本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。

正式な文書は、以下の URL よりダウンロード可能です。

https://www.niap-ccevs.org/pp/pp_gpos_v3.9-add1.pdf

汎用オペレーティングシステム
プロテクションプロファイル

コモンクライテリアプロテクションプロファイルの開発へ向けた NIAP 及び BSI の共同作業

バージョン 3.9
第 2 部：OSPP 評価の一般的アプローチ及び保証アクティビティ

平成 25 年 11 月 12 日　翻訳 暫定第 0.1 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

概論

この文書では、OSPP 第 1 部に提示された汎用オペレーティングシステム及び基本的なセキュリティ機能要件に特化した保証アクティビティのアイディアを提示する。第 1 部は安定的であるとみなされるが、この文書はいまだに作業中の草案であり、数本のホワイトペーパーを取りまとめ、SFR 関連の保証アクティビティを定義することによって作成されている。

ここに取り込まれた 3 本のホワイトペーパーは、以下の話題を取り扱っている。

- 評価に必要とされる開発者文書へのアプローチ
- テストへの一般的アプローチ（個別の SFR に特化したテスト要件は、SFR 関連保証アクティビティの記述に含まれている）
- 脆弱性分析への一般的アプローチ

これらは全体的なフレームワークを提示するものであり、さまざまな SFR に対する保証アクティビティによって支持されている。

特定の話題をまとめて取り扱うために、管理 SFR に対する保証アクティビティは、それらが管理する機能によってまとめられている。これによって、特定の機能の分析及びテストが、その機能に関して許可された構成の定義と変更を行う管理機能と連携して行われることが可能となる。

以下の表は、OSPP 中の各 SFR に対する保証アクティビティの仕様がどこに記載されているかを示したものである。

SFR	**保証アクティビティ**
FAU_GEN.1	セキュリティ監査に関する保証アクティビティ
FAU_GEN.2	セキュリティ監査に関する保証アクティビティ
FAU_SAR.1	セキュリティ監査に関する保証アクティビティ
FAU_SAR.2	セキュリティ監査に関する保証アクティビティ
FAU_SEL.1	セキュリティ監査に関する保証アクティビティ
FAU_STG.1	セキュリティ監査に関する保証アクティビティ
FAU_STG.3	セキュリティ監査に関する保証アクティビティ
FAU_STG.4	セキュリティ監査に関する保証アクティビティ
FDP_ACC.1	利用者データ保護に関する保証アクティビティ
FDP_ACF.1	利用者データ保護に関する保証アクティビティ
FDP_IFC.1	利用者データ保護に関する保証アクティビティ

SFR	保証アクティビティ
FDP_IFF.1	利用者データ保護に関する保証アクティビティ
FDP_RIP.2	利用者データ保護に関する保証アクティビティ
FIA_AFL.1	識別と認証に関する保証アクティビティ
FIA_ATD.1	識別と認証に関する保証アクティビティ
FIA_UAU.1(RITE)	識別と認証に関する保証アクティビティ
FIA_UAU.1(HU)	識別と認証に関する保証アクティビティ
FIA_UAU.5	識別と認証に関する保証アクティビティ
FIA_UAU.7	識別と認証に関する保証アクティビティ
FIA_UID.1	識別と認証に関する保証アクティビティ
FIA_USB.1	識別と認証に関する保証アクティビティ
FIA_PK_EXT.1	識別と認証に関する保証アクティビティ
FMT_MOF.1	識別と認証に関する保証アクティビティ
FMT_MSA.1	利用者データ保護に関する保証アクティビティ
FMT_MSA.3(DAC)	利用者データ保護に関する保証アクティビティ
FMT_MSA.3(NI)	利用者データ保護に関する保証アクティビティ
FMT_MSA.4	利用者データ保護に関する保証アクティビティ
FMT_MTD.1(AE)	セキュリティ監査に関する保証アクティビティ
FMT_MTD.1(AS)	セキュリティ監査に関する保証アクティビティ
FMT_MTD.1(AT)	セキュリティ監査に関する保証アクティビティ
FMT_MTD.1(AF)	セキュリティ監査に関する保証アクティビティ
FMT_MTD.1(CM)	識別と認証に関する保証アクティビティ
FMT_MTD.1(NI)	利用者データ保護に関する保証アクティビティ
FMT_MTD.1(IAT)	識別と認証に関する保証アクティビティ
FMT_MTD.1(IAF)	識別と認証に関する保証アクティビティ

SFR	**保証アクティビティ**
FMT_MTD1(IAU)	識別と認証に関する保証アクティビティ
FMT_REV.1(OBJ)	利用者データ保護に関する保証アクティビティ
FMT_REV.1(USR)	*作業中*
FMT_SMF_RMT.1	*作業中*
FMT_SMR.1	*作業中*
FPT_STM.1	FPT_STM.1 及び FTA_SSL に関する保証アクティビティ
FTA_SSL.1	FPT_STM.1 及び FTA_SSL に関する保証アクティビティ
FTA_SSL.2	FPT_STM.1 及び FTA_SSL に関する保証アクティビティ
FTP_ITC.1	高信頼パス／チャネルに関する保証アクティビティ

この文書は、これらの保証アクティビティの最初の草案であり、また OSPP を用いて行われる最初の試行評価によって完成され、詳細化されることが期待されている。特に、一般的な欠陥仮説のリストはいまだに不完全であるため、この文書の次期バージョンにおいて詳細化される予定である。また、SFR に対する保証アクティビティのさらなる詳細が、試行評価において得られた経験から追加される予定である。

以下に記述する保証アクティビティは、コモンクライテリアのパート 2 及び CEM 中の関連ワークユニットにおいて定義されているセキュリティ保証要件の詳細化を意図している。コモンクライテリアのパート 2 から、この文書の著者らが汎用オペレーティングシステム製品の評価に必要と認めた評価保証アクティビティを反映して、一連の保証コンポーネントが選択されている。この一連の保証コンポーネントはコモンクライテリアのパート 2 において定義される評価保証レベルのひとつではないが、CCRA によってカバーされる保証コンポーネントから構成されている。

最終的な目標は、汎用オペレーティングシステムのように複雑な IT 製品の評価を、可能な限り客観的かつ再現可能なものにすることである。

文書化に関するホワイトペーパー

評価者によって行われる保証アクティビティに関して合意に至るためには、我々が提供を期待する情報のレベルと、その情報を用いる方法に関する評価者への期待について合意する必要がある。我々の提案するアプローチが、このホワイトペーパーに文書化されている。

管理ガイダンス及び利用者ガイダンスに何が期待されるのかについては合意が存在していると我々は確信しているので、その文書化については包括的に論じることはしない。しかし、このホワイトペーパーによって記述された文書中で論じられる一部のシステムエレメントは、管理ガイダンスの内容に影響を与えることになる。これらの側面については、以下で論じる。対象となる文書は、インタフェース文書とアーキテクチャ設計文書に分類される。

この情報を用いてなされる活動の目標のひとつは、評価チームによって分析されテストされたインタフェースの明確なリストをエンドユーザやアプリケーション作成者へ提供することである、ということは重要であるため記憶されたい。

脆弱性分析及びテストを構成するアクティビティは、別個のホワイトペーパーにおいて記述されるべく残されている。

要求される文書化の原則

文書への要件を定式化するにあたっては、コモンクライテリア評価に関してコミュニティが取っている方向に一貫していると我々が感じる、いくつかの原則にしたがった。その原則は、以下のとおりである。

- CC 特有の文書の大規模な作成は奨励されない。評価は、既存の開発者文書に基づいて行われるべきである（should）。ベンダが何らかの文書（セキュリティターゲット）を開発することは避けられないが、この文書化要件の意図は、この文書化を最小限のものとすることである。開発者は、新たな文書を作成するよりも既存の文書を参照することが奨励される。評価されるセキュリティ機能と直接対話するインタフェースに関する情報は、公的に文書化されるべきである（should）。例外（例えば、ラッパが文書化されたインタフェースを形成するが技術的にはインタフェースではなく、「技術的」インタフェースが通知されていないかその仕様が独占的と考えられる場合）はあるかもしれないが、まれなはずである（should）。
- インタフェース記述は、PP/ST 中のセキュリティ要件を実装するセキュリティ機能の仕様を可能とすること、またこの機能が通知されたインタフェースを介してテストされているということをエンドユーザへ例証することに集中して提供されるべきである。インタフェースがセキュリティ機能と間接的に相互作用する場合（例えば、外部のサポートを提供するエンティティへインタフェースを提供する場合）もあるかもしれないが、このようなインタフェースもまた十分に文書化される必要がある。
- ハードウェア及びソフトウェア両方の特権メカニズム、ならびにシステム初期化コードの利用及び悪用はシステム全体のセキュリティに多大な影響を与えるため、実装された特権メカニズムとシステム起動／初期化との間の相互作用及び構造に関連する文書が、アーキテクチャ設計情報として提供されなくてはならない（must）。

- 特権に関する懸念と同様に、製品が採用する保護メカニズムの健全性もまた、製品のセキュリティ体制に決定的な役割を果たしている。これらのメカニズムの特定と、それらが使用されている方法が、アーキテクチャ設計中に記述されなくてはならない（must）。
- 評価の目的は、特定されたインタフェース及び記述されたセキュリティ機能がSFR を満たすこと、そして期待通りに振る舞うことを確実にすることであり、分析及びブラックボックステストによって達成される。もうひとつの目的は、製品の初期化プロセスがセキュアな状態に帰着することを確実にすることである。また、さらに別の目的は、保護メカニズムと特権の使用が十分に記述され検証されているかどうかを判定することである。これらの目的に関連したアクティビティを行っている最中に、文書化されずに残っているセキュリティ関連インタフェースや設計の側面を発見することもあるかもしれないが、それはこのアクティビティの主目的ではない。脆弱性分析を行うことによって製品の攻撃耐性を判定するという最終的な目的においては、開発者から提供されたセットから除外されたインタフェースを評価者が考慮してもよい。
- アーキテクチャ設計の提供には、さまざまなアプローチを取ることが可能である。ベンダが提供した自明な分解でも要件に適合することはあるかもしれないが、我々が期待しているのはシステムの特権アーキテクチャを正確に反映したより堅牢な分解と、評価者とスキームがこのアーキテクチャに関して公的なコメントを提供するという事実が、自明な分解の場合よりもマーケティング的な利点を提供するとみなされることである。

インタフェースとインタフェース仕様

インタフェース仕様に関してここで考慮する 2 つの側面は、評価アクティビティの最中に考慮されるべきインタフェースの特定と、各インタフェースに対して提供される必要のある情報である。我々の提案するアプローチは、PP/ST 中のセキュリティ機能要件と関連付けられたインタフェースのセットを特定すること､及びインタフェースを各 SFR コンポーネントへ対応させることをベンダに要求することである。提供される情報はインタフェースの単なる特定（利用者ガイドやマニュアルページやオンライン文書、あるいは場合によっては通知されないインタフェースの独占的文書中の情報への参照）であって、これらの記述には特定の文書化や要件は課されない。これらのインタフェースは公共向け文書に規定されることが必然とされるため、評価者がインタフェースをテストできなくなるような不足があれば、それもまたエンドユーザへ提示されることになり、そのような不足はベンダによって修正されるか、評価レポート中に注記されることになるであろう。またそのような不足は、脆弱性分析アクティビティの中で調査対象となることが証明されるかもしれない。

インタフェースの特定に加えて､ベンダはインタフェースから該当する SFR への対応付けを示さなくてはならない（must）。これは、製品のセキュリティメカニズムの機能テストの基礎となることだろう。

ベンダにインタフェースの特定と対応付けを提供させることによって、完全性の疑問が生じることは当然である。すなわち、所与のセキュリティメカニズムに該当するインタフェースがすべて正しく特定され関連付けられていることに関して、エンドユーザがどれほど確信を持てるかということである。モダンなオペレーティングシステムについて完全性の

議論を行うことは非常に困難であると我々が確信しているという事実を考慮すると、開発者が完全に外部インタフェースのセットを決定してそのリストを評価者へ提供すること、あるいは評価者がインタフェース（及びその他の）文書を厳格に分析して完全性を確証することに関しては、要件は存在しない。

しかし、これに関して 2 つの警告がある。まず、対応付けられたインタフェースは ST 中に文書化されることになるため、その文書を読んだエンドユーザは自分の関心のあるメカニズムがテストされたかどうかを判断できるということである。例えば、I&A の 1 つの手法（例えば、パスワードを用いたログオン）がテストされているが、代替メカニズム（例えば、証明書を用いたログオン）はテストされなかった、ということがあり得る。この場合、ログオンに証明書が必要とされる環境でそのシステムを使用したければ、(使用する組織による）追加テストが必要となることを、エンドユーザは知ることになるであろう。

次に、ベンダによって特定または対応付けられていないいかなるインタフェースも、脆弱性分析アクティビティにおける評価チームの調査対象となることである。例えば、評価チームがベンダによって特定されていないインタフェースであって、セキュリティ方針（ST 中の SFR によって強制される方針を意味する)の危殆化に用いられることが可能なものを発見した場合には、脆弱性分析を行うことができ、欠陥が（確認された場合には）ベンダによって対処する必要があるだろう。

アーキテクチャ設計の文書化

評価アクティビティをサポートするために必要とされる設計文書は、製品によって提供される特権及び保護メカニズムとともに、セキュリティメカニズムの一体的な記述に集中して製品のアーキテクチャ的な概観を提示する。また、製品の最初のセキュアな状態への初期化も記述される。ユーザモードまたは同様のドメインにおいて動作する特権プログラムには、特別な注意が払われる。これはセキュリティの危殆化が発生する源となりやすく、またカーネル内部よりも容易に分析ができるためである。

この情報は非独占的であって TOE 要約仕様に含まれることが期待されるため、この設計記述のもうひとつの目標は、アプリケーション開発者やシステムインテグレータを含む利用者のコミュニティが、製品のアーキテクチャ、及び評価範囲に何が含まれていたのかを明確に理解することである。

セキュリティ機能記述

記述する必要のある設計の 1 つの側面は、セキュリティ機能の視点から製品を概観することである。これには、コンポーネント、あるいは場合によってはコンポーネントの集まりの視点からの、SFR に基づいたセキュリティ機能の描写が含まれるであろう。例えば、記述には監査サブシステム、I&A サブシステム、アクセス制御サブシステムなどが提示されることになるであろう。この提示の目標は、SFR の規定するすべての要件をカバーしつつ、複数のメカニズムがどのように連携して動作するか、という議論を提示することである。要件を単にオウム返しにすることは推奨されないが、逆に疑似コードも要求されるべきではない（should not)。この記述は、SFR に記述されているものを越えた、システム特有の詳細を提供することになる。場合によっては、一般的または高レベルで SFR が規定されてもよいし、また特定の実装を反映する「導出された」要件（例えば、テスト可能な主張）の提供が必要とされてもよい。これらの場合、開発者または評価者は、製品の外部インタフェースをこの粒度に対応付けることになる。このレベルの詳細化された情報は、評価者がテストアクティビティを行う助けとなるであろう。

特権アーキテクチャ記述

特権アーキテクチャ記述においては、ハードウェアかソフトウェアか、あるいはその両方によるものかに関わらず、採用されている特権メカニズムを記述する。製品がハードウェアによる特権メカニズム（例えば、汎用オペレーティングシステムやネットワーク製品）を用いている場合には、どのハードウェアメカニズムが用いられているか、用いられている特権の粒度のレベル（例えば、4 つのリングのリング 0 及びリング 3、4 の特権レベルを用いて実装された特権／非特権）、システムのどの部分にさまざまな特権レベルが割り当てられているのか、を記述する。ここで「システムの部分」は、例えば「カーネル」、「デバイスドライバ」といった大規模な単位を意味する。これは、単一のハードウェア特権レベル内で動作しているエンティティを分解して記述することを求めるものではない。記述のこの部分のポイントは、ハードウェアを利用して製品が提供する分離の程度の概観を、読者へ提供することである。

ソフトウェアによる特権を実装する製品については、特権アーキテクチャ記述はソフトウェア特権メカニズムを、粒度のレベル、それぞれの特権レベルがどのリソースへのアクセスを許可されるか、及びそれぞれの特権でどのシステムの部分が動作しているのか、と共に説明する。この議論の目的では、「システムの部分」はハードウェア特権レベルによってグループ分けされる。例えば、（特権モードで動作している）カーネルが 15 個の特権を実装／チェックしている場合、カーネルがこれらの特権を制御していると特定されれば十分であり、さらなるカーネルの分解は必要とされない。非特権ハードウェアモードにおいて特権を実装しているシステムの部分については、それぞれのエンティティ（通常は、プロセスなどのスケジュール可能なエンティティ）が、その動作する特権と共に特定される。製品が複数のハードウェア保護モード（例えば、カーネルがリング 0、ドライバがリング 1、そしてユーザプログラムがリング 3）を実装している場合、ユーザモードプログラムが動作するハードウェアモードのみが、この議論における「非特権ハードウェアモード」とみなされることに注意されたい。

特権の使用または非特権ハードウェアモードの製品の部分へのアクセス（例えば、「高信頼プロセス」）に関連して利用者（管理者も信頼されていない利用者も、コマンドラインまたは GUI タイプのインタフェース、もしくはプログラマチックなインタフェースのいずれを介するものであっても）が利用できるインタフェースは、先ほどの議論と同一の方法で特定される（すなわち、ベンダの標準的な文書中のインタフェースの記述への参照は許容可能である）。これらのインタフェース（ソフトウェア特権メカニズムと共に）は、管理者向けガイド（公的に利用可能な文書の一形態）で議論される。

特権を持つコード及び特権を持つコードによって利用されるリソースは、通常は信頼されない利用者にも可視のコンテナ（例えば、ファイル）中に保持される。記述には、これらのコンテナの特定が含まれなくてはならず、また管理者向けガイドにはこれらのコンテナの推奨される保護が含まれなくてはならない（これは評価者によって検証されることになる）。例えば、カーネルイメージを含むファイル、デバイスドライバの実行可能形式、そして高信頼プロセスが、この記述に含まれることになる。

保護メカニズム記述

特権の使用に加えて、製品にはその他の保護メカニズムが採用されているかもしれない。例としてはデータ実行防止（DEP）、ジェイル、FLASK、アドレス空間配置のランダム化、そしてカナリアなどのスタック保護メカニズムが挙げられる。そのようなメカニズムが製品に使われている場合、記述にはそれらが製品でどのように実装されているか、どの程度

まで用いられているか、そして存在するかもしれないあらゆる制限（例えば、サードパーティのデバイスドライバには、製品の開発者によって書かれたコードとこの分野では同一の要件がなくてもよい、など）が、特定されるべきである。

初期化記述

製品が経験する起動または初期化プロセスは、文書化されなくてはならない（must）。この説明によって、特権アーキテクチャ記述において特定されたファイルや、ロードされたコードによって利用されるあらゆる構成ファイルを含め、システムのさまざまな部分のロード及び実行を参照する詳細なレベルで､発生する処理がカバーされる｡ここでの目的は、どのように製品がそのセキュアな状態へ到達するか、そしてどのように信頼されないエンティティと対話できるようになるか、という点を読者に理解してもらうことである。この記述によって、信頼されないエンティティが初期化プロセスへ悪影響を与える方法が存在するかどうかを、評価者が判断するために十分な詳細情報が提供されることになる。

管理ガイダンス

アーキテクチャ設計によって提示されるシステムの特権メカニズムは、システム管理者によって操作可能なものであり、また場合によっては「使い方」レベルで理解されなくてはならないものである（must）。管理ガイダンスに含まれる情報の大部分はよく理解されているが、システムの特権メカニズム（アーキテクチャ設計に提示される）の側面が管理ガイダンスに提示されなくてはならず、またテストされなくてはならないということは指摘しておく価値がある。

OSPP 機能テスト理念のホワイトペーパー

機能テストは、OSPP 評価の核心的な領域である。その目標は、OSPP 中の SFR を強制する機能が ST 中に特定されるインタフェースを通して規定されたように実装されているという確信を、TOE の利用者に与えることである。これは、各 SFR に関連付けられた保証アクティビティ中で要求されるテスト、及び開発者によって提供されるインタフェース（TSFI）と関連付けられたテストの両方によって、達成される。インタフェースのリスト（公的に利用可能な文書に含まれている）は SFR に対応付けられ、また評価中に行われる保証アクティビティテストの取り組みを補完するために用いられる。テストアクティビティの結果として、すべての SFR（及び SFR から導出されるテストアサーション）がテストされ、またテストアサーションに対応するすべての TSFI が行使される。

機能テスト文書と分析の取り組みを構成するものは、テストカバレージ分析、評価の一部として提供される開発者のテスト証拠資料、そして開発者のテスト証拠資料の評価者による使用及び評価チームテストの立案である。このホワイトペーパーは、これらのアクティビティの一般的なアプローチとともに、開発者及び評価者の両者からのテストに関連した文書の内容に関する要件を概説するものである。

テストの取り組みに全体として何が必要かを効率的に議論するため、開発者のテスト証拠資料及び開発者のテストカバレジアサーションが最初に議論される。続いて評価者のテストカバレージ分析の議論を行う。これには開発者によって作成されたテスト証拠資料（加えて、セキュリティ機能記述、特権アーキテクチャ記述など、開発者によって提供される文書）の利用が含まれる。評価チームのテストへの取り組みの議論（チームのテスト計画に期待される内容及び詳細さの程度、テスト実行への評価チームの参加の見込み、及びテストの結果を含む）についても、概説する。

開発者のテスト証拠資料

モダンなオペレーティングシステムにおいては、機能テストの実行に開発者の多大な労力が費やされる。評価アクティビティ中のテストの取り組みの目標は、開発者のテストツール、アーティファクトなどを用いて、評価者の側の完璧さを犠牲にすることなく TOE テストの実行にかかる時間を短縮することである。この目的を達成するため、開発者によって提供された証拠資料は、SFR 保証アクティビティ中に概説されたすべてのテストが対処されていること、そしてテスト対象となるすべてのインタフェースが、そのインタフェースと対応付けられる SFR の実装における役割に関して行使されていることを、評価者に納得させることができるべきである（should）。

SFR へ具体的に対処するテストケースをベンダが開発する必要はないということは、重要なのでここで指摘しておきたい。模範的には、開発者が開発したテストスイートをすべて（以下に概説する対応付け情報と共に）提供し、評価者はこの情報を用いて、この文書で後に記述されるテストカバレージ分析を行う。もちろん、そのようなテストスイートを開発者が開発することは排除されているわけではないが、要求されてはいない。

開発者によって提供されるテスト証拠資料には、以下のものが含まれる。

- ST 中に特定されるすべての TSFI について、該当する開発者のテストケースの対応付け。
- SFR 保証アクティビティと関連付けられるすべてのテストについて、該当する開発者

のテストケース。ここで、SFR 保証アクティビティテストはインタフェースベースであるよりもシナリオベースである場合が多く、したがって必要とされる機能の一部を複数の既存の開発者テストケースが担当しているかもしれない、ということは重要なので注意されたい。保証アクティビティテストに対処するテストケースを具体的に作り上げることは開発者にとって受容可能であるが、要求されてはいない。開発者は、保証アクティビティのテストケースに規定されるように例証されるべき機能をカバーする（既存の）テストのセットを対応付けるだけで十分なのである。

- 該当するテストケース。理想的な意味での開発者テストケースは、テスト概要、テスト構成、テスト指示、テスト工程、及びテスト結果から構成される。テスト概要には、テストの抽象的な記述と、その機能を行使するためにインタフェースが（一般的な意味で）使われる方法が含まれる。テスト構成には、テストの実行が成功するためにテストに先立って実現されなくてはならないあらゆるテストの設定が含まれる。テスト指示には、テストの実行に関連する情報が含まれる。自動化されたテストについては、これは「このテストを実行せよ」という指示と、出力に関する任意の情報から構成されることになる。手作業によるテストについては、テスト指示は通常、テスト工程と同一になる。テスト工程には、テストを行うためにたどるべき具体的な工程が含まれる。自動化されたテストについては、これはテストスクリプトの内容から構成される。これはコードであってもよいし、スクリプト化されたコマンドライン命令であっても、テストハーネス言語のプログラムなどであってもよい。手作業によるテストについては、これはテストを達成するためにテスト者が行わなくてはならない工程から構成される（例えば、コマンドラインのコマンドや、GUI ベースのインタフェース上でのラジオボタンやチェックボックスの設定やパラメタ入力に関する指示）。テスト結果は、テストの実行から期待される結果から構成される。これらの結果には、テストが TOE に与えた影響に加えて、この結果がどうチェックされるのかが含まれる。自動化されたテストについては、これはテスト工程自体に含まれており、利用者に見える結果は「テスト合格」だけであることが多い。その他の場合（手作業によるテストの場合のほとんど）は、テスト工程を実行しながら多少の確認が行われる。

