保 証 継 続:

CCRA 要求事項

管理: CCDB
識別子: 014
バージョン: 3.0
ステータス: 最終
発行日: 2023-March-09
承認: CCMC

令和 5 年 12 月 翻訳第 1.0 版

独立行政法人情報処理推進機構
セキュリティセンター
セキュリティ技術評価部

目次

1 序論

本文書は、コモンクライテリア承認アレンジメント (CCRA) の下で相互承認可能なアプローチを定義することを目的とし、認証維持、再評価及び再評定のアクティビティを合わせて保証継続と呼ぶ。このアプローチの定義にあたり、「保証継続：CCRA要求事項」は、相互承認されるべき保証継続アクティビティをCCRA加盟国が実施するために求められる最小限の技術的要件を定義することのみを目的としている。

本文書は、保証継続の実施に関して、加盟国が更なる要件を追加することを妨げるものではない。本文書は、コモンクライテリア　バージョン3.1に対応するために改訂されている。

1.1 適用範囲

本文書は、CCの概念に基づき、CC認証製品の認証維持、再評価及び再評定に関する最小限の要求事項としてCCRA加盟国が使用できるように考案されている。

1.2 アプローチ

本文書は、次の観点から保証継続を扱う。

a) 認証維持、再評価及び再評定に関わるプロセスの記述を含む、保証継続の枠組みの根拠を示す技術的概念の説明

b) 変更の特性に関するガイダンス（該当する場合）

c) 影響分析の実施に関するガイダンス（該当する場合）

d) 影響分析報告書の内容と記述に関する要求事項（該当する場合）

1.3 構成

本文書は5章からなる。序論 (第1章)、本書における技術的概念 (第2章) 、変更の特性に関する議論 (第3章)、影響分析の実施方法 (第4章)、影響分析報告書の内容と記述に関する要求事項 (第5章)。

2 技術的概念

2.1 保証継続の目的

保証継続の目的は、開発者がIT消費者コミュニティに対して、タイムリーで効率よく保証された製品の提供が可能となることである。

コモンクライテリア評価認証書の授与によって、IT製品又はシステムがセキュリティ対策方針を満たしているという確信を基盤として、TOEが定義された保証要件を全て満たしているということを評価監督機関（認証機関）に納得させるために必要な評価作業が全て行われたということが示される。

保証継続は、認証TOEやその環境に対しての変更を行うことによって、以前実施された評価作業があらゆる状況において繰り返される必要がないと認めるものである。したがって、保証継続は、ITセキュリティ評価の重複を最小限に抑え、個別の評価者アクションが再度実施される必要があるかどうかの決定を可能とするアプローチを定義している。

2.2 用語

明確にするために、次の用語は本パラダイムの記述に使用される。

a) *認証TOE* とは、評価されて認証書が発行されたTOEのバージョンを表す。

b) *変更TOE* とは、認証TOEに対して部分的に変更が加えられたバージョンを表す。例えば次のものである。

- TOE又はTOEが機能の一部となっている製品の新しいリリース
- 発見されたバグを修正するために適用されるパッチ適用済の認証TOE
- 認証TOEと同様の基本バージョンであるが、新たなセキュリティターゲットに追加された新たな運用環境 (例えば、異なるハードウェア又はソフトウェアプラットフォーム) にあるTOE

c) *維持TOE* とは、認証TOEに対して認証維持プロセスを経て、以前の認証の適用される変更TOEを表す。つまり、認証TOEに与えられた保証が、維持TOEにも適用されることを意味している。

d) *再評定TOE* とは、*再評定* を経た、以前の*認証TOE* を表す。

e) *認証維持追加情報* とは、認証製品リストの注記のように、認証TOEの認証書に追加される追加情報を表す。認証維持追加情報には、維持TOEのバージョンが記載される。更新された認証書の発行は行わない。

f) *影響分析報告書 (IAR)* とは、認証TOEへの変更の影響分析が記録された報告書を表す。IARは、認証維持追加情報への追加を希望する開発者によって作成される。

g) *認証維持報告書* とは、認証維持プロセスで受入れられた認証TOEに対して行われた変更が記述されている、公開された報告書を表す。

h) *再評定報告書* とは、TOEのバージョン、適用可能なガイダンスのリスト、及び到達したAVA_VANレベルを識別する報告書を表す。この報告書はスポンサーの選択に応じて公開される。

i) *保証ベースライン* とは、評価者と開発者の両方によって行われたアクティビティの結果、すなわち認証TOEに対する証拠として記録されたもの、又は提出されたもので、その証拠に対する変更が測ることができるものを表す。

j) *開発者証拠* とは、TOE評価の際に評価者に対して提供される必要な全ての項目を表す。

k) *認証維持* とは、認証TOE (又は*開発環境* の観点) に対して行われた一つ又は複数の変更が、当該TOEの保証に不都合な影響を及ぼしていないことを確認するためのプロセスを表す。

l) *再評価* とは、認証TOE (又はその他の保証手段) に対して行われた変更によって、新たな保証ベースラインを確立するために行われる独立した評価者アクティビティが要求されることを確認するためのプロセスを表す。再評価は、以前の評価の結果を再利用しようと努める。

m) *再評定* とは、必要に応じて関連する侵入テストを含め、初回に認証された製品の脆弱性分析を、セキュリティターゲットで当初要求されたのと同じレベルで更新するプロセスを表す。*再評定* は*臨時に* 又は定期的に実施できる。これは、TOEは変更されていないが、攻撃に関わる各種状況の変化を評定して、TOEが初回に認証されたときと同じレベルの耐性に今もなお達しているかどうかを確認する必要がある場合の、*再評価* の特殊な場合と見なすことができる。

n) *開発環境* とは、TOEの開発、配付、立ち上げ、欠陥修正に関する全ての手順のことをいう。AGD_PREファミリと共に、ALCクラスでカバーされた全ての概念を含む。

o) *サブセット評価* は、TOEへの小さな変更に開発環境への変更が含まれる場合に適用される。承認を受けたCC評価機関は、開発環境への変更により影響を受ける保証コンポーネントを識別し、その変更を踏まえた上で、それらの保証コンポーネントのみについて再評価を行い、*部分的ETR* を作成する。

p) *部分的ETR* は、*サブセット評価* の出力である。*サブセット評価* を行った承認を受けたCC評価機関によって作成され、影響を受けた保証コンポーネントについて、当初の認証TOEのETRのセクションに相応の詳細度で提供される。

q) 評価監督機関（認証機関）とは、評価制度によって、特定のコミュニティのためにCCを運営する機関であり、従って規格を制定し、そのコミュニティにおける機関によって行われる評価の品質を監理する。この用語が使われるときは、評価

