CC 及び CEM 補足文書

完全適合、選択ベースの SFR、
オプションの SFR

2017 年 5 月

バージョン 0.5

CCDB-2017-05-xxx

平成 30 年 3 月翻訳第 1.0 版
独立行政法人情報処理推進機構
技術本部　セキュリティセンター
情報セキュリティ認証室

IPA まえがき

はじめに

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

本文書の目的は別途定められた期間限定で有効な完全適合(Exact Conformance)の評価トライアルに使用を許可された CC の補足文書のドラフト「コモンクライテリア　バージョン 3.1 及び関連する情報技術セキュリティ評価のための共通評価方法」(May 2017)（以下原文）の翻訳文書である。

正式版が発行された際には、本文書を正式版で置き換えるものとする。

なお、翻訳に際しては、原文の明らかな間違いは修正し、CC/CEM の本文と原文との表現の違いに関しては原文に従って翻訳した。

原文

CC and CEM addenda

Exact Conformance, Selection-Based SFRs, Optional SFRs
CCDB-2017-05-xxx

序文

本文書は、コモンクライテリア　バージョン 3.1 及び関連する情報技術セキュリティ評価のための共通評価方法の補足文書のドラフトであり、トライアル用として使用することを承認されている。最終的な承認を得た後で、本文書は「ドラフト」の注意書きを削除してアップデートされ、これらの文書の次期バージョンに統合される予定である。

技術編集者:

文書履歴:

V0.5、2017 年 5 月 : 最初のリリース、トライアル用

特別使用分野: なし

目次

Table of contents

【訳注】[1] 原文では「Changes to *APE_CCL.1.11C* and work units associated with *APE_CCL.1.11C*」と記述されている。

1 序説

1.1 概要

1 アップデートされた CCRA は、調達者が自分達のセキュリティニーズを特定するために使用することができるメカニズムとして、cPP を導入している。CCRA の付属書 K.3 内の特定の cPP 関連の要件は、次のように言い換えられる: cPP に適合を主張する CCRA 認証書は、かかる cPP と関係するサポート文書に定義された保証要件のみをカバーし、かかる cPP に定義されたセキュリティ機能要件のみを表さなければならない。

2 このため、PP に対する ST の既存の正確適合及び論証適合の種別への追加が必要となる:つまり、上記の要件に対処するための「完全適合」の概念である。

3 正確/論証適合とは違って、PP に対する完全適合を主張する ST 作成者は、各自の判断で、(SFR 及び SAR 等の)要件を追加したり変更したりすることはできない。「完全適合」した ST に使用される要件のセット(SFR 及び SAR)は、PP においてまたは PP 構成によって定義される。このタイプの適合は、iTC(PP または PP モジュール作成者)によって選択・同意された SFR のみが、適合する ST に含まれることを保証する。

4 セキュリティ機能性の複雑性と多様性が高まるにつれ、cPP が記述するような一般的なセキュリティ課題または技術分野と密接な関係があるが、その技術のすべての実装を支援または対処するわけではない機能を、ある既定の実装が含むかもしれない。この場合、その機能性を許可されたオプションとして表現することが望ましく、その機能性を記述する SFR と関連する評価アクティビティが両方 PP に含まれているが、PP に適合するために ST 作成者によって選ばれる必要はない。そのため、本補足文書は、ST 作成者が選択することができるオプションの要件の概念も定義する。それらのオプションの要件は、追加の脅威、対策方針、または OSP を必要としない限り、完全適合の遵守を維持しながら、ST 作成者が含めるか含めないかのオプションを持つ SFR である。これによって、完全適合ステートメントを持つ PP または PP モジュールにおいて、そうでなければ可能ではないはずの柔軟性を持たせることができる。

5 次に、特定の SFR は、複雑でセキュアでない可能性のある実装を必要とするかもしれない機能を特定する選択肢を持っている。選択肢内のそのような複雑な機能性のための要件のすべてを含むことは、扱いにくく理解不可能な要件につながる可能性がある; そのため、本補足文書は、ある選択が行われた場合に ST 作成者が適合する ST に含めなければならない選択ベースの要件の概念も定義する。

6 完全適合が、正確適合または論証適合に取って代わったり、正確適合または論証適合が PP の有効な適合ステートメントであることを妨げたりすることはない。

7 完全適合ステートメント、選択ベースの SFR、及びオプションの SFR をサポートするフレームワークは、第 2 章に定義されている。CC パート 3 セキュリティ保証要件に必要とされる追加は、第 3 章に定義されており、評価方法の追加は、第 4 章に示されている。変更は、既存の CC の構成物(構成概念)と密接に関連している

ので、本補足文書の表現は、単なる独立型のテキストではなく、文脈内における既存の CC 文書（Rev.5）への変更を示す。

1.2 適用範囲

8 本文書は、プロテクションプロファイル及び PP 構成に対する「完全適合」の定義と適用に関して、選択ベースのセキュリティ機能要件（SFR）の定義と使用に関して、及び、オプションの SFR の定義と使用に関して、コモンクライテリア（CC）のフレームワークを拡張する。本文書は、選択ベースの SFR、オプションの SFR を含み、完全適合を必要とする、プロテクションプロファイルの作成と評価について、CC パート 1、パート 3、及び CEM を補完するために使用される。

1.3 読者

9 本文書は、PP 作成者、ST 作成者、及び評価者を対象としている。

1.4 規定の参照

10 以下の参照文書は、本文書に適用される。

11 [CC-1] 情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 5 版、2017 年 4 月。パート 1: 概説と一般モデル。CCMB-2017-04-001。

12 [CC-2] 情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 5 版、2017 年 4 月。パート 2:セキュリティ機能コンポーネント。CCMB-2017-04-002。

13 [CC-3] 情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 5 版、2017 年 4 月。パート 3:セキュリティ保証コンポーネント。CCMB-2017-04-003。

14 [CEM] 情報技術セキュリティ評価のための共通方法、バージョン 3.1、改訂第 5 版、2017 年 4 月。評価方法。CCMB-2017-04-004。

1.5 用語と定義

([CC-1]、4.1 節に追加)

15 本文書の目的のために、以下の用語及び定義を適用する。これらの用語は、[CC-1]、4.1 節の用語リストに含まれるものとしてみなされるべきである。

16 **完全適合(exact conformance)** - PP に含まれるすべての要件が ST にも存在し、それ以外の要件は存在しない、PP と ST 間の階層的関係で、「正確適合」の特別なケースである。

17 完全適合は、PP 作成者が、PP で表現される機能性及び保証要件のみが、適合する PP 構成、PP、または ST にて主張されることを要求する場合に使用されることが想定される。

18 **オプションのセキュリティ機能要件(optional Security Functional Requirement)** − PP のセキュリティ課題記述の言及された側面に貢献するが、適合する ST の SFR リストに含めることも含めないことも可能な、プロテクションプロファイルにおける SFR。

19 **選択ベースのセキュリティ機能要件(selection-based Security Functional Requirement)** − PP のセキュリティ課題記述の言及された側面に貢献し、特定の PP で識別された選択操作が実行される場合には、適合する ST の SFR リストに含めなければならない、プロテクションプロファイルにおける SFR。

2 CC パート 1 への追加条項

20 完全適合、選択ベースの SFR、及びオプションの SFR の概念をサポートするために必要な追加は、CC パート 1 を通して変更を必要とする。いくつかの変更は、導入される構成物（構成概念）の 1 つ以上に関連するため、本章は、[CC-1]への変更を順番に構成している。

2.1 *8.1.3 選択操作への変更*

([CC-1]、8.1.3 節に追加; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

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

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

a) 選択を未完了のままにする。

b) 1 つまたは複数の項目を選んで、選択を完了する。

c) いくつかの選択肢を削除し、2 つ以上を残すことにより、選択を制限する。

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

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

25 B.9 節に示すように、PP は、選択ベースの SFR と呼ばれる SFR のセットを定義することができる。SFR のセットは、PP における他の SFR 内の選択と関連付けられる。これらの SFR は、1) PP で識別された選択肢が、関連する選択ベースの SFR を持つことを示す場合、及び 2)その選択が PP 作成者または ST 作成者によってなされる場合、PP または ST に含まれなければならない。上記 a)の場合は、PP 作成者は選択ベースの SFR リストを変更しないままとする。上記 c)の場合は、PP 作成者は、削除された選択肢に対応する任意の選択ベースの SFR をリストから削除することとする。上記 b)の場合は、PP 作成者及び ST 作成者は、適切な選択ベースの SFR をその PP/ST の SFR リストに含めることとする。

2.2 *9.3 プロテクションプロファイルへの変更*

([CC-1]、9.3 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

26 ST が常に特定の TOE(MinuteGap v18.5 Firewall など)について記述するのに対して、PP は TOE 種別(ファイアウォールなど)について記述することを意図してい

る。したがって、異なる評価で使用される様々な ST のテンプレートとして、同じ PP を使用してもよい。PP の詳細については、附属書 B を参照のこと。

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

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

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

– 購入プロセスの一部として要件を特定する政府または大企業。

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

– PP に完全適合が要求されると記載されている場合、ST は PP に対して完全に適合しなければならない;

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

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

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

30 一般に、ST または PP は複数の PP に対する適合を主張することができるが、完全適合という性格上(つまり、PP が完全適合を要求する場合、その PP によって特定される SFR 及び SAR のみが適合する ST または PP において許可される)、追加の条項を定める必要がある。PP がその適合ステートメントにおいて完全適合を要求する場合、同時に他の PP または ST によって主張が許可される追加の PP があるなら、追加の PP(つまり、その PP *と併用を許可される* PP)についても特定しなければならない。これらの追加の PP も、その適合ステートメントにおいて完全適合を要求しなければならない。

31 そして、ST は、少なくとも 1 つの PP が完全適合ステートメントを持つ複数の PP に対して、1)ST が適合を主張しているすべての PP が完全適合要件を持つ場合、及び 2)ST が適合を主張しているすべての PP が、すべての他の PP の適合ステートメントにおいて「許可」されるものとして識別される場合のみ、完全適合を主張できる。

32 複数の PP に適合を主張する PP の場合も同様であるが、この場合、追加の条項が存在する。適合が主張されている PP の適合ステートメントは、「主張する PP」の適合ステートメントにおいてその PP を主張することが許可されているもの(つまり、*「主張を許可」*)として、「主張する PP」を識別しなければならない。

33 追加の情報については、附属書 D を参照のこと。

34 完全適合を要求しない PP が 1 つ以上あるケースにおいて、ST が複数の PP への適合を主張する場合、(上述したように)各 PP で定められる方法(つまり、正確適合か論証適合のどちらか)で各 PP に適合しなければならない。つまり、ST は一部の PP に対して正確適合し、その他の PP に対して論証適合する場合がある。

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

36 ST は、以下の場合に PP に対して同等またはより制限的である:

– ST を満たすすべての TOE が PP も満たし、かつ

– PP を満たすすべての運用環境が ST も満たす。

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

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

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

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

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

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

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

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

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

a) **セキュリティ課題定義:**

– ST は、すべての脅威、前提条件、及び OSP を含め、PP のセキュリティ課題定義を含まなければならない。PP に示されていない脅威、前提条件、または OSP は含めてはならない。

b) **セキュリティ対策方針:**

– ST は、PP 内の TOE のセキュリティ対策方針のすべてを含まなければならず、PP に示されていない追加の TOE のセキュリティ対策方針を特定することはできない;

