JISEC-CERT-2022-C21

JISEC

影響分析報告書
作成ガイダンス

第 2.1 版

独立行政法人情報処理推進機構 JISEC

2022 年 4 月 1 日　発行

改訂履歴

版数	発行日	おもな変更点
2.1	2022/4/1	JISEC 規程及び所属の名称変更

目　次

1. はじめに

本書は、保証継続申請を検討する際の参考として、TOE 及び環境に対する変更が、保証継続の範囲内であるかの判断についての考え方及び保証継続申請に必要な「影響分析報告書」の記載内容についての事例を示したものです。

保証継続の意義やプロセスについては「保証継続：CCRA 要求事項」[1]を、保証継続制度に関する規程や手続きについては「IT セキュリティ認証等に関する要求事項（CCM-02)」[2]及び「IT セキュリティ認証申請等のための手引(CCM-02-A)」[3]を参照してください。

2. 用語

本ガイダンスで使用する用語は、「保証継続：CCRA 要求事項」[1]の定義と同義です。下記に主な用語の定義を記載します。

・認証 TOE

評価がされ、既に「認証書」が発行された TOE のバージョン。

・変更 TOE

認証 TOE あるいは認証 TOE のセキュリティに係る開発環境や運用環境に対する変更がなされたバージョン。

・開発者証拠

TOE の評価の際に評価機関に提出しなければならないすべての証拠資料。

・保証継続

認証 TOE 及び環境に対して行われた変更を識別し、過去の評価を活用して保証を与えること。「認証維持」と「再評価」が含まれる。

・認証維持

認証 TOE に対する変更が、認証時点の保証に悪影響を及ぼしていないことを確認すること。

・再評価

認証維持ができない場合に、評価機関が新規の場合と同等の評価を行うこと。

・サブセット評価

認証維持が可能な場合で、開発環境の保証手段の変更が含まれている場合に、評価機関が開発環境の変更によって影響のある保証コンポーネント（例えば ALC_DEL.1）だけを評価すること。

3. 保証継続適用の判断について

認証維持が対象とする認証 TOE に対する「変更」は、認証 TOE から派生した新製品や新機能を意図するものではありません。認証 TOE で評価されたセキュリティ機能の範囲において、ソフトウェアやガイダンスの不具合の修正や TOE の機能自体に変更のない動作環境の追加など、第三者による評価を実施せずとも、開発者（申請者）が自らの責任で保証に対する悪影響がないことを実証ならびに宣言できる「変更」のみが認証維持の条件となります。

基本的に、認証 TOE の変更については、評価者による評価に影響を与えないこと、つまり、認証 TOE の評価に用いられた開発者証拠の内容が意味的には変更されないことが認証維持の条件となります。また、認証 TOE の開発環境の変更については、開発環境の変更の影響が開発環境の範囲にとどまり、認証 TOE に影響を及ぼさないことが認証維持の条件となります。そのため、認証維持可能な開発環境の変更には、認証 TOE の変更の場合とは異なり、評価者による評価に影響を与える変更も含まれることになります。ただし、その場合の認証維持では、評価者によるサブセット評価が必要となります。

開発者は、認証 TOE 及び環境に対する「変更」について、認証 TOE のセキュリティの保証に対する影響を分析し、セキュリティ上の大きな影響を与えるもの（major）であるか、影響が小さいもの（minor）であるかを判断します。認証 TOE 及び環境に対する変更が、セキュリティ上小さな影響(minor)にとどまることを開発者が客観的に論証することができれば、認証維持の対象となります。

例えば、TOE が提供するセキュリティ機能に関する実装の変更や、ガイダンスに記載されている注意事項や使用方法などの変更は、影響が大きいと考えられます。一方、セキュリティ機能とは関係のない出力メッセージの修正や誤字によるガイダンスの修正などは、影響は小さいと考えられます。また、開発環境における入退出管理のしくみや手続きなどの変更は、認証 TOE の機能やガイダンスに影響を及ぼすことはないため、影響は小さいと考えらえます。

ただし、認証 TOE 及び環境に対する「変更」が、セキュリティ上の大きな影響を与えるもの（major）であるか、影響が小さいもの（minor）であるかの判断は、ここで述べられている例を含め、絶対的な指標はありません。