  テストケースに関する以上の記述は、開発者から普通に得られるものを詳述したものである。開発者は上にリストしたすべての情報を含まないテストケースを持っているかもしれないし、また書き記された手続きではなく、開発者テスト要員の文書化されていない専門能力に依存しているかもしれない。開発者には、上記のセクションが明確に区分されたテストケースの提供や、何らかの基準への適合は要求されていない。評価者は開発者によって提供された情報を用いてカバレージ分析（事項で説明する）を行って、何らかの不足が特定されればそれに対処する。

- 使用されたテストツールの記述。この記述は、少なくともテストツールが TOE へ与える影響を評価者が判断できるものでなくてはならない（shall）。ツールの使い方の指示、ツールの構成などに関する追加的な情報は、テストツールの使用に関して開発者から提供されるサポートのレベルに依存して、要求されるかもしれない。

評価者のカバレージ分析

評価者は、利用できる情報に基づいてテストカバレージ分析を行う。これには、SFR 保証アクティビティテストと開発者テストケースへの対応付け、インタフェース仕様、開発者によって提供されたインタフェースと SFR との対応付け（これは提供される証拠資料の一部である）及びテストケースとの対応付け（上述）、セキュリティ機能仕様、特権アーキテ

クチャ記述、そして TSS に含まれる追加的情報が含まれる。全体としての目標は、評価者が、開発者と評価者のテストアクティビティを組み合わせることによって、すべてのインタフェースを行使してセキュリティ要件が SFR に実装されていることを示すことである。

テストカバレージ分析は、2 つの主要なアクティビティから構成される。SFR 保証アクティビティテストが行われていることの分析と、SFR 機能が行使される TSFI がテストされていることの分析である。これら 2 つのアクティビティは、以下で別個に取り扱う。

SFR 保証アクティビティテストのカバレージ分析

SFR 保証アクティビティのテストカバレージ分析を行うため、評価者は以下の手順を実施する。

1. 評価者は、すべての SFR 保証アクティビティテストが、開発者テスト証拠資料中の 1 個以上の開発者テストケースへ対応付けられていることを確証する。SFR 保証アクティビティテストは、評価者によって分析の際に用いられるべきテスト目的として役立つことに注意すべきである（should）（テスト目的は、上記の開発者テストケースの概要と同様のレベルの詳細さで、同一の目的に役立つ）。
2. 開発者のテストケースは保証アクティビティテストを部分的にしかカバーしていない場合が多いため、評価者はいくつかの開発者テストケースを見渡して、保証アクティビティテストによって規定されるアクティビティがカバーされていることを判断する必要がある。場合によっては、開発者テストケースに存在しないパラメタ設定が保証アクティビティテストには必要かもしれない。また別のケースでは、保証アクティビティにはフォーカスしている「シナリオ」の数が多く、開発者のテストケースでは保証アクティビティに要求されるエンドツーエンドの方式でテストされていないかもしれない。開発者によって提供されたテストケースが SFR 保証アクティビティテストのすべての側面に対処していないと評価者が判断した場合、取るべきアクションは少なくとも 2 とおりある。ひとつは、開発者が自分たちのテストスイートに、必要とされる適切なテストを追加することである。もう一方は、その不足を補うチームテストを評価者が準備することである。チームテストケースには、開発者テストケースについてすでに記述した情報が含まれる。

このシナリオにおいて取り込まれる必要のある情報を、表のフォーマットで以下に示す。これは、必要とみなされる任意のチームテストケースの作成に追加されるものである。

SFR	保証アクティビティテスト	開発者テストケース	評価チームテストケース
SFR 本文	保証アクティビティの本文	このインタフェース／SFR をカバーする 1 つまたは複数の開発者テストケースへの参照	開発者テストケースが不十分と考えられる場合、評価チームテストケースへの参照、プラス開発者テストに何が不十分なのかを示す根拠

インタフェースベースのテストカバレージ分析

インタフェースベースのテストカバレージ分析を行う一般的なアプローチを、以下に概説する（評価者への情報の配付と評価者の時間の空きに応じて、これらのアクティビティを行う際に多少の時間的ずれがあるかもしれないということに注意されたい。しかしすべてのアクティビティは行われなくてはならず、また情報の効率的な利用を確実にするために

は順番もかなり重要である）。

1. 評価者は、開発者から提供された TSFI から SFR への追跡によって、すべての SFR 及びすべての TSFI が開発者のテスト証拠資料中に特定されており、また少なくとも 1 つのテストケースへ追跡できることが示されていることを確証する。SFR がテストケースへ追跡できない場合、評価者はこれがその特定の SFR について意味があることに合意すべきである（should）。この時点で評価者はテストケースを評価しておらず、単に後で必要とされる情報が利用できることを確認しているのみである。

2. SFR には複数の試験可能な側面が含まれていることが普通であり、このホワイトペーパーではこれを「テストアサーション」と呼んでいる。テストアサーションは、SFR の本文またはそのエレメントから直接取られた試験可能な個別の言明、TSS から直接取られた試験可能な言明、またはベンダの提供する文書及び SFR と関連するセキュリティ機能の記述の中に含まれる情報の結果として導出された試験可能な言明である。評価者は、（最初のステップでチェックされた）SFR から TSFI への追跡を、列挙された SFR（下記の表を参照）に関係するテストアサーションへ拡張する。TSFI が SFR へ対応付けられている場合、その TSFI はその SFR と関連付けられた 1 個以上のテストアサーションと対応付けられていなくてはならない（must）。

3. 次に評価者は、TSFI に対応付けられたテストアサーションのそれぞれについて、1 つ以上のテスト目的を独立して判定する。そのインタフェースについて何をテストする必要があるかについて「新鮮な見方」を提供するため、これを評価者が開発者テスト証拠資料を参照せずに行うことが重要である。評価者はインタフェース記述だけでなく、提供された TSS 及び操作ガイダンスも考慮する。以下は、テスト目的の判定に関するガイドラインである。

    a. 制約を課す SFR エレメントについては、（該当する条件が満たされた際に）その機能が成功できることを確証し、また任意の特定された制約が課されることを確証するテスト目的が存在すべきである（should）。

    b. 属性ベース（例えば特権）の制約については、最小セットの属性によって成功が許可される場合と、単一の属性が欠けたのみで失敗に終わる場合とが、テスト目的によって対処されるべきである（should）。

    c. 複数の SFR 関連オブジェクトを操作できる TSFI については、すべてのオブジェクトがテスト目的によって対処されるべきである（should）。

    d. セキュリティ属性を設定できる能力を持つ TSFI（一般的には管理 TSFI）については、設定することによって（例えば）単に GUI の値が変化したことでなく意図した結果が実際に得られることが、テスト目的によって要求されるべきである（should）。

    テスト目的は、詳細さのレベルにおいて開発者テスト概要と同等であるべきである（should）。テスト工程のレベルまで詳細であるべきではないが、2 人の異なるテストコーダーへ提供された場合に、実質的に同一の機能をテストできるようなテストケースがコーディングされるほど詳細でなくてはならない（must）。

4. 次に評価者は、TSFI から開発者テストケースへの対応付けを用いて、各 TSFI について該当するテストケースを特定する。それぞれのインタフェースについて、評価者は開発者によって行われたテスト（開発者テスト概要の記載による）を、評価者によっ

て開発されたテスト目的と比較する。評価者の裁量により、開発者テスト工程それ自体を調査して、テストの範囲に関する情報をさらに得ることもできる。インタフェースの主要なセキュリティ機能がテストされることを確認する以外にも、評価者は開発者側のテストの「深さ」が適切であることをチェックして確証する。これには、そのテストケースに用いられたものだけでなく、任意の入力に対してその特定のインタフェースが望ましい機能を果たすことを評価者が納得できる程度に、そのインタフェースを行使することが必要となる。例えば、あるインタフェースによってセキュリティ属性が設定できる場合、テストには 2 つ以上の妥当な値と、少なくとも 1 つの不当な値が含まれているべきである（should）。開発者のテストの取り組みが不足していると評価者がみなした場合には、取るべきアクションは少なくとも 2 とおりある。ひとつは、開発者が自分たちのテストスイートに、必要とされる適切なテストを追加することである。もう一方は、その不足を補うチームテストを評価者が準備することである。チームテストには、開発者テストケースについてすでに記述した情報が含まれる。

モダンなオペレーティングシステムに存在するインタフェースの複雑さのため、すべてのインタフェースのすべてのパラメタのすべての値を完全にテストすることは不可能である。評価者はカバレージ分析中に特定されたすべてのテスト（すなわち、すべての開発者テストプラス任意のチームテスト）を実行し、すべての TSFI を行使しなくてはならない一方で、インタフェースが取り得る値に関しては、完全ではないテストを行うことが多少は許容される。「テストの深さ : 要件及び文書」（下記）の項では、この問題について、及び評価者のアクティビティと文書化に関する要件について、さらに詳細な議論を行う。

このシナリオにおいて取り込まれる必要のある情報を、表のフォーマットで以下に示す。これは、必要とみなされる任意のチームテストケースの作成に追加されるものである。

SFR	テストアサーション	TSFI	テスト目的	開発者テストケース	評価者テストケース
SFR 本文	SFR に関連する具体的なテスト可能なアサーション（例えば、SFR 本文または TSS からの）	テストアサーションのテストに用いられる TSFI	評価者によって作成された、特定されたインタフェースを介して SFR をテストする目的	このインタフェース／SFR をカバーする開発者テストケースへの参照	開発者テストケースが不十分と考えられる場合、評価チームテストケースへの参照、プラス開発者テストに何が不十分なのかを示す根拠

評価者によるテストへの取り組み

上に概略を示したテストカバレージ分析に加えて、評価者によるテストへの取り組みには、評価テスト計画の作成、場合によって評価チームテストケースの作成、テストの実行、そしてテスト結果の報告が含まれる。評価者によるテストへの取り組みの文書化のフォーマットは重要ではないが、参照を容易とするため以下の議論では評価者がテストへの取り組みを計画し、実行し、そしてその結果を文書化するために利用する文書の集合を「テストレポート」と呼ぶことにする。これは実際には、例えばテストカバレージ分析、テスト計画、テストケース、テスト結果レポートなど、さまざまな文書を含む可能性があるが、これらの文書が提示される方法は、必要とされる内容に影響すべきではない（should not）。テストレポートの各パートが、以下のセクションで議論される。

テスト計画には、評価者によって行われようとしているテストの設定及び実行に関するいくつかの種類の情報が含まれている。評価者にはテストカバレージ分析中に特定されたすべてのテストを実行することが期待されるため、テスト計画文書にはこれが実施される工程が、必要とされるシステム及び要員の面から、用いられる特別なテストアーティファクト／ツールの面から、そしてテストの順番の面から記述される。

テスト計画にはテストされるプラットフォームが特定され、またテスト計画には含まれていないが ST に含まれているプラットフォームについては、そのプラットフォームをテストしないことについての正当化がテスト計画に提供される。この正当化は、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、行われようとしているテストにその違いが影響しないという論拠が示されなくてはならない（must）。例えば、ハードウェア／ソフトウェア総体としてのインタフェース（プロセッサの命令体系、ネットワークインタフェース、バスアクセス可能なハードウェアの特性など）が 2 つのハードウェアコンポーネント（例えば、2 つのデスクトップシステム）で同一であれば、それらのプラットフォームは「同等」であると言って差し支えないであろう。しかし、単にその違いが影響しないと主張するだけでは十分ではない。根拠が提供されなくてはならない（must）。ST 中のすべてのプラットフォームがすべてのテストによってテストされる場合には、根拠は必要とされない。すべてのプラットフォームがテスト計画には含まれているが、各プラットフォームではテストのサブセットのみが実行されるという場合もあるかもしれない。この場合にも同様に、これが受容可能である理由をテスト計画の中で提供する必要がある。

テスト計画にはテストされるべきプラットフォームが完全に特定され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも特定されなくてはならない。テストの一部として、または標準的なテスト前の条件として、各プラットフォームの設置及び設定については評価者が AGD 文書にしたがうことが期待されていることには注意すべきである（should）。これには、特別なテストドライバまたはツールも含まれるかもしれない。

評価者は、テストカバレージ分析で特定されたすべてのテストケースを実施しなくてはならない（shall）。前述したように、これはすべての TSFI がすべての取り得る値についてテストされなくてはならないという意味ではない。しかし、選択されたテストについては正当化の提供が必要とされる。これについては、下記「テストの深さ：要件及び文書」の項でさらに議論されている。

テストケースには、実行されるテストの手順（自動化されたものと手作業によるものの両方について）が含まれる。評価チームの立会いの下で開発者がテストの一部を実行することは許容されるが、どのテストが評価チームの「立会い」の下で行われ、どのテストが評価チームによって実行されたのかは、テストレポート中に明確にされなくてはならないことには注意べきである（should）。手作業によるテストの立会いにおいては、評価者は手順ごとのチェックリストを作成し、開発者がテストケース中の手順にしたがっていることを確実にしなくてはならない（shall）。テストが実行されたことの「証明」として、テスト結果を評価チームへ開発者が単に送付することは、一般的には認められない。

テストへの取り組みの結果として、評価者はテストの実際の結果を文書化する。これには、スクリーンショット、ログ、そしてチェックリストなどが含まれるかもしれない。この情報は、テストレポート中に含まれる。実際のテスト結果が期待される結果と非自明な理由で（例えば、インタフェースが考えられていたものと異なる動作をする（非自明）、コマンドの打ち間違いまたはテスト設定の一部を忘れたこと（自明））異なっている場合、これは

テストレポート中に文書化され、さらにテストの再実行が成功したことを示す再テスト（あるいは、テストの再作成や削除が必要な場合には、適切な記述とテストカバレージ分析中の影響を受けるインタフェース／SFR の再分析）が記述される。

テストの深さ：要件及び文書

実際のテストのカバレージに関して、さらに詳細な議論に値する 2 つの側面が存在する。ひとつは複数の異なる TSFI を有するセキュリティメカニズムのテストであり、もうひとつは個別の TSFI に関して行われる必要のあるテストの量（これは、第 1 の側面のより一般的な場合である）。

モダンなオペレーティングシステムには、さまざまな方法でアクセスされる集中型のメカニズムがいくつか含まれている。監査、アクセス制御、そして識別と認証メカニズムは、その例である。開発者によって配付される文書には、いわゆる「グレイボックス」テスト手法をサポートする「伝統的」な TSF 内部文書はもはや存在しない。ブラックボックス手法は評価にコストの問題を引き起こす可能性があるが、これによって高い客観性と再現性が得られ、また通知されたインタフェースが規定されたように動作すると「評価された」ことが、より説得力を持って例証される。したがって、同一の基盤メカニズムへのさまざまな TSFI がテストされる度合いには、違いがあるべきではない（should not）。

第 2 の側面は、個別の TSFI のテストに関するものである。TSFI はいくつかのパラメタを取るのが普通であり、またこれらのパラメタはいくつかの値を取り得る。いくつかの異なる値の組み合わせを用いてテストアサーションが成り立つことを例証することができ、また他のいくつかの値の組み合わせを用いて境界ケースやパラメタ制約のふるまいを例証することができる。しかし、この値のセットを累積しても、そのインタフェースのテストパラメタとして提供可能な値の取り得る範囲や値の組み合わせに比べればごく一部に過ぎないのが普通である。ここで、ある特定の TSFI が「十分にテストされた」と評価者がみなせるのはどういう場合か、という疑問が生じる。

これが、すべての状況ですべての TSFI について成り立つことを可能とするような、客観的な基準は存在しない。さらに内部文書の不足は、例えばコードパスカバレージなどの定量的手段や、実装に関わる問題などに影響する。したがって最も重要な基準となるのは、1) 各テストアサーションのすべての側面がテストされること、 2) 複数（2 個以上）の値（該当する場合）がテストアサーションの証明に用いられること、 3) 境界条件がテストされること、そして 4) テスト実施の際に用いられる値は文書化され、テストへの取り組みの実際の範囲が読者にとって明確とならなくてはならないことである。

OSPP 脆弱性分析ホワイトペーパー

概論

このホワイトペーパーでは、OSPP 中に定義される保証アクティビティの一部としての、脆弱性分析に関するアプローチについての提言を行う。このアプローチの目的は、不可欠かつ設計に関係した脆弱性を効率的な方法で評価者が検出できるような方法論を定義することである。

提示するアプローチは、バッファオーバフロー、パラメタ検証の非自明な欠陥、あるいは非自明な競合条件などの実装に関連した脆弱性を系統的に特定するようには設計されていない。この種の脆弱性の系統的な特定に関連したアプローチは、OSPP 適合オペレーティングシステムの保証アクティビティの範囲外である。評価アクティビティが行われている最中、評価者がそのような脆弱性の実例を検出することもあるだろう（この場合には、もちろん開発者による対処が必要とされる）が、このような発見は系統的な分析によってではなく、偶然になされる場合が多い。

客観性と再現性を達成するためには、評価者が一連の明確に定義されたアクティビティにしたがい、そして他者が評価者の論述をたどって評価者のレポートと同一の結論に達することができるような形で結果を文書化することが重要である。これは、異なる評価機関が全く同一の種類の脆弱性を特定したり、全く同一の結論に達したりすることを保証するものではないが、このアプローチによって可能な限り客観的かつ再現可能な結果が確実に得られる。

脆弱性分析／テストの一部として行われる詳細なアクティビティが、初期の OS 評価の途上で十分に開発されることが期待される。また、OS 評価を継続するにつれて、さらなる詳細化が継続することも期待される。これらの詳細なアクティビティが OS 技術委員会によって合意されることは、重要なので注意されたい。

脆弱性分析の概要

ここで提示する一般的な欠陥仮説を確立するためのアプローチは、3 つの方法を視野に入れている。

- 共通脆弱性一覧（CVE）から導出された、OSPP 中の欠陥仮説のリスト、
- その技術に特有の教訓から導出された OSPP 中の欠陥仮説のリスト、またやはり共通脆弱性一覧（CWE）／共通攻撃パターン一覧及び類別（CAPEC）項目から導出されたその他の技術コミュニティからのインプット、ならびに
- 参照された公的リソースをも含め、この保証ホワイトペーパーで前述したベンダから提供された証拠資料及び SFR に基づいて評価者に利用可能な情報から導出された欠陥仮説のリスト。

最初の項目は、この文書に記述された手順にしたがって評価の途上で作成される必要がある。これは、公に知られた脆弱性を持つ製品を認証してしまうことを避けるため、評価テクニカルレポートの作成時において最新のものである必要がある。

2 番目の項目は、公的な情報源に含まれる情報に関連した問題があるものの、この仮説のリストは評価チームが確認する具体的な項目へ詳細化が可能であり、また OSPP に含める

ことができる（ST 作成時に作成されるのではなく）と我々は確信している。

しかし、上記の 3 番目の種類には問題がある。これらの仮説は評価されようとしている特定の製品に依存している（そして我々のホワイトペーペーで概説されているように証拠資料が提供されようとしている）ため、これらの仮説を事前にリスト化することは不可能である。もしそれができたとしても、仮説はあまりに一般的であり、アクティビティの範囲を特定するための実用性は限定される。

これらの種類の仮説の脆弱性分析／仮説生成アクティビティについて、我々が適当と考える範囲と高レベル手続きに関して合意を形成するため、この領域での受容可能な原則と我々が考えるものに関して以下の提言を行う。この領域の重要な側面は、評価者がスキームからの同意を必要とする場合、及び評価者がスキームへ通知する必要なく開発者と直接対話できる場合である。

評価者に利用可能な情報

評価者は当然、開発者によって提供される情報へアクセスできる。これは我々の文書化ホワイトペーパー中の概要によるものと、ST 中に記される保証アクティビティに必要とされる情報との両方である。これは、開発者が提供しなくてはならない最小セットを定義する。ホワイトペーパー／保証アクティビティに規定される要件を満たすために必要な文書の提供を開発者に要請すること（スキームへの通知なしに）は、そのような文書が提供されていないと評価者が感じるのであれば、評価者の自由である。より情報が必要だということにベンダが賛成しない場合、評価者とベンダは自分たちの見解を文書化し、その後の進め方についてスキームから指導を受けることになる。

欠陥生成及びテスト

評価者は、ホワイトペーパー及び保証アクティビティに概説されているように、自分たちに提供されている情報に基づいて欠陥仮説を定式化する。仮説は評価中に策定され（評価に先立ってではなく）、システムのセキュリティ機能が（ST 中の SFR によって記述されているように）危殆化可能であることを例証しなくてはならない（must）。

このガイドにしたがった開発者から提供される必要のない材料（例えば、インターネットのメーリングリストから収集した情報、あるいは開発者によって提供されたセットに含まれないインタフェースに関するインタフェース文書を読むことによって得られた情報）に基づいて評価者が欠陥を定式化する場合、そのような欠陥仮説は、これらの仮説に関して開発者のインプットを求める前にスキームによって検討され、承認後に文書化されることになる（欠陥のソース、悪用シナリオなど）。これは、スキームへリストを提出して承認を求めることによって､あるいは CB と ITSEF との間で､理想的には開発者も参加した上で、あり得る脆弱性に関して話し合い、スキームの承認を得るためのミーティングを行うことによって実現される。このようにして、開発者もまた仮説への対抗手段についてアイディアを提出することができる。

上記のいずれの場合であっても（後者の場合にはスキームが欠陥のさらなる調査を承認したと仮定して）、評価者は各欠陥仮説を TOE について詳細化し、開発者によって提供された情報を用いてそれに反証を試みることになる。このプロセス中、開発者へ追加的な証拠資料（例えば、ソースコード、詳細設計、技術スタッフとの協議など）の明示的な要請を行わない限り、評価者はスキームに相談することなく自由に開発者と対話して欠陥が存在

するどうか判定して構わない。この手順の結果は、反証された欠陥仮説のセットと、反証されていないと評価者が感じている欠陥仮説のセットとなる。

反証されなかった欠陥仮説のそれぞれについて、評価者は（場合によっては再度）上記の手続きにしたがって、以下の適切なセットを提供することによって欠陥記述を最終的に詳細化する：その仮説の策定に用いられたソース文書、及びそれが特定の TOE 機能に対して危殆化を引き起こすおそれのある理由、その欠陥仮説がそれまでに提供された証拠資料によって証明も反証もできなかった論拠の提供、そしてさらに欠陥仮説を調査するために必要な情報の種類の定義である。この情報は、次にスキームへ渡されて、追加的情報の要請が承認される。承認された場合、開発者は要請された証拠資料を提供して欠陥仮説を反証する（または、当然のことだが欠陥を認める）。評価者は次に、欠陥仮説の反証が成功したか、証明に成功して欠陥が特定されたか、あるいはペネトレーションテストの取り組みの一部としてさらなる調査が必要とされるかという自分の判断を交えて証拠資料を要約することになる。これもまた、ミーティングまたは図表の作成によって対処が可能である。重要なのは、結果が文書化されることである。

報告

このセクションは現在のところ、明確に OSPP のパイロットフェーズを意図したものであり、後に変更されるべきものである。

開発者は、厳密に要求されるものよりも多くの情報を提供できるのであるから、どの証拠資料が用いられ、どの欠陥が調査されたのかを正確に判定する何らかの方法があるはずであると、我々は感じている。同様に、評価機関が制約されない環境下で行える分析量はスキームと期間によって異なるかもしれないということを我々は理解している一方で、我々は OSPP の脆弱性分析アクティビティのベースラインクレジットを確立し、その最低ラインを満たす（超える、ではなく）ものに信認を与えたいだけなのである。この目標の達成を助けるために、我々は生成されたすべての欠陥仮説、欠陥仮説の生成に用いられたすべての文書、そして欠陥仮説のそれぞれがどのように解決されたのかを、評価チームが報告しなくてはならないと感じている。欠陥仮説を考え出すために用いられた文書を特定するにあたって、それがホワイトペーパー／保証アクティビティによって正確に要求されたものであるかどうか、及びその文書の性質（ソースコード、低レベル設計、開発者の技術ノードなど）を読者が判断できるように、評価チームは文書を特徴づけなくてはならない（must）。この評価の結論においては、すべての「関与したスキーム」（OSPP 開発プロジェクトに関して）がこの情報をレビューし、将来の OSPP 評価をサポートする文書への影響を判断する（例えば、特定の種類の文書に基づいて多数の欠陥仮説が生成された場合には、この領域の追加的な文書が将来の評価には必要とされるかもしれない）。したがって参加するパイロット開発者は、この情報の共有に関してスキームと明示的に合意しなくてはならない。公的に文書化された脆弱性（上記リストの最初の 2 つの項目）に関する合意された情報のみがスキーム外部へ公表され、評価の脆弱性分析の部分に関する報告が求められることになる。

