サポート文書
ガイダンス

開発者証拠の収集

2012 年 4 月

バージョン 1.5

CCDB-2012-04-005

平成 26 年 8 月翻訳第 1.0 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

IPA まえがき

はじめに

本書は、「IT セキュリティ評価及び認証制度」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 Supporting Document (以下、CC サポート文書という)を翻訳した文書である。

原文

Collection of Developer Evidence

Version 1.5
April 2012 CCDB-2012-04-005

まえがき

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 バージョン2、3及びそれに関連する共通評価方法を補完することを目的としたサポート文書である。

サポート文書は、「ガイダンス文書」または「必須技術文書」でもある。「ガイダンス文書」は、規格適用の相互承認を必要としない分野への固有のアプローチや規格適用に焦点を当てる文書であり、そのため規格という性格のものではない。「必須技術文書」は、サポート文書の適用範囲に含まれる評価への適用が義務付けられている文書である。必須技術文書の使用は、必須であるだけでなく、それを適用した結果発行される認証書は、CCRAのもとで承認されている。

技術編集者：NLNCSA

改訂履歴：
V1.5、2012年4月：初版リリース。

特殊用途の分野：なし

謝辞：
以下に示される組織、及びJoint Interpretation Working Group の下部組織は、本コモンクライテリア関係文書の作成に寄与した。

フランス：	*Agence Nationale de la Sécurité des Systèmes d'Information*
ドイツ：	*Bundesamt für Sicherheit in der Informationstechnik*
イタリア：	*Organismo di Certificazione della Sicurezza Informatica*
オランダ：	*Netherlands National Communications Security Agency*
スペイン：	*Ministerio de Administraciones Públicas and Centro Criptológico Nacional*
英国：	*Communications-Electronics Security Group (CESG)*

また、以下の組織に加入しているスマートカードベンダ、評価機関、その他の企業による作業の貢献に対して感謝の意を表する。

- *e-Europe*
- *International Security Certification Initiative (ISCI)*

目次

1 背景

1 この目的は、コモンクライテリア（評価基準）の効果的かつ柔軟的な適用を促進することである。開発者が提供物件を評価への入力として供給する形式には、かなりの柔軟性がある。この説明では、開発者が選択してもよいオプション、及び評価者がクライテリアISO/IEC 17025の要件に適合すると回答してもよい方法の一部、ならびに相互認証を検査する。また、この解釈では、完全に範囲外の作業を評価者が引き受ける危険性があることがある場合を識別及び検討する。

2 クライテリアの表現方法については、特殊な種類の各証拠を含む特定文書を開発者が提供すべきであることを意味している。通常、その場合には最も効率的になるため、証拠をレビューするために評価者が要求する労力は最小限に抑えられる。しかし、証拠の形式に関する明確な要件はなく、情報内容だけが規定されている。特殊な例では、開発者が証拠をより普及した形式で示す場合により効率的になり、これには、評価者の整理及びレビューするかなりの労力が必要となる。これが客観的かつ公平に実行できれば、証拠の*収集*は完全に正確で受け入れることができる。

3 開発者が用意する提供物からの評価判定の客観的な正当化に重点が置かれている。客観的な正当化が可能でない場合、作業は、証拠の収集ではなく、*作成*になる。本書で*作成*の側面が提示されるのは、読者が*収集*と区別をしやすくするために限られる。本書では、評価で使われる根拠資料の作成方法に関しては記述しない。

4 本書では、CCで要求される証拠取得のために許可されている二つの方法を区別しない。

- 従来の方法による証拠資料 ：開発者は、すべての必要な情報を直接配付する
- 情報：既存の開発者証拠資料に基づき、証拠報告書（回答済み質問票など）の収集に書き込まれた報告書に書かれた追加情報で完結する

2 解釈

5 これは、CC基準とは独立した解釈である。

6 開発者はCCが要求する情報を提供する責任を負う。評価者は以下のような提供情報の一部を例外的に収集してもよい。

a) 評価者の寄与物件が開発者によって十分に承認されている

収集プロセス中に評価者が提供する情報は、開発者に受け入れられて、TOE の証拠資料構成管理に統合されなければならない。つまり、補完的 な評価証拠として登録されなければならない。

