ISO/IEC15408(CC)
評価証拠資料作成･レビュー講座

平成18年11月21日

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

IPA

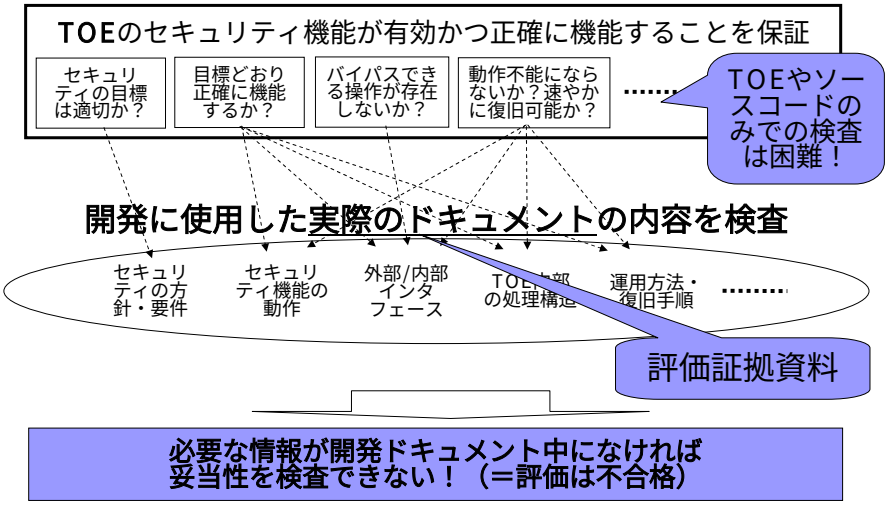
目　次（1／2）

目　次（2／2）

評価証拠資料の作成・レビューのポイント

- 開発
- テスト
- ガイダンス文書
- 配付と運用
- 構成管理
- ライフサイクルサポート
- 脆弱性評価

CC評価とは



必要な情報が開発ドキュメント中になければ
妥当性を検査できない！（＝評価は不合格）

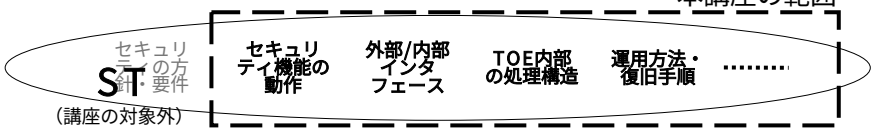
注：実際に使用したオリジナルのドキュメントを提出すること！

本講座の目標

検査(CC評価)に必要とされる情報を、**実際のTOEのとおりに**正確に開発ドキュメントに盛り込んでおくこと

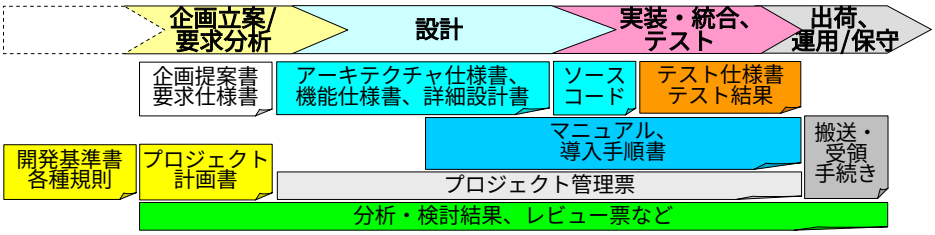
講座の目標：以下について理解すること
①CC評価に必要な情報とは何か
②セキュリティ(CC評価)の観点での留意点

本講座の範囲



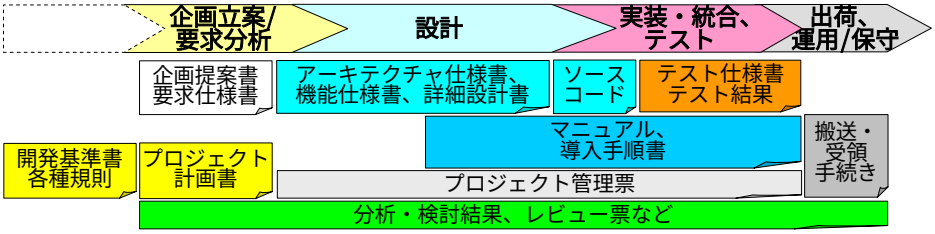
開発プロセスの一環として、CC評価の観点のレビューを行うことにより、
・CC評価に耐えうる開発ドキュメントを効率的に準備できる
・セキュリティ(特にCC)上の不備の早期発見・早期修正が可能になる

評価証拠資料のイメージ(1) ～開発ドキュメントの例～

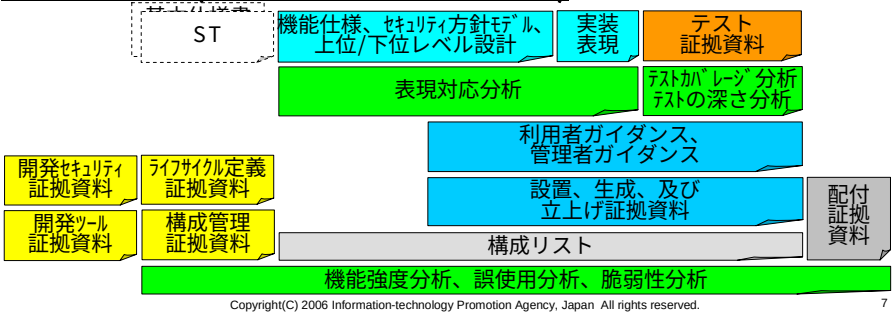


開発基準書、各種規則	組織共通の開発プロセス･開発技法、組織･開発サイトの基準･規則など
プロジェクト計画書	プロジェクトの体制、開発作業の内容･分担･成果物･責任者、スケジュールなど
プロジェクト管理票	プロジェクト成果物の一覧や開発状況（成果物の最新バージョンなど）の管理
企画提案書 / 要求仕様書	企画に基づく基本仕様、顧客要求の分析結果に基づく要求仕様など開発目標
アーキテクチャ仕様書、機能仕様書、詳細設計書、ソースコード	基本仕様/要求仕様に基づいて作成された、アーキテクチャ（ハードやネットワーク構成など）、機能及び外部インタフェース、ソフトウェア内部の処理構造など
テスト仕様書、テスト結果	製品/システムまたはその構成要素のテスト内容とその結果
マニュアル、導入手順書	製品/システムの操作方法、使用条件や導入手順の説明
搬送･受領手続き	製品の搬送や受領に関わる手続きや方法（搬送手段、受領確認方法など）
分析･検討結果、レビュー票など	各種ドキュメント作成過程における分析･検討またはレビューの内容とその結果

評価証拠資料のイメージ(2) ～開発ドキュメント例との対応～



評価証拠資料(本講座で使用される用語)



各評価証拠資料の概要(1)

開発プロセス	開発ドキュメント	評価証拠資料	評価証拠資料の概要
開発着手時、またはそれ以前	開発基準書、各種規則 プロジェクト計画書	ライフサイクル定義証拠資料	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）
		開発セキュリティ証拠資料	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
		開発ツール証拠資料	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
		構成管理証拠資料	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
開発着手～完了	プロジェクト管理票	構成リスト	TOEを開発するために作成した資材（ドキュメント類など）や開発成果のリスト
企画立案要求分析	基本仕様書、要求仕様書	－	－
	－	*ST*	TOEが実現すべき（＝開発目標となる）セキュリティ機能とそれが必要となる根拠（脅威と対策の分析など）

斜体下線は、CCで新規に作成する開発ドキュメント

各評価証拠資料の概要(2)

開発プロセス	開発ドキュメント	評価証拠資料	評価証拠資料の概要 (注：セキュリティに関わる部分が評価範囲)
設計	アーキテクチャ仕様書、機能仕様書、詳細設計書	機能仕様、上位レベル設計、下位レベル設計	開発目標のTOE機能（セキュリティ機能を含む）を、外部から見える動作（機能仕様）、内部の処理論理（上位レベル設計、下位レベル設計）などの観点で記述したもの
	ソースコード	実装表現	TOE機能（セキュリティ機能を含む）を実行コード相当のレベルで記述したもの（ソースコード、ハードウェア図面など）
	分析・検討結果、レビュー票など	*表現対応分析*	基本仕様/要求仕様･ST～機能仕様～上位レベル設計～下位レベル設計～実装表現までの設計の過程において、セキュリティ機能が適切に詳細化されていることを分析した結果
	―	*セキュリティ方針モデル*	STで決定したセキュリティ方針（アクセス制御則など）を、制御対象とその状態、適用される規則などの観点からモデル化したもの（状態遷移図など）
実装・統合、テスト	テスト仕様書、テスト結果	テスト証拠資料	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
	分析・検討結果、レビュー票など	*テストカバレージ分析、テストの深さ分析*	テスト仕様を決定するために、テストが必要な範囲（テストすべきセキュリティ機能とインタフェース）を分析した結果

斜体下線は、CCで新規に作成する開発ドキュメント

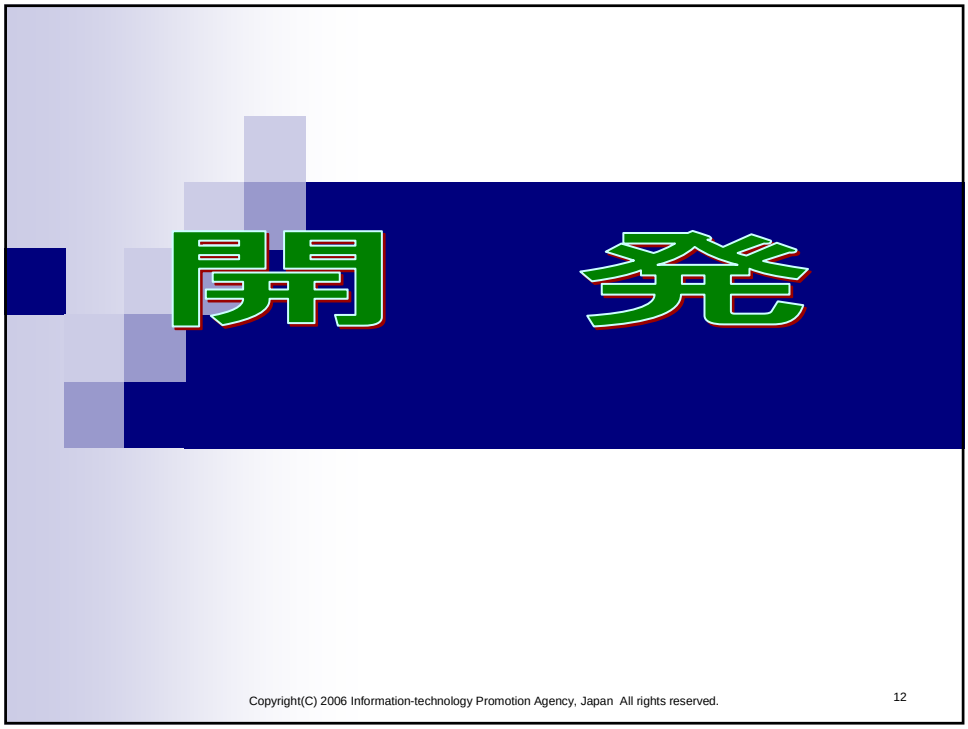
各評価証拠資料の概要(3)

開発プロセス	開発ドキュメント	評価証拠資料	評価証拠資料の概要 (注：セキュリティに関わる部分が評価範囲)
設計～出荷	操作マニュアル、導入手順書	利用者ガイダンス、管理者ガイダンス	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（利用者･管理者）に配付されるもの
		設置、生成、及び立上げ証拠資料	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もの
～出荷	搬送・受領手続き	配付証拠資料	正しく動作する（改ざんやすり替えなどが行われることなく）TOEを購入者が受領できるようにするための手続きや手段について記述したもの
開発着手～完了	分析・検討結果、レビュー票	*機能強度分析*	想定した攻撃力に十分に対抗しうるセキュリティ機能強度（パスワード長など）を決定するための分析内容とその結果
		誤使用分析	TOEの運用中に想定されるセキュリティ機能の異常状態（動作エラー、ハードウェア障害、運用ミスなど）を洗い出し、それらが対処済み、または利用者によって適切に対処できることを分析した結果
		脆弱性分析	開発ドキュメントの内容から、セキュリティ機能が適切に機能しない要因（脆弱性）を洗い出し、それらが対処済み、または想定した攻撃力では表面化しないことを分析した結果

斜体下線は、CCで新規に作成する開発ドキュメント

本講座の範囲

- CC v2.x 及び CEM v1.0/v2.3に基づく
- EAL4で要求されていることを各評価クラス別に説明
- EAL毎の詳細な違いやEAL5以上については、CC/CEMを参照のこと（本講座の対象外）
  - CC Part3
    「開発者アクションエレメント」
    「証拠の内容・提示エレメント」
  - CEM
    評価者サブアクティビティの「入力」
    各「ワークユニット」（ex. ADV_FSP.1-1、など）



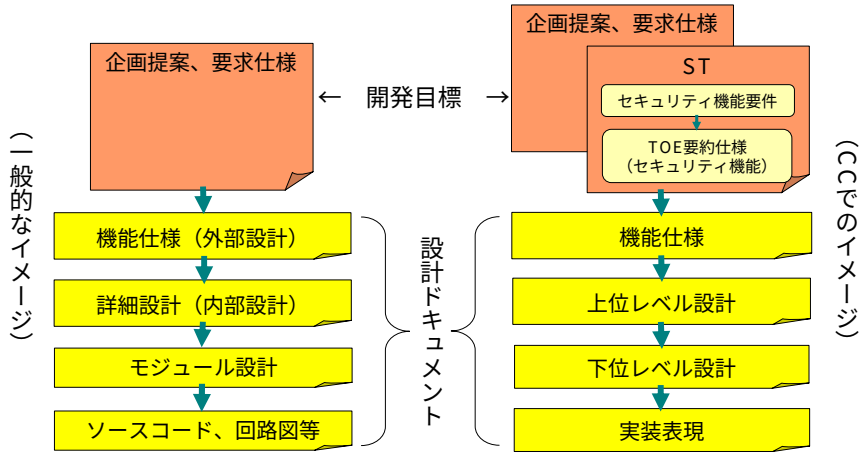
開発

目的

- STで定義したセキュリティ機能が、設計ドキュメントに正確かつ完全に詳細化・具体化され、実装されていることを保証する。
- TOE外部から見えるインタフェースを介したアクセスが、セキュリティ機能により保護されていることを保証する。