監督機関（認証機関）そのもの、又は評価監督機関（認証機関）の代理に任命された機関を意味する。

当初の評価を受けた製品又はシステムをTOEと表す。当初の評価が完了して認証書が授与されたならば、それは認証TOEとなる。認証TOE（変更TOE）の後続のバージョンが認証維持追加情報に追加された後、そのバージョンが維持TOEとなる。

2.3 前提条件

本文書は、次の前提条件を考慮して書かれている。

a) 評価監督機関（認証機関）は、開発者及び開発者提供証拠を適切なレベルで信頼していると想定される。

b) 評価監督機関（認証機関）は、保証継続の実施の基準として、スキームが「保証継続：CCRA要求事項」を使用するが、本文書に記述されている以上の要件を含んでもよいと想定される。

c) CCRAにおける認証維持について、開発者は、当初の評価が実施されたところと同じ評価監督機関（認証機関）のみにIARを提出できるものと想定される。

d) 大きな変更及び小さな変更の特性において、複数の評価監督機関（認証機関）の間で一貫性があることを保証する手段があるものと想定される。

2.4 保証継続の枠組み

保証継続は、認証TOEやその環境に変更が加えられた場合、以前に実施された評価作業を必ずしも全ての状況で繰り返す必要がないという事実を活用しようとするものである。そのため、保証継続の枠組みは、*認証維持*、*再評価* 及び*再評定* のプロセスを定義し、それぞれが以前の評価作業を承認するためものである。

認証維持とは、開発者によって実施されるプロセスで、そのTOEについての認証維持追加情報を追加するためのプロセスを表す。TOE、IT環境、開発環境 への変更が、保証ベースラインに悪影響を与えないことが論証されなければならない。

再評価とは、開発者が認証TOEへの変更が保証ベースラインへ悪影響を与えないことを論証できなかった場合（又は論証しないことを選択した場合）に、変更TOEに対する評価を表す。

再評定とは、攻撃に関わる各種状況の変化に対する、以前に認証されたTOEの評価を表す。

認証維持プロセスは、初回認証の日以降に発見された新たな脆弱性又は攻撃手法に対するTOEの耐性に関しては保証を与えるものではないことに留意することが重要である。そのような保証は、再評価又は再評定によってのみ得ることがで

きる。認証維持では、保証ベースラインへ与えるTOE変更の影響のみを考慮しており、進化していく攻撃に関わる各種状況を考慮するものではない。

図2.1と図2.2は、保証継続の主な経路を示す。認証維持と再評価の両方のプロセスは、同じ出発点、つまり、認証TOEに対する変更が行われた場合[ボックス1]から始まる。本変更には、発見された不具合の修正用に作られたパッチ、機能の強化、新機能の追加、ガイダンス文書の明確化、又は認証TOEに対するその他の変更等がある。再評定の具体的な例は、認証TOEに何の変更もされていないが新規の脅威又は攻撃技術が考慮される場合である。

