補足-0210

第 2 版

平成 16 年 8 月

独立行政法人情報処理推進機構
セキュリティセンター
情報セキュリティ認証室

はじめに

本書は、「IT セキュリティ評価及び認証制度」で規定の基準及び方法の中の「認証機関が公開する評価基準補足文書」、「認証機関が公開する評価方法補足文書」に相当する文書であり、規格として公開している CC 及び CEM を補足するためのものである。
本補足は、“ CCIMB Interpretations-0407”から 2002 年 2 月以前及びその後に改訂された解釈を翻訳した文書であり、明らかな編集上の誤りを除いては、原文の記載事項に関わる変更は行っていない。

本補足は、“ 補足-0210 第 2 版 ” として識別する。

注：

1. 本書中の CC は、認証機関が公開している”Common Criteria for Information Technology Security Evaluation version 2.1”である。また、CEM は、認証機関が公開している”Common Methodology for Information Technology Security Evaluation Part2 version 1.0”である。
2. 改訂された解釈は、タイトルに“ ｒx ”(x は、改訂履歴を示す)を付記してある。
   また、変更箇所は、左欄外の「変更線」によって識別される。なお、一部翻訳の修正を行った箇所についても「変更線」によって識別している。
3. 本書中の CC で記載してある段落番号については、規格として公開している CC の翻訳文書には段落番号が付与されていない。このため、該当箇所については、CC を参照のこと。また、本翻訳に際し、原文においてタイトル名など一部不整合な個所があったので、本書ではすべて統一した形式にて記述してある。

参考文献：

CCIMB Interpretations (as of 15 February 2002)
CCIMB Interpretations (as of 01 December 2003)

目　次

解釈－003

発効日：2002 年 2 月 11 日

サブジェクト：構成リストに記載されている構成要素の一意の識別

参照文献：CC v2.1 パート 3、ACM_CAP、CEM v1.0、ACM_CAP

問題：
構成リストは、該当するバージョン番号など、すべての構成要素を一意に識別する必要があるのか。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を要求するが、ACM_CAP.2.4C は、構成リスト自体が、該当するバージョン番号などで、各構成要素を一意に識別することを明白に要求していない。

解釈：
ACM_CAP.2 の意図は、開発者がドラフトないしは他の方法のどちらかで、評価証拠として提出されている TOE 構成要素の各バージョンに関する一意のリファレンスを提供することである。構成リストは、評価中の TOE の各構成要素のバージョンを含むことのみを必要としており、従って構成リストでは、構成要素を一意に識別しなければならない。しかしながら、開発者が評価証拠として提出していた構成要素の初期段階のドラフトについては、評価者は CM 証拠資料に記述されている、一意の識別方法と同じ方法で、これらのドラフトもまた一意の識別を所有していることを確認する必要がある。

変更：
CC では、下記の新しい保証エレメントが、ACM_CAP.2.3C、ACM_CAP.3.3C、ACM_CAP.4.3C、及び ACM_CAP.5.3C の後に加えられる。

「構成リストは、TOE を構成するすべての構成要素を一意に識別しなければならない。」

CEM では、

- 新しいエレメントに対応して、新しいアクションが段落 659、938、及びワークユニット ACM_CAP.4-6 の後に挿入される。

- 現行のワークユニット ACM_CAP.2-7、ACM_CAP.3-8、及び ACM_CAP.4-9(並

びにそれらの補助ガイダンステキスト)は、この新しいアクションの下に移される。

・ 現行のワークユニット ACM_CAP.2-7、ACM_CAP.3-8、及び ACM_CAP.4-9 のテキストは、下記と置き換えられる。

「評価者は、CM 証拠資料と一致する程度まで構成要素が識別されていることを決定するために構成要素を検査しなければならない。」

及びそれに続くガイダンステキスト。

「CM システムが、すべての構成要素を一意に識別するという保証は、構成要素の識別を検査することによって得られる。TOE を構成する構成要素、及び開発者が評価証拠として提出する構成要素に関するドラフトの両方については、評価者は、各構成要素が CM 証拠資料に記述されている一意の識別方法と一致するやり方で、一意の識別を持っていることを確認する。

解釈－004

発効日：2001 年 11 月 12 日

サブジェクト：不明確な ACM_SCP.*.1C 要件

参照文献：CC v2.1 パート 3 ACM_SCP.*.1C; CEM v1.0 ACM_SCP.2

問題：
ACM_SCP.*.1C は、「設計証拠資料」が CM システムによって追跡されることを要求する。この用語は、他の場所では用いられず、明らかに直接には ADV 要件に対応しない（なぜなら、この用語は実装表現を除外するように思われるからである）。

解釈：
ACM_SCP は、追加の CM 能力（すなわち、「追跡」への要件）を課すのではなく、追加要素まで ACM_CAP の要件を拡張することを意図しているものと解釈されている。

ACM_SCP.1.1C は、以下が構成要素に含まれていなければならないことを要求する：
実装表現、及び ST の保証コンポーネントによって要求される評価証拠。

変更：
CC パート 3 では、下記の変更がなされる。

- 下記が段落 257 の後に挿入される（ACM_CAP に対する最後の部分の適用上の注釈）

  ACM_CAP は、構成要素リストで識別されているすべての要素に対して課される CM 要件を識別する。TOE 自体を除いて、ACM_CAP は、構成要素リストの内容を開発者の裁量に任せている。（ACM_SCP は、構成要素リストに含めなければならない特定の要素を識別するために用いることができ、それ故に CM によってカバーされる。）

- 段落 274 及び 275（ACM_SCP の目的）は、下記と置き換えられる。

  このファミリの目的は、構成要素として含めなければならない要素を要求することになり、それ故に ACM_CAP の CM 要件下に置かれる。これらの追加要素に

対して構成管理を適用すれば、TOE の完全性が維持されるという追加の保証を提供する。

・ 段落 276（ACM_SCP に関するコンポーネントのレベル付け）は、下記と置き換えられる。

このファミリのコンポーネントは、以下のどれが構成要素として、含まれることを要求されるかに基づいて、レベル付けされている。
実装表現；ST の保証コンポーネントによって要求される評価証拠；セキュリティ欠陥；及び開発ツールと関連情報。

・ 段落 277 の直前に、下記が ACM_SCP に対する適用上の注釈の新しい最初の段落として挿入される。

ACM_ CAP は、構成要素のリスト及びこのリスト上の各要素が CM 下に置かれることを要求するが、ACM_CAP は TOE 自体を除いては、構成要素リストの内容については開発者の裁量に任せる。ACM_SCP は、構成要素リストに含まれなければならない要素を識別し、それによって ACM_CAP の CM 要件の範囲に含めることで、この裁量を狭めている。

・ 段落 277、279 及び 280（ACM_SCP に対する適用上の注釈）は、下記のように変更される。

「CM システムによって追跡される」は、「構成要素のリストに含まれる」に置き換えられる。

・ 段落 278（ACM_SCP に対する 2 番目の適用上の注釈）は、下記と置き換えられる。

ACM_SCP.1.1C もまた、ST の他の保証コンポーネントが要求する評価証拠を、構成要素のリストに含めるべきであるということを要求する。

・ 段落 281、282 及び 284（ACM_SCP.1、ACM_SCP.2、及び ACM_SCP.3 の第 1 の目的）は、それぞれ下記と置き換えられる。

CM システムは、CM 下に置かれていた要素に対してのみ変更を管理することが

できる（すなわち構成要素リストで識別されている構成要素）。TOE 実装及び ST の他の保証コンポーネントが要求する評価証拠を 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。

- 段落 283 及び 285（ACM_SCP.2 及び ACM_SCP.3 の第 2 の目的）は下記のように変更される。

  「CM 下でセキュリティ欠陥を追跡する能力は、・・・を保証する」は、「CM 下にセキュリティ欠陥を置くことは、・・・を保証する」に置き換えられる。

- ACM_SCP.*.1D は次のように変更される。

  ACM_SCP.*.1D　**開発者は、TOE に対する構成要素のリストを提供しなければならない。**

- ACM_SCP.*.1C は、次のように変更される。

  ACM_SCP.1.1C　**構成要素のリストは、以下を含まなければならない。実装表現、及び ST の保証コンポーネントによって要求される評価証拠。**

  ACM_SCP.2.1C　構成要素のリストは、以下を含まなければならない。実装表現；**セキュリティ欠陥；**及び ST の保証コンポーネントによって要求される評価証拠。

  ACM_SCP.3.1C　構成要素のリストは、以下を含まなければならない。実装表現；セキュリティ欠陥；**開発ツールと関連情報；及び** ST の保証コンポーネントによって要求される評価証拠。

- ACM_SCP.*.2C は、削除される。

CEM では、下記の変更がなされる。

- 段落 953 及び 1327（ACM_SCP.1 及び ACM_SCP.2 サブアクティビティそれぞれへの入力）は、それぞれ、下記のように変更される。

  「構成管理証拠資料」は、「構成要素リスト」に変更される。

・　ワークユニット 3:ACM_SCP.1-1 及び 4:ACM_SCP.2-1 は、それぞれ次のように置き換えられる。

評価者は、構成要素リストが CC によって要求される一連の要素を含むことを**チェックしなければならない。**

・　段落 955（ワークユニット 3:ACM_SCP.1-1 のガイダンス）は次のように置き換えられる。

リストは下記のものを含む。

a)　TOE 実装表現（すなわち TOE を構成するコンポーネントまたはサブシステム）。ソフトウェアのみの TOE では、実装表現は、ソースコードだけで構成することができる。ハードウェアプラットフォームが含まれる TOE では、実装表現は、ソフトウェア、ファームウェア、及びハードウェア記述の組み合わせを意味することができる。

b)　ST の保証コンポーネントによって要求される評価証拠。

・　段落 1329（ワークユニット 4:ACM_SCP.2-1 のガイダンス）は下記に置き換えられる。

リストは下記のものを含む。

a)　TOE 実装表現（すなわち TOE を構成するコンポーネントまたはサブシステム）ソフトウェアのみの TOE では、実装表現は、ソースコードだけで構成することができる。ハードウェアのプラットフォームが含まれる TOE では、実装表現は、ソフトウェア、ファームウェア、及びハードウェア記述の組み合わせを意味することができる。

b)　ST の保証コンポーネントによって要求される評価証拠。

c)　実装に関連する報告されたセキュリティ欠陥の詳細を記録するのに用いられる証拠資料（例えば、開発者の問題データベースから得られる問題状況報告）

- ワークユニット 3:ACM_SCP.1-2 及び 4:ACM_SCP.2-2、並びにそれらに関連するガイダンスは、削除される。

根拠：
ACM_CAP は、既にすべての構成要素に、すべての CM 要件を適用するものとして記載されている。従って ACM_SCP が行う必要があるのは、TOE 自体（構成要素に対する ACM_CAP 要件）に加えて、どのような追加要素を構成要素のリストに含まなければならないかを示すことのみである。

ACM_SCP は、追加の CM 能力（すなわち「追跡」への要件）を課すのではなく、追加要素に対する ACM_CAP の要件を展開することを意図しているものと解釈される。構成要素の管理は、ACM_CAP.*.9C によって完全にカバーされている(ACM_CAP.3 及びそれ以上に現れる)。

解釈－006

発効日：2000 年 10 月 15 日

サブジェクト：仮想マシン記述

参照文献：CC v2.0　パート 3　ADV_HLD.*.5C

問題：
ADV_HLD.*.5C における下層のハードウェア、ファームウェア、及びソフトウェアへの参照は、不明確である。このエレメントによって要求される情報は、TOE 内に含まれるメカニズム（コンポーネントの他の個所で扱われている）よりも、（もしあれば）むしろ TOE が動作する仮想マシンに関係するものである。従って、その情報は、IT 環境に関する情報に対する要件と考えることができる。

解釈：
「下層のハードウェア、ファームウェア、及びソフトウェア」という語句は、TOE 内に含まれるメカニズム（コンポーネントの他の個所で扱われている）よりも、（もしあれば）むしろ TOE が動作する仮想マシンに関する ADV_HLD.*.5C によって要求される情報を意味すると解釈されており、従ってその情報は、IT 環境に関する情報に対する要件である。

変更：
CEM：既に CEM パート 2 バージョン 1.0 で対応される。

CC：下記の段落が、ADV_HLD に対する最後の適用上の注釈に続いて追加される(CC v2.1 段落 328)

> ADV_HLD.*.5C における「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」という語句は、TOE 内に含まれるメカニズム（コンポーネントの他の個所で扱われている）よりも、（もしあれば）むしろ TOE が動作する仮想マシンに関係する。従ってその情報は、IT 環境に関する情報に対する要件である。

解釈－008

発効日：2001 年 7 月 31 日

サブジェクト：追加及び適合のオーバーラップ

参照文献：CC v2.1 パート 1　5.4 節、CEM パート 2 v1.0　ASE_INT

問題：
保証パッケージの概念は、パッケージに対する評価要件なしに、「追加」及び「適合」の定義を含めたものである。保証パッケージは、保証パッケージに他の保証コンポーネントを加えても同じように有効である、なぜなら保証パッケージの内容は任意のものだからである。

解釈：
保証パッケージは、「あらかじめ定義されていない」ほど、「任意のもの」ではない。1 つの定義された保証パッケージに追加することは可能であり、その追加された保証要件全体を、新しい保証パッケージとして定義することができる。この問題を明らかにし、潜在的な消費者に、評価の結果をより明確にするために、CC は、下記の変更に詳述されているように、解釈される。

