



情報技術セキュリティ評価のための 共通方法論

CEM-99/045

パート 2 :
評価方法論

バージョン 1.0
1999 年 8 月

平成 13 年 2 月翻訳第 1.0 版
情報処理振興事業協会
セキュリティセンター

IPA まえがき

本書の目的

本書は、「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(Common Criteria for Information Technology Security Evaluation)」を基にした評価に関するガイドである「Common Methodology for Information Technology Security Evaluation (CEM)」を日本語訳したものである。本書は、情報処理振興事業協会(略称 IPA)におけるセキュリティ評価・認証プロジェクトの評価技術タスクフォース(略称 CCTF)において、評価作業のための補助資料として作成されたものである。したがって、本翻訳書は、セキュリティ評価方法の基準書ではないが、情報セキュリティに関心をもつ人にとって、CC、CEM を理解するための参考資料として役立つことも期待している。

使用上の注意

本書は、用語、記述内容等に不備がある可能性がある。疑問点については下記に記載した CEM で確認していただきたい。本書は、参照利用されることのみを目的とし、本書の改変、及び他への転載は禁止する。

参考文献

Common Methodology for Information Technology Security Evaluation (CEM)

Part1: Introduction and general model Version 0.6 97/01/11 CEM-97/017

Part2: Evaluation Methodology Version 1.0 August 1999 CEM-99/045

掲載ホームページアドレス <http://csrc.nist.gov/cc/cem/cemlist.htm>

Common Criteria for Information Technology Security Evaluation (CC)

Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

掲載ホームページアドレス <http://csrc.nist.gov/cc/ccv20/ccv2list.htm>

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 2.1

パート 1：概説と一般モデル 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

パート 2：セキュリティ機能要件 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

パート 3：セキュリティ保証要件 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

著作権について

本書がベースにしている CEM の著作権は、以下に示す 7 つの政府機関 (“the Common Criteria Project Sponsoring Organizations” と総称) が有している。したがって、CEM の使用、複製、配布、及び改変の権利は、the Common Criteria Project Sponsoring Organizations にある。情報処理振興事業協会は、CEM を日本語翻訳し、参照利用のみを目的として公開することを、the Common Criteria Project Sponsoring Organizations より許可された。

The Common Criteria Project Sponsoring Organizations:

- Canada: Communications Security Establishment
- France: Service Central de la Securite des Systemes d’Information
- Germany: Bundesamt fur Sicherheit in der Informationstechnik
- Netherlands: Netherlands National Communications Security Agency
- United Kingdom: Communications-Electronics Security Group
- United States: National Institute of Standards and Technology
- United States: National Security Agency

まえがき

この文書、「情報技術セキュリティ評価のための共通方法論 (Common Methodology for Information Technology Security Evaluation : CEM)」 第 1.0 版は、国際 IT セキュリティ評価コミュニティによる使用のために発行されている。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 (Common Criteria for Information Technology Security Evaluation : CC)」 と対をなす文書であり、広範囲な国際協力の結果物である。評価によって得られた実際の経験、及び受け取った解釈の要求は、CEM のさらなる発展に使用される。

CEM のオブザベーション報告用のテンプレートは、この文書の最後に添付されている。あらゆるオブザベーション報告書は、以下に示す 1 つまたはいくつかのスポンサー組織の連絡先に提出されるべきである。

カナダ :

Communications Security Establishment
Canadian Common Criteria Evaluation and
Certification Scheme
P.O. Box 9703, Terminal
Ottawa, Ontario, Canada K1G 3Z4
Tel:+1.613.991.7543, Fax:+1.613.991.7455
E-mail:criteria@cse-cst.gc.ca
WWW:<http://www.cse-cst.gc.ca/cse/english/cc.html>

ドイツ :

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Abteilung V
Postfach 20 03 63
D-53133 Bonn, Germany
Tel:+49.228.95820.300, Fax:+49.228.9582.427
E-mail:cc@bsi.de
WWW:<http://www.bsi.de/cc>

英国 :

Communications-Electronics Security Group
Compusec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE, United Kingdom
Tel:+44.1242.221.491 ext.5257,
Fax:+44.1242.252.291
E-mail:criteria@cesg.gov.uk
WWW:<http://www.cesg.gov.uk/cchtml>
FTP:<ftp://ftp.cesg.gov.uk/pub>

米国 - NSA :

National Security Agency
Attn:V1, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755-6740,
U.S.A.
Tel:+1.410.854.4458, Fax:+1.410.854.7512
E-mail:common_criteria@radium.ncsc.mil
WWW:<http://www.radium.ncsc.mil/tpep/>

フランス :

Service Central de la Sécurité des Systèmes
d'Information (SCSSI)
Centre de Certification de la Sécurité des
Technologies de l'Information
18, rue du docteur Zamenhof
F-92131 Issy les Moulineaux, France
Tel:+33.1.41463784, Fax:+33.1.41463701
E-mail:ssi20@calva.net
WWW:<http://www.scssi.gouv.fr>

オランダ :

Netherlands National Communications Security
Agency
P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel:+31.70.3485637, Fax:+31.70.3486503
E-mail:criteria@nlncsa.minbuza.nl
WWW:<http://www.tno.nl/instit/fel/refs/cc.html>

米国 - NIST :

National Institute of Standards and Technology
Computer Security Division
100 Bureau Drive, MS: 8930
Gaithersburg, Maryland 20899, U.S.A.
Tel:+1.301.975.5390, Fax:+1.301.948.0279
E-mail:criteria@nist.gov
WWW:<http://csrc.nist.gov/cc>

目次

1 章 序説	1
1.1 有効範囲.....	1
1.2 構成.....	1
1.3 文書の表記規則.....	2
1.3.1 用語.....	2
1.3.2 動詞の使用.....	3
1.3.3 一般的評価ガイダンス.....	3
1.3.4 CC 構造と CEM 構造間の関係.....	3
1.4 評価者の判定.....	5
2 章 一般的評価タスク	7
2.1 序説.....	7
2.2 評価入力タスク.....	7
2.2.1 目的.....	7
2.2.2 適用上の注釈.....	7
2.2.3 評価証拠サブタスクの管理.....	8
2.3 評価出力タスク.....	9
2.3.1 目的.....	9
2.3.2 適用上の注釈.....	9
2.3.3 OR サブタスクを記述する.....	9
2.3.4 ETR サブタスクを記述する.....	10
2.4 評価サブアクティビティ.....	17
3 章 PP 評価	19
3.1 序説.....	19
3.2 目的.....	19
3.3 PP 評価関係.....	19
3.4 PP 評価アクティビティ.....	20
3.4.1 TOE 記述の評価 (APE_DES.1)	20
3.4.2 セキュリティ環境の評価 (APE_ENV.1)	21
3.4.3 PP 概説の評価 (APE_INT.1)	24
3.4.4 セキュリティ対策方針の評価 (APE_OBJ.1)	26
3.4.5 IT セキュリティ要件の評価 (APE_REQ.1)	30
3.4.6 明示された IT セキュリティ要件の評価 (APE_SRE.1)	40
4 章 ST 評価	43
4.1 序説.....	43
4.2 目的.....	43
4.3 ST 評価関係.....	43
4.4 ST 評価アクティビティ.....	45
4.4.1 TOE 記述の評価 (ASE_DES.1)	45

4.4.2	セキュリティ環境の評価 (ASE_ENV.1)	47
4.4.3	ST 概説の評価 (ASE_INT.1)	49
4.4.4	セキュリティ対策方針の評価 (ASE_OBJ.1)	52
4.4.5	PP 主張の評価 (ASE_PPC.1)	55
4.4.6	IT セキュリティ要件の評価 (ASE_REQ.1)	57
4.4.7	明示された IT セキュリティ要件の評価 (ASE_SRE.1)	67
4.4.8	TOE 要約仕様の評価 (ASE_TSS.1)	69
5 章	EAL1 評価	74
5.1	導入	74
5.2	目的	74
5.3	EAL1 評価関係	74
5.4	構成管理アクティビティ	75
5.4.1	CM 能力の評価 (ACM_CAP.1)	75
5.5	配付及び運用アクティビティ	77
5.5.1	設置、生成及び立上げの評価 (ADO_IGS.1)	77
5.6	開発アクティビティ	79
5.6.1	適用上の注釈	79
5.6.2	機能仕様の評価 (ADV_FSP.1)	79
5.6.3	表現対応の評価 (ADV_RCR.1)	85
5.7	ガイダンス文書アクティビティ	86
5.7.1	適用上の注釈	86
5.7.2	管理者ガイダンスの評価 (AGD_ADM.1)	86
5.7.3	利用者ガイダンスの評価 (AGD_USR.1)	90
5.8	テストアクティビティ	93
5.8.1	適用上の注釈	93
5.8.2	独立テストの評価 (ATE_IND.1)	93
6 章	EAL2 評価	99
6.1	導入	99
6.2	目的	99
6.3	EAL2 評価関係	99
6.4	構成管理アクティビティ	101
6.4.1	CM 能力の評価 (ACM_CAP.2)	101
6.5	配付及び運用アクティビティ	104
6.5.1	配付の評価 (ADO_DEL.1)	104
6.5.2	設置、生成及び立上げの評価 (ADO_IGS.1)	107
6.6	開発アクティビティ	109
6.6.1	適用上の注釈	109
6.6.2	機能仕様の評価 (ADV_FSP.1)	110
6.6.3	上位レベル設計の評価 (ADV_HLD.1)	116
6.6.4	表現対応の評価 (ADV_RCR.1)	120
6.7	ガイダンス文書アクティビティ	122
6.7.1	適用上の注釈	122
6.7.2	管理者ガイダンスの評価 (AGD_ADM.1)	122
6.7.3	利用者ガイダンスの評価 (AGD_USR.1)	126
6.8	テストアクティビティ	129

目次

6.8.1	適用上の注釈.....	129
6.8.2	カバレッジの評価 (ATE_COV.1)	129
6.8.3	機能テストの評価 (ATE_FUN.1)	132
6.8.4	独立テストの評価 (ATE_IND.2)	137
6.9	脆弱性評価アクティビティ	145
6.9.1	TOE セキュリティ機能強度の評価 (AVA_SOF.1)	145
6.9.2	脆弱性分析の評価 (AVA_VLA.1)	149
7章	EAL3 評価	155
7.1	導入.....	155
7.2	目的.....	155
7.3	EAL3 評価関係	155
7.4	構成管理アクティビティ	157
7.4.1	CM 能力の評価 (ACM_CAP.3)	157
7.4.2	CM 範囲の評価 (ACM_SCP.1)	162
7.5	配付及び運用アクティビティ	164
7.5.1	配付の評価 (ADO_DEL.1)	164
7.5.2	設置、生成及び立上げの評価 (ADO_IGS.1)	167
7.6	開発アクティビティ	169
7.6.1	適用上の注釈.....	169
7.6.2	機能仕様の評価 (ADV_FSP.1)	170
7.6.3	上位レベル設計の評価 (ADV_HLD.2)	176
7.6.4	表現対応の評価 (ADV_RCR.1)	181
7.7	ガイダンス文書アクティビティ	183
7.7.1	適用上の注釈.....	183
7.7.2	管理者ガイダンスの評価 (AGD_ADM.1)	183
7.7.3	利用者ガイダンスの評価 (AGD_USR.1)	187
7.8	ライフサイクルサポートアクティビティ	190
7.8.1	開発セキュリティの評価 (ALC_DVS.1)	190
7.9	テストアクティビティ	194
7.9.1	適用上の注釈.....	194
7.9.2	カバレッジの評価 (ATE_COV.2)	196
7.9.3	深さの評価 (ATE_DPT.1)	199
7.9.4	機能テストの評価 (ATE_FUN.1)	202
7.9.5	独立テストの評価 (ATE_IND.2)	207
7.10	脆弱性評価アクティビティ	215
7.10.1	誤使用の評価 (AVA_MSU.1)	215
7.10.2	TOE セキュリティ機能強度の評価 (AVA_SOF.1)	219
7.10.3	脆弱性分析の評価 (AVA_VLA.1)	223
8章	EAL4 評価	229
8.1	序説.....	229
8.2	目的.....	229
8.3	EAL4 評価関係	229
8.4	構成管理アクティビティ	231
8.4.1	CM 自動化の評価 (ACM_AUT.1)	231
8.4.2	CM 能力の評価 (ACM_CAP.4)	234

8.4.3	CM 範囲の評価 (ACM_SCP.2)	240
8.5	配付及び運用アクティビティ	242
8.5.1	配付の評価 (ADO_DEL.2)	242
8.5.2	設置、生成及び立上げの評価 (ADO_IGS.1)	245
8.6	開発アクティビティ	247
8.6.1	適用上の注釈	247
8.6.2	機能仕様の評価 (ADV_FSP.2)	248
8.6.3	上位レベル設計の評価 (ADV_HLD.2)	254
8.6.4	実装表現の評価 (ADV_IMP.1)	259
8.6.5	下位レベル設計の評価 (ADV_LLD.1)	262
8.6.6	表現対応の評価 (ADV_RCR.1)	266
8.6.7	セキュリティ方針モデリングの評価 (ADV_SPM.1)	268
8.7	ガイダンス文書アクティビティ	272
8.7.1	適用上の注釈	272
8.7.2	管理者ガイダンスの評価 (AGD_ADM.1)	272
8.7.3	利用者ガイダンスの評価 (AGD_USR.1)	276
8.8	ライフサイクルサポートアクティビティ	279
8.8.1	開発セキュリティの評価 (ALC_DVS.1)	279
8.8.2	ライフサイクル定義の評価 (ALC_LCD.1)	283
8.8.3	ツールと技法の評価 (ALC_TAT.1)	285
8.9	テストアクティビティ	287
8.9.1	適用上の注釈	287
8.9.2	カバレッジの評価 (ATE_COV.2)	289
8.9.3	深さの評価 (ATE_DPT.1)	292
8.9.4	機能テストの評価 (ATE_FUN.1)	295
8.9.5	独立テストの評価 (ATE_IND.2)	300
8.10	脆弱性評価アクティビティ	308
8.10.1	誤使用の評価 (AVA_MSU.2)	308
8.10.2	TOE セキュリティ機能強度の評価 (AVA_SOF.1)	313
8.10.3	脆弱性分析の評価 (AVA_VLA.2)	317
附属書 A 用語集		331
A.1	省略語及び頭字語	331
A.2	用語	331
A.3	参照資料	333
附属書 B 一般的評価ガイダンス		335
B.1	目的	335
B.2	サンプリング	335
B.3	一貫性分析	338
B.4	依存性	340
B.4.1	アクティビティの間の依存性	340
B.4.2	サブアクティビティの間の依存性	340
B.4.3	アクションの間の依存性	340
B.5	サイト訪問	341
B.6	TOE 境界	342
B.6.1	製品及びシステム	342

目次

B.6.2	TOE.....	342
B.6.3	TSF.....	342
B.6.4	評価.....	342
B.6.5	認証.....	343
B.7	脅威及び FPT 要件.....	344
B.7.1	FPT クラスを必ずしも必要としない TOE.....	345
B.7.2	保証ファミリへの影響.....	345
B.8	機能強度及び脆弱性分析.....	346
B.8.1	攻撃能力.....	348
B.8.2	攻撃能力の計算.....	349
B.8.3	機能強度分析の例.....	353
B.9	制度の責任.....	355
附属書 C	CEM オブザベーション報告書の提供.....	357
C.1	序説.....	357
C.2	CEMOR のフォーマット.....	357
C.2.1	オブザベーションの例.....	358

図一覧

図 1.1	CC 構造と CEM 構造の対応付け	4
図 1.2	判定割付規則の例	5
図 2.1	PP 評価用の ETR 情報内容	11
図 2.2	TOE 評価用の ETR 情報内容	14
図 2.3	一般評価モデル	18
図 5.1	TSF インタフェース	81
図 6.1	TSF インタフェース	111
図 6.2	テストカバレッジ証拠の概念的枠組み	131
図 7.1	TSF インタフェース	171
図 7.2	テストカバレッジ分析の概念的枠組み	198
図 7.3	テストの深さ分析の概念的枠組み	201
図 8.1	TSF インタフェース	250
図 8.2	テストカバレッジ分析の概念的枠組み	291
図 8.3	テストの深さ分析の概念的枠組み	294

表一覧

表 B.1	脆弱性の分析及び攻撃能力	347
表 B.2	TOE セキュリティ機能強度と攻撃能力	347
表 B.3	攻撃能力の計算	352
表 B.4	脆弱性のレート付け	353

1章 序説

1.1 有効範囲

- 1 「情報技術セキュリティ評価のための共通方法論 (Common Methodology for Information Technology Security Evaluation : 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 (Common Criteria for Information Technology Security Evaluation : 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記述している。
- 2 このバージョンの有効範囲は、CCに定義されているようにプロテクションプロファイル及びEAL1からEAL4のTOEの評価に制限されている。EAL5からEAL7及びその他の保証パッケージを使用した評価のガイダンスは提供しない。CEMは、CC第2.1版に基づいており、CC Interpretations Management Board (CCIMB)との相互作用の結果によるフィードバックを含む。
- 3 CEMの対象読者は、主にCCを適用する評価者であり、評価者アクションを確認する認証者、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読者が2次対象読者である。
- 4 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。個々の制度により、そのような解釈の処理が決定するが、これらは相互承認協定の対象とすることができる。個々の制度によって処理することができる方法論関連アクティビティの一覧は、附属書B.9に記述されている。
- 5 CEMパート1、v0.6はCEMの一般モデルを定義しているが、現在改定中である。したがって、CEMパート2の内容がCEMパート1と矛盾すると思われる部分についてはパート2が優先する。パート1の将来バージョンは、そのような矛盾を解決するだろう。

1.2 構成

- 6 この部 *CEM* パート2は、以下の章で構成されている。
- 7 1章 *序説* では、目的、構成、文書規則と用語、及び評価者判定を記述する。
- 8 2章 *一般評価タスク* では、すべての評価アクティビティに関連するタスクを記述する。これらは、入力を管理し、出力を準備するために使用されるタスクである。
- 9 3章 *PP評価* では、プロテクションプロファイルの評価方法論をCCパート3のAPEクラスに基づいて記述する。
- 10 4章 *ST評価* では、セキュリティターゲットの評価方法論をCCパート3のASEクラスに基づいて記述する。

- 11 5章から8章では、CCパート3に定義されている評価保証レベル EAL1 から EAL4 の評価方法論を記述する。
- 12 附属書 A *用語集*では、CEM で使用されている用語及び参照を定義し、省略語、頭字語を示す。
- 13 附属書 B *一般評価ガイダンス*では、3章から8章に記述されているいくつかのアクティビティに共通するガイダンスを示す。
- 14 附属書 C *CEM オブザベーション報告書の提供*では、CEM オブザベーション報告書ガイダンス、オブザベーション例、及びオブザベーション報告に使用するテンプレートを提供する。

1.3 文書の表記規則

1.3.1 用語

- 15 この部の附属書 A に記載されている用語集には、本書で特別の方法で使用されている用語だけが含まれている。大部分の用語は、それらの受け入れられている定義に従って使用されている。
- 16 用語「アクティビティ」(*activity*)は、CCパート3の保証クラスの適用を記述するために使用されている。
- 17 用語「サブアクティビティ」(*sub-activity*)は、CCパート3の保証コンポーネントの適用を記述するために使用されている。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。
- 18 用語「アクション」(*action*)は、CCパート3の評価者アクションエレメントに関係している。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。
- 19 用語「ワークユニット」(*work unit*)は、評価作業の最も詳細なレベルである。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 アクション内で証拠または開発者アクションエレメントの CC の内容・提示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 4:ALC_TAT.1-2 などのシンボルにより識別されている。このシンボルの最初の数字 (4) は、EAL を示し、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。
- 20 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。例えば、4:ADV_FSP.2-7 のラベルの付いた追加の

1章 序説

ワークユニットが EAL4 に追加されたために、FSP ワークユニットのその後の順次番号は、1 だけずれている。そこで、ワークユニット 3:ADV_FSP.1-8 は、いまではワークユニット 4:ADV_FSP.2-9 によりミラーされている。それぞれの番号は直接対応しなくなったが、いずれも同じ要件を表す。

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

1.3.2 動詞の使用

- 22 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 *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 *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。

- 23 ガイダンス文を伴うワークユニットとサブタスクは、さらに評価での CC 語の適用方法を説明している。助動詞「すべきである」(*should*) は、記述されている方式が非常に望ましいが他の方法も正当化される場合に使用されている。助動詞「することができる」(*may*) は、いくつかのことが許されるが、優先するものが示されないところで使用されている。

- 24 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、用語集が参照されるべきである。

1.3.3 一般的評価ガイダンス

- 25 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 B 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。

1.3.4 CC 構造と CEM 構造間の関係

- 26 CC 構造（すなわち、クラス、ファミリー、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 1.1 は、クラス、コンポーネント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の結果である。

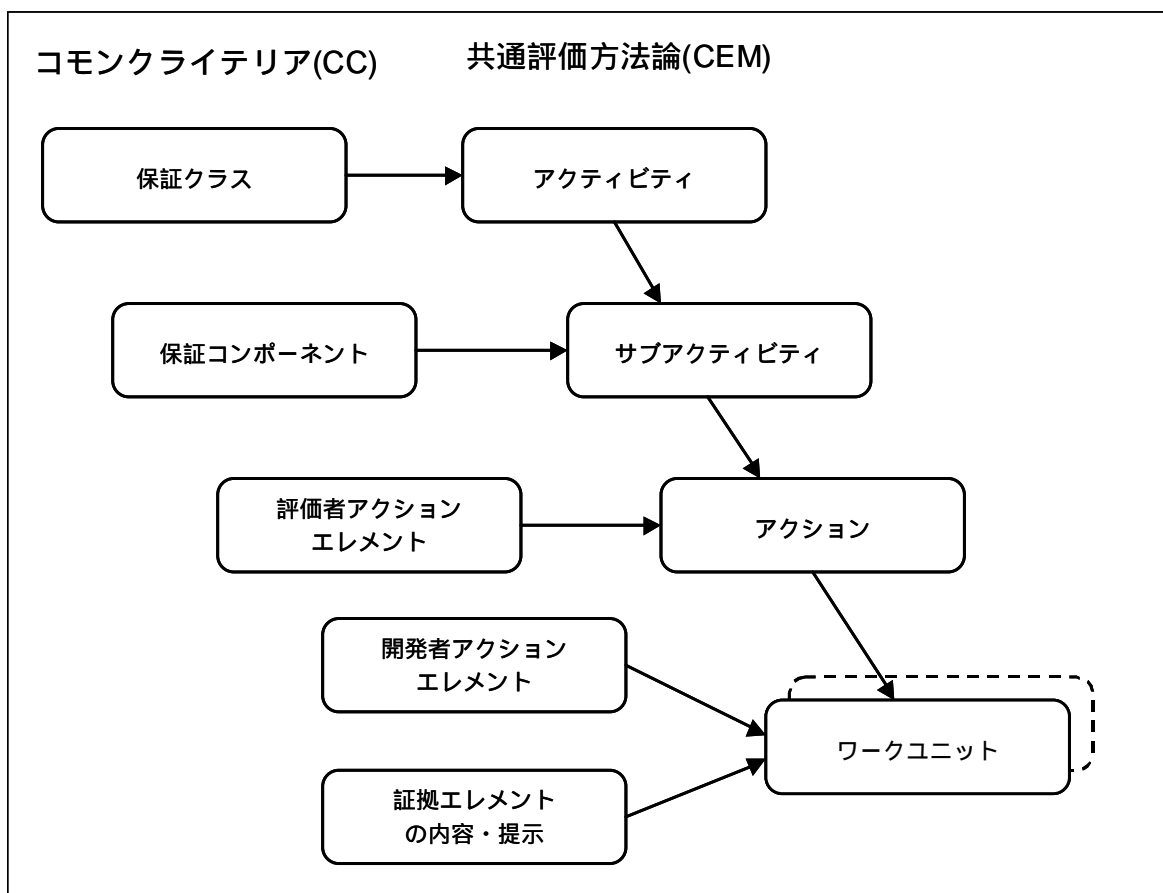


図 1.1 CC 構造と CEM 構造の対応付け

1.4 評価者の判定

27 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、5.3 節の記述に従って、評価結果が割り付けられる。

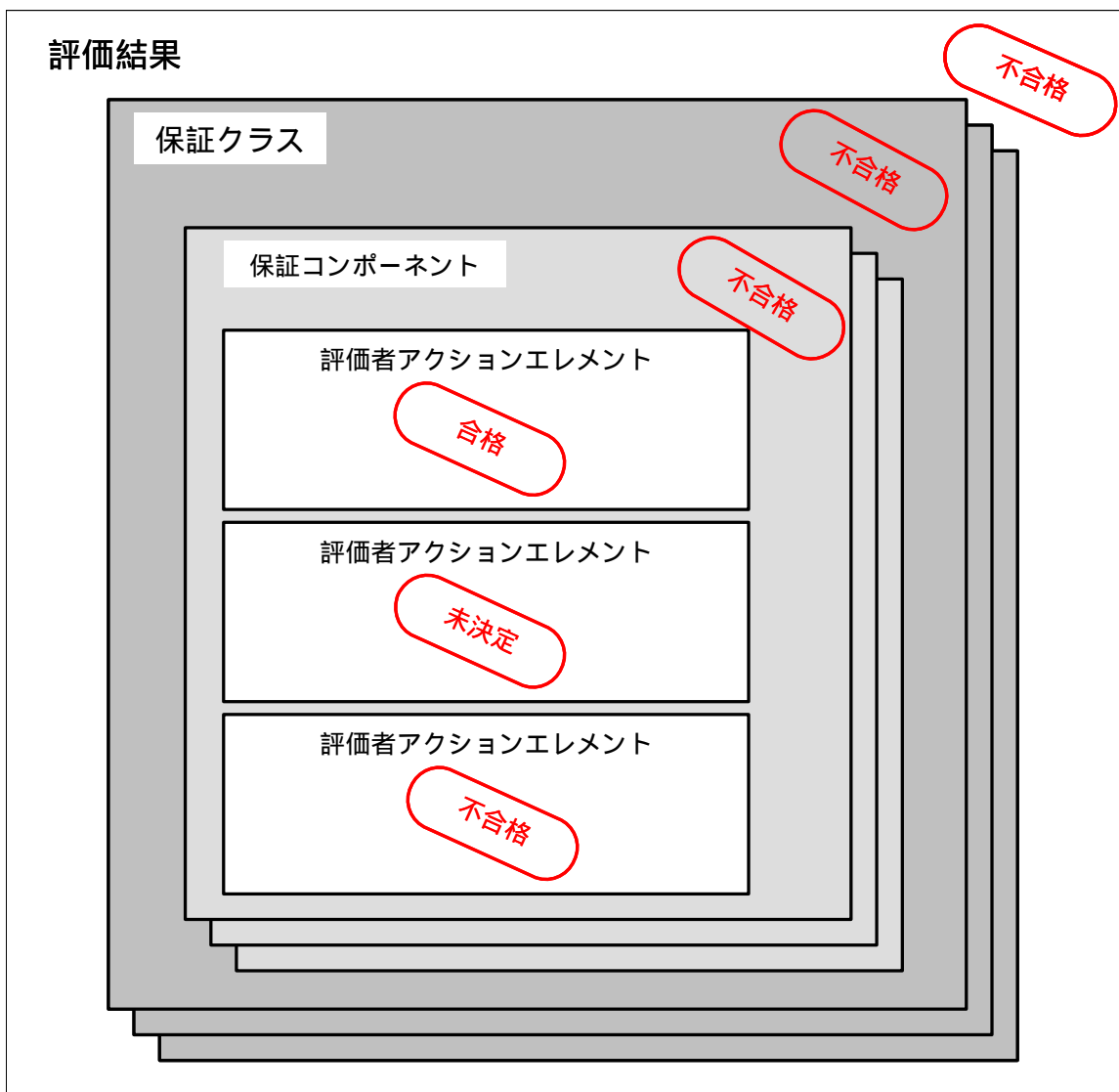


図 1.2 判定割付規則の例

28 CEM は、次の 3 つの相互に排他的な判定状態を認識する。

- 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と定義される。エレメントが合格するための条件は、関係する CEM アクションの構成要素ワークユニットとして定義される。

- b) 「未決定」(*inconclusive*) 判定の条件は、CC 評価者アクションエレメントに
関係する CEM アクションの 1 つまたはいくつかのワークユニットを評価者が
完了していないことと定義される。
- c) 「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
を決定したことと定義される。

29 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下されるまでそ
のままになっている。

30 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 1.2
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。

2章 一般的評価タスク

2.1 序説

31 全ての評価には、PP または TOE (ST を含む) の評価にかかわらず入力タスクと出力タスクの 2 つの共通なタスクがある。これら 2 つのタスクは、評価証拠の管理及び報告作成に関連しており、この章で記述されている。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、規範となる関連付けられたサブタスクがある。

32 CC ではこれらの評価タスクに対して特定の要件を必要としないが、CEM のパート 1 で定義されている普遍的な原則への適合を保証するために必要であるため、CEM では必須である。CEM のこの部以外に記述されているアクティビティとは異なり、これらのタスクは CC 評価者アクションエレメントにマッピングしないため、関連する判定を持たず、CEM に従うために実行される。

2.2 評価入力タスク

2.2.1 目的

33 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、繰り返し可能で、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。

2.2.2 適用上の注釈

34 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。

35 評価者がスポンサーと共に必要な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。

36 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。

37 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る場合があるが、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場合がある。

- 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。

38 評価証拠草案は、開発と共に 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 の評価中に使用される場合もある。

2.2.3 評価証拠サブタスクの管理

2.2.3.1 構成制御

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

40 CC 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。

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

2.2.3.2 廃棄

42 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つまたはいくつか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

2.2.3.3 機密性

43 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。

44 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。

2章 一般的評価タスク

2.3 評価出力タスク

2.3.1 目的

45 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必要とする場合、あるいは追加情報を OR または ETR に含めることを必要とする場合がある。CEM はこれらの報告への情報の追加を排除しない。CEM は最低限の情報を示しているだけである。

46 一貫した評価結果の報告により、結果の繰り返し可能性及び再現可能性における普遍的な原則を容易に得ることができる。この一貫性には、ETR 及び OR で報告される情報の種類及び量が対象となる。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、監督者の責任である。

47 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

2.3.2 適用上の注釈

48 CEM のこのバージョンでは、再評価及び再使用を裏付ける評価者証拠の規定のため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において支援する評価者作業によって得られる情報はまだ決定されていない。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、評価が実行される元になる制度が参照されるべきである。

2.3.3 OR サブタスクを記述する

49 OR は、明確化を要求する（例えば、要件の適用の監督者から）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評価者に提供する。

50 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**。

51 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することもできる。

52 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) 厳正さの評定（例えば、不合格判定の暗示、評価に対する進行の延期、評価が完了する前に解決を要求）

- 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

53 OR の対象読者及び報告を処理する手続きは、報告の内容及び制度の性質に依存する。制度は、OR の異なる種類を区別し、あるいは追加の種類を、必要な情報及び配付に関連する違いによって（例えば、評価 OR を監督者及びスポンサーに）定義することができる。

2.3.4 ETR サブタスクを記述する

2.3.4.1 目的

54 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**。

55 ETR には開発者またはスポンサーが著作権を持つ情報が含まれる場合がある。

56 CEM は ETR の最低の内容要件を定義するが、制度で追加の内容及び特定の表象的及び構造的要件を指定することができる。例えば、制度は特定の予備材料（例えば、権利の放棄、及び著作権条項）を ETR 内で報告することを要件とする場合がある。

57 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。

58 ETR は監督判定を提供する際に監督者を支援するが、監督に必要な情報のすべてを提供しない場合があり、提出された証拠資料の結果が要求された基準に対して評価が実行されたことを制度が確認するために必要な証拠を提供しない場合があることが予想される。この局面は CEM の適用範囲外であり、その他の監督方法を使用して満たされるべきである。

2.3.4.2 PP 評価用の ETR

59 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 2.1 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。

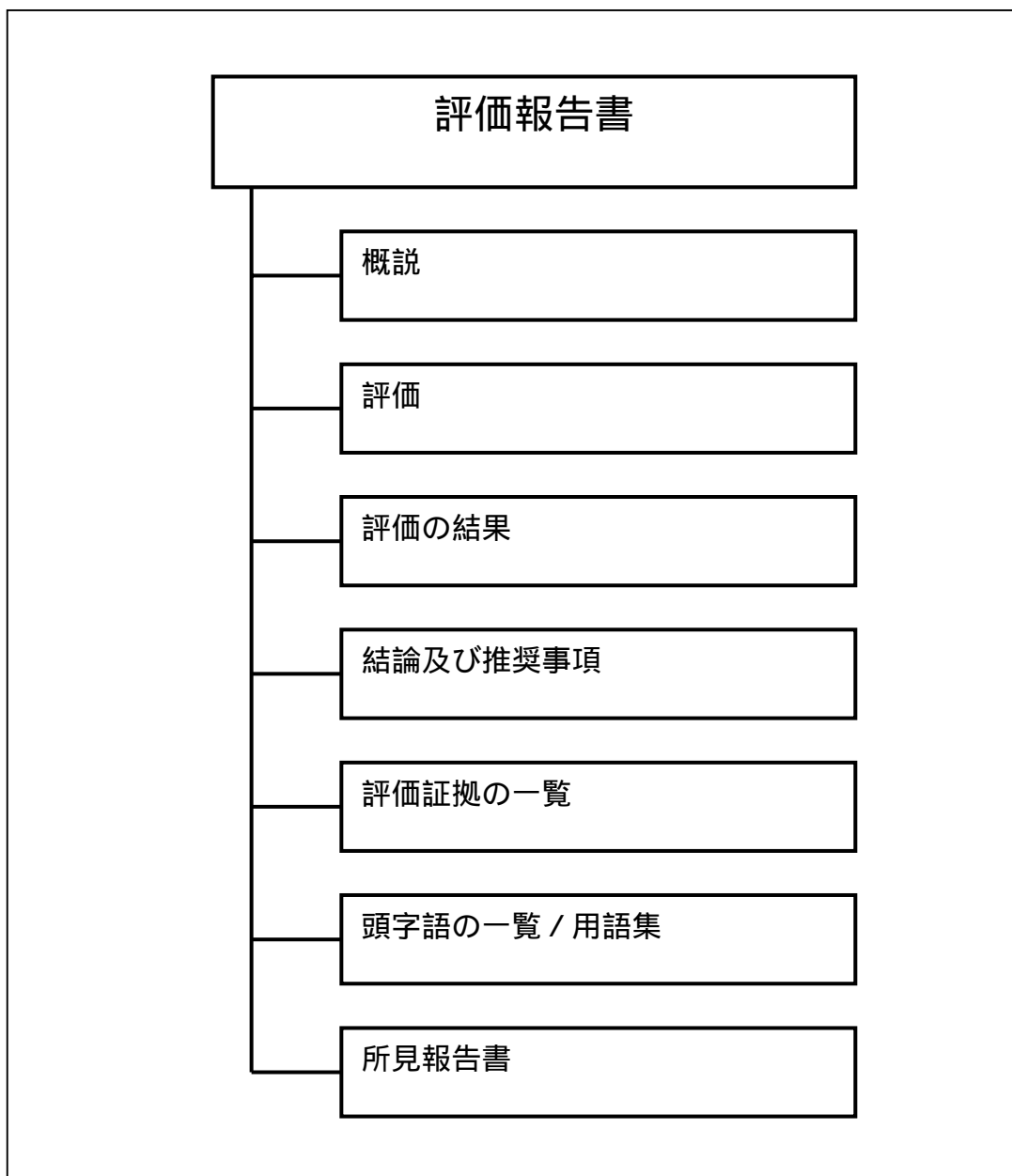


図 2.1 PP 評価用の ETR 情報内容

2.3.4.2.1

序説

60

評価者は、評価制度識別情報を **報告しなければならない**。

61

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。

62

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**。

63

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。

64

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**。

65 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監督者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。

66 評価者は、開発者の識別を **報告しなければならない**。

67 PP 開発者の識別は、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。

68 評価者は、スポンサーの識別を **報告しなければならない**。

69 スポンサーの識別は、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。

70 評価者は、評価者の識別を **報告しなければならない**。

71 評価者の識別は、評価を実行し、評価証拠に責任がある当事者を識別するために必要である。

2.3.4.2.2 評価

72 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**。

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

74 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**。

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

2.3.4.2.3 評価の結果

76 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**。

77 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なものとし、評価証拠が基準の各局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 ワークユニットのレベル詳細を提供することができる。

2.3.4.2.4 結論及び推奨事項

78 評価者は、評価の結論、特に CC パート 1 の 5 章に定義され、1.4 節の評価者判定に記述されている判定の割付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**。

79 評価者は、監督者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機能についての言及が含まれる場合がある。

2章 一般的評価タスク

2.3.4.2.5 評価証拠の一覧

80 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
- 一意のリファレンス（例えば、発行日及びバージョン番号）

2.3.4.2.6 頭字語の一覧/用語集

81 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**。

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

2.3.4.2.7 所見報告書

83 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**。

84 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。

2.3.4.3 TOE 評価用の ETR

85 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 2.2 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。

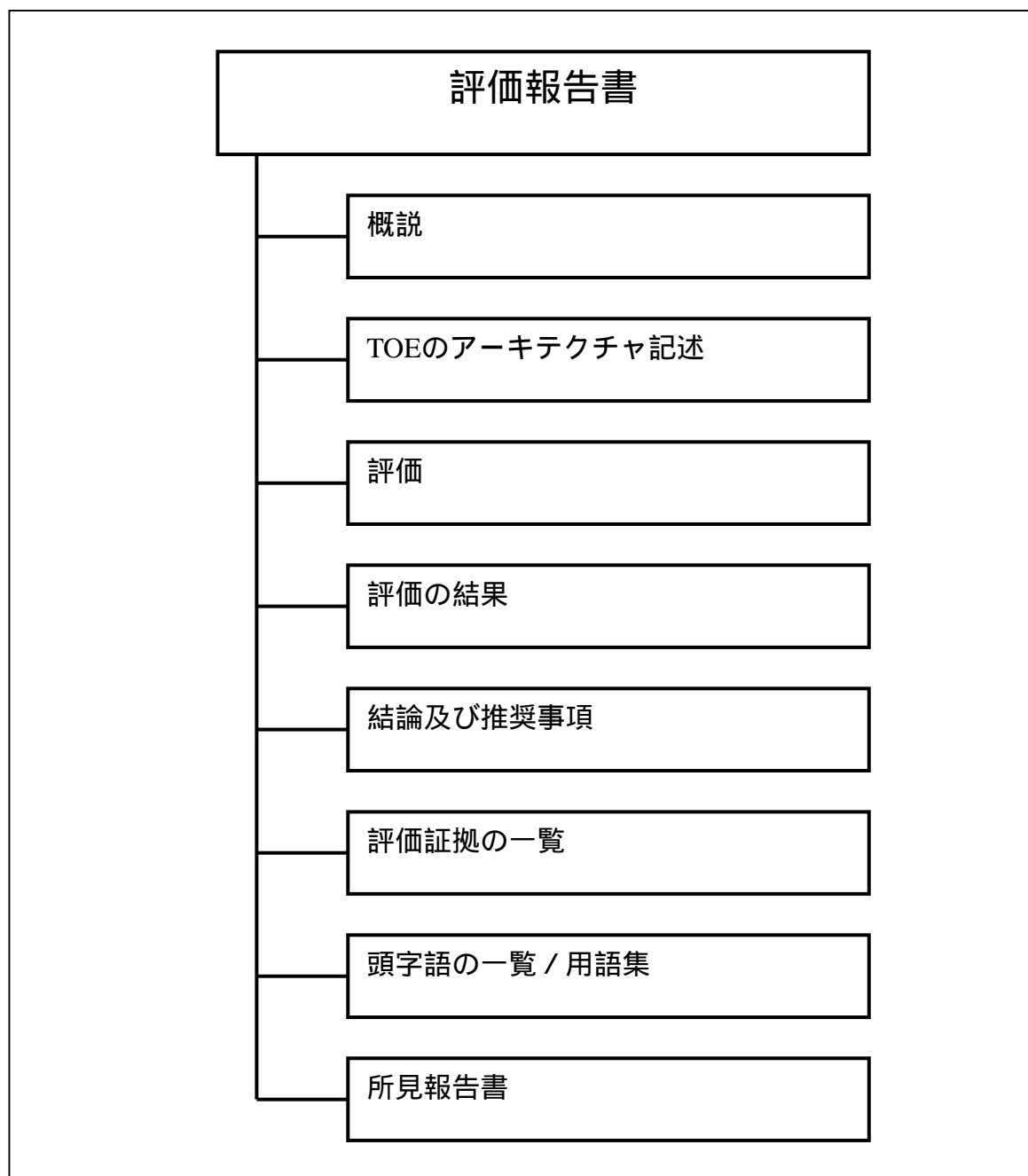


図 2.2 TOE 評価用の ETR 情報内容

2.3.4.3.1 序説

86 評価者は、評価制度識別情報を **報告しなければならない**。

87 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。

88 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**。

2章 一般的評価タスク

- 89 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。
- 90 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**。
- 91 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監督者が検証するために評価対象を識別する。
- 92 TOE が 1 つまたは複数の PP 要件を満たしていることを ST が求める場合、ETR は対応する PP 参照を **報告しなければならない**。
- 93 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。
- 94 評価者は、開発者の識別を **報告しなければならない**。
- 95 TOE 開発者の識別は、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。
- 96 評価者は、スポンサーの識別を **報告しなければならない**。
- 97 スポンサーの識別は、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。
- 98 評価者は、評価者の識別を **報告しなければならない**。
- 99 評価者の識別は、評価を実行し、評価証拠に責任がある当事者を識別するために必要である。
- 2.3.4.3.2 TOE のアーキテクチャ記述
- 100 評価者は、該当する場合、"開発 - 上位レベル設計 (ADV_HLD)" 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**。
- 101 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 に上位レベル設計 (ADV_HLD) 要件がない場合、これは適用されないため、満たされているものとみなされる。
- 2.3.4.3.3 評価
- 102 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**。
- 103 評価者は、TOE の評価に使用する評価基準、方法論、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。
- 104 評価者は、あらゆる評価に関する制約、評価結果の配付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**。
- 105 評価者は、法律または法令の側面、組織、機密性などに関する情報を含めることができる。

2.3.4.3.4 評価の結果

106 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

107 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なものとし、評価証拠が基準の各局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 ワークユニットのレベル詳細を提供することができる。

108 評価者は、ワークユニットが明確に必要とするすべての情報を **報告しなければならない**。

109 AVA 及び ATE アクティビティの場合、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る。

2.3.4.3.5 結論及び推奨事項

110 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 5 章に定義され、1.4 節の評価者判定に記述されている判定の割付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**。

111 評価者は、監督者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機能についての言及が含まれる場合がある。

2.3.4.3.6 評価証拠の一覧

112 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
- 一意のリファレンス（例えば、発行日及びバージョン番号）

2.3.4.3.7 頭字語の一覧/用語集

113 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**。

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

2章 一般的評価タスク

2.3.4.3.8 所見報告

- 115 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**。
- 116 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。

2.4 評価サブアクティビティ

- 117 図 2.3 は、評価で実行される作業の概要を提供する。
- 118 評価証拠は、評価の種類によって異なる場合がある（PP 評価は、PP のみを必要とするが、TOE 評価では TOE 特有の証拠を必要とする）。評価出力は ETR または OR になる可能性がある。評価サブアクティビティは多様であり、TOE 評価の場合、CC パート 3 の保証要件に依存する。
- 119 3 章から 8 章の各章は、評価に必要な評価作業に基づいて同様に構成されている。3 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。4 章では、ST に必要な作業について取り扱う。ただし、この作業では分離した評価結果は得られない。5 章から 8 章では、EAL1 から EAL4（ST との組み合わせにおける）の評価結果を得るために必要な作業について取り扱う。これらの各章は、独立したものであるため、他の章に含まれている文章が繰り返し記述されている場合がある。

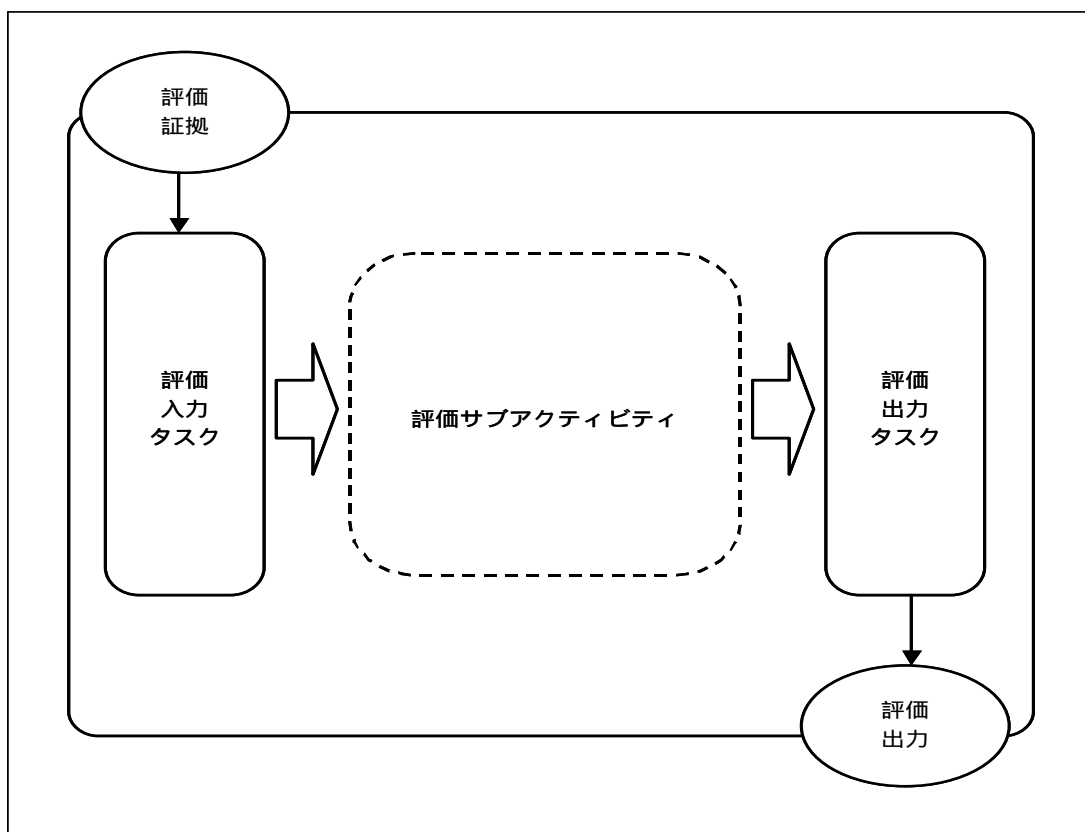


図 2.3 一般評価モデル

3章 PP 評価

3.1 序説

120 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論は、PP で主張されている EAL (またはその他の保証基準セット) に関係なく各 PP 評価で同一である。CEM の以降の章では特定の EAL での評価の実施について記述しているが、この章は評価されるあらゆる PP に適用される。

121 この章の評価方法論は、CC パート 1 の特に附属書 B、及び CC パート 3 の APE クラスに指定されている PP の要件に基づいている。

3.2 目的

122 PP は製品またはシステムの種別の説明である。それ自体定義された組織のセキュリティ方針を強化する IT セキュリティ要件を識別し、定義された前提条件に基づき、定義された脅威に対抗することを期待されている。

123 PP 評価の目的は、PP が以下の点を満たしているかどうかを決定することである。

- a) 完全である。セキュリティ要件によって、それぞれの脅威に対抗し、それぞれの組織のセキュリティ方針が強化されている。
- b) 必要十分である。IT セキュリティ要件は、脅威及び組織のセキュリティ方針に適切である。
- c) 適切である。PP は、内部的に一貫していなければならない。

3.3 PP 評価関係

124 完全な PP 評価を実施するアクティビティは、次のことを扱う。

- a) 評価入力タスク (2 章)
- b) 以下のサブアクティビティを含む PP 評価アクティビティ
 - 1) TOE 記述の評価 (3.4.1 節)
 - 2) セキュリティ環境の評価 (3.4.2 節)
 - 3) PP 概説の評価 (3.4.3 節)
 - 4) セキュリティ対策方針の評価 (3.4.4 節)
 - 5) IT セキュリティ要件の評価 (3.4.5 節)
 - 6) 明示された IT セキュリティ要件の評価 (3.4.6 節)

c) 評価出力タスク (2章)

- 125 評価入力及び評価出力タスクについては 2 章で記述している。評価アクティビティは、CC パート 3 に記載されている APE 保証要件から引き出される。
- 126 PP 評価を構成するサブアクティビティは、この章に記述されている。サブアクティビティは、一般的に、ほぼ同時に開始することができるが、評価者は、サブアクティビティの間のいくつかの依存性を考慮する必要がある。依存性のガイダンスについては、附属書 B.4 を参照のこと。
- 127 明示された IT セキュリティ要件サブアクティビティの評価は、CC パート 2 またはパート 3 から抽出されたものではないセキュリティ要件が IT セキュリティ要件ステートメントに含まれている場合にのみ適用される。

3.4 PP 評価アクティビティ

3.4.1 TOE 記述の評価 (APE_DES.1)

3.4.1.1 目的

- 128 このサブアクティビティの目的は、TOE 記述に TOE の目的及びその機能性の理解の助けとなる関連情報が含まれているかどうか、及び記述が完全で一貫しているかどうかを決定することである。

3.4.1.2 入力

- 129 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

3.4.1.3 評価者アクション

- 130 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。

a) APE_DES.1.1E

b) APE_DES.1.2E

c) APE_DES.1.3E

3.4.1.3.1 アクション APE_DES.1.1E

APE_DES.1.1C

- APE_DES.1-1 評価者は、TOE 記述が TOE の製品またはシステムの種別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**。

- 131 評価者は、TOE 記述が読者に製品またはシステムの意図する使用に対する一般的な理解を提供するに十分であり、評価のための説明を提供していることを決定する。

3章 PP 評価

製品またはシステムの種別の例は、次のとおりである。ファイアウォール、スマートカード、暗号化モデム、ウェブサーバ、イントラネット。

132 製品またはシステムの種別によって明らかにいくつかの機能が TOE に期待される場合がある。この機能がない場合、評価者は TOE 記述にこのことが適切に説明されているかどうかを決定する。この例の 1 つとして、TOE 記述にネットワークに接続されえないことが記述されているファイアウォールタイプの TOE があげられる。

APE_DES.1-2 評価者は、TOE 記述が一般的な用語で TOE の IT 機能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**。

133 評価者は、TOE 記述が IT について、特に TOE によって提供されるセキュリティ機能について、読者がそれらの機能について一般的に理解するために十分に詳細なレベルで説明していることを決定する。

3.4.1.3.2 アクション APE_DES.1.2E

APE_DES.1-3 評価者は、TOE 記述が理路整然とし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**。

134 TOE 記述のステートメントは、ステートメントの文及び構造が対象読者（すなわち、開発者、評価者及び消費者）に理解可能である場合、理路整然としている。

APE_DES.1-4 評価者は、TOE 記述が内部的に一貫し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**。

135 評価者は、PP のこの節が TOE の一般の趣旨を定義しているに過ぎないことに留意する。

136 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3.4.1.3.3 アクション APE_DES.1.3E

APE_DES.1-5 評価者は、TOE 記述が PP のその他の部分と一貫し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**。

137 評価者は、TOE 記述が PP 内の他の箇所では考慮されていない脅威、セキュリティ機能または TOE の構成について記述しないことを特に決定する。

138 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3.4.2 セキュリティ環境の評価 (APE_ENV.1)

3.4.2.1 目的

139 このサブアクティビティの目的は、PP における TOE セキュリティ環境のステートメントが TOE 及びその環境が取り扱う対象とするセキュリティ問題の明確で一貫した定義を提供しているかどうかを決定することである。

- 3.4.2.2 入力
- 140 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
- 3.4.2.3 評価者アクション
- 141 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。
- a) APE_ENV.1.1E
- b) APE_ENV.1.2E
- 3.4.2.3.1 アクション APE_ENV.1.1E
- APE_ENV.1.1C
- APE_ENV.1-1 評価者は、TOE セキュリティ環境のステートメントがあらゆる前提条件について識別し、説明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**。
- 142 前提条件は、TOE の意図する用法についての前提条件と、TOE の使用環境についての前提条件に分割することができる。
- 143 評価者は、TOE の意図する用法についての前提条件が、TOE の意図する適用、TOE による保護を必要とする資産の潜在的な価値、及び TOE の用法の可能な制限のような側面を取り扱うことを決定する。
- 144 評価者は、TOE の意図する用法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、消費者は自らが意図する用法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、消費者が TOE を意図しない環境で使用する結果となる場合がある。
- 145 評価者は、TOE の使用環境についての前提条件が環境の物理的、人的、及び接続性の側面を扱っていることを決定する。
- a) 物理的側面には、TOE がセキュアな方法で機能するために TOE または付属周辺機器の物理的場所について行う必要がある前提条件が含まれる。以下に例を挙げる。
- 管理者コンソールが管理者にのみ制限されている領域にあることを想定する。
 - TOE のすべてのファイル記憶域が TOE が実行しているワークステーション上にあることを想定する。
- b) 人的側面には、TOE がセキュアな方法で機能するために、TOE 環境内の TOE の利用者及び管理者、またはその他の個人（潜在的な脅威エージェントを含む）について行う必要がある前提条件が含まれる。以下に例を挙げる。

3章 PP 評価

- 利用者が特定のスキルまたは専門知識を持っていることを想定する。
- 利用者が特定の最低取扱許可を持っていることを想定する。
- 管理者がアンチウイルスデータベースを月ごとに更新することを想定する。

c) 接続性の側面には、TOE がセキュアな方法で機能するために、TOE と TOE の外部にある他の IT システムまたは製品（ハードウェア、ソフトウェア、ファームウェア、またはそれらの組み合わせ）との接続に関する必要があるあらゆる前提条件が含まれる。以下に例を挙げる。

- TOE によって生成されたログファイルを保存するために最低でも 100MB の外部ディスクスペースがあることを想定する。
- TOE が特定のワークステーションで実行される唯一の非オペレーティングシステムアプリケーションであると想定する。
- TOE のフロッピードライブが使用不可能になっていると想定する。
- TOE が信頼できないネットワークに接続されないことを想定する。

146 評価者は、TOE の使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、消費者は自らが意図する環境が環境への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環境で使用される結果となる場合がある。

APE_ENV.1.2C

APE_ENV.1-2 評価者は、TOE セキュリティ環境のステートメントがあらゆる脅威について識別し、説明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**。

147 TOE 及びその環境のセキュリティ対策方針が前提条件及び組織のセキュリティ方針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適用されず、満たされているものとみなされる。

148 評価者は、すべての識別された脅威が識別された脅威エージェント、攻撃、及び攻撃の対象となる資産に関して明確に説明されていることを決定する。

149 評価者はまた、脅威エージェントが専門知識、資源、及び動機を取り扱うことによって特性が表され、攻撃が攻撃方法、悪用される脆弱性、及び機会によって特性が表されることを決定する。

APE_ENV.1.3C

APE_ENV.1-3 評価者は、TOE セキュリティ環境のステートメントがあらゆる組織のセキュリティ方針について識別し、説明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**。

150 TOE のセキュリティ対策方針及び環境が前提条件及び脅威からのみ派生するものである場合、組織のセキュリティ方針を 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適用されず、満たされているものとみなされる。

- 151 評価者は、組織のセキュリティ方針ステートメントが、TOE または TOE が使用される環境を制御する組織によって規定されたその環境が従わなければならない規則、実践またはガイドラインに関して作成されていることを決定する。組織のセキュリティ方針の例は、政府によって規定されている標準に従うためのパスワード生成及び暗号化要件である。
- 152 評価者は、各組織のセキュリティ方針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許可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。
- 3.4.2.3.2 アクション APE_ENV.1.2E
- APE_ENV.1-4 評価者は、TOE セキュリティ環境のステートメントが理路整然と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**。
- 153 TOE セキュリティ環境のステートメントは、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。
- APE_ENV.1-5 評価者は、TOE セキュリティ環境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**。
- 154 内部的に一致していない TOE セキュリティ環境のステートメントの例は次のとおりである。
- 攻撃方法が脅威エージェントの能力範囲内にはない脅威を含む TOE セキュリティ環境のステートメント。
 - 「TOE をインターネットに接続してはならない」という組織のセキュリティ方針及び脅威エージェントがインターネットからの侵入者であるという脅威を含む TOE セキュリティ環境のステートメント。
- 155 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。
- 3.4.3 PP 概説の評価 (APE_INT.1)
- 3.4.3.1 目的
- 156 このサブアクティビティの目的は、PP 概説が完全で PP のすべての部分と一貫しているか、及び PP を正しく識別しているかどうかを決定することである。
- 3.4.3.2 入力
- 157 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
- 3.4.3.3 評価者アクション
- 158 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。
- a) APE_INT.1.1E

3章 PP 評価

b) APE_INT.1.2E

c) APE_INT.1.3E

3.4.3.3.1 アクション APE_INT.1.1E

APE_INT.1.1C

APE_INT.1-1 評価者は、PP 概説が PP を識別、カタログ化、登録及び相互参照するために必要な PP 識別情報を提供していることを**チェックしなければならない**。

159 評価者は、PP 識別情報に以下が含まれていることを決定する。

- a) PP を管理及び一意に識別するために必要な情報（例えば、PP のタイトル、バージョン番号、発行日、作成者、スポンサー組織）
- b) PP の開発に使用された CC のバージョンの明示
- c) 登録情報。PP が評価前に登録された場合。
- d) 相互参照。PP が他の PP と比較される場合。
- e) 制度が要求する追加情報。

APE_INT.1.2C

APE_INT.1-2 評価者は、PP 概説によって叙述的形式で PP 概要が含まれていることを**チェックしなければならない**。

160 PP 概要の目的は、十分詳細な PP の内容の簡潔な要約（詳細な記述は、TOE 記述に記載されている）を提供し、潜在的な PP 利用者が PP が興味あるものであるかを決定できるようにすることである。

3.4.3.3.2 アクション APE_INT.1.2E

APE_INT.1-3 評価者は、PP 概説が理路整然としていることを決定するために、その PP 概説を**検査しなければならない**。

161 PP 概説は、ステートメントの文及び構造が対象読者（すなわち、開発者、評価者及び消費者）に理解可能である場合、理路整然としている。

APE_INT.1-4 評価者は、PP 概説が内部的に一貫していることを決定するために、その PP 概説を**検査しなければならない**。

162 内部的一貫性分析は、PP の内容の要約を提供する PP 概要に焦点を当てる。

163 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3.4.3.3.3 アクション APE_INT.1.3E

APE_INT.1-5 評価者は、PP 概説が PP のその他の部分と一貫し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**。

164 評価者は、PP 概要が TOE の正確な要約を提供することを決定する。特に、評価者は PP 概要が TOE 記述と一貫していること、及び評価の範囲外のセキュリティ機能の存在について記述または暗示していないことを決定する。

165 評価者は、CC 適合主張が PP の残りの部分と一貫性があることも決定する。

166 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3.4.4 セキュリティ対策方針の評価 (APE_OBJ.1)

3.4.4.1 目的

167 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完全に一貫して記述されているかどうか、及びセキュリティ対策方針が識別された脅威に対処し、識別された組織のセキュリティ方針を達成し、述べられている前提条件と一貫しているかどうかを決定することである。

3.4.4.2 入力

168 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

3.4.4.3 評価者アクション

169 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) APE_OBJ.1.1E

b) APE_OBJ.1.2E

3.4.4.3.1 アクション APE_OBJ.1.1E

APE_OBJ.1.1C

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 TOE 及びその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**。

170 評価者は、各セキュリティ対策方針に対して、それが TOE、環境、またはその両方に適用することが意図されているかどうかが明確に特定されていることを決定する。

APE_OBJ.1.2C

3章 PP 評価

APE_OBJ.1-2 評価者は、TOE のすべてのセキュリティ対策方針が対抗されるべき識別された脅威の側面、及び/または TOE が満たす必要がある組織のセキュリティ方針の側面にまでさかのぼれることを決定するために、セキュリティ対策方針根拠を**検査しなければならない**。

171 評価者は、TOE の各セキュリティ対策方針が最低でも 1 つの脅威または組織のセキュリティ方針にまでさかのぼれることを決定する。

172 たど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、脅威または組織のセキュリティ方針ステートメントが不完全であるか、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.1.3C

APE_OBJ.1-3 評価者は、環境のセキュリティ対策方針が TOE 環境によって対抗されるべき識別された脅威の側面、及び/または TOE 環境によって満たされるべき組織のセキュリティ方針の側面、及び/または TOE の環境で満たされるべき前提条件にまでさかのぼれることを決定するために、セキュリティ対策方針根拠を**検査しなければならない**。

173 評価者は、環境の各セキュリティ対策方針が最低でも 1 つの前提条件、脅威または組織のセキュリティ方針にまでさかのぼれることを決定する。

174 たど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、脅威、前提条件または組織のセキュリティ方針ステートメントが不完全であるか、または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.1.4C

APE_OBJ.1-4 評価者は、各脅威に対して、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**。

175 セキュリティ対策方針が脅威にまでさかのぼれない場合、このワークユニットは不合格になる。

176 評価者は、脅威に対する正当化が、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た場合、脅威が取り除かれ、脅威が受入れ可能なレベルに軽減されるか、または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。

177 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達成されると、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。

178 脅威の除去の例は、次のとおりである。

- エージェントから攻撃方法を使用する能力を除去する
- 抑止によって脅威エージェントの動機を除去する
- 脅威エージェントを除去する（例えば、頻繁にネットワークをクラッシュさせるマシンをネットワークから取り外す）

- 179 脅威の軽減の例は、次のとおりである。
- 脅威エージェントの攻撃方法を制限する
 - 脅威エージェントの機会を制限する
 - 行われた攻撃が成功する可能性を減少させる
 - 脅威エージェントからより多くの専門知識または資源を必要とする
- 180 脅威の影響の緩和の例は、次のとおりである。
- 資産のバックアップを頻繁に行う
 - TOE のスペアコピーを取る
 - 通信セッションで使用されるキーを頻繁に変更し、1 つのキーが破られた場合の影響を相対的に少なくする
- 181 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、それ自体の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する単なる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、この正当化はこの場合最小になる可能性がある。
- APE_OBJ.1.5C
- APE_OBJ.1-5 評価者は、各組織のセキュリティ方針に対して、セキュリティ対策方針がその組織のセキュリティ方針をカバー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**。
- 182 セキュリティ対策方針が組織のセキュリティ方針にまでさかのぼれない場合、このワークユニットは不合格になる。
- 183 評価者は、組織のセキュリティ方針が、組織のセキュリティ方針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た場合、組織のセキュリティ方針が実装されることを実証することを決定する。
- 184 評価者は、組織のセキュリティ方針にまでさかのぼる各セキュリティ対策方針が達成されると、実際に組織のセキュリティ方針の実装に寄与することも決定する。
- 185 セキュリティ対策方針根拠において提供される組織のセキュリティ方針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、それ自体の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、特定の組織のセキュリティ方針を実装する意図を反映する単なる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、この正当化はこの場合最小になる可能性がある。
- APE_OBJ.1-6 評価者は、各前提条件に対して、環境に対するセキュリティ対策方針がその前提条件をカバー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**。
- 186 環境に対するセキュリティ対策方針が前提条件にまでたどれない場合、このワークユニットは不合格になる。

3章 PP 評価

- 187 前提条件は、TOE の意図する使用法についての前提条件、または TOE の使用環境についての前提条件のどちらかである。
- 188 評価者は、TOE の意図する使用法についての前提条件に対する正当化が、その前提条件にまでさかのぼる環境に対するすべてのセキュリティ対策方針が達成された場合、意図する使用法がサポートされることを実証することを決定する。
- 189 評価者は、TOE の意図する使用法についての前提条件にまでさかのぼる環境に対する各セキュリティ対策方針が達成されると、実際に意図する使用法のサポートに寄与することも決定する。
- 190 評価者は、TOE の使用環境についての前提条件に対する正当化が、その前提条件にまでさかのぼる環境に対するすべてのセキュリティ対策方針が達成された場合、その環境が前提条件と一貫していることを実証することを決定する。
- 191 評価者は、TOE の使用環境についての前提条件にまでさかのぼる環境に対する各セキュリティ対策方針が達成されると、環境が実際に前提条件と一貫して寄与することも決定する。
- 192 セキュリティ対策方針根拠において提供される前提条件に対する環境におけ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、それ自体の正当化を構成しないことに注意すること。環境のセキュリティ対策方針が、前提条件の単なる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、この正当化はこの場合最小になる可能性がある。
- 3.4.4.3.2 アクション APE_OBJ.1.2E
- APE_OBJ.1-7 評価者は、セキュリティ対策方針のステートメントが理路整然と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**。
- 193 セキュリティ対策方針のステートメントは、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。
- APE_OBJ.1-8 評価者は、セキュリティ対策方針のステートメントが完全であ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**。
- 194 セキュリティ対策方針のステートメントは、セキュリティ対策方針がすべての識別された脅威に対抗するために十分であり、すべての識別された組織のセキュリティ方針及び前提条件をカバーしている場合、完全である。このワークユニットは、APE_OBJ.1-4、APE_OBJ.1-5 及び APE_OBJ.1-6 ワークユニットとともに実行することができる。
- APE_OBJ.1-9 評価者は、セキュリティ対策方針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**。
- 195 セキュリティ対策方針のステートメントは、セキュリティ対策方針が互いに矛盾していない場合、内部的に一貫している。そのような矛盾の例には、「利用者の識別情報は決して解除してはならない」及び「ある利用者の識別情報を他の利用者が利用可能である」という2つのセキュリティ対策方針がある。

196 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3.4.5 IT セキュリティ要件の評価 (APE_REQ.1)

3.4.5.1 目的

197 このサブアクティビティの目的は、TOE セキュリティ要件 (TOE セキュリティ機能要件及び TOE セキュリティ保証要件の両方) 及び IT 環境のセキュリティ要件が完全に一貫して記述されており、セキュリティ対策方針を達成する TOE の開発のための適切な基礎を提供するかどうかを決定することである。

198 入力

199 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

3.4.5.2 評価者アクション

200 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) APE_REQ.1.1E

b) APE_REQ.1.2E

3.4.5.2.1 アクション APE_REQ.1.1E

APE_REQ.1.1C

APE_REQ.1-1 評価者は、TOE セキュリティ機能要件のステートメントが CC パート 2 機能要件コンポーネントから抽出された TOE セキュリティ機能要件を識別していることを決定するために、そのステートメントを **チェックしなければならない**。

201 評価者は、パート 2 から抽出されたすべての TOE セキュリティ機能要件コンポーネントが、パート 2 の個別のコンポーネントの参照または PP での再現によって識別されていることを決定する。

APE_REQ.1-2 評価者は、TOE セキュリティ機能要件コンポーネントの各参照が正しいことを **チェックしなければならない**。

202 評価者は、CC パート 2 の TOE セキュリティ機能要件コンポーネントの各参照について、参照されたコンポーネントが CC パート 2 に存在するかどうかを決定する。

APE_REQ.1-3 評価者は、PP で再現されたパート 2 から抽出された各 TOE セキュリティ機能要件コンポーネントが正しく再現されていることを **チェックしなければならない**。

203 評価者は、要件が許可された操作を検査せずに、TOE セキュリティ機能要件のステートメントで正しく再現されていることを決定する。コンポーネント操作の正確性の検査は、APE_REQ.1-11 ワークユニットで実行される。

3章 PP 評価

APE_REQ.1.2C

- APE_REQ.1-4 評価者は、TOE セキュリティ保証要件のステートメントが CC パート 3 保証要件コンポーネントから抽出された TOE セキュリティ保証要件を識別していることを決定するために、そのステートメントを**チェックしなければならない**。
- 204 評価者は、パート 3 から抽出されたすべての TOE セキュリティ保証要件コンポーネントが、EAL の参照、パート 3 の個別のコンポーネントの参照または PP での再現によって識別されていることを決定する。
- APE_REQ.1-5 評価者は、TOE セキュリティ保証要件コンポーネントの各参照が正しいことを**チェックしなければならない**。
- 205 評価者は、CC パート 3 TOE セキュリティ保証要件コンポーネントの各参照について、参照されたコンポーネントが CC パート 3 に存在するかどうかを決定する。
- APE_REQ.1-6 評価者は、PP で再現されたパート 3 から抽出された各 TOE セキュリティ保証要件コンポーネントが正しく再現されていることを**チェックしなければならない**。
- 206 評価者は、要件が許可された操作を検査せずに、TOE セキュリティ保証要件のステートメントで正しく再現されていることを決定する。コンポーネント操作の正確性の検査は、APE_REQ.1-11 ワークユニットで実行される。

APE_REQ.1.3C

- APE_REQ.1-7 評価者は、TOE セキュリティ保証要件のステートメントが、CC パート 3 に定義されているように EAL を含んでいるか、または EAL を含んでいないことを適切に正当化しているかを決定するために、そのステートメントを**検査しなければならない**。
- 207 EAL が含まれていない場合、評価者は、TOE 保証要件のステートメントに EAL が含まれていない理由を正当化が取り扱うことを決定する。この正当化は、EAL を含めることが不可能、望ましくない、または不適切であった理由について取り扱うか、または EAL1 を構成するファミリの特定のコンポーネント（ACM_CAP、ADO_IGS、ADV_FSP、ADV_RCR、AGD_ADM、AGD_USR、及び ATE_IND）を含めることが不可能、望ましくない、または不適切であった理由について取り扱うことができる。

APE_REQ.1.4C

- APE_REQ.1-8 評価者は、TOE セキュリティ保証要件のステートメントが適切であることを、セキュリティ要件根拠が十分に正当化して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**。
- 208 保証要件に EAL が含まれている場合、正当化は、その EAL のすべての個々のコンポーネントを取り扱うというよりは、EAL 全体として取り扱うことができる。保証要件にその EAL への追加コンポーネントが含まれている場合、評価者は各追加が個別に正当化されることを決定する。保証要件に明示的に述べられた保証要件が含まれている場合、評価者は明示的に述べられたそれぞれの保証要件の使用が個別に正当化されることを決定する。

- 209 評価者は、セキュリティ要件根拠が、セキュリティ環境及びセキュリティ対策方針のステートメントを与えられた場合、保証要件が十分であることを十分に正当化していることを決定する。例えば、知識のある攻撃者に対する防御が必要な場合、明白なセキュリティの弱点以外を検出しない AVA_VLA.1 を特定することは不適切である。
- 210 正当化には、以下のような理由も含まれる。
- a) 制度、政府、またはその他の組織によって課される特定要件
 - b) TOE セキュリティ機能要件からの依存性であった保証要件
 - c) TOE とともに使用されるシステム及び/または製品の保証要件
 - d) 消費者要件
- 211 各 EAL の意図の概要及び目標は、CC パート 3 の 6.2 節に記述されている。
- 212 評価者は、保証要件が適切であるかどうかの決定は主観的であり、したがって正当化が十分であるかの分析を過度に厳密にしないことに留意すべきである。
- 213 保証要件に EAL が含まれていない場合、このワークユニットは APE_REQ.1-7 ワークユニットとともに実行される場合がある。
- APE_REQ.1.5C
- APE_REQ.1-9 評価者は、該当する場合、IT 環境に対するセキュリティ要件が識別されていることを **チェックしなければならない**。
- 214 PP に IT 環境に対する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適用されず、満たされているものとみなされる。
- 215 評価者は、TOE がそのセキュリティ対策方針を達成するためにセキュリティ機能を提供するための環境内のその他の IT 上の TOE の依存性が、IT 環境に対するセキュリティ要件として PP で明確に識別されていることを決定する。
- 216 IT 環境に対するセキュリティ要件の例には、ファイアウォールがあり、それは管理者の認証及び監査データの永久保存を提供するための下層のオペレーティングシステムに依存する。この場合、IT 環境に対するセキュリティ要件に FAU 及び FIA クラスからのコンポーネントが含まれる。
- 217 IT 環境のセキュリティ要件には機能要件及び保証要件の両方を含めることができる。
- 218 IT 環境への依存の例には、ソフトウェア暗号モジュールがある。これは定期的に独自のコードを検証して、コードが改ざんされた場合に自分自身を使用不可能にする。回復できるようにするために、要件 FPT_RCV.2 (自動回復) を持っている。いったん使用不可能にすると自分自身で回復できないため、IT 環境ではこれが要件になっている。FPT_RCV.2 の依存性の 1 つは AGD_ADM.1 (管理者ガイダンス) である。したがって、この保証要件は、IT 環境の保証要件となる。

3章 PP 評価

- 219 評価者は、IT 環境のセキュリティ要件が TSF を参照する場合、TOE のセキュリティ機能よりも環境のセキュリティ機能を参照することに留意する。
- APE_REQ.1.6C
- APE_REQ.1-10 評価者は、IT セキュリティ要件におけるすべての完了した操作が識別されていることを**チェックしなければならない**。
- 220 PP には未完了の操作があるエレメントを含めることができる。つまり、PP には、割付または選択に対する未完了の操作を含むセキュリティ機能要件ステートメントを含めることができる。したがって操作は、PP を具体化する ST で完了される。これにより、ST 開発者が TOE、及び特定の PP への適合を主張する対応する ST を開発する際により高い柔軟性が与えられる。
- 221 CC パート 2 機能コンポーネントに許可されている操作は、割付、繰返し、選択、及び詳細化である。割付及び選択操作は、コンポーネント内で特に示されている場合のみ許可される。繰返し及び詳細化は、すべての機能コンポーネントに対して許可されている。
- 222 CC パート 3 保証コンポーネントに許可されている操作は、繰返し及び詳細化である。
- 223 評価者は、すべての操作が、使用される各コンポーネント内で識別されていることを決定する。完了及び未完了操作は、それらを区別可能で、操作が完了しているかどうか明瞭になる方法で識別される必要がある。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.1-11 評価者は、操作が正しく実行されることを決定するために、IT 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**。
- 224 評価者は、セキュリティ要件に対する操作を PP で実行し完了する必要があることに留意する。
- 225 評価者は、それぞれのステートメントを、それが派生するエレメントと比較し、以下のことを決定する。
- a) 割付の場合、選択されたパラメタまたは変数の値が、割付で要求される指定された型に従っていること
 - b) 選択の場合、選択された要素（複数可）がエレメントの選択部分内で指定された 1 つまたは複数の要素であること。評価者は、選択された要素の数が要件に適切であることも決定する。要件には、1 つの要素のみ選択する必要があるもの（例えば、FAU_GEN.1.1.b）、複数の要素を選択できるもの（例えば、FDP_ITT.1.1 第 2 操作）がある。
 - c) 詳細化の場合、コンポーネントは詳細化された要件を満たす TOE が詳細化されていない要件も満たすような方法で詳細化されること。詳細化された要件がこの境界を越えた場合、拡張要件とみなされる。

