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 5: セキュリティ要件の定義済みパッケージ

2022 年 11 月

CC:2022
改訂第 1 版

CCMB-2022-11-005

令和 5 年 9 月 翻訳第 1.0 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
セキュリティ技術評価部

目次

IPA まえがき

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

Part5: Pre-defined packages of security requirements CC:2022 Revision 1

November 2022 CCMB-2022-11-005

まえがき

本バージョンは、2017 年に CC v3.1 改訂第 5 版として発行されて以来、最初の大幅改訂となる「情報技術セキュリティ評価のためのコモンクライテリア」(CC:2022)である。

歴史的に、CC 標準は共通評価方法(CEM)とともに、IT セキュリティ分野におけるコモンクライテリア認証書の承認に関する協定(CCRA)の参加国によって開発・維持され、その後、ISO(国際標準化機構)及び IEC(国際電気標準会議)が維持する標準として公表されてきた。しかし、CC:2022 と CEM:2022 は、まず ISO/IEC 標準として開発され、その後、CCRA により CC と CEM の新バージョンとして発行されたものである。CC:2022 の ISO 版は ISO/IEC 15408-1:2022～15408-5:2022 として 5 パートで発行され、CEM:2022 の ISO 版は ISO/IEC 18045:2022 として 1 パートで発行されている。

CC:2022 は、以下のパートから構成されている。

— 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

— パート4（新規）：評価方法及び評価アクティビティの仕様のための枠組み

— パート5(新規)：セキュリティ要件の定義済みパッケージ

CC:2022 は、CC v3.1 が発行されて以来用いられてきた標準の新しい使用方法を、正式に規定することを目的としている。CC v3.1 が発行されて以来、新しい保証パラダイムが開発され、附属書や補遺として標準に追加されてきた。これには、評価が適合主張の範囲を超えることを禁止する完全適合の概念や、個々のセキュリティ機能を評価するために、評価アクティビティを使用して、機能に特化した保証や客観性のあるガイドラインを提供するという概念が含まれる。また、標準の前回の大幅な改訂以降、重要性が増した機能要件の形式化も含まれている。CC:2022 の発行は、これらの開発を標準そのものに完全に統合する。

CC:2022 には、新しい ISO/IEC 15408:2022 標準の編集中に提供されたパート 4 とパート 5 が CC の新しいオリジナルパートとして含まれていることを強調する価値がある。これらは、旧版 CC v3.1 R5 を大幅に強化する。パート 5 は、CC v.3.1 改訂第 5 版のパート 3 の関連する節に基づいている。

CC:2022 は、次のような具体的な変更点を取り入れている。

— 文書が再構成され、新たなパートが追加された。

  — パート4：評価方法及び評価アクティビティの仕様の方法を定義している。

  — パート5：事前に定義された保証パッケージを列挙したもので、このバージョンで新たに導入されたものもある。

— 以下の技術的な変更が導入された。

  — 用語が見直され、更新された。

— 新しい機能要件及び新しい保証要件が導入された。

— 完全適合の種別が導入された。

— 低保証のプロテクションプロファイル(PP)が削除され、直接根拠PPが導入された。

— マルチ保証評価が導入された。

— 保証の統合が導入された。

CCの全てのパートはCommon Criteria Portal (www.commoncriteriaportal.org)で見ることができる。

本書で使用されている商標は、利用者の便宜を図るための参考情報であり、推奨を意味するものではない。

法定通知

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は、以下に示す政府機関が貢献した。ISO/IEC とともに、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 2022 パート 1 からパート 5(「CC:2022」と呼ぶ)の著作権の共同保有者として、これらの政府機関はここに、ISO/IEC 15408 及びその派生版(それらの国での採用を含む)の改訂版において ISO/IEC に CC:2022 を複製する非排他的許可を与える。ただし、CC:2022 を適切な方法で使用、複製、配布、翻訳、変更する権利は、これらの政府機関が保有する。ISO/IEC はその見返りとして、前述の政府機関に対し、成果物である CC:2022 パート 1 からパート 5 を、彼らが適切と考えるライセンスで使用することを許可する。前述の政府機関は、文書の一部分の修正や再利用を含め、文書の利用者がテキストを再利用することを常に支援しており、今後もこの方針に従う予定である。

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

序説

この文書は、セキュリティ要件の定義済みパッケージを提供する。このようなセキュリティ要件は、評価の整合性を図る上で利害関係者にとって有益である。また、セキュリティ要件のパッケージ化により、プロテクションプロファイル(PP)やセキュリティターゲット(ST)の開発の手間も軽減できる。

CC パート 1 で、パッケージという用語を定義し、基本的な概念を説明している。

注：この文書では、用語を他のテキストと区別するために、ボールドやイタリック体を使用している場合がある。ファミリ内のコンポーネント間の関係は、ボールド表記を用いて強調表示される。この表記では、全ての新しい要件をボールドで表示する必要がある。階層型のコンポーネントでは、前のコンポーネントの要件を超えて強化又は変更されたとき、要件がボールドで表示される。また、前のコンポーネントを超えて許可される新しい操作又は拡張操作も、ボールドで強調表示される。

イタリック体の使用は、正確な意味を持つテキストであることを示す。セキュリティ保証要件では、この表記は評価に関連する特別な動詞に使用される。

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 5：セキュリティ要件の定義済みパッケージ

1 適用範囲

この文書は、関係者の共通利用を支援するために有用であることが確認されたセキュリティ保証要件とセキュリティ機能要件のパッケージを提供する。

例：保証パッケージの例には、評価保証レベル(EAL)や統合保証レベル(CAP)がある。

この文書は以下を提示する。

— *評価保証レベル(EAL)*ファミリは、PP や ST で参照され、評価対象(TOE)の評価中に提供されるべき適切なセキュリティ保証を規定する、セキュリティ保証コンポーネントの事前に定義されたセットを指定するパッケージのファミリである。

— *統合保証(CAP)*ファミリは、統合 TOE の評価中に提供されるべき適切なセキュリティ保証を指定するために使用される、セキュリティ保証コンポーネントのセットを指定するパッケージのファミリである。

— *コンポジット製品(COMP)*パッケージは、コンポジット製品の TOE の評価時に適切なセキュリティ保証を規定するために使用される一連のセキュリティ保証コンポーネントを指定するパッケージである。

— *プロテクションプロファイル保証(PPA)*ファミリは、プロテクションプロファイル評価時に提供する適切なセキュリティ保証の指定に使用される、一連のセキュリティ保証コンポーネントを指定するパッケージのファミリである。

— *セキュリティターゲット保証(STA)*ファミリは、セキュリティターゲット評価時に提供する適切なセキュリティ保証の指定に使用される、一連のセキュリティ保証コンポーネントを指定するパッケージのファミリである。

この文書の利用者には、セキュアな IT 製品の消費者、開発者、評価者が含まれる。

2 規定の参照

以下の文書は、その内容の一部又は全部がこの文書の要求事項となるように本文中で参照されている。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。

情報技術セキュリティ評価のためのコモンクライテリア、CC:2022、改訂第1版、2022年11月 — パート1：概説と一般モデル

情報技術セキュリティ評価のためのコモンクライテリア、CC:2022、改訂第1版、2022年11月 — パート3：セキュリティ保証コンポーネント

3 用語と定義

本文書の目的のために、CC パート 1 及び CC パート 3 で使用された用語、定義、及び略語を適用する。

ISO と IEC は、標準化で使用する用語データベースを以下のアドレスで管理している。

— ISO Online browsing platform: https://www.iso.org/obp

— IEC Electropedia: https://www.electropedia.org/

4 評価保証レベル

4.1 ファミリ名

このパッケージのファミリ名は「評価保証レベル(EAL)」である。

4.2 評価保証レベルの概要

4.2.1 一般

EAL は、得られる保証のレベルと、そのレベルの保証を得るためのコスト及び可能性とを比較考量する段階的な尺度を提供する。CC パート 1 のアプローチは、評価終了時における TOE の保証の概念と、TOE が運用されている間のその保証の維持の概念を区別して識別している。