b) 承認は認証機関によって事前に与えられる

プロジェクトを開始する前に、ITSEF 及び開発者は、この方法を使用する可能性があるタスクについて合意しなければならない。この合意は、評価登録中に認証機関に対して公式に通知しなければならず、これによって、評価で選択された手法の認証機関による承認を通知及び取得することができる。この方法を用いて評価できるタスクが ALC、ADV、及び ATE であることを、認証機関にはすでに通知されている。しかし、各評価では、開発者から直接提供される証拠資料の種類、及び評価者に収集される情報の種類を評価者が認証機関に通知しなければならない。

c) 評価者の寄与物件は評価チームの他のメンバーによって独立してレビューされ、彼らのレビューは ETR(または中間評価報告書)に証拠資料として提示される

評価報告書は、古典的な手法ではあるが ISO/IEC 17025 に従って、すでに系統的にレビューされている。証拠の収集中に開発者が生成する特定の情報については、レビュー担当者の注意は特に、評価者によって証拠の作成が行われていない（証拠の収集のみである）ことの検証に集中している。

2.1 証拠の収集

7 国際的に合意されたクライテリア及び方法に従って、開発者は指定された証拠を提供しなければならないが、その形式は規定されていない。証拠は保証コンポーネントのすべての要件に対処する単一文書で提示される場合もあれば、多数の文書から収集される必要がある場合もある。多数の個々の情報源及び形式からの証拠収集は、正当な評価者作業である。理想的な開発者の提供物件に近づける作業文書を評価者が構成することが都合の良い場合があるが、それは必須ではない。評価者の作業は、主観的な*作成*ではなく、開発者が提供した資料の客観的な*収集*に限定されなければならず、その作業を反復可能、再現可能、及び公平にしなければならない。適切なテストは、有能な評価者が基本的に同じ結果を取得するかどうかである。

8 証拠の客観的な収集は、評価者にとって妥当なものである。これはコンサルティングとして見なすべきではないため、独立チームによって実行される必要はない。

2.1.1 証拠収集が有用になる時期の決定

9 証拠収集方法は、証拠資料の変更による再評価を減らすために評価者によって使用できる。この方法によって以下の事項が可能になることに留意することが必要である。

- CC 要件に対応できる場合、開発者の実務を考慮に入れる（方法を実務に合わせる）
- 評価保証レベルに影響を与えずに、評価の限定的な作業負荷を考慮に入れる

10 評価問題のかなりの部分は、反復に関連する証拠資料に起因する。つまり、保証コンポーネントに要求される情報の内容が何回かの証拠資料の反復後に最終的に検証できるとしても、情報が最初は不完全であったり、証拠資料に一貫性がなかったりする。この方法の目標は、非公開/内部の開発者証拠資料の反復を最小限に抑えることである（これは、セキュリティターゲットまたは製品のガイダンス証拠資料には適用できない）。

11 この方法の2番目の目標は、CCのためだけに書く証拠資料でなく、できる限り、開発者によって使用される実際の証拠資料に関する評価作業に基づくようにすることである。評価者は、「証拠の収集」を使用して、開発後に書かれたいくつかの開発者証拠資料をできる限り制限する。

12 重要な注釈：この方法は、最終評価で不合格の判定とならない証拠資料上の問題を対象とする。通常、SFRが実際に実装されていないと結論づけることを許可する、評価者によって発行される「証拠資料上の問題」は、「証拠収集」方法によって解決されない。そのため、この方法は、開発者がすべての情報を、収集する必要なく直接配付しなければならないと考える古典的な手法と同じ評価レベルを保証する。

13 2つの異なる方法は、CCで要求される証拠の取得を可能にし、証拠資料と情報（記入済み質問票などの収集された証拠を記入した証拠資料）の評価事例に応じて考慮されなければならない。

2.1.2 特定評価の証拠の収集範囲の決定

14 開発者及び評価者はまず、ADV、ALC、ATEの評価タスクに関連する既存の開発者証拠資料の評定をしなければならない。一部の初期証拠資料は、これらの評価アクティビティに関係する評価者に対して利用可能でなければならず、そうでない場合、評価のいくつかの側面は対処されないことは明らかである。提供される情報のレベルによって、評価者及び認証機関に、評価が肯定的な結果で合格できたという十分な信頼が与えられる。

15 この評定では、対象の評価保証レベルを考慮に入れる。この初期評定が行われたら、評価者は、証拠収集の使用法の目標とする範囲が論理的に受け入れられるかどうかを結論づけて、開発者によって（どの評価アクティビティ、または評価アクティビティの一部に対応する）どのような種類の証拠資料を直接提供するか、及び評価者によってどのような情報が収集されるかについて認証機関に通知する。その後、認証機関は、使用する証拠の収集の範囲を承認するかどうかを決定できる。

