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

2022 年 11 月

CC:2022
改訂第 1 版

CCMB-2022-11-001

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

Part1: Introduction and general model CC:2022 Revision 1

November 2022 CCMB-2022-11-001

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

CCは、IT製品のセキュリティ機能性、及びセキュリティ評価時にIT製品に適用される保証手段に対する共通要件のセットを提供することにより、独立したセキュリティ評価の結果間の比較を可能にする。当該IT製品は、ハードウェア、ファームウェア、又はソフトウェアに実装されることがある。

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、消費者がこれらのIT製品がセキュリティのニーズを満たしているかどうかを判断するのに役立つと考えられる。

CCは、セキュリティ機能性を有するIT製品の開発、評価及び/又は調達のための指針として役立つ。

CCは意図的に柔軟性を持たせており、幅広いIT製品の様々なセキュリティ特性に対して、様々な評価手法を適用することが可能である。したがって、この規格の利用者は、この柔軟性が誤使用されないように注意する必要がある。例えば、CCを不適切な評価方法/評価アクティビティ、無関係なセキュリティ特性、不適切なIT製品とともに用いると、無意味な評価結果をもたらす可能性がある。

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。

CCが扱うのは、許可されない暴露、改変、又は使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、これら3つのカテゴリ以外のITセキュリティの側面にも適用してもよい。CCは、(悪意がある又はその他の)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。CCは、ITの他の分野でも適用可能だが、これらの分野での適用可能性を主張するものではない。

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又はサポートできると認められる。

b) 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。

注1：基準方法については、CEMで定義されている。CCのパート4は、CEMから評価アクティビティと評価方法をさらに導き出すために使用することができる。

c) CCでは、評価監督機関が基準を適用するための管理上・法律上の枠組みは扱わない。しかし、そのような枠組みの中で、評価を目的としてCCを用いることが期待される。

d) 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部分の全てを含めて、十分な運用環境におけるIT製品(又はその集合)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評定には、他の技法の方がより適しているため、認定者(accreditor)はこれらの側面に対して別個に備えるべきである。

e) 暗号化アルゴリズム固有の品質評定のための基準は、CCでは対象とされない。暗号の数学的特性について独立した評定が必要な場合は、CCが適用される評価制度において、そのような評定について規定しなければならない。

注2：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1：概説と一般モデル

1　適用範囲

本書は、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基礎として使用される、規格の各所で提示される評価の一般モデルを規定する。

本書は、CCの全パートの概要を説明する。CCの各パートについて記述し、標準の全てのパートで使用される用語と略語を定義し、評価対象(TOE)の中核概念を確立し、評価の枠組みを記述し、評価基準が向けられる対象読者を記述する。IT製品の評価に必要な基本的なセキュリティ概念について紹介している。

本書では、以下を紹介する。

— プロテクションプロファイル(PP)、PPモジュール、PP構成、パッケージ、セキュリティターゲット(ST)及び適合種別の主要概念

— モデル全体を通してのセキュリティコンポーネントの構成についての記述

— CCパート2及びCCパート3に記載されている機能及び保証コンポーネントを、許可された操作によって調整することができる様々な操作

— CEMに記載されている評価方法に関する一般的な情報

— CEMから派生した評価方法(EM)及び評価アクティビティ(EA)を開発するために、CCパート4を適用するためのガイダンス

— CCパート5で事前に定義された評価保証レベル(EAL)についての一般情報

— 評価制度の適用範囲に関する情報

2 規定の参照

本書の適用には、以下の参考文献が不可欠である。日付のある文献については、引用された版のみが適用される。日付のない文献については、参照した文書の最新版(改訂を含む)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2：セキュリティ機能コンポーネント

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

情報技術セキュリティ評価のための共通方法、CEM:2022、改訂第1版、2022年11月 — 評価方法論

ISO/IEC IEEE 24765, *システム及びソフトウェアエンジニアリング — 用語集*

3　用語と定義

本書の目的には、CC パート 2、CC パート 3、CEM、ISO24765、及び以下に示す用語及び定義が適用される。

ISO 及び IEC は、標準化で使用する用語データベースを次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/

ボールド体で表示されている用語は、それ自体が本節で定義されている。

3.1
アクション (action)
評価者(3.45)又は*開発者*(3.33)のアクティビティを文書化したもの。

注 1：評価者アクションと開発者アクションは、CC パート 3 で要求される。

3.2
管理者 (administrator)
TOE セキュリティ機能性(TSF)(3.92)によって実装される全ての方針に関して信頼レベルを有する*エンティティ*(3.36)。

注1：全ての*プロテクションプロファイル(PP)*(3.68)やセキュリティターゲット(ST)が、管理者に対して同じレベルの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*評価対象(TOE)*(3.90)のSTの方針を常に遵守することが想定される。これらの方針の中には、TOEの機能性に関連するものもあれば、*運用環境*(3.63)に関連するものもある。

3.3
有害なアクション (adverse action)
脅威エージェント(3.91)が*資産*(3.4)に対して行う*アクション*(3.1)

3.4
資産 (asset)
評価対象(TOE)(3.90)の所有者がおそらく価値を置く*エンティティ*(3.36)

3.5
割付 (assignment)
機能又は保証コンポーネントにおいて識別されたパラメタの仕様

3.6
保証 (assurance)
評価対象(TOE)(3.90)が*セキュリティ機能要件(SFR)*(3.78)を満たしていると確信できる根拠

3.7
保証パッケージ (assurance package)
セキュリティ保証要件(3.76)の名前付きセット

例：「EAL3」

3.8
攻撃能力 (attack potential)
評価対象(TOE)(3.90)の脆弱性を突くために必要な労力の指標

注1：この労力は、攻撃者に関連する特性(専門知識、資源、動機など)と脆弱性自体に関連する特性(機会の窓、暴露までの時間など)の関数として表現される。

3.9
攻撃対象領域 (attack surface)
ターゲット及びその機能へのアクセスを試みることができるポイントから構成される、ターゲットへの論理的又は物理的インタフェースのセット

例1：支払端末の筐体は、そのデバイスの物理的な攻撃対象領域の一部である。

例2：ネットワークデバイスへの接続に利用可能な通信プロトコルは、そのネットワークデバイスの論理攻撃対象領域の一部である。

3.10
追加 (augmentation)
1つ以上の要件をパッケージに追加すること。

注1：*機能パッケージ*(3.51)の場合、このような追加は1つのパッケージの文脈でのみ考慮され、他のパッケージ又は*プロテクションプロファイル(PP)*(3.68)もしくは*セキュリティターゲット(ST)*(3.82)との枠組みでは考慮されない。

注2：*保証パッケージ*(3.7)の場合、追加とは、1つ以上の*セキュリティ保証要件(SAR)*(3.76)を指す。

3.11
許可利用者 (authorized user)
セキュリティ機能要件(SFR)(3.78)に従い、*評価対象(TOE)*(3.90)に対して操作を行うことができる*エンティティ*(3.36)

3.12
基本コンポーネント (base component)
1つ以上の*依存コンポーネント*(3.31)にサービスや資源を提供する、マルチコンポーネント製品における独立した*エンティティ*(3.36)

注1：特に「*統合TOE*」(3.21)及び「コンポジット製品/*コンポジットTOE*」(3.25)に適用される。

3.13
基本プロテクションプロファイル (base Protection Profile)
基本PP(base PP)
PP構成(3.69)を構築するための基礎として使用される、*PPモジュール*(3.71)の*PPモジュール基盤*(3.72)の一部として、PPモジュールで指定された*プロテクションプロファイル*(3.68)

3.14
基本PPモジュール(base PP-Module)
別のPPモジュールで指定された*PPモジュール*(3.71)で、そのPPモジュールの*PPモジュール基盤*(3.72)の一部として、*PP構成*(3.69)を構築するための基礎として使用される

注1：PPモジュールで基本PPモジュールを指定すると、基本PPモジュールのPPモジュール基盤を暗黙のうちに含む。

3.15
基本評価対象 (base target of evaluation)
基本TOE(base TOE)
それ自体が評価の対象である、*基本コンポーネント*(3.12)

注1：特に「*統合TOE*」(3.21)及び「コンポジット製品/*コンポジットTOE*」(3.25)に適用される。

3.16
クラス (class)
〈分類〉 共通の関心事項を持つファミリのグループ

注 1：クラスは、セキュリティ機能性クラスを定義するパート 2 とセキュリティ保証クラスを定義するパート 3 でさらに定義される。

3.17
コンポーネント (component)
〈分類〉 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

3.18
コンポーネント (component)
〈統合〉 製品内で資源及びサービスを提供する*エンティティ*(3.36)

3.19
コンポーネント評価対象 (component target of evaluation)
コンポーネントTOE(component TOE)
他の*統合TOE*(3.21)のコンポーネントとなる(評価済みの)*評価対象(TOE)*(3.90)

3.20
統合保証パッケージ (composed assurance package)
CAP
事前に定義された統合保証の尺度の一点を表す、主にACO *クラス*(3.16)から抽出されたコンポーネントで構成される*保証パッケージ*(3.7)

3.21
統合評価対象 (composed target of evaluation)
統合TOE(composed TOE)

TOEセキュリティ機能性(TSF)(3.92)の間にセキュリティ関係を有する2つ以上の別々に識別されたコンポーネントのみからなる*評価対象(TOE)*(3.90)

注1：個別に識別された各コンポーネントは、それ自体がTOEである。

3.22
統合評価 (composed evaluation)
統合TOEに適用される特定の評価技法を用いた*統合TOE*(3.21)の評価

注1：この評価技法は、CCパート3で定義されているACO保証*クラス*(3.16)を参照している。

3.23
コンポジット評価 (composite evaluation)
特定のコンポジット評価技法を用いた*コンポジットTOE/製品*(3.25)の評価

注1：この評価技法は、ADV、ALC、ASE、ATE、AVA*クラス*(3.16)に対してCCパート3で規定されているCOMP関連保証ファミリを参照している。

3.24
コンポジット製品 (composite product)
評価済みの*基本コンポーネント(基本TOE)*(3.15)と*依存コンポーネント*(3.31)の2階層で構成される2つ以上のコンポーネントからなる製品。

3.25
コンポジット評価対象 (composite target of evaluation)
コンポジットTOE(composite TOE)
基本TOE(3.15)と*依存コンポーネント*(3.31)を含む*コンポジット製品*(3.24)の一部

注1：コンポジットTOEにおける依存コンポーネントは、1つ以上の依存コンポーネントから構成することができる。簡略化のため、それらは「1つの依存コンポーネント」とみなされる。

注2：コンポジットTOEは、*基本コンポーネント*(3.12)又は基本TOEからそれぞれ独立したパートを含むことができる。簡略化のため、そのようなパートは依存コンポーネントに属するとみなされる。

注3：*コンポジット評価*(3.23)は、インクリメンタルアプローチで、多コンポーネント/多階層化製品に必要なだけ適用することができる。

3.26
構成管理 (configuration management)
CM
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、指定された要件への適合を検証する。

[出典：ISO/IEC IEE 24765:2017, 3.779 1]

3.27
構成管理システム (configuration management system)
開発者(3.33)が、製品のライフサイクルにおいて、その製品の構成を開発し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)

注1：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。

3.28
対抗する (counter)、動詞
脅威を根絶又は軽減するための、特定の脅威に対する行動又は対応

3.29
論証適合 (demonstrable conformance)
DC
PP/STがPP/PP構成の汎用セキュリティ課題を解決する同等又はより制限的な解決策を提供する、*プロテクションプロファイル(PP)*(3.68)/*セキュリティターゲット*(3.82)(PP/ST)とPP、又はSTと*PP構成*(3.69)間との関係

3.30
依存性 (dependency)
コンポーネントを含む*プロテクションプロファイル(PP)*(3.68)、*セキュリティターゲット(ST)*(3.82)、*機能パッケージ*(3.51)又は*保証パッケージ*(3.7)が、依存すると識別されている他のコンポーネントを含む、又はそうではない理由となる根拠を含む、コンポーネント間の関係

3.31
依存コンポーネント (dependent component)
1つ以上の*基本コンポーネント*(3.12)によるサービス及び資源の提供に依存するマルチコンポーネント製品における*依存エンティティ*(3.36)

注1：特に*「統合TOE」*(3.21)及び「コンポジット製品/*コンポジットTOE*」(3.25)に適用される。

3.32
依存評価対象 (dependent target of evaluation)
依存TOE(dependent TOE)
それ自体が評価の対象である*依存コンポーネント*(3.31)

注1：これは*「統合TOE」*(3.21)にのみ適用され、「コンポジット製品/*コンポジットTOE*」(3.25)には適用されない。

3.33
開発者 (developer)
評価対象(TOE)(3.90)の開発責任を有する組織

3.34

直接根拠 (direct rationale)
セキュリティ課題定義(SPD)(3.80)エレメントが、*セキュリティ機能要件(SFR)*(3.78)及び場合によっては*運用環境*(3.63)に対応する*セキュリティ対策方針*(3.79)に直接マッピングされた、*プロテクションプロファイル*(3.68)、*PPモジュール*(3.71)又は*セキュリティターゲット*(3.82)の一種

注1：直接根拠には、*評価対象(TOE)*(3.90)のセキュリティ対策方針は含まれない。

3.35
エレメント (element)
〈分類〉 *セキュリティ保証要件(SAR)*(3.76)又は*セキュリティ機能要件(SFR)*(3.78)に割付されたセキュリティニーズの自己完結した記述

3.36
エンティティ (entity)
特性のセット又は集合によって記述される、識別可能な項目

注1：エンティティには、被験者、利用者(外部のIT製品を含む)、オブジェクト、情報、セション及び/又は資源が含まれる。

3.37
評価 (evaluation)
PP構成(3.69)、*プロテクションプロファイル(PP)*(3.68)、*セキュリティターゲット(ST)*(3.82)又は*評価対象(TOE)*(3.90)を、定義されている基準に照らして審査すること

3.38
評価アクティビティ (evaluation activity)
EA
1つ以上のワークユニットから派生したアクティビティ

注 1：ワークユニットは CEM で定義されている。

注2：派生メカニズムは、CCパート4で定義されている。

3.39
評価保証レベル (evaluation assurance level)
EAL
事前に定義された保証尺度のポイントを表す、*セキュリティ保証要件*(3.76)の形式的なパッケージ

注 1：EAL は CC パート 5 で定義されている。

3.40
評価監督機関 (evaluation authority)
評価制度(3.42)を運用している団体

注1：評価制度を適用することにより、評価監督機関は標準を設定し、特定のコミュニティ内の機関が実施する評価の質を監視する。

3.41
評価方法 (evaluation method)
EM
特定のコンテキストに適用するための1つ以上の*評価アクティビティ*(3.38)のセット

3.42
評価制度 (evaluation scheme)
IT製品セキュリティの評価を行うためのルール、手順及び管理

注1：評価制度は、CCの全てのパートを実装する。

3.43
評価報告書 (evaluation technical report)
ETR
評価者(3.45)が作成し、*評価監督機関*(3.40)に提出する*総合判定*(3.66)とその正当化の文書

3.44
コンポジット評価用の評価報告書 (evaluation technical report for composite evaluation)
コンポジット評価用のETR (ETR for composite evaluation)
ETR_COMP
基本コンポーネント(3.12)の*評価者*(3.45)が、評価した基本コンポーネントの*評価報告書(ETR)*(3.43)から作成した、*コンポジット評価*(3.23)アプローチで使用することを目的とした文書

注1：コンポジット評価用のETRは、基本コンポーネントとその評価に属するものであり、コンポジット評価手法を用いる場合、当該基本コンポーネントを有するコンポジット製品の評価に使用される。

注2：基本コンポーネントに関連するコンポジット評価用のETRは、すでに評価された当該基本コンポーネントを統合したコンポジット製品のコンポジット評価に必要な情報を提供するために設定されるものである。これにより、コンポジット製品*評価者*(3.45)及び各コンポジット製品*評価監督機関*(3.40)は、基本コンポーネントについて検討・実施された攻撃経路及びテスト、並びに基本コンポーネントが実施した対抗策の有効性を理解できる。

3.45
評価者 (evaluator)
与えられた評価基準及び関連する評価方法に従って評価を行うために割り当てられた個人

注1：評価標準の例として、CEMに示された関連する評価方法を持つCCがある。

[出典：ISO/IEC 19896-1:2018, 3.5]

3.46
完全適合 (exact conformance)
EC
STの全ての要件がPP/PP構成のみから抽出されている、*プロテクションプロファイル(PP)*(3.68)又は*PP構成*(3.69)と*セキュリティターゲット(ST)*(3.82)の間の階層的関係

注1：STは、1つ以上のPPへの完全適合を主張することができるが、1つのPP構成へのみ適合することが許される。

3.47
悪用可能脆弱性 (exploitable vulnerability)
TOEの*運用環境*(3.63)において*セキュリティ機能要件(SFR)*(3.78)の侵害に利用可能な、*評価対象(TOE)*(3.90)の弱点

3.48
拡張セキュリティ要件 (extended security requirement)
CCのどのパートにも記載されていない、本書のルールに従って開発されたセキュリティ要件

注1：拡張セキュリティ要件は、CCパート2に記載された形式と構文を保持する。

注2：拡張セキュリティ要件は、*セキュリティターゲット(ST)*(3.82)、*プロテクションプロファイル(PP)*(3.68)又は*PPモジュール*(3.71)の作成者が定義することができる。

3.49
外部エンティティ (external entity)
利用者 (user)
TOE境界の外から*評価対象(TOE)*(3.90)と相互作用する、人間の技術システム又はそのコンポーネントの1つ

3.50
ファミリ (family)
〈分類〉 同様の目的を共有するが、重点や厳密さが異なるコンポーネントのセット

3.51
機能パッケージ (functional package)
セキュリティ課題定義(SPD)(3.80)及びSPDから導き出された*セキュリティ対策方針*(3.79)を伴うことがある、*セキュリティ機能要件*(3.78)の名前付きセット

3.52
グローバル保証パッケージ (global assurance package)
マルチ保証評価(3.60)において、*評価対象(TOE)*(3.90)全体に適用される*保証パッケージ*(3.7)

注1：グローバル保証パッケージは拡張保証コンポーネントを含むことができる。

3.53
ガイダンス文書 (guidance documentation)
評価対象(TOE)(3.90)の配付、準備、運用、管理及び/又は使用を記述した文書

3.54
実装表現 (implementation representation)

TOE セキュリティ機能性(TSF)(3.92)の最も抽象度の低い表現で、特に、さらなる設計の*詳細化*(3.73)なしにTSF自体を作成するために使用されるもの

注1：後にコンパイルされるソースコードや、実際のハードウェアを構築するために使用されるハードウェア図面は、実装表現の一部の例である。

3.55
内部的に一貫した(形容詞) (internally consistent, adj.)
エンティティ(3.36)の各側面間に明らかな矛盾が存在しないこと

注1：証拠資料に関しては、文書内に互いに矛盾するとみなされるようなステートメントがないことを意味する。

3.56
解釈 (interpretation)
標準又は評価制度要件の明確化又は補強

3.57
繰返し (iteration)
同じコンポーネントで2つ以上の異なる要件を表現すること

3.58
階層化 (layering)
コンポーネントの個別のグループが階層的に構成され、それぞれ独立した依存性を持つことで、あるコンポーネントがその階層より下のコンポーネントにサービスを依存し、その上のコンポーネントにサービスを提供する設計技法

3.59
モジュール (module)
ユニットの実装に適したレベルで規定されたアーキテクチャ・ユニット

注1：*評価対象(TOE)*(3.90)のモジュールへの分割に関連するプロパティは、CCパート3、ADV_TDS及びADV_INTファミリで説明する。

3.60
マルチ保証評価 (multi-assurance evaluation)
各PP構成コンポーネントがそれ自身の保証要件のセットと関連付いている*PP構成*(3.68)を用いた、*評価対象(TOE)*(3.90)の評価

注1：PP構成コンポーネントのうち少なくとも1つは、他のコンポーネントと異なる保証要件を含む。

3.61
オブジェクト (object)
情報を含む、又は受け取り、サブジェクトが操作を行う、*評価対象(TOE)*(3.90)内の*エンティティ*(3.36)

3.62
操作 (operation)
〈オブジェクトに対して〉オブジェクトに対してサブジェクトが行う特定の種別の*アクション*(3.1)

3.63
運用環境 (operational environment)
TOE境界の外にある全てのものから構成される、*評価対象(TOE)*(3.90)が運用される環境

3.64
オプションのセキュリティ機能要件 (optional Security Functional Requirement)
オプションのSFR(optional SFR)
PPのセキュリティ課題の記述の記載された側面に寄与するものの、適合PP又は適合*セキュリティターゲット(ST)*(3.82)のSFRのリストに含めることは必須ではない、*プロテクションプロファイル(PP)*(3.68)、*機能パッケージ*(3.51)、*PPモジュール*(3.71)の*セキュリティ機能要件(SFR)*(3.78)

注1：オプションのSFRは、PP、機能パッケージ、PPモジュール本体に記載された適切な*セキュリティ課題定義(SPD)*(3.80)エレメントの脅威及び/又は組織のセキュリティ方針(OSP)を扱うことができ、また、(オプションのSFRによってのみ対処されるという点で)それ自体がオプションである関連するSPDエレメント/対策方針を参照することもできる。

3.65
組織のセキュリティ方針 (organizational security policy)
OSP
組織に対するセキュリティ規則、手続き、又はガイドラインのセット

注1：方針は、特定の*運用環境*(3.63)に関連することができる。

3.66
総合判定 (overall verdict)
評価者(3.45)が評価結果に関して発行したステートメント

注1：ステートメントは、「合格(pass)」又は「不合格(fail)」で表現される。

3.67
潜在的脆弱性 (potential vulnerability)
疑われるが、確認されていない弱点

注1：疑いは、*セキュリティ機能要件(SFR)*(3.78)を侵害するような仮定される攻撃経路より生じる。

3.68
プロテクションプロファイル (Protection Profile)
PP
評価対象(TOE)(3.90)種別のセキュリティニーズの実装に依存しないステートメント

3.69
プロテクションプロファイル構成 (Protection Profile Configuration)

PP構成(PP-Configuration)
少なくとも1つの *プロテクションプロファイル(PP)*(3.68)と、追加の空でないPPと*PPモジュール*(3.71)(関連するPPモジュール基盤も含む)のセットを含む、*評価対象(TOE)*(3.90)種別のセキュリティニーズの実装に依存しないステートメント

3.70
プロテクションプロファイル構成コンポーネント (Protection Profile Configuration component)
PP構成コンポーネント (PP-Configuration component)
PP構成(3.69)に含まれる *プロテクションプロファイル(PP)*(3.68)又は*PPモジュール*(3.71)

3.71
プロテクションプロファイルモジュール (Protection Profile module)
PPモジュール(PP-Module)
1つ以上の基本*プロテクションプロファイル*(3.68)及び場合によってはいくつかの*基本PPモジュール*(3.14)を補完する、*評価対象(TOE)*(3.90)種別のセキュリティニーズの実装に依存しないステートメント

3.72
プロテクションプロファイルモジュール基盤 (Protection Profile Module Base)
PPモジュール基盤 (PP-Module Base)
PP構成(3.69)を構築するための基礎としてPPモジュールが指定する、*PPモジュール*(3.71)、*プロテクションプロファイル(PP)*(3.68)、又はその両方のセット

注1：PPモジュール基盤の概念は、あるPPモジュールの基盤が、それ自身の基盤を持つ別のPPモジュールを含むことができ、その基盤がPPモジュールを含むという点で反復的である。しかし、この「連鎖」は、PPだけを基盤に持つPPモジュールで終了する。

3.73
詳細化 (refinement)
セキュリティコンポーネントに詳細を追加すること

3.74
残存脆弱性 (residual vulnerability)
評価対象(TOE)(3.90)の*運用環境*(3.63)では悪用できないが、TOEの運用環境で想定されるよりも大きな*攻撃能力*(3.8)を持つ攻撃者が*セキュリティ機能要件(SFR)*(3.78)の侵害に利用できるような弱点

3.75
役割 (role)
利用者と*評価対象(TOE)*(3.90)の間で許可される相互作用を確立する、規則の事前に定義されたセット

3.76
セキュリティ保証要件 (security assurance requirement)
SAR

評価対象(TOE)(3.90)の開発・配付のための条件やプロセス及び、それらの条件やプロセスから生み出される証拠に関して*評価者*(3.45)に求められる*アクション*(3.1)に言及するセキュリティ要件

3.77
セキュリティ属性 (security attribute)
セキュリティ機能要件(SFR)(3.78)を定義する際に使用され、その値がSFRを実施する際に使用される、対象者、利用者、オブジェクト、情報、セション及び/又は資源の特性

注1：利用者は、外部のIT製品を含めることができる。

3.78
セキュリティ機能要件 (security functional requirement)
SFR
特定の*セキュリティターゲット(ST)*(3.82)又は*プロテクションプロファイル(PP)*(3.68)で定義される、*評価対象(TOE)*(3.90)の*セキュリティ課題定義(SPD)*(3.80)の充足に寄与するセキュリティ要件

注1：セキュリティ機能要件は、*直接根拠*(3.34)モデルのように直接対応することも、一般モデルのようにTOEの*セキュリティ対策方針*(3.79)を通じて間接的に対応することもできる。

3.79
セキュリティ対策方針 (security objective)
識別された*脅威*に*対抗する*(3.28)こと、及び/又は識別された組織のセキュリティ方針及び/又は前提条件を満たすことを目的とするステートメント

3.80
セキュリティ課題 (security problem)
セキュリティ課題定義 (security problem definition)
SPD
評価対象(TOE)(3.90)が対処しようとするセキュリティの特性や範囲を形式的に定義したステートメント

注1：このステートメントは、TOE及びその運用環境が対抗すべき*脅威*(3.63)、TOE及びその運用環境が実施する組織のセキュリティ方針(OSP)、TOEの運用環境について充足される前提条件の組み合わせで構成される。

注2：SPDエレメントには、脅威、OSP及び前提条件が含まれる。

3.81
セキュリティ要件 (security requirement)
特定の*セキュリティターゲット(ST)*(3.82)又は*プロテクションプロファイル(PP)*(3.68)で定義される、*評価対象(TOE)*(3.90)のセキュリティ仕様の一部となる要件

注1：要件は、CCで規定された言語、すなわち形式及び構文で記述される。

3.82
セキュリティターゲット (Security Target)
ST

セキュリティ課題定義(3.80)に基づく、*評価対象(TOE)*(3.90)のセキュリティ要件の実装依存のステートメント

3.83
選択 (selection)
コンポーネント内のリストから1つ以上の項目を特定すること

3.84
選択ベースのセキュリティ機能要件 (selection-based security functional requirement)
選択ベースのSFR(selection-based SFR)
PP/PPモジュール/機能パッケージで識別された選択肢が関連を示す場合に、適合PP又はSTに含まれるべきPP、PPモジュール、又は機能パッケージの*セキュリティ課題定義*(3.80)の主張された側面に寄与する、*プロテクションプロファイル(PP)*(3.78)、*PPモジュール*(3.71)、又は*機能パッケージ*(3.51)の*セキュリティ機能要件(SFR)*(3.78)

3.85
単一保証評価 (single-assurance evaluation)
1組の保証要件で行う*評価対象(TOE)*(3.90)の評価

3.86
正確適合 (strict conformance)
SC
PPの全ての要件はPP/STにも存在する、*プロテクションプロファイル(PP)*(3.68)とPP/*セキュリティターゲット(ST)*(3.82)の間の階層的関係

注1：この関係は、「STは、PPにある全てのステートメントを含むが、それ以上のステートメントを含むことができる」と言い換えることができる。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。

3.87
サブTOEセキュリティ機能性 (sub-TOE security functionality)
サブTSF (sub-TSF)
1つの*PP構成*(3.69)コンポーネントに定義されたセキュリティ機能要件(SFR)を正しく実施するために信頼される、*評価対象(TOE)*(3.90)の全てのハードウェア、ソフトウェア、ファームウェアの複合機能性

注1：このSFRのセットは、PP構成コンポーネントの依存性、方針、*セキュリティ課題定義(SPD)*(3.80)エレメントによって閉じられる。

注2：サブTSFの概念は、PP構成及び適合セキュリティターゲット(ST)の仕様と評価に関連して適用される。単一保証アプローチでは使用できるが、マルチ保証アプローチでは使用しなければならない。つまりサブTSFは、マルチ保証PP構成及び適合マルチ保証STで定義されなければならない。

注3：各サブTSFは、マルチ保証PP構成/STのセキュリティ保証要件(SAR)と関連付けられる。この文書の他の部分では、SARのセットは*保証パッケージ*(3.7)になり得る。

注4：サブTSFはTSFの特性を有する。

3.88
サブジェクト (subject)
評価対象(TOE)(3.90)において、オブジェクトに対して操作を行う*エンティティ*(3.36)

3.89
調整 (tailoring)
機能パッケージ(3.51)への1つ以上の機能要件の追加、及び/又は、機能パッケージの*セキュリティ機能要件(SFR)*(3.78)への1つ以上の選択の追加

注1：このような調整は、1つのパッケージの文脈でのみ考慮され、他のパッケージ、*プロテクションプロファイル(PP)*(3.68)、又はPPモジュールとの文脈では考慮されない。

注2：SFRの選択項目は、追加選択項目で置き換えることができる。

注3：選択項目は、PP又はPPモジュールによって主張されるパッケージに対してのみ追加することができる。STは、パッケージ名調整のパッケージ適合を主張することはできない。

3.90
評価対象 (target of evaluation)
TOE
評価対象である、ガイダンスを伴う可能性のあるソフトウェア、ファームウェア及び/又はハードウェアのセット

3.91
脅威エージェント (threat agent)
評価対象(TOE)(3.90)が保護する*資産*(3.4)に対して有害な*アクション*(3.3)を行使する可能性がある*エンティティ*(3.36)

3.92
TOEセキュリティ機能性 (TOE security functionality)
TSF
セキュリティ機能要件(SFR)(3.78)を正しく実施するために信頼される*評価対象(TOE)*(3.90)の全てのハードウェア、ソフトウェア、ファームウェアの複合機能性

3.93
TOE種別 (TOE type)
評価対象(TOE)(3.90)のグループに共通する特性のセット

注1：TOE種別は、*プロテクションプロファイル(PP)*(3.68)において、より明確に定義することができる。

3.94
書き換え (translation)
標準化された言語でセキュリティ要件を記述するプロセス

注1：この文脈での書き換え(translation)という用語の使用は、文字通りの意味ではなく、標準化された言語で表現された全ての*セキュリティ機能要件(SFR)*(3.78)を*セキュリティ対策方針*(3.79)に戻すこともできることを意味するものではない。

3.95
脆弱性 (vulnerability)
何らかの環境で*セキュリティ機能要件(SFR)*(3.78)の侵害に利用できる、*評価対象(TOE)*(3.90)の弱点

4 略語

AP	保証パッケージ (assurance package)
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 (composition assurance package)
CD	コンパクトディスク (compact disk)
CM	構成管理 (configuration management)
COMP	コンポジット製品保証パッケージ (composite product assurance package)
DAC	任意アクセス制御 (discretionary access control)
DC	論証適合 (demonstrable conformance)
DPA	差動電力解析 (differential power analysis)
DRBG	決定論的ランダムビット生成器 (deterministic random bit generator)
EA	評価アクティビティ (evaluation activity)
EAL	評価保証レベル (evaluation assurance level)
EC	完全適合 (exact conformance)
EM	評価方法 (evaluation method)
EMS	電磁スペクトル (electromagnetic spectrum)
ETR	評価報告書 (evaluation technical report)
GAP	グローバル保証パッケージ (global assurance package)
GB	ギガバイト (gigabyte)
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)
HSM	ハードウェアセキュリティモジュール (hardware security module)
HTTPS	ハイパーテキストトランスファープロトコルセキュア (hypertext transfer protocol secure)
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)
IPsec	IPセキュリティ (IP security (protocol))
IT	情報技術 (information technology)

LDAP	ライトウェイトディレクトリアクセスプロトコル (lightweight directory access protocol)
MAC	必須アクセス制御 (mandatory access control)
MB	メガバイト (megabyte)
MBps	メガバイト/秒 (megabytes per second)
OR	所見報告書 (observation report)
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 (organizational security policy)
OTP	ワンタイムプログラマブル (one-time programmable)
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)
PPA	プロテクションプロファイル保証パッケージ (protection profile assurance package)
RAM	ランダムアクセスメモリ (random access memory)
RBG	ランダムビット生成器 (random bit generator)
RNG	乱数生成器 (random number generator)
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)
SC	正確適合 (strict conformance)
SFP	セキュリティ機能方針 (security function policies)
SFR	セキュリティ機能要件 (security functional requirement)
SPA	単純電力解析 (simple power analysis)
SPD	セキュリティ課題定義 (security problem definition)
SSH	セキュアシェル (secure shell)
ST	セキュリティターゲット (security target)
STA	セキュリティターゲット保証パッケージ (security target assurance package)
TCP	伝送制御プロトコル (transmission control protocol)
TLS	トランスポートレイヤーセキュリティ (transport layer security)
TOE	評価対象 (target of evaluation)

TSF	TOEセキュリティ機能性 (TOE security functionality)
TSFI	TSFインタフェース (TSF interface)
USB	ユニバーサルシリアルバス (universal serial bus)
VPN	仮想プライベートネットワーク (virtual private network)

5 概要

5.1 一般

この章では、CCの主な概念を紹介する。評価対象(TOE)の概念、CCの対象読者、CCにおける資料を提示するためのアプローチを明らかにする。

5.2 CC 記述

5.2.1 一般

CCは、以下に示すように、異なるが関連性のあるパートのセットとして提示される。

a) **CCパート1「概説と一般モデル」**は、CCの導入部分である。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) **CCパート2「セキュリティ機能コンポーネント」**は、TOEのセキュリティ機能要件(SFR)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では、セキュリティ機能コンポーネントのセットをカタログ化し、ファミリ及びクラスを編成している。

c) **CCパート3「セキュリティ保証コンポーネント」**は、TOEのセキュリティ保証要件(SAR)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では、セキュリティ保証コンポーネントのセットをカタログ化し、ファミリ及びクラスを編成している。また、CCパート3では、PP、ST及びTOEの評価基準を定義している。

d) **CCパート4「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」**は、PP、ST及びそれらをサポートする文書に含まれる可能性のある評価方法及びアクティビティの仕様のための標準的な枠組みを規定し、評価者がCCの他のパートに記述されたモデルを用いた評価を支援する際に使用する。CEMは、CCパート4の基礎となる。

e) **CCパート5「セキュリティ要件の定義済みパッケージ」**は、利害関係者による共通使用を支援するために有用であると確認されたセキュリティ保証及びSFRのパッケージを規定する。規定されるパッケージの例としては、評価保証レベル(EAL)、統合保証パッケージ(CAP)などがある。

CCの適用において、推奨されるオプションが選択されない場合は、必ず正当とする理由を提供しなければならない。

CCをサポートするために、他の文書が発行されている。参考文献には、サポート文書のリストが掲載されている。

注：CEMは、CCに従って実施されるITセキュリティ評価のための基本的な方法を規定する。

5.2.2 対象読者

5.2.2.1 一般

TOEのセキュリティ特性の評価に一般的な関心を持つ主なグループは、消費者(リスク所有者)、開発者、技術ワーキンググループ、評価者、及びその他、の5つである。CCに記載された情報は、CCの主要な利用者であるこれら全てのグループのニーズをサポートするように構成されている。これらのグループは、5.2.2.2～5.2.2.6で説明するように、この基準から恩恵を受けることができる。

5.2.2.2 消費者(リスク所有者)

CCは、評価プロセスの基本的な目的及び正当な理由のため、評価がリスク所有者のニーズを満たすことを保証するために記述されている。

リスク所有者は、TOEが自分たちのセキュリティニーズを満たしているかどうかを判断するために、評価結果を利用することができる。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。また、リスク所有者は、評価結果を利用して、異なるTOEを比較することができる。

CCは、リスク所有者、特に消費者グループや関心のあるコミュニティの人々に、セキュリティ要件を明確な方法で表現するための、PPと呼ばれる実装に依存しない体系を提供する。

5.2.2.3 開発者

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、TOEがPPで規定された消費者からのセキュリティ要求を満たすことを示すために、1つ以上のPPに適合することができる。

CCは、これらの要件に対するTOEの評価をサポートするため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使用される。また、その証拠の内容及び提示も定義されている。

5.2.2.4 技術ワーキンググループ

CCは、PP、PPモジュールと構成、パッケージ、サポート文書やガイダンスの準備及び開発を行う技術ワーキンググループを支援することを目的としている。技術ワーキンググループは、消費者(リスク所有者)、開発者、評価者、学識経験者を含むステークホルダーで構成される。

5.2.2.5 評価者

CCは、評価者がTOE、ST、PP、PP構成のセキュリティ要件への適合について判断する際に使用する基準を含んでいる。CCは、評価者が実行すべき一般的なアクションのセットを記述している。

注：CCは、これらのアクションを実行する際に従うべき手順については規定していない。これらの手順の詳細については、13章に記載されている。

5.2.2.6 その他

CCは、TOEのITセキュリティ特性の仕様と評価を目的としているが、ITセキュリティに関心や責任を持つ全ての関係者の参照資料としても有用である。CCに含まれる情報から恩恵を受けることができるその他の利害関係者には、以下のようなものがある。

a) 組織のITセキュリティ方針及び要件を決定し、それを満たす責任を負うシステム管理者及びシステムセキュリティオフィサー

b) ITソリューション(TOEで構成されるか、TOEを含むことができる)のセキュリティの妥当性を評定する責任を負う、内部及び外部の監査人

c) IT製品のセキュリティ特性の仕様に責任を持つセキュリティ立案者及び設計者

d) 特定の環境で使用するITソリューションを承認する責任を負う認定者

e) 評価の依頼及び支援に責任を有する評価のスポンサー

f) ITセキュリティ評価プログラムの管理・監督に責任を持つ評価監督機関

g) ITセキュリティに関する研究を行う学術関係者

表1は、それぞれの対象読者グループに対するCCの各パートの関心を示したものである。

表1—「ITセキュリティの評価基準」へのロードマップ

CC:2022のパート	消費者(リスク所有者)	開発者	技術ワーキンググループ	評価者	その他
パート1	PP、PPモジュール、PP構成、STの構造及び統合に関する背景情報、参考、ガイダンスに使用すべきである。 TOEのセキュリティ仕様及びセキュリティ課題定義(SPD)の開発に使用しなければならない。	PP、PPモジュール、PP構成、STの構造及び統合に関する背景情報、参考、ガイダンスに使用すべきである。 TOEのセキュリティ仕様の開発に使用しなければならない。	PP、PPモジュール、PP構成、STの構造及び統合に関する背景情報、参考、ガイダンスに使用すべきである。 パッケージ、PP、PPモジュール及びPP構成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、PPモジュール、PP構成、STの構造及び統合に関する背景情報、参考、ガイダンスに使用すべきである。 PP、PP構成、及びSTを評価する際に使用しなければならない。	PP、PPモジュール、PP構成、STの構造及び統合に関する背景情報、参考、ガイダンスに使用できる。

CC:2022のパート	消費者(リスク所有者)	開発者	技術ワーキンググループ	評価者	その他
パート2	リスク環境に対応したセキュリティ機能コンポーネントのステートメントを策定する際に、ガイダンス及び参照として使用しなければならない。	パッケージ、PP、PPモジュールのセキュリティ機能コンポーネントのステートメントを解釈する際に参照として使用しなければならない。 STを開発するときに使用しなければならない。 IT製品のセキュリティ機能性を策定する際に使用することができる。	パッケージ、PP、PPモジュールのセキュリティ機能コンポーネントのステートメントを策定する際に参照として使用しなければならない。	パッケージ、PP、PPモジュールに記載されているセキュリティ機能コンポーネント、又はSTのセキュリティ機能要件(SFR)を評価する際に参照として使用しなければならない。	パッケージ、PP、PPモジュールに記載されているセキュリティ機能コンポーネント、又はSTのセキュリティ機能要件(SFR)をレビューする際の参考として使用できる。
パート3	リスク環境に要求されるセキュリティ保証を決定する際に、ガイダンスや参照として使用しなければならない。	パッケージ、PP、PPモジュール、PP構成におけるセキュリティ保証コンポーネントのステートメントを解釈する際に参照として使用しなければならない。 STを開発する際に使用しなければならない。 開発プロセスを策定又は改善する際に使用することができる。	パッケージ、PP、PPモジュール、PP構成におけるセキュリティ保証コンポーネントのステートメントを作成する際に参照として使用しなければならない。	パッケージ、PP、PPモジュール、PP構成に記載されているセキュリティ機能コンポーネント、又はSTのセキュリティ保証要件を評価する際に参照として使用しなければならない。	パッケージ、PP、PPモジュール、PP構成に記載されているセキュリティ機能コンポーネント、又はSTのセキュリティ保証要件をレビューする際の参考として使用できる。

CC:2022のパート	消費者(リスク所有者)	開発者	技術ワーキンググループ	評価者	その他
パート4	評価方法及び/又は評価アクティビティを構成する際の参考及び背景情報として使用すべきである。	評価方法及び/又は評価アクティビティの構成において、参考及びガイダンスとして使用すべきである。	評価方法及びアクティビティの構成において、参考及びガイダンスとして使用すべきである。	評価方法及びアクティビティの構成において、参考及びガイダンスとして使用すべきである。 具体的な評価方法及びアクティビティを策定する際に使用すべきである。	評価方法及びアクティビティの構成において、参考及びガイダンスとして使用できる。
パート5	主張されるセキュリティ要件の事前に定義されたパッケージの内容を決定する際に参照するべきである。	事前に定義されたセキュリティ要件パッケージへの適合を主張するSTを開発する際に使用しなければならない。 事前に定義されたセキュリティ要件パッケージに適合する評価用TOEを準備する際に参照しなければならない。	事前に定義されたセキュリティ要件パッケージへの適合を主張するPP、PPモジュール、PP構成を開発する際に使用しなければならない。	事前に定義されたセキュリティ要件パッケージへの適合を主張するPP、PPモジュール及びPP構成、又はSTを評価する際に参照として使用しなければならない。	主張されたセキュリティ要件の事前定義パッケージの内容を決定する際の参考として使用できる。

5.3 評価対象(TOE)

5.3.1 一般

CCは、評価対象に柔軟であるため、一般に理解されているようなIT製品の境界に縛られることはない。そのため、評価の枠組みにおいて、CCは「TOE」(Target of Evaluation)という用語を使用する。

TOEが完全なIT製品で構成されている場合もあるが、そうである必要はない。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、又はそれらの組み合わせにすることもできる。

CCに関しては、TOEとIT製品間の正確な関係は、IT製品の一部のみを含むTOEの評価を、IT製品全体の評価として誤認させるべきではないという一点においてのみ重要である。

例：TOEの例としては、インタフェースが少なく、攻撃対象領域が小さく、サプライチェーンがよく知られていることを特徴とするデバイスが挙げられる。

— ネットワーク機器

— 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

— 仮想化システム

— 集積回路

— 集積回路の暗号化コプロセッサ

— モバイルデバイス用のアプリケーション

— 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

TOEはまた、より複雑であり、大きなインタフェース/大きなインタフェース群及び/又は複数のコンポーネント、複数の製造/統合段階、フィールドアップグレード可能な製品などを特徴とし得る。

— 全ての端末、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(LAN)

— モバイル機器

— ゲートウェイ及びハブ

— 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

— 多機能プリンターなどの多機能デバイス

— ハードウェア・セキュリティ・モジュール(HSM)

5.3.2 TOE境界

TOE境界の概念は、STの仕様の基本である。

TOEは、完全なIT製品(又は製品)、IT製品の一部、又は様々なコンポーネントで構成される。STは、顧客に配付されるTOEの物理的及び論理的な範囲の概要を明確に説明しなければならない。

TOE境界内にないIT製品の部分は、評価対象外であり、*IT製品の非TOE部分*と呼ばれる。

5.3.3 TOEの様々な形態

CCでは、保証基準との関係で、TOEは複数の形態を取る可能性がある。

注：これらの保証基準には、TOEのサンプルを必要とするテスト(ATE)と脆弱性分析(AVA)、ソースコードなどの実装表現を必要とする設計(ADV_IMP)、TOEの構成リストを必要とするライフサイクル(ALC)などがある。

例：ソフトウェアTOEのTOE形態

— 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

— オープンソースディストリビューションの特定のバージョンのソースコード

— 顧客に発送する準備の整った物理メディアとマニュアルを入れたボックス

— 安全なダウンロードにより利用可能なバイナリファイル

— インストール済みの運用バージョン

ハードウェアTOEのTOE形態

— 集積回路のレイアウト

— メモリマッピング

— ウェハー

— モジュール

これらは全てTOEとみなされ、CCで「TOE」という用語が使用される場合は、文脈によって記述される形態が決定される。

5.3.4 TOEの様々な構成

一般に、IT製品は、様々なオプションを有効又は無効にすることで、多くの方法で構成することができる。CCに従って行われる評価では、TOEが特定の要件を満たしているかどうかが判断される。TOEのガイダンス部分がTOEの可能な構成を制約することはよくあることで、つまりTOEのガイダンスはIT製品の一般的なガイダンスと異なることがある。

例：オペレーティングシステムのIT製品。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)。

一般に、IT製品がTOEを含むか、又はTOEである場合、製品の構成はより厳しく管理される必要がある。なぜなら、いくつかの構成オプションはTOEが要件を満たさないことにつながる可能性があるからである。

このため、多くの構成を許可する一般的なIT製品のガイダンス文書と、セキュリティに関連する方法で異なることのない1つ又は一連の構成しか許可しないTOEのガイダンス文書との間には、予想される違いがある。

TOEのガイダンス文書が複数の構成を許可している場合、これらの構成はまとめて「TOE」と呼ばれ、各構成はTOEに課された要件を満たさなければならない。

5.3.5 TOEの運用環境

TOE境界の外は全てTOEの運用環境に属する。TOEがIT製品の一部である場合、IT製品はTOE以外の部分を持つことができる。そのようなTOE以外の部分もTOEの運用環境の一部である。

STは、前提条件を記述し、TOE自体が提供するセキュリティ機能性とともに、脅威を軽減し、組織のセキュリティ方針(OSP)を実施しなければならない運用環境のセキュリティ対策方針を定義しなければならない。

運用環境のセキュリティ対策方針は、TOEのセキュリティ機能性をサポートすることができる。

STは、評価済みのTOEを適切に使用するための十分な情報を利用者に提供するために、TOE環境に対する明確な要件を策定しなければならない。

例：安全な鍵の生成と注入の前提及びプロセスは、CCパート2のFCSコンポーネントを使用して指定されたTOE暗号サービスをサポートする運用環境のセキュリティ対策方針の一例である。

