# 付録：認証維持適用のためのチェックリスト(V3.0)

本チェックリストは、変更TOEが認証維持の対象となるかどうかを判断するために必要な検討事項をまとめたリストです。

手順１で、「チェック項目」の内容について、該当すれば「Yes」、該当しなければ「No」の判定をし、その欄の「認証維持可否の判断」に従ってチェックを進めます。「認証維持可否の判断」の結果、検討が必要と判断された（次のチェックに進めない）場合、次表の手順2の補足説明を参考に再評価等の検討をしてください。補足説明には、開発環境のサブセット評価を伴う認証維持の場合も含まれています。

チェックリストはCC Ver3.1以降を想定しています。

【手順1】

以下の全チェック項目に対し、「Yes、No」で判定を行います。認証TOEのEALが「EAL」欄のレベルに含まれているものはすべてチェックの対象となります。EALが該当しなければ次のチェックに進みます。判定の結果、ひとつでも検討が必要と判断された場合は、手順2の「再評価のための補足説明」を参考に再評価等の検討が必要となります。

| 項番 | チェック項目 | EAL |
| --- | --- | --- |
| 判定 | 認証維持可否の判断 |
| 1.1 | 認証TOEの有効期限の3か月前を経過している。 | 1以上 |
| Yes | 認証維持の対象とならない。 |
| No | 1.2のチェックに進む。 |
| 1.2 | TOE名称やバージョンの変更、動作環境プラットフォーム追加等、認証TOEと変更TOEを、調達者が識別する手段がある。 | 1以上 |
| Yes | 1.3のチェックに進む。 |
| No | 変更TOEの識別について再検討が必要。 |
| 1.3 | TOE名称に変更がある場合、変更されたTOE名称は認証TOEのST中の「TOE概要」や「TOE記述」に記載されている調達者の期待するTOEの機能性や評価範囲を反映している。 | 1以上 |
| Yes | 1.4のチェックに進む。 |
| No | 変更TOEの名称について再検討が必要。 |
| 1.4 | 変更TOEは、以下の変更を含む。・機能仕様において、セキュリティ機能の外部インタフェースが新たに追加された。または既存の外部インタフェースが削除された。 | 1以上 |
| ・セキュリティ機能を実現する実装表現（ソースコードやハードウェア図面）に変更がある。 | 4以上 |
| ・ガイダンスにセキュリティ事項に関する変更がある。 | 1以上 |
| ・TOEの変更により、リグレッションテスト以外の新たな開発者テストや脆弱性分析が必要となる。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 1.5のチェックに進む。 |
| 1.5 | ST中の記述に変更・追加がある。ただし以下の項目は除く。・ST作成日や、STバージョンなどのST識別情報、及び更新情報・TOE名称、またはTOEバージョン | 1以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 2.1のチェックに進む。 |
| 2.1 | TOEセキュリティ機能の外部インタフェースにおいて以下の変更がある。・認証TOEの評価において、SFR実施及びSFR支援に分類されたTOEの外部インタフェースの目的、使用方法、パラメタに変更がある。 | 1以上 |
| ・TOEのいずれかの外部インタフェースの目的、使用方法、パラメタに変更がある。 | 2以上 |
| ・認証TOEの評価において、SFR実施に分類されたTOEの外部インタフェースのエラーメッセージに変更がある。 | 2以上 |
| ・TOEのいずれかの外部インタフェースのエラーメッセージに変更がある。 | 4以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 2.2のチェックに進む。 |
| 2.2 | 認証TOEにおいて識別されたサブシステムに以下の変更があるか。・サブシステムの機能、ふるまいに変更がある。・セキュリティ機能外部インタフェースに対応するサブシステムインタフェースに変更がある。 | 2以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 2.3のチェックに進む。 |
