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3：セキュリティ保証要件

1999年8月

バージョン2.1

CCIMB-99-033

平成 13 年 1 月翻訳第 1.2 版
情報処理振興事業協会
セキュリティセンター

IPAまえがき

本書の目的

本書は、情報技術セキュリティ評価のための評価基準であるコモンクライテリア(Common Criteria ： CC)バージョン2.1を日本語訳したものである。本書は、情報処理振興事業協会(略称IPA)におけるセキュリティ評価・認証プロジェクトの評価技術タスクフォース(略称CCTF)において、評価作業のための補助資料として作成されたものである。したがって、本翻訳書は、セキュリティ評価の規格書ではないが、情報セキュリティに関心をもつ人にとって、CCを理解するための参考資料として役立つことも期待している。

* CC Version 2.1は、情報セキュリティ技術のセキュリティ評価に関する統一基準であり、カナダ、フランス、ドイツ、オランダ、イギリス、アメリカ６カ国によるCCプロジェクトにより作成された。CC Version 2.1は、国際標準のISO/IEC 15408:1999と同等の評価基準書である。

使用上の注意

本書は、用語及び体裁の統一、記述内容などに不備がある可能性がある。疑問点については CC Version 2.1で確認していただきたい。本書は、参照利用されることのみを目的とし公開される。本書の改変、及び他への転載は禁止する。

参考文献

Common Criteria for Information Technology Security Evaluation

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

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

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

著作権について

まえがき

情報技術セキュリティ評価のためのコモンクライテリア(CC 2.1)の本バージョンは、国際標準のISO/IEC 15408:1999に合わした改訂版である。さらに、本書は、その使用を促進するために、体裁が整えられている。本文書を使用して書かれたセキュリティ仕様書、及びその仕様書に従っていることを示したIT製品/システムは、ISO/IEC 15408:1999に従っているとみなされる。

CC 2.0は1998年5月に発刊された。続いて、相互承認協定は、調印に加わった組織によって実行された評価結果の相互承認の基礎として、CCを使用することが確立された。

ISO/IEC JTC 1は、1999年6月に、マイナーな、主に編集上の修正をしてCC 2.0を採用した。

CCバージョン2.1は、次のパートから構成される:

- パート1: 概説と一般モデル
- パート2: セキュリティ機能要件
- パート3: セキュリティ保証要件

次の法定通知は、要請により、CCのすべてのパートに記載してある。

以下に示す、またパート1附属書Aに完全に識別した、7つの政府組織(“the Common Criteria Project Sponsoring Organisations”と呼ばれる集団)は、情報技術セキュリティ評価ためのコモンクライテリア バージョン2.1のパート1から3(CC 2.1と呼ぶ)の著作権を共有したまま、ISO/IEC 15408国際標準の継続的な開発/維持の中で、CC 2.1を使用するためにISO/IECに対し、排他的でないライセンスを許可している。ただし、適切と思われる場合にCC 2.1を使用、複製、配布、翻訳及び改変する権利は、the Common Criteria Project Sponsoring Organisationsが保有する。

カナダ:	Communications Security Establishment
フランス:	Service Central de la Sécurité des Systèmes d’Information
ドイツ:	Bundesamt für Sicherheit in der Informationstechnik
オランダ:	Netherlands National Communications Security Agency
英国:	Communications-Electronics Security Group
米国:	National Institute of Standards and Technology
米国:	National Security Agency

目次

図一覧

表一覧

1　適用範囲

このパート **3** は、**CC** の保証要件を定義している。ここには、保証を測定するための尺度を定義する評価保証レベル（**EAL**）、保証レベルが構成される個々の保証コンポーネント、**PP** と **ST** の評価のための基準が含まれている。

1.1　CCパート3の構成

第 **1** 章は、このパート **3** の概説と枠組みである。

第 **2** 章は、保証クラス、ファミリ、コンポーネント、及び評価保証レベルの提示構造とそれらの関係を記述している。第 **8** 章から第 **14** 章に記述されている保証クラスとファミリの特徴についても記述している。

第 **3** 章、第 **4** 章、及び第 **5** 章では、**PP** と **ST** の評価基準を簡単に紹介し、次にこれらの評価に使われるファミリとコンポーネントについて詳しく説明している。

第 **6** 章は、**EAL** を詳細に定義している。

第 **7** 章は、保証クラスを簡単に紹介し、次に第 **8** 章から **14** 章では、それらのクラスを詳細に定義している。

第 **15** 章、及び第 **16** 章は、保証の維持の評価基準を簡単に紹介し、その後で、それらのファミリとコンポーネントを詳細に定義している。

附属書 **A** は、保証コンポーネントの間の依存性を要約している。

附属書 **B** は、**EAL** と保証コンポーネントの間の相互参照を示している。

1.2　CC保証の枠組み

この節の目的は、保証に対する **CC** の手法を支持する原理を示すことである。この節を理解することにより、読者は、**CC** 保証要件の合理的根拠を理解できる。

1.2.1　CC の原理

CC の原理は、セキュリティ及び組織のセキュリティ方針を犯す脅威を明確に表現し、提案するセキュリティ手段が意図する目的に対して明らかに十分であることである。

そこで、脆弱性の可能性、脆弱性を実行させる能力（意図的悪用または意図しない誘発）、及び

脆弱性が実行されることにより引き起こされる損害の範囲を軽減する手段が採用されるべきである。さらに、脆弱性のその後の識別と、及び脆弱性が悪用または誘発されることの排除、緩和、及び/または通知を容易にする手段が採用されるべきである。

1.2.2 保証手法

CC の原理は、信頼されるべき **IT** 製品またはシステムの評価（有効な調査）に基づいて保証を提供することである。評価は、保証を提供する伝統的な手段であり、先行する評価基準書の基礎である。既存の手段と調和を取るために、**CC** は、同様の原理を採用している。**CC** は、適用範囲、深さ、及び厳格性を一層強調することにより、専門の評価者による、証拠資料及び結果としての **IT** 製品またはシステムの有効性を測定することを提案している。

CC は、保証を得るための他の手段の相対的利点を排除していないし、またそれらについての注釈も行っていない。保証を得るための別の手法に関する調査が継続されている。成熟した別の手法がこれらの調査活動から明らかになれば、それらを、この **CC** に含めることが考慮される。現在の **CC** は、将来それらを取り入れることができるように構成されている。

1.2.2.1 脆弱性の重要性

不正入手及び善意であるとしてもセキュアでない行動の両方に対してセキュリティ方針に違反する機会を悪用するよう活発に求める脅威エージェントが存在すると想定されている。脅威エージェントは、意図せずにセキュリティの脆弱性を誘発し、組織に損害を与えることがある。機密に関わる情報を処理する必要があり、十分に信頼された製品またはシステムを使用できないために、**IT** の障害をもたらす重大な危険が存在する。したがって、**IT** セキュリティの違反が重大な損失をもたらすことがある。

IT セキュリティ違反は、ビジネスでの **IT** の適用時に、脆弱性の意図的悪用または意図しない誘発によって引き起こされる。
IT 製品とシステムで起きる脆弱性を阻止する手順を踏まなければならない。可能な限り脆弱性は、次のようにすべきである。

- **a)** 排除 － つまり、すべての実行可能な脆弱性を明らかにし、排除または無効にする有効な手順を踏むべきである。
- **b)** 最小化 － つまり、脆弱性の実行による可能性がある影響を、容認できる残留レベルにまで軽減するための有効な手順を踏むべきである。
- **c)** 監視 － つまり、残留する脆弱性を実行させる試みを検出し、損失を抑える手順を踏むことができるようにする有効な手順を踏むべきである。

1.2.2.2 脆弱性の原因

脆弱性は、以下での障害により起きることがある。

- **a)** 要件 － つまり、**IT** 製品またはシステムは、必要とされるすべての機能と特徴を所有しているが、なお、セキュリティに不適切であるか、または効果的でない脆弱性を含む。
- **b)** 構成 － つまり、**IT** 製品またはシステムがその仕様を満たしていない、及び/また

は構成標準が十分でないかまたは設計上の選択が正しくない結果、脆弱性が導入される。

c) 運用 － つまり、**IT** 製品またはシステムは、正しい仕様に従って正しく構成されているが、運用の管理が不適切である結果、脆弱性が導入された。

1.2.2.3 CC 保証

保証は、**IT** 製品またはシステムがセキュリティ対策方針を達成しているという確信の根拠である。保証は、実証されない主張、これまでの関連する経験、または特別の経験などのソースを参照することにより得ることができる。ただし、この **CC** は、能動的な調査を通して保証を提供する。能動的な調査とは、セキュリティ特性を決定するための **IT** 製品またはシステムの評価である。

1.2.2.4 評価を通した保証

評価は、保証を得るための伝統的な手段であり、**CC** の手法の基礎となっている。評価技法には、次のものが含まれるが、必ずしもこれだけに限定されない。

a) 処理及び手続きの分析とチェック
b) 処理及び手続きが適用されていることのチェック
c) **TOE** 設計表現の間の対応の分析
d) 要件に対する **TOE** 設計表現の分析
e) 証拠書類の検証
f) ガイダンス文書の分析
g) 開発された機能テストと提供された結果の分析
h) 独立機能テスト
i) 脆弱性（欠陥仮説法を含む）の分析
j) 侵入テスト

1.2.3 CC 評価保証の尺度

CC 原理は、評価のための労力が大きくなれば、それだけ大きな保証結果が得られること、目標は、必要な保証レベルを提供するために必要な最小の労力を適用することであると主張している。労力のレベルは、次のことに基づいて増加する。

a) 適用範囲 － つまり、**IT** 製品またはシステムの含まれる部分が多くなると、労力は大きくなる。
b) 深さ － つまり、詳細な設計や詳細な実装を使用すると、労力は大きくなる。
c) 厳格性 － つまり、より構造化された、形式的な方法で適用されると、労力は大きくなる。

2　セキュリティ保証要件

2.1　構造

次の節では、保証クラス、ファミリ、コンポーネント、**EAL** を表すために使用される構造と、それらの関係について記述する。

図 **2.1** は、この **CC** パート **3** に定義されている保証要件を例示している。保証要件の最も抽象的なセットは、クラスと呼ばれる。各クラスには、保証ファミリが含まれ、保証ファミリには、保証コンポーネントが含まれ、保証コンポーネントには、保証エレメントが含まれる。クラスとファミリは、保証要件を分類するための分類方法を提供するために使われる。一方、コンポーネントは、**PP/ST** に保証要件を特定するために使われる。

2.1.1　クラスの構造

図 **2.1** は、保証クラスの構造を示す。

2.1.1.1 クラス名

各保証クラスには、一意の名前が割り付けられる。この名前は、保証クラスが扱うトピックを示す。

保証クラス名の一意の短い形式も提供される。これは、保証クラスを参照するための主要な手段である。採用されている規則では、"**A**"の次にクラス名に関係する **2** 文字が続く。

2.1.1.2 クラスの概説

各保証クラスには、クラスの構成を記述し、クラスの意図を説明する支援の文が含まれている導入の節がある。

2.1.1.3 保証ファミリ

各保証クラスには、少なくとも **1** つの保証ファミリが含まれる。保証ファミリの構造については、次の節で説明する。

図 2.1 ― 保証クラス/ファミリ/コンポーネント/エレメントの階層

2.1.2 保証ファミリの構造

図 **2.1** は、保証ファミリの構造を示す。

2.1.2.1 ファミリ名

各保証ファミリには一意の名前が割り付けられる。この名前は、保証ファミリが扱うトピックについての記述情報を提供する。各保証ファミリは、同じ意図を持つ他のファミリが含まれている保証クラスの中に置かれる。

保証ファミリ名の一意の短い形式も提供される。これは、保証ファミリを参照するために使われる主な手段である。採用されている規則では、クラス名の短い形式が使われ、その後に下線文字が続き、次にファミリ名に関係する **3** 文字が続く。

2.1.2.2 目的

保証ファミリの目的の節は、保証ファミリの意図を表す。

この節は、ファミリが対処することを意図している、**CC** 保証の枠組みに特に関係する目的を記述する。保証ファミリの記述は、全般的なレベルにとどめている。目的に必要な特別な詳細は、特定の保証コンポーネントに組み込まれる。

2.1.2.3 コンポーネントのレベル付け

各保証ファミリには、**1** つまたは複数の保証コンポーネントが含まれる。保証ファミリのこの節は、使用可能なコンポーネントについて記述し、それらの区別を説明する。主な目的は、保証ファミリが、**PP/ST** に対する保証要件の必要な部分または有用な部分であることが決定された後、これらの保証コンポーネントを区別することである。

複数のコンポーネントが含まれている保証ファミリは、レベル付けが行われ、コンポーネントにレベルを付ける方法の根拠が示される。この根拠は、適用範囲、深さ、及び/または厳格性の観点からである。

2.1.2.4 適用上の注釈

保証ファミリの適用上の注釈の節が存在する場合には、保証ファミリの追加情報が含まれる。この情報は、保証ファミリの利用者（例えば、**PP** と **ST** の作成者、**TOE** の設計者、評価者）に特に関心があるべきである。表現は、非形式的であり、例えば、使用上の制約及び特別の注意が必要となる領域に関する警告が扱われる。

2.1.2.5 保証コンポーネント

各保証ファミリは、少なくとも **1** つの保証コンポーネントを持つ。次の節に保証コンポーネントの構造を示す。

2.1.3 保証コンポーネント構造

図 **2.2** は、保証コンポーネント構造を示す。

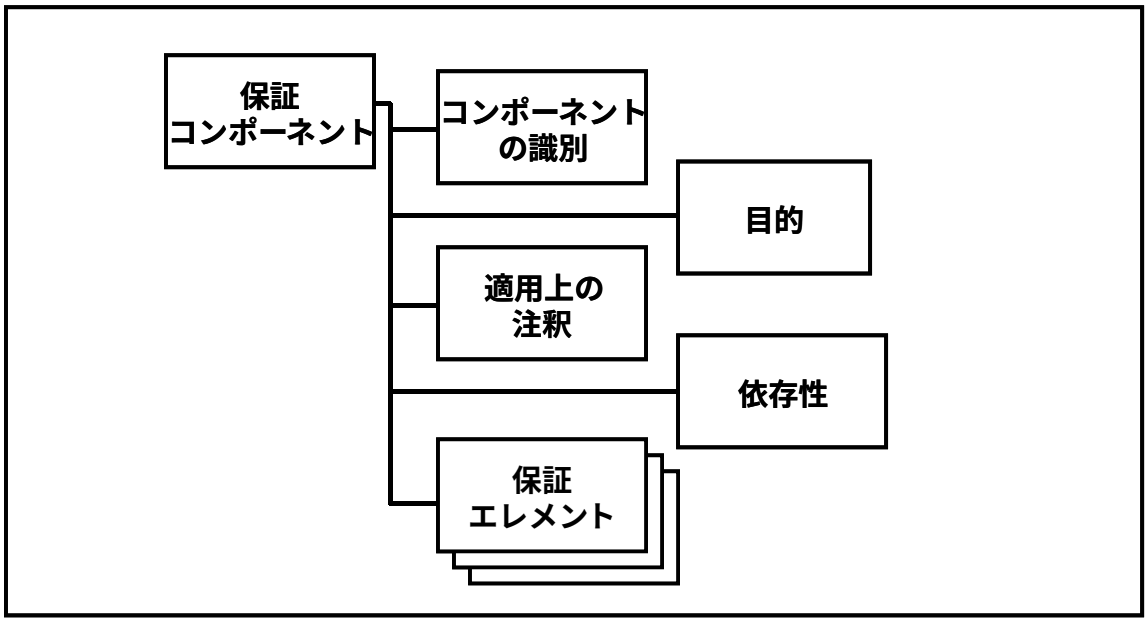

図 2.2 ― 保証コンポーネントの構造

ファミリ内のコンポーネントの関係は、ボールド文字で強調表示される。新規、階層内でこれまでのコンポーネントの要件を越えて拡張または修正されている要件のこれらの部分は、ボールドで表示される。同じボールド表記が、依存性にも使用される。

2.1.3.1 コンポーネントの識別

コンポーネント識別の節は、コンポーネントを識別、分類、登録及び参照するために必要な記述情報を提供する。

各保証コンポーネントには、一意の名前が割り付けられる。この名前は、保証コンポーネントが扱うトピックについての記述情報を提供する。各保証コンポーネントは、セキュリティ対策方針を共有する保証ファミリの中に置かれる。

保証コンポーネント名の一意の短い形式も提供される。これは、保証コンポーネントを参照するために使われる主な手段である。使用される規定では、ファミリ名の短い形式が使用され、次にピリオドが続き、次に数字が続く。各ファミリの中のコンポーネントに対する数字は、**1** から順に割り付けられる。

2.1.3.2 目的

保証コンポーネントの目的の節が存在する場合には、特定保証コンポーネントの特別の目的が含

まれる。この節を持つ保証コンポーネントに対しては、コンポーネントの特別の意図を示し、目的をさらに詳細に説明する。

2.1.3.3 適用上の注釈

保証コンポーネントの適用上の注釈の節が存在する場合には、コンポーネントを容易に使用するための追加情報が含まれる。

2.1.3.4 依存性

保証コンポーネントの間の依存性は、コンポーネントが自己完結型ではなく、他のコンポーネントの存在に依存するときに起きる。

各保証コンポーネントは、他の保証コンポーネントに依存性の完全なリストを提供する。あるコンポーネントは、「依存性：なし」を示す。これは、いかなる依存性も存在しないことを示す。依存したコンポーネントが、他のコンポーネントに依存している場合もある。

依存性リストは、必要とされる最小限の保証コンポーネントのセットを識別する。依存性リストにおいて、コンポーネントのさらに上位にあるコンポーネントも、依存性を満たすために使用することができる。

特別な状況では、指定された依存性が適用できないことがある。**PP/ST** の作成者は、なぜ、指定された依存性が適用できないのか、その根拠を示すことで、その依存性を満たさないことを選択できる。

2.1.3.5 保証エレメント

保証エレメントのセットが各保証コンポーネントに提供される。保証エレメントは、さらに分割しても、意味のある評価結果が得られないセキュリティ要件である。これは、この **CC** で認定されている最低のセキュリティ要件である。

各保証エレメントは、保証エレメントの以下の **3** つのセットの **1** つに属するものとして識別される。

a) 開発者アクションエレメント：開発者が行わなければならないアクティビティ。このアクションのセットは、次に続くエレメントのセットに参照されている証拠資料によってさらに評価付けされる。開発者アクションの要件は、エレメント番号の後に"**D**"の文字を追加することによって識別される。

b) 証拠の内容・提示エレメント：必要とされる証拠、証拠が示すべきもの、証拠が伝えるべき情報。証拠の内容・提示の要件は、エレメント番号の終わりに"**C**"の文字を追加することによって識別される。

c) 評価者アクションエレメント：評価者が行うべきアクティビティ。このアクションのセットには、証拠の内容・提示エレメントに記述されている要件が満たされていることの確認が明示的に含まれる。開発者がすでに行っているものに加えて実行すべき明示的なアクションと分析も含まれる。暗黙の評価者アクションも、証拠の内容・提

示要件によって示されていない開発者のアクションエレメントの結果として実行される。評価者アクションの要件は、エレメント番号の終わりに"**E**"の文字を追加することにより識別される。

開発者アクションと証拠の内容・提示は、**TOE** セキュリティ機能に保証を示す開発者の責任を表すために使用される保証要件を定義する。これらの要件を満たすことにより、開発者は、**TOE** が **PP** または **ST** の機能と保証の要件を満たしていることの確信を増すことができる。

評価者アクションは、評価の **2** つの側面での評価者の責任を定義する。最初の側面は、第 **4** 章と第 **5** 章の **APE** クラスと **ASE** クラスに従った **PP/ST** の正当性の確認である。**2** 番目の側面は、**TOE** がその機能と保証の要件に従っていることの検証である。**PP/ST** が正当であり、要件が **TOE** によって満たされていることを実証することにより、評価者は、**TOE** がセキュリティ対策方針を達成するという確信の根拠を提供することができる。

開発者アクションエレメント、証拠の内容・提示エレメント、及び明示的評価者アクションエレメントは、**TOE** の **ST** においてなされるセキュリティ主張の検証に費やされなければならない評価者の労力を識別している。

2.1.4 保証エレメント

各エレメントは、満たす必要がある要件を表す。要件のこれらの文は、明確、簡潔、及び曖昧でないことが意図されている。したがって、重文は存在しない。各分離可能な要件は、個別のエレメントとして記述される。

エレメントは、暗黙の要件となる略称のようないくつかの定義語を使用するのではなく、使用される用語として一般的な辞書の意味を用いて書かれている。したがって、エレメントは、明示的な要件として書かれ、*予約語は使用されていない*。

CC パート **2** と対照的に、割付も選択の操作も、**CC** パート **3** のエレメントに関係していない。ただし、必要に応じて、パート **3** の改良が行われるかもしれない。

2.1.5 EAL 構造

図 **2.3** は、このパート **3** に定義されている **EAL** 及び関連する構造を示す。図は、保証コンポーネントの内容を示しているが、この情報は、**CC** に定義されている実際のコンポーネントを参照することにより、**EAL** に含まれていることが意図されていることに注意のこと。

2.1.5.1 EAL 名

各 **EAL** に一意の名前が割り付けられる。この名前は、**EAL** の意図についての記述情報を提供する。

EAL 名の一意の短い形式も提供される。これは、**EAL** を参照するときに使われる主要な手段である。

2.1.5.2 目的

EAL の目的の節は、**EAL** の意図を表す。

2.1.5.3 適用上の注釈

EAL の適用上の注釈の節が存在する場合には、**EAL** の利用者（例えば、**PP** と **ST** の作成者、この **EAL** を目標としている **TOE** の設計者、評価者）に特に関心のある情報が含まれる。表現は、非形式的であり、例えば、使用上の制約及び特別の注意が必要となる領域に関する警告が扱われる。

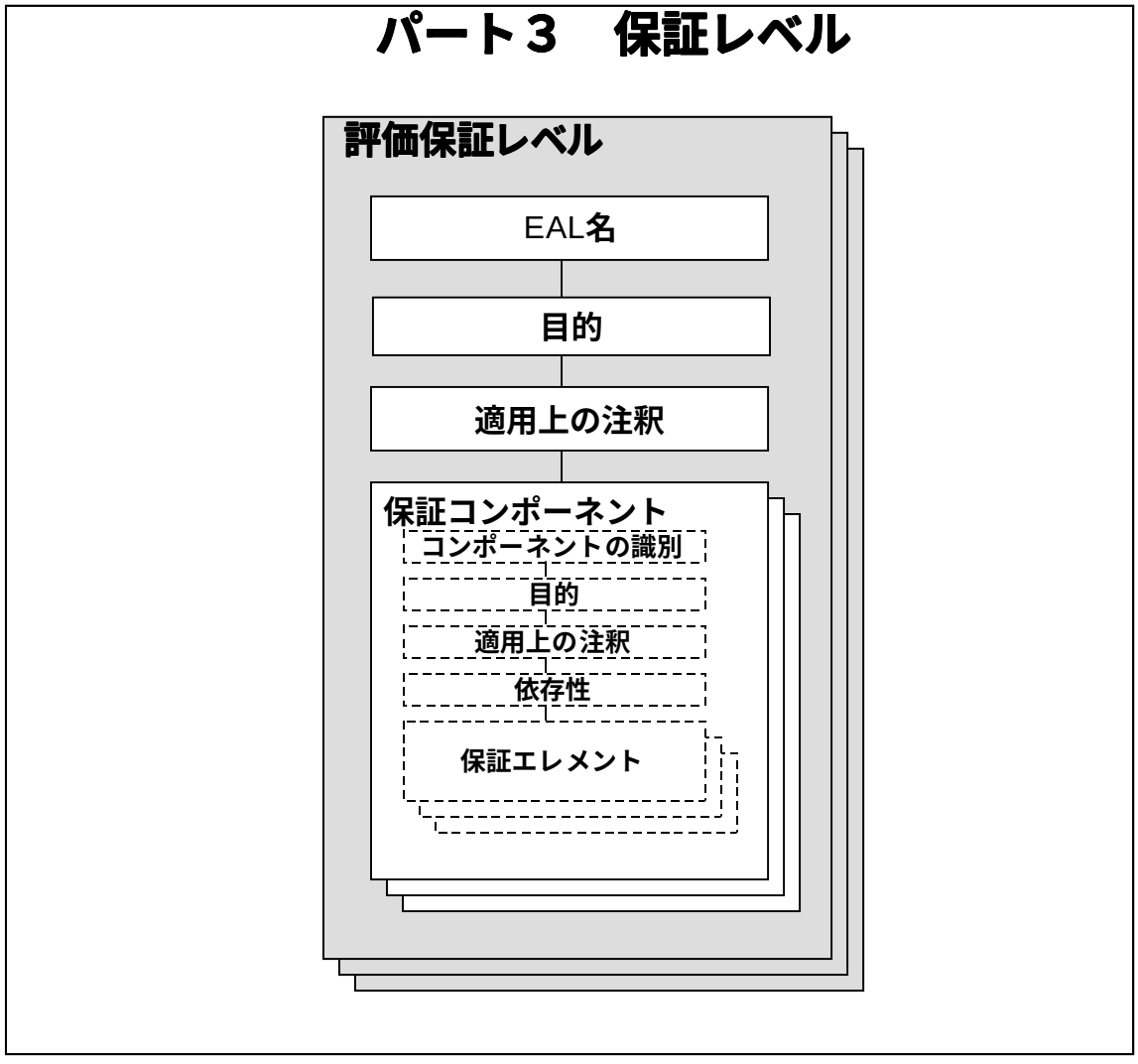

図 2.3 － EAL 構造

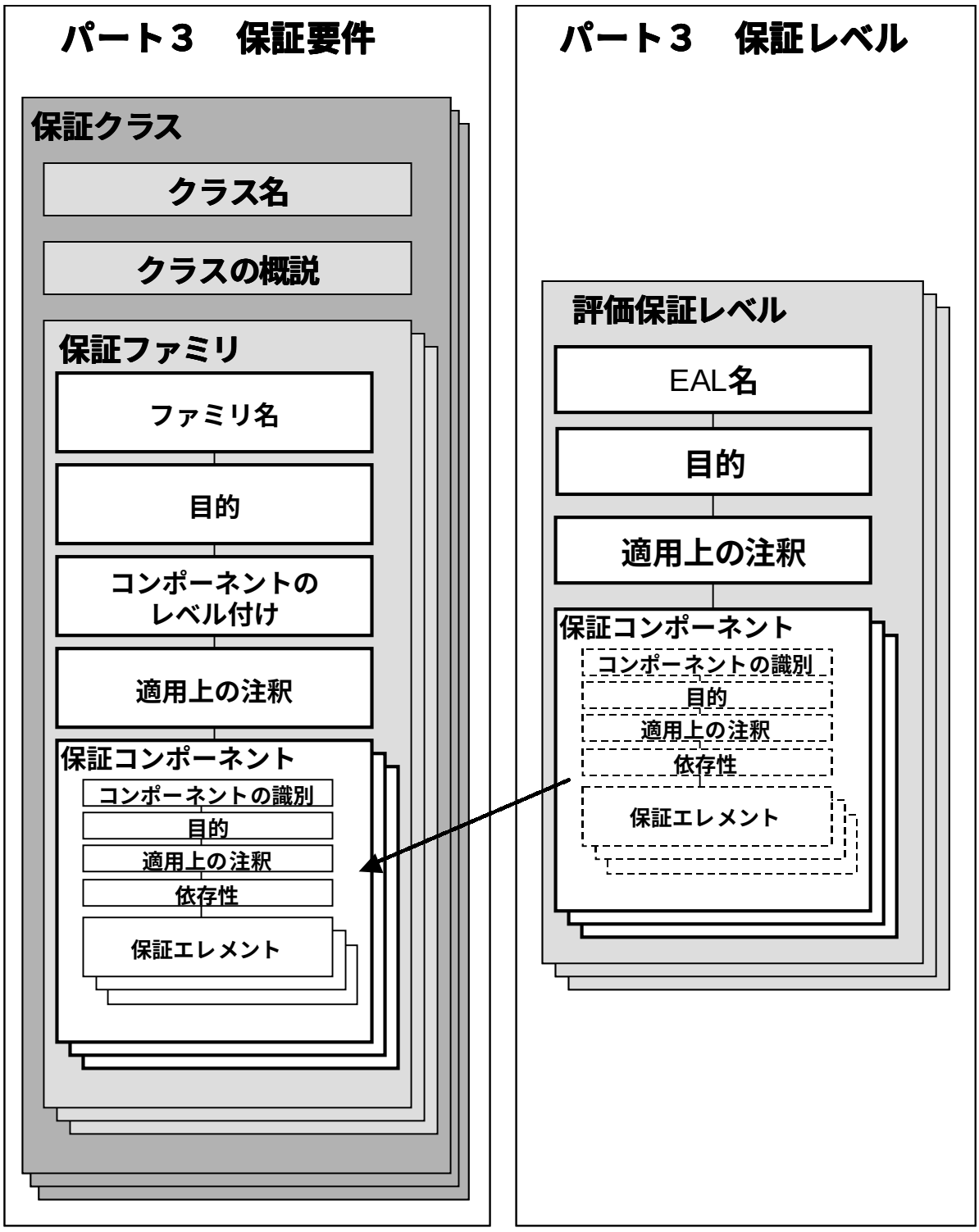

図 2.4 ― 保証及び保証レベルの関連

2.1.5.4 保証コンポーネント

各 **EAL** に対して、保証コンポーネントのセットが、選択されている。

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

a) 他の保証ファミリから追加の保証コンポーネントを含める。

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

2.1.6 保証と保証レベルの関係

図 **2.4** は、**CC** に定義されている保証要件と保証レベルの関係を示す。保証コンポーネントは、さらに保証エレメントに分解されるが、保証エレメントは、保証レベルにより個々に参照することはできない。図の矢印は、**EAL** からクラスの中の定義されている保証コンポーネントへの参照を表すことに注意のこと。

2.2 コンポーネントの分類

このパート **3** には、関係する保証に基づいてグループ化されたファミリのクラスとコンポーネントが含まれている。各クラスの最初には、クラスの中のファミリと各ファミリのコンポーネントを示す図が存在する。

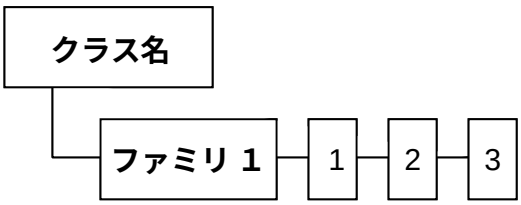

図 2.5 ― サンプルクラスのコンポーネント構成図

上記の図 **2.5** において、記載されているクラスには、単一のファミリが含まれている。ファミリには、直線的に階層化されている **3** つのコンポーネントが含まれている（つまり、コンポーネント **2** は、特定のアクション、特定の証拠、またはアクションまたは証拠の厳格性の観点から、コンポーネント **1** 以上を必要とする）。このパート **3** の保証ファミリは、すべて直線的階層であるが、直線性は、将来追加される保証ファミリに対する必須の基準ではない。

2.3 プロテクションプロファイル及びセキュリティターゲット評価基準クラス構造

プロテクションプロファイルとセキュリティターゲット評価に対する要件は、保証クラスとして取り扱われ、下記の他の保証クラスに使用されるのと同様の構造を用いて表される。明らかな相

違点は、関連するファミリ記述にはコンポーネントのレベル付けの節が存在しないことである。その理由は、各ファミリは単一のコンポーネントだけを持ち、その結果、レベル付けが行われないためである。

このパート **3** の第 **3** 章の表 **3.1**、**3.2**、**3.3**、及び **3.4** は、**APE** と **ASE** の両方のクラスに対して、構成ファミリの要約と省略名を示している。**APE** ファミリの叙述的要約は、**CC** パート **1**、附属書 **B**、**B.2.2** から **B.2.6** に記載されている。一方、**ASE** ファミリの叙述的要約は、**CC** パート **1**、附属書 **C**、**C.2.2** から **C.2.8** に記載されている。

2.4 パート3での用語の使用

以下はこのパート **3** で正確な方法で使用されている用語のリストである。それらの用語は一般的な英語であり、それらの使用は、下記の説明に限定されるが、辞書の定義と一致するため、それらを用語集に含める価値がないと考えた。ただし、これらの用語の説明は、このパート **3** を開発するときにガイダンスとして使用されたので、一般的理解に役立つはずである。

チェックする(Check) － この用語は、「確認する」または「検証する」と同様であるが、それほど厳格ではない。この用語は、評価者による迅速な決定を必要とし、おそらく、単なる通り一遍の分析を必要とするか、まったく分析を必要としない。

理路整然とした(Coherent) － エンティティは、論理的順序で並べられ、識別できる意味を持つ。証拠資料では、これは、対象読者が理解できるかどうかの観点から、文書の実際のテキストと文書構造の両方に関係する。

完全な(Complete) － エンティティのすべての必要な部分が提供されている。証拠資料に関して、これは、抽象化のレベルにおいてこれ以上の説明が必要ない詳細レベルで、すべての関連する情報がカバーされていることを意味する。

確認する(Confirm) － この用語は、なにかを詳細にレビューする必要があること、及び充足性を独立して決定する必要があることを示すために使用される。必要とされる厳格性のレベルは、内容によって異なる。この用語は、評価者アクションにのみ適用される。

一貫した(Consistent) － この用語は、複数のエンティティの関係を記述し、これらのエンティティの間に明らかな矛盾が存在しないことを示す。

対抗する(Counter)（動詞） － この用語は、一般的にセキュリティ対策方針が特定の脅威に対抗する文脈で使用されるが、その結果、脅威が完全に根絶されることを必ずしも示さない。

実証する(Demonstrate) － この用語は、「証明する」**(proof)**ほど厳格ではない結論に導く分析を意味する。

記述する(Describe) ― この用語は、エンティティのある種の特定の詳細が提供されることを要求する。

決定する(Determine) ― この用語は、特定の結論に到達することを目的として、独立の分析が行われることを要求する。この用語の利用は「確認する」または「検証する」と異なる。なぜなら、これらの他の用語は、レビューする必要がある分析がすでに行われていることを暗示するが、「決定する」の用語の使用は、通常、これまでに分析が行われていないときの真に独立した分析を暗示するからである。

保証する(Ensure) ― この用語は、それだけで使用される場合、アクションとその結果の間の強い因果関係を暗示する。この用語の前には、一般的に、「助ける」**(helps)**の単語が置かれる。これは、結果が、そのアクションだけでは完全に確実でないことを示す。

徹底的(Exhaustive) ― この用語は、**CC** では、分析または他のアクティビティの実施に関して使用されている。これは、「系統的」**(systematic)**と関連があるが、曖昧でない計画に従って分析またはアクティビティを行うために方法論的手法が取られた点だけでなく、採用されたその計画が、あらゆる可能な手段が取られたことを十分に保証することを示すという点において、かなり強意である。

説明する(Explain) ― この用語は、「記述する」及び「実証する」の両方とは異なる。これは、行われたアクションの道筋が必ずしも最適であったかどうかを実際に論証せずに、「何故」**(Why?)**の質問に答えることを意図している。

内部的に一貫した(Internally consistent) ― エンティティの各部分の間に明らかな矛盾が存在しない。証拠資料に関して、これは、相互に矛盾すると取られる文が証拠資料内に存在しないことを意味する。

正当化(Justification) ― この用語は、結論に導く分析を意味するが、実証よりも厳格である。この用語は、論理的な論証の各手順を非常に注意深く、完全に説明することに関して、重大な厳格性を要求する。

相互サポート(Mutually supportive) ― この用語は、エンティティのグループの関係を記述し、エンティティが相互に矛盾せず、そしてタスクを実行するときに他のエンティティを助ける特性を保有していることを示す。すべての個々のエンティティがそのグループの他のエンティティを直接サポートすることを決定する必要はない。むしろ、行われるのは、より一般的な決定である。

証明する(Prove) ― これは、数学的な意味で形式的な分析を意味する。これは、すべての面で完全に厳格である。一般的に、「証明する」は、高いレベルの厳格性において **2** つの **TSF** 表現の間の対応を示したいときに使用される。

特定する(Specify) ― この用語は、「記述する」と同じ文脈で使用されるが、さらに厳格で正確であることを意図している。「定義する」**(define)**とほとんど同じである。

たどる(Trace)（動詞） ― この用語は、厳格性の最小レベルで **2** つのエンティティの間で非形式的対応が必要なことを示すために使用される。

検証する(Verify) ― この用語は、文脈において「確認する」と同様であるが、さらに厳格な意味合いを持つ。評価者のアクションの文脈でこの用語が使用されるときは、評価者に独立の労力を要求することを示す。

2.5 保証の分類

保証クラス、ファミリ、及び各ファミリの省略名を表 **2.1** に示す。

2.6 保証クラス及びファミリの概要

以下に第 **8** 章から第 **14** 章の保証クラスとファミリを要約する。これらのクラスとファミリの要約は、第 **8** 章から第 **14** 章に現れるのと同じ順に記載されている。

保証クラス	保証ファミリ	省略名
ACMクラス：構成管理	CM 自動化	ACM_AUT
	CM 能力	ACM_CAP
	CM 範囲	ACM_SCP
ADOクラス：配付と運用	配付	ADO_DEL
	設置、生成、及び立上げ	ADO_IGS
ADVクラス：開発	機能仕様	ADV_FSP
	上位レベル設計	ADV_HLD
	実装表現	ADV_IMP
	TSF内部構造	ADV_INT
	下位レベル設計	ADV_LLD
	表現対応	ADV_RCR
	セキュリティ方針モデル化	ADV_SPM
AGDクラス：ガイダンス文書	管理者ガイダンス	ADG_ADM
	利用者ガイダンス	ADG_USR
ALCクラス：ライフサイクルサポート	開発セキュリティ	ALC_DVS
	欠陥修正	ALC_FLR
	ライフサイクル定義	ALC_LCD
	ツールと技法	ALC_TAT
ATEクラス：テスト	カバレージ	ATE_COV
	深さ	ATE_DPT
	機能テスト	ATE_FUN
	独立テスト	ATE_IND
AVAクラス：脆弱性評定	隠れチャネル分析	AVA_CCA
	誤使用	AVA_MSU
	TOEセキュリティ機能強度	AVA_SOF
	脆弱性分析	AVA_VLA

表 2.1 ― 保証ファミリの内訳と対応

2.6.1 ACM クラス：構成管理

構成管理（**CM**）は、**TOE** 及びその他の関係する情報の改良と修正のプロセスにおいて、統制と管理を要求することにより、**TOE** の完全性が保たれるのを助ける。構成管理は、**TOE** の許可されない修正、追加、または排除を防止し、評価に使用される **TOE** と証拠資料が、配付のため

に準備されたものであることを保証する。

2.6.1.1 CM 自動化（ACM_AUT）

構成管理の自動化は、構成要素を管理するために使用される自動化のレベルを確立する。

2.6.1.2 CM 能力（ACM_CAP）

構成管理能力は、構成管理システムの特徴を定義する。

2.6.1.3 CM 範囲（ACM_SCP）

構成管理範囲は、構成管理システムが管理する必要がある **TOE** 項目を示す。

2.6.2 ADO クラス：配付と運用

保証クラス **ADO** は、**TOE** のセキュアな配付、設置、及び運用上の使用に関する手段、手順、及び標準に対する要件を定義し、**TOE** が提供するセキュリティ保護が転送、設置、立上げ、及び運用中に危険にさらされないようにする。

2.6.2.1 配付（ADO_DEL）

配付は、最初の配付とその後の一部の修正の両方において、利用者への **TOE** の運搬中にセキュリティを維持するために使用される手続きを扱う。これには、配付される **TOE** の信頼性を示すための特別の手続きまたは操作が含まれる。そのような手続きと手段は、**TOE** が提供するセキュリティのための保護が運搬中に何ら危害が加えられなかったことを確認するための根拠となる。配付要件に従うことは、必ずしも **TOE** が評価されるときに決定されないが、**TOE** を利用者に配送するために開発者が開発した手続きを評価することは可能である。

2.6.2.2 設置、生成、及び立上げ（ADO_IGS）

設置、生成、及び立上げは、**TOE** のマスタコピーと同一の保護特性を示すために、管理者が **TOE** のコピーを設定し、稼動することを要求する。設置、生成、及び立上げ手順は、管理者が **TOE** 設定パラメタとそれらが **TSF** へどのように影響するかを理解するという確信を提供する。

2.6.3 ADV クラス：開発

保証クラス **ADV** は、**ST** の **TOE** 要約仕様から実際の実装までの **TSF** の手順ごとの詳細化の要件を定義する。その結果の各 **TSF** 表現は、**TOE** の機能要件が満たされているかどうかを評価者が決定するのを助ける情報を提供する。

2.6.3.1 機能仕様（ADV_FSP）

機能仕様は、**TSF** を記述し、**TOE** セキュリティ機能要件を完全で正確にな具象化したものでなければならない。機能仕様は、**TOE** への外部インタフェースの詳細も示す。**TOE** の利用者は、このインタフェースを通して **TSF** と対話することが期待される。

2.6.3.2 上位レベル設計（ADV_HLD）

上位レベル設計は、**TSF** 機能仕様を **TSF** の主要な構成部分に詳細化する最上位レベル設計仕様

である。上位レベル設計は、**TSF** の基本構造と主要なハードウェア、ファームウェア、及びソフトウェアエレメントを識別する。

2.6.3.3 実装表現（ADV_IMP）

実装表現は、**TSF** の最も抽象的でない表現である。適切なソースコード、ハードウェア図面などの表現で **TSF** の詳細な内部動作を示す。

2.6.3.4 TSF 内部構造（ADV_INT）

TSF 内部構造要件は、**TSF** の必要な内部構造を詳述する。

2.6.3.5 下位レベル設計（ADV_LLD）

下位レベル設計は、上位レベル設計をプログラム及び/またはハードウェアを作成するための基礎として使用できる詳細レベルへ詳細化する詳細な設計仕様である。

2.6.3.6 表現対応（ADV_RCR）

表現対応は、**TOE** 要約仕様から、提供される最も抽象的でない **TSF** 表現までの、使用可能な **TSF** 表現の、すべての隣接する対の間のマッピングの実証である。

2.6.3.7 セキュリティ方針モデル化（ADV_SPM）

セキュリティ方針モデルは、**TSP** のセキュリティ方針の構造化表現であり、機能仕様が **TSP** のセキュリティ方針に一致し、最終的に **TOE** セキュリティ機能要件に一致していることを保証するために使用される。これは、機能仕様、セキュリティ方針モデル、及びモデル化されたセキュリティ方針の間の対応付けを通して達成される。

2.6.4 AGD クラス：ガイダンス文書

保証クラス **AGD** は、開発者が提供する運用証拠資料の理解の容易性、記述範囲、及び完全性に対する要件を定義する。利用者向けとと管理者向けの **2** 種類の情報を提供するこの証拠資料は、**TOE** のセキュアな運用において重要な要因である。

2.6.4.1 管理者ガイダンス（AGD_ADM）

管理ガイダンスの要件は、環境上の制約を **TOE** の管理者と運用者が理解するのを助ける。管理者ガイダンスは、**TOE** をセキュアな方法で管理し、**TSF** 特権とプロテクション機能を効果的に使用する方法についての詳細で正確な情報を **TOE** 管理者に提供するために、開発者が利用できる主要な手段である。

2.6.4.2 利用者ガイダンス（AGD_USR）

利用者ガイダンスの要件は、利用者がセキュアな方法で **TOE** を運用するのを助ける（例えば、**PP** または **ST** が想定する利用上の制約が明確に説明され、示されなければならない）。利用者ガイダンスは、**TOE** 利用者に **TOE** の保護機能を正確に使用する方法についての必要な背景と特定の情報を提供するために開発者が使用できる主要な手段である。利用者ガイダンスは、**2** つのことを行わなければならない。第一に、利用者に見えているセキュリティ機能が何を行い、それ

らがどのように使用されるかを説明し、利用者が情報を一貫性があり効率的な方法で保護できるようにする必要がある。第二に、**TOE** のセキュリティを維持する上での利用者の役割を説明する必要がある。

2.6.5 ALC クラス：ライフサイクルサポート

保証クラス **ALC** は、欠陥の修正手続きと方針、ツールと技法の正しい使用、開発環境を保護するために使用されるセキュリティ手段など、**TOE** 開発のすべての手続きに対して適切に定義されたライフサイクルモデルを採用することによって保証の要件を定義する。

2.6.5.1 開発セキュリティ（ALC_DVS）

開発セキュリティは、開発環境で使用される物理的、手続き的、人的、及びその他のセキュリティ手段を扱う。これには、開発場所の物理的セキュリティと開発担当者の選任と採用の管理が含まれる。