これを行うひとつの理由は、TC における今後の進展である。

SFR 関連保証アクティビティ

概論

このセクションでは、SFR 関連の保証アクティビティを定義し、SFR 中になされた主張がどのように開発者文書（TSS、場合によっては追加的な設計情報、インタフェース仕様、ガイダンス、及びテスト）によってサポートされる必要があるかについて、またなされた主張に TOE が適合していることを確認するために評価者が何をする必要があるのかについて、詳細に規定する。

セキュリティ監査に関する保証アクティビティ

FAU_GEN.1：監査データ生成に関する保証アクティビティ

背景

オペレーティングシステムが大規模な監査機能を持っていて、記録される事象がすべてセキュリティ関連というわけではない場合も多い。したがって、プロテクションプロファイル中の FAU_GEN.1 に定義される一般的な事象種別にマップされる、オペレーティングシステムが記録できる事象の種類及び関連する監査記録を特定することが必要である。これは通常、オペレーティングシステムによって維持管理されている監査証跡中の 1 つ以上の記録種別である。オペレーティングシステムが正しく監査記録を生成でき、また監査記録には FAU_GEN.1 によって要求される情報が含まれていることを確認するのは、評価者のタスクである。

TOE 要約仕様（TSS）

期待

TOE 要約仕様はオペレーティングシステムが監査記録を生成する原理を簡潔に記述し、また FAU_GEN.1 によって要求される監査記録の生成に用いられる監査メカニズムを明示しなくてはならない（shall）。これは単一のシステムコンポーネントである場合が多く、その場合にはそのコンポーネントの名前を挙げて、そのコンポーネントがどこへ監査記録を保存するか、どのように監査記録が保護されるかを定義することだけが要求される。TSS は、監査記録が保存される、または抽出可能な（TSF の特定の機能によってのみ抽出できる場合）監査記録フォーマットを定義する開発者文書への参照を示すべきである（should）。管理ユーザ（及び評価者）が、さらに加工と分析を行うために監査記録を抽出できる方法が記述されることは重要である。TSS 中の記述は、それが開発者文書への十分な参照を含んでおり、それによって監査証跡中の監査記録を分析するテストケースを評価者が生成できるならば、きわめて一般的であってもよい。

評価者のアクティビティ

評価者は TSS 及び TSS が参照する文書を分析し、この情報によって以下が可能であることを検証する。

1. FAU_GEN.1 によって定義される事象に関連した監査記録を含む監査証跡を特定すること
2. FAU_GEN.1 に定義される各事象の記録種別を特定すること

3. FAU_GEN.1 によって必要とされる情報を含む監査記録の記述を検証すること

4. 監査記録を抽出し分析するために用いられるインタフェースを特定すること

機能仕様

期待

監査記録は通常、オペレーティングシステムが実行中に発生する特定の事象に関連している。定義済みの事象の多くは利用者のアクションに関連しているが、このような場合には事象に関連する TSFI が特定される必要がある。このことは、評価者がこれらのインタフェースを用いて特定の事象を発生させ、その後生成が期待される監査記録が実際に監査証跡中に保存されていることを検証するために重要である。

したがって評価者は、TSFI を用いて FAU_GEN.1 に定義される事象を発生させるために十分な情報が得られることを確実にする必要がある。

FAU_GEN.1 に定義される監査対象事象の一部には、それを引き起こす TSFI が複数存在するかもしれない、ということは注意しておく価値がある。このような場合、これらすべてのインタフェースが関連する監査記録を実際に生成するということも、保証される必要がある。評価者は、開発者によって提供される設計情報を用いて、すべてのインタフェースをテストする必要はないという論拠を示してもよい。例えば TSF 内部の異なるインタフェースが共通の実行パスを利用していることと、監査記録の生成がこの共通実行パス内で行われることを設計情報が明確に示している場合、評価者はこれらのインタフェースの 1 つについてのみテストを行うことを正当化できる。

評価者のアクティビティ

評価者は、利用者のアクションへ直接結び付けられるすべての監査事象が、その事象が引き起こされる TSFI へ対応付けられることを確実にする必要がある。評価者はこれらのインタフェースを、そのインタフェースの仕様に関して明確な問題が特定できない程度にまで分析し、このインタフェースを使ってテストを行う方法の理解を確実にする。インタフェースを用いてテストが行われる際に、さらに詳細な分析が行われる。

このアクティビティの結果として評価者は、FAU_GEN.1 に定義される監査対象事象のすべてについて、その事象を引き起こすために使われるインタフェースへの対応付けを持たなくてはならない（shall）。そのようなインタフェースが存在しない事象については、評価者はそのようなインタフェースが期待できない（開発者によって提供される情報に基づいて）理由の正当化を提供しなくてはならず（shall）、またそれ以外の方法でこれらの事象を引き起こす方法に関して評価者の意見を示すことになる。これが、これらの事象に対する監査記録の生成をテストするテストケースの基礎となる。

アーキテクチャ設計

期待

TOE の設計には、監査記録生成機能の概要とともに、以下の潜在的な問題へ対処する「保証ケース」が提供される必要がある：監査機能をバイパスまたはかく乱することによって生成されるべき際に監査記録が生成されない問題、監査記録に含まれるべき情報が監査記録生成機能によって収集される以前及びその際に改変される問題、そして発生しなかった事象の監査記録を生成してしまわないように監査記録生成機能を悪用から保護する問題。また、TOE 設計情報には FAU_GEN.1 によって要求される監査記録のフォーマット及び内

容が、FAU_GEN.1 によって要求される詳細情報を記録の内容に対応付ける形で記述される必要がある。この情報は、既存の開発者文書への参照によって提示されてもよい（また、そうすべきである（should））。

評価者のアクティビティ

開発者によって提供される TOE 設計情報は、FAU_GEN.1 の機能の分析における以下の問題に十分対応できるものである必要がある。

1. 評価者は、FAU_GEN.1 によって必要とされる監査対象事象へ対応付けられるすべての監査記録のフォーマット及び構造の記述を特定できる必要がある。開発者は、監査記録を TOE 内部の監査証跡に保存されるものとして記述してもよいし、あるいは TOE の一部として開発者によって提供されるツールを用いて TOE 内部の監査証跡から抽出される監査記録の内容及びフォーマットを記述してもよい。後者の場合には、FAU_GEN.1 によって要求されるすべての監査記録を十分に抽出し分析できるようなこのツールの使い方の記述を、開発者が行うことが必要とされる。
2. 評価者は、監査記録が TOE の一部によってではなく、TSF によって実際に生成されることを特定できる必要がある。開発者は、監査記録の生成が利用者によって影響されたり、あるいはバイパスされたりする可能性について十分な論拠を提示する必要がある。
3. 評価者は、TSF が監査記録に保存する情報を収集する場所を特定できる必要がある。開発者は、この情報が改変を受けないという十分な論拠を提示する必要がある。
4. 評価者は、TOE が監査記録の生成に用いる機能を信頼できない利用者が呼び出すことは不可能であり、FAU_GEN.1 に定義される事象について TSF が生成した監査記録と区別できない監査記録を作成する監査機能を利用して全く起こらなかった事象の監査記録を生成することはできない、と特定できる必要がある。

利用者ガイダンス

期待

FAU_GEN.1 に関連する利用者ガイダンスは、監査記録の抽出権限を持っている利用者がこれを行う方法を説明する必要がある。さらに、すべての期待される監査記録が生成されており、監査記録が期待される情報を含んでいることを検証するため、監査記録から個別の情報を提示または抽出する方法についても説明する必要がある。

評価者のアクティビティ

評価者は、生成可能な監査記録に関する情報、監査記録を抽出する方法、及び個別の監査記録中の FAU_GEN.1 に規定される情報を特定する方法が利用者ガイダンスに含まれていることを確証する必要がある。この情報は FAU_GEN.1 のテストができるために、また FAU_GEN.1 中の要件に対応付けられるさまざまな監査記録にすべての必要な情報が含まれていることを確実にするために必要とされる。

テスト

期待

開発者は、自分のテストスイートからテスト結果を提示して、以下を例証することができるべきである（should）。

1. 監査記録が生成されるべきときに生成されていること、及び
2. 監査記録に期待される情報が含まれ、また正しく事象を反映していること。

このために特に必要とされるテストはほとんどないのが普通である。監査記録の生成は、（基本 OSPP 中の FAU_GEN.1 に記述される事象の場合）TOE によって提供されるセキュリティ機能の呼び出しと関連しており、その具体的なセキュリティ機能はいずれにしろテストされる必要があるからである。監査記録の生成を検証するため、一般的には FAU_GEN.1 に規定されるすべての監査可能事象をオンにして TOE はテストされるべきである（should）。ストレステストの一環として行われるのでない限り、この大規模な監査の実行に関連したタイミングのオーバヘッドは無視できる。純粋な機能テストに追加して行われるストレステストまたはファズテストは、実際に監査される監査対象事象がない、またはごく少数となる構成で行われることになるだろう。

このテストは、セキュリティターゲット中の FAU_GEN.1 に定義されるすべての監査事象をカバーし、FAU_GEN.1.1 に定義される事象のそれぞれについて、監査記録が作成され、FAU_GEN.1.2 に定義される監査事象の情報が含まれていることを示さなくてはならない（shall）。

評価者のアクティビティ

評価者は、開発者によって提示されたテスト結果を、完全性及び正確性の点から分析する。開発者が大量のテスト結果を作成して膨大な数の監査記録が生成されている場合には、これらの結果をサンプリングする戦略について、開発者と評価者は共同して取り組むべきことに注意されたい。このサンプルには、FAU_GEN.1.1 に定義されるすべての事象について監査記録が正しく生成されていることを例証する事例が含まれるべきである（should）。

サンプル中にこれらの監査記録が見当たらない場合、これらの監査記録に関連した事象を引き起こすと期待され、したがってこれらの記録を作成すると期待される、自分自身のテストケースを評価者は定義する。評価者は、これらの監査記録が正しく生成されることを検証する。

テストが行われた後、監査記録はテスト結果の一部として抽出され、期待される監査事象及び監査記録の内容と比較される必要がある。評価者は、FAU_GEN.1 に定義される事象のそれぞれについて、期待される監査記録が生成され、監査記録が期待される内容を示すことを確証する必要がある。

FAU_GEN.2：利用者識別情報の関連付けに関する保証アクティビティ

背景

利用者の責任追跡性という対策方針を達成するため、監査記録に記録された事象が、その事象を引き起こした利用者にまで追跡できることが必要とされる（その事象が利用者のアクションに直接関係している場合）。この責任追跡性は、その利用者の代理として動作しているサブジェクトが、そのセキュリティ属性のひとつとして異なる利用者 ID を割り当てられた場合であっても、確実にする必要がある（has to）。多くのオペレーティングシステムでは、信頼されないプログラムを用いた利用者には許可されないであろうアクションを行うために、高信頼サブジェクトのセキュリティ属性である「利用者 ID」が、OS の制御下で変更されることを許可している。

FAU_GEN.2 は、たとえこのような場合であっても、事象を引き起こした利用者の識別情

報が利用者と関連付け可能であることを要求している。これは、事象を引き起こした利用者の ID が直接監査記録に書き込まれることを要求しているわけではない、という点に注意されたい。

別の監査記録が、この ID の変更を事象の監査記録へ容易かつ明確に結びつけることができるように監査しているならば、そのような監査対象事象とその事象を引き起こした利用者の識別情報とを関連付ける能力があることになる。

さらに、オペレーティングは利用者が何らかのプロセス間通信機能を用いて高信頼サブジェクトへサービスを要求することを許可してもよい。この場合にも、その要求の処理中に監査記録が生成される際、そのサービスを要求した利用者の識別情報を関連付けることができなくてはならない（must）。

TOE 要約仕様（TSS）

期待

TSS は、関連する事象を引き起こした利用者へ「束縛」されていない（監査記録の作成時点で）サブジェクトによって監査記録が作成されることがあり得る状況を、特定し記述しなくてはならない（shall）。

そのような場合にも TSS は、事象を引き起こした利用者の識別情報が事象の監査記録と関連付けられる方法を説明しなくてはならない（shall）。その利用者の識別情報が監査記録の一部ではない場合、TSS は監査記録を評価する者が監査記録と、その監査記録に記録された事象を引き起こした利用者との関連付けを容易かつ明確に確立する方法を記述しなくてはならない（shall）。

評価者のアクティビティ

評価者は、この情報によって監査記録とその事象を引き起こした利用者との明確な結び付きを確立できることを検証するため、TSS 及び TSS が参照する文書を分析する。

機能仕様

期待

監査記録の記述には、監査記録とその監査記録の作成に至った事象を引き起こした利用者との間の関連付けを確立するために必要であると記述された情報がすべて含まれていなくてはならない（shall）。

評価者のアクティビティ

評価者は、提供された情報によって監査記録に記録された事象を引き起こした利用者とその監査記録そのものとの間の明確な関連付けができることを検証する。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、事象を発生させた利用者と監査記録との間の関連付けが確立される方法を正しく記述していることを検証する。

利用者ガイダンス

期待

事象を発生させた利用者と監査記録との間の関連付けを確立するために特定の構成が必要とされる場合、この構成とこの構成に至るための手順がガイダンス中に正確かつ完全に記述されることが期待される。

評価者のアクティビティ

事象を発生させた利用者と監査記録との間の関連付けを確立するために特別な構成が必要とされる場合、評価者はこのガイダンスにしたがって、事象を発生させた利用者と監査記録との間の関連付けを確立できるように TOE を構成する。

テスト

期待

開発者は、事象を発生させた利用者と監査記録との間の関連付けが確立できることを自分のテストの中で例証することが期待される。テストは、関連する事象を引き起こした利用者へ「束縛」されていない（監査記録の作成時点で）サブジェクトによって監査記録が作成されるような、TSS 中に特定されるすべての場合をカバーしなくてはならない（shall）。テストケースは、その事象を引き起こした 1 人またはそれ以上の利用者を特定しなくてはならない（must）。

評価者のアクティビティ

評価者は、関連する事象を引き起こした利用者へ「束縛」されていない（監査記録の作成時点で）サブジェクトによって監査記録が作成されるような、TSS 中に特定されるすべての場合を提供されたテストケースがカバーしていることを検証する。評価者は、これらのテストケースによって生成された監査記録を抽出し、その監査記録を作成させることになった事象とその事象を引き起こした利用者との関連付けを確立できるかどうかを判定する。評価者は自分自身のテストケースを定義して実行し、生成された監査記録を収集して、その監査記録を作成させることになった事象とその事象を引き起こした利用者との関連付けを確立できるかどうかを判定する。

FAU_SAR.1：監査レビュー及び FAU_SAR.2：限定監査レビューに関する保証アクティビティ

背景

監査記録の読み取りは、その権限のある利用者のみに限定されなくてはならない。この権限は、役割または特権へ割り当てられるか、あるいは監査データの読み取りを支配するより複雑なルールが存在してもよい。監査記録の読み取りに用いられるインタフェース、及びそれらのインタフェースを用いて監査記録を読み取る際の監査記録のフォーマットを記述した文書が、提供される必要がある。

TOE 要約仕様（TSS）

期待

TSS には、利用者に監査データの読み取りが許可される場合が記述されなくてはならない（shall）。TSS または TSS が参照する文書には、監査記録の読み取りに用いられるインタフェースと、それらのインタフェースを用いて監査記録を読み取る際の監査記録のフォーマットが記述される必要がある。

監査データの読み取りに通常のファイルインタフェースが用いられ、監査データを読み取ることのできる利用者の限定にファイルアクセス制御機能が用いられる場合には、ファイル中の監査データのフォーマットが、監査記録中の情報を正確に特定し解釈することができる程度に記述される必要がある。

評価者のアクティビティ

また評価者は、利用者に監査データの読み取りが許可されるために満たされる必要のある正確な条件をこの情報によって特定できるかどうかを検証するために、TSS 及び TSS が参照する文書を分析する。また評価者は、監査記録が提供される方法に関して提供される情報を分析し、FAU_GEN.2 によって要求されるすべての情報が提供され、その情報が意図した目的に適していることを確証する。

意図した目的は、直接監査データを読み取ること（このためにはデータが印刷可能な形式であることが要求される）であってもよいし、プログラムによる後処理に適したフォーマットであってもよい。いずれの場合にも、FAU_GEN.2 によって要求される情報は特定可能であることが必要であり、また正確に解釈できるように記述されている必要がある。

機能仕様

期待

機能仕様には、適切な権限のある利用者によって監査データを読み取るために使われるインタフェースが特定されなくてはならない（shall）。機能仕様またはガイダンス（あるいはその両方）には、これらのインタフェースを用いて監査データを読み取るために利用者が満たす必要のある条件が完全かつ正確に記述される必要がある。機能仕様には、監査記録から FAU_GEN.2 によって要求される情報を抽出できるような方法で監査データを提示する方法が記述される必要がある。

評価者のアクティビティ

評価者は、監査データのアクセスのために提供された情報が、監査データを読み取るために満たされなくてはならない条件を完全に記述しており、その記述がセキュリティターゲットの FAU_SAR.1.1 に提供された規定と一貫していることを検証する。検証者は、データが提供される方法の記述によって FAU_GEN.1 によって必要とされる情報を抽出できることを検証する。

注意：この要件は、必要とされる情報がガイダンス文書中に提供される場合にも満たされる。この場合、評価者はガイダンス文書を用いて下記のアクティビティを行う。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、監査データが読み取られる方法と監査データが提示されるフォーマットについて正しく記述していることを検証する。

利用者ガイダンス

期待

ガイダンス（または機能仕様）には、利用者に監査データの読み取りを許可するために満たされなくてはならない条件が説明されている必要がある。ガイダンスには、監査記録が提示されるフォーマットが説明されている必要がある。

評価者のアクティビティ

機能仕様に関する評価者のアクティビティを参照。

テスト

期待

開発者は、監査データの読み取り条件が強制されること、及び監査記録が読み取られる方法を、自分のテスト中で例証することが期待される。

評価者のアクティビティ

この SFR に関する評価者のアクティビティは、2 つの主要な側面から構成される。

1. 適切な権限のある利用者のみが監査データへアクセスできることの検証
2. 意図した処理に適した形式（直接読み取りまたは何らかのプログラムによる後処理）で必要とされる情報が監査データに含まれることの検証

最初の側面に関して、評価者は監査データの読み取りのために満たされなくてはならない条件をアクセス制御アルゴリズムとして取り扱い、FDP_ACF.1 中で任意アクセス制御に関するテストに概説されたものと同一の方法でテストが行われることを要求する。

2 番目の側面に関して、評価者は記述されたインタフェースを介して監査データを取得し、FAU_GEN.1 によって要求される情報が意図した処理に適した形式で抽出できることを検証する。このテストサンプルには、FAU_GEN.1 に定義されるすべての事象に対応する監査記録が含まれている必要がある。

FAU_SEL.1 : 選択的監査及び FMT_MTD.1(AE)TSF データの管理 : 監査事象に関する保証アクティビティ

背景

性能上の理由から、またディスクスペースを節約するため、設置においては FAU_GEN.1 に定義されるすべての事象について常に監査記録が生成されるわけではないのが普通である。したがって OSPP では、FAU_SEL.1 に定義される基準を用いて実際に監査される事

象を制約できることが要求される。SFR FMT_MTD.1(AE) には、FAU_GEN.1 に定義される監査対象事象の全体セットから実際に監査される事象のセットを選択するために利用者が満たさなければならない条件が定義される。

TOE 要約仕様（TSS）

期待

TSS には、FAU_SEL.1 に定義される基準に適合して実際に監査される事象のセットを制約する方法が説明される必要がある。また TSS にも、この監査対象事象のセットを管理する方法が、この管理に用いられるインタフェースを参照して記述される必要がある。

評価者のアクティビティ

評価者は、TSS 及び TSS が参照する文書中の説明が、FAU_SEL.1 に定義される要件と一貫していること（すなわち、FAI_SEL.1 に定義される基準にしたがって監査可能事象のセットを制約できること）、及び FMT_MTD.1(AE) に定義されるこの管理操作を行うために満たされなくてはならない条件と一貫していることを検証する。

機能仕様

期待

機能仕様には、適切な権限のある利用者によって監査されるべき事象のセットを管理するために使われるインタフェースが特定されなくてはならない（shall）。機能仕様またはガイダンス（あるいはその両方）には、これらのインタフェースを用いて監査される事象を管理するために利用者が満たす必要のある条件が完全かつ正確に記述される必要がある。

評価者のアクティビティ

評価者は、監査されるべき事象を管理するために提供されている情報に、監査される事象を管理するために満たされなくてはならない条件が完全に記述されていること、そしてこの記述がセキュリティターゲットの FAU_SEL.1 及び FMT_MTD.1(AE) 中に提供される仕様と一貫していることを検証する。

注意：この要件は、必要とされる情報がガイダンス文書中に提供される場合にも満たされる。この場合、評価者はガイダンス文書を用いて下記のアクティビティを行う。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、これらの SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、監査事象が管理される方法と監査されるべき事象の選択に関する可能性について、正しく記述していることを検証する。

利用者ガイダンス

期待

ガイダンス（または機能仕様）には、利用者に監査対象事象のセットの管理を許可するために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

機能仕様に関する評価者のアクティビティを参照。

テスト

期待

開発者は、監査対象事象のセットを管理するための条件が強制されていることと、FAU_SEL.1 に定義される基準にしたがって管理可能事象を制約できる方法を自分のテスト中で例証することが期待される。

評価者のアクティビティ

これらの SFR に関する評価者のアクティビティは、3 つの主要な側面から構成される。

1. 適切な権限のある利用者のみが監査対象事象のセットを管理できることの検証。
2. 監査対象事象のセットが、FAU_SEL.1 に定義される基準にしたがって制約できることの検証。
3. TOE が、定義された事象を正確に監査することの検証。

最初の側面に関して、評価者は監査対象事象のセットの管理のために満たされなくてはならない条件をアクセス制御アルゴリズムとして取り扱い、FDP_ACF.1 中で任意アクセス制御に関するテストに概説されたものと同一の方法でテストが行われることを要求する。

2 番目及び 3 番目の側面に関して、評価者は FAU_SEL.1 に言及される基準のそれぞれについてテストケースを特定し、これらの基準にしたがって監査対象事象のセットを設定し、適切な監査記録を生成するであろうテストプログラムを実行し、そして監査記録を生成する条件が定義された際には監査記録が生成され、監査記録を生成しない条件が定義された場合には作成されないことを検証する。

FAU_STG.1：保護された監査証跡ストレージに関する保証アクティビティ

背景

不正な監査記録の削除から監査証跡を保護することは、OS によって提供されるファイル保護メカニズムを、この保護メカニズムの使用方法に関する具体的なガイダンスと共に用いて行われる場合が多い。これが当てはまり、監査証跡に特有の保護メカニズムが実装されていない場合には、この SFR の評定はファイル保護メカニズムの評定及び監査証跡に特有のガイダンスの評定によってカバーされる。TOE に監査記録を不正な削除から保護する監査証跡に特有の機能が実装されている場合にのみ、機能仕様、アーキテクチャ設計、及びテストに関する保証アクティビティが行われる必要がある。

TOE 要約仕様（TSS）

期待

TSS には、監査記録が不正な削除から保護される方法を記述されなくてはならない（shall）。

評価者のアクティビティ

評価者は TSS 及び TSS が参照する文書を分析し、TOE が監査証跡に特有の保護メカニズムを利用しているかどうかを特定する。これが事実であった場合、評価者は FAU_STG.1 に関して定義される保証アクティビティの完全なセットを行う必要がある。そうでない場合には、評価者は利用される一般的な保護メカニズムが他の SFR（通常はストレージオブジェクトへのアクセス制御に関するもの）によってカバーされていることを検証し、そこに定義される保証アクティビティを参照する。この場合評価者は、監査証跡の保護のために提供されているガイダンスによって、保護メカニズムが正しく利用されることが確実になっていることを検証するだけでよい。

機能仕様

期待

機能仕様には、そのような（例えば保護の管理の側面への）インタフェースが存在する場合、監査証跡の保護に用いられる監査証跡に特有のインタフェースを特定しなくてはならない（shall）。

機能仕様には、監査証跡から監査記録を削除する、または監査証跡からすべての記録を削除する、監査証跡に特有のインタフェースが存在するかどうかが特定される必要がある。これらが存在する場合、機能仕様にはその使い方とこれらのインタフェースの利用者の権限が検証される方法が記述される必要がある。

評価者のアクティビティ

評価者は、監査証跡から記録を削除する、または監査証跡からすべての記録を削除するために提供されている情報が、監査証跡から記録を削除するために満たさなくてはならない条件を完全に記述していることを検証する。

注意：この要件は、必要とされる情報がガイダンス文書中に提供される場合にも満たされる。この場合、評価者はガイダンス文書を用いて下記のアクティビティを行う。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、監査データが読み取られる方法と監査データが提示されるフォーマットについて正しく記述していることを検証する。

利用者ガイダンス

期待

ガイダンス（または機能仕様）には、利用者に監査記録の削除を許可するために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