設計ドキュメントの詳細化・具体化

基本仕様や要求仕様及びSTで定義した開発目標の機能（セキュリティ機能を含む）を正しく実装するように、段階的に詳細化・具体化する。



評価に必要な資料(1)

以下の**記述内容**を含む設計ドキュメントが評価される。
（注：説明上、CC評価の区分で分類しているが、実際のドキュメントをこのとおりに分ける必要はない）

- **機能仕様書**
  TOE機能（セキュリティ機能を含む）の仕様・外部設計。
  TOEが外部へ公開するインタフェースとTOEの各機能のふるまい（外部からの指示や入力に対する動作や出力など）を説明したもの。

- **上位レベル設計書**
  機能仕様書のとおりにTOE機能（セキュリティ機能を含む）を動作させるための処理構造に関する詳細設計・内部設計。TOEの各機能の処理を分担する各部分（以降「サブシステム」と呼ぶ）ごとに、そのインタフェースと処理内容を説明したもの。

- **下位レベル設計書**
  上位レベル設計書のとおりにサブシステムを動作させるための処理方法のさらに詳細な内部設計（いわゆるモジュール設計など）。

評価に必要な資料(2)

- **実装表現**
  TOE機能（セキュリティ機能を含む）の最も詳細な表現形式（ソースコード、回路図、ハードウェア記述言語、など）。

- **表現対応分析書**
  ST（TOE要約仕様）～機能仕様書～上位レベル設計書～下位レベル設計書～実装表現までの各記述レベル間のセキュリティ機能の対応関係を示したもの。

- **セキュリティ方針モデル**
  TOE内で保護資産や資源がどのように保護されるかについて定めた規則集。この規則集（TOEセキュリティ方針(TSP)）は、ST記載のTOEセキュリティ機能要件と一貫する。

設計ドキュメントの評価に共通の考え方

- セキュリティ機能に関わる記述箇所に対して、STで定義したセキュリティ機能及び機能要件が正確かつ完全に詳細化・具体化されているかどうかが厳密に検査される。
  - 正確：STで定義したとおり／想定する動作環境で意図したとおり
  - 完全：STに記載のすべて／機能や処理に足りない部分がない
- セキュリティに関わらないTOE機能の記述箇所に対しては、TOEのセキュリティ（脅威の発生やセキュリティ機能の動作）に影響しないことが確認できればよい。

機能仕様の評価の目的

- 利用者やTOE外の機器等に提供される公開インタフェースを介した利用者データやTSFデータ、セキュリティ属性へのアクセスがセキュリティ機能により保護されていること。
- セキュリティ機能の部分の仕様が、STのTOE要約仕様で定義したセキュリティ機能を正確かつ完全に詳細化したものであること。

機能仕様書の記載事項(1)

- 外部インタフェースの仕様 4:ADV_FSP.2-5

利用者やTOE外の機器等に対してTOEが提供するインタフェースの仕様を記述する。

- 外部インタフェースから得られる効果
  ・入力（データ、パラメタ、ファイルなど）
  ・動作内容と結果
  - 入力に対する処理の概要
  - 出力先と出力内容
  ex.「～処理の結果を画面に表示する」、
  「データを暗号化して保存する」

- エラー処理とエラー出力
  ・正常でないケース（失敗時、障害時、など）
  ・それに対する処理と外部へ出力するエラーメッセージやエラーコード
  ex.「識別または認証に失敗した場合、失敗した旨の表示（図xx）を行う。」

機能仕様書の記載事項(2)

- セキュリティ機能の仕様 4:ADV_FSP.2-5

外部インタフェースを介して、セキュリティ機能がどのように動作するか、セキュリティ機能の動作にどのように影響するかについての記述を含める。
（このような外部インタフェースをTSFIと呼ぶ）

- 外部インタフェースとの関係がわかるように記述する。
  例えば、「外部インタフェースの仕様」の一部として、セキュリティ機能の動作に関連する情報を含めてもよい。
- TOE要約仕様の内容を正確に詳細化し、かつ機能仕様として不足している情報がないこと (4:ADV_RCR.1-1)
  → その検証結果のまとめ ⇒ 表現対応分析書（後述）
- セキュリティ機能失敗時のエラー処理/出力を明確にすること
- すべての動作モードを区別して記述すること（もしあれば）
  同じコマンドでも状態や権限によって動作が異なる場合など

TSFI: TOE Security Functions Interfaces

機能仕様書の記載事項(3)

- 機能仕様から漏れているTSFIがないことの論証（EAL4）

4:ADV_FSP.2-7

  - TOE要約仕様の内容を正確に詳細化し、かつ機能仕様として不足している情報がないこと
  - その他に、セキュリティ機能を必要とする外部インタフェースはないか？を論証すること

例えば
「識別認証機能は画面Aから呼び出され、その仕様の記述はTOE要約仕様を正確にカバーできている。
しかし、本当に画面Aからだけ呼び出されれば十分か？
識別認証機能が必要な外部インタフェースは他にはないのか？」

機能仕様書の記述形式の例

N. *利用者識別認証機能*
　本機能は、旅費清算システムを利用する申請者及び承認者を識別し、本人確認をするためのものである。
N.1 動作概要
　旅費清算システムのURLが入力されると最初に、旅費清算システムは識別認証画面（図N-1）を表示する。画面上でユーザIDとパスワードが入力されると、登録済みのユーザIDとパスワードと照合する。一致する場合、各利用者に応じた旅費清算トップ画面（第M章参照）を表示する。不一致の場合、本人確認に失敗した旨の画面（図N-2）を表示する。
N.2 外部インタフェース仕様
N.2.1 *識別認証画面*（図N-1）
(1)入力
　(a)ユーザID：英数字５文字以上１０文字以下の文字列で、・・・
　(b)パスワード：英数字及び記号から構成される７文字以上１２文字以下の文字列で、・・・
(2)処理内容
　：
(3)出力
　(a)識別認証成功時
　：
　(b)識別認証失敗時
　識別認証失敗画面（図N-2）を表示する。また、監査ログに・・・を記録する。
(4)例外処理
　：

M. *旅費申請・承認機能*
　：
付録A. セキュリティ機能が完全に表現されている根拠
　：

留意点(1)

- TSFI及びセキュリティ機能の仕様に関して、読者（設計書やガイダンス文書の作成者など）に誤解を与える（仕様の解釈が変わる）記述はNG。 4:ADV_FSP.2-2
  - 曖昧な用語
  - 機能仕様内で一貫性のない内容
  - 意図・読み方が不明な図表 4:ADV_FSP.2-1
- ST記載のセキュリティ機能要件と一貫し、かつ不足がないこと。 4:ADV_FSP.2-8 4:ADV_FSP.2-9
- 他の評価証拠、特にガイダンス文書に記述される情報に対して、一貫しており不足がないこと。 4:ADV_FSP.2-5

留意点(2)

- すべての外部インタフェースが識別されていること。
  ⇒外部インタフェースであることが明確に読み取れること。 4:ADV_FSP.2-3
  - STや機能仕様の文中から外部インタフェース(TSFI)の存在が読み取れるにもかかわらず、その仕様がまったく説明されていない場合はNG
  - 例えば、外部インタフェース毎に一意の名称を付与したり、節・項目を設けて説明したりするとよい
- 機能仕様から漏れているTSFIがないかどうかは評価者により検査される。 4:ADV_FSP.2-4
  注：EAL4の場合、開発者による論証も要求される 4:ADV_FSP.2-7
  ⇒ とはいえ、外部インタフェース(TSFI)を漏れなく把握することは、脆弱性分析を行う上で重要

上位レベル設計の評価の目的

- 機能仕様で定義したとおりにセキュリティ機能(TSF)が動作するように、処理構造の観点から、正確かつ完全に詳細化されていること。
  （処理構造の観点での各TOE構成要素を「サブシステム」と呼ぶ）

- セキュリティ機能(TSF)の動作に関係するサブシステムのすべてのインタフェース仕様が定義されており、特に、外部から見えているインタフェースがどれであるか明確になっていること。

TSF: TOE Security Functions

上位レベル設計書の記載事項(1)

- 処理構造の観点での仕様 4:ADV_HLD.2-3

  実現方式や処理方式などの観点から、TOE機能をいくつかの処理部分（サブシステム）に分割して、各サブシステムのインタフェースの仕様を記述する。

  - サブシステムの定義 4:ADV_HLD.2-4
    - ・各サブシステムの位置付け
      - TOE機能全体（特にセキュリティ機能）との関係
      - 各サブシステム間の関係、など
    - ・各サブシステムインタフェースの定義 4:ADV_HLD.2-7
      - エントリポイントの名称
      - 目的や用途（インタフェースの概要） 4:ADV_HLD.2-9
      - 使用方法*（インタフェースの詳細仕様）

  - *サブシステムインタフェースの使用方法 4:ADV_HLD.2-9
    - ・入力項目、出力項目
    - ・処理内容
    - ・エラー処理（例外処理を含む）及びエラー出力

エントリポイント: サブシステムレベルでのインタフェース識別子

上位レベル設計書の記載事項(2)

- 外部から見えるインタフェース　4:ADV_HLD.2-8

  各サブシステムのすべてのインタフェースを定義した上で、どのインタフェースが外部から見えているのかを明確にする。

  - TSFIのエントリポイント

    TSFI（外部に公開しているインタフェース）に対応するエントリポイントは必ず存在する。

  - 処理構造上、外部から見えているエントリポイント

    TOEから見ると内部インタフェースとして使用していても、外部からそのインタフェースが見えている場合があることに注意する。

上位レベル設計書の記載事項(3)

- セキュリティ機能との関係

  - セキュリティ機能を構成する処理　(4:ADV_RCR.1-2)

    機能仕様に定義したとおりにセキュリティ機能が動作するために必要な、サブシステムの処理内容を正確かつ完全に含める。

  - TOEのセキュリティ状態に与える影響　4:ADV_HLD.2-4

    そのサブシステムが実行された結果、TOEのセキュリティに関わるもの（利用者データ、TSFデータ、セキュリティ属性など）にどのような影響を与えるかがわかるようにする。

  - セキュリティ機能の動作への関与の有無の識別（EAL4）　4:ADV_HLD.2-10

    セキュリティ機能の動作に関係するサブシステムとそれ以外のサブシステムを明確に区別すること。

上位レベル設計書の記載事項(4)

- TSFが依存するTOE外のセキュリティ機能 4:ADV_HLD.2-5

  STにIT環境のセキュリティ機能要件が含まれている場合、以下を含める。

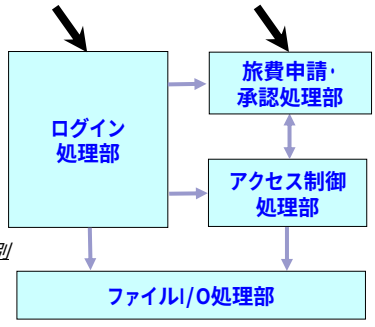
  - TSFが意図したとおりに動作するために必要となるハードウェア、ファームウェア、ソフトウェアの一覧とその説明
  - 特にTSFの動作が下層(IT環境)のハードウェア、ファームウェア、ソフトウェアに依存する場合、各サブシステムから下層のセキュリティ機能を使用する方法 4:ADV_HLD.2-6
  - ST記載のIT環境のセキュリティ要件と一貫していること

上位レベル設計書の記述形式の例

1. 全体構成
   ＃TOE機能全体とそれを処理する各サブシステムとの関係
   ＃各サブシステム間の関係、などの概要

2. サブシステムの仕様
2.2 ログイン処理部
(1)処理概要
   ＃各サブシステムの目的、他のサブシステムとの関係
   ログイン画面から入力されたIDとパスワードの組と
   登録済みのIDとパスワードの組の照合を行い、
   一致した場合、・・・。

(2)インタフェース仕様
   ＃エントリポイント名称、外部/内部インタフェースの識別
   ＃各インタフェースの目的、他のサブシステムとの関係
   ＃入出力及びエラー出力の詳細
   (a) I&A(...)
   利用者から入力されたIDとパスワードを受け付ける
   外部インタフェースであり、この入力と登録済みの・・・
   ・・・
(3)処理内容
   ＃サブシステムの処理を構成する処理項目、エラー処理、他
   ・・・
2.2 旅費申請・承認処理部
・・・



図：全体構成

留意点

- セキュリティ機能に関係するサブシステムの仕様に関して、読者（下位レベル設計書の作成者など）に誤解を与える（仕様の解釈が変わる）記述はNG。
  - 曖昧な用語 4:ADV_HLD.2-2
  - 上位レベル設計内で一貫性のない内容
  - 意図・読み方が不明な図表 4:ADV_HLD.2-1
- 外部から見えるすべてのサブシステムインタフェースが識別されていること。 4:ADV_HLD.2-8

  ⇒ 外部から見えるインタフェースを漏れなく特定することは、脆弱性分析を行う上で重要
- ST記載のセキュリティ機能要件と一貫し、かつ不足がないこと。 4:ADV_HLD.2-11 4:ADV_HLD.2-12

下位レベル設計の評価の目的

- 上位レベル設計で定義したとおりにサブシステムが動作するように、実装と同等レベルの詳細度で、正確かつ完全に具体化されていること。
  （「サブシステム」の処理を細分化した各要素を「モジュール」と呼ぶ）
- セキュリティ機能(TSF)の動作に関係するモジュールのすべてのインタフェース仕様が定義されており、特に、外部から見えているインタフェースがどれであるか明確になっていること。

TSF: TOE Security Functions

下位レベル設計書の記載事項(1)

- 実装者の観点での設計の具体化 4:ADV_LLD.1-3

  サブシステムを細分化した処理単位（モジュール）を定義し、実際に実装する際に必要な詳細度で、各モジュールの仕様を具体的に記述する。

  - モジュールの定義
    - ・モジュールの目的 4:ADV_LLD.1-4
      - 意図する処理の概要 4:ADV_LLD.1-5
      - 他のモジュールとの関係
        処理結果に依存する、サービスを提供する
    - ・各モジュールインタフェースの定義 4:ADV_LLD.1-7
      - エントリポイントの名称（関数名など） 4:ADV_LLD.1-9
      - 目的や用途（インタフェースの概説）
      - 使用方法（インタフェースの具体的な仕様）

