

参考資料



情報技術セキュリティのための 共通評価方法論

CEM-2001/0015R

パート 2 :
評価方法論

補 足 :
ALC_FLR 欠陥修正

バージョン 1.1
2002 年 2 月

平成 15 年 7 月翻訳第 1.0 版
情報処理振興事業協会
セキュリティセンター

IPA まえがき

本書の目的

本書は、情報技術セキュリティ評価のためのコモンクライテリアを基にした評価に関するガイド「Common Methodology for Information Technology Security Evaluation (CEM)」の補足文書である「ALC_FLR: Flaw Remediation」を日本語訳したものである。本書は、情報処理振興事業協会(略称 IPA)セキュリティセンターにおいて、セキュリティ評価のための補助資料として作成されたものである。

使用上の注意

本書は、用語、記述内容等に不備がある可能性がある。疑問点については下記に記載した CEM で確認していただきたい。本書は、参照利用されることのみを目的とし、本書の改変、及び他への転載は禁止する。

参考文献

Common Methodology for Information Technology Security Evaluation (CEM)

Part1: Introduction and general model Version 0.6 97/01/11 CEM-97/017

Part2: Evaluation Methodology Version 1.0 August 1999 CEM-99/045

CEM Supplement: ALC_FLR: Flaw Remediation February 2002 CEM-2001/0015R

掲載ホームページアドレス <http://www.commoncriteria.org/>

Common Criteria for Information Technology Security Evaluation (CC)

Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

掲載ホームページアドレス <http://www.commoncriteria.org/>

情報技術セキュリティ評価のための共通方法論

パート 1：概説と一般モデル バージョン 0.6 翻訳第 1.0 版 平成 13 年 2 月 IPA セキュリティセンター

パート 2：評価方法論 バージョン 1.0 翻訳第 1.0 版 平成 13 年 2 月 IPA セキュリティセンター

情報技術セキュリティ評価のためのコモンクライテリア バージョン 2.1

パート 1：概説と一般モデル 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

パート 2：セキュリティ機能要件 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

パート 3：セキュリティ保証要件 翻訳第 1.2 版 平成 13 年 1 月 IPA セキュリティセンター

翻訳上の注釈：

1. correction、correcting、corrective の訳を、以前は“修正”としていたが、remediation も修正と訳しているため、“訂正”とした。なお、すでに発行されている CC パート 3 の ALC_FLR 保証要件の日本語訳も対象となるが、本書の附属書 A と置き換わることに注意のこと。

著作権について

本書がベースにしている CEM の著作権は、以下に示す 7 つの政府機関 (“the Common Criteria Project Sponsoring Organizations”と総称) が有している。したがって、CEM の使用、複製、配布、及び改変の権利は、the Common Criteria Project Sponsoring Organizations にある。

The Common Criteria Project Sponsoring Organizations:

- Canada: Communications Security Establishment
- France: Service Central de la Securite des Systemes d’Information
- Germany: Bundesamt fur Sicherheit in der Informationstechnik
- Netherlands: Netherlands National Communications Security Agency
- United Kingdom: Communications-Electronics Security Group
- United States: National Institute of Standards and Technology
- United States: National Security Agency

まえがき

本書は、国際的な IT セキュリティ評価コミュニティが使用するために the Common Criteria sponsoring organisations によって発行されている。本書は、情報技術セキュリティのための共通評価方法論(CEM) パート2、バージョン 1.0 への補足であり、そしてそれ故にそのドキュメントの一部と見なすことができる。この補足の発行は、コモンクライテリア承認アレンジメントの用語を変更しないが、セキュリティターゲットに ALC_FLR ファミリを含む、評価に関する共通方法論の基準を提供する。

補足のこのバージョンは、この更新されたまえがきと少数の編集上の変更を行っている。これらの変更は左欄外の「変更線」によって識別される。

本書に関するすべてのコメントは、<http://www.commoncriteria.org> で定義された解釈に対する要求 (the Request for Interpretation) プロセスによって提出されるべきである。

1 章 序説

- 1 1999 年 8 月に、情報技術セキュリティのための共通評価方法論(CEM)パート 2、バージョン 1.0 は情報技術セキュリティ評価のためのコモンプライテリア(CC)バージョン 2.1 に定義されるように、評価保証レベル(EAL) 1 から 4 の保証コンポーネントを適用するのに使用される方法論について記述し公開された。しかしながら、CEM は、APE と ASE のクラス以外は残りの部分の保証要件の適用に関して方法論を定義していない。
- 2 本書は、解釈 CCIMB-INTERP-062 及び CCIMB-INTERP-092 を含む ALC_FLR ファミリ(欠陥修正)の CC 保証要件を適用するための方法論を提供することで、CEM を補う。この補足は CCIMB-INTERP-094 に置き換わる。このファミリの保証コンポーネントは CC パート 3 EAL のどれにも含まれていないけれども、それらはどのような PP 及び ST に組み込むこともできる。
- 3 CEM が更新されるとき、CEM の新バージョンに本書の内容が組み込むことが計画されている。

1.1 適用

- 4 ALC_FLR 要件は CC に定義された EAL の中で使用されない。PP と ST の中の保証要件は定義された EAL に必ずしも制限されないので、ALC_FLR ファミリからのものを含む他の保証コンポーネントを含むことが可能である。すなわち、ALC_FLR のどのコンポーネントも、CC の中の保証パッケージのどれとも合わせて PP/ST の一部として使用することができる。

1.2 内容

- 5 本書は 4 つの節を含んでいる。本書のこの序説、本書の基礎をなす技術的概念、コンポーネント ALC_FLR.1、ALC_FLR.2 及び ALC_FLR.3 に関する方法論、及び CC の ALC_FLR ファミリに対する置換テキストを含んだ附属書。
- 6 これらのコンポーネントの各々については、関連する評価者アクションが記述されている。コンポーネントの目的は、評価者ワークユニットが実行される入力といっしょに与えられる。その後、CC 評価者アクションエレメントによって要求されるか、CC 開発者アクションエレメントによって示される評価者アクションが続く。これらの CC 証拠の内容・提示エレメントまたは開発者アクションエレメントの各々は、イタリック体のテキストに含まれ、そのエレメント及び何らかの付加ガイダンスに対する方法論ワークユニットが続く。この補足内では、各ワークユニットで最初にでたものがボールド体で提示される。
- 7 ワークユニットは左欄外において *ALC_FLR.1-2* のようなシンボルによって識別される。このシンボルでは、文字列の *ALC_FLR.1* が CC コンポーネント(つまり CEM のサブアクティビティ)を示し、また最終の数字(2)は、これが ALC_FLR.1 サブアクティビティの 2 番目のワークユニットであることを示す。

- 8 読者は、これらの要件に関連した目的と適用上の注釈について付加的な詳細に関して、CCを見ることを忘れてはいけません。

2 章 基礎をなす技術的概念

- 9 この章は本書の他の部分が基づくべき技術的概念を記す。これらの概念は定義される用語及び適用上の注釈の2つのカテゴリに分割され、それらのすべては3章に記述されるコンポーネントに関する方法論に当てはまる。他の用語及び頭字語はCC及びCEMの中で使用され説明される。