– ST は、PP で定義されたとおり、運用環境のセキュリティ対策方針のすべてを含まなければならず、PP に示されていない追加の運用環境のセキュリティ対策方針を特定することはできない;

c) **セキュリティ要件:** ST は、次の例外を除き、PP に示されているすべての SFR と SAR を含まなければならない:

– PP においてオプションの SFR として指定されている SFR(B.9 節を参照のこと)は、完全適合する ST から除外することができる;

– PP において選択ベースの SFR として指定されている SFR(8.1.3 節及び B.9 節を参照のこと)は、ST 作成者がその含有を要求する選択をしていない場合には、除外することができる。

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

a) **セキュリティ課題定義:**

– ST は、PP のセキュリティ課題定義を含まなければならず、追加の脅威及び OSP を特定することができる; 次の 2 項目で説明される 2 つの例外を除き、PP 内で定義されたとおり、すべての前提条件を含まなければならない;

– PP 内で特定された前提条件(または前提条件の一部)に対処する、PP 内で定義された運用環境のセキュリティ対策方針のすべてが、ST 内の TOE のセキュリティ対策方針に置き換えられる場合、この前提条件(または前提条件の一部)を、ST より省略することができる;

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

b) **セキュリティ対策方針**:

– ST は、PP の TOE のセキュリティ対策方針のすべてを含まなければならず、追加の TOE のセキュリティ対策方針を特定することもできる;

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

– ST は、PP での特定の運用環境のセキュリティ対策方針が、ST 内の TOE のセキュリティ対策方針であることを特定することができる。これは、セキュリティ対策方針の*再割付*と呼ばれる。セキュリティ対策方針が TOE に再割付される場合、セキュリティ対策方針の根拠では、どの前提条件が、または前提条件の一部がもはや必要でないかを、明確にしなければならない;

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

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

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

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

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

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

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

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

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

2.3 *9.5 複数のプロテクションプロファイルの使用への変更*

([CC-1]、9.5 節に追加; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

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

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

45 しかし、上述のとおり、完全適合を要求する PP には追加の条項があり、上述の連鎖に使用されるすべての PP は完全適合ステートメントを要求し、その連鎖内のすべての他の PP との結合が許可される連鎖内のすべての PP を識別する。さらに、他の PP への適合を主張したすべての PP は、それらへの適合主張を許可されたものとして、それらの PP の適合ステートメントにリストされていなければならない。

2.4 *10.5 適合主張への変更*

([CC-1]、10.5 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

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

a) PP または ST が適合を主張する CC のバージョンを記述する。

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

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

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

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

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

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

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

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

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

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

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

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

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

48 「完全適合」の適合ステートメントを持つ PP によって特定されている任意のパッケージは、完全適合の定義により、そのパッケージの適合ステートメントが「パッケージ名適合」である場合のみ、PP または ST の適合主張において許可されることに注意するべきである。PP によって特定されていないパッケージ、または「パッケージ名追加」の主張は、完全適合ステートメントを持つ PP に対して許可されない。

49 TOE が所定の ST で正常に評価された場合、ST の適合主張は、その TOE に当てはまる点にも注意のこと。したがって、TOE は、例えば CC パート 2 適合にもなり得る。

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

a) *PP 適合* - PP または TOE は、適合結果の一部として記載されている特定の PP を満たしている。

b) *適合ステートメント*(PP のみ) - このステートメントは、PP または ST がこの PP に適合しなければならない方法、つまり完全、正確、または論証適合を記述する。完全適合の場合、ステートメントには、(完全適合主張において)PP と共に使用することが許可されている PP 及びパッケージ、この PP

を PP 構成の基本 PP として使用することができる PP モジュール、及び PP に対する適合主張を許可されている PP も含まれる。この適合ステートメントの詳細については、附属書 B を参照のこと。

51 CC のバージョン、CC パート 2 及び CC パート 3、SFR 及び SAR パッケージに関する標準の CC 適合主張、及び標準の PP 主張のほかに、

– PP 構成は、基本 PP の適合ステートメントを満たす、適合する ST に適用できる、完全適合、正確適合、または論証適合のうちの一つの適合ステートメントを提供しなければならない、

– 基本 PP が完全適合の適合ステートメントを持つ場合、その基本 PP のセット内のすべての基本 PP は、完全適合の適合ステートメントを持たなければならない;すべての基本 PP の適合ステートメントにおいて、それらの PP の組み合わせを許可しなければならない;及び、その基本 PP と共に使用される PP 構成内のすべてのモジュールを許可しなければならない。

– ST は 1 つ以上の PP 構成に適合を主張することもある。1 つ以上の PP 構成への適合主張は、PP 構成に対する適合主張が、正確適合または論証適合である場合のみ許可される。

2.5 *A.5 セキュリティ機能要件(SFR)*への変更

([CC-1]、A.5 節に追加; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

52 ST のこの節では、ST が以下とどのように適合するかを記述する:

– 本国際標準のパート 2 及びパート 3;

– プロテクションプロファイル(存在する場合);

– パッケージ(存在する場合)。

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

54 プロテクションプロファイルに対する ST の適合の記述では、ST は適合が主張されているプロテクションプロファイル [2]をリストする。この説明については、10.5 節を参照のこと。

55 パッケージに対する ST の適合の記述では、ST は適合が主張されているパッケージをリストする。この説明については、10.5 節を参照のこと。

56 セキュリティターゲットは、標準プロテクションプロファイルと同じ方法で PP 構成を使用できる。つまり、ST の適合主張には、ST が適合する PP 構成を識別する PP

【訳注】[2] 原文では「packages」と記述されている。

主張を含めることができる。しかし、PP 構成が完全適合を要求する場合、ST は単一の PP 構成を主張するのみしかできず、他の PP 構成を組み合わせることはできない。

2.6 *A.9.1 セキュリティ機能要件(SFR)への変更*

([CC-1]、A.9.1 節に追加; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

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

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

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

58 ST で特定される SFR は、PP で特定される SFR、及び附属書 D で概説される PP の適合ステートメントに依存する。ST が主張する、すべてのオプションの SFR 及び選択ベースの SFR は、この節に含まれる。

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

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

2.7 *B.2 PP の必須の内容への変更*

([CC-1]、B.2 節を変更、段落 444;「f) セキュリティ要件」の項目のみ、下記のとおり変更されている。)

f) TOE のセキュリティ対策方針から標準化された言語への書き換えを提供する*セキュリティ要件*。この標準化された言語は、SFR の形式をとる。SFR のセットには、オプションの SFR 及び選択ベースの SFR を含む。また、この節では SAR について定義する;

2.8 *B.5 適合主張(APE_CCL)への変更*

([CC-1]、B.5 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

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

62 PP の適合ステートメントでは、ST 及び/またはその他の PP がその PP にどのように適合しなければならないかを述べる。PP 作成者は、「完全」適合、「正確」適合、または「論証」適合のいずれを要求するかを選択する。「完全」適合を要求する場合、PP 作成者は以下の情報を特定するオプションもある:

63 A) PP または ST が、対象の PP と組み合わせて適合を主張でき、さらに完全適合も維持される、その他の PP。

64 B) PP または ST が、対象の PP と組み合わせて適合を主張でき、さらに完全適合も維持されるパッケージ。

65 C) PP 構成において対象の PP を基本 PP として特定し、その PP モジュールと一緒に使用できる PP モジュール。

66 D) 対象の PP に対する適合主張を許可され、さらに完全適合も維持される、その他の PP。

67 これに関するより詳細については、附属書 D を参照のこと。

2.9 *B.9 セキュリティ要件(APE_REQ)への変更*

([CC-1]、B.9 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

68 この節は、以下に概説されるオプションの SFR 及び選択ベースの SFR の仕様を除いて、A.9 節で説明した ST のセキュリティ要件の節と同じである。ただし、PP において操作を完了する際の規則は、ST において操作を完了する際の規則とはやや異なっている点に注意のこと。これについては、8.1 節でより詳細に説明する。

69 PP は、オプションの SFR として SFR のセットを識別できる。これらの SFR は、適合する PP または ST に含めることができ、たとえそれらを含めた PP の適合ステートメントが完全適合を要求する場合でも可能である。

70 PP は、選択ベースの SFR のセットを識別できる。選択ベースとして識別される各 SFR(または SFR のセット)については、PP 作成者は、その PP に含まれる SFR の特定の選択と、その選択が他の PP または ST 作成者によってなされた場合に含まれるべき選択ベースの SFR との間の依存性を PP が明確に示すことを更に保証する。

2.10 *B.13.2 適合主張への変更*

([CC-1]、B.13.2 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

71 PP 構成と同じ方法で解釈する PP の適合主張には、以下が含まれる:

– 基本 PP において適合が主張される PP への適合。

– 基本 PP からの SAR パッケージ(定義済み EAL を含む)への適合。異なる EAL を持つ基本 PP を結合する問題は、それらのすべての PP に適合する ST のように取り扱われなければならない(つまり、ST はすべての基本 PP の最低 EAL のレベルを主張しなければならない)。

– 基本 PP からの適合ステートメント(完全適合、正確適合、または論証適合)。異なる適合ステートメントを持つ基本 PP を結合する問題は、それらのすべての PP に適合する ST のように取り扱われなければならない。

72 完全適合を持つ基本 PP は、他の適合の種別を持つ基本 PP と組み合わせることが許可されない点に注意のこと。

73 PP モジュールが完全適合を持つ基本 PP のセットから適合主張を継承した場合、PP モジュールもまた、その PP モジュールを持つ PP 構成(完全適合を要求する基本 PP と組み合わせて)において特定されることを許可された、その他の PP モジュールのセットをその適合ステートメントのリストに載せることができる。こうして、要件のセット(この例では、PP モジュール内の要件)の作成者達の完全適合の概念を維持することができ、その PP モジュールへの適合を主張した際に書いた要件と組み合わせて、他に特定する要件について管理することができる。

2.11 *B.13.6 セキュリティ機能要件への変更*

([CC-1]、B.13.6 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

74 PP 構成と同じ方法で解釈する PP の SFR のセットには、以下が含まれる:

– PP 構成の PP モジュールの SFR すべて。

– PP モジュールにおいて詳細化されている SFR を除く、基本 PP の SFR すべて。これは、基本 PP の選択ベース及びオプションの SFR を含むことができる。

75 評価中に PP 構成において実施される一貫性分析は、このセットが有効であることを保証しなければならない。

2.12 *B.14.5 適合主張への変更*

([CC-1]、B.14.5 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

76 この節では、以下への PP モジュールの適合について記述する:

– コモンクライテリアのパート 2: CC バージョン及び拡張セキュリティ要件、

– SFR パッケージ。

77 PP モジュールは、いかなる PP、PP モジュール、または PP 構成にも適合を主張できない。

78 PP モジュールは、基本 PP からの SAR パッケージ(定義済み EAL を含む)への適合を継承する。異なる EAL を持つ基本 PP を結合する問題は、それらのすべての PP に適合する ST のように取り扱われなければならない。

79 PP モジュールは、基本 PP からの適合ステートメント(完全適合、正確適合、または論証適合)を継承する。異なる適合ステートメントを持つ基本 PP を結合する問題は、それらのすべての PP に適合する ST のように取り扱われなければならない。