  - モジュールインタフェースの使用方法 4:ADV_LLD.1-9
    - ・入力項目、出力項目
    - ・処理内容
    - ・エラー処理（例外処理を含む）及びエラー出力

下位レベル設計書の記載事項(2)

- 外部から見えるインタフェース 4:ADV_LLD.1-8

  各モジュールへのすべてのインタフェースを定義した上で、どのインタフェースが外部から見えているのかを明確にする。

  - TSFIのエントリポイント

    TSFI（外部に公開しているインタフェース）に対応するエントリポイントは必ず存在する。

  - 処理構造上、外部から見えているエントリポイント

    TOEから見ると内部インタフェースとして使用していても、外部からそのインタフェースが見えている場合があることに注意する。

下位レベル設計書の記載事項(3)

- セキュリティ機能との関係
  - セキュリティ機能の動作の正確かつ完全な具体化

    (4:ADV_RCR.1-3)

    サブシステム内のセキュリティ機能の動作に関係する処理部分を正確かつ完全に具体化する。
  - セキュリティ機能の動作への関与の有無の識別

    4:ADV_LLD.1-5

    4:ADV_LLD.1-10

    セキュリティ機能の処理を構成しているモジュールとそれ以外のモジュールを明確に区別すること。

下位レベル設計の記述形式の例

N. **識別・認証処理部**
N.1 モジュール構成
＃サブシステムと構成する各モジュールの関係、
＃各モジュール間の関係（処理順序など）

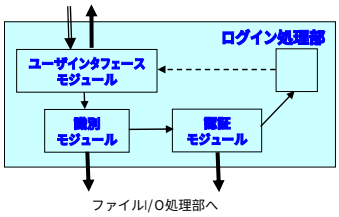
N.2 モジュール仕様
N.2.1 ユーザインタフェースモジュール
(1)概要
＃各モジュールの目的、他のモジュールとの関係など

(2)インタフェース
＃入力、出力、エラー出力

(3)処理内容
＃入力とそれに基づく処理の流れ
＃失敗時/障害時のエラー処理

N.2.2 識別モジュール
・・・

N.2.3 認証モジュール
・・・



図：ログイン処理部のモジュール構成

留意点

- セキュリティ機能に関係するモジュールの仕様に関して、読者（実装者など）に誤解を与える（仕様の解釈が変わる）記述はNG。
  - 曖昧な用語
  - 下位レベル設計内で一貫性のない内容
  - 意図・読み方が不明な図表

  4:ADV_LLD.1-2
  4:ADV_LLD.1-1

- 外部から見えるすべてのモジュールインタフェースが識別されていること。

  4:ADV_LLD.1-8

  ⇒ 外部から見えるインタフェースを漏れなく特定することは、脆弱性分析を行う上で重要

- ST記載のセキュリティ機能要件と一貫し、かつ不足がないこと。

  4:ADV_LLD.1-11
  4:ADV_LLD.1-12

実装表現の記載事項及び留意点

- より具体化することなくTOEを生成することができる表現（これ以上、詳細な表現はない）

  4:ADV_IMP.1-1

  - ソースコード、回路図、ハードウェア記述言語、など

- セキュリティ機能の動作の正確かつ完全な具体化
  - 下位レベル設計に記載したセキュリティ機能に関係する処理を正確かつ完全に実装表現に変換する

    (4:ADV_RCR.1-4)
  - ST記載のセキュリティ機能要件と一貫し、かつ不足がないこと。

    4:ADV_IMP.1-4
    4:ADV_IMP.1-3

- 内部的に一貫していること

  コールする側とされる側のインタフェースの一貫性、など

- セキュリティ機能の実装表現の一部を提供すればよい

  4:ADV_IMP.1-2

  評価者は、提供された部分が実装の妥当性を評価する上で必要な部分が提供されているかどうかを判断する→不足していれば追加提供の要求

表現対応分析の評価の目的

- STで決定したセキュリティ機能が、正確かつ完全に詳細化・具体化されていることを開発者自身が検証し、その証拠を残す。

表現対応分析書の記載内容及び留意点

- STで定義したセキュリティ機能が正確かつ完全に詳細化・具体化されたことを検証する。
  - セキュリティ機能のTOE要約仕様とTSFI及び関連するセキュリティ機能の仕様 4:ADV_RCR.1-1
  - TSFI及び関連するセキュリティ機能の仕様とサブシステムの仕様 4:ADV_RCR.1-2
  - サブシステムの仕様とモジュールの仕様 4:ADV_RCR.1-3
  - モジュールの仕様と実装表現 4:ADV_RCR.1-4
- 検証結果の対応表では、該当する記述箇所が特定できるような表記とする。
  例えば、
  - インタフェース、エントリポイントなどの識別名称
  - 文書名と章・節・項目番号、見出し名、ページ番号など
  - ソースコードのファイル名、関数名など

表現対応分析表の記述例

ST (TOE 要約仕様)	機能仕様	上位レベル設計	下位レベル設計	実現技術
6.1.1 識別・認証機能	2.1 コンソールログイン画面		3.1.1識別モジュール	ident() [i_and_a.c]
	2.2 ネットワークログイン画面		.1.2認証モジュール	auth() [i_and_a.c]
	5.1.1 識別・認証機能		⋮	
6.1.2 アクセス制御機能	3.1 copyコマンド			
	3.2 moveコマンド			
	4.1 アクセス制御リス			

STに定義したセキュリティ機能に対応する仕様をどこに記述したか？
・セキュリティ機能の動作
・外部インタフェース
・その他（関連ファイルのフォーマットなど）

仕様書の構成が、例えば、

2.1 識別・認証機能
2.1.1コンソールログイン画面
2.1.2ネットワークログイン画面
2.1.3・・・

であれば、記述箇所の示し方は、「2.1 識別・認証機能」のみとなるかもしれない。

分析したと主張できる程度に記述箇所を特定する。

章節レベルで十分な場合もあれば、ページ番号も必要な場合があるかもしれない。
また、複数の文書に分かれている場合、文書名も必要となる。

セキュリティ方針モデルの目的

- TOEの利用中/運用中を通して、TOEがセキュアであるために、TOEが実施すべきセキュリティ方針(TSP)を明確にする。
- TOEセキュリティ方針モデルも考慮することにより、適切な機能仕様であることの保証を高める。

セキュリティ方針モデルの記載事項(1)

- セキュリティ方針モデル　4:ADV_SPM.1-1

  STのTOEセキュリティ機能要件やTOEセキュリティ対策方針に基づいて、TOEセキュリティ方針(TSP)のモデルを記述する。

  - TOEのセキュリティの概念　4:ADV_SPM.1-4
    ・保護資産
    ・確保すべきセキュリティ（機密性、完全性、可用性など）
  - セキュリティ方針に関わる規則　4:ADV_SPM.1-2　4:ADV_SPM.1-3
    ex. アクセス制御規則、情報フロー制御規則、など
  - 関連するエンティティの定義　4:ADV_SPM.1-4
    サブジェクト、オブジェクト、セキュリティ属性、TSFデータ、など
  - セキュアな状態の定義　4:ADV_SPM.1-4
    セキュリティ属性やTSFデータを用いて表現
    ・規則の適用前のセキュアな初期状態
    ・規則の適用後のセキュアな状態

セキュリティ方針モデルの記載事項(2)

- セキュリティ方針モデルの根拠

  セキュリティ方針モデルが妥当であり、かつ機能仕様に適切に詳細化されている根拠を記述する。

  - セキュリティ機能要件との一貫性　4:ADV_SPM.1-5
    各TOEセキュリティ機能要件の定義内容と一貫していることを示す。
  - セキュリティ機能要件との完全性　4:ADV_SPM.1-6
    STのすべてのセキュリティ機能要件のすべての定義内容を含んでいることを示す。
  - 機能仕様との一貫性
    - 機能仕様のセキュリティ機能との対応関係　4:ADV_SPM.1-7
    - その対応が妥当である根拠　4:ADV_SPM.1-8
      ・規則の内容
      ・セキュアな状態の定義

セキュリティ方針モデルの記述例

1. TOEのセキュリティの概念
　本TOEの保護資産はXXX、YYY、・・・である。
XXXは、TOEに入力されてから・・・までの間の機密性が確保されなければならず、・・・。
YYYは、・・・

2. 個々のセキュリティ方針モデル
　2.1 利用者データ保護セキュリティ方針モデル
　・・・

　2.2 識別認証セキュリティ方針モデル

　2.2.1 概要
　　本セキュリティ方針は、本TOEの～機能を利用しようとする利用者が許可された人物かどうかを識別し、本人確認を行うものである。
　　このセキュリティ方針は、「1.1 利用者データ保護セキュリティ方針モデル」を実施する前に必ず実施されなければならない。

　2.2.2 エンティティの定義
利用者：・・・
・・・

　2.2.3 規則
(1)外部からTOE内にアクセスがあるすべての場合に、他の処理の前に必ずTOEは利用者に対する識別・認証を実行する。
(2)入力された利用者IDがTOEに登録済みである場合のみ、TOEは識別を成功と判断する。
(3)入力されたパスワードが、識別に成功したユーザIDに対応付けられているパスワードと完全に一致する場合のみ、TOEは認証を成功と判断する。
(4)・・・

　2.2.4 初期条件
　　利用者IDは英数字・・・を、またそのパスワードは英数字記号・・・を満たさなければならない。
・・・

　2.3 管理セキュリティ方針モデル

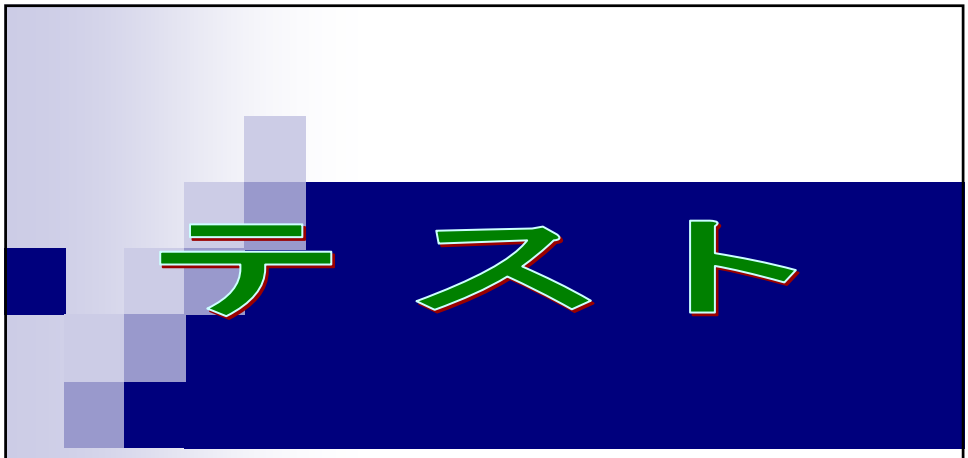
留意点

- セキュリティ機能要件で明示されたセキュリティ方針と明示されないセキュリティ方針の両方を含めること
  - 明示された方針　4:ADV_SPM.1-2
    アクセス制御規則、情報フロー制御規則
  - 明示されない方針　4:ADV_SPM.1-3
    その他のデータ保護方針(FDP)、識別・認証方針(FIA)、監査方針(FAU)、暗号方針(FCS)、セキュリティ管理方針(FMT)など
- 根拠では、記述箇所の対応関係(表現対応分析表など)とその対応が妥当である理由が必要　4:ADV_SPM.1-7　4:ADV_SPM.1-8
- 記述を詳細にし過ぎないほうがよい
  詳細にし過ぎると、規則がカバーする利用/運用の状態・範囲に考慮漏れの恐れがあるため

  ⇒セキュリティ機能要件の内容をカバーできる程度に

EALによる違い

- EAL1
  機能仕様に相当する設計ドキュメントと、ST～機能仕様間の表現対応分析
- EAL2
  機能仕様及び*上位レベル設計*に相当する設計ドキュメントと、ST～*上位レベル設計*までの表現対応分析
- EAL3
  機能仕様及び*上位レベル設計*に相当する設計ドキュメントと、ST～上位レベル設計までの表現対応分析
- EAL4
  機能仕様、上位レベル設計、*下位レベル設計*、及び*実装表現*に相当する設計ドキュメントと、ST～*下位レベル設計*までの表現対応分析と、*セキュリティ方針モデル*



テスト

目的

ITシステムまたは製品が持つセキュリティ機能が、設計書に記述されているセキュリティ機能の仕様どおりに動作することを保証する。

評価に必要な資料

- **テスト証拠資料**
  テスト手順、実際のテスト結果など。
- **テストの妥当性を判断する資料**
  実施したテストが、セキュリティ機能の動作確認として妥当であると判断するための資料。
  (テストカバレージ分析、テストの深さ分析)
- **機能仕様書、上位レベル設計書**
  セキュリティ機能について、外部インタフェース、サブシステムを観点に記述した設計書。

テスト証拠資料

実際にテストを実施した証拠として、以下の内容を含む資料を準備する。 4:ATE_FUN.1-1

1. テスト計画
2. テスト手順
3. 期待するテスト結果
4. 実際のテスト結果

テスト証拠資料

1.テスト計画

実施するテストの内容を整理したテストの事前準備資料。資料には、以下の情報を含める。

- ①セキュリティ機能名 4:ATE_FUN.1-2
- ②テストの目標 4:ATE_FUN.1-3
- ③テストの方法 4:ATE_FUN.1-3
- ④テスト環境 4:ATE_FUN.1-3

テスト証拠資料

1.テスト計画(つづき)

①セキュリティ機能名　4:ATE_FUN.1-2

テストするセキュリティ機能名を記述する。

②テストの目標　4:ATE_FUN.1-3

セキュリティ機能の動作確認としてこれから実施するテストの目標（何を確認するのか）を記述する。

テスト証拠資料

1.テスト計画(つづき)

③テストの方法　4:ATE_FUN.1-3

テストを実施するための方法を記述する。テスト用ツールを使用する等

④テスト環境　4:ATE_FUN.1-3

セキュリティ機能のテストを実施するために必要な環境を記述する。

テスト証拠資料

4:ATE_FUN.1-6
4:ATE_FUN.1-7
4:ATE_FUN.1-8

2. テスト手順

各セキュリティ機能について、期待されるテスト結果を取得するために必要な「⑤テスト手順」や「⑥テストのための初期条件」を記述する。

「テストの初期条件」は、テストの実施順序など、テストを再現するために必要な条件を全て記述する。

テスト証拠資料

4:ATE_FUN.1-10

3. 期待されるテスト結果

どのようなテスト結果が取得できればテストが成功したか判断するための情報として「⑦期待されるテスト結果」を記述する。

テスト証拠資料

4. 実際のテスト結果 4:ATE_FUN.1-11

実際にテストを実施した結果を添付する。

留意点

実際のテスト結果がバイナリデータのような状態で取得されている場合（容易に内容確認ができない状態）、「期待されるテスト結果」と「実際のテスト結果」の比較が行えるような手順を提供する。

