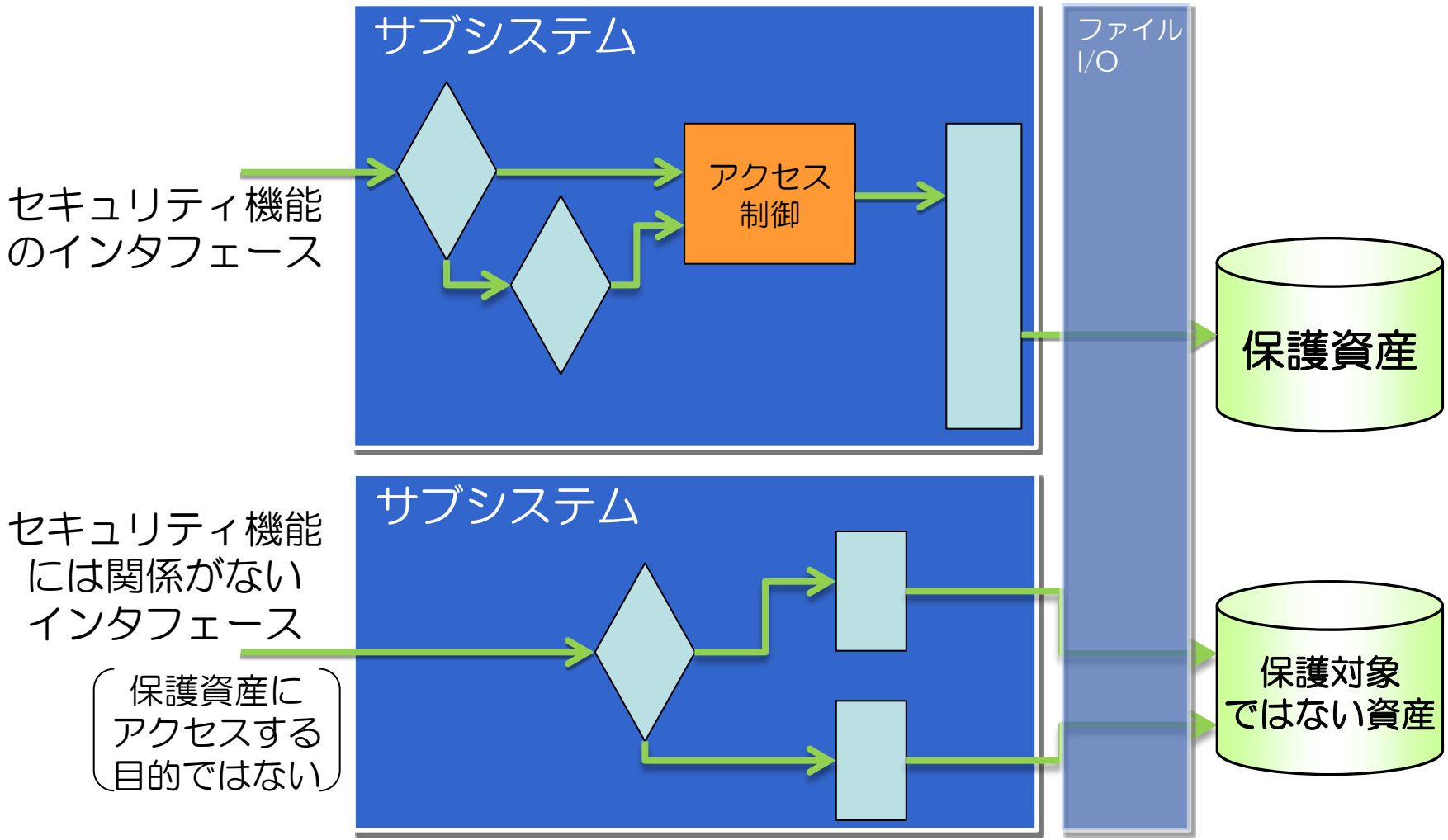
TSFの非バイパス性とは

非バイパス性が不十分な状態



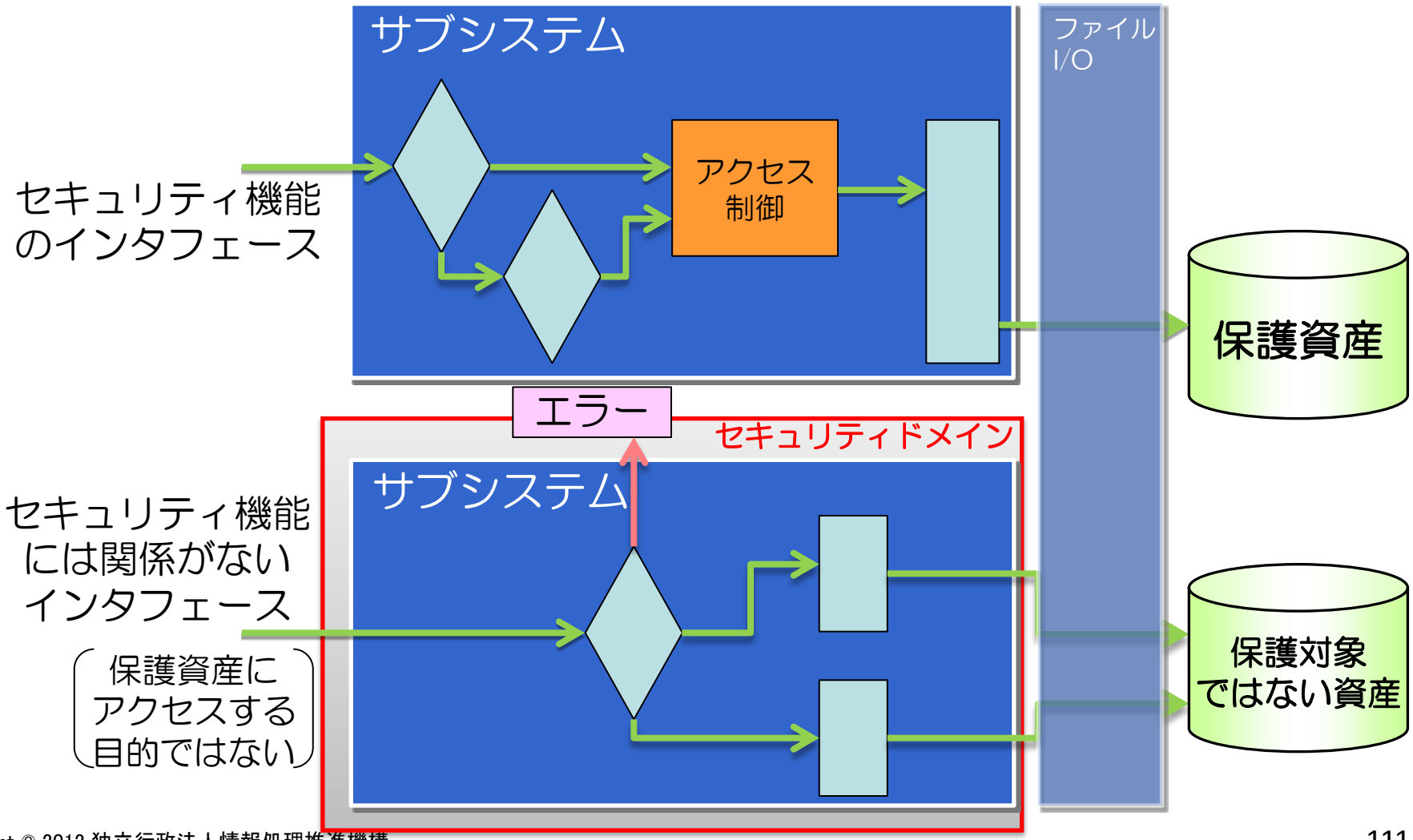
TSFの非バイパス性とは

非バイパス性が十分な状態(1)



TSFの非バイパス性とは

非バイパス性が十分な状態(2)



TSFの非バイパス性の実現

とにかくバイパス経路を作らない。例えば・・

「必ず通る処理」でセキュリティ機能が働くようにする

必ず通る処理 ⇒ ファイルI/Oのシステムコール, ディスクI/Oのドライバ など

(インタフェースが多い場合対策)

認証された者からの入力かどうかを必ずチェックする

= 認証セッションの維持・管理

(認証のバイパス対策)

TSFの非バイパス性の実現

意図せずバイパス経路ができる場合にも注意。例えば・・

必要のないインタフェースは外から使えないように(OSのインタフェースなど)

(意図しないインタフェース対策)

強い暗号アルゴリズムを使い、暗号鍵生成に使うシード等も秘密にする

(暗号の解読対策)