80 完全適合を持つ基本 PP は、他の適合の種別を持つ基本 PP と組み合わせることが許可されない点に注意のこと。

81 PP モジュールが完全適合を持つ基本 PP のセットから適合主張を継承した場合、PP モジュールもまた、その PP モジュールを持つ PP 構成(完全適合を要求する基本 PP と組み合わせて)において特定されることを許可された、その他の PP モジュールのセットをその適合ステートメントのリストに載せることができる。こうして、要件のセット(この例では、PP モジュール内の要件)の作成者達の完全適合の概念を維持することができ、その PP モジュールへの適合を主張した際に書いた要件と組み合わせて、他に特定する要件について管理することができる。

2.13 *B.15.1 PP 構成の必須の内容への変更*

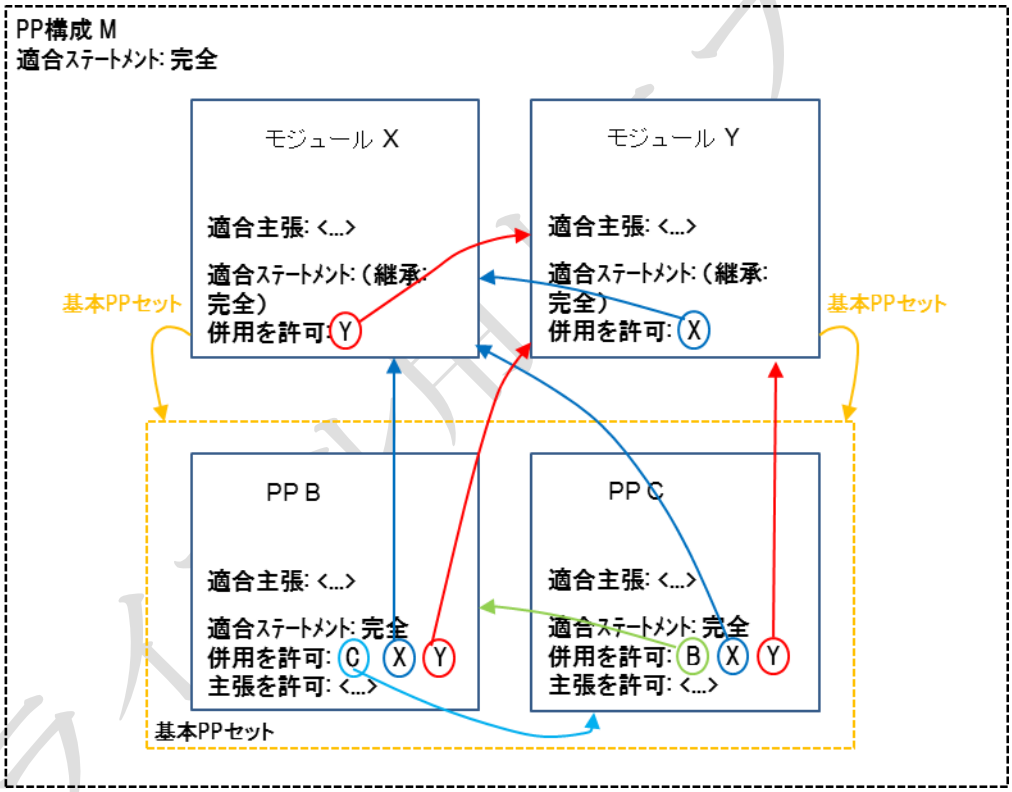
([CC-1]、B.15.1 節、段落 531 を変更; 適合ステートメントの項目のみ、下記に示すとおり変更される。)

– この PP 構成への適合が、完全適合、正確適合、または論証適合のいずれであるべきかを特定する*適合ステートメント*、

2.14 *B.15.5 PP 構成適合ステートメント[3] への変更*

([CC-1]、B.15.5 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

82 *適合ステートメント*は、このPP構成への適合が、完全適合、正確適合、または論証適合のいずれであるべきかを特定する。PP構成内の基本PP(及びPPモジュール)が完全適合ステートメントを持つ場合、そのPP構成内のすべての基本PP(及びPPモジュール)は、完全適合ステートメントを持たなければならない。更に、そのPP構成内のすべての基本PP及びPPモジュールは、それぞれの適合ステートメントにすべての他の基本PP及びPPモジュールの組み合わせを許可しなければならない。これは、以下の例に示される。



83

84 この例では、PP構成(「M」と名付ける)が、PPモジュールX及びYに対する適合ステートメントにおいて、完全適合を特定する。PPモジュールX及びYのどちらにも(共に完全適合を要求する)PP B及びPP C という2つのPPが基本PPのセットとしてリストされている。これが、「完全適合」の適合ステートメントを持つ評価可能なPP構成であるためには、以下のステートメント(図に示す)が満たされなければならない:

1. PP モジュールは、それらの基本 PP から適合ステートメントを継承するので、その適合ステートメントは完全適合である。

【訳注】[3] 原文では「B.15.5 Conformance claims」と記述されている。

2. PP モジュールが完全適合を要求するため、PP 構成は完全適合を要求しなければならない。

3. PP B は、PP C、PP モジュール X、及び PP モジュール Y と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

4. PP C は、PP B、PP モジュール X、及び PP モジュール Y と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

5. PP モジュール X は、PP モジュール Y と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

6. PP モジュール Y は、PP モジュール X と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

85 PP 構成への適合を主張するいかなる ST も、PP 構成において主張される種類の適合に適合しなければならない。

2.15 *C.2.3 選択操作* への変更

([CC-1]、C.2.3 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

86 8.1.3 節に記述されているとおり、選択操作は、特定のコンポーネントに PP/ST 作成者が複数の項目から選択しなければならないエレメントが含まれる場合に行う。

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

88 8.1.3 節はまた、選択ベースの SFR の概念について記述している。下記は、そのような SFR の例である。

89 FTP_ITC.1.1 TSF は、[選択: IPsec、SSH、TLS、HTTPS]を使用して、…間の高信頼通信チャネルを提供できなければならない

90 *適用上の注釈:*

91 *FTP_ITC.1.1 の最初の選択では、ST 作成者は TOE がサポートする 1 つまたは複数のメカニズムを選択し、それらの選択に対応して選ばれる PP の附属書 B 内の選択ベースの要件が ST に含まれることを確実にする。*

92 *(事例 PP の)**附属書 B***

93 *ST 作成者が FTP_ITC.1.1 において「IPsec」を選択した場合、以下の SFR が ST に含まれる:*

94 *FCS_IPSEC_EXT.1 [...]*

2.16 *C.5 オプションの SFR の追加*

(新規;この節は、[CC-1]の C.4 節に続く。)

95 **C.5 オプションの SFR**

96 オプションの SFR は、その PP のセキュリティ課題定義の側面に対処するが、PP 内の他の(オプションではない)SFR を補完する SFR として、プロテクションプロファイルにおいて特定される。したがって、そのような SFR を ST に含めるかどうかは、TOE が特定された機能性を支援するかどうかによって、ST 作成者の裁量に任せている。

97 ST は、正確適合主張または論証適合主張をすることによって、PP に対する適合を主張し、(PP において特定されるものに加えて)ST に SFR を追加できるため、それらの PP 内のオプションの要件は不要となることもある点に注意すべきである。しかし、完全適合を要求する PP に対する適合を主張する場合、オプションの要件は、ST が適合主張する機能性の仕様において、(PP 作成者による規制下で)制約された柔軟性を可能にするために有用な手法である。

2.17 *D.1 序説への変更*

([CC-1]、D.1 節を変更; 文脈及び適用をわかりやすくするために、節全体が下記のとおり繰り返され、変更箇所がハイライトされている。)

98 PP は、ST の「テンプレート」として使用されることを意図している。つまり、PP は利用者のニーズのセットを記述し、その PP に適合する ST はこれらのニーズを満たす TOE を記述する。

99 PP は、別の PP のテンプレートとしても使用できることに注意のこと。つまり、PP は他の PP への適合を主張することができる。この場合は、ST と PP の場合とまったく同様である。明確にするために、この附属書では ST/PP の場合のみを記述するが、この記述は PP/PP の場合にも当てはまる。

100 CC では、部分的な適合は認められない。もし、PP が主張するならば、PP または ST は、ひとつ、あるいは複数の参照 PP に完全に適合しなければならない(オプションの SFR または選択ベースの SFR の場合、CC に概説されるとおり、これらの種別の SFR の含有または排除は、それでも「完全な適合」であると見なされる点に注意のこと)。しかし、3 種類の適合(「完全適合」、「正確適合」、及び「論証適合」)があり、許可される適合の種別は、PP によって決定される。つまり、PP は、(PP 適合ステートメントで)ST に対して許可される適合の種別を記載する(B.5 節を参照のこと)。9.5 節に示されるとおり、PP が完全適合を指定する場合、ST は、その PP 単独、または、完全適合を要求する、明示的に識別された他の PP との組み合わせのいずれかである場合に限り、その PP に対して適合を主張することができる。そのような適合ステートメントが、ST が適合を主張している複数の PP に含まれている場合の正確適合と論証適合の区別は、ST が個別の基準で適合主張してもよい各 PP に適用可能である。つまり、ST は一部の PP に対して正確適

合し、その他の PP に対して論証適合する場合がある。ST が、論証適合または正確適合を要求するいかなる PP に対しても常に完全適合または正確適合できる一方で、PP が明示的に許可している場合にのみ、ST は論証可能な方法で PP に適合することが許可される。

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

102 PP 適合とは、PP または ST が（ST が評価された製品に対するものであるならば、その製品も同様に）、その PP のすべての要件を満たすことを意味する。

103 公開されている PP は通常は論証適合を要求している。これは、PP 適合を主張する ST は、PP で記述される一般的なセキュリティ課題に対する解決策を提供しなければならないが、PP で記述されるものと同等かより制限的であれば、どのような方法でも提供することができることを意味する。「同等またはより制限的」については、CC で詳細に定義されるが、ST が TOE に対して同等かそれ以上の制限を課し、TOE の運用環境に対して同等かそれ以下の制限を課すならば、原則、PP と ST は異なるエンティティの記述、異なる概念の使用など、まったく異なるステートメントを含んでもよいことを意味する。

2.18 *D.2 完全適合*の追加

(新規;この節は、[CC-1]の D.1 節に続き、完全適合、正確適合、そして論証適合の階層的な概念を保持する。） このため、現在の[CC-1]の D.2 節や D.3 節は、それぞれ、D.3 と D.4 に番号が付け替えられる。)

104 **D.2 完全適合**

105 完全適合は、PP の要件が満たされ、ST が追加の機能性を含むことなく、それらの要件(SFR)を完全に具体化していることの証拠を要求する PP 作成者を対象としている。要するに、ST は、TOE が追加の主張をすることなく、PP において要求されることを実施することを特定する。