| 2.3 | 認証TOEにおいて識別されたモジュールに以下の変更がある。・サブシステムに対応するモジュール構成に変更がある。・モジュールの機能、ふるまいに変更がある。・モジュールのインタフェースに変更がある。 | 4以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 2.4のチェックに進む。 |
| 2.4 | 認証TOEに対し以下の変更がある。・TOEが識別する利用者ごとにアクセスできる資源（ファイルやメモリ空間）を管理する方式（アクセス権やセキュリティ特性）に変更がある。・TOEがダウン状態から運用状態に至る初期化においてセキュリティ保持のための仕組みに変更がある。・TOEのセキュリティ機能自体を保護するための仕組みに変更がある。・セキュリティ機能の実施に影響あるかどうか不明なセキュリティ機能以外の外部インタフェースが変更、追加された。 | 2以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 2.5のチェックに進む。 |
| 2.5 | 認証TOEにおいて識別されたモジュールに対応する実装表現（ソースコード等）の変更がある。または、対応するか不明な実装表現の変更がある。 | 4以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 3.1のチェックへ進む。 |
| 3.1 | TOEが識別する役割（管理者、監査者、一般利用者など）、あるいはその役割が持つ権限（特定の機能や資源にアクセスできる権限）に変更がある。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 3.2のチェックへ進む。 |
| 3.2 | TOEの利用者における役割ごとに定められた、以下の事項に変更がある。・セキュアな使用のために必要となる利用者が実施すべき事項。・セキュアな使用を要求されるTOEインタフェース（パラメタ範囲、リターンコード、応答・エラーメッセージ、デフォルト値など）。・セキュリティ特性の変更や障害発生時の利用者が対処すべき事項。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 3.3のチェックへ進む。 |
| 3.3 | TOEの運用準備のための手続きや環境構築において、以下のようなセキュリティに係る事項に変更がある。・TOEのバージョンや完全性の確認手順。・TOE運用においてセキュリティ上必要とされるTOEの設定、システム要件、環境の要件、構築手順。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 4.1のチェックへ進む。 |
| 4.1 | TOEまたはそれを構成する要素の管理について、以下の変更がある。・調達者がTOEを（ラベルやバージョン確認コマンド等で）識別する手段の提供方法の変更・削除。 | 1以上 |
| ・開発者がTOEを構成する要素を識別する手段の変更。・開発者が認証TOEの保証要件の評価証拠として提出した資料を識別する手段の変更。 | 2以上 |
| ・TOEを構成する要素及び保証要件の証拠資料を管理する手続き、権限、使用する管理ツールの変更。 | 3以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 4.2のチェックへ進む。 |
| 4.2 | TOEを調達者に配付する際、TOEのセキュリティを維持するための手続きに関して、以下の事項に変更がある。・TOEの各配付ポイントや調達者が受け取った後に実施すべき手続き。・手続きで使用する機能や手段。・セキュリティ維持のための配付手続きを実施する部門、施設、責任者。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 4.3のチェックに進む。 |
| 4.3 | TOEの開発環境における以下のセキュリティ対策に変更がある。・開発環境への物理的アクセス制御（入室制限など）。・開発資源（ファイルやツール等）への論理的アクセス制御。・開発環境における手続き（変更承認、持出し規制、訪問者取扱い等）。・開発スタッフの選定基準、手順。・セキュリティ対策実施・監視の責任者・役割。 | 3以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 4.4のチェックに進む。 |
