情報技術
セキュリティ評価のための
共通方法

評価方法

2017 年 4 月

バージョン **3.1**
改訂第 **5** 版

CCMB-2017-04-004

平成 29 年 7 月翻訳第 1.0 版
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

IPA まえがき

はじめに

本書は、「IT セキュリティ評価及び認証制度」において、「認証機関が公開する評価方法」の規格として公開している Common Evaluation Methodology (以下、CEM という)を翻訳した文書である。

原文

Common Methodology for Information Technology Security Evaluation

Evaluation methodology Version 3.1 Revision 5
April 2017 CCMB-2017-04-004

まえがき

情報技術セキュリティ評価のための共通方法の本バージョン(CEM v3.1)は、2005 年に CEM v2.3 が公開されて以来、最初の主要な改訂版である。

CEM v3.1 は、重複する評価アクティビティを排除し、製品の最終保証にあまり役立たないアクティビティを削減または排除し、誤解を減らすために CEM 用語を明確にし、セキュリティ保証が必要である領域に対する評価アクティビティを再構築し焦点を当て、必要に応じて新しい CEM 要件を追加することを目的としている。

商標:

- UNIX は、米国及びその他の諸国の The Open Group の登録商標である。
- Windows は、米国及びその他の諸国の Microsoft Corporation の登録商標である。

法定通知:

以下に示す政府組織は、情報技術セキュリティ評価のための共通方法の本バージョンの作成に貢献した。これらの政府組織は、情報技術セキュリティ評価のための共通方法、バージョン 3.1 *(CEM* 3.1 *と呼ぶ)の著作権を共有したまま、ISO/IEC 18045 国際標準の継続的な開発/維持の中で、CEM* 3.1 *を使用するために ISO/IEC に対し、排他的でないライセンスを許可している。ただし、適切と思われる場合に CEM* 3.1 *を使用、複製、配布、翻訳、及び改変する権利は、これらの政府組織が保有する。*

オーストラリア:	*The Australian Signals Directorate;*
カナダ:	*Communications Security Establishment;*
フランス:	*Agence Nationale de la Sécurité des Systèmes d'Information;*
ドイツ:	*Bundesamt fur Sicherheit in der Informationstechnik;*
日本:	*独立行政法人情報処理推進機構 (Information-technology Promotion Agency);*
オランダ:	*Netherlands National Communications Security Agency;*
ニュージーランド:	*Government Communications Security Bureau;*
韓国:	*National Security Research Institute;*
スペイン:	*Ministerio de Administraciones Publicas and Centro Criptologico Nacional;*
スウェーデン:	*Swedish Defence Materiel Administration;*
英国:	*National Cyber Security Centre;*
米国:	*The National Security Agency and the National Institute of Standards and Technology*

目次

図一覧

表一覧

1 序説

1 情報技術セキュリティ評価のための共通方法(CEM)の対象読者は、主に CC を適用する評価者と評価者アクションを確認する認証者であり、評価スポンサー、開発者、PP/ST 作成者、及び IT セキュリティに関心があるその他の関係者が二次対象読者である。

2 CEM は、IT セキュリティ評価に関するすべての疑問についてここで回答されるものではなく、さらなる解釈が必要であることを認識している。これらは相互承認アレンジメントの対象となるかもしれないが、個々の制度がそのような解釈の扱いを決定する。個々の制度によって処理することができる方法関連アクティビティの一覧は、附属書 A に記述されている。

2 適用範囲

3 情報技術セキュリティ評価のための共通方法(CEM)は、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)と対をなす文書である。CEM は、評価者によって実施される CC で定義された基準及び評価証拠を使用した CC 評価を行うための最低限のアクションを定義している。

4 CEM は、まだ一般的に同意されたガイダンスが存在しないような、CC の高い保証コンポーネントのための評価者のアクションは定義しない。

3 規定の参照

5 以下の参照文書は、本文書の適用のために不可欠である。日付の付いている参照資料については、指定した版のみが適用される。日付のない参照資料については、(修正を含む)最新版の参照文書が適用される。

[CC] 情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 5 版、2017 年 4 月

4 用語と定義

6 本文書の目的のために、以下の用語及び定義を適用する。

7 ボールド活字で表されている用語は、それ自体、この節に定義されている。

8 **アクション(action)** - CC パート 3 の評価者アクションエレメント。これらのアクションは、評価者アクションとして明示的に記述されているか、または CC パート 3 の保証コンポーネント内の開発者アクション(暗黙の評価者アクション)から暗黙に引き出される。

9 **アクティビティ(activity)** - CC パート 3 の保証クラスの適用。

10 **チェックする(check)** - 単純な比較により**判定**を下すこと。評価者の専門知識は必要とされない。この動詞を使用する文は、マッピングされるものを記述する。

11 **評価用提供物件(evaluation deliverable)** - 1 つまたは複数の評価または評価監督アクティビティを実行するために評価者または評価監督機関がスポンサーまたは開発者に要求する任意の資源。

12 **評価証拠(evaluation evidence)** - 有形の評価用提供物件。

13 **評価報告書(evaluation technical report)** - **総合判定**及びその正当化を提示した報告書。評価者が作成し、評価監督機関に提出される。

14 **検査する(examine)** - 評価者の専門知識を使用した分析により**判定**を下すこと。この動詞を使用する文は、分析されるものと分析のための特性を識別する。

15 **解釈(interpretation)** - CC、CEM または**制度**要件の明確化または敷衍。

16 **方法(methodology)** - IT セキュリティ評価に適用される原則、手続き及びプロセスのシステム。

17 **所見報告書(observation report)** - 評価中に、問題の明確化を要求したり、問題を識別するために評価者が作成する報告書。

18 **総合判定(overall verdict)** - 評価の結果に関して評価者が出す*合格(pass)*または*不合格(fail)*のステートメント。

19 **監督判定(oversight verdict)** - 評価監督アクティビティの結果に基づいて*総合判定(overall verdict)*を確認または拒否する、評価監督機関が出すステートメント。

20 **記録する(record)** - 評価中に行われた作業を後で再構築することができるようにするための十分に詳細な手順、事象、観察、洞察、及び結果を文書による記述として保持すること。

21 **報告する(report)** - 評価結果とサポート材料を**評価報告書**または**所見報告書**に含めること。

22 **制度(scheme)** - 評価監督機関(evaluation authority)が規定する規則のセット。IT セキュリティ評価を実施するために必要な基準と**方法**など、評価環境を定義する。

23 **サブアクティビティ(sub-activity)** - CC パート 3 の保証コンポーネントの適用。評価は、保証ファミリの単一の保証コンポーネントに対して行われるために、保証ファミリは、CEM で明示的に取り扱われていない。

24 **追跡(tracing)** - 2 つのエンティティのセットの間の単純な方向的関係。最初のセットのどのエンティティが 2 番目のセットのどのエンティティに対応するかを示す。

25 **判定(verdict)** - CC 評価者アクションエレメント、保証コンポーネント、またはクラスに関して評価者が発行する*合格*、*不合格*または*未決定(inconclusive)*ステートメント。

総合判定も参照のこと。

26 **ワークユニット(work unit)** - 評価作業の最も詳細なレベル。

各 CEM アクションは、1 つまたは複数のワークユニットからなる。それらのワークユニットは、CEM アクション内で CC の証拠の内容提示エレメントまたは開発者アクションエレメントによってグループ化される。ワークユニットは、CEM でそれらが引き出された CC エレメントと同じ順番に提示される。ワークユニットは、左余白に ALC_TAT.1-2 などのシンボルにより識別されている。このシンボルの文字列***ALC_TAT.1***は、CC コンポーネント(すなわち、CEM サブアクティビティ)を示し、最後の数字(2)は、これが***ALC_TAT.1***サブアクティビティの 2 番目のワークユニットであることを示している。

5 記号と略語

CEM	情報技術セキュリティ評価のための共通方法(Common Methodology for Information Technology Security Evaluation)
ETR	評価報告書(Evaluation Technical Report)
OR	所見報告書(Observation Report)

6 概要

6.1 CEM の構成

27 7 章では、CEM で使用される表記規則を定義する。

28 8 章では、CC 評価者アクションエレメントにマッピングしないため、関連する判定を持たない一般評価タスクについて説明する。

29 9 章では、PP の評価結果を得るために必要な作業について取り扱う。

30 11 章から 17 章では、保証クラスによって構成される評価アクティビティを定義する。

31 附属書 A では、評価結果の技術的証拠を提供するために使用する基本評価技法を扱う。

32 附属書 B では、脆弱性分析基準の説明及びその適用の例を提供する。

7 文書の表記規則

7.1 用語

33 各エレメントがファミリ内のすべてのコンポーネントの識別シンボルの最後の数字を保持している CC と異なり、CEM は、CC 評価者アクションエレメントがサブアクティビティからサブアクティビティへ変化するとき、新しいワークユニットを導入する。その結果、ワークユニットは変わらないが、ワークユニットの識別シンボルの最後の数字は変化する。

34 CC 要件から直接引き出されない必要な方法特有の評価作業は、*「タスク」(task)*または*「サブタスク」(sub-task)*と呼ばれる。

7.2 動詞の使用

35 すべてのワークユニットとサブタスクの動詞の前には助動詞*「しなければならない」(shall)*が置かれている。動詞と*「しなければならない」(shall)*は両方とも***ボールドイタリック***活字で表されている。助動詞*「しなければならない」(shall)*は、提供されている文が必須の場合にのみ使用されている。そのため、ワークユニットとサブタスク内でのみ使用されている。ワークユニットとサブタスクには、判定を下すために評価者が行わなければならない必須アクティビティが含まれている。

36 ワークユニットとサブタスクを伴うガイダンステキストは、評価での CC 用語の適用方法にさらなる説明を与えている。動詞の使用方法は、これらの動詞に関するISO 定義に従っている。助動詞*「するべきである」(should)*は、記述されている方法が非常に望ましい場合に使用されている。*「することができる」(may)*を含む他のすべての助動詞は、記述されている(いくつかの)方法は許されるが、推奨されるものではなく、非常に望ましいものでもない場合、すなわち、単なる説明に過ぎない場合に使用されている。

37 動詞*「チェックする」(check)*、*「検査する」(examine)*、*「報告する」(report)*、及び*「記録する」(record)*は、CEM のこの部で正確な意味で使用されている。それらの定義については、4 章が参照されるべきである。

7.3 一般的評価ガイダンス

38 複数のサブアクティビティに適用可能な資料は、1 箇所に集められている。広範囲(アクティビティとEAL 両方)に適用可能なガイダンスは、附属書 A に集められている。単一のアクティビティの複数のサブアクティビティに関するガイダンスは、そのアクティビティの序説に示されている。ガイダンスが 1 つだけのサブアクティビティに関係する場合、ガイダンスは、そのサブアクティビティ内に示されている。

7.4 CC 構造と CEM 構造間の関係

39 CC 構造(すなわち、クラス、ファミリ、コンポーネント、及びエレメント)と CEM 構造の間には直接の関係が存在する。図 1 は、クラス、ファミリ、及び評価者アクションエレメントからなる CC 構造と CEM アクティビティ、サブアクティビティ、及びアクションの間の対応を示している。ただし、いくつかの CEM ワークユニットは、CC 開発者アクション及び内容・提示エレメントに記載されている要件から発生する可能性がある。

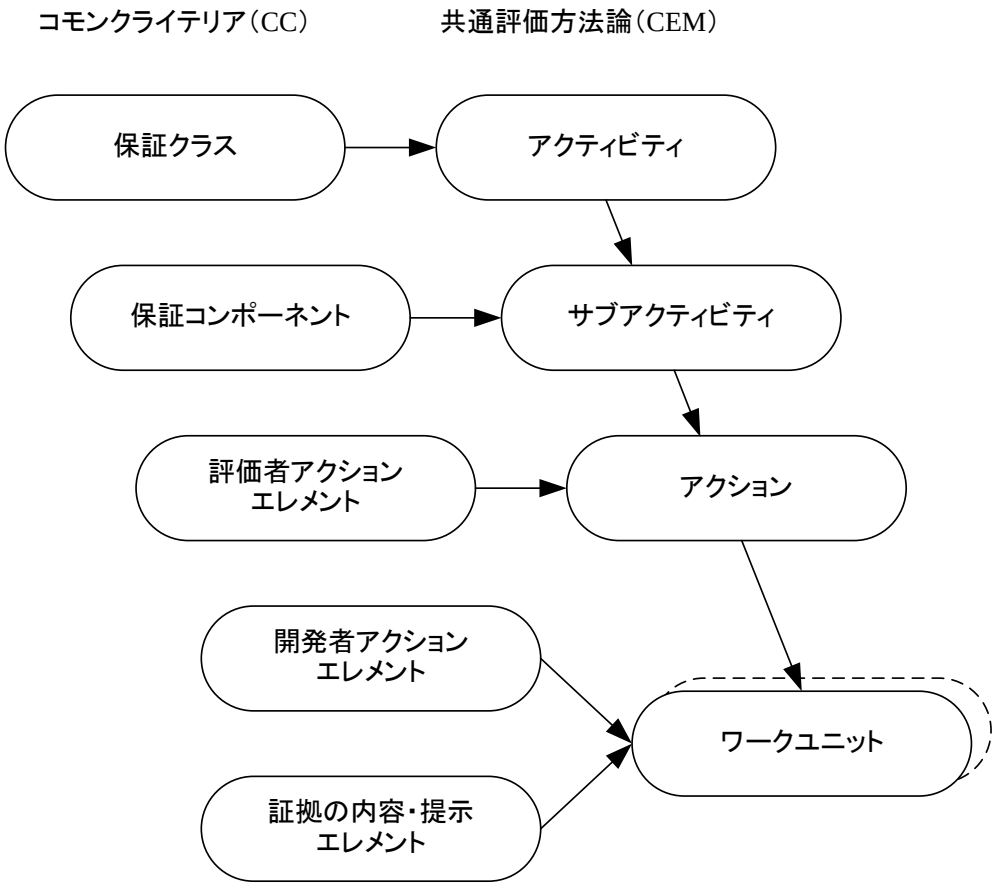

図 1　　CC 構造と CEM 構造のマッピング

8 評価プロセスと関連タスク

8.1 序説

40 この章では、評価プロセスの概要を提供し、評価を実施するとき評価者によって実行することが意図されるタスクを定義する。

41 各評価は、PP または TOE (ST を含む)の評価にかかわらず、同じプロセスに従い、入力タスク、出力タスク、評価サブアクティビティ、及び評価監督機関タスクに対する技術的有効性の実証の 4 つの共通な評価者タスクを含む。

42 入力タスクと出力タスクは、評価証拠の管理及び報告書作成に関連しており、この章で完全に記述されている。それぞれのタスクには、すべての CC 評価(PP または TOE の評価)に適用され、規定となる関連付けられたサブタスクがある。

43 評価サブアクティビティは、この章では簡単な説明のみが記述され、以下の章で完全に記述されている。

44 評価サブアクティビティとは異なり、入力タスクと出力タスクは CC 評価者アクションエレメントにマッピングしないので関連する判定を持たず、普遍的な原則への適合を保証するため、及び CEM に従うために実行される。

45 評価監督機関タスクに対する技術的有効性の実証は、出力タスク結果の評価監督機関分析によって遂行することもでき、評価サブアクティビティに対する入力を理解する評価者によって実証を含めることもできる。このタスクは、関連付けられた評価者判定を持たないが、評価監督機関判定を持つ。このタスクに合格するための詳細な基準は、附属書 A.5 に示すように、評価監督機関の裁量に任されている。

8.2 評価プロセスの概要

8.2.1 目的

46 この節では、方法の一般モデルを提示し、次のものを識別する:

a) 評価プロセスに関わる当事者の役割と責任;

b) 一般評価モデル。

8.2.2 役割の責任

47 一般モデルは、スポンサー、開発者、評価者、及び評価監督機関の各役割を定義する。

48 スポンサーは、評価の依頼及び支援に対する責任を持つ。これは、スポンサーが評価に対する様々な合意(例えば、評価の委託)を確立することを意味する。さらに、スポンサーは評価者に評価証拠が提供されることを保証する責任を持つ。

49 開発者は、TOE を作成し、スポンサーの代わりに評価に必要な証拠(例えば、訓練、設計情報)を提供する責任を持つ。

50 評価者は、評価の状況において必要な評価タスクを実行する。評価者は、スポンサーの代わりに開発者から、またはスポンサーから直接評価証拠を受け取り、評価サブアクティビティを実行し、評価監督機関に対して評価評定の結果を提供する。

51 評価監督機関は、制度を確立及び維持し、評価者により実施された評価を監視し、評価者が提供する評価結果に基づいた認証書、及び認証/確認の報告書を発行する。

8.2.3 役割の関係

52 過度の影響が評価に不適切な影響を与えるのを防ぐには、一部の役割の分割が必要となる。これは、開発者及びスポンサーの役割が単一のエンティティによって満たされる場合を除き、上記の役割が異なるエンティティによって担われることを意味する。

53 さらに、一部の評価(例えば、EAL1 評価)では、開発者がプロジェクトに関わる必要がない場合がある。この場合、評価者にTOEを提供し、評価証拠を生成するのは、スポンサーである。

8.2.4 一般評価モデル

54 評価プロセスは、評価入力タスク、評価出力タスク、及び評価サブアクティビティを実行している評価者で構成される。図 2 は、これらのタスクとサブアクティビティの関係の概要を提供する。

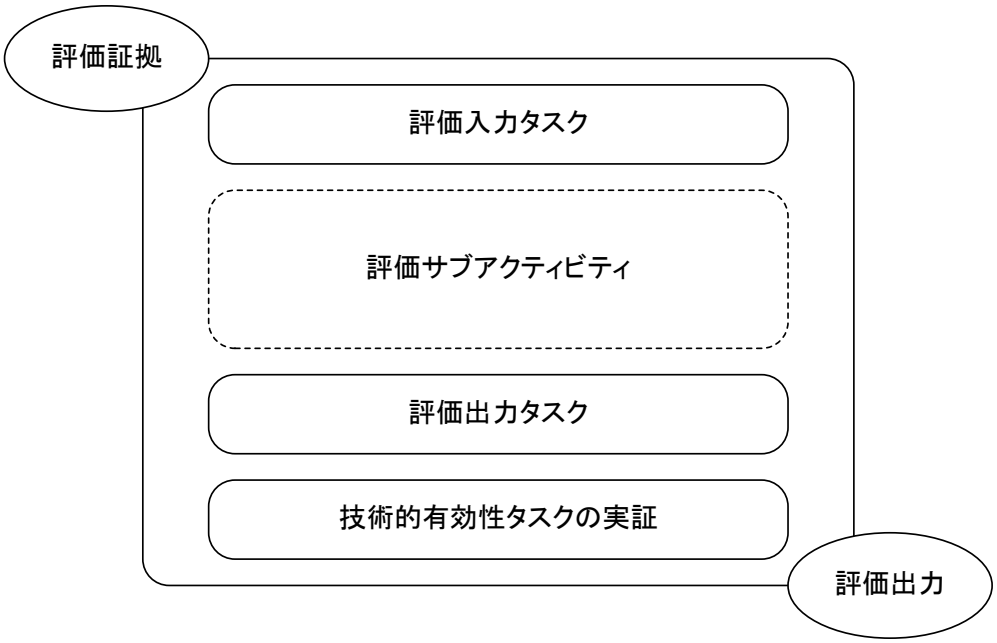

図 2 一般評価モデル

55 評価プロセスは、スポンサーと評価者の間に最初の接触がなされる場合に、準備フェーズの後に置くことができる。このフェーズの間に実行される作業及び様々な役割の関与は、異なることがある。通常、このステップの間に、評価者が実現可能性分析を実行して、評価の成功する可能性を評定する。

8.2.5 評価者の判定

56 評価者は、CC の要件に判定を下し、CEM の要件には判定を下さない。判定が下される最も詳細な CC 構造は、評価者アクションエレメントである(明示的または暗黙)。判定は、対応する CEM アクションとそれを構成するワークユニットを実行した結果として適用可能な CC 評価者アクションエレメントに下される。最後に、CC パート 1、10 章の「評価結果」の記述に従って、評価結果が割り付けられる。

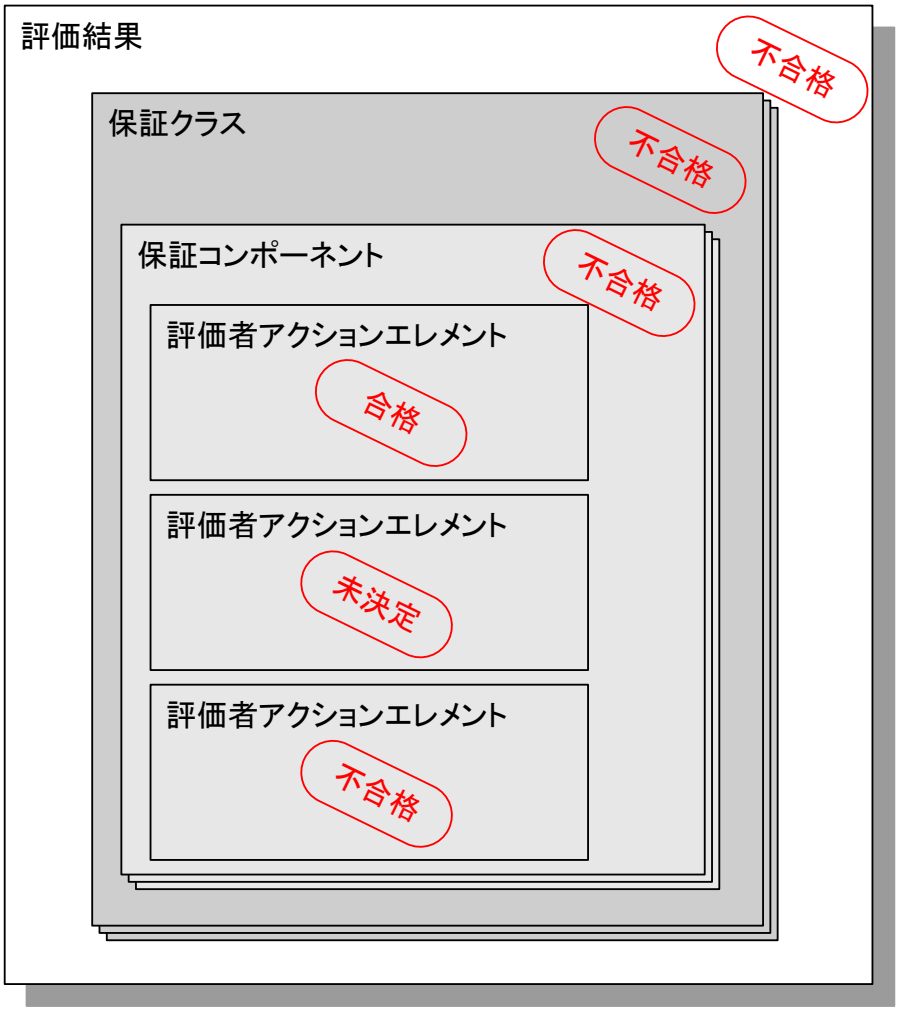

図 3 判定割当規則の例

57 CEM は、次の 3 つの相互に排他的な判定状態を承認する:

a) *「合格」(pass)*判定の条件は、評価者が CC 評価者アクションエレメントを完了し、評価されている PP、ST または TOE の要件が満たされていることを決定したことと定義される。エレメントが合格するための条件は、次のように定義される:

1) 関係する CEM アクションの構成要素ワークユニットである;

2) これらのワークユニットを実行するために要求されるすべての評価証拠が理路整然としており、評価者が十分に、及び完全に全体を理解できる;

3) これらのワークユニットを実行するために要求されるすべての評価証拠に、明白な内部不一致または他の評価証拠との不一致がない。明白なという表現は、ここではワークユニットを実行する際に評価者がこの不一致を検出することを意味し、評価者は、ワークユニットが実行されるたびに、評価証拠全体にわたる完全な一貫性分析を保証するべきではない。

b) *「不合格」(fail)*判定の条件は、評価者が CC 評価者アクションエレメントを完了し、評価されている PP、ST、または TOE の要件が満たされていないことを決定したこと、証拠が理路整然としていないこと、あるいは評価証拠内に明白な不一致が検出されたことと定義される;

c) すべての判定は、最初は*未決定*であり、*合格*または*不合格*の判定が割り当てられるまでそのままになっている。

58 総合判定は、すべての構成要素判定も*合格*である場合に限り、*合格*である。図 3 に示す例では、1 つの評価者アクションエレメントの判定が*不合格*であると、対応する保証コンポーネント、保証クラス、及び総合判定に対する判定も*不合格*となる。

8.3 評価入力タスク

8.3.1 目的

59 このタスクの目的は、評価者が評価に必要な正しいバージョンの評価証拠を利用できることを保証し、適切に保護することである。これがなければ、評価の技術的な正確性が保証されず、繰返し可能で、再現可能な結果が得られるような方法で評価が実行されることが保証されない。

8.3.2 適用上の注釈

60 必要な評価証拠すべてを提供する責任はスポンサーにある。ただし、ほとんどの評価証拠は、スポンサーの代わりに開発者によって作成され、供給される可能性がある。

61 保証要件は、TOE 全体に適用されるので、TOE のすべての部分に付随するすべての評価証拠は、評価者が入手できる状態となっていなければならない。このような評価証拠の範囲及び要求される内容は、開発者が TOE の各部分に対して持っている管理レベルとは、無関係である。例えば、設計が要求される場合、TOE 設計(ADV_TDS)要件は、TSF の一部であるすべてのサブシステムに適用される。さらに、実施されている手続きを要求する保証要件(例えば、CM 能力(ALC_CMC)と配付(ALC_DEL))もまた、TOE 全体(別の開発者によって作成された部分を含む)に適用される。

62 評価者がスポンサーとともに要求される評価証拠の目録を作成することが推奨される。この目録は、証拠資料への参照セットの場合がある。この目録には評価者が必要な証拠を簡単に見つけられるよう支援する十分な情報(例えば、各文書の簡単な要約、または少なくとも明確なタイトル、関連する節の指示)を含んでいるべきである。

63 これは必要な評価証拠内に含まれる情報であり、特定の文書構造ではない。サブアクティビティ用の評価証拠は、別々の文書で提供されるかもしれないし、または一冊の文書でサブアクティビティの入力要件のいくつかを満たすかもしれない。

64 評価者は、変更のない正式に発行されたバージョンの評価証拠を必要とする。ただし、例えば評価者が早期に非公式な評定を行うのを助けるために、評価証拠草案が評価中に提供されてもよいが、判定の根拠としては使用されない。以下に挙げるような特定の適切な評価証拠の草案バージョンを参照することが評価者にとって役立つことがある:

a) テスト証拠資料。評価者がテスト及びテスト手順の早期評定を行えるようにする;

b) 設計文書。評価者に TOE 設計を理解するための背景を提供する;

c) ソースコードまたはハードウェア図面。評価者が開発者の標準の適用を評定できるようにする。

65 評価証拠草案は、開発とともに TOE の評価が実行される場合に使用される可能性が高い。ただし、評価者によって識別された問題を解決するために、開発者が追加作業を実行する必要がある(例えば、設計または実装の誤りを修正する)場合、または既存の証拠資料に提供されていないセキュリティの評価証拠を提供する(例えば、元の TOE が CC の要件に合致するように開発されていない)場合には、開発済の TOE の評価中に評価証拠草案が使用されることもある。

8.3.3 評価証拠サブタスクの管理

8.3.3.1 構成制御

66 評価者は、評価証拠の構成制御(configuration control)を*実行しなければならない*。

67 CC では、評価者が評価証拠の各要素を受領した後に、それを識別し所在位置を定めることができること、また文書の特定のバージョンが評価者の所有にあるかどうかを決定することができることを意味する。

68 評価者は、評価証拠が評価者の所有にある間に、改ざんや損失から、その評価証拠を*保護しなければならない*。

8.3.3.2 処置

69 制度は、評価完了時点で、評価証拠の処置を制御することができる。評価証拠の処置は、以下の 1 つまたは複数によって実行されるべきである:

a) 評価証拠の返却;

b) 評価証拠の保管;

c) 評価証拠の破棄。

8.3.3.3 機密性

70 評価者は、評価の手順において、スポンサー及び開発者の商用機密に関わる情報(例えば、TOE 設計情報、特殊ツール)にアクセスすることができ、また国有機密に関わる情報にアクセスすることができる。制度は、評価証拠の機密性を維持するための評価者に対する要件を強いることができる。スポンサー及び評価者は、制度に一貫性が保たれている限りにおいて追加要件を相互に合意することができる。

71 機密性要件は、評価証拠の受領、取扱、保管、及び処置を含む評価作業の多くの局面に影響する。

8.4 評価サブアクティビティ

72 評価サブアクティビティは、PP 評価と TOE 評価のどちらであるかによって異なる。さらに、TOE 評価の場合、サブアクティビティは選択した保証要件に依存する。

8.5 評価出力タスク

8.5.1 目的

73 この節の目的は、所見報告書(OR)及び評価報告書(ETR)を記述することである。制度においては、個々のワークユニットの報告などの追加の評価者報告を要求することがある。あるいは追加情報を OR または ETR に含めることを要求することがある。CEM は最低限の情報のみを示しているため、CEM はこれらの報告への情報の追加を排除しない。

74 一貫した評価結果の報告により、結果の繰返し可能性及び再現可能性における普遍的な原則の達成を容易にすることができる。この一貫性では、ETR 及び OR で報告される情報の種類及び量を扱う。複数の異なる評価における ETR 及び OR の一貫性を保つことは、評価監督機関の責任である。

75 評価者は、報告の情報内容に対する CEM 要件を満たすために以下の 2 つのサブタスクを実行する:

a) OR サブタスクを記述する(評価の状況において必要な場合);

b) ETR サブタスクを記述する。

8.5.2 評価出力の管理

76 評価者は、評価監督機関に ETR を提供する。また、提供可能になった時点ですべての OR も提供する。ETR 及び OR の取り扱いの管理に対する要件は、制度によって確立される。この制度には、スポンサーまたは開発者への提供を含めることができる。ETR 及び OR には、機密情報または著作権を持つ情報が含まれることがあり、スポンサーに提供する前に不適切な部分の整理が必要なことがある。

8.5.3 適用上の注釈

77 CEM のこのバージョンでは、再評価や再使用を支援するための評価者証拠の提供の要件が明示的に述べられていない。再評価または再使用のための情報がスポンサーによって要求される場合、評価が実施された制度に相談するべきである。

8.5.4 OR サブタスクを記述する

78 OR は、評価者に(例えば、要件の適用に関する評価監督機関からの)明確化を要求するためのメカニズム、または評価の局面における問題を識別するためのメカニズムを提供する。

79 不合格判定の場合、評価者は評価結果を反映する OR を***提供しなければならない***。それ以外の場合、評価者は OR を明確化の必要性を表す 1 つの方法として使用してもよい。

80 各 OR において、評価者は以下の項目について***報告しなければならない：***

a) 評価される PP または TOE の識別情報;

b) その過程において所見が生成される評価タスクまたはサブアクティビティ;

c) 所見;

d) 重大度の評定(例えば、不合格判定を意味する、評価に対する進行を妨げる、評価が完了する前に解決を要求する);

e) 問題の解決に責任がある組織の識別;

f) 解決に推奨されるタイムテーブル;

g) 所見の解決に失敗した場合の評価への影響の評定。

81 OR の対象読者及び報告を処理する手続きは、報告内容の性質及び制度に依存する。制度は、OR の異なる種類を区別し、あるいは追加の種類を、必要な情報及び提供先に関連する違いによって(例えば、評価監督機関及びスポンサーへの評価 OR)定義することができる。

8.5.5 ETR サブタスクを記述する

8.5.5.1 目的

82 評価者は、判定の技術的な正当性を示すために ETR を***提供しなければならない***。

83 CEM は ETR に関する最低限の内容の要件を定義するが、制度では、追加の内容及び特定の表象的及び構造的要件を特定することができる。例えば、特定の導入(例えば、権利の放棄、及び著作権についての章)を ETR 内で報告することを、制度にて要求することができる。

84 ETR の読者は情報セキュリティの一般概念、CC、CEM、評価手法及び IT の知識を持っているものと想定されている。

85 ETR は、評価が要求された基準に対して行われたことを評価監督機関が確認するのを支援する。しかし、証拠資料の結果が必要な情報のすべてを提供しないことがあり、制度によって特に要求される追加情報を必要とすることも予想される。この局面は CEM の適用範囲外である。

8.5.5.2 PP 評価用の ETR

86 この節では、PP 評価用の ETR の最低限の内容を記述する。ETR の内容は、図 4 に示されている; この図は、ETR 文書の構造的概略を構成する際にガイドとして使用することができる。

図 4　　PP 評価用の ETR 情報内容

8.5.5.2.1　　**序説**

87　　評価者は、評価制度識別情報を*報告しなければならない*。

88　　評価制度識別情報(例えば、ロゴ)は、評価監督に責任を持つ制度を曖昧さなく識別するために必要な情報である。

89　　評価者は、ETR 構成制御識別情報を*報告しなければならない*。

90　　ETR 構成制御識別情報には、ETR を識別する情報(例えば、名前、日付、及びバージョン番号)が含まれる。

91　　評価者は、PP 構成制御識別情報を*報告しなければならない*。

92　　PP 構成制御識別情報(例えば、名前、日付、及びバージョン番号)は、判定が評価者によって正しく下されたことを評価監督機関が検証するために評価対象を識別するために必要である。

93 評価者は、開発者の識別情報を***報告しなければならない***。

94 PP 開発者の識別情報は、PP の作成に責任がある当事者を識別するために必要である。

95 評価者は、スポンサーの識別情報を***報告しなければならない***。

96 スポンサーの識別情報は、評価者に評価証拠を提供する責任がある当事者を識別するために必要である。

97 評価者は、評価者の識別情報を***報告しなければならない***。

98 評価者の識別情報は、評価を実行し、評価判定に責任がある当事者を識別するために必要である。

8.5.5.2.2 評価

99 評価者は、使用する評価方法、技法、ツール及び基準を***報告しなければならない***。

100 評価者は、PP の評価に使用する評価基準、方法、及び解釈を参照する。

101 評価者は、あらゆる評価に関する制約、評価結果の処理に関する制約、及び評価結果に影響する評価の実行中に行われる前提条件を***報告しなければならない***。

102 評価者は、法律または法令の側面、組織、機密性などに関した情報を含めることができる。

8.5.5.2.3 評価の結果

103 評価者は、対応するCEMアクションとそれを構成するワークユニットを実行した結果として、APEアクティビティを構成する各保証コンポーネントに対する判定及び裏付ける根拠を***報告しなければならない***。

104 根拠は、CC、CEM、検査された解釈及び評価証拠を使用して判定を正当化し、評価証拠が基準の各側面をどのように満たすか、または満たさないかを示す。実行される作業、使用される方法、及び結果からの導出の記述を含む。根拠は CEM ワークユニットレベルの詳細を提供することができる。

8.5.5.2.4 結論及び推奨事項

105 評価者は、評価の結論、特に CC パート 1 の 10 章の「評価結果」に定義され、8.2.5 に記述されている判定の割り当てによって決定される総合判定について***報告しなければならない***。

106 評価者は、評価監督機関に役立つ推奨事項を提供する。これらの推奨事項には、評価中に発見された PP の欠点または特に役立つ特徴についての言及が含まれる場合がある。

8.5.5.2.5 評価証拠の一覧

107 評価者は、各評価証拠要素について、以下の情報を***報告しなければならない：***

- 発行者(例えば、開発者、スポンサー);
- タイトル;

- 一意の参照(例えば、発行日及びバージョン番号)。

8.5.5.2.6 頭字語の一覧/用語集

108 評価者は、ETR 内で使用される頭字語または省略語を***報告しなければならない***。

109 CC または CEM ですでに定義された用語は ETR で繰返し定義する必要はない。

8.5.5.2.7 所見報告

110 評価者は、評価中に作成された OR 及びそのステータスを一意に識別する完全な一覧を***報告しなければならない***。

111 各 OR について、一覧には識別情報及びタイトルまたは内容の簡単な要約を含んでいるべきである。

8.5.5.3 TOE 評価用の ETR

112 この節では、TOE 評価用の ETR の最低限の内容を記述する。ETR の内容は、図 5 に示されている。この図は、ETR 文書の構造的アウトラインを構成する際にガイドとして使用することができる。

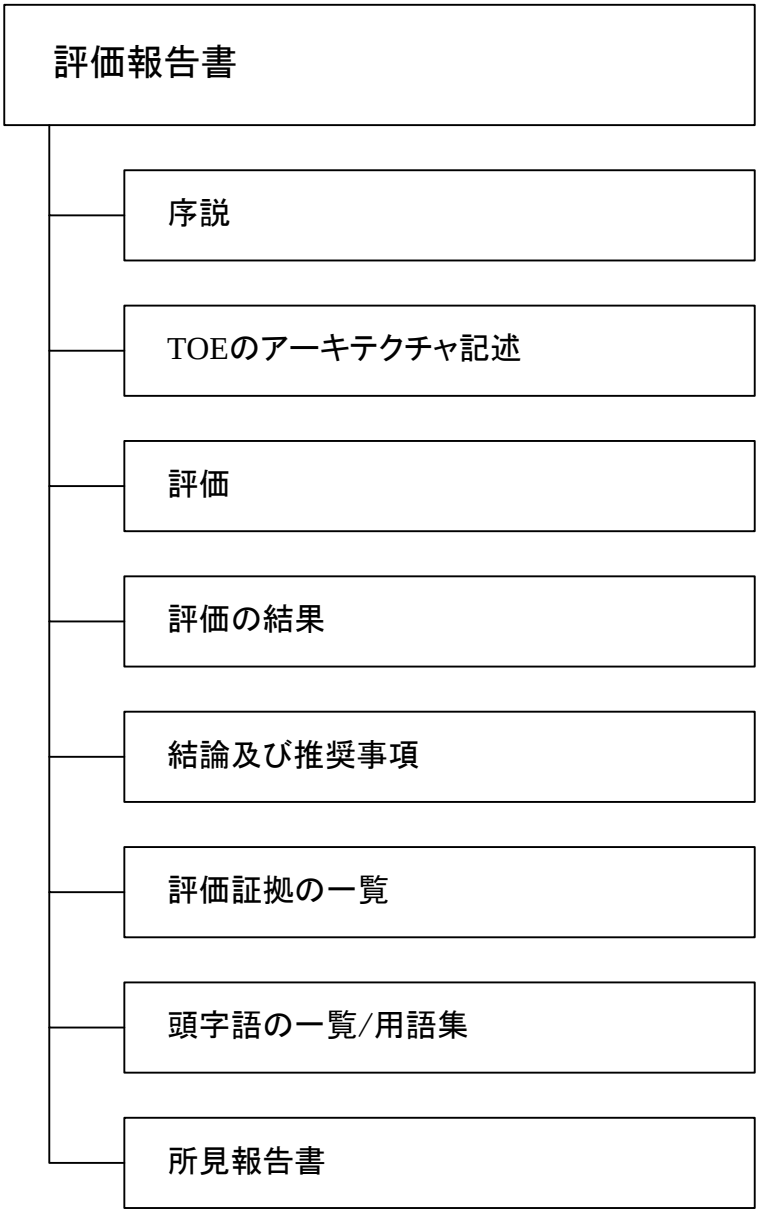

図 5　　TOE 評価用の ETR 情報内容

8.5.5.3.1　　序説

113　　評価者は、評価制度識別情報を*報告しなければならない*。

114　　評価制度識別情報(例えば、ロゴ)は、評価監督に責任を持つ制度を曖昧さなく識別するために必要な情報である。

115　　評価者は、ETR 構成制御識別情報を*報告しなければならない*。

116　　ETR 構成制御識別情報には、ETR を識別する情報(例えば、名前、日付、及びバージョン番号)が含まれる。

117　　評価者は、ST 及び TOE 構成制御識別情報を*報告しなければならない*。

118 ST 及び TOE 構成制御識別情報は、判定が評価者によって正しく下されたことを評価監督機関が検証するために、評価された対象を識別する。

119 TOE が 1 つまたは複数の PP 要件を満たしていることを ST が要求する場合、ETR は対応する PP 参照を報告しなければならない。

120 PP 参照には、PP を一意に識別する情報(例えば、タイトル、日付、及びバージョン番号)が含まれる。

121 評価者は、開発者の識別情報を***報告しなければならない***。

122 TOE 開発者の識別情報は、TOE の作成に責任がある当事者を識別するために必要である。

123 評価者は、スポンサーの識別情報を***報告しなければならない***。

124 スポンサーの識別情報は、評価者に評価証拠を提供する責任がある当事者を識別するために必要である。

125 評価者は、評価者の識別情報を***報告しなければならない***。

126 評価者の識別情報は、評価を実行し、評価判定に責任がある当事者を識別するために必要である。

8.5.5.3.2 TOE のアーキテクチャ記述

127 評価者は、該当する場合、TOE 設計(ADV_TDS)というタイトルの CC 保証ファミリ内に記述されている評価証拠に基づいてTOE及びその主要なコンポーネントの上位レベル記述を***報告しなければならない***。

128 この節の目的は、主要コンポーネントのアーキテクチャ上の分離の度合いの特性を表すことである。ST に TOE 設計(ADV_TDS)要件がない場合、これは該当しないため、満たされているものとみなされる。

8.5.5.3.3 評価

129 評価者は、使用する評価方法、技法、ツール及び基準を***報告しなければならない***。

130 評価者は、TOE の評価に使用する評価基準、方法、及び解釈またはテストを実行するために使用する装置を参照することができる。

131 評価者は、あらゆる評価に関する制約、評価結果の提供に関する制約及び評価結果に影響する評価の実行中に行われる前提条件を***報告しなければならない***。

132 評価者は、法律または法令の側面、組織、機密性などに関した情報を含めることができる。

8.5.5.3.4 評価の結果

133 TOE が評価される各アクティビティにおいて、評価者は以下の項目について***報告しなければならない***：

- 考慮されるアクティビティのタイトル;

- 対応するCEMアクションとそれを構成するワークユニットを実行した結果として、このアクティビティを構成する各保証コンポーネントに対する判定及び裏付ける根拠。

134 根拠は、CC、CEM、検査された解釈及び評価証拠を使用して評価を正当化し、評価証拠が基準の各側面をどのように満たすか、または満たさないかを示す。それは、実行される作業、使用される方法、及び結果からの導出の記述を含む。根拠は CEM ワークユニットレベルの詳細を提供することができる。

135 評価者は、ワークユニットが明確に要求されるすべての情報を***報告しなければならない***。

136 AVA及びATEアクティビティでは、ETR 内で報告する情報を識別するワークユニットが定義されている。

8.5.5.3.5 結論及び推奨事項

137 評価者は、TOE が関連する ST を満たしているかどうかに関係する評価の結論、特に CC パート1の10章「評価結果」に定義され、8.2.5に記述されている判定の割り当ての適用によって決定される総合判定について***報告しなければならない***。

138 評価者は、評価監督機関に役立つ推奨事項を提供する。これらの推奨事項には、評価中に発見された IT 製品の欠点または特に役立つ特徴についての言及が含まれる場合がある。

8.5.5.3.6 評価証拠の一覧

139 評価者は、各評価証拠要素について、以下の情報を***報告しなければならない***：

- 発行者(例えば、開発者、スポンサー);
- タイトル;
- 一意の参照(例えば、発行日及びバージョン番号)。

8.5.5.3.7 頭字語の一覧/用語集

140 評価者は、ETR 内で使用される頭字語または省略語を***報告しなければならない***。

141 CC または CEM ですでに定義された用語は ETR で繰返し定義する必要はない。

8.5.5.3.8 所見報告

142 評価者は、評価中に作成された OR 及びそのステータスを一意に識別する完全な一覧を***報告しなければならない***。

143 各 OR について、一覧には識別情報及びタイトルまたは内容の簡単な要約を含んでいるべきである。

9 APE クラス: プロテクションプロファイル評価

9.1 序説

144 この章では、PP 評価について記述する。PP 評価の要件及び方法は、PP で主張されている EAL (またはその他の保証要件セット)に関係なく各 PP 評価で同一である。この章の評価方法は、CC パート 3 の APE クラスに特定されている PP の要件に基づいている。

145 CC パート 1 の附属書 A、B、及び C、操作のためのガイダンスは、ここでの概念を明確にし、多くの例を提供するため、この章はこれらの附属書とともに使用されるべきである。

9.2 適用上の注釈

9.2.1 認証された PP の評価結果の再使用

146 1 つまたは複数の認証された PP に基づいている PP を評価している間に、これらの PP が認証されたという事実を再使用できることがある。評価中の PP が、脅威、OSP、セキュリティ対策方針、及び/またはセキュリティ要件を、適合が主張されている PP の脅威、OSP、セキュリティ対策方針、及び/またはセキュリティ要件に追加しない場合は、認証済みの PP の結果の再使用の有用性は大きくなる。評価中の PP に認証済みの PP より多くの内容が含まれている場合、再使用はまったく役に立たない可能性がある。

147 評価者は、特定の分析またはその分析の一部がすでに PP 評価の一部として実行された場合は、その分析を部分的にしか行わないかまったく行わないことによって、PP 評価結果を再使用できる。これを実行する場合、評価者は PP 内の分析が正しく実行されたことを想定するべきである。

148 この例としては、適合が主張されている PP にあるセキュリティ要件のセットが含まれており、これらが評価の間に内部的に一貫していることが決定された場合などが該当するだろう。評価されている PP が完全に同じ要件を使用する場合は、ST 評価の間に一貫性分析を繰返す必要はない。評価されている PP が 1 つまたは複数の要件を追加する場合、またはこれらの要件に基づいて操作を実行する場合は、分析を繰返す必要がある。ただし、元の要件が内部的に一貫している事実を使用して、この一貫性分析の作業を削減できる場合がある。元の要件が内部的に一貫している場合、評価者は以下の点だけを決定する必要がある:

a) すべての新しい及び/または変更された要件のセットが内部的に一貫している、及び

b) すべての新しい及び/または変更された要件のセットが元の要件と一貫している。

149 この理由により分析が行われない場合、または分析が部分的にしか行われない場合、評価者は、それぞれの場合について ETR に注釈を記述する。

9.3 PP 概説(APE_INT)

9.3.1 サブアクティビティの評価(APE_INT.1)

9.3.1.1 目的

150 このサブアクティビティの目的は、PP が正しく識別されているかどうか、及び PP 参照と TOE 概要が相互に一貫しているかどうかを決定することである。

9.3.1.2 入力

151 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP

9.3.1.3 アクション APE_INT.1.1E

APE_INT.1.1C ***PP 概説は、PP 参照と TOE 概要を含めなければならない。***

APE_INT.1-1 評価者は、PP 概説が PP 参照と TOE 概要を含んでいることを***チェックしなければならない。***

APE_INT.1.2C ***PP 参照は、PP を一意に識別しなければならない。***

APE_INT.1-2 評価者は、PP 参照が PP を一意に識別していることを決定するために、その PP 参照を***検査しなければならない。***

152 評価者は、PP をその他の PP と簡単に区別できるように、PP 参照が PP 自体を識別することと、さらに PP 参照がその PP の各バージョンも(例えば、バージョン番号及び/または公表日を含めることによって)一意に識別することを決定する。

153 PP は、一意の参照をサポートできる何らかの参照方式を持つべきである(例えば、番号、文字、日付の使用)。

APE_INT.1.3C ***TOE 概要は、TOE の使用法及び主要なセキュリティ機能の特徴を要約しなければならない。***

APE_INT.1-3 評価者は、TOE 概要が TOE の使用法と主要なセキュリティ機能の特徴を記述していることを決定するために、その TOE 概要を***検査しなければならない。***

154 TOE 概要では、TOE で期待されている使用法と主要なセキュリティ機能の特徴を簡潔に(つまり、数段落で)記述するべきである。TOE 概要は、PP が消費者及び潜在的な TOE 開発者にとって興味あるものであるかどうかを各自がすばやく決定できるようにするべきである。

155 評価者は、概要が TOE 開発者及び消費者にとって十分に明確であり、各自が意図されている TOE の使用法と主要なセキュリティ機能の特徴についての一般的な理解を得るために十分な情報が含まれていることを決定する。

APE_INT.1.4C ***TOE 概要は、TOE 種別を識別しなければならない。***

APE_INT.1-4 評価者は、TOE 概要が TOE 種別を識別していることを***チェックしなければならない。***

APE_INT.1.5C ***TOE 概要は、TOE が利用できるTOE 以外のハードウェア/ソフトウェア/ファームウェアを識別しなければならない。***

APE_INT.1-5 評価者は、TOE が利用できる TOE 以外のハードウェア/ソフトウェア/ファームウェアを TOE 概要が識別していることを決定するために、その TOE 概要を***検査しなければならない。***

156 ある TOE は単独で実行できるが、別のある TOE (特にソフトウェア TOE)は、動作のために追加のハードウェア、ソフトウェア、またはファームウェアを必要とする。PP のこの節では、PP 作成者は、実行する TOE に対して利用できるすべてのハードウェア、ソフトウェア、及び/またはファームウェアを列挙する。

157 この識別は、潜在的消費者と TOE 開発者の TOE が列挙されたハードウェア、ソフトウェア、及びファームウェアとともに操作できるかどうかを決定するために、潜在的消費者と TOE 開発者にとって十分に詳細なものにするべきである。

9.4 適合主張(APE_CCL)

9.4.1 サブアクティビティの評価(APE_CCL.1)

9.4.1.1 目的

158 このサブアクティビティの目的は、様々な適合主張の有効性を決定することである。これらは、PP が CC、他の PP、及びパッケージに対してどのように適合しているかを記述する。

9.4.1.2 入力

159 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP;

b) PP が適合を主張する PP;

c) PP が適合を主張するパッケージ。

9.4.1.3 アクション APE_CCL.1.1E

APE_CCL.1.1C ***適合主張は、PP が適合を主張する CC のバージョンを識別する CC 適合主張を含めなければならない。***

APE_CCL.1-1 評価者は、PP が適合を主張する CC のバージョンを識別する CC 適合主張が適合主張に含まれていることを***チェックしなければならない。***

160 評価者は、この PP を開発するために使用された CC のバージョンを CC 適合主張が識別することを決定する。これには、CC のバージョン番号を含めるべきであり、また、CC の国際的な英語バージョンが使用されなかった場合は、使用された CC のバージョンの言語も含めるべきである。

APE_CCL.1.2C ***CC 適合主張は、CC パート 2 に対する PP の適合を CC パート 2 適合または CC パート 2 拡張として記述しなければならない。***

APE_CCL.1-2 評価者は、CC 適合主張が PP に対する CC パート 2 適合または CC パート 2 拡張の主張を述べていることを***チェックしなければならない。***

APE_CCL.1.3C ***CC 適合主張は、CC パート 3 に対する PP の適合を CC パート 3 適合または CC パート 3 拡張として記述しなければならない。***

APE_CCL.1-3 評価者は、CC 適合主張が PP に対する CC パート 3 適合または CC パート 3 拡張の主張を述べていることを***チェックしなければならない。***

APE_CCL.1.4C ***CC 適合主張は、拡張コンポーネント定義と一貫していなければならない。***

APE_CCL.1-4 評価者は、CC パート 2 に対する CC 適合主張が拡張コンポーネント定義と一貫していることを決定するためにその CC 適合主張を***検査しなければならない。***

161 CC 適合主張が CC パート 2 適合を含んでいる場合、評価者は、拡張コンポーネント定義が機能コンポーネントを定義しないことを決定する。

162 CC 適合主張が CC パート 2 拡張を含んでいる場合、評価者は、拡張コンポーネント定義が拡張機能コンポーネントを少なくとも 1 つは定義していることを決定する。

APE_CCL.1-5 評価者は、CC パート 3 に対する CC 適合主張が拡張コンポーネント定義と一貫していることを決定するためにその CC 適合主張を***検査しなければならない。***

163 CC 適合主張が CC パート 3 適合を含んでいる場合、評価者は、拡張コンポーネント定義が保証コンポーネントを定義しないことを決定する。

164 CC 適合主張が CC パート 3 拡張を含んでいる場合、評価者は、拡張コンポーネント定義が拡張保証コンポーネントを少なくとも 1 つは定義していることを決定する。

APE_CCL.1.5C ***適合主張は、PP が適合を主張するPP 及びセキュリティ要件パッケージをすべて識別しなければならない。***

APE_CCL.1-6 評価者は、PP が適合を主張するすべての PP を識別する PP 主張を適合主張が含むことを***チェックしなければならない。***

165 PP が別の PP に対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

166 評価者は、参照される PP が曖昧さなく(例えば、タイトル及びバージョン番号、または PP の概説に含まれている識別によって)識別されることを決定する。

167 評価者は、PP への部分的な適合の主張は許可されないことに留意する。

APE_CCL.1-7 評価者は、PP が適合を主張するすべてのパッケージを識別するパッケージ主張を適合主張が含むことを***チェックしなければならない。***

168 PP がパッケージに対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

169 評価者は、参照されるパッケージが曖昧さなく(例えば、タイトル及びバージョン番号、またはパッケージの概説に含まれている識別によって)識別されることを決定する。

170 評価者は、パッケージへの部分的な適合の主張は許可されないことに留意する。

APE_CCL.1.6C ***適合主張は、パッケージに対する PP の適合をパッケージ適合またはパッケージ追加として記述しなければならない。***

APE_CCL.1-8 評価者は、識別された各パッケージに対して、適合主張がパッケージ名適合またはパッケージ名追加の主張を述べていることを***チェックしなければならない。***

171 PP がパッケージに対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

172 パッケージ適合主張がパッケージ名適合を含む場合、評価者は以下のことを決定する:

a) パッケージが保証パッケージである場合、PP はパッケージに含まれるすべての SAR を含めるが、追加 SAR は含めない。

b) パッケージが機能パッケージである場合、PP はパッケージに含まれるすべての SFR を含めるが、追加 SFR は含めない。

173 パッケージ適合主張がパッケージ名追加を含む場合、評価者は以下のことを決定する:

a) パッケージが保証パッケージである場合、PP はパッケージに含まれるすべての SAR を含み、追加 SAR を少なくとも 1 つ、またはパッケージ内の SAR の上位階層である SAR を少なくとも 1 つ含む。

b) パッケージが機能パッケージである場合、PP はパッケージ内に含まれるすべての SFR を含み、追加 SFR を少なくとも 1 つ、またはパッケージ内の SFR の上位階層である SFR を少なくとも 1 つ含む。

APE_CCL.1.7C ***適合主張根拠は、TOE 種別が、適合が主張されている PP 内の TOE 種別と一貫していることを実証しなければならない。***

APE_CCL.1-9 評価者は、TOE の TOE 種別が各 PP のすべての TOE 種別と一貫していることを決定するために適合主張根拠を***検査しなければならない。***

174 PP が別の PP に対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

175 種別の間の関係は、簡単なもの(別のファイアウォール PP に対する適合を主張しているファイアウォール PP)、またはより複雑なもの(複数の他の PP に対する適合を同時に主張しているスマートカード PP (統合された回路に対する PP、スマートカード OS に対する PP、及びスマートカード上の 2 つのアプリケーションに対する 2 つの PP))である可能性がある。

APE_CCL.1.8C ***適合主張根拠は、セキュリティ課題定義のステートメントが、適合が主張されている PP 内のセキュリティ課題定義のステートメントと一貫していることを実証しなければならない。***

APE_CCL.1-10 評価者は、セキュリティ課題定義のステートメントが、PP の適合ステートメントによる定義に従って、適合が主張されている PP で述べられているセキュリティ課題定義のステートメントと一貫していることを適合主張根拠が実証することを決定するために、その根拠を***検査しなければならない。***

176 評価されている PP が別の PP に対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

177 適合が主張されている PP がセキュリティ課題定義のステートメントを持たない場合、このワークユニットは該当しないため、満たされているものとみなされる。

178 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は次の状態であるかどうかを決定する。

a) 評価されている PP 内の脅威は、適合が主張されている PP 内の脅威のスーパーセットであるか、その PP 内の脅威と同一である;

b) 評価されている PP 内の OSP は、適合が主張されている PP 内の OSP のスーパーセットであるか、その PP 内の OSP と同一である;

c) 適合を主張している PP 内の前提条件は、次の 2 項目で説明される 2 つの例外を除き、適合が主張されている PP 内の前提条件と同一である;

- 適合が主張されている PP からの前提条件（または前提条件の一部）は、この前提条件（または前提条件の一部）に対処する運用環境のセキュリティ対策方針のすべてが、TOE のセキュリティ対策方針に置き換えられる場合、除外することができる;

- 新しい前提条件が、適合が主張されている PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている脅威（または脅威の一部）を軽減せず、適合が主張されている PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている OSP（または OSP の一部）を満たさないことを正当化する理由が示される場合、適合が主張されている PP で定義された前提条件に、前提条件を追加することができる。

適合が主張されている他の PP から前提条件を除外した、または、新しい前提条件を追加した PP を検査する際、評価者は、上記の条件が満たされているかどうかを慎重に決定しなければならない。次の考察で、これらの場合における動機と例を示す:

- 前提条件を除外する例: 適合が主張されている PP は、運用環境が TOE の外部インタフェースに送信されるデータの不正な改変または傍受を防ぐということを述べる前提条件を含むことができる。これは、TOE が、このインタフェースで、平文で完全性保護なしのデータを受け入れ、攻撃者によるこれらのデータへのアクセスを防ぐセキュアな運用環境に設置されると想定される場合に当てはまる。そして、前提条件は、適合が主張されている PP 内で、このインタフェースで交換したデータが、運用環境での適切な手段によって保護されていると述べる運用環境のセキュリティ対策方針にマッピングされる。この PP への適合を主張する PP が、例えば、このインタフェースを経由して転送されたすべてのデータの暗号化と完全性保護のためのセキュアなチャネルを供給することによって、TOE 自身がこれらのデータを保護すると述べる追加のセキュリティ対策方針を持つ、更にセキュアな TOE を定義する場合、対応する運用環境のセキュリティ対策方針と前提条件は、適合を主張する PP から除外することができる。これはまた、対策方針が運用環境から TOE に再割付されるので、対策方針の再割付と呼ばれる。この TOE は、除外した前提条件を満たす運用環境においてなおもセキュアであり、そのため、適合が主張されている PP をやはり満たすという点に注意のこと。

- 前提条件を追加する例: この例では、適合が主張されている PP が「ファイアウォール」型の TOE に対する要件を特定するよう設計されており、他の PP 作成者は、ファイアウォールを実装する TOE に対するこの PP への適合を主張したいと願うが、TOE は更に VPN（仮想プライベートネットワーク）コンポーネントの機能性も提供する。VPN 機能性については、TOE は暗号鍵を必要とし、これらの鍵も運用環境によってセキュアに処理される必要がある（例えば、対称鍵が、ネットワーク接続をセキュアにするために使われ、そのため、ネットワークの他のコンポーネントに対してセキュアな方法で提供される必要がある場合）。この場合、VPN によって使われる暗号鍵が、運用環境によってセキュアに処理されるという前提条件を追加するのは許容できる。この前提条件は、適合が主張されている PP の脅威や OSP に対処しないので、上記に述べた状況を満たす。

- 前提条件を追加する反例: 最初の例の変形として、適合が主張されている PP がそのインタフェースの 1 つに対してセキュアなチャネルを提供するための TOE のセキュリティ対策方針を既に含んでおり、この対策方針はこのインタフェース上のデータの不正な改変または読み取りの脅威にマッピングされる。この場合、この PP への適合を主張する他の PP が、運用環境がこのインタフェース上のデータを改変や不正なデータの読み取りから保護すると想定する運用環境の前提条件を追加することは明らかに許可されない。この前提条件は TOE によって対処されることが意図されている脅威を低減する。従って、この前提条件を追加した PP を満たす TOE は、適合が主張されている PP を自動的に満たさず、よって、この追加は許可されない。

- 前提条件を追加する 2 つ目の反例: ファイアウォールを実装する TOE の上記の例において、TOE が信頼できるデバイスにのみ接続するという一般的な前提条件を追加することは許容できない。というのは、これは明らかにファイアウォールに関する本質的な脅威(つまり、フィルタにかける必要のある信頼できない IP トラフィックがある)を取り除くからである。従って、この追加は許可されない。

179 適合が主張されている PP によって論証適合が要求されている場合、評価中の PP のセキュリティ課題定義のステートメントが、適合が主張されている PP 内のセキュリティ課題定義のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

180 このため、適合主張根拠は、適合を主張する PP 内のセキュリティ課題定義が、適合が主張されている PP 内のセキュリティ課題定義と同等(またはより制限的)であると実証する必要がある。これは、以下を意味する:

- 適合を主張する PP 内のセキュリティ課題定義を満たすすべての TOE は、適合が主張されている PP 内のセキュリティ課題定義も満たす。これはまた、適合が主張されている PP 内に定義された脅威を実現したり、適合が主張されている PP 内に定義された OSP を侵害したりする各事象が、適合を主張する PP 内に述べられた脅威を実現したり、適合を主張する PP 内に定義された OSP を侵害したりすることを実証することによって、間接的に示される。適合を主張する PP 内に述べられた OSP を満たすことは、適合が主張される PP 内に述べられた脅威を防ぐことができ、または、適合を主張する PP 内に述べられた脅威を防ぐことは、適合が主張されている PP 内に述べられた OSP を満たすことができるので、脅威と OSP はお互いに代用できる点に注意のこと;

- 適合が主張されている PP 内のセキュリティ課題定義を満たすすべての運用環境は、適合を主張する PP 内のセキュリティ課題定義も満たす(次の項目の 1 つの例外を除く);

- 適合が主張されている PP の SPD への適合を実証するために必要とされる、適合を主張する PP 内の前提条件のセットのほかに、適合を主張する PP は、更に前提条件を特定することができる。ただし、これらの追加の前提条件が、適合が主張されている PP 内に定義されたセキュリティ課題定義から独立しており、影響を与えない場合に限る。更に詳しくは、適合が主張されている PP に従い、TOE によって対抗する必要のある TOE への脅威を除外する適合を主張する PP 内の前提条件はない。同様に、適合が主張されている PP に従い、TOE によって満たされることが意図されている、適合が主張されている PP 内に述べられた OSP の側面を実現した、適合を主張する PP 内の前提条件はない。

APE_CCL.1.9C ***適合主張根拠は、セキュリティ対策方針のステートメントが、適合が主張されている PP 内のセキュリティ対策方針のステートメントと一貫していることを実証しなければならない。***

APE_CCL.1-11 評価者は、セキュリティ対策方針のステートメントが、PP の適合ステートメントの定義に従って、PP のセキュリティ対策方針のステートメントと一貫していることを決定するために、適合主張根拠を***検査しなければならない。***

181 PP が別の PP に対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

182 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は次の状態であるかどうかを決定する:

- 適合が主張されている PP の TOE のセキュリティ対策方針のすべてが評価中の PP に含まれている。評価中の PP に TOE のセキュリティ対策方針を追加できる点に注意のこと;
- 適合を主張する PP 内の運用環境のセキュリティ対策方針は、次の 2 項目で説明される 2 つの例外を除き、適合が主張されている PP 内の運用環境のセキュリティ対策方針と同一である;
- 適合が主張されている PP からの運用環境のセキュリティ対策方針(またはそのようなセキュリティ対策方針の一部)は、TOE に対して述べられた同じセキュリティ対策方針(の一部)に置き換えられる;
- 新しいセキュリティ対策方針が、適合が主張されている PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている脅威(または脅威の一部)を軽減せず、適合が主張されている PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている OSP(または OSP の一部)を満たさないことを正当化する理由が示される場合、適合が主張されている PP 内に定義されたセキュリティ対策方針に運用環境のセキュリティ対策方針を追加することができる。

適合が主張されている PP から運用環境のセキュリティ対策方針を除外した、または、運用環境のセキュリティ対策方針を新しく追加した、他の PP への適合を主張する PP を検査する際、評価者は、上記の条件が満たされているかどうかを慎重に決定しなければならない。前述のワークユニットにおける前提条件の事例は、ここでも有効である。

183 適合が主張されている PP によって論証適合が要求されている場合、評価されている PP のセキュリティ対策方針のステートメントが、適合が主張されている PP 内のセキュリティ対策方針のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

184 このため、適合主張根拠は、適合を主張する PP 内のセキュリティ対策方針が、適合が主張されている PP 内のセキュリティ対策方針と同等(またはより制限的)であると実証する必要がある。これは、以下を意味する:

- 適合を主張する PP 内の TOE のセキュリティ対策方針を満たすすべての TOE は、適合が主張されている PP 内の TOE のセキュリティ対策方針も満たす;
- 適合が主張されている PP 内の運用環境のセキュリティ対策方針を満たすすべての運用環境は、適合を主張する PP 内の運用環境のセキュリティ対策方針も満たす(次の項目の 1 つの例外を除く);

- 適合が主張されている PP 内に定義されたセキュリティ対策方針のセットへの適合を実証するために使われる、適合を主張する PP 内の運用環境のセキュリティ対策方針のセットのほかに、適合を主張するPPは、更に運用環境のセキュリティ対策方針を特定することができる。ただし、これらのセキュリティ対策方針が、適合が主張されている PP 内に定義された、元々の TOE のセキュリティ対策方針のセットにも、運用環境のセキュリティ対策方針のセットにも影響しない場合に限る。

APE_CCL.1.10C ***適合主張根拠は、セキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントと一貫していることを実証しなければならない。***

APE_CCL.1-12 評価者は、PPの適合ステートメントによる定義に従って、適合が主張されているPPのすべてのセキュリティ要件と PP が一貫していることを決定するために、その PP を***検査しなければならない。***

185 PPが別のPPに対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

186 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は、評価中の PP 内のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントのスーパーセットであるか、またはその PP 内のセキュリティ要件のステートメントと同一であるかを決定する(正確適合の場合)。

187 適合が主張されている PP によって論証適合が要求されている場合、評価中の PP のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

188 次を参照のこと:

- SFR: 適合を主張するPP内の適合根拠は、適合を主張するPP内のSFRによって定義された要件の全体的なセットが、適合が主張されるPP内のSFRによって定義された要件の全体的なセットと同等（またはより制限的）であると実証しなければならない。これは、適合を主張するPP内のすべてのSFRのセットによって定義された要件を満たすすべての TOE が、適合が主張されている PP 内のすべての SFR のセットによって定義された要件も満たすことを意味する;

- SAR: 適合を主張するPPは、適合が主張されるPP内のすべてのSARを含まなければならないが、追加のSARを主張すること、または、SARをより上位階層のSARで置き換えることができる。適合を主張する PP 内の操作の完了は、適合が主張されている PP 内の操作の完了と一貫していなければならない; 適合が主張されているPP内と同じ完了が適合を主張するPP内でも使われるか、SARをより制限的にした完了（詳細化の規則が適用される）かのどちらかである。

APE_CCL.1.11C ***適合ステートメントは、PP に対する任意の PP/ST に必要とされる適合を、正確 PP 適合または論証 PP 適合として記述しなければならない。***

APE_CCL.1-13 評価者は、PP 適合ステートメントが正確 PP 適合または論証 PP 適合の主張を述べていることを***チェックしなければならない。***

9.5 セキュリティ課題定義(APE_SPD)

9.5.1 サブアクティビティの評価(APE_SPD.1)

9.5.1.1 目的

189 このサブアクティビティの目的は、TOE 及び TOE の運用環境によって対処されることが意図されているセキュリティ課題が明確に定義されていることを決定することである。

9.5.1.2 入力

190 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP

9.5.1.3 アクション APE_SPD.1.1E

APE_SPD.1.1C *セキュリティ課題定義は、脅威を記述しなければならない。*

APE_SPD.1-1 評価者は、セキュリティ課題定義が脅威を記述していることを*チェックしなければならない。*

191 セキュリティ対策方針が前提条件及び/または OSP からのみ派生するものである場合、脅威のステートメントを PP に提示する必要はない。この場合、このワークユニットは該当せず、満たされているものとみなされる。

192 評価者は、セキュリティ課題定義が TOE 及び/または TOE の運用環境によって対抗する必要がある脅威を記述していることを決定する。

APE_SPD.1.2C *すべての脅威は、脅威エージェント、資産、及び有害なアクションの観点から記述しなければならない。*

APE_SPD.1-2 評価者は、すべての脅威が脅威エージェント、資産、及び有害なアクションの観点から記述されていることを決定するために、セキュリティ課題定義を*検査しなければならない。*

193 セキュリティ対策方針が前提条件及び OSP からのみ派生するものである場合、脅威のステートメントを PP に提示する必要はない。この場合、このワークユニットは該当せず、満たされているものとみなされる。

194 脅威エージェントは、技能、資源、機会、及び動機などの側面によって、さらに詳細に記述することができる。

APE_SPD.1.3C *セキュリティ課題定義は、OSP を記述しなければならない。*

APE_SPD.1-3 評価者は、セキュリティ課題定義が OSP を記述していることを*検査しなければならない。*

195 セキュリティ対策方針が前提条件及び/または脅威からのみ派生するものである場合、OSP を PP に提示する必要はない。この場合、このワークユニットは該当せず、満たされているものとみなされる。

196 評価者は、TOE 及び/または TOE の運用環境が従う必要がある規則またはガイドラインの観点から OSP ステートメントが作成されることを決定する。

197 評価者は、各 OSP が明確に理解できるように十分な詳細が説明及び/または解釈が行われていることを決定する。セキュリティ対策方針の追跡を可能とするために方針ステートメントの明確な提示が必要である。

APE_SPD.1.4C ***セキュリティ課題定義は、TOE の運用環境についての前提条件を記述しなければならない。***

APE_SPD.1-4 評価者は、セキュリティ課題定義が TOE の運用環境についての前提条件を記述していることを決定するために、その定義を***検査しなければならない。***

198 前提条件がない場合、このワークユニットは、該当せず、満たされているものとみなされる。

199 評価者は、TOE の運用環境についてのそれぞれの前提条件が十分に詳細に説明されていて、消費者は各自の運用環境が前提条件と一致していることを決定できることを決定する。前提条件が明確に理解されていない場合、TOE がセキュアな方法で機能しない運用環境で使用される結果となる場合がある。

9.6 セキュリティ対策方針(APE_OBJ)

9.6.1 サブアクティビティの評価(APE_OBJ.1)

9.6.1.1 目的

200 このサブアクティビティの目的は、運用環境のセキュリティ対策方針が明確に定義されているかどうかを決定することである。

9.6.1.2 入力

201 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP

9.6.1.3 アクション APE_OBJ.1.1E

APE_OBJ.1.1C *セキュリティ対策方針のステートメントは、運用環境のセキュリティ対策方針を記述しなければならない。*

APE_OBJ.1-1 評価者は、セキュリティ対策方針のステートメントが運用環境のセキュリティ対策方針を定義していることを*チェックしなければならない。*

202 評価者は、運用環境のセキュリティ対策方針が識別されていることをチェックする。

9.6.2 サブアクティビティの評価(APE_OBJ.2)

9.6.2.1 目的

203 このサブアクティビティの目的は、セキュリティ対策方針が適切かつ完全にセキュリティ課題定義を扱うかどうか、及び TOE 及びその運用環境の間でのこの課題に対する分担が明確に定義されていることを決定することである。

9.6.2.2 入力

204 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP

9.6.2.3 アクション APE_OBJ.2.1E

APE_OBJ.2.1C *セキュリティ対策方針のステートメントは、TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針を記述しなければならない。*

APE_OBJ.2-1 評価者は、セキュリティ対策方針のステートメントが TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針を定義していることを*チェックしなければならない。*

205 評価者は、セキュリティ対策方針の両カテゴリが明確に識別されており、他のカテゴリから分離されていることをチェックする。

APE_OBJ.2.2C *セキュリティ対策方針根拠は、TOE の各セキュリティ対策方針をそのセキュリティ対策方針によって対抗される脅威及びそのセキュリティ対策方針によって実施される OSP までさかのぼらなければならない。*

APE_OBJ.2-2 評価者は、セキュリティ対策方針根拠が、対策方針によって対抗される脅威及び/または対策方針によって実施される OSP まで、TOE のセキュリティ対策方針のすべてをさかのぼることを***チェックしなければならない。***

206 TOE の各セキュリティ対策方針は、脅威と OSP のいずれか、あるいは脅威と OSP の組み合わせにまでさかのぼることができるが、少なくとも 1 つの脅威または OSP にまでさかのぼらなければならない。

207 さかのぼることに失敗した場合、セキュリティ対策方針根拠が不完全であるか、セキュリティ課題定義が不完全であるか、または TOE のセキュリティ対策方針が役立つ目的を持っていないことを示す。

APE_OBJ.2.3C ***セキュリティ対策方針根拠は、各運用環境セキュリティ対策方針をそのセキュリティ対策方針によって対抗される脅威、そのセキュリティ対策方針によって実施される OSP、及びそのセキュリティ対策方針によって充足される前提条件にまで、さかのぼらなければならない。***

APE_OBJ.2-3 評価者は、セキュリティ対策方針根拠が、セキュリティ対策方針によって対抗される脅威、セキュリティ対策方針によって実施される OSP、及びセキュリティ対策方針によって充足される前提条件にまで、運用環境のセキュリティ対策方針をさかのぼることを***チェックしなければならない。***

208 運用環境の各セキュリティ対策方針は、脅威、OSP、前提条件、あるいは脅威、OSP、及び/または前提条件の組み合わせにまでさかのぼることができるが、少なくとも 1 つの脅威、OSP、または前提条件にまでさかのぼらなければならない。

209 さかのぼることに失敗した場合、セキュリティ対策方針根拠が不完全であるか、セキュリティ課題定義が不完全であるか、または運用環境のセキュリティ対策方針が役立つ目的を持っていないことを示す。

APE_OBJ.2.4C ***セキュリティ対策方針根拠は、セキュリティ対策方針がすべての脅威に対抗することを実証しなければならない。***

APE_OBJ.2-4 評価者は、各脅威について、セキュリティ対策方針がその脅威に対抗するために適していることをセキュリティ対策方針根拠が正当化していると決定するために、その根拠を***検査しなければならない。***

210 脅威にまでさかのぼるセキュリティ対策方針が一つもない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

211 評価者は、脅威に対する正当化が脅威の除去、軽減、または緩和が行われたかどうかを示すことを決定する。

212 評価者は、脅威に対する正当化が、セキュリティ対策方針が十分である(つまり、脅威にまでさかのぼるすべてのセキュリティ対策方針が達成される場合、脅威は除去されるか、十分に軽減されるか、脅威の影響が十分に緩和される)ことを実証することを決定する。

213 セキュリティ対策方針根拠において提供される脅威に対するセキュリティ対策方針からの追跡は、正当化の一部である場合があるが、それ自体では正当化を構成しないことに注意すること。セキュリティ対策方針が、特定の脅威が実現されることを妨げる意図を反映しただけのステートメントである場合であっても、正当化が必要であるが、この正当化は「セキュリティ対策方針 X が脅威 Y に直接対抗する」のように最小になる可能性がある。

214 評価者は、脅威にまでさかのぼる各セキュリティ対策方針が必要である(つまり、セキュリティ対策方針が達成される場合、それは実際に脅威の除去、軽減、または緩和に寄与する)ことも決定する。

APE_OBJ.2.5C ***セキュリティ対策方針根拠は、セキュリティ対策方針がすべての OSP を実施することを実証しなければならない。***

APE_OBJ.2-5 評価者は、各 OSP に対して、セキュリティ対策方針がその OSP を実施するために適していることをセキュリティ対策方針根拠が正当化していること決定するために、その根拠を***検査しなければならない。***

215 OSP にまでさかのぼるセキュリティ対策方針が一つもない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

216 評価者は、OSP に対する正当化が、セキュリティ対策方針が十分である(つまり、その OSP にまでさかのぼるすべてのセキュリティ対策方針が達成される場合、OSP は実施される)ことを実証することを決定する。

217 評価者は、OSP にまでさかのぼる各セキュリティ対策方針が必要である(つまり、セキュリティ対策方針が達成される場合、それは実際に OSP の実施に寄与する)ことも決定する。

218 セキュリティ対策方針根拠において提供される OSP に対するセキュリティ対策方針からの追跡は、正当化の一部である場合があるが、それだけでは正当化を構成しないことに注意すること。セキュリティ対策方針が、特定の OSP を実施する意図を反映しただけのステートメントである場合、正当化が必要であるが、この正当化は「セキュリティ対策方針 X が OSP Y を直接実施する」のように最小になる可能性がある。

APE_OBJ.2.6C ***セキュリティ対策方針根拠は、運用環境のセキュリティ対策方針がすべての前提条件を充足することを実証しなければならない。***

APE_OBJ.2-6 評価者は、運用環境に対する各前提条件について、運用環境のセキュリティ対策方針がその前提条件を充足するのに適していることを示す適切な正当化を、セキュリティ対策方針根拠が含んでいることを決定するために、その根拠を***検査しなければならない。***

219 運用環境のセキュリティ対策方針が前提条件にまでさかのぼることができない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

220 評価者は、TOE の運用環境に関する前提条件に対する正当化が、セキュリティ対策方針が十分である(つまり、前提条件にまでさかのぼるすべての運用環境のセキュリティ対策方針が達成される場合、運用環境は前提条件を充足する)ことを実証することを決定する。

221 評価者は、TOE の運用環境に関する前提条件にまでさかのぼる運用環境の各セキュリティ対策方針が必要である(つまり、セキュリティ対策方針が達成される場合、それは前提条件を充足する運用環境に寄与する)ことも決定する。

222 セキュリティ対策方針根拠において記述される、前提条件に対する運用環境のセキュリティ対策方針からの追跡は、正当化の一部である場合があるが、それだけでは正当化を構成しないことに注意すること。運用環境のセキュリティ対策方針が、前提条件の単なる再記述である場合であっても、正当化が必要であるが、この正当化は「セキュリティ対策方針 X は前提条件 Y を直接充足する」のように最小になる可能性がある。

9.7 拡張コンポーネント定義(APE_ECD)

9.7.1 サブアクティビティの評価(APE_ECD.1)

9.7.1.1 目的

223 このサブアクティビティの目的は、拡張コンポーネントが明確に、曖昧さなく定義されているかどうか、及びそれが必要であるかどうか、つまり既存の CC パート 2 または CC パート 3 のコンポーネントを使用して明確に表現される可能性がないかどうかを決定することである。

9.7.1.2 入力

224 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP

9.7.1.3 アクション APE_ECD.1.1E

APE_ECD.1.1C ***セキュリティ要件のステートメントは、すべての拡張セキュリティ要件を識別しなければならない。***

APE_ECD.1-1 評価者は、拡張要件として識別されていないセキュリティ要件のステートメントにおけるすべてのセキュリティ要件は、CC パート 2 または CC パート 3 で示されていることを***チェックしなければならない。***

APE_ECD.1.2C ***拡張コンポーネント定義は、各拡張セキュリティ要件に対応する拡張コンポーネントを定義しなければならない。***

APE_ECD.1-2 評価者は、拡張コンポーネント定義が各拡張セキュリティ要件に対応する拡張コンポーネントを定義することを***チェックしなければならない。***

225 PP に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

226 単一の拡張コンポーネントは、拡張セキュリティ要件の複数の繰返しを定義するために使用することができ、各繰返しに対してこの定義を繰返す必要はない。

APE_ECD.1.3C ***拡張コンポーネント定義は、各拡張コンポーネントが既存の CC コンポーネント、ファミリ、及びクラスにどのように関連するかを記述しなければならない。***

APE_ECD.1-3 評価者は、各拡張コンポーネントが既存の CC コンポーネント、ファミリ、及びクラスにどのようにあてはまるかを拡張コンポーネント定義が記述していることを決定するために、その拡張コンポーネント定義を***検査しなければならない。***

227 PP に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

228 評価者は、各拡張コンポーネントが次のいずれかであることを決定する:

a) 既存の CC パート 2 または CC パート 3 ファミリのメンバ、または

b) PP で定義された新しいファミリのメンバ。

229 拡張コンポーネントが既存の CC パート 2 または CC パート 3 ファミリのメンバである場合、評価者は、拡張コンポーネントがそのファミリのメンバであるべき理由、及びそのファミリの他のコンポーネントにどのように関連しているかを拡張コンポーネント定義が適切に記述していることを決定する。

230 拡張コンポーネントが PP で定義された新しいファミリのメンバである場合、評価者は、拡張コンポーネントが既存のファミリにあてはまらないことを確認する。

231 PP が新しいファミリを定義している場合、評価者は各新しいファミリが次のいずれかであることを決定する:

a) 既存の CC パート 2 または CC パート 3 クラスのメンバ、または

b) PP で定義された新しいクラスのメンバ。

232 ファミリが既存の CC パート 2 または CC パート 3 クラスのメンバである場合、評価者は、ファミリがそのクラスのメンバであるべき理由、及びファミリがそのクラス内の他のファミリにどのように関連するかを拡張コンポーネント定義が適切に記述していることを決定する。

233 ファミリが PP で定義された新しいクラスのメンバである場合、評価者は、ファミリが既存のクラスに対して適切ではないことを確認する。

APE_ECD.1-4 評価者は、拡張コンポーネントの各定義がそのコンポーネントのすべての適用可能な依存性を識別することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

234 PP に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

235 評価者は、PP 作成者が見過ごした適用可能な依存性が一つもないことを確認する。

APE_ECD.1.4C ***拡張コンポーネント定義は、提示モデルとして既存の CC コンポーネント、ファミリ、クラス、及び方法を使用しなければならない。***

APE_ECD.1-5 評価者は、各拡張機能コンポーネントが提示モデルとして既存の CC パート 2 コンポーネントを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

236 PP に拡張 SFR が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

237 評価者は、拡張機能コンポーネントが CC パート 2、7.1.3 節、「コンポーネント構造」と一貫していることを決定する。

238 拡張機能コンポーネントが操作を使用する場合、評価者は、拡張機能コンポーネントが CC パート 1、8.1 節、「操作」と一貫していることを決定する。

239 拡張機能コンポーネントが既存の機能コンポーネントを下位階層とする場合、評価者は、拡張機能コンポーネントが CC パート 2、7.2.1 節、「コンポーネント変更の強調表示」と一貫していることを決定する。

APE_ECD.1-6 評価者は、新しい機能ファミリの各定義が提示モデルとして既存の CC 機能ファミリを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

240 PP が新しい機能ファミリを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

241 評価者は、すべての新しい機能ファミリが CC パート 2、7.1.2 節、「ファミリ構造」と一貫するように定義されていることを決定する。

APE_ECD.1-7 評価者は、新しい機能クラスの各定義が提示モデルとして既存の CC 機能クラスを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

242 PP が新しい機能クラスを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

243 評価者は、すべての新しい機能クラスが CC パート 2、7.1.1 節、「クラス構造」と一貫するように定義されていることを決定する。

APE_ECD.1-8 評価者は、拡張保証コンポーネントの各定義が提示モデルとして既存の CC パート 3 コンポーネントを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

244 PP に拡張 SAR が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

245 評価者は、拡張保証コンポーネントが CC パート 3、7.1.3 節、「保証コンポーネント構造」と一貫していることを決定する。

246 拡張保証コンポーネントが操作を使用する場合、評価者は、拡張保証コンポーネントが CC パート 1、8.1 節、「操作」と一貫していることを決定する。

247 拡張保証コンポーネントが既存の保証コンポーネントを下位階層とする場合、評価者は、拡張保証コンポーネントが CC パート 3、7.1.3 節、「保証コンポーネント構造」と一貫していることを決定する。

APE_ECD.1-9 評価者は、定義された各拡張保証コンポーネントに対して、適用可能な方法が提供されたことを決定するために、拡張コンポーネント定義を***検査しなければならない。***

248 PP に拡張 SAR が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

249 評価者は、各拡張 SAR の各評価者アクションエレメントについて、1 つまたは複数のワークユニットが提供されており、指定された評価者アクションエレメントに対するすべてのワークユニットを成功裏に実行することによりそのエレメントが達成されたことが実証されることを決定する。

APE_ECD.1-10 評価者は、新しい保証ファミリの各定義が提示モデルとして既存の CC 保証ファミリを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

250 PP が新しい保証ファミリを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

251 評価者は、すべての新しい保証ファミリが CC パート 3、7.1.2 節、「保証ファミリの構造」と一貫するように定義されていることを決定する。

APE_ECD.1-11 評価者は、新しい保証クラスの各定義が提示モデルとして既存の CC 保証クラスを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

252 PP が新しい保証クラスを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

253 評価者は、すべての新しい保証クラスが CC パート 3、7.1.1 節、「保証クラス構造」と一貫するように定義されていることを決定する。

APE_ECD.1.5C ***拡張コンポーネントは、エレメントに対する適合または非適合を実証できるように、評価可能で客観的なエレメントで構成されていなければならない。***

APE_ECD.1-12 評価者は、適合または非適合を実証できるように、各拡張コンポーネントの各エレメントが評価可能であり、客観的な評価要件を述べることを決定するために、拡張コンポーネント定義を***検査しなければならない。***

254 PP に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

255 評価者は、拡張機能コンポーネントのエレメントがテスト可能であり、適切な TSF 表現を通じて追跡可能である方法で述べられていることを決定する。

256 評価者は、拡張保証コンポーネントのエレメントが評価者の主観的な判定を必要としないことも決定する。

257 評価者は、評価可能で客観的であることがすべての評価基準に対して適切であるにもかかわらず、このような特性を証明するための正式な方法が存在しないことは周知の事実であることに留意する。このため、既存の CC 機能コンポーネント及び保証コンポーネントは、この要件に従って構成するものを決定するためのモデルとして使用される。

9.7.1.4 アクション APE_ECD.1.2E

APE_ECD.1-13 評価者は、各拡張コンポーネントが既存のコンポーネントを使用して明確に表現できないことを決定するために、拡張コンポーネント定義を***検査しなければならない。***

258 PP に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

259 評価者は、この決定を行うときに、CC パート 2 及び CC パート 3 からのコンポーネント、PP で定義された他の拡張コンポーネント、これらのコンポーネントの組み合わせ、及びこれらのコンポーネントに対して可能な操作を考慮するべきである。

260 評価者は、このワークユニットの役割は、コンポーネントの不要な重複、つまり、他のコンポーネントを使用して明確に表現できるコンポーネントを排除することであることに留意する。評価者は、既存のコンポーネントを使用して拡張コンポーネントを表現する方法を探す試みとして、操作を含むコンポーネントのすべての可能な組み合わせに対する徹底的探索を行うべきではない。

9.8 セキュリティ要件(APE_REQ)

9.8.1 サブアクティビティの評価(APE_REQ.1)

9.8.1.1 目的

261 このサブアクティビティの目的は、SFR と SAR が明確で曖昧さがなく十分に定義されているかどうか、及び SFR と SAR が内部的に一貫しているかどうかを決定することである。

9.8.1.2 入力

262 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP

9.8.1.3 アクション APE_REQ.1.1E

APE_REQ.1.1C *セキュリティ要件のステートメントは SFR 及び SAR を記述しなければならない。*

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

263 評価者は、各 SFR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 2 の個別のコンポーネントに対する参照によって;

b) PP の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) PP が適合を主張する PP に対する参照によって;

d) PP が適合を主張するセキュリティ要件パッケージに対する参照によって;

e) PP での再現によって。

264 すべての SFR に対して同じ識別手段を使用する必要はない。

APE_REQ.1-2 評価者は、セキュリティ要件のステートメントが SAR を記述していることを***チェックしなければならない。***

265 評価者は、各 SAR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 3 の個別のコンポーネントに対する参照によって;

b) PP の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) PP が適合を主張する PP に対する参照によって;

d) PP が適合を主張するセキュリティ要件パッケージに対する参照によって;

e) PP での再現によって。

266 すべての SAR に対して同じ識別手段を使用する必要はない。

APE_REQ.1.2C ***SFR とSAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語が定義されなければならない。***

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

267 評価者は、PP が以下のすべてを定義することを決定する:

- SFR で使用されるサブジェクトとオブジェクト(の種別);
- サブジェクト、利用者、オブジェクト、情報、セッション、及び/または資源のセキュリティ属性(の種別)、これらの属性が取りうる値、及びこれらの値間の関係(例えば、トップシークレット(top_secret)の値は秘密(secret)の値より「高い」);
- SFR で使用される操作(の種別)及びこれらの操作の影響;
- SFR 内の外部エンティティ(の種別);
- 操作を完了することにより SFR 及び/または SAR に導入された他の用語のうち、直ちに理解されないか、またはそれぞれの辞書の定義の範囲外で使用されている用語。

268 このワークユニットの目的は、SFR と SAR が明確に定義されており、曖昧な用語の導入によって誤解が発生しないことを保証することである。このワークユニットは、PP 作成者に強制的に各単語を定義させるなどの極端な方法として、解釈されるべきではない。セキュリティ要件のセットの一般的な読者は、IT、セキュリティ、及びコモンクライテリアに関する適度な知識を持っているものと想定されるべきである。

269 上記のすべては、グループ、クラス、役割、種別によって提示したり、理解しやすくなるようなその他のグループ化または特性化によって提示したりすることができる。

270 評価者は、これらの列挙と定義をセキュリティ要件の一部にする必要はなく、別の節に(一部または全体が)配置される可能性があることに留意する。これは、特に、同じ用語が PP の残りの部分で使用される場合に該当する。

APE_REQ.1.3C ***セキュリティ要件のステートメントは、セキュリティ要件のすべての操作を識別しなければならない。***

APE_REQ.1-4 評価者は、セキュリティ要件のステートメントがセキュリティ要件のすべての操作を識別することを***チェックしなければならない。***

271 評価者は、すべての操作が、使用される各 SFR または SAR 内で識別されていることを決定する。これには、完了した操作と未完了の操作の両方が含まれる。識別は、活字印刷上の区別、周辺の文章内での明示的な識別、またはその他の特徴的な手段で達成できる。

APE_REQ.1.4C ***すべての操作は正しく実行しなければならない。***

APE_REQ.1-5 評価者は、すべての割付操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

272 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.1-6 評価者は、すべての繰返し操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

273 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.1-7 評価者は、すべての選択操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

274 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.1-8 評価者は、すべての詳細化操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

275 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.1.5C ***セキュリティ要件の各依存性が満たされていなければならない。また、満たされない依存性がある場合は、セキュリティ要件根拠によってそのことが正当化されなければならない。***

APE_REQ.1-9 評価者は、セキュリティ要件の各依存性が満たされていること、または満たされていない依存性をセキュリティ要件根拠が正当化することを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

276 依存性は、セキュリティ要件のステートメント内の関連するコンポーネント(またはそれに対して上位階層のコンポーネント)を含めることによって満たされる。依存性を満たすために使用されたコンポーネントは、必要に応じて、実際に依存性を満たすことを保証するために、操作によって変更するべきである。

277 依存性が満たされないことの正当化は、次のいずれかを取り扱うべきである:

a) 依存性が必要でないまたは役立たない理由。この場合、それ以上に詳細な情報は不要;または

b) 依存性が TOE の運用環境によって対処されていること。この場合、運用環境のセキュリティ対策方針がこの依存性をどのように対処するかを正当化によって記述するべきである。

APE_REQ.1.6C ***セキュリティ要件のステートメントは、内部的に一貫していなければならない。***

APE_REQ.1-10 評価者は、セキュリティ要件のステートメントが内部的に一貫していることを決定するために、そのステートメントを***検査しなければならない。***

278 評価者は、すべての SFR と SAR の組み合わされたセットが内部的に一貫していることを決定する。

279 評価者は、異なるセキュリティ要件が同じ種別の開発者の証拠、事象、操作、データ、実行されるテストなどに対して適用されるか、"すべてのオブジェクト"、"すべてのサブジェクト"などに対して適用されるすべての場合において、これらの要件が競合しないことを決定する。

280 いくつかの考えられる競合は、次のとおりである:

a) 特定の暗号アルゴリズムの設計を秘密に保持することを特定する拡張 SAR、及びオープンソースレビューを特定する別の拡張 SAR;

b) サブジェクト識別情報のログ記録を特定する FAU_GEN.1 監査データ生成、これらのログにアクセスできる利用者を特定する FDP_ACC.1 サブセットアクセス制御、及びサブジェクトの一部のアクションが他のサブジェクトに対して観察不能であるべきであることを特定する FPR_UNO.1 観察不能性。あるアクティビティを参照できるべきではないサブジェクトがこのアクティビティのログにアクセスできる場合、これらの SFR は競合する;

c) 不要になった情報の削除を特定する FDP_RIP.1 サブセット残存情報保護、及び TOE を前の状態に戻すことができることを特定する FDP_ROL.1 基本ロールバック。前の状態へのロールバックに必要な情報が削除されている場合、これらの要件は競合する;

d) 特に一部の繰返しが同じサブジェクト、オブジェクト、または操作を扱う場合の、FDP_ACC.1 サブセットアクセス制御の複数の繰返し。1 つのアクセス制御 SFR がサブジェクトによるオブジェクトに対する操作の実行を許可し、別のアクセス制御 SFR がこれを許可しない場合、これらの要件は競合する。

9.8.2 サブアクティビティの評価(APE_REQ.2)

9.8.2.1 目的

281 このサブアクティビティの目的は、SFR と SAR が明確で曖昧さがなく十分に定義されているかどうか、SFR と SAR が内部的に一貫しているかどうか、及び SFR が TOE のセキュリティ対策方針を満たしているかどうかを決定することである。

9.8.2.2 入力

282 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP

9.8.2.3 アクション APE_REQ.2.1E

APE_REQ.2.1C *セキュリティ要件のステートメントは SFR 及び SAR を記述しなければならない。*

APE_REQ.2-1 評価者は、セキュリティ要件のステートメントが SFR を記述していることを*チェックしなければならない。*

283 評価者は、各 SFR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 2 の個別のコンポーネントに対する参照によって;

b) PP の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) PP が適合を主張する PP 内の個別のコンポーネントに対する参照によって;

d) PP が適合を主張するセキュリティ要件パッケージ内の個別のコンポーネントに対する参照によって;

e) PP での再現によって。

284 すべての SFR に対して同じ識別手段を使用する必要はない。

APE_REQ.2-2 評価者は、セキュリティ要件のステートメントが SAR を記述していることを***チェックしなければならない。***

285 評価者は、各 SAR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 3 の個別のコンポーネントに対する参照によって;

b) PP の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) PP が適合を主張する PP 内の個別のコンポーネントに対する参照によって;

d) PP が適合を主張するセキュリティ要件パッケージ内の個別のコンポーネントに対する参照によって;

e) PP での再現によって。

286 すべての SAR に対して同じ識別手段を使用する必要はない。

APE_REQ.2.2C ***SFR と SAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語が定義されなければならない。***

APE_REQ.2-3 評価者は、SFR 及び SAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語が定義されていることを決定するために、PP を***検査しなければならない。***

287 評価者は、PP が以下のすべてを定義することを決定する:

- SFR で使用されるサブジェクトとオブジェクト(の種別);
- サブジェクト、利用者、オブジェクト、情報、セッション、及び/または資源のセキュリティ属性(の種別)、これらの属性が取りうる値、及びこれらの値間の関係(例えば、トップシークレット(top_secret)の値は秘密(secret)の値より「高い」);
- SFR で使用される操作(の種別)及びこれらの操作の影響;
- SFR 内の外部エンティティ(の種別);
- 操作を完了することにより SFR 及び/または SAR に導入された他の用語のうち、直ちに理解されないか、またはそれぞれの辞書の定義の範囲外で使用されている用語。

288 このワークユニットの目的は、SFR と SAR が明確に定義されており、曖昧な用語の導入によって誤解が発生しないことを保証することである。このワークユニットは、PP 作成者に強制的に各単語を定義させるなどの極端な方法として、解釈されるべきではない。セキュリティ要件のセットの一般的な読者は、IT、セキュリティ、及びコモンクライテリアに関する適度な知識を持っているものと想定されるべきである。

289 上記のすべては、グループ、クラス、役割、種別によって提示したり、理解しやすくなるようなその他のグループ化または特性化によって提示したりすることができる。

290 評価者は、これらの列挙と定義をセキュリティ要件の一部にする必要はなく、別の節に(一部または全体が)配置される可能性があることに留意する。これは、特に、同じ用語が PP の残りの部分で使用される場合に該当する。

APE_REQ.2.3C *セキュリティ要件のステートメントは、セキュリティ要件のすべての操作を識別しなければならない。*

APE_REQ.2-4 評価者は、セキュリティ要件のステートメントがセキュリティ要件のすべての操作を識別することを*チェックしなければならない。*

291 評価者は、すべての操作が、使用される各 SFR または SAR 内で識別されていることを決定する。これには、完了した操作と未完了の操作の両方が含まれる。識別は、活字印刷上の区別、周辺の文章内での明示的な識別、またはその他の特徴的な手段で達成できる。

APE_REQ.2.4C *すべての操作は正しく実行しなければならない。*

APE_REQ.2-5 評価者は、すべての割付操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを*検査しなければならない。*

292 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.2-6 評価者は、すべての繰返し操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを*検査しなければならない。*

293 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.2-7 評価者は、すべての選択操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを*検査しなければならない。*

294 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.2-8 評価者は、すべての詳細化操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを*検査しなければならない。*

295 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

APE_REQ.2.5C *セキュリティ要件の各依存性が満たされていなければならない。また、満たされない依存性がある場合は、セキュリティ要件根拠によってそのことが正当化されなければならない。*

APE_REQ.2-9 評価者は、セキュリティ要件の各依存性が満たされていること、または満たされていない依存性をセキュリティ要件根拠が正当化することを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

296 依存性は、セキュリティ要件のステートメント内の関連するコンポーネント(またはそれに対して上位階層のコンポーネント)を含めることによって満たされる。依存性を満たすために使用されたコンポーネントは、必要に応じて、実際に依存性を満たすことを保証するために、操作によって変更するべきである。

297 依存性が満たされないことの正当化は、次のいずれかを取り扱うべきである:

a) 依存性が必要でないまたは役立たない理由。この場合、それ以上に詳細な情報は不要; または

b) 依存性が TOE の運用環境によって対処されていること。この場合、運用環境のセキュリティ対策方針がこの依存性をどのように対処するかを正当化によって記述するべきである。

APE_REQ.2.6C ***セキュリティ要件根拠は、各 SFR を TOE のセキュリティ対策方針にまでさかのぼらなければならない。***

APE_REQ.2-10 評価者は、セキュリティ要件根拠が各 SFR を TOE のセキュリティ対策方針にまでさかのぼることを***チェックしなければならない。***

298 評価者は、各 SFR が少なくとも 1 つの TOE のセキュリティ対策方針にまでさかのぼることを決定する。

299 さかのぼることに失敗した場合、セキュリティ要件根拠が不完全であるか、TOE のセキュリティ対策方針が不完全であるか、または SFR が役立つ目的を持っていないことを示す。

APE_REQ.2.7C ***セキュリティ要件根拠は、SFR が TOE のセキュリティ対策方針のすべてを満たすことを実証しなければならない。***

APE_REQ.2-11 評価者は、TOE の各セキュリティ対策方針について、SFR がその TOE のセキュリティ対策方針を満たすために適していることをセキュリティ要件根拠が正当化することを決定するために、セキュリティ要件根拠を***検査しなければならない。***

300 TOE のセキュリティ対策方針にまでさかのぼる SFR が一つもない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

301 評価者は、TOE のセキュリティ対策方針に対する正当化が、SFR が十分である(つまり、対策方針にまでさかのぼるすべての SFR が満たされている場合、TOE のセキュリティ対策方針は達成される)ことを実証することを決定する。

302 TOE のセキュリティ対策方針にまでさかのぼる SFR が、未完了の割付、あるいは未完了または制限された選択を持っている場合、評価者は、これらの操作の考えられる個別の完了または完了の組み合わせについて、セキュリティ対策方針がまだ満たされていることを決定する。

303 評価者は、TOE のセキュリティ対策方針にまでさかのぼる各 SFR が必要である(つまり、SFR が満たされている場合、それは実際にセキュリティ対策方針の達成に寄与する)ことも決定する。

304 セキュリティ要件根拠において提供される TOE のセキュリティ対策方針に対する SFR からの追跡は、正当化の一部である場合があるが、それだけでは正当化を構成しないことに注意すること。

APE_REQ.2.8C ***セキュリティ要件根拠は、なぜ SAR が選ばれたかを説明しなければならない。***

APE_REQ.2-12 評価者は、セキュリティ要件根拠が、SAR が選ばれた理由を説明していることを***チェックしなければならない。***

305 評価者は、説明が理路整然としており、PP の残りの部分との明白な不一致が SAR 及び説明に含まれていない限り、いかなる説明も正しいことに留意する。

306 SAR と PP の残りの部分との明白な不一致の例として、非常に能力の高い脅威エージェントが含まれているにもかかわらず、このような脅威エージェントから保護しない AVA_VAN SAR が選ばれた場合が挙げられる。

APE_REQ.2.9C ***セキュリティ要件のステートメントは、内部的に一貫していなければならない。***

APE_REQ.2-13 評価者は、セキュリティ要件のステートメントが内部的に一貫していることを決定するために、そのステートメントを***検査しなければならない。***

307 評価者は、すべての SFR と SAR の組み合わされたセットが内部的に一貫していることを決定する。

308 評価者は、異なるセキュリティ要件が同じ種別の開発者の証拠、事象、操作、データ、実行されるテストなどに対して適用されるか、"すべてのオブジェクト"、"すべてのサブジェクト"などに対して適用されるすべての場合において、これらの要件が競合しないことを決定する。

309 いくつかの考えられる競合は、次のとおりである:

a) 特定の暗号アルゴリズムの設計を秘密に保持することを特定する拡張 SAR、及びオープンソースレビューを特定する別の拡張 SAR;

b) サブジェクト識別情報のログ記録を特定する FAU_GEN.1 監査データ生成、これらのログにアクセスできる利用者を特定する FDP_ACC.1 サブセットアクセス制御、及びサブジェクトの一部のアクションが他のサブジェクトに対して観察不能であるべきであることを特定する FPR_UNO.1 観察不能性。あるアクティビティを参照できるべきではないサブジェクトがこのアクティビティのログにアクセスできる場合、これらの SFR は競合する;

c) 不要になった情報の削除を特定する FDP_RIP.1 サブセット残存情報保護、及び TOE を前の状態に戻すことができることを特定する FDP_ROL.1 基本ロールバック。前の状態へのロールバックに必要な情報が削除されている場合、これらの要件は競合する;

d) 特に一部の繰返しが同じサブジェクト、オブジェクト、または操作を扱う場合の、FDP_ACC.1 サブセットアクセス制御の複数の繰返し。1 つのアクセス制御 SFR がサブジェクトによるオブジェクトに対する操作の実行を許可し、別のアクセス制御 SFR がこれを許可しない場合、これらの要件は競合する。

10 ACE クラス: プロテクションプロファイル構成評価

10.1 序説

310 PP モジュールで参照されるすべての基本 PP は、PP 構成の評価の前に評価されなければならない。

311 PP 構成を評価する一つの可能性は、PP 構成を構成する PP 及び PP モジュールのすべてのコンポーネントをフラット化し、その結果の PP を標準 PP として評価することである。

312 複数の PP モジュールによって構成される PP 構成を、PP モジュールごとに評価するというもう一つの可能性もある。プロテクションプロファイル Pi と PP モジュール Mj から構成される PP 構成を例にとると、PP 構成の評価は、図 6 に示されるように、以下のステップで進める:

a) 最初にプロテクションプロファイル P_i をすべて個別に評価する;

b) PP モジュール M_1 とプロテクションプロファイル P_i から構成される PP 構成 C_1 を評価する;

c) PP モジュール M_{i+1} と標準 PP として見なされる PP 構成 C_i から構成される、PP 構成 C_{i+1} を評価する(CC パート 1 の B.13 節を参照のこと);

d) すべての PP モジュールについてステップ c)[1]を繰返す。

313 ステップ b)及び c)[2]は、それぞれ以下の 2 つのステップで実行される:

a) 基本 PP と PP モジュールの評価 (サブアクティビティの評価(ACE_MCO.1))

b) PP 構成のほかのエレメントへの評価(一貫性評定)の拡大 (サブアクティビティの評価(ACE_CCO.1))

【訳注】[1] 原文では、「step 3」 と記述されている。

【訳注】[2] 原文では、「Steps 2 and 3」 と記述されている。

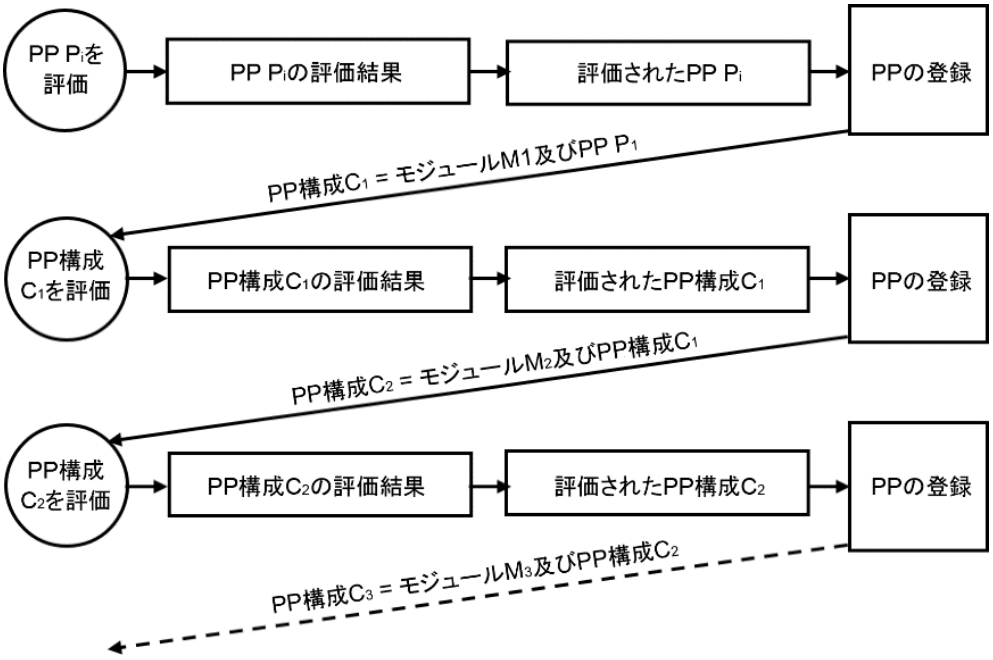

図 6 - PP 構成の評価

314 ACE 評価方法は、APE の評価方法に基づいている。共通する部分は、この文書には重複されていないが、参照される。

10.2 PP モジュール概説 (ACE_INT)

10.2.1 サブアクティビティの評価 (ACE_INT.1)

10.2.1.1 目的

315 このサブアクティビティの目的は、PP モジュールが正しく識別されているかどうか、及び基本 PP と TOE 概要が相互に一貫しているかどうかを決定することである。

10.2.1.2 入力

316 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP モジュール;

b) その基本 PP。

10.2.1.3 適用上の注釈

317 *APE_INT.1.1E のすべてのアクションが適用される。*

10.2.1.4 アクション ACE_INT.1.1E

ACE_INT.1.1C ***PP モジュール概説は、CC パート1 の B.14.3.2 節に従って、その論理構造と PP モジュールとの関係を含め、PP モジュールが依存するすべての基本 PP を一意に識別しなければならない。***

ACE_INT.1-1 評価者は、PP モジュール概説が、PP モジュールが依存する基本 PP を識別することを ***チェックしなければならない。***

ACE_INT.1.2C ***TOE 概要は、その基本 PP の TOE 概要に関して、PP モジュールによって導入される違いを識別しなければならない。***

ACE_INT.1-2 評価者は、TOE 概要が、その基本 PP の TOE 概要に関して、PP モジュールによって導入される違いを識別することを ***チェックしなければならない。***

10.3 PP モジュール適合主張 (ACE_CCL)

10.3.1 サブアクティビティの評価 (ACE_CCL.1)

10.3.1.1 目的

318 このサブアクティビティの目的は、様々な適合主張の有効性を決定することである。これらは、PP モジュールが CC パート 2 及び SFR パッケージに対してどのように適合しているかを記述する。

10.3.1.2 入力

319 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP モジュール;

b) PP が適合を主張する SFR パッケージ。

10.3.1.3 アクション ACE_CCL.1.1E

ACE_CCL.1.1C ***適合主張は、PP モジュールが適合を主張する CC のバージョンを識別する CC 適合主張を含めなければならない。***

ACE_CCL.1-1 評価者は、PP モジュールが適合を主張する CC のバージョンを識別する CC 適合主張が適合主張に含まれていることを***チェックしなければならない。***

