



**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**

パート 1: 概説と一般モデル

2009年7月

**バージョン 3.1
改訂第3版 最終版**

CCMB-2009-07-001

平成 21 年 12 月翻訳第 1.0 版 最終版
独立行政法人 情報処理推進機構
セキュリティセンター
情報セキュリティ認証室

IPA まえがき

はじめに

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

原文

Common Criteria for Information Technology Security Evaluation

Part1: Introduction and general model Version 3.1 Revision 3 Final
July 2009 CCMB-2009-07-001

まえがき

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の本バージョン(CC v3.1)は、2005年にCC v2.3が公開されて以来、最初の主要な改訂版である。

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

CCバージョン3.1は、次のパートから構成される:

パート1: 概説と一般モデル

パート2: セキュリティ機能コンポーネント

パート3: セキュリティ保証コンポーネント

商標

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

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

法定通知:

以下に示す政府組織は、情報技術セキュリティ評価のためのコモンクライテリアの本バージョンの開発に貢献した。これらの政府組織は、情報技術セキュリティ評価のためのコモンクライテリア、バージョン3.1のパート1から3(CC 3.1と呼ぶ)の著作権を共有したまま、ISO/IEC 15408 国際標準の継続的な開発/維持の中で、CC 3.1を使用するために ISO/IEC に対し、排他的でないライセンスを許可している。ただし、適切と思われる場合に CC 3.1 を使用、複製、配布、翻訳及び改変する権利は、これらの政府組織が保有する。

オーストラリア/ニュージーランド:	<i>The Defence Signals Directorate and the Government Communications Security Bureau;</i>
カナダ:	<i>Communications Security Establishment;</i>
フランス:	<i>Direction Centrale de la Securite des Systemes d'Information;</i>
ドイツ:	<i>Bundesamt fur Sicherheit in der Informationstechnik;</i>
日本:	<i>独立行政法人 情報処理推進機構(Information-technology Promotion Agency);</i>
オランダ:	<i>Netherlands National Communications Security Agency;</i>
スペイン:	<i>Ministerio de Administraciones Publicas and Centro Criptologico Nacional;</i>
英国:	<i>Communications-Electronics Security Group;</i>
米国:	<i>The National Security Agency and the National Institute of Standards and Technology</i>

目次

1	序説	11
2	適用範囲	13
3	規定の参照	14
4	用語と定義	15
4.1	CCにおける共通の用語と定義.....	15
4.2	ADVクラスに関連する用語及び定義.....	20
4.3	AGDクラスに関連する用語及び定義.....	25
4.4	ALCクラスに関連する用語及び定義.....	25
4.5	AVAクラスに関連する用語及び定義.....	29
4.6	ACOクラスに関連する用語及び定義.....	30
5	記号と略語	31
6	概要	33
6.1	TOE.....	33
6.1.1	TOEの様々な形態.....	33
6.1.2	TOEの様々な構成.....	34
6.2	CCの対象読者.....	34
6.2.1	消費者.....	34
6.2.2	開発者.....	35
6.2.3	評価者.....	35
6.2.4	その他の対象者.....	35
6.3	CCの各パート.....	35
6.4	評価の枠組み.....	36
7	一般モデル	38
7.1	資産及び対抗策.....	38
7.1.1	対抗策の十分性.....	40
7.1.2	TOEの正確性.....	41
7.1.3	運用環境の正確性.....	42
7.2	評価.....	42
8	セキュリティ要件の調整	44
8.1	操作.....	44
8.1.1	繰返し操作.....	44
8.1.2	割付操作.....	45
8.1.3	選択操作.....	46
8.1.4	詳細化操作.....	46

8.2	コンポーネント間の依存性.....	47
8.3	拡張コンポーネント.....	47
9	プロテクションプロファイル及びパッケージ	49
9.1	序説	49
9.2	パッケージ.....	49
9.3	プロテクションプロファイル	49
9.4	PP及びパッケージの使用	52
9.5	複数のプロテクションプロファイルの使用.....	53
10	評価結果	54
10.1	序説	54
10.2	PPの評価の結果.....	55
10.3	ST/TOEの評価の結果.....	55
10.4	適合主張	55
10.5	ST/TOEの評価結果の使用.....	56
	附属書A セキュリティターゲットの仕様(参考).....	57
A.1	本附属書の目的及び構造.....	57
A.2	STの必須の内容	57
A.3	STの使用.....	58
A.3.1	STの使用法.....	58
A.3.2	STの不適切な使用法.....	59
A.4	ST概説(ASE_INT).....	59
A.4.1	ST参照及びTOE参照.....	59
A.4.2	TOE概要.....	60
A.4.3	TOE記述.....	61
A.5	適合主張(ASE_CCL).....	62
A.6	セキュリティ課題定義(ASE_SPD).....	62
A.6.1	序説.....	62
A.6.2	脅威.....	63
A.6.3	組織のセキュリティ方針(OSP).....	63
A.6.4	前提条件	63
A.7	セキュリティ対策方針(ASE_OBJ)	64
A.7.1	上位レベル解決策	65
A.7.2	部分的な解決策	65
A.7.3	セキュリティ対策方針とセキュリティ課題定義の関係.....	66
A.7.4	セキュリティ対策方針: 結論	68
A.8	拡張コンポーネント定義(ASE_ECD).....	68

目次

A.9	セキュリティ要件(ASE_REQ)	68
A.9.1	セキュリティ機能要件(SFR).....	68
A.9.2	セキュリティ保証要件(SAR).....	70
A.9.3	SAR及びセキュリティ要件根拠.....	70
A.9.4	セキュリティ要件: 結論.....	71
A.10	TOE要約仕様(ASE_TSS)	72
A.11	STを使用して回答できる質問	72
A.12	低保証セキュリティターゲット	73
A.13	STでの他の標準の参照	74
附属書B	プロテクションプロファイルの仕様(参考)	76
B.1	本附属書の目的及び構造	76
B.2	PPの必須の内容	76
B.3	PPの使用	77
B.3.1	PPの使用法.....	77
B.3.2	PPの不適切な使用法.....	78
B.4	PP概説(APE_INT)	78
B.4.1	PP参照.....	78
B.4.2	TOE概要.....	78
B.5	適合主張(APE_CCL)	80
B.6	セキュリティ課題定義(APE_SPD)	80
B.7	セキュリティ対策方針(APE_OBJ)	80
B.8	拡張コンポーネント定義(APE_ECD)	80
B.9	セキュリティ要件(APE_REQ)	80
B.10	TOE要約仕様	80
B.11	低保証プロテクションプロファイル	80
B.12	PPでの他の標準の参照	81
附属書C	操作のためのガイダンス(参考)	82
C.1	序説	82
C.2	操作の例	82
C.2.1	繰返し操作.....	82
C.2.2	割付操作.....	82
C.2.3	選択操作.....	82
C.2.4	詳細化操作.....	83
C.3	コンポーネントの編成	83
C.3.1	クラス.....	84
C.3.2	ファミリー.....	84
C.3.3	コンポーネント.....	84

C.3.4	エレメント	84
C.4	拡張コンポーネント.....	84
C.4.1	拡張コンポーネントを定義する方法.....	84
附属書D	PP適合(参考).....	86
D.1	序説	86
D.2	正確適合	86
D.3	論証適合	87
附属書E	参考文献(参考)	88
E.1	ISO / IEC標準とガイダンス.....	88
E.2	その他の標準とガイダンス	88

図一覧

図 1	CM及び製品ライフサイクルの用語.....	29
図 2	セキュリティの概念と関係.....	39
図 3	評価の概念と関係.....	40
図 4	PP, ST及びTOEの内容間関係.....	52
図 5	評価結果.....	54
図 6	セキュリティターゲットの内容.....	58
図 7	セキュリティ対策方針とセキュリティ課題定義間の追跡.....	66
図 8	セキュリティ課題定義、セキュリティ対策方針、及びセキュリティ要件間の関係.....	71
図 9	低保証セキュリティターゲットの内容.....	74
図 10	プロテクションプロファイルの内容.....	77
図 11	低保証プロテクションプロファイルの内容.....	81

表一覧

表 1	コモンクライテリアのロードマップ	36
-----	------------------------	----

1 序説

- 1 CC は、独立したセキュリティ評価結果間の比較を可能にするものである。このため、CC は IT 製品のセキュリティ機能性¹とセキュリティ評価の際に当該 IT 製品に適用される保証手段に関する共通要件のセットを規定している。当該 IT 製品は、ハードウェア、ファームウェア、またはソフトウェアに実装されることがある。
- 2 評価プロセスでは、当該 IT 製品のセキュリティ機能性とそれらに適用される保証手段が、これらの要件を満たしていることの信頼のレベルを明らかにする。評価結果は、これらの IT 製品がセキュリティニーズを満たしているかどうかについて、消費者が判断する際に役立つであろう。
- 3 CC は、セキュリティ機能性を備えた IT 製品の開発、評価、及び/または調達のためのガイドとして役立つ。
- 4 CC は、幅広い IT 製品の様々なセキュリティ特性に対して、幅広い評価方法を適用できるように、意図的に柔軟にしてある。したがって、この規格の利用者には、この柔軟性が誤用されないように注意するよう、警告しなければならない。例えば、CC を不適切な評価方法、不適切なセキュリティ特性、または不適切な IT 製品とともに用いると、無意味な評価結果を生じるかもしれない。
- 5 このため、IT 製品が評価を受けたという事実は、評価対象のセキュリティ特性と使用された評価方法の枠組みにおいてのみ意味を持つ。評価監督機関は、製品、特性、及び方法を慎重にチェックして、評価により有意な結果が提供されることを確認することを薦める。また、評価対象の製品の購入者は、評価対象の製品が有用であり、購入者に固有な状況及びニーズに適用可能であるかどうかを判断するために、この枠組みを慎重に検討することを薦める。
- 6 CC が扱うのは、許可されない暴露、改変、または利用不能からの資産の保護である。一般に、これら 3 種類のセキュリティ障害に関する保護のカテゴリはそれぞれ機密性、完全性、及び可用性と呼ばれる。CC はまた、これら 3 つ以外の IT セキュリティの側面にも適用してもよい。CC は、(悪意があるまたはその他の)人間の活動から生じるリスクと、人間以外の活動から生じるリスクに対して適用できる。なお、CC は、IT セキュリティ以外の IT 分野にも適用してもよいが、このような分野での適用可能性は主張していない。
- 7 いくつかの項目には、専門的な技法が必要であったり、IT セキュリティにとってあまり重要でなかったりすることから、CC の範囲外とみなされるものがある。以下にこれらの項目の一部を示す。
 - a) CC は、IT セキュリティ機能性に直接関係しない管理上のセキュリティ手段に関するセキュリティ評価基準は含んでいない。しかし、多くの場合、セキュリティのかなりの部分が組織的、人的、物理的、及び手続き的管理のような管理上の手段によって実現またはサポートできると認められる。
 - b) 電磁波放射制御のような IT セキュリティの技術上の物理的側面の評価は、特に対象としていないが、扱われる概念の多くはその領域にも適用することができる。

【訳注】¹ セキュリティ機能性 (security functionality) - SFR を実現する個々のソフトウェアやハードウェア機能が、TOE においてどのように全体として SFR を実現しているかに関する特性。

- c) CC では、基準を適用する際に、使用するべき評価方法については扱わない。この方法については、CEM に記述する。
- d) CC では、評価監督機関が基準を適用するうえでの管理上・法律上の枠組みについても扱わない。しかし、そうした枠組み状況においても、評価を目的として CC を用いることが期待される。
- e) 認定(accreditation)における評価結果を用いるための手続きは、CC の範囲外である。認定は、非 IT 部分のすべてを含めて、十分な運用環境における IT 製品(またはその集合)の運用を、機関が認めるための管理上のプロセスである。評価プロセスの結果は、認定プロセスへの入力となる。しかし、非 IT 関連の特性、及びそれら非 IT 関連の特性と IT セキュリティ部分との関係の判定には、他の技法の方がより適しているため、認定者(creditor)はこれらの側面に対して別個に備えるべきである。
- f) 暗号化アルゴリズム固有の品質評価のための基準は、CC では対象とされない。暗号の数学的特性に対する独立の判定が必要な場合、CC が適用される評価制度は、そうした判定に備えたものでなければならない。

8 文書を通して使用される「できる」(can)、「参考」(informative)、「してもよい」(may)、「規定」(normative)、「しなければならない」(shall)や「すべき」(should)などの ISO 用語は、ISO/IEC 専門業務用指針第 2 部で定義される。この規格を使用した場合には、すべきである(should)には、追加の意味があることに注意のこと。下記の注を参照。CC で「すべきである」(should)を使用するために、以下の定義が与えられている。

9 **すべきである(should)** 規定テキストにおいて、「すべきである」(should)は、「他の可能性に言及せずあるいはそれを排除せず、複数の可能性の中から 1 つの可能性が特に適切であること、またはある処置が好ましいが必ずしも必要ではない」を示す(ISO/IEC 専門業務用指針第 2 部)。

CC では、「必ずしも必要ではない」とは、別の可能性の選択は、好ましい選択肢を選択しなかったことを正当とする理由を要求することを意味すると解釈される。

2 適用範囲

- 10 CC のパート1 では、IT セキュリティ評価の一般的な概念及び原則を明らかにし、全体として IT 製品のセキュリティ特性評価のためのベースとして使用される、規格の各所で提示される評価の一般モデルを特定する。
- 11 パート1は、CC 規格のすべてのパートの概要を提供する。規格のいろいろなパートを記述する； 規格の全パートを通して用いられる用語と略語の定義、評価対象 (TOE) の中心概念を明らかにする； 評価の枠組み、及び評価基準を扱う読者を記述する。IT 製品の評価に必要な基本的なセキュリティ概念の紹介がされる。
- 12 CC パート2 及び CC パート3 に記述される機能及び保証コンポーネントは、許可された操作によって調整することができるが、その様々な操作を定義する。
- 13 プロテクションプロファイル (PP) の主要概念、セキュリティ要件のパッケージ、及び適合の話題が特定され、評価の影響、評価結果が記述される。CC のこのパートはセキュリティターゲット (ST) の仕様に対するガイドラインを与え、モデルを通してコンポーネントの構造の記述を示す。評価手法についての一般的な情報は CEM で記述し、評価制度の範囲が示される。

3 規定の参照

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

[CC-2] 情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 3 版、2009 年 7 月、パート 2:セキュリティ機能コンポーネント

[CC-3] 情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 3 版、2009 年 7 月、パート 3:セキュリティ保証コンポーネント

[CEM] 情報技術セキュリティ評価のための共通方法、バージョン 3.1、改訂第 3 版、2009 年 7 月

4 用語と定義

15 本文書の目的のために、以下の用語及び定義を適用する。

16 この 4 章では、CC 全体にわたって特別な意味で用いられる用語のみを示す。CC に用いられる一般用語の一部の組み合わせのうち、この 4 章に含まれていないものについては、分かりやすくするためにそれぞれの文脈において説明している。

4.1 CCにおける共通の用語と定義

17 **有害なアクション(adverse actions)** 脅威エージェントが資産に対して行うアクション。

18 **資産(assets)** TOE の所有者が一般に価値を認めるエンティティ。

19 **割付(assignment)** (CC の)コンポーネントまたは要件内の識別されたパラメタを特定すること。

20 **保証(assurance)** TOE が SFR を満たしていることを信頼するための根拠。

21 **攻撃能力(attack potential)** TOE の攻撃に際して費やされた労力の尺度。攻撃者の技能、資源、及び動機の観点から表現される。

22 **追加(augmentation)** 1 つまたは複数の要件をパッケージに追加すること。

23 **認証データ(authentication data)** 要求される利用者の識別情報を検証する際に用いられる情報。

24 **許可された利用者(authorised user)** SFR に従って操作を実行することができる TOE 利用者。

25 **クラス(class)** 共通の関心事項を共有する CC ファミリのグループ。

26 **理路整然とした(coherent)** 論理的順序で並べられ、識別できる意味を持つ。

証拠資料では、これは、対象読者が理解できるかどうかの観点から、文書の実際のテキストと文書構造の両方に関係する。

27 **完全な(complete)** エンティティのすべての必要な部分が提供されている特性。

証拠資料に関して、抽象化のレベルにおいて、これ以上の説明が必要ない詳細レベルで、すべての関連する情報が証拠資料において扱われていることを意味する。

28 **コンポーネント(component)** 要件が基づくことができる最小の選択可能なエレメントのセット。

29 **統合保証パッケージ(composed assurance package)** CC の定義済み統合保証尺度での程度を表す、CC パート 3(主に ACO クラス)から抽出された要件からなる保証パッケージ。

30 **確認する(confirm)** 何かを詳細にレビューし、独立して充足性を決定することを宣言する。

必要とされる厳格性のレベルは、内容によって異なる。この用語は、評価者アクションにのみ適用される。

- 31 **接続性(connectivity)** TOEと外部のITエンティティとの対話を可能にするTOEの特性。
これには、任意の環境または構成において任意の距離を介して、有線または無線手段によって行われるデータ交換が含まれる。
- 32 **一貫した(consistent)** エンティティの間に明らかな矛盾が存在しないような、複数のエンティティ間の関係。
- 33 **対抗する(counter) (動詞)** 攻撃に対処する。特定の脅威の影響が緩和されるが、必ずしも根絶されない。
- 34 **論証適合(demonstrable conformance)** STが、PPにおける一般のセキュリティ課題を解く解決法を提供するような、STとPP間の関係。

PP及びSTは、異なるエンティティについて論じる、異なる概念を使用するなど、まったく異なるステートメントを含むことができる。論証適合は、複数の同様のPPがすでに存在する(または今後生じると思われる)TOEの種別にも適している。これによって、ST作成者はすべてのPPに対する適合を同時に主張し、作業量を減らすことができる。
- 35 **実証する(demonstrate)** 「証明」(proof)ほど厳格ではない分析によって得られる結論を提供する。
- 36 **依存性(dependency)** PP、ST、またはパッケージに、依存するコンポーネントに基づく要件が含まれる場合、通常、依存されるコンポーネントに基づく要件もそのPP、ST、またはパッケージに含まれなければならないというコンポーネント間の関係。
- 37 **記述する(describe)** エンティティの特定の詳細を提供する。
- 38 **決定する(determine)** 特定の結論に達するために、独立した分析をもとに特定の結論を確認する。

この用語の使用は、通常、これまでにどんな分析も行われていない場合の、真の独立した分析を暗示する。「確認する」(confirm)または「検証する」(verify)の用語と比較すると、これらの用語は、レビューする必要がある分析がすでに行われていることを暗示する。
- 39 **開発環境(development environment)** TOEが開発される環境。
- 40 **エレメント(element)** 必要なセキュリティの不可分のステートメント。
- 41 **保証する(ensure)** アクションとその結果の間の強い因果関係を保証する。

この用語の前に「助ける」(help)の単語が置かれているときは、結果が、そのアクションだけでは完全に確実でないことを示す。
- 42 **評価(evaluation)** 定義された基準に対するPP、ST、またはTOEの評定。
- 43 **評価保証レベル(evaluation assurance level)** CCの定義済み保証尺度での程度を表す、CCパート3から抽出された保証要件のセットで、保証パッケージを形成する。

用語と定義

- 44 **評価監督機関(evaluation authority)** 標準を定め、特定のコミュニティ内の機関が実施する評価の品質を監視し、評価制度に基づき特定のコミュニティに対して CC を履行する機関。
- 45 **評価制度(evaluation scheme)** 評価監督機関が特定のコミュニティにおいて CC を適用する際の規範となる管理及び規制の枠組み。
- 46 **徹底的(exhaustive)** 曖昧でない計画に従って分析またはアクティビティを行うためにとられる系統的アプローチの特性。
- この用語は、CC では、分析または他のアクティビティの実施に関して使用されている。これは、「系統的」(systematic)と関連があるが、曖昧でない計画に従って分析またはアクティビティを行うために方法的手法が取られた点だけでなく、採用されたその計画が、あらゆる可能な手段が取られたことを十分に保証することを示すという点において、かなり強意である。
- 47 **説明する(explain)** 一連のアクションをとる理由を説明するための論証を与える。
- この用語は、「記述する」(describe)及び「実証する」(demonstrate)とは異なる。これは、行われたアクションの道筋が必然的に最適であったという論証を実際に試みることなく、「何故」(Why?) の質問に答えることを意図している。
- 48 **要件拡張(extension)** CC のパート 2 に含まれていない機能要件、及び/または CC のパート 3 に含まれていない保証要件を、ST または PP に追加すること。
- 49 **外部エンティティ(external entity)** TOE の外部にあって TOE と対話することができる人間または IT のエンティティ。
- 50 **ファミリー(family)** 同様の目標を共有するが、重点または厳密さが異なるコンポーネントのセット。
- 51 **形式的(formal)** 確立した数学上の概念に基づいて、意味が定義された制限付き構文言語で表現すること。
- 52 **ガイダンス証拠資料(guidance documentation)** TOE の配付、準備、運用、管理、及び/または使用について記述した証拠資料。
- 53 **識別情報(identity)** TOE の文脈において、エンティティ(例えば、利用者、プロセス、またはディスク)を一意に識別する表現。
- そのような表現の例は文字列である。人間の利用者に対して、フルネームまたは略称、または(なお特有の)仮名で表現することが出来る。
- 54 **非形式的(informal)** 自然言語で表現すること。
- 55 **TSF 間転送(inter TSF transfers)** TOE と他の信頼できる IT 製品のセキュリティ機能との間でデータを通信すること。
- 56 **内部通信チャンネル(internal communication channel)** TOE 内部の別々の部分間の通信チャンネル。
- 57 **TOE 内転送(internal TOE transfer)** TOE 内部の別々の部分間でデータを通信すること。

- 58 **内部的に一貫した(internally consistent)** エンティティの各側面間に明らかな矛盾が存在しないこと。
また、証拠資料に関しては、相互に矛盾するとみなされるステートメントが証拠資料内に存在しないことを意味する。
- 59 **繰返し(iteration)** 複数の異なる要件を表現するために同じコンポーネントを使用すること。
- 60 **正当化(justification)** 結論に導く分析
「正当化」は実証よりも厳格である。この用語は、論理的な論証の各手順を非常に注意深く、完全に説明することに関して、重大な厳格性を要求する。
- 61 **オブジェクト(object)** 情報を格納または受信し、サブジェクトによる操作の実行対象となる TOE 内の受動的なエンティティ。
- 62 **操作(CC のコンポーネントでの) (operation, (on a component of the CC))** コンポーネントを改変または繰り返すこと。
コンポーネントで許可される操作は、割付、繰返し、詳細化、及び選択である。
- 63 **操作(オブジェクトでの) (operation, (on a object))** サブジェクトによってオブジェクトに対し実行される特定のタイプのアクション。
- 64 **運用環境(operational environment)** TOE が運用される環境。
- 65 **組織のセキュリティ方針(organisational security policy)** 組織に対するセキュリティ規則、手続き、またはガイドラインのセット。
方針は特定の運用環境に関係してもよい。
- 66 **パッケージ(package)** セキュリティ機能要件またはセキュリティ保証要件のいずれかの名前付きセット。
パッケージの例としては、「EAL3」。
- 67 **PP 評価(Protection Profile evaluation)** 定義済みの基準に照らした PP の評価。
- 68 **プロテクションプロファイル(Protection Profile)** TOE の種別に対するセキュリティニーズについての実装に依存しないステートメント。
- 69 **証明する(prove)** 数学的な意味で形式的な分析により対応を示す。
これは、すべての面で完全に厳格である。一般的に、「証明する」(prove)は、2 つの TSF 表現間の一致を厳格性の高いレベルで示すことが要求されるときに使用される。
- 70 **詳細化(refinement)** コンポーネントに詳細を追加すること。
- 71 **役割(role)** 利用者と TOE との間に許可される対話を規定する規則の定義済みセット。
- 72 **秘密(secret)** 特定の SFP を実施するために許可された利用者、及び/または TSF にしか知らせてはならない情報。