消費電力や処理時間が、秘密の情報の内容によらず一定に近くなるようにする

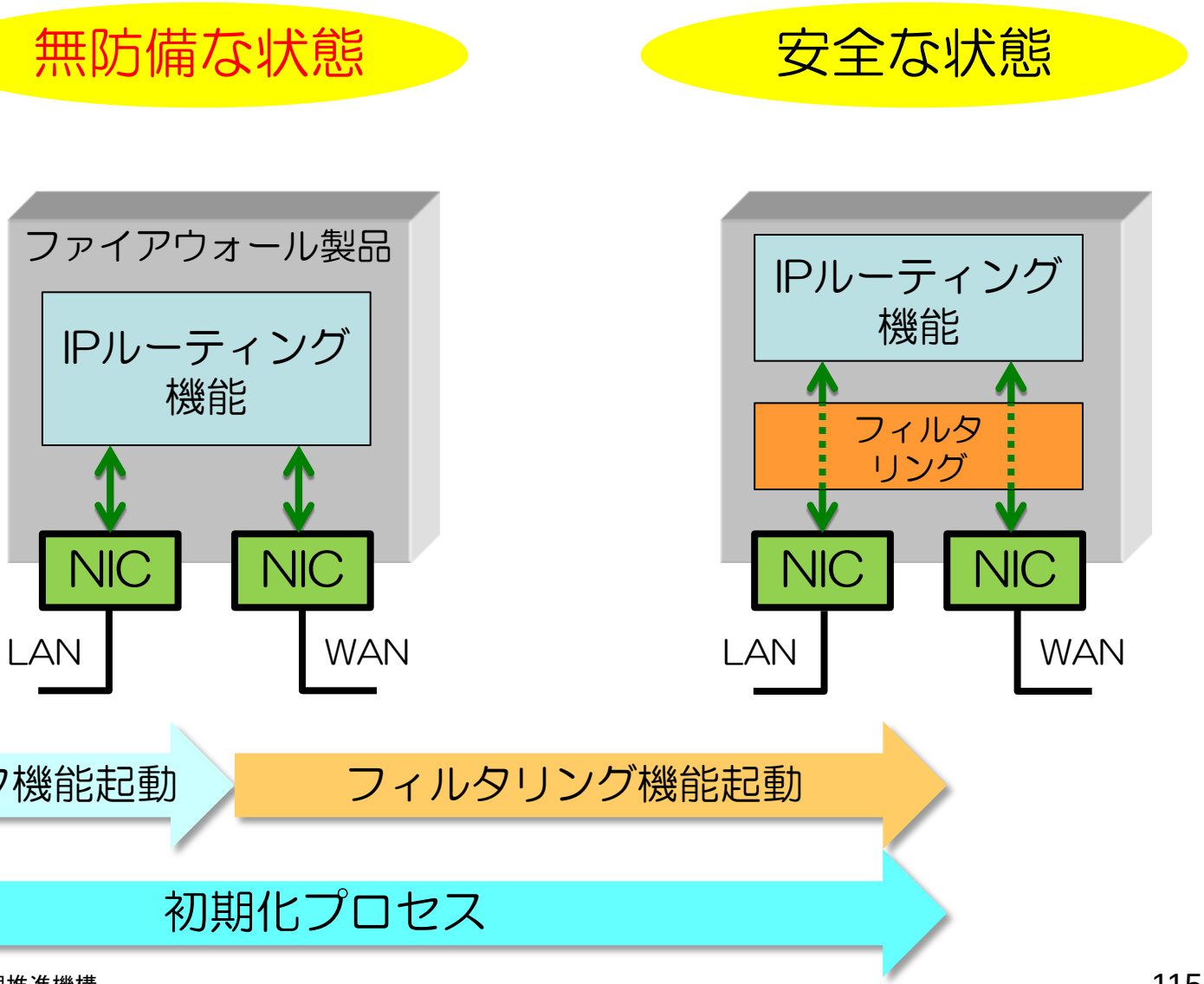
(隠れチャネル対策)

TSFの非バイパス性の記載事項

- セキュリティ機能のインタフェース
  - 保護資産などにアクセスする際に、セキュリティ機能が必ず働く理由
- セキュリティ機能には関係ないインタフェース
  - どのように使っても、保護資産やセキュリティ機能にアクセスできない理由
- 意図しないインタフェース
  - どのようなインタフェースがある可能性を考え、どのような対策をしたか