320 評価者は、この PP モジュールを開発するために使用された CC のバージョンを CC 適合主張が識別することを決定する。これには、CC のバージョン番号を含めるべきであり、また、CC の国際的な英語バージョンが使用されなかった場合は、使用された CC のバージョンの言語も含めるべきである。

ACE_CCL.1.2C ***CC 適合主張は、CC パート 2 に対する PP モジュールの適合を CC パート 2 適合または CC パート 2 拡張として記述しなければならない。***

ACE_CCL.1-2 評価者は、CC 適合主張が PP モジュールに対する CC パート 2 適合または CC パート 2 拡張の主張を述べていることを***チェックしなければならない。***

ACE_CCL.1.3C ***適合主張は、PP モジュールが適合を主張するセキュリティ機能要件パッケージをすべて識別しなければならない。***

ACE_CCL.1-3 評価者は、PP モジュールが適合を主張するセキュリティ機能要件パッケージのすべてを識別するパッケージ主張が適合主張に含まれていることを***チェックしなければならない。***

321 PP モジュールがセキュリティ機能要件パッケージへの適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

322 評価者は、参照されるセキュリティ機能要件パッケージが曖昧さなく(例えば、タイトル及びバージョン番号、またはセキュリティ機能要件パッケージの概説に含まれている識別によって)識別されることを決定する。

323 評価者は、セキュリティ機能要件パッケージへの部分的な適合の主張は許可されないことに留意する。

ACE_CCL.1.4C ***CC 適合主張は、拡張コンポーネント定義と一貫していなければならない。***

ACE_CCL.1-4 評価者は、CC パート 2 に対する CC 適合主張が拡張コンポーネント定義と一貫していることを決定するために CC 適合主張を***検査しなければならない。***

324 CC 適合主張が CC パート 2 適合を含んでいる場合、評価者は、拡張コンポーネント定義が機能コンポーネントを定義しないことを決定する。

325 CC 適合主張が CC パート 2 拡張を含んでいる場合、評価者は、拡張コンポーネント定義が拡張機能コンポーネントを少なくとも 1 つは定義していることを決定する。

10.4 PP モジュールセキュリティ課題定義 (ACE_SPD)

10.4.1 サブアクティビティの評価 (ACE_SPD.1)

10.4.1.1 適用上の注釈

326 *APE_SPD.1.1E のすべてのアクションが適用される。*

10.5 PP モジュールセキュリティ対策方針 (ACE_OBJ)

10.5.1 サブアクティビティの評価 (ACE_OBJ.1)

10.5.1.1 適用上の注釈

327 *APE_OBJ.2.1E のすべてのアクションが適用される。*

10.6 PP モジュール拡張コンポーネント定義 (ACE_ECD)

10.6.1 サブアクティビティの評価 (ACE_ECD.1)

10.6.1.1 適用上の注釈

328 *APE_ECD.1.1E 及び APE_ECD.1.2E のすべてのアクションが適用される。*[3]

【訳注】[3] 原文では「APE_ECD.1.1E」のみ。

10.7 PP モジュールセキュリティ要件 (ACE_REQ)

10.7.1 サブアクティビティの評価 (ACE_REQ.1)

10.7.1.1 適用上の注釈

329 *APE_REQ.2.1E のすべてのアクションが、PP モジュール内の空である SAR 部分を考慮することなく、適用される。*

10.8 PP モジュール一貫性 (ACE_MCO)

10.8.1 サブアクティビティの評価 (ACE_MCO.1)

10.8.1.1 目的

330 このサブアクティビティの目的は、その基本 PP に関連する PP モジュールの一貫性を決定することである。

10.8.1.2 入力

331 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP モジュール;

b) その基本 PP。

10.8.1.3 アクション ACE_MCO.1.1E

ACE_MCO.1.1C ***一貫性根拠は、PP モジュールの TOE 種別が、PP モジュール概説で識別されている基本 PP の TOE 種別と一貫していることを実証しなければならない。***

ACE_ MCO.1-1 評価者は、PP モジュールの TOE 種別が、基本 PP のすべての TOE 種別と一貫していることを決定するために一貫性根拠を***検査しなければならない。***

332 種別の間の関係は、簡単なもの(PP モジュールが、関連する追加のセキュリティ機能性を提供する TOE を考慮できる)、またはより複雑なもの(所定のセキュリティ機能性を特定の方法で提供する TOE)である可能性がある。

ACE_MCO.1.2C ***一貫性根拠は、セキュリティ課題定義のステートメントが、PP モジュール概説で識別されている基本 PP のセキュリティ課題定義のステートメントと一貫していることを実証しなければならない。***

ACE_ MCO.1-2 評価者は、PP モジュールのセキュリティ課題定義のステートメントが、基本 PP で述べられているセキュリティ課題定義のステートメントと一貫していることを PP モジュール一貫性根拠が実証することを決定するために、その根拠を***検査しなければならない。***

333 特に、評価者は、次の点を決定するために一貫性根拠を検査する:

a) PP モジュールの脅威、前提条件、及び OSP のステートメントが、基本 PP のそれらに矛盾しない。

b) PP モジュールの前提条件のステートメントが、基本 PP の範囲外の側面に対処している。その場合、エレメントの追加が許可される。

ACE_MCO.1.3C ***一貫性根拠は、セキュリティ対策方針のステートメントが、PP モジュール概説で識別されている基本 PP のセキュリティ対策方針のステートメントと一貫していることを実証しなければならない。***

ACE_MCO.1-3 評価者は、PP モジュールのセキュリティ対策方針のステートメントが、その基本 PP のセキュリティ対策方針のステートメントと一貫していることを決定するために、一貫性根拠を***検査しなければならない。***

334 特に、評価者は、次の点を決定するために一貫性根拠を検査する:

a) PP モジュールにおける TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針のステートメントが、基本 PP のそれらに矛盾しない。

b) PP モジュールの運用環境のセキュリティ対策方針のステートメントが、基本 PP の範囲外の側面に対処している。その場合、エレメントの追加が許可される。

ACE_MCO.1.4C ***一貫性根拠は、セキュリティ要件のステートメントが、PP モジュール概説で識別されている基本PP のセキュリティ要件のステートメントと一貫していることを実証しなければならない。***

ACE_MCO.1-4 評価者は、PP モジュールのセキュリティ要件のステートメントがその基本 PP のセキュリティ要件のステートメントと一貫していること、つまり PP モジュールの SFR が基本 PP の SFR を完了または詳細化し、PP モジュール及び基本 PP の SFR のセット全体との間で一切矛盾が生じないことを決定するために、一貫性根拠を***検査しなければならない。***

10.9 PP 構成一貫性 (ACE_CCO)

10.9.1 サブアクティビティの評価 (ACE_CCO.1)

10.9.1.1 目的

335 このサブアクティビティの目的は、PP 構成及びそのコンポーネントが正しく識別されているかどうかを決定することである。

336 このサブアクティビティの目的は、プロテクションプロファイル及び PP モジュールのセット全体について、PP 構成の一貫性も決定することである。

337 このアクティビティに要求される一貫性分析については、PP 構成の評価中に基本 PP のどの部分を再評価すべきかを決定するために、CEM の 9.2.1 節の適用上の注釈(9.2.1、認証された PP の評価結果の再使用)を適用可能である。

10.9.1.2 入力

338 このサブアクティビティ用の評価証拠は、次のとおりである:

a) PP 構成参照;

b) PP 構成コンポーネントステートメント;

c) コンポーネントステートメントにおいて識別される PP 及び PP モジュール。

10.9.1.3 アクション ACE_CCO.1.1E

ACE_CCO.1.1C ***PP 構成参照は、PP 構成を一意に識別しなければならない。***

ACE_ CCO.1-1 評価者は、PP 構成参照が PP 構成を一意に識別していることを決定するために、PP 構成参照を***検査しなければならない。***

339 評価者は、PP 構成をその他の PP、PP 構成、及び PP モジュールと簡単に区別できるように、PP 構成参照が PP 構成自体を識別することと、さらに PP 構成参照がその PP 構成の各バージョンも(例えば、バージョン番号及び/または公表日を含めることによって)一意に識別することを決定する。

340 PP 構成は、一意の参照をサポートできる何らかの参照方式を持つべきである(例えば、番号、文字、日付の使用)。

ACE_CCO.1.2C ***コンポーネントステートメントは、PP 構成を構成するプロテクションプロファイルと PP モジュールを一意に識別しなければならない。***

ACE_ CCO.1-2 評価者は、PP 構成コンポーネントステートメントが PP 構成に含まれるプロテクションプロファイル及び PP モジュールを一意に識別していることを決定するために、その PP 構成コンポーネントステートメントを***検査しなければならない。***

341 プロテクションプロファイルは、認証され、セキュリティターゲットで使用可能な状態であるべきである。

ACE_CCO.1.3C ***適合ステートメントは、PP 構成の適合の種別が、正確適合か論証適合かを特定しなければならない。適合主張は、PP 構成とその下層の基本 PP 及び PP モジュールが適合を主張する CC のバージョンを識別する CC 適合主張を含めなければならない。***

ACE_CCO.1-3 評価者は、PP 構成適合ステートメントが、要求される適合の種別(正確適合または論証適合)を特定することを決定するために、その適合ステートメントを***検査しなければならない。***

342 評価者は、PP 構成とその下層の基本 PP 及び PP モジュールが適合を主張する CC のバージョンを識別する CC 適合主張が適合主張に含まれていることを***チェックしなければならない。***

343 評価者は、PP 構成とその下層の基本 PP 及び PP モジュールに関連するすべての CC のバージョンの間に互換性があることを決定するために、PP 構成適合主張を***検査しなければならない。***

344 PP 構成コンポーネントステートメントで識別されるプロテクションプロファイルの少なくとも 1 つが正確適合を主張する場合、PP 構成適合主張も正確適合を記述しなければならない。PP 構成とその下層の基本 PP 及び PP モジュールで使用される CC のバージョンには互換性があることが必要である。互換性が明確でない場合は、認証スキームがガイダンスを提供すべきである。

ACE_CCO.1.4C ***SAR ステートメントは、この PP 構成に適用される SAR のセットまたは定義済み EAL を特定しなければならない。***

ACE_CCO.1-4 評価者は、PP 構成 SAR ステートメントが SAR の適格なパッケージを特定していることを決定するために、その SAR ステートメントを***検査しなければならない。***SAR パッケージは、CC パート 3 のコンポーネントとともに組み込むことも、PP 構成を構成するプロテクションプロファイルの 1 つに記述される特定の SAR パッケージを参照することも可能である。

345 SAR のセットが CC パート 3 から生じる場合、評価者は、それが適格であること、つまりそれが依存性に関して閉じていること、または依存性放棄の適切な根拠が SAR ステートメントによって提供されていることを***チェックしなければならない。***

346 評価者は、PP 構成の SAR のセットが、PP 構成に含まれる各プロテクションプロファイルの SAR について一貫していること、つまり各プロテクションプロファイルのどの SAR コンポーネントに対しても、PP 構成がそのファミリ階層において同じ階層または上位階層のコンポーネントを提供することを***チェックしなければならない。***プロテクションプロファイルの SAR コンポーネントが標準コンポーネントの詳細化である場合、PP 構成の対応する SAR コンポーネントには、それらの詳細化が含まれなければならない。2 つのプロテクションプロファイルが同じ SAR コンポーネントを詳細化する場合、評価者は、その詳細化に矛盾がなく、PP 構成の対応する SAR コンポーネントがその両方を満たしていることを***チェックしなければならない。***

ACE_CCO.1.5C ***PP モジュールが依存する基本 PP は、PP 構成のコンポーネントステートメントにおいて識別されるプロテクションプロファイルに属さなければならない。***

ACE_CCO.1-5 評価者は、PP モジュールの基本 PP が、その PP 構成のために選択された PP のセットに含まれていることを***チェックしなければならない。***

10.9.1.4 アクション ACE_CCO.1.2E

ACE_ CCO.1-6 評価者は、PP 構成のコンポーネントステートメントにおいて識別されるすべてのプロテクションプロファイルと PP モジュールで構成される PP 構成に一貫性があることをチェックしなければならない。つまり評価者は、PP 構成に含まれるプロテクションプロファイルと PP モジュールのセット全体との間で一切矛盾が生じないことを***チェックしなければならない。***

347 評価者はこの作業を様々な方法で編成できるが、実際の編成は、複数の PP 構成の評価結果を一度に導き出すかどうかの意思による。

348 例えば、評価者は以下の 2 つのステップで処理することができる:

a) PP 構成を構成するプロテクションプロファイルのセットの一貫性を評定する、

b) 続いて、PP モジュールを一度に 1 つずつ追加することによって、PP 構成の一貫性の評定を段階的に進める;

349 ほかには、PP と PP モジュールを融合させつつ段階的に実施する方法、または PP 構成の定義(CC パート 1 の附属書 B を参照のこと)をフラット化し、エレメントのセット全体の一貫性を評定するという方法もある。

350 C が PP 構成のサブセットで、X が C に追加されるべき PP または PP モジュールである場合、段階的な一貫性分析のステップは以下で構成される:

- X の SPD、対策方針、及び SFR が C のステートメントと矛盾しないことの評定;
- X の前提条件及び環境の対策方針が、C のものと同じであるか、C の範囲外であるセキュリティの側面に対処するかのどちらかである。

351 X が PP モジュールで、C がその基本 PP すべてを含み、サブアクティビティの評価(ACE_MCO.1)が X で成功した場合、一貫性分析のステップは、これらの基本 PP とは違う C のコンポーネントに関してのみ実行される必要があることに注意のこと。

11 ASE クラス: セキュリティターゲット評価

11.1 序説

352 この章では、ST 評価を記述する。ST は、TOE 評価サブアクティビティを実行するための基礎と枠組みを提供するので、ST 評価はこれらのサブアクティビティの前に開始されるべきである。この章の評価方法は、CC パート 3 の ASE クラスに特定されている ST の要件に基づいている。

353 CC パート 1 の附属書 A、B、及び C、操作のためのガイダンスは、ここでの概念を明確にし、多くの例を提供するため、この章はこれらの附属書とともに使用されるべきである。

11.2 適用上の注釈

11.2.1 認証された PP の評価結果の再使用

354 1 つまたは複数の認証された PP に基づいている ST を評価している間に、これらの PP が認証されたという事実を再使用できることがある。ST が、脅威、OSP、前提条件、セキュリティ対策方針及び/またはセキュリティ要件を、PP の脅威、OSP、前提条件、セキュリティ対策方針及び/またはセキュリティ要件に追加しない場合は、認証された PP の結果の再使用の有用性は大きくなる。認証された PP より多くの内容が ST に含まれている場合、再使用はまったく役に立たない可能性がある。

355 評価者は、特定の分析またはその分析の一部がすでに PP 評価の一部として実行された場合は、その分析を部分的にしか行わないかまったく行わないことによって、PP 評価結果を再使用できる。これを実行する場合、評価者は PP 内の分析が正しく実行されたことを想定するべきである。

356 この例としては、PP にあるセキュリティ要件のセットが含まれており、これらが PP 評価の間に内部的に一貫していることが決定された場合が該当するだろう。ST が完全に同じ要件を使用する場合は、ST 評価の間に一貫性分析を繰返す必要はない。ST が 1 つまたは複数の要件を追加する場合、またはこれらの要件に対して操作を実行する場合は、分析を再度行う必要がある。ただし、元の要件が内部的に一貫している事実を使用して、この一貫性分析の作業を削減できる場合がある。元の要件が内部的に一貫している場合、評価者は以下の点だけを決定する必要がある:

a) すべての新しい及び/または変更された要件のセットが内部的に一貫している; 及び

b) すべての新しい及び/または変更された要件のセットが元の要件と一貫している。

357 この理由により分析が行われない場合、または分析が部分的にしか行われない場合、評価者は、それぞれの場合について ETR に注釈を記述する。

11.3 ST 概説(ASE_INT)

11.3.1 サブアクティビティの評価(ASE_INT.1)

11.3.1.1 目的

358 このサブアクティビティの目的は、ST 及び TOE が正しく識別されているかどうか、TOE が順序立てて 3 つの抽象レベル(TOE 参照、TOE 概要、及び TOE 記述)で正しく記述されているかどうか、これらの 3 つの記述が相互に一貫しているかどうかを決定することである。

11.3.1.2 入力

359 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.3.1.3 アクション ASE_INT.1.1E

ASE_INT.1.1C ***ST 概説は、ST 参照、TOE 参照、TOE 概要、及び TOE 記述を含めなければならない。***

ASE_INT.1-1 評価者は、ST 概説が ST 参照、TOE 参照、TOE 概要、及び TOE 記述を含んでいることを***チェックしなければならない。***

ASE_INT.1.2C ***ST 参照は、ST を一意に識別しなければならない。***

ASE_INT.1-2 評価者は、ST 参照が ST を一意に識別していることを決定するために、その ST 参照を***検査しなければならない。***

360 評価者は、ST をその他の ST と簡単に区別できるように、ST 参照がその ST 自体を識別することと、さらに ST 参照がその ST の各バージョンも(例えば、バージョン番号及び/または公表日を含めることによって)一意に識別することを決定する。

361 CM システムが提供されている評価では、評価者は構成リストをチェックすることにより参照の一意性の正当性を確認することができる。その他の場合、ST は一意の参照をサポートできる何らかの参照方式を持つべきである(例えば、番号、文字、日付の使用)。

ASE_INT.1.3C ***TOE 参照は、TOE を一意に識別しなければならない。***

ASE_INT.1-3 評価者は、TOE 参照が TOE を一意に識別していることを決定するために、その TOE 参照を***検査しなければならない。***

362 評価者は、ST がどの TOE を参照するかが明確であるように、TOE 参照が TOE を一意に識別することと、さらに TOE 参照がその TOE のバージョンも(例えば、バージョン/リリース/ビルド番号、またはリリース日を含めることによって)識別することを決定する。

363 評価の最後には、評価者は、TOE 参照、及び TOE の物理的コンポーネントに関連付けられた一意の識別子が、ALC_CMC.x.1C に関連するワークユニットで評価される TOE 及び ALC_CMS.x.2C に関連するワークユニットで評価される構成リストに割り付けられた識別子と一貫していることを***チェックしなければならない。***

ASE_INT.1-4 評価者は、TOE 参照が誤解を招かないことを決定するために、その TOE 参照を***検査しなければならない。***

364 TOE が 1 つ以上の既知の製品に関連している場合、TOE 参照にこれを反映させることができる。ただし、これを使用することによって消費者に誤解を与えないようにするべきであり、製品のどの部分が評価されているかを明確にしなければならない。

365 TOE が、適切に実行するために必須の TOE 以外のハードウェア/ソフトウェア/ファームウェアを必要とする場合、TOE 参照には、TOE によって使用される、TOE 以外のハードウェア/ソフトウェア/ファームウェアの名称を含めることができる。ただし、TOE 以外のハードウェア/ソフトウェア/ファームウェアが評価されていないことを明確にする必要がある。

ASE_INT.1.4C ***TOE 概要は、TOE の使用法及び主要なセキュリティ機能の特徴を要約しなければならない。***

ASE_INT.1-5 評価者は、TOE 概要が TOE の使用法と主要なセキュリティ機能の特徴を記述していることを決定するために、その TOE 概要を***検査しなければならない。***

366 TOE 概要では、TOE の使用法と主要なセキュリティ機能の特徴を簡潔に(つまり、数段落で)記述するべきである。TOE 概要は、TOE が各自のセキュリティに対するニーズに適しているかどうかを潜在的な消費者がすばやく決定できるようにするべきである。

367 TOE 概要は、製品によって提供されるセキュリティ機能の特徴を記述することができ、利用者はその製品種別からセキュリティ機能の特徴を期待するかもしれない。しかし、評価されるセキュリティ機能の特徴と評価されないセキュリティ機能の特徴を明確にしなければならない。

368 TOE 概要は、TOE 記述、セキュリティ対策方針、セキュリティ機能要件、及び TOE 要約仕様など、セキュリティターゲットのその他の節で提供される情報と一貫していなければならない。評価済みのセキュリティ機能の特徴が ST 全体を通して一貫して記述されていることを保証するのに加え、これは、評価されていないセキュリティ機能の特徴はすべて ST 概要の中でのみ論じられることを意味している。

369 統合 TOE に対する ST 内の TOE 概要は、個別のコンポーネント TOE の使用法と主要なセキュリティ上の特徴よりも、統合 TOE の使用法と主要なセキュリティ機能の特徴を記述するべきである。

370 評価者は、概要が消費者にとって十分に明確であり、各自が意図されている TOE の使用法と主要なセキュリティ機能の特徴についての一般的な理解を得るために十分な情報を含んでいることを決定する。

ASE_INT.1.5C ***TOE 概要は、TOE 種別を識別しなければならない。***

ASE_INT.1-6 評価者は、TOE 概要が TOE 種別を識別していることを***チェックしなければならない。***

ASE_INT.1-7 評価者は、TOE 種別が誤解を招かないことを決定するために、TOE 概要を***検査しなければならない。***

371 TOE 種別に基づいて、一般的な消費者が TOE の特定の機能性を期待している場合がある。この機能性が TOE にない場合、評価者は、TOE 概要にこの機能性の欠落が適切に説明されることを決定する。

372 また、TOE が特定の運用環境で動作できるべきであることを一般的な消費者が TOE 種別に基づいて期待する TOE もある。TOE がこのような運用環境で動作できない場合、評価者は TOE 概要にこのことが適切に説明されることを決定する。

ASE_INT.1.6C ***TOE 概要は、TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェアを識別しなければならない。***

ASE_INT.1-8 評価者は、TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェアを TOE 概要が識別していることを決定するために、その TOE 概要を***検査しなければならない。***

373 ある TOE は単独で実行できるが、別のある TOE (特にソフトウェア TOE)は、動作のために追加のハードウェア、ソフトウェア、またはファームウェアを必要とする。TOE がハードウェア、ソフトウェア、またはファームウェアを必要としない場合、このワークユニットは、該当しないため、満たされているものとみなされる。

374 評価者は、TOE の動作に必要な追加ハードウェア、ソフトウェア、及びファームウェアを TOE 概要が識別することを決定する。この識別は、徹底的なものである必要はないが、TOE の潜在的な消費者が、各自の現在のハードウェア、ソフトウェア、及びファームウェアが TOE の使用をサポートするかどうか、及び、これに該当しない場合にどの追加ハードウェア、ソフトウェア、及び/またはファームウェアが必要であるかを決定するのに十分に詳細なものである必要がある。

ASE_INT.1.7C ***TOE 記述は、TOE の物理的範囲を記述しなければならない。***

ASE_INT.1-9 評価者は、TOE 記述が TOE の物理的範囲を記述していることを決定するために、その TOE 記述を***検査しなければならない。***

375 評価者は、TOE 記述が、TOE を構成するハードウェア、ファームウェア、ソフトウェア、及びガイダンスの各部分をリストしており、読者がその各部分について一般的な理解を得るために十分に詳細なレベルでそれらについて記述していることを決定する。

376 TOE 記述は少なくとも以下のエレメントを対象とする:

a) TOE の個別に配付された各部分。これらは各部分の一意の識別子及びその時点の形式(binary、wafer、inlay、*.pdf、*.doc、*.chm など)によって識別される。

b) TOE 消費者が各部分を利用できるよう、開発者が用いる配付方法(ウェブサイトからのダウンロードやクーリエ配送など)。

377 物理的記述には、評価済みの TOE 構成に関する明確なステートメントも含まれる。1 つの製品に複数の物理的な部分があり、それゆえ複数の構成が存在する場合、評価済みの構成は簡潔に記述され、識別されなければならない。

378 評価者は、ハードウェア、ファームウェア、ソフトウェア、またはガイダンスの各部分が TOE の一部であるかどうかについて、誤解を招く可能性がないことも決定する。

ASE_INT.1.8C ***TOE 記述は、TOE の論理的範囲を記述しなければならない。***

ASE_INT.1-10 評価者は、TOE 記述が TOE の論理的範囲を記述していることを決定するために、その TOE 記述を***検査しなければならない。***

379 評価者は、TOE 記述が TOE によって提供される論理的なセキュリティ機能の特徴について、読者が一般的な理解を得るために十分な詳細レベルで説明していることを決定する。

380 評価者は、TOE が論理的なセキュリティ機能の特徴を提供するかどうかについて、誤解を招く可能性がないことも決定する。

381 統合 TOE の ST は、統合 TOE の論理的範囲の記述の大部分を提供するために、コンポーネント TOE の ST で提供されたコンポーネント TOE の論理的範囲の記述を参照できる。ただし、評価者は、個別のコンポーネントのどの機能が統合 TOE 内に存在しないか、また、そのために、統合 TOE の機能ではなくなっているかを、統合 TOE の ST が明確に説明することを決定する。

11.3.1.4 アクション ASE_INT.1.2E

ASE_INT.1-11 評価者は、TOE 参照、TOE 概要、及び TOE 記述が相互に一貫していることを決定するために、その TOE 参照、TOE 概要、及び TOE 記述を***検査しなければならない。***

11.4 適合主張(ASE_CCL)

11.4.1 サブアクティビティの評価(ASE_CCL.1)

11.4.1.1 目的

382 このサブアクティビティの目的は、様々な適合主張の有効性を決定することである。これらは、ST と TOE が CC に対してどのように適合しているか、ST が PP とパッケージに対してどのように適合しているかを記述する。

11.4.1.2 入力

383 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) ST が適合を主張する PP;

c) ST が適合を主張するパッケージ。

11.4.1.3 アクション ASE_CCL.1.1E

ASE_CCL.1.1C ***適合主張は、ST と TOE が適合を主張する CC のバージョンを識別する CC 適合主張を含めなければならない。***

ASE_CCL.1-1 評価者は、ST と TOE が適合を主張する CC のバージョンを識別する CC 適合主張が適合主張に含まれていることを***チェックしなければならない。***

384 評価者は、この ST を開発するために使用された CC のバージョンを CC 適合主張が識別することを決定する。これには、CC のバージョン番号を含めるべきであり、また、CC の国際的な英語バージョンが使用されなかった場合は、使用された CC のバージョンの言語も含めるべきである。

385 統合 TOE の場合、評価者は、コンポーネントに対して主張された CC のバージョンと統合 TOE に対して主張された CC のバージョンの相違を考慮する。バージョンが異なる場合、評価者は、バージョン間の相違によって主張の競合が発生するかどうかを評定する。

386 基本 TOE と依存 TOE に対する CC 適合主張が CC の異なる主要なリリースに対するものである場合(例えば、1 つのコンポーネント TOE 適合主張が CC v2.x であり、別のコンポーネント TOE 適合主張が CC v3.x である場合)は、CC は下位互換性を提供することを目的として開発された(厳格な意味ではこれは達成されていない可能性があるが、原則的には達成されているものと解釈する)ため、統合 TOE の適合主張は CC の以前の方のリリースになる。

ASE_CCL.1.2C ***CC 適合主張は、CC パート 2 に対する ST の適合を CC パート 2 適合または CC パート 2 拡張として記述しなければならない。***

ASE_CCL.1-2 評価者は、CC 適合主張が ST に対する CC パート 2 適合または CC パート 2 拡張の主張を述べていることを***チェックしなければならない。***

387 統合 TOE の場合、評価者は、この主張が CC パート 2 と一貫しているだけではなく、各コンポーネント TOE による CC パート 2 への適合の主張とも一貫しているかどうかを考慮する。つまり、1 つ以上のコンポーネント TOE が CC パート 2 拡張を主張している場合は、統合 TOE も CC パート 2 拡張を主張するべきである。

388 追加 SFR が基本 TOE に対して主張されている場合は、個々のコンポーネント TOE がパート 2 適合であっても、統合 TOE の CC 適合主張は CC パート 2 拡張になることがある(***ASE_CCL.1.6C*** に対する統合 TOE ガイダンスを参照のこと)。

ASE_CCL.1.3C ***CC 適合主張は、CC パート 3 に対する ST の適合を CC パート 3 適合または CC パート 3 拡張として記述しなければならない。***

ASE_CCL.1-3 評価者は、CC 適合主張が ST に対する CC パート 3 適合または CC パート 3 拡張の主張を述べていることを***チェックしなければならない。***

ASE_CCL.1.4C ***CC 適合主張は、拡張コンポーネント定義と一貫していなければならない。***

ASE_CCL.1-4 評価者は、CC パート 2 に対する CC 適合主張が拡張コンポーネント定義と一貫していることを決定するためにその CC 適合主張を***検査しなければならない。***

389 CC 適合主張が CC パート 2 適合を含んでいる場合、評価者は、拡張コンポーネント定義が機能コンポーネントを定義しないことを決定する。

390 CC 適合主張が CC パート 2 拡張を含んでいる場合、評価者は、拡張コンポーネント定義が拡張機能コンポーネントを少なくとも 1 つは定義していることを決定する。

ASE_CCL.1-5 評価者は、CC パート 3 に対する CC 適合主張が拡張コンポーネント定義と一貫していることを決定するためにその CC 適合主張を***検査しなければならない。***

391 CC 適合主張が CC パート 3 適合を含んでいる場合、評価者は、拡張コンポーネント定義が保証コンポーネントを定義しないことを決定する。

392 CC 適合主張が CC パート 3 拡張を含んでいる場合、評価者は、拡張コンポーネント定義が拡張保証コンポーネントを少なくとも 1 つは定義していることを決定する。

ASE_CCL.1.5C ***適合主張は、ST が適合を主張する PP 及びセキュリティ要件パッケージをすべて識別しなければならない。***

ASE_CCL.1-6 評価者は、ST が適合を主張するすべての PP を識別する PP 主張が適合主張に含まれていることを***チェックしなければならない。***

393 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

394 評価者は、参照される PP が曖昧さなく(例えば、タイトル及びバージョン番号、または PP の概説に含まれている識別によって)識別されることを決定する。ST が正確適合または論証適合を主張する PP のみが、適合主張の節で識別されることが許可され、これは、PP または PP 構成への部分適合の主張が許可されないことを意味する。

395 このため、統合ソリューションを必要とする PP への適合は、統合 TOE の ST で主張できる。このような PP への適合は、コンポーネント TOE が統合ソリューションを満たさないため、コンポーネント TOE の評価中は不可能だろう。これは、「統合」PP が統合評価手法の使用(ACO コンポーネントの使用)を許可する場合にのみ可能である。

396 統合 TOE の ST は、統合 ST を構成するコンポーネント TOE の ST を識別する。統合 TOE は、基本的にコンポーネント TOE の ST への適合を主張している。

ASE_CCL.1-7 評価者は、ST が適合を主張するすべてのパッケージを識別するパッケージ主張を適合主張が含むことを***チェックしなければならない。***

397 ST がパッケージへの適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

398 評価者は、参照されるパッケージが曖昧さなく(例えば、タイトル及びバージョン番号、またはパッケージの概説に含まれている識別によって)識別されることを決定する。

399 評価者は、統合 TOE の派生元であるコンポーネント TOE の STも曖昧さなく識別されていることを決定する。

400 評価者は、パッケージへの部分的な適合の主張は許可されないことに留意する。

ASE_CCL.1.6C ***適合主張は、パッケージへの ST の適合をパッケージ適合またはパッケージ追加として記述しなければならない。***

ASE_CCL.1-8 評価者は、識別された各パッケージに対して、適合主張がパッケージ名適合またはパッケージ名追加の主張を述べていることを***チェックしなければならない。***

401 ST がパッケージへの適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

402 パッケージ適合主張がパッケージ名適合を含む場合、評価者は以下のことを決定する:

a) パッケージが保証パッケージである場合、ST はパッケージに含まれるすべての SAR を含めるが、追加 SAR は含めない。

b) パッケージが機能パッケージである場合、ST はパッケージに含まれるすべての SFR を含めるが、追加 SFR は含めない。

403 パッケージ適合主張がパッケージ名追加を含む場合、評価者は以下のことを決定する:

a) パッケージが保証パッケージである場合、ST はパッケージ内に含まれるすべての SAR を含み、追加 SAR を少なくとも 1 つ、またはパッケージ内の SAR の上位階層である SAR を少なくとも 1 つ含む。

b) パッケージが機能パッケージである場合、ST はパッケージ内に含まれるすべての SFR を含み、追加 SFR を少なくとも 1 つ、またはパッケージ内の SFR の上位階層とである SFR を少なくとも 1 つ含む。

ASE_CCL.1.7C ***適合主張根拠は、TOE 種別が、適合が主張されている PP 内の TOE 種別と一貫していることを実証しなければならない。***

ASE_CCL.1-9 評価者は、TOE の TOE 種別が各 PP のすべての TOE 種別と一貫していることを決定するために適合主張根拠を***検査しなければならない。***

404 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

405 種別の間の関係は、簡単なもの(ファイアウォール PP に対する適合を主張しているファイアウォール ST)、またはより複雑なもの(複数の PP に対する適合を同時に主張しているスマートカード ST(統合された回路に対する PP、スマートカード OS に対する PP、及びスマートカード上の 2 つのアプリケーションに対する 2 つの PP))である可能性がある。

406 統合 TOE の場合、評価者は、コンポーネント TOE の TOE 種別が統合 TOE 種別と一貫していることを適合主張根拠が実証するかどうかを決定する。これは、コンポーネント TOE 及び統合 TOE の両方の種別が同じである必要があることを意味するのではなく、コンポーネント TOE が統合 TOE を提供するための統合に適していることを意味する。どの SFR が統合の結果としてのみ含まれ、基本 TOE 及び依存 TOE(例えば、EALx)の評価で SFR として検査されなかったかを統合 TOE の ST 内で明確にすべきである。

ASE_CCL.1.8C ***適合主張根拠は、セキュリティ課題定義のステートメントが、適合が主張されている PP 内のセキュリティ課題定義のステートメントと一貫していることを実証しなければならない。***

ASE_CCL.1-10 評価者は、セキュリティ課題定義のステートメントが、PP の適合ステートメントによる定義に従って、適合が主張されている PP で述べられているセキュリティ課題定義のステートメントと一貫していることを適合主張根拠が実証することを決定するために、その根拠を***検査しなければならない。***

407 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

408 PP にセキュリティ課題定義のステートメントがない場合、このワークユニットは該当しないため、満たされているものとみなされる。

409 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は次の状態であるかどうかを決定する:

a) ST 内の脅威は、適合が主張されている PP 内の脅威のスーパーセットであるか、その PP 内の脅威と同一である;

b) ST 内の OSP は、適合が主張されている PP 内の OSP のスーパーセットであるか、その PP 内の OSP と同一である;

c) ST 内の前提条件は、次の 2 項目で説明される 2 つの例外を除き、適合が主張されている PP 内の前提条件と同一である;

- PP からの前提条件(または前提条件の一部)は、この前提条件(または前提条件の一部)に対処する運用環境のセキュリティ対策方針のすべてが、TOE のセキュリティ対策方針に置き換えられる場合、除外することができる;

- 新しい前提条件が、PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている脅威(または脅威の一部)を軽減せず、PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている OSP(または OSP の一部)を満たさないことの根拠が示される場合、PP 内に定義された前提条件に、前提条件を追加することができる。

PP から前提条件を除外した、または、新しい前提条件を追加した、PP への適合を主張する ST を検査する際、評価者は、上記の条件が満たされているかどうかを慎重に決定しなければならない。次の考察で、これらの場合における動機と例を示す:

- 前提条件を除外する例: PP は、運用環境が TOE の外部インタフェースに送信されるデータの不正な改変または傍受を防ぐということを述べる前提条件を含むことができる。これは、TOE が、このインタフェースで、平文で完全性保護なしのデータを受け入れ、攻撃者によるこれらのデータへのアクセスを防ぐセキュアな運用環境に設置されると想定される場合に当てはまる。そして、前提条件は、PP 内で、このインタフェースで交換したデータが、運用環境での適切な手段によって保護されていると述べる運用環境のセキュリティ対策方針にマッピングされる。この PP への適合を主張する ST が、例えば、このインタフェースを経由して転送されたすべてのデータの暗号化と完全性保護のためのセキュアなチャネルを供給することによって、TOE 自身がこれらのデータを保護すると述べる追加のセキュリティ対策方針を持つ、更にセキュアな TOE を定義する場合、対応する運用環境のセキュリティ対策方針と前提条件は、ST から除外することができる。これはまた、対策方針が運用環境から TOE に再割付されるので、対策方針の再割付と呼ばれる。この TOE は、除外した前提条件を満たす運用環境においてなおもセキュアであり、そのためやはり PP を満たすという点に注意のこと。

- 前提条件を追加する例: この例では、PP が「ファイアウォール」型の TOE に対する要件を特定するよう設計されており、ST 作成者は、ファイアウォールを実装する TOE に対するこの PP への適合を主張したいと願うが、TOE は更に VPN（仮想プライベートネットワーク）コンポーネントの機能性も提供する。VPN 機能性については、TOE は暗号鍵を必要とし、これらの鍵も運用環境によってセキュアに処理される必要がある（例えば、対称鍵が、ネットワーク接続をセキュアにするために使われ、そのため、ネットワークの他のコンポーネントに対してセキュアな方法で提供される必要がある場合）。この場合、VPN によって使われる暗号鍵が、運用環境によってセキュアに処理されるという前提条件を追加するのは許容できる。この前提条件は、PP の脅威や OSP に対処しないので、上記に述べた状況を満たす。

- 前提条件を追加する反例: 最初の例の変形として、PP がそのインタフェースの 1 つに対してセキュアなチャネルを提供するための TOE のセキュリティ対策方針を既に含んでおり、この対策方針はこのインタフェース上のデータの不正な改変または読み取りの脅威にマッピングされる。この場合、この PP への適合を主張する ST が、運用環境がこのインタフェース上のデータを改変や不正なデータの読み取りから保護すると想定する運用環境の前提条件を追加することは明らかに許可されない。この前提条件は TOE によって対処されることが意図されている脅威を低減する。従って、この前提条件を追加した ST を満たす TOE は、PP を自動的に満たさず、よって、この追加は許可されない。

- 前提条件を追加する 2 つ目の反例: ファイアウォールを実装する TOE の上記の例において、TOE が信頼できるデバイスにのみ接続するという一般的な前提条件を追加することは許容できない。というのは、これは明らかにファイアウォールに関する本質的な脅威（つまり、フィルタにかける必要のある信頼できない IP トラフィックがある）を取り除くからである。従って、この追加は許可されない。

410 PP によって論証適合が要求されている場合、ST のセキュリティ課題定義のステートメントが、適合が主張されている PP 内のセキュリティ課題定義のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

411 このため、適合主張根拠は、ST 内のセキュリティ課題定義が、PP 内のセキュリティ課題定義と同等（またはより制限的）であると実証する必要がある。これは、以下を意味する:

- ST 内のセキュリティ課題定義を満たすすべての TOE は、PP 内のセキュリティ課題定義も満たす。これはまた、PP 内に定義された脅威を実現したり、PP 内に定義された OSP を侵害したりする各事象が、ST 内に述べられた脅威を実現したり、ST 内に定義された OSP を侵害したりすることを実証することによって、間接的に示される。ST 内に述べられた OSP を満たすことは、PP 内に述べられた脅威を防ぐことができ、または、ST 内に述べられた脅威を防ぐことは、PP 内に述べられた OSP を満たすことができるので、脅威と OSP はお互いに代用できる点に注意のこと;

- PP 内のセキュリティ課題定義を満たすすべての運用環境は、ST 内のセキュリティ課題定義も満たす（次の項目の 1 つの例外を除く）;

- PP の SPD への適合を実証するために必要とされる、ST 内の前提条件のセットのほかに、ST は、更に前提条件を特定することができる。ただし、これらの追加の前提条件が、PP 内に定義されたセキュリティ課題定義から独立しており影響を与えない場合に限る。更に詳しくは、PP に従い、TOE によって対抗する必要のある TOE への脅威を除外する ST 内の前提条件はない。同様に、PP に従い、TOE によって満たされることが意図されている PP 内に述べられた OSP の側面を実現した ST 内の前提条件はない。

412 統合 TOE の場合、評価者は、統合 TOE のセキュリティ課題定義がコンポーネント TOE の ST で指定されたセキュリティ課題定義と一貫しているかどうかを考慮する。これは、論証適合の観点から決定される。特に、評価者は、次の点を決定するために適合主張根拠を検査する:

a) 統合 TOE の ST 内の脅威ステートメント及び OSP は、コンポーネント ST からの脅威ステートメント及び OSP に矛盾しない。

b) コンポーネント ST で想定されているあらゆる前提条件は、統合 TOE の ST 内で充足される。つまり、統合 ST 内でもその前提条件が提示されるか、統合 ST 内で前提条件は前提条件以外として積極的に対処されるべきである。前提条件は、前提条件で意図された関心事項を満たす機能性を提供するための統合 TOE 内の要件の指定によって、積極的に対処することができる。

ASE_CCL.1.9C ***適合主張根拠は、セキュリティ対策方針のステートメントが、適合が主張されている PP 内のセキュリティ対策方針のステートメントと一貫していることを実証しなければならない。***

ASE_CCL.1-11 評価者は、セキュリティ対策方針のステートメントが、適合が主張されている PP の適合ステートメントの定義に従って、PP のセキュリティ対策方針のステートメントと一貫していることを決定するために、適合主張根拠を***検査しなければならない。***

413 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

414 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は次の状態であるかどうかを決定する:

- 適合が主張されている PP の TOE のセキュリティ対策方針のすべてが ST に含まれている。評価中の ST に TOE のセキュリティ対策方針を追加できる点に注意のこと;

- ST 内の運用環境のセキュリティ対策方針は、次の 2 項目で説明される 2 つの例外を除き、適合が主張されている PP 内の運用環境のセキュリティ対策方針と同一である。;

- PP からの運用環境のセキュリティ対策方針（またはそのようなセキュリティ対策方針の一部）は、TOE に対して述べられた同じセキュリティ対策方針（の一部）に置き換えられる;

- 新しいセキュリティ対策方針が、PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている脅威（または脅威の一部）を軽減せず、PP 内の TOE のセキュリティ対策方針によって対処されることが意図されている OSP（または OSP の一部）を満たさないことを正当化する理由が示される場合、PP 内に定義されたセキュリティ対策方針に運用環境のセキュリティ対策方針を追加することができる。

PP からの運用環境のセキュリティ対策方針を除外した、または、運用環境のセキュリティ対策方針を新しく追加した、PP への適合を主張する ST を検査する際、評価者は、上記の条件が満たされているかどうかを慎重に決定しなければならない。前述のワークユニットにおける前提条件の事例に関する例は、ここでも有効である。

415 適合が主張されている PP によって論証適合が要求されている場合、ST のセキュリティ対策方針のステートメントが、適合が主張されている PP のセキュリティ対策方針のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

416 このため、適合主張根拠は、ST 内のセキュリティ対策方針が、PP 内のセキュリティ対策方針と同等（またはより制限的）であると実証する必要がある。これは、以下を意味する:

- ST 内の TOE のセキュリティ対策方針を満たすすべての TOE は、PP 内の TOE のセキュリティ対策方針も満たす;

- PP 内の運用環境のセキュリティ対策方針を満たすすべての運用環境は、ST 内の運用環境のセキュリティ対策方針も満たす（次の項目の 1 つの例外を除く）;

- PP 内に定義されたセキュリティ対策方針のセットへの適合を実証するために使われる、ST 内の運用環境のセキュリティ対策方針のセットのほかに、ST は、更に運用環境のセキュリティ対策方針を特定することができる。ただし、これらのセキュリティ対策方針が、適合が主張されている PP 内に定義された、元々の TOE のセキュリティ対策方針のセットにも、運用環境のセキュリティ対策方針のセットにも影響しない場合に限る。

417 統合 TOE の場合、評価者は、統合 TOE のセキュリティ対策方針がコンポーネント TOE の ST で指定されたセキュリティ対策方針と一貫しているかどうかを考慮する。これは、論証適合の観点から決定される。特に、評価者は、次の点を決定するために適合主張根拠を検査する:

a) 依存 TOE の ST 内の運用環境の IT に関連するセキュリティ対策方針のステートメントは、基本 TOE の ST 内の TOE のセキュリティ対策方針のステートメントと一貫している。依存 TOE の ST 内の環境のセキュリティ対策方針のステートメントが、基本 TOE の ST 内の TOE のセキュリティ対策方針のステートメントのすべての局面を扱うことは期待されない。

b) 統合 ST 内のセキュリティ対策方針のステートメントは、コンポーネント TOE の ST 内のセキュリティ対策方針のステートメントと一貫している。

418 PP によって論証適合が要求されている場合、ST のセキュリティ対策方針のステートメントが、PP 内の、または統合 TOE の ST の場合はコンポーネント TOE の ST 内のセキュリティ対策方針のステートメントと少なくとも同等であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

ASE_CCL.1.10C ***適合主張根拠は、セキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントと一貫していることを実証しなければならない。***

ASE_CCL.1-12 評価者は、PP の適合ステートメントによる定義に従って、適合が主張されている PP のすべてのセキュリティ要件と ST が一貫していることを決定するために、その ST を***検査しなければならない。***

419 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

420 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は、ST 内のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントのスーパーセットであるか、またはその PP 内のセキュリティ要件のステートメントと同一であるかを決定する(正確適合の場合)。

421 適合が主張されている PP によって論証適合が要求されている場合、ST のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

422 次の通り:

- SFR: ST 内の適合根拠は、 ST 内の SFR によって定義された要件の全体的なセットが、PP 内の SFR によって定義された要件の全体的なセットと同等（またはより制限的）であると実証しなければならない。これは、ST 内のすべての SFR のセットによって定義された要件を満たすすべての TOE が、PP 内のすべての SFR のセットによって定義された要件も満たすことを意味する;

- SAR: ST は、PP 内のすべての SAR を含まなければならないが、追加の SAR を主張すること、または、SAR をより上位階層の SAR で置き換えることができる。ST 内の操作の完了は、PP 内の操作の完了と一貫していなければならない； PP 内と同じ完了が ST 内でも使われるか、SAR をより制限的にした完了（詳細化の規則が適用される）かのどちらかである。

423 統合 TOE の場合、評価者は、統合 TOE のセキュリティ要件がコンポーネント TOE の ST で指定されたセキュリティ要件と一貫しているかどうかを考慮する。これは、論証適合の観点から決定される。特に、評価者は、次の点を決定するために適合根拠を検査する:

a) 依存 TOE の ST 内の運用環境の IT に関連するセキュリティ要件のステートメントは、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントと一貫している。依存 TOE の ST 内の環境のセキュリティ要件のステートメントが、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントのすべての局面を扱うことは期待されない。これは、一部の SFR を統合 TOE の ST 内のセキュリティ要件のステートメントに追加しなければならない場合があるからである。ただし、基本内のセキュリティ要件のステートメントは、依存コンポーネントの動作をサポートするべきである。

b) 依存 TOE の ST 内の運用環境の IT に関連するセキュリティ対策方針のステートメントは、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントと一貫している。依存 TOE の ST 内の環境のセキュリティ対策方針のステートメントが、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントのすべての局面を扱うことは期待されない。

c) 統合 ST 内のセキュリティ要件のステートメントは、コンポーネント TOE の ST 内のセキュリティ要件のステートメントと一貫している。

424 適合が主張されている PP によって論証適合が要求されている場合、ST のセキュリティ要件のステートメントが、PP 内の、または統合 TOE の ST の場合はコンポーネント TOE の ST 内のセキュリティ要件のステートメントと少なくとも同等であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

11.5 セキュリティ課題定義(ASE_SPD)

11.5.1 サブアクティビティの評価(ASE_SPD.1)

11.5.1.1 目的

425 このサブアクティビティの目的は、TOE 及び TOE の運用環境によって対処されることが意図されているセキュリティ課題が明確に定義されていることを決定することである。

11.5.1.2 入力

426 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.5.1.3 アクション ASE_SPD.1.1E

ASE_SPD.1.1C *セキュリティ課題定義は、脅威を記述しなければならない。*

ASE_SPD.1-1 評価者は、セキュリティ課題定義が脅威を記述していることを*チェックしなければならない。*

427 すべてのセキュリティ対策方針が前提条件及び/または OSP からのみ派生するものである場合、脅威のステートメントを ST に提示する必要はない。この場合、このワークユニットは、該当しないため、満たされているものとみなされる。

428 評価者は、セキュリティ課題定義が TOE 及び/または運用環境によって対抗する必要がある脅威を記述していることを決定する。

ASE_SPD.1.2C *すべての脅威は、脅威エージェント、資産、及び有害なアクションの観点から記述しなければならない。*

ASE_SPD.1-2 評価者は、すべての脅威が脅威エージェント、資産、及び有害なアクションの観点から記述されていることを決定するために、セキュリティ課題定義を*検査しなければならない。*

429 すべてのセキュリティ対策方針が前提条件及び/または OSP からのみ派生するものである場合、脅威のステートメントを ST に提示する必要はない。この場合、このワークユニットは、該当しないため、満たされているものとみなされる。

430 脅威エージェントは、技能、資源、機会、及び動機などの側面によって、さらに詳細に記述することができる。

ASE_SPD.1.3C *セキュリティ課題定義は、OSP を記述しなければならない。*

ASE_SPD.1-3 評価者は、セキュリティ課題定義が OSP を記述していることを*検査しなければならない。*

431 すべてのセキュリティ対策方針が前提条件及び脅威からのみ派生するものである場合、OSP を ST に提示する必要はない。この場合、このワークユニットは、該当しないため、満たされているものとみなされる。

432 評価者は、TOE 及び/または TOE の運用環境が従う必要がある規則またはガイドラインの観点から OSP ステートメントが作成されることを決定する。

433 評価者は、各 OSP が明確に理解できるように十分な詳細が説明及び/または解釈が行われていることを決定する。セキュリティ対策方針の追跡を可能とするために方針ステートメントの明確な提示が必要である。

ASE_SPD.1.4C ***セキュリティ課題定義は、TOE の運用環境についての前提条件を記述しなければならない。***

ASE_SPD.1-4 評価者は、セキュリティ課題定義が TOE の運用環境についての前提条件を記述していることを決定するために、その定義を***検査しなければならない。***

434 前提条件がない場合、このワークユニットは、該当せず、満たされているものとみなされる。

435 評価者は、TOE の運用環境についてのそれぞれの前提条件が十分に詳細に説明されていて、消費者は各自の運用環境が前提条件と一致していることを決定できることを決定する。前提条件が明確に理解されていない場合、TOE がセキュアな方法で機能しない運用環境で使用される結果となる場合がある。

11.6 セキュリティ対策方針(ASE_OBJ)

11.6.1 サブアクティビティの評価(ASE_OBJ.1)

11.6.1.1 目的

436 このサブアクティビティの目的は、運用環境のセキュリティ対策方針が明確に定義されているかどうかを決定することである。

11.6.1.2 入力

437 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.6.1.3 アクション ASE_OBJ.1.1E

ASE_OBJ.1.1C *セキュリティ対策方針のステートメントは、運用環境のセキュリティ対策方針を記述しなければならない。*

ASE_OBJ.1-1 評価者は、セキュリティ対策方針のステートメントが運用環境のセキュリティ対策方針を定義していることを*チェックしなければならない。*

438 評価者は、運用環境のセキュリティ対策方針が識別されていることをチェックする。

11.6.2 サブアクティビティの評価(ASE_OBJ.2)

11.6.2.1 目的

439 このサブアクティビティの目的は、セキュリティ対策方針が適切かつ完全にセキュリティ課題定義を扱うかどうか、及び TOE 及びその運用環境の間でのこの課題に対する分担が明確に定義されていることを決定することである。

11.6.2.2 入力

440 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.6.2.3 アクション ASE_OBJ.2.1E

ASE_OBJ.2.1C *セキュリティ対策方針のステートメントは、TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針を記述しなければならない。*

ASE_OBJ.2-1 評価者は、セキュリティ対策方針のステートメントが TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針を定義していることを*チェックしなければならない。*

441 評価者は、セキュリティ対策方針の両カテゴリが明確に識別されており、他のカテゴリから分離されていることをチェックする。

ASE_OBJ.2.2C *セキュリティ対策方針根拠は、TOE の各セキュリティ対策方針をそのセキュリティ対策方針によって対抗される脅威及びそのセキュリティ対策方針によって実施される OSP までさかのぼらなければならない。*

ASE_OBJ.2-2 評価者は、セキュリティ対策方針根拠が、対策方針によって対抗される脅威及び/または対策方針によって実施される OSP まで、TOE のセキュリティ対策方針のすべてをさかのぼることを***チェックしなければならない。***

442 TOE の各セキュリティ対策方針は、脅威と OSP のいずれか、あるいは脅威と OSP の組み合わせにまでさかのぼることができるが、少なくとも 1 つの脅威または OSP にまでさかのぼらなければならない。

443 さかのぼることに失敗した場合、セキュリティ対策方針根拠が不完全であるか、セキュリティ課題定義が不完全であるか、または TOE のセキュリティ対策方針が役立つ目的を持っていないことを示す。

ASE_OBJ.2.3C ***セキュリティ対策方針根拠は、運用環境の各セキュリティ対策方針をそのセキュリティ対策方針によって対抗される脅威、そのセキュリティ対策方針によって実施される OSP、及びそのセキュリティ対策方針によって充足される前提条件にまでさかのぼらなければならない。***

ASE_OBJ.2-3 評価者は、セキュリティ対策方針根拠が、セキュリティ対策方針によって対抗される脅威、セキュリティ対策方針によって実施される OSP、及びセキュリティ対策方針によって充足される前提条件にまで、運用環境のセキュリティ対策方針をさかのぼることを***チェックしなければならない。***

444 運用環境の各セキュリティ対策方針は、脅威、OSP、前提条件、あるいは脅威、OSP、及び/または前提条件の組み合わせにまでさかのぼることができるが、少なくとも 1 つの脅威、OSP、または前提条件にまでさかのぼらなければならない。

445 さかのぼることに失敗した場合、セキュリティ対策方針根拠が不完全であるか、セキュリティ課題定義が不完全であるか、または運用環境のセキュリティ対策方針が役立つ目的を持っていないことを示す。

ASE_OBJ.2.4C ***セキュリティ対策方針根拠は、セキュリティ対策方針がすべての脅威に対抗することを実証しなければならない。***

ASE_OBJ.2-4 評価者は、各脅威について、セキュリティ対策方針がその脅威に対抗するために適していることをセキュリティ対策方針根拠が正当化していること決定するために、その根拠を***検査しなければならない。***

446 脅威にまでさかのぼるセキュリティ対策方針が一つもない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

447 評価者は、脅威に対する正当化が脅威の除去、軽減、または緩和が行われたかどうかを示すことを決定する。

448 評価者は、脅威に対する正当化が、セキュリティ対策方針が十分である(つまり、脅威にまでさかのぼるすべてのセキュリティ対策方針が達成される場合、脅威は除去されるか、十分に軽減されるか、脅威の影響が十分に緩和される)ことを実証することを決定する。

449 セキュリティ対策方針根拠において提供される脅威に対するセキュリティ対策方針からの追跡は、正当化の一部である場合があるが、それだけでは正当化を構成しないことに注意すること。セキュリティ対策方針が、特定の脅威が実現されることを妨げる意図を反映しただけのステートメントである場合であっても、正当化が必要であるが、この正当化は「セキュリティ対策方針 X が脅威 Y に直接対抗する」のように最小になる可能性がある。

450 評価者は、脅威にまでさかのぼる各セキュリティ対策方針が必要である(つまり、セキュリティ対策方針が達成される場合、それは実際に脅威の除去、軽減、または緩和に寄与する)ことも決定する。

ASE_OBJ.2.5C ***セキュリティ対策方針根拠は、セキュリティ対策方針がすべての OSP を実施することを実証しなければならない。***

ASE_OBJ.2-5 評価者は、各 OSP について、セキュリティ対策方針がその OSP を実施するために適していることをセキュリティ対策方針根拠が正当化していること決定するために、その根拠を***検査しなければならない。***

451 OSP にまでさかのぼるセキュリティ対策方針が一つもない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

452 評価者は、OSP に対する正当化が、セキュリティ対策方針が十分である(つまり、その OSP にまでさかのぼるすべてのセキュリティ対策方針が達成される場合、OSP は実施される)ことを実証することを決定する。

453 評価者は、OSP にまでさかのぼる各セキュリティ対策方針が必要である(つまり、セキュリティ対策方針が達成される場合、それは実際に OSP の実施に寄与する)ことも決定する。

454 セキュリティ対策方針根拠において提供される OSP に対するセキュリティ対策方針からの追跡は、正当化の一部である場合があるが、それだけでは正当化を構成しないことに注意すること。セキュリティ対策方針が、特定の OSP を実施する意図を反映しただけのステートメントである場合、正当化が必要であるが、この正当化は「セキュリティ対策方針 X が OSP Y を直接実施する」のように最小になる可能性がある。

ASE_OBJ.2.6C ***セキュリティ対策方針根拠は、運用環境のセキュリティ対策方針がすべての前提条件を充足することを実証しなければならない。***

ASE_OBJ.2-6 評価者は、運用環境に対する各前提条件について、運用環境のセキュリティ対策方針がその前提条件を充足するのに適していることを示す適切な正当化を、セキュリティ対策方針根拠が含んでいることを決定するために、その根拠を***検査しなければならない。***

455 前提条件にまでさかのぼる運用環境のセキュリティ対策方針が一つもない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

456 評価者は、TOE の運用環境に関する前提条件に対する正当化が、セキュリティ対策方針が十分である(つまり、前提条件にまでさかのぼるすべての運用環境のセキュリティ対策方針が達成される場合、運用環境は前提条件を充足する)ことを実証することを決定する。

457 評価者は、TOE の運用環境に関する前提条件にまでさかのぼる運用環境の各セキュリティ対策方針が必要である(つまり、セキュリティ対策方針が達成される場合、それは前提条件を充足する運用環境に寄与する)ことも決定する。

458 セキュリティ対策方針根拠において記述される、前提条件に対する運用環境のセキュリティ対策方針からの追跡は、正当化の一部である場合があるが、それだけでは正当化を構成しないことに注意すること。運用環境のセキュリティ対策方針が、前提条件の単なる再記述である場合であっても、正当化が必要であるが、この正当化は「セキュリティ対策方針 X は前提条件 Y を直接充足する」のように最小になる可能性がある。

11.7 拡張コンポーネント定義(ASE_ECD)

11.7.1 サブアクティビティの評価(ASE_ECD.1)

11.7.1.1 目的

459 このサブアクティビティの目的は、拡張コンポーネントが明確に、曖昧さなく定義されているかどうか、及びそれが必要であるかどうか、つまり既存の CC パート 2 または CC パート 3 のコンポーネントを使用して明確に表現される可能性がないかどうかを決定することである。

11.7.1.2 入力

460 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.7.1.3 アクション ASE_ECD.1.1E

ASE_ECD.1.1C ***セキュリティ要件のステートメントは、すべての拡張セキュリティ要件を識別しなければならない。***

ASE_ECD.1-1 評価者は、拡張要件として識別されていないセキュリティ要件のステートメントにおけるすべてのセキュリティ要件は、CC パート 2 または CC パート 3 で示されていることを***チェックしなければならない。***

ASE_ECD.1.2C ***拡張コンポーネント定義は、各拡張セキュリティ要件に対応する拡張コンポーネントを定義しなければならない。***

ASE_ECD.1-2 評価者は、拡張コンポーネント定義が各拡張セキュリティ要件に対応する拡張コンポーネントを定義することを***チェックしなければならない。***

461 ST に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

462 単一の拡張コンポーネントは、拡張セキュリティ要件の複数の繰返しを定義するために使用することができ、各繰返しに対してこの定義を繰返す必要はない。

ASE_ECD.1.3C ***拡張コンポーネント定義は、各拡張コンポーネントが既存の CC コンポーネント、ファミリ、及びクラスにどのように関連するかを記述しなければならない。***

ASE_ECD.1-3 評価者は、各拡張コンポーネントが既存の CC コンポーネント、ファミリ、及びクラスにどのようにあてはまるかを拡張コンポーネント定義が記述していることを決定するために、その拡張コンポーネント定義を***検査しなければならない。***

463 ST に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

464 評価者は、各拡張コンポーネントが次のいずれかであることを決定する:

a) 既存の CC パート 2 または CC パート 3 ファミリのメンバ; または

b) ST で定義された新しいファミリのメンバ。

465 拡張コンポーネントが既存の CC パート 2 または CC パート 3 ファミリのメンバである場合、評価者は、拡張コンポーネントがそのファミリのメンバであるべき理由、及びそのファミリの他のコンポーネントにどのように関連しているかを拡張コンポーネント定義が適切に記述していることを決定する。

466 拡張コンポーネントが ST で定義された新しいファミリのメンバである場合、評価者は、拡張コンポーネントが既存のファミリにあてはまらないことを確認する。

467 ST が新しいファミリを定義している場合、評価者は各新しいファミリが次のいずれかであることを決定する:

a) 既存の CC パート 2 または CC パート 3 クラスのメンバ; または

b) ST で定義された新しいクラスのメンバ。

468 ファミリが既存の CC パート 2 または CC パート 3 クラスのメンバである場合、評価者は、ファミリがそのクラスのメンバであるべき理由、及びファミリがそのクラス内の他のファミリにどのように関連するかを拡張コンポーネント定義が適切に記述していることを決定する。

469 ファミリが ST で定義された新しいクラスのメンバである場合、評価者は、ファミリが既存のクラスにあてはまらないことを確認する。

ASE_ECD.1-4 評価者は、拡張コンポーネントの各定義がそのコンポーネントのすべての適用可能な依存性を識別することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

470 ST に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

471 評価者は、ST 作成者が見過ごした適用可能な依存性が一つもないことを確認する。

ASE_ECD.1.4C ***拡張コンポーネント定義は、提示モデルとして既存の CC コンポーネント、ファミリ、クラス、及び方法を使用しなければならない。***

ASE_ECD.1-5 評価者は、各拡張機能コンポーネントが提示モデルとして既存の CC パート 2 コンポーネントを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

472 ST に拡張 SFR が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

473 評価者は、拡張機能コンポーネントが CC パート 2、7.1.3 節、「コンポーネント構造」と一貫していることを決定する。

474 拡張機能コンポーネントが操作を使用する場合、評価者は、拡張機能コンポーネントが CC パート 1、8.1 節、「操作」と一貫していることを決定する。

475 拡張機能コンポーネントが既存の機能コンポーネントを下位階層とする場合、評価者は、拡張機能コンポーネントが CC パート 2、7.2.1 節、「コンポーネント変更の強調表示」と一貫していることを決定する。

ASE_ECD.1-6 評価者は、新しい機能ファミリの各定義が提示モデルとして既存の CC 機能ファミリを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

476 ST が新しい機能ファミリを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

477 評価者は、すべての新しい機能ファミリが CC パート 2、7.1.2 節、「ファミリ構造」と一貫するように定義されていることを決定する。

ASE_ECD.1-7 評価者は、新しい機能クラスの各定義が提示モデルとして既存の CC 機能クラスを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

478 ST が新しい機能クラスを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

479 評価者は、すべての新しい機能クラスが CC パート 2、7.1.1 節、「クラス構造」と一貫するように定義されていることを決定する。

ASE_ECD.1-8 評価者は、拡張保証コンポーネントの各定義が提示モデルとして既存の CC パート 3 コンポーネントを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

480 ST に拡張 SAR が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

481 評価者は、拡張保証コンポーネントが CC パート 3、7.1.3 節、「保証コンポーネント構造」と一貫していることを決定する。

482 拡張保証コンポーネントが操作を使用する場合、評価者は、拡張保証コンポーネントが CC パート 1、8.1 節、「操作」と一貫していることを決定する。

483 拡張保証コンポーネントが既存の保証コンポーネントを下位階層とする場合、評価者は、拡張保証コンポーネントが CC パート 3、7.1.3 節、「保証コンポーネント構造」と一貫していることを決定する。

ASE_ECD.1-9 評価者は、定義された各拡張保証コンポーネントに対して、適用可能な方法が提供されたことを決定するために、拡張コンポーネント定義を***検査しなければならない。***

484 ST に拡張 SAR が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

485 評価者は、各拡張 SAR の各評価者アクションエレメントについて、1 つまたは複数のワークユニットが提供されており、指定された評価者アクションエレメントに対するすべてのワークユニットを成功裏に実行することによりそのエレメントが達成されたことが実証されることを決定する。

ASE_ECD.1-10 評価者は、新しい保証ファミリの各定義が提示モデルとして既存の CC 保証ファミリを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

486 ST が新しい保証ファミリを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

487 評価者は、すべての新しい保証ファミリが CC パート 3、7.1.2 節、「保証ファミリの構造」と一貫するように定義されていることを決定する。

ASE_ECD.1-11 評価者は、新しい保証クラスの各定義が提示モデルとして既存の CC 保証クラスを使用することを決定するために、拡張コンポーネント定義を***検査しなければならない。***

488 ST が新しい保証クラスを定義しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

489 評価者は、すべての新しい保証クラスが CC パート 3、7.1.1 節、「保証クラスの構造」と一貫するように定義されていることを決定する。

ASE_ECD.1.5C ***拡張コンポーネントは、エレメントに対する適合または非適合を実証できるように、評価可能で客観的なエレメントで構成されていなければならない。***

ASE_ECD.1-12 評価者は、適合または非適合を実証できるように、各拡張コンポーネントの各エレメントが評価可能であり、客観的な評価要件を述べることを決定するために、拡張コンポーネント定義を***検査しなければならない。***

490 ST に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

491 評価者は、拡張機能コンポーネントのエレメントがテスト可能であり、適切な TSF 表現を通じて追跡可能である方法で述べられていることを決定する。

492 評価者は、拡張保証コンポーネントのエレメントが評価者の主観的な判定を必要としないことも決定する。

493 評価者は、評価可能で客観的であることがすべての評価基準に対して適切であるにもかかわらず、このような特性を証明するための正式な方法が存在しないことは周知の事実であることに留意する。このため、既存の CC 機能コンポーネント及び保証コンポーネントは、この要件に対する適合を構成するものを決定するためのモデルとして使用される。

11.7.1.4 アクション ASE_ECD.1.2E

ASE_ECD.1-13 評価者は、各拡張コンポーネントが既存のコンポーネントを使用して明確に表現できないことを決定するために、拡張コンポーネント定義を***検査しなければならない。***

494 ST に拡張セキュリティ要件が含まれていない場合、このワークユニットは該当しないため、満たされているものとみなされる。

495 評価者は、この決定を行うときに、CC パート 2 及び CC パート 3 からのコンポーネント、ST で定義された他の拡張コンポーネント、これらのコンポーネントの組み合わせ、及びこれらのコンポーネントに対して可能な操作を考慮するべきである。

496 評価者は、このワークユニットの役割は、コンポーネントの不要な重複、つまり、他のコンポーネントを使用して明確に表現できるコンポーネントを排除することであることに留意する。評価者は、既存のコンポーネントを使用して拡張コンポーネントを表現する方法を探す試みとして、操作を含むコンポーネントのすべての可能な組み合わせに対する徹底的探索を行うべきではない。

11.8 セキュリティ要件(ASE_REQ)

11.8.1 サブアクティビティの評価(ASE_REQ.1)

11.8.1.1 目的

497 このサブアクティビティの目的は、SFR と SAR が明確で曖昧さがなく十分に定義されているかどうか、及び SFR と SAR が内部的に一貫しているかどうかを決定することである。

11.8.1.2 入力

498 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.8.1.3 アクション ASE_REQ.1.1E

ASE_REQ.1.1C *セキュリティ要件のステートメントは、SFR 及び SAR を記述しなければならない。*

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

499 評価者は、各 SFR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 2 の個別のコンポーネントに対する参照によって;

b) ST の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) ST が適合を主張する PP に対する参照によって;

d) ST が適合を主張するセキュリティ要件パッケージに対する参照によって;

e) ST での再現によって。

500 すべての SFR に対して同じ識別手段を使用する必要はない。

ASE_REQ.1-2 評価者は、セキュリティ要件のステートメントが SAR を記述していることを*チェックしなければならない。*

501 評価者は、各 SAR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 3 の個別のコンポーネントに対する参照によって;

b) ST の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) ST が適合を主張する PP に対する参照によって;

d) ST が適合を主張するセキュリティ要件パッケージに対する参照によって;

e) ST での再現によって。

502 すべての SAR に対して同じ識別手段を使用する必要はない。

ASE_REQ.1.2C ***SFR とSAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語は、定義されなければならない。***

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

503 評価者は、ST が以下のすべてを定義することを決定する:

- SFR で使用されるサブジェクトとオブジェクト(の種別);
- サブジェクト、利用者、オブジェクト、情報、セッション、及び/または資源のセキュリティ属性(の種別)、これらの属性が取りうる値、及びこれらの値間の関係(例えば、トップシークレット(top_secret)の値は秘密(secret)の値より「高い」);
- SFR で使用される操作(の種別)及びこれらの操作の影響;
- SFR 内の外部エンティティ(の種別);
- 操作を完了することにより SFR 及び/または SAR に導入された他の用語のうち、直ちに理解されないか、またはそれぞれの辞書の定義の範囲外で使用されている用語。

504 このワークユニットの目的は、SFR と SAR が明確に定義されており、曖昧な用語の導入によって誤解が発生しないことを保証することである。このワークユニットは、ST 作成者に強制的に各単語を定義させるなどの極端な方法として、解釈されるべきではない。セキュリティ要件のセットの一般的な読者は、IT、セキュリティ、及びコモンクライテリアに関する適度な知識を持っているものと想定されるべきである。

505 上記のすべては、グループ、クラス、役割、種別によって提示したり、理解しやすくなるようなその他のグループ化または特性化によって提示したりすることができる。

506 評価者は、これらの列挙と定義をセキュリティ要件の一部にする必要はなく、別の節に(一部または全体が)配置される可能性があることに留意する。これは、特に、同じ用語が ST の残りの部分で使用される場合に該当する。

ASE_REQ.1.3C ***セキュリティ要件のステートメントは、セキュリティ要件のすべての操作を識別しなければならない。***

ASE_REQ.1-4 評価者は、セキュリティ要件のステートメントがセキュリティ要件のすべての操作を識別することを***チェックしなければならない。***

507 評価者は、すべての操作が、使用される各 SFR または SAR 内で識別されていることを決定する。識別は、活字印刷上の区別、周辺の文章内での明示的な識別、またはその他の特徴的な手段で達成できる。

ASE_REQ.1.4C ***すべての操作は、正しく実行されなければならない。***

ASE_REQ.1-5 評価者は、すべての割付操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

508 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.1-6 評価者は、すべての繰返し操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

509 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.1-7 評価者は、すべての選択操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

510 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.1-8 評価者は、すべての詳細化操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

511 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.1.5C ***セキュリティ要件の各依存性は、満たされていなければならない。また、満たされない場合は、セキュリティ要件根拠によってそのことが正当化されなければならない。***

ASE_REQ.1-9 評価者は、セキュリティ要件の各依存性が満たされていること、または満たされていない依存性を正当化するセキュリティ要件根拠が提供されていることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

512 依存性は、セキュリティ要件のステートメント内の関連するコンポーネント(またはそれに対して上位階層のコンポーネント)を含めることによって満たされる。依存性を満たすために使用されたコンポーネントは、必要に応じて、実際に依存性を満たすことを保証するために、操作によって変更するべきである。

513 依存性が満たされないことの正当化は、次のいずれかを取り扱うべきである:

a) 依存性が必要でないまたは役立たない理由。この場合、それ以上に詳細な情報は不要;

b) 依存性が TOE の運用環境によって対処されていること。この場合、運用環境のセキュリティ対策方針がこの依存性をどのように対処するかを正当化によって記述するべきである。

ASE_REQ.1.6C ***セキュリティ要件のステートメントは、内部的に一貫していなければならない。***

ASE_REQ.1-10 評価者は、セキュリティ要件のステートメントが内部的に一貫していることを決定するために、そのステートメントを***検査しなければならない。***

514 評価者は、すべての SFR と SAR の組み合わされたセットが内部的に一貫していることを決定する。

515 評価者は、異なるセキュリティ要件が同じ種別の開発者の証拠、事象、操作、データ、実行されるテストなどに対して適用されるか、"すべてのオブジェクト"、"すべてのサブジェクト"などに対して適用されるすべての場合において、これらの要件が競合しないことを決定する。

516 いくつかの考えられる競合は、次のとおりである:

a) 特定の暗号アルゴリズムの設計を秘密に保持することを特定する拡張 SAR、及びオープンソースレビューを特定する別の拡張 SAR;

b) サブジェクト識別情報のログ記録を特定する FAU_GEN.1 監査データ生成、これらのログにアクセスできる利用者を特定する FDP_ACC.1 サブセットアクセス制御、及びサブジェクトの一部のアクションが他のサブジェクトに対して観察不能であるべきであることを特定する FPR_UNO.1 観察不能性。あるアクティビティを参照できるべきではないサブジェクトがこのアクティビティのログにアクセスできる場合、これらの SFR は競合する;

c) 不要になった情報の削除を特定する FDP_RIP.1 サブセット残存情報保護、及び TOE を前の状態に戻すことができることを特定する FDP_ROL.1 基本ロールバック。前の状態へのロールバックに必要な情報が削除されている場合、これらの要件は競合する;

d) 特に一部の繰返しが同じサブジェクト、オブジェクト、または操作を扱う場合の、FDP_ACC.1 サブセットアクセス制御の複数の繰返し。1 つのアクセス制御 SFR がサブジェクトによるオブジェクトに対する操作の実行を許可し、別のアクセス制御 SFR がこれを許可しない場合、これらの要件は競合する。

11.8.2 サブアクティビティの評価(ASE_REQ.2)

11.8.2.1 目的

517 このサブアクティビティの目的は、SFR と SAR が明確で曖昧さがなく十分に定義されているかどうか、SFR と SAR が内部的に一貫しているかどうか、及び SFR が TOE のセキュリティ対策方針を満たしているかどうかを決定することである。

11.8.2.2 入力

518 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.8.2.3 アクション ASE_REQ.2.1E

ASE_REQ.2.1C ***セキュリティ要件のステートメントは、SFR 及び SAR を記述しなければならない。***

ASE_REQ.2-1 評価者は、セキュリティ要件のステートメントが SFR を記述していることを***チェックしなければならない。***

519 評価者は、各 SFR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 2 の個別のコンポーネントに対する参照によって;

b) ST の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) ST が適合を主張する PP 内の個別のコンポーネントに対する参照によって;

d) ST が適合を主張するセキュリティ要件パッケージ内の個別のコンポーネントに対する参照によって;

e) ST での再現によって。

520 すべての SFR に対して同じ識別手段を使用する必要はない。

ASE_REQ.2-2 評価者は、セキュリティ要件のステートメントが SAR を記述していることを***チェックしなければならない。***

521 評価者は、すべての SAR が次の手段のいずれかによって識別されることを決定する:

a) CC パート 3 の個別のコンポーネントに対する参照によって;

b) ST の拡張コンポーネント定義内の拡張コンポーネントに対する参照によって;

c) ST が適合を主張する PP 内の個別のコンポーネントに対する参照によって;

d) ST が適合を主張するセキュリティ要件パッケージ内の個別のコンポーネントに対する参照によって;

e) ST での再現によって。

522 すべての SAR に対して同じ識別手段を使用する必要はない。

ASE_REQ.2.2C ***SFR とSAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語は、定義されなければならない。***

ASE_REQ.2-3 評価者は、SFR 及び SAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語が定義されていることを決定するために、ST を***検査しなければならない。***

523 評価者は、ST が以下のすべてを定義することを決定する:

- SFR で使用されるサブジェクトとオブジェクト(の種別);
- サブジェクト、利用者、オブジェクト、情報、セッション、及び/または資源のセキュリティ属性(の種別)、これらの属性が取りうる値、及びこれらの値間の関係(例えば、トップシークレット(top_secret)の値は秘密(secret)の値より「高い」);
- SFR で使用される操作(の種別)及びこれらの操作の影響;
- SFR 内の外部エンティティ(の種別);
- 操作を完了することにより SFR 及び/または SAR に導入された他の用語のうち、直ちに理解されないか、またはそれぞれの辞書の定義の範囲外で使用されている用語。

524 このワークユニットの目的は、SFR と SAR が明確に定義されており、曖昧な用語の導入によって誤解が発生しないことを保証することである。このワークユニットは、ST 作成者に強制的に各単語を定義させるなどの極端な方法として、解釈されるべきではない。セキュリティ要件のセットの一般的な読者は、IT、セキュリティ、及びコモンクライテリアに関する適度な知識を持っているものと想定されるべきである。

525 上記のすべては、グループ、クラス、役割、種別によって提示したり、理解しやすくなるようなその他のグループ化または特性化によって提示したりすることができる。

526 評価者は、これらの列挙と定義をセキュリティ要件の一部にする必要はなく、別の節に(一部または全体が)配置される可能性があることに留意する。これは、特に、同じ用語が ST の残りの部分で使用される場合に該当する。

ASE_REQ.2.3C ***セキュリティ要件のステートメントは、セキュリティ要件のすべての操作を識別しなければならない。***

ASE_REQ.2-4 評価者は、セキュリティ要件のステートメントがセキュリティ要件のすべての操作を識別することを***チェックしなければならない。***

527 評価者は、すべての操作が、使用される各 SFR または SAR 内で識別されていることを決定する。識別は、活字印刷上の区別、周辺の文章内での明示的な識別、またはその他の特徴的な手段で達成できる。

ASE_REQ.2.4C ***すべての操作は、正しく実行されなければならない。***

ASE_REQ.2-5 評価者は、すべての割付操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

528 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.2-6 評価者は、すべての繰返し操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

529 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.2-7 評価者は、すべての選択操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

530 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.2-8 評価者は、すべての詳細化操作が正しく実行されることを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

531 操作の正しい実行に関するガイダンスについては、CC パート 1、附属書 C、「操作のためのガイダンス」を参照のこと。

ASE_REQ.2.5C ***セキュリティ要件の各依存性は、満たされていなければならない。また、満たされない場合は、セキュリティ要件根拠によってそのことが正当化されなければならない。***

ASE_REQ.2-9 評価者は、セキュリティ要件の各依存性が満たされていること、または満たされていない依存性をセキュリティ要件根拠が正当化することを決定するために、セキュリティ要件のステートメントを***検査しなければならない。***

532 依存性は、セキュリティ要件のステートメント内の関連するコンポーネント(またはそれに対して上位階層のコンポーネント)を含めることによって満たされる。依存性を満たすために使用されたコンポーネントは、必要に応じて、実際に依存性を満たすことを保証するために、操作によって変更するべきである。

533 依存性が満たされないことの正当化は、次のいずれかを取り扱うべきである:

a) 依存性が必要でないまたは役立たない理由。この場合、それ以上に詳細な情報は不要; または

b) 依存性が TOE の運用環境によって対処されていること。この場合、運用環境のセキュリティ対策方針がこの依存性をどのように対処するかを正当化によって記述するべきである。

ASE_REQ.2.6C ***セキュリティ要件根拠は、各 SFR を TOE のセキュリティ対策方針にまでさかのぼらなければならない。***

ASE_REQ.2-10 評価者は、セキュリティ要件根拠が各 SFR を TOE のセキュリティ対策方針にまでさかのぼることを***チェックしなければならない。***

534 評価者は、各 SFR が少なくとも 1 つの TOE のセキュリティ対策方針にまでさかのぼることを決定する。

535 さかのぼることに失敗した場合、セキュリティ要件根拠が不完全であるか、TOE のセキュリティ対策方針が不完全であるか、または SFR が役立つ目的を持っていないことを示す。

ASE_REQ.2.7C ***セキュリティ要件根拠は、SFR が TOE のセキュリティ対策方針のすべてを満たすことを実証しなければならない。***

ASE_REQ.2-11 評価者は、TOE の各セキュリティ対策方針について、SFR がその TOE セキュリティ対策方針を満たすために適していることをセキュリティ要件根拠が実証することを決定するために、そのセキュリティ要件根拠を***検査しなければならない。***

536 TOE のセキュリティ対策方針にまでさかのぼる SFR が一つもない場合、このワークユニットに関係する評価者アクションは不合格判定になる。

537 評価者は、TOE のセキュリティ対策方針に対する正当化が、SFR が十分である(つまり、対策方針にまでさかのぼるすべての SFR が満たされている場合、TOE のセキュリティ対策方針は達成される)ことを実証することを決定する。

538 評価者は、TOE のセキュリティ対策方針にまでさかのぼる各 SFR が必要である(つまり、SFR が満たされている場合、それは実際にセキュリティ対策方針の達成に寄与する)ことも決定する。

539 セキュリティ要件根拠において提供される TOE のセキュリティ対策方針に対する SFR からの追跡は、正当化の一部である場合があるが、それだけでは正当化を構成しないことに注意すること。

ASE_REQ.2.8C ***セキュリティ要件根拠は、なぜ SAR が選ばれたかを説明しなければならない。***

ASE_REQ.2-12 評価者は、セキュリティ要件根拠が、SAR が選ばれた理由を説明していることを***チェックしなければならない。***

540 評価者は、説明が理路整然としており、ST の残りの部分との明白な不一致が SAR 及び説明に含まれていない限り、いかなる説明も正しいことに留意する。

541 SAR と ST の残りの部分との明白な不一致の例として、非常に能力の高い脅威エージェントが含まれているにもかかわらず、このような脅威エージェントから保護しない AVA_VAN SAR が選ばれた場合が挙げられる。

ASE_REQ.2.9C *セキュリティ要件のステートメントは、内部的に一貫していなければならない。*

ASE_REQ.2-13 評価者は、セキュリティ要件のステートメントが内部的に一貫していることを決定するために、そのステートメントを***検査しなければならない。***

542 評価者は、すべての SFR と SAR の組み合わされたセットが内部的に一貫していることを決定する。

543 評価者は、異なるセキュリティ要件が同じ種別の開発者の証拠、事象、操作、データ、実行されるテストなどに対して適用されるか、"すべてのオブジェクト"、"すべてのサブジェクト"などに対して適用されるすべての場合において、これらの要件が競合しないことを決定する。

544 いくつかの考えられる競合は、次のとおりである:

a) 特定の暗号アルゴリズムの設計を秘密に保持することを特定する拡張 SAR、及びオープンソースレビューを特定する別の拡張保証要件;

b) サブジェクト識別情報のログ記録を特定する FAU_GEN.1 監査データ生成、これらのログにアクセスできる利用者を特定する FDP_ACC.1 サブセットアクセス制御、及びサブジェクトの一部のアクションが他のサブジェクトに対して観察不能であるべきであることを特定する FPR_UNO.1 観察不能性。あるアクティビティを参照できるべきではないサブジェクトがこのアクティビティのログにアクセスできる場合、これらの SFR は競合する;

c) 不要になった情報の削除を特定する FDP_RIP.1 サブセット残存情報保護、及び TOE を前の状態に戻すことができることを特定する FDP_ROL.1 基本ロールバック。前の状態へのロールバックに必要な情報が削除されている場合、これらの要件は競合する;

d) 特に一部の繰返しが同じサブジェクト、オブジェクト、または操作を扱う場合の、FDP_ACC.1 サブセットアクセス制御の複数の繰返し。1 つのアクセス制御 SFR がサブジェクトによるオブジェクトに対する操作の実行を許可し、別のアクセス制御 SFR がこれを許可しない場合、これらの要件は競合する。

11.9 TOE 要約仕様(ASE_TSS)

11.9.1 サブアクティビティの評価(ASE_TSS.1)

11.9.1.1 目的

545 このサブアクティビティの目的は、TOE 要約仕様がすべての SFR を扱うかどうか、及び TOE 要約仕様が TOE の他の順序立てられた記述と一貫しているかどうかを決定することである。

11.9.1.2 入力

546 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.9.1.3 アクション ASE_TSS.1.1E

ASE_TSS.1.1C ***TOE 要約仕様は、TOE がどのように各 SFR を満たすかを記述しなければならない。***

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

547 評価者は、セキュリティ要件のステートメントにある各 SFR に対して、その SFR がどのように満たされるかについての記述を TOE 要約仕様が提供することを決定する。

548 評価者は、各記述の目的が開発者がどのように各 SFR を満たそうとしているのかを高いレベルの視点で TOE の潜在的な消費者に提供することであること、また、そのために記述を過度に詳細にするべきではないことに留意する。例えばパスワード認証メカニズムが FIA_UAU.1, FIA_SOS.1 及び FIA_UID.1.を実装するように、しばしばいくつかの SFR がひとつの文脈に実装される。そのため、ふつう、TSS はひとつひとつの SFR に対するテキストによる長いリストでは構成されないが、SFR の完全なグループはひとつの文節により網羅される。

549 統合 TOE の場合、評価者は、どのコンポーネントが各 SFR を提供するか、または各 SFR を満たすためにコンポーネントがどのように組み合わされるか、が明確であることも決定する。

11.9.1.4 アクション ASE_TSS.1.2E

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

550 TOE 概要、TOE 記述、及び TOE 要約仕様は、詳細度を増加させていくように、順序立てられた構成で TOE を記述する。このため、これらの記述は一貫している必要がある。

11.9.2 サブアクティビティの評価(ASE_TSS.2)

11.9.2.1 目的

551 このサブアクティビティの目的は、TOE 要約仕様がすべての SFR を扱うかどうか、TOE 要約仕様が干渉、論理的な改ざん、及びバイパスを扱うかどうか、及び TOE 要約仕様が TOE の他の順序立てられた記述と一貫しているかどうかを決定することである。

11.9.2.2 入力

552 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST

11.9.2.3 アクション ASE_TSS.2.1E

ASE_TSS.2.1C ***TOE 要約仕様は、TOE がどのように各 SFR を満たすかを記述しなければならない。***

ASE_TSS.2-1 評価者は、TOE がどのように各 SFR を満たすかを TOE 要約仕様が記述することを決定するために、その TOE 要約仕様を***検査しなければならない。***

553 評価者は、セキュリティ要件のステートメントにある各 SFR に対して、その SFR がどのように満たされるかについての記述を TOE 要約仕様が提供することを決定する。

554 評価者は、各記述の目的が開発者がどのように各 SFR を満たそうとしているのかを高いレベルの視点で TOE の潜在的な消費者に提供することであること、また、そのために記述を過度に詳細にするべきではないことに留意する。例えばパスワード認証メカニズムが FIA_UAU.1, FIA_SOS.1 及び FIA_UID.1.を実装するように、しばしばいくつかの SFR がひとつの文脈に実装される。そのため、ふつう、TSS はひとつひとつの SFR に対するテキストによる長いリストでは構成されないが、SFR の完全なグループはひとつの文節により網羅される。

555 統合 TOE の場合、評価者は、どのコンポーネントが各 SFR を提供するか、または各 SFR を満たすためにコンポーネントがどのように組み合わされるか、が明確であることも決定する。

ASE_TSS.2.2C ***TOE 要約仕様は、TOE がどのように干渉や論理的な改ざんから自身を保護するかを記述しなければならない。***

ASE_TSS.2-2 評価者は、TOE がどのように干渉及び論理的な改ざんから自身を保護するかを TOE 要約仕様が記述することを決定するために、その TOE 要約仕様を***検査しなければならない。***

556 評価者は、各記述の目的が開発者がどのように干渉及び論理的な改ざんに対する保護を提供しようとしているのかを高いレベルの視点で TOE の潜在的な消費者に提供することであること、また、そのために記述を過度に詳細にするべきではないことに留意する。

557 統合 TOE の場合、評価者は、どのコンポーネントが保護を提供するか、または保護を提供するためにコンポーネントがどのように組み合わされるか、が明確であることも決定する。

ASE_TSS.2.3C ***TOE 要約仕様は、TOE がどのようにバイパスから自身を保護するかを記述しなければならない。***

ASE_TSS.2-3 評価者は、TOE がどのようにバイパスから自身を保護するかを TOE 要約仕様が記述することを決定するために、その TOE 要約仕様を***検査しなければならない。***

558 評価者は、各記述の目的が開発者がどのようにバイパスに対する保護を提供しようとしているのかを高いレベルの視点で TOE の潜在的な消費者に提供することであること、また、そのために記述を過度に詳細にするべきではないことに留意する。

559 統合 TOE の場合、評価者は、どのコンポーネントが保護を提供するか、または保護を提供するためにコンポーネントがどのように組み合わされるか、が明確であることも決定する。

11.9.2.4 アクション ASE_TSS.2.2E

ASE_TSS.2-4 評価者は、TOE 要約仕様が TOE 概要及び TOE 記述と一貫していることを決定するために、その TOE 要約仕様を***検査しなければならない。***

560 TOE 概要、TOE 記述、及び TOE 要約仕様は、詳細度を増加させていくように、順序立てられた構成で TOE を記述する。このため、これらの記述は一貫している必要がある。

12 ADV クラス: 開発

12.1 序説

561 開発アクティビティの目的は、TSF がどのようにして SFR を満たすのか、及びどのようにしてそれらの SFR の実装が改ざんされたりバイパスされたりすることがないようにするのかを理解するための適切性の観点から設計証拠資料を評価することである。これは、TSF 設計証拠資料の次第に詳細になる記述を検査することによって理解することができる。設計証拠資料は、機能仕様(TSF のインタフェースを記述する)、TOE 設計記述(要求されている SFR に関連する機能を実行するためにどのように機能するかという観点から TSF のアーキテクチャを記述する)、及び実装記述(ソースコードレベルの記述)からなる。加えて、セキュリティアーキテクチャ記述(TSF のセキュリティの実施が弱体化されたりバイパスされたりしないしくみを説明するために TSF のアーキテクチャ上の特性を記述する)、内部構造の記述(TSF がどのように構成されているかを分かりやすく記述する)、及びセキュリティ方針モデル(TSF が実施するセキュリティ方針を形式的に記述する)も存在する。

12.2 適用上の注釈

562 設計証拠資料の CC 要件は、提供される情報の量及び詳細さと、情報の提示の形式性の程度によってレベル付けされている。低い方のレベルでは、TSF のセキュリティ上最も重要な部分が最も詳細に記述されており、セキュリティ上の重要性が比較的低い部分については要約のみが示される。さらなる保証は、TSF のセキュリティ上最も重要な部分に関する情報の量や、セキュリティ上の重要性が比較的低い部分についての詳細を増やすことによって得られる。最大の保証が達成されるのは、すべての部分の完全な詳細と情報が提供されたときである。

563 CC は、文書の形式性の程度(すなわち、非形式的かそれとも準形式的か)が階層的であるとみなす。非形式的文書は、自然言語で表された文書である。本方法は、使用すべき特定の言語を規定しない。その件は、制度に任されている。以降の段落は、各種の非形式的文書の内容を区別している。

564 機能仕様は、TSF に対するインタフェースの目的と使用方法を規定する。例えば、オペレーティングシステムが本人であることを示す方法、ファイルを作成する方法、ファイルを変更または削除する方法、ファイルにアクセスできる他の利用者を定義する許可を設定する方法、遠隔マシンと通信する方法を利用者に提示する場合、その機能仕様には、これら各々の機能の記述と、TSF に対する外部から見えるインタフェースとの相互作用を通じてそれらの機能性が実現されるしくみの記述が含まれる。そのような事象の発生を検出し、記録する監査機能性も含まれている場合には、この監査機能性の記述も機能仕様に含まれることが期待される。この機能性は、技術的には利用者によって外部インタフェースで直接呼び出されることはないが、利用者の外部インタフェースで何が起きるかによって確実に影響される。

565 設計記述は、それぞれが理解可能なサービスまたは機能を提供する論理的な区分(サブシステムまたはモジュール)の観点から表現される。例えば、ファイアウォールは、パケットフィルタリング、遠隔管理、監査、接続レベルフィルタリングを取り扱うサブシステムで構成することができる。ファイアウォールの設計記述は、とられるアクションを、入力パケットがファイアウォールに到着したときに各サブシステムがとるアクションとして記述する。

12.3 セキュリティアーキテクチャ(ADV_ARC)

12.3.1 サブアクティビティの評価(ADV_ARC.1)

12.3.1.1 目的

566 このサブアクティビティの目的は、TSF が改ざんされたりバイパスされたりしないように構成されているかどうか、及びセキュリティドメインを提供する TSF でそれらのドメインが互いに分離されているかどうかを決定することである。

12.3.1.2 入力

567 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計;

d) セキュリティアーキテクチャ記述;

e) 実装表現(利用可能な場合);

f) 利用者操作ガイダンス。

12.3.1.3 適用上の注釈

568 自己保護、ドメイン分離、及び非バイパス性の概念は、パート 2 の SFR で表現されているセキュリティ機能性とは区別される。これは、多くの場合、自己保護や非バイパス性が、TSF に直接観察可能なインタフェースを持たないからである。これらはむしろ TOE の設計によって達成される TSF の特性であり、その設計の正しい実装によって実施される。また、これらの特性の評価は、メカニズムの評価ほど直接的ではない。機能性の不在のチェックは機能性の存在のチェックより困難なためである。しかし、これらの特性が満たされていることの決定は、メカニズムが正しく実装されていることの決定と同じように重要である。

569 全体的なアプローチとしては、まず開発者が、上述の特性を満たす TSF と、それらの特性が実際に満たされていることを分析によって確認できる証拠を(証拠資料の形で)提供する。評価者には、その証拠を調べ、TOE のために配付されるその他の証拠と組み合わせて、特性が達成されていることを決定する責任がある。ワークユニットは、提供されなければならない情報の詳細に関するものと、評価者が行う実際の分析に関するものとして捉えることができる。

570 セキュリティアーキテクチャ記述は、ドメインがどのように定義され、TSF がそれらのドメインをどのように分離するかについて記述する。信頼できないプロセスが TSF にアクセスして変更することを回避するものについて記述する。TSF の制御下にあるすべての資源が適切に保護され、SFR に関連するすべてのアクションが TSF によって仲介されることを保証するものについて記述する。環境が次のいずれかにおいて果たす役割(例えば、下層環境によって正しく呼び出されることを想定した場合、セキュリティ機能性がどのように呼び出されるか)を説明する。要するに、セキュリティアーキテクチャ記述は、どのように TOE が各種の *セキュリティ*サービスを提供するように考慮されているかを説明する。

571 評価者が行う分析は、TOE のために提供されるすべての開発証拠にわたって、提供されている証拠の詳細レベルで行われなければならない。保証レベルが低い場合は、上位レベルの設計表現しか利用できないため、例えば TSF の自己保護を完全に分析することなどは期待すべきでない。また評価者は、以降のワークユニットで検査される特性を評定する際には、必ず分析の他の部分(例えば、TOE 設計の分析)から収集された情報を使用する必要がある。

12.3.1.4 アクション ADV_ARC.1.1E

ADV_ARC.1.1C ***セキュリティアーキテクチャ記述は、TOE 設計文書に記述されている SFR 実施抽象概念の記述に見合った詳細レベルでなければならない。***

ADV_ARC.1-1 評価者は、証拠で提供されている情報が、機能仕様とTOE設計文書に含まれているSFR実施抽象概念の記述に見合った詳細レベルで提示されていることを決定するために、セキュリティアーキテクチャ記述を***検査しなければならない。***

572 機能仕様に関しては、評価者は、記述されている自己保護機能性が、TSFI に明白に現れる影響をカバーしていることを保証するべきである。そうした記述には、TSF の実行可能イメージに対する保護や、オブジェクト(例えば、TSF によって使用されるファイル)に対する保護などが含まれる。評価者は、TSFI を通じて呼び出される可能性がある機能性が記述されていることを保証する。

573 サブアクティビティ(ADV_TDS.1)の評価またはサブアクティビティ(ADV_TDS.2)の評価が含まれる場合、評価者は、TSFドメイン分離に寄与するすべてのサブシステムがどのように動くかに関する情報がセキュリティアーキテクチャ記述に含まれていることを保証する。

574 サブアクティビティ(ADV_TDS.3)の評価以上が利用できる場合は、評価者は、セキュリティアーキテクチャ記述が実装依存の情報も含むことを保証する。こうした記述には、例えば、TSF の弱体化(バッファオーバフローなど)を防ぐようなパラメタチェックのためのコーディング規則に関連する情報や、コール操作やリターン操作のためのスタック管理に関する情報などが含まれる。評価者は、詳細レベルがセキュリティアーキテクチャ記述と実装表現との間に曖昧さがほとんどないレベルになっていることを保証するために、メカニズムの記述をチェックする。

575 セキュリティアーキテクチャ記述が機能仕様または TOE 設計文書に記述されないモジュール、サブシステムあるいはインタフェースに言及する場合、このワークユニットに関係する評価者アクションは不合格判定になる。

ADV_ARC.1.2C ***セキュリティアーキテクチャ記述は、TSF によって維持されるセキュリティドメインを、SFR と一貫する形で記述しなければならない。***

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

576 セキュリティドメインとは、TSF によって提供される、有害な可能性があるエンティティが使用するための環境を指す。例えば、一般的なセキュアなオペレーティングシステムでは、アクセス権やセキュリティ特性が制限されたプロセスにより使用される一連の資源(アドレス空間、プロセスごとの環境変数など)が提供される。評価者は、開発者によるセキュリティドメインの記述が、TOEによって要求されるすべてのSFRを考慮したものになっていることを決定する。

577 中にはこうしたドメインが存在しない TOE もあるが、これは、利用者が利用できるすべての対話が TSF によって厳しく制約されているためである。例えば、パケットフィルタリングファイアウォールはそうした TOE に該当する。パケットフィルタリングファイアウォールでは、LAN 上または WAN 上の利用者が TOE と対話することはないため、セキュリティドメインは必要ない。TSF によって維持されるのは、利用者のパケットを分離するためのデータ構造だけである。ドメインがないことが主張されている場合、評価者は、その主張を支持する証拠があること、及びそのようなドメインが実際に不要であることを保証する。

ADV_ARC.1.3C ***セキュリティアーキテクチャ記述は、TSF の初期化プロセスのセキュリティがどのようにして確保されるのかを記述しなければならない。***

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

578 TSF の初期化に関連してセキュリティアーキテクチャ記述で提供される情報の対象は、電源をオンにしたりリセットを行った際に発生する TSF の初期セキュア状態(TSF のすべての部分が運用可能な状態)への移行に関与する TOE コンポーネントである。セキュリティアーキテクチャ記述におけるこの説明では、システム初期化コンポーネントと、「ダウン」状態から初期セキュア状態への移行において発生する処理が列挙されているべきである。

579 セキュアな状態が達成されると、この初期化機能を実行するコンポーネントにアクセスできなくなる場合もよくあるが、そのような場合は、セキュリティアーキテクチャ記述でそれらのコンポーネントを識別し、TSF が確立された後に信頼できないエンティティがそれらのコンポーネントにアクセスできなくなるしくみを説明する。この点に関しては、1)セキュアな状態が達成されると、信頼できないエンティティがこれらのコンポーネントにアクセスすることはできない、または 2)信頼できないエンティティにこれらのコンポーネントへのインタフェースを提供する場合は、それらの TSFI を使用して TSF を改ざんすることはできない、のいずれかの特性が保持されている必要がある。

580 TSF の初期化に関連する TOE コンポーネントは、それ自体 TSF の一部として扱われ、その観点から分析される。ただし、TSF の一部として扱われるとしても、ADV_INT の内部構造要件を満たす必要はないことが(TSF 内部 ADV_INT によって)正当化されることも多いので注意するべきである。

ADV_ARC.1.4C ***セキュリティアーキテクチャ記述は、TSF が改ざんから自分自身を保護することを実証しなければならない。***

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

581 「自己保護」とは、結果として TSF が変更される場合もあるような外部のエンティティによる操作から自分自身を保護する TSF の能力を指す。他の IT エンティティに依存している TOE では、他の IT エンティティによって提供されるサービスを使用して機能を実行することも多い。そのような場合は、TSF 単体では自分自身を保護していない。なぜなら、その保護の一部は、他の IT エンティティに依存することによって提供されるからである。セキュリティアーキテクチャ記述の目的においては、*自己保護*の概念は、TSF が自身の TSFI を通じて提供するサービスのみに適用され、TSF が使用する下層の IT エンティティによって提供されるサービスには適用されない。

582 一般に自己保護は、TOE に対するアクセスの物理的及び論理的な制限からハードウェアベースの手段(例えば、「実行リング」やメモリ管理機能性)やソフトウェアベースの手段(例えば、信頼できるサーバでの入力の境界チェック)に至るまで、様々な手段によって達成される。評価者は、そうしたメカニズムのすべてが記述されていることを決定する。

583 評価者は、TSF が利用者入力によって自分自身を破壊しないように TSF は利用者入力をどのように処理するかが、設計記述でカバーされていることを決定する。例えば TSF は、特権の概念を実装し、特権モードのルーチンを使用して利用者入力を処理することによって、自分自身を保護することができる。それ以外にも、TSF は特権レベルやリングなどのプロセッサベースの分離メカニズムを利用する、TSF はソフトウェアドメインの分離の実装に寄与する(利用者のアドレス空間とシステムのアドレス空間を明確に区別するなど)ソフトウェア保護構造やコーディング規則を実装する、TSF は環境によって提供される支援を TSF の保護に利用する、などの方法もある。

584 ドメイン分離機能に寄与するすべてのメカニズムが記述されている。評価者は、自己保護に寄与する機能性について、セキュリティアーキテクチャ記述に含まれていないものが記述されていないかどうかを決定するために、他の証拠(機能仕様、TOE 設計、TSF 内部構造の記述、セキュリティアーキテクチャ記述のその他の部分、実装表現など、TOE の保証パッケージに含まれているもの)から得た知識を利用するべきである。

585 自己保護メカニズムの記述の正確さとは、実装される内容が忠実に記述されているという特性である。評価者は、自己保護メカニズムの記述に不一致がないかどうかを決定するために、他の証拠(機能仕様、TOE 設計、TSF 内部構造の証拠資料、セキュリティアーキテクチャ記述のその他の部分、実装表現など、TOE の ST に含まれているもの)を使用するべきである。TOE の保証パッケージに実装表現(ADV_IMP)が含まれている場合は、評価者は実装表現のサンプルを選択する。評価者はその選択されたサンプルについて記述が正確であることも保証するべきである。特定の自己保護メカニズムがシステムのアーキテクチャでどのように機能するのか、または機能し得るのかを評価者が理解できない場合は、その記述が不正確かもしれない。

ADV_ARC.1.5C ***セキュリティアーキテクチャ記述は、TSF が SFR 実施機能性のバイパスを防ぐことを実証しなければならない。***

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

586 非バイパス性とは、TSF のセキュリティ機能性(SFR によって特定されている)が常に呼び出されるという特性である。例えば、ファイルのアクセス制御が TSF の機能として SFR で特定されている場合、TSF のアクセス制御メカニズムを呼び出さずにファイルにアクセスできるインタフェースがあってはならない(ローディスクアクセスが発生するインタフェースなど)。

587 TSF メカニズムをバイパスできないようにするしくみについての記述では、通常、TSF と TSFI に基づく系統的な論証が要求される。TSF がどのように機能するかの記述(機能仕様や TOE 設計証拠資料など、設計の分解の証拠に含まれる)は、TSS の情報とともに、保護される資源や提供されるセキュリティ機能の理解に必要な背景を評価者に提供する。機能仕様は、資源や機能へのアクセスに使用される TSFI の記述を提供する。

588 評価者は、TSF のバイパスに使うことのできるインタフェースがないことを保証するために、提供される記述(及び開発者によって提供される機能仕様などのその他の情報)を評定する。これは、利用可能なインタフェースはすべて、ST で主張されている SFR とは無関係である(SFR を満たすために使用される要素との対話も行われない)か、そうでなければ、他の開発証拠に記述されたセキュリティ機能性を、記述された方法で使用しなければならないことを意味する。例えば、ゲームは SFR とは無関係であると考えられるが、その場合は、どうしてセキュリティに影響を与えないかの説明がなければならない。一方、利用者データへのアクセスはアクセス制御の SFR に関連すると考えられるので、データアクセスインタフェースを通じて呼び出された場合にセキュリティ機能性がどのように機能するかの説明が記述される。利用可能なすべてのインタフェースについて、こうした説明が必要である。

589 以下は記述の例である。まず、TSF がファイルの保護を提供するとする。さらに、オープン、読み取り、及び書き込みのための「従来の」システムコールの TSFI では、TOE 設計に記述されているファイル保護メカニズムが呼び出されるが、それ以外に、バッチジョブ機能(バッチジョブの作成、ジョブの削除、未処理のジョブの改変)へのアクセスを提供する TSFI も存在するとする。評価者は、ベンダが提供する記述から、この TSFI が「従来の」インタフェースの場合と同じ保護メカニズムを呼び出すことを決定できるべきである。これは、例えば、TOE 設計の適切な節(バッチジョブ機能の TSFI がそのセキュリティ対策方針を*どのようにして*達成するのかが論じられている)を参照することによって可能となる。

590 同じ例で、現在の時刻を表示することだけを目的とする TSFI があったとする。この場合、評価者は、この TSFI では保護されている資源を一切操作できないこと、及びこの TSFI は一切のセキュリティ機能性を呼び出すべきでないことが、記述の中で適切に論証されていることを決定するべきである。

591 別のパイパス例として、暗号鍵の機密性を維持する TSF を仮定する(暗号鍵は暗号操作に使用できるが、暗号鍵の読み書きは許可されない)。ある攻撃者が装置に直接的かつ物理的にアクセスできる場合、この攻撃者は、装置の電力消費や装置の正確なタイミング、さらには装置の電磁波放射といった副次的チャネルを検査し、それによって暗号鍵を推測できる場合がある。

592 このような副次的チャネルが存在する場合、実証では、ランダムインターナルクロックやデュアルライン技術など、これらの副次的チャネルの発生を防止するためのメカニズムを取り扱うべきである。これらのメカニズムは、純粋な設計に基づく論証とテストの組み合わせによって検証される。

593 最後に、保護されている資源ではなくセキュリティ機能性を使用する例として、FCO_NRO.2 発信の強制的証明(TSF が ST で特定されている情報種別の発信元の証拠を提供することを要求する)を含む ST について検討する。ここで、「情報種別」には、TOE によって電子メールで送信されるすべての情報が含まれるとする。このような場合、評価者は、電子メールを送信するために呼び出される可能性があるすべての TSFI が「発信元の証拠の生成」機能を実行することが詳細に述べられていることを保証するために、記述を検査するべきである。この記述では、利用者ガイダンスを参照するなどして、電子メールが発信される可能性があるすべての場所(例えば、電子メールプログラムやスクリプト/バッチジョブからの通知)と、それらの場所でそれぞれどのようにして証拠生成機能が呼び出されるかが示される。

594 また評価者は、主張された SFR の全体のセットについて各インタフェースが分析されているという点において、記述が包括的であることを保証するべきである。そのためには、補足情報(TOE のために提供されている機能仕様、TOE 設計、セキュリティアーキテクチャ記述のその他の部分、利用者操作ガイダンス、及び場合によっては実装表現まで)を検査して、インタフェースのすべての側面が記述に正確に盛り込まれていることを決定しなければならない場合もある。評価者は、各 TSFI がどの SFR に影響するのかを(補足情報となる証拠資料の TSFI 及びその実装についての記述から)考慮し、それらの側面がカバーされているかどうかを決定するために記述を検査するべきである。

12.4 機能仕様(ADV_FSP)

12.4.1 サブアクティビティの評価(ADV_FSP.1)

12.4.1.1 目的

595 このサブアクティビティの目的は、パラメタの記述の観点から、少なくとも SFR 実施及び SFR 支援の TSFI について、開発者によって上位レベルの記述が提供されているかどうかを決定することである。これらの記述の正確さを測定する際に利用が期待できる証拠はほかに要求されていないため、評価者が保証できるのは、記述が信頼できそうかどうかだけである。

12.4.1.2 入力

596 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) 利用者操作ガイダンス;

12.4.1.3 アクション ADV_FSP.1.1E

ADV_FSP.1.1C ***機能仕様は、SFR 実施及び SFR 支援の各 TSFI の目的と使用方法を記述しなければならない。***

ADV_FSP.1-1 評価者は、機能仕様が SFR 支援及び SFR 実施の各 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。***

597 TSFI の目的とは、インタフェースによって提供される機能性を要約する一般的なステートメントである。そこで意図されているのは、インタフェースに関連するアクション及び結果の完全なステートメントではなく、そのインタフェースが何のために使用されるものなのかを読者が大まかに理解できるようにするためのステートメントである。評価者は、目的が存在することだけでなく、そこに TSFI が正確に反映されていることも、パラメタの記述など、インタフェースに関するその他の情報を考慮に入れて決定するべきである。この作業は、このコンポーネントの他のワークユニットと組み合わせて行うことができる。

