情報技術
セキュリティ評価のための
コモンクライテリア

パート 4: 評価方法及び評価アクティビティの
仕様のための枠組み

2022 年 11 月

CC:2022
改訂第 1 版

CCMB-2022-11-004

令和 5 年 9 月 翻訳第 1.0 版
独立行政法人情報処理推進機構
セキュリティセンター
セキュリティ技術評価部

目次

IPA まえがき

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

原文

Common Criteria for Information Technology Security Evaluation

Part4: Framework for the specification of evaluation methods and activities

CC:2022 Revision 1

November 2022 CCMB-2022-11-004

まえがき

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

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

CC:2022 は、以下のパートから構成されている。

— パート1：概説と一般モデル

— パート2：セキュリティ機能コンポーネント

— パート3：セキュリティ保証コンポーネント

— パート4(新規)：評価方法及び評価アクティビティの仕様のための枠組み

— パート5(新規)：セキュリティ要件の定義済みパッケージ

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

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

CC:2022 は、次のような具体的な変更点を取り入れている。

— 文書が再構成され、新たなパートが追加された。

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

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

— 以下の技術的な変更が導入された。

  — 用語が見直され、更新された。

— 新しい機能要件及び新しい保証要件が導入された。

— 完全適合の種別が導入された。

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

— マルチ保証評価が導入された。

— 保証の統合が導入された。

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

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

法定通知

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

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

序説

CCは、IT製品のセキュリティ機能に関する一般的な要件と、セキュリティ評価時にIT製品に適用される保証手段の一般的な要件を提供することにより、独立したセキュリティ評価結果間の比較を可能にする。CEMは、CCで規定されたいくつかの保証要件に対応する評価方法を提供する。

CCパート1のセキュリティ評価モデルでは、CEMで定義された高水準の一般的な評価アクティビティを識別するが、より具体的な評価アクティビティ(EA)は、これらの一般的なアクティビティを特定の評価コンテキストに適合させたものとして定義できる。例えば、セキュリティ機能要件(SFR)又はセキュリティ保証要件(SAR)を特定の技術又は評価対象(TOE)種別に適用する場合などである。このような評価アクティビティの仕様は、すでに実務者の間で実現されており、評価アクティビティを定義するための仕様の必要性が生じている。

本書は、CEMのワークユニットから評価アクティビティを派生し、評価アクティビティを評価方法(EM)にグループ化するための枠組みを記述している。評価アクティビティと評価方法は、プロテクションプロファイル(PP)及びそれをサポートするあらゆる文書に含めることができる。PP、PP構成、PPモジュール、パッケージ、又はセキュリティターゲット(ST)が、特定の評価方法/評価アクティビティを使用することを識別している場合、評価者は、評価者判定を割り付ける際に、関連する評価方法/評価アクティビティに従い、それを報告することがCEMにより要求される。CCパート1に示すように、場合によっては評価方法/評価アクティビティを認めない場合もあり、その場合は、評価監督機関(evaluation authority)がその評価方法/評価アクティビティを要求するSTに従って評価を実施しないと決定することもできる。

本書では、拡張SARの評価アクティビティを定義することも認めており、その場合、評価アクティビティの導出は、拡張SARに定義された同等のアクションエレメント及びワークユニットに関連する。本書において、SARにCEM又はCCパート3を使用することが参照されている箇所(評価アクティビティの根拠を定義する場合など)は、拡張SARの場合、代わりにその拡張SARのために定義された同等のアクションエレメント及びワークユニットへの参照が適用される。

明確化のため、本書は評価方法及び評価アクティビティを定義する方法を規定するが、具体的な評価方法又は評価アクティビティは定義しない。

次の注釈は、CCの他パート及びCEMにおいて、これらの文書における太字及び斜体の使用について記述している。本書ではこれらの規則を使用しないが、CCの他パート及びCEMとの整合性を保つため、この注釈を残している。

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

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

情報技術セキュリティ評価のためのコモンクライテリア ― パート4：評価方法及び評価アクティビティの仕様のための枠組み

1　適用範囲

本書は、客観的で、反復可能かつ再現可能な評価方法及び評価アクティビティを規定するための標準化された枠組みを提供する。

本書は評価方法及び評価アクティビティを評価、採用、維持する方法については特定しない。これらの点については、各自の専門分野で評価方法及び評価アクティビティを開発した者が責任を持つべき事項である。

2 規定の参照

本文中では、以下の文書を、その内容の一部又は全部が本書の要件となるように引用している。日付の古い文献については、引用された版のみが適用される。日付のない文献については、引用した文献の最新版(改訂を含む)が適用される。

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

情報技術セキュリティ評価のためのコモンクライテリア、CC:2022、改訂第1版、2022年11月 — パート2：セキュリティ機能コンポーネント

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

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

3 用語と定義

本書では、CCパート1、CCパート2、CCパート3及びCEMの用語と定義が適用される。

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

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

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

4 評価方法及び評価アクティビティの一般的なモデル

4.1 概念とモデル

CEMは、CCパート3に定義された保証クラス、ファミリ、コンポーネントのほとんどについて、評価者が評定に至るために実施する一般的なワークユニットのセットを定義している。CCパート3のSARの構造とCEMのワークユニットとの関係は、CEMに記載されており、図1に要約されている。

