コモンクライテリア　アセッサ
登録ガイダンス

バージョン 1.1
平成 22 年 8 月 23 日

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

1. はじめに

本資料は、コモンクライテリア アセッサ登録の要件となる申請基準について、文書審査や面接審査でどのような基準を確認するかについて説明したものです。本資料は IT セキュリティ評価基準であるコモンクライテリア(CC)とその評価基準を用いた評価手法に関する知識を有する方を対象とします。

本資料で用いる用語は「コモンクライテリア アセッサ登録制度運用規程 CA-01」（以下規定 CA-01）で定義されているものを用います。また本資料より規程 CA-01 の内容が優先されますので、あわせて参照願います。

2. 背景

CC に基づく評価は、開発者がその評価基準の意図を理解していない状況では、個々の評価者からの要求事項を満たすための形式的な対応に終始し、セキュリティ品質を高める活動に十分結び付けられないまま評価が進行していくこととなります。また、その結果として評価の指摘に対する適切で効率的な対応ができず、評価コストの増大を招くことになります。

一般的に開発者は、開発作業に追われ CC で求める個々の要求を詳細に理解することは困難な立場にいます。また、評価者は中立公正を期すために指導的な助言を控える傾向にあります。このような状態では、やはりセキュリティ品質を高めるための効果的な作業や認証取得のための効率的な作業が行えないことは自明です。

コモンクライテリア アセッサは、CC の用語を理解し、かつその意義を開発プロセスに具体的に射影して説明をすることができる、いわば開発者と評価者の溝を埋めるための役割を担うことが期待されます。

3. 審査手順

審査には文書審査と面接があります。文書審査では、申請書類から、申請者が基準を満たしていることを確認するほか、開発元レビュー報告書のレビュー内容を確認します。審査員は面接の中でアセッサ申請者に、開発元レビュー報告書の記述に関して補足的な説明や内容の確認を求めることもあります。

4. 文書審査（開発元レビュー報告書）

コモンクライテリア アセッサ登録申請の文書審査の対象として、開発元レビュー報告書を提出していただきます。この開発元レビュー報告書の内容から、審査員はコモンクライテリア アセッサ登録の申請基準(規程 CA-01 第 3 章)を満たしていることを確認します。基準の主な内容は、情報処理技術に関する知識及び実務経験と、CC に基づく開発プロセスの

セキュリティ品質検査能力を有することです。

開発元レビュー報告書は、規程 CA-01 別表に掲げられている保証コンポーネントを最低限含めた保証コンポーネントのレビュー結果を記述します。形式は、CEM に規定された評価報告書の構成に準じていただきますが、レビュー内容の記述方法は自由です。各ワークユニットで求められている内容が、その対象となる TOE の開発においてどのように考慮されているかを、アセッサは TOE 全体のセキュリティ目標や TOE の特性などとの一貫性や、その主張をサポートする客観的で十分な開発証拠資料とともにレビューし、報告書に記載します。ここでは、評価者が作成する評価報告書のようにワークユニットの合否の判定を求めてはいません。評価者の評価作業への有用な入力となる開発者の考え方を記述することになります。

開発元レビュー報告書に対する審査の観点では、その目的から評価機関の作成する評価報告書のような個々の検査項目（ワークユニット）の正確かつ完全な評価結果の記述を求めるものではありません。開発におけるセキュリティをどのように考えたのか、TOE の特性や開発元セキュリティポリシーなどを考慮した TOE に係るレビュー結果が示されていることが重要なポイントとなります。その結果として、個々のワークユニットの個別のレビュー結果は、全体として一貫された観点で示されていることを審査では確認します。以下に例を示します。

開発元レビューの観点の例：

・*ST 評価*

開発者にセキュリティターゲットの意義を理解してもらう能力を有することが確認の大きな目標です。消費者に TOE のセキュリティ目標を、目的意識を持って理解させる論理展開がセキュリティターゲットにおいてできていることを、アセッサはワークユニットを通じて検査するでしょう。

たとえば、「資産」についてであれば、

・TOE が守るべき資産が明確に定義されているか
・定義された資産と使用環境の矛盾はないか
・資産の価値と TOE 運用労力、投資のバランスは無理がないものか
・資産の価値と攻撃者能力、攻撃手法のバランスは無理がないものか

といった内容の考慮は、技術文書を書くものとして CC の世界を知らなくても達成できることです。さらに「資産が明確に定義」されているということは、抽象的な概念ではなく消費者が資産の形式、格納場所、資産価値を理解できる等、その TOE の特性にしたがった判断が必要となります。

アセッサは、開発者が、CCのワークユニットを意識したり、それらを満たすための歪なST作成したりすることのないよう、CCで検査すべき本来の目的を理解

させ、CCの言葉を使わずに開発者に対する指摘を行います。

・*機能仕様評価*

開発者が、上位仕様が完全に実装に反映される過程を保証した開発をするために、どのような設計資料が必要であるかは（それを実際に開発過程において作成しているか否かは別として）理解できるはずです。しかしながら、CC における個々のワークユニットが、それらとどのように関連するかということは、開発者にとっての興味の範囲ではありませんし、それらを理解することは大きな負荷となるでしょう。

アセッサは、ワークユニットの内容を理解し、仕様書において完全性や正確性をより確実にするための望ましい形式、項目を開発プロセスに落とし込むことをレビューの成果として期待されます。

たとえば、すべてのエラーメッセージを識別していることを、ワークユニットからは単に仕様書の形式の検査が目的であるような印象を開発者に与えがちです。しかし、その機能におけるエラーの内容を把握することで、本来のセキュリティ機能のふるまいの理解のためのより有用な入力となるとともに、その機能の延長でアクセスしている資源などが明らかになり、機能仕様の正しさ、危惧すべきセキュリティ事項を評価の過程で認識することが可能となります。

アセッサは、開発者にワークユニットを直接押し付けるのではなく、設計や仕様書においてどのようなことが懸念され、どのような情報を開発者自身が仕様書に書き留めることにより、実装および保守の品質の向上が図れるかを理解させます。

以上のように、開発元レビュー報告書では、個々のワークユニットが満たされているという説明からスタートするのではなく、まず全体としてどのような方針のもと、アセッサはレビューを実施し、それらがどのように開発セキュリティに寄与したかという明確な主張がなされていることが重要です。そのレビューの結果として、各ワークユニットがどのように満たされ、それが第三者判断に耐えうる客観性を持つというアセッサの考察を審査の対象として確認します。

なお、本登録制度は「IT セキュリティ評価及び認証制度」とは完全に独立したものであり、開発元レビュー報告書のレビュー結果と、そのレビュー対象とした評価対象(TOE)の評価結果とは相互になんら影響を与えるものではありません。つまり、開発元レビュー報告書のレビュー結果が、対象とした TOE の評価結果と合致する必要はありません。

5. 面接

面接では、文書審査において十分な確認ができなかった点と開発元レビューをアセッサ申請者自身が実施したことを、審査員がインタビュー形式で確認します。この際、確認の一環として開発証拠資料（対象製品の設計書や脆弱性分析書など）を使用し説明をしていただくことがありますので、アセッサ申請者は開発証拠資料にアクセスできる状況で、面接を受けていただきます。面接時間は約 1 時間半を想定しています。