| 4.4 | TOEの開発、製造、テスト、配付、設置、運用までの製品の一連の段階において、製品の管理に使用される手続き、ツール、技法（認証TOEにて定義されている）のいずれかに変更がある。 | 3以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 4.5のチェックに進む。 |
| 4.5 | TOEの開発ツール（プログラム言語、開発支援設計システムなど）に変更がある。 | 4以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 4.6のチェックに進む。 |
| 4.6 | TOEがICカード等のハードウェアである場合の製造プロセス（製造工程、製造装置など）に変更がある。 | － |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 4.7のチェックに進む。 |
| 4.7 | 認証TOEで評価されたTOEセキュリティに係る、以下のような障害情報の管理から開示までのプロセスの変更がある。・TOEセキュリティに係る問題報告受入れ手順・TOEセキュリティに係る問題管理手順と管理項目・TOEセキュリティに係る問題事項情報の利用者への提示手順 | ALC\_FLR適用時 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 5.1のチェックに進む。 |
| 5.1 | TOEのセキュリティ機能の既存のテスト項目に対する変更あるいは新たなテスト項目の追加がある。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 5.2のチェックに進む。 |
| 5.2 | 認証TOEにおいて実施したテストに対するリグレッションテストを実施した結果、動作が期待される結果と異なる項目がある。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 6.1のチェックに進む。 |
| 6.1 | 認証TOEにおいて宣言した保証要件以外の変更がセキュリティ事項に影響を与えている。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えている可能性がある。 |
| No | 6.2のチェックに進む。 |
| 6.2 | 認証TOEに対する認証時点からのすべての変更を対象に、複数の変更がある場合に、個々の変更については影響が小さいことを論証することができるが、複数の変更を組合せた場合に影響が小さいことを論証することができない。 | 1以上 |
| Yes | 変更が認証維持の範囲を超えているため再評価が必要。 |
| No | 認証TOEと変更TOEの差分に対し、セキュリティに影響がないことを分析し、その結果を「影響分析報告書」として報告する。 |

【手順2】

該当項番の補足説明を参考に、再評価の検討をしてください。再評価の必要がないと判断でされた場合、その根拠となる分析を「影響分析報告書」に記述することを留意し、手順1のチェックを再開してください。

| 項番 | 再評価のための補足説明 |
| --- | --- |
| 1.1 | 認証書の有効期限を超えている、又は、有効期限間近の認証TOEに対しては、認証維持申請はできません。 |
| 1.2 | 認証TOEと変更TOEの名称やバージョンが異なる場合や動作プラットフォームの追加など、調達者が理解できる変更点に関する記載が可能である必要があります。例えば、以下のような場合には、認証TOEと変更TOEとのバージョンの変更や識別手段の提供等を検討する必要があります。・TOE自体にバグ修正や内部仕様の変更があるにも係らず、TOEの名称やバージョンに反映されない。・TOEの動作環境に追加があるが、調達者に対して適切な変更説明を提供できない。 |
| 1.3 | TOE名称の変更が、単純な製品商標の変更を反映したもの（機械的な文字列上の置換）であれば、STにおける意味的な変更はなされないと思われます。しかし、TOE名称が機能や評価範囲を含んでいるような場合、変更された結果、TOEの名称が示す機能性や評価の範囲が、ST読者がそのTOEの種別から期待する機能性や、評価の範囲と一致しなくなる可能性があります。TOE名称の変更においては、STで説明されているTOEの種別や範囲を反映したTOE名称となることが前提となります。 |