2.6.5.2 欠陥修正（ALC_FLR）

欠陥修正は、**TOE** が開発者によってサポートされている間は、**TOE** の消費者によって発見された欠陥が追跡され、修正されることを保証する。将来的な欠陥修正要件の遵守については、**TOE** の評価時には決定できないが、開発者が欠陥を追跡、補修し、消費者に補修を配付するために適した手続きと方針であるかを評価することは可能である。

2.6.5.3 ライフサイクル定義（ALC_LCD）

ライフサイクル定義は、開発者が **TOE** を作り出すために使用する工学的実践に開発プロセスと運用サポート要件に識別されている考慮事項とアクティビティが含まれるようにする。セキュリティ分析と証拠の提出が開発プロセスと運用サポートアクティビティの不可欠な要素として規則的に行われるとき、要件と **TOE** との対応の信頼はより大きいものとなる。このコンポーネントは、いずれかの特定の開発プロセスを指示することを意図していない。

2.6.5.4 ツールと技法（ALC_TAT）

ツールと技法は、**TOE** を分析し、実装するために使用される開発ツールを定義する必要性を扱う。開発ツールとそれらのツールの実装に依存するオプションに関する要件が含まれる。

2.6.6 ATE クラス：テスト

保証クラス **ATE** は、**TSF** が **TOE** セキュリティ機能要件を満たすことを実証するテスト要件を記述する。

2.6.6.1 カバレージ（ATE_COV）

カバレージは、開発者が **TOE** に対して行う機能テストの完全性を扱う。**TOE** セキュリティ機能をテストする範囲を示す。

2.6.6.2 深さ（ATE_DPT）

深さは、開発者が **TOE** をテストする詳細レベルを扱う。セキュリティ機能のテストは、**TSF** 表

現の分析から導き出される情報の深さに基づく。

2.6.6.3 機能テスト（ATE_FUN）

機能テストは、**TSF** が **ST** の要件を満たすために必要な特性を示すことを立証する。機能テストは、**TSF** が少なくとも選択された機能コンポーネントの要件を満たすことを保証する。ただし、機能テストは、**TSF** が予期されている以上のことを行わないことを立証しない。このファミリは、開発者が行う機能テストに焦点を当てる。

2.6.6.4 独立テスト（ATE_IND）

独立テストは、開発者以外の者（例えば、第三者）が行わなければならない **TOE** の機能テストの程度を特定する。このファミリは、開発者テストに含まれていないテストを導入することにより、価値を付加する。

2.6.7 AVA クラス：脆弱性評定

保証クラス **AVA** は、悪用可能な脆弱性の識別に対する要件を定義する。特に、**TOE** の構成、運用、誤使用、または不正な構成において導入されるそれらの脆弱性を扱う。

2.6.7.1 隠れチャネル分析（AVA_CCA）

隠れチャネル分析は、意図する **TSP** に違反して悪用できる意図しない通信チャネルを検出し、分析するために行われる。

2.6.7.2 誤使用（AVA_MSU）

誤使用分析は、ガイダンス証拠資料を理解している管理者または利用者が、**TOE** がセキュアでない方法で構成され、運用されていることを合理的に決定できるかどうかを調査する。

2.6.7.3 TOE セキュリティ機能強度（AVA_SOF）

機能強度分析は、確率的または順列的メカニズム（例えば、パスワードまたはハッシュ機能）によって実現される **TOE** セキュリティ機能を扱う。そのような機能をバイパス、非活性化、または破壊できない場合でも、直接攻撃することによりそれらを打ち破ることは可能である。レベルまたは特定の数値尺度がこれらの機能のそれぞれの強度に対して求められる。機能強度分析は、そのような機能がその要求に一致しているかまたはそれを越えているかどうかを決定するために行われる。例えば、パスワードメカニズムの機能強度分析は、パスワードスペースが十分に大きいことを示すことにより、パスワード機能が強度主張を満たしていることを示すことができる。

2.6.7.4 脆弱性分析（AVA_VLA）

脆弱性分析は、開発におけるそれぞれの詳細化の段階で入り込んだ可能性のある欠陥の識別で構成される。以下に関する必要な情報の収集を通して侵入テストが定義される：**(1) TSF** の完全性（**TSF** は、すべての仮定される脅威に対抗するか？）、及び **(2)** すべてのセキュリティ機能の間の依存性。これらの可能性のある脆弱性は、それらが、実際に、**TOE** のセキュリティを損なうために悪用可能であるかどうかを決定するための侵入テストを通して評価される。

2.7 維持の分類

保証維持要件は、保証クラスとして取り扱われ、上記に定義されているクラス構造を使用して提示される。

保証維持ファミリ、及び各ファミリの省略名を表 **2.2** に示す。

保証クラス	保証ファミリ	省略名
ＡＭＡクラス：保証維持	保証維持計画	AMA_AMP
	TOEコンポーネント分類報告	AMA_CAT
	保証維持の証拠	AMA_EVD
	セキュリティ影響分析	AMA_SIA

表 2.2 ― 保証維持クラスのコンポーネント構成

2.8 保証クラスとファミリの維持の概要

以下に第 **16** 章の保証クラスとファミリの要約を示す。クラスとファミリの要約は、それらが第 **16** 章に現れるのと同じ順に記載されている。

2.8.1 AMA クラス：保証維持

保証クラス **AMA** は、**TOE** またはその環境が変更されても、**TOE** が継続的にそのセキュリティターゲットを達成し続ける保証レベルを維持することを目的としている。このクラスの各ファミリは、**TOE** の評価が成功した後に適用される開発者と評価者のアクションを識別する。ただし、いくつかの要件は、評価時に適用することもできる。

2.8.1.1 保証維持計画（AMA_AMP）

保証維持計画は、**TOE** またはその環境に変更が行われるときに、評価された **TOE** に確立された保証が維持されるように、開発者が実施する計画と手続きを識別する。

2.8.1.2 TOE コンポーネント分類報告（AMA_CAT）

TOE コンポーネント分類報告は、セキュリティへの関連性に従って、**TOE** のコンポーネント（例えば、**TSF** サブシステム）を分類する。この分類は、開発者がセキュリティ影響分析を行うための焦点となる。

2.8.1.3 保証維持の証拠（AMA_EVD）

保証維持の証拠は、**TOE** の保証が保証維持計画に従って開発者によって維持されていることの

確信をもたらすことを求める。

2.8.1.4 セキュリティ影響分析（AMA_SIA）

セキュリティ影響分析は、**TOE** が評価された後に、開発者が行った **TOE** に影響を及ぼすすべての変更に関するセキュリティ影響の分析を通して、**TOE** における保証が維持されているという確信をもたらすことを求める。

3　プロテクションプロファイル及びセキュリティターゲット評価基準

3.1　概要

この章では、**PP** と **ST** の評価基準を紹介する。評価基準は、第 **4** 章、「**APE** クラス：プロテクションプロファイル評価」及び第 **5** 章、「**ASE** クラス：セキュリティターゲット評価」に詳しく記述されている。

一般的に **PP** 及び **ST** 評価が **TOE** 評価の前に行われるために、これらの基準は、このパートに示されている最初の要件である。それらは、**PP** または **ST** が **TOE** 評価に意味のある基礎となるかどうかを見出すために、**TOE** の評定、及び機能と保証要件の評価に関する情報の中で、特別の役割を果たす。

これらの評価基準は、第 **7** 章から第 **14** 章までの要件とはいくらか異なるが、開発者と評価者のアクティビティは、**PP**、**ST** 及び **TOE** 評価と同等であるために、同様の方法で示されている。

PP 及び **ST** クラスは、**TOE** クラスとは異なり、**PP** または **ST** クラスのすべての要件が **PP** または **ST** 評価に対して考慮される必要がある。一方、**TOE** クラスに示されている要件は、広範囲のトピックを扱っているが、特定の **TOE** にそれらすべてが考慮される必要はない。

PP と **ST** の評価基準は、**CC** パート **1** の附属書 **B** と附属書 **C** に示されている情報に基づく。次の章に示されている **APE** クラスと **ASE** クラスの要件の有用な背景情報が、そこに示されている。

3.2　プロテクションプロファイル基準の概要

3.2.1　プロテクションプロファイルの評価

PP 評価の目標は、**PP** が完全で、一貫性があり、技術的に信頼でき、その結果、１つまたは複数の評価可能な **TOE** に対する要件の記述として使用することに適していることを実証することである。そのような **PP** は、**PP** 登録機関へ登録するのに相応しいものである。

3.2.2　セキュリティターゲット評価基準との関係

CC パート **1** の附属書 **B** と **C** に記述されているように、一般的な **PP** と **TOE** に特有な **ST** の間には構造と内容において多くの類似点がある。その結果、**PP** を評価する基準には、**ST** に対する要件と同様の要件が数多く含まれ、両者に対する基準は、同様の方法で示される。

3.2.3 評価者の作業

3.2.3.1 CC 要件のみに基づく評価のための評価者の作業

標準外要件が含まれていない **PP** の評価を行う評価者は、表 **3.1** に記述されている **APE** クラスの要件を適用しなければならない。

クラス	ファミリ	省略名
APEクラス：プロテクションプロファイルの評価	プロテクションプロファイル、TOE記述	APE_DES
	プロテクションプロファイル、セキュリティ環境	APE_ENV
	プロテクションプロファイル、PP概説	APE_INT
	プロテクションプロファイル、セキュリティ対策方針	APE_OBJ
	プロテクションプロファイル、ITセキュリティ要件	APE_REQ

表 3.1 ― プロテクションプロファイルファミリ ― CC 要件のみ

3.2.3.2 CC 拡張評価のための評価者の作業

標準外要件が含まれる **PP** の評価を行う評価者は、表 **3.2** に記述されている **APE** クラスの要件を適用しなければならない。

クラス	ファミリ	省略名
APEクラス：プロテクションプロファイルの評価	プロテクションプロファイル、TOE記述	APE_DES
	プロテクションプロファイル、セキュリティ環境	APE_ENV
	プロテクションプロファイル、PP概説	APE_INT
	プロテクションプロファイル、セキュリティ対策方針	APE_OBJ
	プロテクションプロファイル、ITセキュリティ要件	APE_REQ
	プロテクションプロファイル、明示されたITセキュリティ要件	APE_SRE

表 3.2 ― プロテクションプロファイルファミリ ― CC 拡張要件

3.3 セキュリティターゲット基準の概要

3.3.1 セキュリティターゲット評価

ST 評価の目標は、**ST** が完全で、一貫性があり、技術的に信頼でき、その結果、対応する **TOE** の評価の基礎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。

3.3.2 パート３の他の評価基準との関係

TOE の評価には、**ST** 評価及び対応する **TOE** 評価の **2** つの識別された段階が存在する。**ST** 評価の要件については、この章と第 **6** 章で説明するが、**TOE** 評価の要件は、第 **7** 章から第 **14** 章に示されている。

ST 評価には **PP** 主張の評価が含まれる。**ST** が **PP** への適合を主張しない場合、**ST** の **PP** 主張部分には、**TOE** がいずれの **PP** にも適合していないという記述を含めなければならない。

3.3.3 評価者の作業

3.3.3.1 CC 要件のみに基づく評価のための評価者の作業

標準外要件が含まれていない **ST** の評価を行う評価者は、表 **3.3** に記述されている **ASE** クラスの要件を適用しなければならない。

クラス	ファミリ	省略名
ASEクラス：セキュリティターゲット評価	セキュリティターゲット、TOE記述	ASE_DES
	セキュリティターゲット、セキュリティ環境	ASE_ENV
	セキュリティターゲット、ST概説	ASE_INT
	セキュリティターゲット、セキュリティ対策方針	ASE_OBJ
	セキュリティターゲット、PP主張	ASE_PPC
	セキュリティターゲット、ITセキュリティ要件	ASE_REQ
	セキュリティターゲット、TOE要約仕様	ASE_TSS

表 3.3 － セキュリティターゲットファミリ － CC 要件のみ

3.3.3.2 CC 拡張評価のための評価者の作業

標準外要件が含まれる **ST** の評価を行う評価者は、表 **3.4** に記述されている **ASE** クラスの要件を適用しなければならない。

クラス	ファミリ	省略名
ASEクラス：セキュリティターゲット評価	セキュリティターゲット、TOE記述	ASE_DES
	セキュリティターゲット、セキュリティ環境	ASE_ENV
	セキュリティターゲット、ST概説	ASE_INT
	セキュリティターゲット、セキュリティ対策方針	ASE_OBJ
	セキュリティターゲット、PP主張	ASE_PPC
	セキュリティターゲット、ITセキュリティ要件	ASE_REQ
	セキュリティターゲット、明示されたITセキュリティ要件	ASE_SRE
	セキュリティターゲット、TOE要約仕様	ASE_TSS

表 3.4 － セキュリティターゲットファミリ － CC 拡張要件

4　APEクラス：プロテクションプロファイル評価

PP 評価の目標は、**PP** が完全で、一貫性があり、技術的に信頼できることを実証することである。評価された **PP** は、**ST** の開発の基礎として使用できる。そのような **PP** は、登録機関へ登録するのに相応しいものである。

図 **4.1** は、このクラスの中のファミリを示す。

図 4.1 ― プロテクションプロファイル評価クラスのコンポーネント構成

4.1　TOE記述（APE_DES）

目的

TOE 記述は、**TOE** のセキュリティ要件の理解を助ける。**TOE** 記述の評価は、**TOE** 記述が理路整然としていて、内部的な一貫性、**PP** の他のすべての部分との一貫性があることを示す必要がある。

APE_DES.1　プロテクションプロファイル、TOE 記述、評価要件

依存性：

APE_ENV.1　プロテクションプロファイル、セキュリティ環境、評価要件
APE_INT.1　プロテクションプロファイル、**PP** 概説、評価要件
APE_OBJ.1　プロテクションプロファイル、セキュリティ対策方針、評価要件
APE_REQ.1　プロテクションプロファイル、**IT** セキュリティ要件、評価要件

開発者アクションエレメント：

APE_DES.1.1D　**PP**開発者は、**PP**の一部として**TOE**記述を提供しなければならない。

証拠の内容・提示エレメント：

APE_DES.1.1C　**TOE**記述は、少なくとも製品の種別と**TOE**の概括的な**IT**機能を記述しなければならない。

評価者アクションエレメント：

APE_DES.1.1E　評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

APE_DES.1.2E　評価者は、**TOE**記述が理路整然としていて内部的な一貫性があることを確認しなければならない。

APE_DES.1.3E　評価者は、**TOE**記述が**PP**の他の部分との一貫性があることを確認しなければならない。

4.2　セキュリティ環境（APE_ENV）

目的

PP の **IT** セキュリティ要件が十分であるかどうかを決定するには、解決すべきセキュリティ問題をすべての評価者が明確に理解することが重要である。

APE_ENV.1　プロテクションプロファイル、セキュリティ環境、評価要件

依存性： なし

開発者アクションエレメント：

APE_ENV.1.1D　**PP開発者は、PPの一部としてTOEセキュリティ環境の記述を提供しなければならない。**

証拠の内容・提示エレメント：

APE_ENV.1.1C　**TOEセキュリティ環境の記述は、TOEの意図する使用とTOEの使用環境についてのあらゆる前提条件を識別し、説明しなければならない。**

APE_ENV.1.2C　**TOEセキュリティ環境の記述は、TOEまたはその環境のいずれかによる保護が必要な資産に対する、判明しているまたは想定されるあらゆる脅威を識別し、説明しなければならない。**

APE_ENV.1.3C　**TOEセキュリティ環境の記述は、TOEが従うべきあらゆる組織のセキュリティ方針を識別し、説明しなければならない。**

評価者アクションエレメント：

APE_ENV.1.1E　**評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

APE_ENV.1.2E　**評価者は、TOEセキュリティ環境の記述が理路整然としていて、内部的に一貫性があることを確認しなければならない。**

4.3 PP概説（APE_INT）

目的

PP 概説には、**PP** 登録機関を運用するために必要な文書管理と概要の情報が含まれる。**PP** 概説の評価は、**PP** が正しく識別され、**PP** の他のすべての部分と一貫性があることを示すために必要である。

APE_INT.1 プロテクションプロファイル、PP 概説、評価要件

依存性：

APE_DES.1 プロテクションプロファイル、**TOE** 記述、評価要件
APE_ENV.1 プロテクションプロファイル、セキュリティ環境、評価要件
APE_OBJ.1 プロテクションプロファイル、セキュリティ対策方針、評価要件
APE_REQ.1 プロテクションプロファイル、**IT** セキュリティ要件、評価要件

開発者アクションエレメント：

APE_INT.1.1D **PP開発者は、PPの一部としてPP概説を提供しなければならない。**

証拠の内容・提示エレメント：

APE_INT.1.1C **PP概説には、PPを識別、カタログ、登録、及び相互参照するために必要となるラベル情報と記述情報を提供するPP識別が含まれなければならない。**

APE_INT.1.2C **PP概説には、PPを叙述的形式で要約しているPP概要が含まれなければならない。**

評価者アクションエレメント：

APE_INT.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

APE_INT.1.2E **評価者は、PP概説が理路整然としていて、内部的に一貫性があることを確認しなければならない。**

APE_INT.1.3E **評価者は、PP概説がPPの他の部分と一貫性があることを確認しなければならない。**

4.4　セキュリティ対策方針（APE_OBJ）

目的

セキュリティ対策方針は、セキュリティの問題に対する意図する対応の簡潔な記述である。セキュリティ対策方針の評価は、記述されている対策方針がセキュリティの問題に適切に対処していることを実証する必要がある。セキュリティ対策方針は、**TOE** に対するセキュリティ対策方針と、環境に対するセキュリティ対策方針に分類される。**TOE** に対するセキュリティ対策方針と環境に対するセキュリティ対策方針は、対抗すべき識別された脅威、及び/またはそれぞれが従うべき方針と前提条件にまでさかのぼられることが示されなければならない。

APE_OBJ.1　プロテクションプロファイル、セキュリティ対策方針、評価要件

依存性：

APE_ENV.1　プロテクションプロファイル、セキュリティ環境、評価要件

開発者アクションエレメント：

APE_OBJ.1.1D　PP開発者は、PPの一部としてセキュリティ対策方針の記述を提供しなければならない。

APE_OBJ.1.2D　PP開発者は、セキュリティ対策方針根拠を提供しなければならない。

証拠の内容・提示エレメント：

APE_OBJ.1.1C　セキュリティ対策方針の記述は、TOEとその環境に対するセキュリティ対策方針を定義しなければならない。

APE_OBJ.1.2C　TOEのセキュリティ対策方針は、明確に記述され、TOEが対抗する識別された脅威の側面、及び/またはTOEが従う組織のセキュリティ方針にまでさかのぼられなければならない。

APE_OBJ.1.3C　環境のセキュリティ対策方針は、明確に記述され、TOEが完全には対抗しない識別された脅威の側面、及び/またはTOEが完全には従わない組織のセキュリティ方針または前提条件にまでさかのぼられなければならない。

APE_OBJ.1.4C　セキュリティ対策方針根拠は、記述されているセキュリティ対策方針が、セ

キュリティに対する識別された脅威に対抗するのに適していることを実証しなければならない。

APE_OBJ.1.5C **セキュリティ対策方針根拠は、記述されているセキュリティ対策方針が識別されている組織のセキュリティ方針と前提条件のすべてをカバーするのに適していることを実証しなければならない。**

評価者アクションエレメント：

APE_OBJ.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

APE_OBJ.1.2E **評価者は、セキュリティ対策方針の記述が完全であり、理路整然としていて、内部的に一貫性があることを確認しなければならない。**

4.5　ITセキュリティ要件（APE_REQ）

目的

TOE に対して選択され、**PP** に提示または引用されている **IT** セキュリティ要件は、それらが、内部的に一貫性があり、セキュリティ対策方針を達成する **TOE** の開発を導くものであることを確認するために、評価されなければならない。

PP に表されているセキュリティ対策方針は、適合する **TOE** により必ずしもすべて満たされるとは限らない。それは、いくつかの **TOE** は、**IT** 環境によって満たされるある種の **IT** セキュリティ要件に依存することがあるためである。この場合、環境 **IT** セキュリティ要件は、明確に記述され、**TOE** 要件との関係において評価されなければならない。

このファミリは、**PP** が評価可能な **TOE** の要件の記述として使用するのに適していることを、評価者が決定できるようにする評価要件を示す。明示された要件の評価に必要な追加の基準は、**APE_SRE** ファミリで取り扱われる。

適用上の注釈

「**IT** セキュリティ要件」の用語は、「**TOE** セキュリティ要件」及び任意選択として含まれる「**IT** 環境に対するセキュリティ要件」を意味する。

「**TOE** セキュリティ要件」の用語は、「**TOE** セキュリティ機能要件」及び/または「**TOE** セキュリティ保証要件」を意味する。

APE_REQ.1 コンポーネントでは、「適切」**(appropriate)**の用語は、あるエレメントが、ある場合においてオプションが可能であることを示すために使用される。どのようなオプションが適用可能かは、**PP** に示される文脈によって異なる。これらすべての側面に関する詳細情報は、**CC** パート **1** の附属書 **B** に記述されている。

APE_REQ.1　プロテクションプロファイル、IT セキュリティ要件、評価要件

依存性：

APE_OBJ.1　プロテクションプロファイル、セキュリティ対策方針、評価要件

開発者アクションエレメント：

APE_REQ.1.1D **PP開発者は、PPの一部としてITセキュリティ要件の記述を提供しなければならない。**

APE_REQ.1.2D **PP開発者は、セキュリティ要件根拠を提供しなければならない。**

証拠の内容・提示エレメント：

APE_REQ.1.1C **TOEセキュリティ機能要件の記述は、CCパート2の機能要件コンポーネントから引き出されたTOEセキュリティ機能要件を識別しなければならない。**

APE_REQ.1.2C **TOEセキュリティ保証要件の記述は、CCパート3の保証要件コンポーネントから引き出されたTOEセキュリティ保証要件を識別しなければならない。**

APE_REQ.1.3C **TOEセキュリティ保証要件の記述には、CCパート3に定義されている評価保証レベル（EAL）を１つ含めなければならない。**

APE_REQ.1.4C **証拠は、TOEセキュリティ保証要件の記述が適切であることを正当化しなければならない。**

APE_REQ.1.5C **PPは、もし適切なら、IT環境に対するセキュリティ要件を識別しなければならない。**

APE_REQ.1.6C **PPに含まれるITセキュリティ要件に対するすべての完了した操作が識別されなければならない。**

APE_REQ.1.7C **PPに含まれるITセキュリティ要件に対する未完了の操作が識別されなければならない。**

APE_REQ.1.8C **PPに含まれているITセキュリティ要件の間の依存性が満たされなければならない。**

APE_REQ.1.9C **証拠は、依存性が満たされないことが適切であることの理由を正当化しなければならない。**

APE_REQ.1.10C **PPには、SOF-基本、SOF-中位、またはSOF-高位のいずれかを適切なものとして、TOEセキュリティ機能要件に対する最小機能強度レベルの記述が含まれなければならない。**

APE_REQ.1.11C **PPは、明示された機能強度が適切であるあらゆる特定のTOEセキュリティ機**

能要件を、特定の数値尺度と共に識別しなければならない。

APE_REQ.1.12C セキュリティ要件根拠は、PPの最小機能強度レベルが、明示された機能強度主張と共に、TOEのセキュリティ対策方針と一貫していることを実証しなければならない。

APE_REQ.1.13C セキュリティ要件根拠は、ITセキュリティ要件がセキュリティ対策方針を達成するのに適していることを実証しなければならない。

APE_REQ.1.14C セキュリティ要件根拠は、ITセキュリティ要件のセットが一体となって相互にサポートし、内部的に一貫性がある全体を形成することを実証しなければならない。

評価者アクションエレメント：

APE_REQ.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

APE_REQ.1.2E 評価者は、ITセキュリティ要件の記述が完全で、理路整然としていて、内部的に一貫性があることを確認しなければならない。

4.6　明示されたITセキュリティ要件（APE_SRE）

目的

慎重に考慮した結果、**CC** パート **2** または **CC** パート **3** のいずれの要件コンポーネントも **IT** セキュリティ要件の全体またはその一部に直ちに適用できない場合、**PP** の作成者は、**CC** を参照しない別の要件を記述できる。そのような要件の使用は、正当化されなければならない。

このファミリは、明示された要件が明確に、曖昧さなく表現されていることを評価者が決定できるようにする評価要件を示す。正当な明示されたセキュリティ要件と連携した、**CC** から取り出された要件の評価は、**APE_REQ** ファミリによって取り扱われる。

PP に提示または引用された **TOE** に対する、明示された **IT** セキュリティ要件は、それらが明確に、曖昧さなく表現されていることを実証するために、評価する必要がある。

適用上の注釈

既存の **CC** コンポーネントとエレメントの要件と同様の構造にて、明示された要件の系統的な記述には、同様のラベル付け、表現方法、及び詳細レベルの選択が含まれる。

モデルとして **CC** 要件を使用することは、要件が明確に識別できること、要件が自己完結していること、各要件の適用が可能であり、その特定の要件に対する **TOE** の適合記述に基づく意味ある評価結果が得られることを意味する。

「**IT** セキュリティ要件」の用語は、「**TOE** セキュリティ要件」及び任意選択として含まれる「**IT** 環境のセキュリティ要件」を意味する。

「**TOE** セキュリティ要件」の用語は、「**TOE** セキュリティ機能要件」及び/または「**TOE** セキュリティ保証要件」を意味する。

APE_SRE.1　プロテクションプロファイル、明示された IT セキュリティ要件、評価要件

依存性：

APE_REQ.1　プロテクションプロファイル、IT セキュリティ要件、評価要件

開発者アクションエレメント：

APE_SRE.1.1D **PP開発者は、PPの一部としてITセキュリティ要件の記述を提供しなければならない。**

APE_SRE.1.2D **PP開発者は、セキュリティ要件根拠を提供しなければならない。**

証拠の内容・提示エレメント：

APE_SRE.1.1C **CCを参照せずに明示されるすべてのTOEセキュリティ要件は、識別されなければならない。**

APE_SRE.1.2C **CCを参照せずに明示されるIT環境に対するすべてのセキュリティ要件は、識別されなければならない。**

APE_SRE.1.3C **証拠は、セキュリティ要件が明示されなければならない理由を正当化しなければならない。**

APE_SRE.1.4C明示されたITセキュリティ要件は、提示モデルとしてCC要件コンポーネント、ファミリ及びクラスを使用しなければならない。

APE_SRE.1.5C **明示されたITセキュリティ要件は、評価可能でなければならず、TOEの適合または非適合が決定可能であり、系統的に実証することが可能なように客観的な評価要件を記述しなければならない。**

APE_SRE.1.6C **明示されたITセキュリティ要件は、明確に、曖昧さなく表現されなければならない。**

APE_SRE.1.7C **セキュリティ要件根拠は、保証要件が、明示されたTOEセキュリティ機能要件をサポートするために適用可能であり、適していることを実証しなければならない。**

評価者アクションエレメント：

APE_SRE.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

APE_SRE.1.2E **評価者は、明示されたITセキュリティ要件のすべての依存性が識別されていることを決定しなければならない。**

5　ASEクラス：セキュリティターゲット評価

ST 評価の目標は、**ST** が完全で、一貫性があり、技術的に信頼でき、その結果、対応する **TOE** 評価の基礎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。

図 **5.1** は、このクラスのファミリを示す。

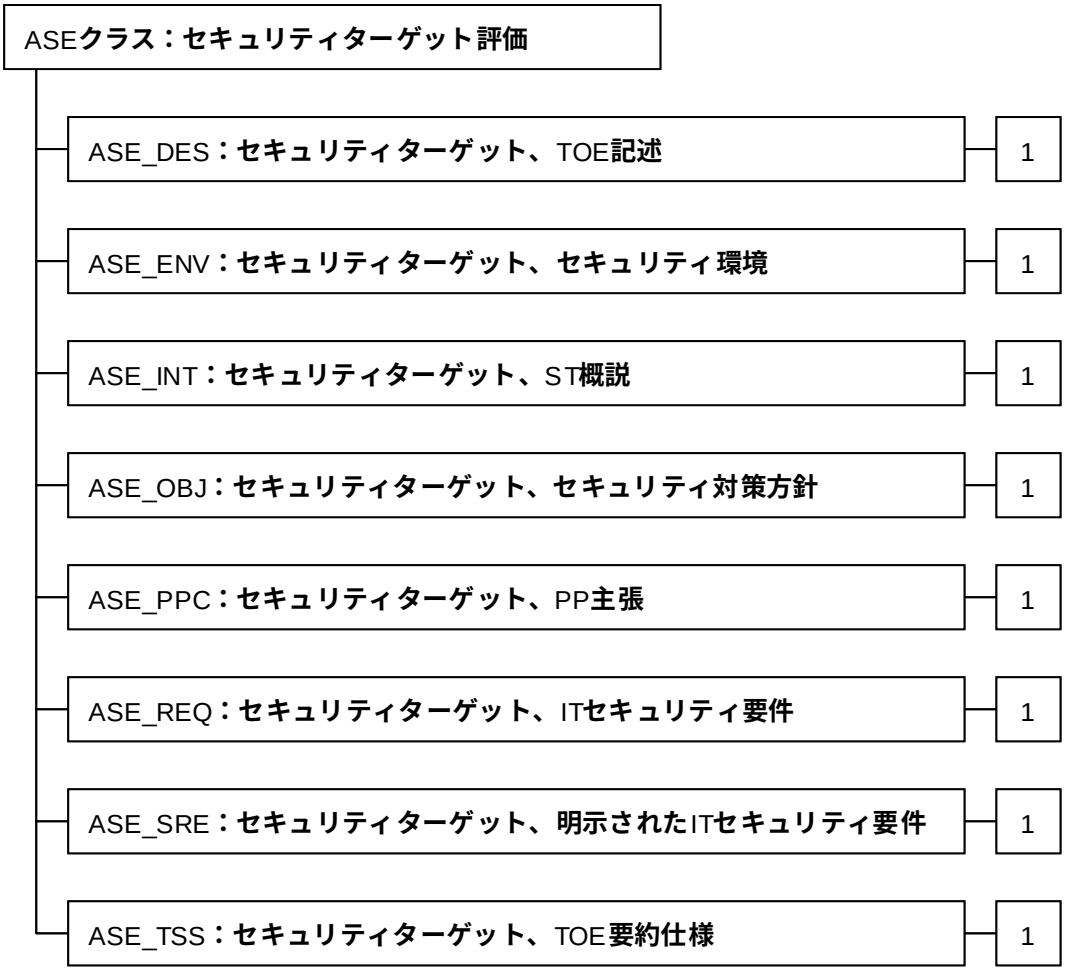

図 5.1 ― セキュリティターゲット評価クラスのコンポーネント構成

5.1　TOE記述（ASE_DES）

目的

TOE 記述は、**TOE** のセキュリティ要件の理解を助ける。**TOE** 記述の評価は、**TOE** 記述に理路整然としていて、内部的な一貫性、**ST** の他のすべての部分との一貫性があることを示す必要がある。

ASE_DES.1　セキュリティターゲット、TOE 記述、評価要件

依存性：

ASE_ENV.1　セキュリティターゲット、セキュリティ環境、評価要件
ASE_INT.1　セキュリティターゲット、ST 概説、評価要件
ASE_OBJ.1　セキュリティターゲット、セキュリティ対策方針、評価要件
ASE_PPC.1　セキュリティターゲット、PP 主張、評価要件
ASE_REQ.1　セキュリティターゲット、IT セキュリティ要件、評価要件
ASE_TSS.1　セキュリティターゲット、TOE 要約仕様、評価要件

開発者アクションエレメント：

ASE_DES.1.1D　開発者は、STの一部としてTOE記述を提供しなければならない。

証拠の内容・提示エレメント：

ASE_DES.1.1C　TOE記述は、少なくとも、物理的及び論理的方法の両方において一般的用語によりTOEの製品またはシステムの種別、適用範囲と境界を記述しなければならない。

評価者アクションエレメント：

ASE_DES.1.1E　評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ASE_DES.1.2E　評価者は、TOE記述が理路整然として、内部的な一貫性があることを確認しなければならない。

ASE_DES.1.3E　評価者は、TOE記述がSTの他の部分との一貫性があることを確認しなければ

ならない。

5.2　セキュリティ環境（ASE_ENV）

目的

ST の **IT** セキュリティ要件が十分であるかどうかを決定するためには、解決すべきセキュリティの問題をすべての評価者が明確に理解することが重要である。

ASE_ENV.1　セキュリティターゲット、セキュリティ環境、評価要件

依存性： なし

開発者アクションエレメント：

ASE_ENV.1.1D　開発者は、**ST**の一部として**TOE**セキュリティ環境の記述を提供しなければならない。

証拠の内容・提示エレメント：

ASE_ENV.1.1C　**TOE**セキュリティ環境の記述は、**TOE**の意図する使用と**TOE**の使用環境についてのあらゆる前提条件を識別し、説明しなければならない。

ASE_ENV.1.2C　**TOE**セキュリティ環境の記述は、**TOE**またはその環境のいずれかによる、保護が必要な資産に対する、判明しているまたは想定されるあらゆる脅威を識別し、説明しなければならない。

ASE_ENV.1.3C　**TOE**セキュリティ環境の記述は、**TOE**が従うべきあらゆる組織のセキュリティ方針を識別し、説明しなければならない。

評価者アクションエレメント：

ASE_ENV.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ASE_ENV.1.2E　評価者は、**TOE**セキュリティ環境の記述が理路整然としていて、内部的に一貫性があることを確認しなければならない。

5.3 ST概説（ASE_INT）

目的

ST 概説には識別情報とインデックス情報が含まれる。**ST** 概説の評価は、**ST** が正しく識別され、**ST** の他のすべての部分と一貫性があることを示すために必要である。

ASE_INT.1 セキュリティターゲット、ST 概説、評価要件

依存性：

ASE_DES.1 セキュリティターゲット、**TOE** 記述、評価要件
ASE_ENV.1 セキュリティターゲット、セキュリティ環境、評価要件
ASE_OBJ.1 セキュリティターゲット、セキュリティ対策方針、評価要件
ASE_PPC.1 セキュリティターゲット、**PP** 主張、評価要件
ASE_REQ.1 セキュリティターゲット、**IT** セキュリティ要件、評価要件
ASE_TSS.1 セキュリティターゲット、**TOE** 要約仕様、評価要件

開発者アクションエレメント：

ASE_INT.1.1D 開発者は、STの一部としてST概説を提供しなければならない。

証拠の内容・提示エレメント：

ASE_INT.1.1C ST概説には、ST及びそれが参照するTOEを管理、識別するために必要となるラベル情報と記述情報を提供するST識別が含まれなければならない。

ASE_INT.1.2C ST概説には、STを叙述的形式で要約しているST概要が含まれなければならない。

ASE_INT.1.3C ST概説には、TOEに対するCC適合の評価可能な主張を記述したCC適合主張が含まれなければならない。

評価者アクションエレメント：

ASE_INT.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ASE_INT.1.2E 評価者は、ST概説が理路整然としていて、内部的に一貫性があることを確認しなければならない。

ASE_INT.1.3E　評価者は、ST概説がSTの他の部分と一貫性があることを確認しなければならない。

5.4　セキュリティ対策方針（ASE_OBJ）

目的

セキュリティ対策方針は、セキュリティの問題に対する意図する対応の簡潔な記述である。セキュリティ対策方針の評価は、記述されている対策方針がセキュリティの問題に適切に対処していることを実証する必要がある。セキュリティ対策方針は、**TOE** に対するセキュリティ対策方針と、環境に対するセキュリティ対策方針に分類される。**TOE** に対するセキュリティ対策方針と環境に対するセキュリティ対策方針は、対抗すべき識別された脅威、及び/またはそれぞれが従うべき方針と前提条件にまでさかのぼられることが示されなければならない。

ASE_OBJ.1　セキュリティターゲット、セキュリティ対策方針、評価要件

依存性：

ASE_ENV.1　セキュリティターゲット、セキュリティ環境、評価要件

開発者アクションエレメント：

ASE_OBJ.1.1D　**開発者は、STの一部としてセキュリティ対策方針の記述を提供しなければならない。**

ASE_OBJ.1.2D　**開発者は、セキュリティ対策方針根拠を提供しなければならない。**

証拠の内容・提示エレメント：

ASE_OBJ.1.1C　**セキュリティ対策方針の記述は、TOEとその環境に対するセキュリティ対策方針を定義しなければならない。**

ASE_OBJ.1.2C　**TOEのセキュリティ対策方針は、明確に記述され、TOEが対抗する識別された脅威の側面、及び/またはTOEが従う組織のセキュリティ方針にまでさかのぼられなければならない。**

ASE_OBJ.1.3C　**環境のセキュリティ対策方針は、明確に記述され、TOEが完全には対抗しない識別された脅威の側面、及び/またはTOEが完全には従わない組織のセキュリティ方針または前提条件にまでさかのぼられなければならない。**

ASE_OBJ.1.4C **セキュリティ対策方針根拠は、記述されているセキュリティ対策方針が、セキュリティに対する識別された脅威に対抗するのに適していることを実証しなければならない。**

ASE_OBJ.1.5C **セキュリティ対策方針根拠は、記述されているセキュリティ対策方針が識別されている組織のセキュリティ方針と前提条件のすべてを扱うのに適していることを実証しなければならない。**

評価者アクションエレメント：

ASE_OBJ.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

ASE_OBJ1.2E **評価者は、セキュリティ対策方針の記述が完全であり、理路整然としていて、内部的に一貫性があることを確認しなければならない。**

5.5　PP主張（ASE_PPC）

目的

セキュリティターゲット **PP** 主張の評価の目的は、**ST** が **PP** の正確に具象化したものであるかどうかを決定することである。

適用上の注釈

このファミリは、**PP** 主張がある場合にのみ適用される。その他の場合、開発者のアクションと評価者のアクションは必要ない。

PP 主張が行われるとき追加の評価アクティビティが必要となるが、**ST** 評価の労力は、**PP** 評価結果を **ST** 評価に再使用できるために、**PP** が使用されない場合よりも一般的に小さくなる。

ASE_PPC.1　セキュリティターゲット、PP 主張、評価要件

依存性：

ASE_OBJ.1　セキュリティターゲット、セキュリティ対策方針、評価要件
ASE_REQ.1　セキュリティターゲット、IT セキュリティ要件、評価要件

開発者アクションエレメント：

ASE_PPC.1.1D　開発者は、STの一部としてPP主張を提供しなければならない。

ASE_PPC.1.2D　開発者は、それぞれの提供されたPP主張に対してPP主張根拠を提供しなければならない。

証拠の内容・提示エレメント：

ASE_PPC.1.1C　各PP主張は、適合が主張されているPPを、その主張に必要とされる適性を含めて識別しなければならない。

ASE_PPC.1.2C　各PP主張は、PPの許可された操作を満たしているか、そうでなければPP要件をさらに適正化するようなITセキュリティ要件の記述を識別しなければならない。

ASE_PPC.1.3C　各PP主張は、PPに含まれているものに加え、STに含まれているセキュリティ

対策方針とITセキュリティ要件の記述を識別しなければならない。

評価者アクションエレメント：

ASE_PPC.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ASE_PPC.1.2E　評価者は、PP主張がPPを正確に具象化したものであることを確認しなければならない。

5.6　ITセキュリティ要件（ASE_REQ）

目的

TOE に対して選択され、**ST** に提示または引用されている **IT** セキュリティ要件は、それらが内部的に一貫性があり、セキュリティ対策方針を達成する **TOE** の開発を導くものであることを確認するために、評価されなければならない。

このファミリは、**ST** が対応する **TOE** に対する要件の記述として使用するのに適していることを、評価者が決定できるようにする評価要件を示す。明示された要件の評価に必要な追加の基準は、**ASE_SRE** ファミリで取り扱われる。

適用上の注釈

「**IT** セキュリティ要件」の用語は、「**TOE** セキュリティ要件」及び任意選択として含まれる「**IT** 環境に対するセキュリティ要件」を意味する。

「**TOE** セキュリティ要件」の用語は、「**TOE** セキュリティ機能要件」及び/または「**TOE** セキュリティ保証要件」を意味する。

ASE_REQ.1 コンポーネントでは、「適切」**(appropriate)**の用語は、あるエレメントが、ある場合においてオプションが可能であることを示すために使用される。どのようなオプションが適用可能かは、**ST** に示される文脈によって異なる。これらすべての側面に関する詳細情報は、**CC** パート **1** の附属書 **C** に含まれている。

ASE_REQ.1　セキュリティターゲット、IT セキュリティ要件、評価要件

依存性：

ASE_OBJ.1　セキュリティターゲット、セキュリティ対策方針、評価要件

開発者アクションエレメント：

ASE_REQ.1.1D　開発者は、STの一部としてITセキュリティ要件の記述を提供しなければならない。

ASE_REQ.1.2D　開発者は、セキュリティ要件根拠を提供しなければならない。

証拠の内容・提示エレメント：

ASE_REQ.1.1C **TOEセキュリティ機能要件の記述は、CCパート2の機能要件コンポーネントから引き出されたTOEセキュリティ機能要件を識別しなければならない。**

ASE_REQ.1.2C **TOEセキュリティ保証要件の記述は、CCパート3の保証要件コンポーネントから引き出されたTOEセキュリティ保証要件を識別しなければならない。**

ASE_REQ.1.3C **TOEセキュリティ保証要件の記述には、CCパート3に定義されている評価保証レベル（EAL）を１つ含めなければならない。**

ASE_REQ.1.4C **証拠は、TOEセキュリティ保証要件の記述が適切であることを正当化しなければならない。**

ASE_REQ.1.5C **STは、もし適切なら、IT環境に対するセキュリティ要件を識別しなければならない。**

ASE_REQ.1.6C **STに含まれているITセキュリティ要件に対する操作は、識別され、実施されなければならない。**

ASE_REQ.1.7C **STに含まれるITセキュリティ要件の間の依存性は、満たされなければならない。**

ASE_REQ.1.8C **証拠は、依存性が満たされないことが適切であることの理由を正当化しなければならない。**

ASE_REQ.1.9C **STには、SOF-基本、SOF-中位またはSOF-高位のいずれかを適切なものとして、TOEセキュリティ機能要件に対する最小機能強度レベルの記述が含まれなければならない。**

ASE_REQ.1.10C **STは、明示された機能強度が適切であるあらゆる特定のTOEセキュリティ機能要件を、特定の数値尺度と共に識別しなければならない。**

ASE_REQ.1.11C **セキュリティ要件根拠は、STの最小機能強度レベルが、明示された機能強度主張と共に、TOEのセキュリティ対策方針と一貫していることを実証しなければならない。**

ASE_REQ.1.12C **セキュリティ要件根拠は、ITセキュリティ要件がセキュリティ対策方針を達成するのに適していることを実証しなければならない。**

ASE_REQ.1.13C **セキュリティ要件根拠は、ITセキュリティ要件のセットが一体となって相互**

にサポートし、内部的に一貫性がある全体を形成することを実証しなければならない。

評価者アクションエレメント：

ASE_REQ.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

ASE_REQ.1.2E **評価者は、ITセキュリティ要件の記述が完全で、理路整然としていて、内部的に一貫性があることを確認しなければならない。**

5.7　明示されたITセキュリティ要件（ASE_SRE）

目的

慎重に考慮した結果、**CC** パート **2** または **CC** パート **3** のいずれの要件コンポーネントも **IT** セキュリティ要件の全体またはその一部に直ちに適用できない場合、**ST** の作成者は、**CC** を参照しない別の要件を記述できる。そのような要件の使用は、正当化されなければならない。

このファミリは、明示された要件が明確に、曖昧さなく表現されていることを評価者が決定することができるようにする評価要件を示す。正当な明示されたセキュリティ要件と連携した、**CC** から取り出された要件の評価は、**ASE_REQ** ファミリによって取り扱われる。

ST に提示または引用された **TOE** に対する、明示された **IT** セキュリティ要件は、それらが明確に、曖昧さなく表現されていることを実証ために、評価する必要がある。

適用上の注釈

既存の **CC** コンポーネントとエレメントの要件と同等の構造にて、明示された要件の系統的な記述には、同様のラベル付け、表現方法、及び詳細レベルの選択が含まれる。
モデルとして **CC** 要件を使用することは、要件が明確に識別できること、それらが自己完結していること、各要件の適用が可能であり、その特定の要件に対する **TOE** の適合記述に基づく意味ある評価結果が得られることを意味する。