変更がセキュリティ上どのように影響があるかの判断は、認証 TOE の保証範囲の理解と開発者分析による論証により行われます。変更が、認証 TOE の保証範囲に明らかに係らない場合、変更 TOE は認証維持の対象となります。変更が、認証 TOE の保証範囲に影響を及ぼす可能性がある場合には、その影響が大きい(major)のであれば再評価が必要となり、影響が小さい(minor)のであれば、その論証とともに影響分析報告書を作成することになります。

変更が、認証 TOE の保証範囲に及ぼす影響の大きさを判断する参考資料として、付録に「認証維持適用のチェックリスト」を掲載してあります。内容は、それぞれの保証レベルではどのような項目が評価し保証されているかを簡単にまとめたものとなっています。変更箇所の個々の詳細な影響分析を開始する前に、変更が保証の範囲とどの程度の関連があるかをチェックすることで、影響分析報告書の作成をせずに再評価を決断したり、深い分析の対象を絞ったりす

ることができます。もちろん、再評価においても開発者による影響分析報告書は、評価者にとって有用な入力となるため、セキュリティ影響の範囲や保証継続申請に係らず、影響分析報告書を作成する選択もあります。

開発者は、変更 TOE の影響分析で、変更が認証 TOE の保証レベルに対して及ぼす影響が小さいことを論証します。この論証は、技術的背景とともに、十分な検査が開発者により実施された結果として報告されなければなりません。十分な検査は、認証 TOE の保証レベルよりさらに深いレベルで実施する必要があります。たとえば、TOE セキュリティ機能とは関連のない内部仕様の変更は、認証 TOE におけるセキュリティ機能の外部インタフェース仕様に直接的な変更をもたらさないという主張は不十分です。変更箇所の実装表現をたどった結果、セキュリティ機能の外部インタフェースの一部のパラメタやメッセージに影響があることが判明することもあります。動作環境の変更において TOE 外部インタフェース仕様に変更がないと主張する場合も、そのインタフェースの呼び出し手順、呼び出しタイミング、渡されるパラメタにより、認証 TOE では活性化されていなかったロジックを通る可能性を開発者は十分考慮するべきです。

認証機関は、開発者の提出した影響分析報告書を検査し、認証維持が可能か否かの判断をします。検査の過程で開発者主張の根拠に不明な点があれば、影響分析の過程の詳細な資料提供の要請や開発者との直接的な質疑を実施し、内容を確認します。影響分析報告書の記述内容については本書の 4 章を参考にしてください。

なお、認証書発行日から 2 年以上経過した TOE に関しては、本制度において認証維持の対象とはならないことに注意してください。また、認証 TOE が認証を取得した以後に発見された新たな脆弱性や攻撃手法への対抗についても、認証維持の範囲には含まれません。そのような場合に、安全な製品を供給するためには、再評価による保証を得る必要があります。

4. 影響分析報告書作成について

開発者は、変更が認証 TOE の保証の範囲にて不利な影響を及ぼさないと判断した場合、変更内容の分析を実施し、セキュリティへの影響を検査します。保証継続申請にあたり、影響分析の結果を報告書として作成しなければなりません。影響分析報告書に記載すべき最小限の内容は、「保証継続：CCRA 要求事項」[1]の 5 章に記述されています。

影響分析報告書は、変更が認証 TOE の保証範囲に影響を及ぼさないことが客観的に理解できるように、必要によっては非公開情報も含めて、十分詳細に記述しなければなりません。影響分析報告書は、認証機関より公開されることはありません。認証機関は、調達者に保証の維持が可能であることを報告するため、影響分析報告書をもとに「保証継続報告書」を作成します。「保証継続報告書」は開発者のレビューと同意を得たのち公開されます。

以下に影響分析報告書の作成において留意すべき点や例を、影響分析報告書の構成に従って示します。なお、章構成以外の記述形式は任意であり、必ずしも事例に従う必要はありません。