用語と定義

- 73 **セキュアな状態(secure state)** TSF データに一貫性があり、TSF が SFR の正しい実施を継続している状態。
- 74 **セキュリティ属性(security attribute)** サブジェクト、利用者(外部 IT 製品を含む)、オブジェクト、情報、セッション、及び/または資源の特性であり、SFR の定義及び SFR の実施においてその値が使用される。
- 75 **セキュリティ機能方針(security function policy)** TSF によって実施され、SFR のセットとして表現できる特定のセキュリティのふるまいを記述する規則のセット。
- 76 **セキュリティ対策方針(security objective)** 識別された脅威に対抗すること、及び/または識別された組織のセキュリティ方針及び/または前提条件を満たすことを目的とするステートメント。
- 77 **セキュリティ課題(security problem)** TOE が対処しようとする特性やセキュリティの範囲を、形式的な作法で定義するステートメント。
- このステートメントは、以下の組み合わせから構成される:
- TOE によって対抗される脅威、
 TOE によって実行される OSP、そして
 TOE とその運用環境に対し維持される前提条件。
- 78 **セキュリティ要件(security requirement)** TOE のセキュリティ対策方針の達成に貢献するために、標準化された言語によって述べられる要件。
- 79 **セキュリティターゲット(Security Target)** 識別された特定の TOE に対するセキュリティニーズについての実装に依存するステートメント。
- 80 **選択(selection)** コンポーネント内のリストから 1 つまたは複数の項目を特定すること。
- 81 **準形式的(semiformal)** 意味が定義された制限付き構文言語で表現すること。
- 82 **特定する(specify)** エンティティについて、厳格で正確な作法で、特定の詳細を提供する。
- 83 **正確適合(strict conformance)** PP に含まれるすべての要件が、ST にも存在するという、PP と ST 間の階層的関係。
- この関係は、「ST には、PP のすべてのステートメントを含めなければならないが、それ以上のステートメントを加えることができる」としておおまかに定義することができる。正確適合は、単一の方法で準拠する必要がある厳格な要件のための使用が想定される。
- 84 **ST 評価(ST evaluation)** 定義済みの基準に照らした ST の評定。
- 85 **サブジェクト(subject)** オブジェクトに対して操作を実行する TOE の能動的なエンティティ。
- 86 **評価対象(target of evaluation)** ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び/またはハードウェアのセット。
- 87 **脅威エージェント(threat agent)** 資産において悪影響を及ぼす行為を行うことのできるエンティティ

- 88 **TOE 評価(TOE evaluation)** 定義済みの基準に照らした TOE の評定。
- 89 **TOE 資源(TOE resource)** TOE 内において使用可能または消費可能なもの。
- 90 **TOE セキュリティ機能(TOE Security Functionality)** SFR の正しい実施のために必要とされる TOE のすべてのハードウェア、ソフトウェア、及びファームウェアの複合機能。
- 91 **たどる(trace)(動詞)** 厳格性の最小なレベルで 2 つのエンティティ間の非形式的対応分析を実施する。
- 92 **TSF 範囲外転送(transfers outside of the TOE)** TSF の制御下でないエンティティに対して TSF が仲介するデータの通信。
- 93 **翻訳(translation)** 標準的言語でセキュリティ要件を記述する過程を記述する。
- この文脈において、翻訳という表現は文字通りではなく、標準言語で表現されたすべての SFR がセキュリティ対策方針に言い戻すことができることを暗示してはいない。
- 94 **高信頼チャンネル(trusted channel)** TSF と遠隔の信頼できる IT 製品が、必要な信頼をもって通信することができる手段。
- 95 **高信頼 IT 製品(trusted IT product)** TOE と同等のセキュリティ機能要件を持ちセキュリティ機能要件を正しく実施するとみなされる TOE 以外の IT 製品。
- 高信頼 IT 製品の例には、別個に評価された製品がある。
- 96 **高信頼パス(trusted path)** 利用者と TSF が必要な信頼をもって通信する手段。
- 97 **TSF データ** SFR 実施が依存する TOE のふるまいのためのデータ。
- 98 **TSF インタフェース(TSF interface)** 外部エンティティ(または、TSF 外にある TOE 内のサブジェクト)が TSF にデータを供給し、TSF からデータを受信し、TSF からサービスを呼び出す手段。
- 99 **利用者(user)** 外部エンティティを参照のこと。
- 100 **利用者データ(user data)** 利用者に関するデータで、TSF のふるまいに影響を与えないもの。
- 101 **検証する(verify)** 厳格に詳細にレビューし、充足性を独立して決定する。
- 「確認する」(confirm)も参照。この用語は、さらに厳格な意味合いを持つ。用語「検証する(verify)」は、評価者に独立した労力を要求する評価者のアクションの文脈において使用される。

4.2 ADVクラスに関連する用語及び定義

- 102 次の用語は、ソフトウェアの内部構造に対する要件で使用される。これらの用語の一部は、「IEEE Std 610.12-1990」 *IEEE Std 610.12-1990 Standard glossary of software engineering terminology, Institute of Electrical and Electronics Engineers* に由来する。
- 103 **管理者(administrator)** TSF が実装するすべての方針に関して完全な信頼を得ているエンティティ。

用語と定義

すべての PP または ST が、管理者に対し同じ信頼レベルを想定しているわけではない。一般的に管理者は、TOE の ST における方針にいつも従うと想定される。これらの方針の一部は TOE の機能に関係してもよいし、残りは運用環境に関係してもよい。

- 104 **コールツリー(call tree)** システム内のモジュールを、モジュールが相互に呼び出すことを示す図の形式で識別する。

出典「IEEE Std 610.12-1990」。

- 105 **凝集度(cohesion)** 単一のソフトウェアモジュールによって実行されるタスクが相互に関連するモジュール強度の方法とその度合い。

「IEEE Std 610.12-1990」

凝集度には、偶発的、通信的、機能的、論理的、連続的、時間的の各タイプがある。これらの凝集度のタイプは、それぞれの用語により記述される。

- 106 **偶発的凝集度(coincidental cohesion)** この特性を持つモジュールは、関連がまったくない、またはほとんどないアクティビティを実行する。

「IEEE Std 610.12-1990」

凝集度(cohesion)参照。

- 107 **通信的凝集度(communicational cohesion)** ある機能が同じモジュール内の他の機能に対して出力を生成するか、または他の機能からの出力を使用する機能を含むモジュール。

「IEEE Std 610.12-1990」

- 108 凝集度(cohesion)参照。

- 109 通信的に凝縮するモジュールの例としては、必須チェック、裁量チェック、及び能力チェックを含んだアクセスチェックモジュールが挙げられる。

- 110 **複雑性(complexity)** ソフトウェアの理解、及び分析、テスト、保守に関する難易度を示す指標。

「IEEE Std 610.12-1990」

- 111 複雑性を軽減することは、モジュール分解、階層化、及び最小化を使用する場合の最終目標である。結合度及び凝集度を管理することは、この目標に大きく寄与する。

- 112 ソフトウェアエンジニアリング分野では、ソースコードの複雑性を測定するための尺度の開発の試みに、多大な労力が費やされてきた。これらの尺度の多くは、演算子やオペランドの数、制御フローグラフの複雑性(循環的複雑性)、ソースコードの行数、実行可能コードに対するコメントの比率、その他の類似する指標のような、簡単に算定できるソースコードの特性を使用する。より簡単に理解できるコードを生成するうえで、コーディング標準が有効な手段であることが分かってきた。

- 113 この TSF 内部構造(ADV_INT)ファミリーは、すべてのコンポーネントで複雑性分析を要求する。開発者は、複雑性が十分に軽減されたことを主張する際に、その裏付けを提供することを期待される。この裏付けには、開発者が使用したプログラミング標準、及びすべてのモジュールが標準に準拠していることの明示(あるいはソフトウェアエンジニアリングの論証により正当化された一部の例外が存在することの明示)が含まれる。ソースコードの特性を測定するために使用したツールの結果が含まれることもある。または、開発者が適切とみなすその他の裏付けを含むこともある。
- 114 **結合度(coupling)** ソフトウェアモジュール間の相互依存の方法とその度合い。
「IEEE Std 610.12-1990」
結合には、コール、共通、内容の各タイプがある。以下に、その特徴を示す:
- 115 **コール結合(call coupling)** 2つのモジュール間の関係。
コール結合の例としては、データ、スタンプ、制御がある。
- 116 **コール結合(データ) (call coupling (data))** 厳密に単一のデータ項目を表すコールパラメタの使用を通じて通信する、2つのモジュール間の関係。
コール結合(call coupling)参照。
- 117 **コール結合(スタンプ) (call coupling (stamp))** 複数のフィールドからなるコールパラメタ、または意味のある内部構造を持つコールパラメタの使用を通じた、2つのモジュール間の関係。
コール結合(call coupling)参照。
- 118 **コール結合(制御) (call coupling (control))** モジュールの一方が、他方の内部ロジックに影響するように意図された情報を渡す場合の、2つのモジュール間の関係。
コール結合(call coupling)参照。
- 119 **共通結合(common coupling)** 共通データ領域または共通システム資源を共有する2つのモジュール間の関係。
- 120 グローバル変数は、それを使用するモジュールが共通結合されていることを示す。グローバル変数による共通結合は、一般に許可されているが、その程度は限定される。
- 121 例えば、グローバル領域に置かれているが、単一のモジュールのみが使用する変数は、配置が不適切であり、削除するべきである。このほかに、グローバル変数の適切性を評定する際には、次の要因を検討する必要がある:

- a) グローバル変数を改変するモジュールの数: 一般に、グローバル変数の内容を制御する責任は1つのモジュールのみに割り当てべきであるが、第2のモジュールと責任を共有する状況も発生する。このような場合は、十分な正当性を提示する必要がある。2つより多いモジュール間でこの責任を共有することは受け入れられない(この評定を行う際には、変数の内容について実際に責任を負うモジュールを注意して決定すべきである。例えば、単一のルーチンを使用して変数を改変する場合に、ルーチンが単にその呼び出し側から要求された改変を実行すると、呼び出し側モジュールが責任を負うことになり、責任を負うモジュールが複数になる可能性がある)。さらに、複雑さ決定の一環として、2つのモジュールがグローバル変数の内容について責任を負う場合は、それらのモジュール間で改変がどのように調整されるかが明確に示されるべきである。
- b) グローバル変数を参照するモジュールの数: 一般に、グローバル変数を参照するモジュールの数に制限はないが、多数のモジュールが参照する場合は、有効性と必要性を検査すべきである。

122 **コンテンツ結合 (content coupling)** 一方が他方の内部を直接参照できる場合の、2つのモジュール間の関係。

例えば、他方のモジュールのコードを改変する場合やその内部ラベルを参照する場合。その結果、一方のモジュールの内容の一部または全部が、他方のモジュールに実質的に包含される。内容結合は非通知型モジュールインタフェースを使用しているとみなすことができる;これは、通知型モジュールインタフェースのみを使用するコール結合とは対照的である。

123 **ドメイン分離(domain separation)** TSFが各利用者とTSFに対して個々のセキュリティドメインを定義し、利用者のプロセスが、TSFの別の利用者のセキュリティドメイン、またはTSFの内容に影響を与えることができる利用者プロセスが存在しないことを保証するセキュリティアーキテクチャ特性。

124 **機能的凝集度(functional cohesion)** 単一の目的に関連するアクティビティを実行するモジュールの機能特性。

「IEEE Std 610.12-1990」

この特性を持つモジュールは、単一の目的に関連するアクティビティを実行する。機能的に凝集するモジュールは、スタックマネージャやキューマネージャのように、単一タイプの入力を単一タイプの出力に変換する。凝集度 (cohesion)も参照。

125 **相互作用(interaction)** エンティティ間の一般的な通信ベースの関係。

126 **インタフェース(interface)** コンポーネントまたはモジュールと対話するための手段。

127 **階層化(layering)** ある層がサービスに関して階層内でそれより下の層にのみ依存し、さらにそのサービスをそれより上の層にのみ提供するように、モジュールの独立したグループが、個々の責任を持つよう階層的に体系化された設計技法。

厳密な階層化によって、各層がその直下の層からのみサービスを受け、その直上の層にのみサービスを提供するように制約を強化できる。

- 128 **論理的凝集度(logical cohesion)** 類似するアクティビティを異なるデータ構造で実行するモジュールの手続き的凝縮度の特性。
モジュールの機能が、別々の入力に対して、関連しているが異なっている操作を実行する場合、そのモジュールは論理的凝集度を示す。凝集度(cohesion)も参照。
- 129 **モジュール分解(modular decomposition)** 設計、開発及び評価を容易にする目的でシステムをコンポーネントに分割するプロセス。
「IEEE Std 610.12-1990」
- 130 **非バイパス性(TSF の) (non-bypassability (of the TSF))** すべての SFR 関連アクションが TSF によって仲介されるセキュリティアーキテクチャ特性。
- 131 **手続き的凝集度(procedural cohesion)** 論理的凝集度(logical cohesion)参照。
- 132 **セキュリティドメイン(security domain)** 能動的なエンティティがアクセス権を有する資源の集まり。
- 133 **連続的凝集度(sequential cohesion)** モジュールにおいて、各機能の出力がその次の機能の入力となる機能を含むモジュール。
「IEEE Std 610.12-1990」
連続的に凝集するモジュールの例としては、監査レコードを書き出す機能及び特定タイプの監査違反の累積数をカウントし続ける機能を含んだモジュールが挙げられる。
- 134 **ソフトウェアエンジニアリング(software engineering)** ソフトウェアの開発、運用、保守に対し、系統的かつ統制的で定量化可能な手法を適用すること。つまり、ソフトウェアに工学技術を適用すること。
「IEEE Std 610.12-1990」
一般的な工学技術の実践と同様に、工学技術の原則を適用する際には、ある程度の判断を用いなければならない。
選択には、モジュール分解、階層化、及び最小化の手段の適用以外にも、数多くの要因が影響する。例えば、開発者が、当初は実装されないが将来使用するアプリケーションを念頭に置いてシステムを設計することがある。この場合、開発者は将来使用するアプリケーションを処理するロジックを、それらのアプリケーションを完全に実装する前に組み込むことを選択してもよい。さらに、まだ実装されていないモジュールに対するコールをいくつか組み込んで、コールスタブをそのまま残してもよい。適切に構造化されたプログラムからのこのような逸脱に対して開発者が示す正当性は、適切なソフトウェアエンジニアリングの分野を適用するとともに判断を用いて評定する必要がある。
- 135 **時間的凝集度(temporal cohesion)** この特性を持つモジュールでは、機能を同時に実行する必要がある。
「IEEE Std 610.12-1990」出典。時間的に凝集するモジュールの例としては、初期化、回復、シャットダウンなどのモジュールが挙げられる。
- 136 **TSF 自己保護(TSF self-protection)** TSF 以外のコードまたはエンティティによって、TSF が破損されることのないセキュリティアーキテクチャ特性

4.3 AGDクラスに関連する用語及び定義

137 **設置(installation)** TOE をその運用環境に組み入れ、運用状態にする人間の利用者によって実行される手続き。

この操作は、TOE を受領して受け入れた後に通常は 1 回のみ実行される。TOE は ST により許可された設定にすることが期待されている。同様のプロセスを開発者が実行しなければならない場合、それらのプロセスは、ALC: ライフサイクルサポート全体を通じて「生成」(generation)と表される。TOE に、定期的に繰り返す必要のない初期立ち上げが必要である場合、そのプロセスはここでは設置として分類される。

138 **運用(operation)** TOE の使用フェーズで、これには、配付及び準備後の TOE の「通常使用」、管理、及び保守が含まれる。

139 **準備(preparation)** 配付された TOE の顧客による受け入れと、起動、初期化、立ち上げ、運用可能な状態への TOE の移行などを含む設置で構成される、製品のライフサイクルフェーズにおけるアクティビティ。

4.4 ALCクラスに関連する用語及び定義

140 **受入れ基準(acceptance criteria)** 受入れ手続きを実行する際に適用される基準(例えば、文書レビューの成功、またはソフトウェア、ファームウェア、ハードウェアにおけるテストの成功)。

141 **受入れ手続き(acceptance procedure)** 新たに作成または改変された構成要素を TOE の一部として受け入れるか、またはそれらの構成要素をライフサイクルの次のステップに移すために実行される手続き。

142 これらの手続きによって、受け入れ責任のある役割または個人、及び受け入れを決定するために適用される基準が識別される。

143 受入れ状況にはいくつかのタイプがあり、その一部は重複してもよい:

- a) 構成管理システムに最初に要素を受け入れる場合。特に、他の製造者のソフトウェア、ファームウェア、及びハードウェアコンポーネントを TOE に組み込む場合(「統合」);
- b) TOE の構成の各段階(例えば、モジュール、サブシステム、完成した TOE の品質管理)で、構成要素を次のライフサイクルフェーズに移す場合;
- c) 異なる開発サイト間での構成要素(例えば、TOE または準備製品の部分)の転送後;
- d) 消費者への TOE の配付後。

144 **構成管理(configuration management)** 以下の技術、管理上の指針及び調査に適用される原則:構成アイテムの機能的及び物理的特性を識別して文書化する、それらの特性の変更を制御する、変更処理及び実施状況を記録及び報告する、特定の要求への適合を検証する。

「IEEE Std 610.12-1990」

145 **CM 証拠資料(CM documentation)** CM 出力、CM リスト(構成リスト)、CM システム記録、CM 計画及び CM 用法証拠資料を含むすべての CM 証拠資料。

- 146 **構成管理証拠(configuration management evidence)** CM システムの正しい運用を確信するために使用されるすべての要素。
- 例えば、CM 出力、開発者が提供する根拠、評価者がサイト訪問中に行った観察記録、実験またはインタビューが含まれる。
- 147 **構成要素(configuration item)** TOE の開発中に CM システムによって管理されるオブジェクト。
- これらは、TOE の一部または評価文書や開発ツールのような TOE の開発に関連するオブジェクトかもしれない。CM 要素は、CM システムに直接格納されるか(例えばファイル)、またはそれらのバージョンと共に参照によって格納されてもよい(例えばハードウェア部品)。
- 148 **構成リスト(configuration list)** 完全な製品の特定バージョンに関連する各構成管理要素の正確なバージョンを伴う特定の製品のすべての構成要素をリストする構成管理出力文書。
- このリストによって、製品の評価済みバージョンに属する要素と、製品の別のバージョンに属するその要素の別バージョンとを区別することが可能となる。最終的な構成管理リストは、特定の製品の特定バージョンに対する固有の文書である(このリストは構成管理ツール内の電子文書にすることができる。その場合は、システムの実出力ではなく、システム特定のビューまたはシステムの一部として参照できる。ただし、実際に評価で使用される場合は、おそらく評価証拠資料の一部として構成リストが配付される)。構成リストは、ALC_CMC の構成管理要件下にある要素を定義する。
- 149 **構成管理出力(configuration management output)** 構成管理システムによって生成または実施された、構成管理に関連する結果。
- これらの構成管理関連結果は、文書(例えば、データが出力された用紙、構成管理システム記録、ロギングデータ、ハードコピー、電子出力データ)、及びアクション(構成管理の指示を実行するための手動による措置)として発生する。このような構成管理出力の例には、構成リスト、構成管理計画、及び/または製品ライフサイクルの間のふるまいがある。
- 150 **構成管理計画(configuration management plan)** TOE に対し構成管理システムがどのように使用されるかの記述。
- 構成管理計画を発行する目的は、スタッフメンバがそれぞれの責務を明確に把握できるようにすることである。構成管理システム全体の観点では、構成管理計画を出力文書とみなすことができる(構成管理システムのアプリケーションの一部として生成することができるため)。具体的なプロジェクトの観点では、構成管理計画は用法文書である。なぜなら、プロジェクトチームのメンバが、プロジェクトの期間中に実行しなければならないステップを理解するために使用するからである。構成管理計画は、特定の製品に対するシステムの用法を定義する。別の製品に対して、同じシステムが異なる範囲で用いられてもよい。つまり構成管理計画は、TOE の開発中に使用される会社の構成管理システムの実出力を定義し、記述する。
- 151 **構成管理システム(configuration management system)** 製品のライフサイクルにおいて、開発者がその製品の設定を開発及び保守するために使用する手続きとツールのセット(それらの証拠資料も含む)。
- 構成管理システムでは、厳格性の度合い及び機能は様々である。上位レベルでは、構成管理システムで欠陥修正、変更管理、及びその他の追跡メカニズムを自動化することができる。

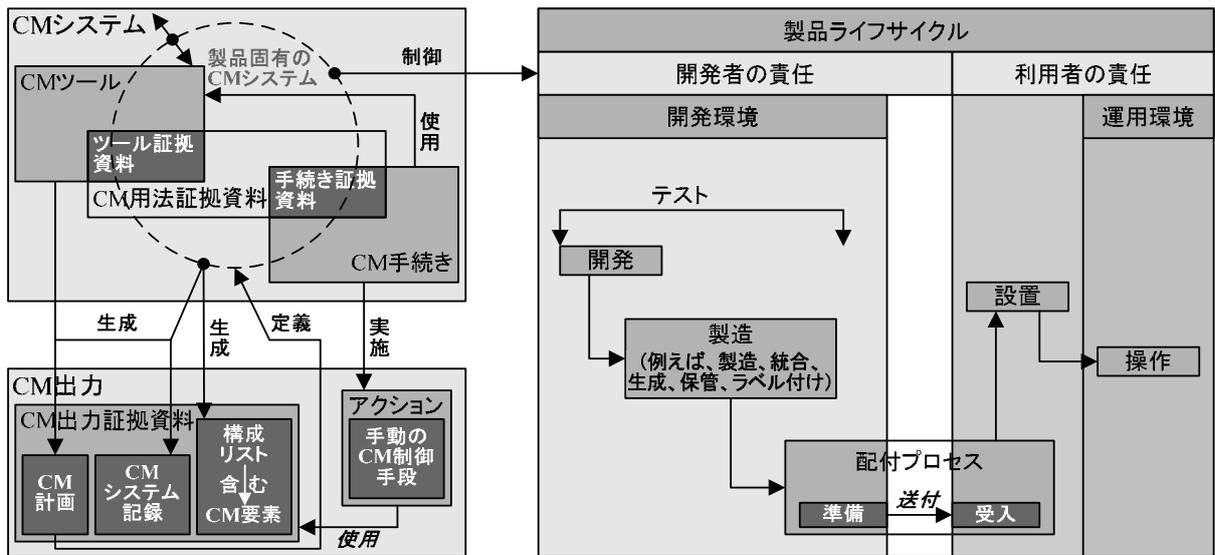
- 152 **構成管理システム記録(configuration management system record)** 重要な構成管理アクティビティを証拠資料として提出する構成管理システムの運用中に生成される出力。
構成管理システム記録の例には、構成管理要素変更管理用紙や構成管理要素アクセス許可紙が含まれる。
- 153 **構成管理ツール(configuration management tool)** 構成管理システムを実現またはサポートする手動操作の、または自動化されたツール。
例えば、TOE の部分のバージョンを管理するツールなどが含まれる。
- 154 **構成管理用法証拠資料(configuration management usage documentation)** 例えば、ハンドブック、規則、及び/またはツールと手続きの証拠資料などを使用して、構成管理システムがどのように定義され、適用されるかを記述する構成管理システムの一部。
- 155 **配付(delivery)** 完成した TOE の製造環境から顧客の下への移送。
製品ライフサイクルのフェーズには、開発サイトでのパッケージングと保管を含むことができるが、未完成の TOE や TOE の部分を開発者間または開発サイト間で移送する処理は含まれない。
- 156 **開発者(developer)** TOE の開発に責任を負う組織。
- 157 **開発(development)** TOE の実装表現の生成に関する製品ライフサイクルのフェーズ。
ALC 要件全般では、開発及び関連用語(開発者、開発する)が、より一般的な意味で開発と製造を含むように意図されている。
- 158 **開発ツール(development tool)** TOE の開発と製造をサポートするツール(該当する場合はテストソフトウェアも含む)。
例えばソフトウェア TOE の場合は、プログラミング言語、コンパイラ、リンカ、及び生成ツールが通常は開発ツールである。
- 159 **実装表現(implementation representation)** 最も抽象度の低い TSF の表現。特に、それ以上の設計の詳細化をすることなく、それ自体で TSF を作成するのに使用される表現。
すぐコンパイルされる状態にあるソースコード、または実際のハードウェアの製造に用いられるハードウェア図面は、実装表現の一部の例である。
- 160 **ライフサイクル(life-cycle)** オブジェクト(例えば、製品やシステム)が存在する期間における一連の段階。
- 161 **ライフサイクル定義(life-cycle definition)** ライフサイクルモデルの定義。
- 162 **ライフサイクルモデル(life-cycle model)** ある特定のオブジェクトのライフサイクルの管理で使用される段階とそれらの関係、各段階の連鎖がどのようなものか、及び段階の有する上位レベルの特性の記述。