「**IT** セキュリティ要件」の用語は、「**TOE** セキュリティ要件」及び任意選択として含まれる「**IT** 環境のセキュリティ要件」を意味する。

「**TOE** セキュリティ要件」の用語は、「**TOE** セキュリティ機能要件」及び/または「**TOE** セキュリティ保証要件」を意味する。

ASE_SRE.1　セキュリティターゲット、明示された IT セキュリティ要件、評価要件

依存性：

ASE_REQ.1　セキュリティターゲット、IT セキュリティ要件、評価要件

開発者アクションエレメント：

ASE_SRE.1.1D　開発者は、STの一部としてITセキュリティ要件の記述を提供しなければなら

ない。

ASE_SRE_1.2D 開発者は、セキュリティ要件根拠を提供しなければならない。

証拠の内容・提示エレメント：

ASE_SRE.1.1C CCを参照せずに明示されるすべてのTOEセキュリティ要件は、識別されなければならない。

ASE_SRE.1.2C CCを参照せずに明示されるIT環境に対するすべてのセキュリティ要件は、識別されなければならない。

ASE_SRE.1.3C 証拠は、セキュリティ要件が明示されなければならない理由を正当化しなければならない。

ASE_SRE.1.4C明示されたITセキュリティ要件は、提示モデルとしてCC要件コンポーネント、ファミリ及びクラスを使用しなければならない。

ASE_SRE.1.5C 明示されたITセキュリティ要件は、評価可能でなければならず、TOEの適合または非適合が決定可能であり、系統的に実証することが可能なように、客観的な評価要件を記述しなければならない。

ASE_SRE.1.6C 明示されるITセキュリティ要件は、明確に、曖昧さなく表現されなければならない。

ASE_SRE.1.7C セキュリティ要件根拠は、保証要件が、明示されたTOEセキュリティ機能要件をサポートするために適用可能であり、適していることを実証しなければならない。

評価者アクションエレメント：

ASE_SRE.1.1E 評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ASE_SRE.1.2E 評価者は、明示されたITセキュリティ要件のすべての依存性が識別されていることを決定しなければならない。

5.8　TOE要約仕様（ASE_TSS）

目的

TOE 要約仕様は、機能要件を満たすために主張されるセキュリティ機能と保証要件を満たすために取られる保証手段の上位レベルの定義を提供する。

適用上の注釈

IT セキュリティ機能と **TOE** セキュリティ機能要件の関係は、「多数対多数」の関係とすることができる。それにもかかわらず、**TSF** を明確に定義できるためには、各セキュリティ機能は、少なくとも **1** つのセキュリティ要件を満たすことに貢献しなければならない。この条件を満たさないセキュリティ機能は、通常、必要とされるべきでない。ただし、セキュリティ機能が少なくとも **1** つのセキュリティ要件を満たさなければならないと言う条件は、極めて一般的な方法で表現されるので、**TOE** に役立つことが明らかになったすべてのセキュリティ機能は、正当と認められることに注意のこと。

保証手段の記述は、**CC** から取られていない保証要件が **ST** に含まれる場合に特に関連性がある。**ST** の **TOE** セキュリティ保証要件が **CC** 評価保証レベルまたは他の **CC** 保証コンポーネントだけに基づく場合、保証手段は、保証要件が満たされることを示す文書の参照の形で示すことができる。

ASE_TSS.1 コンポーネントでは、「適切」**(appropriate)**の用語は、あるエレメントが、ある場合においてオプション可能であることを示すために使用される。どのようなオプションが適用可能かは、**ST** の特定の文脈によって異なる。これらすべての側面の詳細な情報は、**CC** パート **1** 附属書 **C** に示されている。

ASE_TSS.1　セキュリティターゲット、TOE 要約仕様、評価要件

依存性：

ASE_REQ.1　セキュリティターゲット、IT セキュリティ要件、評価要件

開発者アクションエレメント：

ASE_TSS.1.1D　開発者は、STの一部としてTOE要約仕様を提供しなければならない。

ASE_TSS.1.2D　開発者は、TOE要約仕様根拠を示さなければならない。

証拠の内容・提示エレメント：

ASE_TSS.1.1C **TOE要約仕様は、ITセキュリティ機能とTOE保証手段を記述しなければならない。**

ASE_TSS.1.2C **TOE要約仕様は、ITセキュリティ機能をTOEセキュリティ機能要件にまでたどり、どのITセキュリティ機能がどのTOEセキュリティ機能要件を満たすか、そして各ITセキュリティ機能が少なくとも1つのTOEセキュリティ機能要件を満たすことに貢献していることが分かるようにしなければならない。**

ASE_TSS.1.3C **ITセキュリティ機能は、それらの意図を理解するのに必要な詳細レベルまで非形式的なスタイルで定義されなければならない。**

ASE_TSS.1.4C **STに含まれるセキュリティメカニズムへのすべての参照は、それらに関係のあるセキュリティ機能にまでたどられ、どのセキュリティメカニズムが各機能の実装で使用されているかが分かるようにしなければならない。**

ASE_TSS.1.5C **TOE要約仕様根拠は、ITセキュリティ機能がTOEセキュリティ機能要件を満たすのに適していることを実証しなければならない。**

ASE_TSS.1.6C **TOE要約仕様根拠は、指定されたITセキュリティ機能の組合せがTOEセキュリティ機能要件を満たすように一体となって働くことを実証しなければならない。**

ASE_TSS.1.7C **TOE要約仕様は、保証手段を保証要件にまでたどり、どの手段がどの要件を満たすのに貢献しているかが分かるようにしなければならない。**

ASE_TSS.1.8C **TOE要約仕様根拠は、保証手段がTOEのすべての保証要件を満たすことを実証しなければならない。**

ASE_TSS.1.9C **TOE要約仕様は、適切な確率的または順列的メカニズムによって実現されるすべてのITセキュリティ機能を識別しなければならない。**

ASE_TSS.1.10C **TOE要約仕様は、それが適切な各ITセキュリティ機能に対して、特定の数値尺度として、またはSOF-基本、SOF-中位、SOF-高位のいずれかにより、機能強度の主張を示さなければならない。**

評価者アクションエレメント：

ASE_TSS.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

ASE_TSS.1.2E　評価者は、TOE要約仕様が完全で、理路整然としていて、内部的に一貫性があることを確認しなければならない。

6　評価保証レベル

評価保証レベル（**EAL**）は、得られる保証のレベルと、保証の度合いを取得するためのコスト及び可能性を、バランスさせる段階的な尺度を提供する。**CC** のアプローチは、評価の終了時における **TOE** の保証のコンセプトと、**TOE** の運用使用中のその保証の維持のコンセプトを区別して識別している。

CC パート **3** のファミリとコンポーネントが、必ずしもすべて **EAL** に含まれないことに注意しなければならない。これは、これらが意味のある望ましい保証を提供しないことを意味するものではない。これらのファミリとコンポーネントが、それらが利用される **PP** と **ST** の **EAL** の追加とみなされることが期待される。

6.1　評価保証レベル（EAL）の概要

表 **6.1** は、**EAL** の要約を示している。列は、階層的に並べられた **EAL** のセットに相当し、一方、行は、保証ファミリに相当する。その結果として得られるマトリックスの各数字は、該当する所で特定の保証コンポーネントを識別している。

次の節に概説されているように、**7** つの階層的に並べられた評価保証レベルが **TOE** の保証のレート付けのために **CC** に定義されている。それらは、各 **EAL** がそれより低位のすべての **EAL** よりも多くの保証を表すため階層的に並べられている。**EAL** から **EAL** への保証の増加は、同じ保証ファミリから階層的に上位の保証コンポーネントへの*置換*（つまり、厳格性、適用範囲、及び/または深さを拡大させる）及び他の保証ファミリからの保証コンポーネントの*追加*（つまり、新しい要件を追加する）によって達成される。

これらの **EAL** は、このパート **3** の第 **2** 章に記述されている保証コンポーネントの適切な組合せからなる。さらに正確には、各 **EAL** は、各保証ファミリから **1** つより多くのコンポーネントは含まれず、どのコンポーネントのすべての保証依存性が処置されている。

EAL は、**CC** に定義されているが、保証の他の組合せを表すことも可能である。特に、「追加」**(**augmentation**)**の注記は、**EAL** への保証コンポーネントの追加（**EAL** にまだ含まれていない保証ファミリから）、または保証コンポーネントの置換（同じ保証ファミリの他の階層的に上位の保証コンポーネントによる）を許す。**CC** に定義されている保証構造において、**EAL** は追加されることのみが可能である。「**EAL** は構成する保証コンポーネントを欠く」の注記は、標準では有効な主張として認められない。追加は、それと共に、**EAL** に追加された保証コンポーネントの有効性と追加された重要性を正当化する主張者の側の義務をもたらす。**EAL** は、明示された保証要件によって拡張することもできる。

保証クラス	保証ファミリ	評価保証レベルに基づく保証コンポーネント						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
構成管理	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
配付と運用	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
開発	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
ガイダンス文書	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
ライフサイクルサポート	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
テスト	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
脆弱性評定	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

表 6.1 — 評価保証レベルの要約

6.2 評価保証レベルの詳細

次の節では、**EAL** を定義する。その際、特別の要件とそれらの要件の単調な部分とは、ボールド体を用いることにより差を強調している。

6.2.1 評価保証レベル 1（EAL1）－ 機能テスト

目的

EAL1 は、正しい運用のかなりの信頼が要求されるが、セキュリティへの脅威が重大とみなされないところに適用可能である。個人情報または同様の情報の保護に関して当然の配慮がなされているとの論旨をサポートするために、独立の保証が要求されるところで価値がある。

EAL1 は、仕様に対する独立テスト、提供されたガイダンス証拠資料の調査など、顧客に対して有効な **TOE** の評価を提供する。**EAL1** 評価は、**TOE** の開発者の支援を受けずに、最小の費用でできるものを意図されている。

このレベルの評価は、**TOE** の機能がその証拠資料に対してある程度一貫しており、識別された脅威に対し有効な保護を与える証拠を提供するべきである。

保証コンポーネント

EAL1（表 6.2 を参照）は、セキュリティのふるまいを理解するために、機能とインタフェースの仕様、及びガイダンス証拠資料を使用して、セキュリティ機能の分析により基本レベルの保証を提供する。

分析は、TOE セキュリティ機能の独立テストによってサポートされる。

この EAL は、評価されていない IT 製品またはシステムに比べ、意義のある保証の増加を提供する。

保証クラス	保証コンポーネント
構成管理	ACM_CAP.1 バージョン番号
配付と運用	ADO_IGS.1 設置、生成、及び立上げ手順
開発	ADV_FSP.1 非形式的機能仕様
	ADV_RCR.1 非形式的対応の実証
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
テスト	ATE_IND.1 独立テスト – 準拠

表 6.2 ― EAL1

6.2.2　評価保証レベル 2（EAL2）－ 構造化テスト

目的

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

そこで、**EAL2** は、開発者または利用者が完全な開発記録が簡単に使用可能でない場合に、低レベルから中レベルの独立に保証されたセキュリティを必要とする環境に適用可能である。そのような状態は、従来のシステムの安全性を高めるとき、または開発者へのアクセスが制限されるところで起きる。

保証コンポーネント

EAL2（表 **6.3** を参照）は、セキュリティのふるまいを理解するために、**TOE** の機能とインタフェースの仕様、ガイダンス証拠資料、**及び上位レベル設計**を使用して、セキュリティ機能の分析により保証を提供する。

分析は、**TOE** セキュリティ機能の独立テスト、**機能仕様に基づく開発者テストの証拠、開発者テスト結果の選択的な独立した確認、機能強度分析、明らかな脆弱性（例えば、公知になっているもの）に対する開発者の探索の証拠**によってサポートされる。

また、EAL2 は、TOE の構成リストとセキュアな配付手続きの証拠を通して保証を提供する。

この EAL は、開発者テスト、脆弱性分析、さらに詳細な TOE 仕様に基づく独立テストを要求することにより、EAL1 からの意義のある保証の増加を表す。

保証クラス	保証コンポーネント
構成管理	**ACM_CAP.2 構成要素**
配付と運用	**ADO_DEL.1 配付手続き**
	ADO_IGS.1 **設置、生成、及び立上げ手順**
開発	ADV_FSP.1 **非形式的機能仕様**
	ADV_HLD.1 記述的上位レベル設計
	ADV_RCR.1 **非形式的対応の実証**
ガイダンス文書	AGD_ADM.1 **管理者ガイダンス**
	AGD_USR.1 **利用者ガイダンス**
テスト	**ATE_COV.1 カバレージの証拠**
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立試験 - サンプル
脆弱性評定	**AVA_SOF.1 TOE セキュリティ機能強度評価**
	AVA_VLA.1 開発者脆弱性分析

表 6.3 ー EAL2

6.2.3　評価保証レベル 3（EAL3）－ 方式的テスト、及びチェック

目的

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

EAL3 は、開発者または利用者が中レベルの独立に保証されたセキュリティを必要とし、大幅なリエンジニアリングを必要とせずに、**TOE** とその開発の完全な調査を必要とする状況に適用できる。

保証コンポーネント

EAL3（表 **6.4** を参照）は、セキュリティのふるまいを理解するために、**TOE** の機能とインタフェースの仕様、ガイダンス証拠資料、及び上位レベル設計を使用して、セキュリティ機能の分析により保証を提供する。

分析は、**TOE** セキュリティ機能の独立テスト、機能仕様**と上位レベル設計**に基づく開発者テストの証拠、開発者テスト結果の選択的な独立した確認、機能強度分析、明らかな脆弱性（例えば、公知になっているもの）に対する開発者の探索の証拠によってサポートされる。

また、**EAL3** は、**開発環境管理**、**TOE 構成管理の使用**、及びセキュアな配付手続きの証拠を通して保証を提供する。

この EAL は、セキュリティ機能のさらに完全なテストカバレージ、及び TOE が開発中に改ざんされることがないことをかなり信頼させるメカニズム及び/または手順を要求することにより、EAL2 からの意義のある保証の増加を表す。

保証クラス	保証コンポーネント
構成管理	**ACM_CAP.3 許可の管理**
	ACM_SCP.1 TOE の CM 範囲
配付と運用	ADO_DEL.1 配付手続き
	ADO_IGS.1 設置、生成、及び立上げ手順
開発	ADV_FSP.1 非形式的機能仕様
	ADV_HLD.2 セキュリティ実施上位レベル設計
	ADV_RCR.1 非形式的対応の実証
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
ライフサイクルサポート	**ALC_DVS.1 セキュリティ手段の識別**
テスト	**ATE_COV.2 カバレージの分析**
	ATE_DPT.1 テスト：上位レベル設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
脆弱性評定	**AVA_MSU.1 ガイダンスの検査**
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.1 開発者脆弱性分析

表 6.4 － EAL3

6.2.4　評価保証レベル 4（EAL4）－ 方式的設計、テスト、及びレビュー

目的

EAL4 は、厳格であるが、多くの専門家の知識、スキル、及びその他の資源を必要としない正常な商業的開発習慣に基づいて、有効なセキュリティエンジニアリングから最大の保証を開発者が得られるようにする。**EAL4** は、既存の製品ラインに対し改良することが、経済的に実現可能であると思われる最上位レベルである。

そこで、**EAL4** は、開発者または利用者が従来商品 **TOE** に中レベルから高レベルの独立に保証されたセキュリティを必要とし、追加のセキュリティに特有のエンジニアリングコストを負担する用意ができている状況に適用可能である。

保証コンポーネント

EAL4（表 **6.5** を参照）は、セキュリティのふるまいを理解するために、**TOE** の機能と**完全な**インタフェースの仕様、ガイダンス証拠資料、上位レベルと**下位レベル**の設計、**及び実装のサブセット**を使用して、セキュリティ機能の分析により保証を提供する。**保証は、TOE セキュリティ方針の非形式的モデルを通して、さらに得られる。**

分析は、**TOE** セキュリティ機能の独立テスト、機能仕様と上位レベル設計に基づく開発者テストの証拠、開発者テスト結果の選択的な独立した確認、機能強度分析、脆弱性に対する開発者の探索の証拠、**及び攻撃能力が低い侵入攻撃者に対する抵抗力を実証する独立の脆弱性分析**によってサポートされる。

また、**EAL4** は、開発環境管理、**自動化を含む追加の TOE** 構成管理の使用、及びセキュアな配付手続きの証拠を通して保証を提供する。

この EAL は、さらに多くの設計の記述、実装のサブセット、及び TOE が開発中または配付中に改ざんされないことを信頼させる向上したメカニズム及び/または手順を要求することにより、EAL3 からの意義のある保証の増加を表す。

保証クラス	保証コンポーネント
構成管理	**ACM_AUIT.1 部分的な CM 自動化**
	ACM_CAP.4 生成の支援と受入手続き
	ACM_SCP.2 問題追跡の CM 範囲
配付と運用	**ADO_DEL.2 改変の検出**
	ADO_IGS.1 設置、生成、及び立上げ手順
開発	**ADV_FSP.2 完全に定義された外部インタフェース**
	ADV_HLD.2 セキュリティ実施上位レベル設計
	ADV_IMP.1 TSF の実装のサブセット
	ADV_LLD.1 記述的下位レベル設計
	ADV_RCR.1 非形式的対応の実証
	ADV_SPM.1 非形式的な TOE セキュリティ方針モデル
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
ライフサイクルサポート	**ALC_DVS.1 セキュリティ手段の識別**
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
	ALC_TAT.1 明確に定義された開発ツール
テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト：上位レベル設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
脆弱性評定	**AVA_MSU.2 分析の確認**
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.2 独立脆弱性テスト

表 6.5 ― EAL4

6.2.5　評価保証レベル 5（EAL5）－ 準形式的設計、及びテスト

目的

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

そこで、**EAL5** は、開発者または利用者が計画された開発において独立に保証される上位レベルのセキュリティを必要とし、専門家のセキュリティエンジニアリング技法による非合理的なコストを負担することのない厳格な開発方法を必要とする状況に適用可能である。

保証コンポーネント

EAL5（表 **6.6** を参照）は、セキュリティのふるまいを理解するために、**TOE** の機能と完全なインタフェースの仕様、ガイダンス証拠資料、上位レベルと下位レベルの設計、及び**すべての**実装を使用して、セキュリティ機能の分析により保証を提供する。保証は、**TOE** セキュリティ方針の**形式的**モデル、**及び機能仕様と上位レベル設計の準形式的表現及びそれらの間の対応の準形式的実証**を通して、さらに得られる。また、モジュール化された **TOE** 設計も必要となる。

分析は、**TOE** セキュリティ機能の独立テスト、機能仕様と上位レベル設計**と下位レベル設計**に基づく開発者テストの証拠、開発者テスト結果の選択的な独立した確認、機能強度分析、脆弱性に対する開発者の探索の証拠、及び攻撃能力が**中程度の**侵入攻撃者に対する抵抗力を実証する独立の脆弱性分析によってサポートされる。**また、分析には、開発者の隠れチャネル分析の確認も含まれる。**

また、**EAL5** は、開発環境管理、自動化を含む**包括的な TOE** 構成管理の使用、及びセキュアな配付手続きの証拠を通して保証を提供する。

この EAL は、準形式的設計記述、完全な実装、さらに構造化された（その結果、分析可能な）アーキテクチャ、隠れチャネル分析、及び開発中に TOE が改ざんされることがないことを信頼させる向上したメカニズム及び/または手順を要求することにより、EAL4 からの意義のある保証の増加を表す。

保証クラス	保証コンポーネント
構成管理	ACM_AUIT.1 部分的な CM 自動化
	ACM_CAP.4 生成の支援と受入手続き
	ACM_SCP.3 開発ツールの CM 範囲
配付と運用	ADO_DEL.2 改変の検出
	ADO_IGS.1 設置、生成、及び立上げ手順
開発	**ADV_FSP.3 準形式的機能仕様**
	ADV_HLD.3 準形式的上位レベル設計
	ADV_IMP.2 TSF の実装
	ADV_INT.1 モジュール方式
	ADV_LLD.1 記述的下位レベル設計
	ADV_RCR.2 準形式的対応の実証
	ADV_SPM.3 形式的な TOE セキュリティ方針モデル
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.2 標準化されたライフサイクルモデル
	ALC_TAT.2 実装標準への準拠
テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.2 テスト：下位レベル設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
脆弱性評定	**AVA_CCA.1 隠れチャネル分析**
	AVA_MSU.2 分析の確認
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.3 中程度の抵抗力

表 6.6 ― EAL5

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

目的

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

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

保証コンポーネント

EAL6（表 **6.7** を参照）は、セキュリティのふるまいを理解するために、**TOE** の機能と完全なインタフェースの仕様、ガイダンス証拠資料、上位レベルと下位レベルの設計、及び実装の**構造化表現**を使用して、セキュリティ機能の分析により保証を提供する。保証は、**TOE** セキュリティ方針の形式的モデル、及び機能仕様と上位レベル設計**と下位レベル設計**の準形式的表現及びそれらの間の対応の準形式的実証を通して、さらに得られる。また、モジュール化され、**階層化された TOE** 設計も必要となる。

分析は、**TOE** セキュリティ機能の独立テスト、機能仕様と上位レベル設計と下位レベル設計に基づく開発者テストの証拠、開発者テスト結果の選択的な独立した確認、機能強度分析、脆弱性に対する開発者の探索の証拠、及び攻撃能力が**高い**侵入攻撃者に対する抵抗力を実証する独立の脆弱性分析によってサポートされる。また、分析には、開発者の**系統的**隠れチャネル分析の確認も含まれる。

また、**EAL6** は、**構造化開発プロセス**、開発環境管理、**完全**な自動化を含む包括的 **TOE** 構成管理の使用、及びセキュアな配付手続きの証拠を通して保証を提供する。

この EAL は、さらなる包括的分析、実装の構造的表現、さらなるアーキテクチャ構造（例えば、階層化）、さらに包括的な独立脆弱性分析、系統的隠れチャネル識別、向上した構成管理と開発環境管理を要求することにより、EAL5 からの意義のある保証の増加を表す。

保証クラス	保証コンポーネント
構成管理	**ACM_AUIT.2 完全な CM 自動化**
	ACM_CAP.5 進んだサポート
	ACM_SCP.3 開発ツールの CM 範囲
配付と運用	ADO_DEL.2 改変の検出
	ADO_IGS.1 設置、生成、及び立上げ手順
開発	**ADV_FSP.3 準形式的機能仕様**
	ADV_HLD.4 準形式的上位レベル説明
	ADV_IMP.3 TSF の構造化実装
	ADV_INT.2 複雑さの軽減
	ADV_LLD.2 準形式的な下位レベル設計
	ADV_RCR.2 準形式的な対応の実証
	ADV_SPM.3 形式的な TOE セキュリティ方針モデル
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
ライフサイクルサポート	**ALC_DVS.2 セキュリティ手段の十分性**
	ALC_LCD.2 標準化されたライフサイクルモデル
	ALC_TAT.3 実装標準への準拠－すべての部分
テスト	**ATE_COV.3 カバレージの厳格な分析**
	ATE_DPT.2 テスト：下位レベル設計
	ATE_FUN.2 順序付けられた機能テスト
	ATE_IND.2 独立テスト - サンプル
脆弱性評定	**AVA_CCA.2 系統的隠れチャネル分析**
	AVA_MSU.3 セキュアでない状態の分析とテスト
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.4 高い抵抗力

表 6.7 － EAL6

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

目的

EAL7 は、リスクが非常に高い状態での適用及び/または資産の高い価値が、さらに高いコストを正当化するところでのセキュリティ **TOE** の開発に適用される。**EAL7** の実際的な適用は、現在、広範な形式的分析に従うセキュリティ機能が強く重要視されている **TOE** に限られる。

保証コンポーネント

EAL7（表 **6.8** を参照）は、セキュリティのふるまいを理解するために、**TOE** の機能と完全なインタフェースの仕様、ガイダンス証拠資料、上位レベルと下位レベルの設計、及び実装の構造化表現を使用して、セキュリティ機能の分析により保証を提供する。保証は、**TOE** セキュリティ方針の形式的モデル、**機能仕様と上位レベル設計の形式的表現**、下位レベル設計の準形式的表現、及び**適切に、**それらの間の対応の**形式的及び**準形式的実証を通して、さらに得られる。モジュール化され、階層化された、**簡潔な TOE** 設計も必要となる。

分析は、**TOE** セキュリティ機能の独立テスト、機能仕様と上位レベル設計と下位レベル設計**と実装表現**に基づく開発者テストの証拠、開発者テスト結果の**完全な**独立した確認、機能強度分析、脆弱性に対する開発者探索の証拠、及び攻撃能力が高い侵入攻撃者に対する抵抗力を実証する独立の脆弱性分析によってサポートされる。また、分析には、開発者の系統的隠れチャネル分析の検証も含まれる。

また、**EAL7** は、構造化開発プロセス、開発環境管理、完全な自動化を含む包括的な **TOE** 構成管理の使用、及びセキュアな配付手続きの証拠を通して保証を提供する。

この EAL は、形式的表現と形式的対応、及び包括的テストを使用するさらに包括的な分析を要求することにより、EAL6 からの意義のある保証の増加を示す。

保証クラス	保証コンポーネント
構成管理	ACM_AUIT.2 完全な CM 自動化
	ACM_CAP.5 進んだサポート
	ACM_SCP.3 開発ツールの CM 範囲
配付と運用	**ADO_DEL.3 改変の防止**
	ADO_IGS.1 設置、生成、及び立上げ手順
開発	**ADV_FSP.4 形式的機能仕様**
	ADV_HLD.5 形式的上位レベル設計
	ADV_IMP.3 TSF の構造化実装
	ADV_INT.3 複雑さの最小化
	ADV_LLD.2 準形式的下位レベル設計
	ADV_RCR.3 形式的対応の実証
	ADV_SPM.3 形式的な TOE セキュリティ方針モデル
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
ライフサイクルサポート	ALC_DVS.2 セキュリティ手段の十分性
	ALC_LCD.3 測定可能なライフサイクルモデル
	ALC_TAT.3 実装標準への準拠－すべての部分
テスト	ATE_COV.3 カバレージの厳格な分析
	ATE_DPT.3 テスト：実装表現
	ATE_FUN.2 順序付けられた機能テスト
	ATE_IND.3 独立テスト - 完全
脆弱性評定	AVA_CCA.2 系統的隠れチャネル分析
	AVA_MSU.3 セキュアでない状態の分析とテスト
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.4 高い抵抗力

表 6.8 － EAL7

7　保証クラス、ファミリ、及びコンポーネント

次の **7** つの章では、保証コンポーネントの詳細な要件をクラスとファミリによりグループに分けてアルファベット順に提供する。

8　ACMクラス：構成管理

構成管理（**CM**）は、**TOE** の実装において、機能要件と仕様が実装されることを確立する方法、手段である。**CM** は、**TOE** 及びその関係する情報の改良と修正のプロセスにおいて、統制と管理を要求することにより、この目的を満たす。**CM** システムは、あらゆる変更を追跡する手段を提供し、すべての変更が許可されたものであることを保証することにより、**TOE** 構成要素の完全性を保証する。

図 **8.1** は、このクラスのファミリと、各ファミリのコンポーネントの階層を示す。

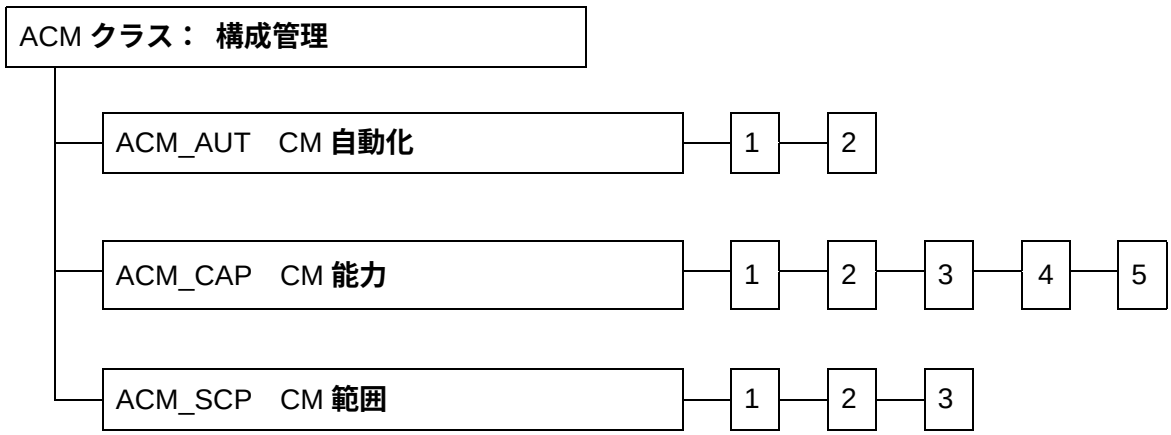

図 8.1 ― 構成管理クラスのコンポーネント構成

8.1 CM自動化（ACM_AUT）

目的

自動化された **CM** ツール導入の目的は、 **CM** システムの効率化である。自動化された **CM** システムも手作業の **CM** システムもバイパスされたり、無視されたり、許可されていない修正を防止するには不十分であるが、自動化されたシステムの方が、人の誤りや不注意に対し影響を受けにくい。

コンポーネントのレベル付け

このファミリのコンポーネントは、自動化された手段によって管理される構成要素の集合に基づいて、レベル付けされている。

適用上の注釈

ACM_AUT.1.1C は、**TOE** の実装表現に関連する要件である。**TOE** の実装表現は、物理的な **TOE** を構成するすべてのハードウェア、ソフトウェア、及びファームウェアから成る。ソフトウェアのみの **TOE** の場合は、実装表現は、単にソースとオブジェクトコードから成る。

ACM_AUT.1.2C は、**TOE** の生成を支援するための自動化された手段を **CM** システムが提供することへの要件である。これは、正しい構成要素が **TOE** の生成に使用されているかを決定することを助けるための自動化された手段を **CM** システムが提供することを要求する。

ACM_AUT.2.5C は、**TOE** とその前のバージョンとの間の変更を明確にするための自動化された手段を **CM** システムが提供することへの要件である。**TOE** の以前のバージョンが存在しない場合でも、**TOE** と **TOE** の将来のバージョンとの間の変更を明確にするための自動化された手段を開発者が提供する必要がある。

ACM_AUT.1 部分的な CM 自動化

目的

実装表現が複雑なものや、複数の開発者が開発するような開発環境では、自動化ツールなしでの変更の管理は困難である。特に、このような自動化ツールでは、開発中発生する多数の変更を支援し、これらの変更が許可されたものであることを保証できることが必要とされる。このコンポーネントの目的は、実装表現が、自動化された手段によって管理されることを保証することである。

依存性：

ACM_CAP.3　許可の管理

開発者アクションエレメント：

ACM_AUT.1.1D　開発者は、CMシステムを使用しなければならない。

ACM_AUT.1.2D　開発者は、CM計画を提供しなければならない。

証拠の内容・提示エレメント：

ACM_AUT.1.1C　CMシステムは、TOEの実装表現に対して、許可された変更のみができる自動化された手段を提供しなければならない。

ACM_AUT.1.2C　CMシステムは、TOEの生成を支援する自動化された手段を提供しなければならない。

ACM_AUT.1.3C　CM計画は、CMシステムで使用される自動化ツールについて記述しなければならない。

ACM_AUT.1.4C　CM計画は、CMシステムでどのように自動化ツールを使用するか記述しなければならない。

評価者アクションエレメント：

ACM_AUT.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ACM_AUT.2 完全な CM 自動化

目的

構成要素が複雑なものや、複数の開発者が開発するような開発環境では、自動化ツールなしでの変更の管理は困難である。特に、このような自動化ツールでは、開発中発生する多数の変更を支援し、これらの変更が許可されたものであることを保証できることが必要とされる。このコンポーネントの目的は、すべての構成要素が、自動化された手段で管理されることを保証することである。

TOE のバージョン間の変更を確認し、他の構成要素の修正によって影響を受ける構成要素を識

別する自動化された手段を提供することは、**TOE** の連続するバージョンの間の修正の影響を決定するのを助ける。その結果、このことは、**TOE** に対する変更の結果がすべての構成要素で相互に矛盾がないかどうかを決定するために、有益な情報を提供できる。

依存性：

ACM_CAP.3 許可の管理

開発者アクションエレメント：

ACM_AUT.2.1D 開発者は、**CM**システムを使用しなければならない。

ACM_AUT.2.2D 開発者は、**CM**計画を提供しなければならない。

証拠の内容・提示エレメント：

ACM_AUT.2.1C **CM**システムは、**TOE**の実装表現、**及び他のすべての構成要素に対して、**許可された変更のみができる自動化された手段を提供しなければならない。

ACM_AUT.2.2C **CM**システムは、 **TOE**の生成を支援する自動化された手段を提供しなければならない。

ACM_AUT.2.3C **CM**計画は、**CM**システムで使用される自動化ツールについて記述しなければならない。

ACM_AUT.2.4C **CM**計画は、**CM**システムでどのように自動化ツールを使用するか記述しなければならない.

ACM_AUT.2.5C **CMシステムは、TOEとその前のバージョンとの間の変更を確認するための自動化された手段を提供しなければならない。**

ACM_AUT.2.6C **CMシステムは、ある構成要素の修正により影響を受けるすべての他の構成要素を特定するための、自動化された手段を提供しなければならない。**

評価者アクションエレメント：

ACM_AUT.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

8.2 CM能力（ACM_CAP）

目的

CM システムの能力は、構成要素の事故による、または許可されない修正が起きる可能性と取り組む。**CM** システムは、設計の初期段階から後続する保守作業までを通して、**TOE** の完全性を保証しなければならない。

このファミリは、以下の目的を含んでいる。
a)消費者に送る前に、**TSF** が正確で完全であることを保証する。
b)評価中に、構成要素の漏れがないことを保証する。
c)TOE 構成要素の許可されない修正、追加、排除を防止する。

コンポーネントのレベル付け

このファミリのコンポーネントは、**CM** システムの能力がどのようなものか、開発者により提供された **CM** 証拠資料の適用範囲、**CM** システムがセキュリティ要件を満たすことの正当性を開発者が提供できるかどうかに基づいて、レベル付けされている。

適用上の注釈

ACM_CAP.2 は、構成要素を参照するいくつかのエレメントを導入する。**ACM_SCP** ファミリは、構成要素が **CM** システムによって追跡されるための要件を含んでいる。

ACM_CAP.2.3C は、構成リストが提供されることへの要件である。構成リストには、**CM** システムによって維持されるすべての構成要素が含まれる。

ACM_CAP.2.6C は、**CM** システムが、すべての構成要素を一意に識別することへの要件である。この要件は、構成要素への修正に対し、新たな一意の識別情報を割り当てることを含む。

ACM_CAP.3.8C は、**CM** システムが **CM** 計画に従って機能していることを実証する証拠への要件である。このような証拠の例は、**CM** システムが出力する画面のスナップショットや監査証跡のような証拠資料、または開発者による **CM** システムの詳細な実演である。評価者は、**CM** システムが **CM** 計画に従って機能していることを示すのに、この証拠が十分であるかを決定する責任がある。

ACM_CAP.3.9C は、すべての構成要素が **CM** システム下で維持されていることの証拠を提供することへの要件である。構成要素は、構成リストにある要素を指すため、この要件は、**CM** リストのすべての要素が、**CM** システム下で維持されていることを述べている。

ACM_CAP.4.11C は、**CM** システムが **TOE** の生成を支援することへの要件である。
すなわち、**CM** システムは、**TOE** 生成時に正しい構成要素が使用されていることを決定するのを助ける情報、または電子的手段を提供することが要求される。

ACM_CAP.1 バージョン番号

目的

TOE のどの段階のものが評価されているかの観点から、曖昧さのないことを保証するために、一意のリファレンスが要求される。**TOE** をそのリファレンスでラベル付けすることは、**TOE** の利用者が **TOE** のどの段階のものを使用しているかを知ることができることを保証する。

依存性： なし

開発者アクションエレメント：

ACM_CAP.1.1D　開発者は、TOEのリファレンスを提供しなければならない。

証拠の内容・提示エレメント：

ACM_CAP.1.1C　TOEのリファレンスは、TOEのバージョン毎に一意でなければならない。

ACM_CAP.1.2C　TOEは、そのリファレンスでラベル付けされなければならない。

評価者アクションエレメント：

ACM_CAP.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ACM_CAP.2　構成要素

目的

TOE のどの段階のもの**(instance)**が評価されているかの観点から、曖昧さのないことを保証するために、一意のリファレンスが要求される。**TOE** をそのリファレンスでラベル付けすることは、**TOE** の利用者が **TOE** のどの段階のものを使用しているかを知ることができることを保証する。

構成要素の一意の識別情報は、**TOE** の構成をより明快に理解することを導き、その結果どの要素が **TOE** のための評価要件の対象になるか決定することを助ける。

依存性： なし

開発者アクションエレメント：

ACM_CAP.2.1D 開発者は、**TOE**のリファレンスを提供しなければならない。

ACM_CAP.2.2D 開発者は、CMシステムを使用しなければならない。

ACM_CAP.2.3D 開発者は、CM証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ACM_CAP.2.1C TOEのリファレンスは、**TOE**のバージョン毎に一意でなければならない。

ACM_CAP.2.2C TOEは、そのリレファレンスでラベル付けされなければならない。

ACM_CAP.2.3C CM証拠資料は、構成リストを含まなければならない。

ACM_CAP.2.4C 構成リストは、TOEを構成する構成要素を記述しなければならない。

ACM_CAP.2.5C CM証拠資料は、構成要素を一意に識別する方法を記述しなければならない。

ACM_CAP.2.6C CMシステムは、すべての構成要素を一意に識別しなければならない。

評価者アクションエレメント：

ACM_CAP.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ACM_CAP.3 許可の管理

目的

TOE のどの段階のもの**(instance)**が評価されているかの観点から、曖昧さのないことを保証するために、一意のリファレンスが要求される。**TOE** をそのリファレンスでラベル付けすることは、**TOE** の利用者が **TOE** のどの段階のものを使用しているかを知ることができることを保証する。

構成要素の一意の識別情報は、**TOE** の構成をより明快に理解することを導き、その結果どの要素が **TOE** のための評価要件の対象になるか決定することを助ける。

許可されていない修正が **TOE** に対して行われないことを保証する管理の提供と、また、**CM** システムが適切に機能しかつ使用されていることを保証することは、**TOE** の完全性を維持することを助ける。

依存性：

ACM_SCP.1　TOE の CM 範囲
ALC_DVS.1　セキュリティ手段の識別

開発者アクションエレメント：

ACM_CAP.3.1D　開発者は、**TOE**のリレファレンスを提供しなければならない。

ACM_CAP.3.2D　開発者は、**CM**システムを使用しなければならない。

ACM_CAP.3.3D　開発者は、**CM**証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ACM_CAP.3.1C　**TOE**のリファレンスは、**TOE**のバージョン毎に一意でなければならない。

ACM_CAP.3.2C　**TOE**は、そのリファレンスでラベル付けされなければならない。

ACM_CAP.3.3C　**CM**証拠資料は、構成リスト**とCM計画**を含まなければならない。

ACM_CAP.3.4C　構成リストは、**TOE**を構成する構成要素を記述しなければならない。

ACM_CAP.3.5C　**CM**証拠資料は、構成要素を一意に識別する方法を記述しなければならない。

ACM_CAP.3.6C　**CM**システムは、すべての構成要素を一意に識別しなければならない。

ACM_CAP.3.7C　**CM計画は、CMシステムがどのように使用されるかを記述しなければならない。**

ACM_CAP.3.8C　**CMシステムが、CM計画に従って機能していることを実証しなければならない。**

ACM_CAP.3.9C　**CM証拠資料は、CMシステム下ですべての構成要素が効果的に維持され続けていることの証拠を提供しなければならない。**

ACM_CAP.3.10C　**CMシステムは、許可された変更のみが構成要素に対して行われる手段を提供しなければならない。**

評価者アクションエレメント：

ACM_CAP.3.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ACM_CAP.4　生成の支援と受入手続き

目的

TOE のどの段階のもの**(instance)**が評価されているかの観点から、曖昧さのないことを保証するために、一意のリファレンスが要求される。**TOE** をそのリファレンスでラベル付けすることは、**TOE** の利用者が **TOE** のどの段階のものを使用しているかを知ることができることを保証する。

構成要素の一意の識別情報は、**TOE** の構成をより明快に理解することを導き、その結果どの要素が **TOE** のための評価要件の対象になるか決定することを助ける。

許可されていない修正が **TOE** に対して行われないことを保証する管理の提供と、また、**CM** システムが適切に機能しかつ使用されていることを保証することは、**TOE** の完全性を維持することを助ける。

受入手続きの目的は、構成要素のいかなる生成や修正も許可されていることを確認することである。

依存性：

ACM_SCP.1　**TOE** の **CM** 範囲
ALC_DVS.1　セキュリティ手段の識別

開発者アクションエレメント：

ACM_CAP.4.1D　開発者は、**TOE**のリファレンスを提供しなければならない。

ACM_CAP.4.2D　開発者は、**CM**システムを使用しなければならない。

ACM_CAP.4.3D　開発者は、**CM**証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ACM_CAP.4.1C　**TOE**のリファレンスは、**TOE**のバージョン毎に一意でなければならない。

ACM_CAP.4.2C　**TOE**は、そのリファレンスでラベル付けされなければならない。

ACM_CAP.4.3C **CM**証拠資料は、構成リスト、**CM**計画、**及び受入計画**を含まなければならない。

ACM_CAP.4.4C 構成リストは、**TOE**を構成する構成要素を記述しなければならない。

ACM_CAP.4.5C **CM**証拠資料は、構成要素を一意に識別する方法を記述しなければならない。

ACM_CAP.4.6C **CM**システムは、すべての構成要素を一意に識別しなければならない。

ACM_CAP.4.7C **CM**計画は、**CM**システムがどのように使用されるかを記述しなければならない。

ACM_CAP.4.8C **CM**システムが、**CM**計画に従って機能していることを証拠により示さなければならない。

ACM_CAP.4.9C **CM**証拠資料は、**CM**システム下ですべての構成要素が効果的に維持され続けていることの証拠を提供しなければならない。

ACM_CAP.4.10C **CM**システムは、許可された変更のみが構成要素に対して行われる手段を提供しなければならない。

ACM_CAP.4.11C **CMシステムは、TOEの生成を支援しなければならない。**

ACM_CAP.4.12C **受入計画は、修正もしくは新規に生成された構成要素をTOEの一部として受け入れるための手続きを記述しなければならない。**

評価者アクションエレメント：

ACM_CAP.4.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ACM_CAP.5 進んだサポート

目的

TOE のどの段階のもの**(instance)**が評価されているかの観点から、曖昧さのないことを保証するために、一意のリファレンスが要求される。**TOE** をそのリファレンスでラベル付けすることは、**TOE** の利用者が **TOE** のどの段階のものを使用しているかを知ることができることを保証する。

構成要素の一意の識別は、**TOE** の構成をより明快に理解することを導き、その結果どの要素が **TOE** のための評価要件の対象になるか決定することを助ける。

許可されていない修正が **TOE** に対して行われないことを保証する管理の提供と、また、**CM** システムが適切に機能しかつ使用されていることを保証することは、**TOE** の完全性を維持することを助ける。

受入手続きの目的は、構成要素のいかなる生成や修正も許可されていることを確認することである。

統合手続きは、管理された構成要素のセットからの **TOE** の生成が、許可された方法で正しく実行されることを保証する助けとなる。

CM システムが、**TOE** の生成に使用する資材のマスタコピーを識別できること要求することは、その資材の完全性が、適切な技術的、物理的、及び手続き的保護手段により保護されることを保証する助けとなる。

依存性：

ACM_SCP.1　TOE の **CM** 範囲
ALC_DVS.2　セキュリティ手段の十分性

開発者アクションエレメント：

ACM_CAP.5.1D　開発者は、**TOE**のリファレンスを提供しなければならない。

ACM_CAP.5.2D　開発者は、**CM**システムを使用しなければならない。

ACM_CAP.5.3D　開発者は、**CM**証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ACM_CAP.5.1C　**TOE**のリファレンスは、**TOE**のバージョン毎に一意でなければならない。

ACM_CAP.5.2C　**TOE**は、そのリファレンスでラベル付けされなければならない。

ACM_CAP.5.3C　**CM**証拠資料は、構成リスト、**CM**計画、受入計画**、及び統合手続き**を含まなければならない。

ACM_CAP.5.4C　構成リストは、**TOE**を構成する構成要素を記述しなければならない。

ACM_CAP.5.5C　**CM**証拠資料は、構成要素を一意に識別する方法を記述しなければならない。

ACM_CAP.5.6C **CM**システムは、すべての構成要素を一意に識別しなければならない。

ACM_CAP.5.7C **CM**計画は、**CM**システムがどのように使用されるかを記述しなければならない。

ACM_CAP.5.8C **CM**システムが、**CM**計画に従って機能していることを証拠により示さなければならない。

ACM_CAP.5.9C **CM**証拠資料は、**CM**システム下ですべての構成要素が効果的に維持され続けていることの証拠を提供しなければならない。

ACM_CAP.5.10C **CM**システムは、許可された変更のみが構成要素に対して行われる手段を提供しなければならない。

ACM_CAP.5.11C **CM**システムは、**TOE**の生成を支援しなければならない。

ACM_CAP.5.12C 受入計画は、修正もしくは新規に生成された構成要素を**TOE**の一部として受け入れるための手続きを記述しなければならない。

ACM_CAP.5.13C **統合手続きは、TOEの製造工程にCMシステムがどのように適用されるかを記述しなければならない。**

ACM_CAP.5.14C **CMシステムは、構成要素をCMに受け入れる責任のある人はその開発者でないことを要求しなければならない。**

ACM_CAP.5.15C **CMシステムは、TSFを構成する構成要素を明確に識別しなければならない。**

ACM_CAP.5.16C **CMシステムは、最低限、修正者、日時を含む監査証跡で、TOEのすべての修正についての監査を支援しなければならない。**

ACM_CAP.5.17C **CMシステムは、TOEの生成に使用されるすべての資材のマスタコピーを識別できなければならない。**

ACM_CAP.5.18C **CM証拠資料は、開発のセキュリティ手段と共にCMシステムの使用が、TOEに対して許可された変更のみが許されることを、実証しなければならない。**

ACM_CAP.5.19C **CM証拠資料は、統合手続きを使用することによって、TOEが許可された方法で正しく生成されることを保証できることを、実証しなければならない。**

ACM_CAP.5.20C **CM証拠資料は、CMシステムが、構成要素をCMに受け付ける責任者がその開発者でないことを保証するのに十分であることを、実証しなければならな**

い。

ACM_CAP.5.21C CM証拠資料は、受入手続きが、すべての構成要素に対する十分で適切な変更のレビューを提供することを正当化しなければならない。

評価者アクションエレメント：

ACM_CAP.5.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

8.3 CM範囲（ACM_SCP）

目的

このファミリの目的は、すべての必要な **TOE** 構成要素が、**CM** システムによって追跡されることを保証することである。これは、**CM** システムの能力によってこれらの構成要素の完全性が保護されていることを保証する助けとなる。

このファミリは、以下の目的を含んでいる。

a)TOE の実装表現が、追跡されることを保証する。

b)問題レポートを含むすべての必要な証拠資料が、開発または運用中に追跡されることを保証する。

c)構成オプション（例えば、コンパイラスイッチ）が、追跡されることを保証する。

d)開発ツールが、追跡されることを保証する。

コンポーネントのレベル付け

このファミリのコンポーネントは、以下のどれが **CM** システムによって追跡されるかに基づいて、レベル付けされている。
TOE の実装表現；設計証拠資料；テスト証拠資料；利用者用証拠資料；管理者用証拠資料；**CM** 証拠資料； セキュリティ欠陥； 開発ツール

適用上の注釈

ACM_SCP.1.1C は、**CM** システムにより、**TOE** の実装表現が追跡されることを要件とする。**TOE** の実装表現は、物理的 **TOE** を構成するすべてのハードウェア、ソフトウェア、及びファームウェアから成る。ソフトウェアのみの **TOE** の場合は、実装表現は、単にソースとオブジェクトコードから成る。

ACM_SCP.1.1C はまた、**CM** システムにより、**CM** 証拠資料が追跡されることを要件とする。**CM** 証拠資料には、**CM** 計画や、**CM** システムを構成するツールの現バージョン情報が含まれる。

ACM_SCP.2.1C は、**CM** システムにより、セキュリティ欠陥が追跡されることを要件とする。これは、現状のセキュリティ欠陥の詳細だけでなく、以前のセキュリティ欠陥とその解決についての情報が維持されることを要求する。

ACM_SCP.3.1C は、**CM** システムにより、開発ツールとそれに関連する情報が追跡されることを要件とする。開発ツールの例として、プログラミング言語とコンパイラが挙げられる。**TOE** の生成に付随する情報（コンパイラオプション、インストール／生成のオプション、構築オプションなど）が、開発ツールに関連する情報の例である。

ACM_SCP.1　TOE の CM 範囲

目的

CM システムは、**CM** 下に置かれた要素に対してのみ変更を管理することができる。**TOE** の実装表現、設計、テスト、利用者用、及び管理者用の証拠資料、及び **CM** 証拠資料を **CM** 下に置くことは、これらが適切な許可を伴う管理された方法で修正がなされることの保証をもたらす。

依存性：

ACM_CAP.3　許可の管理

開発者アクションエレメント：

ACM_SCP.1.1D　開発者は、CM証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ACM_SCP.1.1C　CM証拠資料は、最小限、以下がCMシステムにより追跡されることを示さなければならない。TOE の実装表現、設計証拠資料、テスト証拠資料、利用者用証拠資料、管理者用証拠資料、及びCM証拠資料

ACM_SCP.1.2C　CM証拠資料は、どのように構成要素がCMシステムによって追跡されるかを記述しなければならない。

評価者アクションエレメント：

ACM_SCP.1.1E　評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない.