変更：
この解釈に対応するために、CC v2.1、パート 1 には、下記の変更がなされる。

- 下記の文章が CC v2.1 パート 1 の段落 175 の最後に加えられる。

  評価の結果には、「適合結果」も含まれなければならない。

- CC パート 1、5.4 節/項の表題は、「適合結果」に変更される。

- CC パート 1、5.4 節/項は、下記のテキストに置き換えられる。

  適合結果は、評価に合格した TOE または PP によって満たされる要件の集合の源を識別する。この適合結果には、パート 2（機能要件）、パート 3（保証要件）及びもし該当するならば、あらかじめ定義された一連の要件（例えば、EAL、プ

ロテクションプロファイル）に関して示される。

適合結果は、以下のうちの 1 つからなる。

パート 2 適合 ― PP または TOE は、その機能要件がパート 2 の機能コンポーネントのみに基づく場合、パート 2 適合となる。

パート 2 拡張 ― PP または TOE は、その機能要件がパート 2 にない機能コンポーネントを含む場合、パート 2 拡張となる。

これに、下記のうちの 1 つが加えられる。

パート 3 適合 ― PP または TOE は、その保証要件がパート 3 の保証コンポーネントのみに基づく場合、パート 3 適合となる。

パート 3 拡張 ― PP または TOE は、その保証要件がパート 3 にない保証要件を含む場合、パート 3 拡張となる。

さらに、適合結果には、一連の定義された要件に関して作成されたステートメントが含まれるかもしれない。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 TOE は、その要件（機能または保証）が適合結果に記載されているパッケージにあるすべてのコンポーネントを含む場合、あらかじめ定義され、名前を付けられた機能及び/または保証パッケージ（例えば、EAL）に適合している。

***パッケージ名*追加** ― PP または TOE は、その要件（機能または保証）が適合結果に記載されているパッケージにあるすべてのコンポーネントの適切なスーパーセットであるならば、あらかじめ定義され、名前を付けられた機能及び/または保証パッケージ（例えば、EAL）に関する追加となる。

最後に、適合結果には、プロテクションプロファイルに関して作成されたステートメントが含まれるかもしれない。その場合には下記が含まれる。

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

この解釈に対応するために、下記の変更が、CEM パート 2 v1.0 になされる。

- 段落 335 から 340 までは、下記に置き換えられる。

  評価者は、CC 適合主張がパート 3 適合またはパート 3 拡張のいずれかを含でいることを決定する。

  パート 3 拡張が主張され、保証要件パッケージがパート 3 の保証要件を含む場合、評価者は CC 適合主張がパート 3 にあるどの保証要件が主張されているのかを述べているかを決定する。

  パッケージング名適合が主張される場合、評価者は CC 適合主張がどのパッケージが主張されているかを述べているかを決定する。

  パッケージング名追加が主張される場合、評価者は CC 適合主張がどのパッケージングが主張されており、そのパッケージングに対してどの追加が主張されているかを述べているかを決定する。

  PP 適合が主張される場合、評価者は CC 適合が PP または複数の PP 適合がそれに対して主張されているかを述べているかを決定する。

根拠：
この新しい呼称によって、評価の結果は、潜在的な消費者に対してより有意義なものとなる。

例えば、US 農務省は、EAL2 オペレーティングシステムのためのプロテクションプロファイルを作るかもしれない。ヨーロッパ中央銀行は、このプロファイルを採用し、パート 2 からデータ完全性要件を、パート 3 からいくつかの保証要件を加え（すべての存在する EAL3 要件ではないが）、結果として自分自身のプロファイルを発行するかもしれない。カナダ保健省は、この結果のプロファイルを採用し、これにパート 2 から転送中データ保護要件、自分自身の保証要件を追加し、結果としてプロファイルを発行するかもしれない。これらのプロファイルは、以下のディスクリプタと共に、プロテクションプロファイル登録に記載されるだろう。

US 農務省 ― パート 2 適合、及びパート 3 適合

ヨーロッパ中央銀行 — パート 2 適合、パート 3 適合、及び US 農務省プロファイルへの適合
カナダ保健省 — パート 2 適合、パート 3 拡張、及び US 農務省並びにヨーロッパ中央銀行プロファイルへの適合

例を拡張するために、追加のパート 3 コンポーネント Y だけでなく、EAL3 に対して存在するパート 3 要件を加えて、カナダ保健省プロファイルにおける一連の要件に対する製品の成功した評価を想像しなさい。この TOE の評価登録におけるエントリは、以下の評価ディスクリプタを持つであろう。

パート 2 適合
コンポーネント X を用いたパート 3 拡張
コンポーネント Y を用いた EAL3 追加
US 農務省プロファイル、ヨーロッパ中央銀行プロファイル、及びカナダ保健省プロファイルを用いた PP 適合

解釈－009

発効日：2001 年 4 月 13 日

サブジェクト：「対抗する」の定義

参照文献：CC v2.1 パート 3　14 ページ、段落 75

問題：
対抗の定義は不正確である。厳密に言えば、対策方針が脅威に対抗することはできない。つまり、対策方針とは、脅威に対抗するのに必要とされるものについてのステートメントである。

解釈：
対策方針は、単に目標についてのステートメントにすぎない。それは、その存在によって、単独で脅威に対抗するものではない。つまり、脅威が緩和されるのは、対策方針が達成されたときである。

変更：
CC パート 3、段落 75 は以下で置き換えられる。

> **対抗する**(動詞)―この用語は、一般的に、特定の脅威の影響が緩和されるが、必ずしも根絶されないという文脈で使用される。

解釈－013

発効日：2000 年 10 月 15 日

サブジェクト：単一の TOE における複数のドメインに対する複数の SOF 主張

参照文献：CC v2.1 パート 3 AVA_SOF 及び ASE_REQ.1.9C

問題：
CC は、TOE に対して単一の最小 SOF 主張がなされるべきであることを暗に示している。これは、複数のドメインで動作する TOE にとって不適切である。

解釈：
複数のドメインで動作する TOE に対する PP あるいは ST に、各ドメインごとに最小 SOF レベルを定義することが容認される。CC は、以下の変更に詳述されるように解釈される。CEM は、この問題に、段落 236、237、425 及び 426 で対応する。

変更：
新しい段落が、段落 157(APE_REQ)及び段落 178(ASE_REQ)の後に付け加わる。

> CC は所与の TOE 内で、複数の SOF ドメインの有効性を承認する。一つの SOF ドメインは、意図された環境の文脈において、特定の機能強度レベルが適切な TOE のサブセット(論理的または物理的)である。これによって、一つの TOE に対し、ある機能性は、他の機能性よりも高い最小強度要件を持つことが許される。複数の SOF ドメインを持つ TOE に対し、「最小機能強度」という語句は、ドメインによって識別された、各ドメインの最小機能強度を含むセットを示すために用いられる。加えて、要件根拠では、セキュリティ対策方針を満たすことにそのドメインがどのような影響を与えるかを考慮して、各ドメインに対する SOF レベルを考えなければならない。

解釈－016

発効日：2002 年 2 月 11 日

サブジェクト：ADO_DEL の目的

参照文献：CC v2.1:パート 3 ADO_DEL；CEM v1.0 ADO_DEL

問題：
ADO_DEL における CC の目的のステートメントは、TOE の完全性の保護だけを指しているにもかかわらず、コンポーネントでは、もっと一般的なセキュリティという用語を用いている。ある種の TOE にとっては、配付に対して機密性及び可用性が問題になるかもしれず、これを特定する現行の保証コンポーネントが存在しないということが論じられてよい。

解釈：
ADO_DEL の目的は、配送中の TOE のセキュリティ(例えば、機密性、完全性、可用性)を維持することである。ADO_DEL.2 及び ADO_DEL.3 で導入される技術的手段は、完全性の問題だけに対応することが要求される。

変更：
CC パート 3 では、以下の変更がなされる。

- ADO_DEL に対する目的のステートメント(CC パート 3、段落 289)は、以下で置き換えられる。

  > 配付要件は、TOE の配送中に TOE のセキュリティが維持されるという保証を提供するのに必要な手段を詳述する、システム管理及び配送設備並びに手続きを要求する。TOE の確実な配送のため、TOE の配送に用いられる手続きは、配付中の TOE のセキュリティに関係して PP/ST で識別された脅威に対応する。

- CC パート 3 段落 290 の「～への修正を検出、及び防止する」という語は、「～のセキュリティを維持する」に置き換えられる。

- 以下は、CC パート 3 段落 290 の後に、適用上の注釈として含められる。

これらの手続きは、次のような問題を考慮することができよう。

- 消費者が受け取った TOE が TOE のマスターコピーと正確に一致することを保証する。
- TOE の現行のバージョンに対するあらゆる改ざんを避ける/検出する。
- 誤ったバージョンの TOE の送付を防止する。
- 消費者に対し、TOE の配送に関する不要な知識を与えない。
- 配付中に TOE が横取りされるのを避ける/検出する。
- TOE の配送が遅らされ、あるいは止められるのを避ける。

手続きは、すべての面(完全性、機密性、可用性)における TOE の保護を考慮するが、ADO_DEL.2 及び ADO_DEL.3 に導入される技術的手段は、完全性の問題だけに対応することが要求される。

CEM において、以下の変更がなされる。

- ADO_DEL.1 に対する目的のステートメント(CEM 段落 664 及び 960)は、以下で置き換えられる。

  このサブアクティビティの目的は、配付証拠資料が、TOE を利用者のサイトに配送するときに TOE のセキュリティを維持するのに用いられるすべての手続きを記述しているかどうかを決定することである。

- ADO_DEL.2 に対する目的のステートメント(CEM 段落 1334)は、以下で置き換えられる。

  このサブアクティビティの目的は、配付証拠資料が、TOE を利用者のサイトに配送するときに、TOE のセキュリティを維持し、かつその修正あるいは置換の検出に用いられるすべての手続きを記述しているかどうかを決定することである。

- CEM 段落 668、964 及び 1338 において、「完全性」という用語は、「TOE のセキュリティ」で置き換えられる。

- CEM 段落 669、965 及び 1339 は、以下で置き換えられる。

配付証拠資料において強調されるのは、おそらく完全性に関連する手段であるが、それは、TOE 配付中の完全性を維持するため、技術的な手段の適用が要求されるためである。しかしながら、ある種の TOE の配付においては、機密性及び可用性が関心事項となるだろう。従ってセキュアな配付のこれらの側面に関係する手続きもまた、手続きの中で議論されるべきである。

根拠：

ADO_DEL は、配送中の TOE の完全性維持だけに制約されるべきではない。このコンポーネントは、PP/ST で特定された脅威に従って、TOE を配送するときのセキュリティ維持に必要な手続きを開発者が記述すべきように特定されている。これは、内容・提示エレメント ADO_DEL.*.1 と一致しており、そこでは、ADO_DEL.*.1 は、「・・・を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・・・」と述べている。

解釈－019

発効日：2002 年 2 月 11 日

サブジェクト：保証の繰返し

参照文献:CC v2.1 パート 1、4.4.1.3 節; パート 2、2.1.4 節; パート 3、2.1.4 節、段落 5; CEM v1.0、段落 220-222 及び 410-411

問題：
繰返しは、保証コンポーネントにおいて許されるか(CC パート 3、2.1.4 節(段落 56)を見よ)。CC パート 1、4.4.1.3 節(段落 148)は、それを明確に許可している。

解釈：
繰返しは、保証コンポーネントに対して許可されており、特に、これらのコンポーネント内の保証エレメントに詳細化が施されるような場合はそうである。パート 2 機能コンポーネントに適用されるのと同じ操作がパート 3 保証コンポーネントにも適用される。付記すれば、現時点では、パート 3 保証コンポーネントに明示的な割付あるいは選択操作を含むものはない。しかしながら、このことは、将来、パート 3 保証コンポーネントが割付あるいは選択操作を含むことを妨げるものではない。

変更：
以下の変更が、CC に対してなされる。

- CC パート 2 の 2.1.4 節は、削除される。
- CC パート 3 の段落 56 は、削除される。
- CC パート 1 では、段落 148 は、以下の文で置き換えられる。

  CC 機能及び保証コンポーネントは、CC に定義されているとおりに用いることもでき、あるいは、セキュリティ対策方針を満たすために許可された操作の使用を通して修整することもできる。コンポーネント内のエレメントに詳細化が施されたとき、PP/ST 作成者は、そのような詳細化がなされたことを明確に識別しなければならない。PP/ST 作成者は、また、この要件に依存する他の要件への依存性

の必要性が満たされていることにも注意しなければならない。許可された操作は、以下のセットから選択される。

繰返し：種々の操作で 2 回以上コンポーネントを使用することを許す。
割付：パラメタの特定を許す。
選択：リストから、一つあるいはそれ以上の項目の特定を許す。
詳細化：詳細の追加を許す。

繰返し
同一の要件の異なる側面をカバーすることが必要な場合(例えば、2 種類以上の利用者の識別)、各側面をカバーするために、同一のコンポーネントの繰返し使用が許可される。

繰返しは、要件コンポーネントのレベルに向けたものであるが、常にコンポーネントの各繰返しの全文を反復する必要があるのではない。もし、繰返しを常に行うと、コンポーネント内のエレメントの中には、変更されることなく何回も反復されるものが出てくるだろう。PP または ST では、詳細化、あるいは割付の完了、または選択操作によって、その都度、変更される要件エレメントだけを反復することが許されている。(詳細化された要件の繰返しに関するさらなるガイダンスについては、詳細化を参照)。

割付
コンポーネントの中には、セキュリティ対策方針を満たすために、PP または ST に組み込む値のセットを PP/ST の作成者が特定することを可能にするパラメタを含むエレメントを持つものがある。これらのエレメントは、各パラメタとそのパラメタに割り付け得る値への制約を明確に識別する。