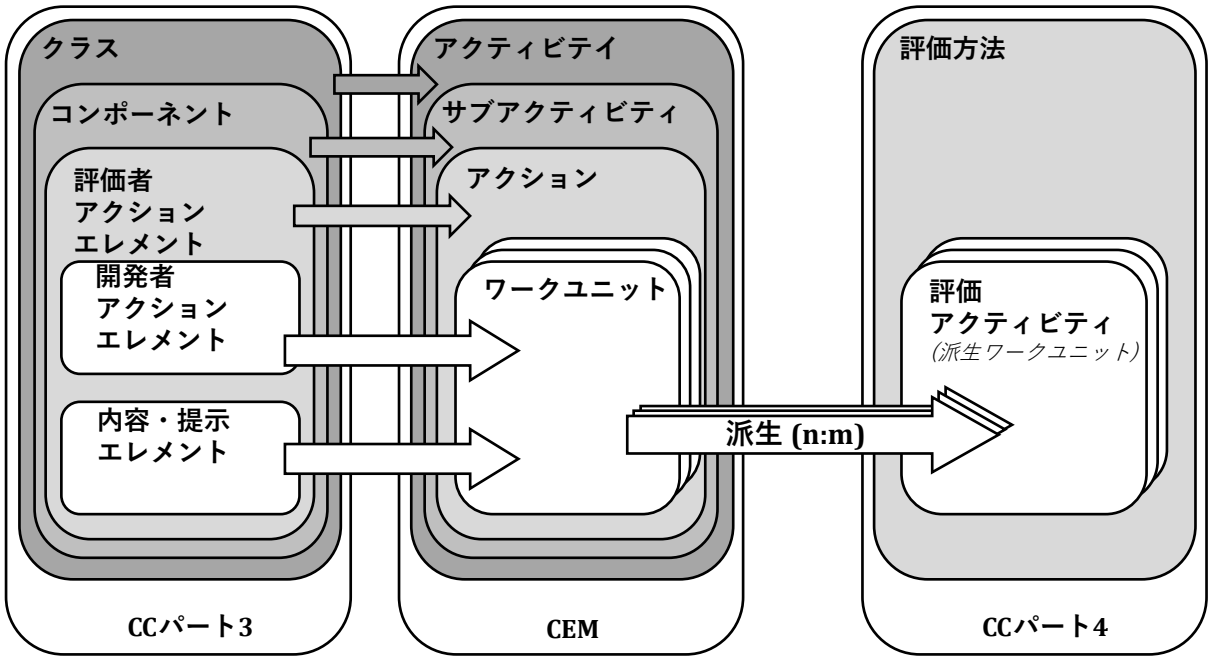

図 1 — CC パート 3 及び CEM の構造と本書の構造とのマッピング

新しい評価方法及び評価アクティビティを定義する上で注意すべき点は、CEMでは各アクション(CCパート3の評価者アクションエレメント又は暗黙の評価者アクションエレメントを表す)は、評価者が実施するワークユニットのセットとして表現されている点である。

本書では、CEMの一般的なワークユニットから新たな評価アクティビティを派生させ、特定の評価コンテキストで使用することを目的とした評価方法として組み合わせる方法を規定する。このような評価コンテキストの典型的な例としては、特定のTOE種別や特定の技術種別が挙げられる。

例1

TOE 種別：ネットワーク機器

技術種別：特定の暗号機能

評価方法及び評価アクティビティが特定のPP、PPモジュール、PP構成と共に用いられることが要求される場合、PP又はPPモジュール又はPP構成は、その適合ステートメントにおいてその要求を識別しなければならない。評価方法及び評価アクティビティが、特定のパッケージで使用されることが要求される場合、そのパッケージは、セキュリティ要件の節でこの要求を識別しなければならない。STがPP、PP構成、又はパッケージへの適合を主張する結果として、評価方法及び評価アクティビティがSTによって主張される場合、STは、その適合主張で使用される評価方法/評価アクティビティを識別しなければならない。いずれの場

合も、CCパート4への適合を正式に主張することはできない(PP、PPモジュール、PP構成及びパッケージの内容は、CCパート1でより詳細に記述されている)。

PP、PP構成、PPモジュール、パッケージは、複数の評価方法又は別々の評価アクティビティのセットを使用することができる。

例2：PPで使用される暗号操作とセキュアチャネルプロトコルに別々の評価方法が定義されている場合、複数の評価方法を使用することができる。

注：完全適合が使用される場合、CCパート1は、評価方法/評価アクティビティがPP構成において定義されることを認めないと述べている。つまり、使用される評価方法/評価アクティビティは、PPとPPモジュールに含まれるが、PP構成には含まれない。

PP、PPモジュール、PP構成、又はパッケージが、ある評価方法/評価アクティビティを使用することを識別する場合、これは、要件を述べ、使用する評価方法/評価アクティビティの定義を参照するという標準的な表現を用いて行われる。STは、STが適合を主張するPP、PPモジュール、PP構成又はパッケージに含まれる要求される評価方法及び評価アクティビティのみを識別しなければならない(すなわち、ST自体は、いかなる評価方法や評価アクティビティを追加、修正又は削除してはならない)。STは、STが要求する全ての評価方法/評価アクティビティ(すなわち、STが適合を主張するPP、PPモジュール、PP構成、又はパッケージが要求するものを含む)を識別し、評価者やST読者が確認・参照できる単一のリストが存在するようにしなければならない。

評価方法及び評価アクティビティは、それらを要求する文書内で(例えば、PPの一部として)、又は外部的に別の文書で(あるいはその両方の組み合わせで)定義することができる。上記のように識別が必要であるが、評価方法/評価アクティビティのテキストを他の文書に転載する必要はない(例えば、STは、適合を主張するPPから評価方法/評価アクティビティの全文を含める必要はない)。

4.2 評価方法及び評価アクティビティの派生

一般に、評価アクティビティ及び評価方法の定義は、そのワークユニットの一部又は全部をより具体化することを目指してSARから開始する場合と、そのSFRに関連するワークユニットの特定の側面を定義することを目指してSFRから開始する場合がある。

SARから開始する場合、プロセスのガイドラインは次のとおりである。

a) 少なくとも一つの個々の評価アクティビティ又は評価アクティビティのグループを導き出すために、関連するCEMワークユニットを識別すること。

b) 評価アクティビティを派生させる元の各ワークユニットについて、以下のことを行うこと。

   1) 実施すべき具体的な作業及び評価基準の観点から、新たな評価アクティビティを6.2に記述されているように定義すること(必要な場合は、6.2.8に記述されている合格/不合格の基準を含む)。

   2) 必要に応じて、評価アクティビティを評価方法にグループ化すること。

   3) 5.2.10及び6.2.10に記述されているように、新しい評価アクティビティとそれらをグループ化した評価方法の根拠を記述すること。

      例：根拠には、派生元のワークユニットの開発者アクションエレメント、及び、内容・提示エレメントへの参照を含めることができる。

SFRから開始する場合のガイドラインは、次のとおりである。

a) 関連するSFRを識別すること。

b) 特定のSFRに対応するSAR(CCパート3又は拡張SARのセット、あるいはその両方から)及び対応するCEMワークユニットを識別すること。

c) 実施すべき具体的な作業及び評価基準の観点から、新たな評価アクティビティを6.2に記述されているように定義すること(必要な場合は、6.2.8に記述されている合格/不合格の基準を含む)。

例：評価アクティビティは、(ASEから派生した)TOE要約仕様における特定のSFRの表現の検査、(AGDから派生した)ガイダンス文書におけるSFRの表現の検査、及び(ATEから派生した)SFRの特定のテストの実施を定義することができる。

d) 影響を受けるSARのワークユニットを新しい評価アクティビティにマッピングすること。

e) 5.2.10及び6.2.10に記述されているように、新しい評価アクティビティとそれらをグループ化した評価方法の根拠を記述すること。

作成者はSAR又はSFRから開始することを選択できるが、SARは最終的に全てのSFRをカバーすることに注意すること。上記のようにSFRから始めることは、SARが特定のSFRにどのように適用されるかの詳細を明らかにする際に有用であり、SFRをその評価アクティビティの記述と一緒に提示する際に有用な手法である。