| 1.4 | セキュリティ機能仕様に対する変更は、評価を要する事項となり、認証維持の対象となりません。ただし、ソースコードの変更が上位設計のレベルではまったく影響なく、仕様の変更がないなど、保証レベルに応じて変更の内容を判断することになります。ガイダンス（運用マニュアルの他、インストール・セットアップガイド等も含む）における、セキュリティ事項に関する変更は、TOEの利用者への影響が顕著であり、再評価を要する事項となります。ただし、TOE名称やバージョンの変更に伴う記述の変更など、セキュリティ事項と関連しない変更であれば、その内容が影響を及ぼさないことを分析する作業となります。変更TOEでは、リグレッションテストの結果を示す必要がありますが、テストの範囲は認証TOEで宣言した機能の確認を超えるものではありません。認証TOEの認証取得以降に発見された新たな脆弱性や脅威に対するテストも、認証維持の範囲ではありません。ここで、変更の影響について判断ができない場合には、再評価を要すると考えてください。また、変更によりセキュリティに係る仕様や保証への影響はない、あるいはほとんど影響がないと判断された場合には、手順1に戻りチェックを継続し、さらなる詳細なチェックを行います。 |
| 1.5 | STとの整合は、変更TOEにおいても必須となります。TOEの名称変更やSTの更新に伴う識別情報や更新情報については、多くの場合セキュリティ事項に影響を与えませんが、前提条件、脅威、OSP、機能要件や保証要件が変更された場合には再評価が必要となります。TOEの動作環境が追加された場合、その環境自体の完全な互換を証明できない限りは、新たに追加された環境での評価が必要となります。完全な互換を証明できるとは、自社で製作しているハードウェアの物理的なデザインや名称など、ソフトウェアであるTOEの動作に影響がないことを、影響分析報告書において責任とともに説明できることを意味します。変更箇所や互換に関する十分な証拠のない他社ハードウェアやソフトウェアに対応する場合、セキュリティ機能への影響を評価するために再評価が必要となります。保証手段として記述された、開発者証拠の名称やバージョンの変更については、実際に変更された内容に十分な注意が必要です。保証手段（各種手順や仕様など）の内容に係らない変更であると判断した場合、その変更が影響ないことを分析し、確認することになります。保証手段に係る変更であった場合、新たな保証手段を適用した環境での再評価が必要となります。 |
| 2.1 | 多くの評価は機能仕様（セキュリティ機能インタフェースの目的と使用方法）に基づいて実施されます。セキュリティ機能の要件が正確に機能仕様に反映されていることが評価の前提となっています。そのため、機能仕様への変更は再評価が必要です。インタフェースの変更とは、直接的なパラメタやふるまいのほか、セキュリティ機能に係る管理データ、構成ファイル、出力ファイルの仕様変更なども含まれます。エラーメッセージの変更は、多くの場合明示的な機能仕様やソースの変更を意味しますが、セキュリティ機能が依存する下層の変更に起因する場合もあります（セキュリティ機能実施の延長で発生した資源確保に関するエラーなど）。このようなエラーメッセージについては、表記上の差異の範囲と判断可能であれば、そのエラーメッセージが変更TOEにおいてもセキュリティ事項に関与しないことを分析することとなります。エラーメッセージの変更が意味的なものであり、その影響が判断できない場合には再評価となります。CC Ver3.1以降では、SFR実施、支援等の分類があります。それぞれのインタフェースがどの分類かは、認証TOEの評価報告書に記載されているはずです。 |
| 2.2 | TOEのセキュリティ機能の外部インタフェースの変更がない場合も、サブシステムレベルでは、それぞれのふるまいやサブシステム間のやりとりに変更があるかもしれません。セキュリティ機能の実施において、TOEがどのように設計され機能するかを入力とし、セキュリティ機能の実装の妥当性を評価します。よってサブシステムの変更は、評価の入力が更新されることを意味し、再評価が必要となります。非SFR実施と主張されたサブシステムの変更でも、評価において非SFR実施であることを決定する必要があるため、再評価の対象となります。 |