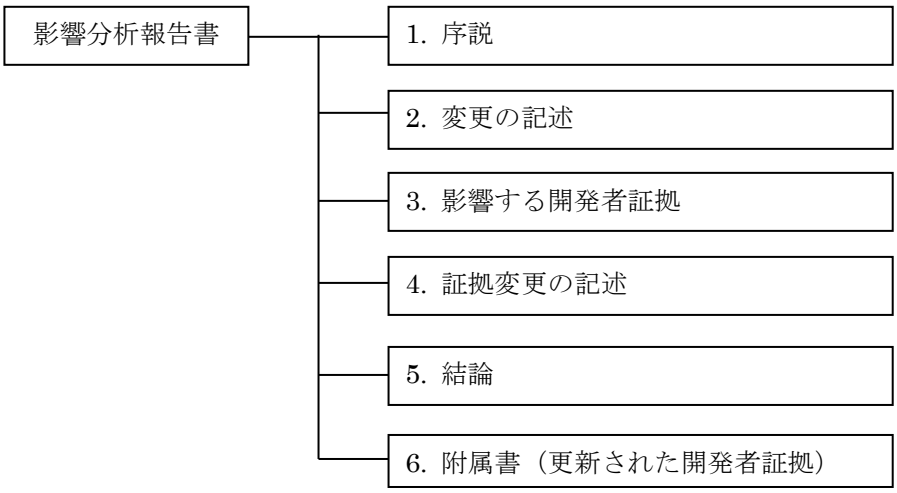

図 1　影響分析報告書の構成

(1)　序説

序説では、必要な各資料についての識別情報を記述します。また、当該報告書の取り扱いなど、開発者が特に注意を要すると判断した情報を含めることもできます。

1.1 影響分析報告書識別
名称:　JISEC Ewallet SecureTrade 影響分析報告書
バージョン:　1.0.1
作成日:　2022 年 2 月 2 日
作成:　JISEC 株式会社
1.2 TOE 識別
TOE 名称:　JISEC Ewallet SecureTrade
バージョン:　Rev. 3

開発者:　　JISEC 株式会社
1.3 認証 TOE 識別
認証番号:　　C0XXX
TOE 名称 :　　JISEC Ewallet SecureTrade
バージョン:　　Rev. 2
評価保証レベル:　EAL3
適合する PP:　　なし
:

認証 TOE の ST、評価報告書、認証報告書についても、同様に識別を記述します。

(2)　変更の記述

変更の記述では、認証 TOE 及び環境に対して行われた全ての変更について記述します。ここでは、その変更内容がセキュリティに影響を及ぼさないと判断されたものも含めて、すべて記述します。

変更の記述では、変更理由、TOE を含む製品に対する変更、開発環境に対する変更、IT 環境に対する変更をそれぞれ記述します。

①　変更の目的

変更の記述では、はじめに TOE の変更が必要になった背景を説明します。本節では、認証 TOE と比較して変更された内容を概要レベルで記述します。個々の変更点の詳細は次節以降で記述します。

2.1 変更の目的

認証 TOE に対し、新たな動作ハードウェアに関するガイダンスへの追記、性能上の改善及び不具合修正が行われている。以下に変更の概要を示す。

1）　TOE が動作する JISEC Ewallet に新たに Type D が追加されたため、その対応のためのガイダンス修正。これに関する TOE プログラム自身の変更はない。

2）認証失敗時の自動リブートに時間が掛かるため、ブート時間の短縮のためのプログラム修正。

3）ログ情報取得中のタイミングで、監査ログが規定容量に達しファイルのリネームが行われた場合、ログ情報が空となる実装バグのプログラム修正。

仕様変更のない小さなバグ修正などが複数ある場合、本節ではまとめて目的を述べ(実装における境界値の問題や性能改善など)、個々の内容については次節以降で言及してもかまいません。

②　製品に対する変更

本記述内容は、認証 TOE に対して行われた変更について記述します。記述の詳細度は、第三者（認証機関）が開発者による影響分析の主張を理解できるだけの情報を含むことが要求されます。場合によっては、認証維持の適用判断に必要な追加の証拠資料の提出

を求められることがあります。

変更した対象が何か（ソースコードなのか、手順書なのか)、なぜ変更したのか、具体的にどのように変更したのかを、認証 TOE の保証範囲への影響が理解できるように明確に記述してください。例えば、認証 TOE の保証レベルが EAL2 であれば、機能仕様及びサブシステムのレベルの影響が理解できるような詳細情報が必要であり、そのためには機能仕様やサブシステムのレベルの設計書に記述されないような詳細な情報が必要になる場合がありますが、ソースコードレベルでの記述までは求められません。

