

参考資料



情報技術セキュリティのための 共通評価方法論

CEM-97/017

パート 1： 概説と一般モデル

バージョン 0.6

97/01/11

平成 15 年 8 月翻訳第 1.1 版
情報処理振興事業協会
セキュリティセンター

IPA まえがき

本書の目的

本書は、情報技術セキュリティ評価のためのコモンクライテリアを基にした評価に関するガイドである「Common Methodology for Information Technology Security Evaluation (CEM)」を日本語訳したものである。本書は、情報処理振興事業協会(略称 IPA)において、セキュリティ評価のための補助資料として作成されたものである。したがって、本翻訳書は、セキュリティ評価方法の基準書ではないが、情報セキュリティに関心をもつ人にとって、CC、CEM を理解するための参考資料として役立つことも期待している。

使用上の注意

本書は、用語、記述内容等に不備がある可能性がある。疑問点については下記に記載した CEM で確認していただきたい。本書は、参照利用されることのみを目的とし、本書の改変、及び他への転載は禁止する。

(本翻訳文書は、青で示される変更を一部行っている。)

参考文献

Common Methodology for Information Technology Security Evaluation (CEM)

Part1: Introduction and general model Version 0.6 97/01/11 CEM-97/017

Part2: Evaluation Methodology Version 1.0 August 1999 CEM-99/045

掲載ホームページアドレス <http://csrc.nist.gov/cc/cem/cemlist.htm>

Common Criteria for Information Technology Security Evaluation (CC)

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

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

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

掲載ホームページアドレス <http://csrc.nist.gov/cc/ccv20/ccv2list.htm>

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 2.1

パート1：概説と一般モデル 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

パート2：セキュリティ機能要件 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

パート3：セキュリティ保証要件 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

著作権について

本書がベースにしている CEM の著作権は、以下に示す 7 つの政府機関 (“the Common Criteria Project Sponsoring Organizations” と総称) が有している。したがって、CEM の使用、複製、配布、及び改変の権利は、the Common Criteria Project Sponsoring Organizations にある。情報処理振興事業協会は、CEM を日本語翻訳し、参照利用のみを目的として公開することを、the Common Criteria Project Sponsoring Organizations より許可された。

The Common Criteria Project Sponsoring Organizations:

- Canada: Communications Security Establishment
- France: Service Central de la Securite des Systemes d'Information
- Germany: Bundesamt fur Sicherheit in der Informationstechnik
- Netherlands: Netherlands National Communications Security Agency
- United Kingdom: Communications-Electronics Security Group
- United States: National Institute of Standards and Technology
- United States: National Security Agency

まえがき

情報技術セキュリティ評価のコモンクライテリア(Common Criteria)バージョン 1.0 の出版物に従い、本書は、コモンクライテリアを提供するために必要となる、共通評価方法論(Common Evaluation Methodology)の最初の原則とモデルを提供する。

本書は、国際的なセキュリティコミュニティでレビューするために発行される。受け取ったコメントはすべて、共通評価方法論の今後の開発のために考慮される。

あらゆるオブザベーション報告書は、CEM の連絡先 (cem@cse.dnd.ca) または以下に示す 1 つまたはいくつかのスポンサー組織の連絡先へ、本書の附属書 B に含まれているオブザベーションを報告するためのテンプレートを使用して提出されるべきである。

National Institute of Standards and Technology
Computer Security Division
NIST North Building, Room 426
Gaithersburg, Maryland 20899
U.S.A.
Tel: (+1)(301)975-2934, Fax: (+1)(301)926-2733
E-mail:csd@nist.gov
<http://csrc.nsl.nist.gov>

Communications Security Establishment
Criteria Coordinator
R2B IT Security Standards and Initiatives
P.O. Box 9703, Terminal
Ottawa, Canada K1G 3Z4
Tel:(+1)(613)991-7409, Fax: (+1)(613)991-7411
E-mail:criteria@cse.dnd.ca
<ftp:ftp.cse.dnd.ca>
<http://www.cse.dnd.ca>

Bundesamt für Sicherheit in der Informationstechnik
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: (+49)228 9582 300, Fax: (+49)228 9582 427
E-mail:cc@bsi.de

Netherlands National Communications Security Agency
P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel: (+31) 70 3485637, Fax: (+31).70.3486503
E-mail:criteria@nlncsa.minbuza.nl

National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 21122
U.S.A.
Tel: (+1)(410)859-4458, Fax: (+1)(410)684-7512
E-mail:common_criteria@radium.ncsc.mil

UK IT Security and Certification Scheme
Senior Executive
P.O. Box 152
Cheltenham GL52 5UF
United Kingdom
Tel: (+44) 1242 235739, Fax: (+44)1242 235233
E-mail: ccv1.0@itsec.gov.uk
[ftp: ftp.itsec.gov.uk](ftp:ftp.itsec.gov.uk)
<http://www.itsec.gov.uk>

Service Central de la Sécurité des Systèmes d'Information
Bureau Normalisation, Critères Communs
18 rue du docteur Zamenhof
92131 Issy les Moulineaux
France
Tel: (+33)(1)41463784, Fax: (+33)(1)41463701
E-mail:106174.1363@compuserve.com

本書には、i から iv、及び 1 から 23 までのページ数が付けられている。

D R A F T

目次

1章 序説	1
1.1 目的.....	1
1.2 対象読者.....	1
1.3 関係する当事者及び予想される利益.....	1
1.4 有効範囲.....	2
1.5 文書の構成.....	3
1.6 文書の表記規則及び用語.....	4
2章 評価の普遍的原則	5
2.1 普遍的原則のステートメント及び説明.....	5
2.1.1 適切性.....	5
2.1.2 不偏性.....	5
2.1.3 客観性.....	5
2.1.4 反復性及び再現性.....	5
2.1.5 結果の妥当性.....	6
2.2 想定.....	6
2.2.1 費用効果.....	6
2.2.2 方法論の発展.....	6
2.2.3 再使用可能性.....	6
2.2.4 用語.....	6
3章 一般モデル	7
3.1 役割の責任.....	7
3.1.1 スポンサー.....	7
3.1.2 開発者.....	7
3.1.3 評価者.....	7
3.1.4 監督者.....	8
3.1.5 役割の関係.....	8
3.2 評価プロセスの概要.....	10
3.2.1 準備.....	10
3.2.2 実行.....	12
3.2.3 結論.....	14
附属書 A 用語集	17
A.1 省略語及び頭字語.....	17
A.2 用語.....	17
A.3 参照資料.....	20
附属書 B CEM オブザベーション報告書 (CEMOR)	21
B.1 序説.....	21