例：ADV_SPM.1.2C TSP モデルは、モデル化が可能な TSP のすべての方針の規則及び特性を記述しなければならない。

詳細化：TSP モデルは、アクセス制御のみを扱う必要がある。

アクセス制御方針が TSP の唯一の方針である場合、これが有効な詳細化である。TSP に識別及び認証方針もあり、アクセス制御のみをモデル化する必要があることを記述することが詳細化を意味する場合、これは有効な詳細化ではない。

詳細化の特殊なケースには編集上の詳細化がある。この場合、英語の文法に合わせるために文を書き換えるなど、要件に小さな変更が行われる。この変更によって要件の意味を変更することはできない。

編集上の詳細化の例には、単一のアクションを持つ FAU_ARP.1 がある。PP 作成者は、"The TSF shall take *inform the operator* upon detection of a potential security violation" という記述を、"The TSF shall *inform the operator* upon detection of a potential security violation" と書き換えることができる。

評価者は、編集上の詳細化を明確に識別する必要があることに留意する（ワークユニット APE_REQ.1-10 を参照）。

- d) 繰返しの場合、コンポーネントの各繰返しがそのコンポーネントの別の繰返しとはそれぞれ異なること（最低でもコンポーネントの 1 つのエレメントが別のコンポーネントの対応するエレメントと異なっていること）、またはコンポーネントが TOE の異なる部分に適用されること。

APE_REQ.1.7C

APE_REQ.1-12 評価者は、PP に含まれる IT セキュリティ要件におけるすべての未完了操作が識別されていることを **検査しなければならない**。

226 評価者は、すべての操作が、使用される各コンポーネント内で識別されていることを決定する。完了及び未完了操作は、それらを区別可能で、操作が完了しているかどうか明瞭になる方法で識別される必要がある。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.1.8C

APE_REQ.1-13 評価者は、IT セキュリティ要件ステートメントで使用されるコンポーネントに要求される依存性が満たされることを決定するために、IT 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**。

227 依存性は、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）が TOE セキュリティ要件のステートメントに含まれることにより、または TOE の IT 環境によって満たされていると主張される要件として、満たすことができる。

228 CC が依存性を含めることによって依存性分析のサポートを提供していても、これはその他の依存性が存在しない正当化ではない。その他の依存性の例には、「すべてのオブジェクト」または「すべてのサブジェクト」を参照するエレメントがある。

3章 PP 評価

この場合、依存性はオブジェクトまたはサブジェクトが列挙される別のエレメントまたはエレメントのセット内の詳細化で存在可能である。

229 IT 環境内で必要なセキュリティ要件の依存性は、PP で記述し、満たされるべきである。

230 評価者は、CC ではすべての依存性を満たす必要がないことに留意する。以下のワークユニットを参照すること。

APE_REQ.1.9C

APE_REQ.1-14 評価者は、セキュリティ要件の依存性が満たされないそれぞれの場合に適切な正当化が提供されていることを決定するために、セキュリティ要件根拠を**検査しなければならない**。

231 評価者は、識別されたセキュリティ対策方針がある場合に、正当化が依存性の必要でない理由を説明していることを決定する。

232 評価者は、依存性を満たさないことはセキュリティ要件のセットがセキュリティ対策方針を適切に取り扱う妨げにならないことを確認する。この分析は、APE_REQ.1.13C によって取り扱われる。

233 適切な正当化の例は、ソフトウェア TOE がセキュリティ対策方針「失敗した認証は利用者の識別情報及び日時とともにログに記録しなければならない」を持ち、FAU_GEN.1（監査データ生成）をこのセキュリティ対策方針を満たす機能要件として使用することがある。FAU_GEN.1 は、FPT_STM.1（高信頼タイムスタンプ）への依存性を含む。TOE が時計メカニズムを含んでいないため、FPT_STM.1 は PP 作成者によって IT 環境の要件として定義される。PP 作成者は、以下の正当化によって、この要件を満たさないことを示す。「この特定の環境においてタイムスタンプメカニズムに対する攻撃が可能であるため、環境は高信頼タイプスタンプを提供できない。ただし、脅威エージェントの中には、タイプスタンプメカニズムに対して攻撃を実行できないものもあり、これらの脅威エージェントによるいくつかの攻撃は、攻撃の日時をログに記録することによって分析することができる。」

APE_REQ.1.10C

APE_REQ.1-15 評価者は、PP が TOE セキュリティ機能要件に対する最小機能強度レベルのステートメントを含み、このレベルが SOF-基本、SOF-中位または SOF-高位のいずれかであることを**チェックしなければならない**。

234 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。

235 暗号化アルゴリズムの強度は、CC の適用範囲外である。機能強度は、非暗号である確率的または順列的メカニズムにのみ適用する。したがって、PP が最小限の SOF 主張を含む場合、この主張は CC 評価に関連する暗号メカニズムにも適用しない。そのような暗号メカニズムが TOE に含まれる場合、評価者は、PP にアルゴリズム強度の評定は評価の部分を構成しないという明確なステートメントが含まれることを決定する。

236 PP 作成者が、各ドメインに対して最低強度の機能レベルを持つ方が TOE 全体に対して 1 つの包括的な最低強度の機能レベルを持つよりも適切であると思った場合、TOE は複数の別々のドメインを含む。この場合、TOE セキュリティ機能要件を別々のセットに分け、それぞれのセットに関連する機能レベルに異なる最低強度を持たせることができる。

237 この例としては、公の場所にある利用者端末、及び物理的にセキュアな場所にある管理者端末を持つ分散端末システムがある。利用者端末の認証要件は、それらに関連する SOF-中位を持ち、管理者端末の認証要件は、それらに関連する SOF-基本を持つ。TOE が、TOE の潜在的な消費者に利用者端末の認証メカニズムを攻撃することは簡単であると思わせるような最低強度の SOF-基本の機能レベルを持つと述べるよりも、PP 作成者は TOE を利用者ドメインと管理者ドメインに分けて TOE セキュリティ機能要件をそれらのドメインに属するセットに分割し、最低強度の SOF-基本の機能レベルを管理者ドメインに属するセットに割り付け、最低強度の SOF-中位の機能レベルを利用者ドメインに属するセットに割り付ける。

APE_REQ.1.11C

APE_REQ.1-16 評価者は、PP が明示された機能強度が適切であるあらゆる特定の TOE セキュリティ機能要件を、特定の数値尺度とともに識別していることを **チェックしなければならない**。

238 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。

239 明示された機能強度主張は、SOF-基本、SOF-中位、SOF-高位、または定義された特定の数値尺度のいずれかになる。特定の数値尺度が使用されている場合、評価者はこれらが特定された機能要件のタイプに適切であること、及び特定された数値尺度が強度主張として評価可能であることを決定する。

240 機能強度数値尺度の妥当性及び適切さに関する詳細なガイダンスは、制度によって提供される。

APE_REQ.1.12C

APE_REQ.1-17 評価者は、最小機能強度レベルが明示された機能強度主張とともに TOE のセキュリティ対策方針と一貫していることを、セキュリティ要件根拠が実証して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**。

241 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。

242 評価者は、根拠が、TOE セキュリティ環境のステートメントで記述されているように攻撃者の持ちうる専門知識、資源、動機に関する詳細を考慮することを決定する。例えば、TOE が高い攻撃能力を持っている攻撃者に対する防御を提供する必要がある場合、SOF-基本主張は不適切である。

243 評価者は根拠がセキュリティ対策方針の特定の強度関連特性を考慮することも決定する。評価者は対策方針に対する要件からの追跡を使用して、該当する場合特定の

3章 PP 評価

強度関連特性を持つ対策方針を追跡する要件がそれらに関連する適切な機能強度の主張を持っていることを決定できる。

APE_REQ.1.13C

- APE_REQ.1-18 評価者は、TOE セキュリティ要件が TOE に対するセキュリティ対策方針にまでさかのぼれ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**。
- 244 評価者は、それぞれの TOE セキュリティ機能要件が TOE に対する最低でも 1 つのセキュリティ対策方針にまでさかのぼれることを決定する。
- 245 たど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、セキュリティ対策方針が不完全であるか、または TOE セキュリティ機能要件が役立つ目的を持っていないことを示す。
- 246 また、必須ではないが、いくつかまたはすべての TOE セキュリティ保証要件が TOE のセキュリティ対策方針にまでさかのぼることもできる。
- 247 TOE のセキュリティ対策方針にまでさかのぼる TOE セキュリティ保証要件の例としては、脅威「TOE になると考えられる装置を使用して無意識に情報を公開する利用者」を含む PP 及びその脅威に対処する TOE のセキュリティ対策方針「TOE には明確にバージョン番号が示されていなければならない」がある。この TOE のセキュリティ対策方針は、ACM_CAP.1 を満たすことによって達成でき、したがって PP 作成者はその TOE のセキュリティ対策方針に対して ACM_CAP.1 にまでさかのぼる。
- APE_REQ.1-19 評価者は、IT 環境に対するセキュリティ要件がその環境に対するセキュリティ対策方針にまでさかのぼれ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**。
- 248 評価者は、IT 環境のそれぞれの機能セキュリティ要件がその環境に対する最低でも 1 つのセキュリティ対策方針にまでさかのぼれることを決定する。
- 249 たど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、環境のセキュリティ対策方針が不完全であるか、または IT 環境に対する機能セキュリティ要件が役立つ目的を持っていないことを示す。
- 250 また、必須ではないが、いくつかまたは IT 環境のすべてのセキュリティ保証要件がその環境のセキュリティ対策方針にまでさかのぼることもできる。
- APE_REQ.1-20 評価者は、TOE の各セキュリティ対策方針に対して、TOE セキュリティ要件がそのセキュリティ対策方針を満たすのに適していることを示す適切な正当化を含んでい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**。
- 251 TOE セキュリティ要件が TOE のセキュリティ対策方針にまでさかのぼれない場合、このワークユニットは不合格になる。

- 252 評価者は、TOE のセキュリティ対策方針が、対策方針にまでさかのぼるすべての TOE セキュリティ要件が満たされた場合、TOE のセキュリティ対策方針が達成されることを実証することを決定する。
- 253 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 TOE セキュリティ要件が満たされると、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。
- 254 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 TOE セキュリティ要件からの追跡は、正当化の一部である場合があるが、それ自体の正当化を構成しないことに注意すること。
- APE_REQ.1-21 評価者は、IT 環境の各セキュリティ対策方針に対して、IT 環境に対するセキュリティ要件がその IT 環境のセキュリティ対策方針を満たすのに適していることを示す適切な正当化を、セキュリティ要件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**。
- 255 IT 環境のセキュリティ要件が IT 環境のセキュリティ対策方針にまでさかのぼれない場合、このワークユニットは不合格になる。
- 256 評価者は、環境のセキュリティ対策方針のための正当化が、IT 環境のセキュリティ対策方針にまでさかのぼる IT 環境に対するすべてのセキュリティ要件が満たされた場合、IT 環境のセキュリティ対策方針が達成されることを実証することを決定する。
- 257 評価者は、IT 環境のセキュリティ対策方針にまでさかのぼる各 IT 環境に対するセキュリティ要件が満たされると、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。
- 258 セキュリティ要件根拠において提供される IT 環境のセキュリティ対策方針に対する IT 環境に対するセキュリティ要件からの追跡は、正当化の一部である場合があるが、それ自体の正当化を構成しないことに注意すること。
- APE_REQ.1.14C
- APE_REQ.1-22 評価者は、IT セキュリティ要件のセットが内部的に一貫していることを、セキュリティ要件根拠が実証して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**。
- 259 評価者は、異なる IT セキュリティ要件が実行される同じタイプの事象、操作、データ、テストに適用され、これらの要件が競合する可能性があるすべての場合において、これがその場合でない適切な正当化が提供されることを決定する。
- 260 例えば、PP に利用者の個別の責任に対する要件が利用者の匿名要件とともに含まれている場合、これらの要件が競合しないことを示す必要がある。これには監査可能事象に、利用者の匿名が要求される操作に関連する個々の利用者の責任が要求されないことを示すことが含まれる場合がある。
- 261 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3章 PP 評価

APE_REQ.1-23 評価者は、IT セキュリティ要件のセットが全体として相互サポート可能な構造を構成することを、セキュリティ要件根拠が実証して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**。

262 このワークユニットは、IT セキュリティ要件からセキュリティ対策方針への追跡を検査するワークユニット APE_REQ.1-18 及び APE_REQ.1-19、及び IT セキュリティ要件がセキュリティ対策方針を満たすために適切であるかどうかを検査するワークユニット APE_REQ.1-20 及び APE_REQ.1-21 内で実行される決定に基づく。このワークユニットでは、評価者が、他の IT セキュリティ要件からのサポートがないためにセキュリティ対策方針が達成できない場合がある可能性を考慮することが要求される。

263 このワークユニットは、以前のワークユニットで取り扱われた依存性分析にも基づく。これは機能要件 A が機能要件 B に依存する場合、B が定義によって A を支持するためである。

264 評価者は、セキュリティ要件根拠が、機能要件がこれらの要件の間に依存関係がないことが示されている場合であっても必要に応じて相互に支援することを実証することを決定する。この実証では、以下のセキュリティ機能要件を取り扱うべきである。

- a) FPT_RVM.1 など、ほかのセキュリティ機能要件のバイパスを防ぐ
- b) FPT_SEP など、ほかのセキュリティ機能要件の改ざんを防ぐ
- c) FPT_MOF.1 など、ほかのセキュリティ機能要件の非活性化を防ぐ
- d) FAU クラスのコンポーネントなど、ほかのセキュリティ機能要件の無効化を狙った攻撃の検出を可能にする

265 評価者は、分析の際に実行された操作を考慮に入れ、それらが要件間の相互サポートに影響するかどうかを決定する。

3.4.5.2.2 アクション APE_REQ.1.2E

APE_REQ.1-24 評価者は、IT セキュリティ要件のステートメントが理路整然と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**。

266 IT セキュリティ要件のステートメントは、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。

APE_REQ.1-25 評価者は、IT セキュリティ要件のステートメントが完全であ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**。

267 このワークユニットは、APE_REQ.1.1E 及び APE_SRE.1.1E によって要求されるワークユニット、特にセキュリティ要件根拠についての評価者の検査から結果を引き出す。

268 セキュリティ要件のステートメントは、セキュリティ要件が TOE のすべてのセキュリティ対策方針が満たされていることを保証するのに十分であると評価者が判断した場合、完全である。

APE_REQ.1-26 評価者は、IT 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**。

269 このワークユニットは、APE_REQ.1.1E 及び APE_SRE.1.1E によって要求されるワークユニット、特にセキュリティ要件根拠についての評価者の検査から結果を引き出す。

270 セキュリティ要件のステートメントは、セキュリティ対策方針が完全には満たされないなどセキュリティ要件がほかのセキュリティ要件と競合することがないと評価者が決定した場合、内部的に一貫している。

271 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3.4.6 明示された IT セキュリティ要件の評価 (APE_SRE.1)

3.4.6.1 目的

272 このサブアクティビティの目的は、CC の参照なしに述べられたセキュリティ機能要件またはセキュリティ保証要件が適切で妥当であるかどうかを決定することである。

3.4.6.2 適用上の注釈

273 この節は、PP が CC パート 2 またはパート 3 のいずれかの参照なしに明示された IT セキュリティ要件を含んでいる場合にのみ適用する。そうでない場合は、この節内のすべてのワークユニットは適用されず、満たされているものとみなされる。

274 APE_SRE 要件は APE_REQ 要件に置き換わるのではなく、追加されるものである。これは、CC パート 2 またはパート 3 のいずれかの参照なしに明示された IT セキュリティ要件が APE_SRE 基準、またその他すべてのセキュリティ要件と組み合わせ、APE_REQ 基準によって評価される必要があることを意味する。

3.4.6.3 入力

275 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

3.4.6.4 評価者アクション

276 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) APE_SRE.1.1E

b) APE_SRE.1.2E

3章 PP 評価

3.4.6.4.1 アクション APE_SRE.1.1E

APE_SRE.1.1C

APE_SRE.1-1 評価者は、IT セキュリティ要件のステートメントが、CC の参照なしに明示されたすべての TOE セキュリティ要件を識別していることを**チェックしなければならない**。

277 CC パート 2 機能コンポーネントを使用して特定されていない TOE セキュリティ機能要件は、それ自体として明確に識別される必要がある。同様に、CC パート 3 保証コンポーネントを使用して特定されていない TOE セキュリティ保証要件も、それ自体として明確に識別される必要がある。

APE_SRE.1.2C

APE_SRE.1-2 評価者は、IT セキュリティ要件のステートメントが、CC の参照なしに明示された IT 環境に対するすべてのセキュリティ要件を識別していることを**チェックしなければならない**。

278 CC パート 2 機能コンポーネントを使用して特定されていない IT 環境に対するセキュリティ機能要件は、それ自体として明確に識別される必要がある。同様に、CC パート 3 保証コンポーネントを使用して特定されていない IT 環境に対するセキュリティ保証要件も、それ自体として明確に識別される必要がある。

APE_SRE.1.3C

APE_SRE.1-3 評価者は、各々の明示された IT セキュリティ要件が明示的に述べられなければならない理由を、セキュリティ要件根拠が適切に正当化して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**。

279 評価者は、各々の明示された IT セキュリティ要件に対して、既存の機能コンポーネントまたは保証コンポーネント（それぞれ CC パート 2 及び CC パート 3 から）を該当する明示されたセキュリティ要件を表すために使用できない理由を正当化が説明することを決定する。評価者は、この決定においてこれらの既存のコンポーネントに対する操作（すなわち、割付、繰返し、選択、または詳細化）の実行可能性を考慮に入れる。

APE_SRE.1.4C

APE_SRE.1-4 評価者は、要件が CC 要件コンポーネント、ファミリー、及びクラスを提示のためのモデルとして使用することを決定するために、各々の明示された IT セキュリティ要件を**検査しなければならない**。

280 評価者は、明示された IT セキュリティ要件が CC パート 2 またはパート 3 コンポーネントと同じスタイル、同等の詳細レベルで提示されていることを決定する。評価者は、機能要件が個別の機能エレメントに分割されること、及び保証要件が開発者アクション、証拠の内容・提示、及び評価者アクションエレメントを特定することも決定する。

APE_SRE.1.5C

APE_SRE.1-5 評価者は、各々の明示された IT セキュリティ要件が、TOE の適合または非適合が決定可能で系統立てて実証できるように、測定可能でかつ客観的な評価要件を述べていることを決定するために、その要件を**検査しなければならない**。

281 評価者は、機能要件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。評価者は、保証要件が主観的な評価者判定の必要を避けることも決定する。

APE_SRE.1.6C

APE_SRE.1-6 評価者は、各々の明示された IT セキュリティ要件が、明確に、曖昧さなく表現されていることを決定するために、その要件を**検査しなければならない**。

APE_SRE.1.7C

APE_SRE.1-7 評価者は、保証要件があらゆる明示された TOE セキュリティ機能要件をサポートするのに適切で妥当であることを、セキュリティ要件根拠が実証して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**。

282 評価者は、特定された保証要件の適用が各々の明示されたセキュリティ機能要件に対して意味のある評価結果をもたらすかどうか、またはほかの保証要件が特定されるべきかどうかを決定する。例えば、明示されたセキュリティ機能要件が特有の文書による証拠（TSP モデルなど）、テストの深さ、または分析（TOE セキュリティ機能の強度分析または隠れチャンネル分析など）の必要性を暗示する場合がある。

3.4.6.4.2 アクション APE_SRE.1.2E

APE_SRE.1-8 評価者は、あらゆる明示された IT セキュリティ要件の依存性のすべてが識別されていることを決定するために、IT 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**。

283 評価者は、いかなる適用可能な依存性も PP 作成者が見過ごすことがないように保証する。

284 依存性の例は次のとおりである。明示された機能要件が監査に言及する場合は、FAU クラスのコンポーネント。明示された保証要件が TOE のソースコードまたは実装表現に言及する場合は、ADV_IMP。

4章 ST 評価

4.1 序説

285 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状況を提供するので、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。TOE 評価のサブアクティビティ検出により ST への変更が行われる可能性があるため、ST の最終判定は、TOE 評価が完了するまでできない。

286 ST 評価の要件及び方法論は、ST で主張されている EAL（またはその他の保証基準セット）に関係なく各 ST 評価で同一である。CEM の以降の章では特定の EAL での評価の実行について記述しているが、この章は評価されるあらゆる ST に適用される。

287 この章の評価方法論は、CC パート 1 の特に附属書 C、及び CC パート 3 の ASE クラスに指定されている ST の要件に基づいている。

4.2 目的

288 ST は製品またはシステムの説明である。それ自体セキュリティ機能及び定義された組織のセキュリティ方針を強化するセキュリティメカニズムを識別し、定義された前提条件に基づき、定義された脅威に対抗することを期待されている。また、製品またはシステムが正しく脅威に対抗し、組織のセキュリティ方針を強化するという保証を提供する手段を定義することも期待されている。

289 ST 評価の目的は、ST が以下の点を満たしているかどうかを決定することである。

- a) 完全である。セキュリティ機能によって、それぞれの脅威に対抗し、それぞれの組織のセキュリティ方針が強化されている。
- b) 必要十分である。セキュリティ機能が脅威及び組織のセキュリティ方針に適しており、保証手段がセキュリティ機能が正しく実装されるという十分な保証を提供する。
- c) 適切である。ST は、内部的に一貫していなければならない。
- d) 正確に具体化されている。ST が 1 つまたは複数の PP を満たすことを求めた場合、ST はそれぞれ参照された PP の完全で正確な具体化である必要がある。この場合、PP 評価結果の多くが ST 評価で再使用されることがある。

4.3 ST 評価関係

290 完全な ST 評価を実施するアクティビティは、次のことを扱う。

- a) 評価入力タスク（2章）

b) 以下のサブアクティビティを含む ST 評価アクティビティ

- 1) TOE 記述の評価 (4.4.1 節)
- 2) セキュリティ環境の評価 (4.4.2 節)
- 3) ST 概説の評価 (4.4.3 節)
- 4) セキュリティ対策方針の評価 (4.4.4 節)
- 5) PP 主張の評価 (4.4.5 節)
- 6) IT セキュリティ要件の評価 (4.4.6 節)
- 7) 明示された IT セキュリティ要件の評価 (4.4.7 節)
- 8) TOE 要約仕様の評価 (4.4.8 節)

c) 評価出力タスク (2 章)

- 291 評価入力及び評価出力タスクについては 2 章で記述している。評価アクティビティは、CC パート 3 に記載されている ASE 保証要件から引き出される。
- 292 ST 評価を構成するサブアクティビティは、この章に記述されている。サブアクティビティは、一般的に、ほぼ同時に開始することができるが、評価者は、サブアクティビティの間のいくつかの依存性を考慮する必要がある。依存性のガイダンスについては、附属書 B.4 を参照のこと。
- 293 PP 主張の評価及び明示された IT セキュリティ要件サブアクティビティの評価は、常に実行する必要はない。PP 主張サブアクティビティの評価は、PP 主張が行われた場合のみ適用し、明示された IT セキュリティ要件サブアクティビティの評価は、CC パート 2 またはパート 3 から抽出されたものではないセキュリティ要件が IT セキュリティ要件ステートメントに含まれている場合にのみ適用する。
- 294 ST に必要ないくつかの情報が参照として含まれている場合がある。例えば、PP への適合が主張されている場合、環境及び脅威についての情報のような PP 内の情報は ST の一部と考えられ、ST の基準に従うべきである。
- 295 ST が評価された PP への適合を主張し、その PP の内容に大幅に基づく場合、PP 評価結果を上記のサブアクティビティの多くを実行する際に再使用することができる。特に、セキュリティ環境のステートメント、セキュリティ対策方針及び IT セキュリティ要件の評価を行うときに再使用することができる。ST は、複数の PP に適合していることを主張することが許可されている。

4.4 ST 評価アクティビティ

4.4.1 TOE 記述の評価 (ASE_DES.1)

4.4.1.1 目的

296 このサブアクティビティの目的は、TOE 記述に TOE の目的及びその機能性の理解の助けとなる関連情報が含まれているかどうか、及び記述が完全で一貫しているかどうかを決定することである。

4.4.1.2 入力

297 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

4.4.1.3 適用上の注釈

298 TOE と消費者が購入する製品との間に違いがある場合がある。この問題に関しては、附属書 B.6 に記述されている。

4.4.1.4 評価者アクション

299 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。

a) ASE_DES.1.1E

b) ASE_DES.1.2E

c) ASE_DES.1.3E

4.4.1.4.1 アクション ASE_DES.1.1E

ASE_DES.1.1C

ASE_DES.1-1 評価者は、TOE 記述が TOE の製品またはシステムの種別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**。

300 評価者は、TOE 記述が読者に製品またはシステムの意図する使用に対する一般的な理解を提供するに十分であり、評価のための説明を提供していることを決定する。製品またはシステムの種別の例は、次のとおりである。ファイアウォール、スマートカード、暗号モデム、ウェブサーバ、イントラネット。

301 製品またはシステムの種別によって明らかにいくつかの機能が TOE に期待される場合がある。この機能がない場合、評価者は TOE 記述にこのことが適切に説明されているかどうかを決定する。この例の 1 つとして、TOE 記述にネットワークに接続されえないことが記述されているファイアウォールタイプの TOE があげられる。

- ASE_DES.1-2 評価者は、TOE 記述が一般的な用語で TOE の物理的範囲及び境界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**。
- 302 評価者は、TOE 記述がそれらのソフトウェアコンポーネント及び/またはモジュールについて、読者が一般的に理解するために十分に詳細なレベルで TOE を構成するハードウェア、ファームウェア、及びソフトウェアコンポーネント及び/またはモジュールについて説明していることを決定する。
- 303 TOE が製品と同一でない場合、評価者は TOE 記述が TOE と製品間の物理的関係を適切に説明していることを決定する。
- ASE_DES.1-3 評価者は、TOE 記述が一般的な用語で TOE の論理範囲及び境界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**。
- 304 評価者は、TOE 記述が IT について、特に TOE によって提供されるセキュリティ機能について、読者がそれらの機能について一般的に理解するために十分に詳細なレベルで説明していることを決定する。
- 305 TOE が製品と同一でない場合、評価者は TOE 記述が TOE と製品間の論理的関係を適切に説明していることを決定する。
- 4.4.1.4.2 アクション ASE_DES.1.2E
- ASE_DES.1-4 評価者は TOE 記述が理路整然としていることを決定するために、ST を**検査しなければならない**。
- 306 TOE 記述のステートメントは、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。
- ASE_DES.1-5 評価者は、TOE 記述が内部的に一貫していることを決定するために、ST を**検査しなければならない**。
- 307 評価者は、ST のこの節が TOE の一般の趣旨を定義しているに過ぎないことに留意する。
- 308 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。
- 4.4.1.4.3 アクション ASE_DES.1.3E
- ASE_DES.1-6 評価者は、TOE 記述が ST のその他の部分と一貫していることを決定するために、ST を**検査しなければならない**。
- 309 評価者は、TOE 記述が ST の他の箇所では考慮されていない脅威、セキュリティ機能または TOE の構成について記述していないことを特に決定する。
- 310 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

4 章 ST 評価

4.4.2 セキュリティ環境の評価 (ASE_ENV.1)

4.4.2.1 目的

311 このサブアクティビティの目的は、ST における TOE セキュリティ環境のステートメントが TOE 及びその環境が取り扱う対象とするセキュリティ問題の明確で一貫した定義を提供しているかどうかを決定することである。

4.4.2.2 入力

312 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

4.4.2.3 評価者アクション

313 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ASE_ENV.1.1E

b) ASE_ENV.1.2E

4.4.2.3.1 アクション ASE_ENV.1.1E

ASE_ENV.1.1C

ASE_ENV.1-1 評価者は、あらゆる前提条件について識別し、説明していることを決定するために、TOE セキュリティ環境のステートメントを**検査しなければならない**。

314 前提条件は、TOE の意図する使用法についての前提条件と、TOE の使用環境についての前提条件に分割することができる。

315 評価者は、TOE の意図する使用法についての前提条件が、TOE の意図する適用、TOE による保護を必要とする資産の潜在的な価値、及び TOE の使用法の可能制限のような側面を取り扱うことを決定する。

316 評価者は、TOE の意図する使用法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、消費者は自らが意図する使用法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、消費者が TOE を意図しない環境で使用する結果となる場合がある。

317 評価者は、TOE の使用環境についての前提条件が環境の物理的、人的、及び接続性の側面を扱っていることを決定する。

a) 物理的側面には、TOE がセキュアな方法で機能するために TOE または付属周辺機器の物理的場所について行う必要がある前提条件が含まれる。以下に例を挙げる。

- 管理者コンソールが管理者にのみ制限されている領域にあることを想定する。

- TOE のすべてのファイル記憶域が TOE が実行しているワークステーション上にあることを想定する。
- b) 人的側面には、TOE がセキュアな方法で機能するために、TOE 環境内の TOE の利用者及び管理者、またはその他の個人（潜在的な脅威エージェントを含む）について行う必要がある前提条件が含まれる。以下に例を挙げる。
- 利用者が特定のスキルまたは専門知識を持っていることを想定する。
 - 利用者が特定の最低取扱許可を持っていることを想定する。
 - 管理者がアンチウイルスデータベースを月ごとに更新することを想定する。
- c) 接続性の側面には、TOE がセキュアな方法で機能するために、TOE と TOE の外部にある他の IT システムまたは製品（ハードウェア、ソフトウェア、ファームウェア、またはそれらの組み合わせ）との接続に関する必要があるあらゆる前提条件が含まれる。以下に例を挙げる。
- TOE によって生成されたログファイルを保存するために最低でも 100MB の外部ディスクスペースがあることを想定する。
 - TOE が特定のワークステーションで実行される唯一の非オペレーティングシステムアプリケーションであると想定する。
 - TOE のフロッピードライブが使用不可能になっていると想定する。
 - TOE が信頼できないネットワークに接続されないことを想定する。

318 評価者は、TOE の使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、消費者は自らが意図する環境が環境への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環境で使用される結果となる場合がある。

ASE_ENV.1.2C

ASE_ENV.1-2 評価者は、あらゆる脅威について識別し、説明していることを決定するために、TOE セキュリティ環境のステートメントを**検査しなければならない**。

319 TOE 及びその環境のセキュリティ対策方針が前提条件及び組織のセキュリティ方針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適用されず、満たされているものとみなされる。

320 評価者は、すべての識別された脅威が識別された脅威エージェント、攻撃、及び攻撃の対象となる資産に関して明確に説明されていることを決定する。

321 評価者はまた、脅威エージェントが専門知識、資源、及び動機を取り扱うことによって特性が表され、攻撃が攻撃方法、悪用される脆弱性、及び機会によって特性が表されることを決定する。

ASE_ENV.1.3C

ASE_ENV.1-3 評価者は、TOE セキュリティ環境のステートメントがあらゆる組織のセキュリティ方針について識別し、説明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**。

4 章 ST 評価

- 322 TOE のセキュリティ対策方針及び環境が前提条件及び脅威からのみ派生するものである場合、組織のセキュリティ方針を 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適用されず、満たされているものとみなされる。
- 323 評価者は、組織のセキュリティ方針ステートメントが、TOE または TOE が使用される環境を制御する組織によって規定されたその環境が従わなければならない規則、実践またはガイドラインに関して作成されていることを決定する。組織のセキュリティ方針の例は、政府によって規定されている標準に従うためのパスワード生成及び暗号化要件である。
- 324 評価者は、各組織のセキュリティ方針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許可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。

4.4.2.3.2 アクション ASE_ENV.1.2E

- ASE_ENV.1-4 評価者は、TOE セキュリティ環境のステートメントが理路整然と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**。
- 325 TOE セキュリティ環境のステートメントは、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。
- ASE_ENV.1-5 評価者は、TOE セキュリティ環境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**。
- 326 内部的に一致していない TOE セキュリティ環境のステートメントの例は次のとおりである。
- 攻撃方法が脅威エージェントの能力範囲内にはない脅威を含む TOE セキュリティ環境のステートメント。
 - 「TOE をインターネットに接続してはならない」という組織のセキュリティ方針及び脅威エージェントがインターネットからの侵入者であるという脅威を含む TOE セキュリティ環境のステートメント。
- 327 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

4.4.3 ST 概説の評価 (ASE_INT.1)

4.4.3.1 目的

- 328 このサブアクティビティの目的は、ST 概説が完全で ST のすべての部分と一貫しているか、及び ST を正しく識別しているかどうかを決定することである。

4.4.3.2 入力

- 329 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

- 4.4.3.3 評価者アクション
- 330 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。
- a) ASE_INT.1.1E
 - b) ASE_INT.1.2E
 - c) ASE_INT.1.3E
- 4.4.3.3.1 アクション ASE_INT.1.1E
- ASE_INT.1.1C
- ASE_INT.1-1 評価者は、ST 概説が ST 及びそれが参照する TOE を管理及び識別するために必要な ST 識別情報を提供していることを**チェックしなければならない**。
- 331 評価者は、ST 識別情報に以下が含まれていることを決定する。
- a) ST を管理及び一意に識別するために必要な情報（例えば、ST のタイトル、バージョン番号、発行日、作成者）
 - b) ST が参照する TOE を管理及び一意に識別するために必要な情報（例えば、TOE の識別情報、TOE のバージョン番号）
 - c) ST の開発に使用された CC のバージョンの明示。
 - d) 制度が要求する追加情報。
- ASE_INT.1.2C
- ASE_INT.1-2 評価者は、ST 概説によって叙述的形式で ST 概要が含まれていることを**チェックしなければならない**。
- 332 ST 概要の目的は、十分詳細な ST の内容の簡潔な要約（詳細な記述は、TOE 記述に記載されている）を提供し、潜在的な消費者が TOE（及び残りの ST）に興味あるものであるかを決定できるようにすることである。
- ASE_INT.1.3C
- ASE_INT.1-3 評価者は、ST 概説が TOE に対する CC 適合の主張を述べる CC 適合主張を含んでいることを**チェックしなければならない**。
- 333 評価者は、CC 適合主張が CC パート 1 の 5.4 節に一致していることを決定する。
- 334 評価者は、CC 適合主張がパート 2 適合またはパート 2 拡張のいずれかを含んでいることを決定する。
- 335 評価者は、CC 適合主張がパート 3 適合を含むか、パート 3 追加及びパート 3 拡張の 1 つまたは両方を含んでいることを決定する。

4 章 ST 評価

- 336 パート 3 適合が主張される場合、評価者は CC 適合主張がどの EAL または保証パッケージが主張されているかを述べていることを決定する。
- 337 パート 3 追加が主張される場合、評価者は CC 適合主張が、どの EAL または保証パッケージが主張されているか、及びその EAL または保証パッケージのどの追加が主張されているかを述べていることを決定する。
- 338 パート 3 拡張が主張され、保証要件がパート 3 にない追加保証要件と関連している EAL の形式である場合、評価者は、CC 適合主張がどの EAL が主張されているかを述べていることを決定する。
- 339 パート 3 拡張が主張され、保証要件がパート 3 にない保証要件を含む保証パッケージの形式である場合、評価者は CC 適合主張がパート 3 にあるどの保証要件が主張されているかを述べていることを決定する。
- 340 PP への適合が主張される場合、評価者は CC 適合主張がどの PP または複数の PP の適合が主張されているかを述べていることを決定する。
- 341 評価者は、PP への適合が主張される場合は ASE_PPC.1 基準が適用され、パート 2 拡張またはパート 3 拡張が主張される場合は ASE_SRE.1 基準が適用されることに留意する。
- 4.4.3.3.2 アクション ASE_INT.1.2E
- ASE_INT.1-4 評価者は、ST 概説が理路整然としていることを決定するために、その ST 概説を **検査しなければならない**。
- 342 ST 概説は、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。
- ASE_INT.1-5 評価者は、ST 概説が内部的に一貫していることを決定するために、その ST 概説を **検査しなければならない**。
- 343 内部的一貫性分析は、ST の内容の要約を提供する ST 概要に焦点を当てる。
- 344 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。
- 4.4.3.3.3 アクション ASE_INT.1.3E
- ASE_INT.1-6 評価者は、ST 概説が ST のその他の部分と一貫していることを決定するために、ST を **検査しなければならない**。
- 345 評価者は、ST 概要が TOE の正確な要約を提供することを決定する。特に、評価者は ST 概要が TOE 記述と一貫していること、及び評価の範囲外のセキュリティ機能の存在について記述または暗示していないことを決定する。
- 346 評価者は、CC 適合主張が ST の残りの部分と一貫性があることも決定する。
- 347 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

4.4.4 セキュリティ対策方針の評価 (ASE_OBJ.1)

4.4.4.1 目的

348 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完全に一貫して記述されているかどうか、及びセキュリティ対策方針が識別された脅威に対処し、識別された組織のセキュリティ方針を達成し、述べられている前提条件と一貫しているかどうかを決定することである。

4.4.4.2 入力

349 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

4.4.4.3 評価者アクション

350 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ASE_OBJ.1.1E

b) ASE_OBJ.1.2E

4.4.4.3.1 アクション ASE_OBJ.1.1E

ASE_OBJ.1.1C

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 TOE 及びその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**。

351 評価者は、各セキュリティ対策方針に対して、それが TOE、環境、またはその両方に適用することが意図されているかどうかを明確に特定されていることを決定する。

ASE_OBJ.1.2C

ASE_OBJ.1-2 評価者は、TOE のすべてのセキュリティ対策方針が対抗されるべき識別された脅威の側面、及び/または TOE が満たす必要がある組織のセキュリティ方針の側面にまでさかのぼれることを決定するために、セキュリティ対策方針根拠を **検査しなければならない**。

352 評価者は、TOE の各セキュリティ対策方針が最低でも 1 つの脅威または組織のセキュリティ方針にまでさかのぼれることを決定する。

353 たど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、脅威または組織のセキュリティ方針ステートメントが不完全であるか、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.1.3C

4章 ST 評価

ASE_OBJ.1-3 評価者は、環境のセキュリティ対策方針が TOE 環境によって対抗されるべき識別された脅威の側面、及び/または TOE 環境によって満たされるべき組織のセキュリティ方針の側面、及び/または TOE の環境で満たされるべき前提条件にまでさかのぼれることを決定するために、セキュリティ対策方針根拠を**検査しなければならない**。

354 評価者は、環境の各セキュリティ対策方針が最低でも 1 つの前提条件、脅威または組織のセキュリティ方針にまでさかのぼれることを決定する。

355 たど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、脅威、前提条件または組織のセキュリティ方針ステートメントが不完全であるか、または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.1.4C

ASE_OBJ.1-4 評価者は、各脅威に対して、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**。

356 セキュリティ対策方針が脅威にまでさかのぼれない場合、このワークユニットは不合格になる。

357 評価者は、脅威に対する正当化が、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た場合、脅威が取り除かれ、脅威が受入れ可能なレベルに軽減されるか、または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。

358 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達成されると、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。

359 脅威の除去の例は、次のとおりである。

- エージェントから攻撃方法を使用する能力を除去する
- 抑止によって脅威エージェントの動機を除去する
- 脅威エージェントを除去する（例えば、頻繁にネットワークをクラッシュさせるマシンをネットワークから取り外す）

360 脅威の軽減の例は、次のとおりである。

- 脅威エージェントの攻撃方法を制限する
- 脅威エージェントの機会を制限する
- 行われた攻撃が成功する可能性を減少させる
- 脅威エージェントからより多くの専門知識または資源を必要とする

361 脅威の影響の緩和の例は、次のとおりである。

- 資産のバックアップを頻繁に行う
- TOE のスペアコピーを取る
- 通信セッションで使用されるキーを頻繁に変更し、1 つのキーが破られた場合の影響を相対的に少なくする

362 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、それ自体の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する単なる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、この正当化はこの場合最小になる可能性がある。

ASE_OBJ.1.5C

ASE_OBJ.1-5 評価者は、各組織のセキュリティ方針に対して、セキュリティ対策方針がその組織のセキュリティ方針をカバー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**。

363 セキュリティ対策方針が組織のセキュリティ方針にまでさかのぼれない場合、このワークユニットは不合格になる。

364 評価者は、組織のセキュリティ方針が、組織のセキュリティ方針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た場合、組織のセキュリティ方針が実装されることを実証することを決定する。

365 評価者は、組織のセキュリティ方針にまでさかのぼる各セキュリティ対策方針が達成されると、実際に組織のセキュリティ方針の実装に寄与することも決定する。

366 セキュリティ対策方針根拠において提供される組織のセキュリティ方針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、それ自体の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、特定の組織のセキュリティ方針を実装する意図を反映する単なる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、この正当化はこの場合最小になる可能性がある。

ASE_OBJ.1-6 評価者は、各前提条件に対して、環境に対するセキュリティ対策方針がその前提条件をカバー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**。

367 環境に対するセキュリティ対策方針が前提条件にまでたどれない場合、このワークユニットは不合格になる。

368 前提条件は、TOE の意図する使用法についての前提条件、または TOE の使用環境についての前提条件のどちらかである。

369 評価者は、TOE の意図する使用法についての前提条件に対する正当化が、その前提条件にまでさかのぼる環境に対するすべてのセキュリティ対策方針が達成された場合、意図する使用法がサポートされることを実証することを決定する。

370 評価者は、TOE の意図する使用法についての前提条件にまでさかのぼる環境に対する各セキュリティ対策方針が達成されると、実際に意図する使用法のサポートに寄与することも決定する。

371 評価者は、TOE の使用環境についての前提条件に対する正当化が、その前提条件にまでさかのぼる環境に対するすべてのセキュリティ対策方針が達成された場合、その環境が前提条件と一貫していることを実証することを決定する。

4章 ST 評価

372 評価者は、TOE の使用環境についての前提条件にまでさかのぼる環境に対する各セキュリティ対策方針が達成されると、環境が実際に前提条件と一貫して寄与することも決定する。

373 セキュリティ対策方針根拠において提供される前提条件に対する環境におけ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、それ自体の正当化を構成しないことに注意すること。環境のセキュリティ対策方針が、前提条件の単なる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、この正当化はこの場合最小になる可能性がある。

4.4.4.3.2 アクション ASE_OBJ.1.2E

ASE_OBJ.1-7 評価者は、セキュリティ対策方針のステートメントが理路整然と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**。

374 セキュリティ対策方針のステートメントは、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。

ASE_OBJ.1-8 評価者は、セキュリティ対策方針のステートメントが完全であ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**。

375 セキュリティ対策方針のステートメントは、セキュリティ対策方針がすべての識別された脅威に対抗するために十分であり、すべての識別された組織のセキュリティ方針及び前提条件をカバーしている場合、完全である。このワークユニットは、ASE_OBJ.1-4、ASE_OBJ.1-5 及び ASE_OBJ.1-6 ワークユニットとともに実行することができる。

ASE_OBJ.1-9 評価者は、セキュリティ対策方針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**。

376 セキュリティ対策方針のステートメントは、セキュリティ対策方針が互いに矛盾していない場合、内部的に一貫している。そのような矛盾の例には、「利用者の識別情報は解除してはならない」及び「ある利用者の識別情報を他の利用者が利用可能である」という2つのセキュリティ対策方針がある。

377 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

4.4.5 PP 主張の評価 (ASE_PPC.1)

378 この節は、ST が 1 つまたは複数の PP との適合を主張する場合にのみ適用する。ST に 1 つまたは複数の PP との適合が主張されていない場合、この節のすべてのワークユニットは適用されず、満たされているものとみなされる。

4.4.5.1 目的

379 このサブアクティビティの目的は、ST が適合を主張される PP の正しい具体化であるかどうかを決定する。

- 4.4.5.2 入力
- 380 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
- 4.4.5.3 評価者アクション
- 381 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。
- a) ASE_PPC.1.1E
 - b) ASE_PPC.1.2E
- 4.4.5.3.1 アクション ASE_PPC.1.1E
- ASE_PPC.1.1C
- ASE_PPC.1-1 評価者は、各々の PP 主張が適合を主張されている PP を識別していることを **チェックしなければならない**。
- 382 評価者は、参照される PP が曖昧さなく識別されること（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）を決定する。評価者は、PP への部分的な適合の主張は CC の下では許可されないことに留意する。
- ASE_PPC.1.2C
- ASE_PPC.1-2 評価者は、各々の PP 主張が、PP の許可された操作を満たす、または PP 要件をさらに適正化するような IT セキュリティ要件ステートメントを識別していることを **チェックしなければならない**。
- 383 ST では、その ST に対して未修正の PP に含まれるセキュリティ要件のステートメントを繰り返す必要はない。しかし、PP のセキュリティ機能要件が未完了の操作を含む場合、または ST の作成者が任意の PP のセキュリティ要件に詳細化操作を適用した場合は、ST におけるこれらの要件を明確に識別しなければならない。
- ASE_PPC.1.3C
- ASE_PPC.1-3 評価者は、各々の PP 主張が、PP に含まれるセキュリティ対策方針及び IT セキュリティ要件に追加されるセキュリティ対策方針及び IT セキュリティ要件を識別していることを **チェックしなければならない**。
- 384 評価者は、ST に含まれるが、PP には含まれていないすべてのセキュリティ対策方針及びセキュリティ要件が明確に識別されていることを決定する。

4 章 ST 評価

4.4.5.3.2 アクション ASE_PPC.1.2E

ASE_PPC.1-4 評価者は、各々の PP 主張に対して、PP から IT セキュリティ要件に実施されたすべての操作が、PP によって設定された境界内にあることを決定するために、ST を**検査しなければならない**。

385 このワークユニットは、PP における未完了の割付または選択操作だけでなく、PP から取り出されたセキュリティ要件に対する詳細化操作の適用もカバーする。

4.4.6 IT セキュリティ要件の評価 (ASE_REQ.1)

4.4.6.1 目的

386 このサブアクティビティの目的は、TOE セキュリティ要件 (TOE セキュリティ機能要件及び TOE セキュリティ保証要件の両方) 及び IT 環境のセキュリティ要件が完全に一貫して記述されており、セキュリティ対策方針を達成する TOE の開発のための適切な基礎を提供するかどうかを決定することである。

4.4.6.2 入力

387 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

4.4.6.3 評価者アクション

388 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ASE_REQ.1.1E

b) ASE_REQ.1.2E

4.4.6.3.1 アクション ASE_REQ.1.1E

ASE_REQ.1.1C

ASE_REQ.1-1 評価者は、TOE セキュリティ機能要件のステートメントが CC パート 2 機能要件コンポーネントから抽出された TOE セキュリティ機能要件を識別していることを決定するために、そのステートメントを**チェックしなければならない**。

389 評価者は、パート 2 から抽出されたすべての TOE セキュリティ機能要件コンポーネントが、パート 2 の個別のコンポーネントの参照、または ST が適合を主張する PP 内の個別のコンポーネントの参照、ST での再現によって識別されていることを決定する。

ASE_REQ.1-2 評価者は、TOE セキュリティ機能要件コンポーネントへの各参照が正しいことを**チェックしなければならない**。

390 評価者は、CC パート 2 の TOE セキュリティ機能要件コンポーネントの各参照について、参照されたコンポーネントが CC パート 2 に存在するかどうかを決定する。

- 391 評価者は、PP 内の TOE セキュリティ機能要件コンポーネントの各参照について、参照されたコンポーネントがその PP に存在するかどうかを決定する。
- ASE_REQ.1-3 評価者は、ST で再現されたパート 2 から抽出された各 TOE セキュリティ機能要件コンポーネントが正しく再現されていることを**チェックしなければならない**。
- 392 評価者は、要件が許可された操作を検査せずに、TOE セキュリティ機能要件のステートメントで正しく再現されていることを決定する。コンポーネント操作の正確性の検査は、ASE_REQ.1-11 及び ASE_REQ.1-12 ワークユニットで実行される。
- ASE_REQ.1.2C
- ASE_REQ.1-4 評価者は、TOE セキュリティ保証要件のステートメントが CC パート 3 保証要件コンポーネントから抽出された TOE セキュリティ保証要件を識別していることを決定するために、そのステートメントを**チェックしなければならない**。
- 393 評価者は、パート 3 から抽出されたすべての TOE セキュリティ保証要件コンポーネントが、EAL の参照、パート 3 の個別のコンポーネントの参照、ST が適合を主張する PP の参照、または ST での再現によって識別されていることを決定する。
- ASE_REQ.1-5 評価者は、TOE セキュリティ保証要件コンポーネントの各参照が正しいことを**チェックしなければならない**。
- 394 評価者は、CC パート 3 の TOE セキュリティ保証要件コンポーネントの各参照について、参照されたコンポーネントが CC パート 3 に存在するかどうかを決定する。
- 395 評価者は、PP 内の TOE セキュリティ保証要件コンポーネントの各参照について、参照されたコンポーネントがその PP に存在するかどうかを決定する。
- ASE_REQ.1-6 評価者は、ST で再現されたパート 3 から抽出された各 TOE セキュリティ保証要件コンポーネントが正しく再現されていることを**チェックしなければならない**。
- 396 評価者は、要件が許可された操作を検査せずに、TOE セキュリティ保証要件のステートメントで正しく再現されていることを決定する。コンポーネント操作の正確性の検査は、ASE_REQ.1-11 及び ASE_REQ.1-12 ワークユニットで実行される。
- ASE_REQ.1.3C
- ASE_REQ.1-7 評価者は、TOE セキュリティ保証要件のステートメントが、CC パート 3 に定義されているように EAL を含んでいるか、または EAL を含んでいないことを適切に正当化しているかを決定するために、そのステートメントを**検査しなければならない**。
- 397 EAL が含まれていない場合、評価者は、TOE 保証要件のステートメントに EAL が含まれていない理由を正当化が取り扱うことを決定する。この正当化は、EAL を含めることが不可能、望ましくない、または不適切であった理由について取り扱うか、または EAL1 を構成するファミリの特定のコンポーネント (ACM_CAP、ADO_IGS、ADV_FSP、ADV_RCR、AGD_ADM、AGD_USR、及び ATE_IND) を含めることが不可能、望ましくない、または不適切であった理由について取り扱うことができる。

ASE_REQ.1.4C

ASE_REQ.1-8 評価者は、TOE セキュリティ保証要件のステートメントが適切であることを、セキュリティ要件根拠が十分に正当化して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**。

398 保証要件に EAL が含まれている場合、正当化は、その EAL のすべての個々のコンポーネントを取り扱うというよりは、EAL 全体として取り扱うことができる。保証要件にその EAL への追加コンポーネントが含まれている場合、評価者は各追加が個別に正当化されることを決定する。保証要件に明示された保証要件が含まれている場合、評価者は各々の明示された保証要件の使用が個別に正当化されることを決定する。

399 評価者は、セキュリティ要件根拠が、セキュリティ環境及びセキュリティ対策方針のステートメントを与えられた場合、保証要件が十分であることを十分に正当化していることを決定する。例えば、知識のある攻撃者に対する防御が必要な場合、明白なセキュリティの弱点以外を検出しない AVA_VLA.1 を特定することは不適切である。

400 正当化には、以下のような理由も含まれる。

- a) ST が適合を主張する PP に示されている保証要件
- b) 制度、政府、またはその他の組織によって課される特定要件
- c) TOE セキュリティ機能要件からの依存性である保証要件
- d) TOE とともに使用されるシステム及び/または製品の保証要件
- e) 消費者要件

401 各 EAL の意図の概要及び目標は、CC パート 3 の 6.2 節に記述されている。

402 評価者は、保証要件が適切であるかどうかの決定は主観的であり、したがって正当化が十分であるかの分析を過度に厳密にしないことに留意するべきである。

403 保証要件に EAL が含まれていない場合、このワークユニットは ASE_REQ.1-7 ワークユニットとともに実行される場合がある。

ASE_REQ.1.5C

ASE_REQ.1-9 評価者は、該当する場合、IT 環境に対するセキュリティ要件が識別されていることを**チェックしなければならない**。

404 ST に IT 環境に対する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適用されず、満たされているものとみなされる。

405 評価者は、TOE がそのセキュリティ対策方針を達成するためにセキュリティ機能を提供するための環境内のその他の IT 上の TOE の依存性が、IT 環境に対するセキュリティ要件として ST で明確に識別されていることを決定する。

- 406 IT 環境に対するセキュリティ要件の例には、ファイアウォールがあり、それは管理者の認証及び監査データの永久保存を提供するための下層のオペレーティングシステムに依存する。この場合、IT 環境に対するセキュリティ要件に FAU 及び FIA クラスからのコンポーネントが含まれる。
- 407 IT 環境のセキュリティ要件には機能要件及び保証要件の両方を含めることができる。
- 408 IT 環境への依存の例には、ソフトウェア暗号モジュールがある。これは定期的に独自のコードを検証して、コードが改ざんされた場合に自分自身を使用不可能にする。回復できるようにするために、要件 FPT_RCV.2 (自動回復) を持っている。いったん使用不可能にすると自分自身で回復できないため、IT 環境ではこれが要件になっている。FPT_RCV.2 の依存性の 1 つは AGD_ADM.1 (管理者ガイダンス) である。したがって、この保証要件は、IT 環境の保証要件となる。
- 409 評価者は、IT 環境のセキュリティ要件が TSF を参照する場合、TOE のセキュリティ機能よりも環境のセキュリティ機能を参照することに留意する。
- ASE_REQ.1.6C
- ASE_REQ.1-10 評価者は、IT セキュリティ要件におけるすべての操作が識別されていることを **チェックしなければならない**。
- 410 CC パート 2 機能コンポーネントに許可されている操作は、割付、繰返し、選択、及び詳細化である。割付及び選択操作は、コンポーネント内で特に示されている場合のみ許可される。繰返し及び詳細化は、すべての機能コンポーネントに対して許可されている。
- 411 CC パート 3 保証コンポーネントに許可されている操作は、繰返し及び詳細化である。
- 412 評価者は、すべての操作が、使用される各コンポーネント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.1-11 評価者は、すべての割付及び選択操作が実行されることを決定するために、IT 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**。
- 413 評価者は、すべてのコンポーネント内でのすべての割付及び選択が完全に実行されるか (コンポーネント内で行う選択が残っていない) または完全に実行されていないことが適切に正当化されていることを決定する。
- 414 操作が完全に実行されていない例には、FTA_MCS.1 (複数同時セッションの基本制限) で同じ利用者に属する同時セッションの数に対する割付操作を実行するとき値の範囲を特定することがある。これに対する適切な正当化は、TOE 設置時に管理者によって値が特定範囲内の値から選択されることである。
- ASE_REQ.1-12 評価者は、すべての操作が正しく実行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**。

415 評価者は、それぞれのステートメントを、それが派生したエレメントと比較し、以下のことを決定する。

- a) 割付の場合、選択されたパラメタまたは変数の値が、割付で要求される指定された型に従っていること。
- b) 選択の場合、選択された要素（複数可）がエレメントの選択部分内で指定された 1 つまたは複数の要素であること。評価者は、選択された要素の数が要件に適切であることも決定する。要件には、1 つの要素のみ選択する必要があるもの（例えば、FAU_GEN.1.1.b）、複数の要素を選択できるもの（例えば、FDP_ITT.1.1 第 2 操作）がある。
- c) 詳細化の場合、コンポーネントは詳細化された要件を満たす TOE が詳細化されていない要件も満たすような方法で詳細化されること。詳細化された要件がこの境界を越えた場合、拡張要件とみなされる。

例：ADV_SPM.1.2C TSP モデルは、モデル化が可能な TSP のすべての方針の規則及び特性を記述しなければならない。

詳細化：TSP モデルは、アクセス制御のみを扱う必要がある。

アクセス制御方針が TSP の唯一の方針である場合、これが有効な詳細化である。TSP に識別及び認証方針もあり、アクセス制御のみをモデル化する必要があることを記述することが詳細化を意味する場合、これは有効な詳細化ではない。

詳細化の特殊なケースには編集上の詳細化がある。この場合、英語の文法に合わせるために文を書き換えるなど、要件に小さな変更が行われる。この変更によって要件の意味を変更することはできない。

編集上の詳細化の例には、単一のアクションを持つ FAU_ARP.1 がある。ST 作成者は、"The TSF shall take *inform the operator* upon detection of a potential security violation" という記述を、"The TSF shall *inform the operator* upon detection of a potential security violation" と書き換えることができる。

評価者は、編集上の詳細化を明確に識別する必要があることに留意する（ワークユニット ASE_REQ.1-10 を参照）。

- d) 繰返しの場合、コンポーネントの各繰返しはそのコンポーネントの別の繰返しとはそれぞれ異なること（最低でもコンポーネントの 1 つのエレメントが別のコンポーネントの対応するエレメントと異なっていること）、またはコンポーネントが TOE の異なる部分に適用されること。

ASE_REQ.1.7C

ASE_REQ.1-13 評価者は、IT セキュリティ要件ステートメントで使用されるコンポーネントに要求される依存性が満たされることを決定するために、IT 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**。

416 依存性は、適切なコンポーネント（またはそれに対して上位階層のコンポーネント）が TOE セキュリティ要件のステートメントに含まれることにより、または

TOE の IT 環境によって満たされていると主張される要件として、満たすことができる。

- 417 CC が依存性を含めることによって依存性分析のサポートを提供していても、これはその他の依存性が存在しない正当化ではない。その他の依存性の例には、「すべてのオブジェクト」または「すべてのサブジェクト」を参照するエレメントがある。この場合、依存性はオブジェクトまたはサブジェクトが列挙される別のエレメントまたはエレメントのセット内の詳細化で存在可能である。
- 418 IT 環境内で必要なセキュリティ要件の依存性は、ST に記述され、満たされるべきである。
- 419 評価者は、CC ではすべての依存性を満たす必要がないことに留意する。以下のワークユニットを参照すること。

ASE_REQ.1.8C

ASE_REQ.1-14 評価者は、セキュリティ要件の依存性が満たされないそれぞれの場合に適切な正当化が提供されていることを決定するために、セキュリティ要件根拠を**検査しなければならない**。

- 420 評価者は、識別されたセキュリティ対策方針がある場合に、正当化が依存性の必要でない理由を説明していることを決定する。
- 421 評価者は、依存性を満たさないことはセキュリティ要件のセットがセキュリティ対策方針を適切に取り扱う妨げにならないことを確認する。この分析は、ASE_REQ.1.12C によって取り扱われる。

422 適切な正当化の例は、ソフトウェア TOE がセキュリティ対策方針「失敗した認証は利用者の識別情報及び日時とともにログに記録しなければならない」を持ち、FAU_GEN.1（監査データ生成）をこのセキュリティ対策方針を満たす機能要件として使用することがある。FAU_GEN.1 は、FPT_STM.1（高信頼タイムスタンプ）への依存性を含む。TOE が時計メカニズムを含んでいないため、FPT_STM.1 は ST 作成者によって IT 環境の要件として定義される。ST 作成者は、以下の正当化によって、この要件が満たさないことを示す。「この特定の環境においてタイムスタンプメカニズムに対する攻撃が可能であるため、環境は高信頼タイプスタンプを提供できない。ただし、脅威エージェントの中には、タイプスタンプメカニズムに対して攻撃を実行できないものもあり、これらの脅威エージェントによるいくつかの攻撃は、攻撃の日時をログに記録することによって分析することができる。」

ASE_REQ.1.9C

ASE_REQ.1-15 評価者は、ST が TOE セキュリティ機能要件に対する最小機能強度レベルのステートメントを含み、このレベルが SOF-基本、SOF-中位または SOF-高位のいずれかであることを**チェックしなければならない**。

- 423 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。

4章 ST 評価

- 424 暗号化アルゴリズムの強度は、CC の適用範囲外である。機能強度は、非暗号である確率的または順列的メカニズムにのみ適用する。したがって、ST が最小限のSOF 主張を含む場合、この主張は CC 評価に関連する暗号メカニズムにも適用しない。そのような暗号メカニズムが TOE に含まれる場合、評価者は、ST にアルゴリズム強度の評定は評価の部分を構成しないという明確なステートメントが含まれることを決定する。
- 425 ST 作成者が、各ドメインに対して最低強度の機能レベルを持つ方が TOE 全体に対して 1 つの包括的な最低強度の機能レベルを持つよりも適切であると思った場合、TOE は複数の別々のドメインを含むことができる。この場合、TOE セキュリティ機能要件を別々のセットに分け、それぞれのセットに関連する機能レベルに異なる最低強度を持たせることができる。
- 426 この例としては、公の場所にある利用者端末、及び物理的にセキュアな場所にある管理者端末を持つ分散端末システムがある。利用者端末の認証要件は、それらに関連する SOF-中位を持ち、管理者端末の認証要件は、それらに関連する SOF-基本を持つ。TOE が、TOE の潜在的な消費者に利用者端末の認証メカニズムを攻撃することは簡単であると思わせるような最低強度の SOF-基本の機能レベルを持つと述べるよりも、ST 作成者は TOE を利用者ドメインと管理者ドメインに分けて TOE セキュリティ機能要件をそれらのドメインに属するセットに分割し、最低強度の SOF-基本の機能レベルを管理者ドメインに属するセットに割り付け、最低強度の SOF-中位の機能レベルを利用者ドメインに属するセットに割り付ける。

ASE_REQ.1.10C

- ASE_REQ.1-16 評価者は、ST が明示された機能強度が適切であるあらゆる特定の TOE セキュリティ機能要件を、特定の数値尺度とともに識別していることを **チェックしなければならない**。

- 427 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。
- 428 明示された機能強度主張は、SOF-基本、SOF-中位、SOF-高位、または定義された特定の数値尺度のいずれかになる。特定の数値尺度が使用されている場合、評価者はこれらが特定された機能要件のタイプに適切であること、及び特定された数値尺度が強度主張として評価可能であることを決定する。

- 429 機能強度数値尺度の妥当性及び適切さに関する詳細なガイダンスは、制度によって提供される。

ASE_REQ.1.11C

- ASE_REQ.1-17 評価者は、最小機能強度レベルが明示された機能強度主張とともに TOE のセキュリティ対策方針と一貫していることを、セキュリティ要件根拠が実証して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**。

- 430 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。

431 評価者は、根拠が、TOE セキュリティ環境のステートメントで記述されているように攻撃者の持ちうる専門知識、資源、動機に関する詳細を考慮することを決定する。例えば、TOE が高い攻撃能力を持っている攻撃者に対する防御を提供する必要がある場合、SOF-基本主張は不適切である。

432 評価者は根拠がセキュリティ対策方針の特定の強度関連特性を考慮することも決定する。評価者は対策方針に対する要件からの追跡を使用して、該当する場合特定の強度関連特性を持つ対策方針を追跡する要件がそれらに関連する適切な機能強度の主張を持っていることを決定できる。

ASE_REQ.1.12C

ASE_REQ.1-18 評価者は、TOE セキュリティ要件が TOE に対するセキュリティ対策方針にまでさかのぼれ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**。

433 評価者は、それぞれの TOE セキュリティ機能要件が TOE に対する最低でも 1 つのセキュリティ対策方針にまでさかのぼれることを決定する。

434 たど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、セキュリティ対策方針が不完全であるか、または TOE セキュリティ機能要件が役立つ目的を持っていないことを示す。

435 また、必須ではないが、いくつかまたはすべての TOE セキュリティ保証要件が TOE のセキュリティ対策方針にまでさかのぼることもできる。

436 TOE のセキュリティ対策方針にまでさかのぼる TOE セキュリティ保証要件の例としては、脅威「TOE になると考えられる装置を使用して無意識に情報を公開する利用者」を含む ST 及びその脅威に対処する TOE のセキュリティ対策方針「TOE には明確にバージョン番号が示されていなければならない」がある。この TOE のセキュリティ対策方針は、ACM_CAP.1 を満たすことによって達成でき、したがって ST 作成者はその TOE のセキュリティ対策方針に対して ACM_CAP.1 にまでさかのぼる。

ASE_REQ.1-19 評価者は、IT 環境に対するセキュリティ要件がその環境に対するセキュリティ対策方針にまでさかのぼれ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**。

437 評価者は、IT 環境のそれぞれの機能セキュリティ要件がその環境に対する最低でも 1 つのセキュリティ対策方針にまでさかのぼれることを決定する。

438 たど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、環境のセキュリティ対策方針が不完全であるか、または IT 環境に対する機能セキュリティ要件が役立つ目的を持っていないことを示す。

439 また、必須ではないが、いくつかまたは IT 環境のすべてのセキュリティ保証要件がその環境のセキュリティ対策方針にまでさかのぼることもできる。

ASE_REQ.1-20 評価者は、TOE の各セキュリティ対策方針に対して、TOE セキュリティ要件がそのセキュリティ対策方針を満たすのに適していることを示す適切な正当化を、セ

4章 ST 評価

セキュリティ要件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**。

- 440 TOE セキュリティ要件が TOE のセキュリティ対策方針にまでさかのぼれない場合、このワークユニットは不合格になる。
- 441 評価者は、TOE のセキュリティ対策方針が、対策方針にまでさかのぼるすべての TOE セキュリティ要件が満たされた場合、TOE のセキュリティ対策方針が達成されることを実証することを決定する。
- 442 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 TOE セキュリティ要件が満たされると、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。
- 443 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 TOE セキュリティ要件からの追跡は、正当化の一部である場合があるが、それ自体の正当化を構成しないことに注意すること。
- ASE_REQ.1-21 評価者は、IT 環境の各セキュリティ対策方針に対して、IT 環境に対するセキュリティ要件がその IT 環境のセキュリティ対策方針を満たすのに適していることを示す適切な正当化を、セキュリティ要件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**。
- 444 IT 環境のセキュリティ要件が IT 環境のセキュリティ対策方針にまでさかのぼれない場合、このワークユニットは不合格になる。
- 445 評価者は、環境のセキュリティ対策方針のための正当化が、IT 環境のセキュリティ対策方針にまでさかのぼる IT 環境に対するすべてのセキュリティ要件が満たされた場合、IT 環境のセキュリティ対策方針が達成されることを実証することを決定する。
- 446 評価者は、IT 環境のセキュリティ対策方針にまでさかのぼる各 IT 環境に対するセキュリティ要件が満たされると、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。
- 447 セキュリティ要件根拠において提供される IT 環境のセキュリティ対策方針に対する IT 環境に対するセキュリティ要件からの追跡は、正当化の一部である場合があるが、それ自体の正当化を構成しないことに注意すること。

ASE_REQ.1.13C

- ASE_REQ.1-22 評価者は、IT セキュリティ要件のセットが内部的に一貫していることを、セキュリティ要件根拠が実証して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**。
- 448 評価者は、異なる IT セキュリティ要件が実行される同じタイプの事象、操作、データ、テストに適用され、これらの要件が競合する可能性があるすべての場合において、これがその場合でない適切な正当化が提供されることを決定する。
- 449 例えば、ST に利用者の個別の責任に対する要件が利用者の匿名要件とともに含まれている場合、これらの要件が競合しないことを示す必要がある。これには監査可

能事象に、利用者の匿名が要求される操作に関連する個々の利用者の責任が要求されないことを示すことが含まれる場合がある。

- 450 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。
- ASE_REQ.1-23 評価者は、IT セキュリティ要件のセットが全体として相互サポート可能な構造を構成することを、セキュリティ要件根拠が実証して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**。
- 451 このワークユニットは、IT セキュリティ要件からセキュリティ対策方針への追跡を検査するワークユニット ASE_REQ.1-18 及び ASE_REQ.1-19、及び IT セキュリティ要件がセキュリティ対策方針を満たすために適切であるかどうかを検査するワークユニット ASE_REQ.1-20 及び ASE_REQ.1-21 内で実行される決定に基づく。このワークユニットでは、評価者が、他の IT セキュリティ要件からのサポートがないためにセキュリティ対策方針が達成できない場合がある可能性を考慮することが要求される。
- 452 このワークユニットは、以前のワークユニットで取り扱われた依存性分析にも基づく。これは機能要件 A が機能要件 B に依存する場合、B が定義によって A を支持するためである。
- 453 評価者は、セキュリティ要件根拠が、機能要件がこれらの要件の間に依存関係がないことが示されている場合であっても必要に応じて相互に支援することを実証することを決定する。この実証では、以下のセキュリティ機能要件を取り扱うべきである。
- a) FPT_RVM.1 など、ほかのセキュリティ機能要件のバイパスを防ぐ
 - b) FPT_SEP など、ほかのセキュリティ機能要件の改ざんを防ぐ
 - c) FMT_MOF.1 など、ほかのセキュリティ機能要件の非活性化を防ぐ
 - d) FAU クラスのコンポーネントなど、ほかのセキュリティ機能要件の無効化を狙った攻撃の検出を可能にする
- 454 評価者は、分析の際に実行された操作を考慮に入れ、それらが要件間の相互サポートに影響するかどうかを決定する。
- 4.4.6.3.2 アクション ASE_REQ.1.2E
- ASE_REQ.1-24 評価者は、IT セキュリティ要件のステートメントが、理路整然と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**。
- 455 IT セキュリティ要件のステートメントは、ステートメントの文及び構造が対象読者（すなわち、評価者及び消費者）に理解可能である場合、理路整然としている。
- ASE_REQ.1-25 評価者は、IT セキュリティ要件のステートメントが完全であ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**。

4章 ST 評価

456 このワークユニットは、ASE_REQ.1.1E 及び ASE_SRE.1.1E によって要求されるワークユニット、特にセキュリティ要件根拠についての評価者の検査から結果を引き出す。

457 セキュリティ要件のステートメントは、要件に対するすべての操作が完了され、セキュリティ要件が TOE のすべてのセキュリティ対策方針が満たされていることを保証するのに十分であると評価者が判断した場合、完全である。

ASE_REQ.1-26 評価者は、IT 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**。

458 このワークユニットは、ASE_REQ.1.1E 及び ASE_SRE.1.1E によって要求されるワークユニット、特にセキュリティ要件根拠についての評価者の検査から結果を引き出す。

459 セキュリティ要件のステートメントは、セキュリティ対策方針が完全には満たされないなどセキュリティ要件がほかのセキュリティ要件と競合することがないと評価者が決定した場合、内部的に一貫している。

460 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

4.4.7 明示された IT セキュリティ要件の評価 (ASE_SRE.1)

4.4.7.1 目的

461 このサブアクティビティの目的は、CC の参照なしに述べられたセキュリティ機能要件またはセキュリティ保証要件が適切で妥当であるかどうかを決定することである。

4.4.7.2 適用上の注釈

462 この節は、ST が CC パート 2 またはパート 3 のいずれかの参照なしに明示された IT セキュリティ要件を含んでいる場合にのみ適用する。そうでない場合は、この節内のすべてのワークユニットは適用されず、満たされているものとみなされる。

463 ASE_SRE 要件は ASE_REQ 要件に置き換わるのではなく、追加されるものである。これは、CC パート 2 またはパート 3 のいずれかの参照なしに明示された IT セキュリティ要件が ASE_SRE 基準、またその他すべてのセキュリティ要件と組み合わせ、ASE_REQ 基準によって評価される必要があることを意味する。

4.4.7.3 入力

464 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

4.4.7.4 評価者アクション

465 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ASE_SRE.1.1E

b) ASE_SRE.1.2E

4.4.7.4.1 アクション ASE_SRE.1.1E

ASE_SRE.1.1C

ASE_SRE.1-1 評価者は、IT セキュリティ要件のステートメントが、CC の参照なしに明示されたすべての TOE セキュリティ要件を識別していることを**チェックしなければならない**。

466 CC パート 2 機能コンポーネントを使用して特定されていない TOE セキュリティ機能要件は、それ自体として明確に識別される必要がある。同様に、CC パート 3 保証コンポーネントを使用して特定されていない TOE セキュリティ保証要件も、それ自体として明確に識別される必要がある。

ASE_SRE.1.2C

ASE_SRE.1-2 評価者は、IT セキュリティ要件のステートメントが、CC の参照なしに明示された IT 環境に対するすべてのセキュリティ要件を識別していることを**チェックしなければならない**。

467 CC パート 2 機能コンポーネントを使用して特定されていない IT 環境に対するセキュリティ機能要件は、それ自体として明確に識別される必要がある。同様に、CC パート 3 保証コンポーネントを使用して特定されていない IT 環境に対するセキュリティ保証要件も、それ自体として明確に識別される必要がある。

ASE_SRE.1.3C

ASE_SRE.1-3 評価者は、各々の明示された IT セキュリティ要件が明示的に述べられなければならない理由を、セキュリティ要件根拠が適切に正当化して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**。

468 評価者は、各々の明示された IT セキュリティ要件に対して、既存の機能コンポーネントまたは保証コンポーネント（それぞれ CC パート 2 及び CC パート 3 から）を該当する明示されたセキュリティ要件を表すために使用できない理由を正当化が説明することを決定する。評価者は、この決定においてこれらの既存のコンポーネントに対する操作（すなわち、割付、繰返し、選択、または詳細化）の実行可能性を考慮に入れる。

ASE_SRE.1.4C

ASE_SRE.1-4 評価者は、要件が CC 要件コンポーネント、ファミリー、及びクラスを提示のためのモデルとして使用することを決定するために、各々の明示された IT セキュリティ要件を**検査しなければならない**。

469 評価者は、明示された IT セキュリティ要件が CC パート 2 またはパート 3 コンポーネントと同じスタイル、同等の詳細レベルで表現されていることを決定する。評価者は、機能要件が個別の機能エレメントに分割されること、及び保証要件が開

4章 ST 評価

発者アクション、証拠の内容・提示、及び評価者アクションエレメントを特定することも決定する。

ASE_SRE.1.5C

ASE_SRE.1-5 評価者は、各々の明示された IT セキュリティ要件が、TOE の適合または非適合が決定可能で系統立てて実証できるように、測定可能でかつ客観的な評価要件を述べていることを決定するために、その要件を**検査しなければならない**。

470 評価者は、機能要件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。評価者は、保証要件が主観的な評価者判定の必要を避けることも決定する。