ワークユニットと新しい評価アクティビティを1対1にマッピングする必要はなく、実際の対応付けは(5.2.10で述べるように)根拠として文書化される。導出は、個々のワークユニット又はワークユニットのグループに関して行うことができ、これを図2に示す。図2のa)の場合、作成者はCEMの各ワークユニットを対応する一つの評価アクティビティに対応付け、b)の場合、作成者は異なる数のワークユニットと評価アクティビティを、アクション(すなわち、ワークユニットの集合)の全ての側面を扱いながら、マッピングする。

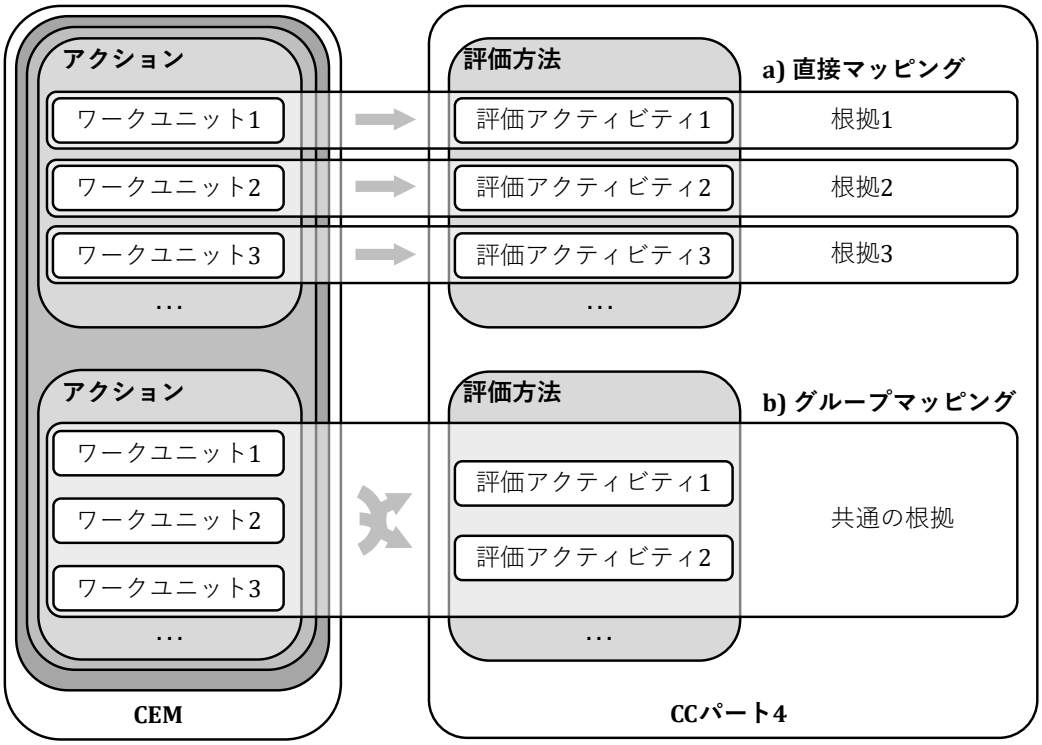

図 2 — CEM と派生した評価アクティビティをマッピングするための選択肢

特定のワークユニットや評価アクティビティの内容によっては、他のアプローチも可能である。つまり、同じ数のワークユニットと評価アクティビティが存在する場合でも、単純な1対1のマッピングは不可能で、したがってアクションレベルでのマッピングが適切である場合がある。より詳細なマッピングの状況は、以下の例で記述されている。

注：これらの例は、記述された評価アクティビティが、評価アクティビティの完全性の根拠の適切性を判断できるコミュニティによって定義されていることを前提としている。これらの例は、マッピングの形式と構造のみに関するものであり、完全性の根拠の性質や受容性には関係しない。

例1

ソフトウェアとハードウェアの両方を含むTOE種別の場合、製造環境とそのプロセスに対処するための追加評価アクティビティを定義することができる。ALC_DVSファミリを考慮すると、ソフトウェア開発環境については既存のALC_DVSワークユニットを全て採用し、関連するハードウェア及び製造の各側面について追加の評価アクティビティを定義することが考えられる。これらの側面には、通常のALC_DVSの範囲を拡張して、開発環境におけるハードウェア設計の保護、開発環境から製造環境へのソフトウェアの安全な転送、製造現場のセキュリティ、配付待ちの製造製品の保護といった項目を追加することができる。また、製造環境でのみ発生するオブジェクトやプロセスに関する以下のような新たな側面を含めることも可能である。

— 製造ラインで使用されるファームウェアが、ファームウェアビルドシステムで作成された正規版から確実に取得されていることの確認

— 製造ラインでTOEをテストするためのテストプログラムの構成管理のチェック

— TOEのテスト又はデバッグ用インタフェースを無効にする操作が正確かつ確実に実行されていることの確認

— 製造中にTOEに鍵又は証明書を注入するために使用される鍵管理システムの物理的及び論理的セキュリティの検査

この例では、オリジナルのALC_DVS.1.1Eのアクションは全て新しい評価アクティビティに含まれるようにマッピングされているが、代替的なアプローチとして、ALC_DVS.1.1Eの個々のワークユニットごとに、そのワークユニットの製造環境を対象とする追加アクティビティを識別し、評価アクティビティを定義することが考えられる。

例2

AVA_VAN.1脆弱性分析が特定のタイプのTOEに適用され、使用するパブリックドメインの脆弱性の情報源に一貫性が求められる場合、使用する特定の情報源を指定することによって、おそらく実施する特定の探索と分析及びテストする潜在的脆弱性のリストを選択する決定基準とともに、パブリックドメインの情報源を探索するAVA_VANワークユニットをカバーする評価アクティビティを定義するというアプローチが可能である。この例では、元のAVA_VAN.1-3ワークユニットが新しい評価アクティビティにマッピングされている。

例3

集積回路のようなハードウェアの評価方法では、回路のインタフェースを利用した操作や情報についての具体的な詳細を評価者に与える必要な入力を定義し、回路のアーキテクチャを検査する評価アクティビティを定義することができる。これらの必要な入力を定義することで、回路の物理的表面、実行可能なプログラミング命令、及び通信インタフェースが関連インタフェースであることを明確にすることができる。

その評価方法の評価アクティビティではさらに、TSFの機能の改ざんや無効化を防ぐための、物理的なプロービングに対する回路の耐性を検査することができる。

テストアクティビティについて、その評価方法の評価アクティビティでは、回路のサブシステムに行き渡るセキュリティ機能のフローチャートとして回路設計を必要な入力に定義することができる。このフローチャートは、評価者がテストケースを作成し、回路のテストカバレッジを確認するために使用することができる。