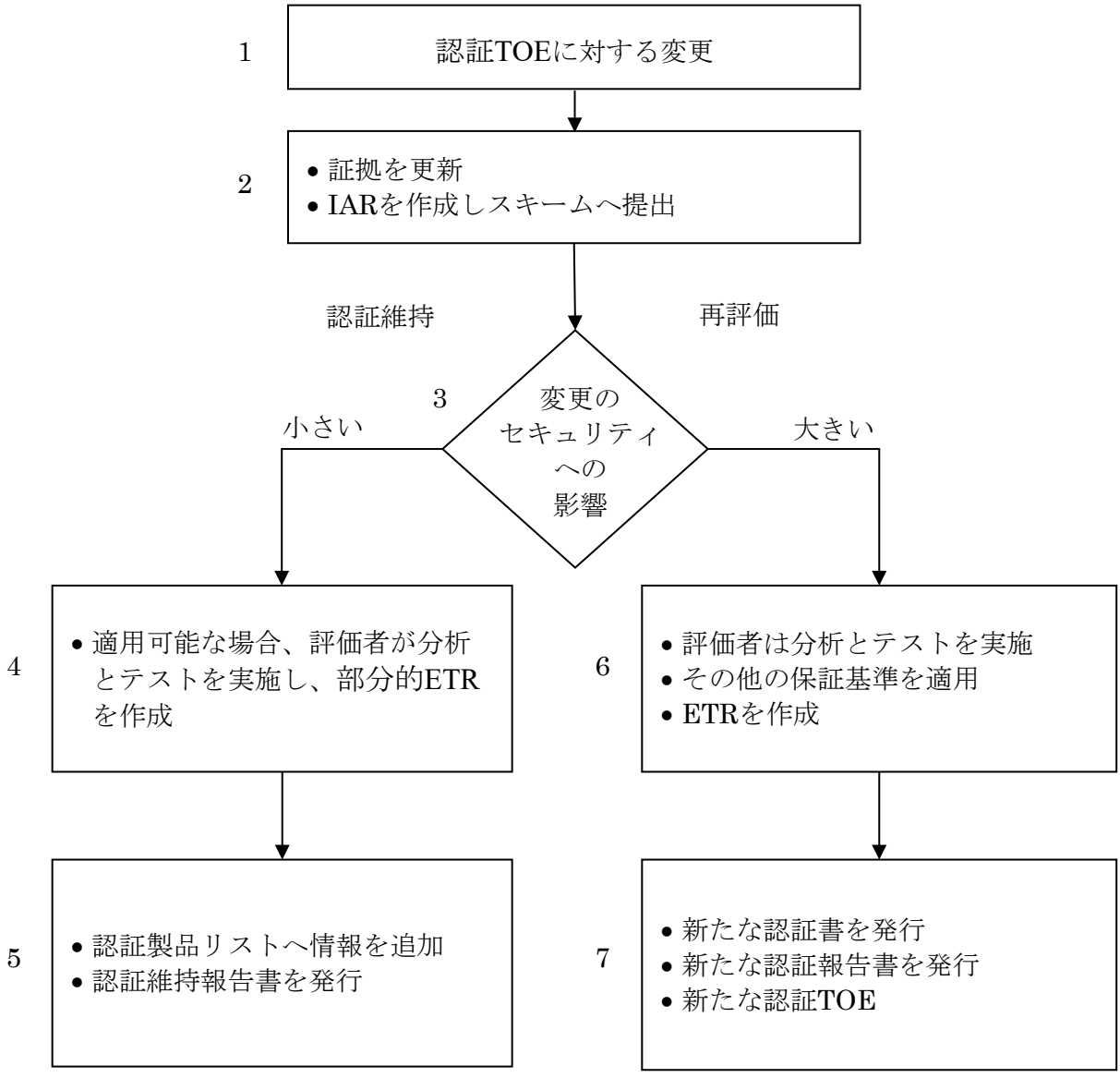

図 2.1　認証維持と再評価

この変更の結果として、保証に与える影響について判定が行われる必要がある[ボックス2]。これは、変更を反映するために更新する必要がある評価証拠の分析、及びTOEに組み込まれる際にそのコードが動作するかを確認するためのリグレッションテストを含む。この判定の基準となるものが影響分析と呼ばれ、TOE開発者によって実施され、影響分析報告書 (IAR) に記録される。IARの内容の詳細については、第5章を参照のこと。

評価監督機関（認証機関）は IAR[1]を使って、それぞれの変更が認証維持に該当するか、又は保証に対して大きな影響を与えるため再評価を要求することが確かに相当であると考えられるかを決定する[ボックス3]。ここで留意すべきは、評価監督機関（認証機関）が認証維持又は再評価の決定において、変更が大きいか、小さいか以外のファクターを使うことがある(認証からの経過時間等)。

もし評価監督機関（認証機関）が、TOEへの変更が小さな影響であることに合意した場合 (*開発環境* の保証手段への変更があったのであれば) 承認されたCC評価機関は保証手段についてのサブセット評価を実施し[ボックス4]、影響を受けた保証コンポーネントをカバーする部分的ETRを評価監督機関（認証機関）に提出する必要がある。保証ベースラインに対して大きな影響を及ぼしていないことに評価監督機関（認証機関）が合意した場合、[ボックス5]に移り、認証製品リストへの認証維持追加情報が作成され、IARを基に認証維持報告書が作成され、当初の認証TOEの認証報告書への追加情報として提供され、公開される。

もし評価監督機関（認証機関）は、この変更が保証ベースラインへの大きな影響を及ぼすと判明した場合、変更TOEは関連する認証を受けるために再評価を受けなければならない。この評価[ボックス6]では、IARと同様に、以前生成した証拠を最大限に利用する。その結果、[ボックス7]にて新しいETR及び新しい認証報告書が作成される。更に、評価監督機関（認証機関）は新しい認証書を発行する。この新しい認証TOEは、将来新たな変更が比較される対象となるベースラインの役割を果たす [ボックス1へ戻る]。

[1] 厳密に言えば、IAR は、認証維持の経路が求められた時のみ必要となる。もし開発者が再評価の経路を選んだ場合は IAR を提出する必要はないが、開発者が再評価作業に役立つ入力として、変更に対する上位の報告書の提出を選択するかもしれない。

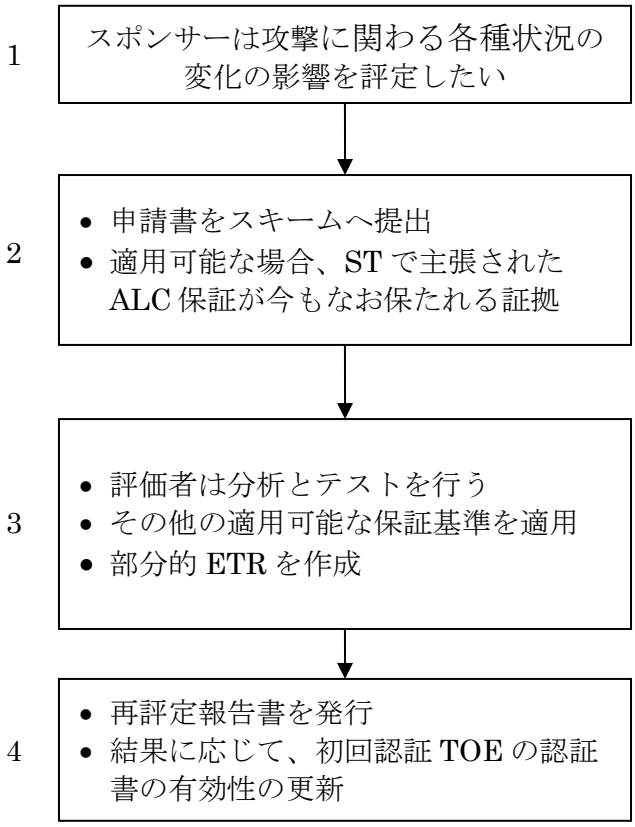

図 2.2　再評定

具体例として、スポンサーが認証TOEの攻撃に関わる各種状況の変化の影響を評定したい場合には、再評定要求が評価監督機関（認証機関）へ提出される[ボックス2]。IARは必要ないが、不必要な評価作業を避けるために、可能な場合はこの段階で開発環境の保証が今も維持されている証拠が提供されるべきである。次に、TOEは評価者による分析とテストを受ける[ボックス3]。攻撃に関わる各種状況の進化によって影響を受ける保証アクティビティ、すなわちAVA_VANファミリのみが再び開始される。そして、十分な証拠が提供できない場合はALCクラスも同様である。