目次

D R A F T

B.2	CEMOR の転送	21
B.3	CEMOR のフォーマット.....	21
B.3.1	オブザベーションの例.....	22

D R A F T

図一覧

図 1.1 セキュリティ評価の主要当事者 2

図 1.2 評価の枠組 3

図 3.1 役割の責任と関係 9

図 3.2 準備段階 11

図 3.3 実行段階 13

図 3.4 結論段階 15

D R A F T

表一覧

表 3.1 個々の評価の間に役割間で適切でない者 9

1 章 序説

1.1 目的

- 1 この文書、共通評価方法論（CEM）は、コモンクライテリア（CC, [CCREF]）を適用する評価を行うために合意された方法論を開発するために準備されている。CEM は、セキュリティ評価の相互承認をサポートする¹。

1.2 対象読者

- 2 CEM は、主に評価者を対象にしている。ただし、開発者、スポンサー、監督者、及び評価結果の公表と使用に関係する当事者など、他の当事者も CEM から役立つ情報を得ることができる。

編集者の注記： CEMEB は、用語「監督者」(Overseer) が最適な呼称でないことを認識している。より良い言葉が提案されることを期待している。

1.3 関係する当事者及び予想される利益

- 3 **プロテクションプロファイル（PP）**の開発者（作成者）は、情報技術（IT）製品の利用者代表のグループまたはベンダーであることが多い。PP 評価は一貫して行われ、PP が独立に正当性を確認されるので、PP 開発者は CEM の適用から利益を得る。
- 4 **評価対象（TOE）**開発者は、IT 製品ベンダー、IT 製品をシステムに組み込むシステムインテグレータ、または IT ソリューションを作り出すその他の形の組織エンティティである。TOE 開発者は、CEM の適用から次のような利益を得る。
 - a) PP 及び**セキュリティターゲット（ST）**に記載されているセキュリティ特性が独立に正当性を確認され、検証されている。
 - b) 開発者の顧客は、TOE が主張されるセキュリティ特性を提供することをさらに容易に確信する。
 - c) 評価済み製品は、セキュアなシステムを構成するためにさらに効果的に使用される。
 - d) CEM は、費用効果の高い、迅速な評価に貢献する
- 5 評価のスポンサーは、評価を委託する組織エンティティである。スポンサーは、開発者（例えば、ベンダーまたはインテグレータ）または購入者（例えば、利用者、委託者、システム管理人、システムセキュリティオフィサ）のいずれでもかまわな

¹ 用語の定義は、初めて使用されるときにボールド活字で示されている用語に対して、附属書 A に示されている。

D R A F T

い。TOE のセキュリティ特性が証拠資料を提出され、そして独立に正当性を確認し検証されて、TOE 群の間を比較することが可能になったので、スポンサーは CEM の適用から利益を得る。

6 評価者は、CEM に従って CC を適用する。CC の一貫性のある適用についての具体的なガイダンスを提供するので、評価者は CEM から利益を得る。

7 監督者は、**評価プロセス**が CC と CEM に従って行われていることを保証するエンティティである。CEM は、評価者が提供する必要がある情報の一貫性のあるセットを定義するので、監督者は CEM から利益を得る。

8 図 1.1 は、セキュリティ評価プロセスの主要当事者を示している。CEM が相互承認をサポートするので、すべての当事者は CEM から利益を得る。

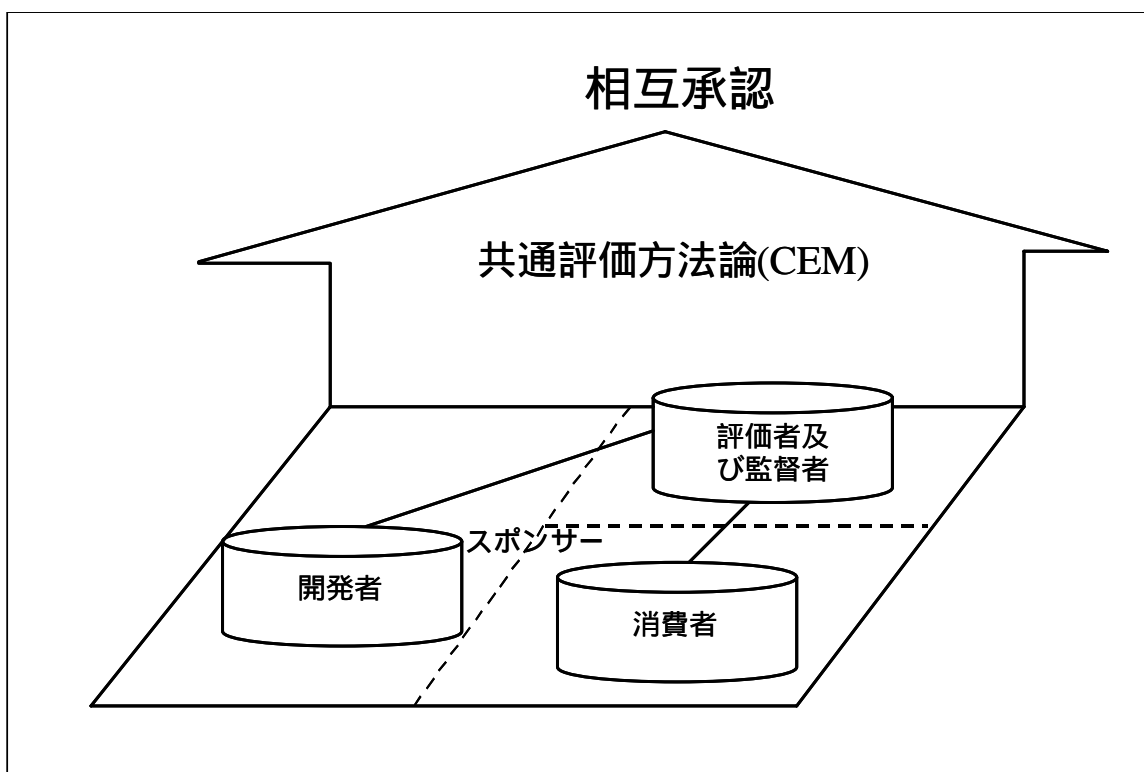


図 1.1 セキュリティ評価の主要当事者

1.4 有効範囲

9 評価プロセスは、評価方法論に準拠するために必要な開発プロセスと監督プロセスのアクションとともに評価中に行われるアクションからなる。開発と監督のプロセスには、評価プロセスと CEM の両方の有効範囲外のアクションが存在する。図 1.2 は、この文書で取り扱う評価の枠組みの有効範囲を示している。