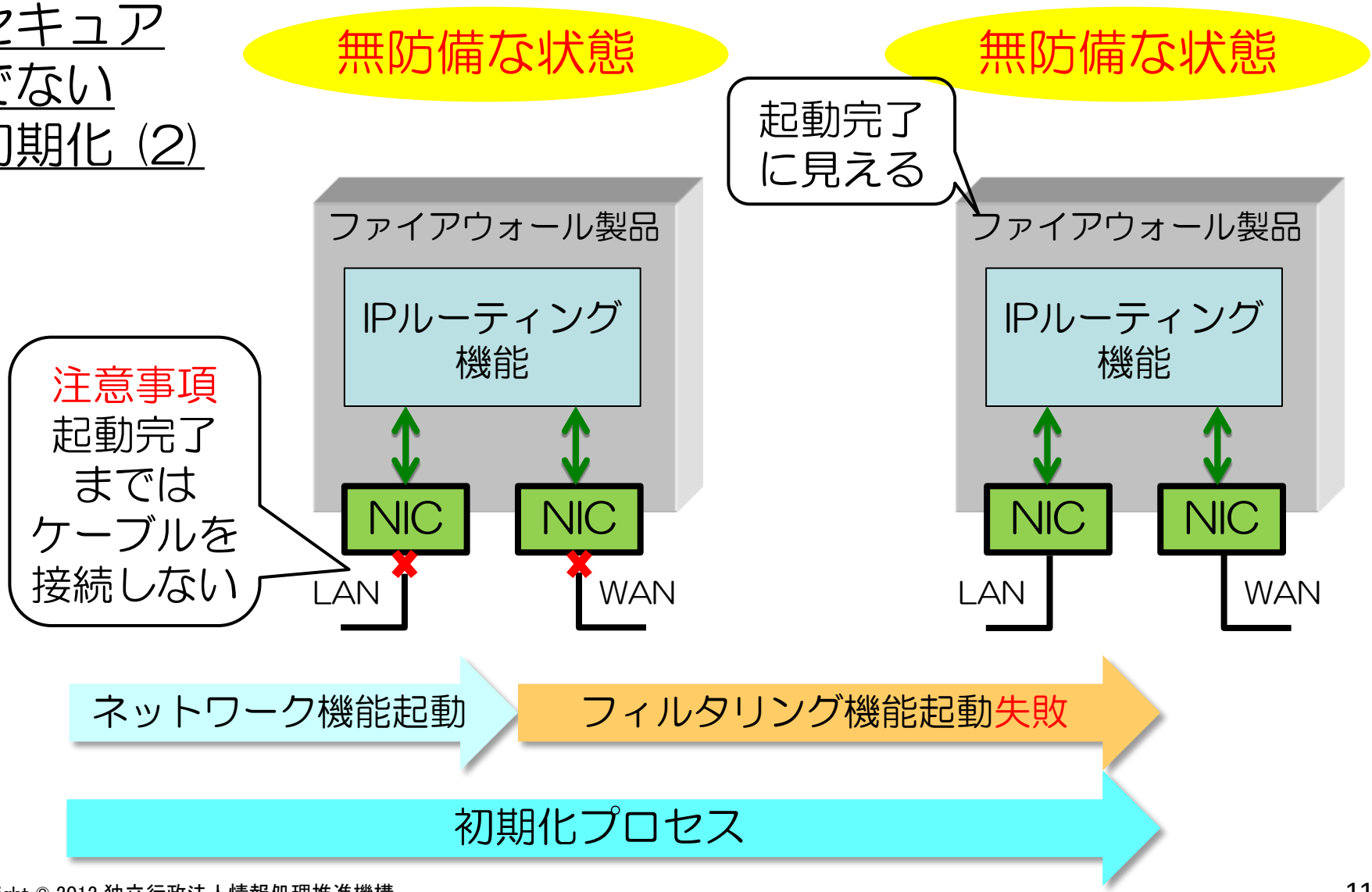
TSFのセキュアな初期化とは

セキュアでない初期化（1）

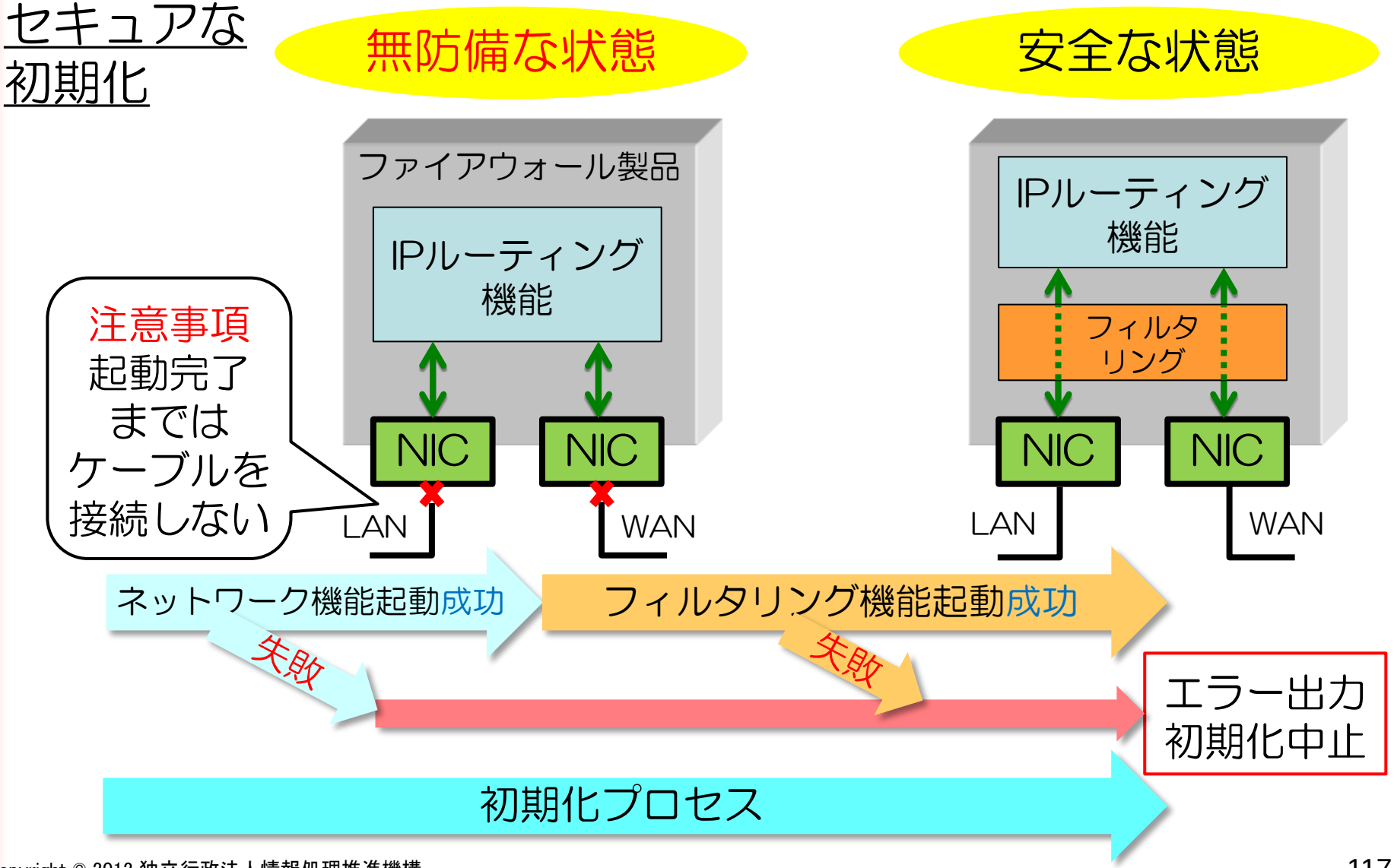


TSFのセキュアな初期化とは