評価者からのETRの受領に対して、スポンサーが望む場合は、評価監督機関（認証機関）が公表可能な再評定報告書を発行する。再評定後に新しい認証書が発行される必要はない。

2.4.1 プロセスに関する記述

保証継続プロセスは、

1. 変更TOEが得た保証、又は

2. 初回認証TOEの認証書の有効性に与える影響

を反映するために、結果的に評価監督機関（認証機関）の認証製品リストへの更新情報として必要な入力、アクション、出力に関して定義される。

上記項目１を果たすため、保証継続は、開発者が変更の影響を分析し、その所見を評価監督機関（認証機関）に提示するメカニズムを提供する。これは、変更があった場合、開発者は保証ベースラインが悪影響を受けないかを決定するために、関連するアクション項目を実施しなければならないことを意味する。このプロセスは、開発者に対する義務として、全ての開発者証拠を維持し（証拠書類への変更に関するIAR内の十分な情報の記録は、その証拠の維持とみなされる）、適切なテストを実施して記録し、以前の分析結果がTOEの変更による影響を受けていないことを確認することを課す。第4章：*影響分析の実施* で、このアクティビティのタイプを更に記述している。保証継続プロセスについては、以下に記述される。

評価監督機関（認証機関）が開発者の分析をレビューし、プロセスを開始するため、開発者は評価監督機関（認証機関）に対して以下の入力が利用可能であるかを確認しなければならない。評価監督機関（認証機関）は既にこれらの入力のいくつかを持っているかもしれない)

a) TOEの認証書 (認証維持追加情報を含む)

b) 認証報告書

c) 評価報告書 (ETR)

d) 認証TOEのセキュリティターゲット

e) 影響分析報告書 (IAR)

評価監督機関（認証機関）が検査に必要な提出物を確認できたら、IARに記述された変更が保証ベースラインに与える影響を決定するために、IAR及び関連の入力に対するレビューに着手する。

評価監督機関（認証機関）によるレビュープロセスでは、開発者との協議を行い、この協議によって完全かつ一貫したIARが完成される。つまり、記録された分析が完了し、評価監督機関（認証機関）が納得するために、IARの内容と記述に関する全ての要求事項（第5章参照）を満たす。 IARレビューは、本文書及び評価監督機関（認証機関）によって発行される関連のガイダンス文書に従って行われなければならず、このレビューの最も重要な点は、保証ベースラインへの明白な影響に基づいて（TOE、IT環境、及び／又は*開発環境* に対する）変更が大きいか、小さいと考えられるかを決定することである。

IARレビューによる2つの結果が考えられる。

i) 評価監督機関（認証機関）は保証ベースラインへの変更の影響が小さいと決定し、認証書が維持TOEに対しても適応されることを示すため、認

証維持追加情報がその後更新される。セクション2.4.2は、認証維持プロセスの更なる詳細を記述している。

ii) 評価監督機関（認証機関）は保証ベースラインへの変更の影響が大きいと決定し、認証維持追加情報は更新されない。このような変更は、再評価において考慮する必要がある。セクション2.4.3は、再評価プロセスの更なる詳細を記述している。

この決定が行われた場合、評価監督機関（認証機関）は、開発者に結果を伝える。影響が大きい場合、小さい場合のいずれの場合であっても、評価監督機関（認証機関）は品質保証プロセスに従って決定の根拠を記録する。このような情報は、コモンクライテリア承認アレンジメント加盟国によって行われる一貫性を保つためのプロセスに提供される。現時点でのエグゼクティブ・サブコミッティ（ES）が、この一貫性維持プロセスの運営を行う機関とする。

2.4.2 認証維持

保証継続－認証維持の目的は、認証TOE、IT環境及び／又は*開発環境* に対する小さな変更（保証に対して、ほとんど又は全く影響を与えないことを示すことができるもの）を許容するものであり、その結果生じたTOEバージョンは、認証TOEと同じ保証レベルが維持できるものとして承認される。

もしTOEへの変更の影響が小さいとみなされる場合、評価監督機関（認証機関）は、*開発環境* への変更の範囲が、*開発環境* 以外の保証コンポーネントにも追加の影響を与えないことを決定しなければならない。*開発環境* 保証手段への変更については、承認された評価機関に、セキュリティターゲットにおける該当する保証コンポーネントについてサブセット評価（セクション2.4.2.1を参照）を実施させる必要がある。サブセット評価のいずれもが問題なく完了した後、更新された認証維持追加情報（セクション2.4.2.2を参照）と認証維持報告書（セクション2.4.2.3を参照）が評価監督機関（認証機関）の認証製品リストに公開される。完成したIARは、開発者と評価監督機関（認証機関）との間のみで共有されるアウトプットとみなされる。

小さな変更に関連する一連の認証維持は、セキュリティ上の影響が複合的であるため、大きな変更と考えられる。この場合、認証維持プロセスによるこれらの小さな変更の組み合わせは、大きな変更として再評価されなければならない（セクション3.2の「セキュリティ上大きな影響をもたらすような複数の小さな変更」に相当する）。

2.4.2.1 *開発環境* の変更の評価

承認された評価機関が、保証手段が変更された*開発環境* の保証コンポーネントのみに焦点を当てて、サブセット評価を行う。評価機関は、その機能について通常のCC評価を行うのと同じ方法でこの評価を実施し、その*開発環境* への変更に