テスト証拠資料

留意点

- テスト環境は、STに記載されているTOEの動作環境と矛盾しないこと 4:ATE_FUN.1-4
- テスト計画とテスト手順は一貫していること 4:ATE_FUN.1-5
- テスト手順に関する記述内容は、実際のテスト手順と一貫していること 4:ATE_FUN.1-9
- 期待されるテスト結果と実際のテスト結果は一貫していること 4:ATE_FUN.1-11
- テスト方法とテスト手順は、セキュリティ機能の期待されるふるまいを実証するのに適していること 4:ATE_COV.2-2 4:ATE_DPT.1-2 4:ATE_DPT.1-3

テストの妥当性を判断する資料

テスト内容の妥当性を判断するための資料として、以下の内容を含む資料を準備する。

1.テストカバレージ分析

テストを実施した範囲（どのセキュリティ機能をテストしたのか）を示す資料。

2.テストの深さ分析

テストを実施したレベル（サブシステム／内部インタフェースまで意識してテストしているか）を示す資料。

テストの妥当性を判断する資料

1. テストカバレージ分析

4:ATE_COV.2-1

- 機能仕様書に記述されているセキュリティ機能／外部インタフェースについて、テストの実施状況を提示する。
- テスト名と機能仕様書のセキュリティ機能／外部インタフェースの対応関係を示す表やマトリクスがある場合は、それを使用することができる。
- 表やマトリクスでなくても、評価者が機能仕様書について系統的にテストされていることが判断できる資料があればよい。

テストの妥当性を判断する資料

留意点

4:ATE_COV.2-1

全てのセキュリティ機能がテストされていなくても問題ない（EAL2）。テストしていないセキュリティ機能は、評価者によってテストされることがある。

全てのセキュリティ機能についてテストされていることが必要（EAL3、EAL4）。

テストの妥当性を判断する資料

留意点（つづき）

4:ATE_COV.2-3

セキュリティ機能／外部インタフェースとテスト証拠資料の対応関係が正しいこと。

例）
データを暗号化してハードディスクに書き込むというセキュリティ機能のテストにおいて、そのテストの実施方法が外部インタフェースの目視による手順が記述されていた場合、対応は不正確である。ハードディスクのデータのダンプなどを取り確認するのが一般的である。

テストの妥当性を判断する資料

2. テストの深さ分析

4:ATE_DPT.1-1

- 外部インタフェースだけではなく、サブシステム（内部インタフェース）を意識してテストしていることを主張する。
- テスト名と上位レベル設計書のセキュリティ機能／インタフェースの対応関係を示す表やマトリクスがある場合は、それを使用することができる。
- 表やマトリクスでなくても、評価者が上位レベル設計書についてテストされていることが判断できる資料があればよい。

テストの妥当性を判断する資料

留意点

4:ATE_DPT.1-4

上位レベル設計書に記述されている全てのサブシステムがテストされていること。

サブシステム間のインタフェース（内部インタフェース）が存在する場合、そのインタフェースについてもテストされていること。

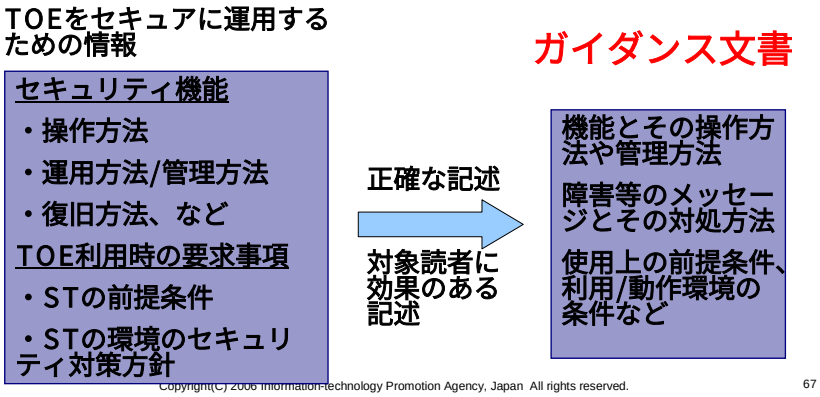
EALによる違い

- EAL1：テストのエビデンスは必要ない
- EAL2：「テスト証拠資料」、「テストの妥当性を判断する資料（テストカバレージ分析）」が必要
- EAL3：「テスト証拠資料」、「テストの妥当性を判断する資料（テストカバレージ分析、テストの深さ分析）」が必要。
- EAL4：EAL3と同様

ガイダンス文書

ガイダンス文書とは

- TOEの使用方法や管理方法を説明したもの。
  CCでは、TOEの運用中にセキュリティ機能が意図したとおりに機能するために必要な、TOEの使用方法や管理方法の説明が評価される。



必要な評価証拠資料

- 管理者ガイダンス
  間違った操作や対処を行うと、TOEのセキュリティに影響を与えるような使用方法・管理方法などについて記述したもの。
  いわゆる「管理者」と呼ばれる、責任や信頼を伴う人物向けのドキュメントまたは記述部分。

- 利用者ガイダンス
  間違った操作や対処を行うと、操作者自身が所有するデータや操作対象のデータに悪影響を与えるような機能の使用方法について記述したもの。
  「管理者」以外の一般利用者向けのドキュメントまたは記述部分。

注：「管理者ガイダンス」「利用者ガイダンス」は、必ずしもドキュメントを分ける必要はなく、必要な情報をそれぞれの対象読者に適切に伝わるように記述してあればよい。

１．管理者ガイダンス

管理者とは

- TOEのセキュリティ上重要な操作の実行権限を持つ人物
  - TOEや利用者の全体に影響するパラメタ設定
  - 利用者の追加/削除、等
- TOEや利用者に対する管理作業の実行権限を持つ人物
  - 監査者
  - データベース管理者
  - 設定の承認を行う承認者
  - 日常運用管理者、等
    - バックアップ / リストア管理者

管理者ガイダンスに必要な情報

1. 管理者が使用できるセキュリティ機能の操作方法
2. TOEのセキュアな管理方法・手段
3. 機能とその利用権限の管理
4. 利用者のふるまいに関する前提条件
5. 管理すべきセキュリティパラメタ
6. セキュリティ関連事象とその対処方法
7. IT環境のセキュリティ機能の運用方法

管理者ガイダンスの記載事項(1)

１．管理者がセキュリティ機能を正しく使用するために、セキュリティ機能の操作方法を記述する。

管理者が操作方法を理解できるように、実際のTOEに基づく以下の情報を含める。

①管理者が使用する外部インタフェース(UI, API等)とその用途

②インタフェースを介して使用できるセキュリティ機能の目的、ふるまい、操作方法など

③その他の情報
1)外部インタフェースの起動方法
（メニュー選択、コマンド、ボタン等）
2)管理者が設定するパラメータと、その有効な値とデフォルト値
3)セキュリティ機能からの応答、メッセージ、リターンコード

4:AGD_ADM.1-1

管理者ガイダンスの記載事項(2)

２．TOEの使用環境において、TOEをセキュアに管理するための方法や手段を記述する。

ST記載の環境のセキュリティ対策方針に従って、TOEを運用・管理するための方法や条件なども記述することに留意。

ex1)前提条件「TOEを外部ネットワークと接続する場合は、外部からの侵入を防止するための機器を介して接続される。」

→使用環境の注意事項として「外部ネットワークとの接続時はファイアウォールを介して接続しなければならない。」などの説明と、ファイアウォールの規則にどのような条件が必要かを明記する。

ex2)環境のセキュリティ対策方針「TOE管理者は、リモート環境でTOEを操作する場合、セキュアシェルを使用する。」

→TOE管理方法の説明として、”telnet”による操作方法を説明するなど、環境のセキュリティ対策方針に従わない記述がないこと。

4:AGD_ADM.1-2

管理者ガイダンスの記載事項(3)

3．権限ごとに使用が制限される機能を適切に運用するために、各機能とその利用権限に関する注意事項を記述する。

使用を制限する機能とその機能の利用権限に関する注意事項として、以下の情報を含める。

①権限管理の概要

②上記の権限管理が必要な理由
その管理が目的とする効果、その管理による目的外の副作用、（もしあれば）他の機能と権限への影響の観点から注意を喚起する。

ex) 監査機能を操作権限を「監査者」、その他のTOE管理機能の操作権限を「管理者」と区別するTOEの場合

「注意！：一般利用者と管理者の両者に不正操作がないことを適切に監査するには、監査者は本製品の一般利用者でも管理者でもあってはならない。もし兼任できるならば、監査者は、監査ログの削除などを行うことにより、自身の不正行為を隠蔽することが可能になることに留意すること！」

4:AGD_ADM.1-3

管理者ガイダンスの記載事項(4)

4．TOEをセキュアに運用するための前提として、管理者の責任の下、利用者に徹底させるべきふるまいについて記述する。

STに記載した利用者のふるまいに関する前提条件を満たすために、管理者のとるべきアクションを記述する。

ex) STの前提条件「TOEの利用者は、自身のパスワードが漏洩しないように管理する。」とした場合

「管理者は、利用者にアカウントを付与する際には必ず、利用者自身のパスワードの秘密保持を遵守するように通知するなど、パスワード管理を徹底させること。」

4:AGD_ADM.1-4

管理者ガイダンスの記載事項(5)

5．セキュリティ機能を有効に機能させるために必要なセキュリティパラメタの設定値について記述する。

セキュリティ機能の効果に影響するすべてのパラメタ（データ）について、以下の情報を記述する。

①パラメタの目的・意味（何のためのパラメタか）

②パラメタの有効な値またはその範囲、デフォルト値

③パラメタのセキュアな値またはその組み合わせ、及びセキュアでない値またはその組み合わせ

ex1)「暗号通信機能のON/OFF：設定画面からON/OFFのいずれかが選択できる（デフォルトでは”OFF”）。常に暗号通信を行うためには、”ON”を選択してOKボタンを押下した後、必ず再起動しなければならない。」

ex2)「ログファイルに記録されなくなるため、セキュアシェルデーモンの起動オプションには”-q”を指定してはいけない。」

4:AGD_ADM.1-5

管理者ガイダンスの記載事項(6)

6．運用中、TOEをセキュアな状態に維持するために、管理者が対処しなければならないセキュリティ関連事象とその対処方法について記述する。

運用中に起こりうるセキュリティ関連事象について、セキュリティを維持・回復するために管理者がとるべきアクションを記述する。

ex1)セキュリティ関連事象の例
- ・監査ログのオーバーフロー
- ・利用者アカウントの追加・削除
- ・利用者の離籍の利用者アカウントの削除
- ・システムエラー　など

ex2)監査ログが満杯に達しているという警告を管理者が受信した場合、管理者が監査記録のバックアップを実施する手順を記述する。

4:AGD_ADM.1-6

管理者ガイダンスの記載事項(7)

7．TOEをセキュアに運用・管理するために、IT環境のセキュリティ機能の使用・運用方法について記述する。

STにおいて、管理者が使用するIT環境のセキュリティ要件を特定した場合、そのセキュリティ機能の適切な使用方法や運用・管理方法を記述する。

ex) IT環境のセキュリティ要件として「高信頼タイムスタンプ（FPT_STM.1）」が特定されている場合

「管理者は、OSの時刻を定期的に正しく設定すること。」

4:AGD_ADM.1-8

２．利用者ガイダンス

利用者とは

- TOEやその利用者に対して管理的な役割をもたない人物（いわゆる一般利用者）
- 多くの場合、悪意の操作の可能性があるなど、完全には信頼できない人物
- TOEの操作ミスを行っても、TOE全体のセキュリティには影響しない
  （操作ミスによる損失は、その本人の権限・責任の範囲の場合など）

利用者ガイダンスに必要な情報

1. 利用者が使用できるセキュリティ機能の操作方法
2. 機能とその利用権限の区別
3. 利用者のふるまいに関する前提条件
4. IT環境のセキュリティ機能の使用方法

利用者ガイダンスの記載事項(1)

１．利用者がセキュリティ機能を正しく使用するために、セキュリティ機能の操作方法を記述する。

利用者が操作方法を理解できるように、実際のTOEに基づく以下の情報を含める。

①利用者が使用する外部インタフェース(UI, API等)とその用途

4:AGD_USR.1-1

②インタフェースを介して使用できるセキュリティ機能の目的、ふるまい、操作方法など

③その他の情報
1)外部インタフェースの起動方法
（メニュー選択、コマンド、ボタン等）
2)利用者が設定するパラメータと、その有効な値とデフォルト値
3)セキュリティ機能からの応答、メッセージ、リターンコード

4:AGD_USR.1-2

利用者ガイダンスの記載事項(2)

2．必要な権限が異なる機能を適切に使用するために、各機能とその利用権限に関する注意事項を記述する。

必要な権限の異なる機能の使用に関する注意事項として、以下の情報を含める。

①機能を使用可能な権限とその権限に必要な能力の概要

②権限にその能力が必要な理由

その使い分けによる効果、適切に使い分けなかった場合の悪影響、（もしあれば）他の機能と権限への影響の観点から注意を喚起する。

ex) データの閲覧のみが可能な権限を「閲覧者」、データの登録・変更が可能な権限を「一般利用者」と区別するTOEの場合

「一般利用者権限でアクセスしたデータはあらゆる操作が可能になるため、誤って削除するとそのデータを復旧することはできません。したがって、通常は、閲覧者権限でデータにアクセスし、必要に応じて一般利用者権限でアクセスすることをお勧めします。」

4:AGD_USR.1-3

利用者ガイダンスの記載事項(3)