注：CC パート 3 のファミリとコンポーネントが、必ずしも全て EAL に含まれない。これは、これらが有意義な望ましい保証を提供しないことを意味するものではない。これらのファミリとコンポーネントは、それらが有用性を提供するプロテクションプロファイル(PP)やセキュリティターゲット(ST)の EAL の追加として考慮されることが期待される。さらに、CC パート 3 にあるいくつかのクラスは、EAL には関係ない。その例として、APE クラスや ACO クラスがある。

各 EAL には、保証コンポーネントのセットが選択されている。

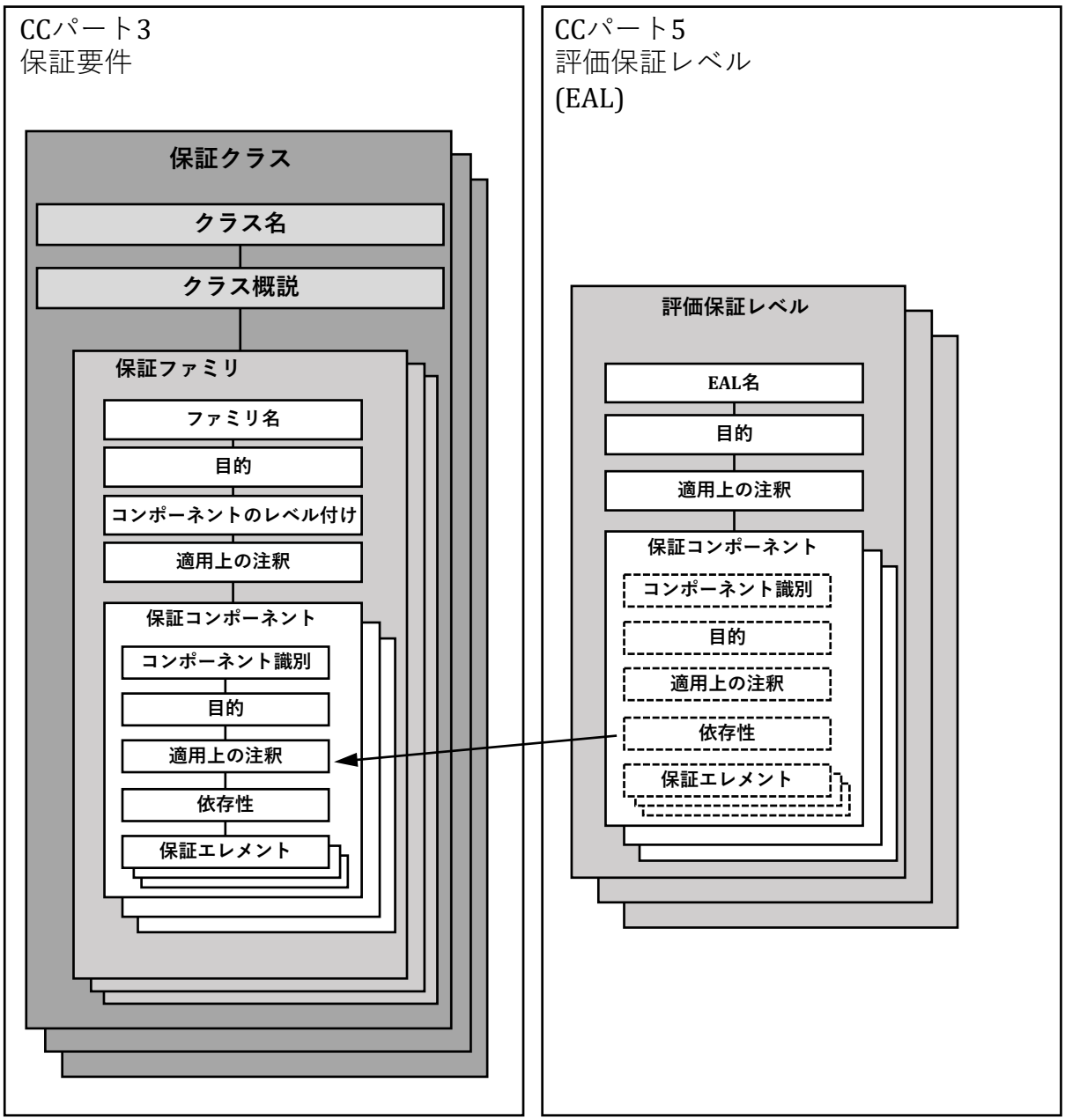
与えられた EAL により提供されているものより上位の保証レベルは、以下のことにより達成させることができる。

a) 他の保証ファミリから追加の保証コンポーネントを取り込む。又は、

b) 保証コンポーネントを同じ保証ファミリの上位レベルの保証コンポーネントで置き換える。

4.2.2 保証と保証レベルの関係

図 1 は、CC パート 3 に定義されているセキュリティ保証要件(SAR)とこの文書に定義されている保証レベルの関係を示す。保証コンポーネントはさらに保証エレメントに分解されるが、保証エレメントを保証レベルによって個々に参照することはできない。



注：図の矢印は、EAL からクラス内で定義されている保証コンポーネントへの参照を表す。

図 1 — 保証と保証レベルの関連

表 1 は、EAL の要約を示している。列は、階層的に並べられた EAL のセットを表し、行は保証ファミリを表す。その結果として得られるマトリックスの各数字は、適用すべき特定の保証コンポーネントを識別している。

グレーで表示されている項目は、EAL では適用されない。しかし、EAL のパッケージへ追加するために使用することができる。

注：表 1 には ALC_FLR、ALC_TDA ファミリを示していないが、EAL への追加としてよく使用される。

表 1 — 評価保証レベルの要約

保証クラス	保証ファミリ	評価保証レベル別の保証コンポーネント						
		EAL1	**EAL2**	**EAL3**	**EAL4**	**EAL5**	**EAL6**	**EAL7**
開発	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
ガイダンス文書	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
ライフサイクルサポート	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
ST評価	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
テスト	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
脆弱性評定	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

4.3 評価保証レベルの目的

4.4 に概説されているように、階層的に並べられた 7 つの評価保証レベルが、TOE の保証のレート付けのためにこの文書に定義されている。それらは、各 EAL がそれより下位の全ての EAL よりも多くの保証を表すため、階層的に並べられている。EAL から EAL への保証の増加は、同じ保証ファミリから階層的に上位の保証コンポーネントへの置換(つまり、厳格性、適用範囲、及び/又は深さを拡大する)及び他の保証ファミリからの保証コンポーネントの追加(つまり、新しい要件を追加する)によって達成される。

これらの EAL は、CC パート 3 に記述されている保証コンポーネントの適切な組み合わせからなる。さらに正確には、各 EAL は各保証ファミリから 1 つ以下のコンポーネントを取り込んでおり、あらゆるコンポーネントの全ての保証依存性を扱っている。

「追加」(augmentation)の概念によって、(EAL にまだ取り込まれていない保証ファミリからの)EAL に対する保証コンポーネントの追加、又は(同じ保証ファミリで階層的に上位の他の保証コンポーネントによる)保証コンポーネントの置換が許可される。CC パート 1 に定義されている保証構造において、EAL は要件を追加されることのみが可能である。「その構成する保証コンポーネントを欠いた EAL」の概念は、有効な主張として CC パート 1 では認められない。追加に伴って、EAL に追加された保証コンポーネントの有効性と付加価値を正当化する義務が主張者の側に課せられる。EAL には、拡張された保証要件を追加することもできる。