16 評価判定は最終的に、初期に配付された一連の証拠資料が十分であることを保証する。実際に、これによって（CCへ厳密に適合するために、または評価者が効率的に理解できるために）開発者によって直接提供されなければならない情報が本当に提供される。そうでない場合、評価判定は不合格となる。

2.1.3 事前アクティビティ：製品に関するトレーニング

17 この段階は、厳密に言えば、証拠収集方法の部分ではない。それでも、評価者が製品環境の枠組み及び評価の枠組みを素早く理解することはメリットになる可能性がある。したがって、評価者は、このトレーニングを利用して、評価中に証拠を収集できるかどうかを判断することができる。また、このトレーニングでは、TOEの範囲を製品と比較して理解することもできる。

18 セキュリティターゲット評価中、評価者は製品機能に関するトレーニングを受けなければならない。

19 このトレーニングによって、以下の事項が可能になるようにしなければならない。

- ST 評価の妥当性を向上する
- FSP 及びガイダンス評価を開始する前に、TOE の機能的知識を取得する

20 このトレーニング中に評価者は、以下の事項を取得しなければならない。

- ST 執筆者による ST の記述
- TSFI 記述に加えて、「TSFI」と見なされない他の製品インタフェースの記述
- TOE との通信をサポートするツールの記述。開発者は、これらのツールを評価者に配付しなければならない。
- 製品全体のアーキテクチャを理解できるための設計情報へのアクセス（TDS コンポーネントの評価保証レベル用）

21 評価者は、この初期トレーニングの最後に、開発者の入力及び証拠資料の状態が「証拠収集」として適していない、または十分でないと結論づける場合は、「証拠収集」が実行可能でないという結論を出す。このため、評価にはCEMの古典的な手法が望ましいであろう。

2.1.4 実際の証拠収集

22 以下のような一部の保証コンポーネントは、証拠収集と関係を持つことはできない。

- ASE_xxx/APE_xxx：ST/PP は、評価全体の基礎となる文書であって、公開にされることが多い。この文書は、評価者が評価の理解をそれに基づかせているため、完全で理路整然としていなければならない。
- AGD_xxx：ガイダンス証拠資料は、ユーザに配付された TOE の一部を構成する。そのため、不備は誤りとなる。評価者が不備を補うことは許容されない。
- 準形式的/形式的方法、つまり、準形式的及び形式的手法に関係するコンポーネントのワークユニットを、証拠の収集を必要とする不完全な証拠資料に関連付けることは基本的に困難である。それでも、証拠の収集は、これらのコンポーネントに使用できる。例えば、使用される形式的方法を理解するために質問票を使用できる。しかし、これは形式的モデル自体には適用できない。

23 評価者が証拠を作成ではなく収集しなければならないという事実のため、評価者が提供する情報は主に、必要な回答を示さない自由な質問で構成される質問票の形式を持つ。実際に、質問票の形式によって、既存の証拠資料に欠如している情報に対応する（どの情報が欠如しているか判断し、対応する質問を用意するために、評価者の事前作業が必要になる）、評価者が実際に要求する情報に関する収集に焦点を当てることができる。

24 評価者は、直接収集された情報（つまり、開発者が与えた回答）と、これらの回答に直接関連付けられた評価者自身の解析/コメントを明確に区別しなければならない。評価者は、直接収集された情報（つまり、開発者による回答）と、これらの回答に直接関連づけられた評価者自身の解析/コメントを明確に区別しなければならない。実際に、同じ文書に開発者の回答と評価者の解析を記載できるため、それらを明確に区別することは基本的なことである。例えば、質問票が表形式である場合、開発者の回答または評価者のコメントの行や列を分けることで区別を付けることができる。

25 認証機関は、インタビューセッションが行われる場合に通知を受け、そのセッションへの参加を決定できる。

2.1.5 評価者の寄与物件は最終的に開発者に承認される

26 証拠が完全に収集されたら、評価者はその証拠を認証機関及び開発者に配付する。開発者は、収集された情報を、補完的な評価証拠になるように充当しなければならない。この証拠は、TOEの構成管理システムに含まれなければならない。

27 開発者は、今後の評価のために開発者自身の証拠資料から直接収集される情報を統合して、再利用し易くすることも決定できるが、それは方法論によって要求されていない。