ACM_SCP.2　問題追跡の CM 範囲

目的

CM システムは、**CM** 下に置かれた要素に対してのみ変更を管理することができる。**TOE** の実装表現、設計、テスト、利用者用、及び管理者用証拠資料、及び **CM** 証拠資料を **CM** 下に置くことは、これらが適切な許可を伴う管理された方法で修正がなされることの保証をもたらす。

CM 下でセキュリティ欠陥を追跡する能力は、セキュリティ欠陥報告が紛失したり、忘れられた

りすることがなく、また、開発者がセキュリティ欠陥をその解決まで追跡することを許す。

依存性：

ACM_CAP.3　許可の管理

開発者アクションエレメント：

ACM_SCP.2.1D　開発者は、**CM**証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ACM_SCP.2.1C　**CM**証拠資料は、最小限、以下が**CM**システムにより追跡されることを示さなければならない。**TOE** の実装表現、設計証拠資料、テスト証拠資料、利用者用証拠資料、管理者用証拠資料、**CM**証拠資料**、及びセキュリティ欠陥**

ACM_SCP.2.2C　**CM**証拠資料は、どのように構成要素が**CM**システムによって追跡されるかを記述しなければならない。

評価者アクションエレメント：

ACM_SCP.2.1E　評価者は、 提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない.

ACM_SCP.3　開発ツールの CM 範囲

目的

CM システムは、**CM** 下に置かれた要素に対してのみ変更を管理することができる。**TOE** の実装表現、設計、テスト、利用者用、及び管理者用証拠資料、及び **CM** 証拠資料を **CM** 下に置くことは、これらが適切な許可を伴う管理された方法で修正がなされることの保証をもたらす。

CM 下でセキュリティ欠陥を追跡する能力は、セキュリティ欠陥報告が紛失したり、忘れられたりすることがなく、また、開発者がセキュリティ欠陥をその解決まで追跡することを許す。

開発ツールは、品質の高いバージョンの **TOE** の生成を保証するのに重要な役割を持つ。このため、これらのツールに対する修正を管理することは重要とされる。

依存性：

ACM_CAP.3　許可の管理

開発者アクションエレメント：

ACM_SCP.3.1D　開発者は、**CM**証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ACM_SCP.3.1C　**CM**証拠資料は、最小限、以下が**CM**システムにより追跡されることを示さなければならない。**TOE** の実装表現、設計証拠資料、テスト証拠資料、利用者用証拠資料、管理者用証拠資料、**CM**証拠資料、セキュリティ欠陥**、及び開発ツールとそれに関連する情報**

ACM_SCP.3.2C　**CM**証拠資料は、どのように構成要素が**CM**システムによって追跡されるかを記述しなければならない。

評価者アクションエレメント：

ACM_SCP.3.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない.

9　ADOクラス：配付と運用

配付と運用は、**TOE** の正しい配付、設置、生成、及び立上げのための要件を提供する。

図 **9.1** は、このクラスのファミリと、各ファミリのコンポーネントの階層を示す。

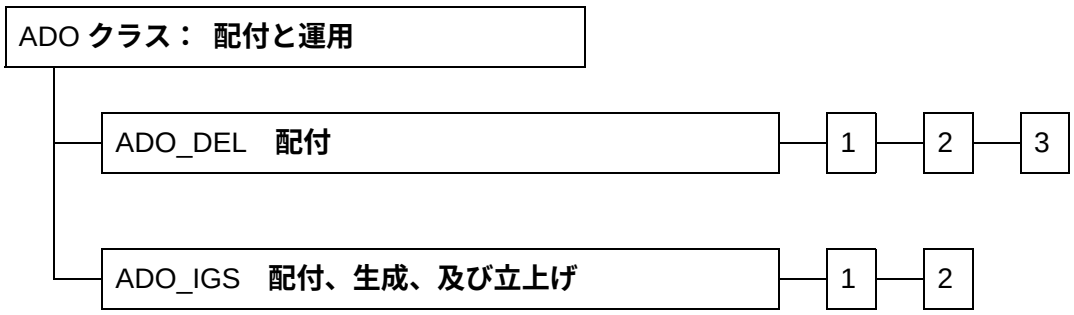

図 9.1 － 配付と運用クラスのコンポーネント構成

9.1 配付 (ADO_DEL)

目的

配付のための要件は、発送者が送ろうとした **TOE** が一切の改変なく、受領者が受け取れる保証を提供するシステム管理、配送の設備と手続きを要求する。配付が正当であるためには、受け取られるものは、正確に **TOE** のマスタコピーに一致しなければならず、現在の版**(version)**への改ざん、または誤った版への置き換えを一切排除しなければならない。

コンポーネントのレベル付け

このファミリのコンポーネントは、配付の間の **TOE** への修正を検出、及び防止するための、開発者への要求の増加に基づいて、レベル付けされている。

ADO_DEL.1 配付手続き

依存性： なし

開発者アクションエレメント：

ADO_DEL.1.1D **開発者は、TOE、または、その一部を利用者に配付するための手続きに関する証拠資料を提出しなければならない。**

ADO_DEL.1.2D **開発者は、配付手続きを使用しなければならない。**

証拠の内容・提示エレメント：

ADO_DEL.1.1C **配付に関する証拠資料は、TOEの版を利用者サイトへ配送するときにセキュリティを維持するために必要なすべての手続きを記述しなければならない。**

評価者アクションエレメント：

ADO_DEL.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

ADO_DEL.2 改変の検出

依存性：

ACM_CAP.3 許可の管理

開発者アクションエレメント：

ADO_DEL.2.1D 開発者は、**TOE**、または、その一部を利用者に配付するための手続きに関する証拠資料を提出しなければならない。

ADO_DEL.2.2D 開発者は、配付手続きを使用しなければならない。

証拠の内容・提示エレメント：

ADO_DEL.2.1C 配付に関する証拠資料は、**TOE**の版を利用者サイトへ配送するときにセキュリティを維持するために必要なすべての手続きを記述しなければならない。

ADO_DEL.2.2C 配付に関する証拠資料は、種々の手続きや技術的手段が、開発者のマスタコピーと利用者サイトで受け取る版の間の改変、または不一致の検出にどう備えているかを記述しなければならない。

ADO_DEL.2.3C 配付に関する証拠資料は、種々の手続きが、たとえ開発者が利用者サイトへ何も送らないような場合にも、開発者に成り済まそうとする試みをいかに検出するかを記述しなければならない。

評価者アクションエレメント：

ADO_DEL.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADO_DEL.3 改変の防止

依存性：

ACM_CAP.3 許可の管理

開発者アクションエレメント：

ADO_DEL.3.1D 開発者は、**TOE**、または、その一部を利用者に配付するための手続きに関する証拠資料を提出しなければならない。

ADO_DEL.3.2D 開発者は、配付手続きを使用しなければならない。

証拠の内容・提示エレメント：

ADO_DEL.3.1C 配付に関する証拠資料は、**TOE**の版を利用者サイトへ配送するときにセキュリティを維持するために必要なすべての手続きを記述しなければならない。

ADO_DEL.3.2C 配付に関する証拠資料は、種々の手続きや技術的手段が、開発者のマスタコピーと利用者サイトで受け取る版の間の改変、または不一致の**防止**にどう備えているかを記述しなければならない。

ADO_DEL.3.3C 配付に関する証拠資料は、種々の手続きが、たとえ開発者が利用者サイトへ何も送らないような場合にも、開発者に成り済まそうとする試みをいかに検出するかを記述しなければならない。

評価者アクションエレメント：

ADO_DEL.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

9.2 設置、生成、及び立上げ(ADO_IGS)

目的

設置、生成、及び立上げ手順は、**TOE** が開発者の意図したようなセキュアな方法で、設置され、生成され、立上げられたことを保証するのに有用である。設置、生成、及び立上げのための要件は、構成管理の元に置かれた **TOE** の実装表現から、利用者環境での最初の運用へのセキュアな転移を要求する。

コンポーネントのレベル付け

このファミリのコンポーネントは、**TOE** の生成オプションがログを記録するかどうかに基づいて、レベル付けされている。

適用上の注釈

これらの要件の適用は、**TOE** が **IT** 製品かシステムか、また、運用可能状態で配付されるか、**TOE** 所有者のサイトで生成されるかなどの点により変化するであろうことが認められている。与えられた **TOE** に対しては、通常、設置、生成、及び立上げに関しての **TOE** 開発者と **TOE** 所有者の間で責任が分割されるが、すべての活動が **1** 個所で発生するような例もある。例えば、スマートカードにおいては、設置、生成、及び立上げのすべての局面は **TOE** の開発者のサイトで実行されるだろう。反対に、設置、生成、及び立上げのすべての局面が **TOE** 所有者のサイトで実行される場合には、**TOE** はソフトウェアの形態で **IT** システムとして配付されるだろう。

評価が始まるまでに **TOE** が既に設置されている場合もある。このような場合には、設置手順の要求や解析は不適当であろう。

更に、生成に関する要件は、**TOE** の実装表現から運用状態の **TOE** の一部を生成する能力を提供する **TOE** にしか適用できない。

設置、生成、及び立上げ手順は、独立した文書として存在してもよいし、他の管理ガイダンスとグループ化されてもよい。この保証ファミリの要件は、**AGD_ADM** ファミリの要件とは別に提示される。というのも、設置、生成、及び立上げ手順は、稀にしか発生せず、おそらく１回限りの使用であるからである。

ADO_IGS.1 設置、生成、及び立上げ手順

依存性：

AGD_ADM.1 管理者ガイダンス

開発者アクションエレメント：

ADO_IGS.1.1D 開発者は、TOEのセキュアな設置、生成、及び立上げの手順に関する証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

ADO_IGS.1.1C 証拠資料は、TOEのセキュアな設置、生成、及び立上げのために必要な手順を記述しなければならない。

評価者アクションエレメント：

ADO_IGS.1.1E評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADO_IGS.1.2E 評価者は、設置、生成、及び立上げの手順がセキュアな構成を結果として生じしめることを決定しなければならない。

ADO_IGS.2 生成ログ

依存性：

AGD_ADM.1 管理者ガイダンス

開発者アクションエレメント：

ADO_IGS.2.1D 開発者は、**TOE**のセキュアな設置、生成、及び立上げの手順に関する証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

ADO_IGS.2.1C 証拠資料は、**TOE**のセキュアな設置、生成、及び立上げのために必要な手順を記述しなければならない。

ADO_IGS.2.2C 証拠資料は、TOEがいかにして、また、いつ生成されたかを正確に決定することができるように、TOEを生成するのに用いられた生成オプションを含むログを作成する手順を記述しなければならない。

評価者アクションエレメント：

ADO_IGS.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADO_IGS.2.2E 評価者は、設置、生成、及び立上げの手順がセキュアな構成を結果として生じしめることを決定しなければならない。

10　ADVクラス：開発

開発クラスは、機能インタフェースから実装表現に至る種々の抽象レベルでの **TSF** を表現するための要件について４つのファミリを含んでいる。開発クラスは、種々の **TSF** 表現間の対応付に対する要件のファミリも含んでおり、これは、最も抽象度の低い表現形態からすべての中間表現を介して、**ST** で定義される **TOE** 要約仕様までの対応付けの実証を最終的に必要とする。更に、**TSP** モデルに対する要件や、**TSP**、**TSP** モデル及び機能仕様間の対応付けに対する要件のファミリがある。また、モジュール方式、階層化、及び複雑さを最少化するような面をカバーする **TSF** の内部構造に関する要件がある。

図 **10.1** は、このクラスのファミリと、各ファミリのコンポーネントの階層を示す。

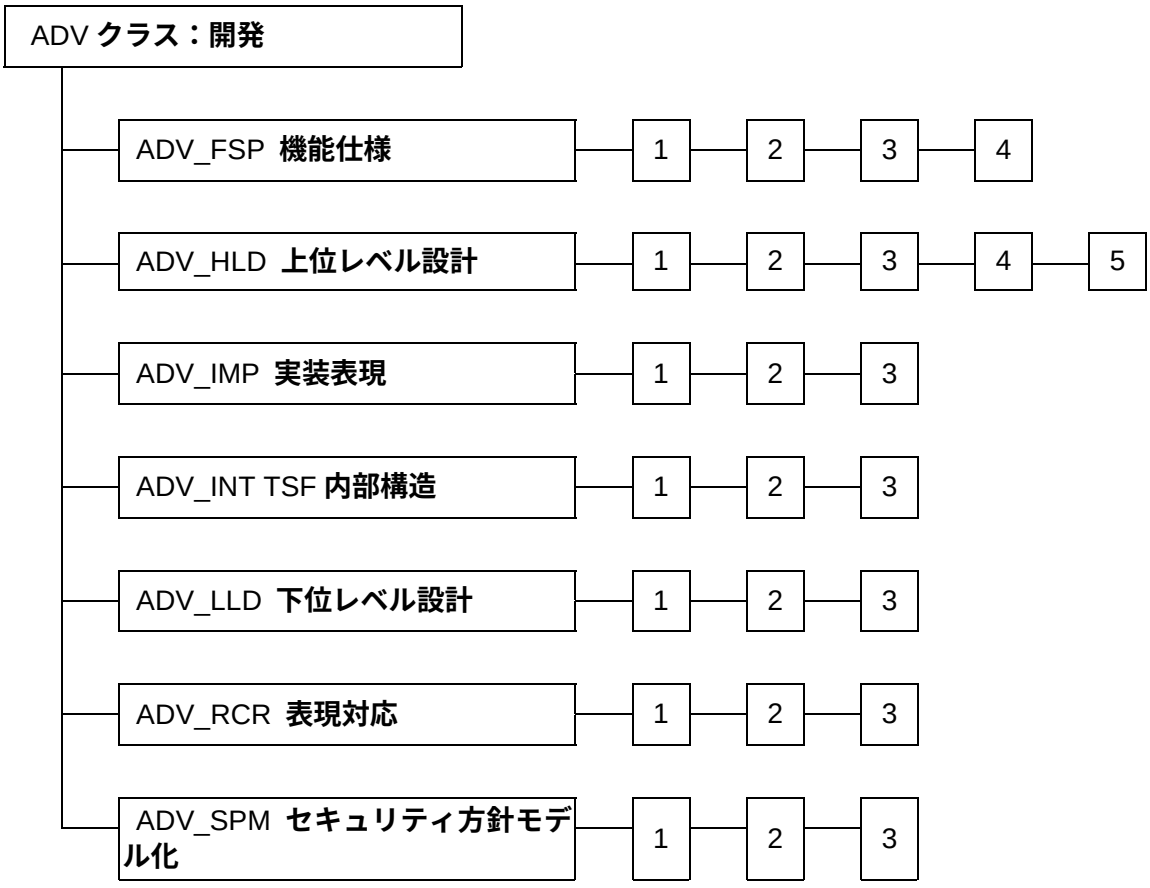

図 10.1 ― 開発クラスのコンポーネント構成

TSF の機能仕様、**TSF** のサブシステムへの分割、サブシステムからモジュールへの分割、モジュールの実装表現、及び証拠として提供されるすべての分割されたものの間の対応付けの実証、の各々がこれらのファミリの表現様式となる。種々の **TSF** 表現に対する要件は、それぞれ異な

るファミリに分かれてはいるが、どの **TSF** 表現のサブセットが必要であるかの特定は **PP/ST** の作成者に任されている。

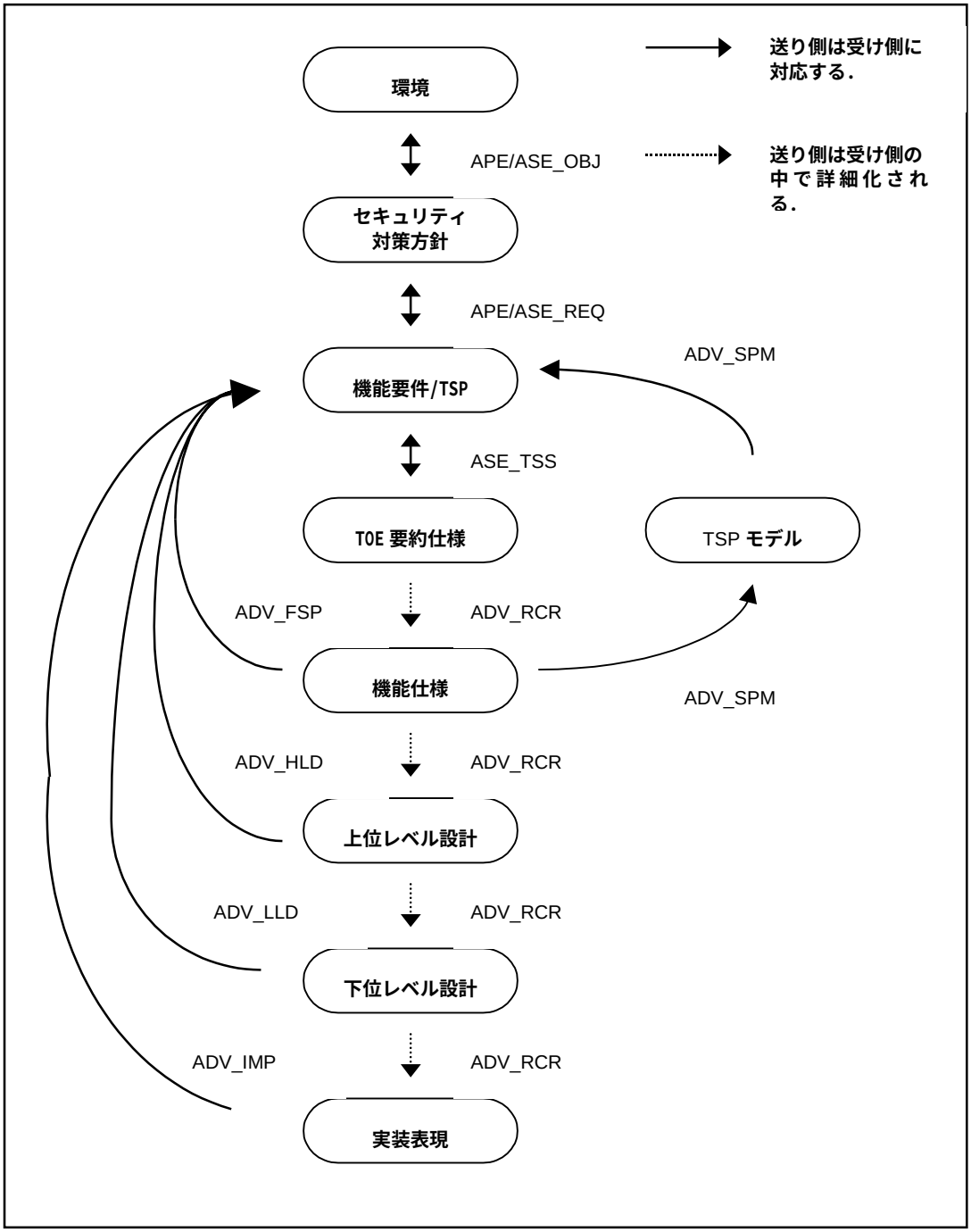

図 10.2 ー TOE 表現と要件の間の関係

図 **10.2** は、種々の **TSF** 表現とそれらが説明されるべき対策方針及び要件、との関係を示している。この図が示すように、**APE** と **ASE** クラスは、機能要件とセキュリティ対策方針間の対応付

けに対する要件、また同様にセキュリティ対策方針と **TOE** の想定環境との対応に対する要件も規定している。**ASE** クラスは、セキュリティ対策方針、機能要件、及び **TOE** 要約仕様間の対応付けに対する要件についても規定している。

これ以外の図 **10.2** で示される対応関係は、すべて **ADV** クラスで定義される。**ADV_SPM** ファミリは、**TSP** と **TSP** モデル間、及び **TSP** モデルと機能仕様間の対応付けに対する要件を規定している。**ADV_RCR** ファミリは、**TOE** 要約仕様から実装表現に至る、すべての利用可能な **TSF** 表現間の対応付けに対する要件を規定している。最終的に、**TSF** 表現に焦点を当てた各保証ファミリ**(**例**:ADV_FSP, ADV_HLD, ADV_LLD, ADV_IMP)**は、その **TSP** 表現を機能要件に関係付ける要件を規定し、この関係付けは、**TOE** セキュリティ要件が記述されたことを確実にすることに役立つ。トレーサビリティ分析は、最上位の **TSF** 表現から、提供されているそれぞれの下位の **TSF** 表現へと常に実施される。**CC** は、**ADV_RCR** ファミリでの依存性を通して、このトレーサビリティ要件を述べる。**ADV_INT** ファミリは、**TSF** の内部構造に関するもので、**TSF** 表現の詳細化のプロセスにのみ間接的に関与しているため、この図には表されていない。

適用上の注釈

TOE セキュリティ方針**(TSP)**は、**TOE** 内で、どのように資源が管理、保護及び配付されるかについて制定された規則集であり、**TOE** セキュリティ機能要件で述べられる。**TSP** は、セキュリティ機能方針**(SFP)**とその他の個々の要件エレメントを組み合わせて **TOE** セキュリティ機能要件によって表現されるため、開発者は **TSP** をわざわざ提供するよう求められることはない。

TOE セキュリティ機能**(TSF)**は、**TSP** の実施に必要となる **TOE** のすべてのパーツである。**TSF** は、直接 **TSP** を実施する機能、及び **TSP** を直接実施しないがより間接的な形態で **TSP** の実施に寄与する機能の双方を含んでいる。

ASE_TSS ファミリ及びこのクラスの幾つかのファミリ中の要件は、幾つかの異なった **TSF** 表現を求めているが、これはそれぞれすべての **TSF** 表現を別々の文書として記述することを必要としているわけではない。実際、要求されているのはこれらの **TSF** 表現についての情報であって、結果としての文書構造ではないために、ひとつの文書が複数の **TSF** 表現に対する証拠資料要件に合致する場合もある。複数の **TSF** 表現がひとつの文書中に混在している場合、開発者は、文書のどの部分が、どの要件に合致しているかを示さなければならない。

3 種の仕様の様式**(**非形式的、準形式的、及び形式的**)**がこのクラスによって義務付けられる。機能仕様、上位レベル設計、下位レベル設計、及び **TSP** モデルは、この中のひとつ、または複数の仕様の様式に従って書かれる。これらの仕様中の曖昧さは、形式化のレベルが高いほど少なくなる。

非形式的仕様とは、自然言語によって普通に書かれる。ここで言う自然言語とは、（オランダ語や、英語、フランス語、ドイツ語など）通常の会話で用いられる言葉を示している。非形式的仕様は、その言語で通常用いられている（例**:**文法や構文）規則として要求されること以外、記法や特別な制約は課されない。記法に関する制約は課されないものの、非形式的仕様では、文脈上、

通常用いられる意味と異なる場合には、定められている用語の意味が定義されていなければならない。

準形式的仕様は、構文制約言語によって書かれ、これに（非形式的な）補足説明が加わっているようなものをいう。構文制約言語とは、文の構成上の制約や、特別な意味を持つキーワードの使用が義務づけられているような自然言語による表現、または（例:データフロー図、状態遷移図、**E-R** 図、データ構造図、プロセスやプログラムの構造図）ダイアグラムなどを用いた表現を示す。

形式的仕様とは、数学的概念に基づいた記法によって書かれ、これに（非形式的な）補足説明が加わっているようなものをいう。これらの数学的概念は、記法の構文と意味、及び論理的な推論を助ける証明規則を定義するために用いられる。形式的記法に用いられる構文意味規則は、どのようにして曖昧さなくその複合概念を認識し、その意味を決定付けるかを定義しなければならない。矛盾が導き出すのが不可能であると言う証拠が必要であり、記法をサポートするすべての規則を定義または参照する必要がある。

重要度の高い保証は、**TSF** が、その各 **TSF** 表現を順にたどれることができることを確認し、**TSP** モデルが機能仕様に対応付けられていることを確認することによって得られる。**ADV_RCR** ファミリは、種々の **TSF** 表現間の対応付けを、**ADV_SPM** ファミリは、**TSP** モデルと機能仕様間の対応付けに対する要件を含んでいる。対応付けは、非形式的な実証、準形式的な実証、または形式的な証明の形態をとることができる。

対応付けの非形式的な実証が求められている場合、これは、単に基本的な対応付けが要求されていることを意味する。対応付けの方法としては、例えば、２次元テーブルによって対応付けをチェックする方法や、設計図の適切な表記法を用いたりする方法が考えられる。他の文書へのポインタや参照が使用されることもできる。

対応付けの準形式的な実証は、対応付けの分析において構造的手法を要求している。この手法は、対応付けで用いられている用語の解釈に制限を加えることによって、非形式的な対応付けで生じる曖昧さを減らさなければならない。他の文書へのポインタや参照が使用されてもよい。

対応付けの形式的な証明は、形式的記法の構文や意味、及び論理的な推論を支援する証明規則を定義するために、確立された数学的概念が使用されることを要求する。セキュリティ特性は、形式的仕様言語で記述可能なことが求められ、かつ、これらのセキュリティ特性は、形式的仕様によって満足されていることが説明される必要がある。他の文書へのポインタや参照が使用されてもよい。

ADV_RCR.*.1C の項目は、それぞれ隣あう **TSF** 表現の組に対して、より抽象的な **TSF** 表現のすべてに関連するセキュリティの機能性が、より抽象性の低い **TSF** 表現において詳細化されることを開発者が証拠として提示する様要求している。**ADV_FSP.*.2E**、**ADV_HLD.*.**２**E**、**ADV_LLD.*.2E**、及び **ADV_IMP.*.**２**E** のエレメントは、それぞれその要件のファミリで表現

されている **TSF** が、**TOE** セキュリティ機能要件の正確なかつ完全な具体化であることを、評価者が決定することを要求している。**TSF** 表現が、**TOE** セキュリティ機能要件の正確で完全な具体化であることを決定するために、評価者は、**ADV_RCR.*.1C** の中で開発者によって提供される証拠を、この決定のための入力として用いることを意図している。**TOE** セキュリティ機能要件と連鎖する **TSF** 表現を順次対応付けることによって、最終的に、このクラスの最終的な目的とも言える、抽象度の最も低い **TSF** 表現から **TOE** セキュリティ機能要件へ対応付けられていることのより確実な保証を得ることができる。評価者が、中間的な **TSF** 表現から **TOE** セキュリティ機能要件への対応付けの決定ができない場合に、最も抽象度の低い **TSF** 表現から、**TOE** セキュリティ機能要件への対応付けを試みることは、正確に評価を進めるにはステップが離れ過ぎるかも知れない。最後に、要求される **TSF** 表現のセットによっては、下位レベル設計、上位レベル設計、または機能仕様が、提供される最も抽象度の低い **TSF** 表現のことがある。

10.1 機能仕様 (ADV_FSP)

目的

機能仕様は、**TSF** のふるまいと利用者から見えるインタフェースの上位の記述である。**TOE** セキュリティ機能要件を表すひとつの具体化である。機能仕様は、すべての **TOE** セキュリティ機能要件が説明されていることを示さなければならない。

コンポーネントのレベル付け

このファミリのコンポーネントは、機能仕様で要求される形式化の度合い、及び **TSF** の外部インタフェースで提供される詳細の度合いに基づいて、レベル付けされている。

適用上の注釈

このファミリの **ADV_FSP.*.2E** エレメントは、機能仕様が **TOE** セキュリティ機能要件の正確かつ完全に具体化したものであることを、評価者が決定する際の要件について規定する。これは、**ADV_RCR** ファミリで要求される **2** 者間の対応に加えて、**TOE** セキュリティ機能要件と機能仕様間の直接の対応を提供する。評価者は、この決定を行うための入力として、**ADV_RCR** で提供される証拠を用いることができ、そして完全性に対する要件は、機能仕様の抽象化の度合いに関連していることを意図している。

ADV_FSP.1.3C では、どのように **TOE** セキュリティ機能要件に向けて述べられているかを理解し、**ST** 中の **TOE** セキュリティ機能要件に対応するテストの仕様設定を可能とするために、機能仕様で十分な情報が提供されていることを意図している。このようなテストが、インタフェース部で生成されるであろう有り得るすべてのリターン値や誤りメッセージを網羅することは必ずしも必要としないが、インタフェースを用いたときの、成功時及び一般的な失敗時の結果は、提供された情報に明確になっていなければならない。

ADV_FSP.2.3C は、機能インタフェースの完全な表現に対する要件を規定している。これは、**TOE** の網羅テストと脆弱性評定の双方をサポートするために必要となる程度の詳細さを要求している。

非形式的、準形式的、形式的といった機能仕様の形式度は、階層的になるように考えられている。**ADV_FSP.1.1C** 及び **ADV_FSP.2.1C** では、適切な個所に対して非形式的な補足説明が付け加えられた、準形式的または形式的機能仕様の表現になっていてもよい。また、**ADV_FSP.3.1C** では、形式的機能仕様となっていてもよい。

ADV_FSP.1 非形式的機能仕様

依存性：

ADV_RCR.1　非形式的対応の実証

開発者アクションエレメント：

ADV_FSP.1.1D　開発者は、機能仕様を提供しなければならない。

証拠の内容・提示エレメント：

ADV_FSP.1.1C　機能仕様は、非形式的な様式で、TSF、及びその外部インタフェースを記述しなければならない。

ADV_FSP.1.2C　機能仕様は、内部的に一貫していなければならない。

ADV_FSP.1.3C　機能仕様は、効果、例外、及び誤りメッセージの詳細を適切に提供することにより、すべての外部TSFインタフェースの目的と使用方法を、記述しなければならない。

ADV_FSP.1.4C　機能仕様は、完全にTSFを表現しなければならない。

評価者アクションエレメント：

ADV_FSP.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_FSP.1.2E　評価者は、機能仕様が、TOEセキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_FSP.2　完全に定義された外部インタフェース

依存性：

ADV_RCR.1　非形式的対応の実証

開発者アクションエレメント：

ADV_FSP.2.1D 開発者は、機能仕様を提供しなければならない。

証拠の内容・提示エレメント：

ADV_FSP.2.1C 機能仕様は、非形式的な様式で、**TSF**、及びその外部インタフェースを記述しなければならない。

ADV_FSP.2.2C 機能仕様は、内部的に一貫していなければならない。

ADV_FSP.2.3C 機能仕様は、**すべての**効果、例外、及び誤りメッセージの**完全な**詳細を提供することにより、すべての外部**TSF**インタフェースの目的と使用方法を記述しなければならない。

ADV_FSP.2.4C 機能仕様は、完全に**TSF**を表現しなければならない。

ADV_FSP.2.5C **機能仕様は、TSFが完全に表現されている根拠を含んでいなければならない。**

評価者アクションエレメント：

ADV_FSP.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_FSP.2.2E 評価者は、機能仕様が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_FSP.3 準形式的機能仕様

依存性：

ADV_RCR.1 非形式的対応の実証

開発者アクションエレメント：

ADV_FSP.3.1D 開発者は、機能仕様を提供しなければならない。

証拠の内容・提示エレメント：

ADV_FSP.3.1C 機能仕様は、**適切な個所に対して非形式的で説明的なテキストによって補足**

される準形式的な様式で、**TSF**、及びその外部インタフェースを記述しなければならない。

ADV_FSP.3.2C 機能仕様は、内部的に一貫していなければならない。

ADV_FSP.3.3C 機能仕様は、すべての効果、例外及び誤りメッセージの完全な詳細を提供することにより、すべての外部**TSF**インタフェースの目的と使用方法を記述しなければならない。

ADV_FSP.3.4C 機能仕様は、完全に**TSF**を表現しなければならない。

ADV_FSP.3.5C 機能仕様は、**TSF**が完全に表現されている根拠を含んでいなければならない。

評価者アクションエレメント：

ADV_FSP.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_FSP.3.2E 評価者は、機能仕様が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_FSP.4 形式的機能仕様

依存性：

ADV_RCR.1 非形式的対応の実証

開発者アクションエレメント：

ADV_FSP.4.1D 開発者は、機能仕様を提供しなければならない。

証拠の内容・提示エレメント：

ADV_FSP.4.1C 機能仕様は、適切な個所に対して非形式的で説明的なテキストによって補足される**形式的な**様式で、**TSF**、及びその外部インタフェースを記述しなければならない。

ADV_FSP.4.2C 機能仕様は、内部的に一貫していなければならない。

ADV_FSP.4.3C 機能仕様は、すべての効果、例外及び誤りメッセージの完全な詳細を提供することにより、すべての外部**TSF**インタフェースの目的と使用方法を記述しなければならない。

ADV_FSP.4.4C 機能仕様は、完全に**TSF**を表現しなければならない。

ADV_FSP.4.5C 機能仕様は、**TSF**が完全に表現されている根拠を含んでいなければならない。

評価者アクションエレメント：

ADV_FSP.4.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_FSP.4.2E 評価者は、機能仕様が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

10.2 上位レベル設計 (ADV_HLD)

目的

TOE の上位レベル設計は、主要な構成単位（サブシステムなど）およびこれらの単位をこれらが提供する機能と関係付ける観点から **TSF** の記述を提供する。上位レベル設計要件は、**TOE** 機能要件の実装に適したアーキテクチャを **TOE** が提供することの保証を提供することを意図している。

上位レベル設計は、機能仕様をサブシステムに詳細化する。**TSF** の各サブシステムについて、上位レベル設計は、その目的、機能を記述し、サブシステムに含まれるセキュリティ機能を識別している。すべてのサブシステム間の相互の関係も、上位レベル設計で定義される。これらの相互関係は、データフロー、コントロールフローなどに対する外部インタフェースとして適切に表現される。

コンポーネントのレベル付け

このファミリのコンポーネントは、上位レベル設計で要求される形式化の度合い、及びインタフェース仕様で要求される詳細の度合いに基づいて、レベル付けされている。

適用上の注釈

開発者は、サブシステムの観点から **TSF** の設計を記述することが期待されている。“ サブシステム ” という用語は、ここでは、**TSF** を比較的少ない数のパーツに分解するという考えを表すのに用いられる。開発者が、“ サブシステム ” という形式が実際には必要とされていない場合でも、開発者は、同様なレベルに分解して表現することを期待されている。例えば、レイヤーや、ドメイン、またはサーバを用いて、設計を同様に分解できる。

“ セキュリティ機能性 ” という用語は、**TOE** で実装されるセキュリティ機能に寄与するために、**1** つのサブシステムが実行する操作の集合を表すために用いられる。この区別は、サブシステムやモジュールといった設計の構成要素が、必ずしも特定のセキュリティ機能に関係している必要がないため行われる。**1** つの与えられたサブシステムが、**1** つまたは複数のセキュリティ機能に直接対応している場合もあり得るが、多くのサブシステムが組み合わされた形で、**1** つのセキュリティ機能が実装されることも可能である。

“ **TSP** 実施サブシステム ” という用語は、直接間接を問わず、**TSP** の実施に貢献するようなサブシステムを示す。

このファミリの **ADV_FSP.*.2E** エレメントは、上位レベル設計が **TOE** セキュリティ機能要件の正確かつ完全な具体化であることを評価者が決定するための要件について規定する。これは、**ADV_RCR** ファミリで要求される **2** 者間の対応に加えて、**TOE** セキュリティ機能要件と上位レ

ベル設計間の直接の対応を提供する。評価者は、この決定を行うための入力として、**ADV_RCR** で提供される証拠を用いることが期待される。完全性への要件は、上位レベル設計の抽象化のレベルと関連することが意図されている。

ADV_HLD.3.8C は、サブシステムに対するインタフェースの完全な表現のための要件を表している。これは、（**ATE_DPT** のコンポーネントを用いた）**TOE** の徹底的なテストと脆弱性評定の両方をサポートするために必要な詳細を提供する。

非形式的、準形式的、形式的といった上位レベル設計の形式度は、階層的になるように考えられている。例えば、**ADV_HLD.1.1C** 及び **ADV_HLD.2.1C** は、準形式的または形式的な上位レベル設計にも適合し、**ADV_HLD.3.1C** 及び **ADV_HLD.4.1C** は、形式的上位レベル設計にも適合できる。

ADV_HLD.1 記述的上位レベル設計

依存性：

ADV_FSP.1　　非形式的機能仕様
ADV_RCR.1　　非形式的対応の実証

開発者アクションエレメント：

ADV_HLD.1.1D 開発者は、TSFの上位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_HLD.1.1C 上位レベル設計の表現は、非形式的でなければならない。

ADV_HLD.1.2C 上位レベル設計は、内部的に一貫していなければならない。

ADV_HLD.1.3C 上位レベル設計は、サブシステムの観点からTSFの構造を記述しなければならない。

ADV_HLD.1.4C 上位レベル設計は、TSFの個々のサブシステムによって提供されるセキュリティ機能性を記述しなければならない。

ADV_HLD.1.5C 上位レベル設計は、TSFが必要とするすべての下層のハードウェア、ファームウェア、及び/またはソフトウェアを、これらのハードウェア、ファームウェア、またはソフトウェアの中に実装されている補助的な保護メカニズムによって提供される機能の説明と共に、識別しなければならない。

ADV_HLD.1.6C **上位レベル設計は、TSFのサブシステムに対するすべてのインタフェースを識別しなければならない。**

ADV_HLD.1.7C **上位レベル設計は、外部から見えるTSFのサブシステムに対するインタフェースを識別しなければならない。**

評価者アクションエレメント：

ADV_HLD.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

ADV_HLD.1.2E **評価者は、上位レベル設計が、TOEセキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。**

ADV_HLD.2 セキュリティ実施上位レベル設計

依存性：

ADV_FSP.1	非形式的機能仕様
ADV_RCR.1	非形式的対応の実証

開発者アクションエレメント：

ADV_HLD.2.1D 開発者は、**TSF**の上位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_HLD.2.1C 上位レベル設計の表現は、非形式的でなければならない。

ADV_HLD.2.2C 上位レベル設計は、内部的に一貫していなければならない。

ADV_HLD.2.3C 上位レベル設計は、サブシステムの観点から**TSF**の構造を記述しなければならない。

ADV_HLD.2.4C 上位レベル設計は、**TSF**の個々のサブシステムによって提供されるセキュリティの機能性を記述しなければならない。

ADV_HLD.2.5C 上位レベル設計は、**TSF**が必要とするすべての下層のハードウェア、ファームウェア、及び/またはソフトウェアを、これらのハードウェア、ファームウェ

ア、またはソフトウェアの中に実装されている補助的な保護メカニズムによって提供される機能の説明と共に、識別しなければならない。

ADV_HLD.2.6C 上位レベル設計は、**TSF**のサブシステムに対するすべてのインタフェースを識別しなければならない。

ADV_HLD.2.7C 上位レベル設計は、外部から見える**TSF**のサブシステムに対するインタフェースを識別しなければならない。

ADV_HLD.2.8C 上位レベル設計は、効果、例外、及び誤りメッセージの詳細を適切に提供することにより、TSFのサブシステムに対するすべてのインタフェースの目的と使用方法を、記述しなければならない。

ADV_HLD.2.9C上位レベル設計は、TSP実施サブシステムとそれ以外のサブシステムに分けて、TOEを記述しなければならない。

評価者アクションエレメント：

ADV_HLD.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_HLD.2.2E 評価者は、上位レベル設計が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_HLD.3 準形式的上位レベル設計

依存性：

ADV_FSP.3　　準形式的機能仕様
ADV_RCR.2　　準形式的対応の実証

開発者アクションエレメント：

ADV_HLD.3.1D 開発者は、**TSF**の上位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_HLD.3.1C 上位レベル設計の表現は、**準形式的**でなければならない。

ADV_HLD.3.2C 上位レベル設計は、内部的に一貫していなければならない。

ADV_HLD.3.3C 上位レベル設計は、サブシステムの観点から**TSF**の構造を記述しなければならない。

ADV_HLD.3.4C 上位レベル設計は、**TSF**の個々のサブシステムによって提供されるセキュリティ機能性を記述しなければならない。

ADV_HLD.3.5C 上位レベル設計は、**TSF**が必要とするすべての下層のハードウェア、ファームウェア、及び/またはソフトウェアを、これらのハードウェア、ファームウェア、またはソフトウェアの中に実装されている補助的な保護メカニズムによって提供される機能の説明と共に、識別しなければならない。