2.1 用語

- 10 語句 *TOE* は *評価対象* を意味する。しかしながら、一旦それが目指して進んでいたゴールが達成されれば、対象はもはや対象ではないという含蓄がある。すなわち、一旦 *TOE* の評価が完了していれば、それはもはや評価の対象ではない。CC は、一旦評価が完了したならば *TOE* を参照する手段を提供しない。ALC_FLR 要件は評価イベント後に対処するその性質によって、付加的なポスト評価 (post-evaluation) 用語に関する必要性を作り出した。さらに、本書に記述されたサブアクティビティに関して、他の用語は正確な意味で使用されている。次の用語がそれ故に定義される。
- 11 認証済み TOE (Certified TOE) - 製品あるいはシステム及びその関連するガイダンス、TOE(評価下であったもの)で、評価を完了した、その ST、認証報告及び発行された認証書。
- 12 TOE のリリース (Release of a TOE) - 認証済み TOE に変更が適用されたリリースである製品あるいはシステム。(オリジナルの認証書は変更の理由にかかわらず変更されたバージョンに適用しないことに注意を払うこと。)
- 13 セキュリティ欠陥の追跡 (Tracking a security flaw) - セキュリティ欠陥の現在のステータス及び履歴がわかること。(それがその存在の時系列に沿っている場合に)
- 14 TOE 利用者 (TOE user) - セキュリティ欠陥に対する処置を受け取る及び実装することに責任を負う利用者組織の中心。これは必ずしも個々の利用者(例えば、AGD_USR 要件の中で使用されるように)でなくてもよいし、セキュリティ欠陥の取り扱いに責任を負う、組織的な代表者であってもよい。用語 *TOE 利用者* の使用は、異なる組織が個々のユーザ毎でもよいしあるいは中央行政機関によって行われてもよい欠陥報告を扱うための異なる手続きを持っていることを認識する。
- 15 TOE ガイダンス (TOE guidance) - 管理者ガイダンス、利用者ガイダンス、欠陥修正ガイダンス、配付手続き及び設置、生成及び立上げ手続き。
- 16 セキュリティ欠陥 (Security flaw) - 単独であるいは他のものと協力して、利用可能な脆弱性を提供する状態。TOE のハードウェア、ソフトウェアあるいはファームウェア部分に関する問題からではなく TOE ガイダンスでの問題から生じる TSP 侵害も、*セキュリティ欠陥* と認められる。製品またはシステムが意図する環境の外で使用される場合、TSP 侵害に帰着する実行のすべてのパスは利用可能ではないだろうし、それ故に、セキュリティ欠陥とみなされない。

2.2 適用上の注釈

- 17 セキュリティ欠陥の修正は、TOE 評価の完了後に発見されたセキュリティ欠陥に対して行われる。(評価の前に、あるいはその評価の間に発見されたセキュリティ欠陥の訂正は、構成管理、脆弱性分析、テストなどの問題である。)
- 18 TOE 開発者の欠陥の報告にたいする責任は、TOE 環境の中で発見されたものまで及び。開発者の欠陥の訂正に対する責任は、環境の中のものまで及ばない。例えば、信頼されるアプリケーションの開発者は、よく下層のオペレーティング・システムを IT 環境であると識別するだろう。アプリケーションで見つかった欠陥は、開発者によって報告され、追跡され、訂正されるだろう。オペレーティング・システムで発見された欠陥は、開発者によって単に報告される必要がある(たぶん単に「オペレーティング・システム X 上でこのアプリケーションを実行してはならない」の表現で)。オペレーティング・システムが TOE 環境で課された要件(あるいは前提条件を満足する)をもはや満たさないと通知された TOE 利用者は、そのとき、オペレーティング・システムの欠陥がオペレーティング・システム開発者によって訂正されるまで、それらの要件/前提条件を満たす別のオペレーティング・システムを見つける必要があるだろう。異なる開発者の TOE を組み合わせる場合、このシナリオは、TOE 利用者が知ることの重要性を強調する。
- 19 このサブアクティビティでは、欠陥修正手続きはセキュリティ欠陥が認証済み TOE 及び TOE のリリースで発見されるとき、守られるべき開発者の手続きに対応するが、それらはそのような手続きが守られていることを検証するための対策を含んでいないことに注意すべきである。ACM_SCP.2 と AMA_EVD.1 のワークユニットはこの検証のサポートにおいて使用することができる。そのような欠陥の訂正は評価済み TOE の修正を要求するので、TOE はもはや認証済みバージョンにならないだろう。
- 20 報告されたセキュリティ欠陥は、それがセキュリティ欠陥でないか(この場合、それ以降は追跡する必要がない)、セキュリティ欠陥であるか(この場合、それが解決されるようなときまで追跡され続ける)を調査が明らかにするときまで、単に「疑いのある」セキュリティ欠陥とみなすことができる。

3章 欠陥修正サブアクティビティ

3.1 欠陥修正の評価(ALC_FLR.1)

3.1.1 目的

21 このサブアクティビティの目的は、開発者が、セキュリティ欠陥の追跡、訂正アクションの識別、及び訂正アクション情報の、TOE 利用者への配付について記述した欠陥修正手続きを確立しているかどうかを決定することである。

3.1.2 入力

22 このサブアクティビティ用の評価証拠は、次のとおりである。

a) 欠陥修正手続きの証拠資料

3.1.3 評価者アクション

23 このサブアクティビティは、次の1つの CC パート3 評価者アクションエレメントからなる。

a) ALC_FLR.1.1E

3.1.3.1 アクション ALC_FLR.1.1E

ALC_FLR.1.1C-欠陥修正手続き証拠資料は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.1-1 **評価者は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するために使用される手続きが記述されていることを決定するために、欠陥修正手続き証拠資料を検査しなければならない。**

24 その手続きでは、各々の疑わしいセキュリティ欠陥が報告されたときから、それが解決されるときまでに、開発者によって講じられるアクションについて記述する。これは、欠陥がセキュリティ欠陥であると確認する最初の検出から、セキュリティ欠陥の解決までの、全時間枠を含んでいる。

25 欠陥がセキュリティ関連ではないと判明した場合、それをさらに追跡する欠陥修正の手続き(ALC_FLR 要件の目的のため)をする必要はない。単に、なぜ欠陥がセキュリティ関連ではないかの説明のみとなる。

26 TOE 利用者のためのセキュリティ欠陥を報告する手段を公表することを、要件は必須とはしないが、それらは、報告されるすべてのセキュリティ欠陥を追跡することを必須とする。すなわち、単にそれが開発者の組織外で生じたからといって、報告されたセキュリティ欠陥を無視することはできない。

ALC_FLR.1.2C-欠陥修正手続きは、欠陥訂正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。

ALC_FLR.1-2 評価者は、それぞれの性質及び影響から、各セキュリティ欠陥の記述が作成されていることを決定するために、これらの手続きの適用を検査しなければならない。