ASE_SRE.1.6C

ASE_SRE.1-6 評価者は、各々の明示された IT セキュリティ要件が、明確に、曖昧さなく表現されていることを決定するために、その要件を**検査しなければならない**。

ASE_SRE.1.7C

ASE_SRE.1-7 評価者は、保証要件があらゆる明示された TOE セキュリティ機能要件をサポートするのに適切で妥当であることを、セキュリティ要件根拠が実証して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**。

471 評価者は、特定された保証要件の適用が各々の明示されたセキュリティ機能要件に対して意味のある評価結果をもたらすかどうか、またはほかの保証要件が特定されるべきかどうかを決定する。例えば、明示されたセキュリティ機能要件が特有の文書による証拠（TSP モデルなど）、テストの深さ、または分析（TOE セキュリティ機能の強度分析または隠れチャンネル分析など）の必要性を暗示する場合がある。

4.4.7.4.2 アクション ASE_SRE.1.2E

ASE_SRE.1-8 評価者は、あらゆる明示された IT セキュリティ要件の依存性のすべてが識別されていることを決定するために、IT 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**。

472 評価者は、いかなる適用可能な依存性も ST 作成者が見過ごすことがないように保証する。

473 依存性の例は次のとおりである。明示された機能要件が監査に言及する場合は、FAU クラスのコンポーネント。明示された保証要件が TOE のソースコードまたは実装表現に言及する場合は、ADV_IMP。

4.4.8 TOE 要約仕様の評価（ASE_TSS.1）

4.4.8.1 目的

474 このサブアクティビティの目的は、TOE 要約仕様が TOE 及びその環境が取り扱う対象とするセキュリティ機能及び保証手段の明確で一貫したハイレベルな定義を提供しているかどうか、及びこれらが特定した TOE セキュリティ要件を満たしているかどうかを決定することである。

- 4.4.8.2 入力
- 475 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
- 4.4.8.3 評価者アクション
- 476 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。
- a) ASE_TSS.1.1E
- b) ASE_TSS.1.2E
- 4.4.8.3.1 アクション ASE_TSS.1.1E
- ASE_TSS.1.1C
- ASE_TSS.1-1 評価者は、TOE 要約仕様が TOE の IT セキュリティ機能及び保証手段を記述していることを**チェックしなければならない**。
- 477 評価者は、TOE 要約仕様が、TOE セキュリティ機能要件を満たすことが主張されるセキュリティ機能、及び TOE セキュリティ保証要件を満たすことが主張される保証手段のハイレベルな定義を提供することを決定する。
- 478 保証手段は、明示的に述べられるか、またはセキュリティ保証要件を満たす文書の参照によって定義することができる（例えば、関連する品質計画、ライフサイクル計画、管理計画）。
- ASE_TSS.1.2C
- ASE_TSS.1-2 評価者は、各 IT セキュリティ機能が少なくとも 1 つの TOE セキュリティ機能要件にまでたどれることを決定するために、TOE 要約仕様を**チェックしなければならない**。
- 479 たどることに失敗した場合、TOE 要約仕様が不完全であるか、TOE セキュリティ機能要件が不完全であるか、または IT セキュリティ機能が役立つ目的を持っていないことを示す。
- ASE_TSS.1.3C
- ASE_TSS.1-3 評価者は、各 IT セキュリティ機能が、その意図を理解するために必要な詳細レベルで非形式的なスタイルで記述されていることを決定するために、その IT セキュリティ機能を**検査しなければならない**。
- 480 いくつかの場合では、IT セキュリティ機能が提供する詳細は対応する TOE セキュリティ機能要件（複数可）で提供されている詳細と同じ程度である。その他の場合は、ST 作成者は、例えば「セキュリティ属性」など一般的な用語の代わりに TOE 特定の用語を使用して、TOE 特定の詳細を含めている場合がある。

4章 ST 評価

481 IT セキュリティ機能を記述する準形式的または形式的スタイルは、同じ機能の非形式的なスタイルの記述が併記されていない限り、ここでは許可されていないことに注意すること。ここでの目標は、機能の完全性または正確性などの特性を決定することではなく、機能の意図を理解することである。

ASE_TSS.1.4C

ASE_TSS.1-4 評価者は、ST のセキュリティメカニズムへのすべての参照が IT セキュリティ機能にまでさかのぼれることを決定するために、TOE 要約仕様を **検査しなければならない**。

482 セキュリティメカニズムの参照は、ST では任意であるが、(例えば、) 特定のプロトコルまたはアルゴリズムを実装する必要がある場合 (例えば、特定のパスワード生成または暗号化アルゴリズム) には適切な場合がある。ST にセキュリティメカニズムの参照が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。

483 評価者は、ST が参照する各セキュリティメカニズムが少なくとも 1 つの IT セキュリティ機能にまでさかのぼれることを決定する。

484 たどることに失敗した場合、TOE 要約仕様が不完全であるか、またはセキュリティメカニズムが役立つ目的を持っていないことを示す。

ASE_TSS.1.5C

ASE_TSS.1-5 評価者は、各 TOE セキュリティ機能要件に対して、IT セキュリティ機能がその TOE セキュリティ機能要件を満たすのに適していることを示す適切な正当化を、TOE 要約仕様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**。

485 IT セキュリティ機能が TOE セキュリティ機能要件にまでさかのぼれない場合、このワークユニットは不合格になる。

486 評価者は、TOE セキュリティ機能要件のための正当化が、要件にまでさかのぼるすべての IT セキュリティ機能が実装された場合、TOE セキュリティ機能要件が満たされることを実証していることを決定する。

487 評価者は、TOE セキュリティ機能要件にまでさかのぼる各 IT セキュリティ機能が実装されると、実際にその要件を満たすことに寄与することも決定する。

488 TOE 要約仕様において提供される TOE セキュリティ機能要件に対する IT セキュリティ機能からの追跡は、正当化の一部である場合があるが、それ自体の正当化を構成しないことに注意すること。

ASE_TSS.1-6 評価者は、IT セキュリティ機能に対する機能強度主張が、TOE セキュリティ機能要件に対する機能強度と一貫していることを決定するために、TOE 要約仕様根拠を **検査しなければならない**。

489 このワークユニットは、ASE_TSS.1-10 ワークユニットの結果から引き出される。

490 評価者は、機能強度主張が適切である各 IT セキュリティ機能に対して、この主張がさかのぼるすべての TOE セキュリティ機能要件に適していることを決定する。

491 通常、適切性は IT セキュリティ機能の機能強度主張が、たどるすべての TOE セキュリティ機能要件の機能強度と等しいか、または高いことを意味するが、例外もある。そのような例外には、認証（例えば、バイオメトリ及び PIN）用の中程度の強度認証要件を実装するために、複数の低強度機能が連続して使用される場合がある。

ASE_TSS.1.6C

ASE_TSS.1-7 評価者は、特定した IT セキュリティ機能の組み合わせが、TOE セキュリティ機能要件を満たすために一緒に機能することを、TOE 要約仕様根拠が実証して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**。

492 このワークユニットは、ワークユニット ASE_REQ.1-23 において TOE セキュリティ機能要件上で実行される相互サポートの決定に基づく。評価者のここでの分析は、IT セキュリティ機能に含まれる追加情報の影響を評定し、そのような情報を含めることによってほかの IT セキュリティ機能をバイパス、改ざん、または非活性化するなどの潜在的なセキュリティの弱点を取り込まないことを決定するべきである。

ASE_TSS.1.7C

ASE_TSS.1-8 評価者は、各保証手段が少なくとも 1 つの TOE セキュリティ保証要件にまでたどれることを決定するために、TOE 要約仕様を **チェックしなければならない**。

493 たどることに失敗した場合、TOE 要約仕様または TOE セキュリティ保証要件のステートメントが不完全であるか、または保証手段が役立つ目的を持っていないことを示す。

ASE_TSS.1.8C

ASE_TSS.1-9 評価者は、各 TOE セキュリティ保証要件に対して、保証手段がその TOE セキュリティ保証要件を満たすことの適切な正当化を、TOE 要約仕様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**。

494 保証手段が TOE セキュリティ保証要件にまでさかのぼれない場合、このワークユニットは不合格になる。

495 評価者は、TOE セキュリティ保証要件のための正当化が、要件にまでさかのぼるすべての保証手段が実装された場合、TOE セキュリティ保証要件が満たされることを実証していることを決定する。

496 評価者は、TOE セキュリティ保証要件にまでさかのぼる各保証手段が実装されると、実際にその要件を満たすことに寄与することも決定する。

497 保証手段は、開発者が保証要件を取り扱う方法を記述する。このワークユニットの目的は、特定された保証手段が保証要件を満たすのに適切であることを決定することである。

4章 ST 評価

- 498 TOE 要約仕様において提供される TOE セキュリティ保証要件に対する保証手段からの追跡は、正当化の一部である場合があるが、それ自体の正当化を構成しないことに注意すること。
- ASE_TSS.1.9C
- ASE_TSS.1-10 評価者は、TOE 要約仕様が、確率的または順列的メカニズムによって実現されるすべての IT セキュリティ機能を識別していることを **チェックしなければならない**。
- 499 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。
- 500 このワークユニットは、ほかの評価証拠の分析が ST でのように識別されない確率的または順列的メカニズムを識別した後に再び使用される場合がある。
- ASE_TSS.1.10C
- ASE_TSS.1-11 評価者は、適切である各 IT セキュリティ機能に対して、TOE 要約仕様が機能強度主張を特定の数値尺度、または SOF-基本、SOF-中位または SOF-高位として述べていることを **チェックしなければならない**。
- 501 TOE セキュリティ保証要件に AVA_SOF.1 が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。
- 4.4.8.3.2 アクション ASE_TSS.1.2E
- ASE_TSS.1-12 評価者は、TOE 要約仕様が完全であ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**。
- 502 TOE 要約仕様は、IT セキュリティ機能及び保証手段が、すべての特定された TOE のセキュリティ要件が満たされることを保証するのに十分であると評価者が判断した場合、完全である。このワークユニットは、ASE_TSS.1-5 及び ASE_TSS.1-9 ワークユニットとともに実行されるべきである。
- ASE_TSS.1-13 評価者は、TOE 要約仕様が理路整然と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**。
- 503 TOE 要約仕様は、文及び構造が対象読者（例えば、評価者及び開発者）に理解可能である場合、理路整然としている。
- ASE_TSS.1-14 評価者は、TOE 要約仕様が内部的に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**。
- 504 TOE 要約仕様は、IT セキュリティ機能または保証手段間で TOE のセキュリティ要件が完全には満たされないなどの競合がないと評価者が決定した場合、内部的に一貫している。
- 505 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

5 章 EAL1 評価

5.1 導入

506 EAL1 は、基本的レベルの保証を提供する。セキュリティ機能は、セキュリティ仕様、及びセキュリティのふるまいを理解するためのガイダンス証拠資料を使用して分析される。TOE セキュリティ機能のサブセットの独立テストが行われる。

5.2 目的

507 この章の目的は、EAL1 評価を行うための最小の評価成果を定義し、評価を行うための方法と手段についてのガイダンスを提供することである。

5.3 EAL1 評価関係

508 EAL1 評価は、次のことを扱う。

- a) 評価入力タスク (2 章)
- b) 次のもので構成される EAL1 評価アクティビティ
 - 1) ST の評価 (4 章)
 - 2) 構成管理の評価 (5.4 節)
 - 3) 配付及び運用文書の評価 (5.5 節)
 - 4) 開発文書の評価 (5.6 節)
 - 5) ガイダンス文書の評価 (5.7 節)
 - 6) テスト (5.8 節)
- c) 評価出力タスク (2 章)

509 評価アクティビティは、CC パート 3 に含まれている EAL1 保証要件から引き出される。

510 ST が TOE 評価サブアクティビティを行うための基礎と状況を提供するために、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。

511 EAL1 評価を構成するサブアクティビティが、この章に記述されている。サブアクティビティは、一般的に、多少とも同時に開始することができるが、評価者は、サブアクティビティの間のいくつかの依存性を考慮する必要がある。

512 依存性のガイダンスについては、附属書 B.4 を参照のこと。

5.4 構成管理アクティビティ

513 構成管理アクティビティの目的は、消費者が評価済み TOE を識別する手助けをすることである。

514 EAL1 での構成管理アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ACM_CAP.1

5.4.1 CM 能力の評価 (ACM_CAP.1)

5.4.1.1 目的

515 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。

5.4.1.2 入力

516 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

5.4.1.3 評価者アクション

517 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

a) ACM_CAP.1.1E

5.4.1.3.1 アクション ACM_CAP.1.1E

ACM_CAP.1.1C

1:ACM_CAP.1-1 評価者は、評価のために提供された TOE のバージョンが一意にリファレンスされていることを**チェックしなければならない**。

518 この保証コンポーネントに対して、開発者が一意のリファレンス以上に CM システムを使用する必要はない。その結果、評価者は、購入することができる TOE の他のバージョンが同じリファレンスを所有していないことをチェックするだけで TOE のバージョンの一意性を検証することができる。CC 要件を超えて 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リファレンスの一意性の正当性を確認することができる。その評価の間に 1 つだけのバージョンが検査されたならば、評価のために提供されたバージョンが一意にリファレンスされていることの証拠としては不完全である。そこで評価者は、一意のリファレンスをサポートできるリファレンスシステム（例えば、数字、文字または日付の使用）を探すべきである。それにもかかわらず、いかなるリファレンスも存

在しない場合、通常、TOE が一意に識別できると評価者が確信しない限り、この要件に対する判定は不合格となる。

- 519 評価者は、TOE の複数のバージョンを検査するようにし（例えば、脆弱性が発見された後のリワーク中に）、2 つのバージョンが別々にリファレンスされることをチェックするべきである。

ACM_CAP.1.2C

- 1:ACM_CAP.1-2 評価者は、評価のために提供された TOE がそのリファレンス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**。

- 520 評価者は、TOE の異なるバージョンを区別することができる一意のリファレンスが 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。

- 521 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、スタートアップルーチンの間に、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。

- 1:ACM_CAP.1-3 評価者は、使用されている TOE リファレンスが一貫していることを**チェックしなければならない**。

- 522 もし、TOE に 2 度以上の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。

- 523 評価者は、TOE リファレンスが ST と一貫性があることも検証する。

- 524 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

5.5 配付及び運用アクティビティ

525 配付及び運用アクティビティの目的は、開発者が意図したのと同じ方法で TOE が設置され、生成され、開始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が適切であることを判断することである。

526 EAL1 での配付及び運用アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ADO_IGS.1

5.5.1 設置、生成及び立上げの評価 (ADO_IGS.1)

5.5.1.1 目的

527 このサブアクティビティの目的は、TOE のセキュアな設置、生成、及び立上げのための手順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。

5.5.1.2 入力

528 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) 管理者ガイダンス

b) セキュアな設置、生成、及び立上げの手順

c) テストに適した TOE

5.5.1.3 適用上の注釈

529 設置、生成及び立上げ手順は、それらが利用者サイトで行われるか、または ST の記述に従って TOE をセキュアな構成にするために必要となる開発サイトで行われるかに関係なく、すべての設置、生成、及び立上げの手順に関係している。

5.5.1.4 評価者アクション

530 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ADO_IGS.1.1E

b) ADO_IGS.1.2E

5.5.1.4.1 アクション ADO_IGS.1.1E

ADO_IGS.1.1C

1:ADO_IGS.1-1 評価者は、TOE のセキュアな設置、生成及び立上げに必要な手順が提供されていることを **チェックしなければならない**。

- 531 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合（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（または影響を受ける部分）は、適用されないために、満たされているものとみなされる。
- 5.5.1.4.2 アクション ADO_IGS.1.2E
- 1:ADO_IGS.1-2 評価者は、TOE のセキュアな設置、生成及び立上げに必要なステップを記述していることを決定するために、提供された設置、生成、及び立上げの手順を**検査しなければならない**。
- 532 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合（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（または影響を受ける部分）は、適用されないために、満たされているものとみなされる。
- 533 設置、生成及び立上げの手順は、次のものに対する詳細な情報を提供することができる。
- a) TSF の制御のもとでのエンティティの設置の特定セキュリティ特性の変更
 - b) 例外及び問題の取扱い
 - c) 適切に、セキュアな設置のための最小限のシステム要件
- 534 設置、生成及び立上げの手順の結果、セキュアな構成となることを確認するために、評価者は、開発者の手順に従って、提供されたガイダンス証拠資料だけを使用して、顧客が（TOE に適用される場合）TOE を設置、生成、及び立上げするために通常行うことが予想されるアクティビティを実行することができる。このワークユニットは、1:ATE_IND.1-2 ワークユニットとともに実行することができる。

5.6 開発アクティビティ

535 開発アクティビティの目的は、TSF が TOE のセキュリティ機能を提供する方法を理解するための適合性の観点から設計証拠資料を評価することである。この理解は、機能仕様（TOE の外部インタフェースを記述している）と表現対応（一貫性を保証するために機能仕様を TOE 要約仕様にマッピングする）を検査することによって得られる。

536 EAL1 の開発アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ADV_FSP.1

b) ADV_RCR.1

5.6.1 適用上の注釈

537 設計証拠資料の CC 要件は、形式性によってレベル付けされている。CC は、文書の形式性の程度（すなわち、非形式的、準形式的または形式的のどれであるか）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。方法論は、使用すべき特定の言語を指示しない。その問題は、制度に任されている。次の段落は、各種の非形式的文書の内容を区別している。

538 非形式的機能仕様は、セキュリティ機能の記述（TOE 要約仕様と同等のレベルでの）及び TSF への外部に見えるインタフェースの記述からなる。例えば、オペレーティングシステムが自己を識別する手段、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、記録する監査機能も含まれている場合には、これらの監査機能の記述も機能仕様に含まれることが期待される。これらの機能は、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、それらは、利用者の外部インタフェースで何が起きるかによって影響される。

539 対応の実証の非形式は、散文形式である必要はない。簡単な 2 次元のマッピングで十分である。例えば、1 つの軸に沿ってモジュールが示され、他の軸に沿ってサブシステムが示され、セルがこれら 2 つの対応を識別するマトリックスは、上位レベル設計と下位レベル設計の間の適切な非形式的対応を提供することができる。

5.6.2 機能仕様の評価（ADV_FSP.1）

5.6.2.1 目的

540 このサブアクティビティの目的は、開発者が TOE のセキュリティ機能の適切な記述を提供しているかどうか及び TOE が提供するセキュリティ機能が ST のセキュリティ機能要件を十分に満たしているかどうかを決定することである。

- 5.6.2.2 入力
- 541 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) 利用者ガイダンス
 - d) 管理者ガイダンス
- 5.6.2.3 評価者アクション
- 542 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。
- a) ADV_FSP.1.1E
 - b) ADV_FSP.1.2E
- 5.6.2.3.1 アクション ADV_FSP.1.1E
- ADV_FSP.1.1C
- 1:ADV_FSP.1-1 評価者は、機能仕様がすべての必要な非形式的説明文を含んで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**。
- 543 機能仕様全体が非形式的である場合、このワークユニットは、適用されないために、満たされているものとみなされる。
- 544 補助的な叙述的記述は、準非形式的または形式的記述だけでは理解するのが困難な機能仕様の部分に必要となる（例えば、形式的表記の意味を明確にするため）。
- ADV_FSP.1.2C
- 1:ADV_FSP.1-2 評価者は、機能仕様が内部的に一貫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**。
- 545 評価者は、TSFI を構成するインタフェースの記述が TSF の機能の記述と一貫していることを保証することにより、機能仕様の正当性を確認する。
- 546 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。
- ADV_FSP.1.3C
- 1:ADV_FSP.1-3 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべてを識別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**。
- 547 用語「外部」(*external*) は、利用者に見えることを意味する。TOE への外部インタフェースは、TSF への直接インタフェースであるかまたは TOE の TSF 以外の部

分へのインタフェースのいずれかである。ただし、これらの TSF 以外のインタフェースは、最終的に TSF にアクセスすることがある。TSF に直接または間接的にアクセスするこれらの外部インタフェースは、一体となって TOE セキュリティ機能インタフェース (TSFI) を構成する。図 5.1 は、TSF (陰影の付いた) 部分と TSF 以外 (空白) の部分を持つ TOE を示している。この TOE には、3 つの外部インタフェースがある。ここで、インタフェース *c* は、TSF への直接インタフェースである。インタフェース *b* は、TSF への間接インタフェースである。インタフェース *a* は、TOE の TSF 以外の部分へのインタフェースである。そこで、インタフェース *b* と *c* が TSFI を構成する。

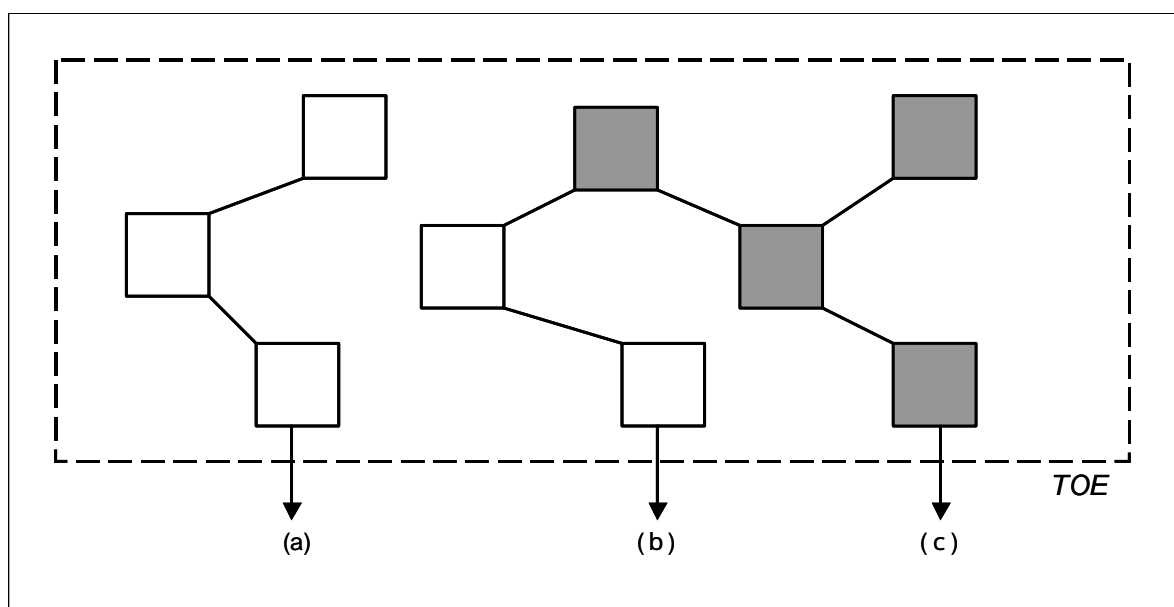


図 5.1 TSF インタフェース

- 548 CC パート 2 (またはその拡張コンポーネント) の機能要件に反映されているすべてのセキュリティ機能は、ある種の外部から見える表示を持つことに注意されるべきである。これらすべてが必ずしもセキュリティ機能をテストすることができるインタフェースとは限らないが、それらは、すべて、ある程度まで外部から見えるものであり、したがって機能仕様に含まれる必要がある。
- 549 TOE の境界を決定するガイダンスについては、附属書 B.6 を参照のこと。
- 1:ADV_FSP.1-4 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべて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**。
- 550 悪意のある利用者からの脅威のない TOE (すなわち、FPT_PHP、FPT_RVM 及び FPT_SEP が ST から正当に除外されている) では、機能仕様 (そして他の TSF 表現記述に展開される) に記述されている唯一のインタフェースは、TSF との間のインタフェースである。FPT_PHP、FPT_RVM、及び FPT_SEP が存在しないことで、セキュリティ機能がバイパスされる心配がないことが想定されるので、他のインタフェースが TSF に与える影響についての心配がない。

- 551 他方、悪意のある利用者またはバイパスの脅威がある TOE（すなわち、FPT_PHP、FPT_RVM、及び FPT_SEP が ST に含まれている）では、すべての外部インタフェースが機能仕様に記述されているが、それは、それぞれの影響が明らかになる程度に限られている。セキュリティ機能へのインタフェース（すなわち、図 5.1 のインタフェース *b* と *c*）は、完全に記述されているが、他のインタフェースは、そのインタフェースを介して TSF へアクセスできない（すなわち、インタフェースは、図 5.1 のタイプ *b* ではなく、タイプ *a*）ことを明確にする範囲すなわちでのみ記述されている。FPT_PHP、FPT_RVM、及び FPT_SEP が含まれていることは、すべてのインタフェースが TSF に影響するおそれがあることを暗示している。各外部インタフェースは、潜在的な TSF インタフェースなので、機能仕様には、インタフェースがセキュリティに適切であるかどうかを評価者が決定できるように十分詳細な各インタフェースの記述を含める必要がある。
- 552 いくつかのアーキテクチャは、外部インタフェースのグループに対して十分詳細にこのインタフェース記述を容易に提示している。例えば、カーネルアーキテクチャでは、オペレーティングシステムへのすべてのコールがカーネルプログラムで取り扱われる。TSP を侵害するかもしれないコールは、そのようにする権限を持つプログラムによってコールされなければならない。権限とともに実行されるすべてのプログラムは、機能仕様を含める必要がある。権限なしに実行されるカーネルの外部のあらゆるプログラムは、TSP に影響を与えることはできず（すなわち、そのようなプログラムは、図 6.1 のタイプ *b* ではなく、タイプ *a* のインタフェースである）そこで、機能仕様から除外することができる。カーネルアーキテクチャが存在する場合、評価者のインタフェース記述の理解は促進されるが、そのようなアーキテクチャは必ずしも必要ない。
- 1:ADV_FSP.1-5 評価者は、TSFI の提示が、効果、例外及び誤りメッセージを記述している各外部インタフェースにおいて、TOE のふるまいを適切に及び正しく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**。
- 553 インタフェースの提示が適切であり、正しいことを評価するために、評価者は、機能仕様、ST の TOE 要約仕様、及び利用者と管理者ガイダンスを使用して、次の要因を評定する。
- a) すべてのセキュリティに関係する利用者入力パラメタ（またはそれらのパラメタの特性化）が識別されるべきである。完全であるために、直接利用者が制御しないパラメタも、それらを管理者が使用できる場合、識別されるべきである。
 - b) レビュー済みガイダンスに記述されているすべてのセキュリティに関係するふるまいは、機能仕様の中で意味(semantics)の記述に反映させるべきである。これには、事象及び各事象の効果としてのふるまいの識別を含めるべきである。例えば、ファイルが要求時に開かれない各理由（例えば、アクセス拒否、ファイルが存在しない、他の利用者がファイルを使用している、利用者は午後 5 時以降ファイルを開くことが許されていない）に異なる誤りコードを提供するような、機能の豊富なファイルシステムインタフェースをオペレーティングシステムが提供する場合、機能仕様は、要求に対してファイルが開かれたか、または誤りコードが戻されたかを説明するべきである。（機能仕様は、誤りに対するこれらの異なる理由のすべてを列挙することができるが、そのような詳細を提供する必要はない。）意味の記述には、セキュリティ要件がインタフェース

に適用される方法（例えば、インタフェースの使用が監査可能な事象であるかどうか、そして可能な場合は記録可能な情報かどうか）を含めるべきである。

- c) すべてのインタフェースは、操作のすべての可能なモードに対して記述される。TSF が権限の概念を提供する場合、インタフェースの記述は、権限がある場合とない場合のインタフェースのふるまいを説明するべきである。
- d) セキュリティに関係するパラメタの記述、及びインタフェースのシンタクス (syntax)に含まれる情報は、すべての証拠資料にわたって一貫しているべきである。

554 上記の検証は、機能仕様と ST の TOE 要約仕様及び開発者が提供する利用者及び管理者ガイダンスをレビューすることによって行われる。例えば、TOE がオペレーティングシステムとその下層のハードウェアである場合、評価者は、評価される TOE に適切であるとして、利用者アクセス可能プログラムの説明、プログラムのアクティビティを制御するために使用されるプロトコルの記述、プログラムのアクティビティを制御するために使用される利用者アクセス可能データベースの記述、及び利用者インタフェース（例えば、コマンド、アプリケーションプログラムインタフェース）を探す。評価者は、プロセッサ命令セットが記述されていることも保証する。

555 評価者が、設計、ソースコード、または他の証拠を検査し、機能仕様から抜けて落ちているパラメタまたは誤りメッセージが含まれることを発見するまでは、機能仕様不完全であることを発見しないようなものであるため、このレビューは繰り返される。

ADV_FSP.1.4C

1:ADV_FSP.1-6 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**。

556 TSF 提示が完全であることを評定するために、評価者は、ST の TOE 要約仕様、利用者ガイダンス、及び管理者ガイダンスを調べる。これらはいずれも、機能仕様の TSF 表現に含まれていないセキュリティ機能を記述するべきでない。

5.6.2.3.2 アクション ADV_FSP.1.2E

1:ADV_FSP.1-7 評価者は、機能仕様 TOE セキュリティ機能要件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**。

557 すべての ST セキュリティ機能要件が機能仕様によって扱われていることを保証するために、評価者は、TOE 要約仕様と機能仕様間のマッピングを作成することができる。そのようなマッピングは、対応 (ADV_RCR.*) 要件を満たしていることの証拠として開発者によってすでに提供されていることがある。その場合には、評価者は、このマッピングが完全であることを単に検証して、すべてのセキュリティ機能要件が機能仕様の適切な TSFI 表現にマッピングされていることを保証することだけが必要である。

1:ADV_FSP.1-8 評価者は、機能仕様 TOE 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、その仕様を**検査しなければならない**。

- 558 特定の特性を備えたセキュリティ機能への各インタフェースに対して、機能仕様の詳細な情報は、ST に特定されているように正確でなければならない。例えば、ST にパスワードの長さが 8 文字でなければならないという利用者認証要件が含まれている場合、TOE は、8 文字のパスワードを持つ必要がある。機能仕様が 6 文字の固定長のパスワードを記述している場合、機能仕様は要件の正確な具体化ではない。
- 559 制御された資源で動作する機能仕様の各インタフェースについて、評価者は、それがセキュリティ要件の 1 つを実施することによる起りうる失敗を示す誤りコードを戻すかどうかを決定する。誤りコードが戻されない場合、評価者は、誤りコードを戻されるべきかどうかを決定する。例えば、オペレーティングシステムは、制御されたオブジェクトを「OPEN (開く)」ためにインタフェースを提示することができる。このインタフェースの記述には、アクセスがそのオブジェクトに許可されていないことを示す誤りコードを含めることができる。そのような誤りコードが存在しない場合、評価者は、それが適切であることを確認するべきである (おそらく、アクセスの仲介は、OPEN ではなく、READ と WRITE で行われるため)。

5.6.3 表現対応の評価 (ADV_RCR.1)

5.6.3.1 目的

560 このサブアクティビティの目的は、開発者が機能仕様に機能 ST の要件を正しく及び完全に実装しているかどうかを決定することである。

5.6.3.2 入力

561 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 要約仕様と機能仕様の間に対応分析

5.6.3.3 評価者アクション

562 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_RCR.1.1E

5.6.3.3.1 アクション ADV_RCR.1.1E

ADV_RCR.1.1C

1:ADV_RCR.1-1 評価者は、機能仕様が TOE セキュリティ機能の正しい、完全な表現であることを決定するために、TOE 要約仕様と機能仕様の間に対応分析を **検査しなければならない**。

563 評価者のこのワークユニットの目標は、TOE 要約仕様に識別されているすべてのセキュリティ機能が機能仕様に表現されていること及びそれらが正確に表現されていることを決定することである。

564 評価者は、TOE 要約仕様の TOE セキュリティ機能と機能仕様の間に対応をレビューする。評価者は、対応が一貫し、正確であることを調べる。対応分析が TOE 要約仕様のセキュリティ仕様と機能仕様のインタフェース記述の間関係を示しているところでは、評価者は、両方のセキュリティ機能が同じであることを検証する。TOE 要約仕様のセキュリティ機能が、対応するインタフェースにおいて正しく、完全に表されている場合、このワークユニットは、満たされる。

565 このワークユニットは、ワークユニット 1:ADV_FSP.1-7 及び 1:ADV_FSP.1-8 とともに行うことができる。

5.7 ガイダンス文書アクティビティ

566 ガイダンス文書アクティビティの目的は、運用 TOE を使用する方法を記述している証拠資料が適切であることを判断することである。そのような証拠資料には、正しくないアクションが TOE のセキュリティに悪影響を与えることがある信頼された管理者と管理者以外の利用者に対する文書と、正しくないアクションが自分自身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信頼できない利用者に対する両方の文書がある。

567 EAL1 でのガイダンス文書アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) AGD_ADM.1

b) AGD_USR.1

5.7.1 適用上の注釈

568 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。

5.7.2 管理者ガイダンスの評価 (AGD_ADM.1)

5.7.2.1 目的

569 このサブアクティビティの目的は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を記述しているかどうかを決定することである。

5.7.2.2 適用上の注釈

570 用語「*管理者*」(*administrator*) は、TOE 構成パラメタの設定など、TOE 内のセキュリティの重要な操作を実行することを任された人間利用者を示す。この操作は、TSP の実施に影響を与えるので、管理者は、これらの操作を行うために必要な特定の権限を有している。管理者(一人または複数)の役割は、TOE の管理者以外の利用者の役割から明確に区別する必要がある。

571 監査者、管理者、または日常的な管理など、TOE により認識され、TSF と相互作用することができる ST に定義された異なる管理者の役割またはグループが存在することができる。各役割は、広範な能力のセットを含むか、または単一の能力であることができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。異なる管理者の役割とグループは、管理者ガイダンスにて考慮されるべきである。

5.7.2.3 入力

572 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) 利用者ガイダンス
- d) 管理者ガイダンス
- e) セキュアな設置、生成、及び立上げの手順

5.7.2.4 評価者アクション

573 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_ADM.1.1E

5.7.2.4.1 アクション AGD_ADM.1.1E

AGD_ADM.1.1C

1:AGD_ADM.1-1 評価者は、管理者ガイダンスが TOE の管理者が利用できる管理セキュリティ機能とインタフェースを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**。

574 管理者ガイダンスには、管理者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

575 管理者ガイダンスには、管理者セキュリティインタフェースと機能の目的、ふるまい、及び相互関係を識別し、記述するべきである。

576 各管理者セキュリティインタフェースと機能に対して、管理者ガイダンスでは、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) 管理者が設定するパラメタ、それらの正当な値とデフォルトの値を記述する。
- 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。

AGD_ADM.1.2C

1:AGD_ADM.1-2 評価者は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を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**。

577 管理者ガイダンスは、ST に記述されているものと一貫する IT 環境の TSP に従って、TOE を操作する方法を記述する。

AGD_ADM.1.3C

1:AGD_ADM.1-3 評価者は、管理者ガイダンスがセキュアな処理環境で管理されなければならない機能と権限に関する警告を含んで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**。

578 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利用者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、管理者ガイダンスに記述されるべきである。

579 管理者ガイダンスでは、管理すべき機能と権限、それらに必要な管理のタイプ、そのような管理の理由を識別する。警告では、期待される効果、考えられる副次的効果、他の機能との考えられる相互作用及び権限を指摘する。

AGD_ADM.1.4C

1:AGD_ADM.1-4 評価者は、管理者ガイダンスが TOE のセキュアな運用に関連する利用者のふるまいに関するすべての前提条件を記述していることを決定するために、そのガイダンスを**検査しなければならない**。

580 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関する情報のみを管理者ガイダンスに含める必要がある。

581 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。

AGD_ADM.1.5C

1:AGD_ADM.1-5 評価者は、管理者ガイダンスが管理者の管理下にあるすべてのセキュリティパラメータを、セキュアな値を適切に示して、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**。

582 各セキュリティパラメータに対して、管理者ガイダンスは、パラメータの目的、パラメータの正当な値とデフォルトの値、そのようなパラメータの安全及び安全でない、個別または組み合わせによる、使用設定を記述するべきである。

AGD_ADM.1.6C

1:AGD_ADM.1-6 評価者は、管理者ガイダンスが TSF の制御下にあるエンティティのセキュリティ特質の変更を含む、実行が必要な管理機能に関連するセキュリティ関連事象の各タイプを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**。

583 セキュリティ関連事象のすべてのタイプは、詳細に記述されているので、管理者は、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管理者が取る必要があるアクション（存在する場合）を知る。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、管理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_ADM.1.7C

1:AGD_ADM.1-7 評価者は、管理者ガイダンスが評価のために提供された他のすべての文書と一貫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**。

584 特に ST には、TOE セキュリティ環境とセキュリティ対策方針に関する TOE 管理者への警告に対する詳細な情報を含めることができる。

585 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_ADM.1.8C

1:AGD_ADM.1-8 評価者は、管理者ガイダンスが管理者に関連する TOE の IT 環境に対するすべての IT セキュリティ要件を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**。

586 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。

587 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。

588 評価者は、TOE の IT 環境に対するセキュリティ要件 (ST のオプションステートメント) を分析し、管理者にとって適切な ST のすべてのセキュリティ要件が管理者ガイダンスに適切に記述されていることを保証するために、それらを管理者ガイダンスと比較するべきである。

5.7.3 利用者ガイダンスの評価 (AGD_USR.1)

5.7.3.1 目的

589 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 が提供するセキュリティ機能とインタフェースを記述しているかどうか、及びこのガイダンスが TOE のセキュアな使用のための説明とガイドラインを提供しているかどうかを決定することである。

5.7.3.2 適用上の注釈

590 TOE によって認識され、TSF と相互作用を行うことができる ST に定義されている異なる利用者の役割とグループが存在することができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。利用者ガイダンスでは、異なる利用者の役割とグループが考慮されるべきである。

5.7.3.3 入力

591 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) 利用者ガイダンス
- d) 管理者ガイダンス
- e) セキュアな設置、生成、及び立上げの手順

5.7.3.4 評価者アクション

592 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_USR.1.1E

5.7.3.4.1 アクション AGD_USR.1.1E

AGD_USR.1.1C

1:AGD_USR.1-1 評価者は、利用者ガイダンスが TOE の非管理者である利用者が使用できるセキュリティ機能とインタフェースを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**。

593 利用者ガイダンスには、利用者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

594 利用者ガイダンスには、セキュリティインタフェースと機能の目的を識別し、記述するべきである。

AGD_USR.1.2C

1:AGD_USR.1-2 評価者は、利用者ガイダンスが TOE により提供された利用者がアクセスできるセキュリティ機能の使用法を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**。

595 利用者ガイダンスには、利用者が使用できるセキュリティインタフェースと機能のふるまいと相互関係を識別し、記述するべきである。

596 利用者が TOE セキュリティ機能を起動することができる場合、利用者ガイダンスに、その機能に対して利用者が使用できるインタフェースの記述を提供する。

597 各インタフェースと機能に対して、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、コマンドボタンなど）。

b) 利用者が設定するパラメタ及びそれらの正当な値とデフォルトの値を記述する。

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。

AGD_USR.1.3C

1:AGD_USR.1-3 評価者は、利用者ガイダンスがセキュアな処理環境で管理されなければならない利用者がアクセスできる機能と権限についての警告を含んで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**。

598 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利用者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。これらの利用者がアクセス可能な機能と権限は、利用者ガイダンスに記述される。

599 利用者ガイダンスでは、使用できる機能と権限、それらに必要となるコマンドのタイプ、そのようなコマンドの理由を識別するべきである。利用者ガイダンスには、管理するべき機能と権限の使用に関する警告を含めるべきであること。警告では、期待される効果、考えられる副次的効果、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_USR.1.4C

1:AGD_USR.1-4 評価者は、利用者ガイダンスが TOE セキュリティ環境のステートメントに記述されている利用者のふるまいについての前提条件に関連した責任を含む、TOE のセキュアな運用に必要なすべての利用者の責任を提示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**。

600 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関係する情報のみを利用者ガイダンスに含める必要がある。

- 601 利用者ガイダンスでは、セキュリティ機能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。
- 602 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。
- 603 利用者ガイダンスでは、利用者が機能を起動することができるかどうかまたは利用者が管理者の助けを必要とするかどうかを示すべきである。

AGD_USR.1.5C

- 1:AGD_USR.1-5 評価者は、利用者ガイダンスが評価のために提供された他のすべての証拠資料と一貫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**。
- 604 評価者は、評価のために提供された利用者ガイダンスとその他のすべての文書が互いに矛盾しないことを保証する。この保証は、ST に TOE セキュリティ環境とセキュリティ対策方針に関する TOE 利用者への警告についての詳細な情報が含まれているときに特に必要となる。
- 605 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_USR.1.6C

- 1:AGD_USR.1-6 評価者は、利用者ガイダンスが利用者に関連する TOE の IT 環境に対するすべてのセキュリティ要件を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**。
- 606 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。
- 607 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。
- 608 評価者は、TOE の IT 環境に対するセキュリティ要件（ST のオプションステートメント）を分析し、利用者にとって適切な ST のすべてのセキュリティ要件が利用者ガイダンスに適切に記述されていることを保証するために、利用者ガイダンスと比較するべきである。

5.8 テスタクティビティ

609 このアクティビティの目的は、TSF のサブセットを独立にテストすることにより、TOE が設計証拠資料に特定されているとおりに、及び ST に特定されている TOE セキュリティ機能要件に従ってふるまうかどうかを決定することである。

610 EAL1 でのテストアクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ATE_IND.1

5.8.1 適用上の注釈

611 評価者のテストサブセットのサイズと構成は、独立テスト (ATE_IND.1) サブアクティビティに記述されているいくつかの要因に依存する。サブセットの構成に影響を与えるそのような要因の 1 つは、評価者が (例えば、組織(scheme)から) アクセスする必要がある情報である *知られている公知の弱点 (known public domain weakness)* である。

612 テストを作成するために、評価者は、それが満たす必要がある要件において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。評価者は、TOE の期待されるふるまい方の理解を得るために、1 度に TSF の 1 つのセキュリティ機能に焦点をあて、ST 要件と機能仕様及びガイダンス証拠資料の関連する部分を検査することができる。

5.8.2 独立テストの評価 (ATE_IND.1)

5.8.2.1 目的

613 このサブアクティビティの目的は、TSF のサブセットを独立にテストすることにより、TSF が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。

5.8.2.2 入力

614 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) 利用者ガイダンス
- d) 管理者ガイダンス
- e) セキュアな設置、生成、及び立上げの手順
- f) テストに適した TOE

5.8.2.3 評価者アクション

615 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ATE_IND.1.1E

b) ATE_IND.1.2E

5.8.2.3.1 アクション ATE_IND.1.1E

ATE_IND.1.1C

1:ATE_IND.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**。

616 テストに使用する TOE は、ACM_CAP.1 サブアクティビティで確証されるのと同じ一意のリファレンスを持つべきである。

617 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個別のハードウェアとソフトウェア実装で構成することができる。評価者は、ST に記述されている各評価済みの構成に一貫するテスト構成が存在することを検証する。

618 評価者は、テスト環境に適用できる ST に記述されている TOE 環境のセキュリティの側面についての前提条件を考慮すべきである。ST にはテスト環境に適用されない前提条件がいくつか存在することがある。例えば、利用者の取扱許可についての前提条件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前提条件は適用するだろう。

619 いずれかのテスト資源（例えば、メータ、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。

1: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**。

620 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、ADO_IGS.1 サブアクティビティ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確信している場合、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て、TOE を設置、生成し、立上げる開発者の手順に従うべきである。

621 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 1:ADO_IGS.1-2 の条件を満たすことができる。

5.8.2.3.2 アクション ATE_IND.1.2E

1: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**。

- 622 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厳密にではなくテストでき得る多くのセキュリティ機能を含めることである。別のテスト方策は、気が付いた問題との関連に基づいたいくつかのセキュリティ機能を含んだテストサブセットを持ち、これらの機能を厳密にテストすることである。
- 623 一般的に、評価者のテスト手法は、これら 2 つの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、ST に識別されているほとんどのセキュリティ機能要件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。
- 624 評価者は、テストする TSF 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セキュリティ機能の数。TOE に含まれているセキュリティ機能の数が少ない場合には、すべてのセキュリティ機能を厳密にテストすることが現実的にできる。多数のセキュリティ機能を持つ TOE では、これは費用効果が悪く、サンプリングが必要になる。
 - b) 評価アクティビティのバランスの維持。テストは通常、評価中の評価者労力の 20 ~ 30% を占める。
- 625 評価者は、サブセットを構成するセキュリティ機能を選択する。この選択は、数多くの要因に依存し、これらの要因の考慮は、テストサブセットサイズの選択にも影響を与える。
- a) TOE の種別に一般的に関係する知られている公知の弱点（例えば、オペレーティングシステム、ファイアウォール）。TOE の種別に関係する知られている公知の弱点は、テストサブセットの選択プロセスに影響する。評価者は、その種別の TOE に対して知られている公知の弱点に対処するそれらのセキュリティ機能をサブセットに含めるべきである（ここでの知られている公知の弱点は、そのような脆弱性を意味せず、この個々の種別の TOE で経験された不十分性または問題領域を意味する）。そのような弱点が知られていない場合には、セキュリティ機能の広い範囲を選択する比較一般的な手法がさらに適している。
 - b) セキュリティ機能の重要性。TOE に対するセキュリティ対策方針の観点から他のセキュリティ機能よりも重要なセキュリティ機能を、テストサブセットに含められるべきである。
 - c) セキュリティ機能の複雑性。複雑なセキュリティ機能は、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めんどろな要求を課す複雑なテストを必要とするかもしれない。逆に複雑なセキュリティ機能は、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。
 - d) 暗黙のテスト。あるセキュリティ機能のテストは、しばしば暗黙に他のセキュリティ機能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、（暗黙にはあるが）テストされるセキュリティ機能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を提供するために使用され、効率的なテスト手法の標的となる。

- e) TOE への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。
- f) 革新的または一般的でない機能。販売広告用の印刷物で強調しているような革新的または一般的でないセキュリティ機能が TOE に含まれている場合、これらは、テストの有力な候補となるべきである。

626 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。

627 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

1: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**。

628 評価者は、ST 及び機能仕様からセキュリティ機能の期待されるふるまいを理解して、機能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、セキュリティ機能を外部インタフェースでテストするか、テストハーネス(test harness)を使用して内部インタフェースでテストするか、または別のテスト手法（例えば、例外状況、コード検査）を採用するべきか。
- b) セキュリティ機能を刺激し、応答を観察するために使用されるセキュリティ機能インタフェース。
- c) テストに存在する必要がある初期条件（すなわち、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) セキュリティ機能を刺激する（例えば、パケットジェネレータ）またはセキュリティ機能を観察する（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。

629 評価者は、一連のテストケースを使用して各セキュリティ機能をテストするのが実際的であることを発見することがある。その場合、各テストケースは、期待されるふるまいの大変特定な局面をテストする。

630 評価者のテスト証拠資料は、必要に応じて、該当する設計仕様、及び ST 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。

1:ATE_IND.1-5 評価者はテストを**実施しなければならない**。

631 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。

1: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) テストするセキュリティ機能のふるまいの識別
- 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) すべての前提となるテスト条件を確立するための指示
- d) セキュリティ機能を刺激するための指示
- e) セキュリティ機能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

632 詳細のレベルは、他の評価者がテストを繰り返し、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、異なっても良いが、全体的な結果は同一であるべきである。

633 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ある場合がある（例えば、テストの実際の結果が、期待される結果と比較するまえに、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。

1: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**。

634 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は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変更を必要とする。この決定とそれを正当とする理由は、評価者に任される。

1: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成果を**報告しなければならない**。

635 ETR に報告される評価者のテスト情報は、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、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、他の評価者や監督者が、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。

- 636 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セキュリティ機能の量とサイズの正当とする理由。
 - c) サブセットを構成するセキュリティ機能の選択基準。サブセットに含めるセキュリティ機能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) テストされたセキュリティ機能。サブセットに含めることに値したセキュリティ機能の簡単なリスト。
 - 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。
- 637 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 に示すべきタイプの情報を提供することだけを意図している。

6 章 EAL2 評価

6.1 導入

638 EAL2 は、低レベルから中レベルの独立に保証されたセキュリティを提供する。セキュリティ機能は、セキュリティのふるまいを理解するための TOE の機能仕様、ガイダンス証拠資料、上位レベル設計を使用して分析される。分析は、TOE セキュリティ機能のサブセットの独立テスト、機能仕様に基づく開発者のテストの証拠、開発者テスト結果の選択的確認、機能強度の分析、開発者による明らかな脆弱性の探索の証拠によってサポートされる。それ以上の保証は、TOE の構成リスト及びセキュアな配付手続きの証拠を通して得られる。

6.2 目的

639 この章の目的は、EAL2 評価を行うための最小の評価成果を定義し、評価を行うための方法と手段についてのガイダンスを提供することである。

6.3 EAL2 評価関係

640 EAL2 評価は、次のことを扱う。

- a) 評価入力タスク (2 章)
- b) 次のもので構成される EAL2 評価アクティビティ
 - 1) ST の評価 (4 章)
 - 2) 構成管理の評価 (6.4 節)
 - 3) 配付及び運用文書の評価 (6.5 節)
 - 4) 開発文書の評価 (6.6 節)
 - 5) ガイダンス文書の評価 (6.7 節)
 - 6) テストの評価 (6.8 節)
 - 7) テスト (6.8 節)
 - 8) 脆弱性評定の評価 (6.9 節)
- c) 評価出力タスク (2 章)

641 評価アクティビティは、CC パート 3 に含まれている EAL2 保証要件から引き出される。

- 642 ST が TOE 評価サブアクティビティを行うための基礎と状況を提供するために、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。
- 643 EAL2 評価を構成するサブアクティビティが、この章に記述されている。サブアクティビティは、一般的に、多少とも同時に開始することができるが、評価者は、サブアクティビティの間のいくつかの依存性を考慮する必要がある。
- 644 依存性のガイダンスについては、附属書 B.4 を参照のこと。

6.4 構成管理アクティビティ

645 構成管理アクティビティの目的は、消費者が評価済み TOE を識別する手助けをすること、及び構成要素が一意に識別されていることを保証することである。

646 EAL2 での構成管理アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ACM_CAP.2

6.4.1 CM 能力の評価 (ACM_CAP.2)

6.4.1.1 目的

647 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決定することである。

6.4.1.2 適用上の注釈

648 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。ACM_CAP.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。

6.4.1.3 入力

649 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

6.4.1.4 評価者アクション

650 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

a) ACM_CAP.2.1E

6.4.1.4.1 アクション ACM_CAP.2.1E

ACM_CAP.2.1C

2:ACM_CAP.2-1 評価者は、評価のために提供された TOE のバージョンが一意にリファレンスされていることを **チェックしなければならない**。

651 評価者は、構成リストをチェックすることによりリファレンスの一意性の正当性を確認し、構成要素が一意に識別されていることを保証するために、開発者の CM シ

システムを使用すべきである。その評価の間に 1 つだけのバージョンが検査されたならば、評価のために提供されたバージョンが一意にリファレンスされていることの証拠としては、不完全である。そこで評価者は、一意のリファレンスをサポートできるリファレンスシステム（例えば、数字、文字または日付の使用）を探すべきである。それにもかかわらず、いかなるリファレンスも存在しない場合、通常、TOE が一意に識別できると評価者が確信しない限り、この要件に対する判定は不合格となる。

- 652 評価者は、TOE の複数のバージョンを検査するようにし（例えば、脆弱性が発見された後のリワーク中に）、2 つのバージョンが別々にリファレンスされることをチェックすべきである。
- 653 ACM_CAP.2.2C
- 2:ACM_CAP.2-2 評価者は、評価のために提供された TOE がそのリファレンス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**。
- 654 評価者は、TOE の異なるバージョンを区別することができる一意のリファレンスが TOE に含まれていることを保証すべきである。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。
- 655 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、スタートアップルーチンの間に、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。
- 2:ACM_CAP.2-3 評価者は、使用されている TOE リファレンスが一貫していることを**チェックしなければならない**。
- 656 もし、TOE に 2 度以上の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。評価者は、提供された CM 証拠資料の一部である構成リストを使用して識別情報の一貫性のある使用を検証することができる。
- 657 評価者は、TOE リファレンスが ST と一貫性があることも検証する。
- 658 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。
- ACM_CAP.2.3C
- 2:ACM_CAP.2-4 評価者は、提供された CM 証拠資料が構成リストを含んでいることを**チェックしなければならない**。

659 構成リストは、構成制御(configuration control)のもとで維持されている要素を識別する。

ACM_CAP.2.4C

2:ACM_CAP.2-5 評価者は、構成リストが TOE を構成する構成要素を識別していることを決定するために、そのリストを**検査しなければならない**。

660 構成リストに含まれるべき構成要素の最小範囲は、ACM_SCP によって与えられる。ACM_SCP コンポーネントが含まれていない場合、評価者は、CM に対する開発者のアプローチに基づいて、ACM_SCP.1 の要件を上限とし（そこに要求されている以上を期待することは適切でないため）、リストの妥当性を評価すべきである。例えば、TOE または証拠資料のいずれかの要素に変更がなされたとき、評価者は、その要素が再発行される粒度のレベルで観察する、または問い合わせることができる。この粒度は、構成リストに現れる構成要素に一致するべきである。

ACM_CAP.2.5C

2:ACM_CAP.2-6 評価者は、構成要素の識別方法が、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、その識別方法を**検査しなければならない**。

ACM_CAP.2.6C

2:ACM_CAP.2-7 評価者は、構成リストが各構成要素を一意に識別していることを**チェックしなければならない**。

661 構成リストには、TOE を構成する構成要素のリストと、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。

6.5 配付及び運用アクティビティ

662 配付及び運用アクティビティの目的は、開発者が意図したのと同じ方法で TOE が設置され、生成され、開始され、変更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が適切であることを判断することである。これには、TOE の輸送中に取られる手続きと、初期化、生成、及び立上げの両方の手順が含まれる。

663 EAL2 での配付及び運用アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ADO_DEL.1

b) ADO_IGS.1

6.5.1 配付の評価 (ADO_DEL.1)

6.5.1.1 目的

664 このサブアクティビティの目的は、配付証拠資料が TOE を利用者サイトへ配送するときの完全性を維持するために使用されるすべての手続きを記述していることを決定することである。

6.5.1.2 入力

665 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) 配付証拠資料

6.5.1.3 評価者アクション

666 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ADO_DEL.1.1E

b) ADO_DEL.1.2D に基づく暗黙の評価者アクション

6.5.1.3.1 アクション ADO_DEL.1.1E

ADO_DEL.1.1C

2:ADO_DEL.1-1 評価者は、配付証拠資料が、TOE の版またはその一部を利用者サイトへ配送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**。

667 用語「必要」(*necessary*)の解釈は、TOE の本質と ST に含まれている情報を考慮する必要がある。提供される保護レベルは、ST に識別されている前提条件、脅威、組織のセキュリティ方針、及びセキュリティ対策方針と一致しているべきである。場合によっては、これらは、配付に対して明示的に表されないことがある。評価者

は、均衡の取れたアプローチが取られ、配付が、その他の点でセキュアな開発処理での明らかな弱点を表さないことを決定するべきである。

- 668 配付手続きは、TOE の識別を決定し、TOE またはそのコンポーネント部分の輸送中の完全性を維持するための適切な手続きを記述する。手続きは、これらの手続きが扱う必要がある TOE の部分を記述する。それには、必要に応じて、物理的または電子的（例えば、インターネットからダウンロードするための）配送の手続きが含まれているべきである。配付手続きは、該当するソフトウェア、ハードウェア、ファームウェア及び証拠資料など、TOE 全体に関連する。
- 669 完全性は、常に TOE の配付で懸念されるために、完全性を重視することは、驚くことではない。機密性と可用性が懸念される場合、それらも、このワークユニットで考慮されるべきである。
- 670 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するべきである。
- 2:ADO_DEL.1-2 評価者は、配付手続きが、選択された手続きとそれが扱う TOE の部分がセキュリティ対策方針を達成するのに適し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**。
- 671 配付手続きの選択の適合性には、特定の TOE（例えば、ソフトウェアかハードウェアか）及びセキュリティ対策方針が影響する。
- 672 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。配送には、公共郵便または民間の配送サービスが受け入れられる。
- 6.5.1.3.2 暗黙の評価者アクション
- ADO_DEL.1.2D
- 2:ADO_DEL.1-3 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**。
- 673 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べきである。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送場所の訪問
 - b) 配付のいくつかの段階、または利用者サイトでの TOE の検査（例えば、改ざん防止シール(tamper proof seals)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
- 674 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

- 675 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、将来の配付で使用される適切な手続きと施設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 (dry run)」を要求することができる。開発者が他の同様の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、保証を提供する上で役に立つことがある。

6.5.2 設置、生成及び立上げの評価 (ADO_IGS.1)

6.5.2.1 目的

676 このサブアクティビティの目的は、TOE のセキュアな設置、生成、及び立上げのための手順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。

6.5.2.2 入力

677 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) 管理者ガイダンス
- b) セキュアな設置、生成、及び立上げの手順
- c) テストに適した TOE

6.5.2.3 適用上の注釈

678 設置、生成及び立上げ手順は、それらが利用者サイトで行われるか、または ST の記述に従って TOE をセキュアな構成にするために必要となる開発サイトで行われるかに関係なく、すべての設置、生成、及び立上げの手順に関係している。

6.5.2.4 評価者アクション

679 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADO_IGS.1.1E
- b) ADO_IGS.1.2E

6.5.2.4.1 アクション ADO_IGS.1.1E

ADO_IGS.1.1C

2:ADO_IGS.1-1 評価者は、TOE のセキュアな設置、生成及び立上げに必要な手順が提供されていることを **チェックしなければならない**。

680 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合（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（または影響を受ける部分）は、適用されないために、満たされているものとみなされる。

6.5.2.4.2 アクション ADO_IGS.1.2E

2:ADO_IGS.1-2 評価者は、TOE のセキュアな設置、生成及び立上げに必要なステップを記述していることを決定するために、提供された設置、生成、及び立上げの手順を **検査しなければならない**。

- 681 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合（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（または影響を受ける部分）は、適用されないために、満たされているものとみなされる。
- 682 設置、生成及び立上げの手順は、次のものに対する詳細な情報を提供することができる。
- a) TSF の制御のもとでのエンティティの設置の特定セキュリティ特性の変更
 - b) 例外及び問題の取扱い
 - c) 適切に、セキュアな設置のための最小限のシステム要件
- 683 設置、生成及び立上げの手順の結果、セキュアな構成となることを確認するために、評価者は、開発者の手順に従って、提供されたガイダンス証拠資料だけを使用して、顧客が（TOE に適用される場合）TOE を設置、生成、及び立上げするために通常行うことが予想されるアクティビティを実行することができる。このワークユニットは、2:ATE_IND.2-2 ワークユニットとともに実行することができる。

6.6 開発アクティビティ

- 684 開発アクティビティの目的は、TSF が TOE のセキュリティ機能を提供する方法を理解するための適合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調べ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（TOE の外部インタフェースを記述する）及び上位レベル設計（内部サブシステムの観点から TOE のアーキテクチャを記述する）からなる。表現対応（一貫性を保証するために TOE の表現を相互にマッピングする）も存在する。
- 685 EAL2 の開発アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。
- a) ADV_FSP.1
 - b) ADV_HLD.1
 - c) ADV_RCR.1

6.6.1 適用上の注釈

- 686 設計証拠資料の CC 要件は、形式性によってレベル付けされている。CC は、文書の形式性の程度（すなわち、非形式的、準形式的または形式的のどれであるか）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。方法論は、使用すべき特定の言語を指示しない。その問題は、制度に任されている。次の段落は、各種の非形式的文書の内容を区別している。
- 687 非形式的機能仕様は、セキュリティ機能の記述（TOE 要約仕様と同等のレベルでの）及び TSF への外部に見えるインタフェースの記述からなる。例えば、オペレーティングシステムが自己を識別する手段、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、記録する監査機能も含まれている場合には、これらの監査機能の記述も機能仕様に含まれることが期待される。これらの機能は、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、それらは、利用者の外部インタフェースで何が起きるかによって影響される。
- 688 非形式的上位レベル設計は、各サブシステムでそのインタフェースでの刺激にตอบสนองして起きる一連のアクションとして表される。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上位レベル設計記述は、取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取るアクションとして記述する。
- 689 対応の実証の非形式は、散文形式である必要はない。簡単な 2 次元のマッピングで十分である。例えば、1 つの軸に沿ってモジュールが示され、他の軸に沿ってサブシステムが示され、セルがこれら 2 つの対応を識別するマトリックスは、上位レベル設計と下位レベル設計の間の適切な非形式的対応を提供することができる。

6.6.2 機能仕様の評価 (ADV_FSP.1)

6.6.2.1 目的

690 このサブアクティビティの目的は、開発者が TOE のセキュリティ機能の適切な記述を提供しているかどうか及び TOE が提供するセキュリティ機能が ST のセキュリティ機能要件を十分に満たしているかどうかを決定することである。

6.6.2.2 入力

691 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) 利用者ガイダンス
- d) 管理者ガイダンス

6.6.2.3 評価者アクション

692 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_FSP.1.1E
- b) ADV_FSP.1.2E

6.6.2.3.1 アクション ADV_FSP.1.1E

ADV_FSP.1.1C

2:ADV_FSP.1-1 評価者は、機能仕様がすべての必要な非形式的説明文を含んで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**。

693 機能仕様全体が非形式的である場合、このワークユニットは、適用されないために、満たされているものとみなされる。

694 補助的な叙述的記述は、準非形式的または形式的記述だけでは理解するのが困難な機能仕様の部分に必要となる（例えば、形式的表記の意味を明確にするため）。

ADV_FSP.1.2C

2:ADV_FSP.1-2 評価者は、機能仕様が内部的に一貫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**。

695 評価者は、TSFI を構成するインタフェースの記述が TSF の機能の記述と一貫していることを保証することにより、機能仕様の正当性を確認する。

696 一貫性の分析のガイダンスについては、附属書 B.3 を参照。

ADV_FSP.1.3C

2:ADV_FSP.1-3 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべてを識別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**。

697 用語「外部」(*external*)は、利用者に見えることを意味する。TOE への外部インタフェースは、TSF への直接インタフェースであるかまたは TOE の TSF 以外の部分へのインタフェースのいずれかである。ただし、これらの TSF 以外のインタフェースは、最終的に TSF にアクセスすることがある。TSF に直接または間接的にアクセスするこれらの外部インタフェースは、一体となって TOE セキュリティ機能インタフェース (TSFI) を構成する。図 6.1 は、TSF (陰影の付いた) 部分と TSF 以外 (空白) の部分を持つ TOE を示している。この TOE には、3 つの外部インタフェースがある。ここで、インタフェース *c* は、TSF への直接インタフェースである。インタフェース *b* は、TSF への間接インタフェースである。インタフェース *a* は、TOE の TSF 以外の部分へのインタフェースである。そこで、インタフェース *b* と *c* が TSFI を構成する。

698 CC パート 2 (またはその拡張コンポーネント) の機能要件に反映されているすべてのセキュリティ機能は、ある種の外部から見える表示を持つことに注意されるべきである。これらすべてが必ずしもセキュリティ機能をテストすることができるインタフェースとは限らないが、それらは、すべて、ある程度まで外部から見えるものであり、したがって機能仕様に含まれる必要がある。

699 TOE の境界を決定するガイダンスについては、附属書 B.6 を参照。

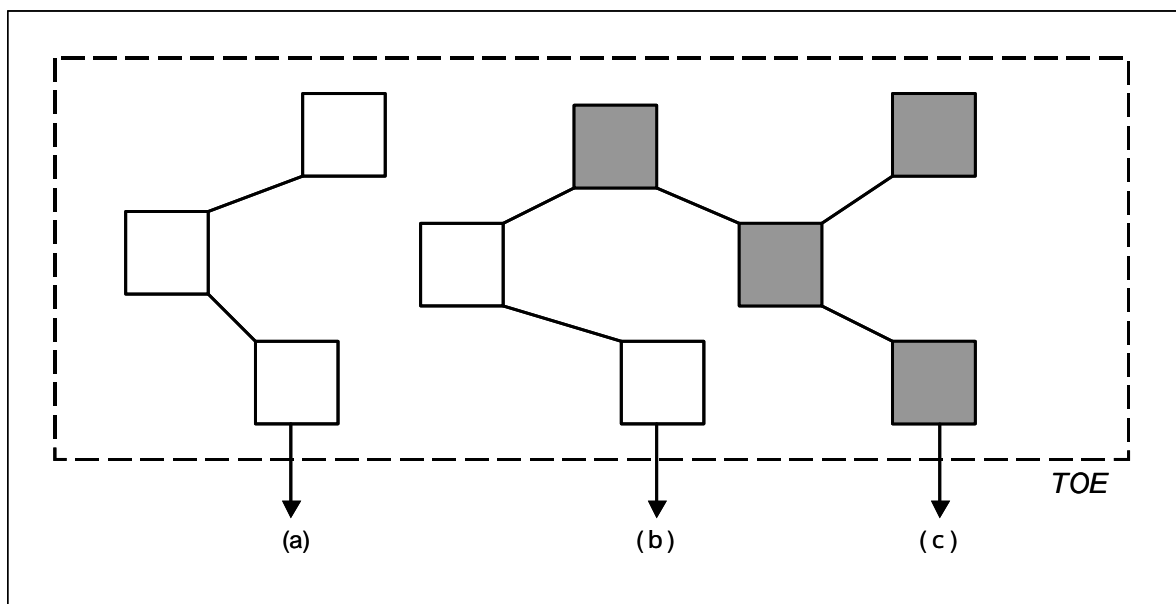


図 6.1 TSF インタフェース

2:ADV_FSP.1-4 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべて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**。

- 700 悪意のある利用者からの脅威のない TOE（すなわち、FPT_PHP、FPT_RVM 及び FPT_SEP が ST から正当に除外されている）では、機能仕様（そして他の TSF 表現記述に展開される）に記述されている唯一のインタフェースは、TSF との間のインタフェースである。FPT_PHP、FPT_RVM、及び FPT_SEP が存在しないことで、セキュリティ機能がバイパスされる心配がないことが想定されるので、他のインタフェースが TSF に与える影響についての心配がない。
- 701 他方、悪意のある利用者またはバイパスの脅威がある TOE（すなわち、FPT_PHP、FPT_RVM、及び FPT_SEP が ST に含まれている）では、すべての外部インタフェースが機能仕様に記述されているが、それは、それぞれの影響が明らかになる程度に限られている。セキュリティ機能へのインタフェース（すなわち、図 6.1 のインタフェース *b* と *c*）は、完全に記述されているが、他のインタフェースは、そのインタフェースを介して TSF へアクセスできない（すなわち、インタフェースは、図 6.1 のタイプ *b* ではなく、タイプ *a*）ことを明確にする範囲でのみ記述されている。FPT_PHP、FPT_RVM、及び FPT_SEP が含まれていることは、すべてのインタフェースが TSF に影響するおそれがあることを暗示している。各外部インタフェースは、潜在的な TSF インタフェースなので、機能仕様には、インタフェースがセキュリティに適切であるかどうかを評価者が決定できるように十分詳細な各インタフェースの記述を含める必要がある。
- 702 いくつかのアーキテクチャは、外部インタフェースのグループに対して十分詳細にこのインタフェース記述を、容易に提示している。例えば、カーネルアーキテクチャでは、オペレーティングシステムへのすべてのコールがカーネルプログラムで取り扱われる。TSP を侵害するかもしれないコールは、そのようにする権限を持つプログラムによってコールされなければならない。権限とともに実行されるすべてのプログラムは、機能仕様に含める必要がある。権限なしに実行されるカーネルの外部のあらゆるプログラムは、TSP に影響を与えることはできず（すなわち、そのようなプログラムは、図 6.1 のタイプ *b* ではなく、タイプ *a* のインタフェースである）そこで、機能仕様から除外することができる。カーネルアーキテクチャが存在する場合、評価者のインタフェース記述の理解は促進されるが、そのようなアーキテクチャは必ずしも必要ない。
- 2:ADV_FSP.1-5 評価者は、TSFI の提示が、効果、例外及び誤りメッセージを記述している各外部インタフェースにおいて、TOE のふるまいを適切に及び正しく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**。
- 703 インタフェースの提示が適切であり、正しいことを評価するために、評価者は、機能仕様、ST の TOE 要約仕様、及び利用者と管理者ガイダンスを使用して、次の要因を評定する。
- a) すべてのセキュリティに関係する利用者入力パラメタ（またはそれらのパラメタの特性化）は識別されるべきである。完全であるために、直接利用者が制御しないパラメタも、それらを管理者が使用できる場合、識別されるべきである。
 - b) レビュー済みガイダンスに記述されているすべてのセキュリティに関係するふるまいは、機能仕様の中で意味(semantics)の記述に反映させられるべきである。これには、事象及び各事象の影響としてのふるまいの識別を含めるべきである。例えば、ファイルが要求時に開かれない各理由（例えば、アクセス拒否、ファイルが存在しない、他の利用者がファイルを使用している、利用者は午後 5 時

以降ファイルを開くことが許されていない)に異なる誤りコードを提供するような、機能の豊富なファイルシステムインタフェースをオペレーティングシステムが提供する場合、機能仕様は、要求に対してファイルが開かれたか、または誤りコードが戻されたかを説明するべきである。(機能仕様は、誤りに対するこれらの異なる理由のすべてを列挙することができるが、そのような詳細を提供する必要はない。)意味の記述には、セキュリティ要件がインタフェースに適用される方法(例えば、インタフェースの使用が監査可能な事象であるかどうか、そして可能な場合は記録可能な情報かどうか)を含めるべきである。

- c) すべてのインタフェースは、操作のすべての可能なモードに対して記述される。TSF が権限の概念を提供する場合、インタフェースの記述は、権限がある場合とない場合のインタフェースのふるまいを説明するべきである。
- d) セキュリティに関係するパラメタの記述、及びインタフェースのシンタクス(syntax)に含まれる情報は、すべての証拠資料にわたって一貫しているべきである。

704 上記の検証は、機能仕様と ST の TOE 要約仕様及び開発者が提供する利用者及び管理者ガイダンスをレビューすることによって行われる。例えば、TOE がオペレーティングシステムとその下層のハードウェアである場合、評価者は、評価される TOE に適切であるとして、利用者アクセス可能プログラムの説明、プログラムのアクティビティを制御するために使用されるプロトコルの記述、プログラムのアクティビティを制御するために使用される利用者アクセス可能データベースの記述、及び利用者インタフェース(例えば、コマンド、アプリケーションプログラムインタフェース)を探す。評価者は、プロセッサ命令セットが記述されていることも保証する。

705 評価者が、設計、ソースコード、または他の証拠を検査し、機能仕様から抜けて落ちているパラメタまたは誤りメッセージが含まれることを発見するまでは、機能仕様不完全であることを発見しないようなものであるため、このレビューは繰り返される。

ADV_FSP.1.4C

2:ADV_FSP.1-6 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**。

706 TSF 提示が完全であることを評定するために、評価者は、ST の TOE 要約仕様、利用者ガイダンス、及び管理者ガイダンスを調べる。これらはいずれも、機能仕様の TSF 表現に含まれていないセキュリティ機能を記述するべきでない。

6.6.2.3.2 アクション ADV_FSP.1.2E

2:ADV_FSP.1-7 評価者は、機能仕様 TOE セキュリティ機能要件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**。

707 すべての ST セキュリティ機能要件が機能仕様によって扱われていることを保証するために、評価者は、TOE 要約仕様と機能仕様間のマッピングを作成することができる。そのようなマッピングは、対応(ADV_RCR.*)要件を満たしていることの証拠として開発者によってすでに提供されていることがある。その場合には、

評価者は、このマッピングが完全であることを単に検証して、すべてのセキュリティ機能要件が機能仕様の適切な TSFI 表現にマッピングされていることを保証することだけが必要である。

2:ADV_FSP.1-8 評価者は、機能仕様が TOE 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、その仕様を**検査しなければならない**。

708 特定の特性を備えたセキュリティ機能への各インタフェースに対して、機能仕様の詳細な情報は、ST に特定されているように正確でなければならない。例えば、ST にパスワードの長さが 8 文字でなければならないという利用者認証要件が含まれている場合、TOE は、8 文字のパスワードを持つ必要がある。機能仕様が 6 文字の固定長のパスワードを記述している場合、機能仕様は要件の正確な具体化ではない。

709 制御された資源で動作する機能仕様の各インタフェースについて、評価者は、それがセキュリティ要件の 1 つを実施することによる起りうる失敗を示す誤りコードを戻すかどうかを決定する。誤りコードが戻されない場合、評価者は、誤りコードを戻されるべきかどうかを決定する。例えば、オペレーティングシステムは、制御されたオブジェクトを「OPEN (開く)」ためにインタフェースを提示することができる。このインタフェースの記述には、アクセスがそのオブジェクトに許可されていないことを示す誤りコードを含めることができる。そのような誤りコードが存在しない場合、評価者は、それが適切であることを確認するべきである (おそらく、アクセスの仲介は、OPEN ではなく、READ と WRITE で行われるため)。

6.6.3 上位レベル設計の評価 (ADV_HLD.1)

6.6.3.1 目的

710 このサブアクティビティの目的は、上位レベル設計が主要な構成ユニット（すなわち、サブシステム）の観点から TSF を記述しているかどうか、及び機能仕様の正しい具体化であるかどうかを決定することである。

6.6.3.2 入力

711 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) 上位レベル設計

6.6.3.3 評価者アクション

712 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_HLD.1.1E
- b) ADV_HLD.1.2E

6.6.3.3.1 アクション ADV_HLD.1.1E

ADV_HLD.1.1C

2:ADV_HLD.1-1 評価者は、上位レベル設計がすべての必要な非形式的説明文を含んでいることを決定するために、その設計を**検査しなければならない**。

713 上位レベル設計全体が非形式的である場合、このワークユニットは、適用されないため、満たされているものとみなされる。

714 準形式的または形式的記述だけでは理解が困難な上位レベル設計のこれらの部分には、補助的な説明的記述が必要となる（例えば、形式的表記の意味を明確にするために）。

ADV_HLD.1.2C

2:ADV_HLD.1-2 評価者は、上位レベル設計の提示が内部的に一貫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**。

715 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

- 716 評価者は、インタフェース仕様がサブシステムの目的の記述と一貫していることを保証することにより、サブシステムインタフェース仕様の正当性を確認する。

ADV_HLD.1.3C

- 2:ADV_HLD.1-3 評価者は、TSF 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、上位レベル設計を**検査しなければならない**。