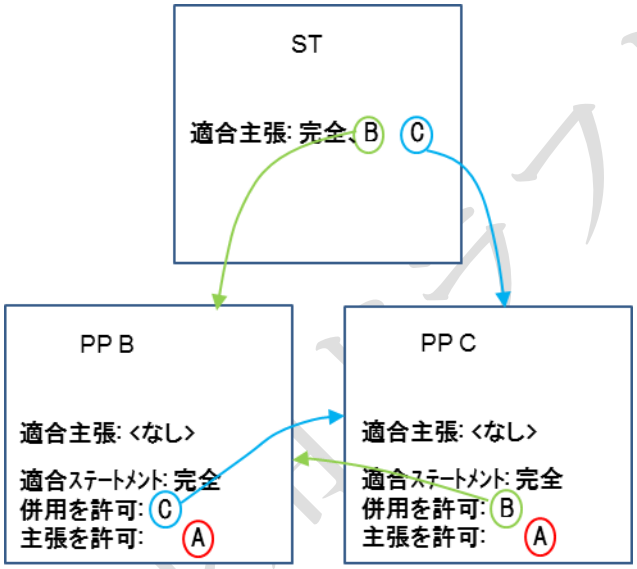
106 CC では、ST 及び PP が複数の PP に適合を主張することが可能である。このため、PP が完全適合を要求する場合、完全適合の背景にある意図を回避する可能性があり、PP 作成者は、正確適合や論証適合よりも、適合する ST のために提供される機能性及び保証をさらに管理できるようになる。例えば、ST が(完全適合を要求する)PP A と(論証適合を要求する)PP B に同時に適合を主張できる場合、これによって、ST が PP A への適合を主張する際に PP A の機能性と組み合わせて使用されることを PP A の作成者が明示的に許可していない SFR を制御することになる。

107 この問題に対処するために、PP の適合ステートメント(B.5 節を参照のこと)は、次の 2 つのステートメントを含めることができる。つまり、ST/PP 作成者が対象の PP と共に同時に適合主張をすることができる PP のステートメント(*併用を許可する*ステートメント)、及び、PP が対象の PP への適合主張を許可されるのかについてのステートメント(*主張を許可された*ステートメント)である。すべての識別された PP は、その適合ステートメントにおいて完全適合を要求しなければならず、またその

適合ステートメントにおいて対象の PP(及び主張されるそのすべての他の PP)をリストしなければならない。

108 これらの概念を明確化する例を 2 つ提示する。1 つは、複数の PP に対する適合を主張する ST に関するもので、もう 1 つは、複数の PP に対する適合を主張しようとする PP に関するものである。

109 ST の例では、PP B の作成者が、ST において PP B への適合を主張できるようにし、さらに PP C と組み合わせて PP B への適合主張もできるように望んでいるとする。この状況を説明図に表すと、以下のようになる。

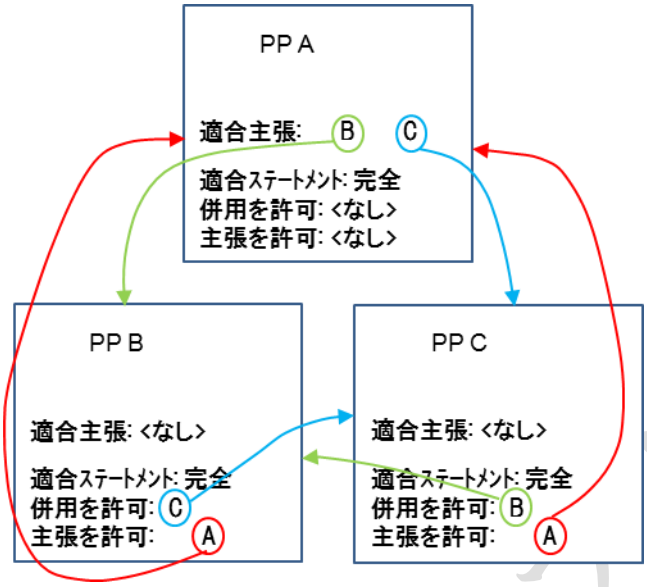


110 この場合、以下を満たす必要がある:

1. PP B と PP C はそれらの適合ステートメントにおいて完全適合を特定する必要がある。
2. PP B は、その適合ステートメントにおいて PP B と併用を許可されるものとして PP C をリストする。
3. PP C は、その適合ステートメントにおいて PP C と併用を許可されるものとして PP B をリストする。

111 これらのステートメントのいずれかが満たされなかった場合、ST は PP B と PP C の両方への(完全)適合を主張できない。なお、PP B と PP C は、PP A によるそれらへの適合主張を持つが、それは ST 適合を決定する上では関係ない点に注意のこと。

112 PP の例も同様である。この例では、PP A は PP B 及び PP C に適合を主張しようとしている。PP B と PP C は完全適合を要求しているため、PP A がこれらへの適合を主張するためには、PP A もその適合ステートメントにおいて完全適合を要求しなければならない。この状況を説明図に表すと、以下のようになる。

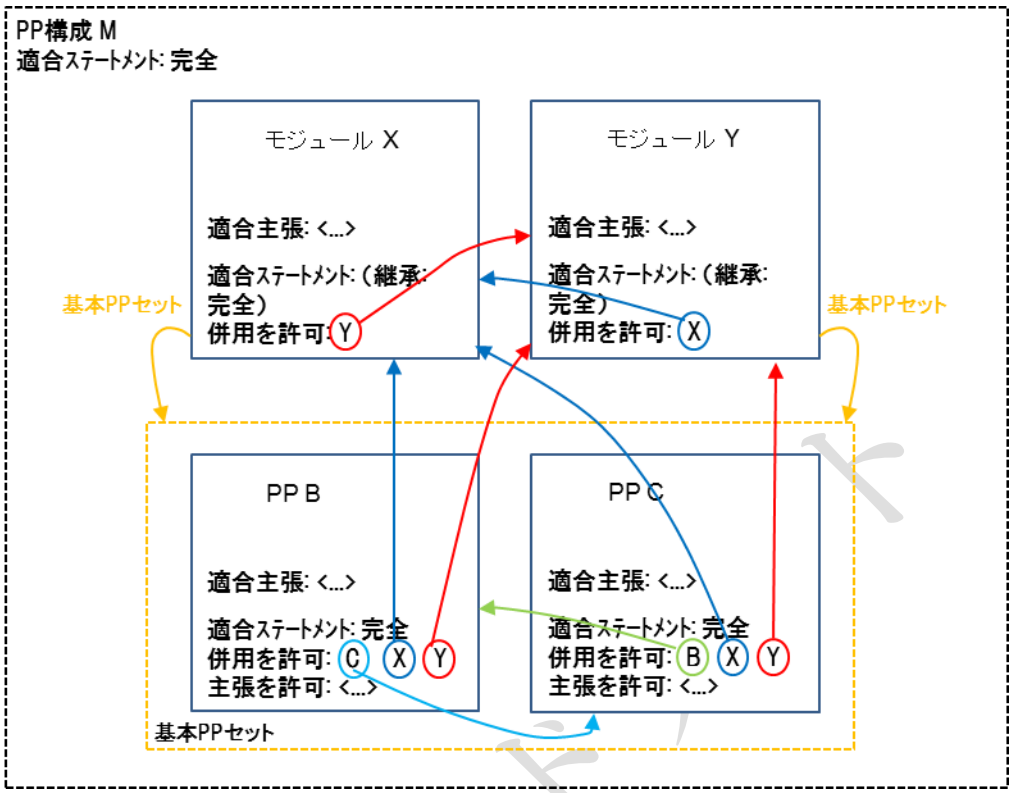


113 この場合、以下を満たす必要がある:

1. PP A、PP B、及び PP C はそれらの適合ステートメントにおいて完全適合を特定する必要がある。
2. PP B は、その適合ステートメントにおいて PP B と併用を許可されるものとして PP C をリストする。
3. PP C は、その適合ステートメントにおいて PP C と併用を許可されるものとして PP B をリストする。
4. PP A は、PP B 及び PP C の両方によって主張が許可されている PP として、それらの適合ステートメントにリストされる必要がある。

114 これらのステートメントのいずれかが満たされなかった場合、PP A は PP B と PP C の両方への(完全)適合を主張できない。

115 この概念はまた、PP モジュール及び PP 構成にも適用される。PP モジュールは基本 PP のセットを識別できる。あるセット内の基本 PP の 1 つが完全適合を要求すれば、すべての基本 PP が完全適合を要求することとなる。モジュールの要件セットが基本 PP との使用を許可されることを確実にするために、各基本 PP が(その適合ステートメントにおいて)、PP 構成で使用される基本 PP として、その基本 PP を特定できるいかなる PP モジュールも識別する。さらに、PP モジュールは、他のどの PP モジュールが PP 構成において組み合わせて使用できるかを特定するのである。その例を以下に示す:



116 この例では、PP構成(「M」と名付ける)が、PPモジュールX及びYに対する適合ステートメントにおいて、完全適合を特定する。PPモジュールX及びYのどちらにも(共に完全適合を要求する)PP B及びPP C という2つのPPが基本PPのセットとしてリストされている。これが、「完全適合」の適合ステートメントを持つ評価可能なPP構成であるためには、以下のステートメント(図に示す)が満たされなければならない;

1. PP モジュールは、それらの基本 PP から適合ステートメントを継承するので、その適合ステートメントは完全適合である。

2. PP モジュールが完全適合を要求するため、PP 構成は完全適合を要求しなければならない。

3. PP B は、PP C、PP モジュール X、及び PP モジュール Y と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

4. PP C は、PP B、PP モジュール X、及び PP モジュール Y と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

5. PP モジュール X は、PP モジュール Y と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

6. PP モジュール Y は、PP モジュール X と共に使用することが許可されることをその適合ステートメントにおいて特定しなければならない。

117 完全適合を使用する典型的な例としては、要件のセット及びそれらの要件の実装について保証を得るために必要なアクティビティについて、テクニカルコミュニティが同意しており、(また PP 及びサポート文書にもそのように特定されており)、一方で、PP に特定されていない機能性の必要性、有効性、及び保証を得るために必要な具体的な方法の解釈については、同意していない場合が挙げられる。

3 CC パート 3 への追加条項

118 [CC-3]の完全適合の概念を実装し検証するために、APE_CCL、ACE_CCL、及び ACE_CCO ファミリについて、エレメントの変更及び追加が必要となる。これらが、本章に示される。選択ベースの SFR 及びオプションの SFR を実装するために、[CC-3]で必要となる変更はない。

3.1 *APE_CCL* への変更

3.1.1 *APE_CCL.1.11C* への変更

([CC-3] APE_CCL.1.11C を変更; 既存のエレメントへの変更がハイライトされている。)

APE_CCL.1.11C 適合ステートメントは、PP に対する任意の PP/ST に必要とされる適合を、完全 PP 適合、正確 PP 適合、または論証 PP 適合として記述しなければならない。

3.1.2 *APE_CCL* への追加

(（新しい）内容エレメントを追加し、[CC-3] APE_CCL を変更。)

APE_CCL.1.12C **適合ステートメントは、評価中の PP と組み合わせて完全適合の主張が許可されているパッケージ及びその他の PP のセットを識別しなければならない。**

APE_CCL.1.13C **適合ステートメントは、評価中の PP を基本 PP として特定できる PP モジュールのセットを識別しなければならない。**

APE_CCL.1.14C **適合ステートメントは、評価中の PP に対する完全適合を主張できるその他の PP のセットを識別しなければならない。**

3.2 *ACE_CCL* への変更

3.2.1 ACE_CCL 開発者エレメントへの追加

(（新しい）開発者エレメントを追加し、[CC-3] ACE_CCL を変更。)

ACE_CCL.1.2D **開発者は、適合ステートメントを提供しなければならない。**

3.2.2 ACE_CCL 内容エレメントへの追加

(（新しい）内容エレメントを追加し、[CC-3] ACE_CCL を変更。)