機能仕様に関する評価者のアクティビティを参照。

テスト

期待

開発者は、監査証跡から記録を削除するための条件が強制され、選択された監査記録のみが削除されることを自分のテスト中で例証することが期待される。

評価者のアクティビティ

この SFR に関する評価者のアクティビティは、2 つの主要な側面から構成される。

1. 適切な権限のある利用者のみが監査証跡から記録を削除できることの検証。

2. 削除を意図した記録のみが実際に削除されることの検証。

最初の側面に関して、評価者は監査記録の削除のために満たされなくてはならない条件をアクセス制御アルゴリズムとして取り扱い、FDP_ACF.1 中で任意アクセス制御に関するテストに概説されたものと同一の方法でテストが行われることを要求する。

2 番目の側面に関して、評価者は選択された監査記録の削除または監査証跡の完全な削除を行い、その後削除のために選択した監査記録のみが削除されていることを検証する。

FAU_STG.3：監査データの損失が生じたおそれのある場合のアクション、FAU_STG.4：監査データの損失の防止、及び FMT_MTD.1(AF) ：TSF データの管理に関する保証アクティビティ

背景

監査データの損失をもたらすおそれのある条件は多数存在する可能性があり、定義済みの閾値に達することはその中のひとつにすぎない。もうひとつの問題は、TSF が TOE をシャットダウンすることになる危機的な状況が TSF によって検出されることである。監査データが自動的に別の高信頼 IT システムへ転送される場合、このシステムの通信リンクのいかなる問題も監査データの損失をもたらすおそれがある。

TOE 要約仕様（TSS）

期待

FAU_STG.3.1 は、TSF が検出可能な監査データの損失のおそれのある条件を TSS にリストし、そのような条件が検出された際の TSF の対応を記述することを ST 作成者に要求している。この対応には、何らかの通知が含まれてもよい。

FAU_STG.4.1 は、監査証跡がそのストレージ制限に達した際の条件に特有のものである。TSS には、監査証跡に空きがなくなった際に TSF が取るアクションを規定し、どの監査記録が損失する可能性があるのか、及び監査証跡に空きがなくなった際に TSF が取るアクションを構成するために正当な管理者がどんな選択肢を取れるのかが説明される必要がある。

FMT_MTD.1(AF) には、監査ストレージが故障した際に取られるアクションの管理が定義される。

評価者のアクティビティ

評価者は、TSS 及び TSS の参照する文書中の説明が、記述された状況への TOE の対応を記述していることと、これが FAU_STG.3 中の規定と一貫していることを検証する。

また評価者は､監査証跡に空きがなくなった際に取られるアクションの記述が FAU_STG.4 中の仕様と一貫していることも検証する。

評価者は、監査証跡の故障の際に TOE によって取られる可能性のあるアクションと、それらのうち管理可能なものが TSS（及び TSS の参照する文書）に定義されていることを確認する。

機能仕様

期待

機能仕様には、適切な権限のある利用者が FAU_STG.3 及び FAU_STG.4 に関連する管理アクティビティを行うために利用できるインタフェースが特定されなくてはならない（shall）。プロテクションプロファイルではそのような管理機能の存在を要求していはいないが、FAU_STG.4 中のオプションとして、監査証跡に空きがなくなった際に取られるアクションのデフォルト値を上書きする機能の規定を許可していることに注意されたい。

機能仕様には、監査ストレージの故障の際に取られるアクションの管理を可能とするインタフェース（これには、例えば別の監査ストレージへの自動的なスイッチなどを可能とする構成インタフェースも含まれる）が特定されなくてはならない（shall）。

評価者のアクティビティ

評価者は、FAU_STG.4 について行うことのできる管理アクションを、提供された記述から特定する。これらは、そのような管理アクティビティに関して特定されたインタフェースと対応付けられ、ST 中の仕様との一貫性が分析される。

評価者は、監査ストレージの故障の際に取られるアクションを管理するための管理インタフェースを特定し、これらによって FMT_MTD.1(AF) に定義される種類の管理が TSS に言及される詳細と共に可能であることを検証する。

アーキテクチャ設計

期待

アーキテクチャ設計には、監査ストレージが事前に定義された制限を越えたことまたは FAU_STG.3 に規定されるその他の任意の条件を TSF が検出する方法と、この場合に取られるアクションが TSF によって開始される方法が説明される必要がある。アーキテクチャ設計には、TSF が監査ストレージの故障を検出する方法と、そのような故障に対応する方法が説明される必要がある。

評価者のアクティビティ

評価者は、これらの記述が ST 中の仕様と一貫していることをチェックする。

利用者ガイダンス

期待

FAU_STG.4 に関する管理アクティビティが存在する場合、ガイダンスにはこれらのアクティビティと、これらのアクティビティを行うために満たされる必要のある条件、そして

監査記録を生成する TOE の機能へこれらのアクティビティが与える影響が説明される必要がある。特に、特定の種類の監査記録が失わる場合や TOE が古い監査記録を上書きし始める場合は、そのことがガイダンス中に説明されなくてはならない。またガイダンスには、監査記録が失われる状況に陥らないためのアドバイスも提供される必要がある（例えば、監査証跡のバックアップ手順を自動的に開始することによって）。ガイダンスには、監査格納失敗の際に取られるアクションについて管理者が取れる選択肢と、これらの各選択肢の結果がどうなるのかが説明される必要がある。

評価者のアクティビティ

管理インタフェースの評定については、機能仕様についての評価者のアクティビティを参照されたい。また評価者は、監査記録の損失を防止するために与えられたガイダンスと監査格納失敗の際のアクションの管理を分析し、これをテストケースの開発に利用する。

テスト

期待

開発者は、FAU_STG.3.1 に定義される条件についてテストケースとテスト結果を提供し、これらの条件のそれぞれによって FAU_STG.3.1 に記述されたアクションを TSF が取ることになることを示すことが期待される。また開発者には、監査証跡に空きがなくなった際に取られるアクションを示すテストケースを提供することも期待される（通常の操作ではこの条件が達成できない場合を除く）。この場合、開発者はアーキテクチャ設計に基づく論拠を提供して、以下を例証する必要がある。

a. 監査証跡に空きがなくなる条件に達したことをテストすることが困難（TOE によって許可される監査証跡のサイズを最小に構成した際であっても）であること、

b. 監査証跡に空きがなくなった場合、TSF がこの場合について FAU_STG.4.1 に記述されたアクションを取ること。

それでも開発者は、FAU_STG.4.1 へのテストケースを開発するために必要と思われる労力の見積もりを提示する必要がある（has to）。開発者は、監査証跡に空きのない状態をシミュレート可能な特定の環境内（例えば、デバッガや仮想環境を用いて）で、監査証跡に空きのない状態に達した TOE の特定の機能が実行されるようなテストケースを提示することを選択してもよい。

監査記録がリモートシステムへ送られる場合、監査証跡に空きのない状況はリモートシステムがもはや監査記録を受け取ることができない状況と同等であることに注意されたい。この場合、監査証跡に「空きのない」状況は、リモートシステムへの接続を切断することによって容易にシミュレート可能である。

可能であれば、監査ストレージの故障をシミュレートするテストもすべきである（should）。例えば、監査ストレージがローカルのディスク上にあり、TOE がディスクを容易に取り外せる場合（例えば USB ディスクの場合）、開発者は監査ストレージをそのようなリムーバブルディスク上に置き、運用中にこのディスクを取り外すケースをテストすることが期待される。

評価者のアクティビティ

評価者は、FAU_STG.3.1 中に列挙されたすべての条件がテストケースによってカバーされていることを検証し、またそれぞれのテストケースで FAU_STG.3.1 に定義されたアクシ

ョンが取られていることをテスト結果が示していることを検証する。

開発者が FAU_STG.4.1 に関するテストを提供している場合、評価者はテスト結果を分析し、FAU_STG.4.1 に規定されるアクションが TOE によって取られていることをテスト結果が明確に示しているかどうか、及びその理由を判定する。

開発者が、FAU_STG.4.1 のテストケースを提供せず、過度の労力なしでは監査証跡に空きのない状況に至ることが不可能な理由の論拠を示している場合、評価者はその論拠への自分の判断を提供し（特定の環境中でこの状況がテストできない理由の論拠を含め）、その後開発者によって提示された論拠を分析して、監査証跡に空きのない場合に TOE が FAU_STG.4.1 に定義されたアクションを取ることを示す。評価者は、評価レポート中にこれらの論拠に関する自分の判断を提供する。開発者によって提示された論拠が受容可能かどうかの最終的な決定は、認証機関によって行われる。

FMT_MTD.1(AF) のテストにあたって、評価者は容易に取り外しできるデバイス上に監査ストレージを構成できるかどうか、あるいはリモートシステムへ送るように構成してこのシステムへのネットワーク接続が容易に切断できるかどうかをチェックする。これが可能である場合、TOE が運用中で監査記録を作成している最中にディスクの取り外しまたはネットワークの切断によって監査ストレージが故障した際の正しいアクションが取られるかどうかを、評価者はテストする。

FMT_MTD.1(AS)：TSF データの管理：監査ストレージに関する保証アクティビティ

背景

この機能は監査ストレージの管理に関係するものであり、監査ストレージの場所及びパラメタの選択及び構成が可能であること、そのようなストレージの作成及び削除、ならびに監査証跡全体のクリアが可能であることが含まれる。監査証跡全体のクリアはすべての監査記録の削除と同等であり、したがって監査ストレージ全体をクリアするための権限は、個別の監査記録を策よするために必要な権限よりも高くなくてはならないことに注意されたい。

注意 : TOE は監査サブシステム中に個別の監査記録の削除を許可する機能を実装してもよく、一方では監査ストレージ全体のクリアをファイルシステムによって実装し、構成によって監査証跡に割り当てられたファイルを削除する（ファイルシステム特有の）権限のみを要求してもよい。この場合、2 つのアクションに要求される権限は互いに独立しているのが通常であり、この場合にはガイダンス中にこれらの権限を調整する方法に関するアドバイスが与えられる必要がある。

TOE 要約仕様（TSS）

期待

TSS には、監査証跡が含まれることを意図したストレージを最初に設定し構成する方法が記述される必要があり、監査証跡ストレージオブジェクトに対して行える操作とこれらの操作を制御する方法が記述される必要がある。

評価者のアクティビティ

評価者は、監査証跡ストレージオブジェクトの作成から、監査証跡ストレージオブジェクトとしての割り当て及び最初の構成、（可能な場合には）監査証跡ストレージのクリア、再

割り当てなどの管理、そして（可能な場合には）監査証跡ストレージオブジェクトの削除に至るライフサイクルが監査証跡ストレージ管理でカバーされていることを検証する。これらすべてのアクションについて、そのアクションを行うために必要とされる権限が規定される必要がある。評価者は、この管理モデルが他の監査証跡機能の管理と一貫していることを検証する。

機能仕様

期待

機能仕様には、適切な権限のある利用者が FMT_MTD.1(AS) に関連した管理アクティビティを行うために用いられるインタフェースが特定されなくてはならない（shall）。

評価者のアクティビティ

評価者は、提供された記述から、FMT_MTD.1(AS) に関して行うことのできる管理アクションを特定する。これらは、そのような管理アクティビティに関して特定されたインタフェースと対応付けられ、ST 中の仕様との一貫性が分析される。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、監査データストレージオブジェクトが管理される方法について正しく記述していることを検証する。

利用者ガイダンス

期待

ガイダンス（または機能仕様）には、利用者に監査証跡ストレージオブジェクトの管理を許可するために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

管理インタフェースの評定については、機能仕様についての評価者のアクティビティを参照されたい。

テスト

期待

開発者は、FMT_MTD.1(AS) に定義される個別の管理アクティビティに関してテストケースとテスト結果を提供し、利用者がそのアクティビティを行うために要求される権限を持っている際に、その管理アクティビティが行えることと、規定された影響があることを示すことが期待される。また開発者は、利用者が必要とされる権限を持っていない際には FMT_MTD.1(AS) に定義される管理アクティビティが行えないことを示すテストケースを提供することも期待される。

評価者のアクティビティ

評価者は、FMT_MTD.1(AS) に列挙されたすべての管理アクティビティがテストケースによってカバーされていることを検証し、またテストケースのそれぞれにおいてその管理アクティビティを行う利用者に十分な権限がある場合にその管理アクティビティに規定された影響があることをテスト結果が示していることを検証する。また評価者は、必要な権限なしに FMT_MTD.1(AS) に規定された管理操作を行おうとする試みが失敗するということがテストによって例証されることを検証する。

FMT_MTD.1(AT)：TSF データの管理：監査の閾値に関する評価アクティビティ

背景

この機能は、FAU_STG.3.1 に定義されるアクションを引き起こす閾値の設定に関するものである。

TOE 要約仕様（TSS）

期待

TSS には、FAU_STG.3.1 に定義されたアクションを引き起こす監査ストレージの閾値が管理される方法が記述される必要がある。

評価者のアクティビティ

評価者は、TSS 中に記述された機能に、監査証跡の閾値が管理される方法と、このアクションにどのインタフェースが利用できるかが規定されていることを検証する。

機能仕様

期待

機能仕様には、適切な権限のある利用者が FAU_STG.3.1 によって用いられる監査証跡の閾値を管理するために使われるインタフェースが特定されていなくてはならない（shall）。

評価者のアクティビティ

評価者は記述から、監査証跡の閾値が管理される方法を特定する。この記述には、この管理アクションを行うためにどの権限が必要とされるか、及びこの閾値の取り得る値の制限は何か、ということが規定されている必要がある。評価者は、閾値の取り得る値に意味があることを検証する（例えば、負の値や監査証跡の容量の 100%を超える値でないこと）。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、監査データストレージオブジェクトが管理される方法について

正しく記述していることを検証する。

利用者ガイダンス

期待

ガイダンス（または機能仕様）には、利用者に監査証跡ストレージの閾値の管理を許可するために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

管理インタフェースの評定については、機能仕様についての評価者のアクティビティを参照されたい。

テスト

期待

開発者は、監査証跡の閾値の設定に関するテストケースとテスト結果を提供することが期待される。開発者は、監査証跡の閾値として異なる値を用いて FAU_STG.3.1 のテストを実行し、定義された閾値を越えた際に FAU_STG.3.1 に定義されたアクションが正しく取られることを示すことが期待される。

評価者のアクティビティ

評価者は、その閾値の値が設定された方法とは独立して、閾値を越えた時に FAU_STG.3.1 に定義されたアクションが取られていることが、テスト結果によって示されていることを検証する。

利用者データ保護に関する保証アクティビティ

FDP_ACC.1「サブセットアクセス制御」、FDP_ACF.1「セキュリティ属性に基づいたアクセス制御」に関する保証アクティビティ

背景

オペレーティングシステムは、その定義するオブジェクトへのアクセスを制御する必要がある。OSPP 基本部では、異なる利用者間でデータの共有が可能なすべてのオブジェクトについて、アクセス制御方針が存在することを要求している。オペレーティングシステムは異なる種類のオブジェクトに異なるアクセス制御方針を実装してもよく、またその場合にはセキュリティターゲットには FDP_ACC.1 及び FDP_ACF.1 の複数のインスタンスが必要とされる。さらに OSPP では、1 種類の名前付きオブジェクトに対して少なくとも 1 つのアクセス制御方針が、単一の利用者の粒度にまでアクセスを細かく定義できる機能を提供することを要求している。

OSPP では、異なる利用者間でデータの共有に用いられるオブジェクトがアクセス制御方針によってカバーされることを要求しているが、オペレーティングシステムはアクセス制御方針を、利用者の特定のオペレーティングシステム機能へのアクセスや、特定の特権の利用、あるいはデータの共有に用いられないその他の種類の「オブジェクト」を制御するために使ってもよい。セキュリティターゲットでも、これらのアクセス制御方針を定義することになるだろう。

ST 作成者は、各アクセス制御方針について、SFR 中で以下を定義する必要がある。

- アクセス制御方針によってカバーされるオブジェクトの種類、サブジェクトまたは利用者の種類、及び操作。
- （アクセス制御方針中で定義される種類の）サブジェクト／利用者が（アクセス制御方針中で定義される種類の）オブジェクトに対するアクセス制御方針でカバーされる操作のひとつを行えるかどうかを TOE が判定するために使われる正確なルール。アクセス制御方針が競合するアクセス権の定義を許可している場合、これらの競合が解決される方法がアルゴリズムによって定義される必要がある。

異なる種類のサブジェクトまたは利用者、あるいは異なる操作に対してのルールが異なる場合、異なるアクセス制御方針に同一の種類のオブジェクトが現れるかもしれないことに注意されたい。

また、アクセス制御方針によって利用されるルールそのものも、管理可能であるかもしれないことにも、注意されたい。セキュリティターゲットでは固定したルールセットの定義が必要とされる場合、ガイダンスでは TOE がこのルールを設定する方法が説明される必要があり、またルールセットの管理は信頼された管理者に限定（または無効と）される必要があり、さらに管理者には「評価された構成ガイド」中でこのルールセットを変更しないようアドバイスされる必要がある。

アクセス制御方針それ自体の評定と、(利用者及び) オブジェクトのセキュリティ属性の管理、さらにはアクセス制御判定を行う際に用いられるその他の TSF データとの間には、強い依存性が存在する。これによって、アクセス制御方針の保証アクティビティと、アクセス制御方針で用いられる TSF データの管理との間に、重複が生じることになる。評価者は管理 SFR に関連する評定を 2 度行うことは避けるべきであり（should not）、必要な場合

には FDP_ACC 及び FDP_ACF の自分の評定中に管理 SFR について行われた評定を参照すべきである。

TOE 要約仕様（TSS）

期待

TOE 要約仕様（または TSS が参照する公的な文書）には、TOE がアクセス制御方針の実装に用いるメカニズムと方針中で用いられるセキュリティ属性が、簡潔に記述されなくてはならない（shall）。例えば TOE が「パーミッションビット」と「アクセス制御リスト」との組み合わせを用いる場合、TOE 要約仕様ではこれを説明する必要があり、またこれらの管理方法についても説明する必要がある。このことは、アクセス制御方針中に言及される任意のその他のセキュリティ属性についても適用される。これらのセキュリティ属性の管理に関して、TOE 要約仕様には以下に関する情報が提供される必要がある。

- 各セキュリティ属性が初期化される方法、特にセキュリティ属性のデフォルト値が何なのか
- どのようにセキュリティ属性の値が変更できるか（それが可能な場合）及び変更が許可されるかどうかの判断に TOE が用いるルールは何か

さらに、TOE 要約仕様（または TSS が参照する公的な文書）には以下が記述されている必要がある。

- 利用者／サブジェクトが新たなオブジェクトの作成を要求する際に満たされるべき条件（1 つのアクセス制御方針で言及されるすべてのオブジェクトについて）、
- 新たなオブジェクトが作成される際に割り当てられるデフォルトのアクセス権を決定するルール（1 つのアクセス制御方針で言及されるすべてのオブジェクトについて）、
- 利用者／サブジェクトがオブジェクトの削除を要求する際に満たされるべき条件（1 つのアクセス制御方針で言及されるすべてのオブジェクトについて）。

評価者のアクティビティ

評価者はまず、SFR 中に定義されるアクセス制御アルゴリズム（これは TSS 中で詳細化されている可能性がある）を分析し、これらが完全であり、方針を定義するルール中で用いられるすべての可能なセキュリティ属性の組み合わせについてイエスまたはノーの判定を提供するものであるかを検証する。

評価者は、SFR と TSS を一貫性について分析する。SFR 中に列挙されるすべてのアクセス制御方針は、TSS 中にも同一の種類のオブジェクト、サブジェクト及び操作について記述されるべきであり、また方針中で言及されるすべてのセキュリティ属性について、TSS にはそれらが管理できるかどうか、及びその方法について説明される必要がある。評価者は、各アクセス制御方針について、そのアクセス制御方針のルールで言及されるセキュリティ属性のリストを構築し、各セキュリティ属性について TSS に管理可能ではない（または TSS によって内部的に管理される）であると言及されているか、あるいはそのセキュリティ属性の管理を支配するルールが定義されているかのどちらかであることを検証する。次に評価者は、すべてのアクセス制御方針についてアクセス制御方針でカバーされるサブジェクト／利用者の種類、オブジェクトの種類、及び操作を定義する完全なモデルと、方針によってアクセスが許可されるかどうかを TOE が判定するために用いられるルールの

完全なセットを持つべきである（should）。また評価者は、アクセス制御方針のルールに用いられるすべてのセキュリティ属性のリストとともに、これらのセキュリティ属性が管理できるかどうかを判定するルールを持つ。さらに評価者は、新たなオブジェクトが作成できる場合を判定するルールとともに、作成時に割り当てられるオブジェクトのセキュリティ属性の値とオブジェクトが削除できる場合を判定するルールを持つ。

評価者は、このアクセス制御方針のモデルを用いて、このモデル中の完全性と不整合をチェックする。不整合の例としては、2 つ以上のアクセス制御方針に現れるオブジェクトの種類であって、評価者がサブジェクト／利用者及び操作の種類にも重複を特定し、また重複する部分のルールが 2 つの方針の間で異なる場合が挙げられる。不整合のもうひとつの例としては、別の操作を暗示する操作のルールが、暗示された操作よりも多くのアクセスを提供する（例えば、「読み取り」操作を許可されないようなルールによって「読み取り及び書き込み」操作が許可される）場合が挙げられるであろう。

機能仕様

期待

機能仕様（これは公的に利用できる）には、アクセス制御が強制される TSF へのすべてのインタフェースが、アクセス制御方針またはアクセス制御方針中で利用されるセキュリティ属性の管理に用いられるすべてのインタフェースとともに、特定されなくてはならない（shall）。アクセス制御が強制されるそれぞれのインタフェースについて、アクセスが拒否された場合に呼び出し側へどのように通知されるのかが記述される必要がある。すべてのインタフェースは、それらをアクセス制御方針または管理アクティビティのテストに用いることができるように、記述される必要がある。

評価者のアクティビティ

評価者は、アクセス制御が強制されるものとして特定されたすべてのインタフェースについて、そのインタフェースによって対処されるオブジェクトの種類及び 1 つまたは複数のアクセス制御方針の操作が特定され、さらにアクセス制御方針の記述へ対応付けられていることを検証する。インタフェースの記述に、セキュリティターゲット中のアクセス制御方針記述に定義されているものよりも多くのオブジェクトまたはより多くの操作（アクセス制御方針の対象として）が言及されている場合、評価者はこれを不整合としてフラグを立てる必要がある。これが不整合でないことを評価機関及びスキームが受け入れられるような説明を開発者が提供できない限り、セキュリティターゲットを更新してこの不整合を除去することが必要とされる。

さらに評価者は、セキュリティターゲットの主張するすべてのセキュリティ属性が管理可能であり、管理インタフェースは機能仕様中に特定され、セキュリティターゲット中に定義される管理アクションが可能であり、また管理機能のテストに利用できるようにこれらのインタフェースが記述されていることを検証する。

注意: この評定は、管理領域の SFR について行われる評定アクティビティと重複するため、評価者は管理アクティビティの様々な側面が 1 回のみ評定されることを確実にする。評価者は、FDP_ACC/FDP_ACF について行われるアクティビティの中から管理に関連した SFR を分析する際に行われる評定を参照してもよいし、あるいはその逆を行ってもよい。

アーキテクチャ設計

期待

TOE 設計文書（セキュリティターゲット中の TSS、機能仕様、及び評価用に提供された任意の追加的設計関連文書から成る）では、1 つまたは複数のアクセス制御方針の実装の原則が、特に TSF によってセキュリティ属性が保存され維持管理される方法及び場所を中心として、説明されている必要がある。これらのセキュリティ属性の内部表現が外部インタフェースから可視である場合には、セキュリティ属性の内部表現も公的な文書中に記述される必要がある。TOE 設計では、TOE アーキテクチャのメカニズムによってセキュリティ属性が保護される方法が記述される必要がある。

TOE 設計文書には、アクセス制御メカニズムがバイパス不可能な根拠が含まれる必要がある。

永続的ストレージオブジェクトへのアクセスを行う大部分のオペレーティングシステムは、そのオブジェクトが「オープン」される際にアクセス制御を行い、オブジェクトへアクセス操作が行われるたびには行わない。利用者／サブジェクトがオブジェクトの「オープン」状態を維持できる限り、「オープン」中にチェックされるアクセス操作については、たとえその後アクセスが失効していたとしても、アクセス操作が行われるかもしれない。そのことが TOE 設計、機能仕様、またはガイダンスに記述されている限り、これは許容可能である。

場合によっては、単一のオブジェクトに異なる名前やそのオブジェクトへのリンクを利用してアクセスが行われることがある。設計には、オブジェクトが参照される方法に関わらず、アクセス制御ルールが適用されることが説明されている必要がある。