ADV_HLD.3.6C 上位レベル設計は、**TSF**のサブシステムに対するすべてのインタフェースを識別しなければならない。

ADV_HLD.3.7C 上位レベル設計は、外部から見える**TSF**のサブシステムに対するインタフェースを識別しなければならない。

ADV_HLD.3.8C 上位レベル設計は、**すべての**効果、例外、及び誤りメッセージの**完全な**詳細を提供することにより、**TSF**のサブシステムに対するすべてのインタフェースの目的と使用方法を記述しなければならない。

ADV_HLD.3.9C上位レベル設計は、**TSP**実施サブシステムとそれ以外のサブシステムに分けて、**TOE**を記述しなければならない。

評価者アクションエレメント：

ADV_HLD.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_HLD.3.2E 評価者は、上位レベル設計が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_HLD.4 準形式的上位レベル説明

依存性：

ADV_FSP.3 準形式的機能仕様
ADV_RCR.2 準形式的対応の実証

開発者アクションエレメント：

ADV_HLD.4.1D 開発者は、**TSF**の上位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_HLD.4.1C 上位レベル設計の表現は、準形式的でなければならない。

ADV_HLD.4.2C 上位レベル設計は、内部的に一貫していなければならない。

ADV_HLD.4.3C 上位レベル設計は、サブシステムの観点から**TSF**の構造を記述しなければならない。

ADV_HLD.4.4C 上位レベル設計は、**TSF**の個々のサブシステムによって提供されるセキュリティ機能性を記述しなければならない。

ADV_HLD.4.5C 上位レベル設計は、**TSF**が必要とするすべての下層のハードウェア、ファームウェア、及び/またはソフトウェアを、これらのハードウェア、ファームウェア、またはソフトウェアの中に実装されている補助的な保護メカニズムによって提供される機能の説明と共に、識別しなければならない。

ADV_HLD.4.6C 上位レベル設計は、**TSF**のサブシステムに対するすべてのインタフェースを識別しなければならない。

ADV_HLD.4.7C 上位レベル設計は、外部から見える**TSF**のサブシステムに対するインタフェースを識別しなければならない。

ADV_HLD.4.8C 上位レベル設計は、すべての効果、例外、及び誤りメッセージの完全な詳細を提供することにより、**TSF**のサブシステムに対するすべてのインタフェースの目的と使用方法を記述しなければならない。

ADV_HLD.4.9C上位レベル設計は、**TSP**実施サブシステムとそれ以外のサブシステムに分けて、**TOE**を記述しなければならない。

ADV_HLD.4.10C **上位レベル設計は、分離を達成するための識別された手段が、非TSP実施機能からTSP実施機能の明確かつ効果的な分離を、すべての保護メカニズムも含めて、保証するのに十分であることを正当化しなければならない。**

ADV_HLD.4.11C **上位レベル設計は、TSFメカニズムが、上位レベル設計において識別されるセキュリティ機能を実装するために十分であることを正当化しなければならない。**

評価者アクションエレメント：

ADV_HLD.4.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_HLD.4.2E 評価者は、上位レベル設計が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_HLD.5 形式的上位レベル設計

依存性：

ADV_FSP.4　　形式的機能仕様
ADV_RCR.3　　形式的対応の実証

開発者アクションエレメント：

ADV_HLD.5.1D 開発者は、**TSF**の上位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_HLD.5.1C 上位レベル設計の表現は、**形式的**でなければならない。

ADV_HLD.5.2C 上位レベル設計は、内部的に一貫していなければならない。

ADV_HLD.5.3C 上位レベル設計は、サブシステムの観点から**TSF**の構造を記述しなければならない。

ADV_HLD.5.4C 上位レベル設計は、**TSF**の個々のサブシステムによって提供されるセキュリティ機能性を記述しなければならない。

ADV_HLD.5.5C 上位レベル設計は、**TSF**が必要とするすべての下層のハードウェア、ファームウェア、及び/またはソフトウェアを、これらのハードウェア、ファームウェア、またはソフトウェアの中に実装されている補助的な保護メカニズムによって提供される機能の説明と共に、識別しなければならない。

ADV_HLD.5.6C 上位レベル設計は、**TSF**のサブシステムに対するすべてのインタフェースを識別しなければならない。

ADV_HLD.5.7C 上位レベル設計は、外部から見える**TSF**のサブシステムに対するインタフェースを識別しなければならない。

ADV_HLD.5.8C 上位レベル設計は、すべての効果、例外、及び誤りメッセージの完全な詳細を提供することにより、**TSF**のサブシステムに対するすべてのインタフェースの目的と使用方法を記述しなければならない。

ADV_HLD.5.9C上位レベル設計は、**TSP**実施サブシステムとそれ以外のサブシステムに分けて、**TOE**を記述しなければならない。

ADV_HLD.5.10C上位レベル設計は、分離を達成するための識別された手段が、非**TSP**実施機能から**TSP**実施機能との明確かつ効果的な分離を、すべての保護メカニズムも含めて、保証するのに十分であることを正当化しなければならない。

ADV_HLD.5.11C上位レベル設計は、**TSF**メカニズムが、上位レベル設計において識別されるセキュリティ機能を実装するために十分であることを正当化しなければならない。

評価者アクションエレメント：

ADV_HLD.5.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_HLD.5.2E 評価者は、機能仕様が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

10.3　実装表現　(ADV_IMP)

目的

ソースコードや、ファームウェア、ハードウェア設計図面などの形態での実装表現の記述は、**TSF** の詳細な内部動作を表現しており、その分析に役立てる。

コンポーネントのレベル付け

このファミリのコンポーネントは、提供された実装表現の完全さと構造に基づいて、レベル付けされている。

適用上の注釈

実装表現は、最も抽象度の低い **TSF** 表現の表記法、特にそれ以上設計の詳細化なしに、それ自身で **TSF** を作るのに用いられるようなものを表現するのに用いる。すぐコンパイルされる状態にあるソースコード、または実際のハードウェアの製造に用いられるハードウェア図面は、実装表現の一部の例である。

評価者は、（脆弱性分析、テストカバレージ分析、または追加的な評価者によるテストの識別など）他の評価活動を直接的に支援するために、実装表現を用いることは可能である。**PP/ST** の作成者には、実装が完全であり、また **PP/ST** の中のその他のすべての要件に対する必要性に対して包括的に十分であることを要求するコンポーネントを選択することが望まれる。

ADV_IMP.1 TSF の実装のサブセット

適用上の注釈

ADV_IMP.1.1D は、開発者が **TSF** の一部分に対して実装表現を提供することを要求している。これは次の意味がある。**TSF** の少なくともある一部分に対するアクセスは、**TOE** のその部分**(**検証が、使用されたメカニズムの理解と保証を非常に高めることができる部分**)**に対する実装表現を検証する機会を評価者に与える。実装表現のサンプルの提供は、評価者に、詳細化を行う手法における保証を得るためのトレーサビリティの証拠をサンプルとして取得させ、そして実装表現自体の表現を評価させることにもなる。

ADV_IMP.1.2E エレメントは、抽象度の最も低い **TSF** 表現が **TOE** セキュリティ機能要件の正確かつ完全な具体化であることを評価者が決定する要件を定義する。これは、**ADV_RCR** ファミリで要求される **2** 者間の対応に加えて、**TOE** セキュリティ機能要件と抽象度の最も低い **TSF** 表現間の直接の対応を提供する。この決定をするための入力として **ADV_RCR** で提供される証拠を評価者が使用することを期待している。このコンポーネントに対する抽象度の最も低い

TSF 表現は、提供された実装表現と、対応する実装表現が提供されていない下位レベル設計の部分を合わせたものである。

依存性：

ADV_LLD.1	**記述的下位レベル設計**
ADV_RCR.1	**非形式的対応の実証**
ALC_TAT.1	**明確に定義された開発ツール**

開発者アクションエレメント：

ADV_IMP.1.1D **開発者は、TSFの選定された一部分について、実装表現を提供しなければならない。**

証拠の内容・提示エレメント：

ADV_IMP.1.1C **実装表現は、それ以上の設計上の決定を必要とせずに、TSFが生成されうるほどの詳細レベルまでTSFを曖昧さなく定義しなければならない。**

ADV_IMP.1.2C **実装表現は、内部的に一貫していなければならない。**

評価者アクションエレメント：

ADV_IMP.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

ADV_IMP.1.2E **評価者は、提供された最も抽象度が低いTSF表現が、TOEセキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。**

ADV_IMP.2　TSF の実装

適用上の注釈

ADV_IMP.2.2E エレメントは、実装表現が、**TOE** セキュリティ機能要件の正確かつ完全な具体化であることを評価者が決定する要件を定義する。これは、**ADV_RCR** ファミリで要求される **2** 者間の対応に加えて、**TOE** セキュリティ機能要件と実装表現の間で直接の対応を提供する。評価者は、この決定を行うための入力情報として、**ADV_RCR** が提供する証拠を使用するものと想定されている。

依存性：

ADV_LLD.1　記述的下位レベル設計
ADV_RCR.1　非形式的対応の実証
ALC_TAT.1　明確に定義された開発ツール

開発者アクションエレメント：

ADV_IMP.2.1D　開発者は、**TSF**全体の実装表現を提供しなければならない。

証拠の内容・提示エレメント：

ADV_IMP.2.1C　実装表現は、それ以上の設計上の決定を必要とせずに、**TSF**を生成できるような詳細レベルまで**TSF**を曖昧さなく定義しなければならない。

ADV_IMP.2.2C　実装表現は、内部的に一貫していなければならない。

ADV_IMP.2.3C　**実装表現は、実装のすべての部分の関係を記述しなければならない。**

評価者アクションエレメント：

ADV_IMP.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_IMP.2.2E　評価者は、**実装表現**が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_IMP.3　TSF の構造化実装

適用上の注釈

ADV_IMP.3.2E エレメントは、実装表現が、**TOE** セキュリティ機能要件の正確かつ完全な具体化であることを評価者が決定する要件を定義する。これは、**ADV_RCR** ファミリで要求される **2** 者間の対応に加えて、**TOE** セキュリティ機能要件と実装表現の間で直接の対応を提供する。評価者は、この決定を行うための入力情報として、**ADV_RCR** が提供する証拠を使用するものと想定されている。

依存性：

ADV_INT.1　モジュール方式

ADV_LLD.1 記述的下位レベル設計
ADV_RCR.1 非形式的対応の実証
ALC_TAT.1 明確に定義された開発ツール

開発者アクションエレメント：

ADV_IMP.3.1D 開発者は、**TSF**全体の実装表現を提供しなければならない。

証拠の内容・提示エレメント：

ADV_IMP.3.1C 実装表現は、それ以上の設計上の決定を必要とせずに、**TSF**を生成できるような詳細レベルまで**TSF**を曖昧さなく定義しなければならない。

ADV_IMP.3.2C 実装表現は、内部的に一貫性がなければならない。

ADV_IMP.3.3C 実装表現は、実装のすべての部分の関係を記述しなければならない。

ADV_IMP.3.4C 実装表現は、小さく理解可能なセクションに構造化されなければならない。

評価者アクションエレメント：

ADV_IMP.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_IMP.3.2E 評価者は、実装表現が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

10.4　TSF内部構造（ADV_INT）

目的

このファミリは、**TSF** の内部構造を扱う。要件は、モジュール性、階層化（抽象のレベルを分離し、循環的な依存性を最小にする）、方針実施メカニズムの複雑さの最小化、**TSF** 内の **TSP** 実施機能以外の量の最小化に対して表される。その結果、簡単に分析できる **TSF** となる。

モジュール設計は、**TSF** 要素の間の相互依存性を減らし、**1** つのモジュールの変更または誤りが、**TOE** 全体に影響を与えるリスクを減らす。そこで、モジュール設計は、**TSF** の他の要素との相互作用の範囲を決定する基礎を提供し、予期しない結果が起きないことの保証を高めると共に、テストセットを設計、評価する基礎を提供する。

TSP 実施機能に対する階層化と単純な設計の使用は、**TSF** の複雑さを減らす。次にこれは、**TSF** を理解し易いものにし、**TOE** セキュリティ機能要件が実装において正確かつ完全に実現されることの保証を高める。

TSP を実施しない **TSF** 内の機能の量を最小にすることは、**TSF** 内の欠陥の可能性を減らす。モジュール方式と階層構造を組み合わせることにより、評価者は、**TSP** の実施に必要な機能だけに焦点を絞ることが可能になる。

設計上の複雑さを最小にすることは、コードが理解されるという保証に貢献する。つまり、**TSF** のコードの複雑さが減れば減るほど、それだけ **TSF** の設計の理解は高まる。設計上の複雑さの最小化は、参照検証メカニズムの主要な特質である。

コンポーネントのレベル付け

このファミリのコンポーネントは、必要となる構造と最小化の量に基づいて、レベル付けされている。

適用上の注釈

「**TSF** の部分」の用語は、使用可能な **TSF** 表現に基づき各種の詳細を備えた **TSF** の部分を表すために使用される。機能仕様はインタフェースの観点から識別を可能にし、上位レベル設計はサブシステムの観点から識別を可能にし、下位レベル設計はモジュールの観点から識別を可能にし、そして実装表現は実装単位の観点から識別を可能にする。

ADV_INT.2.5C と **ADV_INT.3.5C** エレメントは、階層間の相互作用の最小化に対応する。それでもなお、階層間で相互作用を行うことは可能であるが、そのような場合、開発者は、これらの相互作用が必要であり、合理的に回避できないことを実証しなければならない。

ADV_INT.2.6C は、**TSP** に識別されているアクセス制御及び/または情報フロー制御方針を実施する **TSF** の部分の複雑さを最小にすることを要求することにより、参照モニタの概念を導入する。**ADV_INT.3.6C** は、**TSF** 全体の複雑さを最小にすることを要求することにより、参照モニタの概念をさらに発展させる。

このファミリのコンポーネントの中のいくつかのエレメントは、アーキテクチャの記述と呼ばれる。アーキテクチャの記述は、下位レベル設計と同様の抽象レベルにあり、**TSF** のモジュールに関係する。下位レベル設計は、**TSF** のモジュールの設計を記述するが、アーキテクチャの記述の目的は、適用される **TSF** のモジュール方式、階層構造、複雑さの最小化の証拠を提供することである。下位レベル設計と実装表現の両方は、これらの **TSF** 表現が必要なモジュール方式と階層構造を備え、複雑さが最小化されていることの保証を提供するために、アーキテクチャの記述に適合する必要がある。

ADV_INT.1　モジュール方式

依存性：

ADV_IMP.1　TSF の実装のサブセット
ADV_LLD.1　記述的下位レベル設計

開発者アクションエレメント：

ADV_INT.1.1D　開発者は、設計のモジュール間の不要な相互作用を避けるモジュール方式でTSFを設計し、構造化しなければならない。

ADV_INT.1.2D　開発者は、アーキテクチャの記述を提供しなければならない。

証拠の内容・提示エレメント：

ADV_INT.1.1C　アーキテクチャの記述は、TSFのモジュールを識別しなければならない。

ADV_INT.1.2C　アーキテクチャの記述は、TSFの各モジュールの目的、インタフェース、パラメタ、及び効果を記述しなければならない。

ADV_INT.1.3C　アーキテクチャの記述は、TSF設計が不要な相互作用を避けるために大部分が独立したモジュールを提供する方法を記述しなければならない。

評価者アクションエレメント：

ADV_INT.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満

たしていることを確認しなければならない。

ADV_INT.1.2E　評価者は、下位レベル設計と実装表現の両方が、アーキテクチャの記述に適合していることを決定しなければならない。

ADV_INT.2　複雑さの軽減

適用上の注釈

このコンポーネントは、**TSP** で識別されているアクセス制御及び/または情報フロー制御方針を実施する **TSF** の部分の複雑さを最小にすることを要求することにより、参照モニタの概念を導入する。

依存性：

ADV_IMP.1　**TSF** の実装のサブセット
ADV_LLD.1　記述的下位レベル設計

開発者アクションエレメント：

ADV_INT.2.1D　開発者は、設計のモジュール間の不要な相互作用を避けるモジュール方式で**TSF**を設計し、構造化しなければならない。

ADV_INT.2.2D　開発者は、アーキテクチャの記述を提供しなければならない。

ADV_INT.2.3D　開発者は、設計の階層間の相互作用を最小にする階層方式でTSFを設計し、構造化しなければならない。

ADV_INT.2.4D　開発者は、アクセス制御及び/または情報フロー制御方針を実施するTSFの部分の複雑さを最小にする方法でTSFを設計し、構造化しなければならない。

証拠の内容・提示エレメント：

ADV_INT.2.1C　アーキテクチャの記述は、**TSF**のモジュールを識別し、**アクセス制御及び/または情報フロー制御方針を実施するTSFの部分を特定**しなければならない。

ADV_INT.2.2C　アーキテクチャの記述は、**TSF**の各モジュールの目的、インタフェース、パラメタ、及び効果を記述しなければならない。

ADV_INT.2.3C　アーキテクチャの記述は、**TSF**設計が不要な相互作用を避けるために大部分が

独立したモジュールを提供する方法を記述しなければならない。

ADV_INT.2.4C　アーキテクチャの記述は、階層構造アーキテクチャを記述しなければならない。

ADV_INT.2.5C　アーキテクチャの記述は、相互作用が最小化されていることを示し、それらがそのように留まることを正当化しなければならない。

ADV_INT.2.6C　アーキテクチャの記述は、アクセス制御及び/または情報フロー制御方針を実施するTSFの部分が、複雑さを最小化するためにどのように構造化されているかを記述しなければならない。

評価者アクションエレメント：

ADV_INT.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_INT.2.2E　評価者は、下位レベル設計と実装表現の両方が、アーキテクチャの記述に適合していることを決定しなければならない。

ADV_INT.3　複雑さの最小化

適用上の注釈

このコンポーネントは、参照モニタ特性「簡単で分析が可能」が完全に対応されることを要求する。このコンポーネントが、機能要件 **FPT_RVM.1** 及び **FPT_SEP.3** と組み合わされるとき、参照モニタの概念が完全に実現される。

依存性：

ADV_IMP.2　TSF の実装
ADV_LLD.1　記述的下位レベル設計

開発者アクションエレメント：

ADV_INT.3.1D　開発者は、設計のモジュール間の不要な相互作用を避けるモジュール方式でTSFを設計し、構造化しなければならない。

ADV_INT.3.2D　開発者は、アーキテクチャの記述を提供しなければならない。

ADV_INT.3.3D 開発者は、設計の階層間の相互作用を最小にする階層方式で**TSF**を設計し、構造化しなければならない。

ADV_INT.3.4D 開発者は、**TSF全体**の複雑さを最小にする方法で**TSF**を設計し、構造化しなければならない。

ADV_INT.3.5D **開発者は、すべてのアクセス制御及び/または情報フロー制御方針を実施するTSFの部分を、それらが簡単で分析が可能になるように設計し、構造化しなければならない。**

ADV_INT.3.6D **開発者は、目的がTSFに関係しない機能が、TSFモジュールから除外されていることを保証しなければならない。**

証拠の内容・提示エレメント：

ADV_INT.3.1C アーキテクチャの記述は、**TSF**のモジュールを識別し、アクセス制御及び/または情報フロー制御方針を実施する**TSF**の部分を特定しなければならない。

ADV_INT.3.2C アーキテクチャの記述は、**TSF**の各モジュールの目的、インタフェース、パラメタ、及び効果を記述しなければならない。

ADV_INT.3.3C アーキテクチャの記述は、**TSF**設計が不要な相互作用を避けるために大部分が独立したモジュールを提供する方法を記述しなければならない。

ADV_INT.3.4Cアーキテクチャの記述は、階層構造アーキテクチャを記述しなければならない。

ADV_INT.3.5C アーキテクチャの記述は、相互作用が最小化されていることを示し、それらがそのように留まることを正当化しなければならない。

ADV_INT.3.6C アーキテクチャの記述は、複雑さを最小化するために**TSF全体が**どのように構造化されているかを記述しなければならない。

ADV_INT.3.7C **アーキテクチャの記述は、TSFにTSP実施モジュール以外を含めることを正当化しなければならない。**

(訳者注：**ADV_INT.3.2C**の「効果」の原文は、**side-effects**であるが**effectts**の誤りとして訳す。**)**

評価者アクションエレメント：

ADV_INT.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_INT.3.2E 評価者は、下位レベル設計と実装表現の両方が、アーキテクチャの記述に適合していることを決定しなければならない。

ADV_INT.3.3E **評価者は、アクセス制御及び/または情報フロー制御方針を実施するTSFの部分が単純であり、分析が可能であることを確認しなければならない。**

10.5 下位レベル設計 (ADV_LLD)

目的

TOE の下位レベル設計は、モジュール、それらの相互関係及び依存関係の観点から **TSF** の内部動作の記述を提供する。下位レベル設計は、**TSF** サブシステムが、正確かつ効果的に詳細化されていることの保証を提供する。

下位レベル設計は、**TSF** の各モジュールについて、その目的、機能、インタフェース、依存関係、及び **TSP** 実施機能の実装を記述する。

コンポーネントのレベル付け

このファミリのコンポーネントは、下位レベル設計で要求される形式化の度合い、及びインタフェース仕様で要求される詳細の度合いに基づいて、レベル付けされている。

適用上の注釈

“**TSP** 実施モジュール”という用語は、**TSP** の正しい実施のために信頼されなければならないあらゆるモジュールを示す。

“セキュリティ機能性”という用語は、**TOE** で実装されるセキュリティ機能に寄与するために、１つのモジュールが実行する操作の集合を表すために用いられる。この区別は、モジュールが、必ずしも特定のセキュリティ機能に関連している必要がないため行われる。一つの与えられたモジュールが、**1** つまたは複数のセキュリティ機能に直接対応している場合もあり得るが、多くのモジュールが組み合わされる形で、**1** つのセキュリティ機能が実装されることも可能である。

ADV_LLD.*.6C エレメントは、下位レベル設計がどのように各 **TSP** 実施機能を提供しているか記述すること要求する。この要件は、各々のモジュールが設計展望からどのように実装されていることが期待されるかの記述を、下位レベル設計が提供することを意図している。

ADV_LLD.*.2E エレメントは、下位レベル設計が **TOE** セキュリティ機能要件の正確かつ完全な実現であることを、評価者が決定する要件を定義する。これは、**ADV_RCR** ファミリで要求される対ごとの対応関係に加えて、**TOE** セキュリティ機能と下位レベル設計の間で直接的な対応関係を提供する。評価者は、この判断を行う入力として **ADV_RCR** で提供される証拠を使用することが期待される。そして完全性への要件は、下位レベル設計の抽象度のレベルと関連することが意図されている。

ADV_LLD.2.9C は、モジュールに対するインタフェースの完全な表現のための要件を表している。これは、**(ATE_DPT** からのコンポーネントを使用して**)TOE** の徹底的なテストと脆弱性評定の両方をサポートするために必要な詳細を提供する。

非形式的、準形式的、形式的はといった下位レベル設計の形式度は、階層的になるように考えられている。例えば、**ADV_LLD.1.1C** は、準形式的または形式的な下位レベル設計にも適合し、**ADV_LLD.2.1C** は、形式的下位レベル設計にも適合できる。

ADV_LLD.1　記述的下位レベル設計

依存性：

ADV_HLD.2　セキュリティ実施上位レベル設計
ADV_RCR.1　非形式的な対応の実証

開発者アクションエレメント：

ADV_LLD.1.1D　開発者は、TSFの下位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_LLD.1.1C　下位レベル設計の表現は、非形式的でなければならない。

ADV_LLD.1.2C　下位レベル設計は、内部的に一貫していなければならない。

ADV_LLD.1.3C　下位レベル設計は、モジュールの観点からTSFを記述しなければならない。

ADV_LLD.1.4C　下位レベル設計は、各々のモジュールの目的を記述しなければならない。

ADV_LLD.1.5C　下位レベル設計は、提供されるセキュリティ機能性と他のモジュールへの依存関係の観点からモジュール間の関係を定義しなければならない。

ADV_LLD.1.6C　下位レベル設計は、各々のTSP実施機能がどのように提供されるかを記述しなければならない。

ADV_LLD.1.7C　下位レベル設計は、TSFのモジュールに対するすべてのインタフェースを識別しなければならない。

ADV_LLD.1.8C　下位レベル設計は、外部から見えるTSFのモジュールに対するインタフェースを識別しなければならない。

ADV_LLD.1.9C　下位レベル設計は、効果、例外、及び誤りメッセージの詳細を適切に提供することにより、TSFのモジュールに対するすべてのインタフェースの目的と使

用方法を、記述しなければならない。

ADV_LLD.1.10C　下位レベル設計は、TSP実施モジュールとそれ以外のモジュールに分けて、TOEを記述しなければならない。

評価者アクションエレメント：

ADV_LLD.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_LLD.1.2E　評価者は、下位レベル設計が、TOEセキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_LLD.2　準形式的な下位レベル設計

依存性：

ADV_HLD.3　準形式的な上位レベル設計
ADV_RCR.2　準形式的な対応の実証

開発者アクションエレメント：

ADV_LLD.2.1D　開発者は、**TSF**の下位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_LLD.2.1C　下位レベル設計の表現は、**準形式的**でなければならない。

ADV_LLD.2.2C　下位レベル設計は、内部的に一貫していなければならない。

ADV_LLD.2.3C　下位レベル設計は、モジュールの観点から**TSF**を記述しなければならない。

ADV_LLD.2.4C　下位レベル設計は、各々のモジュールの目的を記述しなければならない。

ADV_LLD.2.5C　下位レベル設計は、提供されるセキュリティ機能性と他のモジュールへの依存関係の観点からモジュール間の関係を定義しなければならない。

ADV_LLD.2.6C　下位レベル設計は、各々の**TSP**実施機能がどのように提供されるかを記述しなければならない。

ADV_LLD.2.7C　下位レベル設計は、**TSF**のモジュールに対するすべてのインタフェースを識別しなければならない。

ADV_LLD.2.8C　下位レベル設計は、外部から見える**TSF**のモジュールに対するインタフェースを識別しなければならない。

ADV_LLD.2.9C　下位レベル設計は、**すべての**効果、例外、及び誤りメッセージの**完全な**詳細を提供することにより、**TSF**のモジュールに対するすべてのインタフェースの目的と使用方法を記述しなければならない。

ADV_LLD.2.10C　下位レベル設計は、**TSP**実施に係わるモジュールとそれ以外のモジュールに分けて、**TOE**を記述しなければならない。

評価者アクションエレメント：

ADV_LLD.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_LLD.2.2E　評価者は、下位レベル設計が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

ADV_LLD.3　形式的な下位レベル設計

依存性：

ADV_HLD.5　形式的な上位レベル設計
ADV_RCR.3　形式的な対応の実証

開発者アクションエレメント：

ADV_LLD.3.1D　開発者は、**TSF**の下位レベル設計を提供しなければならない。

証拠の内容・提示エレメント：

ADV_LLD.3.1C　下位レベル設計の表現は、**形式的**でなければならない。

ADV_LLD.3.2C　下位レベル設計は、内部的に一貫していなければならない。

ADV_LLD.3.3C　下位レベル設計は、モジュールの観点から**TSF**を記述しなければならない。

ADV_LLD.3.4C 下位レベル設計は、各々のモジュールの目的を記述しなければならない。

ADV_LLD.3.5C 下位レベル設計は、提供されるセキュリティ機能性と他のモジュールへの依存関係の観点からモジュール間の関係を定義しなければならない。

ADV_LLD.3.6C 下位レベル設計は、各々の**TSP**実施機能がどのように提供されるかを記述しなければならない。

ADV_LLD.3.7C 下位レベル設計は、**TSF**のモジュールに対するすべてのインタフェースを識別しなければならない。

ADV_LLD.3.8C 下位レベル設計は、外部から見える**TSF**のモジュールに対するインタフェースを識別しなければならない。

ADV_LLD.3.9C 下位レベル設計は、すべての効果、例外、及び誤りメッセージの完全な詳細を提供することにより、**TSF**のモジュールに対するすべてのインタフェースの目的と使用方法を記述しなければならない。

ADV_LLD.3.10C 下位レベル設計は、**TSP**実施に係わるモジュールとそれ以外のモジュールに分けて、**TOE**を記述しなければならない。

評価者アクションエレメント：

ADV_LLD.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_LLD.3.2E 評価者は、下位レベル設計が、**TOE**セキュリティ機能要件の正確かつ完全な具体化であることを決定しなければならない。

10.6 表現対応 (ADV_RCR)

目的

種々の **TSF** 表現**(**すなわち、**TOE** 要約仕様、機能仕様、上位レベル設計、下位レベル設計、実装表現**)**の間の対応は、提供された最も抽象度の低い **TSF** 表現に対し、正確かつ完全な要件の実装をゆだねる。この結論は、すべての隣接した表現の抽象概念の間で、段階的に詳細化し、対応関係決定の累積の結果で達成される。

コンポーネントのレベル付け

このファミリのコンポーネントは、種々の **TSF** 表現の間の対応の形式化の要求されるレベルに基づいて、レベル付けされている。

適用上の注釈

開発者は、評価者に対して、提供された最も詳細なまたは最も抽象度の低い **TSF** 表現が、**ST** 中の機能要件として明示された機能の、正確で、一貫した、完全な実現であることを実証しなければならない。これは、隣接する表現の間の対応を、同じ度合いの厳密さで示すことによって達成される。

このファミリの要件は、**TSP** モデルや **TSP** に関係する対応関係を示すことを意図していない。むしろ、図 **10.2** に示すように、提供された種々の **TSF** 表現**(**すなわち、**TOE** 要約仕様、機能仕様、上位レベル設計、下位レベル設計、実装表現**)**の間での対応を示すことを意図している。

ADV_RCR.*.1C エレメントは、隣接する **TSF** 表現の間で詳細化されるべきものの範囲の定義において、“ すべての関連したセキュリティ機能性 ” を参照している。**TOE** 要約仕様と機能仕様の間で詳細化のために、このエレメントは、**TOE** 要約仕様の **TOE** セキュリティ機能が、機能仕様で詳細化されることのみ要求し、**(TOE** 要約仕様で与えられる**)**保証手段について詳細を機能仕様に含めることは要求していない。実装表現が、**TSF** のサブセットのみが提供される場合**(ADV_IMP.1)**、下位レベル設計と実装表現の間で要求される詳細化は、実装表現で提供されるセキュリティ機能性に限定される。他のすべての場合、このエレメントは、より抽象度の高い **TSF** 表現のすべての部分が、抽象度の低い **TSF** 表現にて詳細化されることを要求している。

非形式的、準形式的、形式的といった隣接した **TSF** 表現の間の対応の形式度は、階層的になるように考えられている。例えば、**ADV_RCR2.2C** 及び **ADV_RCR3.2C** は、形式的な対応の証明にも適合し、その形式度のレベルにおける要件がない場合は、対応の実証は、非形式的、準形式的、または形式的にしてもかまわない。

ADV_RCR.1　非形式的対応の実証

依存性： なし

開発者アクションエレメント：

ADV_RCR.1.1D **開発者は、提供するTSF表現の隣接するすべての組の間の対応の分析を提供しなければならない。**

証拠の内容・提示エレメント：

ADV_RCR.1.1C **提供されたTSF表現の隣接する各々の組に対し、分析は、より抽象度の高いTSF表現のすべての関連するセキュリティ機能性が、抽象度の低いTSF表現に、正確かつ完全に詳細化されていることを実証しなければならない。**

評価者アクションエレメント：

ADV_RCR.1.1E **評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

ADV_RCR.2　準形式的対応の実証

依存性： なし

開発者アクションエレメント：

ADV_RCR.2.1D 開発者は、提供する**TSF**表現のすべての隣接する組の間の対応の分析を提供しなければならない。

証拠の内容・提示エレメント：

ADV_RCR.2.1C 提供された**TSF**表現の隣接する各々の組に対し、分析は、より抽象度の高い**TSF**表現のすべての関連するセキュリティ機能性が、抽象度の低い**TSF**表現に、正確かつ完全に詳細化されていることを実証しなければならない。

ADV_RCR.2.2C **提供されたTSF表現の隣接する各々の組に対し、どちらの表現も最低限、準形式的である部分に対しては、表現のそれらの部分の間の対応の実証は、準**

形式的でなければならない。

評価者アクションエレメント：

ADV_RCR.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_RCR.3　形式的対応の実証

適用上の注釈

開発者は、以下の要件に示すように、表現形式の厳密さのレベルとつりあったレベルで、対応関係を実証するか証明しなければならない。例えば、対応する表現がともに形式的に示されている場合は、対応関係が証明されなければならない。

依存性： なし

開発者アクションエレメント：

ADV_RCR.3.1D 開発者は、提供する**TSF**表現の隣接するすべての組の間の対応の分析を提供しなければならない。

ADV_RCR.3.2D **対応する表現がともに形式的である部分については、開発者は、対応を証明しなければならない。**

証拠の内容・提示エレメント：

ADV_RCR.3.1C 提供された**TSF**表現の隣接する各々の組に対し、分析は、より抽象度の高い**TSF**表現のすべての関連するセキュリティ機能が、抽象度の低い**TSF**表現に、正確かつ完全に詳細化されていることを**証明または**実証しなければならない。

ADV_RCR.3.2C 提供された**TSF**表現の隣接する各々の組に対し、**一方の**表現が**準形式的で、そして他方が**最低限、準形式的である部分に対しては、それらの間での対応の実証は、準形式的でなければならない。

ADV_RCR.3.3C **提供されたTSF表現の隣接する各々の組に対し、どちらの表現も形式的である部分で、それらの部分の間での対応の証明は、形式的でなければならない。**

評価者アクションエレメント：

ADV_RCR.3.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_RCR.3.2E　**評価者は、形式的な分析を選択的に検証することによって、対応の証明の正確さを決定しなければならない。**

10.7 セキュリティ方針モデル化 (ADV_SPM)

目的

このファミリの目的は、機能仕様におけるセキュリティ機能が、**TSP** 中の方針を実施することの追加的な保証を提供することである。これは、**TSP** の方針のサブセットに基づくセキュリティ方針モデルの開発し、また機能仕様、セキュリティ方針モデルと **TSP** の方針の間の対応を確立することにより、達成される。

コンポーネントのレベル付け

このファミリのコンポーネントは、**TSP** モデルで要求される形式化の度合い、及び **TSP** モデルと機能仕様の間の対応で要求される形式化の度合いに基づいて、レベル付けされている。

適用上の注釈

TSP はどのような方針を含めても良いが、ある種の方針のモデル化は現状の技術ではできないため、それらの方針のサブセットに対してだけ、**TSP** モデルが伝統的に表現されている。現状の技術が、モデル化できる方針を決定する、そして **PP/ST** 作成者は、モデル化が可能であり、従って、モデル化を要求される特定の機能とそれに関連する方針を識別しなければならない。最低、アクセス制御方針と情報フロー制御方針**(**それらが **TSP** の部分である場合**)**は、技術の範囲内であるので、モデル化することを要求されている。

このファミリの各々のコンポーネントは、**TSP** モデル中にある、**TSP** の適用可能な方針の規則と特質を記述し、また **TSP** モデルが **TSP** の対応する方針を満足することを保証する要件を含む。**TSP** モデルの“規則”と“特質”は、開発されるモデルのタイプ**(**例えば、状態遷移、非干渉**)**に柔軟性を許すことを意図している。例えば、規則は、“特性”**(**例えば、簡単なセキュリティ特性**)**で表現して良いし、また特質は、“初期状態”、“セキュアな状態”、“サブジェクト”、“オブジェクト”のような定義として表現して良い。

非形式的、準形式的、形式的といった **TSP** モデル、及び **TSP** モデルと機能仕様の間で対応の形式化のレベルは、階層的になるように考えられている。例えば、**ADV_SPM.1.1C** は、準形式的または形式的な **TSP** モデルにも適合し、**ADV_SPM.2.1C** は、形式的な **TSP** モデルにも適合できる。さらに、**ADV_SPM.2.5C** 及び **ADV_SPM.3.5C** は、形式的な対応の証明にも適合できる。最後に、その形式度のレベルにおける要件がない場合は、対応の実証は、非形式的、準形式的、または形式的のいずれでもよい。

ADV_SPM.1　非形式的な TOE セキュリティ方針モデル

依存性：

ADV_FSP.1　非形式的な機能仕様

開発者アクションエレメント：

ADV_SPM.1.1D 開発者は、TSPモデルを提供しなければならない。

ADV_SPM.1.2D 開発者は、機能仕様とTSPモデルの間の対応を実証しなければならない。

証拠の内容・提示エレメント：

ADV_SPM.1.1C TSPモデルは、非形式的でなければならない。

ADV_SPM.1.2C TSPモデルは、モデル化できるすべてのTSP方針の規則と特質を記述しなければならない。

ADV_SPM.1.3C TSPモデルは、モデル化できるすべてのTSP方針に関して、一貫し完全であることを実証する根拠を含まなければならない。

ADV_SPM.1.4C TSPモデルと機能仕様の間の対応の実証は、機能仕様におけるセキュリティ機能のすべてが、TSPモデルに関して、一貫し完全であることを示さなければならない。

評価者アクションエレメント：

ADV_SPM.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_SPM.2　準形式的な TOE セキュリティ方針モデル

依存性：

ADV_FSP.1　非形式的な機能仕様

開発者アクションエレメント：

ADV_SPM.2.1D 開発者は、**TSP**モデルを提供しなければならない。

ADV_SPM.2.2D 開発者は、機能仕様と**TSP**モデルの間の対応を実証しなければならない。

証拠の内容・提示エレメント：

ADV_SPM.2.1C **TSP**モデルは、**準形式的**でなければならない。

ADV_SPM.2.2C **TSP**モデルは、モデル化できるすべての**TSP**方針の規則と特質を記述しなければならない。

ADV_SPM.2.3C **TSP**モデルは、モデル化できるすべての**TSP**方針に関して、一貫し完全であることを実証する根拠を含まなければならない。

ADV_SPM.2.4C **TSP**モデルと機能仕様の間の対応の実証は、機能仕様におけるセキュリティ機能のすべてが、**TSP**モデルに関して、一貫し完全であること示さなければならない。

ADV_SPM.2.5C **機能仕様が少なくとも準形式的な場合、TSPモデルと機能仕様の間の対応の実証は、準形式的でなければならない。**

評価者アクションエレメント：

ADV_SPM.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ADV_SPM.3　形式的な TOE セキュリティ方針モデル

依存性：

ADV_FSP.1　非形式的な機能仕様

開発者アクションエレメント：

ADV_SPM.3.1D 開発者は、**TSP**モデルを提供しなければならない。

ADV_SPM.3.2D 開発者は、機能仕様と**TSP**モデルの間の対応を実証するか、**または適切に証明**しなければならない。

証拠の内容・提示エレメント：

ADV_SPM.3.1C **TSP**モデルは、**形式的で**なければならない。

ADV_SPM.3.2C **TSP**モデルは、モデル化できるすべての**TSP**方針の規則と特質を記述しなければならない。

ADV_SPM.3.3C **TSP**モデルは、モデル化できるすべての**TSP**方針に関して、一貫し完全であることを実証する根拠を含まなければならない。

ADV_SPM.3.4C **TSP**モデルと機能仕様の間の対応の実証は、機能仕様におけるセキュリティ機能のすべてが、**TSP**モデルに関して、一貫し完全であること示さなければならない。

ADV_SPM.3.5C 機能仕様が**準形式的**な場合、**TSP**モデルと機能仕様の間の対応の実証は、準形式的でなければならない。

ADV_SPM.3.6C **機能仕様が、形式的な場合、TSPモデルと機能仕様の間の対応の証明は、形式的でなければならない。**

評価者アクションエレメント：

ADV_SPM.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

11　AGDクラス：ガイダンス文書

ガイダンス文書クラスは、利用者と管理者のガイダンス証拠資料に対する要求を提供する。**TOE** をセキュアに管理し使用するため、**TOE** のセキュアなアプリケーションについての、すべての関連する側面を記述することが必要である。

図 11.1 は、このクラスのファミリと、各ファミリのコンポーネントの階層を示す。

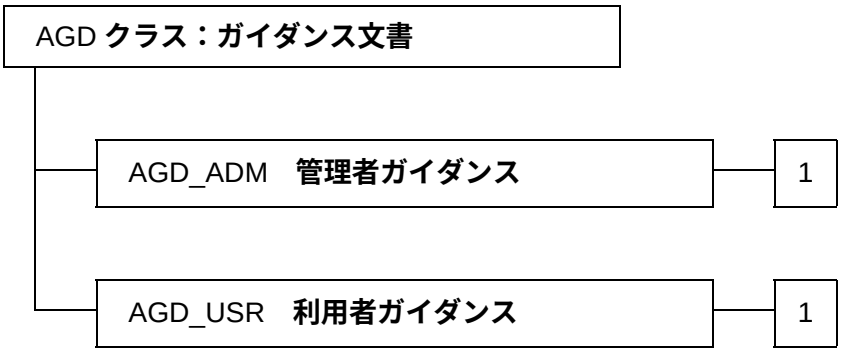

図 11.1 ― ガイダンス文書クラスのコンポーネント構成

11.1　管理者ガイダンス (AGD_ADM)

目的

管理者ガイダンスは、最大のセキュリティが得られるよう、正しい方法で **TOE** を構成し、保守し、管理することに責任のある人たちに使用されることを目的として書かれた文書である。
TOE のセキュアな運用は、**TSF** が正しく実行されることによるので、これらの機能を実施する責任のある人たちは、**TSF** に信頼されている。
管理者ガイダンスは、**TOE** により提供されるセキュリティ機能を管理者が理解できるように助けることを目的としている。管理者がセキュリティ上の重大な行為を遂行するために必要な機能や、セキュリティ上の重大な情報を提供するための機能などを含んでいる。

コンポーネントのレベル付け

このファミリは、ただ **1** つのコンポーネントより成る。

適用上の注釈

AGD_ADM.1.3C 及び **AGD_ADM.1.7C** の要件は、**PP/ST** に記述されている **TOE** セキュリティ環境とセキュリティ対策方針に関する **TOE** の利用者へのあらゆる警告が、適切に管理者ガイダンスに記述されていることを包含する。

AGD_ADM.1.5C で述べられたセキュアな値という概念は、管理者がセキュリティパラメタを管理しているということに関連する。ガイダンスは、このようなパラメタについて、セキュアな及びセキュアでない設定が記述される必要がある。この考えは、**CC** パート **2** のコンポーネント **FMT_MSA.2** の使用に関連する。

AGD_ADM.1　管理者ガイダンス

依存性：

ADV_FSP.1　非形式な機能仕様書

開発者アクションエレメント：

AGD_ADM.1.1D　開発者は、システム管理者向けに、管理者ガイダンスを提供しなければならない。

証拠の内容・提示エレメント：

AGD_ADM.1.1C 管理者ガイダンスは、TOEの管理者が利用できる管理機能とインタフェース

を記述しなければならない。

AGD_ADM.1.2C 管理者ガイダンスは、管理者がセキュアにTOEを管理する方法を記述しなければならない。

AGD_ADM.1.3C 管理者ガイダンスは、セキュアな処理環境において管理されなければならない機能と権限についての警告を含まなければならない。

AGD_ADM.1.4C 管理者ガイダンスは、TOEのセキュアな運用に関連する利用者のふるまいについてのすべての前提条件を記述しなければならない。

AGD_ADM.1.5C 管理者ガイダンスは、管理者の管理下にあるすべてのセキュリティパラメタを、適切にセキュアな値を示して、記述しなければならない。

AGD_ADM.1.6C 管理者ガイダンスは、TSFの制御下にあるセキュリティ特質の変更を含む、実行が必要な管理機能に関連するセキュリティ関連事象の各タイプを記述しなければならない。

AGD_ADM.1.7C 管理者ガイダンスは、評価のために提供された他のすべての証拠資料と一貫していなければならない。

AGD_ADM.1.8C 管理者ガイダンスは、管理者に関連する、IT環境でのすべてのセキュリティ要件を記述しなければならない。

評価者アクションエレメント：

AGD_ADM.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

11.2　利用者ガイダンス (AGD_USR)

目的

利用者ガイダンスは、管理者以外の **TOE** 利用者、その他 **TOE** の外部インタフェースを使用する者（例えばプログラマ）に使用されることを目的とされた資料である。利用者ガイダンスは、**TSF** により提供されるセキュリティ機能を記述し、そのセキュアな使用のため、警告を含む使用法やガイドラインを提供する。

利用者ガイダンスは、**TOE** を使用に関する前提条件の基礎と、悪意のない利用者、アプリケーションの提供者、その他 **TOE** の外部インタフェースを使用する者が **TOE** のセキュアな運用を理解し、意図したように使用することについて一定量の信頼を提供する。