受け入れ得る値をあいまいさなく記述、あるいは列挙できるエレメントのあらゆる側面は、パラメタによって表現することができる。パラメタは、属性であってもよく、あるいは要件を特定の値あるいは値の範囲に狭める規則であってもよい。例えば、セキュリティ対策方針に基づき、コンポーネント内のエレメントは、定められた操作が何度か実行されるべきであることを述べられる。この場合、割付は、そのパラメタで使用されるべき数あるいは数の範囲を規定することになる。

選択
これは、コンポーネント内のエレメントの範囲を狭めるために、リストから一つ

あるいはそれ以上の項目を取り上げる操作である。

詳細化
すべてのコンポーネントについて、PP/ST 作成者は、セキュリティ対策方針を満たすために、追加の詳細を特定することによって、受け入れられる実装のセットを制限することが許可されている。コンポーネント内のエレメントの詳細化は、これらの技術的詳細を付加することからなる。
コンポーネントへの変更が有効な詳細化であると見なされるために、その変更は、以下のすべての条件を満たさねばならない。

- 詳細化された要件を満たす TOE は、PP/ST の文脈で解釈されるように、本来の要件も満たす。
- 詳細化された要件が繰り返される場合、各繰返しは、要件の範囲のサブセットだけに対応することが許される。しかしながら、繰返しをすべて合わせたものを一緒にして、本来の要件の全体の範囲が満たされねばならない
- 詳細化された要件は、本来の要件の範囲を拡張しない。
- 詳細化された要件は、本来の要件の依存性のリストを変更しない。

有効な詳細化の例を示す。

1) 完了した割付の内容を理解しやすくするための、あるいは文法的正確さに対応するための変更など、単なる編集上の変更。

2) PP/ST で使われる際の文脈によるもので、要件の範囲を置き換えることのない変更。例えば、「TOE 利用者」と述べた要件を「TOE telnet 利用者」に変更することは、TOE の利用者が telnet 利用者だけの場合に有効な詳細化となろう。

3) 要件の範囲を拡張せずに、実装に関する許容できるアプローチの情報を提供する変更。有効な詳細化の一例は、要件を「検証する能力を提供する」から「暗号チェックサムを実装することにより、検証する能力を提供する」に変更することである。この変更は、既存の要件の実装に用いられるメカニズムの性質に制限を与えるが、本来の範囲を拡張しない。

CC パート 1 では、段落 199 a)及び a)1)は、以下の文で置き換えられる。

PP のこのパートは、TOE あるいはその環境によって満たされねばならない詳細化された IT セキュリティ要件を定義する。IT セキュリティ要件は、以下のとおりに述べられなければならない。

a) 同一要件の異なる側面をカバーする必要があるとき(例えば、2 種類以上の利用者の識別)、各側面をカバーする同一のパート 2 コンポーネントの反復使用(すなわち、繰返し操作を適用すること)が可能である。**TOE セキュリティ要件**のステートメントは、TOE に対するセキュリティ対策方針を満たすため、TOE 及びその評価の裏づけとなる証拠が満足する必要のある機能及び保証セキュリティ要件を定義しなければならない。TOE セキュリティ要件は以下のとおりに述べられなければならない。

1) **TOE セキュリティ機能要件**のステートメントは、パート 2 の適用可能なところから取り出した機能コンポーネントとして、TOE に対する機能要件を定義すべきである。

AVA_SOF.1 が TOE セキュリティ保証要件(例えば EAL2 及びその上)に含まれる場合、TOE セキュリティ機能要件のステートメントは、確率的または順列的メカニズム(例えばパスワードあるいはハッシュ関数)によって実現される TOE セキュリティ機能の最小強度レベルを含まなければならない。すべてのこのような機能は、この最小レベルを満たさなければならない。レベルは、SOF-基本、SOF-中位、SOF-高位のいずれかでなければならない。レベルの選択は、識別された TOE のセキュリティ対策方針と一致するものでなければならない。オプションとして、TOE についてのあるセキュリティ対策方針を満たすため、選択した機能要件に対して特定の機能強度の尺度を定義することができる。

TOE セキュリティ機能強度評価(AVA_SOF.1)の一環として、個別の TOE セキュリティ機能に対してなされた強度主張、及び全体の最小強度レベルが TOE によって満たされているかどうかが評定される。

CC パート 1 では、段落 215 a)及び a)1)は、以下の文で置き換えられる。

ST のこのパートは、TOE あるいはその環境によって満たされねばならない詳細化され

た IT セキュリティ要件を定義する。IT セキュリティ要件は、以下のとおりに述べられなければならない。

a) 同一要件の異なる側面をカバーする必要があるとき(例えば、2 種類以上の利用者の識別)、各側面をカバーする同一のパート 2 コンポーネントの反復使用(すなわち、繰返し操作を適用すること)が可能である。**TOE セキュリティ要件**のステートメントは、TOE に対するセキュリティ対策方針を満たすため、TOE 及びその評価の裏づけとなる証拠が満足する必要のある機能及び保証セキュリティ要件を定義しなければならない。TOE セキュリティ要件は以下のとおりに述べられなければならない。

1) **TOE セキュリティ機能要件**のステートメントは、パート 2 の適用可能なところから取り出した機能コンポーネントとして、TOE に対する機能要件を定義すべきである。

AVA_SOF.1 が TOE セキュリティ保証要件(例えば EAL2 及びその上)に含まれる場合、TOE セキュリティ機能要件のステートメントは、確率的または順列的メカニズム(例えばパスワードあるいはハッシュ関数)によって実現される TOE セキュリティ機能の最小強度レベルを含まなければならない。すべてのこのような機能は、この最小レベルを満たさなければならない。レベルは、SOF-基本、SOF-中位、SOF-高位のいずれかでなければならない。レベルの選択は、識別された TOE のセキュリティ対策方針と一致するものでなければならない。オプションとして、TOE についてのあるセキュリティ対策方針を満たすため、選択した機能要件に対して特定の機能強度の尺度を定義することができる。

TOE セキュリティ機能強度評価(AVA_SOF.1)の一環として、個別の TOE セキュリティ機能に対してなされた強度主張、及び全体の最小強度レベルが TOE によって満たされているかどうかが評定される。

以下の変更が CEM に対してなされる。

- 段落 220 の 2 番目の文章は、以下のとおりに言い換えられる。

「すなわち、PP は、割付あるいは選択に対する未完了の操作を含む IT セキュ

リティ要件ステートメントを含むことができる。」

- 段落 221 及び 222 は、以下で置き換えられる。

  「CC パート 2 及びパート 3 コンポーネントに対して許可される操作は、割付、繰返し、選択、及び詳細化である。割付及び選択操作は、コンポーネントにおいて特定的に指示された場所でだけ許可される。繰返し及び詳細化は、すべてのコンポーネントに対して許可される。」

- 段落 410 及び 411 は、以下で置き換えられる。

  CC パート 2 及びパート 3 コンポーネントに対して許可される操作は、割付、繰返し、選択、及び詳細化である。割付及び選択操作は、コンポーネントにおいて特定的に指示された場所でだけ許可される。繰返し及び詳細化は、すべてのコンポーネントに対して許可される。

根拠：
機能及び保証コンポーネントに対して許可される操作の種別間には差がないので、CC パート 1 は、これら許可された操作に対応するのに最も適切な場所であり、CC パート 2 及び CC パート 3 の両方での同一トピックスをカバーすることによって冗長性を避けている。CEM は、方法論においてこのことを明確にするため、同様に更新される。

CC パート 3 の段落 56 は、そこに書かれているように、有効な操作としての繰返し、割付及び選択について一切の言及を除外している。しかしながら、保証コンポーネントの繰返しは許可されており、かつ CC の将来のバージョンは、割付及び/または選択操作を含む一つあるいはそれ以上の保証コンポーネントを含むことが可能である。

解釈－024

発効日：2001 年 2 月 16 日

サブジェクト：商用の「既製品」（COTS）製品について要求される評価証拠

参照文献：CC V2.1 パート 3

問題：
TOE には、セキュリティ機能性を提供する別の開発者の製品が含まれる。その製品が、評価される TOE に含まれるためには、いかなる評価証拠が要求されているのだろうか。問題となっているのは、開発者が、その製品の独占的な情報にアクセスする方法を持っていない場合、開発者がそれらの製品に対する十分な構成管理（ACM）、開発（ADV）及び脆弱性分析（AVA）の証拠を提供することができるかである。

解釈：
保証要件は、TOE 全体（開発者の直接制御下にない製品を含む）に適用され、関連情報は、要求される分析及びテストを行うために、評価者が、入手可能な状態でなければならない。CEM は、下記の変更に詳述されるように、解釈される。

変更：
下記のテキストは、CEM パート 2 の段落 34 の最後に加えられる。

> 保証要件は、TOE 全体に適用されるので、TOE を構成するすべての製品に付随する評価証拠は、評価者が入手できる状態となっていなければならない。このような評価証拠の範囲及び必要とされる内容は、開発者が TOE の一部である各製品に対して持っている管理レベルとは、無関係である。例えば、上位レベル設計が必要とされる場合、ADV_HLD 要件は、TSF の一部であるすべてのサブシステムに適用される。さらに、手続きの導入が要求される保証要件（例えば、ACM_CAP 及び ADO_DEL）もまた、TOE 全体（別の開発者によるいかなる製品をも含む）に適用される。

解釈－025

発効日：2001 年 7 月 31 日

サブジェクト：ハードウェアの記述に要求される詳細レベル

参照文献：CEM v1.0、B.6.2 節及び B.6.3 節

問題：
ベンダーが開発したソフトウェア及び汎用の「PC」ファームウェア/ハードウェアを含む TOE のハードウェア及びファームウェアに関して、どの程度の詳細レベルを提供しなければならないのか。「汎用」識別情報（例えば、Pentium ベースの PC、10-Base-T ネットワークインタフェースカード、SCSI ディスクドライブ）によって、TOE ハードウェアコンポーネントを識別することで、十分なのか。あるいは、その代わりに、評価構成（例えば、Intel P5-233Mhz、Intel Starfire 2-レビジョン 6.2 マザーボード、70ns EDO RAM の 16Mb、3Com 3C509 NICS、Quantum Fireball 4.3 SCSI ディスクドライブ、Adaptec 2940W SCSI アダプタ）の各コンポーネントの正確な仕様を特定することが必要だろうか。

解釈：
TOE のハードウェア及びファームウェア箇所は、TOE のソフトウェア箇所と同程度の詳細レベルで、記述されねばならない。

ASE_INT 及び ETR で要求されているように、TOE を識別する際には、ハードウェアの識別レベルは、主張されているセキュリティ機能及びセキュリティ保証に対してハードウェアの機能が与える影響によって決定される。TOE 識別は、すべてのセキュリティ関連情報を把握するために必要な詳細度でなければならない。

ADV クラスのコンポーネントによって要求される TSF を記述する際には、主張されているセキュリティを提供するハードウェアの機能は、ハードウェアが、それらの機能をどのように提供するかという観点から記述される。

変更：

- 以下の段落は、CEM の B.6.2 節の段落 1817 の後に挿入される。

  この評価構成は、TOE が基礎としている製品の一部として、入手できるかもし

れないが、評価構成に含まれているハードウェアを、評価構成に含まれていないハードウェアと区別するために、十分詳細に識別される。この識別によって、TOEがセキュアに動作するために、どのような製品を購入しなければならないのか、また、どのような構成オプションを用いなければならないのかが利用者にとって明らかになる。

・ 次の段落は、CEM の B.6.3 節の段落 1818 の後に挿入される。

TSF のハードウェア部分は、関連のある開発証拠資料（機能仕様、上位レベル設計、下位レベル設計）及びテスト証拠資料に関する保証要件に見合った詳細レベルで記述される。ハードウェアの識別レベルは、ハードウェアの機能が、主張されているセキュリティ機能及びセキュリティ保証に対して与える影響によって決定される。

根拠：
ハードウェアの識別は、利用者が TOE を識別するために使用される。この識別は、TOEが、その評価構成において動作するために、利用者がどのような製品を購入しなければならないのか、また、どのような構成オプションを用いなければならないのか知るのに十分なものでなければならない。

識別よりさらに詳細なハードウェアに関する記述は、保証に見合う程度で、ハードウェアを分析するために、評価者に提供される。この記述には、関連のある開発証拠資料（機能仕様、上位レベル設計、下位レベル設計）及びテスト証拠資料の分析が含まれている。

詳細の程度は、主張されているセキュリティに依存する。例えば、問題を指摘した記述に引用されている例では、もし、隠れチャネル分析が、評価の一部として行われた場合と同じように、プロセッサのクロック速度は、それが要因でないならば、参照されないであろう。

解釈－027

発効日：2001 年 2 月 16 日

サブジェクト：AGD_ADM における事象及び機能

参考文献：CC v2.1、パート 3　AGD_ADM.1.1C

問題：
AGD_ADM.1.6C では、以下のとおりに述べられる。

管理者ガイダンスは、TSF の制御下にあるエンティティのセキュリティ属性の変更など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.1.1C には、管理者機能を定義しなければならないと規定されている。事象(AGD_ADM.1.6C）は、機能(AGD_ADM.1.1C）と同じだろうか、または、何か異なるものだろうか。

解釈：
セキュリティ関連事象及び管理機能は、同一ではない。CC は、下記の変更に詳述されるように、解釈される。

変更：
下記の適用上の注釈は、AGD_ADM の段落 375 の後に加えられる。

> AGD_ADM.1.6C は、管理者ガイダンスが、すべてのセキュリティ関連事象への適切な管理者の対応を記述することを要求する。多くのセキュリティ関連事象は、管理機能の実施結果であるが、必ずしもこのような場合になるとは限らない（例えば、監査ログが満杯になる、侵入が検出される)。さらに、セキュリティ関連事象は、管理者機能の特定の連鎖の結果として起こるかもしれない。または、逆に、数個のセキュリティ関連事象が、1 つの機能によって、誘発されるかもしれない。