5.4 本書に含まれる資料の提示

一般的なモデルは、6章に示されており、IT製品のセキュリティ機能性の評価、セキュリティ課題の定義、セキュリティ課題に対応するセキュリティ要件の仕様に関連する概念を説明している。同様のセキュリティ課題を持つリスク所有者のニーズに関連するセキュリティ要件、パッケージ、PP、PPモジュール、PP構成の仕様に関連する概念を紹介している。

CCパート2及びCCパート3で規定されるセキュリティ要件の特定方法及びセキュリティコンポーネントの完了について、7章及び8章で説明する。

パッケージ、PP、PPモジュール、PP構成及びSTのコア構成要素に関する要件及び推奨事項は、9章、10章、11章及び11.3.3で説明する。

TOE、ST、PP、PP構成に対する評価と評価結果に関する要件及び推奨事項は、13章に記載されている。

最後に、統合保証のトピックは、14章に記載されている。

6 一般モデル

6.1 背景

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パート2、CCパート3、CCパート4、CCパート5は、これらの概念の使用を拡大し、ここに記述されたアプローチが使用されることを前提としている。また、評価アクティビティを実施しようとするCCの利用者には、CEMが適用される。

CCでは、一連のセキュリティ概念と用語を用いてセキュリティを論じている。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。しかし、概念そのものは、CCが適用されるITセキュリティ課題のクラスを限定することを意図していない。6章は、読者がITセキュリティの知識を持っていることを前提としており、この分野のチュートリアルとして機能することは意図していない。

6.2 資産とセキュリティ管理策

セキュリティは、運用環境内の資産の保護に関わるものである。

例1：資産の例として、ファイルやサーバの内容がある。

このような資産範囲に関する運用環境の例としては、以下のようなものがある。

— サーバが設置されているデータセンター

— サーバを世界と接続する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

— サーバを他のサーバ及び/又はやワークステーションと接続するLAN

— サーバ又は特定のファイルからの情報を利用する利用者の日常的な環境

— サーバ及び/又は特定のファイルに通信機能を提供する一般的なオフィス環境

資産の多くは情報の形をとり、情報の所有者が定めた要件を満たす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、そのような情報の可用性、まき散らし、及び改変が厳密に制御され、運用環境に実装されたセキュリティ管理策によって資産が脅威から保護されることを要求することができる。図1は、これらの上位レベルの概念と関係を示す。

注：ISO/IEC 27001は、情報セキュリティ管理システムの確立、実装、保守、及び継続的な改善のための要件を規定しており、管理策の仕様も含まれている。

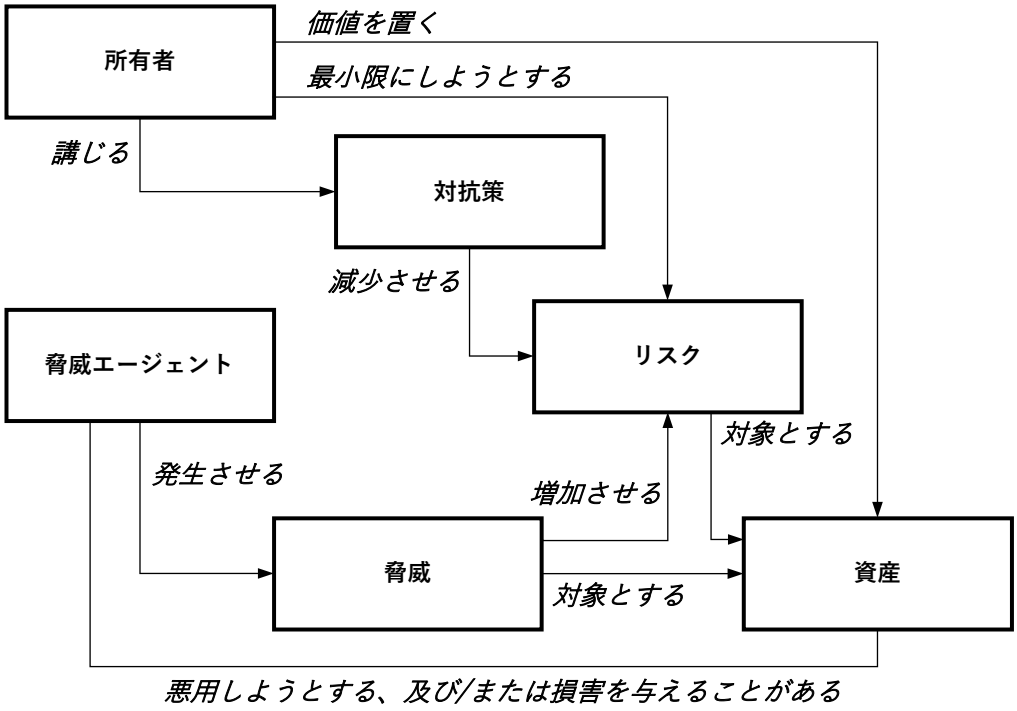


図1 — セキュリティの概念と関係

利害関係のある資産を保護することは、その資産に価値を置く所有者の責任である。実在する又は想定される脅威エージェントも資産に価値を置き、所有者の利益に反する方法で資産を悪用しようとすることがある。

例2：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。

資産の所有者は、そのような脅威を、資産の価値の減少につながる、資産の潜在的な侵害の原因として認識することができる。セキュリティ特有の侵害には、一般的に、資産の機密性の喪失、資産の完全性の喪失、及び資産の可用性の喪失が含まれるが、これらに限定されるものではない。

したがって、これらの脅威は、脅威が実現する可能性と、脅威が実現した場合に資産に与える影響に基づき、資産にリスクを生じさせる。その後、資産に対するリスクを低減するための管理策が課される。これらの管理策は、IT関連の管理策(ファイアウォール及びスマートカードなど)と非ITの管理策(警備員及び手続きなど)で構成される。セキュリティ管理策及びその実施・管理方法に関するより一般的な議論については、ISO/IEC 27001及びISO/IEC 27002も参照すること。

資産の所有者は、それらの資産に対して責任を負う可能性があるため、資産を脅威にさらすリスクを受け入れるという決定を擁護できるべきである。

この決定を擁護するための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。

— 管理策が十分である：適用された管理策が主張する動作を実行する場合、資産に対する脅威は対抗される。

— 管理策が正しい：適用された管理策が主張する動作を実行する場合。

資産の所有者の多くは、セキュリティ管理策の十分性と正確性を判断するのに必要な知識、専門知識、又は資源を持ち合わせておらず、セキュリティ管理策の開発者の主張のみに頼ることを必ずしも望んでいない。したがって、これらの消費者は、セキュリティ管理策の評価を依頼することで、一部又は全てのセキュリティ管理策の十分性と正確性に対する信頼性を高めることを選択できる。

図2は、本章で議論する評価の概念と関係を記述する。

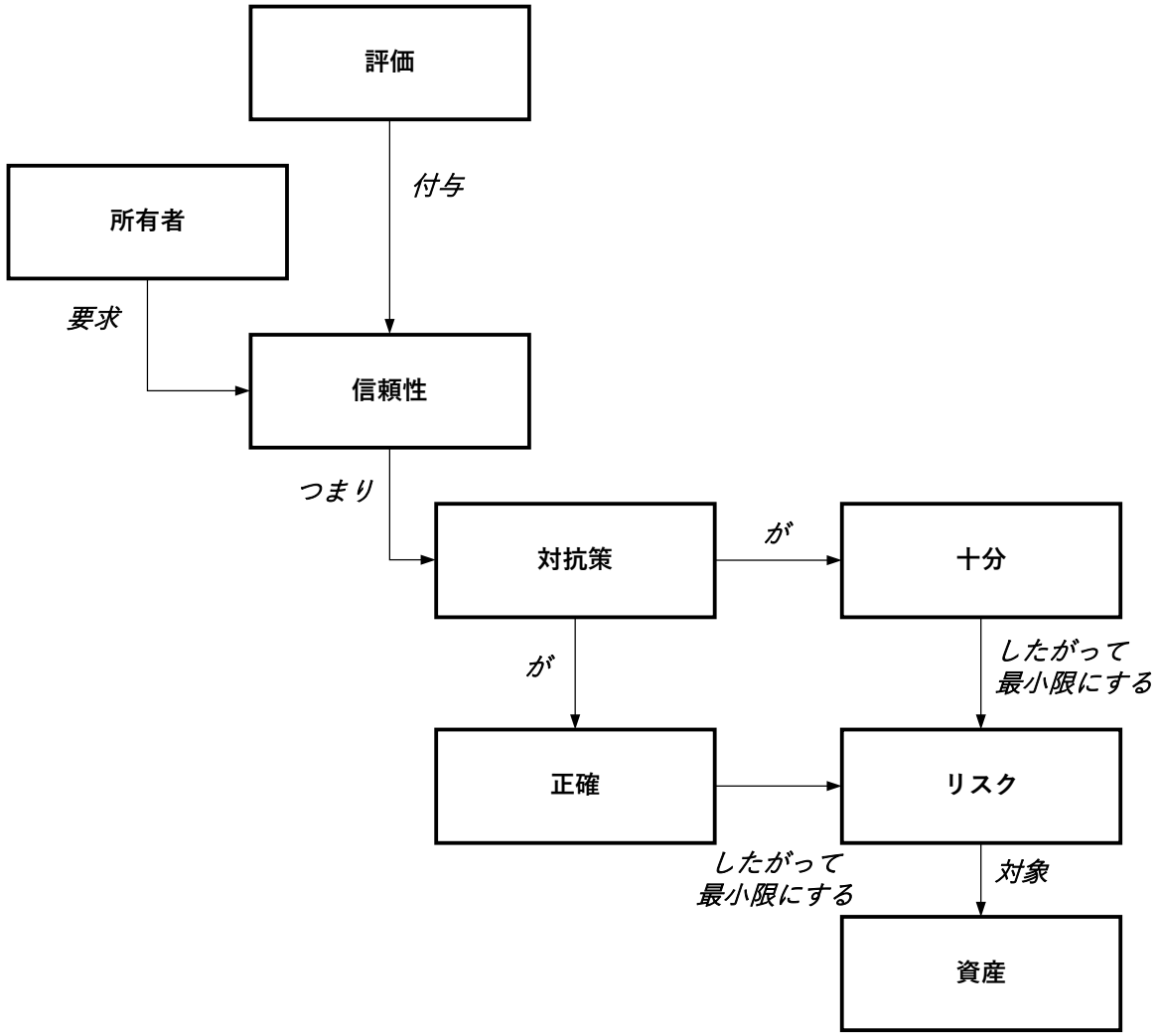


図2 — 評価の概念と関係

評価において、セキュリティターゲット(ST)と呼ばれる構成物を通じて、セキュリティ管理策の十分性が分析される。

6.3 CCのパラダイムのコアとなる構成物

6.3.1 一般

CCは、IT製品の評価のための柔軟な枠組みを定義している。

消費者グループと技術コミュニティがセキュリティニーズを表現できるように、また、これらのニーズを表現する適切な文書の作成を容易にするために、パラダイムでは5つの構成物(パッケージ、PP、PPモジュール、PP構成、ST)が規定されている。

評価は消費者(リスク所有者)の様々な保証ニーズに応える必要があるため、CCは、適切に形成されたセキュリティ保証コンポーネント(CCパート3)や拡張保証コンポーネントを定義するメカニズム(CCパート1)などの様々なツールを提供する。

また、CCの利用者は、EALを含む事前定義されたパッケージ(CCパート5に基づく)から、又は、評価方法と評価アクティビティを定義するフレームワーク(CCパート4)及び関連する評価方法(CEMに基づく)から、選択することもできる。

6.3.2 適合種別

消費者(リスク所有者)のニーズに応えるため、PP及びPP構成に対する3種類の適合が定義されている。これらは、完全適合、正確適合及び論証適合である。これらは附属書Eで詳細に説明されている。

PP、PPモジュール、PP構成は、適合種別を指定しなければならない。

STは、それらの適合種別に従ってPP及びPP構成への適合を主張する。PPは、適合種別に従って、他のPPへの適合を主張することもできる。

PP、PPモジュール、PP構成の適合種別、適合主張、及び適合種別の関係は、附属書Eに記述されており、本書の各章と合わせて使用されなければならない。

6.3.3 セキュリティ要件の伝達

6.3.3.1 パッケージ

パッケージは、頻繁に一緒に使用される関連するセキュリティ要件のセットを記述する。パッケージは、しばしば再利用できるように設計され、それらを使用するPP、PPモジュール及びSTの間で比較可能である。

セキュリティ機能パッケージは、セキュリティプロトコルや他のセキュリティ機能概念を定義するために使用することができる。

セキュリティ保証パッケージは、TOEを開発し構成するための条件やプロセス(仕様、設計、開発、テスト、配付など)を定義するために使用される。

パッケージのコア要件は、9章に記載されている。附属書Aは、パッケージに関する追加情報及び要件を規定し、本書の各章と合わせて使用されなければならない。

CCパート3は、評価基準、及びパッケージを使用する可能性のある評価を受けるST、PP、PPモジュールに対する特定の要件を規定し、CCパート5は、PP、PPモジュール、PP構成、ST作成者が使用できるいくつかの事前に定義された保証パッケージを規定している。

6.3.3.2 プロテクションプロファイル(PP)

PPはTOE種別、及びそのTOE種別で提供されることが期待されるセキュリティ保証要件(SAR)及びセキュリティ機能要件(SFR)を記述する。

他のPPに基づくPPは、TOE種別をさらに詳細化するために使用することができる。

PPは標準的又は直接根拠のいずれかのアプローチを取ることができる。

PPのコアとなる要件は10章にあり、さらに詳しい情報は附属書Bにあり、本書の各章と合わせて使用されなければならない。

CCパート3は、PPの評価基準を規定する。

6.3.3.3 PPモジュールとPP構成

PP構成は、PPとPPモジュールの概念に基づいている。

PPモジュールは、基本PPの汎用的なTOE種別を詳細化するため、又は基本PPで定義されたTOE種別にオプションで関連付けることができる特定の技術に対するセキュリティ要件を追加するために使用することができる。また、PPモジュールは、他のPPモジュールを基盤にすることもできる。さらに、PP構成は、複数のPPと場合によってはPPモジュールで指定されたTOE種別と要件のセットで構成される(これらはPP構成コンポーネントである)。

この概念については、11章及び附属書Cでより詳細に記述されている。

例：あるPPモジュールは、Bluetooth技術のSFRを記述している。別のPPモジュールは、無線LANクライアントのSFRを記述している。PP構成を使用して、これらの技術のSFRを、オペレーティングシステムPPやモバイルデバイスPPなどのTOE種別を記述するPPと組み合わせることができる。この文脈では、TOE種別を記述するPPは基本PPと呼ばれる。PP構成は、適切なPPとPPモジュールに示された全ての要件を含む仕様を提示するために、どのPPとPPモジュールを組み合わせるかを記述する。

この例では、6つのPP構成を特定することが可能である。

a) Bluetooth搭載したオペレーティングシステム

b) Wirelessクライアント搭載したオペレーティングシステム

c) Bluetooth及びWirelessクライアント搭載したオペレーティングシステム

d) Bluetoothを搭載したモバイルデバイス

e) Wirelessクライアントを搭載したモバイルデバイス

f) Bluetooth及びWirelessクライアントを搭載したモバイルデバイス

6.3.3.4 セキュリティターゲット(ST)

6.3.3.4.1 一般

この節では、STの構造を簡略化して示す。STの概念と内容要件のより詳細で完全な説明は、11.3.3及び附属書Dに記載されており、本書の各章と合わせて使用されなければならない。

CCパート3は、評価基準及び評価中のSTに対する特定の要件を規定する。

6.3.3.4.2 STの目的

STは、TOEのセキュリティ課題定義(SPD)を決定することから始まる重要な文書である。これには、保護すべき資産とその資産に対する脅威を特定することが含まれる。次にSTは、関連する前提条件を検討し、これらの脅威に対抗することを実証するために実施する必要のあるセキュリティ対策を記述する。セキュリティ対策が主張する動作を実行する場合、脅威は対抗される。

セキュリティ対策には、次の2つのグループがある。

a) TOEのセキュリティ対策方針：評価において正確性が判断されるセキュリティ対策を記述する。

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判断されないセキュリティ対策を記述する。

このように分ける理由は、以下のとおりである:

— CCは、IT開発及び製造環境、製品ライフサイクル管理の正確性の評定に適している。運用環境から要求されるセキュリティ対策は、CCによる評価の範囲の対象外である。

— セキュリティ対策の正確性を評定するには時間と費用がかかり、全てのセキュリティ管理の正確性を評定することは不可能な場合がある。

— 一部のセキュリティ対策の正確性は、別の評価ですでに評定されている可能性がある。したがって、この正確性を再度評定することは費用対効果に合わない。

STは、SFRを特定することにより、TOEのセキュリティ対策方針をさらに詳しく説明する。これらのSFRは、正確さを保証し、比較可能性を容易にするために、CCパート2で記述されている標準化された言語で策定されなければならない。

要約すると、ST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SPDに対応し、特に脅威に対抗していること。

— したがって、SFRと運用環境のセキュリティ対策方針は、SPDに対応し、特に脅威に対抗していること。

このことから、正しいTOE、すなわちSFRを満たす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の組み合わせは、脅威に対抗することになる。6.3.3.4.3及び6.3.3.4.4では、TOEの正確性と運用環境の正確性を別々に議論している。

場合によっては、TOEのセキュリティ対策方針を省略し、SFRをSPDに直接マッピングさせたSTを定義することが適切であることがある。これは「直接根拠ST」であり、11.3.3及び附属書Dで詳細に説明されている。

STは、特定のTOEのために独立した文書として定義されてもよいし、既存のPP構成又は1つ以上の既存のPPに適合してもよい。これらの文書により、TOE種別の一般的な定義が可能となり、TOE間の評価結果の比較や効率化が可能となる。

STの仕様に寄与するパッケージ、PP、PPモジュール、PP構成は、6.3.3.1, 6.3.3.2, 6.3.3.3で紹介している。

6.3.3.4.3 TOEの正確性

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。これらの脆弱性を悪用することで、攻撃者は資産に損害を与えることができる、及び/又は悪用することができる。

これらの脆弱性は、例えば、設計の不備、開発中の偶発的な誤り、悪意のあるコードの意図的な追加、構成管理の不備などから発生する可能性がある。

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が実施されることがある。

— 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

STは、正確性を決定するためのこれらのアクティビティを、SARの形で構造的に記述する。これらのSARは、正確さを保証し、比較可能性を容易にするために、CCパート3に記述された標準化された言語で策定されなければならない。

SARを満たしている場合、TOEの正確性には保証があり、したがって、TOEには攻撃者が悪用可能な脆弱性が含まれる可能性は低くなる。TOEの正確性がどの程度保証されているかは、SARそのものによって決定される。

6.3.3.4.4 運用環境の正確性

また、運用環境の仕様や実装が不適切で、脆弱性につながる誤りがある場合もある。これらの脆弱性を悪用することで、攻撃者は資産に損害を与えることができる、及び/又は悪用することができる。

しかし、CCでは、運用環境の正確性についての保証は得られない、すなわち、運用環境は評価されない。

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正確な具体化であるとみなされる。

これは、TOEの消費者が、この運用環境の正確性を決定するために他の方法を使用することを妨げるものではない。

例1：オペレーティングシステムTOEの場合、運用環境のセキュリティ対策方針が「運用環境は、信頼できないネットワークからのエンティティがFTPプロトコルを使用してのみTOEにアクセスできることを保証する」

となっている場合、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構成することができる。

例2：運用環境のセキュリティ対策方針に「運用環境は、全ての管理者が悪意を持って行動しないことを保証しなければならない」と記述がある場合、消費者は、管理者との契約に悪意ある行動に対する懲罰的制裁を含めるよう調整することができるが、この決定は、CC を基礎とした評価には含まれない。

注：インターネットは信頼されないネットワークの一例である。

6.3.4 消費者（リスク所有者）のニーズへの対応

6.3.4.1 一般

消費者(リスク所有者)は、使用する製品がSPDに対応しているという保証を得るために、様々なアプローチをとることができる。6.3.4.2及び6.3.4.3は、これらのアプローチを紹介する。さらに、CCパート4では、保証要件に対する具体的な評価アクティビティを定義する方法を規定する。

6.3.4.2 単一保証評価

単一保証評価は、CCの以前の改訂版で規定されていた評価種別である。単一保証評価では、単一セットのSARがTOE全体に適用される。

単一保証評価のパラダイムは、以下のとおりである。

— TOE全体が同じSARの対象であることを要求する。

— 単一セットのSARがTOEのセキュリティニーズに見合ったものである場合に使用される。

単一の保証評価は、PP又はPP構成への適合を主張できるSTに基づくが、セキュリティ保証コンポーネントの同じセット又はスーパーセットを特定する、主張された全てのPP又はPP構成コンポーネントに依存する。PP又はPP構成への適合を主張しないSTに基づく評価は、その性質上、単一保証評価となる。

6.3.4.3 マルチ保証評価

マルチ保証評価パラダイムは、TOE全体に対してグローバルなSARセットを強制する一方で、TSFの異なる部分(サブTSF)に対して異なる保証要件を適用することからなる。

マルチ保証評価パラダイムは、以下のとおりである。

— 異なるセキュリティニーズが異なる保証を必要とする異種IT製品に一度の評価で対応する。

— 複数のセキュリティ保証要件が、IT製品のセキュリティニーズに関して健全であることを保証する。

技術的には、マルチ保証評価は、1つの(そして唯一の)マルチ保証PP構成に適合するSTによって実行される。マルチ保証PP構成は、TSFの異なる部分に異なるセキュリティ要件を適用することが、そのセキュリティニーズと一貫したものであることを保証する。この評価手法では、各サブTSFは何らかのセキュリティ機能性、例えば認証プロトコル、ファイアウォール方針、ブートプロセス、

暗号化/復号操作を実施し、場合によっては、サブTSFはTOEコンポーネントのサブセット、例えばTPM、暗号ライブラリ、カードリーダに関連付けられることがある。

マルチ保証パラダイムは、特に以下のような状況に関連している。

— 一部のセキュリティ機能性が他の部分よりも高い保証を必要とする製品(例：鍵の格納及び処理ユニット、セキュアブートモジュールなど)。

— セキュリティ機能性の一部が、他の露出度の高い部分ほど高い評価保証を必要としない製品、例えばパーソナルエリアネットワークプロトコルをサポートするインターネットゲートウェイ。

— セキュリティ機能性の一部が全製品で共有され保証要件が同一であり、セキュリティ機能性の一部が異なるユースケース、例えば耐タンパモジュール、ソフトウェアモジュール、COTS などで異なる方法で実装され、異なる保証要件が必要な製品ファミリ。

  例えば、バイオメトリクス認証デバイスのファミリで、match-on-device か match-on-SE のいずれか、又は両方がある場合である。この場合、照合機能を除いた認証デバイスの PP と、異なる種別の照合機能のための 2 つの PP モジュールが生じ、それぞれ専用の保証要件が設定される。デバイスには、3 つの PP 構成を定義することができる。PP モジュールのそれぞれを使用した PP、両方の PP モジュールを使用した PP である。例えば、with-box 技法で保護されたソフトウェア暗号ライブラリかハードウェアベースの暗号ライブラリのいずれかを使用するモバイルアプリケーションのファミリや、IC 及び/又は磁気ストライプリーダを使用する決済端末のファミリでも、同様の状況が発生する。

マルチ保証は、異なる保証パッケージを持つ異なる PP への適合を主張する製品にも関連する。PP 構成を定義し評価することで、マルチ保証パラダイムは、これらの PP 間の不整合の可能性をより適切に制御することができる。基本アクセス制御と拡張アクセス制御の両方を実装した電子パスポートの評価は、その典型的な例であり、これらのアクセス制御メカニズムは、異なるセキュリティ課題と保証要件の対象である。

7 セキュリティ要件の特定

7.1 セキュリティ課題定義(SPD)

7.1.1 一般

SPDは、対処すべきセキュリティ課題を定義するもので、PP、PPモジュール及びSTの中に現れることがある。SPDは、CCに関する限り、公理的であり、すなわち、SPDを導出するプロセスはCCの範囲外である。

SPDエレメントは、例えば、TOEが分散している場合や、オプションの機能要件(7.3.2.6で概説)が指定されている場合など、特定のTOE種別のオプションの構成又は要件と関連付けることができる。これは、SPDエレメント(及び関連する対策方針と機能要件)のオプションの性質が、本書に規定されているように識別される限り、許可される。

注1：評価結果の有用性は、SPDの品質に強く依存する。したがって、優れたSPDを導き出すために、多大な資源を費やし、十分に定義されたプロセス及び分析を使用することは、多くの場合価値がある。ISO/IEC 15446は、SPDの導出に関するガイダンスを示す。

注2：CCパート3によれば、全ての節にステートメントを持つことは必須ではない。脅威を含むPPはOSPを持つ必要はなく、その逆もまた然りである。また、どのPPも前提条件を省略することができる。

注3：TOEが物理的に分散している場合、関連する脅威、OSP及び前提条件は、TOEの運用環境の異なるドメインに分離して議論することが望ましい。

7.1.2 脅威

SPDは、TOE、その運用環境、又はその２つの組み合わせによって対抗する脅威を記述する。

脅威は、脅威エージェントが資産に対して行う有害なアクションで構成される。

有害なアクションは、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。

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やグループなどとして記述することが望ましい。

例1

脅威エージェントの例としては、以下のようなものがある。

— ハッカー

— 利用者

— コンピュータのプロセス

— 事故

脅威エージェントは、専門知識、資源、機会、動機などの属性によってより詳細に記述することができる。

例2

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

7.1.3 組織のセキュリティ方針(OSP)

SPDは、TOE、その運用環境、又はその２つの組み合わせによって実施されるOSPを記述する。

OSPとは、運用環境に課されるセキュリティルール、手順、又はガイドラインのことである。OSPは、TOEの運用環境を管理する組織によって作成されることもあれば、立法機関や規制機関によって作成されることもある。OSPは、TOE及び/又はTOEの運用環境に適用することができる。

例：OSPの例として、以下のものがある。

— 「政府によって使用される全ての製品は、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。」

7.1.4 前提条件

SPDは、セキュリティ機能性を提供できるようにするために運用環境で行われる前提条件を記述する。これらの前提条件を満たさない運用環境にTOEが置かれた場合、TOEが持つセキュリティ機能性を全て提供できない可能性がある。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。

例：前提条件の例として、以下のものがある。

— 製品の TOE 以外の部分に関する前提条件

  — TOE は、ハードウェアベースのルートオブトラストを提供するデバイスに統合されることを前提とする。

— 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前提とする。

注：評価中に、これらの前提条件は真実であるとみなされ、前提条件はいかなる方法でもテストされない。これらの理由から、前提条件は運用環境に対してのみ設定することができる。前提条件はTOEのふるまいに対して設定することは決してできない。なぜなら、評価はTOEに関する主張を評価するものであり、TOEに関する主張が真実であると仮定するものではないためである。しかしながら、ST、PP及びPP構成の評価は、TOEの種別や運用環境に対する、受け入れられなくなる可能性がある非現実的な前提条件を検出するのに役立つ。

7.2 セキュリティ対策方針

7.2.1 一般

セキュリティ対策方針は、セキュリティ課題に対して意図している解決策を簡潔に示した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。

a) 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。セキュリティ対策方針は、あまり詳しすぎない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の知識を持つ潜在的な消費者にとって明確で理解しやすい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書かれている。

b) この解決策を、課題の各部分に対処するためのTOEとその運用環境の役割を反映した、2つの部分的解決策に分割する。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。これらの部分的な解決策は、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。

c) 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。

7.2.2 TOEのセキュリティ対策方針

TOEは、SPDによって定義された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が達成しなければならない目標のセットから構成される。

例：TOEのセキュリティ対策方針の例として、以下のものがある。

— 「TOEは、TOEとサーバ間で送信される全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、全ての利用者を識別認証しなければならない。」

— 「TOEは、PP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。」

TOEが物理的に分散している場合、TOEのセキュリティ対策方針を含む節をいくつかの項に細分化し、これを反映させることが望ましい。

注：直接根拠STでは、TOEのセキュリティ対策方針は含まれない。D.4を参照のこと。

7.2.3 運用環境のセキュリティ対策方針

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を支援する技術的及び手続き的な手段を実装する。この一対の解決策は、運用環境のセキュリティ対策方針と呼ばれ、運用環境が達成しなければならない目標を記述したステートメントのセットからなる。

例

運用環境のセキュリティ対策方針の例として、以下のようなものがある。

— 「運用環境では、TOEを実行するために、OS Linux バージョン3.01bを搭載した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、全ての人間のTOE利用者が、TOEを扱うことを許可する前に適切な訓練を受けることを保証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、TOEから監査サーバに受信した監査ログの機密性を保証しなければならない。」

TOEの運用環境が特性の異なる複数の物理的サイトから構成されている場合は、運用環境のセキュリティ対策方針を含む節を複数の項に細分化し、これを反映することが望ましい。

評価証拠がないために評価されない第三者コンポーネントは運用環境に含まれ、運用環境のセキュリティ対策方針には、第三者コンポーネントが意図したとおりに動作することを含めなければならない。

7.2.4 セキュリティ対策方針とSPDの関係

ST、PP、PPモジュール及びパッケージは、2つの節からなるセキュリティ対策方針の根拠も含まれる。

a) どのセキュリティ対策方針がどのSPDエレメントに対応しているかを示す追跡。

b) 全てのSPDエレメント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。

注：直接根拠PPでは、TOEのセキュリティ対策方針の根拠は含まれない。D.4を参照のこと。

例：脅威が「T17: 脅威エージェントXはAとBの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AとBの間で送信される全ての情報の秘密が保持されることを保証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。

7.2.5 セキュリティ対策方針とSPDの間の追跡

追跡は、セキュリティ対策方針がSPDエレメントまでどのようにさかのぼるかを示し、次のことを示す。

a) *関係のない対策方針は存在しない。*

各セキュリティ対策方針は、少なくとも1つのSPDエレメントまでたどる。

b) *セキュリティ課題定義が完全に網羅されている。*

各SPDエレメントは、それをたどる少なくとも1つのセキュリティ対策方針を有する。

c) *追跡が正確である。*

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３に示す。

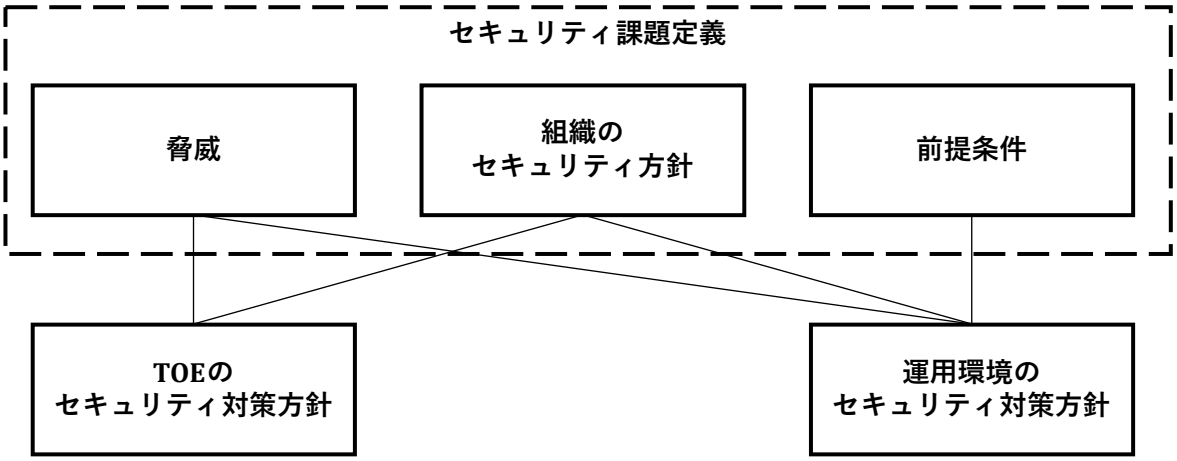


図3 — セキュリティ対策方針とSPDの間の追跡

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及び前提条件についても、同様の議論が成り立つ。

7.2.6 追跡の正当化の提供

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又は前提条件までたどる全てのセキュリティ対策方針が達成された場合、全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)。

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。

SPDの一部がセキュリティ対策方針に酷似している場合、その実証は容易であることもある。

7.2.7 脅威への対抗について

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するのではなく、その脅威を十分に軽減させること、又は関連するリスクを十分に緩和させることを意味する場合もある。

例：脅威を除去する例としては、以下のようなものがある。

— 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、又は保護する。

— 脅威エージェントを除去する。例えば、ネットワークを頻繁にクラッシュさせるマシンをネットワークから取り外す。

脅威を軽減する例は、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又は資源を要求する。

脅威の影響を緩和する例は、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、成功した全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。

7.2.8 セキュリティ対策方針：結論

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、以下の結論が導かれる。全てのセキュリティ対策方針が達成されれば、SPDで定義されたセキュリティ課題は解決されたことになる。全ての脅威は対抗され、全てのOSPは実施され、全ての前提条件は充足される。

注：CCパート3のASE_SPDファミリは、この決定をサポートする。

7.3 セキュリティ要件

7.3.1 一般

6.3.3.4及び6.3.3で述べたように、パッケージ、PP、PPモジュール、PP構成及びSTは、明示されたSPDから導き出されたTOEに適用される詳細なセキュリティ要件を特定する。SFRとSARは、それぞれCCパート2とCCパート3に定義されたセキュリティコンポーネントから抽出されるものであり、標準化された言語で書かれたセキュリティ要件のテンプレートである。セキュリティコンポーネントからセキュリティ要件を導き出す過程には、コンポーネントを消化することが含まれ、「完了」と呼ばれる。

注1：7章において、「作成者」という用語は、ST、PP、PPモジュール、PP構成、パッケージの作成者を含む。

セキュリティ要件は、ST、場合によってはPP、PPモジュール及びパッケージの記述の結果として特定される。セキュリティ要件は、CCパート2、CCパート3、又は8.4に従って拡張コンポーネントとして定義されたコンポーネントを選択することによって特定される。調整プロセスは、8.2の操作を使用する。

注2：STは特定のTOEのセキュリティ要件を特定するものであるため、完全に完了したコンポーネントのみを提示する。PP、PPモジュール及びパッケージは、しばしば未完了のセキュリティコンポーネントを提示するので、それらを基に文書を作成する作成者は適切な柔軟性を持つことができる。

セキュリティ要件は、2つの要件グループから構成されている。

a) ***セキュリティ機能要件***(SFR)：TOEがSPDに対処する方法の標準化された言語による記述。

b) ***セキュリティ保証要件***(SAR)：TOEがSFRを満たす保証を得る方法の記述。

注3：SARは、TOEのSTへの準拠に関わるものである。SARは、セキュリティ対策方針とSFRによってカバーされるSPDの範囲では役割を果たさない。

この2つのグループについては、7.3.2及び7.3.3で説明する。

7.3.2 セキュリティ機能要件(SFR)

7.3.2.1 一般

SFRは、TOEのSPDを満たし、TOEのセキュリティ対策方針に対応するために貢献する。通常、SFRはより詳細な抽象化レベルであるが、完全な書き換えでなければならない(TOEのセキュリティ対策方針に完全に対応しなければならない)。CCが標準化された言語への書き換えを要求するのは、以下の理由からである。

— 評価する対象について正確に記述する。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、標準化された言語に書き換えることで、TOEの機能性をより正確に記述することができる。

— 2つのST間の比較を可能にする。標準化された言語では、同じ用語と概念を使用することが強制される。これにより、作成者がSPDやセキュリティ対策方針を記述する際に異なる用語を使用している場合でも、２つのSTの比較が可能になる(この状況は、STが同じPP又はPP構成に適合している場合には発生しない)。

PP及びPPモジュールの枠組みでは、SFRはいかなる特定の技術的解決策(実装)にも依存しないものでなければならない。

運用環境のセキュリティ対策方針については、運用環境は評価されず、それゆえにその評価を目的とした記述を必要としないため、本書では書き換えは要求されない。

注1：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、参考文献を参照のこと。

注2：運用環境の部分が別の評価で評価される場合もあるが、これはCCの範囲外である。

例：オペレーティングシステムTOEは、運用環境にファイアウォールが存在することを要求することができる。別の評価で、後にファイアウォールを評価することは可能であるが、この評価はOS TOEの評価とは関係ない。

7.3.2.2 この書き換えがサポートされる方法

CCは、次の3つの方法でこの書き換えをサポートする。

a) 事前に定義された「言語」を提供することにより。言語は、評価する対象を正確に記述するために設計されたものである。この言語は、CCパート2で定義された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のSFRへの明確に定義された書き換えとして、この言語の使用は必須であるが、いくつかの例外が存在し、8.4に示されている。

b) 操作を提供することにより。操作は、パッケージ、ST、PP又はPPモジュールの作成者が、TOE又はTOE種別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、SFRを完了及び修正することを可能にするメカニズムである。本書では、割付、選択、繰返し、詳細化の4つの許可操作を定義している。これらについては、8.2でより詳細に説明する。

c) 依存性を提供することにより。依存性は、SFRへのより完全な書き換えをサポートするメカニズムである。CCパート2の言語では、SFRは他のSFRへの依存性を持つことがある。これは、STがそのSFRを使用する場合、一般的にそれらの他のSFRも同様に使用する必要があることを意味する。これにより、STの作成者が必要なSFRを含めることを見落とす可能性が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、8.3でより詳細に説明する。

7.3.2.3 SFRとセキュリティ対策方針の関係

パッケージ、PP、PPモジュール、STには、2つの節からなるSFRの根拠が含まれている。

a) どのSFRがTOEのどのセキュリティ対策方針に対応しているかを示す追跡。

b) TOEの全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ていることを示す正当化のセット。

注：直接根拠アプローチでは、SFRとSPDの間で追跡と根拠を提供する。

7.3.2.4 SFRとTOEのセキュリティ対策方針間の追跡

この追跡は、以下のように、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示す。

a) *関係のないSFRがないこと*：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、それにたどる少なくとも1つのSFRがある。

複数のSFRがたどった先が同じTOE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セキュリティ対策方針を満たすことを示す。

7.3.2.5 追跡の正当化の提供

SFRの根拠では、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全てのSFRが満たされた場合、そのTOEセキュリティ対策方針は達成される。

この実証では、関連するSFRを満たすことがTOEセキュリティ対策方針を達成する上でどのような効果があるかを分析し、実際にそのTOEセキュリティ対策方針が達成されるという結論を導く。

7.3.2.6 特殊なSFRの種別

SFRは、パッケージ、PP、PPモジュールにおいて、オプションの要件又は選択ベースの要件として指定することができる。

A.オプションの要件

オプションの要件は、PP/STが、PP又はPP構成への適合(種別は問わない)を主張するために、PP/STに含まれる必要がないという意味で「オプション」である。

パッケージ、PP及びPPモジュールは、オプションの要件を2つのカテゴリのうちのいずれかで定義することができる。各カテゴリは作成者によって明示的に指定される。

オプションの要件の最初のカテゴリは、選択的なものである。このカテゴリの要件は、PP/STが、要件が定義されているPP又はPP構成への適合(種別は問わない)を主張するために、PP/STに含まれる必要はない。この場合、TOEが要件によって記述された機能性を実装していても、PP/STに要件が含まれることは必須ではない。

オプションの要件の2番目のカテゴリは、条件付きである。TOEが記述された機能性を実装する場合、オプション要件はPP/STに含まれなければならない。TOEがオプションの要件でカバーされる機能性を実装していない場合、その要件はPP/STに含まれない。

注：オプションの要件は、パッケージ、PP、PPモジュールに存在するSPDエレメント、又は要件と特に関連するSPDエレメントに対応して記述することができる。そのような関連は、パッケージ、PP又はPPモジュールで識別される。直接根拠のパッケージ、PP、PPモジュール又はSTは、関連するSPDエレメントを持つオプションの要件のセキュリティ対策方針を定義しないが、通常のパッケージ、PP、PPモジュール又はSTは、関連するSFRとSPDエレメントに対するセキュリティ対策方針を含む。

B.選択ベースの要件

パッケージ、PP、PPモジュールは、選択ベースのSFRのセットを識別することができる。この場合、作成者はさらに、パッケージ/PP/PPモジュールに含まれるセキュリティ機能コンポーネント及び/又はSFRの特定の選択と、その選択が他のPP/ST作成者によって選択された場合に含まれなければならない関連する選択ベースSFR間との依存性を、パッケージ/PP/PPモジュールが明確に示すようにする。これについては、8.2.4.2.で説明する。

7.3.3 セキュリティ保証要件(SAR)

7.3.3.1 一般

SARは、パッケージ、PP、PPモジュール、PP構成及びSTで定義できるTOEの評価方法を記述したものである。この記述では、次の2つの理由から標準化された言語を使用する。

— TOEの評価方法に関する正確な記述を提供する。

— 2つのST間の比較を可能にする。標準化された言語では、同じ用語と概念を使用することが強制される。

この標準化された言語は、CCパート3に定義されたコンポーネントによって表現され、許可される操作は、8章で定義される。この言語の使用は、いくつかの例外はあるものの、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) 操作を提供することにより。操作は、パッケージ/PP/PPモジュール/PP構成/STの作成者がSARを修正することを許可するメカニズムである。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、8.2節でより詳細に説明する。

b) 依存性を提供することにより。依存性は、依存するSARを完了させるために、他のSARから一貫した選択をサポートするメカニズムである。CCパート3の言語では、SARは他のSARへの依存性を持つことがある。これは、パッケージ/PP/PPモジュール/PP構成/STがそのSARを使用する場合、一般的にそれらの他のSARも使用する必要があることを意味する。これにより、作成者が必要なSARを含めることを見落とす可能性がはるかに少なくなるため、パッケージ、ST、PP、PPモジュール、PP構成の完全性が向上する。依存性については、8.3節でより詳細に説明する。

注：CCパート3で定義されたSARは割付や選択を使用しない。しかし、これらの操作を可能にする拡張保証コンポーネントを定義することは可能である。

7.3.3.2 SAR及びセキュリティ要件根拠

保証パッケージ、PP、PPモジュール、PP構成、及びSTは、選択されたSARのセットが適切である理由を説明するセキュリティ要件の根拠も含んでいる。

注：完全適合の場合、PPモジュールはPPモジュール基盤からSARを継承するため、SARの根拠は不要である。

SARは、リスク所有者が評価を受ける際の信頼性に寄与する。CCパート3で示される多くのSARは、開発者がTOEを実装する際に使用する設計・開発プロセス及び開発者テストに関連する。一部のSARは、安全な配付プロセスや欠陥修正など、運用TOEに関連する。評価者の脆弱性分析、独立した機能テストや侵入テストに特に関連するSARもある。

例：SARの選択における矛盾の例として、SPDで脅威エージェントが非常に有能である脅威について言及しているが、SARに含まれる脆弱性分析(AVA_VAN)のレベルが低い(又は存在しない)場合がある。

7.3.4 セキュリティ要件：結論

機能パッケージ/PP/PPモジュール/STのSPDの節では、セキュリティ課題はSPDエレメントである脅威、OSP、前提条件から構成されるものとして定義される。機能パッケージ/PP/PPモジュール/STのセキュリティ対策方針の節では、解決策は次の2つのサブソリューションの形で提供される。

— 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

また、全てのセキュリティ対策方針が満たされれば、セキュリティ課題が解決されることを正当化するために、セキュリティ対策方針根拠が提供される。

セキュリティ要件の節では、TOEのセキュリティ対策方針はSFRに書き換えられ、全てのSFRが満たされた場合に、TOEの全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。

また、TOEの評価方法を示すために、SARのセットが提供され、これらのSARの選定の説明も提供される。SARのセットは、SPDから得られるセキュリティ期待に沿ったものでなければならない。SARの選定の説明は、セキュリティ保証要件根拠の中で行われなければならない。

運用環境そのものは評価対象外であるが、AGD保証クラスがSTに含まれる場合、TOEガイダンスは運用環境のセキュリティ対策方針を完全に反映しなければならず、AGDクラスを使用して評価の一部として評定される。

上記の全ては、次のステートメントにまとめられる。「全てのSFR及びSARが満たされ、運用環境の全てのセキュリティ対策方針が達成された場合、ASE_SPDに定義されたセキュリティ課題が解決される保証が存在する。つまり、全ての脅威が対抗され、全てのOSPが実施され、全ての前提条件が充足される。」。これを図4に示す。

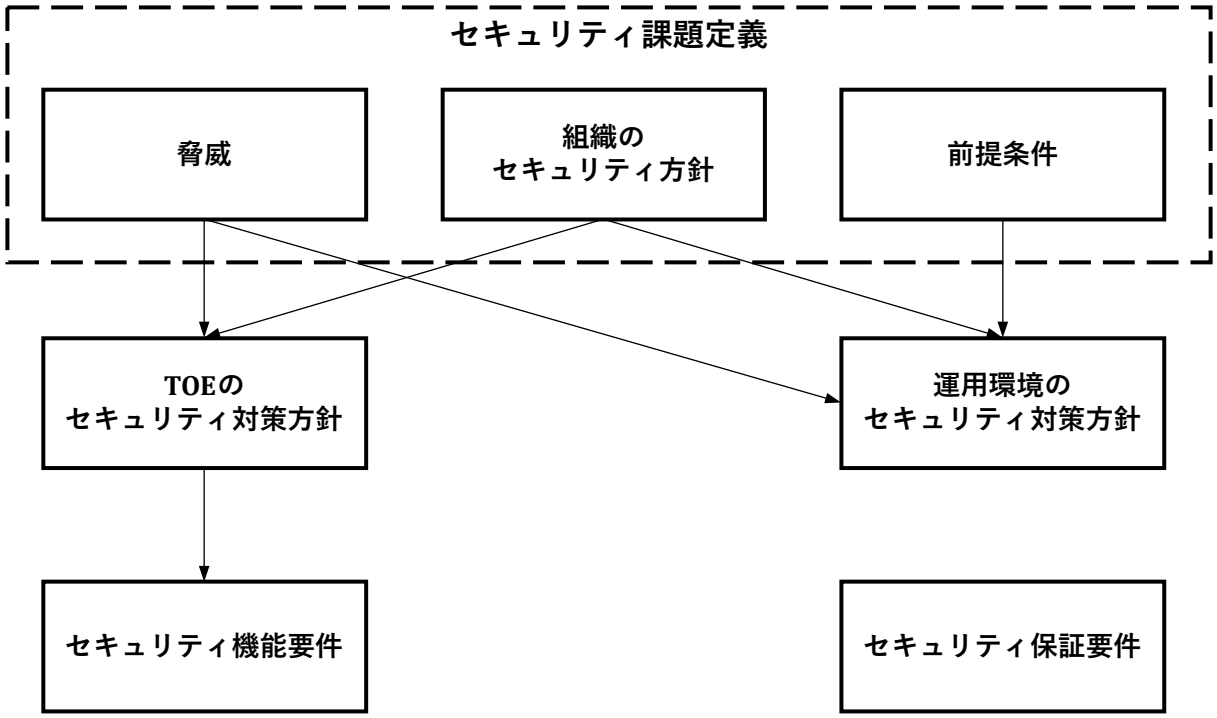


図4 — SPD、セキュリティ対策方針、及びセキュリティ要件の間の関係

評価によって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STを利用するリスク保有者にとって十分であるかどうかは、これらのSARの選定についての説明に記述される。