コンポーネントのレベル付け

このファミリは、ただ **1** つのコンポーネントより成る。

適用上の注釈

AGD_USR.1.3C 及び **AGD_USR.1.5C** の要件は、**PP/ST** に記述されている **TOE** セキュリティ環境とセキュリティ対策方針に関する **TOE** の利用者へのあらゆる警告が、適切に利用者ガイダンスに記述されていることを包含する。

多くの場合、ガイダンスは別々の文書で提供されるのが適切である。例えば、人間の利用者のためのガイダンス、ソフトウェアまたはハードウェアインタフェースを使用するアプリケーションプログラマ及び/またはハードウェア設計者のためのガイダンスなど。

AGD_USR.1　利用者ガイダンス

依存性：

ADV_FSP.1 非形式な機能仕様

開発者アクションエレメント：

AGD_USR.1.1D　開発者は、利用者ガイダンスを提供しなければならない。

証拠の内容・提示エレメント：

AGD_USR.1.1C　利用者ガイダンスは、TOEの非管理者である利用者が利用できる機能とインタフェースを記述しなければならない。

AGD_USR.1.2C　利用者ガイダンスは、TOEにより提供された、利用者がアクセスできるセキュリティ機能の使用法を記述しなければならない。

AGD_USR.1.3C　利用者ガイダンスは、セキュアな処理環境で管理されなければならない、利用者がアクセスできる機能と権限についての警告を含まなければならない。

AGD_USR.1.4C　利用者ガイダンスは、TOEセキュリティ環境の記述の中にある利用者のふるまいについての前提条件に関連したものを含む、TOEのセキュアな運用に必要なすべての利用者の責任を明確に提示しなければならない。

AGD_USR.1.5C　利用者ガイダンスは、評価のために提供された他のすべての証拠資料と一貫していなければならない。

AGD_USR.1.6C　利用者ガイダンスは、利用者に関連する、IT環境でのすべてのセキュリティ要件を記述しなければならない。

評価者アクションエレメント：

AGD_USR.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

12　ALCクラス：ライフサイクルサポート

ライフサイクルサポートは、**TOE** の開発及び保守中に、**TOE** を改良するプロセスに統制と管理を確立するための要件である。セキュリティ分析と証拠の作成が、開発と保守活動の必須部分として標準的に行われるならば、**TOE** のセキュリティ要件と **TOE** との対応の信頼度はより大きくなる。

図 **12.1** は、このクラスのファミリと、各ファミリのコンポーネントの階層を示す。

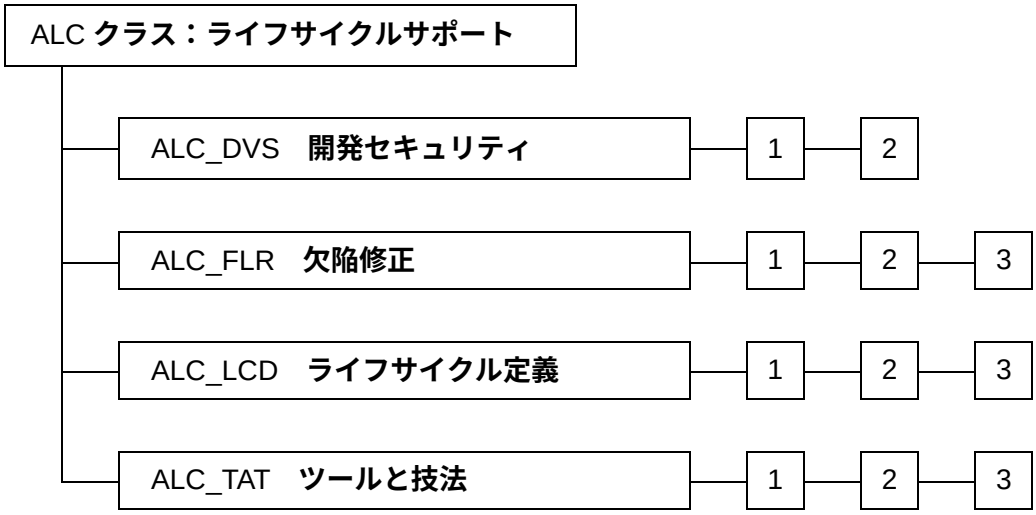

図 12.1 ― ライフサイクルサポートクラスのコンポーネント構成

12.1　開発セキュリティ（ALC_DVS）

目的

開発セキュリティは、**TOE** を保護するため開発環境で使用される、物理的、手続き的、人的、及びその他のセキュリティ手段に関係する。開発セキュリティは、開発場所の物理的セキュリティや開発要員の選定手続きを含む。

コンポーネントのレベル付け

このファミリのコンポーネントは、セキュリティ手段が十分であることの正当化が要求されるかどうかに基づいて、レベル付けされている。

適用上の注釈

このファミリは、開発者サイトに存在する脅威を除去し、減少させるための手段を扱う。逆に **TOE** の利用者サイトでの脅威は、通常、**PP**、または **ST** のセキュリティ環境の章に含まれる。

評価者は、このファミリの要件が満たされているかどうかを確認するために、開発者サイトを訪問する必要があるかどうかを決定しなければならない。

機密性は、開発環境において **TOE** を保護するための論点となるとは限らない。用語「必要がある」**(necessary)**を使用している場合は、適切な保護手段の選択ができる。

ALC_DVS.1 セキュリティ手段の識別

依存性： なし

開発者アクションエレメント：

ALC_DVS.1.1D　開発者は、開発セキュリティ証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

ALC_DVS.1.1C　開発セキュリティ証拠資料は、開発環境のなかでTOEの設計及び実装の機密性や完全性を保護するために必要となる、物理的、手続き的、人的、及びその他の手段をすべて記述しなければならない。

ALC_DVS.1.2C　開発セキュリティ証拠資料は、これらのセキュリティ手段がTOEの開発及び

保守の間を通じて守られる証拠を提供しなければならない。

評価者アクションエレメント：

ALC_DVS.1.1E　評価者は、提供された情報が証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。

ALC_DVS.1.2E　評価者は、セキュリティ手段が、適用されていることを確認しなければならない。

ALC_DVS.2　セキュリティ手段の十分性

依存性：なし

開発者アクションエレメント：

ALC_DVS.2.1D　開発者は、開発セキュリティ証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ALC_DVS.2.1C　開発セキュリティ証拠資料は、開発環境のなかで**TOE**の設計及び実装の機密性と完全性を保護するために必要となる、物理的、手続き的、人的、及びその他の手段をすべて記述しなければならない。

ALC_DVS.2.2C　開発セキュリティ証拠資料は、これらのセキュリティ手段が**TOE**の開発及び保守の間を通じて守られる証拠を提供しなければならない。

ALC_DVS.2.3C　その証拠は、セキュリティ手段が、TOEの機密性と完全性を維持するうえで、必要な保護の水準を提供することを正当化しなければならない。

評価者アクションエレメント：

ALC_DVS.2.1E　評価者は、提供された情報が、証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。

ALC_DVS.2.2E　評価者は、セキュリティ手段が、適用されていることを確認しなければならない。

12.2　欠陥修正（ALC_FLR）

目的

欠陥修正は、発見されたセキュリティの欠陥が開発者により追跡され修正されることを要求する。**TOE** 評価時に、将来欠陥修正手続きが遵守されることを決定できないが、開発者が適切に、欠陥を追跡、修正し、欠陥の情報と修正を配付するための方針と手続きを評価することは可能である。

コンポーネントのレベル付け

このファミリのコンポーネントは、欠陥修正手続きの対象範囲の拡大と、欠陥修正方針の厳密さに基づいて、レベル付けされている。

適用上の注釈

このファミリは、**TOE** の開発者に **TOE** の欠陥を追跡し修正することを要求することにより、**TOE** が将来に渡って維持継続されることを保証するものである。さらに、その欠陥修正を配付するための要件も含んでいる。しかし、このファミリは、現在の評価の範囲を超えた評価要求を課するものではない。

欠陥修正手続きは、可能性のあるすべてのタイプの欠陥についての対処方法を記述しなければならない。ある欠陥は、直ちに修正できないかもしれない。欠陥が修正できず、他の（例えば、手続き的な）手段が取られなければならない場合もありうる。提供される証拠資料は、運用サイトに修正を提供したり、修正が遅れている（その間何をすればよいか）または修正ができない欠陥に関する情報を提供する手続きを含まなければならない。

ALC_FLR.1　基本的な欠陥修正

依存性：なし

開発者アクションエレメント：

ALC_FLR.1.1D　開発者は、欠陥修正手続きについて証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

ALC_FLR.1.1C　欠陥修正手続き証拠資料は、TOEのリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.1.2C　欠陥修正手続きは、欠陥修正方法の調査状況の記述と同時に、各々のセキュ

リティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。

ALC_FLR.1.3C　欠陥修正手続きは、修正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。

ALC_FLR.1.4C　欠陥修正手続き証拠資料は、TOEの利用者に、欠陥情報、修正、及び修正行為のガイダンスを提供するために使用する方法を記述しなければならない。

評価者アクションエレメント：

ALC_FLR.1.1E　評価者は、提供された情報が、証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。

ALC_FLR.2　欠陥報告手続き

依存性：なし

開発者アクションエレメント：

ALC_FLR.2.1D　開発者は、欠陥修正手続きについての証拠資料を提供しなければならない。

ALC_FLR.2.2D　開発者は、利用者からのセキュリティ欠陥の報告とそれらの欠陥の修正要求を受け付け、処理する手続きを確立しなければならない。

証拠の内容・提示エレメント：

ALC_FLR.2.1C　欠陥修正手続き証拠資料は、**TOE**のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.2.2C　欠陥修正手続きは、欠陥修正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。

ALC_FLR.2.3C　欠陥修正手続きは、修正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。

ALC_FLR.2.4C　欠陥修正手続き証拠資料は、**TOE**の利用者に、欠陥情報、修正、及び修正行為のガイダンスを提供するために使用する方法を記述しなければならない。

ALC_FLR.2.5C **報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が修正され、TOEの利用者に修正が発行されることを保証しなければならない。**

ALC_FLR.2.6C **報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる修正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。**

評価者アクションエレメント：

ALC_FLR.2.1E 評価者は、提供された情報が、証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。

ALC_FLR.3　システム化された欠陥修正

依存性：なし

開発者アクションエレメント：

ALC_FLR.3.1D 開発者は、欠陥修正手続きについての証拠資料を提供しなければならない。

ALC_FLR.3.2D 開発者は、利用者からのセキュリティ欠陥の報告とそれらの欠陥の修正要求を受け付け、処理する手続きを確立しなければならない。

ALC_FLR.3.3D **開発者は、TOEに含まれるセキュリティ問題に関する利用者からの報告や問合せを受け付けるための窓口を1つ以上特定しなければならない。**

証拠の内容・提示エレメント：

ALC_FLR.3.1C 欠陥修正手続き証拠資料は、**TOE**のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.3.2C 欠陥修正手続きは、欠陥修正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。

ALC_FLR.3.3C 欠陥修正手続きは、修正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。

ALC_FLR.3.4C 欠陥修正手続き証拠資料は、**TOE**の利用者に、欠陥情報、修正、及び修正行為ガイダンスを提供するために使用する方法を記述しなければならない。

ALC_FLR.3.5C 報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が修正され、**TOE**の利用者に修正が発行されることを保証しなければならない。

ALC_FLR.3.6C 報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる修正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。

ALC_FLR.3.7C **欠陥修正手続きは、セキュリティ欠陥により影響を受ける登録された利用者に、セキュリティ欠陥報告及びそれに関連する修正を自動配付するために、タイムリーな応答を要求する手続きを含まなければならない。**

評価者アクションエレメント：

ALC_FLR.3.1E 評価者は、提供された情報が、証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。

12.3　ライフサイクル定義（ALC_LCD）

目的

開発及び保守の管理が貧弱ならば、**TOE** の実装に欠陥をもたらす、（または **TOE** がセキュリティ要件を満たさない）結果となる。これは、その結果セキュリティ侵害に至る。したがって **TOE** のライフサイクルにおいて、できるだけ早い時期に、**TOE** の開発及び保守のモデルを確立することが重要である。

TOE の開発及び保守のモデルを使用することは、**TOE** に欠陥がない、もしくは **TOE** がすべてのセキュリティ機能要件を満足することを保証するものではない。採用したモデルが、不十分または不適当で、**TOE** の品質に何の利点も生じないことが分かるのみである。専門家のグループ（例えば、学術専門家や標準化組織）で認められたライフサイクルモデルを使用することは、開発及び保守のモデルが **TOE** の全品質の向上に寄与する可能性を高めることができる。

コンポーネントのレベル付け

このファミリのコンポーネントは、ライフサイクルモデルの標準化と計測可能性、及びそのモデルに準拠するための要件の増加に基づいて、レベル付けされている。

適用上の注釈

ライフサイクルモデルは、**TOE** を開発及び保守するために使用する手順、ツール、及び技法を含んでいる。このようなモデルは、設計方法、レビュー手順、プロジェクト管理の統制手段、変更管理手続き、テスト方法、及び受入手続きなどをカバーしている。効果的なライフサイクルモデルは、このような開発及び保守のプロセスの側面を、責任や工程の監視を割り当てる全体の管理機構の中で取り組んでいる。

ライフサイクルの定義は、**TOE** の保守も扱っており、そのため評価の完了後に関係する内容もあるが、評価時に提供された **TOE** のライフサイクル情報の分析を通じて、それらも保証される。

標準化されたライフサイクルモデルとは、専門家のグループ（例えば、学術専門家や標準化組織）で認められたモデルである。

測定可能なライフサイクルモデルとは、**TOE** の開発の特質（例えば、ソースコードの複雑性尺度）を、数値パラメタ、及び/または数値的尺度で測定できるモデルである。

ライフサイクルモデルが、**TOE** のセキュリティ侵害の危険をうまく最小化しているという情報を、開発者が示すことができるならば、このモデルは、**TOE** の開発及び保守に必要な管理方法を提供しているといえる。対象とする **TOE** の環境、及び **TOE** のセキュリティ対策方針につい

て **ST** に書かれた情報は、**TOE** 出荷後のライフサイクルの一部のモデルを定義する上で有用である。

ALC_LCD.1 開発者によるライフサイクルモデルの定義

依存性：なし

開発者アクションエレメント：

ALC_LCD.1.1D 開発者は、**TOE**の開発及び保守で使用されるライフサイクルモデルを確立しなければならない。

ALC_LCD.1.2D 開発者は、ライフサイクル定義証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ALC_LCD.1.1C ライフサイクル定義証拠資料は、**TOE**の開発及び保守で使用されるモデルを記述しなければならない。

ALC_LCD.1.2C ライフサイクルモデルは、**TOE**の開発及び保守の上で必要な管理方法を提供しなければならない。

評価者アクションエレメント：

ALC_LCD.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ALC_LCD.2 標準化されたライフサイクルモデル

依存性：なし

開発者アクションエレメント：

ALC_LCD.2.1D 開発者は、**TOE**の開発及び保守で使用されるライフサイクルモデルを確立しなければならない。

ALC_LCD.2.2D 開発者は、ライフサイクル定義証拠資料を提供しなければならない。

ALC_LCD.2.3D　開発者は、TOEを開発及び保守するために標準化されたライフサイクルモデルを使用しなければならない。

証拠の内容・提示エレメント：

ALC_LCD.2.1C　ライフサイクル定義証拠資料は、**TOE**の開発及び保守で使用されるモデルを記述しなければならない。

ALC_LCD.2.2C　ライフサイクルモデルは、**TOE**の開発及び保守の上で必要な管理方法を提供しなければならない。

ALC_LCD.2.3C　ライフサイクル定義証拠資料は、なぜそのモデルが選ばれたかを説明しなければならない。

ALC_LCD.2.4C　ライフサイクル定義証拠資料は、TOEを開発及び保守するのにどのようにしてそのモデルが使用されるかについて説明しなければならない。

ALC_LCD.2.5C　ライフサイクル定義証拠資料は、標準化されたライフサイクルモデルに準拠していることを実証しなければならない。

評価者アクションエレメント：

ALC_LCD.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ALC_LCD.3　測定可能なライフサイクルモデル

依存性：なし

開発者アクションエレメント：

ALC_LCD.3.1D　開発者は、**TOE**の開発及び保守で使用されるライフサイクルモデルを確立しなければならない。

ALC_LCD.3.2D　開発者は、ライフサイクル定義証拠資料を提供しなければならない。

ALC_LCD.3.3D　開発者は、**TOE**を開発及び保守するために標準化され、**かつ測定可能な**ライフサイクルモデルを使用しなければならない。

ALC_LCD.3.4D　開発者は、標準化され、かつ測定可能なライフサイクルモデルを使用してTOEの開発を測定しなければならない。

証拠の内容・提示エレメント：

ALC_LCD.3.1C　ライフサイクル定義証拠資料は、**モデルに対してTOEの開発を測定するのに用いられた数値パラメタ及び/または数値的尺度の詳細も含んで、TOE**の開発及び保守で使用されるモデルを記述しなければならない。

ALC_LCD.3.2C　ライフサイクルモデルは、**TOE**の開発及び保守の上で必要な管理方法を提供しなければならない。

ALC_LCD.3.3C　ライフサイクル定義証拠資料は、なぜそのモデルが選ばれたかを説明しなければならない。

ALC_LCD.3.4C　ライフサイクル定義証拠資料は、**TOE**を開発及び保守するのにどのようにしてそのモデルが使用されるかについて説明しなければならない。

ALC_LCD.3.5C　ライフサイクル定義証拠資料は、標準化され、**かつ測定可能な**ライフサイクルモデルに準拠していることを実証しなければならない。

ALC_LCD.3.6C　ライフサイクル定義証拠資料は、標準化され、かつ測定可能なライフサイクルモデルを使用して、TOEの開発の測定結果を提供しなければならない。

評価者アクションエレメント：

ALC_LCD.3.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

12.4　ツールと技法（ALC_TAT）

目的

ツールと技法は、**TOE** の開発、分析、及び実装に使用されるツールの選択に関連する。これは、**TOE** の開発時に良く定義されていない、一貫性がなく不正確な開発ツールが使用されるのを防止する要件を含む。また、これには、プログラミング言語、証拠資料、実装標準、及びサポートするランタイムライブラリのような **TOE** の他の部分も含むが、これらに限定されない。

コンポーネントのレベル付け

このファミリのコンポーネントは、実装標準、及び実装に依存するオプションの証拠資料についての記述と範囲に関する要件の増加に基づいて、レベル付けされている。

適用上の注釈

明確に定義された開発ツールが要求される。これらのツールは、さらに詳しく説明しなくても利用できるものである。例えば、標準化組織などにより発行された標準に基づいているプログラム言語や **CAD** システムは、明確に定義されたものと考えられる。

ツールと技法は、開発者が適用する実装標準（**ALC_TAT.2.3D**）、及びサードパーティのソフトウェア、ハードウェア、またはファームウェアなども含んだ **TOE** のすべての部分についての実装標準**(ALC_TAT.3.3D)**を区別している。

要件 **ALC_TAT.1.2.C** は、ソースコードのすべての文が、曖昧でない意味を持つことを保証するために、特にプログラミング言語に適用される。

ALC_TAT.1 明確に定義された開発ツール

依存性：

ADV_IMP.1　TSF 実装の部分集合

開発者アクションエレメント：

ALC_TAT.1.1D　開発者は、TOEに対して使用される開発ツールを識別しなければならない。

ALC_TAT.1.2D　開発者は、開発ツールのオプションの中で実装に依存するものについて証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

ALC_TAT.1.1C 実装に使用されるすべてのツールは、明確に定義されていなければならない。

ALC_TAT.1.2C 開発ツールの証拠資料は、実装に使用されるすべての文の意味を、曖昧さなく定義しなければならない。

ALC_TAT.1.3C 開発ツールの証拠資料は、実装に依存するすべてのオプションの意味を、曖昧さなく定義しなければならない。

評価者アクションエレメント：

ALC_TAT.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ALC_TAT.2 実装標準への準拠

依存性：

ADV_IMP.1 **TSF** 実装の部分集合

開発者アクションエレメント：

ALC_TAT.2.1D 開発者は、**TOE**に対して使用される開発ツールを識別しなければならない。

ALC_TAT.2.2D 開発者は、開発ツールのオプションの中で実装に依存するものについて証拠資料を提出しなければならない。

ALC_TAT.2.3D 開発者は、適用された実装標準を記述しなければならない。

証拠の内容・提示エレメント：

ALC_TAT.2.1C 実装に使用されるすべてのツールは、明確に定義されていなければならない。

ALC_TAT.2.2C 開発ツールの証拠資料は、実装に使用されるすべての文の意味を、曖昧さなく定義しなければならない。

ALC_TAT.2.3C 開発ツールの証拠資料は、実装に依存するすべてのオプションの意味を、曖昧さなく定義しなければならない。

評価者アクションエレメント：

ALC_TAT.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ALC_TAT.2.2E　**評価者は、実装標準が、適用されていることを確認しなければならない。**

ALC_TAT.3　実装標準への準拠－すべての部分

依存性：

ADV_IMP.1　TSF 実装の部分集合

開発者アクションエレメント：

ALC_TAT.3.1D　開発者は、**TOE**に対して使用される開発ツールを識別しなければならない。

ALC_TAT.3.2D　開発者は、開発ツールのオプションの中で実装に依存するものについて証拠資料を提出しなければならない。

ALC_TAT.3.3D　開発者は、**TOEのすべて部分に対する**実装標準を記述しなければならない。

証拠の内容・提示エレメント：

ALC_TAT.3.1C　実装に使用されるすべてのツールは、明確に定義されていなければならない。

ALC_TAT.3.2C　開発ツールの証拠資料は、実装に使用されるすべての文の意味を、曖昧さなく定義しなければならない。

ALC_TAT.3.3C　開発ツールの証拠資料は、実装に依存するすべてのオプションの意味を、曖昧さなく定義しなければならない。

評価者アクションエレメント：

ALC_TAT.3.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ALC_TAT.3.2E　評価者は、実装標準が、適用されていることを確認しなければならない。

13　ATEクラス：テスト

このクラスは、4つのファミリを含む：カバレージ（**ATE_COV**）、深さ（**ATE_DPT**）、独立テスト（例えば、評価者によって実行される機能テスト）（**ATE_IND**）、及び機能テスト（**ATE_FUN**）。テストは、**TOE**セキュリティ機能要件が満たされていることの立証を支援する。テストは、**TOE**が少なくとも**TOE**セキュリティ機能要件を満たすことの保証を提供するが、テストは**TOE**が仕様で定められたもの以外をしないことは実証できない。テストは、またそれらの仕様に対するサブシステム及びモジュールのテストのように、**TSF**の内部構造に向かって行われる。

カバレージ及び深さについては、ファミリのコンポーネントを適用することの柔軟性を増すために、機能テストとは分離されている。しかし、これらの3つのファミリの要件は、一緒に適用することが意図されている。

独立テストのファミリは、他のファミリに要件を支援するのに必要な情報を提供する依存関係を持つが、主として独立した評価者の行為に関わるものである。

このクラスは、**TSF**がその仕様どおりに動作することの確認に重点を置いている。これは機能要件に基づく積極的テストと、望ましくないふるまいが起こらないことをチェックする消極的テストの両方を含んでいる。このクラスは、利用者にセキュリティ方針の侵害を可能にする脆弱性を見出すことを目的とするような侵入テストは述べていない。侵入テストは、**TSF**の設計・実装での脆弱性を識別するために、特別に探索する**TOE**の分析に基づくし、かつクラス**AVA**での脆弱性評定にて別に述べられている。

図13.1は、このクラスのファミリと、各ファミリのコンポーネントの階層を示す。

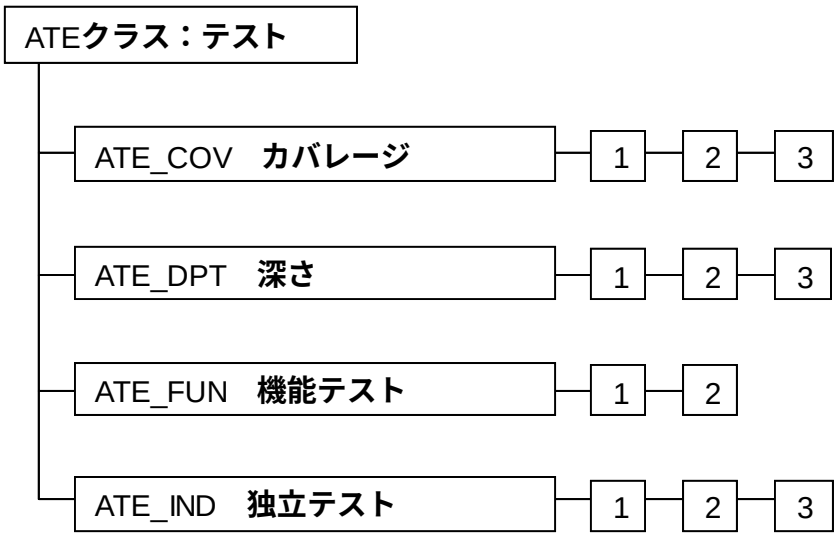

図 13.1 ― テストクラスのコンポーネント構成

13.1　カバレージ（ATE_COV）

目的

このファミリは、テストカバレージの完全性を扱うテストの側面について述べる。即ち、どの**TSF**がテストされたかの範囲について述べ、かつ**TSF**が仕様どおりに動作することを実証するにテストが十分であるか否かを述べる。

コンポーネントのレベル付け

このファミリのコンポーネントは、インタフェーステストの厳格さ、及び**TSF**が機能仕様どおりに動作することを実証するテストの十分さの分析の厳格さに基づいて、レベル付けされている。

ATE_COV.1 カバレージの証拠

目的

このコンポーネントの目的は、**TSF**がその機能仕様に対応してテストされていることを確立することである。これは、対応に対する開発者の証拠の検査を通して達成される。

適用上の注釈

テストの目的は、**TSF**を網羅することであるが、テストを機能仕様とテストデータ自身に非形式的にマッピングする以外に、この主張を検証するものを提供する要件はない。

このコンポーネントで、開発者はどのようにして、識別されたテストが、機能仕様に記述された**TSF**に対応するかを示すことを要求される。これは、対応の記述（多分、表を使うこと）により達成可能である。評価時のテスト計画を立案するときに、この情報が評価者を支援することを要求されている。このレベルでは、開発者による**TSF**の全側面の完全なカバレージに対する要件はないため、評価者はこの領域の欠如を考慮する必要がある。

依存性：

ADV_FSP.1　非形式的機能仕様
ATE_FUN.1　機能テスト

開発者アクションエレメント：

ATE_COV.1.1D　開発者は、テストカバレージの証拠を提供しなければならない。

証拠の内容・提示エレメント：

ATE_COV.1.1C　テストカバレージの証拠は、テスト証拠資料で識別されたテストと機能仕様

に記述されたTSFとの対応を提示しなければならない。

評価者アクションエレメント：

ATE_COV.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_COV.2 カバレージの分析

目的

このコンポーネントの目的は、**TSF**がその機能仕様に対応して系統的にテストされたことを確立することである。これは、開発者の対応分析の検査を通して達成される。

適用上の注釈

開発者は、識別されたテストが機能仕様に記述されたセキュリティ機能のすべてのテストを含んでいることを実証することを要求される。分析は、テストとセキュリティ機能の対応を示すだけではなく、評価者に対して、機能がどのようにして実行されるかを決定するのに十分な情報も、また提供しなければならない。この情報は追加の評価者テストの計画に利用可能である。このレベルにて、開発者は機能仕様内の機能の各々がテストされることを実証しなければならないが、各機能のテストの量は完全である必要はない。

依存性：

ADV_FSP.1　非形式的機能仕様
ATE_FUN.1　機能テスト

開発者アクションエレメント：

ATE_COV.2.1D　開発者は、テストカバレージの**分析**を提供しなければならない。

証拠の内容・提示エレメント：

ATE_COV.2.1C　テストカバレージの**分析**は、テスト証拠資料で識別されたテストと機能仕様に記述された**TSF**との対応を**実証**しなければならない。

ATE_COV.2.2C　テストカバレージの分析は、機能仕様に記述されたTSFとテスト証拠資料で識別されたテストとの対応が完全であることを実証しなければならない。

評価者アクションエレメント：

ATE_COV.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_COV.3 カバレージの厳格な分析

目的

このコンポーネントの目的は、**TSF**がその機能仕様に対応して系統的にかつ徹底的にテストされたことを確立することである。これは、開発者の対応分析の検査を通して達成される。

適用上の注釈

開発者は、識別されたテストが全セキュリティ機能を網羅していること、及び各セキュリティ機能のテストが完全であることの説得力ある論証を提供することを要求される。これらは徹底的にテストされるので、評価者にとって機能仕様に基づく**TSF**インタフェースの追加の機能テストを考え出す余地は殆ど残っていない。しかしながら、評価者はそのようなテストを考え出すことに努めなければならない。

依存性：

ADV_FSP.1　非形式的機能仕様
ATE_FUN.1　機能テスト

開発者アクションエレメント：

ATE_COV.3.1D　開発者は、テストカバレージの分析を提供しなければならない。

証拠の内容・提示エレメント：

ATE_COV.3.1C　テストカバレージの分析は、テスト証拠資料で識別されたテストと機能仕様に記述された**TSF**との対応を実証しなければならない。

ATE_COV.3.2C　テストカバレージの分析は、機能仕様に記述された**TSF**とテスト証拠資料で識別されたテストとの対応が完全であることを実証しなければならない。

ATE_COV.3.3C　**テストカバレージの分析は、機能仕様で識別されたTSFのすべての外部インタフェースが完全にテストされていることを厳格に実証しなければならない。**

評価者アクションエレメント：

ATE_COV.3.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

13.2　深さ（ATE_DPT）

目的

このファミリのコンポーネントは、**TSF**がテストされた詳細さのレベルを取り扱う。セキュリティ機能のテストは、表現の分析から引き出された情報の更なる深さに基づいている。

目的は、**TOE**の開発中の誤りを取り逃がすリスクに対抗することである。さらに、このファミリのコンポーネントは、特にテストが**TSF**の内部構造により深く関係することにより、挿入された如何なる悪意のコードをも発見できる可能性がある。

特定の内部インタフェースを実行するテストは、**TSF**が期待された外部セキュリティのふるまいを見せるだけではなく、このふるまいが内部メカニズムの正常な動作から起こることの保証を提供することができる。

コンポーネントのレベル付け

このファミリのコンポーネントは、上位レベル設計から実装表現までの**TSF**表現で提供された詳細の量に基づいて、レベル付けされている。このレベルは、**ADV**クラスで提供された**TSF**表現を反映する。

適用上の注釈

証拠資料と証拠の量とタイプは、一般的に**ATE_FUN**から選択されたコンポーネントによって決められる。

機能仕様書のレベルのテストは、**ATE_COV**に述べられている。

このファミリの原則は、テストレベルが、得ようとする保証レベルに対して適切であることである。より高いコンポーネントが適用される場合、テスト結果は**TSF**の実装がその設計と一貫していることを実証する必要がある。例えば、上位レベル設計（**HLD**）はサブシステムの各々についてだけでなく、サブシステム間のインタフェースについても十分詳細に記述しなければならない。テスト結果は、サブシステム間の内部インタフェースが実行されていることを示さなければならない。これは、**TSF**の外部インタフェースからのテストを通じて、またはテストハーネス(test harness)を使用するなどして、サブシステムインタフェースを分離してのテストによって達成される。内部インタフェースのある側面が外部インタフェースを介してテストできない場合、それらの側面がテストを必要としないことの正当性が有るか、内部インタフェースが直接テストされる必要が有るかである。後者の場合、上位レベル設計は直接テストを容易にするのに十分詳細化されている必要がある。このファミリのより高いレベルのコンポーネントは、設計が具体的になるときに現れる内部インタフェースの正常動作をチェックすることを目的とする。これらのコンポーネントが適用される場合、**TSF**の外部インタフェースだけを使ったテストの深さについて、

十分な証拠を提供することがより困難になるであろう、そして通常、モジュールテストが必要となるであろう。

ATE_DPT.1 テスト：上位レベル設計

目的

TSFのサブシステムは、**TSF**の内部動作について上位レベルの記述を提供する。何らかの欠点の存在を実証するために、サブシステムレベルのテストは、**TSF**サブシステムが正しく実現されている保証を提供する。

適用上の注釈

開発者は、**TSF**の上位レベル設計のテストを“サブシステム”の観点から記述することを期待されている。”サブシステム”は、**TSF**を比較的少数の部分に分解する概念を表現するのに用いられる。

依存性：

ADV_HLD.1　記述的上位レベル設計
ATE_FUN.1　機能テスト

開発者アクションエレメント：

ATE_DPT.1.1D　開発者は、テストの深さの分析を提供しなければならない。

証拠の内容・提示エレメント：

ATE_DPT.1.1C　深さの分析は、テスト証拠資料で識別されたテストが、TSFがその上位レベル設計にしたがって動作することを実証するに十分であることを実証しなければならない。

評価者アクションエレメント：

ATE_DPT.1.1E　評価者は､提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_DPT.2 テスト：下位レベル設計

目的

TSFのサブシステムは、**TSF**の内部動作について上位レベルの記述を提供する。何らかの欠点の存在を実証するために、サブシステムレベルのテストは、**TSF**サブシステムが正しく実現されている保証を提供する。

TSFのモジュールは、**TSF**の内部動作についての記述を提供する。何らかの欠点の存在を実証するために、モジュールレベルのテストは、**TSF**モジュールが正しく実現されている保証を提供する。

適用上の注釈

開発者は、**TSF**の上位レベル設計のテストを“サブシステム”の観点から記述することを期待されている。“サブシステム”は、**TSF**を比較的少数の部分に分解する概念を表現するのに用いる。

開発者は、**TSF**の下位レベル設計のテストを“モジュール”によって記述することを期待されている。“モジュール”は、**TSF**の各“サブシステム”を比較的少数の部分に分解する概念を表現するのに用いる。

依存性：

ADV_HLD.2　セキュリティ実施上位レベル設計
ADV_LLD.1　記述的下位レベル設計
ATE_FUN.1　機能テスト

開発者アクションエレメント：

ATE_DPT.2.1D　開発者は、テストの深さの分析を提供しなければならない。

証拠の内容・提示エレメント：

ATE_DPT.2.1C　深さの分析は、テスト証拠資料で識別されたテストが、**TSF**がその上位レベル設計、**及び下位レベル設計**にしたがって動作することを実証するに十分であることを実証しなければならない。

評価者アクションエレメント：

ATE_DPT.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たすしていることを確認しなければならない。

ATE_DPT.3 テスト：実装表現

目的

TSFのサブシステムは、**TSF**の内部動作について上位レベルの記述を提供する。何らかの欠点の存在を実証するために、サブシステムレベルのテストは、**TSF**サブシステムが正しく実現されている保証を提供する。

TSFのモジュールは、**TSF**内部動作についての記述を提供する。何らかの欠点の存在を実証するために、モジュールレベルのテストは、**TSF**モジュールが正しく実現されている保証を提供する。

TSFの実装表現は、**TSF**の内部動作について詳細な記述を提供する。何らかの欠点の存在を実証するために、実装レベルのテストは、**TSF**実装が正しく実現されている保証を提供する。

適用上の注釈

開発者は、**TSF**の上位レベル設計のテストを“サブシステム”の観点から記述することを期待されている。“サブシステム”は、**TSF**を比較的少数の部分に分解する概念を表現するのに用いる。

開発者は、**TSF**の下位レベル設計のテストを“モジュール”の観点から記述することを期待されている。“モジュール”は、**TSF**の各“サブシステム”を比較的少数の部分に分解する概念を表現するのに用いる。

TSFの実装表現は、**TSF**自身（例えば、コンパイルされるソースコード）を生成させるのに使用されるものである。

依存性：

ADV_HLD.2 セキュリティ実施上位レベル設計
ADV_IMP.2 **TSFの実装**
ADV_LLD.1 記述的下位レベル設計
ATE_FUN.1 機能テスト

開発者アクションエレメント：

ATE_DPT.3.1D 開発者は、テストの深さの分析を提供しなければならない。

証拠の内容・提示エレメント：

ATE_DPT.3.1C 深さの分析は、テスト証拠資料で識別されたテストが、**TSF**がその上位レベル設計、下位レベル設計、**及び実装表現**にしたがって動作することを実証するのに十分であることを実証しなければならない。

評価者アクションエレメント：

ATE_DPT.3.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

13.3　機能テスト（ATE_FUN）

目的

開発者による機能テストは、**TSF**が**PP/ST**の機能要件を満たすに必要な能力を示すことを実証する。機能テストは、**TSF**が少なくともセキュリティ機能要件を満たす保証を提供するが、**TSF**が仕様以外のことをしないことを実証しない。“機能テスト”ファミリは、証拠資料と必要な支援ツールのタイプと量、開発者テストで何が実証されるかに焦点を置いている。機能テストは、必要なセキュリティ機能が提供されていることの積極的な確認に限定せず、特に望ましくないふるまい（しばしば、機能要件の逆に基づく）が無いことをチェックする消極的テストも含む。

このファミリは、未発見の欠点の公算が比較的少ないという保証を提供するのに寄与する。

ATE_COV、**ATE_DPT**、**ATE_FUN**のファミリは、開発者により提供されるべきテストの証拠を定義するのに組み合わせて使用される。評価者による独立機能テストは、**ATE_IND**で規定される。

コンポーネントのレベル付け

このファミリは、2つのコンポーネントを含み、上位は順序依存性を分析することを要求する。

適用上の注釈

テスト遂行の手順は、テスト環境、テスト条件、テストデータのパラメタと値を含むテストプログラムとテストスイート(test suites)を使うための指示を提供することを期待されている。テスト手順は、またテスト入力からテスト結果がどのように引き出されるかを示さなければならない。

このファミリは、すべてのテストの計画、手順、結果の記述に対する要件を規定する。このため、提供されねばならない情報量は、**ATE_COV**、**ATE_DPT**の使用により変動する。

順序依存性は、特定のテストの実行がうまくいくかどうかが、特定の状態の存在に依存する場合に関係する。例えば、テスト**A**の実行の成功から生じる状態がテスト**B**の実行の成功に必須であるため、順序依存性は、テスト**A**がテスト**B**の直前に実行されることを要求する。このようにして、テスト**B**の失敗が順序依存性の問題に関係しているかも知れない。前述の例で、テスト**B**は、テスト**A**ではなくてテスト**C**がそれの直前に実行されたために失敗するかも知れない、またはテスト**B**の失敗はテスト**A**の失敗に関係しているかも知れない。

ATE_FUN.1 機能テスト

目的

目的は、開発者がすべてのセキュリティ機能の実行が仕様どおりであることを実証することである。開発者は、テストを実行し、テスト証拠資料を提供することを要求される。

依存性：なし。

開発者アクションエレメント：

ATE_FUN.1.1D　開発者は、TSFをテストし、結果を証拠資料で提出しなければならない。

ATE_FUN.1.2D　開発者は、テスト証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ATE_FUN.1.1C　テスト証拠資料は、テスト計画、テスト手順記述、期待されるテスト結果、実際のテスト結果から構成されなければならない。

ATE_FUN.1.2C　テスト計画は、テストされるセキュリティ機能を識別し、実行されるテストの目標を記述しなければならない。

ATE_FUN.1.3C　テスト手順記述は、実行されるべきテストを識別し、各セキュリティ機能をテストするシナリオを記述しなければならない。これらのシナリオは、他のテストの結果へのすべての順序依存性を含んでいなければならない。

ATE_FUN.1.4C　期待されるテスト結果は、テストの実行が成功したときの予期される出力を示さなければならない。

ATE_FUN.1.5C　開発者が実行したテストによるテスト結果は、各々のテストされたセキュリティ機能が仕様どおりに動作することを実証しなければならない。

評価者アクションエレメント：

ATE_FUN.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_FUN.2 順序付けられた機能テスト

目的

目的は、開発者がすべてのセキュリティ機能の実行が仕様どおりであることを実証することである。開発者は、テストを実行し、テスト証拠資料を提供することを要求される。

このコンポーネントで、追加の目的は、テストされている**TSF**の部分の正しさについて論証が堂々巡りするのを避けるように、テストが構成されていることを保証することである。

適用上の注釈

テスト手順は、テストの順序に関して必須の初期テスト条件を記述できるかもしれないが、これらは順序の正当性を提供していない。テスト順序の分析は、テスト順序に隠されている失敗の可能性が有るので、テストの妥当性を決定する重要な要因である。

依存性：なし。

開発者アクションエレメント：

ATE_FUN.2.1D 開発者は、**TSF**をテストし､結果を証拠資料で提出しなければならない。

ATE_FUN.2.2D 開発者は、テスト証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

ATE_FUN.2.1C テスト証拠資料は、テスト計画、テスト手順記述、期待されるテスト結果、実際のテスト結果から構成されなければならない。

ATE_FUN.2.2C テスト計画は、テストされるセキュリティ機能を識別し、実行されるテストの目標を記述しなければならない。

ATE_FUN.2.3C テスト手順記述は、実行されるべきテストを識別し、各セキュリティ機能をテストするシナリオを記述しなければならない。これらのシナリオは、他のテストの結果へのすべての順序依存性を含んでいなければならない。

ATE_FUN.2.4C 期待されるテスト結果は、テストの実行が成功したときの予期される出力を示さなければならない。

ATE_FUN.2.5C 開発者が実行したテストによるテスト結果は、各々のテストされたセキュリティ機能が仕様どおりに動作することを実証しなければならない。

ATE_FUN.2.6C　テスト証拠資料は、テスト手順の順序依存性の分析を含まなければならない。

評価者アクションエレメント：

ATE_FUN.2.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

13.4　独立テスト（ATE_IND）

目的

目的は、セキュリティ機能が仕様どおりに機能することを実証することである。

追加の目的は、仕様の不正な実装や仕様に準拠していないコードの見落としとなる、開発者側のテスト結果の不正な評価のリスクに対抗することである。

コンポーネントのレベル付け

レベル付けは、テスト証拠資料の量、テスト支援、及び評価者テストの量に基づいている。

適用上の注釈

このファミリに規定されるテストは、評価者以外の専門知識を有する組織（例えば、独立した研究所、客観的な消費者組織）による支援も可能である。テストは、他の保証作業の遂行と密接に結びついた**TOE**の理解を要求する、さらに、評価者はそのような支援を受ける場合、このファミリの要件が適切に述べられていることを保証する責任を有する。

このファミリは、**TSF**の独立機能テストの程度を扱う。独立機能テストは、全体、または一部において、開発者機能テストを繰り返す形式でも良い。それは、また開発者テストの範囲や深さを広げるとか、**TOE**が適用可能な明らかな公知になっているセキュリティの弱点をテストするとかの、開発者機能テストへの追加の形式でも良い。これらのアクティビティは補完的であり、テスト結果の可用性とカバレージ、及び**TSF**の機能の複雑性を考慮して、**TOE**毎に適切な組合せが計画されなければならない。テスト計画は、他の保証アクティビティのレベルと密接に結びついた開発が必要であり、より高い保証が要求されるほど、繰り返しテストのより大きなサンプルや評価者による、より独立した積極的・消極的機能テストを含む。

開発者テストのサンプリングは、開発者が計画したTSFに対するテスト計画を実行し、結果を正しく記録していることの確証を提供することを意図している。選択されるべきサンプルの量は、開発者による機能テスト結果の詳細さと品質によって影響される。評価者は、また追加テストを考え出す範囲と、これらの2つの領域での労力から得られる相対的利益を考察する必要がある。すべての開発者テストの再実行は、可能であり、望ましい場合もあるが、多くの場合、とても困難でかつ生産性の低いものとなる。従って、このファミリの最上位のコンポーネントは注意して使用すべきである。サンプリングは、**ATE_COV**と**ATE_DPT**の両者の要件で提供されるテスト結果を含む、利用可能なテスト結果全体の範囲から行われる。

評価に含まれる**TOE**の異なる構成を考慮することもまた必要である。評価者は、提供された結果の有効性を評価し、それに応じて自らのテストを計画する必要がある。
独立機能テストは、侵入テストとは異なる。侵入テストは、設計及び／または実装の脆弱性に対

する知識のある系統的な探索に基づいている。侵入テストは、**AVA_VLA**ファミリを使用して規定される。

テストに対する**TOE**の適合は、**TOE**へのアクセス、テストの実行に必要な支援の証拠資料、及び情報（あらゆるテストソフトウェアまたはツールを含む）に基づく。そのような支援の必要性は別の保証ファミリへの依存によって述べられている。

加えて、テストに対する**TOE**の適合は、別の考えに基づいている。例えば、開発者より提供された**TOE**のバージョンが最終バージョンとは異なるかも知れない。