| 2.3 | サブシステムは評価者が独自に行うテストや脆弱性の評定への重要な入力となります。EAL4のレベルにおいては、ソースコードなどの実装レベルのガイドとなるモジュールレベルで同様の目的のための情報が求められます。よって、モジュールの変更は、評価のための入力が更新されたことを意味し、再評価が必要となります。モジュールのふるまいには、実現する機能が同じ場合も、アルゴリズムや実装の変更（ローカル変数からグローバル変数への変更）により異なる場合があります。非SFR実施と主張されたモジュールの変更でも、評価において非SFR実施であることを決定する必要があるため、再評価の対象となります。 |
| 2.4 | TOEのセキュリティ機能の設計、実装の妥当性と同様に、それらの機能を保護する仕組みも評価の対象となります。セキュリティ機能を保護する仕組みについては、EAL2や3であればサブシステムレベルで、EAL4であれば実装レベルでの情報を評価の入力とします。これらの仕組みに対する変更が、認証TOEを取得した評価保証レベルで影響があるか分からない場合、再評価の対象となります。また、セキュリティ機能ではない新たな外部インタフェースが、セキュリティ機能に影響を与えるかが分からない場合もやはり再評価の対象となります。影響がないことが明らかであれば、その変更内容が影響を及ぼさないことを、評価保証レベルの詳細度で分析します。 |
| 2.5 | ソースコードのような実装表現は、EAL4のような高い保証レベルを得るためには、評価者テストや脆弱性評定の入力としては重要であり、該当する変更は再評価を要します。 |
| 3.1 | ある利用者にある種の機能の実行や資源の使用を許すが、他の利用者にはそれが許可されないなど、利用者の役割（機能）と権限について明確な説明がガイダンスに記述されています。利用者の役割と権限について変更があった場合、ガイダンスのみならず、他の評価証拠資料（機能仕様やSTなど）との整合性とともに、利用者がセキュアな環境と管理すべき事項が明確に指示されているかの再評価を必要とします。 |
| 3.2 | TOEをセキュアに運用するため、管理者や一般利用者それぞれの役割が行わなければならない操作または関連するセキュリティ事項について変更がある場合、TOEのセキュアな使用のための情報、セキュアでないことの検出について、ガイダンスが誤解なく利用者に提供されていることを再評価する必要があります。セキュアなTOE使用のための管理コマンドの使用条件や資源アクセス時の利用者の手順、バックアップの頻度やパスワード品質に係る指針などの変更、管理や資源のセキュアな使用に必要とされるセキュリティインタフェースでの各種メッセージや構成ファイルにおけるデフォルト値の変更、さらには障害やセキュリティに係る事象発生時に必要となるセーフモードでの操作や退職者のアカウント管理などの変更が行われた場合、それらの内容が明確かつ合理的に利用者にガイダンス等で指示されていることを、機能仕様や設計あるいはSTに記述された運用環境などとの整合を踏まえて評価する必要があります。よって、これらの変更は認証維持の範囲を超えていると判断します。 |
| 3.3 | ガイダンスに記載されているTOEの運用準備や環境構築の手続きが変更されると、多くの場合、TOEの動作や脆弱性分析に影響を及ぼす可能性があります。しかし、TOEのパッケージの開封確認手段だけが変更された場合や、インストールプログラムの操作画面のメッセージだけが変更された場合のように、運用中のTOEの動作や脆弱性分析には影響を与えない場合もあります。TOEの運用準備や環境構築の手続きの変更が、TOEの動作や脆弱性分析に影響を及ぼさないことを、開発者が論証できる場合、認証維持の対象となります。ただし、変更された手続きが適切なものであるかのサブセット評価を伴います。TOEの運用準備や環境構築の手続きの変更が、TOEの動作や脆弱性分析に影響を与える可能性がある場合には、再評価が必要となります。 |