注：PP への完全適合を主張する ST に含まれる EAL には追加できない。

4.4 評価保証レベル

4.4.1 一般

この項では EAL を定義する。その際、特定の要件とそれらの要件の一律的な特性との差異を、ボールド体を用いて強調する。

4.4.2 評価保証レベル 1(EAL1) — 機能テスト

4.4.2.1 パッケージ名

パッケージ名は、評価保証レベル 1(EAL1) — 機能テストである。

4.4.2.2 パッケージ種別

これは、保証パッケージである。

4.4.2.3 パッケージ概要

EAL1 は、正しい運用についてある程度の信頼が要求されるが、セキュリティへの脅威が重大とみなされない場合に適用される。個人情報又は同様の情報の保護に関して当然の配慮がなされているとの論旨をサポートするために、独立の保証が要求されるところで価値がある。

EAL1 は、限定された ST のみを必要とする。TOE に要求されるセキュリティ機能要件(SFR)を単に記述すれば十分であり、脅威、組織のセキュリティ方針(OSP)、及び前提条件からセキュリティ対策方針を通して SFR を導き出す必要はない。

EAL1 は、仕様に対する独立テスト、提供されたガイダンス証拠資料の検査など、顧客が入手できる TOE の評価を提供する。EAL1 評価は、TOE の開発者の支援を受けずに、最小の費用で実施できるように意図されている。

このレベルの評価は、TOE の機能がその証拠資料に対していわば一貫しているという証拠を提供する。

4.4.2.4 パッケージの目的

EAL1 は、限定された ST とその ST 内の SFR の分析により基本レベルの保証を提供する。この分析は、ST のふるまいを理解するために、機能とインタフェースの仕様及びガイダンス証拠資料を使用して行われる。

分析は、公知の潜在的な脆弱性の探索及び TSF の独立テスト(機能及び侵入)によってサポートされる。

また EAL1 は、TOE 及び関連する評価文書の一意の識別情報を通して保証を提供する。

この EAL は、評価されていない IT に比べ、有意義な保証の増加を提供する。[i]

4.4.2.5　保証コンポーネント

表 2 は、EAL1 に含まれる保証コンポーネントを示したものである。

表 2 — EAL1

保証クラス	保証コンポーネント
ADV: 開発	ADV_FSP.1 基本機能仕様
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.1 TOEのラベル付け
	ALC_CMS.1 TOEのCM範囲
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.1 運用環境のセキュリティ対策方針
	ASE_REQ.1 主張されたセキュリティ要件
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_IND.1 独立テスト - 適合
AVA: 脆弱性評定	AVA_VAN.1 脆弱性調査

4.4.3　評価保証レベル 2(EAL2) — 構造テスト

4.4.3.1　パッケージ名

パッケージ名は、評価保証レベル 2(EAL2) — 構造テストである。

4.4.3.2　パッケージ種別

これは、保証パッケージである。

4.4.3.3　パッケージ概要

EAL2 は、設計情報とテスト結果の提供に関して開発者の協力を必要とする。ただし、正常な商業的習慣を越える労力を開発者側に要求するべきではない。したがって、コスト又は時間の投資の大幅な増加を要求するべきではない。

そこで、EAL2 は、開発者又は利用者が完全な開発記録を簡単に使用できない場合に、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必要とする環境に適用できる。そのような状況は、レガシーシステムの安全性を高めるとき、又は開発者へのアクセスが制限されるところで生じる。

4.4.3.4 目的

EAL2 は、**完全な** ST 及びその ST 内の SFR の分析により保証を提供する。この分析は、セキュリティのふるまいを理解するために、機能とインタフェースの仕様、ガイダンス証拠資料、**及び TOE のアーキテクチャの基本的な記述**を使用して行われる。

分析は、TSF の独立テスト、**機能仕様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で独立した確認、及び基本的な攻撃能力を持つ侵入攻撃者に対する抵抗力を実証する(提供された機能仕様、TOE 設計、セキュリティアーキテクチャ記述、及びガイダンス証拠に基づく)脆弱性分析**によってサポートされる。

また、**EAL2** は、**構成管理システムの使用**と**セキュアな配付手続きの証拠**を通して保証を提供する。

この EAL は、**開発者テスト、(公知の脆弱性の探索に加えて)脆弱性分析、さらに詳細な TOE 仕様に基づく独立テストを要求することにより、EAL1 からの**有意義な保証の増加を**表す**。

4.4.3.5 保証コンポーネント

表 3 は、EAL2 に含まれる保証コンポーネントを示したものである。

表 3 — EAL2

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.2 セキュリティ実施機能仕様
	ADV_TDS.1 基本設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.2 CMシステムの使用
	ALC_CMS.2 TOEの一部のCM範囲
	ALC_DEL.1 配付手続き
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_COV.1 カバレージの証拠
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.2 脆弱性分析

4.4.4 評価保証レベル 3(EAL3) — 方式テスト、及びチェック

4.4.4.1 パッケージ名

パッケージ名は、評価保証レベル 3(EAL3) — 方式テスト、及びチェックである。

4.4.4.2 パッケージ種別

これは、保証パッケージである。

4.4.4.3 パッケージ概要

EAL3 は、良心的な開発者が、既存の適切な開発方法を大幅に変更することなく、設計段階で有効なセキュリティエンジニアリングから最大の保証を得られるようにする。

EAL3 は、開発者又は利用者が、中レベルで独立して保証されたセキュリティを必要とし、大幅なリエンジニアリングを行わずに TOE とその開発の完全な調査を必要とする状況で適用される。

4.4.4.4 目的

EAL3 は、完全なセキュリティターゲット及びその ST 内の SFR の分析により保証を提供する。この分析は、セキュリティのふるまいを理解するために、機能とインタフェースの仕様、ガイダンス証拠資料、及び TOE の**設計**の**アーキテクチャ記述**を使用して行われる。

分析は、TSF の独立テスト、機能仕様**及び TOE 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で独立した確認、及び基本的な攻撃能力を持つ侵入攻撃者に対する抵抗力を実証する(提供された機能仕様、TOE 設計、セキュリティアーキテクチャ記述、及びガイダンス証拠に基づく)脆弱性分析によってサポートされる。

また、**EAL3** は、**開発環境管理**の使用、**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保証を提供する。

この EAL は、**セキュリティ機能性**の**さらに完全な**テスト**カバレージ**、及び **TOE が開発中に改ざんされないというある程度の信頼を提供するメカニズム及び/又は手続き**を要求することにより、**EAL2** からの有意義な保証の増加を表す。

4.4.4.5 保証コンポーネント

表 4 は、EAL3 に含まれる保証コンポーネントを示したものである。

表 4 — EAL3

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.3 完全な要約を伴う機能仕様
	ADV_TDS.2 アーキテクチャ設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.3 許可の管理
	ALC_CMS.3 実装表現のCM範囲
	ALC_DEL.1 配付手続き

保証クラス	保証コンポーネント
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト：基本設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.2 脆弱性分析

4.4.5 評価保証レベル 4(EAL4) — 方式設計、テスト、及びレビュー

4.4.5.1 パッケージ名

パッケージ名は、評価保証レベル 4(EAL4) — 方式設計、テスト、及びレビューである。

4.4.5.2 パッケージ種別

これは、保証パッケージである。

4.4.5.3 パッケージ概要

EAL4 は、厳格ではあるが、多大な専門知識、スキル、及びその他の資源を必要としない正常な商業的開発習慣に基づいて、有効なセキュリティエンジニアリングから最大の保証を開発者が得られるようにする。EAL4 は、既存の製品ラインへのレトロフィットが経済的に実現可能であると思われる最上位レベルである。