3．利用者がTOEをセキュアに利用できるための前提として、利用者が遵守しなければならないふるまいについて記述する。

STに記載した前提条件を満たすよう、利用者が適切に行動できるように以下のような情報を含めるべきである。

①セキュリティ機能を効果的に使用するためのアドバイス・注意喚起

ex)アドバイス・注意喚起の例

- パスワードの決め方、推奨する変更頻度
- 利用者ファイルの推奨するバックアップ頻度
- 不適切なアクションに伴う悪影響、など

②利用者単独で実施できるかどうか

ex)「パスワードを定期的に変更しなければならない。なお、パスワードを変更するには、管理者への依頼が必要である。」

4:AGD_USR.1-4

利用者ガイダンスの記述事項(4)

4．TOEをセキュアに利用するために必要な、IT環境のセキュリティ機能の使用方法について記述する。

STにおいて、利用者が使用するIT環境のセキュリティ要件を特定した場合、そのセキュリティ機能の適切な使用方法を記述する。

ex) IT環境のセキュリティ要件として「識別・認証機能（FIA_UID&FIA_UAU)」が特定されている場合

「利用者は、本ツールを利用するにあたり、まずOSに登録されたアカウントでログインを行わなければならない。」

4:AGD_USR.1-6

3．ガイダンスの留意点

ガイダンスと他の文書は矛盾してはならない。

- ex) セキュリティ機能使用についての一般的なガイドラインと矛盾しない
- ex) STと矛盾しない
- ex) 機能仕様、上位レベル設計、下位レベル設計と矛盾しない
- ex) セキュリティ方針モデルと矛盾しない

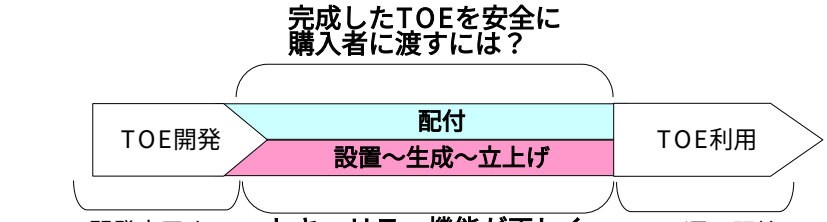
4:AGD_ADM.1-7 4:AGD_USR.1-5

配付と運用

IPA

配付と運用とは

- 完成したTOEを開発サイトから利用者に安全に受け渡し（配付）、セキュリティ機能が有効に機能する状態（運用可能な状態）に立ち上げるための手続きや手順を記述したもの



～TOE開発完了まで
・構成管理
・開発セキュリティ
・設計/実装、テスト
など

セキュリティ機能が正しく動作する状態にするには？

TOE運用開始から～
・セキュリティ機能
・利用者/管理者による利用方法/管理方法

必要な評価証拠資料

- **配付証拠資料**
  TOEを改ざんされることなく購入者に配付するための手続きや手順を記述したもの。
  （配送手続き書、受領手続き書、など）

- **設置、生成、及び立上げ証拠資料**
  TOEを適切な使用環境に設置し、適切な構成で配置し、適切な設定で立ち上げるための条件、手順、設定などを記述したもの。
  （設置手順書、インストールガイドなど）

注：それぞれの資料は、通常、そこに記述される手続き・手順を実施する人物（開発者、開発側の代行者、購入者など）が入手し、閲覧できるように、適宜、別ドキュメントに分離してもよい。

配付の目的

- 設備、手続き、技術的手段などにより、TOEを製造環境から購入者の設置環境まで、セキュリティ（特に完全性）が維持されるように配付すること

- いわゆる「配送」だけでなく、開発サイトでのパッケージングや保管のフェーズも考慮する必要がある

- 「配送」も、TOEの開発者だけでなくその他の関与者（TOE開発者と同一組織の出荷部門、配送業者、販売代理店など）についても考慮する必要がある

配付の考慮点

1．購入者が受け取ったTOEが、開発者が作成したTOE(マスターコピー)と正確に一致することを保証する。（完全性が求められる場合。**必須**）

- TOEに対する改ざんを防止する／検出する。
- 誤ったバージョンのTOE、不正なTOEの送付を防止する。

2．正しい購入者の元にTOEを送り届けることを保証する。（機密性が求められる場合）

- 購入者や配付の関係者へのなりすましを防止する／検出する。

配付証拠資料の記載事項(1)

1．TOEを購入者に安全に配付するために必要な手続きを記述する。

TOE及び各種ガイダンス文書を配付する手段と、それぞれの配付手段においてセキュリティを維持するための手続き・方法や技術的手段などを記述する。

ex1)TOEが経由する組織・場所
出荷部門、倉庫、運送業者、販売代理店、など
ex2)配付の関与者
1)開発側：発送承認手続き、受領確認手続き、など
2)購入者：ダウンロード手順書、など
ex3)配送手段
1)物理的
セキュリティシール付きケースの運搬、封印付き封筒の郵送、など
2)電子的
署名付きファイルのダウンロード、など

4:ADO_DEL.2-1

配付証拠資料の記載事項(2)

2．開発したTOEと同一であることを判断するための方法・手段を記述する。

開発者が作成したTOEと同じものが購入者まで届けられるための開発側及び購入者での確認方法や技術的手段などを記述する。

ex）
1)開発サイト
製造番号と出荷票の比較、チェックサムの検証、など
2)購入者
TOEのヘルプ画面、CDラベルと納品書の比較、電子署名の検証など

4:ADO_DEL.2-2

配付証拠資料の記載事項(3)

3．開発者になりすまされないための手続き・手段を記述する。

TOE配付の関与者（開発者、代理店、配送業者など）になりすますことにより、不正な製品をTOEであると偽って配付することを防止または検出するための手続きや技術的な手段を記述する。

ex)
1)手続き的な手段
身分証明書の提示、署名・確認印付きの受領証の返送、など

2)技術的な手段
電子証明書付きの電子書名、など

4:ADO_DEL.2-3

留意点

- 配付証拠資料のとおりに配付が実施されているかどうか、作業者へのインタビュー、配付手続きの実演、記録の有無によって確認される。

4:ADO_DEL.2-4

設置、生成、及び立上げの目的

- 完成したTOEの状態から、開発者が意図したとおりに有効にセキュリティ機能が動作する状態にすること
- 設置/運用環境で購入者によって行われる場合だけでなく、その他の場所（開発サイトなど）で購入者以外（TOE開発者、TOE組み込み製品の開発者など）によって行われる場合も考慮すること

設置、生成、及び立上げ資料の記載事項

１．TOEのセキュリティ機能が有効に機能する状態にもっていくための方法を記述する。

TOEを適切な環境に設置し、適切な構成で配置し、適切な設定で立ち上げるための方法条件、手順、設定などを記述する。

4:ADO_IGS.1-1

・TOEが動作可能になるまでのすべての手順

・セキュリティに関わるパラメタの初期設定
ex) セキュリティ機能のON/OFFに関わる注意事項、など

・インストール失敗時の適切な対処・復旧手順

・設置環境に関する最小限のシステム要求事項
ex) TOE及びそのセキュリティ機能が動作するためのOS/DBへの設定、など

4:ADO_IGS.1-2

EALによる違い

■ EALによる違い

＜EAL1＞
・TOE が開発者の意図したようなセキュアな方法で、設置され、生成され、立上げする手順を記述する。

＜EAL2～3＞
・上記に加え、利用者サイトへ配送途中のTOEのセキュリティを維持するために必要なすべての手順を記述する。

＜EAL４＞
・上記に加え、 TOEのすり替えや改ざんを検出し、対処する方法を記述が必要となる。

構成管理

IPA

構成管理の目的

目的 = TOEとその構成要素の完全性を保証

1. TOEが正しい構成要素から正確に生成できることを保証する。
2. 許可されていない人物による構成要素の変更や、承認されていない内容への構成要素の変更を防止する。
3. 変更履歴を追跡して、変更ミスや不正な変更などを適切に復旧できるようにする。
4. 公開されるSTや認証報告書と照合することで、製品が認証済みであることを購入者が確認できるようにする。

評価の対象となる資料

- **構成リスト**
  TOEを生成するために必要な開発対象物件（ソースコード、マニュアル、仕様書・設計書など；以降、“構成要素”と呼ぶ）のリスト。TOEを生成するための正しいバージョンを特定できる必要があるため、構成要素は構成管理の対象にしなければならない。
- **構成管理証拠資料**
  構成管理の手続き・方法・手順を規定した社内基準・規定・ガイドライン（例えば、プロジェクト管理基準、開発作業規定、開発ガイドライン）などの総称。
- **構成要素の操作履歴**
  ソースコード変更などの構成要素に対する操作の記録。例えば、ツールのログ、変更要求指示書、作業報告書など。

構成管理に関わる用語

- **構成要素**
  TOEを生成するために作成・変更が必要な開発対象であり、構成管理の対象になる物件。例えば、ソースコード、マニュアル、仕様書・設計書、STなど。
- **ツール**
  構成管理下での開発作業（特にソースコードへのアクセス制御とTOEの自動生成）を支援するツール。

評価対象となる開発者作業

1. TOE名称・バージョン番号の表記
2. 構成リストの作成
3. 構成管理計画、受入れ計画の作成
4. 構成要素の操作の記録
5. ツールの使用

評価対象となる開発者作業

1. TOE名称・バージョン番号の表記
2. 構成リストの作成
3. 構成管理計画、受入れ計画の作成
4. 構成要素の操作の記録
5. ツールの使用

1. TOE名称・バージョン番号の表記

開発者は、調達者及び開発者が正しく認識できるように、曖昧さのないTOE名称とバージョン番号を決定し、表記しなければならない。

4:ACM_CAP.4-1

表記対象の物件

- 出荷時のTOE (消費者が受け取る形態)
  - ソフトウェアTOEのバージョン表示機能
  - ハードウェア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
  - 箱などのパッケージへの印字やラベル貼付
  - CD-ROMなどの記録媒体への印字やラベル貼付

4:ACM_CAP.4-2

- 構成リスト

4:ACM_CAP.4-1

TOE名称・バージョン番号の表記例

- 構成リスト上の記載例

IPA **ソフトウェア** Ver.2.0
開発文書リスト Ver.1.1
2005 **年** 2 **月** 1 **日**

構成要素名	バージョン番号	作成日
IPA ソフトウェア ST	1.8	2004.4.1
IPA ソフトウェア 機能仕様書	1.0	2004.6.1
IPA ソフトウェア 詳細設計書	1.0	2004.8.1
IPA ソフトウェア 利用者マニュアル	1.2	2005.2.1
IPA ソフトウェア 管理者マニュアル	1.1	2005.2.1
IPA ソフトウェア インストール手順書	1.1	2005.2.1
⋮	⋮	⋮

不適切なケース

- 後継製品や他製品との区別ができない場合

4:ACM_CAP.4-1

- 名称・バージョン番号とも記載されていても、購入者が正しく確認できない場合
  - 密封された筐体内に記載されており、筐体を破壊しないかぎり確認できない。
  - 名称とバージョン番号がセットで記載されていない。

4:ACM_CAP.4-2

留意点

- TOEの名称・バージョン番号は、ST記載のものと一致しなければならない。
  4:ACM_CAP.4-3
- 評価用（例えばテスト用）に提供するTOEも、その名称・バージョン番号が確認できなければならない。
  4:ACM_CAP.4-2
- 名称・バージョン番号の命名規則は、TOEの異なるバージョンを曖昧なく識別できるものでなければならない。
  4:ACM_CAP.4-1

評価対象となる開発者作業

1. TOE名称・バージョン番号の表記
2. 構成リストの作成
3. 構成管理計画、受入れ計画の作成
4. 構成要素の操作の記録
5. ツールの使用

2. 構成リストの作成

開発者は、TOEを作成するための構成要素を正確に特定できるように、構成要素の正しいバージョンのリストを作成しなければならない。

4:ACM_CAP.4-4　4:ACM_CAP.4-7　4:ACM_CAP.4-8

構成管理の対象となる物件

- TOEの実装表現（ソースコード、回路図、ハードウェア記述言語等）
- STに保証手段として定義した文書
  - マニュアル、取扱説明書など
  - 機能仕様書、設計書
  - テスト仕様書、他
- セキュリティ欠陥に関する報告書
  - 欠陥報告書の管理台帳など

4:ACM_CAP.4-8　4:ACM_SCP.2-1

構成リストに記載する情報

- 開発対象TOEの名称・バージョン番号

4:ACM_CAP.4-3

- 当該TOEに対応する各構成要素の名称・バージョン番号

4:ACM_CAP.4-7

構成リストの記述例

- 構成リストの記述例

IPA **ソフトウェア** Ver.2.0
開発文書リスト Ver.1.1
2005 **年** 2 **月** 1 **日**

構成要素名	バージョン番号	作成日
IPA ソフトウェア ST	1.8	2004.4.1
IPA ソフトウェア 機能仕様書	1.0	2004.6.1
IPA ソフトウェア 詳細設計書	1.0	2004.8.1
IPA ソフトウェア 利用者マニュアル	1.2	2005.2.1
IPA ソフトウェア 管理者マニュアル	1.1	2005.2.1
IPA ソフトウェア インストール手順書	1.1	2005.2.1
⋮	⋮	⋮

不適切なケース

- 構成要素のバージョンをユニークに特定できない場合
  - Ex.「XXX機能仕様書 2005年度版」
  - ただし“2005年度版”のような表現が常に間違いというわけではない。
    Ex.「開発作業規定 2005年度版」

4:ACM_CAP.4-7

- 明らかに構成管理が必要な構成要素が記載されていない場合
  - TOEの実装表現(ソースコード等)や同梱する文書(マニュアル等)などが構成リストに含まれていない

4:ACM_CAP.4-8 4:ACM_SCP.2-1

留意点

- 「構成リスト」として新たに文書を作成する必要はない。その手段は書類、電子ファイル、ツールの出力のいずれであってもよい。

4:ACM_CAP.4-4

- 構成リストの記載内容は、各構成要素そのものに記載される名称・バージョン番号と一致しなければならない。

4:ACM_CAP.4-10

- 名称・バージョン番号などの命名規則は、異なるバージョンを曖昧なく識別できるものであればよい。（作成日/更新日、タイムスタンプなども可）

4:ACM_CAP.4-7

評価対象となる開発者作業

1. TOE名称・バージョン番号の表記
2. 構成リストの作成
3. 構成管理計画、受入れ計画の作成
4. 構成要素の操作の記録
5. ツールの使用

3. 構成管理計画、受入れ計画の作成

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、これに従って開発を行わなければならない。

4:ACM_CAP.4-5 4:ACM_CAP.4-6

構成管理計画、受入れ計画の記載事項概要

① TOEバージョンの識別方法

② 構成管理の範囲と構成要素の識別方法

③ 構成要素の不正な操作を防止するための手続き・方法

④ 適正な構成要素からTOEを正しく生成するための手続き・方法

⑤ 構成要素の操作履歴として記録する項目

構成管理計画、受入れ計画の記載事項概要

① TOEバージョンの識別方法

② 構成管理の範囲と構成要素の識別方法

③ 構成要素の不正な操作を防止するための手続き・方法

④ 適正な構成要素からTOEを正しく生成するための手続き・方法

⑤ 構成要素の操作履歴として記録する項目

構成管理計画、受入れ計画の記載事項①

- TOEのバージョンの識別方法
  - TOEに付与するバージョン番号やリビジョン番号などの命名規則
    ⇒記述例(1)