598 インタフェースを通じて利用可能なアクションが、TOE のセキュリティ方針を実施するうえで何らかの役割を果たしている場合(TSF に課されている SFR のいずれかにたどれるアクションがインタフェースにある場合)、そのインタフェースは *SFR 実施*である。ここで言う方針とは、アクセス制御方針に限定されるものではなく、ST に含まれている SFR のいずれかで特定されるあらゆる機能性を指す。なお、インタフェースには様々なアクション及び結果が含まれている可能性があり、その中には、SFR 実施のものもそれ以外のものもあるので注意する必要がある。

599 SFR 実施機能性が依存しているが、TOE のセキュリティ方針を保持するために正しく機能することだけが要求されるアクションへのインタフェース(またはそのアクションに関連するインタフェースを通じて利用可能なアクション)は、*SFR 支援*と呼ばれる。SFR 実施機能性が一切依存していないアクションへのインタフェースは、*SFR 非干渉*と呼ばれる。

600 インタフェースを SFR 支援または SFR 非干渉とする場合、そのインタフェースには SFR 実施のアクションや結果が含まれてはならないという点に注意するべきである。一方、SFR 実施インタフェースは、SFR 支援アクションを含むこともできる(例えば、システムの時刻を設定するアクションは SFR 実施アクションで、それと同じインタフェースを使用するシステムの日付を表示するアクションは SFR 支援という場合もある)。純粋な SFR 支援インタフェースの例としては、信頼できない利用者と、利用者モードで実行される TSF の一部の両方が使用するシステムコールインタフェースなどがある。

601 このレベルでは、開発者がわざわざインタフェースを SFR 実施や SFR 支援に分類するとは考えにくい。しかし、実際に分類されていた場合は、評価者が、証拠資料(例えば、利用者操作ガイダンス)から可能となる範囲で、その識別が正しいことを検証するべきである。この識別のアクティビティは、このコンポーネントの複数のワークユニットで必要となる。

602 より一般的なケース、すなわち開発者によってインタフェースが分類されていない場合は、評価者はまず自分でインタフェースの識別を行ってから、必要な情報(このワークユニットの情報や目的)が存在するかどうかを決定する必要がある。ここでもまた、裏付けとなる証拠がないためにこの識別は困難となり、該当するインタフェースがすべて正しく識別されているという保証のレベルも低くなる。それでも評価者は、TOE について利用可能なその他の証拠を検査して、できる限り完全なカバレージを保証する。

ADV_FSP.1-2 評価者は、SFR 支援及び SFR 実施の各 TSFI の使用方法が記述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。***

603 SFR 支援及び SFR 実施の TSFI の識別については、ワークユニット ADV_FSP.1-1 を参照のこと。

604 TSFI の使用方法とは、アクションを呼び出して TSFI に関連する結果を取得するためには、インタフェースをどのように操作するのかを要約したものである。評価者は、機能仕様の中のこの資料を読むことにより、各インタフェースの使用方法を決定できるべきである。これは必ずしも、各 TSFI にそれぞれ異なる使用方法が必要ということではない。例えば、カーネルコールを呼び出す一般的な方法を記述してから、その一般的なスタイルを使用する各インタフェースを識別することも可能である。インタフェースの種別が変わると、別の使用方法の仕様が必要になる。API、ネットワークプロトコルインタフェース、システム設定パラメタ、及びハードウェアバスインタフェースには、それぞれにまったく異なる使用方法がある。機能仕様を評価する評価者と同様に、機能仕様を作成する開発者も、このことを考慮に入れて作業するべきである。

605 証拠資料によって、信頼できない利用者はその機能性にアクセスできないとされている管理インタフェースについては、その機能にアクセスできないようにする方法が機能仕様に記述されていることを評価者が保証する。このアクセス不可能性は、開発者のテストスイートでテストされる必要があるという点に注意するべきである。

ADV_FSP.1.2C ***機能仕様は、SFR 実施及びSFR 支援の各 TSFI に関連するすべてのパラメタを識別しなければならない。***

ADV_FSP.1-3 評価者は、TSFI の提示が SFR 実施及び SFR 支援の各 TSFI に関連するすべてのパラメタを識別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。***

606 SFR 支援及び SFR 実施の TSFI の識別については、ワークユニット ADV_FSP.1-1 を参照のこと。

607 評価者は、識別された TSFI のすべてのパラメタが記述されていることを保証するために、機能仕様を検査する。パラメタとは、インタフェースに対する明示的な入力または出力であり、そのインタフェースのふるまいを制御する。例えば、API に渡される引数、特定のネットワークプロトコルのパケットの様々なフィールド;Windows レジストリの個々のキーの値;チップの一連のピンでやり取りされる信号;などがパラメタである。

608 該当する TSFI のすべてのパラメタが識別されていることについて多くの保証を得るのは困難だが、評価者は、評価のために提供されているその他の証拠(例えば、利用者操作ガイダンス)もチェックして、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べきである。

ADV_FSP.1.3C ***機能仕様は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類の根拠を示さなければならない。***

ADV_FSP.1-4 評価者は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類が正しいことを決定するために、開発者によって提供される根拠を***検査しなければならない。***

609 このコンポーネントの残りのワークユニットで要求される分析を行うのに十分な証拠資料が開発者によって提供されていて、SFR 実施及び SFR 支援のインタフェースは明示的に識別されていない場合、このワークユニットは満たされているものとみなされるべきである。

610 このワークユニットの対象として想定されているのは、開発者が TSFI の一部を記述せずに、その部分について、SFR 非干渉であるためこのコンポーネントの他の要件の対象にはならないと主張している場合である。そのような場合、開発者は、この特性化に対する根拠を提供する。その根拠では、評価者がその根拠や、影響を受けるインタフェースの特性(例えば、「カラーパレットの操作」など、TOE に関する上位レベルの機能)を把握し、それらが SFR 非干渉であるという主張が支持されていると理解できるだけの詳細さが必要とされる。保証のレベルからして、評価者は、SFR 実施もしくは SFR 支援のインタフェースについて提供されている以上の詳細を期待すべきではない。実際、詳細はそれよりはるかに少ないのが普通である。ほとんどの場合は、開発者が提供する根拠の節でインタフェースが個別に取り上げられている必要性があるとすべきではない。

ADV_FSP.1.4C ***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。***

ADV_FSP.1-5 評価者は、追跡によって SFR が対応する TSFI にリンクされることを***チェックしなければならない。***

611 追跡は、どの SFR がどの TSFI に関連するかを示す指針として、開発者が提供する。この追跡は表のように単純化できる。評価者は、続くワークユニットで追跡を入力として使用して、その完全さと正確さを検証する。

12.4.1.4 アクション ADV_FSP.1.2E

ADV_FSP.1-6 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。***

612 すべての SFR が機能仕様、及びテストカバレージ分析によってカバーされていることを保証するために、評価者は開発者の追跡を土台にすることができる(ADV_FSP.1-5の TOE セキュリティ機能要件と TSFI の間のマッピングを参照のこと)。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、詳細レベルが要件のコンポーネントレベルより下、さらにはエレメントレベルより下でなければならない場合もあるので注意する必要がある。

613 例えば、FDP_ACC.1コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1の割付に 10 の規則が含まれていたとして、その 10 の規則が 3 つの異なる TSFI によってカバーされていた場合、評価者がFDP_ACC.1を TSFI A、B、及び C にマッピングして、ワークユニットが完了したと主張するのは適切でない。この場合、評価者は、FDP_ACC.1 (規則 1)を TSFI A に、FDP_ACC.1 (規則 2)を TSFI B にという形でマッピングを行うべきである。また、インタフェースがラッパーインタフェースである場合も考えられるが(例えば、IOCTL)、その場合には、特定のインタフェースの特定のパラメタセットに固有のマッピングが必要となる。

614 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。また、TSFI に関連付けられているパラメタは完全に特定されていなければならないため、評価者は、SFR のすべての側面がインタフェースレベルで実装されているように見えるかどうかを決定できるべきであるという点も重要である。

ADV_FSP.1-7 評価者は、機能仕様が SFR の正確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。***

615 TSF 境界で見ることのできる効果をもたらす ST の各機能要件について、要件によって記述されている必要な機能性が、その要件に関連付けられている TSFI の情報によって特定される。例えば、アクセス制御リストの要件が ST に含まれていて、その要件にマッピングされている唯一の TSFI で Unix スタイルの保護ビットの機能性が特定されていた場合、その機能仕様は、その要件に対しては正確ではない。

616 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。

12.4.2 サブアクティビティの評価(ADV_FSP.2)

12.4.2.1 目的

617 このサブアクティビティの目的は、TSFI の目的、使用方法、及びパラメタの観点から、開発者によって TSFI の記述が提供されているかどうかを決定することである。さらに、SFR 実施の各 TSFI の SFR 実施アクション、結果、及び誤りメッセージも記述されている必要がある。

12.4.2.2 入力

618 ワークユニットで必要とされるこのサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計。

619 TOE の ST に含まれている場合に使用されるこのサブアクティビティ用の評価証拠は、次のとおりである:

a) セキュリティアーキテクチャ記述;

b) 利用者操作ガイダンス。

12.4.2.3 **アクション** ADV_FSP.2.1E

ADV_FSP.2.1C ***機能仕様は、完全に TSF を表現しなければならない。***

ADV_FSP.2-1 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。***

620 TSFI の識別は、このサブアクティビティの他のすべてのアクティビティの必要条件となる。TSFI を識別するためには、TSF が識別されていなければならない(TOE 設計(ADV_TDS)ワークユニットの一部として行われる)。このアクティビティは、インタフェースの大きなグループ(ネットワークプロトコル、ハードウェアインタフェース、設定ファイル)に欠けているものがないことを保証するために上位レベルで行うことも、機能仕様の評価と並行して下位レベルで行うこともできる。

621 このワークユニットの評定を行うとき、評価者は、機能仕様にリストされているインタフェースの観点から TSF のすべての部分が扱われていることを決定する。TSF のすべての部分にそれぞれ対応するインタフェース記述があるべきである。対応するインタフェースがない部分がある場合は、それが受け入れられるかどうかを評価者が決定する。

ADV_FSP.2.2C ***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.2-2 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。***

622 TSFI の目的とは、インタフェースによって提供される機能性を要約する一般的なステートメントである。そこで意図されているのは、インタフェースに関連するアクション及び結果の完全なステートメントではなく、そのインタフェースが何のために使用されるものなのかを読者が大まかに理解できるようにするためのステートメントである。評価者は、目的が存在することだけでなく、そこに TSFI が正確に反映されていることも、アクションの記述や誤りメッセージなど、インタフェースに関するその他の情報を考慮に入れて決定するべきである。

ADV_FSP.2-3 評価者は、各 TSFI の使用方法が記述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。***

623 TSFI の使用方法とは、アクションを呼び出して TSFI に関連する結果を取得するためには、インタフェースをどのように操作するのかを要約したものである。評価者は、機能仕様の中のこの資料を読むことにより、各インタフェースの使用方法を決定できるべきである。これは必ずしも、各 TSFI にそれぞれ異なる使用方法が必要ということではない。例えば、カーネルコールを呼び出す一般的な方法を記述してから、その一般的なスタイルを使用する各インタフェースを識別することも可能である。インタフェースの種別が変わると、別の使用方法の仕様が必要になる。API、ネットワークプロトコルインタフェース、システム設定パラメタ、及びハードウェアバスインタフェースには、それぞれにまったく異なる使用方法がある。機能仕様を評価する評価者と同様に、機能仕様を作成する開発者も、このことを考慮に入れて作業するべきである。

624 証拠資料によって、信頼できない利用者はその機能性にアクセスできないとされている管理インタフェースについては、その機能にアクセスできないようにする方法が機能仕様に記述されていることを評価者が保証する。このアクセス不可能性は、開発者のテストスイートでテストされる必要があるという点に注意するべきである。

625 評価者は、使用方法の記述のセットが存在することだけでなく、それらが各 TSFI を正確にカバーしていることも決定するべきである。

ADV_FSP.2.3C ***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.2-4 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に識別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。***

626 評価者は、各 TSFI のすべてのパラメタが記述されていることを保証するために、機能仕様を検査する。パラメタとは、インタフェースに対する明示的な入力または出力であり、そのインタフェースのふるまいを制御する。例えば、API に渡される引数、特定のネットワークプロトコルのパケットの様々なフィールド、Windows レジストリの個々のキーの値、チップの一連のピンでやり取りされる信号などがパラメタである。

627 すべてのパラメタが TSFI に含まれていることを決定するには、評価者は、パラメタの効果の説明が記述に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(アクションや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、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、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。

ADV_FSP.2-5 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。***

628 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。

629 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。

ADV_FSP.2.4C ***各 SFR 実施 TSFI について、機能仕様は、その TSFI に関連する SFR 実施アクションを記述しなければならない。***

ADV_FSP.2-6 評価者は、TSFI の提示が SFR 実施 TSFI に関連する SFR 実施アクション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。***

630 インタフェースを通じて利用可能なアクションが、TSF に課されている SFR のいずれかにたどれる場合、そのインタフェースは *SFR 実施*である。ここで言う方針とは、アクセス制御方針に限定されるものではなく、ST に含まれている SFR のいずれかで特定されるあらゆる機能性を指す。なお、インタフェースには様々なアクション及び結果が含まれている可能性があり、その中には、SFR 実施のものもそれ以外のものもあるので注意する必要がある。

631 開発者には、インタフェースを SFR 実施として「分類」することは要求されない。同様に、インタフェースを通じて利用できるアクションを SFR 実施として識別することも要求されない。開発者によって提供される証拠を検査して、必要な情報が含まれていることを決定するのが、評価者の責任である。SFR 実施 TSFI と、それらの TSFI を通じて利用できる SFR 実施アクションが開発者によって識別されていた場合、評価者は、評価のために提供されているその他の情報(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス)と、インタフェースのために提示されているその他の情報(パラメタ、パラメタの記述、誤りメッセージなど)に基づいて、その完全さ及び正確さを判断しなければならない。

632 この場合(開発者が SFR 実施 TSFI の SFR 実施の情報のみを提供している場合)、評価者は、間違って分類されているインタフェースがないことも保証する。これは、評価のために提供されているその他の情報(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス)や、SFR 実施と分類されていないインタフェースのために提示されているその他の情報(例えば、パラメタやパラメタの記述)を検査することによって行われる。

633 開発者がすべてのインタフェースについて同じレベルの情報を提供している場合、評価者は、これまでの段落までで述べたのと同じ種別の分析を行う。評価者は、どのインタフェースが SFR 実施でどのインタフェースがそうでないかを決定し、その後、SFR 実施アクションについて SFR 実施の側面が適切に記述されていることを保証するべきである。

634 SFR 実施アクションとは、主張されている SFR の実施を提供する、任意の外部インタフェースで見ることのできるアクションである。例えば、ST に監査の要件が含まれていた場合、監査関連のアクションは SFR 実施になるため、記述されていなければならない。これは、そのアクションの結果が、通常は呼び出されたインタフェースでは見ることができない場合でも変わらない(監査では、あるインタフェースでの利用者のアクションの結果として、別のインタフェースで見ることができる監査記録が生成されるため、このような場合が一般的である)。

635 記述には、SFR に関して TSFI アクションがどのような役割を果たすのかを読者が理解できるレベルが要求される。評価者は、そのインタフェースに対するテストケースを生成(及び評定)できるだけの詳細さが記述に必要であるということを忘れないようにするべきである。記述が不明確であったり詳細さに欠けていたりして、TSFI に対して意味のあるテストを実施できない場合、その記述は不適切であると考えられる。

ADV_FSP.2.5C ***各 SFR 実施 TSFI について、機能仕様は、SFR 実施アクションに関連する処理によって発生する誤りメッセージを記述しなければならない。***

ADV_FSP.2-7 評価者は、TSFI の提示が各 SFR 実施 TSFI に関連する SFR 実施アクションによって発生する可能性がある誤りメッセージ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。***

636 このワークユニットは、SFR 実施 TSFI と SFR 実施アクションのセットが正しく識別されていることを保証するために、ワークユニット ADV_FSP.2-6 とともに(またはその後に)実行されるべきである。必要以上の情報(例えば、各インタフェースに関連するすべての誤りメッセージ)が開発者によって提供されることがある。その場合、評価者は、どの情報が SFR 実施 TSFI の SFR 実施アクションに関連するかを決定し、完全さ及び正確さの評定の対象をそれらに制限するべきである。

637 誤りは、記述されているインタフェースによって様々な形をとる。API の場合、誤りコードを返す、グローバルな誤り状態を設定する、誤りコードで特定のパラメタを設定するなどの操作が、インタフェース自体によって行われる。設定ファイルの場合は、パラメタの設定に誤りがあると、ログファイルに誤りメッセージが書き込まれる。ハードウェア PCI カードの場合は、誤り状態によってバスで信号が発生したり、CPU に対する例外条件が発生したりする。

638 誤り(及び関連する誤りメッセージ)は、インタフェースの呼び出しを通じて発生する。インタフェースの呼び出しに応じて発生する処理で誤り状態が検出されると、誤りメッセージが(実装固有のメカニズムによって)生成される。これは、インタフェース自身から返される戻り値である場合もあれば、インタフェースの呼び出しの後にグローバルな値が設定されてチェックされる場合もある。一般に TOE には、「ディスクフル」や「資源のロック」など、資源の基本的な状態を原因とする下位レベルの誤りメッセージがいくつか用意されている。これらの誤りメッセージは、多数の TSFI にマッピングされている場合もあるが、インタフェース記述の詳細の漏れを見つけるために使用できる。例えば、「ディスクフル」メッセージを生成する TSFI があり、その TSFI のアクションの記述に、その TSFI でディスクへのアクセスが発生する理由についての明白な記述がない場合、評価者は、その記述が正確かどうかを決定するために、その TSFI に関連するその他の証拠(セキュリティアーキテクチャ(ADV_ARC)や TOE 設計(ADV_TDS))を検査する必要がある。

639 TSFI の誤りメッセージの記述が正確かつ完全であることを決定するには、評価者は、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス)や、その TSFI について利用可能なその他の証拠(パラメタやワークユニットADV_FSP.2-6の分析)に照らしてインタフェース記述を評価する。

ADV_FSP.2.6C ***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。***

ADV_FSP.2-8 評価者は、追跡によって SFR が対応する TSFI にリンクされることを***チェックしなければならない。***

640 追跡は、どの SFR がどの TSFI に関連するかを示す指針として、開発者が提供する。この追跡は表のように単純化できる。評価者は、続くワークユニットで追跡を入力として使用して、その完全さと正確さを検証する。

12.4.2.4 **アクション** ADV_FSP.2.2E

ADV_FSP.2-9 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。***

641 すべての SFR が機能仕様、及びテストカバレージ分析によってカバーされていることを保証するために、評価者は開発者の追跡を土台にすることができる(ADV_FSP.2-8の TOE セキュリティ機能要件と TSFI の間のマッピングを参照のこと。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、詳細レベルが要件のコンポーネントレベルより下、さらにはエレメントレベルより下でなければならない場合もあるので注意する必要がある)。

642 例えば、FDP_ACC.1コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1の割付に 10 の規則が含まれていたとして、その 10 の規則が 3 つの異なる TSFI によってカバーされていた場合、評価者がFDP_ACC.1を TSFI A、B、及び C にマッピングして、ワークユニットが完了したと主張するのは適切でない。この場合、評価者は、FDP_ACC.1 (規則 1)を TSFI A に、FDP_ACC.1 (規則 2)を TSFI B にという形でマッピングを行うべきである。また、インタフェースがラッパーインタフェースである場合も考えられるが(例えば、IOCTL)、その場合には、特定のインタフェースの特定のパラメタセットに固有のマッピングが必要となる。

643 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。また、TSFI に関連付けられているパラメタ、アクション、及び誤りメッセージは完全に特定されていなければならないため、評価者は、SFR のすべての側面がインタフェースレベルで実装されているように見えるかどうかを決定できるべきであるという点も重要である。

ADV_FSP.2-10 評価者は、機能仕様が SFR の正確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。***

644 TSF 境界で見ることのできる効果をもたらす ST の各機能要件について、要件によって記述されている必要な機能性が、その要件に関連付けられているTSFIの情報によって特定される。例えば、アクセス制御リストの要件が ST に含まれていて、その要件にマッピングされている唯一の TSFI で Unix スタイルの保護ビットの機能性が特定されていた場合、その機能仕様は、その要件に対しては正確ではない。

645 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。

12.4.3 サブアクティビティの評価(ADV_FSP.3)

12.4.3.1 目的

646 このサブアクティビティの目的は、TSFIの目的、使用方法、及びパラメタの観点から、開発者によって TSFI の記述が提供されているかどうかを決定することである。さらに、各 TSFI のアクション、結果、及び誤りメッセージについても、それらが SFR 実施かどうかを決定できる程度に記述されていること、SFR 実施 TSFI については他の TSFI より詳しく記述されていることが必要とされる。

12.4.3.2 入力

647 ワークユニットで必要とされるこのサブアクティビティ用の評価証拠は、次のとおりである。

a) ST;

b) 機能仕様;

c) TOE 設計。

648 TOE の ST に含まれている場合に使用されるこのサブアクティビティ用の評価証拠は、次のとおりである:

a) セキュリティアーキテクチャ記述;

b) 実装表現;

c) TSF 内部構造の記述;

d) 利用者操作ガイダンス;

12.4.3.3 **アクション** ADV_FSP.3.1E

ADV_FSP.3.1C ***機能仕様は、完全に TSF を表現しなければならない。***

ADV_FSP.3-1 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。***

649 TSFI の識別は、このサブアクティビティの他のすべてのアクティビティの必要条件となる。TSFI を識別するためには、TSF が識別されていなければならない(TOE 設計(ADV_TDS)ワークユニットの一部として行われる)。このアクティビティは、インタフェースの大きなグループ(ネットワークプロトコル、ハードウェアインタフェース、設定ファイル)に欠けているものがないことを保証するために上位レベルで行うことも、機能仕様の評価と並行して下位レベルで行うこともできる。

650 このワークユニットの評定を行うとき、評価者は、機能仕様にリストされているインタフェースの観点から TSF のすべての部分が扱われていることを決定する。TSF のすべての部分にそれぞれ対応するインタフェース記述があるべきである。対応するインタフェースがない部分がある場合は、それが受け入れられるかどうかを評価者が決定する。

ADV_FSP.3.2C ***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.3-2 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。***

651 TSFI の目的とは、インタフェースによって提供される機能性を要約する一般的なステートメントである。そこで意図されているのは、インタフェースに関連するアクション及び結果の完全なステートメントではなく、そのインタフェースが何のために使用されるものなのかを読者が大まかに理解できるようにするためのステートメントである。評価者は、目的が存在することだけでなく、そこに TSFI が正確に反映されていることも、アクションの記述や誤りメッセージなど、インタフェースに関するその他の情報を考慮に入れて決定するべきである。

ADV_FSP.3-3 評価者は、各 TSFI の使用方法が記述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。***

652 TSFI の使用方法とは、アクションを呼び出して TSFI に関連する結果を取得するためには、インタフェースをどのように操作するのかを要約したものである。評価者は、機能仕様の中のこの資料を読むことにより、各インタフェースの使用方法を決定できるべきである。これは必ずしも、各 TSFI にそれぞれ異なる使用方法が必要ということではない。例えば、カーネルコールを呼び出す一般的な方法を記述してから、その一般的なスタイルを使用する各インタフェースを識別することも可能である。インタフェースの種別が変わると、別の使用方法の仕様が必要になる。API、ネットワークプロトコルインタフェース、システム設定パラメタ、及びハードウェアバスインタフェースには、それぞれにまったく異なる使用方法がある。機能仕様を評価する評価者と同様に、機能仕様を作成する開発者も、このことを考慮に入れて作業するべきである。

653 証拠資料によって、信頼できない利用者はその機能性にアクセスできないとされている管理インタフェースについては、その機能にアクセスできないようにする方法が機能仕様に記述されていることを評価者が保証する。このアクセス不可能性は、開発者のテストスイートでテストされる必要があるという点に注意するべきである。

654 評価者は、使用方法の記述のセットが存在することだけでなく、それらが各 TSFI を正確にカバーしていることも決定するべきである。

ADV_FSP.3.3C ***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.3-4 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に識別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。***

655 評価者は、各 TSFI のすべてのパラメタが記述されていることを保証するために、機能仕様を検査する。パラメタとは、インタフェースに対する明示的な入力または出力であり、そのインタフェースのふるまいを制御する。例えば、API に渡される引数、特定のネットワークプロトコルのパケットの様々なフィールド、Windows レジストリの個々のキーの値、チップの一連のピンでやり取りされる信号などがパラメタである。

656 すべてのパラメタが TSFI に含まれていることを決定するには、評価者は、パラメタの効果の説明が記述に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(アクションや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、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、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。

ADV_FSP.3-5 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。***

657 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。

658 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。

ADV_FSP.3.4C ***各 SFR 実施 TSFI について、機能仕様は、その TSFI に関連する SFR 実施アクションを記述しなければならない。***

ADV_FSP.3-6 評価者は、TSFI の提示が SFR 実施 TSFI に関連する SFR 実施アクション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。***

659 インタフェースを通じて利用可能なアクションが、TOE のセキュリティ方針を実施するうえで何らかの役割を果たしている場合(TSF に課されている SFR のいずれかにたどれるアクションがインタフェースにある場合)、そのインタフェースは SFR 実施である。ここで言う方針とは、アクセス制御方針に限定されるものではなく、ST に含まれている SFR のいずれかで特定されるあらゆる機能性を指す。なお、インタフェースには様々なアクション及び結果が含まれている可能性があり、その中には、SFR 実施のものもそれ以外のものもあるので注意する必要がある。

660 開発者には、インタフェースを SFR 実施として「分類」することは要求されない。同様に、インタフェースを通じて利用できるアクションを SFR 実施として識別することも要求されない。開発者によって提供される証拠を検査して、必要な情報が含まれていることを決定するのが、評価者の責任である。SFR 実施 TSFI と、それらの TSFI を通じて利用できる SFR 実施アクションが開発者によって識別されていた場合、評価者は、評価のために提供されているその他の情報(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス)と、インタフェースのために提示されているその他の情報(パラメタ、パラメタの記述、誤りメッセージなど)に基づいて、その完全さ及び正確さを判断しなければならない。

661 この場合(開発者が SFR 実施 TSFI の SFR 実施の情報のみを提供している場合)、評価者は、間違って分類されているインタフェースがないことも保証する。これは、評価のために提供されているその他の情報(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス)や、SFR 実施と分類されていないインタフェースのために提示されているその他の情報(例えば、パラメタやパラメタの記述)を検査することによって行われる。このほか、この決定を行うときには、ワークユニットADV_FSP.3-7とADV_FSP.3-8で行った分析も使用する。

662 開発者がすべてのインタフェースについて同じレベルの情報を提供している場合、評価者は、これまでの段落までで述べたのと同じ種別の分析を行う。評価者は、どのインタフェースが SFR 実施でどのインタフェースがそうでないかを決定し、その後、SFR 実施アクションについて SFR 実施の側面が適切に記述されていることを保証するべきである。この場合、評価者は、この SFR 実施の分析を行う過程で、ワークユニット ADV_FSP.3-8 に関連する作業の大半を行えるべきである。

663 SFR 実施アクションとは、主張されている SFR の実施を提供する、任意の外部インタフェースで見ることのできるアクションである。例えば、ST に監査の要件が含まれていた場合、監査関連のアクションは SFR 実施になるため、記述されていなければならない。これは、そのアクションの結果が、通常は呼び出されたインタフェースでは見ることができない場合でも変わらない(監査では、あるインタフェースでの利用者のアクションの結果として、別のインタフェースで見ることができる監査記録が生成されるため、このような場合が一般的である)。

664 記述には、SFR に関して TSFI アクションがどのような役割を果たすのかを読者が理解できるレベルが要求される。評価者は、そのインタフェースに対するテストケースを生成(及び評定)できるよう詳細に記述すべきであるということを忘れないようにするべきである。記述が不明確であったり詳細さに欠けていたりして、TSFI に対して意味のあるテストを実施できない場合、その記述は不適切であると考えられる。

ADV_FSP.3.5C ***各 SFR 実施 TSFI について、機能仕様は、その TSFI の呼び出しに関連する SFR 実施アクション及び例外によって発生する直接的誤りメッセージを記述しなければならない。***

ADV_FSP.3-7 評価者は、TSFI の提示が各 SFR 実施 TSFI の呼び出しによって発生する可能性がある誤りメッセージ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。***

665 このワークユニットは、SFR 実施 TSFI のセットが正しく識別されていることを保証するために、ワークユニット ADV_FSP.3-6 とともに(またはその後に)実行されるべきである。評価者は、この要件及び関連するワークユニットでは、SFR 実施 TSFI に関連するすべての直接的誤りメッセージ(これらはSFR実施アクションに関連する)が記述されている必要があるということに注意すべきである。これは、この保証レベルでは、インタフェースの SFR 実施の側面がすべて適切に記述されているかどうかを決定するときに、誤りメッセージの記述によって提供される「追加の」情報を使用するべきだからである。例えば、TSFI に関連する誤りメッセージ(例えば、「アクセスは拒否されました」)によって、SFR 実施の決定またはアクションが発生したことが示されているのに、SFR 実施アクションの記述には、その特定の SFR 実施メカニズムについての言及がない場合、その記述は完全ではない可能性がある。

666 誤りは、記述されているインタフェースによって様々な形をとる。API の場合、誤りコードを返す、グローバルな誤り状態を設定する、誤りコードで特定のパラメタを設定するなどの操作が、インタフェース自体によって行われる。設定ファイルの場合は、パラメタの設定に誤りがあると、ログファイルに誤りメッセージが書き込まれる。ハードウェア PCI カードの場合は、誤り状態によってバスで信号が発生したり、CPU に対する例外条件が発生したりする。

667 誤り(及び関連する誤りメッセージ)は、インタフェースの呼び出しを通じて発生する。インタフェースの呼び出しに応じて発生する処理で誤り状態が検出されると、誤りメッセージが(実装固有のメカニズムによって)生成される。これは、インタフェース自身から返される戻り値である場合もあれば、インタフェースの呼び出しの後にグローバルな値が設定されてチェックされる場合もある。一般に TOE には、「ディスクフル」や「資源のロック」など、資源の基本的な状態を原因とする下位レベルの誤りメッセージがいくつか用意されている。これらの誤りメッセージは、多数の TSFI にマッピングされている場合もあるが、インタフェース記述の詳細の漏れを見つけるために使用できる。例えば、「ディスクフル」メッセージを生成する TSFI があり、その TSFI のアクションの記述に、その TSFI でディスクへのアクセスが発生する理由についての明白な記述がない場合、評価者は、その記述が正確かどうかを決定するために、その TSFI に関連するその他の証拠(セキュリティアーキテクチャ(ADV_ARC)や TOE 設計(ADV_TDS))を検査する必要がある。

668 TSFI の誤りメッセージの記述が正確かつ完全であることを決定するには、評価者は、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス)や、その TSFI について提供されているその他の証拠(SFR 実施アクションの記述、SFR 支援及び SFR 非干渉アクションの要約、結果など)に照らしてインタフェース記述を評価する。

ADV_FSP.3.6C ***機能仕様は、各 TSFI に関連する SFR 支援及び SFR 非干渉アクションを要約しなければならない。***

ADV_FSP.3-8 評価者は、TSFI の提示が各 TSFI に関連する SFR 支援及び SFR 非干渉アクションを要約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。***

669 このワークユニットの目的は、SFR 実施アクションに関する詳細(ワークユニット ADV_FSP.3-6 で提供)を、残りのアクション(SFR 実施ではないアクション)の要約によって補足することである。ここでは、SFR 実施 TSFI を通じて呼び出されるものも、SFR 支援または SFR 非干渉 TSFI を通じて呼び出されるものも含め、すべての SFR 支援及び SFR 非干渉アクションがカバーされる。すべての SFR 支援及び SFR 非干渉アクションに関するこのような要約により、TSF によって提供される機能をより全体的に捉えられるようになる。評価者はこれを、アクションや TSFI の分類に誤りがないかどうかを決定するために使用するべきである。

670 ここで提供される情報は、SFR 実施アクションに対して要求される情報より抽象的である。読者がアクションの内容を理解できる程度に詳細であるべきだが、例えば、そのアクションに対するテストを記述できるほど詳細である必要はない。評価者にとって重要なのは、そのアクションが SFR 支援、あるいは SFR 非干渉であると明確に決定できるだけの情報が必要だということである。そのレベルの情報がない場合、その要約は不十分であり、もっと多くの情報を入手する必要がある。

ADV_FSP.3.7C ***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。***

ADV_FSP.3-9 評価者は、追跡によって SFR が対応する TSFI にリンクされることを***チェックしなければならない。***

671 追跡は、どの SFR がどの TSFI に関連するかを示す指針として、開発者が提供する。この追跡は表のように単純化できる。評価者は、続くワークユニットで追跡を入力として使用して、その完全さと正確さを検証する。

12.4.3.4 アクション ADV_FSP.3.2E

ADV_FSP.3-10 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。***

672 すべての SFR が機能仕様、及びテストカバレージ分析によってカバーされていることを保証するために、評価者は開発者の追跡を土台にすることができる(ADV_FSP.3-9の TOE セキュリティ機能要件と TSFI の間のマッピングを参照のこと。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、詳細レベルが要件のコンポーネントレベルより下、さらにはエレメントレベルより下でなければならない場合もあるので注意する必要がある)。

673 例えば、FDP_ACC.1コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1の割付に 10 の規則が含まれていたとして、その 10 の規則が 3 つの異なる TSFI によってカバーされていた場合、評価者がFDP_ACC.1を TSFI A、B、及び C にマッピングして、ワークユニットが完了したと主張するのは適切でない。この場合、評価者は、FDP_ACC.1 (規則 1)を TSFI A に、FDP_ACC.1 (規則 2)を TSFI B にという形でマッピングを行うべきである。また、インタフェースがラッパーインタフェースである場合も考えられるが(例えば、IOCTL)、その場合には、特定のインタフェースの特定のパラメタセットに固有のマッピングが必要となる。

674 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。また、TSFI に関連付けられているパラメタ、アクション、及び誤りメッセージは完全に特定されていなければならないため、評価者は、SFR のすべての側面がインタフェースレベルで実装されているように見えるかどうかを決定できるべきであるという点も重要である。

ADV_FSP.3-11 評価者は、機能仕様が SFR の正確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。***

675 TSF 境界で見ることのできる効果をもたらす ST の各機能要件について、要件によって記述されている必要な機能性が、その要件に関連付けられている TSFI の情報によって特定される。例えば、アクセス制御リストの要件が ST に含まれていて、その要件にマッピングされている唯一の TSFI で Unix スタイルの保護ビットの機能性が特定されていた場合、その機能仕様は、その要件に対しては正確ではない。

676 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。

12.4.4 サブアクティビティの評価(ADV_FSP.4)

12.4.4.1 目的

677 このサブアクティビティの目的は、TSFI が完全かつ正確に記述されているかどうか及びSTのセキュリティ機能要件がTSFIに実装されているように見えるかどうかを評価者が決定できるような形で、開発者がすべての TSFI を完全に記述しているかどうかを決定することである。

12.4.4.2 入力

678 ワークユニットで必要とされるこのサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計。

679 TOE の ST に含まれている場合に使用されるこのサブアクティビティ用の評価証拠は、次のとおりである:

a) セキュリティアーキテクチャ記述;

b) 実装表現;

c) TSF 内部構造の記述;

d) 利用者操作ガイダンス;

12.4.4.3 適用上の注釈

680 機能仕様は、TSF へのインタフェース(TSFI)を構造的に記述する。サブアクティビティの評価(ADV_TDS.1)との依存関係があるため、評価者はこのサブアクティビティの作業を始める前に TSF の識別を完了していることが期待される。TSF の構成要素に関する確かな知識がないと、TSFI の完全性を評定することはできない。

681 このファミリに含まれる様々なワークユニットを実行する際、評価者には、様々な要素(TSFI 自体やTSFIの個々のコンポーネント(パラメタ、アクション、誤りメッセージなど))の正確さ及び完全さの評定が求められる。この分析を行う際には、評価者は、評価のために提供されている証拠資料を使用することが期待される。これには、ST 及び TOE 設計のほか、利用者操作ガイダンス、セキュリティアーキテクチャ記述、実装表現などのその他の証拠資料も含まれる。証拠資料は、繰り返し方式で検査するべきである。例えば、評価者が TOE 設計で、ある特定の機能がどのように実装されるのかを読み取ることはできたが、その機能をインタフェースから呼び出す方法がわからなかったとする。この場合、評価者は、特定の TSFI の記述の完全さを疑うか、機能仕様からインタフェースが完全に抜け落ちていることを疑うことになる。この種の分析アクティビティを ETR に記述することは、ワークユニットが適切に実行された根拠を示すための主要な方法となる。

682 機能要件には、その機能性の全体または一部が、特定のメカニズムによってではなく、アーキテクチャによって示されるものもあるということを認識しておくべきである。この例には、残存情報保護(FDP_RIP)の要件を実装するメカニズムの実装がある。一般にこのようなメカニズムは、ふるまいが存在しないことを保証するために実装されるが、それをテストするのは困難であり、通常は分析によって検証される。このような機能要件が ST に含まれている場合、評価者は、インタフェースを持たないこの種の SFR が存在する可能性があり、それは機能仕様の欠陥とみなされるべきではないという認識を持つことが期待される。

12.4.4.4 アクション ADV_FSP.4.1E

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.4-1 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。***

683 TSFI の識別は、このサブアクティビティの他のすべてのアクティビティの必要条件となる。TSFI を識別するためには、TSF が識別されていなければならない(TOE 設計(ADV_TDS)ワークユニットの一部として行われる)。このアクティビティは、インタフェースの大きなグループ(ネットワークプロトコル、ハードウェアインタフェース、設定ファイル)に欠けているものがないことを保証するために上位レベルで行うことも、機能仕様の評価と並行して下位レベルで行うこともできる。

684 このワークユニットの評定を行うとき、評価者は、機能仕様にリストされているインタフェースの観点から TSF のすべての部分が扱われていることを決定する。TSF のすべての部分にそれぞれ対応するインタフェース記述があるべきである。対応するインタフェースがない部分がある場合は、それが受け入れられるかどうかを評価者が決定する。

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.4-2 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。***

685 TSFI の目的とは、インタフェースによって提供される機能性を要約する一般的なステートメントである。そこで意図されているのは、インタフェースに関連するアクション及び結果の完全なステートメントではなく、そのインタフェースが何のために使用されるものなのかを読者が大まかに理解できるようにするためのステートメントである。評価者は、目的が存在することだけでなく、そこに TSFI が正確に反映されていることも、アクションの記述や誤りメッセージなど、インタフェースに関するその他の情報を考慮に入れて決定するべきである。

ADV_FSP.4-3 評価者は、各 TSFI の使用方法が記述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。***

686 TSFI の使用方法とは、アクションを呼び出して TSFI に関連する結果を取得するためには、インタフェースをどのように操作するのかを要約したものである。評価者は、機能仕様の中のこの資料を読むことにより、各インタフェースの使用方法を決定できるべきである。これは必ずしも、各 TSFI にそれぞれ異なる使用方法が必要ということではない。例えば、カーネルコールを呼び出す一般的な方法を記述してから、その一般的なスタイルを使用する各インタフェースを識別することも可能である。インタフェースの種別が変わると、別の使用方法の仕様が必要になる。API、ネットワークプロトコルインタフェース、システム設定パラメタ、及びハードウェアバスインタフェースには、それぞれにまったく異なる使用方法がある。機能仕様を評価する評価者と同様に、機能仕様を作成する開発者も、このことを考慮に入れて作業するべきである。

687 証拠資料によって、信頼できない利用者はその機能性にアクセスできないとされている管理インタフェースについては、その機能にアクセスできないようにする方法が機能仕様に記述されていることを評価者が保証する。このアクセス不可能性は、開発者のテストスイートでテストされる必要があるという点に注意するべきである。

688 評価者は、使用方法の記述のセットが存在することだけでなく、それらが各 TSFI を正確にカバーしていることも決定するべきである。

ADV_FSP.4-4 評価者は、TSFI の完全性を決定するために、機能仕様を**検査しなければならない**。

689 評価者は、考えられるタイプのインタフェースを識別するために、設計証拠資料を使わなければならない。評価者は、開発者の文書には記載のない潜在的な TSFI を探すために、設計証拠資料とガイダンス文書を検索しなければならない。このようにして、開発者により定義された TSFI 一式が不完全であることが示される。評価者は、どのような追加 TSFI も存在しないことを最も下位レベルの設計まで、あるいは実装表現によりチェックし、開発者によって提示された TSFI が完全であるという主張を**検査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.4-5 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に識別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。***

690 評価者は、各 TSFI のすべてのパラメタが記述されていることを保証するために、機能仕様を検査する。パラメタとは、インタフェースに対する明示的な入力または出力であり、そのインタフェースのふるまいを制御する。例えば、API に渡される引数、特定のネットワークプロトコルのパケットの様々なフィールド、Windows レジストリの個々のキーの値、チップの一連のピンでやり取りされる信号などがパラメタである。

691 すべてのパラメタが TSFI に含まれていることを決定するには、評価者は、パラメタの効果の説明が記述に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(アクションや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、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、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。

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。***

692 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。

693 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。

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.4-7 評価者は、TSFI の提示がすべての TSFI に関連するすべてのアクション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。***

694 評価者は、すべてのアクションが記述されていることを保証するためにチェックする。インタフェースを通じて利用可能なアクションは、(TSF によってアクションがどのように提供されるのかを記述する TOE 設計とは対照的に)そのインタフェースが何を行うのかを記述する。

695 インタフェースのアクションは、インタフェースを通じて呼び出すことができる機能性を記述する。また、*標準アクション*と *SFR 関連アクション*とに分類できる。標準アクションとは、インタフェースが何を行うかの記述である。この記述に対して提供される情報の量は、インタフェースの複雑さによって決まる。SFR 関連アクションとは、任意の外部インタフェースで見ることができるアクションである(例えば、インタフェースの呼び出しによって(ST に監査の要件が含まれている場合に)発生する監査アクティビティについて、通常は呼び出されたインタフェースではアクションの結果を見ることができないが、記述するべきである)。インタフェースのパラメタによっては、インタフェースを通じて呼び出すことができるアクションが数多くある場合もある(例えば API では、最初のパラメタで「サブコマンド」を指定して、その後に、そのサブコマンドに固有のパラメタを指定する場合がある。一部の Unix システムの IOCTL API などはそうしたインタフェースの 1 つである)。

696 TSFI のアクションの記述が完全であることを決定するには、評価者は、アクションの説明が記述に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(パラメタの記述や誤りメッセージなど)をレビューするべきである。評価者は、機能仕様に含まれていないアクションの証拠が記述されていないかどうかを確認するために、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス、実装表現)も分析するべきである。

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の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.4-8 評価者は、TSFI の提示が各 TSFI の呼び出しによって発生するすべての誤りメッセージ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。***

697 誤りは、記述されているインタフェースによって様々な形をとる。API の場合、誤りコードを返す、グローバルな誤り状態を設定する、誤りコードで特定のパラメタを設定するなどの操作が、インタフェース自体によって行われる。設定ファイルの場合は、パラメタの設定に誤りがあると、ログファイルに誤りメッセージが書き込まれる。ハードウェア PCI カードの場合は、誤り状態によってバスで信号が発生したり、CPU に対する例外条件が発生したりする。

698 誤り(及び関連する誤りメッセージ)は、インタフェースの呼び出しを通じて発生する。インタフェースの呼び出しに応じて発生する処理で誤り状態が検出されると、誤りメッセージが(実装固有のメカニズムによって)生成される。これは、インタフェース自身から返される戻り値である場合もあれば、インタフェースの呼び出しの後にグローバルな値が設定されてチェックされる場合もある。一般に TOE には、「ディスクフル」や「資源のロック」など、資源の基本的な状態を原因とする下位レベルの誤りメッセージがいくつか用意されている。これらの誤りメッセージは、多数の TSFI にマッピングされている場合もあるが、インタフェース記述の詳細の漏れを見つけるために使用できる。例えば、「ディスクフル」メッセージを生成する TSFI があり、その TSFI のアクションの記述に、その TSFI でディスクへのアクセスが発生する理由についての明白な記述がない場合、評価者は、その記述が完全かつ正確かどうかを決定するために、その TSFI に関連するその他の証拠(セキュリティアーキテクチャ(ADV_ARC)や TOE 設計(ADV_TDS))を検査する必要がある。

699 評価者は、各 TSFI について、そのインタフェースが呼び出されたときに返すことができる誤りメッセージの正確なセットを決定できることを決定する。評価者は、誤りのセットが完全であるように見えるかどうかを決定するために、インタフェースに提供されている証拠をレビューする。さらにこの情報を、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス、実装表現)に照らしてチェックして、言及されている処理によって発生する誤りの中に、機能仕様に含まれていないものがないことを保証する。

ADV_FSP.4-9 評価者は、TSFI の提示が各 TSFI の呼び出しによって発生するすべての誤りメッセージの意味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。***

700 正確かどうかを決定するには、評価者は誤りの意味を理解できなければならない。例えば、インタフェースで 0、1、または 2 の数字コードが返される場合、「*foo()*インタフェースの呼び出しによって発生する可能性がある誤りは 0、1、または 2 である」のように値が羅列されているだけの機能仕様では、評価者がその誤りを理解することはできないだろう。代わりに評価者は、誤りが「*foo()*インタフェースの呼び出しによって発生する可能性がある誤りは 0(成功)、1(ファイルが見つからない)、または 2(指定したファイル名が間違っている)である」のような形で記述されていることを保証するためにチェックする。

701 TSFI の呼び出しによって発生する誤りの記述が完全であることを決定するには、評価者は、そのようなインタフェースを使用することによって発生する可能性がある誤り状態が説明さ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(パラメタの記述やアクションなど)を検査する。評価者は、TSFI に関連する誤り処理について、機能仕様に含まれていないものが記述されていないかどうかを確認するために、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス、実装表現)もチェックする。

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。***

ADV_FSP.4-10 評価者は、追跡によって SFR が対応する TSFI にリンクされることを***チェックしなければならない。***

702 追跡は、どの SFR がどの TSFI に関連するかを示す指針として、開発者が提供する。この追跡は表のように単純化できる。評価者は、続くワークユニットで追跡を入力として使用して、その完全さと正確さを検証する。

12.4.4.5 **アクション** ADV_FSP.4.2E

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。***

703 すべての SFR が機能仕様、及びテストカバレージ分析によってカバーされていることを保証するために、評価者は開発者の追跡を土台にすることができる(ADV_FSP.4-10 の TOE セキュリティ機能要件と TSFI の間のマッピングを参照のこと。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、詳細レベルが要件のコンポーネントレベルより下、さらにはエレメントレベルより下でなければならない場合もあるので注意する必要がある)。

704 例えば、FDP_ACC.1コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1の割付に 10 の規則が含まれていたとして、その 10 の規則が 3 つの異なる TSFI によってカバーされていた場合、評価者がFDP_ACC.1を TSFI A、B、及び C にマッピングして、ワークユニットが完了したと主張するのは適切でない。この場合、評価者は、FDP_ACC.1 (規則 1)を TSFI A に、FDP_ACC.1 (規則 2)を TSFI B にという形でマッピングを行うべきである。また、インタフェースがラッパーインタフェースである場合も考えられるが(例えば、IOCTL)、その場合には、特定のインタフェースの特定のパラメタセットに固有のマッピングが必要となる。

705 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。また、TSFI に関連付けられているパラメタ、アクション、及び誤りメッセージは完全に特定されていなければならないため、評価者は、SFR のすべての側面がインタフェースレベルで実装されているように見えるかどうかを決定できるべきであるという点も重要である。

ADV_FSP.4-12 評価者は、機能仕様が SFR の正確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。***

706 TSF 境界で見ることのできる効果をもたらす ST の各機能要件について、要件によって記述されている必要な機能性が、その要件に関連付けられている TSFI の情報によって特定される。例えば、アクセス制御リストの要件が ST に含まれていて、その要件にマッピングされている唯一の TSFI で Unix スタイルの保護ビットの機能性が特定されていた場合、その機能仕様は、その要件に対しては正確ではない。

707 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。

12.4.5 サブアクティビティの評価(ADV_FSP.5)

12.4.5.1 目的

708 このサブアクティビティの目的は、TSFI が完全かつ正確に記述されているかどうか及び ST のセキュリティ機能要件が TSFI に実装されているように見えるかどうかを評価者が決定できるような形で、開発者がすべての TSFI を完全に記述しているかどうかを決定することである。インタフェースの完全さは、実装表現に基づいて判断される。

12.4.5.2 入力

709 ワークユニットで必要とされるこのサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計;

d) 実装表現。

710 TOE の ST に含まれている場合に使用されるこのサブアクティビティ用の評価証拠は、次のとおりである:

a) セキュリティアーキテクチャ記述;

b) TSF 内部構造の記述;

c) 形式的セキュリティ方針モデル;

d) 利用者操作ガイダンス;

12.4.5.3 アクション ADV_FSP.5.1E

ADV_FSP.5.1C ***機能仕様は、完全に TSF を表現しなければならない。***

ADV_FSP.5-1 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。***

711 TSFI の識別は、このサブアクティビティの他のすべてのアクティビティの必要条件となる。TSFI を識別するためには、TSF が識別されていなければならない(TOE 設計(ADV_TDS)ワークユニットの一部として行われる)。このアクティビティは、インタフェースの大きなグループ(ネットワークプロトコル、ハードウェアインタフェース、設定ファイル)に欠けているものがないことを保証するために上位レベルで行うことも、機能仕様の評価と並行して下位レベルで行うこともできる。

712 このワークユニットの評定を行うとき、評価者は、機能仕様にリストされているインタフェースの観点から TSF のすべての部分が扱われていることを決定する。TSF のすべての部分にそれぞれ対応するインタフェース記述があるべきである。対応するインタフェースがない部分がある場合は、それが受け入れられるかどうかを評価者が決定する。

ADV_FSP.5.2C ***機能仕様は、準形式的スタイルを使用して TSFI を記述しなければならない。***

ADV_FSP.5-2 評価者は、機能仕様が準形式的スタイルを使用して表現され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。***

713 準形式的表現は、明確に定義された構文を持つ標準化された形式を特徴とする。これにより、非形式的表現に見られるような曖昧さが軽減される。準形式的な形式の意図は、表現に対する読者の理解を高めることにあるため、何らかの構造的表現方法(擬似コード、フローチャート、ブロック図など)を使用することが適切である(必須ではない)。

714 評価者はこのアクティビティのために、インタフェース記述が構造的な一貫した形で記述されていること、及び共通の用語が使用されていることを保証するべきである。また、インタフェースの準形式的表現では、インタフェースの表現の詳細レベルが TSFI 全体でほぼ一貫していることも必要とされる。機能仕様では、インタフェースの一部について外部の仕様を参照することが認められるが、その場合も、それらの外部の仕様自体が準形式的でなければならない。

ADV_FSP.5.3C ***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.5-3 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。***

715 TSFI の目的とは、インタフェースによって提供される機能性を要約する一般的なステートメントである。そこで意図されているのは、インタフェースに関連するアクション及び結果の完全なステートメントではなく、そのインタフェースが何のために使用されるものなのかを読者が大まかに理解できるようにするためのステートメントである。評価者は、目的が存在することだけでなく、そこに TSFI が正確に反映されていることも、アクションの記述や誤りメッセージなど、インタフェースに関するその他の情報を考慮に入れて決定するべきである。

ADV_FSP.5-4 評価者は、各 TSFI の使用方法が記述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。***

716 TSFI の使用方法とは、アクションを呼び出して TSFI に関連する結果を取得するためには、インタフェースをどのように操作するのかを要約したものである。評価者は、機能仕様の中のこの資料を読むことにより、各インタフェースの使用方法を決定できるべきである。これは必ずしも、各 TSFI にそれぞれ異なる使用方法が必要ということではない。例えば、カーネルコールを呼び出す一般的な方法を記述してから、その一般的なスタイルを使用する各インタフェースを識別することも可能である。インタフェースの種別が変わると、別の使用方法の仕様が必要になる。API、ネットワークプロトコルインタフェース、システム設定パラメタ、及びハードウェアバスインタフェースには、それぞれにまったく異なる使用方法がある。機能仕様を評価する評価者と同様に、機能仕様を作成する開発者も、このことを考慮に入れて作業するべきである。

717 証拠資料によって、信頼できない利用者はその機能性にアクセスできないとされている管理インタフェースについては、その機能にアクセスできないようにする方法が機能仕様に記述されていることを評価者が保証する。このアクセス不可能性は、開発者のテストスイートでテストされる必要があるという点に注意するべきである。

718 評価者は、使用方法の記述のセットが存在することだけでなく、それらが各 TSFI を正確にカバーしていることも決定するべきである。

ADV_FSP.5-5 評価者は、TSFI の完全性を決定するために、機能仕様を***検査しなければならない。***

719 評価者は、考えられるタイプのインタフェースを識別するために、設計証拠資料を使わなければならない。評価者は、開発者の文書には記載のない潜在的な TSFI(これは、開発者により定義された TSFI 一式が不完全であることを表す)を探すために、設計証拠資料とガイダンス文書を検索しなければならない。評価者は、どのような追加 TSFI も存在しないことを最も下位レベルの設計まで、あるいは実装表現によりチェックし、開発者によって提示された TSFI が完全であるという主張を***検査しなければならない。***

ADV_FSP.5.4C ***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.5-6 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に識別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。***

720 評価者は、各 TSFI のすべてのパラメタが記述されていることを保証するために、機能仕様を検査する。パラメタとは、インタフェースに対する明示的な入力または出力であり、そのインタフェースのふるまいを制御する。例えば、API に渡される引数、特定のネットワークプロトコルのパケットの様々なフィールド、Windows レジストリの個々のキーの値、チップの一連のピンでやり取りされる信号などがパラメタである。

721 すべてのパラメタが TSFI に含まれていることを決定するには、評価者は、パラメタの効果の説明が記述に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(アクションや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、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、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。

ADV_FSP.5-7 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。***

722 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。

723 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。

ADV_FSP.5.5C **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.5-8 評価者は、TSFI の提示がすべての TSFI に関連するすべてのアクション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。***

724 評価者は、すべてのアクションが記述されていることを保証するためにチェックする。インタフェースを通じて利用可能なアクションは、(TSF によってアクションがどのように提供されるのかを記述する TOE 設計とは対照的に)そのインタフェースが何を行うのかを記述する。

725 インタフェースのアクションは、インタフェースを通じて呼び出すことができる機能性を記述する。また、*標準アクション*と *SFR 関連アクション*とに分類できる。標準アクションとは、インタフェースが何を行うかの記述である。この記述に対して提供される情報の量は、インタフェースの複雑さによって決まる。SFR 関連アクションとは、任意の外部インタフェースで見ることができるアクションである(例えば、インタフェースの呼び出しによって(ST に監査の要件が含まれている場合に)発生する監査アクティビティについて、通常は呼び出されたインタフェースではアクションの結果を見ることができないが、記述するべきである)。インタフェースのパラメタによっては、インタフェースを通じて呼び出すことができるアクションが数多くある場合もある(例えば API では、最初のパラメタで「サブコマンド」を指定して、その後に、そのサブコマンドに固有のパラメタを指定する場合がある。一部の Unix システムの IOCTL API などはそうしたインタフェースの 1 つである)。

726 TSFI のアクションの記述が完全であることを決定するには、評価者は、アクションの説明が記述に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(パラメタの記述や誤りメッセージなど)をレビューするべきである。評価者は、機能仕様に含まれていないアクションの証拠が記述されていないかどうかを確認するために、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス、実装表現)も分析するべきである。

ADV_FSP.5.6C ***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.5-9 評価者は、TSFI の提示が各 TSFI の呼び出しによって発生するすべての誤りメッセージ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。***

727 誤りは、記述されているインタフェースによって様々な形をとる。API の場合、誤りコードを返す、グローバルな誤り状態を設定する、誤りコードで特定のパラメタを設定するなどの操作が、インタフェース自体によって行われる。設定ファイルの場合は、パラメタの設定に誤りがあると、ログファイルに誤りメッセージが書き込まれる。ハードウェア PCI カードの場合は、誤り状態によってバスで信号が発生したり、CPU に対する例外条件が発生したりする。

728 誤り(及び関連する誤りメッセージ)は、インタフェースの呼び出しを通じて発生する。インタフェースの呼び出しに応じて発生する処理で誤り状態が検出されると、誤りメッセージが(実装固有のメカニズムによって)生成される。これは、インタフェース自身から返される戻り値である場合もあれば、インタフェースの呼び出しの後にグローバルな値が設定されてチェックされる場合もある。一般に TOE には、「ディスクフル」や「資源のロック」など、資源の基本的な状態を原因とする下位レベルの誤りメッセージがいくつか用意されている。これらの誤りメッセージは、多数の TSFI にマッピングされている場合もあるが、インタフェース記述の詳細の漏れを見つけるために使用できる。例えば、「ディスクフル」メッセージを生成する TSFI があり、その TSFI のアクションの記述に、その TSFI でディスクへのアクセスが発生する理由についての明白な記述がない場合、評価者は、その記述が完全かつ正確かどうかを決定するために、その TSFI に関連するその他の証拠(ADV_ARC や ADV_TDS)を検査する必要がある。

729 評価者は、各 TSFI について、そのインタフェースが呼び出されたときに返すことができる誤りメッセージの正確なセットを決定できることを決定する。評価者は、誤りのセットが完全であるように見えるかどうかを決定するために、インタフェースに提供されている証拠をレビューする。さらにこの情報を、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス、実装表現)に照らしてチェックして、言及されている処理によって発生する誤りの中に、機能仕様に含まれていないものがないことを保証する。

ADV_FSP.5-10 評価者は、TSFI の提示が各 TSFI の呼び出しによって発生するすべての誤りメッセージの意味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。***

730 正確かどうかを決定するには、評価者は誤りの意味を理解できなければならない。例えば、インタフェースで 0、1、または 2 の数字コードが返される場合、「*foo()*インタフェースの呼び出しによって発生する可能性がある誤りは 0、1、または 2 である」のように値が羅列されているだけの機能仕様では、評価者がその誤りを理解することはできないだろう。代わりに評価者は、誤りが「*foo()*インタフェースの呼び出しによって発生する可能性がある誤りは 0(成功)、1(ファイルが見つからない)、または 2(指定したファイル名が間違っている)である」のような形で記述されていることを保証するためにチェックする。

731 TSFI の呼び出しによって発生する誤りの記述が完全であることを決定するには、評価者は、そのようなインタフェースを使用することによって発生する可能性がある誤り状態が説明さ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(パラメタの記述やアクションなど)を検査する。評価者は、TSFI に関連する誤り処理について、機能仕様に含まれていないものが記述されていないかどうかを確認するために、評価のために提供されているその他の証拠(例えば、TOE 設計、セキュリティアーキテクチャ記述、利用者操作ガイダンス、実装表現)もチェックする。

ADV_FSP.5.7C ***機能仕様は、TSFI の呼び出しによって発生しないすべての誤りメッセージを記述しなければならない。***

ADV_FSP.5-11 評価者は、機能仕様が TSFI の呼び出しによって発生しないすべての誤りメッセージを完全かつ正確に記述していることを決定するために、その仕様を***検査しなければならない。***

732 このワークユニットは、TSFI の呼び出しによって発生する誤りメッセージについて記述したワークユニット ADV_FSP.5-9 を補足するものである。この 2 つのワークユニットの組み合わせにより、TSF によって生成される可能性があるすべての誤りメッセージがカバーされる。

733 評価者は、機能仕様の内容を、実装表現に含まれる誤りメッセージの生成の事例と比較することによって、機能仕様の完全さ及び正確さを評定する。こうした誤りメッセージのほとんどは、すでにワークユニット ADV_FSP.5-9 によってカバーされているものである。

734 一般に、このワークユニットに関連する誤りメッセージは、生成されるとは想定されていないが、正しいプログラミングの実践のために作成されるものである。例えば、一連の case のそれぞれの結果となるアクションを定義する case ステートメントは、想定されていないすべての状況に適用される最後の *else* ステートメントで終了することができる。これにより、TSF が未定義の状態に陥らないことが保証される。しかし、実行パスがこの *else* ステートメントに到達することは想定されていないため、この *else* ステートメントの中で誤りメッセージが生成されることはない。この誤りメッセージは、生成されることはなくても、機能仕様には含まれていなければならない。

ADV_FSP.5.8C ***機能仕様は、TSF の実装に含まれているが TSFI の呼び出しによって発生しない各誤りメッセージについて、その根拠を示さなければならない。***

ADV_FSP.5-12 評価者は、機能仕様が、TSF の実装に含まれているが TSFI の呼び出しによって発生しない各誤りメッセージについて、その根拠を示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。***

735 評価者は、ワークユニット ADV_FSP.5-11 で確認されたすべての誤りメッセージについて、それらが TSFI から呼び出されない理由となる根拠が含まれていることを保証する。

736 この根拠では、前のワークユニットで説明したように、問題の誤りメッセージは実行ロジックを完全にするために提供されるものであり、生成されることは想定されていない、という事実を示すだけでかまわない。評価者は、そうした誤りメッセージのそれぞれについて、その根拠が論理的であることを保証する。

ADV_FSP.5.9C ***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。***

ADV_FSP.5-13 評価者は、追跡によって SFR が対応する TSFI にリンクされることを***チェックしなければならない。***

737 追跡は、どの SFR がどの TSFI に関連するかを示す指針として、開発者が提供する。この追跡は表のように単純化できる。評価者は、続くワークユニットで追跡を入力として使用して、その完全さと正確さを検証する。

12.4.5.4 アクション ADV_FSP.5.2E

ADV_FSP.5-14 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。***

738 すべての SFR が機能仕様、及びテストカバレージ分析によってカバーされていることを保証するために、評価者は開発者の追跡を土台にすることができる(ADV_FSP.5-13 の TOE セキュリティ機能要件と TSFI の間のマッピングを参照のこと。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、詳細レベルが要件のコンポーネントレベルより下、さらにはエレメントレベルより下でなければならない場合もあるので注意する必要がある)。

739 例えば、FDP_ACC.1コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1の割付に 10 の規則が含まれていたとして、その 10 の規則が 3 つの異なる TSFI によってカバーされていた場合、評価者がFDP_ACC.1を TSFI A、B、及び C にマッピングして、ワークユニットが完了したと主張するのは適切でない。この場合、評価者は、FDP_ACC.1 (規則 1)を TSFI A に、FDP_ACC.1 (規則 2)を TSFI B にという形でマッピングを行うべきである。また、インタフェースがラッパーインタフェースである場合も考えられるが(例えば、IOCTL)、その場合には、特定のインタフェースの特定のパラメタセットに固有のマッピングが必要となる。

740 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。また、TSFI に関連付けられているパラメタ、アクション、及び誤りメッセージは完全に特定されていなければならないため、評価者は、SFR のすべての側面がインタフェースレベルで実装されているように見えるかどうかを決定できるべきであるという点も重要である。

ADV_FSP.5-15 評価者は、機能仕様が SFR の正確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。***

741 TSF 境界で見ることのできる効果をもたらす ST の各機能要件について、要件によって記述されている必要な機能性が、その要件に関連付けられている TSFI の情報によって特定される。例えば、アクセス制御リストの要件が ST に含まれていて、その要件にマッピングされている唯一の TSFI で Unix スタイルの保護ビットの機能性が特定されていた場合、その機能仕様は、その要件に対しては正確ではない。

742 評価者は、TSF 境界ではほとんどあるいはまったく見ることのできない要件(例えば、FDP_RIP)については、TSFI への完全なマッピングは期待されないということを認識する必要がある。それらの要件の分析は、ST に含まれている場合に、TOE 設計(ADV_TDS)の分析で行われる。

12.4.6 サブアクティビティの評価(ADV_FSP.6)

743 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

12.5 実装表現(ADV_IMP)

12.5.1 サブアクティビティの評価(ADV_IMP.1)

12.5.1.1 目的

744 このサブアクティビティの目的は、開発者によって提供される実装表現が、他の分析アクティビティで使用するのに適しているかどうかを決定することである。この*適切さ*は、このコンポーネントの要件に対する適合性によって判断される。

12.5.1.2 入力

745 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 実装表現;

b) 開発ツールの証拠資料(ALC_TATの結果);

c) TOE 設計記述。

12.5.1.3 適用上の注釈

746 情報不足によって分析アクティビティが制限されることのないように、実装表現全体が提供される。とはいえ、分析アクティビティが行われる際にすべての表現が検査されるわけではない。そのようなことは、ほとんどすべての場合に現実的でないうえ、たいていは、実装表現のターゲットサンプリングに比べて TOE の保証が高くなるわけでもない。このサブアクティビティについては特にそう言える。長い時間をかけて実装表現の特定の部分の要件を検証し、その後、別の部分を使用して他のワークユニットの分析を行うというのは、評価者にとって生産的とは言えない。したがって、評価者には、他のファミリ(ATE_IND、AVA_VAN、ADV_INTなど)のワークユニットで行われる分析に最も関係のある TOE の部分から実装表現のサンプルを選択することが推奨される。

12.5.1.4 アクション ADV_IMP.1.1E

ADV_IMP.1.1C ***実装表現は、それ以上の設計上の決定を必要とせずに、TSF を生成できるような詳細レベルまで TSF を定義しなければならない。***

ADV_IMP.1-1 評価者は、実装表現が、それ以上の設計上の決定を必要とせずに、TSF を生成できるような詳細レベルまで TSF を定義していることを***チェックしなければならない。***

747 ソースコードや、実際のハードウェアの製造に用いられるハードウェア図及び/または IC ハードウェア設計言語コードやレイアウトデータは、実装表現の一部の例である。評価者は、実装表現が適切なレベル(さらなる設計上の決定を必要とする擬似コードなどのレベルではなく)に達しているという確信を得るために、実装表現をサンプリングする。評価者には、開発者の方向性が正しいことを確認するために、最初に実装表現を簡単にチェックすることが推奨される。その一方で、実装の検査を必要とする他のワークユニットの作業の間にも、このチェックの大半を行うことが推奨される。そうすることによって、このワークユニットで検査したサンプルが適切であるという保証が得られる。

ADV_IMP.1.2C ***実装表現の形式は、開発要員が使用する形式でなければならない。***

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。***

748 実装表現は、開発者によって、実際の実装への変換に適した形式で操作される。例えば開発者は、最終的にコンパイルされて TSF の一部となるソースコードを含むファイルを使用することができる。開発者は、評価者が分析において自動化の技法を使用できるように、自分たちが使用する形式で実装表現を提供する。これにより、検査される実装表現が、実際に TSF の作成に使用されるものであるという信頼も高まる(ワードプロセッサ文書などの別の表現形式で提供される場合とは対照的)。ただし、開発者は他の形式の実装表現も使用できるという点に注意するべきである。それらの形式の実装表現も一緒に提供される。全体的な目標は、評価者の分析を最大限に高める情報を提供することである。

749 評価者は、開発者が使用できるバージョンであるという確信を得るために、実装表現をサンプリングする。このサンプルによって、実装表現のすべての部分が要件に適合しているという保証が得られるようにする。ただし、実装表現全体の完全な検査は必要ない。

750 ある種の実装表現には、コンパイルや実行時の解釈の実際の結果を、実装表現のみから決定するのを困難にしたり不可能にしたりするような規則がある。例えば C 言語コンパイラでは、コンパイラディレクティブによって、コードの特定の部分全体が除外されたり含まれたりする。

751 ある種の実装表現では、理解や分析に対する重大な障害が持ち込まれるために、追加の情報が必要になることがある。例えば、隠蔽されているソースコードや、理解や分析を妨げるその他の形で分かりにくくされているコードがこれに該当する。一般に、このような形式の実装表現は、TOE 開発者によって使用されているバージョンの実装表現に対して、コードを隠蔽したり分かりにくくしたりするプログラムが実行された結果である。隠蔽されている表現はコンパイルの対象であり、元の隠蔽されていない表現より(構造の観点からは)実装に近いと言えるが、そのように分かりにくくされているコードを提供すると、その表現に関連する分析作業にかかる時間が大幅に増加する可能性がある。このような形式の表現が作成される場合は、隠蔽されていない表現を提供できるように、使用されている隠蔽ツール/アルゴリズムについての詳細がコンポーネントで必要とされる。この追加の情報は、隠蔽のプロセスによって弱体化しているセキュリティメカニズムがないという確信を得るために使用できる。

752 評価者は、実装表現の解釈に必要なすべての情報が提供されているという確信を得るために、実装表現をサンプリングする。ツールは、ツールと技法(ALC_TAT)コンポーネントによって参照されているものである点に注意する必要がある。評価者には、開発者の方向性が正しいことを確認するために、最初に実装表現を簡単にチェックすることが推奨される。その一方で、実装の検査を必要とする他のワークユニットの作業の間にも、このチェックの大半を行うことが推奨される。そうすることによって、このワークユニットで検査したサンプルが適切であるという保証が得られる。

ADV_IMP.1.3C ***TOE 設計記述と実装表現のサンプルの間のマッピングは、両者の対応を実証しなければならない。***

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。***

753 評価者は、実装表現の一部とTOE設計記述が正しいことを検証することによって、存在の決定(ワークユニット ADV_IMP.1-1 で特定される)を補強する。関心の対象となる TOE 設計記述の部分について、TOE 設計記述で提供されている記述が実装表現に正確に反映されていることを検証する。

754 例えば、利用者の識別及び認証に使用されるログインモジュールが TOE 設計記述で識別されていたとする。この場合、評価者は、利用者認証が重要視されるなら、TOE 設計記述に記述されているサービスが、対応するコードで実際に実装されていることを検証する。このほか、機能仕様に記述されているパラメタをコードが受け取っているかどうかも、検証する価値がある場合がある。

755 もう 1 つ注意すべきポイントとして、開発者は、選択されるサンプルが確実にカバーされるように実装表現全体のマッピングを行うか、サンプルが選択されてからマッピングを行うかを選択しなければならない。1 つ目の方法では、作業量は増えるが、評価が始まる前に完了できる。2 つ目の方法では、作業量は減るが、必要な証拠が作成されるまで評価アクティビティが中断されることになる。

12.5.2 サブアクティビティの評価(ADV_IMP.2)

756 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

12.6 TSF 内部構造(ADV_INT)

12.6.1 サブアクティビティの評価(ADV_INT.1)

12.6.1.1 目的

757 このサブアクティビティの目的は、定義された TSF のサブセットが、欠陥の可能性を低減し、欠陥をもたらすことなくより簡単に保守を実行できるように設計及び構成されているかどうかを決定することである。

12.6.1.2 入力

758 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) TOE 設計記述;

c) 実装表現(ADV_IMPが主張されている保証の一部である場合);

d) TSF 内部記述と正当化;

e) コーディング標準の証拠資料(ALC_TATの結果)。

12.6.1.3 適用上の注釈

759 内部構造の記述の役割は、TSF の設計及び実装の構造の証拠を提供することである。

760 設計の構造には、TSF の構成部分、及び TSF の設計に使用される手続きという 2 つの側面がある。TSF が TOE 設計(ADV_TDSを参照のこと)で表現された設計と一致する方法で設計されている場合、TSF 設計の評定は明白である。設計手続き(ALC_TATを参照のこと)に従っている場合、TSF 設計手続きの評定も同様に明白である。

761 TSF が手続きベースのソフトウェアを用いて実装されている場合、この構造はその *モジュール性*に基づいて評定される。つまり、内部構造の記述で識別されるモジュールは、TOE 設計(TOE 設計(ADV_TDS))で識別されるモジュールと同じである。モジュールは 1 つまたは複数のソースコードファイルで構成される。これらのソースコードファイルはコンパイル可能な最小単位であり、それ以上分解することはできない。

762 このコンポーネントでの割付の使用により、割付ADV_INT.1.1Dで明示的に識別される TSF のサブセットにおいて、残りの TSF よりも厳しい制約が課せられる。TSF 全体は、適切なエンジニアリングの原則を使用して設計され、適切に構成された TSF となるべきであるが、この特性について具体的に分析されるのは、特定されたサブセットのみである。評価者は、開発者がコーディング標準を使用することで理解可能な TSF が作成されることを決定する。

763 このコンポーネントの主要目的は、TSF のサブセットの実装表現が(開発者と評価者の両方の)保守及び分析に役立つ理解可能なものになっていることを保証することである。

12.6.1.4 アクション ADV_INT.1.1E

ADV_INT.1.1C ***正当化は、「適切に構成された」の意味を判断するために使用される特性を説明しなければならない。***

ADV_INT.1-1 評価者は、TSF が適切に構成されているかどうかを決定するための基準が正当化で識別されていることを決定するために、正当化を***検査しなければならない。***

764 評価者は、適切に構成されているという特性を決定するための基準が、正当化で明確に定義されていることを検証する。一般に、容認される基準は、技術的分野の業界標準から作成される。例えば、直線的に実行される手続き型ソフトウェアは、IEEE 標準(*IEEE 標準 610.12-1990*)に定義されているようなソフトウェアエンジニアリングのプログラミング手法を遵守していれば、一般には適切に構成されているとみなされる。例えば、TSF のサブセットにおける手続き型ソフトウェアの部分に対する基準として、次のものが識別される:

a) モジュール分解に使用されるプロセス

b) 実装の開発に使用されるコーディング標準

c) TSF のサブセットによって示される最大許容レベルのモジュール間結合の記述

d) TSF のサブセットのモジュールによって示される最小許容レベルの凝集度の記述

765 TOE で使用されるその他の種別の技術(例えば、非手続き型ソフトウェア(オブジェクト指向プログラミングなど)、広く普及している汎用ハードウェア(PC マイクロプロセッサなど)、特殊目的のハードウェア(スマートカードプロセッサなど))については、「適切に構成」されていることの基準の適切性を決定するために、評価者は評価監督機関のガイダンスを求めるべきである。

ADV_INT.1.2C ***TSF 内部構造の記述は、割り付けられた TSF のサブセットが適切に構成されていることを実証しなければならない。***

ADV_INT.1-2 評価者は、TSF 内部構造の記述で割り付けられた TSF のサブセットが識別されていることを決定するために、この記述を***チェックしなければならない。***

766 このサブセットは、抽象化のいずれかの層で TSF の内部構造という観点から識別される場合がある。例えば、TOE 設計で識別されるように、TSF の構造エレメントの観点から識別できる場合(監査サブシステムなど)や、実装の観点から識別できる場合(*encrypt.c* 及び *decrypt.c* ファイルや、6227 IC チップなど)がある。

767 このサブセットを、主張されている SFR(例えば FPR_ANO.2 で定義されている匿名性を提供する TSF の一部分)の観点から識別することは、分析の焦点が定まらないため、不十分である。

ADV_INT.1-3 評価者は、割り付けられた TSF のサブセットが適切に構成されていることを TSF 内部構造の記述が実証していることを決定するために、この記述を***チェックしなければならない。***

768 評価者は、TSF のサブセットがADV_INT.1-1の基準をどのように満たしているかを内部構造の記述が適切に説明していることを保証するために、その記述を検査する。

769 例えば、TSF のサブセットにおける手続き型ソフトウェアの部分がどのように以下の基準を満たすかを説明する:

a) TSF のサブセットで識別されるモジュールと TOE 設計(ADV_TDS)で記述されているモジュールが 1 対 1 で対応していること

b) モジュール分解プロセスが TSF 設計にどのように反映されているか

c) コーディング標準が使用されていないまたは満たされていないすべての場合に対する正当化

d) 許容範囲外の結合または凝集度に対する正当化

12.6.1.5 アクション ADV_INT.1.2E

ADV_INT.1-4 評価者は、割り付けられたTSFのサブセットのTOE設計が適切に構成されていることを***実証しなければならない。***

770 評価者は、正当化の正確さを検証するために、TOE 設計のサンプルを検査する。例えば、TOE 設計のサンプルを分析して、設計標準に準拠していることなどを決定する。サブセットに対してアクティビティを行うすべての領域と同様に、評価者はサンプルのサイズと範囲の正当化を提供する。

771 サブシステム及びモジュールへの TOE の分解の記述は、TSF のサブセットが適切に構成されていることが自明であることを立論する。TSF を構成する手続き(ALC_TATで検査)に従っていることを検証することで、TSF のサブセットが適切に構成されていることが自明となる。

ADV_INT.1-5 評価者は、割り付けられた TSF のサブセットが適切に構成されていることを***決定しなければならない。***

772 ADV_IMPが主張されている保証の一部でない場合、このワークユニットは該当しないため、満たされているものとみなされる。

773 評価者は、内部構造の記述の正確さを検証するために、TSF のサブセットのサンプルを検査する。例えば、TSF のサブセットにおける手続き型ソフトウェアの部分のサンプルを分析して、その凝集度と結合、コーディング標準への準拠などを決定する。サブセットに対してアクティビティを行うすべての領域と同様に、評価者はサンプルのサイズと範囲の正当化を提供する。

12.6.2 サブアクティビティの評価(ADV_INT.2)

12.6.2.1 目的

774 このサブアクティビティの目的は、TSF が欠陥の可能性を低減し、欠陥をもたらすことなくより簡単に保守を実行できるように設計及び構成されているかどうかを決定することである。

12.6.2.2 入力

775 このサブアクティビティ用の評価証拠は、次のとおりである:

a) モジュール設計の記述;

b) 実装表現(ADV_IMPが主張されている保証の一部である場合);

c) TSF 内部構造の記述;

d) コーディング標準の証拠資料(ALC_TATの結果)。

12.6.2.3 適用上の注釈

776 内部構造の記述の役割は、TSF の設計及び実装の構造の証拠を提供することである。

777 設計の構造には、TSF の構成部分、及び TSF の設計に使用される手続きという 2 つの側面がある。TSF が TOE 設計(ADV_TDSを参照のこと)で表現された設計と一致する方法で設計されている場合、TSF 設計の評定は明白である。設計手続き(ALC_TATを参照のこと)に従っている場合、TSF 設計手続きの評定も同様に明白である。

778 TSF が手続きベースのソフトウェアを用いて実装されている場合、この構造はその *モジュール性*に基づいて評定される。つまり、内部構造の記述で識別されるモジュールは、TOE 設計(TOE 設計(ADV_TDS))で識別されるモジュールと同じである。モジュールは 1 つまたは複数のソースコードファイルで構成される。これらのソースコードファイルはコンパイル可能な最小単位であり、それ以上分解することはできない。

779 このコンポーネントの主要目的は、TSF の実装表現が(開発者と評価者の両方の)保守及び分析に役立つ理解可能なものになっていることを保証することである。

12.6.2.4 アクション ADV_INT.2.1E

ADV_INT.2.1C ***正当化は、「適切に構成された」の意味を判断するために使用される特性を記述しなければならない。***

ADV_INT.2-1 評価者は、TSF が適切に構成されているかどうかを決定するための基準が正当化で識別されていることを決定するために、正当化を***検査しなければならない。***

780 評価者は、適切に構成されているという特性を決定するための基準が、正当化で明確に定義されていることを検証する。一般に、容認される基準は、技術的分野の業界標準から作成される。例えば、直線的に実行される手続き型ソフトウェアは、IEEE 標準(*IEEE 標準 610.12-1990*)に定義されているようなソフトウェアエンジニアリングのプログラミング手法を遵守していれば、一般には適切に構成されているとみなされる。例えば、TSF の手続き型ソフトウェアの部分に対する基準として、次のものが識別される:

a) モジュール分解に使用されるプロセス

b) 実装の開発に使用されるコーディング標準

c) TSF によって示される最大許容レベルのモジュール間結合の記述

d) TSF のモジュールによって示される最小許容レベルの凝集度の記述

781 TOE で使用されるその他の種別の技術(例えば、非手続き型ソフトウェア(オブジェクト指向プログラミングなど)、広く普及している汎用ハードウェア(PC マイクロプロセッサなど)、特殊目的のハードウェア(スマートカードプロセッサなど))については、「適切に構成」されていることの基準の適切性を決定するために、評価監督機関に相談するべきである。

ADV_INT.2.2C ***TSF 内部構造の記述は、TSF 全体が適切に構成されていることを実証しなければならない。***

ADV_INT.2-2 評価者は、TSF が適切に構成されていることを TSF 内部構造の記述が実証していることを決定するために、この記述を***検査しなければならない。***

782 評価者は、TSF がADV_INT.2-1の基準をどのように満たしているかを内部構造の記述が適切に説明していることを保証するために、その記述を検査する。

783 例えば、TSF の手続き型ソフトウェアの部分がどのように以下の基準を満たすかを説明する:

a) TSF で識別されるモジュールとTOE 設計(ADV_TDS)で記述されているモジュールが 1 対 1 で対応していること

b) モジュール分解プロセスが TSF 設計にどのように反映されているか

c) コーディング標準が使用されていないまたは満たされていないすべての場合に対する正当化

d) 許容範囲外の結合または凝集度に対する正当化

12.6.2.5 **アクション** ADV_INT.2.2E

ADV_INT.2-3 評価者は、TOE 設計が適切に構成されていることを***決定しなければならない。***

784 評価者は、正当化の正確さを検証するために、TSF のサンプルの TOE 設計を検査する。例えば、TOE 設計のサンプルを分析して、設計標準に準拠していることなどを決定する。サブセットに対してアクティビティを行うすべての領域と同様に、評価者はサンプルのサイズと範囲の正当化を提供する。

785 サブシステム及びモジュールへの TOE の分解の記述は、TSF のサブセットが適切に構成されていることが自明であることを立論する。TSF を構成する手続き(ALC_TATで検査)に従っていることを検証することで、TSF のサブセットが適切に構成されていることが自明となる。

ADV_INT.2-4 評価者は、TSF が適切に構成されていることを***決定しなければならない。***

786 ADV_IMPが主張されている保証の一部でない場合、このワークユニットは該当しないため、満たされているものとみなされる。

787 評価者は、内部構造の記述の正確さを検証するために、TSF のサンプルを検査する。例えば、TSF の手続き型ソフトウェアの部分のサンプルを分析して、その凝集度と結合、コーディング標準への準拠などを決定する。サブセットに対してアクティビティを行うすべての領域と同様に、評価者はサンプルのサイズと範囲の正当化を提供する。

12.6.3 サブアクティビティの評価(ADV_INT.3)

788 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

12.7 セキュリティ方針モデル化(ADV_SPM)

12.7.1 サブアクティビティの評価(ADV_SPM.1)

789 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

12.8 TOE 設計(ADV_TDS)

12.8.1 サブアクティビティの評価(ADV_TDS.1)

12.8.1.1 入力

790 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) セキュリティアーキテクチャ記述;

d) TOE 設計。

12.8.1.2 アクション ADV_TDS.1.1E

ADV_TDS.1.1C ***設計は、サブシステムの観点から TOE の構造を記述しなければならない。***

ADV_TDS.1-1 評価者は、TOE 全体の構造がサブシステムの観点から記述されていることを決定するために、TOE 設計を***検査しなければならない。***

791 評価者は、TOE のすべてのサブシステムが識別されていることを保証する。TOE のこの記述は、TSF を構成する TOE の部分が識別されているワークユニット ADV_TDS.1-2 に対する入力として使用される。つまり、この要件は、TSF のみについてのものではなく、TOE 全体についてのものである。

792 TOE (及び TSF)は、抽象の複数の階層(つまり、サブシステム及びモジュール)で記述することができる。TOE の複雑さに応じて、設計は、CC パート 3 附属書の A.4、「ADV_TDS: サブシステム及びモジュール」での記述に従い、サブシステム及びモジュールの観点から記述することができる。この保証レベルでは、分解は「サブシステム」レベルであることのみが必要である。

793 このアクティビティを実行する際に、評価者は、TOE に対して提示されるその他の証拠(例えば、ST、利用者操作ガイダンス)における TOE の記述が、TOE 設計に含まれる記述と一貫していることを決定するために、このような証拠を検査する。

ADV_TDS.1.2C ***設計は、TSF のすべてのサブシステムを識別しなければならない。***

ADV_TDS.1-2 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。***

794 ワークユニット ADV_TDS.1-1 では、TOE のすべてのサブシステムが識別され、TSF 以外のサブシステムの特徴が正しく表されていたことが決定された。その作業に基づいて、TSF 以外のサブシステムとして特徴が表されなかったサブシステムは、正確に識別されるべきである。評価者は、準備手続き(AGD_PRE)のガイダンスに従って設置し、構成されたハードウェア及びソフトウェアについて、各サブシステムが TSF の一部またはそれ以外のものとして考慮されていることを決定する。

ADV_TDS.1.3C ***設計は、TSF の各 SFR 支援または SFR 非干渉サブシステムのふるまいの要約を提供しなければならない。***

ADV_TDS.1-3 評価者は、サブシステムが SFR 支援もしくは、SFR 非干渉であることを評価者が決定できるように TSF の各 SFR 支援もしくは、SFR 非干渉サブシステムが記述されてい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。***

795 システム内でどのように機能するかについて、SFR 支援及び SFR 非干渉サブシステムを詳細に記述する必要はない。ただし、評価者は、開発者によって提供された証拠に基づいて、上位レベルの記述を持たないサブシステムが、SFR 支援または SFR 非干渉であることを決定する。サブシステムの分類の要点は、開発者に、SFR 支援及び SFR 非干渉サブシステムに対して提供する情報は、SFR 実施サブシステムに対する情報よりも少なくてよいとしているため、開発者が均一のレベルの詳細な証拠資料を提供する場合、このワークユニットの大部分が満たされることに留意すること。

796 SFR 支援サブシステムは、SFR を実装するために SFR 実施サブシステムが依存しているサブシステムであるが、SFR 実施サブシステムほど直接的な役割を果たさない。SFR 非干渉サブシステムは、支援の役割においても実施の役割においても、SFR を実装するために依存されないサブシステムである。

ADV_TDS.1.4C ***設計は、SFR 実施サブシステムの SFR 実施のふるまいを要約しなければならない。***

ADV_TDS.1-4 評価者は、TOE 設計が SFR 実施サブシステムの SFR 実施のふるまいの完全で正確な上位レベルの要約を提供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。***

797 開発者は、サブシステムを SFR 実施、SFR 支援及び SFR 非干渉として指示できるが、これらの「タグ」は、開発者が提供する必要がある情報の量と種別を記述するためだけに使用され、もし開発者の工学的プロセスが必要な証拠資料を提供しない場合に開発者が開発する必要のある情報の量を制限するために使用することができる。サブシステムが開発者によって分類されているかどうかに関係なく、TOE においてサブシステムがそれぞれの役割(SFR 実施など)に対する適切な情報を持つことを決定し、開発者が特定のサブシステムに必要な情報を提供するのに失敗した場合に開発者から適切な情報を取得するのは、評価者の責任である。

798 SFR 実施のふるまいは、サブシステムが*どのように*SFR を実装する機能性を提供するかを参照する。評価者の評定の目標は、各 SFR 実施サブシステムが機能する方法を評価者が理解できるようにすることである。ふるまいの要約に対して提供される情報は、ふるまいの記述によって提供される情報ほど詳細である必要はない。例えば、データ構造またはデータ項目は、詳細に記述する必要がない可能性がある。ただし、これは特定の TOE に対して「上位レベル」が何を意味するかに関する評価者の決定であり、このワークユニットに対する適切な判定を行うために、評価者は(たとえ、それがサブシステムのふるまいに対して提供されている情報と同等であることが判明しても)、開発者から十分な情報を取得する。

799 ただし、「完全な」保証は、このワークユニットの目標でも要件でもないため、評価者は、このワークユニットについての判定を行うために必要な証拠の量と構成を決定する際に、判断を行う必要があることに注意のこと。

800 評価者は、完全さ及び正確さを決定するために、その他の利用可能な情報(例えば、機能仕様、セキュリティアーキテクチャ記述)を検査する。これらの文書の機能性の要約は、このワークユニットの証拠に対して提供されているものと一貫しているべきである。

ADV_TDS.1.5C ***設計は、TSF の SFR 実施サブシステム間、及び TSF の SFR 実施サブシステムと TSF のその他のサブシステム間の相互作用の記述を提供しなければならない。***

ADV_TDS.1-5 評価者は、TSF のサブシステム間の相互作用が記述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。***

801 SFR 実施サブシステムとその他のサブシステムの間の相互作用を記述する目標は、TSF がどのように機能を実行するかを読者がよりよく理解できるようにすることである。これらの相互作用は、実装レベル(例えば、1 つのサブシステム内のルーチンから別のサブシステム内のルーチンに渡されるパラメタ、グローバル変数、ハードウェアサブシステムから割り込み処理サブシステムへのハードウェア信号(例えば、割り込み))で特徴を表す必要はないが、別のサブシステムによって使用される特定のサブシステムに対して識別されるデータエレメントは、この説明に含まれる必要がある。サブシステム間(例えば、ファイアウォールシステムの規則のベースの構成に対する責任を持つサブシステムと実際にこれらの規則を実装するサブシステム)の制御関係もすべて記述するべきである。

802 評価者は、記述の完全さを評定する際に、独自の判断を使用する必要がある。相互作用の理由が明確でない場合、または記述されるように見えない(例えば、サブシステムのふるまいの記述の検査中に発見された)SFR 関連の相互作用がある場合、評価者は、この情報が開発者によって提供されることを保証する。ただし、特定のサブシステムのセットの間の相互作用が、開発者によって不完全に記述されていたとしても、完全な記述が TSF によって提供される機能性全体やセキュリティ機能性の理解の助けにならないことを評価者が決定できる場合は、評価者は、記述を十分なものと考えることを選択することができ、そのための完全さを追求しないようにすることができる。

ADV_TDS.1.6C **マッピングは、すべての TSFI が、それらが呼び出す TOE 設計で記述されているふるまいを追跡することを実証しなければならない。**

ADV_TDS.1-6 評価者は、TOE 設計が、機能仕様で記述されている TSFI から TOE 設計で記述されている TSF のサブシステムへの完全で正確なマッピングを含む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。***

803 TOE 設計で記述されているサブシステムは、TSF が TSF の SFR 実施部分に対して詳細レベルでどのように機能するか、及び TSF のその他の部分に対して、より上位のレベルでどのように機能するかについての記述を提供する。TSFI は、実装がどのように実行されるかの記述を提供する。開発者からの証拠は、操作が TSFI で要求される場合に最初に関わるサブシステムを識別し、主に機能性の実装に責任のある様々なサブシステムを識別する。各 TSFI に対する完全な「コールツリー」は、このワークユニットでは必要ではない。

804 評価者は、すべての TSFI が少なくとも 1 つのサブシステムにマッピングされることを保証することによって、マッピングの完全さを評定する。正確さの検証は、より複雑である。

805 正確さの最初の側面は、TSF 境界で各 TSFI がサブシステムにマッピングされることである。この決定は、サブシステム記述及び相互作用をレビューすることによって、及びアーキテクチャでのサブシステムの場所を決定するこの情報から、行うことができる。正確さの次の側面は、マッピングが意味を持つことである。例えば、アクセス制御を扱う TSFI を、パスワードをチェックするサブシステムにマッピングするのは、正確ではない。評価者は、この決定を行う際に再度判断を使用するべきである。目標は、この情報が、評価者の、SFR のシステム及び実装、及び TSF 境界にあるエンティティが TSF と対話できる方法の理解への助けになることである。SFR がサブシステムによって正確に記述されているかどうかについての評定の大半は、他のワークユニットで実行される。

12.8.1.3 **アクション** ADV_TDS.1.2E

ADV_TDS.1-7 評価者は、すべての ST セキュリティ機能要件が TOE 設計に含まれることを決定するために、TOE セキュリティ機能要件及び TOE 設計を***検査しなければならない。***

806 評価者は、TOE セキュリティ機能要件と TOE 設計の間のマッピングを作成することができる。このマッピングは、機能要件からサブシステムのセットに対して作成される可能性が高い。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、要件のコンポーネントレベルより下、さらにはエレメントレベルより下の詳細さが必要になる場合もあるので注意する必要がある。

807 例えば、FDP_ACC.1 サブセットアクセス制御コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1 サブセットアクセス制御の割付に 10 の規則が含まれていたとして、その 10 の規則が 15 モジュール内の特定の場所に実装された場合、評価者が FDP_ACC.1 サブセットアクセス制御を 1 つのサブシステムにマッピングして、ワークユニットが完了したと主張するのは適切でない。代わりに、評価者は、FDP_ACC.1 サブセットアクセス制御(規則 1)をサブシステム A、ふるまい x、y、及び z にマッピングし、FDP_ACC.1 サブセットアクセス制御(規則 2)をサブシステム A、ふるまい x、p、及び q にマッピングするなどのように、マッピングする可能性がある。

ADV_TDS.1-8 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。***

808 評価者は、ST の TOE セキュリティ機能要件の節にリストされている各セキュリティ要件に対応し、TSF がその要件をどのように満たしているかを正確に詳述している設計記述が TOE 設計内にあることを保証する。このため、評価者は、任意の機能要件の実装に責任のあるサブシステムの集合を識別し、それらのサブシステムを検査して要件がどのように実装されるかを理解する必要がある。最後に、評価者は、要件が正確に実装されたかどうかを評定する。

809 例えば、ST 要件が役割によるアクセス制御メカニズムを指定した場合、評価者は、このメカニズムの実装に寄与するサブシステムを最初に識別する。これは、TOE 設計についての深い知識または理解に基づいて、または前のワークユニットで行われた作業によって、行われることがある。この追跡は、サブシステムの識別のためだけに行われるもので、完全な分析ではないことに注意のこと。

810 次のステップは、サブシステムが実装するのはどのようなメカニズムであるかを理解することである。例えば、設計が UNIX スタイルの保護ビットに基づいてアクセス制御を記述した場合、その設計は、上記で使用された ST 例で示しているアクセス制御要件の正確な具体化にならない。評価者が、詳細がないためにメカニズムが正確に実装されたことを決定できなかった場合、評価者は、すべての SFR 実施サブシステムが識別されたかどうか、または適切な詳細がそれらのサブシステムに提供されたかどうかを評定することが必要になる。

12.8.2 サブアクティビティの評価(ADV_TDS.2)

12.8.2.1 入力

811 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) セキュリティアーキテクチャ記述;

d) TOE 設計。

12.8.2.2 アクション ADV_TDS.2.1E

ADV_TDS.2.1C ***設計は、サブシステムの観点から TOE の構造を記述しなければならない。***

ADV_TDS.2-1 評価者は、TOE 全体の構造がサブシステムの観点から記述されていることを決定するために、TOE 設計を***検査しなければならない。***

812 評価者は、TOE のすべてのサブシステムが識別されていることを保証する。TOE のこの記述は、TSF を構成する TOE の部分が識別されているワークユニット ADV_TDS.2-2 に対する入力として使用される。つまり、この要件は、TSF のみについてのものではなく、TOE 全体についてのものである。

813 TOE (及び TSF)は、抽象の複数の階層(つまり、サブシステム及びモジュール)で記述することができる。TOE の複雑さに応じて、設計は、CC パート 3 附属書の A.4、「ADV_TDS: サブシステム及びモジュール」での記述に従い、サブシステム及びモジュールの観点から記述することができる。この保証レベルでは、分解は「サブシステム」レベルであることのみが必要である。

814 このアクティビティを実行する際に、評価者は、TOE に対して提示されるその他の証拠(例えば、ST、利用者操作ガイダンス)における TOE の記述が、TOE 設計に含まれる記述と一貫していることを決定するために、このような証拠を検査する。

ADV_TDS.2.2C ***設計は、TSF のすべてのサブシステムを識別しなければならない。***

ADV_TDS.2-2 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。***

815 ワークユニット ADV_TDS.2-1 では、TOE のすべてのサブシステムが識別され、TSF 以外のサブシステムの特徴が正しく表されていたことが決定された。その作業に基づいて、TSF 以外のサブシステムとして特徴が表されなかったサブシステムは、正確に識別されるべきである。評価者は、準備手続き(AGD_PRE)のガイダンスに従って設置し、構成されたハードウェア及びソフトウェアについて、各サブシステムが TSF の一部またはそれ以外のものとして考慮されていることを決定する。

ADV_TDS.2.3C ***設計は、TSF の各 SFR 非干渉サブシステムのふるまいの要約を提供しなければならない。***

ADV_TDS.2-3 評価者は、サブシステムが SFR 非干渉であることを評価者が決定できるように TSF の各 SFR 非干渉サブシステムが記述されてい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。***

816 システム内でどのように機能するかについて、SFR 非干渉サブシステムを詳細に記述する必要はない。ただし、評価者は、開発者によって提供された証拠に基づいて、詳細な記述を持たないサブシステムが SFR 非干渉であることを決定する。サブシステムの分類の要点は開発者が SFR 非干渉サブシステムに対しては SFR 実施サブシステム及び SFR 支援サブシステムに対する情報よりも少ない情報を提供するようにすることであるため、開発者が均一のレベルの詳細な証拠資料を提供する場合、このワークユニットの大部分が満たされる。

817 SFR 非干渉サブシステムは、SFR 実施サブシステム及び SFR 支援サブシステムが依存しないサブシステムである。つまり、SFR 非干渉サブシステムは、SFR 機能性の実装において何の役割も果たさない。

ADV_TDS.2.4C ***設計は、SFR 実施サブシステムの SFR 実施のふるまいを記述しなければならない。***

ADV_TDS.2-4 評価者は、TOE 設計が SFR 実施サブシステムの SFR 実施のふるまいの完全で正確で詳細な記述を提供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。***

818 開発者はサブシステムを SFR 実施、SFR 支援、及び SFR 非干渉として指示できるが、これらの「タグ」は、開発者が提供する必要がある情報の量と種別を記述するためだけに使用され、もし開発者の工学的プロセスが必要な証拠資料を提供しない場合に開発者が開発する必要のある情報の量を制限するために使用することができる。サブシステムが開発者によって分類されているかどうかに関係なく、TOE においてサブシステムがそれぞれの役割(SFR 実施など)に対する適切な情報を持つことを決定し、開発者が特定のサブシステムに必要な情報を提供するのに失敗した場合に開発者から適切な情報を取得するのは、評価者の責任である。

819 SFR 実施のふるまいは、サブシステムが*どのように*SFR を実装する機能性を提供するかを参照する。ふるまいの詳細な記述は、アルゴリズム記述のレベルではないが、通常、どのような主要データとデータ構造であるか、どのような制御関係がサブシステム内に存在するか、及びこれらのエレメントがどのように一体となって機能し SFR 実施のふるまいを提供するかという観点から、機能性がどのように提供されているかということを説明する。こうした記述は、次に続くワークユニットを実行する際に評価者が考慮するべき SFR 支援のふるまいも参照する。

820 評価者は、完全さ及び正確さを決定するために、その他の利用可能な情報(例えば、機能仕様、セキュリティアーキテクチャ記述)を検査する。これらの文書の機能性の記述は、このワークユニットの証拠に対して提供されている記述と一貫しているべきである。

ADV_TDS.2.5C ***設計は、SFR 実施サブシステムの SFR 支援及び SFR 非干渉のふるまいを要約しなければならない。***

ADV_TDS.2-5 評価者は、TOE 設計が SFR 実施サブシステムの SFR 支援及び SFR 非干渉のふるまいの完全で正確な上位レベルの要約を提供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。***

821 開発者はサブシステムを SFR 実施、SFR 支援、及び SFR 非干渉として指示できるが、これらの「タグ」は、開発者が提供する必要がある情報の量と種別を記述するためだけに使用され、もし開発者の工学的プロセスが必要な証拠資料を提供しない場合に開発者が開発する必要のある情報の量を制限するために使用することができる。サブシステムが開発者によって分類されているかどうかに関係なく、TOE においてサブシステムがそれぞれの役割(SFR 実施など)に対する適切な情報を持つことを決定し、開発者が特定のサブシステムに必要な情報を提供するのに失敗した場合に開発者から適切な情報を取得するのは、評価者の責任である。

822 前のワークユニットとは異なり、このワークユニットは、SFR 支援あるいは SFR 非干渉である SFR 実施サブシステムに対して提供されている情報を評定するために、評価者を必要とする。この評定の目標は、2 つに分かれる。第 1 に、これにより、各サブシステムがどのように機能するかについての評価者の理解が深まるようになるべきである。第 2 に、この評定で、SFR 実施のサブシステムによって示されるすべての SFR 実施のふるまいが記述されていることを評価者が決定できるようにする。前のワークユニットとは異なり、SFR 支援あるいは SFR 非干渉のふるまいに対して提供されている情報は、SFR 実施のふるまいによって提供されている情報ほど詳細である必要はない。例えば、SFR 実施機能性に関係しないデータ構造またはデータ項目については、まったく関係ない場合であれば、詳細に記述する必要がない可能性がある。ただし、これは特定の TOE に対して「上位レベル」が何を意味するかに関する評価者の決定であり、このワークユニットに対する適切な判定を行うために、評価者は(たとえ、それが SFR 実施サブシステムの一部に対して提供されている情報と同等であることが判明しても)開発者から十分な情報を取得する。

823 ただし、「完全な」保証はこのワークユニットの目標でも要件でもないため、評価者は、このワークユニットについての判定を行うために必要な証拠の量と構成を決定する際に、判断を実行する必要があることに注意すること。

824 評価者は、完全さ及び正確さを決定するために、その他の利用可能な情報(例えば、機能仕様、セキュリティアーキテクチャ記述)を検査する。これらの文書の機能性の要約は、このワークユニットの証拠に対して提供されているものと一貫しているべきである。特に、ふるまいは SFR 実施、SFR 支援または SFR 非干渉のいずれかであるため、機能仕様は、機能仕様によって記述されている TSF インタフェースを実装するために必要なふるまいがサブシステムによって完全に記述されていることを決定するために使用されるべきである。

ADV_TDS.2.6C ***設計は、SFR 支援サブシステムのふるまいを要約しなければならない。***

ADV_TDS.2-6 評価者は、TOE 設計が SFR 支援サブシステムのふるまいの完全で正確な上位レベルの要約を提供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。***

825 開発者はサブシステムを SFR 実施、SFR 支援、及び SFR 非干渉として指示できるが、これらの「タグ」は、開発者が提供する必要がある情報の量と種別を記述するためだけに使用され、もし開発者の工学的プロセスが必要な証拠資料を提供しない場合に開発者が開発する必要のある情報の量を制限するために使用することができる。サブシステムが開発者によって分類されているかどうかに関係なく、TOE においてサブシステムがそれぞれの役割(SFR 実施など)に対する適切な情報を持つことを決定し、開発者が特定のサブシステムに必要な情報を提供するのに失敗した場合に開発者から適切な情報を取得するのは、評価者の責任である。

826 前の 2 つのワークユニットとは異なり、このワークユニットは、SFR 支援サブシステムについての情報を提供するために開発者を(及び、評定するために評価者を)必要とする。こうしたサブシステムは、SFR 実施サブシステムの記述によって、また、ワークユニット ADV_TDS.2-7 における相互作用の記述によって参照されるべきである。評価者の評定の目標は、前のワークユニットと同様に、2 つに分かれる。第 1 に、これにより、各 SFR 支援サブシステムがどのように機能するかについて、評価者が理解できるようになるべきである。第 2 に、評価者は、サブシステムが SFR 実施のふるまいを支援する方法が明確になるようにふるまいが十分に詳細に要約されること、また、ふるまい自体が SFR 実施ではないことを決定する。SFR 支援サブシステムのふるまいに対して提供されている情報は、SFR 実施のふるまいによって提供される情報ほど詳細である必要はない。例えば、SFR 実施機能性に関係しないデータ構造またはデータ項目については、まったく関係ない場合であれば、詳細に記述する必要がない可能性がある。ただし、これは特定の TOE に対して「上位レベル」が何を意味するかに関する評価者の決定であり、このワークユニットに対する適切な判定を行うために、評価者は(たとえ、それが SFR 実施サブシステムの一部に対して提供されている情報と同等であることが判明しても)開発者から十分な情報を取得する。

827 ただし、「完全な」保証はこのワークユニットの目標でも要件でもないため、評価者は、このワークユニットについての判定を行うために必要な証拠の量と構成を決定する際に、判断を実行する必要があることに注意すること。

828 評価者は、完全さ及び正確さを決定するために、その他の利用可能な情報(例えば、機能仕様、セキュリティアーキテクチャ記述)を検査する。これらの文書の機能性の要約は、このワークユニットの証拠に対して提供されているものと一貫しているべきである。

ADV_TDS.2.7C ***設計は、TSF のすべてのサブシステム間の相互作用の記述を提供しなければならない。***

ADV_TDS.2-7 評価者は、TSF のサブシステム間の相互作用が記述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。***

829 サブシステム間の相互作用を記述する目標は、TSF がどのように機能を実行するかを読者がよりよく理解できるようにすることである。これらの相互作用は、実装レベル(例えば、1 つのサブシステム内のルーチンから別のサブシステム内のルーチンに渡されるパラメタ、グローバル変数、ハードウェアサブシステムから割り込み処理サブシステムへのハードウェア信号(例えば、割り込み))で特徴を表す必要はないが、別のサブシステムによって使用される特定のサブシステムに対して識別されるデータエレメントは、この説明に含まれる必要がある。サブシステム間(例えば、ファイアウォールシステムの規則のベースの構成に対する責任を持つサブシステムと実際にこれらの規則を実装するサブシステム)の制御関係もすべて記述するべきである。

830 開発者はサブシステム間のすべての相互作用の特徴を表すべきであるが、評価者は記述の完全さを評定する際に独自の判断を使用する必要があることに注意するべきである。相互作用の理由が明確でない場合、または記述されるように見えない(例えば、サブシステムのふるまいの記述の検査中に発見された)SFR 関連の相互作用がある場合、評価者は、この情報が開発者によって提供されることを保証する。ただし、特定のサブシステムのセットの間の相互作用が、開発者によって不完全に記述されていたとしても、完全な記述が TSF によって提供される機能性全体やセキュリティ機能性の理解の助けにならないことを評価者が決定できる場合は、評価者は、記述を十分なものと考えることを選択することができ、そのための完全さを追求しないようにすることができる。

ADV_TDS.2.8C ***マッピングは、すべての TSFI が、それらが呼び出す TOE 設計で記述されているふるまいを追跡することを実証しなければならない。***

ADV_TDS.2-8 評価者は、TOE 設計が、機能仕様で記述されている TSFI から TOE 設計で記述されている TSF のサブシステムへの完全で正確なマッピングを含む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。***

831 TOE 設計で記述されているサブシステムは、TSF が TSF の SFR 実施部分に対して詳細レベルでどのように機能するか、及び TSF のその他の部分に対して、より上位のレベルでどのように機能するかについての記述を提供する。TSFI は、実装がどのように実行されるかの記述を提供する。開発者からの証拠は、操作が TSFI で要求される場合に最初に関わるサブシステムを識別し、主に機能性の実装に責任のある様々なサブシステムを識別する。各 TSFI に対する完全な「コールツリー」は、このワークユニットでは必要ではない。

832 評価者は、すべての TSFI が少なくとも 1 つのサブシステムにマッピングされることを保証することによって、マッピングの完全さを評定する。正確さの検証は、より複雑である。

833 正確さの最初の側面は、TSF 境界で各 TSFI がサブシステムにマッピングされることである。この決定は、サブシステム記述及び相互作用をレビューすることによって、及びアーキテクチャでのサブシステムの場所を決定するこの情報から、行うことができる。正確さの次の側面は、マッピングが意味を持つことである。例えば、アクセス制御を扱う TSFI を、パスワードをチェックするサブシステムにマッピングするのは、正確ではない。評価者は、この決定を行う際に再度判断を使用するべきである。目標は、この情報が、評価者の、SFR のシステム及び実装、及び TSF 境界にあるエンティティが TSF と対話できる方法の理解への助けになることである。SFR がサブシステムによって正確に記述されているかどうかについての評定の大半は、他のワークユニットで実行される。

12.8.2.3 **アクション** ADV_TDS.2.2E

ADV_TDS.2-9 評価者は、すべての ST セキュリティ機能要件が TOE 設計に含まれることを決定するために、TOE セキュリティ機能要件及び TOE 設計を***検査しなければならない。***