そこで、EAL4 は、開発者又は利用者が従来の商品としての TOE に独立して保証された中レベルから高レベルのセキュリティを必要とし、セキュリティ特有のエンジニアリングコストを追加で負担する用意ができている状況で適用される。

4.4.5.4 目的

EAL4 は、完全な ST 及びその ST 内の SFR の分析により保証を提供する。この分析は、セキュリティのふるまいを理解するために、機能と**完全な**インタフェースの仕様、ガイダンス証拠資料、TOE の**基本モジュール**設計の記述、及び**実装のサブセット**を使用して行われる。

分析は、TSF の独立テスト、機能仕様及び TOE 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で独立した確認、及び**強化基本的な**攻撃能力を持つ侵入攻撃者に対する抵抗力を実証する(提供された機能仕様、TOE 設計、**実装表現**、セキュリティアーキテクチャ記述、及びガイダンス証拠に基づく)脆弱性分析によってサポートされる。

また、**EAL4** は、開発環境管理の使用、**自動化を含む追加の** 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保証を提供する。

この EAL は、さらに多くの**設計記述**、**TSF 全体に対する実装表現**、及び TOE が開発中に改ざんされないという信頼を提供する**向上した**メカニズム及び/又は手順を要求することにより、**EAL3** からの有意義な保証の増加を表す。

4.4.5.5 保証コンポーネント

表 5 は、EAL4 に含まれる保証コンポーネントを示したものである。

表 5 — EAL4

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.4 完全な機能仕様
	ADV_IMP.1 TSFの実装表現
	ADV_TDS.3 基本モジュール設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.4 製造サポート、受入れ手続き、及び自動化
	ALC_CMS.4 問題追跡のCM範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
	ALC_TAT.1 明確に定義された開発ツール
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト：基本設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.3 焦点を置いた脆弱性分析

4.4.6 評価保証レベル 5(EAL5) — 準形式的設計、及びテスト

4.4.6.1 パッケージ名

パッケージ名は、評価保証レベル 5(EAL5) — 準形式的設計、及びテストである。

4.4.6.2 パッケージ種別

これは、保証パッケージである。

4.4.6.3 パッケージ概要

EAL5 は、専門的なセキュリティエンジニアリング技法を中程度に適用することによりサポートされる厳格な商業的開発習慣に基づいて、セキュリティエンジニアリングから最大の保証を開発者が得られるようにする。そのような TOE は、おそらく EAL5 保証を達成する意図を持って設計され、開発される。専門的な技法を適用しない厳格な開発と比較して、EAL5 要件による追加のコストは、大きくはないと思われる。

そこで、EAL5 は、開発者又は利用者が計画された開発において独立して保証される高レベルのセキュリティを必要とし、専門的なセキュリティエンジニアリング技法による非合理的なコストを負担することのない厳格な開発アプローチを必要とする状況で適用される。

4.4.6.4 目的

EAL5 は、完全な ST 及びその ST 内の SFR の分析により保証を提供する。この分析は、セキュリティのふるまいを理解するために、機能と完全なインタフェースの仕様、ガイダンス証拠資料、TOE の設計の記述、及び実装を使用して行われる。**また、モジュール化された TSF 設計も必要となる。**

分析は、TSF の独立テスト、機能仕様に基づく開発者テストの証拠、TOE 設計、開発者テスト結果の選択的で独立した確認、及び**中程度の**攻撃能力を持つ侵入攻撃者に対する抵抗力を実証する**独立した**脆弱性分析によってサポートされる。

また、**EAL5** は、開発環境管理の使用、自動化を含む**包括的な** 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保証を提供する。

この EAL は、**準形式的設計記述**、さらに**構造化された(それによって分析可能な)アーキテクチャ**、及び開発中に TOE が改ざんされないという信頼を提供する向上したメカニズム及び/又は手続きを要求することにより、**EAL4** からの有意義な保証の増加を表す。

4.4.6.5 保証コンポーネント

表 6 は、EAL5 に含まれる保証コンポーネントを示したものである。

表 6 — EAL5

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.5 追加の誤り情報を伴う完全な準形式的機能仕様
	ADV_IMP.1 TSFの実装表現
	ADV_INT.2 適切に構成された内部構造
	ADV_TDS.4 準形式的モジュール設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス

保証クラス	保証コンポーネント
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.4 製造サポート、受入れ手続き、及び自動化
	ALC_CMS.5 開発ツールのCM範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
	ALC_TAT.2 実装標準への準拠
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.3 テスト: モジュール設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.4 系統的脆弱性分析

4.4.7 評価保証レベル 6(EAL6) — 準形式的検証済み設計、及びテスト

4.4.7.1 パッケージ名

パッケージ名は、評価保証レベル 6(EAL6) — 準形式的検証済み設計、及びテストである。

4.4.7.2 パッケージ種別

これは、保証パッケージである。

4.4.7.3 パッケージ概要

EAL6 は、重大なリスクに対して価値の高い資産を保護するためのプレミアム TOE を作り出すために、セキュリティエンジニアリング技法の厳格な開発環境への適用から、高い保証を開発者が得られるようにする。

そこで、EAL6 は、保護される資産の価値が追加コストを正当化するリスクの高い状況で適用するセキュリティ TOE の開発に適用される。

4.4.7.4 目的

EAL6 は、完全な ST 及びその ST 内の SFR の分析により保証を提供する。この分析は、セキュリティのふるまいを理解するために、機能と完全なインタフェースの仕様、ガイダンス証拠資料、TOE の設計、及び実装を使用して行われる。**追加の保証が、選択された TOE セキ**

ュリティ方針の形式的モデル、及び機能仕様と TOE 設計の準形式的表現を通して得られる。モジュール化され、**階層化された、簡潔な** TSF 設計も必要となる。

分析は、TSF の独立テスト、機能仕様に基づく開発者テストの証拠、TOE 設計、開発者テスト結果の選択的で独立した確認、及び**高い**攻撃能力を持つ侵入攻撃者に対する抵抗力を実証する独立した脆弱性分析によってサポートされる。

また、**EAL6** は、**構造化された**開発プロセスの使用、**開発**環境管理の使用、**完全な**自動化を含む包括的 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保証を提供する。

この EAL は、**さらなる包括的分析**、**実装の構造化された表現**、さらなる**アーキテクチャ構造(例えば階層化)**、**さらに包括的な独立した脆弱性分析**、及び向上した**構成管理**と開発**環境管理**を要求することにより、**EAL5** からの有意義な保証の増加を表す。

4.4.7.5 保証コンポーネント

表 7 は、EAL6 に含まれる保証コンポーネントを示したものである。

表 7 — EAL6

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.5 追加の誤り情報を伴う完全な準形式的機能仕様
	ADV_IMP.2 TSFの実装表現の完全なマッピング
	ADV_INT.3 最小限複雑な内部構造
	ADV_SPM.1 形式的なTOEセキュリティ方針モデル
	ADV_TDS.5 完全な準形式的モジュール設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.5 進んだサポート
	ALC_CMS.5 開発ツールのCM範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.2 セキュリティ手段の十分性
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
	ALC_TAT.3 実装標準への準拠 - 全ての部分
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_COV.3 カバレージの厳格な分析

保証クラス	保証コンポーネント
	ATE_DPT.3 テスト: モジュール設計
	ATE_FUN.2 順序付けられた機能テスト
	ATE_IND.2 独立テスト - サンプル
AVA: 脆弱性評定	AVA_VAN.5 高度な系統的脆弱性分析