163

製造(production) 製造ライフサイクルフェーズは、開発フェーズに続き、実装表現から TOE の実装への変換、つまり顧客に配付できる状態への変換で構成される。

このフェーズは、TOE の製造、統合、生成、内部転送、保管、及びラベル付けで構成することができる。

用語と定義



*CM証拠資料=CM用法証拠資料+CM出力証拠資料

図1 CM及び製品ライフサイクルの用語

4.5 AVAクラスに関連する用語及び定義

- 164 **隠れチャンネル(covert channel)** 利用者がマルチレベル分離方針及びTOEの観察不能性要件にひそかに違反することを可能にするために実施される不正信号チャンネル。
- 165 **遭遇した潜在的脆弱性(encountered potential vulnerability)** 評価者が評価アクティビティを実行中に識別した、SFRの侵害に使用される可能性のあるTOEの潜在的脆弱性。
- 166 **悪用可能脆弱性(exploitable vulnerability)** TOEの運用環境でSFRを侵害するために使用されることがあるTOEの弱点。
- 167 **監視攻撃(monitoring attacks)** 攻撃方法の包括的なカテゴリ。これには、ガイダンス文書に対応した方法でTOEを運用することにより、TOEの機密内部データの開示を目的とする受動的な解析技術が含まれる。
- 168 **潜在的脆弱性(potential vulnerability)** 疑われるが、確認されていない弱点。
疑いは、SFRを侵略するような仮定される攻撃経路より生じる。
- 169 **残存脆弱性(residual vulnerability)** TOEの運用環境では悪用できないが、TOEの運用環境において予想を超える攻撃が可能な攻撃者が、SFRを侵害するために使用されることがある弱点。
- 170 **脆弱性(vulnerability)** ある環境のSFRを侵害するために使用されることがあるTOEの弱点。

4.6 ACOクラスに関連する用語及び定義

- 171 **基本コンポーネント(base component)** 統合 TOE 内のエンティティ。それ自体が評価のサブジェクトとなっていて、依存するコンポーネントにサービスと資源を提供する。
- 172 **互換(コンポーネント) (compatible (components))** 一貫した運用環境で、各コンポーネントの対応するインタフェースを通じて、他のコンポーネントによって要求されるサービスを提供することのできるコンポーネントの特性。
- 173 **コンポーネント TOE(component TOE)** 他の統合 TOE の一部で評価に合格した TOE。
- 174 **統合 TOE(composed TOE)** 評価に合格した 2 つ以上のコンポーネントのみで構成される TOE。
- 175 **依存コンポーネント(dependent component)** 統合 TOE 内のエンティティ。それ自体が評価のサブジェクトであり、基本コンポーネントによるサービスの提供に依存する。
- 176 **機能インタフェース(functional interface)** セキュリティ機能要件の実施に直接かわらない TOE 機能へのアクセスを利用者に提供する(外部)インタフェース。
- 統合 TOE では、これは統合 TOE の運用をサポートするために依存コンポーネントによって要求され、基本コンポーネントによって提供されるインタフェースである。

5 記号と略語

177

以下の略語は、CC の 1 つ以上のパートで用いられる:

API	アプリケーションプログラミングインタフェース(Application Programming Interface)
CAP	統合保証パッケージ(Composed Assurance Package)
CC	コモンクライテリア(Common Criteria)
CCRA	ITセキュリティ分野でのコモンクライテリア認証書の承認に関するアレンジメント(Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security)
CM	構成管理(Configuration Management)
DAC	任意アクセス制御(Discretionary Access Control)
EAL	評価保証レベル(Evaluation Assurance Level)
GHz	ギガヘルツ(Gigahertz)
GUI	グラフィカルユーザインタフェース(Graphical User Interface)
IC	集積回路(Integrated Circuit)
IOCTL	入出力制御(Input Output Control)
IP	インターネットプロトコル(Internet Protocol)
IT	情報技術(Information Technology)
MB	メガバイト(Mega Byte)
OS	オペレーティングシステム(Operating System)
OSP	組織のセキュリティ方針(Organisational Security Policy)
PC	パーソナルコンピュータ(Personal Computer)
PCI	周辺コンポーネント相互接続(Peripheral Component Interconnect)
PKI	公開鍵基盤(Public Key Infrastructure)
PP	プロテクションプロファイル(Protection Profile)
RAM	ランダムアクセスメモリ(Random Access Memory)
RPC	リモートプロシージャコール(Remote Procedure Call)
SAR	セキュリティ保証要件(Security Assurance Requirement)
SFR	セキュリティ機能要件(Security Functional Requirement)
SFP	セキュリティ機能方針(Security Function Policy)
SPD	セキュリティ課題定義(Security Problem Definition)
ST	セキュリティターゲット(Security Target)
TCP	伝送制御プロトコル(Transmission Control Protocol)
TOE	評価対象(Target of Evaluation)
TSF	TOE セキュリティ機能(TOE Security Functionality)

TSFI	TSF インタフェース(TSF Interface)
VPN	仮想プライベートネットワーク(Virtual Private Network)

6 概要

178 この章では、CC の主な概念について述べ、「TOE」の概念、CC の対象読者、及び CC の
他の章で資料を提示するためのアプローチを明らかにする。

6.1 TOE

179 CC は、評価対象に関して柔軟であるため、一般に理解されているような IT 製品の境界に
関連付けられていない。そのため評価の中では、CC は「TOE」(評価対象)という用語を使用する。

180 TOE は、ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び/またはハードウェア
のセットとして定義される。

181 TOE が IT 製品で構成される場合もあるが、そうである必要もない。TOE は、IT 製品、IT
製品の一部、IT 製品のセット、製品にならない固有な技術、またはそれらの組み合わせに
することもできる。

182 CC に関する限り、TOE と IT 製品間の正確な関係は、以下の 1 つの側面のみに関して重
要である。つまり、IT 製品の一部のみを含む TOE の評価は、IT 製品全体の評価と誤解さ
れる記述とするべきではない。

183 TOE の例を以下に示す：

ソフトウェアアプリケーション；

オペレーティングシステム；

オペレーティングシステムと組み合わせたソフトウェアアプリケーション；

オペレーティングシステム及びワークステーションと組み合わせたソフトウェアアプリ
ケーション；

ワークステーションと組み合わせたオペレーティングシステム；

スマートカード集積回路；

スマートカード集積回路の暗号化コプロセッサ；

すべての端末、サーバ、ネットワーク機器、及びソフトウェアを含むローカルエリア
ネットワーク；

通常データベースアプリケーションと関連付けられるリモートクライアントソフトウェア
を除くデータベースアプリケーション。

6.1.1 TOEの様々な形態

184 CC では、TOE は次のような複数の形態を取ることがある(ソフトウェア TOE の場合)：

構成管理システムのファイルのリスト；

コンパイルされたばかりの単一のマスタコピー；

顧客に発送する準備の整った CD-ROM とマニュアルを入れたボックス;
インストール済みの運用バージョン。

185 以上のすべてが TOE とみなされる。CC の残りの部分で「TOE」という用語が使用される場合、文脈によって意味する形態が決定される。

6.1.2 TOEの様々な構成

186 一般に、IT 製品はいろいろな方法で構成され、様々な方法でインストールされ、様々なオプションを有効または無効にすることができる。CC 評価中に TOE が特定の要件を満たしているかどうか決定されると、この構成の柔軟性が、TOE のすべての可能な構成が要件を満たさなければならないという問題をもたらすことがある。このため、TOE のガイダンス部分では、TOE で可能な構成を強硬に制限することがある。つまり、TOE のガイダンスは、IT 製品の一般ガイダンスとは異なることがある。

187 この一例としては、オペレーティングシステムの IT 製品がある。この製品は、多くの方法で構成できる(例えば、利用者の種別、利用者の数、許可/禁止される外部接続の種別、オプションの有効化/無効化など)。

188 多くのオプション(例えば、すべての種別の外部接続の許可またはシステム管理者の認証の不要など)によって、TOE が要件を満たさなくなることがあるため、同じ IT 製品が TOE となり、要件の妥当なセットで評価される場合は、構成をなおさら厳格に制御するべきである。

189 このため、一般に、IT 製品のガイダンス(多くの構成を許可する)と TOE のガイダンス(唯一の構成またはセキュリティ関連の方法に関して異なる構成のみを許可する)の間には相違がある。

190 TOE のガイダンスでも複数の構成が許可される場合、これらの構成は一括して「TOE」と呼ばれ、各構成が TOE に課される要件を満たさなければならない。

6.2 CCの対象読者

191 TOE のセキュリティ特性の評価に一般的関心を有するのは、3 つのグループ、すなわち消費者、開発者、及び評価者である。この CC パート1で示す基準は、3 つのグループすべてのニーズに対応できるように構成されている。この 3 つのグループはすべて、CC の主な利用者とみなされており、以下の段落で説明するようにこの基準からの恩恵を被ることができる。

6.2.1 消費者

192 CC は、評価により消費者のニーズが満たされることを保証するように記述されているが、それは、これが評価プロセスの基本的な目的であり、正当な理由だからである。

193 消費者は、TOE がそれぞれのセキュリティニーズを満たしているかどうかを決定する一助として、評価結果を用いることができる。これらのセキュリティニーズは、リスク分析と方針の方向付けの双方の結果として、通常識別される。消費者はまた、様々な TOE を比較する場合に評価結果を用いることもできる。

194 CC は、消費者、特に関心を持つ消費者のグループ及びコミュニティに対して、セキュリティ要件を明確に表現するための、プロテクションプロファイル(PP)と呼ばれる実装に依存しない体系を提供する。

概要

6.2.2 開発者

195 CCは、TOEの評価の準備と支援、及び各TOEが満たすべきセキュリティ要件の識別において、開発者をサポートすることを目的としている。これらの要件は、セキュリティターゲット(ST)と呼ばれる実装に依存する構成物に含まれている。このSTは、1つ以上のPPに基づき、当該PPの規定に従って消費者からのセキュリティ要件に準拠していることを示すことができる。

196 CCは、これらの要件に対してTOEの評価を裏付けるのに必要な証拠を提供する責任及びアクションを決定するために用いることができる。また、その証拠の内容及び提示も定義されている。

6.2.3 評価者

197 CCは、セキュリティ要件に対するTOEの適合について判断を下す際に、評価者が用いる基準を含んでいる。CCは、評価者が実施しなければならない一般的なアクションのセットを記述する。CCは、それらのアクションの実行に当たって従うべき手続きを具体的に述べていないことに注意のこと。これらの手順の詳細については、6.4節を参照のこと。

6.2.4 その他の対象者

198 CCは、TOEのITセキュリティ特性の仕様と評価に向かって志向していると同時に、ITセキュリティに関係または責任のあるすべての関係者のための参考資料としても役に立つことがある。以下に、CCに含まれている情報から恩恵を受けることができるその他の利益グループをいくつか示す：

- a) 組織のITセキュリティ方針と要件の決定及び実現に責任のある、システム管理者やシステムセキュリティ担当役員；
- b) (TOEから構成された、またはTOEを含む)ITソリューションのセキュリティの妥当性評価に責任のある、内部及び外部の監査員；
- c) IT製品のセキュリティ特性の仕様に責任のある、セキュリティ立案者及び設計者；
- d) 特定の環境内におけるITソリューション使用の承認に責任のある、認定者；
- e) 評価の依頼及び支援に責任のある、評価のスポンサー；
- f) ITセキュリティ評価計画の管理及び監督に責任のある、評価監督機関。

6.3 CCの各パート

199 CCは、以下に示すように別のものであるが、関連する3つのパートとして提供されている。各パートの記述に用いられている用語については、7章で説明する。

- a) **パート1「概説と一般モデル」**は、CCの序説である。ITセキュリティ評価の一般的な概念及び原則を定義し、評価の一般モデルを提示する。
- b) **パート2「セキュリティ機能コンポーネント」**は、TOEの機能要件の基となる標準テンプレートとして、機能コンポーネントのセットを規定している。CCパート2は、機能コンポーネントのセットをカタログ化し、ファミリー及びクラスを編成している。

- c) **パート3「セキュリティ保証コンポーネント」**は、TOEの保証要件の基となる標準テンプレートとして、保証コンポーネントのセットを規定している。CCパート3は、保証コンポーネントのセットをカタログ化し、ファミリー及びクラスを編成している。また、PP及びSTの評価基準も定義しており、評価保証レベル(EAL)と呼ばれる7つの定義済み保証パッケージも示している。

200 上記のCCの3つのパートを支援するために、その他の文書が公開されており、CEMは基礎としてCCを用いたITセキュリティ評価のための手法を提供する。技術的根拠に関する資料やガイダンス文書を含め、その他の文書も公開されることが予想される。

201 以下の表に、3つの主な対象読者グループがCCの各パートをどのように利用すべきかを示す。

	消費者	開発者	評価者
パート1	予備知識のために使用、及び参照のために使用しなければならない。PPの構成についてのガイダンス。	予備知識及び参照目的のために使用。TOEのセキュリティ仕様の開発のために使用しなければならない。	PP及びSTの構成において、参照資料として、及びガイダンスとして、使用しなければならない。
パート2	TOEの要件のステートメントを定式化する際のガイダンス及び参照資料として使用。	TOEの機能要件のステートメントを解釈する際、及びTOEの機能仕様を定式化する際の参照資料として使用しなければならない。	機能要件のステートメントを解釈する際に、参照資料として使用しなければならない。
パート3	必要な保証レベルを決定する際のガイダンスとして使用。	TOEの保証要件のステートメントを解釈する際、及びTOEの保証アプローチを決定する際の参照資料として使用。	保証要件のステートメントを解釈する際の参照資料として使用。

表1 コモンクライテリアのロードマップ

6.4 評価の枠組み

202 評価結果間の比較可能性を高めるには、標準を定め、評価の品質を監視し、評価設備と評価者が遵守しなければならない規則を管理する信頼すべき評価制度の枠組みの中で評価が実施されるべきである。

203 CCは、規制上の枠組みに関する要件を記述していない。しかしながら、こうした評価結果に対する相互承認の目標を達成するには、様々な評価監督機関の規制上の枠組み間の一貫性が必要になる。

204 評価結果の間でより大きな比較可能性を達成するための2番目の方法は、評価結果を生成するために共通の方法を使用することである。CCでは、この方法はCEMで説明されている。

205 共通評価方法を用いることは、結果の再現性と客観性に寄与するが、それだけでは十分とは言えない。評価基準の多くは、一貫性を達成するのがより難しい専門家の判断と予備知識の適用を要求する。評価結果の一貫性を高めるために、最終評価結果は認証プロセスにかけられることもある。

概要

- 206 認証プロセスは、通常公開される最終的な認証書または承認書の提供に至る独立した評価結果の検査である。認証プロセスは、IT セキュリティ基準の適用における一貫性を高める手段である。
- 207 評価制度及び認証プロセスは、当該制度及びプロセスを実行する評価監督機関の責任であり、CC の範囲外である。

7 一般モデル

208 この章では、概念が用いられるべき枠組み、CC における概念を適用するアプローチを含め、CC 全体にわたって用いられる一般的概念を示す。CC のパート1の利用者が参照しなければならないCC のパート2とパート3 では、これらの概念の使用について詳述しており、ここに述べるアプローチを用いることを前提としている。さらに、評価アクティビティを実施しようとする CC の利用者に対しては、CEM が当てはまる。この章は、IT セキュリティについて相応の知識があることを前提としており、この分野に関する手引きの役割を果たすことは意図していない。

209 CC は、セキュリティについてセキュリティの概念と用語のセットを用いて論じている。これらの概念及び用語を理解していることが、CC を効果的に用いるための必要条件である。ただし、概念自体は極めて一般的なものであり、CC が適用されるITセキュリティの課題の種類を限定することを意図したものではない。

7.1 資産及び対抗策

210 セキュリティは、資産の保護に関係する。資産とは、何者かによって価値が認められるエンティティである。資産の例を次に示す：

ファイルまたはサーバの内容；

投票で投じられた票の真正性；

電子商取引の処理の可用性；

高価なプリンタの使用可能性；

機密施設への立ち入り。

ただし、価値とは非常に主観的であるため、ほとんどすべてのものが資産になりうる。

211 このような資産がある環境は、運用環境と呼ばれる。運用環境の(側面の)例を次に示す：

a) 銀行のコンピュータールーム；

b) インターネットに接続されたコンピュータネットワーク；

c) LAN；

d) 一般的なオフィス環境。

212 資産の多くは情報の形をとり、情報の所有者が規定した要件を満たす IT 製品によって保存されたり、処理されたり、伝送されたりする。情報の所有者は、このような情報の可用性、まき散らし、及び改変を厳しく管理し、対抗策によって資産を脅威から保護することが必要になる。図 2 に、このような上位レベルの概念と関係を示す。

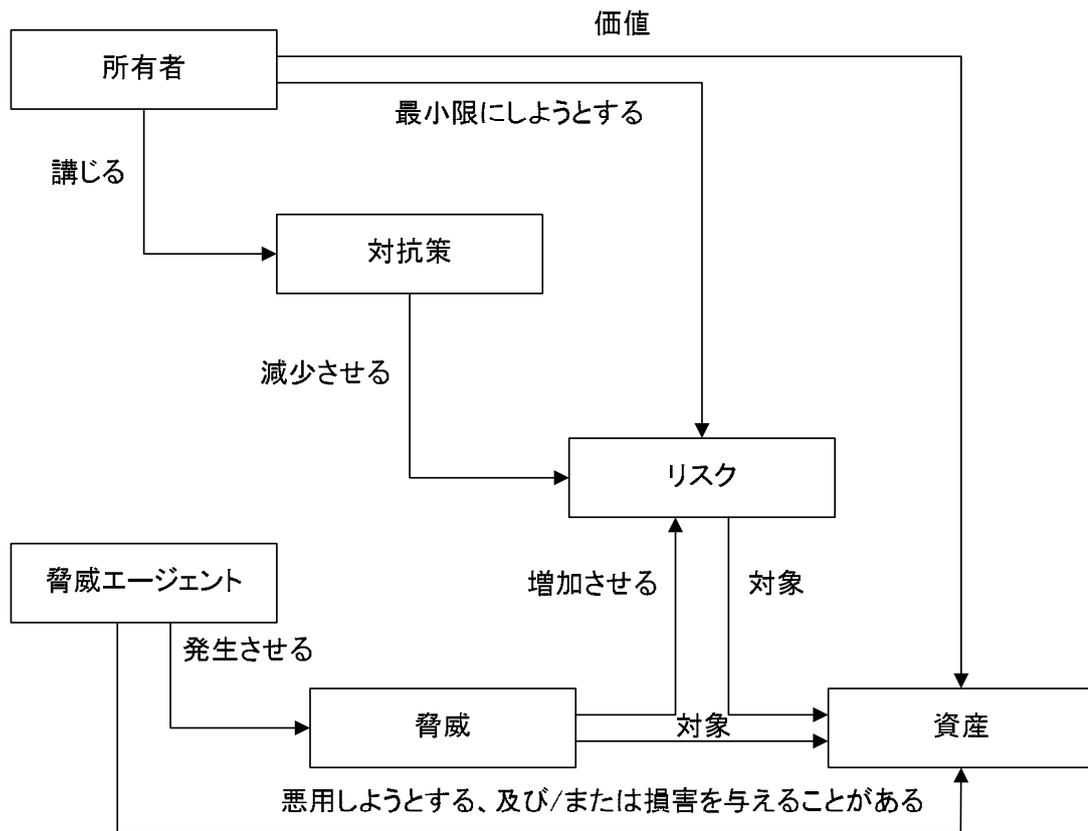


図2 セキュリティの概念と関係

- 213 対象となる資産を保護することは、それらの資産の価値を認識している所有者の責任である。実在するまたは想定される脅威エージェントもまたその資産の価値を認識しており、所有者の利益に反する形で資産を悪用しようとすることがある。脅威エージェントの例には、ハッカー、悪意のある利用者、(誤りを犯すことがある)悪意のない利用者、コンピュータ処理、及び事故などがある。
- 214 資産の所有者は、そうした脅威を、所有者にとっての資産の価値が減少することになるような資産の侵害の可能性と捉えるであろう。一般に、セキュリティ固有の侵害には、資産の機密性の損失、資産の完全性の損失、及び資産の可用性の損失などがあるが、これらだけではない。
- 215 したがって、このような脅威が実現する可能性と、その場合の資産への影響に基づいて、脅威から資産に対するリスクが生じる。その後、資産へのリスクを減らすために、対抗策が講じられる。対抗策は、IT 対抗策(ファイアウォール及びスマートカードなど)と非IT の対抗策(警備及び手続きなど)から構成されることがある。セキュリティ対抗策(管理策)についての総合的な詳解については、ISO/IEC 27001 及び ISO/IEC 27002 も参照すること。
- 216 資産に対する責任は資産の所有者が負う(負わされる)ことがあるため、所有者は資産を脅威にさらすリスクを受け入れる判断を擁護できるべきである。
- 217 この判断を擁護するための2つの重要な要素は、以下のことを証明できるかどうかである:

対策が十分であること。つまり、対策が主張する動作を実行する場合、資産への脅威は対抗される；

対策が正確であること。つまり、対策が主張する動作を実行すること。

218

資産の所有者の多くは、対策の十分性及び正確性を判断するのに必要な知識、技能、または資源を欠いているが、場合によっては対策の開発者の主張だけに頼ることを望まないこともある。したがって、資産の所有者は、対策の評価を依頼することにより、対策の一部または全部の十分性及び正確性に対する信頼度を向上させることを選択できる。