ACE_CCL.1.5C **適合ステートメントは、評価中のモジュールと組み合わせて、PP 構成において使用されることができる、他の PP モジュールを識別しなければならない。**

3.3 *ACE_CCO* への変更

3.3.1 *ACE_CCO.1.3C* への変更

([CC-3] ACE_CCL.1.3C を変更; 既存のエレメントへの変更がハイライトされている。)

ACE_CCO.1.3C 適合ステートメントは、PP 構成に対して要求される適合が、完全適合、正確適合、論証適合のいずれかを特定しなければならない。適合主張は、PP 構成とその下層の基本 PP 及び PP モジュールが適合を主張する CC のバージョンを識別する CC 適合主張を含めなければならない。

4 CEM への追加条項

119 完全適合、選択ベースの SFR、及びオプションの SFR の概念をサポートするために必要な追加は、[CEM]にわたる複数のワークユニットの変更及び追加を必要とする。本章は、これらの変更について、まずファミリによってグループ分けを行い、次に特定のエレメント及び関連するワークユニットによってグループ分けを行って示す。

4.1 *APE_CCL* に関連するワークユニットへの変更

4.1.1 *APE_CCL.1.5C* に関連するワークユニットへの変更

([CEM] APE_CCL.1.5C に関連するワークユニットを変更。ワークユニット APE_CCL.1-6a、APE_CCL.1-6b、及び APE_CCL.1-7a を追加。番号後の文字は、[CEM] の既存の番号を変更しないで、本文書によってなされる変更を一意に識別するために使用される。)

APE_CCL.1-6a 評価者は、PP が適合を主張する各 PP に対して、適合主張におけるすべての他の PP がその PP と共に主張することが許可されることをその PP の適合ステートメントが許可することを*チェックしなければならない*。

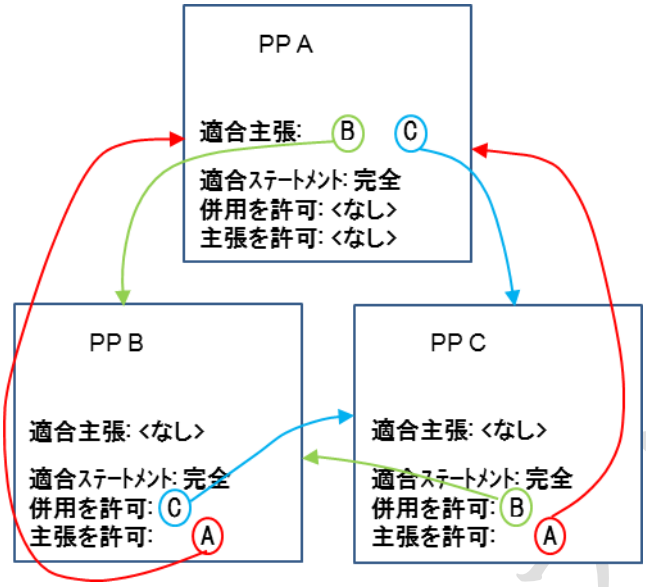
120 PP が他の PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

121 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

122 適合が主張されている PP が正確適合または論証適合を要求する場合(さらに、評価される PP が PP のセットに対する完全適合を主張している場合)、PP がその他の PP に対する完全適合を主張するなら、それらの他の PP も完全適合を要求しなければならないため、このワークユニットは不合格となる。

123 評価者は、適合が主張されている PP の適合ステートメントが、評価される PP の適合主張の節において、その PP と「共に主張することが許可」されるものとして識別された各 PP をリストすることを決定する。なお、これは、その PP が完全適合を要求する場合、及び評価される PP が完全適合を要求する場合にのみ該当する点に注意のこと。

124 例えば、PP A が評価され、PP B と PP C に適合を主張する場合を想定する。これを図にして以下に示す。すべての PP は、それらの適合ステートメントにおいて完全適合を要求する。このワークユニットでは、評価者は、PP B が(その適合ステートメントにおいて)PP B と共に(他の PP によって; この場合は PP A)主張されることができる PP として「PP C」をリストすることを決定する。同様に、評価者は、PP C が(その適合ステートメントにおいて)PP C と共に(他の PP によって; この場合は PP A)主張されることができる PP として「PP B」をリストすることを決定する。



APE_CCL.1-6b 評価者は、PP が適合を主張する各 PP に対して、その PP の適合ステートメントが、その PP と共に適合主張を許可された PP として評価される PP をリストしていることを*チェックしなければならない*。

125 PP が他の PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

126 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

127 適合が主張されている PP が正確適合または論証適合を要求する場合(さらに、評価される PP が PP のセットに対する完全適合を主張している場合)、PP がその他の PP に対する完全適合を主張するなら、それらの他の PP も完全適合を要求しなければならないため、このワークユニットは不合格となる。

128 評価者は、評価される PP が適合を主張する各 PP を検査する。評価者は、すべての PP が完全適合を要求することを決定する。評価者は、その PP の適合ステートメントが、その PP に対する適合主張を許可されたものとして評価される PP をリストすることを決定する。上記の例では、PP A(評価される PP)が、PP B と PP C それぞれの適合ステートメントにおいて、それらの PP に対する適合主張を許可されたものとして PP B と PP C の両方に(PP A は PP B と PP C の両方に対する適合を主張しているため)リストされなければならない。

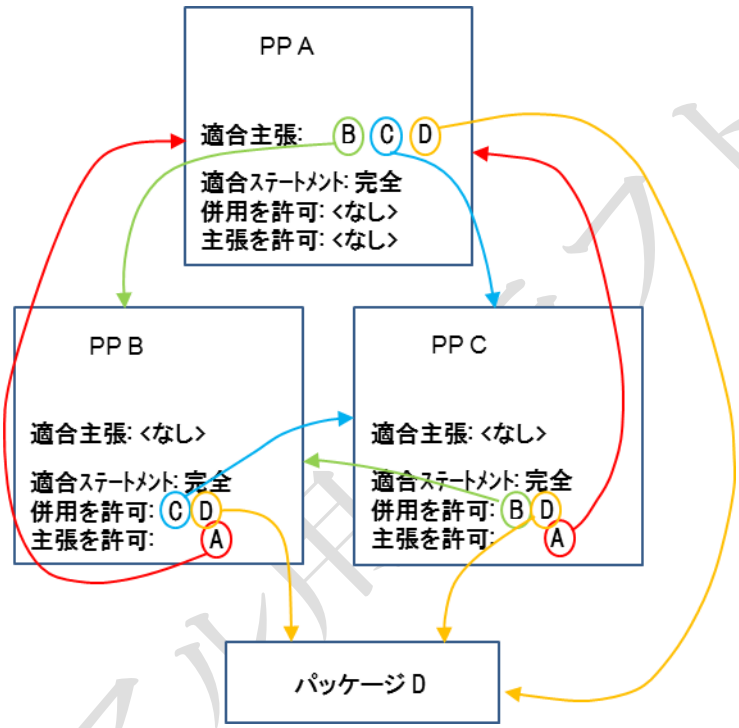
APE_CCL.1-7a 評価者は、PP が適合を主張する各 PP の適合ステートメントに、評価される PP の適合主張において識別される各パッケージがリストされていることを*チェックしなければならない*。

129 PP がパッケージへの適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

130 PP が他の PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

131 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

132 このワークユニットは、評価される PP が、1)完全適合を要求し、2)他の PP への完全適合を主張し、3)パッケージへの適合を主張する場合にのみ該当する。これらのケースでは、評価者は、適合が主張されている各 PP において、それらの PP と共に使用することが許可されるものとして(単体または複数の)パッケージがリストされていることを保証する。その例を以下に示す:



133 この例では、PP A は PP B 及び PP C に(完全)適合を主張しており、さらにパッケージ D にも適合を主張している(PP A への適合ステートメントが完全適合を要求するため、パッケージ D への適合主張はパッケージ D 適合でなければならず、パッケージ D 追加は許可されない)。したがって、このワークユニットでは、評価者は、PP B と PP C の両方への適合ステートメントを検査する。これらは、その PP と共に適合主張において使用することが許可されるものとして、パッケージ D をリストしなければならない。

4.1.2 *APE_CCL.1.6C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_CCL.1-8 を変更; 前後関係を理解するため、ワークユニット全体が複写され、変更箇所がハイライトされている。)

APE_CCL.1-8 評価者は、識別された各パッケージに対して、適合主張がパッケージ名適合またはパッケージ名追加の主張を述べていることを*チェックしなければならない*。

134 PP がパッケージに対する適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

135 パッケージ適合主張がパッケージ名適合を含む場合、評価者は以下のことを決定する:

a) パッケージが保証パッケージである場合、PP はパッケージに含まれるすべての SAR を含めるが、追加 SAR は含めない。

b) パッケージが機能パッケージである場合、PP はパッケージに含まれるすべての SFR を含めるが、追加 SFR は含めない。

136 パッケージ適合主張がパッケージ名追加を含む場合、評価者は以下のことを決定する:

a) パッケージが保証パッケージである場合、PP はパッケージに含まれるすべての SAR を含み、追加 SAR を少なくとも 1 つ、またはパッケージ内の SAR の上位階層である SAR を少なくとも 1 つ含む。

b) パッケージが機能パッケージである場合、PP はパッケージ内に含まれるすべての SFR を含み、追加 SFR を少なくとも 1 つ、またはパッケージ内の SFR の上位階層である SFR を少なくとも 1 つ含む。

c) PP への適合ステートメントは「正確適合」か「論証適合」かのどちらかである。

4.1.3 *APE_CCL.1.8C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_CCL.1-10 を変更。ワークユニット が長いため、及びマイナーな変更が必要なため、すべてのワークユニットをここで複写しない。代わりに、下記のように、ワークユニットの 3 番目の番号付きの段落として、挿入する。(つまり、既存の段落 177 と 178 の間である。))

137 評価される PP によって完全適合が要求されている場合、このワークユニットは該当しない (この PP が適合を主張している PP の適合ステートメントにおいて、評価される PP をリストする際に作業が実行されている) ため、満たされているものとみなされる。

4.1.4 *APE_CCL.1.9C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_CCL.1-11 を変更。ワークユニット が長いため、及びマイナーな変更が必要なため、すべてのワークユニットをここで複写はしない。代わりに、下記のように、ワークユニットの 2 番目の番号付きの段落として、挿入する。(つまり、既存の段落 181 と 182 の間である。))

138 評価される PP によって完全適合が要求されている場合、このワークユニットは該当しない (この PP が適合を主張している PP の適合ステートメントにおいて、評価される PP をリストする際に作業が実行されている) ため、満たされているものとみなされる。

4.1.5 *APE_CCL.1.10C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_CCL.1-12 を変更; 前後関係を理解するため、ワークユニット全体が複写され、変更箇所がハイライトされている。)

APE_CCL.1-12 評価者は、PP の適合ステートメントによる定義に従って、適合が主張されている PP のすべてのセキュリティ要件と PP が一貫していることを決定するために、その PP を*検査しなければならない*。

139 PP が他の PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

140 適合が主張されている PP によって完全適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は、適合が主張されている PP 内のセキュリティ要件のステートメントが、以下を許容項目として、評価される PP 内のセキュリティ要件のステートメントに 1)完全に含まれ、及び 2)SFR コンポーネントレベルで(階層的に高いコンポーネントや低いコンポーネントは許可されない等)これと同一であるかどうかを決定する:

– PP 内の SFR は評価される PP において繰り返されることも、詳細化されることもできる。

– 適合が主張されている PP においてオプションとして識別される SFR は、評価される PP に含まれることも、含まれないこともある。

– 適合が主張されている PP において、特定の選択に対する選択ベースとして定義されるすべての SFR は、それを含む基準となる選択が、評価される PP に存在する場合、含まれなければならない。

141 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は、評価中の PP 内のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントのスーパーセットであるか、またはその PP 内のセキュリティ要件のステートメントと同一であるかを決定する(正確適合の場合)。

142 適合が主張されている PP によって論証適合が要求されている場合、評価中の PP のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

143 次を参照のこと:

– SFR: 適合を主張する PP 内の適合根拠は、適合を主張する PP 内の SFR によって定義された要件の全体的なセットが、適合が主張される PP 内の SFR によって定義された要件の全体的なセットと同等(またはより制限的)であると実証しなければならない。これは、適合を主張する PP 内のすべての SFR のセットによって定義された要件を満たすすべての TOE が、適合が主張されている PP 内のすべての SFR のセットによって定義された要件も満たすことを意味する;

– SAR: 適合を主張する PP は、適合が主張される PP 内のすべての SAR を含まなければならないが、追加の SAR を主張すること、または、SAR をより上位階層の SAR で置き換えることができる。適合を主張する PP 内の操作の完了は、適合が主張されている PP 内の操作の完了と一貫していなければならない; 適合が主張されている PP 内と同じ完了が適合を主

張する PP 内でも使われるか、SAR をより制限的にした完了（詳細化の規則が適用される）かのどちらかである。

4.1.6 *APE_CCL.1.11C* に関連するワークユニットへの変更

([CC-3] に対応する、[CEM]APE_CCL.1.11C のステートメントの変更、及びワークユニット APE_CCL.1-13 への変更; 前後関係を理解するため、テキスト全体が複写され、変更箇所がハイライトされている。)

APE_CCL.1.11C ***適合ステートメントは、PP に対する任意の PP/ST に必要とされる適合を、完全 PP 適合、正確 PP 適合、または論証 PP 適合として記述しなければならない。***

APE_CCL.1-13 評価者は、PP 適合ステートメントが、完全 PP 適合、正確 PP 適合、または論証 PP 適合の主張を述べていることを *チェックしなければならない*。

4.1.7 *APE_CCL.1.12C* 及び関連するワークユニットの追加

([CC-3] に対応する、[CEM]APE_CCL.1.12C のステートメントの追加、及び関連する（新しい）ワークユニットの追加。)

APE_CCL.1.12C ***適合ステートメントは、評価中の PP と組み合わせて完全適合の主張が許可されているパッケージ及びその他の PP のセットを識別しなければならない。***

APE_CCL.1-14 評価者は、適合ステートメントが、評価される PP と組み合わせて、(ST または PP において)完全適合の主張が許可されている PP のセットをリストすることを決定するために、その適合ステートメントを *チェックしなければならない*。

144 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

145 PP が他の PP と組み合わせてそれへの完全適合の主張を許可されない場合、PP のリストは必要なく、このワークユニットは満たされているものとみなされる。

146 リストが存在することを決定する以外に、評価者がすべきアクションはない。

APE_CCL.1-15 評価者は、適合ステートメントが、評価される PP に対して(ST または PP において)完全適合を主張される際、その評価される PP と組み合わせて許可されるパッケージのセットをリストすることを決定するために、その適合ステートメントを *チェックしなければならない*。

147 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

148 PP がパッケージと組み合わせてそれへの完全適合を主張することを許可しない場合、パッケージのリストは必要なく、このワークユニットは満たされているものとみなされる。

149 リストが存在することを決定する以外に、評価者がすべきアクションはない。

4.1.8 *APE_CCL.1.13C* 及び関連するワークユニットの追加

([CC-3]に対応する、[CEM]APE_CCL.1.13C のステートメントの追加、及び関連する(新しい)ワークユニットの追加。)

APE_CCL.1.13C ***適合ステートメントは、評価中の PP を基本 PP として特定することが許可される PP モジュールのセットを識別しなければならない。***

APE_CCL.1-16 評価者は、適合ステートメントが、PP 構成において PP を基本 PP として使用することを許可される PP モジュールのセットをリストすることを決定するために、その適合ステートメントを*チェックしなければならない*。

150 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

151 PP が PP 構成において PP モジュールを基本 PP として使用することが許可されない場合、評価者は PP モジュールがリストされていないことを確認する。

152 リストが存在することを決定する以外に、評価者がすべきアクションはない。

APE_CCL.1-17 評価者は、PP を基本 PP としてリストする各 PP モジュールに対して、同じ基本セット内でその PP モジュールによってリストされるすべての他の PP が、評価される PP と共に使用することが許可されるものとしてリストされることを決定するために、適合ステートメント*をチェックしなければならない*。

153 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

154 PP が PP 構成において PP モジュールを基本 PP として使用することを許可しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

155 評価者は、対象の PP の適合ステートメントにおいて識別された各 PP モジュールに対して特定される基本 PP のリストを検査する。PP モジュールには、複数の基本 PP のセットが存在し得るが、評価者が検査しなければならないセットは、評価される PP を含むセットのみである。評価者は、そのセットにリストされるすべての他の PP に対して、評価される PP の適合ステートメントに、対象の PP と共に使用することが許可されるものとしてそれらの他の PP がリストされることを決定する。

156 例えば、PP A が評価されるとする。PP A はその適合ステートメントにおいて完全適合を特定する。PP A はまた、PP 構成において PP モジュール X 及び PP モジュール Y と共に使用できることも特定している。PP モジュール X は基本 PP のセット(PP A、PP B、PP C)を 1 つのみ特定する。一方で、PP モジュール Y は基本 PP のセットを 3 つ特定する(セット 1 は PP A と PP B、セット 2 は PP C と PPQ、セット 3 は PP A と PP D)。

157 このワークユニットでは、評価者は以下を決定する:

158 1) PP モジュール X と PP モジュール Y が、PP A の適合ステートメントにおいて「許可された」PP モジュールとしてリストされていること。

159 2) PP モジュール X については、PP A は適合ステートメントにおいて、PP A と共に使用することが許可されるものとして PP B 及び PP C をリストする必要がある。

160 3) PP モジュール Y については、PP A は適合ステートメントにおいて、基本セット 1 の PP A と共に使用することが許可されるものとして PP B をリストする必要がある。

161 4) PP モジュール Y については、基本セット 2 には PP A が含まれないため、評価者は基本セット 2 を無視する。

162 5) PP モジュール Y については、PP A は適合ステートメントにおいて、基本セット 3 の PP A と共に使用することが許可されるものとして PP D をリストする必要がある。

4.1.9 *APE_CCL.1.14C* 及び関連するワークユニットの追加

([CC-3]に対応する、[CEM]APE_CCL.1.14C のステートメントの追加、及び関連する(新しい)ワークユニットの追加。)

APE_CCL.1.14C ***適合ステートメントは、評価中の PP に対する完全適合を主張できるその他の PP のセットを識別しなければならない。***

APE_CCL.1-18 評価者は、適合ステートメントが、評価中の PP と共に完全適合を主張することを許可される PP のセットをリストすることを決定するために、その適合ステートメントを *チェックしなければならない。*

163 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

164 他の PP がその PP へ完全適合を主張することを PP が許可しない場合、リストは空となるため、このワークユニットは満たされているものとみなされる。

165 リストが存在することを決定する以外に、評価者がすべきアクションはない。

166

4.2 *APE_REQ* に関連するワークユニットへの変更

4.2.1 *APE_REQ.1.2C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_REQ.1-3 への変更; 前後関係を理解するため、ワークユニット全体が複写され、変更箇所がハイライトされている。)

APE_REQ.1-3 評価者は、SFR 及び SAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語が定義されていることを決定するために、PP を *検査しなければならない。*

167 評価者は、PP が以下のすべてを定義することを決定する:

- SFR で使用されるサブジェクトとオブジェクト(の種別);
- サブジェクト、利用者、オブジェクト、情報、セッション、及び/または資源のセキュリティ属性(の種別)、これらの属性が取りうる値、及びこれらの値間の関係(例えば、トップシークレット(top_secret)の値は秘密(secret)の値より「高い」);
- SFR で使用される操作(の種別)及びこれらの操作の影響;
- SFR 内の外部エンティティ(の種別);
- *オプションの* SFR として扱われるべき SFR;つまり、この PP への適合を主張する PP または ST に含めるか含めないかは、PP/ST 作成者の裁量となる SFR。
- 操作を完了することにより SFR 及び/または SAR に導入された他の用語のうち、直ちに理解されないか、またはそれぞれの辞書の定義の範囲外で使用されている用語。

168 このワークユニットの目的は、SFR と SAR が明確に定義されており、曖昧な用語の導入によって誤解が発生しないことを保証することである。このワークユニットは、PP 作成者に強制的に各単語を定義させるなどの極端な方法として、解釈されるべきではない。セキュリティ要件のセットの一般的な読者は、IT、セキュリティ、及びコモンクライテリアに関する適度な知識を持っているものと想定されるべきである。

169 上記のすべては、グループ、クラス、役割、種別によって提示したり、理解しやすくなるようなその他のグループ化または特性化によって提示したりすることができる。

170 評価者は、これらのリストと定義をセキュリティ要件のステートメントの一部にする必要はなく、別の節に(一部または全体が)配置される可能性があることに留意する。これは、特に、同じ用語が PP の残りの部分で使用される場合に該当する。

4.2.2 *APE_REQ.1.3C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_REQ.1-4 への変更; 前後関係を理解するため、ワークユニット全体が複写され、変更箇所がハイライトされている。)

APE_REQ.1-4 評価者は、セキュリティ要件のステートメントがセキュリティ要件のすべての操作を識別することを*チェックしなければならない*。

171 評価者は、すべての操作が、使用される各 SFR または SAR 内で識別されていることを決定する。これには、完了した操作と未完了の操作の両方が含まれる。識別は、活字印刷上の区別、周辺の文章内での明示的な識別、またはその他の特徴的な手段で達成できる。

172 PP が*選択ベースの* SFR を定義する場合、評価者は、SFR 内の選択と、その選択が PP/ST 作成者によってなされた場合に PP/ST に含まれるべき選択ベースの SFR との間の依存性を、PP が明確に識別することを決定する。

4.2.3 *APE_REQ.2.2C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_REQ.2-3 への変更; 前後関係を理解するため、ワークユニット全体が複写され、変更箇所がハイライトされている。)

APE_REQ.2-3 評価者は、SFR 及び SAR で使用されるすべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部のエンティティ及びその他の用語が定義されていることを決定するために、PP を*検査しなければならない*。

173 評価者は、PP が以下のすべてを定義することを決定する:

– SFR で使用されるサブジェクトとオブジェクト(の種別);

– サブジェクト、利用者、オブジェクト、情報、セッション、及び/または資源のセキュリティ属性(の種別)、これらの属性が取りうる値、及びこれらの値間の関係(例えば、トップシークレット(top_secret)の値は秘密(secret)の値より「高い」);

– SFR で使用される操作(の種別)及びこれらの操作の影響;

– SFR 内の外部エンティティ(の種別);

– *オプションの* SFR として扱われるべき SFR;つまり、この PP への適合を主張する PP または ST に含めるか含めないかは、PP/ST 作成者の裁量となる SFR。