ついて、保証ベースラインが維持されている十分な証拠を評価監督機関（認証機関）に提供するような部分的ETRを作成する。

2.4.2.2 認証維持追加情報

認証維持追加情報は、認証TOEから派生した複数の維持TOEを一覧にした、認証TOEの認証書への追加情報として提供する。

認証維持追加情報の実際の様式は、本文書では指定しない。追加情報として最もふさわしい様式は、各評価監督機関（認証機関）の認証製品リストへの維持TOEの識別子の追加である。追加情報として必要な情報は次のとおりである。

a) 認証TOEに関連する各維持TOEについての一意の識別子

b) 維持TOEに対応するセキュリティターゲットへの参照 (もしセキュリティターゲットへの唯一の変更が、TOEのバージョンに対するものである場合には、当初のセキュリティターゲットが参照される。)

c) 公開されている認証維持報告書への参照

2.4.2.3 認証維持報告書

認証維持報告書は、認証TOEの認証報告書への追加情報と考えられる。認証維持報告書は、認証維持プロセスで承認された認証TOEに対する変更の詳細を提供する。

認証維持報告書に記載される情報は、基本的にはIARの内容のサブセットである。IARの次のセクションは認証維持報告書に含まれるべきである。

a) 序説

b) 変更の記述

c) 影響のある開発者証拠

これらのセクションのそれぞれの内容については、第5章：影響分析報告書に記述されている。これらのセクションは、認証維持報告書を作成する際に、必要に応じて保護された技術情報の削除や言い換えによるサニタイズを行ってもよい。

認証維持報告書には、認証報告書への参照も含むべきであり、その認証報告書への追加情報であることを示すべきである。

評価監督機関（認証機関）は、維持TOEに関連する有益な情報をユーザに提供することが望ましい。そのような情報も認証維持報告書に含まれる。

2.4.3 再評価

認証TOEへの変更が大きな影響があると決定された場合は、より具体的な分析及び独立した評価者による変更TOEの保証の評価が必要である。再評価は過去の評価の枠組みの中で行われ、適用できる過去の評価結果を再利用できるものとする。

開発者は、最初からIARの作成を行わずに、再評価を直接選択することもできる(例えば、変更が著しく、変更TOEが認証TOEに対してわずかな類似点しかないと判断される場合)。あるいは、著しい変更があったとしても、開発者が変更TOEと認証TOEの相違点のセキュリティ影響分析を実施してもよい。

もしIARが提出されたら、変更TOEが、認証TOEから変更されずに残っている、変更TOEの一部分を識別する基礎として活用されるだろう。全ての評価と同様に、未変更のTOEの部分は既に実施済のものとして再度分析の必要はなく、以前の評価結果をできるだけ再利用することができる。そのために、新しいETRは、当初のTOEのETRから導き出される。

変更TOEの評価が完了した際、新たなETRが、変更TOEの認証報告書や認証書と共に生成される。この変更TOEが将来行われる変更に対する更新されたベースラインとなる。

2.4.4 再評定

TOEの初回認証以降に攻撃に関わる各種状況が変わったときには、認証書保持者はTOEの耐性の再評定を望むかもしれない。再評定は、初回評価を行った評価機関によって行われ、適用できる過去の全ての評価結果を再利用できるものとする。AVA_VANファミリに関するタスクのみが再び開始され、また関連する場合は、今もなお満足している十分な証拠が提供できないALCクラスのタスクも同様である。

製品の脆弱性分析を更新するときには、評価機関は次を考慮してもよい。

- 初回評価で確立された潜在的脆弱性のリストは、脆弱性分析を更新するために再利用される。攻撃手法や攻撃能力は時間の経過とともに進化するため、攻撃のレート付けが初回認証から変更されることがある。初回に残存とされていた脆弱性を評定するために、新たな侵入テストを実施することもある。
- 初回認証中に対処されなかった新たな潜在的脆弱性、および関連する攻撃方法は、公開の場で利用できる情報源（CEMのワークユニットAVA_VAN.*-3参照）およびその他の評価証拠（CEMのワークユニットAVA_VAN.2-4以上参照）を調査することによって特定される。これらの新たな潜在的脆弱性は、初回AVA_VANレベルに従って、脆弱性分析を更新するのに使用される。

再評定 は初回のセキュリティターゲットに基づいているため、セキュリティ課題に変更を加えることはできず、新たな攻撃技術や進化した攻撃技術のみがカバーされる。

TOEの再評定が完了すると、再評定されたTOEの再評定報告書とともに、新しいETRが作成される。

そして初回認証書の有効性は次の表に従って更新される。

再評定結果	再評定報告書を公開	再評定報告書を非公開
肯定的[2]	初回認証書の有効性は延長される	変更なし
否定的	初回認証書の有効性は変わらない。再評定TOEによって到達したAVA_VANレベルは公開しなければならない	初回認証書はもはや有効ではないとみなされ、アーカイブされた認証書リストに移される

証明書の有効性が延長される場合、CCRAに定められた適用ルールに基づき、新たな有効期間が設定される。

.

[2] 肯定的とは、TOE が、セキュリティターゲットで初回に主張されたのと同じ AVA_VAN コンポーネントに適合していると再評定されることを意味する。

3 変更の特性

評価監督機関（認証機関）は、認証TOEの保証への（変更による）影響について決定するために、IARに記述される変更内容を検査する。

小さな変更 とは、その変更の影響が、(開発者はその変更については標準的なリグレッションテストを実施したと想定されるが)、評価者アクティビティを開発者とは独立して再度適用しなければならないような範囲の保証に影響を及ぼさないほど十分に小さいもの、又は当初の評価時にとられたその他の保証手段に対して追加の影響を与えないと思われる*開発環境* への変更のことである。その一方で、変更が*大きい* と考えられるものは、変更が保証にかなりの影響を及ぼし（上記に述べた*開発環境* を除く)、その結果、独立した評価者アクティビティの再適用が必要となる。したがって、小さな変更は*認証維持* と呼ばれ、開発者のみによって行われるが、大きな変更は*再評価* と呼ばれ、評価者によって行われる。

認証TOEに与える変更の影響と認証TOEの保証に与える変更の影響の相違点に留意することが重要である。TOEの広範に渡って影響を及ぼすような幅広い変更が、TOEの保証に対して何ら影響を及ぼさない場合もあれば、TOEの保証に大きな影響を与える場合もある。 同様に、変更がTOEのごく一部分のみに影響する場合でも、TOEの保証に対して何ら影響を及ぼさない場合もあれば、TOEの保証に大きな影響を与える場合もある。