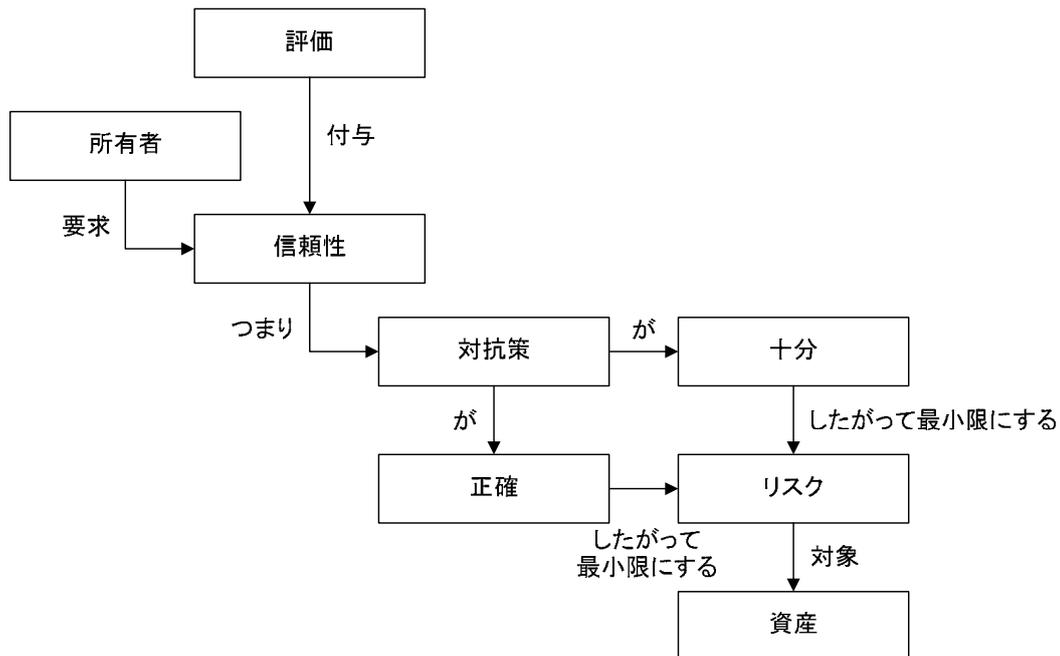


図3 評価の概念と関係

7.1.1 対策の十分性

219 評価において、対策の十分性は、セキュリティターゲットと呼ばれる構成物を通じて分析される。この節では、この構成物の概要を示す。より詳細で完全な記述については、附属書 A を参照のこと。

220 セキュリティターゲットでは、初めに資産及び資産への脅威について記述する。次に、セキュリティターゲットは、(セキュリティ対策方針の形式で)対策を記述し、その対策が脅威に対抗するために十分であること、つまり対策が主張する動作を実行する場合、脅威が対抗されることを実証する。

221 次に、セキュリティターゲットは、対策を以下の 2 つのグループに分ける：

- a) TOE のセキュリティ対策方針： 評価において正確性が決定される対策を記述する；
- b) 運用環境のセキュリティ対策方針： 評価において正確性が決定されない対策を記述する。

一般モデル

- 222 このように分ける理由は、以下のとおりである:
- CC は、IT 対抗策の正確性の評価にのみ適している。したがって、非 IT の対抗策 (警備員、手続きなど) は、常に運用環境に属する。
- 対抗策の正確性の評価には時間と資金がかかるため、すべての IT 対抗策の正確性を評価することは不可能なことがある。
- 一部の IT 対抗策の正確性は、別の評価ですでに評価されていることがある。したがって、この正確性を再び評価することは、費用効率が良くない。
- 223 TOE(評価において正確性が評価される IT 対抗策)にとって、セキュリティターゲットは、セキュリティ機能要件(SFR)に関して TOE のセキュリティ対策方針のより詳細な記述を要求する。SFR は、厳格さを保証し、比較可能性を容易にするために、(CC パート 2 で記述する)標準化された言語で体系的に作り上げられている。
- 224 要するに、セキュリティターゲットでは以下のことを実証する:
- SFR が TOE のセキュリティ対策方針を満たしていること;
- TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針が、脅威に対抗すること;
- したがって、SFR 及び運用環境のセキュリティ対策方針が脅威に対抗すること。
- 225 つまり、(SFR を満たす)正しい TOE と(運用環境のセキュリティ対策方針を満たす)正しい運用環境によって、脅威に対抗する。次の 2 つの節では、TOE の正確性と運用環境の正確性について個別に記述する。
- 7.1.2 TOEの正確性**
- 226 TOE は正確に設計及び実装されず、脆弱性の原因となる誤りが含まれることがある。このような脆弱性に付け込まれ、攻撃者によって資産に損害が与えられる、及び/または悪用されることがある。
- 227 このような脆弱性は、開発中の不慮の誤り、不十分な設計、悪意あるコードの意図的な追加、不十分なテストなどから生じることがある。
- 228 TOE の正確性を決定するために、以下のような様々なアクティビティを実施できる:
- TOE のテスト;
- TOE の様々な設計形態の検査;
- TOE の開発環境の物理的セキュリティの検査。
- 229 セキュリティターゲットでは、セキュリティ保証要件(SAR)の形式で、正確性を決定するために、これらのアクティビティについて構造的に記述する。SAR は、厳格さを保証し、比較可能性を容易にするために、(CC パート 3 で記述する)標準化された言語で体系的に作り上げられている。

230 SAR が満たされている場合は、TOE の正確性が保証されるため、攻撃者に悪用される脆弱性が TOE に含まれる可能性が低くなる。TOE の正確性に関する保証の量は、SAR 自体によって決定される：つまり、少数の「弱い」SAR ではわずかな保証が生じ、多数の「強力な」SAR では多くの保証が生じる。

7.1.3 運用環境の正確性

231 運用環境も正確に設計及び実装されず、脆弱性の原因となる誤りが含まれることがある。このような脆弱性に付け込まれ、攻撃者によって資産に損害が与えられたり、悪用されたりすることがある。

232 ただし、CC では、運用環境の正確性に関して保証は得られない。言い換えれば、運用環境は評価されない(次の節を参照のこと)。

233 評価に関する限り、運用環境は、そのセキュリティ対策方針の 100% 正確な具体化であるとみなされる。

234 これによって、TOE の消費者が、以下のような他の方法を使用して、運用環境の正確性を決定することが妨げられることはない：

OS の TOE で、運用環境のセキュリティ対策方針に「運用環境では、(インターネットなどの)信頼できないネットワークからのエンティティは ftp によってのみ TOE にアクセスできるようにしなければならない」と記述されている場合、消費者は評価済みのファイアウォールを選択し、TOE への ftp アクセスのみを許可するようにそのファイアウォールを設定することができる；

運用環境のセキュリティ対策方針に「運用環境では、すべての管理者が悪意を持って行動しないようにしなければならない」と記述されている場合、消費者は、悪意ある行動に対する懲罰を含むように、管理者との契約を見直すことができる。ただし、この決定は CC 評価には含まれない。

7.2 評価

235 CC は、以下に記述する ST/TOE 評価と、CC パート 3 で定義する PP 評価の 2 種類の評価を認識する。多くの場合に、CC は、ST/TOE 評価に言及するために、(修飾子なしで)評価という用語を使用する。

236 CC では、ST/TOE 評価は次の 2 つのステップからなる：

- a) ST 評価： TOE 及び運用環境の十分性を決定する；
- b) TOE 評価： TOE の正確性を決定する。上述したように、TOE 評価では、運用環境の正確性は評価しない。

237 ST の評価は、(CC パート 3 で定義される)セキュリティターゲット評価基準をセキュリティターゲットに適用することによって実施する。ASE 基準を適用する正確な方法は、使用する評価方法によって決定される。

238 TOE の評価は、より複雑である。TOE の評価への主な入力、TOE 及び ST が含まれるが、通常、設計文書または開発者テスト結果など、開発環境からの入力も含まれる評価証拠である。

一般モデル

- 239 TOE の評価では、(セキュリティターゲットから)SAR を評価証拠に適用する。特定の SAR を適用する正確な方法は、使用する評価方法によって決定される。
- 240 SAR の適用結果の証拠資料を提出する方法と、作成する必要がある報告書及びその詳細の度合いは、使用する評価方法と、その元で評価が実施される評価制度によって決定される。
- 241 TOE 評価プロセスの結果は、次のいずれかとなる：
- 満たされていない SAR があるため、TOE が ST に規定される SFR を満たすという指定されたレベルの保証が存在するわけではないとするステートメント；
- すべての SAR が満たされているため、TOE が ST に規定される SFR を満たすという指定されたレベルの保証が存在するとするステートメント。
- 242 TOE 評価は、TOE 開発が完了した後に、または TOE 開発と並行して実施してもよい。
- 243 ST/TOE 評価結果を記述する方法については、10 章で説明する。この評価結果では、TOE が適合を主張する PP 及びパッケージも識別する。これらの構成物については、次の章で説明する。

8 セキュリティ要件の調整

8.1 操作

244 CC 機能及び保証コンポーネントは、CC パート 2 及び CC パート 3 に定義されている通りに用いこともでき、あるいは許可された操作の使用を通して調整することもできる。操作を使用する場合、PP/ST 作成者は、この要件に依存する他の要件の依存性の必要性が満たされていることにも注意するべきである。許可された操作は、以下のセットから選択される:

繰返し: 種々の操作で 2 回以上コンポーネントを使用することができる;

割付: パラメタを特定することができる;

選択: リストから、1 つまたは複数の項目を特定することができる;

詳細化: 詳細を追加することができる。

245 割付及び選択操作は、コンポーネントにおいて特定の指示された場所だけで許可される。繰返し及び詳細化は、すべてのコンポーネントに対して許可される。各操作について以下にさらに詳細に記述する。

246 CC パート 2 附属書は選択と割付の有効な完了のガイダンスを提供する。このガイダンスはどのように操作を完了するかの規定の指示を提供し、PP/ST 作成者は逸脱を正当とする理由を述べない限り、これらの指示に従わなければならない。

- a) 「なし(none)」は、明示的に提供されている場合にのみ、選択の完了のための選択として有効である。

選択の完了のために提供されるリストは、空であってはならない。

もし、「なし(None)」という選択肢を選ぶなら、他の追加の選択肢を選択してはならない。もし、選択において選択肢に「なし(None)」が与えられていない場合、その選択が「から 1 つのみ選択」と明示的に述べていない限り、選択肢を「及び(and)」や「または(or)」で結合することが認められる。

選択の操作は、必要であれば繰返しによって纏めてもよい。この場合、各々の繰返しに対する選択の適用可能性は、他の繰返しの選択の対象と重ならないようにすべきである。それらは排他的であると意図されているためである。

- b) 割付の完了に対し、CC パート 2 附属書は、「なし(none)」が有効な選択であることを決定するために参照されなければならない。

8.1.1 繰返し操作

247 繰返し操作は、すべてのコンポーネントで実行することができる。PP/ST 作成者は、同じコンポーネントに基づく複数の要件を加えることによって、繰返し操作を行う。コンポーネントのそれぞれの繰返しは、そのコンポーネントの他のすべての繰返しとは異ならなければならない。これは、異なる方法で割付及び選択を完了するか、異なる方法で詳細化を適用することによって実現される。

248 異なる繰返しは、明確な根拠と、これらの要件との間の追跡のために、一意に識別するべきである。

セキュリティ要件の調整

249 時々、繰返し操作は、それらの繰返しの代わりに、値の範囲またはリストで割付操作を実行することもできるコンポーネントで用いることが可能であることに注意することが大切である。この場合、作成者は、範囲の値に全体根拠を提供する必要があるか、または、各々の値に対して個別の根拠を持つ必要があるかを考慮し、もっとも適切な選択肢を選ぶことができる。作成者はまた、値に対し個々の追跡が要求されないか、留意すべきである。

8.1.2 割付操作

250 割付操作は、特定のコンポーネントに PP/ST 作成者によって設定されるパラメタ付きのエレメントが含まれる場合に行なう。パラメタは、制限のない変数、または変数を特定の範囲の値に狭める規則にすることができる。

251 PPのエレメントに割付が含まれる場合には常に、PP 作成者は次の4つのいずれかを行わなければならない:

- a) 割付を未完了のままにする。PP 作成者は、FIA_AFL.1.2「不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、**[割付: アクションのリスト]**を実行しなければならない」を PP に加えることができる。
- b) 割付を完了する。例えば、PP 作成者は、FIA_AFL.1.2「不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、**今後サブジェクトに結合することを外部エンティティに禁じなければならない**」を PP に加えることができる。
- c) 許可する値の範囲をさらに制限するために割付の範囲を狭める。例えば、PP 作成者は、FIA_AFL.1.1「TSF は、**...[割付: 4~9 の間の正の整数]回の不成功の認証試行が生じたときを検出しなければならない**」を PP に加えることができる。
- d) 割付を選択に変えることにより、割付の範囲を狭める。例えば、PP 作成者は、FIA_AFL.1.2「不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、**[選択: 今後サブジェクトに結合することを利用者に禁止、管理者に通知]**しなければならない」を PP に加えることができる。

252 STのエレメントに割付が含まれる場合には常に、ST 作成者は上記の b)に示すように割付を完了しなければならない。オプション a)、c)、及び d)は、ST では許可されない。

253 オプション b)、c)、及び d)で選択する値は、割付で要求される指定された型に適合しなければならない。

254 割付が(サブジェクトなどの)セットで完了される場合は、次のように、サブジェクトのセットだけでなく、セットのエレメントを導出できるセットの記述をリストすることができる:

すべてのサブジェクト

種別 X のすべてのサブジェクト

サブジェクト a を除くすべてのサブジェクト

ただし、どのサブジェクトを指しているかが明確であることを条件とする。

8.1.3 選択操作

255 選択操作は、特定のコンポーネントに PP/ST 作成者が複数の項目から選択しなければならないエレメントが含まれる場合に行う。

256 PP のエレメントに選択が含まれる場合には常に、PP 作成者は次の 3 つのいずれかを行うことができる:

- a) 選択を未完了のままにする。
- b) 1 つまたは複数の項目を選んで、選択を完了する。
- c) いくつかの選択肢を削除し、2 つ以上を残すことにより、選択を制限する。

257 ST のエレメントに選択が含まれる場合には常に、ST 作成者は上記の b) に示すように選択を完了しなければならない。オプション a) 及び c) は、ST では許可されない。

258 b) 及び c) で選択する 1 つ以上の項目は、選択で提供される項目から取得しなければならない。

8.1.4 詳細化操作

259 詳細化操作は、すべての要件で実行することができる。PP/ST 作成者は、要件を変更することによって詳細化を実行する。詳細化の最初の規則は、その PP/ST の文脈において、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ということである(つまり、詳細化された要件は、元の要件に比べ「より厳格」でなければならない)。詳細化がこの規則を満たさない場合、その詳細化によって生じる要件は拡張要件とみなされ、拡張要件として扱わなければならない。

260 詳細化の最初の規則は、その PP/ST の文脈において、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ということである(つまり、詳細化された要件は、元の要件に比べ「より厳格」でなければならない)。

261 この規則に対する唯一の例外として、PP/ST 作成者は、全部ではなく一部のサブジェクト、オブジェクト、操作、セキュリティ属性、及び/または外部エンティティに適用するために SFR を詳細化することができる。

262 ただし、この例外は、適合を主張する PP から取得された SFR の詳細化には適用されない。このような SFR は、PP 内の SFR よりも少ないサブジェクト、オブジェクト、操作、セキュリティ属性、及び/または外部エンティティに適用するように詳細化することはできない。

263 詳細化の 2 番目の規則は、詳細化は元のコンポーネントに関連付けなければならないことである。

264 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、または読者にとってより理解しやすくす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。

8.2 コンポーネント間の依存性

265 コンポーネント間には、依存性が存在する場合がある。依存性は、あるコンポーネントが自立的ではなく、セキュリティ機能または保証を提供するために、別のコンポーネントの存在に依存する場合に生じる。

266 CC パート3 のいくつかの保証コンポーネントが、CC パート3 の保証コンポーネントに依存性を持つことがあるのと同様に、CC パート2 の機能コンポーネントは、一般に他の機能コンポーネントに依存性を持つ。CC パート2 の、CC パート3 コンポーネントへの依存性も定義してもよい。ただし、拡張機能コンポーネントが保証コンポーネントに依存したり、またはその反対の依存性が生じることがある。

267 コンポーネントの依存性の記述は、CC パート2 及び CC パート3 のコンポーネントの定義を参照することによって決定される。TOE セキュリティ要件の完全性を保証するには、依存性のあるコンポーネントに基づく要件を PP 及び ST に組み込むときに依存性が満たされるべきである。依存性はパッケージを構成するときにも考慮に入れるべきである。

268 言い換えれば、コンポーネント A がコンポーネント B に依存する場合、PP/ST にコンポーネント A に基づくセキュリティ要件が含まれるときには常に、PP/ST は次のいずれかを含まなければならない:

- a) コンポーネント B に基づくセキュリティ要件;
- b) コンポーネント B に対して上位階層関係にあるコンポーネントに基づくセキュリティ要件;
- c) PP/ST にコンポーネント B に基づくセキュリティ要件が含まれない理由を示す正当化。

269 a)及び b)のケースで、依存性のためにセキュリティ要件が含まれる場合、実際に依存性を満たすような特定の方法で、セキュリティ要件に対する操作(割付、繰返し、詳細化、選択)を完了することが必要になる場合がある。

270 c)のケースで、セキュリティ要件を含まないことの正当化では、次のいずれかを示すべきである:

依存性が必要または有用ではない理由、または

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

依存性が、その他の SFR によって、その他の方法で対処されること(拡張 SFR、SFR の組み合わせなど)。

8.3 拡張コンポーネント

271 CC では、次の2つの例外を除いて、要件は、CC パート2 または CC パート3 のコンポーネントに基づかなければならない:

- a) パート2のSFRに書き換えることができないTOEのセキュリティ対策方針が存在する、または(暗号の評価に関してなど)パート3のSARに書き換えることができない第三者の要件(法律、規格など)が存在する;
- b) CCパート2及び/またはCCパート3のコンポーネントに基づいてセキュリティ対策方針を書き換えることができるが、著しい困難及び/または複雑さを伴う。

272 いずれの場合にも、PP/ST作成者は、独自のコンポーネントを定義する必要がある。これらの新しく定義されるコンポーネントは、拡張コンポーネントと呼ばれる。拡張コンポーネントに基づく拡張SFR及びSARに文脈及び意味を提供するには、正確に定義された拡張コンポーネントが必要である。

273 新しいコンポーネントを正確に定義した後に、PP/ST作成者はこれらの新しく定義した拡張コンポーネントに基づいて1つまたは複数のSFRまたはSARを作成し、他のSFR及びSARと同じ方法で使用することができる。この時点以降、CCに基づくSAR及びSFRと、拡張コンポーネントに基づくSAR及びSFRは区別されない。拡張コンポーネントの要件の詳細は、CCパート3の拡張コンポーネント定義(APE_ECD)及び拡張コンポーネント定義(ASE_ECD)を参照。

9 プロテクションプロファイル及びパッケージ

9.1 序説

274 関心を持つ消費者のグループ及びコミュニティがそれぞれのセキュリティニーズを表現できるようにし、ST の記述を容易にするために、CC の本パートはパッケージ及びプロテクションプロファイル(PP)の2つの特有な構成物を規定している。次の2つの節ではこれらの構成物についてより詳細に説明し、その後の節で各構成物を使用する方法を示す。

9.2 パッケージ

275 パッケージとは、セキュリティ要件の名前付きセットである。パッケージは、次のいずれかである。

SFR のみを含む機能パッケージ、または

SAR のみを含む保証パッケージ。

276 SFR と SAR の両方を含む混合パッケージは許可されない。

277 パッケージは、任意の当事者が定義することができ、再利用されることが意図されている。この目標のために、パッケージには組み合わせにより有用かつ有効になる要件を含むべきである。パッケージは、より大きなパッケージ、PP、及びSTの構成物内で使用できる。現在、パッケージの評価に対する基準はないため、SFR または SAR の任意のセットをパッケージにすることができる。

278 保証パッケージの例には、CC パート 3 で定義される評価保証レベル(EAL)がある。現時点で、このバージョンの CC に対する機能パッケージは存在しない。

9.3 プロテクションプロファイル

279 ST が常に特定の TOE(MinuteGap v18.5 Firewall など)について記述するのに対して、PP は TOE 種別(ファイアウォールなど)について記述することを意図している。したがって、異なる評価で使用される様々なSTのテンプレートとして、同じPPを使用してもよい。PPの詳細については、附属書 B を参照のこと。

280 一般に、ST は TOE の要件を記述し、TOE の開発者によって作成される。これに対して、PP は TOE 種別の一般要件を記述するため、一般に以下の者によって記述される：

所定の TOE 種別の要件について合意の形成を求めている利用者コミュニティ；

TOE の開発者、または TOE の種別に対する最低ベースラインの確立を求めている類似の TOE の開発者グループ；

購入プロセスの一部として要件を特定する政府または大企業。

281 PP は、PP に対して許可される ST の適合の種別を決定する。つまり、PP は、次のように(PP 適合ステートメントで)ST に対して許可される適合の種別を記載する(B.5 節を参照のこと)：

PP に正確適合が要求されると記載されている場合、ST は PP に対して正確に適合しなければならない；

PP に論証適合が要求されると記載されている場合、ST は PP に対して正確または論証可能な方法で適合しなければならない。

282 言い換えれば、PP が明示的に許可している場合にのみ、ST は論証可能な方法で PP に適合することが許可される。

283 ST は、複数の PP への適合を主張する場合、(上述したように)各 PP で定められる方法で各 PP に適合しなければならない。つまり、ST は一部の PP に対して正確適合し、その他の PP に対して論証適合する場合がある。

284 ST は関連する PP に適合しているか、適合していないかのいずれかであることに注意のこと。CC では、「部分的な」適合は認められない。したがって、PP/ST 作成者が PP に対する適合を主張できなくなるほど負担の大きい PP にならないようにすることは、PP 作成者の責任である。

285 ST は、以下の場合に PP に対して同等またはより制限的である：

ST を満たすすべての TOE が PP も満たし、かつ

PP を満たすすべての運用環境が ST も満たす。

簡単に言えば、ST は、TOE に同等以上の制限を課し、TOE の運用環境に同等以下の制限を課さなければならない。

286 この一般的なステートメントは、以下のような ST の様々な節でより具体的にすることができる：

a) **セキュリティ課題定義**: ST の適合根拠では、ST のセキュリティ課題定義が PP のセキュリティ課題定義と同等(またはより制限的)であることを実証しなければならない。これは以下のことを意味する：

ST のセキュリティ課題定義を満たすすべての TOE は、PP のセキュリティ課題定義も満たす；

PP のセキュリティ課題定義を満たすすべての運用環境は、ST のセキュリティ課題定義も満たす。

b) **セキュリティ対策方針**: ST の適合根拠では、ST のセキュリティ対策方針が PP のセキュリティ対策方針と同等(またはより制限的)であることを実証しなければならない。これは以下のことを意味する：

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

PP の運用環境のセキュリティ対策方針を満たすすべての運用環境は、ST の運用環境のセキュリティ対策方針も満たす。

287 プロテクションプロファイルの正確適合が指定されている場合、以下の要件が適用される：

a) **セキュリティ課題定義**: ST は、PP のセキュリティ課題定義を含まなければならない、追加の脅威及び OSP を特定できるが、追加の前提条件を特定することはできない。

b) **セキュリティ対策方針**：

STは、PPのTOEに対するすべてのセキュリティ対策方針を含まなければならないが、TOEに対する追加のセキュリティ対策方針を特定することができる；

STは、(次の項目を除き)運用環境に対するすべてのセキュリティ対策方針を含まなければならないが、運用環境に対する追加のセキュリティ対策方針を特定することはできない；