D R A F T

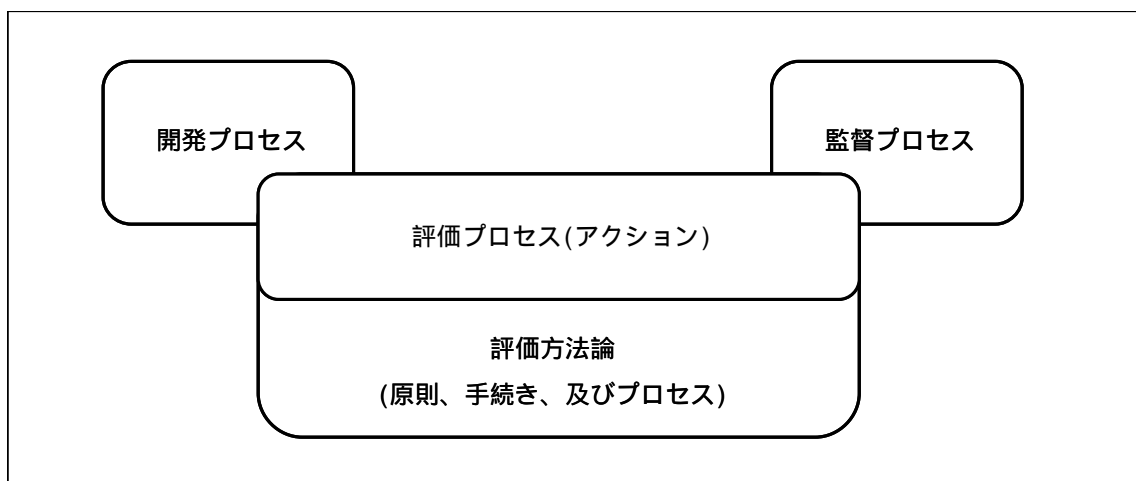


図 1.2 評価の枠組

- 10 この文書は、IT セキュリティ評価に適用される原則、手続き及びプロセス（アクション）を取り扱う。これらの規則の国または地域での実装（例えば、**制度**）は取り扱わない。

1.5 文書の構成

- 11 この文書は、3つのパートから構成されている。このパート、パート1は、評価の原則及び一般的モデルについて説明している。目的は、評価の側面が CEM で完全に取り扱われていない場合、評価の原則への参照は、一連のアクションを決定する上での価値あるガイダンスを提供するべきである。
- 12 この方法論を採用する制度には、パート2の規範的エレメントの実装を実施することが求められる。制度の実装は、パート1に記述されている評価の普遍的な原則に対して維持される必要がある。
- 13 パート2では、CCのパート3によって委任されたアクションを詳細化することにより、評価プロセスを記述している。関係する異なる当事者のアクティビティを取り扱うとともに、評価プロセスの記述は、評価方法論に準拠するために開発プロセス及び監視プロセス中に行う必要があるアクションを記述する。
- 14 パート3では、評価結果を完全に使用するための評価方法論の拡張を記述している。例えば、パート3には、**評価用提供物件**の内容及び要件定義に対するガイダンスが含まれている。

訳者の注記： CEM パート3は、未発行である。(2001年2月現在)

1.6 文書の表記規則及び用語

15 このパートの附属書 A.1 に示されている省略語及び頭字語は、初出時に説明されている。テキストの節と図は、必要に応じて参照されている。他の文書の参照は、参照されている資料を識別するための省略語を使用して行われている。完全な参照リストは、このパートの附属書 A.3 に示されている。

16 用語の定義は、本書での初出時に、ボールド活字で示されている。このパートの附属書 A.2 に記載されている用語の定義は、本書で特別な方法で使用されている用語に対してだけ行われている。大部分の用語は、それらの受け入れられている定義に従って使用されている。

17 動詞の形「しなければならない」(*shall*) 及び「してはならない」(*shall not*) は、CEM に準拠するために厳格に従ねばならない要件を示すために使用される。

18 動詞の形「ねばならない」(*must*) 及び「してはいけない」(*must not*) は、要件の中で避けることができない状況を記述するために使用される。

19 動詞の形「すべきである」(*should*) 及び「する」(*will*) は、いくつかの可能性の中で他に言及することなくまたは他を排除することなく、特に適切であるとして 1 つを推奨すること、またはある一連のアクションが好ましいが、必ずしも必要ではないこと、または(否定形「すべきでない」(*should not*) において) ある種の可能性または一連のアクションが問題視されるが、CEM では禁止されていないことを示すために使用される。

20 動詞の形「することができる」(*may*) 及び「する必要がない」(*need not*) は、CEM の制限内で許される一連のアクションを示すために使用される。動詞の形「できる」(*can*) 及び「できない」(*cannot*) は、有形的、物理的、または原因的な可能性と能力の CEM のステートメントに使用される。

2 章 評価の普適的原則

21 評価の普適的原則が、この章で説明されている。これらの原則は、評価のための基礎である。原則を実施するのは、評価方法論だけではない。評価に関係する当事者及びこの方法論の適用を管理する制度についての想定もまた、原則の実施に貢献せねばならない。

2.1 普適的原則のステートメント及び説明

22 この節では、評価の普適的原則について説明する。各サブセクションで原則について述べ、その後に簡単な説明が続く。

2.1.1 適切性

23 原則：意図する保証レベルを達成するために採用する評価アクティビティは、*適切でなければならない*。

24 評価に関係する当事者はすべて、目標の**評価保証レベル**（EAL）のガイダンス及び要件に一致する厳格度で、それぞれの必要なタスクを実行しなければならない。

2.1.2 不偏性

25 原則：すべての評価は、*偏りから開放されていないなければならない*。

26 評価に関係する当事者はいずれも、評価されている評価対象（TOE）またはプロテクションプロファイル（PP）に対する肯定的/否定的な先入観を持つてはならない。適切な技術的監督は、利害の対立を取り除く制度とともに、残っている先入観をごくわずかなレベルにまで減らすべきである。相互承認と制度は、受け入れ不可能な利害の対立の概念を詳細に指摘せねばならない。

2.1.3 客観性

27 原則：評価結果は、最小限の主観的判断または意見で*得なければならない*。

28 個人は、意見または判断から完全に開放されることはできない。明確に定義された方法論と**解釈**に基づく適切な技術的監督は、意見と判断を受け入れ可能なレベルへ減少させるべきである。