4.4.8 評価保証レベル 7(EAL7) — 形式的検証済み設計、及びテスト

4.4.8.1 パッケージ名

パッケージ名は、評価保証レベル 7(EAL7) — 形式的検証済み設計、及びテストである。

4.4.8.2 パッケージ種別

これは、保証パッケージである。

4.4.8.3 パッケージ概要

EAL7 は、リスクが非常に高い状況及び/又は資産の高い価値によってさらに高いコストが正当化されるところで適用するセキュリティ TOE の開発に適用される。現在、EAL7 の実際的な適用は、広範な形式的分析に従うセキュリティ機能性が強く重要視されている TOE に限られる。

4.4.8.4 目的

EAL7 は、完全な ST 及びその ST 内の SFR の分析により保証を提供する。この分析は、セキュリティのふるまいを理解するために、機能と完全なインタフェースの仕様、ガイダンス証拠資料、TOE の設計、及び**構造化された**実装の**提示**を使用して行われる。追加の保証が、選択 TOE セキュリティ方針の形式的モデル、及び機能仕様と TOE 設計の準形式的表現を通して得られる。モジュール化され、階層化された、簡潔な TSF 設計も必要となる。

分析は、TSF の独立テスト、機能仕様に基づく開発者テストの証拠、TOE 設計**と実装表現**、開発者テスト結果の**完全で**独立した確認、及び高い攻撃能力を持つ侵入攻撃者に対する抵抗力を実証する独立した脆弱性分析によってサポートされる。

また、**EAL7** は、構造化開発プロセスの使用、開発環境管理の使用、完全な自動化を含む包括的な 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保証を提供する。

この EAL は、**形式的表現**と**形式的対応**、及び**包括的テストを使用する**さらに包括的な分析を要求することにより、**EAL6** からの有意義な保証の増加を表す。

4.4.8.5 保証コンポーネント

表 8 は、EAL7 に含まれる保証コンポーネントを示したものである。

表 8 — EAL7

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.6 追加の形式的仕様を伴う完全な準形式的機能仕様
	ADV_IMP.2 TSFの実装表現の完全なマッピング

評価保証レベル

保証クラス	保証コンポーネント
	ADV_INT.3 最小限複雑な内部構造
	ADV_SPM.1 形式的なTOEセキュリティ方針モデル
	ADV_TDS.6 形式的な上位レベルの設計提示を伴う完全な準形式的モジュール設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.5 進んだサポート
	ALC_CMS.5 開発ツールのCM範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.2 セキュリティ手段の十分性
	ALC_LCD.2 測定可能なライフサイクルモデル
	ALC_TAT.3 実装標準への準拠 - 全ての部分
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様
ATE: テスト	ATE_COV.3 カバレージの厳格な分析
	ATE_DPT.4 テスト: 実装表現
	ATE_FUN.2 順序付けられた機能テスト
	ATE_IND.3 独立テスト - 完全
AVA: 脆弱性評定	AVA_VAN.5 高度な系統的脆弱性分析

5 統合保証パッケージ(CAP)

5.1 ファミリ名

パッケージのファミリ名は「統合保証パッケージ(CAP)」である。

5.2 統合保証パッケージ(CAP)の概要

5.2.1 一般

CAP の構造は、EAL の構造と似ている。この 2 種類のパッケージの主な違いは、それぞれが適用される TOE の種類にある。EAL はコンポーネント TOE に適用され、CAP は統合 TOE に適用される。

図 2 は、この文書に定義されている CAP 及び関連する構造を示す。

注：図は、保証コンポーネントの内容を示しているが、この情報は、CC パート 3 に定義されている実際のコンポーネントを参照することにより、CAP に含まれていることが意図されている。

一部の依存性は、統合 TOE アクティビティが依存する依存コンポーネントの評価中に実行されるアクティビティを識別する。依存性が依存コンポーネントアクティビティ上にあることが明示的に識別されていない場合、依存性は、統合 TOE の別の評価アクティビティに対するものである。

与えられた CAP により提供されているものより上位の保証レベルは、以下のことにより達成させることができる:

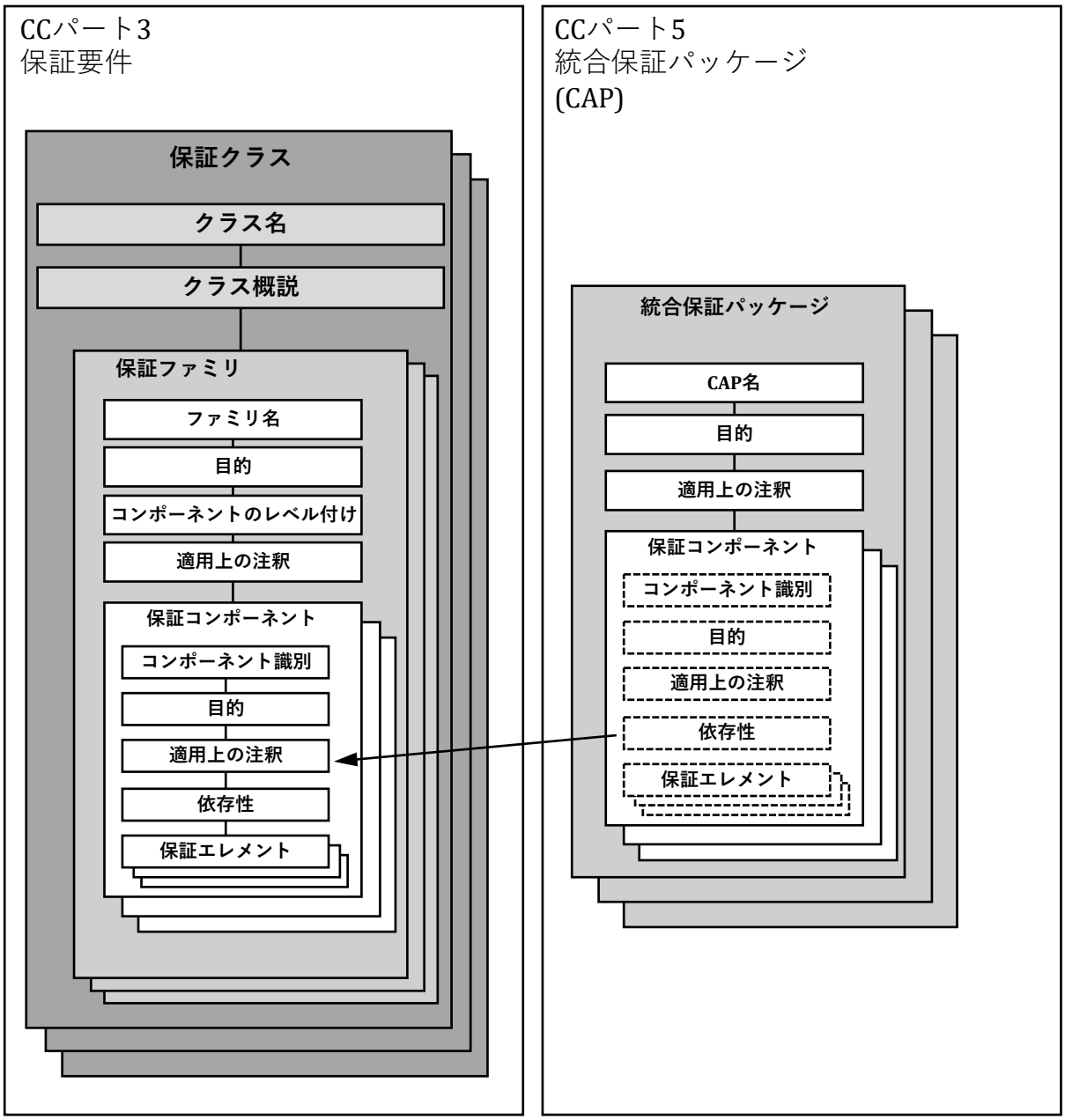
a) 他の保証ファミリから追加の保証コンポーネントを取り込む。又は、

b) 保証コンポーネントを同じ保証ファミリの上位レベルの保証コンポーネントで置き換える。

CAP 保証パッケージに含まれる ACO: 統合コンポーネントは、コンポーネントに対して意味のある保証を提供しないため、コンポーネント TOE 評価に対する追加として使用されてはいけない。