例4

暗号的に検証可能なファームウェア更新を提供するネットワーク機器のようなTOEタイプの場合、評価アクティビティは、暗号更新プロセスに要求される特定の性質を確認するために、評価者がセキュリティターゲットとガイダンス文書をどのようにレビューすることが要求されるかについて具体的な詳細を示すことができる。

他の評価アクティビティでは、TOEの受入機能をテストするために、現在のファームウェアの検証、アップデートの可用性、アップデートの取得、暗号署名を用いたアップデート源の検証、特定の種類の無効なアップデートの利用をカバーする特定のテストケースを定義することが可能である。

4.3 評価方法及び評価アクティビティの記述における動詞の使用法

CCパート1で動詞が定義されている場合、評価アクティビティの記述では、その定義に従ってのみ動詞を使用しなければならない。別の動詞が評価方法において定義されている場合は、その評価方法において、評価アクティビティに使用するため、その別の動詞を使用することができる。そのような動詞の定義では、(単純なチェックとは異なり)評価者の判断がどの程度関与するのかを明確にしなければならない。

例：プロトコルの自動テスト生成を含む評価方法は、プロトコルパラメータの列挙型に適用される動詞「カバー(cover)」を定義し、利用可能なパラメータ長内でパラメータの全ての定義及び未定義の値

を試すことを意味することができる。その場合、評価アクティビティは、「評価者はPaymentModeフィールドをカバーしなければならない」といった形で記述することができる。

本書では、*チェックする(check)*、*検査する(examine)*、*報告する(report)*、*記録する(record)*などの評価者アクションの動詞は、CCパート1で定義された意味で使用される。

4.4 評価方法及び評価アクティビティの記述のための規約

以下の段落は、CCパート3及びCEMで使用される、評価方法及び評価アクティビティの記述における一貫性を保つための規約について記述している。

全てのワークユニット及びサブタスクの動詞の後に助動詞「しなければならない(shall)」を置き、動詞と「しなければならない(shall)」の両方をイタリック体の太字で表示する。助動詞「しなければならない(shall)」は、提供されたテキストが必須である場合にのみ使用され、したがって、ワークユニットとサブタスクの中でのみ使用される。ワークユニットとサブタスクには、評価者が評定を割り付けるために実行しなければならない必須のアクティビティが含まれている。

ワークユニット及びサブタスクに付随するガイダンステキストは、評価におけるワークユニット及びサブタスクの適用方法について、さらなる説明を提供する。

5 評価方法の構造

5.1 概要

評価方法とその構成要素である評価アクティビティは、特定の評価コンテキストで使用するために定義される。例えば、特定の機能から特定の製品タイプにまで及ぶ特定の技術分野に対して個別の評価方法を定義することができる。極端な例では、特定の製品に対して、その製品独自の機能が評価されるが、評価の可視性、反復性、再現性をサポートする個別に定義された方法を使用してその製品を評価することが必要な場合にも、個別の評価方法を定義することができる。

例：個別の評価方法を定義することができる評価コンテキストは以下のとおり。

— ネットワーク機器、スマートカード、バイオメトリクス機器、モバイル機器などの特定の製品種別

— 暗号機能、暗号プロトコル、電子証明書の検証、識別認証スキームなど、複数の製品種別で再利用される特定のセキュリティ機能

評価方法は、個々の評価アクティビティの集合で構成され、評価アクティビティが一体となって識別された評価コンテキストに関連する目標を達成する方法についての追加情報が含まれる。

評価方法の記述には、以下が含まれる。

a) 評価方法の定義及び維持管理に責任を持つエンティティの識別。

b) 評価方法の意図する範囲、評価方法における評価アクティビティを導き出す目的、適用を意図する評価コンテキスト、及び評価方法の既知の制限、又は評価方法によってカバーされることを意図しない側面を識別する。

c) 評価方法に含まれる評価アクティビティを実施するために必要なツールタイプ及び/又は評価者の能力。

d) 評価方法の適用結果の報告に関するあらゆる要件。

e) 評価方法の評価アクティビティが扱うCEMの各ワークユニット(又は拡張SARの場合は同等のもの)の識別。

f) 評価方法の派生元の拡張SARの識別(該当する場合)。

g) 評価アクティビティの記述において、CCパート1で定義された動詞の代わりに使用される追加の動詞。

どの内容エレメントが必須であるかの識別、及び内容エレメントが評価方法及びその評価アクティビティ間でどのように分配されるかを含む内容の更なる記述は、5.2及び6.2で示され、表1に要約されている。内容エレメントが任意である場合(例えば、特定の評価者の能力の識別、又は必要なツールタイプ)、その部分は関連する定義から単に省略することができる。つまり、空白の節を含める必要はない。

5.2 評価方法の仕様

5.2.1 概要

評価方法は、5.2.2～5.2.12で特定された情報に基づいて規定される。5.2.2～5.2.12の個々のエレメントに記載されている場合を除き、この情報の提供又は提示に特定の形式は要求されない。5.2.2～5.2.12で評価方法の記述を特定する目的は、評価に用いる保証技術を明確に識別でき、評価方法を適切に(意図したコンテキストで)使用し、一貫した評価結果を支援することである。

一般に、評価方法の記述には、その評価方法に含まれる個々の評価アクティビティの記述が含まれると考えることができる。つまり、評価方法の記述の側面は、評価アクティビティの記述から推測することができる。