STは、PPでの運用環境に対する特定のセキュリティ対策方針が、STではTOEのセキュリティ対策方針であることを特定できる。これは、セキュリティ対策方針の再割付と呼ばれる。セキュリティ対策方針がTOEに再割付される場合、セキュリティ対策方針根拠では、どの前提条件が、または前提条件の一部がもはや必要でなくなったかを、明確にしなければならない。

- c) **セキュリティ要件:** STは、PPのすべてのSFR及びSARを含まなければならないが、追加のまたは上位階層のSFR及びSARを主張することができる。ST内の操作の完了は、PP内の操作の完了と一致していなければならない。つまり、STでPPと同じ完了を使用するか、要件をより制限的にした完了を使用する(詳細化の規則を適用する)。

288 プロテクションプロファイルの論証適合が指定されている場合、以下の要件が適用される：

STには、PPに対して「同等またはより制限的」とみなされる根拠を含まなければならない。

論証適合では、PP作成者は解決すべき共通のセキュリティ課題を記述し、その解決のために必要な要件に対する一般的ガイドラインを、解決策を特定するには複数の方法があり得ることを認識して提供することができる。

289 PP評価を行うか否かは、任意である。CCパート3のリストに従ってAPE基準を適用することにより、評価が実施される。この評価の目標は、PPが完全で、一貫性があり、技術的に信頼でき、別のPPまたはSTを構築するためのテンプレートとして使用するのに適していることを実証することである。

290 評価済みのPPに基づいてPP/STを構築することには、以下の2つの利点がある：

PPに誤り、曖昧さ、または相違が存在するリスクが大きく低下する。新しいSTの記述または評価中に、(PPの評価によって捕捉されていたはずの)PPの問題が発見された場合、PPが訂正されるまでに多くの時間がかかることがある。

新しいPP/STの評価では、評価済みPPの評価結果をしばしば再利用して、新しいPP/STの評価作業をより少ない労力で終わらせることができる。

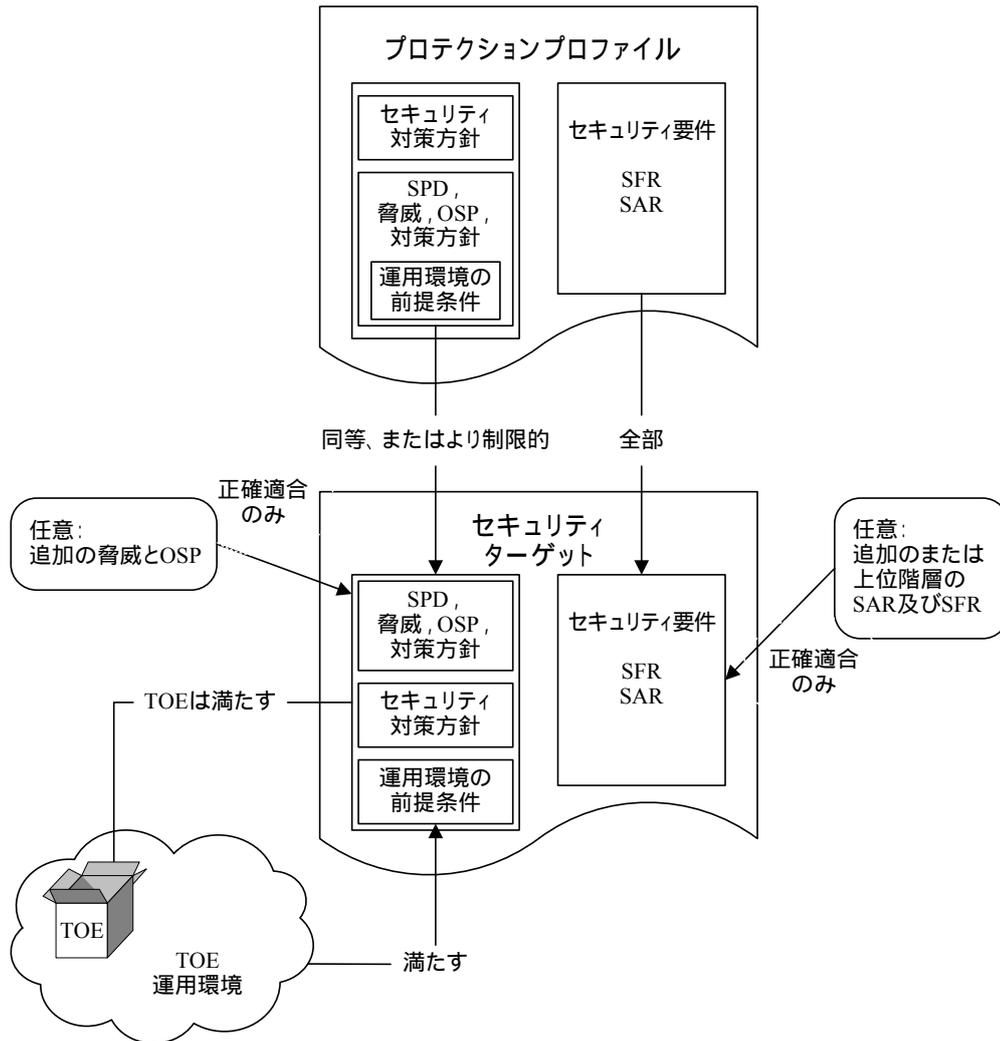


図4 PP, ST 及び TOE の内容間の関係

9.4 PP及びパッケージの使用

291 STが1つ以上のパッケージ及び/またはプロテクションプロファイルへの適合を主張する場合、その ST の評価により、(ST のその他の特性に加えて)その ST が適合を主張しているパッケージ及び/または PP に実際に適合していることが実証される。適合の判断の詳細については、附属書 A を参照のこと。

292 これによって、次のプロセスが可能になる:

- a) 特定の種別の IT セキュリティ製品の購入を求めている組織は、そのセキュリティニーズを PP に記述し、その評価を受け、公開する;
- b) 開発者は PP を入手し、この PP への適合を主張する ST を記述し、この ST の評価を受ける;
- c) 次に、開発者は TOE を構築し(または既存の TOE を使用し)、ST に照らしこの TOE の評価を受ける。

293 この結果、開発者は、その TOE が組織のセキュリティニーズに適合していることを証明できる。このため、組織はその TOE を購入することができる。パッケージにも同様の考え方を適用できる。

9.5 複数のプロテクションプロファイルの使用

294 CC では、PP を他の PP に適合させ、これによって各 PP が前の PP に基づいている一連の PP を構成することができる。

295 例えば、集積回路用の PP とスマートカード OS 用の PP を入手し、両方の PP への適合を主張するスマートカード PP(IC 及び OS)を構成するためにこれらを使用することができる。次に、スマートカードの PP とタブレットの読み込みに関する PP に基づいて、公共輸送用のスマートカードに関する PP を記述できる。最後に、開発者はこの公共輸送用スマートカードの PP に基づいて ST を構成できる。

10 評価結果

10.1 序説

296 この章では、CEMに従い実施されたPP及びST/TOEの評価から期待される結果を示す。

297 PPの評価は、評価済みのPPのカタログとなる。

298 STの評価は、TOEの評価の枠内で用いられる中間の結果となる。

299 ST/TOEの評価は、評価済みのTOEのカタログとなる。多くの場合、これらのカタログは特定のTOEではなく、そのTOEの基となるIT製品を参照する。したがって、カタログにIT製品が存在しても、IT製品全体が評価を受けていると解釈するべきではない。ST/TOEの評価の実際の範囲は、STによって定義される。このようなカタログの例として、参考文献を参照。

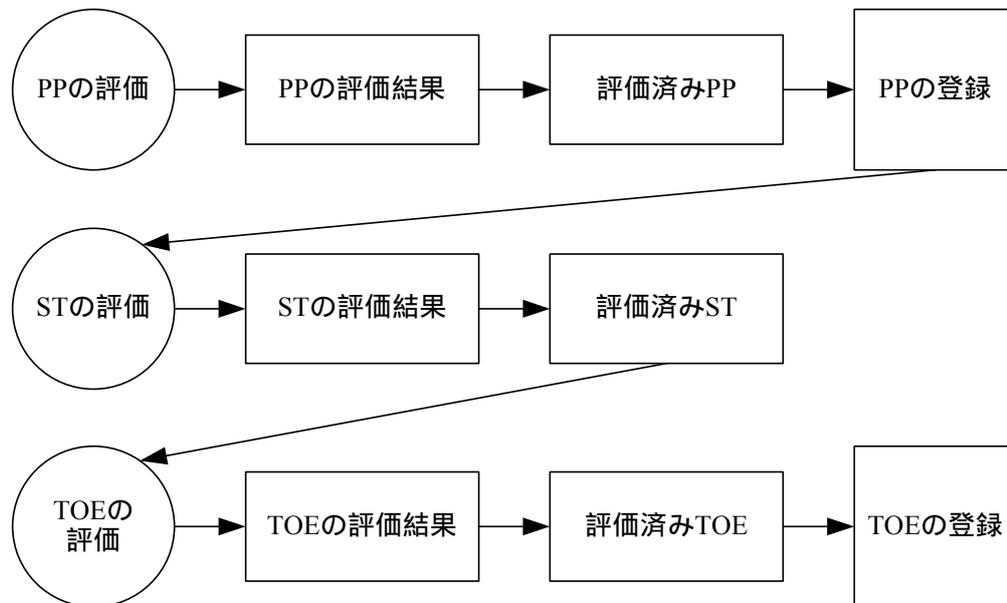


図5 評価結果

300 STは、パッケージ、評価済みのPP、または評価を受けていないPPに基づくことがある。ただし、STは何かに基づいて構築する必要はないため、これは必須ではない。

301 評価は、セキュリティ評価の結果を表現する絶対的な客観的尺度がない場合でも、証拠として引用することができる客観的で再現性のある結果をもたらすべきである。評価基準のセットが存在するということは、評価が意味のある結果をもたらす、評価監督機関間での評価結果に対する相互承認の技術的基礎を提供するのに必要な条件である。

302 評価結果は、TOEのセキュリティ特性についての特定の種類の調査の成果を意味する。そうした評価結果は、あらゆる適用環境における使用への適合を自動的に保証するものではない。特定の適用環境へのTOEの使用を承認するかどうかの判断は、評価結果を含め、多くのセキュリティ上の課題の検討に基づく。

10.2 PPの評価の結果

303 CC パート 3 は、PP が完全で、一貫性があり、技術的に信頼でき、その結果、ST の開発において使用するのに適していることを評価者が記述するために参照しなければならない評価基準を含んでいる。

304 評価の結果には、「適合主張」も含まれなければならない(10.4 節を参照のこと)。

10.3 ST/TOEの評価の結果

305 CC は、TOE が ST の SFR を満たしていることを示す十分な保証が存在するかどうかを評価者が決定するために参照しなければならない評価基準を含んでいる。したがって、TOE の評価の結果として、ST に対する合否ステートメントを記述しなければならない。ST 及び TOE の評価の結果、どちらも合格ステートメントが記述された場合、その基本となる製品には登録簿に登録される資格が与えられる。評価の結果には、次の節で定義する「適合主張」も含まれなければならない。

306 評価結果は後に認証プロセスで使用されることがあるが、この認証プロセスは CC の範囲外である。

10.4 適合主張

307 適合主張は、評価に合格した PP または ST によって満たされる要件の集合の源を識別する。この適合主張は、以下のような CC 適合主張を含む：

a) PP または ST が適合を主張する CC のバージョンを記述する。

b) 以下のいずれかとして、CC パート 2(セキュリティ機能要件)への適合を記述する：

CC パート 2 適合 PP または ST は、その PP または ST のすべての SFR が CC パート 2 の機能コンポーネントのみに基づく場合、CC パート 2 適合となる、または

CC パート 2 拡張 PP または ST は、その PP または ST の少なくとも 1 つの SFR が CC パート 2 の機能コンポーネントに基づいていない場合、CC パート 2 拡張となる。

c) 以下のいずれかとして、CC パート 3(セキュリティ保証要件)への適合を記述する：

CC パート 3 適合 PP または ST は、その PP または ST のすべての SAR が CC パート 3 の保証コンポーネントのみに基づく場合、CC パート 3 適合となる、または

CC パート 3 拡張 PP または ST は、その PP または ST の少なくとも 1 つの SAR が CC パート 3 の保証コンポーネントに基づいていない場合、CC パート 3 拡張となる。

308 さらに、適合主張には、パッケージに関して作成されたステートメントを含んでもよい。そのような場合には以下のうちの 1 つからなる：

パッケージ名適合 PP または ST は、以下のいずれかの場合、あらかじめ定義されたパッケージ(例えば、EAL)に適合している：

その PP または ST の SFR が、パッケージ内の SFR と同じ、または

その PP または ST の SAR が、パッケージ内の SAR と同じ。

パッケージ名追加 PPまたはSTは、以下の場合、あらかじめ定義されたパッケージの追加となる:

PPまたはSTのSFRにはパッケージ内のすべてのSFRが含まれるが、少なくとも1つの追加のSFR、またはパッケージ内のSFRよりも階層の高い1つのSFRがある。

PPまたはSTのSARにはパッケージ内のすべてのSARが含まれるが、少なくとも1つの追加のSAR、またはパッケージ内のSARよりも階層の高い1つのSARがある。

309 TOEが所定のSTで正常に評価された場合、STの適合主張は、そのTOEにも当てはまる。したがって、TOEは、例えばCCパート2適合にすることができることに注意のこと。

310 最後に、適合主張には、プロテクションプロファイルに関する次の2つのステートメントを含んでもよい:

- a) **PP適合** PPまたはTOEは、適合結果の一部として記載されている特定のPPを満たしている。
- b) **適合ステートメント(PPのみ)** このステートメントは、PPまたはSTがこのPPに適合しなければならない方法、つまり正確または論証を記述する。この適合ステートメントの詳細については、附属書Bを参照のこと。

10.5 ST/TOEの評価結果の使用

311 ST及びTOEが評価されると、TOEが運用環境とともに脅威に対抗することについて、(STに定義される)保証が資産の所有者に与えられる。評価結果は、資産の所有者が資産を脅威にさらすリスクを受け入れるかどうかを判断する際に用いることができる。

312 ただし、資産の所有者は次のことを慎重に確認するべきである:

- a) STのセキュリティ課題定義が資産の所有者のセキュリティ課題と一致していること;
- b) 資産の所有者の運用環境が、STに記述された運用環境のセキュリティ対策方針に適合している(または適合させることができる)こと。

313 上記のいずれかに当てはまらない場合、そのTOEは資産の所有者の目的に適していない場合がある。

314 また、評価済みTOEの運用が開始されることになれば、これまで分からなかったTOE内の誤りや脆弱性が表面化する場合がある。この場合、開発者は(脆弱性を修正するために)TOEを訂正または評価の範囲から脆弱性を排除するためにSTを変更することができる。いずれの場合も、古い評価結果はもはや有効ではない。

315 信頼の回復が必要であると思われる場合は、再評価が必要である。CCは再評価のために使用できるが、再評価を行うための手続きの詳細な説明は、CCの本パートの範囲外である。

附属書A セキュリティターゲットの仕様(参考)

A.1 本附属書の目的及び構造

316 この附属書の目的は、セキュリティターゲット(ST)の概念を説明することである。本附属書では、ASE 基準の定義は行わない。この定義は、CC パート 3 にあり、参考文献にある文書によりサポートされている。

317 本附属書は、次の 4 つの主要なパートから構成されている:

- a) *ST の必須の内容*。これについては、A.2 節で概要を示し、A.4 節から A.10 節でより詳細に説明する。これらの節では、ST の必須の内容と各内容間の相互関係について説明し、例を示す。
- b) *ST の使用法*。これについては、A.3 節で概要を示し、A.11 節でより詳細に説明する。これらの節では、ST の使用法と、ST を使用して回答できるいくつかの質問について説明する。
- c) *低保証 ST*。低保証 ST は、内容が削減された ST である。これについては、A.12 節で詳細に説明する。
- d) *標準への準拠の主張*。A.13 節では、ST 作成者が、TOE が特定の標準を満たしていることを主張する方法を説明する。

A.2 ST の必須の内容

318 図 6 は、CC パート 3 で参照される ST の必須の内容を示す。図 6 は ST の構造的アウトラインとしても使用することができるが、別の構造も使用可能である。例えば、セキュリティ要件根拠が非常に長くなる場合は、セキュリティ要件の節の代わりに、ST の附属書にそれを記述することができる。ST の個別の節と、各節の内容について、以下に簡単に概要を示し、A.4 節から A.10 節でより詳細に説明する。通常、ST には次のことを記述する:

- a) 抽象レベルの異なる TOE の 3 つの叙述的記述を含む *ST 概説*、
- b) ST が PP 及び/またはパッケージへの適合を主張するかどうかと、主張する場合にはその PP 及び/またはパッケージを示す *適合主張*、
- c) 脅威、OSP、及び前提条件を示す *セキュリティ課題定義*、
- d) TOE のセキュリティ対策方針と TOE の運用環境のセキュリティ対策方針で、セキュリティ課題の解決策を分担する方法を示す *セキュリティ対策方針*、
- e) 新しい(つまり CC パート 2 または CC パート 3 に含まれていない)コンポーネントを定義することができる *拡張コンポーネント定義(任意)*。これらの新しいコンポーネントは、拡張機能要件及び拡張保証要件を定義するために必要である;
- f) TOE のセキュリティ対策方針から標準言語への書き換えを提供する *セキュリティ要件*。この標準言語は、SFR の形式をとる。また、この節では SAR について定義する;
- g) TOE で SFR を実装する方法を示す *TOE 要約仕様*。

319

内容が削減された低保証STもある。これについては、A.12節で詳細に説明する。本附属書のすべての他の部分では、すべての内容を含むSTを前提としている。

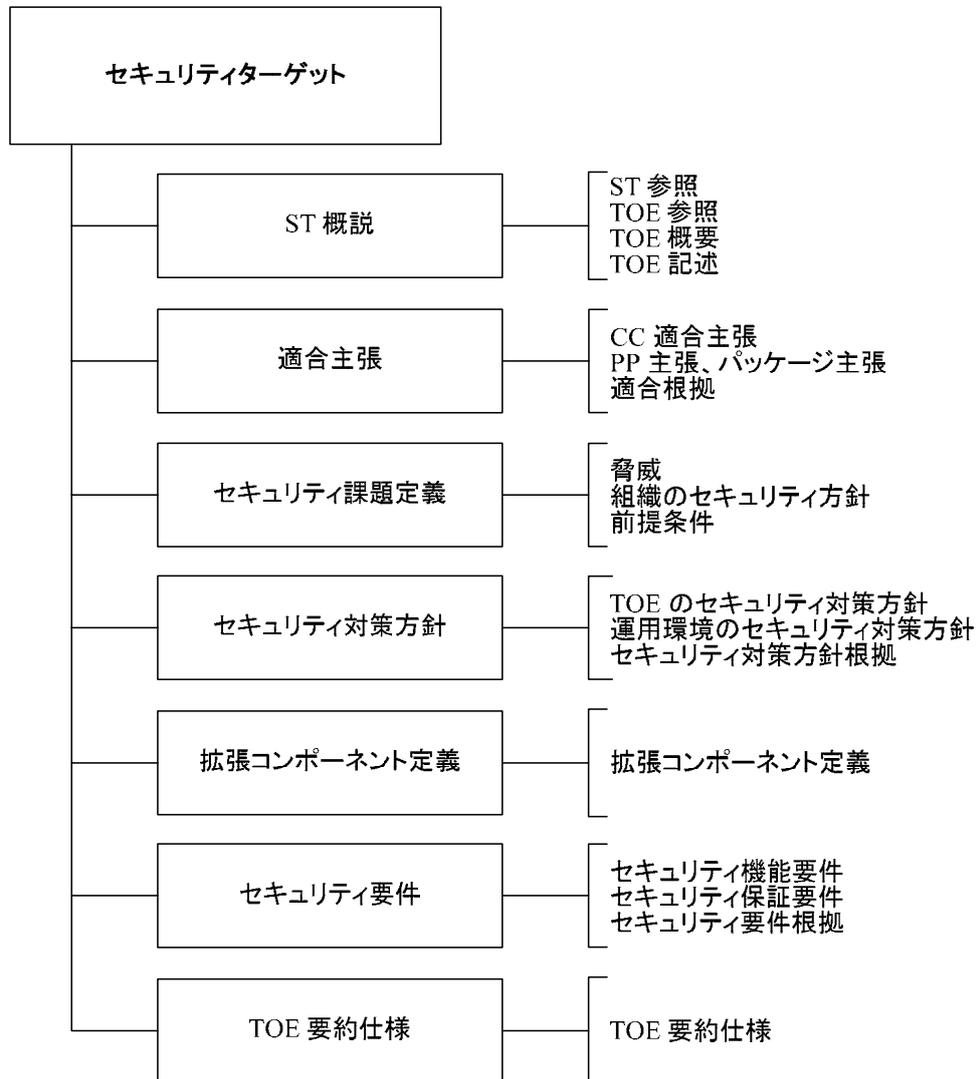


図6 セキュリティターゲットの内容

A.3 ST の使用

A.3.1 ST の使用法

320

一般的な ST は、次の 2 つの役割を果たす:

評価前及び評価中に、ST は「評価する対象」を特定する。この役割において、ST は、TOE の正確なセキュリティ特性及び正確な評価範囲に関する、開発者と評価者間での合意の基礎となる。この役割では、技術的な正確さ及び完全さが重要な課題となる。A.7 節では、この役割で ST を使用する方法を説明する。

セキュリティターゲットの仕様(参考)

評価後に、STは「評価された対象」を特定する。この役割において、STは、TOEの開発者または再販業者とTOEの潜在的な消費者間での合意の基礎となる。STは抽象的な方法でTOEの正確なセキュリティ特性を記述する。そして、TOEはそのSTを満たすことが評価されているため、潜在的な消費者はこの記述を信頼できる。この役割では、使用及び理解の容易さが重要な課題となる。A.11節では、この役割でSTを使用する方法を説明する。

A.3.2 STの不適切な使用法

321 STが果たすべきではない2つの役割は次のとおりである(これらに限定されない):

詳細な仕様: STは、比較的高い抽象レベルのセキュリティ仕様を目的としている。一般に、STには詳細なプロトコル仕様、詳細なアルゴリズム及び/またはメカニズムの記述、詳細な運用についての長い説明などを記述するべきではない。

完全な仕様: STは、全体仕様ではなく、セキュリティ仕様を目的としている。セキュリティに関係しない限り、相互運用性、物理的なサイズ及び重量、要求される電圧などの特性は、STに記述するべきではない。つまり、一般にSTは完全な仕様自体ではなく、完全な仕様の一部である。

A.4 ST概説(ASE_INT)

322 ST概説では、次の3つの抽象レベルで叙述的な方法によりTOEについて記述する:

- a) ST及びSTが参照するTOEの識別資料を提供するST参照及びTOE参照;
- b) TOEについて簡潔に記述するTOE概要;
- c) TOEについてより詳細に記述するTOE記述。