| 4.1 | TOE識別の提供は、調達者が適切なTOE（評価されたTOE）を使用していることを保証することになります。この手段を変更した場合、TOEの構成管理だけでなく、TOEのガイダンスやテストにも影響が及びます。そのため、適切なTOEの使用の保証ができることの再評価が必要となります。TOEを構成する個々の要素の識別と管理（追跡性）は、TOEの開発・修正手続きが適切であり、TOEが一意に識別できることを保証するものです。たとえば、ソースコードを修正したものが、前のバージョンとは異なるTOEの構成要素となり最終的にどのTOEを形成することを追跡できる、構成要素を管理する手順、権限が明確であり、それに従い運用されているなどは、開発過程において意図しない設計の実装が紛れ込むことを防ぎます。それらの構成管理に関する変更が、TOEを識別する手段やガイダンスなど、構成管理以外の部分に影響を及ぼさないことを、開発者が論証できる場合、認証維持の対象となります。ただし、変更された構成管理の手続き等が構成要素を適切に管理できるかのサブセット評価を伴います。構成管理の構成要素は、認証TOEで採用された保証要件により、機能仕様書やソースコード、開発に用いるツール、セキュリティ欠陥報告記録などが対象となります。それらの構成要素の変更に伴って、構成要素に付けられるバージョン番号等の識別子が、評価された手順に従って更新されることは問題ありません。 |
| 4.2 | セキュリティ維持の配付手続きは、TOEを製造環境から調達者が受け取り設置環境へ移動するまで、パッケージング、保管、配送といったすべての過程を含みます。手続きとしては、完全性維持のため、シュリンクラップパッケージやセキュリティシールにより、改ざんの有無を調達者が確認したり、機密性維持のためデータを暗号化し、調達者に別経路で鍵を送付したりする方法があります。配付手続きに関する変更が、TOE機能やガイダンスなど、配付手続き以外の部分に影響を及ぼさないことを、開発者が論証できる場合、認証維持の対象となります。ただし、変更された配付手続きがセキュリティ維持に適切なものであるかのサブセット評価を伴います。また、配付手続きの変更に伴って受入れ手続きだけが影響を受け、受入れ手続き以外のガイダンスやTOE機能に影響を及ぼさないことを、開発者が論証できる場合にも、認証維持の対象となります。この場合は、変更された配付手続きと受入れ手続きを記述したガイダンスのサブセット評価が必要です。配付手続きに関する変更が、配付手続きと受入れ手続き以外の部分に影響を与える可能性がある場合には、再評価が必要となります。 |
| 4.3 | 開発環境のセキュリティ手続きの安易な変更等によりこの段階で持ち込まれた脆弱性は、運用の段階でTOEのセキュリティに多大な影響を与える可能性があります。また、開発作業を外部に委託するなどTOEの機密情報の開示範囲や管理レベルが変わると、TOEの脆弱性評定、つまり、TOEに対する攻撃のしやすさに影響を与える可能性があります。開発環境のセキュリティに関する変更が、TOEの脆弱性評定に影響を及ぼさないことを、開発者が論証できる場合、認証維持の対象となります。ただし、変更された手続きがTOEの設計情報等の保護に適切なものであるかのサブセット評価を伴います。開発環境のセキュリティに関する変更が、TOEの脆弱性評定に影響を与える可能性がある場合には、再評価が必要となります。 |
| 4.4 | TOEのライフサイクルが定義され、各段階で使用される手続き、ツールあるいは技法が、開発や保守で必要となる管理方法であれば欠陥がTOEにもたらされる可能性が減少すると考えられます。用いられるコーディング規約やテスト手法の変更や管理体制や責任範囲の変更などは、品質への確信が変わる可能性があります。ライフサイクルに関する変更が、TOEの品質に影響を及ぼさないことが論証できる場合、認証維持の対象となりますが、変更部分のサブセット評価を伴います。ライフサイクルに関する変更が、TOEの品質に影響を及ぼす可能性がある場合、再評価が必要となります。 |
| 4.5 | TOE開発に用いられるツール（プログラム言語、開発支援など）が、認知された標準のものではなく明確なシンタクスが完全に明らかにできないような場合や、標準ツールであっても実装依存や独自の機能が含まれる場合、プログラム言語と実行オブジェクトの間の一貫性を決定できません。また、開発者の意図と異なる実行オブジェクトが、脆弱性の要因になる可能性もあります。認証TOEとは異なるツールで開発されたTOEは、この点に関して再評価が必要となります。仕様変更がなく、かつ同じ使用方法でリビジョン違いのコンパイラを用いた結果は、TOEに大きな影響を与えないかも知れません。一方、同じリビジョンのコンパイラでも、異なるコンパイルオプションを用いた結果は、実行可能コードの意味に影響を与える可能性は高いと言えるでしょう。開発ツールの変更が、実行可能コードの意味に影響を及ぼさないことを、開発者が論証できる場合、認証維持の対象となります。影響について明確な証拠がない場合、再評価により保証を得る必要があります。 |