2.1.4 反復性及び再現性

29 原則：同じ**評価証拠**による同じ要件に対する同じ TOE または PP の繰り返される評価は、*同じ結果をもたらさなければならない*。

30 各**評価者アクションエレメント**の結果は、誰が評価を行うかに関係なく、同じ結果をもたらすべきである。要件は、評価の間で一貫した方法で解釈されるべきである。再現性は、反復性と異なる。前者は、評価者間の一貫性に関するものであり、後者は、同じ評価者による結果の一貫性に関するものである。

2.1.5 結果の妥当性

31 原則：評価の結果は、完全で、技術的に正しくなければならない。

32 評価の出力は、TOE または PP の優れた判断と正確な技術的評価を示さなければならない。評価のプロセスと結果は、CC、CEM 及び制度の要件が満たされていることを保証するために、技術的監督を受けるべきである。

2.2 想定

33 普遍的原則には、評価の環境及び関係するすべての当事者のアクティビティについて多くの想定がなされている。原則は、これらの想定の有効性に依存する。

2.2.1 費用効果

34 想定：評価の価値は、関係する当事者が費やす時間、資源、及び資金を相殺するべきである。

35 TOE 及び PP の評価の価値と、時間と資源の消費の間の均衡を常にとらねばならない。

2.2.2 方法論の発展

36 想定：評価での環境的及び技術的要因の変更の影響は、十分に考慮された一貫性のある方法で評価方法論に反映されるべきである。

37 環境の変化と新しい技術は、TOE または PP を評価するために使用する技法の有効性に影響することがある。さらに、評価方法論は、環境を考慮するべきであるとともに、評価された TOE または PP の目的に合致していることを保証するために、新しい技術に適用されねばならない。

2.2.3 再使用可能性

38 想定：評価では、これまでの評価結果を効果的に使用すべきである。

39 TOE または PP の評価結果及び評価の途中で生じる解釈は、同じ条件が適用される場合、その後の評価で役に立つ。再使用可能性は、評価された TOE または PP が他の TOE または PP に組み入れられる場合、特に役に立つ。評価結果及び評価方法論の内容と構造は、再使用可能性をサポートすべきである。

2.2.4 用語

40 想定：共通の標準名称を評価に関係するすべての当事者が使用すべきである。

41 評価結果の一貫性のある技術的品質を保証し、評価の間での理解とコミュニケーションの一貫性のある理解を提供するために、すべての関係する当事者は、共通の標準名称、及び用語が実際に意味することについての共通の理解を共有せねばならない。

3章 一般モデル

42 この章は、方法論の一般モデルを示し、次のものを識別している。

- a) 評価プロセスに関する当事者の役割と責任
- b) 評価結果の上位レベル特性を含む上位レベル評価プロセス

43 一般モデルは、特定の制度を規定しないが、それには、すべての制度が評価の相互承認を満たすために準拠しなければならない要件が含まれるべきである。

3.1 役割の責任

44 一般モデルは、次の役割を定義する：スポンサー、開発者、評価者、及び監督者。各役割は、方法論に識別されている責任を持つ。一般モデルは、普遍的原則、特に不偏の普遍的原則に忠実に従って、組織または他のエンティティが1つまたは複数の役割を果たすことを排除しない。制度は、国の法律及び規制の遵守を保証するために、追加の要件を課すことがある。

3.1.1 スポンサー

45 スポンサーの責任には、次のものが含まれる。

- a) 評価に必要な合意の確立（例えば、評価の委託）
- b) 評価者に評価用提供物件（例えば、評価証拠、トレーニング、及びサポート）が提供されることの保証

3.1.2 開発者

46 開発者の責任には、次のものが含まれる。

- a) 評価のサポート
- b) 評価証拠の開発及び維持

3.1.3 評価者

47 評価者の責任には、次のものが含まれる。

- a) 評価証拠（例えば、証拠資料、PP、ST、TOEのコピー）の受取り
- b) CCが要求する評価者アクションの実行
- c) 必要に応じた、評価サポートの要求及び受取り（開発者によるトレーニング、監督者による解釈）
- d) **監督用提供物件の提供**

- e) 監督者への**総合判定**及び**中間判定**の証拠資料の提出及び正当化の提示
- f) 普遍的原則及び適切な制度への準拠

3.1.4 監督者

48 監督者の責任には、次のものが含まれる。

- a) 制度が必要とする評価の監視
- b) 監督用提供物件の受取り及びレビュー
- c) 評価が普遍的原則に従い、CEM を履行していることを保証する条件の作成
- d) 制度及び基準の解釈及びガイダンスを提供することによる評価のサポート
- e) 総合判定の承認または不承認
- f) 評価監督機関に対する**監督判定**の証拠資料の提出及び正当化の提示

3.1.5 役割の関係

49 この節には、役割の間関係を記述している図と表が含まれている。図 3.1 は、それぞれの役割の責任及びこれらの役割の間関係を要約している。

50 表 3.1 は、個々の評価への適切でない者の観点からの役割の必要な分離を記述している。適切でない者は、個々の評価に役割を果たす個人による普遍的原則の違反と定義されている。行と列の交点の「No」は、その行の役割がその列の役割に適切でない者として許されていないことを示している。