TSFサブセットのリファレンスは、評価者が、実施する評価の目的に一致する適切な一連のテストを設計できるようにすることを意図する。

ATE_IND.1 独立テスト - 準拠

目的

このコンポーネントにおける目的は、セキュリティ機能が仕様どおりに機能することを実証することである。

適用上の注釈

このコンポーネントは、開発者テスト結果の使用について述べていない。そのような結果が利用できない場合や開発者テストが確認なく承認されている場合に有効である。評価者は、**TOE**セキュリティ機能要件が満たされていることを確認する目的で、テストを考え出し、遂行することを要求される。近道は、すべての可能なテストを実施するよりも、代表的なテストを通じて正常動作の自信を得ることである。この目的のために計画されるテスト範囲は方法論の成果であり、特定の**TOE**の背景と他の評価アクティビティとのバランスを考慮する必要がある。

依存性：

ADV_FSP.1　非形式的機能仕様
AGD_ADM.1　管理者ガイダンス
AGD_USR.1　利用者ガイダンス

開発者アクションエレメント：

ATE_IND.1.1D　開発者は、テストのためにTOEを提供しなければならない。

証拠の内容・提示エレメント：

ATE_IND.1.1C　TOEは、テストに適していなければならない。

評価者アクションエレメント：

ATE_IND.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_IND.1.2E　評価者は、TSFのサブセットを、TOEが仕様どおりに動作することを確認するために、適切にテストしなければならない。

ATE_IND.2 独立テスト - サンプル

目的

目的は、セキュリティ機能が仕様どおりに機能することを実証することである。評価者テストは、開発者テストのサンプルの選択と繰り返しを含む。

適用上の注釈

開発者テストの効果的な再現に必要な資材を、開発者が評価者に提供すべきであることを意図している。これは、機械読取り可能なテスト証拠資料やテストプログラムなどを含んでいる。

このコンポーネントは、テストの計画を補うために、評価者が開発者からの利用可能なテスト結果を入手する要件を含んでいる。評価者は、得られた結果に対しより確信を得るために、開発者テストのサンプルを繰り返すであろう。そのような確信を確立するために、評価者は開発者テストを足場として、別の方法で**TOE**を実行させる追加テストを実施する。正当性が確認された開発者テスト結果の基盤を使うことにより、評価者は単に開発者自身の労力や与えられた固定レベルの資源を使うことで可能となる以上に、より広い範囲の条件で、**TOE**が正常に動作することの確信が得られる。開発者が**TOE**のテストを完了しているとの確信を得ることで、評価者は、また証拠資料の調査や専門家の知識で特別に関心がある領域のテストに適切に集中するより多くの自由が得られる。

依存性：

ADV_FSP.1　非形式的機能仕様
AGD_ADM.1　管理者ガイダンス
AGD_USR.1　利用者ガイダンス
ATE_FUN.1　機能テスト

開発者アクションエレメント：

ATE_IND.2.1D　開発者は、テストのための**TOE**を提供しなければならない。

証拠の内容・提示エレメント：

ATE_IND.2.1C **TOE**は、テストに適していなければならない。

ATE_IND.2.2C **開発者は、TSFの開発者機能テストで使用されたものと同等の一連の資源を提供しなければならない。**

評価者アクションエレメント：

ATE_IND.2.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_IND.2.2E 評価者は、**TSF**のサブセットを、**TOE**が仕様どおりに動作することを確認するために、適切にテストしなければならない。

ATE_IND.2.3E **評価者は、開発者テスト結果を検証するために、テスト証拠資料内のテストのサンプルを実行しなければならない。**

ATE_IND.3 独立テスト - 完全

目的

目的は、すべてのセキュリティ機能が仕様どおりに機能することを実証することである。評価者テストは、開発者テストをすべて繰り返すことを含む。

適用上の注釈

開発者テストの効果的な再現に必要な資材を、開発者が評価者に提供することを意図している。これは、マシン読取り可能なテスト証拠資料やテストプログラムなどを含んでいる。

このコンポーネントでは、評価者はテスト計画の一部として、開発者テストのすべてを繰り返さなければならない。前のコンポーネントと同様に、評価者はまた、開発者が行ったのとは異なる方法で、**TOE**を実行させることを目的とするテストを実施する。開発者テストが徹底的に行われている場合には、これを行う余地は殆ど残っていないであろう。

依存性：

ADV_FSP.1 非形式的機能仕様
AGD_ADM.1 管理者ガイダンス
AGD_USR.1 利用者ガイダンス
ATE_FUN.1 機能テスト

開発者アクションエレメント：

ATE_IND.3.1D 開発者は、テストのための**TOE**を提供しなければならない。

証拠の内容・提示エレメント：

ATE_IND.3.1C **TOE**は、テストに適していなければならない。

ATE_IND.3.2C 開発者は、**TSF**の開発者機能テストで使用されたものと同等の一連の資源を提供しなければならない。

評価者アクションエレメント：

ATE_IND.3.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

ATE_IND.3.2E 評価者は、**TSF**のサブセットを、**TOE**が仕様どおりに動作することを確認するために、適切にテストしなければならない。

ATE_IND.3.3E 評価者は、開発者テスト結果を検証するために、テスト証拠資料内の**すべての**テストを実行しなければならない。

14　AVAクラス：脆弱性評定

クラスは、悪用されうる隠れチャネルの存在、**TOE**の誤使用や設定誤りの可能性、確率的または順列的メカニズムが破られる可能性、及び**TOE**の開発または運用で入り込む悪用されうる脆弱性の可能性を扱う。

図**14.1**は、このクラスのファミリと、各ファミリのコンポーネントの階層を示す。

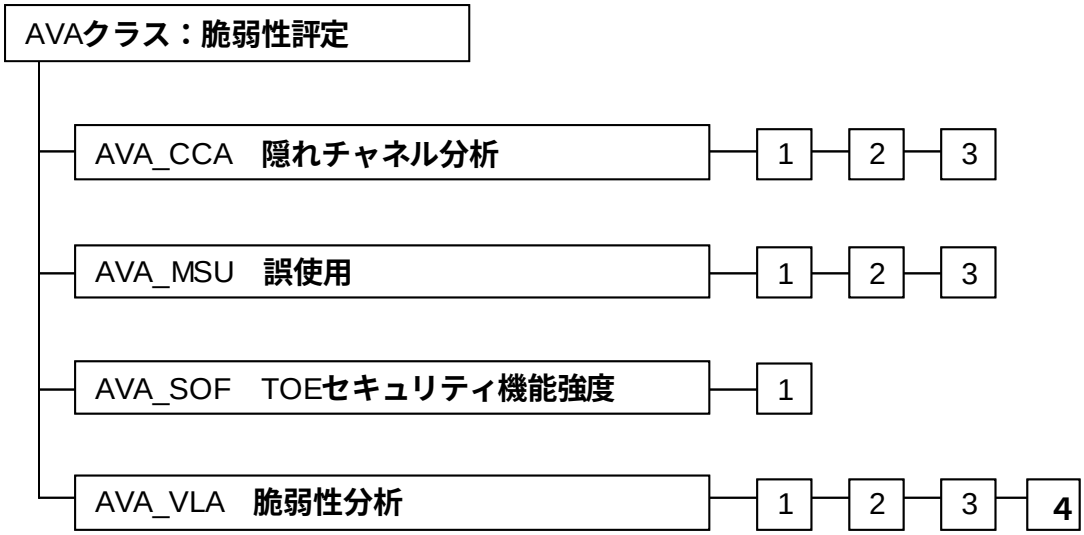

図 14.1 ― 脆弱性評定クラスのコンポーネント構成

14.1　隠れチャネル分析 (AVA_CCA)

目的

隠れチャネル分析は、意図的に作ったものでないが悪用される可能性がある信号チャネル**(**すなわち、不正な情報フロー**)**の存在、及び潜在的な容量の決定を行うことである。

保証要件は、意図的に作ったものではないが**SFP**を侵害するのに使われるかもしれない信号パスが存在するという脅威を扱う。

コンポーネントのレベル付け

コンポーネントは、隠れチャネル分析の厳密さの度合いによって、レベル付けされている。

適用上の注釈

チャネル容量の見積もりは、実際のテスト測定と同様、非形式的な工学的な測定によってなされる。

隠れチャネル分析において前提条件とする例として、プロセッサ速度、システムまたはネットワークの構成、メモリサイズ、キャッシュサイズなどがある。

テストを通じての隠れチャネル分析の選択的確認で、評価者は隠れチャネル分析のすべての側面の検証を行うことができる**(**例えば、識別、容量の見積もり、排除、監視、悪用のシナリオ**)**。ただし、隠れチャネル分析結果のすべてを実証することが要求されているのではない。

このファミリは、情報フロー制御**SFP**だけに適用するものなので、**ST**に情報フォロー制御**SFP**が含まれない場合は、保証要件のこのファミリは適用できない。

AVA_CCA.1 隠れチャネル分析

目的

隠れチャネルの非形式的探索によって、識別可能な隠れチャネルを識別することを目的とする。

依存性：

ADV_FSP.2	**完全に定義された外部インタフェース**
ADV_IMP.2	**TSFの実装**
AGD_ADM.1	**管理者ガイダンス**

AGD_USR.1　　利用者ガイダンス

開発者アクションエレメント：

AVA_CCA.1.1D　開発者は、情報フロー制御方針ごとに隠れチャネルを探索しなければならない。

AVA_CCA.1.2D　開発者は、隠れチャネル分析の証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_CCA.1.1C　分析証拠資料は、隠れチャネルを識別し、その容量を見積もらなくてはならない。

AVA_CCA.1.2C　分析証拠資料は、隠れチャネルの存在を決定するのに使われた手順と、隠れチャネル分析を実行するのに必要な情報を記述しなければならない。

AVA_CCA.1.3C　分析証拠資料は、隠れチャネル分析中になされたすべての前提条件を記述しなければならない。

AVA_CCA.1.4C　分析証拠資料は、最悪ケースのシナリオに基づいて、チャネル容量の見積もりに用いた方法を記述しなければならない。

AVA_CCA.1.5C　分析証拠資料は、各々の識別された隠れチャネルに対して、最悪ケースの悪用シナリオを記述しなければならない。

評価者アクションエレメント：

AVA_CCA.1.1E　評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_CCA.1.2E　評価者は、隠れチャネル分析結果は、TOEがその機能要件を満たすことを示しているのを確認しなければならない。

AVA_CCA.1.3E　評価者は、テストによって、選択的に隠れチャネル分析の正当性を確認しなければならない。

AVA_CCA.2　系統的隠れチャネル分析

目的

目的は、隠れチャネルの系統的探索によって、識別可能な隠れチャネルを識別することである。

適用上の注釈

系統的方法で隠れチャネル分析を行うために、開発者は、場当たり的なやり方で隠れチャネルの識別を行うのとは逆に、構造的かつ再現性のある方法で隠れチャネルの識別をする必要がある。

依存性：

ADV_FSP.2	完全に定義された外部インタフェース
ADV_IMP.2	**TSF**の実装
AGD_ADM.1	管理者ガイダンス
AGD_USR.1	利用者ガイダンス

開発者アクションエレメント：

AVA_CCA.2.1D開発者は、情報フロー制御方針ごとに隠れチャネルを探索しなければならない。

AVA_CCA.2.2D　開発者は、隠れチャネル分析の証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_CCA.2.1C　分析証拠資料は、隠れチャネルを識別し、その容量を見積もらなければならない。

AVA_CCA.2.2C　分析証拠資料は、隠れチャネルの存在を決定するのに使われた手順と、隠れチャネル分析を実行するのに必要な情報を記述しなければならない。

AVA_CCA.2.3C　分析証拠資料は、隠れチャネル分析中になされたすべての前提条件を記述しなければならない。

AVA_CCA.2.4C　分析証拠資料は、最悪ケースのシナリオに基づいて、チャネル容量の見積もりに用いた方法を記述しなければならない。

AVA_CCA.2.5C　分析証拠資料は、各々の識別された隠れチャネルに対して、最悪ケースの悪用シナリオを記述しなければならない。

AVA_CCA.2.6C　**分析証拠資料は、隠れチャネルの識別に使用した方法が系統的なものであることの証拠を提示しなければならない。**

評価者アクションエレメント：

AVA_CCA.2.1E 評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_CCA.2.2E 評価者は、隠れチャネル分析結果は、**TOE**がその機能要件を満たすことを示しているのを確認しなければならない。

AVA_CCA.2.3E 評価者は、テストによって、選択的に隠れチャネル分析の正当性を確認しなければならない。

AVA_CCA.3 徹底的隠れチャネル分析

目的

目的は、隠れチャネルの徹底的探索によって、識別可能な隠れチャネルを識別することである。

適用上の注釈

徹底的方法による隠れチャネル分析は、隠れチャネル識別のために使われた計画が、隠れチャネル探索に対してあらゆる方法がとられたことを保証するのに十分であるという追加証拠の提出を要求する。

依存性：

ADV_FSP.2	完全に定義された外部インタフェース
ADV_IMP.2	**TSF**の実装
AGD_ADM.1	管理者ガイダンス
AGD_USR.1	利用者ガイダンス

開発者アクションエレメント：

AVA_CCA.3.1D開発者は、情報フロー制御方針ごとに隠れチャネルを探索しなければならない。

AVA_CCA.3.2D 開発者は、隠れチャネル分析の証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_CCA.3.1C 分析証拠資料は、隠れチャネルを識別し、その容量を見積もらなければならない。

AVA_CCA.3.2C 分析証拠資料は、隠れチャネルの存在を決定するのに使われた手順と、隠れチ

ャネル分析を実行するのに必要な情報を記述しなければならない。

AVA_CCA.3.3C 分析証拠資料は、隠れチャネル分析中になされたすべての前提条件を記述しなければならない。

AVA_CCA.3.4C 分析証拠資料は、最悪ケースのシナリオに基づいて、チャネル容量の見積もりに用いた方法を記述しなければならない。

AVA_CCA.3.5C 分析証拠資料は、各々の識別された隠れチャネルに対して、最悪ケースの悪用シナリオを記述しなければならない。

AVA_CCA.3.6C 分析証拠資料は、隠れチャネル識別に使用した方法が**徹底的な**ものであることの証拠を提示しなければならない。

評価者アクションエレメント：

AVA_CCA.3.1E 評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_CCA.3.2E 評価者は、隠れチャネル分析結果は、**TOE**がその機能要件を満たすことを示しているのを確認しなければならない。

AVA_CCA.3.3E 評価者は、テストによって、選択的に隠れチャネル分析の正当性を確認しなければならない。

14.2 誤使用 (AVA_MSU)

目的

誤使用は、**TOE**の管理者または利用者が、合理的にセキュアであると判断しているにもかかわらず、セキュアでない方法で**TOE**が構成され使用され得るかどうかを調査する。

目的は、以下のとおり。

a) 利用者や管理者が検出できずに、**TOE**をセキュアでない方法で構成または設置してしまう可能性を最小にする。
b) 操作中の人間やそれ以外の誤りが、セキュリティ機能を不活性化し、無効にし、または活性化するのを失敗させたりして、検出されないセキュアでない状態に陥ってしまう危険を最小にする。

コンポーネントのレベル付け

コンポーネントは、開発者が提出すべき証拠の量と、分析が厳密性に基づいて、レベル付けされている。

適用上の注釈

矛盾した、誤解を招く、不完全な、または合理的でないガイダンスは、**TOE**の利用者に**TOE**がセキュアでないときにそれがセキュアであると信じさせ、結果として脆弱性を生じさせてしまうかもしれない。

矛盾したガイダンスの例として、同一の入力に対して異なる結果が出るように読めるような二つのガイダンス指示があげられる。

誤解を招くガイダンスの例として、１つのガイダンスの指示が何通りにも解釈でき、そのうちの**1**つで、セキュアでない状態が生じるかもしれない記述があげられる。

不完全なガイダンスの例として、重要な物理的セキュリティ要件のリストから重要な項目が欠落し、リストが完全であると信じた管理者がその項目を見逃してしまうことがあげられる。

不合理なガイダンスの例として、運用上、きわめて面倒で負担の大きい手順を要求するものがあげられる。

ガイダンス証拠資料が、提出されなければならない。これは、既存の利用者または管理者用証拠資料の中に含まれていてもよく、それらと別に提出されてもよい。別に提出される場合、評価者はその証拠資料が**TOE**と共に供給されていることを確認する必要がある。

AVA_MSU.1 ガイダンスの検査

目的

目的は、誤解・不合理さ・矛盾がガイダンス証拠資料にないこと、すべての操作モードにおけるセキュアな手順が提示されていることを保証することである。セキュアでない状態は容易に検出できなければならない。

依存性：

ADO_IGS.1	**設置、生成、及び立上げ手順**
ADV_FSP.1	**非形式的機能仕様**
AGD_ADM.1	**管理者ガイダンス**
AGD_USR.1	**利用者ガイダンス**

開発者アクションエレメント：

AVA_MSU.1.1D **開発者は、*ガイダンス*証拠資料を提供しなければならない。**

証拠の内容・提示エレメント：

AVA_MSU.1.1C **ガイダンス証拠資料は、TOEの操作のすべてのモード(障害や操作誤りのあとの操作も含む)、それらの結果、及びセキュアな操作を維持するために知っておくべきことを識別しなければならない。**

AVA_MSU.1.2C **ガイダンス証拠資料は、完全で、明白で、矛盾なく、合理的なものでなくてはならない。**

AVA_MSU.1.3C **ガイダンス証拠資料は、意図した環境について、すべての前提条件を列挙しなければならない。**

AVA_MSU.1.4C **ガイダンス証拠資料は、外部のセキュリティ手段(外部の手続き的、物理的、及び人的な管理を含む)に対するすべての要件を列挙しなければならない。**

評価者アクションエレメント：

AVA_MSU.1.1E **評価者は、提出される情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。**

AVA_MSU.1.2E **評価者は、提出されたガイダンス証拠資料だけを使って、すべての構成、及び導入手順を再現し、TOEがセキュアに構成され使用されることを確認しなければならない。**

AVA_MSU.1.3E **評価者は、ガイダンス証拠資料を用いれば、すべてのセキュアでない状態が検出できることを決定しなければならない。**

AVA_MSU.2 分析の確認

目的

目的は、誤解・不合理さ・矛盾がガイダンス証拠資料にないこと、すべての操作モードにおけるセキュアな手順が提示されていることを保証することである。セキュアでない状態は、容易に検出できなければならない。このコンポーネントでは、これらの目的が達成されていることを追加保証するため、開発者によるガイダンス証拠資料の分析が要求される。

依存性：

ADO_IGS.1	設置、生成、及び立上げ手順
ADV_FSP.1	非形式的機能仕様
AGD_ADM.1	管理者ガイダンス
AGD_USR.1	利用者ガイダンス

開発者アクションエレメント：

AVA_MSU.2.1D 開発者は、ガイダンス証拠資料を提供しなければならない。

AVA_MSU.2.2D **開発者は、ガイダンス証拠資料の分析に関する証拠資料を提出しなければならない。**

証拠の内容・提示エレメント：

AVA_MSU.2.1C ガイダンス証拠資料は、**TOE**の操作のすべてのモード**(**障害や操作誤りのあとの操作も含む**)**、それらの結果、及びセキュアな操作を維持するために知っておくべきことを識別しなければならない。

AVA_MSU.2.2C ガイダンス証拠資料は、完全で、明白で、矛盾なく、合理的なものでなくてはならない。

AVA_MSU.2.3C ガイダンス証拠資料は、意図した環境について、すべての前提条件を列挙しなければならない。

AVA_MSU.2.4C ガイダンス証拠資料は、外部のセキュリティ手段**(**外部の手続き的、物理的、及び人的な管理を含む**)**に対するすべての要件を列挙しなければならない。

AVA_MSU.2.5C **分析証拠資料は、ガイダンス証拠資料が完全なものであることを実証しなければならない。**

評価者アクションエレメント：

AVA_MSU.2.1E 評価者は、提出される情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_MSU.2.2E 評価者は、提出されたガイダンス証拠資料だけを使って、すべての構成、導入手順、**及びその他の手順を選択的に**再現し、**TOE**がセキュアに構成され使用されることを確認しなければならない。

AVA_MSU.2.3E 評価者は、ガイダンス証拠資料を用いれば、すべてのセキュアでない状態が検出できることを決定しなければならない。

AVA_MSU.2.4E **評価者は、TOEの操作のすべてのモードにおけるセキュアな操作のためにガイダンスが提供されていることが分析証拠資料に示されていることを確認しなければならない。**

AVA_MSU.3 セキュアでない状態の分析とテスト

目的

目的は、誤解・不合理さ・矛盾がガイダンス証拠資料にないこと、すべての操作モードにおけるセキュアな手順が提示されていることを保証することである。セキュアでない状態は、容易に検出できなければならない。このコンポーネントでは、これらの目的が達成されていることを追加保証するため、開発者によるガイダンス証拠資料の分析が要求され、この分析は評価者によるテストを通して、正当性を確認しながら確認**(validated and confirmed)**される。

適用上の注釈

このコンポーネントでは、評価者は、**TOE**がセキュアでない状態に入ったかどうか、いつ入ったかが容易に検出できることを保証するためのテストを行うことが要求される。このテストは、侵入テストの特別の側面と考えてよい。

依存性：

ADO_IGS.1	設置、生成、及び立上げ手順
ADV_FSP.1	非形式的機能仕様
AGD_ADM.1	管理者ガイダンス

AGD_USR.1　　利用者ガイダンス

開発者アクションエレメント：

AVA_MSU.3.1D 開発者は、ガイダンス証拠資料を提供しなければならない。

AVA_MSU.3.2D 開発者は、ガイダンス証拠資料の分析に関する証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_MSU.3.1C ガイダンス証拠資料は、**TOE**の操作のすべてのモード**(**障害や操作誤りのあとの操作も含む**)**、操作の結果、及びセキュアな操作を維持するために知っておくべきことを識別しなければならない。

AVA_MSU.3.2C ガイダンス証拠資料は、完全で、明白で、矛盾なく、合理的なものでなくてはならない。

AVA_MSU.3.3C ガイダンス証拠資料は、意図した環境について、すべての前提条件を列挙しなければならない。

AVA_MSU.3.4C ガイダンス証拠資料は、外部のセキュリティ手段**(**外部の手続き的、物理的、及び人的な管理を含む**)**に対するすべての要件を列挙しなければならない。

AVA_MSU.3.5C 分析証拠資料は、ガイダンス証拠資料が完全なものであることを実証しなければならない。

評価者アクションエレメント：

AVA_MSU.3.1E 評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_MSU.3.2E 評価者は、提出されたガイダンス証拠資料だけを使って、すべての構成、導入手順、及びその他の手順を選択的に再現し、**TOE**がセキュアに構成され使用されることを確認しなければならない。

AVA_MSU.3.3E 評価者は、ガイダンス証拠資料を用いれば、すべてのセキュアでない状態が検出できることを決定しなければならない。

AVA_MSU.3.4E 評価者は、**TOE**の操作のすべてのモードにおけるセキュアな操作のためにガイダンスが提供されていることが分析証拠資料に示されていることを確認しなければならない。

AVA_MSU.3.5E **評価者は、管理者または利用者がガイダンス証拠資料を理解することによって、TOEがセキュアでない方法で構成され操作されているかどうかを合理的に決定できる、ということを決定するために独立テストを実施しなければならない。**

14.3　TOEセキュリティ機能強度（AVA_SOF)

目的

TOEのあるセキュリティ機能が、バイパス、不活性化、破壊され得ないとしても、それを支えるセキュリティメカニズムの概念に脆弱性があれば、そのセキュリティ機能は破られるかもしれない。これらの機能について、そのメカニズムにおけるセキュリティのふるまいとそれを破るのに必要な労力についての定量的または統計的分析結果を用いて、そのセキュリティのふるまいを評価付けすることができる。評価付けは、**TOE**セキュリティ機能強度主張の形式で行われる。

コンポーネントのレベル付け

このファミリでは、コンポーネントは**1**つのみである。

適用上の注釈

セキュリティ機能は、セキュリティメカニズムによって実現される。例えば、パスワードメカニズムは、識別・認証セキュリティ機能を実現するために使用できる。

TOEセキュリティ機能強度評価は、セキュリティメカニズムのレベルに対して行われるが、その結果によって、識別された脅威に対抗する、関連するセキュリティ機能の能力が分かる。

TOEセキュリティ機能強度分析においては、少なくとも、目標とする評価保証レベルに対する**ST**を含んだすべての**TOE**提供物件の内容を考慮すべきである。

AVA_SOF.1　TOE セキュリティ機能強度評価

依存性：

ADV_FSP.1　非形式的機能仕様
ADV_HLD.1　記述的上位レベル設計

開発者アクションエレメント：

AVA_SOF.1.1D　開発者は、STにおいてTOEセキュリティ機能強度主張を有するものとして識別された各メカニズムに対し、TOEセキュリティ機能強度分析を行わなければならない。

証拠の内容・提示エレメント：

AVA_SOF.1.1C　TOEセキュリティ機能強度主張を有する各メカニズムに対し、TOEセキュリ

ティ機能強度分析は、PP/STに定義された最小強度レベルと同等以上であることを示さねばならない。

AVA_SOF.1.2C　特定のTOEセキュリティ機能強度主張を有する各メカニズムに対し、TOEセキュリティ機能強度分析は、PP/STに定義された特定の機能強度の数値尺度と同等以上であることを示さねばならない。

評価者アクションエレメント：

AVA_SOF.1.1E　評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_SOF.1.2E　評価者は、強度主張が正しいことを確認しなければならない。

14.4 脆弱性分析 (AVA_VLA)

目的

脆弱性分析とは、**TOE**の構造及び予期される操作の評価を通して、または他の方法**(**例えば、欠陥仮説法**)**によって、識別された脆弱性が利用者による**TSP**侵害を許してしまうかどうかを決定するための評定のことである。

脆弱性分析は、資源**(**例えば、データ**)**に許可されないアクセスを許す、**TSF**を妨害または変更できることを許す、または他の利用者の許可された能力を妨害することができる、といった欠陥を利用者が見つけられるような脅威を扱う。

コンポーネントのレベル付け

レベル付けは、開発者と評価者による脆弱性分析の厳密さの度合いに基づいている。

適用上の注釈

脆弱性分析は、セキュリティ脆弱性の存在を確かめるために開発者が実施するものである。目標とする評価保証レベルに従い、**ST**を含む**TOE**提供物件すべての内容を十分に調べねばならない。評価者による独立脆弱性分析の支援に役立つと思われる場合、評価者がその情報を利用できるよう、開発者は識別された脆弱性の処分について証拠資料提出する必要がある。

開発者分析の意図は、意図した**TOE**の環境において、識別されたどの脆弱性も悪用できないこと、**TOE**が明白な侵入攻撃に耐えることを確認することである。

明白な脆弱性とは、**TOE**についての理解、技能、高度な技術、資源などをほとんど持たなくとも悪用できるような脆弱性のことである。それらは、**TSF**インタフェース記述から読み取れるかもしれない。明白な脆弱性には、公知になっているもの、開発者が知っているべき、または評価監督機関から入手できるその詳細が含まれる。

系統的方法で脆弱性に対する探索を行うためには、開発者は、場当たり的なやり方で脆弱性を識別するのではなく、体系的で再現性のある方法で脆弱性を識別していく必要がある。脆弱性の探索が系統的に行われたことの関連証拠として、欠陥の探索のベースとなったすべての**TOE**証拠資料の識別を含まなければならない。

独立脆弱性分析は、開発者が識別した脆弱性をさらに超えて行われる。評価者分析の主な意図は、低**(AVA_VLA.2)**、中**(AVA_VLA.3)**、高**(AVA_VLA.4)**の**3**レベルの攻撃能力を持つ攻撃者の侵入攻撃に、**TOE**が耐え得るかどうかを決定することである。この意図を実現するために、まず評価者は、識別されたすべての脆弱性について悪用可能性を評定する。その手段として、侵入テストが用いられる。**TOE**への侵入を試みる場合、評価者は、低**(AVA_VLA.2)**、中**(AVA_VLA.3)**、高

(AVA_VLA.4)のどれかの攻撃能力を持った攻撃者の役割を想定しなければならない。コンポーネント**AVA_VLA.2**から**AVA_VLA.4**の状況では、評価者は、そのような攻撃者による脆弱性のすべての悪用を「明白な侵入攻撃」**(AVA_VLA.*.2C**エレメントに関して**)**とみなさなければならない。

AVA_VLA.1　開発者脆弱性分析

目的

脆弱性分析は、明白なセキュリティ脆弱性の存在を確かめ、かつ**TOE**の意図する環境においてそれらが悪用され得ないことを確認するため、開発者によって実施される。

適用上の注釈

評価者は、別の部分の評価をしているときに、脆弱性の悪用の可能性が識別されたとき、追加テストの実施を考慮すべきである。

依存性：

ADV_FSP.1　非形式的機能仕様
ADV_HLD.1　記述的上位レベル設計
AGD_ADM.1　管理者ガイダンス
AGD_USR.1　利用者ガイダンス

開発者アクションエレメント：

AVA_VLA.1.1D　開発者は、TOE提供物件に対して、利用者がTSPを侵害し得る明白な方法を探す分析を行い、証拠資料を提出しなければならない。

AVA_VLA.1.2D　開発者は、明白な脆弱性の処置について証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_VLA.1.1C　証拠資料では、識別されたすべての脆弱性に対して、TOEの意図した環境においてはそれらの脆弱性が悪用され得ないことを示さなければならない。

評価者アクションエレメント：

AVA_VLA.1.1E　評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_VLA.1.2E　評価者は、開発者脆弱性分析に基づき侵入テストを行い、明白な脆弱性への対処が行われていることを保証しなければならない。

AVA_VLA.2　独立脆弱性テスト

目的

脆弱性分析は、セキュリティ脆弱性の存在を確かめ、かつ**TOE**の意図する環境においてそれらが悪用され得ないことを確認するため、開発者によって実施される。

評価者は、評価者独立脆弱性分析に基づき、低い攻撃能力を持つ攻撃者によって行われる侵入攻撃に、**TOE**が耐え得るかどうかを決定するために、独立侵入テストを実施する。

依存性：

ADV_FSP.1　非形式的機能仕様
ADV_HLD.2　**セキュリティ実施上位レベル設計**
ADV_IMP.1　**TSF実装のサブセット**
ADV_LLD.1　**記述的下位レベル設計**
AGD_ADM.1　管理者ガイダンス
AGD_USR.1　利用者ガイダンス

開発者アクションエレメント：

AVA_VLA.2.1D　開発者は、**TOE**提供物件に対して、利用者が**TSP**を侵害し得る**方法**を探す分析を行い、証拠資料を提出しなければならない。

AVA_VLA.2.2D　開発者は、**識別された**脆弱性の処置について証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_VLA.2.1C　証拠資料では、識別されたすべての脆弱性に対して、**TOE**の意図した環境においてはそれらの脆弱性が悪用され得ないことを示さなければならない。

AVA_VLA.2.2C　証拠資料は、識別された脆弱性について、TOEが明白な侵入攻撃に耐え得ることを正当化しなければならない。

評価者アクションエレメント：

AVA_VLA.2.1E 評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_VLA.2.2E 評価者は、開発者脆弱性分析に基づき侵入テストを行い、**識別された**脆弱性への対処が行われていることを保証しなければならない。

AVA_VLA.2.3E **評価者は、独立脆弱性分析を行わなければならない。**

AVA_VLA.2.4E **評価者は、独立脆弱性分析に基づき、意図した環境において、新たに識別された脆弱性が悪用され得るかどうかを決定するため、独立侵入テストを実施しなければならない。**

AVA_VLA.2.5E **評価者は、低い攻撃能力を持つ攻撃者による侵入攻撃にTOEが耐えられることを決定しなければならない。**

AVA_VLA.3 中程度の抵抗力

目的

脆弱性分析は、セキュリティ脆弱性の存在を確かめ、かつ**TOE**の意図する環境においてそれらが悪用され得ないことを確認するため、開発者によって実施される。

評価者は、評価者独立脆弱性分析に基づき、中程度の攻撃能力を持つ攻撃者によって行われる侵入攻撃に、**TOE**が耐え得るかどうか決定するために、独立侵入テストを実施する。

依存性：

ADV_FSP.1 非形式的機能仕様
ADV_HLD.2 セキュリティ実施上位レベル設計
ADV_IMP.1 **TSF**実装のサブセット
ADV_LLD.1 記述的下位レベル設計
AGD_ADM.1 管理者ガイダンス
AGD_USR.1 利用者ガイダンス

開発者アクションエレメント：

AVA_VLA.3.1D 開発者は、**TOE**提供物件に対して、利用者が**TSP**を侵害し得る方法を探す分析を行い、証拠資料を提出しなければならない。

AVA_VLA.3.2D 開発者は、識別された脆弱性の処置について証拠資料を提出しなければならない。

証拠の内容・提示エレメント：

AVA_VLA.3.1C 証拠資料では、識別されたすべての脆弱性に対して、**TOE**の意図した環境においてはそれらの脆弱性が悪用され得ないことを示さなければならない。

AVA_VLA.3.2C 証拠資料は、識別された脆弱性について、**TOE**が明白な侵入攻撃に耐え得ることを正当化しなければならない。

AVA_VLA.3.3C **証拠は、脆弱性に対する探索が系統的であることを示さなければならない。**

評価者アクションエレメント：

AVA_VLA.3.1E 評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_VLA.3.2E 評価者は、開発者脆弱性分析に基づき侵入テストを行い、識別された脆弱性への対処が行われていることを保証しなければならない。

AVA_VLA.3.3E 評価者は、独立脆弱性分析を行わなければならない。

AVA_VLA.3.4E 評価者は、独立脆弱性分析に基づき、意図した環境において、新たに識別された脆弱性が悪用され得るかどうかを決定するため、独立侵入テストを実施しなければならない。

AVA_VLA.3.5E 評価者は、**中程度の**攻撃能力を持つ攻撃者による侵入攻撃に**TOE**が耐えられることを決定しなければならない。

AVA_VLA.4 高い抵抗力

目的

脆弱性分析は、セキュリティ脆弱性の存在を確かめ、かつ**TOE**の意図する環境においてそれらが悪用され得ないことを確認するため、開発者によって実施される。

評価者は、評価者独立脆弱性分析に基づき、高い攻撃能力を持つ攻撃者によって行われる侵入攻

撃に、**TOE**が耐え得るかどうか決定するために、独立侵入テストを実施する。

依存性：

ADV_FSP.1 非形式的機能仕様
ADV_HLD.2 セキュリティ実施上位レベル設計
ADV_IMP.1 **TSF**実装のサブセット
ADV_LLD.1 記述的下位レベル設計
AGD_ADM.1 管理者ガイダンス
AGD_USR.1 利用者ガイダンス

開発者アクションエレメント：

AVA_VLA.4.1D 開発者は、**TOE**提供物件に対して、利用者が**TSP**を侵害し得る方法を探す分析を行い、証拠資料を提出しなくてはならない。

AVA_VLA.4.2D 開発者は、識別された脆弱性の処置について証拠資料を提出しなくてはならない。

証拠の内容・提示エレメント：

AVA_VLA.4.1C 証拠資料では、識別されたすべての脆弱性に対して、**TOE**の意図した環境においてはそれらの脆弱性が悪用され得ないことを示さなければならない。

AVA_VLA.4.2C 証拠資料は、識別された脆弱性について、**TOE**が明白な侵入攻撃に耐え得ることを正当化しなければならない。

AVA_VLA.4.3C 証拠は、脆弱性に対する探索が系統的であることを示さなければならない。

AVA_VLA.4.4C **分析証拠資料は、その分析がTOE提供物件を完全に分析の対象にしている正当性を提供しなければならない。**

評価者アクションエレメント：

AVA_VLA.4.1E 評価者は、提出された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AVA_VLA.4.2E 評価者は、開発者脆弱性分析に基づき侵入テストを行い、識別された脆弱性への対処が行われていることを保証しなければならない。

AVA_VLA.4.3E 評価者は、独立脆弱性分析を行わなくてはならない。

AVA_VLA.4.4E 評価者は、独立脆弱性分析に基づき、意図した環境において、新たに識別された脆弱性が悪用され得るかどうかを決定するため、独立侵入テストを実施しなければならない。

AVA_VLA.4.5E 評価者は、**高い**攻撃能力を持つ攻撃者による侵入攻撃に**TOE**が耐えられることを決定しなければならない。

15　保証維持の枠組み

15.1　はじめに

この章は、保証維持クラス（**AMA**）がサポートする保証維持の枠組みについて解説する。そこで、**AMA** 要件を適用する **1** つの可能な方法を理解するのに役立つ情報を提供する。

保証の維持は、**TOE** が、第 **4** 章から第 **5** 章及び第 **8** 章から第 **14** 章の基準に対して評価され、認証された後で適用される概念である。保証の維持要件は、**TOE** またはその環境に変更が行われるときに、**TOE** がセキュリティターゲットに適合し続けることを保証することを目的としている。そのような変更には、新しい脅威または脆弱性の発見、利用者要件の変更、認証された **TOE** で検出されたバグの修正、提供された機能へのその他の更新などがある。

保証が維持されていることを決定する **1** つの方法は、**TOE** の再評価によるものである。ここでの「再評価」**(re-evaluation)**の用語は、**TOE** の認証済みバージョンになされたすべてのセキュリティに関する変更に対処し、これまでの評価結果を、これらがなお有効な場合に再使用する **TOE** の新しいバージョンの評価を意味する。ただし、多くの場合、保証が維持され続けるようにするために、**TOE** のすべての新しいバージョンを再評価するのは実際的ではない。

そこで、**AMA** クラスの主な目標は、**TOE** の新しいバージョンの形式的再評価を必ずしも必要とせずに、**TOE** に確立された保証が維持されているという確信を提供するために適用できる要件のセットを定義することである。**AMA** クラスは、再評価の必要性を完全には排除しない。場合によっては、変更があまりにも重大であるために、保証が維持されるようにするには、再評価だけが信頼できる。それゆえ、このクラスの要件は、必要なときに **TOE** のコスト効率の優れた再評価をサポートする第 **2** の目標を持つ。

いずれの **AMA** 要件も満たしていない場合でも、第 **4** 章から第 **5** 章及び第 **8** 章から第 **14** 章の基準に対して **TOE** の新しいバージョンを再評価することが可能であることに注意する必要がある。しかしながら、**AMA** クラスにはそのような再評価のサポートに使用できる要件が含まれている。

保守開発者及び評価者アクションは、**TOE** が評価され、認証された後で適用されることが意図されているが、下記のように、いくつかの要件は、評価の時点で適用できる。明確にするために、次の用語がこの枠組みの記述で使用されている。

a) **TOE** の「*認証済みバージョン*」は、評価され、認証されたバージョンを表す。

b) **TOE** の「*現行バージョン*」は、いくつかの点で認証済みバージョンとは異なるバージョンを表す。例えば、これには次のものがある。

- **TOE** の新しいリリース
- 発見されたバグを後で修正するためにパッチが適用された認証済みバージョン

— **TOE** の同じ基本バージョン、ただし、ハードウェアまたはソフトウェアのプラットフォームが異なる

このクラスの開発者と評価者の役割は、**CC** パート **1** に記述されている。ただし、必ずしも、このクラスの要件にゆだねられる評価者が **TOE** の認証済みバージョンの評価者と同じであるとは限らない。

形式的再評価を必ずしも必要とせずに、**TOE** に保証が維持されるようにするために、このクラスの要件は、**TOE** がそのセキュリティターゲットに適合し続けることを示す証拠（例えば、開発者テストの証拠）を維持する義務を開発者に課している。

15.2 保証維持サイクル

この節では、概念の使用を示すことを意図した、保証維持ファミリとコンポーネントの使用の可能な **1** つの手法について記述する。この例は、次の **3** つのフェーズに分割できる「保証維持サイクル」にモデル化されている。

a) *受入フェーズ*。サイクルの開始時、サイクル中の保証維持のための開発者の計画と手続きが開発者により確立され、評価者により独立に正当性が確認される。

b) *監視フェーズ*。開発者は、サイクル中のいくつかの点で **TOE** の保証が、確立された計画と手続きに従って維持されているという証拠を提供する。保証維持のこの証拠は、評価者により独立にチェックされる。

c) *再評価フェーズ*。サイクルを完了する。**TOE** の更新されたバージョンが、認証済みバージョン以降の **TOE** に影響を与える変更に基づく再評価のために提出される。

AMA 内のファミリは、主にこれらのフェーズの最初の **2** つを取り扱い、**3** 番目のフェーズをサポートする。これらのフェーズは、保証維持要件の適用の記述を助けるためにのみここに記述されている。これらのフェーズが形式的に組み込んだ保証維持スキームを要求する意図はない。

保証維持サイクルを次の図 **15.1** に示す。

この例において、**TOE** は、受入フェーズが成功裡に終了した（つまり、保証維持のための開発者の計画と手続きが受け入れられた）ときにのみ監視フェーズに入ることができる。開発者が監視フェーズ中にこれらの計画または手続きに変更を行った場合、**TOE** は、変更を受け入れるために、受入フェーズに再度入る必要がある。

監視フェーズ中、開発者は、保証維持の計画と手続きに従い、**TOE** に影響を与える変更のセキュリティ影響分析を行う（セキュリティ影響分析）。このフェーズのいくつかの点で、評価者は、開発者の作業を（監査により）独立にチェックする。開発者は、計画と手続きが守られ、セキュリティ影響分析が正しく行われることを保証する必要がある。

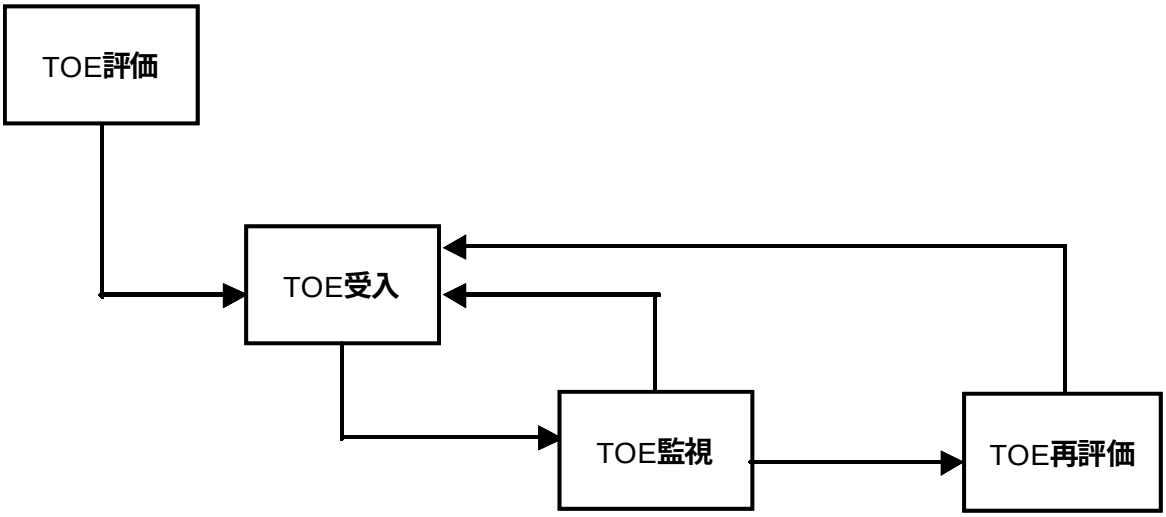

図 15.1 ― 保証維持サイクルの例

そこで、**TOE** が監視フェーズに入った後、開発者が作成した **TOE** の新しいバージョンに対して、**TOE** の保証が維持されているという確信を持つことが可能になる。

変更を受ける **TOE** は、無期限に監視フェーズに留まることはない。いずれかの時点で、**TOE** の再評価が必要となる。再評価が必要となる時期の決定は、特に重要な変更だけでなく、**TOE** への累積的変更によって決まる。例えば、非常に多くの小さな変更は、大きな変更と同等の影響を保証に与えることがある。開発者の保証維持計画は、監視フェーズ中に **TOE** に行われる変更の範囲を定義する（下記の節 **15.3.1** を参照）。

同様の方法で監視フェーズ中に **TOE** を「格上げする」（つまり、保証レベルを高める）ことはできない。これは、**TOE** の評価（これまでの評価結果を適切に再使用する）によってのみ達成することができる。

TOE の保証維持状況は、保証維持手続きが守られていないこと、その結果、**TOE** の保証が未定であることが発見された場合、再検討する必要がある。場合によっては、開発者は、**TOE** を再評価に再提出し、その後で、新たに保証維持サイクルを開始する必要がある。

15.2.1 TOE 受入

この例では、保証維持サイクルの **TOE** 受入フェーズは、次のように詳細化することができる。そこでは、保証維持計画と **AMA** クラスの **TOE** コンポーネント分類報告ファミリが使用されている。