全てのTOEに対して起こり得る全ての変更を予測することは不可能であり、その起こり得る全ての変更の影響（かつ、その起こり得る変更が大きいか、小さいか）を識別することは不可能である。したがって、変更によるセキュリティ影響が大きいか、小さいかを識別する不変の方法は存在しない。次の例は、一般的なガイドラインとして、大きな変更と小さな変更の相違点、及び例外事例についても提供するものである。

3.1 代表的な小さな変更

小さな変更は、通常TOEについてのいずれの主張に対しても影響を及ぼさないようなTOEへの変更からなる。認証維持とすることが適切である小さな変更の例を次に示す。

- 認証TOEを変更しないIT環境に対する変更

例えば、基本となるハードウェア（ハードウェアがTOEの一部分ではない場合)の変更、又はインタフェースが未変更の場合で、TOEの範囲外に位置付けられる製品のソフトウェア部分の変更は、小さな変更となるであろう。しかし、インタフェースの変更も伴う場合には、大きな変更となるであろう。

- 保証証拠に影響を及ぼすことがない認証TOEに対する変更

例えば、TOEがEAL1にて認証されている場合、ソースコード及び／又はハードウェア回路図への変更は、保証のための証拠資料に何ら影響を及ぼさない。ただ

し、開発者はこの変更について標準的なリグレッションテストを実施する必要がある。

- 保証証拠のエディトリアルな変更（文法的、誤記、体裁）

例えば、機能仕様書へのエディトリアルな変更で追加的な明確化を提供するものはおそらく小さい変更であろう。しかし、もしPPが *exact* 適合[3] と指定している場合、STのセキュリティ対策方針の記述、又は環境の記述に対するエディトリアルな変更であっても、大きな変更となるだろう。

- 開発環境に対する変更

その他の保証手段に対して追加の影響を与えないことが示される*開発環境* への変更は、一般的に小さな変更と考えられる。この例としては、ALC_CMC.2を主張した認証において開発者が合格し、何らかの理由で構成管理ツールが変更されたような場合が該当する。もし開発者が影響分析報告書の中で、このプロセスはもともと適切であったその他の保証手段に対して追加の影響を与えないという説得力のある根拠を提供できるなら、これは小さな変更と考えられる。

- STの表面的な変更

STの識別、又はTOEの識別子に対する変更（例えば、製品名の変更）は、小さな変更と考えられる。脅威、OSP、前提条件、又はセキュリティ対策方針のいずれかの記述が、セキュリティ要件の変更を必要としない変更である場合、小さな変更となるだろう。しかし、もし要件記述のいずれかに変更がある場合は、大きな変更となる。

3.2 代表的な大きな変更

大きな変更は、通常TOEの主張に対する変更から成り、(必ずしもそうではないが) TOEに対する変更となることが多い。再評価とすることが適切である大きな変更の例を次に示す。

- 主張された保証要件に対する変更

新たな保証手段の追加と現存の保証手段の削除の両方を含む。

[3] *Exact* 適合 とは、PP 作成者が必要なものを正確に指定する場合を指す。PP の内容及び本文から逸脱したいかなるものも ST が適合を主張できないことを意味する。（適合の度合いに関する詳細は、試用のための ASE の更新情報を参照）

-主張された機能要件に対する変更

TOEの範囲の変更をもたらすことになり、正確さと健全性のため、再評価が必要となる。

- セキュリティ上大きな影響をもたらすような、複数の小さな変更

変更がそれぞれ単独では小さな影響であっても、小さな変更の集合が大きなセキュリティ上の影響をもたらすことがある。このような組み合わせが考えられる場合には、再評価が必要となる。

バグの修正が認証TOEに対する変更の範囲はさまざまであり、認証TOEの保証への影響もさまざまであることに注意すべきである。すなわち、「バグ修正」は、大きな変更又は小さな変更のどちらにもなり得るものである。

4 影響分析の実施

4.1 入力

以下は、影響分析プロセスへの入力である。

a) 認証TOEに対応する開発者証拠

b) 変更の記述(おそらく、ライフサイクル品質プロセス及び手続きにて生成される

4.2 準備作業

TOEのセキュリティ分類は、変更が認証維持の範囲内であるかどうかの評定に役立つツールとして利用できる。例えば、変更が影響分析（報告書）に記述されるとき、保証ベースラインにて提供された開発者証拠に対する変更の影響を識別するためにセキュリティ分類を参考にすることが可能である。

セキュリティ分類は、セキュリティ関連の開発ツール、セキュアな配付手順、開発者セキュリティ手続き、開発ライフサイクルアクティビティ、又は構成管理システムの利用や管理に影響するセキュリティ関連手続き等を含む。

TOEへの追加は選択したアプローチに従ってセキュリティ分類される必要があり、修正箇所はセキュリティ分類がレビューを受けている必要があることに注意すべきである。

4.3 影響分析の実施におけるステップ

認証維持の間、修正された開発者証拠の内容と記述された判定結果がまだ認証の状態を満たしていることを確認するのは、開発者の責任である。開発者証拠における変更の影響を識別することで、開発者は変更によるセキュリティへの影響を結論づけることができる。

ステップ1 - 認証TOEの識別

認証TOEの保証ベースラインに対して提供された開発者証拠を、認証TOEを含めて決定する。全ての変更はこのベースラインに対して適用される。

ステップ2 - 変更の識別及び記述

認証TOEに対応する製品に関して、製品への変更を記述する。

認証TOEの開発環境に関して、開発環境への変更を識別し、記述する。

これらの変更は、何が行われたかを理解するために必要な内容の詳細度で記載されるが、どのように行われたかについては必ずしも必要ではない。

ステップ3 - 影響を受ける開発者証拠の決定

このステップの目的は、前ステップからの各々の変更を考慮し、開発者証拠のどれが更新される必要があるかを決定することである。このステップは、認証

TOEの保証パッケージに含まれる各々の保証コンポーネント、保証コンポーネントに対する変更の影響、そのコンポーネントのために提供された証拠を順番に考慮し、体系的な方法で行う。以下のリストは、そのようなアプローチを促進するのに使用される。