A.4.1 ST参照及びTOE参照

323 STには、特定のSTを識別する明確なST参照が含まれる。一般的なST参照は、タイトル、バージョン、作成者、及び公表日から構成される。ST参照は、例えば「MauveRAM Database ST、バージョン 1.3、MauveCorp仕様チーム、2002年10月11日」のように記述する。

324 STには、そのSTへの適合を主張するTOEを識別するTOE参照も含まれる。一般的なTOE参照は、開発者名、TOE名、及びTOEバージョン番号から構成される。TOE参照は、例えば「MauveCorp MauveRAM Database v2.11」のように記述する。単一のTOEが何度も評価を受け(例えばそのTOEの様々な消費者によって)、その結果複数のSTが存在することがある場合は、この参照は必ずしも一意ではない。

325 TOEが1つ以上の既知の製品から構成される場合、製品名を参照することにより、TOE参照にこのことを反映させることができる。ただし、これを使用することによって消費者に誤解を与えないようにするべきである。製品の主要な部分または主要なセキュリティ機能性が評価において考慮されていないにもかかわらず、TOE参照にこの点が反映されていない状況は、許されない。

326 ST参照及びTOE参照によって、ST及びTOEのインデックス化及び参照と、評価済みTOE/製品リストの要約への組み込みが容易になる。

A.4.2 TOE 概要

327 TOE 概要は、セキュリティニーズを満たし、使用するハードウェア、ソフトウェア、及びファームウェアでサポートされている TOE を見つけるために、評価済み TOE/製品のリストに目を通している TOE の潜在的な消費者を対象としている。TOE 概要の一般的な長さは、数段落である。

328 そのため、TOE 概要では、TOE の使用法及びその主要なセキュリティ機能の特徴について簡潔に説明し、TOE 種別を識別し、TOE に必要な主要な TOE 以外のハードウェア/ソフトウェア/ファームウェアを識別する。

A.4.2.1 TOE の使用法及び主要なセキュリティ機能の特徴

329 TOE の使用法及び主要なセキュリティ機能の特徴に関する記述は、セキュリティ面から見た TOE の機能とセキュリティに関する TOE の用途について、ごく一般的な情報を示すことを目的としている。この節は、(潜在的な)TOE 消費者のために、事業運営面から見た TOE の使用法と主要なセキュリティ機能の特徴について、TOE 消費者が理解する言葉を使用して記述すべきである。

330 この例を次に示す。「MauveCorp MauveRAM Database v2.11 は、ネットワーク環境での使用を想定したマルチユーザ向けデータベースである。このデータベースでは、1,024 人の利用者が同時にアクティブになることができる。パスワード/トークン及び生体認証を使用でき、偶発的なデータ破損を防止し、10,000 トランザクションをロールバックすることができる。この監査機能の特徴は柔軟に設定可能であり、一部の利用者及びトランザクションに対して詳細な監査を実施する一方で、その他の利用者及びトランザクションのプライバシーを保護することができる。」

A.4.2.2 TOE 種別

331 TOE 概要では、ファイアウォール、VPNファイアウォール、スマートカード、暗号化モデム、イントラネット、ウェブサーバ、データベース、ウェブサーバ及びデータベース、LAN、ウェブサーバ及びデータベースを伴う LAN など、TOE の一般的な種別を識別する。

332 TOE がすぐに利用できる種別に属さない場合には、「なし(none)」を使用することができる。

333 TOE 種別は消費者に誤解を与えることがある。例を次に示す：

TOE が特定の機能性を備えないにもかかわらず、その TOE 種別のために TOE がそれを備えるものと期待されることがある。例を次に示す：

識別/認証機能性をサポートしていない ATM カード種別の TOE;

非常に一般的に使用されているプロトコルをサポートしていないファイアウォール種別の TOE;

証明書取消し機能性のない PKI 種別の TOE。

TOE が特定の運用環境で動作できないにもかかわらず、その TOE 種別のために TOE がその環境で動作するものと期待されることがある。例を次に示す：

セキュリティターゲットの仕様(参考)

PC がネットワークに接続されず、フロッピードライブと CD/DVD プレーヤーを持っていない場合のみ、安全に機能させることができる PC オペレーティングシステム種別の TOE;

ファイアウォールを通じて接続できるすべての利用者に悪意がない場合のみ、安全に機能させることができるファイアウォール。

A.4.2.3 必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア

334 他の IT に依存しない TOE もあるが、多くの TOE(特にソフトウェア TOE)は、TOE 以外の追加のハードウェア、ソフトウェア及び/またはファームウェアに依存する。後者の場合に、TOE 概要では、この TOE 以外のハードウェア、ソフトウェア、及び/またはファームウェアを識別する必要がある。

追加のハードウェア/ソフトウェア/ファームウェアについての完全かつ詳細な識別をする必要はないが、潜在的な消費者が、TOE を使用するために必要な主なハードウェア、ソフトウェア、及び/またはファームウェアコンポーネントを判断するために十分な完全かつ詳細な識別を行うべきである。

335 ハードウェア/ソフトウェア/ファームウェア識別の例を次に示す:

Yaiza オペレーティングシステムのバージョン 3.0 アップデート 6b、c、7 またはバージョン 4.0 を実行し、1GHz 以上のプロセッサ及び 512MB 以上の RAM を搭載した標準 PC;

Yaiza オペレーティングシステムのバージョン 3.0 アップデート 6d を実行し、1.0 WM ドライバセットを備えた WonderMagic 1.0 グラフィックスカード、1GHz 以上のプロセッサ及び 512MB 以上の RAM を搭載した標準 PC;

Yaiza OS のバージョン 3.0(以上)を実行している標準 PC;

CleverCard SB2067 集積回路;

QuickOS スマートカードオペレーティングシステムのバージョン 2.0 を実行している CleverCard SB2067 集積回路;

運輸省長官の事務局で 2002 年 12 月に設置された LAN。

A.4.3 TOE 記述

336 TOE 記述は、TOE の叙述的記述で、数ページにわたることがある。TOE 記述では、TOE 概要より詳細に、TOE のセキュリティ機能に関する一般的な理解を評価者及び潜在的な消費者に与えるべきである。TOE 記述は、その TOE が合致するより幅広い用途を記述するために使用することもできる。

337 TOE 記述では、TOE の物理的な範囲、つまり TOE を構成するすべてのハードウェア、ファームウェア、ソフトウェア、及びガイダンスの各部分のリストを記述する。このリストは、各部分の包括的な理解を読者に与えるために十分な詳細レベルで記述するべきである。

338 TOE 記述では、TOE の論理的な範囲、つまり TOE によって提供される論理セキュリティ機能の特徴についても、包括的な理解を読者に与えるために十分な詳細レベルで説明するべきである。この記述は、TOE 概要で記述される主要なセキュリティ機能の特徴よりも詳細にすることが求められる。

339 物理的及び論理的範囲の重要な特性は、特定の部分または機能が TOE に含まれるか、あるいは TOE の範囲外であるかどうかについて、曖昧な点を残さない方法で、TOE を記述することである。これは、TOE が TOE 以外のエンティティと相互に関連し、簡単に分離できない場合には特に重要である。

340 TOE が TOE 以外のエンティティと相互に関連している例を次に示す：

TOE が IC 全体ではなく、スマートカード IC の暗号化コプロセッサである場合；

TOE が暗号化プロセッサを除くスマートカード IC である場合；

TOE が MinuteGap Firewall v18.5 のネットワークアドレス変換部分である場合。

A.5 適合主張(ASE_CCL)

341 ST のこの節では、ST が以下とどのように適合するかを記述する：

本国際標準のパート2及びパート3；

プロテクションプロファイル(存在する場合)；

パッケージ(存在する場合)。

342 ST を CC に適合させる方法の記述は、使用する CC のバージョンと、ST に拡張セキュリティ要件が含まれるかどうか(A.8 節を参照のこと)の 2 つの項目から構成される。

343 プロテクションプロファイルに対する ST の適合性の記述では、ST は適合性を主張するプロテクションプロファイルをリストする。この説明については、10.4 節を参照のこと。

344 パッケージに対する ST の適合性の記述では、ST は適合性を主張するパッケージをリストする。この説明については、10.4 節を参照のこと。

A.6 セキュリティ課題定義(ASE_SPD)

A.6.1 序説

345 セキュリティ課題定義では、対処する必要があるセキュリティ課題を定義する。CC に関する限り、セキュリティ課題定義は自明のこととして扱われる。つまり、セキュリティ課題定義を引き出すプロセスは、CC の範囲外である。

346 しかし、評価結果の有用性は ST に大きく依存し、ST の有用性はセキュリティ課題定義の質に大きく依存することに注意するべきである。したがって、良好なセキュリティ課題定義を引き出すために、多くの資源を費やし、明確に定義されたプロセス及び分析を使用するに値することがある。

347 CC パート3 に従い、すべての節にステートメントを記述することは必須ではないことに注意する必要がある。ST に脅威が存在する場合は OSP を記述する必要はなく、その逆もあてはまる。また、ST には前提条件が無くても良い。

348 TOE が物理的に分散している場合は、TOE 運用環境の個別領域ごとに関連する脅威、OSP、及び前提条件を記述することが望ましい場合がある。

セキュリティターゲットの仕様(参考)

A.6.2 脅威

349 セキュリティ課題定義のこの節では、TOE、その運用環境、またはこれら 2 つの組み合わせによって対抗する必要がある脅威を示す。

350 脅威は、資産に対する脅威エージェントの有害なアクションから構成される。

351 有害なアクションとは、脅威エージェントが資産に対して行うアクションである。これらのアクションは、資産価値を生じる資産の 1 つ以上の特性に影響を与える。

352 脅威エージェントは個々のエンティティとして記述することができるが、場合によってはエンティティの種別、エンティティのグループなどとして記述の方が適切である。

353 脅威エージェントの例には、ハッカー、利用者、コンピュータのプロセス、及び事故などがある。脅威エージェントは、技能、資源、機会、及び動機などの側面によって、さらに詳細に記述することができる。

354 脅威の例を次に示す：

企業のネットワークから秘密ファイルをリモートにコピーするハッカー(優れた技能、標準的な機器を有し、この行為に対して報酬を受け取る)；

広域ネットワーク(WAN)のパフォーマンスを大幅に低下させるワーム；

利用者のプライバシーを侵害するシステム管理者；

機密電子通信を盗聴しているインターネット上の何者か。

A.6.3 組織のセキュリティ方針(OSP)

355 セキュリティ課題定義のこの節では、TOE、その運用環境、またはこれら 2 つの組み合わせによって実施する必要がある OSP を示す。

356 OSP とは、実際または仮想上の組織によって、その運用環境において現在及び/または将来に課される(または課されると推定される)セキュリティの規則、手続き、またはガイドラインである。OSP は TOE の運用環境を管理する組織によって規定される場合もあれば、または立法機関もしくは規制機関によって規定される場合もある。OSP は、TOE 及び/または TOE の運用環境に適用できる。

357 OSP の例を次に示す：

政府によって使用されるすべての製品は、パスワード生成及び暗号化に関して国家基準に適合しなければならない；

システム管理者の特権と部門機密に対する許可を持つ利用者のみが、部門ファイルサーバを管理できるようにしなければならない。

A.6.4 前提条件

358 セキュリティ課題定義のこの節では、セキュリティ機能性を提供できるようにするために、その運用環境に対して設定する前提条件を示す。TOE がこれらの前提条件を満たさない運用環境に配置される場合、その TOE はそのセキュリティ機能性のすべては提供することができなくなる可能性がある。前提条件には、運用環境の物理的条件、人的条件及び接続に関する条件などがある。

359

前提条件の例を次に示す:

運用環境の物理的側面に関する前提条件:

TOE は電磁波の放射を最小限にするように設計された部屋に配置されることを前提とする;

TOE の管理者コンソールがアクセスの制限された領域に配置されることを前提とする。

運用環境の人的側面に関する前提条件:

TOE の利用者が TOE を運用するために十分に訓練を受けることを前提とする;

国家機密として分類される情報に対して、TOE の利用者が承認を受けることを前提とする;

TOE の利用者がパスワードを書き留めないことを前提とする。

運用環境の接続の側面に関する前提条件:

TOE を実行するために、ディスク領域が最低 10GB の PC ワークステーションを利用できることを前提とする;

TOE は、このワークステーションで実行されている OS 以外の唯一のアプリケーションであることを前提とする;

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。

360

評価中に、これらの前提条件は満たされているとみなされる。つまり、前提条件は決してテストされることはない。このため、前提条件は運用環境のみに対して設定できる。評価では TOE に関する主張が正しいことを前提とせず、TOE に関する主張を評価するため、TOE のふるまいに関して前提条件を設定することはできない。

A.7 セキュリティ対策方針(ASE_OBJ)

361

セキュリティ対策方針は、セキュリティ課題定義によって定義される課題に対して意図している解決策の簡潔かつ抽象的なステートメントである。セキュリティ対策方針には、次の 3 つの役割がある:

課題に対して、自然言語で記述された上位レベルの解決策を提供する;

この解決策を 2 つの部分的な解決策に分割する。これらの部分的な解決策には、異なるエンティティのそれぞれが課題の一部に対処しなければならないことが反映されている;

これらの部分的な解決策が課題に対する完全な解決策を形成することを実証する。

A.7.1 上位レベル解決策

362 セキュリティ対策方針は、過剰な詳細のない簡潔かつ明確なステートメントのセットから構成される。これらの組み合わせによって、セキュリティ課題に対する上位レベルの解決策が形成される。セキュリティ対策方針の抽象化のレベルは、TOE について知識のある潜在的消費者にとって明確で、理解可能にすることを目的としている。セキュリティ対策方針は自然言語で記述する。

A.7.2 部分的な解決策

363 ST では、上位レベルセキュリティ解決策は、セキュリティ対策方針によって記述されるように、2 つの部分的解決策に分割される。このような 2 つの部分的解決策は、TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針と呼ばれる。これは、部分的解決策が、TOE 及び運用環境という 2 種類の異なるエンティティによって提供されることを反映している。

A.7.2.1 TOE のセキュリティ対策方針

364 TOE は、セキュリティ課題定義によって定義される課題の特定の部分を解決するために、セキュリティ機能性を提供する。この部分的解決策は TOE のセキュリティ対策方針と呼ばれ、課題の特定の部分を解決するために TOE が達成すべき目標のセットから構成される。

365 TOE のセキュリティ対策方針の例を次に示す：

TOE は、TOE とサーバ間で送信されるすべてのファイルの内容の秘密を保持しなければならない；

TOE は、TOE が提供する送信サービスへのアクセスを許可する前に、すべての利用者を識別し、認証しなければならない；

TOE は、ST の附属書 3 に記述されるデータアクセス方針に従って、データに対する利用者のアクセスを制限しなければならない。

366 TOE が物理的に分散している場合は、これを反映するために、TOE のセキュリティ対策方針を含む ST の節を複数の項に分割することが望ましい場合がある。

A.7.2.2 運用環境のセキュリティ対策方針

367 TOE の運用環境は、TOE が(TOE のセキュリティ対策方針によって定義される)セキュリティ機能性を正しく提供できるように TOE を支援する技術及び手続きに関する手段を実装する。この部分的解決策は運用環境のセキュリティ対策方針と呼ばれ、運用環境で達成すべき目標を記述するステートメントのセットから構成される。

368 運用環境のセキュリティ対策方針の例を次に示す：

運用環境では、TOE を実行するために OS Inux バージョン 3.01b が動作しているワークステーションを提供しなければならない；

運用環境では、TOE の操作を許可する前に、すべての人間の TOE 利用者が適切な訓練を受けるようにしなければならない；

TOE の運用環境では、管理者及び管理者に随行された保守員に TOE への物理的アクセスを制限しなければならない；

運用環境では、中央監査サーバに送信する前に、TOE によって生成される監査ログの機密性を確保しなければならない。

369 TOE の運用環境が特性の異なる複数のサイトから構成されている場合は、これを反映するために、運用環境のセキュリティ対策方針を含む ST の節を複数の項に分割することが望ましい場合がある。

A.7.3 セキュリティ対策方針とセキュリティ課題定義の関係

370 ST には、次の 2 つの節からなるセキュリティ対策方針根拠も含まれる:

どのセキュリティ対策方針が、どの脅威、OSP、及び前提条件に対処するかを示す追跡;

すべての脅威、OSP、及び前提条件がセキュリティ対策方針によって効果的に対処されることを示す正当化のセット。

A.7.3.1 セキュリティ対策方針とセキュリティ課題定義の間の追跡

371 追跡は、セキュリティ対策方針が、セキュリティ課題定義で記述される脅威、OSP、及び前提条件までどのようにさかのぼるかを示す。

- a) *偽りの対策方針の禁止*: 各セキュリティ対策方針は、少なくとも 1 つの脅威、OSP、または前提条件までたどる。
- b) *セキュリティ課題定義に関する完全性*: 各脅威、OSP、及び前提条件には、各々までたどる少なくとも 1 つのセキュリティ対策方針がある。
- c) *正確な追跡*: 前提条件は常に運用環境について TOE により設定されるため、TOE のセキュリティ対策方針は前提条件までさかのぼらない。CC パート 3 により許可される追跡を図 7 に示す。

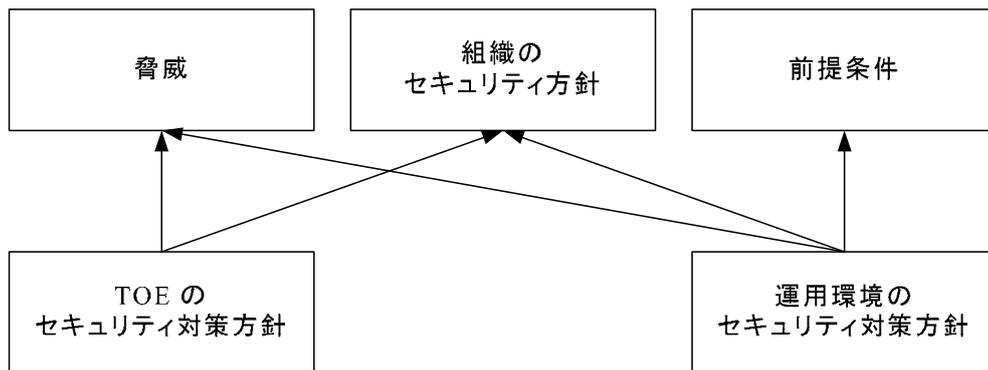


図 7 セキュリティ対策方針とセキュリティ課題定義の間の追跡

372 複数のセキュリティ対策方針がたどった先が同じ脅威になることがあるが、その場合、これらのセキュリティ対策方針の組み合わせがその脅威に対抗することを示す。OSP 及び前提条件にも同じことが当てはまる。

セキュリティターゲットの仕様(参考)

A.7.3.2 追跡の正当化の提供

- 373 セキュリティ対策方針根拠では、追跡が有効であることも実証する：特定の脅威、OSP または前提条件までたどるすべてのセキュリティ対策方針が達成された場合、すべての与えられた脅威、OSP 及び前提条件は対処される(すなわち、それぞれは、対抗、実施、及び充足される)。
- 374 この実証では、関連セキュリティ対策方針を達成することによる、脅威への対抗、OSP の実施、及び前提条件の充足への効果を分析し、実際に対抗、実施、及び充足されるという結論を導く。
- 375 セキュリティ課題定義の一部がいくつかのセキュリティ対策方針と非常に似ているような一部の状況では、実証は非常に簡単になることがある。例えば：脅威が「T17: 脅威エージェント X は AB 間の転送時に秘密情報を読み取る」、TOE のセキュリティ対策方針が「OT12: TOE は AB 間で送信されるすべての情報の秘密が確実に保持されるようにしなければならない」の場合、「T17 は OT12 によって直接対抗される」と実証される。

A.7.3.3 脅威への対抗について

- 376 脅威への対抗とは、必ずしもその脅威を除去することを意味せず、脅威を十分に減らすこと、または脅威を十分に緩和することを意味する場合もある。

- 377 脅威の除去の例は、次のとおりである：

脅威エージェントから有害なアクションを実行する能力を除去する；

有害なアクションを資産に対して行うことができなくなるように、資産を移動、変更、または保護する；

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)。

- 378 脅威の軽減の例は、次のとおりである：

有害なアクションを実行する脅威エージェントの能力を制限する；

脅威エージェントが有害なアクションを実行する機会を制限する；

実行された有害なアクションが成功する可能性を減少させる；

抑止によって脅威エージェントが有害なアクションを実行する動機を減少させる；

脅威エージェントにより多くの専門知識または資源を要求する。

- 379 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；

資産のスペアコピーを取る；

資産に保険をかける；

適切なアクションをとることができるように、成功したすべての有害なアクションが適切な時機に必ず検出されるようにする。

A.7.4 セキュリティ対策方針: 結論

380 セキュリティ対策方針及びセキュリティ対策方針根拠に基づいて、すべてのセキュリティ対策方針が達成された場合セキュリティ課題定義(ASE_SPD)で定義されるセキュリティ課題は解決される、という結論を下すことができる。つまり、すべての脅威が対抗され、すべてのOSPが実施され、すべての前提条件が充足される。

A.8 拡張コンポーネント定義(ASE_ECD)

381 多くの場合、STのセキュリティ要件(次の節を参照のこと)は、CCパート2またはCCパート3のコンポーネントに基づく。ただし、場合によっては、CCパート2またはCCパート3のコンポーネントに基づかないSTの要件が存在することがある。この場合は、新しいコンポーネント(拡張コンポーネント)を定義しなければならず、この定義は拡張コンポーネント定義で行うべきである。これについての詳細は、附属書C.4を参照のこと。

382 この節では、拡張コンポーネントのみを扱い、拡張要件(拡張コンポーネントに基づく要件)については扱わない。拡張要件はセキュリティ要件(次の節を参照のこと)に含めるべきであり、すべての目的のために、CCパート2またはCCパート3のコンポーネントに基づく要件と同じにする。

A.9 セキュリティ要件(ASE_REQ)

383 セキュリティ要件は、以下の2つのグループの要件から構成される:

- a) *セキュリティ機能要件(SFR)*: TOEのセキュリティ対策方針から標準言語への書き換え;
- b) *セキュリティ保証要件(SAR)*: TOEがSFRを満たすという保証を取得する方法の記述。

384 これらの2つのグループについては、次の2つの節で説明する:

A.9.1 セキュリティ機能要件(SFR)

385 SFRは、TOEのセキュリティ対策方針の書き換えである。通常、これらはより詳細な抽象レベルで記述されるが、完全な書き換えにしなければならない(セキュリティ対策方針には、すべて対応しなければならない)、また、特定の技術的ソリューション(実装)に依存しないようにしなければならない。CCは、次のような複数の理由のために、標準言語への書き換えを要求する:

評価する対象について正確に記述するため。TOEのセキュリティ対策方針は一般に自然言語で作成されるため、標準言語への書き換えによって、TOEの機能性をより正確に記述できる。

2つのST間の比較を可能にするため。セキュリティ対策方針の記述においてSTの作成者ごとに異なる用語を使用することがあるが、標準言語では、同じ用語及び概念を使用する。これによって比較が簡単になる。

386 CCでは、運用環境のセキュリティ対策方針に対して、書き換えは要求されない。これは、運用環境が評価されず、それゆえに、評価を目的とした記述を必要としないためである。運用システムのセキュリティ評定に関連する項目に関しては、参考文献参照。

セキュリティターゲットの仕様(参考)

387 運用環境の部分は別の評価として評価される場合があるが、これは現在の評価の範囲外である。例えば、OS TOE は、運用環境でファイアウォールの設置を要求することがある。別の評価において、後にファイアウォールを評価するかもしれないが、この評価は OS TOE の評価とは関係がない。