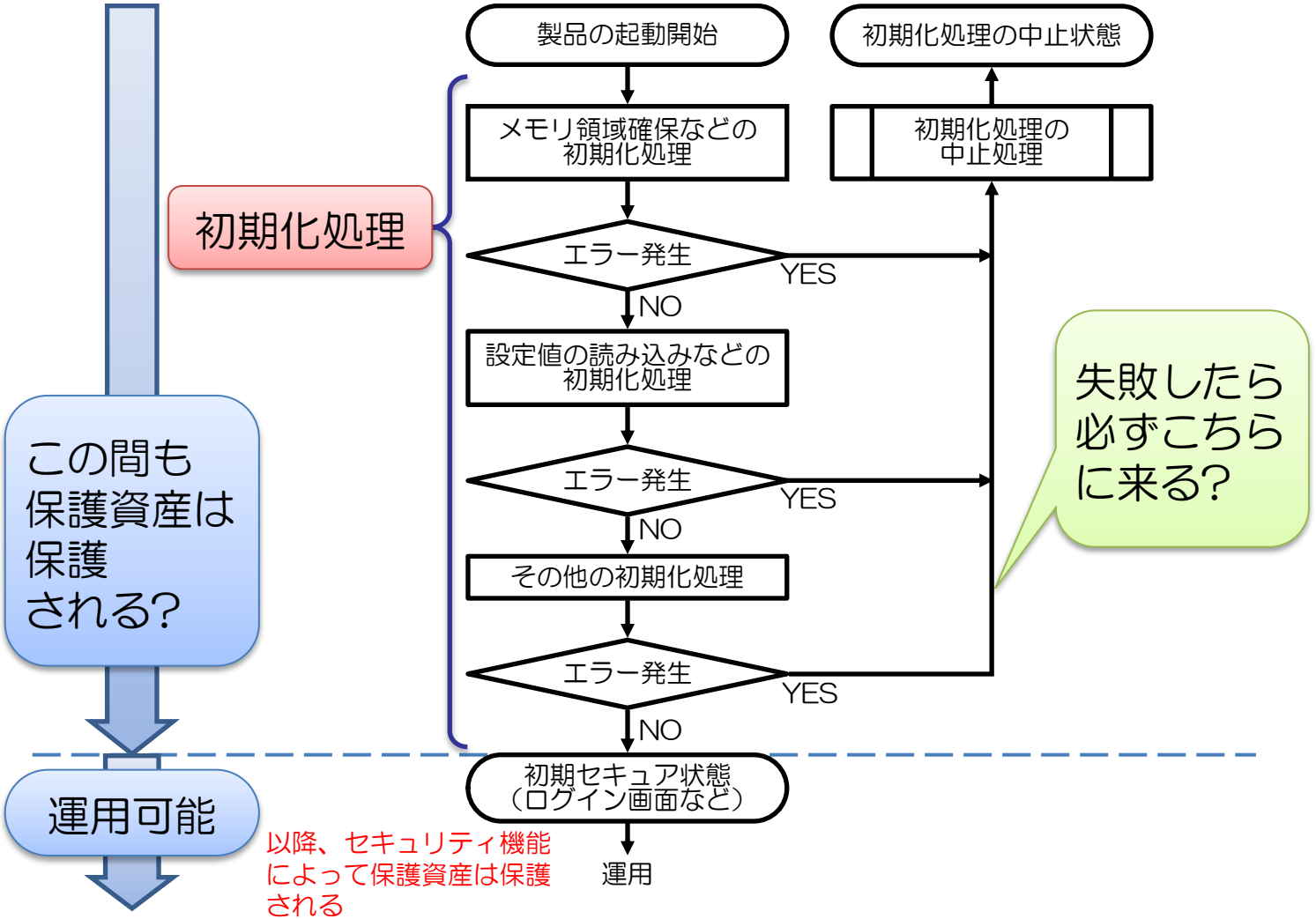
セキュアでない初期化 (2)



TSFのセキュアな初期化とは



TSFのセキュアな初期化とは



TSFのセキュアな初期化の記載事項

- 初期化処理の特定
  - 仕様書のどの部分か?
  - すべての起動方法の説明 (再起動等も含む)
  - 初期セキュア状態の説明
  - 起動から初期セキュア状態に至るまでの処理概要

- 初期化対象のセキュリティ機能の完全性確保
  - 初期化処理が以下のいずれかの結果となる理由
    - 初期セキュア状態を正しく達成できる
    - 初期セキュア状態は達成できないが安全な状態である