解釈－031 r1

更新日：2002 年 10 月 25 日

サブジェクト：明白な脆弱性

参照文献：CC v2.0、CCv2.1 パート 3、AVA_VLA；CEM、AVA_VLA.1、AVA_VLA.2

問題：
AVA_VLA.1 は、開発者が、明白な脆弱性について、識別し、テストすることを要求し、さらに、評価者が一連の識別された脆弱性の適切性を検証し、すべての明白な脆弱性が処置されたことを保証するために侵入テストを行うことを要求する。CC は、「明白な脆弱性」を定義する。しかしながら、公知の情報は、非常に変動する。従って、新しい脆弱性が、TOE が凍結された時点と、評価者が評価報告書を仕上げた時点との間に現れることが考えられる（かなりありうる）。これにより、2 つの明白な疑問が生じる。

1) 評価のどの時点で、新しい「明白な脆弱性」に対する公知の監視を中止するべきなのか。
2) ベンダーは、ST または TOE が対処しない脆弱性を処置するために、どのような義務を持っているのか。

解釈：
疑問 1 に関して、監視を中止すべき時点は、国内制度の問題であり、従ってコモンクライテリア解釈の範囲外にある。この問題は、相互承認の枠組みで、より直接的に対処されるケースであろう。

疑問 2 に関して、制度によって規定された時間枠（疑問 1 への回答参照）において発見された、明示された要件を満たす TOE の能力、あるいは明示された脅威に対抗する TOE の能力に影響を与えるすべての脆弱性は、直接 TOE によって、または、意図された環境における適切なステートメントを通して、処置されなければならない。その他のすべての脆弱性は、評価の範囲外であり、処置する必要はない。

変更：
CEM において、以下の段落が段落 899、1255、及び 1722 の後に挿入される。

公知の情報は非常に変動する。よって、開発者が脆弱性分析を実施した時点と評価を完了した時点との間に新たな脆弱性が公知として報告されることは起こりうる。公知情報の監視を中止する時点は評価監督機関の問題であり、よってガイダンスや合意が評価監督機関から求められるべきである。

解釈－032

発効日：2000 年 10 月 15 日

サブジェクト：ASE_TSS における機能強度分析

参照文献：CC v2.1; パート 1、附属書 C; パート 3、ASE_TSS

問題：
CC パート 1（段落 217）と、CC パート 3（ASE_TSS.1.10C）との間には、機能強度分析を、ST の中で提供しなければならないかどうかということについて、矛盾があるように思われる。

解釈：
意図されていたのは､ST における TOE セキュリティ機能強度分析への要求ではなかった。CC は、下記の変更に詳述されるように、解釈される。

変更：
以下の修正が、CC パート 1、段落 217 a)3)になされる。

・「これらの機能すべてについて、TOE セキュリティ機能強度分析を行わなければならない。」は、次のように置き換えられる。

> 「これらの機能のそれぞれについて TOE セキュリティ機能強度主張を行わなければならない。」

・次の文章は、削除される。

> 「機能強度に関して提供する証拠は、評価者が独立評定を行ったり、強度主張が適切かつ正確であることを確認したりするのに十分なものでなければならない。」

解釈－033

発効日：2000 年 10 月 15 日

サブジェクト：パート 3 における「チェックする(check)」の使用

参照文献：CC v2.1 AMA_SIA.*.2E

問題：
AMA_SIA.*.2E では、動詞「チェックする」が使用されいている。しかしながら、記述されている評価者アクションでは、「確認する」が適切であることを示している。これは、CC パート 3 では唯一の「チェックする」の使用のため、2.4 での定義を取り除くことができる。

解釈：
「チェックする」は AMA_SIA では間違って用いられており、「チェックする」は CC パート 3 の 2.4 節から取り除かれるべきである。

変更：
AMA_SIA.1.2E 及び AMA_SIA.2.2E における「チェックする」の使用は、「確認する」に置き換え、CC パート 3 の段落 70 は削除される。

解釈－037

発効日：2001 年 2 月 16 日

サブジェクト：製品または TOE に関する ACM とは

参照文献：CC v2.1、パート 3 ACM クラス

問題：
ACM 要件は、TOE が製品全体であるという仮定で、書かれているように思われる。TOE が製品のサブセットであるとき、ACM は製品全体に適用されるのか。

評価のスポンサーが開発者ではないとき、ACM は、（1）スポンサーが TOE を受け取る時点までのみに適用されるのか、あるいは（2）評価の終了まで適用されるのか。

解釈：
ACM 要件は、TOE 及び TOE に関連する情報を含む。TOE がある製品のサブセットである場合、TOE である製品のその部分のみが、ACM 要件に含まれる必要がある。

ACM 要件は、CM が評価の終了までの期間、適切であり、使用されていることを要求する。

変更：
以下の適用上の注釈は、CC パート 3 8.2 節*（CM 能力（ACM_CAP））の目的節、現行の段落 250 の後に加えられる。*(*訳者注：原文では「8.9 節」と書かれているが、「8.2 節」の誤りである。)*

> TOE がある製品のサブセットである場合、ACM 要件は、全体としてその製品に適用されるのではなく、TOE 構成要素のみに適用される。
>
> CM は、設計段階の初期から適用され、将来に渡って継続することが望まれるが、一方 ACM は、CM が評価の終了までの期間、適切であり、使用されていることを要求する。

根拠：
CC 評価は、製品に関するものではなく、TOE に関するものである。TOE が製品のサブセットである場合、TOE 以外の IT に課されている ACM 要件はない。

CM は、初期の設計段階から、すべての次に続く維持アクション（CC パート 3、段落 249）を通じて、TOE の完全性を保証すべきであるが、ACM 要件は、CM が評価時に適切であることのみを規定する。さらに、ACM は評価の終了後、将来に渡ってスポンサーが CM を適用することを要求するものではない。

解釈－038

発効日：2002 年 2 月 11 日

サブジェクト：C&P(表示・提示)エレメントにおける「少なくとも(as a minimum)」[*1]の使用

*(*1 注：CC v2.1 パート 3 翻訳版において、"as a minimum"の訳は、ACM_CAP.5.16C では「最低限」、ACM_SCP.*.1C では「最小限」としている。)*

参照文献：CC v2.1 パート 1、附属書 C.2.7; パート 2、附属書 E.1（FCS_CKM）;
パート 3、APE_DES.1.1C、ASE_DES.1.1C、ACM_CAP.5.16C、ACM_SCP.*.1C、AMA_AMP.1.11C、及び AMA_CAT.1.1C エレメント; CEM v1.0、ACM_SCP

問題：
CC は証拠の内容・提示エレメントにおいて、「少なくとも」という語句を時々使用する。この語句を使用するときには、CC は開発者に追加の情報を提供することを明示的に許可する。この語句が使用されていない場合には、CC は開発者が追加の情報を提供することを許可していないのだろうか。

解釈：
CC は、明示的に要求されているものに対して、追加の情報を提供することを開発者に許可する。従って「少なくとも」という語句は、不必要である。

変更：
以下の修正が、CC v2.1 パート 1 になされる。

- 「少なくとも」という語句は、段落 217 から削除される。[*2]
  *(*2 注：CC v2.1 パート 1 翻訳版には適用しない。)*

以下の変更が、CC v2.1 パート 2 になされる。

- 段落 696 の最初の文章は削除される。その段落は、次のようになる。

TOE は、すべての鍵のライフサイクルに関わる必要はないので、他の段階を含めるかどうかは、実装に用いられる鍵管理戦略に依存する。（例えば、TOE は、暗号鍵の生成と、配付だけを行うかもしれない。）

以下の変更が、CC v2.1 パート 3 になされる。

・ 「少なくとも」[*1]という語句は、CCパート 3 の以下のエレメントから削除される。

APE_DES.1.1C
ASE_DES.1.1C
ACM_CAP.5.16C
ACM_SCP.*.1C
AMA_AMP.1.11C

・ CC パート 3 では、15.3.2 節、 段落 549

「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。」

は、次のように変更される。

「TOE コンポーネント分類は、そのコンポーネントが、TSP 実施または非 TSP 実施のいずれかであるかを示さなければならない。」

・ CC パート 3、AMA_CAT.1.1C

「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。」

は、次のように変更される。

「TOE コンポーネント分類は、そのコンポーネントが、TSP 実施または非 TSP 実施のいずれかであるかを示さなければならない。」

以下の変更が、CEM v1.0 になされる。

・　「少なくとも」という語句は、段落 952 及び 1326 から削除される。

・　段落 955 及び 1329 の最初の各行は、次のように変更される。

「リストには最低限以下のものを含むべきである。」

解釈－043

発効日：2001 年 2 月 16 日

サブジェクト：APE/ASE_OBJ.1 における「明確に記述される」の意味

参照文献：CC v2.1 パート 3　APE_OBJ.1、ASE_OBJ.1

問題：
ASE_OBJ.1.2C 及び ASE_OBJ.1.3C では、［・・・］のセキュリティ対策方針は、明確に記述され、[･･･]されなければならない、と記述されている。これは、ASE_OBJ.1.2E に「理路整然とした」という要件があるので、不必要であると思われる。

解釈：
ASE_OBJ.1.2/3C 及び APE_OBJ.1.2/3C における用語「明確に記述される」の使用は、本質的には、ASE_OBJ.1.2E 及び APE_OBJ.1.2E における「理路整然とした」という要件の重複である。よって、その用語は無視するべきである。

変更：
「明確に記述され、」という語は、APE_OBJ.1.2C、APE_OBJ.1.3C、 ASE_OBJ.1.2C、及び ASE_OBJ.1.3C から、削除される。

根拠：
これは、CC における ASE 及び APE クラスの他の部分で取られた手法と一致する。CC パート 1 B/C.2.5 における「明確に記述される」という要求は、APE/ASE_OBJ.1.2E における「理路整然とした」という要件に相当する。CEM は、「明確に記述される」という用語の使用を全く扱わず、ワークユニットからその用語ははずしている。

解釈－049

発効日：2001 年 2 月 16 日

サブジェクト：環境によって対処される脅威

参照文献：CC v2.1 パート 1 附属書 B/C.2.5、パート 3 APE/ASE_OBJ.1.3C

問題：
CC パート 1 B.2.5 及び C.2.5 では、次のように述べられる。

> 環境のセキュリティ対策方針は、明確に記述する必要があり、また TOE が完全には対抗できない識別された脅威、［・・・］の側面にまでさかのぼれなければならない。

PP/ST において、環境が脅威のみを含み、OSP または前提条件を含まない場合には、環境のセキュリティ対策方針が、それ自体で脅威に対抗することが認められるだろうか。あるいは、**常に** 1 つまたはそれ以上の TOE のセキュリティ対策方針と共に、脅威に対抗するべきなのか。

解釈：
CC パート 1 段落 196 b)及び 212 b)では、次のように述べられている。

> 脅威の記述は、TOE またはその環境において固有の保護が必要な資産に対する*脅威をすべて含めなければならない。
> *(*訳者注：原文は「資産に対する」が欠落しているが、意味不明となるため挿入した。)*

この記述は、環境における対策によって完全に対抗される脅威を含めることを認めると解釈される。CC は、下記の変更で詳細な解釈を行う。

変更：
以下のテキストは、CC パート 1、段落 198 及び 214 の 3 番目の文章の後に挿入される。

> 脅威は 1 つまたはそれ以上の TOE の対策方針、1 つまたはそれ以上の環境の対策方針、またはこれらの組み合わせによって対抗される。

以下のテキストは、CEM の段落 172 及び 355 の後に新しい段落として、挿入される。

> 従って、1 つまたはそれ以上の環境の対策方針は、脅威を完全に対処することができる。極端なケースは、TOE のセキュリティ対策方針がない場合であろう。この場合、PP/ST 構成の有効性はあるとはいえ、そのような TOE については、TOE のセキュリティ機能要件はないので、すべての脅威及び OSP が環境によって対処されるような TOE の有用性に疑問の余地がある。そのような TOE の認証/有効性の確認は、制度の問題である。

根拠：

脅威は、それらがセキュアな TOE 操作に関連する場合には、PP/ST に含まれるべきである。従って、環境の対策方針は、脅威を完全に対処できるであろう。極端なケースは、TOE のセキュリティ対策方針がない場合であろう。この場合、PP/ST 構成の有効性はあるとはいえ、そのような TOE については、TOE のセキュリティ機能要件はないので、すべての脅威及び OSP が環境によって対処されるような TOE の有用性に疑問の余地がある。そのような TOE の認証/有効性の確認は、制度の問題である。

解釈－051 r1

更新日：2002 年 10 月 25 日

サブジェクト：C&P(表示・提示)エレメントなしの「証拠資料」の使用

参照文献：CC v2.1 パート 3、ADO_IGS.1.1C、ADO_IGS.2.2C、AVA_VLA.1.1C、AVA_VLA.2.2C； CEM、AVA_VLA.1、AVA_VLA.2

問題：
どの証拠資料が、内容・提示の要件を満たさなければならないのか、CC が詳説していない例が 2 つある。すなわち、ADO_IGS 及び AVA_VLA である。これらは、開発者アクションエレメントの同じ証拠資料を参照するのだろうか。

解釈：
ADO_IGS 及び AVA_VLA ファミリの内容・提示エレメントは、これらのファミリの開発者アクションエレメントにおいて識別された証拠資料に適用される。