評価者のアクティビティ

評価者は、アクセス制御方針の実装の原則が、セキュリティターゲットや機能仕様、及びガイダンス中の方針の記述と一貫していることを検証する。評価者は、ストレージ及びアクセス制御方針に用いられるセキュリティターゲットの管理の記述が完全（セキュリティターゲット中に言及されるものに関して）であること、及びそれらが利用され管理される方法に関してセキュリティターゲット及びガイダンス中の記述と一貫していることを検証する。これを行う最良の方法は、各セキュリティ属性をセキュリティターゲット、機能仕様、設計、及びガイダンス中の記述と対応付ける表を作り、そしてこれらの記述が一貫していることを検証することである。

オブジェクトがさまざまな異なる方法で参照できる場合、評価者はこれらの異なる方法を TOE 設計、機能仕様、及び利用者ガイダンスから抽出し、オブジェクトが参照される方法に関わらずアクセス制御が強制されることを確証するために十分な情報を TOE 設計が提供しているかどうかを判定する。それでもまだ評価者が確信できない場合には、追加的なテストケースによって対処してもよい。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

利用者ガイダンスには、アクセスが許可されるかどうかの判定に用いられる異なるアクセス制御方針が、そのアルゴリズムとともに、記述されることが期待される。またガイダンスには、アルゴリズムのルール中で使用される一連のセキュリティ属性に基づいてアルゴリズムがどんな判定を行うかを利用者が理解できるように、アクセス制御アルゴリズムに関する説明が必要とされる。

利用者ガイダンスには、アクセス制御方針及びアクセス制御ルールによって用いられるセ

キュリティ属性の管理方法が記述され、個別の管理操作を行うために満たされる必要のある条件が特定されることが期待される。開発者がその公的な文書をどのような構造としているかにもよるが､この情報は管理に用いられるインタフェースと共に記述されてもよく、これはもちろんこの情報を提供する上で許容される方法である。

利用者ガイダンスには、方針をセキュアに設定する方法と、アクセス制御またはセキュリティ属性の管理に責任を持つ利用者がアクセス制御ルールに用いられているセキュリティ属性の現在の状態を問い合わせる方法についての説明が期待される｡またガイダンスには、アルゴリズムのルール中で使用される一連のセキュリティ属性に基づいてアルゴリズムがどんな判定を行うかを利用者が理解できるように、アクセス制御アルゴリズムに関する説明が必要とされる。

特定のセキュリティ属性を管理することを許可された者が、アクセス制御方針に用いられているその他のセキュリティ属性の状態を問い合わせることは、必ずしも可能ではないかもしれない。例えば、自分の「所有」しているオブジェクトのアクセス制御リストの変更が許可されている利用者は、自分がアクセス権をグループに割り当てることが許可されていたとしても、グループに属するメンバーのリストを問い合わせることは許可されていないかもしれない。この概念とそのセキュアな使い方がガイダンスに説明されている限り、このことはセキュリティの問題とはみなされない。

評価者のアクティビティ

評価者は、異なるアクセス制御方針のアルゴリズムが完全かつ正確に利用者ガイダンス中に記述されていることを検証する。

また評価者は、管理可能なすべてのセキュリティ属性について、利用者ガイダンスに以下が記述されていることを検証する。

- その管理方法
- 利用者が個別の管理操作を行うことが許可される場合を定義するルール
- アクセス制御方針のふるまいに関する管理操作の影響
- 直ちに明らかではないような副作用の可能性。これらの副作用がセキュリティの問題につながる恐れのある場合には警告と共に。例としては、オブジェクトをどの利用者からもアクセス不可能としてしまうような管理操作が挙げられるであろう。
- （問い合わせ操作を行うために満たされる必要のある条件を含めて）

また評価者は、セキュリティ属性にデフォルト値を設定し、管理操作を行うために必要とされる特権を割り当て､そしてアクセス制御方針をアクティベートするステップを含めて、それぞれのアクセス制御方針を初期化し構成するすべてのステップがガイダンスに記述されていることを検証する。

さらにガイダンスには、アクセス制御に関連するセキュリティ属性の即時失効を TOE が実施しない状況が説明され、利用者のアクセスが失効するようにセキュリティ属性が変更された後もかなりの時間だけその利用者がオブジェクトにアクセスできるような状況を避けるための方法を示すガイダンスが提供されることが要求される。例えば、その時点でオブジェクトへのアクティブなアクセスパスを利用者が持っているかどうかを判定する方法と、このアクセスパスを強制的にクローズさせるために正当な管理者が取ることのできる

アクションをガイダンスで説明することができるであろう。

評価者は、自分が実施する必要のあるテストケースを定義する際に、ガイダンスを利用してアクセス制御方針の構成や、アクセス権及びアクセス制御アルゴリズムに用いられるその他のセキュリティ属性の定義及び変更を行う。

テスト

期待

テストケースは、開発者によって提供され評価者によって実行されても、あるいは評価者によって開発されても、どちらでもよい。

テストケースには、以下をカバーすることが要求される。

- セキュリティターゲット中に言及されるすべてのアクセス制御アルゴリズム
- アクセス制御アルゴリズムのそれぞれについて、アルゴリズムを通過するすべてのパス（セキュリティターゲットでの定義による）、特に「イエス」または「ノー」の判定と共にアルゴリズムが停止する、アルゴリズムの各リーフ
- アクセス制御アルゴリズムに用いられるセキュリティ属性の設定の組み合わせの代表的なセット

また、アクセス制御アルゴリズムに用いられるセキュリティ属性の管理に用いられる管理機能についても、テストケースの存在が必要とされる。これらのテストケースは、すべてのセキュリティ属性をカバーし、それぞれのセキュリティ属性は属性の値の代表的なセットをカバーする必要がある。テストケースには、以下が示される必要がある。

- セキュリティ属性の管理を行うための条件が強制されること（管理要求が拒否されるテストケースを含め）
- セキュリティ属性の値が、アクセス制御アルゴリズムに記述された影響を及ぼすこと。
- セキュリティ属性の値が問い合わせ可能であること（必要な条件が満たされた場合）

注意 : これらのテストケースは、一部の管理 SFR の評定に要求されるテストケースと重複するであろう。これらのテストを 2 度実行する必要はもちろんないが、単にテストケースを FDP_ACC/FDP_ACF に関する SFR と管理 SFR の両方に対応付けるだけでもよい。

異なる方法でオブジェクトがアクセス可能な場合には、追加的なテストケースが必要とされる。オブジェクトへアクセス可能な方法のそれぞれについて、アクセス制御が強制されることを例証するテストケースの存在が必要とされる。オブジェクトへアクセス可能な方法のそれぞれについて、アルゴリズムを通過するすべてのパスがテストされる必要はないことに注意されたい。

評価者のアクティビティ

評価者は、、セキュリティターゲットに言及されるアクセス制御方針のそれぞれについて、アクセス制御アルゴリズムを通過するすべてのパスが少なくとも 1 つのテストケースによってカバーされていることを示す十分なテストケースが提供され（そのテスト結果と共に）ていることを検証する。その後、評価者はセキュリティ属性のリストをテストケースと対

応付けて、すべてのセキュリティ属性が代表的な値のセットでカバーされていることを示す。代表的な値のセットは、セキュリティ属性の値のセット全体と、それがアクセス制御方針へ与えることが期待される影響に依存する。

例えばアクセス制御リストがセキュリティ属性の場合、テストケースはすべての可能なアクセスの種類について存在が必要とされるが、（もちろん）すべての利用者については必要ない。

また評価者は、各管理機能をテストケースへ対応付け、すべての管理機能がテストケースによってカバーされていることを示す。

多くの場合、上記のカバレージを示すために必要とされるよりもかなり多くのテストケースを開発者は持っている。開発者から提供されたテストケースのサブセットを用いて上記の必要とされる対応付けを評価者が完了した際には、このサブセット以外の開発者のテストケースを評価者が分析する必要はない。

評価者は、自分が分析したテストケースに見つけ出せなかったセキュリティ属性の組み合わせを特定し、これらの組み合わせの一部を用いて一連のテストを実行し、その結果がアクセス制御方針の定義と一貫していることを検証する。

FDP_IFC.1 サブセット情報フロー制御及び FDP_IFF.1 単純なセキュリティ属性に関する保証アクティビティ

背景

基本 OSPP に適合するオペレーティングシステムには、TOE へ向かうネットワークトラフィック及びサブジェクトが生成し外部 IT エンティティへ送信されるネットワークトラフィックへの基本的なフィルタリングを行うことのできる、構成可能な機能を提供することが求められる。フィルタリングルールは、レイヤ 2 トラフィックまたはレイヤ 3 トラフィックあるいはその両方に行われるものであってよい。レイヤ 3 については少なくとも、基本的な「マッチング」ルールが定義でき、IP アドレス、TCP ポート番号、UDP ポート番号、ネットワークプロトコル、及び TCP ヘッダフラグに基づいて、特定の未認証の外部 IT エンティティへの、及びそれからのトラフィックを禁止するフィルタリングルールを管理者が管理できることが TOE に必要とされる。レイヤ 2 については、管理者が MAC アドレス及び VLAN タグに基づくフィルタリングルールを定義して、これらの属性に関するマッチング基準に基づいてトラフィックを許可または除外できることが必要とされる。

これら 2 つの SFR に関連する SFR は、フィルタリングルールを定義するために管理者が満たさなくてはならない条件を定義する FMT_MSA.3(NI) である。

TOE 要約仕様（TSS）

期待

TSS（または TSS の参照する公的な文書）には、以下と共に TOE が実装するネットワークトラフィックのフィルタリングルールの種類が記述される必要がある。

- そのルールが適用されるネットワークトラフィック
- フィルタリングルールが基づくことができるネットワークプロトコルデータ
- ルールが「発火」するための定義可能な基準

- ルールが「発火」した際に取ることができるアクション

また TSS（または TSS の参照する公的な文書）には、フィルタリングルールの定義またはアクティベートあるいはその両方に用いられる管理インタフェースが記述される必要がある。

評価者のアクティビティ

評価者は TSS に言及されるネットワークプロトコル、ネットワークプロトコルデータ、ルールが「発火」するための基準、及び可能なアクションが FDP_IFC.1 及び FDP_IFF.1 の定義と一貫していること、すなわち SFR に定義された基準及びルールがすべて TSS または TSS の参照する公的な文書中の記述に対応付けられることを検証する。FDP_IFF.1 に定義された機能にマッチするルールを管理者が定義可能であることは、FMT_MTD.1(NI) に関する保証アクティビティ中で検証されることに注意されたい。

機能仕様

期待

FDP_IFC.1 及び FDP_IFF.1 の影響をテストするために用いられるインタフェースは、外部ネットワークインタフェース、オペレーティングシステム上で動作するサブジェクトがネットワークトラフィックの送信及び受信に利用できるインタフェース、及び管理者がフィルタリングルールの定義及び管理に利用できるインタフェース（これは FMT_MTD.1(NI) に関する保証アクティビティ中で分析されテストされる）である。FDP_IFC.1 及び FDP_IFF.1 の実装を検証するため、ネットワークインタフェースはそれらがサポートするネットワークプロトコルの仕様（レイヤ 3 まで）と共に記述される必要があり、またサブジェクトがネットワークトラフィックの送信及び受信に利用できるインタフェースは、ネットワーク情報フロー方針のルールがテスト可能なレイヤでネットワークデータの送信及び受信を可能とするパラメタと共に記述される必要がある。

評価者のアクティビティ

評価者は、それを使ってフィルタリングルールの影響をテストできる程度にまで、インタフェースが記述されていることを検証する。

アーキテクチャ設計

期待

フィルタリングルールのすべての影響が TSFI において直接テストできない場合には、どの TSFI 内部インタフェースがフィルタリングルールの影響のテストに利用できるか、及びこれらのインタフェースを使ってテストを行う方法がアーキテクチャ設計に説明される必要がある。

評価者のアクティビティ

評価者は、フィルタリングルールのすべての影響が TSFI において直接テストできない場合には、機能仕様に記述された TSFI 全体と TSF 内部インタフェースでフィルタリングルールのすべての影響を十分にテストできることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

利用者ガイダンスに関する具体的な期待はない。

評価者のアクティビティ

なし。

テスト

期待

開発者は、以下の場合をテストするテストケースを提示することが要求される。

- 単一のセキュリティ属性のそれぞれについて、それに基づいた単一のフィルタルールによって、そのルールが「発火」する場合には定義されたアクションが取られ、そのルールが「発火」しない場合には取られないことを示すこと
- 2 個以上のフィルタルールの組み合わせで、そのフィルタルールの組み合わせで取られることが期待されるアクションが実際に取られることを示すこと。FMT_MSA.1(NI) に関する保証アクティビティでは、フィルタルールの可能な組み合わせのそれぞれについて、検査されたパケットに関して TOE が取るアクションを開発者文書から明確に特定できることを評価者が検証することが要求されていることに注意されたい。評価者は、この仕様を開発者の文書から取り、以下の場合について期待される結果を規定する。
    - 異なるセキュリティ属性を用い、異なるアクションを定義するフィルタルールの組み合わせ
    - 可能であれば、同一のセキュリティ属性を用いるが異なるアクションを定義するフィルタルールの組み合わせ
- FDP_IFF.1.4 及び FDP_IFF.1.5 に列挙されるすべての例外

評価者のアクティビティ

評価者は、上に定義された場合にしたがって、異なるフィルタルールを TOE に順番に構成しなくてはならない（shall）。次に評価者は、1 つ以上の外部 IT エンティティから TOE へのネットワークトラフィックを開始し、外部 IT エンティティから TOE 内のサブジェクトへのトラフィックがブロックされるべきフィルタルールのセットと外部 IT エンティティから TOE 内のサブジェクトへのトラフィックが許可されるべきフィルタルールのセットのそれぞれについてテストを行い、そして TOE がその仕様にしたがって動作していることを検証しなくてはならない（shall）。同様に評価者は、TOE 内のサブジェクトから外部 IT エンティティへのネットワークトラフィックについて、上に定義された場合に応じた異なるルールセットを用いてテストを行い、TOE 内部のサブジェクトから外部 IT エンティティへのネットワークトラフィックについて、TOE がその仕様にしたがって動作していることを検証しなくてはならない（shall）。評価者は、開発者によって提供されたテストケースを再利用してもよいが、これらを変更されたルールセットと共に用い、また場合によってはこれらのテストケースを変更して開発者のテストケースでは対処されていなかったパラメタの組み合わせをカバーすべきである（should）。

テストケースは、以下をカバーする必要がある。

- FDP_IFF.1.3 に列挙されたすべてのセキュリティ属性、及びすべてのセキュリティ属性について取り得るアクションのそれぞれについて少なくとも 1 つのテスト

ケース

- 異なるセキュリティ属性について複数のルールを含むルールセット及び正しいアクションが取られることをテストするテストケース。またこの場合には、取り得るアクションのそれぞれについて少なくとも 1 つのテストケースが必要である

FDP_RIP.2 残存情報の保護に関する保証アクティビティ

背景

残存情報は、数多くのオブジェクトやリソースに、それらが異なるサブジェクトまたは利用者へ再割り当てされた際に存在する可能性がある。カバーされる必要のある例を以下に挙げる。

- オブジェクト関連の TSF データ（例えばディレクトリエントリ、オブジェクトのセキュリティ属性）を含めた、永続的ストレージオブジェクト（ファイルシステムオブジェクト）における残存
- メインメモリオブジェクトにおける残存
- 信頼されないサブジェクトによって読み書きされる可能性のあるプロセッサオブジェクトにおける残存（例えば、汎用レジスタ、浮動小数点レジスタ）

TOE 要約仕様（TSS）

期待

TSS（または TSS の参照する公的な文書）には、残存が生じる可能性のあるリソースが特定され、それらのリソースのそれぞれについてサブジェクトまたは利用者によって保存された情報をそのリソースが別の利用者またはサブジェクトへアクセス可能とする前に利用できなくするために TOE によって実装されている戦略が簡潔に記述される必要がある。TOE がすべてのリソースについてオブジェクトの再利用を強制するために特定の初期化または構成あるいはその両方の手順を必要とする場合、このこと及び必要な手順が TSS 中に特定される必要がある（必要に応じて追加的な公的文書への参照と共に）。

評価者のアクティビティ

評価者は、少なくともアクセス制御 SFR 中に言及されたオブジェクトに関連するすべてのリソース（オブジェクトによって占有されていた空間の部分的な開放を含む）、メインメモリ及びプロセッサリソースが、TSS 中のオブジェクトの再利用に関連した記述中で対処されており、またその記述にはリソースの以前の内容に関する情報を確実に利用できなくするために用いられる戦略が十分に説明されていることを検証する。

機能仕様

期待

オブジェクトの再利用に関する直接的な TSF インタフェースは存在しない。その代わり、オブジェクトの再利用の機能の影響が確認できるインタフェースが特定される必要がある。

評価者のアクティビティ

オブジェクトの再利用を必要とすると特定されたリソースのそれぞれについて、評価者は開発者によって提供された TSFI から以下を特定する。

- リソースの解放に用いることのできるインタフェース
- リソースの再割り当てに用いることのできるインタフェース
- 再割り当て後のリソースの内容を読み出すために用いることのできるインタフェース

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、オブジェクトの再利用が行われる方法について正しく記述していることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

オブジェクトの再利用が行われる方法の詳細を規定するために使うことのできる管理機能がある場合を除き、オブジェクトの再利用に関連した具体的なガイダンスに関する期待は存在しない。そのような管理機能がある場合であって、オブジェクトの再利用の要件が満たされない構成を TOE が許可している場合には、オブジェクト再利用機能がアクティブであることを確実にするために取る必要がある構成手順がガイダンスに明確に記述される必要がある。

評価者のアクティビティ

TOE がすべてのリソースについてオブジェクト再利用機能を提供するために特定の初期化及び構成が行われる必要のある場合にのみ、オブジェクトの再利用機能を確実にアクティブとするように TOE を初期化または構成あるいはその両方を行うために必要なインタフェース及びパラメタを、TSS の記述にしたがって評価者は特定する。これは、オブジェクトの再利用機能のテストのために TOE を用いる前に必要とされる。

テスト

期待

テストは、オブジェクトの再利用の対象となる必要のあるリソースを割り当てるために用いられるすべてのインタフェースをカバーし、またその後リソースに、異なるサブジェクトによる以前の利用からの情報が含まれている可能性があるかどうかの分析を行うことが期待される。テストには、リソースの以前の利用から残された情報を取得するすべての試みをカバーすることが期待される。

テストは、少なくとも以下の場合をカバーする必要がある。

- 永続的ストレージオブジェクトの、そのオブジェクトが作成されてから書き込みが行われたことのない領域からの読み取りの試行。

- 動的ストレージ割り当てを用いて取得されたが、まだサブジェクトによって書き込まれたことのないメインストレージ領域からの読み取り。
- コンテキストスイッチ後の利用者アクセス可能なプロセッサレジスタの読み取り。
- オブジェクトの再利用の対象として列挙されたその他のリソースであってサブジェクトへ割り当てられたものからの、サブジェクトによってこれらのリソースへ情報が配置される以前の読み取り。

評価者のアクティビティ

評価者は、オブジェクトの再利用が定義されているすべてのリソースがテストによってカバーされていることを検証し、以前の情報へのアクセスが不可能であることを示す。評価者は、新たに割り当てられたリソースの読み取りが可能なすべての TSFI がテストスイートに含まれており、いかなる場合にも以前の情報へのアクセスが不可能であることを検証する。

FMT_MSA.1 オブジェクトのセキュリティ属性の管理に関する保証アクティビティ

背景

オブジェクトのセキュリティ属性には、アクセス制御方針の強制に用いられるすべてのオブジェクトのセキュリティ属性が含まれる。

TOE 要約仕様（TSS）

期待

TSS（または TSS の参照する公的な文書）には、アクセス制御管理の強制、管理、及び監査方針に用いられるオブジェクトセキュリティ属性が、それらが管理可能な場合を定義するルールとともに、列挙されている必要がある。

評価者のアクティビティ

評価者は、アクセス制御、オブジェクト管理及びオブジェクト関連監査方針のルール内で SFR 中に言及されるオブジェクトのセキュリティ属性のリストを、TSS に管理可能として列挙されているものと比較する。TSS に管理可能と言及されているがどの SFR でも使われていないオブジェクトのセキュリティ属性について、評価者はそれらの目的を明確にする必要がある。SFR に言及されているが TSS には管理可能と定義されていないオブジェクトのセキュリティ属性について、評価者はこれらのオブジェクトセキュリティ属性がオブジェクトの所有者にも任意の他の利用者にも管理できないことを検証する必要がある。

機能仕様

期待

オブジェクトのセキュリティ属性を管理するために用いられるインタフェースは、TSS に管理可能として列挙されているすべてのオブジェクトのセキュリティ属性について特定される必要がある。

評価者のアクティビティ

評価者は、管理可能として列挙されているすべてのオブジェクトのセキュリティ属性につ

いて管理インタフェースが特定され、記述されていることを検証し、また FMT_MSA.1 に列挙されているすべての管理アクションがこれらのインタフェースを用いて行えることを検証する。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれによって TSS 中になされた言明が正しく詳細化されており、オブジェクトのセキュリティ属性が管理される方法が正しく記述されていることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

ガイダンス（または機能仕様）には、利用者にオブジェクトのセキュリティ属性の管理を許可するために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

評価者は、オブジェクトのセキュリティ属性の管理のためのガイダンス中に定義された条件が、FMT_MSA.1 に定義された条件と一致していることを検証する。

テスト

期待

開発者は、オブジェクトのセキュリティ属性の管理に用いられるインタフェースのテストを、その機能テストの一部として行うことが期待される。これは、例えば、これらのインタフェースを用いてオブジェクトのセキュリティ属性を設定してアクセス制御アルゴリズムの異なる側面がテストされるようなアクセス制御方針のテストにオブジェクトのセキュリティ属性が用いられる場合に、SFR のテストと連携して行われることが多い。

評価者のアクティビティ

評価者は、テストにオブジェクトのセキュリティ属性の管理に用いられると定義されたすべてのインタフェース及びすべてのオブジェクトのセキュリティ属性が含まれ、個別のオブジェクトのセキュリティ属性について十分な値のセットがカバーされていることを検証する。評価者は、オブジェクトのセキュリティ属性の設定の影響がテストされていることを検証する（アクセス制御アルゴリズムのテストの一部として行われる場合が多い）。

FMT_MSA.3(DAC) 静的な属性の初期化に関する保証アクティビティ

背景

任意アクセス制御方針の強制に用いられるすべてのセキュリティ属性のデフォルト値は、オブジェクトが作成された際にデフォルトで定義された利用者のセット（通常は所有者）にアクセスが限定されるように定義される必要がある。これは、新たなオブジェクトが作

成された際にそのような制約的なデフォルト値に初期化される必要のあるオブジェクトのセキュリティ属性だけでなく、アクセス制御方針中で用いられるその他のセキュリティ属性にも適用される。一部のセキュリティ属性は、（FMT_MSA.4 の定義により）別のオブジェクトから継承されてもよく、これらの場合のデフォルト値は継承された値となることに注意されたい。これらの継承された値がどのように割り当てられるかというルールは FMT_MSA.4 に定義されており、FMT_MSA.4 に関する保証アクティビティ中で分析される。

TOE 要約仕様（TSS）

期待

任意アクセス制御方針に用いられるすべてのオブジェクトのセキュリティ属性について、TSS（または TSS の参照する公的な文書）には、新たなオブジェクトが作成される際にこれらが初期化される方法と、これらの初期デフォルト値が定義される方法が記述される必要がある。

また TSS には、これらのデフォルト値が管理可能かどうかとその方法、これらの管理アクティビティに用いられるインタフェースは何か、そしてこれらの管理アクティビティを行うためにどの条件が満たされる必要があるのかについて記述される必要がある。

評価者のアクティビティ

評価者は、任意アクセス制御方針に用いられるセキュリティ属性の初期化のアルゴリズムが、すべてのセキュリティ属性について定義されていることを検証する。評価者は、デフォルト値によって定義された利用者のセット（例えば所有者及び管理者）のみにアクセスが限定されることを検証する。評価者は、管理可能なデフォルト値、及びこれらの管理アクティビティを行うために満たされる必要のある条件が、FMT_MSA.3(DAC) 中の仕様と一貫していることを検証する。

機能仕様

期待

TSS では、任意アクセス制御方針の強制に用いられるセキュリティ属性のデフォルト値を管理するために使われるインタフェースを特定し、これらのインタフェースの仕様を参照する。

評価者のアクティビティ

評価者は、SFR 中及び TSS 中に言及された管理アクティビティがこれらのインタフェースを用いて行えること、及びテスト中にこれらのインタフェースを利用するために記述が十分であることを検証する。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS 中で追加的な設計文書が参照されている場合、評価者はこれによって TSS 中で行われた言明が正しく詳細化されており、また任意アクセス制御方針の強制に用いられるセキュリティ属性のデフォルト値の管理方法が正しく記述されていることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