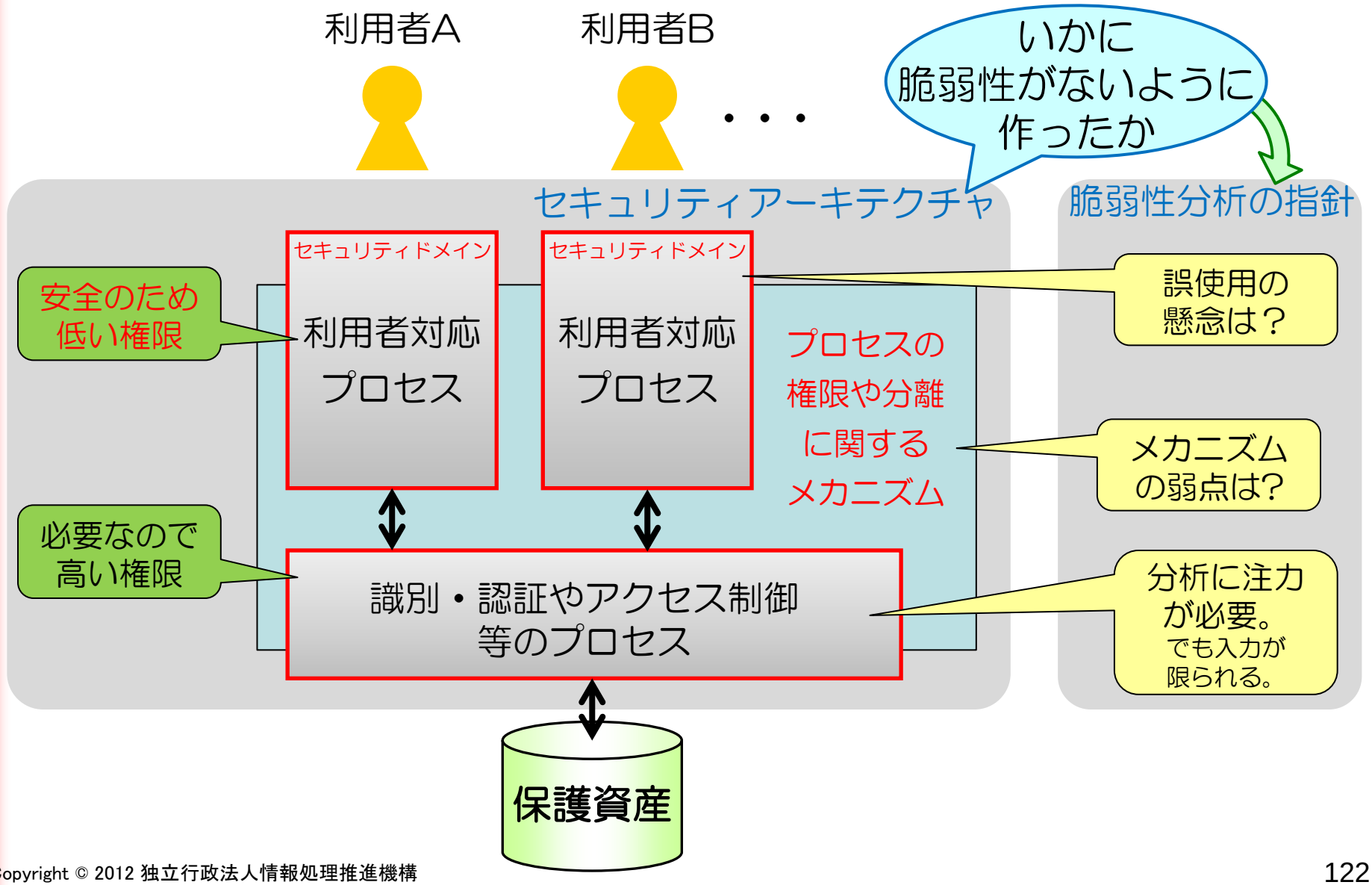
TSFのセキュアな初期化の記載事項

- 初期化処理中の保護資産の保護
  - 初期化処理の間も保護資産が安全に保たれる理由
- 初期化処理の悪用防止
  - 初期化処理が終わった後に、初期化処理の悪用が防がれる理由

セキュリティアーキテクチャに関する注意点

- TOEが実現するメカニズムはテストされていること
  - 1から作ったかどうかに係わらず、テストをした証拠が必要
- TOEが実現するメカニズムは、仕様書や実装表現で検証できること
  - 検証できるくらいに、詳細であることが必要

セキュリティアーキテクチャと分析の指針



IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

おわりに

評価の分類と必要な証拠資料(1)

クラス	ファミリ	要求される評価証拠資料の概要
要件定義（ASE）	*セキュリティターゲット(ASE)*	*TOEが実現すべき(＝開発目標となる)セキュリティ機能要件(SFR)とそれが必要となる根拠(脅威と対策の分析など)*
開発（ADV）	機能仕様(ADV_FSP)、TOE設計(ADV_TDS)、実装表現(ADV_IMP)	セキュリティ機能に関する外部設計(機能仕様)、内部設計(TOE設計)、ソースコードや回路図(実装表現) *マッピング(SFRと機能仕様(TSFI)、TSFIとTOE設計、TOE設計と実装表現)*
	セキュリティアーキテクチャ(ADV_ARC)	*セキュリティ機能が不当な影響を受けずに確実に動作することを示したもの*
テスト（ATE）	機能テスト(ATE_FUN)	TOE機能(セキュリティ機能を含む)のテスト仕様と実際のテスト結果
	カバレージ(ATE_COV)、深さ(ATE_DPT)	*充分なテストが実施されているかを分析した結果*
ガイダンス（AGD）	利用者操作ガイダンス(AGD_OPE)	TOE機能(セキュリティ機能を含む)の操作方法や障害時の復旧方法などを記述したもので、TOE購入者に配付される操作マニュアル
	準備手続き(AGD_PRE)	TOE機能(セキュリティ機能を含む)が適切に動作するための導入・設定方法について記述したインストレーションマニュアル