製品への変更に関して、次の観点を考慮すべきである。

a) セキュリティターゲットに影響を及ぼすか？

b) TOEの参照に影響を及ぼすか？

c) TOEの構成要素のリストに影響を及ぼすか？

d) TSFの抽象概念レベル、つまり、機能仕様、TOE設計、実装表現などに影響を及ぼすか？

e) アーキテクチャ記述に影響を及ぼすか (もし保証ベースラインがADV_ARCファミリのコンポーネントを含む場合)？

f) 機能仕様書のTSFIから、TOE設計で入手可能なコンポーネント構成の最低レベルまで (もし保証ベースラインがADV_TDSファミリのコンポーネントを含む場合)、並びに実装表現まで (もし保証ベースラインがADV_IMPファミリのコンポーネントを含む場合) のマッピングに影響を及ぼすか？

g) ガイダンス文書に影響を及ぼすか (もし保証ベースラインがAGDクラスのコンポーネントを含む場合)？

h) テスト証拠資料、つまり、テストカバレージ分析、テストの深さ分析、又はテスト証拠資料に影響を及ぼすか (もし保証ベースラインがATEクラスのコンポーネントを含む場合)？

i) 脆弱性分析に影響を及ぼすか？

開発環境の変更に関して、次の観点を考慮すべきである。

a) セキュリティターゲットに影響を及ぼすか？

b) CM証拠資料に影響を及ぼすか？

c) 配付手順に影響を及ぼすか (もし保証ベースラインがALC_DELクラスファミリのコンポーネントを含む場合)？

d) 配付TOEのセキュアな受入れ、TOEのセキュアな設置、運用環境のセキュアな準備に必要な手順に影響を及ぼすか？

e) 開発者セキュリティ手順に影響を及ぼすか (もし保証ベースラインがALC_DVSファミリのコンポーネントを含む場合)？

f) 欠陥修正手順に影響を及ぼすか (もし保証ベースラインがALC_FLRファミリのコンポーネントを含む場合)？

g) ライフサイクルモデルに影響を及ぼすか（もし保証ベースラインがALC_LCDファミリのコンポーネントを含む場合)？

h) 開発ツールに影響を及ぼすか (もし保証ベースラインがALC_TATファミリのコンポーネントを含む場合)？

i) 製造プロセスへの変更はあったか (特にハードウェアコンポーネントについて)？

全ての開発者証拠の影響は、可能性がある影響が識別されることを確認するために、変更の記述に基づいて考慮すべきである。

STが当初のSTに実質的に類似ではあっても、STは影響を受けることがあるので留意すること。もしTOEが変更された場合、それは少なくともTOEバージョン番号に対する変更を含んでいる。

IARの前回バージョンは、この分析の入力として使用される。

一部の開発者アクションエレメントに関して、この決定はシンプルかもしれない(例えば、変更TOEに関する新たなグラフィカルユーザインタフェースが、TOEに使われるのと同じように配付されても、ALC_DELにおいて悪影響はない) が、一方で、その他の要件ではもっと難しいかもしれない (例えば、ユーザインタフェースサブシステムのTOE設計が、新たなGUIの導入によって変更されて、ADV_TDSで提供される資料への影響があるか？

このステップの出力は、影響を受ける開発者アクションエレメントのリストである。

ステップ4 -開発者証拠に対する必要な修正の実施

このステップの目的は、対応する証拠エレメントの内容と記述を検討するために、影響を受けた開発者証拠 (前ステップで識別されたもの) がそれぞれどのように修正されるべきかを決定することである。それらの変更を実際に実装する前に、開発者証拠に必要な変更を集めてまとめれば十分である。

証拠を更新するためには、テスト (リグレッションテスト) が必要となるだろう。例えば、開発者は評価のために提供した開発者テストのサンプルを再現するかもしれない。

IARに関しては、保証ベースラインのテストコンポーネントに応じて、どのように開発者テストが更新されたかについての十分な情報が必要となる。もし新しいテストが変更に対処するために記述された場合、それらは影響分析報告書にテストの目的と共に識別される。しかしながら、テストの個別のテストステップを含めたテストスクリプトを提供するという観点でのテストの詳細は要求されない。

もしTSFへの変更が入手可能な下位レベルのTSF抽象表現で「不可視」の場合(例えば、TSFコンポーネント構成の下位レベルがADV_TDS.2コンポーネントで表現され、いくつかのソースコードが認証維持の間に変更されたりするが、その

ような変更は、TOE設計のサブシステムへの修正を必要としない)、それは開発者が、その変更がどのようにテストされたかを示し、IARにおいて関連する根拠を提供すれば、十分である。

このステップの出力は、更新された証拠のリストである（これは、「どこで」、「なぜ」、「何を」という、証拠に対する変更のリストとしての形式をとればよい）。

ステップ5 - 結論

認証TOEの保証において識別された変更の総合的な影響を決定する。結論：小さな、又は大きな影響。

第３章の「変更の特性に関する議論」を参照。

4.4 出力

a) 影響分析報告書（IAR）:

b) 更新された開発者証拠

5 影響分析報告書 (IAR)

本章では、影響分析報告書に要求される最小限の内容について記述する。IARの内容を図5.1に示す。本図は、IAR文書の構造的な概要を構築する際のガイドとして用いられるものである。IARは、認証維持プロセスの入力として要求される。