8 セキュリティコンポーネント

8.1 セキュリティコンポーネントの階層構造

8.1.1 一般

CCパート2及びCCパート3は、セキュリティ要件を特定する際に使用しなければならないセキュリティコンポーネントのカタログを提供する。このカタログでは、コンポーネントを4つのレベルで階層構造に整理している。

— 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

— これ以上分解することができないエレメント

8.1.2 クラス

機能クラスの要件は、CCパート2の6.1.2に記載されている。保証クラスの要件は、CCパート3の6.2.に記載されている。

クラスは、ファミリのセットから構成される。

例：クラスの例には、利用者の識別、利用者の認証、利用者とサブジェクトの結合に焦点を置く「FIA：識別と認証」クラスがある。

8.1.3 ファミリ

機能ファミリの要件は、CCパート2の6.1.3に記載されている。保証ファミリの要件は、CCパート3の6.3.に記載されている。

ファミリは、コンポーネントのセットで構成される。

例：ファミリの例には、「FIA：識別及び認証クラス」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。

8.1.4 コンポーネント

機能コンポーネント構造に関する要件は、CCパート2の6.1.4に記載されている。保証コンポーネントの要件は、CCパート3の6.4に記載されている。

コンポーネントは、エレメントのセットで構成される。

例：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。

8.1.5 エレメント

機能エレメントの要件は、CCパート2の6.1.4に記載されている。保証エレメントの要件は、CCパート3の6.5.に記載されている。

例：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。

8.2 操作

8.2.1 一般

CCパート2とCCパート3はセキュリティコンポーネントのカタログを提供し、本書は作成者に、ある状況下でコンポーネントカタログを拡張する機能を提供する。セキュリティコンポーネントに操作を適用することで、PP、PPモジュール、パッケージ、STを作成する際に、作成者のニーズに合わせて正確に調整することができる。

セキュリティコンポーネントは、CCパート2及びCCパート3で定義されたとおりに正確に使用することもできるし、許可された操作を使用して調整することもできる。

操作を使用する場合、作成者は、この要件に依存する他の要件の依存性要求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、次のセットから選択される。

a) 繰返し：コンポーネントを、様々な操作で複数回使用することができる。

b) 割付：パラメタを特定することができる。

c) 選択：リストからの1つ以上の項目を特定することができる。

d) 詳細化：詳細を追加することができる。

割付及び選択操作は、コンポーネントで具体的に指示されている場合にのみ許可される。繰返し及び詳細化は、全てのセキュリティ要件で許可されている。各操作について以下にさらに詳細に記述する。

CCパート2附属書は、選択と割付の有効な完了に関するガイダンスを提供する。このガイダンスは、操作を完了する方法についての指示を提供し、作成者が逸脱を正当化しない限り、これらの指示に従わなければならない。

— 「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)」が選択された場合、追加の選択オプションは選択できない。もし、選択のオプションとして「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「又は(or)」で結合することが認められる。

  選択の操作は、必要に応じて繰返しと組み合わせてもよい。この場合、各々の繰返しに対して選択されたオプションの適用可能性は、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。

— 割付の完了については、「なし(none)」が有効な完了であることを決定するために、CCパート2附属書を参照しなければならない。

8.2.2 繰返し

繰返し操作は、全てのコンポーネントで実行することができる。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で、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全ての繰返しとは異なっていなければならない。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。

異なる繰返しは、これらの要件との間の明確な根拠と追跡を可能にするために、一意に識別するべきである。繰返しの識別は、読者にとって意味のあるものであるべきである。

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

— 暗号操作(RSA署名)(FCS_COP.1(RSA署名))

— 暗号操作(AESデータ暗号化/復号化)(FCS_COP.1(AESデータ暗号化/復号化))

注：場合によっては、繰返し操作は、コンポーネントの繰返しの代わりに、値の範囲又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を用いることが可能である。その場合、作成者は、値の範囲に対して全体的な根拠を提供する必要があるか、又は、値ごとに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、これらの値に対して個別の追跡が必要かどうかを検討する。

8.2.3 割付

割付操作は、特定のコンポーネントに作成者が設定するパラメタを持つ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、又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。

PP、PPモジュール、又はPP/PPモジュール内のパッケージのエレメントに割付が含まれる場合、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。

例1：作成者は、PP、PPモジュール又はパッケージに次のFIA_AFL.1.2を含めることができる。

「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]しなければならない。**」

この場合、ST作成者はFIA_AFL.1.2をこのように完了させることができる。

「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、その外部エンティティが今後いかなるサブジェクトにも結合することを防止しなければならない。」

b) 割付を完了する。

例2：作成者は、PP、PPモジュール又はパッケージに次のFIA_AFL.1.2を含めることができる。

「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、その外部エンティティが今後いかなるサブジェクトにも結合することを防止しなければならない。」

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3：作成者は、PP、PPモジュール又はパッケージに次のFIA_AFL.1.1を含めることができる。

「TSFは、…、[割付: 正の整数値]回の不成功認証試行が生じたときを検出しなければならない。」

この場合、ST作成者はFIA_AFL.1.1をこのように完了させることができる。

「TSFは、…、**3**回の不成功認証試行が生じたときを検出しなければならない。」

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4：作成者は、PP、PPモジュール又はパッケージに次のFIA_AFL.1.2を含めることができる。

「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: 利用者が今後いかなるサブジェクトにも結合することを防止、管理者に通知]しなければならない。」

この場合、ST 作成者は FIA_AFL.1.2 をこのように完了させることができる。

「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、**利用者が今後いかなるサブジェクトにも結合することを防止**しなければならない。」

ST作成者は、全ての割付を完了しなければならない。

オプションb)、及びc)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。

割付がセットで完了する場合、作成者は、どのサブジェクトを意味しているかが明確である限り、セットのエレメントを導き出すことができるセットの記述を提供するべきである。

例5：セットが「サブジェクト」である場合。

— 全てのサブジェクト

— 種別Xの全てのサブジェクト

— サブジェクトaを除く全てのサブジェクト

8.2.4 選択

8.2.4.1 一般

選択操作は、特定のコンポーネントに作成者が複数の項目から選択する必要があるエレメントが含まれる場合に行う。

PP、PPモジュール、又はパッケージのエレメントに選択が含まれる場合、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しておく。

b) 1つ以上の項目を選んで、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。

PP、PPモジュール又はパッケージのエレメントが選択を含む場合、ST作成者は、上記b)に示すように、その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。

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

例：選択を持つエレメントの例を次に示す。

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。」

8.2.4.2 選択ベースのセキュリティ機能コンポーネントとSFR

PP、PPモジュール又はパッケージは、選択ベースSFRと呼ばれるセキュリティ機能コンポーネント及び/又はSFRのセットを定義することができる。このコンポーネント及び/又はSFRのセットは、PP、PPモジュール又はパッケージの別のコンポーネント及び/又はSFRで行われた選択に関連している。関連する選択ベースのコンポーネント及び/又はSFRは、以下の場合にPP、PPモジュール、パッケージ又はSTに含まれなければならない。

— PP、PPモジュール又はパッケージの中で識別された選択項目が、関連する選択ベースのSFRを持つことを示す。

— その選択は作成者によってなされたものである。

PP、PPモジュール又はパッケージは、選択ベースのコンポーネント及び/又はSFRがグループ化されるように構成することができる。

作成者が選択操作を未完了のままにしておく必要がある場合、作成者は未完了の選択操作に関連する選択ベースコンポーネント及び/又はSFRを変更せずに残しておかなければならない。

作成者が選択を完了させる必要がある場合、作成者はPP、PPモジュール、パッケージ又はSTのSFRのリストに、適切な選択ベースのコンポーネント及び/又はSFRを含めるべきである。

選択操作が制限される場合、すなわち、選択項目の全てではなく一部が削除される場合、作成者は、選択から削除された選択肢に対応する選択ベースのコンポーネント及び/又はSFRをリストから削除しなければならない。

以下は、そのようなSFRの別の例である。

例：選択ベースSFRの一例、ここではFTP_ITC.1.1が選択を持つSFRで、FCS_IPSEC.1が選択ベースのSFRである場合。

FTP_ITC.1.1 TSFは、...間の信頼できる通信チャネルを提供するために[選択: IPsec、SSH、TLS、HTTPS]を使用できなければならない。

適用上の注釈：

FTP_ITC.1.1 の選択において、ST作成者はTOEがサポートするメカニズムを選択し、選択したメカニズムに対応する本PPの附属書Bの選択ベースの要件がSTに含まれていることを保証する。

また、例示PPの附属書Bでは：

ST作成者がFTP_ITC.1.1で「IPsec」を選択した場合、以下のSFRがST内に含まれる。

FCS_IPSEC.1 [...]

8.2.5 詳細化

詳細化操作は、全ての要件に対して実行することができる。作成者は、その要件を変更することで、詳細化を実行する。

注1：一連の詳細化された繰返し操作を使用して、サブジェクト、オブジェクト、操作、セキュリティ属性及び/又は外部エンティティを全てカバーすることができるが、各個別の詳細化はそうではない。

詳細化の最初の規則は、PP、PPモジュール、パッケージ又はSTの文脈において、詳細化された要件を満たすTOEは、詳細化されていない要件も満たすこと、すなわち、詳細化された要件は元の要件よりも「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、結果として生じる詳細化要件は拡張要件とみなされ、7.3に従って拡張要件として扱われなければならない。

例1：有効な詳細化の例を次に示す。

FIA_UAU.2.1「TSFは、その利用者を代行する全ての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、その利用者を代行する全ての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。

この規則に対する唯一の例外として、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/又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。ただし、この例外は、適合を主張するPP、PPモジュール又はパッケージから取得したSFRを詳細化する場合には適用されない。これらのSFRは、元のPP、PPモジュール又はパッケージの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/又は外部エンティティに適用するように詳細化されてはならない。

例2：このような例外の例を次に示す。

FIA_UAU.2.1「TSFは、その利用者を代行する全ての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、その利用者を代行する全ての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。

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3：電磁放射の防止に関する追加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。

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、又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場合がある。この変更によって要件の意味を変更することは、いかなる方法でも認められない。

例4：編集による詳細化の例として、次のようなものがある。

SFR FPT_FLS.1「TSFは、以下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つのCPUの故障**」 これは次のように詳細化することができる 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つのCPUの故障**」 もしくは FPT_FLS.1、「TSFは、**1つのCPUが故障した**ときはセキュアな状態を保持しなくてはならない。」

8.3 コンポーネント間の依存性

コンポーネント間に依存性が存在することがある。依存性は、あるコンポーネントが自立しておらず、セキュリティ機能性又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。

CCパート2の機能コンポーネントは、通常、他の機能コンポーネントへの依存性を持っている。CCパート3の保証コンポーネントの一部も依存性を持っており、その依存性は他のCCパート3コンポーネントにも及ぶ可能性がある。

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することができる。拡張された機能/保証コンポーネントも同様に依存性を定義することができる。

コンポーネントの依存性の記述は、CCパート2、CCパート3、又は拡張コンポーネント定義で与えられるコンポーネント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ために、依存性のあるコンポーネントに基づく要件がPP、PPモジュール、パッケージ又はSTに組み込まれる場合、依存性が満たされるべきである。パッケージを構築する際には依存性も考慮すべきである。すなわち、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、PPモジュール、パッケージ又はSTがコンポーネントAに基づくセキュリティ要件を含むときは常に、PP、PPモジュール、パッケージ又はSTは以下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より階層的に上位のコンポーネントに基づくセキュリティ要件。

c) PP、PPモジュール、パッケージ又はSTが、コンポーネントBに基づくセキュリティ要件を含まない理由の正当化。

ケースa)及びb)において、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。

c)の場合、セキュリティ要件を含まないことの正当化では、次のいずれかに対処するべきである:

— 依存性が必要ない、又は役立たない理由、又は

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

— 依存性が他のSFRによって他の方法で対処されていること(例えば、拡張SFR、SFRの組み合わせ)。

8.4 拡張コンポーネント

8.4.1 一般

セキュリティ要件は、以下の3つ[i]の例外を除き、CCパート2又は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) CCパート2のコンポーネントを使用してSFRに書き換えられないTOEのセキュリティ対策方針がある。

b) CCパート2のコンポーネントに基づいてTOEのセキュリティ対策方針はSFRに書き換えられるが非常に困難及び/又は複雑さを伴う。

c) CCパート3のコンポーネントを使用してSARに書き換えられない第三者要件がある。

例：暗号の評価に関する法律や規制。

このような場合、作成者は拡張コンポーネントと呼ばれる新しいコンポーネントを定義する必要がある。拡張コンポーネントに基づいて拡張された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。

新しいコンポーネントを正確に定義した後に、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つ以上のSFR又は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から抽出されたSFRやSARと拡張コンポーネントに基づくSFRやSAR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。拡張コンポーネントの詳細については、D.3.6でも説明されている。

8.4.2 拡張コンポーネントの定義

パッケージ、PP、PPモジュール又はSTの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に当てはま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。

また、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全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。

例

可能な依存性の例としては、以下のようなものがある。

a) 監査に関連する拡張コンポーネントは、FAU：セキュリティ監査クラスのコンポーネントに対する依存性を含むことができる。

b) データを改変又はアクセスする拡張コンポーネントは、アクセス制御方針(FDP_ACC)ファミリのコンポーネントに対する依存性を含めることができる。

c) 特定の設計記述を使用する拡張コンポーネントは、適切なADV：開発ファミリに対する依存性を含めることができる。

拡張機能コンポーネントの場合、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、適用可能な監査情報及び関連する運用情報を含めなければならない。拡張保

証コンポーネントの場合、作成者は、CEMで規定される方法と同様に、コンポーネントの適切な評価方法を定めることもできる。

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が、その場合、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パート2又はCCパート3で記載されたものと同様に定義しなければならない。

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が、その場合、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パート2又はCCパート3で定義されたものと同様に定義しなければならない。

9 パッケージ

9.1 一般

パッケージは、セキュリティコンポーネント又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、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。

2つ以上のパッケージが互いに関連している場合、それらはパッケージファミリの一部として提示されることがある(A.2参照)。

パッケージは、PP、PPモジュール、PP構成及びSTによって主張され、より大きなパッケージを構成するために使用されてもよい。作成者は、主張されたパッケージや使用されたパッケージの名称を変更してはならない。

注1：CCではパッケージを評価するための個別の基準は示されていないが、そのようなパッケージがPP、PPモジュール又はSTに含まれる場合、それらはAPE、ACE又はASEの基準を用いて評価されることになる。

注2：CCパート5は、EALのような一般的に使用されるパッケージを規定し、それらは事前に定義され、PP、PPモジュールとPP構成又はST作成者が使用することができる。

機能パッケージは、PP構成が直接主張することはできず、PP構成コンポーネントの一部としなければならない。

パッケージに関する詳細情報は附属書Aに記載されている。

9.2 パッケージ種別

9.2.1 一般

パッケージは、以下のいずれかでなければならない。

— 機能パッケージ：機能コンポーネント又は要件を含むが、保証コンポーネント又は要件は含まないパッケージ、又は

— 保証パッケージ：保証コンポーネント又は要件を含むが、機能コンポーネント又は要件を含まないパッケージ。

機能と保証の両方のコンポーネント又は要件を含む混合パッケージを指定してはならない。

全てのパッケージは、以下を含まなければならない。

a) パッケージ識別：一意の名前、短い名前、バージョン、日付、スポンサー、及びCCの関連パートを示す。

b) パッケージ種別：保証パッケージ又は機能パッケージのいずれか。

c) パッケージ概要：パッケージの目的を叙述的に記述したもの。

d) 適用上の注釈：パッケージに関する追加情報を記述したもの。

e) 評価方法及び/又は評価アクティビティの識別(CEMから派生した評価方法/評価アクティビティが指定された場合)。

f) 1つ以上のセキュリティコンポーネント又は要件。

g) 拡張コンポーネントが指定されている場合、パッケージは拡張コンポーネント定義を含む。

h) パッケージに含まれる機能コンポーネント又は保証コンポーネント/要件を選択する根拠を提供するコンポーネントの根拠。

9.2.2 保証パッケージ

保証パッケージは保証コンポーネント又は要件のセットを含んでおり、それらはCCパート3から抽出されるか、拡張保証コンポーネントであるか、あるいはその両方の組み合わせである。

保証パッケージは、SPDやセキュリティ対策方針、セキュリティ機能コンポーネントや要件を含めてはならない。

保証パッケージは、PP、PPモジュール、PP構成及びSTの中で使用することができる。事前に定義された階層的な保証パッケージのセットは、CCパート5に記載されている。

例：CCパート5で定義されているEALは、CCパート3から抽出されたSARで構成されている。EALは、事前に定義されたセキュリティ保証パッケージである。

9.2.3 機能パッケージ

機能パッケージは機能コンポーネント又は要件のセットを含んでおり、それらはCCパート2から抽出されるか、拡張機能コンポーネント又は要件であるか、あるいはその両方の組み合わせである。

機能パッケージは、SPD及びそのSPDから導き出されたセキュリティ対策方針を含むことができる。パッケージがSPDを定義する場合、機能パッケージのセキュリティ対策方針が与えられなければならない。対策方針には、TOEのセキュリティ対策方針(直接根拠アプローチを用いる場合は省略される)、運用環境のセキュリティ対策方針、及びセキュリティ対策方針根拠が含まれる。

機能パッケージは、セキュリティ機能性を構成ブロックに構造化する手段として、PP、PPモジュール及びST内で使用されることがある。

機能パッケージは、他の機能パッケージへの依存性を持つことがある。そのような依存性は、機能パッケージに文書化されなければならず、PP、PPモジュール又はSTにも文書化される場合がある。

例：PPは機能パッケージAを定義し、それを含む。パッケージAは依存性を持たない。機能パッケージB、C、Dは別の場所で定義されている。パッケージDは依存性を持たないが、パッケージCはパッケージBに依存する。STは、以下のPPとパッケージの組み合わせへの適合を主張することができる。

— STは、PP(機能パッケージAを含む)への適合を主張する。

— STは、PP及び機能パッケージBへの適合を主張する。

— STは、PP及び機能パッケージB及びCへの適合を主張する。

— STは、PP及び機能パッケージDへの適合を主張する。

— STは、PP及び機能パッケージB、C及びDへの適合を主張する。

以下は許可されない。

— STは、PP及び機能パッケージCへの適合を主張する(パッケージCはパッケージBに依存するため、単独で主張することはできないので、これは許可されない)。

9.3 パッケージの依存性

パッケージは、その中に含まれるコンポーネントの依存性を全て満たすとは限らない。しかし、パッケージを含むPP、PPモジュール、PP構成又はSTによって、依存性を満たさなければならない。つまり、全ての依存性を満たすことを保証するか、依存性を満たさない理由を説明する根拠を含めることは、作成者の責任である。これについては、8.3.で説明する。

9.4 評価方法と評価アクティビティ

パッケージは、CEMから派生した評価方法/評価アクティビティを含むことができる。CEMから派生した評価方法/評価アクティビティがパッケージを評価するために使用される場合、関連するセキュリティ要件の節に次の形式のステートメントを含めることによって、これらを識別しなければならない。

「*このパッケージは、<参照>で定義された評価方法/評価アクティビティを使用することを要求する。*」

このステートメントで、*<参照>*は、関連する評価方法及び評価アクティビティの所在の識別に置き換えられる。この参照は、パッケージを含む文書に対してでも、1つ以上の別の文書に対してでもよい。

注：CCパート4は、このような派生を実行するための枠組みを規定する。

10 プロテクションプロファイル(PP)

10.1 一般

PPは一般的なTOE種別を記述するためのものである。したがって、PPは以下のように使用することができる。

— PPのTOE種別に適合するTOEのSTテンプレートとして使用する。

— TOE種別をさらに詳細化するために、他のPPのテンプレートとして使用する。

— この枠組みでは基本PPとして知られており、PPモジュールの基盤として使用する。

PPの詳細な記述は、附属書Bに記載されている。

注：STは、特定のTOEに対する要件を記述するものであり、通常、そのTOEの開発者がスポンサーとなっている。

10.2 PP概説

PPの概説は、PPの参照識別子を含まなければならない。

PPの概説は、TOE種別の記述を含むPPの概要を含まなければならない。

PPの参照識別子は、カタログの中で一意でなければならない。

例：TOE種別は「ファイアウォール」とすることができる。

詳細化したTOE種別は、「ステートフルインスペクションファイアウォール」とすることができる。

そのTOE種別に関連する特定のTOEは、「MinuteGap Firewall v18.5」とすることができる。

PPは、TOE種別の一般的な要件を記述するものであり、通常、次のような人がスポンサーとなる。

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

— TOEの開発者、又は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セキュリティ要件を指定する政府又は大企業などの組織。

10.3 適合主張と適合ステートメント

この節において、イタリック体のテキストの使用は、PPのテキストに表示しなければならないテキストそのものを示す。

PPの適合主張は、以下のとおりである。

a) PPが適合を主張するCCの関連パートの版を記載しなければならない。

b) CCパート2への適合を、以下のいずれかとして記述しなければならない。

— 「*CCパート2適合*」

そのPPの全てのSFRがCCパート2の機能コンポーネントにのみ基づいている場合、PPはCCパート2適合である。又は

— 「*CCパート2拡張*」

そのPP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、PPはCCパート2拡張である。

c) CCパート 3 への適合を、以下のいずれかとして記述しなければならない。

— 「*CCパート3適合*」

そのPPの全てのSARがCCパート3の保証コンポーネントのみに基づいている場合、PPはCCパート3適合である。又は

— 「*CCパート3拡張*」

そのPP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、PPはCCパート3拡張である。

d) 他のPPに関する適合主張を含むこともできる。

— 「*PP適合*」

PPは、他の特定のPPを満たす場合、「PP適合」である。

e) パッケージ適合の主張を含むことができる。

PPの中で、複数のパッケージを主張することができる。

パッケージの主張がなされる場合、各パッケージの主張について以下のいずれかのステートメントで構成されなければならない。

— 「*パッケージ適合*」

以下の場合、PPはパッケージに適合する。

— 機能パッケージの場合、機能パッケージの全ての構成部分(SPD、セキュリティ対策方針、SFR)が、PPの対応する部分に変更なく存在する。

— 保証パッケージの場合、そのPPのSARは、保証パッケージ内のSARと同一である。

— パッケージのSFRの選択を制限するPPは、相変わらずパッケージ適合を主張することができる。

— 「*パッケージ追加*」

以下の場合、PPはパッケージの追加を主張する。

— 機能パッケージの場合、そのPPの全ての構成部分(SPD、セキュリティ対策方針、SFR)は機能パッケージで与えられた全ての構成部分を含むが、少なくとも1つの追加のSFR又は機能パッケージのSFRよりも階層的に上位の1つのSFRがある。

— 保証パッケージの場合、そのPPのSARは、保証パッケージの全てのSARを含むが、少なくとも1つの追加のSAR、又は保証パッケージのSARよりも階層的に上位の1つのSARがある。

— 「*パッケージ調整*」

以下の場合、PPはパッケージの調整を主張する。

— 機能パッケージの場合、そのPPの全ての構成部分(SPD、セキュリティ対策方針、SFR)は機能パッケージで与えられた全ての構成部分を含むが、パッケージでの既存の選択がされているSFRに対して追加の選択項目を持ち、オプションとして、少なくとも1つの追加のSFR及び/又は機能パッケージのSFRより階層的に上位の1つのSFRがある。

— 保証パッケージ及び ST は、調整を主張(又は実行)してはならない。

PPでは、複数のパッケージを主張することができる。

PPがPPへの正確適合又は論証適合を主張する場合、PPがパッケージを追加しない限り、それらが適合を主張するPPで主張されたパッケージへの適合も主張してはならない。PPが<パッケージ>追加を主張するのは、PPが適合を主張するPPによって主張されたパッケージの他に、PPがパッケージを追加する場合のみである。

注1：PPは、PPへの完全適合を主張することはできない。

f) PPは適合主張の根拠を含まなければならない。

適合主張の根拠は、作成者が適合主張と適合ステートメントを選択した根拠と論理的根拠を記述する。

g) PPは、適合ステートメントを提供しなければならない。

適合ステートメントは、他のPP又はSTがこのPPに適合する方法を記述しなければならない：適合ステートメントは、次のいずれかでなければならない。

— 「*完全適合*」

完全適合が要求されるとPPが述べている場合、STは完全な方法でPPに適合しなければならない。つまり、適合するSTは、PPと同一のSPD及び対策方針を含み、全ての割付と選択が解決されたPPのSFRの同じセットを含まなければならない。

— 「*正確適合*」

正確適合が要求されるとPPが述べている場合、PP/STは正確な方法でPPに適合しなければならない。つまり、適合PP/STはPPのSPD、対策方針、及びSFRのスーパーセットを含まなければならない。新しい前提条件(もしあれば)がPPのSPDを弱めることはなく、全てのPPのSFRが割付及び選択を変更しないか、必要に応じて解決する。

正確適合により、適合PP/STはPPのSPD、対策方針及びSFRのセット、つまりPP/STで定義されたスーパーセットは、全てのSFRが解決されたPPのものと同一であってよい。

— 「*論証適合*」

論証適合が要求されるとPPが述べている場合、PP/STは、正確又は論証可能な方法でPPに適合しなければならない。つまり、適合PP/STは、PPのSPDのスーパーセットと同等のSPD、対策方針のセット、及びSFRのセットを含まなければならない。ただし、新しい前提条件(もしあれば)はPPのSPDを弱めず、適合PP/STのSFRのセットはPPのSFRを意味する。

論証適合では、適合するPP/STが異なるが同等のステートメントを使用することができ、また、PPで与えられたステートメントを変更せずに、正確適合の場合と同様に、単にスーパーセットを定義することができる。

注2：言い換えれば、PP/STは、PPが明示的に許可している場合にのみ、論証可能な方法でPPに適合することが許可される。

注3：PPモジュール及びPP構成は、PPへの適合を主張することはできない。詳細は、11.2及び11.3を参照のこと。

適合ステートメントには、CEMから派生した評価方法/評価アクティビティへの参照を含めることもできる。CEMから派生した評価方法/評価アクティビティがPPを評価するために使用される場合、関連するセキュリティ要件の節に次の形式のステートメントを含めることによって、これらを識別しなければならない。

「*このPPは、<参照>で定義された評価方法/評価アクティビティを使用することを要求する。*」

このステートメントで、*<参照>*は、関連する評価方法及び評価アクティビティの所在の識別に置き換えられる。この参照は、PPを含む文書に対してでも、1つ以上の別の文書に対してでもよい。

注4：PP/STは、PPに適合するかしないかのどちらかである。CCでは、「部分的」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。PPの適合ステートメント及び主張の詳細については、附属書Bを参照のこと。

10.4 セキュリティ保証要件(SAR)

CCパート3(場合によっては拡張)に準拠するPPは、TOE全体に適用されるSARのセットを定義しなければならない。

PPは、適用されるSARのセットに特徴的な名前を定義することができる。ただし、SARのセットが(追加された)事前に定義されたEAL(EAL1～EAL7)又は適用可能な外部参照で定義された(追加された)保証パッケージである場合、同じ名前を使用しなければならない。

注：事前に定義されたEALは、CCパート5に示されている。

10.5 正確適合及び論証適合に共通する追加要件

10.5.1 適合主張及び適合ステートメント

PP/STが複数のPPに対して正確適合及び論証適合のいずれかを主張する場合、PP/STは各PPに、そのPPで述べられている方法によって適合しなければならない。つまり、PP/STは、あるPPには正確適合し、他のPPには論証適合することができる。

PP/STがPPに適合するのは、PP/STがこのPPと同等かそれ以上の制約がある場合、すなわち、以下の場合である。

— PP/STを満たす全てのTOEがPPを満たし、かつ

— PPを満たす全ての運用環境はPP/STも満たす。

言い換えれば、PP/STはTOEに同等以上の要件を課し、TOEの運用環境に同等以下の条件を課さなければならない。

この一般的な記述は、PP/STの異なる構成要素、すなわちSPD、TOEのセキュリティ対策方針、環境のセキュリティ対策方針、セキュリティ機能及びSARにも当てはまる。

10.5.2 セキュリティ課題定義(SPD)

PP/STの適合根拠は、PP/STのSPDがPPのSPDと同等か、それよりも制限的であることを実証しなければならない。すなわち、以下のことを実証しなければならない。

— PP/STのSPDを満たす全てのTOEは、PPのSPDも満たす。

— PPのSPDを満たす全ての運用環境は、PP/STのSPDも満たす。

10.5.3 セキュリティ対策方針

PP/STの適合根拠は、PP/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か、それよりも制限的であること、すなわち、以下のことを実証しなければならない。

— PP/STのTOEのセキュリティ対策方針を満たす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運用環境は、PP/STの運用環境のセキュリティ対策方針も満たす。

10.6 正確適合に特有の追加要件

10.6.1 セキュリティ課題定義(SPD)に対する要件

PP/STはPPのSPDを含み、さらに追加の脅威とOSPを指定することができる。次の2項目で説明される2つの例外を除き、PP内で定義されたとおり、全ての前提条件を含まなければならない。

— PPで指定された前提条件(又は前提条件の一部)は、この前提条件(又は前提条件の一部)に対処するPPで定義された運用環境の全てのセキュリティ対策方針が、PP/STのTOEのセキュリティ対策方針に置き換えられる場合、PP/STから除外することができる。

— 新しい前提条件が、PP内のTOEのセキュリティ対策方針によって対処されることが意図されている脅威(又は脅威の一部)を軽減しない場合、及び、この前提条件がPP内のTOEのセキュリティ対策方針によって対処されることが意図されているOSP(又はOSPの一部)を満たさない場合、この新しい前提条件は、PP/ST内のPPで定義された前提条件のセットに追加してもよい。

10.6.2 セキュリティ対策方針に対する要件

PP/STは、

— PPのTOEのセキュリティ対策方針の全てを含まなければならず、追加のTOEのセキュリティ対策方針を指定することもできる。

— 次の2項目で説明される2つの例外を除き、PPで定義されたとおり、運用環境のセキュリティ対策方針の全てを含まなければならない。

— PPでの運用環境の特定のセキュリティ対策方針を、PP/STではTOEのセキュリティ対策方針として指定することができる。これは、セキュリティ対策方針の再割り当てと呼ばれる。セキュリティ対策方針がTOEのセキュリティ対策方針に再割り当てされる場合、セキュリティ対策方針の正当化は、どの前提条件/OSP又は前提条件/OSPの一部がもはや必要でないかを明確にしなければならない。

— これらの新しい対策方針が、PP内のTOEのセキュリティ対策方針によって対処されるべきである脅威(又は脅威の一部)を軽減しない場合、及び、これらの対策方針が、PP内のTOEのセキュリティ対策方針によって対処されるべきであるOSP(又はOSPの一部)を満たさない場合、追加の運用環境のセキュリティ対策方針を指定することができる。

10.6.3 セキュリティ要件に対する要件

PP/STは、

— PPの全てのSFRとSARを含まなければならない。

— 追加又は階層的に上位のSFRとSARを主張することができる。STの操作の完了は、PPのそれと内部的に一貫したものでなければならない。PP/STでは、PPのそれと同じ完了が使われるか、要件をより制限的にするものが使われる。

注：詳細化の規則が適用される。

10.7 論証適合に特有の追加要件

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、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、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、提供することができる。

PP/STは、なぜPP/STがPPと「同等又はより制限的」であると考えられるかについての根拠を含まなければならない。

10.8 完全適合に特有の追加要件

10.8.1 一般

完全適合は、PP作成者が、作成したPPに関してSTが適合を主張する内容を制御する必要がある場合に使用される。これは、PPへの適合を主張するSTが、PP作成者が考慮しなかった追加のSPD、セキュリティ対策方針又は要件を含まないことを、PP作成者が要求する場合に使用される。

適合ステートメントで完全適合を要求するPPは、オプションのSFR及びこれらのSFRをサポートするために必要なSPDエレメントを定義することができる。ST(又はPPモジュール)は、完全適合の主張を維持しながら、これらのオプションのSFR(及び必要なSPDエレメント)を要件に含めてもよい。

完全適合のPPは、他のいかなる適合種別のPPに対しても適合を主張してはならない。完全適合の種別を持つPPは、正確適合及び論証適合の種別を持つPP又はPPモジュールも含むPP構成に含めてはならない。

注：正確適合/論証適合PPと完全適合PPの両方への適合を主張することは不可能である。なぜなら、それは、完全適合PPに要件又はSPDエレメントを追加することを意味するからであり、この操作は明示的に禁止されている。

STがPPへの完全適合を主張する「単純な」ケースでは、PP作成者の意見を求める必要なく、評価中にSPD、セキュリティ対策方針、SFR、SAR間の対応が実証されるため、STが完全適合か否かの曖昧さはない。

しかし、SPDエレメント、セキュリティ対策方針、及びSFRの複数のセットを組み合わせることができる他のケースも許可される。これらのケースでは、完全適合PP作成者が自分のPPに対する適合主張を制御する能力を維持するメカニズムが必要となる。これらのメカニズムは、以下の節で説明する。

例：複雑なケースとして、PPモジュールが基本PPとしてPPを使用することを目的としている場合や、STが2つのPPへの適合を主張する場合などがある。

PPが完全適合を要求する場合、そのPPが指定するSFRとSARのみが適合するSTで許可される。これらのセキュリティ要件は、PPで指定されたSPD及びセキュリティ対策方針に関連しており、これらは適合するSTにも含まれる。完全適合PPのSFRは、(ASE_CCL.1-12のCEMに記載されているように)繰返しと詳細化をすることができる。

10.8.2 適合主張及び適合ステートメント

PPが適合ステートメントで完全適合を要求する場合、

a) PPは、他のどのPP及びPPモジュールがPPとともに適合主張に含まれることが許可されるかを述べる、併用許可ステートメントを含まなければならない。

b) STが完全適合を主張することができる全ての追加PPは、完全適合要件も持たなければならない。

c) STが適合を主張する全ての追加PPは、それぞれの併用許可ステートメントでPPを識別しなければならない。

d) PP構成を通じて主張される全ての追加PPモジュールは、それぞれの併用許可ステートメントにおいてPPを識別しなければならない。

PPモジュールは、適合ステートメントにおいてそれ自身の基本PP/PPモジュールを識別する必要はないが、PPモジュール概説において、PPモジュール基盤を識別しなければならない。

10.9 PPの使用について

PP/STが1つ以上のPP、場合によっては1つ以上のパッケージに適合すると主張する場合、そのPP/STの評価には、そのPP/STが実際に主張するPP及び/又はパッケージに適合していることを実証することが含まれる。この適合の判断の詳細は、附属書A及び附属書Bに記載されている。

これにより、次のプロセスが可能となる。

a) 特定の種別のITセキュリティ製品を取得しようとする組織は、そのセキュリティニーズをPPに記述し、このPPの評価を受けて公開する。

b) 開発者はこのPPを入手し、その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(又は既存のTOEを使用し)、STに対してこのTOEの評価を受ける。

その結果、評価済みのTOEはPPで定義された組織の要件を満たし、その組織はそれゆえTOEがセキュリティのニーズを満たしていると確信することができる。パッケージにも同様の考え方を適用できる。

10.10 複数のPPがある場合の適合ステートメントと適合主張

10.10.1 一般

CCは、STとPPの両方が複数のPPへの適合を主張することを認める。STが複数のPPへの適合を主張するケースは、11.3.3で説明する。10.10は、PPが複数のPPへの適合を主張するケースを扱う。

10.10.2 正確適合及び論証適合が指定されている場合

PPが複数のPPへの適合を主張できるようにすることで、PPのチェーンを構築することができ、チェーンの中の各PPは前のPPに基づいている。

例：集積回路用とスマートカードOS用のPPを使用して、両者への適合を主張するスマートカードPP(IC及びOS)を構成することができる。次に、このスマートカードPPを使用して、例えば、タコグラフ・カード、ペイメント・カード、電子パスポートなど、様々なユースケースのための特定のPPを開発することができる。そして開発者は、これらのPPのいずれかに適合するSTを構成することができる。

10.10.3 完全適合が指定されている場合

PPは、他のPP又はPPの組み合わせに対する完全適合を主張してはならない。

注：そのような機能性の組み合わせが必要な場合、適合を主張したいPPからなるPP構成を作成することによって達成できる。

11 モジュール式要件の構成

11.1 一般

TOEのセキュリティ機能のモジュール式記述を可能にするために、STはPPの代わりにPP構成への適合を主張することができる。このようなPP構成は、PPモジュール基盤を含むPPとPPモジュールのセットで構成される。

PP構成は、単一保証評価又はマルチ保証評価のいずれかに対応するように構成することができる。単一保証評価では、PP構成の全コンポーネントに保証要件の単一のセットが適用される。マルチ保証評価では、PP構成の全コンポーネントに適用される保証要件の単一のグローバルなセットが存在するが、さらに各コンポーネント(PP又はPPモジュール)は、自身が対象となる保証要件の独自のセットを有する。以下の節では、これら2つの評価手法の内容に関する詳細を示す。これらの手法を用いた実際の評価については、13章で説明する。

11.2 PPモジュール

11.2.1 一般

PPモジュールは、SPDエレメント、TOEと運用環境のセキュリティ対策方針、及びSFRの内部的に一貫したセットであり、1つ以上のPPと場合によっては他のPPモジュールの文脈で定義される。

PPとは異なり、PPモジュールは、このTOE種別の製品全てに対して一律に要求されるわけではない、所定のTOE種別のセキュリティ機能に対処する。

PPとは異なり、PPモジュールはPP構成においてのみ使用されなければならない。PP/STはPPモジュールへの適合を直接主張することはできない。

例：TOE種別の全ての製品に一律に要求できない機能の例として、バイオメトリクスを用いた認証、Bluetoothセキュリティ機能、及び無線LANクライアントがある。

11.2.2 PPモジュール基盤

あるPPモジュールは、PP及び場合によっては他のPPモジュールのセットからなる1つ以上のPPモジュール基盤を指定する。当該PPモジュールがPP構成で使用されるときはいつでも、そのPPモジュール基盤の1つが必要である。10章及び附属書Bを参照のこと。

11.2.3 PPモジュールの要件

11.2.3.1 一般

PPモジュールは、参照識別子で識別しなければならない。

PPモジュールの参照識別子は、カタログ内で一意でなければならない。

PPモジュールは、PP構成においてPPモジュールとともに使用する必要がある1つ以上のPPモジュール基盤を定義しなければならない。

PPモジュールは、そのPPモジュール基盤のそれぞれに関連するTOE種別を特定しなければならない。

PPモジュールは、新しいSPDエレメントや対策方針を導入することができ、また、PPモジュール基盤のSPDエレメント又は対策方針のいくつかを詳細化することもできる。

PPモジュールは、PPモジュール基盤のSFRを詳細化した、又は新規のSFRの空でないセットを定義しなければならない。

あるPPモジュールを含むPP構成への適合を主張するSTは、そのPPモジュールのSPDエレメント、セキュリティ対策方針及びSFRを、PP構成に属するPPモジュール基盤のものと合わせて含まなければならない。

注1：PPモジュールで定義されたTOE種別は、そのPPモジュール基盤の各々で定義されたTOE種別を補足できる。

PPモジュールは、PPモジュール及びそのPPモジュール基盤の各々で定義されたエレメントを合わせたものが矛盾を招かないことを保証する一貫性根拠を提供しなければならない。

注2：直接根拠PPモジュールでは、TOEのセキュリティ対策方針は含まれない。

PPモジュールの評価は、それだけでは意味がない。PPモジュールは、PP構成の一部として、少なくとも1つのPPモジュール基盤とともに評価されなければならない。

PPモジュールに関する詳細情報は、C.1.に記載されている。

11.2.3.2 直接根拠

PPモジュールは、そのPPモジュール基盤も直接根拠アプローチを使用する場合に限り、直接根拠アプローチを使用することができる。

11.2.3.3 適合主張及び適合ステートメント

この節において、イタリック体のテキストの使用は、PPモジュールのテキストに表示しなければならないテキストそのものを示す。

PPモジュールの適合主張は、以下のとおりである。

a) PPモジュールが適合を主張するCCの関連パートの版を記載しなければならない。

b) CCパート2への適合を以下のいずれかとして記述しなければならない。

— 「*CCパート2適合*」

注1：PPモジュールの全てのSFRがCCパート2の機能コンポーネントにのみ基づいている場合、PPモジュールはCCパート2適合である。

又は

— 「*CCパート2拡張*」

注2：PPモジュールの少なくとも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、PPモジュールはCCパート2拡張である。

c) 機能パッケージに関してなされる適合主張を含むことができる。PPモジュールは、1つ以上の機能パッケージを主張することができる。

注 3：PP モジュールは、PP モジュール基盤の PP 又は PP モジュールのいずれかがすでに適合を主張している機能パッケージへの適合を主張してはならない。この規則の例外は、PP モジュールがその機能パッケージを PP モジュール基盤のインスタンスとして追加又は調整する場合である。この場合、PP モジュールはその機能パッケージをパッケージ適合主張のステートメントの中で「パッケージ追加」又は「パッケージ調整」(必要に応じて)として主張する。

機能パッケージの主張がなされる場合、パッケージごとに以下のいずれかの主張で構成されなければならない。

— 「*パッケージ適合*」

PPモジュールは、SPD、セキュリティ対策方針、及びSFRを含む、機能パッケージの全ての構成部分が、PPモジュールの対応する部分に変更なく存在する場合、パッケージに適合する。

— 「*パッケージ追加*」

PPモジュールに含まれるSPD、セキュリティ対策方針、及びSFRを含む機能パッケージの全ての構成部分が、機能パッケージで与えられたものと同一であるが、追加又は機能パッケージのSFRよりも階層的に上位の少なくとも1つのSFRを含む場合、PPモジュールはパッケージの追加を主張する。

— 「*パッケージ調整*」

PPモジュールに含まれるSPD、セキュリティ対策方針、及びSFRを含む機能パッケージの全ての構成部分が、機能パッケージで与えられたものと同一であるが、パッケージの既存の選択を持つSFRの追加の選択項目があり、オプションとして少なくとも 1 つの追加SFR及び/又は機能パッケージのSFRよりも階層的に上位の1つのSFRを持つ場合、PPモジュールはパッケージの調整を主張する。

d) CCパート3に関する適合主張を含まなければならない。CCパート3への適合主張は、以下のいずれかでなければならない。

— 「*CCパート3適合*」

そのPPモジュール内の全てのSARがCCパート3の保証コンポーネントのみに基づいている場合、PPモジュールはCCパート3適合である。

又は

— 「*CCパート3拡張*」

そのPPモジュールの少なくとも1つのSARが、CCパート3の保証コンポーネントに基づかない場合、PPモジュールはCCパート3拡張である。

— PPモジュールの適合主張は、保証パッケージに関する適合主張を含むことができる。PPモジュールは、1つ以上の保証パッケージを主張することができる。主張する保証パッケージ間の重複は許される。構造上、階層的に上位のSARが他よりも優先され、PP構成に適用される。

正確及び論証可能な場合、PPモジュールは、例えばALCベースのパッケージとADVベースのパッケージのように、複数の保証パッケージへの適合を主張することができる。

パッケージの主張がなされる場合、各パッケージについて以下の主張のいずれかで構成されなければならない。

— 「*パッケージ適合*」

PPモジュールは、保証パッケージの全ての構成部分が変更されることなくPPモジュールに存在する場合、保証パッケージに適合する。

— 「*パッケージ追加*」

PPモジュールは、PPモジュールに含まれている保証パッケージの全ての構成部分が保証パッケージに与えられたものと同一であるが、追加又はパッケージに含まれているSARよりも階層的に上位の少なくとも1つのSARを含まなければならない場合、保証パッケージの拡張を主張する。

PPモジュールの適合ステートメントは、以下のとおりである。

e) PP構成の一部として、STがこのPPモジュールに適合する方法を記述しなければならない適合ステートメントを提供しなければならない。適合ステートメントは、以下のいずれかでなければならない。

— 「*完全適合*」

PPモジュールは、その全てのPPモジュール基盤が完全適合である場合にのみ、完全適合を要求しなければならない。STは、PP構成の一部として、PPモジュールに完全適合しなければならない。さらに

— 併用許可ステートメントは、(PPモジュール基盤のセットにはない)他のどのPP及びPPモジュールが、そのPPモジュールとともにPP構成で使用を許可されるかを述べなければならない。

— 定義されるPPモジュールのPPモジュール基盤にある各PP及びPPモジュールと、PP構成においてPPモジュールとともに指定することが許可されている追加PP及びPPモジュール(PPモジュール基盤にないもの)の全てが、それぞれの併用許可ステートメントで定義されるPPモジュールを識別しなければならない。

— また、参照される全てのPPモジュール基盤は、完全適合を要求しなければならない。

— 「*正確適合*」

PPモジュールが正確適合を要求されると記載されている場合、STは、PP構成の一部として、PPモジュールに正確な方法で適合しなければならない。

— 「*論証適合*」

PPモジュールが論証適合を要求すると述べている場合、STはPP構成の一部として、PPモジュールに対して正確又は論証可能な方法で適合しなければならない。PPモジュールが明示的にこれを許可する場合、STは、PP構成の一部として、論証可能な方法でのみPPモジュールに適合することが許可される。

注1：PPモジュール基盤が全て正確適合又は論証適合を要求するわけではないが、PPモジュールは、正確適合又は論証適合を要求することができる。論証適合と正確適合の組み合わせは、PP構成の評価で確認される。

注2：正確適合又は論証適合を明示的に宣言することにより、スポンサーは各PPモジュールにおいて、そのPPモジュール基盤から独立して、最も適切なステートメントを作成することができる。

注3：PPモジュール基盤は、PPモジュールの適合ステートメントで指定する必要はない。

f) CEMから派生した評価方法/評価アクティビティへの言及を含むこともできる。

CEMから派生した評価方法/評価アクティビティがPPモジュールを評価するために使用される場合、関連するセキュリティ要件の節に次の形式のステートメントを含めることによって、これらを識別しなければならない。

「*このPPモジュールは、<参照>で定義される評価方法/評価アクティビティを使用することを要求する。*」

このステートメントで、*<参照>*は、関連する評価方法及び評価アクティビティの所在の識別に置き換えられる。この参照は、PPモジュールを含む文書に対してでも、1つ以上の別の文書に対してでもよい。