A.9.1.1 CC がこの書き換えをサポートする方法

388 CC は、次の 3 つの方法で、この書き換えをサポートする:

- a) 評価する対象を正確に記述することを目的とし、事前に定義された正確な「言語」を提供する。この言語は、CC パート 2 で定義されるコンポーネントのセットとして定義する。TOE のセキュリティ対策方針から SFR への明確に定義された書き換えとしてこの言語を使用することは必須であるが、一部の例外が存在する(8.3 節を参照のこと)。
- b) 操作を提供する。つまり、TOE のセキュリティ対策方針のより正確な書き換えを提供するために、ST 作成者が SFR を改変することを許可するメカニズムを提供する。CC の本パートでは、4 つの許可された操作を定義する: 割付、選択、繰返し、及び詳細化。これらについては、8.1 節でより詳細に説明する。
- c) 依存性を提供する。つまり、SFR へのより完全な書き換えをサポートするメカニズムを提供する。CC パート 2 の言語では、SFR は他の SFR に依存することがある。これは、ST がその SFR を使用する場合、一般に他の SFR も使用する必要があることを意味する。これによって、ST の作成者が加える必要がある SFR を見過ごす可能性ははるかに少なくなるため、ST の完全性が向上する。依存性については、附属書 8.2 節でより詳細に説明する。

A.9.1.2 SFR とセキュリティ対策方針の関係

389 ST には、SFR についての次の 2 つの節から構成されるセキュリティ要件根拠も含まれる:

どの SFR が、TOE のどのセキュリティ対策方針に対処するかを示す追跡;

TOE のすべてのセキュリティ対策方針が SFR によって効果的に対処されることを示す正当化のセット。

A.9.1.2.1 SFR と TOE のセキュリティ対策方針間の追跡

390 この追跡は、SFR がどのように TOE のセキュリティ対策方針にまでさかのぼるかを以下に示す:

- a) *偽りの SFR の禁止*: 各 SFR は、少なくとも 1 つのセキュリティ対策方針までさかのぼる。
- b) *TOE のセキュリティ対策方針に関する完全性*: TOE の各セキュリティ対策方針には、当該セキュリティ対策方針にたどる少なくとも 1 つの SFR が必要である。

391 複数の SFR がたどった先が同じ TOE のセキュリティ対策方針になることがあるが、その場合、これらのセキュリティ要件の組み合わせがその TOE のセキュリティ対策方針を満たすことを示す。

A.9.1.2.2 追跡の正当化の提供

392 セキュリティ要件根拠では、追跡が有効であることを実証する。つまり、特定の TOE のセキュリティ対策方針までたどるすべての SFR が満たされた場合、その TOE のセキュリティ対策方針は達成される。

393 この実証では、関連 SFR を満たすことによる、TOE のセキュリティ対策方針の達成への効果を分析し、実際にその TOE のセキュリティ対策方針が達成されるという結論を導く。

394 SFR が TOE のセキュリティ対策方針と非常に似ているような場合には、実証は非常に簡単になることがある。

A.9.2 セキュリティ保証要件(SAR)

395 SAR は、TOE を評価する方法の記述である。この記述では、次の 2 つの理由のために標準言語を使用する:

TOE の評価方法について正確に記述するため。標準言語の使用は、正確に記述し、曖昧さをなくすために役立つ。

2 つの ST 間の比較を可能にするため。評価の記述において ST の作成者ごとに異なる用語を使用することがあるが、標準言語では、同じ用語及び概念を使用する。これによって比較が簡単になる。

396 標準言語は、CC パート 3 で定義されるコンポーネントのセットとして定義されている。いくつかの例外は存在するが、この言語の使用は必須である。CC は、次の 2 つの方法でこの言語を拡張する:

- a) 操作を提供する。ST 作成者が SAR を改変することを許可するメカニズムを提供する。CC には、割付、選択、繰返し、及び詳細化の 4 つの操作がある。これらについては、8.1 節でより詳細に説明する。
- b) 依存性を提供する。つまり、SAR へのより完全な書き換えをサポートするメカニズムを提供する。CC パート 3 の言語では、SAR は他の SAR に依存することがある。これは、ST がその SAR を使用する場合、一般に他の SAR も使用する必要があることを意味する。これによって、ST の作成者が加える必要がある SAR を見過ごす可能性ははるかに少なくなるため、ST の完全性が向上する。依存性については、8.2 節でより詳細に説明する。

A.9.3 SAR 及びセキュリティ要件根拠

397 ST には、SAR の特定のセットを適切とみなす理由を説明するセキュリティ要件根拠も含まれる。この説明に対して特定の要件は存在しない。この説明の目的は、この特定のセットが選択された理由を、ST の読者が理解できるようにすることである。

398 非一貫性の例としては、セキュリティ課題の記述で、脅威エージェントの能力が非常に高い脅威が言及されているが、SAR に含まれる脆弱性分析(AVA_VAN)のレベルが低い(または存在しない)場合がある。

A.9.4 セキュリティ要件: 結論

399 ST のセキュリティ課題定義では、セキュリティ課題は脅威、OSP、及び前提条件から構成されるものとして定義される。ST のセキュリティ対策方針の節で、解決策は次の 2 つの解決策の形式で提供される:

 TOE のセキュリティ対策方針;

 運用環境のセキュリティ対策方針。

400 また、すべてのセキュリティ対策方針が達成された場合は、セキュリティ課題が解決されることを示すセキュリティ対策方針根拠が提供される。つまり、すべての脅威が対抗され、すべての OSP が実施され、すべての前提条件が充足される。

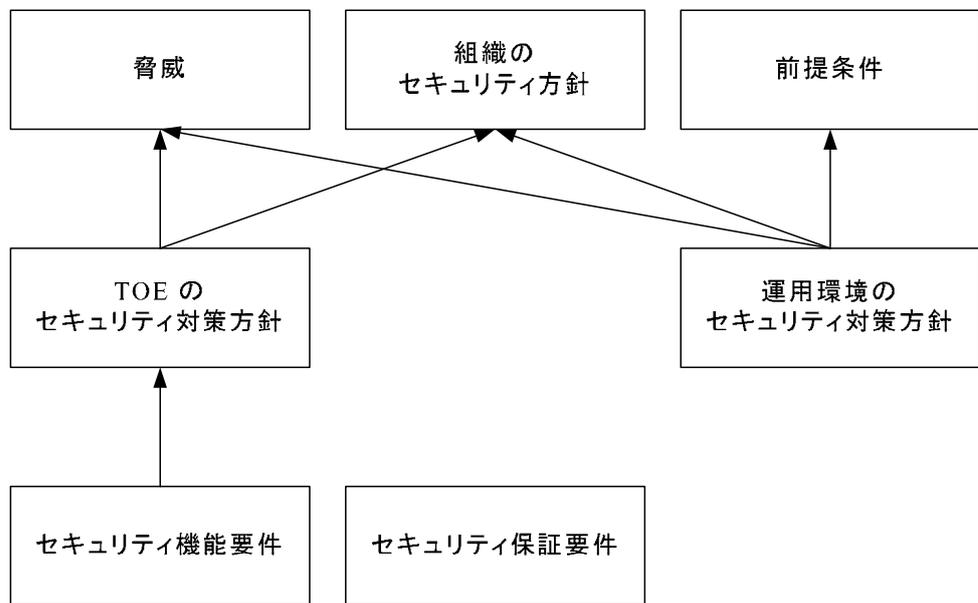


図 8 セキュリティ課題定義、セキュリティ対策方針、及びセキュリティ要件の関係

401 ST のセキュリティ要件の節で、TOE のセキュリティ対策方針は SFR に書き換えられ、すべての SFR が満たされた場合に、TOE のすべてのセキュリティ対策方針が達成されることを示すセキュリティ要件根拠が提供される。

402 また、SAR の選択についての説明とともに、TOE の評価方法を示す SAR のセットが提供される。

403 上記のすべては、次のステートメントに纏めることができる。すべての SFR 及び SAR が満たされ、運用環境のすべてのセキュリティ対策方針が達成された場合、ASE_SPD で定義されるセキュリティ課題が解決される、つまり、すべての脅威が対抗され、すべての OSP が実施され、すべての前提条件が充足されるという保証が得られる。図 8 にこれを示す。

404 得られる保証の総量は SAR によって定義され、この保証の量が十分であるかどうかは、SAR の選択についての説明によって定義される。

A.10 TOE 要約仕様(ASE_TSS)

- 405 TOE 要約仕様の目的は、TOE がどのようにすべての SFR を満たすかについての記述を、TOE の潜在的な消費者に提供することである。TOE 要約仕様では、この目的のために TOE が使用する一般的な技術的メカニズムを示すべきである。この記述の詳細レベルは、潜在的な消費者が TOE の一般的な形態及び実装を理解できる程度にするべきである。
- 406 例えば、TOE がインターネット PC で、SFR に認証を特定する FIA_UAU.1 が含まれる場合、TOE 要約仕様では、パスワード、トークン、虹彩スキャンなど、この認証を行う方法を示すべきである。SFR を満たすために TOE が使用する適用規格のような、より詳細な情報またはより詳細な記述も提供することができる。

A.11 ST を使用して回答できる質問

- 407 評価後に、ST は「評価された対象」を特定する。この役割において、ST は、TOE の開発者または再販業者と TOE の潜在的な消費者間での合意の基礎となる。したがって、ST では次のような質問に回答することができる(これらに限定されない):
- a) *多数の既存の ST/TOE の中で、必要な ST/TOE をどのように見つけることができるか。* この質問には、TOE の簡潔な(数段落の)要約を示す TOE 概要で回答する;
 - b) *この TOE は当方の既存の IT 基盤に適合するか。* この質問には、TOE を実行するために必要な主要なハードウェア/ファームウェア/ソフトウェアエレメントを識別する TOE 概要で回答する;
 - c) *この TOE は当方の既存の運用環境に適合するか。* この質問には、動作させるために TOE が運用環境に課すすべての制約を識別する、運用環境のセキュリティ対策方針で回答する;
 - d) *TOE は何をするか(関心のある読者向け)。* この質問には、TOE の簡潔な(数段落の)要約を示す TOE 概要で回答する;
 - e) *TOE は何をするか(潜在的な消費者向け)。* この質問には、TOE のより詳細な(数ページの)要約を示す TOE 記述で回答する;
 - f) *TOE は何をするか(技術者向け)。* この質問には、TOE が使用するメカニズムについて上位レベルの記述をする TOE 要約仕様で回答する;
 - g) *TOE は何をするか(専門家向け)。* この質問には、抽象的かつ高度に技術的な記述を提供する SFR と、追加の詳細を提供する TOE 要約仕様で回答する;
 - h) *TOE は当方の政府/組織によって定義される課題に対応するか。* 政府または組織がこの解決策を定義するためにパッケージ及び/または PP を定義している場合、この回答は ST が適合するすべてのパッケージ及び PP をリストする ST の適合主張の節にある;
 - i) *TOE は当方のセキュリティ課題に対応するか(専門家向け)。* TOE が対抗する脅威は何か。どのような組織のセキュリティ方針を実施するか。運用環境についてどのような前提条件を設定しているか。これらの質問には、セキュリティ課題定義で回答する;

- j) どの程度 TOE を信頼することができるか。この回答は、セキュリティ要件の節の SAR にある。SAR によって、TOE を評価するために使用された保証レベル、つまり TOE の正確性に関して評価が提供する信頼度が提供される。

A.12 低保証セキュリティターゲット

408 ST の記述は簡単な作業ではなく、特に低保証評価では、評価全体において開発者及び評価者が行う全作業のうち大部分を占めることがある。このため、低保証 ST を記述することもできる。

409 CC は、EAL 1 評価のために低保証 ST を使用することを許可しているが、EAL 2 以上では許可していない。低保証 ST は、低保証 PP への適合のみを主張することができる(附属書 B を参照のこと)。通常の ST(つまり、すべての内容を含むもの)は、低保証 PP への適合を主張することができる。

410 低保証 ST では、通常の ST に比べて次のように内容が大幅に削減されている:

セキュリティ課題定義を記述する必要はない;

TOE のセキュリティ対策方針を記述する必要がない。ただし、運用環境のセキュリティ対策方針は記述しなければならない;

ST にセキュリティ課題定義がないため、セキュリティ対策方針根拠を記述する必要はない;

ST には TOE のセキュリティ対策方針がないため、セキュリティ要件根拠は、満たされていない依存性(存在する場合)のみを正当化する必要がある。

411 残りのすべての内容を以下に示す:

- a) TOE 及び ST への参照;
- b) 適合主張;
- c) 次のような様々な叙述的記述;
 - 1. TOE 概要;
 - 2. TOE 記述;
 - 3. TOE 要約仕様。
- d) 運用環境のセキュリティ対策方針;
- e) SFR 及び SAR(拡張コンポーネント定義を含む)とセキュリティ要件根拠(依存性が満たされていない場合のみ)。

412

低保証 ST の削減された内容を図 9 に示す。

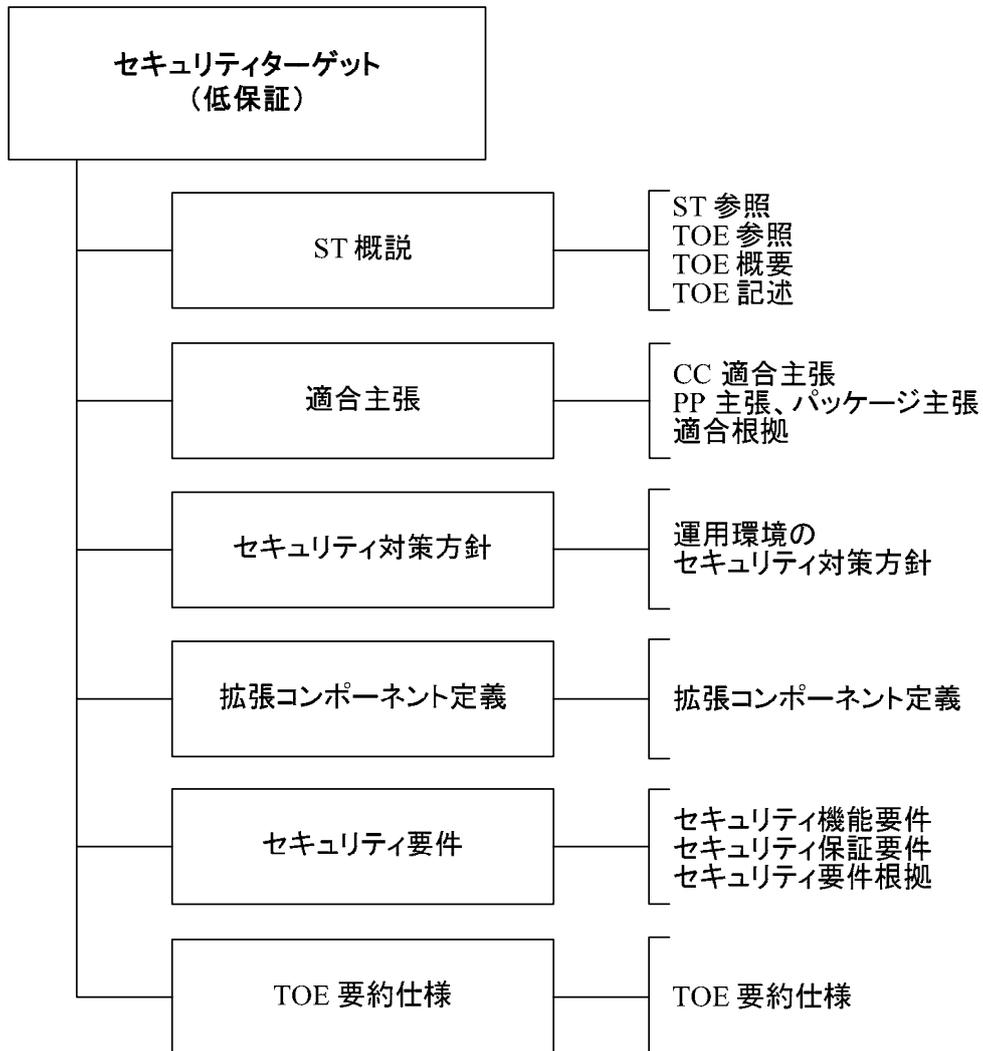


図 9 低保証セキュリティターゲットの内容

A.13 ST での他の標準の参照

413

場合によって、ST 作成者は、特定の暗号標準またはプロトコルなどの外部標準を参照しようとすることがある。CC では、次の 3 つの方法によってこれを行うことができる:

- a) 組織のセキュリティ方針(またはその一部)として。

例えば、パスワードを選択する方法を定義する政府標準が存在する場合、これは ST で組織のセキュリティ方針として言及することができる。これにより、(例えば TOE の利用者がパスワードを標準に従って選択する必要がある場合は)環境のセキュリティ対策方針が導出され、TOE がパスワードを生成する場合は、TOE のセキュリティ対策方針と、それに続いて適切な SFR(おそらく FIA クラス)が導出されることがある。どちらの場合にも、開発者の根拠によって、TOE のセキュリティ対策方針と SFR が OSP を満たすために適切

であることを明確にする必要がある。OSP が SFR によって実装される場合、評価者はこれが実際に明確であるかどうかを次のように検査する(そして、この検査のためにその標準を調査することを決定する場合がある)。

- b) SFR の詳細化で使用される技術標準(例えば暗号標準)として。

この場合、標準への適合は TOE による SFR の充足の一部であり、標準の全文が SFR の一部であるかのように扱われる。適合性は、SFR に対するその他の適合と同様に、後に決定される。つまり、ADV:開発及び ATE:テスト中に、設計の分析及びテストによって、SFR が TOE で完全かつ十分に実装されていることが分析される。標準の特定部分のみへの参照が必要な場合、その部分は SFR の詳細化で明確に記述するべきである。

- c) TOE 要約仕様で言及される技術標準(例えば暗号標準)として。

TOE 要約仕様は、SFR を実現する方法の説明としてのみ考慮に入れられ、SFR または ADV:開発のために配付される文書のような厳格な実装要件としては決して使用されない。したがって、TSS が技術標準を参照し、これが ADV:開発証拠資料に反映されていない場合、評価者は非一貫性を検出することができるが、標準の充足性をテストするための決められたアクティビティは存在しない。

附属書B プロテクションプロファイルの仕様(参考)

B.1 本附属書の目的及び構造

- 414 この附属書の目的は、プロテクションプロファイル(PP)の概念を説明することである。本附属書では、APE 基準の定義は行わない。この定義は、CC パート 3 にあり、参考文献にある文書によりサポートされている。
- 415 PP と ST は非常に重複しているため、本附属書では PP と ST の相違点に重点を置く。ST と PP 間で同一の事項については、附属書 A で説明する。
- 416 本附属書は、次の 4 つの主要なパートから構成されている：
- a) *PP の必須の内容*。これについては、B.2 節で概要を示し、B.4 節から B.9 節でより詳細に説明する。これらの節では、PP の必須の内容と各内容間の相互関係について説明し、例を示す。
 - b) *PP の使用法*。これについては、B.3 節で概要を示す。
 - c) *低保証PP*。低保証 PP は、内容の削減された PP である。これについては、B.11 節で詳細に説明する。
 - d) *標準への準拠の主張*。B.12 節では、PP 作成者が、TOE が特定の標準を満たしていることを主張する方法を説明する。

B.2 PP の必須の内容

- 417 図 10 に、CC パート3記述の PP に必須の内容を示す。図 10 は PP の構造的アウトラインとしても使用することができる。ただし、別の構造も使用可能である。例えば、セキュリティ要件根拠が非常に長くなる場合は、セキュリティ要件の節の代わりに、PP の附属書にそれを記述することができる。PP の個別の節と、各節の内容について、以下に簡単に概要を示し、B.4 節から B.9 節でより詳細に説明する。PP の内容は、次のとおりである：
- a) TOE 種別の叙述的記述を含む *PP 概説*、
 - b) PP が PP 及び/またはパッケージへの適合を主張するかどうかと、主張する場合にはその PP 及び/またはパッケージを示す *適合主張*、
 - c) 脅威、OSP、及び前提条件を示す *セキュリティ課題定義*、
 - d) TOE のセキュリティ対策方針と TOE の運用環境のセキュリティ対策方針で、セキュリティ課題の解決策を分担する方法を示す *セキュリティ対策方針*、
 - e) 新しい(つまり CC パート 2 または CC パート 3 に含まれていない)コンポーネントを定義することができる *拡張コンポーネント定義*。これらの新しいコンポーネントは、拡張機能要件及び拡張保証要件を定義するために必要である；
 - f) TOE のセキュリティ対策方針から標準言語への書き換えを提供する *セキュリティ要件*。この標準言語は、SFR の形式をとる。また、この節では SAR について定義する；

418

内容を削減された低保証 PP もある。これについては、B.11 節で詳細に説明する。これを除いて、本附属書のすべての他の部分では、すべての内容を含む PP の使用を前提としている。

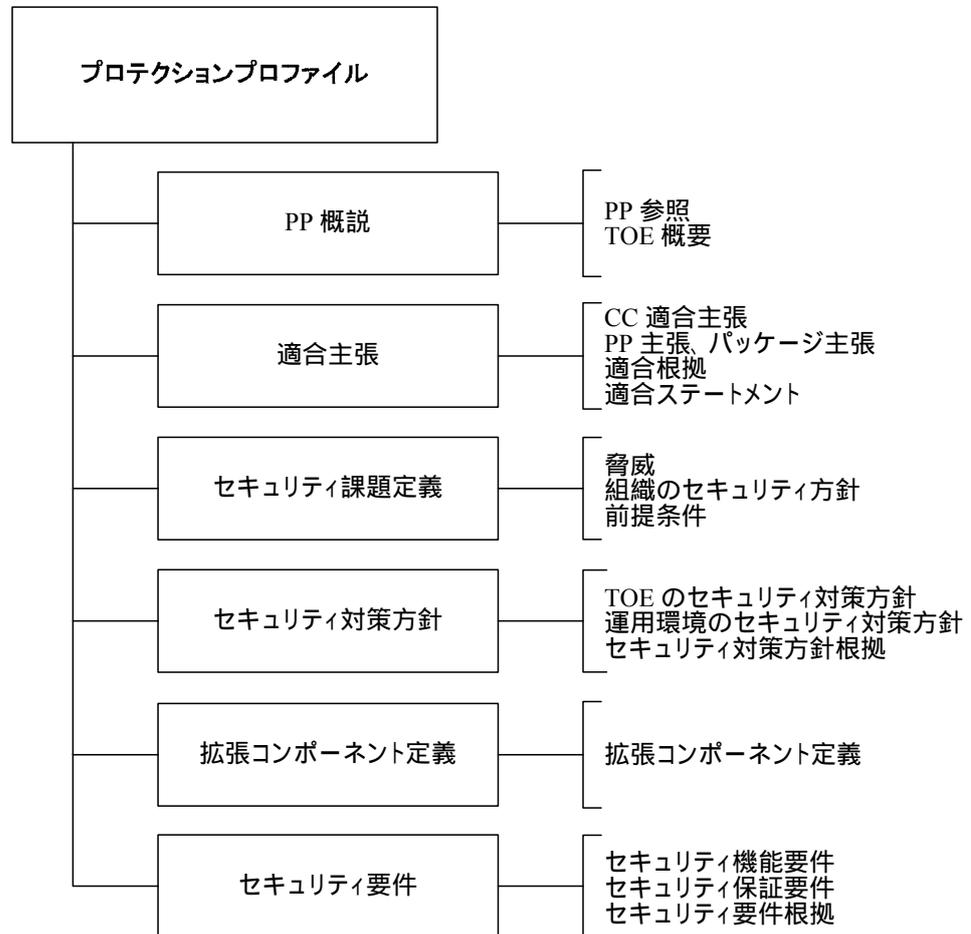


図 10 プロテクションプロファイルの内容

B.3 PP の使用

B.3.1 PP の使用法

419

一般に、PP は利用者コミュニティ、規制組織、または開発者グループがセキュリティニーズの共通セットを定義する場合のニーズのステートメントである。PP は、このセットを参照する手段を消費者に提供し、このようなニーズを背景とする将来の評価を容易にする。