No.	変更種別	概要	詳細
S2-1	性能改善	認証失敗時の自動リブート時間の改善	ブートルーチンプログラムを変更し、ブート時に行う TSF パラメタ値の検証、ネットワークリリース及びネットワーク再構築について、認証失敗フラグが立ち、かつシステムエラーフラグが立っていない場合はそれらの処理をスキップするようにした。

③　開発環境に対する変更

本記述内容は、開発環境に対して行われた変更について記述します。認証 TOE において保証要件とされている範囲の変更について、影響が少ないと判断される点を含めてすべての変更点を列挙します。たとえば、構成管理における TOE の構成要素のバージョンの変更、構成要素の識別方法の変更、構成管理手順の変更など、すべての変更を記述します。

D3-1	開発セキュリティ	開発環境への入室制御機器の変更	社員カードの更新により、開発ルームへの入室制御機器が、旧社員カード（磁気）による認証から、新社員カード（非接触型 IC)による認証となった。入室手順等には変更はない。

④　IT 環境に対する変更

認証 TOE における IT 環境に対して行われた変更について記述します。これらは、TOE が依存する外部サービスなど、評価対象であるセキュリティ機能が必要とするハードウェア、ファームウェアそしてソフトウェア及び TOE の動作環境としてのハードウェア、ファームウェアそしてソフトウェアのすべてを対象とします。

E2-1	動作ハードウェア	動作ハードウェアの追加	動作ハードウェアである「JISEC SecureSwitch 07」の OEM 供給機「ISEC SS V.7」での動作保証の追加。

(3)　影響する開発者証拠

認証 TOE の評価において使用した開発者証拠に変更あるいは追加が必要となるものをすべて識別します。認証 TOE の評価において使用した開発者証拠は、認証 TOE の評価報告書に一覧が記述されています。

開発者は、先の変更の記述において示された TOE や環境に対する変更により、どの開発者証拠を更新する必要があるかを決定します。この決定については、認証 TOE のそれぞれの保証コンポーネントを考慮した体系的な方法で行わなければなりません。本項では、更新される開発者証拠の識別のみを記します。保証コンポーネントごとに影響の有無を「保証継続：CCRA 要求事項」[1]の 4 章「影響分析の実施」を参考に決定していきます。たとえば、下表のような開発者アクションエレメントごとに関連する開発証拠の詳細を識別し、その影響をチェックしていく方法などがあります。

開発者 アクションエレメント	開発者証拠
ASE_INT.1	JISEC SmartModule セキュリティターゲット　Version3.1
	ST 概説
ASE_CCL.1	JISEC SmartModule セキュリティターゲット　Version3.1
	適合主張
…	…
ATE_FUN.1	JISEC SmartModule 機能テスト仕様書

本項では、識別した開発者証拠から、更新が必要であるもののみを影響する開発者証拠としてリストすることが求められています。変更内容が、認証 TOE の保証の範囲とどのように関連し、どのように影響を与えるかについては、次項の記述となります。

(4)　証拠変更の記述

「(3)　影響する開発者証拠」で識別したすべての開発者証拠に対する変更について、概要を記述します。変更内容の記述レベルは、開発者証拠の変更の詳細を記述する必要はありませんが、開発者証拠のどこを(where)なぜ(why)何を(what)変更したかについて明確かつ簡潔に記述します。

本項では、保証コンポーネントごと、変更項目ごとあるいは更新される開発者証拠ごとなど、適当な単位でそれらの関連とともに変更内容を記載します。

JISEC EasyLAN 機能仕様書			
項番	No	変更内容	変更箇所
S1-1(F)	1	FDDI 非サポート対応として ・インストールメニューから FDDI を削除	2.1.2
	2	・エラー番号[4]の FDDI メッセージを削除。	2.5