PPモジュールの適合種別、主張及び適合ステートメントに関する詳細な情報及び要件については、附属書Cを本書の各章と合わせて使用しなければならない。

11.2.3.4 保証要件

PPモジュールは、PPモジュールで定義されたTSFに適用されるSARのセットを定義しなければならない。これは、PPモジュール基盤から引き継ぐか、PPモジュール作成者が明示的に宣言することができる。

PPモジュールは、そのSARのセットに特徴的な名前を定義することができる。ただし、PPモジュールが(追加された)事前に定義されたEAL(EAL1～EAL7)又は適用可能な外部参照で定義された(追加された)保証パッケージを宣言する場合、又はSARのセットをそのPPモジュール基盤から引き継ぐ場合は、同じ名前が使用されなければならない。

PPモジュールは、そのSARセットの内部的に一貫したものであることを正当化する保証根拠を提供しなければならない。すなわち、

— PPモジュールのSPDに定義された脅威モデルに関するSARセットの一貫性。

— PPモジュールがSARのセットをPPモジュール基盤から引き継いでいない場合、PPモジュールのPPモジュール基盤で定義された全てのSARセットとのSARセットの一貫性。

注1：一貫性とは、矛盾がないことを意味する。SARとSPDの間の矛盾の例は、高度な技術を持つ脅威エージェントを、定義上これらの脅威エージェントを考慮できない低いAVA_VANレベルと一緒に考慮することである。

注2：PPモジュールの保証根拠は、PPモジュールで定義されたSARのセットが、PPモジュールとそのPPモジュール基盤(共有資産がある場合)で共有される資産に期待されるセキュリティを損なうことがないことを保証する。

注3：PPモジュールレベルでの保証根拠は、PP構成レベルでの保証要件の一貫性を保証するために寄与するが、十分ではない。11.3.2.4を参照のこと。

注4：保証根拠は、内部的に一貫したものを実証するために、PPモジュール内のSARのセットと事前に定義されたEALの関係に依存することができる。

11.3 PP構成

11.3.1 一般

PP構成は、適合を主張することができる一連の要件を構築するための仕様である。

PP構成は、一般的なTOE種別を記述することを意図している。

— PP構成は、PP構成のTOE種別に合致するTOEのSTテンプレートとして使用することができる。

— PP構成は、他のPP構成、PP又はPPモジュールのテンプレートとして使用することはできない。

PP構成は、PP及びPPモジュール(PP構成のコンポーネント)のセットを含み、PP/PPモジュールを介した間接的な場合を除き、いかなる機能パッケージへの適合も主張することはできない。PP構成は、SARを含み、保証パッケージへの適合を主張することができる。

2種類のPP構成が識別され、それぞれ構築に関する要件が異なり、消費者(リスク所有者)のニーズに応じて適用される。これらは以下のとおりである。

— 単一保証PP構成：これは、PP構成のコンポーネントに適用されるSARのセットが同一である構成種別を記述している。

— マルチ保証PP構成：これはPP構成のコンポーネントのSARが同一でない構成種別を記述している。

11.3.2 PP構成に対する要件

11.3.2.1 一般

PP構成は、参照で識別しなければならない。

PP構成の参照識別子は、カタログ内で一意でなければならない。

PP構成は、参照によってPP構成を構成する全てのPP及びPPモジュールを一意に識別するリストである、PP構成コンポーネントステートメントを定義しなければならない。PP構成は、1つのPP及び少なくとも別のPP構成コンポーネントを含まなければならない。PPモジュール基盤の1つがPP構成にも含まれている限り、PPモジュールを含んでもよい。関連するPPモジュールがないPPを含んでいてもよい。

PP構成は、それが適用されるTOE種別を定義しなければならない。

PP構成には、そのコンポーネントで定義されたSPD、セキュリティ対策方針、SFR及び機能パッケージが参照により正確に含まれる。追加エレメントの指定は、そのコンポーネントの1つで行わなければならない。

PP構成は、そのコンポーネントで定義されたエレメントを合わせたものが矛盾を招かないことを保証する一貫性根拠を提供しなければならない。

マルチ保証PP構成は、そのコンポーネントで定義されるサブTSFの観点からTSFの構成を記述しなければならない。また、各サブTSFに対して、対応するコンポーネントと一貫したSARのセットを定義しなければならない。

注：異なるSARのセットを持つ1つのPPと1つのPPモジュールを含むマルチ保証PP構成の場合、TSFの構成は以下のとおりである：TSFはPPとPPモジュールに定義されたSFRを合わせたものであり、PPのTSF及びPPモジュールのTSFから成る2つのサブTSFが存在する。2つのサブTSFを定義する2つのPPで構成されるPP構成も同じ構成である。

マルチ保証PP構成に含まれるサブTSFは、一部重複する可能性がある。このことは、適用される保証要件に影響を与えない。各サブTSFは、それ自身のSARのセットに対して評価しなければならない。つまり、重複する部分は、複数の保証要件に対して評価される可能性がある。

PP構成は、以下のとおりである。

— B.5及びC.2.3に記述された直接根拠アプローチの文脈で使用することができる。この場合、PP構成の全てのコンポーネントは直接根拠アプローチも使用しなければならない。

— 本書で記述された以上の追加内容を含んではならない。

11.3.2.2 コンポーネントステートメント

PP構成は、以下のとおりである。

— PP構成の全コンポーネントをコンポーネントステートメントで識別しなければならない。コンポーネントステートメントは、1つのPP及び少なくとも別のコンポーネントを含まなければならない。

注1：コンポーネントステートメントについては、C.3.3.でより詳細に記述されている。

— 他のPP構成への適合を主張してはならない。

注2：これを望む場合、両方のPP構成からの全てのコンポーネントを1つの新しい定義されたPP構成に直接含めることによって、その効果を達成することができ、そこで完全適合をチェックし、維持することができる。

— PP構成に含まれる全てのPPモジュールのPPモジュール基盤を含まなければならない。PPモジュールがPPモジュール基盤の別のセットを定義する場合、これらのセットのうち1つのみ、PP構成に使用されなければならない。

— PPモジュールのPPモジュール基盤よりも多くのPPを選択することができる。

— 単一保証PP構成の場合、PP構成で定義された各コンポーネントに対応するサブTSFを識別することができる。

— マルチ保証PP構成の場合、PP構成で定義された各コンポーネントに対応するサブTSFを識別しなければならない。

完全適合を要求するPP構成では、全てのPP構成コンポーネントは、それぞれの併用許可ステートメントで互いを指定しなければならない。

併用許可ステートメントに記載する例外として、PPモジュールは、そのPPモジュール基盤に含まれるPP又はPPモジュールを併用許可ステートメントに記載してはならない(それらは、PPモジュールの基盤であるという事実によって、明示的に許可されているため)。

11.3.2.3 適合主張及び適合ステートメント

この節において、イタリック体のテキストの使用は、PP構成のテキストに表示しなければならないテキストそのものを示す。

PP構成の適合主張は、以下のとおりである。

a) PP構成コンポーネントが適合を主張するCCの関連パートの版を記載しなければならない。

b) CCパート2(SFR)への適合を、以下のいずれかとして記述しなければならない。

— 「*CCパート2適合*」

PP構成内の全てのPP及びPPモジュールがCCパート2適合である場合、PP構成はCCパート2適合である。

又は

— 「*CCパート2拡張*」

少なくとも1つのPP又はPPモジュールが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、PP構成はCCパート2拡張である。

c) CCパート3(セキュリティ保証要件)への適合を、次のいずれかとして記述しなければならない。

— 「*CCパート3適合*」

PP構成は、そのコンポーネントから単純に引き継がれる可能性があるそのPP構成の全てのSARが、CCパート3の保証コンポーネントのみに基づいている場合、CCパート3適合である。
又は、

— 「*CCパート3拡張*」

PP構成は、そのコンポーネントから単純に引き継がれる可能性があるそのPP構成の少なくとも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拡張である。

d) 保証パッケージ適合の主張を含むことができる。

PP構成では、1つ以上のパッケージを主張することができる。保証パッケージの主張を行う場合、各パッケージの主張について、次のいずれかのステートメントで構成しなければならない。

— 「*パッケージ適合*」

PP構成は、そのコンポーネントから引き継がれる可能性があるPP構成のSARが保証パッケージのSARと同一である場合、保証パッケージに適合する。

— 「*パッケージ追加*」

PP構成は、次の場合、保証パッケージの追加を主張する。そのコンポーネントから引き継がれる可能性があるそのPP構成のSARは、保証パッケージの全てのSARを含むが、少なくとも1つの追加のSAR又は保証パッケージのSARより階層的に上位の1つのSARがある。

e) 機能パッケージ適合の主張を含めてはならない。機能パッケージは、PP構成のコンポーネントによって主張されてもよい。

f) 他のPP構成、PP、PPモジュールに関する適合主張を含めてはならない。

PP構成は、STがPP構成に適合しなければならない方法を記述した適合ステートメントを、以下のように提供しなければならない。

g) 全てのPPとPPモジュールが同じ適合種別であるPP構成では、適合ステートメントは、単一の適合種別、すなわち、次のうちの1つを提供しなければならない。

— 「*完全適合*」

PP構成に完全適合が要求されると記載されている場合、STはPP構成に対して完全な方法で適合しなければならない。

— 「*正確適合*」

PP構成に正確適合が要求されると記載されている場合、STはPP構成に対して正確な方法で適合しなければならない。

— 「*論証適合*」

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

h) PP及びPPモジュールが全て同じ適合種別を要求しないPP構成の場合、適合ステートメントは、PP構成を構成するPP及びPPモジュールのそれぞれが要求する適合種別のリストを提供しなければならない。STは、それぞれのPPとPPモジュールに対してそれらが要求する方法で適合することにより、PP構成に適合しなければならない。

注：これは、正確適合及び論証適合にのみ適用される。PP構成では、完全適合と他の適合種別との組み合わせは許可されないためである。

複数の適合の互換性は、異なる適合を要求する複数の PP への適合を ST が主張する場合と同様に、ST 評価で検証されなければならない。

i) CEMから派生した評価方法/評価アクティビティの参照も含むことができる。CEMから派生した評価方法/評価アクティビティがPP構成に関連する場合、適合ステートメントは、次の形式のステートメントも含まなければならない。

「*このPP構成は、<参照>で定義された評価方法/評価アクティビティを使用することを要求する。*」

このステートメントで、*<参照>*は、関連する評価方法及び評価アクティビティの所在の識別に置き換えられる。この参照は、PP構成そのものに対してでも、1つ以上の別の文書に対してでもよい。

注1：1つ以上のPP構成コンポーネントに適用される追加のEM/EAの指定は、正確適合又は論証適合の種別のPP構成にのみに許可される。

注2：C.2.2.5で扱う、完全適合の場合のPPモジュールの適合ステートメントには、意味がある

11.3.2.4 保証要件

PP構成は、適用される保証要件及び関連する根拠が定義されたSARステートメントを提供しなければならない。

単一保証PP構成は、全てのPP構成コンポーネントに対して、1組のSARを定義しなければならない。完全適合の場合、このSARのセットは、個々のPP構成コンポーネントで宣言されたものと同一でなければならない。正確適合及び論証適合の場合、このSARのセットは、個々のPP構成コンポーネントで宣言されたものと同一であるか、又は追加されなければならない。

マルチ保証PP構成は、以下のことを定義しなければならない。

— TOE全体に適用されるグローバルなSARのセット。完全適合の場合、このSARのセットは、個々のPP構成コンポーネントのSARの共通サブセットと同一でなければならない。正確適合及び論証適合の場合、このSARのセットは、個々のPP構成コンポーネントのSARの共通サブセットと同一であるか、追加されるものでなければならない。

— 各サブTSFについて、適用されるSARのセット。完全適合の場合、このSARのセットは、サブTSFのPP構成コンポーネントで宣言されたSARのセットと同一でなければならない。正確適合及び論証適合の場合、サブTSFのPP構成コンポーネントで宣言されたSARのセットと同一であるか、追加されるものでなければならない。

PP構成は、SARステートメントを定義するために、CCパート5で定義された事前に定義されたEAL(EAL1～EAL7)、外部参照で定義された保証パッケージ、及び/又はPP構成自体で定義されたSARを使用できる。

注1：マルチ保証評価では、事前に定義された複数のEALを適用することができる。しかし、一般的なモデルのPPと同じ理由で、PP構成は、事前に定義されたEALとは異なるSAR、及び/又は拡張SARを含むSARのセットを主張することができる。

PP構成は、TOE全体及び各サブTSFに適用されるSARのセットについて、特徴的な名前を定義することができる。ただし、(追加された)事前に定義されたEAL、又はPP構成のコンポーネントの1つ又は別の外部参照で定義された(追加された)保証パッケージを使用する場合、同じ名前を使用する必要がある。

マルチ保証PP構成は、以下の保証の根拠を提供しなければならない。

— PP構成内のPP及びPPモジュールのSPDで定義された脅威モデルに関するグローバルなSARのセットの一貫性、

— グローバルなSARのセット及びサブTSFのSARの全てのセットの相互の一貫性。

完全適合の場合のグローバルなSARのセットの構築において、サブTSFが階層的に異なるSARを指定する場合、マルチ保証PP構成の作成者は、階層的に最も下位のSARを選択する。例えば、ADV_FSP.1、ADV_FSP.2、ADV_FSP.3の3つのサブTSFがそれぞれ存在する場合、グローバルなSARのセットにはADV_FSP.1が含まれる。しかし、サブTSFの1つにADV_FSPコンポーネントが含まれていない場合、ADV_FSPはグローバルなSARのセットには含まれない。正確/論証適合の場合には、マルチ保証PP構成の作成者は、(ADV_FSPコンポーネントを定義していないサブTSFが存在する場合で

も)保証の根拠が一貫している限り、ADV_FSP.1又はより高いコンポーネントを選択して、そのサブTSFの一部に対する保証要件を追加することができる。

注2：ほとんどの場合(及び完全適合の場合には常に)、グローバルなSARのセットは、全てのサブTSFに適用される共通のSARのセットとして構築することができる。しかし、一般モデルにおけるSTの場合と同様に、(正確又は論証適合の種別の)PP構成は、追加又はより高いSARを要求することができる。PP構成の評価は、異なるSARのセットを定義する2つ以上のPPへの適合の一般モデルと同様に、及びSTが適合を主張するPP構成に定義されたSARのセットを拡張することができるマルチ保証STのアプローチと同様に、主張の一貫性を保証する。

注3：PP構成は、グローバルなSARのセット/保証パッケージとして、全てのサブTSFに適用される共通のSARのセットに含まれるものより少ない保証要件を主張することはできない。

注4：PP構成の保証根拠は、複数のSARのセットが、PP構成のPPとPPモジュール間で共有される資産に期待される安全性を損なわないことの保証に寄与している。PP構成の保証根拠は、PP及びPPモジュールで示された保証根拠に依存及び/又は再利用している。

完全適合のPP構成では、(PP構成による)各サブTSFのSARの追加は許可されない。

もし、追加SARが指定された場合、又はSARが階層的に上位のSARに置き換えられた場合、PP構成のコンポーネントが要求する派生した評価方法/評価アクティビティは、PP構成が要求する評価方法/評価アクティビティを実証するために、保証根拠の中で以下のように対処されなければならない。

— EM/EAは依然として適切である、すなわち、新しいSARはコンポーネントのEM/EA及びそれらが提供する保証に影響を及ぼさない。又は、

— EM/EAは、コンポーネントの元のEM/EAに対する定義された詳細化によって対処される。その結果得られる、PP構成に要求されるEM/EAは、そのコンポーネントに適用される元のEM/EAと同じかそれ以上の保証を生成する。又は、

— EM/EAは、追加のEM/EAによって補完される。その結果得られるEM/EAは、コンポーネントに適用される元のEM/EAと同じかそれ以上の保証を生成する。

例1：下位階層のSARのための証拠資料の検査であったアクティビティが、階層的に上位のSARのために追加テストが必要な場合、元の証拠資料評価アクティビティを、テストを要求する追加の評価アクティビティで補完することができる。

例2：図5に、1つのPP(A)と2つのPPモジュール(XとY)を持つマルチ保証PP構成の例を示す。これは、SAR_C、すなわちPP構成コンポーネントA、X、Yのそれぞれの共通のSARのセットからなるTOE全体のグローバルなSARのセットのデフォルトの構成を示している。例では、A、X、Yで定義されたサブTSFに適用されるSARのセットも同様に変更されない。

注5：規則では、SARのセットの追加を許可している。

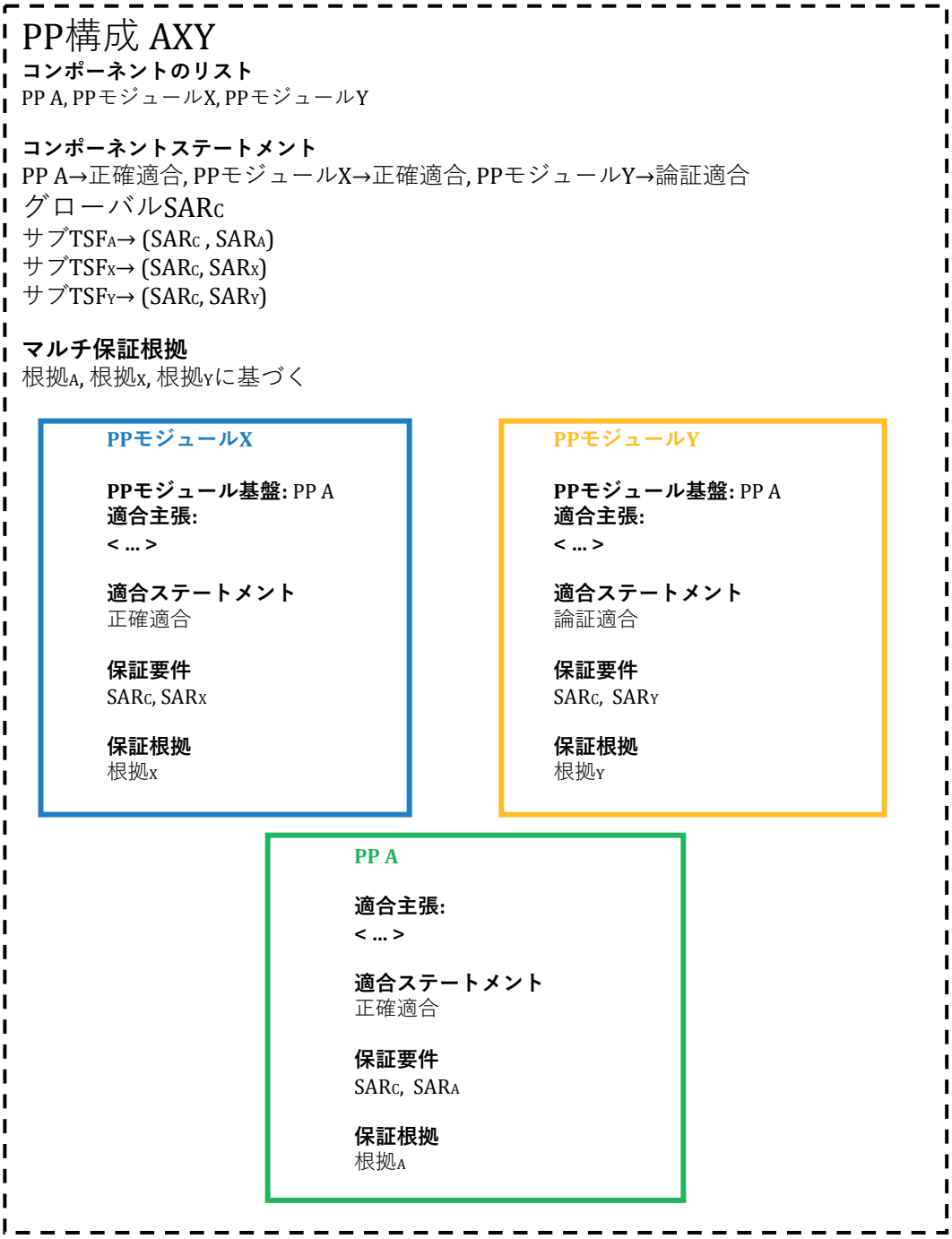


図5 — PP構成の例

11.3.3 PP構成の使用方法

図6に単一保証とマルチ保証のPP構成の使用方法を示す。図7は、PP構成のコンポーネントの詳細を示す。図8にPP、PP構成、STの評価に使用される保証クラスを示す。

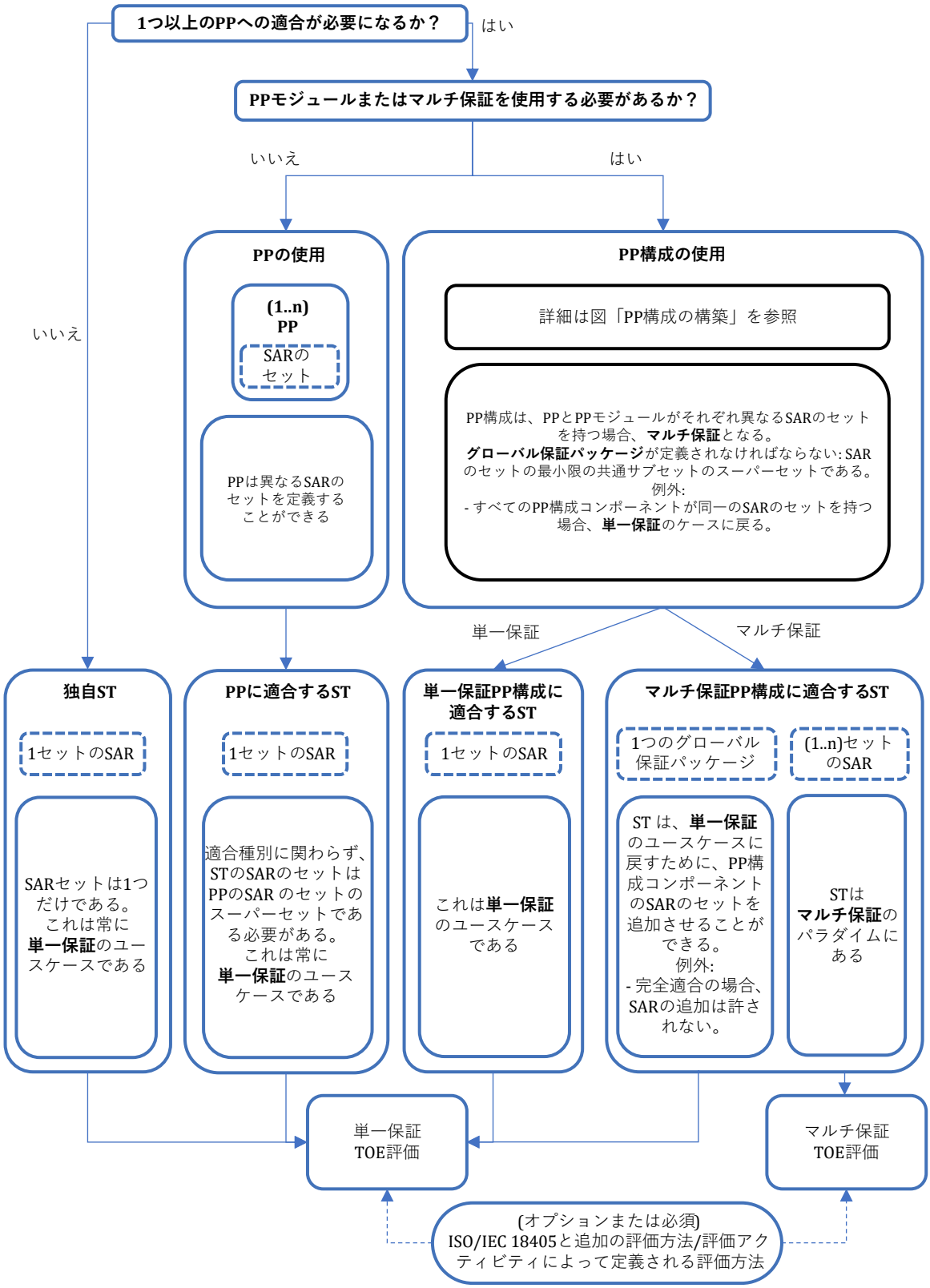
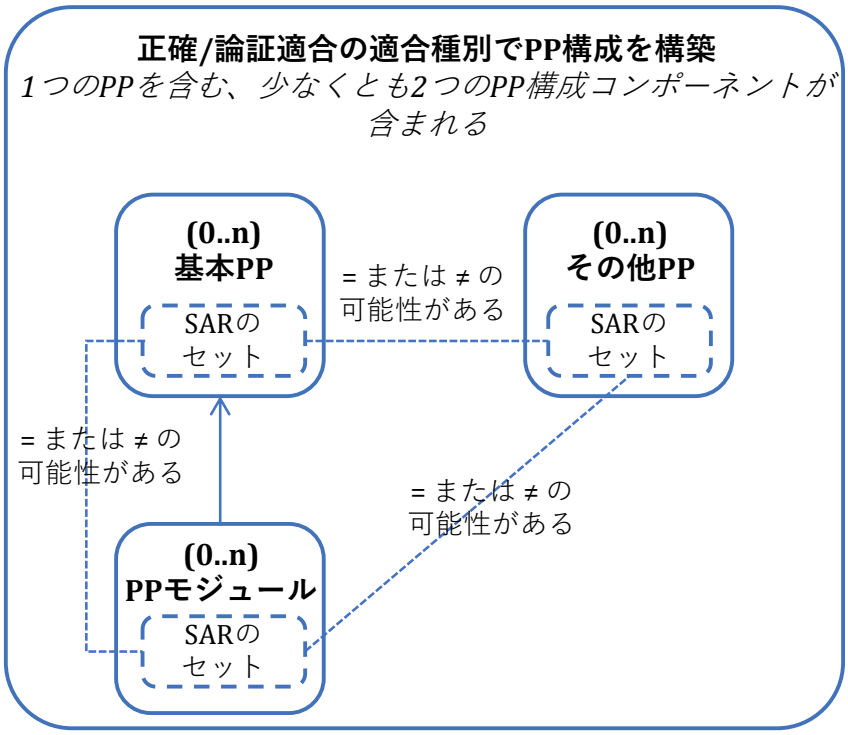


図6 — 単一及びマルチ保証PP構成の使用方法



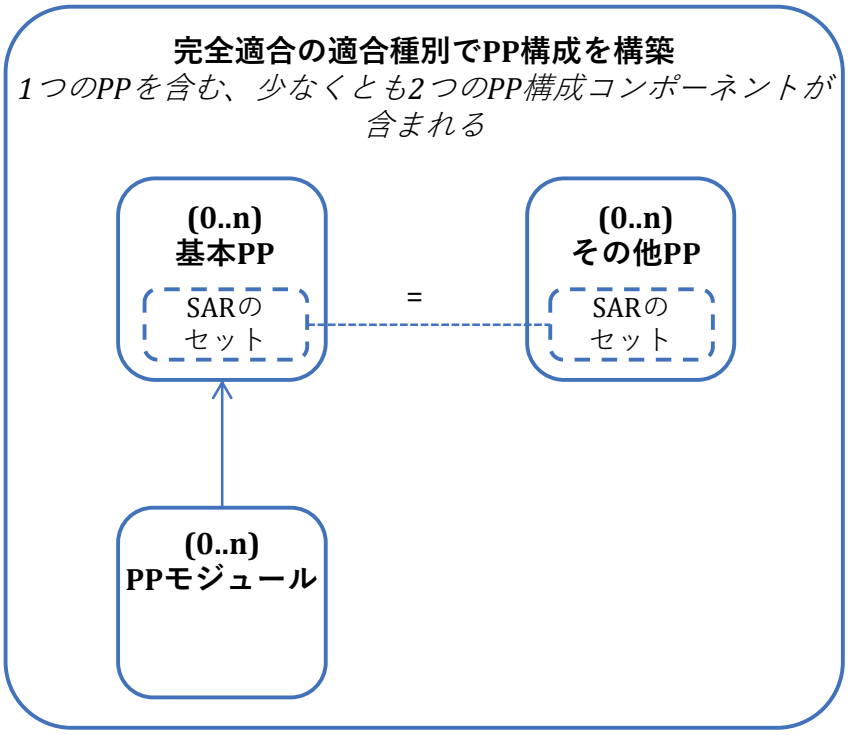


図7 — PPコンポーネントの統合

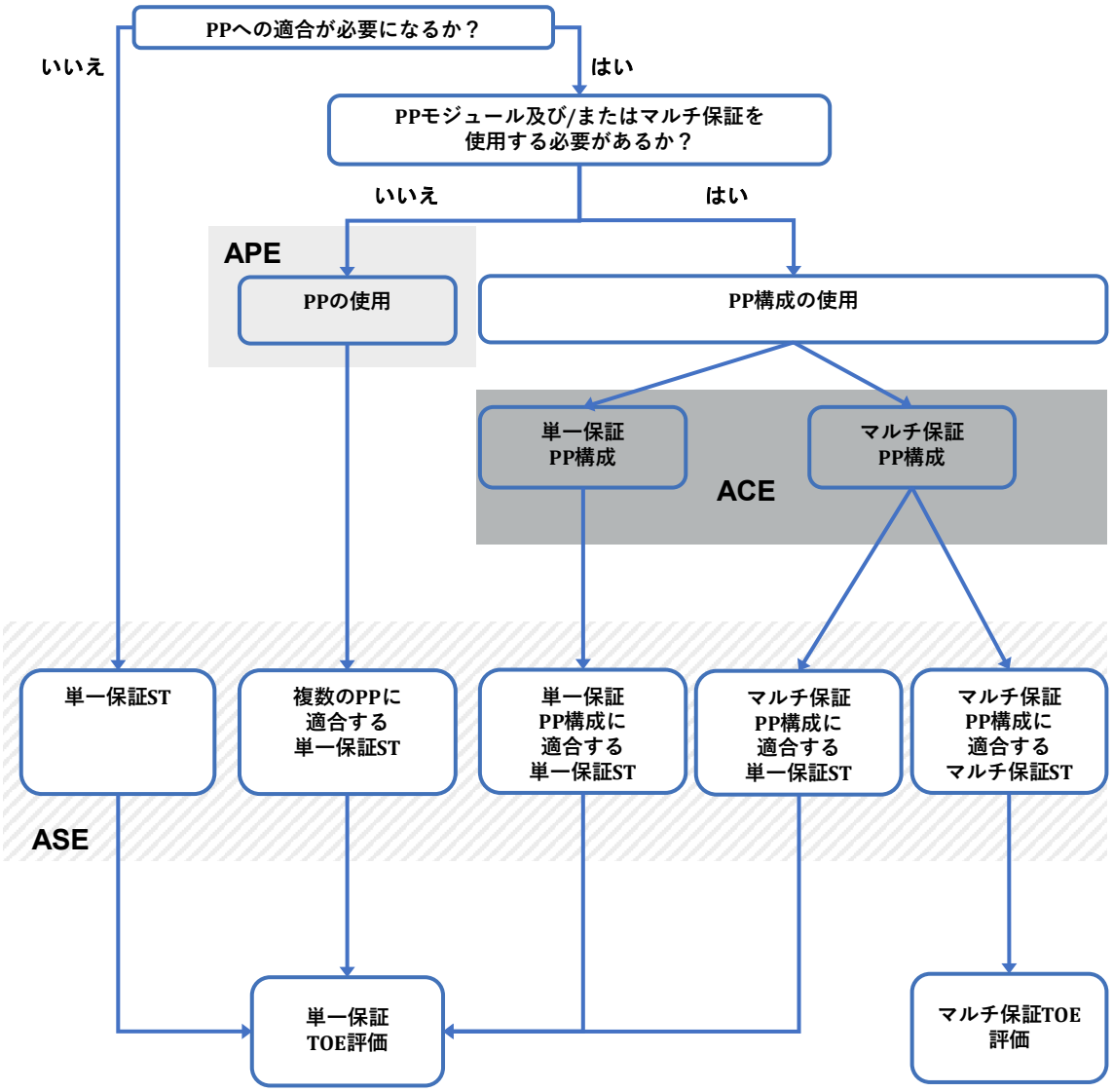


図8 — PP、PP構成、STの評価に使用される保証クラス

12 セキュリティターゲット(ST)

12.1 一般

STは、特定のTOE、TOEの評価に適用される適合主張、対処すべきセキュリティ課題、TOE及びその運用環境のセキュリティ対策方針、主張されたセキュリティ課題の解決に適用されるセキュリティ要件、及びTOEを評価のために十分に記述するために必要な追加資料を記述した文書である。STは一般に、特定のTOEに関連するTOE種別のセキュリティ課題及びセキュリティ要件を記述したPP又はPP構成に基づく。

STは通常、開発者によって作成され、STの対象読者には評価者、認証機関、評価済みのTOEのエンド利用者が含まれる。

STに関する詳細な情報については、附属書Dを本書の各章と合わせて使用しなければならない。

12.2 適合主張及びステートメント

この節において、イタリック体のテキストの使用は、STのテキストに表示しなければならないテキストそのものを示す。

STの適合主張は、以下のとおりである。

a) STが適合を主張するCCの関連パートの版を記載しなければならない。

b) CCパート2(SFR)への適合を、以下のいずれかとして記述しなければならない。

— 「*CCパート2適合*」

STの全てのSFRがCCパート2の機能コンポーネントのみに基づいている場合、STはCCパート2適合である。又は

— 「*CCパート2拡張*」

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、STはCCパート2拡張である。

注1：TOEがSTに対して成功裏に評価された場合、STの適合主張はそのTOEにも当てはまる。したがって、TOEはCCパート2適合を主張することもできる。

c) CCパート3(セキュリティ保証要件)への適合を、以下のいずれかとして記述しなければならない。

— 「*CCパート3適合*」

そのSTの全てのSARがCCパート3の保証コンポーネントのみに基づいている場合、STはCCパート3適合である。又は

— 「*CCパート3拡張*」

そのST内の少なくとも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、STはCCパート3拡張である。

d) パッケージに関する適合主張を含むことができる。

パッケージ適合の主張がなされる場合、各パッケージについて以下のいずれかの主張で構成されなければならない。

— 「*パッケージ適合*」

以下の場合、STはパッケージに適合する。

— 機能パッケージの場合、機能パッケージの全ての構成部分(SPD、セキュリティ対策方針、SFR)が、STの対応する部分に変更なく存在する。

— 保証パッケージの場合、そのSTのSARは、保証パッケージ内のSARと同一である。

— 「*パッケージ追加*」

以下の場合、STはパッケージの追加を主張する。

— 機能パッケージの場合、機能パッケージの全ての構成部分(SPD、セキュリティ対策方針、SFR)がSTの対応する部分に存在するが、STは少なくとも1つの追加SFR又はパッケージ内のSFRよりも階層的に上位の1つのSFRを含む。

— 保証パッケージの場合、STは保証パッケージの全てのSARを含むが、少なくとも1つの追加SAR又は保証パッケージのSARよりも階層的に上位の1つのSARを含む。

— 「*パッケージ調整*」

STは、調整を主張又は実行してはならない。

STでは、複数のパッケージを主張することができる。

STがPPへの完全適合を主張する場合、PPが主張するパッケージを含む、いかなるパッケージへの適合も主張してはならない。

STがPPへの正確適合又は論証適合を主張する場合、STがPPで主張されたパッケージを追加しない限り、PPで主張されたパッケージへの適合も主張してはならない。つまり、PPはパッケージを<パッケージ>適合、<パッケージ>追加、<パッケージ>調整として主張することができるが、STが自らPP内のパッケージの適合/追加/調整バージョンを追加しない場合、STはパッケージへの適合を主張しないことになる。STが<パッケージ>追加を主張するのは、PPによって主張されたパッケージの他に、STがパッケージを追加する場合のみである。

STがPP構成への適合を主張する場合、PP構成のコンポーネントが主張するいかなる機能パッケージを含め、いかなる機能パッケージへの適合も主張してはならない。

STがPP構成への正確適合又は論証適合を主張する場合、STがPP構成で主張された保証パッケージを追加しない限り、PP構成で主張された保証パッケージへの適合も主張してはならない。つまり、PP構成は保証パッケージを<パッケージ>適合又は<パッケージ>追加として主張することができるが、STが自らPP構成内のパッケージの適合/追加バージョンを追加しない場合、STは保証パッケージへの適合は主張しないことになる。STが<パッケージ>追加を主張するのは、PP構成によって主張された保証パッケージの他に、STが保証パッケージを追加する場合のみである。

注2：完全適合のために、パッケージへの適合を主張するPP、又はパッケージへの適合を主張するコンポーネントを持つPP構成への適合を主張することが許可されるが、それらはSTの適合主張には反映されない。

e) PPに関する適合主張を含むこともできる。

— 「*PP適合*」

PP又はTOEは、特定のPPを満たす。

直接根拠STは、1つ以上の他の直接根拠PPへの適合のみを主張することができる。（附属書B参照）

f) PP構成に関する適合主張を含むこともできる。

— STは、厳密に1つのPP構成への適合を主張することができる。

— 直接根拠STは、そのPP構成が直接根拠アプローチを使用する場合にのみ、PP構成への適合を主張しなければならない。

注3：PP構成の評価は、いかなる製品評価から独立して、前もって実施することができる。また、PP構成の評価は、ST適合主張の評価に先立ち、適合するSTの評価中に行うことも可能である。PP構成の評価については、13.3を参照のこと。

PP モジュールは、1 つ以上の PP モジュール基盤の上に特定の PP 構成を構築するために使用される。したがって、PP モジュールは、主張された PP 構成を通じてのみ、ST によって使用されなければならない。

g) STが適合を主張するいかなるパッケージ、PP、PPモジュール、又はPP構成の適合ステートメントにCEMから派生した評価方法/評価アクティビティが識別された場合、適合主張は、次の形式の主張も含まなければならない。

「*TOEは、<参照>で定義された評価方法/評価アクティビティを用いて評価される。*」

このステートメントで、*<参照>*は、関連する評価方法及び評価アクティビティの所在の識別に置き換えられる。

評価方法/評価アクティビティを参照するSTは、ST内で評価方法/評価アクティビティのテキストを再現する必要はない。

STは、STが主張するパッケージ、PP、PPモジュール、又はPP構成に含まれる評価方法/評価アクティビティについてのみ適合を主張しなければならない。

注4：読者は、STがPP又はPP構成を主張しないが、パッケージを直接指定できる場合があることに注意する。

ST は、複数の PP への適合を主張することができる。そのような PP の 1 つが完全適合の種別を持っている場合、全ての PP は、その完全適合の種別でなければならない。そうでない場合、PP は、正確適合及び論証適合の種別が混在することができ、ST 評価の一部として、論証適合及び正確適合の組み合わせの一貫性の正当性が確認されなければならない。

STの適合主張に関する詳細及び要件は、附属書Dを参照のこと。

適合種別に関する詳細及び要件は、附属書Eを参照のこと。

12.3 保証要件

CCパート3(場合によっては拡張)の適合を主張するSTは、TOEに適用されるグローバルなSARのセットを定義しなければならない。

STは、適用されるSARのセットに対して特徴的な名前を定義することができる。ただし、(追加された)事前に定義されたEAL又は適用可能な外部参照で定義された(追加された)保証パッケージを使用する場合、同じ名前を使用する必要がある。

STにおいて追加SARが指定される場合、又はSARが階層的に上位のSARと置き換えられる場合、STが使用する評価方法/評価アクティビティが実証されるよう、保証根拠の中で以下のように対処されなければならない。

— EM/EAは依然として適切である、すなわち、新しいSARはSTで使用するために指定されたEM/EA及びそれらが提供する保証に影響を及ぼさない。又は、

— EM/EAは、STが指定する元のEM/EAに対する定義された詳細化によって対処される。その結果得られる、STに要求されるEM/EAは、STに適用される元のEM/EAと同じかそれ以上の保証を生成する。又は、

— EM/EAは、追加のEM/EAによって補完される。その結果得られるEM/EAは、STに適用される元のEM/EAと同じかそれ以上の保証を生成する。

例：下位階層のSARのための証拠資料の検査であったアクティビティが、階層的に上位のSARのために追加の

テストが必要な場合、元の証拠資料評価アクティビティを、テストを要求する追加の評価アクティビティで補完することができる。

12.4 完全適合の場合の追加要件

12.4.1 適合主張の追加要件

STは、完全適合PP/PP構成と同時に完全適合の種別ではない他のPPへの適合を主張してはならない。すなわち、完全適合のPP/PP構成は、正確又は論証適合と組み合わせてはならない。

12.4.2 SPDの追加要件

完全適合を主張するSTは、以下のとおりである。

— 完全適合を主張する全てのパッケージ及びPP又はPP構成のSPDを、全てのSPDエレメントを含めて、含なければならない。

— 完全適合を主張するパッケージ又はPP/PP構成に存在しないSPDエレメントを含んではならない。

注：PP構成からSTにインスタンス化されるSPDは、PP構成のコンポーネント(PP及びPPモジュール)に存在するSPDエレメントを正確に含む。PP構成コンポーネントを組み合わせてSPDエレメントを変更したり除去したりすることができる(例えば、基本PPの前提条件は、その基本PPの上にあるPPモジュールによって対抗される脅威となることができる)ため、STに現れる結果はこれらの種類の変更を考慮することに注意。11.3を参照のこと。

12.4.3 セキュリティ対策方針のための追加要件

完全適合を主張するSTは、以下のとおりである。

— 適合を主張するPPの全てに指定されているTOEのセキュリティ対策方針を全て含まなければならない。

— 適合を主張するPPの組み合わせに指定されていないTOEのセキュリティ対策方針を追加で指定してはならない。

— 適合を主張するPPの組み合わせに指定されている運用環境のセキュリティ対策方針を全て含まなければならない。

— 適合を主張するPPの組み合わせに存在しない、運用環境のセキュリティ対策方針を追加で指定してはならない。

同じことがPP構成にも言える。PP構成からSTにインスタンス化されるセキュリティ対策方針は、PP構成のコンポーネントに存在するセキュリティ対策方針を正確に含む。PP構成コンポーネントを組み合わせてセキュリティ対策方針を変更したり、削除したりすることができる(例えば、基本PPの環境のセキュリティ対策方針が、その基本PPを使用するPPモジュールではTOEのセキュリティ対策方針になる可能性がある)ため、結果のSTにはこの種の変更が反映されることに注意するべきである。

12.4.4 セキュリティ要件に関する追加要件

STは、以下の例外を除き、PPに含まれる全てのSARとPP構成コンポーネントに含まれる全てのSFRを含まなければならない。

— ST作成者は、追加の、又は階層的に上位のセキュリティ要件を含めてはならない。

— PP又はPPモジュールの選択ベースのSFRとして指定されたSFRは、それらを含めることを要求する選択項目がST作成者によって選択されない場合には、除外されなければならない。

— PP又はPPモジュールのオプションのSFRとして指定されたSFRは、完全適合の主張を維持したまま、含まれたり含まれなかったりすることがある。

注1：完全適合PPのSFRは、(ASE_CCL.1-12のCEMに記載されているように)繰返しと詳細化をすることができる。

注2：オプション及び選択ベースのSFRに関する詳細については、7.3.2.6を参照のこと。

注3：PP適合に関する詳細については、附属書Eを参照のこと。

12.5 マルチ保証の場合の追加要件

マルチ保証STは、正確に1つのマルチ保証PP構成への適合を主張し、他のPP又はPP構成への適合を主張してはならない。

マルチ保証STは、TSFをサブTSFで構成し、サブTSFの各々に対して特定のSARのセット及び、TOE全体に対してグローバルなSARのセットを主張しなければならない。これは、マルチ保証PP構成への適合によってのみ達成できる。STで定義されたTSF構造はPP構成から引き継がれ、STでそれらに適用されるSARのセットはPP構成で定義されたものと同一であるか、追加されたもののいずれかである。

マルチ保証STは、要求される適合規則を満たす範囲で、新しいエレメントがPP構成の最低1つのPP又はPPモジュールを完了するように、追加SFR(及び必要に応じて関連SPDとセキュリティ対策方針)で(正確適合又は論証適合の種別の)マルチ保証PP構成を拡張できる。すなわち、新しいSFRはPP構成のコンポーネントによって定義されたサブTSFの拡張を目的としている。結果として、拡張されたサブTSFは、元のPP/PPモジュールで定義されたSARの対象となる。

マルチ保証STは、マルチ保証PP構成で定義されたSARのセットを主張できる、又は正確適合又は論証適合の種別の場合、一般モデルのSTと同様に、SARの「追加」セットを主張する根拠を提供することもできる。

それぞれのSARのセットに従って2つ以上のPPに適合するために、そのPPで構成されるマルチ保証PP構成が定義され、STによって主張されなければならない。

マルチ保証PP構成への適合を主張し、適用される全てのSARのセットをTOE全体及びサブTSFの全てについて同じSARのセットに到達するように追加するSTは、単一保証STとなる。この場合、TOEの

評価は単一保証の評価手法に従わなければならない。これは、正確適合及び論証適合の種別のPP構成にのみ許可される。

複数のPPへの適合を主張するSTは、TOE全体に適用されるグローバルなSARのセットを定義することのみが可能であり、その結果単一保証STが生じる。PPに関する単一保証STの保証要件の一貫性を保証するためのASE規則が適用される。

1つの単一保証PP構成への適合を主張するST、すなわちTOE全体及びその部分に対してSARの1つのセットのみを定義するSTは、マルチ保証STになることはできない。その理由は、マルチ保証の一貫性ルールはPP構成のレベルで定義されるからである。これを達成するために、PP構成から派生したマルチ保証PP構成が定義され、評価されなければならない。

マルチ保証PP構成とSTの詳細については、12.4.2を参照のこと。マルチ保証PP構成への適合を主張するSTは、各サブTSFに対して適用されるSARのセットを定義することにより、マルチ保証STになることができる。これは、PP構成から引き継がれるSARと同じセット又は、PP構成で提供される保証根拠の更新を要求する、より大きなセット(追加、正確適合及び論証適合の種別の場合にのみ有効)のいずれかである。

マルチ保証STは、TOE全体及び各サブTSFに適用されるSARのセットについて、特徴的な名前を定義することができる。この名前は、PP構成で与えられた名前と一貫したものでなければならない。(追加された)事前に定義されたEAL又は適用可能な外部参照で定義された(追加された)保証パッケージの使用は、同じ名前を使用する必要がある。

PP構成への正確適合又は論証適合を主張し、適合を主張するPP構成のSARのセットを拡張するマルチ保証STは、拡張の一貫性を正当化する保証根拠を提供しなければならない。

マルチ保証STは、マルチ保証PP構成の適合ステートメントにおいて識別される個々の適合種別のそれぞれ及び全てに適合しなければならない。

注：複数のPPへの適合を主張するSTは、TOE全体に適用されるグローバルなSARのセットのみを定義できる。この場合、PPに関するSTの保証要件の一貫性を保証するためのASE規則が適用される。