- 717 上位レベル設計に関して、用語「サブシステム」(*subsystem*)は、大きな関連するユニット(メモリ管理、ファイル管理、プロセス管理など)を意味する。設計を基本的な機能領域に分解することは、設計を理解するのに役に立つ。

- 718 上位レベル設計を調べる主な目的は、評価者の TOE の理解を助けることである。開発者によるサブシステム定義と各サブシステム内の TSF のグループ化の選択は、TOE の意図する動作を理解する上で上位レベル設計を役に立つものにする重要な局面である。このワークユニットの一部として、評価者は、開発者が提示するサブシステムの数が適切であるかどうか、及びサブシステム内の機能のグループ化の選択が適切であるかどうかを評定するべきである。評価者は、TSF のサブシステムへの分解が、TSF の機能がどのように提供されるかを上位レベルで理解するために評価者にとって十分であることを保証するべきである。

- 719 上位レベル設計を記述するために使用されるサブシステムを「サブシステム」と呼ぶ必要はない。ただし、それは、同様の分解レベルを表しているべきである。例えば、設計は、「層」または「マネージャ」を使用して分解することもできる。

ADV_HLD.1.4C

- 2:ADV_HLD.1-4 評価者は、上位レベル設計が各サブシステムのセキュリティ機能を記述していることを決定するために、その設計を**検査しなければならない**。

- 720 サブシステムのセキュリティ機能のふるまいは、サブシステムが何を行うかの記述である。これには、サブシステムがその機能を使用して実行するように指示されるアクションと、サブシステムが TOE のセキュリティ状態に与える影響(例えば、サブジェクト、オブジェクト、セキュリティデータベースの変更など)の記述を含めるべきである。

ADV_HLD.1.5C

- 2:ADV_HLD.1-5 評価者は、上位レベル設計が TSF で必要とされるすべてのハードウェア、ファームウェア、及びソフトウェアを識別していることを決定するために、その設計を**チェックしなければならない**。

- 721 ST に IT 環境の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、適用されないために、満たされているものとみなされる。

- 722 ST に IT 環境に対するセキュリティ要件のオプションステートメントが含まれている場合、評価者は、上位レベル設計に記述される TSF が必要とするハードウェア、ファームウェア、またはソフトウェアのリストと、IT 環境のセキュリティ要件のステートメントを比較して、それらが一致することを決定する。ST の情報は、TOE が実行される下層の抽象マシンの特性を表す。

723 上位レベル設計に ST に含まれていない IT 環境のセキュリティ要件が含まれている場合、またはそれらが ST に含まれているものと異なる場合、この不一致は、アクション ADV_HLD.1.2E のもとで評価者によって評定される。

2:ADV_HLD.1-6 評価者は、下層のハードウェア、ファームウェア、またはソフトウェアで実装されている補助的な保護メカニズムが提供する機能の提示を、上位レベル設計が含んでいることを決定するために、その設計を**検査しなければならない**。

724 ST に IT 環境の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、適用されないために、満たされているものとみなされる。

725 TOE が実行される下層抽象マシンが提供する機能の提示は、TSF の一部である機能の提示と同じ詳細レベルである必要はない。提示は、TOE セキュリティ対策方針をサポートするために TOE が依存する IT 環境のセキュリティ要件を実装するハードウェア、ファームウェア、またはソフトウェアに提供されている機能を TOE が使用する方法を説明するべきである。

726 IT 環境のセキュリティ要件のステートメントは、ハードウェア、ファームウェア、またはソフトウェアの各種の異なる組み合わせにより満足することができる場合には特に、抽象的でもよい。テストアクティビティの一部として、評価者に IT 環境のセキュリティ要件を満たしていると主張されている下層マシンの少なくとも 1 つ以上の実例が提供される場合、評価者は、これが TOE の必要なセキュリティ機能を提供するかどうかを決定することができる。この評価者による決定には、下層マシンのテストまたは分析は必要ない。それによって提供されることが期待される機能が実際に存在することを決定するだけである。

ADV_HLD.1.6C

2:ADV_HLD.1-7 評価者は、上位レベル設計が TSF サブシステムへのインタフェースを識別していることを**チェックしなければならない**。

727 上位レベル設計には、各サブシステムに対する、各入口点の名前が含まれている。

ADV_HLD.1.7C

2:ADV_HLD.1-8 評価者は、上位レベル設計が、外部から見える TSF のサブシステムに対するインタフェースを識別していることを**チェックしなければならない**。

6.6.3.3.2 アクション ADV_HLD.1.2E

2:ADV_HLD.1-9 評価者は、上位レベル設計が TOE 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、その設計を**検査しなければならない**。

728 評価者は、各 TOE セキュリティ機能の上位レベル設計を分析し、機能が正確に記述されていることを保証する。評価者は、機能が上位レベル設計に含まれていない依存性を持っていないことも保証する。

729 評価者は、ST と上位レベル設計の両方で IT 環境のセキュリティ要件も分析し、それらが一致することを保証する。例えば、ST に監査証跡を格納するための TOE セキュリティ機能要件が含まれていて、さらに上位レベル設計では監査証跡の格納は、

IT 環境によって行われると述べられている場合、上位レベル設計は、TOE セキュリティ機能要件の正確な具体化ではない。

2:ADV_HLD.1-10 評価者は、上位レベル設計が TOE セキュリティ機能要件の完全な具体化であることを決定するために、その設計を **検査しなければならない**。

730 すべての ST セキュリティ機能要件が上位レベル設計で扱われていることを保証するために、評価者は、TOE セキュリティ機能要件と上位レベル設計の間のマッピングを作成することができる。

6.6.4 表現対応の評価 (ADV_RCR.1)

6.6.4.1 目的

731 このサブアクティビティの目的は、開発者が上位レベル設計に機能 ST の要件及び機能仕様を正しく及び完全に実装しているかどうかを決定することである。

6.6.4.2 入力

732 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) 上位レベル設計
- d) TOE 要約仕様と機能仕様の間の対応分析
- e) 機能仕様と上位レベル設計の間の対応分析

6.6.4.3 評価者アクション

733 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_RCR.1.1E

6.6.4.3.1 アクション ADV_RCR.1.1E

ADV_RCR.1.1C

2:ADV_RCR.1-1 評価者は、機能仕様が TOE セキュリティ機能の正しい、完全な表現であることを決定するために、TOE 要約仕様と機能仕様の間の対応分析を **検査しなければならない**。

734 評価者のこのワークユニットの目標は、TOE 要約仕様に識別されているすべてのセキュリティ機能が機能仕様に表現されていること及びそれらが正確に表現されていることを決定することである。

735 評価者は、TOE 要約仕様の TOE セキュリティ機能と機能仕様の間の対応をレビューする。評価者は、対応が一貫し、正確であることを調べる。対応分析が TOE 要約仕様のセキュリティ仕様と機能仕様のインタフェース記述の間の関係を示しているところでは、評価者は、両方のセキュリティ機能が同じであることを検証する。TOE 要約仕様のセキュリティ機能が、対応するインタフェースにおいて正しく、完全に表されている場合、このワークユニットは、満たされる。

736 このワークユニットは、ワークユニット 2:ADV_FSP.1-7 及び 2:ADV_FSP.1-8 とともに行うことができる。

2:ADV_RCR.1-2 評価者は、上位レベル設計が機能仕様の正しい、完全な表現であることを決定するために、機能仕様と上位レベル設計の間の対応分析を**検査しなければならない**。

737 評価者は、対応分析、機能仕様、及び上位レベル設計を使用して、機能仕様に識別されている各セキュリティ機能を上位レベル設計に記述されている TSF サブシステムにマッピングできることを保証する。各セキュリティ機能に対して、対応は、どの TSF サブシステムがその機能のサポートにかかわるかを示す。評価者は、上位レベル設計に各セキュリティ機能の正しい実現の記述が含まれていることを検証する。

6.7 ガイダンス文書アクティビティ

738 ガイダンス文書アクティビティの目的は、運用 TOE を使用する方法を記述している証拠資料が適切であることを判断することである。そのような証拠資料には、正しくないアクションが TOE のセキュリティに悪影響を与えることがある信頼された管理者と管理者以外の利用者に対する文書と、正しくないアクションが自分自身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信頼できない利用者に対する両方の文書がある。

739 EAL2 でのガイダンス文書アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) AGD_ADM.1

b) AGD_USR.1

6.7.1 適用上の注釈

740 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。

6.7.2 管理者ガイダンスの評価 (AGD_ADM.1)

6.7.2.1 目的

741 このサブアクティビティの目的は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を記述しているかどうかを決定することである。

6.7.2.2 適用上の注釈

742 用語「*管理者*」(*administrator*) は、TOE 構成パラメタの設定など、TOE 内のセキュリティの重要な操作を実行することを任された人間利用者を示す。この操作は、TSP の実施に影響を与えるので、管理者は、これらの操作を行うために必要な特定の権限を有している。管理者(一人または複数)の役割は、TOE の管理者以外の利用者の役割から明確に区別する必要がある。

743 監査者、管理者、または日常的な管理など、TOE により認識され、TSF と相互作用することができる ST に定義された異なる管理者の役割またはグループが存在することができる。各役割は、広範な能力のセットを含むか、または単一の能力であることができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。異なる管理者の役割とグループは、管理者ガイダンスにて考慮されるべきである。

6.7.2.3 入力

744 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順

6.7.2.4 評価者アクション

745 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_ADM.1.1E

6.7.2.4.1 アクション AGD_ADM.1.1E

AGD_ADM.1.1C

2:AGD_ADM.1-1 評価者は、管理者ガイダンスが TOE の管理者が利用できる管理セキュリティ機能とインタフェースを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**。

746 管理者ガイダンスには、管理者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

747 管理者ガイダンスは、管理者セキュリティインタフェースと機能の目的、ふるまい、及び相互関係を識別し、記述するべきである。

748 各管理者セキュリティインタフェースと機能に対して、管理者ガイダンスは、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) 管理者が設定するパラメタ、それらの正当な値とデフォルトの値を記述する。
- 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。

AGD_ADM.1.2C

2:AGD_ADM.1-2 評価者は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を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**。

749 管理者ガイダンスは、ST に記述されているものと一貫する IT 環境の TSP に従って、TOE を操作する方法を記述する。

AGD_ADM.1.3C

2:AGD_ADM.1-3 評価者は、管理者ガイダンスがセキュアな処理環境で管理されなければならない機能と権限に関する警告を含んで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**。

750 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利用者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、管理者ガイダンスに記述されるべきである。

751 管理者ガイダンスでは、管理すべき機能と権限、それらに必要な管理のタイプ、そのような管理の理由を識別する。警告では、期待される効果、考えられる副次的効果、他の機能と権限との考えられる相互作用を指摘する。

AGD_ADM.1.4C

2:AGD_ADM.1-4 評価者は、管理者ガイダンスが TOE のセキュアな運用に関連する利用者のふるまいに関するすべての前提条件を記述していることを決定するために、そのガイダンスを**検査しなければならない**。

752 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関する情報のみを管理者ガイダンスに含める必要がある。

753 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。

AGD_ADM.1.5C

2:AGD_ADM.1-5 評価者は、管理者ガイダンスが管理者の管理にあるすべてのセキュリティパラメータを、セキュアな値を適切に示して、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**。

754 各セキュリティパラメータに対して、管理者ガイダンスは、パラメータの目的、パラメータの正当な値とデフォルトの値、そのようなパラメータの安全及び安全でない、個別または組み合わせによる、使用設定を記述するべきである。

AGD_ADM.1.6C

2:AGD_ADM.1-6 評価者は、管理者ガイダンスが TSF の制御下にあるエンティティのセキュリティ特質の変更を含む、実行が必要な管理機能に関連するセキュリティ関連事象の各タイプを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**。

755 セキュリティ関連事象のすべてのタイプは、詳細に記述されているので、管理者は、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管理者が取る必要があるアクション（存在する場合）を知る。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、管理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_ADM.1.7C

2:AGD_ADM.1-7 評価者は、管理者ガイダンスが評価のために提供された他のすべての文書と一貫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**。

756 特に ST には、TOE セキュリティ環境とセキュリティ対策方針に関する TOE 管理者への警告に対する詳細な情報を含めることができる。

757 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_ADM.1.8C

2:AGD_ADM.1-8 評価者は、管理者ガイダンスが管理者に関連する TOE の IT 環境に対するすべての IT セキュリティ要件を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**。

758 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。

759 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。

760 評価者は、TOE の IT 環境に対するセキュリティ要件 (ST のオプションステートメント) を分析し、管理者にとって適切な ST のすべてのセキュリティ要件が管理者ガイダンスに適切に記述されていることを保証するために、それらを管理者ガイダンスと比較するべきである。

6.7.3 利用者ガイダンスの評価 (AGD_USR.1)

6.7.3.1 目的

761 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 が提供するセキュリティ機能とインタフェースを記述しているかどうか、及びこのガイダンスが TOE のセキュアな使用のための説明とガイドラインを提供しているかどうかを決定することである。

6.7.3.2 適用上の注釈

762 TOE によって認識され、TSF と相互作用を行うことができる ST に定義されている異なる利用者の役割とグループが存在することができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。異なる利用者の役割とグループは、利用者ガイダンスにて考慮されるべきである。

6.7.3.3 入力

763 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順

6.7.3.4 評価者アクション

764 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_USR.1.1E

6.7.3.4.1 アクション AGD_USR.1.1E

AGD_USR.1.1C

2:AGD_USR.1-1 評価者は、利用者ガイダンスが TOE の非管理者である利用者が使用できるセキュリティ機能とインタフェースを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。**

765 利用者ガイダンスには、利用者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

766 利用者ガイダンスには、セキュリティインタフェースと機能の目的を識別し、記述すべきである。

AGD_USR.1.2C

2:AGD_USR.1-2 評価者は、利用者ガイダンスが TOE により提供された利用者がアクセスできるセキュリティ機能の使用法を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**。

767 利用者ガイダンスには、利用者が使用できるセキュリティインタフェースと機能のふるまいと相互関係を識別し、記述すべきである。

768 利用者が TOE セキュリティ機能を起動することができる場合、利用者ガイダンスに、その機能に対して利用者が使用できるインタフェースの記述を提供する。

769 各インタフェースと機能に対して、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、コマンドボタンなど）
- b) 利用者が設定するパラメタ及びそれらの正当な値とデフォルトの値を記述する。
- 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。

AGD_USR.1.3C

2:AGD_USR.1-3 評価者は、利用者ガイダンスがセキュアな処理環境で管理されなければならない利用者がアクセスできる機能と権限についての警告を含んで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**。

770 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利用者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。これらの利用者がアクセス可能な機能と権限は、利用者ガイダンスに記述される。

771 利用者ガイダンスでは、使用できる機能と権限、それらに必要となるコマンドのタイプ、そのようなコマンドの理由を識別すべきである。利用者ガイダンスには、管理すべき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、考えられる副次的効果、他の機能と権限との考えられる相互作用を指摘すべきである。

AGD_USR.1.4C

2:AGD_USR.1-4 評価者は、利用者ガイダンスが TOE セキュリティ環境の記述の中にある利用者のふるまいについての前提条件に関連した責任を含む、TOE のセキュアな運用に必要なすべての利用者の責任を提示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**。

- 772 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関係する情報のみを利用者ガイダンスに含める必要がある。
- 773 利用者ガイダンスでは、セキュリティ機能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。
- 774 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。
- 775 利用者ガイダンスでは、利用者が機能を起動することができるかどうかまたは利用者が管理者の助けを必要とするかどうかを示すべきである。

AGD_USR.1.5C

2:AGD_USR.1-5 評価者は、利用者ガイダンスが評価のために提供された他のすべての証拠資料と一貫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**。

- 776 評価者は、評価のために提供された利用者ガイダンスとその他のすべての文書が互いに矛盾しないことを保証する。この保証は、ST に TOE セキュリティ環境とセキュリティ対策方針に関する TOE 利用者への警告についての詳細な情報が含まれているときに特に必要となる。
- 777 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_USR.1.6C

2:AGD_USR.1-6 評価者は、利用者ガイダンスが利用者に関連する TOE の IT 環境に対するすべてのセキュリティ要件を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**。

- 778 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。
- 779 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。
- 780 評価者は、TOE の IT 環境に対するセキュリティ要件（ST のオプションステートメント）を分析し、利用者にとって適切な ST のすべてのセキュリティ要件が利用者ガイダンスに適切に記述されていることを保証するために、利用者ガイダンスと比較するべきである。

6.8 テスタクティビティ

781 このアクティビティの目的は、TSF のサブセットを独立にテストすることにより、TOE が設計証拠資料に特定されているとおり、及び ST に特定されている TOE セキュリティ機能要件に従ってふるまうかどうかを決定することである。

782 EAL2 のテストアクティビティには、次のコンポーネントに関係するサブアクティビティが含まれる。

a) ATE_COV.1

b) ATE_FUN.1

c) ATE_IND.2

6.8.1 適用上の注釈

783 評価者は、開発者のテストを分析し、セキュリティ機能が特定どおりに実行されることを実証するため及び開発者のテストに対する手法を理解するためにそれらが十分であることを決定する。評価者は、また、開発者のテスト結果を信頼するために、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を実行する。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。このサブセットに対する評価者のテストは、特に開発者のテストに欠点がある場合、開発者のテストとは異なるテスト手法を取る。

784 評価者のテストサブセットのサイズと構成に影響するその他の要因は、独立テスト (ATE_IND.2) サブアクティビティに記述されている。サブセットの構成に影響を与えるそのような要因の 1 つは、評価者が (例えば、組織(scheme)から) アクセスする必要がある情報である *知られている公知の弱点 (known public domain weakness)* である。

785 開発者のテスト証拠資料が適切であること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、それが満たす必要がある要件において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。評価者は、TOE の期待されるふるまい方を理解するために、1 度に TSF の 1 つのセキュリティ機能に焦点をあて、ST 要件と機能仕様及びガイダンス証拠資料の該当する部分を検査することができる。

6.8.2 カバレッジの評価 (ATE_COV.1)

6.8.2.1 目的

786 このサブアクティビティの目的は、開発者のテストカバレッ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の間に対応を示しているかどうかを決定することである。

6.8.2.2 適用上の注釈

787 開発者が提供するカバレッジ分析は、評価証拠として提供されるテストと機能仕様の間に対応を示す必要がある。ただし、カバレッジ分析は、すべてのセキュリティ

機能がテストされていること、または TSF へのすべての外部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。そのような欠点は、独立テスト (ATE_IND.2) サブアクティビティ中に評価者が考慮する。

6.8.2.3

入力

788

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) 機能仕様
- b) テスト証拠資料
- c) テストカバレッジ証拠

6.8.2.4

評価者アクション

789

このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_COV.1.1E

6.8.2.4.1

アクション ATE_COV.1.1E

ATE_COV.1.1C

2: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の間に対応が正確であることを決定するために、テストカバレッジ証拠を**検査しなければならない**。

790

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なカバレッジ証拠は、完全なカバレッジを示すことよりむしろ、カバレッジの範囲を明らかにする。カバレッジが十分でない場合、評価者は、補うために独立テストのレベルを増やすべきである。

791

図 6.2 は、機能仕様に記述されているセキュリティ機能と、それらをテストするために使用されるテスト証拠資料に示されているテストの間の概念的枠組みを示している。テストには、テストの依存性または実行されるテストの全体的目標によって、1 つまたは複数のセキュリティ機能を含めることができる。

792

テストカバレッジ証拠に示されるテストとセキュリティ機能の識別は、識別されているテストとテストされたセキュリティ機能の機能仕様との明確な対応を示すことにより、曖昧でなくされるべきである。

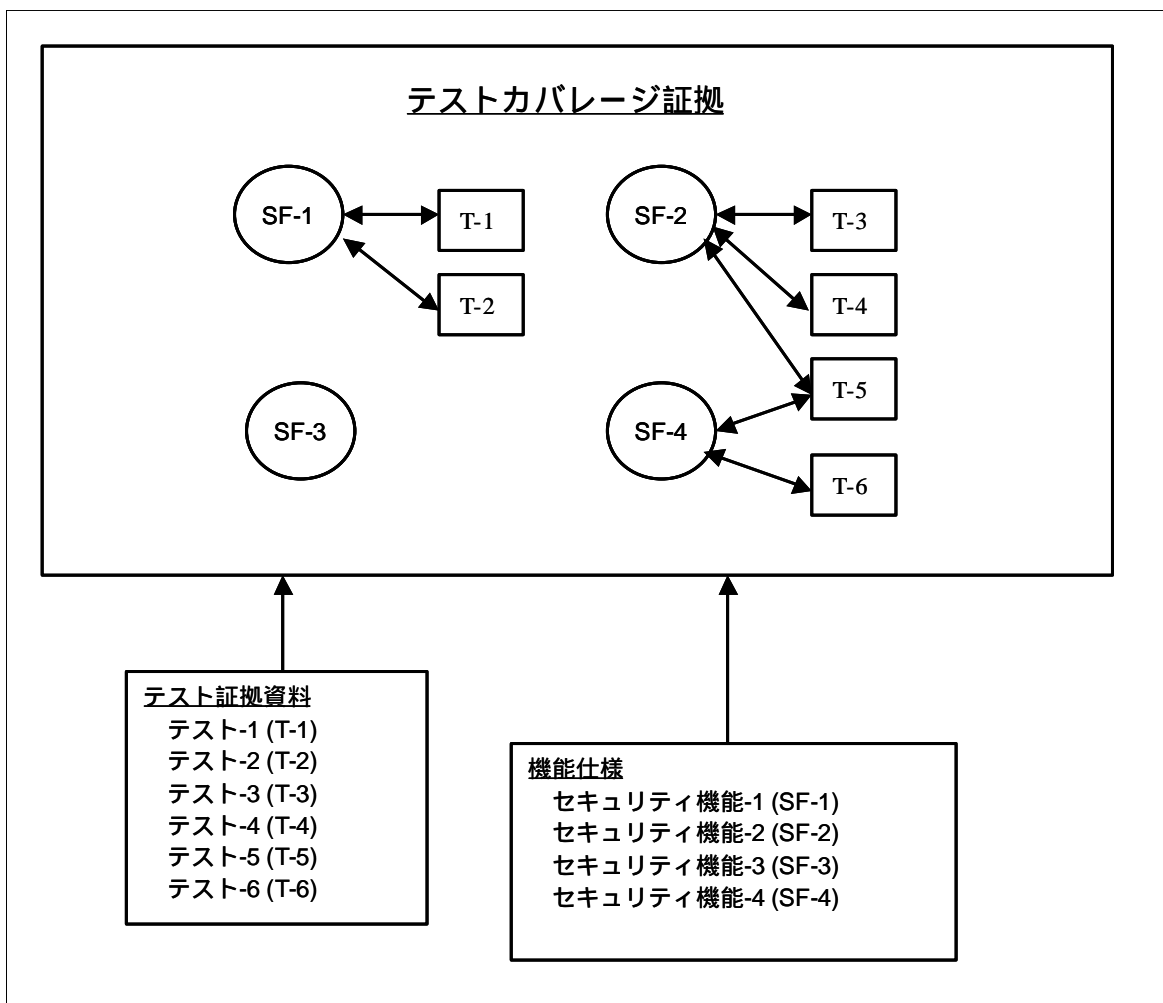


図 6.2 テストカバレッジ証拠の概念的枠組み

793

図 6.2 において、SF-3 は、それに関するテストが行われていないため、機能仕様に関するカバレッジは不完全である。しかしながら、カバレッジ証拠が機能仕様に識別されているセキュリティ機能の完全なカバレッジを示す必要はないために、不完全なカバレッジは、このサブアクティビティの判定に影響しない。

6.8.3 機能テストの評価 (ATE_FUN.1)

6.8.3.1 目的

794 このサブアクティビティの目的は、セキュリティ機能が特定されたとおりに実行されることを実証するのに、開発者の機能テスト証拠資料が十分であるかどうかを決定することである。

6.8.3.2 適用上の注釈

795 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、カバレッジ保証コンポーネントに依存する。

796 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が、特定されたとおりに実行しないことを示しているセキュリティ機能はいずれも、それが機能するか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。

6.8.3.3 入力

797 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) テスト手順

6.8.3.4 評価者アクション

798 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_FUN.1.1E

6.8.3.4.1 アクション ATE_FUN.1.1E

ATE_FUN.1.1C

2:ATE_FUN.1-1 評価者は、テスト証拠資料にテスト計画、テスト手順記述、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**。

ATE_FUN.1.2C

2:ATE_FUN.1-2 評価者は、テスト計画がテストされるセキュリティ機能を識別していることを**チェックしなければならない**。

EAL2:ATE_FUN.1

- 799 テストされるセキュリティ機能を識別するために使用できる 1 つの方法は、個々のセキュリティ機能を特定している機能仕様の適切な部分を参照することである。
- 800 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。
- 801 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 2:ATE_FUN.1-3 評価者は、テスト計画が実行されるテストの目標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**。
- 802 テスト計画は、セキュリティ機能をテストする方法とテストが行われるテスト構成についての情報を提供する。
- 803 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。
- 804 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 2:ATE_FUN.1-4 評価者は、TOE テスト構成が ST における評価のために識別されている構成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**。
- 805 テストに使用される TOE は、ACM_CAP.2 サブアクティビティによって確証されたのと同じ一意的なリファレンスと開発者が提供するテスト証拠資料を持つべきである。
- 806 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個別のハードウェアとソフトウェア実装で構成することができる。評価者は、ST に記述されている各評価済みの構成に一貫するテスト構成が存在することを検証する。
- 807 評価者は、テスト環境に適用できる ST に記述されている TOE 環境のセキュリティの側面についての前提条件を考慮するべきである。ST にはテスト環境に適用されない前提条件がいくつか存在することがある。例えば、利用者の取扱許可についての前提条件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前提条件は適用するだろう。
- 2:ATE_FUN.1-5 評価者は、テスト計画がテスト手順記述と一貫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**。
- 808 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。
- 809 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ATE_FUN.1.3C

- 2:ATE_FUN.1-6 評価者は、テスト手順記述がテストされる各セキュリティ機能のふるまいを識別していることを**チェックしなければならない**。

- 810 テストされるセキュリティ機能のふるまいを識別するために使用できる 1 つの方法は、テストする個々のふるまいを特定している設計仕様の適切な部分を参照することである。
- 811 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。
- 812 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 2:ATE_FUN.1-7 評価者は、もしあれば順序の依存性を含め、再現できる初期テスト条件を確立するための十分な指示が提供されていることを決定するために、テスト手順記述を**検査しなければならない**。
- 813 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まえに、追加される必要がある。他のテスト結果の順序に依存する一例は、アクセス制御のような他のセキュリティメカニズムに対する監査レコードを作成するために監査機能に頼るまえに、監査機能をテストする必要があることである。順序に依存する他の例としては、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。
- 814 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。
- 815 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 2:ATE_FUN.1-8 評価者は、セキュリティ機能を刺激し、それらのふるまいを観察するための再現可能な手段を取れるように十分な指示が提供されていることを決定するために、テスト手順記述を**検査しなければならない**。
- 816 刺激は、通常、TSFI を通して外部からセキュリティ機能に提供される。一度入力 (input) (刺激(stimulus)) が TSFI に提供されれば、セキュリティ機能のふるまいを TSFI で観察することができる。テスト手順に刺激とこの刺激の結果として期待されるふるまいを曖昧さなく記述した詳細な情報が含まれていない限り、再現可能であると保証されない。
- 817 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。
- 818 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 2:ATE_FUN.1-9 評価者は、テスト手順記述がテスト手順と一貫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**。
- 819 テスト手順記述がテスト手順である場合、このワークユニットは適用されず、条件は満たされているものとみなされる。
- 820 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。

- 821 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ATE_FUN.1.4C

- 2:ATE_FUN.1-10 評価者は、十分な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**。

- 822 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、テスト手法を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。

- 823 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。

- 824 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

ATE_FUN.1.5C

- 2:ATE_FUN.1-11 評価者は、テスト証拠資料の期待されるテスト結果が提供された実際の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**。

- 825 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。

- 826 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。

- 827 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）。

- 828 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変更を行わずに、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のは、開発者の責任である。

- 829 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。

- 830 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

- 831 いずれかのテストの期待されるテスト結果と実際のテスト結果が同じでない場合、セキュリティ機能が正しく働いているとの実証は達成されない。そのようなことは、関係するセキュリティ機能のテストを含める評価者の独立テストの成果に影響を与

える。評価者は、また、このワークユニットが行われる証拠のサンプルを増やすことを考慮するべきである。

2:ATE_FUN.1-12 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成果を**報告しなければならない**。

832 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、他の評価者や監督者が、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。

833 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) 実行された開発者テストの量。開発者テストのカバレッジと深さの範囲の記述。
- d) テスト結果。開発者テストの全体的な結果の記述。

834 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 に示すべきタイプの情報を提供することだけを意図している。

6.8.4 独立テストの評価 (ATE_IND.2)

6.8.4.1 目的

835 このアクティビティの目的は、TSF のサブセットを独立にテストすることにより TOE が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、また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の確信を得ることである。

6.8.4.2 入力

836 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) 利用者ガイダンス
- d) 管理者ガイダンス
- e) セキュアな設置、生成、及び立上げの手順
- f) テスト証拠資料
- g) テストカバレッジ分析
- h) テストに適した TOE

6.8.4.3 評価者アクション

837 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_IND.2.1E
- b) ATE_IND.2.2E
- c) ATE_IND.2.3E

6.8.4.3.1 アクション ATE_IND.2.1E

ATE_IND.2.1C

2: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**。

838 テストに使用される TOE は、ACM_CAP.2 サブアクティビティによって確認されたのと同じ一意的なリファレンスと開発者が提供するテスト証拠資料を持つべきである。

- 839 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個別のハードウェアとソフトウェア実装で構成することができる。評価者は、ST に記述されている各評価済みの構成に一貫するテスト構成が存在することを検証する。
- 840 評価者は、テスト環境に適用できる ST に記述されている TOE 環境のセキュリティの側面についての前提条件を考慮すること。ST にはテスト環境に適用されない前提条件がいくつか存在することがある。例えば、利用者の取扱許可についての前提条件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前提条件は適用するだろう。
- 841 いずれかのテスト資源（例えば、メータ、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。

2: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**。

- 842 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、ADO_IGS.1 サブアクティビティ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確信している場合、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て、TOE を設置、生成し、立上げする開発者の手順に従うべきである。
- 843 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 2:ADO_IGS.1-2 の条件を満たすことができる。

ATE_IND.2.2C

- 2: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**。
- 844 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。

6.8.4.3.2 アクション ATE_IND.2.2E

2:ATE_IND.2-4 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**。

- 845 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厳密にではなくテストでき得る多くのセキュリティ機能を含めることである。別のテスト方策は、気が付いた問題との関連に基づいたいくつかのセキュリティ機能を含んだテストサブセットを持ち、これらの機能を厳密にテストすることである。
- 846 一般的に、評価者のテスト手法は、これら 2 つの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、ST に識別されているほとんどのセ

セキュリティ機能要件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。

847 評価者は、テストする TSF 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、カバレッジ分析及びテスト証拠資料からなる。開発者テスト証拠は、テスト中に開発者がセキュリティ機能をテストした方法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) 特定のセキュリティ機能に対する開発者テストの増加。評価者は、セキュリティ機能をさらに厳密にテストするためにパラメータを変えて、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) 特定のセキュリティ機能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、特定のセキュリティ機能のテスト手法を変更することができる。
- b) テストサブセットに加えるセキュリティ機能の数。TOE に含まれているセキュリティ機能の数が少ない場合には、セキュリティ機能のすべてを厳密にテストすることが現実的にできる。多数のセキュリティ機能を持つ TOE では、これは費用効果が悪く、サンプリングが必要になる。
- 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。ATE_COV.1 の要件により開発者が提供するテストカバレッジのレベルが大きく変動する場合、提供されるカバレッジのレベルは、評価者によって費やされる適切な労力を決定する重要な要因である。

848 評価者は、サブセットを構成するセキュリティ機能を選択する。この選択は、数多くの要因に依存し、これらの要因の考慮は、テストサブセットサイズの選択にも影響を与える。

- a) セキュリティ機能の開発者テストの厳密さ。機能仕様に識別されているセキュリティ機能のいくつかは、それらに関する開発者テスト証拠をほとんど持たないかまたはまったく持たないことができる。追加のテストが必要であると評価者が決定したセキュリティ機能は、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セキュリティ機能またはその様相が特定どおりに動作す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セキュリティ機能を含めるべきである。
- c) TOE の種別に一般的に関係する知られている公知の弱点（例えば、オペレーティングシステム、ファイアウォール）。TOE の種別に関係する知られている公知の弱点は、テストサブセットの選択プロセスに影響する。評価者は、その種別の TOE に対して知られている公知の弱点に対処するそれらのセキュリティ機能をサブセットに含めるべきである（ここでの知られている公知の弱点は、そのような脆弱性を意味せず、この個々の種別の TOE で経験された不十

分性または問題領域を意味する)。そのような弱点が知られていない場合には、セキュリティ機能の広い範囲を選択する比較一般的な手法がさらに適している。

- d) セキュリティ機能の重要性。TOE に対するセキュリティ対策方針の観点から他のセキュリティ機能よりも重要なセキュリティ機能は、テストサブセットに含まれるべきである。
- e) ST でなされている SOF 主張。特定の SOF 主張に対するすべてのセキュリティ機能は、テストサブセットに含まれるべきである。
- f) セキュリティ機能の複雑性。複雑なセキュリティ機能は、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いめんどろな要求を課す複雑なテストを必要とするかもしれない。逆に複雑なセキュリティ機能は、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。
- g) 暗黙のテスト。あるセキュリティ機能のテストは、しばしば暗黙に他のセキュリティ機能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、(暗黙にはあるが) テストされるセキュリティ機能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を提供するために使用され、効率的なテスト手法の標的となる。
- h) TOE への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。
- i) 革新的または一般的でない機能。販売広告用の印刷物で強調しているような革新的または一般的でないセキュリティ機能が TOE に含まれている場合、これらは、テストの有力な候補となるべきである。

849 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。

850 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

2:ATE_IND.2-5 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**。

851 評価者は、ST 及び機能仕様からセキュリティ機能の期待されるふるまいを理解して、機能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、セキュリティ機能を外部インタフェースでテストするか、テストハーネス(test harness)を使用して内部インタフェースでテストするか、または別のテスト手法 (例えば、例外状況、コード検査) を採用するべきか。
- b) セキュリティ機能を刺激し、応答を観察するために使用されるセキュリティ機能インタフェース。

- c) テストに存在する必要がある初期条件（すなわち、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) セキュリティ機能を刺激する（例えば、パケットジェネレータ）またはセキュリティ機能を観察する（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。

852 評価者は、一連のテストケースを使用して各セキュリティ機能をテストするのが実際的であることを発見することがある。その場合、各テストケースは、期待されるふるまいの大変特定な局面をテストする。

853 評価者のテスト証拠資料は、必要に応じて、該当する設計仕様、及び ST 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。

2:ATE_IND.2-6 評価者はテストを**実施しなければならない**。

854 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。

2:ATE_IND.2-7 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) テストするセキュリティ機能のふるまいの識別
- 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) すべての前提となるテスト条件を確立するための指示
- d) セキュリティ機能を刺激するための指示
- e) セキュリティ機能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

855 詳細のレベルは、他の評価者がテストを繰り返し、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、異なっても良いが、全体的な結果は同一であるべきである。

856 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ある場合がある（例えば、テストの実際の結果が、期待される結果と比較するまえに、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。

2:ATE_IND.2-8 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**。

857 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変更を必要とする。この決定とそれを正当とする理由は、評価者に任される。

6.8.4.3.3 アクション ATE_IND.2.3E

2:ATE_IND.2-9 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**。

858 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。

859 テストアクティビティ全体に対する評価者の全体的な労力を考慮して、通常、開発者のテストの 20%が実行されるべきである。ただし、これは、TOE の本質と提供されるテスト証拠によって変化する。

860 開発者のテストはすべて、特定のセキュリティ機能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.2-4 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。

861 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

2:ATE_IND.2-10 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**。

862 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。

863 十分な説明または説明が得られない場合、開発者のテスト結果に対する評価者の確信は落ちるであろうし、評価者はサンプルサイズを増やし、開発者のテストへの確信を取り戻す必要がある場合がある。サンプルサイズを増やしても評価者の懸念を取り去ることができない場合には、開発者テストの全体のセットを繰り返す必要がある。最終的に、ワークユニット ATE_IND.2-4 に識別されている TSF サブセットが適切にテストされるまで、開発者のテストの欠陥は、開発者のテストの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。

2: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成果を**報告しなければならない**。

- 864 ETR に報告される評価者のテスト情報は、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、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、他の評価者や監督者が、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。
- 865 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セキュリティ機能の量とサイズの正当とする理由。
 - c) サブセットを構成するセキュリティ機能の選択基準。サブセットに含めるセキュリティ機能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) テストされたセキュリティ機能。サブセットに含めることに値したセキュリティ機能の簡単なリスト。
 - 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。
- 866 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 に示すべきタイプの情報を提供することだけを意図している。

6.9 脆弱性評価アクティビティ

867 脆弱性評価アクティビティの目的は、意図する環境で TOE の欠陥または弱点が悪用される可能性を決定することである。この決定は、開発者が行う分析に基づいて行われ、評価者の侵入テストによりサポートされる。

868 EAL2 での脆弱性評価アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) AVA_SOF.1

b) AVA_VLA.1

6.9.1 TOE セキュリティ機能強度の評価 (AVA_SOF.1)

6.9.1.1 目的

869 このサブアクティビティの目的は、SOF 主張がすべての確率的または順列的メカニズムに対して ST でなされているかどうか、及び ST でなされている開発者の SOF 主張が正しい分析によって裏付けられているかどうかを決定することである。

6.9.1.2 適用上の注釈

870 SOF 分析は、パスワードメカニズムまたは生物的尺度 (バイオメトリックス) など、本来確率的または順列的メカニズムに対して行われる。暗号化メカニズムも本来確率的であり、強度の観点から多く記述されているが、AVA_SOF.1 は、暗号化メカニズムには適用されない。そのようなメカニズムには、評価者は、制度ガイダンスを探すべきである。

871 SOF 分析は、個々のメカニズムに基づいて行われるが、SOF の全体的な決定は、機能に基づいて行われる。セキュリティ機能を提供するために複数の確率的または順列的メカニズムが採用される場合には、それぞれ個別のメカニズムを分析する必要がある。セキュリティ機能を提供するためにこれらのメカニズムを組み合わせる方法は、その機能の全体的な SOF レベルを決定する。評価者は、メカニズムが機能を提供するために一体となって動作する方法、及び ADV_HLD.1 の依存性によって与えられるそのような情報の最小レベルを理解するために設計情報を必要とする。評価者に提供される実際の設計情報は、EAL によって決定される。提供される情報は、必要なときに、評価者の分析を裏付けるために使用されるべきである。

872 複数の TOE ドメインに関する SOF の説明については、4.4.6 節を参照のこと。

6.9.1.3 入力

873 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) 上位レベル設計

- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) TOE セキュリティ機能強度の分析

6.9.1.4 評価者アクション

874 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) AVA_SOF.1.1E
- b) AVA_SOF.1.2E

6.9.1.4.1 アクション AVA_SOF.1.1E

AVA_SOF.1.1C

2:AVA_SOF.1-1 評価者は、ST に SOF レート付けで表されている SOF 主張に対応する各セキュリティメカニズムに対して開発者が SOF 分析を提供していることを **チェックしなければならない**。

875 SOF 主張が SOF 数値尺度だけで表されている場合、このワークユニットは、適用されず、条件は満たされているものとみなされる。

876 SOF レート付けは、攻撃能力として表される 1 つの SOF-基本、SOF-中位、SOF-高位として表される。CC パート 1 用語集を参照のこと。レート付けとして表された最小の全体的 SOF 要件は、すべての非暗号、確率的または順列的セキュリティメカニズムに適用される。ただし、個々のメカニズムは、全体的 SOF 要件を越えるレート付けとして表された SOF 主張を持つことができる。

877 攻撃するために必要となる攻撃能力を決定するガイダンス、及びレート付けとして SOF を決定するガイダンスについては、附属書 B.8 を参照のこと。

878 SOF 分析は、ST でなされた SOF 主張を正当化する根拠からなる。

AVA_SOF.1.2C

2:AVA_SOF.1-2 評価者は、ST に数値尺度で表されている SOF 主張に対応する各セキュリティメカニズムに対して開発者が SOF 分析を提供していることを **チェックしなければならない**。

879 SOF 主張が SOF レート付けだけで表されている場合、このワークユニットは、適用されず、条件は満たされているものとみなされる。

880 レート付けとして表された最小の全体的 SOF 要件は、すべての非暗号、確率的または順列的メカニズムに適用される。ただし、個々のメカニズムは、全体的 SOF 要件を満たすまたは要件を越える数値尺度として表された SOF 主張を持つことができる。

- 881 SOF 分析は、ST でなされた SOF 主張を正当化する根拠からなる。
AVA_SOF.1.1C 及び AVA_SOF.1.2C
- 2:AVA_SOF.1-3 評価者は、分析を裏付ける主張または前提条件のいずれもが正当であることを決定するために、SOF 分析を**検査しなければならない**。
- 882 例えば、擬似乱数ジェネレータの特定の実装が、SOF 分析が関係するセキュリティメカニズムにシードする必要がある要求されるエントロピーを持っているというのは無効な前提条件である。
- 883 ワーストケースが ST により無効にされない限り、SOF 分析を裏付ける前提条件には、この Worst Case を反映するべきである。多数の異なる可能なシナリオが存在し、これらが人間利用者または攻撃者に依存する場合、すでに述べたように、このケースが無効にされない限り、最小の強度を表すケースが想定されるべきである。
- 884 例えば、最大の論理的パスワードスペースに基づく強度の主張（すなわち、すべての印刷可能な ASCII 文字）は、自然言語パスワードを使用してパスワードスペース及び関係する強度を効果的に減らすのが人間のふるまいであるために、Worst Case とはならない。ただし、自然言語パスワードの使用を最小にするパスワードフィルタなど、ST に識別されている IT 手段を TOE が使用する場合、そのような前提条件は、適切となる。
- 2:AVA_SOF.1-4 評価者は、分析を裏付けるアルゴリズム、原理、特性及び計算が正しいことを決定するために、SOF 分析を**検査しなければならない**。
- 885 このワークユニットの本質は、考慮されているメカニズムのタイプに大きく依存する。附属書 B.8 は、パスワードメカニズムを使用して実装される識別と認証の機能の SOF 分析の例を示している。分析は、最大のパスワードスペースが最後に SOF レート付けに到達すると考える。生物学的尺度に対して、分析は、メカニズムのスプーフィング（偽造）されやすさに影響を与える解決策とその他の要因を考慮するべきである。
- 886 レート付けとして表される SOF は、セキュリティメカニズムを打ち負かすために必要となる最小の攻撃能力に基づく。SOF レート付けは、CC パート 1 用語集の攻撃能力に関して定義されている。
- 887 攻撃能力のガイダンスについては、附属書 B.8 を参照のこと。
- 2:AVA_SOF.1-5 評価者は、各 SOF 主張が満たされているかまたは越えていることを決定するために、SOF 分析を**検査しなければならない**。
- 888 SOF 主張のレート付けのガイダンスについては、附属書 B.8 を参照のこと。
- 2:AVA_SOF.1-6 評価者は、SOF 主張を持つすべての機能が ST に定義されている最小強度レベルを持つことを決定するために、SOF 分析を**検査しなければならない**。

6.9.1.4.2 アクション AVA_SOF.1.2E

2:AVA_SOF.1-7 評価者は、すべての確率的または順列的メカニズムが SOF 主張を持つことを決定するために、機能仕様、上位レベル設計、利用者ガイダンス及び管理者ガイダンスを**検査しなければならない**。

889 確率的または順列的メカニズムによって実現されるセキュリティ機能の開発者による識別は、ST 評価中に検証される。ただし、TOE 要約仕様がその活動を行うために使用可能な唯一の証拠である場合、そのようなメカニズムの識別は不完全なことがある。このサブアクティビティへの入力として必要な追加の評価証拠は、ST にまだ識別されていない追加の確率的または順列的メカニズムを識別することができる。その場合、ST は、追加の SOF 主張を反映するために適切に更新する必要がある。また、開発者は、評価者アクション AVA_SOF.1.1E への入力としての主張を正当化する追加の分析を提供する必要がある。

2:AVA_SOF.1-8 評価者は、SOF 主張が正しいことを決定するために、その主張を**検査しなければならない**。

890 SOF 分析に主張または前提条件（例えば、毎分可能な認証の試みの数）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に確認すべきである。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。

6.9.2 脆弱性分析の評価 (AVA_VLA.1)

6.9.2.1 目的

891 このサブアクティビティの目的は、TOE が、その意図する環境において、悪用される可能性のある明らかな脆弱性を持つかどうかを決定することである。

6.9.2.2 適用上の注釈

892 このサブアクティビティでの用語「ガイダンス」(*guidance*)の使用は、利用者ガイダンス、管理者ガイダンス、セキュアな設置、生成及び立上げ手順を意味する。

893 悪用される可能性のある脆弱性の考えは、ST のセキュリティ対策方針と機能要件によって決まる。例えば、セキュリティ機能がバイパスされるのを阻止するための手段が ST で必要とされない場合 (FPT_PHP, FPT_RVM と FPT_SEP が存在しない)、バイパスに基づく脆弱性は、考慮されるべきでない。

894 脆弱性は、公知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 つの局面は、関係しているが、別のものである。脆弱性が公知になってい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。

895 次の用語は、ガイダンスで特定の意味で使用される。

- a) 脆弱性 (*vulnerability*) – ある環境のセキュリティ方針を破るために使用されることがある TOE の弱点。
- b) 脆弱性分析 (*vulnerability analysis*) – TOE の脆弱性の系統的な探索、及び TOE の意図される環境との関係を決定するための発見されたこれらの評価。
- c) 明らかな脆弱性 (*obvious vulnerability*) – TOE、技術的精巧さ及び資源の最小の理解が必要となる、悪用される可能性のある脆弱性。
- d) 潜在的脆弱性 (*potential vulnerability*) – TOE において、(仮定される攻撃経路によって) 存在が疑われるが、確認のない脆弱性。
- e) 悪用可能脆弱性 (*exploitable vulnerability*) – TOE の意図する環境で悪用される可能のある脆弱性。
- f) 悪用不能脆弱性 (*non-exploitable vulnerability*) – TOE の意図する環境で悪用される可能性のない脆弱性。
- g) 残存脆弱性 (*residual vulnerability*) – TOE の意図する環境で予想される以上の攻撃能力を持つ攻撃者が悪用できない、悪用される可能性のない脆弱性。
- h) 侵入テスト (*penetration testing*) – TOE の意図する環境での識別された TOE の潜在的脆弱性の悪用される可能性を検査するために行われるテスト。

6.9.2.3 入力

896 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順
- g) 脆弱性分析
- h) 機能強度の主張分析
- i) テストに適した TOE

897 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) 明らかな脆弱性に関する現在の情報（監督者からの）

6.9.2.4 評価者アクション

898 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) AVA_VLA.1.1E
- b) AVA_VLA.1.2E

6.9.2.4.1 アクション AVA_VLA.1.1E

AVA_VLA.1.1C

2:AVA_VLA.1-1 評価者は、明らかな脆弱性に対する探索がすべての該当する情報を考慮したことを決定するために、開発者の脆弱性分析を**検査しなければならない**。

899 開発者の脆弱性分析は、少なくともすべての評価用提供物件と公知になっている情報源において、明らかな脆弱性に対する開発者の探索を扱うべきである。評価者は、評価用提供物件を独立脆弱性分析（AVA_VLA.1 で必要ない）のためではなく、開発者の明らかな脆弱性の探索を評価するための基礎として使用するべきである。

2:AVA_VLA.1-2 評価者は、明らかな各脆弱性が記述されていること及び TOE の意図する環境でそれが悪用されることがない理由に対する根拠が示されていることを決定するために、開発者の脆弱性分析を**検査しなければならない**。

900 開発者は、TOE 及び公知になっている情報源の知識に基づいて明らかな脆弱性を探索することが期待される。明らかな脆弱性だけを識別する必要がある場合、詳細な分析は、期待されない。開発者は、上記の定義に基づいてこの情報を選別し、明らかな脆弱性が意図する環境で悪用される可能性がないことを示す。

- 901 評価者は、開発者の次の3つの局面に関心を持つ必要がある。
- a) 開発者の分析がすべての評価用提供物件を考慮したかどうか
 - b) 意図する環境で明らかな脆弱性が悪用されないようにするための適切な手段が取られているかどうか
 - c) 明らかな脆弱性がいくつか識別されずに残っているかどうか
- 902 評価者は、悪用される可能性がないことを決定するための基礎として開発者によって使用されない限り、識別された脆弱性が明らかであるかどうかに関心を持たされるべきでない。そのような場合、評価者は、識別された脆弱性に対する攻撃能力の低い攻撃者に対する抵抗力を決定することによってこの主張の正当性を確認する。
- 903 *明らかな脆弱性の概念は、攻撃能力の概念に関係していない。後者は、独立脆弱性分析中に評価者によって決定される。このアクティビティは、AVA_VLA.1 に対して行われないうえに、通常、攻撃能力に基づく評価者による探索と選別は存在しない。ただし、それでも評価者は、評価の途中で潜在的な脆弱性を発見することがある。これらに対処する方法の決定は、明らかな脆弱性と低い攻撃能力の概念の定義を参照して行われる。*
- 904 明らかな脆弱性のいくつかが識別されずに残っているかどうかの決定は、開発者の分析の正当性の評価、使用可能な公知になっている脆弱性情報との比較、その他の評価アクティビティの途中で評価者が識別したそれ以外の脆弱性との比較に制限される。
- 905 脆弱性は、次の1つまたはいくつかの条件が存在する場合、悪用される可能性がないと呼ばれる。
- a) (IT または IT 以外の) 環境のセキュリティ機能または手段が意図する環境の脆弱性の悪用を阻止する。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 TOE の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。
 - b) 脆弱性は、悪用可能であるが、攻撃能力が中程度または高い攻撃者のみが悪用可能。例えば、セッションハイジャック攻撃への分散 TOE の脆弱性は、明らかな脆弱性を悪用するために必要となる、より以上の攻撃能力を必要とする。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。
 - c) 脅威に対抗すると主張されていないか、または違反可能な組織のセキュリティ方針が ST により達成されると主張されていない。例えば、ST が利用可能方針の主張を行わず、TCP SYN 攻撃（ホストが接続要求サービスを行えないようにする共通のインターネットプロトコルへの攻撃）を受けやすいファイアウォールは、この脆弱性だけでこの評価者のアクションに不合格とするべきでない。
- 906 脆弱性を悪用するために必要な攻撃能力の決定のガイダンスについては、附属書 B.8 を参照のこと。

- 2:AVA_VLA.1-3 評価者は、開発者の脆弱性分析が ST 及びガイダンスに一貫していることを決定するために、その分析を**検査しなければならない**。
- 907 開発者の脆弱性分析は、TOE 機能に対する特定の構成または設定を示して、脆弱性に対処することができる。そのような運用上の制約が効果的であり、ST と一貫していると思われる場合、消費者がそれらを採用できるように、すべてのそのような構成と設定がガイダンスに満たされるように記述されるべきである。
- 6.9.2.4.2 アクション AVA_VLA.1.2E
- 2:AVA_VLA.1-4 評価者は、開発者の脆弱性分析に基づいて、侵入テストを**考え出さなければならない**。
- 908 評価者が侵入テストを準備するのは、次の場合である。
- a) 脆弱性が悪用されることがないとの理由に対する開発者の根拠が評価者の考えでは疑わしい場合、開発者の分析に対して反証することを試みる必要がある。
 - b) TOE が、意図する環境で、開発者が考慮していない明らかな脆弱性を持つことを決定する必要がある。評価者は、開発者が考慮していない明らかな公知になっている脆弱性に関する、(例えば、監督者からの)現在の情報にアクセスを持つべきであり、また、その他の評価アクティビティの結果として識別された潜在的な脆弱性を持つことができる。
- 909 評価者が明らかになっていない脆弱性(公知になっている脆弱性を含む)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まえに、テストを行う必要がある。評価の専門知識の結果として、評価者が明らかになっていない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。
- 910 疑わしい明らかな脆弱性を理解し、評価者は、TOE の脆弱性をテストするための最も可能性の高い方法を決定する。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セキュリティ機能インターフェース
 - b) テストに存在する必要がある初期条件(すなわち、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) セキュリティ機能を刺激するか、またはセキュリティ機能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、明らかな脆弱性をテストするために特別の装置が必要になることはない)
- 911 評価者は、おそらく、一連のテストケースを使用して侵入テストを行うのが有用であることを見つけ出し、この場合、各テストケースは、特定の明らかな脆弱性をテストすることになる。

2:AVA_VLA.1-5 評価者は、開発者の脆弱性分析に基づき、テストを再現可能にするに十分な詳細さで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) テストする TOE の明らかな脆弱性の識別
- 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説明
- c) すべての侵入テスト前提初期条件を確立するための説明
- d) TSF を刺激するための説明
- e) TSF のふるまいを観察するための説明
- f) すべての期待される結果と、期待される結果に対応する観察されたふるまいについて実行されるべき必要な分析の記述
- 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説明

912 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繰り返し、同等の結果を得ることができるようにすることである。

2:AVA_VLA.1-6 評価者は、開発者の脆弱性分析に基づいて、侵入テストを**実施しなければならない**。

913 評価者は、TOE の侵入テストを行うための基礎として、ワークユニット 2:AVA_VLA.1-4 の結果の侵入テスト証拠資料を使用するが、これは、評価者が追加の特別の侵入テストを行うことを排除しない。必要に応じて、評価者は、評価者が行った場合に侵入テスト証拠資料に記録される、侵入テスト中に得られた情報の結果として特別のテストを考え出すことができる。そのようなテストは、期待されない結果または観察をどこまでも追求するか、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必要がある。

2:AVA_VLA.1-7 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**。

914 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。相違には、いずれも正当性が示されるべきである。

2:AVA_VLA.1-8 評価者は、TOE が、意図する環境において、悪用される可能性のある明らかな脆弱性を持っていないことを決定するために、すべての侵入テストの結果とすべての脆弱性分析の結論を**検査しなければならない**。

915 結果が、意図する環境で悪用される可能性のある明らかな脆弱性を TOE が持っていることを示す場合、評価者アクションの結果は、不合格判定となる。

2:AVA_VLA.1-9 評価者は、ETR に、テスト手法、構成、深さ及び結果を示しながら評価者の侵入テストの成果を**報告しなければならない**。

916 ETR に報告される侵入テスト情報は、全体的な侵入テスト手法及びこのサブアクティビティから得られた成果を伝えることを評価者に許す。この情報を提供する意

図は、評価者の侵入テストの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、他の評価者と監督者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。

917 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) テストされたセキュリティ機能侵入。侵入テストの焦点となったセキュリティ機能の簡単なリスト。
- 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。

918 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侵入テストに関する、ETR に示すべきタイプの情報を提供することだけを意図している。

2:AVA_VLA.1-10 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採用された CEM アクティビティ、評価者に既知である、公開されたもので読んでいる、など）
- b) 影響のあるセキュリティ機能、達成されない対策方針、侵害される組織のセキュリティ方針及び顕在化される脅威
- c) 説明
- d) 意図する環境で悪用されるか否か（すなわち、悪用され得るか残存か）
- e) 脆弱性を識別した評価の関係者（例えば、開発者、評価者）の識別

7章 EAL3 評価

7.1 導入

919 EAL3 は、中レベルの保証を提供する。セキュリティ機能は、セキュリティのふるまいを理解するための TOE の機能仕様、ガイダンス証拠資料、及び上位レベル設計を使用して分析される。分析は、TOE セキュリティ機能のサブセットの独立テスト、機能仕様及び上位レベル設計に基づく開発者のテストの証拠、開発者テスト結果の選択的確認、機能強度の分析、開発者による明らかな脆弱性の探索の証拠によってサポートされる。それ以上の保証は、開発環境制御、TOE 構成管理の使用、及びセキュアな配付手続きの証拠を通して得られる。

7.2 目的

920 この章の目的は、EAL3 評価を行うための最小の評価成果を定義し、評価を行うための方法と手段についてのガイダンスを提供することである。

7.3 EAL3 評価関係

921 EAL3 評価は、次のことを扱う。

- a) 評価入力タスク (2章)
- b) 次のもので構成される EAL3 評価アクティビティ
 - 1) ST の評価 (4章)
 - 2) 構成管理の評価 (7.4 節)
 - 3) 配付及び運用文書の評価 (7.5 節)
 - 4) 開発文書の評価 (7.6 節)
 - 5) ガイダンス文書の評価 (7.7 節)
 - 6) ライフサイクルサポートの評価 (7.8 節)
 - 7) テストの評価 (7.9 節)
 - 8) テスト (7.9 節)
 - 9) 脆弱性評定の評価 (7.10 節)
- c) 評価出力タスク (2章)

922 評価アクティビティは、CC パート 3 に含まれている EAL3 保証要件から引き出される。

- 923 ST が TOE 評価サブアクティビティを行うための基礎と状況を提供するために、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。
- 924 EAL3 評価を構成するサブアクティビティが、この章に記述されている。サブアクティビティは、一般的に、多少とも同時に開始することができるが、評価者は、サブアクティビティの間のいくつかの依存性を考慮する必要がある。
- 925 依存性のガイダンスについては、附属書 B.4 を参照のこと。

7.4 構成管理アクティビティ

926 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をすること、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が適切であることを保証することである。これには、どんな変更が追跡され、そしてどのように起こり得る変更が具体化されるかの詳細を含む。

927 EAL3 での構成管理アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ACM_CAP.3

b) ACM_SCP.1

7.4.1 CM 能力の評価 (ACM_CAP.3)

7.4.1.1 目的

928 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、及びこれらの要素を変更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。

7.4.1.2 入力

929 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

7.4.1.3 評価者アクション

930 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

a) ACM_CAP.3.1E

7.4.1.3.1 アクション ACM_CAP.3.1E

ACM_CAP.3.1C

3:ACM_CAP.3-1 評価者は、評価のために提供された TOE のバージョンが一意にリファレンスされていることを**チェックしなければならない**。

931 評価者は、構成リストをチェックすることによりリファレンスの一意性の正当性を確認し、構成要素が一意に識別されていることを保証するために、開発者の CM システムを使用すべきである。その評価の間に 1 つだけのバージョンが検査されたならば、評価のために提供されたバージョンが一意にリファレンスされていること

の証拠としては、不完全である。そこで評価者は、一意のリファレンスをサポートできるリファレンスシステム（例えば、数字、文字または日付の使用）を探すべきである。それにもかかわらず、いかなるリファレンスも存在しない場合、通常、TOE が一意に識別できると評価者が確信しない限り、この要件に対する判定は不合格となる。

- 932 評価者は、TOE の複数のバージョンを検査するようにし（例えば、脆弱性が発見された後のリワーク中に）、2 つのバージョンが別々にリファレンスされることをチェックするべきである。

ACM_CAP.3.2C

- 3:ACM_CAP.3-2 評価者は、評価のために提供された TOE がそのリファレンス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**。

- 933 評価者は、TOE の異なるバージョンを区別することができる一意のリファレンスが 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。

- 934 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、スタートアップルーチンの間に、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。

- 3:ACM_CAP.3-3 評価者は、使用されている TOE リファレンスが一貫していることを**チェックしなければならない**。

- 935 もし、TOE に 2 度以上の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。評価者は、提供された CM 証拠資料の一部である構成リストを使用して識別情報の一貫性のある使用を検証することができる。

- 936 評価者は、TOE リファレンスが ST と一貫性があることも検証する。

- 937 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ACM_CAP.3.3C

- 3:ACM_CAP.3-4 評価者は、提供された CM 証拠資料が構成リストを含んでいることを**チェックしなければならない**。

- 938 構成リストは、構成制御(configuration control)のもとで維持されている要素を識別する。

3:ACM_CAP.3-5 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**。

ACM_CAP.3.4C

3:ACM_CAP.3-6 評価者は、構成リストが TOE を構成する構成要素を識別していることを決定するために、そのリストを**検査しなければならない**。

939 構成リストに含まれるべき構成要素の最小範囲は、ACM_SCP によって与えられる。

ACM_CAP.3.5C

3:ACM_CAP.3-7 評価者は、構成要素の識別方法が、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、その識別方法を**検査しなければならない**。

ACM_CAP.3.6C

3:ACM_CAP.3-8 評価者は、構成リストが各構成要素を一意に識別していることを**チェックしなければならない**。

940 構成リストには、TOE を構成する構成要素のリストと、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。

ACM_CAP.3.7C

3:ACM_CAP.3-9 評価者は、CM 計画が、TOE 構成要素の完全性を維持するために 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**。

941 CM 計画には、次の記述を含めることができる。

- a) 構成管理手続きに従う TOE 開発環境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、変更または削除）。
- b) 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タイプの構成要素（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）。
- c) 許可された個人だけが構成要素を変更できるように保証するために使用される手続き。
- d) 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。
- e) 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）、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拠または変更管理レコードに記録される。

- f) TOE バージョンのバージョン管理及び一意にリファレンスするための手法（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）。

ACM_CAP.3.8C

3:ACM_CAP.3-10 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**。

942 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 ACM_CAP.3.9C 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。

3:ACM_CAP.3-11 評価者は、CM システムが CM 計画の記述に従って使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**。

943 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タイプの CM 関連操作（例えば、作成、変更、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。

944 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

945 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とのさらなる確信は、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認することができる。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べきである。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、それらに置き換えるものではないことに注意すべきである。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 計画とレコード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。

946 評価者がこのアクティビティを確認するために開発サイトを訪問することが予想される。

947 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

ACM_CAP.3.9C

3:ACM_CAP.3-12 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**。

- 948 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タイプの構成要素（例えば、上位レベル設計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詳細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べきである。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。
- 949 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 950 ACM_CAP.3.10C
- 3:ACM_CAP.3-13 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**。
- 951 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、CM システム手続きにより生成され、ワークユニット 3:ACM_CAP.3-12 の一部としてすでに検査された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 システムのデモンストレーションに立ち会うこともできる。

7.4.2 CM 範囲の評価 (ACM_SCP.1)

7.4.2.1 目的

952 このサブアクティビティの目的は、開発者が少なくとも、TOE 実装表現、設計、テスト、利用者及び管理者ガイダンス、及び CM 証拠資料に対して構成管理を行うかどうかを決定することである。

7.4.2.2 入力

953 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) 構成管理証拠資料

7.4.2.3 評価者アクション

954 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

a) ACM_SCP.1.1E

7.4.2.3.1 アクション ACM_SCP.1.1E

ACM_SCP.1.1C

3:ACM_SCP.1-1 評価者は、構成リストに CM システムによって追跡される CC が必要とする要素の最小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**。

955 リストには少なくとも次のものを含むべきである。

a) 保証の目標レベルを達成するために必要なすべての証拠資料

b) その他の設計証拠資料 (例えば、下位レベル設計)

c) テストソフトウェア (適用される場合)

d) TOE 実装表現 (すなわち、TOE を構成するコンポーネントまたはサブシステム)。ソフトウェアのみの TOE では、実装表現は、ソースコードだけで構成することができる。ハードウェアプラットフォームが含まれる TOE では、実装表現は、ソフトウェア、ファームウェア、及びハードウェア (またはリファレンスプラットフォーム) 説明の組み合わせを意味することができる。

ACM_SCP.1.2C

3:ACM_SCP.1-2 評価者は、手続きが、どのように各構成要素のステータスが TOE のライフサイクルを通して追跡されることができるかを記述していることを決定するために、CM 証拠資料を **検査しなければならない**。

956 手続きは、CM 計画にまたは CM 証拠資料を通して詳細に記述することができる。含まれる情報には、次のもの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することができるように、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を割り付ける方法、及びそれらを CM システムに組み入れる方法。
- c) 構成要素の置き換えられたバージョンを識別するために使用される方法。
- d) TOE 開発及び保守ライフサイクルの各段階（すなわち、要件仕様、設計、ソースコード開発、オブジェクトコード生成から実行可能コードまで、モジュールテスト、実装及び運用）を通して構成要素を識別し、追跡するために使用される方法。
- e) ある時点で構成要素の現在のステータスを割り付けるため及び開発フェーズ（すなわち、ソースコード開発、オブジェクトコード生成から実行可能コードまで、モジュールテスト及び証拠資料）での表現の各種のレベルを通して各構成要素を追跡するために使用される方法。
- f) 1 つの構成要素が変更された場合、変更する必要がある他の構成要素を決定することができるように、構成要素の間の対応を識別するために使用される方法。

957

この情報のいくつかに対する CM 証拠資料の分析は、ACM_CAP で詳細に記述されているワークユニットで満たされていることがある。

7.5 配付及び運用アクティビティ

958 配付及び運用アクティビティの目的は、開発者が意図したのと同じ方法で TOE が設置され、生成され、開始され、変更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が適切であることを判断することである。これには、TOE の輸送中に取られる手続きと、初期化、生成、及び立上げの両方の手順が含まれる。

959 EAL3 での配付及び運用アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ADO_DEL.1

b) ADO_IGS.1

7.5.1 配付の評価 (ADO_DEL.1)

7.5.1.1 目的

960 このサブアクティビティの目的は、配付証拠資料が TOE を利用者サイトへ配送するときの完全性を維持するために使用されるすべての手続きを記述していることを決定することである。

7.5.1.2 入力

961 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) 配付証拠資料

7.5.1.3 評価者アクション

962 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ADO_DEL.1.1E

b) ADO_DEL.1.2D に基づく暗黙の評価者アクション

7.5.1.3.1 アクション ADO_DEL.1.1E

ADO_DEL.1.1C

3:ADO_DEL.1-1 評価者は、配付証拠資料が、TOE の版またはその一部を利用者サイトへ配送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**。

963 用語「必要」(*necessary*) の解釈は、TOE の本質と ST に含まれている情報を考慮する必要がある。提供される保護レベルは、ST に識別されている前提条件、脅威、組織のセキュリティ方針、及びセキュリティ対策方針と一致しているべきである。場合によっては、これらは、配付に対して明示的に表されないことがある。評価者

は、均衡の取れたアプローチが取られ、配付が、その他の点でセキュアな開発プロセスでの明らかな弱点を表さないことを決定するべきである。

964 配付手続きは、TOE の識別を決定し、TOE またはそのコンポーネント部分の輸送中の完全性を維持するための適切な手続きを記述する。手続きは、これらの手続きが扱う必要がある TOE の部分を記述する。それには、必要に応じて、物理的または電子的（例えば、インターネットからダウンロードするための）配送の手続きが含まれるべきである。配付手続きは、該当するソフトウェア、ハードウェア、ファームウェア及び証拠資料など、TOE 全体に関連する。

965 完全性は、常に TOE の配付で懸念されるために、完全性を重視することは、驚くことではない。機密性と可用性が懸念される場合、それらも、このワークユニットで考慮されるべきである。

966 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するべきである。

3:ADO_DEL.1-2 評価者は、配付手続きが選択された手続きとそれが扱う TOE の部分がセキュリティ対策方針を達成するのに適していることを決定するために、その配付手続きを**検査しなければならない**。

967 配付手続きの選択の適合性には、特定の TOE（例えば、ソフトウェアかハードウェアか）及びセキュリティ対策方針が影響する。

968 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。配送には、公共郵便または民間の配送サービスが受け入れられる。

7.5.1.3.2 暗黙の評価者アクション

ADO_DEL.1.2D

3:ADO_DEL.1-3 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**。

969 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べきである。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送場所の訪問
- b) 配付のいくつかの段階、または利用者サイトでの TOE の検査（例えば、改ざん防止シール(tamper proof seals)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

970 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

- 971 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、将来の配付で使用される適切な手続きと施設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 (dry run)」を要求することができる。開発者が他の同様の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、保証を提供する上で役に立つことがある。

7.5.2 設置、生成及び立上げの評価 (ADO_IGS.1)

7.5.2.1 目的

972 このサブアクティビティの目的は、TOE のセキュアな設置、生成、及び立上げのための手順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。

7.5.2.2 入力

973 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) 管理者ガイダンス
- b) セキュアな設置、生成、及び立上げの手順
- c) テストに適した TOE

7.5.2.3 適用上の注釈

974 設置、生成及び立上げ手順は、それらが利用者サイトで行われるか、または ST の記述に従って TOE をセキュアな構成にするために必要となる開発サイトで行われるかに関係なく、すべての設置、生成、及び立上げの手順に関係している。

7.5.2.4 評価者アクション

975 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADO_IGS.1.1E
- b) ADO_IGS.1.2E

7.5.2.4.1 アクション ADO_IGS.1.1E

ADO_IGS.1.1C

3:ADO_IGS.1-1 評価者は、TOE のセキュアな設置、生成及び立上げに必要な手順が提供されていることを **チェックしなければならない**。

976 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合 (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 (または影響を受ける部分) は、適用されないために、満たされているものとみなされる。

7.5.2.4.2 アクション ADO_IGS.1.2E

3:ADO_IGS.1-2 評価者は、TOE のセキュアな設置、生成及び立上げに必要なステップを記述していることを決定するために、提供された設置、生成、及び立上げの手順を **検査しなければならない**。

- 977 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合（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（または影響を受ける部分）は、適用されないために、満たされているものとみなされる。
- 978 設置、生成及び立上げの手順は、次のものに対する詳細な情報を提供することができる。
- a) TSF の制御のもとでのエンティティの設置の特定セキュリティ特性の変更
 - b) 例外及び問題の取扱い
 - c) 適切に、セキュアな設置のための最小限のシステム要件
- 979 設置、生成及び立上げの手順の結果、セキュアな構成となることを確認するために、評価者は、開発者の手順に従って、提供されたガイダンス証拠資料だけを使用して、顧客が（TOE に適用される場合）TOE を設置、生成、及び立上げするために通常行うことが予想されるアクティビティを実行することができる。このワークユニットは、3:ATE_IND.2-2 ワークユニットとともに実行することができる。

7.6 開発アクティビティ

- 980 開発アクティビティの目的は、TSF が TOE のセキュリティ機能を提供する方法を理解するための適合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（TOE の外部インタフェースを記述する）及び上位レベル設計（内部サブシステムの観点から TOE のアーキテクチャを記述する）からなる。表現対応（一貫性を保証するために TOE の表現を相互にマッピングする）も存在する。
- 981 EAL3 の開発アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。
- a) ADV_FSP.1
 - b) ADV_HLD.2
 - c) ADV_RCR.1

7.6.1 適用上の注釈

- 982 設計証拠資料の CC 要件は、形式性によってレベル付けされている。CC は、文書の形式性の程度（すなわち、非形式的、準形式的または形式的のどれであるか）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。方法論は、使用すべき特定の言語を指示しない。その問題は、制度に任されている。次の段落は、各種の非形式的文書の内容を区別している。
- 983 非形式的機能仕様は、セキュリティ機能の記述（TOE 要約仕様と同等のレベルでの）及び TSF への外部に見えるインタフェースの記述からなる。例えば、オペレーティングシステムが自己を識別する手段、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、記録する監査機能も含まれている場合には、これらの監査機能の記述も機能仕様に含まれることが期待される。これらの機能は、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、それらは、利用者の外部インタフェースでなにが起きるかによって影響される。
- 984 非形式的上位レベル設計は、各サブシステムでそのインタフェースでの刺激に回答して起きる一連のアクションとして表される。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上位レベル設計記述は、取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取るアクションとして記述する。
- 985 対応の実証の非形式は、散文形式である必要はない。簡単な 2 次元のマッピングで十分である。例えば、1 つの軸に沿ってモジュールが示され、他の軸に沿ってサブシステムが示され、セルがこれら 2 つの対応を識別するマトリックスは、上位レベル設計と下位レベル設計の間の適切な非形式的対応を提供することができる。

7.6.2 機能仕様の評価 (ADV_FSP.1)

7.6.2.1 目的

986 このサブアクティビティの目的は、開発者が TOE のセキュリティ機能の適切な記述を提供しているかどうか及び TOE が提供するセキュリティ機能が ST のセキュリティ機能要件を十分に満たしているかどうかを決定することである。

7.6.2.2 入力

987 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) 利用者ガイダンス
- d) 管理者ガイダンス

7.6.2.3 評価者アクション

988 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_FSP.1.1E
- b) ADV_FSP.1.2E

7.6.2.3.1 アクション ADV_FSP.1.1E

ADV_FSP.1.1C

3:ADV_FSP.1-1 評価者は、機能仕様がすべての必要な非形式的説明文を含んで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**。

989 機能仕様全体が非形式的である場合、このワークユニットは、適用されないために、満たされているものとみなされる。

990 補助的な叙述的記述は、準非形式的または形式的記述だけでは理解するのが困難な機能仕様の部分に必要となる（例えば、形式的表記の意味を明確にするため）。

ADV_FSP.1.2C

3:ADV_FSP.1-2 評価者は、機能仕様が内部的に一貫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**。

991 評価者は、TSFI を構成するインタフェースの記述が TSF の機能の記述と一貫していることを保証することにより、機能仕様の正当性を確認する。

992 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ADV_FSP.1.3C

3:ADV_FSP.1-3 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべてを識別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**。

993 用語「外部」(*external*)は、利用者に見えることを意味する。TOE への外部インタフェースは、TSF への直接インタフェースであるかまたは TOE の TSF 以外の部分へのインタフェースのいずれかである。ただし、これらの TSF 以外のインタフェースは、最終的に TSF にアクセスすることがある。TSF に直接または間接的にアクセスするこれらの外部インタフェースは、一体となって TOE セキュリティ機能インタフェース (TSFI) を構成する。図 7.1 は、TSF (陰影の付いた) 部分と TSF 以外 (空白) の部分を持つ TOE を示している。この TOE には、3 つの外部インタフェースがある。ここで、インタフェース c は、TSF への直接インタフェースである。インタフェース b は、TSF への間接インタフェースである。インタフェース a は、TOE の TSF 以外の部分へのインタフェースである。そこで、インタフェース b と c が TSFI を構成する。