834 評価者は、TOE セキュリティ機能要件と TOE 設計の間のマッピングを作成することができる。このマッピングは、機能要件からサブシステムのセットに対して作成される可能性が高い。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、要件のコンポーネントレベルより下、さらにはエレメントレベルより下の詳細さが必要になる場合もあるので注意する必要がある。

835 例えば、FDP_ACC.1 サブセットアクセス制御コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1 サブセットアクセス制御の割付に 10 の規則が含まれていたとして、その 10 の規則が 15 モジュール内の特定の場所に実装された場合、評価者が FDP_ACC.1 サブセットアクセス制御を 1 つのサブシステムにマッピングして、ワークユニットが完了したと主張するのは適切でない。代わりに、評価者は、FDP_ACC.1 サブセットアクセス制御(規則 1)をサブシステム A、ふるまい x、y、及び z にマッピングし、FDP_ACC.1 サブセットアクセス制御(規則 2)をサブシステム A、ふるまい x、p、及び q にマッピングするなどのように、マッピングする可能性がある。

ADV_TDS.2-10 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。***

836 評価者は、ST の TOE セキュリティ機能要件の節にリストされている各セキュリティ要件に対応し、TSF がその要件をどのように満たしているかを正確に詳述している設計記述が TOE 設計内にあることを保証する。このため、評価者は、任意の機能要件の実装に責任のあるサブシステムの集合を識別し、それらのサブシステムを検査して要件がどのように実装されるかを理解する必要がある。最後に、評価者は、要件が正確に実装されたかどうかを評定する。

837 例えば、ST 要件が役割によるアクセス制御メカニズムを指定した場合、評価者は、このメカニズムの実装に寄与するサブシステムを最初に識別する。これは、TOE 設計についての深い知識または理解に基づいて、または前のワークユニットで行われた作業によって、行われることがある。この追跡は、サブシステムの識別のためだけに行われるもので、完全な分析ではないことに注意のこと。

838 次のステップは、サブシステムが実装するのはどのようなメカニズムであるかを理解することである。例えば、設計が UNIX スタイルの保護ビットに基づいてアクセス制御を記述した場合、その設計は、上記で使用された ST 例で示しているアクセス制御要件の正確な具体化にならない。評価者が、詳細がないためにメカニズムが正確に実装されたことを決定できなかった場合、評価者は、すべての SFR 実施サブシステムが識別されたかどうか、または適切な詳細がそれらのサブシステムに提供されたかどうかを評定することが必要になる。

12.8.3 サブアクティビティの評価(ADV_TDS.3)

12.8.3.1 目的

839 このサブアクティビティの目的は、TOE 設計が TSF 境界を決定するために十分な TOE の記述をサブシステムの観点から提供するかどうか、及び TSF 内部構造の記述をモジュール(及び、オプションとして上位レベル抽象)の観点から提供するかどうかを決定することである。これは、SFR 実施モジュールの詳細な記述、及び SFR が完全に正確に実装されていることを評価者が決定するために十分な SFR 支援モジュール及び SFR 非干渉モジュールについての情報を提供する。このように、TOE 設計は、実装表現の説明を提供する。

12.8.3.2 入力

840 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) セキュリティアーキテクチャ記述;

d) TOE 設計。

12.8.3.3 適用上の注釈

841 TOE 設計に関して評価者が保証しなければならない 3 つのタイプのアクティビティがある。第 1 に、評価者は、TSF 境界が適切に記述されていることを決定する。第 2 に、評価者は、開発者がこのサブシステムの内容及び提示の要件に適合しており、TOE に対して提供されるその他の証拠資料と一貫している証拠資料を提供したことを決定する。最後に、評価者は、システムがどのように実装されているかを理解し、また、その知識を使用して、機能仕様内の TSFI が適切に記述されること、及びテスト情報が適切に(「ATE クラス: テスト」ワークユニットで行われた) TSF をテストすることを保証するために、(詳細レベルで) SFR 実施モジュールに対して、及び(より低い詳細レベルで) SFR 支援及び SFR 非干渉モジュールに対して提供される設計情報を分析しなければならない。

842 開発者は TSF の完全な記述を提供する義務がある(SFR 実施モジュールは SFR 支援または SFR 非干渉モジュールよりもより詳細であるが)が、評価者は分析を実行する際に判断を使用することが期待されるということが重要である。評価者は各モジュールを調べることを期待されるが、各モジュールを検査する際の詳細のレベルは、場合によって異なる。評価者は、システムのセキュリティ上のモジュールの機能性の効果を決定するための十分な理解を得るために各モジュールを分析する。モジュールを分析する必要がある際の分析の深さはシステム内のそのモジュールの役割によって異なる可能性がある。この分析の重要な側面は、評価者が、記述されている機能性が正しいこと、及び SFR 支援または SFR 非干渉モジュールの暗黙の指示(下記を参照のこと)がシステムアーキテクチャ内の役割によってサポートされていることを決定するために、提供されているその他の証拠資料(TSS、機能仕様、セキュリティアーキテクチャ記述、及び TSF 内部構造文書)を使用するべきであることである。

843 開発者はモジュールを SFR 実施、SFR 支援、及び SFR 非干渉として指示できるが、これらの「タグ」は、開発者が提供する必要がある情報の量と種別を記述するためだけに使用され、もし開発者の工学的プロセスが必要な証拠資料を提供しない場合に開発者が開発する必要のある情報の量を制限するために使用することができる。モジュールが開発者によって分類されているかどうかに関係なく、TOE においてモジュールがそれぞれの役割(SFR 実施など)に対する適切な情報を持つことを決定し、開発者が特定のモジュールに必要な情報を提供するのに失敗した場合に開発者から適切な情報を取得するのは、評価者の責任である。

12.8.3.4 アクション ADV_TDS.3.1E

ADV_TDS.3.1C ***設計は、サブシステムの観点から TOE の構造を記述しなければならない。***

ADV_TDS.3-1 評価者は、TOE 全体の構造がサブシステムの観点から記述されていることを決定するために、TOE 設計を***検査しなければならない。***

844 評価者は、TOE のすべてのサブシステムが識別されていることを保証する。TOE のこの記述は、TSF を構成する TOE の部分が識別されているワークユニット ADV_TDS.3-2 に対する入力として使用される。つまり、この要件は、TSF のみについてのものではなく、TOE 全体についてのものである。

845 TOE (及び TSF)は、抽象の複数の階層(つまり、サブシステム及びモジュール)で記述することができる。TOE の複雑さに応じて、設計は、CC パート 3 附属書の A.4、「ADV_TDS: サブシステム及びモジュール」での記述に従い、サブシステム及びモジュールの観点から記述することができる。「モジュール」レベル(ADV_TDS.3-2 を参照のこと)だけで記述できる非常に簡単な TOE の場合、このワークユニットは該当しないため、満たされているものとみなされる。

846 このアクティビティを実行する際に、評価者は、TOE に対して提示されるその他の証拠(例えば、ST、利用者操作ガイダンス)における TOE の記述が、TOE 設計に含まれる記述と一貫していることを決定するために、このような証拠を検査する。

ADV_TDS.3.2C ***設計は、モジュールの観点から TSF を記述しなければならない。***

ADV_TDS.3-2 評価者は、TSF 全体がモジュールの観点から記述されてい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。***

847 評価者は、その他のワークユニット内の特定の特性についてモジュールを検査する。このワークユニットでは、評価者は、モジュール記述が TSF の一部だけではなく、TSF 全体を含むことを決定する。評価者は、この決定を行う際に、評価に対して提供されるその他の証拠(例えば、機能仕様、セキュリティアーキテクチャ記述)を使用する。例えば、機能仕様に TOE 設計記述に記述されるように見えない機能性に対するインタフェースが含まれている場合、TSF の一部が適切に含まれていない可能性がある。この決定は、繰返しプロセスになる可能性があり、その場合、他の証拠について行われる分析の回数が多いほど、証拠資料の完全さに関してより多くの信頼を得ることができる。

848 サブシステムとは異なり、モジュールは、実装表現のレビューに対するガイドとしての役割を果たすことができる詳細レベルで実装を記述する。モジュールの記述は、その記述からモジュールの実装を作成できるものであるべきであり、その結果の実装は 1)提示されるインタフェースの観点から実際の TSF 実装と同一であり、2) 設計で言及されるインタフェースの使用において同一であり、そして、3) TSF モジュールの目的の記述と機能的に同等である。例えば、RFC 793 は TCP プロトコルの上位レベル記述を提供する。これは、必ずしも実装には依存していない。これは、豊富な詳細を提供するが、実装固有のものではないため、適切な設計記述では**ない**。実際の実装は RFC で指定されているプロトコルを追加でき、実装の選択(例えば、実装の様々な部分において、グローバルデータを使用するかまたはローカルデータを使用するか)は実行される分析に対して影響を与える可能性がある。TCP モジュールの設計記述は、(RFC 793 で定義されたインタフェースだけではなく)実装によって提示されるインタフェース、及び TCP を(TSF の一部であったと想定して)実装しているモジュールに関連する処理のアルゴリズム記述をリストする。

ADV_TDS.3.3C ***設計は、TSF のすべてのサブシステムを識別しなければならない。***

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。***

849 設計がモジュールの観点からだけ提示されている場合、これらの要件のサブシステムはモジュールと同等であり、アクティビティはモジュールレベルで実行されるべきである。

850 ワークユニット ADV_TDS.3-1 では、TOE のすべてのサブシステムが識別され、TSF 以外のサブシステムの特徴が正しく表されていたことが決定された。その作業に基づいて、TSF 以外のサブシステムとして特徴が表されなかったサブシステムは、正確に識別されるべきである。評価者は、準備手続き(AGD_PRE)のガイダンスに従って設置し、構成されたハードウェア及びソフトウェアについて、各サブシステムが TSF の一部またはそれ以外のものとして考慮されていることを決定する。

ADV_TDS.3.4C ***設計は、TSF の各サブシステムの記述を提供しなければならない。***

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。***

851 設計がモジュールの観点からだけ提示されている場合、このワークユニットは、次に続くワークユニットで行われる評定によって満たされているものとみなされる。この場合、評価者側での明示的なアクションは必要ない。

852 モジュール記述に加えてTSFのサブシステムレベルの記述を是認するのに十分複雑なシステムでは、サブシステムレベルの記述の目標は、評価者に、次に続くモジュール記述の文脈を提供することである。このため、評価者は、サブシステムレベルの記述が、設計においてセキュリティ機能要件をどのように達成するかの記述を(ただし、モジュール記述の抽象レベルよりは高いレベルで)含んでいることを保証する。この記述は、モジュール記述に合わせて調整されたレベルで使用されるメカニズムを説明するべきである。これは、モジュール記述に含まれている情報を理性的に評定するために必要なロードマップを評価者に提供する。しっかりしたサブシステム記述のセットは、評価者が最も重要な検査対象となるモジュールを決定する、つまり SFR の実施に関して最も関連する TSF の一部に評価アクティビティの焦点を当てるガイドとして役立つ。

853 評価者は、TSF のすべてのサブシステムが記述を持つことを保証する。記述は SFR の実装の実施または支援においてサブシステムが果たす役割に重点を置くべきであるが、SFR 関連の機能性を理解するための文脈が提供されるように、十分な情報を提示しなければならない。

ADV_TDS.3-5 評価者は、サブシステムが SFR 非干渉であることを評価者が決定できるよう、TSF の各 SFR 非干渉サブシステムが記述されてい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。***

854 設計がモジュールの観点からだけ提示されている場合、このワークユニットは、次に続くワークユニットで行われる評定によって満たされているものとみなされる。この場合、評価者側での明示的なアクションは必要ない。

855 SFR 非干渉サブシステムは、SFR 実施サブシステム及び SFR 支援サブシステムが依存しないサブシステムである。つまり、SFR 非干渉サブシステムは、SFR 機能性の実装において何の役割も果たさない。

856 評価者は、TSF のすべてのサブシステムが記述を持つことを保証する。記述は SFR の実装の実施または支援においてサブシステムが果たさない役割に重点を置くべきであるが、SFR 非干渉の機能性を理解するための文脈が提供されるように、十分な情報を提示しなければならない。

ADV_TDS.3.5C ***設計は、TSF のすべてのサブシステム間の相互作用の記述を提供しなければならない。***

ADV_TDS.3-6 評価者は、TSF のサブシステム間の相互作用が記述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。***

857 設計がモジュールの観点からだけ提示されている場合、このワークユニットは、次に続くワークユニットで行われる評定によって満たされているものとみなされる。この場合、評価者側での明示的なアクションは必要ない。

858 モジュール記述に加えてTSFのサブシステムレベルの記述を是認するのに十分複雑なシステムでは、サブシステム間の相互作用の記述の目標は、TSF がどのようにその機能を実行するかを読者がよりよく理解できるようにすることである。これらの相互作用は、実装レベル(例えば、1 つのサブシステム内のルーチンから別のサブシステム内のルーチンに渡されるパラメタ、グローバル変数、ハードウェアサブシステムから割り込み処理サブシステムへのハードウェア信号(例えば、割り込み))で特徴を表す必要はないが、別のサブシステムによって使用される特定のサブシステムに対して識別されるデータエレメントは、この説明に含まれるべきである。サブシステム間(例えば、ファイアウォールシステムの規則のベースの構成に対する責任を持つサブシステムと実際にこれらの規則を実装するサブシステム)の制御関係もすべて記述するべきである。

859 開発者はサブシステム間のすべての相互作用の特徴を表すべきであるが、評価者は記述の完全さを評定する際に独自の判断を使用する必要があることに注意するべきである。相互作用の理由が明確でない場合、または記述されるように見えない(例えば、モジュールレベルの証拠資料の検査中に検出された) SFR 関連の相互作用がある場合、評価者は、この情報が開発者によって提供されることを保証する。ただし、特定のサブシステムのセットの間の相互作用が、開発者によって不完全に記述されていたとしても、完全な記述が TSF によって提供される機能性全体やセキュリティ機能性の理解の助けにならないことを評価者が決定できる場合は、評価者は、記述を十分なものと考えることを選択することができ、そのための完全さを追求しないようにすることができる。

ADV_TDS.3.6C ***設計は、TSF のサブシステムから TSF のモジュールへのマッピングを提供しなければならない。***

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。***

860 設計がモジュールの観点からだけ提示されている場合、このワークユニットは満たされているものとみなされる。

861 モジュール記述に加えて TSF のサブシステムレベルの記述を是認するのに十分複雑な TOE では、開発者はどのように TSF のモジュールがサブシステムに割り当てられているかを示す簡単なマッピングを提供する。これによって、評価者にモジュールレベルの評定を実行する際のガイドが提供される。完全さを決定するには、評価者は、各マッピングを検査し、すべてのサブシステムが少なくとも 1 つのモジュールにマッピングされること、及びすべてのモジュールが正確に 1 つのサブシステムにマッピングされることを決定する。

ADV_TDS.3-8 評価者は、TSF サブシステムと TSF のモジュールの間のマッピングが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。***

862 設計がモジュールの観点からだけ提示されている場合、このワークユニットは満たされているものとみなされる。

863 モジュール記述に加えて TSF のサブシステムレベルの記述を是認するのに十分複雑な TOE では、開発者はどのように TSF のモジュールがサブシステムに割り当てられているかを示す簡単なマッピングを提供する。これによって、評価者にモジュールレベルの評定を実行する際のガイドが提供される。評価者は、その他のワークユニットの実行とともにマッピングの正確さをチェックするように選択することができる。「不正確な」マッピングとは、機能がその内部で使用されていないサブシステムにモジュールが間違って関連付けられているマッピングである。マッピングはより詳細な分析をサポートするガイドとなることを想定しているため、評価者は、このワークユニットに対して適切な労力を注ぐように注意すること。マッピングの正確さを検証するための広範な評価者資源を費やす必要はない。このワークユニットまたはその他のワークユニットの一部としてカバーされない設計に関連する誤解を招く不正確さは、このワークユニットに関連付けられ、訂正されるべきである。

ADV_TDS.3.7C ***設計は、目的と他のモジュールとの関係の観点から各 SFR 実施モジュールを記述しなければならない。***

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。***

864 開発者はモジュールを SFR 実施、SFR 支援、及び SFR 非干渉として指示できるが、これらの「タグ」は、開発者が提供する必要がある情報の量と種別を記述するためだけに使用され、もし開発者の工学的プロセスが必要な証拠資料を提供しない場合に開発者が開発する必要のある情報の量を制限するために使用することができる。モジュールが開発者によって分類されているかどうかに関係なく、TOE においてモジュールがそれぞれの役割(SFR 実施など)に対する適切な情報を持つことを決定し、開発者が特定のモジュールに必要な情報を提供するのに失敗した場合に開発者から適切な情報を取得するのは、評価者の責任である。

865 モジュールの目的は、モジュールがどのような機能を満たしているかを示す記述を提供する。評価者はここで注意が必要である。このワークユニットの重点は、SFR の実装が信頼できることについて決定できるようにモジュールがどのように機能するかを評価者が理解できるようにすること、及びADV_ARCコンポーネントに対して実行されるアーキテクチャ分析をサポートすることであるべきである。評価者がモジュールの操作、及びその他のモジュールや全体としての TOE との関係について適切に理解している限り、評価者は、達成すべきこの作業の目的を考慮すべきであり、開発者が行う証拠資料の実際的な作業には(例えば、自明の実装表現のための完全なアルゴリズム記述を要求するなどして)関わるべきではない。

866 モジュールは下位レベルにあるため、利用者操作ガイダンス、機能仕様、TSF 内部構造、またはセキュリティアーキテクチャ記述などのその他の証拠資料からの完全さ及び正確さの影響を決定するのは困難である可能性がある。ただし、評価者は、目的が正確かつ完全に記述されていることを保証するために役立てることができる範囲で、これらの文書内に提示される情報を使用する。この分析は、機能仕様における TSFI を TSF のモジュールにマッピングする ADV_TDS.3.10C エレメントのワークユニットに対して実行される分析によって、支援が可能である。

ADV_TDS.3.8C ***設計は、各 SFR 実施モジュールの SFR 関連インタフェース、それらのインタフェースからの戻り値、及びその他のモジュールとの相互作用及び他の SFR 実施モジュールに対して呼び出される SFR 関連インタフェースの観点から各 SFR 実施モジュールを記述しなければならない。***

ADV_TDS.3-10 評価者は、各 SFR 実施モジュールによって提示されるインタフェースの記述に SFR 関連パラメタの正確かつ完全な記述、各インタフェースに対する呼び出し規約、及びインタフェースによって直接戻されるすべての値が含ま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。***

867 モジュールの SFR 関連インタフェースは、提供された SFR 関連操作を呼び出す手段として、及び入力を提供する手段として、またはモジュールからの出力を受け取る手段として、その他のモジュールによって使用されるインタフェースである。これらのインタフェースの特定における目的は、テスト中にこれらのインタフェースの実行を許可することである。SFR 関連でないモジュール間インタフェースは、テストにおける要因ではないため、特定または記述する必要はない。同様に、SFR 関連の実行パス(固定された内部パスなど)の通過において要因とならないその他の内部インタフェースも、テストにおける要因ではないため、特定または記述する必要はない。

868 SFR 関連インタフェースは、どのように呼び出されるかという観点から、及び戻されるすべての値の観点から記述される。この記述には、SFR 関連パラメタのリスト、及びこれらのパラメタの記述が含まれる。グローバルデータも、呼び出されたときにモジュールによって(入力または出力として)使用される場合に、パラメタとみなされる。パラメタが値のセット(例えば「フラグ」パラメタ)を受け取ることを期待されていた場合、処理しているモジュールに影響を与えるパラメタが受け取る可能性がある値の完全なセットが指定される。同様に、データ構造を表すパラメタは、データ構造の各フィールドが識別及び記述されるように記述される。異なるプログラミング言語は、不明瞭になる可能性がある追加の「インタフェース」を持つ可能性がある。この例として挙げられるのは、C++でオーバロードしている演算子/関数である。クラス記述におけるこの「暗黙のインタフェース」は、下位レベルの TOE 設計の一部としても記述される。モジュールは 1 つのインタフェースのみを提示する可能性があるが、関連するインタフェースの小規模なセットをモジュールが提示することのほうがより一般的である。

869 モジュールに対するパラメタ(入力及び出力)の評定の観点から、グローバルデータのあらゆる使用についても考慮しなければならない。モジュールはデータを読み取るまたは書き込む場合に、グローバルデータを「使用する」。このようなパラメタの記述が(使用される場合に)完全であることを保証するには、評価者は、TOE 設計でモジュールについて提供されるその他の情報(インタフェース、アルゴリズム記述など)、及びワークユニット ADV_TDS.3-9 で評定されるグローバルデータの特定のセットの記述を使用する。例えば、評価者は、最初に提示された機能及びインタフェース(特にインタフェースのパラメタ)を検査することによってモジュールが実行する処理を決定する。次に、評価者は、処理が TOE 設計で識別されている任意のグローバルデータ領域に「触れる」ように見えるかどうかを確認するためのチェックを行うことができる。その後、評価者は、「触れられた」ように見える各グローバルデータ領域について、グローバルデータ領域が、評価者が検査しているモジュールによって入力または出力の手段としてリストされることを決定する。

870 呼び出し規約は、インタフェースを通じてモジュールの機能性を利用するプログラムを作成していた場合に、そのモジュールのインタフェースを正しく呼び出すために使用できるプログラミング参照型の記述である。これには、グローバル変数に関して実行する必要がある任意のセットアップを含む、必要な入力及び出力が含まれる。

871 インタフェースを通じて戻される値は、パラメタまたはメッセージを通じて渡される値、「C」プログラム関数コールの形式で関数コール自体が戻す値、またはグローバルな手段(*ix 形式のオペレーティングシステムにおける特定のエラールーチンなど)を通じて渡される値を参照する。

872 記述が完全であることを保証するには、評価者は、TOE 設計でモジュールについて提供されるその他の情報(例えば、アルゴリズム記述、使用されているグローバルデータ)を使用して、モジュールの機能を実行するために必要なすべてのデータがモジュールに対して提示されているように見えること、及びその他のモジュールによって検査中のモジュールが提供することを期待されている任意の値がそのモジュールによって戻されるものとして識別されることを保証する。評価者は、処理の記述がインタフェースに渡されるもの、またはインタフェースから渡されるものとしてリストされている情報に一致することを保証することによって、正確さを決定する。

ADV_TDS.3.9C ***設計は、目的及びその他のモジュールとの相互作用の観点から各 SFR 支援モジュールまたは SFR 非干渉モジュールを記述しなければならない。***

ADV_TDS.3-11 評価者は、SFR 支援及び SFR 非干渉モジュールが正しく分類されてい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。***

873 開発者が様々なモジュールに対して様々な量の情報を提供している場合、暗黙の分類が行われる。つまり、(例えば)SFR 関連インタフェース(***ADV_TDS.3.10C*** を参照のこと)に提示される詳細を持つモジュールは、SFR 実施モジュールとなりうるモジュールであるが、評価者による検査によってそれらの特定のセットが SFR 支援もしくは SFR 非干渉であるという決定が導かれる可能性がある。(例えば)目的及びその他のモジュールとの相互作用の記述のみを持つモジュールは、SFR 支援もしくは SFR 非干渉として「暗黙の分類」が行われる。

874 これらの場合、このワークユニットに対する評価者の主要な重点は、SFR 支援もしくは SFR 非干渉として暗黙の分類が行われた各モジュールに対して提供される証拠、及びその他のモジュールについての評価情報(TOE 設計、機能仕様、セキュリティアーキテクチャ記述、及び利用者操作ガイダンス)からモジュールが本当に SFR 支援もしくは SFR 非干渉であるかどうかについての決定を試みることである。この保証のレベルでは、いくつかの誤りは許容されるべきであり、評価者は、指定されたモジュールが SFR 支援もしくは SFR 非干渉として分類されているとしても、そうであるかについての絶対的な確証を持つ必要はない。ただし、提供された証拠によって SFR 支援もしくは SFR 非干渉モジュールが SFR 実施であることが示される場合、評価者は、明確な不一致を解決するために開発者からの追加情報を要求する。例えば、モジュール A (SFR 実施モジュール)に対する証拠資料が、モジュール A がモジュール B をコールして特定の種別の構造についてアクセスチェックを実行することを示すものとする。評価者がモジュール B に関連する情報を検査する場合、評価者は、開発者が提供した情報のすべては、目的及び相互作用のセットである(このため、モジュール B については SFR 支援もしくは SFR 非干渉として暗黙の分類が行われる)ことを発見する。モジュール A からの目的及び相互作用の検査において、評価者はアクセスチェックを実行するモジュール B についての言及がないこと、及びモジュール A はモジュール B の相互作用の対象となるモジュールとしてリストされないことを発見する。この時点では、評価者は、モジュール A 及び及びモジュール B で提供される情報間の不一致を解決することを、開発者に提案するべきである。

875 別の例としては、評価者が ADV_TDS.3.2D によって提供されたようにモジュールに対する TSFI のマッピングを検査する場合がある。この検査は、モジュール C が利用者の識別を必要とする SFR に関連していることを示す。また、評価者がモジュール C に関連する情報を検査する場合、評価者は、開発者が提供した情報のすべては、目的及び相互作用のセットである(このため、モジュール C については SFR 支援もしくは SFR 非干渉として暗黙の分類が行われる)ことを発見する。モジュール C に対して提示される目的及び相互作用の検査において、評価者は、利用者の識別に関連して TSFI に対するマッピングとしてリストされるモジュール C が SFR 実施として分類されない理由を決定することはできない。ここでもまた、評価者は、この不一致を解決することを開発者に提案するべきである。

876 最後の例は、逆の観点からのものである。前の例と同様に、開発者は、目的及び相互作用のセットで構成されているモジュール D (このため、モジュール D については SFR 支援もしくは SFR 非干渉として暗黙の分類が行われる)に関連する情報を提供している。評価者は、モジュール D に対する目的及び相互作用を含む、提供されるすべての証拠を検査する。目的は、相互作用はその記述と一貫しており、モジュール D が SFR 実施であることを示すものは存在しないという、TOE におけるモジュール D の機能の意味のある記述を提供することのように見える。この場合、評価者は、モジュール D が正しく分類されていることを「単に確認するために」にモジュール D についてのより多くの情報を要求するべきではない。開発者は義務を果たし、モジュール D の暗黙の分類において評価者が持っている保証の結果は(定義によって)この保証レベルに対して適切である。

ADV_TDS.3-12 評価者は、各 SFR 支援もしくは SFR 非干渉モジュールの目的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。***

877 モジュールの目的の記述は、モジュールがどのような機能を満たしているかを示す。この記述から、評価者は、モジュールの役割についての包括的な情報を得られるべきである。記述が完全であることを保証するには、評価者は、コールされているモジュールに対する理由がモジュールの目的と一貫しているかどうかを評定するために、その他のモジュールとモジュールとの相互作用について提供される情報を使用する。モジュールの目的からは明らかでない機能性またはモジュールの目的と矛盾する機能性が相互作用の記述に含まれる場合、評価者は、問題が正確さと完全さのどちらの問題であるかを決定する必要がある。評価者は、1 つの文で表現された目的に基づいた意味のある分析は不可能である可能性があるため、短すぎる目的については注意するべきである。

878 モジュールは下位レベルにあるため、利用者操作ガイダンス、機能仕様、セキュリティアーキテクチャ記述、または TSF 内部文書などのその他の証拠資料からの完全さ及び正確さの影響を決定するのは困難である可能性がある。ただし、評価者は、目的が正確かつ完全に記述されていることを保証するために役立てることができる範囲で、これらの文書内に提示される情報を使用する。この分析は、機能仕様における TSFI を TSF のモジュールにマッピングする ADV_TDS.3.10C エレメントのワークユニットに対して実行される分析によって、支援が可能である。

ADV_TDS.3-13 評価者は、その他のモジュールと SFR 支援モジュール、もしくは SFR 非干渉モジュールとの相互作用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。***

879 パート 3 要件及びこのワークユニットの観点から、用語「相互作用」は*インタフェース*より低い厳密さを伝えることを意図していることに注意することが重要である。相互作用は、実装レベル(例えば、1 つのモジュール内のルーチンから別のモジュール内のルーチンに渡されるパラメタ、グローバル変数、ハードウェアサブシステムから割り込み処理サブシステムへのハードウェア信号(例えば、割り込み))で特徴を表す必要はないが、別のモジュールによって使用される特定のモジュールに対して識別されるデータエレメントは、この説明に含まれるべきである。モジュール間(例えば、ファイアウォールシステムの規則のベースの構成に対する責任を持つモジュールと実際にこれらの規則を実装するモジュール)の制御関係もすべて記述するべきである。

880 モジュールは下位レベルにあるため、利用者操作ガイダンス、機能仕様、セキュリティアーキテクチャ記述、または TSF 内部構造文書などのその他の証拠資料から完全さ及び正確さの影響を決定するのは困難である可能性がある。ただし、評価者は、機能が正確かつ完全に記述されていることを保証するために役立てることができる範囲で、これらの文書内に提示される情報を使用する。この分析は、機能仕様における TSFI を TSF のモジュールにマッピングする ***ADV_TDS.3.10C*** エレメントのワークユニットに対して実行される分析によって、支援が可能である。

881 その他のモジュールとモジュールとの相互作用は、単なるコールツリータイプの文書を超えて行われる。相互作用は、モジュールが他のモジュールと対話する理由の機能的な観点から記述される。モジュールの目的は、モジュールが他のモジュールにどのような機能を提供するかを記述することであり、相互作用は、この機能を達成するために、その他のモジュールからモジュールが依存する対象を記述するべきである。

ADV_TDS.3.10C ***マッピングは、すべての TSFI が、それらが呼び出す TOE 設計で記述されているふるまいを追跡することを実証しなければならない。***

ADV_TDS.3-14 評価者は、TOE 設計が、機能仕様で記述されている TSFI から TOE 設計で記述されている TSF のモジュールへの完全で正確なマッピングを含む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。***

882 TOE 設計で記述されているモジュールは、TSF の実装の記述を提供する。TSFI は、実装がどのように実行されるかの記述を提供する。開発者からの証拠は、操作が TSFI で要求される場合に最初に呼び出されるモジュールを識別し、主に機能性の実装に責任のあるモジュールまで呼び出される一連のモジュールを識別する。ただし、各 TSFI に対する完全なコールツリーは、このワークユニットでは必要ではない。複数のモジュールを識別する必要があるのは、入力の条件付けまたは多重入力の分割以外の機能性を持たない「エントリポイント」モジュールまたはラッパーモジュールが存在する場合である。これらのモジュールのいずれかに対するマッピングは、評価者に役立つ情報をまったく提供しない可能性がある。

883 評価者は、すべての TSFI が少なくとも 1 つのモジュールにマッピングされることを保証することによって、マッピングの完全さを評定する。正確さの検証は、より複雑である。

884 正確さの最初の側面は、TSF 境界で各 TSFI がモジュールにマッピングされることである。この決定は、モジュール記述及びそのインタフェース/相互作用をレビューすることによって行うことができる。正確さの次の側面は、識別された最初のモジュールと、主に TSF で提示される機能の実装に責任のあるモジュールとの間のモジュールの連鎖を各 TSFI が識別することである。これは、入力の前処理がどれだけ行われるかによって、最初のモジュールになったり、いくつかのモジュールになったりする可能性がある。TSFI がすべての類似の種別(例えば、システムコール)である場合、前処理のモジュールであることを示す 1 つの指標は、多数の TSFI に対して呼び出されることであることに注意するべきである。正確さの最後の側面は、マッピングが意味を持つことである。例えば、アクセス制御を扱う TSFI を、パスワードをチェックするモジュールにマッピングするのは、正確ではない。評価者は、この決定を行う際に再度判断を使用するべきである。目標は、この情報が、評価者の、SFR のシステム及び実装、及び TSF 境界にあるエンティティが TSF と対話できる方法の理解への助けになることである。SFR がモジュールによって正確に記述されているかどうかについての評定の大半は、他のワークユニットで実行される。

12.8.3.5 アクション ADV_TDS.3.2E

ADV_TDS.3-15 評価者は、すべての ST セキュリティ機能要件が TOE 設計に含まれることを決定するために、TOE セキュリティ機能要件及び TOE 設計を***検査しなければならない。***

885 評価者は、TOE セキュリティ機能要件と TOE 設計の間のマッピングを作成することができる。このマッピングは、機能要件からサブシステムのセットに対して、及びのちに、モジュールに対して作成される可能性が高い。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、要件のコンポーネントレベルより下、さらにはエレメントレベルより下の詳細さが必要になる場合もあるので注意する必要がある。

886 例えば、FDP_ACC.1 サブセットアクセス制御コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1 サブセットアクセス制御の割付に 10 の規則が含まれていたとして、その 10 の規則が 15 モジュール内の特定の場所に実装された場合、評価者が FDP_ACC.1 サブセットアクセス制御を 1 つのサブシステムにマッピングして、ワークユニットが完了したと主張するのは適切でない。代わりに、評価者は、FDP_ACC.1 サブセットアクセス制御(規則 1)をサブシステム A のモジュール x、y、及び z にマッピングし、FDP_ACC.1 サブセットアクセス制御(規則 2)をサブシステム A のモジュール x、p、及び q にマッピングするなどのように、マッピングする可能性がある。

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。***

887 評価者は、TOE セキュリティ機能要件と TOE 設計の間のマッピングを作成することができる。このマッピングは、機能要件からサブシステムのセットまでに対して作成される可能性が高い。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、要件のコンポーネントレベルより下、さらにはエレメントレベルより下の詳細さが必要になる場合もあるので注意する必要がある。

888 例えば、ST 要件が役割によるアクセス制御メカニズムを指定した場合、評価者は、このメカニズムの実装に寄与するサブシステム及びモジュールを最初に識別する。これは、TOE 設計についての深い知識または理解に基づいて、または前のワークユニットで行われた作業によって、行われることがある。この追跡は、サブシステム及びモジュールの識別のためだけに行われるもので、完全な分析ではないことに注意のこと。

889 次のステップは、サブシステム及びモジュールが実装するのはどのようなメカニズムであるかを理解することである。例えば、設計が UNIX スタイルの保護ビットに基づいてアクセス制御を記述した場合、その設計は、上記で使用された ST 例で示しているアクセス制御要件の正確な具体化にならない。評価者が、詳細がないためにメカニズムが正確に実装されたことを決定できなかった場合、評価者は、すべての SFR 実施サブシステム及びモジュールが識別されたかどうか、または適切な詳細がそれらのサブシステム及びモジュールに提供されたかどうかを評定することが必要になる。

12.8.4 サブアクティビティの評価(ADV_TDS.4)

12.8.4.1 目的

890 このサブアクティビティの目的は、TOE 設計が TSF 境界を決定するために十分な TOE の記述をサブシステムの観点から提供するかどうか、及び TSF 内部構造の記述をモジュール(及び、オプションとして上位レベル抽象)の観点から提供するかどうかを決定することである。これは、SFR 実施モジュール及び SFR 支援モジュールの詳細な記述、及び SFR が完全に正確に実装されていることを評価者が決定するために十分な SFR 非干渉モジュールについての情報を提供する。このように、TOE 設計は、実装表現の説明を提供する。

12.8.4.2 入力

891 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) セキュリティアーキテクチャ記述;

d) TOE 設計。

12.8.4.3 適用上の注釈

892 TOE 設計に関して評価者が保証しなければならない 3 つのタイプのアクティビティがある。第 1 に、評価者は、TSF 境界が適切に記述されていることを決定する。第 2 に、評価者は、開発者がこのサブシステムの内容及び提示の要件に適合しており、TOE に対して提供されるその他の証拠資料と一貫している証拠資料を提供したことを決定する。最後に、評価者は、システムがどのように実装されているかを理解し、また、その知識を使用して、機能仕様内の TSFI が適切に記述されること、及びテスト情報が適切に(「ATE クラス: テスト」ワークユニットで行われた) TSF をテストすることを保証するために、(詳細レベルで) SFR 実施モジュールに対して、及び(より低い詳細レベルで) SFR 支援及び SFR 非干渉モジュールに対して提供される設計情報を分析しなければならない。

12.8.4.4 アクション ADV_TDS.4.1E

ADV_TDS.4.1C ***設計は、サブシステムの観点から TOE の構造を記述しなければならない。***

ADV_TDS.4-1 評価者は、TOE 全体の構造がサブシステムの観点から記述されていることを決定するために、TOE 設計を***検査しなければならない。***

893 評価者は、TOE のすべてのサブシステムが識別されていることを保証する。TOE のこの記述は、TSF を構成する TOE の部分が識別されているワークユニット ADV_TDS.4-4 に対する入力として使用される。つまり、この要件は、TSF のみについてのものではなく、TOE 全体についてのものである。

894 TOE (及び TSF)は、抽象の複数の階層(つまり、サブシステム及びモジュール)で記述することができる。TOE の複雑さに応じて、設計は、CC パート 3 附属書の A.4、「ADV_TDS: サブシステム及びモジュール」での記述に従い、サブシステム及びモジュールの観点から記述することができる。「モジュール」レベル(ADV_TDS.4-2 を参照のこと)だけで記述できる非常に簡単な TOE の場合、このワークユニットは該当しないため、満たされているものとみなされる。

895 このアクティビティを実行する際に、評価者は、TOE に対して提示されるその他の証拠(例えば、ST、利用者操作ガイダンス)における TOE の記述が、TOE 設計に含まれる記述と一貫していることを決定するために、このような証拠を検査する。

ADV_TDS.4.2C ***設計は、各モジュールを SFR 実施、SFR 支援、または SFR 非干渉として指示し、モジュールの観点から TSF を記述しなければならない。***

ADV_TDS.4-2 評価者は、TSF 全体がモジュールの観点から記述されてい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。***

896 評価者は、その他のワークユニット内の特定の特性についてモジュールを検査する。このワークユニットでは、評価者は、モジュール記述が TSF の一部だけではなく、TSF 全体を含むことを決定する。評価者は、この決定を行う際に、評価に対して提供されるその他の証拠(例えば、機能仕様、アーキテクチャ記述)を使用する。例えば、機能仕様に TOE 設計記述に記述されるように見えない機能性に対するインタフェースが含まれている場合、TSF の一部が適切に含まれていない可能性がある。この決定は、繰返しプロセスになる可能性があり、その場合、他の証拠について行われる分析の回数が多いほど、証拠資料の完全さに関してより多くの信頼を得ることができる。

897 サブシステムとは異なり、モジュールは、実装表現のレビューに対するガイドとしての役割を果たすことができる詳細レベルで実装を記述する。モジュールの記述は、その記述からのモジュールの実装を作成できるものであるべきであり、その結果の実装は 1) 提示されるインタフェースの観点から実際の TSF 実装と同一であり、2) 設計で言及されるインタフェースの使用において同一であり、そして、3) TSF モジュールの目的の記述と機能的に同等である。例えば、RFC 793 は TCP プロトコルの上位レベル記述を提供する。これは、必ずしも実装には依存していない。これは、豊富な詳細を提供するが、実装固有のものではないため、適切な設計記述ではない。実際の実装は RFC で指定されているプロトコルを追加でき、実装の選択(例えば、実装の様々な部分で、グローバルデータを使用するかまたはローカルデータを使用するか)は実行される分析に対して影響を与える可能性がある。TCP モジュールの設計記述は、(RFC 793 で定義されたインタフェースだけではなく)実装によって提示されるインタフェース、及び TCP を(TSF の一部であったと想定して)実装しているモジュールに関連する処理のアルゴリズム記述をリストする。

ADV_TDS.4-3 評価者は、TSF モジュールは SFR 実施、SFR 支援、または SFR 非干渉として識別されることを決定するために、その TOE 設計を***チェックしなければならない。***

898 (SFR の実施において特定のモジュールが果たす役割に従って)各モジュールを指示することの目的は、開発者がセキュリティ上の役割をほとんど果たさない TSF の一部についての情報をより少なく提供するようにすることである。情報が評価の枠組みの範囲外から収集された場合に発生する可能性があることであるが、要件で要求されるよりも多くの情報または詳細を開発者が提供することは、常に許される。そのような場合でも、開発者は、モジュールを SFR 実施、SFR 支援、または SFR 非干渉として指示しなければならない。

899 これらの指示の正確さは、評価の進行に伴って継続的にレビューされる。実際の場合よりも重要性が低いとする(及び、そのために情報が少なくなること)モジュールの指示の誤りが懸念される。目立った指示の誤りは、すぐに明らかになる可能性がある(例えば、利用者識別(FIA_UID)が、主張されている SFR の 1 つである場合、認証モジュールを SFR 実施以外の任意のものとして指示するなど)が、その他の指示の誤りについては TSF に対する理解が深まるまで発見されない可能性がある。このため、評価者は、これらの指示は開発者の最初で最大の労力を費やす対象であるが、変更されることがあること忘れないようにしなければならない。さらに詳しいガイダンスは、これらの指示の正確さを検査するワークユニット ADV_TDS.4-17 で提供される。

ADV_TDS.4.3C ***設計は、TSF のすべてのサブシステムを識別しなければならない。***

ADV_TDS.4-4 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。***

900 設計がモジュールの観点からだけ提示されている場合、これらの要件のサブシステムはモジュールと同等であり、アクティビティはモジュールレベルで実行されるべきである。

901 ワークユニット ADV_TDS.4-1 では、TOE のすべてのサブシステムが識別され、TSF 以外のサブシステムの特徴が正しく表されていたことが決定された。その作業に基づいて、TSF 以外のサブシステムとして特徴が表されなかったサブシステムは、正確に識別されるべきである。評価者は、準備手続き(AGD_PRE)のガイダンスに従って設置し、構成されたハードウェア及びソフトウェアについて、各サブシステムが TSF の一部またはそれ以外のものとして考慮されていることを決定する。

ADV_TDS.4.4C ***設計は、適切な箇所に対して非形式的で説明的なテキストで補足される、TSF の各サブシステムの準形式的記述を提供しなければならない。***

ADV_TDS.4-5 評価者は、サブシステム、モジュール、及びそれらのインタフェースを記述するのに用いられる準形式的な表記が定義されているのか、あるいは参照されているのかを決定するために、TDS 文書を***検査しなければならない。***

902 準形式的な表記は、スポンサーもしくは参照される該当規格によって定義されうる。評価者は、文章のどの部分において機能やインタフェースが準形式的に記述され、どの表記が使用されているのかを概略する、セキュリティ機能と、それらのインタフェースとのマッピングを提供すべきである。評価者は、すべての使用されている準形式的表記を検査し、それが準形式的なスタイルであることを確認し、TOE に対する準形式的表記の使用方法の妥当性を正当化しなければならない。

903 準形式的表現とは、非形式的表現におこりうる曖昧さを軽減する、明確に定義された構文を持つ標準化された形式により特徴付けられることに留意する。機能仕様で使われるすべての準形式的表記の構文は、定義されるか、もしくは対応する標準を参照しなければならない。評価者は、機能仕様を表現するのに用いられる準形式的表記が、セキュリティに関連した機能を表現することができることを検証する。これを決定するために、評価者は、SFR を参照し、ST に記述される TSF セキュリティ機能と、それに対応する FSP の準形式的表記による記述を比較することができる。

ADV_TDS.4-6 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。***

904 設計がモジュールの観点からだけ提示されている場合、このワークユニットは、次に続くワークユニットで行われる評定によって満たされているものとみなされる。この場合、評価者側での明示的なアクションは必要ない。

905 モジュール記述に加えてTSFのサブシステムレベルの記述を是認するのに十分複雑なシステムでは、サブシステムレベルの記述の目標は、評価者に、次に続くモジュール記述の文脈を提供することである。このため、評価者は、サブシステムレベルの記述が、設計においてセキュリティ機能要件をどのように達成するかの記述を(ただし、モジュール記述の抽象レベルよりは高いレベルで)含んでいることを保証する。この記述は、モジュール記述に合わせて調整されたレベルで使用されるメカニズムを説明するべきである。これは、モジュール記述に含まれている情報を理性的に評定するために必要なロードマップを評価者に提供する。しっかりしたサブシステム記述のセットは、評価者が最も重要な検査対象となるモジュールを決定する、つまり SFR の実施に関して最も関連する TSF の一部に評価アクティビティの焦点を当てるガイドとして役立つ。

906 評価者は、TSF のすべてのサブシステムが記述を持つことを保証する。記述は SFR の実装の実施または支援においてサブシステムが果たす役割に重点を置くべきであるが、SFR 関連の機能性を理解するための文脈が提供されるように、十分な情報を提示しなければならない。

ADV_TDS.4-7 評価者は、サブシステムが SFR 非干渉であることを評価者が決定できるように TSF の各 SFR 非干渉サブシステムが記述されてい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。***

907 設計がモジュールの観点からだけ提示されている場合、このワークユニットは、次に続くワークユニットで行われる評定によって満たされているものとみなされる。この場合、評価者側での明示的なアクションは必要ない。

908 SFR 非干渉サブシステムは、SFR 実施サブシステム及び SFR 支援サブシステムが依存しないサブシステムである。つまり、SFR 非干渉サブシステムは、SFR 機能性の実装において何の役割も果たさない。

909 評価者は、TSF のすべてのサブシステムが記述を持つことを保証する。記述は SFR の実装の実施または支援においてサブシステムが果たさない役割に重点を置くべきであるが、SFR 非干渉の機能性を理解するための文脈が提供されるように、十分な情報を提示しなければならない。

ADV_TDS.4.5C ***設計は、TSF のすべてのサブシステム間の相互作用の記述を提供しなければならない。***

ADV_TDS.4-8 評価者は、TSF のサブシステム間の相互作用が記述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。***

910 設計がモジュールの観点からだけ提示されている場合、このワークユニットは、次に続くワークユニットで行われる評定によって満たされているものとみなされる。この場合、評価者側での明示的なアクションは必要ない。

911 モジュール記述に加えて TSF のサブシステムレベルの記述を是認するのに十分複雑なシステムでは、サブシステム間の相互作用の記述の目標は、TSF がどのように機能を実行するかを読者がよりよく理解できるようにすることである。これらの相互作用は、実装レベル(例えば、1 つのサブシステム内のルーチンから別のサブシステム内のルーチンに渡されるパラメタ、グローバル変数、ハードウェアサブシステムから割り込み処理サブシステムへのハードウェア信号(例えば、割り込み))で特徴を表す必要はないが、別のサブシステムによって使用される特定のサブシステムに対して識別されるデータエレメントは、この説明に含まれる必要がある。サブシステム間(例えば、ファイアウォールシステムの規則のベースの構成に対する責任を持つサブシステムと実際にこれらの規則を実装するサブシステム)の制御関係もすべて記述するべきである。

912 開発者はサブシステム間のすべての相互作用の特徴を表すべきであるが、評価者は記述の完全さを評定する際に独自の判断を使用する必要があることに注意するべきである。相互作用の理由が明確でない場合、または記述されるように見えない(例えば、モジュールレベルの証拠資料の検査中に検出された) SFR 関連の相互作用がある場合、評価者は、この情報が開発者によって提供されることを保証する。ただし、特定のサブシステムのセットの間の相互作用が、開発者によって不完全に記述されていたとしても、完全な記述が TSF によって提供される機能性全体やセキュリティ機能性の理解の助けにならないことを評価者が決定できる場合は、評価者は、記述を十分なものと考えることを選択することができ、そのための完全さを追求しないようにすることができる。

ADV_TDS.4.6C ***設計は、TSF のサブシステムから TSF のモジュールへのマッピングを提供しなければならない。***

ADV_TDS.4-9 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。***

913 設計がモジュールの観点からだけ提示されている場合、このワークユニットは満たされているものとみなされる。

914 モジュール記述に加えて TSF のサブシステムレベルの記述を是認するのに十分複雑な TOE では、開発者はどのように TSF のモジュールがサブシステムに割り当てられているかを示す簡単なマッピングを提供する。これによって、評価者にモジュールレベルの評定を実行する際のガイドが提供される。完全さを決定するために、評価者は、各マッピングを検査し、すべてのサブシステムが少なくともひとつのモジュールにマッピングされ、すべてのモジュールが丁度ひとつのサブシステムにマップされることを決定する。

ADV_TDS.4-10 評価者は、TSF のモジュールに対する TSF のサブシステムとのマッピングが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。***

915 設計がモジュールの観点からだけ提示されている場合、このワークユニットは満たされているものとみなされる。

916 モジュール記述に加えて TSF のサブシステムレベルの記述を是認するのに十分複雑な TOE では、開発者はどのように TSF のモジュールがサブシステムに割り当てられているかを示す簡単なマッピングを提供する。これによって、評価者にモジュールレベルの評定を実行する際のガイドが提供される。評価者は、その他のワークユニットの実行とともにマッピングの正確さをチェックするように選択することができる。「不正確な」マッピングとは、機能がその内部で使用されていないサブシステムにモジュールが間違って関連付けられているマッピングである。マッピングはより詳細な分析をサポートするガイドとなることを想定しているため、評価者は、このワークユニットに対して適切な労力を注ぐように注意すること。マッピングの正確さを検証するための広範な評価者資源を費やす必要はない。このワークユニットまたはその他のワークユニットの一部としてカバーされない設計に関連する誤解を招く不正確さは、このワークユニットに関連付けられ、訂正されるべきである。

ADV_TDS.4.7C ***設計は、目的とその他のモジュールとの関係の観点から各 SFR 実施及び SFR 支援モジュールを記述しなければならない。***

ADV_TDS.11 評価者は、各 SFR 実施モジュール及び SFR 支援モジュールの目的、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。***

917 開発者はモジュールを SFR 実施、SFR 支援及び SFR 非干渉として指示できるが、これらの「タグ」は、開発者が提供する必要がある情報の量と種別を記述するためだけに使用され、もし開発者の工学的プロセスが必要な証拠資料を提供しない場合に開発者が開発する必要のある情報の量を制限するために使用することができる。モジュールが開発者によって分類されているかどうかに関係なく、TOE においてモジュールがそれぞれの役割(SFR 実施など)に対する適切な情報を持つことを決定し、開発者が特定のモジュールに必要な情報を提供するのに失敗した場合に開発者から適切な情報を取得するのは、評価者の責任である。

918 モジュールの目的は、モジュールがどのような機能を満たしているかを示す記述を提供する。評価者はここで注意が必要である。このワークユニットの重点は、SFR の実装が信頼できることについて決定できるようにモジュールがどのように機能するかを評価者が理解できるようにすること、及びADV_ARCサブシステムに対して実行されるアーキテクチャ分析をサポートすることであるべきである。評価者がモジュールの操作、及びその他のモジュールや全体としての TOE との関係について適切に理解している限り、評価者は、達成すべきこの作業の目的を考慮すべきであり、開発者が行う証拠資料の実際的な作業には(例えば、自明の実装表現のための完全なアルゴリズム記述を要求するなどして)関わるべきではない。

919 モジュールは下位レベルにあるため、利用者操作ガイダンス、機能仕様、TSF 内部構造文書、またはセキュリティアーキテクチャ記述、などのその他の証拠資料から完全さ及び正確さの影響を決定するのは困難である可能性がある。ただし、評価者は、機能が正確かつ完全に記述されていることを保証するために役立てることができる範囲で、これらの文書内に提示される情報を使用する。この分析は、機能仕様における TSFI を TSF のモジュールにマッピングする***ADV_TDS.4.10C*** エレメントのワークユニットに対して実行される分析によって、支援が可能である。

ADV_TDS.4.8C ***設計は、各 SFR 実施モジュール及び SFR 支援モジュールの SFR 関連インタフェース、それらのインタフェースからの戻り値、その他のモジュールとの相互作用、及びその他の SFR 実施または SFR 支援モジュールに対して呼び出される SFR 関連インタフェースの観点から各 SFR 実施モジュール及び SFR 支援モジュールを記述しなければならない。***

ADV_TDS.4-12 評価者は、各 SFR 実施モジュール及び SFR 支援モジュールによって提示されるインタフェースの記述に SFR 関連パラメタの正確かつ完全な記述、各インタフェースに対する呼び出し規約、及びインタフェースによって直接戻されるすべての値が含ま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。***

920 モジュールの SFR 関連インタフェースは、提供された SFR 関連操作を呼び出す手段として、及び入力を提供する手段として、またはモジュールからの出力を受け取る手段として、その他のモジュールによって使用されるインタフェースである。これらのインタフェースの特定における目的は、テスト中にこれらのインタフェースの実行を許可することである。SFR 関連でないモジュール間インタフェースは、テストにおける要因ではないため、特定または記述する必要はない。SFR 関連の実行パス(固定された内部パスなど)の通過において要因とならないその他の内部インタフェースも同様である。

921 SFR 支援モジュールの SFR 関連インタフェースは、SFR 実施モジュールから直接または間接的に呼び出されるような、SFR 支援モジュールのすべてのインタフェースである。それらのインタフェースは、そのような呼び出しにおいて使用されるすべてのパラメタを伴い記述される必要がある。これにより、評価者は SFR 実施モジュールの動作の文脈において SFR 支援モジュールを呼び出す目的を理解することができる。

922 SFR 関連インタフェースは、どのように呼び出されるかという観点から、及び戻されるすべての値の観点から記述される。この記述には、パラメタのリスト、及びこれらのパラメタの記述が含まれる。グローバルデータも、呼び出されたときにモジュールによって(入力または出力として)使用される場合に、パラメタとみなされる。パラメタが値のセット(例えば「フラグ」パラメタ)を受け取ることを期待されていた場合、処理しているモジュールに影響を与えるパラメタが受け取る可能性がある値の完全なセットが指定される。同様に、データ構造を表すパラメタは、データ構造の各フィールドが識別及び記述されるように記述される。異なるプログラミング言語は、不明瞭になる可能性がある追加の「インタフェース」を持つ可能性がある。この例として挙げられるのは、C++でオーバロードしている演算子/関数である。クラス記述におけるこの「暗黙のインタフェース」は、下位レベルの TOE 設計の一部としても記述される。モジュールは 1 つのインタフェースのみを提示する可能性があるが、関連するインタフェースの小規模なセットをモジュールが提示することのほうがより一般的である。

923 モジュールに対するパラメタ(入力及び出力)の評定の観点から、グローバルデータのあらゆる使用についても考慮しなければならない。モジュールはデータを読み取るまたは書き込む場合に、グローバルデータを「使用する」。このようなパラメタの記述が(使用される場合に)完全であることを保証するには、評価者は、TOE 設計でモジュールについて提供されるその他の情報(インタフェース、アルゴリズム記述など)、及びワークユニット ADV_TDS.4-12 で評定されるグローバルデータの特定のセットの記述を使用する。例えば、評価者は、最初に提示された機能及びインタフェース(特にインタフェースのパラメタ)を検査することによってモジュールが実行する処理を決定する。次に、評価者は、処理が TDS 設計で識別されている任意のグローバルデータ領域に「触れる」ように見えるかどうかを確認するためのチェックを行うことができる。その後、評価者は、「触れられた」ように見える各グローバルデータ領域について、グローバルデータ領域が、評価者が検査しているモジュールによって入力または出力の手段としてリストされることを決定する。

924 呼び出し規約は、インタフェースを通じてモジュールの機能性を利用するプログラムを作成していた場合に、そのモジュールのインタフェースを正しく呼び出すために使用できるプログラミング参照型の記述である。これには、グローバル変数に関して実行する必要がある任意のセットアップを含む、必要な入力及び出力が含まれる。

925 インタフェースを通じて戻される値は、パラメタまたはメッセージを通じて渡される値、「C」プログラム関数コールの形式で関数コール自体が戻す値、またはグローバルな手段(*ix 形式のオペレーティングシステムにおける特定のエラールーチンなど)を通じて渡される値を参照する。

926 記述が完全であることを保証するには、評価者は、TOE 設計でモジュールについて提供されるその他の情報(例えば、アルゴリズム記述、使用されているグローバルデータ)を使用して、モジュールの機能を実行するために必要なすべてのデータがモジュールに対して提示されているように見えること、及びその他のモジュールによって検査中のモジュールが提供することを期待されている任意の値がそのモジュールによって戻されるものとして識別されることを保証する。評価者は、処理の記述がインタフェースに渡されるもの、またはインタフェースから渡されるものとしてリストされている情報に一致することを保証することによって、正確さを決定する。

ADV_TDS.4.9C ***設計は、目的及びその他のモジュールとの相互作用の観点から各 SFR 非干渉モジュールを記述しなければならない。***

ADV_TDS.4-13 評価者は、SFR 非干渉モジュールが正しく分類されてい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。***

927 ワークユニット ADV_TDS.4-2 で述べたように、SFR 非干渉のモジュールについて要求される情報は、他のものより少ない。このワークユニットに対する評価者の主要な重点は、SFR 非干渉として暗黙の分類が行われた各モジュールに対して提供される証拠、及びモジュールが本当に SFR 非干渉であるかどうかについての評価(TOE 設計におけるその他のモジュールについての情報、TOE 設計、機能仕様、セキュリティアーキテクチャ記述、利用者操作ガイダンス、TSF 内部構造文書、及び場合によっては実装表現までも)から決定を試みることである。この保証のレベルでは、いくつかの誤りは許容されるべきであり、評価者は、指定されたモジュールが SFR 非干渉として分類されているとしても、そうであるかについての絶対的な確証を持つ必要はない。ただし、提供された証拠によって SFR 非干渉モジュールが SFR 実施または SFR 支援であることが示される場合、評価者は、明確な不一致を解決するために開発者からの追加情報を要求する。例えば、モジュール A (SFR 実施モジュール)に対する証拠資料が、モジュール A がモジュール B をコールして特定の種別の構造についてアクセスチェックを実行することを示すものとする。評価者がモジュール B に関連する情報を検査する場合、評価者は、開発者が情報として、目的及び相互作用のセットのみを提供した(このため、モジュール B については SFR 支援もしくは SFR 非干渉として暗黙の分類が行われる)ことを発見する。モジュール A からの目的及び相互作用を検査する場合、評価者はアクセスチェックを実行するモジュール B についての言及がないことを発見し、モジュール A はモジュール B の相互作用の対象となるモジュールとしてリストされない。この時点では、評価者は、モジュール A 及びモジュール B で提供される情報間の不一致を解決することを、開発者に提案するべきである。

928 別の例としては、評価者が ADV_TDS.4.2D によって提供されたようにモジュールに対する TSFI のマッピングを検査する場合がある。この検査は、モジュール C が利用者の識別を必要とする SFR に関連していることを示す。また、評価者がモジュール C に関連する情報を検査する場合、評価者は、開発者が提供した情報のすべては、目的及び相互作用のセットである(このため、モジュール C については SFR 非干渉として暗黙の分類が行われる)ことを発見する。モジュール C に対して提示される目的及び相互作用の検査において、評価者は、利用者の識別に関連して TSFI に対するマッピングとしてリストされるモジュール C が SFR 実施または SFR 支援として分類されない理由を決定することはできない。ここでもまた、評価者は、この不一致を解決することを開発者に提案するべきである。

929 最後の例は、逆の状況について示す。前の例と同様に、開発者は、目的と相互作用のセットで構成されているモジュール D (このため、モジュール D については SFR 非干渉として暗黙の分類が行われる)に関連する情報を提供している。評価者は、モジュール D に対する目的及び相互作用を含む、提供されるすべての証拠を検査する。目的は、相互作用はその記述と一貫しており、モジュール D が SFR 実施または SFR 支援であることを示すものは存在しないという、TOE におけるモジュール D の機能の意味のある記述を提供することのように見える。この場合、評価者は、モジュール D が正しく分類されていることを「単に確認するために」にモジュール D についてのより多くの情報を要求するべきではない。開発者は義務を果たし、モジュール D の暗黙の分類において評価者が持っている保証の結果は(定義によって)この保証レベルに対して適切である。

ADV_TDS.4-14 評価者は、各 SFR 非干渉モジュールの目的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。***

930 モジュールの目的の記述は、モジュールがどのような機能を満たしているかを示す。この記述から、評価者は、モジュールの役割についての包括的な情報を得られるべきである。記述が完全であることを保証するには、評価者は、コールされているモジュールに対する理由がモジュールの目的と一貫しているかどうかを評定するために、その他のモジュールとモジュールとの相互作用について提供される情報を使用する。モジュールの目的からは明らかでない機能性またはモジュールの目的と矛盾する機能性が相互作用の記述に含まれる場合、評価者は、問題が正確さと完全さのどちらの問題であるかを決定する必要がある。評価者は、1 つの文で表現された目的に基づいた意味のある分析は不可能である可能性があるため、短すぎる目的については注意するべきである。

931 モジュールは下位レベルにあるため、利用者操作ガイダンス、機能仕様、セキュリティアーキテクチャ記述、または TSF 内部構造文書などのその他の証拠資料から完全さ及び正確さの影響を決定するのは困難である可能性がある。ただし、評価者は、機能が正確かつ完全に記述されていることを保証するために役立てることができる範囲で、これらの文書内に提示される情報を使用する。この分析は、機能仕様における TSFI を TSF のモジュールにマッピングする ***ADV_TDS.4.10C*** エレメントのワークユニットに対して実行される分析によって、支援が可能である。

ADV_TDS.4-15 評価者は、その他のモジュールと SFR 非干渉モジュールとの相互作用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。***

932 パート 3 要件及びこのワークユニットの観点から、用語「*相互作用*」は*インタフェース*より低い厳密さを伝えることを意図していることに注意することが重要である。相互作用は、実装レベル(例えば、1 つのモジュール内のルーチンから別のモジュール内のルーチンに渡されるパラメタ、グローバル変数、ハードウェアサブシステムから割り込み処理サブシステムへのハードウェア信号(例えば、割り込み))で特徴を表す必要はないが、別のモジュールによって使用される特定のモジュールに対して識別されるデータエレメントは、この説明に含まれるべきである。モジュール間(例えば、ファイアウォールシステムの規則のベースの構成に対する責任を持つモジュールと実際にこれらの規則を実装するモジュール)の制御関係もすべて記述するべきである。

933 その他のモジュールとモジュールとの相互作用は、様々な方法で保存できる。TOE 設計の意図は、評価者が TOE 設計の全体にわたって SFR 支援及び SFR 非干渉モジュールの役割を(部分的には、モジュール相互作用の分析を通じて)理解できるようにすることである。この役割を理解することは、評価者のワークユニット ADV_TDS.4-8 の実行の助けとなる。

934 その他のモジュールとモジュールとの相互作用は、単なるコールツリータイプの文書を超えて行われる。相互作用は、モジュールが他のモジュールと対話する理由の機能的な観点から記述される。モジュールの目的は、モジュールが他のモジュールにどのような機能を提供するかを記述することであり、相互作用は、この機能を達成するために、その他のモジュールからモジュールが依存する対象を記述するべきである。

935 モジュールは下位レベルにあるため、利用者操作ガイダンス、機能仕様、セキュリティアーキテクチャ記述、または TSF 内部構造文書などのその他の証拠資料から完全さ及び正確さの影響を決定するのは困難である可能性がある。ただし、評価者は、相互作用が正確かつ完全に記述されていることを保証するために役立てることができる範囲で、これらの文書内に提示される情報を使用する。

ADV_TDS.4.10C ***マッピングは、すべての TSFI が、それらが呼び出す TOE 設計で記述されているふるまいを追跡することを実証しなければならない。***

ADV_TDS.4-16 評価者は、TOE 設計が、機能仕様で記述されている TSFI から TOE 設計で記述されている TSF のモジュールへの完全で正確なマッピングを含む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。***

936 TOE 設計で記述されているモジュールは、TSF の実装の記述を提供する。TSFI は、実装がどのように実行されるかの記述を提供する。開発者からの証拠は、操作が TSFI で要求される場合に最初に呼び出されるモジュールを識別し、主に機能性の実装に責任のあるモジュールまで呼び出される一連のモジュールを識別する。ただし、各 TSFI に対する完全なコールツリーは、このワークユニットでは必要ではない。複数のモジュールを識別する必要があるのは、入力の条件付けまたは多重入力の分割以外の機能性を持たない「入力点」モジュールまたはラッパーモジュールが存在する場合である。これらのモジュールのいずれかに対するマッピングは、評価者に役立つ情報をまったく提供しない可能性がある。

937 評価者は、すべての TSFI が少なくとも 1 つのモジュールにマッピングされることを保証することによって、マッピングの完全さを評定する。正確さの検証は、より複雑である。

938 正確さの最初の側面は、TSF 境界で各 TSFI がモジュールにマッピングされることである。この決定は、モジュール記述及びそのインタフェース/相互作用をレビューすることによって行うことができる。正確さの次の側面は、識別された最初のモジュールと、主に TSF で提示される機能の実装に責任のあるモジュールとの間のモジュールの連鎖を各 TSFI が識別することである。これは、入力の前処理がどれだけ行われるかによって、最初のモジュールになったり、いくつかのモジュールになったりする可能性がある。TSFI がすべての類似の種別(例えば、システムコール)である場合、前処理のモジュールであることを示す 1 つの指標は、多数の TSFI に対して呼び出されることであることに注意するべきである。正確さの最後の側面は、マッピングが意味を持つことである。例えば、アクセス制御を扱う TSFI を、パスワードをチェックするモジュールにマッピングするのは、正確ではない。評価者は、この決定を行う際に再度判断を使用するべきである。目標は、この情報が、評価者の、SFR のシステム及び実装、及び TSF 境界にあるエンティティが TSF と対話できる方法の理解への助けになることである。SFR がモジュールによって正確に記述されているかどうかについての評定の大半は、他のワークユニットで実行される。

12.8.4.5 アクション ADV_TDS.4.2E

ADV_TDS.4-17 評価者は、すべての ST セキュリティ機能要件が TOE 設計に含まれることを決定するために、TOE セキュリティ機能要件及び TOE 設計を***検査しなければならない。***

939 評価者は、TOE セキュリティ機能要件と TOE 設計の間のマッピングを作成することができる。このマッピングは、機能要件からサブシステムのセットに対して、及びのちに、モジュールに対して、作成される可能性が高い。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、要件のコンポーネントレベルより下、さらにはエレメントレベルより下の詳細さが必要になる場合もあるので注意する必要がある。

940 例えば、FDP_ACC.1 サブセットアクセス制御コンポーネントには、割付を持つエレメントが含まれている。ST で、FDP_ACC.1 サブセットアクセス制御の割付に 10 の規則が含まれていたとして、その 10 の規則が 15 モジュール内の特定の場所に実装された場合、評価者が FDP_ACC.1 サブセットアクセス制御を 1 つのサブシステムにマッピングして、ワークユニットが完了したと主張するのは適切でない。代わりに、評価者は、FDP_ACC.1 サブセットアクセス制御(規則 1)をサブシステム A のモジュール x、y、及び z にマッピングし、FDP_ACC.1 サブセットアクセス制御(規則 2)をサブシステムAの x、p、及び q にマッピングするなどのように、マッピングする可能性がある。

ADV_TDS.4-18 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。***

941 評価者は、TOE セキュリティ機能要件と TOE 設計の間のマッピングを作成することができる。このマッピングは、機能要件からサブシステムのセットに対して、作成される可能性が高い。このマッピングには、機能要件に対して ST 作成者によって実行される操作(割付、詳細化、選択)のために、要件のコンポーネントレベルより下、さらにはエレメントレベルより下の詳細さが必要になる場合もあるので注意する必要がある。

942 例えば、ST 要件が役割によるアクセス制御メカニズムを指定した場合、評価者は、このメカニズムの実装に寄与するサブシステム及びモジュールを最初に識別する。これは、TOE 設計についての深い知識または理解に基づいて、または前のワークユニットで行われた作業によって、行われることがある。この追跡は、サブシステム及びモジュールの識別のためだけに行われるもので、完全な分析ではないことに注意のこと。

943 次のステップは、サブシステムとモジュールが実装するのはどのようなメカニズムであるかを理解することである。例えば、設計が UNIX スタイルの保護ビットに基づいてアクセス制御を記述した場合、その設計は、上記で使用された ST 例で示しているアクセス制御要件の正確な具体化にならない。評価者が、詳細がないためにメカニズムが正確に実装されたことを決定できなかった場合、評価者は、すべての SFR 実施サブシステムとモジュールが識別されたかどうか、または適切な詳細がそれらのサブシステムとモジュールに提供されたかどうかを評定することが必要になる。

12.8.5 サブアクティビティの評価(ADV_TDS.5)

944 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

12.8.6 サブアクティビティの評価(ADV_TDS.6)

945 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

13 AGD クラス: ガイダンス文書

13.1 序説

946 ガイダンス文書アクティビティの目的は、利用者がセキュアな方法で TOE をどのように扱うことができるかを記述している証拠資料の適切性を判断することである。そのような証拠資料は、正しくないアクションが TOE のセキュリティまたは自分のデータのセキュリティに悪影響を与える可能性がある様々なタイプの利用者(例えば、TOE の受入れ、設置、管理、または運用を行う利用者)を考慮するべきである。

947 ガイダンス文書クラスは、第 1 に準備手続き(配付された TOE を、ST に記述された環境に評価構成を移行するために実行する必要があるすべての操作、つまり TOE の受入れと設置)に関するファミリ、第 2 に利用者操作ガイダンス(評価構成で TOE の運用中に実行する必要があるすべての操作、つまり運用と管理)に関するファミリの 2 つのファミリに分割される。

13.2 適用上の注釈

948 ガイダンス文書アクティビティは、TOE のセキュリティに関係する機能とインタフェースに適用される。TOE のセキュアな構成は、ST に記述されている。

13.3 利用者操作ガイダンス(AGD_OPE)

13.3.1 サブアクティビティの評価(AGD_OPE.1)

13.3.1.1 目的

949 このサブアクティビティの目的は、利用者ガイダンスが、TSF により提供されたセキュリティ機能性とインタフェースについて利用者の役割ごとに記述しているかどうか、TOE のセキュアな使用のための指示とガイドラインを提供しているかどうか、操作のすべてのモードに対してセキュアな手続きを取り扱っているかどうか、TOE のセキュアでない状態を容易に阻止及び検出することができるかどうかを決定すること、またはガイダンスが誤解を招いたり、不合理であったりするかどうかを決定することである。

13.3.1.2 入力

950 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計(適用可能な場合);

d) 利用者ガイダンス;

13.3.1.3 アクション AGD_OPE.1.1E

AGD_OPE.1.1C ***利用者操作ガイダンスは、適切な警告を含め、セキュアな処理環境で管理するべき、利用者がアクセス可能な機能と権限について、利用者の役割ごとに記述しなければならない。***

AGD_OPE.1-1 評価者は、利用者操作ガイダンスが、適切な警告を含め、セキュアな処理環境で管理するべき、利用者がアクセス可能な機能と権限について利用者の役割ごとに記述していることを決定するために、そのガイダンスを***検査しなければならない。***

951 TOE の構成は、TOE の異なる機能を使用するための異なる権限を持つことを異なる利用者の役割に許すことができる。これは、ある利用者にはある種の機能を実行することが許可されるが、他の利用者にはそれが許可されないことを意味する。これらの機能と権限は、利用者ガイダンスで、利用者の役割ごとに記述されるべきである。

952 利用者ガイダンスでは、管理する必要がある機能と権限、それらに必要となるコマンドのタイプ、及びそのようなコマンドの理由を利用者の役割ごとに識別する。利用者ガイダンスには、これらの機能と権限の使用に関する警告を含めるべきである。警告では、期待される効果、考えられる 2 次的効果、他の機能と権限との考えられる相互作用を指摘するべきである。

AGD_OPE.1.2C ***利用者操作ガイダンスは、TOE により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを利用者の役割ごとに記述しなければならない。***

AGD_OPE.1-2 評価者は、利用者操作ガイダンスが TOE により提供された利用可能なインタフェースのセキュアな使用法を利用者の役割ごとに記述していることを決定するために、そのガイダンスを***検査しなければならない。***

953 利用者ガイダンスでは、TSF の効果的な使用に関するアドバイス(例えば、パスワード構成方法のレビュー、利用者ファイルバックアップの望ましい頻度、利用者アクセス権限を変更したときの影響の説明)を提供するべきである。

AGD_OPE.1.3C ***利用者操作ガイダンスは、利用可能な機能とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、必要に応じてセキュアな値を示し、利用者の役割ごとに記述しなければならない。***

AGD_OPE.1-3 評価者は、利用者操作ガイダンスが、利用可能なセキュリティ機能性とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、適切にセキュアな値を示して、利用者の役割ごとに記述していることを決定するために、そのガイダンスを***検査しなければならない。***

954 利用者ガイダンスには、利用者インタフェースで認識できるセキュリティ機能性の概要を含めるべきである。

955 利用者ガイダンスは、セキュリティインタフェースと機能性の目的、ふるまい、及び相互関係を識別し、記述するべきである。

956 利用者がアクセスできる各インタフェースに対して、利用者ガイダンスでは、次のことを行うべきである:

a) インタフェースを起動する方法を記述する(例えば、コマンド行、プログラミング言語システムコール、メニュー選択、コマンドボタン);

b) 利用者によって設定されるパラメタ、それらのパラメタの特定の目的、正当な値とデフォルトの値、そのようなパラメタのセキュア及びセキュアでない、個別または組み合わせによる、使用設定を記述する;

c) 即時 TSF 応答、メッセージ、またはリターンコードを記述する。

957 評価者は、機能仕様及び ST に記述されている TSF が利用者操作ガイダンスと一貫していることを決定するために、これらの文書を考慮するべきである。評価者は、人間の利用者のすべてのタイプが利用可能な TSFI を通して、セキュアな使用を可能にするために、利用者操作ガイダンスが完全であることを保証する必要がある。評価者は、補足的に、ガイダンスとこれらの文書の間の非形式的マッピングを準備することができる。このマッピングからの欠落はいずれも、不完全性を示す。

AGD_OPE.1.4C ***利用者操作ガイダンスは、TSF の制御下にあるエンティティのセキュリティ特性の変更を含む、利用者がアクセス可能で実行が必要な機能に関連するセキュリティ関連事象の各タイプについて、利用者の役割ごとに明確に提示しなければならない。***

AGD_OPE.1-4 評価者は、利用者操作ガイダンスが、TSF の制御下にあるエンティティに関するセキュリティ特質の変更、及び障害や操作誤りの後の操作を含む、実行が必要な利用者機能に関連するセキュリティ関連事象の各タイプを利用者の役割ごとに記述していることを決定するために、そのガイダンスを***検査しなければならない。***

958 セキュリティ関連事象のすべてのタイプは、発生する可能性がある事象とセキュリティを維持するために各利用者が取る必要があるアクション(存在する場合)を各利用者がわかるように、利用者の役割ごとに詳細に記述されている。TOE の運用中に発生するセキュリティ関連事象(例えば、監査証跡のオーバフロー、システム故障、利用者レコードの更新、利用者が組織を離れるときの利用者アカウントの削除)は、利用者がセキュアな運用を維持するために介入できるように適切に定義される。

AGD_OPE.1.5C ***利用者操作ガイダンスは、TOE の操作のすべての可能なモード(障害や操作誤りの後の操作を含む)、それらの結果、及びセキュアな運用を維持するために必要なことを識別しなければならない。***

AGD_OPE.1-5 評価者は、利用者操作ガイダンスが TOE の操作のすべての可能なモード(必要に応じて、障害または操作誤りの後の操作を含む)、それらの結果及びセキュアな運用を維持するために必要なことを識別していることを決定するために、そのガイダンスとその他の評価証拠を***検査しなければならない。***

959 その他の評価証拠、特に機能仕様は、評価者がガイダンスに十分なガイダンス情報が含まれていることを決定するために使用するべき情報源を提供する。

960 テスト証拠資料が保証パッケージに含まれている場合、この証拠で提供された情報は、ガイダンスに十分なガイダンス証拠資料が含まれていることを決定するためにも使用できる。テストステップで提供された詳細は、提供されたガイダンスが TOE の使用と管理に十分であることを確認するために使用できる。

961 評価者は、人間に見える TSFI をセキュアに使用するためのガイダンスとその他の評価証拠を比較し、TSFI に関係するガイダンスがその TSFI のセキュアな使用(すなわち、SFR と一貫している)に十分であることを決定するために、一度に 1 つずつ TSFI に焦点をあてるべきである。評価者は、考えられる不一致を探索してインタフェースの間の関係も考慮するべきである。

AGD_OPE.1.6C ***利用者操作ガイダンスは、ST に記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を、利用者の役割ごとに記述しなければならない。***

AGD_OPE.1-6 評価者は、利用者操作ガイダンスが、ST に記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を、利用者の役割ごとに記述していることを決定するために、そのガイダンスを***検査しなければならない。***

962 評価者は、ST の運用環境のセキュリティ対策方針を分析し、利用者ガイダンスに、関連するセキュリティ手段が利用者の役割ごとに適切に記述されていることを決定する。

963 利用者ガイダンスに記述されるセキュリティ手段には、手続き的、物理的、人的及び接続性の側面に関するすべての外部の手段を含めるべきである。

964 TOE のセキュアな設置に関連する手段は、準備手続き(AGD_PRE)で検査されることに注意のこと。

AGD_OPE.1.7C ***利用者操作ガイダンスは、明確で、合理的なものでなければならない。***

AGD_OPE.1-7 評価者は、利用者操作ガイダンスが明確であることを決定するために、そのガイダンスを***検査しなければならない。***

965 ガイダンスは、管理者または利用者により誤って解釈され、TOE または TOE が提供するセキュリティに有害な方法で使用される場合、不明確である。

AGD_OPE.1-8 評価者は、利用者操作ガイダンスが合理的であることを決定するために、そのガイダンスを***検査しなければならない。***

966 ガイダンスが ST と一貫していない、またはセキュリティの維持が過度に負担の大きい TOE の使用または運用環境を要求する場合、ガイダンスは合理的でない。

13.4 準備手続き(AGD_PRE)

13.4.1 サブアクティビティの評価(AGD_PRE.1)

13.4.1.1 目的

967 このサブアクティビティの目的は、TOE のセキュアな準備のための手続きとステップが証拠資料として提出され、その結果、セキュアな構成となるかどうかを決定することである。

13.4.1.2 入力

968 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 準備手続きを含む TOE;

c) 開発者の配付手続きの記述(適用可能な場合);

13.4.1.3 適用上の注釈

969 準備手続きは、ST の記述のように TOE をセキュアな構成にするために必要な、すべての受入れと設置の手続きについて言及する。

13.4.1.4 アクション AGD_PRE.1.1E

AGD_PRE.1.1C ***準備手続きは、開発者の配付手続きに従って配付された TOE のセキュアな受入れに必要なすべてのステップを記述しなければならない。***

AGD_PRE.1-1 評価者は、提供された受入れ手続きに、開発者の配付手続きに従った TOE のセキュアな受入れに必要なステップが記述されていることを決定するために、その手続きを***検査しなければならない。***

970 開発者の配付手続きによって、受入れ手続きが適用されること、または適用できることが予期されない場合は、このワークユニットは該当しないため、満たされているものとみなされる。

971 受入れ手続きには、少なくとも、ST に示されるように TOE のすべての部分が正しいバージョンで配付されたことを利用者がチェックする必要があることを含めるべきである。

972 受入れ手続きには、開発者の配付手続きで暗示されている配付された TOE を受け入れるために利用者が実行する必要があるステップを反映するべきである。

973 受入れ手続きは、適用可能な場合は、以下についての詳細情報を提供するべきである:

a) 配付された TOE が完全に評価されたものであることの確認;

b) 配付された TOE の改変/なりすましの検出。

AGD_PRE.1.2C ***準備手続きには、TOE のセキュアな設置、及び ST に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述しなければならない。***

AGD_PRE.1-2 評価者は、提供された設置手続きに、TOE のセキュアな設置、及び ST のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なステップが記述されていることを決定するために、その手続きを***検査しなければならない。***

974 設置手続きが適用されること、または適用できることが予期されない場合(例えば、TOE が運用状態ですでに配付されているため)、このワークユニットは該当しないため、満たされているものとみなされる。

975 設置手続きは、適用可能な場合は、次の項目についての詳細情報を提供するべきである:

a) セキュアな設置のための最小限のシステム要件;

b) ST によって提供されたセキュリティ対策方針に従った運用環境の要件;

c) 利用者が、評価済み構成相当の運用 TOE を得るために実行しなければならないステップ。このような記述は、各ステップに、現在のステップの成功、失敗、もしくは問題かにより、次のステップを決定する明確な方法を含まなければならない;

d) TSF 制御下のエンティティに関する設置固有のセキュリティ特性(例えば、パラメタ、設定、パスワード)の変更;

e) 例外及び問題の取り扱い。

13.4.1.5 **アクション** AGD_PRE.1.2E

AGD_PRE.1-3 評価者は、提供された準備手続きだけを使用して TOE とその運用環境をセキュアに準備できることを決定するために、TOE の準備に必要なすべての利用者手続きを***実行しなければならない。***

976 準備では、評価者が、TOE を配付可能な状態から、TOE の受入れと設置を含め運用可能であり、ST で特定されている TOE のセキュリティ対策方針と一貫する SFR を実施する状態に進めることを要求する。

977 評価者は、開発者の手続きだけに従うべきであり、提供された準備手続きだけを使用して、顧客が TOE の受入れと設置のために通常実行することが予期されるアクティビティを実行することができる。それらのことを行うときに直面する困難はいずれも、ガイダンスが不完全である、明確でない、または不合理であることを示す。

978 このワークユニットは、独立テスト(ATE_IND)のもとで評価アクティビティとともに実行することができる。

979 統合 TOE 評価に対する依存コンポーネントとして TOE が使用されることが判明している場合、評価者は、統合 TOE で使用される基本コンポーネントによって運用環境が満たされていることを保証するべきである。

14 ALC クラス: ライフサイクルサポート

14.1 序説

980 ライフサイクルサポートアクティビティの目的は、開発者が TOE の開発から保守に使用する手続きの適切性を決定することである。これらの手続きには、開発者が使用するライフサイクルモデル、構成管理、TOE の開発の全期間で使用されるセキュリティ手段、TOE のライフサイクルを通して開発者が使用するツール、セキュリティ欠陥の扱い、及び配付アクティビティが含まれる。

981 TOE の不十分な制御の開発と保守の結果、実装に脆弱性がもたらされることがある。定義されたライフサイクルモデルに従うことは、この領域の制御を改善するのに役に立つ。TOE に対して使用される測定可能なライフサイクルモデルは、TOE の開発の進行を評定する際に曖昧さを除去できる。

982 構成管理アクティビティの目的は、消費者が評価済み TOE を識別するのを手助けすること、構成要素が一意に識別されていることを保証すること、及び TOE に対して行われる変更を管理し追跡するために、開発者によって使用される手続きの適切性を保証することである。これには、どんな変更が追跡されるか、どのように起こり得る変更が具体化されるか、そして誤りの範囲を減らすために使用される自動化の程度についての詳細を含む。

983 開発者セキュリティ手続きは、TOE 及びそれに関係する設計情報を干渉または暴露から保護することを意図している。開発プロセスへの干渉は、脆弱性の意図的な持ち込みをもたらすことがある。設計情報の暴露は、脆弱性のさらに容易な悪用を可能にする。手続きの適切性は、TOE の本質と開発プロセスに依存する。

984 開発者及び開発プロセスに関係した第三者による、明確に定義された開発ツールの使用及び実装標準の適用は、詳細化に脆弱性が意図せずに持ち込まれないようにするのに役に立つ。

985 欠陥修正アクティビティは、セキュリティ欠陥を追跡すること、訂正アクションを識別すること、及び TOE 利用者に対して訂正アクション情報を配付することを意図している。

986 配付アクティビティの目的は、TOE が消費者に対して改変されることなく配付されていることを保証するために使用される手続きの証拠資料の適切性を判断することである。

14.2 CM 能力(ALC_CMC)

14.2.1 サブアクティビティの評価(ALC_CMC.1)

14.2.1.1 目的

987 このサブアクティビティの目的は、開発者が TOE を明確に識別しているかどうかを決定することである。

14.2.1.2 入力

988 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) テストに適した TOE。

14.2.1.3 アクション ALC_CMC.1.1E

ALC_CMC.1.1C ***TOE は、その一意の参照でラベル付けされなければならない。***

ALC_CMC.1-1 評価者は、評価のために提供された TOE がその参照でラベル付けされていることを***チェックしなければならない。***

989 評価者は、ST で述べられている一意の参照が TOE に含まれていることを保証するべきである。これは、ラベルの付いたパッケージまたは媒体、または運用可能 TOE が表示するラベルによって行うことができる。これは、消費者が(例えば、購入または使用時に) TOE を識別できるようにするものである。

990 TOE は、TOE を簡単に識別する方法を提供することができる。例えば、ソフトウェア TOE は、立上げルーチンの間に、またはコマンド行の入力に対応して TOE の名前とバージョン番号を表示することができる。ハードウェアまたはファームウェア TOE は、TOE に物理的に刻印されている部品番号により識別することができる。

991 また、TOE に対して提供された一意の参照は、TOE を構成する各コンポーネントの一意の参照の組み合わせである可能性がある(例えば、統合 TOE である場合)。

ALC_CMC.1-2 評価者は、使用されている TOE 参照が一貫していることを***チェックしなければならない。***

992 もし、TOE に 2 度以上ラベルが付けられているならば、ラベルは一貫している必要がある。例えば、TOE の一部として提供されるラベルの付いたガイダンス証拠資料を、評価される運用可能 TOE に関係付けることができるべきである。これにより消費者は、TOE の評価済みバージョンを購入したこと、このバージョンを設置したこと、ST に従って TOE を運用するためのガイダンスの正しいバージョンを所有していることを確信できる。

993 評価者は、TOE 参照が ST と一貫性があることも検証する。

994 このワークユニットが統合 TOE に適用される場合、以下のものが適用される。統合 IT の TOE は一意の(複合)参照でラベル付けされないが、個別のコンポーネントのみは適切な TOE 参照でラベル付けされる。立上げ及び/または運用中など、その IT の TOE に対するさらなる開発では、複合参照でラベル付けされる必要がある場合がある。統合 TOE が構成コンポーネント TOE として配付される場合、配付された TOE 要素には複合参照が含まれない。ただし、統合 TOE の ST は、統合 TOE に対する一意の参照を含み、統合 TOE を構成するコンポーネントを識別する。消費者は、これにより、適切な要素が含まれているかどうかを決定することができる。

14.2.2 サブアクティビティの評価(ALC_CMC.2)

14.2.2.1 目的

995 このサブアクティビティの目的は、開発者がすべての構成要素を一意に識別する CM システムを使用するかどうかを決定することである。

14.2.2.2 入力

996 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) テストに適した TOE;

c) 構成管理証拠資料。

14.2.2.3 適用上の注釈

997 このコンポーネントには、CM システムが使用されていることを決定するための暗黙の評価者アクションが含まれる。ここでの要件は、TOE の識別と構成リストの提供に限られるため、このアクションは、既存のワークユニットですでに扱われ、かつ既存のワークユニットの範囲に限られている。サブアクティビティの評価(ALC_CMC.3)での要件は、これら 2 つの要素を超えて拡大され、運用のより明示的な証拠が必要となる。

14.2.2.4 アクション ALC_CMC.2.1E

ALC_CMC.2.1C ***TOE は、その一意の参照でラベル付けされなければならない。***

ALC_CMC.2-1 評価者は、評価のために提供された TOE がその参照でラベル付けされていることを***チェックしなければならない。***

998 評価者は、ST で述べられている一意の参照が TOE に含まれていることを保証するべきである。これは、ラベルの付いたパッケージまたは媒体、または運用可能 TOE が表示するラベルによって行うことができる。これは、消費者が(例えば、購入または使用時に) TOE を識別できるようにするものである。

999 TOE は、TOE を簡単に識別する方法を提供することができる。例えば、ソフトウェア TOE は、立上げルーチンの間に、またはコマンド行の入力に対応して TOE の名前とバージョン番号を表示することができる。ハードウェアまたはファームウェア TOE は、TOE に物理的に刻印されている部品番号により識別することができる。

1000 また、TOE に対して提供された一意の参照は、TOE を構成する各コンポーネントの一意の参照の組み合わせである可能性がある(例えば、統合 TOE である場合)。

ALC_CMC.2-2 評価者は、使用されている TOE 参照が一貫していることを***チェックしなければならない。***

1001 もし、TOE に 2 度以上ラベルが付けられているならば、ラベルは一貫している必要がある。例えば、TOE の一部として提供されるラベルの付いたガイダンス証拠資料を、評価される運用可能 TOE に関係付けることができるべきである。これにより消費者は、TOE の評価済みバージョンを購入したこと、このバージョンを設置したこと、ST に従って TOE を運用するためのガイダンスの正しいバージョンを所有していることを確信できる。

1002 評価者は、TOE 参照が ST と一貫性があることも検証する。

1003 このワークユニットが統合 TOE に適用される場合、以下のものが適用される。統合 IT の TOE は一意の(複合)参照でラベル付けされないが、個別のコンポーネントのみは適切な TOE 参照でラベル付けされる。立上げ及び/または運用中など、その IT の TOE に対するさらなる開発では、複合参照でラベル付けされる必要がある場合がある。統合 TOE が構成コンポーネント TOE として配付される場合、配付された TOE 要素には複合参照が含まれない。ただし、統合 TOE の ST は、統合 TOE に対する一意の参照を含み、統合 TOE を構成するコンポーネントを識別する。消費者は、これにより、適切な要素が含まれているかどうかを決定することができる。

ALC_CMC.2.2C ***CM 証拠資料は、構成要素を一意に識別する方法を記述しなければならない。***

ALC_CMC.2-3 評価者は、構成要素の識別方式が、どのように構成要素が一意に識別されるかを記述していることを決定するために、その識別方式を***検査しなければならない。***

1004 手続きは、TOE のライフサイクルを通して各構成要素のステータスをどのように追跡できるかを記述するべきである。手続きは、CM 計画で、または CM 証拠資料の全体を通して、詳述することができる。含まれる情報では、次の内容を記述するべきである:

a) 同じ構成要素のバージョンを追跡できるように、各構成要素を一意に識別する方法;

b) 構成要素に一意の識別情報が割り付けられる方法、及び CM システムにそれらの情報が入力される方法;

c) 構成要素の過去のバージョンを識別するために使用される方法。

ALC_CMC.2.3C ***CM システムは、すべての構成要素を一意に識別しなければならない。***

ALC_CMC.2-4 評価者は、CM 証拠資料と一貫した方法で構成要素が識別されていることを決定するために構成要素を***検査しなければならない。***

1005 CM システムが、すべての構成要素を一意に識別するという保証は、構成要素の識別情報を検査することによって得られる。TOE を構成する構成要素、及び開発者が評価証拠として提出する構成要素に関するドラフトの両方について、評価者は、各構成要素が CM 証拠資料に記述されている一意の識別方法と一致するやり方で、一意の識別を持っていることを確認する。

14.2.3 サブアクティビティの評価(ALC_CMC.3)

14.2.3.1 目的

1006 このサブアクティビティの目的は、すべての構成要素を一意に識別する CM システムを開発者が使用するかどうか、及びこれらの要素を改変する能力が適切に制御されているかどうかを決定することである。

14.2.3.2 **入力**

1007 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) テストに適した TOE;

c) 構成管理証拠資料。

14.2.3.3 **アクション** ALC_CMC.3.1E

ALC_CMC.3.1C ***TOE は、その一意の参照でラベル付けされなければならない。***

ALC_CMC.3-1 評価者は、評価のために提供された TOE がその参照でラベル付けされていることを***チェックしなければならない。***

1008 評価者は、ST で述べられている一意の参照が TOE に含まれていることを保証するべきである。これは、ラベルの付いたパッケージまたは媒体、または運用可能 TOE が表示するラベルによって行うことができる。これは、消費者が(例えば、購入または使用時に) TOE を識別できるようにするものである。

1009 TOE は、TOE を簡単に識別する方法を提供することができる。例えば、ソフトウェア TOE は、立上げルーチンの間に、またはコマンド行の入力に対応して TOE の名前とバージョン番号を表示することができる。ハードウェアまたはファームウェア TOE は、TOE に物理的に刻印されている部品番号により識別することができる。

1010 また、TOE に対して提供された一意の参照は、TOE を構成する各コンポーネントの一意の参照の組み合わせである可能性がある(例えば、統合 TOE である場合)。

ALC_CMC.3-2 評価者は、使用されている TOE 参照が一貫していることを***チェックしなければならない。***

1011 もし、TOE に 2 度以上ラベルが付けられているならば、ラベルは一貫している必要がある。例えば、TOE の一部として提供されるラベルの付いたガイダンス証拠資料を、評価される運用可能 TOE に関係付けることができるべきである。これにより消費者は、TOE の評価済みバージョンを購入したこと、このバージョンを設置したこと、ST に従って TOE を運用するためのガイダンスの正しいバージョンを所有していることを確信できる。

1012 評価者は、TOE 参照が ST と一貫性があることも検証する。

1013 このワークユニットが統合 TOE に適用される場合、以下のものが適用される。統合 IT の TOE は一意の(複合)参照でラベル付けされないが、個別のコンポーネントのみは適切な TOE 参照でラベル付けされる。立上げ及び/または運用中など、その IT の TOE に対するさらなる開発では、複合参照でラベル付けされる必要がある場合がある。統合 TOE が構成コンポーネント TOE として配付される場合、配付された TOE 要素には複合参照が含まれない。ただし、統合 TOE の ST は、統合 TOE に対する一意の参照を含み、統合 TOE を構成するコンポーネントを識別する。消費者は、これにより、適切な要素が含まれているかどうかを決定することができる。

ALC_CMC.3.2C ***CM 証拠資料は、構成要素を一意に識別する方法を記述しなければならない。***

ALC_CMC.3-3 評価者は、構成要素の識別方式が、どのように構成要素が一意に識別されるかを記述していることを決定するために、その識別方式を***検査しなければならない。***

1014 手続きは、TOE のライフサイクルを通して各構成要素のステータスをどのように追跡できるかを記述するべきである。手続きは、CM 計画で、または CM 証拠資料の全体を通して、詳述することができる。含まれる情報では、次の内容を記述するべきである:

a) 同じ構成要素のバージョンを追跡できるように、各構成要素を一意に識別する方法;

b) 構成要素に一意の識別情報が割り付けられる方法、及び CM システムにそれらの情報が入力される方法;

c) 構成要素の過去のバージョンを識別するために使用される方法。

ALC_CMC.3.3C ***CM システムは、すべての構成要素を一意に識別しなければならない。***

ALC_CMC.3-4 評価者は、CM 証拠資料と一貫した方法で構成要素が識別されていることを決定するために構成要素を***検査しなければならない。***

1015 CM システムが、すべての構成要素を一意に識別するという保証は、構成要素の識別情報を検査することによって得られる。TOE を構成する構成要素、及び開発者が評価証拠として提出する構成要素に関するドラフトの両方について、評価者は、各構成要素が CM 証拠資料に記述されている一意の識別方法と一致するやり方で、一意の識別を持っていることを確認する。

ALC_CMC.3.4C ***CM システムは、許可された変更のみが構成要素に対して行われる手段を提供しなければならない。***

ALC_CMC.3-5 評価者は、CM アクセス制御手段が、構成要素への許可されない不当なアクセスを阻止するのに有効であることを決定するために、CM 計画に記述されているそのアクセス制御手段を***検査しなければならない。***

1016 評価者は、多数の方法を使用して CM アクセス制御手段が有効であることを決定することができる。例えば、評価者は、アクセス制御手段を実行して、手続きがバイパスされないことを保証することができる。評価者は、***ALC_CMC.3.8C*** が要求する CM システム手続きによって生成される出力を使用することができる。評価者は、採用されているアクセス制御手段が有効に機能していることを保証するために、CM システムの実証に立ち会うこともできる。

ALC_CMC.3.5C ***CM 証拠資料は、CM 計画を含まなければならない。***

ALC_CMC.3-6 評価者は、提供された CM 証拠資料が CM 計画を含んでいることを***チェックしなければならない。***

1017 CM 計画は1つの文書にまとめられる必要はないが、しかしどこで CM 計画の様々な箇所を検出できるのかを記述する別個の文書が存在することが推奨される。もし CM 計画が複数の文書により提供されるならば、次のワークユニットのリストは、要求される内容に関するガイダンスを提供する。

ALC_CMC.3.6C ***CM 計画は、TOE の開発に対して CM システムがどのように使用されるかを記述しなければならない。***

ALC_CMC.3-7 評価者は、CM 計画が、TOE の開発のために CM システムがどのように使用されるかを記述していることを決定するために、その計画を***検査しなければならない。***

1018 CM 計画には、適用できる場合、次の記述が含まれる:

a) 構成管理手続きに従う TOE 開発で行われるすべてのアクティビティ(例えば、構成要素の作成、改変または削除、データバックアップ、アーカイブ);

b) 使用可能にする必要がある手段(例えば、CM ツール、用紙);

c) CM ツールの利用法: TOE の完全性を維持するために CM システムの利用者が CM ツールを正しく操作するために必要な詳細;

d) CM 制御下にあるその他のオブジェクト(開発コンポーネント、ツール、評定環境など);

e) 個々の構成要素を操作するために必要な個人の役割と責任(異なる役割を異なる種別の構成要素(例えば、設計証拠資料またはソースコード)に識別することができる);

f) CM の実体(例えば、変更管理組織、インタフェース管理作業グループ)がどのように導入され、担当者が配置されるか;

g) 変更管理の記述;

h) 許可された個人だけが構成要素を変更できるよう保証するために使用される手続き;

i) 構成要素への同時変更の結果として、同時性の問題が発生しないよう保証するために使用される手続き;

j) 手続きを適用した結果として生成される証拠。例えば、構成要素の変更に対して、CM システムは、変更の記述、変更の責任、影響を受けるすべての構成要素の識別、ステータス(例えば、保留または完了)、及び変更の日付と時刻を記録する。これは、行われた変更の監査証跡または変更管理記録に記録される;

k) TOE バージョンのバージョン管理及び一意に参照するための手法(例えば、オペレーティングシステムでのパッチのリリースの扱い、及びその後のそれらの適用の検出)。

ALC_CMC.3.7C ***証拠は、すべての構成要素が CM システム下で維持されていることを実証しなければならない。***

ALC_CMC.3-8 評価者は、構成リストに識別されている構成要素が CM システムによって維持されていることを***チェックしなければならない。***

1019 開発者が採用する CM システムは、TOE の完全性を維持するべきである。評価者は、構成リストに含まれている各種別の構成要素(例えば、設計文書またはソースコードモジュール)に対して、CM 計画に記述されている手続きによって生成された証拠の例が存在することをチェックするべきである。この場合、サンプリング手法は、CM 要素を制御するために CM システムで使用される粒度レベルによって決まる。例えば、10,000 ソースコードモジュールが構成リストに識別されている場合、それが 5 つまたはただ 1 つ存在する場合とは異なるサンプリング方策が適用される必要がある。このアクティビティで重視することは、小さな誤りを検出することではなく、CM システムが正しく運用されていることを保証するべきである。

1020 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

ALC_CMC.3.8C ***CM システムが、CM 計画に従って機能していることを証拠により実証しなければならない。***

ALC_CMC.3-9 評価者は、CM 証拠資料が、CM 計画が識別している CM システムの記録を含んでいることを確かめるために、その証拠資料を*チェックしなければならない。*

1021 CM システムが作り出す出力は、CM 計画が適用されていること、及びすべての構成要素が ***ALC_CMC.3.7C*** が要求するように、CM システムによって維持されていることを評価者が確信するために必要とする証拠を提供するべきである。出力例には、変更管理用紙、または構成要素アクセス許可用紙を含めることができる。

ALC_CMC.3-10 評価者は、CM システムが CM 計画に従って運用されていることを決定するために、証拠を*検査しなければならない。*

1022 評価者は、CM システムのすべての操作が、証拠資料として提出された手続きに従って行われていることを確認するために、構成要素に対し実行された各種別の CM 関連操作(例えば、作成、改変、削除、前のバージョンへの復帰)をカバーする証拠のサンプルを選択して検査するべきである。評価者は、証拠が CM 計画のその操作に識別されている情報のすべてを含んでいることを確認する。証拠を検査するためには、使用されている CM ツールにアクセスする必要がある場合がある。評価者は、証拠をサンプリングすることを選択できる。

1023 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

1024 CM システムが正しく運用されていることと構成要素が有効に維持されていることのさらなる信頼は、選ばれた開発スタッフとのインタビューの手段によって確証することができる。そのようなインタビューを行うとき、評価者は、CM 手続きが CM 証拠資料に記述されているとおりに適用されていることを確認するのに加え、CM システムが実際にどのように使用されているかを深く理解することを目的とする。そのようなインタビューは、記録による証拠の検査を補足するものであり、それらを置き換えるものではないことに注意するべきである。また、記録による証拠だけで要件が満たされる場合、それらは不要である。しかしながら、CM 計画の範囲が広い場合、いくつかの局面(例えば、役割と責任)が CM 計画と記録だけからは明確でない場合がある。これもインタビューによる明確化が必要となるひとつのケースである。

1025 評価者がこのアクティビティを確証するために開発サイトを訪問することが予想される。

1026 サイト訪問のガイダンスについては、A.4、「サイト訪問」を参照のこと。

14.2.4 サブアクティビティの評価(ALC_CMC.4)

14.2.4.1 目的

1027 このサブアクティビティの目的は、開発者が TOE 及びそれに関係する構成要素を明確に識別しているかどうかを、及び CM システムが人為的誤りまたは怠慢による影響を受けないように、自動化ツールによりこれらの要素を改変する能力が適切に制御されているかどうかを決定することである。

14.2.4.2 入力

1028 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) テストに適した TOE;

c) 構成管理証拠資料。

14.2.4.3 アクション ALC_CMC.4.1E

ALC_CMC.4.1C ***TOE は、その一意の参照でラベル付けされなければならない。***

ALC_CMC.4-1 評価者は、評価のために提供されたTOEがその参照でラベル付けされていることを***チェックしなければならない。***

1029 評価者は、ST で述べられている一意の参照が TOE に含まれていることを保証するべきである。これは、ラベルの付いたパッケージまたは媒体、または運用可能 TOE が表示するラベルによって行うことができる。これは、消費者が(例えば、購入または使用時に) TOE を識別できるようにするものである。

1030 TOE は、TOE を簡単に識別する方法を提供することができる。例えば、ソフトウェア TOE は、立上げルーチンの間に、またはコマンド行の入力に対応して TOE の名前とバージョン番号を表示することができる。ハードウェアまたはファームウェア TOE は、TOE に物理的に刻印されている部品番号により識別することができる。

1031 また、TOE に対して提供された一意の参照は、TOE を構成する各コンポーネントの一意の参照の組み合わせである可能性がある(例えば、統合 TOE である場合)。

ALC_CMC.4-2 評価者は、使用されている TOE 参照が一貫していることを***チェックしなければならない。***

1032 もし、TOE に 2 度以上ラベルが付けられているならば、ラベルは一貫している必要がある。例えば、TOE の一部として提供されるラベルの付いたガイダンス証拠資料を、評価される運用可能 TOE に関係付けることができるべきである。これにより消費者は、TOE の評価済みバージョンを購入したこと、このバージョンを設置したこと、ST に従って TOE を運用するためのガイダンスの正しいバージョンを所有していることを確信できる。

1033 評価者は、TOE 参照が ST と一貫性があることも検証する。

1034 このワークユニットが統合 TOE に適用される場合、以下のものが適用される。統合 TOE は一意の(複合)参照でラベル付けされないが、個別のコンポーネントのみは適切な TOE 参照でラベル付けされる。立上げ及び/または運用中など、その統合 TOE に対するさらなる開発では、複合参照でラベル付けされる必要がある場合がある。統合 TOE が構成コンポーネント TOE として配付される場合、配付された TOE 要素には複合参照が含まれない。ただし、統合 TOE の ST は、統合 TOE に対する一意の参照を含み、統合 TOE を構成するコンポーネントを識別する。消費者は、これにより、適切な要素が含まれているかどうかを決定することができる。

ALC_CMC.4.2C ***CM 証拠資料は、構成要素を一意に識別する方法を記述しなければならない。***

ALC_CMC.4-3 評価者は、構成要素の識別方式が、どのように構成要素が一意に識別されるかを記述していることを決定するために、その識別方式を***検査しなければならない。***

1035 手続きは、TOE のライフサイクルを通して各構成要素のステータスをどのように追跡できるかを記述するべきである。手続きは、CM 計画で、または CM 証拠資料の全体を通して、詳述することができる。含まれる情報では、次の内容を記述するべきである:

a) 同じ構成要素のバージョンを追跡できるように、各構成要素を一意に識別する方法;

b) 構成要素に一意の識別情報が割り付けられる方法、及び CM システムにそれらの情報が入力される方法;

c) 構成要素の過去のバージョンを識別するために使用される方法。

ALC_CMC.4.3C ***CM システムは、すべての構成要素を一意に識別しなければならない。***

ALC_CMC.4-4 評価者は、CM 証拠資料と一貫した方法で構成要素が識別されていることを決定するために構成要素を***検査しなければならない。***

1036 CM システムが、すべての構成要素を一意に識別するという保証は、構成要素の識別情報を検査することによって得られる。ALC_CMS で識別される構成要素について、評価者は、各構成要素が CM 証拠資料に記述されている一意の識別方法と一致するやり方で、一意の識別を持っていることを確認する。

ALC_CMC.4.4C ***CM システムは、許可された変更のみが構成要素に対して行われる自動化された手段を提供しなければならない。***

ALC_CMC.4-5 評価者は、CM アクセス制御手段について、構成要素への許可されないアクセスの阻止が自動化され有効であることを決定するために、CM 計画(***ALC_CMC.4.6C*** を参照のこと)に記述されているそのアクセス制御手段を***検査しなければならない。***

1037 評価者は、多数の方法を使用して CM アクセス制御手段が有効であることを決定することができる。例えば、評価者は、アクセス制御手段を実行して、手続きがバイパスされないことを保証することができる。評価者は、***ALC_CMC.4.10***C が要求する CM システム手続きによって生成される出力を使用することができる。評価者は、採用されているアクセス制御手段が有効に機能していることを保証するために、CM システムの実証に立ち会うこともできる。

ALC_CMC.4.5C ***CM システムは、自動化された手段によって TOE の製造をサポートしなければならない。***

ALC_CMC.4-6 評価者は、TOE の製造をサポートする自動化された手続きについて CM 計画(***ALC_CMC.4.6C*** を参照のこと)を***チェックしなければならない。***

1038 用語「製造」は、TOE を実装表現から最終顧客に配付するために受入れ可能な状態に移すまで、開発者が採用するプロセスに適用される。

1039 評価者は、CM 計画に自動化された製造サポート手続きが存在することを検証する。

1040 以下は、TOE の製造をサポートする自動化された手段の例である:

- ソフトウェア TOE の場合、(多くのソフトウェア開発ツールとともに提供されるような)「作成」ツール;
- ハードウェア TOE の場合、実際に属する部分のみが組み合わされていることを(例えば、バーコードを使用することによって)自動的に確認するツール。

ALC_CMC.4-7 評価者は、TOE 製造サポート手続きが、TOE がその実装表現を反映するように生成されたことを保証するのに有効であることを決定するために、その TOE 製造サポート手続きを***検査しなければならない。***

1041 製造サポート手続きは、明確に定義された方法で実装表現から最終的な TOE を製造するためにどのツールを使用する必要があるかを記述するべきである。規則、指示文、またはその他の必要な構造は、ALC_TAT の下で記述される。

1042 評価者は、製造サポート手続きに従うことによって、TOE を生成するために正しい構成要素が使用されることを決定する。例えば、ソフトウェア TOE では、自動化された製造手続きがすべてのソースファイル及び関係するライブラリがコンパイルされたオブジェクトコードに含まれることを保証するチェックが含まれる。さらに、手続きは、コンパイラオプション及び同等のその他のオブジェクトが一意に定義されていることを保証するべきである。ハードウェア TOE の場合、このワークユニットには、自動的な製造手続きによって、互いに属し合う部分がともに組み立てられており、不足部分がないことについてのチェックが含まれる可能性がある。

1043 これにより、顧客は、設置のために配付される TOE のバージョンが実装表現から曖昧ではない方法で派生しており、ST で記述されたように SFR を実装することを確信できる。

1044 評価者は、CM システムが TOE を製造する能力を必ずしも保有していないこと、しかし、人為的誤りの可能性を減らすことに役に立つプロセスのための支援を提供するべきであることを知っておくべきである。