– 操作を完了することにより SFR 及び/または SAR に導入された他の用語のうち、直ちに理解されないか、またはそれぞれの辞書の定義の範囲外で使用されている用語。

174 このワークユニットの目的は、SFR と SAR が明確に定義されており、曖昧な用語の導入によって誤解が発生しないことを保証することである。このワークユニットは、PP 作成者に強制的に各単語を定義させるなどの極端な方法として、解釈されるべきではない。セキュリティ要件のセットの一般的な読者は、IT、セキュリティ、及びコモンクライテリアに関する適度な知識を持っているものと想定されるべきである。

175 上記のすべては、グループ、クラス、役割、種別によって提示したり、理解しやすくなるようなその他のグループ化または特性化によって提示したりすることができる。

176 評価者は、これらのリストと定義をセキュリティ要件のステートメントの一部にする必要はなく、別の節に(一部または全体が)配置される可能性があることに留意する。これは、特に、同じ用語が PP の残りの部分で使用される場合に該当する。

4.2.4 *APE_REQ.2.3C* に関連するワークユニットへの変更

([CEM] ワークユニット APE_REQ.2-4 への変更; 前後関係を理解するため、ワークユニット全体が複写され、変更箇所がハイライトされている。)

APE_REQ.2-4 評価者は、セキュリティ要件のステートメントがセキュリティ要件のすべての操作を識別することを*チェックしなければならない*。

177 評価者は、すべての操作が、使用される各 SFR または SAR 内で識別されていることを決定する。これには、完了した操作と未完了の操作の両方が含まれる。識別は、活字印刷上の区別、周辺の文章内での明示的な識別、またはその他の特徴的な手段で達成できる。

178 PP が*選択ベースの* SFR を定義する場合、評価者は、SFR 内の選択と、その選択が PP/ST 作成者によってなされた場合に PP/ST に含まれるべき選択ベースの SFR との間の依存性を、PP が明確に識別することを決定する。

4.3 *ACE_CCL* に関連するワークユニットへの変更

4.3.1 *ACE_CCL.1.5C* 及び関連するワークユニットの追加

([CC-3]に対応する、[CEM]APE_CCL.1.5C のステートメントの追加、及び関連する(新しい)ワークユニットの追加。)

ACE_CCL.1.5C ***適合ステートメントは、評価中のモジュールと組み合わせて、PP 構成において使用できる、その他の PP モジュールを識別しなければならない。***

ACE_CCL.1-5 評価者は、適合ステートメントが、PP モジュールを含む PP 構成の*コンポーネントステートメント*において特定できる PP モジュールのセットをリストすることを決定するために、その適合ステートメントを*チェックしなければならない*。

179 基本 PP がその適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

180 PP モジュールが(PP 構成において)他の PP モジュールと共に使用することが許可されない場合、PP モジュールの適合ステートメントで識別されたその他の PP モジュールはなく、評価者は、PP 構成が、PP 構成のコンポーネントステートメントにおける他の PP モジュールを含まないことを保証する。

181 PP 構成のコンポーネントステートメントが他の PP モジュールを含まない場合、評価者は、コンポーネントステートメントにリストされるすべての PP モジュールが PP モジュールの適合ステートメントに含まれることを保証する。

4.4 *ACE_CCO* に関連するワークユニットへの変更

4.4.1 *ACE_CCO.1.3C* 及び関連するワークユニットへの変更

([CC-3]に対応する、[CEM]APE_CCL.1.3C のステートメントへの変更; ワークユニット ACE_CCO.1-3 への変更; (新しい)ワークユニット ACE_CCO.1-3a の追加 (R5 の行番号を維持するため)。前後関係を理解するため、テキスト全体が複写され、変更箇所がハイライトされている。)

ACE_CCO.1.3C ***適合ステートメントは、PP 構成の適合に対して要求される適合が、完全適合、正確適合、論証適合のいずれかを特定しなければならない。適合主張は、PP 構成とその下層の基本 PP 及び PP モジュールが適合を主張する CC のバージョンを識別する CC 適合主張を含めなければならない。***

ACE_CCO.1-3 評価者は、PP 構成適合ステートメントが、要求される適合の種別(完全適合、正確適合、または論証適合)を特定することを決定するために、その適合ステートメントを*検査しなければならない*。

182 評価者は、PP 構成とその下層の基本 PP 及び PP モジュールが適合を主張する CC のバージョンを識別する CC 適合主張が適合主張に含まれていることを*チェックしなければならない*。

183 評価者は、PP 構成とその下層の基本 PP 及び PP モジュールに関連するすべての CC のバージョンの間に互換性があることを決定するために、PP 構成適合主張を*検査しなければならない*。

184 PP 構成コンポーネントステートメントで識別されるプロテクションプロファイルの少なくとも 1 つが完全適合を要求する場合、PP 構成適合主張も完全適合を要求しなければならない。PP 構成コンポーネントステートメントで識別される PP で完全適合を要求する PP がないが、少なくとも 1 つが正確適合を要求する場合、PP 構成適合ステートメントも正確適合を要求しなければならない。

185 PP 構成とその下層の基本 PP 及び PP モジュールで使用される CC のバージョンには互換性があることが必要である。互換性が明確でない場合は、認証スキームがガイダンスを提供すべきである。

ACE_CCO.1-3a 評価者は、各基本 PP に対して、コンポーネントステートメントに特定されたすべての PP モジュールが、その基本 PP と共に使用することが許可されるものとしてリストされていることを決定するために、PP 構成コンポーネントステートメントを*検査しなければならない*。

186 PP 構成が、その適合ステートメントにおいて完全適合を要求しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

187 評価者は、PP 構成コンポーネントステートメントにおける各基本 PP を検査する。各 PP に対して、評価者は、PP 構成コンポーネントステートメントにリストされる各 PP モジュールが PP の適合ステートメントにもリストされていることを決定する。

4.5 *ASE_CCL* に関連するワークユニットへの変更

4.5.1 *ASE_CCL.1.5C* に関連するワークユニットへの変更

(ASE_CCL.1.5C に関連する [CEM] ワークユニットを変更。ワークユニット ASE_CCL.1-6 を改変; 変更箇所がハイライトされたテキスト全体が含まれる。ワークユニット ASE_CCL.1-6a 及び ASE_CCL.1-7a を追加。番号後の文字は、[CEM] の既存の番号を変更しないで、本文書によってなされる変更を一意に識別するために使用される。)

ASE_CCL.1-6 評価者は、ST が適合を主張するすべての PP を識別する PP 主張が適合主張に含まれていることを*チェックしなければならない*。

188 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

189 評価者は、参照される PP が曖昧さなく(例えば、タイトル及びバージョン番号、または PP の概説に含まれている識別によって)識別されることを決定する。ST が完全適合、正確適合、または論証適合を主張する PP のみが、適合主張の節で識別されることが許可され、これは、PP または PP 構成への部分適合の主張が許可されないことを意味する。

190 このため、統合ソリューションを必要とする PP への適合は、統合 TOE の ST で主張できる。このような PP への適合は、コンポーネント TOE が統合ソリューションを満たさないため、コンポーネント TOE の評価中は不可能だろう。これは、「統合」PP が統合評価手法の使用(ACO コンポーネントの使用)を許可する場合にのみ可能である。

191 統合 TOE の ST は、統合 ST を構成するコンポーネント TOE の ST を識別する。統合 TOE は、基本的にコンポーネント TOE の ST への適合を主張している。

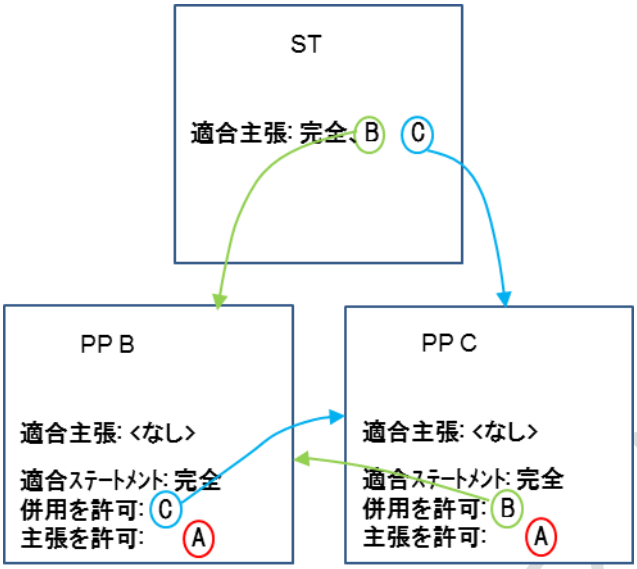
ASE_CCL.1-6a 評価者は、ST が適合を主張する各 PP に対して、適合主張におけるすべての他の PP がその PP と共に主張することが許可されることをその PP の適合ステートメントが許可することを*チェックしなければならない*。

192 ST が PP への適合を主張しない場合、または 1 つの PP に対してのみ適合を主張する場合、このワークユニットは該当しないため、満たされているものとみなされる。

193 ST が PP への完全適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

194 評価者は、適合が主張されている PP の適合ステートメントが、ST の適合主張の節において、その PP と「共に主張するものが許可」されるものとして識別される各 PP をリストすることを決定する。なお、これは、その PP が完全適合を要求し、ST が完全適合を主張する場合にのみ該当する。

195 例えば、ST が評価され、PP B と PP C に適合を主張する場合を想定する。これを図にして以下に示す。ST は完全適合を主張しているため、すべての PP はそれらの適合ステートメントにおいて完全適合を要求する。このワークユニットでは、評価者は、PP B が(その適合ステートメントにおいて)PP B と共に(ST によって)主張されることができる PP として「PP C」をリストすることを決定する。同様に、評価者は、PP C が(その適合ステートメントにおいて)PP C と共に(ST によって)主張されることができる PP として「PP B」をリストすることを決定する。



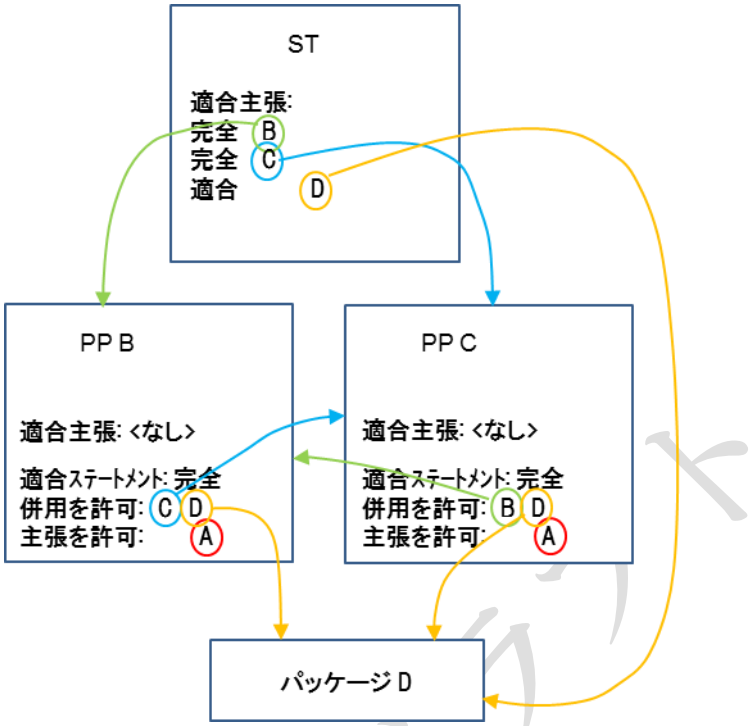
ASE_CCL.1-7a 評価者は、ST が適合を主張する各 PP の適合ステートメントにおいて、ST の適合主張で識別される各パッケージがリストされていることを*チェックしなければならない*。