図3は、本書で記述される評価方法の内容を示したものである。評価方法を記述するための必須の構造を定義するものではない。

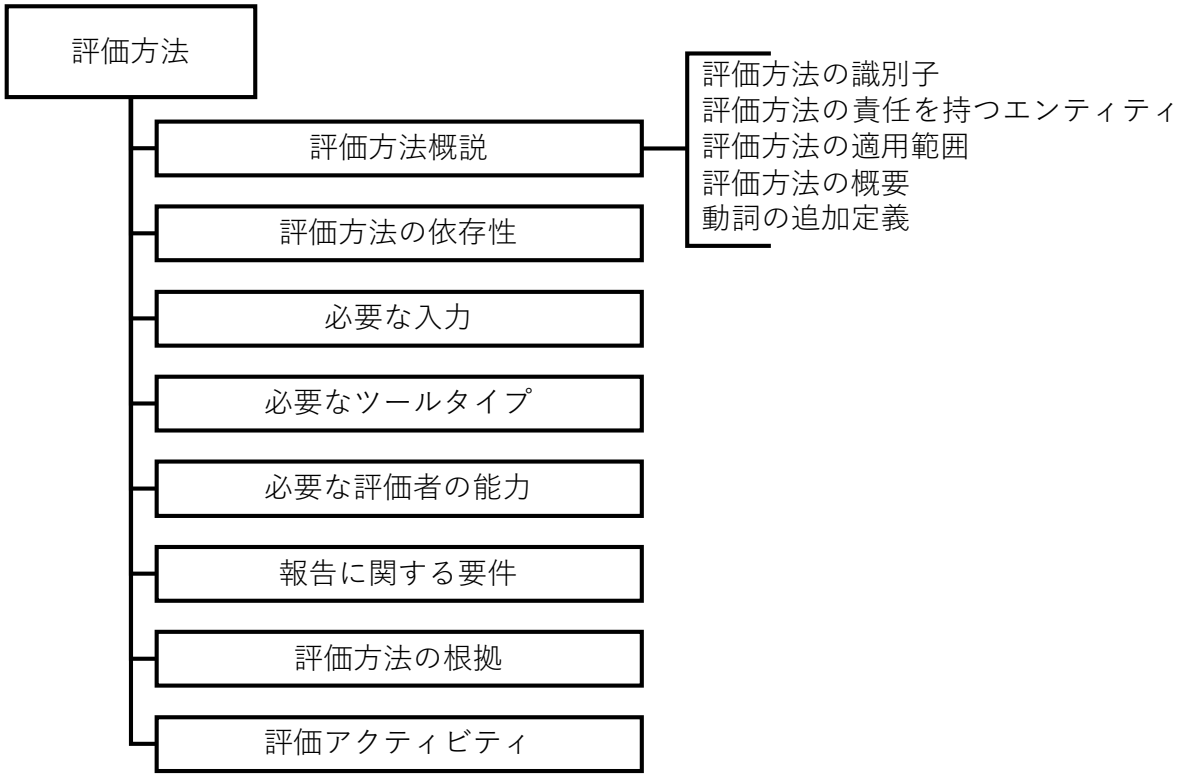

図 3 — 評価方法の内容

図3に示す内容については、5.2及び6.2で詳しく記述し、評価方法及び評価アクティビティを規定するための必須要件と任意要件の概要を表1に示す。

表 1 — 評価方法(EM)及び評価アクティビティ(EA)間の内容配分

内容エレメント	評価方法	評価アクティビティ
識別子	必須	必須
責任を持つエンティティ	必須	該当なし
適用範囲	必須	該当なし

内容エレメント	評価方法	評価アクティビティ
依存性	評価方法又は評価アクティビティレベルで任意	
必要な入力	評価方法又は評価アクティビティレベルで必須	
必要なツールタイプ	評価方法又は評価アクティビティレベルで任意	
必要な評価者の能力	評価方法又は評価アクティビティレベルで任意	
報告に関する要件	評価方法又は評価アクティビティレベルで任意	
根拠	評価方法又は評価アクティビティレベルで必須	
評価アクティビティ	必須	該当なし
追加の動詞の定義	任意	該当なし
目的	該当なし	必須
評価アクティビティとSFR、SAR、その他の評価アクティビティとの関連性	該当なし	任意
評定戦略	該当なし	必須
合格/不合格の基準	該当なし	任意
該当なし：評価方法又は評価アクティビティには該当しない。		

5.2.2 評価方法の識別

評価方法の定義は、評価において適用される評価アクティビティのセットを曖昧さなく識別するために一意の識別子を含めなければならない。識別子は、評価方法が全体として適用されることを意図していることを反映し、(単に評価アクティビティのレベルでなく、むしろ)評価方法レベルで割付されるべきであり、このレベルでの根拠と定義された目的及び目標に従わなければならない。評価アクティビティのセットが一つの評価方法にグループ化されていたとしても、その評価方法に含まれる評価アクティビティの完全なセットを、元の評価方法に含まれるものと同じ根拠で使用した場合のみ、同じ評価方法として識別されなければならない。評価方法をより小さな評価アクティビティのサブセットに分割する必要がある場合は、それぞれのサブセットに対して、独自の根拠を持つ別々の評価方法を定義しなければならない。

例1：評価方法を含むサポート文書又はPPのタイトルとバージョン番号で表される一意の識別子

例2：登録機関より取得した識別子

5.2.10に記述されているように、評価方法は、(例えば、他のPPやPPモジュールで使用するために)他の評価方法と重ね合わせることができる。この場合、元の評価方法の根拠が(5.2.10で述べたように)まだ有効であれば、元の評価方法の識別子が使用されなければならない。しかし、根拠が重ね合わせの一部において変更された場合、関連するPPモジュール、PP構成又はPPで定義された別の識別子を使用しなければならない。ここでの意図は、論理的根拠が大幅に変更された場合、異なる識別子が使用されることを保証することである。

5.2.3 評価方法の責任を持つエンティティ

評価方法の定義には、その評価方法の定義及び維持管理に責任をもつエンティティを明記しなければならない。

例：責任を持つエンティティの例としては、評価機関、標準化団体、業界ワーキンググループ、又は技術コミュニティがある。

5.2.4 評価方法の適用範囲

評価方法の定義では、以下のような適用範囲を記述しなければならない。

a) 保証の目標を要約した簡潔な記述及びそれらが評価方法内の評価アクティビティによってどのように実行されるかの抽象度の高い記述の観点からの、評価方法の目的。

b) 評価方法の適用が意図されている評価コンテキスト。例えば、スマートカードやネットワーク機器などのTOE種別、又は、ある種のデータ伝送やデータ保存に適用されるある種のアルゴリズムやモードを用いた暗号機能などの機能種別について記述することができる。

c) 評価方法の既知の制限、又は評価方法が意図しない側面。

評価アクティビティは、1つ又は複数のSFRに限定して適用するように定義することができる。評価方法がこのようなSFRに限定した評価アクティビティを含む場合、評価範囲の項では、評価方法が定義される個々のSFRとSFRが定義されている場所(例えば、CCパート2やPPで定義されている拡張SFR)を識別しなければならない。CCパート2に定義されていない拡張SFRについては、異なる情報源で異なる内容のSFRを参照するために同じSFR名を使用できるため、場所の識別は特に重要である(評価方法がどのSFRにも特化していない場合、この項は必要ない)。

同様に、評価アクティビティは、1つ又は複数の拡張SAR(すなわち、CCパート3で定義されていないSAR)に限定して適用するように定義することができる。評価方法にそのような評価アクティビティが含まれる場合、適用範囲の項で関連する拡張SARとそれらが定義されている場所(例えばPP内)を識別しなければならない。拡張SFRと同様に、同じSAR名が異なる内容のSARを参照するために異なる情報源で使用されることがあるため、場所の識別は特に重要である(評価方法がいかなる拡張SARにも適用されない場合、この項は必要ない)。