ガイダンス（または機能仕様）には、任意アクセス制御方針の強制に用いられるセキュリティ属性のデフォルト値の管理が利用者に許可されるために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

評価者は、セキュリティ属性のデフォルト値を管理するためのガイダンス中に定義された条件が、FMT_MSA.3(DAC) に定義された条件と一致していることを検証する。

テスト

期待

開発者は、任意アクセス制御方針の強制に用いられるセキュリティ属性のデフォルト値を管理するためのインタフェースのテストを、その機能テストの一部として行うことが期待される。これは、これらのインタフェースを用いてオブジェクトのセキュリティ属性のデフォルト値を設定してアクセス制御アルゴリズムの異なる側面がテストされるようなアクセス制御方針の SFR のテストと連携して行われることが多い。

評価者のアクティビティ

評価者は、任意アクセス制御方針の強制に用いられるセキュリティ属性のデフォルト値を管理するものと定義されたすべてのインタフェースがテストに含まれ、個別のセキュリティ属性について十分な値のセットがカバーされていることを検証する。評価者は、セキュリティ属性の設定の影響がテストされていることを検証する（アクセス制御アルゴリズムのテストの一部として行われる場合が多い）。

FMT_MSA.3(NI) 静的な属性の初期化に関する保証アクティビティ

背景

ネットワーク情報フロー方針の強制に用いられるすべてのセキュリティ属性のデフォルト値は、デフォルトルールの何らかのセットによって、またはまったく何のルールもない状態に定義される必要がある。

TOE 要約仕様（TSS）

期待

ネットワーク情報フロー方針に用いられるすべてのセキュリティ属性について、TSS（または TSS の参照する公的な文書）には、これらが初期化される方法と、これらの初期デフォルト値が定義される方法が記述される必要がある。また TSS には、これらのデフォルト値が管理可能かどうかとその方法、これらの管理アクティビティに用いられるインタフェースは何か、そしてこれらの管理アクティビティを行うためにどの条件が満たされる必要があるのかについて記述される必要がある。注意：これらの管理アクションが FMT_MTD.1(NI) に関するものと大幅に重複しており、FMT_MTD.1(NI) に関して定義さ

れた保証アクティビティによってカバーされることは十分にあり得る。

評価者のアクティビティ

評価者は、ネットワーク情報フロー方針に用いられるセキュリティ属性の初期化のアルゴリズムが､すべてのセキュリティ属性について定義されていることを検証する｡評価者は、このデフォルト値が FMT_MSA.3(NI) 中の仕様を満たしていることを検証する｡評価者は、管理可能なデフォルト値、及びこれらの管理アクティビティを行うために満たされる必要のある条件が、FMT_MSA.3(NI) 中の仕様と一貫していることを検証する。

機能仕様

期待

TSS では、ネットワーク情報フロー方針の強制に用いられるセキュリティ属性のデフォルト値を管理するために使われるインタフェースを特定し、これらのインタフェースの仕様を参照する。

評価者のアクティビティ

評価者は、SFR 中及び TSS 中に言及された管理アクティビティがこれらのインタフェースを用いて行えること、及びテスト中にこれらのインタフェースを利用するために記述が十分であることを検証する。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS 中で追加的な設計文書が参照されている場合、評価者はこれによって TSS 中で行われた言明が正しく詳細化されており、またネットワーク情報フロー方針の強制に用いられるセキュリティ属性のデフォルト値の管理方法が正しく記述されていることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

ガイダンス（または機能仕様）には、ネットワーク情報フロー方針の強制に用いられるセキュリティ属性のデフォルト値の管理が利用者に許可されるために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

評価者は、セキュリティ属性のデフォルト値を管理するためのガイダンス中に定義された条件が、 FMT_MSA.3(NI) に定義された条件と一致していることを検証する。

テスト

期待

開発者は、ネットワーク情報フロー方針の強制に用いられるセキュリティ属性のデフォル

ト値の管理に用いられるインタフェースのテストを、その機能テストの一部として行うことが期待される。これは、これらのインタフェースを用いてオブジェクトのセキュリティ属性のデフォルト値を設定してネットワーク情報フロー方針の異なる側面がテストされるようなネットワーク情報フロー方針の SFR のテストと連携して行われることが多い。

評価者のアクティビティ

評価者は、ネットワーク情報フロー方針の強制に用いられるセキュリティ属性のデフォルト値の管理に用いられると定義されたすべてのインタフェースがテストに含まれ、個別のセキュリティ属性について十分な値のセットがカバーされていることを検証する。評価者は、セキュリティ属性の設定の影響がテストされていることを検証する（フィルタリングルールのテストの一部として行われる場合が多い）。

FMT_MSA.4 セキュリティ属性値の継承に関する保証アクティビティ

背景

任意アクセス制御方針によってカバーされる新たなオブジェクトが作成される際、その新しいオブジェクトは既存のオブジェクトからセキュリティ属性を継承してもよい。これは、オブジェクトが階層構造の一部であって、新たなオブジェクトが階層中の次に高いレベルからセキュリティ属性を継承する場合によく行われる。継承は階層的オブジェクト構造に限定されるものではなく、新たなオブジェクトが何らかのグループのメンバーとなり、そしてそのグループから何らかのセキュリティ属性を引き継ぐ場合にも行われる。

継承は、新たなオブジェクトに関するオブジェクトセキュリティ属性の初期化の特別なケースである。

TOE 要約仕様（TSS）

期待

TSS（または TSS の参照する公的な文書）には、新たなオブジェクトが作成される際に継承されるオブジェクトのセキュリティ属性が特定される必要があり、また継承のルールは何か、そしてどこから継承されるのかについて記述が必要とされる。

評価者のアクティビティ

評価者は、任意アクセス制御方針に用いられるセキュリティ属性の継承のアルゴリズムが、継承されるすべてのセキュリティ属性について定義されていることを検証する。

機能仕様

期待

継承ルールが管理可能な場合を除き、この SFR に関連するインタフェースは存在しないのが普通である。継承は、新たなオブジェクトが作成される際に自動的に行われる。継承ルールが管理可能な場合、ST には FMT_MTD ファミリ中の SFR が定義され、その SFR には利用者にこの管理アクティビティを行うことが許可されるために満たされなくてはならない条件が記述される必要がある。

評価者のアクティビティ

継承ルールが管理可能な場合以外は、なし。継承ルールが管理可能な場合は、継承ルールの管理に用いられるインタフェースによって管理アクションが定義できることを、分析に

よって示す必要がある。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれが TSS 中になされた言明を正しく詳細化し、オブジェクトのセキュリティ属性の値が継承される方法について正しく記述していることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

なし。

評価者のアクティビティ

なし。

テスト

期待

開発者は、新たなオブジェクトを作成し、その後継承される予定のオブジェクトセキュリティ属性の値が正しく継承されていることを検証することによって、継承ルールをテストすることが期待される。

評価者のアクティビティ

評価者は、テストが継承可能なすべてのオブジェクトセキュリティ属性を、これらの属性への異なる値を用いてカバーしていることを検証する。

FMT_MTD.1(NI) TSF データの管理：ネットワークフィルタリングルールに関する保証アクティビティ

背景

ネットワークデータフィルタリングルールには、管理可能であり、適切な権限のある管理者にネットワークデータフィルタリングルールの定義、問い合わせ、変更、及び削除を可能とすることが必要とされる。TOE は、例えば特定の利用者にフィルタリングルールの問い合わせを許可するが変更権や削除権は与えないように、異なる操作に必要とされる権限を区別してもよい。そのような区別が異なる管理アクションについて存在する場合、これは SFR 中に表現される必要がある。

TOE 要約仕様（TSS）

期待

TSS（または TSS の参照する公的な文書）には、ネットワークデータフィルタリングルー

ルを定義する方法と、それらを閲覧、アクティベート、変更、及び削除する方法が説明される必要がある。また TSS には、これらのアクティビティに用いられるインタフェースと、利用者にこれらの管理アクティビティのいずれかを行う際に満たすことが必要とされる条件を特定することが必要とされる。

評価者のアクティビティ

評価者は、TSS 中に記述された管理機能及びインタフェースによって FMT_MTD.1(NI) に定義されるすべての管理アクションが可能であること、及び利用者にこれらのアクティビティを行う際に満たすことが必要とされる条件が、SFR 中の記述と一貫していることを検証する。

機能仕様

期待

機能仕様には、ネットワークデータフィルタリングルールの管理に用いられるインタフェースを定義することと、これらのルールを管理するための構文、各フィルタリングルールの正確な意味、そしてネットワークデータフィルタリングルールを定義、アクティベート、問い合わせ、変更、及び削除するための機能を定義することが必要とされる。また、利用者が管理アクションのそれぞれを行うために満たさなくてはならない条件も定義される必要がある（機能仕様中またはガイダンス文書中のどちらかで）。

評価者のアクティビティ

評価者は、インタフェースの記述が FMT_MTD.1(NI) に定義されるすべての管理アクティビティを行うのに十分であり、FDP_IFC.1 及び FDP_IFF.1 に定義されるすべての側面をカバーするフィルタリングルールの定義が可能であることを検証する。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれによって TSS 中になされた言明が正しく詳細化され、ネットワークデータフィルタリングルールが管理される方法が正しく記述されていることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

これがすでに機能仕様の評定中でカバーされているのでない限り、ガイダンスには利用者がネットワークデータフィルタリングルールのさまざまな管理アクティビティを行うために満たさなければならない条件の記述が期待される。さらにガイダンスには、さまざまなルールの意味の説明とルールのセット中で起こる可能性のある競合が対処される方法の定義が期待される。

評価者のアクティビティ

評価者は、ガイダンスにネットワークデータフィルタリングルールの意味が、ルールセット中で競合する可能性のあるルールの側面を含めて記述されており、評価者が定義するルールの各セットについてネットワークトラフィックへ与えることが期待される影響を判定できることを検証する。

テスト

期待

FMT_MTD.1(NI) のテストは、FDP_IFC.1 及び FDP_IFF.1 に定義されたテストと連携して行われることが期待される。管理インタフェースは、ネットワーク情報フロー方針のテストに用いられたネットワークフィルタリングルールのセットを定義するために用いられる。

さらに開発者には、利用者がさまざまな管理アクティビティを行うために満たさなければならない条件が、管理インタフェースによって強制されることをテストすることが期待される。テストケースは、アクセス制御アルゴリズムのテストと同様に、利用者の管理アクションを行う権利を判定するアルゴリズムのすべての分岐をカバーしなくてはならない（shall）。

評価者のアクティビティ

評価者は、テストケースによって管理アクティビティのすべての組み合わせと、利用者の管理アクションを行う権利を判定するアルゴリズムのすべての分岐がカバーされていることを検証しなくてはならない（shall）。

FMT_REV.1(OBJ) 失効：オブジェクトのセキュリティ属性に関する保証アクティビティ

背景

オブジェクトのセキュリティ属性の失効は、FMT_MSA.1 において対処されるオブジェクトのセキュリティ属性の管理の特別なケースである。したがって、オブジェクトのセキュリティ属性の失効は FMT_MSA.1 の評定と非常に類似した方法で取り扱われ、また FMT_MSA.1 に関する保証アクティビティと組み合わせて行われるべきである（should）。

TOE 要約仕様（TSS）

期待

TSS（または TSS の参照する公的な文書）には、失効可能なオブジェクトのセキュリティ属性が列挙される必要があり、また失効が行われる方法及び利用者がオブジェクトのセキュリティ属性の失効を行うためにどの条件を満たさなければならないのかが説明される必要がある。これらの条件が異なるオブジェクトのセキュリティ属性について異なる場合、これらの差異は SFR 中で定義される必要がある。

評価者のアクティビティ

評価者は、SFR 中に言及されるオブジェクトのセキュリティ属性のリストを、失効可能として TSS に列挙されているものと比較して、これらのリストが同一であることを確実にする。

機能仕様

期待

オブジェクトのセキュリティ属性を失効させるために用いられるインタフェースは、TSS に失効可能として列挙されているすべてのオブジェクトのセキュリティ属性について特定される必要がある。

評価者のアクティビティ

評価者は、失効可能として列挙されているすべてのオブジェクトのセキュリティ属性について、管理インタフェースが特定され記述されていること、及びこれらによってオブジェクトのセキュリティ属性を失効させることができることを検証する。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれによって TSS 中になされた言明が正しく詳細化され、オブジェクトのセキュリティ属性が失効される方法が正しく記述されていることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

ガイダンス（または機能仕様）には、利用者にオブジェクトのセキュリティ属性の失効を許可するために満たされなくてはならない条件が説明されている必要がある。

評価者のアクティビティ

評価者は、オブジェクトのセキュリティ属性の失効のためのガイダンス中に定義された条件が、FMT_REV.1(OBJ) に定義された条件と一致していることを検証する。

テスト

期待

開発者は、オブジェクトのセキュリティ属性の失効に用いられるインタフェースのテストを、その機能テストの一部として行うことが期待される。これは、オブジェクトのセキュリティ属性が、例えば、これらのインタフェースを用いてオブジェクトのセキュリティ属性のデフォルト値を失効させてアクセス制御アルゴリズムの異なる側面がテストされるようなアクセス制御方針のテストに用いられる場合に、SFR のテストと連携して行われることが多い。

評価者のアクティビティ

評価者は、テストにオブジェクトのセキュリティ属性の失効に用いられると定義されたすべてのインタフェース及びすべてのオブジェクトのセキュリティ属性が含まれていることを検証する。評価者は、オブジェクトのセキュリティ属性の失効の影響がテストされていることを検証する（アクセス制御アルゴリズムのテストの一部として行われる場合が多い）。

識別と認証に関する保証アクティビティ

FIA_AFL.1：認証失敗時の取り扱いに関する保証アクティビティ

TOE 要約仕様（TSS）

評価者は、TOE が認証失敗を取り扱う際に期待される動作に関する詳細を、TSS 中に提供されるセキュリティ機能記述から見つけ出すことになる。TOE 中の I&A 機能に関する議論が、試行の失敗が発生した際に何が起こるかを含め、TOE が認証を行うために採用するすべての手法を記述することになる。評価者はこの記述を調査して、この SFR 中に特定される認証手法のそれぞれが十分に記述されており、また試行の失敗が閾値に達した、または閾値を超えた際に何が起こるのかが明確になっていることを確証する。最低でも、パスワードベースの認証がカバーされていなくてはならない（must）。管理者と信頼されない利用者とで TOE が異なるふるまいをする場合があってもよく、これは要件の詳細化によって、要件の繰返しによって、もしくは認証事象中またはアクションのリストの割付に取り込むことを試みることによって、SFR 中に取り込むことができる。

機能仕様

I&A 機能に意図される動作を理解した上で、評価者はインタフェース仕様を参照してどのインタフェースが I&A をサポートしているのかを判断する。開発者には、インタフェースから I&A 機能への対応付けを、FIA_UAU.5 に対応するものを含めて提供することが要求され、また評価者はセキュリティ機能記述中に提示された I&A の手法の記述が提供されたインタフェースに含まれていること、及びその逆を確証する。失敗時の取り扱いの対象とならない認証が行われるインタフェースが存在するかもしれないが、この SFR に列挙される認証手法及び認証事象と一貫性がある限り、これは許容可能である。例えば、スマートカードを採用した TOE への認証を行うが、スマートカードの利用における認証失敗は認証手法の失敗とはみなされないようなインタフェースが存在するかもしれない。

しかし、通知されたインタフェースの記述に、失敗した認証試行に関連したアクションが取られることが示されており、また要件中の認証手法がこれに採用されていることを分析中に評価者が発見した場合、評価者は開発者と協力してこの不一致を解決しなくてはならない（must）。他方では、要件に規定されていない認証手法を採用したインタフェースを評価者が発見した場合、さらなるアクションは必要とされない。これは製品の主張されたセキュリティ機能の範囲外となるためである。

利用者操作ガイダンス

評価者は、閾値を管理するため、及び彼らの側に要求される起こり得るアクションへ反応するためのガイダンスが、SFR 中の言明と一貫していることを判定する。

テスト

TOE のふるまいを検証するために用いられるテストの数が、この要件の対象となる認証手法の数、これらの手法を呼び出すインタフェース、さらには取られるアクションの数に依存するのはもちろんである。評価者には、考慮すべき認証手法、各手法と関連付けられる可能性のある認証事象、及び取られることになるアクションを含んだマトリックスを作成することが推奨される。ここでも、所与の同一の認証手法に対してさえさまざまなアクションが取られる可能性があるため、テストアクティビティ中ですべての組み合わせが対処されることが非常に重要である。例えば、信頼されない利用者が正しいローカルパスワー

ドの入力を連続して 3 回失敗した際には、管理者によるアクションが取られるまでその利用者のアカウントは無効となったりロックされたりするかもしれない。他方では、管理ユーザが正しいローカルパスワードの入力を連続して 3 回失敗した際には、管理ユーザのアカウントは 30 秒間無効となるかもしれない。そのため、TOE の失敗時の取り扱いメカニズムの複雑さによって、テストの性質や数は変動することになる。

テスト 1：評価者は、適切な権限を有した上で、操作ガイダンスにしたがって各認証手法について（パスワードベースは最低限必要、その他は割付に応じて存在してもよい）認証試行の不成功の回数を構成しなくてはならない（shall）。

テスト 2：評価者は、テスト対象の認証手法を用いて認証の成功を試行しなくてはならない（shall）。認証が成功した後、評価者は X 回の認証試行の失敗を試みる（認証事象のリストに規定される「ルール」にしたがって回数は決定される）。試行の失敗回数が満たされた際、TOE がその利用者を感電させ、十分な電流で多大な損害を与えることを評価者は確認しなくてはならない（shall）。

テスト 3：評価者は、信頼されない利用者として、認証試行の不成功回数の制限を強制する変数の変更を試みなくてはならない（shall）。制御変数の変更は、成功してはならない（shall）。

FIA_ATD.1：利用者属性の定義に関する保証アクティビティ

TOE 要約仕様（TSS）

評価者は、定義された各利用者について維持管理される利用者セキュリティ属性を、TSS 中に列挙されたものの中から見つけ出すことになる。利用者のセキュリティ属性のリストは FIA_ATD.1 に特定されているものとは違っていてもよく、また FIA_ATD.1 において割り当てられた追加的な利用者セキュリティ属性の文脈における最小セットを拡張するために使われてもよい。TSS 中に特定された利用者セキュリティ属性のリストが FIA_ATD.1 中のものと異なっている場合、要求される利用者セキュリティ属性の関連付け及びカバレージを示す明確な対応付けが TSS に提供されなくてはならない（must）。利用者と関連付けられたセキュリティに関連しない任意の属性が、TSS 中に特定される必要はない。

インタフェース仕様

TSS 中に特定された利用者セキュリティ属性を考慮して、評価者はインタフェース仕様を参照しどのインタフェースが FIA_ATD.1 をサポートしているかを判断する。開発者には、FIA_ATD.1 へ対応付けられるものを含め、I&A 機能へのインタフェースの対応付けを提供することが要求され、また評価者は TSS に特定されたセキュリティ属性を作成、閲覧、変更、及び削除するために利用できる手法の記述が、セキュリティ機能記述中に提示されていることを確証する。

該当するインタフェースの例としては、利用者を作成及び削除するために使われるもの、さらには既存の利用者のセキュリティ属性のいずれかを変更する（例えば、グループの追加／削除、パスワードの変更）ために利用できる任意のインタフェースなどが挙げられる。

しかし、通知されたインタフェースであってその記述がセキュリティ属性の作成または変更が行えることを示しているのに FIA_ATD.1 に対応付けられていないものを発見した場合には、評価者は開発者と協力してこの不一致を解決しなくてはならない（must）。他方では、FIA_ATD.1 中に特定されていない（すなわち、セキュリティ関連ではない）属性を操作するインタフェースを評価者が発見した場合、さらなるアクションは必要とされない。

これは製品の主張されたセキュリティ機能の範囲外となるためである。

利用者操作ガイダンス

評価者は、利用者セキュリティ属性の作成、閲覧、変更、及び削除に関する管理ガイダンスが、全体として（例えば、利用者の作成／削除）または部分的に（例えば、パスワードの変更）、FIA_ATD.1 と一貫していることを判定する。評価者は、少なくとも利用者の作成及び削除に関する指示を見つけ出すべきである（should）。1 つ以上の利用者セキュリティ属性を個別に操作するための追加的な指示が利用できてもよく、利用できる場合には特定されるべきである（should）。

管理ガイダンス中の、利用者の作成または初期定義に用いられるインタフェースの記述は、作成時に割り当て可能な必要とされる利用者属性のそれぞれを特定するために役立つべきである（should）。個別のセキュリティ属性を操作するために用いられる任意のインタフェースの記述は、該当する属性を明確に特定すべきである（should）。

テスト

FMT_MTD.1(IAU) を参照されたい。ここでは該当する制約と共に利用できるインタフェースがテストされる。

FIA_UAU.1(RITE)：認証のタイミングに関する保証アクティビティ

TOE 要約仕様（TSS）

評価者は TSS を調査し、リモート IT 認証をサポートするものと、リモート IT エンティティが認証される前に許可される可能性のあるものの両方について、情報フローが特定されていることを判定しなくてはならない（shall）。FDP_IFC／FDP_IFF 要件の実装方法に関する TSS 中の情報は、これらの要件を満たすように実装されるメカニズムによって何が許可されるかを詳述することになるため、この情報の重要な部分となる。TOE が運用利用のために構成される際、許可されるプロトコルは FDP_IFC／FDP_IFF を実装する機能によってサポートされるパラメタの構成によって決定されることになるため、リモート IT エンティティの認証前に何が許可され何が許可されないのかの項目別のリストを提供することは可能ではないかもしれない。しかし、評価者は TSS 中に提供される情報によって読者が FDP_IFC／FDP_IFF 要件をサポートする構成メカニズムと、その結果として生ずる能力及び機能であって認証前にリモート IT エンティティに利用可能であるものとの関係を理解できることを判定しなくてはならない（shall）。

インタフェース仕様

リモート IT エンティティによって用いられるインタフェースは、FDP_IFC.1、FDP_IFF.1、及び FTP_ITC.1 に関する保証アクティビティによってカバーされる。

利用者操作ガイダンス

操作ガイダンスには、構成と TOE がリモート IT エンティティからの情報を受け入れる際のルールとの関係、及びエンドポイントが認証されていることを必要とせずにフローを受け入れることの影響を記述する情報が含まれるべきである（should）。管理者が（提供されたガイダンスに基づいて）FDP_IFC／FDP_IFF 要件を満たすために実装されたルールの構成への反応として TOE によって行われることになる処理（許可されるサービスに関して、例えば ICMP の通過を許可することによりリモートエンティティは認証されていなくても TOE を「ping」できるようになる）を判定することは可能であるべきである（should）。

また管理ガイダンスはリモート認証をサポートするための TOE の構成をカバーすることになる。評価者は、操作ガイダンスを調査して、認証の前に必要となる準備的なステップ（例えば、事前共有鍵、トンネル、証明書などの資格情報資料の確立）があれば、それが記述されていることを判定しなくてはならない（shall）。サポートされている認証手法のそれぞれについて、認証を成功するための明確な指示が操作ガイダンスに提供されていることを評価者は確証しなくてはならない（shall）。これらの構成アクティビティのすべてのうち一部は、FTP_ITC.1 に関する保証アクティビティ中でも対処される。

テスト

評価者は、サポートされているリモート認証手法のそれぞれについて、以下のテストを行わなくてはならない（shall）。

テスト 1：評価者は操作ガイダンスを用いて、そのログイン手法に関してサポートされている適切な資格情報を構成しなくてはならない（shall）。その資格情報／ログイン手法について、正しい認証関連情報の提供によってシステムへのアクセスが可能となる一方で、不正な情報の提供によってアクセスが拒否されることを評価者は示さなくてはならない（shall）。

この機能に関するテストは、FDP_IFC.1、FDP_IFF.1、及び FTP_ITC.1 に関するテストアクティビティ中でも対処されている。

FIA_UAU.1(HU)：認証のタイミングに関する保証アクティビティ

TOE 要約仕様（TSS）

RFC に規定された機能のスーパーセットを提供する利用者のリモート認証に用いられるプロトコルを TOE が実装している場合、あるいはそのプロトコルが RFC や他の公開された文書に規定されていない場合、利用者が認証される前に発生する実装されているプロトコルの部分が TSS に記述される。利用者がローカルに TOE へログオンする前に許可される割付中に列挙されるアクションのそれぞれについて、TOE によって提供される機能が TSS に記述されなくてはならない（shall）。

評価者は TSS を調査して、製品でサポートされるログオン手法のそれぞれ（ローカル、リモート（HTTPS、SSH など））が TSS に記述されていることを判定しなくてはならない（shall）。この記述には、許可される／用いられる資格情報、発生するあらゆるプロトコルのトランザクション、そして何が「認証の成功」に相当するのかに関する情報が含まれなくてはならない（shall）。