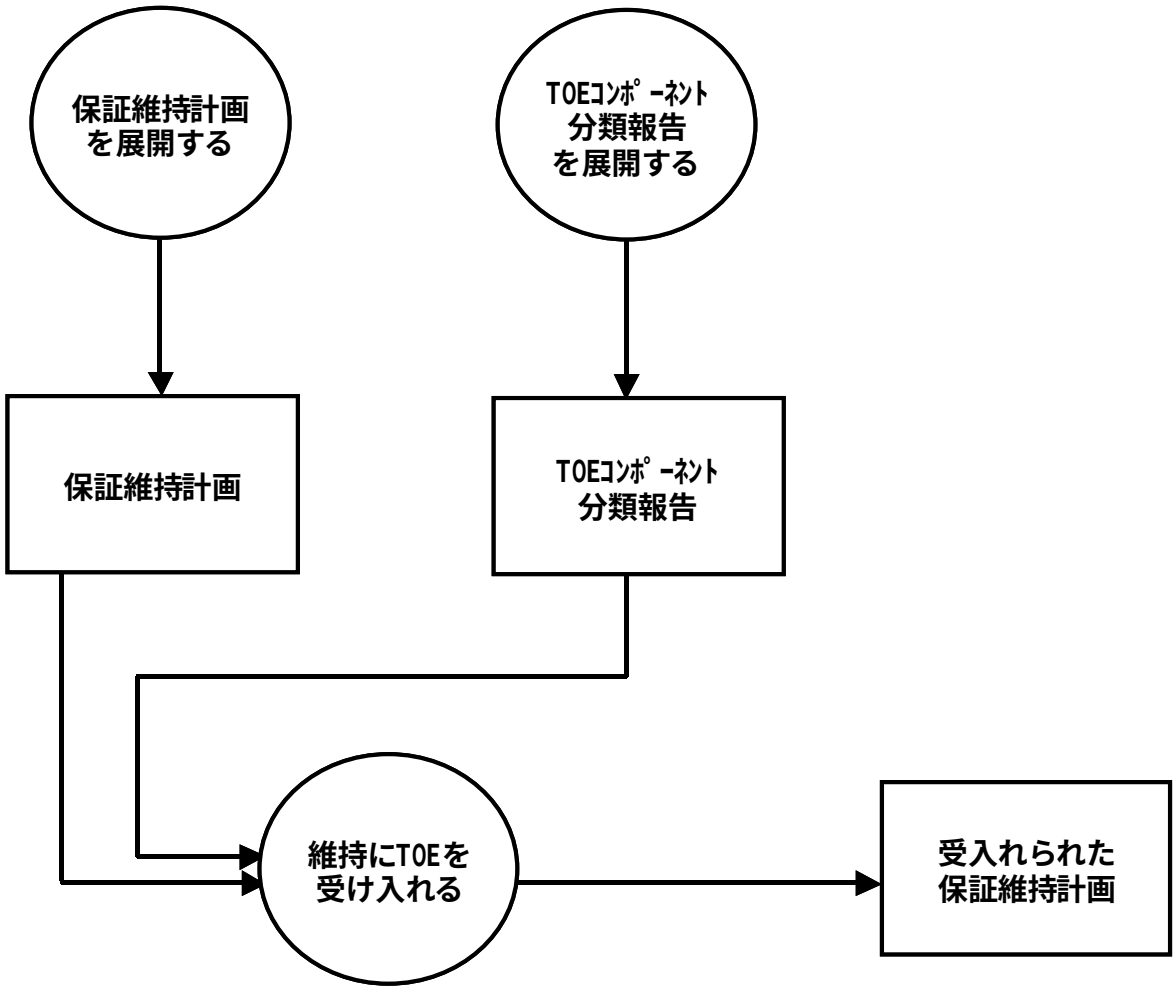

図 15.2 ― TOE 受入手法の例

15.2.2 TOE 監視

保証維持サイクルの **TOE** 監視フェーズは、次のように詳細化される。そこでは、**AMA** クラスの保証維持の証拠とセキュリティ影響分析ファミリが使用されている。

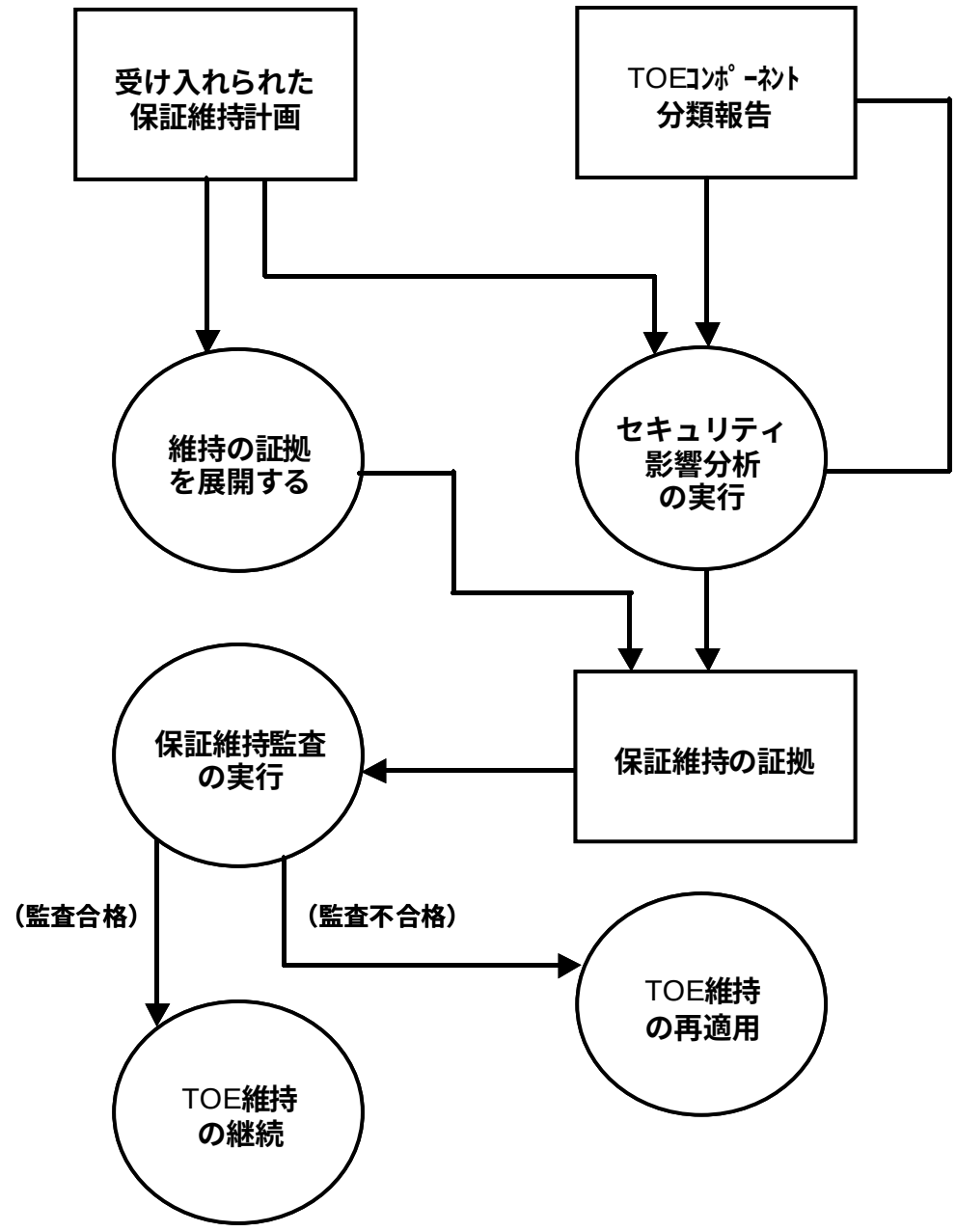

図 15.3 ― TOE 監視手法の例

15.2.3 再評価

この例の維持サイクルの **3** 番目のフェーズは、再評価フェーズである。このフェーズでは、評価者は、影響分析と保証維持の証拠を使って **TOE** の各部分を再テストする。その場合、対象保証レベルに適用可能な保証コンポーネントが使用される。

再評価アクティビティは、**AM** 計画でスケジュールされるか、または保証維持アクティビティが不適切とみなされる **TOE** またはその環境への予期されない重大な変更に対応して必要となる。

15.3 保証維持クラスとファミリ

保証維持手法をサポートするために、**AMA** クラスが開発された。これは、表 **15.1** に示す **4** つのファミリで構成されている。

保証クラス	保証ファミリ	略称
AMAクラス：保証維持	保証維持計画	AMA_AMP
	TOEコンポーネント分類報告	AMA_CAT
	保証維持の証拠	AMA_EVD
	セキュリティ影響分析	AMA_SIA

表 15.1 ― 保証維持ファミリの内訳と対応

15.3.1 保証維持計画

AM 計画は、評価結果及び **TOE** コンポーネントの分類の定義に関して、保証維持の基準線を明確に識別する。

保証維持計画（**AM** 計画）は、**TOE** またはその環境が変更されるとき、認証済み **TOE** に確立された保証が維持されることを保証するために、開発者が実施する計画と手続きを識別する。**1** つの **AM** 計画が **1** つの保証維持サイクルを扱う。

AM 計画は、再評価を起動せずに **TOE** に行うことができる変更の範囲を定義する。従うべき特定の手法は、スキームに依存するが、次の変更のタイプは、**AM** 計画の範囲外であり、再評価によってのみ対処される。

a) セキュリティターゲットに対する重大な変更（つまり、セキュリティ環境、セキュリティ対策方針またはセキュリティ機能要件の重大な変更、または保証要件の何らかの追加）

b) **TSP** 実施と分類された外部 **TSF** インタフェースに対する重大な変更

c) （保証要件に **ADV_HLD.1** または上位コンポーネントが含まれる場合）**TSP** 実施と

分類された **TSF** サブシステムへの重大な変更

保守中に行われる変更の手法は、評価された構成のセキュリティの自動的検証のサポートを助ける、**TOE** が提供する機能による影響を受けることに注意しなければならない。そのような機能は、不適切なまたは損害を与える変更が、運用中の **TOE** に適用されるのを妨げる。

規則のさらに詳細な規定は、**CC** の範囲外である。特にそれは重大な変更を構成するものの定義は、評価される **TOE** のタイプとセキュリティターゲットの内容に依存するためである。

AM 計画は、**TOE** の保証が保証維持サイクルの間維持されることを保証するために適用される手続きを定義するか参照する必要がある。適用すべき **4** つのタイプの手続きが識別されている。

a) 構成管理手続き。開発者のセキュリティ影響分析のサポートによって **TOE** への変更を管理、記録するとともに、証拠資料（**AM** 計画自体を含む）をサポートする。

b) 「保証の証拠」を維持する手続き（つまり、適切な保証要件が必要とする文書の証拠の維持)。これの重要な面は、**TOE** のセキュリティ機能の機能テストと、特に開発者の回帰テスト方針である。

c) **TOE** に影響を与える変更（これには、識別し、追跡する必要がある新しい脅威または攻撃方法など、**TOE** 環境内の変化が含まれることに注意）のセキュリティ影響分析、及び変更が行われるときの **TOE** コンポーネント分類報告の維持を支配する手続き。

d) 報告されたセキュリティの欠陥の追跡と修正を扱う欠陥修正手続き（**ALC_FLR.1** が必要とする)。

AM 計画は、保証維持サイクルの終了（つまり、予定された再評価の完了）まで有効であることが期待されている。その後は、新しい **AM** 計画が必要となる。**AM** 計画は、開発者が計画に従わない場合、または計画の範囲外の変更を **TOE** に行う場合、または **TOE** がその環境に対する有効性を保つためにそのような変更を行わなければならない場合、無効になることが期待される。新しい監視フェーズに入る前に,更新された **AM** 計画が再提出され、受け入れられなければならない。

AM 計画は、開発者が保証維持プロセスをモニタする責任を持つ開発者セキュリティ分析者を識別することを要求する。この役割は、複数の個人が担うことができる。開発者セキュリティ分析者は、役割を担うための必須の前提条件として、**TOE**、評価結果及び適用可能な保証要件を理解している必要がある。要件は、到達すべき知識と経験のレベルを特定しない。ただし、将来の開発者セキュリティ分析者は、なんらかの訓練プログラムを受け、知識または経験の不足を補う必要がある。開発者セキュリティ分析者は、**AM** 計画の要件とそれに関係する手続きが守られることを保証するために、開発者の組織内で十分な権限を持つ必要がある。

15.3.2 TOE コンポーネント分類報告

TOE コンポーネント分類報告の目的は、セキュリティとの関係において **TOE** のコンポーネント（例えば、**TSF** サブシステム）を分類することにより、**AM** 計画を補足することである。こ

の分類は、開発者のセキュリティ影響分析と **TOE** のその後の再評価に対して中心的な働きをする。
TOE コンポーネント分類報告のチェックは、受入フェーズ中に行われる。評価者のチェックは、**TOE** の認証済みバージョンに対する報告のバージョンに関してのみ適用される。**AM** 計画に識別された保証維持手続きは、**TOE** に変更が行われるときに開発者が **TOE** コンポーネント分類報告を更新することを要求するが、評価者は、その文書を再レビューすることを要求されない。ただし、そのような更新は、監視フェーズで検査される可能性が高い。

TOE コンポーネント分類報告は、維持されている保証レベルに対するすべての **TSF** 表現を扱う。
TOE コンポーネント分類報告は、以下のものも識別する。

a)TOE の外部にあり（例えば、ハードウェアまたはソフトウェアプラットフォーム）、**ST** に定義されている **IT** セキュリティ要件を満たすハードウェア、ファームウェアまたはソフトウェアコンポーネント。

b) 修正された場合、**TOE** がその **ST** に適合するという必要な保証に影響する開発ツール。

TOE コンポーネント分類報告は、**TOE** コンポーネントの分類に使用される手法の記述も提供する。少なくとも、**TOE** コンポーネントは、“ **TSP** 実施 ” または “ **TSP** 実施以外 ” のいずれかとして分類されなければならない。分類スキームの記述は、開発者セキュリティ分析者が新しい **TOE** コンポーネントが割り付けられるカテゴリ、及び **TOE** またはその **ST** への変更の後に既存の **TOE** コンポーネントのカテゴリを変更する時を決定できるようにすることを意図している。

TOE コンポーネントの最初の分類は、**TOE** の評価をサポートするために開発者が提供し、評価者が独立に正当性を確認する証拠に基づいて行われる。文書の維持は、開発者セキュリティ分析者の責任であるが、その最初の内容は、**TOE** 評価の結果に基づく。

TOE の将来のバージョンに保証が維持される要件が存在するところでは、**ST** に **AMA_CAT.1** を含めると役に立つ。これは、保証維持がこのクラスの要件の適用により達成されるか、または **TOE** の定期的な再評価によって達成されるかに関係なく適用される。

15.3.3 保証維持の証拠

TOE の保証が **AM** 計画に従って開発者によって維持されているという確信が確立される必要がある。これは、**TOE** の保証が維持されていることを実証する証拠（評価者によって独立にチェックされる）の提供を通して達成される。このチェック（「**AM** 監査」と呼ぶ）は、一般的に **TOE** の保証維持サイクルの監視フェーズ中に定期的に適用される。

AM 監査は、**AM** 計画に定義されている予定に従って行われる。そこで、**AMA_EVD.1** が要求する開発者と評価者のアクションは、保証維持サイクルの監視フェーズ中で **1** 度以上呼出される。評価者は、**TOE** 開発環境を訪れて、必要な証拠を調べる必要がある。ただし、チェックを行う他の方法も、排除されていない。

開発者は、**AM** 計画に参照されている保証維持手続きが守られているという証拠を提供する必要がある。これには次のものが含まれる。

a) 構成管理記録

b) セキュリティ影響分析によって参照されている証拠資料。例えば、**TOE** コンポーネント分類報告の現行バージョン、及び設計の更新、テスト証拠資料、ガイダンス文書の新しいバージョンなどのすべての適用可能な保証要件の証拠。

c) セキュリティ欠陥の追跡の証拠

開発者のセキュリティ影響分析（**AMA_EVD.1** が依存する **AMA_SIA.1** が必要とする）の評価者のチェックは、**AM** 監査の中心的な働きをする。その結果、**AM** 監査は、開発者の分析の確証（その結果、分析の質に対する確信）を提供し、それにより **TOE** の現行バージョンで保証が維持されているという開発者の主張の正当性を確認することに役立つ。

AM 監査は、評価者が **TOE** の現行バージョンに機能テストが行われていることを確認することを要求する。これは、**TOE** セキュリティ機能が指定されたとおりに機能し続けることの確実な証拠をテスト証拠資料が提供するので、別のチェックとして強調される。評価者は、テスト証拠資料を抽出し、開発者のテストが、セキュリティ機能が指定されたとおりに機能し、テストのカバレージと深さが維持されている保証レベルに釣り合うことを示していることを確認する。

15.3.4 セキュリティ影響分析

セキュリティ影響分析の目的は、認証された以降の **TOE** に影響するすべての変更がセキュリティに与える影響に対する、開発者が行う分析を通して、**TOE** に保証が維持されていることの確信を提供することである。これらの要件は、監視フェーズまたは再評価フェーズ中に適用される。

開発者のセキュリティ影響分析は、**TOE** コンポーネント分類報告に基づいて行われる。**TSP** 実施 **TOE** コンポーネントへの変更は、**TOE** が変更の後もその **ST** に適合し続けるという保証に影響することがある。そこで、そのようなすべての変更は、それらが **TOE** の保証を損なうことがないことを示すセキュリティ影響分析を必要とする。

このファミリのコンポーネントは、次に続く **AM** 監査または **TOE** の再評価のいずれかのサポートで使用することができる。

AM 監査に関しては、評価者のセキュリティ影響分析のレビューは、次に続く監査アクティビティの中心的な働きをする。監査アクティビティは、次に開発者の分析の確証を提供しなければならない。

セキュリティ影響分析は、新しいまたは修正された **TOE** コンポーネントに関して、**TOE** の認証済みバージョンからの変更を識別する。評価者は、関連する **AM** 監査または **TOE** の関連する再評価のいずれかで、この情報の正確性をチェックする。

再評価のサポートにおけるセキュリティ影響分析の提供は、**TOE** の保証の必要なレベルを確立

するために必要となる評価者の労力レベルを減らさなければならない。セキュリティ影響分析の完全な調査を必要とする **AMA_SIA.2** の適用は、再評価に最大の利益をもたらすはずである。評価者がセキュリティ影響分析を再評価で実際に使用することを希望する正確で詳細な条件は、**CC** の範囲外である。

16　AMAクラス：保証維持

保証の維持クラスは、**TOE**が**CC**に対して認証された後で適用されることを意図した要件を提供する。これらの要件は、**TOE**またはその環境に変更が行われても、**TOE**がセキュリティターゲットに適合し続けることを保証することを目的としている。そのような変更には、新たな脅威または脆弱性の発見、利用者要件の変更、認証済み**TOE**で発見されたバグの修正などがある。

このクラスは、図**16.1**に示すように、**4**つのファミリと、その中のコンポーネントの階層で構成されている。

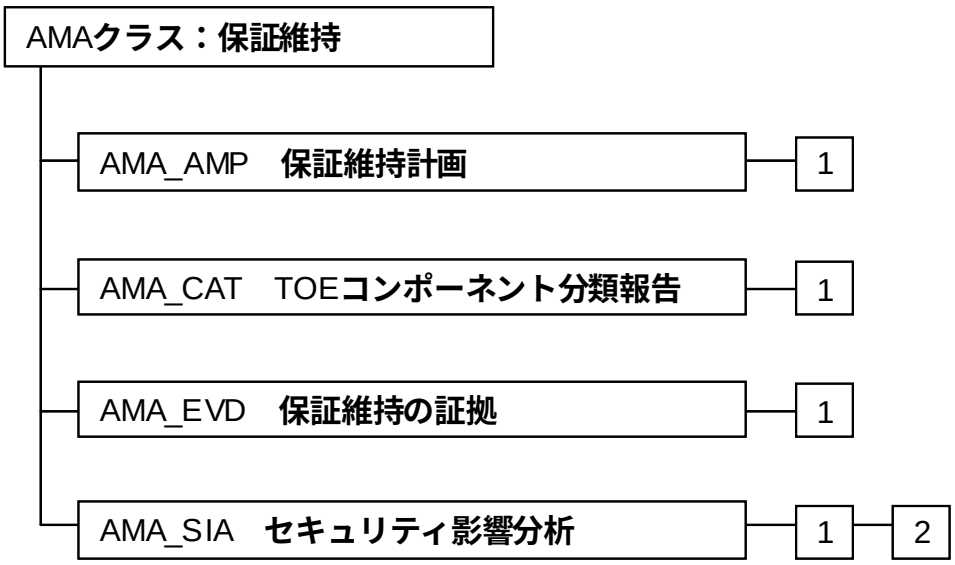

図 16.1 ― 保証維持クラスのコンポーネント構成

16.1 保証維持計画 (AMA_AMP)

目的

保証維持計画**(AM**計画**)**は、**TOE**またはその環境に変更が行われるときに、認証済み**TOE**に確立された保証が維持されることを保証するために、開発者が実行しなければならない計画と手続きを識別する。**AM**計画は、**TOE**ごとに固有のものであり、開発者自身の実務や手順に合わせて作られる。

コンポーネントのレベル付け

このファミリは、ただ**1**つのコンポーネントより成る。

適用上の注釈

AM計画は、**1**回の保証維持サイクルを扱う。これは、**TOE**の最新の評価完了から次の計画された再評価完了までの期間である。

要件**AMA_AMP.1.2C**及び**AMA_AMP.1.3C**は、**TOE**コンポーネントの分類の定義及び評価結果に関して、保証維持のための基準の明確な識別を提供する。**TOE**コンポーネント分類報告は、**AMA_CAT**ファミリの要件に従うべきもので、開発者セキュリティ分析者が行うセキュリティ影響分析の基礎となる。

AMA_AMP.1.4Cが要求するように、この計画が扱う変更の範囲の定義は、変更される**TOE**のコンポーネントのカテゴリと変更が行われる表現レベルに関するものでなければならない**(**必要に応じて、**TOE**コンポーネント分類報告を参照する**)**。

AMA_AMP.1.5Cは、**TOE**の新規リリースに対する開発者の*現行*計画の記述を必要とする。この計画は、変更されることがあり得るので、**AM**計画の更新が必要となる。ただし、この文脈において、用語「*新規リリース*」**(new release)**には、バグ修正を組み込むための**TOE**のマイナー**(**「計画されない」**)**リリースは含まれないことに注意。

AMA_AMP.1.6Cは、**AM**監査**(**下記の**AMA_EVD**ファミリを参照**)**、及び提案されたスケジュールの正当性と一緒に目標とする**TOE**再評価のための計画されたスケジュールの定義を要求する。このスケジュールは、経過時間**(**例えば、年次**AM**監査**)**に関して定義するか、または**TOE**の特定の新しいリリースに結び付けることができる。計画されたスケジュールは、その期間中に予想される**TOE**への変更、及び**TOE**の評価から**AM**計画確立までの経過期間も考慮しなければならない。特に、**AM**計画の範囲外の変更は再評価のきっかけになる。

AMA_AMP.1　保証維持計画

依存性：

ACM_CAP.2	**構成要素**
ALC_FLR.1	**基本的な欠陥修正**
AMA_CAT.1	**TOEコンポーネント分類報告**

開発者アクションエレメント：

AMA_AMP.1.1D 開発者は、AM計画を提供しなければならない。

証拠の内容・提示エレメント：

AMA_AMP.1.1C AM計画は、TOEが提供するセキュリティ機能など、TOEの簡単な記述を含むかまたは参照しなければならない。

AMA_AMP.1.2C AM計画は、TOEの認証済みバージョンを識別し、評価結果を参照しなければならない。

AMA_AMP.1.3C AM計画は、TOEの認証済みバージョンのTOEコンポーネント分類報告を参照しなければならない。

AMA_AMP.1.4C AM計画は、計画が扱うTOEへの変更の範囲を定義しなければならない。

AMA_AMP.1.5C AM計画は、TOEライフサイクルを記述しなければならず、重大なセキュリティの影響を持つと思われる計画された変更の簡単な記述と共に、TOEの新しいリリースに対する現在の計画を識別しなければならない。

AMA_AMP.1.6C AM計画では、AM監査の計画スケジュールと次回TOE再評価の目標日付を述べ、正当性を示して、保証維持サイクルを記述しなければならない。

AMA_AMP.1.7C AM計画は、TOEの開発者セキュリティ分析者の役割を担う個人(複数可)を識別しなければならない。

AMA_AMP.1.8C AM計画は、AM計画に記載または参照された手続きが守られていることを、開発者セキュリティ分析者の役割がどのようにして保証するかについて記述しなければならない。

AMA_AMP.1.9C AM計画は、TOEに影響する変更について、そのセキュリティ影響分析に関係するすべての開発者アクションが正しく実行されることを、開発者セキュリ

ティ分析者の役割がどのように保証するかを記述しなければならない。

AMA_AMP.1.10C CAM計画は、識別された開発者セキュリティ分析者が、TOEのセキュリティターゲット、機能仕様及び上位レベル設計(必要な場合)、TOEの認証済みバージョンの評価結果とすべての適用可能な保証要件を十分に理解していることの正当性を示さなければならない。

AMA_AMP.1.11C CAM計画は、TOEの保証を維持するために適用される手続きを記述または参照しなければならない。これには、少なくとも、構成管理、保証証拠の維持、TOEに影響する変更のセキュリティ影響分析の実行、及び欠陥修正の手続きが含まれなければならない。

評価者アクションエレメント：

AMA_AMP.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AMA_AMP.1.2E 評価者は、提示されたTOEのAM監査と再評価のスケジュールが受け入れることができるものであること、及び提示されたTOEの変更と矛盾していないことを確認しなければならない。

16.2 TOEコンポーネント分類報告 (AMA_CAT)

目的

TOEコンポーネント分類報告の目的は、**TOE**のコンポーネント**(**例えば、**TSF**サブシステム**)**を、それらのセキュリティとの関係に従って分類することにより**AM**計画を補足することである。この分類は、開発者のセキュリティ影響分析と**TOE**のその後の再評価で中心的な働きをする。

コンポーネントのレベル付け

このファミリは、ただ**1**つのコンポーネントより成る。

適用上の注釈

AMA_CAT.1.1の「最小抽象**TSF**表現」の用語は、維持されている保証のレベルに対して提供された**TSF**の最小抽象表現を表す。例えば、**TOE**が**EAL3**の保証レベルに維持される場合、最小抽象**TSF**表現は上位レベル設計であり、以下の**TOE**コンポーネントが分類されなければならない。

a) 機能仕様において識別可能なすべての外部**TSF**インタフェース

b) 上位レベル設計において識別可能なすべての**TSF**サブシステム

AMA_CATは少なくとも**2**つのカテゴリが定義されることを要求するが、開発者のセキュリティ影響分析に焦点を絞るのを助けるために、**TSF**実施カテゴリをさらに細分することが適切な場合がある**(TOE**の種別によるが**)**。例えば、**TSF**実施コンポーネントは、以下の場合に「*セキュリティに極めて重要*」または「*セキュリティをサポート*」のいずれかに分類することができる。

a) セキュリティに極めて重要な**TOE**コンポーネントは、セキュリティターゲットに定義されている少なくとも**1**つの**IT**セキュリティ機能の実施に*直接*責任を持つコンポーネントである。

b) セキュリティをサポートする**TOE**コンポーネントは、いずれの**IT**セキュリティ機能の実施にも*直接*責任を持たない**(**そのためセキュリティに極めて重要ではない**)**が、**IT**セキュリティ機能を支援すると当てにされているコンポーネントである。このカテゴリには、**TOE**コンポーネントの以下の**2**つの明確なタイプが含まれる。

- セキュリティに極めて重要な**TOE**コンポーネントにサービスを提供し、そのために正しく働くことが当てにされるコンポーネント
- そのようなサービスは提供しないが、不正な方法でふるまう**(**脆弱性を導入する**)**ことがないという信頼が必要なコンポーネント

AMA_CAT.1.3Cは、そのツールが修正された場合、**TOE**がセキュリティターゲットに適合していることの保証に影響するすべての開発ツール**(**例えば、オブジェクトコードを作成するために使われるコンパイラ**)**の識別を必要とする。

AMA_CAT.1　TOE コンポーネント分類報告

依存性：

ACM_CAP.2　構成要素

開発者アクションエレメント：

AMA_CAT.1.1D 開発者は、**TOE**の認証済みバージョンの**TOE**コンポーネント分類報告を提供しなければならない。

証拠の内容・提示エレメント：

AMA_CAT.1.1C **TOE**コンポーネント分類報告は、抽象度が最も高いものから低いものまでの各**TSF**表現において識別し得る**TOE**の各コンポーネントを、セキュリティとの関連性によって分類しなければならない。少なくとも、**TOE**コンポーネントは、**TSP**実施または非**TSP**実施のいずれかに分類されなければならない。

AMA_CAT.1.2C **TOE**コンポーネント分類報告は、**TOE**に導入される新しいコンポーネントをどのように分類するか、及び**TOE**またはセキュリティターゲットの変更に伴い、いつ既存の**TOE**コンポーネントを再分類するかを決定できるようにするために、使用される分類スキームを記述しなければならない。

AMA_CAT.1.3C **TOE**コンポーネント分類報告は、改変された場合に**TOE**がセキュリティターゲットを満たすという保証に影響する、開発環境で使われるすべてのツールを識別しなければならない。

評価者アクションエレメント：

AMA_CAT.1.1E 評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AMA_CAT.1.2E 評価者は、**TOE**コンポーネントとツールの分類、及び使用される分類スキームが適切であり、認証済みバージョンの評価結果と矛盾していないことを確認しなければならない。

16.3　保証維持の証拠 (AMA_EVD)

目的

このファミリの目的は、**TOE**の保証が**AM**計画に従って開発者によって維持されていることの確信を確立することである。これは、評価者によって独立にチェックされる、**TOE**の保証が維持されていることを実証する証拠の提供によって達成される。このチェックは、「**AM**監査」と呼ばれ、**AM**計画が終了するまでの間に定期的に適用される。

コンポーネントのレベル付け

このファミリは、ただ**1**つのコンポーネントより成る。

適用上の注釈

このファミリには、**ACM**、**ATE**、及び**AVA**のクラスに定義されている保証要件と同様のいくつかの証拠要件が含まれる。ただし、**AM**監査は、評価者がこれらのクラスのコンポーネントが要求するのと同程度に証拠を調査することを要求しない。むしろ、保証維持手続きが正しく守られていることの確信を確立するために、サンプリング方式を要求する。

AM監査の一部として、評価者は、**TOE**の認証済みバージョンから変更された**TOE**のコンポーネントの識別に関して、構成リストとセキュリティ影響分析が**TOE**の現行バージョンと一貫性があることをサンプリング方式によりチェックする。

AMA_EVD.1.3Cは、**AM**計画の保証維持手続きが守られていることの証拠の提供を要求する。これは、**AMA_AMP.1.11C**に参照されているすべての手続き、つまり、構成管理、保証証拠の維持、セキュリティ影響分析の実行、及び欠陥修正に関係する手続きの適用の証拠を扱う。

AMA_EVD.1.4Cで要求される証拠には、**TOE**の現行バージョンの識別された脆弱性のリストの提供が含まれる。これは、元の評価保証要件と同じレベルまで、現行バージョンに、**TOE**環境で悪用可能なセキュリティの弱点が含まれていないことを保証する重要性から、別の要件として強調される。**AMA_EVD_1.4C**のリストには、下記から生じる脆弱性が含まれなければならない。

- **a)** **AVA_VLA.1**または上位のコンポーネント**(TOE**の認証済みバージョンが必要とする場合**)**が要求する開発者の分析
- **b)** **ALC_FLR.1(TOE**の認証済みバージョンが必要とする場合は**ALC_FLR.2)**が要求する欠陥修正手続きが扱う、その他の報告されたセキュリティ欠陥

AMA_EVD.1.5Eは、機能テストが**TOE**の現行バージョンで行われていること、及びテストのカバレージと深さが、維持されている保証のレベルと同等であるということを評価者が確認することを要求する。このチェックは、**TOE**の現行バージョンのテスト証拠資料のサンプリングによって行われる。

AMA_EVD.1　維持プロセスの証拠

依存性：

AMA_AMP.1　保証維持計画
AMA_SIA.1　セキュリティ影響分析のサンプリング

開発者アクションエレメント：

AMA_EVD.1.1D 開発者セキュリティ分析者は、**TOE**の現行バージョンに対する**AM**証拠資料を提供しなければならない。

証拠の内容・提示エレメント：

AMA_EVD.1.1C **AM**証拠資料には、構成リストと**TOE**の識別された脆弱性のリストが含まれなければならない。

AMA_EVD.1.2C 構成リストは、**TOE**の現行バージョンを構成する構成要素を記述しなければならない。

AMA_EVD.1.3C **AM**証拠資料は、**AM**計画に記載または参照されている手続きが守られているという証拠を提供しなければならない。

AMA_EVD.1.4C **TOE**の現行バージョンの識別された脆弱性のリストは、各脆弱性に対して、その脆弱性が**TOE**の意図された環境で悪用できないことを示さなければならない。

評価者アクションエレメント：

AMA_EVD.1.1E 評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AMA_EVD.1.2E 評価者は、**AM**計画に記載または参照されている手続きが守られていることを確認しなければならない。

AMA_EVD.1.3E 評価者は、**TOE**の現行バージョンのセキュリティ影響分析が構成リストと一貫性があることを確認しなければならない。

AMA_EVD.1.4E 評価者は、**TOE**の現行バージョンのセキュリティ影響分析に記載されているすべての変更が**AM**計画によって扱われている変更の範囲内であることを確認しなければならない。

AMA_EVD.1.5E 評価者は、維持されている保証レベルと同等の程度まで、TOEの現行バージョン対する機能テストが実行されたことを確認しなければならない。

16.4　セキュリティ影響分析 (AMA_SIA)

目的

セキュリティ影響分析の目的は、**TOE** が認証された以降の **TOE** に影響するすべての変更のセキュリティへの影響について開発者が行う分析を通して、**TOE** に保証が維持されているという確証を提供することである。

コンポーネントのレベル付け

このファミリは、**2**つのコンポーネントで構成されている。それらは、評価者が開発者のセキュリティ影響分析の正当性を確認する度合いに従ってレベル付けされている。

適用上の注釈

AMA_SIA.1は、サンプリング方式により開発者のセキュリティ影響分析の正当性を確認することを要求する。**TOE**の現行バージョンに保証が維持されていることの確信を確立するのにサンプリング方式が十分とは思えないが、正式の再評価は必要ないと考えられる場合、**AMA_SIA.2**の方が好ましいことがある。

このファミリの両方のコンポーネントは、**TOE**の現行バージョンにおける、すべての新しい、及び修正された**TOE**コンポーネント**(**認証済みバージョンと比較して**)**を識別するためのセキュリティ影響分析を要求する。この情報の正確性は、**(**サンプリングによる**)**関連する**AM**監査、または、構成リストが**ACM_CAP**のもとでチェックされるときは、関連する**TOE**の再評価のどちらかを通してチェックされる。

AMA_SIA.1　セキュリティ影響分析のサンプリング

依存性：

AMA_CAT.1　TOEコンポーネント分類報告

開発者アクションエレメント：

AMA_SIA.1.1D　開発者セキュリティ分析者は、TOEの現行バージョンに対して、認証済みバージョンと比較してTOEに影響するすべての変更を扱うセキュリティ影響分析を提供しなければならない。

証拠の内容・提示エレメント：

AMA_SIA.1.1C　セキュリティ影響分析は、TOEの現行バージョンが由来する認証済みTOEを

識別しなければならない。

AMA_SIA.1.2C セキュリティ影響分析は、TSP実施として分類されたすべての新しい、及び修正されたTOEコンポーネントを識別しなければならない。

AMA_SIA.1.3C セキュリティ影響分析は、セキュリティターゲットまたはTSF表現に影響する各変更に対して、変更と、それが下位の表現レベルに対して及ぼすあらゆる影響について簡潔に記述しなければならない。

AMA_SIA.1.4C セキュリティ影響分析は、セキュリティターゲットまたはTSF表現に影響する各変更に対して、変更による影響を受けるすべてのITセキュリティ機能、及びTSP実施として分類されたすべてのTOEコンポーネントを識別しなければならない。

AMA_SIA.1.5C セキュリティ影響分析は、TSFの実装表現またはIT環境の修正をもたらす各変更に対して、要求される保証レベルにおいて、TSFが変更後も正しく実装されていることを示すテスト証拠を識別しなければならない。

AMA_SIA.1.6C セキュリティ影響分析は、構成管理(ACM)、ライフサイクルサポート(ALC)、配付と運用(ADO)、及びガイダンス文書(AGD)保証クラスの各適用可能な保証要件に対して、変更された評価提供物件を識別し、各変更とそれが保証に対して及ぼす影響について簡潔な記述を提供しなければならない。

AMA_SIA.1.7C セキュリティ影響分析は、脆弱性評定(AVA)保証クラスにおいて適用可能な各保証要件に対して、変更された評価提供物件と変更されない評価提供物件を識別し、提供物件を更新するかどうかに関してとられた判断の理由を示さなければならない。

評価者アクションエレメント：

AMA_SIA.1.1E 評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AMA_SIA.1.2E 評価者は、サンプリングにより、セキュリティ影響分析が、TOEの現行バージョンで保証が維持されていることの適切な正当性とともに、変更について、適切な詳細レベルまで証拠資料を提供していることをチェックしなければならない。

AMA_SIA.2　セキュリティ影響分析の調査

依存性：

AMA_CAT.1　TOEコンポーネント分類報告

開発者アクションエレメント：

AMA_SIA.2.1D　開発者セキュリティ分析者は、**TOE**の現行バージョンに対して、認証済みバージョンと比較して**TOE**に影響するすべての変更を扱うセキュリティ影響分析を提供しなければならない。

証拠の内容・提示エレメント：

AMA_SIA.2.1C　セキュリティ影響分析は、**TOE**の現行バージョンが由来する認証済みの**TOE**を識別しなければならない。

AMA_SIA.2.2C　セキュリティ影響分析は、**TSP**実施として分類されたすべての新しい、及び修正された**TOE**コンポーネントを識別しなければならない。

AMA_SIA.2.3C　セキュリティ影響分析は、セキュリティターゲットまたは**TSF**表現に影響する各変更に対して、変更と、それが下位の表現レベルに対して及ぼすあらゆる影響について簡潔に記述しなければならない。

AMA_SIA.2.4C　セキュリティ影響分析は、セキュリティターゲットまたは**TSF**表現に影響する各変更に対して、変更による影響を受けるすべての**IT**セキュリティ機能及び**TSP**実施として分類されたすべての**TOE**コンポーネントを識別しなければならない。

AMA_SIA.2.5C　セキュリティ影響分析は、**TSF**の実装表現または**IT**環境の修正をもたらす各変更に対して、要求される保証レベルにおいて、**TSF**が変更後も正しく実装されていることを示すテスト証拠を識別しなければならない。

AMA_SIA.2.6C　セキュリティ影響分析は、構成管理**(ACM)**、ライフサイクルサポート**(ALC)**、配付と運用**(ADO)**、及びガイダンス文書**(AGD)**保証クラスの各適用可能な保証要件に対して、変更された評価提供物件を識別し、各変更とそれが保証に対して及ぼす影響について簡潔な記述を提供しなければならない。

AMA_SIA.2.7C　セキュリティ影響分析は、脆弱性評定**(AVA)**保証クラスにおいて適用可能な各保証要件に対して、変更された評価提供物件と変更されない評価提供物件を識別し、提供物件を更新するかどうかに関してとられた判断の理由を示さなけれ

ばならない。

評価者アクションエレメント：

AMA_SIA.2.1E 評価者は、提供された情報が証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

AMA_SIA.2.2E 評価者は、サンプリングにより、セキュリティ影響分析が、**TOE**の現行バージョンで保証が維持されていることの適切な正当性とともに、**すべての**変更について、適切な詳細レベルまで証拠資料を提供していることをチェックしなければならない。

17　附属書A（参考）保証コンポーネントの依存性の相互参照

第 **8** 章から第 **14** 章及び第 **16** 章のコンポーネントに記述されている依存性は、保証コンポーネント間の直接の依存性である。表 **A.1** は、直接依存性と間接依存性の両方を要約している。間接依存性は、依存性があると識別されている各コンポーネントのすべての依存性を繰返し含めた累積的結果である。

Comp. Names	AUT	CAP	SCP	DEL	IGS	FSP	HLD	IMP	INT	LLD	RCR	SPM	ADM	USR	DVS	FLR	LCD	TAT	COV	DPT	FUN	IND	CCA	MSU	SOF	VLA
AUT.1-2		**3**	*1*												*1*											
CAP.1-2																										
CAP.3-4			**1**												**1**											
CAP.5			**1**												**2**											
SCP.1-3		**3**													*1*											
DEL.1																										
DEL.2-3		**3**	*1*												*1*											
IGS.1-2						*1*					*1*		**1**													
FSP.1-4											**1**															
HLD.1-2						**1**					**1**															
HLD.3-4						**3**					**2**															
HLD.5						**4**					**3**															
IMP.1-2						*1*	*2*			**1**	**1**							**1**								
IMP.3						*1*	*2*		**1**	**1**	**1**							**1**								
INT.1-2						*1*	*2*	**1**		**1**	*1*							*1*								
INT.3						*1*	*2*	**2**		**1**	*1*							*1*								
LLD.1						*1*	**2**				**1**															
LLD.2						*3*	**3**				**2**															
LLD.3						*4*	**5**				**3**															
RCR.1-3																										
SPM.1-3						**1**					*1*															
ADM.1						**1**					*1*															
USR.1						**1**					*1*															

表 A.1 ― 保証コンポーネントの依存性 [a]

Comp. Names	AUT	CAP	SCP	DEL	IGS	FSP	HLD	IMP	INT	LLD	RCR	SPM	ADM	USR	DVS	FLR	LCD	TAT	COV	DPT	FUN	IND	CCA	MSU	SOF	VLA
DVS.1-2																										
FLR.1-3																										
LCD.1-3																										
TAT.1-3						*1*	*2*	**1**		*1*	*1*															
COV.1-3						**1**					*1*										**1**					
DPT.1						*1*	**1**				*1*										**1**					
DPT.2						*1*	**2**			**1**	*1*										**1**					
DPT.3						*1*	**2**	**2**		**1**	*1*							*1*			**1**					
FUN.1-2																										
IND.1						**1**					*1*		**1**	**1**												
IND.2-3						**1**					*1*		**1**	**1**							**1**					
CCA.1-3						**2**	*2*	**2**		*1*	*1*		**1**	**1**				*1*								
MSU.1-3					**1**	**1**					*1*		**1**	**1**												
SOF.1						**1**	**1**				*1*															
VLA.1						**1**	**1**				*1*		**1**	**1**												
VLA.2-4						**1**	**2**	**1**		**1**	*1*		**1**	**1**				*1*								
AMP.1		**2**														**1**										
CAT.1		**2**																								
EVD.1																										
SIA.1-2																										

表 A.1 — 保証コンポーネントの依存性 [a]

a. 表 **A.1** において、左の列は、特定のコンポーネントのグループを表す（コンポーネント名の最後の **3** 文字とコンポーネント番号または番号の範囲のインディケータを使用している）。表のブランクではない各ボックスは、左の列のコンポーネントが依存する、列の最上位の名前とボックスの番号により識別される特定のコンポーネントを示す。太字で表された番号は、直接の依存性を示す。斜体で表された番号は、間接の依存性を表す。濃い陰影は、コンポーネント自体の交点を示す。**AMA** コンポーネントから保証コンポーネントへの依存性は、表 **A.1** に含まれている。一方、**AMA** 内部依存性は、下記の表 **A.2** に示されている。**AMA** 以外のコンポーネントから **AMA** のコンポーネントへの依存性は存在しない。そこで、表 **A.1** には、**AMA** ファミリを表す列は存在しない。

AMA Comp. Names	AMP	CAT	EVD	SIA
AMP.1		**1**		
CAT.1				
EVD.1	**1**	/		**1**
SIA.1-2		**1**		

表 A.2 — AMA 内部依存性

18 附属書B（参考）EALと保証コンポーネントの相互参照

表 **B.1** は、評価保証レベルと、保証クラス、ファミリ、及びコンポーネントとの関係を示す。

保証クラス	保証ファミリ	評価保証レベルに基づく保証コンポーネント						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
構成管理	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
配付と運用	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
開発	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
ガイダンス文書	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
ライフサイクルサポート	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
テスト	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
脆弱性評定	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

表 B.1 ― 評価保証レベルの要約