注：評価方法の完全性の根拠(5.2.10参照)は、評価方法の適用範囲に関連する更なる情報を提供することができる。

5.2.5 依存性

評価方法の定義は、他の評価方法、評価アクティビティ又はCEMの一般的なアクションへの依存性を全て記述しなければならない。

例：CCパート3の他の開発者アクションエレメント又はCEMのアクションから得た情報に依存する評価方法。

依存性は、評価方法レベル、又は評価方法に含まれる個々の評価アクティビティレベルのいずれかで識別することができる。

5.2.6 開発者又は他のエンティティからの必要な入力

評価方法の定義では、評価アクティビティを実行するために必要な開発者の入力を識別しなければならない。これは、評価方法のレベルでも、評価方法に含まれる個々の評価アクティビティのレベルでもよい。入力の記述は、パート3(拡張SARを扱う場合は同等の一般的な定義)で定義された、評価アクティビティの派生元の一般的なSARの定義を参照することによっても行うことができる。

例：メディア暗号化TOEを扱う評価方法の入力には、鍵階層の特定の詳細の記述に関する要件を定義することができる。

5.2.7 必要なツールタイプ

評価アクティビティに何らかのツールタイプが必要な場合は、評価方法の定義の一部としてリストアップしなければならない。ツールタイプは、評価方法のレベル、又は、評価方法に含まれる個々の評価アクティビティのレベルで識別することができる。

5.2.8 必要な評価者の能力

評価方法は、その評価アクティビティに必要な特定の評価者の能力を識別することができる(参考文献[3]を参照)。特定の評価者の能力を識別する場合、評価方法のレベル、又は評価方法に含まれる個々の評価アクティビティのレベル(又はその両方の組み合わせ)のいずれかで行うことができる。

5.2.9 報告に関する要件

評価方法の記述には、報告要件についての記述を含めることができる。この記述は、評価方法のレベル、個々の評価アクティビティのレベル、又はその両方のレベルで行うことができる。

例1：評価方法レベルでは、一般的な報告要件を与えることができるが、評価アクティビティによっては、特定の所見、正当化、又は特定の質問に対する回答の記載を求めることもできる。

報告に関する要件は、CEMの評価報告書の要件、及び評価の実施に要求される他の標準と整合していなければならない。

例2：評価の実施に要求され得る他の標準の例は、ISO/IEC 17025である。

報告要件は、CEMに記述される評価報告書(ETR)に含まれる報告内容を規定することができるが、作成すべき他の報告書の内容も規定することができる。

例3：公開用と、より限定された配布用(例えば、開発者、評価者及び評価機関)に、別々の報告が定義されることがある。

このように複数の報告が定義されている場合、評価方法(個々の評価アクティビティに関するものを含む)の報告要件は、各報告書で報告されるべき側面を指定することができる。

評価方法が、その派生元のワークユニットで示された以外の報告又は報告の詳細を必要としない場合(又は、追加の報告要件が全て評価アクティビティに記載されている場合)、この節は必要ない。

5.2.10 評価方法の根拠

評価方法における評価アクティビティが、CEMの元のワークユニットから適切に導出されたことを示す根拠を示さなければならない(拡張SARの場合、CEMのワークユニットへの言及は、代わりに、拡張SARの関連する方法論の定義におけるワークユニットに適用される)。これは、評価方法のレベル、又は個々の評価アクティビティのレベルのいずれかで与えることができる。評価方法に含まれる評価アクティビティが6.2.10に従った個々の根拠を持たない場合、評価方法は、CEMのワークユニットから評価アクティビティを導出するための根拠を含まなければならない。その根拠は、特定の技術又はTOE種別の評価の範囲及び深さのために、なぜワークユニットが作り直されたかの説明を含めることができる。その根拠は、さらに、その評価アクティビティが、適用されるCCパート3のアクションエレメントの全ての側面にどのように対処するかを述べなければならない。また、評価方法の適用が意図されて

いる評価コンテキストに関して、アクションエレメント又はワークユニットに対処する方法が完全であることを正当化しなければならない。

評価アクティビティが拡張SARから派生した場合、その根拠は、評価アクティビティがその拡張SARのワークユニットの記述に対応することを正当化しなければならない(拡張コンポーネント定義の評価のためにCEMで定義された方法(CCパート3のAPE_ECD、ACE_ECD及びASE_ECDファミリ)は、ワークユニットを拡張SARの定義の一部として含むことを要求している)。

その根拠は、適切であれば、評価コンテキストに応じた特定の前提条件を識別することができる。

PPモジュールがPP構成の基本PPと共に使用される場合など、異なる要求の情報源が組み合わされる場合、各情報源の評価アクティビティ(例えば、各基本PP/PPモジュールの評価アクティビティ及びPP構成の各コンポーネントの評価アクティビティ)は、組み合わされて結果のTOE全体に適用される。組み合わせの一部として、評価方法は他の評価方法と重ね合わせることができる。ただし、重ね合わせによる変更については、結果として得られる評価方法の根拠の正当性を示す必要がある。重ね合わせは、異なる情報源からの複数の評価アクティビティの範囲が同じである場合に存在する(この例では、基本PPとPPモジュールを用いているが、パッケージがPPで使用され、PPに対して定義されたより具体的な評価方法がパッケージに対して定義された一般的な評価方法に重なる場合など、他の場合もあり得る)。

注：評価アクティビティは、デフォルトではTOE全体に適用されるが、評価方法又は評価アクティビティの定義により、その適用に制限を設けることができる。例えば、特定のセキュアチャネルプロトコルのコンテキストで使用される暗号操作に特化した評価アクティビティを定義することができる：このような評価アクティビティは、保存データの保護というコンテキストで使用される同じ暗号操作には適用されない。

例：ネットワーク機器TOEの基本PPには、TOEがサポートする一般的なセキュアチャネルの評価アクティビティを含む評価方法を定義することが可能である。PPモジュールは、特定のセキュアチャネルタイプを使用したネットワーク機器の特定のリモート管理操作について定義することができる(例えば、特定の操作や特定のプロトコルを指定する)。そして、PPモジュールの評価アクティビティは、基本PPの評価方法を重ね合わせる。つまり、PPモジュールの評価アクティビティは、PPモジュールでカバーされる特定のリモート管理アクティビティに関する基本PPの評価アクティビティを置き換える(他のセキュアチャネル機能は、依然として基本PPの評価方法の評価アクティビティの対象となる)。

重ね合わせの効果は、基礎となる評価方法に以下のような1つ以上の変更を加えることである。

a) 基礎となる評価アクティビティを削除できる。通常、これは、評価アクティビティがもはや関連しないためである(例えば、基本PPのSFRで利用可能な選択値のいくつかがPPモジュールによって削除される場合など)。

b) 基礎となる評価アクティビティを、より具体的な詳細を追加することによって詳細化できる(アクティビティをより厳しくすることができる)。通常、これは、評価コンテキストに追加の詳細を反映するためである(例えば、機能パッケージによってPPのコンテキストに詳細が追加される場合など)。

c) 追加の評価アクティビティが定義される。通常、これは、追加の評価コンテキストを反映する(例えば、機能パッケージによってPPのコンテキストに追加された詳細、又はPP構成に追加されたSARなど)。