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記述例(1)

- *TOEの識別方法*

IPAソフトウェアのリリース版は、対応するバージョン番号 m （m:1～）と、リリース版に対するアップデート番号 n (n:1～99) を使用して、「IPAソフトウェア Ver.m.n」の書式で表記する。

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記載事項概要

① TOEバージョンの識別方法

② 構成管理の範囲と構成要素の識別方法

③ 構成要素の不正な操作を防止するための手続き・方法

④ 適正な構成要素からTOEを正しく生成するための手続き・方法

⑤ 構成要素の操作履歴として記録する項目

構成管理計画、受入れ計画の記載事項②

■ 構成管理の範囲と構成要素の識別方法

□ 管理対象の構成要素
⇒記述例(2-1)

□ 構成要素のバージョンの命名規則
⇒記述例(2-2)

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記述例(2-1)

- ***構成管理の範囲***

本製品では、バージョン管理ツールＣＶＳを使用して、以下の構成要素を管理する。

・ソースコード
・機能仕様書及び設計書
・取扱説明書
・テスト仕様書及びテスト結果
・・・（略）・・・

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記述例(2-2)

- ***構成要素の識別方法***

(1)ソースコード
ソースファイルのパス・ファイル名と、ＣＶＳが各ファイルに付与するバージョン番号により識別する。バージョン番号は”m.n”(m:0～9, n:01～99)の形式でＣＶＳが自動的に付与し、その初期値は“0.01”とする。

(2) 機能仕様書及び設計書
・・・（略）・・・

(3)取扱説明書
・・・（略）・・・

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記載事項概要

① TOEバージョンの識別方法

② 構成管理の範囲と構成要素のバージョンの識別方法

③ 構成要素の不正な操作を防止するための手続き・方法

④ 適正な構成要素からTOEを正しく生成するための手続き・方法

⑤ 構成要素の操作記録として記録する項目の定義

構成管理計画、受入れ計画の記載事項③

- **構成要素に対する不正な操作を防止する手続き・方法**
  - 関係者の役割、権限、責任などの定義
    ⇒記述例(3-1)
  - 構成要素の変更手続き
    ⇒記述例(3-2)
  - 構成要素の受入れ手続き
    ⇒記述例(3-3)
  - 構成要素に対する変更を制御する方法
    ツールを使用する場合は、使用する機能、適用範囲、及びその操作方法・手順を含める
    ⇒記述例(3-4)

4:ACM_CAP.4-11 4:ACM_CAP.4-15 4:ACM_CAP.4-18

構成管理計画、受入れ計画の記述例(3-1)

- *関係者の役割・権限*

本プロジェクトは、仕様書やマニュアルなどの文書を作成する設計グループと、これらの文書に従ってソースコードを編集する開発グループで構成される。各グループは、それぞれ実作業を担当する設計者、プログラマで構成される。

・・・（略）・・・

各構成要素を作成する設計者またはプログラマ（担当者）は、各グループリーダ（GL）が決定する。GLと担当者は構成要素に対する閲覧権限を持つ。GLはグループが担当する構成要素を追加・変更する権限を持ち、担当する構成要素が受け入れ基準を満たしていることを保証する責任を持つ。

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記述例(3-2)

- *構成要素の変更手続き*

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）・・・

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記述例(3-3)

- ***構成要素の受入れ手続き***

(1) 受入れテスト

受入れの対象となる要素がソフトウェアまたはハードウェアを含む場合、要求仕様を満たすかどうかのテストを行い、テスト報告書(様式xx)を作成する。

(2) 受入れレビュー

受入れの対象となる要素がxxxに示す基準を満たすことを確認するために、以下の責任者の元にレビューを実施する。

機能仕様、上位レベル設計、プロジェクト外からの要素の場合・・・PL

下位レベル設計、ソースコードの場合・・GL

・・・（略）・・・

4:ACM_CAP.4-18

構成管理計画、受入れ計画の記述例(3-4)

- ***構成要素のアクセス制御***

(1)ソースコード

アクセス制御リスト(ACL)にユーザIDが登録された担当者のみが、CVSによってソースコードの閲覧・変更を許可される。なお、ACLの変更、ソースコードの新規追加及び削除は、GLにのみ許可される。

・・・（略）・・・

(2)文書

・・・（略）・・・

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記載事項概要

① TOEバージョンの識別方法

② 構成管理の範囲と構成要素の識別方法

③ 構成要素の不正な操作を防止するための手続き・方法

④ 適正な構成要素からTOEを正しく生成するための手続き・方法

⑤ 構成要素の操作履歴として記録する項目

構成管理計画、受入れ計画の記載事項④

- 適正な構成要素からTOEを生成するための手続き・方法
  - 正しいバージョンの構成要素を過不足なく使用していることを保証する方法
    ⇒記述例(4-1)
  - 変更後の構成要素が適正であることを判断するための手続き・基準
    ⇒記述例(4-2)
  - TOEを正しく生成するための手順
    ツールを使用する場合は、使用する機能、適用範囲、及びその操作方法・手順を含める
    ⇒記述例(4-1)

4:ACM_CAP.4-16 4:ACM_CAP.4-17

構成管理計画、受入れ計画の記述例(4-1)

- TOEの生成方法・手順

GNU “make”ツールと “make”の動作（TOE生成オプションを含む）を定義する “Makefile”を使用して、ソースコードからTOEを生成する。なお、この”Makefile”は、ソースコードとともにCVSによって構成管理する。

① ソースコード最新版一式をCVSレポジトリXXXから取り出す (cvs checkout を実行する)。
② ソースコード格納ディレクトリ(/xxx/main/src/)に移動する(cd /xxx/main/src/を実行する)。
③ 表-3を参照して、“ Makefile ”記載のTOE生成オプションが正しいことを確認する。
④ make clean 及び make を実行する。

4:ACM_CAP.4-16 4:ACM_CAP.4-17

構成管理計画、受入れ計画の記述例(4-2)

- TOEの生成手続き

TOEを生成するにあたり、以下の作業を順番に実施する。

① 開発グループGLは、変更要求記録簿、各担当者の作業報告書、及びCVSのログを照らし合わせ、要求どおりにソースコードが変更が実施されたことを確認する。

② 開発グループGLはTOE生成作業指示書兼報告書を作成し、TOE生成の担当者にそれを渡して、TOE生成を指示する。

③ TOE生成の担当者は、 TOE生成作業指示書兼報告書及びTOEの生成方法・手順（3.2節）に従ってTOEを生成する。

④ ・・・（略）・・・

4:ACM_CAP.4-16 4:ACM_CAP.4-17

構成管理計画、受入れ計画の記載事項概要

① TOEバージョンの識別方法

② 構成管理の範囲と構成要素の識別方法

③ 構成要素の不正な操作を防止するための手続き・方法

④ 適正な構成要素からTOEを正しく生成するための手続き・方法

⑤ 構成要素の操作履歴として記録する項目

構成管理計画、受入れ計画の記載事項⑤

- **操作履歴として記録する項目**
  ⇒記述例(5)

  - 操作履歴の形態
    変更指示書、ツールのログ、作業報告書など

  - 記録する項目
    変更ミスなどの早期発見や発見時の適切な復旧に有益な情報
    - 操作の種別（変更、追加など）
    - 変更内容、変更日時
    - 変更を実施した開発者、指示/承認した責任者
    - 変更の影響を受ける構成要素、など

4:ACM_CAP.4-11

構成管理計画、受入れ計画の記述例(5)

- ***構成要素の変更手続き***

・・・（略）・・・

レビューに際しては、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。

・・・（略）・・・

4:ACM_CAP.4-11

留意点

- 「構成管理計画、受入れ計画」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。

4:ACM_CAP.4-4～6

- 関係者は、構成管理計画、受入れ計画の内容（特に各自の関係部分）を理解し、その内容に従って実際に構成管理を実施していなければならない。

- 開発者が構成管理計画、受入れ計画に従って開発したことが、開発者へのインタビューと操作記録（後述）の検査によって確認される。

4:ACM_CAP.4-13 4:ACM_CAP.4-14

評価対象となる開発者作業

1. TOE名称・バージョン番号の表記
2. 構成リストの作成
3. 構成管理計画、受入れ計画の作成
4. 構成要素の操作の記録
5. ツールの使用

4. 構成要素の操作の記録

開発者は、開発中に行われた構成要素の変更履歴を記録しなければならない。

4:ACM_CAP.4-12

留意点

- 操作履歴の形態及び内容は、構成管理証拠資料の内容と一貫していなければならない。
  4:ACM_CAP.4-13
- 操作履歴は適切に保管されており、許可された人物がいつでも確認できる状態でなければならない。
  4:ACM_CAP.4-13
- 操作履歴は、構成管理証拠資料のとおりに構成管理が実施されたことの証拠にもなる。
  4:ACM_CAP.4-13
- 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、開発者へのインタビュー、構成管理の実演、操作履歴の有無によって確認される。
  4:ACM_CAP.4-13

評価対象となる開発者作業

1. TOE名称・バージョン番号の表記
2. 構成リストの作成
3. 構成管理計画、受入れ計画の作成
4. 構成要素の操作の記録
5. ツールの使用

5. ツールの使用

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

（EAL4以上の評価で必須）

4:ACM_AUT.1-1 4:ACM_AUT.1-3

ツールの使用例

- **ソースコードの変更管理(アクセス制御)**
  - ファイルサーバのOSが備えるログイン機能及びアクセス制御機能
  - 市販あるいは開発者独自の構成管理ツールの識別・認証機能及びアクセス制御機能

4:ACM_AUT.1-2

- **TOE生成の自動化**
  - GNU “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

4:ACM_AUT.1-4

ツール使用時の注意事項

- **ツール使用をバイパスする方法がないこと**
  - ファイルサーバ上のソースコードへのリモートアクセスをツールを使用して制御していても、ファイルサーバのコンソールからログインした人物なら誰でもアクセスが可能ならば、構成管理としては不十分である

    4:ACM_AUT.1-2

- **TOEを正しく生成するための条件が適切に維持されていること**
  - TOEを正しく生成するための条件（ソースコード一覧とコンパイルオプション、装置の動作設定など）が適正なものに維持されなければ、間違ったTOEが自動生成される

    4:ACM_AUT.1-4

留意点

- 少なくともソースコードの変更管理(アクセス制御)とTOE生成の自動化にツールを使用する必要がある。

  4:ACM_AUT.1-1 4:ACM_AUT.1-3
- ツールの機能・操作方法は、構成管理証拠資料の内容と一貫していなければならない。

  4:ACM_AUT.1-2 4:ACM_AUT.1-4
- どのツールを使用するのか明確に定められていて、開発者は、構成管理証拠資料に記載された操作方法・手順に従って、ツールを操作できなければならない。

  4:ACM_AUT.1-5 4:ACM_AUT.1-6
- 開発者が実際にツールを使用して開発したことが、開発者へのインタビュー、ツールの使用デモ、操作履歴の有無によって確認される。

  4:ACM_AUT.1-7

EALによる違い

- **EAL1**
  TOEの名称・バージョン番号が調達者にわかるようにする。
- **EAL2**
  構成管理が必要な構成要素を決定して、その名称・バージョン番号を明文化する。
- **EAL3**
  TOEのすべての構成要素を構成管理し、それらに対する不正な変更を防止する手続きを規定・実施する。
- **EAL4**
  セキュリティ欠陥に関する報告書を構成要素に加える。適正な構成要素からTOEを正しく生成するための手続きを規定・実施する。ソースコードのアクセス制御とTOEの自動生成を支援するツールを使用する。

ライフサイクルサポート

ライフサイクルサポートの評価

- 開発から保守までの開発サイクル全体を通して、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。

- 次の３つの側面について保証する。
  - 開発工程全体の管理
  - 開発ツールの信頼性
  - 開発環境のセキュリティ

評価に必要な証拠資料

- ライフサイクル定義証拠資料

- 開発ツール証拠資料

- 開発セキュリティ証拠資料

１．ライフサイクル定義

目的

- 開発工程全体が適切に管理されることにより、各種開発ドキュメントやTOEが適切に作成されたことの保証を高める
- 開発から保守までの各フェーズで使用する開発手続きや開発方法などを明確に規定し、規定されたとおりに実施する。
- 規定どおりに実施することにより、TOEにセキュリティ上の欠陥が入り込む可能性を小さくする。

ライフサイクル定義証拠資料の記載事項

- 開発から保守までの全工程・フェーズ
- 各フェーズで実施する開発手続き
  - 開発体制
    組織構成/プロジェクト体制、各フェーズの責任者や担当部署/担当者、開発場所など
  - 各種の管理方法・手続き
    要員管理や工程管理の方法、設計・レビュー・実装・テスト・バグ修正などの各フェーズや各フェーズ間で採用される作業管理上の手続きなど
- 各フェーズで使用する開発技法・ツール
  - 各種技法・ツール
    設計、実装、テスト、バグ修正などの実施方法・実施手順、各作業を支援するツールなど

4:ALC_LCD.1-1

留意点

- 「ライフサイクル定義証拠資料」なる文書を新たに作成する必要はない。
  該当する情報を記載した文書類があれば、それらをライフサイクル定義の評価証拠として提出すればよい。