994 CC パート 2 (またはその拡張コンポーネント) の機能要件に反映されているすべてのセキュリティ機能は、ある種の外部から見える表示を持つことに注意されるべきである。これらすべてが必ずしもセキュリティ機能をテストすることができるインタフェースとは限らないが、それらは、すべて、ある程度まで外部から見えるものであり、したがって機能仕様に含まれる必要がある。

995 TOE の境界を決定するガイダンスについては、附属書 B.6 を参照のこと。

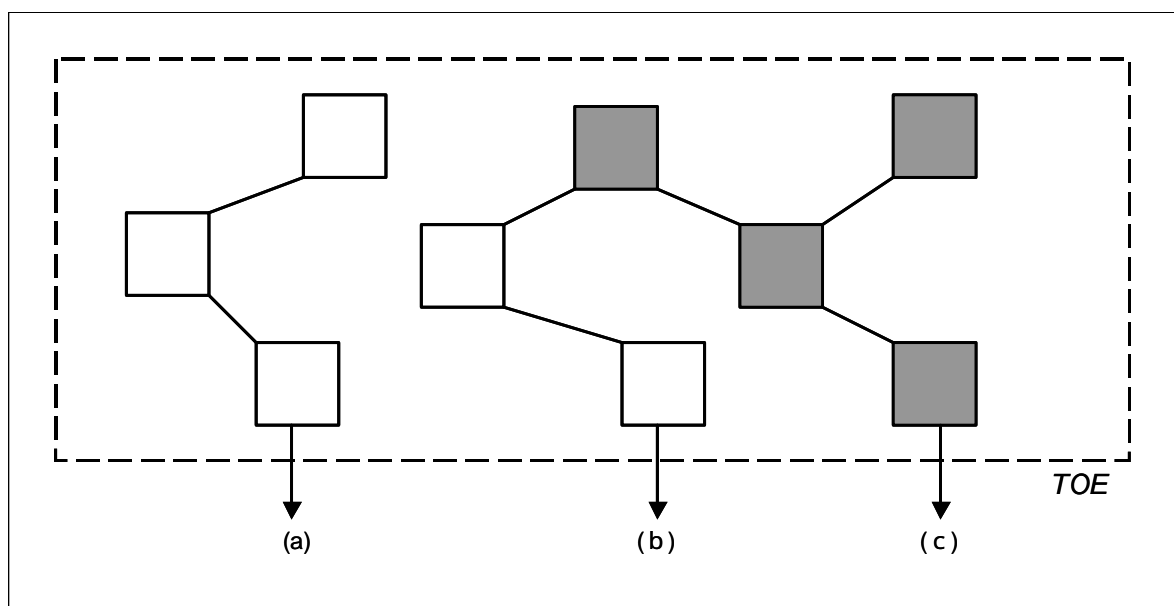


図 7.1 TSF インタフェース

3:ADV_FSP.1-4 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべて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**。

- 996 悪意のある利用者からの脅威のない TOE（すなわち、FPT_PHP、FPT_RVM 及び FPT_SEP が ST から正当に除外されている）では、機能仕様（そして他の TSF 表現記述に展開される）に記述されている唯一のインタフェースは、TSF との間のインタフェースである。FPT_PHP、FPT_RVM、及び FPT_SEP が存在しないことで、セキュリティ機能がバイパスされる心配がないことが想定されるので、他のインタフェースが TSF に与える影響についての心配がない。
- 997 他方、悪意のある利用者またはバイパスの脅威がある TOE（すなわち、FPT_PHP、FPT_RVM、及び FPT_SEP が ST に含まれている）では、すべての外部インタフェースが機能仕様に記述されているが、それは、それぞれの影響が明らかになる程度に限られている。セキュリティ機能へのインタフェース（すなわち、図 7.1 のインタフェース b と c）は、完全に記述されているが、他のインタフェースは、そのインタフェースを介して TSF へアクセスできない（すなわち、インタフェースは、図 7.1 のタイプ b ではなく、タイプ a）ことを明確にする範囲でのみ記述されている。FPT_PHP、FPT_RVM、及び FPT_SEP が含まれていることは、すべてのインタフェースが TSF に影響するおそれがあることを暗示している。各外部インタフェースは、潜在的な TSF インタフェースなので、機能仕様には、インタフェースがセキュリティに適切であるかどうかを評価者が決定できるように十分詳細な各インタフェースの記述を含める必要がある。
- 998 いくつかのアーキテクチャは、外部インタフェースのグループに対して十分詳細にこのインタフェース記述を容易に提示している。例えば、カーネルアーキテクチャでは、オペレーティングシステムへのすべてのコールがカーネルプログラムで取り扱われる。TSP を侵害するかもしれないコールは、そのようにする権限を持つプログラムによってコールされなければならない。権限とともに実行されるすべてのプログラムは、機能仕様を含める必要がある。権限なしに実行されるカーネルの外部のあらゆるプログラムは、TSP に影響を与えることはできず（すなわち、そのようなプログラムは、図 7.1 のタイプ b ではなく、タイプ a のインタフェースである）そこで、機能仕様から除外することができる。カーネルアーキテクチャが存在する場合、評価者のインタフェース記述の理解は促進されるが、そのようなアーキテクチャは必ずしも必要ない。
- 3:ADV_FSP.1-5 評価者は、TSFI の提示が、効果、例外及び誤りメッセージを記述している各外部インタフェースにおいて、TOE のふるまいを適切に及び正しく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**。
- 999 インタフェースの提示が適切であり、正しいことを評価するために、評価者は、機能仕様、ST の TOE 要約仕様、及び利用者と管理者ガイダンスを使用して、次の要因を評定する。
- a) すべてのセキュリティに関係する利用者入力パラメタ（またはそれらのパラメタの特性化）は識別されるべきである。完全であるために、直接利用者が管理しないパラメタも、それらを管理者が使用できる場合、識別されるべきである。
 - b) レビュー済みガイダンスに記述されているすべてのセキュリティに関係するふるまいは、機能仕様の中で意味(semantics)の記述に反映されるべきである。これには、事象及び各事象の効果としてのふるまいの識別を含めるべきである。例えば、オペレーティングシステムが、ファイルが要求時に開かれない各理由（例えば、アクセス拒否、ファイルが存在しない、他の利用者がファイルを使

用している、利用者は午後 5 時以降にファイルを開くことが許されていない) に対して異なる誤りコードを提供するような、機能の豊富なファイルシステムインタフェースを提供する場合、機能仕様は、要求に対してファイルが開かれたか、または誤りコードが戻されたかを説明するべきである。(機能仕様は、誤りに対するこれらの異なる理由のすべてを列挙することができるが、そのような詳細を提供する必要はない。) 意味の記述には、セキュリティ要件がインタフェースに適用される方法(例えば、インタフェースの使用が監査可能な事象であるかどうか、そして可能な場合は記録可能な情報かどうか)を含めるべきである。

- c) すべてのインタフェースは、操作のすべての可能なモードに対して記述される。TSF が権限の概念を提供する場合、インタフェースの記述は、権限がある場合とない場合のインタフェースのふるまいを説明するべきである。
- d) セキュリティに関するパラメタの記述、及びインタフェースのシンタクス(syntax)に含まれる情報は、すべての証拠資料にわたって一貫しているべきである。

1000 上記の検証は、機能仕様と ST の TOE 要約仕様及び開発者が提供する利用者及び管理者ガイダンスをレビューすることによって行われる。例えば、TOE がオペレーティングシステムとその下層のハードウェアである場合、評価者は、評価される TOE に適切であるとして、利用者アクセス可能プログラムの説明、プログラムのアクティビティを制御するために使用されるプロトコルの記述、プログラムのアクティビティを制御するために使用される利用者アクセス可能データベースの記述、及び利用者インタフェース(例えば、コマンド、アプリケーションプログラムインタフェース)を探す。評価者は、プロセッサ命令セットが記述されていることも保証する。

1001 評価者が、設計、ソースコード、または他の証拠を検査し、機能仕様から抜けて落ちているパラメタまたは誤りメッセージが含まれることを発見するまでは、機能仕様不完全であることを発見しないようなものであるため、このレビューは繰り返される。

ADV_FSP.1.4C

3:ADV_FSP.1-6 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**。

1002 TSF 提示が完全であることを評定するために、評価者は、ST の TOE 要約仕様、利用者ガイダンス、及び管理者ガイダンスを調べる。これらはいずれも、機能仕様の TSF 表現に含まれていないセキュリティ機能を記述するべきでない。

7.6.2.3.2 アクション ADV_FSP.1.2E

3:ADV_FSP.1-7 評価者は、機能仕様 TOE セキュリティ機能要件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**。

1003 すべての ST セキュリティ機能要件が機能仕様によって扱われていることを保証するために、評価者は、TOE 要約仕様と機能仕様間のマッピングを作成することができる。そのようなマッピングは、対応(ADV_RCR.*)要件を満たしているこ

との証拠として開発者によってすでに提供されていることがある。その場合には、評価者は、このマッピングが完全であることを単に検証して、すべてのセキュリティ機能要件が機能仕様の適切な TSFI 表現にマッピングされていることを保証することだけが必要である。

3:ADV_FSP.1-8 評価者は、機能仕様が TOE 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、その仕様を**検査しなければならない**。

1004 特定の特性を備えたセキュリティ機能への各インタフェースに対して、機能仕様の詳細な情報は、ST に特定されているように正確でなければならない。例えば、ST にパスワードの長さが 8 文字でなければならないという利用者認証要件が含まれている場合、TOE は、8 文字のパスワードを持つ必要がある。機能仕様が 6 文字の固定長のパスワードを記述している場合、機能仕様は要件の正確な具体化ではない。

1005 制御された資源で動作する機能仕様の各インタフェースについて、評価者は、それがセキュリティ要件の 1 つを実施することによる起りうる失敗を示す誤りコードを戻すかどうかを決定する。誤りコードが戻されない場合、評価者は、誤りコードを戻されるべきかどうかを決定する。例えば、オペレーティングシステムは、制御されたオブジェクトを「OPEN (開く)」ためにインタフェースを提示することができる。このインタフェースの記述には、アクセスがそのオブジェクトに許可されていないことを示す誤りコードを含めることができる。そのような誤りコードが存在しない場合、評価者は、それが適切であることを確認するべきである (おそらく、アクセスの仲介は、OPEN ではなく、READ と WRITE で行われるため)。

7.6.3 上位レベル設計の評価 (ADV_HLD.2)

7.6.3.1 目的

1006 このサブアクティビティの目的は、上位レベル設計が主要な構成ユニット（すなわち、サブシステム）の観点から TSF を記述しているかどうか、これらの構成ユニットへのインタフェースを記述しているかどうか、機能仕様の正しい具体化であるかどうかを決定することである。

7.6.3.2 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) 機能仕様
- c) 上位レベル設計

7.6.3.3 評価者アクション

1008 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_HLD.2.1E
- b) ADV_HLD.2.2E

7.6.3.3.1 アクション ADV_HLD.2.1E

ADV_HLD.2.1C

3:ADV_HLD.2-1 評価者は、上位レベル設計がすべての必要な非形式的説明文を含んでいることを決定するために、その設計を**検査しなければならない**。

1009 上位レベル設計全体が非形式的である場合、このワークユニットは、適用されないため、満たされているものとみなされる。

1010 準形式的または形式的記述だけでは理解が困難な上位レベル設計のこれらの部分には、補助的な説明的記述が必要となる（例えば、形式的表記の意味を明確にするために）。

ADV_HLD.2.2C

3:ADV_HLD.2-2 評価者は、上位レベル設計の提示が内部的に一貫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**。

1011 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

1012 評価者は、インタフェース仕様がサブシステムの目的の記述と一貫されていることを保証することにより、サブシステムインタフェース仕様の正当性を確認する。

ADV_HLD.2.3C

3:ADV_HLD.2-3 評価者は、TSF 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、上位レベル設計を**検査しなければならない**。

1013 上位レベル設計に関して、用語「サブシステム」(*subsystem*)は、大きな関連するユニット(メモリ管理、ファイル管理、プロセス管理など)を意味する。設計を基本的な機能領域に分解することは、設計を理解するのに役に立つ。

1014 上位レベル設計を検査する主な目的は、評価者の TOE の理解を助けることである。開発者によるサブシステム定義と各サブシステム内の TSF のグループ化の選択は、TOE の意図する動作を理解する上で上位レベル設計を役に立つものにする重要な局面である。このワークユニットの一部として、評価者は、開発者が提示するサブシステムの数が適切であるかどうか、及びサブシステム内の機能のグループ化の選択が適切であるかどうかを評定するべきである。評価者は、TSF のサブシステムへの分解が、TSF の機能がどのように提供されるかを上位レベルで理解するために評価者にとって十分であることを保証するべきである。

1015 上位レベル設計を記述するために使用されるサブシステムを「サブシステム」と呼ぶ必要はない。ただし、それは、同様の分解レベルを表しているべきである。例えば、設計は、「層」または「マネージャ」を使用して分解することもできる。

1016 サブシステム定義の選択と評価者の分析の間いくつかの相互作用が存在することがある。この相互作用については、次のワークユニット 3:ADV_HLD.2-10 で検討する。

ADV_HLD.2.4.C

3:ADV_HLD.2-4 評価者は、上位レベル設計が各サブシステムのセキュリティ機能を記述していることを決定するために、その設計を**検査しなければならない**。

1017 サブシステムのセキュリティ機能のふるまいは、サブシステムが何を行うかの記述である。これには、サブシステムがその機能を使用して実行するように指示されるアクションと、サブシステムが TOE のセキュリティ状態に与える効果(例えば、サブジェクト、オブジェクト、セキュリティデータベースの変更など)の記述を含めるべきである。

ADV_HLD.2.5C

3:ADV_HLD.2-5 評価者は、上位レベル設計が TSF で必要とされるすべてのハードウェア、ファームウェア、及びソフトウェアを識別していることを決定するために、その設計を**チェックしなければならない**。

1018 ST に IT 環境の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、適用されないために、満たされているものとみなされる。

1019 ST に IT 環境に対するセキュリティ要件のオプションステートメントが含まれている場合、評価者は、上位レベル設計に記述される TSF が必要とするハードウェア、ファームウェア、またはソフトウェアのリストと、IT 環境のセキュリティ要件のス

ステートメントを比較して、それらが一致することを決定する。ST の情報は、TOE が実行される下層の抽象マシンの特性を表す。

1020 上位レベル設計に ST に含まれていない IT 環境のセキュリティ要件が含まれている場合、またはそれらが ST に含まれているものと異なる場合、この不一致は、アクション ADV_HLD.2.2E のもとで評価者によって評定される。

3:ADV_HLD.2-6 評価者は、下層のハードウェア、ファームウェア、またはソフトウェアで実装されている補助的な保護メカニズムが提供する機能の提示を、上位レベル設計が含んでいることを決定するために、その設計を**検査しなければならない**。

1021 ST に IT 環境の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、適用されないために、満たされているものとみなされる。

1022 TOE が実行される下層抽象マシンが提供する機能の提示は、TSF の一部である機能の提示と同じ詳細レベルである必要はない。提示は、TOE セキュリティ対策方針をサポートするために TOE が依存する IT 環境のセキュリティ要件を実装するハードウェア、ファームウェア、またはソフトウェアに提供されている機能を TOE が使用する方法を説明するべきである。

1023 IT 環境のセキュリティ要件のステートメントは、ハードウェア、ファームウェア、またはソフトウェアの各種の異なる組み合わせにより満足することができる場合には特に、抽象的でもよい。テストアクティビティの一部として、評価者に IT 環境のセキュリティ要件を満たしていると主張されている下層マシンの少なくとも 1 つ以上の実例が提供される場合、評価者は、これが TOE の必要なセキュリティ機能を提供するかどうかを決定することができる。この評価者による決定には、下層マシンのテストまたは分析は必要ない。それによって提供されることが期待される機能が実際に存在することを決定するだけである。

ADV_HLD.2.6C

3:ADV_HLD.2-7 評価者は、上位レベル設計が TSF サブシステムへのインタフェースを識別していることを**チェックしなければならない**。

1024 上位レベル設計には、各サブシステムに対する、各入口点の名前が含まれている。

ADV_HLD.2.7C

3:ADV_HLD.2-8 評価者は、上位レベル設計が、外部から見える TSF のサブシステムに対するインタフェースを識別していることを**チェックしなければならない**。

1025 ワークユニット 3:ADV_FSP.1-3 で述べたように、外部インタフェース（すなわち、利用者に見えるインタフェース）は、直接または間接的に TSF にアクセスすることができる。TSF に直接または間接的にアクセスする外部インタフェースはいずれも、このワークユニットの識別に含まれる。TSF にアクセスしない外部インタフェースを含める必要はない。

ADV_HLD.2.8C

3:ADV_HLD.2-9 評価者は、上位レベル設計が、各サブシステムへのインタフェースを、それらの目的と使用方法の観点から記述し、そして効果、例外及び誤りメッセージの詳細を適切に提供していることを決定するために、その設計を**検査しなければならない**。

1026 上位レベル設計には、各サブシステムのすべてのインタフェースの目的と使用方法の記述を含めるべきである。そのような記述は、あるインタフェースには概括的に、また他のインタフェースにはさらに詳細に提供することができる。提供されるべき効果、例外及び誤りメッセージの詳細のレベルを決定するとき、評価者は、この分析の目的と TOE によるインタフェースの使用を考慮するべきである。例えば、評価者は、TOE の設計が適切である確信を確認するために、サブシステム間の相互作用の本質を理解する必要がある。この理解は、サブシステム間のいくつかのインタフェースの概括的な記述を理解するだけで得られる。特に、他のサブシステムによってコールされない内部サブシステム入力点は、通常、詳細な記述を必要としない。

1027 詳細のレベルは、ATE_DPT 要件を満たすために採用されたテスト手法にも依存する場合がある。例えば、必要となる詳細の量は、外部インタフェースだけを介してテストするテスト手法と、外部と内部の両方のサブシステムインタフェースを介してテストする手法では異なる。

1028 詳細な記述には、入力と出力のパラメタ、インタフェースの効果、生成される例外または誤りメッセージの詳細が含まれる。外部インタフェースの場合、必要な記述は、おそらく、機能仕様に含まれており、上位レベル設計では繰り返すことなく参照することができる。

ADV_HLD.2.9C

3:ADV_HLD.2-10 評価者は、上位レベル設計が TSP 実施サブシステムとそれ以外のサブシステムに分けて TOE を記述していることを**チェックしなければならない**。

1029 TSF は、TSP の実施に依存される必要がある TOE の部分のすべてからなる。TSF には、TSP を直接実施する機能と、TSP を直接実施しないが、間接的な方法で TSP の実施に貢献する機能の両方が含まれているために、すべての TSP 実施サブシステムは TSF に含まれている。TSP の実施に何の役割も果たさないサブシステムは、TSF の一部ではない。サブシステム全体は、その一部が TSF の一部である場合、TSF の一部となる。

1030 ワークユニット 3:ADV_HLD.2-3 で説明したように、開発者によるサブシステム定義及び各サブシステム内での TSF のグループ化の選択は、TOE の意図する運用を理解する上で上位レベル設計を役に立つものにする重要な局面である。ただし、TSP を直接的または間接的に実施するいずれかの機能を備えたサブシステムは、TSF の一部であるために、サブシステム内の TSF のグループ化の選択は TSF の範囲にも影響する。理解が容易であることを目標とすることも重要であるが、必要な分析の量を減らすために TSF の範囲を制限することも役に立つ。理解が容易であることと範囲を減らすことの 2 つの目標は、ときには相反することがある。評価者は、サブシステム定義の選択を評定するとき、このことを忘れないようにするべきである。

7.6.3.3.2 アクション ADV_HLD.2.2E

3:ADV_HLD.2-11 評価者は、上位レベル設計が TOE 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、その設計を**検査しなければならない**。

1031 評価者は、各 TOE セキュリティ機能の上位レベル設計を分析し、機能が正確に記述されていることを保証する。評価者は、機能が上位レベル設計に含まれていない依存性を持っていないことも保証する。

1032 評価者は、ST と上位レベル設計の両方で IT 環境のセキュリティ要件も分析し、それらが一致することを保証する。例えば、ST に監査証跡を格納するための TOE セキュリティ機能要件が含まれていて、さらに上位レベル設計では監査証跡の格納は、IT 環境によって行われると述べられている場合、上位レベル設計は、TOE セキュリティ機能要件の正確な具体化ではない。

1033 評価者は、インタフェース仕様がサブシステムの目的の記述と一貫していることを保証することにより、サブシステムインタフェース仕様の正当性を確認するべきである。

3:ADV_HLD.2-12 評価者は、上位レベル設計が TOE セキュリティ機能要件の完全な具体化であることを決定するために、その設計を**検査しなければならない**。

1034 すべての ST セキュリティ機能要件が上位レベル設計で扱われていることを保証するために、評価者は、TOE セキュリティ機能要件と上位レベル設計の間のマッピングを作成することができる。

7.6.4 表現対応の評価 (ADV_RCR.1)

7.6.4.1 目的

1035 このサブアクティビティの目的は、開発者が上位レベル設計に機能 ST の要件及び機能仕様を正しく及び完全に実装しているかどうかを決定することである。

7.6.4.2 入力

1036 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) 上位レベル設計
- d) TOE 要約仕様と機能仕様の間の対応分析
- e) 機能仕様と上位レベル設計の間の対応分析

7.6.4.3 評価者アクション

1037 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_RCR.1.1E

7.6.4.3.1 アクション ADV_RCR.1.1E

ADV_RCR.1.1C

3:ADV_RCR.1-1 評価者は、機能仕様が TOE セキュリティ機能の正しい、完全な表現であることを決定するために、TOE 要約仕様と機能仕様の間の対応分析を **検査しなければならない**。

1038 評価者のこのワークユニットの目標は、TOE 要約仕様に識別されているすべてのセキュリティ機能が機能仕様に表現されていること及びそれらが正確に表現されていることを決定することである。

1039 評価者は、TOE 要約仕様の TOE セキュリティ機能と機能仕様の間の対応をレビューする。評価者は、対応が一貫し、正確であることを調べる。対応分析が TOE 要約仕様のセキュリティ仕様と機能仕様のインタフェース記述の間の関係を示しているところでは、評価者は、両方のセキュリティ機能が同じであることを検証する。TOE 要約仕様のセキュリティ機能が、対応するインタフェースにおいて正しく、完全に表されている場合、このワークユニットは、満たされる。

1040 このワークユニットは、ワークユニット 3:ADV_FSP.1-7 及び 3:ADV_FSP.1-8 とともに行うことができる。

3:ADV_RCR.1-2 評価者は、上位レベル設計が機能仕様の正しい、完全な表現であることを決定するために、機能仕様と上位レベル設計の間の対応分析を**検査しなければならない**。

1041 評価者は、対応分析、機能仕様、及び上位レベル設計を使用して、機能仕様に識別されている各セキュリティ機能を上位レベル設計に記述されている TSF サブシステムにマッピングできることを保証する。各セキュリティ機能に対して、対応は、どの TSF サブシステムがその機能のサポートにかかわるかを示す。評価者は、上位レベル設計に各セキュリティ機能の正しい実現の記述が含まれていることを検証する。

7.7 ガイダンス文書アクティビティ

1042 ガイダンス文書アクティビティの目的は、運用 TOE を使用する方法を記述している証拠資料が適切であることを判断することである。そのような証拠資料には、正しくないアクションが TOE のセキュリティに悪影響を与えることがある信頼された管理者と管理者以外の利用者に対する文書と、正しくないアクションが自分自身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信頼できない利用者に対する両方の文書がある。

1043 EAL3 でのガイダンス文書アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) AGD_ADM.1

b) ADG_USR.1

7.7.1 適用上の注釈

1044 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。

7.7.2 管理者ガイダンスの評価 (AGD_ADM.1)

7.7.2.1 目的

1045 このサブアクティビティの目的は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を記述しているかどうかを決定することである。

7.7.2.2 適用上の注釈

1046 用語「*管理者*」(*administrator*) は、TOE 構成パラメタの設定など、TOE 内のセキュリティの重要な操作を実行することを任された人間利用者を示す。この操作は、TSP の実施に影響を与えるので、管理者は、これらの操作を行うために必要な特定の権限を有している。管理者(一人または複数)の役割は、TOE の管理者以外の利用者の役割から明確に区別する必要がある。

1047 監査者、管理者、または日常的な管理など、TOE により認識され、TSF と相互作用することができる ST に定義された異なる管理者の役割またはグループが存在することができる。各役割は、広範な能力のセットを含むか、または単一の能力であることができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。異なる管理者の役割とグループは、管理者ガイダンスにて考慮されるべきである。

7.7.2.3 入力

1048 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順

7.7.2.4 評価者アクション

1049 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_ADM.1.1E

7.7.2.4.1 アクション AGD_ADM.1.1E

AGD_ADM.1.1C

3:AGD_ADM.1-1 評価者は、管理者ガイダンスが TOE の管理者が利用できる管理セキュリティ機能とインタフェースを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**。

1050 管理者ガイダンスには、管理者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

1051 管理者ガイダンスは、管理者セキュリティインタフェースと機能の目的、ふるまい、及び相互関係を識別し、記述するべきである。

1052 各管理者セキュリティインタフェースと機能に対して、管理者ガイダンスは、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) 管理者が設定するパラメタ、それらの正当な値とデフォルトの値を記述する。
- 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。

AGD_ADM.1.2C

3:AGD_ADM.1-2 評価者は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を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**。

1053 管理者ガイダンスは、ST に記述されているものと一貫する IT 環境の TSP に従って、TOE を操作する方法を記述する。

AGD_ADM.1.3C

3:AGD_ADM.1-3 評価者は、管理者ガイダンスがセキュアな処理環境で管理されなければならない機能と権限に関する警告を含んで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**。

1054 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利用者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、管理者ガイダンスに記述されるべきである。

1055 管理者ガイダンスでは、管理すべき機能と権限、それらに必要な管理のタイプ、そのような管理の理由を識別する。警告では、期待される効果、考えられる副次的効果、他の機能と権限との考えられる相互作用を指摘する。

AGD_ADM.1.4C

3:AGD_ADM.1-4 評価者は、管理者ガイダンスが TOE のセキュアな運用に関連する利用者のふるまいに関するすべての前提条件を記述していることを決定するために、そのガイダンスを**検査しなければならない**。

1056 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関する情報のみを管理者ガイダンスに含める必要がある。

1057 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。

AGD_ADM.1.5C

3:AGD_ADM.1-5 評価者は、管理者ガイダンスが管理者の管理下にあるすべてのセキュリティパラメータを、セキュアな値を適切に示して、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**。

1058 各セキュリティパラメータに対して、管理者ガイダンスは、パラメータの目的、パラメータの正当な値とデフォルトの値、そのようなパラメータの安全及び安全でない、個別または組み合わせによる、使用設定を記述するべきである。

AGD_ADM.1.6C

3:AGD_ADM.1-6 評価者は、管理者ガイダンスが TSF の制御下にあるエンティティのセキュリティ特質の変更を含む、実行が必要な管理機能に関連するセキュリティ関連事象の各タイプを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**。

1059 セキュリティ関連事象のすべてのタイプは、詳細に記述されているので、管理者は、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管理者が取る必要があるアクション（存在する場合）を知る。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、管理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_ADM.1.7C

3:AGD_ADM.1-7 評価者は、管理者ガイダンスが評価のために提供された他のすべての文書と一貫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**。

1060 特に ST には、TOE セキュリティ環境とセキュリティ対策方針に関する TOE 管理者への警告に対する詳細な情報を含めることができる。

1061 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_ADM.1.8C

3:AGD_ADM.1-8 評価者は、管理者ガイダンスが管理者に関連する TOE の IT 環境に対するすべての IT セキュリティ要件を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**。

1062 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。

1063 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。

1064 評価者は、TOE の IT 環境に対するセキュリティ要件 (ST のオプションステートメント) を分析し、管理者にとって適切な ST のすべてのセキュリティ要件が管理者ガイダンスに適切に記述されていることを保証するために、それらを管理者ガイダンスと比較するべきである。

7.7.3 利用者ガイダンスの評価 (AGD_USR.1)

7.7.3.1 目的

1065 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 が提供するセキュリティ機能とインタフェースを記述しているかどうか、及びこのガイダンスが TOE のセキュアな使用のための説明とガイドラインを提供しているかどうかを決定することである。

7.7.3.2 適用上の注釈

1066 TOE によって認識され、TSF と相互作用を行うことができる ST に定義されている異なる利用者の役割とグループが存在することができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。異なる利用者の役割とグループは、利用者ガイダンスにて考慮されるべきである。

7.7.3.3 入力

1067 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順

7.7.3.4 評価者アクション

1068 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_USR.1.1E

7.7.3.4.1 アクション AGD_USR.1.1E

AGD_USR.1.1C

3:AGD_USR.1-1 評価者は、利用者ガイダンスが TOE の非管理者である利用者が使用できるセキュリティ機能とインタフェースを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**。

1069 利用者ガイダンスには、利用者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

1070 利用者ガイダンスには、セキュリティインタフェースと機能の目的を識別し、記述すべきである。

AGD_USR.1.2C

3:AGD_USR.1-2 評価者は、利用者ガイダンスが TOE により提供された利用者がアクセスできるセキュリティ機能の使用法を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**。

1071 利用者ガイダンスには、利用者が使用できるセキュリティインタフェースと機能のふるまいと相互関係を識別し、記述すべきである。

1072 利用者が TOE セキュリティ機能を起動することができる場合、利用者ガイダンスに、その機能に対して利用者が使用できるインタフェースの記述を提供する。

1073 各インタフェースと機能に対して、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、コマンドボタンなど）
- b) 利用者が設定するパラメタ及びそれらの正当な値とデフォルトの値を記述する。
- 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。

AGD_USR.1.3C

3:AGD_USR.1-3 評価者は、利用者ガイダンスがセキュアな処理環境で管理されなければならない利用者がアクセスできる機能と権限についての警告を含んで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**。

1074 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利用者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。これらの利用者がアクセス可能な機能と権限は、利用者ガイダンスに記述される。

1075 利用者ガイダンスでは、使用できる機能と権限、それらに必要となるコマンドのタイプ、そのようなコマンドの理由を識別すべきである。利用者ガイダンスには、管理すべき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、考えられる副次的効果、他の機能と権限との考えられる相互作用を指摘すべきである。

AGD_USR.1.4C

3:AGD_USR.1-4 評価者は、利用者ガイダンスが TOE セキュリティ環境の記述の中にある利用者のふるまいについての前提条件に関連した責任を含む、TOE のセキュアな運用に必要なすべての利用者の責任を提示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**。

- 1076 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関係する情報のみを利用者ガイダンスに含める必要がある。
- 1077 利用者ガイダンスでは、セキュリティ機能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。
- 1078 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。
- 1079 利用者ガイダンスでは、利用者が機能を起動することができるかどうかまたは利用者が管理者の助けを必要とするかどうかを示すべきである。

AGD_USR.1.5C

- 3:AGD_USR.1-5 評価者は、利用者ガイダンスが評価のために提供された他のすべての証拠資料と一貫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**。
- 1080 評価者は、評価のために提供された利用者ガイダンスとその他のすべての文書が互いに矛盾しないことを保証する。この保証は、ST に TOE セキュリティ環境とセキュリティ対策方針に関する TOE 利用者への警告についての詳細な情報が含まれているときに特に必要となる。
- 1081 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_USR.1.6C

- 3:AGD_USR.1-6 評価者は、利用者ガイダンスが利用者に関連する TOE の IT 環境に対するすべてのセキュリティ要件を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**。
- 1082 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。
- 1083 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。
- 1084 評価者は、TOE の IT 環境に対するセキュリティ要件（ST のオプションステートメント）を分析し、利用者にとって適切な ST のすべてのセキュリティ要件が利用者ガイダンスに適切に記述されていることを保証するために、利用者ガイダンスと比較するべきである。

7.8 ライフサイクルサポートアクティビティ

1085 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 の開発と保守の間に使用する手続きが適切であることを決定することである。そのような手続きは、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。

1086 EAL3 のライフサイクルサポートアクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ALC_DVS.1

7.8.1 開発セキュリティの評価 (ALC_DVS.1)

7.8.1.1 目的

1087 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。

7.8.1.2 入力

1088 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

1089 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ことができる。特に評価者は、開発者の構成管理証拠資料 (ACM_CAP.3 と ACM_SCP.1 サブアクティビティへの入力) を検査する必要がある。手続きが適用されていることを示す証拠も必要となる。

7.8.1.3 評価者アクション

1090 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ALC_DVS.1.1E

b) ALC_DVS.1.2E

7.8.1.3.1 アクション ALC_DVS.1.1E

ALC_DVS.1.1C

- 3: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**。
- 1091 評価者は、情報が明示的に提供されなくても、必要な保護、特に脅威に晒されているセクション、組織のセキュリティ方針及び前提条件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。環境に対するセキュリティ対策方針のステートメントもこの点で有用である。
- 1092 明示的な情報が ST から提供されない場合、評価者は、TOE に意図される環境を考慮して、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、明確な正当化が評価のために提供されるべきである。
- 1093 次のタイプ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 (physical)*。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 (procedural)*。例えば、次のものをカバーする。
 - 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
 - 保護される資材の開発環境の外部への移送
 - 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 (personal)*。例えば、新たな開発スタッフの信頼を確認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。
- 1094 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で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施設、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。開発には、必要に応じて、TOE の複数のコピーの作成などのタスクが含まれる。このワークユニットは、ADO_DEL のワークユニットと重複するべきでない。ただし、評価者は、1 つのサブアクティビティまたは他のアクティビティによってすべての局面が扱われていることを保証するべきである。
- 1095 さらに、開発セキュリティ証拠資料は、セキュリティ手段の実行及び要求される入力と出力の観点から、開発の異なる局面に適用できる異なるセキュリティ手段を記

述することができる。例えば、異なる手続きを、TOE の異なる部分の開発または開発プロセスの異なる段階に適用することができる。

3: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**。

1096 これらには次のことを管理する方針が含まれる。

- 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資材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変更から保護する必要がある資材及びそのような資材を変更することができる開発スタッフのメンバ

1097 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こと。

1098 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、ACM_CAP サブアクティビティ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る必要がある、TOE を変更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。

1099 ACM_CAP 要件は固定されているが、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 のセキュリティ環境セクションに提供される情報に依存する。例えば、ST は、機密事項を扱う就任許可(security clearance)を持つスタッフによって開発される TOE を要求する組織のセキュリティ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。

ALC_DVS.1.2C

3:ALC_DVS.1-3 評価者は、手続きを適用した結果として作成される記録による証拠が生成されたことを決定するために、開発セキュリティ証拠資料を**チェックしなければならない**。

1100 記録による証拠が作成されるとき、評価者は、それを検査して、手続きが遵守されていることを保証する。作成される証拠の例には、エントリログと監査証跡がある。評価者は、証拠をサンプリングすることを選択できる。

1101 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

7.8.1.3.2 アクション ALC_DVS.1.2E

3:ALC_DVS.1-4 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**。

1102 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ているといった、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。

1103 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、監督者と相談して決定されるべきである。

1104 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

7.9 テスタクティビティ

1105 このアクティビティの目的は、TOE が設計証拠資料の特定及び ST に特定されている TOE セキュリティ機能要件に従ってふるまうかどうかを決定することである。これは、開発者が機能テストと上位レベル設計に対して TSF をテストしたことを決定し、開発者のテストのサンプルを実行することによるそれらのテスト結果に確信を持ち、TSF のサブセットをテストすることによって行われる。

1106 EAL3 のテストアクティビティには、次のコンポーネントに関係するサブアクティビティが含まれる。

- a) ATE_COV.2
- b) ATE_DPT.1
- c) ATE_FUN.1
- d) ATE_IND.2

7.9.1 適用上の注釈

1107 評価者のテストサブセットのサイズと構成は、独立テスト (ATE_IND.2) サブアクティビティに記述されているいくつかの要因に依存する。サブセットの構成に影響を与えるそのような要因の 1 つは、評価者が (例えば、組織(scheme)から) アクセスする必要がある情報である *知られている公知の弱点 (known public domain weakness)* である。

1108 CC は、カバレッ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に適用するときの柔軟性を増している。ただし、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、評価者のサブアクティビティ間の作業努力の重複をもたらした。これらの適用上の注釈は、同じアクティビティと EAL の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。

7.9.1.1 TOE の期待されるふるまいの理解

1109 テスト証拠資料が適切であることを正確に評価するまえに、または新しいテストを作成するまえに、評価者は、満たす必要がある要件として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。

1110 評価者は、1 度に TSF の 1 つのセキュリティ機能に焦点を当てることを選択することができる。各セキュリティ機能に対して、評価者は、TOE の期待されるふるまい方の理解を得るために、ST 要件と機能仕様、上位レベル設計、及びガイダンス証拠資料の関連する部分を検査する。

1111 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、外部または内部のいずれかのインタフェースで刺激されるセキュリティ機能を引き起こし、その応答が観察される。ただし、セキュリティ機能をインタフェースで適切にテストできない場合がある (例

えば、残存情報保護機能の場合)。そのような場合には、別の手段を採用する必要がある。

7.9.1.2 セキュリティ機能の期待されるふるまいを検証するための、テスト 対 代替手法

1112 インタフェースで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こと。代替手法が適切であることを決定するのは、評価者の責任である。ただし、代替手法が適切であることを評定するとき、次のことを考慮すること。

- 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を意味することができる。
- b) EAL が下位レベル設計または実装への評価の提示(exposure)と一致しない場合でも、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が容認される。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るために与えられるべきである。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、変更が分析またはその後のテストによって追跡され、対処されたとの証拠が必要となる。

1113 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セキュリティ機能の期待されるふるまいをテストする実際的な手段が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。この代替は、上記の環境でのテストの費用（時間及び/または経費）をできる限り少なくするために開発者に提供される。これは、TOE についての不当に余分の情報を要求する自由を評価者に与えるためのものでもなければ、一般的テストに置き換わるためのものでもない。

7.9.1.3 テストの適切性の検証

1114 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必要がある。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、完全に適切であることを決定する必要がある。

1115 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、インタフェース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及び上位レベル設計と一貫していることを決定しなければならない。テストは、これらの仕様において証拠資料として提出されたふるまいを検証しなければならない。このことは、機能仕様と上位レベル設計に明示的に記述されている各セキュリティ機能ふるまい特性が、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。

1116 TSF のすべては開発者によってテストされる必要があるが、インタフェースの徹底的な仕様テストは要求されない。このアクティビティの全体的な目的は、各セキュ

リティ機能が機能仕様と上位レベル設計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。テスト手順は、テスト機能がテスト中に開発者によって実行された方法の洞察を提供する。評価者は、TOE を独立にテストする追加のテストを開発するときに、この情報を使用する。

7.9.2 カバレッジの評価 (ATE_COV.2)

7.9.2.1 目的

1117 このサブアクティビティの目的は、テスト（証拠資料として提出されている）が、TSF が系統的に機能仕様に対してテストされていることを確認するのに十分であるかどうかを決定することである。

7.9.2.2 入力

- a) ST
- b) 機能仕様
- c) テスト証拠資料
- d) テストカバレッジ分析

7.9.2.3 評価者アクション

このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_COV.2.1E

7.9.2.3.1 アクション ATE_COV.2.1E

ATE_COV.2.1C

3:ATE_COV.2-1 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の間に対応が正確であることを決定するために、テストカバレッジ分析を**検査しなければならない**。

1118 対応は、表またはマトリックスの形を取ることができる。場合によっては、マッピングがテストの対応を十分に示すことができる。その他の場合、根拠（通常、散文）により開発者が提供する対応分析を補足しなければならない場合がある。

1119 図 7.2 は、機能仕様に記述されているセキュリティ機能と、それらをテストするために使用されるテスト証拠資料に示されているテストの間の対応の概念的枠組みを示している。テストには、テストの依存性または実行されるテストの全体的目標によって、1 つまたは複数のセキュリティ機能を含めることができる。

1120 テストカバレッジ分析に示されるテストとセキュリティ機能の識別は、曖昧でなくされる必要がある。テストカバレッジ分析により、評価者は、識別されているテストをテスト証拠資料まで、及びテストされている特定のセキュリティ機能を機能仕様までさかのぼることができる。

3:ATE_COV.2-2 評価者は、TSF の各セキュリティ機能に対するテスト手法が、期待されるふるまいを実証するのに適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**。

1121 このワークユニットのガイダンスは、次の中に見つけることができる。

- a) 適用上の注釈、7.9.1.1 節、TOE の期待されるふるまいの理解
- b) アプリケーションノート、7.9.1.2 節、セキュリティ機能の期待されるふるまいを検証するための、テスト 対 代替手法

3: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セキュリティ機能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**。

1122 このワークユニットのガイダンスは、次の中に見つけることができる。

- a) 適用上の注釈、7.9.1.3 節、テストの適切性の検証

ATE_COV.2.2C

3:ATE_COV.2-4 評価者は、機能仕様に記述されている TSF と、テスト証拠資料に識別されてい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、テストカバレッジ分析を**検査しなければならない**。

1123 機能仕様に記述されているすべてのセキュリティ機能とインタフェースをテストカバレッジ分析に示し、テストにマッピングし、完全性を主張する必要がある。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。図 7.2 が示すように、セキュリティ機能のすべては、それらに関するテストが存在する。それゆえに、完全なテストカバレッジがこの例に示されている。セキュリティ機能がテストカバレッジ分析に識別されているならば、それに対するテストが示されない場合、カバレッジが不完全であることは明らかである。

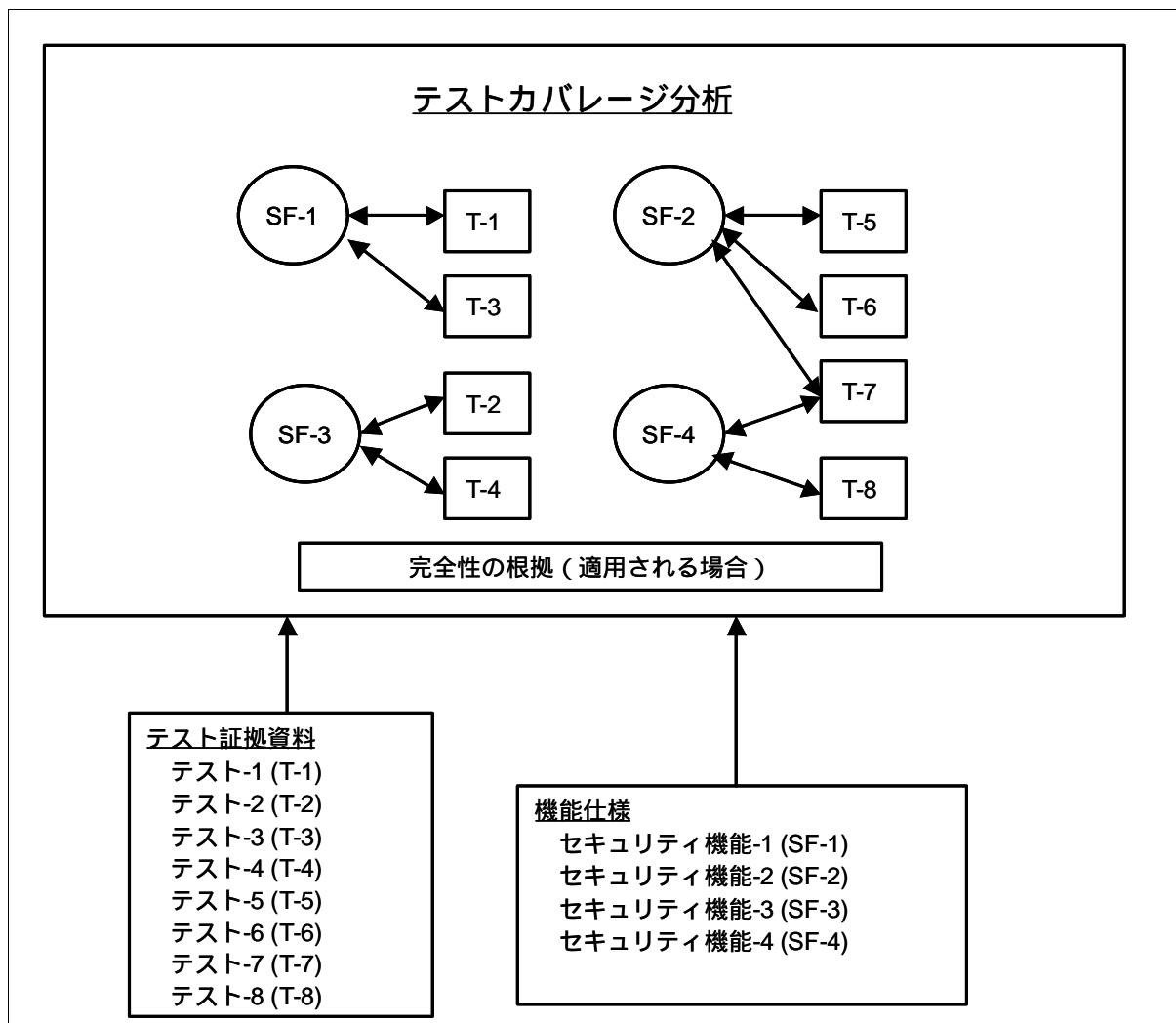


図 7.2 テストカバレッジ分析の概念的枠組み

7.9.3 深さの評価 (ATE_DPT.1)

7.9.3.1 目的

1124 このサブアクティビティの目的は、開発者が TSF をその上位レベル設計と比較してテストしたかどうかを決定することである。

7.9.3.2 入力

- a) ST
- b) 機能仕様
- c) 上位レベル設計
- d) テスト証拠資料
- e) テストの深さ分析

7.9.3.3 評価者アクション

1125 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_DPT.1.1E

7.9.3.3.1 アクション ATE_DPT.1.1E

ATE_DPT.1.1C

3:ATE_DPT.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上位レベル設計とのマッピングのテストの深さ分析を **検査しなければならない。**

1126 テストの深さ分析は、上位レベル設計に記述されているすべてのサブシステムを識別し、テストのこれらのサブシステムへのマッピングを提供する。対応は、表またはマトリックスの形を取ることができる。場合によっては、マッピングがテストの対応を十分に示すことができる。その他の場合、根拠（通常、散文）により開発者が提供する対応分析を補足しなければならない場合がある。

1127 TOE セキュリティ要件にマッピングされ、その要件を満たす上位レベル設計に特定されているすべての設計詳細は、テストが必要であり、それゆえに、テスト証拠資料にマッピングされるべきである。図 7.3 は、上位レベル設計に記述されているサブシステムと、それらをテストするために使用される TOE のテスト証拠資料に示されているテストの間の対応の概念的枠組みを示している。テストには、テストの依存性または実行されるテストの全体的目標によって、1 つまたは複数のセキュリティ機能を含めることができる。

3:ATE_DPT.1-2 評価者は、TSF の各セキュリティ機能に対するテスト手法が、期待されるふるまいを実証するのに適していることを決定するために、開発者のテスト計画を **検査しなければならない。**

- 1128 このワークユニットのガイダンスは、次の中に見つけることができる。
- a) 適用上の注釈、7.9.1.1 節、TOE の期待されるふるまいの理解
 - b) アプリケーションノート、7.9.1.2 節、セキュリティ機能の期待されるふるまいを検証するための、テスト 対 代替手法
- 1129 TSF のテストは、外部インタフェース、内部インタフェース、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、セキュリティ機能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セキュリティ機能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。
- 3:ATE_DPT.1-3 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テスト機能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**。
- 1130 このワークユニットのガイダンスは、次の中に見つけることができる。
- a) 適用上の注釈、7.9.1.3 節、テストの適切性の検証
- 3:ATE_DPT.1-4 評価者は、上位レベル設計に定義されている TSF がテスト証拠資料のテストに完全にマッピングされていることを保証するために、テストの深さ分析を **チェックしなければならない**。
- 1131 テストの深さ分析は、上位レベル設計とテスト計画及び手順の間の対応の完全なステートメントを提供する。上位レベル設計に記述されているすべてのサブシステムと内部インタフェースは、テストの深さ分析に示されている必要がある。テストの深さ分析に示されているサブシステムと内部インタフェースのすべてに対して、完全性を主張するために、それらへマッピングされているテストをもつ必要がある。図 7.3 が示すように、サブシステムと内部インタフェースのすべては、それらに関係するテストが存在する。それゆえに、完全なテストの深さがこの例に示されている。サブシステムと内部インタフェースがテストの深さ分析に識別されているならば、それに対するテストが示されない場合、カバレッジが不完全であることは明らかである。

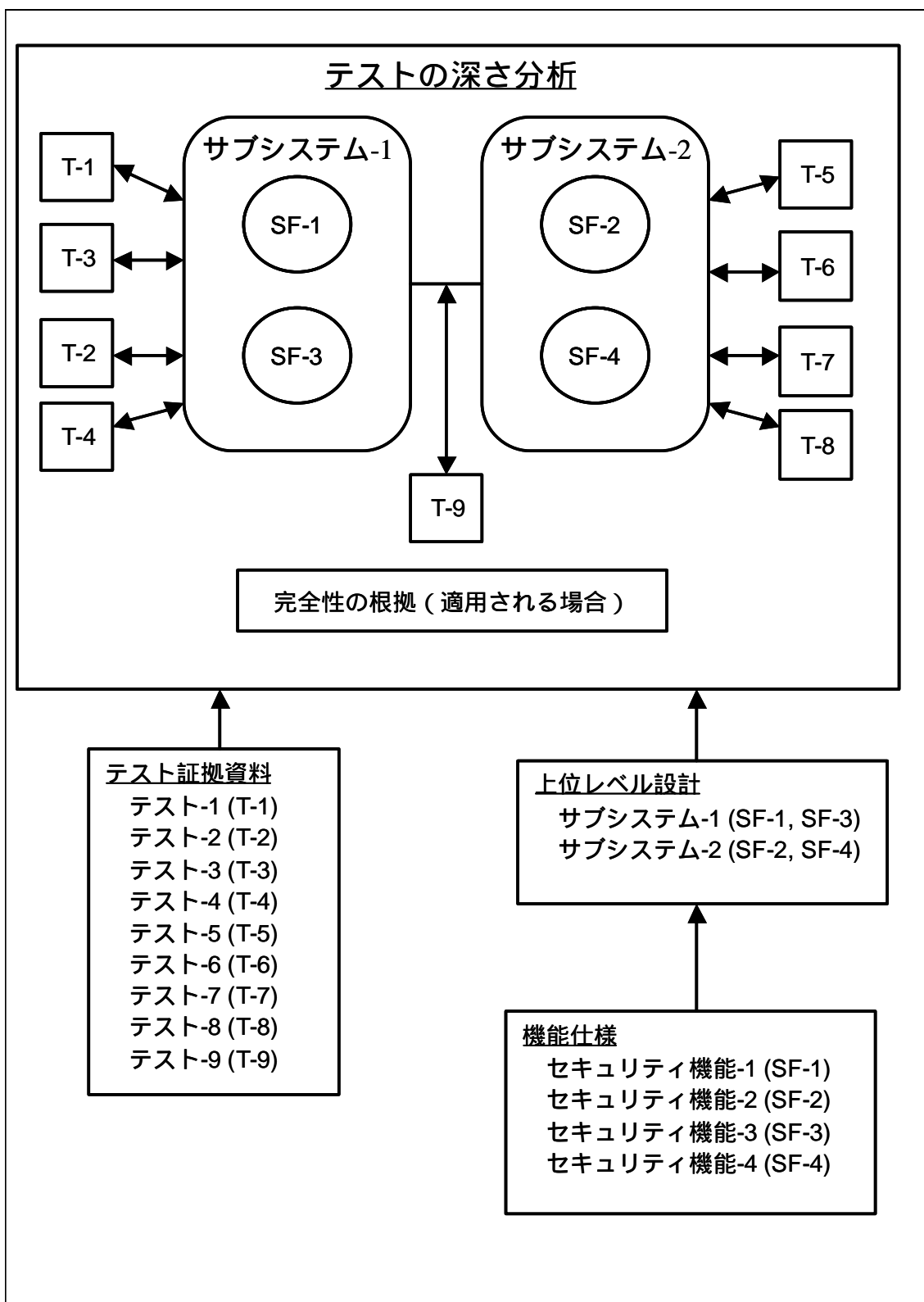


図 7.3 テストの深さ分析の概念的枠組み

7.9.4 機能テストの評価 (ATE_FUN.1)

7.9.4.1 目的

1132 このサブアクティビティの目的は、セキュリティ機能が特定されたとおりに実行されることを実証するのに、開発者の機能テスト証拠資料が十分であるかどうかを決定することである。

7.9.4.2 適用上の注釈

1133 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、カバレッジ保証コンポーネントに依存する。

1134 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が、特定されたとおりに実行しないことを示しているセキュリティ機能はいずれも、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。

7.9.4.3 入力

1135 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) テスト手順

7.9.4.4 評価者アクション

1136 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_FUN.1.1E

7.9.4.4.1 アクション ATE_FUN.1.1E

ATE_FUN.1.1C

3:ATE_FUN.1-1 評価者は、テスト証拠資料にテスト計画、テスト手順記述、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**。

ATE_FUN.1.2C

3:ATE_FUN.1-2 評価者は、テスト計画がテストされるセキュリティ機能を識別していることを**チェックしなければならない**。

EAL3:ATE_FUN.1

- 1137 テストされるセキュリティ機能を識別するために使用できる 1 つの方法は、個々のセキュリティ機能を特定している機能仕様の適切な部分を参照することである。
- 1138 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。
- 1139 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 3:ATE_FUN.1-3 評価者は、テスト計画が実行されるテストの目標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**。
- 1140 テスト計画は、セキュリティ機能をテストする方法とテストが行われるテスト構成についての情報を提供する。
- 1141 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。
- 1142 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 3:ATE_FUN.1-4 評価者は、TOE テスト構成が ST における評価のために識別されている構成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**。
- 1143 テストに使用される TOE は、ACM_CAP.3 サブアクティビティによって確証されたのと同じ一意的リファレンスと開発者が提供するテスト証拠資料を持つべきである。
- 1144 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個別のハードウェアとソフトウェア実装で構成することができる。評価者は、ST に記述されている各評価済みの構成に一貫するテスト構成が存在することを検証する。
- 1145 評価者は、テスト環境に適用できる ST に記述されている TOE 環境のセキュリティの側面についての前提条件を考慮するべきである。ST にはテスト環境に適用されない前提条件がいくつか存在することがある。例えば、利用者の取扱許可についての前提条件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前提条件は適用するだろう。
- 3:ATE_FUN.1-5 評価者は、テスト計画がテスト手順記述と一貫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**。
- 1146 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。
- 1147 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ATE_FUN.1.3C

- 3:ATE_FUN.1-6 評価者は、テスト手順記述がテストされる各セキュリティ機能のふるまいを識別していることを**チェックしなければならない**。

- 1148 テストされるセキュリティ機能のふるまいを識別するために使用できる 1 つの方法は、テストする個々のふるまいを特定している設計仕様の適切な部分を参照することである。
- 1149 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。
- 1150 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 3:ATE_FUN.1-7 評価者は、もしあれば順序の依存性を含め、再現できる初期テスト条件を確立するための十分な指示が提供されていることを決定するために、テスト手順記述を**検査しなければならない**。
- 1151 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まえに、追加される必要がある。他のテスト結果の順序に依存する一例は、アクセス制御のような他のセキュリティメカニズムに対する監査レコードを作成するために監査機能に頼るまえに、監査機能をテストする必要があることである。順序に依存する他の例としては、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。
- 1152 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。
- 1153 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 3:ATE_FUN.1-8 評価者は、セキュリティ機能を刺激し、それらのふるまいを観察するための再現可能な手段を取れるように十分な指示が提供されていることを決定するために、テスト手順記述を**検査しなければならない**。
- 1154 刺激は、通常、TSFI を通して外部からセキュリティ機能に提供される。一度入力 (input) (刺激(stimulus)) が TSFI に提供されれば、セキュリティ機能のふるまいを TSFI で観察することができる。テスト手順に刺激とこの刺激の結果として期待されるふるまいを曖昧さなく記述した詳細な情報が含まれていない限り、再現可能であると保証されない。
- 1155 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。
- 1156 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 3:ATE_FUN.1-9 評価者は、テスト手順記述がテスト手順と一貫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**。
- 1157 テスト手順記述がテスト手順である場合、このワークユニットは適用されず、条件は満たされているものとみなされる。
- 1158 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。

- 1159 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ATE_FUN.1.4C

- 3:ATE_FUN.1-10 評価者は、十分な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**。

- 1160 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、テスト手法を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。

- 1161 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。

- 1162 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

ATE_FUN.1.5C

- 3:ATE_FUN.1-11 評価者は、テスト証拠資料の期待されるテスト結果が提供された実際の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**。

- 1163 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。

- 1164 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。

- 1165 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）。

- 1166 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変更を行わずに、このプロセスが正しいかどうかを評定するために使用することが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のは、開発者の責任である。

- 1167 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。

- 1168 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

- 1169 いずれかのテストの期待されるテスト結果と実際のテスト結果が同じでない場合、セキュリティ機能が正しく働いているとの実証は達成されない。そのようなことは、関係するセキュリティ機能のテストを含める評価者の独立テストの成果に影響を与

える。評価者は、また、このワークユニットが行われる証拠のサンプルを増やすことを考慮するべきである。

3:ATE_FUN.1-12 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。**

1170 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、他の評価者や監督者が、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。

1171 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) 実行された開発者テストの量。開発者テストのカバレッジと深さの範囲の記述。
- d) テスト結果。開発者テストの全体的な結果の記述。

1172 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 に示すべきタイプの情報を提供することだけを意図している。

7.9.5 独立テストの評価 (ATE_IND.2)

7.9.5.1 目的

1173 このアクティビティの目的は、TSF のサブセットを独立にテストすることにより TOE が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、また開発者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の確信を得ることである。

7.9.5.2 入力

1174 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) 利用者ガイダンス
- d) 管理者ガイダンス
- e) セキュアな設置、生成、及び立上げの手順
- f) テスト証拠資料
- g) テストカバレッジ分析
- h) テストの深さ分析
- i) テストに適した TOE

7.9.5.3 評価者アクション

1175 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_IND.2.1E
- b) ATE_IND.2.2E
- c) ATE_IND.2.3E

7.9.5.3.1 アクション ATE_IND.2.1E

ATE_IND.2.1C

3:ATE_IND.2-1 評価者は、テスト構成が ST に特定のとおり評価のもとでの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**。

1176 テストに使用される TOE は、ACM_CAP.3 サブアクティビティによって確認されたのと同じ一意的リファレンスと開発者が提供するテスト証拠資料を持つべきである。

- 1177 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個別のハードウェアとソフトウェア実装で構成することができる。評価者は、ST に記述されている各評価済みの構成に一貫するテスト構成が存在することを検証する。
- 1178 評価者は、テスト環境に適用できる ST に記述されている TOE 環境のセキュリティの側面についての前提条件を考慮するべきである。ST にはテスト環境に適用されない前提条件がいくつか存在することがある。例えば、利用者の取扱許可についての前提条件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前提条件は適用するだろう。
- 1179 いずれかのテスト資源（例えば、メータ、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。

3: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**。

- 1180 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、ADO_IGS.1 サブアクティビティ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確信している場合、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て、TOE を設置、生成し、立上げする開発者の手順に従うべきである。

- 1181 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 3:ADO_IGS.1-2 の条件を満たすことができる。

ATE_IND.2.2C

3: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**。

- 1182 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。

7.9.5.3.2 アクション ATE_IND.2.2E

3:ATE_IND.2-4 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**。

- 1183 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厳密にではなくテストでき得る多くのセキュリティ機能を含めることである。別のテスト方策は、気が付いた問題との関連に基づいたいくつかのセキュリティ機能を含んだテストサブセットを持ち、これらの機能を厳密にテストすることである。

- 1184 一般的に、評価者のテスト手法は、これら 2 つの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、ST に識別されているほとんどのセ

セキュリティ機能要件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。

1185 評価者は、テストする TSF 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、テストカバレッジ分析、テストの深さ分析、及びテスト証拠資料からなる。開発者テスト証拠は、テスト中に開発者がセキュリティ機能をテストした方法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) 特定のセキュリティ機能に対する開発者テストの増加。評価者は、セキュリティ機能をさらに厳密にテストするためにパラメータを変えて、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) 特定のセキュリティ機能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、特定のセキュリティ機能のテスト手法を変更することができる。
- b) テストサブセットに加えるセキュリティ機能の数。TOE に含まれているセキュリティ機能の数が少ない場合には、セキュリティ機能のすべてを厳密にテストすることが現実的にできる。多数のセキュリティ機能を持つ TOE では、これは費用効果が悪く、サンプリングが必要になる。
- 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。

1186 評価者は、サブセットを構成するセキュリティ機能を選択する。この選択は、数多くの要因に依存し、これらの要因の考慮は、テストサブセットサイズの選択にも影響を与える。

- a) セキュリティ機能の開発者テストの厳密さ。機能仕様に識別されているすべてのセキュリティ機能は、ATE_COV.2 で要求されるそれらに関する開発者テスト証拠を備えている必要がある。追加のテストが必要であると評価者が決定したセキュリティ機能は、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セキュリティ機能またはその様相が特定どおりに動作す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セキュリティ機能を含めるべきである。
- c) TOE の種別に一般的に関係する知られている公知の弱点（例えば、オペレーティングシステム、ファイアウォール）。TOE の種別に関係する知られている公知の弱点は、テストサブセットの選択プロセスに影響する。評価者は、その種別の TOE に対して知られている公知の弱点に対処するそれらのセキュリティ機能をサブセットに含めるべきである（ここでの知られている公知の弱点は、そのような脆弱性を意味せず、この特別の種別の TOE で経験された不十分性または問題領域を意味する）。そのような弱点が知られていない場合には、セキュリティ機能の広い範囲を選択する比較一般的な手法がさらに適している。

- d) セキュリティ機能の重要性。TOE に対するセキュリティ対策方針の観点から他のセキュリティ機能よりも重要なセキュリティ機能は、テストサブセットに含まれるべきである。
- e) ST でなされている SOF 主張。特定の SOF 主張に対するすべてのセキュリティ機能はテストサブセットに含まれるべきである。
- f) セキュリティ機能の複雑性。複雑なセキュリティ機能は、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めんどろな要求を課す複雑なテストを必要とするかもしれない。逆に複雑なセキュリティ機能は、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。
- g) 暗黙のテスト。あるセキュリティ機能のテストは、しばしば暗黙に他のセキュリティ機能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、(暗黙にはあるが) テストされるセキュリティ機能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を提供するために使用され、効率的なテスト手法の標的となる。
- h) TOE への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。
- i) 革新的または一般的でない機能。販売広告用の印刷物で強調しているような革新的または一般的でないセキュリティ機能が TOE に含まれている場合、これらは、テストの有力な候補となるべきである。

1187 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。

1188 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

3:ATE_IND.2-5 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**。

1189 評価者は、ST 及び機能仕様からセキュリティ機能の期待されるふるまいを理解して、機能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、セキュリティ機能を外部インタフェースでテストするか、テストハーネス(test harness)を使用して内部インタフェースでテストするか、または別のテスト手法 (例えば、例外状況、コード検査) を採用するべきか。
- b) セキュリティ機能を刺激し、応答を観察するために使用されるセキュリティ機能インタフェース。
- c) テストに存在する必要がある初期条件 (すなわち、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) セキュリティ機能を刺激する（例えば、パケットジェネレータ）またはセキュリティ機能を観察する（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。

1190 評価者は、一連のテストケースを使用して各セキュリティ機能をテストするのが実際的であることを発見することがある。その場合、各テストケースは、期待されるふるまいの大変特定な局面をテストする。

1191 評価者のテスト証拠資料は、必要に応じて、該当する設計仕様、及び ST までさかのぼって各テストの起源を特定すること。

3:ATE_IND.2-6 評価者はテストを**実施しなければならない**。

1192 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。

3:ATE_IND.2-7 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) テストするセキュリティ機能のふるまいの識別
- 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) すべての前提となるテスト条件を確立するための指示
- d) セキュリティ機能を刺激するための指示
- e) セキュリティ機能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

1193 詳細のレベルは、他の評価者がテストを繰り返し、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、異なっても良いが、全体的な結果は同一であるべきである。

1194 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が、期待される結果を比較するまえに、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。

3:ATE_IND.2-8 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**。

1195 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変更を必要とする。この決定とそれを正当とする理由は、評価者に任される。

7.9.5.3.3 アクション ATE_IND.2.3E

3:ATE_IND.2-9 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**。

1196 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。

1197 テストアクティビティ全体に対する評価者の全体的な労力を考慮して、通常、開発者のテストの 20%が実行されるべきである。ただし、これは、TOE の本質と提供されるテスト証拠によって変化する。

1198 開発者のテストはすべて、特定のセキュリティ機能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.2-4 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。

1199 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

3:ATE_IND.2-10 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**。

1200 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。

1201 十分な説明または解明が得られない場合、開発者のテスト結果に対する評価者の確信は落ちるであろうし、評価者はサンプルサイズを増やし、開発者のテストへの確信を取り戻す必要がある場合がある。サンプルサイズを増やしても評価者の懸念を取り去ることができない場合には、開発者テストの全体のセットを繰り返す必要がある。最終的には、ワークユニット ATE_IND.2-4 に識別されている TSF サブセットが適切にテストされるまで、開発者のテストの欠陥は、開発者のテストの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。

3: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成果を**報告しなければならない**。

1202 ETR に報告される評価者のテスト情報は、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、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、他の評価者や監督者が、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。

1203 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セキュリティ機能の量とサイズの正当とする理由。
- c) サブセットを構成するセキュリティ機能の選択基準。サブセットに含めるセキュリティ機能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) テストされたセキュリティ機能。サブセットに含めることに値したセキュリティ機能の簡単なリスト。
- 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。

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 に示すべきタイプの情報を提供することだけを意図している。

7.10 脆弱性評価アクティビティ

1204 脆弱性評価アクティビティの目的は、意図する環境での 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、開発者と評価者が行う分析に基づいて行われ、評価者のテストによりサポートされる。

1205 EAL3 での脆弱性評価アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) AVA_MSU.1

b) AVA_SOF.1

c) AVA_VLA.1

7.10.1 誤使用の評価 (AVA_MSU.1)

7.10.1.1 目的

1206 このサブアクティビティの目的は、ガイダンスが誤解されるか、合理的でないか、または矛盾しているか、操作のすべてのモードに対するセキュアな手順が取り扱われているかどうか、及びガイダンスを使用して容易に TOE の安全でない状態を阻止し、検出することができるかどうかを決定することである。

7.10.1.2 適用上の注釈

1207 このサブアクティビティでの用語「ガイダンス」(*guidance*)の使用は、利用者ガイダンス、管理者ガイダンス、セキュアな設置、生成及び立上げ手順を意味する。ここでの設置、生成及び立上げ手順は、TOE を配付された状態から運用状態にするために行う、管理者が責任を負うすべての手順を意味する。

7.10.1.3 入力

1208 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) 上位レベル設計

d) 利用者ガイダンス

e) 管理者ガイダンス

f) セキュアな設置、生成、及び立上げの手順

g) テスト証拠資料

7.10.1.4 評価者アクション

1209 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。

a) AVA_MSU.1.1E

b) AVA_MSU.1.2E

c) AVA_MSU.1.3E

7.10.1.4.1 アクション AVA_MSU.1.1E

AVA_MSU.1.1C

3:AVA_MSU.1-1 評価者は、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、故障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、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**。

1210 その他の評価証拠、特に機能仕様とテスト証拠資料は、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。

1211 評価者は、セキュリティ機能を安全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、セキュリティ機能に関するガイダンスがそのセキュリティ機能のセキュアな使用（すなわち、TSP と一貫している）に十分であることを決定するために、1 度に 1 つのセキュリティ機能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して機能の間の関係も考慮するべきである。

AVA_MSU.1.2C

3:AVA_MSU.1-2 評価者は、ガイダンスが明白であり、内部的に一貫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**。

1212 ガイダンスは、管理者または利用者によって間違っ構成されており、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。

1213 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

3:AVA_MSU.1-3 評価者は、ガイダンスが完全であり、合理的であることを決定するために、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**。

1214 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 の理解を応用すべきである。

1215 特に評価者は、機能仕様と TOE 要約仕様を考慮するべきである。これらの文書に記述されているすべてのセキュリティ機能は、それらの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。評価者は、補助として、ガイダンスとこれらの文書の間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省略はいずれも、不完全性を示す。

1216 ガイダンスが ST と一致していない、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。

1217 評価者は、AGD_ADM サブアクティビティからワークユニットの実行中に得られた結果がこの検査への有効な入力を提供することに注意するべきである。

AVA_MSU.1.3C

3:AVA_MSU.1-4 評価者は、意図する環境についてのすべての前提条件が明記されていることを決定するために、ガイダンスを**検査しなければならない**。

1218 評価者は、ST の意図する TOE セキュリティ環境についての前提条件を分析し、それらをガイダンスと比較して、管理者または利用者に関する ST の意図する TOE セキュリティ環境についてすべての前提条件がガイダンスに適切に記述されていることを保証する。

AVA_MSU.1.4C

3:AVA_MSU.1-5 評価者は、外部のセキュリティ手段に対するすべての要件が明記されていることを決定するために、ガイダンスを**検査しなければならない**。

1219 評価者は、ガイダンスを分析して、それがすべての外部の手続き的、物理的、人的及び接続管理を列挙していることを保証する。非 IT 環境に対する ST の中でセキュリティ対策方針は、何が必要とされるかを示す。

7.10.1.4.2 アクション AVA_MSU.1.2E

3:AVA_MSU.1-6 評価者は、提供されたガイダンスだけを使用して TOE を構成し、セキュアに使用できることを決定するために、TOE を構成し、設置するために必要なすべての管理者と利用者（適用される場合）手順を**実行しなければならない**。

1220 構成と設置では、評価者は、TOE を配付可能な状態から、運用可能であり、ST に特定されているセキュリティ対策方針に合わせて TSP を実施する状態に進める必要がある。

1221 評価者は、通常、TOE の消費者に提供される利用者と管理者のガイダンスにおいて証拠資料として提出された開発者の手順だけに従うべきである。それらのことを行うときに会う困難はいずれも、ガイダンスが不完全である、明確でない、一致していない、または不合理であることを示す。

1222 このワークユニットの条件を満たすために行われる作業は、評価者アクション ADO_IGS.1.2E の条件を満たすことにも貢献することに注意すること。

7.10.1.4.3 アクション AVA_MSU.1.3E

3:AVA_MSU.1-7 評価者は、消費者が TOE セキュリティ機能を効果的に管理、使用し、セキュアでない状態を検出するための十分なガイダンスが提供されていることを決定するために、ガイダンスを**検査しなければならない**。

1223 TOE は、各種の方法を使用して、消費者が効果的に TOE を安全に使用するのを支援する。ある TOE は、TOE が安全でない状態のときに消費者に警報を出す機能

(特性)を採用し、他の TOE には、高度なガイダンスが提供される。そのガイダンスには、既存のセキュリティ機能を最も効果的に使用するための示唆、ヒント、手順などが含まれている。例えば、安全でない状態を検出するための手助けとして監査機能を使用するためのガイダンス。

1224

このワークユニットの判定に到達するために、評価者は、TOE の機能、その目的と意図する環境、及び使用または利用者についての前提条件を考慮する。評価者は、TOE が安全でない状態に移行する場合、ガイダンスを使用することにより、安全でない状態をタイムリな方法で検出することができるとの合理的予測が存在するとの結論に達するべきである。TOE が安全でない状態に入る可能性は、ST、機能仕様及び TSF の上位レベル設計などの評価に提供されるものを使用して決定することができる。

7.10.2 TOE セキュリティ機能強度の評価 (AVA_SOF.1)

7.10.2.1 目的

1225 このサブアクティビティの目的は、SOF 主張がすべての確率的または順列的メカニズムに対して ST でなされているかどうか、及び ST でなされている開発者の SOF 主張が正しい分析によって裏付けられているかどうかを決定することである。

7.10.2.2 適用上の注釈

1226 SOF 分析は、パスワードメカニズムまたは生物的尺度 (バイオメトリックス) など、本来確率的または順列的メカニズムに対して行われる。暗号化メカニズムも本来確率的であり、強度の観点から多く記述されているが、AVA_SOF.1 は、暗号化メカニズムには適用されない。そのようなメカニズムには、評価者は、制度ガイダンスを探すべきである。

1227 SOF 分析は、個々のメカニズムに基づいて行われるが、SOF の全体的な決定は、機能に基づいて行われる。セキュリティ機能を提供するために複数の確率的または順列的メカニズムが採用される場合には、それぞれ個別のメカニズムを分析する必要がある。セキュリティ機能を提供するためにこれらのメカニズムを組み合わせる方法は、その機能の全体的な SOF レベルを決定する。評価者は、メカニズムが機能を提供するために一体となって動作する方法、及び ADV_HLD.1 の依存性によって与えられるそのような情報の最小レベルを理解するために設計情報を必要とする。評価者に提供される実際の設計情報は、EAL によって決定される。提供される情報は、必要なときに、評価者の分析を裏付けるために使用されるべきである。

1228 複数の TOE ドメインに関する SOF の説明については、4.4.6 節を参照のこと。

7.10.2.3 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) 機能仕様
- c) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) TOE セキュリティ機能強度の分析

7.10.2.4 評価者アクション

1230 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) AVA_SOF.1.1E

b) AVA_SOF.1.2E

7.10.2.4.1 アクション AVA_SOF.1.1E

AVA_SOF.1.1C

3:AVA_SOF.1-1 評価者は、ST に SOF レート付けで表されている SOF 主張に対応する各セキュリティメカニズムに対して開発者が SOF 分析を提供していることを**チェックしなければならない**。

1231 SOF 主張が SOF 数値尺度だけで表されている場合、このワークユニットは、適用されず、条件は満たされているものとみなされる。

1232 SOF レート付けは、攻撃能力として表される 1 つの SOF-基本、SOF-中位、SOF-高位として表される。CC パート 1 用語集を参照のこと。レート付けとして表された最小の全体的 SOF 要件は、すべての非暗号、確率的または順列的セキュリティメカニズムに適用される。ただし、個々のメカニズムは、全体的 SOF 要件を越えるレート付けとして表された SOF 主張を持つことができる。