特殊なケースとして、関連するSARの追加に対応して、基礎となる評価アクティビティが変更される場合がある。通常、これは、PP構成において既存のSARを階層的に上位のSARで置換することを反映する。このような場合、階層化SARの新しい内容に応じて、b)のように詳細を追加し、c)のように評価アクティビティを追加する組み合わせが可能である。

結果として得られる評価方法の根拠は、元の評価方法の根拠で重ね合わせに対して既に行われた考慮に基づいてもよいし(すなわち、重ね合わせの根拠が元の評価方法の定義に既に含まれている場合)、(例えば、PPモジュールの)より具体的な評価方法が、(例えば、基本PPの)元の評価方法への影響を扱う別の根拠を含んでいてもよい。重ね合わせる評価方法(例えば、PPモジュール)が別の根拠を含む場合、これは、結合された部分が使用されるコンテキストを考慮し、結果として得られる評価方法が重ね合わせられた評価方法の関連する側面を保持することを示すものでなければならない。PPを組み合わせて使用する場合も、同じ原則が適用される：元の評価方法が、適用されるコンテキストに応じて許容される変化を記述するか、あるいは、結果として生じる重ね合わせ評価方法が元の評価方法への影響を扱うかである。

評価アクティビティを重ね合わせる根拠は、独立した節であってもよいし、CCパート1に記述されている保証根拠又はセキュリティ要件根拠の一部として含まれていてもよい。

5.2.11 動詞の追加定義

上記4.3で述べたように、評価アクティビティの仕様には、CCパート1で定義されたものに加えて別の動詞を使用することができるが、そのような別の動詞は、評価アクティビティを含む評価方法の一部として定義し、(単なるチェックではなく)評価者の判断がどの程度関与するかを明確にしなければならない。

5.2.12 評価アクティビティのセット

評価方法に含まれる評価アクティビティは、6章に定義された構造を用いて定義されなければならない。

6 評価アクティビティの構造

6.1 概要

個々の評価アクティビティのレベルでは、評価アクティビティが明確な目的、明確な合格/不合格の基準(必要な場合)、及び他の評価アクティビティとの依存性が識別されていることを確認することに重点が置かれている。これは、評価の理解、ひいては各評価におけるアクティビティの一貫した適用を支援することを意図している。

5.2で述べ、表1に要約されているように、評価アクティビティで規定すべき内容は、評価方法レベル、又は個々の評価アクティビティレベルのいずれかに含めることができる。

評価アクティビティの内容は、例えば、テストや分析アクティビティ(例えば、利用者文書にプロトコルで使用するための認証情報の安全な生成が記述されていることを確認する)の短い説明文だけで構成される形式など、様々な形式で提供できることを意図している。さらに、いくつかの評価アクティビティをグループ化し、個々の評価アクティビティで繰り返すのではなく、グループ全体としてコンテンツ要素を記述することができる。評価アクティビティの各内容エレメントは、6.2.1～6.2.10でより詳細に記述され、各エレメントの必須及び任意の状態の概要は、表1に要約されている。

6.2 評価アクティビティの仕様

6.2.1 評価アクティビティの一意の識別

評価アクティビティは、その原文書内で一意に識別されなければならない。また、原文書自体も一意に識別されなければならない。評価アクティビティが評価方法にグループ化されている場合は、評価方法全体の識別子に加えて、個々の評価アクティビティの識別子を定義する(5.2.2参照)。

6.2.2 評価アクティビティの目的

評価アクティビティを実施する目的を記載しなければならない。これは、6.2.3で述べたSFRとSAR、及び6.2.8の合格/不合格の基準を参照して記載してもよいが、目的の記載は、評価者が特定のTOEに合わせて評価アクティビティを変える際の柔軟性と制限を理解する上で、重要である。

6.2.3 評価アクティビティとSFR、SAR、及び他の評価アクティビティとの関連性

評価アクティビティが特定のSFR(おそらく、パッケージ、PP、PPモジュールなどの他の文書に含まれるSFRの特定のインスタンス)に関連する場合は、評価アクティビティ定義の一部として識別しなければならない。

例：評価アクティビティは、適合するSTで使用できる許容値を制限する割付の部分的な完了をもって、特定のPPに記載されたSFRと関連付けることができる。

同様に、特定のSARとの関係も識別されなければならない(これは、関係性について示すべき追加情報がない限り、元のSARのワークユニットから導出した根拠(5.2.10及び6.2.10参照)を通じて達成されるかもしれない)。

評価アクティビティが他の評価アクティビティの完了に依存する場合、依存する評価アクティビティの定義の一部として、依存性及び他の評価アクティビティを識別しなければならない(依存性は、評価方法又は個々の評価アクティビティのいずれかのレベルで識別することができる)。

6.2.4 開発者又は他のエンティティからの必要な入力

5.2.6で述べたように、評価アクティビティへの入力の要求形式と内容に関して、追加の詳細を規定することができる。この追加の詳細は、一般的に評価アクティビティとその合格/不合格の基準の正確な仕様をサポートするために使用される(これは、評価方法のレベル、又は個々の評価アクティビティのレベルのいずれかで行うことができる)。

評価アクティビティが、その派生元のワークユニットで定義されたもの以外の入力を必要としない場合、この節は必要ない。

6.2.5 必要なツールタイプ

評価アクティビティの実行で、そのアクティビティを完了するために、何らかのツールタイプが必要な場合、これらのツールタイプは、評価アクティビティの定義の一部として定義されなければならない。ツールタイプの定義には、評価アクティビティの記述とその合格/不合格の基準に関して評価アクティビティを一貫して実施できるように、その種類のツールを入手又は再現できるように十分な詳細を含まなければならない(これは、評価方法のレベル、又は個々の評価アクティビティのレベルのいずれかで行うことができる)。

評価アクティビティが、その派生元のワークユニットで与えられている、又は暗示されているもの以外の特定のツールタイプを必要としない場合、この節は必要ない。

6.2.6 必要な評価者の能力

5.2.8で述べたように、評価方法は、その評価アクティビティに必要な特定の評価者の能力を識別することができる(参考文献[3]を参照)。特定の評価者の能力を識別する場合、評価方法のレベル、又は評価方法に含まれる個々の評価アクティビティのレベル(又はその両方の組み合わせ)のいずれかで行うことができる。