ALC_CMC.4.6C ***CM 証拠資料は、CM 計画を含まなければならない。***

ALC_CMC.4-8 評価者は、提供された CM 証拠資料が CM 計画を含んでいることを***チェックしなければならない。***

1045 CM 計画は1つの文書にまとめられる必要はないが、しかしどこで CM 計画の様々な箇所を検出できるのかを記述する別個の文書が存在することが推奨される。もし CM 計画が複数の文書により提供されるならば、次のワークユニットのリストは、要求される内容に関するガイダンスを提供する。

ALC_CMC.4.7C ***CM 計画は、TOE の開発に対して CM システムがどのように使用されるかを記述しなければならない。***

ALC_CMC.4-9 評価者は、CM 計画が、TOE の開発のために CM システムがどのように使用されるかを記述していることを決定するために、その計画を***検査しなければならない。***

1046 CM 計画には、適用できる場合、次の記述が含まれる:

a) 構成管理手続きに従う TOE 開発で行われるすべてのアクティビティ(例えば、構成要素の作成、改変または削除、データバックアップ、アーカイブ);

b) 使用可能にする必要がある手段(例えば、CM ツール、用紙);

c) CM ツールの利用法: TOE の完全性を維持するために CM システムの利用者が CM ツールを正しく操作するために必要な詳細;

d) 製造サポート手続き;

e) CM 制御下にあるその他のオブジェクト(開発コンポーネント、ツール、評定環境など);

f) 個々の構成要素を操作するために必要な個人の役割と責任(異なる役割を異なる種別の構成要素(例えば、設計証拠資料またはソースコード)に識別することができる);

g) CM の実体(例えば、変更管理組織、インタフェース管理作業グループ)がどのように導入され、担当者が配置されるか;

h) 変更管理の記述;

i) 許可された個人だけが構成要素を変更できるよう保証するために使用される手続き;

j) 構成要素への同時変更の結果として、同時性の問題が発生しないよう保証するために使用される手続き;

k) 手続きを適用した結果として生成される証拠。例えば、構成要素の変更に対して、CM システムは、変更の記述、変更の責任、影響を受けるすべての構成要素の識別、ステータス(例えば、保留または完了)、及び変更の日付と時刻を記録する。これは、行われた変更の監査証跡または変更管理記録に記録される;

l) TOE バージョンのバージョン管理及び一意に参照するための手法(例えば、オペレーティングシステムでのパッチのリリースの扱い、及びその後のそれらの適用の検出)。

ALC_CMC.4.8C ***CM 計画は、改変もしくは新規に生成された構成要素を TOE の一部として受け入れるための手続きを記述しなければならない。***

ALC_CMC.4-10 評価者は、改変された構成要素または新しく作成された構成要素を TOE の一部として受け入れるために使用する手続きが CM 計画に記述されていることを決定するために、その CM 計画を***検査しなければならない。***

1047 CM 計画の受入れ手続きの記述には、受入れに対する開発者の役割または個人の責任、及び受入れに対して使用される基準を含めるべきである。発生する可能性があるすべての受入れ状況、特に次の状況を考慮するべきである:

a) CM システムに最初に要素を受け入れる場合。特に、他の製造者のソフトウェア、ファームウェア、及びハードウェアコンポーネントを TOE に組み込む場合(「統合」);

b) TOE の構成の各段階(例えば、モジュール、サブシステム、システム)で、構成要素を次のライフサイクルフェーズに移す場合;

c) 異なる開発サイト間での転送後。

1048 統合 TOE で統合される予定の依存コンポーネントにこのワークユニットが適用される場合、CM 計画は、依存 TOE 開発者が取得する基本コンポーネントの制御を考慮するべきである。

1049 コンポーネントを取得する場合、評価者は次の点を検証する:

a) 基本コンポーネント開発者からインテグレータ(依存 TOE 開発者)への各基本コンポーネントの転送は、基本コンポーネント TOE 認証報告で報告されたように、基本コンポーネント TOE のセキュアな配付手続きに従って実行された。

b) 受け取られたコンポーネントは、コンポーネント TOE に対する ST 及び認証報告で述べられているものと同じ識別情報を持っている。

c) 開発者が構成(統合)のために必要とするすべての追加資料が提供されている。これには、コンポーネント TOE の機能仕様の必要な抜粋が含まれる。

ALC_CMC.4.9C ***証拠は、すべての構成要素が CM システム下で維持されていることを実証しなければならない。***

ALC_CMC.4-11 評価者は、構成リストに識別されている構成要素が CM システムによって維持されていることを***チェックしなければならない。***

1050 開発者が採用する CM システムは、TOE の完全性を維持するべきである。評価者は、構成リストに含まれている各種別の構成要素(例えば、設計文書またはソースコードモジュール)に対して、CM 計画に記述されている手続きによって生成された証拠の例が存在することをチェックするべきである。この場合、サンプリング手法は、CM 要素を制御するために CM システムで使用される粒度レベルによって決まる。例えば、10,000 ソースコードモジュールが構成リストに識別されている場合、それが 5 つまたはただ 1 つ存在する場合とは異なるサンプリング方策が適用される必要がある。このアクティビティで重視することは、小さな誤りを検出することではなく、CM システムが正しく運用されていることを保証するべきである。

1051 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

ALC_CMC.4.10C ***CM システムが、CM 計画に従って機能していることを証拠により実証しなければならない。***

ALC_CMC.4-12 評価者は、CM 証拠資料が、CM 計画が識別している CM システムの記録を含んでいることを確かめるために、その証拠資料を***チェックしなければならない。***

1052 CM システムが作り出す出力は、CM 計画が適用されていること、及びすべての構成要素が ***ALC_CMC.4.9C*** が要求するように、CM システムによって維持されていることを評価者が確信するために必要とする証拠を提供するべきである。出力例には、変更管理用紙、または構成要素アクセス許可用紙を含めることができる。

ALC_CMC.4-13 評価者は、CM システムが CM 計画に従って運用されていることを決定するために、証拠を***検査しなければならない。***

1053 評価者は、CM システムのすべての操作が、証拠資料として提出された手続きに従って行われていることを確認するために、構成要素に対し実行された各種別の CM 関連操作(例えば、作成、改変、削除、前のバージョンへの復帰)をカバーする証拠のサンプルを選択して検査するべきである。評価者は、証拠が CM 計画のその操作に識別されている情報のすべてを含んでいることを確認する。証拠を検査するためには、使用されている CM ツールにアクセスする必要がある場合がある。評価者は、証拠をサンプリングすることを選択できる。

1054 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

1055 CM システムが正しく運用されていることと構成要素が有効に維持されていることのさらなる信頼は、選ばれた開発スタッフとのインタビューの手段によって確証することができる。そのようなインタビューを行うとき、評価者は、CM 手続きが CM 証拠資料に記述されているとおりに適用されていることを確認するのに加え、CM システムが実際にどのように使用されているかを深く理解することを目的とする。そのようなインタビューは、記録による証拠の検査を補足するものであり、それらを置き換えるものではないことに注意するべきである。また、記録による証拠だけで要件が満たされる場合、それらは不要である。しかしながら、CM 計画の範囲が広い場合、いくつかの局面(例えば、役割と責任)が CM 計画と記録だけからは明確でない場合がある。これもインタビューによる明確化が必要となるひとつのケースである。

1056 評価者がこのアクティビティを確証するために開発サイトを訪問することが予想される。

1057 サイト訪問のガイダンスについては、A.4、「サイト訪問」を参照のこと。

14.2.5 サブアクティビティの評価(ALC_CMC.5)

14.2.5.1 目的

1058 このサブアクティビティの目的は、開発者が TOE 及びそれに関係する構成要素を明確に識別しているかどうかを、及び CM システムが人為的誤りまたは怠慢による影響を受けないように、自動化ツールによりこれらの要素を改変する能力が適切に制御されているかどうかを決定することである。

14.2.5.2 入力

1059 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) テストに適した TOE;

c) 構成管理証拠資料。

14.2.5.3 アクション ALC_CMC.5.1E

ALC_CMC.5.1C ***TOE は、その一意の参照でラベル付けされなければならない。***

ALC_CMC.5-1 評価者は、評価のために提供された TOE がその参照でラベル付けされていることを***チェックしなければならない。***

1060 評価者は、ST で述べられている一意の参照が TOE に含まれていることを保証するべきである。これは、ラベルの付いたパッケージまたは媒体、または運用可能 TOE が表示するラベルによって行うことができる。これは、消費者が(例えば、購入または使用時に) TOE を識別できるようにするものである。

1061 TOE は、TOE を簡単に識別する方法を提供することができる。例えば、ソフトウェア TOE は、立上げルーチンの間に、またはコマンド行の入力に対応して TOE の名前とバージョン番号を表示することができる。ハードウェアまたはファームウェア TOE は、TOE に物理的に刻印されている部品番号により識別することができる。

1062 また、TOE に対して提供された一意の参照は、TOE を構成する各コンポーネントの一意の参照の組み合わせである可能性がある(例えば、統合 TOE である場合)。

ALC_CMC.5-2 評価者は、使用されている TOE 参照が一貫していることを***チェックしなければならない。***

1063 もし、TOE に 2 度以上ラベルが付けられているならば、ラベルは一貫している必要がある。例えば、TOE の一部として提供されるラベルの付いたガイダンス証拠資料を、評価される運用可能 TOE に関係付けることができるべきである。これにより消費者は、TOE の評価済みバージョンを購入したこと、このバージョンを設置したこと、ST に従って TOE を運用するためのガイダンスの正しいバージョンを所有していることを確信できる。

1064 評価者は、TOE 参照が ST と一貫性があることも検証する。

1065 このワークユニットが統合 TOE に適用される場合、以下のものが適用される。統合 IT の TOE は一意の(複合)参照でラベル付けされないが、個別のコンポーネントのみは適切な TOE 参照でラベル付けされる。立上げ及び/または運用中など、その IT の TOE に対するさらなる開発では、複合参照でラベル付けされる必要がある場合がある。統合 TOE が構成コンポーネント TOE として配付される場合、配付された TOE 要素には複合参照が含まれない。ただし、統合 TOE の ST は、統合 TOE に対する一意の参照を含み、統合 TOE を構成するコンポーネントを識別する。消費者は、これにより、適切な要素が含まれているかどうかを決定することができる。

ALC_CMC.5.2C ***CM 証拠資料は、構成要素を一意に識別する方法を記述しなければならない。***

ALC_CMC.5-3 評価者は、構成要素の識別方式が、どのように構成要素が一意に識別されるかを記述していることを決定するために、その識別方式を***検査しなければならない。***

1066 手続きは、TOE のライフサイクルを通して各構成要素のステータスをどのように追跡できるかを記述するべきである。手続きは、CM 計画で、または CM 証拠資料の全体を通して、詳述することができる。含まれる情報では、次の内容を記述するべきである:

a) 同じ構成要素のバージョンを追跡できるように、各構成要素を一意に識別する方法;

b) 構成要素に一意の識別情報が割り付けられる方法、及び CM システムにそれらの情報が入力される方法;

c) 構成要素の過去のバージョンを識別するために使用される方法。

ALC_CMC.5.3C ***CM 証拠資料は、受入れ手続きが、すべての構成要素に対する十分で適切な変更のレビューを提供することを正当化しなければならない。***

ALC_CMC.5-4 評価者は、受入れ手続きがすべての構成要素に対する十分で適切な変更のレビューを提供することを CM 証拠資料が正当化することを決定するために、その CM 証拠資料を***検査しなければならない。***

1067 CM 証拠資料は、受入れ手続きに従うことによって、適切な品質の部分のみが TOE に組み込まれることを十分に明確にするべきである。

ALC_CMC.5.4C ***CM システムは、すべての構成要素を一意に識別しなければならない。***

ALC_CMC.5-5 評価者は、CM 証拠資料と一貫した方法で構成要素が識別されていることを決定するために構成要素を***検査しなければならない。***

1068 CM システムが、すべての構成要素を一意に識別するという保証は、構成要素の識別情報を検査することによって得られる。TOE を構成する構成要素、及び開発者が評価証拠として提出する構成要素に関するドラフトの両方について、評価者は、各構成要素が CM 証拠資料に記述されている一意の識別方法と一致するやり方で、一意の識別を持っていることを確認する。

ALC_CMC.5.5C ***CM システムは、許可された変更のみが構成要素に対して行われる自動化された手段を提供しなければならない。***

ALC_CMC.5-6 評価者は、CM アクセス制御手段が、構成要素への許可されないアクセスの阻止が自動化され有効であることを決定するために、CM 計画(***ALC_CMC.5.12C*** を参照のこと)に記述されているそのアクセス制御手段を***検査しなければならない。***

1069 評価者は、多数の方法を使用して CM アクセス制御手段が有効であることを決定することができる。例えば、評価者は、アクセス制御手段を実行して、手続きがバイパスされないことを保証することができる。評価者は、***ALC_CMC.5.16C*** が要求するCMシステム手続きによって生成される出力を使用することができる。評価者は、採用されているアクセス制御手段が有効に機能していることを保証するために、CM システムの実証に立ち会うこともできる。

ALC_CMC.5.6C ***CM システムは、自動化された手段によって TOE の製造をサポートしなければならない。***

ALC_CMC.5-7 評価者は、TOE の製造をサポートする自動化された手続きについて CM 計画(***ALC_CMC.5.12C*** を参照のこと)を***チェックしなければならない。***

1070 用語「製造」は、TOE を実装表現から最終顧客に配付するために受入れ可能な状態に移すまで、開発者が採用するプロセスに適用される。

1071 評価者は、CM 計画に自動化された製造サポート手続きが存在することを検証する。

1072 以下は、TOE の製造をサポートする自動化された手段の例である:

- ソフトウェア TOE の場合、(多くのソフトウェア開発ツールとともに提供されるような)「作成」ツール;
- ハードウェア TOE の場合、実際に属する部分のみが組み合わされていることを(例えば、バーコードを使用することによって)自動的に確認するツール。

ALC_CMC.5-8 評価者は、TOE 製造サポート手続きが、TOE がその実装表現を反映するように生成されたことを保証するのに有効であることを決定するために、その TOE 製造サポート手続きを***検査しなければならない。***

1073 製造サポート手続きは、明確に定義された方法で実装表現から最終的な TOE を製造するためにどのツールを使用する必要があるかを記述するべきである。規則、指示文、またはその他の必要な構造は、ALC_TATの下で記述される。

1074 評価者は、製造サポート手続きに従うことによって、TOE を生成するために正しい構成要素が使用されることを決定する。例えば、ソフトウェア TOE では、自動化された製造手続きがすべてのソースファイル及び関係するライブラリがコンパイルされたオブジェクトコードに含まれることを保証するチェックが含まれる。さらに、手続きは、コンパイラオプション及び同等のその他のオブジェクトが一意に定義されていることを保証するべきである。ハードウェアTOEの場合、このワークユニットには、自動的な製造手続きによって、互いに属し合う部分がともに組み立てられており、不足部分がないことについてのチェックが含まれる可能性がある。

1075 これにより、顧客は、設置のために配付されるTOEのバージョンが実装表現から曖昧ではない方法で派生しており、ST で記述されたように SFR を実装することを確信できる。

1076 評価者は、CMシステムがTOEを製造する能力を必ずしも保有していないこと、しかし、人為的誤りの可能性を減らすことに役に立つプロセスのための支援を提供するべきであること、を知っておくべきである。

ALC_CMC.5.7C ***CM システムは、構成要素をCM に受け入れる責任のある人はその開発者でないことを保証しなければならない。***

ALC_CMC.5-9 評価者は、構成要素を受け入れる責任者がその構成要素の開発者ではないことを CM システムが保証することを決定するために、その CM システムを***検査しなければならない。***

1077 受入れ手続きは、構成要素を受け入れる責任者を記述する。これらの記述から、評価者は、構成要素の開発者がどのような場合においても受入れに対しては責任を負わないことを決定できるべきである。

ALC_CMC.5.8C ***CM システムは、TSF を構成する構成要素を識別しなければならない。***

ALC_CMC.5-10 評価者は、CM システムが TSF を構成する構成要素を明確に識別していることを決定するために、その CM システムを***検査しなければならない。***

1078 CM 証拠資料は、CM システムが TSF を構成する構成要素をどのように識別するかを記述するべきである。評価者は、各種別の要素、特に TSF 及び TSF 以外の要素を含め、カバーする構成要素のサンプルを選択し、それらが CM システムによって正しく分類されていることをチェックするべきである。

1079 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

ALC_CMC.5.9C ***CM システムは、監査証跡に発信者、日時を含んでいる自動化された手段により、TOE のすべての変更についての監査をサポートしなければならない。***

ALC_CMC.5-11 評価者は、発信者、日時を含む監査証跡で、自動化された手段による TOE のすべての変更を CM システムがサポートすることを決定するために、その CM システムを***検査しなければならない。***

1080 評価者は、監査証跡のサンプルを検査し、それらが最低限の情報を含んでいるかどうかをチェックするべきである。

ALC_CMC.5.10C ***CM システムは、ある構成要素の変更により影響を受けるすべての他の構成要素を特定するための、自動化された手段を提供しなければならない。***

ALC_CMC.5-12 評価者は、ある構成要素の変更により影響を受けるすべての他の構成要素を識別するための自動化された手段を CM システムが提供することを決定するために、その CM システムを***検査しなければならない。***

1081 CM 証拠資料は、ある構成要素の変更により影響を受けるすべての他の構成要素を CM システムがどのように識別するかを記述するべきである。評価者は、すべての要素の種別をカバーしている構成要素のサンプルを選択し、選択された要素の変更により影響を受けるすべての要素を識別することを決定するために、自動化された手段を実行するべきである。

1082 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

ALC_CMC.5.11C ***CM システムは、TOE の生成元である実装表現のバージョンを識別できなければならない。***

ALC_CMC.5-13 評価者は、TOE が生成される元となる実装表現のバージョンを CM システムが識別できることを決定するために、その CM システムを***検査しなければならない。***

1083 CM 証拠資料は、TOE が生成される元となる実装表現のバージョンを CM システムがどのように識別するかを記述するべきである。評価者は、TOE を製造するために使用される部分のサンプルを選択するべきであり、CM システムが正しいバージョンで対応する実装表現を識別することを検証するために、その CM システムを適用するべきである。

1084 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

ALC_CMC.5.12C ***CM 証拠資料は、CM 計画を含まなければならない。***

ALC_CMC.5-14 評価者は、提供された CM 証拠資料が CM 計画を含んでいることを***チェックしなければならない。***

1085 CM 計画は1つの文書にまとめられる必要はないが、しかしどこで CM 計画の様々な箇所を検出できるのかを記述する別個の文書が存在することが推奨される。もし CM 計画が複数の文書により提供されるならば、次のワークユニットのリストは、要求される内容に関するガイダンスを提供する。

ALC_CMC.5.13C ***CM 計画は、TOE の開発に対して CM システムがどのように使用されるかを記述しなければならない。***

ALC_CMC.5-15 評価者は、CM 計画が、TOE の開発のために CM システムがどのように使用されるかを記述していることを決定するために、その計画を***検査しなければならない。***

1086 CM 計画には、適用できる場合、次の記述が含まれる:

a) 構成管理手続きに従う TOE 開発で行われるすべてのアクティビティ(例えば、構成要素の作成、改変または削除、データバックアップ、アーカイブ);

b) 使用可能にする必要がある手段(例えば、CM ツール、用紙);

c) CM ツールの利用法: TOE の完全性を維持するために CM システムの利用者が CM ツールを正しく操作するために必要な詳細;

d) 製造サポート手続き;

e) CM 制御下にあるその他のオブジェクト(開発コンポーネント、ツール、評定環境など);

f) 個々の構成要素を操作するために必要な個人の役割と責任(異なる役割を異なる種別の構成要素(例えば、設計証拠資料またはソースコード)に識別することができる);

g) CM の実体(例えば、変更管理組織、インタフェース管理作業グループ)がどのように導入され、担当者が配置されるか;

h) 変更管理の記述;

i) 許可された個人だけが構成要素を変更できるよう保証するために使用される手続き;

j) 構成要素への同時変更の結果として、同時性の問題が発生しないよう保証するために使用される手続き;

k) 手続きを適用した結果として生成される証拠。例えば、構成要素の変更に対して、CM システムは、変更の記述、変更の責任、影響を受けるすべての構成要素の識別、ステータス(例えば、保留または完了)、及び変更の日付と時刻を記録する。これは、行われた変更の監査証跡または変更管理記録に記録される;

l) TOE バージョンのバージョン管理及び一意に参照するための手法(例えば、オペレーティングシステムでのパッチのリリースの扱い、及びその後のそれらの適用の検出)。

ALC_CMC.5.14C ***CM 計画は、改変もしくは新規に生成された構成要素を TOE の一部として受け入れるための手続きを記述しなければならない。***

ALC_CMC.5-16 評価者は、改変された構成要素または新しく作成された構成要素を TOE の一部として受け入れるために使用する手続きが CM 計画に記述されていることを決定するために、その CM 計画を***検査しなければならない。***

1087 CM 計画の受入れ手続きの記述には、受入れに対する開発者の役割または個人の責任、及び受入れに対して使用される基準を含めるべきである。発生する可能性があるすべての受入れ状況、特に次の状況を考慮するべきである:

a) CM システムに最初に要素を受け入れる場合。特に、他の製造者のソフトウェア、ファームウェア、及びハードウェアコンポーネントを TOE に組み込む場合(「統合」);

b) TOE の構成の各段階(例えば、モジュール、サブシステム、システム)で、構成要素を次のライフサイクルフェーズに移す場合;

c) 異なる開発サイト間での転送後。

ALC_CMC.5.15C ***証拠は、すべての構成要素が CM システム下で維持されていることを実証しなければならない。***

ALC_CMC.5-17 評価者は、構成リストに識別されている構成要素が CM システムによって維持されていることを***チェックしなければならない。***

1088 開発者が採用する CM システムは、TOE の完全性を維持するべきである。評価者は、構成リストに含まれている各種別の構成要素(例えば、設計文書またはソースコードモジュール)に対して、CM 計画に記述されている手続きによって生成された証拠の例が存在することをチェックするべきである。この場合、サンプリング手法は、CM 要素を制御するために CM システムで使用される粒度レベルによって決まる。例えば、10,000 ソースコードモジュールが構成リストに識別されている場合、それが 5 つまたはただ 1 つ存在する場合とは異なるサンプリング方策が適用される必要がある。このアクティビティで重視することは、小さな誤りを検出することではなく、CM システムが正しく運用されていることを保証するべきである。

1089 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

ALC_CMC.5.16C ***CM システムが、CM 計画に従って機能していることを証拠により実証しなければならない。***

ALC_CMC.5-18 評価者は、CM 証拠資料が、CM 計画が識別している CM システムの記録を含んでいることを確かめるために、その証拠資料を***チェックしなければならない。***

1090 CM システムが作り出す出力は、CM 計画が適用されていること、及びすべての構成要素が ***ALC_CMC.5.15C*** が要求するように、CM システムによって維持されていることを評価者が確信するために必要とする証拠を提供するべきである。出力例には、変更管理用紙、または構成要素アクセス許可用紙を含めることができる。

ALC_CMC.5-19 評価者は、CM システムが CM 計画に従って運用されていることを決定するために、証拠を***検査しなければならない。***

1091 評価者は、CM システムのすべての操作が、証拠資料として提出された手続きに従って行われていることを確認するために、構成要素に対し実行された各種別の CM 関連操作(例えば、作成、改変、削除、前のバージョンへの復帰)をカバーする証拠のサンプルを選択して検査するべきである。評価者は、証拠が CM 計画のその操作に識別されている情報のすべてを含んでいることを確認する。証拠を検査するためには、使用されている CM ツールにアクセスする必要がある場合がある。評価者は、証拠をサンプリングすることを選択できる。

1092 サンプリングのガイダンスについては、A.2、「サンプリング」を参照のこと。

1093 CM システムが正しく運用されていることと構成要素が有効に維持されていることのさらなる信頼は、選ばれた開発スタッフとのインタビューの手段によって確証することができる。そのようなインタビューを行うとき、評価者は、CM 手続きが CM 証拠資料に記述されているとおりに適用されていることを確認するのに加え、CM システムが実際にどのように使用されているかを深く理解することを目的とする。そのようなインタビューは、記録による証拠の検査を補足するものであり、それらを置き換えるものではないことに注意するべきである。また、記録による証拠だけで要件が満たされる場合、それらは不要である。しかしながら、CM 計画の範囲が広い場合、いくつかの局面(例えば、役割と責任)が CM 計画と記録だけからは明確でない場合がある。これもインタビューによる明確化が必要となるひとつのケースである。

1094 評価者がこのアクティビティを確証するために開発サイトを訪問することが予想される。

1095 サイト訪問のガイダンスについては、A.4、「サイト訪問」を参照のこと。

14.2.5.4 **アクション** ALC_CMC.5.2E

ALC_CMC.5-20 評価者は、製造サポート手続きに従うことによって、テストアクティビティに対して開発者が提供したものと同様に TOE が製造されることを決定するために、これらの手続きを***検査しなければならない。***

1096 TOE が小規模なソフトウェア TOE であり、製造がコンパイルとリンクで構成されている場合、評価者は、自分でそれらを再適用することにより製造サポート手続きの適切性を確認することができることがある。

1097 TOE の製造プロセスが(例えば、スマートカードの場合のように)より複雑であり、しかしすでに開始されている場合、評価者は、開発サイトの訪問中に製造サポート手続きの適用を検査するべきである。開発者は、テストアクティビティに対して使用されるサンプルと、開発者が存在している状態で製造された TOE のコピーを比較することができる場合がある。

1098 サイト訪問のガイダンスについては、A.4、「サイト訪問」を参照のこと。

1099 それ以外の場合、評価者の決定は、開発者が提供する記録による証拠に基づいているべきである。

1100 このワークユニットは、実装表現(ADV_IMP)の下で評価アクティビティとともに実行することができる。

14.3 CM 範囲(ALC_CMS)

14.3.1 サブアクティビティの評価(ALC_CMS.1)

14.3.1.1 目的

1101 このサブアクティビティの目的は、開発者が TOE 及び評価証拠に対して構成管理を実行するかどうかを決定することである。これらの構成要素は、CM 能力(ALC_CMC)に従って制御される。

14.3.1.2 入力

1102 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 構成リスト。

14.3.1.3 アクション ALC_CMS.1.1E

ALC_CMS.1.1C *構成リストは、TOE 自体、及び SAR が要求する評価証拠を含まなければならない。*

ALC_CMS.1-1 評価者は、構成リストに次の要素のセットが含まれていることを*チェックしなければならない*:

a) TOE 自体;

b) ST で SAR が要求する評価証拠。

ALC_CMS.1.2C *構成リストは、構成要素を一意に識別しなければならない。*

ALC_CMS.1-2 評価者は、構成リストが各構成要素を一意に識別することを決定するために、その構成リストを*検査しなければならない。*

1103 構成リストには、各要素の使用されているバージョンを一意に識別するための十分な情報(一般的にはバージョン番号)が含まれている。このリストを使用することにより、評価者は、正しい構成要素、各要素の正しいバージョンが評価中に使用されたことをチェックすることができる。

14.3.2 サブアクティビティの評価(ALC_CMS.2)

14.3.2.1 目的

1104 このサブアクティビティの目的は、構成リストに TOE、TOE を構成する部分、及び評価証拠が含まれているかどうかを決定することである。これらの構成要素は、CM 能力(ALC_CMC)に従って制御される。

14.3.2.2 入力

1105 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 構成リスト。

14.3.2.3 アクション ALC_CMS.2.1E

ALC_CMS.2.1C *構成リストは、TOE 自体、SAR が要求する評価証拠、及び TOE を構成する部分を含まなければならない。*

ALC_CMS.2-1 評価者は、構成リストが以下の一連の要素を含むことを*チェックしなければならない。*

a) TOE 自体;

b) TOE を構成する部分;

c) SAR が要求する評価証拠。

ALC_CMS.2.2C *構成リストは、構成要素を一意に識別しなければならない。*

ALC_CMS.2-2 評価者は、構成リストが各構成要素を一意に識別することを決定するために、その構成リストを*検査しなければならない。*

1106 構成リストには、各要素の使用されているバージョンを一意に識別するための十分な情報(一般的にはバージョン番号)が含まれている。このリストを使用することにより、評価者は、正しい構成要素、各要素の正しいバージョンが評価中に使用されたことをチェックすることができる。

ALC_CMS.2.3C *各 TSF 関連の構成要素に対して、構成リストはその要素の開発者を示さなければならない。*

ALC_CMS.2-3 評価者は、構成リストが各 TSF 関連構成要素の開発者を示すことを*チェックしなければならない。*

1107 TOE の開発に単一の開発者のみが関わる場合、このワークユニットは該当しないため、満たされているものとみなされる。

14.3.3 サブアクティビティの評価(ALC_CMS.3)

14.3.3.1 目的

1108 このサブアクティビティの目的は、構成リストに TOE、TOE を構成する部分、TOE 実装表現、及び評価証拠が含まれているかどうかを決定することである。これらの構成要素は、CM 能力(ALC_CMC)に従って制御される。

14.3.3.2 入力

1109 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 構成リスト。

14.3.3.3 アクション ALC_CMS.3.1E

ALC_CMS.3.1C *構成リストは、TOE 自体、SAR が要求する評価証拠、TOE を構成する部分、及び実装表現を含まなければならない。*

ALC_CMS.3-1 評価者は、構成リストに次の要素のセットが含まれていることを***チェックしなければならない*** :

a) TOE 自体;

b) TOE を構成する部分;

c) TOE 実装表現;

d) ST で SAR が要求する評価証拠。

ALC_CMS.3.2C ***構成リストは、構成要素を一意に識別しなければならない。***

ALC_CMS.3-2 評価者は、構成リストが各構成要素を一意に識別することを決定するために、その構成リストを***検査しなければならない。***

1110 構成リストには、各要素の使用されているバージョンを一意に識別するための十分な情報(一般的にはバージョン番号)が含まれている。このリストを使用することにより、評価者は、正しい構成要素、各要素の正しいバージョンが評価中に使用されたことをチェックすることができる。

ALC_CMS.3.3C ***各 TSF 関連の構成要素に対して、構成リストはその要素の開発者を示さなければならない。***

ALC_CMS.3-3 評価者は、構成リストが各 TSF 関連構成要素の開発者を示すことを***チェックしなければならない。***

1111 TOE の開発に単一の開発者のみが関わる場合、このワークユニットは該当しないため、満たされているものとみなされる。

14.3.4 サブアクティビティの評価(ALC_CMS.4)

14.3.4.1 目的

1112 このサブアクティビティの目的は、構成リストに TOE、TOE を構成する部分、TOE 実装表現、セキュリティ欠陥、及び評価証拠が含まれているかどうかを決定することである。これらの構成要素は、CM 能力(ALC_CMC)に従って制御される。

14.3.4.2 入力

1113 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 構成リスト。

14.3.4.3 アクション ALC_CMS.4.1E

ALC_CMS.4.1C ***構成リストは、TOE 自体、SAR が要求する評価証拠、TOE を構成する部分、実装表現、及びセキュリティ欠陥報告及び解決ステータスを含まなければならない。***

ALC_CMS.4-1 評価者は、構成リストに次の要素のセットが含まれていることを***チェックしなければならない：***

a) TOE 自体;

b) TOE を構成する部分;

c) TOE 実装表現;

d) ST で SAR が要求する評価証拠;

e) 実装に関連する報告されたセキュリティ欠陥の詳細を記録するのに用いられる証拠資料(例えば、開発者の問題データベースから得られる問題状況報告)。

ALC_CMS.4.2C ***構成リストは、構成要素を一意に識別しなければならない。***

ALC_CMS.4-2 評価者は、構成リストが各構成要素を一意に識別することを決定するために、その構成リストを***検査しなければならない。***

1114 構成リストには、各要素の使用されているバージョンを一意に識別するための十分な情報(一般的にはバージョン番号)が含まれている。このリストを使用することにより、評価者は、正しい構成要素、各要素の正しいバージョンが評価中に使用されたことをチェックすることができる。

ALC_CMS.4.3C ***各 TSF 関連の構成要素に対して、構成リストはその要素の開発者を示さなければならない。***

ALC_CMS.4-3 評価者は、構成リストが各 TSF 関連構成要素の開発者を示すことを***チェックしなければならない。***

1115 TOE の開発に単一の開発者のみが関わる場合、このワークユニットは該当しないため、満たされているものとみなされる。

14.3.5 サブアクティビティの評価(ALC_CMS.5)

14.3.5.1 目的

1116 このサブアクティビティの目的は、構成リストに TOE、TOE を構成する部分、TOE 実装表現、セキュリティ欠陥、開発ツール及び関連情報、及び評価証拠が含まれているかどうかを決定することである。これらの構成要素は、CM 能力（ALC_CMC）に従って制御される。

14.3.5.2 入力

1117 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 構成リスト。

14.3.5.3 アクション ALC_CMS.5.1E

ALC_CMS.5.1C ***構成リストは、TOE 自体、SAR が要求する評価証拠、TOE を構成する部分、実装表現、セキュリティ欠陥報告及び解決ステータス、及び開発ツール及び関連情報を含まなければならない。***

ALC_CMS.5-1 評価者は、構成リストに次の要素のセットが含まれていることを***チェックしなければならない：***

a) TOE 自体;

b) TOE を構成する部分;

c) TOE 実装表現;

d) ST で SAR が要求する評価証拠;

e) 実装に関連する報告されたセキュリティ欠陥の詳細を記録するのに用いられる証拠資料(例えば、開発者の問題データベースから得られる問題状況報告);

f) 各開発ツールの名前、バージョン、構成及び役割を含む TOE の開発及び製造に関わるすべてのツール(該当する場合はテストソフトウェアを含む)、及び関連証拠資料。

1118 ソフトウェア TOE に対しては次のようになる。「開発ツール」は通常プログラミング言語及びコンパイラになり、「関連証拠資料」はコンパイラオプションとリンカオプションで構成される。ハードウェア TOE の場合、「開発ツール」はハードウェア設計言語、シミュレーションツール及び統合ツール、コンパイラである可能性があり、「関連証拠資料」はこの場合もまたコンパイラオプションを構成する可能性がある。

ALC_CMS.5.2C ***構成リストは、構成要素を一意に識別しなければならない。***

ALC_CMS.5-2 評価者は、構成リストが各構成要素を一意に識別することを決定するために、その構成リストを***検査しなければならない。***

1119 構成リストには、各要素の使用されているバージョンを一意に識別するための十分な情報(一般的にはバージョン番号)が含まれている。このリストを使用することにより、評価者は、正しい構成要素、各要素の正しいバージョンが評価中に使用されたことをチェックすることができる。

ALC_CMS.5.3C ***各 TSF 関連の構成要素に対して、構成リストはその要素の開発者を示さなければならない。***

ALC_CMS.5-3 評価者は、構成リストが各 TSF 関連構成要素の開発者を示すことを***チェックしなければならない。***

1120 TOE の開発に単一の開発者のみが関わる場合、このワークユニットは該当しないため、満たされているものとみなされる。

14.4 配付(ALC_DEL)

14.4.1 サブアクティビティの評価(ALC_DEL.1)

14.4.1.1 目的

1121 このサブアクティビティの目的は、配付証拠資料が、TOE を利用者に配付するときに TOE のセキュリティを維持するのに用いられるすべての手続きを記述しているかどうかを決定することである。

14.4.1.2 入力

1122 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 配付証拠資料。

14.4.1.3 アクション ALC_DEL.1.1E

ALC_DEL.1.1C ***配付証拠資料は、TOE のバージョンを消費者に配送するときにセキュリティを維持するために必要なすべての手続きを記述しなければならない。***

ALC_DEL.1-1 評価者は、配付証拠資料が、TOE のバージョンまたはその一部を消費者に配付するときのセキュリティを維持するために必要なすべての手続きを記述していることを決定するために、その証拠資料を***検査しなければならない。***

1123 配付証拠資料は、TOE またはそのコンポーネント部分の転送中の TOE のセキュリティを維持し、TOE の識別を決定するための適切な手続きを記述する。

1124 配付証拠資料は、TOE 全体に渡るべきであるが、TOE の異なる部分に対する異なる手続きを含んでもよい。評価は、手続きの全体を考慮するべきである。

1125 配付手続きは、製造環境から設置環境(例えば、パッケージング、保管、及び配送)までの配付のすべてのフェーズに適用されるべきである。パッケージングと配付のための標準的な商習慣を受け入れることができる。これには、シュリンクラップパッケージング、セキュリティテープ、または封印された封筒などが含まれる。配付には、物理的(例えば、公共郵便または民間の配付サービス)または電子的(例えば、電子メールまたはインターネットからのダウンロード)手続きを使用できる。

1126 開発者は、改ざんまたはなりすましを検出できることを保証するために、暗号チェックサムまたはソフトウェア署名を使用することができる。また、改ざん防止シールは、機密性が侵害されたかどうかを示す。ソフトウェア TOE に対しては、機密性は暗号化を使用することによって保証できる可能性がある。可用性が関心事項となっている場合、セキュアな転送が要求される可能性がある。

1127 用語「セキュリティを維持するために必要」の解釈は、次の点を考慮する必要がある:

- TOE の本質(例えば、ソフトウェアまたはハードウェアである)。

- 選択された脆弱性評定によって TOE に対して記述されている全体的なセキュリティレベル。意図した環境において特定の能力を持つ攻撃者に対する抵抗力が TOE に要求されている場合、これは TOE の配付に対しても適用するべきである。評価者は、均衡の取れた手法が取られ、配付が、その他の点でセキュアな開発プロセスでの弱点を表さないことを決定するべきである。

- ST によって提供されるセキュリティ対策方針。TOE の完全性は常に重要であるため、配付証拠資料では完全性に関連する手段に強調が置かれる可能性が高い。しかしながら、ある種の TOE の配付においては、機密性及び可用性が関心事項となるだろう。したがって、セキュアな配付のこれらの側面に関係する手続きもまた、手続きの中で議論されるべきである。

14.4.1.4 暗黙の評価者アクション

ALC_DEL.1.2D ***開発者は、配付手続きを使用しなければならない。***

ALC_DEL.1-2 評価者は、配付手続きが使用されることを決定するために、配付プロセスの側面を***検査しなければならない。***

1128 配付手続きの適用をチェックするために評価者が取る手法は、TOE の本質、配付プロセスそれ自体によって決まる。手続きそれ自体の検査に加えて、評価者は、それらが実際に適用されることのいくつかの保証を探す。いくつかの可能な手法は、次のとおりである:

a) 手続きが実際に適用されていることを観察できる配付場所の訪問;

b) 配付のいくつかの段階、または利用者が受け取った後の TOE の検査(例えば、改ざん防止シールのチェック);

c) 評価者が正規のチャネルを通して TOE を入手するときにプロセスが実際に適用されていることの観察;

d) TOE が配付された方法についてのエンド利用者への質問。

1129 サイト訪問のガイダンスについては、A.4、「サイト訪問」を参照のこと。

1130 TOE が新たに開発され、配付手続きをこれから調べなければならない場合がある。これらの場合、適切な手続きとファシリティが将来の配付のために用意できていること、及びすべての関係者が責任を理解していることに、評価者は満足する必要がある。評価者は、実際に可能な場合、配付の「試行」を要求することができる。開発者が他の同様な製品を作成している場合、それらが使用されている手続きを検査することは、保証を提供するうえで役に立つことがある。

14.5 開発セキュリティ(ALC_DVS)

14.5.1 サブアクティビティの評価(ALC_DVS.1)

14.5.1.1 目的

1131 このサブアクティビティの目的は、開発者による開発環境でのセキュリティ制御が、TOE のセキュアな運用が損なわれることがないことを保証するために必要な TOE 設計と実装の機密性と完全性を提供するのに適しているかどうかを決定することである。

14.5.1.2 入力

1132 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 開発セキュリティ証拠資料。

1133 さらに、評価者は、セキュリティ制御が明確に定義され、守られていることを決定するために、その他の提供物件を検査する必要がある可能性がある。特に評価者は、開発者の構成管理証拠資料(サブアクティビティの評価(ALC_CMC.4)「製造サポート及び受入れ手続き」及びサブアクティビティの評価(ALC_CMS.4)「課題追跡の CM カバレージ」に対する入力)を検査する必要がある可能性がある。手続きが適用されていることを示す証拠も必要となる。

14.5.1.3 アクション ALC_DVS.1.1E

ALC_DVS.1.1C ***開発セキュリティ証拠資料は、開発環境での TOE の設計及び実装の機密性と完全性を保護するために必要となる、物理的、手続き的、人的、及びその他のセキュリティ手段をすべて記述しなければならない。***

ALC_DVS.1-1 評価者は、開発セキュリティ証拠資料が、TOE 設計と実装の機密性と完全性を保護するために必要な開発環境で使用されるすべてのセキュリティ手段を詳細に記述していることを決定するために、その証拠資料を***検査しなければならない。***

1134 評価者は、必要な保護を決定するのに役立つ可能性がある情報を求めて、最初に ST を参照することにより、必要な情報を決定する。

1135 明示的な情報が ST から提供されない場合、評価者は、必要な手段を決定する必要がある。開発者の手段が必要に対して不十分であるとみなされる場合、潜在的に悪用可能な脆弱性に基づいて、明確な正当化が評定のために提供されるべきである。

1136 次の種別のセキュリティ手段が、証拠資料を検査するときに、評価者によって考慮される:

a) 物理的。例えば、TOE 開発環境(通常の作業時間とその他の時間)への許可されない不当なアクセスを防止するために使用される物理的アクセス制御;

b) 手続き的。例えば、次のものを扱う:

- 開発環境または開発マシンなどの環境の特定の部分へのアクセスの許可
- 開発者が開発チームを離れるときのアクセス権の取消し

- 定義された受入れ手続きに従った、開発環境の内部及び外部への、及び異なる開発サイト間での保護された対象物の転送
- 開発環境への訪問者の許可と付き添い
- セキュリティ手段の継続的適用を確実にする役割と責任、及びセキュリティ違反の検出。

c) 人的。例えば、新たな開発スタッフの信頼を確証するために行われる管理またはチェック;

d) その他のセキュリティ手段。例えば、開発マシンの論理的保護。

1137 開発セキュリティ証拠資料は、開発が行われる場所を識別し、実行される開発の局面を、各場所及び異なる場所の間の転送に対して適用されるセキュリティ手段とともに記述するべきである。例えば、開発は、1 つの建物内の複数のファシリティ、同じサイトの複数の建物、または複数のサイトで行うことができる。様々な開発サイト間での TOE の一部または未完成の TOE の転送は、開発セキュリティ(ALC_DVS)によって扱われ、完成した TOE の消費者に対する転送は配付(ALC_DEL)で扱われる。

1138 開発には、TOE の製造が含まれる。

ALC_DVS.1-2 評価者は、採用されたセキュリティ手段が十分であることを決定するために、開発の機密性と完全性の方針を***検査しなければならない。***

1139 評価者は、方針の中に以下のことが記述されていることを検査すべきである。

a) 機密を維持する必要がある TOE 開発に関係する情報及びそのような対象物にアクセスできる開発スタッフのメンバ;

b) TOE の完全性を維持するために許可されない不当な改変から保護する必要がある対象物及びそのような対象物を改変することができる開発スタッフのメンバ。

1140 評価者は、これらの方針が開発セキュリティ証拠資料に記述されていること、採用されているセキュリティ手段が方針と一貫していること、及びそれらが完全であることを決定するべきである。

1141 構成管理手続きは、TOE の完全性を保護するのに役に立つこと、及び評価者は、CM 能力(ALC_CMC)に対して行われるワークユニットとの重複を避けるべきであることに注意するべきである。例えば、CM 証拠資料は、開発環境にアクセスすべき役割または個人、及び TOE を改変することができる役割または個人を管理するために必要なセキュリティ手続きを記述することができる。

1142 CM 能力(ALC_CMC)要件は固定されているが、開発セキュリティ(ALC_DVS)に対する要件は必要な手段のみを要求し、TOE の本質、及び ST に提供される情報に依存する。評価者は、そのような方針がこのサブアクティビティのもとで適用されていることを決定する。

14.5.1.4 アクション ALC_DVS.1.2E

ALC_DVS.1-3 評価者は、セキュリティ手段が適用されていることを決定するために、開発セキュリティ証拠資料及び関連する証拠を***検査しなければならない。***

1143 このワークユニットでは、評価者は、TOE の完全性及び関係する証拠資料の機密性が適切に保護されるために、開発セキュリティ証拠資料に記述されたセキュリティ手段が守られていることを決定する必要がある。例えば、これは、提供された記録による証拠を検査することによって決定することができる。記録による証拠は、開発環境を訪問することによって補足されるべきである。開発環境を訪問することにより、評価者は、次のことを行うことができる:

a) セキュリティ手段(例えば、物理的手段)の適用を観察する;

b) 手続きの適用の記録による証拠を検査する;

c) 開発スタッフにインタビューし、開発セキュリティ方針と手続き、それらの責任についての認識をチェックする。

1144 開発サイトの訪問は、使用されている手段に対する確信を得るのに役に立つ手段である。そのような訪問を行わないという決定は、評価監督機関と相談して決定されるべきである。

1145 サイト訪問のガイダンスについては、A.4、「サイト訪問」を参照のこと。

14.5.2 サブアクティビティの評価(ALC_DVS.2)

14.5.2.1 目的

1146 このサブアクティビティの目的は、開発者による開発環境でのセキュリティ制御が、TOE のセキュアな運用が損なわれることがないことを保証するために必要な TOE 設計と実装の機密性と完全性を提供するのに適しているかどうかを決定することである。また、適用された手段が十分であるかどうかを正当化することが意図されている。

14.5.2.2 入力

1147 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 開発セキュリティ証拠資料。

1148 さらに、評価者は、セキュリティ制御が明確に定義され、守られていることを決定するために、その他の提供物件を検査する必要がある可能性がある。特に評価者は、開発者の構成管理証拠資料(サブアクティビティの評価(ALC_CMC.4)「製造サポート及び受入れ手続き」及びサブアクティビティの評価(ALC_CMS.4)「課題追跡の CM カバレージ」に対する入力)を検査する必要がある可能性がある。手続きが適用されていることを示す証拠も必要となる。

14.5.2.3 アクション ALC_DVS.2.1E

ALC_DVS.2.1C ***開発セキュリティ証拠資料は、開発環境での TOE の設計及び実装の機密性と完全性を保護するために必要となる、物理的、手続き的、人的、及びその他のセキュリティ手段をすべて記述しなければならない。***

ALC_DVS.2-1 評価者は、開発セキュリティ証拠資料が、TOE 設計と実装の機密性と完全性を保護するために必要な開発環境で使用されるすべてのセキュリティ手段を詳細に記述していることを決定するために、その証拠資料を***検査しなければならない。***

1149 評価者は、必要な保護を決定するのに役立つ可能性がある情報を求めて、最初に ST を参照することにより、必要な情報を決定する。

1150 明示的な情報が ST から提供されない場合、評価者は、必要な手段を決定する必要がある。開発者の手段が必要に対して不十分であるとみなされる場合、潜在的に悪用可能な脆弱性に基づいて、明確な正当化が評定のために提供されるべきである。

1151 次の種別のセキュリティ手段が、証拠資料を検査するときに、評価者によって考慮される:

a) 物理的、例えば、TOE 開発環境(通常の作業時間とその他の時間)への許可されない不当なアクセスを防止するために使用される物理的アクセス制御;

b) 手続き的、例えば、次のものを扱う:

- 開発環境または開発マシンなどの環境の特定の部分へのアクセスの許可
- 開発者が開発チームを離れるときのアクセス権の取消し
- 定義された受入れ手続きに従った、開発環境の外部への、及び異なる開発サイト間での保護された対象物の転送
- 開発環境への訪問者の許可と付き添い
- セキュリティ手段の継続的適用を確実にする役割と責任、及びセキュリティ違反の検出。

c) 人的、例えば、新たな開発スタッフの信頼を確証するために行われる管理またはチェック;

d) その他のセキュリティ手段、例えば、開発マシンの論理的保護。

1152 開発セキュリティ証拠資料は、開発が行われる場所を識別し、実行される開発の局面を、各場所及び異なる場所の間の転送に対して適用されるセキュリティ手段とともに記述するべきである。例えば、開発は、1 つの建物内の複数のファシリティ、同じサイトの複数の建物、または複数のサイトで行うことができる。様々な開発サイト間での TOE の一部または未完成の TOE の転送は、開発セキュリティ(ALC_DVS)によって扱われ、完成した TOE の利用者に対する転送は配付(ALC_DEL)で扱われる。

1153 開発には、TOE の製造が含まれる。

ALC_DVS.2.2C ***開発セキュリティ証拠資料は、セキュリティ手段が、TOE の機密性と完全性を維持するうえで、必要な保護レベルを提供することを正当化しなければならない。***

ALC_DVS.2-2 評価者は、TOE の機密性と完全性を維持するためにセキュリティ手段が必要な保護のレベルを提供する理由に対して適切な正当化が行われることを決定するために、開発セキュリティ証拠資料を***検査しなければならない。***

1154 TOE または関連情報に対する攻撃は様々な設計及び製造における段階で想定されるため、手段と手続きは、攻撃を防いだり、攻撃をより困難にしたりするために必要とされる適切なレベルにする必要がある。

1155 このレベルは TOE に対して主張される攻撃能力全体に依存するため(選択された脆弱性分析(AVA_VAN)コンポーネントを参照のこと)、開発セキュリティ証拠資料は、TOE の機密性と完全性を維持するために、必要な保護のレベルの正当性を示すべきである。このレベルは、適用されるセキュリティ手段によって達成される必要がある。

1156 保護手段の概念は一貫しているべきであり、正当化には手段がどのように相互をサポートするかについての分析が含まれているべきである。TOE の配付まで関与するすべての役割を持つすべての様々なサイトの開発及び製造のすべての側面は、分析されるべきである。

1157 正当化には、適用されるセキュリティ手段を考慮して、潜在的な脆弱性の分析を含めることができる。

1158 例えば、次のような説得力のある論証が存在する可能性がある。

- 開発者のインフラストラクチャの技術的手段及びメカニズムが、適切なセキュリティレベルを維持するために十分である(例えば、暗号メカニズム、物理的保護メカニズム、CM システムの特性(ALC_CMC.4-5 を参照のこと));

- TOE の実装表現(関連するガイダンス文書を含む)を含んでいるシステムは、「トロイの木馬」コードまたはウイルスによる攻撃など、論理的な攻撃に対する効果的な保護を提供する。分離されたシステムを維持するために必要なソフトウェアのみが設置されている、及び追加ソフトウェアがその後設置されない分離されたシステムで、実装表現が保たれている場合、これは適切である可能性がある。

- このシステムに持ち込まれるデータは、隠れた機能性がシステムに設置されることを防ぐため、慎重に考慮される必要がある。例えば、マシンへのアクセスの取得、いくつかの追加実行可能コード(プログラム、マクロなど)のインストール、または論理的な攻撃を使用してマシンからの情報の取得を行うための独立した試行を行い、これらの手段をテストする必要がある。

- 適切な組織的な(手続き的及び人的な)手段が無条件に実施されている。

ALC_DVS.2-3 評価者は、採用されたセキュリティ手段が十分であることを決定するために、開発の機密性と完全性の方針を***検査しなければならない。***

1159 評価者は、方針の中に以下のことが記述されていることを検査しなければならない。

a) 機密を維持する必要がある TOE 開発に関係する情報及びそのような対象物にアクセスできる開発スタッフのメンバ;

b) TOE の完全性を維持するために許可されない不当な改変から保護する必要がある対象物及びそのような対象物を改変することができる開発スタッフのメンバ。

1160 評価者は、これらの方針が開発セキュリティ証拠資料に記述されていること、採用されているセキュリティ手段が方針と一貫していること、及びそれらが完全であることを決定するべきである。

1161 構成管理手続きは、TOE の完全性を保護するのに役に立つこと、及び評価者は、CM 能力(ALC_CMC)に対して行われるワークユニットとの重複を避けるべきであることに注意するべきである。例えば、CM 証拠資料は、開発環境にアクセスすべき役割または個人、TOE を改変することができる役割または個人を管理するために必要なセキュリティ手続きを記述することができる。

1162 CM 能力(ALC_CMC)要件は固定されているが、開発セキュリティ(ALC_DVS)に対する要件は必要な手段のみを要求し、TOE の本質、及び ST に提供される情報に依存する。例えば、ST は、セキュリティ資格を持つスタッフによって開発される TOE を要求する開発環境のセキュリティ対策方針を識別することができる。評価者は、そのような方針がこのサブアクティビティのもとで適用されていることを決定する。

14.5.2.4 アクション ALC_DVS.2.2E

ALC_DVS.2-4 評価者は、セキュリティ手段が適用されていることを決定するために、開発セキュリティ証拠資料及び関連する証拠を***検査しなければならない。***

1163 このワークユニットでは、評価者は、TOE の完全性及び関係する証拠資料の機密性が適切に保護されるために、開発セキュリティ証拠資料に記述されたセキュリティ手段が守られていることを決定する必要がある。例えば、これは、提供された記録による証拠を検査することによって決定することができる。記録による証拠は、開発環境を訪問することによって補足されるべきである。開発環境を訪問することにより、評価者は、次のことを行うことができる:

a) セキュリティ手段(例えば、物理的手段)の適用を観察する;

b) 手続きの適用の記録による証拠を検査する;

c) 開発スタッフにインタビューし、開発セキュリティ方針と手続き、それらの責任についての認識をチェックする。

1164 開発サイトの訪問は、使用されている手段に対する確信を得るのに役に立つ手段である。そのような訪問を行わないという決定は、評価監督機関と相談して決定されるべきである。

1165 サイト訪問のガイダンスについては、A.4、「サイト訪問」を参照のこと。

14.6 欠陥修正(ALC_FLR)

14.6.1 サブアクティビティの評価(ALC_FLR.1)

14.6.1.1 目的

1166 このサブアクティビティの目的は、開発者がセキュリティ欠陥の追跡、訂正アクションの識別、及びTOE利用者に対する訂正アクション情報の配付を記述する欠陥修正手続きを確立したかどうかを決定することである。

14.6.1.2 入力

1167 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 欠陥修正手続き証拠資料。

14.6.1.3 アクション ALC_FLR.1.1E

ALC_FLR.1.1C ***欠陥修正手続き証拠資料は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。***

ALC_FLR.1-1 評価者は、欠陥修正手続き証拠資料がTOEのリリースごとに報告されたすべてのセキュリティ欠陥を追跡するために使用する手続きを記述していることを決定するために、その欠陥修正手続き証拠資料を***検査しなければならない。***

1168 手続きは、疑わしいセキュリティ欠陥のそれぞれが報告される時間から、その欠陥が解決される時間まで、開発者が実行するアクションを記述する。これには、欠陥がセキュリティ欠陥であることの確認による最初の検出から、セキュリティ欠陥の解決までの欠陥の全体の時間枠が含まれる。

1169 欠陥がセキュリティ関連ではないことが検出される場合、(欠陥修正(ALC_FLR)要件の目的に対して)欠陥修正手続きはその欠陥をさらに追跡する必要はない。欠陥がセキュリティ関連ではないことの理由の説明のみが必要である。

1170 これらの要件では、TOE利用者がセキュリティ欠陥を報告する公表された手段が存在することは要求されないが、報告されるすべてのセキュリティ欠陥を追跡することが要求される。つまり、報告されるセキュリティ欠陥は、開発者の組織の外部から発生するからといって、単純に無視できない。

ALC_FLR.1.2C ***欠陥修正手続きは、欠陥の訂正の調査状況の記述とともに、各々のセキュリティ欠陥の性質と影響の記述が提供されることを要求しなければならない。***

ALC_FLR.1-2 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥の性質及び影響の観点から各セキュリティ欠陥の記述が作成されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1171 手続きは、各セキュリティ欠陥を再現できるように各セキュリティ欠陥の性質及び影響を十分に詳細に記述するために、開発者が実行するアクションを識別する。セキュリティ欠陥の性質の記述は、それが証拠資料における誤り、TSF の設計における欠陥、TSF の実装における欠陥などであるかどうかを扱う。セキュリティ欠陥の影響の記述は、影響を受けるTSF の部分、及びそれらの部分がどのように影響を受けるかを識別する。例えば、パスワード「BACK DOOR」を使用して認証を許可することによって TSF が実施する識別と認証に影響を与える、実装におけるセキュリティ欠陥が見つかる可能性がある。

ALC_FLR.1-3 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥に対する訂正の調査状況が識別されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1172 欠陥修正手続きは、セキュリティ欠陥の様々な段階を識別する。この区別には、少なくとも、報告されている疑わしいセキュリティ欠陥、セキュリティ欠陥であることが確認されている疑わしいセキュリティ欠陥、及び解決方法が実装されているセキュリティ欠陥が含まれる。追加段階(例えば、報告されているが、まだ調査されていない欠陥、調査中の欠陥、解決方法が見つかっているが、まだ実装されていないセキュリティ欠陥)を含めることは許されている。

ALC_FLR.1.3C ***欠陥修正手続きは、各々のセキュリティ欠陥の訂正アクションが識別されることを要求しなければならない。***

ALC_FLR.1-4 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥に対する訂正アクションが識別されることを決定するために、その欠陥修正手続きを***チェックしなければならない。***

1173 訂正アクションは、TOE のハードウェア、ファームウェア、またはソフトウェアの一部に対する修復、TOE ガイダンスの改変、またはその両方で構成することができる。TOE ガイダンスに対する改変(例えば、セキュリティ欠陥を未然に防ぐために実行する手続き的な手段の詳細)を構成する訂正アクションには、(修復が発行されるまで)暫定的な解決方法としてのみ役割を果たす手段、及び(手続き的な手段が最良の解決方法であることが決定される場合に)永続的な解決方法として役割を果たす手段の両方が含まれる。

1174 セキュリティ欠陥の発生源が証拠資料の誤りである場合、訂正アクションは影響を受ける TOE ガイダンスの更新で構成される。訂正アクションが手続き的な手段である場合、この手段には、これらの訂正手続きを反映するために、影響を受ける TOE ガイダンスに対して行われる更新が含まれる。

ALC_FLR.1.4C ***欠陥修正手続き証拠資料は、TOE 利用者に、欠陥情報、訂正、及び訂正アクションについてのガイダンスを提供するために使用する方法を記述しなければならない。***

ALC_FLR.1-5 評価者は、欠陥修正手続き証拠資料が TOE 利用者に対して各セキュリティ欠陥についての必要な情報を提供する手段を記述していることを決定するために、その欠陥修正手続き証拠資料を***検査しなければならない。***

1175 各セキュリティ欠陥に関する*必要な情報*は、記述(ワークユニット ALC_FLR.1-2 の一部として提供されているものと同じ詳細レベルである必要はない)、規定される訂正アクション、及び訂正の実装についての任意の関連するガイダンスで構成されている。

1176 TOE 利用者には、web サイトへの掲示、TOE 利用者への送信、または訂正を適用するために開発者に対して行われる調整などのいくつかの方法で、このような情報、訂正、及び証拠資料の更新を提供することができる。この情報を提供する手段で TOE 利用者がアクションを開始する必要がある場合、任意の TOE ガイダンスに情報を取得するための指示が含まれていることを保証するために、評価者はその TOE ガイダンスを検査する。

1177 情報、訂正、及びガイダンスを提供するために使用される方法の適切性を評定するための唯一の尺度は、TOE 利用者がそれを取得するか受け取ることができるという合理的予測が存在するということである。例えば、1 ヶ月の間必要な情報が web サイトに掲示され、TOE 利用者がこれが発生すること、及びいつ発生する予定であるかを知っている場合の散布の方法について考慮する。これは、特に(例えば、web サイトへの永続的な掲示ほどは)合理的または効果的ではない可能性があるが、TOE 利用者が必要な情報を取得できる可能性があるという点で実現可能である。他方、情報が 1 時間だけ web サイトに掲示され、TOE 利用者がこれについてまたはこれがいつ掲示されるかを知る手段を持たなかった場合、利用者が必要な情報を取得するということは不可能である。

14.6.2 サブアクティビティの評価(ALC_FLR.2)

14.6.2.1 目的

1178 このサブアクティビティの目的は、開発者がセキュリティ欠陥の追跡、訂正アクションの識別、及びTOE利用者に対する訂正アクション情報の配付を記述する欠陥修正手続きを確立したかどうかを決定することである。また、このサブアクティビティは、開発者の手続きが、セキュリティ欠陥の訂正に対して、TOE 利用者からの欠陥報告の受信に対して、及び訂正によって新しいセキュリティ欠陥が持ち込まれていないことの保証に対して、規定するかどうかを決定する。

1179 開発者が TOE 利用者からのセキュリティ欠陥報告に基づいて適切に行動することができるようするために、TOE 利用者は開発者にセキュリティ欠陥報告を提出する方法を理解する必要があり、開発者はこれらの報告を受け取る方法を知る必要がある。TOE 利用者を対象とした欠陥修正ガイダンスは、TOE 利用者が開発者と通信するための方法を理解していることを保証する。欠陥修正手続きはこのような通信における開発者の役割を記述する。

14.6.2.2 入力

1180 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 欠陥修正手続き証拠資料;

b) 欠陥修正ガイダンス証拠資料。

14.6.2.3 アクション ALC_FLR.2.1E

ALC_FLR.2.1C ***欠陥修正手続き証拠資料は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。***

ALC_FLR.2-1 評価者は、欠陥修正手続き証拠資料がTOEのリリースごとに報告されたすべてのセキュリティ欠陥を追跡するために使用する手続きを記述していることを決定するために、その欠陥修正手続き証拠資料を***検査しなければならない。***

1181 手続きは、疑わしいセキュリティ欠陥のそれぞれが報告される時間から、その欠陥が解決される時間まで、開発者が実行するアクションを記述する。これには、欠陥がセキュリティ欠陥であることの確認による最初の検出から、セキュリティ欠陥の解決までの欠陥の全体の時間枠が含まれる。

1182 欠陥がセキュリティ関連ではないことが検出される場合、(欠陥修正(ALC_FLR)要件の目的に対して)欠陥修正手続きはその欠陥をさらに追跡する必要はない。欠陥がセキュリティ関連ではないことの理由の説明のみが必要である。

ALC_FLR.2.2C ***欠陥修正手続きは、欠陥の訂正の調査状況の記述とともに、各々のセキュリティ欠陥の性質と影響の記述が提供されることを要求しなければならない。***

ALC_FLR.2-2 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥の性質及び影響の観点から各セキュリティ欠陥の記述が作成されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1183 手続きは、各セキュリティ欠陥を再現できるように各セキュリティ欠陥の性質及び影響を十分に詳細に記述するために、開発者が実行するアクションを識別する。セキュリティ欠陥の性質の記述は、それが証拠資料における誤り、TSF の設計における欠陥、TSF の実装における欠陥などであるかどうかを扱う。セキュリティ欠陥の影響の記述は、影響を受ける TSF の部分、及びそれらの部分がどのように影響を受けるかを識別する。例えば、パスワード「BACKDOOR」を使用して認証を許可することによって TSF が実施する識別と認証に影響を与える、実装におけるセキュリティ欠陥が見つかる可能性がある。

ALC_FLR.2-3 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥に対する訂正の調査状況が識別されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1184 欠陥修正手続きは、セキュリティ欠陥の様々な段階を識別する。この区別には、少なくとも、報告されている疑わしいセキュリティ欠陥、セキュリティ欠陥であることが確認されている疑わしいセキュリティ欠陥、及び解決方法が実装されているセキュリティ欠陥が含まれる。追加段階(例えば、報告されているが、まだ調査されていない欠陥、調査中の欠陥、解決方法が見つかっているが、まだ実装されていないセキュリティ欠陥)を含めることは許されている。

ALC_FLR.2.3C ***欠陥修正手続きは、各々のセキュリティ欠陥の訂正アクションが識別されることを要求しなければならない。***

ALC_FLR.2-4 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥に対する訂正アクションが識別されることを決定するために、その欠陥修正手続きを***チェックしなければならない。***

1185 *訂正アクション*は、TOE のハードウェア、ファームウェア、またはソフトウェアの一部に対する修復、TOE ガイダンスの改変、またはその両方で構成することができる。TOE ガイダンスに対する改変(例えば、セキュリティ欠陥を未然に防ぐために実行する手続き的な手段の詳細)を構成する訂正アクションには、(修復が発行されるまで)暫定的な解決方法としてのみ役割を果たす手段、及び(手続き的な手段が最良の解決方法であることが決定される場合に)永続的な解決方法として役割を果たす手段の両方が含まれる。

1186 セキュリティ欠陥の発生源が証拠資料の誤りである場合、訂正アクションは影響を受ける TOE ガイダンスの更新で構成される。訂正アクションが手続き的な手段である場合、この手段には、これらの訂正手続きを反映するために、影響を受ける TOE ガイダンスに対して行われる更新が含まれる。

ALC_FLR.2.4C ***欠陥修正手続き証拠資料は、TOE 利用者に、欠陥情報、訂正、及び訂正アクションについてのガイダンスを提供するために使用する方法を記述しなければならない。***

ALC_FLR.2-5 評価者は、欠陥修正手続き証拠資料が TOE 利用者に対して各セキュリティ欠陥についての必要な情報を提供する手段を記述していることを決定するために、その欠陥修正手続き証拠資料を***検査しなければならない。***

1187 各セキュリティ欠陥に関する*必要な情報*は、記述(ワークユニット ALC_FLR.2-2 の一部として提供されているものと同じ詳細レベルである必要はない)、規定される訂正アクション、及び訂正の実装についての任意の関連するガイダンスで構成されている。

1188 TOE 利用者には、web サイトへの掲示、TOE 利用者への送信、または訂正を適用するために開発者に対して行われる調整などのいくつかの方法で、このような情報、訂正、及び証拠資料の更新を提供することができる。この情報を提供する手段で TOE 利用者がアクションを開始する必要がある場合、任意の TOE ガイダンスに情報を取得するための指示が含まれていることを保証するために、評価者はその TOE ガイダンスを検査する。

1189 情報、訂正、及びガイダンスを提供するために使用される方法の適切性を評定するための唯一の尺度は、TOE 利用者がそれを取得するか受け取ることができるという合理的予測が存在するということである。例えば、1 ヶ月の間必要な情報が web サイトに掲示され、TOE 利用者がこれが発生すること、及びいつ発生する予定であるかを知っている場合の散布の方法について考慮する。これは、特に(例えば、web サイトへの永続的な掲示ほどは)合理的または効果的ではない可能性があるが、TOE 利用者が必要な情報を取得できる可能性があるという点で実現可能である。他方、情報が 1 時間だけ web サイトに掲示され、TOE 利用者がこれについてまたはこれがいつ掲示されるかを知る手段を持たなかった場合、利用者が必要な情報を取得するということは不可能である。

ALC_FLR.2.5C ***欠陥修正手続きは、開発者が TOE 利用者からの報告及び TOE の疑わしいセキュリティ欠陥に関する問合せを受け取る手段を記述しなければならない。***

ALC_FLR.2-6 評価者は、開発者がセキュリティ欠陥の報告またはそのような欠陥に対する訂正についての要求を受け入れるための手続きを欠陥修正手続きが記述することを決定するために、その欠陥修正手続きを***検査しなければならない。***

1190 手続きは、TOE 利用者が TOE 開発者と通信するための手段を持っていることを保証する。開発者に連絡するための手段を持つことにより、利用者は、セキュリティ欠陥の報告、セキュリティ欠陥の状況に関する問い合わせ、及び欠陥に対する訂正の要求を行うことができる。この連絡の手段は、セキュリティ関連ではない問題の報告に使用されるより一般的な連絡ファシリティの一部とすることができる。

1191 これらの手続きの利用は TOE 利用者に制限されないが、TOE 利用者のみがこれらの手続きの詳細を積極的に供給される。TOE に対してアクセスできる可能性がある、または TOE について理解している可能性があるその他の人は、同じ手続きを使用して開発者に報告を提出でき、その開発者はその後それらを処理すると予測されている。開発者が識別した手段以外の開発者への報告の提出の手段は、このワークユニットの範囲外である。他の手段によって生成される報告を扱う必要はない。

ALC_FLR.2.6C ***報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が修正され、TOE 利用者に修正手続きが発行されることを保証しなければならない。***

ALC_FLR.2-7 評価者は、欠陥修正手続きの適用が、すべての報告された欠陥が訂正されることを保証するのに役立つことを決定するために、その欠陥修正手続きを***検査しなければならない。***

1192 欠陥修正手続きは、開発者が検出及び報告するセキュリティ欠陥だけではなく、TOE 利用者が報告するセキュリティ欠陥も扱う。手続きは、報告された各セキュリティ欠陥が訂正されることがどのように保証されるかを記述するために、十分に詳細なものである。手続きには、最終的かつ必然的な解決方法に到達するまでの進み方を示す合理的な手順が含まれる。

1193 手続きは、疑わしいセキュリティ欠陥がセキュリティ欠陥であることが決定された時点から、それが解決される時点までに行われたプロセスを記述する。

ALC_FLR.2-8 評価者は、欠陥修正手続きの適用が、各セキュリティ欠陥に対する修正手続きが TOE 利用者に対して発行されていることを保証するのに役立つことを決定するために、その欠陥修正手続きを***検査しなければならない。***

1194 手続きは、セキュリティ欠陥が解決された時点から、修正手続きが提供される時点までに実行されるプロセスを記述する。訂正アクションの配付の手続きは、セキュリティ対策方針と一貫しているべきである。これらの手続きは、保証要件に含まれている場合は、ALC_DELを満たすために証拠資料が提出されているように、TOEの配付に使用される手続きと同一である必要はない。例えば、TOE のハードウェア部分が元は保税品配送業者によって配付されていた場合、欠陥修正の結果のハードウェアに対する更新は同様に保税品配送業者によって配付されるものと予測される。欠陥修正に関連しない更新は、配付(ALC_DEL)要件を満たす証拠資料に示されている手続きに従う。

ALC_FLR.2.7C ***報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる訂正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。***

ALC_FLR.2-9 評価者は、欠陥修正手続きの適用の結果、潜在的な訂正に有害な影響を含まないための保護手段が提供されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1195 分析、テスト、またはこれらの 2 つの組み合わせを使用して、開発者はセキュリティ欠陥が訂正されたときに有害な影響が持ち込まれる可能性を減らすことができる。評価者は、分析とテストのアクションの必要な組み合わせが特定の訂正に対してどのように決定されるかについて、手続きが詳細を提供するかどうかを評定する。

1196 評価者は、セキュリティ欠陥の発生源が証拠資料の問題である場合に、手続きにその他の証拠資料に対する矛盾が持ち込まれないようにする保護手段が含まれることも決定する。

ALC_FLR.2.8C ***欠陥修正ガイダンスは、TOE 利用者が開発者へ TOE の疑わしいセキュリティ欠陥を報告する手段を記述しなければならない。***

ALC_FLR.2-10 評価者は、これらの手続きの適用の結果、TOE 利用者が疑わしいセキュリティ欠陥の報告またはこのようなセキュリティ欠陥に対する訂正の要求を提供するための手段が提供されることを決定するために、欠陥修正ガイダンスを***検査しなければならない。***

1197 ガイダンスは、TOE 利用者が TOE 開発者と通信するための手段を持っていることを保証する。開発者に連絡するための手段を持つことにより、利用者は、セキュリティ欠陥の報告、セキュリティ欠陥の状況に関する問い合わせ、及び欠陥に対する訂正の要求を行うことができる。

14.6.3 サブアクティビティの評価(ALC_FLR.3)

14.6.3.1 目的

1198 このサブアクティビティの目的は、開発者がセキュリティ欠陥の追跡、訂正アクションの識別、及びTOE利用者に対する訂正アクション情報の配付を記述する欠陥修正手続きを確立したかどうかを決定することである。また、このサブアクティビティは、開発者の手続きが、セキュリティ欠陥の訂正に対して、TOE 利用者からの欠陥報告の受信に対して、訂正によって新しいセキュリティ欠陥が持ち込まれていないことの保証に対して、各 TOE 利用者に対する連絡先の確立に対して、及びTOE利用者に対する訂正アクションのタイムリな発行に対して、規定するかどうかを決定する。

1199 開発者が TOE 利用者からのセキュリティ欠陥報告に基づいて適切に行動することができるようするために、TOE 利用者は開発者にセキュリティ欠陥報告を提出する方法を理解する必要があり、開発者はこれらの報告を受け取る方法を知る必要がある。TOE 利用者を対象とした欠陥修正ガイダンスは、TOE 利用者が開発者と通信するための方法を理解していることを保証する。欠陥修正手続きはこのような通信における開発者の役割を記述する。

14.6.3.2 入力

1200 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 欠陥修正手続き証拠資料;

b) 欠陥修正ガイダンス証拠資料。

14.6.3.3 アクション ALC_FLR.3.1E

ALC_FLR.3.1C ***欠陥修正手続き証拠資料は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。***

ALC_FLR.3-1 評価者は、欠陥修正手続き証拠資料が TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するために使用する手続きを記述していることを決定するために、その欠陥修正手続き証拠資料を***検査しなければならない。***

1201 手続きは、疑わしいセキュリティ欠陥のそれぞれが報告される時間から、その欠陥が解決される時間まで、開発者が実行するアクションを記述する。これには、欠陥がセキュリティ欠陥であることの確認による最初の検出から、セキュリティ欠陥の解決までの欠陥の全体の時間枠が含まれる。

1202 欠陥がセキュリティ関連ではないことが検出される場合、(欠陥修正(ALC_FLR)要件の目的に対して)欠陥修正手続きはその欠陥をさらに追跡する必要はない。欠陥がセキュリティ関連ではないことの理由の説明のみが必要である。

ALC_FLR.3.2C ***欠陥修正手続きは、欠陥の訂正の調査状況の記述とともに、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。***

ALC_FLR.3-2 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥の性質及び影響の観点から各セキュリティ欠陥の記述が作成されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1203 手続きは、各セキュリティ欠陥を再現できるように各セキュリティ欠陥の性質及び影響を十分に詳細に記述するために、開発者が実行するアクションを識別する。セキュリティ欠陥の性質の記述は、それが証拠資料における誤り、TSF の設計における欠陥、TSF の実装における欠陥などであるかどうかを扱う。セキュリティ欠陥の影響の記述は、影響を受ける TSF の部分、及びそれらの部分がどのように影響を受けるかを識別する。例えば、パスワード「BACKDOOR」を使用して認証を許可することによって TSF が実施する識別と認証に影響を与える、実装におけるセキュリティ欠陥が見つかる可能性がある。

ALC_FLR.3-3 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥に対する訂正の調査状況が識別されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1204 欠陥修正手続きは、セキュリティ欠陥の様々な段階を識別する。この区別には、少なくとも、報告されている疑わしいセキュリティ欠陥、セキュリティ欠陥であることが確認されている疑わしいセキュリティ欠陥、及び解決方法が実装されているセキュリティ欠陥が含まれる。追加段階(例えば、報告されているが、まだ調査されていない欠陥、調査中の欠陥、解決方法が見つかっているが、まだ実装されていないセキュリティ欠陥)を含めることは許されている。

ALC_FLR.3.3C ***欠陥修正手続きは、各々のセキュリティ欠陥の訂正アクションが識別されることを要求しなければならない。***

ALC_FLR.3-4 評価者は、欠陥修正手続きの適用によって、各セキュリティ欠陥に対する訂正アクションが識別されることを決定するために、その欠陥修正手続きを***チェックしなければならない。***

1205 訂正アクションは、TOE のハードウェア、ファームウェア、またはソフトウェアの一部に対する修復、TOE ガイダンスの改変、またはその両方で構成することができる。TOE ガイダンスに対する改変(例えば、セキュリティ欠陥を未然に防ぐために実行する手続き的な手段の詳細)を構成する訂正アクションには、(修復が発行されるまで)暫定的な解決方法としてのみ役割を果たす手段、及び(手続き的な手段が最良の解決方法であることが決定される場合に)永続的な解決方法として役割を果たす手段の両方が含まれる。

1206 セキュリティ欠陥の発生源が証拠資料の誤りである場合、訂正アクションは影響を受ける TOE ガイダンスの更新で構成される。訂正アクションが手続き的な手段である場合、この手段には、これらの訂正手続きを反映するために、影響を受ける TOE ガイダンスに対して行われる更新が含まれる。

ALC_FLR.3.4C ***欠陥修正手続き証拠資料は、TOE 利用者に、欠陥情報、訂正、及び訂正アクションについてのガイダンスを提供するために使用する方法を記述しなければならない。***

ALC_FLR.3-5 評価者は、欠陥修正手続き証拠資料が TOE 利用者に対して各セキュリティ欠陥についての必要な情報を提供する手段を記述していることを決定するために、その欠陥修正手続き証拠資料を***検査しなければならない。***

1207 各セキュリティ欠陥に関する*必要な情報*は、記述(ワークユニット ALC_FLR.3-2 の一部として提供されているものと同じ詳細レベルである必要はない)、規定される訂正アクション、及び訂正の実装についての任意の関連するガイダンスで構成されている。

1208 TOE 利用者には、web サイトへの掲示、TOE 利用者への送信、または訂正を適用するために開発者に対して行われる調整などのいくつかの方法で、このような情報、訂正、及び証拠資料の更新を提供することができる。この情報を提供する手段で TOE 利用者がアクションを開始する必要がある場合、任意の TOE ガイダンスに情報を取得するための指示が含まれていることを保証するために、評価者はその TOE ガイダンスを検査する。

1209 情報、訂正、及びガイダンスを提供するために使用される方法の適切性を評定するための唯一の尺度は、TOE 利用者がそれを取得するか受け取ることができるという合理的予測が存在するということである。例えば、1 ヶ月の間必要な情報が web サイトに掲示され、TOE 利用者がこれが発生すること、及びいつ発生する予定であるかを知っている場合の散布の方法について考慮する。これは、特に(例えば、web サイトへの永続的な掲示ほどは)合理的または効果的ではない可能性があるが、TOE 利用者が必要な情報を取得できる可能性があるという点で実現可能である。他方、情報が 1 時間だけ web サイトに掲示され、TOE 利用者がこれについてまたはこれがいつ掲示されるかを知る手段を持たなかった場合、利用者が必要な情報を取得するということは不可能である。

1210 開発者に登録する(ワークユニット ALC_FLR.3-12 を参照のこと) TOE 利用者に対しては、この情報の受動的可用性は十分ではない。開発者は、登録された TOE 利用者に情報(またはその可用性の通知)を積極的に送信する必要がある。

ALC_FLR.3.5C ***欠陥修正手続きは、開発者が TOE 利用者からの報告及び TOE の疑わしいセキュリティ欠陥に関する問合せを受け取る手段を記述しなければならない。***

ALC_FLR.3-6 評価者は、欠陥修正手続きの適用の結果、開発者が TOE 利用者から疑わしいセキュリティ欠陥の報告またはこのような欠陥に対する訂正の要求を受信する手段が提供されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1211 手続きは、TOE 利用者が TOE 開発者と通信するための手段を持っていることを保証する。開発者に連絡するための手段を持つことにより、利用者は、セキュリティ欠陥の報告、セキュリティ欠陥の状況に関する問い合わせ、及び欠陥に対する訂正の要求を行うことができる。この連絡の手段は、セキュリティ関連ではない問題の報告に使用されるより一般的な連絡ファシリティの一部とすることができる。

1212 これらの手続きの利用は TOE 利用者に制限されないが、TOE 利用者のみがこれらの手続きの詳細を積極的に供給される。TOE に対してアクセスできる可能性がある、または TOE について理解している可能性があるその他の人は、同じ手続きを使用して開発者に報告を提出でき、その開発者はその後それらを処理すると予測されている。開発者が識別した手段以外の開発者への報告の提出の手段は、このワークユニットの範囲外である。他の手段によって生成される報告を扱う必要はない。

ALC_FLR.3.6C ***欠陥修正手続きは、セキュリティ欠陥により影響を受ける可能性がある登録された利用者に対する、タイムリな応答、セキュリティ欠陥報告及び関連する訂正の自動配付を要求する手続きを含まなければならない。***

ALC_FLR.3-7 評価者は、欠陥修正手続きの適用の結果、各セキュリティ欠陥に関する報告、及び各セキュリティ欠陥に対する関連の訂正によって、影響を受ける可能性がある登録された TOE 利用者のタイムリな提供手段が提供されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1213 タイムリであるかどうかの問題は、セキュリティ欠陥報告と関連する訂正の両方の発行に適用される。ただし、これらは、同じタイミングで発行する必要はない。欠陥報告は、暫定的解決方法が見つかり次第、その解決方法が TOE をオフにするなどの極端な方法であるとしても、生成及び発行されるべきであることが認識されている。同様に、より永続的な(及びより極端ではない)解決方法が見つかった場合、過度の遅延がないように発行するべきである。

1214 報告及び関連する訂正の受信者を、セキュリティ欠陥が影響を与える可能性がある TOE 利用者だけに制限する必要はない。タイムリな方法で行われる場合、すべてのセキュリティ欠陥に対するこのような報告及び訂正をすべての TOE 利用者に提供することが許される。

ALC_FLR.3-8 評価者は、欠陥修正手続きの適用の結果、影響を受ける可能性がある登録された TOE 利用者に対して、報告及び関連する訂正が自動配付されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1215 *自動配付*とは、配付方法に対する人間の関与が許されていないという意味ではない。実際には、配付方法は、場合によっては、報告または訂正の発行が行われないことについて規定された段階的拡大を伴う密接に監視されている手続きを通して、完全に手動の手続きで構成される可能性がある。

1216 報告及び関連する訂正の受信者を、セキュリティ欠陥が影響を与える可能性がある TOE 利用者だけに制限する必要はない。自動的に行われる場合、すべてのセキュリティ欠陥に対するこのような報告及び訂正をすべての TOE 利用者に提供することが許される。

ALC_FLR.3.7C ***報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が修正され、TOE 利用者に修正手続きが発行されることを保証しなければならない。***

ALC_FLR.3-9 評価者は、欠陥修正手続きの適用が、すべての報告された欠陥が修正されることを保証するのに役立つことを決定するために、その欠陥修正手続きを***検査しなければならない。***

1217 欠陥修正手続きは、開発者が検出及び報告するセキュリティ欠陥だけではなく、TOE 利用者が報告するセキュリティ欠陥も扱う。手続きは、報告された各セキュリティ欠陥が修正されることがどのように保証されるかを記述するために、十分に詳細なものである。手続きには、最終的かつ必然的な解決方法に到達するまでの進み方を示す合理的な手順が含まれる。

1218 手続きは、疑わしいセキュリティ欠陥がセキュリティ欠陥であることが決定された時点から、それが解決される時点までに行われたプロセスを記述する。

ALC_FLR.3-10 評価者は、欠陥修正手続きの適用が、各セキュリティ欠陥に対する修正手続きが TOE 利用者に対して発行されていることを保証するのに役立つことを決定するために、その欠陥修正手続きを***検査しなければならない。***

1219 手続きは、セキュリティ欠陥が解決された時点から、修正手続きが提供される時点までに実行されるプロセスを記述する。修正手続きの配付の手続きは、セキュリティ対策方針と一貫しているべきである。これらの手続きは、保証要件に含まれている場合は、配付(ALC_DEL)を満たすために証拠資料が提出されているように、TOE の配付に使用される手続きと同一である必要はない。例えば、TOE のハードウェア部分が元は保税品配送業者によって配付されていた場合、欠陥修正の結果のハードウェアに対する更新は同様に保税品配送業者によって配付されるものと予測される。欠陥修正に関連しない更新は、配付(ALC_DEL)要件を満たす証拠資料に示されている手続きに従う。

ALC_FLR.3.8C ***報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる訂正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。***

ALC_FLR.3-11 評価者は、欠陥修正手続きの適用の結果、潜在的な訂正に有害な影響を含まないための保護手段が提供されることを決定するために、その欠陥修正手続きを***検査しなければならない。***

1220 分析、テスト、またはこれらの 2 つの組み合わせを使用して、開発者はセキュリティ欠陥が訂正されたときに有害な影響が持ち込まれる可能性を減らすことができる。評価者は、分析とテストのアクションの必要な組み合わせが特定の訂正に対してどのように決定されるかについて、手続きが詳細を提供するかどうかを評定する。

1221 評価者は、セキュリティ欠陥の発生源が証拠資料の問題である場合に、手続きにその他の証拠資料に対する矛盾が持ち込まれないようにする保護手段が含まれることも決定する。

ALC_FLR.3.9C ***欠陥修正ガイダンスは、TOE 利用者が開発者へ TOE の疑わしいセキュリティ欠陥を報告する手段を記述しなければならない。***

ALC_FLR.3-12 評価者は、これらの手続きの適用の結果、TOE 利用者が疑わしいセキュリティ欠陥の報告またはこのようなセキュリティ欠陥に対する訂正の要求を提供するための手段が提供されることを決定するために、欠陥修正ガイダンスを***検査しなければならない。***

1222 ガイダンスは、TOE 利用者が TOE 開発者と通信するための手段を持っていることを保証する。開発者に連絡するための手段を持つことにより、利用者は、セキュリティ欠陥の報告、セキュリティ欠陥の状況に関する問い合わせ、及び欠陥に対する訂正の要求を行うことができる。

ALC_FLR.3.10C ***欠陥修正ガイダンスは、TOE 利用者がセキュリティ欠陥報告及び訂正を受け取る資格を得るために開発者へ登録する手段を記述しなければならない。***

ALC_FLR.3-13 評価者は、TOE 利用者が開発者に登録できるようにする手段を欠陥修正ガイダンスが記述することを決定するために、その欠陥修正ガイダンスを***検査しなければならない。***

1223 *TOE 利用者が開発者に登録できるようにする*とは、単純に各 TOE 利用者が開発者に連絡先を提供する方法があることを意味している。この連絡先は、TOE 利用者に影響を与える可能性があるセキュリティ欠陥に関連する情報をセキュリティ欠陥に対する訂正とともに TOE 利用者に提供するために使用される。TOE 利用者の登録は、ソフトウェアライセンスの登録の目的のために、または更新とその他の役立つ情報の取得のために、TOE 利用者が開発者に対して利用者自身を識別するために実行する標準の手続きの一部として達成することができる。

1224 TOE の設置ごとに 1 人の登録された TOE 利用者が存在する必要はない。1 つの組織に対して 1 人の登録された TOE 利用者が存在すれば十分である。例えば、企業の TOE 利用者は、すべての企業のサイトに対応する中央化された購入オフィスを持つ可能性がある。この場合、購入オフィスはすべての TOE 利用者のサイトに対応する十分な連絡先になるため、TOE の TOE 利用者の設置のすべてが登録された連絡先を持つ。

1225 どの場合でも、各 TOE に対して登録された利用者が存在することを保証するには、配付される各 TOE を組織に関連付けることができる必要がある。多数の異なる住所を持つ組織では、これによって、登録された TOE 利用者によって扱われるものと誤って推定される利用者が存在しないことが保証される。

1226 TOE 利用者を登録する必要がないことを注意するべきである。TOE 利用者は登録する手段を提供される必要があるだけである。ただし、登録するように選択する利用者には、情報(または情報の可用性の通知)が直接送信される必要がある。

ALC_FLR.3.11C ***欠陥修正ガイダンスは、TOE に関係するセキュリティ問題に関するすべての報告及び問合せのための特定の連絡先を識別しなければならない。***

ALC_FLR.3-14 評価者は、欠陥修正ガイダンスが TOE に関連するセキュリティ問題に関する利用者の報告及び問い合わせのための特定の連絡先を識別することを決定するために、その欠陥修正ガイダンスを***検査しなければならない。***

1227 ガイダンスには、TOE において検出されたセキュリティ欠陥を報告するために、または TOE において検出されたセキュリティ欠陥に関する問い合わせを行うために、登録された TOE 利用者が開発者と連絡を取り合うために使用する手段が含まれる。

14.7 ライフサイクル定義(ALC_LCD)

14.7.1 サブアクティビティの評価(ALC_LCD.1)

14.7.1.1 目的

1228 このサブアクティビティの目的は、開発者がTOEライフサイクルの証拠資料として提出されたモデルを使用しているかどうかを決定することである。

14.7.1.2 入力

1229 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) ライフサイクル定義証拠資料。

14.7.1.3 アクション ALC_LCD.1.1E

ALC_LCD.1.1C *ライフサイクル定義証拠資料は、TOE の開発及び保守で使用されるモデルを記述しなければならない。*

ALC_LCD.1-1 評価者は、使用されたライフサイクルモデルの証拠資料として提出された記述が、開発と保守のプロセスをカバーしていることを決定するために、その記述を*検査しなければならない。*

1230 ライフサイクルの記述には、次の内容を含めるべきである:

a) TOE のライフサイクルフェーズ及び後続のフェーズとの間の境界についての情報;

b) 開発者が使用する手続き、ツール及び技法(例えば、設計、コーディング、テスト、バグ修正)についての情報;

c) 手続きの適用を決める全体的な管理構造(例えば、ライフサイクルモデルによって扱われる開発や保守のプロセスが必要とする、各手続きに対する個人の責任の識別と記述);

d) 下請け業者が関係する場合、TOE のどの部分が下請け業者によって配付されるかについての情報。

1231 サブアクティビティの評価(ALC_LCD.1)は、使用されるモデルが標準のライフサイクルモデルに従うことを必要としない。

ALC_LCD.1.2C *ライフサイクルモデルは、TOE の開発及び保守で必要な管理方法を提供しなければならない。*

ALC_LCD.1-2 評価者は、ライフサイクルモデルによって記述された手続き、ツール、及び技法の使用が、TOE の開発や保守に必要な明白な貢献を行うことを決定するために、ライフサイクルモデルを*検査しなければならない。*

1232 ライフサイクルモデルに提供される情報は、採用された開発と保守の手続きがセキュリティの欠陥の可能性を最小にするという保証を評価者に与える。例えば、ライフサイクルモデルがレビュープロセスを記述していても、コンポーネントに対する変更を記録する規定がない場合、誤りが TOE にもたらされないという評価者の確信は小さくなくなる。評価者は、モデルの記述と、TOE の開発に関する他の評価者のアクション(例えば、CM 能力(ALC_CMC)で扱われるアクション)を行うことから収集される開発プロセスの理解を比較することにより、さらに確信を得ることができる。ライフサイクルモデルの識別された欠陥は、それらが、当然予想されていたこととして、偶然または故意のいずれかにより TOE に欠陥をもたらすと予想される場合は問題となる。

1233 CC は、特別な開発手法を指定していない。それはメリットにより判断されるべきである。例えば、設計に対するスパイラル、ラピッドプロトタイプ、及びウォータフォールの手法が管理された環境で適用される場合、品質の優れた TOE を作成するためにすべて使用することができる。

14.7.2 サブアクティビティの評価(ALC_LCD.2)

14.7.2.1 目的

1234 このサブアクティビティの目的は、開発者がTOEライフサイクルの証拠資料として提出された、測定可能なモデルを使用しているかどうかを決定することである。

14.7.2.2 入力

1235 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) ライフサイクル定義証拠資料;

c) 使用する基準についての情報;

d) ライフサイクル出力証拠資料。

14.7.2.3 アクション ALC_LCD.2.1E

ALC_LCD.2.1C ***ライフサイクル定義証拠資料は、TOE 及び/または TOE の開発の品質を測定するために使用された数値パラメタ及び/または数値的尺度の詳細を含む、TOE の開発及び保守で使用されるモデルを記述しなければならない。***

ALC_LCD.2-1 評価者は、使用されたライフサイクルモデルの証拠資料として提出された記述が、TOE の開発を測定するのに使用された数値パラメタ及び/または数値的尺度の詳細を含め、開発と保守プロセスを扱っていることを決定するために、その使用されたライフサイクルモデルの証拠資料として提出された記述を***検査しなければならない。***

1236 ライフサイクルモデルの記述には、次の内容を含める:

a) TOE のライフサイクルフェーズ及び後続のフェーズとの間の境界についての情報;

b) 開発者が使用する手続き、ツール及び技法(例えば、設計、コーディング、テスト、バグ修正)についての情報;

c) 手続きの適用を決める全体的な管理構造(例えば、ライフサイクルモデルによって扱われる開発や保守のプロセスが必要とする、各手続きに対する個人の責任の識別と記述);

d) 下請け業者が関係する場合、TOE のどの部分が下請け業者によって配付されるかについての情報;

e) TOE の開発を測定するために使用されるパラメタ/尺度についての情報。尺度の基準は、通常、信頼できる製品の測定と製造のためのガイドを含み、信頼性、品質、性能、複雑性、及びコストの側面を扱う。評価には、これらのすべての尺度が関連し、これらの尺度は、障害の確率を削減することによって品質を向上し、それによって TOE のセキュリティにおける保証を増加するために使用される。

ALC_LCD.2.2C ***ライフサイクルモデルは、TOE の開発及び保守で必要な管理方法を提供しなければならない。***

ALC_LCD.2-2 評価者は、ライフサイクルモデルによって記述された手続き、ツール、及び技法の使用が、TOE の開発や保守に必要な明白な貢献を行うことを決定するために、ライフサイクルモデルを***検査しなければならない。***

1237 ライフサイクルモデルに提供される情報は、採用された開発と保守の手続きがセキュリティの欠陥の可能性を最小にするという保証を評価者に与える。例えば、ライフサイクルモデルがレビュープロセスを記述していても、コンポーネントに対する変更を記録する規定がない場合、誤りが TOE にもたらされないという評価者の確信は小さくなくなる。評価者は、モデルの記述と、TOE の開発に関する他の評価者のアクション(例えば、CM 能力(ALC_CMC)で扱われるアクション)を行うことから収集される開発プロセスの理解を比較することにより、さらに確信を得ることができる。ライフサイクルモデルの識別された欠陥は、それらが、当然予想されていたこととして、偶然または故意のいずれかにより TOE に欠陥をもたらすと予想される場合は問題となる。

1238 CC は、特別な開発手法を指定していない。それはメリットにより判断されるべきである。例えば、設計に対するスパイラル、ラピッドプロトタイプ、及びウォータフォールの手法が管理された環境で適用される場合、品質の優れた TOE を作成するためにすべて使用することができる。

1239 ライフサイクルモデルで使用される尺度/測定については、これらの尺度/測定が欠陥の可能性を最小にすることにどのように有用に貢献するかを示す証拠を提供する必要がある。これは、ALCの枠組みにおける測定の全体的目標とみなすことができる。結果として、尺度/測定は、その全体的目標を達成する能力またはその全体的目標に貢献する能力に基づいて選択する必要がある。まず、尺度/測定の間の相互関係及び欠陥の数を一定の信頼性を伴って示すことができる場合は、尺度/測定はALCに関して適している。ただし、管理が不適切なプロジェクトは品質の劣化を招き、欠陥を引き起こす危険があるため、TOE 開発の計画及び監視に関する管理目的に役立つ尺度/測定も役立つ。

1240 品質の向上用の尺度を使用することができる可能性がある。この尺度の用途は明確ではない。例えば、予測される製品開発の費用を見積もる尺度が開発プロジェクトに対して適切な予算を規定するために使用されること、及びこの尺度によって資源の不足により引き起こされる品質の問題を防ぐのに役立つことを開発者が示すことができる場合は、この尺度は品質の向上に役立つ可能性がある。

1241 TOE のライフサイクルにおけるすべてのステップが測定可能である必要はない。ただし、評価者は、尺度が TOE の全体的な品質を制御し、発生する可能性があるセキュリティ欠陥をこれによって最小にすることに適していることを手段と手続きの記述から確認するべきである。

ALC_LCD.2.3C ***ライフサイクル出力証拠資料は、測定可能なライフサイクルモデルを使用して TOE の開発の測定結果を提供しなければならない。***

ALC_LCD.2-3 評価者は、ライフサイクル出力証拠資料が、測定可能なライフサイクルモデルを使用して、TOE の開発の測定結果を提供することを決定するために、そのライフサイクル出力証拠資料を***検査しなければならない。***

1242 測定結果と TOE のライフサイクルの進み方は、ライフサイクルモデルに従うべきである。

1243 出力証拠資料には、尺度の数値を含めるだけでなく、測定結果とモデルに基づきとられるアクションも記載すべきである。例えば、テスト中に測定されたいくつかのエラーの割合が、定義された閾値の範囲を超えた場合に、特定の設計フェーズを繰返す必要があるという要件があることがある。この場合、証拠資料は、閾値が実際に満たされなかった場合に、このようなアクションがとられたことを示すべきである。

1244 評価が TOE の開発と並行して行われる場合は、過去に品質の測定が使用されていない可能性がある。この場合、評価者は、品質測定の結果が一定の閾値から逸脱している場合に訂正アクションが定義されているという確信を得るために、計画された手続きの証拠資料を使用するべきである。

14.8 ツールと技法(ALC_TAT)

14.8.1 サブアクティビティの評価(ALC_TAT.1)

14.8.1.1 目的

1245 このサブアクティビティの目的は、開発者が、一貫性があり予測可能な結果をもたらす明確に定義された開発ツール(例えば、プログラミング言語またはコンピュータ支援設計(CAD)システム)を使用しているかどうかを決定することである。

14.8.1.2 入力

1246 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 開発ツール証拠資料;

b) 実装表現のサブセット。

14.8.1.3 適用上の注釈

1247 この作業は、オブジェクトコードに影響を与えるツールにおける特徴の使用法(例えば、コンパイルオプション)を決定することに関して特に、実装表現(ADV_IMP)の下の評価アクティビティと並行して行うことができる。

14.8.1.4 アクション ALC_TAT.1.1E

ALC_TAT.1.1C ***実装に使用される各開発ツールは、明確に定義されていなければならない。***

ALC_TAT.1-1 評価者は、各開発ツールが明確に定義されていることを決定するために、提供された開発ツール証拠資料を***検査しなければならない。***

1248 例えば、明確に定義された言語、コンパイラまたは CAD システムは、ISO 標準など、認知された標準に従ったものであるとみなされる。明確に定義された言語は、そのシンタクスが明確かつ完全に記述され、各構文の意味が詳細に記述されている言語である。

ALC_TAT.1.2C ***各開発ツールの証拠資料は、実装に使用されるすべてのステートメントの意味、及び規則と指示文を曖昧さなく定義しなければならない。***

ALC_TAT.1-2 評価者は、各開発ツールの証拠資料が、実装で使用されるすべてのステートメントの意味、及び規則と指示文を曖昧さなく定義していることを決定するために、その証拠資料を***検査しなければならない。***

1249 開発ツール証拠資料(例えば、プログラミング言語仕様書及び利用者マニュアル)では、TOE の実装表現で使用されるすべてのステートメントを扱い、それらの各ステートメントに対して、そのステートメントの目的と効果の明確で曖昧でない定義を提供するべきである。この作業は、ADV_IMPサブアクティビティで行われる評価者の実装表現の検査と並行して行うことができる。評価者が適用すべき重要なテストは、証拠資料が十分に明確であり、評価者が実装表現を理解することができるかどうかである。証拠資料は、(例えば)読者が使用されるプログラミング言語の専門家であることを想定するべきではない。

1250 証拠資料として提出された標準の使用法を参照することは、その標準を評価者が使用できる場合、この要件を満たす受入れ可能な手法である。標準との相違はいずれも証拠資料が提出されるべきである。

1251 決定的に重要なテストは、評価者がADV_IMPサブアクティビティで扱われるソースコード分析を行うときに、TOE ソースコードを理解できるかどうかである。ただし、次のチェックリストを、問題領域を探すために追加して使用することができる:

a) 言語定義において、「この構文の結果が未定義である」などの表現及び「実装に依存」または「誤り」などの用語は、定義が明確でない領域を示すことがある。

b) 別名の使用(同じメモリ部分を異なる方法で参照できるようにする)は、よくある曖昧さの問題の発生源である。

c) 例外処理(例えば、メモリが不足したりスタックがオーバフローしたときに発生する)は、多くの場合、定義が不完全である。

1252 しかしながら、普通に使用されているほとんどの言語は、十分に定義されているが、いくつかの問題となる構文を持っている。実装言語がほとんど十分に定義されているが、いくつかの問題となる構文が存在する場合、ソースコードの検査を終えるまで、未決定判定を割り付けられるべきである。

1253 評価者は、ソースコードを検査する間、問題のある構文の使用法が脆弱性を持ち込んでいないことを検証するべきである。評価者は、証拠資料として提出された標準によって排除されている構文が使用されていないことも保証するべきである。

1254 開発ツール証拠資料は、実装で使用されるすべての規則と指示文を定義するべきである。

ALC_TAT.1.3C ***各開発ツールの証拠資料は、実装に依存するすべてのオプションの意味を、曖昧さなく定義しなければならない。***

ALC_TAT.1-3 評価者は、開発ツール証拠資料がすべての実装に依存するオプションの意味を曖昧さなく定義していることを決定するために、その証拠資料を***検査しなければならない。***

1255 ソフトウェア開発ツールの証拠資料には、実行可能コードの意味に影響を与える実装依存オプションの定義と、証拠資料として提出された標準言語と異なるオプションの定義を含めるべきである。ソースコードが評価者に提供される場合、使用されたコンパイルとリンクのオプションの情報も提供されるべきである。

1256 ハードウェア設計及び開発ツールの証拠資料は、ツール(例えば、詳細なハードウェア仕様または実際のハードウェア)からの出力に影響を与えるすべてのオプションの使用法を記述するべきである。

14.8.2 サブアクティビティの評価(ALC_TAT.2)

14.8.2.1 目的

1257 このサブアクティビティの目的は、開発者が、一貫性があり予測可能な結果をもたらす明確に定義された開発ツール(例えば、プログラミング言語またはコンピュータ支援設計(CAD)システム)を使用しているかどうか、及び実装標準が適用されているかどうかを決定することである。

14.8.2.2 入力

1258 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 開発ツール証拠資料;

b) 実装標準記述;

c) TSF の提供された実装表現。

14.8.2.3 適用上の注釈

1259 この作業は、オブジェクトコードに影響を与えるツールにおける特徴の使用法(例えば、コンパイルオプション)を決定することに関して特に、ADV_IMPの下の評価アクティビティと並行して行うことができる。

14.8.2.4 アクション ALC_TAT.2.1E

ALC_TAT.2.1C ***実装に使用される各開発ツールは、明確に定義されていなければならない。***

ALC_TAT.2-1 評価者は、各開発ツールが明確に定義されていることを決定するために、提供された開発ツール証拠資料を***検査しなければならない。***

1260 例えば、明確に定義された言語、コンパイラまたは CAD システムは、ISO 標準など、認知された標準に従ったものであるとみなされる。明確に定義された言語は、そのシンタクスが明確かつ完全に記述され、各構文の意味が詳細に記述されている言語である。

ALC_TAT.2.2C ***各開発ツールの証拠資料は、実装に使用されるすべてのステートメントの意味、及び規則と指示文を曖昧さなく定義しなければならない。***

ALC_TAT.2-2 評価者は、各開発ツールの証拠資料が、実装で使用されるすべてのステートメントの意味、及び規則と指示文を曖昧さなく定義していることを決定するために、その証拠資料を***検査しなければならない。***

1261 開発ツール証拠資料(例えば、プログラミング言語仕様書及び利用者マニュアル)では、TOE の実装表現で使用されるすべてのステートメントを扱い、それらの各ステートメントに対して、そのステートメントの目的と効果の明確で曖昧でない定義を提供するべきである。この作業は、ADV_IMPサブアクティビティで行われる評価者の実装表現の検査と並行して行うことができる。評価者が適用すべき重要なテストは、証拠資料が十分に明確であり、評価者が実装表現を理解することができるかどうかである。証拠資料は、(例えば)読者が使用されるプログラミング言語の専門家であることを想定するべきではない。

1262 証拠資料として提出された標準の使用法を参照することは、その標準を評価者が使用できる場合、この要件を満たす受入れ可能な手法である。標準との相違はいずれも証拠資料が提出されるべきである。

1263 決定的に重要なテストは、評価者がADV_IMPサブアクティビティで扱われるソースコード分析を行うときに、TOE ソースコードを理解できるかどうかである。ただし、次のチェックリストを、問題領域を探すために追加して使用することができる:

a) 言語定義において、「この構文の結果が未定義である」などの表現及び「実装に依存」または「誤り」などの用語は、定義が明確でない領域を示すことがある。

b) 別名の使用(同じメモリ部分を異なる方法で参照できるようにする)は、よくある曖昧さの問題の発生源である。

c) 例外処理(例えば、メモリが不足したりスタックがオーバフローしたときに発生する)は、多くの場合、定義が不完全である。

1264 しかしながら、普通に使用されているほとんどの言語は、十分に定義されているが、いくつかの問題となる構文を持っている。実装言語がほとんど十分に定義されているが、いくつかの問題となる構文が存在する場合、ソースコードの検査を終えるまで、未決定判定を割り付けられるべきである。

1265 評価者は、ソースコードを検査する間、問題のある構文の使用法が脆弱性を持ち込んでいないことを検証するべきである。評価者は、証拠資料として提出された標準によって排除されている構文が使用されていないことも保証するべきである。

1266 開発ツール証拠資料は、実装で使用されるすべての規則と指示文を定義するべきである。

ALC_TAT.2.3C ***各開発ツールの証拠資料は、実装に依存するすべてのオプションの意味を、曖昧さなく定義しなければならない。***

ALC_TAT.2-3 評価者は、開発ツール証拠資料がすべての実装に依存するオプションの意味を曖昧さなく定義していることを決定するために、その証拠資料を***検査しなければならない。***

1267 ソフトウェア開発ツールの証拠資料には、実行可能コードの意味に影響を与える実装依存オプションの定義と、証拠資料として提出された標準言語と異なるオプションの定義を含めるべきである。ソースコードが評価者に提供される場合、使用されたコンパイルとリンクのオプションの情報も提供されるべきである。

1268 ハードウェア設計及び開発ツールの証拠資料は、ツール(例えば、詳細なハードウェア仕様または実際のハードウェア)からの出力に影響を与えるすべてのオプションの使用法を記述するべきである。

14.8.2.5 **アクション** ALC_TAT.2.2E

ALC_TAT.2-4 評価者は、証拠資料として提出された実装標準が適用されていることを決定するために、実装プロセスの側面を***検査しなければならない。***

1269 このワークユニットでは、証拠資料として提出された実装標準が適用されているかどうかを決定するために、評価者は TOE の提供された実装表現を分析する必要がある。

1270 評価者は、証拠資料として提出された標準によって排除されている構文が使用されていないことを検証するべきである。

1271 また、評価者は、TOE の設計及び実装プロセス内の定義された標準の適用を保証する開発者の手続きを検証するべきである。このため、記録による証拠は、開発環境を訪問することによって補足されるべきである。開発環境を訪問することにより、評価者は、次のことを行うことができる:

a) 定義された標準の適用の観察;

b) 定義された標準の使用を記述している手続きの適用の記録による証拠の検査;

c) 開発スタッフへのインタビューによる、定義された標準と手続きの適用についての認識のチェック。

1272 開発サイトの訪問は、使用されている手続きに対する確信を得るのに役に立つ手段である。そのような訪問を行わないという決定は、評価監督機関と相談して決定されるべきである。

1273 評価者は、提供された実装表現と適用された実装標準の記述を比較し、それらの使用を検証する。

1274 このレベルでは、TSF の完全な提供された実装表現は実装標準に基づいている必要はないが、TOE 開発者自身が開発した部分のみはこの必要がある。評価者は、TOE 開発者が開発するのはどの部分か、及びサードパーティの開発者が開発するのはどの部分かについての情報を取得するために、CM 範囲(ALC_CMS)で要求される構成リストを調べることができる。

1275 参照される実装標準が提供された実装表現の少なくともいずれかの部分に対して適用されていない場合、このワークユニットに関する評価者アクションは不合格判定になる。

1276 TSF 関連ではない TOE の部分を検査する必要はないことに注意のこと。

1277 このワークユニットは、ADV_IMPの下で評価アクティビティとともに実行することができる。

14.8.3 サブアクティビティの評価(ALC_TAT.3)

14.8.3.1 目的

1278 このサブアクティビティの目的は、開発者及びその下請け業者が、一貫性があり予測可能な結果をもたらす明確に定義された開発ツール(例えば、プログラミング言語やコンピュータ支援設計(CAD)システム)を使用しているかどうか、及び実装標準が適用されているかどうかを決定することである。

14.8.3.2 入力

1279 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 開発ツール証拠資料;

b) 実装標準記述;

c) TSF の提供された実装表現。

14.8.3.3 適用上の注釈

1280 この作業は、オブジェクトコードに影響を与えるツールにおける特徴の使用法(例えば、コンパイルオプション)を決定することに関して特に、ADV_IMPの下の評価アクティビティと並行して行うことができる。

14.8.3.4 アクション ALC_TAT.3.1E

ALC_TAT.3.1C ***実装に使用される各開発ツールは、明確に定義されていなければならない。***

ALC_TAT.3-1 評価者は、各開発ツールが明確に定義されていることを決定するために、提供された開発ツール証拠資料を***検査しなければならない。***

1281 例えば、明確に定義された言語、コンパイラまたは CAD システムは、ISO 標準など、認知された標準に従ったものであるとみなされる。明確に定義された言語は、そのシンタクスが明確かつ完全に記述され、各構文の意味が詳細に記述されている言語である。

1282 このレベルでは、TOE に対するサードパーティの貢献者が使用する開発ツールの証拠資料は、評価者の検査に含まれる必要がある。

ALC_TAT.3.2C ***各開発ツールの証拠資料は、実装に使用されるすべてのステートメントの意味、及び規則と指示文を曖昧さなく定義しなければならない。***

ALC_TAT.3-2 評価者は、各開発ツールの証拠資料が、実装で使用されるすべてのステートメントの意味、及び規則と指示文を曖昧さなく定義していることを決定するために、その証拠資料を***検査しなければならない。***

1283 開発ツール証拠資料(例えば、プログラミング言語仕様書及び利用者マニュアル)では、TOE の実装表現で使用されるすべてのステートメントを扱い、それらの各ステートメントに対して、そのステートメントの目的と効果の明確で曖昧でない定義を提供するべきである。この作業は、ADV_IMP サブアクティビティで行われる評価者の実装表現の検査と並行して行うことができる。評価者が適用すべき重要なテストは、証拠資料が十分に明確であり、評価者が実装表現を理解することができるかどうかである。証拠資料は、(例えば)読者が使用されるプログラミング言語の専門家であることを想定するべきではない。

1284 証拠資料として提出された標準の使用法を参照することは、その標準を評価者が使用できる場合、この要件を満たす受入れ可能な手法である。標準との相違はいずれも証拠資料が提出されるべきである。

1285 決定的に重要なテストは、評価者がADV_IMPサブアクティビティで扱われるソースコード分析を行うときに、TOE ソースコードを理解できるかどうかである。ただし、次のチェックリストを、問題領域を探すために追加して使用することができる:

a) 言語定義において、「この構文の結果が未定義である」などの表現及び「実装に依存」または「誤り」などの用語は、定義が明確でない領域を示すことがある。

b) 別名の使用(同じメモリ部分を異なる方法で参照できるようにする)は、よくある曖昧さの問題の発生源である。

c) 例外処理(例えば、メモリが不足したりスタックがオーバフローしたときに発生する)は、多くの場合、定義が不完全である。

1286 しかしながら、普通に使用されているほとんどの言語は、十分に定義されているが、いくつかの問題となる構文を持っている。実装言語がほとんど十分に定義されているが、いくつかの問題となる構文が存在する場合、ソースコードの検査を終えるまで、未決定判定を割り付けられるべきである。

1287 評価者は、ソースコードを検査する間、問題のある構文の使用法が脆弱性を持ち込んでいないことを検証するべきである。評価者は、証拠資料として提出された標準によって排除されている構文が使用されていないことも保証するべきである。

1288 開発ツール証拠資料は、実装で使用されるすべての規則と指示文を定義するべきである。

1289 このレベルでは、TOE に対するサードパーティの貢献者が使用する開発ツールの証拠資料は、評価者の検査に含まれる必要がある。

ALC_TAT.3.3C *各開発ツールの証拠資料は、実装に依存するすべてのオプションの意味を、曖昧さなく定義しなければならない。*

ALC_TAT.3-3 評価者は、開発ツール証拠資料がすべての実装に依存するオプションの意味を曖昧さなく定義していることを決定するために、その証拠資料を***検査しなければならない。***

1290 ソフトウェア開発ツールの証拠資料には、実行可能コードの意味に影響を与える実装依存オプションの定義と、証拠資料として提出された標準言語と異なるオプションの定義を含めるべきである。ソースコードが評価者に提供される場合、使用されたコンパイルとリンクのオプションの情報も提供されるべきである。

1291 ハードウェア設計及び開発ツールの証拠資料は、ツール(例えば、詳細なハードウェア仕様または実際のハードウェア)からの出力に影響を与えるすべてのオプションの使用法を記述するべきである。

1292 このレベルでは、TOE に対するサードパーティの貢献者が使用する開発ツールの証拠資料は、評価者の検査に含まれる必要がある。

14.8.3.5 アクション ALC_TAT.3.2E

ALC_TAT.3-4 評価者は、証拠資料として提出された実装標準が適用されていることを決定するために、実装プロセスの側面を***検査しなければならない。***

1293 このワークユニットでは、証拠資料として提出された実装標準が適用されているかどうかを決定するために、評価者は TOE の提供された実装表現を分析する必要がある。

1294 評価者は、証拠資料として提出された標準によって排除されている構文が使用されていないことを検証するべきである。

1295 また、評価者は、TOE の設計及び実装プロセス内の定義された標準の適用を保証する開発者の手続きを検証するべきである。このため、記録による証拠は、開発環境を訪問することによって補足されるべきである。開発環境を訪問することにより、評価者は、次のことを行うことができる:

a) 定義された標準の適用の観察;

b) 定義された標準の使用を記述している手続きの適用の記録による証拠の検査;

c) 開発スタッフへのインタビューによる、定義された標準と手続きの適用についての認識のチェック。

1296 開発サイトの訪問は、使用されている手続きに対する確信を得るのに役に立つ手段である。そのような訪問を行わないという決定は、評価監督機関と相談して決定されるべきである。

1297 評価者は、提供された実装表現と適用された実装標準の記述を比較し、それらの使用を検証する。

1298 このレベルでは、TSF の完全な提供された実装表現は、サードパーティの貢献を含め、実装標準に基づいている必要がある。このため、評価者が貢献者のサイトを訪問する必要がある可能性がある。評価者は、TOE のどの部分をだれが開発したかを確認するために、CM 範囲(ALC_CMS)で要求される構成リストを調べることができる。

1299 TSF 関連ではない TOE の部分を検査する必要はないことに注意のこと。

1300 このワークユニットは、ADV_IMPの下で評価アクティビティとともに実行することができる。

15 ATE クラス: テスト

15.1 序説

1301 このアクティビティの目的は、TOE が ST での記述に従って、及び(ADVクラスで記述された)評価証拠での仕様に従ってふるまうかどうかを決定することである。この決定は、TSF の開発者自身の機能テスト(機能テスト(ATE_FUN))と評価者による TSF の独立テスト(独立テスト(ATE_IND))をいくつか組み合わせることによって達成される。保証の最小レベルでは、開発者の関与についての要件はないため、テストは評価者によってのみ TOE に関する限られた利用可能な情報を使用して行われる。TOE に関する追加情報のテストと提供の両方に対する開発者の関与が深まるにつれて、また評価者による独立テストアクティビティが増加するにつれて、追加の保証が得られる。

15.2 適用上の注釈

1302 TSF のテストは、評価者によって、またほとんどの場合は開発者によって行われる。評価者のテスト成果は、独自のテストの作成及び実行だけでなく、開発者テストの適切性の評定とそれらのサブセットの再実行を含むものとする。

1303 評価者は、TSFI (機能仕様(ADV_FSP)を参照のこと)が仕様のとおりに動作することを実証するために、及び開発者のテスト手法を理解するために、開発者のテストが十分であるかを決定するためそれらテストの分析をする。同様に、評価者は、TSF の内部的なふるまいと特性を実証するために開発者のテストが十分であるかを決定するために、それらのテストを分析する。

1304 評価者は、開発者のテスト結果に対し確信を得るために、提出された証拠資料に従って開発者のテストのサブセットも実行する。評価者は、この分析結果をTSFサブセットの独立テストへの入力として使用する。このサブセットに関して評価者は、特に開発者のテストに不足がある場合に、開発者のものとは異なるテスト手法をとる。

1305 開発者のテスト証拠資料の適切性を決定するため、または新しいテストを作成するために、評価者は、満たす必要がある SFR において、TSF の望ましい期待されるふるまいを内部的及び TSFI の観点から理解する必要がある。評価者は、まだ ST で分割されていなければ TSF 及び TSFI を ST の機能領域(監査サブシステム、監査関連 TSFI、認証モジュール、認証関連 TSFI など)に従い複数のサブセットに分割し、1 度に 1 つのサブセットに焦点を当てて、ST 要件と開発及びガイダンス証拠資料の関連する部分を検査し TOE の期待されるふるまい方を理解することができる。開発証拠資料に対するこの依存は、カバレージ(ATE_COV)及び深さ(ATE_DPT)はADVへの依存性が必要になることにより強調される。

1306 CC は、カバレージと深さを機能テストから分離し、ファミリのコンポーネントの適用に関する柔軟性を高めている。ただし、それらファミリの要件は、TSF がその仕様に従って動くことを確認するために、一体となって適用されることを意図している。ファミリのこの密接なつながりは、サブアクティビティ間の評価者ワークユニットの一部重複をもたらした。これらの適用上の注釈は、サブアクティビティ間の文の重複をできる限り少なくするために使用される。

15.2.1 TOE の期待されるふるまいの理解

1307 テスト証拠資料の適切性を正確に評価する前に、または新しいテストを作成する前に、評価者は、満たす必要がある要件の観点よりセキュリティ機能の望ましい期待されるふるまいを理解する必要がある。

1308 前述のとおり、評価者は、ST における SFR (監査、認証など)に従って TSF 及び TSFI をサブセットに分割し、1 度に 1 つのサブセットに焦点を当てるように選択することができる。評価者は、関連する TSFI の期待されるふるまい方を理解するために、各 ST 要件と、機能仕様及びガイダンス証拠資料の関連部分を検査する。同様に、評価者は、TSF の関連するモジュールまたはサブシステムの期待されるふるまい方を理解するために、TOE 設計及びセキュリティアーキテクチャ証拠資料の関連する部分を検査する。

1309 期待されるふるまいの理解とともに、評価者はテスト計画を検査し、テスト手法を理解する。ほとんどの場合、テスト手法は、刺激される TSFI とその観察される応答を伴う。外部から見える機能性は、原則としては直接テストすることが可能だが、機能性が TOE の外部から見えない場合(例えば、残存情報保護機能性のテスト)は、別の手段を採用する必要がある。

15.2.2 機能性の期待されるふるまいを検証するための、テストとその代替手法

1310 (外部から見える TSFI が提供されない場合に)特定の機能性をテストするのが実際的でないかまたは適切でない場合、テスト計画では、期待されるふるまいを検証するための代替手法を識別するべきである。代替手法の適切さを決定するのは、評価者の責任である。ただし、代替手法の適切さを評定するとき、次のことが考慮されるべきである:

a) 必要なふるまいが TOE によって示されるべきであることを決定するための実装表現の分析は、容認される代替手法である。これは、ソフトウェア TOE のコード検査またはハードウェア TOE のチップマスク検査に相当する。

b) たとえ主張された保証要件に TOE モジュール(例えば、サブアクティビティの評価(ADV_TDS.3))または実装(実装表現(ADV_IMP))の下位レベルの記述が含まれない場合でも、開発者の統合またはモジュールテストの証拠を使用することは容認される。開発者の統合またはモジュールテストの証拠がセキュリティ機能性の期待されるふるまいを検証するために使用される場合、テストの証拠は TOE の現在の実装を反映していることを注意深く確認すべきである。テストが行われた後にサブシステムまたはモジュールが変更された場合には、通常、その変更が追跡され、分析またはその後のテストにより対処された証拠が必要となる。

1311 代替手法でテスト成果を補足するのは、開発者と評価者の両者が期待されるふるまいをテストする実際的な手段が他に存在しないと決定したときにのみ行うべきであることが強調されるべきである。

15.2.3 テストの適切性の検証

1312 テストの必要条件は、テストのために必要な初期条件を確立するために必要である。それらは、セットする必要があるパラメタとして、または 1 つのテストの完了が他のテストの必要条件を確立する場合にはテストの順序として表すことができる。評価者は、必要条件が観察されたテスト結果を期待されたテスト結果へ偏らせることがないという点で、完全かつ適切であることを決定する必要がある。

1313 テストステップと期待される結果は、検証されるべき方法と期待される結果のみならず、TSFI に適用されるアクションとパラメタを特定する。評価者は、テストステップと期待される結果が機能仕様におけるTSFIの記述と一貫していることを決定しなければならない。このことは、機能仕様に明示的に記述されている TSFI ふるまいの各特性が、そのふるまいを検証するためのテスト結果と期待される結果を持つべきであることを意味する。

1314 このテストアクティビティの全体的な目的は、各サブシステム、モジュール、及び TSFI が、機能仕様、TOE 設計、及びアーキテクチャ記述でのふるまいの主張に対して十分にテストされていることを決定することである。より上位の保証レベルでは、テストに境界テスト及び否定テストも含まれる。テスト手順は、テスト中に開発者によってどのように TSFI、モジュール、及びサブシステムが実行されたかに関する洞察を提供する。評価者は、TSF を独立にテストするための追加のテストを開発するときに、この情報を使用する。

15.3 カバレージ(ATE_COV)

15.3.1 サブアクティビティの評価(ATE_COV.1)

15.3.1.1 目的

1315 このサブアクティビティの目的は、開発者が TSFI をテストしたかどうか、及び開発者のテストカバレージ証拠がテスト証拠資料に識別されているテストと機能仕様に記述されている TSFI の間の対応を示していることを決定することである。

15.3.1.2 入力

1316 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) テスト証拠資料;

d) テストカバレージ証拠。

15.3.1.3 適用上の注釈

1317 開発者が提供するカバレージ分析は、評価証拠として提供されるテストと機能仕様の間の対応を示す必要がある。ただし、カバレージ分析は、すべての TSFI がテストされていること、または TOE へのすべての外部から見えるインタフェースがテストされていることを実証する必要はない。そのような不足は、独立テスト(サブアクティビティの評価(ATE_IND.2))サブアクティビティ中に評価者が考慮する。

15.3.1.4 アクション ATE_COV.1.1E

ATE_COV.1.1C ***テストカバレージの証拠は、テスト証拠資料におけるテストと機能仕様における TSFI との間の対応を提示しなければならない。***

ATE_COV.1-1 評価者は、テスト証拠資料に識別されているテストと機能仕様に記述されている TSFI の間の対応が正確であることを決定するために、テストカバレージ証拠を***検査しなければならない。***

1318 対応は、表またはマトリックスの形を取ることができる。このコンポーネントに必要となるカバレージ証拠は、完全なカバレージを示すことよりむしろ、カバレージの範囲を明らかにする。カバレージが十分でない場合、評価者は、補うために独立テストの水準を増すべきである。

15.3.2 サブアクティビティの評価(ATE_COV.2)

15.3.2.1 目的

1319 このサブアクティビティの目的は、開発者がすべての TSFI をテストしたかどうか、及び開発者のテストカバレージ証拠がテスト証拠資料に識別されているテストと機能仕様に記述されている TSFI の間の対応を示していることを決定することである。

15.3.2.2 **入力**

a) ST;

b) 機能仕様;

c) テスト証拠資料;

d) テストカバレージ分析。

15.3.2.3 **アクション** ATE_COV.2.1E

ATE_COV.2.1C ***テストカバレージの分析は、テスト証拠資料におけるテストと機能仕様における TSFI との間の対応を実証しなければならない。***

ATE_COV.2-1 評価者は、テスト証拠資料におけるテストと機能仕様におけるインタフェースの間の対応が正確であることを決定するために、テストカバレージ分析を***検査しなければならない。***

1320 単純な相互表によりテストの対応を十分に示すことができる。テストカバレージ分析に示されるテストとインタフェースの識別は、曖昧さをなくす必要がある。

1321 評価者は、これが、テスト証拠資料におけるすべてのテストが機能仕様におけるインタフェースにマッピングされる必要があることを暗示していないことに留意する。

ATE_COV.2-2 評価者は、各インタフェースに対するテスト手法が、そのインタフェースの期待されるふるまいを実証することを決定するために、テスト計画を***検査しなければならない。***

1322 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

ATE_COV.2-3 評価者は、テストの必要条件、テストステップ、及び期待される結果が各インタフェースを適切にテストしていることを決定するために、テスト手順を***検査しなければならない。***

1323 このワークユニットのガイダンスは、機能仕様に関係しており、次の中に見つけることができる:

a) 15.2.3、テストの適切性の検証

ATE_COV.2.2C ***テストカバレージの分析は、機能仕様におけるすべての TSFI がテストされていることを実証しなければならない。***

ATE_COV.2-4 評価者は、機能仕様におけるインタフェースとテスト証拠資料におけるテストの間の対応が完全であることを決定するために、テストカバレージ分析を***検査しなければならない。***

1324 完全性を主張するために、機能仕様に記述されているすべての TSFI をテストカバレージ分析に示し、テストにマッピングする必要がある。ただし、インタフェースの徹底的な仕様テストは必要ない。インタフェースが機能仕様に識別されており、それに対してテストがマッピングされていなかった場合、カバレージが不完全であることは明らかである。

1325 評価者は、これが、テスト証拠資料におけるすべてのテストが機能仕様におけるインタフェースにマッピングされる必要があることを暗示していないことに留意する。

15.3.3 サブアクティビティの評価(ATE_COV.3)

1326 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

15.4 深さ(ATE_DPT)

15.4.1 サブアクティビティの評価(ATE_DPT.1)

15.4.1.1 目的

1327 このサブアクティビティの目的は、開発者が TSF サブシステムを TOE 設計及びセキュリティアーキテクチャ記述と比較してテストしたかどうかを決定することである。

15.4.1.2 入力

a) ST;

b) 機能仕様;

c) TOE 設計;

d) セキュリティアーキテクチャ記述;

e) テスト証拠資料;

f) テストの深さ分析。

15.4.1.3 アクション ATE_DPT.1.1E

ATE_DPT.1.1C ***テストの深さの分析は、テスト証拠資料におけるテストと TOE 設計における TSF サブシステムの間の対応を実証しなければならない。***

ATE_DPT.1-1 評価者は、TSF サブシステムのふるまいの記述及びそれらの相互作用の記述がテスト証拠資料に含まれていることを決定するために、テストの深さ分析を***検査しなければならない。***

1328 このワークユニットは、テストと TOE 設計の記述との間の対応の内容を検証する。TSF のアーキテクチャへの信頼の記述(セキュリティアーキテクチャ(ADV_ARC)での)で、特定のメカニズムが挙げられている場合、このワークユニットはテストとそれらメカニズムのふるまいの記述との間の対応も検証する。

1329 単純な相互表がテストの対応を十分に示すことができる。カバレージの深さ分析に示されるテストとふるまい/相互作用の識別は、曖昧さをなくす必要がある。

1330 サブアクティビティ(ATE_DPT.1)の評価が、モジュールレベル(例えばサブアクティブティ(ADV_TDS.3)の評価)の記述を含むTOE設計(ADV_TDS)のコンポーネントと組み合わせて行われる場合、テストケースとサブシステムのふるまいをマップするために必要とされる詳細のレベルは、使用されるモジュール記述からの情報を要求するかもしれない。これは、サブアクティビティ(ADV_TDS.3)の評価は、サブシステムレベルをモジュールレベルにする、つまり、サブシステムを完全に省略してしまうような詳細の記述も許可するためである。

1331 どの場合でも、テストされたふるまいに関して提供された詳細に求められるレベルは、サブアクティビティ(ADV_TDS.2)の評価により定義されるサブシステムのふるまいの記述に対し要求される詳細のレベルと定義することが出来る。(特にワークユニット ADV_TDS.2-4)ふるまいの詳細記述は、通常どのように機能が提供されるのか、つまりどんな主要なデータ及びデータ構造が表現されているのか、どんな制御関係がサブシステムの中に存在しているか、そして、これらの要素は、SFR 実施のふるまいを提供するためにどう一緒に働いているかを説明すると述べている。

1332 評価者は、テスト証拠資料におけるすべてのテストがサブシステムのふるまいまたは相互作用の記述にマッピングされる必要があるわけではないことに留意する。

ATE_DPT.1-2 評価者は、ふるまいの記述に対するテスト手法が、TOE 設計に記述されているそのサブシステムのふるまいを実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1333 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1334 サブアクティビティ(ATE_DPT.1)の評価が、モジュールレベル(例えばサブアクティブティ(ADV_TDS.3)の評価)の記述を含むTOE設計(ADV_TDS)のコンポーネントと組み合わせて行われる場合、テストケースとサブシステムのふるまいをマップするために必要とされる詳細のレベルは、使用されるモジュール記述からの情報を要求するかもしれない。これは、サブアクティビティ(ADV_TDS.3)の評価は、サブシステムレベルをモジュールレベルにする、つまり、サブシステムを完全に省略してしまうような詳細の記述も許可するためである。

1335 どの場合でも、テストされたふるまいに関して提供された詳細に求められるレベルは、サブアクティビティ(ADV_TDS.2)の評価により定義されるサブシステムのふるまいの記述に対し要求される詳細のレベルと定義することが出来る。(特にワークユニット ADV_TDS.2-4)ふるまいの詳細記述は、通常どのように機能が提供されるのか、つまりどんな主要なデータ及びデータ構造が表現されているのか、どんな制御関係がサブシステムの中に存在しているか、そして、これらの要素は、SFR 実施のふるまいを提供するためにどう一緒に働いているかを説明すると述べている。

1336 TSF サブシステムのインタフェースが記述されている場合、それらのサブシステムのふるまいをそれらのインタフェースから直接テストすることができる。それ以外の場合、それらのサブシステムのふるまいは TSFI インタフェースからテストされる。あるいは、この 2 つのテストの組み合わせを採用することができる。どのような方策が使用される場合でも、評価者は、TOE 設計に記述されているふるまいを適切にテストするための妥当性を考慮する。

ATE_DPT.1-3 評価者は、ふるまいの記述に対するテスト手法が、TOE 設計に記述されているサブシステム間の相互作用を実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1337 前のワークユニットではサブシステムのふるまいを扱っているが、このワークユニットではサブシステム間の相互作用を扱う。

1338 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1339 TSF サブシステムのインタフェースが記述されている場合、他のサブシステムとの相互作用をそれらのインタフェースから直接テストすることができる。それ以外の場合、サブシステム間の相互作用は TSFI インタフェースから推測されなければならない。どのような方策が使用される場合でも、評価者は、TOE 設計に記述されているサブシステム間の相互作用を適切にテストするための妥当性を考慮する。

ATE_DPT.1.2C *テストの深さの分析は、TOE 設計内のすべての TSF サブシステムがテストされていることを実証しなければならない。*

ATE_DPT.1-4 評価者は、TSF サブシステムのふるまい及び相互作用のすべての記述がテストされることを決定するために、テスト手順を*検査しなければならない。*

1340 このワークユニットは、ワークユニット ATE_DPT.1-1 の完全性を検証する。TOE 設計で提供されている、TSF サブシステムのふるまいの記述及び TSF サブシステム間の相互作用のすべての記述がテストされなければならない。TSF サブシステムのふるまいの記述または TSF サブシステム間の相互作用の記述が TOE 設計で識別されているが、それに対するテストが示されない場合、テストの深さが不完全であることは明らかである。

1341 サブアクティビティ(ATE_DPT.1)の評価が、モジュールレベル(例えばサブアクティブティ(ADV_TDS.3)の評価)の記述を含むTOE設計(ADV_TDS)のコンポーネントと組み合わせて行われる場合、テストケースとサブシステムのふるまいをマップするために必要とされる詳細のレベルは、使用されるモジュール記述からの情報を要求するかもしれない。これは、サブアクティビティ(ADV_TDS.3)の評価は、サブシステムレベルをモジュールレベルにする、つまり、サブシステムを完全に省略してしまうような詳細の記述も許可するためである。

1342 どの場合でも、テストされたふるまいに関して提供された詳細に求められるレベルは、サブアクティビティ(ADV_TDS.2)の評価により定義されるサブシステムのふるまいの記述に対し要求される詳細のレベルと定義することが出来る。(特にワークユニット ADV_TDS.2-4)ふるまいの詳細記述は、通常どのように機能が提供されるのか、つまりどんな主要なデータ及びデータ構造が表現されているのか、どんな制御関係がサブシステムの中に存在しているか、そして、これらの要素は、SFR 実施のふるまいを提供するためにどう一緒に働いているかを説明すると述べている。

1343 評価者は、これが、テスト証拠資料におけるすべてのテストが TOE 設計におけるサブシステムのふるまい、または相互作用の記述にマッピングされる必要があることを暗示していないことに留意する。

15.4.2 サブアクティビティの評価(ATE_DPT.2)

15.4.2.1 目的

1344 このサブアクティビティの目的は、開発者が全 TSF サブシステムと SFR 実施モジュールを TOE 設計及びセキュリティアーキテクチャの記述と比較してテストしたかどうかを決定することである。

15.4.2.2 **入力**

a) ST;

b) 機能仕様;

c) TOE 設計;

d) セキュリティアーキテクチャ記述;

e) テスト証拠資料;

f) テストの深さ分析。

15.4.2.3 **アクション** ATE_DPT.2.1E

ATE_DPT.2.1C ***テストの深さの分析は、テスト証拠資料におけるテストと TOE 設計における TSF サブシステム及びSFR実施モジュールの間の対応を実証しなければならない。***

ATE_DPT.2-1 評価者は、TSF サブシステムのふるまいの記述とそれらの相互作用の記述がテスト証拠資料に含まれていることを決定するために、テストの深さ分析を***検査しなければならない。***

1345 このワークユニットは、テストと TOE 設計の記述との間の対応の内容を検証する。TSF のアーキテクチャへの信頼の記述(セキュリティアーキテクチャ(ADV_ARC)での)で特定のメカニズムが挙げられている場合、このワークユニットはテストとそれらメカニズムのふるまいの記述との間の対応も検証する。

1346 単純な相互表がテストの対応を十分に示すことができる。カバレージの深さ分析に示されるテストとふるまい/相互作用の識別は、曖昧さをなくす必要がある。

1347 評価者は、テスト証拠資料におけるすべてのテストがサブシステムのふるまいまたは相互作用の記述にマッピングされる必要があるわけではないことに留意する。

ATE_DPT.2-2 評価者は、ふるまいの記述に対するテスト手法が、TOE 設計に記述されているそのサブシステムのふるまいを実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1348 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1349 TSF サブシステムのインタフェースが記述されている場合、それらのサブシステムのふるまいをそれらのインタフェースから直接テストすることができる。それ以外の場合、それらのサブシステムのふるまいは TSFI インタフェースからテストされる。あるいは、この 2 つのテストの組み合わせを採用することができる。どのような方策が使用される場合でも、評価者は、TOE 設計に記述されているふるまいを適切にテストするための妥当性を考慮する。

ATE_DPT.2-3 評価者は、ふるまいの記述に対するテスト手法が、TOE 設計に記述されているサブシステム間の相互作用を実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1350 前のワークユニットではサブシステムのふるまいを扱っているが、このワークユニットではサブシステム間の相互作用を扱う。

1351 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1352 TSF サブシステムのインタフェースが記述されている場合、他のサブシステムとの相互作用をそれらのインタフェースから直接テストすることができる。それ以外の場合、サブシステム間の相互作用は TSFI インタフェースから推測されなければならない。どのような方策が使用される場合でも、評価者は、TOE 設計に記述されているサブシステム間の相互作用を適切にテストするための妥当性を考慮する。

ATE_DPT.2-4 評価者は、SFR 実施モジュールのインタフェースがテスト証拠資料に含まれていることを決定するために、テストの深さ分析を***検査しなければならない。***

1353 このワークユニットは、テストと TOE 設計の記述との間の対応の内容を検証する。TSF のアーキテクチャへの信頼の記述(セキュリティアーキテクチャ(ADV_ARC)での)で、モジュールレベルでの特定のメカニズムが挙げられている場合、このワークユニットはテストとそれらメカニズムのふるまいの記述との間の対応も検証する。

1354 単純な相互表がテストの対応を十分に示すことができる。カバレージの深さ分析に示されるテストと SFR 実施モジュールの識別は、曖昧さをなくす必要がある。

1355 評価者は、テスト証拠資料におけるすべてのテストが SFR 実施モジュールのインタフェースにマッピングされる必要があるわけではないことに留意する。

ATE_DPT.2-5 評価者は、各 SFR 実施モジュールインタフェースに対するテスト手法が、そのインタフェースの期待されるふるまいを実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1356 ワークユニットATE_DPT.2-2ではサブシステムの期待されるふるまいを扱っているが、このワークユニットではATE_DPT.2-4でカバーされている SFR 実施モジュールインタフェースの期待されるふるまいを扱う。

1357 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1358 インタフェースのテストは、そのインタフェース、外部インタフェース、またはそれら両方の組み合わせに対して直接行うことができる。どのような方策が使用される場合でも、評価者は、インタフェースを適切にテストするための妥当性を考慮する。特に評価者は、内部インタフェースでのテストが必要であるかどうか、または外部インタフェースを使用してこれらの内部インタフェースを適切にテストする(暗黙にではあるが)ことができるかどうかを決定する。この決定とそれを正当とする理由は、評価者に任される。

ATE_DPT.2.2C ***テストの深さの分析は、TOE 設計内のすべての TSF サブシステムがテストされていることを実証しなければならない。***

ATE_DPT.2-6 評価者は、TSF サブシステムのふるまい及び相互作用のすべての記述がテストされることを決定するために、テスト手順を***検査しなければならない。***

1359 このワークユニットは、ワークユニット ATE_DPT.2-1 の完全性を検証する。TOE 設計で提供されている、TSF サブシステムのふるまいの記述及び TSF サブシステム間の相互作用のすべての記述がテストされなければならない。TSF サブシステムのふるまいの記述または TSF サブシステム間の相互作用の記述が TOE 設計で識別されているが、それに対するテストが示されない場合、テストの深さが不完全であることは明らかである。

1360 評価者は、これが、テスト証拠資料におけるすべてのテストが TOE 設計におけるサブシステムのふるまいまたは相互作用の記述にマッピングされる必要があることを暗示していないことに留意する。

ATE_DPT.2.3C ***テストの深さの分析は、TOE 設計内の SFR 実施モジュールがテストされていることを実証しなければならない。***

ATE_DPT.2-7 評価者は、SFR 実施モジュールのすべてのインタフェースがテストされていることを決定するために、テスト手順を***検査しなければならない。***

1361 このワークユニットは、ワークユニット ATE_DPT.2-4 の完全性を検証する。TOE 設計で提供されている SFR 実施モジュールのすべてのインタフェースがテストされなければならない。SFR 実施モジュールのいずれかのインタフェースが TOE 設計で識別されているが、それに対するテストが示されない場合、テストの深さが不完全であることは明らかである。

1362 評価者は、これが、テスト証拠資料におけるすべてのテストが TOE 設計における SFR 実施モジュールのインタフェースにマッピングされる必要があることを暗示していないことに留意する。

15.4.3 サブアクティビティの評価(ATE_DPT.3)

15.4.3.1 目的

1363 このサブアクティビティの目的は、開発者が全 TSF サブシステムとモジュールを TOE 設計及びセキュリティアーキテクチャの記述と比較してテストしたかどうかを決定することである。

15.4.3.2 入力

a) ST;

b) 機能仕様;

c) TOE 設計;

d) セキュリティアーキテクチャ記述;

e) テスト証拠資料;

f) テストの深さ分析。

15.4.3.3 アクション ATE_DPT.3.1E

ATE_DPT.3.1C *テストの深さの分析は、テスト証拠資料におけるテストと TOE 設計における TSF サブシステム及びモジュールの間の対応を実証しなければならない。*

ATE_DPT.3-1 評価者は、TSF サブシステムのふるまいの記述とそれらの相互作用の記述がテスト証拠資料に含まれていることを決定するために、テストの深さ分析を***検査しなければならない。***

1364 このワークユニットは、テストと TOE 設計の記述との間の対応の内容を検証する。単純な相互表がテストの対応を十分に示すことができる。カバレージの深さ分析に示されるテストとふるまい/相互作用の識別は、曖昧さをなくす必要がある。

1365 評価者は、テスト証拠資料におけるすべてのテストがサブシステムのふるまいまたは相互作用の記述にマッピングされる必要があるわけではないことに留意する。

ATE_DPT.3-2 評価者は、ふるまいの記述に対するテスト手法が、TOE 設計に記述されているそのサブシステムのふるまいを実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1366 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1367 TSF サブシステムのインタフェースが提供されている場合、それらのサブシステムのふるまいをそれらのインタフェースから直接実行することができる。それ以外の場合、それらのサブシステムのふるまいは TSFI インタフェースからテストされる。あるいは、この 2 つのテストの組み合わせを採用することができる。どのような方策が使用される場合でも、評価者は、TOE 設計に記述されているふるまいを適切にテストするための妥当性を考慮する。

ATE_DPT.3-3 評価者は、ふるまいの記述に対するテスト手法が、TOE 設計に記述されているサブシステム間の相互作用を実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1368 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1369 前のワークユニットではサブシステムのふるまいを扱っているが、このワークユニットではサブシステム間の相互作用を扱う。

1370 TSF サブシステムのインタフェースが提供されている場合、他のサブシステムとの相互作用をそれらのインタフェースから直接実行することができる。それ以外の場合、サブシステム間の相互作用は TSFI インタフェースから推測されなければならない。どのような方策が使用される場合でも、評価者は、TOE 設計に記述されているサブシステム間の相互作用を適切にテストするための妥当性を考慮する。

ATE_DPT.3-4 評価者は、TSF モジュールのインタフェースがテスト証拠資料に含まれていることを決定するために、テストの深さ分析を***検査しなければならない。***

1371 このワークユニットは、テストと TOE 設計の記述との間の対応の内容を検証する。単純な相互表がテストの対応を十分に示すことができる。カバレージの深さ分析に示されるテストとふるまい/相互作用の識別は、曖昧さをなくす必要がある。

1372 評価者は、テスト証拠資料におけるすべてのテストがサブシステムのふるまいまたは相互作用の記述にマッピングされる必要があるわけではないことに留意する。

ATE_DPT.3-5 評価者は、各 TSF モジュールインタフェースに対するテスト手法が、そのインタフェースの期待されるふるまいを実証することを決定するために、テスト計画、テストの必要条件、テストステップ、及び期待される結果を***検査しなければならない。***

1373 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1、TOE の期待されるふるまいの理解

b) 15.2.2、機能性の期待されるふるまいを検証するための、テストとその代替手法

1374 インタフェースのテストは、そのインタフェース、外部インタフェース、またはそれら両方の組み合わせに対して直接行うことができる。どのような方策が使用される場合でも、評価者は、インタフェースを適切にテストするための妥当性を考慮する。特に評価者は、内部インタフェースでのテストが必要であるかどうか、または外部インタフェースを使用してこれらの内部インタフェースを適切にテストする(暗黙にではあるが)ことができるかどうかを決定する。この決定とそれを正当とする理由は、評価者に任される。

ATE_DPT.3.2C ***テストの深さの分析は、TOE 設計内のすべての TSF サブシステムがテストされていることを実証しなければならない。***

ATE_DPT.3-6 評価者は、TSF サブシステムのふるまい及び相互作用のすべての記述がテストされることを決定するために、テスト手順を***検査しなければならない。***

1375 このワークユニットは、ワークユニット ATE_DPT.3-1 の完全性を検証する。TOE 設計で提供されている、TSF サブシステムのふるまいの記述及び TSF サブシステム間の相互作用のすべての記述がテストされなければならない。TSF サブシステムのふるまいの記述または TSF サブシステム間の相互作用の記述が TOE 設計で識別されているが、それに対するテストが示されない場合、テストの深さが不完全であることは明らかである。

1376 評価者は、これが、テスト証拠資料におけるすべてのテストが TOE 設計におけるサブシステムのふるまいまたは相互作用の記述にマッピングされる必要があることを暗示していないことに留意する。

ATE_DPT.3.3C ***テストの深さの分析は、TOE 設計内のすべての TSF モジュールがテストされていることを実証しなければならない。***

ATE_DPT.3-7 評価者は、すべての TSF モジュールのすべてのインタフェースがテストされることを決定するために、テスト手順を***検査しなければならない。***

1377 このワークユニットは、ワークユニット ATE_DPT.3-4 の完全性を検証する。TOE 設計で提供されている TSF モジュールのすべてのインタフェースがテストされなければならない。TSF モジュールのいずれかのインタフェースが TOE 設計で識別されているが、それに対するテストが示されない場合、テストの深さが不完全であることは明らかである。

1378 評価者は、これが、テスト証拠資料におけるすべてのテストが TOE 設計における TSF モジュールのインタフェースにマッピングされる必要があることを暗示していないことに留意する。

15.4.4 サブアクティビティの評価(ATE_DPT.4)

1379 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

15.5 機能テスト(ATE_FUN)

15.5.1 サブアクティビティの評価(ATE_FUN.1)

15.5.1.1 目的

1380 このサブアクティビティの目的は、開発者がテスト証拠資料におけるテストを正しく実行し、証拠資料として提出したかどうかを決定することである。

15.5.1.2 入力

1381 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) テスト証拠資料

15.5.1.3 適用上の注釈

1382 テスト証拠資料が TSF をカバーするために必要とされる範囲は、カバレージ保証コンポーネントに依存する。

1383 提供された開発者テストに対して、評価者は、テストが反復可能であるかどうか、及び評価者の独立テストの成果に開発者テストを使用できる範囲を決定する。開発者のテスト結果より、仕様のとおりに機能しない可能性のある TSFI はいずれも、それが機能するかしないかを決定するために評価者によって独立にテストされるべきである。

15.5.1.4 アクション ATE_FUN.1.1E

ATE_FUN.1.1C ***テスト証拠資料は、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されなければならない。***

ATE_FUN.1-1 評価者は、テスト証拠資料にテスト計画、期待されるテスト結果、及び実際のテスト結果が含まれていることを***チェックしなければならない。***

1384 評価者は、テスト計画、期待されるテスト結果、及び実際のテスト結果がテスト証拠資料に含まれていることをチェックする。

ATE_FUN.1.2C ***テスト計画は、実行されるべきテストを識別し、各テストを実行するシナリオを記述しなければならない。これらのシナリオは、他のテストの結果へのすべての順序依存性を含んでいなければならない。***

ATE_FUN.1-2 評価者は、テスト計画が各テストを実行するシナリオを記述していることを決定するために、その計画を***検査しなければならない。***

1385 評価者は、使用されているテスト構成に関する情報が、TOE の構成についても、また使用されている任意のテスト装置についても、テスト計画によって提供されることを決定する。この情報は、テストが再現可能であることを保証するために、十分詳細に記述するべきである。

1386 評価者は、テストを実行する方法に関する情報がテスト計画によって提供されることも決定する。その情報とは、すべての必要な自動セットアップ手順(及びこれらが実行権限を必要とするかどうか)、適用される入力、これらの入力がどのように適用されるか、出力がどのように取得されるか、すべての自動クリーンアップ手順(及びこれらが実行権限を必要とするかどうか)などである。この情報は、テスト構成が再現可能であることを保証するために、十分詳細に記述するべきである。

1387 評価者は、このワークユニットを実行するとき、サンプリング方策を採用することができる。

ATE_FUN.1-3 評価者は、TOE テスト構成が ST と一貫していることを決定するために、テスト計画を***検査しなければならない。***

1388 開発者のテスト計画で参照されている TOE は、CM 能力(ALC_CMC)サブアクティビティによって確立され ST 概説で識別されているのと同じ、一意の参照を持つべきである。

1389 ST は、評価に対して複数の構成を特定することができる。評価者は、開発者テスト証拠資料で識別されたすべてのテスト構成が ST と一貫していることを検証する。例えば、ST は、設定しなければならない構成オプションを定義する場合があるが、その際に追加の部分を含めることによって、または除外することによって TOE の構成内容に影響を与える可能性がある。評価者は、このような TOE の変動がすべて考慮されていることを検証する。

1390 評価者は、テスト環境に適用できる ST に記述されている運用環境のセキュリティ対策方針を考慮するべきである。テスト環境に適用されないいくつかの運用環境の対策方針が存在することがある。例えば、利用者の利用許可についての対策方針は適用しないことがあるかもしれないが、ネットワークへの単一ポイントでの接続についての対策方針は適用するかもしれない。

1391 評価者は、このワークユニットを実行するとき、サンプリング方策を採用することができる。

1392 このワークユニットが、統合 TOE で使用/統合される可能性のあるコンポーネント TOE に適用される場合(「ACO クラス: 統合」を参照のこと)、以下のものが適用される。評価中のコンポーネント TOE が運用環境における他のコンポーネントに依存して運用をサポートする場合、開発者は、テスト構成の 1 つとして運用環境の要件を満たすために、統合 TOE で使用される他のコンポーネントの使用を考慮することができる。これによって、統合 TOE 評価に必要とされる追加テストの量が削減される。

ATE_FUN.1-4 評価者は、十分な指示がすべての順序依存性に対して提供されることを決定するために、テスト計画を***検査しなければならない。***

1393 初期条件を確立するために、いくつかのステップを実行する必要があることがある。例えば、利用者アカウントは、それらを削除できるようになる前に、追加される必要がある。他のテスト結果の順序依存性の一例としては、監査記録の探索及び分類を考慮するためのテストを実行する前に、監査記録を生成するテストでアクションを実行する必要がある場合がある。順序依存性の他の例としては、あるテストケースが他のテストケースへの入力として使用されるデータファイルを生成する場合がある。

1394 評価者は、このワークユニットを実行するとき、サンプリング方策を採用することができる。

ATE_FUN.1.3C ***期待されるテスト結果は、テストの実行が成功したときの予期される出力を示さなければならない。***

ATE_FUN.1-5 評価者は、すべての期待されるテスト結果が含まれていることを決定するために、テスト証拠資料を***検査しなければならない。***

1395 期待されるテスト結果は、テストが成功裏に実行されたかどうか決定するために必要となる。期待されるテスト結果は、それらが、テスト手法により与えられた期待されるふるまいと曖昧さなく一貫している場合、十分である。

1396 評価者は、このワークユニットを実行するとき、サンプリング方策を採用することができる。

ATE_FUN.1.4C ***実際のテスト結果は、期待されたテスト結果と一貫していなければならない。***

ATE_FUN.1-6 評価者は、テスト証拠資料の実際のテスト結果がテスト証拠資料における期待されるテスト結果と一貫していることを***チェックしなければならない。***

1397 開発者が提供する実際のテスト結果と期待されるテスト結果の比較は、それらの結果の間の不一致を明らかにする。最初にいくらかのデータの削減または統合を行わない限り、実際の結果を直接比較できない場合がある。そのような場合、開発者のテスト証拠資料は、実際のデータを削減または統合するプロセスを記述するべきである。

1398 例えば、開発者は、ネットワーク接続が行われた後でバッファの内容を決定するためにメッセージバッファの内容をテストする必要があるとする。メッセージバッファには、2 進数が含まれている。この 2 進数は、テストをさらに意味のあるものにするためには、他の形式のデータ表現に変換する必要がある。データのこの 2 進数表現の上位レベル表現への変換は、評価者が変換プロセスを実行できるように、開発者が詳細に記述する必要がある(同期または非同期転送、ストップビットの数、パリティなど)。

1399 実際のデータを削減または統合するために使用されるプロセスの記述は、評価者が実際に必要な改変を行うためでなく、このプロセスが正しいかどうかを評定するために使用されることに注意されるべきである。期待されるテスト結果を、実際のテスト結果と簡単に比較できる形式に変換するかは、開発者に委ねられる。

1400 評価者は、このワークユニットを実行するとき、サンプリング方策を採用することができる。

ATE_FUN.1-7 評価者は、テスト手法、構成、深さ、及び結果を概説して開発者のテストの成果を***報告しなければならない。***

1401 ETR に記録される開発者のテスト情報は、全体的なテスト手法及び開発者によって TOE のテストで費やされた成果を評価者に伝えることを可能にする。この情報を提供する意図は、開発者のテスト成果の意味ある概要を伝えることである。ETR 中の開発者テストに関する情報が、特定のテストステップの正確な再現であること、または個々のテストの結果であることを意図していない。意図することは、十分詳細な情報を提供し、他の評価者や評価監督機関が、開発者のテスト手法、実行されたテストの量、TOE テスト構成、開発者テストの全体的な結果を洞察できるようにすることである。

1402 開発者のテスト成果に関する ETR セクションに一般に見られる情報は、次のとおりである:

a) TOE テスト構成。テストをセットアップするため、または後でクリーンアップするために、権限を持つコードが要求されたかどうかを含む、テストされた TOE の特定の構成;

b) テスト手法。採用された全体的な開発者テストの方策の説明;

c) テスト結果。開発者テストの全体的な結果の記述。

1403 このリストは、決して完全なものではなく、開発者テスト成果に関して ETR に示すべき情報のタイプを提供することだけを意図している。

15.5.2 サブアクティビティの評価(ATE_FUN.2)

1404 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

15.6 独立テスト(ATE_IND)

15.6.1 サブアクティビティの評価(ATE_IND.1)

15.6.1.1 目的

1405 このアクティビティの目的は、TSFI のサブセットを独立にテストすることにより、TOE が機能仕様及びガイダンス証拠資料に特定されているとおりにふるまうかどうかを決定することである。

15.6.1.2 入力

1406 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) 利用者操作ガイダンス;

d) 利用者準備ガイダンス;

e) テストに適した TOE。

15.6.1.3 アクション ATE_IND.1.1E

ATE_IND.1.1C ***TOE は、テストに適していなければならない。***

ATE_IND.1-1 評価者は、テスト構成が ST に特定された評価における構成と一貫していることを決定するために、TOE を***検査しなければならない。***

1407 開発者によって提供される TOE は、CM 能力(ALC_CMC)サブアクティビティによって確立され ST 概説で識別されているのと同じ、一意の参照を持つべきである。

1408 ST は、評価に対して複数の構成を特定することができる。TOE は、ST に従ってテストする必要がある多数の異なるハードウェアエンティティ及びソフトウェアエンティティで構成される可能性がある。評価者は、すべてのテスト構成が ST と一貫していることを検証する。

1409 評価者は、テスト環境に適用できる ST に記述されている運用環境のセキュリティ対策方針を考慮し、それらがテスト環境で満たされていることを保証するべきである。テスト環境に適用されないいくつかの運用環境の対策方針が存在することがある。例えば、利用者の利用許可についての対策方針は適用しないことがあるかもしれないが、ネットワークへの単一ポイントでの接続についての対策方針は適用するかもしれない。

1410 いずれかのテスト資源(例えば、メーター、アナライザ)が使用される場合、これらの資源が正しく調整されるようにするのは、評価者の責任である。

ATE_IND.1-2 評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1411 評価者は、各種の方法で TOE の状態を決定することができる。例えば、サブアクティビティの評価(AGD_PRE.1)が既に成功裏に完了しており、評価者がテストに使用されている TOE が適切に設置され、定義された状態にあることを今もなお信頼できる場合、このワークユニットを満たすことになる。そうでない場合には、評価者は、提供されたガイダンスだけを使用し、開発者の手順に従って、TOE を設置し、立ち上げるべきである。

1412 もし TOE が未定義の状態であるために評価者が設置手順を実行しなければならず、このワークユニットが成功裏に完了した場合、ワークユニット AGD_PRE.1-3 を満たすことができる。

15.6.1.4 アクション ATE_IND.1.2E

ATE_IND.1-3 評価者は、テストサブセットを*考え出さなければならない。*

1413 評価者は、TOE に適したテストサブセットとテスト方策を選択する。1 つの極端なテスト方策は、テストサブセットに可能な限り多くのインタフェースを含め、簡易にテストすることである。別のテスト方策は、テストサブセットに気が付いた問題と関連性のある少数のインタフェースを含め、これらのインタフェースを厳密にテストすることである。

1414 一般的に、評価者のテスト手法は、これら両極端な方法の間に収まるべきである。評価者は 1 つ以上のテストを使用して、ほとんどのインタフェースを実行するべきであるが、テストは、徹底的な仕様テストを実証する必要はない。

1415 評価者は、テストするインタフェースのサブセットを選択するとき、次の要因を考慮するべきである:

a) テストサブセットに加えるインタフェースの数。TSF が少数の比較的単純なインタフェースのみを含む場合、インタフェースのすべてを厳密にテストすることが現実的にできる。別の場合では、これは費用効果が悪く、サンプリングが必要になる可能性がある。

b) 評価アクティビティのバランスの維持。テストアクティビティに費やした評価者の労力は、他の評価アクティビティに費やした労力と釣り合いを保つべきである。

1416 評価者は、サブセットを構成するインタフェースを選択する。この選択は、数多くの要因に依存し、以下の要因の考慮は、テストサブセットサイズの選択にも影響を与える:

a) インタフェースの重要性。他のインタフェースよりも重要なインタフェースは、テストサブセットに含めるべきである。「重要性」の 1 つの主要な要因は、セキュリティ関連性(SFR 実施インタフェースは SFR 支援インタフェースよりも重要であり、SFR 支援インタフェースは SFR 非干渉インタフェースよりも重要である。CC パート 3 の機能仕様(ADV_FSP)の節を参照のこと)である。「重要性」のもう 1 つの主要な要因は、(ADVにおける抽象のレベル間の対応を識別するときの決定に従って)このインタフェースにマッピングされる SFR の数である。

b) インタフェースの複雑性。複雑なインタフェースは、開発者または評価者にめんどうな要求を課す複雑なテストを必要とするかもしれず、費用対効果の高い評価を行えない可能性がある。逆に、これらは誤りが見つかりがちな領域であり、サブセットの有力な候補である。評価者は、これらの考慮事項の間でバランスを計る必要がある。

c) 暗黙のテスト。いくつかのインタフェースのテストは、しばしば暗黙に他のインタフェースをテストすることがある。それらをサブセットに含めると、(暗黙にではあるが)テストされるインタフェースの数を最大限に増やすことができる。ある種のインタフェースは、一般的に各種のセキュリティ機能性を提供するために使用され、従って効率的なテスト手法の標的となる。

d) インタフェースタイプ(例えば、プログラムに基づく、コマンド行、プロトコル)。評価者は、TOE がサポートするすべての異なるタイプのインタフェースのテストを含めることを考慮するべきである。

e) 革新的または一般的でない特徴をもたらすインタフェース。販売広告用の印刷物及びガイダンス文書で強調しているような革新的または一般的ではない特徴が TOE に含まれている場合、対応するインタフェースは、テストの有力な候補となるべきである。

1417 このガイダンスは、適切なテストサブセットの選択プロセスで考慮する要因を明記するが、これらは決してすべてではない。

ATE_IND.1-4 評価者は、テストを再現可能にできるように十分詳細に記述されたテストサブセットに対するテスト証拠資料を*作成しなければならない。*

1418 評価者は、ST 及び機能仕様から TSF の期待されるふるまいを理解して、インタフェースをテストする最も適切な方法を決定する必要がある。特に、評価者は、次のことを考慮する:

a) 使用する手法、例えば、外部インタフェースをテストするか、テストハーネスを使用して内部インタフェースをテストするか、または別のテスト手法(例えば例外的な状況で実装表現を利用できる場合、コード検査)を採用するか;

b) テスト及び反応を観察するために使用されるインタフェース;

c) テストに存在する必要がある初期条件(つまり、存在する必要がある特定のオブジェクトまたはサブジェクト及びそれらが持つ必要があるセキュリティ属性);

d) インタフェースを刺激する(例えば、パケットジェネレータ)またはインタフェースを観察する(例えば、ネットワークアナライザ)ために必要となる特別のテスト装置。

1419 評価者は、各テストケースが期待されるふるまいの非常に特殊な局面をテストするような一連のテストケースを用いて、各インタフェースをテストすることが、実用的と感じるかもしれない。

1420 評価者のテスト証拠資料は、関連する 1 つ以上のインタフェースにまでさかのぼって各テストの起源を特定するべきである。

ATE_IND.1-5 評価者はテストを*実施しなければならない。*

1421 評価者は、TOE のテストを実行するための基礎として開発されたテスト証拠資料を使用する。テスト証拠資料は、テストの基礎として使用されるが、これは、評価者が追加の特別のテストを実行することを排除しない。評価者は、テスト中に発見された TOE のふるまいに基づいて新しいテストを考え出すことができる。これらの新しいテストは、テスト証拠資料に記録される。

ATE_IND.1-6 評価者は、テストサブセットを構成するテストについての次の情報を***記録しなければならない*：**

a) テストするインタフェースのふるまいの識別;

b) テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示;

c) すべての必要なテスト条件を確立するための指示;

d) インタフェースを刺激するための指示;

e) インタフェースのふるまいを観察するための指示;

f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述;

g) TOE のテストを終了し、終了後の必要な状態を確立するための指示;

h) 実際のテスト結果。

1422 詳細のレベルは、他の評価者がテストを繰返し、同等の結果を得ることができるものとするべきである。テスト結果のいくつかの特定の詳細(例えば、監査レコードの時刻と日付フィールド)は異なってもよいが、全体的な結果は同一であるべきである。

1423 このワークユニットに表されている情報をすべて提供する必要がない場合がある(例えば、テストの実際の結果と期待される結果を比較する前に、分析を必要としない場合)。この情報を省略する決定は、それを正当とする理由とともに、評価者に任される。

ATE_IND.1-7 評価者は、すべての実際のテスト結果が、期待されたテスト結果と一貫していることを***チェックしなければならない。***

1424 実際のテスト結果と期待されたテスト結果の相違はいずれも、TOE が特定されたとおりに実行しなかったこと、または評価者のテスト証拠資料が正しくないことを示す。期待しない実際の結果は、TOE またはテスト証拠資料の修正保守を必要とし、おそらく影響を受けるテストの再実行とテストのサンプルサイズ、構成の改変を必要とする。この決定とそれを正当とする理由は、評価者に任される。

ATE_IND.1-8 評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者のテストの成果を***報告しなければならない。***

1425 ETR に報告される評価者のテスト情報によって、評価者は、全体的なテスト手法及び評価中のテストアクティビティで費やされた成果を伝えることができる。この情報を提供する意図は、テスト成果の意味ある概要を示すことである。ETR 中のテストに関する情報が、特定のテストの指示または個別のテスト結果の正確な再現となることを意図していない。意図することは、十分詳細な情報を提供し、他の評価者や評価監督機関が、選択されたテスト手法、実行されたテストの量、TOE テスト構成、及びテストアクティビティの全体的な結果を洞察できるようにすることである。

1426 評価者のテスト成果に関する ETR セクションに通常示される情報は、次のとおりである:

a) TOE テスト構成。テストされた TOE の特定の構成;

b) 選択されたサブセットサイズ。評価中にテストされたインタフェースの量及びそのサイズを正当とする理由;

c) サブセットを構成するインタフェースの選択基準。サブセットに含めるインタフェースを選択したときに考慮した要因についての簡単な説明;

d) テストされるインタフェース。サブセットに含めることに値したインタフェースの簡単なリスト;

e) アクティビティの判定。評価中のテスト結果の全体的な判断。

1427 このリストは、必ずしも完全なものではなく、評価中に評価者が行ったテストに関する ETR に示すべき情報のタイプを提供することだけを意図している。

15.6.2 サブアクティビティの評価(ATE_IND.2)

15.6.2.1 目的

1428 このアクティビティの目標は、TSF のサブセットを独立してテストすることにより TOE が設計証拠資料で特定されているとおりにふるまうかどうかを決定すること、及び開発者のテストのサンプルを実行することにより開発者のテスト結果において確信を得ることである。

15.6.2.2 入力

1429 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計記述;

d) 利用者操作ガイダンス;

e) 利用者準備ガイダンス;

f) 構成管理証拠資料;

g) テスト証拠資料;

h) テストに適した TOE。

15.6.2.3 アクション ATE_IND.2.1E

ATE_IND.2.1C ***TOE は、テストに適していなければならない。***

ATE_IND.2-1 評価者は、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を***検査しなければならない。***

1430 開発者によって提供され、テスト計画で識別される TOE は、CM 能力(ALC_CMC)サブアクティビティによって確立され ST 概説で識別されているのと同じ、一意の参照を持つべきである。

1431 ST は、評価に対して複数の構成を特定することができる。TOE は、ST に従ってテストする必要がある多数の異なるハードウェアエンティティ及びソフトウェアエンティティで構成される可能性がある。評価者は、すべてのテスト構成が ST と一貫していることを検証する。

1432 評価者は、テスト環境に適用できる ST に記述されている運用環境のセキュリティ対策方針を考慮し、それらがテスト環境で満たされていることを保証するべきである。テスト環境に適用されないいくつかの運用環境の対策方針が存在することがある。例えば、利用者の利用許可についての対策方針は適用しないことがあるかもしれないが、ネットワークへの単一ポイントでの接続についての対策方針は適用するかもしれない。

1433 いずれかのテスト資源(例えば、メーター、アナライザ)が使用される場合、これらの資源が正しく調整されるようにするのは、評価者の責任である。

ATE_IND.2-2 評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1434 評価者は、各種の方法で TOE の状態を決定することができる。例えば、サブアクティビティの評価(AGD_PRE.1)が既に成功裏に完了しており、評価者がテストに使用されている TOE が適切に設置され、定義された状態にあることを今もなお信頼している場合、このワークユニットを満たすことになる。そうでない場合には、評価者は、提供されたガイダンスだけを使用し、開発者の手順に従って、TOE を設置し、立ち上げるべきである。

1435 もし TOE が未定義の状態であるために評価者が設置手順を実行しなければならず、このワークユニットが成功裏に完了した場合、ワークユニット AGD_PRE.1-3 を満たすことができる。

ATE_IND.2.2C ***開発者は、TSF の開発者機能テストで使用されたものと同等の一連の資源を提供しなければならない。***

ATE_IND.2-3 評価者は、開発者によって提供された一連の資源が、TSF を機能的にテストするために開発者によって使用された一連の資源と同等であることを決定するために、その一連の資源を***検査しなければならない。***

1436 開発者によって使用された一連の資源は、機能テスト(ATE_FUN)ファミリで考慮され、開発者のテスト計画に記載されている。この資源の組み合わせには、研究所へのアクセス及び特別のテスト装置などを含めることができる。開発者が使用したのと同じではない資源は、それらがテスト結果に与える影響の観点から同等である必要がある。

15.6.2.4 **アクション** ATE_IND.2.2E

ATE_IND.2-4 評価者は、開発者テスト計画及び手順の中で見出したテストのサンプルを使用してテストを***実施しなければならない。***

1437 このワークユニットの全体的な目的は、十分な数の開発者テストを実行して、開発者のテスト結果が正当であることを確認することである。評価者は、サンプルのサイズ、及びサンプルを構成する開発者テストを決定する必要がある(A.2 を参照のこと)。

1438 開発者のテストはすべて、特定のインタフェースにまでさかのぼることができる。そこで、サンプルを構成するためのテストを選択するときに考慮する要因は、ワークユニット ATE_IND.2-6 のサブセットの選択に示されているものと同じである。さらに、評価者は、サンプルに含める開発者テストを選択するためにランダムサンプリング方式を採用することができる。

ATE_IND.2-5 評価者は、実際のテスト結果がすべて、期待されたテスト結果と一貫していることを***チェックしなければならない。***

1439 開発者の期待されるテスト結果と実際のテスト結果の間の不一致は、評価者に相違の解決を強く要求する。評価者が発見した不一致は、開発者による正当な説明と開発者が不一致を解決することにより解決することができる。

1440 十分な説明または解明が得られなければ、開発者のテスト結果に対する評価者の信頼が低下する可能性があり、ワークユニット ATE_IND.2-4 に識別されているサブセットが適切にテストされるまで評価者がサンプルサイズを増やすことが必要となる場合がある。開発者によるテストの欠陥は、開発者による TOE（例えば不一致が間違ったふるまいに起因する場合）または開発者のテスト（例えば不一致が間違ったテストに起因する場合）に対する修正アクションまたは評価者による新しいテストの作成に帰着する必要がある。

15.6.2.5 **アクション** ATE_IND.2.3E

ATE_IND.2-6 評価者は、テストサブセットを***考え出さなければならない。***

1441 評価者は、TOE に適したテストサブセットとテスト方策を選択する。1 つの極端なテスト方策は、テストサブセットに可能な限り多くのインタフェースを含め、簡易にテストすることである。別のテスト方策は、テストサブセットに気が付いた問題と関連性のある少数のインタフェースを含め、これらのインタフェースを厳密にテストすることである。

1442 一般的に、評価者のテスト手法は、これら両極端な方法の間に収まるべきである。評価者は 1 つ以上のテストを使用して、ほとんどのインタフェースを実行するべきであるが、テストは、徹底的な仕様テストを実証する必要はない。

1443 評価者は、テストするインタフェースのサブセットを選択するとき、次の要因を考慮するべきである:

a) 開発者テスト証拠。開発者テスト証拠は、テスト証拠資料、利用できるテストカバレージ分析、及び利用できるテストの深さ分析からなる。開発者テスト証拠は、テスト中に開発者がどのように TSF を実行したかについての洞察を提供する。評価者は、TOE を独立にテストするための新しいテストを開発するとき、この情報を適用する。特に評価者は、次のことを考慮するべきである:

   1) インタフェースに対する開発者テストの要件追加。評価者は、インタフェースをさらに厳密にテストするためにパラメタを変えて、さらに多くの同じタイプのテストを行うことができる。

   2) インタフェースに対する開発者テスト方策の補足。評価者は、別のテスト方策を使用してテストすることにより、特定のインタフェースのテスト手法を変えることができる。

b) テストサブセットに加えるインタフェースの数。TSF が少数の比較的単純なインタフェースのみを含む場合、インタフェースのすべてを厳密にテストすることが現実的にできる。別の場合では、これは費用効果が悪く、サンプリングが必要になる可能性がある。

c) 評価アクティビティのバランスの維持。テストアクティビティに費やした評価者の労力は、他の評価アクティビティに費やした労力と釣り合いを保つべきである。

1444 評価者は、サブセットを構成するインタフェースを選択する。この選択は、数多くの要因に依存し、以下の要因の考慮は、テストサブセットサイズの選択にも影響を与える:

a) インタフェースの開発者テストの厳密さ。追加のテストが必要であると評価者が決定したインタフェースは、テストサブセットに含められるべきである。

b) 開発者テスト結果。開発者のテスト結果からインタフェースが適切に実装されていることに評価者が疑いを持つ場合には、評価者は、テストサブセットにそのようなインタフェースを含めるべきである。

c) インタフェースの重要性。他のインタフェースよりも重要なインタフェースは、テストサブセットに含めるべきである。「重要性」の 1 つの主要な要因は、セキュリティ関連性(SFR 実施インタフェースは SFR 支援インタフェースよりも重要であり、SFR 支援インタフェースは SFR 非干渉インタフェースよりも重要である。CC パート 3 のADV_FSP の節を参照のこと)である。「重要性」のもう 1 つの主要な要因は、(ADVにおける抽象のレベル間の対応を識別するときの決定に従って)このインタフェースに対するマッピングされる SFR の数である。

d) インタフェースの複雑性。複雑な実装を必要とするインタフェースは、開発者または評価者に、費用効果の高い評価とはならない面倒な要求を課す複雑なテストを必要とするかもしれない。逆に、これらは誤りが見つかりがちな領域であり、サブセットの有力な候補である。評価者は、これらの考慮事項の間でバランスを計る必要がある。

e) 暗黙のテスト。いくつかのインタフェースのテストは、しばしば暗黙に他のインタフェースをテストすることがある。それらをサブセットに含めると、(暗黙にではあるが)テストされるインタフェースの数を最大限に増やすことができる。ある種のインタフェースは、一般的に各種のセキュリティ機能性を提供するために使用され、従って効率的なテスト手法の標的となる。

f) インタフェースタイプ(例えば、プログラムに基づく、コマンド行、プロトコル)。評価者は、TOE がサポートするすべての異なるタイプのインタフェースのテストを含めることを考慮するべきである。

g) 革新的または一般的でない特徴をもたらすインタフェース。販売広告用の印刷物及びガイダンス文書で強調しているような革新的または一般的ではない特徴が TOE に含まれている場合、対応するインタフェースは、テストの有力な候補となるべきである。

1445 このガイダンスは、適切なテストサブセットの選択プロセスで考慮する要因を明記するが、これらは決してすべてではない。

ATE_IND.2-7 評価者は、テストを再現可能にできるように十分詳細に記述されたテストサブセットに対するテスト証拠資料を*作成しなければならない。*

1446 評価者は、ST、機能仕様、及び TOE 設計記述から TSF の期待されるふるまいを理解して、インタフェースをテストする最も適切な方法を決定する必要がある。特に、評価者は、次のことを考慮する:

a) 使用する手法、例えば、外部インタフェースをテストするか、テストハーネスを使用して内部インタフェースをテストするか、または別のテスト手法(例えば例外状況での、コード検査)を採用するか;

b) テスト及び反応を観察するために使用されるインタフェース;

c) テストに存在する必要がある初期条件(つまり、存在する必要がある特定のオブジェクトまたはサブジェクト及びそれらが持つ必要があるセキュリティ属性);

d) インタフェースを刺激する(例えば、パケットジェネレータ)またはインタフェースを観察する(例えば、ネットワークアナライザ)ために必要となる特別のテスト装置。

1447 評価者は、各テストケースが期待されるふるまいの非常に特殊な局面をテストするような一連のテストケースを用いて、各インタフェースをテストすることが、実用的と感じるかもしれない。

1448 評価者のテスト証拠資料は、関連する 1 つ以上のインタフェースにまでさかのぼって各テストの起源を特定するべきである。

ATE_IND.2-8 評価者はテストを***実施しなければならない。***

1449 評価者は、TOE のテストを実行するための基礎として開発されたテスト証拠資料を使用する。テスト証拠資料は、テストの基礎として使用されるが、これは、評価者が追加の特別のテストを実行することを排除しない。評価者は、テスト中に発見された TOE のふるまいに基づいて新しいテストを考え出すことができる。これらの新しいテストは、テスト証拠資料に記録される。

ATE_IND.2-9 評価者は、テストサブセットを構成するテストについての次の情報を***記録しなければならない：***

a) テストするインタフェースのふるまいの識別;

b) テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示;

c) すべての必要となるテスト条件を確立するための指示;

d) インタフェースを刺激するための指示;

e) インタフェースを観察するための指示;

f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述;

g) TOE のテストを終了し、終了後の必要な状態を確立するための指示;

h) 実際のテスト結果。

1450 詳細のレベルは、他の評価者がテストを繰返し、同等の結果を得ることができるものとするべきである。テスト結果のいくつかの特定の詳細(例えば、監査レコードの時刻と日付フィールド)は異なってもよいが、全体的な結果は同一であるべきである。

1451 このワークユニットに表されている情報をすべて提供する必要がない場合がある(例えば、テストの実際の結果と期待される結果を比較する前に、分析を必要としない場合)。この情報を省略する決定は、それを正当とする理由とともに、評価者に任される。

ATE_IND.2-10 評価者は、すべての実際のテスト結果が、期待されたテスト結果と一貫していることを***チェックしなければならない。***

1452 実際のテスト結果と期待されたテスト結果の相違はいずれも、TOE が特定されたとおりに実行しなかったこと、または評価者のテスト証拠資料が正しくないことを示す。期待しない実際の結果は、TOE またはテスト証拠資料の修正保守を必要とし、おそらく影響を受けるテストの再実行と、テストサンプルサイズと構成の改変を必要とする。この決定とそれを正当とする理由は、評価者に任される。

ATE_IND.2-11 評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者のテストの成果を***報告しなければならない。***

1453 ETR に報告される評価者のテスト情報によって、評価者は、全体的なテスト手法及び評価中のテストアクティビティで費やされた成果を伝えることができる。この情報を提供する意図は、テスト成果の意味ある概要を示すことである。ETR 中のテストに関する情報が、特定のテストの指示または個別のテスト結果の正確な再現となることを意図していない。意図することは、十分詳細な情報を提供し、他の評価者や評価監督機関が、選択されたテスト手法、実行された評価者のテスト量、実行された開発者のテスト量、TOE テスト構成、及びテストアクティビティの全体的な結果を洞察できるようにすることである。

1454 評価者のテストの成果に関する ETR セクションに通常示される情報は、次のとおりである:

a) TOE テスト構成。テストされた TOE の特定の構成。

b) 選択されたサブセットサイズ。評価中にテストされたインタフェースの量及びそのサイズを正当とする理由。

c) サブセットを構成するインタフェースの選択基準。サブセットに含めるインタフェースを選択したときに考慮した要因についての簡単な説明。

d) テストされるインタフェース。サブセットに含めることに値したインタフェースの簡単なリスト。

e) 実行された開発者テスト。実行された開発者テストの量とテストを選択するために使用された基準の簡単な記述。

f) アクティビティの判定。評価中のテスト結果の全体的な判断。

1455 このリストは、必ずしも完全なものではなく、評価中に評価者が行ったテストに関する ETR に示すべき情報のタイプを提供することだけを意図している。

15.6.3 サブアクティビティの評価(ATE_IND.3)

1456 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

16 AVA クラス: 脆弱性評定

16.1 序説

1457 脆弱性評定アクティビティの目的は、運用環境での TOE の欠陥または弱点の悪用される可能性を決定することである。この決定は、評価者による評価証拠の分析と公開の場で利用できる資料の探索に基づいて行われ、評価者の侵入テストによりサポートされる。

16.2 脆弱性分析(AVA_VAN)

16.2.1 サブアクティビティの評価(AVA_VAN.1)

16.2.1.1 目的

1458 このサブアクティビティの目的は、TOE が、その運用環境において、簡単に識別でき、悪用される可能性のある脆弱性を持つかどうかを決定することである。

16.2.1.2 入力

1459 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) ガイダンス証拠資料;

c) テストに適した TOE;

d) 潜在的な脆弱性の識別をサポートするために公開の場で利用できる情報。

1460 このサブアクティビティのその他の入力は、次のとおりである:

a) 潜在的な脆弱性に関する現在の情報(例えば、評価監督機関からの情報)。

16.2.1.3 適用上の注釈

1461 評価者は、評価の別の部分の実施中に検出された潜在的な脆弱性の結果として、追加テストの実施を考慮するべきである。

1462 このサブアクティビティでの用語「ガイダンス」の使用は、操作ガイダンス及び準備ガイダンスを意味する。

1463 潜在的な脆弱性は、公開の場で利用できる情報になっていることもあればなっていないこともあり、悪用するためのスキルが必要となることもあれば必要とならないこともある。これら 2 つの観点は、関係しているが、別のものである。潜在的な脆弱性が公開の場で利用できる情報から識別できるという理由だけで、それが簡単に悪用できると想定されるべきでない。

16.2.1.4 アクション AVA_VAN.1.1E

AVA_VAN.1.1C ***TOE は、テストに適していなければならない。***

AVA_VAN.1-1 評価者は、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を***検査しなければならない。***

1464 開発者によって提供され、テスト計画で識別される TOE は、CM 能力(ALC_CMC)サブアクティビティによって確立され ST 概説で識別されているのと同じ、一意の参照を持つべきである。

1465 ST は、評価のための複数の構成を特定することができる。TOE は、ST に従ってテストする必要がある多数の異なるハードウェアエンティティ及びソフトウェアエンティティで構成される可能性がある。評価者は、すべてのテスト構成が ST と一貫していることを検証する。

1466 評価者は、テスト環境に適用できる ST に記述されている運用環境のセキュリティ対策方針を考慮し、それらがテスト環境で満たされていることを保証するべきである。テスト環境に適用されないいくつかの対策方針が、運用環境用に存在することがある。例えば、利用者の利用許可についての対策方針は適用しないことがあるが、ネットワークへの 1 つのポイントでの接続についての対策方針は適用するだろう。

1467 いずれかのテスト資源(例えば、メーター、アナライザ)が使用される場合、これらの資源が正しく調整されるようにするのは、評価者の責任である。

AVA_VAN.1-2 評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1468 評価者は、各種の方法で TOE の状態を決定することができる。例えば、サブアクティビティの評価(AGD_PRE.1)がこれまでに成功裏に完了していることは、評価者がテストに使用されている TOE が適切に設置され、定義された状態にあることを今もなお信頼している場合、このワークユニットの条件を満たすことになる。そうでない場合には、評価者は、提供されたガイダンスだけを使用し、開発者の手順に従って、TOE を設置し、立ち上げるべきである。

1469 TOE が未定義の状態であるために、評価者が設置手順を実行しなければならない場合、このワークユニットは、成功裏に完了したとき、ワークユニット AGD_PRE.1-3 の条件を満たすことができる。

16.2.1.5 アクション AVA_VAN.1.2E

AVA_VAN.1-3 評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を***検査しなければならない。***

1470 評価者は、TOE で発生する可能性がある潜在的な脆弱性の識別をサポートするために、公開の場で利用できる情報源を検査する。公開の場で利用できる考慮するべき情報源は多数存在する。例えば、特定の技術における既知の脆弱性が報告されるようなメーリングリストや world wide web 上のセキュリティ関連フォーラム。

1471 評価者は、公開の場で利用可能な情報の考慮を上記のものに制約するべきではなく、その他の利用できるすべての関連情報を考慮するべきである。

1472 提供された証拠を検査する間に、評価者は、公知の情報を使用して、潜在的な脆弱性の探索をさらに進める。評価者が関心の分野を識別した場合、評価者は、それらの関心の分野に関連する公開の場で利用できる情報を考慮するべきである。

1473 攻撃者が容易に入手できて、攻撃を識別し、容易にするのを支援する情報の入手の可能性は、想定される攻撃者の攻撃能力を大幅に向上させるのに効果的である。インターネットにおける脆弱性情報と高機能の攻撃ツールのアクセスのしやすさは、この情報が TOE の潜在的な脆弱性を識別し、それらを悪用するために使用されるということの可能性を増大させる。現代の探索ツールによって、評価者がこのような情報を簡単に利用できるようになり、公開されている潜在的な脆弱性及びよく知られている一般的な攻撃に対する抵抗の決定は、費用効果の高い方法で達成できる。

1474 公開の場で利用できる情報の探索は、特に TOE の派生元である製品を参照する情報源に焦点を置くべきである。この探索の範囲の拡張については、次の要因を考慮するべきである。TOE 種別、この TOE 種別の評価者の経験、予想される攻撃能力、及び利用できるADV証拠のレベル。

1475 識別プロセスは繰返して行われ、その場合、1 つの潜在的な脆弱性の識別が、それ以上の調査が必要となる別の関心分野の識別へとつながることがある。

1476 評価者は、公開の場で利用できる情報内で潜在的な脆弱性を識別するために、どのようなアクションがとられたかを報告する。ただし、このタイプの探索では、探索中の検出の結果によって手法が発展する可能性があるため、評価者は、検査の開始前に潜在的な脆弱性の識別における手順を記述できない可能性がある。

1477 評価者は、潜在的な脆弱性の探索を完了する際に、検査された証拠を報告する。

AVA_VAN.1-4 評価者は、ETR 内で、テストの候補となり、運用環境の TOE に適用できる識別された潜在的な脆弱性を***記録しなければならない。***

1478 例えば、評価者が IT または非 IT の運用環境の手段によってその運用環境では潜在的な脆弱性の悪用が防止されることを識別する場合、潜在的な脆弱性についてそれ以上の考慮は不要であることが識別される可能性がある。例えば、TOE への物理的アクセスを許可利用者だけに制限することにより、効果的に潜在的な脆弱性が改ざんに悪用されないようにすることができる。

1479 評価者が運用環境で潜在的な脆弱性が該当しないことを決定する場合、評価者は、それ以上の考慮から潜在的な脆弱性を除外する理由を記録する。それ以外の場合は、評価者は、さらに考慮する対象となる潜在的な脆弱性を記録する。

1480 運用環境の TOE に適用できる潜在的な脆弱性のリストは、侵入テストアクティビティに対する入力として使用でき、評価者が ETR で報告しなければならない。

16.2.1.6 アクション AVA_VAN.1.3E

AVA_VAN.1-5 評価者は、潜在的な脆弱性に対する独立探索に基づいて、侵入テストを***考え出さなければならない。***

1481 評価者は、必要に応じて、公開の場で利用できる情報源の探索の間に識別される潜在的な脆弱性が、運用環境における TOE にどの程度あてはまるかを決定するために、侵入テストを準備する。既知の潜在的な脆弱性に関して、第三者(例えば、評価監督機関からの)によって評価者に提供されたどんな現在の情報も、他の評価アクティビティを実行した結果として生じる潜在的な脆弱性とともに、評価者によって考慮される。

1482 評価者は恐らく、各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することを、実用的だと感じるだろう。

1483 評価者は、基本的な攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が基本的な攻撃能力を超える潜在的な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

AVA_VAN.1-6 評価者は、潜在的な脆弱性のリストに基づき、テストを再現可能にするために十分に詳細に侵入テスト証拠資料を***作成しなければならない。***テスト証拠資料には、次のものを含めなければならない:

a) TOE はどの潜在的な脆弱性の調査のためにテストされるか、その脆弱性の識別;

b) 侵入テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示;

c) すべての侵入テスト前提初期条件を確立するための指示;

d) TSF を刺激するための指示;

e) TSF のふるまいを観察するための指示;

f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述;

g) TOE のテストを終了し、終了後の必要な状態を確立するための指示。

1484 評価者は、公知になっているものの探索中に識別された潜在的な脆弱性のリストに基づいて、侵入テストを準備する。

1485 評価者は、攻撃が功を奏するために基本的な攻撃能力を必要とする脆弱性を超える潜在的な脆弱性の悪用される可能性を決定することを期待されない。ただし、評価の専門知識の結果として、評価者は、基本的な攻撃能力を超える攻撃者のみが悪用できる潜在的な脆弱性を発見することがある。そのような脆弱性は、残存脆弱性として ETR に報告される。

1486 潜在的な脆弱性を理解し、評価者は、TOE にどの程度あてはまるかをテストするための最も適切な方法を決定する。特に、評価者は、次のことを考慮する:

a) TSF を刺激し、応答を観察するために使用される TSFI またはその他の TOE インタフェース;

b) テストに存在する必要がある初期条件(つまり、存在する必要がある特定のオブジェクトまたはサブジェクト及びそれらが持つ必要があるセキュリティ属性);

c) TSFI を刺激するため、または TSFI を観察するために必要となる特別のテスト装置(おそらく、基本的な攻撃能力を想定している潜在的な脆弱性を悪用するために特別の装置が必要になることはない);

d) 物理的なテストを論理的分析に置き換えるべきであるかどうか。初期テストの結果から、繰返し試みられた攻撃が、指定した試行回数の後に成功する可能性が高いことが実証されると推定できる場合は、特に関連する。

1487 評価者は恐らく、各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することを、実用的だと感じるだろう。

1488 テスト証拠資料にこのレベルの詳細を特定する意図は、他の評価者がテストを再現し、同等の結果を得ることができるようにすることである。

AVA_VAN.1-7 評価者は、侵入テストを***実施しなければならない。***

1489 評価者は、TOE の侵入テストの実行のための基礎として、ワークユニット AVA_VAN.1-5 の結果の侵入テスト証拠資料を使用するが、これは、評価者がその場で追加の侵入テストを実行することを排除しない。必要に応じて、評価者は、侵入テスト中に得られた情報の結果としてその場でテストを考え出すことができ、評価者により行われたならば、そのテストは侵入テスト証拠資料に記録される。そのようなテストは、期待されない結果または観察を追求するか、または事前に計画されたテスト中に評価者に示された潜在的な脆弱性を調査するために必要となる可能性がある。

1490 評価者は、基本的な攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が基本的な攻撃能力を超える潜在的な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

AVA_VAN.1-8 評価者は、侵入テストの実際の結果を***記録しなければならない。***

1491 実際のテスト結果の特定の詳細のいくつか(例えば、監査レコードの時刻と日付フィールド)が期待されたものと異なるかもしれないが、全体的な結果は、同一であるべきである。期待されないテスト結果は、調査するべきである。評価への影響は、述べられ、正当化されるべきである。

AVA_VAN.1-9 評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者の侵入テストの成果を***報告しなければならない。***

1492 ETR に報告される侵入テスト情報によって、評価者は全体的な侵入テスト手法及びこのサブアクティビティで費やした成果を伝えることができる。この情報を提供する意図は、評価者の侵入テスト成果の意味ある概要を示すことである。ETR の侵入テストに関する情報が、特定のテストステップの正確な再現であること、または個々の侵入テストの結果であることを意図しない。意図するのは、十分詳細な情報を提供し、他の評価者と評価監督機関が選択された侵入テスト手法、実行された侵入テストの量、TOE テスト構成、侵入テストアクティビティの全体的な結果を洞察できるようにすることである。

1493 評価者の侵入テスト成果に関する ETR セクションに通常示される情報は、次のとおりである:

a) TOE テスト構成。侵入テストが行われた TOE の特定の構成;

b) 侵入テストされた TSFI。侵入テストの焦点となった TSFI 及びその他の TOE インタフェースの簡単なリスト;

c) サブアクティビティの判定。侵入テスト結果の総合判断。

1494 このリストは、必ずしも徹底したものではなく、評価中に評価者が行った侵入テストに関する、ETR に示すべき情報の種別を提供することだけを意図している。

AVA_VAN.1-10 評価者は、TOE が、運用環境において、基本的な攻撃能力を持つ攻撃者に耐えられることを決定するために、すべての侵入テストの結果を***検査しなければならない。***

1495 TOE が、運用環境において、強化基本的な攻撃能力に欠ける攻撃者によって悪用可能な脆弱性があることを結果が示す場合、この評価者アクションは不合格となる。

1496 特定の脆弱性を悪用するために必要な攻撃能力、及び意図された環境でその悪用が可能かどうかを決定するために、附属書 B.4 のガイダンスを使用するべきである。攻撃能力の計算は必ずしもすべての場合に必要となるわけではなく、強化基本的な攻撃能力に欠ける攻撃者によって脆弱性が悪用可能かどうかについて疑問がある場合に限られる。

AVA_VAN.1-11 評価者は、ETR に、すべての悪用され得る脆弱性と残存脆弱性を、次のそれぞれを詳細に述べて***報告しなければならない***:

a) 出所(例えば、脆弱性が予想されたとき実行していた CEM アクティビティ、評価者に既知である、公表されたものを読んで知った、など);

b) 満たされていない SFR(1 つまたは複数);

c) 記述;

d) 運用環境で悪用されるか否か(つまり、悪用される可能性があるか残存か);

e) 識別された脆弱性を実行するために必要な時間量、専門知識のレベル、TOE に関する知識のレベル、機会のレベル、及び装置。及び附属書 B.4 の表 3 及び 4 を使用した対応する値。

16.2.2 サブアクティビティの評価(AVA_VAN.2)

16.2.2.1 目的

1497 このサブアクティビティの目的は、TOE が、その運用環境において、基本的な攻撃能力を持つ攻撃者が悪用できる脆弱性を持つかどうかを決定することである。

16.2.2.2 入力

1498 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計;

d) セキュリティアーキテクチャ記述;

e) ガイダンス証拠資料;

f) テストに適した TOE;

g) 考えられる潜在的な脆弱性の識別をサポートするために公開の場で利用できる情報。

1499 このサブアクティビティの暗黙の評価証拠の残りの部分は、保証パッケージに含まれているコンポーネントによって異なる。各コンポーネントに対して提供された証拠は、このサブアクティビティで入力として使用される。

1500 このサブアクティビティのその他の入力は、次のとおりである:

a) 公知になっている潜在的な脆弱性及び攻撃に関する現在の情報(例えば、評価監督機関からの情報)。

16.2.2.3 適用上の注釈

1501 評価者は、評価の別の部分の実施中に検出された潜在的な脆弱性の結果として、追加テストの実施を考慮するべきである。

16.2.2.4 アクション AVA_VAN.2.1E

AVA_VAN.2.1C ***TOE は、テストに適していなければならない。***

AVA_VAN.2-1 評価者は、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を***検査しなければならない。***

1502 開発者によって提供され、テスト計画で識別される TOE は、CM 能力(ALC_CMC)サブアクティビティによって確立され ST 概説で識別されているのと同じ、一意の参照を持つべきである。

1503 ST は、評価のための複数の構成を特定することができる。TOE は、ST に従ってテストする必要がある多数の異なるハードウェアエンティティ及びソフトウェアエンティティで構成される可能性がある。評価者は、すべてのテスト構成が ST と一貫していることを検証する。

1504 評価者は、テスト環境に適用できる ST に記述されている運用環境のセキュリティ対策方針を考慮し、それらがテスト環境で満たされていることを保証するべきである。テスト環境に適用されないいくつかの対策方針が、運用環境用に存在することがある。例えば、利用者の利用許可についての対策方針は適用しないことがあるが、ネットワークへの 1 つのポイントでの接続についての対策方針は適用するだろう。

1505 いずれかのテスト資源(例えば、メーター、アナライザ)が使用される場合、これらの資源が正しく調整されるようにするのは、評価者の責任である。

AVA_VAN.2-2 評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1506 評価者は、各種の方法で TOE の状態を決定することができる。例えば、サブアクティビティの評価(AGD_PRE.1)がこれまでに成功裏に完了していることは、評価者がテストに使用されている TOE が適切に設置され、定義された状態にあることを今もなお信頼している場合、このワークユニットの条件を満たすことになる。そうでない場合には、評価者は、提供されたガイダンスだけを使用し、開発者の手順に従って、TOE を設置し、立ち上げるべきである。

1507 TOE が未定義の状態であるために、評価者が設置手順を実行しなければならない場合、このワークユニットは、成功裏に完了したとき、ワークユニット AGD_PRE.1-3 の条件を満たすことができる。

16.2.2.5 アクション AVA_VAN.2.2E

AVA_VAN.2-3 評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を***検査しなければならない。***

1508 評価者は、TOE で発生する可能性がある潜在的な脆弱性の識別をサポートするために、公開の場で利用できる情報源を検査する。公開の場で利用できる、評価者が使用を考慮するべき多くの情報源がある。これらは world wide web で利用可能な要素などで、次のものが含まれる:

a) 専門家向け発行物(雑誌、書籍);

b) 調査報告書。

1509 評価者は、公開の場で利用可能な情報の考慮を上記のものに制約するべきではなく、その他の利用できるすべての関連情報を考慮するべきである。

1510 提供された証拠を検査する間に、評価者は、公知の情報を使用して、潜在的な脆弱性の探索をさらに進める。評価者が関心の分野を識別した場合、評価者は、それらの関心の分野に関連する公開の場で利用できる情報を考慮するべきである。

1511 攻撃者が容易に入手できて、攻撃を識別し、容易にするのを支援する情報の入手の可能性は、想定される攻撃者の攻撃能力を大幅に向上させるのに効果的である。インターネットにおける脆弱性情報と高機能の攻撃ツールのアクセスのしやすさは、この情報が TOE の潜在的な脆弱性を識別し、それらを悪用するために使用されるということの可能性を増大させる。現代の探索ツールによって、評価者がこのような情報を簡単に利用できるようになり、公開されている潜在的な脆弱性及びよく知られている一般的な攻撃に対する抵抗の決定は、費用効果の高い方法で達成できる。

1512 公開の場で利用できる情報の探索は、TOE の派生元である製品を特に参照する情報源に焦点を置くべきである。この探索の範囲の拡張については、次の要因を考慮するべきである。TOE 種別、この TOE 種別の評価者の経験、予想される攻撃能力、及び利用できるADV証拠のレベル。

1513 識別プロセスは繰返して行われ、その場合、1 つの潜在的な脆弱性の識別が、それ以上の調査が必要となる別の関心分野の識別へとつながることがある。

1514 評価者は、証拠内の潜在的な脆弱性を識別するために、どのようなアクションがとられたかを報告する。ただし、このタイプの探索では、探索中の検出の結果によって手法が発展する可能性があるため、評価者は、検査の開始前に潜在的な脆弱性の識別における手順を記述できない可能性がある。

1515 評価者は、潜在的な脆弱性の探索を完了する際に、検査された証拠を報告する。この証拠の選択は、攻撃者が取得できるものと想定されている証拠に関連する、評価者によって識別された関心の分野から派生するか、評価者によって提供された別の根拠に従って行うことができる。

16.2.2.6 アクション AVA_VAN.2.3E

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

1516 TOE の仕様及び証拠資料が分析され、TOE の潜在的な脆弱性が仮定されるかまたは推測されることにより、証拠の探索が完了されるべきである。次に、仮定された潜在的な脆弱性のリストには、潜在的な脆弱性が存在することの予測される確率、及び悪用される可能性がある脆弱性が存在することを想定して、それを悪用するために必要な攻撃能力、それがもたらす制御または弱体化の範囲に基づいて優先順位が付けられる。潜在的な脆弱性の優先順位が付けられたリストは、TOE に対する侵入テストを指示するために使用される。

1517 セキュリティアーキテクチャ記述は、TSF が信頼できないサブジェクトによる干渉からどのように自己を保護し、セキュリティ実施機能性のバイパスを阻止するかを引証していることから、開発者脆弱性分析を提供する。したがって評価者は、TSF を侵害する手段を探索するための基礎として、TSF の保護に関するこの記述を使用するべきである。

1518 運用環境で TOE が満たす SFR に従って、評価者の独立脆弱性分析は、次の各見出しの一般的な潜在的脆弱性を考慮するべきである:

a) 評価監督機関から提供されることもある、評価されている TOE の種別に関する一般的な潜在的脆弱性;

b) バイパス;

c) 改ざん;

d) 直接攻撃;

e) 監視;

f) 誤使用。

1519 項目 b)から f)については、附属書 B でさらに詳しく説明する。

1520 セキュリティアーキテクチャ記述は、上記の一般的な各潜在的脆弱性を踏まえて考慮されるべきである。TSF の保護を破り、TSF を侵害する手段を探索するために、各潜在的脆弱性が考慮されるべきである。

AVA_VAN.2-5 評価者は、ETR 内で、テストの候補となり、運用環境の TOE に適用できる識別された潜在的な脆弱性を***記録しなければならない。***

1521 例えば、評価者が IT または非 IT の運用環境の手段によってその運用環境では潜在的な脆弱性の悪用が防止されることを識別する場合、潜在的な脆弱性についてそれ以上の考慮は不要であることが識別される可能性がある。例えば、TOE への物理的アクセスを許可利用者だけに制限することにより、効果的に潜在的な脆弱性が改ざんに悪用されないようにすることができる。

1522 評価者が運用環境で潜在的な脆弱性が該当しないことを決定する場合、評価者は、それ以上の考慮から潜在的な脆弱性を除外する理由を記録する。それ以外の場合は、評価者は、さらに考慮する対象となる潜在的な脆弱性を記録する。

1523 運用環境の TOE に適用できる潜在的な脆弱性のリストは、侵入テストアクティビティに対する入力として使用でき、評価者が ETR で報告しなければならない。

16.2.2.7 アクション AVA_VAN.2.4E

AVA_VAN.2-6 評価者は、潜在的な脆弱性に対する独立探索に基づいて、侵入テストを***考え出さなければならない。***

1524 評価者は、必要に応じて、公開の場で利用できる情報源の探索及び TOE ガイダンスと設計証拠の分析の間に識別される潜在的な脆弱性が、運用環境における TOE にどの程度あてはまるかを決定するために、侵入テストを準備する。既知の潜在的な脆弱性に関して、第三者(例えば、評価監督機関からの)によって評価者に提供されたどんな現在の情報も、他の評価アクティビティを実行した結果として生じる潜在的な脆弱性とともに、考慮される。

1525 評価者は、脆弱性の探索におけるセキュリティアーキテクチャ記述の考慮(AVA_VAN.2-4 で詳述)に関連して、アーキテクチャ特性を確認するためにテストを実行するべきであることに留意する。この場合、セキュリティアーキテクチャ特性の反証を試みる否定テストが必要となる可能性がある。侵入テストの方策を開発する際に、評価者は、セキュリティアーキテクチャ記述の主要な各特性が、機能テスト(15 で考慮)または評価者侵入テストでテストされることを保証する。

1526 評価者は恐らく、各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することを、実用的だと感じるだろう。

1527 評価者は、基本的な攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が基本的な攻撃能力を超える悪用可能な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

1528 潜在的な脆弱性を悪用するために必要な攻撃能力の決定に関するガイダンスは、附属書 B.4 に記載されている。

1529 強化基本、中、または高の攻撃能力を持つ攻撃者によってのみ悪用可能と仮定された潜在的な脆弱性のために、この評価者アクションが不合格になることはない。分析がこの仮定を裏付ける場合、これらを侵入テストの入力としてこれ以上考慮する必要はない。ただし、そのような脆弱性は、残存脆弱性として ETR に報告される。

1530 基本的な攻撃能力を持つ攻撃者によって悪用される可能性があると仮定され、セキュリティ対策方針の違反となる潜在的な脆弱性は、TOE に対する侵入テストを指示するために使用されるリストを構成する優先順位の最も高い潜在的な脆弱性とするべきである。

AVA_VAN.2-7 評価者は、潜在的な脆弱性のリストに基づき、テストを再現可能にするために十分に詳細に侵入テスト証拠資料を***作成しなければならない。***テスト証拠資料には、次のものを含めなければならない:

a) TOE はどの潜在的な脆弱性の調査のためにテストされるか、その脆弱性の識別;

b) 侵入テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示;

c) すべての侵入テスト前提初期条件を確立するための指示;

d) TSF を刺激するための指示;

e) TSF のふるまいを観察するための指示;

f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述;

g) TOE のテストを終了し、終了後の必要な状態を確立するための指示。

1531 評価者は、公知になっているものの探索及び評価証拠の分析の間に識別された潜在的な脆弱性のリストに基づいて、侵入テストを準備する。

1532 評価者は、攻撃が功を奏するために基本的な攻撃能力を必要とする脆弱性を超える潜在的な脆弱性の悪用される可能性を決定することを期待されない。ただし、評価の専門知識の結果として、評価者は、基本的な攻撃能力を超える攻撃者のみが悪用できる潜在的な脆弱性を発見することがある。そのような脆弱性は、残存脆弱性として ETR に報告される。

1533 潜在的な脆弱性を理解し、評価者は、TOE にどの程度あてはまるかをテストするための最も適切な方法を決定する。特に、評価者は、次のことを考慮する:

a) TSF を刺激し、反応を観察するために使用される TSFI またはその他の TOE インタフェース(評価者は、(ADV_ARCによる要求に従い)セキュリティアーキテクチャの記述で記述されているものなど、TSF の特性を実証するために、TSFI 以外の TOE へのインタフェースを使用する必要がある可能性がある。これらの TOE インタフェースは TSF の特性をテストする手段を提供するが、これらはテストの対象ではないことに注意するべきである);

b) テストに存在する必要がある初期条件(つまり、存在する必要がある特定のオブジェクトまたはサブジェクト及びそれらが持つ必要があるセキュリティ属性);

c) TSFI を刺激するため、または TSFI を観察するために必要となる特別のテスト装置(おそらく、基本的な攻撃能力を想定している潜在的な脆弱性を悪用するために特別の装置が必要になることはない);

d) 物理的なテストを論理的分析に置き換えるべきであるかどうか。初期テストの結果から、繰返し試みられた攻撃が、指定した試行回数の後に成功する可能性が高いことが実証されると推定できる場合は、特に関連する。

1534 評価者は恐らく、各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することを、実用的だと感じるだろう。

1535 テスト証拠資料にこのレベルの詳細を特定する意図は、他の評価者がテストを再現し、同等の結果を得ることができるようにすることである。

AVA_VAN.2-8 評価者は、侵入テストを***実施しなければならない。***

1536 評価者は、TOE の侵入テストの実行のための基礎として、ワークユニット AVA_VAN.2-6 の結果の侵入テスト証拠資料を使用するが、これは、評価者がその場で追加の侵入テストを実行することを排除しない。必要に応じて、評価者は、侵入テスト中に得られた情報の結果としてその場でテストを考え出すことができ、評価者により行われたならば、そのテストは侵入テスト証拠資料に記録される。そのようなテストは、期待されない結果または観察を追求するか、または事前に計画されたテスト中に評価者に示された潜在的な脆弱性を調査するために必要となる可能性がある。

1537 侵入テストが仮定される潜在的な脆弱性が存在することを示さない場合には、評価者は、評価者自身の分析が正しくないかどうか、または評価用提供物件が正しくないか不完全であるかどうかを決定するべきである。

1538 評価者は、基本的な攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が基本的な攻撃能力を超える悪用可能な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

AVA_VAN.2-9 評価者は、侵入テストの実際の結果を***記録しなければならない。***

1539 実際のテスト結果の特定の詳細のいくつか(例えば、監査レコードの時刻と日付フィールド)が期待されたものと異なるかもしれないが、全体的な結果は、同一であるべきである。期待されないテスト結果は、調査するべきである。評価への影響は、述べられ、正当化されるべきである。

AVA_VAN.2-10 評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者の侵入テストの成果を***報告しなければならない。***

1540 ETR に報告される侵入テスト情報によって、評価者は全体的な侵入テスト手法及びこのサブアクティビティで費やした成果を伝えることができる。この情報を提供する意図は、評価者の侵入テスト成果の意味ある概要を示すことである。ETR の侵入テストに関する情報が、特定のテストステップの正確な再現であることまたは個々の侵入テストの結果であることを意図しない。意図するのは、十分詳細な情報を提供し、他の評価者と評価監督機関が選択された侵入テスト手法、実行された侵入テストの量、TOE テスト構成、侵入テストアクティビティの全体的な結果を洞察できるようにすることである。

1541 評価者の侵入テスト成果に関する ETR セクションに通常示される情報は、次のとおりである:

a) TOE テスト構成。侵入テストが行われた TOE の特定の構成;

b) 侵入テストされた TSFI。侵入テストの焦点となった TSFI 及びその他の TOE インタフェースの簡単なリスト;

c) サブアクティビティの判定。侵入テスト結果の総合判断。

1542 このリストは、必ずしも徹底したものではなく、評価中に評価者が行った侵入テストに関する、ETR に示すべき情報の種別を提供することだけを意図している。

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

1543 TOE が、運用環境において、強化基本的な攻撃能力に欠ける攻撃者によって悪用可能な脆弱性があることを結果が示す場合、この評価者アクションは不合格となる。

1544 特定の脆弱性を悪用するために必要な攻撃能力、及び意図された環境でその悪用が可能かどうかを決定するために、附属書 B.4 のガイダンスを使用するべきである。攻撃能力の計算は必ずしもすべての場合に必要となるわけではなく、強化基本的な攻撃能力に欠ける攻撃者によって脆弱性が悪用可能かどうかについて疑問がある場合に限られる。

AVA_VAN.2-12 評価者は、ETR に、すべての悪用され得る脆弱性と残存脆弱性を、次のそれぞれを詳細に述べて*報告しなければならない*:

a) 出所(例えば、脆弱性が予想されたとき実行していた CEM アクティビティ、評価者に既知である、公表されたものを読んで知った、など);

b) 満たされていない SFR(1 つまたは複数);

c) 記述;

d) 運用環境で悪用されるか否か(つまり、悪用される可能性があるか残存か);

e) 識別された脆弱性を実行するために必要な時間量、専門知識のレベル、TOE に関する知識のレベル、機会のレベル、及び装置。及び附属書 B.4 の表 3 及び 4 を使用した対応する値。

16.2.3 サブアクティビティの評価(AVA_VAN.3)

16.2.3.1 目的

1545 このサブアクティビティの目的は、TOE が、その運用環境において、強化基本的な攻撃能力を持つ攻撃者が悪用できる脆弱性を持つかどうかを決定することである。

16.2.3.2 入力

1546 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計;

d) セキュリティアーキテクチャ記述;

e) 選択された実装サブセット;

f) ガイダンス証拠資料;

g) テストに適した TOE;

h) 考えられる潜在的な脆弱性の識別をサポートするために公開の場で利用できる情報;

i) 基本設計のテスト結果。

1547 このサブアクティビティの暗黙の評価証拠の残りの部分は、保証パッケージに含まれているコンポーネントによって異なる。各コンポーネントに対して提供された証拠は、このサブアクティビティで入力として使用される。

1548 このサブアクティビティのその他の入力は、次のとおりである:

a) 公知になっている潜在的な脆弱性及び攻撃に関する現在の情報(例えば、評価監督機関からの情報)。

16.2.3.3 適用上の注釈

1549 評価アクティビティの実施中に、評価者は関心の分野を識別することもある。これらは、証拠が関連付けられているアクティビティの要件を証拠は満たすが、評価者が不安を抱いている TOE 証拠の特定の部分である。例えば、特定のインタフェース仕様が特に複雑に見えるため、TOE の開発または TOE の運用において誤りが発生しやすくなる可能性がある。この段階では、明白な潜在的な脆弱性は存在しないが、さらに調査が必要である。これは、さらに調査が必要なため、遭遇により識別される範囲を越えている。

1550 潜在的な脆弱性の識別に焦点を置いた手法は、含まれている情報から明らかになるような潜在的な脆弱性の識別を目的とした、証拠の分析である。この手法は事前に決定されていないため、これは、構造化されていない分析になる。焦点を置いた脆弱性分析のさらに詳しいガイダンスは、附属書 B.2.2.2.2 に記載されている。

16.2.3.4 アクション AVA_VAN.3.1E

AVA_VAN.3.1C ***TOE は、テストに適していなければならない。***

AVA_VAN.3-1 評価者は、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を***検査しなければならない。***

1551 開発者によって提供され、テスト計画で識別される TOE は、CM 能力(ALC_CMC)サブアクティビティによって確立され ST 概説で識別されているのと同じ、一意の参照を持つべきである。

1552 ST は、評価のための複数の構成を特定することができる。TOE は、ST に従ってテストする必要がある多数の異なるハードウェアエンティティ及びソフトウェアエンティティで構成される可能性がある。評価者は、すべてのテスト構成が ST と一貫していることを検証する。

1553 評価者は、テスト環境に適用できる ST に記述されている運用環境のセキュリティ対策方針を考慮し、それらがテスト環境で満たされていることを保証するべきである。テスト環境に適用されないいくつかの対策方針が、運用環境用に存在することがある。例えば、利用者の利用許可についての対策方針は適用しないことがあるが、ネットワークへの 1 つのポイントでの接続についての対策方針は適用するだろう。

1554 いずれかのテスト資源(例えば、メーター、アナライザ)が使用される場合、これらの資源が正しく調整されるようにするのは、評価者の責任である。

AVA_VAN.3-2 評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1555 評価者は、各種の方法で TOE の状態を決定することができる。例えば、サブアクティビティの評価(AGD_PRE.1)がこれまでに成功裏に完了していることは、評価者がテストに使用されている TOE が適切に設置され、定義された状態にあることを今もなお信頼している場合、このワークユニットの条件を満たすことになる。そうでない場合には、評価者は、提供されたガイダンスだけを使用し、開発者の手順に従って、TOE を設置し、立ち上げるべきである。

1556 TOE が未定義の状態であるために、評価者が設置手順を実行しなければならない場合、このワークユニットは、成功裏に完了したとき、ワークユニット AGD_PRE.1-3 の条件を満たすことができる。

16.2.3.5 アクション AVA_VAN.3.2E

AVA_VAN.3-3 評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を***検査しなければならない。***

1557 評価者は、TOE で発生する可能性がある潜在的な脆弱性の識別をサポートするために、公開の場で利用できる情報源を検査する。公開の場で利用できる、評価者が使用を考慮するべき多くの情報源がある。これらは world wide web で利用可能な要素などで、次のものが含まれる:

a) 専門家向け発行物(雑誌、書籍);

b) 調査報告書;

c) カンファレンスの記録。

1558 評価者は、公開の場で利用可能な情報の考慮を上記のものに制約するべきではなく、その他の利用できるすべての関連情報を考慮するべきである。

1559 提供された証拠を検査する間に、評価者は、公知の情報を使用して、潜在的な脆弱性の探索をさらに進める。評価者が関心の分野を識別した場合、評価者は、それらの関心の分野に関連する公開の場で利用できる情報を考慮するべきである。

1560 攻撃者が容易に入手できて、攻撃を識別し、容易にするのを支援する情報の入手の可能性は、想定される攻撃者の攻撃能力を大幅に向上させるのに効果的である。インターネットにおける脆弱性情報と高機能の攻撃ツールのアクセスのしやすさは、この情報が TOE の潜在的な脆弱性を識別し、それらを悪用するために使用されるということの可能性を増大させる。現代の探索ツールによって、評価者がこのような情報を簡単に利用できるようになり、公開されている潜在的な脆弱性及びよく知られている一般的な攻撃に対する抵抗の決定は、費用効果の高い方法で達成できる。

1561 公開の場で利用できる情報の探索は、TOE の派生元である製品の開発で使用される技術を参照する情報源に焦点を置くべきである。この探索の範囲の拡張については、次の要因を考慮するべきである。TOE 種別、この TOE 種別の評価者の経験、予想される攻撃能力、及び利用できるADV証拠のレベル。

1562 識別プロセスは繰返して行われ、その場合、1 つの潜在的な脆弱性の識別が、それ以上の調査が必要となる別の関心分野の識別へとつながることがある。

1563 評価者は、証拠内の潜在的な脆弱性を識別するために、どのようなアクションがとられたかを報告する。ただし、このタイプの探索では、探索中の検出の結果によって手法が発展する可能性があるため、評価者は、検査の開始前に潜在的な脆弱性の識別における手順を記述できない可能性がある。

1564 評価者は、潜在的な脆弱性の探索を完了する際に、検査された証拠を報告する。この証拠の選択は、攻撃者が取得できるものと想定されている証拠に関連する、評価者によって識別された関心の分野から派生するか、評価者によって提供された別の根拠に従って行うことができる。

16.2.3.6 アクション AVA_VAN.3.3E

AVA_VAN.3-4 評価者は、TOE に存在する可能性がある潜在的な脆弱性を識別するために、ST、ガイダンス証拠資料、機能仕様、TOE 設計、セキュリティアーキテクチャ記述、及び実装表現に焦点を置いた探索を***実施しなければならない。***

1565 欠陥仮説法が使用される必要があり、これにより、仕様及び開発証拠とガイダンス証拠が分析され、TOE の潜在的な脆弱性が仮定されるかまたは推測される。

1566 評価者は、TOE の開発における潜在的な欠陥及び TOE の特定された運用方法における潜在的な誤りを識別するために、TOE 提供物件から取得した TOE 設計及び運用の知識を使用して、欠陥仮説法を実施する。

1567 セキュリティアーキテクチャ記述は、TSF が信頼できないサブジェクトによる干渉からどのように自己を保護し、セキュリティ実施機能性のバイパスを阻止するかを引証していることから、開発者脆弱性分析を提供する。したがって評価者は、この証拠の分析から TSF 保護についての理解を確立し、他の開発ADVの証拠から得られた知識でこれを発展させるべきである。

1568 採用される手法は評価アクティビティの実施中に行われた証拠の検査中に識別された関心の分野に従い、評価のために提供された開発及びガイダンス証拠の代表的なサンプルが探索されたことを保証する。

1569 サンプリングのガイダンスについては、附属書 A.2 を参照のこと。このガイダンスは、サブセットの選択時に、次のものに対する理由を示しながら考慮されるべきである:

a) 選択で使用された手法;

b) 検査される証拠がその手法をサポートするのに適切か。

1570 関心分野は、セキュリティアーキテクチャ記述で詳述されている特定の保護機能の特徴の十分性に関係している場合がある。

1571 脆弱性分析の間に考慮される証拠は、攻撃者が取得できるものと想定されている証拠に関連する可能性がある。例えば、開発者は TOE 設計及び実装表現を保護することができ、その場合、攻撃者が利用できると想定される情報は、機能仕様とガイダンス(公開の場で利用できる)のみである。このため、TOE における保証の目的が TOE 設計と実装表現の要件が満たされることを保証することである場合でも、これらの設計表現は、関心分野をさらに調査するためだけに探索される可能性がある。

1572 他方、情報源が公開の場で利用できる場合は、攻撃者がその情報源に対するアクセスを持ち、TOE への攻撃を試行する際にこれを使用できると想定することが合理的である。このため、情報源は、焦点を置いた検査手法で考慮されるべきである。

1573 考慮される証拠のサブセットの選択の例を次に示す:

a) 機能仕様から実装表現まで、設計抽象のすべてのレベルが提供される場合の評価については、攻撃者が利用できるインタフェースの詳細を機能仕様が提供し、実装表現がすべてのその他の設計抽象で行われた設計上の決定を組み込むため、機能仕様及び実装表現の情報の検査が選択される可能性がある。このため、TOE 設計情報は、実装表現の一部として考慮される。

b) 評価に対して提供された各設計表現における情報の特定のサブセットの検査。

c) 評価に対して提供される各設計表現を通した特定の SFR のカバレージ。

d) 各設計表現内の様々な SFR を考慮し、評価に対して提供された各設計表現の検査。

e) (例えば、制度から)評価者が受け取った現在の潜在的な脆弱性情報に関連する評価に対して提供された証拠の様々な側面の検査。

1574 潜在的な脆弱性の識別に対するこの手法は、順序付けられ計画された手法をとること、つまり、体系的な方法を検査に適用することである。評価者は、どのような証拠が考慮されるか、検査される証拠内の情報、この情報が考慮される方法、及び立てられる仮定の観点から使用される方法を記述する。

1575 仮定に含まれる可能性があるいくつかの例を次に示す:

a) 外部インタフェースで攻撃者に対して利用可能な状態になっているインタフェースに対する誤った形式の入力の考慮;

b) セキュリティアーキテクチャ記述で引用されているプロセス分離などの主要なセキュリティメカニズムを検査し、分離の劣化をもたらす可能性がある内部バッファオーバフローを仮定;

c) TOE 実装表現においては作成されることになっており、その時点では完全には TSF によって制御されておらず、SFR を損なうために攻撃者によって使用される可能性がある任意のオブジェクトを識別するための探索。

1576 例えば、評価者は、インタフェースが TOE の潜在的な弱点の分野であることを識別し、「機能仕様及び TOE 設計で提供されたすべてのインタフェース仕様が潜在的な脆弱性を仮定するために探索される」という探索に対する手法を特定し、続けてこの仮定で使用される方法を説明することができる。

1577 識別プロセスは繰返して行われ、その場合、1 つの潜在的な脆弱性の識別が、それ以上の調査が必要となる別の関心分野の識別へとつながることがある。

1578 評価者は、証拠内の潜在的な脆弱性を識別するために、どのようなアクションがとられたかを報告する。ただし、このタイプの探索では、探索中の検出の結果によって手法が発展する可能性があるため、評価者は、検査の開始前に潜在的な脆弱性の識別における手順を記述できない可能性がある。

1579 評価者は、潜在的な脆弱性の探索を完了する際に、検査された証拠を報告する。この証拠の選択は、攻撃者が取得できるものと想定されている証拠に関連する、評価者によって識別された関心の分野から派生するか、評価者によって提供された別の根拠に従って行うことができる。

1580 運用環境で TOE が満たす SFR に従って、評価者の独立脆弱性分析は、次の各見出しの一般的な潜在的脆弱性を考慮するべきである:

a) 評価監督機関から提供されることもある、評価されている TOE の種別に関する一般的な潜在的脆弱性;

b) バイパス;

c) 改ざん;

d) 直接攻撃;

e) 監視;

f) 誤使用。

1581 項目 b)から f)については、附属書 B でさらに詳しく説明する。

1582 セキュリティアーキテクチャ記述は、上記の一般的な各潜在的脆弱性を踏まえて考慮されるべきである。TSF の保護を破り、TSF を侵害する手段を探索するために、各潜在的脆弱性が考慮されるべきである。

AVA_VAN.3-5 評価者は、ETR 内で、テストの候補となり、運用環境の TOE に適用できる識別された潜在的な脆弱性を***記録しなければならない。***

1583 例えば、評価者が IT または非 IT の運用環境の手段によってその運用環境では潜在的な脆弱性の悪用が防止されることを識別する場合、潜在的な脆弱性についてそれ以上の考慮は不要であることが識別される可能性がある。例えば、TOE への物理的アクセスを許可利用者だけに制限することにより、効果的に潜在的な脆弱性が改ざんに悪用されないようにすることができる。

1584 評価者が運用環境で潜在的な脆弱性が該当しないことを決定する場合、評価者は、それ以上の考慮から潜在的な脆弱性を除外する理由を記録する。それ以外の場合は、評価者は、さらに考慮する対象となる潜在的な脆弱性を記録する。

1585 運用環境の TOE に適用できる潜在的な脆弱性のリストは、侵入テストアクティビティに対する入力として使用でき、評価者が ETR で報告しなければならない。

16.2.3.7 アクション AVA_VAN.3.4E

AVA_VAN.3-6 評価者は、潜在的な脆弱性に対する独立探索に基づいて、侵入テストを***考え出さなければならない。***

1586 評価者は、必要に応じて、公開の場で利用できる情報源の探索及び TOE ガイダンスと設計証拠の分析の間に識別される潜在的な脆弱性が、運用環境における TOE にどの程度あてはまるかを決定するために、侵入テストを準備する。既知の潜在的な脆弱性に関して、第三者(例えば、評価監督機関からの)によって評価者に提供されたどんな現在の情報も、他の評価アクティビティを実行した結果として生じる潜在的な脆弱性とともに、考慮される。

1587 評価者は、脆弱性の探索におけるセキュリティアーキテクチャ記述の考慮(AVA_VAN.3-4 で詳述)に関連して、アーキテクチャ特性を確認するためにテストを実行するべきであることに留意する。ATE_DPTからの要件が SAR に含まれている場合、開発者テスト証拠には、セキュリティアーキテクチャ記述で詳述されている特定のメカニズムの正しい実装を確認するために実行されたテストが組み込まれる。ただし、開発者テストには TSF を保護するアーキテクチャ特性のすべての側面のテストが必ずしも含まれない。これは、このテストの大部分が、本質的に特性の反証を試みる否定テストであるためである。侵入テストの方策を開発する際に、評価者は、セキュリティアーキテクチャ記述のすべての側面が、機能テスト(15 で考慮)または評価者侵入テストでテストされることを保証する。

1588 各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することは、おそらく実用的だろう。

1589 評価者は、強化基本的な攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が強化基本的な攻撃能力を超える悪用可能な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

1590 潜在的な脆弱性を悪用するために必要な攻撃能力の決定に関するガイダンスは、附属書 B.4 に記載されている。

1591 中程度から高い攻撃能力を持つ攻撃者によってのみ悪用可能と仮定された潜在的な脆弱性のために、この評価者のアクションは不合格にはならない。分析がこの仮定を裏付ける場合、これらを侵入テストの入力としてこれ以上考慮する必要はない。ただし、そのような脆弱性は、残存脆弱性として ETR に報告される。

1592 基本的な攻撃能力または強化基本的な攻撃能力を持つ攻撃者によって悪用される可能性があると仮定され、セキュリティ対策方針の違反となる潜在的な脆弱性は、TOE に対する侵入テストを指示するために使用されるリストを構成する優先順位の最も高い潜在的な脆弱性とするべきである。

AVA_VAN.3-7 評価者は、潜在的な脆弱性のリストに基づき、テストを再現可能にするために十分に詳細に侵入テスト証拠資料を***作成しなければならない。***テスト証拠資料には、次のものを含めなければならない:

a) TOE はどの潜在的な脆弱性の調査のためにテストされるか、その脆弱性の識別;

b) 侵入テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示;

c) すべての侵入テスト前提初期条件を確立するための指示;

d) TSF を刺激するための指示;

e) TSF のふるまいを観察するための指示;

f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述;

g) TOE のテストを終了し、終了後の必要な状態を確立するための指示。

1593 評価者は、公知になっているものの探索及び評価証拠の分析の間に識別された潜在的な脆弱性のリストに基づいて、侵入テストを準備する。

1594 評価者は、攻撃が功を奏するために強化基本的な攻撃能力を必要とする脆弱性を超える潜在的な脆弱性の悪用される可能性を決定することを期待されない。ただし、評価の専門知識の結果として、評価者は、基本的な攻撃能力を超える攻撃者のみが悪用できる潜在的な脆弱性を発見することがある。そのような脆弱性は、残存脆弱性として ETR に報告される。

1595 潜在的な脆弱性を理解し、評価者は、TOE にどの程度あてはまるかをテストするための最も適切な方法を決定する。特に、評価者は、次のことを考慮する:

a) TSF を刺激し、反応を観察するために使用される TSFI またはその他の TOE インタフェース(評価者は、(ADV_ARCによる要求に従い)セキュリティアーキテクチャの記述で記述されているものなど、TSF の特性を実証するために、TSFI 以外の TOE へのインタフェースを使用する必要がある可能性がある。これらの TOE インタフェースは TSF の特性をテストする手段を提供するが、これらはテストの対象ではないことに注意するべきである);

b) テストに存在する必要がある初期条件(つまり、存在する必要がある特定のオブジェクトまたはサブジェクト及びそれらが持つ必要があるセキュリティ属性);

c) TSFI を刺激するため、または TSFI を観察するために必要となる特別のテスト装置(おそらく、強化基本的な攻撃能力を想定している潜在的な脆弱性を悪用するために特別の装置が必要になることはない);

d) 物理的なテストを論理的分析に置き換えるべきであるかどうか。初期テストの結果から、繰返し試みられた攻撃が、指定した試行回数の後に成功する可能性が高いことが実証されると推定できる場合は、特に関連する。

1596 評価者は恐らく、各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することを、実用的だと感じるだろう。

1597 テスト証拠資料にこのレベルの詳細を特定する意図は、他の評価者がテストを再現し、同等の結果を得ることができるようにすることである。

AVA_VAN.3-8 評価者は、侵入テストを***実施しなければならない。***

1598 評価者は、TOE の侵入テストの実行のための基礎として、ワークユニット AVA_VAN.3-6 の結果の侵入テスト証拠資料を使用するが、これは、評価者がその場で追加の侵入テストを実行することを排除しない。必要に応じて、評価者は、侵入テスト中に得られた情報の結果としてその場でテストを考え出すことができ、評価者により行われたならば、そのテストは侵入テスト証拠資料に記録される。そのようなテストは、期待されない結果または観察を追求するか、または事前に計画されたテスト中に評価者に示された潜在的な脆弱性を調査するために必要となる可能性がある。

1599 侵入テストが仮定される潜在的な脆弱性が存在することを示さない場合には、評価者は、評価者自身の分析が正しくないかどうか、または評価用提供物件が正しくないか不完全であるかどうかを決定するべきである。

1600 評価者は、強化基本的な攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が強化基本的な攻撃能力を超える悪用可能な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

AVA_VAN.3-9 評価者は、侵入テストの実際の結果を***記録しなければならない。***

1601 実際のテスト結果の特定の詳細のいくつか(例えば、監査レコードの時刻と日付フィールド)が期待されたものと異なるかもしれないが、全体的な結果は、同一であるべきである。期待されないテスト結果は、調査するべきである。評価への影響は、述べられ、正当化されるべきである。

AVA_VAN.3-10 評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者の侵入テストの成果を***報告しなければならない。***

1602 ETR に報告される侵入テスト情報によって、評価者は全体的な侵入テスト手法及びこのサブアクティビティで費やした成果を伝えることができる。この情報を提供する意図は、評価者の侵入テスト成果の意味ある概要を示すことである。ETR の侵入テストに関する情報が、特定のテストステップの正確な再現であることまたは個々の侵入テストの結果であることを意図しない。意図するのは、十分詳細な情報を提供し、他の評価者と評価監督機関が選択された侵入テスト手法、実行された侵入テストの量、TOE テスト構成、侵入テストアクティビティの全体的な結果を洞察できるようにすることである。

1603 評価者の侵入テスト成果に関する ETR セクションに通常示される情報は、次のとおりである:

a) TOE テスト構成。侵入テストが行われた TOE の特定の構成;

b) 侵入テストされた TSFI。侵入テストの焦点となった TSFI 及びその他の TOE インタフェースの簡単なリスト;

c) サブアクティビティの判定。侵入テスト結果の総合判断。

1604 このリストは、必ずしも徹底したものではなく、評価中に評価者が行った侵入テストに関する、ETR に示すべき情報の種別を提供することだけを意図している。

AVA_VAN.3-11 評価者は、TOE が、運用環境において、強化基本的な攻撃能力を持つ攻撃者に耐えられることを決定するために、すべての侵入テストの結果を***検査しなければならない。***

1605 TOE が、運用環境において、中程度の攻撃能力に欠ける攻撃者によって悪用可能な脆弱性を持っていることを結果が示す場合、この評価者のアクションは不合格となる。

1606 特定の脆弱性を悪用するために必要な攻撃能力、及び意図された環境でその悪用が可能かどうかを決定するために、附属書 B.4 のガイダンスを使用するべきである。攻撃能力の計算は必ずしもすべての場合に必要となるわけではなく、中程度の攻撃能力に欠ける攻撃者によって脆弱性が悪用可能かどうかについて疑問がある場合に限られる。

AVA_VAN.3-12 評価者は、ETR に、すべての悪用され得る脆弱性と残存脆弱性を、次のそれぞれを詳細に述べて***報告しなければならない：***

a) 出所(例えば、脆弱性が予想されたとき実行していた CEM アクティビティ、評価者に既知である、公表されたものを読んで知った、など);

b) 満たされていない SFR(1 つまたは複数);

c) 記述;

d) 運用環境で悪用されるか否か(つまり、悪用される可能性があるか残存か);

e) 識別された脆弱性を実行するために必要な時間量、専門知識のレベル、TOE に関する知識のレベル、機会のレベル、及び装置。及び附属書 B.4 の表 3 及び 4 を使用した対応する値。

16.2.4 サブアクティビティの評価(AVA_VAN.4)

16.2.4.1 目的

1607 このサブアクティビティの目的は、TOE が、その運用環境において、中程度の攻撃能力を持つ攻撃者が悪用できる脆弱性を持つかどうかを決定することである。

16.2.4.2 入力

1608 このサブアクティビティ用の評価証拠は、次のとおりである:

a) ST;

b) 機能仕様;

c) TOE 設計;

d) セキュリティアーキテクチャ記述;

e) 実装表現;

f) ガイダンス証拠資料;

g) テストに適した TOE;

h) 考えられる潜在的な脆弱性の識別をサポートするために公開の場で利用できる情報;

i) 基本設計のテスト結果。

1609 このサブアクティビティの暗黙の評価証拠の残りの部分は、保証パッケージに含まれているコンポーネントによって異なる。各コンポーネントに対して提供された証拠は、このサブアクティビティで入力として使用される。

1610 このサブアクティビティのその他の入力は、次のとおりである:

a) 公知になっている潜在的な脆弱性及び攻撃に関する現在の情報(例えば、評価監督機関からの情報)。

16.2.4.3 適用上の注釈

1611 系統的分析手法は、証拠の構造化された検査の形式をとる。この方法では、分析が採用する構造と形式を評価者が特定する必要がある(つまり、焦点が置かれた分析とは異なり、分析が実行される方法が事前に決定されている)。この方法は、考慮される情報及び考慮される方法/理由の観点で特定される。系統的な脆弱性分析についてのさらに詳しいガイダンスは、附属書 B.2.2.2.3 に記載されている。

16.2.4.4 アクション AVA_VAN.4.1E

AVA_VAN.4.1C ***TOE は、テストに適していなければならない。***

AVA_VAN.4-1 評価者は、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を***検査しなければならない。***

1612 開発者によって提供され、テスト計画で識別される TOE は、CM 能力(ALC_CMC)サブアクティビティによって確立され ST 概説で識別されているのと同じ、一意の参照を持つべきである。

1613 ST は、評価のための複数の構成を特定することができる。TOE は、ST に従ってテストする必要がある多数の異なるハードウェアエンティティ及びソフトウェアエンティティで構成される可能性がある。評価者は、すべてのテスト構成が ST と一貫していることを検証する。

1614 評価者は、テスト環境に適用できる ST に記述されている運用環境のセキュリティ対策方針を考慮し、それらがテスト環境で満たされていることを保証するべきである。テスト環境に適用されないいくつかの対策方針が、運用環境用に存在することがある。例えば、利用者の利用許可についての対策方針は適用しないことがあるが、ネットワークへの 1 つのポイントでの接続についての対策方針は適用するだろう。

1615 いずれかのテスト資源(例えば、メーター、アナライザ)が使用される場合、これらの資源が正しく調整されるようにするのは、評価者の責任である。

AVA_VAN.4-2 評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1616 評価者は、各種の方法で TOE の状態を決定することができる。例えば、サブアクティビティの評価(AGD_PRE.1)がこれまでに成功裏に完了していることは、評価者がテストに使用されている TOE が適切に設置され、定義された状態にあることを今もなお信頼している場合、このワークユニットの条件を満たすことになる。そうでない場合には、評価者は、提供されたガイダンスだけを使用し、開発者の手順に従って、TOE を設置し、立ち上げるべきである。

1617 TOE が未定義の状態であるために、評価者が設置手順を実行しなければならない場合、このワークユニットは、成功裏に完了したとき、ワークユニット AGD_PRE.1-3 の条件を満たすことができる。

16.2.4.5 アクション AVA_VAN.4.2E

AVA_VAN.4-3 評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を***検査しなければならない。***

1618 評価者は、TOE で発生する可能性がある潜在的な脆弱性の識別をサポートするために、公開の場で利用できる情報源を検査する。公開の場で利用できる、評価者が使用を考慮するべき多くの情報源がある。これらは world wide web で利用可能な要素などで、次のものが含まれる:

a) 専門家向け発行物(雑誌、書籍);

b) 調査報告書;

c) カンファレンスの記録。

1619 評価者は、公開の場で利用可能な情報の考慮を上記のものに制約するべきではなく、その他の利用できるすべての関連情報を考慮するべきである。

1620 提供された証拠を検査する間に、評価者は、公知の情報を使用して、潜在的な脆弱性の探索をさらに進める。評価者が関心の分野を識別した場合、評価者は、それらの関心の分野に関連する公開の場で利用できる情報を考慮するべきである。

1621 攻撃者が容易に入手できて、攻撃を識別し、容易にするのを支援する情報の入手の可能性は、想定される攻撃者の攻撃能力を大幅に向上させるのに効果的である。インターネットにおける脆弱性情報と高機能の攻撃ツールのアクセスのしやすさは、この情報が TOE の潜在的な脆弱性を識別し、それらを悪用するために使用されるということの可能性を増大させる。現代の探索ツールによって、評価者がこのような情報を簡単に利用できるようになり、公開されている潜在的な脆弱性及びよく知られている一般的な攻撃に対する抵抗の決定は、費用効果の高い方法で達成できる。

1622 公開の場で利用できる情報の探索は、TOE の派生元である製品の開発で使用される技術を参照する情報源に焦点を置くべきである。この探索の範囲の拡張については、次の要因を考慮するべきである。TOE 種別、この TOE 種別の評価者の経験、予想される攻撃能力、及び利用できるADV証拠のレベル。

1623 識別プロセスは繰返して行われ、その場合、1 つの潜在的な脆弱性の識別が、それ以上の調査が必要となる別の関心分野の識別へとつながることがある。

1624 評価者は、実行される探索については詳細を示し、公開の場で利用できる資料における潜在的な脆弱性を識別するために使用される手法を記述する。これは、攻撃者が取得できるものと想定されている証拠に関連する、評価者によって識別された関心の分野などの要因によって引き起こされる可能性がある。ただし、この種別の探索では、探索中の検出の結果によって手法がさらに発展することは認められる。したがって、評価者は、手法として記述したアクションに加えて、潜在的な脆弱性をもたらすものと考えられる問題をさらに調査するために使用される任意のアクションも報告し、潜在的な脆弱性の探索を完了する際に検査された証拠を報告する。

16.2.4.6 アクション AVA_VAN.4.3E

AVA_VAN.4-4 評価者は、TOE に存在する可能性がある潜在的な脆弱性を識別するために、ST、ガイダンス証拠資料、機能仕様、TOE 設計、セキュリティアーキテクチャ記述、及び実装表現の系統的分析を***実施しなければならない。***

1625 系統的な脆弱性分析についてのガイダンスは、附属書 B.2.2.2.3 で規定される。

1626 潜在的な脆弱性の識別に対するこの手法は、順序付けられ計画された手法をとるものである。検査では、体系的な方法が適用される。評価者は、この情報が考慮される方法、及び立てられる仮定の観点から使用される方法を記述する。

1627 欠陥仮説法が使用される必要があり、これにより、ST、開発(機能仕様、TOE 設計、及び実装表現)及びガイダンス証拠が分析され、TOE の脆弱性が仮定されるかまたは推測される。

1628 評価者は、TOE の開発における潜在的な欠陥及び TOE の特定された運用方法における潜在的な誤りを識別するために、TOE 提供物件から取得した TOE 設計及び運用の知識を使用して、欠陥仮説法を実施する。

1629 セキュリティアーキテクチャ記述は、TSF が信頼できないサブジェクトによる干渉からどのように自己を保護し、セキュリティ実施機能性のバイパスを阻止するかを引証していることから、開発者脆弱性分析を提供する。したがって評価者は、この証拠の分析から TSF 保護についての理解を確立し、他の開発 ADV の証拠から得られた知識でこれを発展させるべきである。

1630 脆弱性の系統的探索に使用される手法は、評価者による開発及びガイダンス証拠の評定の結果で識別された関心の分野を考慮することである。ただし、評価者は、TSF の保護を侵害することのできる手段を探索するために、セキュリティアーキテクチャ分析の各側面も考慮するべきである。セキュリティアーキテクチャ記述に示されている資料に基づき、他の ADV の証拠から関係する問題を必要に応じて取り入れながら系統的分析を構築すると役に立つ場合がある。そうすれば、ADVの証拠のその他すべての資料が考慮されることを保証するように、この分析をさらに発展させることができる。

1631 証拠を検査しているときに立てられる可能性があるいくつかの仮説の例を次に示す:

a) 外部インタフェースで攻撃者に対して利用可能な状態になっているインタフェースに対する誤った形式の入力の考慮;

b) セキュリティアーキテクチャ記述で引用されているプロセス分離などの主要なセキュリティメカニズムを検査し、分離の劣化をもたらす可能性がある内部バッファオーバフローを仮定;

c) TOE 実装表現においては作成されることになっており、その時点では完全には TSF によって制御されておらず、SFR を損なうために攻撃者によって使用される可能性がある任意のオブジェクトを識別するための探索。

1632 例えば、評価者は、インタフェースが TOE の潜在的な弱点の分野であることを識別し、「提供された証拠内のすべてのインタフェース仕様が潜在的な脆弱性を仮定するために探索される」という探索に対して手法を特定し、続けてこの仮定で使用された方法を説明することができる。

1633 また、評価アクティビティの実施中に、証拠の検査中に評価者が識別した関心の分野。関心の分野は、このコンポーネントに関連付けられたその他のワークユニット(特に AVA_VAN.4-7、AVA_VAN.4-5、及び AVA_VAN.4-6 といった、侵入テストの開発及び実施によって、調査対象となる関心の分野、または潜在的な脆弱性がさらに識別されるようなもの) の実施中に、識別される可能性もある。

1634 ただし、開発及びガイダンス証拠のサブセットまたはそれらの内容のサブセットのみの検査は、この厳密さのレベルでは許可されない。手法の記述は、提供物件を探索するために使用される手法がそれらの提供物件が提供するすべての情報を考慮しているという確信を提供することで、使用される系統的手法が完全であるということの実証を提供するべきである。

1635 潜在的な脆弱性の識別に対するこの手法は、順序付けられ計画された手法をとること、つまり、検査に対して体系的な方法を適用することである。評価者は、証拠がどのように考慮されるか、つまり、この情報が考慮される方法、及び立てられる仮定の観点から、使用される方法を記述する。この手法は評価監督機関によって同意されるべきであり、評価監督機関は、評価者が脆弱性分析に対して使用するべきである追加手法の詳細を提供し、評価者によって考慮されるべきである追加情報を識別することができる。

1636 潜在的な脆弱性を識別する体系的な方法は事前に定義されるが、識別プロセスは繰返して行われる可能性があり、その場合、1 つの潜在的な脆弱性の識別によって、それ以上の調査が必要な別の関心の分野の識別が導かれることがある。

1637 運用環境で TOE が満たす SFR に従って、評価者の独立脆弱性分析は、次の各見出しの一般的な潜在的脆弱性を考慮するべきである:

a) 評価監督機関から提供されることもある、評価されている TOE の種別に関する一般的な潜在的脆弱性;

b) バイパス;

c) 改ざん;

d) 直接攻撃;

e) 監視;

f) 誤使用。

1638 項目 b)から f)については、附属書 B でさらに詳しく説明する。

1639 セキュリティアーキテクチャ記述は、上記の一般的な各潜在的脆弱性を踏まえて考慮されるべきである。TSF の保護を破り、TSF を侵害する手段を探索するために、各潜在的脆弱性が考慮されるべきである。

AVA_VAN.4-5 評価者は、ETR 内で、テストの候補となり、運用環境の TOE に適用できる識別された潜在的な脆弱性を***記録しなければならない。***

1640 例えば、評価者が IT または非 IT の運用環境の手段によってその運用環境では潜在的な脆弱性の悪用が防止されることを識別する場合、潜在的な脆弱性についてそれ以上の考慮は不要であることが識別される可能性がある。例えば、TOE への物理的アクセスを許可利用者だけに制限することにより、効果的に潜在的な脆弱性が改ざんに悪用されないようにすることができる。

1641 評価者が運用環境で潜在的な脆弱性が該当しないことを決定する場合、評価者は、それ以上の考慮から潜在的な脆弱性を除外する理由を記録する。それ以外の場合は、評価者は、さらに考慮する対象となる潜在的な脆弱性を記録する。

1642 運用環境の TOE に適用できる潜在的な脆弱性のリストは、侵入テストアクティビティに対する入力として使用でき、評価者が ETR で報告しなければならない。

16.2.4.7 アクション AVA_VAN.4.4E

AVA_VAN.4-6 評価者は、潜在的な脆弱性に対する独立探索に基づいて、侵入テストを***考え出さなければならない。***

1643 評価者は、必要に応じて、公開の場で利用できる情報源の探索及び TOE ガイダンスと設計証拠の分析の間に識別される潜在的な脆弱性が、運用環境における TOE にどの程度あてはまるかを決定するために、侵入テストを準備する。評価者は、既知の潜在的脆弱性に関して、第三者(例えば、評価監督機関)によって評価者に与えられるどんな現在の情報も、他の評価アクティビティがもたらすどんな遭遇する潜在的な脆弱性とあわせ、考慮する。

1644 評価者は、脆弱性の探索におけるセキュリティアーキテクチャ記述の考慮(AVA_VAN.4-3 で詳述)に関連して、アーキテクチャの特性を確認するためにテストを実行するべきであることに留意する。ATE_DPTからの要件が SAR に含まれている場合、開発者テスト証拠には、セキュリティアーキテクチャ記述で詳述されている特定のメカニズムの正しい実装を確認するために実行されたテストが組み込まれる。ただし、開発者テストには TSF を保護するアーキテクチャ特性のすべての側面のテストが必ずしも含まれない。これは、このテストの大部分が、本質的に特性の反証を試みる否定テストであるためである。侵入テストの方策を開発する際に、評価者は、セキュリティアーキテクチャ記述のすべての側面が、機能テスト(15 で考慮)または評価者侵入テストでテストされることを保証する。

1645 評価者は恐らく、各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することを、実用的だと感じるだろう。

1646 評価者は、中程度の攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が中程度の攻撃能力を超える悪用可能な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

1647 潜在的な脆弱性を悪用するために必要な攻撃能力の決定に関するガイダンスは、附属書 B.4 に記載されている。

1648 中程度（もしくはそれ以下）の攻撃能力を持つ攻撃者によって悪用される可能性があると仮定され、セキュリティ対策方針の違反となる潜在的な脆弱性は、TOE に対する侵入テストを指示するために使用されるリストを構成する優先順位の最も高い潜在的な脆弱性とするべきである。

AVA_VAN.4-7 評価者は、潜在的な脆弱性のリストに基づき、テストを再現可能にするために十分に詳細に侵入テスト証拠資料を***作成しなければならない。***テスト証拠資料には、次のものを含めなければならない:

a) TOE はどの潜在的な脆弱性の調査のためにテストされるか、その脆弱性の識別;

b) 侵入テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示;

c) すべての侵入テスト前提初期条件を確立するための指示;

d) TSF を刺激するための指示;

e) TSF のふるまいを観察するための指示;

f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述;

g) TOE のテストを終了し、終了後の必要な状態を確立するための指示。

1649 評価者は、公知になっているものの探索及び評価証拠の分析の間に識別された潜在的な脆弱性のリストに基づいて、侵入テストを準備する。

1650 評価者は、攻撃が功を奏するために中程度の攻撃能力を必要とする脆弱性を超える潜在的な脆弱性の悪用される可能性を決定することを期待されない。ただし、評価の専門知識の結果として、評価者は、中程度の攻撃能力を超える攻撃能力を持つ攻撃者のみが悪用できる潜在的な脆弱性を発見することがある。そのような脆弱性は、残存脆弱性として ETR に報告される。

1651 潜在的な脆弱性を理解し、評価者は、TOE にどの程度あてはまるかをテストするための最も適切な方法を決定する。特に、評価者は、次のことを考慮する:

a) TSF を刺激し、反応を観察するために使用される TSFI またはその他の TOE インタフェース(評価者は、(ADV_ARCによる要求に従い)セキュリティアーキテクチャの記述で記述されているものなど、TSF の特性を実証するために、TSFI 以外の TOE へのインタフェースを使用する必要がある可能性がある。これらの TOE インタフェースは TSF の特性をテストする手段を提供するが、これらはテストの対象ではないことに注意するべきである);

b) テストに存在する必要がある初期条件(つまり、存在する必要がある特定のオブジェクトまたはサブジェクト及びそれらが持つ必要があるセキュリティ属性);

c) TSFI を刺激するため、または TSFI を観察するために必要となる特別なテスト装置;

d) 物理的なテストを論理的分析に置き換えるべきであるかどうか。初期テストの結果から、繰返し試みられた攻撃が、指定した試行回数の後に成功する可能性が高いことが実証されると推定できる場合は、特に関連する。

1652 評価者は恐らく、各テストが特定の潜在的な脆弱性をテストする、一連のテストケースを用いて侵入テストを実行することを、実用的だと感じるだろう。

1653 テスト証拠資料にこのレベルの詳細を特定する意図は、他の評価者がテストを再現し、同等の結果を得ることができるようにすることである。

AVA_VAN.4-8 評価者は、侵入テストを***実施しなければならない。***

1654 評価者は、TOE の侵入テストの実行のための基礎として、ワークユニット AVA_VAN.4-6 の結果の侵入テスト証拠資料を使用するが、これは、評価者がその場で追加の侵入テストを実行することを排除しない。必要に応じて、評価者は、侵入テスト中に得られた情報の結果としてその場でテストを考え出すことができ、評価者により行われたならば、そのテストは侵入テスト証拠資料に記録される。そのようなテストは、期待されない結果または観察を追求するか、または事前に計画されたテスト中に評価者に示された潜在的な脆弱性を調査するために必要となる可能性がある。

1655 侵入テストが仮定される潜在的な脆弱性が存在することを示さない場合には、評価者は、評価者自身の分析が正しくないかどうか、または評価用提供物件が正しくないか不完全であるかどうかを決定するべきである。

1656 評価者は、中程度の攻撃能力を必要とした脆弱性を超える潜在的な脆弱性(公知になっている潜在的な脆弱性を含む)をテストすることは期待されない。ただし、場合によっては、悪用される可能性を決定する前に、テストを行う必要がある。評価の専門知識の結果として、評価者が中程度の攻撃能力を超える悪用可能な脆弱性を発見したとき、これは、残存脆弱性として ETR に報告される。

AVA_VAN.4-9 評価者は、侵入テストの実際の結果を***記録しなければならない。***

1657 実際のテスト結果の特定の詳細のいくつか(例えば、監査レコードの時刻と日付フィールド)が期待されたものと異なるかもしれないが、全体的な結果は、同一であるべきである。期待されないテスト結果は、調査するべきである。評価への影響は、述べられ、正当化されるべきである。

AVA_VAN.4-10 評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者の侵入テストの成果を***報告しなければならない。***

1658 ETR に報告される侵入テスト情報によって、評価者は全体的な侵入テスト手法及びこのサブアクティビティで費やした成果を伝えることができる。この情報を提供する意図は、評価者の侵入テスト成果の意味ある概要を示すことである。ETR の侵入テストに関する情報が、特定のテストステップの正確な再現であることまたは個々の侵入テストの結果であることを意図しない。意図するのは、十分詳細な情報を提供し、他の評価者と評価監督機関が選択された侵入テスト手法、実行された侵入テストの量、TOE テスト構成、侵入テストアクティビティの全体的な結果を洞察できるようにすることである。

1659 評価者の侵入テスト成果に関する ETR セクションに通常示される情報は、次のとおりである:

a) TOE テスト構成。侵入テストが行われた TOE の特定の構成;

b) 侵入テストされた TSFI。侵入テストの焦点となった TSFI 及びその他の TOE インタフェースの簡単なリスト;

c) サブアクティビティの判定。侵入テスト結果の総合判断。

1660 このリストは、必ずしも徹底したものではなく、評価中に評価者が行った侵入テストに関する、ETR に示すべき情報の種別を提供することだけを意図している。

AVA_VAN.4-11 評価者は、TOE が、運用環境において、中程度の攻撃能力を持つ攻撃者に耐えられることを決定するために、すべての侵入テストの結果を***検査しなければならない。***

1661 TOE が、運用環境において、高い攻撃能力に欠ける攻撃能力を持つ攻撃者によって悪用可能な脆弱性を持っていることを結果が示す場合、この評価者のアクションは不合格となる。

1662 特定の脆弱性を悪用するために必要な攻撃能力、及び意図された環境でその悪用が可能かどうかを決定するために、附属書 B.4 のガイダンスを使用するべきである。攻撃能力の計算は必ずしもすべての場合に必要となるわけではなく、高い攻撃能力に欠ける攻撃者によって脆弱性が悪用可能かどうかについて疑問がある場合に限られる。

AVA_VAN.4-12 評価者は、ETR に、すべての悪用され得る脆弱性と残存脆弱性を、次のそれぞれを詳細に述べて***報告しなければならない：***

a) 出所(例えば、脆弱性が予想されたとき実行していた CEM アクティビティ、評価者に既知である、公表されたものを読んで知った、など);

b) 満たされていない SFR(1 つまたは複数);

c) 記述;

d) 運用環境で悪用されるか否か(つまり、悪用される可能性があるか残存か)。

e) 識別された脆弱性を実行するために必要な時間量、専門知識のレベル、TOE に関する知識のレベル、機会のレベル、及び装置。及び附属書 B.4 の表 3 及び 4 を使用した対応する値。

16.2.5 サブアクティビティの評価(AVA_VAN.5)

1663 一般的なガイダンスはない。このサブアクティビティのガイダンスについては制度を調べるべきである。

17 ACO クラス: 統合

17.1 序説

1664 このアクティビティの目的は、統合 TOE に対する ST での定義に従ってコンポーネントをセキュアに統合できるかどうかを決定することである。これは、コンポーネントの設計の検査及び脆弱性分析の実施によってサポートされている、コンポーネント間のインタフェースの検査及びテストによって達成される。

17.2 適用上の注釈

1665 依存コンポーネントの依存(ACO_REL)ファミリは、依存コンポーネントが自身のセキュリティサービスを提供するためにその運用環境における IT に依存している(統合 TOE 評価における基本コンポーネントによって満たされた)部分を識別する。この依存は、依存コンポーネントにより基本コンポーネントによって提供されると期待されるインタフェースの観点から識別される。その後、開発証拠(ACO_DEV)は、基本コンポーネントのコンポーネント評価中に基本コンポーネントのどのインタフェースが(TSFI として)考慮されたかを決定する。

1666 依存コンポーネントの依存(ACO_REL)では、コンポーネントの統合に関する技術的な統合の問題(例えば、オペレーティングシステムの非 TSF インタフェースの記述、統合の規則など)に対処するために必要となる可能性がある他の証拠が扱われないことに注意するべきである。これは、統合のセキュリティ評定の範囲外であり、機能の統合の問題である。

1667 統合 TOE のテスト(ACO_CTT)の一部として、評価者は、特定されたとおりに機能することを確認するために、統合 TOE インタフェースでの統合 TOE SFR のテスト、及び依存コンポーネントが依存する基本コンポーネントのインタフェースのテストを実行する。選択されたサブセットでは、統合 TOE で使用される基本コンポーネントの構成/使用に対して行われた変更の考えられる影響が考慮される。これらの変更は、基本コンポーネントの評価中に決定された基本コンポーネントの構成から識別される。開発者は、基本コンポーネントの各インタフェースに対してテスト証拠を提供する(カバレージに対する要件は基本コンポーネントの評価に適用される要件と一貫している)。

1668 統合の根拠(ACO_COR)では、評価者は、適切な保証手段が基本コンポーネントに適用されているかどうか、及び評価構成で基本コンポーネントが使用されているかどうかを決定する必要がある。これには、依存コンポーネントが必要とするすべてのセキュリティ機能性が基本コンポーネントの TSF 内にあったかどうかについての決定が含まれる。統合の根拠(ACO_COR)の要件は、それぞれが充足されることが実証されていることの証拠を作成することによって満たすことができる。この証拠は、セキュリティターゲット及びコンポーネント評価の公開報告書(例えば、認証報告書)の形にすることができる。

1669 他方、上記のいずれかが充足されていない場合、元の評価中に得られた保証が影響を受けない理由について論証を作成できる可能性がある。これが不可能な場合、扱われていない基本コンポーネントの側面に対する追加評価証拠が提供されなければならない可能性がある。その後、この資料は、開発証拠(ACO_DEV)で評定される。

1670 例えば、エンティティ間の相互作用(CC パート 3 の附属書 B.3「統合 IT エンティティ間の相互作用」を参照のこと)で記述されているように、依存コンポーネントは、基本コンポーネント評価に含まれたものより多くのセキュリティ機能性を統合 TOE で提供することを基本コンポーネントに要求する可能性がある。これは、依存コンポーネントの依存(ACO_REL)及び開発証拠(ACO_DEV)のファミリの適用中に決定される。この場合、統合の根拠(ACO_COR)に対して提供されている統合の根拠の証拠は、基本コンポーネントの評価から得られた保証が影響を受けないことを実証する。これは、次のような手段によって達成することができる:

a) TSF の拡張部分に関連する証拠に焦点を当てた基本コンポーネントの再評価の実行;

b) TSF の拡張部分が TSF の他の部分に影響を与えることができないことの実証、及び TSF の拡張部分が必要なセキュリティ機能性を提供することの証拠の提供。

17.3 統合の根拠(ACO_COR)

17.3.1 サブアクティビティの評価(ACO_COR.1)

17.3.1.1 入力

1671 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 統合 ST;

b) 統合の根拠;

c) 依存情報;

d) 開発情報;

e) 一意の識別情報。

17.3.1.2 アクション ACO_COR.1.1E

ACO_COR.1.1C ***統合の根拠は、基本コンポーネントが、依存コンポーネントの TSF を支援する要求に従い構成された場合、依存コンポーネントのものと少なくとも同じ保証のレベルが、基本コンポーネントの支援機能性に対して得られることを実証しなければならない。***

ACO_COR.1-1 評価者は、開発情報で詳述されていない依存コンポーネントが依存しているインタフェースを識別するために、開発情報と依存情報による対応分析を***検査しなければならない。***

1672 このワークユニットにおける評価者の目標は次の 2 つに分かれる:

a) 依存コンポーネントが依存しているインタフェースのうちどれに適切な保証手段が適用されているかを決定すること。

b) 基本コンポーネントの評価中に基本コンポーネントに適用された保証パッケージに、依存コンポーネントの評価中に依存コンポーネントに適用されたパッケージと同じ保証要件またはより高い階層の保証要件が含まれていることを決定すること。

1673 評価者は、開発情報で考慮されていない依存情報で識別されているインタフェースの識別を助けるために、開発証拠(ACO_DEV)アクティビティ(例えば、ACO_DEV.1-2、ACO_DEV.2-4、ACO_DEV.3-6)の間に作成される開発情報において対応の追跡を使用することができる。

1674 評価者は、開発情報に含まれていない依存情報において記述されている SFR 実施インタフェースを記録する。これらは、ACO_COR.1-3 ワークユニットに入力を提供し、さらに保証が要求される基本コンポーネントの部分の識別を助ける。

1675 基本コンポーネントと依存コンポーネントの両方が同じ保証パッケージに対して評価されていれば、基本コンポーネント評価の部分的な保証のレベルが少なくとも依存コンポーネントの保証のレベルと同じであるかどうかを決定するのは簡単である。一方、コンポーネントの評価中にコンポーネントに適用された保証パッケージが異なる場合、評価者は、基本コンポーネントに適用された保証要件が、いずれも依存コンポーネントに適用された保証要件よりも高い階層にあることを決定する必要がある。

ACO_COR.1-2 評価者は、依存 TSF によって依存されており、含まれている基本コンポーネントインタフェースについて、基本コンポーネントの評価中にインタフェースが考慮されたかどうかを決定するために、統合の根拠を***検査しなければならない。***

1676 ST、コンポーネント公開評価報告書(認証報告書など)、及び基本コンポーネントのガイダンス文書はいずれも、基本コンポーネントの範囲と境界についての情報を提供する。ST は、統合 TOE の論理的範囲及び境界の詳細を提供して、評価の範囲内に存在した製品の一部にインタフェースが関連するかどうかを評価者が決定できるようにする。ガイダンス証拠資料は、統合TOEに対するすべてのインタフェースの使用についての詳細を提供する。ガイダンス証拠資料には評価の範囲に含まれない製品のインタフェースの詳細を含めることができるが、ST における範囲を決定する情報から、または評価構成を扱うガイダンスの一部を通して、このようなインタフェースは識別可能であるべきである。公開評価報告書は、統合 TOE の使用に対する必要な追加制約を提供してもよい。

1677 このため、これらの入力の組み合わせによって、統合の根拠で記述されているインタフェースに必要な保証が関連付けられているかどうか、またはさらなる保証が必要かどうかを評価者は決定できる。評価者は、ACO_COR.1-3 の間に考慮される、追加保証が要求される基本コンポーネントのインタフェースを記録する。

ACO_COR.1-3 評価者は、必要な保証手段が基本コンポーネントに対して適用されていることを決定するために、統合の根拠を***検査しなければならない。***

1678 統合 TOE で基本コンポーネントの同じ部分が使用され、それらが一貫した方法で使用される場合は、基本コンポーネントに対する評価判定、及び結果として生じる保証を再使用できる。

1679 必要な保証手段がすでにコンポーネントに適用されているかどうか、及び保証手段を適用する必要がまだあるコンポーネントの部分を決定するために、評価者は ACO_DEV.*.2E アクションの出力及びワークユニット ACO_COR.1-1 及び ACO_COR.1-2 を使用するべきである:

a) 依存情報(依存コンポーネントの依存(ACO_REL))で識別されているが、開発情報(開発証拠(ACO_DEV))では説明されていないインタフェースについては、追加情報が必要である(ACO_COR.1-1 で識別される)。

b) 基本コンポーネントから統合 TOE で一貫しない状態で使用されているインタフェース(開発証拠(ACO_DEV)及び依存コンポーネントの依存(ACO_REL)で提供される情報に相違がある)の場合、使用中の相違の影響を考慮する必要がある(ACO_DEV.*.2E で識別される)。

c) 保証が事前に得られていない統合の根拠で識別されているインタフェースには、追加情報が必要である(ACO_COR.1-2 で識別される)。

d) 依存情報、統合の根拠、及び開発情報で一貫して記述されているインタフェースについては、基本コンポーネント評価の結果を再利用できるため、追加アクションは必要とされない。

1680 依存情報によって要求されると報告されているが、開発情報に含まれていない基本コンポーネントのインタフェースは、さらに保証が要求される基本コンポーネントの部分を示す。このインタフェースは、基本コンポーネントへの入口点を識別する。

1681 開発情報及び依存情報の両方に含まれているインタフェースについては、統合 TOE において、基本コンポーネント評価と一貫した方法でインタフェースが使用されているかどうかを評価者は決定する必要がある。インタフェースの使用方法は、基本コンポーネントと統合 TOE の両方においてインタフェースの使用が一貫していることを決定するために、開発証拠(ACO_DEV)アクティビティ中に考慮される。考慮対象として残っているのは、基本コンポーネント及び統合 TOE の構成が一貫しているかどうかの決定である。これを決定するには、構成が一貫していることを保証するために、評価者が各々のガイダンス証拠資料を考慮する(一貫したガイダンス証拠資料に関しては、以下のさらに詳しいガイダンスを参照のこと)。証拠資料からの逸脱は、考えられる影響を決定するために評価によってさらに詳しく分析される。

1682 依存情報及び開発情報で一貫して記述されており、ガイダンスが基本コンポーネント及び統合 TOE に対して一貫しているインタフェースについては、要求される保証のレベルが提供されている。

1683 以下に、基本コンポーネントで得られる保証、統合 TOE に対して提供される証拠、及び矛盾が識別されている場合に評価者によって実行される分析の間の一貫性を決定する方法についてのガイダンスを示す。

17.3.1.2.1 開発

1684 依存情報は、基本コンポーネントと対応することになる依存コンポーネント内のインタフェースを識別する。依存情報で識別されているインタフェースが開発情報で識別されていない場合は、基本コンポーネントがどのように要求されたインタフェースを提供するかの正当な理由が統合の根拠によって提供される。

1685 依存情報において識別されているインタフェースが開発情報で識別されているが、記述間で矛盾がある場合、さらに分析が必要になる。評価者は、基本コンポーネントの評価及び統合 TOE の評価で考慮されている基本コンポーネントの使用の相違を識別する。評価者は、インタフェースをテストするために、(統合 TOE のテスト(ACO_CTT)の実施中に)実行されるテストを考え出す。

1686 統合 TOE で使用されるときの基本コンポーネント及び依存コンポーネントのパッチステータスを、コンポーネント評価中のコンポーネントのパッチステータスと比較するべきである。コンポーネントにパッチが適用されている場合は、評価されたコンポーネントの SFR に対する潜在的な影響を含めたパッチの詳細が統合の根拠に含められる。評価者は、提供された変更の詳細を考慮し、コンポーネント SFR に対する変更の潜在的な影響の正確さを検証するべきである。その上で評価者は、パッチによって行われる変更をテストによって検証するべきかどうかを考慮するべきであり、必要なテスト手法を識別する。テストは、コンポーネントのコンポーネント評価のために実行された適切な評価者/開発者テストを繰返す形をとることができる。あるいは、改変されたコンポーネントを確認するための新しいテストを評価者が考え出すことが必要になる場合がある。

1687 個々のコンポーネントのいずれかがコンポーネント評価完了後に保証継続性アクティビティの対象であった場合、評価者は、統合 TOE に対する独立脆弱性分析アクティビティ(統合の脆弱性分析(ACO_VUL))の間に保証継続アクティビティで評定された変更を考慮する。

17.3.1.2.2 ガイダンス

1688 統合 TOE に対するガイダンスは、個別のコンポーネントに対するガイダンスを多く参照する可能性がある。必要になると予測されている最小のガイダンスは、特に統合 TOE の準備(設置)中における、依存コンポーネント及び基本コンポーネントに対するガイダンスの適用における順序依存性の識別である。

1689 準備手続き(AGD_PRE)及び利用者操作ガイダンス(AGD_OPE)ファミリを統合 TOE についてのガイダンスに適用することに加え、逸脱を識別するために、コンポーネントと統合 TOE に対するガイダンス間の一貫性を分析する必要がある。

1690 統合 TOE ガイダンスが基本コンポーネント及び依存コンポーネントのガイダンスを参照する場合、一貫性についての考慮は各コンポーネントに対して提供されているガイダンス証拠資料間の一貫性(つまり、基本コンポーネントガイダンスと依存コンポーネントガイダンスの間の一貫性)に制限される。ただし、統合 TOE に対して追加ガイダンスが提供される場合、コンポーネントに対して提供されるガイダンスについては、コンポーネントに対するガイダンス証拠資料と統合 TOE に対するガイダンス証拠資料の間の一貫性も要求されるため、さらに多くの分析が要求される。

1691 この場合の *一貫した状態*とは、*ガイダンス*が同じである、または組み合わされた場合に個別のコンポーネントの運用についての追加制約が、機能/保証コンポーネントの *詳細化*と同じ方法で課せられる、という意味であると理解される。

1692 (開発証拠(ACO_DEV)に対する入力として使用した、または上記で説明されている開発の側面など)利用可能な情報を使用して、評価者は、コンポーネント評価で特定された基本コンポーネントの構成からの逸脱の考えられる影響をすべて決定できる可能性がある。ただし、(基本コンポーネント評価が TOE 設計(ADV_TDS)の要件を含んでいた場合の)上位の EAL については、基本コンポーネントに対する詳細な設計抽象が統合 TOE に対する開発情報の一部として配付される場合を除き、ガイダンスに対する改変の考えられる影響は、内部構造が不明であるため、完全には決定できない可能性がある。この場合、評価者は分析の残存リスクを報告する。

1693 これらの残存リスクは、統合 TOE に対する公開評価報告書に含まれる。

1694 評価者は、ガイダンスにおけるこれらの相違は評価者の独立テストアクティビティ(統合 TOE のテスト(ACO_CTT))への入力になる点に注意する。

1695 統合 TOE に対するガイダンスは、特に設置、及び依存コンポーネントの設置手順に関連した基本コンポーネントの設置手順の順序の観点から、コンポーネントに対するガイダンスに追加することができる。個別のコンポーネントの設置の手順の順序付けは変更するべきではないが、交互に行う必要である場合がある。評価者は、コンポーネントの評価中に行なわれるAGD_PREアクティビティの要件をガイダンスがまだ満たすことを保証するために、このガイダンスを検査する。

1696 基本コンポーネントのインタフェースが、基本コンポーネントの TSFI として識別されているものに加えて、依存コンポーネントによって依存されていることが依存情報で識別される可能性がある。基本コンポーネントにおけるこのような追加インタフェースの使用に対するガイダンスの提供が必要になる可能性がある。統合 TOE の消費者が基本コンポーネントに対するガイダンス証拠資料を受け取る場合、基本コンポーネントに対するAGD_PRE及びAGD_OPEの判定の結果は、基本コンポーネントの評価で考慮されるインタフェースに対して再利用できる。ただし、依存コンポーネントが依存する追加インタフェースについては、基本コンポーネントに対するガイダンス証拠資料が、基本コンポーネント評価における適用に従って、AGD_PRE及びAGD_OPEの要件を満たすことを評価者が決定する必要がある。

1697 基本コンポーネントの評価中に考慮されており、そのため、保証がすでに得られているインタフェースについては、統合 TOE に対する各インタフェースの利用についてのガイダンスが基本コンポーネントに対して提供されているものと一貫していることを、評価者は保証する。統合 TOE に対するガイダンスが基本コンポーネントに対するガイダンスと一貫していることを決定するために、評価者は、統合 TOE 及び基本コンポーネントの両方に対して提供されているガイダンスへの各インタフェースのマッピングを実行するべきである。その後、評価者はガイダンスを比較して、一貫性を決定する。

1698 コンポーネントのガイダンスと一貫しているものとみなされる統合 TOE ガイダンスで提供される追加制約の例は、次のとおりである(コンポーネントについてのガイダンスが示され、その後に、追加制約を提供するものとみなされる統合 TOE に対するガイダンスの例が続く):

- コンポーネント:パスワードの長さは、英数字を含めて、最短でも 8 文字に設定する必要がある。
- 統合 TOE:パスワードの長さは、英数字及び*次の特殊文字のうち少なくとも 1 文字*を含めて、最短でも 10 文字に設定する必要がある:*( ) { } ^ < > - _*
- 注:(パスワードが推測される可能性を考慮して)強さのレート付けに同等またはより高い数値尺度が達成された場合にのみ、統合 TOE に英字と数字の両方を含めるという指定を削除するとともに、パスワードの長さを[*整数>8*]文字に増やすことが容認される。
- コンポーネント:WWW Publishing Service 及び ICDBReporter サービスは、レジストリの設定において無効にされる。
- 統合 TOE:*Publishing Service*、*ICDBReporter サービス*、*リモートプロシージャコール(RPC)ロケータ及びリモートプロシージャコール(RPC)サービス*は、レジストリの設定において無効にされる。
- コンポーネント:アカウントログファイルに含まれる属性として、日付、時刻、事象の種別、サブジェクト識別情報、及び成功/失敗を選択する。
- 統合 TOE:アカウントログファイルに含まれる属性として、日付、時刻、事象の種別、サブジェクト識別情報、成功/失敗、*事象メッセージ*、*及びプロセススレッド*を選択する。

1699 統合 TOE に対するガイダンスが基本コンポーネントに対して提供されるガイダンスから逸脱する(詳細化ではない)場合、評価者は、ガイダンスに対する改変の潜在的なリスクを評定する。評価者は、(公知として提供されている情報、公開評価報告書(例えば、認証報告書)における基本コンポーネントのアーキテクチャの記述、ガイダンス証拠資料の残りの部分からのガイダンスの文脈を含めた)利用可能な情報を使用して、統合 TOE の SFR に対するガイダンスへの改変の影響の可能性を識別する。

1700 依存コンポーネント評価中に、設置の試行が基本コンポーネントを使用して依存コンポーネントの環境要件を満たした場合、統合 TOE に対するこのワークユニットは満たされているものとみなされる。依存コンポーネントの評価中に、ワークユニット AGD_PRE.1-3 を満たすように基本コンポーネントが使用されなかった場合、評価者は、AGD_PRE.1-3 で特定されたガイダンスに従って、統合 TOE を準備するために、統合 TOE に対して提供される利用者手続きを適用する。これによって、評価者は、統合 TOE に対して提供される準備ガイダンスが、統合 TOE とその運用環境をセキュアに準備するために十分であることを決定できるようになる。

17.3.1.2.3 ライフサイクル

配付

1701 統合 TOE の配付に対して使用される異なる配付メカニズムが存在する(つまり、コンポーネントの評価中に定義され、評定されるセキュアな配付手続きに従ってコンポーネントが消費者に配付されない)場合、統合 TOE に対する配付手続きには、コンポーネントの評価中に適用される配付(ALC_DEL)の要件に対する評価が必要になる。

1702 統合 TOE は、統合された製品として配付されたり、コンポーネントを個別に配付することを必要としたりする可能性がある。

1703 コンポーネントが個別に配付される場合、基本コンポーネント及び依存コンポーネントの配付の結果は再利用される。基本コンポーネントに対するガイダンス証拠資料での記述に従って、特定されたガイダンスを使用し、利用者の責任である配付の側面をチェックすることによって、評価者による依存コンポーネントの試行設置中に、基本コンポーネントの配付がチェックされる。

1704 統合 TOE が新しいエンティティとして配付される場合、そのエンティティの配付の方法は、統合 TOE 評価アクティビティで考慮する必要がある。

1705 統合 TOE 要素に対する配付手続きの評定は、任意の追加要素(例えば、統合 TOE に対する追加ガイダンス文書)が配付手続きで考慮されることを保証しながら、任意のその他の「コンポーネント」TOE に対してのように、配付(ALC_DEL)についての方法に従って実行される。

CM 能力

1706 統合 TOE の一意の識別はサブアクティビティの評価(ALC_CMC.1)の適用中に考慮され、その統合 TOE を構成する要素はサブアクティビティの評価(ALC_CMS.2)の適用中に考慮される。

1707 統合 TOE に対して追加ガイダンスを作成できるが、(サブアクティビティの評価(ALC_CMC.1)中に統合 TOE の一意の識別の一部として考慮されている)このガイダンスの一意の識別は、ガイダンスの十分な制御とみなされる。

1708 残りの(上記で考慮されていない)「ALC クラス: ライフサイクルサポート」のアクティビティの判定は、統合 TOE の統合中にそれ以上の開発が実行されないため、基本コンポーネント評価から再利用できる。

1709 統合は、消費者サイトで、または統合 TOE が統合された製品として配付される場合には依存コンポーネント開発者のサイトで実行されるものと想定されるため、開発セキュリティに対してさらに考慮されることはない。消費者サイトでの制御は、CC の考慮の範囲外である。統合が依存コンポーネントのサイトと同じサイトである場合、すべてのコンポーネントは、統合 TOE に対する構成要素とみなされ、そのため、どのような場合でも依存コンポーネント開発者のセキュリティ手続きの下で考慮されるべきであるため、追加要件またはガイダンスは不要である。

1710 統合中に採用されるツールと技法は、依存コンポーネント開発者によって提供される証拠において考慮される。基本コンポーネントに関連する任意のツール/技法は、基本コンポーネントの評価中に考慮されている。例えば、基本コンポーネントがソースコードとして配付され、消費者(例えば、統合を実行している依存コンポーネント開発者)によるコンパイルが必要な場合、基本コンポーネントの評価中に、コンパイラは適切な引数とともに特定及び評定されている。

1711 さらに詳細な要素の開発は行われないため、統合 TOE に対して適用可能なライフサイクル定義は存在しない。

1712 コンポーネントに対する欠陥修正の結果は、統合 TOE には適用可能ではない。統合 TOE に対する保証パッケージに欠陥修正が含まれている場合、欠陥修正(ALC_FLR)の要件は、(任意の要件追加に対してのように)統合 TOE 評価中に適用される。

17.3.1.2.4 テスト

1713 依存コンポーネントのテストに対して使用される構成には、運用環境における IT に対する要件を満たすために基本コンポーネントが含まれているべきであるため、統合 TOE は、依存コンポーネントの評価の「ATE クラス: テスト」アクティビティの実施中にテストされている。依存コンポーネント評価のための依存コンポーネントのテストで基本コンポーネントが使用されなかった場合、またはいずれかのコンポーネントの構成がその評価構成から変化した場合、「ATE クラス: テスト」の要件を満たすために依存コンポーネント評価で実行される開発者テストは、統合 TOE において繰返される。

17.4 開発証拠(ACO_DEV)

17.4.1 サブアクティビティの評価(ACO_DEV.1)

17.4.1.1 目的

1714 このサブアクティビティの目的は、依存コンポーネントをサポートするために基本コンポーネントによって適切なセキュリティ機能性が提供されることを決定することである。これは、基本コンポーネントのインタフェースが、依存コンポーネントによって要求される、依存情報で特定されているインタフェースと一貫していることを決定するための、基本コンポーネントのインタフェースの検査によって達成される。

1715 インタフェースがいったん識別され、目的が記述されると、インタフェース仕様の残りの詳細は基本コンポーネントの評価から再利用できるため、サブアクティビティの評価(ADV_FSP.2)を満たすために必要なすべての側面がサブアクティビティの評価(ACO_DEV.1)に要求されるわけではないが、基本コンポーネントのインタフェースの記述は、サブアクティビティの評価(ADV_FSP.2)と一貫した詳細のレベルで提供される。

17.4.1.2 入力

1716 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 統合 ST;

b) 開発情報;

c) 依存情報。

17.4.1.3 アクション ACO_DEV.1.1E

ACO_DEV.1.1C ***開発情報は、統合 TOE で使用される基本コンポーネントの各インタフェースの目的を記述しなければならない。***

ACO_DEV.1-1 評価者は、開発情報が各インタフェースの目的を記述していることを決定するために、その開発情報を***検査しなければならない。***

1717 基本コンポーネントは、依存 TSF を提供する際に、依存コンポーネントとの相互作用をサポートするインタフェースを提供する。各インタフェースの目的は、TOE 設計(サブアクティビティの評価(ADV_TDS.1))のサブシステム間で提供される、依存コンポーネント TSF 機能性に対するインタフェースの記述と同じレベルで記述される。この記述は、依存コンポーネント TSF が要求するサービスを基本コンポーネントがどのように提供するかについての知識を読者に提供する。

1718 このワークユニットは、基本コンポーネントの TSFI であるインタフェースに対する基本コンポーネントの機能仕様の提供によって満たすことができる。

ACO_DEV.1.2C ***開発情報は、依存コンポーネントの TSF を支援するために、基本コンポーネントと依存コンポーネントの、統合 TOE で使用されるインタフェース間の対応を示さなければならない。***

ACO_DEV.1-2 評価者は、基本コンポーネントのインタフェースと依存コンポーネントが依存するインタフェースの間の対応が正しいことを決定するために、開発情報を***検査しなければならない。***

1719 基本コンポーネントのインタフェースと依存コンポーネントが依存するインタフェースとの間の対応は、マトリックスまたは表の形を取ることができる。依存コンポーネントが依存するインタフェースは、(依存コンポーネントの依存(ACO_REL)アクティビティの間の検査に従って)依存情報で識別される。

1720 このアクティビティの間には、対応が正しく、基本コンポーネントのインタフェースが可能な限りどのような場合でも依存コンポーネントによって要求されるインタフェースにマッピングされることを保証していること以外には、依存コンポーネントが依存しているインタフェースのカバレージの完全性を決定するための要件は存在しない。カバレージの完全性は、統合の根拠(ACO_COR)のアクティビティで考慮される。

17.4.1.4 アクション ACO_DEV.1.2E

ACO_DEV.1-3 評価者は、インタフェースが一貫して記述されていることを決定するために、開発情報及び依存情報を***検査しなければならない。***

1721 評価者のこのワークユニットの目標は、基本コンポーネントに対する開発情報及び依存コンポーネントに対する依存情報に記述されているインタフェースが一貫して表現されていることを決定することである。

17.4.2 サブアクティビティの評価(ACO_DEV.2)

17.4.2.1 目的

1722 このサブアクティビティの目的は、依存コンポーネントをサポートするために基本コンポーネントによって適切なセキュリティ機能性が提供されることを決定することである。これは、基本コンポーネントのインタフェース及び関連するセキュリティのふるまいが、依存コンポーネントによって要求される、依存情報で特定されているインタフェースと一貫していることを決定するための、基本コンポーネントのインタフェースとセキュリティのふるまいの検査によって達成される。

17.4.2.2 入力

1723 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 統合 ST;

b) 開発情報;

c) 依存情報。

17.4.2.3 アクション ACO_DEV.2.1E

ACO_DEV.2.1C ***開発情報は、統合 TOE で使用される基本コンポーネントの各インタフェースの目的及び使用方法を記述しなければならない。***

ACO_DEV.2-1 評価者は、開発情報が各インタフェースの目的を記述していることを決定するために、その開発情報を***検査しなければならない。***

1724 基本コンポーネントは、依存 TSF を提供する際に、依存コンポーネントとの相互作用をサポートするインタフェースを提供する。各インタフェースの目的は、TOE 設計(サブアクティビティの評価(ADV_TDS.1))のサブシステム間で提供される、依存コンポーネント TSF 機能性に対するインタフェースの記述と同じレベルで記述される。この記述は、依存コンポーネント TSF が要求するサービスを基本コンポーネントがどのように提供するかについての知識を読者に提供する。

1725 このワークユニットは、基本コンポーネントの TSFI であるインタフェースに対する基本コンポーネントの機能仕様の提供によって満たすことができる。

ACO_DEV.2-2 評価者は、開発情報が各インタフェースの使用方法を記述していることを決定するために、その開発情報を***検査しなければならない。***

1726 インタフェースの使用方法とは、操作を呼び出してインタフェースに関連する結果を取得するためにインタフェースがどのように操作されるかを要約したものである。評価者は、開発情報におけるこの資料を読むことにより、各インタフェースの使用方法を決定できるべきである。これは必ずしも、インタフェースごとに個別の使用方法が必要ということではない。例えば、API を呼び出す一般的な方法を記述してから、その一般的なスタイルを使用する各インタフェースを識別することも可能である。

1727 このワークユニットは、基本コンポーネントの TSFI であるインタフェースに対する基本コンポーネントの機能仕様の提供によって満たすことができる。

ACO_DEV.2.2C ***開発情報は、依存コンポーネントの SFR の実施を支援する、基本コンポーネントのふるまいの上位レベルの記述を提供しなければならない。***

ACO_DEV.2-3 評価者は、依存コンポーネント SFR の実施をサポートする基本コンポーネントのふるまいを開発情報が記述していることを決定するために、その開発情報を***検査しなければならない。***

1728 依存コンポーネントは、基本コンポーネントによるサービスの提供を受けるために基本コンポーネントのインタフェースを呼び出す。呼び出される基本コンポーネントのインタフェースについて、開発情報は、基本コンポーネントの関連するセキュリティのふるまいの上位レベルの記述を提供しなければならない。基本コンポーネントのセキュリティのふるまいの記述は、インタフェースが呼び出されたときに基本コンポーネントが必要なサービスをどのように提供するかを概説する。この記述は、ADV_TDS.1.4Cで提供される記述と同様のレベルで行われる。このため、依存コンポーネントによって呼び出されるインタフェースが基本コンポーネントの TSFI である場合は、基本コンポーネント評価からの TOE 設計証拠の提供によってこのワークユニットが満たされる。依存コンポーネントによって呼び出されるインタフェースが基本コンポーネントの TSFI でない場合、関連するセキュリティのふるまいは、基本コンポーネントの TOE 設計証拠で必ずしも記述されない。

ACO_DEV.2.3C ***開発情報は、依存コンポーネントの TSF を支援するために、基本コンポーネントと依存コンポーネントの、統合 TOE で使用されるインタフェース間の対応を示さなければならない。***

ACO_DEV.2-4 評価者は、基本コンポーネントのインタフェースと依存コンポーネントが依存するインタフェースの間の対応が正しいことを決定するために、開発情報を***検査しなければならない。***

1729 基本コンポーネントのインタフェースと依存コンポーネントが依存するインタフェースとの間の対応は、マトリックスまたは表の形を取ることができる。依存コンポーネントが依存するインタフェースは、(依存コンポーネントの依存(ACO_REL)の間の検査に従って)依存情報で識別される。

1730 このアクティビティの間には、対応が正しく、基本コンポーネントのインタフェースが可能な限りどのような場合でも依存コンポーネントによって要求されるインタフェースにマッピングされることを保証していること以外には、依存コンポーネントが依存しているインタフェースのカバレージの完全性を決定するための要件は存在しない。カバレージの完全性は、統合の根拠(ACO_COR)のアクティビティで考慮される。

17.4.2.4 アクション ACO_DEV.2.2E

ACO_DEV.2-5 評価者は、インタフェースが一貫して記述されていることを決定するために、開発情報及び依存情報を***検査しなければならない。***

1731 評価者のこのワークユニットの目標は、基本コンポーネントに対する開発情報及び依存コンポーネントに対する依存情報に記述されているインタフェースが一貫して表現されていることを決定することである。

17.4.3 サブアクティビティの評価(ACO_DEV.3)

17.4.3.1 目的

1732 このサブアクティビティの目的は、依存コンポーネントをサポートするために基本コンポーネントによって適切なセキュリティ機能性が提供されることを決定することである。これは、基本コンポーネントのインタフェース及び関連するセキュリティのふるまいが、依存コンポーネントによって要求される、依存情報で特定されているインタフェースと一貫していることを決定するための、基本コンポーネントのインタフェースとセキュリティのふるまいの検査によって達成される。

1733 インタフェース記述に加え、そのインタフェースが基本コンポーネントの TSF の一部を形成したかどうかを評価者が決定できるようにするために、依存コンポーネントによって要求されるセキュリティ機能性を提供する基本コンポーネントのサブシステムが記述される。

17.4.3.2 入力

1734 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 統合 ST;

b) 開発情報;

c) 依存情報。

17.4.3.3 アクション ACO_DEV.3.1E

ACO_DEV.3.1C ***開発情報は、統合 TOE で使用される基本コンポーネントの各インタフェースの目的及び使用方法を記述しなければならない。***

ACO_DEV.3-1 評価者は、開発情報が各インタフェースの目的を記述していることを決定するために、その開発情報を***検査しなければならない。***

1735 基本コンポーネントは、依存 TSF を提供する際に、依存コンポーネントとの相互作用をサポートするインタフェースを提供する。各インタフェースの目的は、TOE 設計(サブアクティビティの評価(ADV_TDS.1))のサブシステム間で提供される、依存コンポーネント TSF 機能性に対するインタフェースの記述と同じレベルで記述される。この記述は、依存コンポーネント TSF が要求するサービスを基本コンポーネントがどのように提供するかについての知識を読者に提供する。

1736 このワークユニットは、基本コンポーネントの TSFI であるインタフェースに対する基本コンポーネントの機能仕様の提供によって満たすことができる。

ACO_DEV.3-2 評価者は、開発情報が各インタフェースの使用方法を記述していることを決定するために、その開発情報を***検査しなければならない。***

1737 インタフェースの使用方法とは、操作を呼び出してインタフェースに関連する結果を取得するためにインタフェースがどのように操作されるかを要約したものである。評価者は、開発情報におけるこの資料を読むことにより、各インタフェースの使用方法を決定できるべきである。これは必ずしも、インタフェースごとに個別の使用方法が必要ということではない。例えば、API を呼び出す一般的な方法を記述してから、その一般的なスタイルを使用する各インタフェースを識別することも可能である。

1738 このワークユニットは、基本コンポーネントの TSFI であるインタフェースに対する基本コンポーネントの機能仕様の提供によって満たすことができる。

ACO_DEV.3.2C ***開発情報は、統合TOE で使用される基本コンポーネントのインタフェースを提供する基本コンポーネントのサブシステムを識別しなければならない。***

ACO_DEV.3-3 評価者は、依存コンポーネントに対するインタフェースを提供する基本コンポーネントのすべてのサブシステムが識別されていることを決定するために、開発情報を***検査しなければならない。***

1739 基本コンポーネントの TSFI の一部を形成するとみなされているインタフェースについては、そのインタフェースに関連するサブシステムが基本コンポーネント評価中に TOE 設計(ADV_TDS)アクティビティで考慮されるサブシステムとなる。基本コンポーネントの TSFI の一部を形成しなかった依存コンポーネントが依存するインタフェースは、基本コンポーネント TSF の外部のサブシステムにマッピングされる。

ACO_DEV.3.3C ***開発情報は、依存コンポーネントの SFR の実施を支援する、基本コンポーネントのサブシステムのふるまいの上位レベルの記述を提供しなければならない。***

ACO_DEV.3-4 評価者は、依存コンポーネント SFR の実施をサポートする基本コンポーネントサブシステムのふるまいを開発情報が記述していることを決定するために、その開発情報を***検査しなければならない。***

1740 依存コンポーネントは、基本コンポーネントによるサービスの提供を受けるために基本コンポーネントのインタフェースを呼び出す。呼び出される基本コンポーネントのインタフェースについて、開発情報は、基本コンポーネントの関連するセキュリティのふるまいの上位レベルの記述を提供しなければならない。基本コンポーネントのセキュリティのふるまいの記述は、インタフェースが呼び出されたときに基本コンポーネントが必要なサービスをどのように提供するかを概説する。この記述は、ADV_TDS.1.4Cで提供される記述と同様のレベルで行われる。このため、依存コンポーネントによって呼び出されるインタフェースが基本コンポーネントの TSFI である場合は、基本コンポーネント評価からの TOE 設計証拠の提供によってこのワークユニットが満たされる。依存コンポーネントによって呼び出されるインタフェースが基本コンポーネントの TSFI でない場合、関連するセキュリティのふるまいは、基本コンポーネントの TOE 設計証拠で必ずしも記述されない。

ACO_DEV.3.4C ***開発情報は、インタフェースから基本コンポーネントのサブシステムへのマッピングを提供しなければならない。***

ACO_DEV.3-5 評価者は、基本コンポーネントのインタフェースとサブシステムとの間の対応が正しいことを決定するために、開発情報を***検査しなければならない。***

1741 基本コンポーネント評価からの TOE 設計及び機能仕様の証拠を利用できる場合は、この証拠を使用して、統合 TOE で使用されている基本コンポーネントのインタフェースとサブシステムの間の対応の正確さを検証することができる。基本コンポーネント TSFI の一部を形成した基本コンポーネントのインタフェースは、基本コンポーネントの機能仕様で記述され、関連するサブシステムは基本コンポーネントの TOE 設計証拠で記述される。この 2 つの間の追跡は、基本コンポーネントの TOE 設計証拠で提供される。

1742 ただし、基本コンポーネントインタフェースが基本コンポーネントの TSFI の一部を形成しなかった場合は、開発情報で提供されるサブシステムのふるまいの記述を使用して対応の正確さが検証される。

ACO_DEV.3.5C ***開発情報は、依存コンポーネントの TSF を支援するために、基本コンポーネントと依存コンポーネントの、統合 TOE で使用されるインタフェース間の対応を示さなければならない。***

ACO_DEV.3-6 評価者は、基本コンポーネントのインタフェースと依存コンポーネントが依存するインタフェースの間の対応が正しいことを決定するために、開発情報を***検査しなければならない。***

1743 基本コンポーネントのインタフェースと依存コンポーネントが依存するインタフェースとの間の対応は、マトリックスまたは表の形を取ることができる。依存コンポーネントが依存するインタフェースは、(依存コンポーネントの依存(ACO_REL)の間の検査に従って)依存情報で識別される。

1744 このアクティビティの間には、対応が正しく、基本コンポーネントのインタフェースが可能な限りどのような場合でも依存コンポーネントによって要求されるインタフェースにマッピングされることを保証していること以外には、依存コンポーネントが依存しているインタフェースのカバレージの完全性を決定するための要件は存在しない。カバレージの完全性は、統合の根拠(ACO_COR)のアクティビティで考慮される。

17.4.3.4 **アクション** ACO_DEV.3.2E

ACO_DEV.3-7 評価者は、インタフェースが一貫して記述されていることを決定するために、開発情報及び依存情報を***検査しなければならない。***

1745 評価者のこのワークユニットの目標は、基本コンポーネントに対する開発情報及び依存コンポーネントに対する依存情報に記述されているインタフェースが一貫して表現されていることを決定することである。

17.5 依存コンポーネントの依存(ACO_REL)

17.5.1 サブアクティビティの評価(ACO_REL.1)

17.5.1.1 目的

1746 このサブアクティビティの目的は、必要な機能性が基本コンポーネントで使用できること、及びその機能性が呼び出される手段を決定するために十分な情報を開発者の依存証拠が提供しているかどうかを決定することである。これらは、上位レベル記述の観点から提供される。

17.5.1.2 入力

1747 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 統合 ST;

b) 依存コンポーネント機能仕様;

c) 依存コンポーネント設計;

d) 依存コンポーネントアーキテクチャ設計;

e) 依存情報。

17.5.1.3 適用上の注釈

1748 基本コンポーネントと相互に作用する TSF を持つ依存コンポーネントには、その基本コンポーネントによって提供される機能性(例えば、リモート認証、リモート監査データ格納)が必要である。このような場合、エンド利用者のための統合 TOE の構成の担当者に対して、呼び出されたサービスを記述する必要がある。この証拠資料を必要とする根拠は、統合 TOE のインテグレータが、依存コンポーネントに有害な影響を与える可能性があるのは基本コンポーネントにおけるどのようなサービスであるかを決定し、開発証拠(ACO_DEV)ファミリの適用時にコンポーネントの互換性を決定するために照合する情報を提供するのを支援することである。

17.5.1.4 アクション ACO_REL.1.1E

ACO_REL.1.1C ***依存情報は、依存コンポーネントTSF が依存する基本コンポーネントハードウェア、ファームウェア及び/またはソフトウェアの機能性を記述しなければならない。***

ACO_REL.1-1 評価者は、依存コンポーネントTSF が依存する基本依存ハードウェア、ファームウェア、及び/またはソフトウェアの機能性を依存情報が記述していることを決定するために、その依存情報を***チェックしなければならない。***

1749 評価者は、依存コンポーネント TSF が基本コンポーネントのハードウェア、ファームウェア、及びソフトウェアによって提供されることを要求するセキュリティ機能性の記述を評定する。このワークユニットで重視するのは、情報の正確さの評定ではなく、この記述の詳細のレベルである(情報の正確さの評定は、次のワークユニットの焦点である)。

1750 この基本コンポーネントの機能性の記述は、TOE 設計(TOE 設計(ADV_TDS))で提供される、TSF のコンポーネントの記述のレベル以上に詳細にする必要はない。

ACO_REL.1-2 評価者は、依存情報が依存コンポーネントの運用環境に対して特定されている対策方針を正確に反映することを決定するために、その依存情報を***検査しなければならない。***

1751 依存情報には、依存コンポーネントが依存する基本コンポーネントのセキュリティ機能性の記述が含まれる。依存情報が依存コンポーネントの運用環境の期待に一貫していることを保証するために、評価者は、依存情報を依存コンポーネントに対する ST における環境の対策方針のステートメントと比較する。

1752 例えば、依存情報は依存コンポーネント TSF が基本コンポーネントに依存して監査データを格納及び保護することを主張するが、その他の評価証拠(例えば、依存コンポーネント設計)が依存コンポーネント TSF 自体が監査データの格納及び保護を行っていることを明確に表している場合、これは不正確性を示す。

1753 運用環境の対策方針には IT 以外の手段によって満たすことができる対策方針が含まれる可能性があることに注意するべきである。基本コンポーネント環境によって提供されることが期待されているサービスは、依存コンポーネント ST における IT による運用環境のセキュリティ対策方針の記述において記述される可能性があるが、環境に対するこのような期待すべてを依存情報に記述する必要はない。

ACO_REL.1.2C ***依存情報は、依存コンポーネント TSF が基本コンポーネントからサービスを要求するために使用するすべての相互作用を記述しなければならない。***

ACO_REL.1-3 評価者は、依存コンポーネント TSF が基本コンポーネントからサービスを要求するために使用する、依存コンポーネントと基本コンポーネントの間のすべての相互作用を依存情報が記述していることを決定するために、その依存情報を***検査しなければならない。***

1754 依存コンポーネント TSF は、基本コンポーネントの TSF 内に存在しなかった基本コンポーネントのサービスを要求する可能性がある(CC パート 3、B.3、「統合 IT エンティティ間の相互作用」を参照のこと)。

1755 基本コンポーネントの機能性に対するインタフェースは、TOE 設計(サブアクティビティの評価(ADV_TDS.1))のサブシステム間で提供される、依存コンポーネント TSF 機能性に対するインタフェースの記述と同じレベルで記述される。

1756 依存コンポーネントと基本コンポーネントの間の相互作用を記述する目的は、依存コンポーネント TSF が依存コンポーネントのセキュリティ機能性の動作をサポートするサービスの提供のためにどのように基本コンポーネントに依存しているかについて知識を提供することである。これらの相互作用は、実装レベル(例えば、あるコンポーネント内のルーチンから別のコンポーネント内のルーチンに渡されるパラメタ)で特徴を表す必要はないが、別のコンポーネントによって使用される特定のコンポーネントに対して識別されるデータエレメントは、この記述に含まれるべきである。このステートメントは、相互作用が必要である理由を読者が大まかに理解するのに役立つべきである。

1757 インタフェースの正確性及び完全性は、ワークユニット ACO_REL.1-1 及び ACO_REL.1-2 で評定された、TSF が基本コンポーネントによって提供されることを要求するセキュリティ機能性に基づいている。以前のワークユニットで記述されているすべての機能性をこのワークユニットで識別されているインタフェースにマッピングすること、及び逆方向のマッピングを行うことは可能であるべきである。記述された機能性に対応しないインタフェースも、不十分性を示す。

ACO_REL.1.3C ***依存情報は、依存 TSF が、基本コンポーネントによる干渉及び改ざんから自分自身をどのように保護するかを記述しなければならない。***

ACO_REL.1-4 評価者は、依存 TSF が基本コンポーネントによる干渉及び改ざんからどのように自分自身を保護しているかを決定するために、その依存情報を***検査しなければならない。***

1758 依存コンポーネントが基本コンポーネントによる干渉及び改ざんからどのように自分自身を保護するかの記述は、ADV_ARC.1-4に必要な詳細レベルと同じレベルで提供される。

17.5.2 サブアクティビティの評価(ACO_REL.2)

17.5.2.1 目的

1759 このサブアクティビティの目的は、必要な機能性が基本コンポーネントで使用できること、及びその機能性が呼び出される手段を決定するために十分な情報を開発者の依存証拠が提供しているかどうかを決定することである。これは、依存コンポーネントと基本コンポーネントの間のインタフェース、及び依存コンポーネントによって呼び出されるインタフェースからの戻り値の観点から提供される。

17.5.2.2 入力

1760 このサブアクティビティ用の評価証拠は、次のとおりである:

a) 統合 ST;

b) 依存コンポーネント機能仕様;

c) 依存コンポーネント設計;

d) 依存コンポーネント実装表現;

e) 依存コンポーネントアーキテクチャ設計;

f) 依存情報。

17.5.2.3 適用上の注釈

1761 基本コンポーネントと相互に作用する TSF を持つ依存コンポーネントには、その基本コンポーネントによって提供される機能性(例えば、リモート認証、リモート監査データ格納)が必要である。このような場合、エンド利用者のための統合 TOE の構成の担当者に対して、呼び出されたサービスを記述する必要がある。この証拠資料を必要とする根拠は、統合 TOE のインテグレータが、依存コンポーネントに有害な影響を与える可能性があるのは基本コンポーネントにおけるどのようなサービスであるかを決定し、開発証拠(ACO_DEV)ファミリの適用時にコンポーネントの互換性を決定するために照合する情報を提供するのを支援することである。

17.5.2.4 アクション ACO_REL.2.1E

ACO_REL.2.1C ***依存情報は、依存コンポーネントTSF が依存する基本コンポーネントハードウェア、ファームウェア及びまたはソフトウェアの機能性を記述しなければならない。***

ACO_REL.2-1 評価者は、依存コンポーネント TSF が依存する基本依存ハードウェア、ファームウェア、及び/またはソフトウェアの機能性を依存情報が記述していることを決定するために、その依存情報を***チェックしなければならない。***

1762 評価者は、依存コンポーネント TSF が基本コンポーネントのハードウェア、ファームウェア、及びソフトウェアによって提供されることを要求するセキュリティ機能性の記述を評定する。このワークユニットで重視するのは、情報の正確さの評定ではなく、この記述の詳細のレベルである(情報の正確さの評定は、次のワークユニットの焦点である)。

1763 この基本コンポーネントの機能性の記述は、TOE 設計(TOE 設計(ADV_TDS))で提供される、TSF のコンポーネントの記述のレベル以上に詳細にする必要はない。

ACO_REL.2-2 評価者は、依存情報が依存コンポーネントの運用環境に対して特定されている対策方針を正確に反映することを決定するために、その依存情報を***検査しなければならない。***

1764 依存情報には、依存コンポーネントが依存する基本コンポーネントのセキュリティ機能性の記述が含まれる。依存情報が依存コンポーネントの運用環境の期待に一貫していることを保証するために、評価者は、依存情報を依存コンポーネントに対する ST における環境の対策方針のステートメントと比較する。

1765 例えば、依存情報は依存コンポーネント TSF が基本コンポーネントに依存して監査データを格納及び保護することを主張するが、その他の評価証拠(例えば、依存コンポーネント設計)が依存コンポーネント TSF 自体が監査データの格納及び保護を行っていることを明確に表している場合、これは不正確性を示す。

1766 運用環境の対策方針には IT 以外の手段によって満たすことができる対策方針が含まれる可能性があることに注意するべきである。基本コンポーネント環境によって提供されることが期待されているサービスは、依存コンポーネント ST における IT による運用環境のセキュリティ対策方針の記述において記述される可能性があるが、環境に対するこのような期待すべてを依存情報に記述する必要はない。

ACO_REL.2.2C ***依存情報は、依存コンポーネント TSF が基本コンポーネントからサービスを要求するために使用するすべての相互作用を記述しなければならない。***

ACO_REL.2-3 評価者は、依存コンポーネント TSF が基本コンポーネントからサービスを要求するために使用する、依存コンポーネントと基本コンポーネントの間のすべての相互作用を依存情報が記述していることを決定するために、その依存情報を***検査しなければならない。***

1767 依存コンポーネント TSF は、基本コンポーネントの TSF 内に存在しなかった基本コンポーネントのサービスを要求する可能性がある(CC パート 3、B.3、「統合 IT エンティティ間の相互作用」を参照のこと)。

1768 基本コンポーネントの機能性に対するインタフェースは、TOE 設計(サブアクティビティの評価(ADV_TDS.1))のサブシステム間で提供される、依存コンポーネント TSF 機能性に対するインタフェースの記述と同じレベルで記述される。

1769 依存コンポーネントと基本コンポーネントの間の相互作用を記述する目的は、依存コンポーネント TSF が依存コンポーネントのセキュリティ機能性の動作をサポートするサービスの提供のためにどのように基本コンポーネントに依存しているかについて知識を提供することである。これらの相互作用は、実装レベル(例えば、あるコンポーネント内のルーチンから別のコンポーネント内のルーチンに渡されるパラメタ)で特徴を表す必要はないが、別のコンポーネントによって使用される特定のコンポーネントに対して識別されるデータエレメントは、この記述に含まれるべきである。このステートメントは、相互作用が必要である理由を読者が大まかに理解するのに役立つべきである。

1770 インタフェースの正確性及び完全性は、ワークユニットACO_REL.2-1及びACO_REL.2-2で評定された、TSF が基本コンポーネントによって提供されることを要求するセキュリティ機能性に基づいている。以前のワークユニットで記述されているすべての機能性をこのワークユニットで識別されているインタフェースにマッピングすること、及び逆方向のマッピングを行うことは可能であるべきである。記述された機能性に対応しないインタフェースも、不十分性を示す。

ACO_REL.2.3C ***依存情報は、使用されるインタフェース及びそれらのインタフェースからの戻り値の観点から各相互作用を記述しなければならない。***

ACO_REL.2-4 依存情報は、使用されるインタフェース及びそれらのインタフェースからの戻り値の観点から各相互作用を記述しなければならない。

1771 依存コンポーネント TSF が基本コンポーネントへのサービス要求を行う際に使用するインタフェースの識別情報によって、インテグレータは、基本コンポーネントが必要な対応するインタフェースをすべて提供するかどうかを決定することができる。これは、依存コンポーネントが期待する戻り値の仕様を通じてさらに詳しく理解される。評価者は、(ACO_REL.2-3での分析に従って)特定された各相互作用についてインタフェースが記述されることを保証する。

ACO_REL.2.4C ***依存情報は、依存 TSF が、基本コンポーネントによる干渉及び改ざんから自分自身をどのように保護するかを記述しなければならない。***

ACO_REL.2-5 評価者は、依存TSFが基本コンポーネントによる干渉及び改ざんからどのように自分自身を保護しているかを決定するために、その依存情報を***検査しなければならない。***

1772 依存コンポーネントが基本コンポーネントによる干渉及び改ざんからどのように自分自身を保護するかの記述は、ADV_ARC.1-4に必要な詳細レベルと同じレベルで提供される。

17.6 統合 TOE のテスト(ACO_CTT)

17.6.1 サブアクティビティの評価(ACO_CTT.1)

17.6.1.1 目的

1773 このサブアクティビティの目的は、依存コンポーネントが依存する各基本コンポーネントインタフェースについて、開発者がテストを正しく実行し、証拠資料として提出したかどうかを決定することである。この決定の一環として、評価者は、開発者が実行したテストのサンプルを繰返すとともに、すべての統合 TOE SFR 及び依存コンポーネントが依存する基本コンポーネントのインタフェースの期待されるふるまいが実証されることを保証するために必要な追加のテストを実行する。

17.6.1.2 入力

1774 このサブアクティビティ用の評価証拠は、次のとおりである:

a) テストに適した統合 TOE;

b) 統合 TOE のテストの証拠;

c) 依存情報;

d) 開発情報。

17.6.1.3 アクション ACO_CTT.1.1E

ACO_CTT.1.1C ***統合 TOE 及び基本コンポーネントインタフェーステスト証拠資料は、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されなければならない。***

ACO_CTT.1-1 評価者は、統合 TOE のテスト証拠資料がテスト計画、期待されるテスト結果、及び実際のテスト結果で構成されていることを決定するために、この証拠資料を***検査しなければならない。***

1775 依存コンポーネントの運用環境における IT の要件を満たすために基本コンポーネントが使用された場合は、依存コンポーネントの評価からテスト証拠を提供することで、このワークユニットを満たすことができる。

1776 以下を決定するために、ATE_FUN.1.1E を満たすために必要なすべてのワークユニットが適用される:

a) テスト証拠資料が、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されること;

b) テスト証拠資料に、テストが繰返し可能であることを保証するために必要な情報が含まれていること;

c) 基本コンポーネントのテストに適用された開発者の労力のレベル。

ACO_CTT.1-2 評価者は、基本コンポーネントインタフェースのテスト証拠資料がテスト計画、期待されるテスト結果、及び実際のテスト結果で構成されていることを決定するために、この証拠資料を***検査しなければならない。***

1777 統合 TOE で依存コンポーネントが依存するこれらのインタフェースは、評価に成功した基本コンポーネントの TSFI であるため、基本コンポーネントの評価からテスト証拠を提供することで、このワークユニットを満たすことができる。依存コンポーネントが依存する基本コンポーネントのインタフェースが、実際に評価済み基本コンポーネントの TSFI であったかどうかの決定は、ACO_COR アクティビティで行われる。

1778 以下を決定するために、ATE_FUN.1.1E を満たすために必要なすべてのワークユニットが適用される:

a) テスト証拠資料が、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されること;

b) テスト証拠資料に、テストが繰返し可能であることを保証するために必要な情報が含まれていること;

c) 基本コンポーネントのテストに適用された開発者の労力のレベル。

ACO_CTT.1.2C ***開発者が実行した統合 TOE テストのテスト証拠資料は、TSF が仕様どおりにふるまうことを実証しなければならない。***

ACO_CTT.1-3 評価者は、開発者が実行した統合 TOE テストによって TSF が仕様どおりにふるまうことが実証されなければならないことを決定するために、テスト証拠資料を***検査しなければならない。***

1779 評価者は、開発者によってテストされた SFR を識別するために、テスト計画に記述されたテストと統合 TOE に対して特定された SFR の間のマッピングを作成するべきである。

1780 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1 章

b) 15.2.2 章

1781 開発者によってテストされた統合 TOE の SFR が期待したとおりにふるまうことを決定するために、テストの実行が成功したときの出力(ATE_FUN.1.3C で評定)をマッピングと比較することができる。

ACO_CTT.1.3C ***開発者が実行した基本コンポーネントインタフェーステストのテスト証拠資料は、依存コンポーネントが依存する基本コンポーネントインタフェースが仕様どおりにふるまうことを実証しなければならない。***

ACO_CTT.1-4 評価者は、開発者が実行した基本コンポーネントインタフェーステストによって、依存コンポーネントが依存する基本コンポーネントインタフェースが仕様どおりにふるまうことが実証されなければならないことを決定するために、テスト証拠資料を***検査しなければならない。***

1782 評価者は、開発者によってテストされた基本コンポーネントインタフェースを識別するために、テスト計画に記述されたテストと(依存情報で特定され、ACO_REL で検査された)依存コンポーネントが依存する基本コンポーネントのインタフェースの間のマッピングを作成するべきである。

1783 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1 章

b) 15.2.2 章

1784 開発者によってテストされた基本コンポーネントのインタフェースが期待したとおりに動作することを決定するために、テストの実行が成功したときの出力(ATE_FUN.1.3Cで評定)をマッピングと比較することができる。

ACO_CTT.1.4C ***基本コンポーネントは、テストに適していなければならない。***

ACO_CTT.1-5 評価者は、統合 TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1785 統合 TOE が適切に設置され、定義された状態にあることを決定するために、開発者からテスト用に提供された TOE に ATE_IND.2-1 及び ATE_IND.2-2 ワークユニットが適用される。

ACO_CTT.1-6 評価者は、開発者によって提供された一連の資源が、基本コンポーネントを機能的にテストするために基本コンポーネントの開発者が使用した一連の資源と同等であることを決定するために、その一連の資源を***検査しなければならない。***

1786 提供された一連の資源が、統合 TOE で使用される基本コンポーネントを機能的にテストするために使用された資源と同等であることを決定するために、ATE_IND.2-3 ワークユニットが適用される。

17.6.1.4 **アクション** ACO_CTT.1.2E

ACO_CTT.1-7 評価者は、統合 TOE セキュリティターゲットで特定されている SFR のサブセットに対して、開発者テスト結果を検証するために ATE_IND.2.2E に従ってテストを**実行しなければならない。**

1787 評価者は、ATE_IND.2.2E を満たすために必要なすべてのワークユニットを適用して、関連するワークユニットで指示されているように、統合 TOE のすべての分析、結果、及び判定について ETR に報告する。

17.6.1.5 **アクション** ACO_CTT.1.3E

ACO_CTT.1-8 評価者は、統合TOEセキュリティターゲットで特定されている SFR のサブセットに対して、TSF が特定されたとおりに機能することを確認するために、ATE_IND.2.3E に従ってテストを**実行しなければならない。**

1788 評価者は、ATE_IND.2.3E を満たすために必要なすべてのワークユニットを適用して、それらのワークユニットで指示されているように、統合 TOE のすべての分析、結果、及び判定について ETR に報告する。

1789 評価者は、テストする統合 TOE の TSF のインタフェースを選択するときに、評価済みバージョンまたは構成のコンポーネントに対する改変を考慮に入れるべきである。評価済みのコンポーネントに対する改変には、導入されたパッチ、ガイダンス証拠資料が改変されたことによる構成の変更、コンポーネントの TSF に含まれていなかったコンポーネントの追加部分への依存などが含まれる。これらの改変は、統合の根拠(ACO_COR)アクティビティ中に識別される。

17.6.2 サブアクティビティの評価(ACO_CTT.2)

17.6.2.1 目的

1790 このサブアクティビティの目的は、依存コンポーネントが依存する各基本コンポーネントインタフェースについて、開発者がテストを正しく実行し、証拠資料として提出したかどうかを決定することである。この決定の一環として、評価者は、開発者が実行したテストのサンプルを繰返すとともに、統合 TOE 及び依存コンポーネントが依存する基本コンポーネントのインタフェースの期待されるふるまいを完全に実証するために必要な追加のテストを実行する。

17.6.2.2 入力

1791 このサブアクティビティ用の評価証拠は、次のとおりである:

a) テストに適した統合 TOE;

b) 統合 TOE のテスト証拠;

c) 依存情報;

d) 開発情報。

17.6.2.3 アクション ACO_CTT.2.1E

ACO_CTT.2.1C ***統合 TOE 及び基本コンポーネントインタフェーステスト証拠資料は、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されなければならない。***

ACO_CTT.2-1 評価者は、統合 TOE のテスト証拠資料がテスト計画、期待されるテスト結果、及び実際のテスト結果で構成されていることを決定するために、この証拠資料を***検査しなければならない。***

1792 依存コンポーネントの運用環境における IT の要件を満たすために基本コンポーネントが使用された場合は、依存コンポーネントの評価からテスト証拠を提供することで、このワークユニットを満たすことができる。

1793 以下を決定するために、ATE_FUN.1.1E を満たすために必要なすべてのワークユニットが適用される:

a) テスト証拠資料が、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されること;

b) テスト証拠資料に、テストが繰返し可能であることを保証するために必要な情報が含まれていること;

c) 基本コンポーネントのテストに適用された開発者の労力のレベル。

ACO_CTT.2-2 評価者は、基本コンポーネントインタフェースのテスト証拠資料がテスト計画、期待されるテスト結果、及び実際のテスト結果で構成されていることを決定するために、この証拠資料を***検査しなければならない。***

1794 統合 TOE で依存コンポーネントが依存するこれらのインタフェースは、評価に成功した基本コンポーネントの TSFI であるため、基本コンポーネントの評価からテスト証拠を提供することで、このワークユニットを満たすことができる。依存コンポーネントが依存する基本コンポーネントのインタフェースが、実際に評価済み基本コンポーネントの TSFI であったかどうかの決定は、ACO_COR アクティビティ中に行われる。

1795 以下を決定するために、ATE_FUN.1.1E を満たすために必要なすべてのワークユニットが適用される:

a) テスト証拠資料が、テスト計画、期待されるテスト結果、及び実際のテスト結果から構成されること;

b) テスト証拠資料に、テストが繰返し可能であることを保証するために必要な情報が含まれていること;

c) 基本コンポーネントのテストに適用された開発者の労力のレベル。

ACO_CTT.2.2C ***開発者が実行した統合 TOE のテストによるテスト証拠資料は、TSF が仕様どおりに動作し、完全であることを実証しなければならない。***

ACO_CTT.2-3 評価者は、統合 TOE のテストに関連するテスト証拠資料内のテストと、統合 TOE セキュリティターゲットの統合 TOE の SFR との間における、正確な対応をテスト証拠資料が提供していることを決定するために、この証拠資料を***検査しなければならない。***

1796 単純な相互表がテストの対応を十分に示すことができる。テスト証拠資料に示されているテストと SFR の間の対応は、曖昧にならないように識別される必要がある。

ACO_CTT.2-4 評価者は、開発者が実行した統合 TOE テストによって TSF が仕様どおりにふるまうことを実証しなければならないことを決定するために、テスト証拠資料を***検査しなければならない。***

1797 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1 章

b) 15.2.2 章

1798 開発者によってテストされた統合 TOE の SFR が期待したとおりに動作することを決定するために、テストの実行が成功したときの出力(ATE_FUN.1.3C で評定)をマッピングと比較することができる。

ACO_CTT.2.3C ***開発者が実行した基本コンポーネントインタフェーステストのテスト証拠資料は、依存コンポーネントが依存する基本コンポーネントインタフェースが仕様どおりに動作し、完全であることを実証しなければならない。***

ACO_CTT.2-5 評価者は、依存コンポーネントが依存する基本コンポーネントインタフェースのテストに関連するテスト証拠資料内のテストと、依存情報で特定されたインタフェースとの間における、正確な対応をテスト証拠資料が提供していることを決定するために、この証拠資料を***検査しなければならない。***

1799 単純な相互表がテストの対応を十分に示すことができる。テスト証拠資料に示されているテストとインタフェースの間の対応は、曖昧にならないように識別される必要がある。

ACO_CTT.2-6 評価者は、開発者が実行した基本コンポーネントインタフェーステストによって、依存コンポーネントが依存する基本コンポーネントインタフェースが仕様どおりにふるまうことが実証されなければならないことを決定するために、テスト証拠資料を***検査しなければならない。***

1800 このワークユニットのガイダンスは、次のものの中に見つけることができる:

a) 15.2.1 章

b) 15.2.2 章

1801 開発者によってテストされた基本コンポーネントのインタフェースが期待したとおりに動作することを決定するために、テストの実行が成功したときの出力(ATE_FUN.1.3Cで評定)をマッピングと比較することができる。

ACO_CTT.2.4C ***基本コンポーネントは、テストに適していなければならない。***

ACO_CTT.2-7 評価者は、統合 TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1802 統合 TOE が適切に設置され、定義された状態にあることを決定するために、開発者からテスト用に提供された TOE に ATE_IND.2-1 及び ATE_IND.2-2 ワークユニットが適用される。

ACO_CTT.2-8 評価者は、開発者によって提供された一連の資源が、基本コンポーネントを機能的にテストするために基本コンポーネントの開発者が使用した一連の資源と同等であることを決定するために、その一連の資源を***検査しなければならない。***

1803 提供された一連の資源が、統合 TOE で使用される基本コンポーネントを機能的にテストするために使用された資源と同等であることを決定するために、ATE_IND.2-3 ワークユニットが適用される。

17.6.2.4 **アクション** ACO_CTT.2.2E

ACO_CTT.2-9 統合 TOE セキュリティターゲットで特定された SFR の正しいふるまいを実証するために、ATE_IND.2.2E に従ってテストが選択され、実行される。

1804 評価者は、ATE_IND.2.2E を満たすために必要なすべてのワークユニットを適用して、関連するワークユニットで指示されているように、統合 TOE のすべての分析、結果、及び判定について ETR に報告する。

17.6.2.5 **アクション** ACO_CTT.2.3E

ACO_CTT.2-10 評価者は、統合 TOE セキュリティターゲットで特定されている SFR のサブセットに対して、TSF が特定されたとおりに機能することを確認するために、ATE_IND.2.3E に従ってテストを***実行しなければならない。***

1805 評価者は、ATE_IND.2.3E を満たすために必要なすべてのワークユニットを適用して、それらのワークユニットで指示されているように、統合 TOE のすべての分析、結果、及び判定について ETR に報告する。

1806 評価者は、テストする統合 TOE の TSF のインタフェースを選択するときに、評価済みバージョンまたは構成の、コンポーネントに対する改変を考慮に入れるべきである。評価済みのコンポーネントに対する改変には、導入されたパッチ、ガイダンス証拠資料が改変されたことによる構成の変更、コンポーネントの TSF に含まれていなかったコンポーネントの追加部分への依存などが含まれる。これらの改変は、統合の根拠(ACO_COR)アクティビティ中に識別される。

ACO_CTT.2-11 評価者は、基本コンポーネントへのインタフェースのサブセットが特定されたとおりに機能することを確認するために、サブアクティビティの評価(ATE_IND.2)に従って、そのサブセットのテストを*実行しなければならない。*

1807 評価者は、ATE_IND.2.3E を満たすために必要なすべてのワークユニットを適用して、それらのワークユニットで指示されているように、統合 TOE のすべての分析、結果、及び判定について ETR に報告する。

1808 評価者は、テストする基本コンポーネントのインタフェースを選択するときに、評価済みバージョンまたは設定の基本コンポーネントに対する改変を考慮に入れるべきである。特に、評価者は、基本コンポーネントの評価中には考慮されなかった基本コンポーネントのインタフェースの正しいふるまいを実証するテストの開発を考慮するべきである。基本コンポーネントに対するこれらの追加インタフェースやその他の改変は、統合の根拠(ACO_COR)アクティビティ中に識別される。

17.7 統合の脆弱性分析(ACO_VUL)

17.7.1 サブアクティビティの評価(ACO_VUL.1)

17.7.1.1 目的

1809 このサブアクティビティの目的は、統合 TOE が、その運用環境において、簡単に悪用される可能性のある脆弱性を持つかどうかを決定することである。

1810 開発者は、コンポーネントの評価から報告された残存脆弱性の詳細を提供する。評価者は、報告された残存脆弱性の処置の分析を実行し、また、コンポーネントの新たな潜在的脆弱性(つまり、基本コンポーネントの評価以降に公知として報告された問題)を識別するために、公知になっているものの探索を実行する。その後、評価者は、侵入テストを実行して、基本的な攻撃能力を持つ攻撃者が運用環境の TOE で潜在的脆弱性を悪用できないことを実証する。

17.7.1.2 入力

1811 このサブアクティビティ用の評価証拠は、次のとおりである:

a) テストに適した統合 TOE;

b) 統合 ST;

c) 統合の根拠;

d) ガイダンス証拠資料;

e) 発生する可能性があるセキュリティの脆弱性の識別をサポートするために公開の場で利用できる情報;

f) 各コンポーネントの評価中に報告された残存脆弱性。

17.7.1.3 適用上の注釈

1812 サブアクティビティの評価(AVA_VAN.1)の適用上の注釈を参照のこと。

17.7.1.4 アクション ACO_VUL.1.1E

ACO_VUL.1.1C ***統合 TOE は、テストに適していなければならない。***

ACO_VUL.1-1 評価者は、統合 TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1813 統合 TOE が適切に設置され、定義された状態にあることを決定するために、その統合 TOE に ATE_IND.2-1 及び ATE_IND.2-2 ワークユニットが適用される。

1814 保証パッケージにACO_CTTファミリからのコンポーネントが含まれる場合、評価者はこれが満たされていることを実証するために、ワークユニットACO_CTT*-1の結果を参照することができる。

ACO_VUL.1-2 評価者は、IT エンティティに関連するコンポーネントの ST における前提条件と対策方針が、他のコンポーネントによって満たされることを決定するために、統合 TOE の構成を***検査しなければならない。***

1815 コンポーネントの ST には、ST により関連付けられる、そのコンポーネントを使用する可能性がある他のコンポーネントについての前提条件が含まれている場合がある。例えば、基本コンポーネントとして使用されるオペレーティングシステムの ST には、オペレーティングシステムにロードされるアプリケーションが特権モードで実行されないという前提条件が含まれる可能性がある。これらの前提条件及び対策方針は、統合 TOE の他のコンポーネントによって満たされる。

17.7.1.5 **アクション** ACO_VUL.1.2E

ACO_VUL.1-3 評価者は、基本コンポーネント評価からの残存脆弱性が運用環境の統合 TOE で悪用される可能性がないことを決定するために、それらの残存脆弱性を***検査しなければならない。***

1816 基本コンポーネントの評価中に製品で識別され、基本コンポーネントで悪用不能であることを実証された脆弱性のリストは、このアクティビティへの入力として使用される。評価者は、脆弱性が悪用不能であるとみなされたときの前提が統合 TOE で維持されていること、あるいは組み合わせによって潜在的脆弱性が再びもたらされたかどうかを決定する。例えば、基本コンポーネントの評価中に特定のオペレーティングシステムサービスが無効にされていることが想定される場合に、そのサービスが統合 TOE 評価で有効にされているときは、以前に調べたそのサービスに関連する潜在的脆弱性をここで考慮するべきである。

1817 また、基本コンポーネントの評価で判明した既知の悪用不能脆弱性のこのリストを、統合 TOE 内の他のコンポーネント(例えば、依存コンポーネント)の既知の悪用不能脆弱性に照らして考慮するべきである。これは、単独では悪用不能な潜在的脆弱性が、別の潜在的脆弱性を含んでいる IT エンティティと統合されたときに悪用可能となる場合を考慮するためである。

ACO_VUL.1-4 評価者は、依存コンポーネント評価からの残存脆弱性が運用環境の統合 TOE で悪用される可能性がないことを決定するために、それらの残存脆弱性を***検査しなければならない。***

1818 依存コンポーネントの評価中に製品で識別され、依存コンポーネントで悪用不能であることを実証された脆弱性のリストは、このアクティビティへの入力として使用される。評価者は、脆弱性が悪用不能であるとみなされたときの前提が統合 TOE で維持されていること、あるいは組み合わせによって潜在的脆弱性が再びもたらされたかどうかを決定する。例えば、依存コンポーネントの評価中に運用環境の要件を満たしている IT からサービス要求への応答として特定の値が返されないことが想定される場合に、統合 TOE の評価で基本コンポーネントからその値が提供されるときは、以前に調べたその戻り値に関連する潜在的脆弱性をここで考慮するべきである。

1819 また、依存コンポーネントの評価で判明した既知の悪用不能脆弱性のこのリストを、統合 TOE 内の他のコンポーネント(例えば、基本コンポーネント)の既知の悪用不能脆弱性に照らして考慮するべきである。これは、単独では悪用不能な潜在的脆弱性が、別の潜在的脆弱性を含んでいる IT エンティティと統合されたときに悪用可能となる場合を考慮するためである。

17.7.1.6 **アクション** ACO_VUL.1.3E

ACO_VUL.1-5 評価者は、基本コンポーネントの評価の完了以降に知られることになった、基本コンポーネントで発生する可能性があるセキュリティ脆弱性の識別をサポートするために、公開の場で利用できる情報源を***検査しなければならない。***

1820 評価者は、基本コンポーネントの脆弱性を探索するために、AVA_VAN.1-2 の記述に従って、公知の情報を使用する。

1821 攻撃者が潜在的脆弱性を悪用するために必要とする攻撃能力が大幅に低減されたことを評価者が把握した場合を除いて、基本コンポーネントの評価より前に公開の場で利用可能であった潜在的脆弱性の調査をそれ以上進める必要はない。これは、基本コンポーネント評価以降に何らかの新しい技術が導入され、潜在的脆弱性の悪用が単純になっている可能性がある。

ACO_VUL.1-6 評価者は、依存コンポーネントの評価の完了以降に知られることになった、依存コンポーネントで発生する可能性があるセキュリティ脆弱性の識別をサポートするために公開の場で利用できる情報源を***検査しなければならない。***

1822 評価者は、AVA_VAN.1-2 の記述に従って、公知の情報を使用して依存コンポーネントでの脆弱性を探索する。

1823 攻撃者が潜在的脆弱性を悪用するために必要とする攻撃能力が大幅に引き下げられたことを評価者が把握した場合を除いて、依存コンポーネントの評価より前に公開の場で利用可能であった潜在的脆弱性の調査をそれ以上進める必要はない。これは、依存コンポーネント評価以降何らかの新しい技術が導入され、潜在的脆弱性の悪用が単純になっている可能性がある。

ACO_VUL.1-7 評価者は、ETR 内で、テストの候補となり、運用環境の統合 TOE に適用できる識別された潜在的なセキュリティ脆弱性を***記録しなければならない。***

1824 脆弱性が運用環境の統合 TOE に関連しているかどうかを決定するために、ST、ガイダンス証拠資料、及び機能仕様が使用される。

1825 評価者が運用環境で脆弱性が該当しないことを決定する場合、評価者は、それ以上の考慮から脆弱性を除外する理由を記録する。それ以外の場合は、評価者は、さらに考慮する対象となる潜在的な脆弱性を記録する。

1826 運用環境の統合 TOE に適用できる潜在的な脆弱性のリストは、侵入テストアクティビティ(つまり、ACO_VUL.1.4E)に対する入力として使用でき、評価者が ETR で報告しなければならない。

17.7.1.7 アクション ACO_VUL.1.4E

ACO_VUL.1-8 評価者は、AVA_VAN.1.3E で詳述されているように、侵入テストを***実施しなければならない。***

1827 評価者は、評価者アクション AVA_VAN.1.3E を満たすために必要なすべてのワークユニットを適用して、それらのワークユニットで指示されている統合 TOE のすべての分析及び判定について ETR に報告する。

1828 また評価者は、開発者から提供された統合 TOE がテストに適していることを決定するために、評価者アクション AVA_VAN.1.1E のワークユニットを適用する。

17.7.2 サブアクティビティの評価(ACO_VUL.2)

17.7.2.1 目的

1829 このサブアクティビティの目的は、統合 TOE が、その運用環境において、基本的な攻撃能力を持つ攻撃者が悪用できる脆弱性を持つかどうかを決定することである。

1830 開発者は、コンポーネントについて報告された残存脆弱性、及び基本コンポーネントと依存コンポーネントの組み合わせを通じてもたらされた脆弱性について、処置の分析を提供する。評価者は、コンポーネントの新たな潜在的脆弱性(つまり、コンポーネントの評価の完了以降に公知として報告された問題)を識別するために、公知になっているものの探索を実行する。評価者は、統合 TOE の独立脆弱性分析及び侵入テストも実行する。

17.7.2.2 入力

1831 このサブアクティビティ用の評価証拠は、次のとおりである:

a) テストに適した統合 TOE;

b) 統合 ST;

c) 統合の根拠;

d) 依存情報;

e) ガイダンス証拠資料;

f) 発生する可能性があるセキュリティ脆弱性の識別をサポートするために公開の場で利用できる情報;

g) 各コンポーネントの評価中に報告された残存脆弱性。

17.7.2.3 適用上の注釈

1832 サブアクティビティの評価(AVA_VAN.2)の適用上の注釈を参照のこと。

17.7.2.4 アクション ACO_VUL.2.1E

ACO_VUL.2.1C ***統合 TOE は、テストに適していなければならない。***

ACO_VUL.2-1 評価者は、統合 TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1833 統合 TOE が適切に設置され、定義された状態にあることを決定するために、その統合 TOE に ATE_IND.2-1 及び ATE_IND.2-2 ワークユニットが適用される。

1834 保証パッケージに ACO_CTT ファミリが含まれる場合、評価者はこれが満たされていることを実証するために、ワークユニット統合 TOE テスト(ACO_CTT)*-1 の結果を参照することができる。

ACO_VUL.2-2 評価者は、IT エンティティに関連するコンポーネントの ST における前提条件と対策方針が、他のコンポーネントによって満たされることを決定するために、統合 TOE の構成を***検査しなければならない。***

1835 コンポーネントの ST には、ST により関連付けられる、そのコンポーネントを使用する可能性がある他のコンポーネントについての前提条件が含まれている場合がある。例えば、基本コンポーネントとして使用されるオペレーティングシステムの ST には、オペレーティングシステムにロードされるアプリケーションが特権モードで実行されないという前提条件が含まれる可能性がある。これらの前提条件及び対策方針は、統合 TOE の他のコンポーネントによって満たされる。

17.7.2.5 アクション ACO_VUL.2.2E

ACO_VUL.2-3 評価者は、基本コンポーネント評価からの残存脆弱性が運用環境の統合 TOE で悪用される可能性がないことを決定するために、それらの残存脆弱性を***検査しなければならない。***

1836 基本コンポーネントの評価中に製品で識別され、基本コンポーネントで悪用不能であることを実証された脆弱性のリストは、このアクティビティへの入力として使用される。評価者は、脆弱性が悪用不能であるとみなされたときの前提が統合 TOE で維持されていること、あるいは組み合わせによって潜在的脆弱性が再びもたらされたかどうかを決定する。例えば、基本コンポーネントの評価中に特定のオペレーティングシステムサービスが無効にされていることが想定される場合に、そのサービスが統合 TOE 評価で有効にされているときは、以前に調べたそのサービスに関連する潜在的脆弱性をここで考慮するべきである。

1837 また、基本コンポーネントの評価で判明した既知の悪用不能脆弱性のこのリストを、統合 TOE 内の他のコンポーネント(例えば、依存コンポーネント)の既知の悪用不能脆弱性に照らして考慮するべきである。これは、単独では悪用不能な潜在的脆弱性が、別の潜在的脆弱性を含んでいる IT エンティティと統合されたときに悪用可能となる場合を考慮するためである。

ACO_VUL.2-4 評価者は、依存コンポーネント評価からの残存脆弱性が運用環境の統合 TOE で悪用される可能性がないことを決定するために、それらの残存脆弱性を***検査しなければならない。***

1838 依存コンポーネントの評価中に製品で識別され、依存コンポーネントで悪用不能であることを実証された脆弱性のリストは、このアクティビティへの入力として使用される。評価者は、脆弱性が悪用不能であるとみなされたときの前提が統合 TOE で維持されていること、あるいは組み合わせによって潜在的脆弱性が再びもたらされたかどうかを決定する。例えば、依存コンポーネントの評価中に運用環境の要件を満たしている IT からサービス要求への応答として特定の値が返されないことが想定される場合に、統合 TOE の評価で基本コンポーネントからその値が提供されるときは、以前に調べたその戻り値に関連する潜在的脆弱性をここで考慮するべきである。

1839 また、依存コンポーネントの評価で判明した既知の悪用不能脆弱性のこのリストを、統合 TOE 内の他のコンポーネント(例えば、基本コンポーネント)の既知の悪用不能脆弱性に照らして考慮するべきである。これは、単独では悪用不能な潜在的脆弱性が、別の潜在的脆弱性を含んでいる IT エンティティと統合されたときに悪用可能となる場合を考慮するためである。

17.7.2.6 アクション ACO_VUL.2.3E

ACO_VUL.2-5 評価者は、基本コンポーネントの評価の完了以降に知られることになった、基本コンポーネントで発生する可能性があるセキュリティ脆弱性の識別をサポートするために公開の場で利用できる情報源を**検査しなければならない**。

1840 評価者は、基本コンポーネントの脆弱性を探索するために、AVA_VAN.2-2 の記述に従って、公知の情報を使用する。

1841 攻撃者が潜在的脆弱性を悪用するために必要とする攻撃能力が大幅に低減されたことを評価者が把握した場合を除いて、基本コンポーネントの評価より前に公開の場で利用可能であった潜在的脆弱性の調査をそれ以上進める必要はない。これは、基本コンポーネント評価以降何らかの新しい技術が導入され、潜在的脆弱性の悪用が単純になっている可能性がある。

ACO_VUL.2-6 評価者は、依存コンポーネントの評価の完了以降に知られることになった、依存コンポーネントで発生する可能性があるセキュリティ脆弱性の識別をサポートするために公開の場で利用できる情報源を***検査しなければならない。***

1842 評価者は、依存コンポーネントの脆弱性を探索するために、AVA_VAN.2-2 の記述に従って、公知の情報を使用する。

1843 攻撃者が潜在的脆弱性を悪用するために必要とする攻撃能力が大幅に低減されたことを評価者が把握した場合を除いて、依存コンポーネントの評価より前に公開の場で利用可能であった潜在的脆弱性の調査をそれ以上進める必要はない。これは、依存コンポーネント評価以降、何らかの新しい技術が導入され、潜在的脆弱性の悪用が単純になっている可能性がある。

ACO_VUL.2-7 評価者は、ETR 内で、テストの候補となり、運用環境の統合 TOE に適用できる識別された潜在的なセキュリティ脆弱性を***記録しなければならない。***

1844 脆弱性が運用環境の統合 TOE に関連しているかどうかを決定するために、ST、ガイダンス証拠資料、及び機能仕様が使用される。

1845 評価者が運用環境で脆弱性が該当しないことを決定する場合、評価者は、それ以上の考慮から脆弱性を除外する理由を記録する。それ以外の場合は、評価者は、さらに考慮する対象となる潜在的な脆弱性を記録する。

1846 運用環境の統合 TOE に該当する潜在的脆弱性のリストは、侵入テストアクティビティ(つまり、ACO_VUL.2.5E)に対する入力として使用でき、評価者が ETR で報告しなければならない。

17.7.2.7 アクション ACO_VUL.2.4E

ACO_VUL.2-8 評価者は、統合 TOE で発生する可能性があるセキュリティ脆弱性を識別するために、統合 TOE の ST、ガイダンス証拠資料、依存情報、及び統合の根拠の探索を***実施しなければならない。***

1847 独立評価者脆弱性分析で統合 TOE のコンポーネントを考慮する形態は、コンポーネント評価について AVA_VAN.2.3E で証拠資料として提出されている考慮の形態と若干異なる。これは、保証パッケージに関連する設計の抽象の階層が必ずしもすべて考慮されないからである。これらの階層はコンポーネントの評価中にすでに考慮されているが、その証拠を統合 TOE 評価で利用できない可能性がある。ただし、AVA_VAN.2.3E に関連するワークユニットに記述されている一般的な手法は適用可能で、評価者による統合 TOE の潜在的脆弱性の探索はこの手法に基づくべきである。

1848 統合 TOE で使用される個々のコンポーネントの脆弱性分析は、個々のコンポーネントの評価中にすでに実行されている。統合 TOE の評価中における脆弱性分析の焦点は、コンポーネントの統合の結果として生じた脆弱性や、評価コンポーネント構成と統合 TOE 構成の間でコンポーネントの使用方法が変更されたために生じた脆弱性を識別することである。

1849 評価者は、依存コンポーネントの依存情報で詳述されているコンポーネントの構造、基本コンポーネントの開発情報と統合の根拠、及び依存コンポーネントの設計情報に関する知識を使用する。評価者は、この情報から基本コンポーネントと依存コンポーネントがどのように相互作用するかを理解し、この相互作用の結果生じる可能性がある潜在的脆弱性を識別する。

1850 評価者は、統合 TOE の設置、立上げ、及び運用のために提供されている新しいガイダンスを考慮して、この改訂後のガイダンスを通じてもたらされる潜在的脆弱性を識別する。

1851 個々のコンポーネントのいずれかに対し、コンポーネントの評価の完了以降に保証継続アクティビティが実行されている場合、評価者は独立脆弱性分析でパッチを考慮する。保証継続アクティビティの公開報告書(例えば、保守報告書)に示されている変更関連情報は、変更の入力資料の主な情報源となる。この情報は、変更によって発生するガイダンス証拠資料の更新、及びベンダの web サイトなどで公知となっている変更関連情報によって補足される。

1852 パッチ、またはコンポーネントの構成における評価構成からの逸脱について、そのすべての影響を確立する証拠を欠くことに起因して識別されるリスクは、評価者の脆弱性分析で証拠資料として提出される。

17.7.2.8 アクション ACO_VUL.2.5E

ACO_VUL.2-9 評価者は、AVA_VAN.2.4E で詳述されているように、侵入テストを***実施しなければならない。***

1853 評価者は、評価者アクション AVA_VAN.2.4E を満たすために必要なすべてのワークユニットを適用して、それらのワークユニットで指示されている統合 TOE のすべての分析及び判定について ETR に報告する。

1854 また評価者は、開発者から提供された統合 TOE がテストに適していることを決定するために、評価者アクション AVA_VAN.2.1E のワークユニットを適用する。

17.7.3 サブアクティビティの評価(ACO_VUL.3)

17.7.3.1 目的

1855 このサブアクティビティの目的は、統合 TOE が、その運用環境において、強化基本的な攻撃能力を持つ攻撃者が悪用できる脆弱性を持つかどうかを決定することである。

1856 開発者は、コンポーネントについて報告された残存脆弱性、及び基本コンポーネントと依存コンポーネントの組み合わせを通じてもたらされた脆弱性について、処置の分析を提供する。評価者は、コンポーネントの新たな潜在的脆弱性(つまり、コンポーネント評価の完了以降に公知として報告された問題)を識別するために、公知になっているものの探索を実行する。評価者は、統合 TOE の独立脆弱性分析及び侵入テストも実行する。

17.7.3.2 入力

1857 このサブアクティビティ用の評価証拠は、次のとおりである:

a) テストに適した統合 TOE;

b) 統合 ST;

c) 統合の根拠;

d) 依存情報;

e) ガイダンス証拠資料;

f) 発生する可能性があるセキュリティ脆弱性の識別をサポートするために公開の場で利用できる情報;

g) 各コンポーネントの評価中に報告された残存脆弱性。

17.7.3.3 **適用上の注釈**

1858 サブアクティビティの評価(AVA_VAN.3)の適用上の注釈を参照のこと。

17.7.3.4 **アクション** ACO_VUL.3.1E

ACO_VUL.3.1C ***統合 TOE は、テストに適していなければならない。***

ACO_VUL.3-1 評価者は、統合 TOE が適切に設置され、定義された状態にあることを決定するために、その TOE を***検査しなければならない。***

1859 統合 TOE が適切に設置され、定義された状態にあることを決定するために、その統合 TOE に ATE_IND.2-1 及び ATE_IND.2-2 ワークユニットが適用される。

1860 保証パッケージに ACO_CTT ファミリが含まれる場合、評価者はこれが満たされていることを実証するために、ワークユニット統合 TOE テスト(ACO_CTT)*-1 の結果を参照することができる。

ACO_VUL.3-2 評価者は、IT エンティティに関連するコンポーネントの ST における前提条件と対策方針が、他のコンポーネントによって満たされることを決定するために、統合 TOE の構成を***検査しなければならない。***

1861 コンポーネントの ST には、ST により関連付けられる、そのコンポーネントを使用する可能性がある他のコンポーネントについての前提条件が含まれている場合がある。例えば、基本コンポーネントとして使用されるオペレーティングシステムの ST には、オペレーティングシステムにロードされるアプリケーションが特権モードで実行されないという前提条件が含まれる可能性がある。これらの前提条件及び対策方針は、統合 TOE の他のコンポーネントによって満たされる。

17.7.3.5 **アクション** ACO_VUL.3.2E

ACO_VUL.3-3 評価者は、基本コンポーネント評価からの残存脆弱性が運用環境の統合 TOE で悪用される可能性がないことを決定するために、それらの残存脆弱性を***検査しなければならない。***

1862 基本コンポーネントの評価中に製品で識別され、基本コンポーネントで悪用不能であることを実証された脆弱性のリストは、このアクティビティへの入力として使用される。評価者は、脆弱性が悪用不能であるとみなされたときの前提が統合 TOE で維持されていること、あるいは組み合わせによって潜在的脆弱性が再びもたらされたかどうかを決定する。例えば、基本コンポーネントの評価中に特定のオペレーティングシステムサービスが無効にされていることが想定される場合に、そのサービスが統合 TOE 評価で有効にされているときは、以前に調べたそのサービスに関連する潜在的脆弱性をここで考慮するべきである。

1863 また、基本コンポーネントの評価で判明した既知の悪用不能脆弱性のこのリストを、統合 TOE 内の他のコンポーネント(例えば、依存コンポーネント)の既知の悪用不能脆弱性に照らして考慮するべきである。これは、単独では悪用不能な潜在的脆弱性が、別の潜在的脆弱性を含んでいる IT エンティティと統合されたときに悪用可能となる場合を考慮するためである。

ACO_VUL.3-4 評価者は、依存コンポーネント評価からの残存脆弱性が運用環境の統合 TOE で悪用される可能性がないことを決定するために、それらの残存脆弱性を***検査しなければならない。***

1864 依存コンポーネントの評価中に製品で識別され、依存コンポーネントで悪用不能であることを実証された脆弱性のリストは、このアクティビティへの入力として使用される。評価者は、脆弱性が悪用不能であるとみなされたときの前提が統合 TOE で維持されていること、あるいは組み合わせによって潜在的脆弱性が再びもたらされたかどうかを決定する。例えば、依存コンポーネントの評価中に運用環境の要件を満たしている IT からサービス要求への応答として特定の値が返されないことが想定される場合に、統合 TOE の評価で基本コンポーネントからその値が提供されるときは、以前に調べたその戻り値に関連する潜在的脆弱性をここで考慮するべきである。

1865 また、依存コンポーネントの評価で判明した既知の悪用不能脆弱性のこのリストを、統合 TOE 内の他のコンポーネント(例えば、基本コンポーネント)の既知の悪用不能脆弱性に照らして考慮するべきである。これは、単独では悪用不能な潜在的脆弱性が、別の潜在的脆弱性を含んでいる IT エンティティと統合されたときに悪用可能となる場合を考慮するためである。

17.7.3.6 **アクション** ACO_VUL.3.3E

ACO_VUL.3-5 評価者は、基本コンポーネントの評価の完了以降に知られることになった、基本コンポーネントで発生する可能性があるセキュリティ脆弱性の識別をサポートするために公開の場で利用できる情報源を**検査しなければならない**。

1866 評価者は、基本コンポーネントの脆弱性を探索するために、AVA_VAN.3-2 の記述に従って、公知の情報を使用する。

1867 攻撃者が潜在的脆弱性を悪用するために必要とする攻撃能力が大幅に低減されたことを評価者が把握した場合を除いて、基本コンポーネントの評価より前に公開の場で利用可能であった潜在的脆弱性の調査をそれ以上進める必要はない。これは、基本コンポーネント評価以降何らかの新しい技術が導入され、潜在的脆弱性の悪用が単純になっている可能性がある。

ACO_VUL.3-6 評価者は、依存コンポーネントの評価の完了以降に知られることになった、依存コンポーネントで発生する可能性があるセキュリティ脆弱性の識別をサポートするために公開の場で利用できる情報源を***検査しなければならない。***

1868 評価者は、依存コンポーネントの脆弱性を探索するために、AVA_VAN.3-2 の記述に従って、公知の情報を使用する。

1869 攻撃者が潜在的脆弱性を悪用するために必要とする攻撃能力が大幅に低減されたことを評価者が把握した場合を除いて、依存コンポーネントの評価より前に公開の場で利用可能であった潜在的脆弱性の調査をそれ以上進める必要はない。これは、依存コンポーネント評価以降何らかの新しい技術が導入され、潜在的脆弱性の悪用が単純になっている可能性がある。

ACO_VUL.3-7 評価者は、ETR 内で、テストの候補となり、運用環境の統合 TOE に適用できる識別された潜在的なセキュリティ脆弱性を***記録しなければならない。***

1870 脆弱性が運用環境の統合 TOE に関連しているかどうかを決定するために、ST、ガイダンス証拠資料、及び機能仕様が使用される。

1871 評価者が運用環境で脆弱性が該当しないことを決定する場合、評価者は、それ以上の考慮から脆弱性を除外する理由を記録する。それ以外の場合は、評価者は、さらに考慮する対象となる潜在的な脆弱性を記録する。

1872 運用環境の統合 TOE に該当する潜在的脆弱性のリストは、侵入テストアクティビティ(つまり、ACO_VUL.3.5E)に対する入力として使用することができ、評価者が ETR で報告しなければならない。

17.7.3.7 アクション ACO_VUL.3.4E

ACO_VUL.3-8 評価者は、統合 TOE で発生する可能性があるセキュリティ脆弱性を識別するために、統合 TOE の ST、ガイダンス証拠資料、依存情報、及び統合の根拠の探索を***実施しなければならない。***

1873 独立評価者脆弱性分析でコンポーネントを考慮する形態は、コンポーネント評価について AVA_VAN.3.3E で証拠資料として提出されている考慮の形態と若干異なる。これは、保証パッケージに関連する設計の抽象の階層が必ずしもすべて考慮されないからである。これらの階層は基本コンポーネントの評価中にすでに考慮されているが、その証拠を統合 TOE 評価で利用できない可能性がある。ただし、AVA_VAN.3.3E に関連するワークユニットに記述されている一般的な手法は適用可能で、評価者による統合 TOE の潜在的脆弱性の探索はこの手法に基づくべきである。

1874 統合 TOE で使用される個々のコンポーネントの脆弱性分析は、そのコンポーネントの評価中にすでに実行されている。統合 TOE の評価中における脆弱性分析の焦点は、コンポーネントの統合の結果として生じた脆弱性や、コンポーネントの評価中に決定されたコンポーネントの構成と統合 TOE 構成の間でコンポーネントの使用方法が変更されたために生じた脆弱性を識別することである。

1875 評価者は、依存コンポーネントの依存情報で詳述されているコンポーネントの構造、基本コンポーネントの統合の根拠と開発情報、及び依存コンポーネントの設計情報に関する知識を使用する。評価者は、この情報から基本コンポーネントと依存コンポーネントがどのように相互作用するかを理解する。

1876 評価者は、統合 TOE の設置、立上げ、及び運用のために提供されている新しいガイダンスを考慮して、この改訂後のガイダンスを通じてもたらされる潜在的脆弱性を識別する。

1877 個々のコンポーネントのいずれかに対し、コンポーネント評価の完了以降に保証継続アクティビティが実行されている場合、評価者は独立脆弱性分析でパッチを考慮する。保証継続アクティビティの公開報告書(例えば、保守報告書)に示されている変更関連情報。この情報は、変更によって発生するガイダンス証拠資料の更新、及びベンダの web サイトなどで公知となっている変更関連情報によって補足される。

1878 パッチ、またはコンポーネントの構成における評価構成からの逸脱について、そのすべての影響を確立する証拠を欠くことに起因して識別されるリスクは、評価者の脆弱性分析で証拠資料として提出される。

17.7.3.8 アクション ACO_VUL.3.5E

ACO_VUL.3-9 評価者は、AVA_VAN.3.4E で詳述されているように、侵入テストを***実施しなければならない。***

1879 評価者は、評価者アクション AVA_VAN.3.4E を満たすために必要なすべてのワークユニットを適用して、それらのワークユニットで指示されている統合 TOE のすべての分析及び判定について ETR に報告する。

1880 また評価者は、開発者から提供された統合 TOE がテストに適していることを決定するために、評価者アクション AVA_VAN.3.1E のワークユニットを適用する。

附属書A　一般的評価ガイダンス

（規定）

A.1　目的

1881　この章の目的は、評価結果の技術的証拠を提供するために使用される一般的なガイダンスを扱うことである。そのような一般的ガイダンスの使用は、評価者が行う作業の目的、反復性及び再現性を達成するのに役に立つ。

A.2　サンプリング

1882　この節は、サンプリングの一般的なガイダンスを提供する。サンプリングを行う必要がある特定の評価者アクション要素のそれらのワークユニットに特定の詳細な情報が示されている。

1883　サンプリングは、評価証拠の必要なセットのいくつかのサブセットを検査し、それらが全体のセットを表していると仮定する、評価者の定義された手順である。評価者は、全体の証拠を分析せずに特定の評価証拠が正しいことを十分に確信することができる。サンプリングの理由は、保証の適切なレベルを維持しながら資源を節約することである。証拠のサンプリングは、次の 2 つの可能な結果を提供することができる。

a)　サブセットが誤りを示さない場合、評価者は、セット全体が正しいことを確信できる。

b)　サブセットが誤りを示す場合、セット全体の正当性が疑問視される。発見されたすべての誤りを解決するだけでは、評価者に必要な確信を与えるのに十分ではなく、その結果、評価者は、サブセットのサイズを増やすか、この特定の証拠のサンプリングの使用を停止する必要がある。

1884　サンプリングは、証拠のセットが、本質的に比較的同質である、例えば、証拠が明確に定義されたプロセスで作成されている場合、信頼できる結論に達するために使用できる技法である。

1885　CC に識別されている場合のサンプリング、CEM ワーク要素で明確に扱われている場合のサンプリングは、評価者アクションを実行するための費用効果の高い手法として認識される。その他の領域でのサンプリングは、特定のアクティビティを全部通して実行することが、他の評価アクティビティと不釣り合いな労力を要求し、そして、これがそれ相応の保証を追加しないような、例外的な場合にのみ許される。このような場合、その領域でのサンプリングの使用の根拠を示す必要がある。大きく複雑な TOE 評価には、さらに多くの労力を必要とすることが当然であるために、TOE が大きく複雑であること、またそれが多くのセキュリティ機能要件を持つことは、十分な根拠とならない。むしろ、この例外は、TOE 開発手法が、特定の CC 要件に対して多量の資料をもたらし、通常はそれをすべてチェックまたは検査する必要があるが、そのようなアクションがそれ相応に保証を高めることが期待されないような場合に制限されることを意図している。

1886　サンプリングは、TOE のセキュリティ対策方針と脅威への考えられる影響を考慮して、正当化する必要がある。その影響は、サンプリングの結果として除かれるものに依存する。サンプリングされる証拠の性質、及びセキュリティ機能を縮小または無視しないとの要件も考慮する必要がある。

1887 TOE の実装に直接関係する証拠(例えば、開発者のテスト結果)のサンプリングは、プロセスが守られているかどうかを決定することに関係するサンプリングと異なる手法を必要とすることが認識されるべきである。多くの場合、評価者は、プロセスが守られていること、サンプリング方策が推奨されていることを決定する必要がある。開発者のテスト結果をサンプリングするための手法は異なる。その理由は、前者のケースは、プロセスが適切であることを保証することに関係し、後者は、TOE が正しく実装されていることを決定することに関係するためである。一般的に、プロセスが適切であることを保証するために必要となるものより大きなサンプルサイズが、TOE の正しい実装に関係する場合に分析されるべきである。

1888 評価者が、開発者テストの繰返しに、より大きな重点を置くことが適切な場合がある。例えば、評価者に実行が任されている独立テストと、広範な開発者テストセットに含まれるテストの間に、表面的な違いしか見られない場合(開発者がカバレージ(ATE_COV)と深さ(ATE_DPT)の基準を満たすために必要以上のテストを実行したことが原因と考えられる)は、評価者が開発者テストの繰返しに、より焦点を絞ることが適切となる。これは、必ずしも開発テストを繰返すために比率の高いサンプルが必要となることを意味しないので注意のこと。事実、広範な開発者テストセットが提供されることで、評価者は比率の低いサンプルを正当化することができる。

1889 開発者が自動化されたテストスイートを使用して機能テストを実行した場合は、一般に、開発者テストのサンプルのみを繰返すよりも、テストスイート全体を再実行する方が評価者にとって簡単である。ただし、評価者には、自動テストの結果が誤っていないことをチェックする義務が生じる。この場合、一部のテストを他のテストより優先して選び、十分なサンプルサイズを保証するための原則を等しく適用して、このチェックを自動テストスイートのサンプルに対して実行する必要があることを意味している。

1890 サンプリングが実行されるときは、常に次の原則が守られるべきである:

a) サンプリングはランダムに行うのではなく、すべての証拠の代表となるように選択されるべきである。サンプルのサイズと構成は、常に正当化されなければならない。

b) サンプリングが TOE の正しい実装に関係している場合、サンプルは、サンプリングされる領域に関係するすべての局面の代表であるべきである。特に、選択は、各種のコンポーネント、インタフェース、開発者及び運用サイト(複数ある場合)、及びハードウェアプラットフォームのタイプ(複数ある場合)をカバーするべきである。サンプルサイズは、評価の費用効果と釣り合うべきであり、TOE に依存する要因(例えば、TOE のサイズと複雑性、証拠資料の量)の総数に依存する。

c) 開発者テストが繰返し可能であり、再現可能であるという証拠を具体的に得ることにサンプリングが関係している場合、使用されるサンプルは、開発者テストのすべての明確な局面(さまざまなテスト体制など)を表すために十分でなければならない。使用されるサンプルは、開発者の機能テストプロセスにおける系統的な問題を検出するために十分でなければならない。開発者テストの繰返しと独立テストの実行を組み合わせることによる評価者の貢献は、TOE の主要な留意事項に対処するために十分でなければならない。

d) サンプリングが、プロセス(例えば、訪問者の管理または設計レビュー)が守られている証拠を得ることに関係する場合、評価者は、手順が守られているという納得のいく確信を得るために十分な情報をサンプリングするべきである。

e) スポンサーと開発者にはサンプルの正確な構成が事前に知らされるべきでないが、これはサンプル及びサポート用提供物件、例えば、テストハーネス(test harness)と機器の、評価スケジュールに従った評価者へのタイムリな配付が保証されることを条件とする。

f) サンプルの選択には、可能な範囲で偏りをもつべきでない（常に最初または最後の要素を選択するべきでない）。理想的には、サンプルの選択は、評価者以外の者が行うべきである。

1891 サンプルに見つかる誤りは、系統的または散発的のいずれかに分類することができる。誤りが系統的である場合、問題を修正し、完全に新しいサンプルが使用されるべきである。適切に説明される場合、散発的誤りは、説明が確認されるべきであるが、新しいサンプルを必要とせずに解決することができる。評価者は、サンプルサイズを増やすかまたは別のサンプルを使用するかの決定において判定を使用するべきである。

A.3 依存性

1892 一般的に、必要となる評価アクティビティ、サブアクティビティ、及びアクションは、任意の順序でまたは並行して行うことができる。ただし、評価者が考慮する必要がある異なる種類の依存性が存在する。この節は、異なるアクティビティ、サブアクティビティ、及びアクションの間の依存性の一般的ガイダンスを提供する。

A.3.1 アクティビティの間の依存性

1893 場合によっては、異なる保証クラスが関係するアクティビティのシーケンスを推奨するかまたはそれを必要とすることもある。特定の具体例は、ST アクティビティである。ST は TOE 評価アクティビティを実行するための基礎と状況を提供するので、ST 評価アクティビティは、これらのアクティビティの前に開始される。ただし、ST 評価の最終的判定は、TOE 評価中のアクティビティによる検出によって ST に変更が加えられる可能性があるため、TOE 評価が完了するまで可能ではない。

A.3.2 サブアクティビティの間の依存性

1894 CC パート3のコンポーネント間で識別された依存性を、評価者は考慮する必要がある。ほとんどの依存性は、サブアクティビティの評価(AVA_VAN.1)がサブアクティビティの評価(ADV_FSP.1)及びサブアクティビティの評価(AGD_OPE.1)に対する依存性を主張するなど、一方向のものである。相互の依存性の例も存在し、その場合、両方のコンポーネントが互いに依存する。この一例が、サブアクティビティの評価(ATE_FUN.1)及びサブアクティビティの評価(ATE_COV.1)である。

1895 サブアクティビティには、それが一方向に依存するサブアクティビティがすべて成功裏に完了した場合にのみ、通常、合格判定を割り付けることができる。例えば、サブアクティビティの評価(AVA_VAN.1)に対する合格判定は、通常、サブアクティビティの評価(ADV_FSP.1)及びサブアクティビティの評価(AGD_OPE.1)に関連するサブアクティビティにも合格判定が割り付けられている場合にのみに割り付けることができる。相互依存の場合、これらのコンポーネントの順序は、どのサブアクティビティを最初に実行するかを決定する評価者によって決められる。これは、合格判定は、通常、両方のサブアクティビティが成功した場合にのみ割り付けることができることを示すことに注意のこと。

1896 そこで、サブアクティビティが他のサブアクティビティに影響するかどうかを決定するとき、評価者は、このアクティビティが、いずれかの従属サブアクティビティからの考えられる評価結果に依存するかどうかを考慮するべきである。実際、従属サブアクティビティがこのサブアクティビティに影響し、すでに完了している評価者アクションを再度行わなければならないことがある。

1897 重要な依存性の影響は、評価者が欠陥を検出した場合に起きる。1 つのサブアクティビティを実行した結果、欠陥が識別される場合、従属サブアクティビティへ合格判定を割り付けることは、それが依存するサブアクティビティに関係するすべての欠陥が解決されるまで、可能ではない。

A.3.3 アクションの間の依存性

1898 あるアクション中に評価者によって生成された結果が他のアクションを行うために使用される場合がある。例えば、完全性と一貫性に対するアクションは、内容・提示のチェックが完了するまで、完了することができない。これは、例えば、PP/ST の構成部分を評価した後で、評価者が PP/ST の根拠を評価することを推奨されることを意味する。

A.4 サイト訪問

A.4.1 序説

1899 保証クラスALCには以下に対する要件が含まれる。

a) TOE の完全性が保護されるようにするための構成管理の適用;

b) TOE が提供するセキュリティ保護が利用者への転送中に損なわれないようにするための、TOE のセキュアな配付にかかわる手段、手続き、及び標準;

c) 開発環境を保護するために使用されるセキュリティ手段。

1900 開発サイトを訪問することは、手続きが証拠資料に記述されているのと一貫した方法で守られていることを、評価者が決定するときに役に立つ手段である。

1901 サイトを訪問する理由には次のものがある:

a) CM システムが CM 計画に記述されているとおりに使用されていることを観察するため;

b) 配付手続きが配付証拠資料に記述されているとおりに実際に適用されていることを観察するため;

c) TOE の開発及び保守中に、開発セキュリティ証拠資料の記述どおりにセキュリティ手段が適用されていることを観察するため。

1902 特定及び詳細な情報が、次のサイト訪問が行われるアクティビティのワークユニットに示されている:

a) CM 能力(ALC_CMC).n(n>=3 とする)(特にワークユニット ALC_CMC.3-10 = ALC_CMC.4-13 = ALC_CMC.5-19);

b) 配付(ALC_DEL)(特にワークユニット ALC_DEL.1-2);

c) 開発セキュリティ(ALC_DVS)(特にワークユニット ALC_DVS.1-3 = ALC_DVS.2-4)。

A.4.2 一般的な手法

1903 評価の途中で、多くの場合、評価者が開発者に何度か会うことが必要となる。費用を削減するために、サイト訪問を他の打合せと組み合わせることは優れた計画を行う上での提案である。例えば、構成管理のため、開発者のセキュリティのため、及び配付のためのサイト訪問を組み合わせることができる。すべての開発フェーズをチェックするために、同じサイトを何度も訪問することが必要となることもある。開発は、1 つの建物内の複数の施設、同じサイトの複数の建物、または複数のサイトで行われる可能性があることが考慮されるべきである。

1904 最初の訪問は、評価の早い段階でスケジュールされるべきである。評価が TOE の開発フェーズ中に開始される場合、必要に応じて、修正アクションを取ることができる。評価が TOE の開発後に開始される場合、早い段階でサイト訪問を行うと、適用される手続きに重大な欠陥が現れた場合に修正処置を講じることが可能となる。これにより、不要な評価労力を避けることができる。

1905 インタビューも、記述されている手続きが、行われている事を反映しているかどうかを決定するための有効な手段である。そのようなインタビューを行うとき、評価者は、分析される開発サイトでの手続き、それらが実際にどのように使用されるか、及びそれらが提供された評価証拠に記述されているとおりに適用されているかどうかを深く理解することを目的とする。そのようなインタビューは、補足であり、評価証拠の検査に置き換えるものではない。

1906 サイト訪問を準備する最初のステップとして、評価者は保証クラスALCに関する評価者ワークユニットを、サイト訪問の結果について記述している側面を除いて実行するべきである。関連する開発者証拠資料によって提供される情報、及びこの証拠資料で回答が得られなかった未解決の質問に基づいて、評価者は、サイト訪問で解決する必要がある質問のチェックリストをまとめる。

1907 ALCクラスとチェックリストに関する評価レポートの最初のバージョンは、サイト訪問に関して評価監督機関に相談するための入力となる。

1908 チェックリストは、サイト訪問の際に、関連する手段、その適用、及び結果の検査によって、また、インタビューによって回答が得られる質問がどれであるかの指針となる。該当する場合は、必要なレベルの信頼を得るためにサンプリングが使用される(A.2 節を参照のこと)。

1909 サイト訪問の結果は記録され、保証クラスALCに関する評価レポートの最終バージョンの入力となる。

1910 信頼を得るための他の手法が、同等レベルの保証を提供するよう考慮されるべきである(例えば、評価証拠を分析するなど)。訪問を行わないという決定はいずれも、評価監督機関と相談して行われるべきである。適切なセキュリティ基準と方法は、情報セキュリティ管理システム領域の他の標準に基づくべきである。

A.4.3 チェックリストの準備のためのオリエンテーションガイド

1911 以下では、監査の際にチェックされるべきトピックについて、いくつかのキーワードが示されている。

A.4.3.1 構成管理の側面

1912 基本

- 構成リストの項目。TOE、ソースコード、実行時ライブラリ、設計証拠資料、開発ツールを含む(ALC_CMC.3-8)。

- TOE のさまざまなバージョンに対する設計証拠資料、ソースコード、利用者ガイダンスの追跡。

- 設計及び開発プロセス、テスト計画、テスト分析、品質管理の各手続きにおける構成システムの統合。

1913 テスト分析

- TOE の特定の構成とバージョンに対するテスト計画と結果の追跡。

1914 開発システムに対するアクセス制御

- アクセス制御とログに関する方針。

- プロジェクト固有のアクセス権の割付と変更に関する方針。

1915 取扱許可

- 顧客に対する TOE 及び利用者ガイダンスの取扱許可に関する方針。

- 展開前のコンポーネント及び TOE のテストと承認に関する方針。

A.4.3.2 開発セキュリティの側面

1916 インフラストラクチャ

- 開発サイトへの物理的なアクセス制御のためのセキュリティ手段、及びそれらの手段の有効性に関する根拠。

1917 組織的手段

- 開発環境のセキュリティに関する会社の組織構造。

- 開発、製造、テスト、及び品質保証の組織的な分離。

1918 人的な手段

- 開発セキュリティに関する人員の教育手段。

- 内部情報の非公開の手段と法的合意。

1919 アクセス制御

- セキュアなオブジェクト(例えば、TOE、ソースコード、実行時ライブラリ、設計証拠資料、開発ツール、利用者ガイダンス)及びセキュリティ方針の割付。

- アクセス制御及び認証情報の取り扱いに関する方針と責任。

- 開発サイトへのあらゆる種類のアクセスのログ及びログデータの保護に関する方針。

1920 データの入力、処理、及び出力

- 出力及び出力装置(プリンタ、プロッタ、及びディスプレイ)に対するセキュリティ手段。
- ローカルネットワーク及び通信接続のセキュリティ保護。

1921 文書及びデータ媒体の保管、移送、及び破棄

- 文書及びデータ媒体の取り扱いに関する方針。
- 選別された文書の破棄及びそれらの事象のログに関する方針と責任。

1922 データ保護

- データ及び情報の保護に関する方針と責任(例えば、バックアップの実行など)。

1923 危機管理計画

- 緊急時の対応と責任。
- アクセス制御に関する危機管理手段の証拠資料。
- 極端なケースでの保護における適切な対応に関する人員の情報(例えば、バックアップの実行など)。

A.4.4 チェックリストの例

1924 サイト訪問用チェックリストの例は、監査を準備するための表及び監査の結果を提示するための表で構成される。

1925 以下に示すチェックリスト構造は、準備段階のものである。新たな指針の具体的な内容に応じて、変更が必要になる場合がある。

1926 チェックリストは、序説(A.4.1 節)で示されたサブジェクトに従って 3 つのセクションに分割される。

a) 構成管理システム。

b) 配付手続き。

c) 開発中のセキュリティ手段。

1927 これらのセクションは、実際の CC クラスALC、特に CM 能力(ALC_CMC)。n(n>=3 とする)、配付(ALC_DEL)、開発セキュリティ(ALS_DVS)の各ファミリに対応する。

1928 これらのセクションは、さらに CEM の関連するワークユニットに対応する行に分割される。

1929 チェックリストの列には次のものが含まれる。

- 連続する番号、
- 参照されるワークユニット、
- 対応する開発者証拠資料への参照、
- 開発者手段の明示的な再現、

- 訪問時に明確にされる特別な注釈と質問(示された手段の適用を検証する標準評価者タスクの範囲を超える)、

- 訪問中の検査の結果。

1930 監査の準備及び報告用に個別のチェックリストを作成する場合は、準備用リストで結果の列が省略され、報告用リストで注釈と質問の列が省略される。それ以外の列は、両方のリストで同一であるべきである。

表 1　EAL 4 でのチェックリストの例(抜粋)

A. CM システムの検査(ALC_CMC.4及びALC_CMS.4)					
番号	ワーク ユニット	開発者 証拠資料	手段	質問と注釈	結果
A.1	ALC_CMC. 4-11、 ALC_CMC. 4-12	「構成管理 システム」、 第 x 章...	ソースコードファイルを自動管理するシステムで、利用者プロファイル及び段階的なアクセス権を管理し、利用者の識別情報と認証をチェックすることができる。	ソースコードファイルの読み取りまたは更新に、利用者認証が必要か。	利用者に機密文書へのアクセス権がない場合、その利用者にはファイルリストにその文書さえ表示されない。
...	...	...	...	...	...
B. 配付手続きの検査(ALC_DEL.1)					
番号	ワーク ユニット	開発者 証拠資料	手段	質問と注釈	結果
B.1	ALC_DEL. 1-1、 ALC_DEL. 1-2	「TOE の 配付」 第 x 章...	ソフトウェアは、PGP で署名され、暗号化されて顧客に送信される。	---	評価者は、プロセスをチェックし、記述どおりであり、さらにチェックサムも送信されることを確認した。
...	...	...	...	...	...
C. 組織及びインフラストラクチャの開発者セキュリティの検査 (ALC_DVS.1、ALC_LCD.1、ALC_TAT.1)					
番号	ワーク ユニット	開発者 証拠資料	手段	質問と注釈	結果
C.1	ALC_DVS. 1-1、 ALC_DVS. 1-2	「開発環境 のセキュリ ティ」第 x 章...(構内)	構内はセキュリティフェンスで保護されている。	フェンスは構内への簡単な侵入を阻止できるだけの十分な強度と高さを備えているか。	評価者は、フェンスの強度と高さが十分であるとみなした。
C.2	ALC_DVS. 1-1、 ALC_DVS. 1-2	「開発環境 のセキュリ ティ」第 x 章...(建物)	建物にアクセスする可能性には次のものがある。受付から見渡すことが可能で、受付に人がいないときには閉鎖されるメインエントランス。及び 2 枚のローラーシャッターで保護されている商品受付へのアクセス。	アクセスの可能性はそれですべてか。	示されているアクセスの可能性以外に、外部から開けることのできない非常用出口がある。前述のローラーシャッターは、内部からしか操作できない。
...	...		...	...	...

A.5 制度の責任

1931 この CEM は、監督（制度）機関のもとで行われる評価が行わなければならない最小限の技術的作業を記述している。ただし、評価結果の相互認識が依存しないアクティビティまたは方式が存在することも（明示的及び暗黙の両方で）認識している。完全であり明確であるため、及び CEM の適用が終わり、個別の制度の方法の適用すべき箇所の始まりをより詳細に示すために、次のことが制度の自由裁量に任されている。制度は、次のものを提供することを選択することができるが、特定しないでおくことを選択することもできる(このリストが完全なものになるようにあらゆる努力がなされてきた。ここに示されてもいなければ CEM で取り扱われてもいないサブジェクトに出合った評価者は、サブジェクトの漏れを援助する制度のもとで決定するために、評価制度に相談するべきである)。

1932 制度が特定することを選択できるものには、次のものがある:

a) 評価が十分に行われたことを保証するために必要になるもの - 各制度は、明らかになったことを監督機関に提出することを評価者に要求するか、監督機関が評価者の作業を再度実行することを要求するか、またはすべての評価機関が適切であり、同等であることを制度に保証するその他の手段により、技術的有効性、作業の理解、及び評価者の作業を検証する手段を持っている;

b) 評価が完了したときに評価証拠を処分するためのプロセス;

c) 機密に対するあらゆる要件(評価者の責任、及び評価中に得られた情報の非暴露に対する);

d) 評価中に問題が検出されたときに取るべき一連のアクション(問題が解決された後、評価を続けるか、または評価を直ちに終了し、直された製品が評価のために再提出されなければならないかどうか);

e) 提供しなければならない証拠資料を記述する特定の(自然)言語;

f) ETR に提出しなければならない記録された証拠 － この CEM は、ETR に最低限報告する必要があるものを特定している。ただし、個々の制度は、追加の情報を含めることを要求することができる;

g) 評価者に要求される追加の報告(ETR 以外の) － 例えば、テスト報告;

h) 制度が要求する特定の OR、例えば、そのような OR の構造、受取人など;

i) ST 評価からの結果として記述される報告書の特定の内容の構造 － 制度には、評価の対象が TOE であっても ST であっても、評価結果を詳述するすべての報告用に特定の形式が存在する場合がある;

j) 必要な追加の PP/ST 識別情報;

k) ST に明示的に記述されている要件の適切さを決定するためのあらゆるアクティビティ;

l) 再評価及び再使用を支援する評価者証拠の提供のための要件;

m) 制度識別情報、ロゴ、商標などの特定の取り扱い;

n) 暗号を取り扱うための特定のガイダンス;

o) 制度の取り扱いと適用、国内と国際的な解釈;

p) テストが可能でないときのテストに代わる適切な代替手法のリストまたは特性;

q) テスト中に評価者が行ったステップを、評価監督機関が決定することができるメカニズム;

r) 望ましいテスト手法(存在する場合): 内部インタフェースまたは外部インタフェースにおける;

s) 評価者の脆弱性分析を行う受入れ可能な手段のリストまたは特性(例えば、欠陥仮説法);

t) 考慮する必要がある脆弱性と弱点に関する情報。

附属書B　脆弱性評定(AVA)
(参考)

1933　本附属書では、AVA_VAN基準の説明及びその適用の例を提供する。本附属書では、AVA基準の定義は行わない。定義は、CC パート3の「AVA クラス: 脆弱性評定」の節にある。

1934　本附属書は、次の 2 つの主要なパートから構成されている:

a) *独立脆弱性分析を完了するためのガイダンス*。これについては、B.1 節で概要を示し、B.2 節でより詳細に説明する。これらの節では、評価者が独立脆弱性分析の構成にどのように取り組むべきであるかを説明する。

b) 攻撃者の想定される攻撃能力の特性を表す方法、及びその攻撃能力の使用方法。これについては、B.3 節から B.5 節で説明する。これらの節では、攻撃能力の特性をどのように表すことができるか、及びその能力をどのように使用するべきであるかを説明し、例を示す。

B.1　脆弱性分析とは

1935　脆弱性評定アクティビティの目的は、運用環境での TOE の欠陥または弱点の存在と悪用される可能性を決定することである。この決定は、評価者が実行する分析に基づいており、評価者テストによりサポートされる。

1936　最も低いレベルの脆弱性分析(AVA_VAN)では、評価者が、公開の場で利用できる情報の検索を行って TOE の既知の弱点を識別する。一方、高いレベルでは、評価者が TOE 評価証拠の構造化された分析を実行する。

1937　脆弱性分析の実行には、次の 3 つの主要な要素がある:

a) 潜在的脆弱性の識別;

b) 識別された潜在的脆弱性が、関連する攻撃能力の攻撃者に、SFR を侵害する攻撃を許すかを決定する評価。

c) 識別された潜在的脆弱性が、TOE の運用環境で悪用される可能性があるかどうかを決定する侵入テスト。

1938　脆弱性の識別は、さらに、探索される証拠、及びその証拠を探索して潜在的脆弱性を識別する処理の困難性に分けることができる。同様に、侵入テストは、攻撃方法を識別するための潜在的脆弱性の分析、及びその攻撃方法の実証に分けることができる。

1939　これらの主要な要素には反復性がある。つまり、潜在的脆弱性の侵入テストが、さらなる潜在的脆弱性の識別につながることがある。このため、これらは単独の脆弱性分析アクティビティとして実行される。

B.2 脆弱性分析の評価者による構成

1940 評価者脆弱性分析の意図は、基本(AVA_VAN.1及びAVA_VAN.2)、強化基本(AVA_VAN.3)、中(AVA_VAN.4)、または高(AVA_VAN.5)のレベルの攻撃能力を持つ攻撃者の侵入攻撃に、TOE が耐え得るかどうかを決定することである。まず評価者は、識別されたすべての潜在的脆弱性について悪用の可能性を評定する。その手段として、侵入テストが用いられる。評価者は、TOE への侵入を試みる際に、基本(AVA_VAN.1及びAVA_VAN.2)、強化基本(AVA_VAN.3))、中(AVA_VAN.4)、または高(AVA_VAN.5)のレベルの攻撃能力を持つ攻撃者の役割を想定するべきである。

1941 評価者は、他の評価アクティビティの実施中に発見した潜在的脆弱性を考慮する。これらの潜在的脆弱性に TOE が耐え得るかどうかを決定する評価者侵入テストは、基本(AVA_VAN.1及びAVA_VAN.2)、強化基本(AVA_VAN.3)、中(AVA_VAN.4)、または高(AVA_VAN.5)のレベルの攻撃能力を持つ攻撃者の役割を想定しながら行うべきである。

1942 ただし、脆弱性分析は分離されたアクティビティとして実行されるべきではない。この分析は、ADV及びAGDと密接に関連する。評価者は、潜在的脆弱性または「関心の分野」の識別に重点をおいて、これらのその他の評価アクティビティを実行する。したがって、評価者は一般的な脆弱性に関するガイダンス(B.2.1 節で提供)を熟知している必要がある。

B.2.1 一般的な脆弱性に関するガイダンス

1943 次の 5 つのカテゴリで、一般的な脆弱性について解説する。

B.2.1.1 バイパス

1944 バイパスには、攻撃者が下記の方法でセキュリティの実施を回避できるあらゆる手段が含まれる:

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

b) 他の場合には拒否されるべき、権限またはその他の能力の継承;

c) (機密性が問題となる場合)保護が不十分な領域に格納またはコピーされた機密に関わるデータの読み取り。

1945 次の各事項が評価者の独立脆弱性分析で考慮されるべきである(該当する場合)。

a) インタフェースまたはユーティリティの機能を悪用する攻撃は、一般に、それらのインタフェースに必要なセキュリティが実施されていない点を利用する。例えば、アクセス制御の実施レベルよりも低いレベルで実施されている機能性にアクセスするケースが挙げられる。関連する要素には、次のものが含まれる:

1) 事前に定義された TSFI の呼び出し順序を変更する;

2) 追加の TSFI を呼び出す;

3) 期待しない状況または期待しない目的でコンポーネントを使用する;

4) あまり抽象的でない表現に導入されている実装詳細を使用する;

5) アクセスチェック時から使用時までの遅延を使用する。

b) 事前に定義されたコンポーネント呼び出し順序の変更は、TSFI を呼び出す(例えば、アクセスするためにファイルを開き、次にそこからデータを読み取る)ために TOE へのインタフェース(例えば、利用者コマンド)が呼び出される順序が予定されている場合に考慮されるべきである。TSFI が TOE のインタフェースの１つ(例えば、アクセス制御チェック)で呼び出される場合、評価者は、シーケンスの後の時点でコールを行うかまたはそれを一切省略することにより、制御をバイパスできるかどうかを考慮するべきである。

c) 追加コンポーネントの(事前に決められた順序の中での)実行は、前述と同様の攻撃形式であるが、その決められた順序のある時点で他の TOE インタフェースの呼び出しが行われる。また、ネットワークトラフィックアナライザを使用してネットワーク上で受け渡しされる機密に関わるデータの傍受による攻撃を含めることもできる(ここでの追加コンポーネントとはネットワークトラフィックアナライザ)。

d) 期待しない状況または期待しない目的でのコンポーネントの使用には、TSF をバイパスするために関係のない TOE インタフェースを使用して、達成が設計も意図もされていない目的を達成することが含まれる。隠れチャネルは、このタイプの攻撃の例である(隠れチャネルの詳細については、B.2.1.4 を参照のこと)。証拠資料に記述されていないインタフェース(安全でないかもしれない)の使用も、このカテゴリに含まれる。このようなインタフェースには、証拠資料に記述されていないサポートとヘルプ機能を含むことができる。

e) 下位表現に含められる実装詳細を使用する場合、攻撃者は、詳細化プロセスの結果、TOE にもたらされる追加の機能、資源または属性を悪用する可能性がある。追加の機能性は、ソフトウェアモジュールに含まれるテストハーネスコードと実装プロセス中に導入されるバックドアを含むこともできる。

f) チェック時から使用時までの遅延の使用には、次のシナリオが含まれる。アクセス制御チェックが行われてアクセスが許可されると、その後に、攻撃者は、アクセスチェックが行われた時点では適用されたチェックが働かない状況を作ることができる例としては、利用者が、機密性の高いデータを読み取って利用者端末に送信するバックグラウンドプロセスを作成し、その後にログアウトして再び低い機密レベルでログインする場合が挙げられる。利用者がログオフした時にバックグラウンドプロセスが終了しない場合は、MAC のチェックのバイパスが有効になるであろう。

g) 権限を継承することによる攻撃は、通常、制御されないまたは期待されない方法で特権を持つあるコンポーネントから抜けることにより、そのコンポーネントの権限または能力を不正に獲得することによって行われる。関連する要素には、次のものが含まれる:

1) 実行可能であることが意図されていないデータを実行する、またはデータを実行可能にする;

2) コンポーネントに期待しない入力を生成する;

3) 下位レベルコンポーネントがある前提条件及び特性に依存する場合、それらを無効にする。

h) 実行可能であることが意図されていないデータを実行するか、またはデータを実行可能にすることには、ウイルスが関係する攻撃が含まれる(例えば、ファイルが編集またはアクセスされるときに自動的に実行される実行可能コードまたはコマンドをファイルに入れ、ファイルの所有者が持つ権限を継承する)。

i) コンポーネントに期待されない入力を生成することは、攻撃者が悪用できる予期しない影響を与えることができる。例えば、利用者が下層のオペレーティングシステムにアクセスする場合に TSF のバイパスが可能であると、パスワードが認証されている間に各種の制御またはエスケープシーケンスを押すことによる効果を検査することにより、ログインシーケンスの後にそのようなアクセスが可能となる場合がある。

j) 下位レベルのコンポーネントが依存する前提条件及び特性を無効にすることには、アプリケーションの TSF をバイパスするために、アプリケーションの制約から抜け出て下層のオペレーティングシステムへのアクセスを得ることによる攻撃が含まれる。この場合、アプリケーションの利用者がそのようなアクセスを得ることはできないという前提条件は無効となる。下層のデータベース管理システム上のアプリケーションに対する同様の攻撃を想像することができる。この場合も、攻撃者がアプリケーションの制約を抜け出ることができる場合に、TSF がバイパスされる可能性がある。

k) (機密性が問題となる場合)保護が不十分な領域に格納されている機密に関わるデータを読むことによる攻撃には、機密に関わるデータへのアクセスを得る手段として考慮されるべき次の問題が含まれる:

1) ディスクを漁る;

2) 保護されていないメモリへのアクセス;

3) 共用書き込み可能ファイルまたはその他の共用資源(例えば、スワップファイル)へのアクセスの悪用;

4) アクセス利用者が入手できるものを決定するための誤り回復の実施。例えば、クラッシュ後、自動ファイル回復システムは、指し示されていないファイル(ディスク上に存在するが指し示すための名前がない)に対して遺失物取り扱いディレクトリ(lost and found directory)を採用する場合がある。TOE が強制アクセス制御を実装している場合、このディレクトリが保持されているセキュリティレベル(例えば、システムにおいて高い)、及びこのディレクトリにアクセスできる利用者は誰かを検査するのは重要である。

1946 評価者は様々な方法でバックドアを識別することができる。主な技法として次の 2 つが挙げられる。第 1 の技法は、誤使用の可能性があるインタフェースをテストすることである。このテスト中に、評価者によって何かのはずみにバックドアが識別されることがある。第 2 の技法は、TSF の各外部インタフェースのデバッグモードでのテストを通して、証拠資料に記述されているインタフェースのテストの一部として呼び出されないモジュールをすべて識別し、その呼び出されないコードがバックドアかどうか判断するために検査することである。

1947 サブアクティビティの評価(ADV_IMP.2)及びALC_TAT.2、または上位コンポーネントが保証パッケージに含まれるソフトウェア TOE の場合、評価者は、コンパイル段階でバックドアが導入されないことを決定するために、そのツールを分析する際に、コンパイラによってコンパイル段階でリンクされるライブラリ及びパッケージについて考慮することができる。

B.2.1.2 改ざん

1948 改ざんには、例えば次の操作によって、攻撃者が TSF のふるまいに影響を与える攻撃(破壊または非活性化)が含まれる:

a) TSF があるデータの機密性または完全性に依存するような場合、そのデータへアクセスする;

b) 一般的でないまたは期待されない状況に TOE を強制的に対応させる;

c) セキュリティの実施を無効にするか、または遅らせる;

d) TOE の物理的改変。

1949 次の各事項が評価者の独立脆弱性分析で考慮されるべきである(該当する場合)。

a) 機密性または完全性が保護されているデータにアクセスすることによる攻撃には次のものが含まれる:

1) 直接または間接に内部データを読み取る、書き込む、または改変する;

2) 期待しない状況または期待しない目的でコンポーネントを使用する;

3) 抽象の上位レベルでは見えないコンポーネント間のインタフェースを使用する。

b) 内部データの直接的または間接的な読み取り、書き込み、または改変には、考慮されるべき次のタイプの攻撃が含まれる:

1) 利用者パスワードなど、内部に格納されている「秘密」を読み取る;

2) セキュリティ実施メカニズムがある内部データに依存する場合、その内部データを偽造する;

3) 環境変数(例えば、論理名)、または構成ファイルまたは一時ファイル内のデータを改変する。

c) 高信頼プロセスを欺いて、通常はアクセスしない保護ファイルを改変させることが可能な場合がある。

d) 評価者は、次の「危険な特性」も考慮するべきである:

1) コンパイラによって TOE に組み込まれるソースコード(例えば、ログインソースコードを改変することが可能な場合がある);

2) 対話式デバッガー及びパッチ機能(例えば、実行可能イメージを改変することが可能な場合がある);

3) ファイルが保護されていない場合、デバイスコントローラレベルで変更を行う可能性;

4) ソースコードに存在し、オプションとして含めることができる診断コード;

5) TOE に残された開発者ツール。

e) 期待しない状況または期待しない目的でコンポーネントを使用することには、(例えば) TOE がオペレーティングシステムの上に作られたアプリケーションである場合、(例えば、より高い権限を獲得する目的で)自己のコマンドファイルを改変するためにワードプロセッサパッケージまたはその他のエディタの知識を利用者が悪用することが含まれる。

f) 抽象の上位レベルでは見えないコンポーネント間のインタフェースを使用することには、資源への共用アクセスを悪用する攻撃(あるコンポーネントによる資源の改変が、他の(高信頼)コンポーネントのふるまいに影響を与えられる)が含まれる。例えば、ソースコードレベルでグローバルデータまたは共有メモリまたはセマフォなどの間接メカニズムの使用を通して影響を与えられる。

g) TOE を一般的でないまたは期待しない状況に対応させる攻撃が、常に考慮されるべきである。関連する要素には、次のものが含まれる:

1) コンポーネントに期待しない入力を生成する;

2) 下位レベルコンポーネントがある前提条件及び特性に依存する場合、それらを無効にする。

h) コンポーネントへの期待しない入力の生成には、次の場合の TOE のふるまいを調査することが含まれる:

1) コマンド入力バッファオーバフロー(おそらく、「スタックをクラッシュさせる」またはその他の格納領域の上書き(攻撃者が悪用できるかもしれない)、または、暗号化されていないパスワードなど、機密に関する情報が含まれているクラッシュダンプの強制が起こる);

2) 正当でないコマンドまたはパラメタの入力(パラメタを介してデータが戻ることを期待するインタフェースに読み取り専用パラメタを提供したり、SQL インジェクションや書式文字列など解析に失敗する不正な形式の入力を提供したりすることが含まれる);

3) 監査証跡に挿入されるファイルの終わりマーカー(例えば、CTRL-Z または CTRL-D)または null 文字。

i) 下位レベルがある前提条件及び特性に依存する場合、それらを無効にすることには、セキュリティ関連データが特定の形式であることまたは特定の範囲の値であることをソースコードが(明示的または暗黙に)想定するという、ソースコードでの誤りを悪用する攻撃が含まれる。これらの場合、評価者は、データを異なる形式にするかまたは別の値にすることにより、そのような前提条件を無効にすることができるかどうか、及びそのような場合、攻撃者に利益をもたらすかどうかを決定するべきである。

j) TSF の正しいふるまいは、資源が限界に達するかまたはパラメタが最大値に達する極端な状況で無効になる前提条件に依存する場合がある。評価者は、(実際的な場合)限度に達したときの TOE のふるまいを考慮するべきである。例えば:

1) 日付の変更(例えば、クリティカルな日付の閾値を過ぎたときの TOE のふるまいを検査する);

2) ディスクが一杯になる;

3) 利用者の最大数を越える;

4) 監査ログが一杯になる;

5) コンソールのセキュリティアラームキューが飽和状態になる;

6) 通信コンポーネントに大きく依存する複数利用者 TOE の様々な部分がオーバロードしている;

7) トラフィックの負荷でネットワークまたは個々のホストが利用不能になる;

8) バッファまたはフィールドが一杯になる。

k) セキュリティの実施を無効にするか、または遅らせることによる攻撃には次の要素が含まれる:

1) 順序を混乱させるために割り込みまたはスケジューリング機能を使用する;

2) 同時性を混乱させる;

3) 抽象の上位レベルでは見えないコンポーネント間のインタフェースを使用する。

l) 順序を混乱させるための割り込みまたはスケジューリング機能の使用には、次の場合の TOE のふるまいの調査が含まれる:

1) コマンドが割り込まれる(CTRL-C、CTRL-Y などによる);

2) 最初の割り込みに応答が出されるまえに、次の割り込みが出される。

m) セキュリティ上クリティカルなプロセス(例えば、監査デーモン)を停止することによる影響が検査されるべきである。同様に、監査記録のログ、またはアラームの発行や受信を遅らせて、管理者の役に立たないようにする(攻撃がすでに成功しているため)ことが可能な場合がある。

n) 同時性の混乱には、複数のサブジェクトが同時にアクセスを試みるときの TOE のふるまいの調査が含まれる。TOE は、2 つのサブジェクトが同時にアクセスしようとするときに必要となるインターロックに対処できるが、さらにサブジェクトが存在する場合は、ふるまいの定義が明確でなくなることがある。例えば、クリティカルなセキュリティプロセスが必要とする資源に別の 2 つのプロセスがアクセスしていると、クリティカルなセキュリティプロセスが資源待機状態になることがある。

o) 抽象の上位レベルでは見えないコンポーネント間のインタフェースの使用は、時間的な要求が厳しい(time-critical)高信頼プロセスを遅らせる手段を提供することがある。

p) 物理的攻撃は、物理的プロービング、物理的操作、物理的改変、物理的置き換えに分類することができる。

1) TOE の内部構造を狙った TOE への侵入(例えば、内部の通信インタフェース、配線、またはメモリの読み取り)による物理的プロービング。

2) 物理的操作には、TOEの内部構造に対してTOEの内部改変を目的に実行されるもの(例えば、光学的障害誘発を相互作用プロセスとして使用する)、TOE の外部インタフェースに対して実行されるもの(例えば、電源または時計の異常)、及び TOE 環境に対して実行されるもの(例えば、温度の変更)がある。

3) 通常の操作では拒否されるべきである権限またはその他の能力を継承するための、TOE の内部のセキュリティ実施の性質に対する物理的改変。こうした改変は、光学的障害誘発などによって引き起こされる可能性がある。物理的改変による攻撃は、実行前に TSF 内部プログラムのデータ転送に障害を発生させるなどして、TSF 自体の改変をもたらす可能性もある。攻撃者による TOE への物理的アクセスを防止するためのその他の手段(おそらくは環境的手段)がない場合、TSF 自体を改変するこの種のバイパスにより、すべての TSF が危険にさらされる可能性があることに注意のこと。

4) 物理的置き換えは、TOE の配付中または運用中に TOE を別の IT エンティティに置き換える。開発環境から利用者への TOE の配付中に行われる置き換えは、セキュアな配付手続き(開発セキュリティ(ALC_DVS)の下で考慮された手続きなど)の適用によって防止されるべきである。運用中に行われる TOE の置き換えは、利用者ガイダンスと運用環境の組み合わせを通じて考慮することができる。これにより利用者は、TOE と対話していることに確信を持てるようになる。

B.2.1.3 直接攻撃

1950 直接攻撃には、順列的メカニズム、確率的メカニズム、またはその他のメカニズムが直接攻撃に耐え得ることを確認するための強度テストに必要なあらゆる侵入テストの識別が含まれる。

1951 例えば、擬似乱数ジェネレータの特定の実装が、セキュリティメカニズムを実現するために必要なエントロピーを持つというのは間違った想定である場合がある。

1952 確率的または順列的メカニズムが、セキュリティ属性値の選択(例えば、パスワード長の選択)、あるいは人間の利用者によるデータエントリ(例えば、パスワードの選択)に依存する場合は、最悪のケースを反映した想定が行われるべきである。

1953 確率的または順列的メカニズムは、このサブアクティビティへの入力として必要な評価証拠(セキュリティターゲット、機能仕様、TOE 設計、及び実装表現サブセット)の調査中に識別されるべきである。また、その他の TOE (例えば、ガイダンス)証拠資料が、その他の確率的または順列的メカニズムを識別する場合もある。

1954 設計証拠またはガイダンスに主張または想定(例えば、毎分可能な認証の試行回数)が含まれている場合、評価者は、これらが正しいことを独立して確認するべきである。これは、テストまたは独立分析によって達成することができる。

1955 暗号アルゴリズムの弱点に依存する直接攻撃は、CC の範囲外であるため、脆弱性分析(AVA_VAN)で考慮されるべきでない。暗号アルゴリズムの実装の正確性は、ADV及びATEアクティビティで考慮される。

B.2.1.4 監視

1956 情報はエンティティの特性間の関係に関する抽象的な概念であり、信号がシステムに関する情報を含む(TOE がこの信号に反応できる場合)。TOE 資源は、利用者データによって表される情報を処理及び格納する。したがって情報は以下のような特徴を持つ:

a) 情報は、TOE 内転送または TOE からのエクスポートにより、利用者データとともにサブジェクト間を流れることができる;

b) 情報は、生成され、他の利用者データに対して渡すことができる;

c) 情報は、情報を表すデータに対する操作を監視することから得られる。

1957 利用者データによって表される情報は、データに対する操作を制御するために、「秘密ではない」、「機密」、「秘密」、「トップシークレット」などの値を持つ「秘密区分レベル」のようなセキュリティ属性によって特徴付けることができる。操作により、この情報、ひいてはセキュリティ属性を変更することができる。例えば、FDP_ACC.2 は、「無害化(sanitarisation)」によってレベルの低下を表現したり、データの組み合わせによってレベルの上昇を表現したりできる。これは、制御されたオブジェクトに対する制御されたサブジェクトの制御された操作に焦点を当てた情報フロー分析の 1 つの側面である。

1958 別の側面は***不正情報フロー***の分析である。この側面は、FDP_ACC ファミリによって扱われる利用者データを含むオブジェクトへの直接アクセスよりも一般的である。情報フロー制御方針の制御下で情報を伝達する***意図しない***信号チャネルもまた、この情報を含むオブジェクトまたはこの情報に関連するオブジェクトの処理を監視することによって引き起こされる場合がある(例えば、副次的チャネル)。***意図した***信号チャネルは、資源を操作するサブジェクト、及びこうした操作を観察するサブジェクトまたは利用者の観点から識別される場合がある。従来、隠れチャネルは、改変または調節される資源に従って、タイミングチャネルまたは格納チャネルとして識別されてきた。その他の監視攻撃に関しては、TOE の使用は SFR により変動する。

1959 隠れチャネルは、通常、観察不能性及びマルチレベル分離方針の要件が TOE に含まれる場合に適用される。隠れチャネルは、脆弱性分析及び設計アクティビティの実行中に決まって発見されるため、テストを実施するべきである。ただし、こうした監視攻撃は、通常、「隠れチャネル分析」と一般に呼ばれる専門的な分析技法を通じてのみ識別される。これらの技法をテーマにした研究が数多く行われており、このテーマに関する報告書が多数公開されている。隠れチャネル分析の実施に関するガイダンスは、評価監督機関に求めるべきである。

1960 *意図しない*情報フローの監視攻撃には、ガイダンス文書に対応した方法で TOE を操作することにより、TOE の機密内部データの開示を目的とする受動的な分析技法が含まれる。

1961 副次的チャネル分析には、TOE の物理的漏洩に基づく暗号解読技法が含まれる。物理的漏洩は、タイミング情報、及び TSF の計算時における電力消費または電力放射によって発生する可能性がある。タイミング情報は、(TOE へのネットワークアクセスができる)遠隔地の攻撃者も収集することができる。電力ベースの情報チャネルを収集する場合、攻撃者は TOE 環境の近くにいる必要がある。

1962 盗聴技法には、コンピュータディスプレイの電磁波放射や光学的放射など、TOE の近くで発生するとは限らないあらゆる形式のエネルギーの傍受が含まれる。

1963 監視には、SSL 実装に対する攻撃など、プロトコルの欠陥の悪用も含まれる。

B.2.1.5 誤使用

1964 誤使用が発生する要因には次のものが挙げられる:

a) 不完全なガイダンス文書;

b) 不合理なガイダンス;

c) 意図されたものでない TOE の誤構成;

d) TOE の強制的例外のふるまい。

1965 ガイダンス文書が不完全であると、SFR に従って TOE を操作する方法が利用者に理解されない場合がある。評価者は、ガイダンスが完全であることを決定するために、他の評価アクティビティを実行することによって得られた TOE の知識を応用すべきである。特に、評価者は機能仕様を考慮するべきである。この文書に記述されている TSF は、人間の利用者に提供されている TSFI を通じたセキュアな管理と使用を可能にするために、必要に応じてガイダンスに記述されるべきである。さらに、各種操作モードを考慮して、すべての操作モードに対してガイダンスが提供されていることを保証するために、各種操作モードが考慮されるべきである。

1966 評価者は、補足的に、ガイダンスとこれらの文書の間の非形式的マッピングを準備することができる。このマッピングでの欠落は、不完全性を示すことがある。

1967 TOE の使用または運用環境に対して、ST と一致しない要求や、セキュリティを維持する上で負荷が大きい要求がガイダンスで行われている場合、そのガイダンスは合理的でないとみなされる。

1968 TOE は、消費者が SFR に従って TOE を効果的に使用できるように支援し、意図しない誤構成を防止するために様々な方法を使用することができる。ある TOE が、その TOE と SFR が一致していない状態のときに消費者に警告する機能性(特徴)を採用することがある一方で、他の TOE は、既存のセキュリティ機能の特徴を効果的に使用するための示唆、ヒント、手順などを含んだ高度なガイダンスとともに配付されることがある。例えば、SFR が危険にさらされている状態、つまり安全でない状態であることを検出するための一助として監査という特徴を使用するためのガイダンスなどが挙げられる。

1969 評価者は、TOE の機能性、その目的、及び運用環境のセキュリティ対策方針を考慮することで、ガイダンスの使用によって、安全でない状態への移行をタイムリに検出できるという合理的予測が存在するかどうかを結論付ける。

1970 TOE が安全でない状態に移行する可能性は、TOE の保証パッケージに含まれているコンポーネントの証拠として提供される ST、機能仕様、その他の設計表現(例えば、TOE 設計(ADV_TDS)のコンポーネントが含まれている場合は、TOE/TSF 設計仕様)などの評価用提供物件を使用して決定することができる。

1971 TSF の強制的例外のふるまいの例としては次のものが挙げられる。ただし、これらには限定されない:

a) スタートアップ、クローズダウンまたは誤り回復が行われるときの TOE のふるまい;

b) 極端な状況下での TOE のふるまい(オーバロードまたは漸近的ふるまいとも呼ばれる)。特にこの場合、TSF の部分的な非活性化や無効化を招く可能性がある;

c) 前述の改ざんに関する節に記述されている攻撃によって生じる、意図的でない誤構成または安全でない使用の可能性。

B.2.2 潜在的脆弱性の識別

1972 潜在的脆弱性は、評価者によって様々なアクティビティで識別される。例えば、評価アクティビティで明らかになる場合や、脆弱性を探索するための証拠分析によって識別される場合がある。

B.2.2.1 遭遇による識別

1973 遭遇による脆弱性の識別では、評価者が評価アクティビティの実施中に潜在的脆弱性を識別する。つまり、潜在的脆弱性の識別を明確な目的として証拠が分析されているときではない。

1974 遭遇による識別という方法は、評価者の経験と知識に依存するもので、評価監督機関によって確認及び指導される。再現性のない手法ではあるが、報告された潜在的脆弱性から得られた結論の反復性を保証するために文書化される。

1975 この方法に形式的な分析基準は必要とされない。潜在的脆弱性は、知識と経験の結果として、提供される証拠から識別される。ただし、この識別方式は、特定の証拠のサブセットに制約されない。

1976 評価者は、TOE タイプの技術、及び文書化されて公開されている既知のセキュリティ欠陥に関する知識があるものとみなされる。想定される知識レベルは、TOE タイプに関係するセキュリティ関連メーリングリスト、普及している製品と技術のセキュリティ問題を調査する機関が発行する定例公報(バグ、脆弱性、セキュリティ欠陥に関するリスト)から得られる知識である。AVA_VAN.1またはAVA_VAN.2に関しては、この知識を、特定のカンファレンスの記録や、大学の研究機関が発行する詳細な論文にまで広げることは期待されていない。ただし、最新の知識を利用できるように、評価者は公知の資料の探索を行う必要があるかもしれない。

1977 AVA_VAN.3からAVA_VAN.5に関しては、公開の場で利用できる情報の探索を、カンファレンスの記録や、大学の研究機関及びその他の関連組織が研究・調査によって作成する論文にまで広げることが期待されている。

1978 例えば、潜在的脆弱性は次のような経緯で生じる(評価者がどのようにして潜在的脆弱性を発見するか):

a) 評価者が、ある証拠の検査中に、同様の製品種別で識別された潜在的脆弱性を思い出し、評価中の TOE にも同じ脆弱性があることを確信する場合;

b) 評価者が、ある証拠の検査中にインタフェースの仕様の欠陥を発見し、それが潜在的脆弱性を表している場合。

1979 これには、特定の製品種別における一般的な脆弱性について記載された IT セキュリティ資料または評価者が購読しているセキュリティ関連メーリングリストを通じて、TOE の潜在的脆弱性を認識することも含まれる場合がある。

1980 攻撃方法は、これらの潜在的脆弱性から直接開発することができる。このため、発見された潜在的脆弱性は、評価者の脆弱性分析に基づいて侵入テストを生成する際に照合される。評価者が潜在的脆弱性に遭遇するための明確なアクションはない。このため、評価者への指示は、AVA_VAN.1.2E 及びAVA_VAN.*.4E で特定された暗黙のアクションを通じて行われる。

1981 公知の脆弱性と攻撃に関する最新の情報は、評価監督機関などによって、評価者に提供される。この情報は、検出された脆弱性及び攻撃方法を、評価者が侵入テスト開発時に照合する際に考慮する。

B.2.2.2 分析による識別

1982 次の分析タイプは、評価者アクションの観点から提供される。

B.2.2.2.1 構造化されていない分析

1983 (サブアクティビティの評価(AVA_VAN.2)で)評価者によって実行される構造化されていない分析では、評価者が一般的な脆弱性(B.2.1 を参照)を考慮することができる。また、評価者は、同様の技術タイプでの欠陥に関する各自の経験と知識を利用することもできる。

B.2.2.2.2 焦点を置いた分析

1984 評価アクティビティの実施中に、評価者は関心の分野を識別することもできる。これらは、証拠が関連付けられているアクティビティの要件を証拠は満たすが、評価者が不安を抱いている TOE 証拠の特定の部分である。例えば、特定のインタフェース仕様が特に複雑に見えるため、TOE の開発または TOE の運用において誤りが発生しやすくなる可能性がある。この段階では、明白な潜在的な脆弱性は存在しないが、さらに調査が必要である。これは、さらに調査が必要なため、遭遇により識別される範囲を越えている。

1985 潜在的脆弱性と関心の分野の違いは次のとおりである:

a) 潜在的脆弱性 - 弱点を悪用するための攻撃方法または TOE に関連する脆弱性情報を、評価者が認識している。

b) 関心の分野 - 他の場所で提供された情報に基づいて、評価者が関心の分野を潜在的脆弱性として考慮に入れることができる。評価者は、インタフェース仕様を確認することで、インタフェースが極端に(不必要に)複雑であるために潜在的脆弱性がその分野に存在するかもしれないことを識別するが、この最初の検査ではそれが明らかにならない。

1986 脆弱性を識別するための焦点を置いた手法とは、含まれている情報から明らかになる潜在的脆弱性を識別することを目的とした証拠の分析である。この手法は事前に決定されていないため、これは、構造化されていない分析になる。潜在的脆弱性を識別するためのこの手法は、サブアクティビティの評価(AVA_VAN.3)に必要な独立脆弱性分析の中で使用できる。

1987 この分析は、様々な手法で実現可能であり、どの手法でも同一レベルの信頼が得られる。どの手法にも、実行される証拠の検査について厳密な形式はない。

1988 使用される手法は、証拠がAVA/AGDサブアクティビティの要件を満たしていることを判断するための、評価者による証拠の評定の結果によって方向付けられる。このため、潜在的脆弱性の存在に関する証拠の調査は、次のどれによって方向付けてもよい:

a) 評価アクティビティの実施中に証拠を検査することで識別された関心の分野;

b) アーキテクチャ設計の分析中(サブアクティビティの評価(ADV_ARC.1)での分析など)に識別された、分離を提供する特別な機能性への依存性。バイパス不可能であることを判断するためにさらなる分析を必要とする;

c) TOE での潜在的脆弱性を仮定するための、証拠の代表検査。

1989 評価者は、証拠内の潜在的な脆弱性を識別するために、どのようなアクションがとられたかを報告する。ただし評価者は、検査を始める前に、潜在的脆弱性を識別する手順を記述することはできない場合がある。手法は、評価アクティビティの結果によって漸進的に発展する。

1990 関心の分野は、TOE 評価に対して特定された SAR を満たすために提供されるあらゆる証拠の検査から生じる可能性がある。公開の場でアクセスできる情報も考慮される。

1991 評価者が実行するアクティビティは再現可能であり、結論を得るために実行される手順は異なっていても、TOE での保証レベルという点で同一の結論を得ることができる。評価者は、実行した分析の形式を文書化するため、結論を得るために実際に実行された手順も再現可能である。

B.2.2.2.3 系統的分析

1992 系統的分析手法は、証拠の構造化された検査の形式をとる。この方法では、分析が採用する構造と形式を評価者が特定する必要がある(つまり、焦点が置かれた識別方法とは異なり、分析が実行される方法が事前に決定されている)。この方法は、考慮される情報及び考慮される方法/理由の観点で特定される。潜在的脆弱性を識別するためのこの手法は、サブアクティビティの評価(AVA_VAN.4)及びサブアクティビティの評価(AVA_VAN.5)に必要な独立脆弱性分析の中で使用できる。

1993 この証拠の分析は、意図的で、かつ手法が事前に計画されており、分析への入力として識別されたすべての証拠を考慮に入れる。

1994 保証パッケージで特定されている(ADV)保証要件を満たすために提供されるすべての証拠は、潜在的脆弱性識別アクティビティへの入力として使用される。

1995 この分析の「系統的」という記述は、この潜在的脆弱性の識別で順序付けられかつ計画された手法が使用されるという特性を表現しようとして使用されている。検査では「方法」または「体系」が適用される。評価者は、どのような証拠が考慮されるか、検査される証拠内の情報、この情報が考慮される方法、及び立てられる仮定の観点から使用される方法を記述する。

1996 仮定に含まれる可能性があるいくつかの例を次に示す:

a) 外部インタフェースで攻撃者に対して利用可能な状態になっているインタフェースに対する誤った形式の入力の考慮;

b) ドメイン分離などのセキュリティメカニズムを検査し、分離の劣化をもたらす可能性がある内部バッファオーバフローを仮定;

c) TOE 実装表現においては作成されることになっており、その時点では完全には TSF によって制御されておらず、SFR を損なうために攻撃者によって使用される可能性がある任意のオブジェクトを識別するための分析。

1997 例えば、評価者は、インタフェースが TOE の潜在的な弱点の分野であることを識別し、「機能仕様及び TOE 設計で提供されたすべてのインタフェース仕様が潜在的な脆弱性を仮定するために分析される」という分析に対する手法を特定し、続けてこの仮定で使用される方法を説明することができる。

1998 この識別方式は、TOE を攻撃する構想を提供し、その構想は、評価者が TOE の潜在的脆弱性の侵入テストを完成させて実行するであろう。この識別方式の根拠は、TOE で実行される悪用可能かどうかの決定のカバレージ及び深さの証拠を提供するであろう。

B.3 攻撃能力の使用

B.3.1 開発者

1999 攻撃能力は、PP/ST 作成者が、脅威の環境及び保証コンポーネントの選択を考慮して、PP/ST の開発中に使用する。ここでは、想定される TOE の攻撃者が持つ攻撃能力が、基本、強化基本、中、または高として一般的に特徴付けられるという決定が行われる場合がある。あるいは、攻撃者が保有すると予想される個別要因の特定レベルを、PP/ST で特定する場合がある(例えば、攻撃者が、特殊機器へのアクセスが可能な TOE 技術タイプのエキスパートであると想定される場合)。

2000 PP/ST 作成者は、リスク評定時に開発した脅威プロファイルを考慮する(CC の範囲外であるが、セキュリティ課題定義の観点、または低保証 ST での要求ステートメントの観点から、PP/ST の開発に対する入力として使用される)。この後の節で説明するいずれかの手法の観点からこの脅威プロファイルを考慮することで、TOE が抵抗する攻撃能力の特定が可能となる。

B.3.2 評価者

2001 攻撃能力は、特に、ST 評価及び脆弱性評定アクティビティ中に 2 つの異なる方法で評価者によって考慮される。

2002 攻撃能力は、評価者が、脆弱性分析サブアクティビティの実施中に、攻撃者が持つ特定の攻撃能力を想定した攻撃に TOE が耐え得るかどうかを決定するために使用する。潜在的脆弱性が TOE で悪用可能であると決定した場合、評価者は、意図する環境のすべての局面を、攻撃者の想定攻撃能力も含めて考慮したうえで、それが悪用可能であることを確認しなければならない。

2003 したがって評価者は、セキュリティターゲットの脅威ステートメントで提供される情報を使用して、攻撃者が攻撃を成功させるために必要とする最小限の攻撃能力を決定し、攻撃に対する TOE の抵抗力についての結論を出す。表 2 は、この分析と攻撃能力との関係を示している。

脆弱性 コンポーネント	TOE は、次の攻撃能力を持つ攻撃者に対抗する	残存脆弱性は、次の攻撃能力を持つ攻撃者のみが悪用できる
VAN.5	高	高より上
VAN.4	中	高
VAN.3	強化基本	中
VAN.2	基本	強化基本
VAN.1	基本	強化基本

表 2　脆弱性のテストと攻撃能力

2004 上の表の残存脆弱性の列に示されている「高より上」エントリは、潜在的脆弱性を悪用するために攻撃者が「高」よりも高い攻撃能力を持つことを必要とする潜在的脆弱性を表す。ここで残存と分類される脆弱性は、TOE に既知の弱点が存在するが、現在の運用環境では、想定される攻撃能力を使用して弱点を悪用できないという事実を反映している。

2005 脆弱性の悪用を防止する対抗策を運用環境で講じることにより、すべての攻撃能力レベルにおいて潜在的脆弱性を「実行不可能」とみなすことができる。

2006 脆弱性分析は、確率的または順列的メカニズムにアクセスするものを含むすべての TSFI に適用される。TSFI の設計及び実装の正確性に関する想定は行われない。また、攻撃方法または攻撃者と TOE の相互作用に対して制約は課せられない - 攻撃が可能な場合は、脆弱性分析でその攻撃が考慮される。表 2 に示すように、脆弱性保証コンポーネントに対する評価の成功は、要求された脅威レベルから保護するように TSF が設計され、実装されていることを表す。

2007 評価者は、個々の潜在的脆弱性について攻撃能力を計算する必要はない。場合によっては、攻撃方法を開発する際に、その攻撃方法の開発と実行に必要な攻撃能力が、運用環境の攻撃者に想定される攻撃能力と釣り合っているかどうかが明らかになる。悪用可能なことが決定されたすべての脆弱性に対し、評価者は、攻撃者に想定される攻撃能力のレベルで悪用が可能かどうかを決定するために攻撃能力計算を実行する。

2008 代替手法が適用される必須ガイダンスを評価監督機関が提供しない場合、攻撃能力の計算が必要なときには、以下で説明する手法が必ず適用される。この後の表 3 及び表 4 に示す値は、数学的に証明されたものではない。このため、これらの表の値は、技術種別及び特定の環境に応じて調整する必要がある場合がある。評価者は、評価監督機関からガイダンスを求めるべきである。

B.4 攻撃能力の計算

B.4.1 攻撃能力の適用

2009 攻撃能力は、専門知識、資源、及び動機によって決まる。これらの要因を表現及び定量化する複数の方法がある。また、特定の TOE タイプに対し、これ以外の要因が適用されることもある。

B.4.1.1 動機の取り扱い

2010 動機は、攻撃者及び攻撃者が望む資産に関するいくつかの観点を記述するために使用することができる攻撃能力の要因である。第一に、動機は、攻撃の可能性を暗示することができる - 高い動機付けが記述されている脅威からは攻撃が差し迫っていることを、または動機付けされていない脅威からは攻撃が予想されないことを推測できる。ただし、この 2 つの極端なレベルの動機を除いて、動機から攻撃が起きる確率を引き出すのは困難である。

2011 第二に、動機は、攻撃者または資産の所有者にとっての金銭的またはそれ以外の資産価値を暗示することができる。非常に価値の高い資産は、価値の低い資産に比べて、攻撃を動機付ける可能性が高い。ただし、非常に一般的な方法は別として、資産の価値は主観的であるため(つまり、資産の所有者にとっての資産価値に大きく左右されるため)に、資産価値を動機に関連付けることは困難である。

2012 第三に、動機は、攻撃者が攻撃を成功させるための専門知識と資源を暗示することができる。動機付けの高い攻撃者は、資産を保護する手段を打破するための十分な専門知識と資源を得る可能性が高いと推測できる。逆に、十分な専門知識と資源を備えた攻撃者でも、その動機が低い場合は、それらを使用して攻撃を成功させようとはしないと推測できる。

2013 評価を準備し、実行する過程において、ある時点で動機の 3 つの観点すべてが考慮される。第一の観点である攻撃の可能性は、開発者を評価に向かわせる場合がある。攻撃者が攻撃を行うために十分に動機付けられていると開発者が考える場合、評価は、攻撃者の労力に対抗する TOE の能力を保証することができる。システム評価などにおいて運用環境が明確に定義されている場合は、攻撃の動機レベルが判明している場合があり、それが対抗策の選択に影響を与える。

2014 第二の観点を考慮するとき、資産の所有者は、資産の価値(ただし、測定された)が資産に対する攻撃を動機付けるのに十分であると考える場合がある。評価が必要であると判断されると、試行されそうな攻撃の方法と、それらの攻撃で使用される専門知識及び資源を決定するために攻撃者の動機が考慮される。検査後、開発者は、特にAVA要件コンポーネントにおいて、脅威に対する攻撃能力に釣り合った適切な保証レベルを選択することができる。評価の過程で、特に脆弱性評定アクティビティを完了した結果として、評価者は、TOE が、その運用環境で動作する際に、識別された専門知識と資源を備えた攻撃者を十分に阻止できるかどうかを決定する。

2015 PP 作成者は、TOE (PP の要件に適合)の置かれる運用環境を熟知しているため、攻撃者の動機を定量化することができる場合がある。このため、PP での攻撃能力の表現に、動機が、その定量化に必要な方法及び尺度とともに、明示的に組み込まれる可能性がある。

B.4.2 攻撃能力の特徴付け

2016 この節では、攻撃能力を決定する要因を検査し、評価プロセスのこの側面から主観性をある程度排除するために役立つガイドラインを提供する。

B.4.2.1 攻撃能力の決定

2017 攻撃能力の決定は、攻撃を作成し、その攻撃が TOE に成功裏に適用可能であることを実証するための労力(必要なテスト装置の設定及び構築を含む)、すなわち、TOE 内の脆弱性の悪用に必要な労力を識別することである。攻撃が成功裏に適用可能であることを実証する場合は、研究によって示された結果を拡張して有効な攻撃を作成する際の困難について考慮する必要がある。例えば、ある 1 回の試行によって機密データ項目(キーなど)のいくつかのビットまたはバイトが明らかになる場合、そのデータ項目の残りがどのようにして取得されるかを考慮する必要がある(この例では、いくつかのビットはさらなる試行によって測定されるが、それ以外のビットは徹底的探索などの異なる技法によって検出されることがある)。攻撃に関して次の 2 点が明確に実証されている場合、すべての試行を行わなくても完全な攻撃を識別できることがある。すなわち、1 つは TOE 資産へのアクセスが確保されていること、もう 1 つは対象となるAVA_VANコンポーネントに従って悪用目的の完全な攻撃が現実に実行可能であることである。対象となるAVA_VANコンポーネントに従って悪用目的の完全な攻撃が現実に実行可能であることを実証するために、完全な攻撃を実行する以外に方法がない場合がある。そして、それを実際に必要であるリソースに基づいて評定する。潜在的脆弱性の識別から得られる成果物の 1 つとして想定されているのは、別の TOE インスタンスの脆弱性を悪用する際に使用可能な攻撃の実行方法に関する段階的説明を提供するシナリオである。

2018 多くの場合、評価者は、完全な悪用を実行するのではなく、悪用のパラメタを見積もる。この見積もりとその根拠は、ETR において証拠資料として提出される。

B.4.2.2 考慮する必要がある要因

2019 脆弱性を悪用するために必要な攻撃能力を分析するとき、次の要因が考慮されるべきである:

a) 識別して悪用するために要する時間(***所要時間***);

b) 必要な技術的専門知識(***専門知識***);

c) TOE 設計と運用の知識(***TOE の知識***);

d) ***機会***;

e) 悪用に必要な ***IT ハードウェア/ソフトウェアまたはその他の機器***。

2020 多くの場合、これらの要因は、独立ではなく、かなりの程度、相互に置き換えることができる。例えば、専門知識またはハードウェア/ソフトウェアは、時間に置き換えることができる。次にこれらの要因について説明する(各要因のレベルは、規模の小さなものから順に説明する)。その場合は、より「安価な」組み合わせを悪用フェーズで考慮する。

2021 ***所要時間***は、攻撃者が、TOE に特定の潜在的脆弱性が存在することを識別し、攻撃方法を開発し、さらに TOE に対して攻撃を仕掛けるために必要な労力を持続させる時間の合計である。この要因を考慮する際には、最悪のケースのシナリオを使用して必要な時間を見積もる。識別されている時間は、次のとおりである:

a) 1 日未満;

b) 1 日～1 週間;

c) 1 週間～2 週間;

d) 2 週間～1 ヶ月;

e) 6 ヶ月に達するまで 1 ヶ月ずつ追加した値;

f) 6 ヶ月以上。

2022 「***専門家の専門知識***」(Specialist expertise)は、基本原理、製品種別、または攻撃方法(例えば、インターネットプロトコル、UNIX オペレーティングシステム、バッファオーバフロー)についての一般的な知識のレベルを意味する。識別されているレベルは、次のとおりである:

a) 「しろうと」(Layman)は、エキスパートや熟練者と比べて知識が乏しく、特別の専門知識を持っていない;

b) 「熟練者」(Proficient)は、製品またはシステム種別のセキュリティのふるまいを理解しているという点で知識が豊富である;

c) 「エキスパート」(Expert)は、製品またはシステム種別で実装されている、実装の基礎となるのアルゴリズム、プロトコル、ハードウェア、構造、セキュリティのふるまい、採用されているセキュリティの原理と概念、新しい攻撃を定義するための技術とツール、暗号、製品種別に対する従来型の攻撃、攻撃方法などを理解している。

d) 攻撃の各ステップに対処するために、様々な分野に関するエキスパートレベルの専門知識が求められる状況を考慮して、「複数のエキスパート」レベルが導入されている。

2023 複数の種類の専門知識が必要となる場合がある。デフォルトでは、様々な専門知識要因の中でより高度なものが選択される。非常に特殊なケースでは、「複数のエキスパート」レベルを使用できる。ただし、HW 操作と暗号化技術などのようにまったく異なる分野に関する専門知識でなければならないことに注意するべきである。

2024 ***TOE の知識***は、TOE に関係する特定の専門知識を意味する。これは、一般的な専門知識とは区別されるが、それに関係がないことはない。識別されているレベルは、次のとおりである:

a) TOE に関する公開情報(例えば、インターネットから得られる);

b) TOE に関する制限的な情報(例えば、開発者組織内で管理され、秘密保持契約の下で他の組織と共有される知識);

c) TOE の機密に関わる情報(例えば、開発者組織内の極秘チーム間で共有され、その特定のチームのメンバのみがアクセスできる知識);

d) TOE に関する危機的な情報(例えば、少数の個人のみが把握している知識。この知識へのアクセスは、厳格な need to know basis (情報を知る必要がある者だけが知るという原則)及び個別の条件で非常に厳しく管理される)。

2025 TOE の知識は、設計抽象度に従って等級付けされるが、これは TOE の基準によって TOE でのみ行うことができる。一部の TOE 設計は公開情報源(またはかなりの部分が公開情報源に基づいている)であるため、設計表現は公開または最高でも制限的として分類されるであろうが、一方で他の TOE の実装表現は、攻撃を助長する情報を攻撃者に与えるであろうことから、非常に厳密に管理されており、そのために機密に関わる、あるいは危機的であるとみなされる。

2026 複数の種類の知識が必要となる場合がある。そのような場合、様々な知識要因の中でより高度なものが選択される。

2027 ***機会***も重要な考慮事項であり、***所要時間***要因と関係がある。脆弱性の識別または悪用には、検出される可能性が高まるくらいに、TOE へのかなりの量のアクセスを必要とする場合がある。攻撃方法の中には、オフラインでかなりの労力を必要とし、悪用するための TOE への簡単なアクセスだけを必要とするものがある。またアクセスは、継続的であるかまたは多数のやりとりを必要とする場合がある。

2028 TOE によっては、攻撃者が取得できる TOE のサンプルの数が***機会***と同一視されることがある。これは特に、TOE に侵入して SFR を侵害する試みによって TOE が破壊されるかもしれず、その TOE サンプル(例えば、ハードウェアデバイス)をそれ以降のテストで使用できなくなる場合に関係する。このような場合、TOE の配付が管理され、そのために攻撃者が TOE のサンプルを追加で取得するために労力を費やさなければならないことがよくある。

2029 この説明における機会の意味は次のとおりである:

a) 「不必要/無制限」のアクセスは、攻撃があらゆる機会の実現を必要としないことを意味する。これは、TOE へのアクセス中に検出されるリスクがなく、攻撃に必要な数の TOE サンプルに問題なくアクセスできるためである;

b) 「容易」は、アクセスの必要な期間が 1 日未満であり、攻撃の実行に必要な TOE サンプルの数が 10 未満であることを意味する;

c) 「中」は、アクセスの必要な期間が 1 ヶ月未満であり、攻撃の実行に必要な TOE サンプルの数が 100 未満であることを意味する;

d) 「困難」は、少なくとも 1 ヶ月のアクセスを必要とするか、または攻撃の実行に必要な TOE サンプルの数が 100 以上であることを意味する;

e) 「なし」は、攻撃を実行するための十分な機会が得られないことを意味する(悪用されようとする資産が利用可能な期間または侵害を受けやすい期間が、攻撃を実行するために必要な機会の期間よりも短い場合。例えば、攻撃に 2 週間を要するが、資産キーが毎週変更される場合)。もう 1 つのケースとして、攻撃の実行に必要な十分な数の TOE サンプルに攻撃者がアクセスできない場合が挙げられる。例えば、TOE がハードウェアで、攻撃が成功する代わりにその TOE が攻撃中に破壊される可能性が非常に高く、攻撃者が 1 つの TOE サンプルにしかアクセスできない場合である。

2030 この要因の考慮によって、時間の可用性に対する要件が、得られる機会の時間を上回るために悪用を遂行できないことを判断できる場合がある。

2031 ***IT ハードウェア/ソフトウェアまたはその他の機器***は、脆弱性を識別または悪用するために必要な機器を意味する。

a) 「標準機器」(Standard equipment)は、脆弱性の識別または攻撃の目的で攻撃者が容易に使用することができる。この機器は、TOE 自体の一部(例えば、オペレーティングシステムのデバッガー)であるか、または簡単に入手する(例えば、インターネットからのダウンロード、プロトコルアナライザ、または簡単な攻撃スクリプト)ことができる。

b) 「特殊機器」(Specialised equipment)は、攻撃者が容易に入手することはできないが、過度の労力を費やすことなく入手することができる。これには、大きすぎない対価で得られる機器(例えば、電力解析ツール、インターネットで接続されている数百台の PC の使用などが、このカテゴリに分類されるであろう)、またはより広範な攻撃スクリプトやプログラムの開発が含まれる。攻撃の各ステップに対処するために、特殊機器で構成された、通常とは明らかに異なるテストベンチが必要になる場合、これは「特別注文」としてレート付けされることになる。

c) 「特別注文機器」(Bespoke equipment)は、特別に製造する必要があるか(例えば、非常に精巧なソフトウェア)、または機器がきわめて特殊であるためにその配付が管理されている(おそらく制限されている)ことから、一般には容易に入手できない。あるいは、機器が非常に高価である。

d) 攻撃の各ステップに対処するために、様々な種類の特別注文機器が必要となる状況を考慮して、「複数の特別注文」レベルが導入されている。

2032 専門家の専門知識及び ***TOE の知識***は、TOE を攻撃するために人が必要とする情報に関するものである。攻撃者の専門知識(攻撃者が、補完的な知識領域を持つ 1 人または複数の人員である場合もある)と、攻撃で機器を効果的に使用する能力との間には、暗黙の関係が存在する。攻撃者の専門知識が乏しいほど、機器(IT ハードウェア/ソフトウェアまたはその他の機器)を使用する可能性が低下する。同様に、専門知識が豊富であるほど、攻撃で機器が使用される可能性が増加する。暗黙ではあるが、この専門知識と機器使用の関係は、例えば、エキスパートの攻撃者による機器の使用が環境的手段によって阻止される場合、または、他者の労力によって、専門知識をほとんど必要とせずに効果的に使用できる攻撃ツールが作成され、無料で配付されている(例えば、インターネットで)場合は、必ずしも適用されない。

B.4.2.3 攻撃能力の計算

2033 表 3 は、前の節で説明した要因を識別し、各要因の絶対的な価値に数値を関連付けている。

2034 要因が範囲の境界に近づくとき、評価者は、表のそれらの中間値を使用するように考慮すべきである。例えば、攻撃を実行するために 20 のサンプルが必要である場合は、その要因に対して 1 と 4 の間の値を選択してよい。あるいは、公開の場で利用できる設計に基づいた設計に対して開発者が変更を加えている場合は、それらの設計変更の影響についての開発者の見解に従って、0 と 3 の間の値が選択されるべきである。この表は、ガイドとして示されている。

2035 表内の「**」の仕様は、***機会***を考慮した場合、この要因に関して前述した箇所に示されている時間目盛から導けるものとはみなされない。これらの仕様は、意図された運用環境にある TOE で特定の理由により潜在的脆弱性を悪用できないことを識別する。例えば、定期巡回が行われるような既知の環境(つまりシステムの場合)の TOE で、TOE へのアクセスは一定時間で検出されるが、攻撃者がその 2 週間の非検出期間中に TOE にアクセスできなかった場合が挙げられる。ただし、TOE がネットワークに接続されてリモートアクセスが可能である場合、または TOE の物理的な環境が不明である場合には、これが当てはまらないであろう。

要因	値
所要時間	
<= 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	
しろうと	0
熟練者	3*(1)
エキスパート	6
複数のエキスパート	8
TOE の知識	
公開	0
制限的	3
機密	7
危機的	11
機会	
不必要/無制限のアクセス	0
容易	1
中	4
困難	10
なし	**(2)
機器	
標準	0
特殊	4(3)
特別注文	7
複数の特別注文	9

(1)攻撃経路を完全なものにするために複数の熟練者が必要になる場合でも、その専門知識レベルは依然として「熟練者」にとどまる(レート付けの値が 3 になる)。
(2)TOE の意図する運用環境におけるその他の手段のために、攻撃経路が悪用可能でないことを示す。
(3)攻撃の各ステップに対処するために、特殊機器で構成された、通常とは明らかに異なるテストベンチが必要になる場合、これは「特別注文」としてレート付けされるべきである。

表 3　攻撃能力の計算

2036 識別された潜在的脆弱性に対するTOEの抵抗力を決定するために、次のステップを適用するべきである:

a) 運用環境の TOE に対して実行可能な攻撃シナリオ{AS1, AS2, ..., ASn}を定義する。

b) 各攻撃シナリオについて、論理的分析を実行し、表 3 を使用して該当する攻撃能力を計算する。

c) 必要な場合は、各攻撃シナリオについて、論理的分析を確認または反証するために侵入テストを実行する。

d) すべての攻撃シナリオ{AS1, AS2, ..., ASn}を 2 つのグループに分ける:

1) 成功した攻撃シナリオ(すなわち、SFR の侵害に成功した攻撃シナリオ)。

2) 成功しないことが実証された攻撃シナリオ。

e) 成功した攻撃シナリオの各々に対して表 4 を適用し、TOE の抵抗力と選択した AVA_VAN保証コンポーネントとの間に矛盾がないか確認する。表 4 の最後の列を参照のこと。

f) 矛盾が 1 つでも見つかった場合、脆弱性評定は不合格になる。例えば、ST の作成者がAVA_VAN.5コンポーネントを選択し、21 ポイント(高)の攻撃能力を持つ攻撃シナリオが TOE のセキュリティを侵害したとする。この場合、TOE は「中」の攻撃力を持つ攻撃者に対する抵抗力がある。これはAVA_VAN.5に矛盾するため、脆弱性評定は不合格になる。

2037 表 4 の「値」列は、SFR を侵害する攻撃シナリオの攻撃能力値(表 3 を使用して計算されたもの)の範囲を示している。

値	シナリオの悪用に必要な攻撃能力	TOE は、次の攻撃能力を持つ攻撃者に対抗する	満たされる保証コンポーネント	不合格になるコンポーネント
0-9	基本	レート付けなし	-	AVA_VAN.1、AVA_VAN.2、AVA_VAN.3、AVA_VAN.4、AVA_VAN.5
10-13	強化基本	基本	AVA_VAN.1、AVA_VAN.2	AVA_VAN.3、AVA_VAN.4、AVA_VAN.5
14-19	中	強化基本	AVA_VAN.1、AVA_VAN.2、AVA_VAN.3	AVA_VAN.4、AVA_VAN.5
20-24	高	中	AVA_VAN.1、AVA_VAN.2、AVA_VAN.3、AVA_VAN.4	AVA_VAN.5
=>25	高より上	高	AVA_VAN.1、AVA_VAN.2、AVA_VAN.3、AVA_VAN.4、AVA_VAN.5	-

表 4　脆弱性及び TOE 抵抗力のレート付け

2038 このような手法は、すべての状況または要因を考慮することはできないが、標準的なレート付けを行うために必要となる攻撃への抵抗力の明確なレベルを示すはずである。起きることがないような機会への依存などのその他の要因は、この基本モデルに含まれていないが、評価者は、この基本モデルが示す以外のレート付けの根拠を示すために、それらを使用することができる。

2039 個別にレート付けされる多数の脆弱性は、攻撃への高い抵抗力を示すのに対して、複数の脆弱性の組み合わせは低い全体的レート付けが適用されることを示すことがあるので注意されるべきである。1 つの脆弱性の存在が、別の脆弱性の悪用を容易にすることもある。

2040 PP/ST の作成者が、攻撃能力表を使用して TOE が耐え得るべき攻撃レベルを決定する場合(脆弱性分析(AVA_VAN)コンポーネントの選択)、次のように進めるべきである。SFR を侵害してはいけない、すべての異なる攻撃シナリオ（すなわち、すべての異なるタイプの攻撃者、そして/または、作成者が考えているのとは異なる攻撃のタイプ）に対して、そのような成功しない各攻撃シナリオに想定される攻撃能力の様々な値を決定するために、表 3 による分析を何度か行うべきである。PP/ST 作成者は、表 4 から主張される TOE 抵抗力レベルを決定するために、それらの最高値を選ぶ。TOE 抵抗は少なくとも、この最高値と等しくなければならない。PP/ST 作成者は、表 4 から主張される TOE 抵抗力レベルを決定するために、それらの最高値を選ぶ。TOE 抵抗力は少なくとも、この最高値と等しくなければならない。例えば、TOE セキュリティ方針を侵害してはいけない、そのような方法で決定しているすべての攻撃シナリオの、攻撃の可能性の最高値は中である。したがって、TOE 抵抗力は少なくとも中(すなわち、中か高)であるとする。ゆえに、PP/ST 作者は適切な保証コンポーネントとして AVA_VAN.4 (中に対し)か AVA_VAN.5 のどちらか(高に対し)を選ぶことができる。

B.5 直接攻撃の計算例

2041 直接攻撃の対象となるメカニズムは、多くの場合システムのセキュリティにとって極めて重要であり、開発者は多くの場合これらのメカニズムを強化する。例えば、TOE は、別のユーザのパス番号を繰り返し推測する機会を持つ攻撃者によって破られる可能性がある簡単なパス番号認証メカニズムを使用する可能性がある。システムは、パス番号とその使用を様々な方法で制限することによって、このメカニズムを強化できる。評価の途中で、この直接攻撃の分析が次のように進められる可能性がある:

2042 ST 及び設計証拠から収集された情報が、識別と認証が広く分散された端末からのネットワーク資源へのアクセスを制御するための基礎を提供していることを示している。端末への物理的アクセスは、効果的な手段で制御されていない。端末へのアクセスの期間は、効果的な手段で制御されていない。システムの許可利用者は、最初にシステムを使用することを許可されるとき及びそれ以降の利用者による要求により、自分のパス番号を選択する。システムは、利用者が選択するパス番号に次の制限を設けている:

a) パス番号は、4 桁から 6 桁の間でなければならない;

b) 連続する数字シーケンス(7、6、5、4、3 など)は許されない;

c) 数字の繰返しは許されない(各数字は、一意であること)。

2043 パス番号を選択するとき利用者には次のようなガイダンスが行われる。パス番号はできる限りランダムであるべきである、及び、誕生日など、いずれにしても利用者に関係があるべきでない。

2044 パス番号スペースは、次のように計算される:

a) 人間の使用パターンは、パスワードスペースを探す手法に影響を与える可能性がある重要な考慮事項である。最悪のケースのシナリオを想定し、利用者が 4 桁だけで構成される数字を選択する場合、各数字が一意であると仮定するときのパス番号の順列の個数は、次のとおりである:

$$7(8)(9)(10) = 5040$$

b) 増えていくシーケンスは 7 通り可能であり、減っていくシーケンスも同じである。シーケンスを不許可とした後のパス番号スペースは、次のようになる:

$$5040 - 14 = 5026$$

2045 設計証拠から集められたさらなる情報によると、パス番号メカニズムには、端末ロッキングという特徴が備わって設計されている。6 回目の認証の試みが失敗したとき、端末は 1 時間ロックされる。失敗した認証カウントは、5 分後にリセットされるので、攻撃者は、最大で 5 分ごとに 5 回、言い換えると、1 時間に 60 のパス番号の入力を試みることができる。

2046 平均して、攻撃者は、正しいパス番号を入力するまでに、2513 分に 2513 のパス番号を入力する必要があるであろう。平均的な成功する攻撃は、その結果、以下よりもわずかに短い時間で発生するであろう:

$$\frac{2513min}{60\frac{min}{hour}} \approx 42hours$$

2047 前のセクションで記述した攻撃能力を計算する手法を使用することにより、しろうとが、(TOE に簡単にアクセスできる場合は)数日以内に、標準の機器を使用して、TOE の知識なしに、メカニズムを打ち負かすことが可能であり、値は、1 となることを識別する。結果の合計が1である場合、攻撃が成功するために必要な攻撃能力は、基本とみなされる攻撃能力未満になるため、レート付けされない。