図9は、PP Aと2つのPPモジュールX及びYから構成されるPP構成「AXY」への適合を主張するマルチ保証STの一例を示す。TSF構造は、A、X、Yで定義されたサブTSFで構成される。グローバルなSARのセット(SAR_C)及びサブTSFに適用される複数のSARのセットは、追加なしでPP構成から得られる。

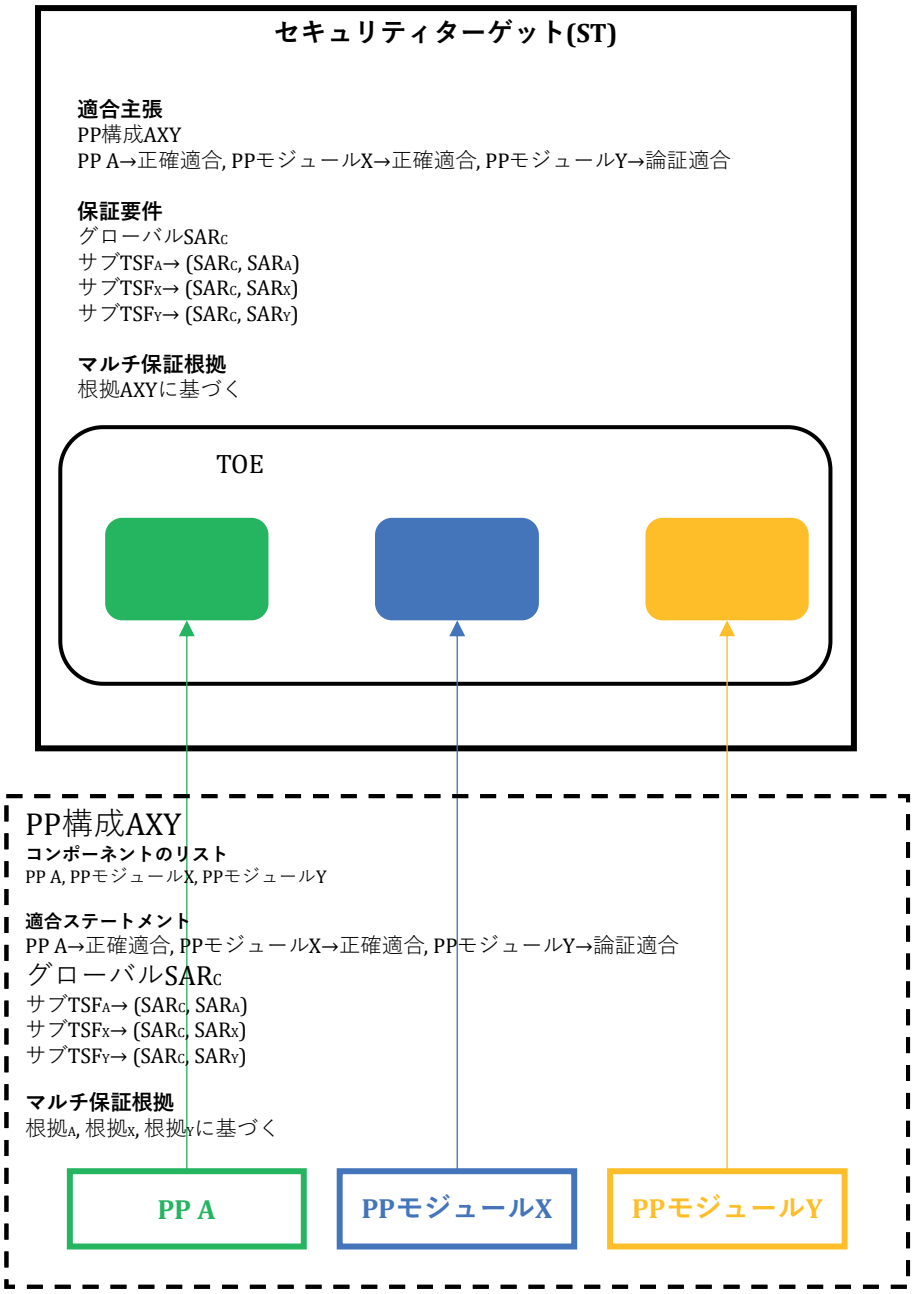


図9 — マルチ保証STの例

13 評価及び評価結果

13.1 一般

本章は、CEM及び/又は追加の評価方法及びアクティビティに従って実施されるPP、PP構成及びST/TOEの評価から期待される結果を示す。

評価の目的は、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提供することである。

注1：関連する最新技術に従うことと、十分なレベルの再現性との間のトレードオフがしばしば必要である。したがって、客観性や再現性といった特性は、標準では絶対的なものとしてではなく、様々な方法でアプローチできる目標として捉えられている。例えば、CCパート4は、CEMから評価アクティビティを導き出す際に、客観性と再現性を維持するための枠組みを規定している。

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結果を表している。このような結果は、特定の適用環境での使用に対する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。

図10は、TOEの評価結果に信頼性を持たせるために必要な様々な評価を記述する。

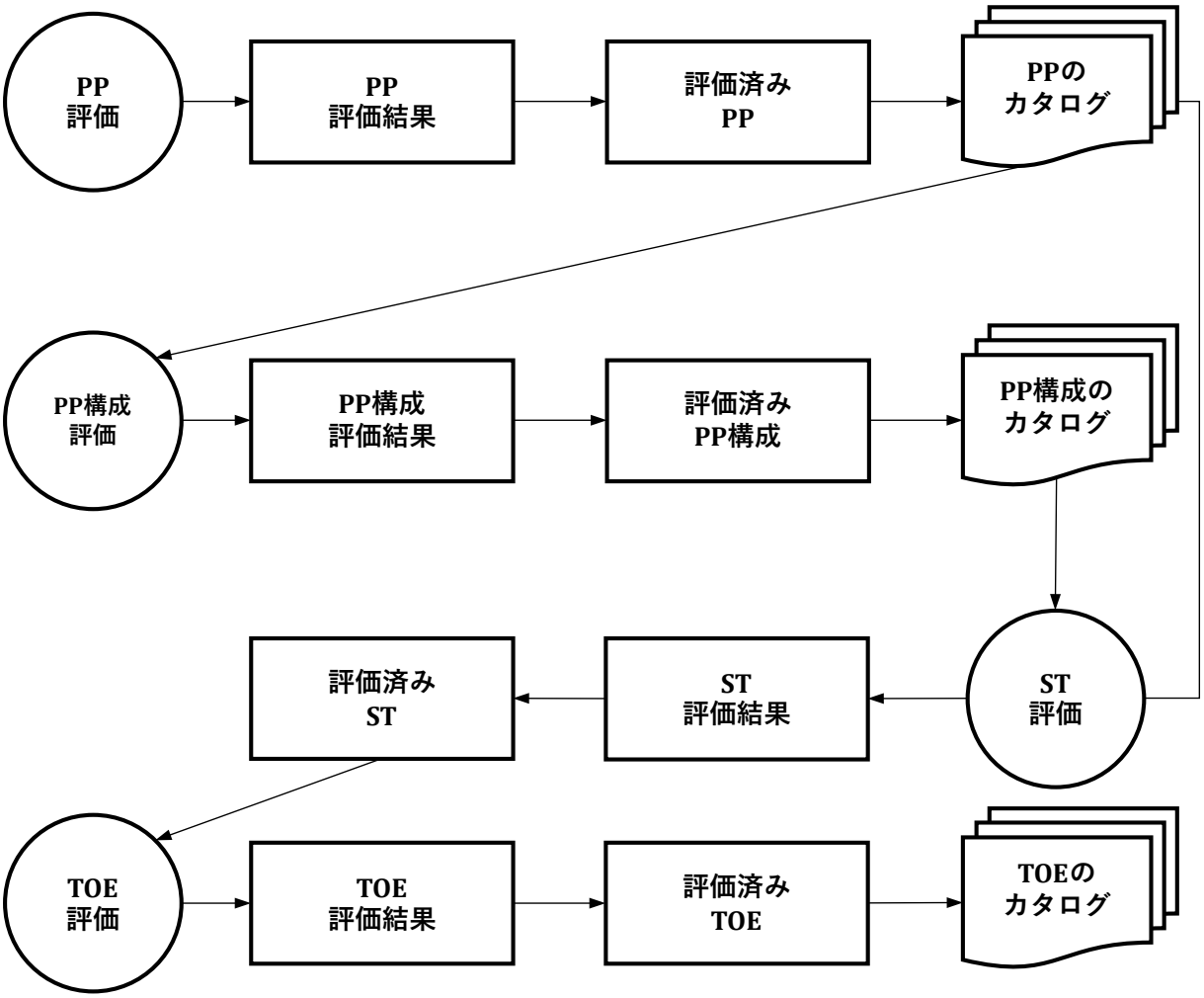


図10 — 評価の流れ

CCは4種類の評価について基準を示す。

a) PP評価。13.3に記述されている、CCパート3に記載されたAPEクラスに基づく。

b) PP構成評価。13.3に記述されている、CCパート3に記載されたACEクラスに基づく。

c) ST評価。13.4に記述されている、CCパート3に記載されたASEクラスに基づく。

d) TOE評価。13.5に記述されている、評価済みのST及びSTによって主張されたセキュリティ要件の評価基準に基づく。

PP及びPP構成の評価は、PP及び/又はPP構成がCCの要件を満たしている確信を提供する。PP及びPP構成のカタログは、カタログに含めるための基準を定義する監督機関等により維持されることができる。

注2：カタログへの掲載基準は、CCの範囲外である。

PPモジュールは、PP構成に基づく評価の一部としてのみ評価される。

パッケージは、PP構成、PP、又はST評価の一部としてのみ評価される。

注3：実際には、いくつかの評価されていないPP構成への適合を主張するSTは、最初にPP構成の評価を行うことによって、評価することができる。

ST評価は、TOE評価の枠内で使用される中間の結果となる。オプションとして、STはパッケージ、PP、PP構成に対する適合主張とともに開発される場合がある。

ST/TOE評価により、評価済みのTOEのカタログが作成できる。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、IT製品がカタログに掲載されているからといって、そのIT製品全体が評価されたと解釈することはできず、実際のSTがTOE評価の実際の範囲を定義している。

このようなカタログの例については、「参考文献」を参照のこと。

13.2 評価の枠組み

評価結果間の比較可能性を高めるために、評価は評価制度の枠組み内で実行されるべきである。

注1：CCは、評価制度に関する要件を明示していない。

これらの評価結果を生成する共通の評価方法を使用することによって、評価結果間のより大きな比較可能性をサポートすることも達成される。共通評価方法を使用することは、評価結果の再現性と客観性に寄与するが、それだけでは十分ではない。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背景知識の適用を必要とする。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がある。

注2：CCは、開発者や評価者の能力を評定するための要件を規定していない。ISO/IEC 198963は、評価プロセスでサポートとして使用できるCC評価者の能力要件を規定している。しかし、基本的な方法論のコンピテンシーを扱っているだけで、評定方法については扱っていない。

— 既定の製品タイプでADV、ATE、又はAVA_VAN評価を行うために要求されるような技術固有の知識とスキル。

— ASE、APE、又はACEの評価を行う際に通常要求される分野固有の知識。

さらに、CCに従って行われる評価で要求される特定のスキルは、追加の能力評定方法が必要になることがある。例えば、形式手法に関連するスキルを評定する場合などである。

CCについては、ITセキュリティ評価の一般的な方法がCEMに記載されている。より具体的な評価方法及びアクティビティは、CCのパート4に示された枠組みを用いるか、標準保証コンポーネントを詳細化するか、又は拡張保証コンポーネントを定義することにより、CEMから導き出すことができる。

PP 作成者は、CEM に記載された IT セキュリティ評価の一般的な方法論を、技術に特化した評価アクティビティを含む方法で追加することが必要になることもある。

認証プロセスは、CCの範囲外であるが、最終的な証明書や承認書の作成につながる評価結果の独立した検査を含むことができ、これは一般に公開することができる。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。

13.3 PP及びPP構成の評価

評価済みのPP/PP構成に関してPPやSTを構築することは、以下の2つの利点がある。

— PP/PP構成に誤り、曖昧さ、又は相違が存在するリスクが大きく低下する。PP/PP構成の評価中に発見されるはずの問題が、新しいSTの作成中又は評価中に発見された場合、PP/PP構成が訂正されるまでにかなりの時間が経過する可能性がある。

— 新しいPP/PP構成の評価は、以前の評価結果を再利用することができ、新しいPP/PP構成の評価に費やす労力は少なくて済む。

PPの評価が要求される場合、CCパート 3 に記載されているAPE基準が使用されなければならない。

PP構成の評価が要求される場合、CCパート3に記載されているACE基準が使用されなければならない。

この評価の目的は、PP又はPP構成が完全で、内部的に一貫した、技術的に信頼でき、ST又は別のPP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。

PP及びPP構成の評価結果の記載方法は、13.7に記述されている。

注：PPモジュールは個別に評価されない。PPモジュールを使用するPP構成を評価する過程で評価される。

13.4 ST評価

ST評価は、TOEの十分性、運用環境、及びTOEに含まれる記述と要件の内部一貫性を判断する。

ST評価は、CCパート3で定義されるASE評価基準を適用することによって実施されなければならない。ASE基準を適用するために使用される方法及びアクティビティは、CEMに規定されるSTに関連する評価方法、又はCEMから派生する評価方法/評価アクティビティによって決定される。派生した評価方法/評価アクティビティは、CCとCEMの枠組みの外で正当性が確認される。

本書/シリーズの利用者は、評価制度が必ずしも特定の評価方法/評価アクティビティの使用を承認しているわけではないことに留意するべきである。STは、評価方法/評価アクティビティを要求することができ、評価制度はこのSTに従って評価を実施しないことを決定することができる。

STの評価結果の記載方法は13.7に記述されている。これらの結果は、STが適合を主張するPP及びパッケージも識別する。

13.5 TOEの評価

TOE評価は、STで定義された基準に対するTOEの正確性を判定する。前に述べたように、TOE評価では、運用環境の正確性は評定しない。

TOE評価は、より複雑である。TOEの評価への主な入力は、TOE及びSTが含まれるが、通常、設計文書又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。

TOE評価は、評価証拠に(STから)SARを適用することからなる。特定のSARをTOEに適用する方法は、CEM及びCEMから派生した評価方法/評価アクティビティによって決定される。派生した評価方法/評価アクティビティは、CC及びCEMの枠組みの外で正当性が確認される。本書/シリーズの利用者は、評価制度が特定の評価方法/評価アクティビティの使用を必ずしも承認するとは限らないことに留意するべきである。STは、評価方法/評価アクティビティを要求することがあり、評価制度は、このSTに従った評価を実施しないことを決定することができる。

SARの適用結果の証拠資料に記載する方法と、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。

TOE評価は、TOE開発が完了した後に、又はTOE開発と並行して実施することも可能であるが、この評価において適切な保証コンポーネントが選択されることが前提である。

ST/TOE評価結果の記載方法については、13.7で説明する。

13.6 評価方法及び評価アクティビティ

CCパート3に記載されているセキュリティ保証クラスごとに、一般的なIT評価方法及びアクティビティがCEMで規定されている。CEMに記載されている評価方法及びアクティビティは上位レベルであり、技術の種類、評価保証レベル、又は記述されたセキュリティ課題によっては、より具体的な評価方法と評価アクティビティの規定が必要となることがある。

CEMから派生した評価方法/評価アクティビティは、PP、PPモジュール及びパッケージへの組み込みとして、又は別のサポート文書として公開することができる。

13.7 評価結果

13.7.1 PPの評価結果

PPの評価結果には、10.3に従った「適合主張」が含まれなければならない。

注：CCパート3はAPEクラスのPPの評価基準を規定する。

13.7.2 PP構成評価結果

PP構成の評価結果には、11.3に従った「適合主張」が含まれなければならない。

PP構成が評価されると、ST評価はPP構成の評価結果に依存する場合がある。

注1：CCパート3は、ACEクラスのPP構成の評価基準を規定する。

注2：PP構成の評価は、評価方法に影響を与えることなく、以下の2つの状況で生じる可能性がある。

— いかなる製品評価からも独立した評価、又は、

— PP構成への適合を主張するST評価の最初のステップとしての評価。そうでなければ、適合主張は意味がなくなり、この側面でSTの評価が不合格となる。

13.7.3 ST/TOEの評価結果

13.7.3.1 一般

STの評価結果には、12.2に定義される「適合主張」を含まなければならない。

TOE評価の成功には、ST評価の成功が必要である。TOE評価プロセスの結果は、以下のいずれかである。

— 全てのSARが満たされているため、TOEがSTに記載されるSFRを満たすという指定された保証レベルであるとするステートメント。

— 満たされていないSARがあるため、TOEがSTに記載されるSFRを満たすという指定された保証レベルではないとするステートメント。

注：評価結果は後に認証プロセスで使用される場合があるが、この認証プロセスはCCの範囲外である。

TOEの評価の結果、合格となった場合、その基礎となる製品は、評価合格製品のカタログに掲載される資格を得ることができる。

13.7.3.2 ST/TOE評価結果の使用

ST及びTOEが評価されると、資産所有者は、STで定義されているように、TOEが運用環境とともに、明示された脅威に対抗するという保証を得ることができる。評価結果は、資産所有者が、資産を脅威にさらすことに関連するリスク受容の判断の一部として使用することができる。

ただし、リスク所有者は、以下の点を注意深く確認するべきである。

a) STのSPDが自らのセキュリティ課題に合致している。

b) 自分の運用環境が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(又は適合させることができる)。

c) TOE評価の枠組みの中で開発者によって提供されたガイダンス文書が、TOEの設置、設定、及び運用中に遵守されている。

これらの条件のいずれかが当てはまらない場合、関連する保証は信頼できず、評価結果はリスク受容の決定に応じて処理するべきである。

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発見される可能性がある。その場合、開発者は(脆弱性に対処するために)TOEを訂正、又は新たに識別された脆弱性を評価範囲から除外する方法で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。

注：保証を維持する場合は、再評価が必要である。CCはこの再評価のために使用できるが、再評価の詳細な手順は本書の範囲外である。

13.8 マルチ保証評価

マルチ保証PP構成の場合、CCパート3に記載されているACE要件は、異なるSARの組み合わせのセットが、PP構成を構成するPP及びPPモジュールのSPDに定義されているように、基礎となる資産の期待されたセキュリティを損なわないことを保証する。

マルチ保証STの場合、CCパート3に記載されているASE要件は、STがACE保証要件を満たすマルチ保証PP構成に適合することを保証する。これは、サブTSFにおけるTSFの構成及びそれらに適用されるSARのセットが、PP構成と一貫していることを意味する。各サブTSFに対して、マルチ保証STは、対応するコンポーネント(PP又はPPモジュール)のPP構成で定義されたSARのセットと同一又は追加されたSARのセットを主張することを意味する。

マルチ保証評価に適用される標準の一般モデルは、TOEのセキュリティを保証するために評価者がTSFを評価することを要求する。マルチ保証の枠組みでは、評価者はサブTSFのそれぞれを評価する際に、さらにTOE全体への影響を考慮する。

実際には、マルチ保証評価は、異なるPPによる同じTOEの複数評価と見なすことができる。マルチ保証評価では、これらの評価が一緒に実行できることを保証するために要求される一貫性検査が追加される。これは特に、サブTSFに関連するSARのセットが、他のサブTSFに影響を与えないことを意味する。したがって、１つのサブTSFのSARが要求する証拠が、他のサブTSFのために選択されたSARによって悪影響を受けることはない。

例：PP構成が1つのサブTSFに対してAVA_VAN.3を選択した場合を考えてみる。その場合、ADV_TDS.3は依存性によって要求される。このサブTSFに対するADV_TDS.3の評価は、TOEに定義された他のサブTSFのADV_TDSレベルに関係なく、定義上、TOEの全てのサブシステムを考慮することになる。

マルチ保証STに適合するTOEのマルチ保証評価は、STに定義されているように、TOE全体のグローバルなSARのセットに対する評価、及び各サブTSFの対応するSARのセットに対する評価から成る。評価アクティビティの順序は評価者に任されている。最適な順序は、サブTSFに関するTSFの実際の構造、グローバルなSARのセットとサブTSFに適用されるSARセットの違いなどの要因による。

1つのマルチ保証PP構成に適合するTOE(及びST)へのマルチ保証評価の制限と、ACEのマルチ保証一貫性規則の定義により、他の保証クラスへの影響を制限することができる。マルチ保証評価の実行は、CEMで定義されているように、全ての保証クラスの統一された解釈を適用することで構成されている。マルチ保証評価の枠組みでは、SARが「TOE」に言及する場合、それはTOE全体を指す。SARが「TSF」に言及する場合、そのSARが適用されるサブTSFを指す。

マルチ保証STは、STが適合を主張するPP構成で定義されたサブTSFの、TSFの構成を反映する。このTSFの構成は、TOEのサブシステムやモジュールにおける実装の構成を説明するものではなく、既定のセキュリティ機能のセット(サブTSF)と特定の保証要件とを関連付けるものである。サブTSFは、異なるサブシステム/モジュールのセットによって実装されることもあるが、ある程度の重複があることもある。サブシステム又はモジュールは、2つの異なるサブTSFに属する機能を実装できる。これは、2つのSARのセットが共通のサブシステム又はモジュールに適用される(すなわち、SARのセットを合わせたものが適用される)ことを意味する。どちらの場合も、各サブTSFについて、

他の全てのサブTSFはTOEに属し、対応するサブシステム/モジュールは、サブTSFの要件の観点[ii]から評価しなければならない。

14 保証の統合

14.1 一般

IT製品は、ほとんどの場合、複数のコンポーネントから構成され、そのうちのいくつかが評価され、いくつかは評価されない。独立した製品コンポーネントは別々に評価されることが多く、単一のコンポーネントのセキュリティ保証を統合して製品全体のセキュリティ保証を決定するという問題が生じる。

例：ソフトウェアを評価済みハードウェアと統合し、IT製品を作る。

保証の統合は、以下の点に依存する。

— 統合の種別

— コンポーネント評価が基づいたセキュリティ機能方針及びOSP

— 主張されるセキュリティ保証、例えば保証レベル

— 製品全体の総合的なセキュリティ方針

統合モデルの概念については、14.2.で説明する。このような統合モデルにおけるセキュリティ保証を提供できる評価方法は、14.3に示す。統合アプローチにおける個々の製品コンポーネントに関連する評価結果の再利用に関する考察は、14.4で述べる。14.5では、コンポジット評価手法とマルチ保証評価手法間の関係について述べる。

14.2 統合モデル

14.2.1 階層化統合モデル

この種別の統合では、図11に示すように、あるコンポーネントが別のコンポーネントの上に構築される。

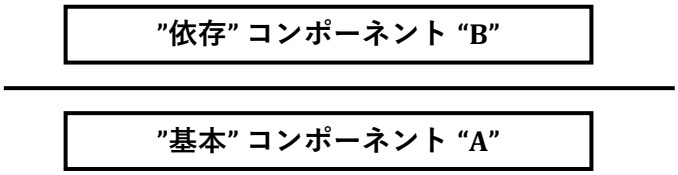


図11 — 階層化統合モデル

階層化統合モデルに関して、以下の前提条件がある。

— 基本コンポーネントは、依存コンポーネントに依存していない。

— 基本コンポーネントは、依存コンポーネントによって改変されることはない。

— 依存コンポーネントは基本コンポーネントの機能性を使用し、その逆はない。

このような統合を実行する者は、次のことを考慮するべきである。

— 依存コンポーネントは、基本コンポーネントの評価範囲にあるセキュリティ機能性以外の機能性にも依存することができる。

図11に記述された階層化統合モデルを明確にするために、2つの例を挙げる。

例1：最初の主な例は、スマートカード分野からのものであり、階層化統合モデルの評価技法が定義されている。この文脈では、スマートカードは、2つの部分の組み合わせで構築される。

— ハードウェア集積回路(IC)部分(基本コンポーネント)

— その上にあるソフトウェア部分(依存コンポーネント)

ソフトウェア部分は、基礎となるハードウェアの評価済みのセキュリティ機能性に属さない機能性に依存することができる。ただし、一般に、ハードウェアのほとんど全ての命令は、ハードウェアのセキュリティ機能性の一部であり、ソフトウェア部分のセキュリティ機能性を実装するために使用される。

スマートカードのソフトウェア部分は、それ自体が階層化されている可能性があり、以下のものから構成されている。

— アプリケーション機能性が統合されている可能性がある「オペレーティングシステム」層(基本コンポーネント)

— その上に、異なるアプリケーションを含む「アプリケーション」層(依存コンポーネント)

これらの部分は全て、特定の目的を持った異なる役割担当者によって開発されることができる。

例2：パーソナルコンピュータ上で稼働するアプリケーションは、オペレーティングシステム(OS)が基本コンポーネントとして機能し、アプリケーション層が依存コンポーネントとして機能するという同じ原則に従う。アプリケーションは、OSによって提供される識別と認証を使用し、独自のオブジェクトをOSファイルシステムの上に構築し、そしてOSのアドレス空間の管理と分離の上に独自のアプリケーション構造を構築し、特定の特性(例えば、耐障害性、情報フロー制御)を実施する必要がある。OSがすでに評価されている場合は、アプリケーション層のセキュリティ機能性を基本コンポーネントの評価済みセキュリティ機能性に分解することができる。これが不可能な場合、依存コンポーネントはそれ自体でセキュリティ機能性を実装する。さらに、依存コンポーネントは、基礎となる基本コンポーネントの評価済みセキュリティ機能性に属さない機能性に依存することができる。

14.2.2 ネットワーク型又は双方向型統合モデル

この種別の統合コンポーネントでは、図12に示すように、あるコンポーネントが、何らかの通信チャネルを介して通信する別のコンポーネントの特定の機能性を使用する。

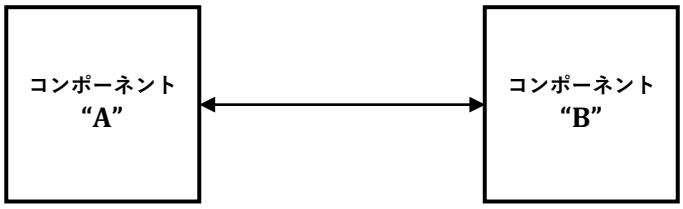


図12 — ネットワーク型又は双方向型の統合モデル

ネットワーク型又は双方向型の統合モデルに関して、以下の前提条件がある。

— セキュリティの相互依存関係が明確に記述されている。

— 両製品は、定義されていないチャネルや影響が生じないように分離されている。

— 両製品は、通信チャネルを保護するために必要な機能性を実装している。

例1：外部LDAPサーバ(コンポーネント「B」)の機能性を使用するアプリケーション(コンポーネント「A」)。

このような統合を行う者は、次のことを考慮する。

— セキュリティ機能性が合わない可能性がある。

例2：アクセス制御は、異なるオブジェクトに基づくことができる。

— コンポーネントに対する前提条件が有効でない場合がある。

例3：別のコンポーネントに転送される重要なデータの保護に関する前提条件。

— セキュリティ機能性は、望ましくない副作用をもたらす可能性がある。

例4：隠れチャネルから暗号鍵が漏れる。

このような問題が識別された場合、適切な緩和策の決定とともに、明確に文書化する必要がある。

14.2.3 組込み型統合モデル

この種別の統合では、図13に示すように、コンポーネントがより大きなコンポーネント、又は製品の一部として使用される。

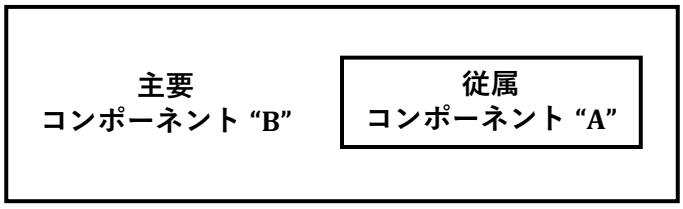


図13 — 組み込み型統合モデル

組み込み型統合モデルに関して、以下の前提条件がある。

— 通常、コンポーネント間に分離はない。

— 各部分は、意図したもの以外のチャネル及びインタフェースを介して、他の部分に影響を与える可能性がある。

例：大規模な製品の一部として、特定のセキュリティ機能を提供するライブラリやサブシステム。

このような統合を行う者は、コンポーネントが分離されていないことにより以下のような可能性があることを考慮するべきである。

— 他のコンポーネントのセキュリティ機能性をバイパスする可能性。

— 他のコンポーネントや製品全体のセキュリティ機能性やセキュリティ方針を改変する可能性。

— 多くの重大な副作用を引き起こす可能性。

注：分離が特定されている場合、CCパート3のADV_ARCに評価基準が記載されている。

14.3 統合モデルにおける保証を提供するための評価技法

14.3.1 一般

14.2に記述されている統合モデルを利用するIT製品(TOE)の評価において、信頼性と再現性のある評価結果を達成するためには、それに対応する適切に定義された評価方法が必要である。

14.3.2及び14.3.3は、階層化統合モデルの評価技法を扱う。14.3.2では、CCパート3で定義されたACOクラスを統合TOEにどのように使用することができるかを記述し、14.3.3では、業界ですでに広く適用され、複数の利点を示すコンポジット製品の評価技法を規定している(14.3.3.1参照)。

他の2つの統合モデル(双方向型及び組み込み型)は、CCで定義された構成概念では明示的には対処されていない。

14.3.2 統合TOEのためのACOクラス

CCパート3で規定されるACOクラスは、14.2に記述されているように階層化された統合モデルを用いて2つのTOEから統合されるTOEに対応し、その両方が個別に評価されている。これらのコンポーネントTOEは、図14に示すように、基本TOE及び依存TOEとして記述することができる。このような場合、統合TOEの評価にはACOクラスが使用される。

このような統合TOEの評価は、両TOE間の相互作用の評価からなり、基本TOEと依存TOEの両方からの評価結果の再利用が行われる。

CCパート5は、統合TOEの保証レベルを決定するために使用できる事前に定義されたCAPを規定する。

ACOクラスは、「強化基本」保証レベルまで適用可能である。

図14 — ACOクラスを使用した統合TOEの評価

14.3.3 コンポジット製品に対するコンポジット評価

14.3.3.1 一般

コンポジット評価技法は、14.2に記述されているコンポジット製品の階層化統合モデルに対応し、以下の目的を達成するために考案されたものである。

— 基本コンポーネントの評価を単独で行い、複数の依存コンポーネント及び顧客に対応する。

— 評価済みの基本コンポーネントとともに使用する1つ以上の依存コンポーネントを作成する。

— 評価済みの基本コンポーネントの上に依存コンポーネントを設置し、高い信頼性を維持したまま評価作業を軽減する。

コンポジット評価技法は、これらの目的を達成するために、知識の移転と評価証拠の再利用を行う方法を記述している。

CCパート3のADV、ALC、ASE、ATE、AVAクラスで規定されているCOMP関連保証ファミリは、この階層化モデルを用いたコンポジット製品に関連する評価基準を規定する。

14.3.3.2 目的

この保証の統合方法は、独立して評価される1つの基本コンポーネントと1つの依存コンポーネントから構成される階層化製品に適用される。

注：依存コンポーネントは、1つ以上の依存サブコンポーネントから構成される可能性がある。簡略化のため、以下ではこれらを「1つの依存コンポーネント」とみなす。

コンポジット製品は、すでに評価された基本コンポーネント(その基本TOEを含む)と依存コンポーネントを統合して作成される。これにより、基本TOEはコンポジットTOEの一部となる。コンポジ

ット評価手法では、基本TOEに対してすでに得られた評価結果は再利用され、コンポジット製品の評価の中で依存コンポーネントの評価を行い、特に基本TOEと依存コンポーネント間の関係の評価に重点を置く。したがって、保証レベルは、依存コンポーネントのみではなく、コンポジット製品全体に対して主張され、適用される。

基本コンポーネント(基本TOEを含む)及び依存コンポーネントを持つコンポジット製品は、効率的に評価されることを目的としている。具体的なコンポジット評価技法は、このようなコンポジット製品の評価を最適化することを目的として設定されている。

ACOベースの評価とは異なり、統合の技法を用いずに一度に評価する類似製品との直接比較が可能である。さらに、保証レベルには制限がない。すなわち、ACOがCAP要件によって「強化基本」の攻撃能力までの制限を受けるのに対し、コンポジット製品は、CCパート3のAVA_VAN.5で定義される「高」の攻撃能力までの耐性を含む、事前に定義された任意のEAL又は明確に定義された保証パッケージを主張することができる。この目的は、追加の保証クラスを定義することではなく、コンポジット評価のための追加の保証要件を定義することである。

例：高度な保証を要求するスマートカードデバイスの例として、決済や電子署名のアプリケーションがある。

14.3.3.3 コンポジット製品及びコンポジットTOEの設計

コンポジット製品は、1つの基本コンポーネント(その基本TOEを含む)及び1つの依存コンポーネントから構成され、評価の観点から、以下の規則と制約がコンポジット製品及びそのコンポジットTOE部分に適用される。

— 基本コンポーネントは、コンポジット製品の基礎となる独立した階層を構築し、基本TOEを含んでいる。基本コンポーネントとその基本TOEは、すでに評価されていなければならない。

— 依存コンポーネントは、基本コンポーネントに依存するコンポジット製品の補助層を構築し、コンポジット評価の枠組みの中で評価されなければならない。

— コンポジットTOEはコンポジット製品の一部であり、依存コンポーネント全体と基本TOEをカバーする。コンポジット製品を正確かつ安全に実行するために、基本TOE機能性のスーパーセットがより詳細に要求される。

  注1：コンポジットTOEは、基本コンポーネント/基本TOEに依存しない部分を含むことができる。簡略化のため、そのような部分は依存コンポーネントに属するとみなされる。

— 依存コンポーネントは、基本コンポーネント内にあるが基本TOEの外側にある基本コンポーネントの機能性(つまり、基本コンポーネントのTOE以外の部分にある機能)に依存することはできない。

— コンポジット製品のTOE以外の部分は、基本コンポーネント機能性、特に基本TOE機能性を使用することができる。通常、コンポジット評価は、コンポジット製品のこのTOE以外の部分が、

直接又は基本コンポーネントの機能性を使用することによって、依存コンポーネントと干渉しないことを決定する必要がある。

— コンポジット製品のTOE以外の部分、特に評価済みの基本コンポーネントのTOE以外の部分(つまり、基本TOEの外にある基本コンポーネントの部分)は、コンポジットTOEの運用環境の一部とみなされる。

注2：コンポジット評価は、目的とするコンポジット製品のEALとは独立して適用される。選択されたEALにより、一部の評価アクティビティが適用されない場合、それらもまた適用されることが期待されない。

注3：本書は、基本コンポーネントの保証レベルがコンポジット評価レベルと同等以上の場合のみを扱う。

注4：基本コンポーネントと依存コンポーネントの両方がCCを用いてすでに評価されている場合、コンポジット評価作業は、以前の基本コンポーネント評価と以前の依存コンポーネント評価の両方からすでに得られた結果に依存する可能性がある。しかしながら、本文書で定義されたコンポジット評価の目的は、依然として達成されなければならない。

図15は、コンポジット評価手法の枠組みにおけるコンポジット製品及びコンポジットTOEの一般的な設計と階層化を示す。

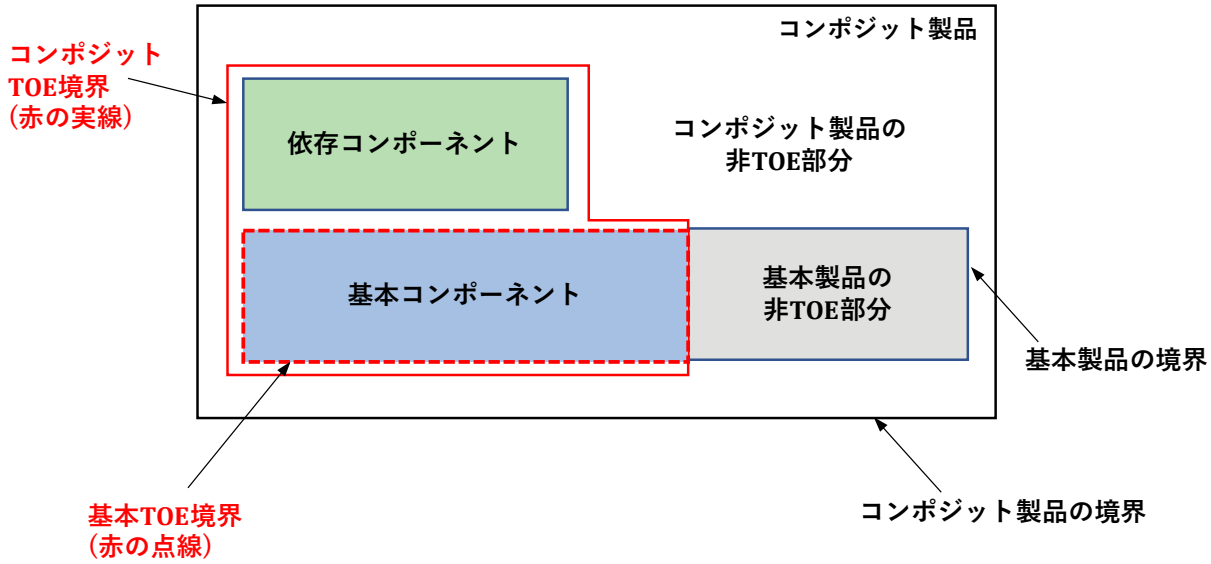


図15 — コンポジット評価

複数の統合ステップが互いに続くことができる。言い換えれば、基本コンポーネント自体が、すでに評価された基本コンポーネント及び依存コンポーネントからなるコンポジット製品になり得る。

14.3.3.4 役割分担

基本コンポーネント及びコンポジット製品、より正確には基本TOE及びコンポジットTOEの両方が評価を受けている。したがって、どちらにも、スポンサー、開発者、評価者、評価監督機関が存在する。

コンポジット製品の評価に対処するコンポジット評価モデルの場合、基本コンポーネントとその基本TOEの事前の最終評価が期待される。コンポジット評価は、すでに評価された基本コンポーネントの評価結果を再利用して、コンポジット製品の評価を行う。したがって、コンポジット製品の評価は、基本コンポーネントとの関係を含む依存コンポーネントの評価に焦点を当て、関連する評価結果を含む基本TOEを考慮に入れて行われる。

実際には、コンポジット製品は依存コンポーネント及び基本コンポーネントの統合から生じるので、コンポジット製品開発者は存在しない。代わりに、ここでの開発者に関連する役割は以下のとおりである。

— 依存コンポーネント開発者。依存コンポーネント(及び、該当する場合はさらにコンポジット製品のTOE以外の部分)の実装に責任を持つ。

— 基本コンポーネント開発者。基本コンポーネントの実装に責任を持つ。

— コンポジット製品インテグレータ。基本コンポーネント及び依存コンポーネントの統合を担当する。

この役割モデルに対応するため、コンポジット評価手法及び技法では、上記の依存コンポーネント開発者、基本コンポーネント開発者、コンポジット製品インテグレータに対する追加評価アクティビティを定義している。

注1：すでに述べたように、依存コンポーネントは個別の評価を受けている場合があるが、この以前の評価の評価者及び評価監督機関はここでは考慮しない。基本コンポーネント及び依存コンポーネントが別々に評価された場合、それぞれにスポンサー、開発者、評価者、評価監督機関が存在することになる。

注2：一般的なケースと同様に、役割担当者が同一である場合もある。また、コンポジット評価の文脈では、役割担当者が複数の役割を持つような場合もある。各評価では、これらの一般的な役割に特定の組織や人物を関連付けることになる。

例1

— 基本コンポーネント開発者は、基本コンポーネントスポンサーでもあり得る。

— 基本コンポーネント評価監督機関は、コンポジット製品評価監督機関であることもある。

注3：コンポジット製品インテグレータは、開発者とは異なる役割である。このインテグレータは、場合によっては、先に定義した開発者の一人でもあり得るが、常にそうであるとは限らない。

次の例は、コンポジット製品のインテグレータの役割を示す。

例2

— ネイティブスマートカード：基盤となる基本コンポーネントは集積回路であり、基本コンポーネントの開発者は集積回路(チップ)製造者である。依存コンポーネントはカードオペレーティングシステム及びそのアプリケーションであり、依存コンポーネント開発者はスマートカードオペレーティングシステム

及びアプリケーションの開発者である。この場合、コンポジット製品インテグレータの役割は、以下のとおりである。

— チップ製造者がオペレーティングシステムのコアをチップのROMに組み込み、次に、

— カードの製造者は通常、オペレーティングシステム及びアプリケーションの一部をチップのNVメモリ(EEPROM及び/又はフラッシュ)にロードする。

— Java Cardテクノロジ対応デバイス：基盤となる基本コンポーネントはチップ上のJava Cardシステム(Java Cardランタイム環境、仮想マシン、API)であり、基本コンポーネントの開発者はカード製造者/発行者である。依存コンポーネントはJava Cardアプレットであり、依存コンポーネント開発者の役割を果たすアプレット開発者によって開発されることができる。この場合、コンポジット製品インテグレータの役割は、ドメイン/アプリケーションサービスプロバイダ又はトラストセンターがアプレットをロードし、しばしば電子的にカードをパーソナライズすることによって果たすことができる。

14.3.3.5 アクションエレメント及び要求される情報

コンポジット製品の評価を可能にするために、コンポジット評価技法は、2つの主要な問題点を識別し、以下のルールを導き出す。

— 基本コンポーネント及び依存コンポーネントのセキュリティメカニズムの定義、統合、テストにギャップがあるため、コンポジット製品が安全でないことがある。特に、次の特性が適用される。

— 保護すべき資産は、専用のコンポジット製品STで定義された最終的なコンポジット製品の資産である。

— これらの資産の保護に関係するセキュリティメカニズムは、基本コンポーネント及び依存コンポーネントによって提供されるものである。

— 基本コンポーネントが提供するセキュリティメカニズム及びセキュリティサービスの一部は、依存コンポーネントが基本TOEに対して許可する設定、プログラミング、又はアクティベーションを必要とする場合がある。

— 最終的なコンポジット製品に対して、評価が実行され検証される。

この趣旨で、コンポジット評価技法は、基本コンポーネントの評価、依存コンポーネントの開発、及びコンポジット製品の評価に関わる役割担当者によって実行される特定のアクションエレメントを定義する。

— しかし、前述のアクションエレメントは、役割担当者間の情報共有が不十分であるため、実行できない可能性がある。これを避けるために、コンポジット評価技法では、各アクションエレメントにどの情報が必要かを明確に定義している。

表2及び表3は、コンポジット製品STにおいてどのSARを選択しなければならないか、及び依存コンポーネント開発者、コンポジット製品評価者、及びコンポジット製品評価監督機関がコンポジット評価を許可しサポートするために要求される情報を定義する。

表2 — 依存コンポーネント開発者に提供されるべき情報

アクションエレメントを定義するSAR	必要な情報	情報の発信者
コンポジット製品のセキュリティターゲットの一貫性(ASE_COMP)	基本コンポーネントのST。 コンポジット製品STを構築し、基本コンポーネントと依存コンポーネントの間でセキュリティ定義の一貫性を保証するための情報。 依存コンポーネントが管理又は使用する必要がある、基本コンポーネントのセキュリティメカニズム及びセキュリティサービスに関連する情報。	基本コンポーネント開発者
コンポジット設計適合(ADV_COMP)	基本コンポーネントのセキュリティメカニズムや、依存コンポーネントが管理又は利用しなければならないセキュリティサービスに関連する情報(通常はガイダンスや利用者のマニュアルの形式)。	基本コンポーネント開発者

潜在的に、コンポジット製品評価者は、そのような評価済みの基本コンポーネントを統合するコンポジット製品のコンポジット評価を実行するために、基本コンポーネント評価の全ての詳細な結果を必要としない。しかし、基本コンポーネントの評価結果を再利用するために、コンポジット製品の評価者は、基本コンポーネント及び依存コンポーネントが干渉する保証手段に関する補完的な情報を必要とする。特に、依存コンポーネントが基本コンポーネントによって課されるセキュリティ要件を満たしているかの検査、及びコンポジット製品の脆弱性分析のために、コンポジット製品の評価者は、評価済み基本コンポーネントの利用者ガイダンス、基本コンポーネント評価監督機関の関連レポート(評価者が提供した評価結果の受け入れを確認する評価済み製品のレポート)、及び14.3.3.6に記述されたいわゆる*コンポジット評価用のETR*(ETR_COMP)などを活用する。

以上より、コンポジット評価技法を活用するためには、コンポジット評価のために選択された保証パッケージ(例えば、EAL)に要求される標準的な情報量に加え、表3に概説されているような情報が必要である。

表3 — コンポジット製品評価者及びコンポジット製品評価監督機関に提供される情報

アクションエレメントを定義するSAR	必要な情報	情報の発信者
	基本コンポーネントのST。	基本コンポーネント開発者

アクションエレメントを定義するSAR	必要な情報	情報の発信者
コンポジット製品のセキュリティターゲットの一貫性(ASE_COMP)	基本コンポーネントと依存コンポーネントの間でセキュリティ定義の一貫性を保証するためのコンポジット製品STに関連する情報。 依存コンポーネントが管理又は使用する必要がある、基本コンポーネントのセキュリティメカニズム及びセキュリティサービスに関連する情報。	
	コンポジット製品のST(基本コンポーネントのSTとコンポジット製品のSTの互換性に関する情報を含む)。	依存コンポーネント開発者
構成部品の統合と配付手続きの一貫性チェック(ALC_COMP)	コンポジット構成証拠。 最終コンポジット製品に統合されている、評価済み基本コンポーネント及び依存コンポーネントの明確なバージョン情報を含む構成リストに基づく、バージョンの正確性の組織的証拠。基本コンポーネント開発者及び依存コンポーネント開発者が定めたセキュリティ対策が、コンポジット製品インテグレータによって実際に適用されているという証拠エレメント。	コンポジット製品インテグレータ
	配付及び受入れ手続きの証拠。 基本コンポーネント開発者及び依存コンポーネント開発者の配付手続きと、コンポジット製品インテグレータの受入れ手続きの適合に関する情報。 役割担当者から別の役割担当者へ送信されるコンポーネント(依存コンポーネント及び基本コンポーネント)が安全に受信され、受け入れられ、パラメタ化されているという組織的な証拠。	コンポジット製品インテグレータ 基本コンポーネント開発者 依存コンポーネント開発者
コンポジット設計適合(ADV_COMP)	基本コンポーネント関連の統合要件及び推奨事項(通常、利用者ガイダンスを含む)。	基本コンポーネント開発者
	コンポジット評価用のETR。 基本コンポーネントに関連する統合要件及び推奨事項。	基本コンポーネント評価者
	設計適合の証拠。 コンポジット製品が基本コンポーネント関連の統合要件及び推奨事項を満たしている証拠。基本コンポーネントの利用者ガイダンス及び基本コンポーネント評価監督機関の報告書によって課された依存コンポーネント設計に関する要件が、コンポジット製品においてどのように満たされているかについての証拠エレメントを包含している。そのような要件に従わなかった場	コンポジット製品インテグレータ 依存コンポーネント開発者