5.2.2 保証と保証パッケージの関係

図 2 は、この文書に定義されている SAR と CAP の関係を示す。保証コンポーネントはさらに保証エレメントに分解されるが、保証エレメントを保証パッケージによって個々に参照することはできない。



注：図の矢印は、クラス内で定義されている保証コンポーネントへの CAP からの参照を表す。

図 2 — 保証及び統合保証パッケージ(CAP)の関連

5.3 統合保証パッケージ(CAP)の目的

CAP は、統合 TOE について、得られる保証のレベルと、そのレベルの保証を得るためのコスト及び可能性とを比較考量する段階的な尺度を提供する。

注：CAP には、CC パート 3 のファミリとコンポーネントが少数しか含まれない。これは、すでに評価されたエンティティ(基本コンポーネントと依存コンポーネント)の評価結果に基づくという CAP の性質によるもので、CAP が有意義な望ましい保証を提供しないことを意味するものではない。

CAP は統合 TOE に適用されなければならない。統合 TOE は、コンポーネント TOE 評価が実施された、もしくは評価中の、コンポーネントで構成される(CC パート 3 附属書 B を参照のこと)。個別のコンポーネントは、EAL、又は ST で特定された別の保証パッケージに対して

認証される。統合 TOE の保証の基本レベルは EAL1 の適用により得られることが期待される。これは、一般的に公知に利用できるコンポーネントについての情報を使用して達成できる(EAL1 は、コンポーネントと統合 TOE の両方に対して、それらの仕様どおりに適用できる)。CAP は、統合 TOE に対して EAL1 より上の EAL を適用するよりも上位のレベルの保証を得る代替アプローチを提供する。

依存コンポーネントは、環境内の IT プラットフォーム要件を満たすために、以前に評価、認証された基本コンポーネントを使用して評価を受けることができるが、これによりコンポーネント間の相互作用の形式的な保証又は統合の結果による脆弱性の持ち込みの可能性は提供されない。CAP は、これらの相互作用を考慮し、より上位レベルの保証で、コンポーネント間のインタフェースそれ自体がテストのサブジェクトとなることを保証する。統合 TOE の脆弱性分析も、コンポーネントを統合した結果として脆弱性が持ち込まれる可能性を考慮して実行される。

表 9 は、CAP の要約を示している。列は、階層的に並べられた CAP のセットを表し、行は保証ファミリを表す。その結果として得られるマトリックスの各数字は、適用すべき特定の保証コンポーネントを識別している。

5.4 に概説されているように、階層的に並べられた 3 つの CAP が、統合 TOE の保証のレート付けのためにこの文書に定義されている。それらは、各 CAP がそれより下位の全ての CAP よりも多くの保証を表すために、階層的に並べられている。CAP から CAP への保証の増加は、同じ保証ファミリから階層的に上位の保証コンポーネントへの置換(つまり、厳格性、適用範囲、及び/又は深さを拡大する)及び他の保証ファミリからの保証コンポーネントの追加(つまり、新しい要件を追加する)によって達成される。このような増加によって、個々のコンポーネント TOE について得られる評価結果への影響を識別できるように、構成の分析が強化される。

これらの CAP は、CC パート 3 の 6 章に記述されている保証コンポーネントの適切な組み合わせからなる。さらに正確には、各 CAP は各保証ファミリから 1 つ以下のコンポーネントを取り込んでおり、あらゆるコンポーネントの全ての保証依存性を扱っている。

CAP では、最高でも強化基本的な攻撃能力を持つ攻撃者に対する抵抗力のみが考慮される。これは、ACO_DEV から提供される設計情報のレベルに起因しており、攻撃能力に関連付けられたいくつかの要因(統合 TOE の知識)を制限し、評価者が実行可能な脆弱性分析の厳格性に影響を与える。したがって、統合 TOE の保証レベルは制限されるが、統合 TOE 内の個別のコンポーネントの保証はかなり高くなる場合がある。

表 9 は、CAP の要約を示している。

表 9 — 統合保証パッケージの要約

保証クラス	保証 ファミリ	統合保証パッケージ別の 保証コンポーネント		
		CAP-A	**CAP-B**	**CAP-C**
統合	ACO_COR	**1**	1	1
	ACO_CTT	**1**	**2**	2
	ACO_DEV	**1**	**2**	**3**
	ACO_REL	**1**	1	**2**
	ACO_VUL	**1**	**2**	**3**
	AGD_OPE	**1**	1	1

ガイダンス文書	AGD_PRE	**1**	1	1
ライフサイクルサポート	ALC_CMC	**1**	1	1
	ALC_CMS	**2**	2	2
セキュリティターゲット評価	ASE_CCL	**1**	1	1
	ASE_ECD	**1**	1	1
	ASE_INT	**1**	1	1
	ASE_OBJ	**1**	**2**	2
	ASE_REQ	**1**	**2**	2
	ASE_SPD		**1**	1
	ASE_TSS	**1**	1	1

5.4 CAP ファミリのパッケージ

5.4.1 統合保証パッケージ A — 構造的統合

5.4.1.1 パッケージ名

パッケージ名は、統合保証パッケージ A — 構造的統合である。

5.4.1.2 パッケージ種別

これは、保証パッケージである。

5.4.1.3 パッケージ概要

CAP-A は、統合 TOE が統合され、その結果である複合物の正しいセキュリティ運用に信頼が要求される場合に適用される。これには、依存コンポーネントからの設計情報とテスト結果の提供に関して依存コンポーネントの開発者に協力を求める必要があるが、基本コンポーネントの開発者の関与は要求されない。

そこで、CAP-A は、開発者又は利用者が完全な開発記録を簡単に使用できない場合に、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必要とする環境に適用される。

5.4.1.4 目的

CAP-A は、統合 TOE の ST の分析によって保証を提供する。統合 TOE の ST 内の SFR は、セキュリティのふるまいを理解するために、コンポーネント TOE の評価からの出力(例えば、ST、ガイダンス証拠資料)及び統合 TOE 内のコンポーネント TOE 間のインタフェースの仕様を使って分析される。

分析は、依存情報に記述されているように依存コンポーネントが信頼する基本コンポーネントのインタフェースの独立テスト、依存情報、開発情報、及び統合の根拠に基づく開発者テストの証拠、及び開発者テスト結果の選択的で独立した確認によってサポートされる。分析は、評価者による統合 TOE の脆弱性レビューによってもサポートされる。

また CAP-A は、統合 TOE の一意の識別情報(つまり、IT TOE とガイダンス証拠資料)を通して保証を提供する。

5.4.1.5 保証コンポーネント

表 10 は、CAP-A に含まれる保証コンポーネントを示したものである。

表 10 — CAP-A

保証クラス	保証コンポーネント
ACO: 統合	ACO_COR.1 統合の根拠
	ACO_CTT.1 インタフェーステスト
	ACO_DEV.1 機能記述
	ACO_REL.1 基本依存情報
	ACO_VUL.1 統合の脆弱性レビュー
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.1 TOEのラベル付け
	ALC_CMS.1 TOEのCM範囲
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.1 運用環境のセキュリティ対策方針
	ASE_REQ.1 主張されたセキュリティ要件
	ASE_TSS.1 TOE要約仕様