インタフェース仕様

評価者は、リモートとローカルの両方について、TOE への認証に用いられる TSFI を特定しなくてはならない（shall）。評価者は、これらのインタフェースを TSS 中に提供される情報と比較し、リモートユーザ（IT エンティティまたは人間）もしくはローカルユーザに関する認証手法が TSS に記述されているかどうかを判定し、そしてこの手法に対応するインタフェースが存在することを判定しなくてはならない（shall）。サービス（FDP_IFC／FDP_IFF 要件によってカバーされるものの他に）が利用者認証に先立って利用可能であると TSS に列挙されている場合、評価者はこれらのサービスへのインタフェースがインタフェース仕様中に特定されていることを確証する。

利用者操作ガイダンス

リモートユーザについては、利用者をリモートで認証することを許可する TOE の構成に関する情報が操作ガイダンスに含まれていなくてはならない（shall）。これには、利用者によって用いられる資格情報の確立と、プロトコルに応じた TOE 資格情報の構成が含まれてもよい。

テスト

評価者は、サポートされているローカル及びリモート認証手法のそれぞれについて、以下のテストを行わなくてはならない（shall）。

テスト 1：評価者は操作ガイダンスを用いて、そのログイン手法に関してサポートされている適切な資格情報を構成しなくてはならない（shall）。その資格情報／ログイン手法について、正しい認証関連情報の提供によってシステムへのアクセスが可能となる一方で、不正な情報の提供によってアクセスが拒否されることを評価者は示さなくてはならない（shall）。

テスト 2：認証に先立ってローカルユーザへ利用可能となる規定されたサービスのそれぞれについて、評価者はそのサービスが認証を必要とすることなく呼び出せることを確証しなくてはならない（shall）。

FIA_UAU.7：保護された認証フィードバックに関する保証アクティビティ

TOE 要約仕様（TSS）

利用者へ提供されるフィードバックが TOE の制御下にある認証手法のそれぞれについて、TSS には提供されるフィードバックがあいまい化されていること、及びあいまい化される方法（提供しない、マスクする、など）が示される。各認証手法が明示的にカバーされなくてはならず、またログイン手法だけではなく、例えばパスワードの変更などの「再認証」を必要とする手法も含まれなくてはならない。

インタフェース仕様

この情報は、認証機能に用いられるインタフェースの仕様によってカバーされる。

利用者操作ガイダンス

この機能に特有の追加情報は必要とされない。

テスト

評価者は、TSS に記述されたローカル認証の手法それぞれについて、以下のテストを行わなくてはならない（shall）。

テスト 1：評価者は、TOE へローカルな認証を行わなくてはならない（shall）。この試行を行っている間、評価者は認証情報を入力している間に高々あいまい化されたフィードバックしか提供されないことを検証しなくてはならない（shall）。

FIA_UAU.5：複数の認証メカニズムに関する保証アクティビティ

TOE 要約仕様（TSS）

評価者は、利用可能な認証メカニズムが TSS 中に特定されていることを見つけ出す。少なくとも、TSS には利用者名／パスワードベースの認証メカニズムと、FIA_UAU.5 中に割付

された任意のその他のメカニズムが記述されることになる。

また評価者は、利用者名／パスワードベースのメカニズム記述で、FIA_UAU.5.2c 中に選択されたものと一貫した方法でパスワードが期限切れとなる際の TOE のふるまいが説明されていることを見つけ出す。

複数の認証メカニズムが特定されている場合、評価者は、それぞれの場合にどの認証メカニズムが用いられるかを判定するルールを含め、追加的な認証メカニズムと関連付けられたルールを説明する記述をも見つけ出す。

インタフェース仕様

TSS 中の利用可能な認証メカニズムのリストを考慮して、評価者はインタフェース仕様を参照しどのインタフェースが FIA_UAU.5 をサポートしているのかを判断する。開発者は、インタフェースから I&A 機能への対応付けを、FIA_UAU.5 へ対応付けられるものも含めて提供することが求められ、また評価者は利用者の識別情報を認証するために利用可能な手法の記述と、これらの手法と関連付けられたルールとが、セキュリティ機能記述中に提示されていることを確証する。この記述には、認証手法の選択と、成功（例えば、新たなプロセスの作成）及び失敗（例えば、パスワードの期限切れ）条件の両方の結果が対処されるべきである（should）。

複数の認証手法が利用可能な場合、それらの手法のうち一部のみが特定のインタフェースに適用可能であることがあり得るため、このことは明確に特定されるべきである（should）。

しかし、通知されたインタフェースの記述が FIA_UAU.5 に対応付けられない認証手法を示していることを分析中に評価者が発見した場合、評価者は開発者と協力してこの不一致を解決しなくてはならない（must）。

他の一部の機能とは異なり、利用可能な認証手法が評価の文脈において無視されることは一般的には受容可能ではない。

利用者操作ガイダンス

評価者は、認証を要求する機能の管理ガイダンスが FIA_UAU.5 と一貫していることを判定する。評価者は少なくとも、初回のログイン中の認証に関する指示を見つけ出すべきである（should）。パスワードの変更や権限のアクティベートなど、認証を必要とする追加的な機能については追加的な指示が利用できるかもしれない。

複数の認証メカニズムへの TOE のサポートが構成可能である（例えば、ある認証メカニズムを有効にしたり、設定したりできる）場合、ガイダンスにはメカニズムの有効化／無効化、メカニズムの構成、メカニズムの利用のためのルールの定義、などに関する指示があってもよい。可能性は膨大であるため、ここでのアクティビティは追加的なバリエーションへ対処するために評価中に要件追加される必要があるかもしれない。

テスト

FIA_UAU.5 に関するテストアクティビティの大部分は、FIA_UAU.1 のものと連携して実施されるべきである（should）。FIA_UAU.1 に関するテストでは、認証試行の成功と失敗の両方が対処される必要がある一方で、評価者はさらに対応する試行の成功及び失敗が利用できる認証メカニズムのそれぞれの文脈で行われることを確実にしなくてはならない（shall）。それゆえ、評価者はテストの途上ですべてのあり得る認証メカニズムを構成し、そのメカニズムが呼び出されるとともに該当する各インタフェースについて成功と不成功

の両方の場合の結果が得られることを確実にしなくてはならない。

少なくとも、評価者は利用者名／パスワードベースの認証をサポートする各インタフェースについて、利用者パスワードが期限切れの場合に認証試行が失敗することもテストしなくてはならない（shall）。おそらく、評価者は上記のテストによってパスワードが期限切れとなっていない場合に認証試行が成功することはすでにテストしているだろう。

追加的な認証メカニズムを割り当てる可能性を考慮して、この保証アクティビティは追加的な可能性に対処するため評価中に要件追加される必要があるかもしれない。

FIA_UID.1 識別のタイミングに関する保証アクティビティ

FIA_UAU.1 を参照

FIA_USB.1 利用者・サブジェクト間の束縛に関する保証アクティビティ

TOE 要約仕様（TSS）

評価者は、各サブジェクトと関連付けられる利用者セキュリティ属性を、TSS 中に列挙されたものの中から見つけ出すことになる。利用者のセキュリティ属性のリストは FIA_USB.1 に特定されているものとは違っていてもよく、また FIA_USB.1 において割り当てられた追加的な利用者セキュリティ属性の文脈における最小セットを拡張するために使われてもよい。TSS 中に特定された利用者セキュリティ属性のリストが FIA_USB.1 中のものと異なっている場合、要求される利用者セキュリティ属性の関連付け及びカバレージを示す明確な対応付けが TSS に提供されなくてはならない（must）。サブジェクトと関連付けられたセキュリティに関連しない任意の属性が、TSS 中に特定される必要はない。

FIA_USB.1 がアクセス制御判定、セキュリティ管理の制限、及び監査に関連した利用者のセキュリティ属性の割り当てをサポートしている一方で、そのような属性が利用者セキュリティ属性の最小セット（利用者識別情報、グループ、及び役割）を拡張する場合、それらは SFR にのみ特定される必要がある。それとは関係なく、評価者は特定された利用者セキュリティ属性のすべての関連付けが、アクセス制御、セキュリティ管理の制限、及び監査に関連した他の SFR の文脈において TSS に記述されていることを見つけ出す。換言すれば、必要とされる利用者セキュリティ属性のそれぞれの使用は、少なくとも 1 つのセキュリティ機能との関連において TSS 中に記述されることになる。

評価者は、利用者セキュリティ属性がサブジェクトへ割り当てられる方法の記述を見つけ出す。この記述には、新たなサブジェクトへ最初に利用者セキュリティ属性が割り当てられる方法、利用者セキュリティ属性が変更できるかどうか及びその方法、そしてサブジェクトと関連付けられる追加的なセキュリティ属性があればその方法が記述される。この記述は、FIA_ATD.1 に特定される利用者セキュリティ属性と、FIA_USB.1 に特定されるセキュリティ属性とのすべての関連を定義するために役立つ。また、この定義は各サブジェクトに関連するセキュリティ属性の最初の割り当てと変更に関連するすべてのルールを定義することになる。

異なるセキュリティ属性を持つ可能性のある、複数のサブジェクトの種類が存在する場合、TSS にはこれに応じたすべての場合が記述される。

インタフェース仕様

TSS 中に特定された利用者セキュリティ属性を考慮して、評価者はインタフェース仕様を参照しどのインタフェースが FIA_USB.1 をサポートしているかを判断する。開発者には、

FIA_USB.1 へ対応付けられるものを含め、I&A 機能へのインタフェースの対応付けを提供することが要求され、また評価者はサブジェクトを作成しサブジェクトと関連付けられたセキュリティ属性を変更するために利用できる手法の記述が、セキュリティ機能記述中に提示されていることを確証する。

インタフェースは間接的な（例えば、利用者のログインの結果としてプロセスが作成される）可能性も直接的（例えば、新たなプロセスのフォーク）な可能性もあるが、いずれの場合であってもこれらは特定され記述される必要があることに注意されたい。

さらに、サブジェクトと関連付けられたセキュリティ属性が変更できない可能性もあり、この場合には該当するインタフェースの特定や対応付けは必要はない（should not）。

評価者は、特定されたインタフェースのそれぞれについて、最初のセキュリティ属性の割り当て及びその後の変更に関するルールが、TSS に記述され、セキュリティ機能記述にも記述されているとともに TSS と一貫していることを確証しなくてはならない（shall）。

該当するインタフェースとしては、ログインに用いられるインタフェース、プロセスへのインタフェース、ならびに既存のサブジェクトのセキュリティ属性のいずれかを変更するために利用可能な任意のインタフェース（例えば、特権の有効化／無効化、実または実効利用者またはグループ識別子の変更など）などが挙げられる。

しかし、通知されたインタフェースであってその記述が利用者・サブジェクト間束縛機能を示しているのに FIA_USB.1 に対応付けられていないものを発見した場合には､評価者は開発者と協力してこの不一致を解決しなくてはならない（must）。他方では、FIA_USB.1 中に特定されていない（すなわち、セキュリティ関連ではない）属性を操作するインタフェースを評価者が発見した場合、さらなるアクションは必要とされない。これは製品の主張されたセキュリティ機能の範囲外となるためである。

利用者操作ガイダンス

評価者は、サブジェクトの作成及びサブジェクトと関連付けられたセキュリティ属性の変更に関する管理ガイダンスが、FIA_USB.2 と一貫していることを判定する。評価者は、少なくともログイン（利用者のプロセスを作成するもの）の指示を見つけ出すべきである（should）。サブジェクトの 1 つ以上のセキュリティ属性を操作するための追加的な指示が利用できてもよく、利用できる場合には特定されるべきである（should）。

サブジェクトのセキュリティ属性を操作するために用いられる任意のインタフェースの記述は、該当する属性を明確に特定すべきである（should）。

テスト

TOE のふるまいを検証するために用いられるテストの数が､利用者セキュリティ属性の数､これらへのアクセスを提供するインタフェース、そして関連する制限の複雑さに依存するのはもちろんである。評価者には、関連する利用者セキュリティ属性と、これらに最初の割り当て及びその後の変更を行うために利用できるインタフェースとを関連付けるマトリックスを作成することが推奨される。場合によっては、UNIX の『setuid』などの機能のように、属性のグループに対して同時にインタフェースが作用する場合、利用者セキュリティ属性は集合的に取り扱われるかもしれないことに注意されたい。

さらに、特定のルールへの対応付けをマトリックスへ追加して、利用者属性、インタフェース､そしてルールという三つ組みを作成するべきである（should）。ルールは一般的には、

挙動と制約という 2 つの種類に分類されるべきことに注意されたい。挙動ルールは、どのように割り当てや変更が行われるかを記述するために役立つが、例えばどの利用者または役割が操作を行えるかといった制限には役立たない。制約ルールは、例えば可能な属性の範囲または変更を行える役割といった、割り当てや変更の制限を記述するために役立つ。

属性／インタフェース／ルールの三つ組みを考慮して、評価者は制約的なルールの場合のそれぞれについて、以下のテストを行わなくてはならない（shall）。

1. 特定された操作を行うための特定されたルールを満たす最低限必要とされる条件を用いて、特定されたセキュリティ属性を割り当てまたは変更するために、管理ガイダンス中の指示を用いて特定された操作を行う。操作は成功するはずである（should）。評価者は、代替インタフェースを用いて操作が実際に成功したこと、及び該当するセキュリティ属性が割り当てまたは変更されていることを検証すべきである（should）。場合によっては、評価者は他のテスト（例えば、アクセス制御、セキュリティ管理の制約、または監査に関連したものなど）を参照または増強して、結果としてセキュリティ属性が期待通り変更されていることを検証できるはずである（should）。
2. 特定された操作を行うための特定されたルールを満たす最低限必要とされる条件を除いたすべての条件を用いて、特定されたセキュリティ属性を割り当てまたは変更するために、管理ガイダンス中の指示を用いて特定された操作を行う。操作は、適切なエラーと共に失敗するはずである（should）。評価者は、代替インタフェースを用いて操作が実際に成功しなかったこと、及び該当するセキュリティ属性が代入または変更されていないことを検証すべきである（should）。場合によっては、評価者は他のテスト（例えば、アクセス制御、セキュリティ管理の制約、または監査に関連したものなど）を参照または増強して、結果としてセキュリティ属性が期待通り変更されていることを検証できるはずである（should）。
    a. このテストは、複数の制約的な条件がルールに規定されている場合には、それぞれの条件が実際に強制されることを確実にするために、繰り返されるべきである（should）。これは、すべての条件に対して、その 1 つの条件だけが満たされない状態でテストを行うことによって達成できる。

属性／インタフェース／ルールの三つ組みを考慮して、評価者は挙動的なルールの場合のそれぞれについて、以下のテストを行わなくてはならない（shall）。

1. 挙動的ルールにしたがって特定されたセキュリティ属性を割り当てまたは変更するために、管理ガイダンス中の指示を用いて特定された操作を行う。操作は成功するはずである（should）。評価者は、代替インタフェースを用いて操作が実際に成功したこと、及び該当するセキュリティ属性が割り当てまたは変更されていることを検証すべきである（should）。場合によっては、評価者は他のテスト（例えば、アクセス制御、セキュリティ管理の制約、または監査に関連したものなど）を参照または増強して、結果としてセキュリティ属性が期待通り変更されていることを検証できるはずである（should）。
    a. このテストは、複数の挙動的ルールのコンポーネントがルールに規定されている場合には、それぞれの挙動的な条件が期待通りに働くことを確実にするために、繰り返されるべきである（should）。これは、すべての条件に対して、場合ごとになるべく少ない条件を指定することによって達成できる。
    b. このテストは、制約的なルールに関するテストの文脈で、1 つ以上の対応する挙

動的な条件が暗黙に指定されている場合、すでに対処されている可能性があることに注意されたい。

サブジェクトに関連付けられたセキュリティ属性は、一般的には他の要件の文脈でテストされることが期待される。しかし評価者は、アクセス制御、セキュリティ管理の強制、及び監査のテストの組み合わせにおいて、すべてのセキュリティ属性が対処されていることを確実にしなくてはならない（shall）。該当するセキュリティ属性をすべて確実にカバーするためには、追加的なテストが開発される必要があるかもしれない。

上記のテストはセキュリティ属性への割り当て及び変更が TSS、セキュリティ機能記述、及び管理ガイダンスに基づいて期待通り行われることを検証するためには役立つはずだが（should）、すべての最初の、または変更されたセキュリティ属性への割り当ての後、すべての影響されるセキュリティ機能（アクセス制御、セキュリティ管理の強制、及び監査）を包括的に評価者がテストすべきであるとは要求されていないし、期待されてもいない。基本的な考えは、セキュリティ属性の使用が他の該当するセキュリティ機能の文脈においてテストされることであり、ここでは割り当て及び変更が、正確かつ許可された場合にのみ行われるかどうかに焦点が絞られている。

FIA_PK_EXT.1 公開鍵及び FMT_MTD.1(CM) TSF データの管理に関する保証アクティビティ

TOE 要約仕様（TSS）

TSF が公開鍵の使用をサポートしていることを示すために、評価者は TSS に下記の情報が記述されていることを確証しなくてはならない（shall）。

RFC 5280 にしたがった X.509v3 証明書が用いられる場合：

- RFC 5280 の各セクションについて、「しなくてはならない（MUST）」ではない（例えば、「してもよい（MAY）」、「すべきである（SHOULD）」、「すべきではない（SHOULD NOT）」など）あらゆる言明は、標準のその特定の部分を TOE が実装しているかどうか読者が判断できるように、記述されなくてはならない（shall）。
- RFC 5280 の各セクションについて、「しなくてはならない（MUST）」または「すべきである（SHOULD）」言明への不適合があれば、それは記述されなくてはならない（shall）。

TOE に特有の拡張または標準に含まれていない処理であって、TOE が強制すべきセキュリティ要件に影響するかもしれないものがあれば、記述されなくてはならない（shall）。

鍵マテリアルがロード可能であり直接取り扱われる（例えばデジタル証明書なしで鍵が利用される）場合、どの鍵マテリアルの管理の手法が TOE でサポートされているか、及び鍵マテリアル管理操作を行うにはどの条件が満たされる必要があるかについて、TSS に記述されなくてはならない（shall）。

TSS には、実装された公開鍵及び秘密鍵のストアであって、本 PP の要件を満たすために用いられる鍵を含むもののすべてが記述されなくてはならない（shall）。この記述には、これらの鍵がストアへロードされる方法、及び不正なアクセスからストアが保護される方法に関する情報が含まれなくてはならない（shall）。より正確に言えば、リモート IT エンティティの認証に用いられるこれらの鍵マテリアルは管理ユーザによってのみ管理可能で

あるが、信頼されない利用者には自分の使用する鍵を管理する能力があってもよい。

インタフェース仕様

TOE に提供されるインタフェースの集合には、鍵／証明書をロードし管理する方法を規定するものが含まれることになる。TOE に認証局（CA）またはその他の高信頼エンティティから証明書をインポートする能力がある場合、この含まれるインタフェースのセットには高信頼エンティティから鍵マテリアル／証明書をインポートできるように TOE を構成する方法が記述される。またこれには、CA と通信するための高信頼チャネルを設定する方法が含まれてもよい。

利用者操作ガイダンス

操作ガイダンスは管理者へ、鍵マテリアル／証明書をインポートするように TOE を構成する方法に関する指示を提供する。証明書のインポートは CA からであってもよく、また CA が認証されており通信パスが保護されていること（例えば、高信頼チャネル）を確実にする構成ステップを要求してもよい。また、その他の鍵マテリアルを高信頼エンティティからインポートするためにも、このエンティティの認証と高信頼チャネルを介した鍵マテリアルの転送が必要とされる。

またガイダンスには、鍵マテリアルを手作業で（例えば、ポータブルな媒体によって）ロードする方法も管理者へ指示される（これが TOE によってサポートされている場合）。

TOE にあらかじめ鍵または証明書がプリロードされている場合には、ガイダンスによってこれらを管理する方法が管理者へ指示される。多くの場合、このガイダンスは手作業でロードされる鍵または証明書にも該当するか、あるいは CA からインポートされるものにも該当するであろう。ガイダンスには、証明書の信頼関係を有効化または無効化する方法もカバーされる（これが該当する場合）。

テスト

評価者は、TSS 中に記述される実装に適合した鍵マテリアルを TOE が処理することを示すテストを考案しなくてはならない（shall）。

証明書が用いられる場合、評価者は標準及び TSS 中に規定されるように認証パスを形成でき、また標準に規定されるように証明書を検証（CRL の処理を含めた認証パス検証）できなくてはならない（shall）。

評価者は、認証に公開鍵暗号化の使用を要求するシステム内の機能のそれぞれについて、以下のテストを行わなくてはならない（shall）。

テスト 1：証明書が用いられる場合：評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗することを例証しなくてはならない（shall）。次に評価者は、その機能で使われるべき証明書の検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを例証しなくてはならない（shall）。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなくてはならない（shall）。

証明書が用いられない場合：評価者は、この利用者の認証に用いられる鍵が定義されていないか、認証パートナーによって正しくない鍵が用いられている場合、認証が失敗することを例証しなくてはならない（shall）。次に評価者は、その利用者のための鍵をロードし、この鍵を利用した際に認証が成功することを示さなくてはならない（shall）。次に評価者は、その利用者のための鍵を削除（または無効化）し、認証が失敗することを示さなくて

はならない（shall）。

テスト 2：評価者は、操作ガイダンスを用いて証明書／鍵をネットワークデバイスから、また TOE がサポートするポータブル／リムーバブル媒体（例えば、ローカルな CA、ファイルサーバ、USB スティック、CD）からロードすることを試行しなくてはならない（shall）。

テスト 3：評価者は、FTP_ITC.1.3 に特定される機能をサポートするリモート IT エンティティと関連付けられた鍵／証明書の管理を試行する。これらのエンティティについて、管理者の権利を用いてこれらの鍵／証明書を「信頼できる」ものとしたり「信頼できない」ものとしたりできることを確証する。逆に、必要とされる権利以外のすべてを用いて、評価者は信頼関係の変更を試みる。結果は試行の失敗とならなくてはならない（shall）。

FMT_MOF.1 セキュリティ機能のふるまいの管理に関する保証アクティビティ

TOE 要約仕様（TSS）

TSS には、パスワードについて強制される特徴が記述されなくてはならず、またこの強制が行われる点も記述されなくてはならない。

インタフェース仕様

パスワード強制機能を構成するために用いられるインタフェースが特定される。またパスワードを変更するために用いられるインタフェースも特定され、評価者はこれらのインタフェースが FIA_UAU 要件中のパスワードベースの認証に用いられるものと対応していることを確証する。

利用者操作ガイダンス

操作ガイダンスには、利用できるパスワードの特徴、強制メカニズムの設定に関する指示、及び「強い」パスワードと推奨される最小設定についての議論が記述されなくてはならない（shall）。

テスト

評価者はまた、下記のテストを実施しなくてはならない（shall）。単一のテストケースについて、これらのテストの 1 つ以上が実施可能であることに注意されたい。

テスト 1：評価者は、要件を満たすものと、何らかの点で要件を満たさないものと、両方のパスワードを作成しなくてはならない（shall）。それぞれのパスワードについて、評価者は TOE がそのパスワードをサポートしていることを検証しなくてはならない（shall）。評価者にはパスワードのすべての可能な組み合わせをテストすることは求められない（それは不可能でもある）一方で、評価者はすべての文字、ルールの特徴、及び要件に列挙された最小の長さがサポートされていることを確証し、さらにこれらの文字のサブセットをテストに選んだことを正当化しなくてはならない（shall）。

テスト 2：評価者は、パスワードの特徴の特定の組み合わせでパスワードが作成されることを要求するルールを設定し、次にこのパスワードの使用を試みなくてはならない（shall）。特徴の組み合わせは、特徴の幅をカバーしなくてはならないが、必ずしもすべての組み合わせでなくてもよい。評価者は、有効な（ルールにしたがった）ものと無効な（ルールに適合しない）組み合わせの両方を含めることによって、有効なパスワードが受容され無効なパスワードは拒否されることを確認しなくてはならない（shall）。このテストを行うに

あたって、評価者はパスワードの変更を許可するすべてのインタフェースが行使されることを確実にしなくてはならないが、各インタフェースについてすべてのケースが実行される必要はない。

テスト 3：評価者は、パスワードの変更が許可されると規定されたグループのメンバーでない状態でパスワードの構成を試み、パスワードルールの構成が不可能であることを確認しなくてはならない（shall）。