27 その手続きは、それを再現することができるくらい十分に詳細な、セキュリティ欠陥の性質及び影響について記述するために、開発者によって講じられるアクションを識別する。セキュリティ欠陥の性質の記述は、その誤りが、資料内の誤り、TSFの設計の欠陥、TSFの実装の欠陥、その他のどれであるかに対応する。セキュリティ欠陥の影響の記述は、影響が及ぶTSFの部分及びそれらの部分に、どのような影響が及ぶかを識別する。例えば、実装におけるセキュリティ欠陥は、パスワード‘BACKDOOR’による認証を許可することにより、TSFによって実施される識別と認証に影響を及ぼすことが見つかるかもしれない。

ALC_FLR.1-3 評価者は、セキュリティ欠陥ごとの訂正について探索のステータスが識別されていることを決定するために、これらの手続きの適用を検査しなければならない。

28 欠陥修正手続きは、セキュリティ欠陥の異なる段階を識別する。この異なる段階には少なくとも、次のものを含む。その報告が行われた疑わしいセキュリティ欠陥、セキュリティ欠陥の確認が行われた疑わしいセキュリティ欠陥、及びその解決法が実行されたセキュリティ欠陥。追加の段階（例えば、報告が行われたがまだ調査していない欠陥、調査中である欠陥、解決法が見つかったがまだ実行されていないセキュリティ欠陥）を含むことができる。

ALC_FLR.1.3C-欠陥修正手続きは、訂正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。

ALC_FLR.1-4 評価者は、これらの手続きの適用が、各セキュリティ欠陥の訂正アクションを識別することを決定するために、欠陥修正の手続きをチェックしなければならない。

29 訂正アクションは、TOEのハードウェア、ファームウェア、あるいはソフトウェア部分の修理、または、TOEガイダンスの変更、または両方から構成されるかもしれない。TOEガイダンス（例えばセキュリティ欠陥を除去するために取られる手続き的な手段の詳細）の変更を構成する訂正アクションは、恒久的解決法（手続き的な手段が最良の解決法であること決定する際）として役立つものと同様に、暫定的解決法（修理が完了するまで）として役立つ両方の手続き的な手段を含む。

30 セキュリティ欠陥の原因が資料上の誤りである場合、訂正アクションは、影響を受けたTOEガイダンスの更新から構成される。訂正アクションが手続き的な手段である場合、この手段には、これらの訂正する手続きを反映するために影響を受けたTOEガイダンスの更新を含むことになるであろう。

ALC_FLR.1.4C-欠陥修正手続き証拠資料は、TOE利用者に、欠陥情報、訂正、及び訂正行為のガイダンスを提供するために使用する方法を記述しなければならない。

ALC_FLR.1-5 評価者は、TOE利用者に各セキュリティ欠陥についての必要な情報を提供する手段について記述されていることを決定するために、欠陥修正手続きの証拠資料を検査しなければならない。

31 各セキュリティ欠陥に関する必要な情報は、その記述（ワークユニットALC_FLR.1-2の一部として提供される記述と同じ詳細レベルである必要はない）、規定された訂正アクション、及び訂正の実行についてのあらゆる関連するガイダンスから構成される。

- 32 TOE 利用者は、ウェブサイトへの掲載、TOE 利用者への送信、あるいは開発者が訂正をインストールするための取り決めのような、何らかの方法により、情報、訂正、及び資料の最新版を提供されるかもしれない。この情報を提供する手段が、TOE 利用者が起動するアクションを要求する場合、評価者は、それが情報を検索するための指示を含むことを保証するために、あらゆる TOE ガイダンスを検査する。
- 33 情報、訂正、及びガイダンスの提供のために使用される方法の妥当性を評価するためのただ一つの尺度は、TOE 利用者がそれを得るか受け取ることができるという合理的予測である。例えば、必要なデータが 1 か月の間ウェブサイトに掲載され、TOE 利用者は、これが起きること、またこれがいつ起きるかを知っている場合についての公報の方法を考慮すること。これは特に、合理的あるいは有効的とはいえないかもしれない（例えば、ウェブサイトへの恒久的掲載ほどは）が、しかし TOE 利用者が必要な情報を獲得することは実現可能である。一方、わずかに 1 時間だけウェブサイトに情報が掲載され、TOE 利用者がこのこと、あるいはこれがいつ掲載されるかを知る方法を持っていなければ、常に必要な情報を獲得することは実現不可能である。

3.2 欠陥修正の評価(ALC_FLR.2)

3.2.1 目的

34 このサブアクティビティの目的は、開発者が、セキュリティ欠陥の追跡、訂正アクションの識別、及び訂正アクション情報の、TOE 利用者への配付について記述した欠陥修正手続きを確立しているかどうかを決定することである。さらに、このサブアクティビティは、開発者の手続きが、セキュリティ欠陥の訂正、TOE 利用者からの欠陥報告の受領、及び訂正が新しいセキュリティ欠陥を取り込まないという保証を提供しているかどうかを決定することである。

35 開発者が TOE 利用者からのセキュリティ欠陥報告に基づいて適切に行動することができるために、TOE 利用者は、開発者にセキュリティ欠陥報告を提出する方法を理解する必要があり、また、開発者は、これらの報告を受領する方法を知る必要がある。TOE 利用者に向けた欠陥修正ガイダンスは、TOE 利用者が開発者と連絡する方法を理解していることを保証する。欠陥修正手続きは、開発者の役割がそのような連絡であることを記述している。

3.2.2 入力

36 このサブアクティビティ用の評価証拠は、次のとおりである。

- a) 欠陥修正手続きの証拠資料
- b) 欠陥修正ガイダンスの証拠資料

3.2.3 評価者アクション

37 このサブアクティビティは、次の1つの CC パート3 評価者アクションエレメントからなる。

- a) ALC_FLR.2.1E

3.2.3.1 アクション ALC_FLR.2.1E

ALC_FLR.2.1C-欠陥修正手続き証拠資料は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.2-1 評価者は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するために使用される手続きが記述されていることを決定するために、欠陥修正手続き証拠資料を検査しなければならない。

38 その手続きでは、各々の疑わしいセキュリティ欠陥が報告されたときから、それが解決されるときまでに、開発者によって講じられるアクションについて記述する。これは、欠陥がセキュリティ欠陥であると確認する最初の検出から、セキュリティ欠陥の解決までの、全時間枠を含んでいる。

39 欠陥がセキュリティ関連ではないと判明した場合、それをさらに追跡する欠陥修正の手続き(ALC_FLR 要件の目的のため)をする必要はない。単に、なぜ欠陥がセキュリティ関連ではないかの説明のみとなる。

ALC_FLR.2.2C-欠陥修正手続きは、欠陥訂正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。

ALC_FLR.2-2 評価者は、それぞれの性質及び影響から、各セキュリティ欠陥の記述が作成されていることを決定するために、これらの手続きの適用を検査しなければならない。

40 その手続きは、それを再現することができるくらい十分に詳細な、セキュリティ欠陥の性質及び影響について記述するために、開発者によって講じられるアクションを識別する。セキュリティ欠陥の性質の記述は、その誤りが、資料内の誤り、TSFの設計の欠陥、TSFの実装の欠陥、その他のどれであるかに対応する。セキュリティ欠陥の影響の記述は、影響が及ぶTSFの部分及びそれらの部分に、どのような影響が及ぶかを識別する。例えば、実装におけるセキュリティ欠陥は、パスワード‘BACKDOOR’による認証を許可することにより、TSFによって実施される識別と認証に影響を及ぼすことが見つかるかもしれない。

ALC_FLR.2-3 評価者は、セキュリティ欠陥ごとの訂正について探索のステータスが識別されていることを決定するために、これらの手続きの適用を検査しなければならない。

41 欠陥修正手続きは、セキュリティ欠陥の異なる段階を識別する。この異なる段階には少なくとも、次のものを含む。その報告が行われた疑わしいセキュリティ欠陥、セキュリティ欠陥の確認が行われた疑わしいセキュリティ欠陥、及びその解決法が実行されたセキュリティ欠陥。追加の段階（例えば、報告が行われたがまだ調査していない欠陥、調査中である欠陥、解決法が見つかったがまだ実行されていないセキュリティ欠陥）を含むことができる。

ALC_FLR.2.3C-欠陥修正手続きは、訂正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。

ALC_FLR.2-4 評価者は、これらの手続きの適用が、各セキュリティ欠陥の訂正アクションを識別することを決定するために、欠陥修正の手続きをチェックしなければならない。

42 訂正アクションは、TOEのハードウェア、ファームウェア、あるいはソフトウェア部分の修理、または、TOEガイダンスの変更、または両方から構成されるかもしれない。TOEガイダンス（例えばセキュリティ欠陥を除去するために取られる手続き的な手段の詳細）の変更を構成する訂正アクションは、恒久的解決法（手続き的な手段が最良の解決法であること決定する際）として役立つものと同様に、暫定的解決法（修理が完了するまで）として役立つ両方の手続き的な手段を含む。

43 セキュリティ欠陥の原因が資料上の誤りである場合、訂正アクションは、影響を受けたTOEガイダンスの更新から構成される。訂正アクションが手続き的な手段である場合、この手段には、これらの訂正する手続きを反映するために影響を受けたTOEガイダンスの更新を含むことになるであろう。

ALC_FLR.2.4C-欠陥修正手続き証拠資料は、TOE利用者に、欠陥情報、訂正、及び訂正行為のガイダンスを提供するために使用する方法を記述しなければならない。

- ALC_FLR.2-5 評価者は、TOE 利用者に各セキュリティ欠陥についての必要な情報を提供する手段について記述されていることを決定するために、欠陥修正手続きの証拠資料を検査しなければならない。
- 44 各セキュリティ欠陥に関する必要な情報は、その記述（ワークユニット ALC_FLR.2-2 の一部として提供される記述と同じ詳細レベルである必要はない）、規定された訂正アクション、及び訂正の実行についてのあらゆる関連するガイダンスから構成される。
- 45 TOE 利用者は、ウェブサイトへの掲載、TOE 利用者への送信、あるいは開発者が訂正をインストールするための取り決めのような、何らかの方法により、情報、訂正、及び資料の最新版を提供されるかもしれない。この情報を提供する手段が、TOE 利用者が起動するアクションを要求する場合、評価者は、それが情報を検索するための指示を含むことを保証するために、あらゆる TOE ガイダンスを検査する。
- 46 情報、訂正、及びガイダンスの提供のために使用される方法の妥当性を評価するためのただ一つの尺度は、TOE 利用者がそれを得るか受け取ることができるという合理的予測である。例えば、必要なデータが 1 か月の間ウェブサイトに掲載され、TOE 利用者は、これが起きること、またこれがいつ起きるかを知っている場合についての公報の方法を考慮すること。これは特に、合理的あるいは有効的とはいえないかもしれない（例えば、ウェブサイトへの恒久的掲載ほどは）が、しかし TOE 利用者が必要な情報を獲得することは実現可能である。一方、わずかに 1 時間だけウェブサイトに情報が掲載され、TOE 利用者がこのこと、あるいはこれがいつ掲載されるかを知る方法を持っていなければ、常に必要な情報を獲得することは実現不可能である。
- ALC_FLR.2.5C-欠陥修正手続き証拠資料は、開発者が TOE の疑わしいセキュリティ欠陥に関する報告及び問合せを、TOE 利用者から受け取る手段について記述しなければならない。
- ALC_FLR.2-6 評価者は、開発者がセキュリティ欠陥の報告、あるいはそのような欠陥の訂正のための要求を受け入れるための手続きが記述されていることを決定するために、欠陥修正手続きを検査しなければならない。
- 47 その手続きは、TOE 利用者が、TOE 開発者と連絡することができる手段を持っていることを保証する。開発者との接触の手段を持っていることによって、利用者はセキュリティ欠陥の報告、セキュリティ欠陥の状況についての質問及び欠陥の訂正を要求することができる。この接触の手段は、非セキュリティ関連の問題を報告するための、より一般的な接触機能の一部であるかもしれない。
- 48 これらの手続きの使用は、TOE 利用者に制限されない。しかしながら、TOE 利用者だけが、これらの手続きの詳細を能動的に供給される。TOE にアクセスできるもの、あるいは TOE をよく知っているものは、報告を開発者に提出するのに同じ手続きを使うことができ、そして開発者は、それら进行处理することが期待される。開発者によって識別されたもの以外の、開発者に報告を提出するいかなる手段も、このワークユニットの範囲外である。他の手段によって生成された報告には、対応する必要はない。
- ALC_FLR.2.6C-報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が訂正され、TOE 利用者に訂正が発行されることを保証しなければならない。

ALC_FLR

ALC_FLR.2-7 評価者は、これらの手続きの適用が、すべての報告された欠陥が訂正されていることを保証する助けになっていることを決定するために、欠陥修正手続きを検査しなければならない。

49 欠陥修正手続きは、開発者の従業員によって発見され、報告されたセキュリティ欠陥だけではなく、TOE 利用者によって報告されたものもカバーする。それぞれの報告されたセキュリティ欠陥が訂正されていることを、どのように保証されているかを記述できるように、その手続きは十分に詳述される。その手続きは、最終的、必然的な解決に結びつく進行を示す筋道のたったステップを含む。

50 その手続きは、疑わしいセキュリティ欠陥が、セキュリティ欠陥であると判断されるポイントから、それが解決されるポイントまでにとられるプロセスを記述する。

ALC_FLR.2-8 評価者は、これらの手続きの適用が、TOE 利用者が各セキュリティ欠陥のための訂正アクションを発行されることを保証するのに役立つことを決定するために、欠陥修正の手続きを検査しなければならない。

51 その手続きは、訂正アクションが提供されるポイントからセキュリティ欠陥が解決されるポイントまでにとられるプロセスについて記述する。訂正アクションを配付するための手続きは、セキュリティ対策方針と一致するべきである。それらは、保証要件に含まれているならば、ADO_DEL を満たす証拠資料として提出された、TOE を配付するために使用される手続きと必ずしも同一である必要はない。例えば、TOE のハードウェア部分が、契約した運送業者によって最初に配送された場合、欠陥修正に起因するハードウェアへの更新は、契約した運送業者によって同様に配送されることが期待される。欠陥修正と無関係な更新は、ADO_DEL 要件を満たす証拠資料に説明された手続きに従う。

ALC_FLR.2.7C-報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる訂正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。

ALC_FLR.2-9 評価者は、これらの手続きの適用が、結果として潜在的な訂正が逆効果になるものを含んでいないことの保護手段になることを決定するために、欠陥修正手続きを検査しなければならない。

52 分析、テスト、あるいはそれら 2 つのコンビネーションを通じて、開発者はセキュリティ欠陥が修正されるとき、逆効果になるものが取り込まれるという可能性を減じられるかもしれない。評価者は、その手続きが与えられた訂正に対して、分析及びテストアクションの必要な組み合わせが、どのように決定されるようになっているかという詳細を提供しているかどうかを評定する。

53 評価者は、例えば、セキュリティ欠陥の原因が証拠資料の問題である場合、手続きは、他の証拠資料に対する矛盾を引き起こさないような保護手段を含んでいることについても決定する。

ALC_FLR.2.8C-欠陥修正ガイダンスは、TOE 利用者が開発者へ TOE の疑わしいセキュリティ欠陥を報告する手段について記述しなければならない。

ALC_FLR.2-10 評価者は、これらの手続きの適用が、結果として、TOE 利用者が疑わしいセキュリティ欠陥の報告、あるいはそのような欠陥の訂正のための要求を提供する手段に

なるものであることを決定するために、欠陥修正のガイダンスを検査しなければならない。

ガイダンスは、TOE 利用者が TOE 開発者と通信する手段があることを保証する。開発者との接触手段を持っていることによって、利用者は、セキュリティ欠陥を報告すること、セキュリティ欠陥の状況に関して問い合わせること、あるいは、欠陥の訂正を要求することができる。

3.3 欠陥修正の評価(ALC_FLR.3)

3.3.1 目的

54 このサブアクティビティの目的は、開発者が、セキュリティ欠陥の追跡、訂正アクションの識別、及び訂正アクション情報の、TOE 利用者への配付について記述した欠陥修正手続きを確立しているかどうかを決定することである。さらに、このサブアクティビティは、開発者の手続きが、セキュリティ欠陥の訂正、TOE 利用者からの欠陥報告の受領、及び訂正が新しいセキュリティ欠陥を取り込まないという保証、各 TOE 利用者の窓口の確立、及び TOE 利用者への訂正アクションのタイムリな発行を提供しているかどうかを決定することである。

55 開発者が TOE 利用者からのセキュリティ欠陥報告に基づいて適切に行動することができるために、TOE 利用者は、開発者にセキュリティ欠陥報告を提出する方法を理解する必要がある。また、開発者は、これらの報告を受領する方法を知る必要がある。TOE 利用者に向けた欠陥修正ガイダンスは、TOE 利用者が開発者と連絡する方法を理解していることを保証する。欠陥修正手続きは、開発者の役割がそのような連絡であることを記述している。

3.3.2 入力

56 このサブアクティビティ用の評価証拠は、次のとおりである。

- a) 欠陥修正手続きの証拠資料
- b) 欠陥修正ガイダンスの証拠資料

3.3.3 評価者アクション

57 このサブアクティビティは、次の1つの CC パート3 評価者アクションエレメントからなる。

- a) ALC_FLR.3.1E

3.3.3.1 アクション ALC_FLR.3.1E

ALC_FLR.3.1C-欠陥修正手続き証拠資料は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.3-1 評価者は、TOE のリリースごとに報告されたすべてのセキュリティ欠陥を追跡するために使用される手続きが記述されていることを決定するために、欠陥修正手続き証拠資料を検査しなければならない。

58 その手続きでは、各々の疑わしいセキュリティ欠陥が報告されたときから、それが解決されるときまでに、開発者によって講じられるアクションについて記述する。これは、欠陥がセキュリティ欠陥であると確認する最初の検出から、セキュリティ欠陥の解決までの、全時間枠を含んでいる。

- 59 欠陥がセキュリティ関連ではないと判明した場合、それをさらに追跡する欠陥修正の手続き(ALC_FLR 要件の目的のため)をする必要はない。単に、なぜ欠陥がセキュリティ関連ではないかの説明のみとなる。
- 60 ALC_FLR.3.2C-欠陥修正手続きは、欠陥訂正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。
- ALC_FLR.3-2 評価者は、それぞれの性質及び影響から、各セキュリティ欠陥の記述が作成されていることを決定するために、これらの手続きの適用を検査しなければならない。
- 61 その手続きは、それを再現することができるくらい十分に詳細な、セキュリティ欠陥の性質及び影響について記述するために、開発者によって講じられるアクションを識別する。セキュリティ欠陥の性質の記述は、その誤りが、資料内の誤り、TSFの設計の欠陥、TSFの実装の欠陥、その他のどれであるかに対応する。セキュリティ欠陥の影響の記述は、影響が及ぶTSFの部分及びそれらの部分に、どのような影響が及ぶかを識別する。例えば、実装におけるセキュリティ欠陥は、パスワード‘BACKDOOR’による認証を許可することにより、TSFによって実施される識別と認証に影響を及ぼすことが見つかるかもしれない。
- ALC_FLR.3-3 評価者は、セキュリティ欠陥ごとの訂正について探索のステータスが識別されていることを決定するために、これらの手続きの適用を検査しなければならない。
- 62 欠陥修正手続きは、セキュリティ欠陥の異なる段階を識別する。この異なる段階には少なくとも、次のものを含む。その報告が行われた疑わしいセキュリティ欠陥、セキュリティ欠陥の確認が行われた疑わしいセキュリティ欠陥、及びその解決法が実行されたセキュリティ欠陥。追加の段階（例えば、報告が行われたがまだ調査していない欠陥、調査中である欠陥、解決法が見つかったがまだ実行されていないセキュリティ欠陥）を含むことができる。
- ALC_FLR.3.3C-欠陥修正手続きは、訂正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。
- ALC_FLR.3-4 評価者は、これらの手続きの適用が、各セキュリティ欠陥の訂正アクションを識別することを決定するために、欠陥修正の手続きをチェックしなければならない。
- 63 訂正アクションは、TOEのハードウェア、ファームウェア、あるいはソフトウェア部分の修理、または、TOEガイダンスの変更、または両方から構成されるかもしれない。TOEガイダンス（例えばセキュリティ欠陥を除去するために取られる手続き的な手段の詳細）の変更を構成する訂正アクションは、恒久的解決法（手続き的な手段が最良の解決法であること決定する際）として役立つものと同様に、暫定的解決法（修理が完了するまで）として役立つ両方の手続き的な手段を含む。
- 64 セキュリティ欠陥の原因が資料上の誤りである場合、訂正アクションは、影響を受けたTOEガイダンスの更新から構成される。訂正アクションが手続き的な手段である場合、この手段には、これらの訂正する手続きを反映するために影響を受けたTOEガイダンスの更新を含むことになるであろう。
- ALC_FLR.3.4C-欠陥修正手続き証拠資料は、TOE利用者に、欠陥情報、訂正、及び訂正行為のガイダンスを提供するために使用する方法を記述しなければならない。

ALC_FLR

ALC_FLR.3-5 評価者は、TOE 利用者に各セキュリティ欠陥についての必要な情報を提供する手段について記述されていることを決定するために、欠陥修正手続きの証拠資料を検査しなければならない。

65 各セキュリティ欠陥に関する必要な情報は、その記述（ワークユニット ALC_FLR.3-2 の一部として提供される記述と同じ詳細レベルである必要はない）、規定された訂正アクション、及び訂正の実行についてのあらゆる関連するガイダンスから構成される。

66 TOE 利用者は、ウェブサイトへの掲載、TOE 利用者への送信、あるいは開発者が訂正をインストールするための取り決めのような、何らかの方法により、情報、訂正、及び資料の最新版を提供されるかもしれない。この情報を提供する手段が、TOE 利用者が起動するアクションを要求する場合、評価者は、それが情報を検索するための指示を含むことを保証するために、あらゆる TOE ガイダンスを検査する。

67 情報、訂正、及びガイダンスの提供のために使用される方法の妥当性を評価するためのただ一つの尺度は、TOE 利用者がそれを得るか受け取ることができるという合理的予測である。例えば、必要なデータが 1 か月の間ウェブサイトに掲載され、TOE 利用者は、これが起きること、またこれがいつ起きるかを知っている場合についての公報の方法を考慮すること。これは特に、合理的あるいは有効的とはいえないかもしれない（例えば、ウェブサイトへの恒久的掲載ほどは）が、しかし TOE 利用者が必要な情報を獲得することは実現可能である。一方、わずかに 1 時間だけウェブサイトが情報が掲載され、TOE 利用者がこのこと、あるいはこれがいつ掲載されるかを知る方法を持っていなければ、常に必要な情報を獲得することは実現不可能である。

68 開発者に登録する TOE 利用者にとって（ワークユニット ALC_FLR.3_12 参照）この情報の受動的可用性は、十分ではない。開発者は登録された TOE 利用者へ、情報（あるいは、その可用性の通知）を能動的に送らなければならない。

ALC_FLR.3.5C-欠陥修正手続き証拠資料は、開発者が TOE の疑わしいセキュリティ欠陥に関する報告及び問合せを、TOE 利用者から受け取る手段について記述しなければならない。

ALC_FLR.3-6 評価者は、開発者がセキュリティ欠陥の報告、あるいはそのような欠陥の訂正のための要求を受け入れるための手続きが記述されていることを決定するために、欠陥修正手続きを検査しなければならない。

69 その手続きは、TOE 利用者が、TOE 開発者と連絡することができる手段を持っていることを保証する。開発者との接触の手段を持っていることによって、利用者はセキュリティ欠陥の報告、セキュリティ欠陥の状況についての質問及び欠陥の訂正を要求することができる。この接触の手段は、非セキュリティ関連の問題を報告するための、より一般的な接触機能の一部であるかもしれない。

70 これらの手続きの使用は、TOE 利用者に制限されない。しかしながら、TOE 利用者だけが、これらの手続きの詳細を能動的に供給される。TOE にアクセスできるもの、あるいは TOE をよく知っているものは、報告を開発者に提出するのに同じ手続きを使うことができ、そして開発者は、それら进行处理することが期待される。開発者によって識別されたもの以外の、開発者に報告を提出するいかなる手段も、このワークユニットの範囲外である。他の手段によって生成された報告には、対応する必要はない。

ALC_FLR.3.6C-報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が訂正され、TOE 利用者に訂正が発行されることを保証しなければならない。

ALC_FLR.3-7 評価者は、これらの手続きの適用が、すべての報告された欠陥が訂正されていることを保証する助けになっていることを決定するために、欠陥修正手続きを検査しなければならない。

71 欠陥修正手続きは、開発者の従業員によって発見され、報告されたセキュリティ欠陥だけではなく、TOE 利用者によって報告されたものもカバーする。それぞれの報告されたセキュリティ欠陥が訂正されていることを、どのように保証されているかを記述できるように、その手続きは十分に詳述される。その手続きは、最終的、必然的な解決に結びつく進行を示す筋道のたったステップを含む。

72 その手続きは、疑わしいセキュリティ欠陥が、セキュリティ欠陥であると判断されるポイントから、それが解決されるポイントまでにとられるプロセスを記述する。

ALC_FLR.3-8 評価者は、これらの手続きの適用が、TOE 利用者が各セキュリティ欠陥のための訂正アクションを発行されることを保証するのに役立つことを決定するために、欠陥修正の手続きを検査しなければならない。

73 その手続きは、訂正アクションが提供されるポイントからセキュリティ欠陥が解決されるポイントまでにとられるプロセスについて記述する。訂正アクションを配付するための手続きは、セキュリティ対策方針と一致するべきである。それらは、保証要件に含まれているならば、ADO_DEL を満たす証拠資料として提出された、TOE を配付するために使用される手続きと必ずしも同一である必要はない。例えば、TOE のハードウェア部分が、契約した運送業者によって最初に配送された場合、欠陥修正に起因するハードウェアへの更新は、契約した運送業者によって同様に配送されることが期待される。欠陥修正と無関係な更新は、ADO_DEL 要件を満たす証拠資料に説明された手続きに従う。

ALC_FLR.3.7C-報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる訂正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。

ALC_FLR.3-9 評価者は、これらの手続きの適用が、結果として潜在的な訂正が逆効果になるものを含んでいないことの保護手段になることを決定するために、欠陥修正手続きを検査しなければならない。

74 分析、テスト、あるいはそれら 2 つのコンビネーションを通じて、開発者はセキュリティ欠陥が修正されるとき、逆効果になるものが取り込まれるという可能性を減じられるかもしれない。評価者は、その手続きが与えられた訂正に対して、分析及びテストアクションの必要な組み合わせが、どのように決定されるようになっているかという詳細を提供しているかどうかを評定する。

75 評価者は、例えば、セキュリティ欠陥の原因が証拠資料の問題である場合、手続きは、他の証拠資料に対する矛盾を引き起こさないような保護手段を含んでいることについても決定する。

ALC_FLR.3.8C-欠陥修正ガイダンスは、TOE 利用者が開発者へ TOE の疑わしいセキュリティ欠陥を報告する手段について記述しなければならない。

ALC_FLR

ALC_FLR.3-10 評価者は、これらの手続きの適用が、結果として、TOE 利用者が疑わしいセキュリティ欠陥の報告、あるいはそのような欠陥の訂正のための要求を提供する手段になるものであることを決定するために、欠陥修正のガイダンスを検査しなければならない。

ガイダンスは、TOE 利用者が TOE 開発者と通信する手段があることを保証する。開発者との接触手段を持っていることによって、利用者は、セキュリティ欠陥を報告すること、セキュリティ欠陥の状況に関して問い合わせること、あるいは、欠陥の訂正を要求することができる。

ALC_FLR.3.9C-欠陥修正手続きは、セキュリティ欠陥により影響を受ける登録された利用者に、セキュリティ欠陥報告及びそれに関連する訂正を自動配付するために、タイムリな応答を要求する手続きを含まなければならない。

ALC_FLR.3-11 評価者は、これらの手続きの適用が、結果として、各セキュリティ欠陥の報告及び訂正に関連するものに影響されるかもしれない登録された TOE 利用者に対して提供される、タイムリな手段になるかということを決断するために、欠陥修正手続を検査しなければならない。

76 適時の発行は、セキュリティ欠陥報告及び関連する訂正の、両方の発行に適用される。しかしながら、これらを同時に発行する必要はない。「TOE を止める」というような劇的な解であったとしても、仮の解が見つかり次第、欠陥報告が生成され、発行されるべきであるということが認識される。また、より永続的な（そしてあまり劇的ではない）解が見つかる場合、不適切に遅れることなく発行されるべきである。

77 セキュリティ欠陥により影響されるかもしれない TOE 利用者だけに、報告及び関連する訂正の受取人を制限することは不必要である。そのようなタイムリなやり方でなされているならば、すべての TOE 利用者は、すべてのセキュリティ欠陥に対する、そのような報告及び訂正を与えられることが許される。

ALC_FLR.3-12 評価者は、これらの手続きの適用が、結果として、影響されるかもしれない登録された TOE 利用者への報告及び関連する訂正の自動配付になるかということを決断するために、欠陥修正手続きを検査しなければならない。

78 自動配付は、配付方法に関して人間の介在が許されないということを意味しているわけではない。実際、配付方法は、報告または訂正の発行の欠陥における、あらかじめ規定されたエスカレーションを伴う、おそらく緊密にモニターされた手続きを通してなされる、マニュアル化された手続きだけから構成することができる。

79 セキュリティ欠陥により影響されるかもしれない TOE 利用者だけに、報告及び関連する訂正の受取人を制限することは不必要である。そのようなものが自動的になされるようになっていけば、すべての TOE 利用者は、すべてのセキュリティ欠陥に対する、そのような報告及び訂正を与えられることが許される。

ALC_FLR.3.10C-欠陥修正ガイダンスは、TOE利用者が開発者にセキュリティ欠陥報告及び訂正を受け取る資格を得るために登録する手段について記述しなければならない。

ALC_FLR.3-13 評価者は、TOE 利用者が開発者に登録することを可能にする手段について記述していることを決定するために、欠陥修正ガイダンスを検査しなければならない。

- 80 *TOE 利用者を開発者に登録することを可能にすることは、単にそれぞれの TOE 利用者が、開発者に窓口を提供する方法を持つことを意味する。この窓口は、セキュリティ欠陥へのあらゆる訂正に従って、その TOE 利用者に影響するかもしれないセキュリティ欠陥と関連する情報を TOE 利用者に提供するために使用される。TOE 利用者の登録は、ソフトウェアライセンスを登録する目的のため、あるいは更新及び他の有用な情報を獲得するために、TOE 利用者が開発者に、利用者自身を識別させる、標準的な手続の一部として遂行されるかもしれない。*
- 81 設置される TOE 毎に、1 人の登録された TOE 利用者がある必要はない。1 つの組織に対して、1 人の登録された TOE 利用者がいれば十分であろう。例えば、企業の TOE 利用者は、そのすべてのサイトに対して 1 つの集中化された購買部門を持つかもしれない。この場合、購買部門は、TOE 利用者に対して、十分な窓口になるであろう。そうすると、すべての利用者の設置した TOE が、1 つの登録された窓口を持つようになる。
- 82 いずれの場合も、各 TOE に対して登録された利用者があることを保証するために、いくつもの異なる住所を持つ組織に対して、配付された各 TOE を、1 つの組織に関連づけることが可能でなくてはならない。これは、ある登録された TOE 利用者によって、誤ってカバーされていると推測をする利用者がいないことを保証する。
- 83 TOE 利用者は、登録する必要がないことを注意すべきである。彼らは、登録する手段を提供されなければならないだけである。しかしながら、登録することを選択する利用者は、情報（あるいは、その可用性の通知）を直接送られなければならない。
- ALC_FLR.3.11C-欠陥修正ガイダンスは、TOE に含まれるセキュリティ問題に関するすべての報告及び問合せを受け付けるための窓口を識別しなければならない。*
- ALC_FLR.3-14 評価者は、TOE を含むセキュリティ問題に関する報告及び問合せのための特定の窓口が識別されていることを決定するために、欠陥修正ガイダンスを検査しなければならない。**
- 84 ガイダンスは、登録された TOE 利用者が、TOE 内で発見されたセキュリティ欠陥を報告するために開発者とやり取りをすることができ、あるいは TOE 内で発見されたセキュリティ欠陥に関する問合せをすることができる手段を含んでいる。

附属書 A： 欠陥修正の評価基準

- 85 この附属書は解釈 CCIMB-INTERP-062 及び CCIMB-INTERP-092 を含む、CC バージョン 2.1 パート 3 の 12.2 節に置換テキストを提供する。次のテキストは解釈 CCIMB-INTERP-094 に置き換わる。それは読者が本書の主要な本体の中で提供される方法論を理解し用いるのを援助するために提供される。オリジナルの CC 段落番号が参照用のために保持されたことに注意すること。さらに、変更線は変更が CC テキスト内にどこで起こったか示すために使用されている。

12.2 欠陥修正 (ALC_FLR)

目的

- 388 欠陥修正は、発見されたセキュリティ欠陥が開発者により追跡され訂正されることを要求する。TOE 評価時に、将来欠陥修正手続きが遵守されることを決定できないが、開発者が適切に、欠陥を追跡、訂正し、欠陥の情報と訂正を配付するための方針と手続きを評価することは可能である。

コンポーネントのレベル付け

- 389 ファミリのコンポーネントは、欠陥修正手続きの対象範囲の拡大と、欠陥修正方針の厳密さに基づいて、レベル付けされている。

適用上の注釈

- 390 このファミリーは、TOE の開発者に TOE の欠陥を追跡し訂正することを要求することにより、TOE が将来に渡って維持継続されることを保証するものである。さらに、その欠陥訂正を配付するための要件も含んでいる。しかし、このファミリーは、現在の評価の範囲を超えた評価要求を課するものではない。

TOE 利用者は、セキュリティ欠陥に対する処置を受け取る及び実装することに責任を負う利用者組織において、中心であると考えられる。これは必ずしも個々の利用者ではなく、セキュリティ欠陥の取り扱いに責任を負う、組織的な代表者であってもよい。用語「TOE 利用者」の使用は、異なる組織が個々の利用者でもよいしあるいは中央行政機関によって行われてもよい欠陥報告を扱うための異なる手続きを持っていることを認識する。

- 391 欠陥修正手続きは、可能性のあるすべてのタイプの欠陥についての対処方法を記述しなければならない。これらの欠陥は、開発者によって、TOE の利用者によって、あるいは TOE について熟知している他の機関によって報告されるかもしれない。ある欠陥は、直ちに修繕できないかもしれない。欠陥が修正できず、他の（例えば、手続き的な）手段が取られなければならない場合もありうる。提供される証拠資料は、運用サイトに修正を提供したり、修正が遅れている（その間何をすればよいか）または修正ができない欠陥に関する情報を提供する手続きを含まなければならない。

一旦 TOE の評価が完了していれば、それはもはや評価の対象ではない。さらに、この評価済み TOE へのどんな変更も、オリジナルの評価結果がもはや変更されたバージョンに適用できないことになる。このファミリの中で使用される句「TOE のリリース」は、それ故に変更が適用され認証済み TOE のリリースである製品またはシステムのバージョンのことをいう。

ALC_FLR.1 基本的な欠陥修正

依存性：なし

開発者アクションエレメント：

ALC_FLR.1.1D 開発者は、**TOE開発者に対する欠陥修正手続きを提供**しなければならない。

証拠の内容・提示エレメント：

ALC_FLR.1.1C 欠陥修正手続き証拠資料は、TOEのリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.1.2C 欠陥修正手続きは、欠陥訂正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。

ALC_FLR.1.3C 欠陥修正手続きは、訂正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。

ALC_FLR.1.4C 欠陥修正手続き証拠資料は、TOE利用者に、欠陥情報、訂正、及び訂正行為のガイダンスを提供するために使用する方法を記述しなければならない。

評価者アクションエレメント：

ALC_FLR.1.1E 評価者は、提供された情報が、証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。

ALC_FLR.2 欠陥報告手続き

目的

TOE 利用者は、開発者が TOE 利用者からのセキュリティ欠陥報告に基づいて適切に行動することができ、かつ誰に訂正処置を送るかを知ることができるために、開発者にセキュリティ欠陥報告を提出する方法を理解する必要がある。開発者から TOE 利用者への欠陥修正ガイダンスは、TOE 利用者がこの重要な情報に気づいていることを保証する。

ALC_FLR

依存性：なし

開発者アクションエレメント：

- ALC_FLR.2.1D 開発者は、**TOE開発者に対する**欠陥修正手続きを**提供**しなければならない。
- ALC_FLR.2.2D 開発者は、**すべてのセキュリティ欠陥の報告とそれらの欠陥の訂正要求を受け付け、処理する手続きを確立**しなければならない。
- ALC_FLR.2.3D 開発者は、**TOE利用者に対する欠陥修正ガイダンスを提供**しなければならない。

証拠の内容・提示エレメント：

- ALC_FLR.2.1C 欠陥修正手続き証拠資料は、TOEのリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。
- ALC_FLR.2.2C 欠陥修正手続きは、欠陥訂正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。
- ALC_FLR.2.3C 欠陥修正手続きは、訂正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。
- ALC_FLR.2.4C 欠陥修正手続き証拠資料は、TOE利用者に、欠陥情報、訂正、及び訂正行為のガイダンスを提供するために使用する方法を記述しなければならない。
- ALC_FLR.2.5C **欠陥修正手続き証拠資料は、開発者がTOEの疑わしいセキュリティ欠陥に関する報告及び問合せを、TOE利用者から受け取る手段について記述**しなければならない。
- ALC_FLR.2.6C 報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が訂正され、TOE利用者に訂正が発行されることを保証しなければならない。
- ALC_FLR.2.7C 報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる訂正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。
- ALC_FLR.2.8C **欠陥修正ガイダンスは、TOE利用者が開発者へTOEの疑わしいセキュリティ欠陥を報告する手段について記述**しなければならない。

評価者アクションエレメント：

- ALC_FLR.2.1E 評価者は、提供された情報が、証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。

ALC_FLR.3 システム化された欠陥修正

目的

TOE 利用者は、開発者が TOE 利用者からのセキュリティ欠陥報告に基づいて適切に行動することができ、かつ誰に訂正処置を送るかを知ることができるために、

開発者にセキュリティ欠陥報告を提出する方法と、開発者がこれらの訂正処置を受け取ることができるように、開発者に対して TOE 利用者自身を登録する方法を理解する必要がある。開発者から TOE 利用者への欠陥修正ガイダンスは、TOE 利用者がこの重要な情報に気づいていることを保証する。

依存性：なし

開発者アクションエレメント：

ALC_FLR.3.1D 開発者は、TOE開発者に対する欠陥修正手続きを提供しなければならない。

ALC_FLR.3.2D 開発者は、すべてのセキュリティ欠陥の報告とそれらの欠陥の訂正要求を受け付け、処理する手続きを確立しなければならない。

ALC_FLR.3.3D 開発者は、TOE利用者に対する欠陥修正ガイダンスを提供しなければならない。

証拠の内容・提示エレメント：

ALC_FLR.3.1C 欠陥修正手続き証拠資料は、TOEのリリースごとに報告されたすべてのセキュリティ欠陥を追跡するのに使用する手続きを記述しなければならない。

ALC_FLR.3.2C 欠陥修正手続きは、欠陥訂正方法の調査状況の記述と同時に、各々のセキュリティ欠陥の性質と影響の記述が、提供されることを要求しなければならない。

ALC_FLR.3.3C 欠陥修正手続きは、訂正行為が、各々のセキュリティ欠陥を識別することを要求しなければならない。

ALC_FLR.3.4C 欠陥修正手続き証拠資料は、TOE利用者に、欠陥情報、訂正、及び訂正行為ガイダンスを提供するために使用する方法を記述しなければならない。

ALC_FLR.3.5C 欠陥修正手続き証拠資料は、開発者がTOE利用者からのTOEの疑わしいセキュリティ欠陥に関する問合せや、報告を受け取る手段について記述しなければならない。

ALC_FLR.3.6C 報告されたセキュリティ欠陥を処理する手続きは、報告されたすべての欠陥が訂正され、TOE利用者に訂正が発行されることを保証しなければならない。

ALC_FLR.3.7C 報告されたセキュリティ欠陥を処理する手続きは、これらのセキュリティ欠陥のいかなる訂正も、新規の欠陥を引き起こすことのないよう、保護手段を提供しなければならない。

ALC_FLR.3.8C 欠陥修正ガイダンスは、TOE利用者が開発者へTOEの疑わしいセキュリティ欠陥を報告する手段について記述しなければならない。

ALC_FLR.3.9C 欠陥修正手続きは、セキュリティ欠陥により影響を受ける登録された利用者に、セキュリティ欠陥報告及びそれに関連する訂正を自動配付するために、タイムリな応答を要求する手続きを含まなければならない。

ALC_FLR.3.10C 欠陥修正ガイダンスは、TOE利用者が開発者にセキュリティ欠陥報告及び訂正を受け取る資格を得るために登録する手段について記述しなければならない。

ALC_FLR.3.11C 欠陥修正ガイダンスは、TOEに含まれるセキュリティ問題に関するすべての報告及

び問合せを受け付けるための窓口を識別しなければならない。

評価者アクションエレメント：

ALC_FLR.3.1E 評価者は、提供された情報が、証拠の内容・提示に対する要件をすべて満たしていることを確認しなければならない。