変更：
以下の変更が、CC パート 3 に対してなされる。

ADO_IGS.*.1C は、下記と置き換える。

> **設置、生成、及び立上げ証拠資料は、TOE のセキュアな設置、生成、及び立上げのために必要なステップをすべて記述しなければならない。**

ADO_IGS.2.2C は、下記と置き換える。

> **設置、生成、及び立上げ証拠資料は、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。**

AVA_VLA.*に対する開発者アクションエレメントは、下記と置き換える。

> **AVA_VLA.*.1D　開発者は、脆弱性分析を行わなければならない。**

AVA_VLA.*.2D　開発者は、脆弱性分析の証拠資料を提供しなければならない。

AVA_VLA.1 に関する内容・提示エレメントは、下記と置き換える。

AVA_VLA.1.1C　脆弱性分析証拠資料は、利用者が TSP を侵害し得る明白な方法を探すために行われた TOE 提供物件の分析を記述しなければならない。

AVA_VLA.1.2C　脆弱性分析証拠資料は、明白な脆弱性の処置について記述しなければならない。

AVA_VLA.1.3C　脆弱性分析証拠資料は、すべての識別された脆弱性に対して、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 に関する内容・提示エレメントは、下記と置き換える。

AVA_VLA.2.1C　脆弱性分析証拠資料は、利用者が TSP を侵害し得る**方法**を探すために行われた TOE 提供物件の分析を記述しなければならない。

AVA_VLA.2.2C　脆弱性分析証拠資料は、識別された脆弱性の処置について記述しなければならない。

AVA_VLA.2.3C　脆弱性分析証拠資料は、すべての識別された脆弱性に対して、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.2.4C　脆弱性分析証拠資料は、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 に関する内容・提示エレメントは、下記と置き換える。

AVA_VLA.3.1C 脆弱性分析証拠資料は、利用者が TSP を侵害し得る方法を探すために行われた TOE 提供物件の分析を記述しなければならない。

AVA_VLA.3.2C　脆弱性分析証拠資料は、識別された脆弱性の処置について記述しなけ

ればならない。

AVA_VLA.3.3C　脆弱性分析証拠資料は、すべての識別された脆弱性に対して、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.3.4C　脆弱性分析証拠資料は、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.3.5C　脆弱性分析証拠資料は、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 に関する内容・提示エレメントは下記と置き換える。

AVA_VLA.4.1C　脆弱性分析証拠資料は、利用者が TSP を侵害し得る方法を探すために行われた TOE 提供物件の分析を記述しなければならない。

AVA_VLA.4.2C　脆弱性分析証拠資料は、識別された脆弱性の処置について記述しなければならない。

AVA_VLA.4.3C　脆弱性分析証拠資料は、すべての識別された脆弱性について、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.4.4C　脆弱性分析証拠資料は、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.4.5C　脆弱性分析証拠資料は、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.4.6C　脆弱性分析証拠資料は、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。

以下の変更が CEM になされる。

章見出し 6.9.2.4.1 のすぐ下の AVA_VLA.1.1C への参照は以下と入替わる。

AVA_VLA.1.1C、AVA_VLA.1.2C、及び AVA_VLA.1.3C

章見出し 7.10.3.4.1 のすぐ下の AVA_VLA.1.1C への参照は以下と入れ替わる。

AVA_VLA.1.1C、AVA_VLA.1.2C、及び AVA_VLA.1.3C

章見出し 8.10.3.4.1 のすぐ下の AVA_VLA.2.1C 及び AVA_VLA.2.2C への参照は以下と入れ替わる。

AVA_VLA.2.1C、AVA_VLA.2.2C、AVA_VLA.2.3C、及び AVA_VLA.2.4C

解釈－055

発効日：2000 年 10 月 15 日

サブジェクト：パート 2 附属書において参照されている不正確なコンポーネント、FPT_RCV

参照文献：CC v2.0、v2.1; パート 2、附属書、FPT_RCV

問題：
以下のテキスト「・・・FPT_FLS.1 から ADV_SPM.1 への依存性を論証することができる。」が、FPT_RCV に関する利用者のための注釈において見受けられる。これは FPT_FLS.1.1 に関する利用者のための適用上の注釈に対する、カットアンドペーストの誤りのように思われる。

解釈：
これは、カットアンドペーストの誤りである。テキストでは、FPT_FLS.1 ではなく、FPT_RCV の各コンポーネントを示すべきである。

変更：
CC パート 2 の段落 1236 の最後の文章は、次のように書き換えられる。

> 開発者が、セキュアな状態の明確な定義と、なぜそれがセキュアとみなせるべきかの理由を提供すれば、FPT_RCV における各コンポーネントから ADV_SPM.1 への依存性は、論証し取り除くことがができる。

解釈－058

発効日：2001 年 7 月 31 日

サブジェクト：詳細化をめぐっての混乱

参照文献：CC v2.0、v2.1: パート 1　B.2.6、C.2.6 節

問題：
IT 環境に適用されるものとして識別されている要件に関して、「TSF は・・・しなければならない」を「 IT 環境は・・・しなければならない」に変更することは、詳細化または、要件拡張になるのだろうか。

解釈：
IT 環境に適用されるものとして識別されている要件に関して、「TSF は・・・しなければならない」を「IT 環境は・・・しなければならない」に変更することは、詳細化である。

変更：
CC パート 1、B.2.6 節 段落 199 b)は、下記に変更する。

> **IT 環境に対するセキュリティ要件**の任意選択の記述では、TOE の IT 環境が満たすべき IT セキュリティ要件を識別しなければならない。PP のこの部分における要件は、CC パート 2 及びパート 3 から引き出すことができ、もし、そうならば TOE ではなく、IT 環境が要件を満たさねばならないと明確に指摘するために、言い直すべきである。このような言い直しは、詳細化の特別なケースであり、修正された CC コンポーネントに関連する評定要件に関わるサブジェクトではない。TOE が IT 環境に対して仮定された依存性を持たない場合、PP のこの部分は省略することができる。

CC パート 1、C.2.6 節 段落 215 b)は、下記に変更する。

> **IT 環境に対するセキュリティ要件**の任意選択の記述では、TOE の IT 環境が満たすべき IT セキュリティ要件を識別しなければならない。ST のこの部分における要件は CC パート 2 及びパート 3 から引き出すことができ、もし、そうならば TOE ではなく、IT 環境が要件を満たさねばならないと明確に指摘するために、言い直すべきである。このような言い直しは、詳細化の特別なケースであり、修正された CC コンポーネントに

関連する評定要件に関わるサブジェクトではない。TOE が IT 環境に対して仮定された依存性を持たない場合、ST のこの部分は省略することができる。

CC パート 2、段落 1 は下記に変更する。

この CC パート 2 に定義されているセキュリティ機能コンポーネントは、プロテクションプロファイル（PP）またはセキュリティターゲット（ST）に表されているセキュリティ機能要件に対する基礎である。これらの要件は、評価対象（TOE）または TOE の IT 環境に関して予想される望ましいセキュリティのふるまいを記述し、PP または ST に記述されているセキュリティ対策方針を達成することを目的としている。これらの要件は、利用者が IT との直接の対話（すなわち、入力、出力）により、または IT からの応答により、検出できるセキュリティ特性を記述している。

解釈－062

発効日：2001 年 7 月 31 日

サブジェクト：欠陥報告のソースをめぐっての混乱

参照文献：CC v2.1 パート 3　ALC_FLR

問題：

ALC_FLR.*.2D は、「利用者」からの報告に対して受付及び処理を要求する。利用者コミュニティは、処置すべき欠陥報告の複数の潜在的なソースの 1 つに過ぎない。他のソースの例には、学会、コンピュータ緊急対応チーム、及び知的組織が含まれる。

解釈：

*利用者報告*という用語は、TOE の利用者から直接受け取った報告に制限されない。他のソースから受け取った報告を、単に TOE の利用者ではないという理由で、無視することはできない。

変更：

CC パート 3 v2.1 の段落 391 の 2 番目に新しい文章が挿入される。新しい段落 391 は、下記のとおりである。

> 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。これらの欠陥は、開発者によって、TOE の利用者によって、あるいは TOE について熟知している他の機関によって報告されるかもしれない。ある欠陥は、直ちに修繕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。

加えて、要件 ALC_FLR.2.2D 及び ALC_FLR.3.2D における「利用者報告」という用語の使用は、「すべての報告」に変更される。変更の結果は下記のようになる。

> 開発者は、すべてのセキュリティ欠陥の報告とそれらの欠陥の訂正要求を受け付け、処理する手続きを確立しなければならない。

解釈－064

発効日：2001 年 2 月 16 日

サブジェクト：明示された要件に対する明らかに高すぎる基準

参照文献：CC v2.0、CC v2.1 パート 3、APE/ASE_SRE

問題：

APE/ASE_SRE.1.5C は、系統的に実証することができる評価可能な客観的な要件を要求する。しかしながら、セキュリティ要件のまさしくその性質によって、系統的実証をし得る十分に評価可能で、客観的な要件を作り出すことは必ずしも可能ではない。

解釈：

既存のCC機能要件及び保証要件は、このファミリの要件に準拠するモデルとして用いられる。~~CC及びCEMは下記の変更において詳述するように解釈される。~~

(訳者注：“CCIMB Interpretations-0407"にて削除された。)

変更：

この新しい段落は、CC パート 3 段落 164 に続く APE_SRE ファミリの適用上の注釈に加えられる。

> APE_SRE.1.5C 及び APE_SRE.1.6C エレメントは、明示された IT セキュリティ要件が、明確に、曖昧さなく表現されているばかりでなく、評価可能で、客観的でなければならないことを要求する。既存の CC 機能要件及び保証要件は、これらの要件に準拠するモデルとして用いられる。

この新しい段落は、CC パート 3 段落 185 に続く ASE_SRE ファミリの適用上の注釈に加えられる。

> ASE_SRE.1.5C 及び ASE_SRE.1.6C エレメントは、明示された IT セキュリティ要件が、明確に、曖昧さなく表現されているばかりでなく、評価可能で、客観的でなければならないことを要求する。既存の CC 機能要件及び保証要件は、これらの要件に準拠するモデルとして用いられる。

以下の段落は、これらの CEM ワークユニットに添えられる：APE_SRE.1-5 の段落 281 の

後、APE_SRE.1-6 ワークユニットの後、ASE_SRE.1-5 の段落 470 の後、及び ASE_SRE.1-6 ワークユニットの後。

既存の CC 機能要件及び保証要件は、この要件に準拠するモデルとして用いられる。

解釈－065

発効日：2001 年 7 月 31 日

サブジェクト：セキュリティ機能の管理を要求するコンポーネントがない

参照文献：CC v2.1、パート 2 FMT

問題：
FMT クラスに対する CC の記載事項は、セキュリティ管理機能を行う役割に関する制限を特定する。しかし、その記載事項は、TSF がその制限が適用されるセキュリティ管理機能を提供するという明示的な要件を提供していない。一般的な議論では、機能を制限することは、暗に機能が提供されるべきであることを要求している。

解釈：
新しいファミリは、CC パート 2 の FMT クラスに加えられる。これは、TOE によって提供される管理機能の特定を可能にするものである。

変更：
この解釈に対応するために、以下の変更が、CC パート 2 になされる。
以下のファミリは、8 章 FMT クラスに加えられる。

8.x 管理機能の特定（FMT_SMF）

ファミリのふるまい

このファミリは、TOE が提供する管理機能の特定を可能にする。管理機能は、管理者が TOE のセキュリティに関わる側面を制御するパラメタを定義するための TSFI を提供する。それらは、例えばデータ保護属性、TOE 保護属性、監査属性、及び識別認証属性である。管理機能には、バックアップ及びリカバリーのように、運用者が継続した TOE の運用を保証するために行う機能も含まれる。このファミリは、FMT クラスの他のコンポーネントと共に、動作する。このファミリのコンポーネントは、管理機能を要求し、FMT の他のファミリは、これらの管理機能を使用することを制限する。

コンポーネントのレベル付け

FMT_SMF 管理機能の特定	1

FMT_SMF.1 管理機能の特定は、TSF が特定の管理機能を提供することを要求する。

管理：FMT_SMF.1

このコンポーネントに関して予見される管理アクティビティはない。

監査：FMT_SMF.1

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下の事象を監査対象にすべきである。

a) 最小：管理機能の使用

FMT_SMF.1 管理機能の特定

下位階層： なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：TSF によって提供されるセキュリティ管理機能のリスト]。

依存性： なし

以下の節が、附属書 H、セキュリティ管理に加えられる。

H.x 管理機能の特定（FMT_SMF）

このファミリは、TOE が管理機能を特定することを可能にする。割付を実行する際に、リストされる各セキュリティ管理機能は、セキュリティ属性管理、TSF データ管理、またはセキュリティ機能管理のうちのいずれかである。