FMT_MTD.1(IAT) TSF データの管理に関する評価アクティビティ

この SFR に関する保証アクティビティは、これと直接関係する FIA_AFL.1 の要件内に含まれている。

FMT_MTD.1(IAF) TSF データの管理に関する評価アクティビティ

この SFR に関する保証アクティビティは、これと直接関係する FIA_AFL.1 の要件内に含まれている。

FMT_MTD.1(IAU) TSF データの管理に関する評価アクティビティ

TOE 要約仕様（TSS）

関連する利用者セキュリティ属性は、FIA_ATD.1 に関する保証アクティビティ内で特定されている。

さらに評価者は、特定された利用者セキュリティ属性のそれぞれの作成（初期化）、閲覧、変更、及び削除に適用される制約が TSS に記述されていることを見つけ出さなくてはならない（shall）。追加的または代替的な操作が利用できる場合、TSS によってこれらは FMT_MTD.1(IAU) に特定される制御された操作へ対応付けられなくてはならない（must）。制約には、利用者セキュリティ属性のそれぞれに関して、特定の操作を行うことのできる役割、または特定の操作を行えるかどうかを判定するルール、あるいはその両方が、特定されなくてはならない（shall）。制約の記述では、例えば利用者の作成または削除といった利用者のセキュリティ属性を集合的に操作する手法と、例えばパスワードの変更やグループのメンバシップまたは役割の追加／削除といった利用者のセキュリティ属性を個別に（またはグループとして）操作する手法の両方が、必ず対処されなくてはならない（must）。

インタフェース仕様

関連するインタフェースは、FIA_ATD.1 に関する保証アクティビティ内で特定されている。さらに評価者は、特定されたインタフェースのそれぞれについて制約が TSS に記述され、セキュリティ機能記述にも記述されているとともに TSS と一貫していることを確証しなくてはならない（shall）。

利用者操作ガイダンス

関連するガイダンスは、FIA_ATD.1 に関する保証アクティビティ内で特定されている。

しかし、上記のルールが変更対象である場合には、ガイダンスには必要なあらゆる指示が提供されなくてはならない（must）。そのような可能性が幅広い性質のものであることを考慮すれば、所与の TOE の文脈において利用者セキュリティ属性へのアクセスに関するルールが変更可能である場合には、このアクティビティは再考が必要とされるであろう。

管理ガイダンスが該当する制約を特定すべきであるとは必ずしも期待されないが、特定さ

れる場合であって評価者が管理ガイダンスと TSS またはセキュリティ機能記述との間に矛盾を見つけ出した場合には、評価者は開発者と協力してこの不一致を解決しなくてはならない（must）。

テスト

TOE のふるまいを検証するために用いられるテストの数が、利用者セキュリティ属性の数、これらへのアクセスを提供するインタフェース、そして関連する制限の複雑さに依存するのはもちろんである。評価者には、関連する利用者セキュリティ属性と、これらを作成、閲覧、変更、または削除するために利用できるインタフェースとを関連付けるマトリックスを作成することが推奨される。場合によっては、利用者の作成または削除の際に行われるように、属性のグループに対して同時にインタフェースが作用する場合、利用者セキュリティ属性は集合的に取り扱われるかもしれないことに注意されたい。さらに、役割またはルールに基づいた特定の制約への対応付けをマトリックスへ追加して、利用者属性、インタフェース、そして制約という三つ組みを作成するべきである（should）。

属性／インタフェース／制約の三つ組みを考慮して、評価者は制約が役割に関連する場合のそれぞれについて、以下のテストを行わなくてはならない（shall）。

1. その操作を行うことが許可された役割で特定されたセキュリティ属性を操作するために、管理ガイダンス中の指示を用いて特定された操作を行う。操作は成功するはずである（should）。評価者は、代替インタフェースを用いて操作が実際に成功した（例えば、利用者が実際に作成または削除された）ことを検証すべきである（should）。
2. その操作を行うことが許可されていない役割で特定されたセキュリティ属性を操作するために、管理ガイダンス中の指示を用いて特定された操作を行う。操作は、適切なエラーと共に失敗するはずである（should）。評価者は、代替インタフェースを用いて操作が実際に成功しなかった（例えば、利用者が実際に作成または削除されなかった）ことを検証すべきである（should）。

属性／インタフェース／制約の三つ組みを考慮して、評価者は制約がルールに関連する場合のそれぞれについて、以下のテストを行わなくてはならない（shall）。

1. 特定された操作を行うための特定されたルールを満たす最低限必要とされる条件を用いて、特定されたセキュリティ属性を操作するために、管理ガイダンス中の指示を用いて特定された操作を行う。操作は成功するはずである（should）。評価者は、代替インタフェースを用いて操作が実際に成功した（例えば、利用者のパスワードが実際に変更された）ことを検証すべきである（should）。
2. 特定された操作を行うための特定されたルールを満たす最低限必要とされる条件を除いたすべての条件を用いて、特定されたセキュリティ属性を操作するために、管理ガイダンス中の指示を用いて特定された操作を行う。操作は、適切なエラーと共に失敗するはずである（should）。評価者は、代替インタフェースを用いて操作が実際に成功しなかった（例えば、利用者のパスワードが実際に変更されなかった）ことを検証すべきである（should）。
    a. このテストは、複数の条件がルールに規定されている場合には、それぞれの条件が実際に強制されることを確実にするために、繰り返されるべきである（should）。これは、すべての条件に対して、その 1 つの条件だけが満たされない状態でテストを行うことによって達成できる。

FPT_STM.1 及びFTA_SSL に関する保証アクティビティ

FPT_STM.1 高信頼タイムスタンプに関する保証アクティビティ

TOE 要約仕様（TSS）

評価者は TSS を調査して、監査事象の記録、セッションタイムアウト、及び X.509 証明書の失効を含む､時刻を利用する各機能が TSS に列挙されていることを確証しなくてはならない（shall）。TSS には、どのように時刻が維持管理され、そして時刻に関連する各機能の文脈において高信頼とみなされるかについての記述が提供される。これには、時刻へアクセスするために機能が内部インタフェースを利用するか、あるいは外部から可視なインタフェースを利用するかの指摘が含まれるだろう。

評価者は TSS を調査して､システム時刻が高信頼であり単調増加することを確実にするためにどのように維持管理されているのかについての理解を得なくてはならない（shall）。

TOE が、NTP サーバのような外部ソースから時刻を受け取ることができる場合、TSS にはこの通信パスが保護される方法（例えば、IPsec、TLS）が記述され、管理者の定義により認証された IT エンティティのみが時刻を変更できることが確証される。

インタフェース仕様

すべての利用者／アプリケーションがシステム時刻を取得／読み出すことができるインタフェースが存在すべきである（should）。また、ローカルなシステムクロックを設定するために用いられるインタフェースも存在することになる。評価者は、これらのインタフェースを使って時刻を取得し設定する方法がインタフェース仕様に記述されていることを確証する。時刻の設定に関するインタフェース記述には、時刻を設定するためにどんな権利または特権を呼出し者が持たなくてはならないか、規定されるべきである（should）。

TOE が外部エンティティから時刻を受信することをサポートしている場合､インタフェース仕様には時刻を受信するために用いられるインタフェースが記述される。これは、手作業でのアクティビティで行うこともできるし、あるいは周期的に更新を要求するように構成された機能が存在してもよい。

時刻機能と関連付けられたインタフェースを調査する際、評価者はインタフェースの記述が､システム時刻の設定に関して TSS に言明されているものと一貫していることを確証する。

利用者操作ガイダンス

評価者は、操作ガイダンス（これは該当するインタフェースに関するインタフェース仕様を参照しているかもしれない）を調査して、管理者に時刻を設定する方法が指示されていることを確証する。

TOE が外部エンティティを用いて時刻の受信または更新を行うことをサポートしている場合、操作ガイダンスには認証済みのエンティティから時刻を受信するために TOE を設定する方法に関する管理者ガイダンスが提供される。このガイダンスでは、時刻の完全性を危殆化させるおそれのある攻撃から通信パスを確実に保護する方法についての指示が提供されるべきである（should）。例えば、TOE が NTP サーバを利用できるとき、ガイダンスには管理者へ NTP クライアントの構成方法が指示されるだろうし､高信頼チャネルを利用して NTP サーバを認証し､チャネルを通過して転送される情報の完全性が維持されるか、

あるいは何らかの変更があった場合に検出されることを確実にするための方法が指示されるかもしれない。

テスト

テスト 1 : 評価者は、操作ガイドを用いて時刻を設定する。次に評価者は、利用できるインタフェースを使って時刻が正しく設定されたことを確認しなくてはならない（shall）。

テスト 2 : 評価者は、利用できるインタフェースを用いて、信頼されない利用者として時刻の設定を試みる。評価者は、時刻の変更ができてはならない（shall not）。

テスト 3 : [条件付き] TOE が NTP サーバの利用をサポートしており、FTP_ITC.1.3 中の割付が用いられて NTP が機能として割り当てられている場合、評価者は操作ガイダンスを用いて TOE 上に NTP クライアントを構成し、そして NTP サーバとの保護された通信パスを設定しなくてはならない（shall）。評価者は、NTP サーバが期待されたとおり時刻を設定することを確認する。TOE が NTP サーバとの接続を確立するために複数の暗号プロトコルをサポートしている場合、評価者はサポートされているプロトコルのそれぞれを用いてこのテストを行わなくてはならない（shall）。

FTA_SSL.1 TSF 主導のセッションのロック及び FTA_SSL.2 利用者主導のロックに関する保証アクティビティ

TOE 要約仕様（TSS）

評価者は TSS を調査して、インアクティブな時間間隔が経過した（例えば、キーボードまたはマウスのアクティビティがなく、画面へビデオをストリーミングしているアクティブなプログラムがなく、画面にポップアップされているダイアログボックスがない）ことを TOE がどのように判定しているのかを判定しなくてはならない（shall）。また TSS には、時間間隔を設定する能力を何が制御しているのか、そしてその時間間隔はグローバル（すなわち、システムワイド）なのか、それとも利用者のアカウントごとに構成可能なのかも記述される。

また評価者は、TSS の記述から、TOE がどのように画面を判読不能としているのか（例えば、利用者定義のスクリーンセーバーがアクティベートされる、時間間隔が経過した際に何が表示されるのかを管理者が制御する、システム定義の変更できない画面が表示される）を判定する。

評価者は TSS を調査して、どのアクティビティにシステムが反応するのか（例えば、キーボード上のキーの押下、マウスの動き、画面と対話するプログラム）が特定されていて、またアクティビティにシステムがどのように反応するのか、そして利用者に提示されるオプションは何か（例えば、セッションをロック解除するための認証資格情報を入力するダイアログボックス、別の利用者としてログインする能力、マシンをシャットダウンするオプション）が記述されていることを確証しなくてはならない（shall）。

最後に、評価者は TSS を調査して、利用者がロックされたセッションを開始する方法と、利用者がセッションのロックを開始した際に何が起こるのかが記述されていることを確認しなくてはならない（shall）。TSS が、タイムアウトが生じた際と全く同様の方法で振る舞うということもあり得る。そうでない場合、TSS にはふるまいの違いが記述される。

インタフェース仕様

評価者は、これらのコンポーネントと関連付けられたインタフェースに関するインタフェ

ース仕様を調査して、TSS によって定義されるシステム中に存在する機能が、インタフェース記述に言明されているものと一貫していることを判定しなくてはならない（shall）。最低でも、時間間隔の設定、セッションのロック、及びセッションのロック解除の能力を提供するインタフェースが存在すべきである（should）。

利用者操作ガイダンス

評価者は、利用者操作ガイダンスを調査して、インアクティビティ時間間隔を構成する方法が管理者に指示されていることを確証しなくてはならない（shall）。セッションがロックされている際に何が表示されるかを指定する手段を TOE が提供している場合、操作ガイダンスにはこれを行う方法が記述されており、そして評価者はこれが TSS 中に提供される記述と一貫していることを確証しなくてはならない（shall）。

評価者は、システムがアクティビティに反応する際に利用可能なオプション、及びこれらのオプションを利用者が呼び出す方法が、ガイドに記述されていることを確証しなくてはならない（shall）。

評価者は、利用者がセッションのロックを開始する方法がガイドに記述されていることを判定しなくてはならない（shall）。

テスト

評価者は、下記のテストを実施しなくてはならない（shall）。

テスト 1：評価者は操作ガイダンスにしたがって、コンポーネント中に参照されているインアクティビティ時間間隔をいくつかの異なる値に構成する。構成された時間間隔のそれぞれについて、評価者は TOE とのローカルな対話セッションを確立する。次に評価者は、セッションが構成された時間間隔後にロックされ、データの残りがディスプレイ上に表示されていないことを確認する。

テスト 2：評価者は、利用できるインタフェースを用いて適切な権限を持たずに（信頼されない利用者として）タイムアウト時間の設定を試みる。評価者は、タイムアウト時間の変更の試みに失敗しなくてはならない（shall）。

テスト 3：[条件付き] タイムアウト時間を設定する能力を制御するメカニズムの複雑性に依存して、テスト 1 及びテスト 2 のバリエーションが必要となるかもしれない。管理者である必要があるという制約の場合、テストは単純明快であり、すでに記述したとおり行われる。特権またはアクセス制御メカニズムが関連している場合、評価者はタイムアウト時間を変更できる能力をテストする条件を判定する必要があることになる。そのような場合には、評価者はテスト者がタイムアウトを変更するための最小セットの特権またはアクセス制御設定を有していること、そしてタイムアウトの変更が成功することを確証する。次にテスト者は必要となる特権またはアクセス制御設定以外のすべてを有してタイムアウトの変更を試み、今回は失敗する。

テスト 4：評価者は、操作ガイダンス中に規定されているようにセッションのロック機能の開始を試みる。次に評価者は、セッションが構成された時間間隔後にロックされ、データの残りがディスプレイ上に表示されていないことを確認する。

テスト 5：次に評価者は、許可された認証手法のそれぞれについて、セッションのロック解除を試みた際に再認証が必要とされることを確証する。

高信頼パス／チャネルに関する保証アクティビティ

FTP_ITC.1 TSF 間高信頼チャネルに関する保証アクティビティ

背景

他の高信頼 IT 製品への高信頼チャネルを設定する機能は、OSPP に適合するオペレーティングシステムに必要とされる。オペレーティングシステムには、少なくとも SFR 中に必須のものとして列挙された暗号スイートを実装して、SFR から参照される標準に準拠した SSH、TSL、または IPsec プロトコルのうち少なくとも 1 つを実装することが必要とされる。これらの必須暗号スイートには、関連する RFC において「必要（REQUIRED）」と定義された追加的な暗号スイートが含まれるかもしれないことに注意されたい。

TOE 要約仕様（TSS）

期待

TSS（または TSS の参照する公的な文書）には、SFR 及び実装された標準中に規定されたプロトコルが、標準が異なるオプションを許可している場合には採用されるオプションを含めて、列挙される必要がある。

評価者のアクティビティ

評価者は、標準が正しく参照されていること、それらにプロトコルが完全に記述されていること、そして標準で保留されているオプションがあれば、それが TSS または TSS の参照する開発者文書において定義されていることを検証する。

機能仕様

期待

FTP_ITC.1 については、インタフェースはネットワークインタフェース及び高信頼チャネルの設定に用いられるインタフェースである。インタフェース仕様は、（標準が異なるオプションを許可している場合）採用されるオプションの記述と共に標準への参照によって定義されるプロトコル仕様である。利用者が高信頼チャネルを設定するために利用できるインタフェースについては、チャネルの設定に利用者が指定できるオプション、及びチャネルの制御方法がインタフェース記述に記述される必要がある。

注意：TSF が（信頼された管理者によって定義された構成にしたがって）自動的かつ利用者にトランスペアレントに高信頼チャネルを設定する場合には、高信頼チャネルを介した通信を開始するための明示的な利用者インタフェースは存在しないかもしれない。この場合、高信頼チャネルを介した通信をいつ開始するのか、及びどのオプションを用いるのかを判定するために TSF によって用いられる管理インタフェース（これは構成ファイルであるかもしれない）が存在しなくてはならない（must）。

評価者のアクティビティ

評価者は、利用者が高信頼チャネルを用いてリモート IT 製品との通信を開始できる利用者インタフェースが存在するか、あるいは管理者の定義した構成にしたがって高信頼チャネルを介した通信が TSF によって自動的に開始されるのかのどちらかであることを検証する。いずれの場合であっても評価者は、SFR 中に定義されたすべてのオプションと共に FTP_ITC.1 中に規定された高信頼チャネルプロトコルを用いて通信リンクが得られるこ

とを検証する。評価者は、これらのオプションが高信頼チャネルの開始時に選択できるか、あるいは管理インタフェースを介して定義される適切な構成と共に選択できるかのどちらかであることを検証する。

アーキテクチャ設計

期待

TSS に関して定義されるもの以外に、この SFR についてのアーキテクチャ設計に関する期待はこれ以上存在しない。開発者は、この機能をさらに詳細に説明するために、TSS 内で既存の公的な設計文書を参照することもできる。

評価者のアクティビティ

TSS において追加的な設計文書が参照されている場合、評価者はこれによって TSS 中になされた言明が正しく詳細化され、オブジェクトのセキュリティ属性が失効される方法が正しく記述されていることを検証する。

利用者ガイダンス（管理者及び「通常利用者」向け）

期待

ガイダンスには、高信頼チャネルを確立する方法と、高信頼チャネルの設定に用いられるパラメタが説明される必要がある。ガイダンスには、どのオプションを管理者または利用者が選択できるか、及びこれらのオプションが高信頼チャネルの確立及び維持にどのように影響するのかが記述される必要がある。特に、文書化される必要のあるプロトコルの一部として用いられる可能性のある暗号スイートを選択または除外するオプションは、設置によって暗号スイートをセキュアとみなされるもの、あるいは国家的または組織的方針に適合するために用いられる必要のあるものに限定することを可能とするために、文書化される必要がある。

評価者のアクティビティ

評価者は、FTP_ITC.1 中に定義されるプロトコルを、そこに定義されるすべてのオプションと共に用いて高信頼チャネルを設定する方法がガイダンスに記述されていることを検証する。このアクティビティは機能仕様の評定と大幅に重複しており、したがってインタフェースの評定と連携して行われるべきである（should）。

テスト

期待

評価者は、FTP_ITC.1 中に定義されるプロトコルを、リモート IT システムの認証についてのすべてのオプションと、FTP_ITC.1 中に定義される暗号スイートについてのすべてのオプションとともに、テストすることが期待される。テストは、プロトコルの一部として用いられる暗号アルゴリズムを含め、プロトコルが独立して実装されている製品への高信頼チャネルを TOE が設定及び維持できることを確実にするため、プロトコル及び暗号スイートの異なる実装を有する参照システムを用いて行われるべきである（should）。

評価者のアクティビティ

評価者は、テストにすべてのプロトコルと定義されたプロトコルオプションが含まれていることを検証する。評価者は、自分自身自身の参照システムを設定し、このシステムが

FTP_ITC.1 に列挙されたプロトコルの異なる実装を用いていることを確証する。評価者は、TOE のインスタンスへの高信頼チャネルの設定を試みることによって、自分自身のテストを行う。

このテストは、以下の場合をカバーしなくてはならない（shall）。

- TOE によってサポートされていないオプションの使用（例えば、リモートシステムの認証について）の試行。これらの試行は、失敗する必要がある。
- TOE によってサポートされているオプションを使用するが、不正な認証資格情報を提供した試行。これらの試行は、失敗する必要がある。
- 正しい認証資格情報及び正しいプロトコルのバージョンを用いるが、TOE によってサポートされていない暗号スイートを用いた試行。これらの試行は、失敗する必要がある。
- TOE によってサポートされていないプロトコルのバージョン（例えば、サポートされているプロトコルの古いバージョン）を用いた試行。これらの試行は、失敗する必要がある。
- TOE によってサポートされているプロトコルのバージョン、TOE によってサポートされている認証手法、正しい認証資格情報、及び TOE によってサポートされている暗号スイートを用いた試行。これらの試行は、成功する必要がある（ただし、ガイダンスまたは機能仕様に、期待された方法で試行を失敗させるような他の条件が定義されている場合を除く）。

CC の保証コンポーネントへの対応付け

概論

本プロテクションプロファイルの保証アクティビティは CCRA のスコープ中にあることが意図されているため、コモンクライテリアのパート 3 に列挙された保証コンポ—ネントへの対応付けが存在する必要があり、この章で提供される。この文書の以前の章で記述された SFR 関連保証アクティビティは、CC 及び CEM に定義された保証コンポーネント及びアクティビティの技術に特化した詳細化とみなされる。上記のとおり、CC のパート 3 に定義された特定の評価保証レベルに適合することは意図されておらず、また保証アクティビティはそのような既存の評価保証レベルをターゲットとせずに定義されている。

この文書ではここまで SFR 関連の保証アクティビティに焦点を当てていたため、SFR に関連しない保証の側面（ASE 及び ALC クラスからのものなど）はここまで対処されてこなかった。これらのクラスからのコンポーネントは以下に記述された下記の対応付けに含まれており、CC 及び CEM に定義されるように評価において考慮されるべきである（have to）。

選択された SAR コンポーネントは、評価（アクティビティ）のための追加的なガイダンスによってカバーされているもの、または作成グループにおける保証ニーズに関する議論の結果としてクライテリアから純粋に選択されたもののいずれかの分析の結果である。最初のセット（すなわち ADV、ATE、及び AVA クラス）は追加的なガイダンスのすべての詳細化に応じて新たな分析の対象となり、CCRA の条件のカバレージの下で最大限の労力が費やされる。選択されたコンポーネント以外のアクティビティも存在するが、より高度

または追加的なものは完全には満たされないため作成された保証パッケージの一部とはならないことには注意する必要がある（has to）。

以下のセクションは、本プロテクションプロファイルの一部として含まれる保証パッケージを提供するものである。これらのコンポーネント及び関連する評価保証アクティビティの目的における定義に関しては、はるかに具体的なアクティビティがこの文書には定義されていないため、CC 及び CEM を参照されたい。

ASE:

ASE_CCL.1、ASE_ECD.1、ASE_SPD.1 及び ASE_INT.1 は、CC 及び CEM 中の定義にしたがって要求される。

ASE.TSS.1 は含まれているが、TSS 中に提供されることが期待される情報に関して SFR 関連の保証アクティビティ中で大幅な詳細化が行われている。

ASE_OBJ.2 及び ASE_REQ.2 は、追加的な SFR が許可されている場合に要求されることになる（これは、少なくとも本プロテクションプロファイルを用いた最初の試行評価については当てはまらない）。

ADV:

ADV_ARC.1

注意：SFR 関連の保証アクティビティに関してこの文書に提供される記述によって、アーキテクチャ設計に関して大幅な詳細化が提供されている。

ADV_FSP.1

議論の中で、ADV_FSP.1 を越える必要性は認識されたが、ADV_FSP.2 のすべてのエレメントを含める必要性は認識されなかった。ここでの意図は、開発者によって提供されるすべての TSFI が、TSFI を用いたテストケースの開発の際にテストケースの開発や期待されるテスト結果の正しい特定のために用いることが可能な程度にまで、記述されることである。

注意：ADV_TDS ファミリのコンポーネントはこのマッピングに全く含まれていないが、本ドキュメントに記述された SFR 関連の保証アクティビティの記述からの設計関連の側面は、評価中に考慮する必要がある（have to）。ADV_TDS ファミリのコンポーネントが全く含まれていないのは、これらはいずれも本プロテクションプロファイルに適合した製品の設計評価の側面に必要とされる見方にそぐわないためである。

AGD:

含まれているコンポーネントは AGD_PRE.1 及び AGD_OPE.1 である。

SFR 関連の保証アクティビティには、ガイダンス中に見つけ出されることが期待される情報と、これらの側面が評価されるべき方法についての詳細化が含まれていることに注意されたい。

ALC:

含まれているコンポーネントは ALC_CMC.3、ALC_CMS.3、ALC_DEL.1、ALC_LCD.1 及

び ALC_FLR.3 である。

ADV_DVS.1 は含まれておらず、したがって ALC_CMC.3 からの依存性は満たされないことに注意されたい。しかし、評価者は ALC_CMC に関して開発者が記述した CM プロセスが記述どおりに確立されているかどうかを調査することが期待されている。これは、例えば記述されたプロセスの手順が評価者のオンサイトへの訪問中（例えば、独立テストを行うため）に適用されているかどうかを検証することによって、達成することができる。

ATE:

含まれているコンポーネントは ATE_COV.2、ATE_DPT.1、ATE_FUN.1、及び ATE_IND.2 である。

この文書には、SFR 関連のテストアクティビティに関する詳細化が含まれていることに注意されたい。評価終了時にすべての SFR が十分にテストされていることを評価によって確実にすることが必要だ、ということは、本プロテクションプロファイルを開発しているグループ内での合意である。すべての SFR がすべての関連する TSFI においてテストされたという十分な証拠が存在する限り、どの部分のテストがが開発者によって行われ、どの部分のテストが評価機関によって行われたか、などということは二次的な重要性しか持たない。

AVA:

含まれているコンポーネントは AVA_VAN.2 である。