196 ST がパッケージへの適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

197 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

198 ST が PP への完全適合を主張していない場合、このワークユニットは該当しないため、満たされているものとみなされる。

199 このワークユニットは、評価される ST が、1)1 つ以上の PP に対する完全適合を主張し、2)パッケージへの適合を主張する場合にのみ該当する。これらのケースでは、評価者は、適合が主張されている各 PP において、それらの PP と共に使用することが許可されるものとして(単体または複数の)パッケージがリストされていることを保証する。その例を以下に示す:



200 この例では、ST は PP B 及び PP C に(完全)適合を主張しており、さらにパッケージ D にも適合を主張している(PP B 及び PP C への適合主張は完全適合であるため、パッケージ D への適合主張はパッケージ D 適合でなければならず、パッケージ D 追加は許可されない)。したがって、このワークユニットでは、評価者は、PP B と PP C の両方への適合ステートメントを検査する。これらは、その PP と共に適合主張において使用することが許可されるものとして、パッケージ D をリストしなければならない。

4.5.2 *ASE_CCL.1.8C* に関連するワークユニットへの変更

([CEM] ワークユニット ASE_CCL.1-10 を変更。ワークユニット の長さのため、すべてのワークユニットをここで複写はしない。代わりに、下記のように、ワークユニットの 3 番目の番号付きの段落として、挿入する。(つまり、既存の段落 408 と 409 の間である。))

201 適合が主張されている PP によって完全適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は次の状態であるかどうかを決定する:

a) ST 内の脅威は、適合が主張されている PP 内の脅威と同一である(減らす脅威も、追加の脅威もなし)。完全適合が複数の PP に主張されている場合、ST 内の脅威のセットは、適合が主張されているすべての PP 内の脅威を合わせたものと同一でなければならない。

b) ST 内の OSP は、適合が主張されている PP 内の OSP と同一である(減らす OSP も、追加の OSP もなし)。完全適合が複数の PP に主張されている場合、ST 内の OSP のセットは、適合が主張されているすべての PP 内の OSP を合わせたものと同一でなければならない。

c) ST 内の前提条件は、適合が主張されている PP 内の前提条件と同一である(減らす前提条件も、追加の前提条件もなし)。完全適合が複数の PP

に主張されている場合、次の例外を除き、ST 内の前提条件のセットは、適合が主張されているすべての PP 内の前提条件を合わせたものと同一でなければならない;

– PP からの前提条件（または前提条件の一部）は、この前提条件（または前提条件の一部）に対処する運用環境のセキュリティ対策方針のすべてが、ST が適合を主張している他の PP から受け継いだセキュリティ対策方針と同一の TOE セキュリティ対策方針に置き換えられる場合、省略することができる;

このような状況(1 つの PP の前提条件が、他のいずれかの PP の TOE に関するセキュリティ対策方針によって置き換えられる)において ST を検査する際、評価者は、上記の条件が満たされているかどうかを慎重に決定しなければならない。次の考察で、例を示す:

– ある ST が 2 つの PP に対する完全適合を主張している。前のワークユニットでの決定されたとおり、これらの PP はどちらもその適合ステートメントにおいて完全適合を要求しており、どちらの PP も、ST による適合主張において、その PP と「併用を許可」されるものとしてもう一方の PP をリストしている。ST が適合を主張する 1 つの PP は、運用環境が TOE の外部インタフェースに送信されるデータの不正な改変または傍受を防ぐということを述べる前提条件を含んでいる。これは、TOE が、このインタフェースで、平文で完全性保護なしのデータを受け入れ、攻撃者によるこれらのデータへのアクセスを防ぐセキュアな運用環境に設置されると想定される場合に当てはまる。そして、前提条件は、PP 内で、このインタフェースで交換したデータが、運用環境での適切な手段によって保護されていると述べる運用環境のセキュリティ対策方針にマッピングされる。適合 TOE が TOE の外部インタフェースを経由して送信されるデータを保護しなければならないと特定し、この脅威に対処する適切な脅威及びセキュリティ対策方針を持つ、他の PP があるとする。その場合、ST 作成者は、一方の PP から TOE の外部インタフェースを経由して送信されるデータの保護に関連する前提条件と環境セキュリティ対策方針を、例えば、もう一方の PP からこのインタフェースを経由して転送されたすべてのデータの暗号化と完全性保護のためのセキュアなチャネルを供給することによって、TOE 自身がこれらのデータを保護すると述べるセキュリティ対策方針に置き換えることができる。これにより、もう一方の PP からの、対応する運用環境のセキュリティ対策方針と前提条件は ST から省略される。これはまた、対策方針が運用環境から TOE に再割付されるので、対策方針の再割付と呼ばれる。この TOE は、省略した前提条件を満たす運用環境においてなおもセキュアであり、そのため、PP をやはり満たすという点に注意のこと。さらに、ST 内の脅威と対策方針のセットは、なおも、それが完全適合を主張する PP 内の脅威と対策方針をすべて合わせたものでしかない。

4.5.3 *ASE_CCL.1.9C* に関連するワークユニットへの変更

([CEM] ワークユニット ASE_CCL.1-11 を変更。ワークユニット の長さのため、すべてのワークユニットをここで複写はしない。代わりに、下記のように、ワークユニットの 2 番目の番号付きの段落として、挿入する。(つまり、既存の段落 413 と 414 の間である。))

202 適合が主張されている PP によって完全適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は次の状態であるかどうかを決定する:

– 適合が主張されている PP の TOE のセキュリティ対策方針のすべてが ST に含まれている。完全適合の場合は、評価中の ST は、TOE のセキュリティ対策方針を追加することが許可されない点に注意のこと。複数の PP に適合が主張されている場合、TOE のセキュリティ対策方針のセットは、適合が主張されている PP 内の TOE のセキュリティ対策方針を合わせたものと同一でなければならない。

– ST 内の運用環境のセキュリティ対策方針は、適合が主張されている PP 内の運用環境のセキュリティ対策方針と同一である。複数の PP に適合が主張されている場合、運用環境のセキュリティ対策方針のセットは、以下の例外を除き、適合が主張されている PP 内の運用環境のセキュリティ対策方針を合わせたものと同一でなければならない。

– ある PP からの運用環境のセキュリティ対策方針(またはそのようなセキュリティ対策方針の一部)は、他の PP からの同じ TOE のセキュリティ対策方針(の一部)に置き換えられる;

4.5.4 *ASE_CCL.1.10C*[4] に関連するワークユニットへの変更

([CEM] ワークユニット ASE_CCL.1-12[5] への変更; 前後関係を理解するため、ワークユニット全体が複写され、変更箇所がハイライトされている。)

ASE_CCL.1-12 評価者は、PP の適合ステートメントによる定義に従って、適合が主張されている PP のすべてのセキュリティ要件と ST が一貫していることを決定するために、その ST を*検査しなければならない*。

203 ST が PP への適合を主張しない場合、このワークユニットは該当しないため、満たされているものとみなされる。

204 適合が主張されている PP によって完全適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は、適合が主張されている PP 内のセキュリティ要件のステートメントが、以下を許容項目として、ST 内で完全に再現されることを決定する:

【訳注】[4] 原文では「APE_CCL.1.10C」と記述されている。
【訳注】[5] 原文では「APE_CCL.1-12」と記述されている。

– PP 内の SFR は ST において繰り返されることも、詳細化されることもできる。

– 適合が主張されている PP においてオプションとして識別される SFR は、ST に含まれることも、含まれないこともある。

– 適合が主張されている PP において特定の選択に対する選択ベースとして定義されるすべての SFR は、それを含む基準となる選択が ST に存在する場合にのみ、含まれなければならない。選択が ST 作成者によってなされない場合、その選択に関連する選択ベースの SFR は ST に含まれない。

– PP に存在しない追加のセキュリティ要件（SFR または SAR）が、ST に含まれていない。

– 複数の PP に対する完全適合が主張されている場合、評価者は、いずれの PP にも含まれていない追加のセキュリティ要件が ST に含まれていないこと、及び、それらの PP に含まれているセキュリティ要件のすべてが(上記の項目は許容される)が、ST に含まれていることを決定する。

205 適合が主張されている PP によって正確適合が要求されている場合、適合主張根拠は必要とされない。その代わり、評価者は、ST 内のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントのスーパーセットであるか、またはその PP 内のセキュリティ要件のステートメントと同一であるかを決定する(正確適合の場合)。

206 適合が主張されている PP によって論証適合が要求されている場合、ST のセキュリティ要件のステートメントが、適合が主張されている PP 内のセキュリティ要件のステートメントと同等またはより制限的であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

207 次のとおり:

– SFR: ST 内の適合根拠は、ST 内の SFR によって定義された要件の全体的なセットが、PP 内の SFR によって定義された要件の全体的なセットと同等（またはより制限的）であると実証しなければならない。これは、ST 内のすべての SFR のセットによって定義された要件を満たすすべての TOE が、PP 内のすべての SFR のセットによって定義された要件も満たすことを意味する;

– SAR: ST は、PP 内のすべての SAR を含まなければならないが、追加の SAR を主張すること、または、SAR をより上位階層の SAR で置き換えることができる。ST 内の操作の完了は、PP 内の操作の完了と一貫していなければならない; PP 内と同じ完了が ST 内でも使われるか、SAR をより制限的にした完了（詳細化の規則が適用される）かのどちらかである。

208 統合 TOE の場合、評価者は、統合 TOE のセキュリティ要件がコンポーネント TOE の ST で指定されたセキュリティ要件と一貫しているかどうかを考慮する。これは、論証適合の観点から決定される。特に、評価者は、次の点を決定するために適合根拠を検査する:

a) 依存 TOE の ST 内の運用環境の IT に関連するセキュリティ要件のステートメントは、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントと一貫している。依存 TOE の ST 内の環境のセキュリティ要件のステートメントが、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントのすべての局面を扱うことは期待されない。これは、一部の SFR を統合 TOE の ST 内のセキュリティ要件のステートメントに追加しなければならない場合があるからである。ただし、基本内のセキュリティ要件のステートメントは、依存コンポーネントの動作をサポートするべきである。

b) 依存 TOE の ST 内の運用環境の IT に関連するセキュリティ対策方針のステートメントは、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントと一貫している。依存 TOE の ST 内の環境のセキュリティ対策方針のステートメントが、基本 TOE の ST 内の TOE のセキュリティ要件のステートメントのすべての局面を扱うことは期待されない。

c) 統合 TOE の ST[6] 内のセキュリティ要件のステートメントは、コンポーネント TOE の ST 内のセキュリティ要件のステートメントと一貫している。

209 適合が主張されている PP によって論証適合が要求されている場合、ST のセキュリティ要件のステートメントが、PP 内の、または統合 TOE の ST の場合はコンポーネント TOE の ST 内のセキュリティ要件のステートメントと少なくとも同等であることを適合主張根拠が実証できることを決定するために、評価者はその適合主張根拠を検査する。

【訳注】[6] 原文では「in the composed」と記述されている。