FMT_SMF.1 管理機能の特定

このコンポーネントは、提供されるべき管理機能を特定する。

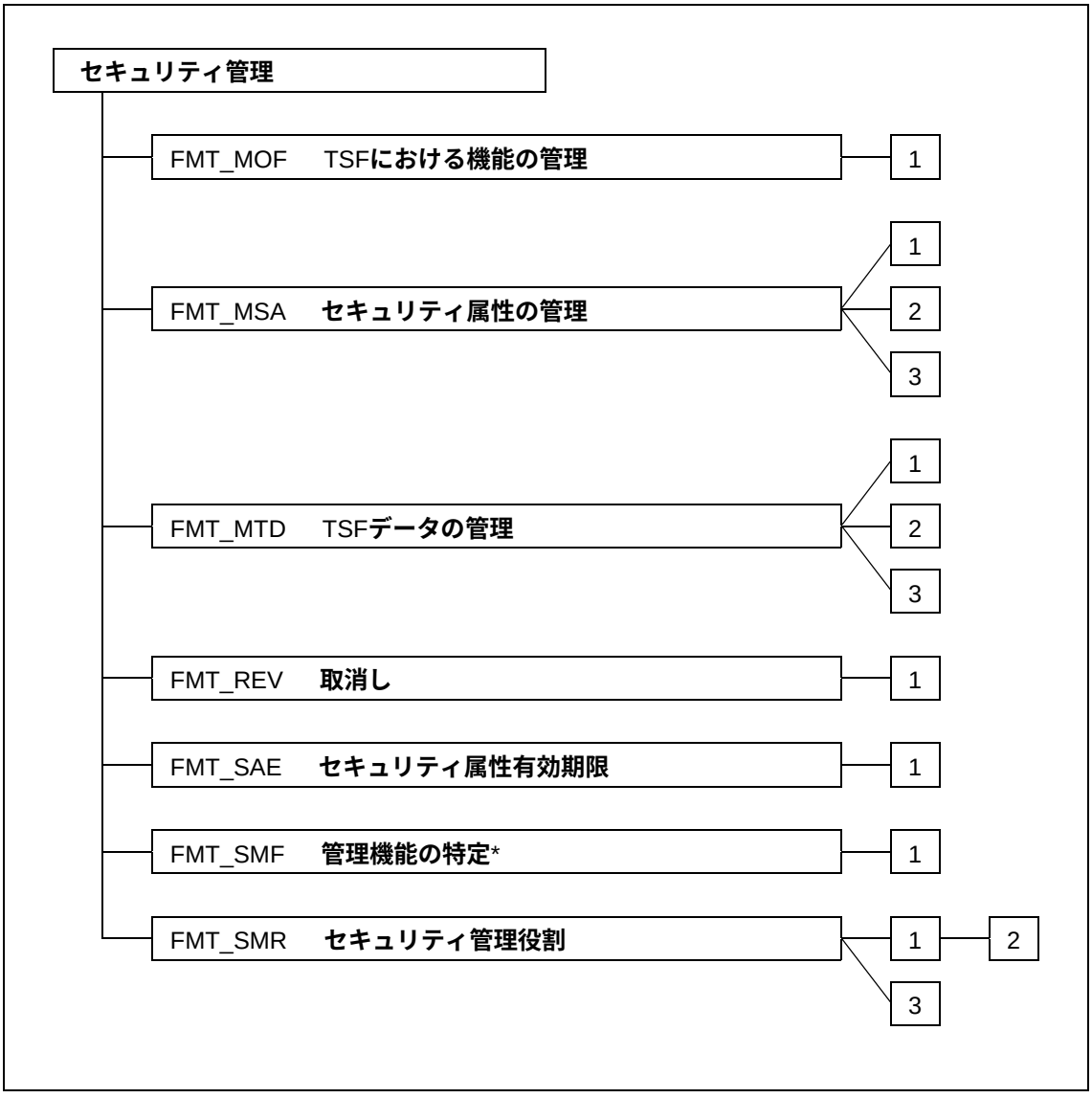
適用上の注釈

PP/ST の作成者は、このコンポーネントによってリストされるべき管理機能の基礎を得るために、PP/ST に含まれるコンポーネントの「管理」の節を調べるべきである。

操作

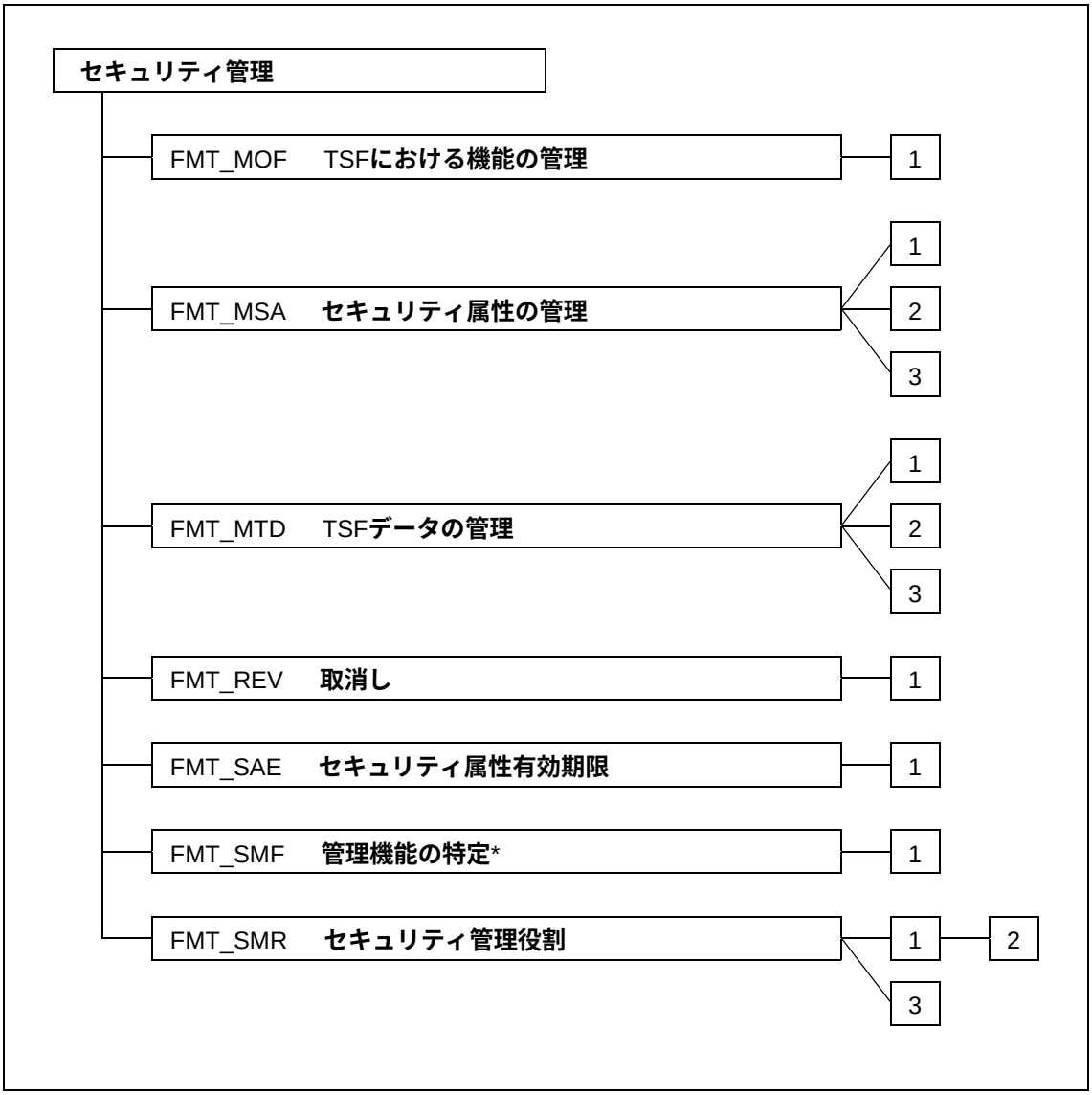
割付：
FMT_SMF.1 では、PP/ST の作成者は、セキュリティ属性管理、TSF データ管理、またはセキュリティ機能管理のいずれかである、TSF により提供される管理機能を特定すべきである。

8 章、図 8.1 は、1 つの階層コンポーネントを持つ追加のファミリーFMT_SMF 管理機能の特定を示すために、修正される。



**訳者注：原文では"Specification of Management"と書かれているが、"Specification of Management Functions"の誤りである。*

H 章、図 H.1 は、1 つの階層コンポーネントをもつ追加のファミリ、FMT_SMF　管理機能の特定を示すために修正されている。



**訳者注：原文では"Specification of Management"と書かれているが、"Specification of Management Functions"の誤りである。*

次の依存性が、FMT_MOF.1 に追加される。FMT_SMF.1 管理機能の特定
次の依存性が、FMT_MSA.1 に追加される。FMT SMF.1 管理機能の特定
次の依存性が、FMT_MTD.1 に追加される。FMT SMF.1 管理機能の特定

解釈－067

発効日：2000 年 10 月 15 日

サブジェクト：ST に欠けている適用上の注釈

参照文献：CC v2.1 附属書 C

問題：
CC パート 1 の附属書 B は、プロテクションプロファイル（PP）に関する適用上の注釈節の存在を示唆する。しかし、CC パート 1 の附属書 C は、セキュリティターゲット（ST）に関する適用上の注釈節の存在を示唆していない。しかしながら、適用上の注釈は、PP と同様に ST にもあるものと思われる。

解釈：
適用上の注釈は、PP の適用上の注釈と類似した様式で、ST のオプション部分となっている。CC は以下の変更に詳細が示されるように解釈される。

変更：
追加の節が、CC パート 1 C.2.8 節の後に加えられる。

適用上の注釈：

ST のこのオプション部分には、ST の理解に関連がある、または有用だと考えられる追加の情報が含まれている。ST が PP の要件に準拠することを主張する場合、PP 適用上の注釈節に含まれているある情報を、ST の他の章に記載することが、適切である場合があることに留意する。例えば、TOE の構造に関する情報は、おそらく分離した適用上の注釈節よりも、TOE 要約仕様または ST 根拠に、より適切に提示される。ST の評価をより容易にするために、この附属書に概説されている ST の提示の構造は規定ではないので、評価に関連する要素を含む適用上の注釈は、その評価の証拠を提供する ST の節の一部として提供することを推奨する。

解釈－069

発効日：2001 年 3 月 30 日

サブジェクト：非形式的なセキュリティ方針モデル

参照文献：CEM、ADV_SPM.1

問題：
ADV_SPM.1 について CEM は、非形式的な TOE セキュリティ方針モデル（ISPM）の評価に対する評価者のアクションを定義する。ST で提示されるものに加えて、この要件を満たすために、さらにどのような追加の資料が必要とされているのか不明確のままである。同様に、ASE が要求するもの以上のどのようなアクションが、ADV_SPM 要件を満たすために必要とされているのか不明確である。

解釈：
ISPM の要件は、セキュリティ方針に関する明確なステートメントによって満たされている。独立した ISPM の必要性は絶対的なものではない。なぜなら、非常に直接的な方針、または ST で非常に明確に表現された方針については、独立した ISPM への必要性はないからである。ASE 及び ADV_SPM によって要求されるアクティビティは、関連があるが、（また、実際には協力して行われているが）、それらは異なったものである。

変更：
CEM では、以下の段落が、段落 1473 の後に加えられる。

> 保証は、TOE セキュリティ機能要件の基礎となっている方針に関する、明示的で一般的なステートメントから得ることができる。得られる保証は、2 つに分かれる。すなわち、実施されているセキュリティ方針の詳細を理解するための簡潔で全体的な補助になるように、各セキュリティ方針の記述を集める。加えて、このような集められた記述によって、相違または不一致（それを、ADV_SPM.*.3C エレメントの一部として探し出さねばならない）を理解するのが容易になる。さらに、その記述は、セキュアな状態についての明確な特性を規定する。（ADV_SPM.*.2C エレメントの一部として探し出さねばならない）。
>
> 非形式的なセキュリティ方針モデル（ISPM）の要件は、セキュリティ方針に関する

明確なステートメントによって満たされている。独立した ISPM の必要性は、絶対的なものではない。なぜなら、非常に直接的な方針、または ST で非常に明確に表現された方針については、独立した ISPM の必要性はないからである。このような場合には、ST の異なる章（例えば、セキュリティ要件、TOE 要約仕様）を、セキュリティ方針の十分なレベルの詳細を提供するために組み合わせることができる。しかしながら、このようなケースは頻繁にはない。例えば、監査要件を TOE セキュリティ機能要件に関するステートメント全体に広げることが可能であるが、それは全体的な方針に関する明確なモデルを提供しないであろう。ST の別の章（おそらく、TOE 要約仕様）が、監査要件を統一的なものにまとめないならば、独立した ISPM を持つことが必要であろう。さもなければ、ST 要件内の矛盾が検出されないままで合格させることになる。

開発者が ST によって満たされるセキュリティ方針のいくつかまたはすべてに対する ISPM 要件を主張する場合、評価者は ADV_SPM.1 コンポーネントの要件を適用することによって、それが事実であることを決定する必要がある。すなわち、その方針が明確に表現されており、モデルが ST の他の部分と一貫することを決定する。ISPM 根拠の一環として、開発者が、その ISPM は、ST によって完全に満たされていると主張する場合、その根拠は、ST の種々の箇所の適合性及び対応の実証を参照すると思われる。このワークユニットを評価するときには、評価者はこの領域の ST 評価の結果を利用してもよい。

CEM では、以下の段落が、段落 1475 の後に加えられる。

開発者が ST によって満たされるセキュリティ方針のいくつかまたはすべてに対する ISPM 要件を主張する場合、評価者は ADV_SPM.1 コンポーネントの要件を適用することによって、それが事実であることを決定する必要がある。すなわち、その方針が明確に表現されており、モデルは ST の残りに関して完全であることを決定する。このワークユニットを評価するときには、評価者は ST の様々な箇所の完全性に関する評価結果を利用してもよい。

根拠：

うまく構成された ST は、自動的に ADV_SPM 要件を満たすものではない。なぜなら、ASE 要件は、ADV_SPM 要件のスーパーセットではないからである（例えば、ST がその方針の規則及び特徴を記述する ASE 要件はない）。