D R A F T

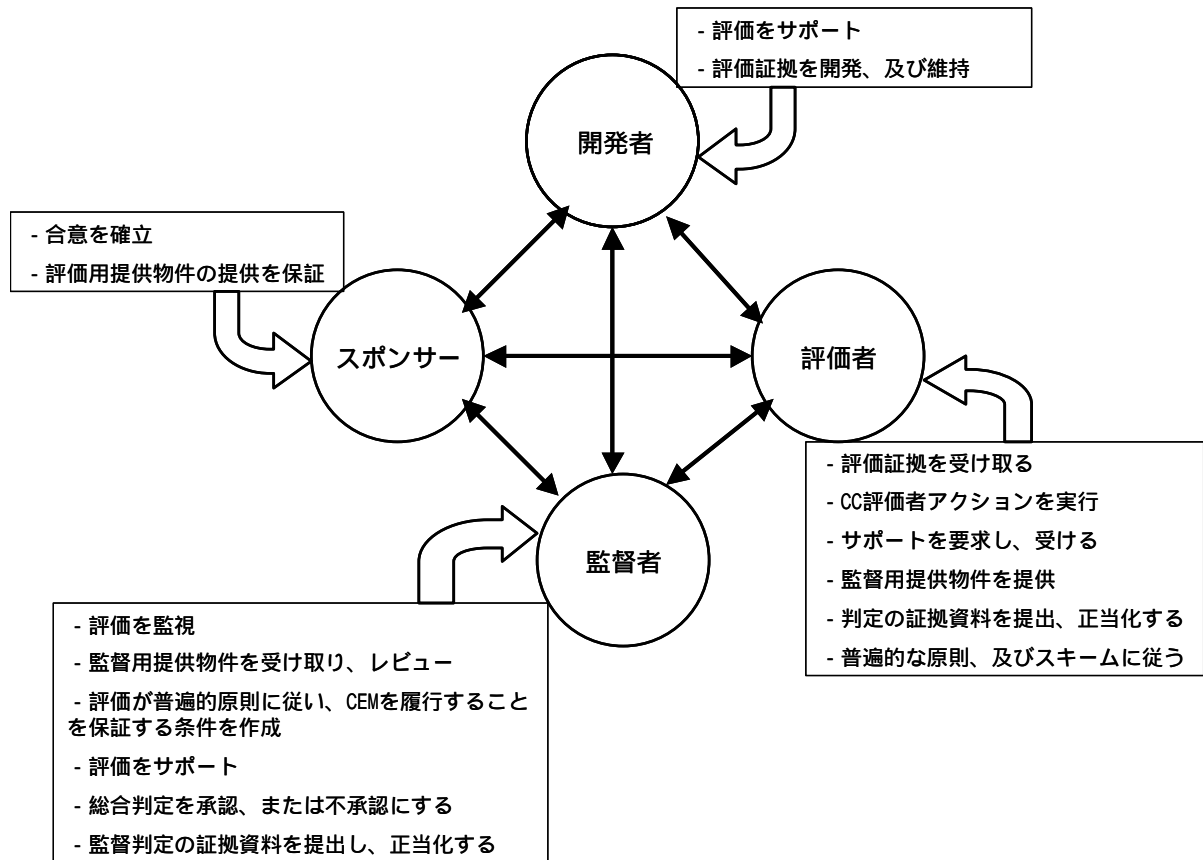


図 3.1 役割の責任と関係

表 3.1 個々の評価の間に役割間で適切でない者

	開発者	スポンサー	評価者	監督者
開発者		Yes	No	No
スポンサー	Yes		No	No
評価者	No	No		No
監督者	No	No	No	

3.2 評価プロセスの概要

51 次に CEM での評価プロセスの上位レベルの概要を示す。評価プロセスは、3 つの段階に分割することができ、それらは重なり合うことがある。

- a) 準備 – この段階では、スポンサーと評価者の間で最初の連絡が行われる。
- b) 実行 – この段階では、評価が行われる。
- c) 結論 – この段階では、評価の結果が配付される。

52 評価の各段階でのこれらの役割の間の相互作用について、次の節で記述する。

3.2.1 準備

53 準備段階（図 3.2 を参照）において、スポンサーは、PP または TOE の評価を開始するために、制度の中の適切な当事者に連絡する。スポンサーは、評価者に PP または ST を提供する。評価者は、スポンサーに適切な情報を要求し、評価が成功する可能性を評定するために、可能性分析を行う。スポンサーまたは開発者は、評価者に評価用提供物件のサブセット（おそらく、原案の形で）を提供する。評価者は、PP または ST をレビューし、評価のための確実な基盤を保証するために必要となる変更についてアドバイスする。評価のための制度の要件が満たされると、評価は次の段階へ進む。

54 可能性出力には、評価用提供物件、評価アクティビティの順序が示されたりリスト及び CC で取り扱われるサンプリング要件についての情報が含まれるべきである（例えば、ATE_IND）。可能性出力には、すべての役割が合意されるべきである。可能性出力の詳細は、各種の要因、特に、評価が PP であるかまたは TOE であるかに依存する。すべての役割は、プロプライエタリ情報の識別と保護に責任を負う。

55 制度に従って、スポンサーと評価者は、通常、この段階で評価の枠組みを定義するために合意に署名する。合意は、制度及び適用される国の法律及び規制による制約を考慮する。

D R A F T

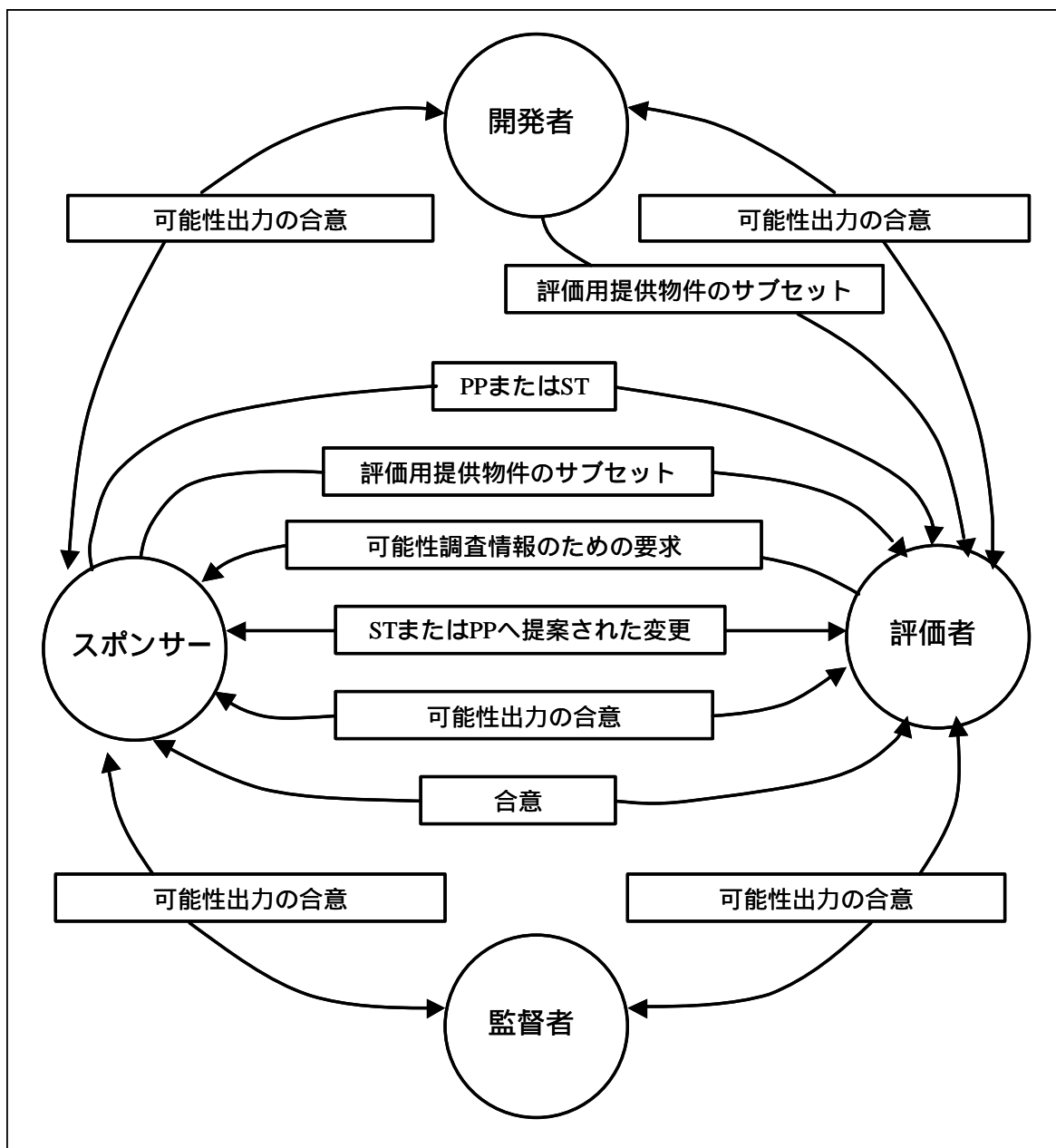


図 3.2 準備段階

3.2.2 実行

- 56 実行段階は、評価プロセスの主要な部分である（図 3.3 を参照）。実行段階において、評価者は、スポンサーまたは開発者から受け取った評価用提供物件をレビューし、保証基準が要求する評価者アクションを実行する。
- 57 評価中、評価者は、**所見報告書**を作成する。評価者は、所見報告書を使用して監督者から要件の適用の明確化を要求することができる。この要求は、将来の評価における要件の一貫性のある適用を保証するための要件の解釈となる。評価者は、潜在的な脆弱性または欠陥を識別するため、及びスポンサーまたは開発者に追加情報を要求するためにも所見報告書を使用することができる。所見報告書の配付は、さらに制度に指定される。
- 58 監督者は、制度が要求する評価を監視する。評価者は、総合判定及び判定の正当化が含まれている**評価報告書**（ETR）を作成する。

D R A F T

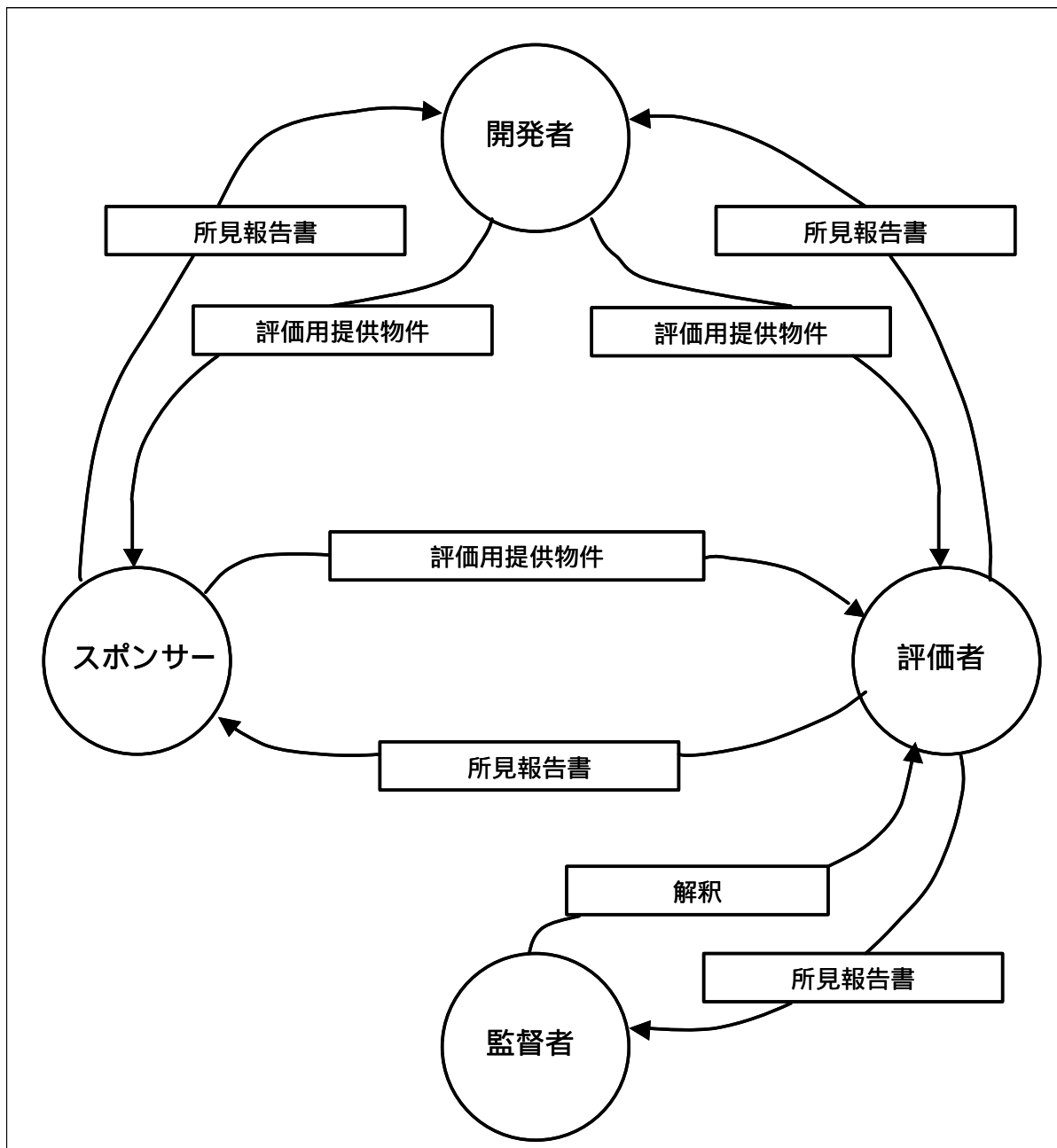


図 3.3 実行段階

3.2.3 結論

- 59 結論段階では（図 3.4 を参照）、評価者は、ETR を監督者に提出する。ETR を取り扱うときの制御の要件は、スポンサーまたは開発者への配付を含む制度によって確立される。ETR には、機密に関わるまたはプロプライエタリ情報を含めることができる。スポンサーは開発者のプロプライエタリデータにアクセスしないので、ETR がスポンサーに渡される前に、プロプライエタリ情報を取り除く必要がある。
- 60 監督者は、CC、CEM、及び制度の要件に従っていることを評価するために、ETR をレビューし、分析する。監督者は、ETR の総合判定に合意するまたは合意しないとの決定（監督判定）を行い、**評価要約報告書（ESR）**を準備する。監督者は、ETR を ESR への主な入力として使用する。評価者は、ESR を準備する監督者へ非開示要件の技術サポート、及び/またはガイダンスを提供することを求められることがある。
- 61 結論段階の終わりに、監督者は、ESR を評価監督機関に渡す。スポンサー、開発者及び評価者は、評価監督機関への公開可能性を保証するために、ESR をレビューする権利を持つべきである。

D R A F T

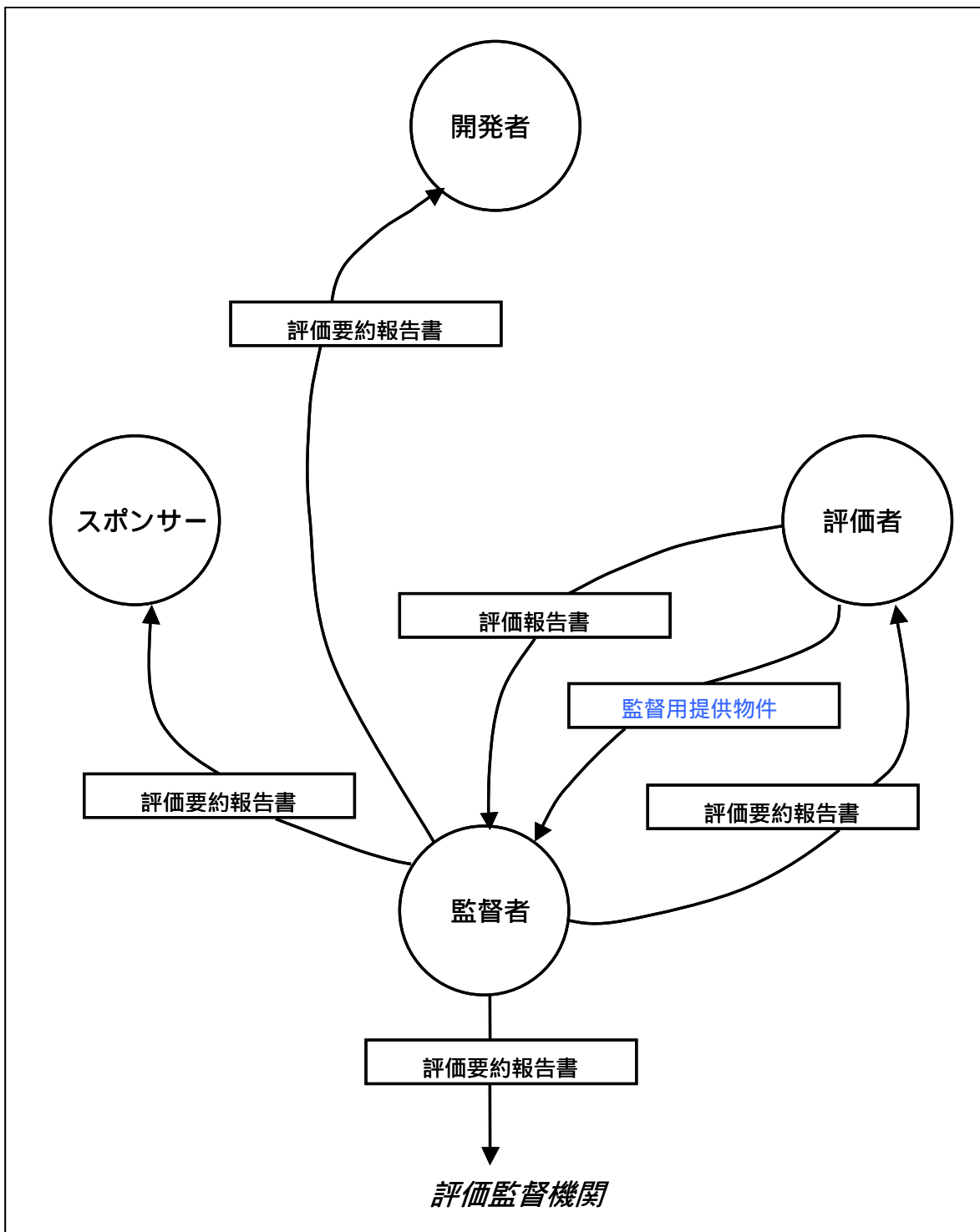


図 3.4 結論段階

D R A F T

附属書 A 用語集

62 この附属書は、このパートで使用されている省略語と頭字語、用語及び参照資料を示す。

A.1 省略語及び頭字語

63	CC	コモンクライテリア (Common Criteria)
64	CEM	共通評価方法論 (Common Evaluation Methodology)
65	EAL	評価保証レベル (Evaluation Assurance Level)
66	ESR	評価要約報告書 (Evaluation Summary Report)
67	ETR	評価報告書 (Evaluation Technical Report)
68	IT	情報技術 (Information Technology)
69	PP	プロテクションプロファイル (Protection Profile)
70	ST	セキュリティターゲット (Security Target)
71	TOE	評価対象 (Target of Evaluation)

A.2 用語

72 ボールド活字で表されている用語は、それ自体、この節に定義されている。用語が他の文書（例えば、CC）に定義されている場合、特に断らない限り、言葉どおりに引用されている。引用先は、定義の後の角括弧の中に示されている。

73 提供物件 (Deliverable):

評価用提供物件 (evaluation deliverable) 及び監督用提供物件 (oversight deliverable) を参照のこと。

74 開発者 (Developer):

3.1 章、3.1.2 節を参照のこと。

75 エレメント (Element):

分割できないセキュリティ要件。 [CCREF]

76 評価 (Evaluation):

定義されている評価基準に対する PP または TOE の評価。

- 77 評価保証レベル (Evaluation Assurance Level) :
CC 保証スケールの 1 つの点を表す (CC の) パート 3 から事前に定義された保証コンポーネントのセット。 [CCREF]
- 78 評価監督機関 (Evaluation Authority) :
評価結果のビジネス適用に責任を持つ団体。そのアクティビティは、CEM の有効範囲外であるが、「証明書」の発行、相互承認合意の作成、及び商用施設 (commercial facilities) の「ライセンス」のような制度規則の定義などのことに関係する。
- 79 評価用提供物件 (Evaluation Deliverable) :
1 つまたはいくつかの評価または監督アクティビティを実行するために評価者または監督者がスポンサーまたは開発者に要求する任意の資源。
- 80 評価証拠 (Evaluation Evidence) :
有形の評価用提供物件。
- 81 評価プロセス (Evaluation Process) :
IT セキュリティ評価を行うために当事者が実行するアクションのセット。
- 82 評価結果 (Evaluation Result) :
編集者の注記 : この用語は、単に一般的な意味で使用されている。
- 83 評価要約報告書 (Evaluation Summary Report) :
監督者によって発行され評価監督機関に提出される、監督判定及びその正当化を証拠資料として提供する報告書。
- 84 評価報告書 (Evaluation Technical Report) :
評価者によって作成され監督者に提出される、総合判定及びその正当化を証拠資料として提供する報告書。
- 85 評価者 (Evaluator) :
3.1 章、3.1.3 節を参照のこと。
- 86 評価者アクションエレメント (Evaluator Action Element) :
TOE のセキュリティターゲットに行われているセキュリティクレームを検証する TOE 評価者の責任を表す、CC に記述されている保証要件。 [CCREF]
- 87 中間判定 (Interim Verdict) :

D R A F T

1 つまたはいくつかの要件に関して**評価者**が出す「合格」、「不合格」、または「未決定」のステートメント。

88 解釈 (Interpretation):

CC、CEM、または**制度**の要件の明確化または展開。

89 方法論 (Methodology):

IT セキュリティ**評価**に適用される原則、手続き、及びプロセスのシステム。

90 所見報告書 (Observation Report):

評価中に問題の明確化を要求したり、問題を識別するために**評価者**が作成する報告書。

91 総合判定 (Overall Verdict):

評価の結果に関して**評価者**が出す「合格」または「不合格」のステートメント。

92 監督者 (Overseer):

3.1 章、3.1.4 節を参照のこと。

93 監督用提供物件 (Oversight Deliverable):

1 つまたはいくつかの評価監督アクティビティを行うために**評価者**に要求する任意の資源。

94 監督判定 (Oversight Verdict):

評価監督アクティビティの結果に基づいて**総合判定**を確認または拒否する、**監督者**が出す「合格」または「不合格」ステートメント。

95 プロテクションプロファイル (Protection Profile):

セキュリティ対策方針、機能、及び関連する根拠を備えた保証要件の再使用可能で完全な組み合わせ。[CCREF]

96 役割 (Role):

編集者の注記: この用語は、単に一般的な意味で使用されている。

97 制度 (Scheme):

IT セキュリティ**評価**を行うために必要な基準と方法論など、評価環境を定義している規則のセット。

98 セキュリティターゲット (Security Target):

D R A F T

識別された TOE を評価するための基礎として使用される、セキュリティ対策方針、機能と保証要件、要約仕様、及び根拠の完全な組み合わせ。 [CCREF]

99 スポンサー (Sponsor):

3.1 章、3.1.1 節を参照のこと。

100 評価対象 (Target of Evaluation):

評価の主題である IT 製品またはシステム。 [CCREF]

101 判定 (Verdict):

総合判定及び中間判定を参照のこと。

A.3 参照資料

CCREF Common Criteria for Information Technology Security Evaluations, Version 1.0, January 1996.

COD Concise Oxford Dictionary.

附属書 B CEM オブザベーション報告書 (CEMOR)

B.1 序説

102 本附属書は、CEM についてコメントするためのメカニズムについて詳しく説明している。

103 このメカニズムは、オブザベーションを明記するために使用する報告書フォーマット、及び CEMOR が送られるべきメールアドレスからなる。

B.2 CEMOR の転送

104 CEMOR は、インターネットメールアドレス cem@cse.dnd.ca へ直接送ることができる。CEMOR は、発信者がこのアドレスに直接送るか、またはこのパートのまえがきに記載されている組織の 1 つを通して送ることができる。通常、確認応答が CEMOR の発信者に送られる。

B.3 CEMOR のフォーマット

105 CEMOR は、テキスト (ASCII) フォーマットだけで転送しなければならない。

106 別々の CEMOR をオブザベーションごとに作成しなければならない。1 つの CEMOR で複数の関係のないオブザベーションを取り扱ってはならない。

107 CEMOR には、次のすべてのフィールドが含まれていなければならない。ただし、いくつかのフィールドは、空白でもかまわない。各フィールドは、ASCII 文字 "\$" で始まり、その後にアラビア数字が続き、最後が ASCII 文字 ":" でなければならない。

\$1: 発信者名

108 発信者の完全な名前。

\$2: 発信者の組織

109 発信者の組織/所属機関。

\$3: リターンアドレス

110 必要に応じて、CEMOR を受け取ったことを確認応答し、明確化を要求するための電子メールまたはその他のアドレス。

D R A F T

\$4: 日付

111 オブザベーションの提出日 YY/MM/DD。

\$5: 発信者の CEMOR 識別情報

112 この識別情報は、発信者によって CEMOR に割り当てられる。この識別情報には、2 つの要件が存在する。その第一は、発信者にとって一意であること、第二は、"CEMOR."で始まらなければならないことである。

\$6: CEMOR のタイトル

113 この CEMOR の短い記述的タイトル。

\$7: CEM 文書参照

114 CEM の影響を受ける領域への単一の参照。このフィールドは、CEM パート番号と節番号を識別しなければならない。さらに、段落番号（または、段落番号が関係ない場合、表または図の番号）もこのフィールドに識別しなければならない。

\$8: オブザベーションの説明

115 オブザベーションの包括的記述。このフィールドの長さに関する制限はない。ただし、テキストだけを含むべきで、ASCII だけで示すことができない図または表を含めてはならない。

\$9: 提案される解決策

116 オブザベーションを取り扱うために提案される解決策。

117 \$\$ CEMOR の終わり

118 CEMOR に関係する情報の終わりを示すために必要となる。

B.3.1 オブザベーションの例

\$1: A. N. Other

\$2: PPs 'R' US

\$3: another@ppsrus.com

\$4: 96/01/31

\$5: CEMOR.ano.comment.1

\$6: 綴りエラー

\$7: パート 1、3.1.5 節、49 段落

D R A F T

\$8: "summarizes" (「要約」)

\$9: UK 英語を使用するのであれば、"summarises"を使用すること。\$\$