S2-1(F)	1	ライセンスキーCD 検証プログラムに IPA 社用のコードの検証ロジックを追加。	3.1.1 A.3

開発者証拠の更新にあたっては、認証 TOE における機能が、変更以外の機能も含めて、正しく動作することを確認すること（回帰テスト）が要求されます。同様に、AVA クラスが保証コンポーネントに含まれている場合は、脆弱性に関しても影響がなかったことを確認します。これらは、認証 TOE に対して行われたテストの再実施などを通じて確認されるでしょう。セキュリティ機能に大きな変更がない場合でも、新たなテストを必要とすることがあるかもしれません。そのような場合、開発者はどのような目的でどのようなテストを追加実施したかを影響分析報告書に含める必要があります。

なお、認証 TOE 評価以降にあらたな脆弱性が顕在化している場合、認証維持ではそれらの保証を対象としないため、「再評価」を受ける必要があります。

(5)　結論

開発者証拠に対する影響を、影響が大きい（Major)変更か、影響が小さい（Minor）変更かの決定を、その判断理由とともに記述します。また、サブセット評価が必要か否かの決定と、その判断理由も記述します。

①　各変更における影響

開発者証拠に対するそれぞれの変更について、認証 TOE の保証へ与える影響を記述します。またその根拠についても、開発者が行った影響分析の結果を「(2) 変更の記述」、「(4) 証拠変更の記述」の内容と関連付けて概説します。

開発者は、その変更がどのような影響を及ぼすかについて、広範囲にかつ十分な深さで分析します。認証された保証範囲すべてについて、影響を及ぼさないことを分析するためには、認証 TOE の保証レベルよりも深いレベルでの分析が必要となります。例えば、あるモジュールのソースコードの変更が直接的な外部インタフェースの変更を伴わないが、間接的に呼ばれるセキュリティ機能のエラーコードに影響を与える場合があります。立上げスクリプトのわずかな変更も、他の機能が想定する立上げタイミングや処理時間に影響を与える場合があります。そのような影響がないことを技術的に説明することが必要です。さらに、開発者は、影響の分析に加えて、実際に予想外の影響がないことを確認する回帰テストも必要となります。

また、開発者は、開発者証拠の一貫性にも注意が必要です。例えば、TOE の表示するメッセージを変更した場合、機能仕様の他に、ガイダンスやテスト仕様にも影響が及びます。

変更に関する影響の分析結果から、開発者はそれらの変更が影響の大きい(Major)変更か、影響の小さい(Minor)変更かを決定し、その根拠とともに本項に報告します。影響が大きいか小さいかを判定する絶対的な指標は存在しません。一般的なガイドラインとし

ては「保証継続：CCRA 要求事項」[1]の 3 章「変更の特性」を参照してください。

【S3-3】クライアント通信切断時のタイムアウト時間の見直し			
本変更は、セキュリティ機能のサービス認証の後処理プロセスのエラー処理に係るプログラムの変更であり、それに伴う仕様書及び管理者ガイダンスへの影響がある。しかしセキュリティ機能の振る舞い及び管理者のセキュアな管理に係るインタフェースの直接的な影響は下記のとおり変更ないと判断され、本変更の影響は小さい(minor)ものと判断される。			
S3-3(F).1		「Flow Manager Utility 機能仕様書」における「サービス認証機能」の仕様において、後処理の影響は以下の通りである。 1）後処理の呼び出し方、パラメタの変更は一切ない。 2）後処理の最中において ・利用者及び他のモジュールとのインタラクションが存在しない。 ・（短縮された7秒間を含め）割り込まれる操作も存在しない。 3）後処理の完了において ・戻されるエラー番号に変更はない。つまりサービス認証機能のエラー処理のエラー番号[7]の場合と仕様の変更はない。 ・後処理の処理タイミングに依存する他の処理は存在しない。 ・管理者インタフェースに示されるメッセージタイミングが7秒早くなるが、S3-2(G).1 の通り影響は小さい。 「Flow Manager Utility 機能仕様書」の変更による影響は小さいと判断する。	ADV_FSP.2
S3-2(G).1		「Flow Manager Utility ガイダンス」の「サービス認証」において、エラーメッセージ表示までの時間についての記述変更（「約 10 秒後」→「3 秒後」）の影響は以下の通りである。 1）サービス認証起動から、エラーメッセージ表示までの時間に関与するセキュリティ管理項目はない。 2）エラーメッセージの表示内容に変更はなく、メッセージ確認後に管理者が取るべき行為も変更はない。 よって、「Flow Manager Utility ガイダンス」の変更による影響は小さいと判断する。	AGD_OPE.1