ADV_SPM 要件は、単に TOE セキュリティ方針の記述を要求するにすぎない。もし、こ

のような記述が、ST のような他の提供物件で入手可能ならば、開発者は別の証拠を提供する必要はない。

解釈－074

発効日：2000 年 10 月 15 日

サブジェクト：ATE_COV.2-3 及び ATE_DPT.1-3 について重複した参考テキスト

参照文献：CEM パート 2、v1.0、段落 1122、1130、1581 及び 1589

問題：
EAL3 に関する CEM の章では、ワークユニット ATE_COV.2-3 及び ATE_DPT.1-3 は、同じ語及び情報テキストを持っている。それらは、両方とも、機能仕様及び上位レベル設計に関係するガイダンスを含む CEM 7.9.1.3 節を参照する。これは、ATE_COV.2 及び ATE_DPT.1 の両方が、セキュリティターゲットに含まれることを暗示するが、必ずしもそうであるとは限らない。

これらの保証コンポーネントのうちの 1 つだけが、セキュリティターゲットの中にあるときには、このガイダンスは誤解を招きやすい。さらに、両方のワークユニットは、同じ語及び参考テキストを持っているので、これら 2 つのワークユニットへの作業努力がどのように異なるかについて、評価者の側に混乱を引き起こすだろう。最後に、7.9.1.3 節は、ATE_COV.2（これは完全性要件を持っている）及び ATE_DPT.1（これはその要件を持っていない）間の厳密な相違を扱わない。これらのワークユニットは、両方とも、EAL4 に関する CEM の章で述べられ、CEM 8.9.1.3 節を参照するので、同じ問題が、これらのワークユニットに関係する。

解釈：
対応するワークユニット ATE_COV 及び ATE_DPT を行うための評価者へのガイダンスは類似しているが、実施中の作業を配慮しなければならない。CEM は、下記の変更で詳述されているように解釈される。

変更：
下記の変更が、CEM ｖ1.0 に行われる。

・ CEM 段落 1122 は、次のように言い換えられる。

このワークユニットのガイダンスは、機能仕様に関係しており、次の中に見つけることができる。

a) 適用上の注釈、7.9.1.3 節、テストの適切性の検証

・ CEM 段落 1130 は、次のように言い換えられる。

このワークユニットのガイダンスは、上位レベル設計に関係しており、次の中に見つけることができる。

a) 適用上の注釈、7.9.1.3 節、テストの適切性の検証

・ CEM 段落 1581 は、次のように言い換えられる。

このワークユニットのガイダンスは、機能仕様に関係しており、次の中に見つけることができる。

a) 適用上の注釈、8.9.1.3 節、テストの適切性の検証

・ CEM 段落 1589 は、次のように言い換える。

このワークユニットのガイダンスは上位レベル設計に関係しており、次の中に見つけることができる。

a) 適用上の注釈、8.9.1.3 節、テストの適切性の検証

根拠

CEM 7.9.1.3 及び 8.9.1.3 節が、テストの適切性を検証する枠組みで機能仕様及び上位レベル設計の両方に対応することは、適切である。

CEM の現在の構造は、EAL のラインに沿っているので、7.9.1.3 及び 8.9.1.3 節は、保証要件が、それぞれ EAL3 または EAL4 のすべてを包含する場合、さらに ATE_COV.2 及び ATE_DPT.1 の両方が、これらの EAL にある場合の状況を扱う。CEM 7.9.1.3.及び 8.9.1.3 節が ATE_COV.2 及び ATE_DPT.1 間の厳密な相違を扱う必要はない。ATE_COV.2 における完全性要件は、7.9.1.3 及び 8.9.1.3 節のどちらも、参照しないワークユニット ATE_COV.2-4 によって対応されている。7.9.1.3.及び 8.9.1.3 節の意味の背景を適切に理解しない評価者は、ことによると、ワークユニット ATE_COV.2-3 を行うときに、ワークユニット ATE_DPT.1-3 に対する意図された評価努力のすべてを行おうと試みるかもしれない。

解釈－075

発効日：2000 年 10 月 15 日

サブジェクト：ATE_FUN.1-4 及び ATE_IND.2-1 について重複した参考テキスト

参照文献：CEM パート 2、v1.0、段落 1602－1604 及び 1635－1637

問題：
:ATE_IND.2-1 に関して参考テキストは、:ATE_FUN.1-4 に関して参考テキストのスーパーセットであり、追加されるすべてのものは、テスト資源に関する追加の短い段落である。最近*:ATE_FUN.1-4 を行った評価者は、ATE_IND.2-1 の大部分は、ATE_FUN.1-4 に類似しているために、完了したと考えるであろう。

解釈：
ワークユニット*:ATE_IND.*-1 及び*:ATE_FUN.*-4 に対する補助的な段落には、不必要なテキストの重複が数箇所ある。

変更：
CEM 段落 806、 1144 及び 1603 は、以下のとおりに言い換えられる。

> ST が評価のために 1 つ以上の構成を規定することは、可能である。TOE は、多くの異なったハードウェア及びソフトウェア実装から成り立っており、その実装を ST に従って、テストする必要がある。評価者は、ST で記述されている各評価構成と一致する開発者テスト証拠資料で識別されているテスト構成があることを検証する。

CEM 段落 617、839、1177 及び 1636 は、以下のとおりに言い換えられる。

> ST が評価のために 1 つ以上の構成を規定することは、可能である。TOE は、多くの異なったハードウェア及びソフトウェア実装から成り立っており、その実装を ST に従って、テストする必要がある。評価者の TOE テスト構成は、ST で記述されている各評価構成と一致するべきである。

CEM616 は、以下のとおりに言い換えられる。

評価者テストに使用される TOE は、ACM_CAP.1 サブアクティビティによって、確証されているのと同じ一意のリファレンスを持つべきである。

CEM 段落 805 は、以下のとおりに言い換えられる。

開発者のテスト計画で参照されている TOE は、ACM_CAP.2 サブアクティビティによって、確証されているのと同じ一意のリファレンスを持つべきである。

CEM 段落 838 は、以下のとおりに言い換えられる。

評価者テストに使用される TOE は、ACM_CAP.2 サブアクティビティによって、確証されているのと同じ一意のリファレンスを持つべきである。

CEM 段落 1143 は、以下のとおりに言い換えられる。

開発者のテスト計画で参照されている TOE は、ACM_CAP.3 サブアクティビティによって、確証されているのと同じ一意のリファレンスを持つべきである。

CEM 段落 1176 は、以下のとおりに言い換えられる。

評価者テストに使用される TOE は、ACM_CAP.3 サブアクティビティによって、確証されているのと同じ一意のリファレンスを持つべきである。

CEM 段落 1602 は、以下のとおりに言い換えられる。

開発者のテスト計画で参照されている TOE は、ACM_CAP.4 サブアクティビティによって、確証されているのと同じ一意のリファレンスを持つべきである。

CEM 段落 1635 は、以下のとおりに言い換えられる。

評価者テストに使用される TOE は、ACM_CAP.4 サブアクティビティによって、確証されているのと同じ一意のリファレンスを持つべきである。

解釈－080

発効日：2000 年 10 月 15 日

サブジェクト：APE_REQ.1-12 は、「決定するために、・・・を検査しなければならない」という文章のスタイルになっていない。

参照文献：CEM パート 2、v1.0 ワークユニット APE_REQ.1-12

問題：
CEM パート 2 のワークユニット APE_REQ.1-12 は、「検査しなければならない」という動詞を用いる他のワークユニットと、一貫しない。

解釈：
評価者は、それに関する決定をするために、あるものを「検査する」。このワークユニットは、そのことを明確にしない。CC は、下記の変更で詳述されているように解釈される。

変更：
CEM のワークユニット APE_REQ.1-12 は、以下のとおりに変更される。

> 評価者は、すべての未完了操作が識別されていることを決定するために、IT セキュリティ要件のステートメントを検査しなければならない。

解釈－084

発効日：2001 年 2 月 16 日

サブジェクト：TOE と環境に対しての異なる対策方針

参照文献：CEM パート 2、v1.0、APE_REQ.1-20、ASE_REQ.1-20

問題：
APE_REQ.1.13C 及び ASE_REQ.1.12C については、CEM は、TOE 及び環境に関する類似したワークユニットに対して、異なる語を用いている。

解釈：
ワークユニット APE_REQ.1-20 及び ASE_REQ.1-20 は、「その ***TOE の***セキュリティ対策方針を満たすのに適している。」を含むべきと解釈する。

変更：
CEM ワークユニット APE_REQ.1-20 及び ASE_REQ.1-20 は、以下のとおりに変更される。

> 評価者は、TOE の各セキュリティ対策方針に対して、TOE セキュリティ要件がその TOE のセキュリティ対策方針を満たすのに適しているという適切な正当化を含んでいることを決定するために、セキュリティ要件根拠を検査しなければならない。

根拠：
TOE セキュリティ要件が、TOE のセキュリティ対策方針を満たすのに適していることは、明確でなければならない。現在言い表されているこのワークユニットでは、「そのセキュリティ対策方針を満たすのに適している」と、「TOE の各セキュリティ対策方針」を言及すべきところを「そのセキュリティ対策方針」と書かれている。ここでの解釈は、ワークユニットが、曖昧ではなく、他のワークユニットと一貫するようになされた。

解釈－085

発効日：2002 年 2 月 11 日

サブジェクト：主張全体への追加の SOF 主張

参照文献：CC v2.1:パート 3 APE_REQ1.11C & ASE_REQ.1.10C、CEM パート 2 段落 239 及び 428

問題：
APE_REQ1.11C、ASE_REQ.1.10C(CEM APE/ASE_REQ.1-16)の下で主張がなされている状況が不明確である。

解釈：
ワークユニット APE/ASE_REQ.1-16 は、PP または ST の作成者が特定の SOF 要件を設定する（例えば、最小レベルよりも高いレベルで、あるいは尺度を用いて）場合について言及している。この表題の下にある要件は、PP または ST の作成者の裁量に任せられる。しかし、PP または ST の他の部分と一致しなければならない（例えば、TOE 記述）。

変更：
CC において、パート 3 に以下の変更がなされる。

・要件 APE_REQ1.11C は、下記のように更新される。

セキュリティ要件に関するステートメントは、明示された機能強度主張が要求されるすべてのセキュリティ機能要件を識別しなければならない。同時に、それぞれのセキュリティ機能要件に対して明示された機能強度主張も識別しなければならない。

・要件 ASE_REQ.1.10C は、下記のように更新される。

セキュリティ要件に関するステートメントは、明示された機能強度主張が要求されるすべてのセキュリティ機能要件を識別しなければならない。同時に、それぞれのセキュリティ機能要件に対して明示された機能強度主張も識別しなければならない。

CEM において、以下の変更を行う。

・ ワークユニット APE_REQ.1-16 は、以下のことを明言するために修正される。

評価者は、PP が明示された機能強度が適用されるすべての特定の TOE セキュリティ機能要件を、特定の機能強度または該当する数値尺度と共に識別していることを**チェックしなければならない。**

・ 以下のテキストが、段落 239 の最後に加えられる。

このワークユニットは、PP の作成者が、特定の SOF 要件を設定する（すなわち PP の全体にわたる SOF 主張よりも上位のもの）、あるいは、数値尺度を使用することを要求する場合のものである。TOE セキュリティ機能要件に対する特定の SOF 主張は、PP の作成者によって特定されることもある。特定の主張が存在しない場合、PP に対する全体の主張は、PP で述べられるすべての TOE セキュリティ機能要件に対して適用される。評価者は、明示された SOF 主張の存在または不在が、PP の他の部分に矛盾しないことを確認するべきである。

・以下の新しい段落を、段落 239 の後に含める。

PP は、SOF 主張に対して多様な仕様を持つことができる。PP に対して全体的な SOF 主張があり得る。また、PP の範囲内で、TOE セキュリティ機能要件は、そのために特定された SOF 主張を持つこともできる。

・ ワークユニット ASE_REQ.1-16 は、以下のことを明言するために修正される。

評価者は、ST が明示された機能強度が適用されるすべての特定の TOE セキュリティ機能要件を、特定の機能強度または該当する尺度と共に識別していることを**チェックしなければならない**。

・ 以下のテキストが、段落 428 の最後に加えられる。

このワークユニットは、ST の作成者が、特定の SOF 要件を設定する（すなわち ST の全体にわたる SOF 主張よりも上位のもの）、あるいは、数値尺度を使

用することを要求する場合のものである。TOE セキュリティ機能要件に対する特定の SOF 主張は、ST の作成者によって特定されることもある。特定の主張が存在しない場合、ST に対する全体の主張は、ST で述べられるすべての TOE セキュリティ機能要件に対して適用される。評価者は、明示された SOF 主張の存在または不在が、ST の他の部分に矛盾しないことを確認するべきである。

・ 以下の新しい段落は、段落 428 の後に挿入される。

ST は、SOF 主張に対して多様な仕様を持つことができる。ST に対して全体的な SOF 主張があり得る。また、ST の範囲内で TOE セキュリティ機能要件は、そのために特定された SOF 主張を持つこともできる。

根拠：

CC での要件は、パート 1 B/C.2.6 に記されているように、AVA_SOF.1 が主張されているすべての場合における最小機能強度に対する主張に関するものである。PP の場合には、その作成者は、TOE 実装が確率的または順列的メカニズムを含むかどうか知らないかもしれない。最小限の SOF 主張を含むことは、TOE の最小限の基準に関する主張であり、それは、確率的または順列的メカニズムが TOE に含まれているかどうかに関するステートメントではなく、要件として記されている。

解釈－092

発効日：2001 年 7 月 31 日

サブジェクト：TOE のリリース

参照文献：CC v2.1 パート 3 ALC_FLR

問題：
ALC_FLR.*.1C には、「TOE の各リリース」という語句が含まれている。この語句がなにを意味するかが不明確である。

解釈：
ALC_FLR では、「TOE の各リリース」という語句は、変更が適用された認証 TOE のリリースである製品またはシステムのことを示す。欠陥修正手続きは、その TOE のライフサイクルを通じて適用される。

変更：
CC パート 3 では、以下の段落が、段落 391 の後に加えられる。

> 一旦 TOE の評価が完了していれば、それはもはや評価の対象ではない。さらに、この評価済み TOE へのどんな変更も、オリジナルの評価結果がもはや変更されたバージョンに適用できないことになる。このファミリの中で使用される句「TOE のリリース」は、それ故に変更が適用され認証済み TOE のリリースである製品またはシステムのバージョンのことをいう。

解釈－094

発効日：2001 年 6 月 31 日

サブジェクト： FLR ガイダンス文書の欠落

参照文献：CC v2.1 パート 3　ALC_FLR

問題：
ALC_FLR.2とALC_FLR.3は、利用者や管理者から開発者が受け取るべき情報の概念について、彼らが欠陥を報告する手段(ALC_FLR.2.5C)や彼らが開発者に登録する手段(ALC_FLR.3.7C)を含め伝えている。しかしながら、いかにセキュリティ欠陥を開発者に報告し、そしていかに彼らを開発者に対し登録するかを明らかにするガイダンスに対応する開発者から利用者あるいは管理者への要件が存在しない。唯一のガイダンス要件は、開発者によってなされる手続きの記述のみである。しかし利用者や管理者が開発者と連絡する手段についてはなにもない。配付されるTOEの一部としてみなされるべきそのようなガイダンスの必要性を満たすような付加的な要件が必要とされる。

解釈：
CC v2.1 パート3の議論は、利用者が報告する方法、開発者がその報告を受け取る方法、そして利用者を開発者に登録する方法を特定するいくつかの要件がまったく抜けている。また、明示的に示されるべき開発者によるアクションが、暗示的である内容・提示の要件がある。下記に詳述する変更は、欠落した必要な要件テキストを満たすものである。

変更：
CCパート3で下記の変更がなされる。

・以下の段落が、ACL_FLR 適用上の注釈節の段落390直後に加えられる。

> TOE利用者は、セキュリティ欠陥に対する処置を受け取る及び実装することに責任を負う利用者組織において、中心であると考えられる。これは必ずしも個々の利用者ではなく、セキュリティ欠陥の取り扱いに責任を負う、組織的な代表者であってもよい。用語「TOE利用者」の使用は、異なる組織が個々の利用者でもよいしあるいは中央行政機関によって行われてもよい欠陥報告を扱うための異なる手続きを持っていることを認識する。

・開発者アクションエレメントALC_FLR.1.1Dは、次のように修正される。

ALC_FLR.1.1D　開発者は、TOE開発者に対する欠陥修正手続きを提供しなければならない。

・以下の目的節が、依存性の節直前のALC_FLR.2に加えられる。

目的：
TOE利用者は、開発者がTOE利用者からのセキュリティ欠陥報告に基づいて適切に行動することができ、かつ誰に訂正処置を送るかを知ることができるために、開発者にセキュリティ欠陥報告を提出する方法を理解する必要がある。開発者からTOE利用者への欠陥修正ガイダンスは、TOE利用者がこの重要な情報に気づいていることを保証する。

・開発者アクションエレメントALC_FLR.2.1Dは、次のように修正される。

ALC_FLR.2.1D　開発者は、TOE開発者に対する欠陥修正手続きを提供しなければならない。

・以下の開発者アクションエレメントが、ALC_FLR.2コンポーネントに加えられる。

ALC_FLR.2.3D　開発者は、TOE利用者に対する欠陥修正ガイダンスを提供しなければならない。

・エレメントALC_FLR.2.5Cは、ALC_FLR.2.6Cに振り直される。

・エレメントALC_FLR.2.6Cは、ALC_FLR.2.7Cに振り直される。

・以下の内容・提示エレメントが、ALC_FLR.2コンポーネントに加えられる。

ALC_FLR.2.5C　欠陥修正手続き証拠資料は、開発者がTOEの疑わしいセキュリティ欠陥に関する報告及び問合せを、TOE利用者から受け取る手段について記述しなければならない。

ALC_FLR.2.8C　欠陥修正ガイダンスは、TOE利用者が開発者へTOEの疑わしい

セキュリティ欠陥を報告する手段について記述しなければならない。

・以下の目的節が、依存性の節直前のALC_FLR.3に加えられる。

目的：
TOE利用者は、開発者がTOE利用者からのセキュリティ欠陥報告に基づいて適切に行動することができ、かつ誰に訂正処置を送るかを知ることができるために、開発者にセキュリティ欠陥報告を提出する方法と、開発者がこれらの訂正処置を受け取ることができるように、開発者に対してTOE利用者自身を登録する方法を理解する必要がある。開発者からTOE利用者への欠陥修正ガイダンスは、TOE利用者がこの重要な情報に気づいていることを保証する。

・開発者アクションエレメントALC_FLR.3.1Dは、次のように修正される。

ALC_FLR.3.1D　開発者は、TOE開発者に対する欠陥修正手続きを提供しなければならない。

・開発者アクションエレメントALC_FLR.3.3Dは、次のように修正される。

ALC_FLR.3.3D　開発者は、TOE利用者に対する欠陥修正ガイダンスを提供しなければならない。

・エレメントALC_FLR.3.5Cは、ALC_FLR.3.6Cに振り直される。

・エレメントALC_FLR.3.6Cは、ALC_FLR.3.7Cに振り直される。

・エレメントALC_FLR.3.7Cは、ALC_FLR.3.9Cに振り直される。

・以下の内容・提示エレメントが、ALC_FLR.3コンポーネントに加えられる。

ALC_FLR.3.5C　欠陥修正手続き証拠資料は、開発者がTOE利用者からのTOEの疑わしいセキュリティ欠陥に関する問合せや、報告を受け取る手段について記述しなければならない。

ALC_FLR.3.8C　欠陥修正ガイダンスは、TOE利用者が開発者へTOEの疑わしい

セキュリティ欠陥を報告する手段について記述しなければならない。

ALC_FLR.3.10C　欠陥修正ガイダンスは、TOE利用者が開発者にセキュリティ欠陥報告及び訂正を受け取る資格を得るために登録する手段について記述しなければならない。

ALC_FLR.3.11C　欠陥修正ガイダンスは、TOEに含まれるセキュリティ問題に関するすべての報告及び問合せを受け付けるための窓口を識別しなければならない。

注意：この解釈ページは、誤植の校正と最後の中点(ALC_FLR.3.11Cのための新しいテキスト)に解釈－062*の結果を取り入れるために更新される必要がある。

*(*訳者注：2001 年 7 月 31 日発行の解釈－062 と併用することにより、このページの更新は必要ない。)*

解釈－095

発効日：2001 年 2 月 16 日

サブジェクト： ACM_SCP に対する ACM_CAP の依存性

参照文献：CC v2.1 パート 3　ACM_CAP

問題：
ACM_CAP.3、4 及び 5 は、ACM_SCP.1 に対して依存性を持っている。これは、間違った依存性であり、削除されるべきである。

解釈：
ACM_CAP.3、4 及び 5 の ACM_SCP.1 に対する依存性は、要求されていない。

変更：
CC における ACM_CAP.3、4 及び 5 の ACM_SCP.1 に対する依存性は、取り除かれる。

根拠：
要求される粒度及び構成管理の範囲に関する明確なステートメントを持っていることは望ましいが、ACM_CAP.2、3、4 または 5 の使用は、TOE の最小限の単一の構成要素を課し、このような理由で独立した要件である。PP/ST の作成者が、構成リストに対する最小限以上の ACM_CAP 要件を望む場合、ACM_SCP のコンポーネントを、追加の保証要件として、PP/ST に含めることができる。

解釈－098

発効日：2002 年 2 月 11 日

サブジェクト：詳細化の制限

参照文献：CC v2.1、パート 1

問題：
詳細化と明示された要件との間の相違は何か。

解釈：
既存の（パート 2 またはパート 3 からの）CC 要件へのいかなる変更も、詳細化または要件拡張のどちらかである。その変更が要件拡張ではなく詳細化であるためには、その変更が以下の条件の両方を満たさなければならない。

- 変更された要件を満たしている TOE は、特定の PP または ST のなかで解釈されたように、変更されていない要件もまた満たすであろう。そして
- 変更された要件は、元来の要件の範囲を拡張しない。

変更：
CC v2.1、パート 1、4.4.1.3 節は、解釈―019 によって更新される。

解釈－116

発効日：2001 年 7 月 31 日

サブジェクト：ADO_DEL の区別できないワークユニット

参照文献：CEM v1.0、ワークユニット*:ADO_DEL.*-1 及び*:ADO_DEL.*-2.

問題：
:ADO_DEL.-1 及び *:ADO_DEL.*-2. 間には、相違はないように思われる。*:ADO_DEL.*-1 が、なにが必要であるかに着目する一方、*:ADO_DEL.*-2 は、なにが適切であるかに焦点をあてている（この区別は CC には見えない）。

解釈：
ADO_DEL.*-1 及び ADO_DEL.*-2 に関連する評価者アクションについては、必要性及び適切性との間に相違はない。すなわち、両者とも、セキュリティ対策方針の範囲内にある。結果として、ワークユニット ADO_DEL.*-2 は、ADO_DEL.*-1 に、何も付言しない（ADO_DEL.*-2 のガイダンスの第 2 段落に記載の例を除く）。

変更：
以下の変更が、CEM に対してなされる。

- 以下の段落が、段落 670、966、及び 1340 の直後に加えられる。

  パッケージングと配付のための標準的な商習慣を受け入れることができる。これには、シュリンクラップパッケージング、セキュリティテープ、または封印された封筒などが含まれる。配付には、公共郵便または民間の配付サービスが受け入れられる。

  配付手続きの選択の適切性は、TOE（例えば、それがソフトウェアであるか、またはハードウェアであるか）、及びセキュリティ対策方針によって影響される。配付手続きが、TOE の異なる部分について異なる場合には、手続きの全体性が、セキュリティ対策方針全体を満たすのに適している。

- ワークユニット 2:ADO_DEL.1-2 及びそのガイダンス（段落 671-672）は、削除さ

れる。

- ワークユニット 3:ADO_DEL.1-2 及びそのガイダンス（段落 967-968）は、削除される。

- ワークユニット 4:ADO_DEL.2-2 及びそのガイダンス（段落 1341-1342）は、削除される。

解釈－120

発効日：2001 年 11 月 12 日

サブジェクト：不明確なプロセス予想のサンプリング

参照文献：CEM v1.0 附属書 B.2

問題：
以下の文章（CEM v1.0 パート 2 B.2 節 p. 348 段落 1791 a）は、不適切である。
「ここでは、プロセス（例えば、訪問者の管理または設計レビュー）が守られていることの証拠を得ることに関係するサンプリングは、パーセント値は適切ではない、［・・・］」

解釈：
必要とされる証拠は、プロセスが守られることである。

変更：
CEM の段落 1791 a)の第 2 段落の前半部分は、以下と置き換えられる。

> ここでは、プロセス（例えば、訪問者の管理または設計レビュー）が守られている証拠を得ることに関係するサンプリングは、パーセント値は適切ではない。評価者は、プロセスが守られているという納得のいく確信を得るために、十分な情報を入手し、サンプルサイズの正当性を示すべきである。

解釈－127 r1

更新日：2002 年 10 月 25 日

サブジェクト：正しい位置にない TSS ワークユニット

参照文献：CEM v1.0 ASE_TSS.1-6

問題：
CEM では、機能に対する SOF 主張を扱うワークユニット ASE_TSS.1-6 は、ASE_TSS.1.10C に記載されるべきである。加えて、CEM では、評価者が分析を行うのか、あるいは開発者によって提供された分析を評価者がチェックするのかが不明確である。

解釈：
ワークユニットは、正しい位置にある。

開発者は、その分析を提供する。

変更：
CEM では、段落 490 は、次のように変更される。

> 評価者は、機能強度主張が適切である各 IT セキュリティ機能に対して、それがさかのぼるすべての TOE セキュリティ機能要件に対しこの主張が適していることを TOE 要約仕様根拠が実証することを決定する。

解釈－128 r1

更新日：2002 年 11 月 25 日

サブジェクト：配付手続きのカバレージ

参照文献：CEM v1.0　4:ADO_DEL.2-1

問題：
段落 1338 では次のように述べられる。

手続きは、TOE のどの部分が、これらの手続きによって取り扱われる必要があるのか記述する（・・・）。配付手続きは、TOE 全体を参照する、・・・

手続きが、すべての TOE を取り扱うのか、または TOE の一部だけを取り扱うのかどうか明確ではない。

解釈：
配付証拠資料は、TOE 全体を扱うべきである。しかし、それには、TOE の異なる部分に対する異なる手続きが含まれてもよい。

変更：
段落 1338 は、以下と置き換えられる。

> 配付証拠資料は、TOE の識別を決定し、TOE またはそのコンポーネント部分の輸送中の TOE セキュリティを維持するための適切な手続きを記述する。配付証拠資料には、適用可能な物理的または電子的（例えば、インターネットからダウンロードする）な配付の手続きが含まれる。配付証拠資料は、TOE 全体に渡るが、TOE の異なる部分に対する異なる手続きを含んでもよい。

解釈－133 r1

更新日：2002 年 10 月 25 日

サブジェクト：AVA_MSU.2 における一貫性分析

参照文献：CEM、パート 2 v1.0 ワークユニット 4:AVA_MSU.2-8

問題：
322 ページの段落 1688 に、一貫性分析に関する附属書への参照がある。このワークユニットには一貫性分析はなく、従って、一貫性分析に関するガイダンスへの参照は有用ではない。

解釈：
一貫性分析は、ワークユニット 4:AVA_MSU.2-8 では必要ではない。

変更：
CEM の 322 ページ段落 1688 は、取り除かれる。