6.2.7 評定戦略

評価アクティビティのこの節は、アクティビティの実行方法に関するガイダンスと詳細を提供しなければならない。評価アクティビティの内容に応じて、以下の内容が含まれる。

a) 開発者又は他のエンティティからの入力が、評価アクティビティに関して完全であることをどのように評価するか。

b) 必要とされるツールタイプの利用方法(ツールの校正やセットアップのためのガイダンスを含む可能性がある)。

c) アクティビティの実行手順に関するガイダンス。

ほとんどの評価アクティビティでは、技術に応じた適応の余地を残すことが重要である。評定戦略の正確な指定と、そのような適応に許容される余地との間の適切なバランスを見つけることは、一方では客観的で再現性のある結果を保証し、他方では意味のある結果を保証するために重要である。開発者が機能要件をどのように実装するかについてより柔軟性がある場合、評価アクティビティの定義には、異なる潜在的な実装に評価を適応させるためのより多くの余地が必要である。このような場合、評価者が行うべきアクションの詳細を規定するのではなく、TOEに特化した改良と適応をどのように行うかについての一般的なガイダンスを評定戦略で提供するべきである。一般に、評価アクティビティからの逸脱/詳細化(つまり、評価アクティビティで要求される事項の省略)は認められない。

評定戦略は、評価者が実行しなければならない複数のステージから構成されることがあり、その場合、それらのステージは、各ステージの期待される結果とともに指定されなければな

らない。ステージによっては、前のステージの結果に依存する場合があり、この場合、評定戦略は、ステージの1つが期待される結果を生成しない場合に評価者が何をする必要があるかについても定義しなければならない。このような場合の例としては、入力を修正して前のステージに戻る、アクティビティの結果として何を文書化するかを示して評価アクティビティを終了する、又は別のステージを継続する、などが挙げられる。

評価コンテキストのニーズと評価アクティビティ自体の性質に応じて、評定戦略は簡潔で、評価アクティビティの一般的な記述の一部を形成することができる(例えば、特定のテスト又は分析アクションを実行する方法の記述)。

6.2.8 合格/不合格の基準

評価アクティビティのこの節では、評価者が、評価アクティビティによってTOEが関連要件を満たしていることが実証されたか、又は関連要件を満たしていないことを決定するために使用する基準を定義することができる。場合によっては、評価アクティビティの派生元のワークユニットの記述に依拠することが適切であるが、他の場合には、評価アクティビティの作成者が、より具体的な基準を記述することが必要又は有益であると判断することができる。最終的に、合格/不合格の基準は、評価アクティビティに示された目的(6.2.2参照)が達成されたかどうかを決定することに関係する。評価アクティビティが個別の合格/不合格の基準を義務付けている場合、これらの基準は、異なる評価において評価アクティビティを実施した結果の一貫性を最大化するものでなければならない。このように具体的な基準を明示することで、同じ証拠があったとしても、異なる評価者がその評価アクティビティに対して異なる結論に達する可能性を最小限にすることができる。したがって、一般的には、合格/不合格の基準はできるだけ具体的にするべきである。

文書を分析するための特定の合格/不合格の基準を達成する方法には、例えば通信スタックの詳細構成の有無や実行環境の失敗トリガーのセットなど、特定の機能の有無の観点から基準を表現することや、特定の「クローズド」質問に対する「はい/いいえ」の回答(おそらく他の「オープン」質問に対して得られた回答でサポートされる)の観点から表現することが含まれる。

テストのための特定の合格/不合格の基準を達成する方法は、チャネル上で成功した通信を観察する、又はチャネルのセットアップが失敗したことを示すエラーメッセージを受け取る、又はメモリアクセス/設定を観察するなど、特定の目に見える結果の観点から基準を表現することである。「TOEがデータを削除する」という表現は、評価者がこの削除をどのように決定するかが明確でないため、一般に合格/不合格の基準としては不適切である。より適切な表現は、「TOEが"ファイルが見つかりません"というエラーを返す」又は「評価者が<名前付きインタフェース呼び出し>を使って、返ってきたファイルリストにファイルが存在しないことを確認する」であろう。評価アクティビティに対する特定の合格/不合格の基準を表現する別の方法として、識別された標準の特定の条項への適合性を決定する観点、又はCEMの攻撃能力モデルやいくつかのIT製品タイプに対して定義された特定の攻撃能力モデルのような参照モデル又は事例のセットとの比較を行う観点が考えられる。

しかし、一般的に基準は、異なるTOE間の実装の詳細の差異を許容する必要があることも認識されている。したがって、合格/不合格の基準は、評価アクティビティに定義された目的の観点から記述することもできる(6.2.2参照)。

評価アクティビティが、その派生元のワークユニットで与えられたもの以外の合格/不合格の基準を必要としない場合は、この節は必要ない。

6.2.9 報告に関する要件

5.2.9で述べたように、評価アクティビティでは、報告に関する特定の要件(ETR及び場合によっては他のアウトプット)を規定することができる。この要件は、評価方法レベル、又は個々の評価アクティビティレベルで規定することができる。このレベルでは、報告に関する要件は、一般に、特定の質問に対する回答、結論の根拠、又は特定の試験の結果の明確な記述を文書化することによって、合格/不合格の基準の可視性及び再現性を支援することを意図しているであろう。特に、合格/不合格の基準が評価者の判断を必要とすると考えられる場合、報告の要件には、判断を下すことや合格・不合格の結論に達することに関与するために定義された特定の要因の記録が含まれていなければならない。

評価アクティビティが、その派生元のワークユニットに記載されている以外の報告又は報告の詳細を必要としない場合、この節は必要ない。

6.2.10 評価アクティビティの根拠

評価アクティビティは、CEM(又は拡張SARの場合は同等のワークユニット定義)の1つ以上のワークユニットからの導出に関する正当化を含まなければならない。その正当化には、特定の技術又はTOE種類の評価の範囲及び深さのために、なぜワークユニットを作り直さなければならなかったかの説明が含まれる場合がある。評価方法(5.2.10参照)及び評価アクティビティレベルの根拠を組み合わせることで、評価方法が適用されるCCパート3のアクションエレメントの全ての側面に対処していることを正当化しなければならない。さらに、組み合わせた根拠は、元のアクションエレメント又はワークユニットからの導出が、評価アクティビティの適用が意図されている評価コンテキストに関して、評価アクティビティが完全であることをどのように保証するかを記述しなければならない。

注：根拠は、ある側面がその特定の評価コンテキストに適用できないことを識別し、正当化することができる。

評価アクティビティが、その派生元のワークユニットとは異なる合格/不合格の基準を定義する場合、その正当化は、新しい基準の実行可能性と有効性の理由を提供しなければならない。

根拠は、適切であれば、評価コンテキストに対してなされる特定の前提条件を識別してもよい。

根拠は、評価方法又は個々の評価アクティビティのいずれのレベルで与えられてもよい。

参考文献

[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、CC:2022、改訂第1版、2022年11月 — パート5：セキュリティ要件の定義済みパッケージ*

[2] ISO/IEC 17025、*試験所及び校正機関の能力に関する一般要求事項*

[3] ISO/IEC 19896-3, *IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators*