保 証 継 続 :

CCRA 要求事項

バージョン **2.1**

2012 年 **6** 月

平成 24 年 10 月翻訳第 1.0a 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

目次

1 序論

1 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の定義を目論むもので、認証維持及び再評価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を目論んでいる。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

2 本文書は、CC の概念に基づき、CC 認証製品の認証維持及び再評価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している。

1.2 アプローチ

3 本文書は、以下の観点から保証継続を扱う。

a) 認証維持及び再評価の両方に関わるプロセスの記述を含む、保証継続のパラダイム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
c) 影響分析の実施に関するガイダンス
d) 影響分析報告書の内容と記述に関する要求事項

1.3 構成

4 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

5 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。

6 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すべ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すべて行われたということが示される。

7 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

8 明確にするために、以下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) *継続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、継続TOEにも適用されることを意味している。

d) *継続追加情報*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。継続追加情報には、継続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。

e) *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、継続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。

f) *保証継続報告書*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。

g) *保証基準*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。

h) *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すべての項目を表す。

i) *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。

j) *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、新たな保証基準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。

k) *開発環境*とは、TOEの開発、配付、立ち上げ、欠陥修正に関するすべ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すべての概念を含む。

l) *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、*部分的評価報告書 (a partial ETR)* を作成する。

m) *部分的評価報告書 (a partial ETR)* は、*サブセット評価* のアウトプットである。*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。

n) *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。

9 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継続追加情報に追加された後、そのバージョンが継続 TOE となる。

2.3 前提条件

10 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 保証継続パラダイム

11 保証継続は、変更された認証 TOE 又はその環境から生じる、一意の TOE 識別子（バージョン番号の増加等）に対する変更が行われるが、以前実施された評価作業を必ずしもすべての状況で繰り返す必要は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、保証継続パラダイムは*認証維持*と*再評価*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。

12 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 についての継続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、保証基準に悪影響を与えないことが論証されなければならない。

13 再評価とは、開発者が認証 TOE への変更が保証基準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。

14 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方法に対する TOE の対策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、再評価によってのみ得ることができる。認証維持では、保証基準へ与える TOE 変更の影響のみを考慮しており、進化していく脅威環境を考慮するものではない。

15 図 2.1 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。

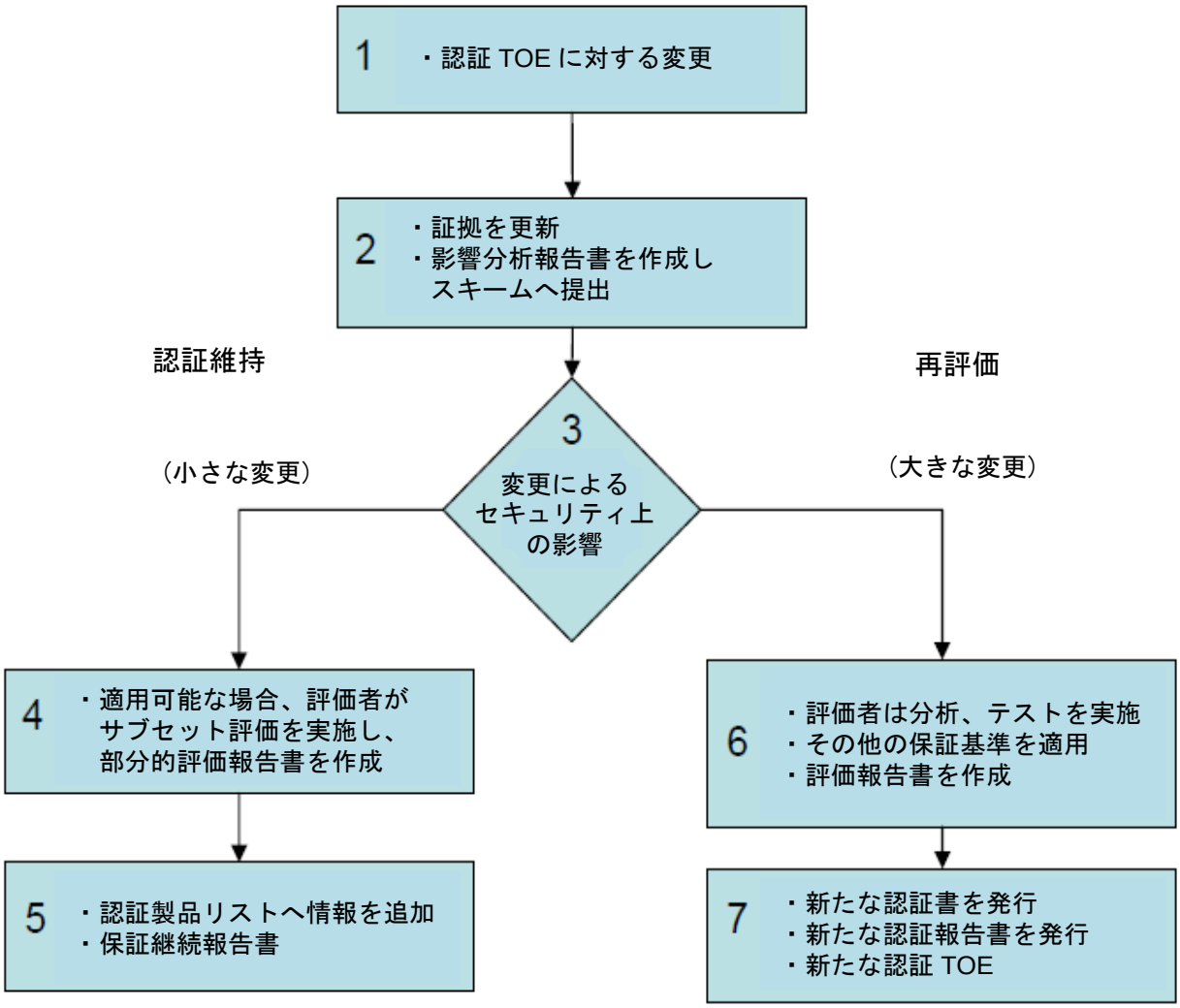

図2.1　保証継続

16 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レ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。

17 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)。

18 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 評価機関は変更された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のみをカバーする*部分的評価報告書*を評価監督機関（認証機関）に提出する必要がある。保証基準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継続追加情報が作成され、IAR を基に保証継続報告書が作成され、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、公表される。

19 もし評価監督機関（認証機関）は、この変更が保証基準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保証基準として提供される[ボックス 1 へ戻る]。

2.4.1 プロセスに関する記述

20 保証継続プロセスは、変更 TOE が得た保証を反映するために、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インプット、アクション、アウトプットに関して定義される。

21 この目的を果たすため、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、開発者は保証基準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、すべ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）、

[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インプットとして、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。

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。

22 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）に対して以下のインプット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）は既にこれらのインプットのいくつかを持っているかもしれない）：

a) TOEの認証書 (継続追加情報を含む)

b) 認証報告書

c) 評価報告書

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)

23 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基準に与える影響を決定するために、IAR 及び関連のインプットに対するレビューに着手する。

24 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すべての要求事項（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、保証基準への明白な影響に基づいて（TOE、IT 環境、*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。

25 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）は保証基準への変更の影響が小さいと決定し、認証書が継続TOEに対しても適応されることを示すため、継続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）は保証基準への変更の影響が大きいと決定し、継続追加情報は更新されない。このような変更の場合は、再評価が必要であるとみなされる。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。

26 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

27 保証継続の目的 ― 認証維持は、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、少し又は全く影響を与えない程度のもの）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。

28 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 CC 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、更新された継続追加情報（セクション 2.4.2.2 を参照）と保証継続報告書（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表される。 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。

29 一般的に、認証維持は認証日から 2 年間まで継続する。ただし、認証書を発行するスキームは、状況が許せば、IT 製品種別や消費者のニーズに基づいて、その認証維持の期間を延長したり短縮したりしてもよい。

2.4.2.1 *開発環境*への変更の評価

30 *開発環境*への変更の評価については、必ずしもすべての保証コンポーネントが再評価されることを要求しない。 承認された CC 評価機関が、*開発環境*に対する変更によって影響を受ける保証コンポーネントのみに焦点を当てた*サブセット評価*を行うことで十分である。 評価機関はその*開発環境*への変更については、保証基準が維持されていることを評価監督機関（認証機関）への十分な証拠を提供するような部分的評価報告書を作成する。

2.4.2.2 継続追加情報

31 継続追加情報は､認証 TOE から導き出された複数の継続 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。

32 継続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継続 TOE の識別子の追加である。

33 継続追加情報として必要な情報は、以下の通りである：

a) 認証TOEに関連する各継続TOEについての一意の識別子

b) 継続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) 公表されている保証継続報告書への参照

2.4.2.3 保証継続報告書

34 保証継続報告書は、認証 TOE の認証報告書への追加情報と考えられる。保証継続報告書は、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。

35 保証継続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 の以下のセクションは保証継続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

36 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、保証継続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。

37 保証継続報告書には、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。

38 評価監督機関（認証機関）は、継続 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。そのような情報も保証継続報告書に含まれる。

2.4.3 再評価

39 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。

40 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。

41 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。すべての評価と同様に、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。

42 変更 TOE の評価が完了した際、新たな ETR は、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基準となる。

3 変更の特性

43 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。

44 *小さな変更*とは、(認証された保証範囲へ与える)影響がごくわずかで、評価者アクティビティが独立に再度適用されなければならないような範囲に対する保証へ影響を及ぼさない十分小さいもの（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)、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。

45 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。

46 すべての TOE に対して起こり得るすべての変更を予測することは不可能であり、その起こり得るすべての変更の影響（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

47 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以下に示す：

a) **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。

b) **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、保証のための文書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。

c) **エディトリアルな変更**（文法的、誤記、体裁）のうち保証のための文書に関するもの
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*[2]適合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。

d) **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と思われる*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。

e) **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

48 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

[2] *Exact* 適合とは、PP 作成者が何が要件であるかを正確に示すような場合を指す；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、試用に関する ASE の更新情報を参照）

きな変更の例を以下に示す：

a) **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。

b) **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。

c) **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。

49 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　インプット

50　以下は、影響分析プロセスへのインプットである：

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

51　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、保証基準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。

52　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。

53　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

54　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

55　認証 TOE の保証基準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。すべての変更はこの基準に対して適用される。

ステップ2－変更の識別及び記述

56　認証 TOE に対応する製品に関連して、製品への変更を記述する。

57 認証 TOE の開発環境に関連して、開発環境への変更を識別し、記述する。

58 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

59 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。

60 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 (もし保証基準が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 (もし保証基準が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 (もし保証基準が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 (もし保証基準がAGDクラスのコンポーネントを含む場合) ？

h) テスト文書、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 (もし保証基準が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？

61 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文書に影響を及ぼすか？

c) 配付手順に影響を及ぼすか (もし保証基準が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 (もし保証基準が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 (もし保証基準が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 (もし保証基準が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 (もし保証基準が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)？

62 すべ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、変更に基づいて考慮すべきである。

63 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。

64 IAR の前回バージョンは、この分析のインプットとして使用される。

65 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？

66 このステップのアウトプットは、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ー開発者証拠に対する必要な修正の実施

67 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。

68 証拠を更新するためには、テスト（レ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。

69 *IAR に関しては、保証基準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。*

70 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。

71 このステップのアウトプットは、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ー結論

72 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 アウトプット

73 以下は、影響分析プロセスのアウトプットである：

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)

74　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 に図示する。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インプットとして要求される。

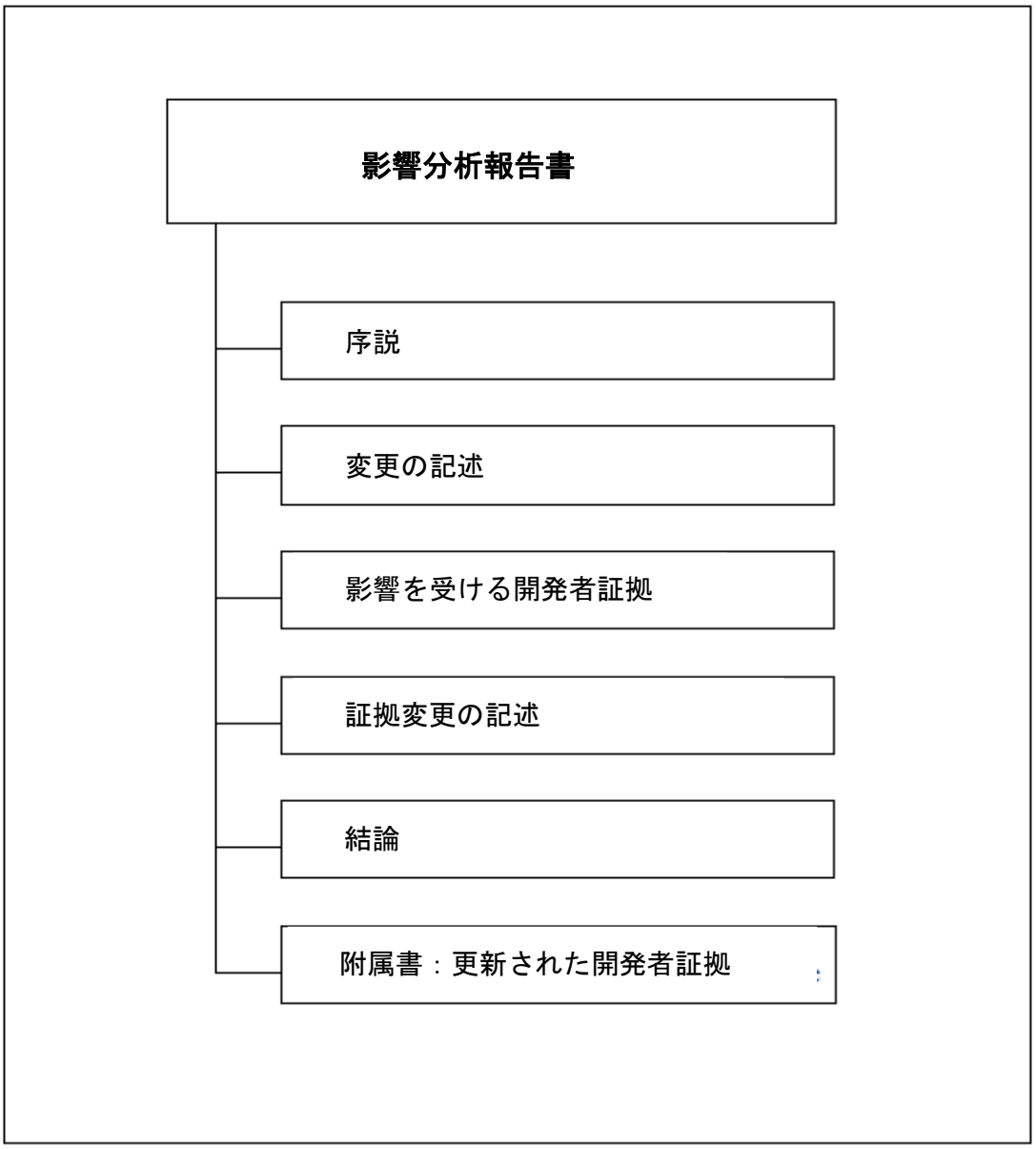

図5.1　IAR情報の内容

5.1　序説

75　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。

76 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。*

77 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、保証基準及びその関連文書をこの基準に対して行ったその他の変更とともに識別する必要がある。*

78 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。***

79 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要求される。*

80 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

81 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。*

82 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

83 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

84 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

85 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。*

86 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 付属書：更新された開発者証拠

87 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)

88 *特に変更された証拠の項目のみ一覧表として記載する必要がある。もし証拠の項目の更新のみが TOE の新しい識別に反映されていれば、それは含める必要はない。*