  4:ALC_LCD.1-1

- 開発・保守工程のすべてのフェーズを網羅するように定義していること

  ⇒詳細過ぎるフェーズの定義は不要

  4:ALC_LCD.1-1

- 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

  ⇒適切に作業が行われない、TOEの品質が落ちる、TOEや開発ドキュメントを紛失するなど、開発全般における悪影響を除去/軽減する効果があること

  4:ALC_LCD.1-2

２．ツール及び技法

目的

- 信頼できるツールや技術が開発に使用されることにより、TOE(セキュリティ機能)が一貫した品質で適切に作成されたことの保証を高める

- 開発に使用する開発ツール・技術が明確に定義されていること
- 開発ツール・技術を使用した作業結果の品質が一貫したものであること

開発ツール証拠資料の記載事項

- 実装表現の文法・構文
  - 実装表現の文法・構文の定義
  - 実装表現の意味を曖昧さなく解釈できる文法・構文

  ⇒開発者向け技術資料（プログラミング言語仕様など）などの提示
  ⇒ツールが準拠している公認の標準（ISO標準など）の明示

  4:ALC_TAT.1-2
- 開発ツールの使用方法
  - ツールの操作方法の明確な説明
  - 実行オプションなどによるツール動作の違いの説明
  - 生成されるTOEに影響する使用法
    コンパイルオプションの定義、など

  ⇒上記を説明する利用者マニュアルなどの提示

  4:ALC_TAT.1-3

留意点

- 「ライフサイクル定義証拠資料」の開発ツール・技法の定義として、ツール名・バージョン、開発元、準拠する標準名などツール・技法を特定できる情報を明示した上で、
  「開発ツール証拠資料」として、そのツール・技法に関連するマニュアル、技術資料、標準文書などを提出すればよい。

- ツールが広く知られた標準(ISOなど)に準拠し、その標準を記載した文書を評価者が入手できるなら、ツール名や標準名などの提示だけでもよい。
- ただし、標準に準拠していない部分（追加部分など）がある場合、標準との相違がわかる文書が必要。

  4:ALC_TAT.1-1

３．開発セキュリティ

目的

- 開発環境に対して適切なセキュリティ対策を実施することにより、TOE(セキュリティ機能)の設計・実装時に改ざんや漏洩が発生しないことを保証する

開発セキュリティ証拠資料の記載事項

- 開発環境のセキュリティ方針
  - TOEの開発に関連する保護すべき資材
    開発ドキュメント、開発ツール、テストツール、TOEなど
  - 保護対象の資材への許可される/許可されないアクセス
    アクセス権限を持つ開発要員、許可される権限の種類など

4:ALC_DVS.1-2

- 開発環境のセキュリティ対策
  開発環境のセキュリティ方針を達成するための具体的なセキュリティ対策・手段
  - 物理的な側面
  - 手続き的な側面
  - 人的な側面
  - その他の側面
    （論理的な側面；構成管理下のアクセス制御など）

4:ALC_DVS.1-1

セキュリティ手段の例(1/3)

開発セキュリティ証拠	実施項目	セキュリティ対策・手段	備考
建屋管理	開発環境の物理的管理	・建屋の保安（訪問者の扱い等）	物理的、手続き的
開発ルーム		・非開発要員の立ち入り制限 ・部屋の施錠管理 ・入室管理	物理的、手続き的
従業員管理	開発要員管理	・従業員就業規則の履行（不正行為の禁止など）	人的
情報保護教育		・設計情報、機密情報の取扱い	人的
開発要員管理		・開発プロジェクト員の構成、責任者の明示 ・守秘義務履行の確認	手続き的

セキュリティ手段の例(2/3)

開発セキュリティ証拠	実施項目	セキュリティ対策・手段	備考
開発管理	データ、情報の管理	・一般の開発とTOEの管理区分の明示	手続き的
物理的対策		・ネットワークの分離	物理的
コンピュータアクセス管理		・アクセス権付与、取り消し ・パスワード管理 ・アクセス記録 ・電子媒体の取り扱い	物理的、手続き的、人的

セキュリティ手段の例(3/3)

開発セキュリティ証拠	実施項目	セキュリティ対策・手段	備考
コンピュータウイルス	データ、情報の管理	・ウイルス検疫、駆除 ・ウイルスパターンファイル更新	物理的、人的
設計情報管理		・設計情報の保管・維持	手続き的
データバックアップ		・データバックアップ	物理的、人的
開発委託		・開発委託先セキュリティ管理	物理的、人的、手続き的
ネットワーク管理	ネットワーク管理	・ネットワーク接続の登録 ・外部ネットとの接続制限	手続き的、その他
機器構成管理	開発機器管理	・開発構成機器の登録、管理	手続き的、その他

留意点

- 明文化された各セキュリティ対策はすべて開発環境において実施されていること
  （評価者により以下が行われる）
  - 記録（入退出記録、監査ログなど）の確認
  - 開発サイトの施設・設備の確認
  - 開発要員へのインタビュー

  4:ALC_DVS.1-3　4:ALC_DVS.1-4
- 開発環境のセキュリティ方針は妥当であること
  特に、保護すべき資材に不足がないこと
- 開発環境のセキュリティ対策は、セキュリティ方針と一貫しており、かつそのすべてをカバーしていること

  4:ALC_DVS.1-2

ＥＡＬによる違い

- ＥＡＬ１： 評価されない
- ＥＡＬ２： 同上
- ＥＡＬ３： *開発セキュリティ*
- ＥＡＬ４： 開発セキュリティ、
  ライフサイクル定義、開発ツール

脆弱性評定

1．脆弱性

脆弱性とは？

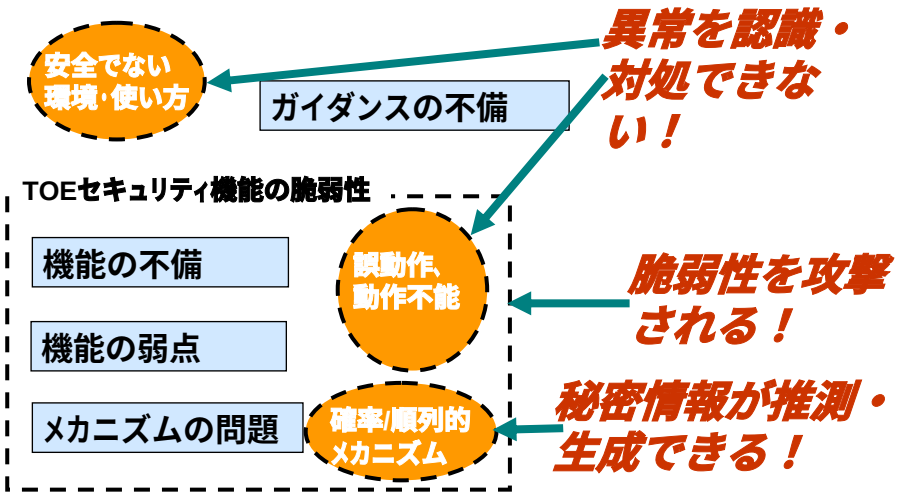
TOEのセキュリティ機能の正常な(STの通りの)動作を妨げるTOEの弱点。

- ガイダンスの不備
- 機能の不備 (設計・実装の誤り)
- 機能の弱点 (論理的・物理的な制約)
- メカニズムの問題

などがある。

脆弱性評定

脆弱性評定とは？



脆弱性評定

異常を認識・対処できない！

TOEの誤使用や設定を誤る危険性の最小化

TOEが安全に動作していないことを認識・対処できない危険性を最小にする。「**誤使用分析書**」を作成する。

脆弱性を攻撃される！

脆弱性の分析

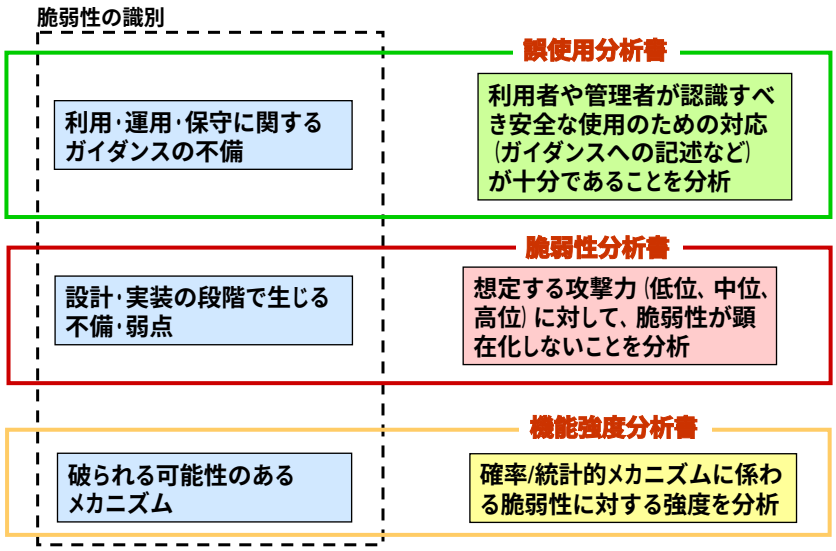
TOEのセキュリティ機能に係わる脆弱性の存在を確かめ、TOEが意図する環境において悪用されないこと、明白な侵入攻撃に対抗できることを検証する。「**脆弱性分析書**」を作成する。

秘密情報が生成できる！

確率的・順列的メカニズムが破られる危険性の分析

確率的・順列的メカニズムの強度が、STに定義された最小強度レベルと同等以上であることを検証する。
「**機能強度分析書**」を作成する。

脆弱性評定で開発者が作成する分析書



２．脆弱性分析書の作成（AVA_VLA）

目的

TOEのセキュリティ機能を侵害する脆弱性を分析する。

識別された脆弱性に関して、明白な侵入攻撃に耐えうることを検証する。

明白な侵入攻撃：TOEに関する最小限の理解、技能、技術、資源によって可能な攻撃

脆弱性の識別

情報源
- 製造に係わった資材（設計書、テスト、など）
- 脆弱性情報データベース
- 一般情報（Internet、書籍・雑誌等）

TOEのすべてのセキュリティ機能に対して、脆弱性を識別する。

4:AVA_VLA.2-1　4:AVA_VLA.2-2

脆弱性事例(1)　ガイダンス

【脆弱性の内容】

前提条件が正確に運用者や利用者に伝わらないため、セキュリティが確保されない環境でTOEが動作する。

【攻撃方法】

前提条件が満足されない環境でTOEを使用し、保護資産を不正に利用する。

【対策】

前提条件を正確にガイダンス文書に記載し、運用者や利用者に認識させる。（「xxの条件を満足しないと、セキュリティが確保されない。」と記載する。多数の注意書きの中に、単に「xxすること。」と記載しただけでは、その重要性を読者は認識できないことがある。）

脆弱性事例(2)　設計・実装

【脆弱性の内容】

TOEの想定する運用環境では、前提条件を満足させるには無理があり、セキュリティが確保されない環境で、TOEが動作する。（製品によっては、利用者がガイダンス文書を読まないで、機能を使用する場合がある。）

【攻撃方法】

前提条件が満足されない環境でTOEを使用し、保護資産を不正に利用する。

【対策】

前提条件が満たされていなければ、TOEの処理を中断して、警告メッセージを表示する。

脆弱性事例(3)　設計・実装

【脆弱性の内容】

エラー処理（ハード障害、他機能からのエラーリターン、操作ミス、入力パラメタのミス、暗号秘密鍵の取得/参照不可、などへの対処）の不備で、セキュリティ機能が動作不能になる。

【攻撃方法】

誤操作、異常なパラメタ値の設定、ハード障害などを誘発し、セキュリティ機能を動作不能にして、保護資産を不正に利用する。

【対策】

エラーによって、セキュリティ機能の正常な動作が不可ならば、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。

脆弱性事例(4)　設計・実装

【脆弱性の内容】

不正利用に係わる警告メッセージを表示しても、知見されないため、セキュリティが確保されない環境で、必要な対処がなされないまま、TOEの処理を継続する。

【攻撃方法】

不正アクセスが検知されないので、不正な利用を継続する。

【対策】

警告のためのメッセージが、関係者に認識されたことを確認する処理を、TOEに組み込む。確認された後に、TOEの処理を継続する。

脆弱性事例(5)　設計・実装

【脆弱性の内容】

メッセージのテキストに、秘密情報（パスワードなど）の推測、セキュリティ属性（役割、権限、グループIDなど）の暴露、攻撃対象（ファイル名称、所有者、当該製品やオペレーティングシステムの識別情報など）の識別などを容易にする情報が含まれている。

【攻撃方法】

テキストの内容を手がかりに秘密情報の推測、セキュリティ属性の把握、攻撃対象の特定を行い、保護資産を不正に利用する。

【対策】

- 関連者の行為に不必要な情報は、表示(通知）しない。
- メッセージテキストには、攻撃者にとって有益な情報を含めない。

脆弱性事例(6)　設計・実装

【脆弱性の内容】

セキュリティ機能をバイパス/非稼動にできる操作が存在する。

【攻撃方法】

- セキュリティ機能をバイパス/非稼動にする操作をした後、保護資産を不正に利用する。
- 権限付与者による当該操作を誘発（ソーシャルエンジニアリングなど）し、保護資産を不正に利用する。

【対策】

- セキュリティ機能のバイパス/非稼動にする操作の実施は、権限付与者に制限する。
- セキュリティ機能のバイパス/非稼動操作時には、当該操作の再確認（誤操作でないことの確認）を行なう。

脆弱性事例(7)　設計・実装

【脆弱性の内容】

利用者が直接、クライアントを操作する場合には、利用者の認証を行っているが、関連のサーバからAPIで呼ばれた場合は、利用者の認証は行なっていない。

【攻撃方法】

不正なクライアントから、関連サーバ経由で、TOEを利用し（認証なしで）、保護資産を不正に利用する。

【対策】

API経由でもクライアントの認証を行う。

脆弱性事例(8)　設計・実装

【脆弱性の内容】

セキュリティ属性値（アクセス権限、フィルタリングルール、など）のデフォルト値が不適切であるため、セキュリティ機能が有効に動作しない。

【攻撃方法】

製品の導入直後（デフォルト値が適用）に、保護資産を不正に利用する。

【対策】

セキュリティ属性値のデフォルトを、TOEが安全サイドで機能するように設定する。

脆弱性事例(9)　設計・実装

【脆弱性の内容】

TOEの機能上、必要でない情報資産が利用できる。
（機能の処理内容から見て、情報資産の利用単位/範囲が不適切。）

【攻撃方法】

アクセス権限の範囲で得た保護資産を暴露する。

【対策】

アクセスできる情報の単位を、TOEの個々の処理で必要最小限のものにする。

脆弱性事例(10)　設計・実装

【脆弱性の内容】

TOEの管理ファイル（アクセス規則、登録利用者のIPアドレス、通信データあて先アドレス、セキュリティ機能管理データ、などが格納）が置換あるいは、データが変更された場合でも、TOEはその管理データに基いて実行する。