一から、もしくは既存資料をベースに新規作成する資料

既存の資料等をそのまま流用、もしくは一部修正

評価の分類と必要な証拠資料(2)

分類	評価証拠資料	評価証拠資料の概要
開発プロセス(ALC)	ライフサイクル定義(ALC_LCD)	開発プロセス(開発着手～保守)の定義(全体フロー、開発体制、各フェーズの作業内容・開発サイト・使用する手法・ツールなど)したもの
	CM能力(ALC_CMC)、CM範囲(ALC_CMS)	TOEを開発するために作成・使用した資材(ドキュメントなど)を構成管理するための手続き・ツール・手順などを規定したもの
	ツールと技法(ALC_TAT)	開発・分析・実装に使用する開発ツール・技術(プログラム言語、コンパイラなど)の使用方法や仕様(言語仕様など)を記述したもの
	開発セキュリティ(ALC_DVS)	開発サイトの物理的、手続き的、人的、及びその他のセキュリティ対策の基準・規定など
	配付(ALC_DEL)	製品を消費者に安全に(改ざんやすり替えなどが行われることなく)配送する手続きや手段について記述したもの

上記はEAL4に要求される証拠資料。この他に、欠陥修正(ALC_FLR)と呼ばれる欠陥(バグ、脆弱性)を修正する手続きに関する評価もあるが、本講座では対象外。

開発者は、選択したEALに応じ必要な評価証拠資料を事前に準備し、評価機関に提出する必要がある。EALやTOEの大きさに応じ、その準備期間や評価期間が異なってくる。

開発証拠資料のCC評価対応

- 証拠資料はCCの要求を満足する必要があり、いくつかの対応方法が考えられる
  - 開発に使用した証拠資料（必要に応じて修正）
  - 開発に使用した証拠資料＋不足情報を別資料で提示
  - CC評価用に新規に資料作成（あまり好ましくない）
- 留意点
  - TOEに実装された実際の仕様を正確に記述すること
    - 最も望ましいのは、実際の開発にCCの考え方を取り入れること
  - 評価の詳細度を考慮すると効率的に対応できる場合がある
    - 例えばSFR実施部分を詳細に記述し、他は概要程度など
  - 早めに評価機関と整合すること
    - TSF、TSFI、SFR実施/支援/非干渉は、評価者によって決定され開発者の判断とは異なる可能性がある

製品の脆弱性をなくすために

- CCの考え方は認証取得しない場合にも有効
  - 要件や運用条件の適切な定義
    - セキュリティターゲットに見られる考え方（本講座の対象外）
  - 要件や仕様の正確な記述（あいまいさの排除）
    - 記述形式の決められたセキュリティ機能要件（SFR）
    - EAL5以上では仕様書も(準)形式的表現
  - 要件から設計/実装への正確なブレークダウン
    - 要件のトレース（インタフェース仕様、内部仕様、実装、テスト、ガイダンス）
  - 脆弱性を防止する設計や内部構造
    - セキュリティアーキテクチャ、内部設計の構造化（EAL5以上）
  - 脆弱性分析と侵入テスト
  - 欠陥の入り込みにくい開発
    - 特に完全性（誤バージョンの混入防止、変更管理など）
    - 製造や構成管理の自動化（人的ミスの排除）

参考資料

- CC/CEM規格

http://www.ipa.go.jp/security/jisec/cc/index.html

- 証拠資料サンプル（TrueCrypt）
  - フランス認証機関が教育用に作成したサンプルの翻訳
    （教育目的でありCC評価合格の内容ではないので注意）

http://www.ipa.go.jp/security/jisec/apdx.html

- 開発者のためのセキュリティアーキテクチャ解説書
  - IPA作成

http://www.ipa.go.jp/security/jisec/apdx.html

問い合わせ先

- 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

TEL：03-5978-7538

FAX：03-5978-7548

Email：jisec@ipa.go.jp

URL：http://www.ipa.go.jp/security/jisec/index.html

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

ご清聴
ありがとうございました