420

したがって、PP は一般に以下のように使用される:

特定の消費者または消費者グループに対する要件仕様の一部。この消費者または消費者グループは、PP を満たしている場合にのみ特定の種別の IT の購入を検討する;

特定の規制組織による規制の一部。この規制組織は、PP を満たしている場合にのみ特定の種別の IT の使用を許可する;

IT 開発者のグループによって定義されるベースライン。この開発者グループは、製作するこの種別のすべての IT がこのベースラインを満たすことに合意する。

ただし、上記の例によってその他の用途が排除されることはない。

B.3.2 PP の不適切な使用法

421 PP が果たすべきではない 3 つの役割は次のとおりである(これらに限定されない):

詳細な仕様 PP は、比較的高い抽象レベルのセキュリティ仕様を目的としている。一般に、PP には詳細なプロトコル仕様、詳細なアルゴリズム及び/またはメカニズムの記述、詳細な運用についての長い説明などを記述するべきではない。

完全な仕様 PP は、全体仕様ではなく、セキュリティ仕様を目的としている。セキュリティに関係しない限り、相互運用性、物理的なサイズ及び重量、要求される電圧などの特性は、PP に記述するべきではない。つまり、一般に PP は完全な仕様自体ではなく、完全な仕様の一部である。

単一製品の仕様 ST とは異なり、PP は単一の製品ではなく、IT の特定の種別について記述することを目的とする。単一の製品のみについて記述する場合は、この目的のために ST を使用することが望ましい。

B.4 PP 概説(APE_INT)

422 PP 概説では、次の 2 つの抽象レベルで叙述的な方法により TOE について記述する:

- a) PP の識別情報を提供する PP 参照;
- b) TOE について簡潔に記述する TOE 概要。

B.4.1 PP 参照

423 PP には、特定の PP を識別する明確な PP 参照が含まれる。一般的な PP 参照は、タイトル、バージョン、作成者、及び公表日から構成される。PP 参照は、例えば「Atlantean Navy CablePhone Encryptor PP、バージョン 2b、アトラス海軍調達局、2003 年 4 月 7 日」のように記述する。参照は、異なる PP 間及び同じ PP の異なるバージョン間で区別できるように、一意にしなければならない。

424 PP 参照によって、PP のインデックス化及び参照と、PP のリストへの組み込みが容易になる。

B.4.2 TOE 概要

425 TOE 概要は、セキュリティニーズを満たし、使用するハードウェア、ソフトウェア、及びファームウェアでサポートされている TOE を見つけるために、評価済み製品のリストに目を通している TOE の潜在的な消費者を対象としている。

426 TOE 概要は、TOE の設計または既存製品の調整で PP を使用することがある開発者も対象としている。

427 TOE 概要の一般的な長さは、数段落である。

プロテクションプロファイルの仕様(参考)

428 そのため、TOE 概要では、TOE の使用法及びその主要なセキュリティ機能の特徴について簡潔に説明し、TOE 種別を識別し、TOE を利用可能な主要な TOE 以外のハードウェア/ソフトウェア/ファームウェアを識別する。

B.4.2.1 TOE の使用法及び主要なセキュリティ機能の特徴

429 TOE の使用及び主要なセキュリティ機能の特徴に関する記述は、TOE が備えるべき機能と、TOE の用途について非常に包括的な情報を示すことを目的としている。この節は、(潜在的な)TOE 消費者のために、事業運営面から見た TOE の使用法と主要なセキュリティ機能の特徴について、TOE 消費者が理解する言葉を使用して記述するべきである。

430 この例を次に示す。「Atlantean Navy CablePhone Encryptor は、Atlantean Navy CablePhone システムを通じて船舶間で秘密情報の通信を実現すべき暗号化デバイスである。このために、最低 32 人の利用者と、最低 100Mbps の暗号化速度をサポートするべきである。これは、船舶間の相互通信と、ネットワーク全体のブロードキャストの両方を実現するべきである」。

B.4.2.2 TOE 種別

431 TOE 概要では、ファイアウォール、VPNファイアウォール、スマートカード、暗号化モデム、イントラネット、ウェブサーバ、データベース、ウェブサーバ及びデータベース、LAN、ウェブサーバ及びデータベースを伴う LAN など、TOE の一般的な種別を識別する。

B.4.2.3 利用可能な TOE 以外のハードウェア/ソフトウェア/ファームウェア

432 他の IT に依存しない TOE もあるが、多くの TOE(特にソフトウェア TOE)は、TOE 以外の追加のハードウェア、ソフトウェア及び/またはファームウェアに依存する。後者の場合に、TOE 概要では、この TOE 以外のハードウェア/ソフトウェア/ファームウェアを識別する必要がある。

433 プロテクションプロファイルは特定の製品について記述されるものではないため、多くの場合、利用可能なハードウェア/ソフトウェア/ファームウェアについて一般的な考え方のみを示すことができる。例えば、プラットフォームがすでに確認されている特定の顧客向けの要件仕様など、一部のその他の場合には、(はるかに)多くの具体的な情報が提供されることがある。

434 ハードウェア/ソフトウェア/ファームウェア識別の例を次に示す:

なし(完全なスタンドアロン TOE);

汎用 PC で動作している Yaiza 3.0 オペレーティングシステム;

CleverCard SB2067 集積回路;

QuickOS スマートカードオペレーティングシステムのバージョン 2.0 を実行している CleverCard SB2067 IC;

運輸省長官の事務局で 2002 年 12 月に設置された LAN。

B.5 適合主張(APE_CCL)

435 PP のこの節では、PP が他の PP 及びパッケージとどのように適合するかを記述する。これは、適合ステートメントのみを除いて、ST の適合主張の節と同じである(A.5 節を参照のこと)。

436 PP の適合ステートメントでは、ST 及び/またはその他の PP がその PP にどのように適合しなければならないかを述べる。PP 作成者は、「正確」適合または「論証」適合のいずれを要求するかを選択する。これに関するより詳細については、附属書 D を参照のこと。

B.6 セキュリティ課題定義(APE_SPD)

437 この節は、A.6 節で説明した ST のセキュリティ課題定義の節と同じである。

B.7 セキュリティ対策方針(APE_OBJ)

438 この節は、A.7 節で説明した ST のセキュリティ対策方針の節と同じである。

B.8 拡張コンポーネント定義(APE_ECD)

439 この節は、A.8 節で説明した ST の拡張コンポーネントの節と同じである。

B.9 セキュリティ要件(APE_REQ)

440 この節は、A.9 節で説明した ST のセキュリティ要件の節と同じである。ただし、PP において操作を完了する際の規則は、ST において操作を完了する際の規則とはやや異なっている点に注意のこと。これについては、8.1 節でより詳細に説明する。

B.10 TOE 要約仕様

441 PP には、TOE 要約仕様は含まれない。

B.11 低保証プロテクションプロファイル

442 通常の PP(つまり、すべての内容を含むもの)に対する低保証 PP の関係は、通常の ST に対する低保証 ST の関係と同じである。つまり、低保証 PP は、以下の内容から構成される。

- a) PP 参照及び TOE 概要から構成される PP 概説;
- b) 適合主張;
- c) 運用環境のセキュリティ対策方針;
- d) SFR 及び SAR(拡張コンポーネント定義を含む)とセキュリティ要件根拠(依存性が満たされていない場合のみ)。

443 低保証 PP は、低保証 PP への適合のみを主張することができる(附属書 B を参照のこと)。通常の PP は、低保証 PP への適合を主張することができる。

低保証 PP の削減された内容を図 11 に示す。

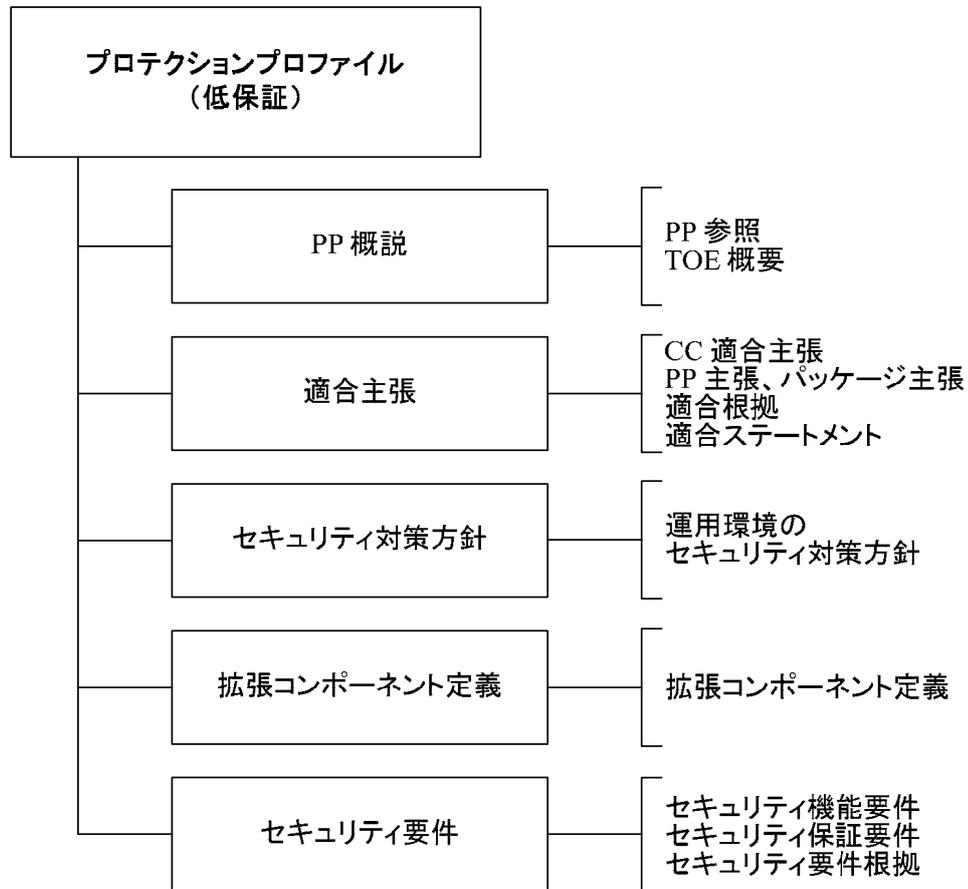


図 11 低保証プロテクションプロファイルの内容

B.12 PP での他の標準の参照

445

この節は、1 つの例外を除き、A.13 節で記述される ST の標準に関する節と同じである。この例外は、PP には TOE 要約仕様がなく、3 番目のオプションは PP に対して無効なことである。

446

SFR の中で標準を参照することが、(その標準の規模及び複雑さと、要求される保証レベルによっては)PP を満たす TOE を開発している開発者に大きな負担をかける可能性があり、標準への適合を評価するための代替的な(CC に関連しない)方法を要求する方が適切な場合があることに、PP 作成者は留意すること。

附属書C 操作のためのガイダンス(参考)

C.1 序説

447 CCパート1で記述されているとおり、プロテクションプロファイル、及びセキュリティターゲットは、あらかじめ定義されたセキュリティ要件を含むと共に、PP及びST作成者がそのコンポーネントリストをある環境で拡張する能力も提供している。

C.2 操作の例

8.1節に、4つのタイプの操作が挙げられている。各種操作例は下記のとおり:

C.2.1 繰返し操作

449 8.1.1節に記述されているとおり、繰返し操作は、すべてのコンポーネントで実行することができる。PP/ST作成者は、同じコンポーネントに基づく複数の要件を加えることによって、繰返し操作を行う。コンポーネントのそれぞれの繰返しは、そのコンポーネントの他のすべての繰返しとは異なっている。これは、異なる方法で割付及び選択を完了するか、異なる方法で詳細化を適用することによって実現される。異なる繰返しは、明確な根拠と、これらの要件との間の追跡のために、一意に識別するべきである。

450 典型的な繰返しの例は、2種類の暗号アルゴリズムの実装を要求するために、2回繰返されているFCS_COP.1がある。一意に識別される各繰返しの例を次に示す。

暗号操作(RSA及びDSA署名)(FCS_COP.1(1))

暗号操作(TLS/SSL:対称鍵操作)(FCS_COP.1(2))

C.2.2 割付操作

451 8.1.2節に記述されているとおり、割付操作は、特定のコンポーネントにPP/ST作成者によって設定されるパラメタ付きの要素が含まれる場合に行なう。パラメタは、制限のない変数、または変数を特定の範囲の値に狭める規則にすることができる。

452 割付を含む要素の例を次に示す: FIA_AFL.1.2「不成功の認証試行が定義した回数に達するか上回ったとき、TSFは、[割付: アクションのリスト]を実行しなければならない」。

C.2.3 選択操作

453 8.1.3節に記述されているとおり、選択操作は、特定のコンポーネントにPP/ST作成者が複数の項目から選択しなければならない要素が含まれる場合に行なう。

454 選択を使用する要素の例を次に示す。FPT_TST.1.1「TSFは、...の正常動作を実証するために、[選択: 初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、条件[割付: 自己テストが作動すべき条件]下で]自己テストのスイートを実行しなければならない」。

C.2.4 詳細化操作

- 455 8.1.4 節に記述されているとおり、詳細化操作は、すべての要件で実行することができる。PP/ST 作成者は、要件を変更することによって詳細化を実行する。
- 456 有効な詳細化の例を次に示す。FIA_UAU.2.1「TSF は、利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない」は、「TSF は、利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に**利用者名/パスワードによる認証が成功することを要求しなければならない**」に詳細化できる。
- 457 詳細化の最初の規則は、その PP/ST の文脈において、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ということである(つまり、詳細化された要件は、元の要件に比べ「より厳格」でなければならない)。
- 458 この規則に対する唯一の例外として、PP/ST 作成者は、全部ではなく一部のサブジェクト、オブジェクト、操作、セキュリティ属性、及び/または外部エンティティに適用するために SFR を詳細化することができる。
- 459 このような例外の例を次に示す。FIA_UAU.2.1「TSF は、利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない」は、「TSF は、利用者を代行する他の TSF 仲介アクションを許可する前に、**インターネットからアクセスしている各利用者に認証が成功することを要求しなければならない**」に詳細化できる。
- 460 所定の詳細化の 2 番目の規則は、詳細化は元のコンポーネントに関連付けなければならないことである。例えば、電磁波放射の防止について別のエレメントを使用して監査コンポーネントを詳細化することは、許可されない。
- 461 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、または読者にとってより理解しやすくす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を以下に示す:
- SFR FPT_FLS.1「TSF は、以下の種別の障害が生じたときはセキュアな状態を保持しなくてはならない: **1 基の CPU の機能停止**」は、FPT_FLS.1「TSF は、以下の 1 種類の障害が生じたときはセキュアな状態を保持しなくてはならない: **1 基の CPU の機能停止**」、さらに FPT_FLS.1「TSF は、**1 基の CPU が機能停止した場合にセキュアな状態を保持しなくてはならない**」に詳細化することができる。

C.3 コンポーネントの編成

- 462 CC は、CC パート 2 及び CC パート 3 のコンポーネントを次の階層構造に編成した:
- ファミリから構成されるクラス
 - コンポーネントから構成されるファミリ
 - エレメントから構成されるコンポーネント
 - エレメント。
- 463 消費者、開発者、及び評価者が特定のコンポーネントを見つけやすいように、クラス、ファミリ、コンポーネント、エレメントは階層状に編成されている。

464 CC は、機能コンポーネントと保証コンポーネントを同じ一般階層様式で提示しており、またそれぞれに対して同じ編成及び用語を用いている。

C.3.1 クラス

465 クラスの例には、利用者の識別、利用者の認証、及び利用者とサブジェクトの結合に焦点を置く FIA クラスがある。

C.3.2 ファミリ

466 ファミリの例には、FIA クラスの一部である利用者認証(FIA_UAU)ファミリがある。このファミリは、利用者の認証に重点を置く。

C.3.3 コンポーネント

467 コンポーネントの例には、偽造されない認証に重点を置く FIA_UAU.3 偽造されない認証がある。

C.3.4 エレメント

468 エレメントの例には、コピーされた認証データの使用の防止に重点を置く FIA_UAU.3.2 がある。

C.4 拡張コンポーネント

C.4.1 拡張コンポーネントを定義する方法

469 PP/ST 作成者が拡張コンポーネントを定義する場合は常に、既存の CC コンポーネントと同様の方法、つまり明確で、曖昧さがなく、評価可能な(そのコンポーネントに基づく要件が TOE に対応するかどうかを系統的に実証することができる)方法で行わなければならない。拡張コンポーネントは、既存の CC コンポーネントと同様のラベル付け、表現方法、及び詳細レベルを使用しなければならない。

470 PP/ST 作成者は、拡張コンポーネントの定義に拡張コンポーネントのすべての適用可能な依存性が含まれることも確認しなければならない。依存性の例は次のとおりである:

- a) 拡張コンポーネントが監査を参照する場合、FAU クラスのコンポーネントに対する依存性を含まなければならないことがある;
- b) 拡張コンポーネントがデータを改変、またはデータにアクセスする場合、FDP_ACC ファミリのコンポーネントに対する依存性を含まなければならないことがある;
- c) 拡張コンポーネントが特定の設計記述を使用する場合、適切な ADV ファミリ(機能仕様など)に対する依存性を含まなければならないことがある。

471 拡張機能コンポーネントの場合、PP/ST 作成者は、既存の CC パート2 コンポーネントと同様に、そのコンポーネントの定義に適用可能な監査及び管理の情報も含まなければならない。拡張保証コンポーネントの場合、PP/ST 作成者は、CEM で規定される方法と同様に、コンポーネントに適切な方法も規定しなければならない。

操作のためのガイダンス(参考)

- 472 拡張コンポーネントは、既存のファミリに配置することができる。この場合、PP/ST 作成者は、これらのファミリがどのように変更されるかを示さなければならない。拡張コンポーネントが既存のファミリに適合しない場合は、新しいファミリに配置しなければならない。新しいファミリは、CC と同様に定義しなければならない。
- 473 新しいファミリは、既存のクラスに配置することができる。この場合、PP/ST 作成者は、これらのクラスがどのように変更されるかを示さなければならない。新しいファミリが既存のクラスに適合しない場合は、新しいクラスに配置しなければならない。新しいクラスは、CC と同様に定義しなければならない。

附属書D PP 適合(参考)

D.1 序説

- 474 PP は、ST の「テンプレート」として使用されることを意図している。つまり、PP は利用者のニーズのセットを記述し、その PP に適合する ST はこれらのニーズを満たす TOE を記述する。
- 475 PP は、別の PP のテンプレートとしても使用できることに注意のこと。つまり、PP は他の PP への適合を主張することができる。この場合は、ST と PP の場合とまったく同様である。明確にするために、この附属書では ST/PP の場合のみを記述するが、この記述は PP/PP の場合にも当てはまる。
- 476 CC では、部分的な適合は認められない。もし、PP が主張するならば、PP または ST は、ひとつ、あるいは複数の参照 PP に完全に適合しなければならない。しかし、2種類の適合(「正確適合」と「論証適合」)があり、許可される適合の種別は、PP によって決定される。つまり、PP は、次のように(PP 適合ステートメントで)ST に対して許可される適合の種別を記載する(B.5 節を参照のこと)。この正確適合と論証適合の識別は、ST が個別の基準で適合主張してもよい各 PP に適用される。つまり、ST は一部の PP に対して正確適合し、その他の PP に対して論証適合する場合がある。ST が常にどんな PP にも正確適合できるのに対して、PP が明示的に許可している場合にも、ST は論証可能な方法で PP に適合することが許可される。
- 477 言い換えれば、PP が明示的に許可している場合にも、ST は論証可能な方法で PP に適合することが許可される。
- 478 PP 適合とは、PP または ST が(ST が評価された製品に対するものであるならば、その製品も同様に)、PP のすべての要件を満たすことを意味する。
- 479 公開されている PP は通常は論証適合を要求している。これは、PP 適合を主張する ST は、PP で記述される一般的なセキュリティ課題に対する解決策を提供しなければならないが、PP で記述されるものと同様かより制限的であれば、どのような方法でも提供することができることを意味する。「同等またはより制限的」については、CC で詳細に定義されるが、ST が TOE に対して同等かそれ以上の制限を課し、TOE の運用環境に対して同等かそれ以下の制限を課すならば、原則、PP と ST は異なるエンティティの記述、異なる概念の使用など、まったく異なるステートメントを含んでもよいことを意味する。

D.2 正確適合

- 480 正確適合は、PP の要件が満たされ、ST の範囲は PP よりも広いことがあるが、ST がその PP の具体化であることの証拠を要求する PP 作成者を対象としている。要するに、ST は、TOE が PP 記載の TOE と同等以上のことを実行し、その運用環境が PP 記載の運用環境と同等以下のことを実施することを特定する。
- 481 正確適合が使用される典型的な例は、製品のセキュリティ要件が PP で規定されているものに正確に合っていることが期待される、選択ベースの調達においてである。
- 482 PP に正確適合するように作成された ST は、PP に記載されている制限に対して追加の制限を記述することもできる。

D.3 論証適合

- 483 論証適合は、ST が PP で記述される一般的なセキュリティ課題に対する適切な解決策であることの証拠を要求する PP の作成者を対象としている。
- 484 正確適合では PP と ST の間に明確なサブセット/スーパーセットタイプの関係がある一方で、論証適合ではこの関係はあまり明確ではなくなる。PP 適合を主張する ST は、PP における一般的なセキュリティ課題に対する解決策を提供しなければならない。しかし、PP で記述されているものと同様かより制限的であれば、どのような方法でも提供することができる。

附属書E 参考文献(参考)

485 この参考文献に、CC の読者に有用となり得る参照と標準を含む。日付のない参照については、読者は参照文書の最新版を参照することを薦める。

E.1 ISO / IEC 標準とガイダンス

- | | |
|-----------------|---|
| [ISO/IEC 15292] | Information technology -- Security techniques -- Protection Profile registration procedures |
| [ISO/IEC 15443] | Information technology -- Security techniques -- A framework for IT security assurance - all parts |
| [ISO/IEC 15446] | Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets |
| [ISO/IEC 19790] | Information technology -- Security techniques -- Security requirements for cryptographic modules |
| [ISO/IEC 19791] | Information technology -- Security techniques -- Security assessment of operational systems |
| [ISO/IEC 27001] | Information technology -- Security techniques -- Information security management systems -- Requirements |
| [ISO/IEC 27002] | Information technology -- Security techniques -- Code of practice for information security management |

E.2 その他の標準とガイダンス

- | | |
|------------------------|---|
| [IEEE Std 610.12-1990] | Institute of Electrical and Electronics Engineers, Standard Glossary of Software Engineering Terminology |
| [CC portal] | Common Criteria portal, February 2009. CCRA, www.commoncriteriaportal.org |