アクションエレメントを定義するSAR	必要な情報	情報の発信者
	合、選択されたコンポジット製品の実装が依然として安全であるという根拠をここに示さなければならない。	
	基本コンポーネント評価監督機関により作成された基本コンポーネント評価の報告書。 (追加)基本コンポーネント関連の統合要件及び推奨事項。	基本コンポーネント評価監督機関
コンポジット機能テスト (ATE_COMP)	テストに適したコンポジット製品サンプル。	コンポジット製品インテグレータ
コンポジット脆弱性評定(AVA_COMP)	*コンポジット評価用のETR*。 コンポジット製品評価者及び各評価監督機関が、基本コンポーネントについて検討・実施された攻撃経路やテスト、基本コンポーネントによって実装された対抗策の有効性、及び基本コンポーネントの利用者ガイダンスに含まれている統合の推奨事項に関連する基本コンポーネントの残存脆弱性に関連する説明を理解できる証拠資料。	基本コンポーネント評価者
	基本コンポーネント評価監督機関により作成された基本コンポーネント評価の報告書。 (追加)基本コンポーネント関連の統合要件及び推奨事項、義務、脆弱性に関する情報。	基本コンポーネント評価監督機関
	基本コンポーネント関連の利用者ガイダンス。	基本コンポーネント開発者

注：基本コンポーネント評価監督機関が作成した基本コンポーネント評価の報告書は、表3に直接記載されていなくても、SAR ASE_COMP、ALC_COMP及びATE_COMPにも関連することがある。

統合の場合、役割担当者を区別するために、「開発者」という用語をさらに明確にする必要がある。ここでは、基本コンポーネント開発者、依存性コンポーネント開発者、コンポジット製品インテグレータは、異なるエンティティである可能性がある。同様に、「評価者」と「評価監督機関(評価制度)」という用語についても、関係する異なるエンティティをさらに区別する必要がある。

基本コンポーネント及び依存コンポーネントの両方がすでに評価されている場合、以前の依存コンポーネントの評価ですでに得られた評価結果を考慮すると、量を減らした評価アクティビティで十分に実施できる可能性がある。しかし、本書で定義されているコンポジット評価タスクは、依然として必要である。

例：スマートカード

スマートカードアーキテクチャは、ハードウェアプラットフォーム及びプラットフォーム上のソフトウェアアプリケーションで構成されている。この場合、プラットフォームは基本コンポーネントであり、アプリケーションは依存コンポーネントである。コンポジット評価では、プラットフォームはすでに評価されており、アプリケーションはコンポジット評価の一部として評価され、プラットフォームの評価結果は再利用される。

ハードウェアプラットフォームは、コンポジット製品の資産保護をサポートする機能性を提供するが、コンポジット製品のふるまいは、セキュリティ機能性の使用、設定、及び起動を行うソフトウェアアプリケーションに依存する。

したがって、ハードウェアプラットフォームの評価結果は、通常、ソフトウェアアプリケーションの実装に対する特定のセキュリティ推奨事項及び条件を提供する。コンポジット評価には、両コンポーネントの組み合わせが悪用可能な脆弱性につながらないかどうかを検査することも含まれる。

コンポジット評価方法及び関連する評価アクティビティが提供され、プラットフォーム開発者から必要な情報を明確にしたステートメントを持つ正確なワークユニットを含み、プラットフォーム評価者からコンポジット製品評価者への情報伝達のための合意された「枠組み」を提供する。

必要な情報は、プラットフォーム評価タスクからすでに入手可能であり、プラットフォーム開発者からの追加作業は必要ない。

開発(ADV)クラスには、さらなる要件はない。

プラットフォームの利用者ガイダンス(AGD)は、コンポジット製品の開発の初期に検討され、情報が必要とされる全てのインタフェースを提供する。

コンポジット製品の開発及び評価は、プラットフォームの評価済みインタフェースの適切な実装に依存する。

プラットフォームとアプリケーション間の関連する全てのインタフェースの適切な使用は、コンポジット評価の範囲内である。

テスト(ATE)及び脆弱性評定(AVA)は、利用可能なプラットフォーム評価結果を活用してコンポジット製品に対して実施される。

14.3.3.6 コンポジット評価用のETR(ETR_COMP)

14.3.3.6.1 文書の目的

コンポジット評価用のETR(ETR_COMP)文書は、そのようなすでに評価済みの基本コンポーネントとのコンポジット評価に必要な情報を提供するために、基本コンポーネントとその評価に関する評価報告書(ETR)から編集される。

注1：標準ETRには通常、基本コンポーネントとその評価に関する専有情報を含んでおり、公開することができない。したがって、このような完全なETRは、外部への配付には適していない可能性がある。ETR_COMP文書に記載される情報は、コンポジット評価をサポートするための基本コンポーネントの完全なETRで提供される情報の重要なサブセットを含んでいる。

ETR_COMP文書の目的は、コンポジット製品の評価者とコンポジット製品の評価監督機関が、基本コンポーネントに対して検討及び実行された攻撃経路とテスト、及び基本コンポーネントによって実装された対策の有効性を理解できるようにすることである。

注2：ETR_COMP文書の内容は、一方では基本コンポーネント開発者及び/又は基本コンポーネント評価者の専有情報を保護し、他方ではコンポジット製品評価者及びコンポジット製品評価監督機関に十分な情報を提供する間の適切なバランスを取る。

14.3.3.6.2 手順

ETR_COMPは、基本コンポーネント評価者が基本コンポーネント評価結果に基づいて作成し、基本コンポーネント評価に関連する完全なETRから導出される。

ETR_COMPは基本コンポーネント評価の一部である。ETR_COMPは基本コンポーネント評価のスポンサーからの要求により提供され検証される。特に基本コンポーネントの評価監督機関の報告書は、基本コンポーネント評価に関わる全ての関係者(すなわち、基本コンポーネント評価者、基本コンポーネント評価監督機関、基本コンポーネント開発者、基本コンポーネント評価のスポンサー)がETR_COMPを受け入れることを宣言している。このようなETR_COMPの検証ステートメントは、特にETR_COMPと元のETRとの一貫性を扱う。ETR_COMPは、基本コンポーネントの基本コンポーネント評価監督機関の報告書において、さらなる再利用のために参照される。

コンポジット評価でETR_COMPを再利用する場合、基本コンポーネント評価の枠組みで基本コンポーネント評価監督機関がETR_COMPを事前に受理していることが要求される。ETR_COMPは、コンポジット評価で使用するために、コンポジット製品評価者及びコンポジット製品評価監督機関に提供される。

ETR_COMPは、基本コンポーネント評価の一部であるため、基本コンポーネント評価者及び基本コンポーネント評価監督機関により、コンポジット評価のアプローチ及びコンポジット製品における基本コンポーネントの意図された安全な使用を考慮して、十分な情報がETR_COMPに提供されることが保証される。

ETR_COMPの受理後に、ETR_COMPで十分に対処されていない基本コンポーネントのセキュリティ問題が発見された場合、基本コンポーネント評価監督機関は、取るべきアクションを決定する。これには、ETR_COMPの適切な更新及び、この更新されたETR_COMPのその後の検証を含めることができる。

さらに、基本コンポーネント評価の一環として、基本コンポーネント評価者は、関連するETR_COMPの基本コンポーネントに対する推奨事項が、基本コンポーネントの利用者ガイダンスに記載されている要件に関して一貫した完全なものであることを保証する。基本コンポーネントの評価監督機関報告書の発行までに解決できない矛盾(要件の欠落を含む)が見つかった場合、基本コンポーネントの評価監督機関は、基本コンポーネントの評価監督機関の報告書に依存コンポーネント開発者の補足情報を追加できる。

コンポジット評価において、現在の基本コンポーネント自体が以前のコンポジット評価に依存しており、現在の評価の依存コンポーネントと以前の基本コンポーネントとの間に直接インタフェース

がある場合、以前のコンポジット評価のETR_COMPも現在のコンポジット製品評価者とコンポジット製品評価監督機関に供給される。

14.3.3.6.3 コンポジット評価用のETRの授受について

ETR_COMP文書は、基本コンポーネント評価者が作成・維持する。しかし、コンポジット評価の場合は、基本コンポーネント開発者が依存コンポーネント開発者の連絡先となる。

依存コンポーネント開発者は、基本コンポーネント開発者に連絡し、ETR_COMPをコンポジット製品評価者の連絡先に配付してもらう。基本コンポーネント開発者は、機密管理規則をチェックし、配付が可能かどうかを判断する。必要であれば、基本コンポーネント開発者は、基本コンポーネント評価監督機関にETR_COMPの配付の意図について連絡する。

基本コンポーネント開発者は、基本コンポーネント評価者に連絡し、コンポジット製品評価者の所定の連絡先へのETR_COMPの配付(セキュアな方法を用い、マークされたバージョンのみを配布)を要求する。配付が許可された場合、基本コンポーネント評価者又は基本コンポーネント開発者のどちらかが、両者の合意に応じてETR_COMPをコンポジット製品評価者に送信する。ETR_COMPの配付プロセスは、基本コンポーネント開発者と基本コンポーネント評価者の間の(通常は契約上の)合意に依存するため、記述された手順から逸脱する可能性がある。ETR_COMP文書は、コンポジット製品評価者への提供時と同様の授受手順を用いて、コンポジット製品評価監督機関にも提供される。

必要に応じて、基本コンポーネント評価者及びコンポジット製品評価者は、追加情報又はより詳細な情報を授受する。これは、常に基本コンポーネント開発者の管理下に置かれる。明確化する場合、基本コンポーネント評価者とコンポジット製品評価者が主な当事者となる。追加の保証ステートメントが必要な場合は、基本コンポーネント評価監督機関も授受に関与する。

複数当事者による情報の授受では、情報の授受及び保護のために識別された全ての管理を考慮することが重要である。

14.3.3.6.4 コンポジット評価用のETRの内容

ETR_COMP文書で提供することが要求される情報は以下のとおりである。

a) 評価済み基本コンポーネントに関する情報

ETR_COMPのこの節は、以下を含む基本コンポーネントの評価に関する正式な情報を提供しなければならない。

— ETR_COMP のバージョン情報

— 基本コンポーネントの曖昧でない識別情報

— 基本コンポーネントの開発者及びスポンサーの識別情報

— 基本コンポーネント評価者及び基本コンポーネント評価監督機関の識別情報

— 基本コンポーネント評価の保証レベル

— 合格/不合格などの正式な評価結果

— 基本コンポーネント及びその評価に関連する ETR への参照

b) 基本コンポーネントの設計に関する情報

ETR_COMPのこの節は、保証クラスADVが要求する成果物に基づいて、基本コンポーネント及びその主要コンポーネントのハイレベルな記述を提供しなければならない。

この節の意図は、基本コンポーネントの主要コンポーネントのアーキテクチャ上の分離の程度を特徴付けること、基本コンポーネントとこの基本コンポーネントを使用する依存コンポーネントとの間の可能な技術依存性を示すこと、及び基本コンポーネント評価の対象となる基本コンポーネントのセキュリティメカニズムを概説することである。

c) 基本コンポーネントの評価済み構成に関する情報

ETR_COMPのこの節は、開発者の構成リスト又は必要に応じて、あるいはケースバイケースで関連する部分に基づいて確立された基本コンポーネントの評価済み構成に関する情報を提供しなければならない。基本コンポーネントは明確に識別可能でなければならず、この識別情報は、基本コンポーネントの評価監督機関の報告書に記載された評価済み構成とリンクされていなければならない。

該当する場合、基本コンポーネントのセキュリティに関連する生成及び設置パラメタ設定を説明し、攻撃に対する防御に及ぼす影響を概説しなければならない(例えば、鍵長、カウンターの上限)。これには、期待される評価済み構成が使用されることを保証するために、依存コンポーネント開発者及び依存コンポーネント評価者がこれらの設定の値を検証する方法を含まなければならない。

この証拠には、基本コンポーネントがセキュアな方法で構成されていることを保証するために、関連する利用者ガイダンスに概説されている基本コンポーネントの設置、生成、起動の手順を含めることができる。

d) 配付手順、関係する開発者及び製造サイト、及びデータ交換に関する情報

コンポジット評価を支援するために、基本コンポーネントの配付手順、依存コンポーネントの受入れ手順、及び開発・製造中に統合される関連データの両方の評価証拠が必要である。

ETR_COMPは、基本コンポーネントの開発・製造に関わるサイトの概要を、各サイトの役割と最新の監査日を含めて、提供しなければならない。

e) 基本コンポーネントの侵入テストに関する情報(考慮された攻撃経路及びテスト結果の概要を含む)、基本コンポーネントのサポート機能の侵入テストに関する情報。

ETR_COMPのこの節は、基本コンポーネントの評価者が基本コンポーネントに対して実施した独立した脆弱性分析に関する情報を、考慮された攻撃シナリオ、実行した侵入テスト、及び攻撃能力の対応するレーティング(見積もり)への言及とともに提供しなければならない。

侵入テストに関する情報は、以下を含まなければならない。

— 脆弱性分析で扱われた全ての攻撃方法を示す概要。

— 考慮された攻撃シナリオや攻撃経路を理解するために必要な詳細。

— 実施された侵入テストの評定とその結果。

攻撃シナリオの記述は、コンポジット製品に追加の対抗策を必要とする攻撃を再現する際に、コンポジット製品の評価者をサポートするために十分な詳細を提供しなければならない。

基本コンポーネントの潜在的脆弱性を基本コンポーネントのガイダンスに従うことで解決しなければならない場合、ガイダンスの特定の節又は可能であればガイダンスの要素への参照を含む要約で、これを明確に概説しなくてはならない。

f) 所見及び推奨事項

評価済みの基本コンポーネント利用者ガイダンスは、基本コンポーネントSTに定義されたセキュアな方法で基本コンポーネントを利用するために必要な全ての情報を含んでいなければならず、特に残存脆弱性や予期せぬふるまいを回避する方法に関する情報を含んでいなければならない。基本コンポーネント評価者は、ETR_COMPが、基本コンポーネント利用者ガイダンスにおいて要件としても扱われている、基本コンポーネントのセキュアな使用に関する推奨事項のみを含むことを保証しなければならない。基本コンポーネント評価者は、基本コンポーネント利用者ガイダンス及びETR_COMPの推奨事項が一貫していること、依存コンポーネント開発者が設計適合の分析を実行できるように利用者ガイダンスの要件が十分具体化されていることを保証しなければならない。

しかし、場合によっては、基本コンポーネントガイダンスの他に追加的な詳細情報が、コンポジット製品評価者が以下のようなコンポジット評価を実施するために必要となる場合がある。

— 基本コンポーネント評価結果に対する所見(例えば、基本コンポーネント評価のための特定の基本コンポーネント構成)。

— コンポジット製品の評価者に対する推奨事項/条件：基本コンポーネント評価結果の使用に関する特定の情報(例えば、コンポジット評価の際に必要な具体的なテストについて)。

このような所見又は推奨事項/条件は、基本コンポーネント評価者及び/又は基本コンポーネント評価監督機関からのものである。

ETR_COMP文書は、STやガイダンスなど、利用可能な他の基本コンポーネントの証拠から情報を複製(例えば、テキストをコピー)することを意図していない。ただし、コンポジット評価は、そのような基本コンポーネント証拠の該当箇所を参照することでサポートされる。

14.3.3.7 報告書及びその妥当性

コンポジット評価の結果は、コンポジット製品のETRという形式でコンポジット製品評価監督機関に提供される。このコンポジット製品ETRには、他の情報の中でも、現在のコンポジット評価の範囲内にある各保証コンポーネントの部分判定に基づくコンポジット評価の最終総合判定が含まれなければならない。コンポジット評価手法の使用法は、コンポジット製品ETR及び該当する場合は、コンポジット製品評価監督機関のコンポジット製品の報告書に示されなければならない。

コンポジット製品及びそのコンポジット評価は、基本コンポーネント及びその関連評価をカバーするため、コンポジット評価は、基本コンポーネントの評価監督機関の報告書の妥当性及び時事性に結びついている。コンポジット製品評価者及びコンポジット製品評価監督機関は、基本コンポーネントに関する基本コンポーネント評価監督機関の有効かつ最新の報告書、又は最低限、当該評価監督機関の報告書の状況についての基本コンポーネント評価監督機関の評定を必要とする。

注1：コンポジット製品評価監督機関は、基本コンポーネントのETR_COMPが有効でない、又は最新でないため、特にその(時代遅れ又は不十分な)脆弱性分析や侵入テストのために、コンポジット評価での再利用に適さない場合、一般的に基本コンポーネントの再評定を求めることがある。この再評定は、脆弱性分析及び侵入テスト(サーベイランスプロセス)の更新に焦点を当てた基本コンポーネントの再評価、又は代替案として、基本コンポーネント評価監督機関の確認ステートメントで構成される。

注2：基本コンポーネントのETR_COMPが関連するコンポジット評価タスクの提出前に発行され、その間に基本コンポーネントに対する最先端の関連する攻撃の実行に大きな変化が生じた場合(例えば、攻撃方法又は攻撃レーティングの大きな変化)、コンポジット製品評価監督機関は、特に新しい攻撃問題に焦点を当てた基本コンポーネントの再評定又は再評価を要求する可能性がある。

注3：報告書(ここでは特に基本コンポーネント評価監督機関の基本コンポーネント関連報告書及びETR_COMP)の有効性及び時事性を決定する規則は、それぞれの評価制度によって定義され、具体的に定義された有効期間に関連付けることができる。

注4：基本コンポーネントのテストの結果、コンポジット製品評価者が何らかの不具合(例えば、攻撃方法や技法の向上による脆弱性)を検出した場合、これらの結果はコンポジット製品評価監督機関に伝達される。コンポジット製品評価監督機関は、基本コンポーネント評価監督機関とともに、基本コンポーネントの再評定や再評価を求めるなど、適切な措置を講じる。

コンポジット製品全体が、互いに構築されたコンポジット製品の連鎖として設定されている場合(基本コンポーネント自体がすでにコンポジット製品である場合など)、このコンポジット製品の連鎖で使用される各ETR_COMP及び評価監督機関報告書の有効性及び最新性が必要である。また、コンポジット製品全体のコンポジット評価で結果を再利用する際には、下位のETR_COMPから上位のETR_COMPへの依存性を全て考慮する。

注5：製品の評価監督機関報告書は、各評価監督機関による製品の評価及びその結果の受入れを宣言する(すなわち、評価監督機関による関連ETRの受入れがなされる)ものである。特に、このような報告書は、製品の評価がCCに従って実施されたことを宣言する。

現在のコンポジット製品及びそのコンポジット評価に対する基本コンポーネント評価監督機関の基本コンポーネントの報告書及びETR_COMPの有効性、時事性及び関連性は、コンポジット製品に対するコンポジット製品評価監督機関の報告書によって認められる。これには、基本コンポーネントの評価が、現在のコンポジット評価とは別のバージョンのCC及びCEMに適合して実施された場合、異なるCC及びCEMのバージョンに属する単一保証コンポーネント(ひいては保証レベル)の同等性の決定及び受け入れが含まれる。

コンポジット製品評価監督機関は、以下の場合、コンポジット製品に対する報告書を発行する。

— コンポジット製品ETRにおけるコンポジット評価の最終総合判定が「合格」である、及び

— 基本コンポーネント評価監督機関の基本コンポーネントの報告書及びETR_COMPの有効性、時事性、関連性が、現在のコンポジット製品及びそのコンポジット評価に対してコンポジット製品評価監督機関によって認められている。

14.4 統合の技法を用いた評価の要件

14.4.1 評価結果の再利用について

IT製品にコンポーネントを統合する場合、製品の単一コンポーネントがすでに評価されており、そのようなコンポーネントの既存の評価結果を再利用することができる可能性がある。しかし、IT製品全体のセキュリティ保証を確認するためには、通常、追加の評価アクティビティが要求され、実行される。

IT製品(TOE)のそのようなコンポーネントに関連する評価結果及び証拠を再利用するには、IT製品(TOE)全体の評価にそれらが利用可能であることが必要である。

14.3.2及び14.3.3は、階層化統合モデルの評価技法を扱う。14.3.2では、統合TOEに対するCCパート3で定義されたACOクラスの使用法を記述し、14.3.3では、コンポジット製品の評価技法を規定する。

IT製品(TOE)のコンポーネントの評価結果及び証拠の再利用は、以下の条件に依存する。

— IT製品(TOE)に使用される統合モデル。

— IT製品(TOE)全体、特にコンポーネント及びそのセキュリティ保証との関係で主張されるセキュリティ保証。

— IT製品(TOE)及びそのコンポーネントに対して主張されるセキュリティ特性。

例：分離、情報フロー制御、耐障害性は、セキュリティ特性の例である。

14.4.2 統合評価の論点

14.4.2.1 統合の根拠

14.2に記述されている統合モデルを使用してコンポーネントからIT製品(TOE)を統合し、その評価に統合の技法を使用する場合、IT製品の評価のために(例えば、コンポジット/統合製品のSTにおいて)統合の根拠が提供されなければならない。これには、少なくとも以下の分析が含まれる。

— IT製品(TOE)に使用される統合モデル

— 特にそのコンポーネント及びそのセキュリティ保証に対する関係において、TOE全体に対して主張されるセキュリティ保証

— コンポーネント及びその機能性のインタフェース及び依存性

— コンポーネントのセキュリティ機能方針及びOSPの統合可能性

— コンポーネントのセキュリティ特性の保持

— 組込み統合モデルについては、正確性の側面

14.4.2.2 脆弱性分析

14.2に記述されている統合モデルを使用してコンポーネントから統合され、その評価に統合の技法を使用するIT製品は、IT製品の提案されたEALを考慮して、CCパート3に記載されたAVAクラスに従って、脆弱性分析を受けなければならない。コンポーネントの脆弱性分析結果を再利用することは可能だが、IT製品(TOE)全体に対する追加の脆弱性分析アクティビティを設計し、実行しなければならない。

脆弱性分析は、IT製品とそのコンポーネントの分析を考慮して設計しなければならない。

14.4.2.3 テスト

14.2に記述されている統合モデルを使用してコンポーネントから統合され、その評価に統合の技法を使用するIT製品は、CCパート3に記載されたATEクラスを使用して、追加テストを受けなければならない。コンポーネントのテスト評価結果を再利用することは可能であるが、IT製品(TOE)全体に対する追加テストを設計し、実行しなければならない。

テストは、IT製品及びそのコンポーネントの解析を考慮して設計されなければならない。

14.4.2.4 統合TOEのためのACOクラスの使用

CCパート3では、統合TOEの評価をサポートするために使用されることを意図したセキュリティ保証コンポーネントを規定するACOクラスを記述している。

CCパート5では、統合TOEの事前に定義された保証パッケージ(CAP：Composed Assurance Package)のファミリを規定しており、得られる保証のレベルと、統合TOEのそのような保証を取得するコスト及び実現可能性とのバランスをとっている。

CAPは、統合製品の提案されたEALを考慮し、指定された厳密さで、正しく統合が行われたことを保証するように設計されている。

14.4.2.5 コンポジット製品に対するコンポジット評価技法の使用

CCパート3は、異なる保証クラスのCOMPファミリを記述しており、コンポジット製品の評価をサポートするために使用することを意図したセキュリティ保証コンポーネントを規定する。これらのCOMPファミリは、コンポジット特有の評価の側面及び問題に対処するために、CCパート3で定義されている他のすでに存在する保証ファミリを適切に補完する保証ファミリとして設定されている。

COMPファミリは、コンポジット製品の提案されたEALを考慮し、指定された厳しさで、統合が正しく実行されたことを保証するように設計されている。

コンポジット製品の評価にコンポジット評価技法を使用するには、対応するETR_COMP及び基本コンポーネント評価監督機関の有効な報告書を伴う、すでに評価済みの基本コンポーネントが必要である。

14.5 統合及びマルチ保証による評価

統合及びマルチ保証の概念は、異なる課題を解決することを目的としている。要約すると、統合評価及びコンポジット評価は、特に複数の役割担当者が関与するTOEに適しており、過去の評価結果の再利用を可能にする評価プロセスを指す。一方、マルチ保証は、特定のセキュリティ課題と運用環境の文脈におけるいくつかのTOEの特性を指す。

統合による評価では、各当事者が開発したセキュリティ機能性の評価を担当する、複数の当事者が関与する可能性があるサプライ及び/又は統合チェーンを持つTOEに対応する。CCは、評価プロセスにおいて評価結果を再利用するための2つのアプローチを標準化している。

a) 統合評価では、相互作用するサブTOEの個々の保証レベルから、TOEの統合保証レベルを取得できる。

b) コンポジット評価では、まずベース層を最初に評価し、ベース層の評価結果を再利用して統合される依存層とベース層を評価するという段階的な方法で階層化されたTOEのEALを得ることを可能にする。

マルチ保証評価では、TOE全体のグローバルな保証レベルを保証しながら、セキュリティ機能性の異なる部分(サブTSF)に異なる保証ニーズが適用されるTOEに焦点を当てる。マルチ保証が導入される以前は、このようなニーズがある場合、スポンサーは同じTOEについて、異なるSTに対して複数の評価を受けなければならなかった。CCは、この概念を用いて、このプロセスを標準化し、最適化する。

TOE/TSFの観点から、マルチ保証評価はあらゆるアーキテクチャに適用され、統合による評価は特定のアーキテクチャに適用される。統合評価は、複数の相互作用するサブTOEからなるTOEに適用され、コンポジット評価は、依存層がベース層に依存しているTOEに適用される。

実際には、マルチ保証及び統合による評価は、評価において併用することができる。

附属書A
(規定)

パッケージの仕様

A.1 本附属書の目的及び構造

この附属書の目的は、パッケージの仕様に関するさらなる情報を与えることである。

注：CCパート3は、パッケージが個別に評価されないため、パッケージの評価基準を定義していない。パッケージがPP、PPモジュール、又はSTに組み込まれると、パッケージの評価は暗黙的に行われる。

A.2 パッケージファミリ

A.2.1 一般

図A.1にパッケージファミリの構造を示す。各部分については以下で説明する。

A.2.2 パッケージファミリ名

関連する目的を持つパッケージは、パッケージファミリとして提示される。この場合、パッケージファミリ名は必須であり、パッケージファミリスポンサーは一意の名前を割り当てるように努める。

A.2.3 パッケージファミリ概要

パッケージファミリとして提示されるパッケージには、ファミリの概要を記載する節があり、ファミリを高いレベルで記述している。

A.2.4 パッケージファミリの目的

パッケージファミリの目的の節は、ファミリの意図を表す。

A.2.5 パッケージ

パッケージファミリには、以下のようなパッケージが1つ以上含まれる。SARのパッケージ及びSFRのパッケージは、同じファミリに混在しない。

A.3 パッケージ

A.3.1 パッケージの必須の内容

A.3.1.1 パッケージ識別

パッケージ識別には、以下のものがある。

a) パッケージの名前。名前は、パッケージの意図に関する一意の記述的情報を提供する。

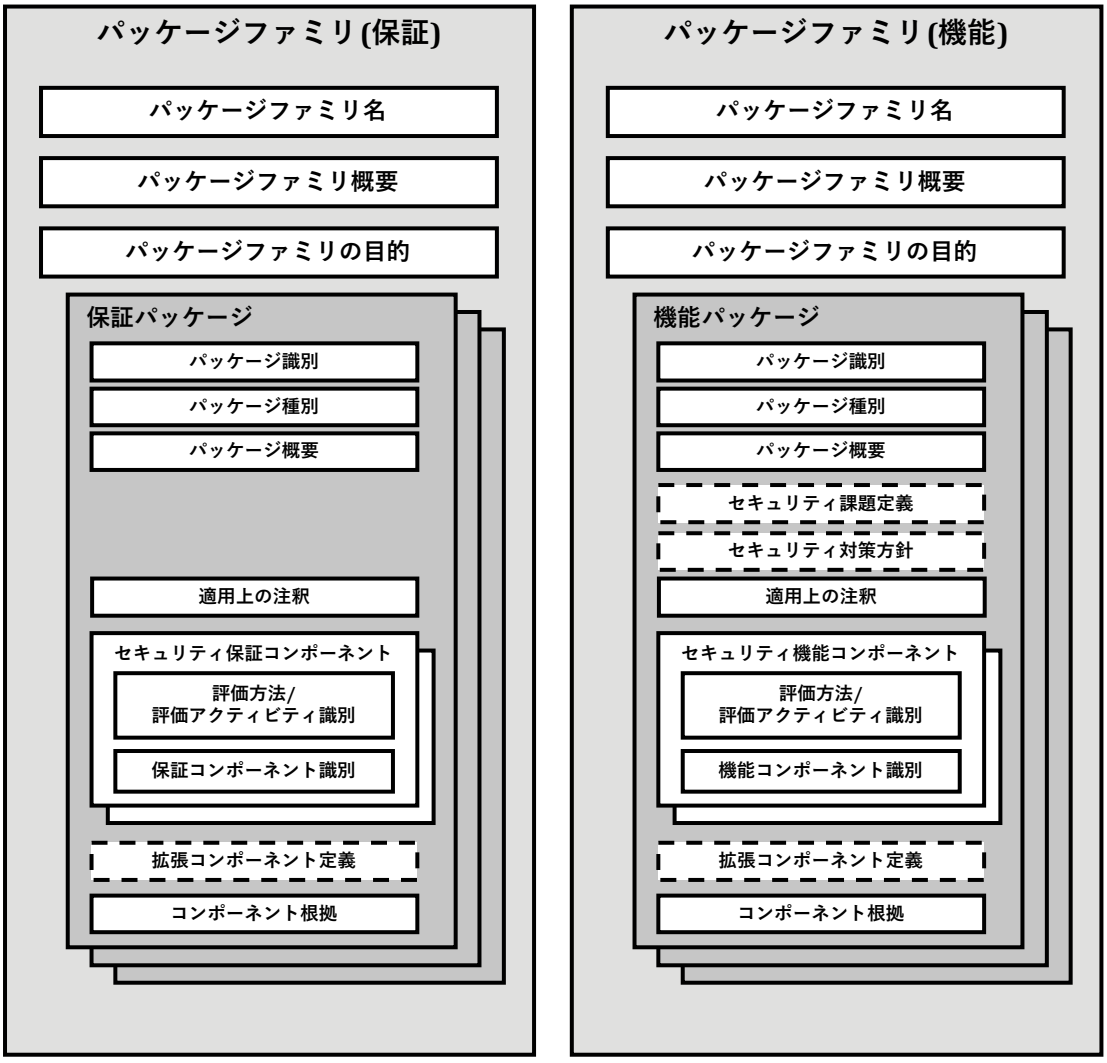
b) パッケージのバージョン情報

c) 最終更新日

d) スポンサー

e) 使用されるCCの版への参照

パッケージには、短い名前も付けることもできる。



図A.1 — 保証パッケージ又は機能パッケージを含むパッケージファミリの構造

例：評価保証レベル1は、「EAL1」とも呼ばれる。

注：CCパート5で定義されたパッケージについては、b)～e)の項目は、CCパート5の版情報に暗黙的に含まれる。

A.3.1.2 パッケージ種別

パッケージは、以下のいずれかの種別として識別される。

a) 機能パッケージ、又は

b) 保証パッケージ

A.3.1.3 パッケージ概要

パッケージは、上位レベルの概要及びパッケージの意図を記載する節を含む。

A.3.1.4 適用上の注釈

適用上の注釈は、以下の例外を除き、任意である。

— 機能パッケージの場合、パッケージに含まれるSFRに関連する追加の監査及び管理要件は、適用上の注釈の節で特定されなければならない。

— 機能パッケージは、他の機能パッケージへの依存性を持つことがある。このような依存性は、機能パッケージに文書化しなければならず、またPP、PPモジュール、又はSTに文書化することもできる。

機能パッケージは、そのパッケージでは満たされないが、そのパッケージを使用する他のパッケージ、PP、PPモジュール、又はSTで満たされることが期待される依存性を持つコンポーネントを指定することもできる。

例：暗号プロトコル(例えば、TLS)の仕様を含むパッケージで、上位レベルのSFRコンポーネントはパッケージで指定されているが、暗号プリミティブは指定されていない。

この場合、依存コンポーネントのオプションリストを機能パッケージの適用上の注釈に記載し、それらのSFRに必要な選択/割付などの追加情報を含めることができる。

注：パッケージの利用者には、PP、PPモジュール、他のパッケージ及びSTの作成者、インテグレータ、評価者が含まれる。

A.3.1.5 コンポーネント(SFR又はSARのいずれか)

パッケージに含まれるセキュリティ要件が記載される。この節ではまた、要件の選択の根拠を提供する。

セキュリティ要件は、選択ベースの要件であってもよい。8.2.4.2を参照のこと。オプションのSFR(及び必要に応じてサポートするSPDエレメント及び対策方針)は、機能パッケージで指定することもできる。

A.3.2 パッケージのオプションの内容

A.3.2.1 セキュリティ課題定義(SPD)(機能パッケージ)

保証パッケージは、この節を含まない。

機能パッケージは、この節を含むことができる。

この節には、機能パッケージが対処するセキュリティ課題を記述するSPDエレメントが含まれる。オプションのSFRに関連するSPDエレメントは、この節で定義することができる。適用上の注釈は、

セキュリティ対策方針(該当する場合)及びオプションのSPDエレメントが関連するSFRを識別するために使用されなくてはならない。

A.3.2.2　セキュリティ対策方針(機能パッケージ)

保証パッケージは、この節を含めてはならない。

機能パッケージは、この節を含むことができる。

直接根拠PP/PPモジュール/STに使用される機能パッケージの場合、TOEのセキュリティ対策方針は含まれてはならない。

機能パッケージのセキュリティ対策方針の節は、SPDから導き出された追加的なTOEセキュリティ対策方針又は運用環境のセキュリティ対策方針を提示する。オプションのSFRに関連するTOEのセキュリティ対策方針は、該当する場合、この節で定義することができる。適用上の注釈は、オプションのセキュリティ対策方針が関連するSPDエレメント及びSFRを識別するために使用されなくてはならない。

A.3.2.3　適用上の注釈

パッケージに適用上の注釈の記載するのは任意である。A.3.1.4を参照のこと。

適用上の注釈の節は、パッケージの利用者が特に関心を持つ情報を含めることもできる。表現は非形式的であり、例えば、使用上の制約及び特別な注意が必要となる領域に関する警告が扱われる。

A.3.2.4　拡張コンポーネント定義

パッケージは拡張コンポーネントを含むことができる。この場合、パッケージには、拡張コンポーネント定義を記載する節が含まれる。

A.3.2.5　評価方法/評価アクティビティ

パッケージは、CEMから派生した評価方法/評価アクティビティを含むことができる。評価方法/評価アクティビティが含まれる場合、適合ステートメントをパッケージのセキュリティ要件の節に含めなければならない(9.4参照)。評価方法/評価アクティビティは、パッケージ文書内で提供してもよいし、外部文書を参照してもよい。

附属書B
(規定)

プロテクションプロファイル(PP)の仕様

B.1 本附属書の目的及び構造

この附属書の目的は、PPの構造及び期待される内容を要約することである。

注1：この附属書は、PPの評価の要件を定義していない。PPの評価基準は、CCパート3のAPEクラスに記載されている。

注2：この附属書は、PP構成とPPモジュールの仕様の要件を規定していない。これらは、附属書Cに記載されている。

この附属書は、以下の主要なパートから構成される。

a) *PPの仕様*

これは、B.2.にまとめられており、以下を含む。

— *PPをどのように使用するか*

— *PPをどのように使用しないか*

b) *PPが含まなければならないもの*

これはB.3にまとめられており、B.3.2からB.3.7でPPの必須の内容、これらの内容間の相互関係、及び例を示してより詳細に記述されている。

c) *標準への適合主張*

B.4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記述する。

d) *直接根拠PP*

直接根拠PPは、SPDの脅威及びOSPがSFRに直接マッピングされ、場合によっては運用環境のセキュリティ対策方針にマッピングされるPPである。これらについてはB.5で詳細に説明する。

B.2 PPの仕様

B.2.1 PPの使用方法

一般に、PPはニーズのステートメントであり、利用者コミュニティ、規制機関、又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。PPは、消費者にこのセットを参照する手段を与え、これらのニーズに対する将来の評価を容易にする。

他の用途を排除するものではないが、PPは通常、次のように使用される。

— 特定の消費者又は消費者グループのための要件仕様の一部であり、その消費者は特定の種別のIT製品がPPを満たしている場合にのみ購入を検討する。

— 特定の規制機関による規制の一部であり、その規制機関は特定の種別のIT製品がPPを満たしている場合にのみ使用を許可する。

— 様々な消費者から提示される共通のセキュリティ課題に対処するため、多くの場合、複数のIT製品開発者を含むグループによって定義され、開発者は共通の市場のニーズを満たすためにこの種別のIT製品を製造する。

B.2.2 PPを使用しない方法

多くの役割の中で、PPが果たさない役割の2つは以下のものである。

— 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の一部となるべきでない。これは、一般にPPは完全な仕様の一部であるが、完全な仕様そのものではないことを意味する。

— 単一製品の仕様

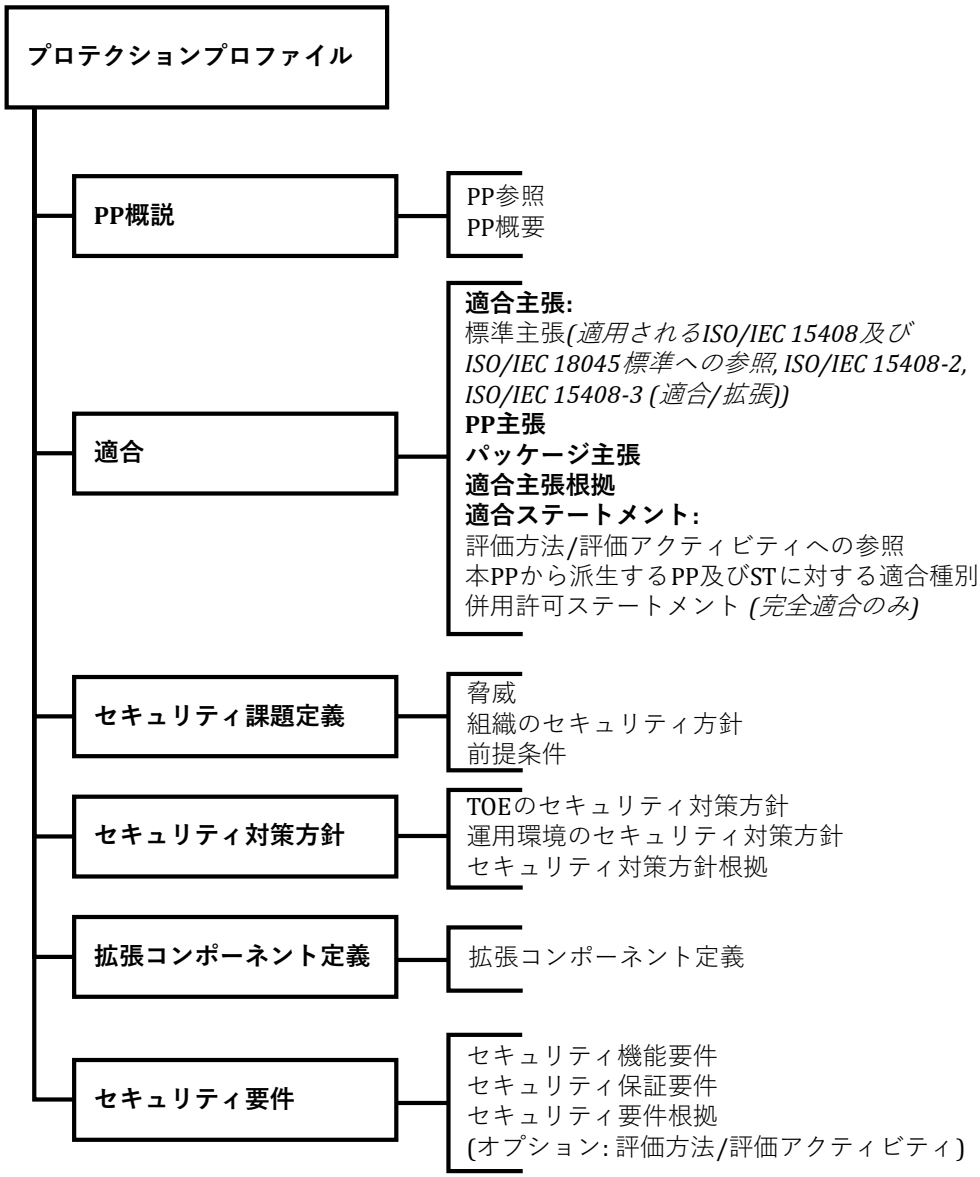
STとは異なり、PPは単一の製品ではなく、IT製品の特定の種別について記述することを目的とする。単一製品のみを記述する場合は、この目的のためにSTを使用することが望ましい。

B.3 PPの必須の内容

B.3.1 一般

PPには2つの種別がある。第一に、「通常の」PPであり、B.3.2からB.3.7に記述されるような完全な内容を含むPPである。第二に、場合によっては、PP作成者は、TOEのセキュリティ対策方針を含むPPとは異なる内容を持つ直接根拠PPを書くことができる。直接根拠PP、及びそれが使用される理由と状況については、B.5で詳細に記述する。本附属書の全ての他の部分では、全ての内容を含むPPを前提としている。

図B.1は、CCパート3に記載されるPPの内容を示す。図B.1はPPの構造的な概要として使用することもできるが、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、PPの附属書にそれを含めることができる。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.3.2からB.3.7でより詳細に説明する。



図B.1 — プロテクションプロファイルの内容

PPは以下を含む。

a) *PP概説*。PP参照及びTOE種別の叙述的記述を含む。

b) *適合主張*。以下を示す。

— CCのどの版の関連パートが適用されるか

— CCパート2及びCCパート3への適合(適合又は拡張)

— PPが他のPP及び/又はパッケージへの適合を主張しているかどうか、もしそうなら、どのPP及びパッケージへの適合を主張しているか、及びその適合の種別

c) *適合ステートメント*。以下を含む。

— CEMから派生した評価方法/評価アクティビティへの言及。

注：評価方法/評価アクティビティの詳細は、オプションとしてPP又は関連するサポート文書に含めることができる。

— 完全適合の場合、PPと組み合わせて使用できるPP及びPPモジュールを示す併用許可ステートメントは、PPのこの節に記載される。

— 派生するST及び他のPPに要求する適合種別。

d) *セキュリティ課題定義*。脅威、OSP及び前提条件を示す。

e) *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とオプションでTOEのセキュリティ対策方針との間でセキュリティ課題の解決策を分担する方法を示す。

f) *拡張コンポーネント定義*。新しいコンポーネント(つまりCCパート2又はCCパート3に含まれていない)を定義することができる。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。

g) *セキュリティ要件*。TOEのセキュリティ対策方針から標準化された言語への書き換えを提供する。この標準化された言語は、SFRの形式をとる。また、PPのこの節は、SARを定義する。

B.3.2 PP概説(APE_INT)

B.3.2.1 一般

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を簡潔に記述するTOE概要。

B.3.2.2 PP参照

PPは、その特定のPPを識別する明確なPP参照を含む。一般的なPP参照は、タイトル、バージョン、スポンサー、及び公表日から構成される。

注：ここで、PPのスポンサー(すなわち、PPの開発に責任を持つエンティティ)と、PPの作成者(PPの作成に責任を持つエンティティ)は区別される。

例：PP参照の例は、「Atlantean Navy CablePhone Encryptor PP, バージョン 2b, アトラス海軍調達局, 2020年4月1日」である。

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、一意にするべきである。PP参照によって、PPのインデックス化及び参照と、PPカタログへの組み込みが容易になる。

B.3.2.3 PP概要

B.3.2.3.1 一般

PP概要は、セキュリティニーズの仕様をサポートできるPPのカタログに目を通しているTOE種別の潜在的な消費者を対象としている。

PP概要は、PPを使用してTOEを設計したり既存製品を適合させたりする開発者も対象としている。

PP概要の一般的な長さは、数段落である。

このため、PP概要は、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で利用可能な主要な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.3.2.3.2 TOE種別の使用法及び主要なセキュリティ機能の特徴

TOE種別の使用法及び主要なセキュリティ機能の記述は、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考えを示すことを目的としている。この節は、PP作成者、TOE開発者、又は潜在的なTOE消費者のために書かれ、TOE種別の使用法と主要なセキュリティ機能を、TOE消費者が理解できる言葉を用いて、ビジネスの観点から説明する。

例：この例は、「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、最低1024人の利用者を許可し、最低500Mb/sの暗号化速度をサポートする。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。」である。

B.3.2.3.3 TOE種別

TOE概要は、PPが扱うTOEの一般的な種別を識別する。例えば、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、モバイルデバイス及びデータベース等である。TOE種別の定義には、TOEのソフトウェアとハードウェアの境界の特徴付けが含まれることが多い。

例：このTOE種別の記述の例は、セキュリティICプロテクションプロファイルから引用したものである。「評価対象(TOE)は、処理ユニット、セキュリティコンポーネント、I/Oポート(接触、非接触、又はUSB、MMCなどの類似インタフェース)、揮発性及び不揮発性メモリ(ハードウェア)で統合されたセキュリティ集積回路(セキュリティIC)である。TOEは、ICメーカーから配付される限り、IC開発者/メーカー独自のIC専用ソフトウェアも含むことができる。(中略)セキュリティIC上で動作するその他のソフトウェアは、セキュリティIC組み込みソフトウェアと呼ばれ、TOEの一部ではない。」

B.3.2.3.4 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

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/又はファームウェアに依存する。後者の場合に、PP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。

PPは特定の製品のために書かれるものではないので、多くの場合、利用可能なハードウェア/ソフトウェア/ファームウェアの一般的な考えしか示すことができない。場合によっては、より具体的な情報を提供することができる。

例1：より具体的な情報が提供される例として、プラットフォームがすでに知られている特定の消費者向けの要求仕様が挙げられる。

例2：ハードウェア/ソフトウェア/ファームウェアの識別の例を次に示す。

— なし(完全にスタンドアロンのTOE)。

— デュアルコア2.10GHz以上のプロセッサ及び4GB以上のRAMを搭載し、プロフェッショナル向けYaizaオペレーティングシステム、バージョン53.0 Update 6b、c、7、又はバージョン54.0を実行する標準的なPC。