1233 攻撃するために必要となる攻撃能力を決定するガイダンス、及びレート付けとして SOF を決定するガイダンスについては、附属書 B.8 を参照のこと。

1234 SOF 分析は、ST でなされた SOF 主張を正当化する根拠からなる。

AVA_SOF.1.2C

3:AVA_SOF.1-2 評価者は、ST に数値尺度で表されている SOF 主張に対応する各セキュリティメカニズムに対して開発者が SOF 分析を提供していることを**チェックしなければならない**。

1235 SOF 主張が SOF レート付けだけで表されている場合、このワークユニットは、適用されず、条件は満たされているものとみなされる。

1236 レート付けとして表された最小の全体的 SOF 要件は、すべての非暗号、確率的または順列的メカニズムに適用される。ただし、個々のメカニズムは、全体的 SOF 要件を満たすまたは要件を越える数値尺度として表された SOF 主張を持つことができる。

1237 SOF 分析は、ST でなされた SOF 主張を正当化する根拠からなる。

AVA_SOF.1.1C 及び AVA_SOF.1.2C

3:AVA_SOF.1-3 評価者は、分析を裏付ける主張または前提条件のいずれもが正当であることを決定するために、SOF 分析を**検査しなければならない**。

1238 例えば、擬似乱数ジェネレータの特定の実装が SOF 分析が関係するセキュリティメカニズムにシードする必要がある要求されるエントロピーを持っているというのは無効な前提条件である。

1239 ワーストケースが ST により無効にされない限り、SOF 分析を裏付ける前提条件には、この Worst Case を反映するべきである。多数の異なる可能なシナリオが存

在し、これらが人間利用者または攻撃者に依存する場合、すでに述べたように、このケースが無効にされない限り、最小の強度を表すケースが想定されるべきである。

- 1240 例えば、最大の論理的パスワードスペースに基づく強度の主張（すなわち、すべての印刷可能な ASCII 文字）は、自然言語パスワードを使用してパスワードスペース及び関係する強度を効果的に減らすのが人間のふるまいであるために、ワーストケースとはならない。ただし、自然言語パスワードの使用を最小にするパスワードフィルタなど、ST に識別されている IT 手段を TOE が使用する場合、そのような前提条件は、適切となる。
- 3:AVA_SOF.1-4 評価者は、分析を裏付けるアルゴリズム、原理、特性及び計算が正しいことを決定するために、SOF 分析を**検査しなければならない**。
- 1241 このワークユニットの本質は、考慮されているメカニズムのタイプに大きく依存する。附属書 B.8 は、パスワードメカニズムを使用して実装される識別と認証の機能の SOF 分析の例を示している。分析は、最大のパスワードスペースが最後に SOF レート付けに到達すると考える。生物的尺度に対して、分析は、メカニズムのスプーフィング（偽造）されやすさに影響を与える解決策とその他の要因を考慮すべきである。
- 1242 レート付けとして表される SOF は、セキュリティメカニズムを打ち負かすために必要となる最小の攻撃能力に基づく。SOF レート付けは、CC パート 1 用語集の攻撃能力に関して定義されている。
- 1243 攻撃能力のガイダンスについては、附属書 B.8 を参照のこと。
- 3:AVA_SOF.1-5 評価者は、各 SOF 主張が満たされているかまたは越えていることを決定するために、SOF 分析を**検査しなければならない**。
- 1244 SOF 主張のレート付けのガイダンスについては、附属書 B.8 を参照のこと。
- 3:AVA_SOF.1-6 評価者は、SOF 主張を持つすべての機能が ST に定義されている最小強度レベルを持つことを決定するために、SOF 分析を**検査しなければならない**。
- 7.10.2.4.2 アクション AVA_SOF.1.2E
- 3:AVA_SOF.1-7 評価者は、すべての確率的または順列的メカニズムが SOF 主張を持つことを決定するために、機能仕様、上位レベル設計、利用者ガイダンス及び管理者ガイダンスを**検査しなければならない**。
- 1245 確率的または順列的メカニズムによって実現されるセキュリティ機能の開発者による識別は、ST 評価中に検証される。ただし、TOE 要約仕様はその活動を行うために使用可能な唯一の証拠である場合、そのようなメカニズムの識別は不完全なことがある。このサブアクティビティへの入力として必要な追加の評価証拠は、ST にまだ識別されていない追加の確率的または順列的メカニズムを識別することができる。その場合、ST は、追加の SOF 主張を反映するために適切に更新する必要がある。また、開発者は、評価者アクション AVA_SOF.1.1E への入力としての主張を正当化する追加の分析を提供する必要がある。

3:AVA_SOF.1-8 評価者は、SOF 主張が正しいことを決定するために、その主張を **検査しなければならない。**

1246 SOF 分析に主張または前提条件（例えば、毎分可能な認証の試みの数）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に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。

7.10.3 脆弱性分析の評価 (AVA_VLA.1)

7.10.3.1 目的

1247 このサブアクティビティの目的は、TOE が、その意図する環境において、悪用される可能性のある明らかな脆弱性を持つかどうかを決定することである。

7.10.3.2 適用上の注釈

1248 このサブアクティビティでの用語「ガイダンス」(*guidance*)の使用は、利用者ガイダンス、管理者ガイダンス、セキュアな設置、生成及び立上げ手順を意味する。

1249 悪用される可能性のある脆弱性の考えは、ST のセキュリティ対策方針と機能要件によって決まる。例えば、セキュリティ機能がバイパスされるのを阻止するための手段が ST で必要とされない場合 (FPT_PHP, FPT_RVM と FPT_SEP が存在しない)、バイパスに基づく脆弱性は、考慮されるべきでない。

1250 脆弱性は、公知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 つの局面は、関係しているが、別のものである。脆弱性が公知になってい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。

1251 次の用語は、ガイダンスで特定の意味で使用される。

- a) 脆弱性 (*vulnerability*) – ある環境のセキュリティ方針を破るために使用されることがある TOE の弱点。
- b) 脆弱性分析 (*vulnerability analysis*) – TOE の脆弱性の系統的な探索、及び TOE の意図される環境へ関係を決定するための発見されたこれら脆弱性の評定。
- c) 明らかな脆弱性 (*obvious vulnerability*) – TOE、技術的精巧さ及び資源の最小の理解が必要となる、悪用される可能性のある脆弱性。
- d) 潜在的脆弱性 (*potential vulnerability*) – TOE において、(仮定される攻撃経路によって) 存在が疑われるが、確認のない脆弱性。
- e) 悪用可能脆弱性 (*exploitable vulnerability*) – TOE の意図する環境で悪用される可能のある脆弱性。
- f) 悪用不能脆弱性 (*non-exploitable vulnerability*) – TOE の意図する環境で悪用される可能性のない脆弱性。
- g) 残存脆弱性 (*residual vulnerability*) – TOE の意図する環境で予想される以上の攻撃能力を持つ攻撃者が悪用できない、悪用される可能性のない脆弱性。
- h) 侵入テスト (*penetration testing*) – TOE の意図する環境での識別された TOE の潜在的脆弱性の悪用される可能性を検査するために行われるテスト。

7.10.3.3 入力

1252 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順
- g) 脆弱性分析
- h) 機能強度の主張分析
- i) テストに適した TOE

1253 このサブアクティビティのその他の入力、次のとおりである。

- a) 明らかな脆弱性に関する現在の情報（監督者からの）

7.10.3.4 評価者アクション

1254 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) AVA_VLA.1.1E
- b) AVA_VLA.1.2E

7.10.3.4.1 アクション AVA_VLA.1.1E

AVA_VLA.1.1C

3:AVA_VLA.1-1 評価者は、明らかな脆弱性に対する探索がすべての該当する情報を考慮したことを決定するために、開発者の脆弱性分析を**検査しなければならない**。

1255 開発者の脆弱性分析は、少なくともすべての評価用提供物件と公知になっている情報源において、明らかな脆弱性に対する開発者の探索を扱うべきである。評価者は、評価用提供物件を独立脆弱性分析（AVA_VLA.1 で必要ない）のためではなく、開発者の明らかな脆弱性の探索を評価するための基礎として使用するべきである。

3:AVA_VLA.1-2 評価者は、明らかな各脆弱性が記述されていること及び TOE の意図する環境でそれが悪用されることがない理由に対する根拠が示されていることを決定するために、開発者の脆弱性分析を**検査しなければならない**。

1256 開発者が TOE 及び公知になっている情報源の知識に基づいて明らかな脆弱性を探索することが期待される。明らかな脆弱性だけを識別する必要がある場合、詳細な分析は、期待されない。開発者は、上記の定義に基づいてこの情報を選別し、明らかな脆弱性が意図する環境で悪用される可能性がないことを示す。

- 1257 評価者は、開発者の分析の次の 3 つの局面に関心を持つ必要がある。
- 開発者の分析がすべての評価用提供物件を考慮したかどうか
 - 意図する環境で明らかな脆弱性が悪用されないようにするための適切な手段が取られているかどうか
 - 明らかな脆弱性がいくつか識別されずに残っているかどうか
- 1258 評価者は、悪用される可能性がないことを決定するための基礎として開発者によって使用されない限り、識別された脆弱性が明らかであるかどうかに関心を持たされるべきでない。そのような場合、評価者は、識別された脆弱性に対する攻撃能力の低い攻撃者に対する抵抗力を決定することによってこの主張の正当性を確認する。
- 1259 *明らかな脆弱性の概念は、攻撃能力の概念に関係していない。後者は、独立脆弱性分析中に評価者によって決定される。このアクティビティは、AVA_VLA.1 に対して行われないうえに、通常、攻撃能力に基づく評価者による探索と選別は存在しない。ただし、それでも評価者は、評価の途中で潜在的な脆弱性を発見することがある。これらに対処する方法の決定は、明らかな脆弱性の定義と低い攻撃能力の概念を参照して行われる。*
- 1260 明らかな脆弱性のいくつかが識別されずに残っているかどうかの決定は、開発者の分析の正当性の評価、使用可能な公知になっている脆弱性情報との比較、その他の評価アクティビティの途中で評価者が識別したそれ以外の脆弱性との比較に制限される。
- 1261 脆弱性は、次の 1 つまたはいくつかの条件が存在する場合、悪用される可能性がないと呼ばれる。
- (IT または IT 以外の) 環境のセキュリティ機能または手段が意図する環境の脆弱性の悪用を阻止する。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 TOE の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。
 - 脆弱性は、悪用可能であるが、攻撃能力が中程度または高い攻撃者のみが悪用可能。例えば、セッションハイジャック攻撃への分散 TOE の脆弱性は、明らかな脆弱性を悪用するために必要となる、より以上の攻撃能力を必要とする。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。
 - 脅威に対抗すると主張されていないか、または違反可能な組織のセキュリティ方針が ST により達成されると主張されていない。例えば、ST が利用可能方針の主張を行わず、TCP SYN 攻撃（ホストが接続要求サービスを行えないようにする共通のインターネットプロトコルへの攻撃）を受けやすいファイアウォールは、この脆弱性だけでこの評価者のアクションに不合格とするべきでない。
- 1262 脆弱性を悪用するために必要な攻撃能力の決定のガイダンスについては、附属書 B.8 を参照のこと。

3:AVA_VLA.1-3 評価者は、開発者の脆弱性分析が ST 及びガイダンスと一貫していることを決定するために、その分析を**検査しなければならない**。

1263 開発者の脆弱性分析は、TOE 機能に対する特定の構成または設定を示して、脆弱性に対処することができる。そのような運用上の制約が効果的であり、ST と一貫していると思われる場合、消費者がそれらを採用できるように、すべてのそのような構成と設定がガイダンスに満たされるように記述されるべきである。

7.10.3.4.2 アクション AVA_VLA.1.2E

3:AVA_VLA.1-4 評価者は、開発者の脆弱性分析に基づいて、侵入テストを**考え出さなければならない**。

1264 評価者が侵入テストを準備するのは、次の場合である。

- a) 脆弱性が悪用されることがないとの理由に対する開発者の根拠が評価者の考えでは疑わしい場合、開発者の分析に対して反証することを試みる必要がある。
- b) TOE が、意図する環境で、開発者が考慮していない明らかな脆弱性を持つことを決定する必要がある。評価者は、開発者が考慮していない明らかな公知になっている脆弱性に関する、(例えば、監督者からの)現在の情報にアクセスを持つべきであり、また、その他の評価アクティビティの結果として識別された潜在的な脆弱性を持つことができる。

1265 評価者が明らかになっていない脆弱性(公知になっている脆弱性を含む)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まえに、テストを行う必要がある。評価の専門知識の結果として、評価者が明らかになっていない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。

1266 疑わしい明らかな脆弱性を理解し、評価者は、TOE の脆弱性をテストするための最も可能性の高い方法を決定する。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セキュリティ機能インターフェース
- b) テストに存在する必要がある初期条件(すなわち、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) セキュリティ機能を刺激するか、またはセキュリティ機能を観測するために必要となる特別のテスト装置(おそらく、明らかな脆弱性をテストするために特別の装置が必要になることはない)

1267 評価者は、おそらく、一連のテストケースを使用して侵入テストを行うのが有用であることを見つけ出し、この場合、各テストケースは、特定の明らかな脆弱性をテストする。

3:AVA_VLA.1-5 評価者は、開発者の脆弱性分析に基づき、テストを再現可能にするに十分な詳細さで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) テストする TOE の明らかな脆弱性の識別
- 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説明
- c) すべての侵入テスト前提初期条件を確立するための説明
- d) TSF を刺激するための説明
- e) TSF のふるまいを観察するための説明
- f) すべての期待される結果と、期待される結果に対応する観察されたふるまいについて実行されるべき必要な分析の記述
- 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説明

1268 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繰り返し、同等の結果を得ることができるようにすることである。

3:AVA_VLA.1-6 評価者は、開発者の脆弱性分析に基づいて、侵入テストを**実施しなければならない**。

1269 評価者は、TOE の侵入テストを行うための基礎として、ワークユニット 3:AVA_VLA.1-4 の結果の侵入テスト証拠資料を使用するが、これは、評価者が追加の特別の侵入テストを行うことを排除しない。必要に応じて、評価者は、評価者が行った場合に侵入テスト証拠資料に記録される、侵入テスト中に得られた情報の結果として特別のテストを考え出すことができる。そのようなテストは、期待されない結果または観察をどこまでも追求するか、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必要がある。

3:AVA_VLA.1-7 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**。

1270 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。相違には、いずれも正当性が示されるべきである。

3:AVA_VLA.1-8 評価者は、TOE が、意図する環境において、悪用される可能性のある明らかな脆弱性を持っていないことを決定するために、すべての侵入テストの結果とすべての脆弱性分析の結論を**検査しなければならない**。

1271 結果が、意図する環境で悪用される可能性のある明らかな脆弱性を TOE が持っていることを示す場合、評価者アクションの結果は、不合格判定となる。

3:AVA_VLA.1-9 評価者は、ETR に、テスト手法、構成、深さ及び結果を示しながら評価者の侵入テストの成果を**報告しなければならない**。

1272 ETR に報告される侵入テスト情報は、全体的な侵入テスト手法及びこのサブアクティビティから得られた成果を伝えることを評価者に許す。この情報を提供する意

図は、評価者の侵入テストの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、他の評価者と監督者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。

1273 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) テストされたセキュリティ機能侵入。侵入テストの焦点となったセキュリティ機能の簡単なリスト。
- 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。

1274 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侵入テストに関する、ETR に示すべきタイプの情報を提供することだけを意図している。

3:AVA_VLA.1-10 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採用された CEM アクティビティ、評価者に既知である、公開されたもので読んでいる、など）
- b) 影響のあるセキュリティ機能、達成されない対策方針、侵害される組織のセキュリティ方針及び顕在化される脅威
- c) 説明
- d) 意図する環境で悪用されるか否か（すなわち、悪用され得るか残存か）
- e) 脆弱性を識別した評価の関係者（例えば、開発者、評価者）の識別

8 章 EAL4 評価

8.1 序説

1275 EAL4 は、中レベルから高レベルの保証を提供する。セキュリティ機能は、セキュリティのふるまいを理解するための機能仕様、ガイダンス証拠資料、TOE の上位レベル設計及び下位レベル設計、実装のサブセットを使用して分析される。分析は、TOE セキュリティ機能のサブセットの独立テスト、機能仕様と上位レベル設計に基づく開発者テストの証拠、開発者テスト結果の選択的確認、機能強度の分析、開発者による脆弱性の探索の証拠、攻撃能力の低い侵入攻撃者に対する抵抗力を実証する独立脆弱性分析によって裏付けられる。さらに、保証は、TOE セキュリティ方針の非形式的モデルの使用と開発環境制御、自動化 TOE 構成管理の使用、セキュアな配付手続きの証拠を通して得られる。

8.2 目的

1276 この章の目的は、EAL4 評価を行うための最小の評価成果を定義し、評価を行うための方法と手段についてのガイダンスを提供することである。

8.3 EAL4 評価関係

1277 EAL4 評価は、次のことを扱う。

- a) 評価入力タスク (2 章)
- b) 次のもので構成される EAL4 評価アクティビティ
 - 1) ST の評価 (4 章)
 - 2) 構成管理の評価 (8.4 節)
 - 3) 配付及び運用文書の評価 (8.5 節)
 - 4) 開発文書の評価 (8.6 節)
 - 5) ガイダンス文書の評価 (8.7 節)
 - 6) ライフサイクルサポートの評価 (8.8 節)
 - 7) テストの評価 (8.9 節)
 - 8) テスト (8.9 節)
 - 9) 脆弱性評定の評価 (8.10 節)
- c) 評価出力タスク (2 章)

- 1278 評価アクティビティは、CC パート 3 に含まれている EAL4 保証要件から引き出される。
- 1279 ST が TOE 評価サブアクティビティを行うための基礎と状況を提供するために、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。
- 1280 EAL4 評価を構成するサブアクティビティは、この章に記述されている。サブアクティビティは、一般的に、多少とも同時に開始することができるが、評価者は、サブアクティビティの間のいくつかの依存性を考慮する必要がある。
- 1281 依存性のガイダンスについては、附属書 B.5 を参照のこと。

8.4 構成管理アクティビティ

1282 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が適切であることを保証することである。これには、どんな変更が追跡され、どのように起こり得る変更が具体化され、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。

1283 EAL4 での構成管理アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ACM_AUT.1

b) ACM_CAP.4

c) ACM_SCP.2

8.4.1 CM 自動化の評価 (ACM_AUT.1)

8.4.1.1 目的

1284 このサブアクティビティの目的は、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、実装表現に対する変更が自動化ツールのサポートにより制御されているかどうかを決定することである。

8.4.1.2 入力

1285 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) 構成管理証拠資料

8.4.1.3 評価者アクション

1286 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ACM_AUT.1.1E

b) ACM_AUT.1.1D に基づく暗黙の評価者アクション

8.4.1.3.1 アクション ACM_AUT.1.1E

ACM_AUT.1.1C

4:ACM_AUT.1-1 評価者は、TOE 実装表現へのアクセスを制御するための自動化手段の記述について CM 計画を **チェックしなければならない**。

4:ACM_AUT.1-2 評価者は、自動化アクセス制御手段が、TOE 実装表現への許可されない変更を阻止するのに有効であることを決定するために、そのアクセス制御手段を **検査しなければならない**。

1287 評価者は、構成管理証拠資料をレビューし、TOE 実装表現を変更することが許可されている個人または役割を識別する。例えば、ひとたび構成管理が行われると、実装表現のエLEMENTへのアクセスは、ソフトウェア統合役割を行う個人だけに許される。

1288 評価者は、許可されていない役割または利用者がそれらをバイパスすることができるかどうかを決定するために、自動化アクセス制御手段を実行するべきである。この決定には、いくつかの基本テストだけが必要となる。

ACM_AUT.1.2C

4:ACM_AUT.1-3 評価者は、実装表現から TOE の生成を支援する自動化手段について CM 証拠資料を**チェックしなければならない**。

1289 このワークユニットでは、用語「生成」(*generation*) は、TOE を実装から最終顧客に配付される状態に移るまで、開発者が採用するプロセスに適用される。

1290 評価者は、CM 証拠資料に自動化生成支援手順が存在することを検証するべきである。

4:ACM_AUT.1-4 評価者は、自動化生成手順が TOE の生成を支援するために使用できることを決定するために、その生成手順を**検査しなければならない**。

1291 評価者は、生成手順に従って TOE の実装表現を反映した TOE が生成されることを決定する。それにより、顧客は、設置のために配付される TOE のバージョンが ST に記述されている TSP を実装することを確信することができる。例えば、ソフトウェア TOE では、自動化生成手順が TSP を実施するために依存する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助けになるチェックが含まれる。

1292 この要件は、支援を提供するためだけのものであることに注意されるべきである。例えば、UNIX メークファイルを構成管理のもとに置く手法は、目的に十分に合致しているべきである。そのような場合、自動化は、TOE の正確な生成に十分に貢献する。自動化手順は、TOE の生成で使用する正しい構成要素を識別するのに役に立つ。

ACM_AUT.1.3C

4:ACM_AUT.1-5 評価者は、CM 計画が CM システムで使用される自動化ツールの情報を含んでいることを**チェックしなければならない**。

ACM_AUT.1.4C

4:ACM_AUT.1-6 評価者は、CM 計画に提供されている自動化ツールに関連する情報が、どのように自動化ツールが使用されるかを記述していることを決定するために、その情報を**検査しなければならない**。

1293 CM 計画に提供されている情報は、TOE の完全性を維持するために CM システムの利用者が自動化ツールを正しく操作するために必要な詳細を提供する。例えば、提供される情報には、次の記述を含めることができる。

EAL4:ACM_AUT.1

- a) ツールが提供する機能
- b) 実装表現への変更を制御するために開発者がこの機能を使用する方法
- c) TOE の生成を支援するために開発者がこの機能を使用する方法

8.4.1.3.2 暗黙の評価者アクション

ACM_AUT.1.1D

4:ACM_AUT.1-7 評価者は、CM 計画に記述されている自動化ツールと手順が使用されていることを決定するために、CM システムを **検査しなければならない**。

1294 このワークユニットは、ACM_CAP が要求する CM システムの使用に対する評価者の検査と並行して行われる追加のアクティビティとみなすことができる。評価者は、ツールと手順が使用されている証拠を探す。これには、ツールと手順の操作を実際に見るための開発サイトへの訪問と、それらの使用を通して作り出される証拠の検査を含めるべきである。

1295 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

8.4.2 CM 能力の評価 (ACM_CAP.4)

8.4.2.1 目的

1296 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、及びこれらの要素を変更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。

8.4.2.2 入力

1297 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

8.4.2.3 評価者アクション

1298 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ACM_CAP.4.1E

8.4.2.3.1 アクション ACM_CAP.4.1E

ACM_CAP.4.1C

4:ACM_CAP.4-1 評価者は、評価のために提供された TOE のバージョンが一意にリファレンスされていることを **チェックしなければならない**。

1299 評価者は、構成リストをチェックすることによりリファレンスの一意性の正当性を確認し、構成要素が一意に識別されていることを保証するために、開発者の CM システムを使用すべきである。その評価の間に 1 つだけのバージョンが検査されたならば、評価のために提供されたバージョンが一意にリファレンスされていることの証拠としては、不完全である。。そこで評価者は、一意のリファレンスをサポートできるリファレンスシステム（例えば、数字、文字または日付の使用）を探すべきである。それにもかかわらず、いかなるリファレンスも存在しない場合、通常、TOE が一意に識別できると評価者が確信しない限り、この要件に対する判定は不合格となる。

1300 評価者は、TOE の複数のバージョンを検査するようにし（例えば、脆弱性が発見された後のリワーク中に）、2 つのバージョンが別々にリファレンスされることをチェックすべきである。

ACM_CAP.4.2C

4:ACM_CAP.4-2 評価者は、評価のために提供された TOE がそのリファレンス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**。

1301 評価者は、TOE の異なるバージョンを区別することができる一意のリファレンスが 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。

1302 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、スタートアップルーチンの間に、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。

4:ACM_CAP.4-3 評価者は、使用されている TOE リファレンスが一貫していることを**チェックしなければならない**。

1303 もし、TOE に 2 度以上の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保有していることを確信できる。評価者は、提供された CM 証拠資料の一部である構成リストを使用して識別情報の一貫性のある使用を検証することができる。

1304 評価者は、TOE リファレンスが ST と一貫性があることも検証する。

1305 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ACM_CAP.4.3C

4:ACM_CAP.4-4 評価者は、提供された CM 証拠資料が構成リストを含んでいることを**チェックしなければならない**。

1306 構成リストは、構成制御(configuration control)のもとで維持されている要素を識別する。

4:ACM_CAP.4-5 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**。

4:ACM_CAP.4-6 評価者は、提供された CM 証拠資料が受入れ計画を含んでいることを**チェックしなければならない**。

ACM_CAP.4.4C

4:ACM_CAP.4-7 評価者は、構成リストが TOE を構成する構成要素を識別していることを決定するために、そのリストを**検査しなければならない**。

1307 構成リストに含まれるべき構成要素の最小範囲は、ACM_SCP によって与えられる。

ACM_CAP.4.5C

4:ACM_CAP.4-8 評価者は、構成要素の識別方法が、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**。

ACM_CAP.4.6C

4:ACM_CAP.4-9 評価者は、構成リストが各構成要素を一意に識別していることを**チェックしなければならない**。

1308 構成リストには、TOE を構成する構成要素のリストと、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。

ACM_CAP.4.7C

4:ACM_CAP.4-10 評価者は、CM 計画が、TOE 構成要素の完全性を維持するために 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**。

1309 CM 計画には、次の記述を含めることができる。

- a) 構成管理手続きに従う TOE 開発環境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、変更または削除）。
- b) 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タイプの構成要素（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）。
- c) 許可された個人だけが構成要素を変更できるように保証するために使用される手続き。
- d) 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。
- e) 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）、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拠または変更管理レコードに記録される。
- f) TOE バージョンのバージョン管理及び一意にリファレンスするための手法（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）。

ACM_CAP.4.8C

4:ACM_CAP.4-11 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**。

1310 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 ACM_CAP.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紙を含めることができる。

4:ACM_CAP.4-12 評価者は、CM システムが CM 計画の記述に従って使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**。

1311 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タイプの CM 関連操作（例えば、作成、変更、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。

1312 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

1313 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とのさらなる確信は、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認することができる。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べきである。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、それらに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。

1314 評価者がこのアクティビティを確認するために開発サイトを訪問することが予想される。

1315 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

ACM_CAP.4.9C

4:ACM_CAP.4-13 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**。

1316 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タイプの構成要素（例えば、上位レベル設計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詳細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べきである。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。

1317 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

ACM_CAP.4.10C

4:ACM_CAP.4-14 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**。

1318 評価者は、多数の方式を使用して 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、CM システム手続きにより生成され、ワークユニット 4:ACM_CAP.4-13 の一部としてすでに検査された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 システムのデモンストレーションに立ち会うこともできる。

1319 開発者は、CM システムの一部として自動化されたアクセス制御手段を提供することがある。その場合、それらが適していることは、コンポーネント ACM_AUT.1 のもとで検証することができる。

ACM_CAP.4.11C

4:ACM_CAP.4-15 評価者は、TOE の生成を支援する手順について CM 証拠資料を**チェックしなければならない**。

1320 このワークユニットでは、用語「生成」(*generation*) は、TOE を実装から最終顧客に配付するために受入れ可能な状態に移るまで、開発者が採用するプロセスに適用される。

1321 評価者は、CM 証拠資料に生成サポート手順が存在することを検証する。開発者が提供する生成サポート手順は、自動化することができる。その場合、それらの存在は、コンポーネント ACM_AUT.1.2C のもとで検証することができる。

4:ACM_CAP.4-16 評価者は、TOE 生成手順が TOE を生成するために正しい構成要素が使用されるように保証するのに助けるのに有効であることを決定するために、その生成手順を**検査しなければならない**。

1322 評価者は、生成サポート手順に従って、顧客が期待する TOE バージョン（すなわち、TOE ST に記述され、正しい構成要素からなる）が生成され、顧客のサイトに設置するために配付されることを決定する。例えば、ソフトウェア TOE では、手順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。

1323 評価者は、CM システムが TOE を生成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。。

ACM_CAP.4.12C

4:ACM_CAP.4-17 評価者は、受入れ手続きが、新たに作成されたまたは変更された構成要素に適用される受入れ基準を記述し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**。

- 1324 受入れ計画は、TOE の構成部分が TOE に組み込む前に適切な品質であることを保証するために使用される手続きを記述する。受入れ計画は、次のものに適用される受入れ手続きを識別すべきである。
- a) TOE の構成の各段階（例えば、モジュール、統合、システム）において
 - b) ソフトウェア、ファームウェア及びハードウェアのコンポーネントの受入れに対して
 - c) すでに評価されているコンポーネントの受入れに対して
- 1325 受入れ基準の記述には、次のものの識別を含めることができる。
- a) そのような構成要素の受入れに対する開発者の役割または個人の責任
 - b) 構成要素が受け入れられる前に適用される受入れ基準（例えば、成功した文書のレビュー、またはソフトウェア、ファームウェアまたはハードウェアの場合の成功したテスト）

8.4.3 CM 範囲の評価 (ACM_SCP.2)

8.4.3.1 目的

1326 このサブアクティビティの目的は、開発者が少なくとも、TOE 実装表現、設計、テスト、利用者及び管理者ガイダンス、CM 証拠資料、及びセキュリティ欠陥に対して構成管理を行うかどうかを決定することである。

8.4.3.2 入力

1327 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) 構成管理証拠資料

8.4.3.3 評価者アクション

1328 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

a) ACM_SCP.2.1E

8.4.3.3.1 アクション ACM_SCP.2.1E

ACM_SCP.2.1C

4:ACM_SCP.2-1 評価者は、構成リストに CM システムによって追跡される CC が必要とする要素の最小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**。

1329 リストには少なくとも次のものを含めること。

a) 保証の目標レベルを達成するために必要なすべての証拠資料

b) テストソフトウェア (適用される場合)

c) TOE 実装表現 (すなわち、TOE を構成するコンポーネントまたはサブシステム)。ソフトウェアのみの TOE では、実装表現は、ソースコードだけで構成することができる。ハードウェアプラットフォームが含まれる TOE では、実装表現は、ソフトウェア、ファームウェア、及びハードウェア (またはリファレンスプラットフォーム) 説明の組み合わせを意味することができる。

d) 実装に関する報告されたセキュリティ欠陥の詳細を記録するために使用された証拠資料 (例えば、開発者の問題報告データベースから引き出された問題ステータス報告書)。

ACM_SCP.2.2C

4:ACM_SCP.2-2 評価者は、手続きが、どのように各構成要素のステータスが TOE のライフサイクルを通して追跡されることができるかを記述していることを決定するために、CM 証拠資料を **検査しなければならない**。

- 1330 手続きは、CM 計画にまたは CM 証拠資料を通して詳細に記述することができる。含まれる情報には、次のもの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することができるように、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を割り付ける方法、及びそれらを CM システムに組み入れる方法。
 - c) 構成要素の置き換えられたバージョンを識別するために使用される方式。
 - d) TOE 開発及び保守ライフサイクルの各段階（すなわち、要件仕様、設計、ソースコード開発、オブジェクトコード生成から実行可能コードまで、モジュールテスト、実装及び運用）を通して構成要素を識別し、追跡するために使用される方式。
 - e) ある時点で構成要素の現在のステータスを割り付けるため及び開発フェーズ（すなわち、ソースコード開発、オブジェクトコード生成から実行可能コードまで、モジュールテスト及び証拠資料）での表現の各種のレベルを通して各構成要素を追跡するために使用される方法。
 - f) 開発ライフサイクルを通して構成要素に関係する欠陥を識別し、追跡するために使用される方法。
 - g) 1 つの構成要素が変更された場合、変更する必要がある他の構成要素を決定することができるように、構成要素の間の対応を識別するために使用される方法。
- 1331 この情報のいくつかに対する CM 証拠資料の分析は、ACM_CAP で詳細に記述されているワークユニットで満たされていることがある。

8.5 配付及び運用アクティビティ

1332 配付及び運用アクティビティの目的は、開発者が意図したのと同じ方法で TOE が設置され、生成され、開始され、変更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が適切であることを判断することである。これには、TOE の輸送中に取られる手続きと、初期化、生成、及び立上げの両方の手順が含まれる。

1333 EAL4 での配付及び運用アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) ADO_DEL.2

b) ADO_IGS.1

8.5.1 配付の評価 (ADO_DEL.2)

8.5.1.1 目的

1334 このサブアクティビティの目的は、配付証拠資料が、TOE を利用者サイトに配送するときに、TOE の完全性を維持し、変更または置換を検出するために使用されるすべての手続きを記述していることを決定することである。

8.5.1.2 入力

1335 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) 配付証拠資料

8.5.1.3 評価者アクション

1336 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ADO_DEL.2.1E

b) ADO_DEL.2.2D に基づく暗黙の評価者アクション

8.5.1.3.1 アクション ADO_DEL.2.1E

ADO_DEL.2.1C

4:ADO_DEL.2-1 評価者は、配付証拠資料が、TOE の版またはその一部を利用者サイトへ配送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**。

1337 用語「必要」(*necessary*)の解釈は、TOE の本質と ST に含まれている情報を考慮する必要がある。提供される保護レベルは、ST に識別されている前提条件、脅威、組織のセキュリティ方針、及びセキュリティ対策方針と一致しているべきである。場合によっては、これらは、配付に対して明示的に表されないことがある。評価者

は、均衡の取れたアプローチが取られ、配付が、その他の点でセキュアな開発プロセスでの明らかな弱点を表さないことを決定するべきである。

1338 配付手続きは、TOE の識別を決定し、TOE またはそのコンポーネント部分の輸送中の完全性を維持するための適切な手続きを記述する。手続きは、これらの手続きが扱う必要がある TOE の部分を記述する。それには、必要に応じて、物理的または電子的（例えば、インターネットからダウンロードするための）配送の手続きが含まれるべきである。配付手続きは、該当するソフトウェア、ハードウェア、ファームウェア及び証拠資料など、TOE 全体に関連する。

1339 完全性は、常に TOE の配付で懸念されるために、完全性を重視することは、驚くことではない。機密性と可用性が懸念される場合、それらも、このワークユニットで考慮されるべきである。

1340 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。

4:ADO_DEL.2-2 評価者は、配付手続きが選択された手続きとそれが扱う TOE の部分がセキュリティ対策方針を達成するのに適していることを決定するために、その配付手続きを**検査しなければならない**。

1341 配付手続きの選択の適合性には、特定の TOE（例えば、ソフトウェアかハードウェアか）及びセキュリティ対策方針が影響する。

1342 パッケージングと配付のための標準的な商業的方法が受け入れられる。これには、シ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。配送には、公共郵便または民間の配送サービスが受け入れられる。

ADO_DEL.2.2C

4:ADO_DEL.2-3 評価者は、配付証拠資料が、開発者のマスタコピーと利用者サイトで受け取った版の間の変更または不一致を検出するために、各種の手続きと技術的な手段を提供する方法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**。

1343 開発者は、チェックサム手順、ソフトウェア署名、改ざん防止シール(tamper proof seals)を使用することにより、改ざん(tampering)を検出することができる。開発者は、発信者の名前を登録し、その名前を受信者に提供するなど、その他の手続き（例えば、書留配達サービス）を採用することもできる。

1344 開発者のマスタコピーと利用者サイトで受け取った版との間の不一致を検出するための技術的な方法は、配付手続きに記述されるべきである。

ADO_DEL.2.3C

4:ADO_DEL.2-4 評価者は、配付証拠資料が、開発者が利用者サイトになにも送らない場合でも、各種のメカニズムと手続きが、なりすましを検出する方法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**。

1345 この要件は、TOE またはその一部を（例えば、開発者と利用者の両方が知っているまたは信頼しているエージェントによって）配付することによって満たすことができる。ソフトウェア TOE には、デジタル署名が適していることがある。

1346 TOE が電子的ダウンロードによって配付される場合、セキュリティは、デジタル署名、完全性チェックサム、または暗号化によって維持することができる。

8.5.1.3.2 暗黙の評価者アクション

ADO_DEL.2.2D

4:ADO_DEL.2-5 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**。

1347 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べきである。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送場所の訪問
- b) 配付のいくつかの段階、または利用者サイトでの 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ンネルを通して 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

1348 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

1349 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、将来の配付で使用される適切な手続きと施設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（dry run）」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、保証を提供する上で役に立つことがある。

8.5.2 設置、生成及び立上げの評価 (ADO_IGS.1)

8.5.2.1 目的

1350 このサブアクティビティの目的は、TOE のセキュアな設置、生成、及び立上げのための手順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。

8.5.2.2 入力

1351 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) 管理者ガイダンス
- b) セキュアな設置、生成、及び立上げの手順
- c) テストに適した TOE

8.5.2.3 適用上の注釈

1352 設置、生成及び立上げ手順は、それらが利用者サイトで行われるか、または ST の記述に従って TOE をセキュアな構成にするために必要となる開発サイトで行われるかに関係なく、すべての設置、生成、及び立上げの手順に関係している。

8.5.2.4 評価者アクション

1353 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADO_IGS.1.1E
- b) ADO_IGS.1.2E

8.5.2.4.1 アクション ADO_IGS.1.1E

ADO_IGS.1.1C

4:ADO_IGS.1-1 評価者は、TOE のセキュアな設置、生成及び立上げに必要な手順が提供されていることを **チェックしなければならない**。

1354 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合（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（または影響を受ける部分）は、適用されないために、満たされているものとみなされる。

8.5.2.4.2 アクション ADO_IGS.1.2E

4:ADO_IGS.1-2 評価者は、TOE のセキュアな設置、生成及び立上げに必要なステップを記述していることを決定するために、提供された設置、生成、及び立上げの手順を **検査しなければならない**。

- 1355 設置、生成及び立上げの手順が再度適用されるかまたは再度適用できることが予想されない場合（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（または影響を受ける部分）は、適用されないために、満たされているものとみなされる。
- 1356 設置、生成及び立上げの手順は、次のものに対する詳細な情報を提供することができる。
- a) TSF の制御のもとでのエンティティの設置の特定セキュリティ特性の変更
 - b) 例外及び問題の取扱い
 - c) 適切に、セキュアな設置のための最小限のシステム要件
- 1357 設置、生成及び立上げの手順の結果、セキュアな構成となることを確認するために、評価者は、開発者の手順に従って、提供されたガイダンス証拠資料だけを使用して、顧客が（TOE に適用される場合）TOE を設置、生成、及び立上げするために通常行うことが予想されるアクティビティを実行することができる。このワークユニットは、4:ATE_IND.2-2 ワークユニットとともに実行することができる。

8.6 開発アクティビティ

- 1358 開発アクティビティの目的は、TSF が TOE のセキュリティ機能を提供する方法を理解するための適合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（TOE の外部インタフェースを記述している）、上位レベル設計（TOE のアーキテクチャを内部サブシステムの観点から記述している）、及び下位レベル設計（TOE のアーキテクチャを内部モジュールの観点から記述している）からなる。さらに、実装記述（ソースコードレベルの記述）、セキュリティ方針モデル（TOE が実施するセキュリティ方針を記述している）、及び表現対応（一貫性を保証するために TOE の表現を相互にマッピングする）が存在する。
- 1359 EAL4 の開発アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。
- a) ADV_FSP.2
 - b) ADV_HLD.2
 - c) ADV_IMP.1
 - d) ADV_LLD.1
 - e) ADV_RCR.1
 - f) ADV_SPM.1

8.6.1 適用上の注釈

- 1360 設計証拠資料の CC 要件は、形式性によってレベル付けされている。CC は、文書の形式性の程度（すなわち、非形式的、準形式的または形式的のどれであるか）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。方法論は、使用すべき特定の言語を指示しない。その問題は、制度に任されている。次の段落は、各種の非形式的文書の内容を区別している。
- 1361 非形式的機能仕様は、セキュリティ機能の記述（TOE 要約仕様と同等のレベルでの）及び TSF への外部に見えるインタフェースの記述からなる。例えば、オペレーティングシステムが自己を識別する手段、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、記録する監査機能も含まれている場合には、これらの監査機能の記述も機能仕様に含まれることが期待される。これらの機能は、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、それらは、利用者の外部インタフェースでなにが起きるかによって影響される。
- 1362 非形式的上位レベル設計は、各サブシステムでそのインタフェースでの刺激に回答して起きる一連のアクションとして表される。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上位レベル設計記述は、取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取るアクションとして記述する。

- 1363 非形式的下位レベル設計は、モジュールでそのインタフェースでの刺激にตอบสนองして起きる一連のアクションとして表される。例えば、仮想プライベートネットワークサブシステムは、セッションキーを作成するモジュール、トラフィックを暗号化するモジュール、トラフィックの復号化するモジュール、トラフィックを暗号化する必要があるかどうかを決定するモジュールで構成することができる。暗号化モジュールの下位レベルの記述は、モジュールが暗号化するトラフィックストリームを受け取ったときに、モジュールが取るステップを記述する。
- 1364 機能仕様は、機能とサービスを記述するが、モデルは、それらの機能とサービスが実施する方針を記述する。非形式的モデルは、単に外部インタフェースで使用可能なサービスまたは機能が実施するセキュリティ方針の記述である。例えば、アクセス制御方針は、保護されている資源とアクセスが許可されるために満たされなければならない条件を記述する。監査方針は、TOE の監査可能な事象を記述し、管理者が選択可能な事象と常に監査される事象の両方を識別する。識別方針と認証方針は、利用者を識別する方法、それらの主張された識別を認証する方法、識別を認証する方法に影響する規則を記述する（例えば、企業のイントラネットの利用者は、認証を必要としないが、外部利用者は、ワンタイムパスワードによって認証される）。
- 1365 対応の実証の非形式は、散文形式である必要はない。簡単な 2 次元のマッピングで十分である。例えば、1 つの軸に沿ってモジュールが示され、他の軸に沿ってサブシステムが示され、セルがこれら 2 つの対応を識別するマトリックスは、上位レベル設計と下位レベル設計の間の適切な非形式的対応を提供することができる。

8.6.2 機能仕様の評価 (ADV_FSP.2)

8.6.2.1 目的

- 1366 このサブアクティビティの目的は、開発者が TOE のすべてのセキュリティ機能の適切な記述を提供しているかどうか及び TOE が提供するセキュリティ機能が ST のセキュリティ機能要件を十分に満たしているかどうかを決定することである。

8.6.2.2 入力

- 1367 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) 利用者ガイダンス
- d) 管理者ガイダンス

8.6.2.3 評価者アクション

1368 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ADV_FSP.2.1E

b) ADV_FSP.2.2E

8.6.2.3.1 アクション ADV_FSP.2.1E

ADV_FSP.2.1C

4:ADV_FSP.2-1 評価者は、機能仕様がすべての必要な非形式的説明文を含んで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**。

1369 機能仕様全体が非形式的である場合、このワークユニットは、適用されないために、満たされているものとみなされる。

1370 補助的な叙述的記述は、準非形式的または形式的記述だけでは理解するのが困難な機能仕様の部分に必要となる（例えば、形式的表記の意味を明確にするため）。

ADV_FSP.2.2C

4:ADV_FSP.2-2 評価者は、機能仕様が内部的に一貫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**。

1371 評価者は、TSFI を構成するインタフェースの記述が TSF の機能の記述と一貫していることを保証することにより、機能仕様の正当性を確認する。

1372 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ADV_FSP.2.3C

4:ADV_FSP.2-3 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべてを識別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**。

1373 用語「外部」(*external*) は、利用者に見えることを意味する。TOE への外部インタフェースは、TSF への直接インタフェースであるかまたは TOE の TSF 以外の部分へのインタフェースのいずれかである。ただし、これらの TSF 以外のインタフェースは、最終的に TSF にアクセスすることがある。TSF に直接または間接的にアクセスするこれらの外部インタフェースは、一体となって TOE セキュリティ機能インタフェース (TSFI) を構成する。図 8.1 は、TSF (陰影の付いた) 部分と TSF 以外 (空白) の部分を持つ TOE を示している。この TOE には、3 つの外部インタフェースがある。ここで、インタフェース *c* は、TSF への直接インタフェースである。インタフェース *b* は、TSF への間接インタフェースである。インタフェース *a* は、TOE の TSF 以外の部分へのインタフェースである。そこで、インタフェース *b* と *c* が TSFI を構成する。

1374 CC パート 2 (またはその拡張コンポーネント) の機能要件に反映されているすべてのセキュリティ機能は、ある種の外部から見える表示を持つことに注意される

べきである。これらすべてが必ずしもセキュリティ機能をテストすることができるインタフェースとは限らないが、それらは、すべて、ある程度まで外部から見えるものであり、したがって機能仕様に含まれる必要がある。

1375 TOE の境界を決定するガイダンスについては、附属書 B.6 を参照のこと。

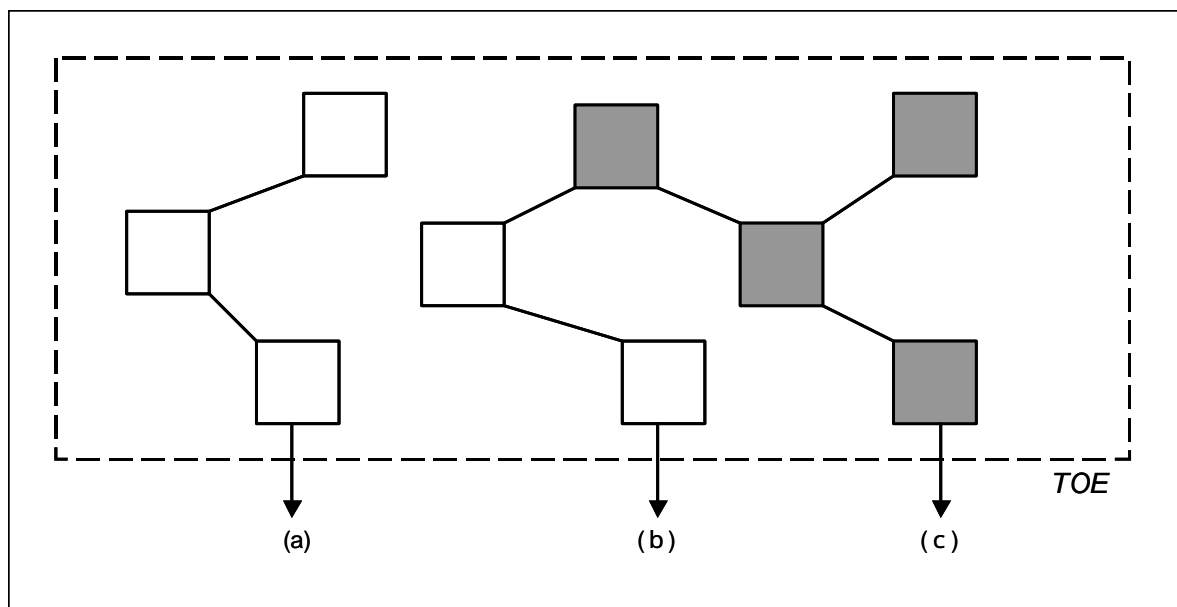


図 8.1 TSF インタフェース

4:ADV_FSP.2-4 評価者は、機能仕様が外部 TOE セキュリティ機能インタフェースのすべて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**。

1376 悪意のある利用者からの脅威のない TOE（すなわち、FPT_PHP、FPT_RVM 及び FPT_SEP が ST から正当に除外されている）では、機能仕様（そして他の TSF 表現記述に展開される）に記述されている唯一のインタフェースは、TSF との間のインタフェースである。FPT_PHP、FPT_RVM、及び FPT_SEP が存在しないことで、セキュリティ機能がバイパスされる心配がないことが想定されるので、他のインタフェースが TSF に与える影響についての心配がない。

1377 他方、悪意のある利用者またはバイパスの脅威がある TOE（すなわち、FPT_PHP、FPT_RVM、及び FPT_SEP が ST に含まれている）では、すべての外部インタフェースが機能仕様に記述されているが、それは、それぞれの影響が明らかになる程度に限られている。セキュリティ機能へのインタフェース（すなわち、図 8.1 のインタフェース *b* と *c*）は、完全に記述されているが、他のインタフェースは、そのインタフェースを介して TSF へアクセスできない（すなわち、インタフェースは、図 8.1 のタイプ *b* ではなく、タイプ *a*）ことを明確にする範囲でのみ記述されている。FPT_PHP、FPT_RVM、及び FPT_SEP が含まれていることは、すべてのインタフェースが TSF に影響するおそれがあることを暗示している。各外部インタフェースは、潜在的な TSF インタフェースなので、機能仕様には、インタフェースがセキュリティに適切であるかどうかを評価者が決定できるように十分詳細な各インタフェースの記述を含める必要がある。

- 1378 いくつかのアーキテクチャは、外部インタフェースのグループに対して十分詳細にこのインタフェース記述を容易に提示している。例えば、カーネルアーキテクチャでは、オペレーティングシステムへのすべてのコールがカーネルプログラムで取り扱われる。TSP を侵害するかもしれないコールは、そのようにする権限を持つプログラムによってコールされなければならない。権限とともに実行されるすべてのプログラムは、機能仕様に含める必要がある。権限なしに実行されるカーネルの外部のあらゆるプログラムは、TSP に影響を与えることはできず（すなわち、そのようなプログラムは、図 8.1 のタイプ *b* ではなく、タイプ *a* のインタフェースである）そこで、機能仕様から除外することができる。カーネルアーキテクチャが存在する場合、評価者のインタフェース記述の理解は促進されるが、そのようなアーキテクチャは必ずしも必要ない。
- 4:ADV_FSP.2-5 評価者は、TSFI の提示が、効果、例外及び誤りメッセージを記述している各外部インタフェースにおいて、TOE の完全なふるまいを適切に及び正しく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**。
- 1379 インタフェースの提示が適切であり、正しいことを評価するために、評価者は、機能仕様、ST の TOE 要約仕様、及び利用者と管理者ガイダンスを使用して、次の要因を評定する。
- a) すべてのセキュリティに関係する利用者入力パラメタ（またはそれらのパラメタの特性化）は識別されるべきである。完全であるために、直接利用者が制御しないパラメタも、それらを管理者が使用できる場合、識別されるべきである。
 - b) レビュー済みガイダンスに記述されている完全なセキュリティに関係するふるまいは、機能仕様の中で意味(semantics)の記述に反映させられるべきである。これには、事象及び各事象の影響としてのふるまいの識別を含めるべきである。例えば、オペレーティングシステムが、ファイルが要求時に開かれない各理由に対して異なる誤りコードを提供するような、機能の豊富なファイルシステムインタフェースを提供する場合、機能仕様は、要求に対してファイルが開かれたか、または要求が拒否されたかを、開く要求が拒否された理由（例えば、アクセス拒否、ファイルが存在しない、他の利用者がファイルを使用している、利用者は午後 5 時以降にファイルを開くことが許されていない）を列挙した説明があるべきである。機能仕様でファイルが要求によって開かれているか、または誤りコードが戻されていることを説明するだけでは不十分である。意味の記述には、セキュリティ要件がインタフェースに適用される方法（例えば、インタフェースの使用が監査可能な事象であるかどうか、そして可能な場合は記録可能な情報かどうか）を含めるべきである。
 - c) すべてのインタフェースは、操作のすべての可能なモードに対して記述される。TSF が権限の概念を提供する場合、インタフェースの記述は、権限がある場合とない場合のインタフェースのふるまいを説明するべきである。
 - d) セキュリティに関係するパラメタの記述、及びインタフェースのシンタックス(syntax)に含まれる情報は、すべての証拠資料にわたって一貫しているべきである。
- 1380 上記の検証は、機能仕様と ST の TOE 要約仕様及び開発者が提供する利用者及び管理者ガイダンスをレビューすることによって行われる。例えば、TOE がオペ

レーティングシステムとその下層のハードウェアである場合、評価者は、評価される TOE に適切であるとして、利用者アクセス可能プログラムの説明、プログラムのアクティビティを制御するために使用されるプロトコルの記述、プログラムのアクティビティを制御するために使用される利用者アクセス可能データベースの記述、及び利用者インタフェース（例えば、コマンド、アプリケーションプログラムインタフェース）を探す。評価者は、プロセッサ命令セットが記述されていることも保証する。

- 1381 評価者が、設計、ソースコード、または他の証拠を検査し、機能仕様から抜けて落ちているパラメタまたは誤りメッセージが含まれることを発見するまでは、機能仕様不完全であることを発見しないようなものであるため、このレビューは繰り返される。

ADV_FSP.2.4C

- 4:ADV_FSP.2.6 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**。

- 1382 TSF 提示が完全であることを評定するために、評価者は、ST の TOE 要約仕様、利用者ガイダンス、及び管理者ガイダンスを調べる。これらはいずれも、機能仕様の TSF 表現に含まれていないセキュリティ機能を記述するべきでない。

ADV_FSP.2.5C

- 4:ADV_FSP.2-7 評価者は、TSF が機能仕様によって完全に表現されていることを確信させる論証を、機能仕様が含ま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**。

- 1383 評価者は、機能仕様から抜け落ちている TSFI のインタフェースが存在しないことを確信させる論証が存在することを決定する。これには、すべての外部インタフェースがカバーされていることを保証するために開発者が使用した手順または方法論の記述を含めることができる。論証は、例えば、評価者が他の評価証拠の中で、コマンド、パラメタ、誤りメッセージ、または TSF へのその他のインタフェースを発見する、それにもかかわらず機能仕様に存在しない場合、不適切であると実証される。

8.6.2.0.1 アクション ADV_FSP.2.2E

- 4:ADV_FSP.2-8 評価者は、機能仕様 TOE セキュリティ機能要件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**。

- 1384 すべての ST セキュリティ機能要件が機能仕様によって扱われていることを保証するために、評価者は、TOE 要約仕様と機能仕様間のマッピングを作成することができる。そのようなマッピングは、対応 (ADV_RCR.*) 要件を満たしていることの証拠として開発者によってすでに提供されていることがある。その場合には、評価者は、このマッピングが完全であることを単に検証して、すべてのセキュリティ機能要件が機能仕様の適切な TSFI 表現にマッピングされていることを保証することだけが必要である。

- 4:ADV_FSP.2-9 評価者は、機能仕様 TOE 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、その仕様を **検査しなければならない**。

- 1385 特定の特性を備えたセキュリティ機能への各インタフェースに対して、機能仕様の詳細な情報は、ST に特定されているように正確でなければならない。例えば、ST にパスワードの長さが 8 文字でなければならないという利用者認証要件が含まれている場合、TOE は、8 文字のパスワードを持つ必要がある。機能仕様が 6 文字の固定長のパスワードを記述している場合、機能仕様は要件の正確な具体化ではない。
- 1386 制御された資源で動作する機能仕様の各インタフェースについて、評価者は、それがセキュリティ要件の 1 つを実施することによる可能な失敗を示す誤りコードを戻すかどうかを決定する。誤りコードが戻されない場合、評価者は、誤りコードを戻されるべきかどうかを決定する。例えば、オペレーティングシステムは、制御されたオブジェクトを「OPEN (開く)」ためにインタフェースを提示することができる。このインタフェースの記述には、アクセスがそのオブジェクトに許可されていないことを示す誤りコードを含めることができる。そのような誤りコードが存在しない場合、評価者は、それが適切であることを確認するべきである（おそらく、アクセスの仲介は、OPEN ではなく、READ と WRITE で行われるため）。

8.6.3 上位レベル設計の評価 (ADV_HLD.2)

8.6.3.1 目的

1387 このサブアクティビティの目的は、上位レベル設計が主要な構成ユニット（すなわち、サブシステム）の観点から TSF を記述しているかどうか、これらの構成ユニットへのインタフェースを記述しているかどうか、機能仕様の正しい具体化であるかどうかを決定することである。

8.6.3.2 入力

1388 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) 上位レベル設計

8.6.3.3 評価者アクション

1389 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_HLD.2.1E
- b) ADV_HLD.2.2E

8.6.3.3.1 アクション ADV_HLD.2.1E

ADV_HLD.2.1C

4:ADV_HLD.2-1 評価者は、上位レベル設計がすべての必要な非形式的説明文を含んでいることを決定するために、その設計を**検査しなければならない**。

1390 上位レベル設計全体が非形式的である場合、このワークユニットは、適用されないため、満たされているものとみなされる。

1391 準形式的または形式的記述だけでは理解が困難な上位レベル設計のこれらの部分には、補助的な説明的記述が必要となる（例えば、形式的表記の意味を明確にするために）。

ADV_HLD.2.2C

4:ADV_HLD.2-2 評価者は、上位レベル設計の表現が内部的に一貫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**。

1392 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

1393 評価者は、インタフェース仕様がサブシステムの目的の記述と一貫されていることを保証することにより、サブシステムインタフェース仕様の正当性を確認する。

ADV_HLD.2.3C

4:ADV_HLD.2-3 評価者は、TSF 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、上位レベル設計を**検査しなければならない**。

1394 上位レベル設計に関して、用語「サブシステム」(*subsystem*)は、大きな関連するユニット(メモリ管理、ファイル管理、プロセス管理など)を意味する。設計を基本的な機能領域に分解することは、設計を理解するのに役に立つ。

1395 上位レベル設計を検査する主な目的は、評価者の TOE の理解を助けることである。開発者によるサブシステム定義と各サブシステム内の TSF のグループ化の選択は、TOE の意図する動作を理解する上で上位レベル設計を役に立つものにする重要な局面である。このワークユニットの一部として、評価者は、開発者が提示するサブシステムの数が適切であるかどうか、及びサブシステム内の機能のグループ化の選択が適切であるかどうかを評定するべきである。評価者は、TSF のサブシステムへの分解が、TSF の機能がどのように提供されるかを上位レベルで理解するために評価者にとって十分であることを保証するべきである。

1396 上位レベル設計を記述するために使用されるサブシステムを「サブシステム」と呼ぶ必要はない。ただし、それは、同様の分解レベルを表しているべきである。例えば、設計は、「層」または「マネージャ」を使用して分解することもできる。

1397 サブシステム定義の選択と評価者の分析の間いくつかの相互作用が存在することがある。この相互作用については、次のワークユニット 4:ADV_HLD.2-10 で検討する。

ADV_HLD.2.4.C

4:ADV_HLD.2-4 評価者は、上位レベル設計が各サブシステムのセキュリティ機能を記述していることを決定するために、その設計を**検査しなければならない**。

1398 サブシステムのセキュリティ機能のふるまいは、サブシステムが何を行うかの記述である。これには、サブシステムがその機能を使用して実行するように指示されるアクションと、サブシステムが TOE のセキュリティ状態に与える影響(例えば、サブジェクト、オブジェクト、セキュリティデータベースの変更など)の記述を含めるべきである。

ADV_HLD.2.5C

4:ADV_HLD.2-5 評価者は、上位レベル設計が TSF で必要とされるすべてのハードウェア、ファームウェア、及びソフトウェアを識別していることを決定するために、その設計を**チェックしなければならない**。

1399 ST に IT 環境の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、適用されないために、満たされているものとみなされる。

1400 ST に IT 環境に対するセキュリティ要件のオプションステートメントが含まれている場合、評価者は、上位レベル設計に記述される TSF が必要とするハードウェア、ファームウェア、またはソフトウェアのリストと、IT 環境のセキュリティ要件のス

ステートメントを比較して、それらが一致することを決定する。ST の情報は、TOE が実行される下層の抽象マシンの特性を表す。

1401 上位レベル設計に ST に含まれていない IT 環境のセキュリティ要件が含まれている場合、またはそれらが ST に含まれているものと異なる場合、この不一致は、アクション ADV_HLD.2.2E のもとで評価者によって評定される。

4:ADV_HLD.2-6 評価者は、下層のハードウェア、ファームウェア、またはソフトウェアで実装されている補助的な保護メカニズムが提供する機能の提示を、上位レベル設計が含んでいることを決定するために、その設計を**検査しなければならない**。

1402 ST に IT 環境の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、適用されないために、満たされているものとみなされる。

1403 TOE が実行される下層抽象マシンが提供する機能の提示は、TSF の一部である機能の提示と同じ詳細レベルである必要はない。提示は、TOE セキュリティ対策方針をサポートするために TOE が依存する IT 環境のセキュリティ要件を実装するハードウェア、ファームウェア、またはソフトウェアに提供されている機能を TOE が使用する方法を説明するべきである。

1404 IT 環境のセキュリティ要件のステートメントは、ハードウェア、ファームウェア、またはソフトウェアの各種の異なる組み合わせにより満足することができる場合には特に、抽象的でもよい。テストアクティビティの一部として、評価者に IT 環境のセキュリティ要件を満たしていると主張されている下層マシンの少なくとも 1 つ以上の実例が提供される場合、評価者は、これが TOE の必要なセキュリティ機能を提供するかどうかを決定することができる。この評価者による決定には、下層マシンのテストまたは分析は必要ない。それによって提供されることが期待される機能が実際に存在することを決定するだけである。

ADV_HLD.2.6C

4:ADV_HLD.2-7 評価者は、上位レベル設計が TSF サブシステムへのインタフェースを識別していることを**チェックしなければならない**。

1405 上位レベル設計には、各サブシステムに対する、各入口点の名前が含まれている。

ADV_HLD.2.7C

4:ADV_HLD.2-8 評価者は、上位レベル設計が、外部から見える TSF のサブシステムに対するインタフェースを識別していることを**チェックしなければならない**。

1406 ワークユニット 4:ADV_FSP.2-3 で述べたように、外部インタフェース（すなわち、利用者に見えるインタフェース）は、直接または間接的に TSF にアクセスすることができる。TSF に直接または間接的にアクセスする外部インタフェースはいずれも、このワークユニットの識別に含まれる。TSF にアクセスしない外部インタフェースを含める必要はない。

ADV_HLD.2.8C

4:ADV_HLD.2-9 評価者は、上位レベル設計が、各サブシステムへのインタフェースを、それらの目的と使用方法の観点から記述し、そして効果、例外及び誤りメッセージの詳細を適切に提供していることを決定するために、その設計を**検査しなければならない**。

1407 上位レベル設計には、各サブシステムのすべてのインタフェースの目的と使用方法の記述を含めるべきである。そのような記述は、あるインタフェースには概括的に、また他のインタフェースにはさらに詳細に提供することができる。提供されるべき効果、例外及び誤りメッセージの詳細のレベルを決定するとき、評価者は、この分析の目的と TOE によるインタフェースの使用を考慮するべきである。例えば、評価者は、TOE の設計が適切である確信を確認するために、サブシステム間の相互作用の本質を理解する必要がある。この理解は、サブシステム間のいくつかのインタフェースの概括的な記述を理解するだけで得られる。特に、他のサブシステムによってコールされない内部サブシステム入力点は、通常、詳細な記述を必要としない。

1408 詳細のレベルは、ATE_DPT 要件を満たすために採用されたテスト手法にも依存する場合がある。例えば、必要となる詳細の量は、外部インタフェースだけを介してテストするテスト手法と、外部と内部の両方のサブシステムインタフェースを介してテストする手法では異なる。

1409 詳細な記述には、入力と出力のパラメタ、インタフェースの効果、生成される例外と誤りメッセージの詳細が含まれる。外部インタフェースの場合、必要な記述は、おそらく、機能仕様に含まれており、上位レベル設計では繰り返すことなく参照することができる。

ADV_HLD.2.9C

4:ADV_HLD.2-10 評価者は、上位レベル設計が TSP 実施サブシステムとそれ以外のサブシステムに分けて TOE を記述していることを**チェックしなければならない**。

1410 TSF は、TSP の実施に依存される必要がある TOE の部分のすべてからなる。TSF には、TSP を直接実施する機能と、TSP を直接実施しないが、間接的な方法で TSP の実施に貢献する機能の両方が含まれているために、すべての TSP 実施サブシステムは TSF に含まれている。TSP の実施に何の役割も果たさないサブシステムは、TSF の一部ではない。サブシステム全体は、その一部が TSF の一部である場合、TSF の一部となる。

1411 ワークユニット 4:ADV_HLD.2-3 で説明したように、開発者によるサブシステム定義及び各サブシステム内での TSF のグループ化の選択は、TOE の意図する運用を理解する上で上位レベル設計を役に立つものにする重要な局面である。ただし、TSP を直接的または間接的に実施するいずれかの機能を備えたサブシステムは、TSF の一部であるために、サブシステム内の TSF のグループ化の選択は TSF の範囲にも影響する。理解が容易であることを目標とすることも重要であるが、必要な分析の量を減らすために TSF の範囲を制限することも役に立つ。理解が容易であることと範囲を減らすことの 2 つの目標は、ときには相反することがある。評価者は、サブシステム定義の選択を評定するとき、このことを忘れないようにするべきである。

8.6.3.3.2 アクション ADV_HLD.2.2E

4:ADV_HLD.2-11 評価者は、上位レベル設計が TOE 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、その設計を**検査しなければならない**。

1412 評価者は、各 TOE セキュリティ機能の上位レベル設計を分析し、機能が正確に記述されていることを保証する。評価者は、機能が上位レベル設計に含まれていない依存性を持っていないことも保証する。

1413 評価者は、ST と上位レベル設計の両方で IT 環境のセキュリティ要件も分析し、それらが一致することを保証する。例えば、ST に監査証跡を格納するための TOE セキュリティ機能要件が含まれていて、さらに上位レベル設計では監査証跡の格納は、IT 環境によって行われると述べられている場合、上位レベル設計は、TOE セキュリティ機能要件の正確な具体化ではない。

1414 評価者は、インタフェース仕様がサブシステムの目的の記述と一貫していることを保証することにより、サブシステムインタフェース仕様の正当性を確認するべきである。

4:ADV_HLD.2-12 評価者は、上位レベル設計が TOE セキュリティ機能要件の完全な具体化であることを決定するために、その設計を**検査しなければならない**。

1415 すべての ST セキュリティ機能要件が上位レベル設計で扱われていることを保証するために、評価者は、TOE セキュリティ機能要件と上位レベル設計の間のマッピングを作成することができる。

8.6.4 実装表現の評価 (ADV_IMP.1)

8.6.4.1 目的

1416 このサブアクティビティの目的は、実装表現が ST の機能要件を十分に満たしているかどうか及び下位レベル設計の正しい具体化であるかどうかを決定することである。

8.6.4.2 入力

1417 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) 下位レベル設計
- c) 実装表現のサブセット

8.6.4.3 評価者アクション

1418 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_IMP.1.1E
- b) ADV_IMP.1.2E

8.6.4.3.1 アクション ADV_IMP.1.1E

ADV_IMP.1.1C

4: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行うことなく、TSF を生成することができる詳細レベルまで TSF を曖昧さなく定義していることを決定するために、その実装表現を **検査しなければならない**。

1419 このワークユニットでは、評価者は、実装表現が分析に適していることを確認する必要がある。評価者は、提供された表現から TSF を生成するために必要なプロセスを考慮すべきである。プロセスが完全に定義されているときに、それ以上の設計上の決定（例えば、ソースコードのコンパイルのみが要求するのか、またはハードウェアの図面からハードウェアの組み立てるをするのか）を必要としない場合、実装表現は、適切であるということができる。

1420 使用するいずれのプログラミング言語も、オブジェクトコードを生成するために使用されるコンパイラオプションとともに、すべてのステートメントの曖昧でない定義により十分に定義されている必要がある。この決定は、ALC_TAT.1 サブアクティビティの一部として行われている。

4:ADV_IMP.1-2 評価者は、実装表現が十分に代表的であることを決定するために、開発者が提供するその実装表現を **検査しなければならない**。

- 1421 開発者は、TSF のサブセットについてのみ実装表現を提供することを要求される。PP または ST が選択されたサブセットを特定している場合、特定されたサブセットも開発者に要求される。開発者は、初期サブセットを選択して提供することができるが、評価者は、追加の部分または別のサブセットを要求することができる。
- 1422 評価者は、サンプリングの原則を適用することにより、サブセットが妥当であり、適切であることを決定する。
- 1423 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 1424 サブセットが適切であることを決定するとき、評価者は、それが TSF メカニズムの実装が正しいことを理解し、保証を得るのを助けるために使用するのに適していることを決定する。この決定を行うとき、評価者は、代表的なサブセットが選択されていることに評価者が満足するように、開発者が使用した表現の別の方式を考慮するべきである。
- 1425 例えば、従来のオペレーティングシステムの方法で実現されている TOE の場合、ソースコードの選択されたサブセットには、例えばコマンドやアプリケーションプログラムなどのカーネルの外部からのサンプルと同様に、カーネルまたは核からのサンプルも含まれているべきである。ソースコードいくつかが別の開発組織によって作成されたことが判明している場合には、選択されたサブセットには、それぞれの異なる作成組織からの例を含めるべきである。実装表現ソースコードに、異なる表現形式のプログラミング言語が含まれている場合、サブセットには、それぞれの異なる言語の例を含めるべきである。
- 1426 実装表現にハードウェア図面が含まれている場合、TOE のいくつかの異なる部分がサブセットに含められているべきである。例えば、デスクトップコンピュータが含まれる TOE では、選択されたサブセットには、メインのコンピュータボードと同様に周辺機器コントローラの例を含めるべきである。
- 1427 サブセットの決定に影響するその他の要因には、次のものがある。
- a) 設計の複雑性（設計の複雑性が TOE の間で異なる場合、サブセットには、複雑性の高い部分をいくつか含めるべきである）
 - b) 制度要件
 - c) TOE の一部に設計上の曖昧さがある可能性を指摘した他の設計分析サブアクティビティ（下位レベル設計または上位レベル設計に関連するワークユニットのような）の結果
 - d) 評価者の独立脆弱性分析（サブアクティビティ AVA_VLA.2）に役に立つ実装表現の部分に関する評価者の判断

ADV_IMP.1.2C

- 4:ADV_IMP.1-3 評価者は、実装表現が内部的に一貫していることを決定するために、その実装表現を**検査しなければならない**。

1428 開発者は実装表現のサブセットだけを提供することを要求されるために、このワークユニットは、評価者が提供されたサブセットだけの一貫性を決定することを要求する。評価者は、実装表現の一部を比較することにより、不一致を探す。例えば、ソースコードの場合、ソースコードのある部分に他の部分のサブプログラムへのコールが含まれている場合、評価者は、コールするプログラムの引数がコールされたプログラムの引数の処理と一致していることを調べる。ハードウェア図面の場合、評価者は同様の事項を、回路図の両端の性質と特性の一致（例えば、電圧レベル、ロジックの方向、信号タイミング要件）として探す。一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

8.6.4.3.2 アクション ADV_IMP.1.2E

4:ADV_IMP.1-4 評価者は、実装表現のサブセットが、サブセットに関連するそれらの TOE セキュリティ機能要件を正確に具体化していることを決定するために、そのサブセットを**検査しなければならない**。

1429 セキュリティ機能を直接提供する実装表現の部分に対して、評価者は、実装が TOE セキュリティ機能要件を満たしていることを決定する。実装表現のサブセットの残りの部分は、いくつかの TOE 機能要件をサポートすることができる。これらの残りの部分についての決定を行うとき、評価者は、下位レベル設計を使用して、実装表現のサブセットが、下位レベル設計に記述されている他の部分との組み合わせにおいて、一体となって機能し、TOE セキュリティ機能要件を具体化するかどうかを評定する。

1430 実装表現のサブセットの残りの部分は、存在する場合、実装サブセットがサポートする TOE セキュリティ機能要件のいずれにも関係していないために、通常、無視することができる。ただし、評価者は、どれだけ離れていても、TOE セキュリティ機能のサポートで間接的な役割を果たす部分を見落とすことがないように注意すべきである。例えば、代表的なオペレーティングシステムにおいて、核（またはカーネル）の部分のソースコードは、TOE セキュリティ機能をサポートする上で直接的な役割を果たさないが、直接の役割を持つ核の部分の正しい機能に干渉することがある。提供された実装表現のサブセットにそのような部分が存在することが発見された場合には、ST がそのような非干渉を要求することを提示し、それらがセキュリティ機能に直接の役割を持つ部分に干渉しないことを評定すべきである。この評定は、通常、TOE セキュリティ機能のサポートで直接的な役割を果たす実装表現の部分に要求される詳細検査と同様のレベルを必要としない。

8.6.5 下位レベル設計の評価 (ADV_LLD.1)

8.6.5.1 目的

1431 このサブアクティビティの目的は、下位レベル設計が ST の機能要件を十分に満たしているかどうか、及び上位レベル設計の正しい有効な詳細化であるかどうかを決定することである。

8.6.5.2 入力

1432 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) 上位レベル設計
- d) 下位レベル設計

8.6.5.3 評価者アクション

1433 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_LLD.1.1E
- b) ADV_LLD.1.2E

8.6.5.3.1 アクション ADV_LLD.1.1E

ADV_LLD.1.C

4:ADV_LLD.1-1 評価者は、下位レベル設計がすべての必要な非形式的説明文を含んでいることを決定するために、その設計を**検査しなければならない**。

1434 下位レベル設計全体が非形式的である場合、このワークユニットは、適用されないため、満たされているものとみなされる。

1435 補助的な説明的記述は、準形式的または形式的記述（例えば、形式的表記の意味を明確にするための）からだけでは理解するのが困難である下位レベル設計の部分に必要である。

ADV_LLD.1.2C

4:ADV_LLD.1-2 評価者は、下位レベル設計の提示が内部的に一貫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**。

1436 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ADV_LLD.1.3C

4:ADV_LLD.1-3 評価者は、下位レベル設計が TSF をモジュールの観点から記述していることを決定するために、その設計を**チェックしなければならない**。

1437 用語「モジュール」(*module*)は、このファミリでサブシステムほど抽象的でないエンティティを指定するために CC により使用されている。これは、モジュールの目的だけでなく、モジュールが目的を達成する方法についてのさらに詳細な情報が含まれていることを意味する。理想的には、下位レベル設計は、そこに記述されているモジュールを実装するために必要な情報のすべてを提供する。このサブアクティビティの後のワークユニットは、十分な詳細レベルが含まれていることを決定するために、詳細な分析を要求する。このワークユニットに対しては、各モジュールが明確に、曖昧さなく識別されていることを評価者が検証することで十分である。

ADV_LLD.1.4C

4:ADV_LLD.1-4 評価者は、下位レベル設計が各モジュールの目的を記述していることを決定するために、その設計を**検査しなければならない**。

1438 下位レベル設計には、各モジュールの目的の記述が含まれている。これらの記述は、モジュールが実行することが期待される機能が何かを伝えるために十分明確にされるべきである。記述は、モジュールの目的の概要を示すべきであり、モジュールインタフェース仕様の詳細なレベルであることを意図しない。

ADV_LLD.1.5C

4:ADV_LLD.1-5 評価者は、下位レベル設計がモジュール間の相互関係を、提供されたセキュリティ機能と他のモジュールへの依存性の観点から定義していることを決定するために、その設計を**検査しなければならない**。

1439 この分析に対して、モジュールは、次の 2 つの方法で相互作用するとみなされる。

- a) 相互にサービスを提供する
- b) セキュリティ機能のサポートで協力する

1440 下位レベル設計には、これらの相互関係の特定の情報を含めるべきである。例えば、あるモジュールが他のモジュールの計算結果に依存する計算を行う場合、これらの他のモジュールはリストアップされるべきである。さらに、あるモジュールがセキュリティ機能のサポートで使用するサービスを他のモジュールに提供する場合、このサービスが記述されるべきである。モジュールの目的の記述は、前のワークユニットで分析されており、この情報を提供するのに十分である。

ADV_LLD.1.6C

4:ADV_LLD.1-6 評価者は、各 TSP 実施機能がどのように提供されるかを、下位レベル設計が記述していることを決定するために、その設計を**検査しなければならない**。

1441 TSP 実施機能は、直接または間接的に TSP を実施する TSF の機能である。

1442 下位レベル設計が十分に詳細化されおり、実装の作成が可能であるかどうかを評定するときに重要なのが下位レベル設計のこの記述である。評価者は、実装者の観点

からこの記述を分析するべきである。評価者にとって、実装者の観点から、モジュールを実装する方法の側面が明確でない場合、記述は不完全である。モジュールが分離したユニット（プログラム、サブプログラム、またはハードウェアコンポーネント）として実装されるべきであるという要件はないことに注意すること。ただし、下位レベル設計は、そのような実装が可能となるように十分詳細化することができる。

ADV_LLD.1.7C

4:ADV_LLD.1-7 評価者は、下位レベル設計が TSF モジュールへのインタフェースを識別していることを**チェックしなければならない**。

1443 下位レベル設計には、各モジュールに対して、モジュールの入口点の名前を含めるべきである。

ADV_LLD.1.8C

4:ADV_LLD.1-8 評価者は、下位レベル設計が、外部から見える TSF のモジュールに対するインタフェースを識別していることを**チェックしなければならない**。

1444 ワークユニット 4:ADV_FSP.2-3 で述べたように、外部インタフェース（すなわち、利用者に見えるインタフェース）は、直接または間接的に TSF にアクセスすることができる。TSF に直接または間接的にアクセスする外部インタフェースはいずれも、このワークユニットの識別に含まれる。TSF にアクセスしない外部インタフェースを含める必要はない。

ADV_LLD.1.9C

4:ADV_LLD.1-9 評価者は、下位レベル設計が、各モジュールへのインタフェースを、それらの目的と使用方法の観点から記述し、そして効果、例外及び誤りメッセージの詳細を適切に提供していることを決定するために、その設計を**検査しなければならない**。

1445 モジュールインタフェースの記述は、あるインタフェースには概括的に、他のインタフェースにはさらに詳細に行われる。効果、例外及び誤りメッセージの必要な詳細レベルを決定するとき、評価者は、この分析の目的と TOE によるインタフェースの使用を考慮するべきである。例えば、評価者は、モジュール間の相互作用の概括的本質を理解し、TOE 設計が適切である確信を確証する必要がある。この理解は、モジュール間のいくつかのインタフェースの概括的な記述を理解するだけで得られる。特に、他のモジュールからコールされない内部入口点は、通常、詳細な記述を必要としない。

1446 このワークユニットは、AVA_VLA サブアクティビティの一部である評価者の独立脆弱性分析とともに行うことができる。

1447 詳細な記述には、入力と出力のパラメタ、インタフェースの効果、生成される例外と誤りメッセージの詳細が含まれる。外部インタフェースの場合、必要な記述は、おそらく、機能仕様に含まれており、上位レベル設計では繰り返すことなく参照することができる。

ADV_LLD.1.10C

4:ADV_LLD.1-10 評価者は、下位レベル設計が TSP 実施モジュールとそれ以外のモジュールに分けて TOE を記述していることを **チェックしなければならない**。

1448 TSF は、TSP の実施に依存される必要がある TOE の部分のすべてからなる。TSF には、TSP を直接実施する機能と、TSP を直接実施しないが、より間接的な方法で TSP の実施に貢献する機能の両方が含まれているために、すべての TSP 実施モジュールは TSF に含まれる。TSP の実施に影響を与えることができないモジュールは、TSF の一部ではない。

8.6.5.3.2 アクション ADV_LLD.1.2E

4:ADV_LLD.1-11 評価者は、下位レベル設計が TOE 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、その設計を **検査しなければならない**。

1449 評価者は、次のことを保証することにより、モジュールインタフェース仕様の正当性を確認する。

- a) インタフェース仕様がモジュールの目的の記述と一貫している。
- b) インタフェース仕様が他のモジュールによるそれらの使用と一貫している。
- c) 各々の TSP 実施機能が正しくサポートされるために必要なモジュール間の相互関係が正しく記述されている。

4:ADV_LLD.1-12 評価者は、下位レベル設計が TOE セキュリティ機能要件の完全な具体化であることを決定するために、その設計を **検査しなければならない**。

1450 評価者は、すべての ST 機能要件が下位レベル設計の適切なセクションにマッピングされていることを保証する。この決定は、ADV_RCR.1 サブアクティビティとともに行われるべきである。

1451 評価者は、下位レベル設計を分析し、TOE の各セキュリティ機能がモジュール仕様によって完全に記述されていること、及び下位レベル設計に指定されていないモジュールに TOE セキュリティ機能が依存しているモジュールが存在しないことを決定する。

8.6.6 表現対応の評価 (ADV_RCR.1)

8.6.6.1 目的

1452 このサブアクティビティの目的は、開発者が ST、機能仕様、上位レベル設計及び下位レベル設計の要件を実装表現において、正しく完全に実施しているかどうかを決定することである。

8.6.6.2 入力

1453 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) 上位レベル設計
- d) 下位レベル設計
- e) 実装表現のサブセット
- f) TOE 要約仕様と機能仕様の間に対応分析
- g) 機能仕様と上位レベル設計の間に対応分析
- h) 上位レベル設計と下位レベル設計の間に対応分析
- i) 下位レベル設計と実装表現のサブセットの間に対応分析

8.6.6.3 評価者アクション

1454 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_RCR.1.1E

8.6.6.3.1 アクション ADV_RCR.1.1E

4:ADV_RCR.1-1 評価者は、機能仕様が TOE セキュリティ機能の正しい、完全な表現であることを決定するために、TOE 要約仕様と機能仕様の間に対応分析を **検査しなければならない**。

1455 評価者のこのワークユニットの目標は、TOE 要約仕様に識別されているすべてのセキュリティ機能が機能仕様に表現されていること及びそれらが正確に表現されていることを決定することである。

1456 評価者は、TOE 要約仕様の TOE セキュリティ機能と機能仕様の間に対応をレビューする。評価者は、対応が一貫し、正確であることを検査する。対応分析が TOE 要約仕様のセキュリティ仕様と機能仕様のインタフェース記述の間関係を示しているところでは、評価者は、両方のセキュリティ機能が同じであることを検

証する。TOE 要約仕様のセキュリティ機能が、対応するインタフェースにおいて正しく、完全に表されている場合、このワークユニットは、満たされる。

1457 このワークユニットは、ワークユニット 4:ADV_FSP.2-8 及び 4:ADV_FSP.2-9 とともに行うことができる。

4:ADV_RCR.1-2 評価者は、上位レベル設計が機能仕様の正しい、完全な表現であることを決定するために、機能仕様と上位レベル設計の間の対応分析を**検査しなければならない**。

1458 評価者は、対応分析、機能仕様、及び上位レベル設計を使用して、機能仕様に識別されている各セキュリティ機能を上位レベル設計に記述されている TSF サブシステムにマッピングできることを保証する。各セキュリティ機能に対して、対応は、どの TSF サブシステムがその機能のサポートにかかわるかを示す。評価者は、上位レベル設計に各セキュリティ機能の正しい実現の記述が含まれていることを検証する。

4:ADV_RCR.1-3 評価者は、下位レベル設計が上位レベル設計の正しい、完全な表現であることを決定するために、上位レベル設計と下位レベル設計の間の対応分析を**検査しなければならない**。

1459 評価者は、対応分析、上位レベル設計、及び下位レベル設計を使用して、下位レベル設計に識別されている各 TSF モジュールを上位レベル設計に記述されている TSF サブシステムにマッピングできることを保証する。各 TOE セキュリティ機能に対しては、対応は、どの TSF モジュールがその機能のサポートにかかわるかを示す。評価者は、下位レベル設計に各セキュリティ機能の正しい実現の記述が含まれていることを検証する。

4:ADV_RCR.1-4 評価者は、実装表現のサブセットが、実装表現に詳細化されている下位レベル設計の一部の正しい、完全な表現であることを決定するために、下位レベル設計とそのサブセットの間の対応分析を**検査しなければならない**。

1460 評価者は、実装表現のサブセットだけを検査するので、このワークユニットは、各 TOE セキュリティ機能を実装表現まで追跡するのではなく、実装表現のサブセットと下位レベル設計の該当する部分への対応分析を評定することによって実施される。このサブセットは、いくつかの機能を取り扱わない場合がある。

8.6.7 セキュリティ方針モデリングの評価 (ADV_SPM.1)

8.6.7.1 目的

1461 このサブアクティビティの目的は、セキュリティ方針モデルがセキュリティ方針の規則と特性を明確にまた一貫して記述しているかどうか、及びこの記述が機能仕様のセキュリティ機能の記述と一致しているかどうかを決定することである。

8.6.7.2 入力

1462 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 セキュリティ方針モデル
- d) 利用者ガイダンス
- e) 管理者ガイダンス

8.6.7.3 評価者アクション

1463 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ADV_SPM.1.1E

8.6.7.3.1 アクション ADV_SPM.1.1E

ADV_SPM.1.1C

4:ADV_SPM.1-1 評価者は、セキュリティ方針モデルがすべての必要な非形式的説明文を含んでいることを決定するために、そのセキュリティ方針モデルを**検査しなければならない**。

1464 セキュリティ方針モデル全体が非形式的である場合、このワークユニットは、適用されず、満たされているものとみなされる。

1465 補助的な叙述的記述が、準形式的または形式的記述だけでは理解が困難なセキュリティ方針モデルの部分に対して必要である（例えば、形式的表記の意味を明確にするために）。

ADV_SPM.1.2C

4:ADV_SPM.1-2 評価者は、ST に明示的に含まれているすべてのセキュリティ方針がモデル化されていることを決定するために、セキュリティ方針モデルを**チェックしなければならない**。

1466 セキュリティ方針は、ST の機能セキュリティ要件の集合によって表される。そこで、セキュリティ方針の本質（それゆえ、モデル化する必要がある方針）を決定す

るために、評価者は、明示的に要求されているそれらの方針に対する ST 機能要件を分析する (ST に含まれている場合、FDP_ACC と FDP_IFC により)。

- 1467 TOE により、形式的/準形式的モデル化は、アクセス制御に対して不可能なことがある。(例えば、インターネットに接続されたファイアウォールに対するアクセス制御方針は、インターネットの状態を完全に定義することができないために、有用な方法で形式的にモデル化することはできない)。形式的または準形式的モデルが可能でないセキュリティ方針には、方針は、非形式的な形式で提供されなければならない。
- 1468 ST に明示的な方針が含まれていない場合 (FDP_ACC と FDP_IFC のいずれも ST に含まれていないために)、このワークユニットは、適用されず、満たされているものとみなされる。
- 4:ADV_SPM.1-3 評価者は、ST で主張されているセキュリティ機能要件が示すすべてのセキュリティ方針がモデル化されていることを決定するために、セキュリティ方針モデルを**検査しなければならない**。
- 1469 明示的に示されている方針 (ワークユニット 4:ADV_SPM.1-2 を参照) に加えて、評価者は、その他の機能セキュリティ要件クラスによって暗示される方針に対する ST 機能要件を分析する。例えば、(FDP_ACC と FDP_IFC ではなく) FDP 要件を含める場合、実施されているデータ保護方針の記述が必要になる。FIA 要件を含める場合、識別と認証の方針の記述をセキュリティ方針モデルに含める必要がある。FAU 要件を含める場合、監査方針の記述が必要となる。その他の機能要件ファミリは、一般的に**セキュリティ方針 (security policies)**と呼ばれるものと関係付けられないが、それにもかかわらず、それらは、セキュリティ方針モデルに含める必要があるセキュリティ方針 (例えば、否認不可、リファレンス仲介、プライバシー) を実施する。
- 1470 セキュリティ方針モデル提示が非形式的である場合、すべてのセキュリティ方針は、モデル化 (すなわち、記述) が可能であり、それらを含める必要がある。形式的または準形式的セキュリティ方針モデルが可能でない場合、方針は、非形式的な形式で提供する必要がある。
- 1471 ST にそのような暗示的な方針が含まれていない場合、このワークユニットは適用されず、満たされているものとみなされる。
- 4:ADV_SPM.1-4 評価者は、TOE のモデル化されたセキュリティのふるまいが明確に表現されていることを決定するために、セキュリティ方針モデルの規則と特性を**検査しなければならない**。
- 1472 規則と特性は、TOE のセキュリティの考え方(posture)を記述する。そのような記述は、評価された、認証済みの ST に含まれていることがある。明確な表現であるとはみなされるためには、そのような記述は、TOE のセキュリティの概念を定義し、TOE によって制御されるエンティティのセキュリティ属性を識別し、それらの属性を変更する TOE アクションを識別するべきである。例えば、方針がデータの完全性の関係に対処しようとする場合、セキュリティ方針モデルは、次のことを行う。
- a) その TOE の完全性の概念を定義する。

- b) TOE が完全性を維持するデータのタイプを識別する。
- c) そのデータを変更できるエンティティを識別する。
- d) データを変更するために潜在的な変更者が従う必要がある規則を識別する。

ADV_SPM.1.3C

4:ADV_SPM.1-5 評価者は、モデル化されたふるまいが、セキュリティ方針（ST の機能要件によって表現されている）によって記述されている方針と一貫していることを決定するために、セキュリティ方針モデル根拠を**検査しなければならない**。

1473 一貫性を決定するとき、評価者は、根拠がセキュリティ方針モデルの各規則または特性記述がセキュリティ方針の意図を正確に反映していることを示していることを検証する。例えば、方針が、アクセス制御が一個人の詳細レベルまで必要であると述べている場合に、TOE のセキュリティのふるまいを利用者グループの制御として記述しているセキュリティ方針モデルには一貫性がないことになる。同様に、方針が利用者グループのアクセス制御が必要であると述べている場合に、TOE のセキュリティのふるまいを個人利用者の制御として記述しているセキュリティ方針モデルには一貫性がないことになる。

1474 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

4:ADV_SPM.1-6 評価者は、モデル化されたふるまいが、セキュリティ方針（すなわち、ST の機能要件によって表現されている）に記述されている方針に対して完全であることを決定するために、セキュリティ方針モデル根拠を**検査しなければならない**。

1475 この根拠が完全であることを決定するとき、評価者は、セキュリティ方針モデルの規則と特性を考慮し、それらの規則と特性を明示的方針ステートメント（すなわち、機能要件）にマッピングする。根拠は、モデル化する必要があるすべての方針が、セキュリティ方針モデルに関連する規則または特性の記述を持っていることを示すべきである。

ADV_SPM.1.4C

4:ADV_SPM.1-7 評価者は、セキュリティ方針モデルの機能仕様対応実証が、機能仕様に記述されている方針の部分を実装するすべてのセキュリティ機能を識別していることを決定するために、その対応実証を**検査しなければならない**。

1476 完全であることを決定するとき、評価者は、機能仕様をレビューし、セキュリティ方針モデルを直接サポートする機能を識別し、これらの機能がセキュリティ方針モデルの機能仕様対応実証に示されていることを検証する。

4:ADV_SPM.1-8 評価者は、セキュリティ方針モデルを実装していると識別されている機能の記述が機能仕様の記述と一貫性があることを決定するために、セキュリティ方針モデルの機能仕様対応実証を**検査しなければならない**。

1477 一貫性があることを実証するために、評価者は、機能仕様対応が、セキュリティ方針モデルに記述されている方針を実装していると識別されている機能の機能仕様の

機能記述がセキュリティ方針モデルと同じ属性と特性を識別していること及びセキュリティ方針モデルと同じ規則を実施していることを示していることを検証する。

- 1478 セキュリティ方針が信頼できない利用者と管理者に対して異なる方法で実施される場合、それぞれに対する方針は、利用者と管理者のガイダンスのそれぞれのふるまいの記述と一貫するように記述される。例えば、遠隔の信頼できない利用者に対して実施される「識別と認証」方針は、アクセス点が物理的にセキュアな領域に限られる管理者に対して実施される方針よりも厳格になる。認証の相違は、利用者と管理者のガイダンスでの認証の記述の相違に対応するべきである。
- 1479 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

8.7 ガイダンス文書アクティビティ

1480 ガイダンス文書アクティビティの目的は、運用 TOE を使用する方法を記述している証拠資料が適切であることを判断することである。そのような証拠資料には、正しくないアクションが TOE のセキュリティに悪影響を与えることがある信頼された管理者と管理者以外の利用者に対する文書と、正しくないアクションが自分自身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信頼できない利用者に対する両方の文書がある。

1481 EAL4 でのガイダンス文書アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

a) AGD_ADM.1

b) ADG_USR.1

8.7.1 適用上の注釈

1482 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。

8.7.2 管理者ガイダンスの評価 (AGD_ADM.1)

8.7.2.1 目的

1483 このサブアクティビティの目的は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を記述しているかどうかを決定することである。

8.7.2.2 適用上の注釈

1484 用語「*管理者*」(*administrator*) は、TOE 構成パラメタの設定など、TOE 内のセキュリティの重要な操作を実行することを任された人間利用者を示す。この操作は、TSP の実施に影響を与えるので、管理者は、これらの操作を行うために必要な特定の権限を有している。管理者(一人または複数)の役割は、TOE の管理者以外の利用者の役割から明確に区別する必要がある。

1485 監査者、管理者、または日常的な管理など、TOE により認識され、TSF と相互作用することができる ST に定義された異なる管理者の役割またはグループが存在することができる。各役割は、広範な能力のセットを含むか、または単一の能力であることができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。異なる管理者の役割とグループは、管理者ガイダンスにて考慮されるべきである。

8.7.2.3 入力

1486 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順
- g) ライフサイクル定義

8.7.2.4 評価者アクション

1487 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_ADM.1.1E

8.7.2.4.1 アクション AGD_ADM.1.1E

AGD_ADM.1.1C

4:AGD_ADM.1-1 評価者は、管理者ガイダンスが TOE の管理者が利用できる管理セキュリティ機能とインタフェースを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**。

1488 管理者ガイダンスには、管理者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

1489 管理者ガイダンスは、管理者セキュリティインタフェースと機能の目的、ふるまい、及び相互関係を識別し、記述するべきである。

1490 各管理者セキュリティインタフェースと機能に対して、管理者ガイダンスは、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式を記述する（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) 管理者が設定するパラメタ、それらの正当な値とデフォルトの値を記述する。
- 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。

AGD_ADM.1.2C

4:AGD_ADM.1-2 評価者は、管理者ガイダンスがセキュアな方法で TOE を管理する方法を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**。

1491 管理者ガイダンスは、ST に記述されているものと一貫する IT 環境の TSP に従って、TOE を操作する方法を記述する。

AGD_ADM.1.3C

4:AGD_ADM.1-3 評価者は、管理者ガイダンスがセキュアな処理環境で管理されなければならない機能と権限に関する警告を含んで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**。

1492 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利用者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、管理者ガイダンスに記述されるべきである。

1493 管理者ガイダンスでは、管理すべき機能と権限、それらに必要な管理のタイプ、そのような管理の理由を識別する。警告では、期待される効果、考えられる副次的効果、他の機能と権限との考えられる相互作用を指摘する。

AGD_ADM.1.4C

4:AGD_ADM.1-4 評価者は、管理者ガイダンスが TOE のセキュアな運用に関連する利用者のふるまいに関するすべての前提条件を記述していることを決定するために、そのガイダンスを**検査しなければならない**。

1494 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関する情報のみを管理者ガイダンスに含める必要がある。

1495 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。

AGD_ADM.1.5C

4:AGD_ADM.1-5 評価者は、管理者ガイダンスが管理者の管理下にあるすべてのセキュリティパラメータを、セキュアな値を適切に示して、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**。

1496 各セキュリティパラメータに対して、管理者ガイダンスは、パラメータの目的、パラメータの正当な値とデフォルトの値、そのようなパラメータの安全及び安全でない、個別または組み合わせによる、使用設定を記述するべきである。

AGD_ADM.1.6C

4:AGD_ADM.1-6 評価者は、管理者ガイダンスが TSF の制御下にあるエンティティのセキュリティ特質の変更を含む、実行が必要な管理機能に関連するセキュリティ関連事象の各タイプを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**。

1497 セキュリティ関連事象のすべてのタイプは、詳細に記述されているので、管理者は、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管理者が取る必要があるアクション（存在する場合）を知る。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、管理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_ADM.1.7C

4:AGD_ADM.1-7 評価者は、管理者ガイダンスが評価のために提供された他のすべての文書と一貫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**。

1498 特に ST には、TOE セキュリティ環境とセキュリティ対策方針に関する TOE 管理者への警告に対する詳細な情報を含めることができる。

1499 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_ADM.1.8C

4:AGD_ADM.1-8 評価者は、管理者ガイダンスが管理者に関連する TOE の IT 環境に対するすべての IT セキュリティ要件を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**。

1500 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。

1501 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。

1502 評価者は、TOE の IT 環境に対するセキュリティ要件 (ST のオプションステートメント) を分析し、管理者にとって適切な ST のすべてのセキュリティ要件が管理者ガイダンスに適切に記述されていることを保証するために、それらを管理者ガイダンスと比較するべきである。

8.7.3 利用者ガイダンスの評価 (AGD_USR.1)

8.7.3.1 目的

1503 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 が提供するセキュリティ機能とインタフェースを記述しているかどうか、及びこのガイダンスが TOE のセキュアな使用のための説明とガイドラインを提供しているかどうかを決定することである。

8.7.3.2 適用上の注釈

1504 TOE によって認識され、TSF と相互作用を行うことができる ST に定義されている異なる利用者の役割とグループが存在することができる。これらの役割の能力とそれらに関する権限は、FMT クラスに記述されている。異なる利用者の役割とグループは、利用者ガイダンスにて考慮されるべきである。

8.7.3.3 入力

1505 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) 上位レベル設計
- d) 利用者ガイダンス
- e) 管理者ガイダンス
- f) セキュアな設置、生成、及び立上げの手順

8.7.3.4 評価者アクション

1506 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) AGD_USR.1.1E

8.7.3.4.1 アクション AGD_USR.1.1E

AGD_USR.1.1C

4:AGD_USR.1-1 評価者は、利用者ガイダンスが TOE の非管理者である利用者が使用できるセキュリティ機能とインタフェースを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**。

1507 利用者ガイダンスには、利用者インタフェースで見ることができるセキュリティ機能の概要を含めるべきである。

1508 利用者ガイダンスには、セキュリティインタフェースと機能の目的を識別し、記述すべきである。

AGD_USR.1.2C

4:AGD_USR.1-2 評価者は、利用者ガイダンスが TOE により提供された利用者がアクセスできるセキュリティ機能の使用法を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**。

1509 利用者ガイダンスには、利用者が使用できるセキュリティインタフェースと機能のふるまいと相互関係を識別し、記述すべきである。

1510 利用者が TOE セキュリティ機能を起動することができる場合、利用者ガイダンスに、その機能に対して利用者が使用できるインタフェースの記述を提供する。

1511 各インタフェースと機能に対して、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、コマンドボタンなど）

b) 利用者が設定するパラメタ及びそれらの正当な値とデフォルトの値を記述する。

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。

AGD_USR.1.3C

4:AGD_USR.1-3 評価者は、利用者ガイダンスがセキュアな処理環境で管理されなければならない、利用者がアクセスできる機能と権限についての警告を含んで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**。

1512 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利用者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。これらの利用者がアクセス可能な機能と権限は、利用者ガイダンスに記述される。

1513 利用者ガイダンスでは、使用できる機能と権限、それらに必要となるコマンドのタイプ、そのようなコマンドの理由を識別すべきである。利用者ガイダンスには、管理すべき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、考えられる副次的効果、他の機能と権限との考えられる相互作用を指摘すべきである。

AGD_USR.1.4C

4:AGD_USR.1-4 評価者は、利用者ガイダンスが TOE セキュリティ環境の記述の中にある利用者のふるまいについての前提条件に関連した責任を含む、TOE のセキュアな運用に必要なすべての利用者の責任を提示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**。

- 1514 利用者のふるまいについての前提条件は、ST の TOE セキュリティ環境のステートメントにさらに詳細に記述することができる。ただし、TOE のセキュアな運用に関係する情報のみを利用者ガイダンスに含める必要がある。
- 1515 利用者ガイダンスでは、セキュリティ機能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。
- 1516 セキュアな運用に必要な利用者の責任の例は、利用者が自らのパスワードの秘密を保つことである。
- 1517 利用者ガイダンスでは、利用者が機能を起動することができるかどうかまたは利用者が管理者の助けを必要とするかどうかを示すべきである。

AGD_USR.1.5C

4:AGD_USR.1-5 評価者は、利用者ガイダンスが評価のために提供された他のすべての証拠資料と一貫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**。

1518 評価者は、評価のために提供された利用者ガイダンスとその他のすべての文書が互いに矛盾しないことを保証する。この保証は、ST に TOE セキュリティ環境とセキュリティ対策方針に関する TOE 利用者への警告についての詳細な情報が含まれているときに特に必要となる。

1519 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

AGD_USR.1.6C

4:AGD_USR.1-6 評価者は、利用者ガイダンスが利用者に関連する TOE の IT 環境に対するすべてのセキュリティ要件を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**。

1520 ST に IT 環境に対する IT 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適用されず、満たされているものとみなされる。

1521 このワークユニットは、IT セキュリティ要件のみに関係し、組織のセキュリティ方針には関係しない。

1522 評価者は、TOE の IT 環境に対するセキュリティ要件（ST のオプションステートメント）を分析し、利用者にとって適切な ST のすべてのセキュリティ要件が利用者ガイダンスに適切に記述されていることを保証するために、利用者ガイダンスと比較するべきである。

8.8 ライフサイクルサポートアクティビティ

- 1523 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 の開発と保守の間に使用する手続きが適切であることを決定することである。これらの手続きには、TOE の開発の全期間で使用されるセキュリティ手段、開発者が使用するライフサイクルモデル、及び TOE のライフサイクルを通して開発者が使用するツールが含まれる。
- 1524 開発者セキュリティ手続きは、TOE 及びそれに関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。
- 1525 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。
- 1526 明確に定義された開発ツールの使用は、詳細化中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。
- 1527 EAL4 のライフサイクルサポートアクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。
- a) ALC_DVS.1
 - b) ALC_LCD.1
 - c) ALC_TAT.1

8.8.1 開発セキュリティの評価 (ALC_DVS.1)

8.8.1.1 目的

- 1528 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。

8.8.1.2 入力

- 1529 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

- 1530 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。特に評価者は、開発者の構成管理証拠資料 (ACM_CAP.4 と ACM_SCP.2 サブアクティビティへの入力) を検査する必要がある。手続きが適用されていることを示す証拠も必要となる。

8.8.1.3 評価者アクション

1531 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。

a) ALC_DVS.1.1E

b) ALC_DVS.1.2E

8.8.1.3.1 アクション ALC_DVS.1.1E

ALC_DVS.1.1C

4: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**。

1532 評価者は、情報が明示的に提供されなくても、必要な保護、特に脅威に晒されているセクション、組織のセキュリティ方針及び前提条件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。環境に対するセキュリティ対策方針のステートメントもこの点で有用である。

1533 明示的な情報が ST から提供されない場合、評価者は、TOE に意図される環境を考慮して、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、明確な正当化が評価のために提供されるべきである。

1534 次のタイプ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 (physical)**。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 (procedural)**。例えば、次のものをカバーする。

- 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
- 保護される資材の開発環境の外部への移送
- 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 (personal)**。例えば、新たな開発スタッフの信頼を確認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。

- 1535 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で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施設、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。開発には、必要に応じて、TOEの複数のコピーの作成などのタスクが含まれる。このワークユニットは、ADO_DELのワークユニットと重複するべきでない。ただし、評価者は、1つのサブアクティビティまたは他のアクティビティによってすべての局面が扱われていることを保証するべきである。
- 1536 さらに、開発セキュリティ証拠資料は、セキュリティ手段の実行及び要求される入力と出力の観点から、開発の異なる局面に適用できる異なるセキュリティ手段を記述することができる。例えば、異なる手続きを、TOEの異なる部分の開発または開発プロセスの異なる段階に適用することができる。
- 4: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**。
- 1537 これらには次のことを管理する方針が含まれる。
- a) 機密を維持する必要がある TOE 開発に関する情報及びそのような資料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変更から保護する必要がある資料及びそのような資料を変更することができる開発スタッフのメンバ
- 1538 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。
- 1539 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、ACM_CAPサブアクティビティ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る必要があるため、TOEを変更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。
- 1540 ACM_CAP要件は固定されているが、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のセキュリティ環境セクションに提供される情報に依存する。例えば、STは、機密事項を扱う就任許可(security clearance)を持つスタッフによって開発されるTOEを要求する組織のセキュリティ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。

ALC_DVS.1.2C

- 4:ALC_DVS.1-3 評価者は、手続きを適用した結果として作成される記録による証拠が生成されたことを決定するために、開発セキュリティ証拠資料を**チェックしなければならない**。
- 1541 記録による証拠が作成されるとき、評価者は、それを検査して、手続きが遵守されていることを保証する。作成される証拠の例には、エントリログと監査証跡がある。評価者は、証拠をサンプリングすることを選択できる。

- 1542 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 8.8.1.3.2 アクション ALC_DVS.1.2E
- 4:ALC_DVS.1-4 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**。
- 1543 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ているといった、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。
- 1544 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、監督者と相談して決定されるべきである。
- 1545 サイト訪問のガイダンスについては、附属書 B.5 を参照のこと。

8.8.2 ライフサイクル定義の評価 (ALC_LCD.1)

8.8.2.1 目的

1546 このサブアクティビティの目的は、開発者が TOE ライフサイクルの引証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。

8.8.2.2 入力

1547 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

8.8.2.3 評価者アクション

1548 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ALC_LCD.1.1E

8.8.2.3.1 アクション ALC_LCD.1.1E

ALC_LCD.1.1C

4:ALC_LCD.1-1 評価者は、使用されたライフサイクルモデルの引証された記述が、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**。

1549 ライフサイクルモデルは、TOE を開発、保守するために使用される手続き、ツール及び技法を網羅する。ライフサイクルモデルの記述には、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）についての情報を含めるべきである。それには、手続きの適用を決める全体的な管理構造を記述するべきである（例えば、ライフサイクルモデルによってカバーさ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）。ALC_LCD.1 は、標準のライフサイクルモデルに従うために使用されるモデルを必要としない。

ALC_LCD.1.2C

4: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**。

1550 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、ACM アクティビティ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。

- 1551 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、及びウォーター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。

8.8.3 ツールと技法の評価 (ALC_TAT.1)

8.8.3.1 目的

1552 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。

8.8.3.2 入力

1553 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

8.8.3.3 適用上の注釈

1554 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機能の使用法（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.1 サブアクティビティと並行して行うことができる。

8.8.3.4 評価者アクション

1555 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ALC_TAT.1.1E

8.8.3.4.1 アクション ALC_TAT.1.1E

ALC_TAT.1.1C

4:ALC_TAT.1-1 評価者は、すべての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**。

1556 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(syntax)が明確に、完全に記述され、各構文の意味(semantic)が詳細に記述されている言語である。

ALC_TAT.1.2C

4:ALC_TAT.1-2 評価者は、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**。

1557 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カバーし、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.1 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。

- 1558 引証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。
- 1559 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ー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。
- 1560 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。
- 1561 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、引証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。

ALC_TAT.1.3C

- 4: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**。
- 1562 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、引証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。
- 1563 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。

8.9 テスタクティビティ

1564 このアクティビティの目的は、TOE が設計証拠資料の特定及び ST に特定されている TOE セキュリティ機能要件に従ってふるまうかどうかを決定することである。これは、開発者が機能テストと上位レベル設計に対して TSF をテストしたことを決定し、開発者のテストのサンプルを実行することによるそれらのテスト結果に確信を持ち、TSF のサブセットをテストすることによって行われる。

1565 EAL4 のテストアクティビティには、次のコンポーネントに関係するサブアクティビティが含まれている。

- a) ATE_COV.2
- b) ATE_DPT.1
- c) ATE_FUN.1
- d) ATE_IND.2

8.9.1 適用上の注釈

1566 評価者のテストサブセットのサイズと構成は、独立テスト (ATE_IND.2) サブアクティビティに記述されているいくつかの要因に依存する。サブセットの構成に影響を与えるそのような要因の 1 つは、評価者が (例えば、組織(scheme)から) アクセスする必要がある情報である *知られている公知の弱点 (known public domain weakness)* である。

1567 CC は、カバレッ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に適用するときの柔軟性を増している。ただし、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、評価者のサブアクティビティ間の作業成果の重複をもたらした。これらの適用上の注釈は、同じアクティビティと EAL の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。

8.9.1.1 TOE の期待されるふるまいの理解

1568 テスト証拠資料が適切であることを正確に評価するまえに、または新しいテストを作成するまえに、評価者は、満たす必要がある要件として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。

1569 評価者は、1 度に TSF の 1 つのセキュリティ機能に焦点を当てることを選択することができる。各セキュリティ機能に対して、評価者は、TOE の期待されるふるまい方の理解を得るために、ST 要件と機能仕様、上位レベル設計、及びガイダンス証拠資料の関連する部分を検査する。

1570 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、外部または内部のいずれかのインタフェースで刺激されるセキュリティ機能を引き起こし、その応答が観察される。ただし、セキュリティ機能をインタフェースで適切にテストできない場合がある (例

えば、残存情報保護機能の場合)。そのような場合には、別の手段を採用する必要がある。

8.9.1.2 セキュリティ機能の期待されるふるまいを検証するための、テスト 対代替手法

1571 インタフェースで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。代替手法が適切であることを決定するのは、評価者の責任である。ただし、代替手法が適切であることを評定するとき、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が、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を意味することができる。
- b) EAL が下位レベル設計または実装への評価の提示(exposure)と一致しない場合でも、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が容認される。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るために与えられるべきである。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、変更が分析またはその後のテストによって追跡され、対処されたとの証拠が必要となる。

1572 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セキュリティ機能の期待されるふるまいをテストする実際的な手段が存在しないと決定したときにのみ行うことが強調されるべきである。この代替は、上記の環境でのテストの費用（時間及びまたは経費）をできる限り少なくするために開発者に提供される。これは、TOE についての不当に余分の情報を要求する自由を評価者に与えるためのものでもなければ、一般的テストに置き換わるためのものでもない。

8.9.1.3 テストの適切性の検証

1573 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必要がある。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、完全に適切であることを決定する必要がある。

1574 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、インタフェース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及び上位レベル設計と一貫していることを決定しなければならない。テストは、これらの仕様において証拠資料として提出されたふるまいを検証しなければならない。このことは、機能仕様と上位レベル設計に明示的に記述されている各セキュリティ機能ふるまい特性が、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。

1575 TSF のすべては開発者によってテストされる必要があるが、インタフェースの徹底的な仕様テストは要求されない。このアクティビティの全体的な目的は、各セキュ

リティ機能が機能仕様と上位レベル設計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。テスト手順は、テスト機能がテスト中に開発者によって実行された方法の洞察を提供する。評価者は、TOE を独立にテストする追加のテストを開発するときに、この情報を使用する。

8.9.2 カバレッジの評価 (ATE_COV.2)

8.9.2.1 目的

1576 このサブアクティビティの目的は、テスト（証拠資料として提出されている）が、TSF が系統的に機能仕様に対してテストされていることを確認するのに十分であるかどうかを決定することである。

8.9.2.2 入力

- a) ST
- b) 機能仕様
- c) テスト証拠資料
- d) テストカバレッジ分析

8.9.2.3 評価者アクション

このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_COV.2.1E.

8.9.2.3.1 アクション ATE_COV.2.1E

ATE_COV.2.1C

4:ATE_COV.2-1 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の間に対応が正確であることを決定するために、テストカバレッジ分析を**検査しなければならない**。

1577 対応は、表またはマトリックスの形を取ることができる。場合によっては、マッピングがテストの対応を十分に示すことができる。その他の場合、根拠（通常、散文）により開発者が提供する対応分析を補足する必要がある。

1578 図 8.2 は、機能仕様に記述されているセキュリティ機能と、それらをテストするために使用されるテスト証拠資料に示されているテストの間の対応の概念的枠組みを示している。テストには、テストの依存性または実行されるテストの全体的目標によって、1 または複数のセキュリティ機能を含めることができる。

1579 テストカバレッジ分析に示されるテストとセキュリティ機能の識別は、曖昧でなくされる必要がある。テストカバレッジ分析により、評価者は、識別されているテストをテスト証拠資料まで、及びテストされている特定のセキュリティ機能を機能仕様までさかのぼることができる。

4:ATE_COV.2-2 評価者は、TSF の各セキュリティ機能に対するテスト手法が、期待されるふるまいを実証するのに適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**。

1580 このワークユニットのガイダンスは、次の中に見つけることができる。

- a) 適用上の注釈、8.9.1.1 節、TOE の期待されるふるまいの理解
- b) 適用上の注釈、8.9.1.2 節、セキュリティ機能の期待されるふるまいを検証するための、テスト 対 代替手法

4: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セキュリティ機能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**。

1581 このワークユニットのガイダンスは、次の中に見つけることができる。

- a) 適用上の注釈、8.9.1.3 節、テストの適切性の検証

ATE_COV.2.2C

4:ATE_COV.2-4 評価者は、機能仕様に記述されている TSF とテスト証拠資料に識別されてい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、テストカバレッジ分析を**検査しなければならない**。

1582 機能仕様に記述されているすべてのセキュリティ機能とインタフェースをテストカバレッジ分析に示し、テストにマッピングし、完全性を主張する必要がある。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。図 8.2 が示すように、セキュリティ機能のすべては、それらに関するテストが存在する。それゆえに、完全なテストカバレッジがこの例に示されている。セキュリティ機能がテストカバレッジ分析に識別されているならば、それに対するテストが示されない場合、カバレッジが不完全であることは明らかである。

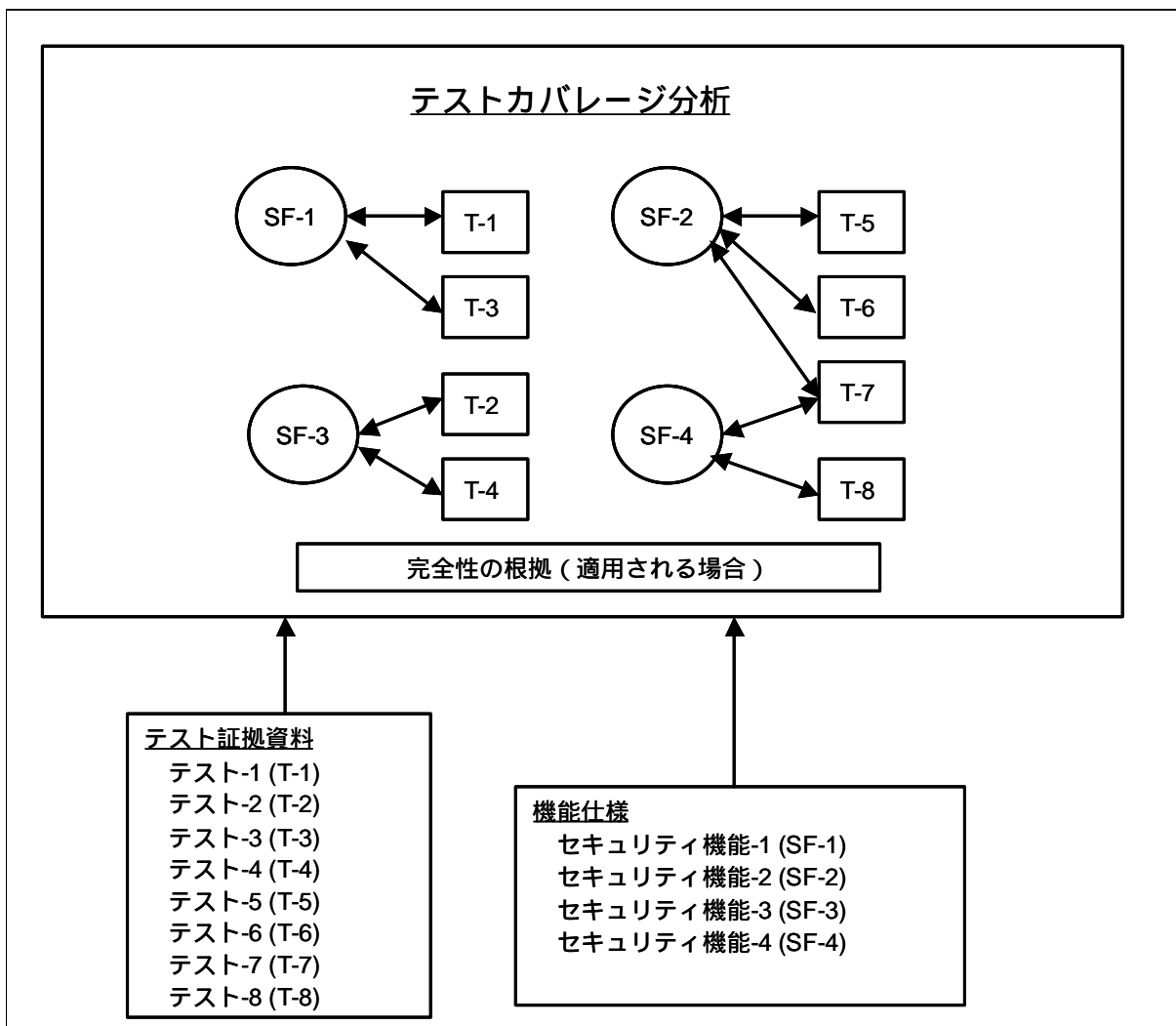


図 8.2 テストカバレッジ分析の概念的枠組み

- 8.9.3 深さの評価 (ATE_DPT.1)**
- 8.9.3.1 目的**
- 1583 このサブアクティビティの目的は、開発者が TSF をその上位レベル設計と比較してテストしたかどうかを決定することである。
- 8.9.3.2 入力**
- a) ST
 - b) 機能仕様
 - c) 上位レベル設計
 - d) テスト証拠資料
 - e) テストの深さ分析
- 8.9.3.3 評価者アクション**
- 1584 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。
- a) ATE_DPT.1.1E.
- 8.9.3.3.1 アクション ATE_DPT.1.1E**
- ATE_DPT.1.1C**
- 4:ATE_DPT.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上位レベル設計とのマッピングのテストの深さ分析を **検査しなければならない。**
- 1585 テストの深さ分析は、上位レベル設計に記述されているすべてのサブシステムを識別し、テストのこれらのサブシステムへのマッピングを提供する。対応は、表またはマトリックスの形を取ることができる。場合によっては、マッピングがテストの対応を十分に示すことができる。その他の場合、根拠（通常、散文）により開発者が提供する対応分析を補足する必要がある。
- 1586 TOE セキュリティ要件にマッピングされ、その要件を満たす上位レベル設計に特定されているすべての設計詳細は、テストが必要であり、それゆえに、テスト証拠資料にマッピングされるべきである。図 8.3 は、上位レベル設計に記述されているサブシステムと、それらをテストするために使用される TOE のテスト証拠資料に示されているテストの間の対応の概念的枠組みを示している。テストには、テストの依存性または実行されるテストの全体的目標によって、1 または複数のセキュリティ機能を含めることができる。
- 4:ATE_DPT.1-2 評価者は、TSF の各セキュリティ機能に対するテスト手法が、期待されるふるまいを実証するのに適していることを決定するために、開発者のテスト計画を **検査しなければならない。**

- 1587 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) 適用上の注釈、8.9.1.1 節、TOE の期待されるふるまいの理解
 - b) 適用上の注釈、8.9.1.2 節、セキュリティ機能の期待されるふるまいを検証するためのテスト 対 代替手法
- 1588 TSF のテストは、外部インタフェース、内部インタフェース、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、セキュリティ機能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セキュリティ機能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。
- 4:ATE_DPT.1-3 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テスト機能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**。
- 1589 このワークユニットのガイダンスは、次の中に見つけることができる。
- a) 適用上の注釈、8.9.1.3 節、テストの適切性の検証
- 4:ATE_DPT.1-4 評価者は、上位レベル設計に定義されている TSF がテスト証拠資料のテストに完全にマッピングされていることを保証するために、テストの深さ分析を **チェックしなければならない**。
- 1590 テストの深さ分析は、上位レベル設計とテスト計画及び手順の間の対応の完全なステートメントを提供する。上位レベル設計に記述されているすべてのサブシステムと内部インタフェースは、テストの深さ分析に示されている必要がある。テストの深さ分析に示されているサブシステムと内部インタフェースのすべてに対して、完全性を主張するために、それらへマッピングされているテストをもつ必要がある。図 8.3 が示すように、サブシステムと内部インタフェースのすべては、それらに関係するテストが存在する。それゆえに、完全なテストの深さがこの例に示されている。サブシステムと内部インタフェースがテストの深さ分析に識別されているならば、それに対するテストが示されない場合、カバレッジが不完全であることは明らかである。

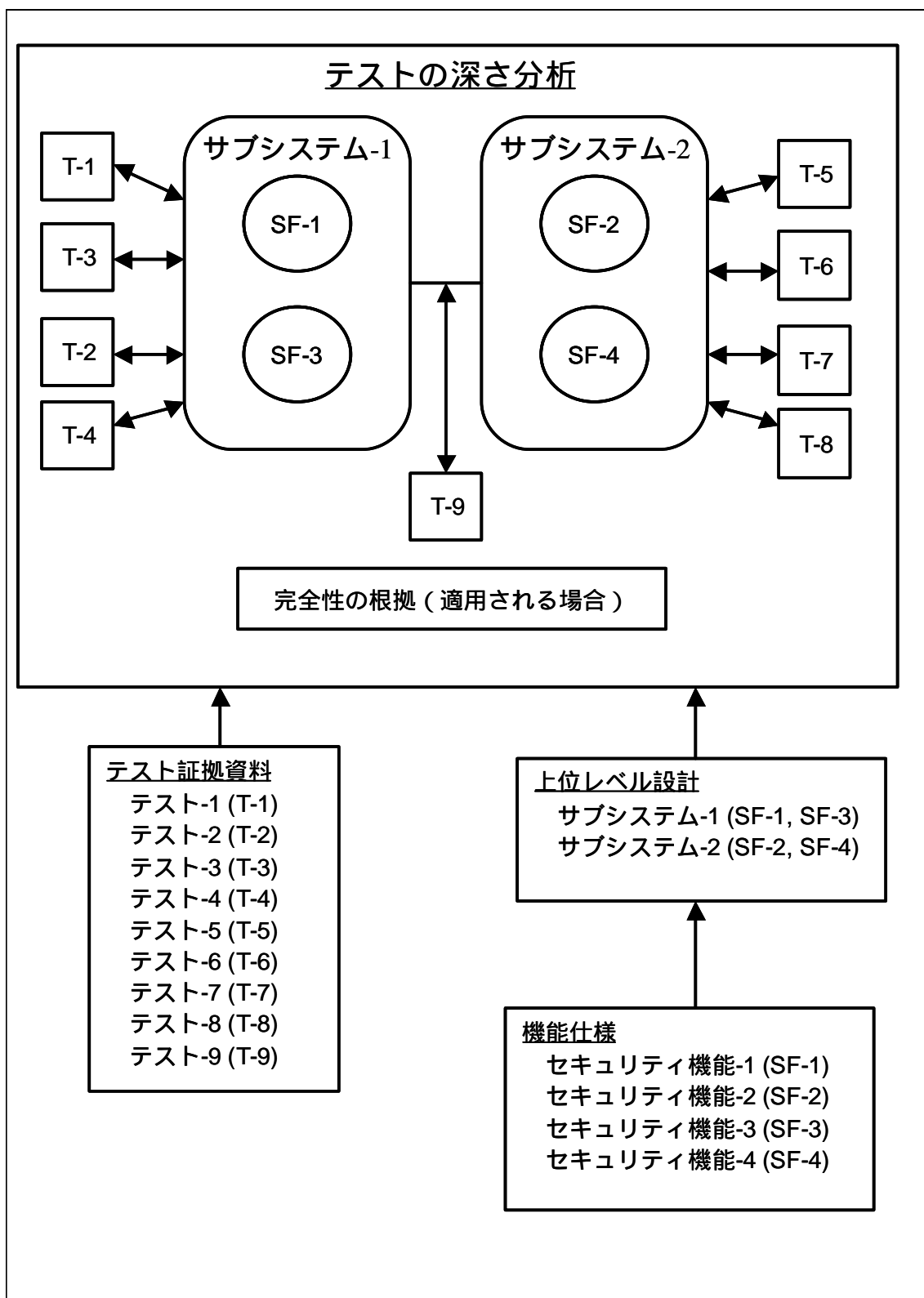


図 8.3 テストの深さ分析の概念的枠組み

8.9.4 機能テストの評価 (ATE_FUN.1)

8.9.4.1 目的

1591 このサブアクティビティの目的は、セキュリティ機能が特定されたとおりに実行されることを実証するのに、開発者の機能テスト証拠資料が十分であるかどうかを決定することである。

8.9.4.2 適用上の注釈

1592 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、カバレッジ保証コンポーネントに依存する。

1593 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が、特定されたとおりに実行しないことを示しているセキュリティ機能はいずれも、評価者が独立にテストして、それが機能するかしないかが決定されるべきである。

8.9.4.3 入力

1594 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) テスト手順

8.9.4.4 評価者アクション

1595 このサブアクティビティは、次の 1 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_FUN.1.1E.

8.9.4.4.1 アクション ATE_FUN.1.1E

ATE_FUN.1.1C

4:ATE_FUN.1-1 評価者は、テスト証拠資料にテスト計画、テスト手順記述、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**。

ATE_FUN.1.2C

4:ATE_FUN.1-2 評価者は、テスト計画がテストされるセキュリティ機能を識別していることを**チェックしなければならない**。

- 1596 テストされるセキュリティ機能を識別するために使用できる 1 つの方法は、個々のセキュリティ機能を特定している機能仕様の適切な部分を参照することである。
- 1597 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。
- 1598 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 4:ATE_FUN.1-3 評価者は、テスト計画が実行されるテストの目標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**。
- 1599 テスト計画は、セキュリティ機能をテストする方法とテストが行われるテスト構成についての情報を提供する。
- 1600 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。
- 1601 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 4:ATE_FUN.1-4 評価者は、TOE テスト構成が ST における評価のために識別されている構成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**。
- 1602 テストに使用される TOE は、ACM_CAP.4 サブアクティビティによって確証されたのと同じ一意的なリファレンスと開発者が提供するテスト証拠資料を持つべきである。
- 1603 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個別のハードウェアとソフトウェア実装で構成することができる。評価者は、ST に記述されている各評価済みの構成に一貫するテスト構成が存在することを検証する。
- 1604 評価者は、テスト環境に適用できる ST に記述されている TOE 環境のセキュリティの側面についての前提条件を考慮するべきである。ST にはテスト環境に適用されない前提条件がいくつか存在することがある。例えば、利用者の取扱許可についての前提条件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前提条件は適用するだろう。
- 4:ATE_FUN.1-5 評価者は、テスト計画がテスト手順記述と一貫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**。
- 1605 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。
- 1606 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ATE_FUN.1.3C

- 4:ATE_FUN.1-6 評価者は、テスト手順記述がテストされる各セキュリティ機能のふるまいを識別していることを**チェックしなければならない**。

- 1607 テストされるセキュリティ機能のふるまいを識別するために使用できる 1 つの方法は、テストする個々のふるまいを特定している設計仕様の適切な部分を参照することである。
- 1608 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。
- 1609 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 4:ATE_FUN.1-7 評価者は、もしあれば順序の依存性を含め、再現できる初期テスト条件を確立するための十分な指示が提供されていることを決定するために、テスト手順記述を**検査しなければならない**。
- 1610 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まえに、追加される必要がある。他のテスト結果の順序に依存する一例は、アクセス制御のような他のセキュリティメカニズムに対する監査レコードを作成するために監査機能に頼るまえに、監査機能をテストする必要があることである。順序に依存する他の例としては、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。
- 1611 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。
- 1612 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 4:ATE_FUN.1-8 評価者は、セキュリティ機能を刺激し、それらのふるまいを観察するための再現可能な手段を取れるように十分な指示が提供されていることを決定するために、テスト手順記述を**検査しなければならない**。
- 1613 刺激は、通常、TSFI を通して外部からセキュリティ機能に提供される。入力 (input) (刺激(stimulus)) が TSFI に提供されれば、セキュリティ機能のふるまいを TSFI で観察することができる。テスト手順に刺激とこの刺激の結果として期待されるふるまいを曖昧さなく記述した詳細な情報が含まれていない限り、再現可能であると保証されない。
- 1614 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。
- 1615 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。
- 4:ATE_FUN.1-9 評価者は、テスト手順記述がテスト手順と一貫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**。
- 1616 テスト手順記述がテスト手順である場合には、このワークユニットは適用されず、満たされているものとみなされる。
- 1617 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。

- 1618 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

ATE_FUN.1.4C

- 4:ATE_FUN.1-10 評価者は、十分な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**。

- 1619 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、テスト手法を与えられた期待されるふるまいと曖昧でなく一貫している場合、十分である。

- 1620 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。

- 1621 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

ATE_FUN.1.5C

- 4:ATE_FUN.1-11 評価者は、テスト証拠資料の期待されるテスト結果が提供された実際の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**。

- 1622 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。

- 1623 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。

- 1624 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）。

- 1625 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変更を行わずに、このプロセスが正しいかどうかを評定するために使用することが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のは、開発者の責任である。

- 1626 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。

- 1627 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

- 1628 いずれかのテストの期待されるテスト結果と実際のテスト結果が同じでない場合、セキュリティ機能が正しく働いているとの実証は達成されない。そのようなことは、関係するセキュリティ機能のテストを含める評価者の独立テストの成果に影響を与

える。評価者は、また、このワークユニットが行われる証拠のサンプルを増やすことを考慮するべきである。

4:ATE_FUN.1-12 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成果を**報告しなければならない**。

1629 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、他の評価者や監督者が、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。

1630 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) 実行された開発者テストの量。開発者テストのカバレッジと深さの範囲の記述。
- d) テスト結果。開発者テストの全体的な結果の記述。

1631 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 に示すべきタイプの情報を提供することだけを意図している。

8.9.5 独立テストの評価 (ATE_IND.2)

8.9.5.1 目的

1632 このアクティビティの目標は、TSF のサブセットを独立にテストすることにより TOE が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、また開発者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の確信を得ることである。

8.9.5.2 入力

1633 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) 利用者ガイダンス
- d) 管理者ガイダンス
- e) セキュアな設置、生成、及び立上げの手順
- f) テスト証拠資料
- g) テストカバレッジ分析
- h) テストの深さ分析
- i) テストに適した TOE

8.9.5.3 評価者アクション

1634 このサブアクティビティは、次の 3 つの CC パート 3 評価者アクションエレメントからなる。

- a) ATE_IND.2.1E
- b) ATE_IND.2.2E
- c) ATE_IND.2.3E

8.9.5.3.1 アクション ATE_IND.2.1E

ATE_IND.2.1C

4:ATE_IND.2-1 評価者は、テスト構成が ST に特定のとおり評価のもとでの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**。

1635 テストに使用される TOE は、ACM_CAP.4 サブアクティビティによって確認されたのと同じ一意的リファレンスと開発者が提供するテスト証拠資料を持つべきである。

1636 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個別のハードウェアとソフトウェア実装で構成することができる。評価者は、ST に記述されている各評価済みの構成に一貫するテスト構成が存在することを検証する。

1637 評価者は、テスト環境に適用できる ST に記述されている TOE 環境のセキュリティの側面についての前提条件を考慮するべきである。ST にはテスト環境に適用されない前提条件がいくつか存在することがある。例えば、利用者の取扱許可についての前提条件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前提条件は適用するだろう。

1638 いずれかのテスト資源（例えば、メータ、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。

4: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**。

1639 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、ADO_IGS.1 サブアクティビティ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確信している場合、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て、TOE を設置、生成し、立上げする開発者の手順に従うべきである。

1640 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 4:ADO_IGS.1-2 の条件を満たすことができる。

ATE_IND.2.2C

4: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**。

1641 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。

8.9.5.3.2 アクション ATE_IND.2.2E

4:ATE_IND.2-4 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**。

1642 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厳格にではなくテストでき得る多くのセキュリティ機能を含める方法である。別のテスト方策は、気が付いた問題との関連に基づいたいくつかのセキュリティ機能を含んだテストサブセットを持ち、これらの機能を厳格にテストすることである。

1643 一般的に、評価者のテスト手法は、これら 2 つの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、ST に識別されているほとんどのセ

セキュリティ機能要件を検査すべきであるが、テストは、徹底的な仕様テストを実証する必要はない。

1644

評価者は、テストする TSF のサブセットを選択するとき、次のファクタを考慮すべきである。

- a) 開発者テスト証拠。開発者テスト証拠は、テストカバレッジ分析、テストの深さ分析、及びテスト証拠資料からなる。開発者テスト証拠は、テスト中に開発者がセキュリティ機能をテストした方法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。具体的に評価者は、次のことを考慮すべきである。
 - 1) 特定のセキュリティ機能に対する開発者テストの増加。評価者は、セキュリティ機能をさらに厳格にテストするためにパラメータを変えて、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) 特定のセキュリティ機能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、特定のセキュリティ機能のテスト手法を変更することができる。
- b) テストサブセットに加えるセキュリティ機能の数。TOE に含まれているセキュリティ機能の数が少ない場合には、セキュリティ機能のすべてを厳格にテストすることが現実的にできる。多数のセキュリティ機能を持つ TOE では、これは費用効果が悪く、サンプリングが必要になる。
- 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。

1645

評価者は、サブセットを構成するセキュリティ機能を選択する。この選択は、数多くのファクタに依存し、これらのファクタの考慮は、テストサブセットサイズの選択にも影響を与える。

- a) セキュリティ機能の開発者テストの厳格さ。機能仕様に識別されているすべてのセキュリティ機能は、ATE_COV.2 が必要とするそれらに関するテスト証拠を備えている必要がある。追加のテストが必要であると評価者が決定したセキュリティ機能は、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セキュリティ機能またはその様相が特定どおりに動作す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セキュリティ機能を含めるべきである。
- c) TOE の種別に一般的に関係する知られている公知の弱点（例えば、オペレーティングシステム、ファイアウォール）。TOE の種別に関係する知られている公知の弱点は、テストサブセットの選択プロセスに影響する。評価者は、その種別の TOE に対する知られている公知の弱点に対処するそれらのセキュリティ機能をサブセットに含めるべきである（ここでの知られている公知の弱点は、そのような脆弱性を意味せず、この特別の種別で経験された不十分性または問題領域を意味する）。そのような弱点が知られていない場合には、セキュリティ機能の広い範囲を選択する比較一般的な手法がさらに適している。

- d) セキュリティ機能の重要性。TOE に対するセキュリティ対策方針の観点から他のセキュリティ機能よりも重要なセキュリティ機能は、テストサブセットに含まれるべきである。
- e) ST でなされている SOF 主張。特定の SOF 主張に対するすべてのセキュリティ機能はテストサブセットに含まれるべきである。
- f) セキュリティ機能の複雑性。複雑なセキュリティ機能は、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めんどろな要求を課す複雑なテストを必要とするかもしれない。逆に複雑なセキュリティ機能は、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。
- g) 暗黙のテスト。あるセキュリティ機能のテストは、しばしば暗黙に他のセキュリティ機能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、(暗黙にはあるが) テストされるセキュリティ機能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を提供するために使用され、効率的なテスト手法の標的となる。
- h) TOE への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。
- i) 革新的または一般的でない機能。販売広告用の印刷物で強調しているような革新的または一般的でないセキュリティ機能が TOE に含まれている場合、これらは、テストの有力な候補となるべきである。

1646 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。

1647 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

4:ATE_IND.2-5 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**。

1648 評価者は、ST 及び機能仕様からセキュリティ機能の期待されるふるまいを理解して、機能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、セキュリティ機能を外部インタフェースでテストするか、テストハーネス(test harness)を使用して内部インタフェースでテストするか、または別のテスト手法 (例えば、例外状況、コード検査) を採用するべきか。
- b) セキュリティ機能を刺激し、応答を観察するために使用されるセキュリティ機能インタフェース。
- c) テストに存在する必要がある初期条件 (すなわち、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) セキュリティ機能を刺激する（例えば、パケットジェネレータ）またはセキュリティ機能を観察する（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。

1649 評価者は、一連のテストケースを使用して各セキュリティ機能をテストするのが実際的であることを発見することがある。その場合、各テストケースは、期待されるふるまいの大変特定の局面をテストする。

1650 評価者のテスト証拠資料は、必要に応じて、該当する設計仕様、及び ST 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。

4:ATE_IND.2-6 評価者は、テストを**実施しなければならない**。

1651 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。

4:ATE_IND.2-7 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) テストするセキュリティ機能のふるまいの識別
- 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) すべての前提となるテスト条件を確立するための指示
- d) セキュリティ機能を刺激するための指示
- e) セキュリティ機能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

1652 詳細のレベルは、他の評価者がテストを繰り返し、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、異なることができるが、全体的な結果は同一であるべきである。

1653 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が、期待される結果を比較するまえに、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。

4:ATE_IND.2-8 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**。

1654 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変更を必要とする。この決定とそれを正当とする理由は、評価者に任される。

8.9.5.3.3 アクション ATE_IND.2.3E

4:ATE_IND.2-9 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**。

1655 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。

1656 テストアクティビティ全体に対する評価者の全体的な労力を考慮して、通常、開発者のテストの 20%が実行されるべきである。ただし、これは、TOE の本質と提供されるテスト証拠によって変化する。

1657 開発者のテストはすべて、特定のセキュリティ機能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ファクタは、ワークユニット ATE_IND.2-4 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。

1658 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

4:ATE_IND.2-10 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**。

1659 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。

1660 十分な説明または説明が得られない場合、開発者のテスト結果に対する評価者の確信は落ちるであろうし、評価者はサンプルサイズを増やし、開発者のテストへの確信を取り戻す必要がある場合がある。サンプルサイズを増やしても評価者の懸念を取り去ることができない場合には、開発者テストの全体のセットを繰り返す必要がある。最終的に、ワークユニット ATE_IND.2-4 に識別されている TSF サブセットが適切にテストされるまで、開発者のテストの欠陥は、開発者のテストの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。

4: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成果を**報告しなければならない**。

1661 ETR に報告される評価者のテスト情報は、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、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、他の評価者や監督者が、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。

1662 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セキュリティ機能の量とサイズの正当とする理由。
- c) サブセットを構成するセキュリティ機能の選択基準。サブセットに含めるセキュリティ機能を選択したときに考慮したファクタについての簡単な説明。
- d) テストされたセキュリティ機能。サブセットに含めることに値したセキュリティ機能の簡単なリスト。
- 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総合判断。

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 に示すべきタイプの情報を提供することだけを意図している。

8.10 脆弱性評価アクティビティ

1663 脆弱性評価アクティビティの目的は、意図する環境での TOE の欠陥または弱点の存在と利用される可能性を決定することである。この決定は、開発者と評価者が行う分析に基づいて行われ、評価者のテストによりサポートされる。

1664 EAL4 での脆弱性評価アクティビティには、次のコンポーネントに関するサブアクティビティが含まれる。

- a) AVA_MSU.2
- b) AVA_SOF.1
- c) AVA_VLA.2

8.10.1 誤使用の評価 (AVA_MSU.2)

8.10.1.1 目的

1665 このサブアクティビティの目的は、ガイダンスが誤解されるか、合理的でないか、または矛盾しているか、操作のすべてのモードに対するセキュアな手順が取り扱われているかどうか、及びガイダンスを使用して容易に TOE の安全でない状態を阻止し、検出することができるかどうかを決定することである。

8.10.1.2 適用上の注釈

1666 このサブアクティビティでの用語「ガイダンス」(*guidance*)の使用は、利用者ガイダンス、管理者ガイダンス、セキュアな設置、生成及び立上げ手順を意味する。ここでの設置、生成及び立上げ手順は、TOE を配付された状態から運用状態にするために行う、管理者が責任を負うすべての手順を意味する。

1667 このコンポーネントには、AVA_MSU.1 に存在しない開発者分析の要件が含まれる。この分析の正当性の確認は、ガイダンス証拠資料の評価者自身の検査に代わるものとして使用されるべきではなく、開発者も誤使用の問題を明示的に取り扱っていることを示す証拠として使用されるべきである。

8.10.1.3 入力

1668 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) 上位レベル設計
- d) 下位レベル設計
- e) 実装表現のサブセット
- f) TOE セキュリティ方針モデル

- g) 利用者ガイダンス
- h) 管理者ガイダンス
- i) セキュアな設置、生成、及び立上げの手順
- j) ガイダンスの誤使用分析
- k) テスト証拠資料
- l) テストに適した TOE

8.10.1.4 評価者アクション

1669 このサブアクティビティは、次の 4 つの CC パート 3 評価者アクションエレメントからなる。

- a) AVA_MSU.2.1E
- b) AVA_MSU.2.2E
- c) AVA_MSU.2.3E
- d) AVA_MSU.2.4E

8.10.1.4.1 アクション AVA_MSU.2.1E

AVA_MSU.2.1C

4:AVA_MSU.2-1 評価者は、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、故障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、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**。

1670 その他の評価証拠、特に機能仕様とテスト証拠資料は、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。

1671 評価者は、セキュリティ機能を安全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、セキュリティ機能に関するガイダンスがそのセキュリティ機能のセキュアな使用（すなわち、TSP と一貫している）に十分であることを決定するために、1 度に 1 つのセキュリティ機能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して機能の間の関係も考慮するべきである。

1672 AVA_MSU.2.2C

4:AVA_MSU.2-2 評価者は、ガイダンスが明白であり、内部的に一貫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**。

1673 ガイダンスは、管理者または利用者によって間違っ構成されており、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。

- 1674 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。
- 4:AVA_MSU.2-3 評価者は、ガイダンスが完全であり、合理的であることを決定するために、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**。
- 1675 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 の理解を応用すべきである。
- 1676 特に評価者は、機能仕様と TOE 要約仕様を考慮すべきである。これらの文書に記述されているすべてのセキュリティ機能は、それらの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。評価者は、補助として、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省略はいずれも、不完全性を示す。
- 1677 ガイダンスが ST と一致していない、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。
- 1678 評価者は、AGD_ADM サブアクティビティからワークユニットの実行中に得られた結果がこの検査への有効な入力を提供することに注意するべきである。

AVA_MSU.2.3C

- 4:AVA_MSU.2-4 評価者は、意図する環境についてのすべての前提条件が明記されていることを決定するために、ガイダンスを**検査しなければならない**。
- 1679 評価者は、ST の意図する TOE セキュリティ環境についての前提条件を分析し、それらをガイダンスと比較して、管理者または利用者に関する ST の意図する TOE セキュリティ環境についてすべての前提条件がガイダンスに適切に記述されていることを保証する。

AVA_MSU.2.4C

- 4:AVA_MSU.2-5 評価者は、外部のセキュリティ手段に対するすべての要件が明記されていることを決定するために、ガイダンスを**検査しなければならない**。
- 1680 評価者は、ガイダンスを分析して、それがすべての外部の手続き的、物理的、人的及び接続管理を列挙していることを保証する。非 IT 環境に対する ST の中でのセキュリティ対策方針は、何が必要とされるかを示す。

AVA_MSU.2.5C

- 4:AVA_MSU.2-6 評価者は、ガイダンスが完全であることを保証するために適切な手段を開発者が取っていることを決定するために、開発者の分析を**検査しなければならない**。
- 1681 開発者の分析は、ST または機能仕様からガイダンスへの、ガイダンスが完全であることを示すためのマッピングから構成することができる。開発者が完全性を実証するために提供した証拠に関係なく、評価者は、ワークユニット AVA_MSU.2-1 から AVA_MSU.2-5 まで及び AVA_MSU.2-7 の実施で検出された欠陥に対する開発者の分析を評定するべきである。

8.10.1.4.2 アクション AVA_MSU.2.2E

4:AVA_MSU.2-7 評価者は、提供されたガイダンスだけを使用して TOE を構成し、セキュアに使用できることを決定するために、TOE を構成し、設置するために必要なすべての管理者と利用者（適用される場合）手順を**実行しなければならない**。

1682 構成と設置では、評価者は、TOE を配付可能な状態から、運用可能であり、ST に特定されているセキュリティ対策方針に合わせて TSP を実施する状態に進める必要がある。

1683 評価者は、通常、TOE の消費者に提供される利用者と管理者のガイダンスにおいて証拠資料として提出された開発者の手順だけに従うべきである。それらのことを行うときに会う困難はいずれも、ガイダンスが不完全である、明確でない、一致していない、または不合理であることを示す。

1684 このワークユニットの条件を満たすために行われる作業は、評価者アクション ADO_IGS.1.2E の条件を満たすことにも貢献することに注意すること。

4:AVA_MSU.2-8 評価者は、提供されたガイダンスだけを使用して、TOE を構成し、セキュアに使用できることを決定するために、ガイダンスに特定されているその他のセキュリティに係る手順を**実行しなければならない**。

1685 評価者は、通常、TOE の消費者に提供される利用者と管理者のガイダンスにおいて証拠資料として提出された開発者の手順だけに従うべきである。

1686 評価者は、このワークユニットを行うとき、サンプリングを採用するべきである。サンプルを選択するとき、評価者は、次のことを考慮するべきである。

- a) ガイダンスの明解性 – 不明解であると考えられるガイダンスがサンプルに含まれるべきである。
- b) 最も頻繁に使用されるガイダンス – あまり頻繁に使用されないガイダンスは、通常、サンプルに含まれるべきではない。
- c) ガイダンスの複雑性 – 複雑なガイダンスは、サンプルに含まれるべきである。
- d) 誤りの重要性 – 誤りがセキュリティに最も大きな重大性を加える手順は、サンプルに含まれるべきである。
- e) TOE の本質 – TOE の通常またはほとんどの使用に係るガイダンスは、サンプルに含まれるべきである。

1687 サンプリングのガイダンスについては、附属書 B.2 を参照のこと。

1688 一貫性の分析のガイダンスについては、附属書 B.3 を参照のこと。

8.10.1.4.3 アクション AVA_MSU.2.3E

4:AVA_MSU.2-9 評価者は、消費者が TOE セキュリティ機能を効果的に管理、使用し、セキュアでない状態を検出するための十分なガイダンスが提供されていることを決定するために、ガイダンスを**検査しなければならない**。

- 1689 TOE は、各種の方法を使用して、消費者が効果的に TOE を安全に使用するのを支援する。ある TOE は、TOE が安全でない状態のときに消費者に警報を出す機能（特性）を採用し、他の TOE には、高度なガイダンスが提供される。そのガイダンスには、既存のセキュリティ機能を最も効果的に使用するための示唆、ヒント、手順などが含まれている。例えば、安全でない状態を検出するための手助けとして監査機能を使用するためのガイダンス。
- 1690 このワークユニットの判定に到達するために、評価者は、TOE の機能、その目的と意図する環境、及び使用または利用者についての前提条件を考慮する。評価者は、TOE が安全でない状態に移行する場合、ガイダンスを使用することにより、安全でない状態をタイムリな方法で検出することができるとの合理的予測が存在するとの結論に達するべきである。TOE が安全でない状態に入る可能性は、ST、機能仕様及び TSF の上位レベル設計などの評価に提供されるものを使用して決定することができる。
- 8.10.1.4.4 アクション AVA_MSU.2.4E
- 4:AVA_MSU.2-10 評価者は、TOE の操作のすべてのモードにおけるセキュアな操作のためにガイダンスが提供されていることを決定するために、ガイダンスの開発者の分析を**検査しなければならない**。
- 1691 評価アクション AVA_MSU.2.1E の結果は、開発者の分析を評価するための基礎を提供するべきである。ガイダンスの誤使用の可能性を評価した後、評価者は、開発者の誤使用分析がこのサブアクティビティの目的に合っていることを決定できるべきである。

8.10.2 TOE セキュリティ機能強度の評価 (AVA_SOF.1)

8.10.2.1 目的

1692 このサブアクティビティの目的は、SOF 主張がすべての確率的または順列的メカニズムに対して ST でなされているかどうか、及び ST でなされている開発者の SOF 主張が正しい分析によって裏付けられているかどうかを決定することである。

8.10.2.2 適用上の注釈

1693 SOF 分析は、パスワードメカニズムまたは生物的尺度 (バイオメトリックス) など、本来確率的または順列的メカニズムに対して行われる。暗号化メカニズムも本来確率的であり、強度の観点から多く記述されているが、AVA_SOF.1 は、暗号化メカニズムには適用されない。そのようなメカニズムには、評価者は、制度ガイダンスを探すべきである。

1694 SOF 分析は、個々のメカニズムに基づいて行われるが、SOF の全体的な決定は、機能に基づいて行われる。セキュリティ機能を提供するために複数の確率的または順列的メカニズムが採用される場合には、それぞれ個別のメカニズムを分析する必要がある。セキュリティ機能を提供するためにこれらのメカニズムを組み合わせる方法は、その機能の全体的な SOF レベルを決定する。評価者は、メカニズムが機能を提供するために一体となって動作する方法、及び ADV_HLD.1 の依存性によって与えられるそのような情報の最小レベルを理解するために設計情報を必要とする。評価者に提供される実際の設計情報は、EAL によって決定される。提供される情報は、必要となときに、評価者の分析を裏付けるために使用されるべきである。

1695 複数の TOE ドメインに関する SOF の説明については、4.4.6 節を参照のこと。

8.10.2.3 入力

1696 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) 上位レベル設計
- d) 下位レベル設計
- e) 実装表現のサブセット
- f) 利用者ガイダンス
- g) 管理者ガイダンス
- h) TOE セキュリティ機能強度の分析

- 8.10.2.4 評価者アクション
- 1697 このサブアクティビティは、次の 2 つの CC パート 3 評価者アクションエレメントからなる。
- a) AVA_SOF.1.1E;
- b) AVA_SOF.1.2E.
- 8.10.2.4.1 アクション AVA_SOF.1.1E
- AVA_SOF.1.1C
- 4:AVA_SOF.1-1 評価者は、ST に SOF レート付けで表されている SOF 主張に対応する各セキュリティメカニズムに対して開発者が SOF 分析を提供していることを**チェックしなければならない**。
- 1698 SOF 主張が SOF 数値尺度だけで表されている場合、このワークユニットは、適用されず、条件は満たされているものとみなされる。
- 1699 SOF レート付けは、攻撃能力として表される 1 つの SOF-基本、SOF-中位、SOF-高位として表される。CC パート 1 用語集を参照のこと。レート付けとして表された最小の全体的 SOF 要件は、すべての非暗号、確率的または順列的セキュリティメカニズムに適用される。ただし、個々のメカニズムは、全体的 SOF 要件を越えるレート付けとして表された SOF 主張を持つことができる。
- 1700 攻撃するために必要となる攻撃能力を決定するガイダンス、及びレート付けとして SOF を決定するガイダンスについては、附属書 B.8 を参照のこと。
- 1701 SOF 分析は、ST でなされた SOF 主張を正当化する根拠からなる。
- AVA_SOF.1.2C
- 4:AVA_SOF.1-2 評価者は、ST に数値尺度で表されている SOF 主張に対応する各セキュリティメカニズムに対して開発者が SOF 分析を提供していることを**チェックしなければならない**。
- 1702 SOF 主張が SOF レート付けだけで表されている場合、このワークユニットは、適用されず、条件は満たされているものとみなされる。
- 1703 レート付けとして表された最小の全体的 SOF 要件は、すべての非暗号、確率的または順列的メカニズムに適用される。ただし、個々のメカニズムは、全体的 SOF 要件を満たすまたは要件を越える数値尺度として表された SOF 主張を持つことができる。
- 1704 SOF 分析は、ST でなされた SOF 主張を正当化する根拠からなる。
- AVA_SOF.1.1C 及び AVA_SOF.1.2C
- 4:AVA_SOF.1-3 評価者は、分析を裏付ける主張または前提条件のいずれもが正当であることを決定するために、SOF 分析を**検査しなければならない**。

- 1705 例えば、擬似乱数ジェネレータの特定の実装が SOF 分析が関係するセキュリティメカニズムにシードする必要がある要求されるエントロピーを持っているというのは無効な想定である。
- 1706 ワーストケースが ST により無効にされない限り、SOF 分析を裏付ける前提条件には、このワーストケースを反映するべきである。多数の異なる可能なシナリオが存在し、これらが人間の利用者または攻撃者に依存する場合、すでに述べたように、このケースが無効にされない限り、最小の強度を表すケースが想定されるべきである。
- 1707 例えば、最大の論理的パスワードスペースに基づく強度の主張（すなわち、すべての印刷可能な ASCII 文字）は、自然言語パスワードを使用してパスワードスペース及び関係する強度を効果的に減らすのが人間のふるまいであるために、ワーストケースとはならない。ただし、自然言語パスワードの使用を最小にするパスワードフィルタなど、ST に識別されている IT 手段を TOE が使用する場合、そのような前提条件は、適切となる。
- 4:AVA_SOF.1-4 評価者は、分析を裏付けるアルゴリズム、原理、特性及び計算が正しいことを決定するために、SOF 分析を **検査しなければならない**。
- 1708 このワークユニットの本質は、考慮されているメカニズムのタイプに大きく依存する。附属書 B.8 は、パスワードメカニズムを使用して実装される識別と認証の機能の SOF 分析の例を示している。分析は、最大のパスワードスペースが最後に SOF レート付けに到達すると考える。生物的尺度に対して、分析は、メカニズムのスプーフィング（偽造）されやすさに影響を与える解決策とその他の要因を考慮するべきである。
- 1709 レート付けとして表される SOF は、セキュリティメカニズムを打ち負かすために必要となる最小の攻撃能力に基づく。SOF レート付けは、CC パート 1 用語集の攻撃能力に関して定義されている。
- 1710 攻撃能力のガイダンスについては、附属書 B.8 を参照のこと。
- 4:AVA_SOF.1-5 評価者は、各 SOF 主張が満たされているかまたは越えていることを決定するために、SOF 分析を **検査しなければならない**。
- 1711 SOF 主張のレート付けのガイダンスについては、附属書 B.8 を参照のこと。
- 4:AVA_SOF.1-6 評価者は、SOF 主張を持つすべての機能が ST に定義されている最小強度レベルを持つことを決定するために、SOF 分析を **検査しなければならない**。
- 8.10.2.4.2 アクション AVA_SOF.1.2E
- 4:AVA_SOF.1-7 評価者は、すべての確率的または順列的メカニズムが SOF 主張を持つことを決定するために、機能仕様、上位レベル設計、下位レベル設計、利用者ガイダンス及び管理者ガイダンスを **検査しなければならない**。
- 1712 確率的または順列的メカニズムによって実現されるセキュリティ機能の開発者による識別は、ST 評価中に検証される。ただし、TOE 要約仕様はその活動を行うために使用可能な唯一の証拠である場合、そのようなメカニズムの識別は不完全なこと

がある。このサブアクティビティへの入力として必要な追加の評価証拠は、ST にまだ識別されていない追加の確率的または順列的メカニズムを識別することができる。その場合、ST は、追加の SOF 主張を反映するために適切に更新する必要がある。また、開発者は、評価者アクション AVA_SOF.1.1E への入力としての主張を正当化する追加の分析を提供する必要がある。

4:AVA_SOF.1-8 評価者は、SOF 主張が正しいことを決定するために、その主張を **検査しなければならない**。

1713 SOF 分析に主張または前提条件（例えば、毎分可能な認証の試みの数）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に確認すべきである。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。

8.10.3 脆弱性分析の評価 (AVA_VLA.2)

8.10.3.1 目的

1714 このサブアクティビティの目的は、TOE が、その意図する環境において、攻撃能力の低い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。

8.10.3.2 適用上の注釈

1715 このサブアクティビティでの用語「ガイダンス」(*guidance*)の使用は、利用者ガイダンス、管理者ガイダンス、セキュアな設置、生成及び立上げ手順を意味する。

1716 悪用される可能性のある脆弱性の考えは、ST のセキュリティ対策方針と機能要件によって決まる。例えば、セキュリティ機能がバイパスされるのを阻止するための手段が ST で必要とされない場合 (FPT_PHP, FPT_RVM と FPT_SEP が存在しない) バイパスに基づく脆弱性は、考慮されるべきでない。

1717 脆弱性は、公知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 つの局面は、関係しているが、別のものである。脆弱性が公知になってい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。

1718 次の用語は、ガイダンスで特定の意味で使用される。

- a) 脆弱性 (*vulnerability*) - ある環境のセキュリティ方針を破るために使用されることがある TOE の弱点。
- b) 脆弱性分析 (*vulnerability analysis*) - TOE の脆弱性の系統的な探索、及び TOE の意図される環境との関係を決定するための発見されたこれらの評価。
- c) 明らかな脆弱性 (*obvious vulnerability*) - TOE、技術的精巧さ及び資源の最小の理解が必要となる、悪用される可能性のある脆弱性。
- d) 潜在的脆弱性 (*potential vulnerability*) - TOE において、(仮定される攻撃経路によって) 存在が疑われるが、確認のない脆弱性。
- e) 悪用可能脆弱性 (*exploitable vulnerability*) - TOE の意図する環境で悪用される可能のある脆弱性。
- f) 悪用不能脆弱性 (*non-exploitable vulnerability*) - TOE の意図する環境で悪用される可能性のない脆弱性。
- g) 残存脆弱性 (*residual vulnerability*) - TOE の意図する環境で予想される以上の攻撃能力を持つ攻撃者が悪用できない、悪用される可能性のない脆弱性。
- h) 侵入テスト (*penetration testing*) - TOE の意図する環境での識別された TOE の潜在的脆弱性の悪用される可能性を検査するために行われるテスト。

8.10.3.3 入力

1719 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) 上位レベル設計
- d) 下位レベル設計
- e) 実装表現のサブセット
- f) TOE セキュリティ方針モデル
- g) 利用者ガイダンス
- h) 管理者ガイダンス
- i) セキュアな設置、生成、及び立上げの手順
- j) 脆弱性分析
- k) 機能強度の主張分析
- l) テストに適した TOE

1720 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) 明らかな脆弱性に関する現在の情報（監督者からの）

8.10.3.4 評価者アクション

1721 このサブアクティビティは、次の 5 つの CC パート 3 評価者アクションエレメントからなる。

- a) AVA_VLA.2.1E
- b) AVA_VLA.2.2E
- c) AVA_VLA.2.3E
- d) AVA_VLA.2.4E
- e) AVA_VLA.2.5E

8.10.3.4.1 アクション AVA_VLA.2.1E

AVA_VLA.2.1C 及び AVA_VLA.2.2C

4:AVA_VLA.2-1 評価者は、脆弱性に対する探索がすべての該当する情報を考慮したことを決定するために、開発者の脆弱性分析を**検査しなければならない**。

1722 開発者の脆弱性分析は、少なくともすべての評価用提供物件と公知になっている情報源において、脆弱性に対する開発者の探索を扱うべきである。

4:AVA_VLA.2-2 評価者は、識別された各脆弱性が記述されていること及び TOE の意図する環境でそれが悪用されることがない理由に対する根拠が示されていることを決定するために、開発者の脆弱性分析を**検査しなければならない**。

1723 脆弱性は、次の 1 つまたはいくつかの条件が存在する場合、悪用される可能性がないと呼ばれる。

- a) (IT または IT 以外の) 環境のセキュリティ機能または手段が意図する環境の脆弱性の悪用を阻止する。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 TOE の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。
- b) 脆弱性は、悪用可能であるが、攻撃能力が中程度または高い攻撃者のみが悪用可能。例えば、セッションハイジャック攻撃への分散 TOE の脆弱性は、低を超えた攻撃能力を必要とする。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。
- c) 脅威に対抗すると主張されていないか、または違反可能な組織のセキュリティ方針が ST により達成されると主張されていない。例えば、ST が利用可能方針の主張を行わず、TCP SYN 攻撃 (ホストが接続要求サービスを行えないようにする共通のインターネットプロトコルへの攻撃) を受けやすいファイアウォールは、この脆弱性だけでこの評価者のアクションに不合格とするべきでない。

1724 脆弱性を悪用するために必要な攻撃能力の決定のガイダンスについては、附属書 B.8 を参照のこと。

4:AVA_VLA.2-3 評価者は、開発者の脆弱性分析が ST 及びガイダンスと一貫していることを決定するために、その分析を**検査しなければならない**。

1725 開発者の脆弱性分析は、TOE 機能に対する特定の構成または設定を示して、脆弱性に対処することができる。そのような運用上の制約が効果的であり、ST と一貫していると思われる場合、消費者がそれらを採用できるように、そのようなすべての構成と設定がガイダンスに満たされるように記述されるべきである。

8.10.3.4.2 アクション AVA_VLA.2.2E

4:AVA_VLA.2-4 評価者は、開発者の脆弱性分析に基づいて、侵入テストを**考え出さなければならない**。

1726 評価者が侵入テストを準備するのは、次の場合である。

- a) 脆弱性が悪用されることがないとの理由に対する開発者の根拠が評価者の考えでは疑わしい場合、開発者の分析に対して反証することを試みる必要がある。
- b) TOE が、意図する環境で、開発者が考慮していない脆弱性を持つことを決定する必要がある。評価者は、開発者が考慮していない明らかな公知になっている脆弱性に関する、(例えば、監督者からの) 現在の情報にアクセスを持つべきであり、また、その他の評価アクティビティの結果として識別された潜在的な脆弱性を持つことができる。

- 1727 評価者は、攻撃の攻撃能力が低い脆弱性（公知になっている脆弱性を含む）をテストすることは期待されない。ただし、多くの場合、必要な攻撃能力を決定するまえに、テストを行う必要がある。評価者の専門知識の結果として、評価者は攻撃能力が低い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。
- 1728 疑われる脆弱性を理解し、評価者は、TOE の脆弱性をテストするための最も可能性の高い方法を決定する。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セキュリティ機能インタフェース
 - b) テストに存在する必要がある初期条件（すなわち、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) セキュリティ機能を刺激するか、またはセキュリティ機能を観察するために必要となる特別のテスト装置
- 1729 評価者は、おそらく、一連のテストケースを使用して侵入テストを行うのが有用であることを見つけ出し、この場合、各テストケースは、特定の脆弱性をテストすることになる。
- 4:AVA_VLA.2-5 評価者は、開発者の脆弱性分析に基づき、テストを再現可能にするに十分な詳細さで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) テストされている TOE 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説明
 - c) すべての侵入テスト前提初期条件を確立するための説明
 - d) TSF を刺激するための説明
 - e) TSF のふるまいを観察するための説明
 - f) すべての期待される結果と、期待される結果に対応する観察されたふるまいについて実行されるべき必要な分析の記述
 - 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説明
- 1730 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繰り返し、同等の結果を得ることができるようにすることである。
- 4:AVA_VLA.2-6 評価者は、開発者の脆弱性分析に基づいて、侵入テストを**実施しなければならない**。
- 1731 評価者は、TOE の侵入テストを行うための基礎として、ワークユニット 4:AVA_VLA.2-4 の結果の侵入テスト証拠資料を使用するが、これは、評価者が追加の特別の侵入テストを行うことを排除しない。必要に応じて、評価者は、評価者が行った場合に侵入テスト証拠資料に記録される、侵入テスト中に得られた情報の結

果として特別のテストを考え出すことができる。そのようなテストは、期待されない結果または観察をどこまでも追求するか、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必要がある。

4:AVA_VLA.2-7 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**。

1732 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。相違には、いずれも正当性が示されるべきである。

4:AVA_VLA.2-8 評価者は、ETR に、テスト手法、構成、深さ及び結果を示しながら評価者の侵入テストの成果を**報告しなければならない**。

1733 ETR に報告される侵入テスト情報は、全体的な侵入テスト手法及びこのサブアクティビティから得られた成果を伝えることを評価者に許す。この情報を提供する意図は、評価者の侵入テストの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、他の評価者と監督者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。

1734 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) テストされたセキュリティ機能侵入。侵入テストの焦点となったセキュリティ機能の簡単なリスト。
- 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。

1735 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侵入テストに関する、ETR に示すべきタイプの情報を提供することだけを意図している。

8.10.3.4.3 アクション AVA_VLA.2.3E

4:AVA_VLA.2-9 評価者は、開発者の脆弱性分析でこれまでに取り扱われていない、可能性のあるセキュリティ脆弱性であることを決定するために、このサブアクティビティへのすべての入力を**検査しなければならない**。

1736 TOE の仕様及び証拠資料が分析された後、TOE の脆弱性が仮定されるかまたは推測される場合には、欠陥仮定方法論が使用されるべきである。次に、仮定された脆弱性のリストには、脆弱性が存在することの予測される確率、及び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、それがもたらす管理または攻撃能力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。

1737 脆弱性を悪用するために必要な攻撃能力の決定のガイダンスについては、附属書 B.8 を参照のこと。

- 1738 中程度から高い攻撃能力を持つ攻撃者のみが悪用可能と仮定された脆弱性は、この評価者のアクションの結果、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。
- 1739 ST に特定されているセキュリティ対策方針の違反とならない、攻撃能力の低い攻撃者が悪用できると仮定された脆弱性は、この評価者のアクションの結果、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。
- 1740 攻撃能力の低い攻撃者が潜在的に悪用可能であると仮定され、セキュリティ対策方針の違反となる脆弱性は、TOE の侵入テストを指示するために使用されるリストからな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。
- 1741 意図する環境に存在する脅威を仮定して、評価者の独立脆弱性分析は、次の各見出しの一般的な脆弱性を考慮するべきである。
- a) 監督者から提供される、評価されている TOE のタイプに関する一般的脆弱性
 - b) バイパス
 - c) 改ざん
 - d) 直接攻撃
 - e) 誤使用
- 1742 項目 b) から e) についてさらに詳しく説明する。
- バイパス
- 1743 バイパスには、攻撃者が下記によるセキュリティの実施を避けるための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) (機密が問題となる場合) 不十分な保護されている領域に格納されている、またはコピーされた機密に関するデータの読取り
- 1744 次のそれぞれ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) インタフェースとユーティリティの機能を悪用する攻撃は、通常、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ことを悪用する。例えば、アクセス制御が実施されているレベルよりも低いレベルで実施されている機能にアクセスすること。該当する要素には、次のものが含まれる。
 - 1) 機能を呼び出すための事前に定義されている順序を変更する

- 2) 追加の機能を実行する
 - 3) 期待しない状況でまたは期待しない目的に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) コンポーネントを呼び出すための事前に定義された順序を変更する必要があるのは、TOE へのインタフェース（例えば、利用者コマンド）があるセキュリティ機能（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）を実行するために呼び出される期待された順序が存在する場合であることが考慮されるべきである。セキュリティ機能が TOE のインタフェースの 1 つで呼び出される場合（例えば、アクセス制御チェック） 評価者は、シーケンスの後の点でコールを行うかまたはそれらをまったく省略することによりセキュリティ機能をバイパスすることが可能かどうかを考慮するべきである。
- c) 追加のコンポーネントを（事前に決められた順序に）実行することは、前に記述したのと同じ形の攻撃であるが、シーケンスのある点での他の TOE インタフェースの呼び出しが含まれる。 それには、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) 期待しない状況でのまたは期待しない目的のためのコンポーネントの使用には、セキュリティ機能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、達成することが設計されていないまたは意図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。 証拠資料として提出されていないインタフェース（安全でない）の使用も、このカテゴリに含まれる（これらには、証拠資料として提出されていないサポートとヘルプ機能が含まれる）。
- e) 下位表現に含められる実装詳細の使用には、再度、隠れチャネルの使用が含まれる。ここでは、攻撃者は、詳細化プロセス（例えば、隠れチャネルとしてのロック変数の使用）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。 追加の機能は、ソフトウェアモジュールに含まれるテストハルネス(test harness)コード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、アクセス制御チェックが行われ、アクセスが許され、次に攻撃者が、アクセスチェックが行われたときに適用された場合、チェックが不合格になった条件を作ることができるシナリオが含まれる。例としては、バックグラウンドプロセスを作成し、より高い機密に関するデータを読み取り、利用者端末に送り、次にログアウトし、再度、低いセンシビリティレベルでログバックする利用者がいる。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、MAC のチェックは効果的にバイパスされたかもしれない。
- 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コンポーネントを終了することにより、権限を持ついくつかのコンポーネ

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。該当する要素には、次のものが含まれる。

- 1) 実行可能であることを意図し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依存する前提条件及び特性を無効にする。
- h) 実行可能であることを意図し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ファイルに実行可能コードまたはコマンドを入れ、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想されない影響を与えることができる。例えば、下層のオペレーティングシステムへのアクセスを入手する場合、TOE が、バイパスすることができるセキュリティ機能を実装しているアプリケーションである場合、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を入手することができる。
- 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、アプリケーションが実装するセキュリティ機能をバイパスするために下層のオペレーティングシステムへのアクセスを得るためにアプリケーションの制約から抜け出す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入手することはできないとの前提条件は、無効となる。セキュリティ機能が下層のデータベース管理システムにアプリケーションによって実装されている場合、同様の攻撃を想像することができる。攻撃者がアプリケーションの制約を抜け出す場合、セキュリティ機能はバイパスすることができる。
- k) 偶然に保護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可能な手段として考慮されるべき次の問題が含まれる。
- 1) ディスクの残存情報から盗む
 - 2) 保護されていないメモリへのアクセス
 - 3) 共有書込み可能ファイルまたはその他の共有資源（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、ラベルなしにディスク上に存在するヘッダのないファイルに対して消失ディレクトリと検出ディレクトリを採用することができる。TOE が必須アクセス制御(Mandatory Access Control)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誰がアクセスするかを検査するのは重要である。

改ざん

1745 改ざんには、例えば、次のことによる、セキュリティ機能またはメカニズムのふるまいに攻撃者が影響を与える（破壊または非活性化）攻撃が含まれる。

- a) セキュリティ機能またはメカニズムがその機密性または完全性に依存する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行わせないかまたは遅らせる。

1746 次のそれぞれ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) セキュリティ機能またはメカニズムにデータの機密性または完全性が含まれ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、または変更する。
 - 2) 期待しない場面でまたは期待しない目的に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の間の干渉を使用する。
- b) 直接または間接的な内部データの読み取り、書き込み、または変更には、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依存する内部データをだます。
 - 3) 構成ファイルまたは一時ファイルの環境変数（例えば、論理名）またはデータを変更する。
- c) 信頼されたプロセスをだまし、通常はアクセスしない保護されたファイルを変更させることが可能である。
- d) 評価者は、次の「危険な特性」も考慮するべきである。
 - 1) コンパイラとともに TOE に常駐するソースコード（例えば、ログインソースコードを変更することが可能）
 - 2) 対話式デバッガ及びパッチ機能（例えば、実行可能イメージを変更することが可能）
 - 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) 期待しない場面または期待しない目的にコンポーネントを使用することには、（例えば）TOE がアプリケーションシステムの上に作られている場合、（例えば、これまで以上に大きな権限を獲得するために）自己のコマンドファイルを変更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する利用者が含まれる。
- f) 抽象の上位レベルでは見えないコンポーネントの間の干渉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が含まれる。その場合、1 つのコンポーネントによる資源の変更は、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、例えば、ソースコードレベルで他の（信頼された）コンポーネントのふるまいに干渉することができる。
- 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。該当する要素には、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依存する前提条件及び特性を無効にする。
- 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 のふるまいを検査することが含まれる。
- 1) コマンド入力バッファオーバーフロー（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の上書き。攻撃者は、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を悪用するかまたは強制することができる）。
 - 2) 無効な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への読取り専用パラメタを提供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（例えば、CTRL/Z または CTRL/D）または null 文字。
- i) 下位レベルが依存する前提条件及び特性を無効にすることには、セキュリティに関係するデータが特定の形式をしていることまたは特定の範囲の値であることをコードが（明示的または暗黙に）想定する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べきである。
- j) セキュリティ機能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されるとの前提条件に依存することができる。評価者は、（実際的な場合）次に示すような限度に達したときの TOE のふるまいを考慮すべきである。

- 1) 日付の変更（例えば、クリティカルな日付のしきい値を過ぎたとき、どのように 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する。
 - 6) 通信コンポーネントに大きく依存する複数利用者 TOE の各種の部分がオーバーロードしている。
 - 7) トラフィックによるネットワークまたは個別ホストのスワッピング
 - 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行わせないか、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の割り込みまたはスケジューリング機能の使用
 - 2) 同時性を混乱させる
 - 3) 抽象の上位レベルで見えないコンポーネントの間の干渉を使用
- 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、次のときの 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) セキュリティに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、管理者には役に立たないために（攻撃はすでに成功しているために）、監査レコードのログまたはアラームの発行または受取りを遅らせることができる。
- 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するときの 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することができるが、さらにサブジェクトが存在するときのふるまいの定義が明確でなくなることがある。例えば、2 つの他のプロセスがクリティカルセキュリティプロセスが必要とする資源にアクセスするとき、クリティカル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見えないコンポーネントの間の干渉の使用は、時間がクリティカルな信頼されたプロセスを遅らせる手段を提供することがある。

直接攻撃

- 1747 直接攻撃には、機能の主張された最小の強度を確認するかまたは反証をあげるために必要な侵入テストの識別が含まれる。この見出しのもとに侵入テストを識別するとき、評価者は、また、セキュリティメカニズムが直接攻撃を受ける結果として存在する脆弱性の可能性を理解するべきである。

誤使用

- 1748 誤使用には、誤使用分析を確認するかまたは反証をあげるために必要な侵入テストの識別が含まれる。考慮する必要がある問題には、次のものがある。
- 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（ときには、オーバロードまたは漸近的ふるまいと呼ばれる）での TOE のふるまい。特にこの場合、セキュリティ実施機能またはメカニズムが非活性化または使用不能状態になることがある。
 - c) 上記の改ざんの節に記述されている攻撃による意図しない誤構成または安全でない使用の可能性。

8.10.3.4.4 アクション AVA_VLA.2.4E

4:AVA_VLA.2-10 評価者は、独立脆弱性分析に基づいて、侵入テストを **考え出さなければならない**。

- 1749 評価者は、評価者アクション AVA_VLA.2.3E で仮定した脆弱性の優先度の付けられたリストに基づいて、侵入テストを準備する。
- 1750 評価者は、攻撃能力の低い攻撃に対する脆弱性を越える脆弱性をテスト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、攻撃能力が低い攻撃者のみが悪用できる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。
- 1751 疑われる脆弱性を理解し、評価者は、TOE の脆弱性をテストするための最も可能性の高い方法を決定する。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セキュリティ機能インターフェース
 - b) テストに存在する必要がある初期条件（すなわち、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) セキュリティ機能を刺激するかまたはセキュリティ機能を観察するために必要となる特別のテスト装置
- 1752 評価者は、おそらく、一連のテストケースを使用して侵入テストを行うのが有用であることを見つけ出し、この場合、各テストケースは、特定の脆弱性をテストすることになる。

4:AVA_VLA.2-11 評価者は、独立脆弱性分析に基づき、テストを再現可能にするに十分な詳細さで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) テストする TOE の明らかな脆弱性の識別
- 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説明
- c) すべての侵入テスト前提初期条件を確立するための説明
- d) TSF を刺激するための説明
- e) TSF のふるまいを観察するための説明
- f) すべての期待される結果と、期待される結果に対応する観察されたふるまいについて実行されるべき必要な分析の記述
- 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説明

1753 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繰り返し、同等の結果を得ることができるようにすることである。

4:AVA_VLA.2-12 評価者は、独立脆弱性分析に基づいて、侵入テストを**実施しなければならない**。

1754 評価者は、TOE の侵入テストを行うための基礎として、ワークユニット AVA_VLA.2-10 の結果の侵入テスト証拠資料を使用するが、これは、評価者が追加の特別の侵入テストを行うことを排除しない。必要に応じて、評価者は、評価者が行った場合に侵入テスト証拠資料に記録される、侵入テスト中に得られた情報の結果として新しいテストを考え出すことができる。そのようなテストは、期待されない結果または観察をどこまでも追求するか、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必要がある。

1755 侵入テストが仮定される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べきである。

4:AVA_VLA.2-13 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**。

1756 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。相違には、いずれも正当性が示されるべきである。

4:AVA_VLA.2-14 評価者は、ETR に、テスト手法、構成、深さ及び結果を示しながら評価者の侵入テストの成果を**報告しなければならない**。

1757 ETR に報告される侵入テスト情報は、全体的な侵入テスト手法及びこのサブアクティビティから得られた成果を伝えることを評価者に許す。この情報を提供する意図は、評価者の侵入テストの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、他の評価者と監督者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。

1758 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) テストされたセキュリティ機能侵入。侵入テストの焦点となったセキュリティ機能の簡単なリスト。
- 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。

1759 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侵入テストに関する、ETR に示すべきタイプの情報を提供することだけを意図している。

8.10.3.4.5 アクション AVA_VLA.2.5E

4:AVA_VLA.2-15 評価者は、TOE が、意図する環境において、低い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とすべての脆弱性分析の結論を**検査しなければならない**。

1760 TOE が、その意図する環境において、中程度以下の攻撃能力を持つ攻撃者によって悪用され得る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。

4:AVA_VLA.2-16 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採用された CEM アクティビティ、評価者に既知である、公開されたもので読んでいる、など）
- b) 影響のあるセキュリティ機能、達成されない対策方針、侵害される組織のセキュリティ方針及び顕在化される脅威
- c) 説明
- d) 意図する環境で悪用されるか否か（すなわち、悪用され得るか残存か）
- e) 脆弱性を識別した評価の関係者（例えば、開発者、評価者）の識別

附属書 A 用語集

1761 この附属書は、CEM で使用されている省略語、頭字語及び用語を示す。ただし、ここには、CC にすでに示された用語は含まれていない。この附属書は、CEM で使用されている参照資料も表す。

A.1 省略語及び頭字語

1762 CEM 情報技術セキュリティ評価のための共通方法論 (Common Methodology for Information Technology Security Evaluation)

1763 ETR 評価報告書 (Evaluation Technical Report)

1764 OR 所見報告書 (Observation Report)

A.2 用語

1765 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。

1766 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、マッピングされているものを記述する。

1767 評価用提供物件 (Evaluation Deliverable):

1 つまたはいくつか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監督者がスポンサーまたは開発者に要求する任意の資源。

1768 評価証拠 (Evaluation Evidence):

有形の評価用提供物件。

1769 評価報告書 (Evaluation Technical Report):

総合判定及びその正当化を文書化した報告書。評価者が作成し、監督者に提出される。

1770 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、分析されているものと分析のための特性を識別する。

1771 解釈 (Interpretation):

CC、CEM または制度要件の明確化または拡充。

1772 方法論 (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。

- 1773 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。
- 1774 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。
- 1775 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を確認または拒否する、監督者が出すステートメント。
- 1776 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。
- 1777 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。
- 1778 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論など、評価環境を定義する。
- 1779 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。
- 1780 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。

A.3 参照資料

- CC** **Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.**
- COD** **Concise Oxford Dictionary, Oxford University Press, Ninth edition, 1995.**
- IEEE** **IEEE Standard Glossary of Software Engineering Terminology, ANSI/IEEE STD 729-1983.**

附属書 B 一般的评价ガイドンス

B.1 目的

1781 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ドンスを扱うことである。そのような一般的ガイドンスの使用は、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。

B.2 サンプリング

1782 この節は、サンプリングの一般的なガイドンスを提供する。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。

1783 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。

1784 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。

1785 CC は、サンプリングが明示的に受け入れられる、次の評価者アクション要素を識別する。

- a) ADV_RCR.3.2E: 「評価者は、形式的な分析を選択的に検証することによって、対応の証明の正確さを決定しなければならない。」
- b) ATE_IND.*.2E: 「評価者は、TSF のサブセットを、TOE が仕様どおりに動作することを確認するために、適切にテストしなければならない。」
- c) ATE_IND.2.3E: 「評価者は、開発者テスト結果を検証するために、テスト証拠資料内のテストのサンプルを実行しなければならない。」
- d) AVA_CCA.*.3E: 「評価者は、テストによって、選択的に隠れチャネル分析の正当性を確認しなければならない。」

- e) AVA_MSU.2.2E 及び AVA_MSU.3.2E: 「評価者は、提出されたガイダンス証拠資料だけを使って、すべての構成、導入手順、及びその他の手順を選択的に再現し、TOE がセキュアに構成され使用されることを確認しなければならない。」
- f) AMA_SIA.1.2E: 「評価者は、サンプリングにより、セキュリティ影響分析が、TOE の現行バージョンで保証が維持されていることの適切な正当性ととも、変更について、適切な詳細レベルまで証拠資料を提供していることをチェックしなければならない。」

1786 さらに、ADV_IMP.1.1D は、開発者が TSF のサブセットについてのみ実装表現を提供することを要求する。サブセットのサンプルは、評価者の同意のもとで選択されるべきである。実装表現のサンプルの提供により、評価者は、実装表現自体の提示を評価し、下位レベル設計と実装表現の間の対応の保証を得るための、追跡性の証拠をサンプリングすることができる。

1787 CC が受け入れるサンプリングに加えて、CEM は、サンプリングが受け入れられるところで次のアクションを識別する。

- a) アクション ACM_CAP*.1E: 「評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。」

ここで、サンプリングは、EAL3 と EAL4 に対する証拠要素 ACM_CAP*.8C と ACM_CAP*.9C の内容と表現に対して受け入れられる。

- b) アクション ATE_FUN.1.1E: 「評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。」

ここで、サンプリングは、EAL2、EAL3 及び EAL4 に対する証拠要素 ATE_FUN.1.3C、ATE_FUN.1.4C、及び ATE_FUN.1.5C の内容と表現に対して受け入れられる。

- c) アクション ALC_DVS.1.1E: 「評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。」

ここで、サンプリングは、EAL3 と EAL4 に対する証拠要素 ALC_DVS.1.2C の内容と表現に対して受け入れられる。

1788 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。

附属書 B 一般的评价ガイドンス

- 1789 サンプルングは、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、サンプルングの結果として除かれるものに依存する。サンプル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。
- 1790 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）のサンプルングは、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ル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、サンプルング方策が推奨されていることを決定する必要がある。ここでの手法は、開発者のテスト結果をサンプルングするときの方法とは異なる。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。
- 1791 次の原則が、サンプルングを行うときには、必ず従うべきである。
- a) サンプルングサイズは、評価の費用効果と釣り合い、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）の総数に依存するべきであるが、TOE 実装に関する材料のサンプルングに対しては 20%の最低サイズをノルマとして採用されるべきである。ここでは、プロセス（例えば、訪問者の管理または設計レビュー）が守られていることの証拠を得ることに関係するサンプルングは、パーセント値は適切でない、そして手続きが守られていることの合理的な確信を得るために評価者が十分な情報をサンプルングするべきである。サンプルサイズには、根拠を示す必要がある。
 - b) サンプルは、サンプル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、セキュリティ機能、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。
 - c) 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資料、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。
 - d) 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。
- 1792 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。

B.3 一貫性分析

1793 この節は、一貫性分析の一般的なガイダンスを提供する。一貫性分析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。

1794 一貫性分析は、評価者の定義された手順である。そこでは、評価用提供物件の特別な部分それ自体が分析される（内部的に一貫している）か、または 1 つまたは複数の他の評価用提供物件と比較される。

1795 CC は、異なる種類の一貫性分析を区別している。

a) 評価者は、評価用提供物件の内部的一貫性を分析する必要がある。例えば、

- ADV_FSP.1.2C: 「機能仕様は、内部的に一貫していなければならない。」
- ADV_HLD.1.2C: 「上位レベル設計は、内部的に一貫していなければならない。」
- ADV_IMP.1.2C: 「実装表現は、内部的に一貫していなければならない。」
- ADV_LLD.1.2C: 「下位レベル設計は、内部的に一貫していなければならない。」

内部的一貫性分析を行うとき、評価者は、提供される提供物件に曖昧な点が含まれていないことを保証する必要がある。評価用提供物件の異なる部分に矛盾する説明が含まれているべきでない。例えば、同じ証拠の非形式的、準形式的、または形式的表現は、相互に一致しているべきである。

評価者は、評価用提供物件のいくつかの部分が別々の文書の中に存在することを考慮すべきである（例えば、セキュアな設置、生成、及び立上げの手順は、3 つの異なる文書に存在することがある）。

b) 評価者は、評価用提供物件が 1 つまたは複数の他の提供物件と一貫性があることを分析する必要がある。例えば、

- AGD_ADM.1.7C: 「管理者ガイダンスは、評価のために提供された他のすべての証拠資料と一貫していなければならない。」
- AGD_USR.1.5C: 「利用者ガイダンスは、評価のために提供された他のすべての証拠資料と一貫していなければならない。」

この一貫性分析では、評価者は、1 つの文書に含まれている機能、セキュリティパラメタ、手順、及びセキュリティ関連事象の記述が評価のために提供された他の文書に含まれている記述と一貫していることを検証する必要がある。これは、評価者が他の情報源との起こりうる不一致を考慮するべきことを意味する。例を次に示す。

- セキュリティ機能の使用についての他のガイドラインと不一致
- ST と不一致（例えば、脅威、セキュアな使用の前提条件、IT 以外のセキュリティ対策方針、または IT セキュリティ機能）
- 機能仕様または下位レベル設計の記述と、一致していないセキュリティパラメタの使用

附属書 B 一般的評価ガイダンス

- 上位レベルまたは下位レベル設計文書に示されている情報に関して、一致していないセキュリティ関連事象の記述
 - 非形式的 TSP モデルとセキュリティ実施機能の矛盾
- c) 評価者は、評価用提供物件が内部的に一貫性があること、及び評価用提供物件が他の提供物件と一貫性があることの両方を分析する必要がある。例えば、
- AVA_MSU.1.2C: 「ガイダンス証拠資料は、完全で、明白で、矛盾なく、合理的なものでなくてはならない。」

ここでは、ガイダンスは全体として、一貫性の要件を満たす必要がある。そのようなガイダンス証拠資料が 1 つの文書に含まれているか、または多くの別々の文書に含まれているとすれば、この要件は、文書内及び文書間のすべてのガイダンスに渡って、の一貫性に及ぶ。

- d) 開発者によって提供される一貫性を実証する必要がある分析を、評価者はチェックする必要がある。例えば、
- ADV_SPM.1.3C: 「TSP モデルは、モデル化できるすべての TSP 方針に関して、一貫し完全であることを実証する根拠を含まなければならない。」
 - ADV_SPM.1.4C: 「TSP モデルと機能仕様の間に対応の実証は、機能仕様におけるセキュリティ機能のすべてが、TSP モデルに関して、一貫し完全であることを示さなければならない。」

これらの場合、一貫性の証拠を提示する必要があるのは、開発者である。ただし、評価者は、必要に応じて、おそらく独立分析を実施し、この分析を理解し、その一貫性を確認する必要がある。

- 1796 一貫性分析は、評価用提供物件を検査することによって行うことができる。評価者は、文書の一貫性分析に合理的で構造化された手法を採用するべきであり、他のワークユニットの一部として行われる、マッピングまたは追跡性のような、他のアクティビティと一緒にすることができる。評価者は、形式的記述（もしあれば）を使用することにより、検出された不一致をいずれも分析することができる。同様に、形式的表記ほど正確ではないが、提供物件の準形式的表記の使用は、提供物件の曖昧な点を減らすために使用することができる。
- 1797 曖昧さは、例えば、不一致な説明から明示的にまたは説明が十分に正確でないときに暗黙的に生じることがある。冗長なことは、それ自体、一貫性の基準に対する不合格判定を想定する十分な理由とはならないことに注意すべきである。
- 1798 提供物件の一貫性チェックでは、すでに実施されたワークユニットのやり直しを必要とするかもしれない漏れを重視する。例えば、セキュリティ対策方針の一貫性チェックは、1 つまたは複数のセキュリティ要件の漏れを識別することができる。このような場合、評価者は、セキュリティ対策方針と TSF の間に対応をチェックするべきである。

B.4 依存性

1799 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、任意の順序に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ドンスを提供する。

B.4.1 アクティビティの間の依存性

1800 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 が TOE 評価アクティビティを行うための基礎と状況を提供するために、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の結果、ST への変更が行われるために、TOE 評価が完了するまで可能ではない。

B.4.2 サブアクティビティの間の依存性

1801 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。この種の依存性の例は、AVA_VLA.1 である。このコンポーネントは、ADV_FSP.1、ADV_HLD.1、AGD_ADM.1 及び AGD_USR.1 への依存性を主張している。

1802 サブアクティビティには、それが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、合格判定を出すことができる。例えば、AVA_VLA.1 への合格判定は、通常、ADV_FSP.1、ADV_HLD.1、AGD_ADM.1 及び AGD_USR.1 に関係するサブアクティビティに合格判定が出されたときのみ出すことができる。

1803 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。

1804 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出すことは、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。

B.4.3 アクションの間の依存性

1805 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。

B.5 サイト訪問

- 1806 この節は、サイト訪問の一般的なガイダンスを提供する。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) ACM_AUT
 - b) ACM_CAP.n (ここで、 $n > 2$)
 - c) ADO_DEL
 - d) ALC_DVS
- 1807 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。
- 1808 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のを観察するため
 - b) 配付手続きが実際に適用されているのを観察するため
 - c) 開発の期間中、セキュリティ手段が適用されているのを観察するため
- 1809 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うことができることが考慮されるべきである。
- 1810 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、早い段階でのサイト訪問は、適用される手続きに重大な欠陥が現れる場合、修正処置を講じることが可能となる。これにより、不要な評価努力を避けることができる。
- 1811 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べきである。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。
- 1812 サイト訪問を準備するとき、評価者は、提供された評価証拠に基づいてチェックリストを作成するべきである。サイト訪問の結果は、記録されるべきである。

- 1813 サイト訪問は、例えば、開発サイトが他の TOE 評価のためにか、または特定の ISO 9000 手続きが守られていることを確認するために最近訪問されている場合、必要と見なさなくてもよい。確信を得るための他の手法が、同等の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、監督者と相談して行われるべきである。

B.6 TOE 境界

- 1814 評価されたものの識別は、ETR、認証書、ST、及び評価済み製品のリストに現れる。「製品」(*products*) は、通常、購入されたり、販売されたりするが、評価は、TOE に関係する。製品の開発者が評価証拠の開発者（すなわち、スポンサー）でもある場合、これを区別することは不要である。ただし、これらの役割は、異なる当事者が果たすために、次のことが、評価と認証への相互関係と影響とともに、CEM で使用されている定義に基づいて合意されている。

B.6.1 製品及びシステム

- 1815 「製品」(*product*) は、使用するために提供されるハードウェア及び/またはソフトウェアの集まりである。ある調達者は、製品のセット（例えば、ワードプロセッサ、スプレッドシート、及びグラフィックスアプリケーション）を他の製品（例えば、オフィスオートメーションシステム）にバンドルしている。ただし、一般の人々、他の製造者、または限られた顧客のいずれかが使用するために、それが提供される場合、その結果のセットは、製品であるとみなされる。
- 1816 「システム」(*system*) は、明らかにされている運用環境での 1 つまたは複数の製品で構成される。製品の評価とシステムの評価との主な相違は、システムの評価には、評価者は、製品の評価に行われるような仮定の環境を理論づけるのではなく、実際の環境を考慮することである。

B.6.2 TOE

- 1817 TOE は、ST の定義に従って評価されるエンティティである。TOE が製品全体を構成する場合もあるが、そのようである必要はない。TOE は、特定の構成または構成のセットの中の、製品、製品の一部、製品のセット、製品にならない固有な技術、またはそれらのすべての組み合わせにすることもできる。この特定の構成または構成のセットは、「評価済み構成」(*evaluated configuration*) と呼ばれる。ST は、TOE とあらゆる関連する製品との関係を明確に記述する。

B.6.3 TSF

- 1818 TSF は、ST に定義されている TOE のセキュリティを実施する TOE 内部のそれらの機能の集まりである。TOE の内部には ST が定義する TOE のセキュリティになにも貢献しない機能が存在することがある。従って、そのような機能は、TSF の一部ではない。

B.6.4 評価

- 1819 すべての評価で、TOE が（定義により）評価される構成の製品またはシステムであるとの暗黙の前提がなされる。この前提を評価のための前提条件のリストに明示

的に含める必要はない。TOE は、評価の厳重な検査を受ける。分析は、評価される構成内だけで行われ、テストは、この評価された構成に対して行われ、悪用される可能性のある脆弱性が、この評価された構成に識別され、前提条件は、評価された構成でのみ適切である。TOE がこの構成から外れうることの容易さは重大であり、AVA_MSU が選択されるところでは考慮しなければならない。これは、TOE 構成の堅牢性、及び検出されることなく起きることがある偶発的または意図的な TOE 構成からの逸脱の影響を考察する。

1820 次の例は、同じバーチャルプライベートネットワーク (VPN) ファイアウォール製品に基づいているすべてが、ST での相違のために異なる評価結果を生じる 3 つの TOE を示している。

1821 **1) VPN 機能がオフになるように構成されている VPN ファイアウォール。ST のすべての脅威は、安全でないネットワークからセキュアなネットワークへのアクセスに関するものである。**

1822 TOE は、VPN 機能がオフになるように構成された VPN ファイアウォールである。管理者が VPN 機能の一部またはすべてが使用されるようにファイアウォールを構成した場合、製品は、評価された構成ではなくなり、そのために、評価されていないとみなされ、セキュリティについて、何も述べることはできない。

1823 **2) ST のすべての脅威は、安全でないネットワークからセキュアなネットワークへのアクセスに関するものである VPN ファイアウォール。**

1824 TOE は、VPN ファイアウォール全体である。VPN 機能は、TOE の一部であるため、評価中に決定する必要があることの 1 つは、VPN 機能を通して安全でないネットワークからセキュアなネットワークへアクセスする手段が存在するかどうかである。

1825 **3) ST のすべての脅威は、安全でないネットワークからセキュアなネットワークへのアクセスまたは安全でないネットワークのトラフィックの信頼性に関するものである VPN ファイアウォール。**

1826 TOE は、VPN ファイアウォール全体である。VPN は、TOE の一部であるため、評価中に決定する必要があることの 1 つは、VPN 機能が ST に記述されている脅威のいずれかの実現を許すかどうかである。

B.6.5 認証

1827 これまでの段落から、ST が異なる同じ製品の評価は、TSF が異なる TOE となることは明らかである。その結果、認証、ETR、ST、及び評価済み製品リストのエントリは、潜在的な顧客にとって役に立つ評価の間で異なるものとなる。

1828 上記の 3 つの異なるファイアウォール評価の例に対して、これらの認証の間の明らかな相違は、3 つの VPN ファイアウォールがすべて次のように TOE を識別する認証となるために、微妙なものとなることに注意すること。

セキュリティターゲット #ABC に識別されている評価済み構成に記述されている、XYZ ファイアウォール製品。

1829 各 ST ABC の識別情報は異なる。

1830 そこで、評価者は、ST が評価の範囲内での機能の観点から TOE を適切に記述していることを保証する必要がある。評価済み製品を購入しようとする顧客は、それらの製品の評価されているセキュリティ機能を決定するために、購入することを考えている製品の ST を参照するために、明確な説明が重要である。

B.7 脅威及び FPT 要件

1831 PP/ST 作成者は、脅威（脅威の観点からは、悪意のある利用者の脅威と TSF の外部インタフェースを通して悪用される可能性のある正しくない実装からの脅威は区別されない）を識別し、FPT_PHP、FPT_SEP、及び/または FPT_RVM を PP/ST に含めるかまたは排除するかどうかを決定するために、これらを使用する。つまり、これらの要件のファミリのすべては、物理的な改ざん(tampering)、利用者の干渉、またはバイパスによる TOE への脅威を前提としている。

- a) TSF の保護の要件は、TOE の環境の説明に直接関係している。改ざんまたはバイパスの脅威が言及されている場合、この脅威に対処するための明示的または暗黙の手段が、TOE またはその環境のいずれかにより提供されなければならない。
- b) 改ざんまたはバイパスの脅威は、一般的に、信頼できないサブジェクト（一般的に人間の利用者）が TOE 環境に存在すること、及び TOE が保護する意向の資産を攻撃する動機が存在することによって示される。
- c) PP/ST のセキュリティ要件の説明を評価するとき、評価者は、セキュリティ対策方針を満たすために TSF 保護が必要となることを決定する。この必要性がすでに確認されている場合、セキュリティ対策方針を満たすための機能要件の存在をチェックする。保護の必要性が識別されているときに、そのような保護が TOE またはその環境によって提供されていない場合、PP/ST 評価サブアクティビティ APE/ASE_REQ には、不合格の判定が下される。

1832 セキュリティ方針を実施することができる場合、TOE に対するなんらかの形の保護が存在しなければならない。結局、TSF が不正行為(corruption)から保護されていない場合、その方針実施機能が期待とおりに実行される保証はない。

1833 この保護は、いろいろな方法で提供することができる。TOE への機能の豊富な（プログラミング）インタフェースを持つ複数の利用者が存在するオペレーティングシステムでは、TSF は、自分自身を保護できなければならない。ただし、TOE がインタフェースが限られているかまたは使用が限られているような場合、必要な保護は、TOE の外部の手段を通して提供することができる。

1834 TOE セキュリティ機能、IT 環境についての前提条件、TOE セキュリティ機能の必要な自己保護を提供するその他の前提条件の組み合わせを選択するのは、PP/ST 作成者の責任である。必要な保護が提供されていることを確認するのは、評価者の責任である。TOE と前提条件によって、必要とされる保護は、FPT クラスからの機能上のセキュリティ要件を要求することができるが、それが可能でない状況が存在する。

B.7.1 FPT クラスを必ずしも必要としない TOE

1835 いくつかの TOE (利用者インタフェースを持たない内蔵 TOE など) がこれらの脅威を受けないことが考えられる。これらの脅威を含むが、FPT_PHP、FPT_RVM、及び FPT_SEP を持たない、機能が豊富な利用者インタフェースを提供する TOE の PP/ST は、おそらく、無効な PP/ST である。FPT 自己保護要件を含む必要がない TOE は、3 つのタイプに分けられる。

B.7.1.1 限られた利用者インタフェースを持つ TOE

1836 限られたインタフェースによって、(信頼できない) 利用者に限られたインタフェースだけを提供する TOE は、悪意のある利用者でさえも TOE を改悪(corrupt) させることができない十分な制約を利用者アクションへ課することができる。例えば、計算機などの機器または利用者認証トークンは、いくつかの可能な入力キーだけを持つことができる。ルータまたはガードなどの通信機器への信頼できない利用者インタフェースは、さらに制限されている。利用者は、間接的にのみ、一般的には、プロトコルデータユニットまたはメッセージを通して通信することができる。

B.7.1.2 適切なセキュリティ方針を実施しない TOE

1837 アクセス制御または情報のフロー制御を実施しない TOE は、多分、TSF の他の利用者のデータにアクセスする利用者についての関心がない。そのような場合、FPT_SEP が暗示する利用者を分離する必要はほとんどない。同様に、(サービスの拒否に対するなどの) 保護を必要とする資産 (IT 資源など) の存在が考えられない場合、FPT 要件は必要ない。

B.7.1.3 環境によって提供される保護

1838 TSF の保護は、多くの場合、TOE 自身ではなく (例えば、アプリケーションが TOE である、信頼されたオペレーティングシステムでアプリケーションが実行される場合など) TOE の環境によって提供される必要がある。そのような場合、評価は、環境メカニズムが必要な保護を提供するかどうかを考慮する。保護手段自体は、正しく機能するものと想定する。ただし、TOE を保護するためにそれらが適用される方法は、評価の範囲に影響することがある。

1839 例えば、オペレーティングシステムがアプリケーションの中のオブジェクトファイルに割り付ける権限は、下層のオペレーティングシステムの TSP に違反するアプリケーションの可能性を決定する。大きく異なる TSF が暗示されるように、オペレーティングシステムの保護手段を異なった方法で使用する、同じアプリケーションの 2 つの実装を考慮することができる。そこで、保護メカニズムが TOE 環境によって実装される場合でも、TSF の決定を行う前に、それらのメカニズムの使用をなお検査する必要がある。

B.7.2 保証ファミリへの影響

1840 PP/ST に FPT 自己保護要件を含めるかまたは除外するかは、次の要件に影響する。

B.7.2.1 ADV

- 1841 改ざんまたはバイパスの脅威が存在しない場合、評価は、TSF の正しい運用に焦点を絞る。これには、TSP の実施に直接または間接的に貢献する TOE の内部のすべての機能を考慮することが含まれる。これらのカテゴリのいずれにも属さない機能は、検査する必要がない (TSF の正しい運用に干渉することがあるこれらの機能の実装に誤りが存在することは、TSF のテストを通して確認される)。
- 1842 自己保護機能が主張されている場合、それらの実装の記述は、TSF の境界を決定することができる保護メカニズムを識別する。TSF の境界とインタフェースの識別は、主張されている TSF 保護メカニズムの効能の決定とともに、評価の範囲を制約することができる。TSF の外部の機能は、正しい TSF の運用に干渉することがないために、この制約は、TSF の外部の機能を除外する。多くの場合、TSF 境界には、TSP の実施に貢献しない機能がいくつか含まれることがある。これらの機能は、評価において検査する必要はない。TSF に含まれないと決定することができるこれらの機能は、評価者が検査する必要はない。

B.7.2.2 AVA_VLA

- 1843 CC の脆弱性分析は、TOE の意図する環境における TOE の運用への脆弱性の影響を決定する。ST に改ざんまたはバイパスの脅威が識別されていない場合、開発者及び評価者による脆弱性の探索は、必要に応じて、そのような攻撃を考慮することを除外するべきである。

B.7.2.3 ATE_IND

- 1844 ATE_IND の適用上の注釈は、TOE に適用される明らかな公知になっている弱点のテストを要求している。TOE を改ざんするまたはバイパスする意向に基づくそのような弱点は、そのような脅威が識別されている場合にのみ考慮する必要がある。

B.8 機能強度及び脆弱性分析

- 1845 比較は、TOE セキュリティ機能強度分析と脆弱性分析の間に重要な相違及び重要な類似が存在することを示す。
- 1846 重要な類似は、攻撃能力の使用に基づく。両方の分析に対して、評価者は、攻撃を行うために攻撃者が必要とする最小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に到達する。表 B.1 及び表 B.2 は、これらの分析と攻撃能力の間の関係を示し、さらに説明している。

表 B.1 脆弱性の分析及び攻撃能力

脆弱性コンポーネント	次の攻撃能力を持つ攻撃者への TOE の抵抗力	次の攻撃能力を持つ攻撃者だけが悪用可能な残りの脆弱性
VLA.4	高	適用されず - 攻撃が成功するのは実際のでない
VLA.3	中	高
VLA.2	低	中

表 B.2 TOE セキュリティ機能強度と攻撃能力

SOF レート付け	攻撃能力のある攻撃者に対する適切な保護	攻撃能力のある攻撃者に対する不十分な保護
SOF-高位	高	適用されず - 攻撃が成功するのは実際のでない
SOF-中位	中	高
SOF-基本	低	中

- 1847 これらの分析の間の重要な相違は、TOE セキュリティ機能の性質と、攻撃の性質に基づいている。TOE セキュリティ機能強度分析は、暗号に基づくものを除いて、確率的または順列的機能に基づいてのみ行われることである。さらに、分析は、確率的または順列的セキュリティ機能が欠陥のない状態で実装され、セキュリティ機能が攻撃中、設計と実装の制約内で使用されるものと仮定する。表 B.2 に示すように、SOF レート付けは、確率的または順列的セキュリティ機能が保護するように設計される攻撃能力として記述されている攻撃を反映している。
- 1848 脆弱性分析は、本来、確率的または順列的であるものを含む、すべての非暗号 TOE セキュリティ機能に適用される。SOF 分析と異なり、セキュリティ機能の設計及び実装が正しいことに関する前提は行われぬ。攻撃方法または攻撃者の TOE との相互作用に対する制約は行われぬ - 攻撃が可能な場合、それは、脆弱性分析で考慮する必要がある。表 B.1 に示すように、脆弱性保証コンポーネントに対する成功した評価は、すべての TOE セキュリティ機能が設計され、保護するために実装される攻撃能力として記述されている、脅威のレベルを反映する。
- 1849 攻撃能力の概念の一般的な使用は、SOF 主張と脆弱性評価の間にリンクを作成するが、このリンクは、SOF 主張と AVA_VLA から選択された保証コンポーネントの間に必須の結合を作成するものとみなすべきでない。例えば、攻撃能力の低い攻撃者への抵抗力を必要とする AVA_VLA.2 の選択は、SOF レート付けの選択を SOF-基本に制約しない。脆弱性が本質的に確率的または順列的機能に存在し、そのような機能が通常、公開インタフェース（例えば、パスワード）の優れた局面であるとすると、PP/ST 作成者は、これらの点への攻撃に対する高いレベルの抵抗力を必要とし、より高い SOF レート付けを選択する。AVA_SOF に対するコンポーネントが主張されているところでは、SOF-基本の最小の主張が必要となる。主張されている AVA_VLA コンポーネントは、SOF 主張に下限を課し、SOF-基本の SOF 主張は、AVA_VLA.3 の選択と一致していないものとみなされるべきである。

B.8.1 攻撃能力

B.8.1.1 攻撃能力の適用

1850 攻撃能力は、専門知識、資源及び動機によって決まる。これらの要因のそれぞれについて説明する。攻撃能力は、特に、ST 評価と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。ST 評価中、評価者は、保証要件コンポーネント、特に AVA クラスのコンポーネントの選択が脅威の攻撃能力と釣り合っているかどうかを決定する (ASE_REQ 1.4C を参照)。保証が釣り合っていない場合は、評価が十分な保証を提供しないか、または評価が不必要にわずらわしいかのいずれかを意味する。脆弱性を評価するとき、評価者は、攻撃能力を、意図する環境での識別された脆弱性が悪用される可能性を決定するための手段として使用する。

B.8.1.2 動機の取扱い

1851 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局面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、攻撃に似たものを暗示することができる – 高く動機づけられていると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、または動機がない脅威からは攻撃が予想されないことを推測することができる。ただし、動機の 2 つの極端なレベルを除いて、動機から攻撃が起きる確率を引き出すのは困難である。

1852 第二に、動機は、攻撃者または資産の所有者のいずれかに、金銭的またはその他の資産の値を、暗示することができる。非常に高価な資産は、価値の低い資産に比べて、攻撃をより多く動機づけることがある。ただし、非常に一般的な方法は別として、資産の価値は、主観的なものであるために、つまり、資産の価値は、資産の所有者による資産に対する価値によって大きく左右されるために、資産価値を動機に関連づけることは困難である。

1853 第三に、動機は、攻撃者が攻撃を行うための専門知識と資源を暗示することができる。高く動機づけられた攻撃者は、資産を保護するための手段を打ち負かすための十分な専門知識と資源を獲得するものと推測することができる。逆に、十分な専門知識と資源を備えた攻撃者は、攻撃者の動機が低い場合、それらを使用して攻撃しようとしないと推測できる。

1854 評価を準備し、実行する途中のどこかで、動機の 3 つの局面のすべてが考慮される。第一の局面は、攻撃と同様に、なにが開発者に評価を行わせるかである。攻撃者が攻撃を行うために十分に動機づけられていると、開発者が信じる場合、評価は、攻撃者の努力に対抗する TOE の能力を保証することができる。例えば、システム評価において、意図する環境が明確に定義されている場合、攻撃の動機レベルが明らかになり、それは、対抗策の選択に影響を与える。

1855 第二の局面を考慮するとき、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づけるのに十分であると信じる。評価が必要であると思われた後、攻撃者の動機が、試みられる攻撃方法と、それらの攻撃で使用される専門知識と資源を決定するとみなされる。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。評価の途中、及び特に脆弱性評定を完了した結果として、評価

者は、TOE が、それが意図する環境で運用されるとき、識別された専門知識と資源を備えた攻撃者に十分に対抗するかどうかを決定する。

B.8.2 攻撃能力の計算

1856 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幾分か取り除くのに役に立つガイドラインを提供する。評価者が適切でないと決定しない限り、この手法が採用されるべきである。評価者が適切でないと決定した場合には、代替手法の有効性を正当化するための根拠が必要となる。

B.8.2.1 識別及び悪用

1857 攻撃者が脆弱性を悪用するためには、最初に脆弱性を識別し、次に悪用しなければならない。これは、ささいな分離のように見えるが、重要な分離である。この例を示すために、最初に、専門化による分析の後、数ヶ月間発見されず、簡単な攻撃方法がインターネットで公表された脆弱性について考えてみる。これを、脆弱性は明らかになっているが、それを悪用するためには非常に多くの時間と資源を必要とする脆弱性とを比較する。明らかに、時間などの要因は、これらの場合、別の方法で取り扱う必要がある。

1858 SOF 分析には、確率的または順列的メカニズムの脆弱性が、多くの場合、自明であるために、悪用される問題が、通常、最も重要である。ただし、常にこのようなケースばかりではないことに注意すること。例えば、暗号化メカニズムでは、微妙な脆弱性の知識が、暴力攻撃の有効性にかなり影響することがある。システム利用者がパスワードとしてファーストネームを選択する傾向があるとの知識は、同様の効果を持つ。AVA_VLA.1 より上の脆弱性に対して、暴露するのが困難な脆弱性の存在は、公表され、多くの場合、ささいな悪用となるために、脆弱性の最初の識別は、さらに重要な考慮事項となる。

B.8.2.2 考慮する必要がある要因

1859 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

- 1) 識別するために要する時間
- 2) 専門家の技術的専門知識
- 3) TOE 設計と運用の知識
- 4) TOE へのアクセス
- 5) 分析に必要な IT ハードウェア/ソフトウェアまたはその他の機器

b) 悪用

- 1) 悪用するために要する時間
- 2) 専門家の技術的専門知識

- 3) TOE 設計と運用の知識
- 4) TOE へのアクセス
- 5) 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

- 1860 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、時間に置き換わることができる。次にこれらの要因について説明する。
- 1861 「時間」(*Time*) は、攻撃者が継続的に攻撃を識別するまたは悪用するために要する時間である。この説明での「数分以内」(*within minutes*) は、攻撃を 30 分以内に識別または悪用することができることを意味する。「数時間以内」(*within hours*) は、攻撃が 1 日以内に成功することを意味する。「数日以内」(*within days*) は、攻撃が 1 ヶ月以内に成功することを意味する。「数ヶ月以内」(*in months*) は、攻撃が成功するために 1 ヶ月以上を要することを意味する。
- 1862 「専門家の専門知識」(*Specialist expertise*) は、アプリケーション領域または製品（例えば、Unix オペレーティングシステム、インターネットプロトコル）の一般的な知識レベルを意味する。識別されているレベルは、次のとおりである。
- a) 「エキスパート」(*Expert*) は、製品またはシステムの種別で実装されている下位アルゴリズム、プロトコル、ハードウェア、構造など、及び採用されているセキュリティの原理や概念を理解している。
 - b) 「熟練」(*Proficient*) 者は、知識があり、製品またはシステムの種別のセキュリティのふるまいを理解している人である。
 - c) 「しろうと」(*Laymen*) は、エキスパートまたは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。
- 1863 「TOE の知識」(*Knowledge of the TOE*) 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 の一般的な目的以外で、TOE についての「情報なし」(*No information*)
 - b) (例えば、利用者ガイドから得られる) TOE に関する「公の情報」(*Public information*)
 - c) (例えば、内部設計情報) TOE についての「機密に関する情報」(*Sensitive information*)
- 1864 ここでは、脆弱性を識別するために必要な情報と、特に機密に関する情報領域で脆弱性を悪用するために必要な情報とを注意深く区別されるべきである。悪用に対する機密情報を要求するのは、一般的ではない。
- 1865 また、「TOE へのアクセス」(*Access to the TOE*) は、重要な考慮事項であり、時間要因と関係を持っている。脆弱性の識別または悪用には、TOE へのかなりの量のアクセスを必要とし、それにより検出される可能性が高まる。攻撃の中には、か

なりのオフラインの努力を必要とし、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セッションを必要とする。この説明での「数分以内」は、30 分以内のアクセスが必要になることを意味し、「数時間以内」は、1 日以内のアクセスを必要とし、「数日以内」は、1 ヶ月以内のアクセスを必要とし、数ヶ月以内は、1 ヶ月以上のアクセスを必要とすることを意味する。TOE へのアクセスにより検出される可能性が高まらない場合（例えば、攻撃者が所持するスマートカード）、この要因は無視されるべきである。

1866 「IT ハードウェア/ソフトウェアまたはその他の機器」(*IT hardware/software or other equipment*) は、脆弱性を識別または悪用するために必要となる機器を意味する。

- a) 「標準機器」(*Standard equipment*) は、脆弱性の識別または攻撃のいずれかのために攻撃者が容易に使用できる機器である。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）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、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、攻撃者が簡単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、一般的な量の機器（例えば、プロトコルアナライザ）の購入、またはさらに広範な攻撃スクリプトまたはプログラムの開発が含まれる。
- c) 「特別注文機器」(*Bespoke equipment*) は、特別に作成する必要があるか（例えば、非常に精巧なソフトウェア）または機器が特殊であり、配付が管理されている（おそらく、制約される）ために、一般には提供されない。あるいは、機器が非常に高価である。インターネットに接続された数百台の PC 使用がこのカテゴリに入る。

1867 「専門家の専門知識及び TOE の知識」(*Specialist expertise and knowledge of the TOE*) 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少なくなるにつれて、機器を使用する可能性が低下する。同様に、専門知識が多くなるにつれて、攻撃で機器が使用される可能性が増加する。暗示的であるが、専門知識と機器の使用との間のこの関係は、例えば、環境的手段がエキスパートの攻撃者の機器の使用を阻止するとき、またはその他の努力を通して、効果的に使用するためにほとんど専門的知識を必要としない攻撃ツールが作成され、無料で配付されているとき（例えば、インターネットを介して）、常には適用されない。

B.8.2.3 計算手法

1868 上記の節は、考慮する必要がある要因を識別している。ただし、評価が標準的に行われるためには、さらにガイダンスが必要となる。次の手法は、このプロセスを支援するために提供されている。適切な評価レベルに一貫するレート付けを達成することを目的として、数字を示している。

1869 表 B.3 は、前の節で説明した要因を識別し、脆弱性を識別して悪用する 2 つの局面に数値を関係付けている。特定の脆弱性に対する攻撃能力を決定するとき、1 つの

値を各要因に対する各欄（10 の値を示している）から選択されるべきである。値を選択するとき、TOE に対する意図する環境が仮定されるべきである。10 の値を合計し、1 つの値にする。次にこの値を表 B.4 でチェックし、レート付けを決定する。

1870

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、TOE へのアクセスが脆弱性を悪用するために 1 時間必要となる場合、またはアクセスが非常に迅速に検出される場合には、その要因に 0 から 4 までの間の値を選択することができる。この表は、ガイドとして示されている。

表 B.3 攻撃能力の計算

要因	範囲	識別値	悪用値
所要時間	< 0.5 時間	0	0
	< 1 日	2	3
	< 1 ヶ月	3	5
	> 1 ヶ月	5	8
	実際的でない	*	*
専門知識	しろうと	0	0
	熟練者	2	2
	エキスパート	5	4
TOE の知識	なし	0	0
	公開	2	2
	機密	5	4
TOE へのアクセス	< 0.5 時間、またはアクセスは検出不能	0	0
	< 1 日	2	4
	< 1 ヶ月	3	6
	> 1 ヶ月	4	9
	実際的でない	*	*
機器	なし	0	0
	標準	1	2
	特殊	3	4
	特別注文	5	6
* 攻撃パスは、攻撃者に有用な時間目盛内で悪用可能でないことを示す。*の値は、いずれも高いレート付けを示す。			

附属書 B 一般的評価ガイダンス

- 1871 特定の脆弱性に対して、異なる攻撃シナリオに対して表を何度かパスすることが必要となる場合がある（例えば、専門知識と時間または機器のトレードオフ）。これらのパスで得られた最小値が保持されるべきである。
- 1872 脆弱性が識別され、それが公知になっている場合、識別値は、最初に脆弱性を識別するのではなく、公知になっている脆弱性を暴露する攻撃者に対して選択されるべきである。
- 1873 次に、脆弱性のレート付けを入手するために、表 B.4 が使用されるべきである。

表 B.4 脆弱性のレート付け

値の範囲	次の攻撃能力を持つ攻撃者への抵抗力	SOF レート付け
<10	レート付けなし	
10-17	低	基本
18-24	中	中
>25	高	高

- 1874 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または攻撃が完了する前に検出される可能性への依存など、その他の要因は、この基本モデルに含まれていないが、評価者が、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。
- 1875 例えば、パスワードメカニズムがレート付けされているときに、攻撃が制限される前にごくわずかの試みだけが許されるように TOE が実装されている場合、強さのレート付けは、ほとんど全体的に、それらのわずかな試みの間の正しい推測の確率に関係することになる。そのような制限は、アクセス制御の一部とみなされる。パスワードメカニズム自体は、例えば、単に SOF-中位のレート付けを受けるのに対して、アクセス制御機能は、SOF-高位と判定されることがある。
- 1876 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、他の脆弱性の存在が表の値を変えるために、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。言い換えると、1 つの脆弱性の存在が他の脆弱性の悪用を容易にすることがある。そのような評定は、開発者及び評価者の脆弱性分析の一部をなすべきである。

B.8.3 機能強度分析の例

- 1877 仮想的パス番号メカニズムの SOF 分析を次に示す。
- 1878 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時及びそれ以降、利用者の要求でシステムを使用することを許可される時、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) 数字の繰り返しは許されない(各数字は、一意であること)

1879 パス番号を選択するとき利用者には次のようなガイドラインが行われる。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。

1880 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、そのために SOF に影響を与える、重要な考慮事項である。ワーストケースシナリオを想定し、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置換の数字は、次のとおりである。

$$7(8)(9)(10) = 5040$$

- b) シーケンスを増やすことができる数は、7であり、シーケンスを減らすことができる数も同じである。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。

$$5040 - 14 = 5026$$

1881 設計証拠から集められたそれ以上の情報に基づいて、パス番号メカニズムは、端末ロッキング機能によって設計される。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。

1882 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。平均的な成功する攻撃は、その結果、以下の場合よりもわずかに発生率が下がる。

$$\frac{2513 \text{ 分}}{60 \frac{\text{分}}{\text{時}}} \approx 42 \text{ 時}$$

- 1883 前の節に記述されている手法を使用するとき、識別値は、そのような機能での脆弱性の存在は明らかであるために、各カテゴリからの最小値となる（合計 0）。悪用に対して、上記の計算に基づき、しろうとは、数日以内に（TOE にアクセスし）、なんの機器も使用せずに、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、11 となる。結果の合計が 11 である場合、攻撃が成功するために必要な攻撃能力は、中以上と決定される。
- 1884 SOF 評価は、CC パート 1 の 2.3 節、用語集に攻撃能力として定義されている。メカニズムは、SOF-基本を主張するために、攻撃能力の低い攻撃者に対する抵抗力がなければならない。パス番号メカニズムは、攻撃能力の低い攻撃者への抵抗力があるために、このパス番号メカニズムの評価は、せいぜい SOF-基本である。

B.9 制度の責任

- 1885 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 が終了するところと個々の制度の方法論が始まることを明確に描くために、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。）
- 1886 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、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し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 に少なくとも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 – 制度は、評価が TOE であるかまたは ST であるかによって、評価の結果の詳細のすべてを報告するための特定の用紙を用意していることがある。
- 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が適切であること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裏付ける評価者証拠の規定のための要件
- m) 制度識別情報、ロゴ、商標などの特定の取扱い
- 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、監督者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での
- s) 評価者の脆弱性分析を行う受け入れ可能な手段のリストまたは特性（例えば、欠陥仮説法(flaw hypothesis methodology)）
- 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 C CEM オブザベーション報告書の提供

C.1 序説

1887 Common Evaluation Methodology Editorial Board (CEMEB)が、IT セキュリティ評価コミュニティで使用するためにこの文書を政府機関に提供する。ただし、この使用が、将来のバージョンで考慮するための文書についてのオブザベーション及び/またはコメントに対する動機を与えることを認識している。

1888 本附属書は、CEM についてコメントするためのメカニズムについて詳しく説明している。このメカニズムは、オブザベーションを明記するために使用する報告書フォーマット、CEM オブザベーション報告書 (CEMOR) からなる。オブザベーションはいずれも、本書のまえがきに記載されている政府機関を通して提出されるべきである。

1889 コメントはいずれも、提供されている CEMOR フォーマットで提出されるべきである。これにより、CEMEB は、すべてのコメントを一般的及び系統的な方法で処理することが可能になる。すべてのレビューを行った者は、可能な限り、識別された概念的な問題、不一致、または技術的困難に対する代替文または明確な解決策を含めるべきである。

C.2 CEMOR のフォーマット

1890 CEMOR には、次のフィールドのすべてが含まれていなければならない。ただし、1 つまたはいくつかのフィールドは、ブランクでも良い。各フィールドは、ASCII 文字"\$"で始まり、その後アラビア数字が続き、最後が ASCII 文字":"でなければならない。

\$1: 発信者名

1891 発信者の完全な名前。

\$2: 発信者の組織

1892 発信者の組織/所属機関。

\$3: リターンアドレス

1893 必要に応じて、CEMOR を受け取ったことを応答し、明確化を要求するための電子メールまたはその他のアドレス。

\$4: 日付

1894 オブザベーションの提出日 YY/MM/DD。

- \$5: 発信者の CEMOR 識別情報**
- 1895 この一意の識別情報は、発信者によって CEMOR に割り付けられる。
- \$6: オブザベーションタイプ**
- 1896 可能なタイプは、「編集」、「技術」、「プログラム」または「その他」。
- \$7: CEMOR のタイトル**
- 1897 この CEMOR の短い記述的タイトル。
- \$8: CEM 文書参照**
- 1898 CEM の影響を受ける領域への単一の参照。このフィールドで、CEM バージョン番号、パート番号及び節番号を識別しなければならない。さらに、段落番号（または、段落番号が関係ない場合、ワークユニット、表または図の番号）もこのフィールドで識別しなければならない。
- \$9: オブザベーションの説明**
- 1899 オブザベーションの包括的記述。このフィールドの長さに関する制限はない。ただし、文章だけを含むべきで、ASCII だけで示すことができない図または表を含めてはならない。
- \$10: 示唆する解決策**
- 1900 オブザベーションに対処するために提案する解決策。
- \$\$ CEMOR の終わり**
- 1901 CEMOR に関係する情報の終わりを示すために必要となる。
- C.2.1 オブザベーションの例**
- \$1: Pat Smith**
- \$2: CC Evals Laboratory**
- \$3: psmith@cclab**
- \$4: 1999/11/10**
- \$5: CEMOR.psmith.comment.1**
- \$6: 技術**
- \$7: 確定的でない判定は、判定ではない**
- \$8: CEM バージョン 1.0、パート 2、1.4 節、段落 28b**

附属書 C CEM オブザベーション報告書の提供

\$9: 判定は、分析の結果であるべきである。判定がまだ下されない場合には、それは判定以外のものとして呼ばれるべきである。確定的でない判定は、作業が完了したことを暗示するが、疑問は残る（すなわち、評価者は、それが合格か不合格か分からない）。

\$10: 2つの判定を持つように CEM を変更する。つまり合格及び不合格。判定が出されるまでは、「判定待ち」(awaiting verdict)と記すべきである。

\$\$

1902

CEMOR は、いくつかを組み合わせることで 1 つにし、提出することができる。この場合、フィールド\$1 から\$4 は、最初のところに一度だけ現れる必要がある。提出するそれぞれの CEMOR に対して、フィールド\$5 から\$10 がその後に現れる。\$\$が最後の CEMOR の後に現れなければならない。