5.4.2 統合保証パッケージ B — 方式的統合

5.4.2.1 パッケージ名

パッケージ名は、統合保証パッケージ B — 方式的統合である。

5.4.2.2 パッケージ種別

これは、保証パッケージである。

5.4.2.3 パッケージ概要

CAP-B は、良心的な開発者が、統合 TOE に統合されたコンポーネント TOE 間の相互作用の影響をサブシステムレベルで理解することから最大の保証を得られるようにする一方で、基本コンポーネントの開発者に要求される関与を最小限に抑える。

CAP-B は、開発者又は利用者が、中レベルで独立して保証されたセキュリティを必要とし、大幅なリエンジニアリングを行わずに統合 TOE とその開発の完全な調査を必要とする状況で適用される。

5.4.2.4 目的

CAP-B は、統合 TOE の**完全な** ST の分析によって保証を提供する。統合 TOE の ST 内の SFR は、セキュリティのふるまいを理解するために、コンポーネント TOE の評価からの出力(例えば、ST、ガイダンス証拠資料)、コンポーネント TOE 間のインタフェースの仕様、及び統合**開発情報に含まれている TOE 設計(TSF サブシステムの記述)**を使って分析される。

分析は、依存情報**(TOE 設計も含む)**に記述されているように依存コンポーネントが信頼する基本コンポーネントのインタフェースの独立テスト、依存情報、開発情報、及び統合の根拠に基づく開発者テストの証拠、及び開発者テスト結果の選択的で独立した確認によってサポートされる。分析は、**基本的な攻撃能力を持つ攻撃者に対する抵抗力を実証する**評価者による統合 TOE の脆弱性**分析**によってもサポートされる。

この CAP は、セキュリティ機能性のより完全なテストカバレージを要求することにより、CAP-A からの有意義な保証の増加を表す。

5.4.2.5 保証コンポーネント

表 11 は、CAP-B に含まれる保証コンポーネントを示したものである。

表 11 — CAP-B

保証クラス	保証コンポーネント
ACO: 統合	ACO_COR.1 統合の根拠
	ACO_CTT.2 厳格なインタフェーステスト
	ACO_DEV.2 設計の基本証拠
	ACO_REL.1 基本依存情報
	ACO_VUL.2 統合の脆弱性分析
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.1 TOEのラベル付け
	ALC_CMS.2 TOEの一部のCM範囲
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様

5.4.3 統合保証パッケージ C — 方式的統合、テスト、及びレビュー

5.4.3.1 パッケージ名

パッケージ名は、統合保証パッケージ C — 方式的統合、テスト、及びレビューである。

5.4.3.2 パッケージ種別

これは、保証パッケージである。

5.4.3.3 パッケージ概要

CAP-C は、統合 TOE のコンポーネント間の相互作用の有効な分析(それは厳格ではあるが、基本コンポーネントの全ての評価証拠への完全なアクセスを必要としない)から、開発者が最大の保証を得られるようにする。

そこで、CAP-C は、開発者又は利用者が従来の商品としての統合 TOE に独立して保証された中レベルから高レベルのセキュリティを必要とし、セキュリティ特有のエンジニアリングコストを追加で負担する用意ができている状況で適用される。

5.4.3.4 目的

CAP-C は、統合 TOE の完全な ST の分析によって保証を提供する。統合 TOE の ST 内の SFR は、セキュリティのふるまいを理解するために、コンポーネント TOE の評価からの出力(例えば、ST、ガイダンス証拠資料)、コンポーネント TOE 間のインタフェースの仕様、及び統合開発情報に含まれている TOE 設計(TSF **モジュール**の記述)を使って分析される。

分析は、依存情報(TOE 設計を含む)に記述されているように依存コンポーネントが信頼する基本コンポーネントのインタフェースの独立テスト、依存情報、開発情報、及び統合の根拠に基づく開発者テストの証拠、及び開発者テスト結果の選択的で独立した確認によってサポートされる。分析は、**強化基本的な**攻撃能力を持つ攻撃者に対する抵抗力を実証する評価者による統合 TOE の脆弱性分析によってもサポートされる。

この CAP は、より多くの**設計記述及びより高い攻撃能力に対する抵抗力の実証**を要求することにより、**CAP-B** からの有意義な保証の増加を表す。

5.4.3.5 保証コンポーネント

表 12 は、CAP-C に含まれる保証コンポーネントを示したものである。

表 12 — CAP-C

保証クラス	保証コンポーネント
ACO: 統合	ACO_COR.1 統合の根拠
	ACO_CTT.2 厳格なインタフェーステスト
	ACO_DEV.3 設計の詳細証拠
	ACO_REL.2 依存情報
	ACO_VUL.3 強化基本的な統合の脆弱性分析
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.1 TOEのラベル付け
	ALC_CMS.2 TOEの一部のCM範囲
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 導出されたセキュリティ要件

保証クラス	保証コンポーネント
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE要約仕様

6 コンポジット製品パッケージ

6.1パッケージ名

パッケージ名は、コンポジット製品パッケージ(COMP)である。

6.2パッケージ種別

このパッケージは保証パッケージである。

6.3パッケージ概要

COMP は、コンポジット製品が適切な基準に従って組み立てられ評価されたことを保証する。

6.4 目的

保証コンポーネント*_COMP は、CC パート 1 の 14 章と 14.3.3 に基づくコンポジット評価技法をコンポジット製品に用いる場合に適用する。目的は以下のとおりである。

— CC パート 1 及び CC パート 3 の要件を考慮し、TOE が既に評価済みの基本コンポーネントと依存コンポーネントで構成されていることを確認する。

— コンポジット製品の ST、ライフサイクル要件、設計、テスト及び脆弱性分析の評価が、CC パート 3 に規定された基準に従って実施されていること。

これらの目的は、コンポジット製品の基本コンポーネントと依存コンポーネントの構成に起因する潜在的な矛盾、不整合又はセキュリティギャップが考慮され、存在しないことを保証するものである。

6.5セキュリティ保証コンポーネント

表 13 は、このパッケージに含まれる保証コンポーネントを示したものである。

表 13 — COMP

保証クラス	保証コンポーネント
ASE: セキュリティターゲット評価	ASE_COMP.1 セキュリティの整合性
ADV: 開発	ADV_COMP.1 基本コンポーネント関連の利用者ガイダンス、コンポジット評価のためのETR、基本コンポーネント評価監督機関報告書の設計の適合
ALC: ライフサイクルサポート	ALC_COMP.1 関連基本コンポーネントへの依存コンポーネントの統合及び配付及び受入れ手続きの一貫性チェック
ATE: テスト	ATE_COMP.1 コンポジット製品の機能テスト
AVA: 脆弱性評定	AVA_COMP.1 コンポジット製品の脆弱性評定

7 プロテクションプロファイル保証

7.1 ファミリ名

このパッケージのファミリ名は「プロテクションプロファイル保証パッケージ(PPA)」である。

7.2 PPA ファミリ概要

PPA ファミリは PP 評価のために以下の 2 つの保証パッケージを提供する。

a) 直接根拠 PP の評価のための保証パッケージ

b) 標準の PP の評価のための保証パッケージ

これらの保証パッケージは、CC パート 1 に記述された各タイプの PP の評価で使用されるコンポーネントを提供する。

表 14 は、PPA の要約を示している。列は PPA のセットを表し、行は保証ファミリを表す。その結果として得られるマトリックスの各数字は、適用すべき特定の保証コンポーネントを識別している。

これらの PPA は、CC パート 3 の 7 章に記述されている保証コンポーネントの適切な組み合わせからなる。さらに正確には、各 PPA は各保証ファミリから 1 つ以下のコンポーネントを取り込んでおり、あらゆるコンポーネントの全ての保証依存性を扱っている。

表 14 — PPA の要約

保証クラス	保証ファミリ	プロテクションプロファイル保証パッケージ別の保証コンポーネント	
		プロテクションプロファイル保証パッケージ - 直接根拠(PPA-DR)	プロテクションプロファイル保証パッケージ - 標準(PPA-STD)
PP評価	APE_CCL	**1**	1
	APE_ECD	**1**	1
	APE_INT	**1**	1
	APE_OBJ	**1**	**2**
	APE_REQ	**1**	**2**
	APE_SPD	**1**	1

7.3 PPA ファミリの目的

PPA の目的は、プロテクションプロファイルが CC パート 1 の要件に適合していることを、評価を通じて保証することを支援することである。

7.4 PPA パッケージ

7.4.1 プロテクションプロファイル保証パッケージ — 直接根拠 PP

7.4.1.1 パッケージ名

パッケージ名は、プロテクションプロファイル保証パッケージ — 直接根拠(PPA-DR)である。

7.4.1.2 パッケージ種別

このパッケージは保証パッケージである。

7.4.1.3 パッケージ概要

PPA_DR は、CC パート 3 で規定された基準を用いて、直接根拠プロテクションプロファイルの評価による保証を提供する。

7.4.1.4 目的

PPA-DR は、直接根拠 PP を評価する場合に適用される。直接根拠 PP が CC パート 1 の要件に適合していることを検証するために使用できる。

7.4.1.5 セキュリティ保証コンポーネント

表 15 は、このパッケージに含まれるセキュリティ保証コンポーネントを示したものである。

表 15 — PPA-DR

保証クラス	保証コンポーネント
APE: プロテクションプロファイル評価	APE_INT.1 PP概説
	APE_CCL.1 適合主張
	APE_SPD.1 セキュリティ課題定義
	APE_OBJ.1 運用環境のセキュリティ対策方針
	APE_ECD.1 拡張コンポーネント定義
	APE_REQ.1 主張されたセキュリティ要件

7.4.2 プロテクションプロファイル保証パッケージ — 標準

7.4.2.1 パッケージ名

パッケージ名は、プロテクションプロファイル保証パッケージ — 標準(PPA-STD)である。

7.4.2.2 パッケージ種別

このパッケージは保証パッケージである。

7.4.2.3 パッケージ概要

PPA_STD は、CC パート 3 で規定された基準を用いて、標準的なプロテクションプロファイルの評価による保証を提供する。

7.4.2.4 目的

PPA-STD は、標準的な PP を評価する場合に適用される。標準的な PP が CC パート 1 の要件に適合していることを検証するために使用できる。

7.4.2.5 セキュリティ保証コンポーネント

PPA_STD は、CC パート 1 で規定されている標準的なプロテクションプロファイルの評価による保証を提供する。表 16 は、PPA_STD に含まれる保証コンポーネントを示したものである。

表 16 — PPA-STD

保証クラス	保証コンポーネント
APE: プロテクションプロファイル評価	APE_INT.1 PP概説
	APE_CCL.1 適合主張
	APE_SPD.1 セキュリティ課題定義
	APE_OBJ.2 セキュリティ対策方針
	APE_ECD.1 拡張コンポーネント定義
	APE_REQ.2 導出されたセキュリティ要件

8 セキュリティターゲット保証

8.1ファミリ名

このパッケージのファミリ名は「セキュリティターゲット保証(STA)」である。

8.2STA ファミリ概要

STA ファミリは ST 評価のために以下の 2 つの保証パッケージを提供する。

a) 直接根拠 ST の評価のための保証パッケージ

b) 標準的な ST の評価のための保証パッケージ

これらの保証パッケージは、CC パート 1 に記述された各タイプの ST の評価で使用されるコンポーネントを提供する。

表 17 は、STA の要約を示している。列は、STA のセットを表し、行は保証ファミリを表す。その結果として得られるマトリックスの各数字は、適用すべき特定の保証コンポーネントを識別している。

これらの STA は、CC パート 3 の 9 章に記述されている保証コンポーネントの適切な組み合わせからなる。さらに正確には、各 STA は各保証ファミリから 1 つ以下のコンポーネントを取り込んでおり、あらゆるコンポーネントの全ての保証依存性を扱っている。

表 17 — STA の要約

保証クラス	保証ファミリ	ST保証パッケージ別の保証コンポーネント	
		セキュリティターゲット保証パッケージ - 直接根拠(STA-DR)	セキュリティターゲット保証パッケージ - 標準(STA-STD)
ST評価	ASE_INT	**1**	1
	ASE_CCL	**1**	1
	ASE_SPD	**1**	1
	ASE_OBJ	**1**	**2**
	ASE_ECD	**1**	1
	ASE_REQ	**1**	**2**
	ASE_TSS	**1**	1

8.3STA ファミリの目的

STA の目的は、セキュリティターゲットが CC パート 1 の要件に適合していることを、評価を通じて保証することを支援することである。

8.4 STA パッケージ

8.4.1 セキュリティターゲット保証パッケージ — 直接根拠

8.4.1.1 パッケージ名

パッケージ名は、セキュリティターゲット保証パッケージ — 直接根拠(STA-DR)である。

8.4.1.2 パッケージ種別

このパッケージ保証パッケージである、

8.4.1.3 パッケージ概要

STA-DR は、CC パート 3 で規定された基準を用いて、直接根拠 ST の評価による保証を提供する。

8.4.1.4 目的

STA-DR は、直接根拠 ST を評価する場合に適用される。直接根拠 ST が CC パート 1 の要件に適合していることを検証するために使用できる。

8.4.1.5 セキュリティ保証コンポーネント

表 18 は、このパッケージに含まれるセキュリティ保証コンポーネントを示したものである。

表 18 — STA-DR

保証クラス	保証コンポーネント
ASE: セキュリティターゲット評価	ASE_INT.1 ST概説
	ASE_CCL.1 適合主張
	ASE_SPD.1 セキュリティ課題定義
	ASE_OBJ.1 運用環境のセキュリティ対策方針
	ASE_ECD.1 拡張コンポーネント定義
	ASE_REQ.1 主張されたセキュリティ要件
	ASE_TSS.1 TOE要約仕様

8.4.2 セキュリティターゲット保証パッケージ — 標準

8.4.2.1 パッケージ名

パッケージ名は、セキュリティターゲット保証パッケージ — 標準(STA-STD)である。

8.4.2.2 パッケージ種別

このパッケージは保証パッケージである。

8.4.2.3 パッケージ概要

STA-STD は、CC パート 3 で規定された基準を用いて、標準的な ST の評価による保証を提供する。

8.4.2.4 目的

STA-STD は、標準的な ST を評価する場合に適用される。標準的な ST が CC パート 1 の要件に適合していることを検証するために使用できる。

8.4.2.5 セキュリティ保証コンポーネント

STA-STD は、CC パート 1 で規定されている標準的な ST の評価による保証を提供する。表 19 は、STA-STD に含まれる保証コンポーネントを示したものである。

表 19 — STA-STD

保証クラス	保証コンポーネント
ASE: セキュリティターゲット評価	ASE_INT.1 ST概説
	ASE_CCL.1 適合主張
	ASE_SPD.1 セキュリティ課題定義
	ASE_OBJ.2 セキュリティ対策方針
	ASE_ECD.1 拡張コンポーネント定義
	ASE_REQ.2 導出されたセキュリティ要件
	ASE_TSS.1 TOE要約仕様

[i] 【訳注】4.4.2.4 の最後の文について、原文では直前の文が繰り返し記述されており、CC v3.1 改訂第 5 版にあったこの一文が削除されている。