— 2xQuad-Coreコアプロセッサと16GB以上のRAMを搭載し、Yaizaオペレーティングシステム、サーバ版バージョン7.0アップデート6dとWonderMagic 12.0グラフィックスカード、1.01 WMドライバセットを実行する標準64ビットサーバ。

— CleverCard SB17067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v12.0を実行するCleverCard SB17067集積回路。

— FP9プロセッサを使用するスマートフォン及びタブレット端末上のYaiza mobile-OS 3.1.6。

B.3.3 適合主張及び適合ステートメント(APE_CCL)

B.3.3.1 一般

PPの適合主張の項では、PPの以下の方法について記述する。

— PPが適用可能なCCの関連パートの版を述べる方法。

— PPがCCパート2及びCCパート3に適合(つまり、適合又は拡張)する方法。

— PPが他のPPを主張する方法(存在する場合)。

— PPがパッケージを主張する方法(存在する場合)。

PPがCCに適合する方法の説明は、使用されるCCの関連パートの版、及びPPが拡張セキュリティ要件を含むかどうか(10.3及びD.3.6参照のこと)の2つの項目から構成される。

PPが他のPPに対して適合を主張する記述は、PPが適合を主張する他のPPをリストすることを意味する。また、主張される適合の種別も識別される。この説明については、10.3を参照のこと。

パッケージに対するPPの適合の記述は、PPが適合を主張するパッケージをリストすることを意味する。この説明については、10.3を参照のこと。

注1：PPモジュールでの適合主張の使用については、C.2.2.5を参照のこと。

注2：直接根拠PPでの適合主張の使用については、B.5.2参照のこと。

PPの適合ステートメントの節は、PPの以下の方法について記述する。

— PPがCEMから派生した評価方法/評価アクティビティを参照する方法。

— PPがPP構成において、他のPP及びPPモジュールと組み合わせて使用することができる方法。完全適合の場合、適合ステートメントが必要である。

適合ステートメントにおいて、評価方法/評価アクティビティへの参照は、PPがPPへの適合を主張するSTに基づく評価中に使用する評価方法/評価アクティビティへの参照を提供することを意味する。これらの評価方法及びアクティビティは、PPに直接含まれる場合もあれば、参照されたサポート文書に記載される場合もある。これらの評価方法及びアクティビティのテキストをPPに再現する必要はない。10.3を参照のこと。

CEMから派生した評価方法/評価アクティビティがPPを評価するために使用される場合、関連するセキュリティ要件の節に次の形式のステートメントを含めることによって、これらを識別しなければならない。

「*このPPは、<参照> で定義された評価方法/評価アクティビティを使用することを要求する。*」

このステートメントで、*<参照>*は、関連する評価方法及び評価アクティビティの所在の識別に置き換えられる。この参照は、PPを含む文書に対してでも、1つ以上の別の文書に対してでもよい。

注3：13.5で概説したように、場合によっては、評価制度が特定のEM/EAを使用することを必ずしも承認しないことがある。

PPの適合種別では、ST及び/又は他の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、「完全」適合、「正確」適合又は「論証」適合のいずれを要求するかを選択する。

B.3.3.2 完全適合

完全適合が選択された場合、PP作成者は、該当する場合、PPの適合主張の節にある併用許可ステートメントに、以下の情報を指定しなければならない。

— このPPに基づくSTが使用する、又はPP構成で使用する、このPPとともに使用することができる他のPP。

— そのPPモジュールのPPモジュール基盤でこのPPを指定する可能性のあるPPモジュール、又はPPも含むPP構成に存在する可能性のあるPPモジュール。

注1：上記のオプションのいずれも行使されない場合、STは、PP自体のみに対する完全適合を主張することができる。

注2：PPは、他のPPに対する完全適合を主張することはできない。

B.3.4 セキュリティ課題定義(SPD) (APE_SPD)

脅威、前提条件、組織のセキュリティ方針(OSP)を含むSPDの情報及び要件については、7.1を参照のこと。

B.3.5 セキュリティ対策方針(APE_OBJ)

TOEのセキュリティ対策方針及び運用環境のセキュリティ対策方針を含むセキュリティ対策方針の情報及び要件については、7.2を参照のこと。

注：直接根拠の場合、TOEのセキュリティ対策方針は含まれない。

B.3.6 拡張コンポーネント定義(APE_ECD)

多くの場合、PPのセキュリティ要件は、CCパート2又はCCパート3に記載されているコンポーネントに基づく。B.3.7を参照のこと。しかし、場合によっては、PPの中にCCパート2又はCCパート3のコンポーネントに基づかない要件が存在する可能性がある。このような場合、新しいコンポーネント、すなわち拡張コンポーネントを定義しなければならず、その定義は「拡張コンポーネントの定義」の節で提供しなければならない。これに関する詳細は、8.4を参照のこと。

注：この節では、拡張コンポーネントのみを扱い、拡張コンポーネントに基づく拡張要件については扱わない。拡張要件は、B.3.7で説明されているようにセキュリティ要件の節に含まれており、全ての目的のために、CCパート2又はCCパート3に記載されたコンポーネントに基づく要件と同じように扱われる。

B.3.7 セキュリティ要件(APE_REQ)

B.3.7.1 一般

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化された言語への書き換え。

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。

これら2つのグループについては、7.3で説明する。

B.3.7.2 PPに要件を含める

他のPPに正確適合するPPの場合、このPPの全ての要件を含めなければならず、また、追加の要件を適合PPに含めてもよい。

他のPPに論証適合するPPの場合、このPPの全ての要件を含めなければならず、又は、それ以外に要件を満たす方法を説明する根拠を適合PPで提供しなければならない。

以下の種別の裁量的要件は、全ての(完全適合、正確適合及び論証適合)適合種別のPPに含めることができる。

PPがオプションの要件を含む場合、適合PPは、これらの要件に関連する必要なSPDエレメントを必ず含むように、これらの要件をインスタンス化してもよい。これは、PPが要求する適合に関係なく行うことができる。オプションのSFRを省略しても、PPへの「部分的適合」にはならないので、許可される。

B.4 PPでの他の標準の参照

場合によっては、PP作成者は特定の暗号標準又はプロトコルのような外部標準を参照する必要がある。CCでは、次の2つの方法でこれを行うことができる。

a) OSP(又はその一部)として。

例1：パスワードをどのように選択しなければならないかを定義する政府標準が存在する場合、これをPPのOSPとして記載することができる。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、あるいは、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、PP作成者の根拠によって、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正当化する必要がある。OSPがSFRによって実装される場合、評価者はこれが実際に正当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) コンポーネント又はセキュリティ要件の詳細化で使用される技術標準として。

例2

> FCS_CKM.1.1 詳細化。「選択：TSF、TOE プラットフォーム]は、指定された暗号鍵生成アルゴリズムに従って、非対称暗号鍵を生成しなければならない。
>
> [選択：
>
> 2048bit 以上の暗号鍵サイズを使用する RSA 方式で、以下を満たすもの：[選択
>
> FIPS PUB 186 4, “Digital Signature Standard (DSS)”, Appendix B.3;
>
> ANSI X9.31-1998, Section 4.1];
>
> 「NIST curves」P-256、P-384 及び[選択：P-521、その他の曲線なし]を使用する ECC 方式であって、以下を満たすもの：FIPS PUB 186 4, “Digital Signature Standard (DSS)”, Appendix B.4;
>
> 2048 ビット以上の暗号鍵サイズを使用する FFC 方式であって、以下を満たすもの：FIPS PUB 186 4, “Digital Signature Standard (DSS)”, Appendix B.1
>
>]」

標準の特定部分のみへの参照が意図されている場合、その部分は SFR の詳細化で明確に記述されなければならない。

注：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、その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。

B.5 直接根拠PP

B.5.1 一般

PPの作成は、PPを基礎として作成されるSTを考慮することを含む。D.4で述べたように、場合によっては、直接根拠STの仕様をサポートするPPを書くことが望まれる。

直接根拠PPの意図は、SPD、運用環境のセキュリティ対策方針、及びSFRの間の間接的なレベルを最小化することである。

状況によっては、TOEのセキュリティ対策方針の定義を省略することが適切な場合がある。この場合、自然言語による記述で強化されたSFR及び環境の対策方針は、SPDに直接対応する。

直接根拠PPは、以下のように構成される。

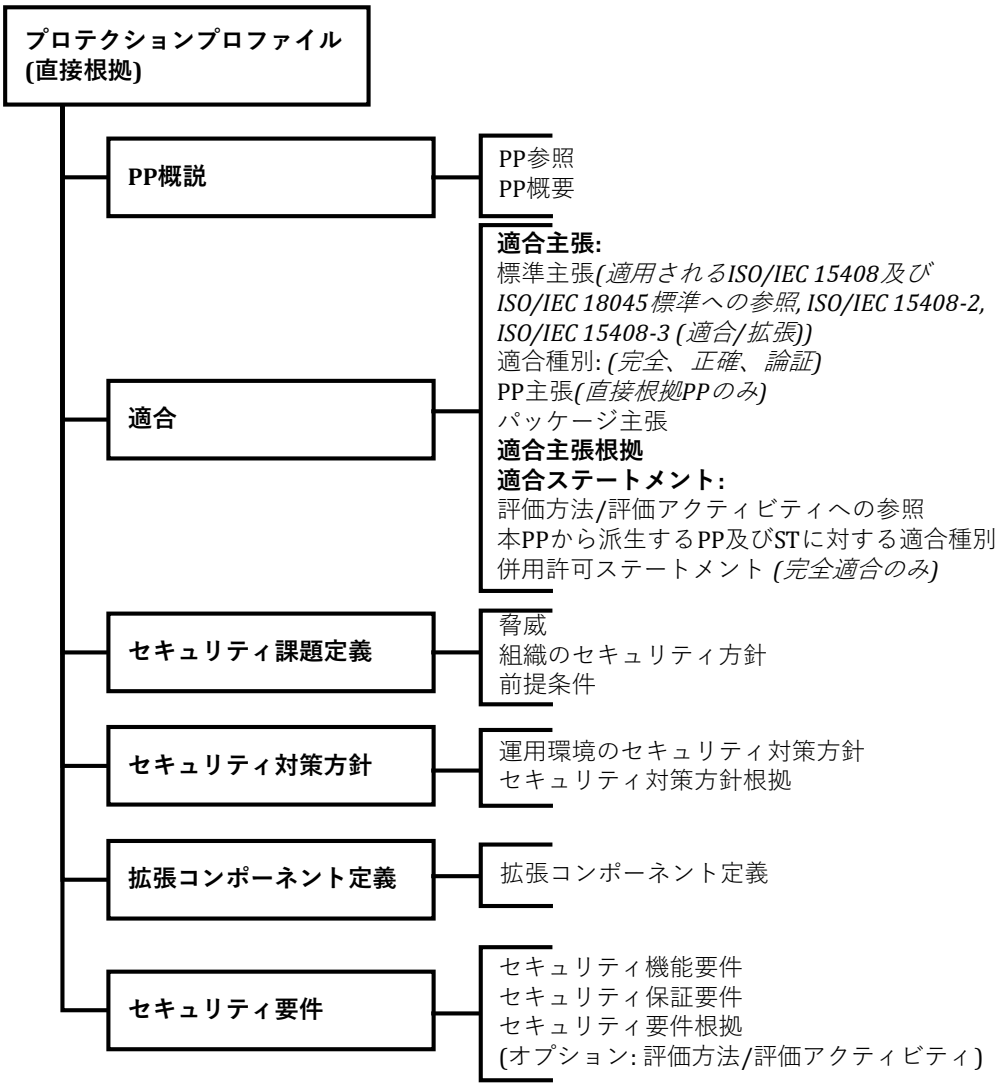
a) PP参照及びTOE概要から構成されるPP概説。

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)。

直接根拠PPの内容を図B.2に示す。



図B.2 — 直接根拠PPの内容

B.5.2 直接根拠PPの適合主張(APE_CCL)

直接根拠PPは、他の直接根拠PPへの適合のみを主張しなければならない。

通常のPPは、直接根拠PPへの適合を主張することができる。

B.5.3 直接根拠PPのセキュリティ対策方針(APE_OBJ)

直接根拠PPは、TOEのセキュリティ対策方針を含むPPと比較すると、セキュリティ対策方針に関して次のような違いがある。

— TOEのセキュリティ対策方針が含まれていない。ただし、運用環境のセキュリティ対策方針は依然として記述しなければならない。

— PPにはTOEのセキュリティ対策方針がないため、運用環境のセキュリティ対策方針についてのみ、セキュリティ対策方針根拠が含まれる。

— 直接根拠PPのセキュリティ要件(APE_REQ)

SFR及び運用環境のセキュリティ対策方針をSPDエレメントに直接マッピングするセキュリティ要件根拠が含まれる。このセキュリティ要件根拠は、SPDの節の各脅威、OSP及び前提条件の直下に配置することが推奨される。通常のPPと同様に、セキュリティ要件根拠は、満たされていないSFRの依存性を正当化する必要もあり、この部分は通常SFRの定義の後に配置する。

B.6 PPのオプションの内容

PPは、CEMから派生した評価方法/評価アクティビティを含むことができる。PPに関連する評価方法/評価アクティビティは、PPの適合ステートメントの節で参照される。10.3を参照のこと。

PP作成者が評価方法/評価アクティビティをPPに含めることを決定した場合、それらは(別の)サポート文書に記述するか、関連するセキュリティ要件とともにPPのセキュリティ要件の節に記述することができる。

附属書C
(規定)

PP モジュール及び PP 構成の仕様

C.1 本附属書の目的及び構造

この附属書の目的は、PPモジュール及びPP構成の構造及び期待される内容をまとめることである。

注：この附属書は、PP構成の評価要件は定義していない。PP構成の評価基準は、CCパート3に示されているACEクラスにある。

C.2 PPモジュールの仕様

C.2.1 PPモジュールの使用

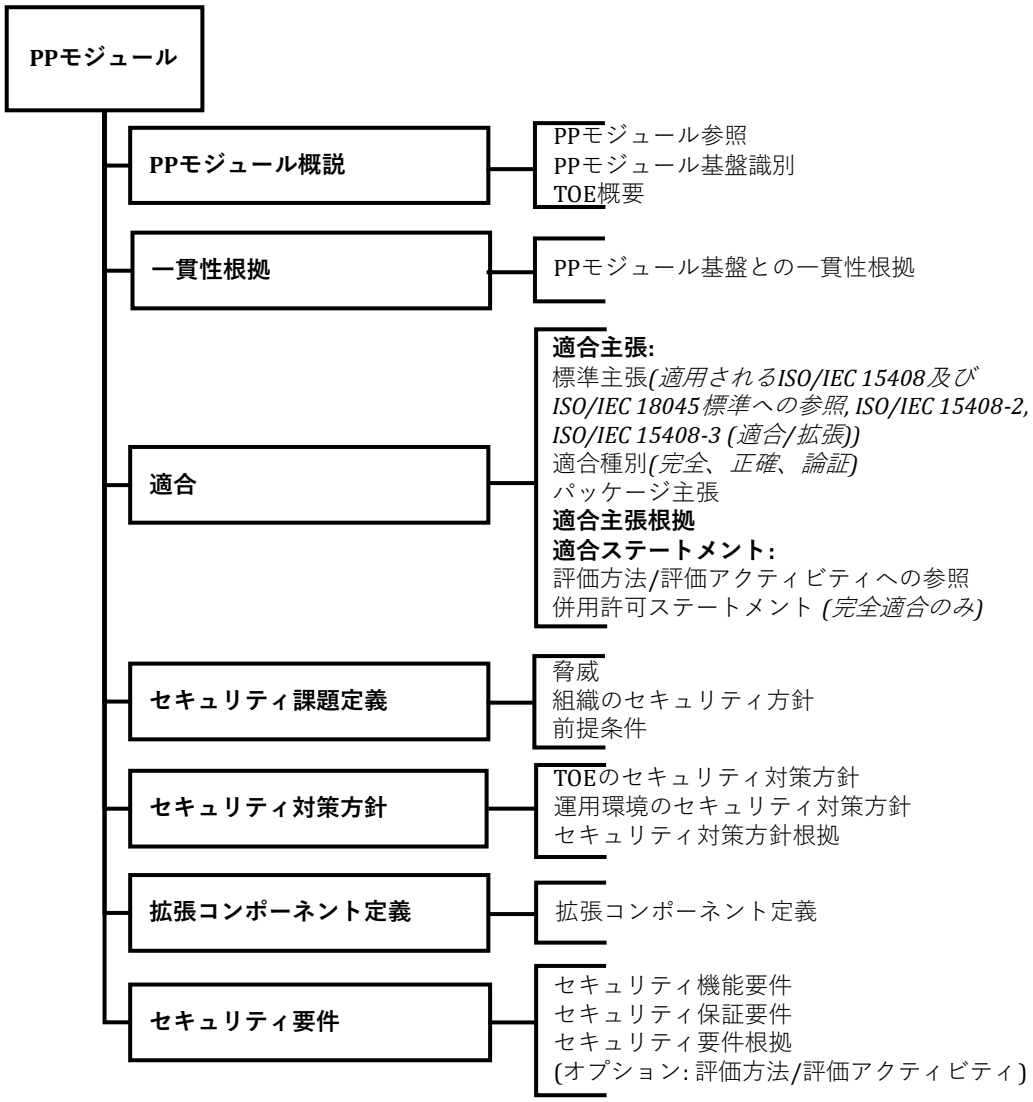
PPモジュールは、利用者や開発者のグループ、規制機関、行政、又は特定の消費者ニーズを満たすその他全てのエンティティのセキュリティステートメントである。PPモジュールは、1つ以上のPP、及びオプションとして他のPPモジュールを補完し、そのPPモジュールの「PPモジュール基盤」と呼ばれ、消費者がこのステートメントを参照できるようにし、それに対する評価及び適合する評価済みのTOEの比較を容易にする。PPモジュールは、このPPモジュール基盤を含むPP構成内でしか使用することができない。

注：基本PPは、PPモジュールに要求されるPPである。基本PPモジュールは、そのPPモジュール基盤とともに、他のPPモジュールに要求されるPPモジュールである。

C.2.2 PPモジュールの必須の内容

C.2.2.1 一般

図C.1にPPモジュールの内容を示す。



図C.1 — PPモジュールの内容

PPモジュールの内容は以下に要約され、その詳細については、C.2.2.2からC.2.3で説明されている。PPモジュールには以下が含まれる。

— *概説*。PPモジュールを識別し、それが基づくPPモジュール基盤を識別し、PPモジュール基盤の基礎となる記述を満たす環境内のTOEの記述を提供する。

— *一貫性根拠*。PPモジュールとそのPPモジュール基盤間の対応を述べる。

— *適合主張*。CCの版、適合ステートメント、及び完全適合の場合は併用許可ステートメント。

— *セキュリティ課題定義*。脅威、前提条件、及びOSPを含む。

— *セキュリティ対策方針の節*。TOE及びその運用環境の対策方針の観点でセキュリティ課題に解決方法を提示する。

— オプションの*拡張機能コンポーネント定義*。CCパート2に含まれていない新しい機能コンポーネントが導入される。

— *セキュリティ機能要件*の節。TOEセキュリティ対策方針の標準化されたステートメントを含む。

— *セキュリティ保証要件*セクション。SARが基本PPから引き継がれる完全適合を除く。

C.2.2.2 PPモジュール概説

C.2.2.2.1 PPモジュール参照

PPモジュール概説では、PPモジュールを識別できるような明確で曖昧でない参照を提供する。一般的な参照は、PPモジュールのタイトル、文書のバージョン、スポンサー、及び公表日で構成される。

PPモジュール参照は、PPカタログでその文書のインデックスとして使用することができる。

C.2.2.2.2 PPモジュール基盤の識別

PPモジュール概説は、そのPPモジュール基盤を識別する。識別は、参照リストで構成される。

例えばPPモジュール基盤{B_1, ..., B_n}と一緒に使うことを要件とするPPモジュールは、次のような形の識別リストを提供する。

$$B_1 \ldots AND \ldots B_n、ただし n \geqq 1$$

このPP/PPモジュールのセットは閉じていなければならない、すなわち、任意のPPモジュールBiに対して、それ自身のPPモジュール基盤はセット{B_1, ..., B_n}に属していなければならない。

注1：これは、セット{B_1, ..., B_n}がいかなるPPモジュールも含まない、又は基本PPのみを必要とし基本PPモジュールを必要としないPPモジュールが少なくとも1つ含まれることを意味する。

PPモジュールは、PPモジュール基盤の代替セット、例えば{S_1, ..., S_k}を許可することもできる。この場合、識別リストには次のように記載される。

$$S_1 \ldots OR \ldots S_k、ただし k \geqq 1$$

そして、PPモジュール基盤の代替セットの識別の展開形は、次のようになる。

$$(B_1 \ldots AND \ldots B_{ni}) \ldots OR \ldots (B_1 \ldots AND \ldots B_{nk})、ただし k \geqq 1、ni \geqq 1$$

注2：ORリストを記述するPPモジュールは、リストの要素Siと同数のPPモジュールと同等である。すなわち、ORリストは、異なる用途のために同様のPPモジュールを定義し維持することを避けるためのショートカットである。

C.2.2.2.3 TOE概要

PPモジュールのTOE概要は、PPモジュールとそのPPモジュール基盤間の一貫性が保証されていれば、PPモジュール基盤のTOE概要を補完することができる。

— PPモジュールのTOE種別は、PPモジュール基盤のTOE種別と同じか、又はPPモジュールの目的を満たすために必要な特定をすることができる。

— PPモジュールは、PPモジュール基盤に記載されたものに加えて、さらなる使用法及び主要なセキュリティ機能を導入することができる。

— PPモジュールは、PPモジュール基盤のステートメントに準拠した、特定の、TOE以外のハードウェア、ソフトウェア、及び/又はファームウェアを指定することができる。

PPモジュールにおいて、PPモジュール基盤のTOE概要を補足する可能性は、PP又はSTにおける、適合を主張する他のPPのTOE概要の補足と同じ意味を持つ。

PPモジュールにおけるTOE概要のステートメントは、そのPPモジュール基盤と同一である場合、すなわち、追加がない場合には、参照によって与えられることがある。PPモジュールは、PPモジュール基盤の別のセットと同数の特定のTOE概要を提供することもある。

C.2.2.3 一貫性根拠

PPモジュールは、そのPPモジュール基盤に関して一貫性根拠を提供しなければならない。

PPモジュールが別のPPモジュール基盤を指定する場合、PPモジュールは別のPPモジュール基盤の数と同数の一貫性根拠を提供しなければならない。

各PPモジュール基盤の一貫性分析は、TOE種別、SPD、対策方針、及びSFRに対して実施されなければならない。最終的には、TOEがPPモジュール基盤及びPPモジュールに記載されたTOE種別の記述を満たし、PPモジュール及びそのPPモジュール基盤に指定されたSFRを全て満たすことができることを実証することを目的とする。一貫性根拠は、PPモジュール及びそのPPモジュール基盤に定義されたSPD、対策方針、SFRの組み合わせが矛盾をもたらさないことを実証しなければならない。

一貫性根拠は、テキストによる正当化と共に、SPD/対策方針/SFR間の対応表を用いることができる。

C.2.2.4 保証根拠

保証根拠は、基本PPから引き継がれる可能性のある適用されるSARのセットとPPモジュールで定義されるSPDとの一貫性、すなわち保証要件と脅威モデルが矛盾していないことを実証しなければならない。

PPモジュールが基本PPからSARのセットを引き継がない場合、保証根拠は、PPモジュール及びそのPPモジュール基盤に共通する資産に関して、PPモジュール及びそのPPモジュール基盤の保証要件が矛盾していないことを実証しなければならない。

C.2.2.5 適合主張及び適合ステートメント

C.2.2.5.1 一般

PPモジュールのこの節は、全てのPPモジュールに含まれなければならず、以下に対してPPモジュールがどのように適合するかを記述する。

— CCパート2、CCパート3、それらの版、及び拡張セキュリティ要件の使用。

— 機能パッケージ及び保証パッケージ。

PPモジュールは、いかなるPP、他のPPモジュール、又はPP構成への適合も主張してはならない。

PPモジュールの適合ステートメントは、要求される適合種別を識別する。完全適合は基本PPから引き継がれ、全てのPPモジュール基盤が同様に完全適合であることが要求される。PPモジュール適合ステートメントは、PPモジュールとともに使用されることが要求される評価方法/評価アクティビティを識別することもできる。

CEMから派生した評価方法/評価アクティビティがPPモジュールを評価するために使用される場合、関連するセキュリティ要件の節に次の形式のステートメントを含めることによって、これらを識別しなければならない。

「*このPPモジュールは、<参照>で定義された評価方法/評価アクティビティを使用することを要求する。*」

ここで、*<参照>*は、PPモジュールに適用される評価方法及び評価アクティビティの所在の識別に置き換えられる。この参照は、パッケージを含む文書に対してでも、1つ以上の別の文書に対してでもよい。

注：評価方法/評価アクティビティは、PPモジュール自体に含まれるか、それらを記述した1つ以上の別個の文書への参照によって含まれるかのいずれかである。

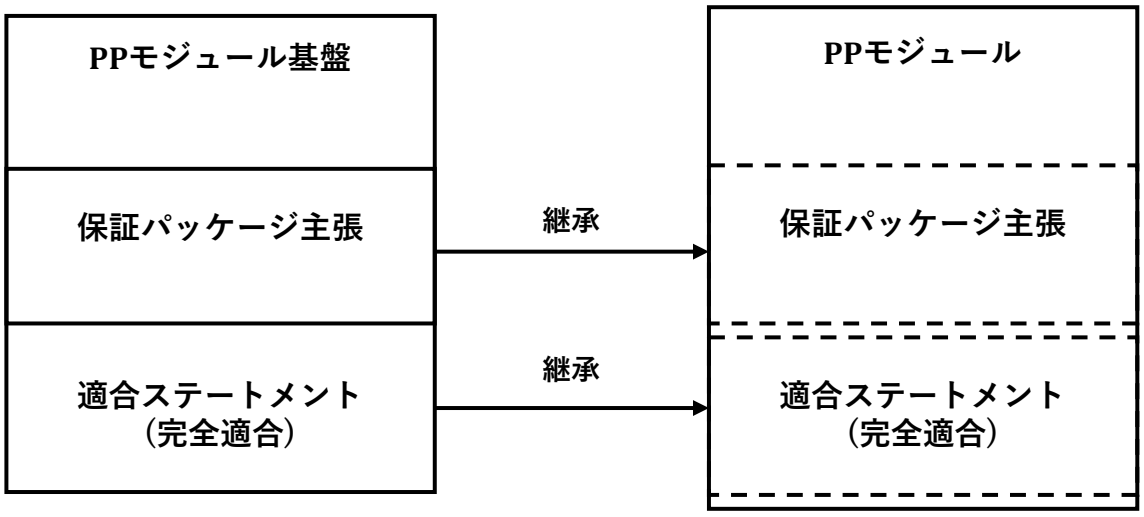
C.2.2.5.2 完全適合

完全適合の場合、併用許可ステートメントには、PPモジュールのPPモジュール基盤のセット以外のPP及びPPモジュールの識別も含まれ、それらは、そのPPモジュールとともにPP構成で使用することが許可されている。

PP構成において、完全適合を要求する全てのコンポーネントは、それの適合ステートメントにおいて、同様に完全適合を要求しなければならない。

注1：これは、PPモジュールの作成者が、PPモジュールで指定された要件と組み合わせて指定できる他の要件を管理するという完全適合の概念を維持する。

図C.2は、完全適合の単一保証の場合、適合主張と適合ステートメントがどのように引き継がれるかを示したものである。



図C.2 — 完全適合の場合の引き継がれた適合主張及び適合ステートメント

注2：完全適合が使用される場合、EM/EAをPP構成で定義することはできない(すなわち、使用されるEM/EAは、PP構成で使用されるPP及びPPモジュールでのみ識別される)。

C.2.2.6 セキュリティ課題定義(SPD)

この節では、PPモジュールによって対処されるセキュリティ課題を定義する。この節は、全ての種別のSPDエレメント、つまり前提条件、脅威、OSPを含むことができる。

PPモジュールは、PPモジュール基盤のセキュリティ課題、ならびにPPモジュールの*概説*で提供されたTOEの定義及びその環境と関連して、セキュリティ課題を定義する。

各SPDエレメントは、PPモジュール基盤に由来するか、全く新しいものであるかのいずれかである。「E」をPPモジュールのSPDエレメントとすると、以下のケースの１つが当てはまる。

— 「E」は識別されたPPモジュール基盤に属する。SPDエレメントへの参照で十分である。

— 「E」は、PPモジュール基盤のSPDエレメントを詳細化したものである。

— 「E」は、TOE又はその環境の追加機能に関連する新しいSPDエレメントである。

注1：詳細化されたSPDエレメントは、SPDの意味に影響を与えることなく、新しいSPDエレメントとして取り扱うことができる。

注2：STができるのと同じ方法で、PPモジュール基盤の範囲外の側面を対象とすることを条件として、PPモジュールは前提条件を導入することが可能である。

C.2.2.7 セキュリティ対策方針

この節では、TOE及びTOEの運用環境のセキュリティ対策方針を定義する。

PPモジュールは、PPモジュール基盤のセキュリティ対策方針との関連で、新しいセキュリティ対策方針を定義する。

各セキュリティ対策方針は、PPモジュール基盤に由来するか、全く新しいものであるかのいずれかである。「O」をPPモジュールの対策方針とすると、以下のケースの1つが当てはまる:

— 「O」はPPモジュール基盤に属する。セキュリティ対策方針への参照で十分である。

— 「O」は、PPモジュール基盤のセキュリティ対策方針を詳細化したものである。

— 「O」は、PPモジュールによって導入された新しい対策方針である。

注：詳細化された対策方針は、対策方針のセット全体の意味に影響を与えることなく、新しい対策方針として取り扱うことができる。

PPモジュールは、PPモジュール基盤の範囲外の側面に対処する場合にのみ、TOEの運用環境の新しい対策方針を導入できる。

PPモジュールがTOE種別を詳細化する場合、PPモジュール基盤の環境のセキュリティ対策方針の一部が、PPモジュールのTOEのセキュリティ対策方針となることがある。

この節は、PPモジュールのSPDとセキュリティ対策方針との間の根拠も定義する。これは、7.2.5に規定されるように、PPモジュールのSPDをそのセキュリティ対策方針に追跡するマッピングと、その追跡が有効であることを実証する正当化からなる。さらに、マッピングは、全てのSPDエレメントがカバーされていることだけでなく、無用なセキュリティ対策方針が存在しないことも示さなければならない。

PPモジュールのセキュリティ対策方針の中には、PPモジュール自体のSPDに属さないPPモジュール基盤のSPDエレメントもカバーしている場合がある。この情報は要求されないが、適用上の注釈において提供することができる。

C.2.2.8 拡張機能コンポーネント定義

本節は、B.3.6で規定したPP及びST拡張コンポーネント節と同一である。

C.2.2.9 セキュリティ要件

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を標準化された言語に書き換えたもの。

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。

これらの2つのグループについては、7.3.で説明する。

C.2.2.9.1 セキュリティ機能要件(SFR)

この節では、PPモジュールのTOEセキュリティ対策方針のセット及びPPモジュール基盤のSFRと関連して、TOEのSFRを定義する。

各セキュリティ機能要件は、PPモジュール基盤に由来するか、全く新しいものであるかのいずれかである。「R」をPPモジュールのセキュリティ機能要件とすると、以下のケースの1つが当てはまる。

— 「R」はPPモジュール基盤に属する。要件への参照で十分である。

— 「R」は、PPモジュール基盤のSFRを詳細化したものである。

— 「R」は、PPモジュールによって導入された新しい要件である。

注：詳細化された要件は、要件のセット全体の意味に影響を与えることなく、新しい要件として取り扱うことができる。

この節は、SFRとPPモジュールのTOEセキュリティ対策方針との間の根拠も定義する。これは、7.2.5に規定されているように、SFRをPPモジュールのTOE対策方針に追跡するマッピングと、その追跡が有効であることを実証する正当化からなる。さらに、マッピングは、TOEの全ての対策方針がカバーされていることだけでなく、無用なセキュリティ機能要件が存在しないことも示さなければならない。

PPモジュールのSFRの中には、PPモジュール自体には属さないPPモジュール基盤のTOEセキュリティ対策方針もカバーしている場合がある。この情報は要求されないが、適用上の注釈において提供することができる。

PPモジュールは、B.3.7でPPに対して以前に規定したように、オプションのSFR(及び必要なSPDエレメント)を定義して含めることができる。

C.2.2.9.2　セキュリティ保証要件(SAR)

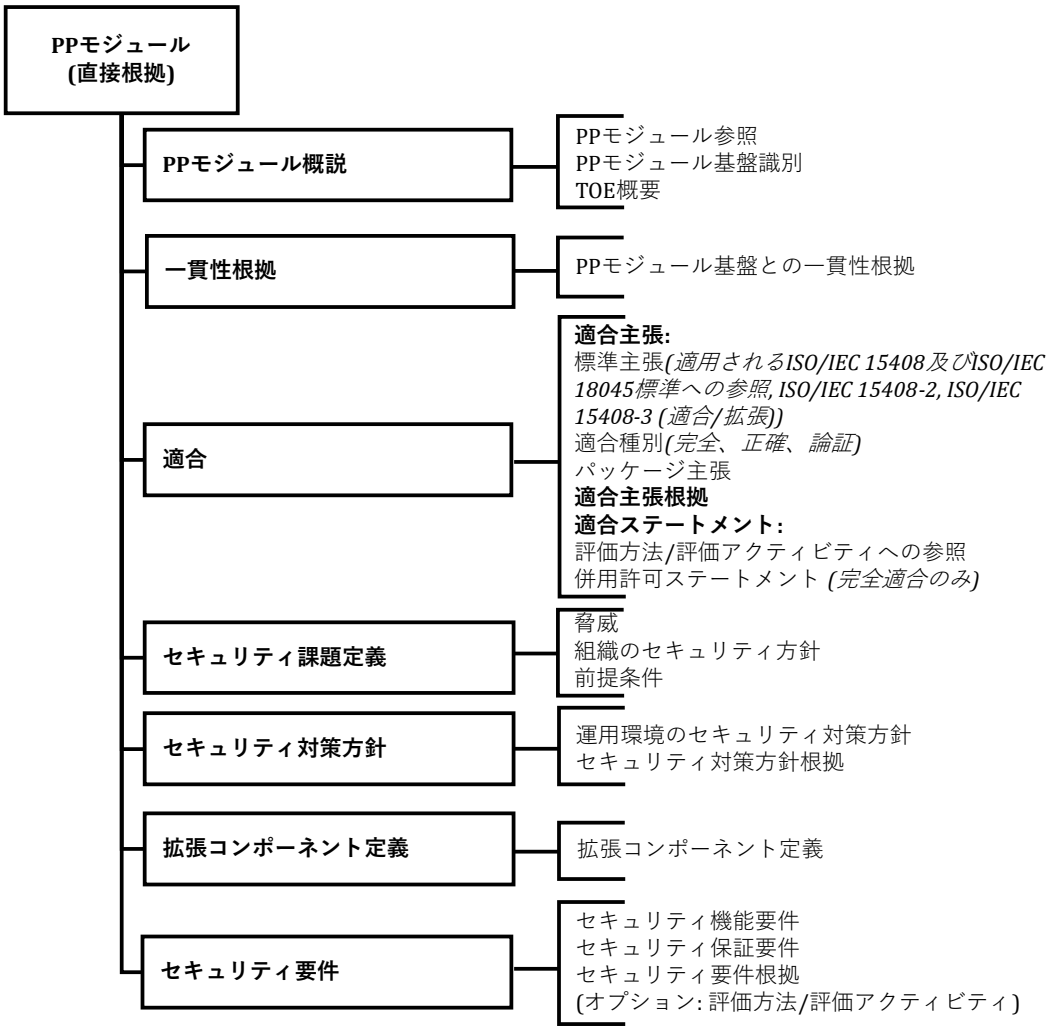
PPモジュールは、このPPモジュールを含むPP構成で使用されるSARのセットを定義する。C.2.2.4に記述された保証の根拠はPPモジュール基盤に関するSARのこのセットの一貫性を保証する。

単一保証を使用するPPモジュールは、そのPPモジュール基盤から、事前に定義されたEALのような保証パッケージを含むSARのセットを引き継ぐ。異なるSARを持つPPモジュール基盤のANDエレメントの課題は解決されなければならず、それら全てのPPに対するPP適合が課題を扱うのと同じ方法で取り扱われる。

C.2.3 直接根拠PPモジュール

PPモジュールは、直接根拠アプローチも使用するPPモジュール基盤のコンポーネントと一緒に使用することを意図して作成することができる。この場合、TOEのセキュリティ対策方針はPPモジュールに含まれず、TOEの運用環境のセキュリティ対策方針が含まれることがある。

直接根拠PPモジュールの内容を図C.3に示す。



図C.3 — 直接根拠PPモジュールの内容

C.2.4 PPモジュール基盤からSPDエレメントを含めるためのガイダンス

PPモジュールに含まれる情報量を制限するために、PPモジュール作成者は以下の規則を適用する。

E、O、Rはそれぞれ、SPD、セキュリティ対策方針、及びPP/PPモジュールQのSFRに属し、RはOに、OはEにマッピングされるものとする。

MをPPモジュールとし、QをMのPPモジュール基盤に属するものとする。

Mは以下の条件を満たさなければならない。E、O、R、及びそれらの間のマッピングがMに属するべきなのは、これらのエレメントの少なくとも1つがMの新しいエレメントに関連付けられる場合のみである。すなわち、以下のいずれかである。

— Mに新しいSPDエレメントE'があり、OがE'にマッピングされている。あるいは

— Mに新しい対策方針O'があり、O'がEにマッピングされているか、又はRがO'にマッピングされている。あるいは

— Mに新しい要件R'があり、R'がOにマッピングされている。

PPモジュールは、新しいニーズを満たすために必要でない限り、PPモジュール基盤の部分を含むことはない。ここでは、詳細化された要素が新しいとみなされる。

C.2.5 PPモジュールのオプションの内容

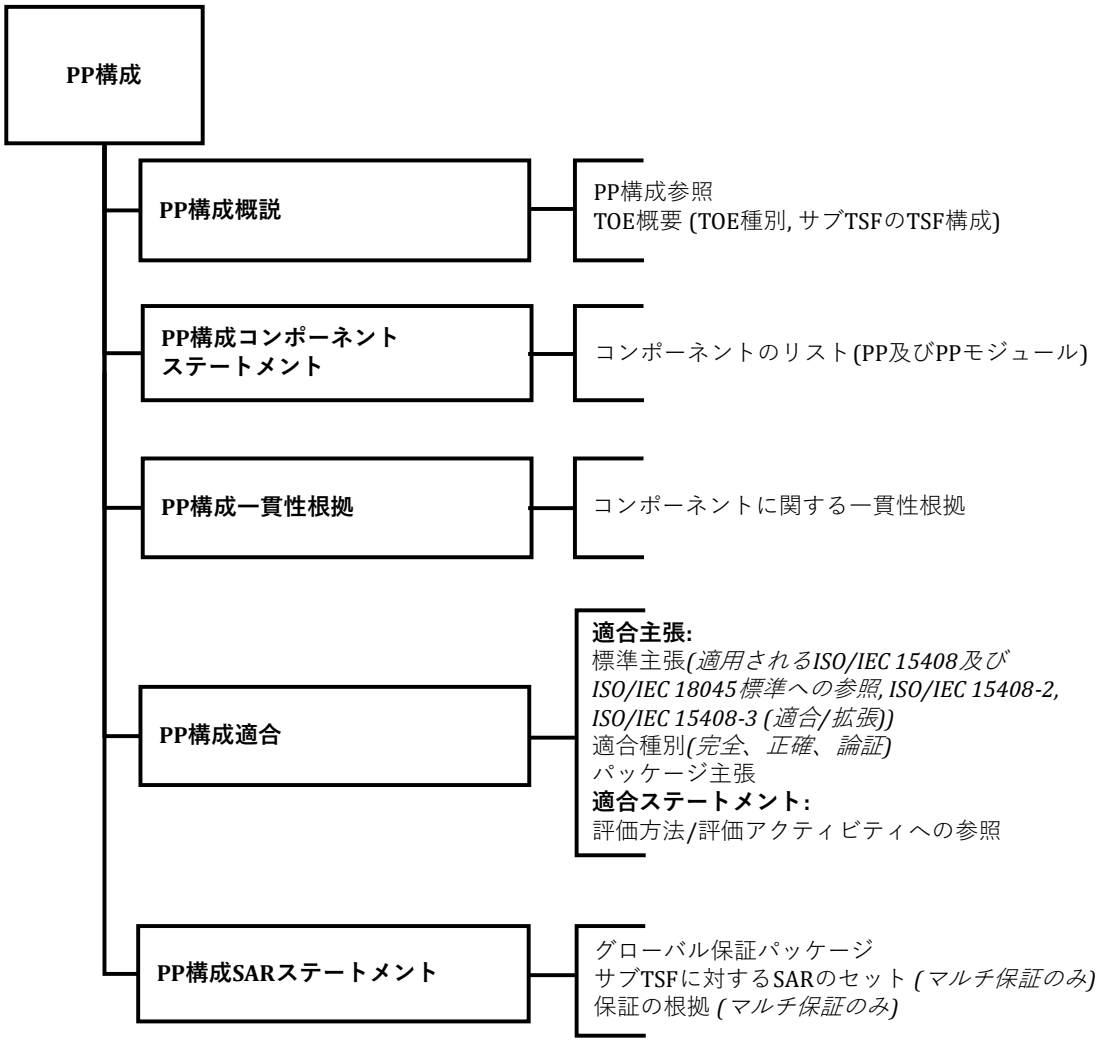
PPモジュールは、オプションとして、CEMから派生した評価方法/評価アクティビティを含むことができる。PPモジュールに関連する評価方法/評価アクティビティは、適合ステートメントの節で識別される。11.2.3.3を参照のこと。

もし、PPモジュール作成者が評価方法及び/又はアクティビティをPPモジュールに含めることを決定した場合、それらは関連するセキュリティ要件とともにセキュリティ要件の節で提供されるか、他の適切な節や外部文書で提供される。適用上の注釈は、適切な場合、PPモジュールの特定の要件と関連付けられるべきである。

C.3 PP構成の規定

C.3.1 一般

PP構成の内容は以下の図C.4に要約され、附属書C.3.2からC.3.7で詳細に説明する。



図C.4 — PP構成の内容

PP構成には、以下が含まれる。

— PP構成を一意に識別する参照。

— PP構成を成すPP及びPPモジュールを識別するコンポーネントステートメント。コンポーネントの閉じたセットを定義するために必要な全てのPPモジュール基盤を含む。

— 適合主張。以下を指定する。CCの関連パートの版、CCパート2及びCCパート3に対する主張、保証パッケージに対する主張、及びこのPP構成に対するSTの適合が、完全、正確、論証、又はコンポーネントのセットから引き継がれた正確及び論証の組み合わせかどうかを定義する適合ステートメント、及び適用できる評価方法/評価アクティビティ。

— TOE種別の記述。

— PP構成コンポーネントによって定義されたサブTSFの観点でのTSFの構成の記述。

— SARステートメント。TOE全体に適用されるSARのセットを指定する。マルチ保証の場合、SARステートメントには、PP構成コンポーネントで定義されたサブTSFに適用されるSARのセットが含まれる。また、SARステートメントには、PP構成とそのコンポーネント間の一貫性を保証するための保証根拠が含まれる。

注：保証パッケージは、CCパート5から抽出されたEALであってもよい。

C.3.2 PP 構成参照

PP構成参照は、明確で曖昧さのない識別情報を提供し、通常はタイトル、バージョン番号、作成者、及び公表日で構成される。

PP構成参照は、カタログで文書のインデックス化するのに使用することができる。

C.3.3 コンポーネントステートメント

PP構成コンポーネントステートメントは、PP構成を構成するPPとPPモジュールを識別する。

PP構成コンポーネントステートメントには、指定されたPPモジュールが必要とするPPモジュール基盤を含めなければならない。PPモジュールが別のPPモジュール基盤を指定する場合、これらのセットのうちの1つのみを、PP構成において参照しなければならない。

注：PP構成は、それのコンポーネントの1つによって主張されるか否かにかかわらず、機能パッケージへの適合を直接主張することはない。

マルチ保証の場合、PP構成のコンポーネントステートメントは、PP構成のコンポーネントによって定義されたサブTSFの観点からTSFの構成を提供しなければならない。

C.3.4 TOE概要

PP構成のTOE概要は、以下を提供しなければならない。

— PP構成への適合を主張するSTが使用するPP構成のTOE種別。

— TOEの期待される使用法及び主要なセキュリティ機能の特徴。

— 利用可能なTOE以外のハードウェア、ソフトウェア及び/又はファームウェア(該当する場合)。

C.3.5 一貫性根拠

PP構成は、コンポーネントの組み合わせの互換性を保証するために、一貫性根拠を提供しなければならない。

一貫性根拠は、TOE概要がPP構成コンポーネントのTOE概要と一貫しており、これらのコンポーネントで定義されたSPD、対策方針、及びSFRの合わせたものが矛盾を招かないことを実証しなければならない。

一貫性根拠は、テキストによる正当化と共に、SPD/対策方針/SFR間の対応表を用いることができる。

C.3.6 適合主張と適合ステートメント

C.3.6.1 CC 適合主張

PP構成に適用されるCCの関連パートの版。

C.3.6.2 適合種別

STによるこのPP構成への適合は、完全、正確、又は論証のいずれか、もしくはPP構成が正確及び論証の両方の適合種別のコンポーネントを含む場合には、正確及び論証の組み合わせでなければならない。

PP構成への適合を主張するSTは、PP構成の適合ステートメントで要求される適合種別に適合しなければならない。

C.3.6.3 保証パッケージ適合主張

適合主張は、PP構成の保証パッケージへの適合を記述する保証パッケージ適合主張を含むことができる。PP構成では、複数のパッケージを主張することができる。

C.3.6.4 評価方法/評価アクティビティ参照ステートメント

PP構成の評価方法/評価アクティビティの適合ステートメントは、それとともに使用されることが要求される評価方法/評価アクティビティを識別することもできる。

正確適合又は論証適合の種別である(完全適合の種別ではない)PP構成は、PP構成のコンポーネントで参照される評価方法/評価アクティビティに加えて、評価方法/評価アクティビティを指定することができる。

C.3.6.5 完全適合のための追加要件

PP構成が、その適合ステートメントにおいて、その適合種別として完全適合を指定する場合、次による。

— PP構成中のいずれかのコンポーネントが完全適合を要求する場合、PP構成中の他の全てのコンポーネントも完全適合を要求しなければならず、PP構成の適合ステートメントは、完全適合を指定しなければならない。

— PP構成中の全てのコンポーネントは、適合主張の節のそれぞれの併用許可ステートメントにおいて、PP構成内の全ての他のコンポーネントがPP構成内で一緒に使用されることを許可しなければならない。

注：PPモジュールは、暗黙的に許可されるため、それ自身のPPモジュール基盤を併用許可ステートメントに含める必要はない。図C.5にその例を示す。

— PP構成に適用される評価方法/評価アクティビティは、PP構成のコンポーネントに含まれるもののみでなければならない。評価方法/評価アクティビティの追加や、PP構成コンポーネントの評価方法/評価アクティビティの変更は許可されない。

図C.5 — PP構成及び完全適合

例：PP構成は、その適合ステートメントにおいて完全適合を要求する。なぜなら、完全適合は両方の基本PPで要求され、したがって、PPモジュールによって引き継がれるからである。PPモジュールXとYは、ともに同一の基本PPセットを持っている。PP B及びPP Cは、いずれも完全適合を要求する。これが「完全適合」の適合ステートメントをもつ評価可能なPP構成であるためには、次の記述(図に示す)が真でなければならない。

a) PPモジュールは基本PPから適合ステートメントを引き継いでいるので、その適合ステートメントは完全適合である。

b) PPモジュールが完全適合を要求しているので、PP構成は完全適合を要求しなければならない。

c) PP Bは、PP C、PPモジュールX及びPPモジュールYとの使用を許可することを、その適合ステートメントに指定しなければならない。

d) PP Cは、PP B、PPモジュールX及びPPモジュールYとの使用を許可することを、その適合ステートメントに指定しなければならない。

e) PPモジュールXは、PPモジュールYとの使用を許可することを、その適合ステートメントに指定しなければならない。

f) PPモジュールYは、PPモジュールXとの使用を許可することを、その適合ステートメントに指定しなければならない。

C.3.7 SARステートメント

PP構成SARステートメントは、このPP構成への適合を主張するSTによって特定されたTOEの評価に適用されるSARのセットを指定する。マルチ保証の場合、PP構成コンポーネントが異なるSARのセットを持つときには、PP構成は、これらのコンポーネントによって定義されるサブTSFの各々に適用されるSARのセットを定義しなければならない。

TOE全体に適用されるSARのセットは、グローバル保証パッケージと呼ばれる。

論証又は正確の種別の場合、グローバル保証パッケージは、PP構成の各コンポーネントに適用されるSARの共通サブセットのスーパーセットである。

完全適合の種別の場合、グローバル保証パッケージは、PP構成のコンポーネントのためのSARの最小共通セットであり、追加は許可されない。

PP構成では、サブTSFのそれぞれに適用されるSARのセットは、対応するPP構成コンポーネントで定義されたSARのセットと同一か、このセットの追加したものでなければならない。

例：SARのセットの例は、CCパート5で事前に定義されたEAL保証パッケージである。

PP構成は、特に共通資産に関して、適用可能なSARのセットとそのコンポーネントで定義されたものとの一貫性を実証するための保証根拠を提供しなければならない。さらに、保証根拠は、SARがPP構成レベルで追加された場合、又は追加のEM/EAがPP構成レベルで指定された場合のPP構成コンポーネントのEM/EAの処置について説明する。

注：PP構成の保証根拠は、PPモジュールで与えられた分析をPP構成の全コンポーネントに拡張する必要がある。通常、これはPP構成コンポーネントのSPDエレメントを展開し、各資産に適用されるSARのセットを分析することで行われる。

附属書D
(規定)

セキュリティターゲット(ST)及び直接根拠 ST の仕様

D.1 本附属書の目的及び構造

この附属書の目的は、STの構成と期待される内容を要約することである。

PPとSTは非常に重複しているため、本附属書ではPPとSTの相違点に焦点を置く。STとPP間で同一の事項については、附属書Bで記述する。

注：この附属書は、STの評価要件は定義していない。STの評価基準は、CCパート3のASEクラスに記載されている。

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の使用方法*

これはD.2.に要約されている。この節では、STはどのように使用されるべきかと、STを使用して回答できるいくつかの質問を記述する。

b) *STが含まなければならない内容*

これはD.3.で詳述される。ここでは、STの必須の内容と各内容間の相互関係を記述し、例を示す。

c) *標準への適合の主張*

D.5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記述する。

d) *直接根拠ST*

直接根拠STは、SFR及び場合によっては運用環境のセキュリティ対策方針がSPDエレメントに直接マッピングされたSTである。D.4は直接根拠STに適用される。

D.2 STの使用

D.2.1 STの使用方法

一般的なSTは、次の2つの役割を果たす:

a) 評価前と評価中に、STは「何が評価されるのか」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。D.3.2及びD.3.5では、この役割においてSTの使用法を説明する。

b) 評価後に、STは「何が評価されたのか」を特定する。この役割において、STは、TOEの開発者又は再販業者と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。D.2.3では、この役割においてSTがどのように使用されるかを記述する。

D.2.2 STを使用しない方法

多くの役割の中で、STが果たすべきでない役割の1つは以下のものである。

— *完全な仕様*

STは、完全な仕様ではなく、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の一部となるべきではない。これは、一般に、STは完全な仕様の一部にはなり得るが、完全な仕様そのものにはなり得ないことを意味する。

D.2.3 STを使用して回答できる質問

評価後に、STは「何が評価されたのか」を特定する。この役割において、STは、TOEの開発者又は再販業者と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概要で対処する。

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概要で対処する。

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が運用環境に課す全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対処する。

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概要で対処する。

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記述で対処する。

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要約仕様で対処する。

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要約仕様で対処する。

h) *TOEは当方の政府/組織によって定義される課題に対処するか。*

政府又は組織がこの解決策を定義するためにパッケージ及び/又はPP及び/又はPP構成を定義している場合、この回答はSTが適合する全てのパッケージ、PP及びPP構成をリストする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処するか(専門家向け)。*

TOEが対抗する脅威は何か。TOEはどのようなOSPを実施するのか。TOEは運用環境についてどのような前提条件を設けているのか。これらの質問はSPDで対処する。

j) *どの程度TOEを信頼することができるか。*

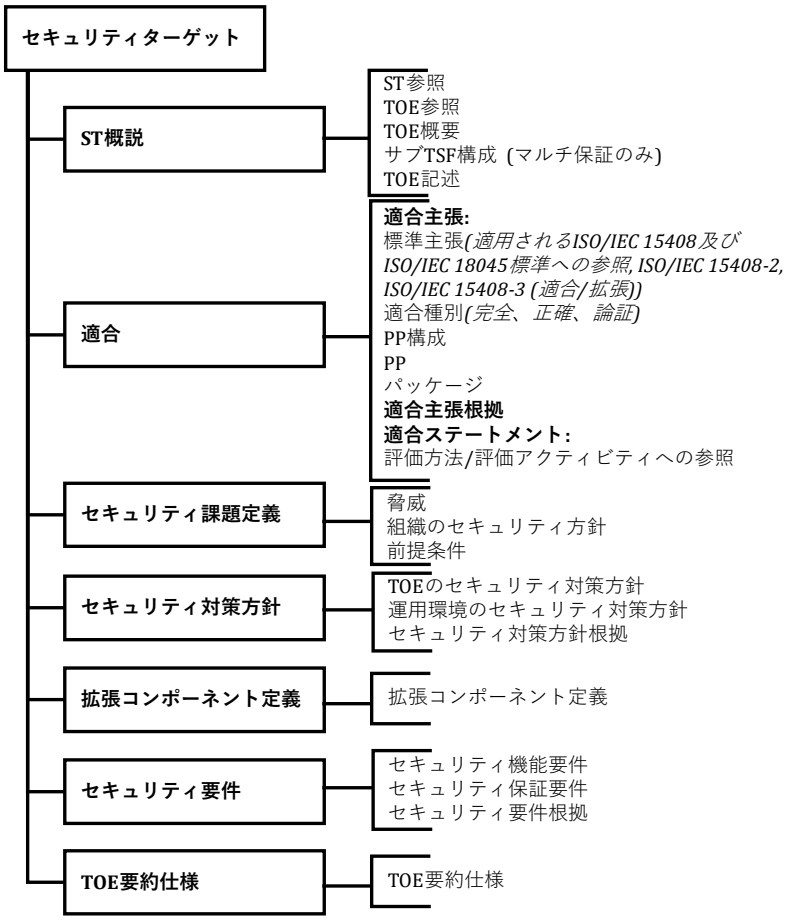
この回答は、セキュリティ要件の節のSARにある。SARによって、TOEを評価するために使用された保証要件、つまりTOEの正確性に関して評価が提供する信頼度が提供される。

D.3 STの必須の内容

D.3.1 一般

STには、2つの種別がある。第一に、D.3.3からD.3.7.2に記述された完全な内容を含むSTである「通常の」STである。第二に、場合によっては、ST作成者はTOEのセキュリティ対策方針を記載しない直接根拠STを使用することがある。直接根拠ST及びそれらが使用される理由及び状況については、D.4で詳細に記述する。この附属書の他の全ての部分は、完全な内容のSTを前提としている。

図D.1は、CCパート3に記載されるSTの内容を示す。



図D.1 — STの内容

図D.1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、D.3.3からD.3.7.2までででより詳細に説明する。STは以下を含む。

a) *ST概説*。抽象レベルの異なるTOEの3つの叙述的記述を含む。

b) *適合主張*。CCパート2及びCCパート3の関連する版へのSTの適合を示す。STがいずれかのPP、PP構成及び/又はパッケージへの適合を主張しているかどうかを示し、主張している場合には、特定のPP、PP構成及び/又はパッケージ、評価方法/評価アクティビティ及び主張する適合種別を識別する。

c) *セキュリティ課題定義*。脅威、OSP、及び前提条件を示す。

d) *セキュリティ対策方針*。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。

e) *拡張コンポーネント定義*(任意)。新しいコンポーネント(つまりCCパート2又はCCパート3に含まれていない)を定義することができる。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) *セキュリティ要件*。TOEのセキュリティ対策方針から標準化された言語への書き換えを提供する。この標準化された言語は、SFRの形式をとる。また、この節ではSARを定義する。

g) *TOE要約仕様*。TOEでSFRを実装する方法を示す。

D.3.2 ST概説(ASE_INT)

D.3.2.1 一般

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参照及びTOE参照。ST及びSTが参照するTOEの識別資料を提供する。

b) TOE概要。TOEについて簡潔に記述する。

c) TOE記述。TOEについてより詳細に記述する。

D.3.2.2 ST参照及びTOE参照

ST参照及びTOE参照は、ST及びTOEのインデックス化及び参照と、カタログへの掲載を容易にする。

STは、特定のSTを識別する明確なST参照を含む。一般的なST参照は、タイトル、バージョン、スポンサー、及び公表日から構成される。

例1：ST参照の例は、「MauveRAM Database ST、バージョン1.3、MauveCorp仕様チーム、2017年10月11日」である。

STは、STへの適合を主張するTOEを識別するTOE参照も含んでいる。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。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)、その結果この参照に関連する複数のSTが存在する。

例2：TOE参照の例は、「MauveCorp MauveRAM Database v5.12」である。

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。製品の主要な部分又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。

D.3.2.3 TOE概要

D.3.2.3.1 一般

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/製品のカタログに目を通している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。

このため、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記述し、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。

マルチ保証STの場合、TOE概要は、STが適合を主張するPP構成に定義されたサブTSFの観点から、TSFの構成も提供する。

D.3.2.3.2　TOEの使用法及び主要なセキュリティ機能の特徴

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。STのこの節は(潜在的な)TOE消費者のために書かれており、TOE消費者が理解できる言葉を用いて、TOEの使用法と主要なセキュリティ機能の特徴をビジネスの観点から記述している。

例：「MauveCorp MauveRAM Database v5.12は、ネットワーク環境で使用することを目的と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。そ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」。

D.3.2.3.3　TOE種別

TOE概要は、TOEの種別を識別する。例えばファイアウォール、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。

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

TOE種別の識別は、消費者に誤解を与えないようにしなければならない。

例：誤解を招くTOE種別の例には、以下のものがある。

— 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。

  例えば、以下のようなものがある。

  — 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。

  — ほぼ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。

— 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全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。

D.3.2.3.4 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

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/又はファームウェアに依存する。後者の場合、TOE概要は、そのようなTOE以外のハードウェア、ソフトウェア、及び/又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、ソフトウェア及び/又はファームウェアを完全かつ詳細に識別する必要はないが、その識別は、潜在的な消費者がTOEを使用するために必要な主要ハードウェア、ソフトウェア及び/又はファームウェアを判断できるほど完全かつ詳細でなければならない。

例：ハードウェア/ソフトウェア/ファームウェアの識別の例を以下に示す。

— Yaizaオペレーティングシステムのバージョン53.0アップデート6b、c、7又はバージョン54.0を実行し、2.10GHz以上のデュアルコアプロセッサ及び4GB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サーバエディションのバージョン7.0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 12.0グラフィックスカード、2つのクアッドコアプロセッサ及び16GB以上のRAMを搭載した標準64bitサーバ。

— CleverCard SB17067集積回路。

— スマートカードオペレーティングシステムQuickOSのv12.0を実行するCleverCard SB17067集積回路。

— 運輸省長官の事務局で2020年12月に設置されたLAN。

D.3.2.3.5 マルチ保証の場合におけるサブTSFでのTSF構成について

マルチ保証ST、すなわちマルチ保証PP構成への適合を主張し、異なるサブTSFに対して複数のSARのセットを定義するSTは、サブTSFにおけるTSFの構成をPP構成から引き継がなければならない。

TOE概要では、このような構成について記述し、場合によっては実際のTOEの詳細について記述する。

D.3.2.4 TOE記述

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提供する。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。

TOE記述では、TOEの物理的な範囲、つまりTOEを構成する全てのハードウェア、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しなければならない。

また、TOE記述は、主要なTOE機能を含むTOEの論理的範囲を説明し、セキュリティ機能の特徴(TSF)の簡単な説明も提供しなければならない。提供する記述は、読者にそれらの機能の一般的な理解を与えるのに十分な詳細レベルでなければならない。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。

物理的及び論理的範囲の重要な特性は、特定の部分又は機能が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統合されており、容易に分離できない場合に特に重要である。

例1：TOEがTOE以外のエンティティと統合されている例を次に示す。

— TOEがスマートカードICの暗号コプロセッサであり、IC全体ではない。

— TOEは、暗号化プロセッサを除いたスマートカードICである。

— TOEは、MinuteGap Firewall v28.2のネットワークアドレス変換部分である。

場合によっては、サードパーティコンポーネントが証拠取得に現実的な困難をもたらすことがある。

例2：評価のための十分な証拠が第三者から入手できない例には、TOEの開発者がソースコード、設計文書、又はテスト証拠を入手できない場合が含まれる。

D.3.3 適合主張(ASE_CCL)

STの適合主張の節は、STがCC、パッケージ、PP、及びPP構成にどのように適合するかを記述する。これは、B.3.3に記述されたPPの適合主張の節と同様であるが、1つの例外として、STは他のSTへの適合を主張することが許可されていないため、STは適合ステートメントを持たない。

PPへの適合を主張するSTと、PP構成への適合を主張するSTとの追加の違いは、以下のとおりである。STは複数のPPへの適合を主張でき、PPの機能パッケージを追加でき、さらにPPと機能パッケージの両方への適合を主張できる。一方、STは正確に1つのPP構成への適合のみを主張でき、追加のPP構成、PP又は機能パッケージは主張できない。

D.3.4 セキュリティ課題定義(SPD)(ASE_SPD)

STのSPDの節は、対処すべきセキュリティ課題をSTがどのように述べているかを記述する。これは、B.3.4に記述されたPPのSPDの節と同一である。

PP及び/又はPP構成に適合するSTでは、STはこれらのPP及びPP構成コンポーネントに定義されたSPDエレメントを全て含む。PP又はPP構成コンポーネントの前提条件が、STにおけるTOEの対策方針となる場合もある。

D.3.5 セキュリティ対策方針(ASE_OBJ)

STのこの節は、B.3.5及びB.5で説明したように、PPのセキュリティ対策方針の節と同一である。

PP及び/又はPP構成に適合するSTの場合、STはこれらのPP及びPP構成コンポーネントに定義された全ての対策方針を含む。PP又はPP構成コンポーネントにおけるTOEの運用環境に関する対策方針が、STにおけるTOEの対策方針となる場合もある。

D.3.6 拡張コンポーネント定義(ASE_ECD)

STのこの節は、B.3.6で説明したPPの拡張コンポーネントの節と同一である。

D.3.7 セキュリティ要件(ASE_REQ)

D.3.7.1 セキュリティ機能要件(SFR)

D.3.7.1.1 一般

STのこの節は、B.3.7で説明したPPのセキュリティ要件の節と同一であるが、全てのSFRは完全にインスタンス化されなければならないため、選択ベースのSFR及びオプションの要件の仕様はSTには適用されないという例外がある。

PP及び/又はPP構成に適合するSTの場合、STはこれらのPP及びPP構成コンポーネントに定義される全てのSFRを含む。

D.3.7.1.2 STにおける要件の包含

PPに完全適合するSTの場合、PPの全ての要件が含まれなければならない。PPに含まれない要件は、STに含まれてはならない。

PPに正確適合するSTの場合、PPの全ての要件が含まれなければならない。

PPに論証適合するSTの場合、PPの全ての要件が含まれるか、そうでなければそれらがどのように満たされるかを説明する根拠がSTに提供されなければならない。

PPへの正確適合又は論証適合を伴うSTの場合、追加のセキュリティ対策方針をサポートする/追加の脅威をカバーする場合、PPにない追加の要件を含めることができる。

PP構成への適合を主張するSTの場合、PPへの適合と同じ規則が適用される。その場合、要件はPP構成のコンポーネント、すなわちPP及びPPモジュールから取得される。PP構成が異なる適合種別(完全適合は他の種別と組み合わせることができないため、正確適合と論証適合のみ)を要求するコンポーネントを含む場合、STは、そのコンポーネント(PP及びPPモジュール)の各々に、それらが要求する方法(正確適合又は論証適合のいずれか)で適合させる。

STがPP又はPP構成への適合を主張し、PP又はPP構成のコンポーネントがオプションの要件を含む場合、STは、これらの要件に関連する必要なSPDエレメントを必ず含むようにしながら、これらの要件をインスタンス化してよい。これは、PP又はPP構成が要求する適合に関係なく実行される可能性がある。STにおいてオプションのSFRを省略することは、PP又はPP構成への「部分的適合」を構成しないので、許可される。

例：SFRにおける外部標準の仕様及びその評価の例

FCS_CKM.1.1の詳細化：「TSF[1]は、指定された暗号鍵生成アルゴリズムに従い、非対称暗号鍵を生成しなければならない。以下を満たす2048ビット以上の暗号鍵サイズを使用するRSA方式。FIPS PUB 1864, “Digital Signature Standard (DSS)”, Appendix B.3[2]。」

次に、TOEによるSFRの充足の一部としての標準への適合は、以下のいずれかの方法で評定される。

— SFRに対して明示的な評価アクティビティが定義されている場合、その評価アクティビティにおける評価者のアクションが実行される。

— SFRに明示的な評価アクティビティが定義されていない場合、STに対して選択されたSARを適用し、標準の全文がSFRの一部として含まれるかのように、その後、適合が決定される。

D.3.7.2 セキュリティ保証要件(SAR)

STは、TOEの評価に適用されるSARのセットを指定する。

STがPP又はPP構成に適合する場合、SARのセットはPP又はPP構成に一貫したものでなければならない。

STがマルチ保証PP構成に適合する場合、以下のいずれかである。

— STは(PP構成に定義されたグローバル保証パッケージと一貫した)TOE及びTSF全体に1セットのSARを適用する。この場合、TOEは単一保証アプローチに従って評価しなければならない。又は、

— STは、TOE全体に適用されるグローバルなSARのセットと、PP構成(PP構成に定義されたSARのセットと一貫した)に定義されたサブTSFの各々に適用されるSARのセットを定義する。この場合、TOEはマルチ保証アプローチに従って評価しなければならない。

マルチ保証ST、及びそれらが適合するPP/PP構成のSARを追加するSTは、SARのセットの一貫性を実証するための保証根拠を提供しなければならない。

D.3.8 TOE要約仕様(ASE_TSS)

TOE要約仕様(TSS)の目的は、TOEの潜在的な消費者に、TOEがどのように全てのSFRを満たしているかの記述を提供することである。TOE要約仕様は、TOEがこの目的のために使用する一般的な技

[1] [選択: **TSF、TOE プラットフォーム**]

[2] [選択:
— RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: [選択:
— FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
— ANSI X9.31-1998, Section 4.1];
— ECC schemes using “NIST curves” P-256, P-384 and [選択: P-521, no other curves] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
— FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1]

術メカニズムを提供する。この記述の詳細レベルは、潜在的な消費者がTOEの一般的な形態と実装を理解するのに十分なものでなければならない。

TSSは、SFRの実装を記述する自然言語の記述を含み、その一部は、管理者及び他の利用者に見える(観察可能な)アーキテクチャの観点から、又は内部的な特徴もしくは特性の観点から、SFRがどのように組み合わさってセキュリティ機能性を提供するかを記述する。

例1：以下は内部的な特徴の例である。

— 資源の再割り当て時に残存データが利用できない。

— ログイン/パスワード認証の失敗条件が隠されている。

— 生体認証の比較スコアを隠蔽する。

例2：TOEはインターネットPCであり、SFRに認証を指定する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。SFRを満たすためにTOEが使用する適用規格のような、より詳細な情報又はより詳細な記述も提供することができる。

例3：TOE要約仕様は、例えば、技術標準を参照することができる。「TOEは、128、192、256ビットの鍵でAES暗号化及び復号化を行う暗号機能性を組み込みソフトウェアに提供する。AESアルゴリズムはISO/IEC 18033-3:2010, 5.2に準拠する。」

注：STはADVへの入力であり、ADVはTSSと他の仕様との間の不一致を指摘することが可能であることを意味する。しかし、専用の評価アクティビティは規定されていない。これは、TSSがTOEによるSFRの実現の概要を提供するが、実装仕様を構成していないことを反映している。

D.4 直接根拠ST

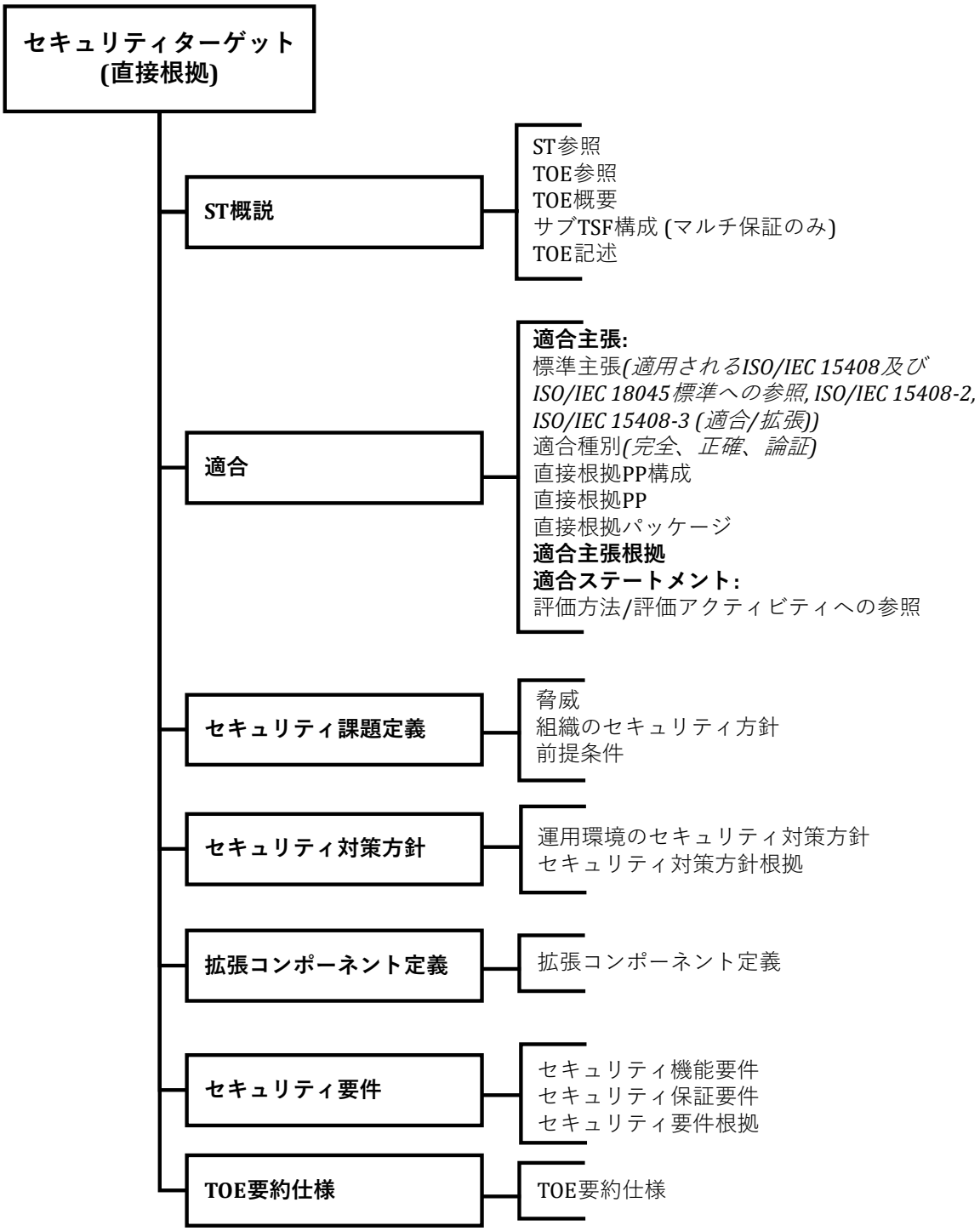
D.4.1 一般

状況によっては、TOEのセキュリティ対策方針の定義を省略することが適切な場合もある。この場合、セキュリティ要件根拠は、SFRと、必要に応じて運用環境のセキュリティ対策方針を、SPDに直接マッピングする。

直接根拠STの意図は、SFRの強化された記述に基づき、SPD、運用環境のセキュリティ対策方針、及びSFR間の間接的なレベルを最小化することである。

直接根拠STに見られる違いは、適合主張、セキュリティ対策方針、SPDの節にある。これらについては、以下のD.4.2及びD.4.3に記述する。

直接根拠STの内容を、図D.2に示す。



図D.2 — 直接根拠STの内容

D.4.2 直接根拠STに対する適合主張(ASE_CCL)

直接根拠STは、他の直接根拠PPへの適合のみを主張しなければならない。12.2及び附属書Bを参照のこと。

直接根拠STは、直接根拠アプローチを使用するPP構成への適合のみを主張しなければならない。12.2を参照のこと。

D.4.3 直接根拠STのセキュリティ課題定義(SPD)(ASE_SPD)

直接根拠STは、TOEのセキュリティ対策方針を含むSTと比較すると、セキュリティ対策方針に関して以下のような違いがある。

— TOEのセキュリティ対策方針が含まれていない。ただし、環境のセキュリティ対策方針は依然として記述しなければならない。

— STにTOEのセキュリティ対策方針がないため、運用環境のセキュリティ対策方針についてのみ、セキュリティ対策方針根拠が含まれる。

D.4.4 直接根拠STのセキュリティ課題要件(ASE_REQ)

SFRと運用環境のセキュリティ対策方針をSPDエレメントに直接対応させるセキュリティ対策方針根拠が含まれている。セキュリティ要件根拠のこの部分は、SPDの節の各脅威、OSP、前提条件の直下に配置することが推奨される。TOEのセキュリティ対策方針を含むSTと同様に、セキュリティ要件根拠も、余分なSFRがないこと、及び満たされていないSFR依存性を正当化する必要もある。この部分の根拠は、通常SFRの定義の後に配置する。

D.5 STでの他の標準の参照

STで標準を参照することは、B.4に記述されているPPの標準の項と同様である。例はD.3.7.1.2及びD.3.7.2に示されている。

附属書E
(規定)

PP/PP 構成適合

E.1 一般

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。すなわち、PP/PP構成は利用者ニーズのセットを記述し、そのPP/PP構成に適合するSTは、それらのニーズを満たすTOEを記述する。

CCはいかなる形の部分的な適合は認められないので、PP/PP構成適合が主張される場合、STは参照されるPP又はPP構成に適合しなければならない。

注1：選択ベース又はオプションのSFRの場合、7.3.2.6に概説されているこれらの種別のSFRの包含又は除外は、部分的な適合とみなされないため、許可される。

CCは、「論証適合」、「正確適合」及び「完全適合」という3つの適合種別を定義しており、許可される適合種別は、PP/PP構成(及び間接的にそのPP及びPPモジュール)によって決定される。すなわち、PP/PP構成は、その適合ステートメントにおいて、派生STに対して許可される適合種別が何であるかを明示する。

10.5で示したように、PP/PP構成が完全適合を指定している場合、STはそのPP/PP構成への完全適合のみを主張しなければならず、STが適合を主張する他のPPも完全適合を要求しなければならない。PPがPP構成に含まれる場合(それ自体、又はPP構成のPPモジュールの基本PPとして)、PP構成自体とPP構成の他の全ての構成要素も完全適合を要求する。

STが適合を主張する複数のPPに適合ステートメントが含まれている場合の論証適合と正確適合との間の区別は、STが個別に適合を主張することができる各PPに適用される。これは、STは一部のPPに対して正確適合し、他のPPに対して論証適合することを意味することがある。

完全適合の種別を持つSTは、PP/PP構成が完全適合の種別であり、これを明示的に許可している場合にのみ、PP/PP構成への適合を主張しなければならない。

STは、PP/PP構成がこれを明示的に許可している場合にのみ、PP/PP構成への論証適合を主張しなければならない。

注2：論証適合とは、PP又はPP構成への適合を主張するSTは、PP/PP構成に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/PP構成に記述されたものと同等又は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。原則として、全体としてSTが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すという条件で、STはPP/PP構成と異なるステートメントを含むことができるということを意味する。

また、あるPPを、正確適合又は論証適合のいずれかを指定する他のPPのテンプレートとして使用することも可能である。すなわち、正確適合及び論証適合のいずれかを指定するPPは、他のPPに対して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。

STがPP構成に適合し、このPP構成が完全適合でない場合、STは、PP構成のコンポーネントの適合種別に応じて、正確適合及び論証適合を要求される場合がある。

PPのPP構成への適合は、適合種別に関係なく許可されない。

E.2 論証適合

論証適合は、STがPP/PP構成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/PP構成のスポンサーを対象としている。

正確適合の場合、PP/PP構成とSTの間に明確なサブセットとスーパーセットのタイプの関係があるが、論証適合の場合、この関係はあまり明確ではない。PP/PP構成への適合を主張するSTは、PP/PP構成に記述しなければならない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、適合主張は、STが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す場合にのみ許可される。

E.3 正確適合

正確適合は、PP/PP構成の要件が満たされ、STの範囲はPP/PP構成よりも広いことがあるが、STがそのPP/PP構成の具体化であることの証拠を要求するPP/PP構成のスポンサーを対象としている。要するに、STは、TOEがPP/PP構成と同等以上のことを実行し、運用環境がPP/PP構成と同等以下のことを実施することを特定する。

例：正確適合が使用される典型的な例は、IT製品のセキュリティ要件がPP/PP構成で指定されているものに一致することが期待される、選択ベースの調達においてである。

PP/PP構成への正確適合を具体化したSTは、PP/PP構成に記載されている制限に対して追加制限を導入することもできる。

E.4 完全適合

E.4.1 一般

完全適合は、PP/PPモジュールの要件が満たされており、STが追加の機能性を含まず、まさにそれらのセキュリティ要件(SFR)の具体化であることの証拠を要求するPP/PP構成のスポンサーを対象としている。要するに、STは、TOEがPP又はPPモジュールを含むPP構成で要求されることを、追加的な主張をすることなく行うことを指定する。

「完全」適合が選択された場合、PP/PPモジュールの作成者は、以下の情報を指定するオプションも有する。

a) STが対象のPP/PPモジュールと組み合わせて適合を主張し、かつ完全適合を維持することができる他のPP。

b) PP/PPモジュールと合わせて指定しても、完全適合を維持することができるPPモジュール。

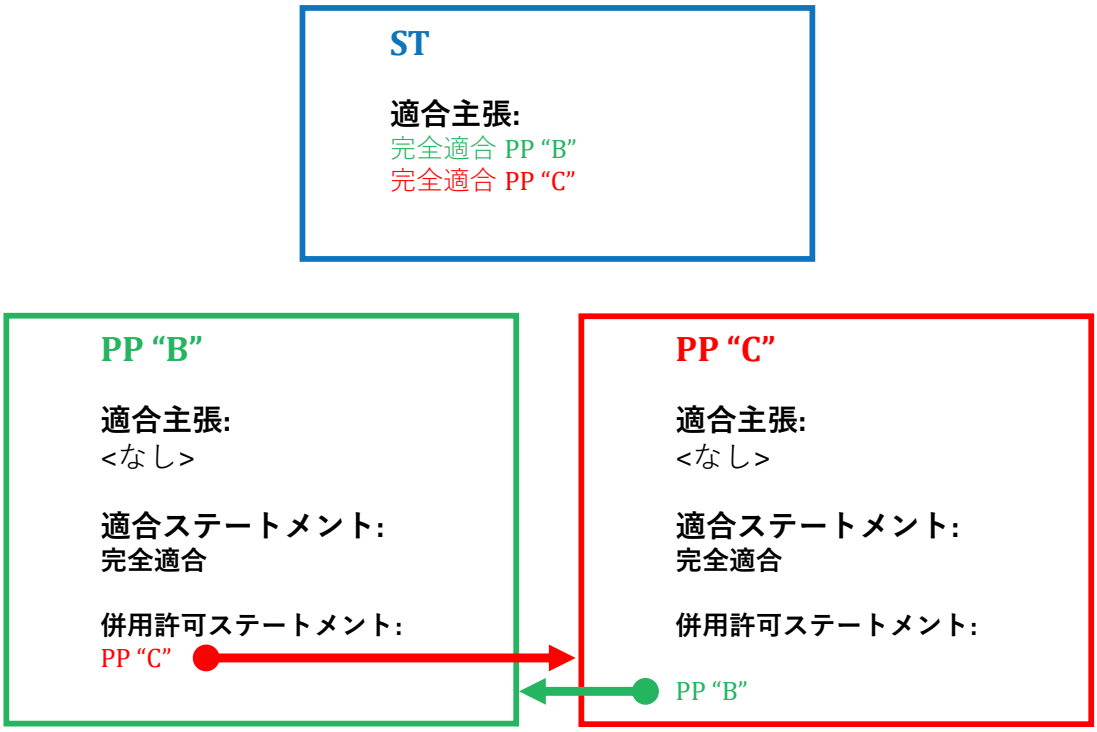
CCは、全てのPPが併用許可ステートメントで完全適合を要求し、指定された他のPPとの併用を許可する限り、STが複数のPPに対して完全適合を主張することを許可する。CCは、PP構成が完全適合を要求し、STが他のPP又はPP構成への適合を主張しない限り、STがPP構成への完全適合を主張することを許可する。

CCはまた、PPが1つ以上のPPへの適合を主張することも許可する。しかし、主張されているPPが完全適合を要求する場合、完全適合の意図を逸脱するおそれが顕在化する。これは、完全適合PPの作成者が適合主張されたPPに使用することが適切でないと考える要件を追加することができるためである。したがって、PPが完全適合を要求する場合、他のPPはそのPPに対していかなる適合種別の主張もしてはならない。この制限は、完全適合PPの作成者に、正確適合又は論証適合のいずれよりも、適合するSTに提供される機能性及び保証についてより多く制御できるようになる。

例1：STがPP A(完全適合を要求)及びPP B(論証適合を要求)への適合を同時に主張できるとすると、STがPP Aへの適合を主張する際に、PP Aの作成者がPP Aの機能性と組み合わせて使用することを明確には承認していないSFRを引き込んでしまうことになる。

上記に示したように、STが複数の完全適合PPとの完全適合を主張することは許可されている。また、PP構成は、完全適合を要求する複数のコンポーネント(PP、基本PP、PPモジュール及び基本PPモジュール)を含むことが許可されている。PP作成者がどのPP構成のコンポーネントを自分のPPとともに適合主張できるかの制御を維持できるように、B.2.3に記述されているPPの併用許可ステートメントを含めることができ、ST作成者が対象PPと同時にどのPPへの適合を主張できるかを指定する。識別された全てのPPは、併用許可ステートメントで完全適合を要求し、また、併用許可ステートメントに対象PP及び主張されている他の全てのPPもリストしなければならない。同じ構成が、PPモジュール及び基本PP、ならびに指定される可能性のある基本PPモジュールに使用される。STが複数のPPへの適合を主張する概念を明確にするために、例2を示す。

例2：STの例では、PP Bの作成者がSTにPP「B」への適合主張を許可し、さらにPP「C」と組み合わせた適合主張も許可したいと考えたとする。この状況は、図E.1に示す。



図E.1 — 複数のPPに対するSTの完全適合

その場合、次のことが真でなければならない。

a) PP B及びPP Cの両方が、適合ステートメントで完全適合を指定しなければならない。

b) PP Bは、PP CをPP Bとの併用を許可するものとして、併用許可ステートメントにリストする。

c) PP Cは、PP BをPP Cとの併用を許可するものとして、併用許可ステートメントにリストする。

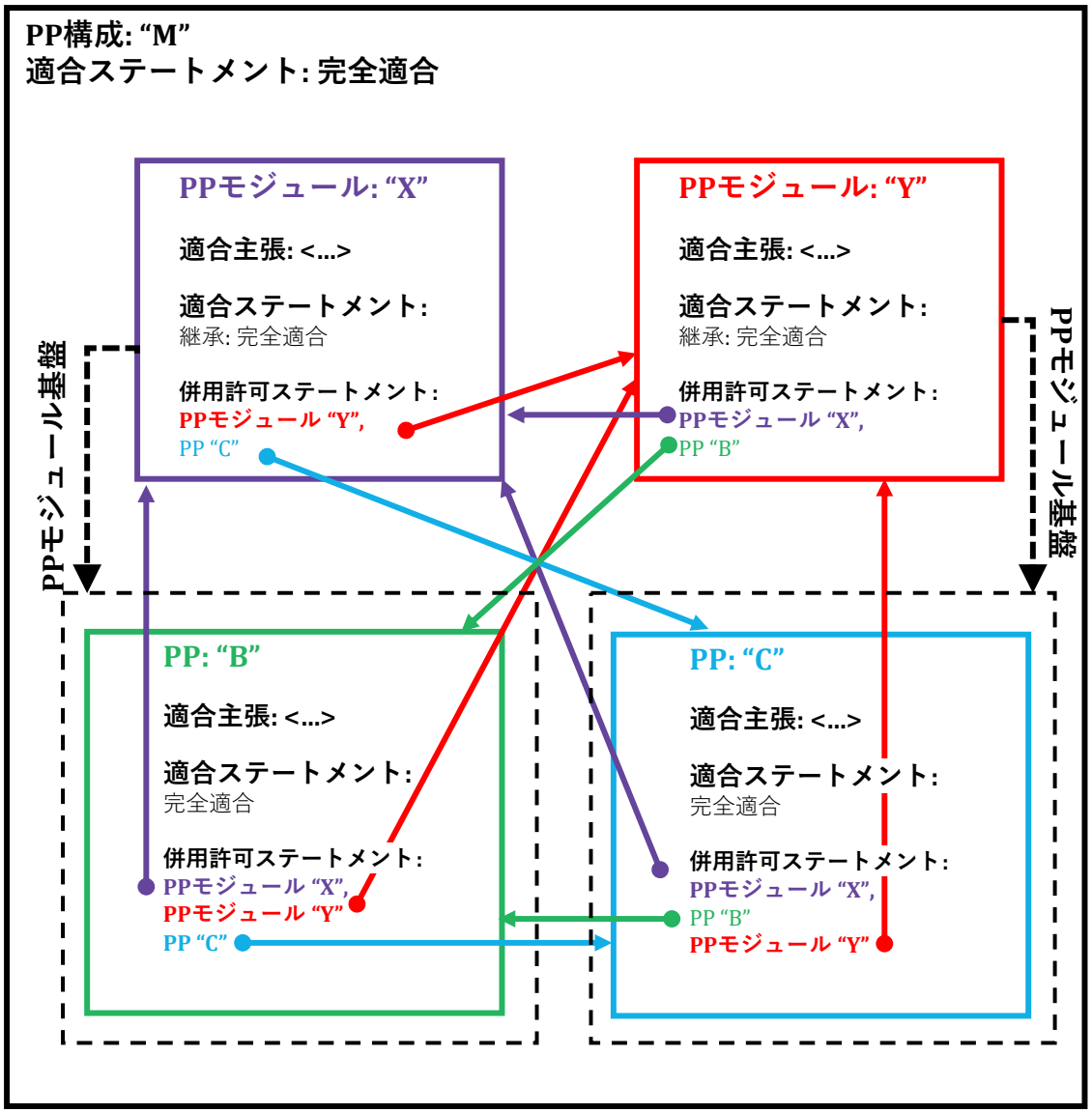
これらのステートメントのいずれかが成立しなかった場合、STはPP B及びCへの完全適合を主張することはできない。

この概念は、PPモジュール及びPP構成にも適用される。PPモジュールは、PPモジュール基盤のセットを識別しなければならない。識別されたPPモジュール基盤の1つが完全適合の適合ステートメントをもつ場合、そのPPモジュールが指定する全てのPPモジュール基盤も、完全適合を指定する適合ステートメントをもたなければならない。さらに、PPモジュールがPPモジュール基盤との使用を許可されることを保証するために、各PPモジュール基盤は、PPモジュール基盤としてPP構成で使用するために指定することを許可するPPモジュールを、その併用許可ステートメントで指定する。

注：その逆は真ではない。PPモジュールは、PP/PPモジュールをPPモジュール基盤として定義することによって暗黙的に指定しているので、併用許可ステートメントでそのPPモジュール基盤を指定する必要はない。

PPモジュールはまた、PPモジュールのPPモジュール基盤の1つとしてまだ含まれていない、他のどのPPモジュール又はPPを、PP構成においてそれと組み合わせて使用することができるかも指定する。

例3：図E.2は、PP及びPPモジュールの両方を含む完全適合のケースを記述する。



図E.2 — 複数のPP及びPPモジュールを含むPP構成との完全適合

E.4.2 完全適合FAQ/チートシート

表E.1は、完全適合のケースについて、よくある質問の概要を示したものである。

表E.1 — 完全適合の概要

PP構成	参照	許可/要求されるか
マルチ保証のモジュール式PP構成で使用可能か	図5	はい
単一保証のモジュール式PP構成で使用可能か	図5	はい
完全適合と正確適合/論証適合の適合種別を混在させることができるか	10.8.1	いいえ
完全適合PP構成で他の完全適合PPが許可されるか		はい
完全適合PP		

PP構成	参照	許可/要求されるか
完全適合PPでオプション/選択ベースのSFRが許可されるか	12.4.1	はい
オプションのSFRに関連する追加のSPDエレメントは許可されるか		はい
他の完全適合PPへの適合の主張(連鎖)は許可されるか	10.8.1 10.10.3 B.3.2.2	いいえ
完全適合PP構成で他の完全適合PPが許可されるか		はい
正確適合又は論証適合PPに基づいて構築することが許可されるか		いいえ
正確適合又は論証適合を主張するPP構成で使用できるか		いいえ
他の完全適合PPが「併用許可」であることを明示する必要があるか		はい
他の完全適合PPモジュールが「併用許可」であることを明示する必要があるか	11.2.3.3 d)	はい
完全適合PPモジュール		
完全適合PPモジュールのオプション/選択ベースSFRは許可されるか	11.2.3.3	はい
完全適合PPモジュールは、PPモジュール基盤のコンポーネントを、併用許可ステートメントに含めない	11.2.3.3 d)	はい
他の完全適合PP及びPPモジュールが併用許可であることを明示する必要があるか	11.2.3.3 d)	はい
全ての併用許可アイテムも完全適合が要求されるか	11.2.3.3 d)	はい
完全適合機能パッケージ		
完全適合機能パッケージのオプション/選択ベースのSFRは許可されるか		はい
機能パッケージはSTで追加できる		いいえ
STの適合主張の中での主張は許可されるか	12.2 d)	いいえ
完全適合ST		
全ての完全適合PPのSPD、及び/又はPP構成コンポーネントを含むことが要求されるか	12.4.3	はい
追加又は階層的に上位のセキュリティ要件は許可されるか	12.4.4	いいえ
選択された選択ベースの要件のみが含まれることが要求されるか	12.4.4	はい
直接根拠アプローチで使用できるか		はい

参考文献

ISO／IEC標準とガイダンス

[1] ISO/IEC 8367, *Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing*

[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、CC:2022、改訂第1版、2022年11月 — パート4：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*

[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、CC:2022、改訂第1版、2022年11月 — パート5：セキュリティ要件の定義済みパッケージ*

[4] ISO/IEC 15446, *Information technology — Security techniques — Guidance for the production of Protection Profiles and ST s*

[5] ISO/IEC/TR 18018:2010, *Information technology — Systems and software engineering — Guide for configuration management tool capabilities*

[6] ISO/IEC/TR 18031:2011, *Information technology — Security techniques — Random bit generation*

[7] ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

[8] ISO/IEC 19608, *Information technology — Security techniques — Guidance for developing security and privacy functional requirements based on ISO/IEC 15408*

[9] ISO/IEC 19249, *Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems, and applications*

[10] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

[11] ISO/IEC 19791, *Information technology — Security techniques — Security assessment of operational systems*

[12] ISO/IEC 19896-1, *IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*

[13] ISO/IEC 19896-3, *IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators*

[14] ISO/IEC 20004, *Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045*

[15] ISO/IEC TR 22216, *Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022*

[16] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[17] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[18] ISO/IEC 27034 (all parts), *Information technology — Application security*

PP及び評価済み製品のカタログ

[19] Common Criteria portal: Certified Products, http://www.commoncriteriaportal.org/products/

[20] Common Criteria portal: Protection Profiles, http://www.commoncriteriaportal.org/pps/

[21] Common Criteria portal: Collaborative Protection Profiles, http://www.commoncriteriaportal.org/pps/?cpp=1

---

[i] 【訳注】8.4.1 の例外は原文では a), b)の 2 つだが、原文 b)は前半部と後半部で異なる事例を記しているため、日本語版では後半部を c)として分割し、3 つの例外としている。

[ii] 【訳注】13.8 の最後の文の「観点」は原文では”prism”。