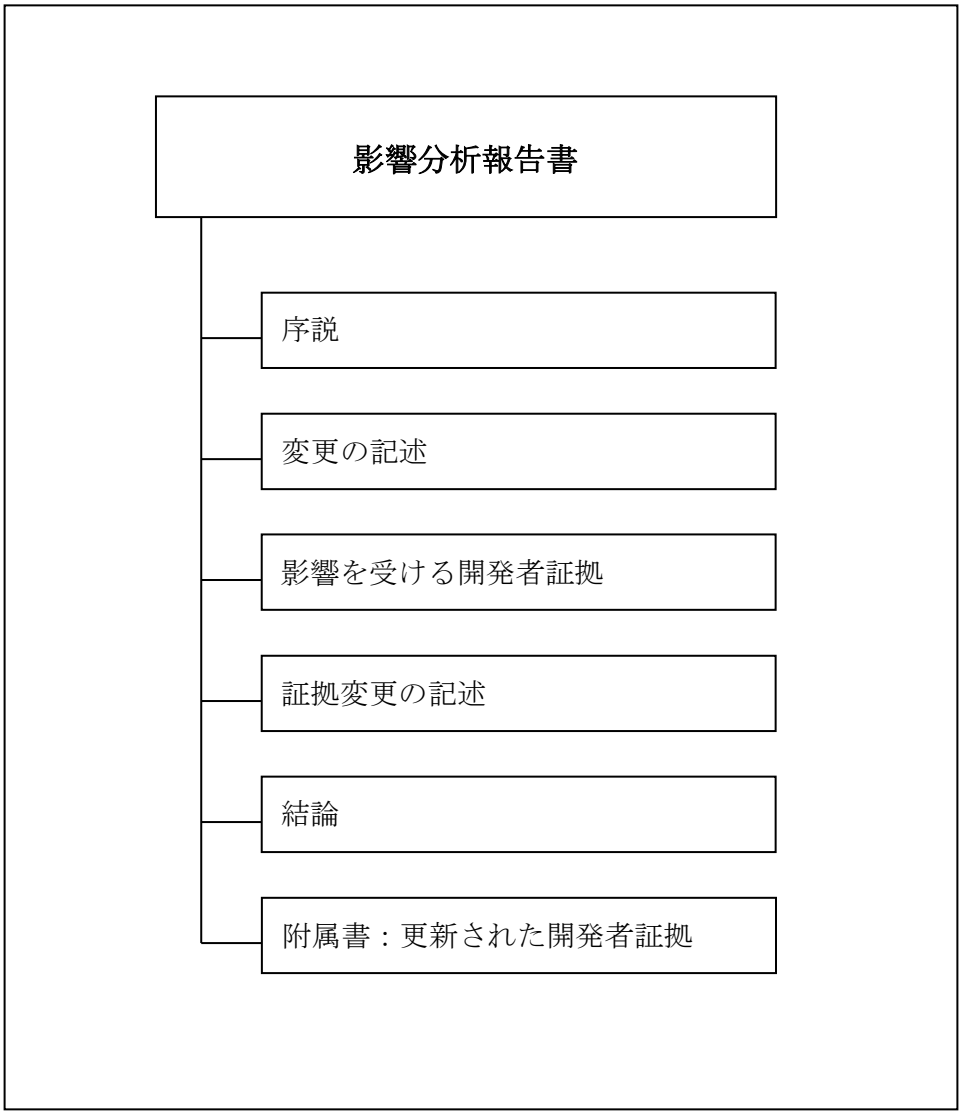

図 5.1　IAR 情報の内容

5.1 序説

開発者は、IARの構成管理識別子を***報告しなければならない。****IARの構成管理識別子は、IARを識別する情報（例えば、名称、日付、バージョン番号）を含む。*

開発者は、現在のTOEの構成管理識別子を***報告しなければならない。****TOEの構成管理識別子は、認証TOEに対する変更を反映したTOEの現在のバージョンを識別する。*

開発者は、ETR、CR（認証報告書）、及び認証TOEの構成管理識別子を***報告しなければならない。****これらの構成管理識別子は、保証ベースライン及びその関連証拠資料をこのベースラインに対して行われたその他の変更とともに識別するために必要である。*

開発者は、認証TOEに関するSTのバージョンについて構成管理識別子を***報告しなければならない。***

開発者は、開発者の識別情報を***報告しなければならない。****TOE開発者の識別情報は、TOEの製造、影響分析の実施、証拠の更新に責任のある者を識別するために必要である。*

開発者は、例えば、本文書の機密性に関する等の法律上の又は法的な観点に照らした情報を**含めてよい。**

5.2 変更の記述

開発者は、製品に対する変更を***報告しなければならない。****識別された変更は、認証TOEに関連した製品に関するものである。*

開発者は、開発環境への変更を***報告しなければならない。****識別された変更は、認証TOEの開発環境に関するものである。*

5.3 影響を受ける開発者証拠

それぞれの変更において、開発者は、開発者証拠の影響をうける項目のリストを***報告しなければならない。****認証TOEに関連した製品へのそれぞれの変更、又は認証TOEの開発環境へのそれぞれの変更に関して、開発者アクションエレメントに対処するために修正されなければならない開発者証拠のあらゆる項目は、識別されなければならない。*

5.4 開発者証拠の修正の記述

開発者は、開発者証拠の影響を受ける項目への必要な修正について***簡潔に記述しなければならない。****開発者証拠の影響を受ける各項目については、証拠エレメントの対応する内容と記述に対処するために必要な修正を簡潔に記述しなければならない。*

5.5 結論

それぞれの変更において、開発者は、保証に対する影響が小さいか、大きいかを***報告しなければならない。****それぞれの変更において、開発者は、報告された影響についての根拠を提供するべきである。開発環境に対して変更が行われる場合は、その他の保証手段に対して追加の影響を与えないことを示す根拠が必要となる。*

開発者は、総合的な影響が小さいか、大きいかを***報告しなければならない。****開発者は、変更の結果を考慮した根拠を含めるべきである。*

5.6 附属書：更新された開発者証拠

開発者は、以下の情報について、開発者証拠のそれぞれの更新された項目を***報告しなければならない。***

- タイトル
- 一意の参照 (例えば、発行日及びバージョン番号等)

特記すべき変更がされた証拠の項目のみを一覧表として記載する必要がある。もし証拠の項目の唯一の更新がTOEの新しい識別の反映である場合は、それを含める必要はない。