| 4.6 | TOEがICカード等のハードウェアである場合、TOEの製造プロセスが変更されると、TOEの物理的特性が変わり、物理的な攻撃に対する耐性が変化する可能性があります。そのため、TOEの製造プロセスの変更によって、TOEの物理的特性への影響の可能性がある場合、物理的な攻撃に対する耐性の再評価が必要となります。 |
| 4.7 | 認証TOEにおいては、TOEにセキュリティ上の問題が発見された場合、開発者が詳細及び対応状況を共有・追跡でき、また必要な関連情報を利用者に届けるための手続きが確立していることを保証されています。これらの欠陥修正の手続きに関する変更が、TOE機能やガイダンスに影響を及ぼさないことを、開発者が論証できる場合、認証維持の対象となります。ただし、変更された手続きが適切なものであるかのサブセット評価を伴います。欠陥修正の手続きに関する変更が、TOE機能やガイダンスに影響を及ぼす可能性がある場合、欠陥修正の手続きだけでなく、TOE機能やガイダンスを含めた再評価が必要となります。たとえば、バグ修正に関する利用者通知が、ダイレクトメールからWeb公開に変わった場合は、その情報を利用者が確実に得るための手続きやガイダンス等が適切であることを再度評価することになります。なお、本チェックは認証TOEにおいて保証クラスALC\_FLRが保証の範囲として宣言されていた場合にのみ対象となります。 |
| 5.1 | テストの変更や追加がある場合、その要因はTOEセキュリティ機能の変更によるものと考えられ、再評価が必要となります。ただし、テスト環境変更が、TOEの外であるハードウェアの性能改善版やTOEのセキュリティ機能が依存しない下層のソフトウェアのリビジョンアップ版を用いたことによるもので、またTOEのインタフェースに変更がない場合、TOEのテスト証拠資料への影響がないこともあります。このような、変更に対する確認テストは、既存のテストとは別に、分析の結果として報告書に示されることとなります。また、変更TOEは認証TOEと同等の機能を有することを期待されており、認証TOE取得後に顕在化した脆弱性などへの対処は認証維持の範囲ではありません。 |
| 5.2 | 変更結果が、セキュリティ機能に予期しない影響を与えていると判断され、認証維持の対象とはなりません。 |
| 6.1 | 基本的に、認証TOEにおいて宣言した保証要件以外の変更が、TOEのセキュリティに影響を与えることはないと考えます。たとえば、EAL2ではソースコードの変更が機能仕様及びサブシステムのレベルで変更がなければ、TOEの保証に影響はありません。しかし、TOEセキュリティに関連する事項が、認証TOEで評価された証拠以外に挿入されるような場合があることに注意が必要です。セキュアな状態を維持するための手続きとして識別されていない文書に、TOEのセキュリティに係る事項が追記された場合は、新たな手続きとして再評価が必要になるかもしれません。開発者は、変更対象が認証TOEで用いられた証拠か否かに係らず、その変更点が保証レベル内で影響がないことを分析しなければなりません。 |
| 6.2 | 単独では影響が小さい変更であっても、それらが累積的にあるいは相互作用として、TOEに大きな影響を与えることが考えられます。たとえば、ソフトウェアの不具合を解決するための複数のパッチが、別々に開発された場合、個々のパッチ単独では問題がなくても、複数のパッチ間で内部的な不整合が発生し、セキュリティに影響を与える可能性があります。また、数多くの変更がされた場合、変更の組合せによる影響が多岐に渡り、開発者が変更全体の影響が小さいことを客観的に論証することが難しくなります。開発者は、個々の変更の影響だけでなく、認証TOEに対する認証時点からのすべての変更の組合せがセキュリティに影響を与えないことを論証しなければなりません。論証ができない場合には、再評価によって客観的な保証を得る必要があります。 |