2.2 証拠作成と証拠収集の比較

28 客観的な証拠収集と主観的な証拠作成の違いは、開発者への自由な質問と誘導尋問の違いを考慮することによって説明される。評価者が明確な仮説を立てて開発者にイエスかノーの確認を求める場合、これは証拠作成の側に該当するが、要求される回答を示さない自由な質問は証拠収集の側に該当する。

29 証拠作成に対応する代表的な質問は、「設計のこの部分にこのSFRが実装されていることを確認できるか?」のようになる。クライテリアの意図は、開発者がTOEのIT特性を熟知していることを実証すべきであること、及びセキュリティ側面に注意してきたことであるため、開発者は、証拠の収集に対応する自由な質問に回答できなければならない。証拠収集に対応する質問は、「このSFRが実装されている設計の部分を示すことができるか?」のようになる。

30 証拠作成に対応する誘導尋問は、評価基準及び、設計情報、開発環境におけるセキュリティ手段の実装などの評価アクティビティの判定に直接関連づけられる情報に関連している。

2.3 軽微な不備

31 評価者は、開発者にインタビューして回答を証拠資料として提出したり、仮説を立てて開発者に確認を求めたりすることによって、開発者が供給する提供物件の軽微な不備に対処してもよい。ただし、評価者は、そのような入力の一貫性を、その他の開発者が供給する資料を用いてチェックすべきである。評価者は、そのように実行する場合は補完作業が過剰にならない、クライテリアで合意される根拠を提供しなければならない。通常は、その情報及び根拠を評価報告書に直接追加できる。

32 これらの軽微な不備は、ケアレスミス、容易に確認できる証拠資料への参照の欠如など、一部の情報に限定されなければならない。証拠作成との違いは、クライテリアに関して開発者によって確認される情報の重要性である。つまり、軽微な不備は、対応する評価アクティビティの判定に影響を与えない不完全性/不整合性に相当しなければならない。

2.4 収集可能な情報の例

33 開発者が対応解析を提供する要件では、必ずしも製品を表にまとめることを要求しない。追跡性が明白である場合、評価者はそのようなまとめ（必要な場合）を証拠収集の一部として作成してもよい。一方、関係する機能の一般的な類似点に基づき対応を推定する必要がある場合、その作業は収集の範囲外になり、証拠作成に相当する。

34 開発者が提供する設計は特定の点においては不完全であると分かることがあり、例えば、すべてのモジュールの完全な詳細が提供されない場合がある。以下のような代替源からの評価者の補足的証拠収集の範囲がある。

a) その他の関連する設計情報。

これには、密接な関係がある TOE の設計文書、標準テキスト（Unix や NT 内部構造に関するものなど）、及び有用な枠組みを提供することがある TOE の対象バージョンに関連する証拠資料（機能仕様書など）が含まれる場合がある。

b) TOE の以前の評価による ETR 内の証拠（つまり、旧バージョンや異なる種類に関係するもの）。

評価者が TOE の以前の評価で TOE セキュリティの内部作業に関する理解を詳細に証拠資料として提出した場合、このような証拠は、評価者が TOE の内部作業の必要とされる全体的な理解を得ることを支援することがある。

c) TOE セキュリティの特定側面に関する開発者の説明。

開発者の説明によって、例えば、特定の TOE セキュリティ機能が実装される方法や個別の TOE サブシステムの内部作業に関する概要などの、TOE の特定部分の全体的な理解を評価者が得ることが支援される場合がある。そのような証拠は、下位レベルの設計を完成するために使用される場合もある。口頭で説明された情報で証拠の一部を表すものは評価者によって証拠資料として提出されなければならず、そのような入力は、その他の開発者が提供した証拠との一貫性をチェックされるべきである。

d) 口頭、書面(電子メールなど)にかかわらず、評価者からの特定の技術的質問の明確化。

このような証拠は、技術的詳細の特定点に関する評価者の理解を確認するために使用されるべきである。

e) 開発者の構成管理システムによって生成される証拠。

このような証拠は、コールツリー（どのモジュールが他のどのモジュールに依存しているかを識別）、モジュールによるグローバルデータ構造の使用などの、モジュール間の相互関係の正確な状況を確立することを支援する上で有用となる場合がある。

f) ソースコードモジュールに関連付けられているモジュールヘッダ

これは通常、ソースコードモジュールまたはヘッダファイル内に含まれる設計証拠の形式を取る。

g) 関連付けられているコメントを含むソースコード自体。

ソースコード自体から詳細設計のかなり大きな割合を導き出すことが実用的であることは予期されないが、ソースコード内のコメントと同様に詳細についての特定の質問を取り上げることが用いられる場合がある。