【攻撃方法】

- TOEの管理ファイルを偽造し、保護資産を不正に利用する。
- TOEの管理データを改ざんし、保護資産を不正に利用する。

【対策】

- TOE管理ファイルの更新権限を、権限付与者に制限する。
- TOE管理ファイル（あるいは、データ）の改ざん検出を行う。

脆弱性事例(１１)　設計・実装

【脆弱性の内容】

大量のログデータが一度に採取されるため（監査ログとメッセージーログの共用などによる）、有用なログデータをタイムリーに検出することは困難である。

【攻撃方法】

APIを利用して、大量のダミーメッセージを発生させ、不正アクセスの検出を困難にする。

【対策】

監査データのロギング機能は専用とする。

脆弱性事例(１２)　設計・実装

【脆弱性の内容】

TOEの保護資産を利用できる非公開のインタフェースが存在している

【攻撃方法】

非公開のインタフェースを使用して、保護資産を不正に利用する。

【対策】

利用者（当該インタフェース公開対象プログラム）の認証を行う。

脆弱性事例(13)　メカニズム

【脆弱性の内容】

確率や統計的な手法で秘密情報（例えば、パスワード）を生成している場合、同じ手法によって、同じ秘密情報を生成することができる。

【攻撃方法】

TOEが使用している手法（文字の組み合わせなど）で、秘密情報を生成する。

【対策】

秘密情報の生成が、実時間内には困難となるような生成規則を導入する。

脆弱性事例(14)　設計・実装

【脆弱性の内容】

物理的な干渉によって、TOEの処理回路を変更したり、参照したりできる。

【攻撃方法】

- 配線加工装置などを使用して処理回路を改ざんし、セキュリティ機能を無効にする。
- 物理的プロービング（探針）により、処理回路を暴露して、同等の機器を偽造する。
- 電子顕微鏡などで回路構成を解析し、機器を偽造する。
- 機器の樹脂や絶縁膜を除去して、回路構成を暴露して、機器を偽造する。

【対策】

- 探針検出機能を装備する。
- 改ざん検出機能を装備する。
- 物理的ストレスの検知機能を装備する。

脆弱性事例(15)　設計・実装

【脆弱性の内容】

TOEのエラー処理（ハード障害、タイムアウト、他モジュールからのエラーリターン、管理情報の破壊、異常な入力データ、バッファオーバフロー、暗号秘密鍵参照エラー、不正な再送、などへの対処）の不備で、セキュリティ機能が動作不能になる。

【攻撃方法】

エラーの発生を誘発し、セキュリティ機能を動作不能にして、保護資産を不正に利用する。

【対策】

エラーによって、セキュリティ機能の正常な動作が不可ならば、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。

脆弱性事例(16)　設計・実装

【脆弱性の内容】

監査ログデータ用のバッファがオーバフローした際、以前の記録データを上書きして、消してしまう。

【攻撃方法】

保護資産を不正に利用した後、ダミーのアクセスを大量に行って、不正利用の痕跡を消す。

【対策】

- バッファがオーバフローする以前に、システム運用者に通知する。
- バッファがオーバフローした場合には、情報資産へのアクセスを中止する。

脆弱性事例(１７)　ガイダンス(保守)

【脆弱性の内容】

追加の機能やパッチを、保護しないで利用者に配付している。

【攻撃方法】

不正プログラムを、追加機能やパッチとして配布し、保護資産を不正に利用する。

【対策】

追加機能やパッチに電子署名を添付し、適用側で検証する。

脆弱性事例(１８)　ガイダンス(運用)

【脆弱性の内容】

セキュリティ機能が動作するために必要な資源が枯渇すると、そのタイムリーな動作が保証できなくなる。

【攻撃方法】

Ｄｏｓ攻撃

【対策】

- セキュリティ機能の動作に必要な資源（各種のバッファ領域など）は、動作環境に応じて、必要な量を確保できるようにしておく。
- 枯渇した場合には、TOEの処理を安全サイド（保護資産の利用は禁止など）で行う。

脆弱性の分類と対処

識別したすべての脆弱性

明白な脆弱性

TOEの公開外部インタフェース(＊)を使用すれば、顕在化する脆弱性

(例：特定のタイミングの操作、仕様の範囲ではないパラメータ指定、など)

TOEの公開外部インタフェースを使用しただけでは顕在化しない脆弱性

セキュリティ対策や前提によって対処していることを検証

TOEの公開外部インタフェースを駆使した攻撃では顕在化しないことを検証

＊：インターネットなどで流通/公開されているもので、簡易に使用できる攻撃方法も含める

4:AVA_VLA.2-2

脆弱性分析書

分析の過程を記載する。
- 分析の対象となる資料と分析作業の内容

識別された脆弱性を記載する。
- 脆弱性の内容（関連するTOEセキュリティ機能の識別を含む）
- 脆弱性の分類（明白な脆弱性か、残存する脆弱性か）
- 検出の情報源と検出に係わった作業
- 関連する脅威（関連する攻撃方法と侵害される保護資産）

明白な脆弱性に対しては、前提条件、または、TOEのセキュリティ対策によって対処していることを検証し、その結果を記載する。

この対処は、STと矛盾せず、適切なガイダンスが提供されていなければならないことに注意。

他の脆弱性（残存脆弱性）に対しては、TOEの公開外部インタフェースを駆使した攻撃（低レベルの攻撃）では、顕在化しないことを検証し、その結果を記載する。

4:AVA_VLA.2-2　4:AVA_VLA.2-3

評価者の分析

侵入テスト

開発者の分析に疑わしい点があるが大丈夫？
開発者が考慮していない視点があるが大丈夫？
独立脆弱性分析で脆弱性の疑いを見つけたが大丈夫？

4:AVA_VLA.2-4～8　4:AVA_VLA.2-10～14

独立脆弱性分析

評価者も欠陥仮定法などで独自に分析を行う。

4:AVA_VLA.2-9

脆弱性のまとめ

開発者と評価者の分析を総合して、低レベルの攻撃に耐えられることを示す。

4:AVA_VLA.2-15　4:AVA_VLA.2-16

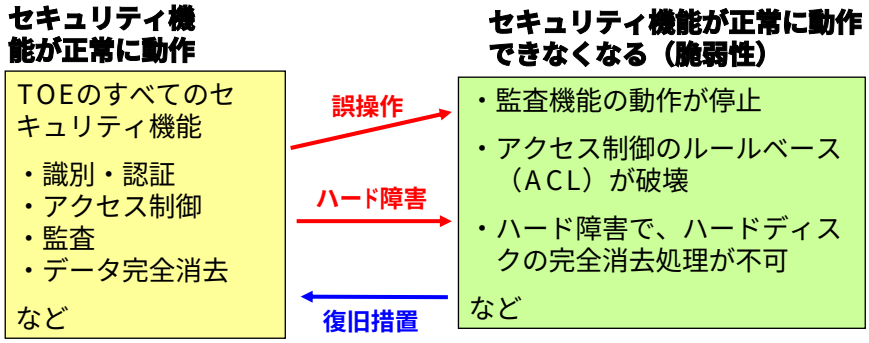
３．誤使用分析書の作成

目的

TOEの運用管理者や利用者向けのガイダンス文書に必要十分な事項が記載されていることを、誤使用に対する分析により、実証する。

注）ガイダンス文書の作成については、ガイダンス文書(AGD)・配付と運用(ADO)クラスを参照。

誤使用分析



TOEのすべてのセキュリティ機能に対して、下記を分析して、誤使用分析書に記載する。

- セキュリティ機能が正常に動作できなくなる脆弱性の識別
- 脆弱性が顕在化する条件（誤操作，ハード障害など）
- 復旧措置

4:AVA_MSU.2-6

ガイダンス文書への記載

TOEの全てのセキュリティ機能の動作に関して、運用管理者や利用者が認識できなければならない事項を、ガイダンス文書に明記する。

正常な動作、あるいは、異常な動作状態にあることを認識（検知）できる。
4:AVA_MSU.2-9

異常な動作状態から正常な動作に復旧できる。
4:AVA_MSU.2-1

セキュリティ機能の仕様とすべての操作を理解できる。
4:AVA_MSU.2-1 4:AVA_MSU.2-2

セキュリティ機能の構成、導入、起動手順を理解できる。
4:AVA_MSU.2-7 4:AVA_MSU.2-8 4:AVA_MSU.2-2

TOE動作のすべての前提条件や環境に係わるセキュリティ対策（物理対策、管理対策など）を理解できる。
4:AVA_MSU.2-4 4:AVA_MSU.2-5 4:AVA_MSU.2-2

操作方法、操作の内容、操作に伴うレスポンス（表示メッセージなど）や確認方法を記載する。

留意点

- すべてのセキュリティ機能の管理・使用法についてガイダンスに記載されること。
- ガイダンスに記載される管理・使用法は、対象の者が**無理なく**実行できること。

4:AVA_MSU.2-3

誤使用分析書

- 誤使用の分析結果
- 誤使用の分析結果にもとづいて、TOEの運用管理者や利用者が認識しなければならない事項はすべて、正確に、漏れなく、明確にガイダンス文書に記載されていることを検証

4:AVA_MSU.2-6 4:AVA_MSU.2-10

4．機能強度分析書の作成

目的

STにおいて、TOEセキュリティ機能強度を主張するものとして識別された各メカニズム(*)に対し、そのセキュリティ機能強度分析を行う。

*例えばパスワードによる認証機能など

機能強度分析の対象

- STの中で識別された確率・順列的メカニズム
- STに提示された強度を備えているかどうか
  - SOF-basic　低レベルの攻撃力に対抗
  - SOF-medium　中レベルの攻撃力に対抗
  - SOF-high　高レベルの攻撃力に対抗
- 確率・順列的メカニズムをTOEが持たない場合、機能強度分析は不要。
- 制度で使用の認められた暗号アルゴリズムが認められた方法で使用される場合は評価の対象外。

4:AVA_SOF.1-1　4:AVA_SOF.1-2

機能強度分析書に記載する情報

- STで識別されたメカニズム名
- 識別された各メカニズムの機能強度の十分性を定量的に分析した結果

4:AVA_SOF.1-3〜6

機能強度の分析(1)

◆以下の表を目安に機能強度を定量分析する。

対抗できる攻撃力の数値目標

＜10	レートなし
10－17	低
18－24	中
＞25	高

★例えば、各分類の合計値が15ならば、低レベルの攻撃には対抗できる
→SOF-basicに相当

攻撃能力の評定表（表の一部）

分類	条件	脆弱性の識別	脆弱性の悪用
所要時間	0.5H〜1日	2	3
	一ヶ月以内	3	5
攻撃者のレベル	熟達者	2	2
	専門家	5	4
攻撃に必要なTOEの知識	公開情報で可	2	2
	秘密情報必要	5	4
TOEアクセス時間	0.5H〜1日	2	4
	一ヶ月以内	3	6
攻撃の道具	汎用ツール	1	2
	専門ツール	3	4

CEM パート2 バージョン1.0 表B.3から抜粋

4:AVA_SOF.1-5

機能強度の分析(2)

計算表の解説

- **脆弱性の識別**
  脆弱性を見つけること。
- **脆弱性の悪用**
  識別した脆弱性を利用して攻撃（悪用）すること。
- **所要時間**
  脆弱性を識別、悪用するために必要な時間
- **TOEアクセス時間**
  脆弱性を識別、悪用するために、TOEを動作させる必要がある場合のそれぞれの時間。

4:AVA_SOF.1-5

機能強度の分析例(１)

PINによる認証メカニズムの場合

＜条件の例＞

・PINは、4桁以上の０～９までの数字
・連続した数字（0000等）は使用不可
・１回の入力に５秒かかる。
・３回入力を間違えたら１０分間ロックする
・TOEの知識なしに攻撃可能
・TOEを攻撃するのにツールは使えない
・・・

機能強度の分析例(2)

PINによる認証メカニズムの場合

＜検証方法の例＞

パスワードの空間のワーストケースを算出
　パスワードが４桁のとき、10^4=10,000（通り）
　連続する数字（0000、1111）＝１０通り
　10,000－10　＝9990
パスワードが合致するまでの試行回数の平均値
　9990/2　＝4995 回
4995回の試行をするのに必要な時間
　（計算略）　約１１日

以上より、
悪用するための所要時間は、最短でも約11日程度が必要。

機能強度の分析例(3)

評定表により、攻撃能力を計算する。

攻撃能力の評定表及び評定結果例

分類	条件	脆弱性の識別	脆弱性の悪用
所要時間	～0.5H	0	
	一ヶ月以内		5
攻撃者のレベル	しろうと	0	0
攻撃に必要な TOEの知識	公開情報で可	0	0
TOEアクセス時間	～0.5H	0	
	一ヶ月以内		6
攻撃の道具	なし	0	0

CEM パート2 バージョン1.0　表B.3から抜粋

＜結論の記述例＞

合計値＝11となり、本メカニズムは低レベルの攻撃に対抗できている（注：低レベルの攻撃にしか対抗できない）。

留意点

強度の分析は、TOEの動作環境において、最悪の場合を想定する。（ただし、前提条件は考慮する。）

4:AVA_SOF.1-3　4:AVA_SOF.1-8

STでSOF主張したすべてのセキュリティメカニズムに対して分析し、下記を満足していることを検証する。

・STに規定の最小機能強度レベル以上である。

・メカニズムごとに設定された機能強度を満足する。

4:AVA_SOF.1-6

セキュリティに関係のある確率・順列的なメカニズムがすべて機能強度分析の対象になっていなければならない。

4:AVA_SOF.1-7

EALによる脆弱性評定の違い

- EAL1：なし
- EAL2：
  ・機能強度の分析をする。
  ・明白な脆弱性に関する分析をする。
- EAL3：
  ・機能強度の分析をする。（EAL２と同じ）
  ・明白な脆弱性に関する分析をする。（EAL２と同じ）
  ・誤使用に関してガイダンス文書を検証する。
- EAL４
  ・機能強度の分析をする。（EAL２と同じ）
  ・すべての脆弱性に関する分析をする。
  ・誤使用に関して分析資料を検証する。

おわりに

IPA

問い合わせ先

■ **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
TEL：03-5978-7538
FAX：03-5978-7548
Email：jisec@ipa.go.jp
URL：http://www.ipa.go.jp/security/jisec/index.html

ご清聴
ありがとうございました