また、変更後の TOE においても認証 TOE と同じようにセキュリティ機能がふるまうことを確認した（回帰テストの）結果も記述します。変更部分が正しく動作することを確認するテストや、変更によって予想外の影響がないことを確認する回帰テストが、新し

く必要になる場合があります。新しく実施したテストの目的と結果も記述します。テストの手順や詳細な情報を影響分析報告書に記述する必要はありません。保証の維持を確認するために、開発者はどのような観点でそのテストを実施したかを記述します。

② 全体における影響

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。開発者は、個々の変更の分析とともに、それらが結果的に全体として TOE に与える影響についても分析を行います。本項では、分析結果から影響の大きさを決定し、その根拠とともに記述します。

【全体】変更全体の TOE への影響			
S1-F 及び S2-F はそれぞれ設置時と運用時における処理の変更であり、お互いのインタラクションは存在しないため、組み合わせによる TOE の動作への影響はない。 よって、変更全体の及ぼす影響は小さい(minor)と判断される。			
（根拠）		**個々の変更の影響の分析【S1-F】【S2-F】で示したように、それぞれの変更箇所は、異なる機能の中の別々の関数の中に閉じた処理であり、外部変数の変更など他プログラムに副作用を及ぼす可能性のある変更は一切ない。それらを組み合わせても新たな副作用が発生することはない。**	

(6) 附属書

当該変更に伴い更新された開発者証拠の識別及び項目一覧を記述します。

① 更新された開発者証拠の一覧

変更 TOE としての開発者証拠を特定するために必要な情報、すなわち開発者証拠の名称、及び発行日やバージョンなどを一覧として記述します。

② 更新された開発者証拠の項目一覧

変更項目を特定するために必要な情報、すなわち更新された各開発者証拠においての変更された項目と、変更箇所を一覧で記述します。影響分析に係らない軽度の変更（たとえば改訂に伴う承認日など）までを含める必要はありません。

5. 注意事項

認証維持の判断及び影響分析報告書の作成において、開発者が特に注意すべき点について、以下に示します。

(1) 開発者の責任

認証維持では、変更 TOE に対して客観的な第三者評価の保証を継続して適用できることの技術的な判断を、開発者が自ら行い調達者に対して宣言することになります。開発者は、変更 TOE に何らかの問題が発生したときには、変更の影響についてどのような分析をおこなったかを検証できる資料の提示など、説明責任を伴うことを認識の上で、認証維持の判断をしてください。

(2) 影響分析報告書の記述

認証機関は、提出された影響分析報告書により個々の変更が保証に与える影響を決定します。影響分析報告書は、認証機関が変更の影響を客観的に理解できるように、技術的分析に裏付けられた根拠の記述が必要です。

影響分析報告書において「影響がないと思われる」など技術的分析を含まない主観的な宣言や相反する分析結果があるなど、認証機関が変更内容や分析根拠の確認を必要と判断した場合、開発者に開発者証拠あるいは追加の証拠資料を求めることがあります。

参考文献

[1] 保証継続：CCRA 要求事項, バージョン 2.1, 2012 年 6 月
[2] IT セキュリティ認証等に関する要求事項（CCM-02），情報処理推進機構
[3] IT セキュリティ認証申請等のための手引（CCM-02-A），情報処理推進機構

付録：認証維持適用のためのチェックリスト

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 における認証書発行日から 2 年以上経過している。		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。	

項番	チェック項目		EAL
	判定	認証維持可否の判断	
	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。	

項番	チェック項目		EAL
	判定	認証維持可否の判断	
	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。		1 以上

項番	チェック項目		EAL
	判定	認証維持可否の判断	
	・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。		
	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

項番	チェック項目		EAL
	判定	認証維持可否の判断	
	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	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	認証後の経過年数が 2 年を超えている TOE は、認証維持の対象とはなりません。
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

項番	再評価のための補足説明
	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。

項番	再評価のための補足説明
	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

項番	再評価のための補足説明
	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、

項番	再評価のための補足説明
	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

項番	再評価のための補足説明
	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。よって新たな脆弱性に対する確認テストのようなものは、保証継続の枠組みとは独立した作業となります。
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、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。